

# ALCASAR

## Étude préliminaire pour la mise en place d'un portail captif dans une école.

Avant de déployer un portail captif dans une école, il est essentiel de bien comprendre les raisons de son utilisation et les objectifs à atteindre :

- La sécurité pour limiter l'accès à Internet et protéger les élèves de contenus inappropriés et des cybermenaces.
- Pour contrôler et pouvoir surveiller et gérer l'utilisation d'Internet par les élèves et le personnel pour s'assurer qu'elle est conforme aux politiques de l'école.
- Pour vérifier l'identité des utilisateurs et offrir des accès différenciés selon le profil (élèves, enseignants, administrateurs).
- Se conformer aux lois et réglementations en matière d'accès à Internet et de protection des données.
- Pour pouvoir utiliser le portail comme outil pédagogique et enseigner aux élèves les bonnes pratiques d'utilisation d'Internet.
- Pour évaluer les besoins pédagogiques, les ressources en ligne nécessaires et les restrictions à mettre en place.

En fonction des besoins identifiés, les fonctionnalités du portail captif peuvent inclure :

- **Page de connexion personnalisée** : Où les utilisateurs doivent s'authentifier avant d'accéder à Internet.
- **Gestion des profils d'utilisateur** : Pour définir des règles d'accès différentes pour les élèves, les enseignants et le personnel administratif.
- **Filtrage de contenu** : Pour bloquer l'accès à des sites inappropriés ou dangereux.
- **Suivi et rapports** : Pour surveiller l'utilisation d'Internet et générer des rapports sur l'activité en ligne.
- **Notifications et alertes** : Pour informer les utilisateurs des politiques d'utilisation et alerter en cas d'accès non autorisé.

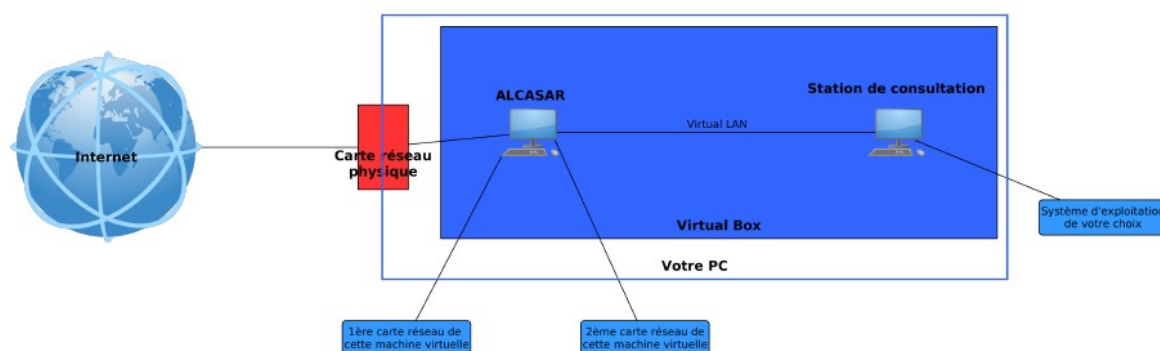
## Procédure d'installation (alcasar.net)

Alcasar peut être installé sur un ordinateur standard équipé de deux cartes réseaux Ethernet. Une carte externe, connectée au fournisseur d'accès internet (FAI), la deuxième, interne, est connectée au commutateur (switch).

Pour desservir les équipements du réseau, l'adresse IP de classe C (254 équipements), est par défaut 192.168.182.1/24.

Alcasar est le serveur DHCP, le serveur DNS, le serveur de temps et le routeur par défaut (default gateway)

Schéma de principe (Tutoriel Alcasar)



Alcasar est un portail captif, c'est-à-dire que les clients passent par une page web spéciale avant d'accéder à internet normalement. Il y a un mécanisme d'authentification et de contrôle avant d'accéder au web. Alcasar protège et filtre les flux par utilisateurs ou groupe d'utilisateurs (antivirus HTTP, filtrage de protocoles réseau, de nom de domaine, d'URLs et d'adresses IP). On peut y appliquer aussi un filtrage par liste rouge (sites interdits) ou par liste verte (sites autorisés).

### • Créer une VM :

#### Installation d'Alcasar

Créer une VM avec au moins 100 Go de disque dur et 8 Go de mémoire vive.

Télécharger le fichier ISO de Linux -Mageia (mageia-8-x86\_64-DVD.iso).

#### Installation du système d'exploitation

Suivre les instructions du fichier ISO.



#### INSTALLATION

- Langue •
- Licence •
- Partitionnement •
- Installation •

#### CONFIGURATION

- Utilisateurs •
- Résumé •
- Mises à jour •
- Quitter •

#### INSTALLATION



Temps  
restant : 4 minutes

Notes de version

Annuler

Détails

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet2	Custom	-	-	-	172.16.0.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.128.0

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
 Bridged to:  Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network  
 Host virtual adapter name: VMware Network Adapter VMnet2

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP:  Subnet mask:

Restore Defaults Import... Export... OK Cancel Apply Help

**VMnet2 (Custom) :** Sous-réseau 172.16.0.0/24

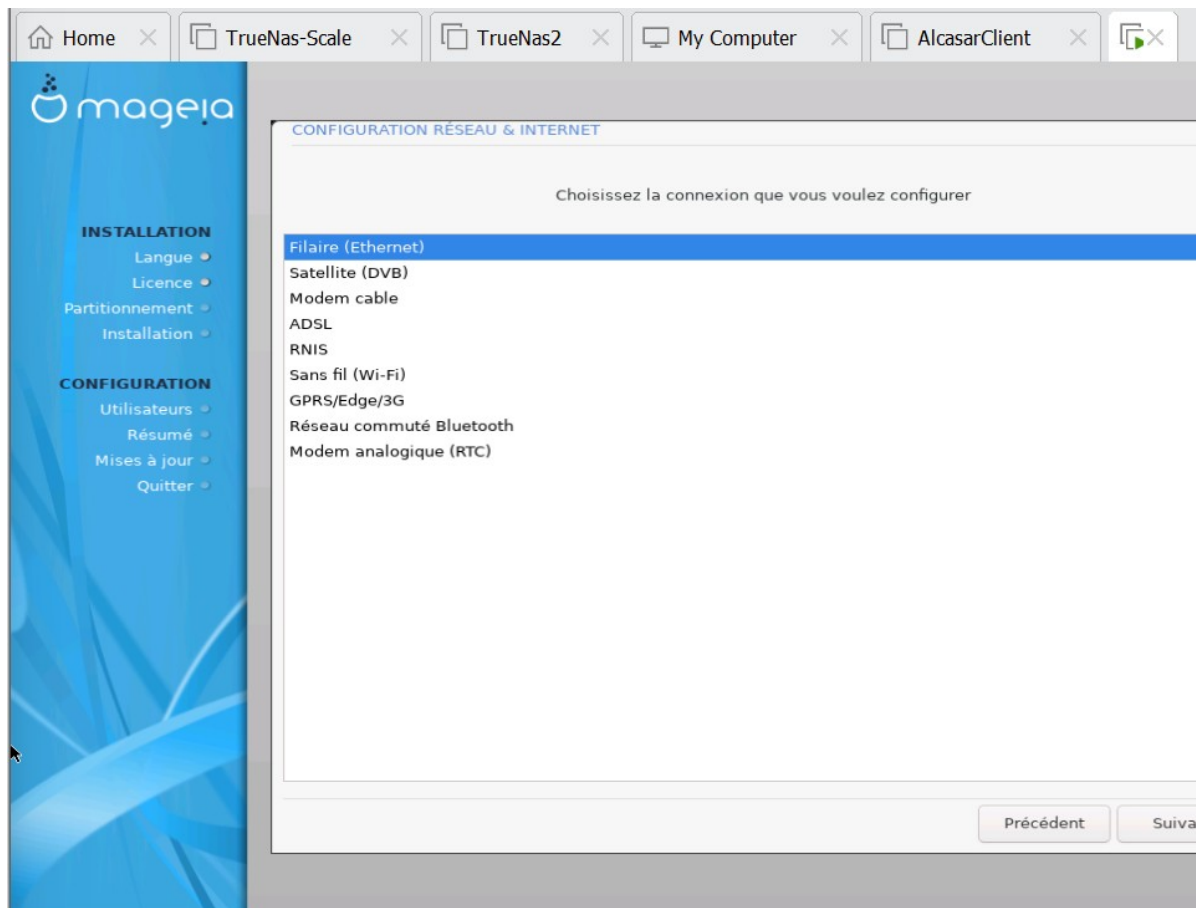
**VMnet8 (NAT) :** Sous-réseau 192.168.128.0/24

**Interfaces réseau dans la VM :**

- **ens32** : 192.168.128.20/24 (connectée à VMnet8)
- **ens33** : Pas d'adresse IP configurée (connectée à VMnet2)

Deux cartes réseaux sont nécessaires pour le fonctionnement d'Alcasar ; une carte externe (WAN) connectée à internet, et une carte interne (LAN).

La carte custom, LAN, qui fonctionne comme un filtre pour se connecter vers l'extérieur avec la carte NAT, pour qu'internet fonctionne.



Ensuite, normalement on doit télécharger l'archive Alcasar depuis le site officiel. Mais, le fichier est déjà décompressé dans l'image ISO de Mageia que l'on a téléchargé. Il nous suffit de nous rediriger vers le répertoire d'Alcasar et d'effectuer les commandes :

```
cd alcasar-x.y  
sh alcasar.sh -i
```

Enregistrer les utilisateurs ; on crée le compte root, le compte utilisateur et on enregistre les mots de passe.

```
-----  
                  ALCASAR V3.6.1 Installation  
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau  
-----  
Par défaut, l'adresse IP d'ALCASAR sur le réseau de consultation est : 192.168.1  
82.1/24  
Voulez-vous utiliser cette adresse et ce plan d'adressage (recommandé) (O/n)? :  
n  
Entrez l'adresse IP d'ALCASAR au format CIDR (a.b.c.d/xx) :
```

On enregistre l'adresse **IP 192.168.128.20/24** qui correspond à l'interface ens32 configurée sur le sous-réseau NAT avec accès à internet.

Faire les mises à jour une fois l'installation terminée avec la commande :  
**dnf update.**


```

Bienvenue sur ALCASAR Version 3.0.1 (Mageia 8)
Connectez-vous à l'URL 'https://alcasar.localdomain/acc/'
Kernel 5.15.126-server-1.mga8 on a Dual-processor x86_64 / tty1
alcasar login: root
Password:
Last login: Thu Jun 27 11:57:18 on tty1
alcasar-LaPlateforme[~]# dnfupdate
-bash: dnfupdate : commande introuvable
alcasar-LaPlateforme[~]# dnf update
Mageia 8 - x86_64                                0.0 B/s | 0 B    00:00
Errors during downloading metadata for repository 'mageia-x86_64':
- Curl error (6): Couldn't resolve host name for https://www.mageia.org/mirrorlist/?release=8&arch=x86_64&section=core&repo=re
lease [Could not resolve host: www.mageia.org]
Error: Failed to download metadata for repo 'mageia-x86_64': Cannot prepare internal mirrorlist: Curl error (6): Couldn't resolv
e host name for https://www.mageia.org/mirrorlist/?release=8&arch=x86_64&section=core&repo=release [Could not resolve host: www.
mageia.org]
Mageia 8 - x86_64 - Updates                        0.0 B/s | 0 B    00:00
Errors during downloading metadata for repository 'updates-x86_64':
- Curl error (6): Couldn't resolve host name for https://www.mageia.org/mirrorlist/?release=8&arch=x86_64&section=core&repo=up
dates [Could not resolve host: www.mageia.org]
Error: Failed to download metadata for repo 'updates-x86_64': Cannot prepare internal mirrorlist: Curl error (6): Couldn't resol
ve host name for https://www.mageia.org/mirrorlist/?release=8&arch=x86_64&section=core&repo=updates [Could not resolve host: ww
w.mageia.org]
Dépôts ignorés : mageia-x86_64, updates-x86_64
Dépendances résolues.
Rien à faire.
Terminé !
alcasar-LaPlateforme[~]# ls
aif-mount/  alcasar-3.6.1/  ALCASAR-passwords.txt  drakx/  grub.default*  tnp/
alcasar-LaPlateforme[~]# cd a
aif-mount/  alcasar-3.6.1/
alcasar-LaPlateforme[~]# cd alcasar-3.6.1/


```

Utiliser la roue crantée, en bas à droite de l'interface, se connecter en tant qu'administrateur avec le mot de passe enregistré sur la VM Alcasar.

Quand on ouvre une page web sur le serveur client, normalement si tout se passe bien, elle se connecte automatiquement sur le portail captif d'Alcasar.



# ALCASAR



**Menu**

- ACCUEIL
- SYSTÈME**
  - Réseau
  - Services
  - LDAP/A.D.
- AUTHENTIFICATION
  - FILTRAGE
  - STATISTIQUES
  - SAUVEGARDES

**Documents**

- Presentation

**Authentification LDAP**

Un port 389 (636 avec SSL) est actif sur ce serveur  
Une connexion LDAP a été établie  
L'authentification a réussie  
Le DN de la base semble correct (1 entrées dans la base)

Éditer la configuration LDAP: OUI ▾


Serveur LDAP:  Assistant  
Adresse IP du serveur

Connexion chiffrée NON ▾  
Utiliser une connexion chiffrée avec SSL (LDAPS)


Vérifier le certificat SSL NON ▾  
Vérifier que le serveur LDAP utilise un certificat connu

Certificat SSL (CA) Parcourir... Aucun fichier sélectionné.

To direct input to this VM, click inside or press Ctrl+G.



# ALCASAR



**Menu**

- ACCUEIL
- SYSTÈME**
  - Réseau
  - Services
  - LDAP/A.D.
- AUTHENTIFICATION
  - FILTRAGE
  - STATISTIQUES
  - SAUVEGARDES

**Documents**

- Presentation

Vérifier le certificat SSL  
Vérifier que le serveur LDAP utilise un certificat connu

NON ▾

Certificat SSL (CA)  
Certificat de l'autorité de certification signant celui du serveur LDAP  
Aucun certificat installé

Parcourir... Aucun fichier sélectionné.

CN de l'utilisateur exploité par ALCASAR:  
CN=Common Name. Laissez vide pour utiliser un accès invité (ou anonyme). Obligatoire sur un AD.  
- Exemple LDAP :  
'uid=username,ou=my\_lan,o=mycompany,c=FR'.  
- Exemple AD : 'username' ou  
'cn=username,cn=Users,dc=server\_name,dc=localdomain'

Mot de passe:  
Laissez vide pour un accès invité (ou anonyme).  
Obligatoire sur un AD

## Installation de OpenLDAP et de l'outil d'administration

Pour l'installation de OpenLDAP et le gestionnaire de comptes LDAP sur Debian 12, suivre le tutoriel de HowToForge :

<https://www.howtoforge.com/how-to-install-openldap-server-on-debian-12/#configuring-ldap-account-manager>

Depuis le terminal de la VM client :

Configurer un nom de domaine pour le serveur Ldap

**hostnamectl set-hostname ldap.mondomaine.local**

On ouvre le fichier **nano /etc/hosts** pour y ajouter l'adresse IP correspondant au serveur Ldap.

On installe le serveur LDAP avec la commande :

**apt install slapd ldap-utils -y**



```
dfsg-5 [144 kB]
1 730 ko réceptionnés en 1s (2 543 ko/s)
Préconfiguration des paquets...
Sélection du paquet libodbc2:amd64 précédemment désélectionné.
(Lecture de la base de données... 150203 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libodbc2_2.3.11-2+deb12u1_amd64.deb ...
Dépaquetage de libodbc2:amd64 (2.3.11-2+deb12u1) ...
Sélection du paquet slapd précédemment désélectionné.
Préparation du dépaquetage de .../slapd_2.5.13+dfsg-5_amd64.deb ...
Dépaquetage de slapd (2.5.13+dfsg-5) ...
Sélection du paquet ldap-utils précédemment désélectionné.
Préparation du dépaquetage de .../ldap-utils_2.5.13+dfsg-5_amd64.deb ...
Dépaquetage de ldap-utils (2.5.13+dfsg-5) ...
Paramétrage de ldap-utils (2.5.13+dfsg-5) ...
Paramétrage de libodbc2:amd64 (2.3.11-2+deb12u1) ...
Paramétrage de slapd (2.5.13+dfsg-5) ...
  Creating new user openldap... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u3) ...
root@ldap:/home/safia#
```

To direct input to this VM, click inside or press Ctrl+G.



Une fois que le serveur OpenLDAP est installé, on exécute la commande :

**dpkg-reconfigure slapd**

Pendant l'installation, on enregistre le mot de passe pour l'administrateur LDAP (admin).

Configuration de slapd

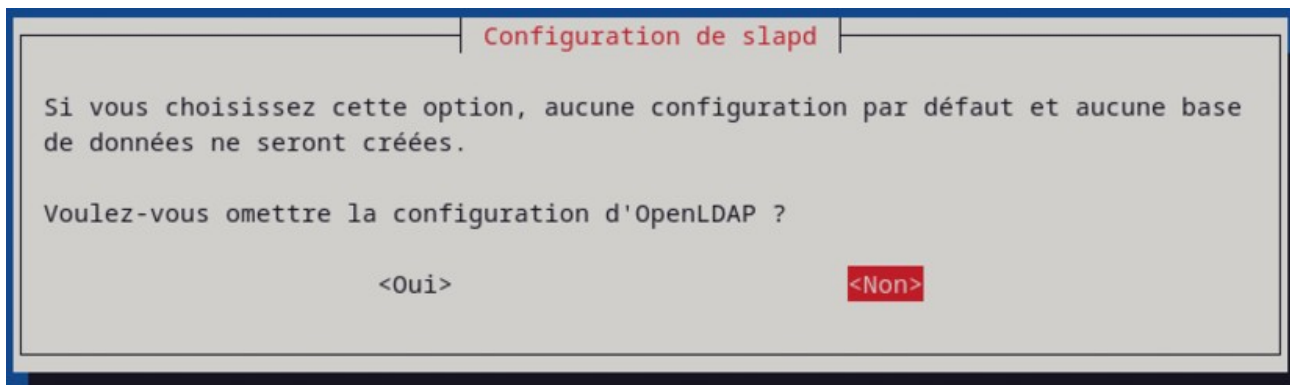
Veuillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.

Mot de passe de l'administrateur :

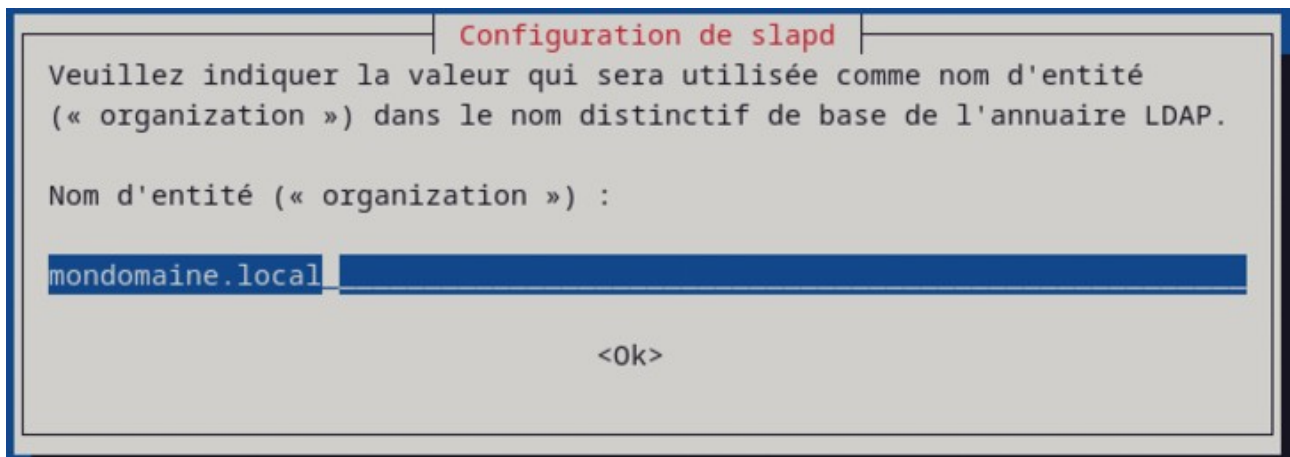
\*\*\*\*\*

<Ok>

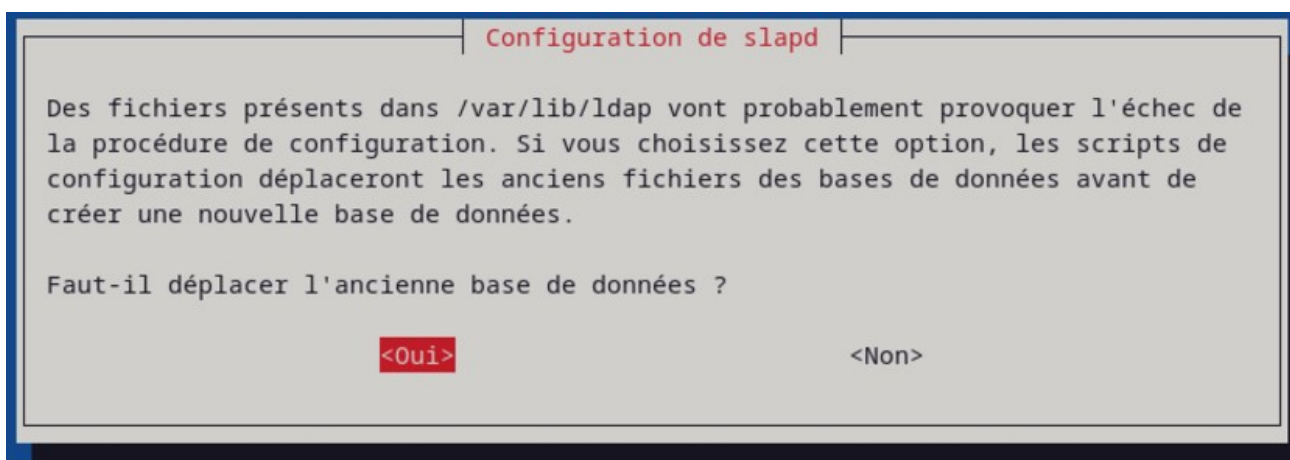
Lorsque il y a l'option « Omettre la configuration par défaut d'OpenLDAP »  
**répondre NON.**



On doit aussi saisir le nom de domaine, dans notre cas ce sera :  
**ldap.mondomaine.local**



Pour l'option « Faut-il déplacer l'ancienne base de données ? »  
répondre **OUI**.



A la fin de la configuration du serveur OpenLDAP on exécute les commandes :  
**systemctl restart slapd**  
**systemctl status slapd**

puis **slapcat**

```
root@ldap:/home/safia# sudo slapcat
dn: dc=mondomaine,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: mondomaine.local
dc: mondomaine
structuralObjectClass: organization
entryUUID: bf419f1e-d587-103e-898a-0750c884173d
creatorsName: cn=admin,dc=mondomaine,dc=local
createTimestamp: 20240713171903Z
entryCSN: 20240713171903.710991Z#000000#000#000000
modifiersName: cn=admin,dc=mondomaine,dc=local
modifyTimestamp: 20240713171903Z

root@ldap:/home/safia# █
```

## Sécurisation d'OpenLDAP avec UFW

On installe UFW, qui est un outil de gestion de pare-feu, pour sécuriser le serveur OpenLDAP pour pouvoir ensuite ouvrir les protocoles LDAP, LDAPS, HTTP et HTTPS.

UFW permet de configurer des règles pour autoriser ou bloquer le trafic réseau entrant et sortant, aidant à protéger le système contre les accès non autorisés.

Il permet d'activer ou de désactiver facilement le pare-feu avec des commandes simples.

Installation avec la commande : **apt install ufw**

Après l'installation, il faut ajouter le profil OpenSSH et activer UFW dès le démarrage du système avec les commandes :

```
ufw allow OpenSSH
ufw enable
```

Le système indique qu'UFW est activé et en cours d'exécution.

```
Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u3) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
root@ldap:/home/safia# ufw allow OpenSSH
bash: ufw : commande introuvable
root@ldap:/home/safia# sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
root@ldap:/home/safia# sudo ufw enable
Firewall is active and enabled on system startup
root@ldap:/home/safia# sudo ufw allow LDAP
Rule added
Rule added (v6)
root@ldap:/home/safia# sudo ufw allow LDAPS
Rule added
Rule added (v6)
root@ldap:/home/safia# sudo ufw allow "WWW Full"
Rule added
Rule added (v6)
root@ldap:/home/safia# █
```

Ensuite, on exécute les commandes suivantes pour LDAP, LDAPS et tous les sites web :

```
ufw allow LDAP
ufw allow LDAPS
ufw allow «WWW Full».
```

On recharge UFW et on applique les modifications avec les commandes :

```
ufw reload
```

```

Rule added (v6)
root@ldap:/home/safia# sudo ufw allow LDAPS
Rule added
Rule added (v6)
root@ldap:/home/safia# sudo ufw allow "WWW Full"
Rule added
Rule added (v6)
root@ldap:/home/safia# sudo ufw reload
Firewall reloaded
root@ldap:/home/safia# sudo ufw status
Status: active

To Action From
--
OpenSSH ALLOW Anywhere
LDAP ALLOW Anywhere
LDAPS ALLOW Anywhere
WWW Full ALLOW Anywhere
OpenSSH (v6) ALLOW Anywhere (v6)
LDAP (v6) ALLOW Anywhere (v6)
LDAPS (v6) ALLOW Anywhere (v6)
WWW Full (v6) ALLOW Anywhere (v6)

root@ldap:/home/safia# █

```

To direct input to this VM, click inside or press Ctrl+G.



**ufw status**

## Création des groupes

Après l'installation du serveur OpenLDAP et de UFW, on peut créer un groupe de base avec un fichier LDIF. Ce fichier servira à stocker les utilisateurs et les groupes OpenLDAP. On utilise la commande :

**nano base.ldif**

```
GNU nano 7.2                                base.ldif
# base.ldif

dn: ou=People,dc=ldap,dc=mondomaine,dc=local
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=ldap,dc=mondomaine,dc=local
objectClass: organizationalUnit
ou: Groups

[ Lecture de 9 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

On a créé deux groupes de base **People** et **Groups**.

Pour ajouter ces nouveaux groupes de base, avec le fichier « base.ldif » on doit exécuter la commande :

```
ldapadd -x -D cn=admin,dc=ldap,dc=mondomaine,dc=local -W -f base.ldif
```

On peut exécuter la commande **ldapsearch** pour retrouver les deux groupes de base « **People** » et « **Groups** » que l'on vient de créer sur le serveur OpenLDAP :

```
ldapsearch -x -b «dc=ldap,dc=mondomaine,dc=local» ou
```

```
# requesting: ou
#

# ldap.mondomaine.local
dn: dc=ldap,dc=mondomaine,dc=local

# People, ldap.mondomaine.local
dn: ou=People,dc=ldap,dc=mondomaine,dc=local
ou: People

# Groups, ldap.mondomaine.local
dn: ou=Groups,dc=ldap,dc=mondomaine,dc=local
ou: Groups

# safia, People, ldap.mondomaine.local
dn: uid=safia,ou=People,dc=ldap,dc=mondomaine,dc=local

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
root@ldap:/home/safia#
```

## Ajouter un nouvel utilisateur

Pour créer un utilisateur, on doit générer un mot de passe chiffré avec la commande :

**slappasswd**

```
safia@ldap:~$ su
Mot de passe :
root@ldap:/home/safia# slappasswd
bash: slappasswd : commande introuvable
root@ldap:/home/safia# sudo slappasswd
New password:
Re-enter new password:
{SSHA}BNfnNGGY6n31btOnI/cX/8jgy6Mp8iFw
root@ldap:/home/safia#
```

4, click inside or press Ctrl+G.



On crée un autre fichier **user.ldif**, avec le mot de passe qui vient d’être généré :

```
GNU nano 7.2 user.ldif
# user.ldif

dn: uid=safia,ou=People,dc=ldap,dc=mondomaine,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn:safia
sn:meradji
userPassword: {SSHA}BNfnNGGY6n31btOnI/cX/8jgy6Mp8iFw
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/safia
shadowlastChange: 0
shadowMax: 0
shadowWarning: 0

[ Lecture de 17 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^N Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

To direct input to this VM, click inside or press Ctrl+G.

Ensuite, pour ajouter cet utilisateur, on exécute la commande :

**ldapsearch -x -b «ou=People,dc=ldap,dc=mondomaine,dc=local»**



```
safia@ldap: ~  
# safia, People, ldap.mondomaine.local  
dn: uid=safia,ou=People,dc=ldap,dc=mondomaine,dc=local  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
cn: safia  
sn: meradji  
loginShell: /bin/bash  
uidNumber: 2000  
gidNumber: 2000  
homeDirectory: /home/safia  
shadowLastChange: 0  
shadowMax: 0  
shadowWarning: 0  
uid: safia  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 3  
# numEntries: 2  
root@ldap:/home/safia#
```

## Installation du gestionnaire de compte LDAP (LAM)

Une fois l'installation du serveur OpenLDAP terminée, on installe un gestionnaire de compte LDAP (LAM LDAP Account Manager) sur notre serveur OpenLDAP.

On exécute la commande :

```
apt instal ldap-account-manager
```

Cette installation comporte des dépendances supplémentaires comme PHP 8.2 et le serveur web Apache2.

```

safia@ldap: ~
+
end/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service
→ /lib/systemd/system/apache-htcacheclean.service.
Paramétrage de libapache2-mod-php8.2 (8.2.20-1~deb12u1) ...

Creating config file /etc/php/8.2/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php8.2
Paramétrage de php-gmp (2:8.2+93) ...
Paramétrage de php-zip (2:8.2+93) ...
Paramétrage de php8.2 (8.2.20-1~deb12u1) ...
Paramétrage de php (2:8.2+93) ...
Paramétrage de ldap-account-manager (8.3-1) ...
Enabling conf ldap-account-manager.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u3) ...
Traitement des actions différées (« triggers ») pour php8.2-cli (8.2.20-1~deb12u1) ...
Traitement des actions différées (« triggers ») pour libapache2-mod-php8.2 (8.2.20-1~de
b12u1) ...
root@ldap:/home/safia#
```

On modifie le paramètre mémoire en ajoutant au fichier de configuration **nano** **/etc/php/8.2/apache2/php.ini** la ligne suivante : `memory_limit = 256M`

Ensuite, on modifie aussi les paramètres IP dans le fichier de configuration : **nano** **/etc/apache2/conf-enabled/ldap-account-manager.conf**

On change les lignes « Require all granted » par « Require IP 127.0.0.1 172.16.0.3 » qui correspond notre serveur OpenLDAP.

127.0.0.1 permet l'accès en local

172.16.0.3 est l'adresse IP de notre serveur OpenLDAP.

```
GNU nano 7.2 /etc/apache2/conf-enabled/ldap-account-manager.conf *

Alias /lam /usr/share/ldap-account-manager

# HSTS header to enforce https:// connections (requires active mod_headers)
# Header always set Strict-Transport-Security "max-age=31536000"

<Directory /usr/share/ldap-account-manager>
    Options +FollowSymLinks
    AllowOverride None
    # Require all granted
Require ip 127.0.0.1 172.16.0.3
    DirectoryIndex index.html
</Directory>

<Directory /var/lib/ldap-account-manager>
    AllowOverride None
</Directory>

<Directory /var/lib/ldap-account-manager/tmp>
    Options -Indexes

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

On enregistre et on quitte le fichier, ensuite on redémarre le serveur apache2 avec la commande :

**systemctl restart apache2**

Pour accéder aux commandes du gestionnaire de compte LAM, il suffit d'ouvrir une page web et de se connecter avec l'IP que l'on a enregistré dans le fichier `/etc/php/8.2/apache2/php.ini`.

Ou, on peut configurer le gestionnaire via un navigateur web :

on utilise, pour accéder à la page web du serveur l'IP 127.0.0.1

Pour la configuration générale du gestionnaire de compte on accède au fichier **`/etc/ldap-account-manager/config.cfg`**

```
GNU nano 7.2 /etc/ldap-account-manager/config.cfg *
password: {CRYPT-SHA512}$6$1XvLx1Lge0kbfs4v$QSCS/8oeK.y1MSL9y6etyQJDkWen0CbsrPZTK1FC7M>
default: lam
logLevel: 4
logDestination: SYSLOG
configDatabaseType: files
configDatabaseServer:
configDatabasePort:
configDatabaseName:
configDatabaseUser:
configDatabasePassword: Y;Vc8tqR.^6DB'Z
license:
sessionTimeout: 30
hideLoginErrorDetails: true
allowedHosts: 127.0.0.1
allowedHostsSelfService:
passwordMinLength: 4
passwordMinUpper: 0
passwordMinLower: 0
passwordMinNumeric: 0
passwordMinSymbol: 0

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

**Pour gérer les utilisateurs à partir de la page web :**

On enregistre un utilisateur (lam par défaut) et on crée le mot de passe spécifique.

LDAP Account Manager

127.0.0.1/lam/templates/login.php

User name

Manager

Password

Language

English (Great Britain)

Login

LDAP server

ldap://localhost:389

Server profile

lam

To direct input to this VM, click inside or press Ctrl+G.

127.0.0.1/lam/templates/config/confImportExport.php

Account Manager - 8.3

Aide

Mot de passe principal

?

Ok

page de connexion

← → ↻ 127.0.0.1/lam/templates/config/mainmanage.php ☆ 🛡️ 📌 ☰

## Paramètres généraux

---

### Configuration storage

Type de base de données    Local file system ?

---

### Paramètres de sécurité

Durée de la session    30 ?

Hide LDAP details on failed login    ☐ ?

Machines autorisées     ?

Certificats SSL    utiliser les certificats d'AC du système ?

Aucun fichier sélectionné.   

← → ↻ 127.0.0.1/lam/templates/config/mainmanage.php ☆ 🛡️ 📌 ☰

Certificats SSL    utiliser les certificats d'AC du système ?

Aucun fichier sélectionné.   

---

### Stratégie de mot de passe

Longueur minimum du mot de passe    0 ?

Nombre minimum de minuscules    0 ?

Nombre minimum de majuscules    0 ?

Nombre minimum de caractères numériques    0 ?

Nombre minimum de symboles    0 ?

Nombre minimum de classes de caractères    0 ?

Le nombre de règles qui doivent correspondre    tout ?

On peut paramétrer la taille et la composition des mots de passe des utilisateurs.

127.0.0.1/lam/templates/config/mainmanage.php

Le nombre de règles qui doivent correspondre

tout

?

Le mot de passe ne doit pas contenir le nom de famille

☐

?

Le mot de passe ne doit pas contenir d'élément du nom d'utilisateur, du prénom ou du nom

☐

?

Vérification externe du mot de passe

?

Connexion

Niveau de journalisation

Avertissement

?

Destination du log

Log système

?

Rapport d'erreur PHP

défaut

?

Modifier le mot de passe principal

Niveau de journalisation

Avertissement

?

Destination du log

Log système

?

Rapport d'erreur PHP

défaut

?

Modifier le mot de passe principal

Nouveau mot de passe principal

?

Entrez le mot de passe à nouveau

Sauvegarder

Annuler

The screenshot shows a web browser window with the address bar displaying "127.0.0.1/lam/templates/config/confmain.php". The page title is "Configuration LDAP". At the top, there is a navigation bar with several links: Tests, Éditeur de profil, Édition multiple, Import / export LDAP, Explorateur de schéma, and Vue arborescente. Below this, there is a section for "Vue arborescence" with a text input field for "Suffixe arborescence" containing "dc=ldap,dc=mondomaine,dc=local".

Below the "Vue arborescence" section, there is a section titled "Paramètres de sécurité" with a lock icon. It contains a dropdown menu for "Méthode de connexion" set to "Liste fixe" and a text input field for "Liste des utilisateurs valides" containing "cn=admin,dc=ldap,dc=mondomaine,dc=local".

Below the "Paramètres de sécurité" section, there is a section titled "Global password policy override" with a lock icon. It contains five dropdown menus for password policy settings: "Longueur minimum du mot de passe", "Nombre minimum de minuscules", "Nombre minimum de majuscules", "Nombre minimum de caractères numériques", and "Nombre minimum de symboles".

At the bottom, there is a section titled "Authentification à 2 facteurs" with a lock icon.

Dans les **paramètres généraux**, il faut configurer les parties suivantes :

- Dans les suffixes arborescence, l'utilisateur admin et le nom de domaine.
- Dans les **paramètres de sécurité**, sélectionner la méthode de connexion comme Liste fixe et les détails de l'utilisateur administrateur pour le serveur OpenLDAP.
- Dans le **mot de passe du profil**, saisir le nouveau mot de passe et répéter.

Cliquer **sur Enregistrer** pour appliquer les modifications.





## Informations serveur

<b>Suffixes gérés</b>	dc=ldap,dc=mondomaine,dc=local
<b>Version de LDAP</b>	3
<b>Suffixe de config</b>	cn=config
<b>Suffixe de schéma</b>	cn=Subschema
<b>Mécanisme SASL</b>	SCRAM-SHA-512, SCRAM-SHA-384, SCRAM-SHA-256, SCRAM-SHA-224, SCRAM-SHA-1, DIGEST-MD5, CRAM-MD5, NTLM

On peut créer des comptes par chargement de **fichiers CSV**. Il faut préalablement préparer un fichier CSV avec les informations nécessaires pour les comptes d'utilisateurs.

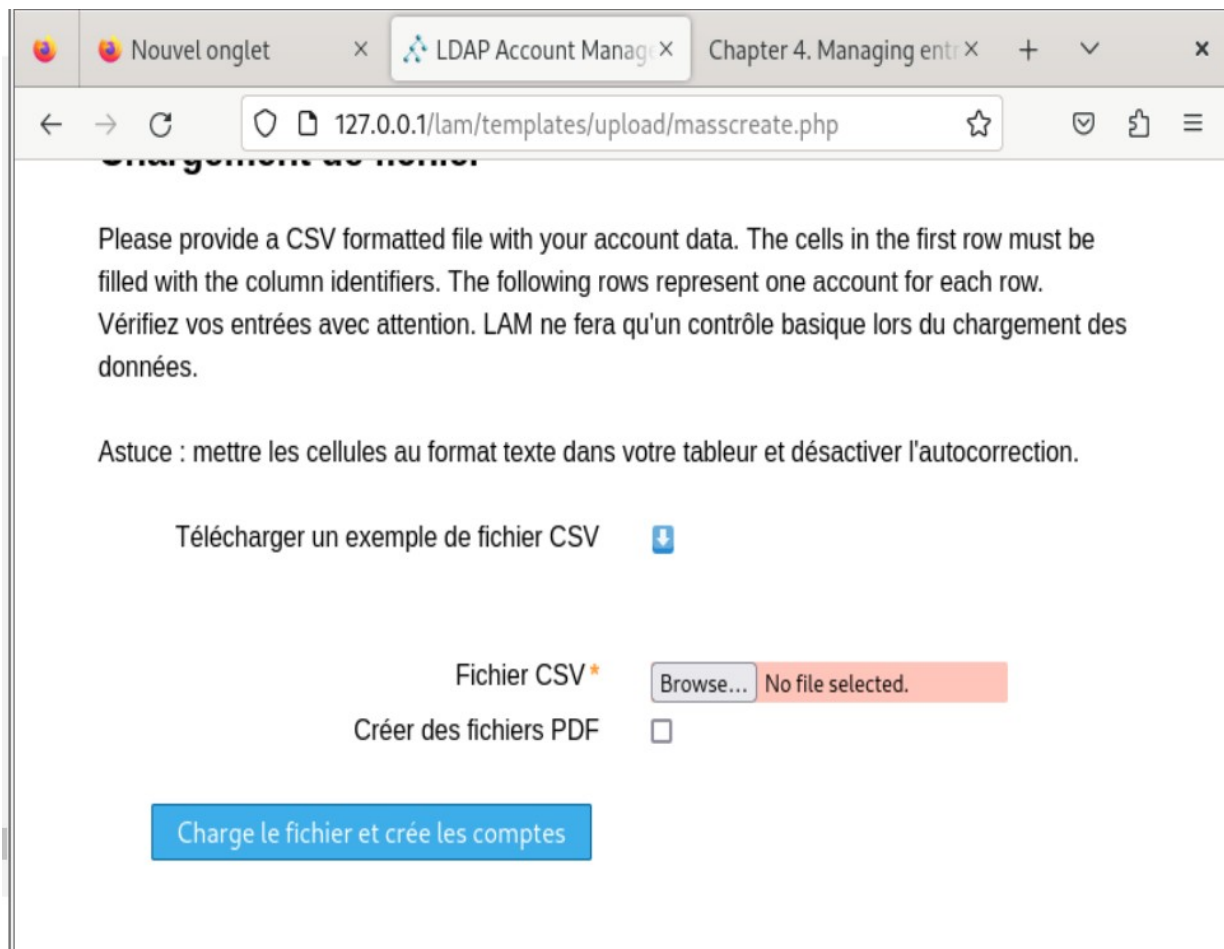
Le fichier dépendra des informations que l'on veut enregistrer pour les comptes utilisateurs.

### Exemple de fichier :

uid,cn,sn,userPassword,uidNumber,gidNumber,homeDirectory

1. jdoe,John Doe,Doe,{SSHA}hashedpassword,1001,100, /home/jdoe
2. asmith,Alice Smith,Smith,{SSHA}hashedpassword,1002,100, /home/asmith

- uid : Identifiant unique de l'utilisateur.
- cn : Nom commun de l'utilisateur.
- sn : Nom de famille.
- userPassword : Mot de passe (généralement sous forme hachée).
- uidNumber : Numéro d'utilisateur.
- gidNumber : Numéro de groupe.
- homeDirectory : Répertoire personnel.



Ensuite, on va sur la section **Types de comptes** pour configurer :

- Dans la section **Utilisateurs** , saisir le domaine de base par défaut pour les utilisateurs OpenLDAP. Dans ce cas, le suffixe par défaut est **People** .
- Dans la section **Groupes** , saisir le domaine de base par défaut du groupe. Dans ce cas, l'autre groupe par défaut est **Groups** .

Cliquer **sur Enregistrer** pour appliquer les modifications.

On peut aussi enregistrer les utilisateurs sous formes de texte ou de tableau.

# Import de texte - [lam.csv]

## Importer

Jeu de caractères : Unicode (UTF-8)

Locale : Par défaut - Français (France)

À partir de la ligne : 1

## Options de séparateur

☐ Largeur fixe

☒ Séparé par

☒ Tabulation ☒ Virgule ☒ Point-virgule ☐ Espace ☐ Autre

☐ Fusionner les séparateurs ☐ Espaces superflus

Séparateur de chaîne de caractères :

"

## Autres options

☐ Formater les champs entre guillemets comme texte ☐ Détecter les nombres spéciaux

☐ Évaluer les formules

## Champs

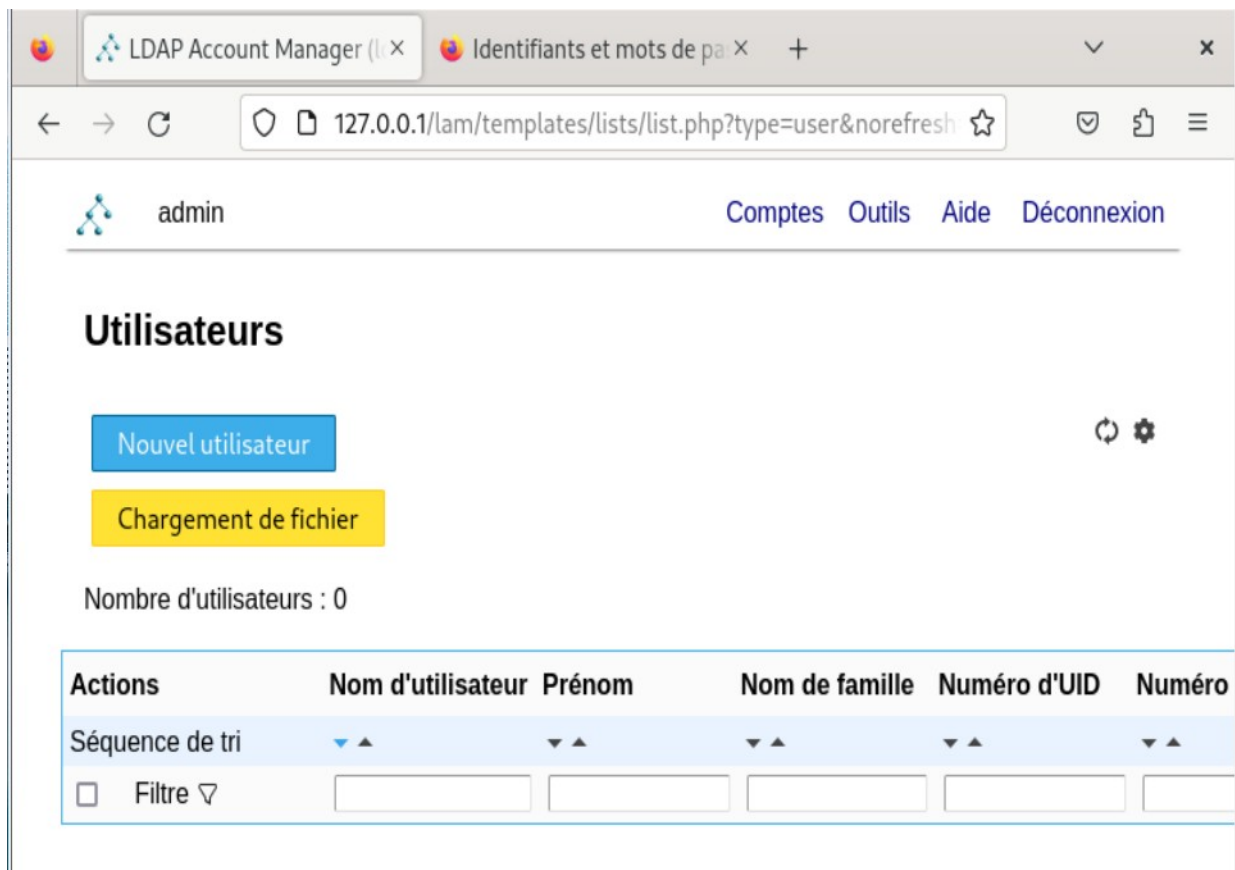
Type de colonne :

	Standard	Standard	Standard	Standard	Standard
1	dn_suffix	dn_rdn	overwrite	inetOrgPerson_firstName	inetOrgPerson_lastName
2	ou=People,dc=my-domain,dc=com	uid	false	Steve	Miller?

Aide

Annuler

OK



LDAP Account Manager (LAM) est une interface Web permettant de gérer les entrées (par exemple les utilisateurs, les groupes, les paramètres DHCP) stockées dans un annuaire LDAP. L'outil LDAP Account Manager a été conçu pour rendre la gestion LDAP aussi simple que possible pour l'utilisateur.

LAM facilite l'administration des entrées LDAP en faisant abstraction des détails techniques du LDAP et en permettant aux administrateurs et aux utilisateurs sans connaissances techniques de gérer le serveur LDAP.