SERVEUR ANNUAIRE

LLDAP sur Debian 11

Noah MAILLET

Projet-SANDBOX

Table of Contents

1 Preface

1.1 Presentation LDAP.

1.1.1 Protocole LDAP.

LDAP (Lightweight Directory Access Protocol) est un protocole de communication standard pour accéder et modifier des services d'annuaire à distance. Il est couramment utilisé pour gérer des informations sur les utilisateurs, les groupes, les services et d'autres entités dans un environnement informatique. LDAP simplifie l'accès aux informations en les stockant dans un annuaire centralisé et en offrant une interface de recherche standardisée. Il est souvent utilisé pour l'authentification et l'autorisation des utilisateurs dans les systèmes informatiques et pour stocker des données sensibles telles que des mots de passe de manière sécurisée. LDAP offre également des fonctionnalités de sécurité avancées telles que l'authentification sécurisée et le contrôle d'accès basé sur les rôles et les groupes.

1.1.2 Service LLDAP.

LLDAP (Lightweight LDAP) est un serveur d'authentification léger offrant une interface LDAP simplifiée et intuitive pour l'authentification. Il s'intègre facilement avec divers backends, allant de KeyCloak à Authelia en passant par Nextcloud et bien d'autres encore.

Son interface utilisateur conviviale facilite la gestion des utilisateurs et permet à ces derniers de modifier leurs propres informations ou de réinitialiser leur mot de passe via e-mail.

LLDAP se concentre sur l'auto-hébergement et est spécifiquement conçu pour des serveurs utilisant des logiciels open source tels que Nextcloud, Airsonic, etc., qui ne prennent en charge que LDAP comme source d'authentification externe.

Bien qu'il ne fournisse pas toutes les fonctionnalités d'un serveur LDAP complet comme OpenLDAP, LLDAP est un système de gestion des utilisateurs léger, facile à installer, à gérer et à utiliser. Il est adapté à ceux qui veulent éviter les complexités de LDAP tout en profitant de ses avantages pour l'authentification.

Les données sont stockées par défaut dans une base de données SQLite, mais vous avez la possibilité d'utiliser MySQL/MariaDB ou PostgreSQL comme backend. De plus, si vous recherchez des fonctionnalités avancées telles que le support OAuth/OpenID ou un proxy inverse, vous pouvez installer d'autres composants comme KeyCloak ou Authelia et les configurer pour utiliser LLDAP comme source de vérité pour les utilisateurs via LDAP.

1.2 Configuration minimale.

Annuaire (https://urlz.fr/pyaD) :

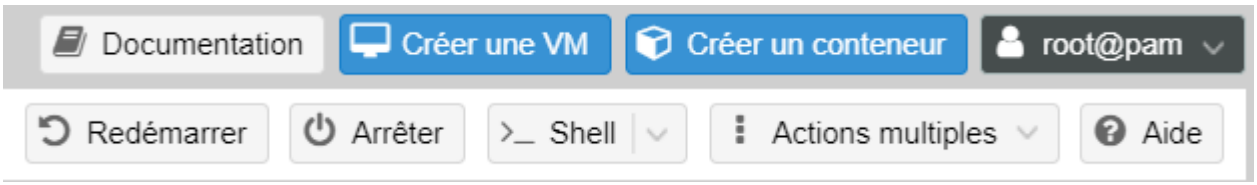
- Processeur : 1 cœur
- RAM : 512Mo
- Espace disque : 10Go

2 Création du conteneur.

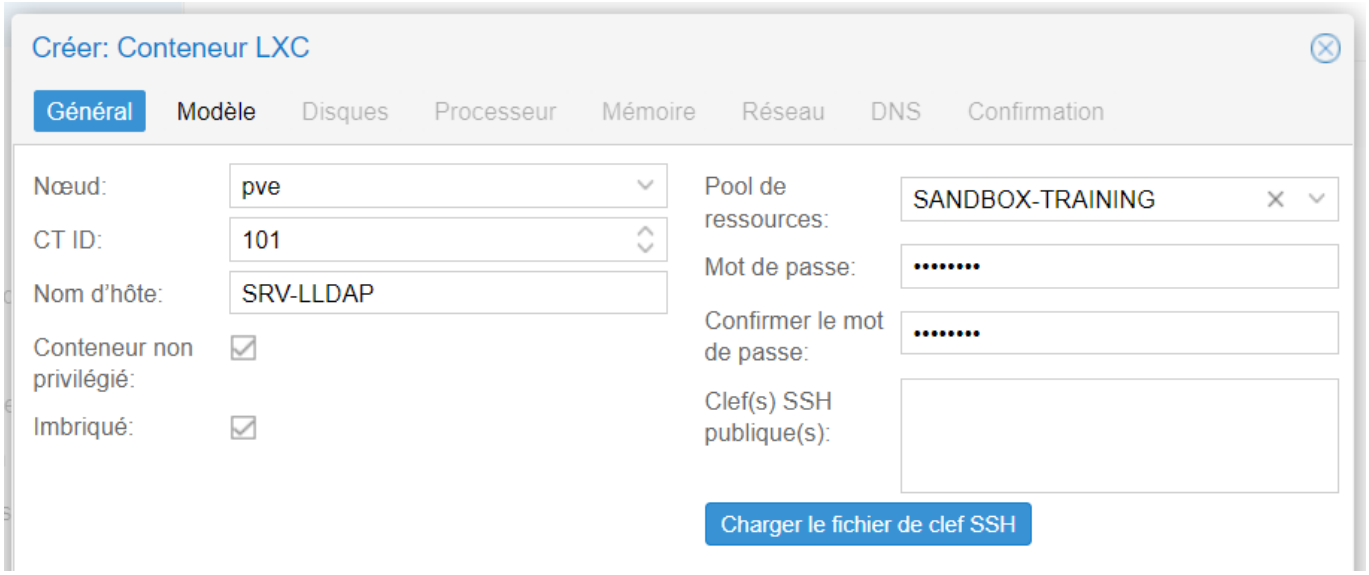
Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est Proxmox.

Vous pouvez installer LLDAP dans tout autre environnement de virtualisation tant que vous respectez la configuration minimale.

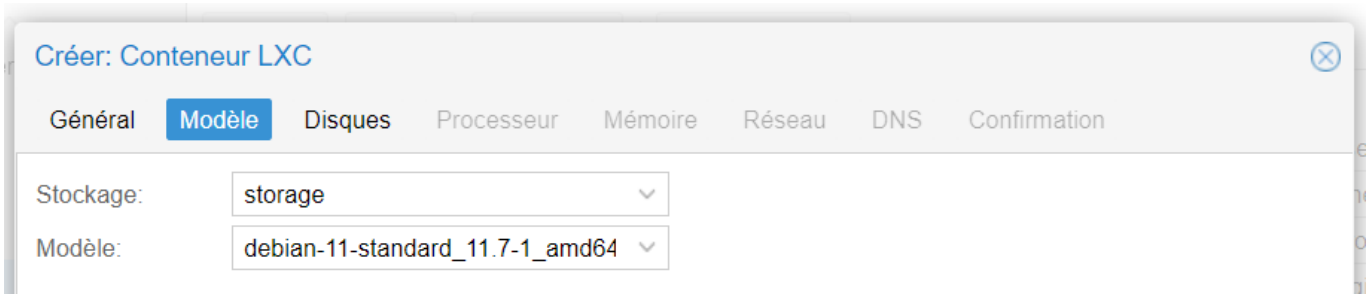
1. Je me connecte à mon proxmox.
2. Créer un conteneur.



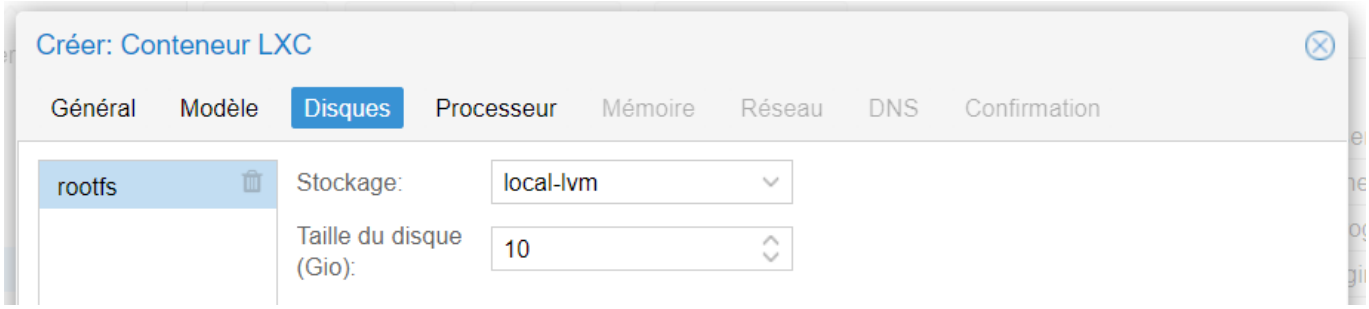
3. Je renseigne le numéro du conteneur, le nom de l'hôte « SRV-LLDAP », le pool de ressource « SANDBOX-TRAINING », configuration du mot de passe. ➔ Suivant.



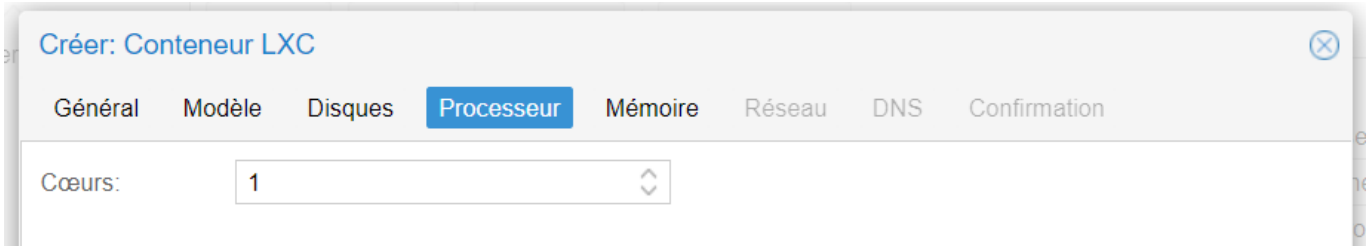
4. Je sélectionne le modèle de mon conteneur ➔ suivant.



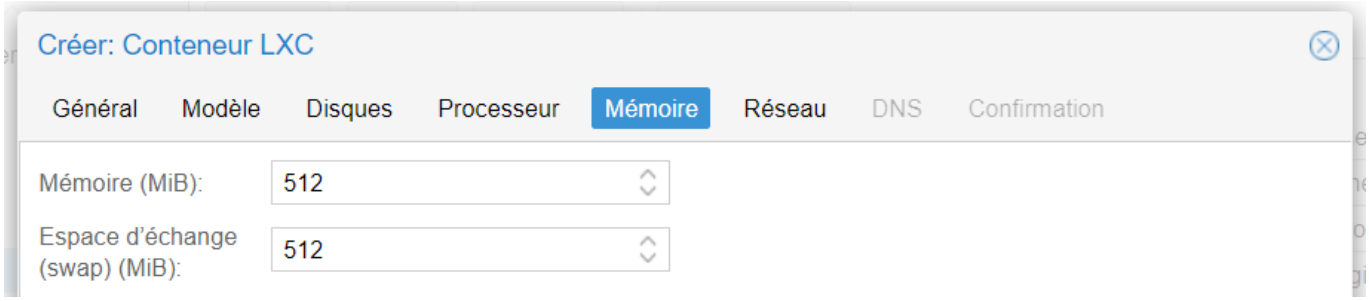
5. J'alloue 10Go de stockage. ➔ Suivant.



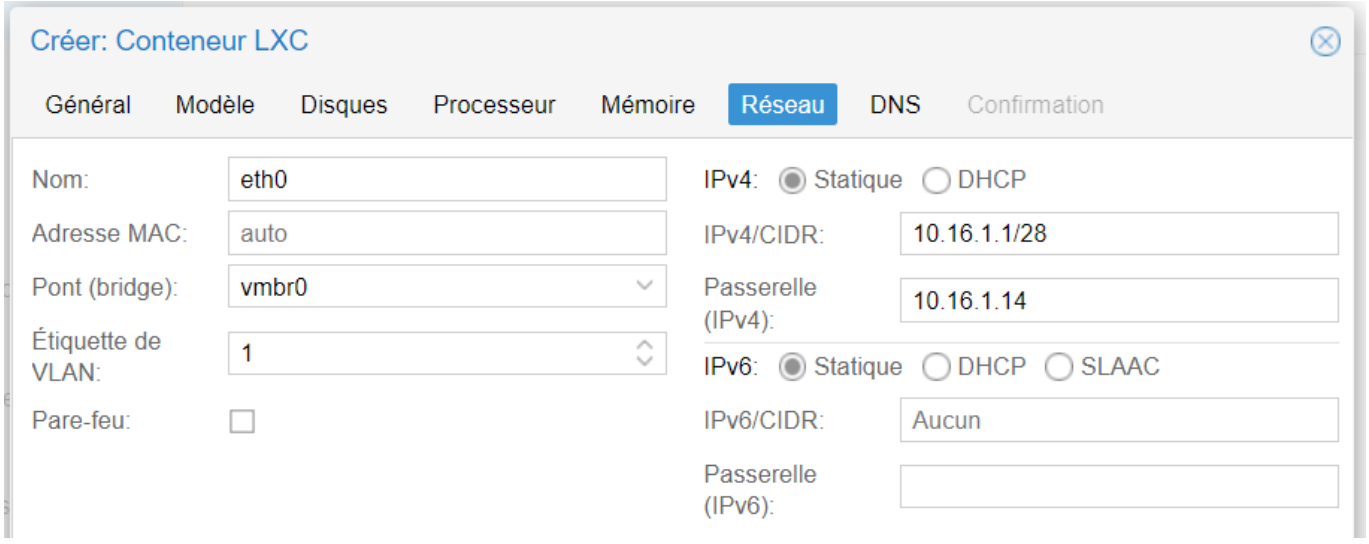
6. J'alloue 1 cœur de processeur. ➔ Suivant.



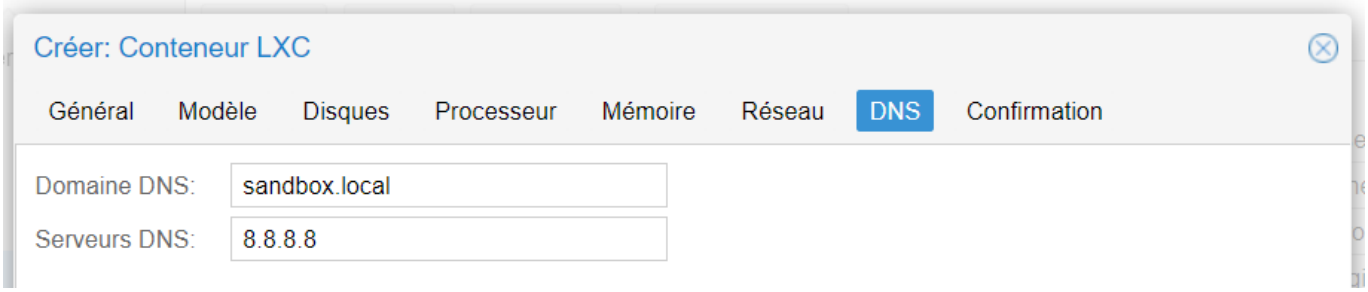
7. Je laisse la configuration par défaut ➔ suivant.



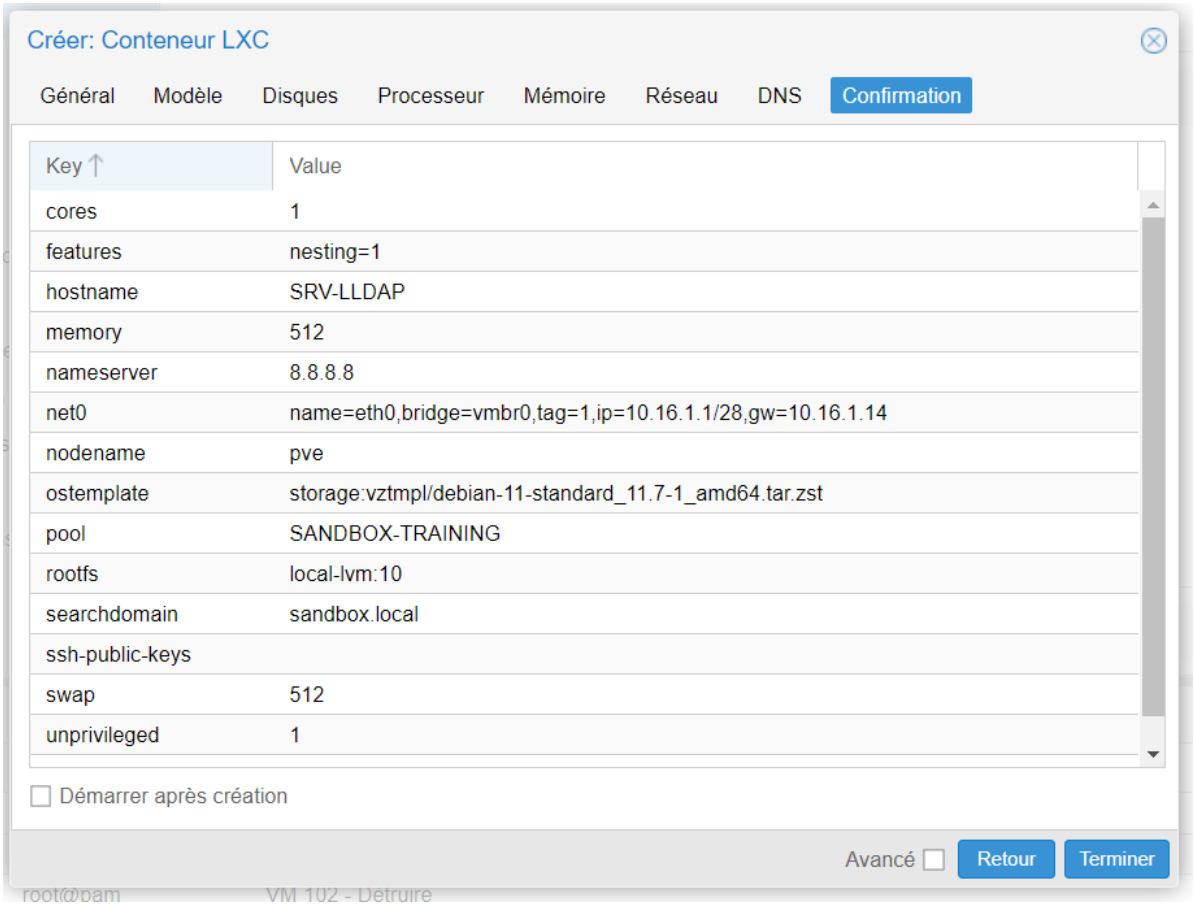
8. Je renseigne le VLAN et les @IP, je décoche l'option pare-feu ➔ Suivant.



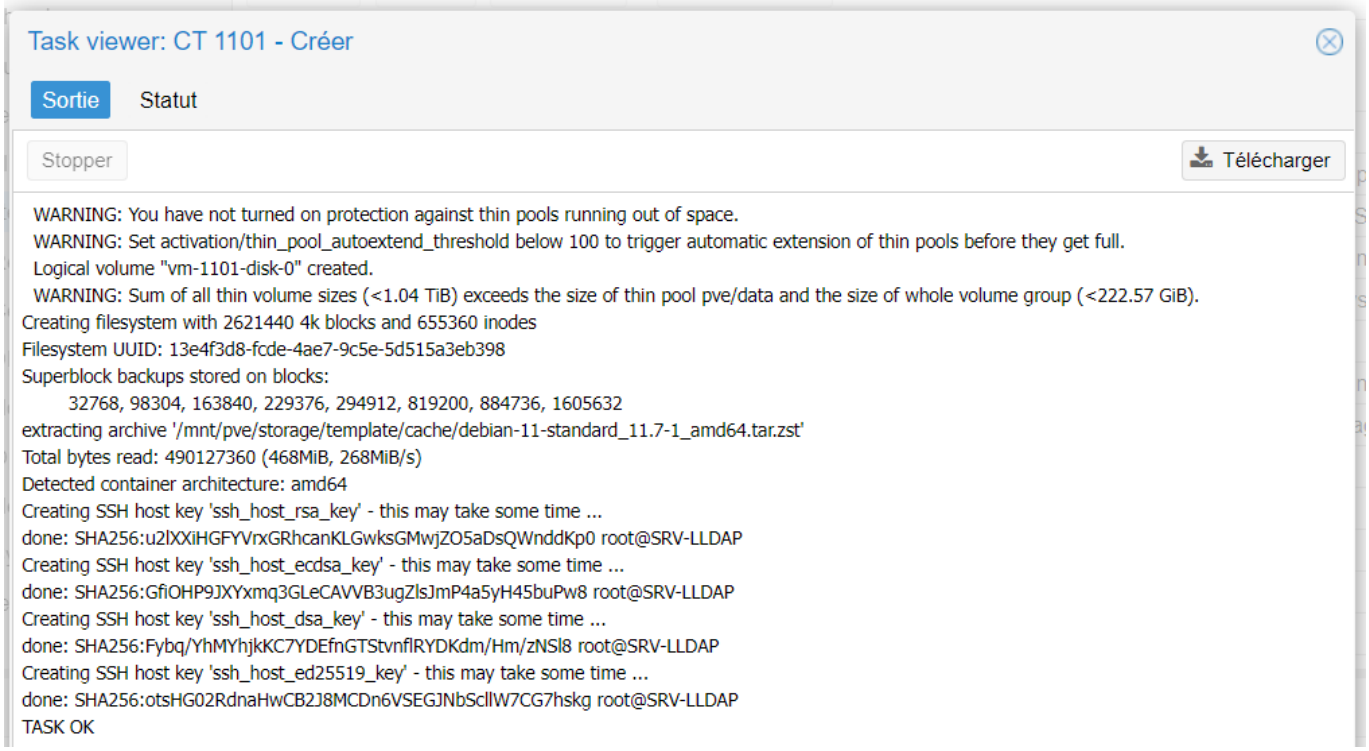
9. Je rentre le nom de domaine et le DNS. ➔ Suivant.



10. Je vérifie que toutes les informations sont correctes ➔ terminer.



11. Le conteneur a été créé.



3 Installation LLDAP.

1. Je me connecte à ma ferme de serveur Proxmox.
2. J'allume le conteneur « SRV-LLDAP ».
3. Je me connecte au conteneur.

```
SRV-LLDAP login: root
Password:
Linux SRV-LLDAP 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar  7 10:40:12 UTC 2024 on tty1
root@SRV-LLDAP:~#
```

4. Test de l'accès à internet.

```
root@SRV-LLDAP:~# ping www.google.fr
PING www.google.fr (142.250.179.67) 56(84) bytes of data.
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=1 ttl=115 time=12.8 ms
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=2 ttl=115 time=12.5 ms
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=3 ttl=115 time=12.3 ms
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=4 ttl=115 time=12.5 ms
^C
--- www.google.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 12.280/12.520/12.821/0.194 ms
root@SRV-LLDAP:~#
```

5. Je mets à jour les paquets.

Commande :

```
apt update && apt upgrade
```

```
root@SRV-LLDAP:~# apt update && apt upgrade
Hit:1 http://security.debian.org bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@SRV-LLDAP:~#
```

6. Ajout du dépôt LLDAP.

Commande :

```
echo 'deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian_11/ /' | sudo tee /etc/apt/sources.list.d/home:Masgalor:LLDAP.list
```

```
root@SRV-LLDAP:~# echo 'deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian_11/ /' | sudo t
ee /etc/apt/sources.list.d/home:Masgalor:LLDAP.list
deb http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian_11/ /
```

7. Ajout du certificat SSL.

Commande:

```
curl -fsSL https://download.opensuse.org/repositories/home:Masgalor:LLDAP/Debian_11/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/home_Masgalor_LLDAP.gpg > /dev/null
```

```
root@SRV-LLDAP:~# curl -fsSL https://download.opensuse.org/repositories/home:Masgalor:LLDAP/Debian_11/Release.key
| gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/home_Masgalor_LLDAP.gpg > /dev/null
```

8. Je mets à jour les paquets et j'installe LLDAP.

Commande :

```
apt update && apt install lldap
```

9. Démarrage et activation du service LLDAP.

Commande :

```
Systemctl enable lldap
Systemctl start lldap
```

```
root@SRV-LLDAP:~# systemctl enable lldap
root@SRV-LLDAP:~# systemctl start lldap
```

4 Configuration LLDAP.

1. Je me connecte à ma ferme de serveur ProxMox.
2. J'allume la machine et je me connecte.
3. Je me rends dans /etc/lldap.

Commande :

cd /etc/lldap

4. J'ouvre le fichier de configuration : lldap_config.toml

Commande :

nano lldap_config.toml

4.1 Base DN for LDAP.

Cette section permet de modifier la racine du serveur LLDAP.

Par défaut la valeur est : ldap_base_dn = « dc=example,dc=com »

Je modifie la valeur par : ldap_base_dn = « dc=sandbox,dc=local »

```
## Base DN for LDAP.
## This is usually your domain name, and is used as a
## namespace for your users. The choice is arbitrary, but will be needed
## to configure the LDAP integration with other services.
## The sample value is for "example.com", but you can extend it with as
## many "dc" as you want, and you don't actually need to own the domain
## name.
ldap_base_dn = "dc=sandbox,dc=local"
```

4.2 Admin username.

Cette section permet de modifier le nom de l'utilisateur.

Dans notre cas de figure, nous n'avons pas besoin de le modifier.

Nous le décommentons juste pour assurer le bon nom de notre admin.

```
## Admin username.
## For the LDAP interface, a value of "admin" here will create the LDAP
## user "cn=admin,ou=people,dc=example,dc=com" (with the base DN above).
## For the administration interface, this is the username.
ldap_user_dn = "admin"
```

4.3 Admin email.

Cette section permet de modifier le mail administrateur.

Nous allons juste changer le FQDN (Full qualified Domain) pour qu'il corresponde à celui de notre domaine.

```
## Admin email.
## Email for the admin account. It is only used when initially creating
## the admin user, and can safely be omitted.
ldap_user_email = "admin@sandbox.local"
```

4.4 Admin password.

Cette section permet de modifier le mot de passe du compte administrateur.

Si vous souhaitez la valeur du mot de passe administrateur vous aurez juste à décommenter la ligne « ldap_user_pass » et remplacer la valeur de « Remplace_with_password ».

```
## Admin password.
## Password for the admin account, both for the LDAP bind and for the
## administration interface. It is only used when initially creating
## the admin user.
## It should be minimum 8 characters long.
## You can set it with the LLDAP_LDAP_USER_PASS environment variable.
## This can also be set from a file's contents by specifying the file path
## in the LLDAP_LDAP_USER_PASS_FILE environment variable
## Note: you can create another admin user for user administration, this
## is just the default one.
ldap_user_pass = "REPLACE_WITH_PASSWORD"
```

Une fois les modifications effectuer vous devez sauvegarder le fichier et redémarrer le service.

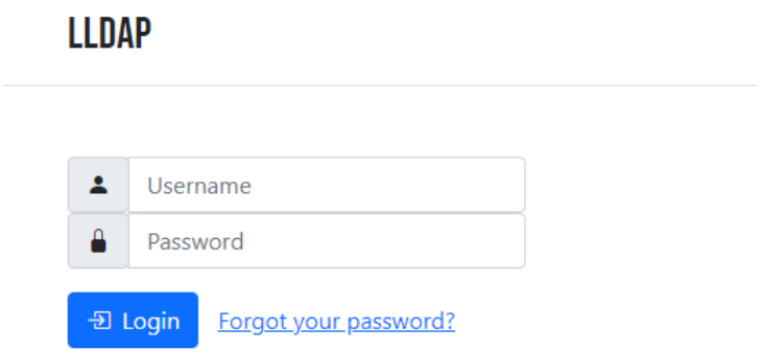
Commande :

systemctl restart lldap.service

5 Interface web.

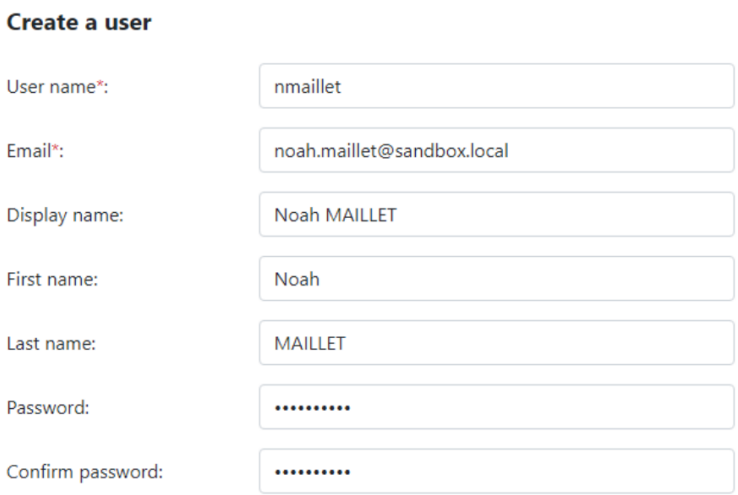
1. Je me connecte à une machine dans le même réseau local que mon Serveur LLDAP.
2. Je tape l'URL du serveur AD avec le port 1710.

http://@IP-SRV-AD:17170/login



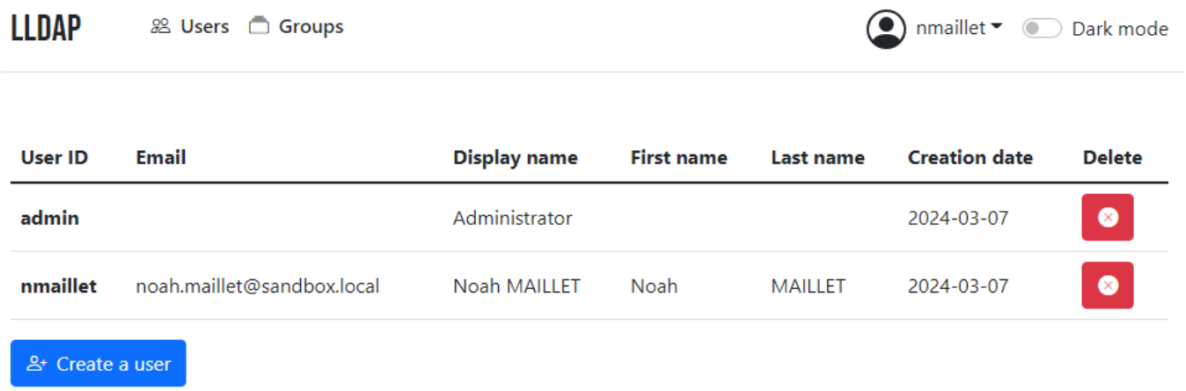
3. Je me connecte avec le compte « admin ».

4. Je créer un utilisateur à mon nom.



5. J’ajoute le compte que j’ai créé dans le groupe administrateur.

6. Je me déconnecte du compte administrateur et je me connecte avec mon nouveau compte.



Si vous avez suivi la procédure jusqu’au bout, vous devriez avoir ce résultat.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com