MODULE 9

Serveur LDAP

Objectifs de ce module :

- ✓ ***Installation de LDAP***
- ✓ ***Configuration des fichiers reliés au serveur***
- ✓ ***Activer le serveur***
- ✓ ***Cas d'usage : Centralisation de l'authentification des comptes usagers.***

Table des matières

Objectifs

Ce module vous permettra de mettre en place un serveur LDAP. Ce module se concentrera sur l'utilisation du serveur dans un contexte d'authentification centralisé des usagers

Les objectifs principaux sont les suivants :

- Installer le serveur slapd (version openLDAP de Ubuntu)
- Configurer les fichiers principaux et connexes.
- Installer un gestionnaire de compte pour LDAP.
- Configurer les clients pour l'authentification pour le serveur LDAP.

Introduction

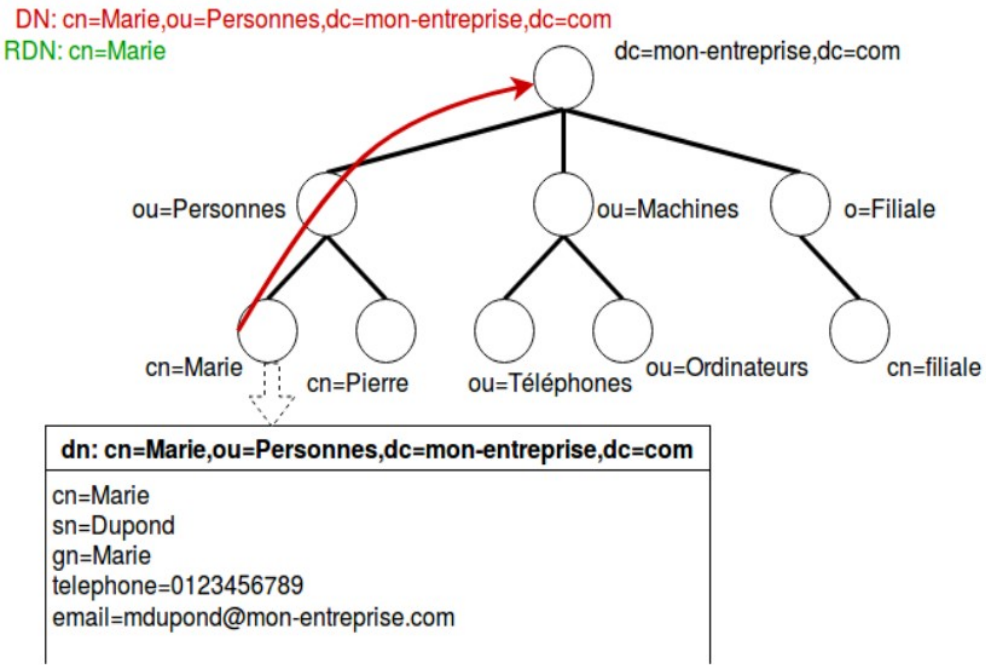
LDAP signifie "Lightweight Directory Access Protocol". C'est le standard pour accéder à un **annuaire**. Un annuaire est une base de données qui va contenir des informations sur des personnes, des machines, des groupes ou toute autre catégorie que vous pourriez imaginer.

Un annuaire se distingue d'une base de données relationnelle par le fait qu'il a une structure hiérarchique et qu'il est très rapide pour chercher et lire des éléments mais plus lent pour les modifier.

Les annuaires 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.). Toutes les applications de votre entreprise (site web, e-mail, comptes système des ordinateurs, etc.) peuvent par exemple utiliser ce service d'annuaire pour valider les identifiants de connexion.

Fonctionnement de LDAP

Tout d'abord, un annuaire LDAP est un 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 assigne des **valeurs**. Chaque entrée appartient au moins à une **classe d'objet** qui définit les attributs de l'entrée.

Par exemple, la classe d'objet "Employés" pourrait définir qu'un "élément" appartenant à cette classe doit contenir les attributs obligatoires :

- nom de famille
- prénom

et peut contenir les attributs facultatifs :

- e-mail
- téléphone
- date de naissance

Chacun des attributs de cet élément aura une valeur. Par exemple, "nom de famille=Dupond".

De nombreux attributs et classes d'objets sont pré-définis mais il est possible de définir les vôtres si besoin. L'ensemble des classes d'objets et attributs utilisés est défini dans le **schéma**. Certains attributs sont particulièrement courants et intéressants à connaître :

Attributs	Fonction
dc (domain component)	une partie d'un nom DNS. Pour une entreprise dont le nom de domaine serait "mon-entreprise.com", alors la racine du DIT aura l'air de "dc=mon-entreprise,dc=com"
cn (common name)	le nom commun. Pour une personne, c'est en général le prénom + le nom de famille
gn (given name)	le prénom
sn (surname)	le nom de famille
o (organization name)	pour une entreprise ce serait le nom de l'entreprise ou de la filiale
ou (organisational unit)	l'unité d'organisation. Pour une entreprise, ce serait le département (commercial, comptabilité, etc.)

Un attribut particulier est le **dn (distinguished name)**, c'est à dire le nom distinct. C'est 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.

Par exemple, le dn de "Marie Dupond" qui travaille chez "mon-entreprise.com" pourrait être "cn=Marie Dupond,ou=Personnes,dc=mon-entreprise,dc=com". On appelle **RDN**, pour **Relative Distinguished Name**, la partie "finale" propre à Marie. Ici le RDN serait "cn=Marie".

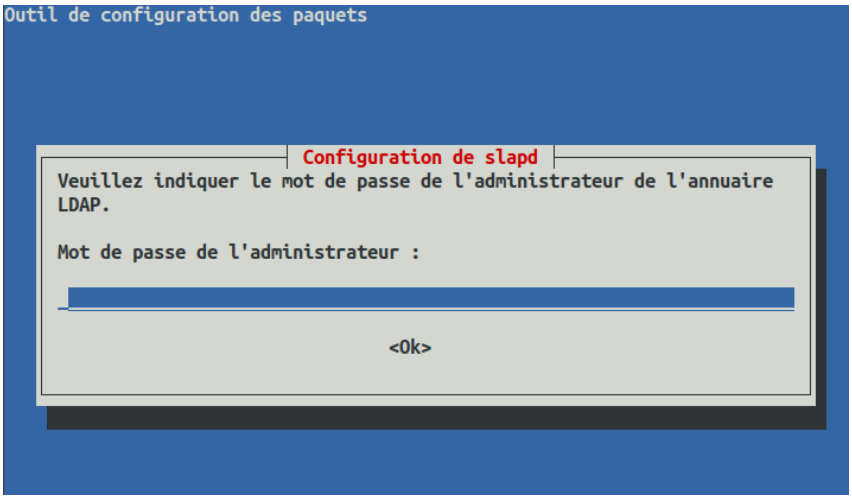
Installation du serveur LDAP dans Ubuntu (ou ses dérivés)

LDAP n'est pas installé par défaut sur une machine Linux Mint. On peut donc installer ce paquet avec le gestionnaire de paquet apt. Pour l'installer, il faut le paquet "slapd" ainsi que les utilitaires reliés à LDAP contenu dans le paquet "ldap-utils". On peut donc y arriver avec la commande suivante:

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

Note importante :
Le service LDAP est automatiquement démarré après son installation.

Après avoir fait la commande pour lancer l'installation, on vous demandera d'entrer le mot de passe de l'administrateur de votre annuaire.



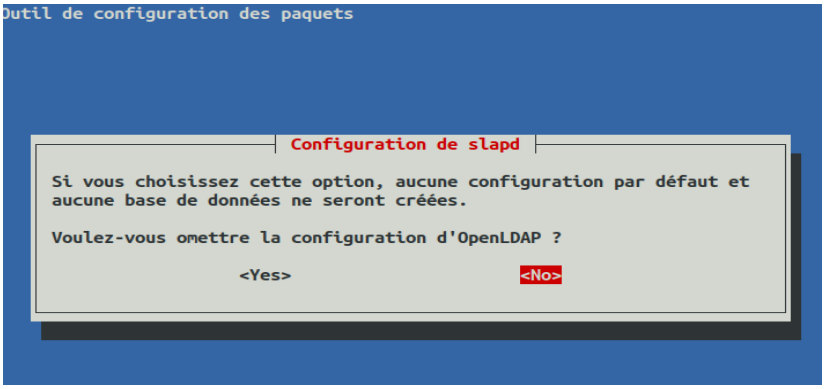
Configuration des fichiers de base

Aussitôt l'installation terminé, l'annuaire est fonctionnel mais les données associées à cet annuaire ne sont pas encore configurées. Définissons la configuration de base de notre annuaire. C'est ici que nous allons utiliser le nom de votre domaine et que nous allons répondre à quelques questions qui permettent de définir l'usage de la base de données rattachée à l'annuaire.

Entrez la commande suivante pour la configuration :

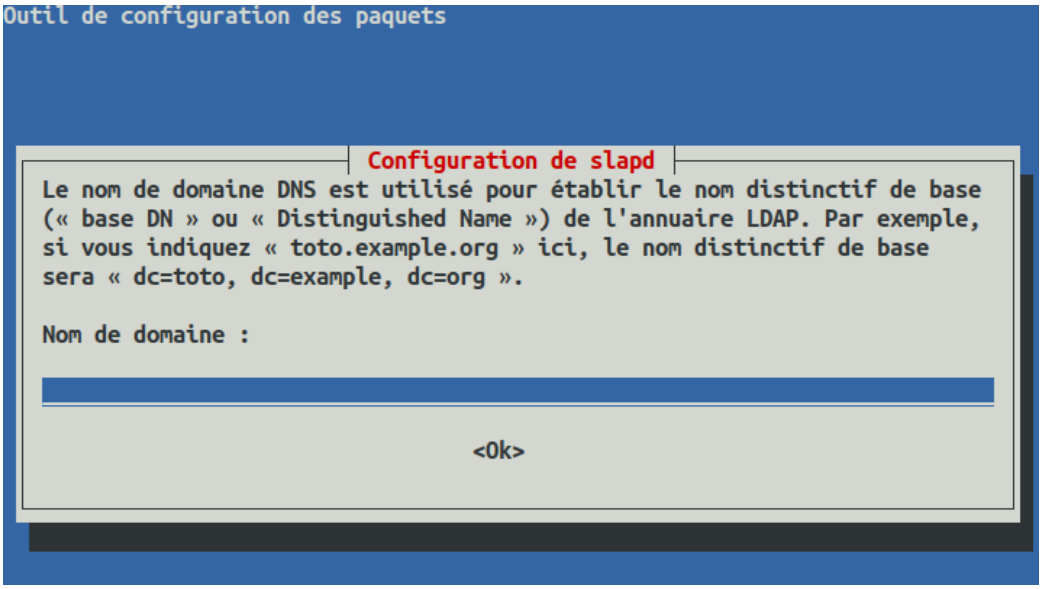
```
dpkg-reconfigure  slapd
```

Vous recevrez les écrans suivants :

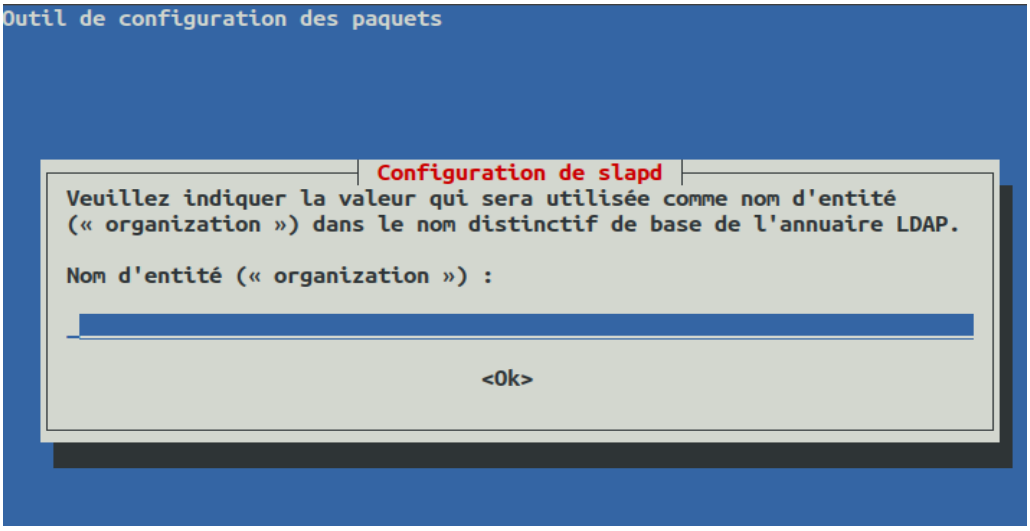


- Répondez non ici.

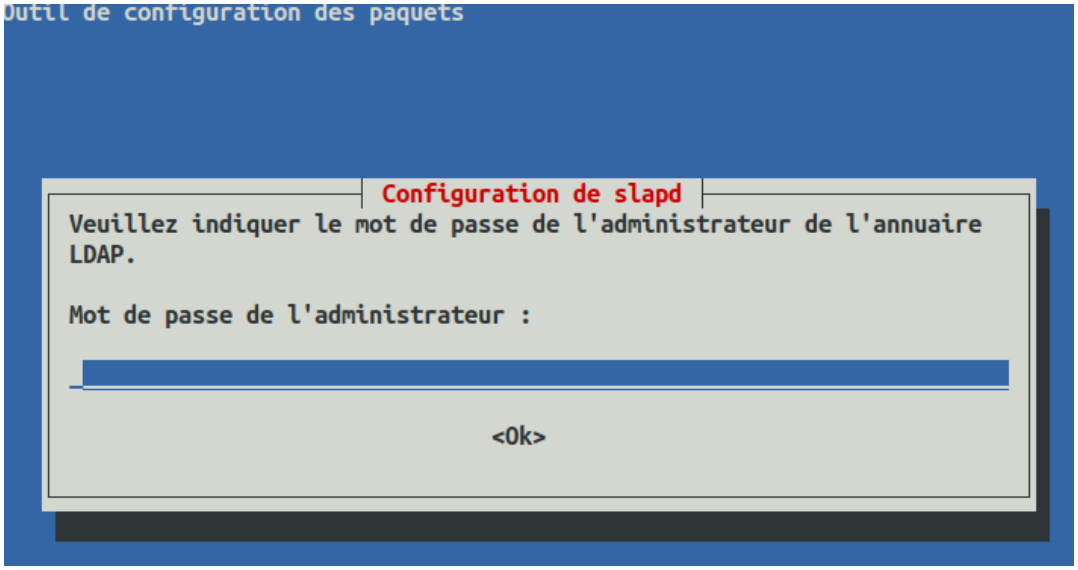
L’écran suivant vous demande d’entrer le nom de domaine de votre annuaire. À des fins de tests seulement, nous allons entrer le domaine « demo.com ». Il s’agira évidemment d’entrer le nom de domaine réel de votre organisation ici.



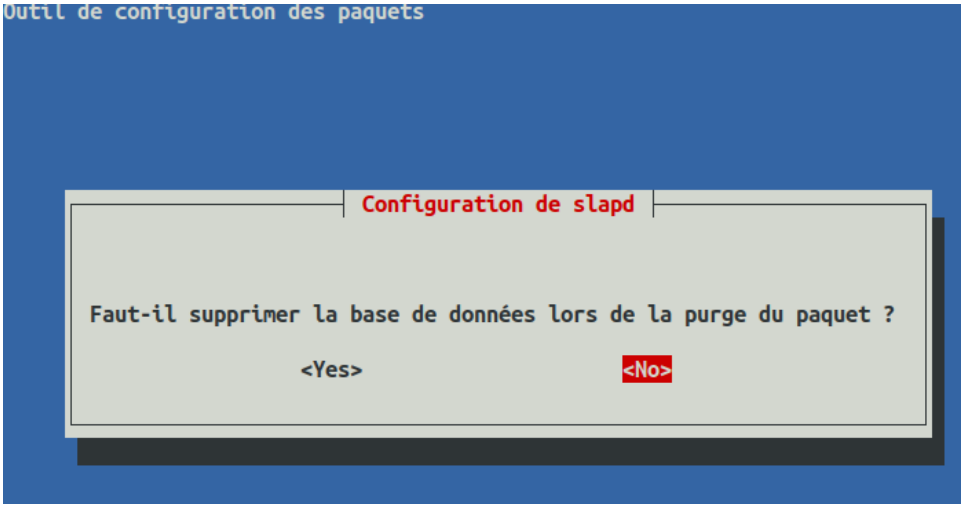
On vous demande ensuite d’entrer le nom de votre organisation comme nom distinctif de base de l’annuaire LDAP. Entrons ici, encore là fictif, le nom « demo ».



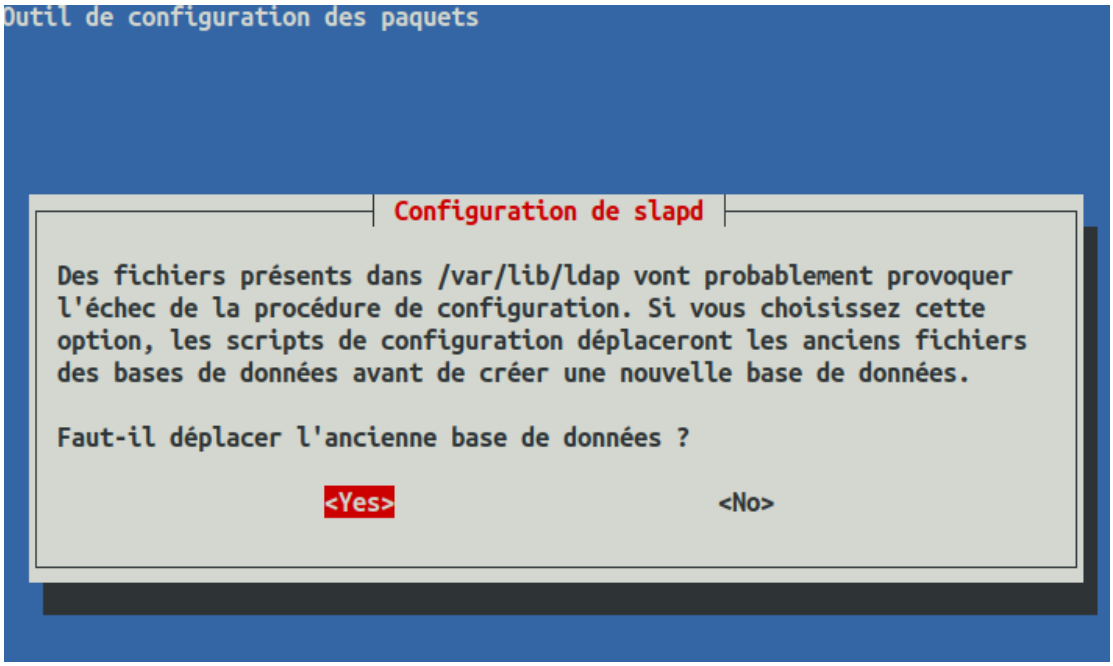
Entrez ensuite le mot de passe de l'administrateur de l'annuaire. Ici, c'est le même mot de passe que vous avez entré lors de l'installation initiale.



Ensuite, entrez « non » afin de ne pas supprimer la base de données. Dans le cas où vous désinstallez LDAP, votre base de données sera sauvegardée et vous pourrez la récupérer lors de la réinstallation de votre annuaire.



- Répondez « oui » à la dernière question

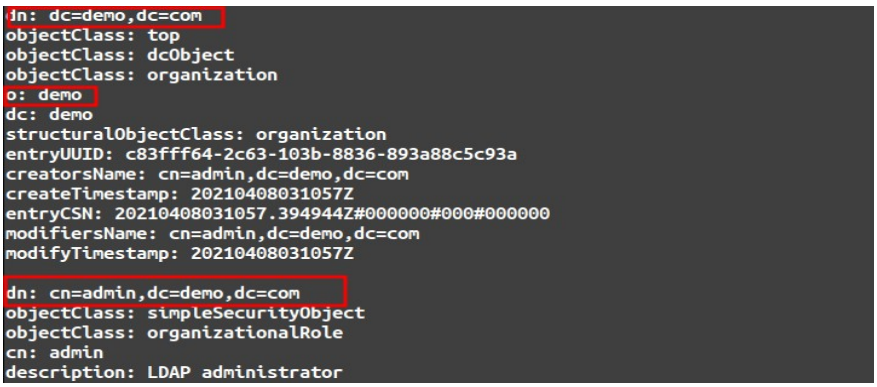


La configuration des fichiers de base de l'annuaire est complétée.

Pour vérifier que l'on a les bonnes informations dans notre annuaire actuellement, vous pouvez entrer la commande :

```
slapcat
```

Vous devriez recevoir une sortie similaire à celle-ci. J'attire votre attention aux encadrés rouges qui montrent bien que le dn est demo.com et que l'organisation (o : demo) est bien le bon nom entré précédemment.



L’utilitaire « ldap-account-manager »

Il existe une série de commande qui vous permettra de peupler votre annuaire avec des entrées reliées à votre organisation. On peut y créer, entre autre, des groupes et des usagers.

Une application intéressante consiste à installer un gestionnaire de compte pour gérer enligne les groupes et les usagers reliés à votre annuaire.

Installation de « ldap-account-manager »

LAM facilite l'administration des entrées LDAP en résumant les détails techniques de LDAP et en permettant aux administrateurs et aux utilisateurs sans connaissances techniques de gérer le serveur LDAP. Si nécessaire, les utilisateurs expérimentés peuvent modifier directement les entrées LDAP via le navigateur LDAP intégré.

Cet utilitaire permet, entre autre, de :

- Gère Unix, Samba 3/4, Kolab 3, Kopano, DHCP, clés SSH, un groupe de noms.
- Prend en charge l'authentification à 2 facteurs
- Prise en charge des profils de création de compte
- Téléchargement de fichier CSV
- Création / suppression automatique des répertoires personnels
- définition des quotas du système de fichiers
- Sortie PDF pour tous les comptes
- schéma et navigateur LDAP
- gère plusieurs serveurs avec différentes configurations

L’utilitaire repose sur le bon fonctionnement des éléments suivants :

- Un annuaire LDAP fonctionnel;
- Un serveur Web Apache;
- le support pour PHP;
- un compte utilisateur avec privilège « sudo ».

Note :

Pour installer apache et PHP, on peut faire la commande :

```
apt -y install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear
```

Lancez l'installation de lam avec :

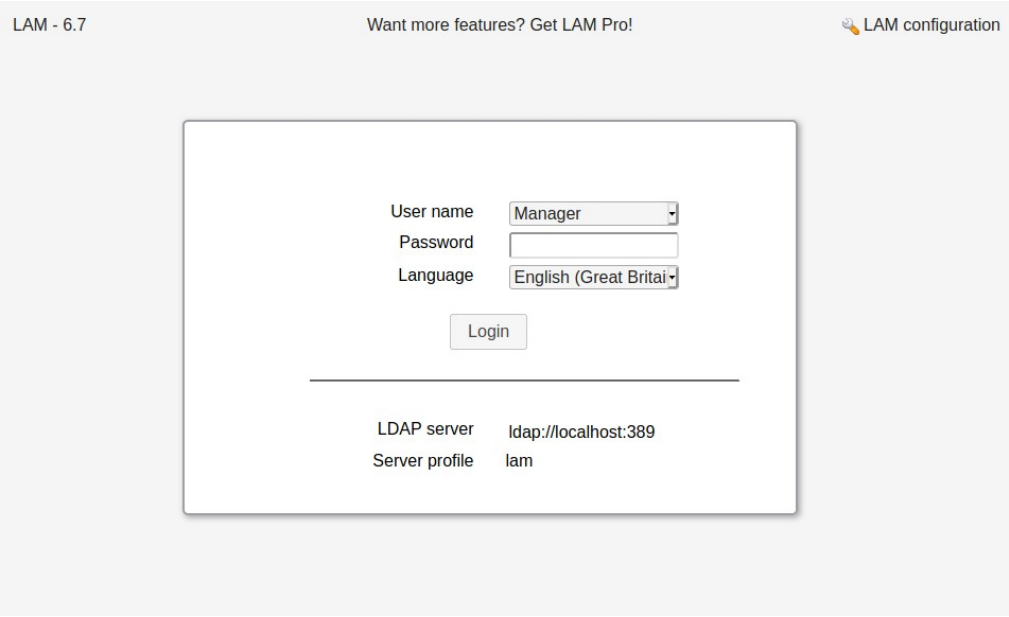
```
apt -y install ldap-account-manager
```

Accès au gestionnaire par un navigateur

Dans un navigateur, entrez l'url suivante :

```
http://adresse_IP_de_votre_annuaire_LDAP/lam
```

Le formulaire de **connexion du** gestionnaire de compte LDAP s'affiche. Nous devons définir notre profil de serveur LDAP en cliquant sur `[LAM configuration]` dans le coin supérieur droit.



Cela vous demandera le mot de passe du profil « lam ». Par défaut, le mot de passe est « lam ».

Dans la fenêtre qui s'affiche, cliquez sur Modifier les profils de serveur(Edit server profiles) (Figure 2).

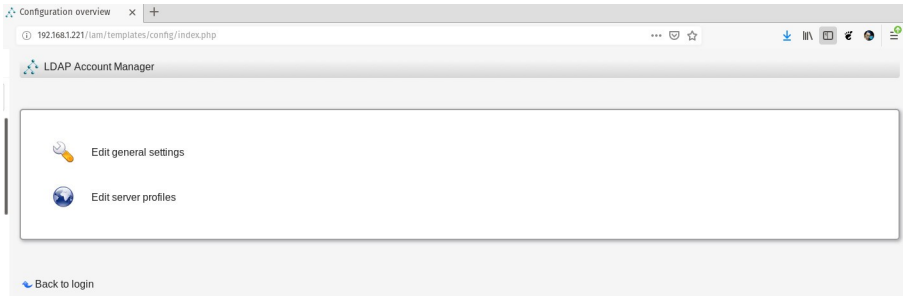


Figure 2: Les options d'édition LAM.

Vous serez invité à entrer le mot de passe du profil par défaut, alors tapez lam et cliquez sur OK. Vous serez alors présenté avec la page des paramètres du serveur (Figure 3).

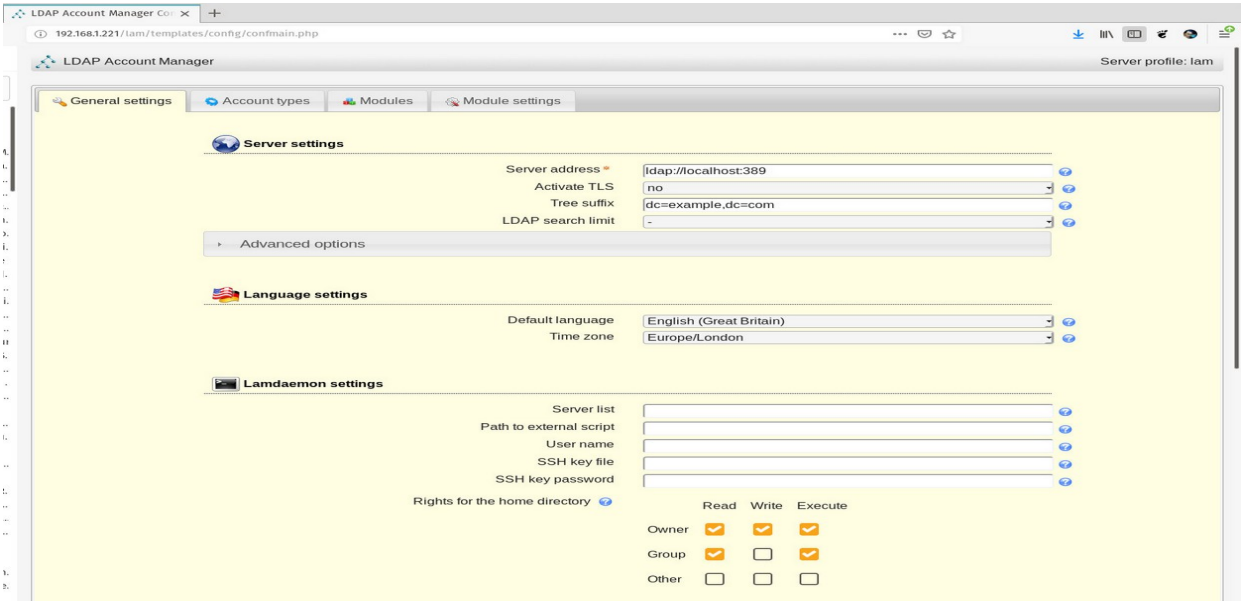


Figure 3: La page des paramètres du serveur LAM.

Dans la section Paramètres du serveur, saisissez l'adresse IP de votre serveur LDAP. Puisque nous installons LAM sur le même serveur qu'OpenLDAP, nous laisserons la valeur par défaut. Si vos serveurs OpenLDAP et LAM ne sont pas sur la même machine, assurez-vous de saisir ici l'adresse IP correcte du serveur OpenLDAP.

Dans l'entrée Suffixe de l'arborescence (Tree suffix), ajoutez les composants de domaine de votre serveur OpenLDAP sous la forme dc = exemple, dc = com.

Toujours en continuant avec notre exemple de domaine (demo.com), nous aurons donc la forme suivante : dc=demo,dc=com

Ensuite, prenez soin des configurations suivantes:

Dans la section Paramètres de sécurité (Figure 4), configurez la liste des utilisateurs valides sous la forme cn = admin, dc = example, dc = com (assurez-vous d'utiliser votre utilisateur administrateur LDAP et les composants de domaine).

Dans notre exemple : cn=admin,dc=demo,dc=com

Figure 4: La section des paramètres de sécurité.

Ensuite dans la section « Profile password », entrez un nouveau mot de passe pour l'administrateur comme montré à la figure 4.1.

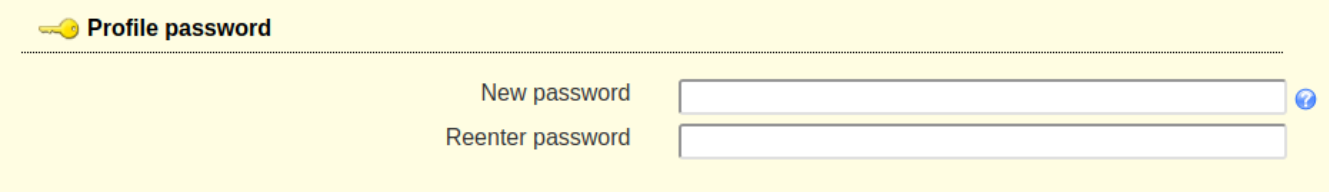
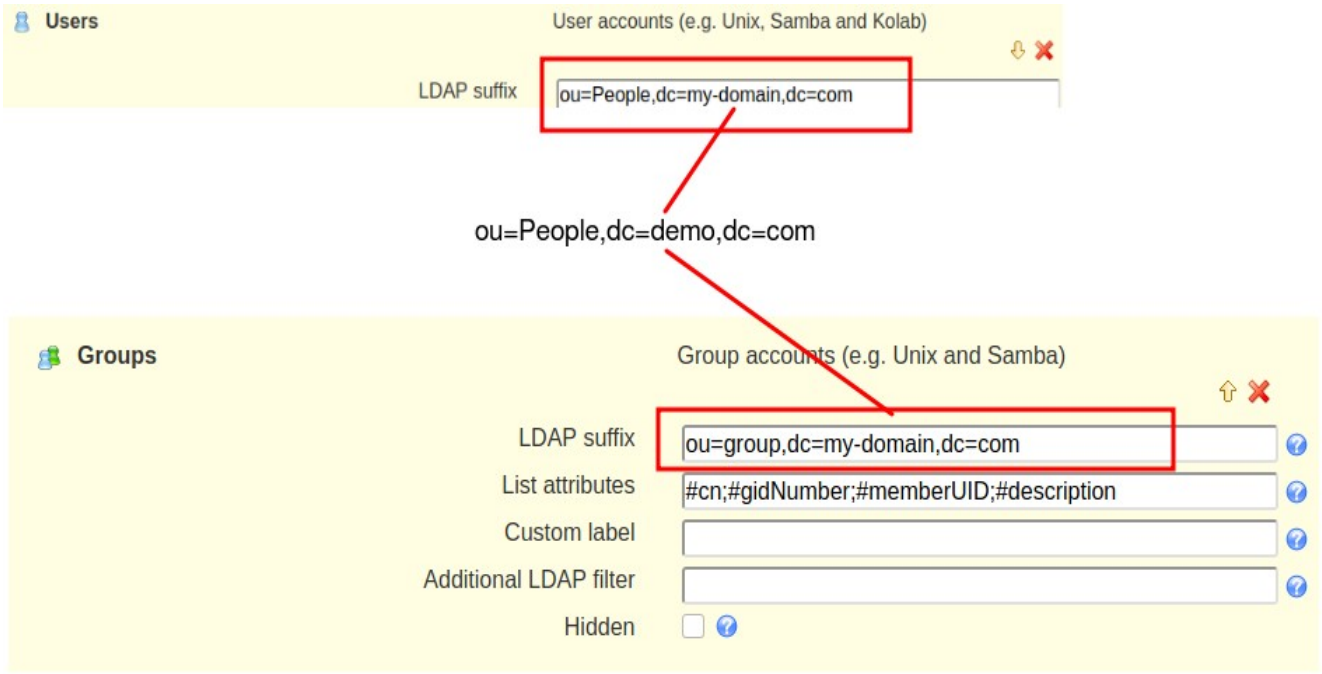


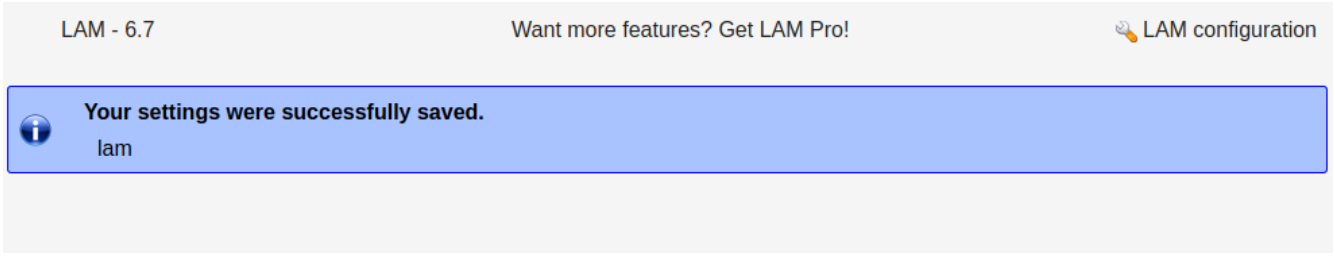
Figure 4.1: Section du mot de passe du profil de l'administrateur

Sélectionnez ensuite l'onglet « Account types » et sélectionnez la catégorie « Active account types » comme le montre la figure suivante :



Assurez-vous ici que le suffixe LDAP pour les usagers et les groupes correspondent au bon nom de domaine que vous avez choisi comme le montre les encadrés

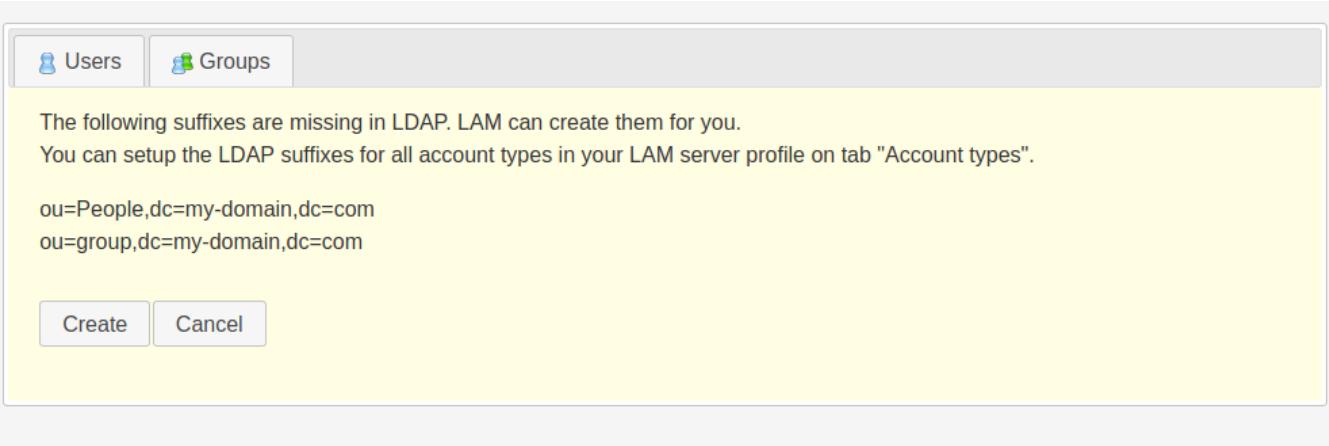
Sauvegardez ensuite avec le bouton « save ». Vous devriez obtenir la confirmation suivante :



Vous revenez alors à la fenêtre de connexion. Vous pourrez alors sélectionnez l'utilisateur qui est administrateur du serveur.

- Sélectionnez « admin » et entrez le mot de passe de cet administrateur.

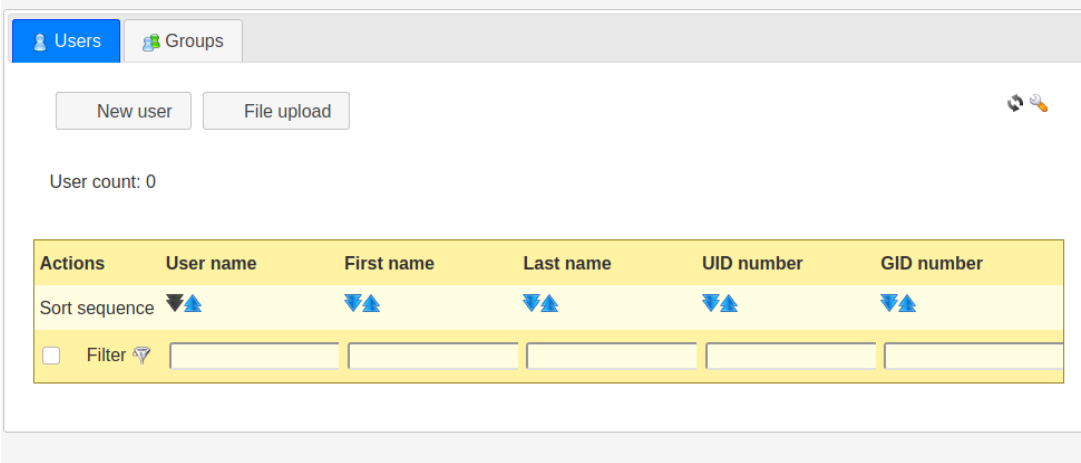
Lorsque vous vous connecterez ensuite avec le compte « admin », il se peut que vous receviez ce message la première fois :



Cliquez le bouton « Create » pour créer les éléments manquants.

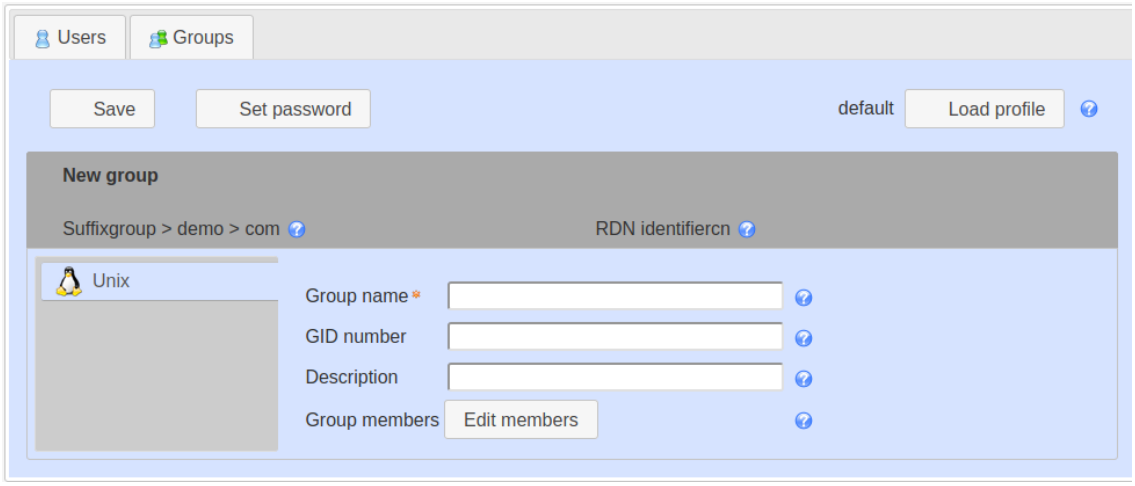
Création d'usager et de groupe dans l'annuaire

Après l'authentification, vous êtes présenté à l'écran où vous pouvez créer des groupes et des usagers.



Les onglets supérieurs « Users » et « Groups » vous permettront de créer un usager ou un groupe.

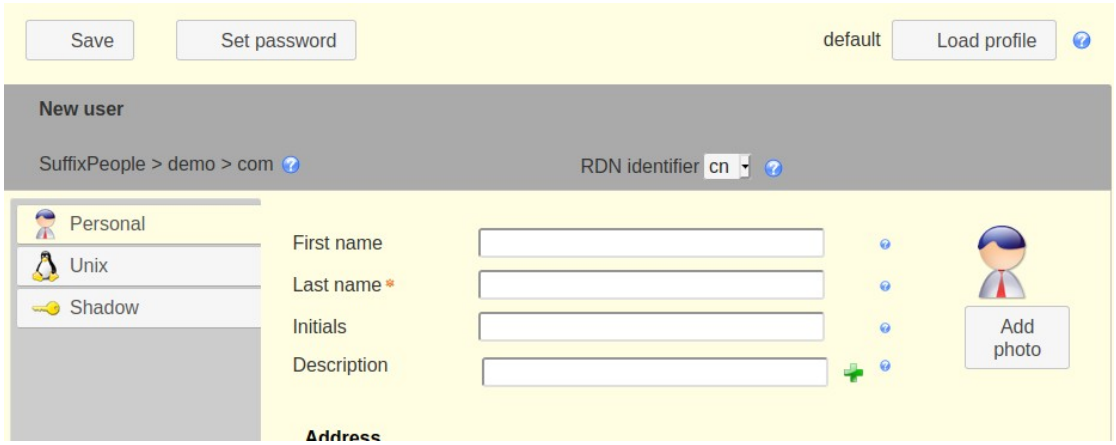
Écran de création d'un groupe



Il s'agit d'entrer le nom du groupe et de sauvegarder.

Écran de création d'un nouvel usager

Cliquez sur Nouvel utilisateur et la fenêtre Nouvel utilisateur s'ouvre (Figure 7), où vous pouvez remplir les espaces nécessaires.



Vous devrez minimalement entrer le nom de famille « Last name » pour pouvoir passer à la prochaine étape.

Dans l’onglet « Unix » à droite, vous pourrez entrer les éléments reliés au compte de l’usager comme montré ci-dessous :

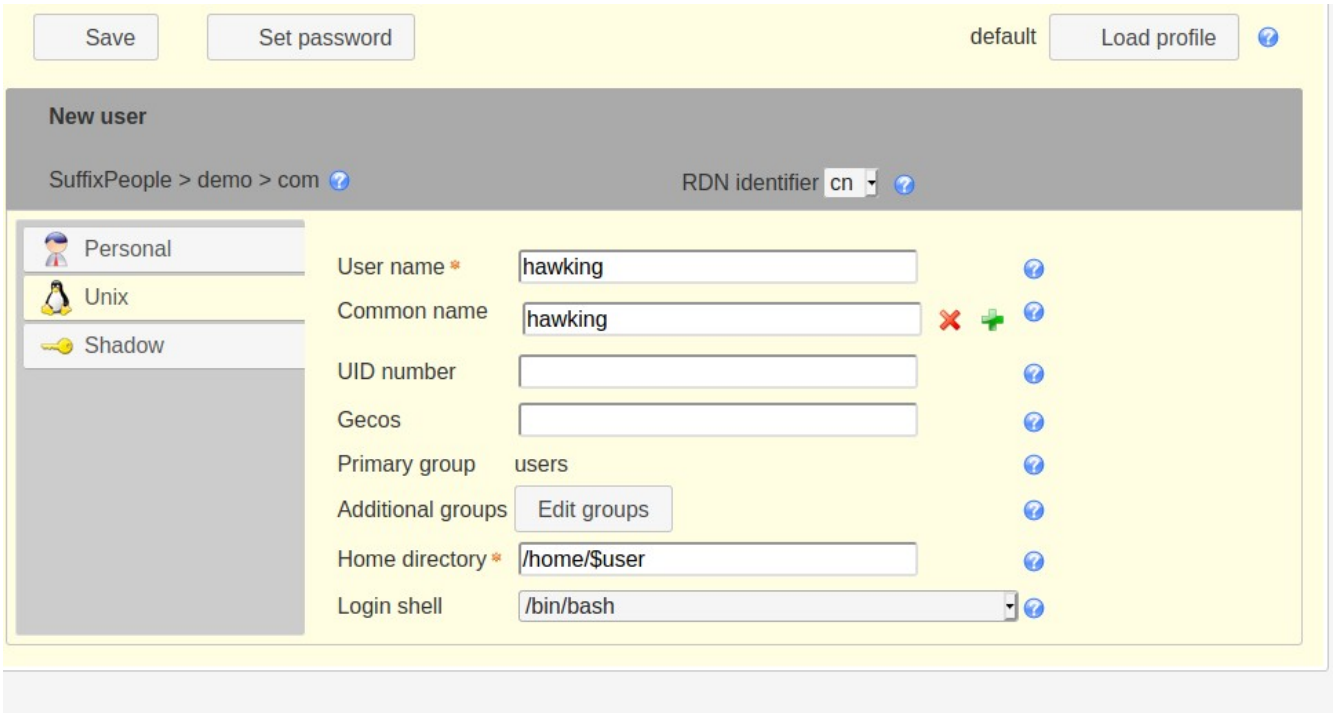


Figure 7: Ajout d'un nouvel utilisateur avec LAM.

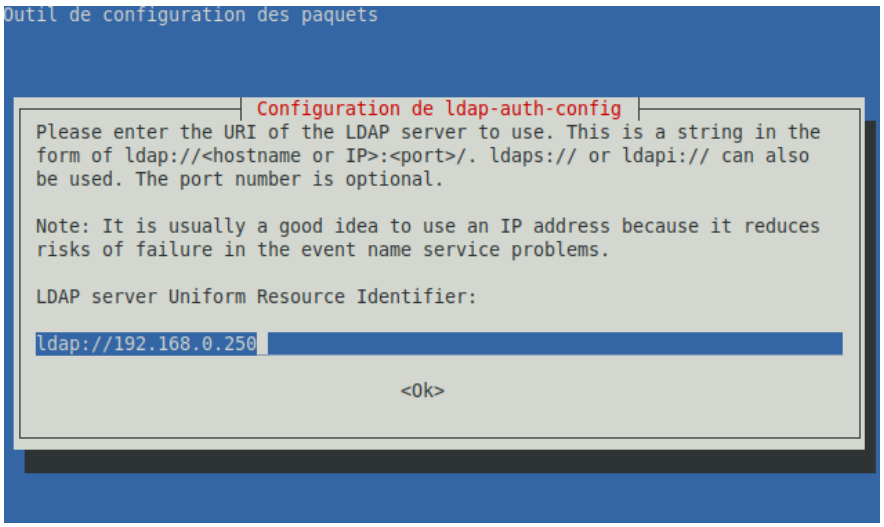
Assurez-vous de cliquer sur Définir le mot de passe afin de pouvoir créer un mot de passe pour le nouvel utilisateur (sinon l'utilisateur ne pourra pas se connecter à son compte). Assurez-vous également de cliquer sur l'onglet Unix, où vous pouvez définir le nom d'utilisateur, le répertoire personnel, le groupe principal, le shell de connexion, etc. Une fois que vous avez entré les informations nécessaires pour l'utilisateur, cliquez sur Enregistrer et le compte utilisateur peut alors être trouvé dans l'arborescence de l'annuaire LDAP.

Configuration d’un client pour une authentification LDAP

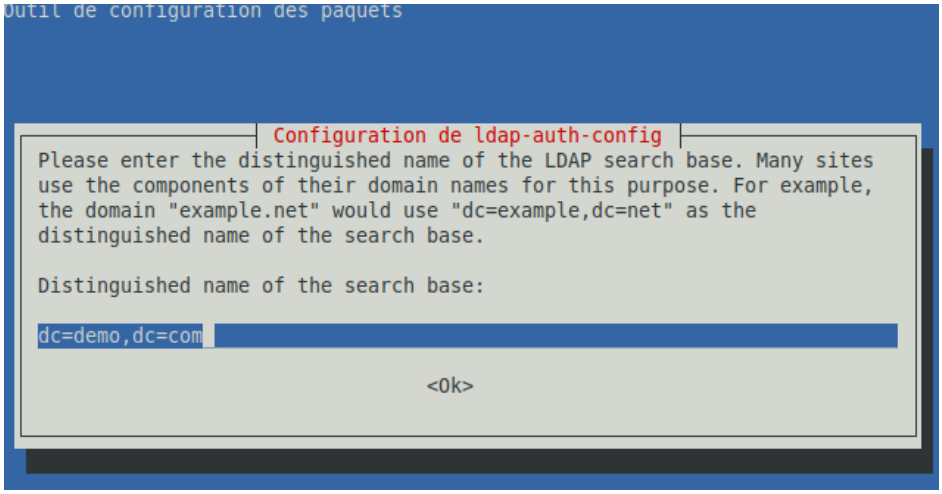
Avec votre serveur configuré et en cours d'exécution, il vous suffit de travailler sur les machines clientes. Connectez-vous à l'un de vos clients (vous devez suivre ces étapes sur tous les clients) et installez le logiciel nécessaire avec la commande suivante:

```
apt-get install  -y   libnss-ldap libpam-ldap ldap-utils nscd
```

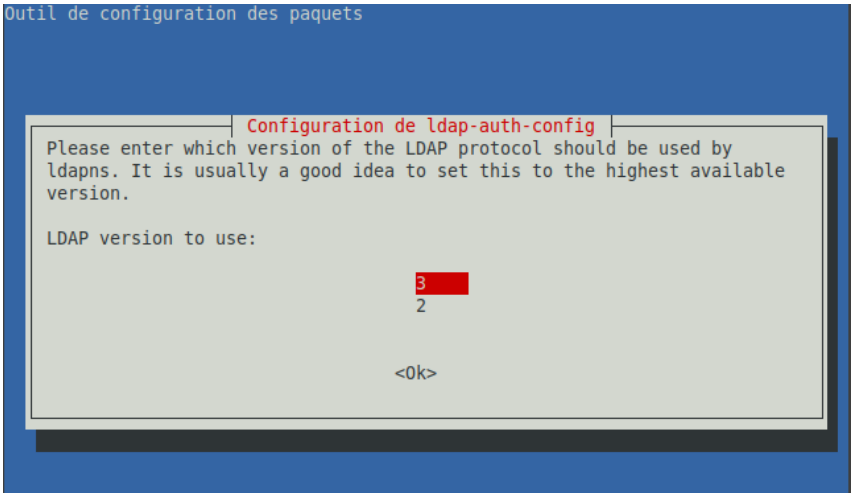
Lors de l'installation, il vous sera demandé de définir l'URI du serveur LDAP (comme montré ci-dessous). L'adresse URI doit être au *format ldap: // SERVER_IP* (où SERVER_IP est l'adresse IP de votre serveur LDAP).



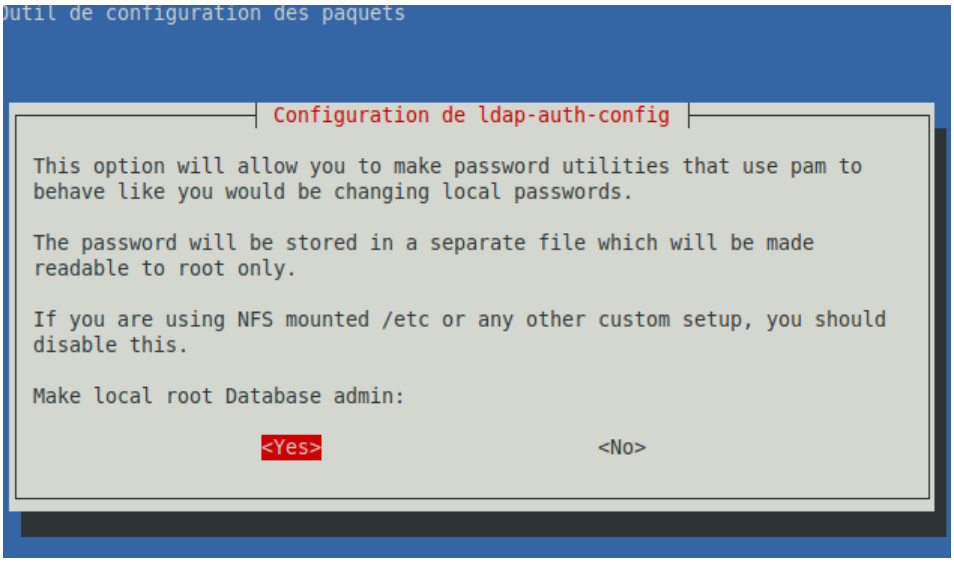
Entrez ensuite le nom de domaine pour votre annuaire comme ci-dessous :



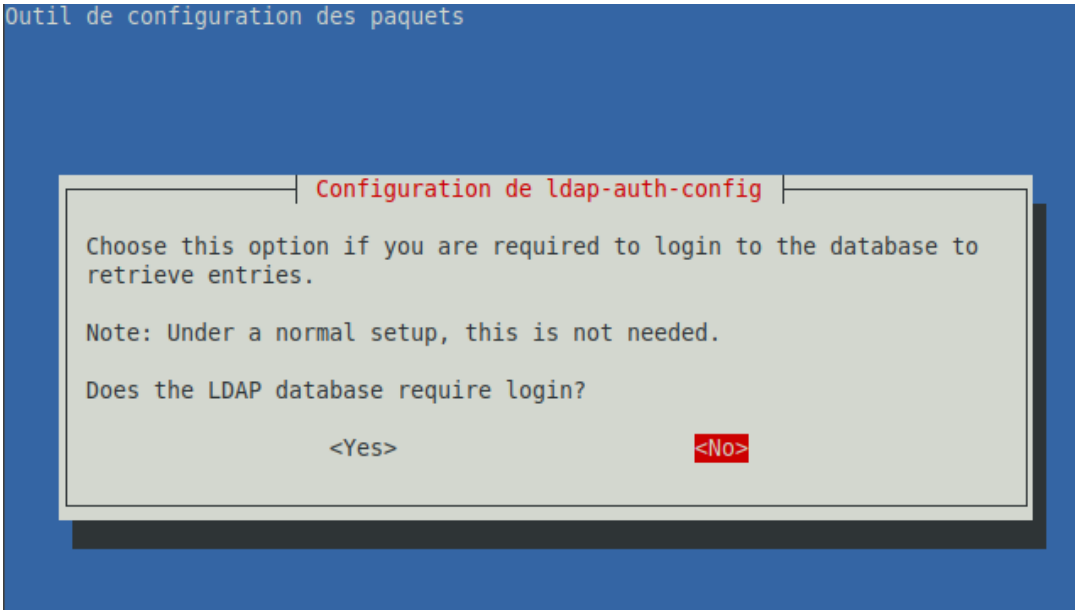
On vous demande la version de LDAP que vous voulez utiliser. Laissez le défaut de la version 3.



Le prochain écran vous demande si vous voulez que le compte « root » du client puisse administrer le serveur LDAP. En fait, le système va associer le compte « root » au compte « admin » du serveur LDAP que nous avons configuré précédemment. ON répond habituellement « oui » à cette question.

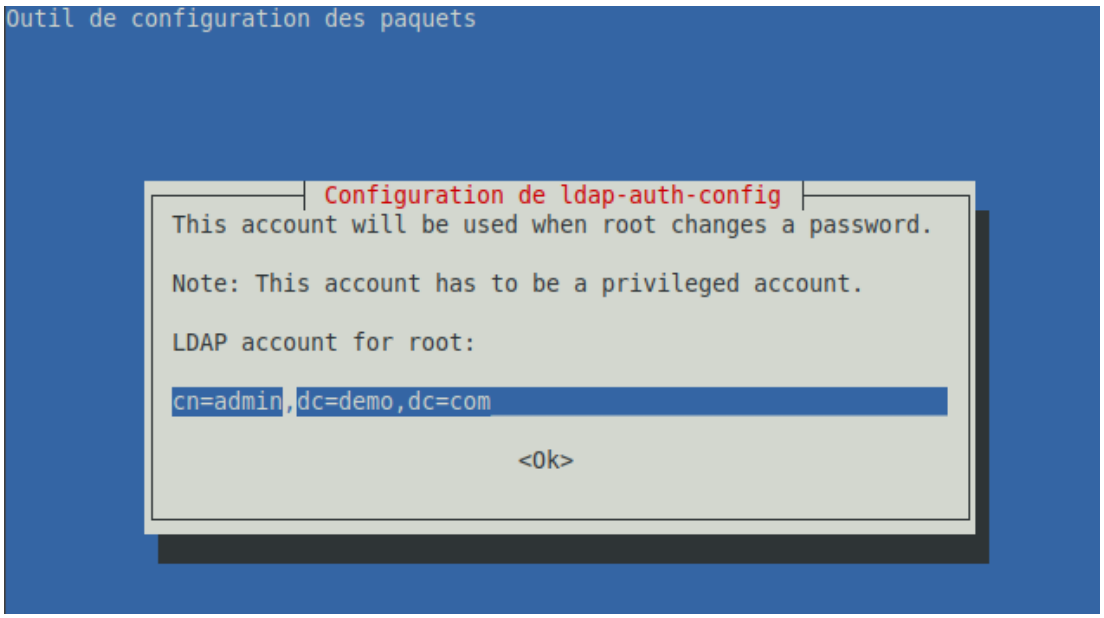


Le prochain écran demande si l'on requiert un login pour pouvoir se brancher à la base de donné. On répond « non » dans ce cas-ci. Comme mentionné, dans un usage normal, on a rarement besoin de cette option.

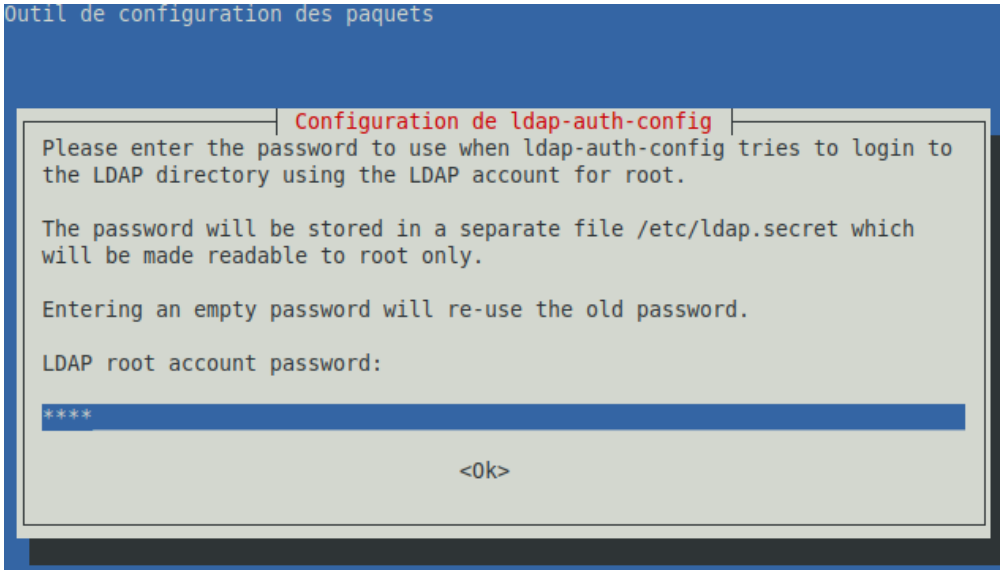


Le prochain écran vous demandera quel compte utilisé dans l'annuaire LDAP lorsque « root » changera un mot de passe d'un usager.

Soyez certain de bien entrer les informations de votre domaine ainsi que le compte qui est administrateur de l'annuaire. Voici un exemple ci-dessous :



Le dernier écran vous demande d'entrer le mot de passe de l'administratreur de votre annuaire LDAP.



Configuration des fichiers pam du client

Nous devons maintenant configurer notre client pour pouvoir s'authentifier auprès du serveur LDAP. Sur le client, ouvrez une fenêtre de terminal et exécutez la commande:

sudo nano /etc/nsswitch.conf	
	Dans ce fichier, ajoutez « ldap » à la fin des lignes suivantes : passwd: compat systemd **ldap** group: compat systemd **ldap** shadow: files **ldap**

Enregistrez et fermez ce fichier.

Ensuite, exécutez la commande :

```
sudo nano   /etc/pam.d/common-password
```

Supprimez use_authtok de la ligne suivante:

password [success=1 user_unknown=ignore default=die] pam_ldap.so ~~use_authtok~~ try_first_pass

Enregistrez et fermez ce fichier.

Exécutez ensuite cette commande :

```
sudo nano    /etc/pam.d/common-session
```

À la fin de ce fichier, ajoutez ce qui suit:

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

Enregistrez et fermez ce fichier.

La ligne ci-dessus créera le répertoire de base par défaut pour tout utilisateur LDAP qui n'a pas de compte local sur le client.

Redémarrez l'ordinateur client puis, lorsque l'écran de connexion s'affiche, essayez de vous connecter avec un utilisateur sur votre serveur OpenLDAP. Il doit s'authentifier et tout va bien. Assurez-vous de configurer tous vos clients de la même manière, afin qu'ils puissent utiliser les services d'annuaire OpenLDAP.

Modification au fichier /etc/hosts

Si vous n'avez pas de serveur DNS, vous devrez vous en bâtir un local à l'aide du fichier hosts.

Sur le serveur sur lequel a été installé LDAP, entrez les lignes suivantes. Évidemment, changez les informations pour refléter vos adresses IP et nom de domaine.

Sur le serveur LDAP

```
sudo  nano /etc/hosts
```

```
192.168.0.250     demo.com    tuxmain.demo.com
192.168.0.100     tuxclient1.demo.com
```

Sur l'ordinateur du client

```
sudo  nano /etc/hosts
```

```
192.168.0.250     tuxmain.demo.com
```

Redémarrage des services

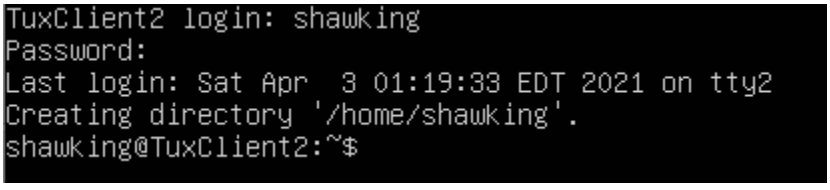
N'oubliez pas, lorsque vous changez quoi que ce soit dans les fichiers de configuration, de redémarrez les services associés.

Pour le serveur LDAP : systemctl restart slapd

Pour le client : redémarrez nscd → systemctl restart nscd

Test d'un compte

Tester le compte que vous avez créé dans votre annuaire LDAP à partir d'un client de votre réseau.



Quelques portions de ce document proviennent du site de OpenClassroom.