

# Linux

## Administration des Système Linux



### Linux-3122

**Auteur(s) :**

Yann BENHAMRON

**Destinataire(s) :**

Easyformer

Date de modification : 20/01/23

Version : 1

# Sommaire

page

<b>1</b>	<b>OBJECTIVES.....</b>	<b>4</b>
<b>2</b>	<b>QU'EST-CE QUE GNU LINUX ?.....</b>	<b>4</b>
<b>3</b>	<b>LES COMMANDES DE BASE .....</b>	<b>5</b>
3.1	QU'EST-CE QU'UNE COMMANDE LINUX ?.....	5
3.2	COMMANDE PWD .....	5
3.3	COMMANDE CD.....	5
3.4	COMMANDE LS .....	5
3.5	COMMANDE CAT .....	6
3.6	COMMANDE CP .....	6
3.7	COMMANDE MV .....	6
3.8	COMMANDE MKDIR.....	6
3.9	COMMANDE RMDIR.....	6
3.10	COMMANDE RM .....	7
3.11	COMMANDE TOUCH .....	7
3.12	COMMANDE LOCATE.....	7
3.13	GREP COMMAND .....	7
3.14	COMMANDE SUDO .....	7
3.15	COMMANDE TAR .....	7
3.16	COMMANDE CHMOD .....	8
3.17	COMMANDE CHOWN .....	8
3.18	COMMANDE PING .....	8
3.19	COMMANDE WGET.....	8
3.20	COMMANDE UNAME .....	8
3.21	COMMANDE TOP .....	8
3.22	COMMANDE HISTORY .....	8
3.23	COMMANDE HOSTNAME.....	9
3.24	COMMANDE USERADD, USERDEL .....	9
3.25	COMMANDE SHUTDOWN .....	9
<b>4</b>	<b>MISE EN PLACE DE BIND9.....</b>	<b>10</b>
4.1	INTRODUCTION .....	10
4.2	INSTALLATION DE BIND9.....	10
4.3	CONFIGURATION DE LA RESOLUTION DE NOM .....	10
4.4	CREATION D'UNE ZONE DE RECHERCHE DIRECT .....	11
4.5	CREATION D'UNE ZONE DE RECHERCHE INVERSE .....	12
4.6	ATTRIBUTION DES ZONES AU SERVEURS DNS .....	12
4.7	VERIFICATION .....	13
<b>5</b>	<b>MISE EN PLACE D'UN VHOST.....</b>	<b>13</b>
5.1	INTRODUCTION .....	13
5.2	INSTALLATION .....	13
5.3	CREATION DE LA STRUCTURE DE REPERTOIRE .....	14
5.4	CREEZ UN NOUVEAU FICHIER D'HOTES VIRTUELS.....	14
5.5	ACTIVEZ LE NOUVEAU FICHIER HOTE VIRTUEL.....	15
5.6	RENSEIGNER LE DOMAINE ET SON ADRESSE IP SUR WINDOWS .....	15
5.7	TESTEZ NOS RESULTATS .....	16
<b>6</b>	<b>MISE EN PLACE S'UN SERVEUR LAMP + WORDPRESS.....</b>	<b>16</b>
6.1	INTRODUCTION .....	16
6.2	INSTALLATION DU SERVEUR LAMP.....	17
6.3	CONFIGURATION DU SERVEUR MARIADB.....	17



6.4	INSTALLEZ PHPMyAdmin .....	18
6.5	INSTALLEZ WORDPRESS.....	19
6.6	CONFIGURATION DE WORDPRESS .....	21
<b>7</b>	<b>MISE EN PLACE D'UN SERVEUR LDAP .....</b>	<b>25</b>
7.1	INTRODUCTION .....	25
7.2	INSTALLATION DE OPENLDAP .....	25
7.3	CONFIGURATION DU SERVEUR OPENLDAP.....	26
7.4	INSTALLATION DU LAM .....	28
7.5	CONFIGURATION DU LAM .....	29
7.6	AJOUTER DES COMPTES D'UTILISATEURS ET DES GROUPES AVEC LDAP ACCOUNT MANAGER .....	32
<b>8</b>	<b>MISE EN PLACE DE SAMBA4.....</b>	<b>34</b>
8.1	INTRODUCTION .....	34
8.2	MISE EN PLACE DE DEBIAN .....	34
8.3	CONFIGURATION RESEAU DE DEBIAN .....	41
8.4	INSTALLATION DE SAMBA 4 .....	44
8.5	PROMOTION EN CONTROLEUR DE DOMAINE .....	45
8.6	CONFIGURER LE FICHIER KRB5.CONF .....	46
8.7	GERER LE SERVICE SAMBA .....	47
8.8	TEST DU SERVEUR DNS .....	48
8.9	CREATION DE LA ZONE DE RECHERCHE INVERSEE ET DE L'ENREGISTREMENT PTR.....	48
8.10	TEST DE NOTRE ZONE INVERSEE ET DE L'ENREGISTREMENT PTR.....	49
8.11	TEST D'AUTHENTIFICATION KERBEROS .....	49
8.12	RELIER UN POSTE DE TRAVAIL WINDOWS 10 A NOTRE DOMAINE TUX.LOCAL.....	50



# 1 Objectives

L'objectif est de pouvoir maîtriser l'installation et la gestion d'un système d'exploitation libre : Ubuntu serveur et Debian 11. Le programme de la sera composé :

- Cours théorique
- Connaitre les commandes de base
- Mise en place d'un serveur DNS avec BIND9 sur Ubuntu 20.04
- Mise en place de Vhost avec Apache sur Ubuntu 20.04
- Mise en place d'un serveur LDAP avec OpenLDAP sur Ubuntu 20.04 + interface graphique LAM
- Mise en place s'un serveur LAMP (Linux Apache Maria DB) avec installation de WordPress
- Bonus : Mise en place de Samba 4 sur DEBIAN 11 (si les objective précédents sont terminé)

## 2 Qu'est-ce que GNU Linux ?

Pour résumer, GNU Linux est un projet de système d'exploitation libre de droit et modifiable à souhait. Issu du travail de GNU initié par Richard Stallman au début des années 80 et du travail de Linus Torvalds, alors jeune étudiant Finlandais en 1992. À l'origine basé sur Unix dont il reprend les principales caractéristiques, Linux est aujourd'hui le système d'exploitations le plus déployer sur internet. D'abord marginal, la stabilité et la flexibilité de ses systèmes l'ont rendu indispensable au fil des années. Malgré ses qualité, Linux souffre d'un manque de communication et de simplicité dans son utilisation ce qui rend encore peu utilisable par le grand publique, bien que des versions comme Ubuntu, pour l'exemple, souhaite rendre son utilisation plus intuitive. De plus, son manque de prise en charge dans le domaine vidéoludique le pousse loin derrière Windows pour le marché des Os clients.



## 3 Les commandes de base

### 3.1 Qu'est-ce qu'une commande Linux ?

Une commande Linux est un programme ou utilitaire qui s'exécute sur la ligne de commande Linux. La ligne de commande (CLI) est un terminal qui permet à l'utilisateur de taper des instructions texte et de les faire exécuter par le système.

### 3.2 Commande pwd

Utilisez la commande `pwd` pour trouver le chemin du répertoire de travail (dossier) dans lequel vous êtes actuellement. La commande retournera un chemin absolu (complet), qui est en fait un chemin de tous les répertoires qui commence par une barre oblique (/). Un exemple de chemin absolu est `/home/utilisateur`.

### 3.3 Commande cd

Pour naviguer dans les fichiers et répertoires de Linux, utilisez la commande `cd`. Elle nécessite soit le chemin d'accès complet, soit le nom du répertoire, selon le répertoire de travail dans lequel vous vous trouvez.

Disons que vous êtes dans `/home/utilisateur/Documents` et que vous voulez aller dans `Photos`, un sous-répertoire de `Documents`. Pour ce faire, il vous suffit de taper la commande suivante : `cd Photos`.

Un autre scénario est possible si vous voulez passer à un répertoire complètement nouveau, par exemple, `/home/utilisateur/Films`. Dans ce cas, vous devez taper `cd` suivi du chemin absolu du répertoire : `cd /home/utilisateur/Films`.

Il existe quelques raccourcis pour vous aider à naviguer rapidement :

- `cd ..` (avec deux points) pour se déplacer d'un répertoire vers le haut
- `cd` pour aller directement au dossier principal (home)
- `cd-` (avec un tiret) pour passer à votre répertoire précédent

Par ailleurs, le Shell de Linux est sensible à la casse. Vous devez donc taper les noms des répertoires exactement comme ils sont.

### 3.4 Commande ls

La commande `ls` est utilisée pour visualiser le contenu d'un répertoire. Par défaut, cette commande affichera le contenu de votre répertoire de travail actuel. Si vous voulez voir le contenu d'autres répertoires, tapez `ls` et ensuite le chemin d'accès du répertoire. Par exemple, tapez `ls /home/utilisateur/Documents` pour voir le contenu de `Documents`.

Il existe des variantes que vous pouvez utiliser avec la commande `ls` :

- `ls -R` énumérera également tous les fichiers dans les sous-répertoires
- `ls -a` affichera les fichiers cachés
- `ls -al` listera les fichiers et les répertoires avec des informations détaillées comme les autorisations, la taille, le propriétaire, etc.



## 3.5 Commande cat

Cat (abréviation de concatenate) est l'une des commandes Linux les plus fréquemment utilisées. Elle est utilisée pour lister le contenu d'un fichier sur le résultat standard (sdout). Pour exécuter cette commande, tapez cat suivi du nom du fichier et de son extension. Par exemple : cat fichier.txt.

Voici d'autres façons d'utiliser la commande cat :

- `cat > nomDeFichier` crée un nouveau fichier
- `cat nomDeFichier1 nomDeFichier2 > nomDeFichier3` joint deux fichiers (1 et 2) et enregistre le résultat de ces derniers dans un nouveau fichier (3)
- pour convertir un fichier en majuscules ou en minuscules, `cat nomDeFichier | tr a-z A-Z > resultat.txt`

## 3.6 Commande cp

Utilisez la commande cp pour copier les fichiers du répertoire actuel dans un autre répertoire. Par exemple, la commande `cp scenery.jpg /home/utilisateur/Photos` créera une copie de scenery.jpg (de votre répertoire actuel) dans le répertoire Photos.

## 3.7 Commande mv

L'utilisation principale de la commande mv est de déplacer des fichiers, bien qu'elle puisse également être utilisée pour renommer des fichiers. Les arguments de mv sont similaires à ceux de la commande cp. Vous devez taper mv, le nom du fichier et le répertoire de destination. Par exemple : `mv fichier.txt /home/utilisateur/Documents`.

Pour renommer les fichiers, la commande Linux est `mv ancien_nom.ext nouveau_nom.ext`

## 3.8 Commande mkdir

Utilisez la commande mkdir pour créer un nouveau répertoire – si vous tapez `mkdir Music`, cela créera un répertoire appelé Music. Il existe également des commandes mkdir supplémentaires :

- Pour générer un nouveau répertoire à l'intérieur d'un autre répertoire, utilisez cette commande de base de Linux `mkdir Music/Nouveau`
- utiliser l'option p (parents) pour créer un répertoire entre deux répertoires existants. Par exemple, `mkdir -p Musique/2020/Nouveau` créera le nouveau répertoire « 2020 ».
- 

## 3.9 Commande rmdir

Si vous avez besoin de supprimer un répertoire, utilisez la commande rmdir. Cependant, rmdir ne vous permet de supprimer que les répertoires vides.



## 3.10 Commande rm

La commande `rm` est utilisée pour supprimer les répertoires et leur contenu. Si vous voulez seulement supprimer le répertoire – comme alternative à `rmdir` – utilisez `rm -r`.

Note : Soyez très prudent avec cette commande et vérifiez à nouveau dans quel répertoire vous vous trouvez. Cela effacera tout et il n'y aura pas d'annulation.

## 3.11 Commande touch

La commande `touch` vous permet de créer un nouveau fichier vierge via la ligne de commande Linux. Par exemple, entrez `touch /home/username/Documents/Web.html` pour créer un fichier HTML intitulé `Web` dans le répertoire `Documents`.

## 3.12 Commande locate

Vous pouvez utiliser cette commande pour localiser un fichier, tout comme la commande de recherche dans Windows. De plus, l'utilisation de l'argument `-i` avec cette commande la rendra insensible à la casse, ce qui vous permettra de rechercher un fichier même si vous ne vous souvenez pas de son nom exact. Pour rechercher un fichier qui contient deux mots ou plus, utilisez un astérisque (\*). Par exemple, la commande « `locate -i school*note` » permettra de rechercher tout fichier contenant les mots « `school` » et « `note` », qu'ils soient en majuscules ou en minuscules.

## 3.13 Grep command

Une autre commande de base de Linux qui est sans aucun doute utile pour une utilisation quotidienne est `grep`. Elle vous permet de rechercher tout le texte d'un fichier donné.

Par exemple, `grep blue notepad.txt` recherchera le mot `blue` dans le fichier `notepad`. Les lignes qui contiennent le mot recherché s'afficheront entièrement.

## 3.14 Commande sudo

Abréviation de « SuperUser Do », cette commande vous permet d'effectuer des tâches qui nécessitent des autorisations administratives ou de root. Cependant, il n'est pas conseillé d'utiliser cette commande pour un usage quotidien car une erreur pourrait facilement se produire si vous avez fait quelque chose d'incorrect.

## 3.15 Commande tar

La commande `tar` est la commande la plus utilisée pour archiver plusieurs fichiers dans un tarball – un format de fichier Linux commun qui est similaire au format `zip`, avec la compression étant optionnelle.

Cette commande est assez complexe et comporte une longue liste de fonctions telles que l'ajout de nouveaux fichiers dans une archive existante, la liste du contenu d'une archive, l'extraction du contenu d'une archive, et bien d'autres encore. Consultez quelques exemples pratiques pour en savoir plus sur les autres fonctions.



## 3.16 Commande chmod

Chmod est une autre commande Linux, utilisée pour modifier les permissions de lecture, d'écriture et d'exécution des fichiers et des répertoires. Comme cette commande est assez compliquée, vous pouvez lire le tutoriel complet afin de l'exécuter correctement.

## 3.17 Commande chown

Sous Linux, tous les fichiers sont la propriété d'un utilisateur spécifique. La commande chown vous permet de changer ou de transférer la propriété d'un fichier à un utilisateur spécifique. Par exemple, `chown linuxuser2 fichier.ext` fera de linuxuser2 le propriétaire du fichier.ext.

## 3.18 Commande ping

Utilisez la commande ping pour vérifier votre état de connectivité à un serveur. Par exemple, en entrant simplement `ping google.com`, la commande vérifiera si vous êtes en mesure de vous connecter à Google et mesurera également le temps de réponse.

## 3.19 Commande wget

Le terminal Linux est très puissant. Vous pouvez même l'utiliser pour télécharger des fichiers sur Internet à l'aide de la commande wget. Pour ce faire, il suffit de taper wget suivi du lien de téléchargement.

## 3.20 Commande uname

La commande uname, abréviation de Unix Name, imprimera des informations détaillées sur votre système Linux comme le nom de la machine, le système d'exploitation, le noyau, etc.

## 3.21 Commande top

Comme un terminal équivalent au gestionnaire de tâches dans Windows, la commande top affichera une liste des processus qui sont en cours d'exécution et la quantité de CPU utilisée par chaque processus. Il est très utile de surveiller l'utilisation des ressources du système, en particulier de savoir quel processus doit être arrêté en cas de surconsommation de ressources.

## 3.22 Commande history

Lorsque vous utilisez Linux depuis un certain temps, vous remarquerez rapidement que vous pouvez exécuter des centaines de commandes chaque jour. Ainsi, l'exécution de la commande history est particulièrement utile si vous voulez revoir les commandes que vous avez entrées auparavant.





## 3.23 Commande hostname

Si vous voulez connaître le nom de votre hôte/réseau, il vous suffit de taper `hostname`. En ajoutant un `-I` à la fin, vous obtiendrez l'adresse IP de votre réseau.

## 3.24 Commande useradd, userdel

Puisque Linux est un système multi-utilisateurs, cela signifie que plusieurs personnes peuvent interagir avec le même système en même temps. `Useradd` est utilisé pour créer un nouvel utilisateur, tandis que `passwd` est l'ajout d'un mot de passe au compte de cet utilisateur. Pour ajouter une nouvelle personne nommée John, tapez `useradd John` et ensuite pour ajouter son mot de passe, tapez `passwd 123456789`.

La suppression d'un utilisateur est très similaire à l'ajout d'un nouvel utilisateur. Pour supprimer le compte d'un utilisateur, tapez, `userdel NomUtilisateur`

## 3.25 Commande shutdown

Le terminal Linux vous permet de tout faire y compris éteindre ou redémarrer votre machine. Pour cela vous allez utiliser la commande `shutdown`. Ce qui est intéressant avec cette commande c'est que vous pouvez éteindre/redémarrer votre ordinateur immédiatement en utilisant le paramètre « `now` ».

Et vous pouvez aussi programmer l'arrêt de la machine à une heure précise.



## 4 Mise en place de BIND9

Un service DNS (Domain Name Service) sert à la résolution de noms de domaine en une adresse IP ou une autre ressource. Ce service est utile notamment pour naviguer sur internet pour ne pas avoir à connaître les IPs des sites web.

### 4.1 Introduction

La mise en place d'un tel service requiert l'utilisation d'un logiciel spécifique. Le plus utilisé est Bind. Cette technologie, maintenue par Internet Systems Consortium est utilisée sur la grande majorité des services DNS existant dans le monde dont la plupart des serveurs DNS racines.

Durant ce TP, nous allons apprendre à mettre en place et configurer un service DNS avec Bind9. Pour ce faire, nous allons prendre le cas simple de la configuration d'un nom de domaine pour un site web. Nous mettrons en place un nom de domaine qui pointera vers différents services tel qu'un serveur web HTTP. Il n'est pas nécessaire que ces services existent réellement.

Pour ce TP, la VM sera en Nat, son réseau est 192.168.10.0/24 et son adresse IP est le 192.168.10.131. Le nom du serveur srv1.

### 4.2 Installation de BIN9

Après avoir configuré le réseau Ubuntu serveur, nous allons mettre en place le serveur DNS de Linux « BIND 9 ». Tout d'abord nous installons les paquets en tapant la commande :

```
apt install bind9
```

### 4.3 Configuration de la résolution de nom

Nous allons configurer le fichier hosts (nano /etc/hosts) et intégrer l'adresse IP du serveur et le FQDN, le nom de domaine sera form.local

```
192.168.10.131 srv1.form.local srv1
127.0.0.1 srv1.form.local
192.168.10.131 form.local
```

Ensuite nous allons configurer la résolution dans /etc/resolv.conf qui va permettre de traduire le nom de domaine en une adresse IP

```
nameserver 192.168.10.131
options edns0 trust-ad
search form.local
```



Et enfin, nous allons renseigner les informations dans le fichier :

```
nano /etc/netplan/00-installer-config.yaml
```

```
network:
  ethernets:
    ens33:
      addresses:
        - 192.168.10.131/24
      gateway4: 192.168.10.254
      nameservers:
        addresses:
          - 192.168.10.131
          - 8.8.8.8
        search: [form.local]
  version: 2
```

## 4.4 Création d'une zone de recherche direct

Nous allons créer une zone de recherche direct qui permettra de résoudre le nom de l'hôte en adresse IP. Dans le répertoire etc/bind, nous allons copier le fichier db.local et le renommer en db.form.local, ce fichier nous permet de configurer la zone de recherche direct :

```
cp db.local db.lam.local
```

Ensuite nous allons entrer dans le fichier db.form.local (nano db.form.local) et procéder aux configurations suivantes :

```
?
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv1.form.local. root.form.local. (
                                2           ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       srv1.form.local.
srv1      IN      A        192.168.10.131
```



## 4.5 Création d'une zone de recherche inversé

Après avoir créer la zone de recherche direct, nous allons créer une zone de recherche inversé, pour résoudre l'adresses IP 192.168.10.131 en noms d'hôte srv1.form.local. Dans le répertoire etc/bind, nous allons copier le fichier db.127 et le renommer en db.form.local.inv, se fichier nous permet de configurer la zone de recherche inverser :

```
cp db.127 db.form.local.inv
```

Ensuite nous allons entrer dans le fichier db.form.local.inv (nano db.form.local.inv) et procéder aux configurations suivantes :

```
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv1.form.local. root.form.local. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       srv1.
131       IN      PTR      srv1.form.local.
```

131 correspond au dernier octet de l'adresse IP de mon serveur : 192.168.10.**131**

## 4.6 Attribution des zones au serveurs DNS

Ensuite nous allons attribuer les zones que l'on a créé au serveurs DNS, pour cela nous accéder au fichier named.conf.local et procéder aux configurations suivantes :

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "form.local" IN {
    type master;
    file "/etc/bind/db.form.local";
};

zone "10.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.form.local.inv";
};
```



## 4.7 Vérification

Après avoir terminé les configurations, redémarrer le service bind9 via la commande :

```
service bind9 restart
```

Ensuite nous allons procéder à des vérifications afin de vérifier si notre DNS est bien configuré, pour cela, taper les commandes suivantes :

```
named-checkzone form.local db.form.local
named-checkzone form.local db.form.local.inv
ping srv1.form.local
nslookup srv1.form.local
nslookup 192.168.10.131
```

## 5 Mise en place d'un Vhost

### 5.1 Introduction

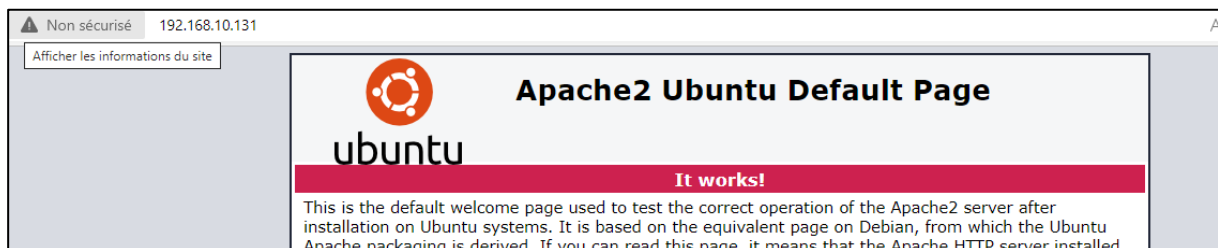
Dans ce prochain TP, nous allons jeter un œil aux hôtes virtuels Apache. Tout d'abord, il faut expliquer qu'un hôte virtuel est une directive de configuration Apache qui nous permettra d'exécuter plusieurs sites Web sur un seul serveur. Le fait qu'ils s'exécutent sur le même serveur physique n'est pas évident pour l'utilisateur final. Avec les hôtes virtuels, nous pourrions spécifier la racine du site (le répertoire qui contient les fichiers du site Web), créer une politique de sécurité distincte pour chaque site, utiliser différents certificats SSL et bien plus encore.

### 5.2 Installation

Pour installer Apache seul, installez simplement le paquet apache2 :

```
apt install apache2
```

À la suite de cette installation notre serveur doit fonctionner et être accessible à l'adresse `http://adresse-IP-du-serveur`. Un message **It Works!** devrait s'afficher dans votre navigateur. Il s'agit du contenu du fichier `/var/www/html/index.html` qui est affiché par défaut.



## 5.3 Création de la structure de répertoire

Nous allons d'abord créer une structure de répertoire qui contiendra les données du site que nous servirons aux visiteurs dans notre répertoire Apache.

```
mkdir /var/www/html/test/
```

Ensuite nous allons copier le fichier index.html dans le répertoire test :

```
cp /var/www/html/index.html /var/www/html/test/
```

## 5.4 Créez un nouveau fichier d'hôtes virtuels

Apache est livré avec un fichier d'hôte virtuel par défaut appelé 000-default.conf, que nous utiliserons comme modèle. Nous allons le copier afin de **créer un fichier d'hôte virtuel** :

```
cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/site1.conf
```

Ouvrez le nouveau fichier dans votre éditeur (nous utilisons nano ci-dessous) :

```
nano /etc/apache2/sites-available/site1.conf
```

Nous adapterons ce fichier pour notre propre domaine.

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies the host name for the virtual host.

    DocumentRoot /var/www/html/test/
    ServerName www.form.local
    ServerAlias form.local
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
```



## 5.5 Activez le nouveau fichier hôte virtuel

Avec nos fichiers d'hôtes virtuels créés, nous devons les activer. Nous utiliserons l'outil a2ensite pour atteindre cet objectif.

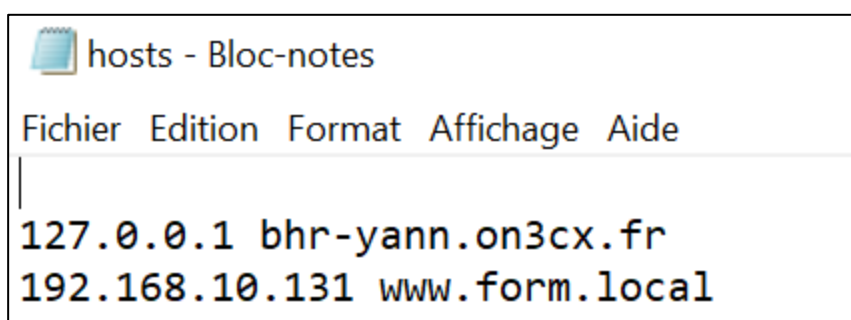
```
a2ensite site1.conf
```

## 5.6 Renseigner le domaine et son adresse IP sur Windows

La dernière étape consiste à modifier le fichier hosts dans notre machine Windows 10, il se trouve dans le répertoire C:\Windows\System32\drivers\etc

Windows (C:) > Windows > System32 > drivers > etc			Rechercher dans : etc
Nom	Modifié le	Type	
hosts	16/09/2022 10:28	Fichier	
lmhosts.sam	15/09/2018 09:31	Fichier SAM	
networks	15/09/2018 09:31	Fichier	
protocol	15/09/2018 09:31	Fichier	
services	15/09/2018 09:31	Fichier	

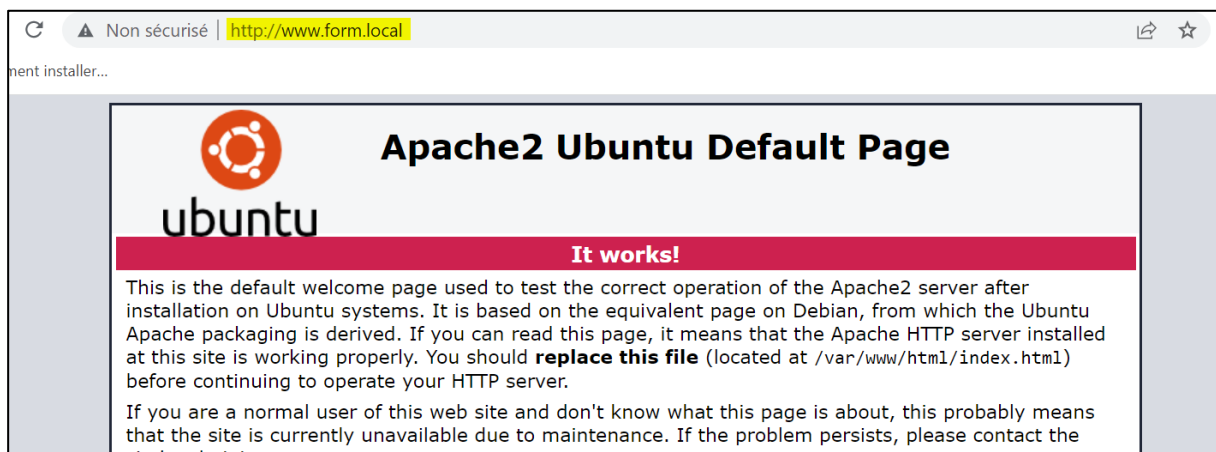
On ajoute l'adresse IP du serveur associé à notre domaine :



## 5.7 Testez nos résultats

Maintenant que notre hôte virtuel est configuré, nous pouvons tester notre configuration en allant sur les domaines que nous avons configurés dans votre navigateur web :

```
http://www.form.local
```



## 6 Mise en place s'un serveur LAMP + WordPress

### 6.1 Introduction

WordPress est une technologie open-source extrêmement populaire pour la création de sites web et de blogs sur l'internet aujourd'hui. Utilisés par 63 % des sites web qui utilisent un système de gestion de contenu (CMS), les sites WordPress représentent 36 % de tous les sites web qui sont actuellement en ligne.

Il existe de nombreuses approches différentes pour accéder à WordPress et certains processus de configuration sont plus complexes que d'autres.

Pour ce TP, nous utiliserons un LAMP (Linux, Apache, MySQL et PHP) stack qui est une option pour une architecture de serveur qui supporte WordPress en fournissant le système d'exploitation Linux, le serveur web Apache, la base de données MySQL et le langage de programmation PHP.





## 6.2 Installation du serveur LAMP

Avant de commencer, nous devons mettre notre système à jour :

```
apt-get update  
apt-get upgrade
```

Installez PHP :

```
apt-get install php-common libapache2-mod-php php-cli
```

Installez le système de base de données MySQL/MariaDB :

```
apt-get install mariadb-server
```

## 6.3 Configuration du serveur MariaDB

Par défaut, le mot de passe administrateur MySQL/MariaDB sera le même que celui de votre utilisateur système. Pour personnaliser la sécurisation de notre base de données, voici la commande à effectuer :

```
mysql_secure_installation
```

- **Change the root password [Y/n] => y** // changez le mot de passe
- **New password** // Entrez votre mot de passe « root »
- **Remove anonymous users [Y/n] => y** // Désactivez ensuite les connexions anonymes
- **Disallow root login remotely? [Y/n] => y** // Désactivez la connexion en « root » depuis une connexion distante
- **Remove test database and access to it? [Y/n] => y** // effacer la base de données de test créée par défaut
- **Reload privilege tables now? [Y/n] => y** // Il reste à charger les nouveaux paramètres

Pour tester l'accès à notre base de données, voici la commande à utiliser dans notre terminal :

```
mysql -u root -p  
show databases  
exit
```



## 6.4 Installez phpMyAdmin

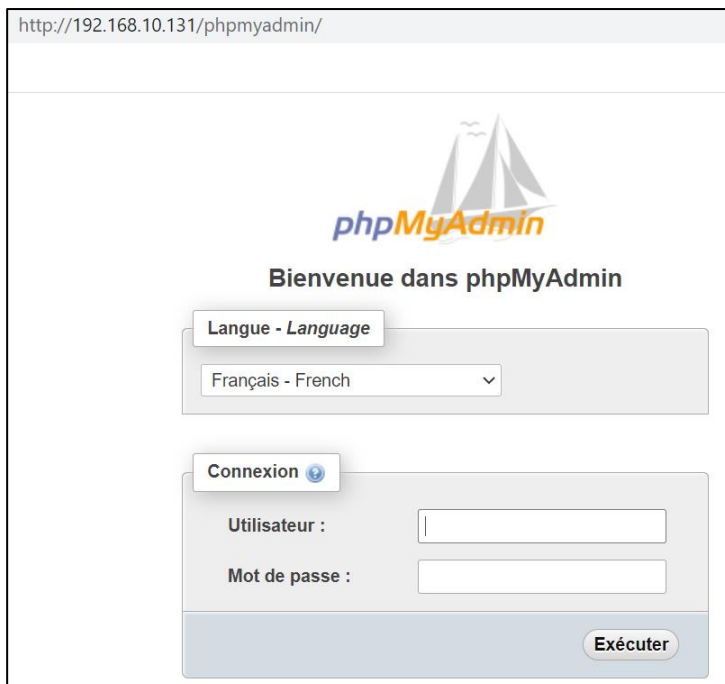
PhpMyAdmin est une application Web de gestion pour les systèmes de gestion de base de données MySQL et MariaDB. Il va nous permettre de gérer notre base de donnée via une interface web. Pour pouvoir installer PhpMyAdmin, utilisez la commande suivant :

```
apt-get install phpmyadmin
```

Afin d'accéder à l'interface de gestion de phpMyAdmin, vous devons finaliser la configuration notre serveur Apache. Pour cela, on édite le fichier de configuration Apache. Afin de nous connecter, nous devons au préalable créer un utilisateur possédant les droits administrateurs pour phpMyAdmin :

```
mysql -u root -p
CREATE USER 'my_user'@'localhost' IDENTIFIED BY 'my_password';
GRANT ALL PRIVILEGES ON * . * TO 'my_user'@'localhost';
FLUSH PRIVILEGES;
Quit
```

Accédez ensuite à l'interface via [http://IP\\_du\\_serveur/phpmyadmin/](http://IP_du_serveur/phpmyadmin/) :

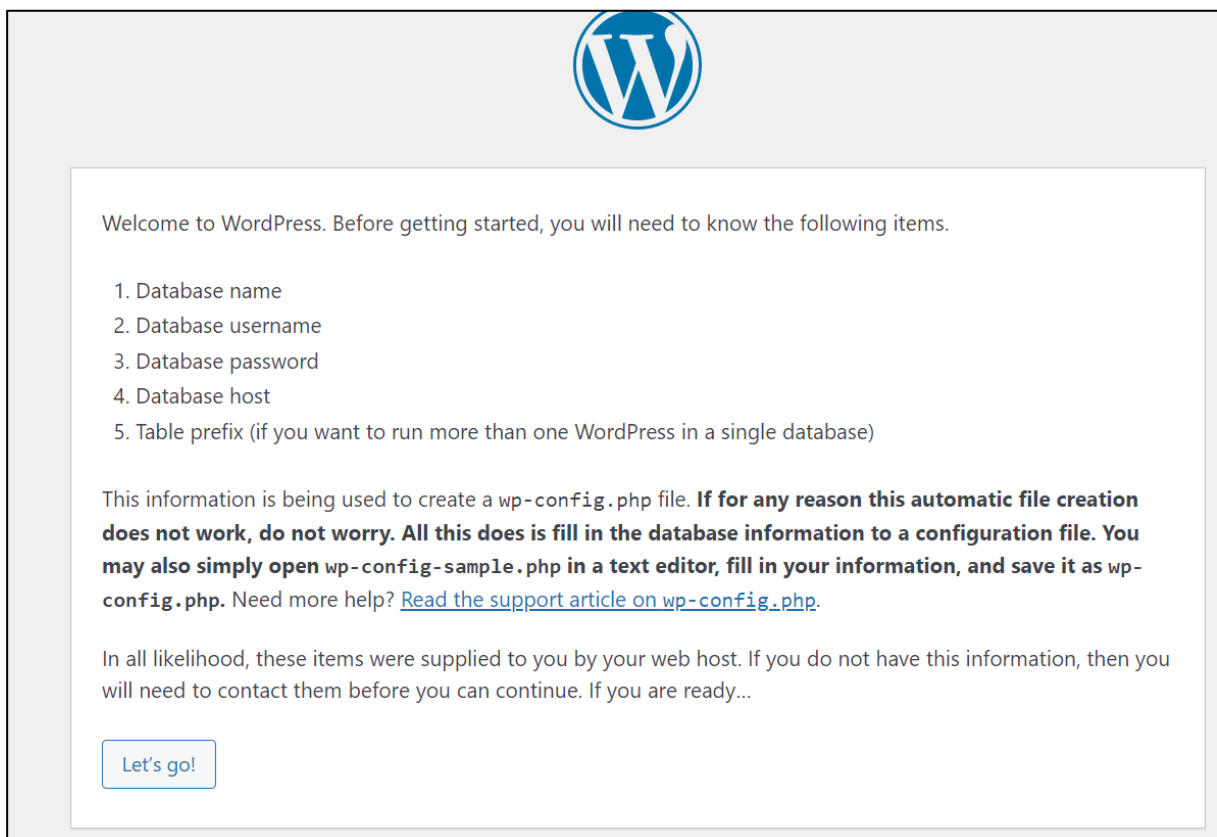


## 6.5 Installez WordPress

Téléchargez, décompressez et copiez le contenu dans un nouveau dossier appelé mywebsite:

```
cd /usr/src
wget https://wordpress.org/latest.tar.gz
tar xpf latest.tar.gz
cp -r wordpress /var/www/html/
```

Ce dossier contenant WordPress est maintenant accessible sur <http://IP-du-serveur/wordpress/>. Maintenant créez une base nommée wordpress en ligne de commande ou via phpMyAdmin. Pour notre cas nous allons la créer via phpMyAdmin.



Dans le menu, sélectionner « nouvelle base de donnée » :




Dans la base de donnée, on donne un nom à notre nouvelle base de donnée (exemple: wordpress) et on sélectionne « créer »



## 6.6 Configuration de WordPress

On retourne sur la page d'accueil de WordPress et on sélectionne « let's go » :




Welcome to WordPress. Before getting started, you will need to know the following items.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

This information is being used to create a `wp-config.php` file. **If for any reason this automatic file creation does not work, do not worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? [Read the support article on wp-config.php.](#)

In all likelihood, these items were supplied to you by your web host. If you do not have this information, then you will need to contact them before you can continue. If you are ready...

Sur l'écran suivant, entrez le nom de votre base de données MySQL wordpress, l'utilisateur, le mot de passe et l'hôte, puis appuyez sur Soumettre.



Below you should enter your database connection details. If you are not sure about these, contact your host.

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="my_user"/>	Your database username.
Password	<input type="text" value="my_password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if <code>localhost</code> does not work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.



WordPress va tester de se connecter à notre base de données et si cela fonctionne, un bouton "Lancer l'installation" va s'afficher. Cliquez dessus.

Unable to write to wp-config.php file.

You can create the wp-config.php file manually and paste the following text into it.

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 */
```

After you've done that, click "Run the installation".

[Run the installation](#)

Si sa vous renvoi a la première page d'installation, il faudra créer le fichier wp-config.php manuellement dans le répertoire wordpress et copier le scripte dans ce fichier :

```
nano /usr/src/wordpress/wp-config.php
```

Ensuite il faudra donner les droits à l'utilisateur « my\_user » :

```
chmod -R 777 /var/www/
```



Il ne reste que quelques champs à renseigner comme le titre du site (modifiable ultérieurement) et la création d'un premier compte utilisateur. Je dirais même d'un compte administrateur, car ce compte sera admin du site. Évitez les identifiants trop évidents comme "admin", "administrateur", "webadmin", "adminwordpress", etc... Prenez quelque chose de plus original et personnel !

Choisissez un mot de passe complexe pour cet utilisateur, indiquez l'adresse e-mail associée et cliquez sur "Installer WordPress". Si vous désirez monter votre site tranquillement sans qu'il soit indexer par Google et consort, cochez la case associée à l'option "Visibilité par les moteurs de recherche".

## Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

### Information needed

Please provide the following information. Do not worry, you can always change these settings later.

Site Title

La Team Rocket

Username

yann

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password

yann

Hide

Very weak

**Important:** You will need this password to log in. Please store it in a secure location.

Confirm Password

☒ Confirm use of weak password

Your Email

azerty@hotmail.com

Double-check your email address before continuing.

Search engine visibility

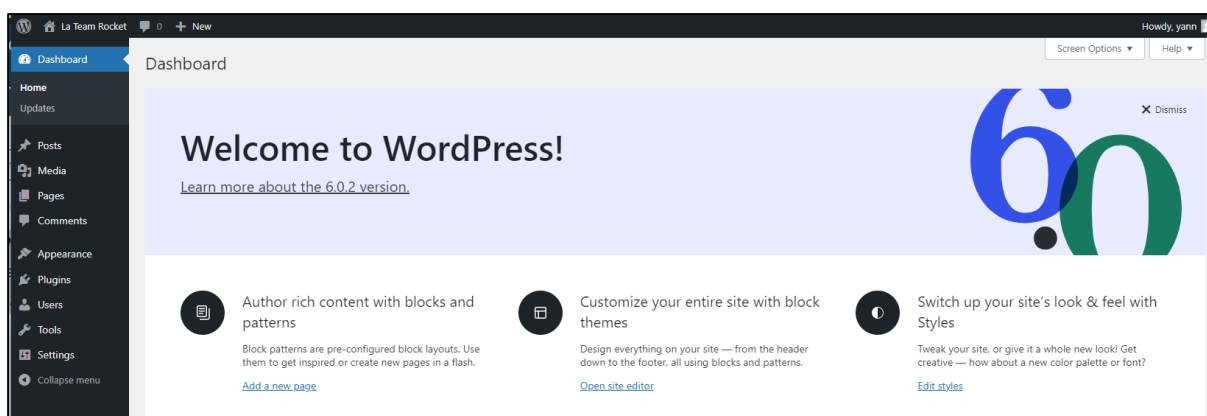
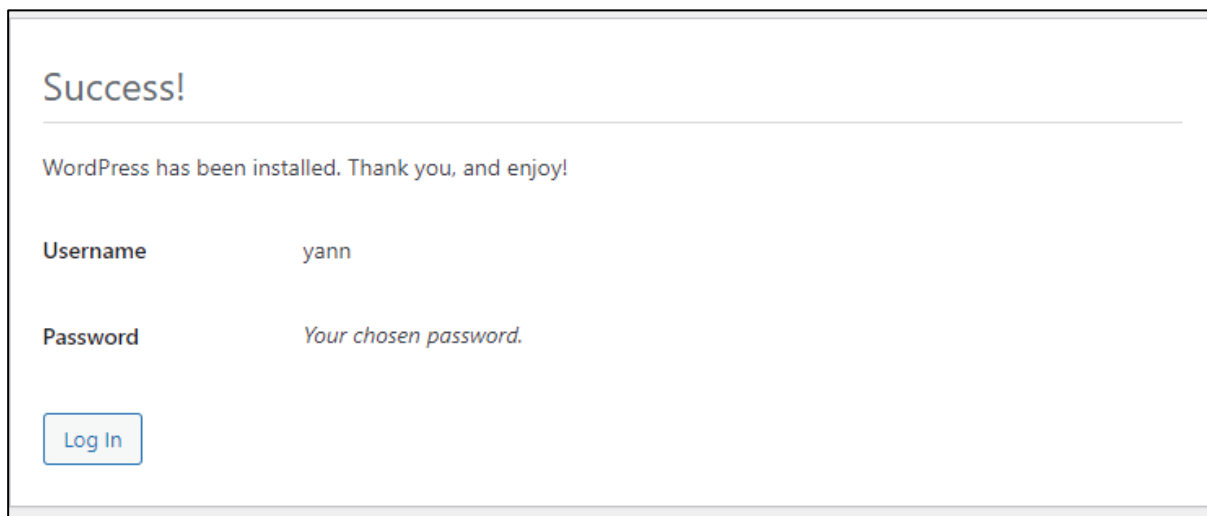
☐ Discourage search engines from indexing this site

It is up to search engines to honor this request.

Install WordPress



WordPress est installé ! Cliquez sur le bouton "Se connecter". Sur la page de connexion qui apparaît, authentifiez-vous avec le compte admin que vous venez de créer, pour ma part "yann".





## 7 Mise en place d'un serveur LDAP

### 7.1 Introduction

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'interrogation et de modification d'un service d'annuaire X.500 exécuté sur TCP/IP. La version actuelle de LDAP est LDAPv3, telle que définie dans RFC4510, et l'implémentation dans Ubuntu est OpenLDAP."

Ainsi, le protocole LDAP accède aux annuaires LDAP. Voici quelques concepts et termes clés :

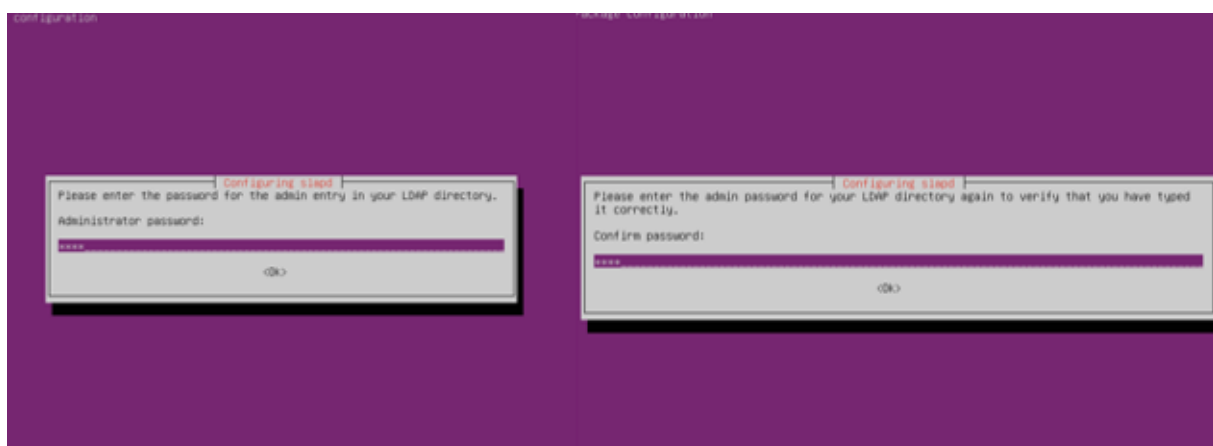
- Un répertoire LDAP est une arborescence d'entrées de données de nature hiérarchique qui est appelée arborescence du répertoire d'information (DIT).
- Une entrée se compose d'un ensemble d'attributs.
- Un attribut possède un type (un nom/description) et une ou plusieurs valeurs.
- Chaque attribut doit être défini dans au moins une classe d'objet.
- Les attributs et classes d'objets sont définis dans les schémas (une classe d'objet est en fait considérée comme un type particulier d'attribut).
- Chaque entrée a un identifiant unique : son Distinguished Name (DN ou dn). Celui-ci, à son tour, consiste en un nom distinctif relatif (RDN) suivi du DN de l'entrée parent.
- Le DN de l'entrée n'est pas un attribut. Il n'est pas considéré comme faisant partie de l'entrée elle-même.

### 7.2 Installation de OpenLDAP

Nous allons installer le serveur LDAP avec OpenLDAP qui permettra de centraliser nos utilisateurs, pour cela :

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

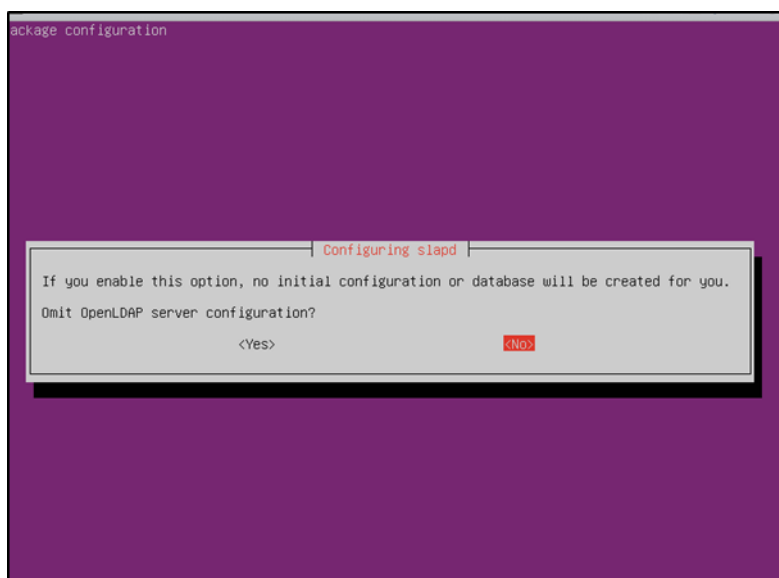
Entrer un mot de passe pour l'administrateur :



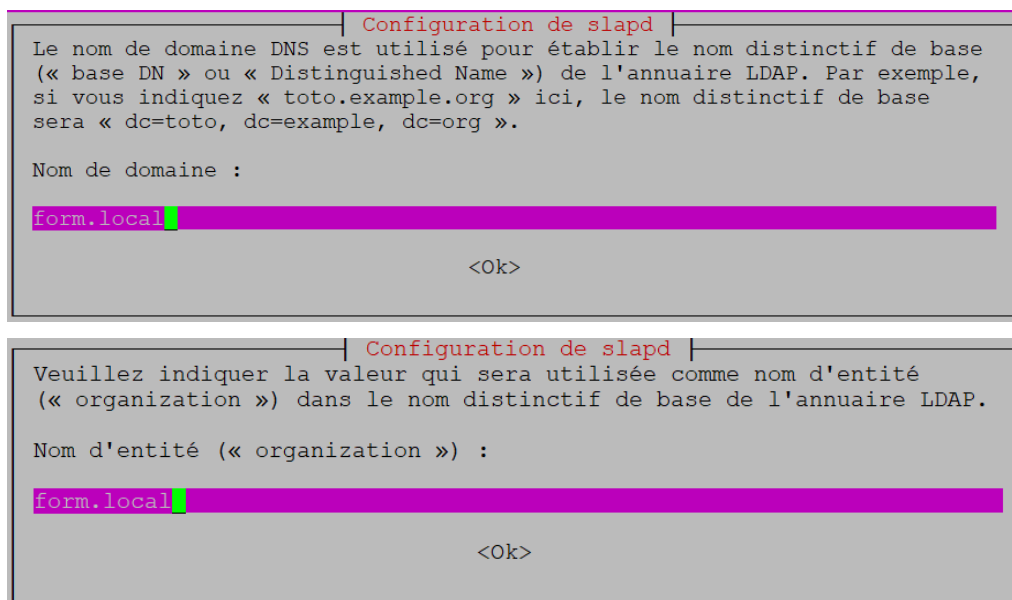
## 7.3 Configuration du serveur OpenLDAP

Ensuite nous allons configurer OpenLDAP :

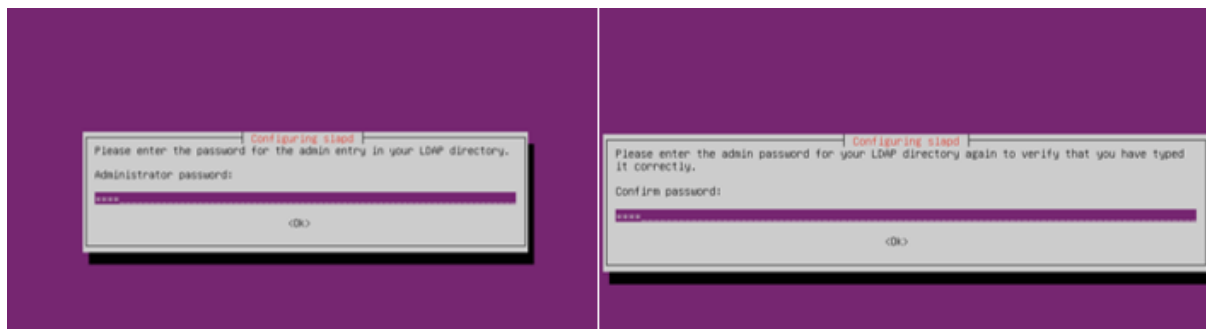
```
sudo dpkg-reconfigure slapd
```



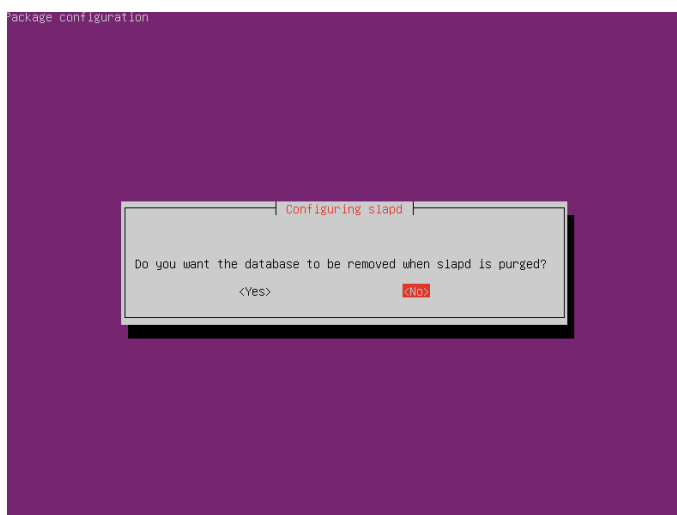
Insérer le domaine :



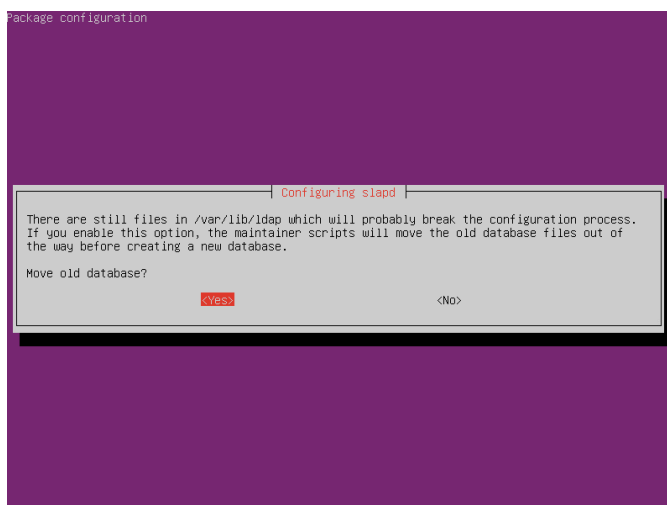
Entrer un mot de passe de l'administrateur :



Ensuite choisissez si votre base de données soit supprimer si vous supprimer OpenLDAP : Non



Choisissez Oui. Les fichiers de données seront déplacés de /var/lib/ldap vers /var/backup.



## 7.4 Installation du LAM

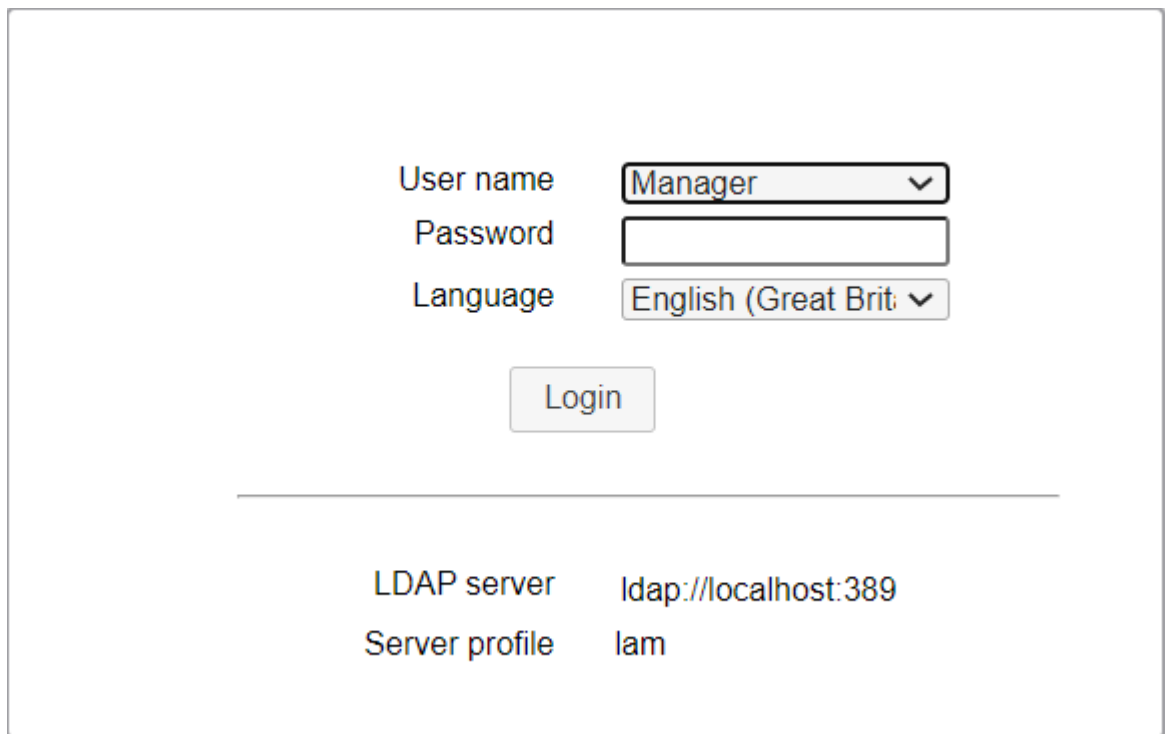
Après avoir installé et configuré OpenLDAP, nous allons pouvoir installer le LAM (Ldap Account Manager).

Le LAM est une interface Web permettant de gérer les entrées (par exemple, les utilisateurs, les groupes) stockées dans l'annuaire OpenLDAP. LAM a été conçu pour rendre la gestion LDAP aussi simple que possible pour l'utilisateur. Pour cela nous allons télécharger les paquets LAM via la commande :

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

Après avoir installé LAM, aller sur le navigateur web et taper :

```
Adresse-IP-du-serveur/lam
```



The screenshot shows the LAM web interface. It features a login form with the following elements:

- User name:** A dropdown menu with "Manager" selected.
- Password:** A text input field.
- Language:** A dropdown menu with "English (Great Brit" selected.
- Login:** A button below the form fields.

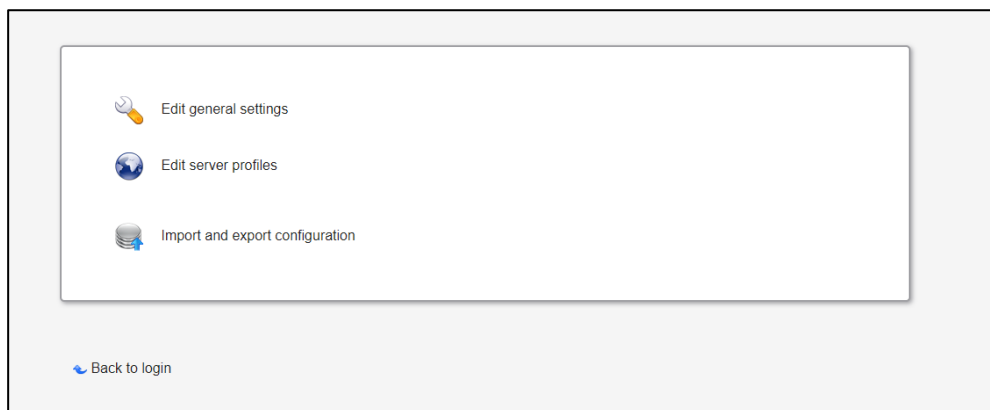
Below the login form, there is a horizontal line and the following configuration information:

- LDAP server:** ldap://localhost:389
- Server profile:** lam

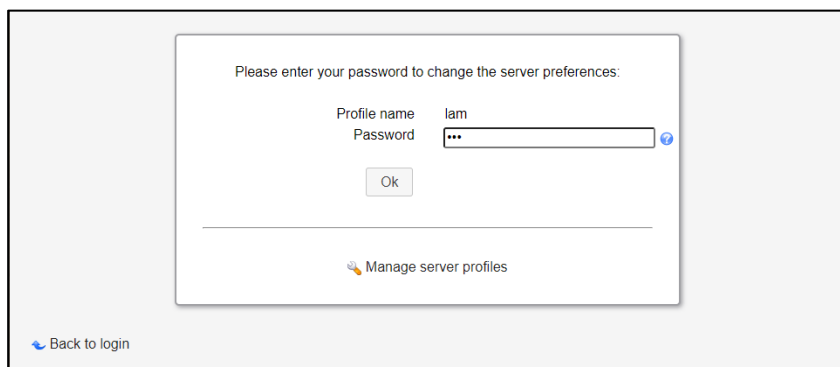


## 7.5 Configuration du Lam

Avant de pouvoir créer et gérer nos utilisateurs, Nous devons définir notre profil de serveur LDAP en cliquant sur [LAM configuration] dans le coin supérieur droit. Ensuite, sélectionner « Edit server profiles » :



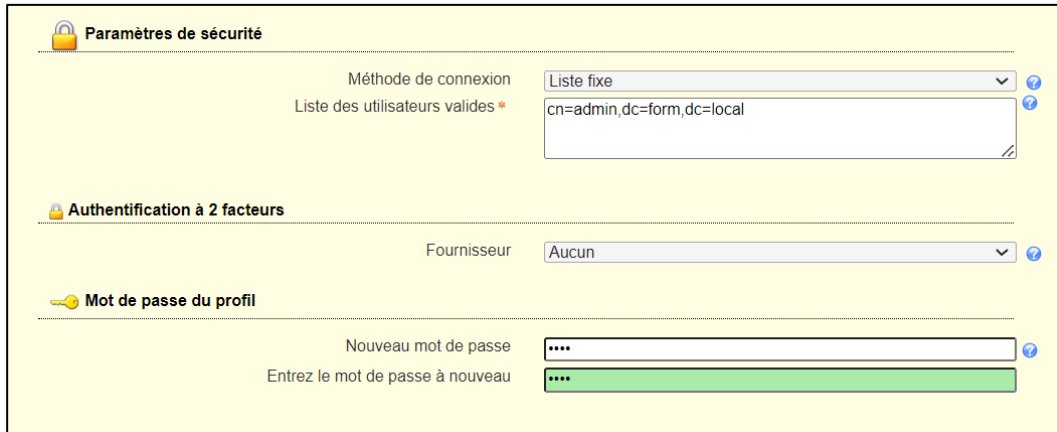
Cela nous demandera le nom du profil LAM Mot de passe : lam (mot de passe par défaut)



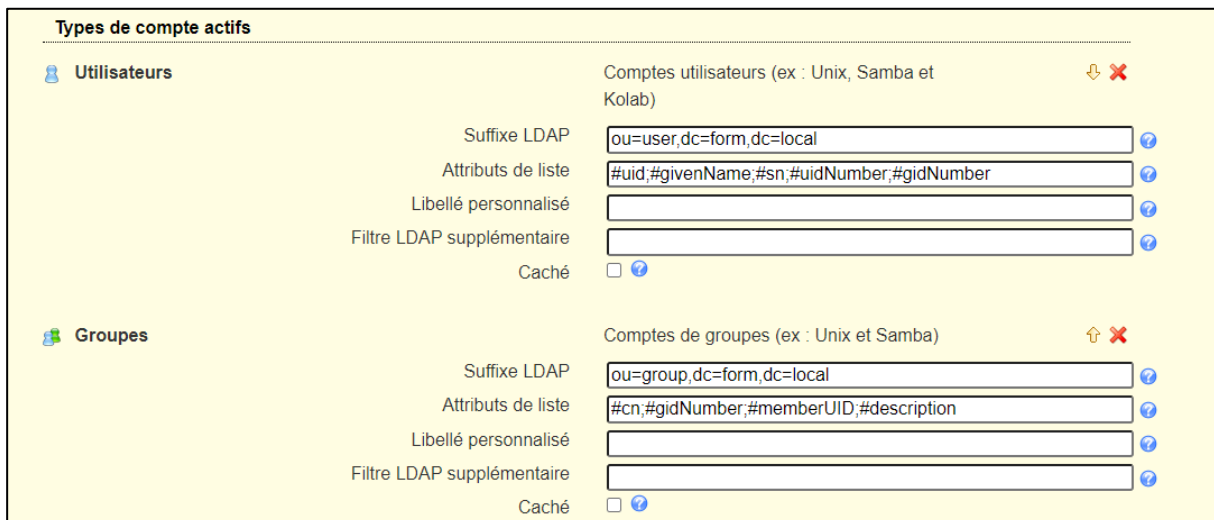
Il faudra définir l'adresse IP du serveur LDAP et le Tree suffix. Le mien ressemble à ci-dessous, vous devez utiliser les composants de votre domaine tels qu'ils sont définis dans le nom d'hôte du serveur. Et à la fin, définissez la langue.

A screenshot of a configuration form titled 'Paramètres du serveur'. It contains several fields: 'Adresse du serveur' (ldap://192.168.10.131:389), 'Activer TLS' (non), 'Suffixe arborescence' (dc=form,dc=local), and 'Nombre maximum de résultats retournés par la recherche LDAP' (-). Each field has a help icon (question mark in a circle). At the bottom, there is a section for 'Options avancées'.

Changer le « Profile Password », c'est à la fin de la page Paramètres généraux, il va nous permettre de nous connecter au LAM en tant qu'administrateur. Ensuite il faudra définir la connexion au tableau de bord en spécifiant le compte d'utilisateur administrateur « admin » et les composants du domaine dans la section « List of valid users » : cn=admin,dc=form,dc=local



Nous allons à la page « Types de compte » et nous allons définir le suffixe LDAP et les attributs de liste des types de compte actifs. Lorsque que nous avons terminé avec les paramètres, cliquez sur le bouton « Enregistrer » en bas de la page.



Maintenant nous allons connecter au compte admin au tableau de bord LAM pour commencer à gérer les comptes d'utilisateurs et les groupes.

Nom d'utilisateur

admin

Mot de passe

....

Langue

Français (France)

Connexion

---

Serveur LDAP

ldap://192.168.10.131:389

Profil du serveur

lam

Les suffixes suivants sont absent du LDAP. LAM peut les créer pour vous.  
Vous pouvez définir les suffixes LDAP pour tous vos types de comptes dans le profil de votre serveur LAM, à l'onglet "Types de comptes".

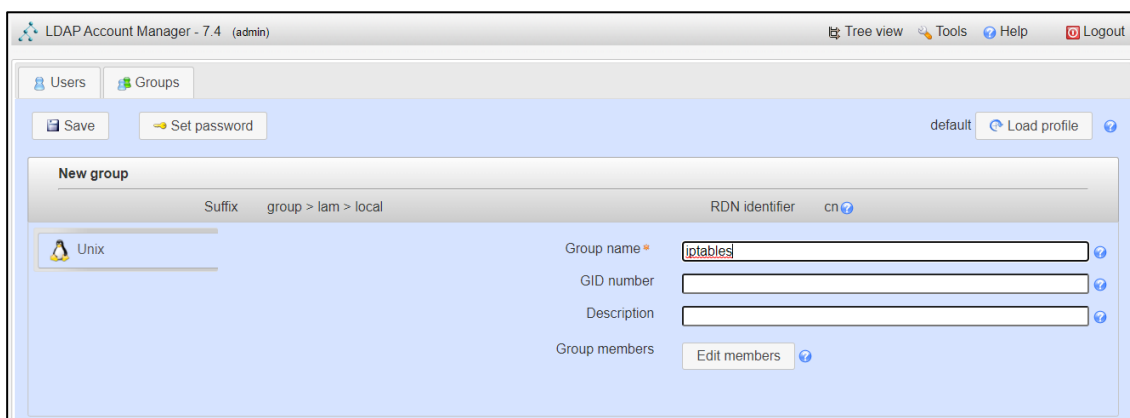
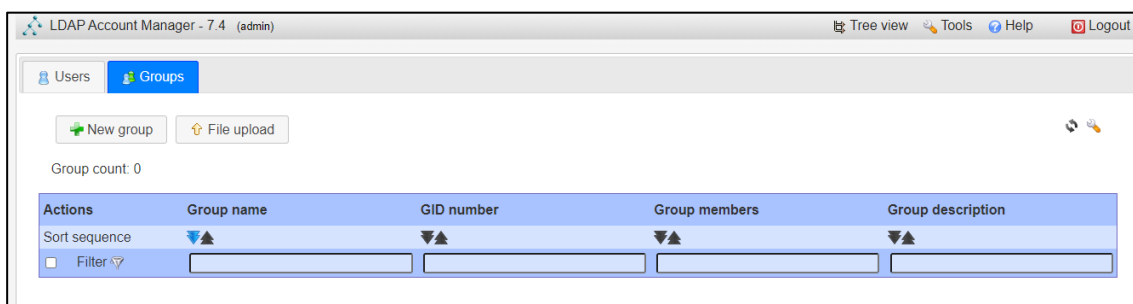
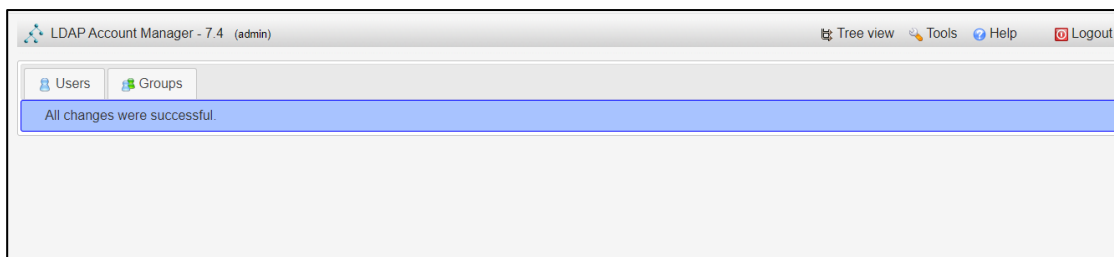
ou=user,dc=form,dc=local  
ou=group,dc=form,dc=local

Créer Annuler



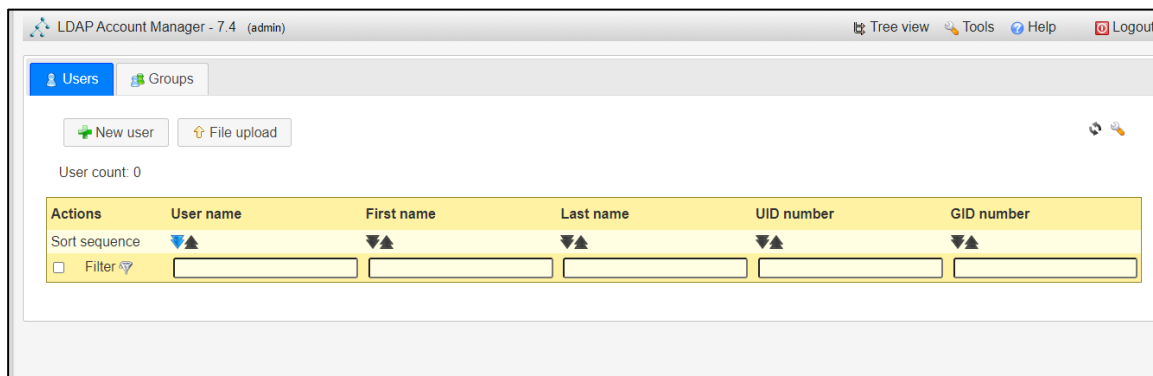
## 7.6 Ajouter des comptes d'utilisateurs et des groupes avec LDAP Account Manager

Avant de créer un utilisateur, nous devons obligatoirement créer un groupe d'utilisateurs. Pour cela cliquez sur Groups > New group. Donnez au groupe un nom, un ID de groupe facultatif et une description. Faites de même pour ajouter d'autres groupes.

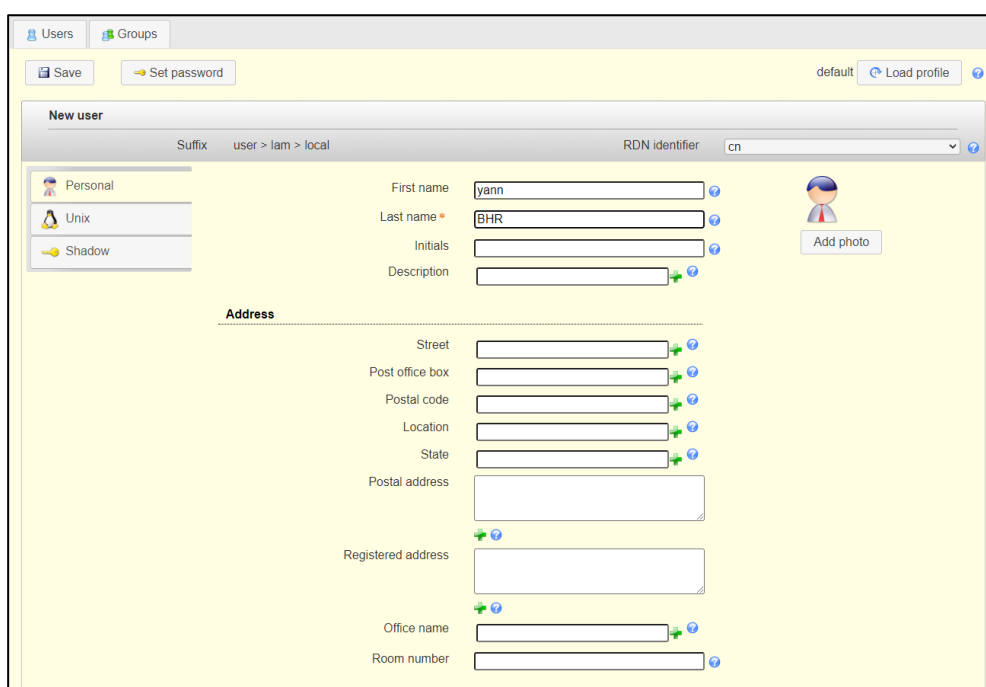




Une fois que les groupes pour les comptes d'utilisateurs sont créés, cliquez sur **Users > New user** pour ajouter un nouveau compte d'utilisateur à notre serveur LDAP. Nous disposons de trois sections pour la gestion des utilisateurs :



**Personal :** Ceci contient les informations personnelles de l'utilisateur telles que le prénom, le nom, le courriel, le téléphone, le service, l'adresse, etc. Pour notre cas nous allons entrer seulement le Nom et le prénom de l'utilisateur.



## 8 Mise en place de Samba4

### 8.1 Introduction

Samba-AD est un logiciel libre sous licence GPLv3 qui reproduit le comportement de Microsoft Active Directory. Samba Active Directory embarque les mêmes fonctionnalités que Microsoft Active Directory. Vous profitez donc des outils RSAT comme les GPO, les outils de contrôle DHCP et DNS, etc. Samba Active Directory est un service dont l'utilisation est gratuite. Vous n'aurez pas besoin de payer de droit d'utilisation comme avec les CAL de Microsoft

Samba-AD permet de créer et de gérer un domaine Active Directory :

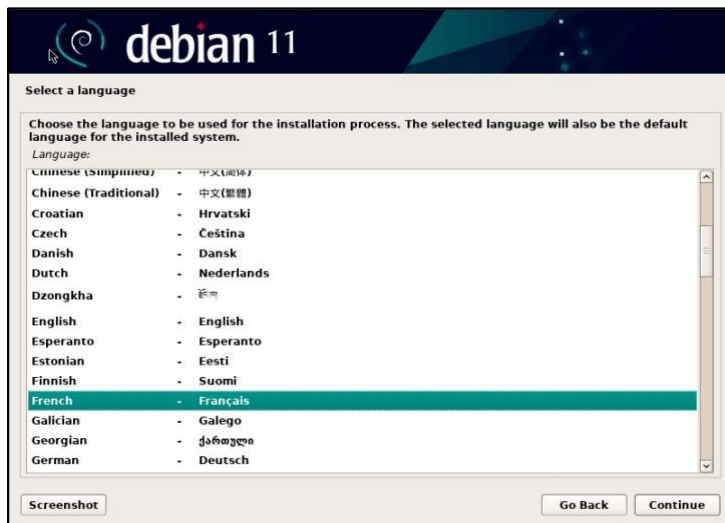
- Annuaire LDAP
- Service de noms DNS
- Service de gestion de temps NTP
- Service d'authentification transparente Kerberos
- Service de distribution de jetons d'authentification KDC
- Réplication multi AD
- Stratégies de sécurité GPO

### 8.2 Mise en place de Debian

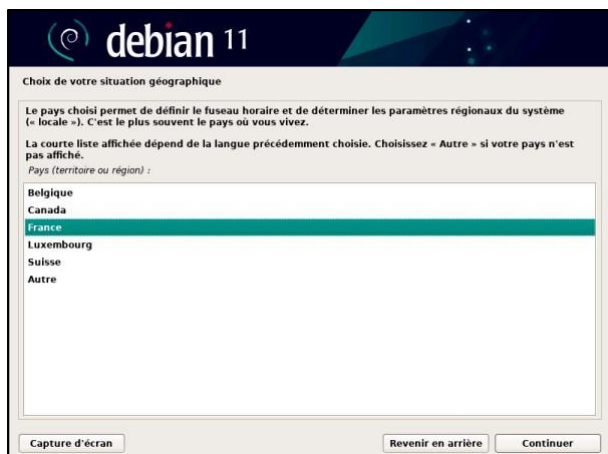
Pour ce TP, nous allons utiliser Debian 11. En ce qui concerne notre carte réseau, elle sera en Nat, l'adresse réseau sera 192.168.8.0/24 et le nom du serveur sera tux.local. Lors du démarrage de la machine virtuelle, sélectionnez la méthode d'installation, pour notre cas, on choisit Graphical install.



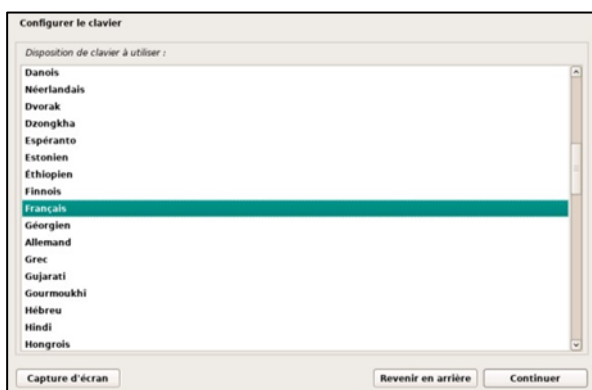
Sélectionner la langue : French



Sélectionner le fuseau horaire : France



Pour la disposition du clavier, sélectionner Français



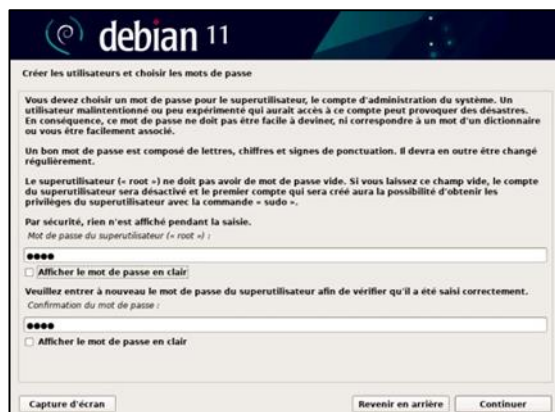
Indiquez un nom pour votre machine (srv1).



Pour le domaine, nous allons choisir tux.local



Entrez le mot de passe du Super utilisateur (« root »).



Créez le premier utilisateur du système en entrant son nom complet, son identifiant puis son mot de passe.



debian 11

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (= root -), pour l'utilisation courante du système.

**Veillez indiquer le nom complet du nouvel utilisateur.** Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

yann

Capture d'écran Revenir en arrière Continuer



debian 11

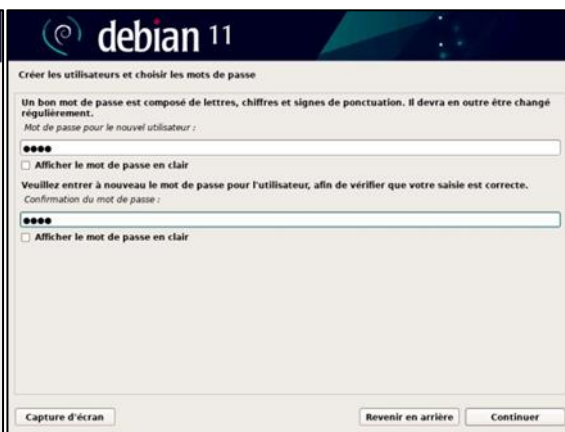
Créer les utilisateurs et choisir les mots de passe

**Veillez choisir un identifiant (= login -) pour le nouveau compte.** Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :

yann

Capture d'écran Revenir en arrière Continuer



debian 11

Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

••••

☐ Afficher le mot de passe en clair

**Veillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.**

Confirmation du mot de passe :

••••

☐ Afficher le mot de passe en clair

Capture d'écran Revenir en arrière Continuer



Pour le partitionnement du disque système, Choisissez « Assisté – utiliser un disque entier » et ensuite sélectionnez le disque où Debian sera installé.



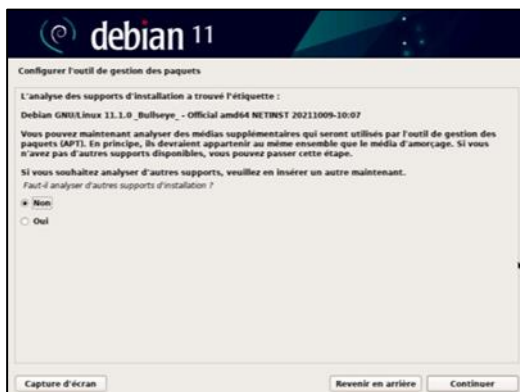
Nous définissons la manière dont les partitions seront gérées.



Enfin, sélectionnez Terminer le partitionnement et appliquer les changements, cliquez sur Continuer puis sur Oui.



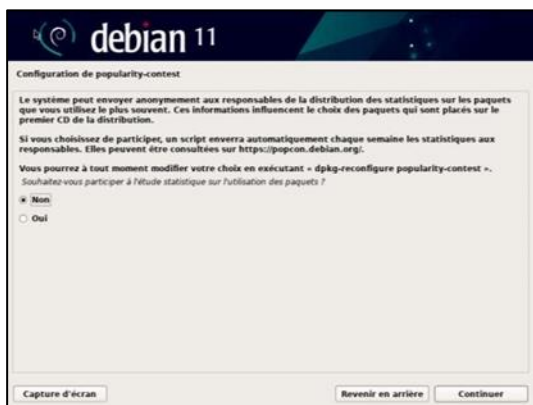
Choisissez de ne pas analyser un autre CD/DVD comme source pour les paquets.



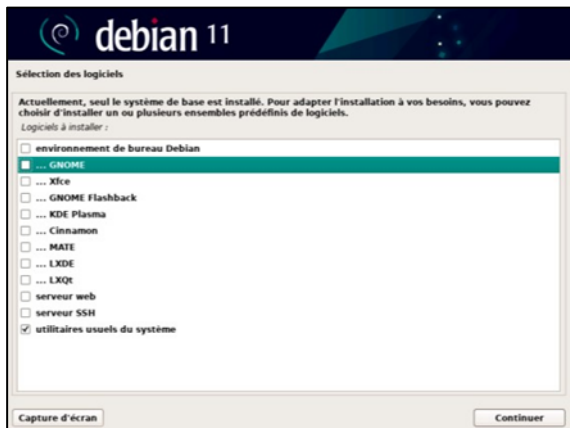
Configuration du gestionnaire de paquets : sélectionnez France, un miroir situé en France puis laissez le mandataire HTTP vide.



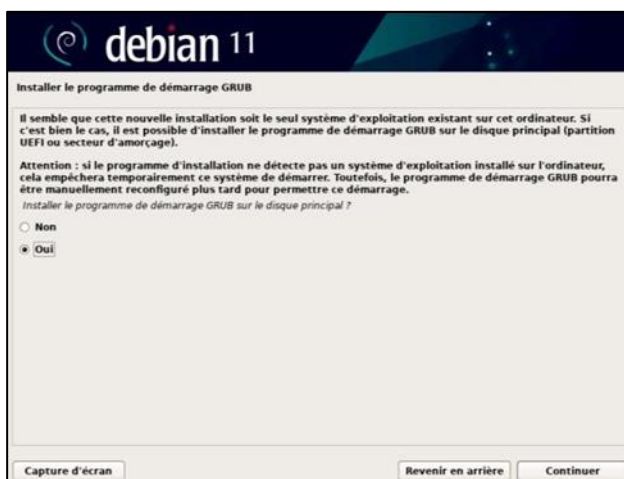
Choisissez si vous souhaitez ou non participer à l'étude statistique sur l'utilisation des paquets.



Sélectionnez uniquement les utilitaires usuels du système.



Dans l'écran suivant, choisissez « Oui » pour installer le chargeur de démarrage Grub sur le disque dur principal.



Dans la fenêtre suivante, choisissez le disque sur lequel le chargeur grub sera installé,





Une fois l'installation terminée, le programme d'installation vous demandera de redémarrer le système une fois.



Entrez l'identifiant et le mot de passe de Super utilisateur.

```
Debian GNU/Linux 11 srv1 tty1

srv1 login: root
Password:
Linux srv1 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) 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.
root@srv1:~# _
```

## 8.3 Configuration réseau de Debian

Après avoir terminé l'installation de votre serveur Debian, la première chose est de mettre à jour les paquets :

```
Apt update
Apt upgrade
```



Ensuite nous allons mettre notre adresse IP en statique mais avant nous devons connaître quel adresse IP à été fournis par le DHCP, pour cela nous devons utiliser la commande « **ifconfig** » :

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.8.70 netmask 255.255.255.0 broadcast 192.168.8.255
    inet6 fe80::20c:29ff:fe30:ae2d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:30:ae:2d txqueuelen 1000 (Ethernet)
    RX packets 40 bytes 4699 (4.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 4681 (4.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Maintenant que nous connaissons notre adresse IP et le nom de notre interface (ens33), nous allons le mettre en statique, pour cela nous allons éditer le fichier « interfaces » qui se situe dans le répertoire « network » :

```
nano /etc/network/interfaces.
```

Nous allons procéder aux configurations suivantes :

- Allow-hotplug
- Iface ens33 inet static (adresse IP en mode statique)
- Address : 192.168.8.70 (adresse ip du serveur)
- Netmask : 255.255.255.0 (masque de sous réseau en /24)
- Gateway : 192.168.8.254 (passerelle par défaut)
- Dns-domain : tux.local (le nom de domaine)
- Dns-nameservers : 192.168.8.70,8.8.8.8,127.0.0.1

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
address 192.168.8.70
netmask 255.255.255.0
gateway 192.168.8.254
dns-domain tux.local
dns-nameservers 192.168.8.70,8.8.8.8,127.0.0.1
```

Ensuite, afin que le système puisse prendre en compte nos modifications, nous allons redémarrer le réseau, activer la carte réseau (ens33) et au cas où, redémarrer notre serveur :

```
Systemctl restart networking.service
Ifup ens33
Reboot now
```



Après avoir redémarrer le serveur, nous allons éditer le fichier hosts pour la résolution de nom :

```
nano /etc/hosts
```

Vous ne devez pas mettre la boucle locale 127.0.0.1 devant le vrai hostname du serveur, respectez bien l'exemple.

```
127.0.0.1    localhost
192.168.8.70  srv1.tux.local  srv1

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Maintenant la dernière étape consistera à renseigner la zone de recherche DNS, pour cela éditez le fichier :

```
nano /etc/resolv.conf
```

```
GNU nano 5.4
domain tux.local
search tux.local
nameserver 192.168.8.70
nameserver 127.0.0.1
nameserver 8.8.8.8
```



## 8.4 Installation de Samba 4

Avant toute chose, la mise à jour du système :

```
apt-get update
apt-get upgrade
```

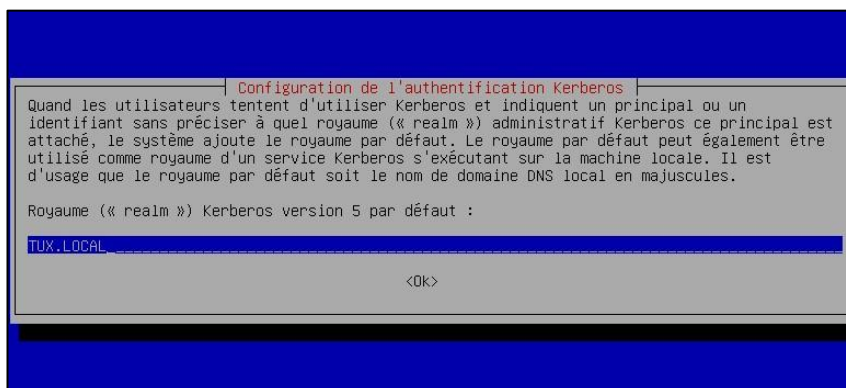
Pour installer Samba 4, il nous faudra les paquets suivants :

- **Samba** : Samba est une mise en œuvre du protocole SMB/CIFS pour les systèmes Unix, fournissant une interopérabilité de partage de fichiers et d'imprimantes entre Microsoft Windows, OS X et les systèmes basés sur UNIX. Samba offre la possibilité de fonctionner comme un contrôleur de domaine du genre NT4, et permet d'intégrer à la fois les domaines NT4 et les services « Active Directory » en tant que serveur membre.
- **Winbind** : winbind est un composant de la suite de programmes Samba qui résout le problème de connexion unifiée. Winbind utilise une implémentation UNIX des appels Microsoft RPC, des modules d'authentification enfichables (PAM) et du commutateur de service de noms (NSS) pour permettre aux utilisateurs de domaine Windows NT d'apparaître et de fonctionner en tant qu'utilisateurs UNIX sur une machine UNIX.
- **Krb5-config** : Protocole de sécurité pour authentifier les utilisateurs, les ordinateurs et les services de manière centralisée sur un réseau, en vérifiant leurs informations d'identification par rapport aux entrées existantes dans la base de données Kerberos.
- **smbclient**
- **krb5-user**
- **Dnsutils**

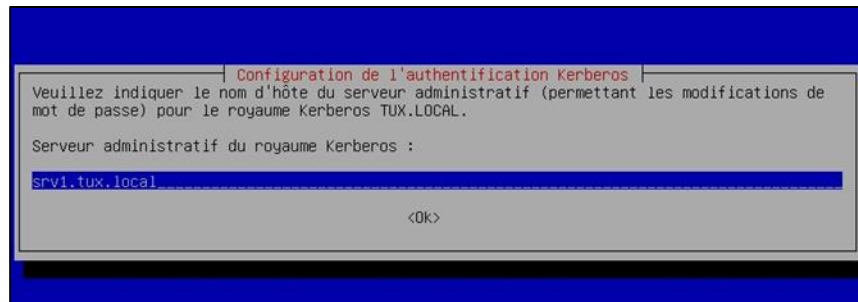
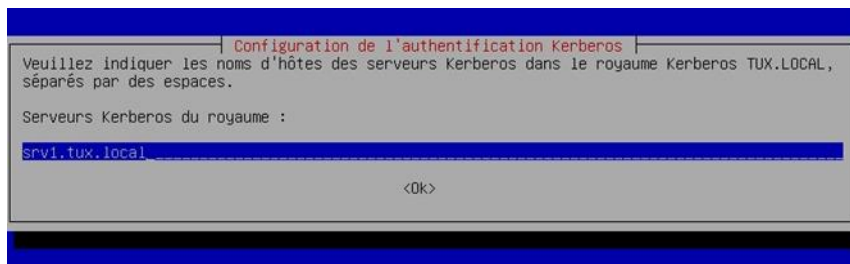
Smbclient krb5-user dnsutils seront utilisé pour les tests. Pour installer les paquets, utiliser la commande suivante :

```
apt-get install samba winbind krb5-config smbclient krb5-user dnsutils
```

Lors de l'installations des paquets, il nous demandera de configurer l'authentification Kerberos. On saisit le nom du « royaume », pour nous ça sera notre nom de domaine : TUX.LOCAL en MAJUSCULE.



Ensuite on doit spécifier le FQDN, pour notre cas, ça sera srv1.tux.local en minuscule



## 8.5 Promotion en contrôleur de domaine

On va maintenant exécuter la commande qui va promouvoir notre serveur en contrôleur de domaine. On va d'abord supprimer le smb.conf originale :

```
rm /etc/samba/smb.conf
```

Puis on lance la commande de promotion :

```
samba-tool domain provision --use-rfc2307 --interactive
```

Lorsque l'on lancera cette commande, on nous demandera de renseigner :

- Realm : TUX.LOCAL
- DOMAIN : TUX
- Serveur : On n'ajoute rien
- Dns backend : On n'ajoute rien
- Dns Forwarder : Adresse IP du serveur (8.8.8.8)
- Choisissez un mot de passe pour le compte administrateur (le mot de passe doit contenir au minimum) :
  - 1 majuscule, 1 minuscule, 7 caractère, 1 caractère spécial

Petite information, si ces informations sont déjà renseignées entre crochet [...], taper Entrer.



## 8.6 Configurer le fichier krb5.conf

Une fois l'opération terminée, on va remplacer le fichier `krb5.conf` d'origine par celui généré par `samba-tool`. D'abord, on supprime l'ancien :

```
rm /etc/krb5.conf
```

Puis on copie celui généré par `samba-tool`. Son emplacement est affiché dans le résultat de la commande de promotion. Dans mon cas il se trouve ici :

```
cp /var/lib/samba/private/krb5.conf /etc/
```

Ensuite nous allons éditer le fichier `krb5.conf` via la commande `nano /etc/krb5.conf` et procéder aux modifications suivantes et enregistrez le fichier. :

```
[libdefaults]
    default_realm = TUX.LOCAL
    dns_lookup_realm = true
    dns_lookup_kdc = true
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true

[realms]
TUX.LOCAL = {
    kdc = srv1.tux.local
    admin_server = srv1.tux.local
    default_domain = tux.local
    database_module = ldapconf
}

[domain_realm]
    .tux.local = TUX.LOCAL
    tux.local = TUX.LOCAL
```



Après avoir modifier et enregistre le fichier krb5.conf, il est important de faire un reboot de la machine, sinon samba ne pourra pas prendre compte les modifications et il ne pourra pas démarrer correctement :

```
reboot now
```

## 8.7 Gérer le service samba

Sachez que vous pouvez démarrer manuellement les services Samba AD en tapant simplement :

```
samba
```

Pour automatiser le démarrage des services au démarrage du système :

```
systemctl unmask samba-ad-dc
```

Pour démarrer le service, taper :

```
systemctl enable samba-ad-dc  
systemctl start samba-ad-dc
```

Et pour vérifier que samba fonctionne, taper :

```
systemctl status samba-ad-dc
```

```
Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2021-12-17 17:08:12 CET; 5s ago
  Docs: man:samba(8)
        man:samba(7)
        man:smb.conf(5)
Main PID: 577 (samba)
Status: "samba: ready to serve connections..."
Tasks: 60 (limit: 2303)
Memory: 203.4M
CPU: 2.775s
CGroup: /system.slice/samba-ad-dc.service
├─577 samba: root process
├─578 samba: tfork waiter process(579)
├─579 samba: task[s3fs] pre-fork master
├─580 samba: tfork waiter process(581)
├─581 samba: task[rpc] pre-fork master
├─582 samba: tfork waiter process(583)
├─583 samba: task[nbt] pre-fork master
└─584 samba: tfork waiter process(585)
```



## 8.8 Test du serveur DNS

Après redémarrage du serveur, tous les services doivent être lancés automatiquement. Maintenant, on va tester le bon fonctionnement du serveur DNS interne de Samba. Pour cela on va traduire un enregistrement de type SRV via la commande :

```
host -t SRV _ldap._tcp.tux.local
```

Cette commande doit afficher :

```
_ldap._tcp.infotrucs.lan has SRV record 0 100 389 srv1.tux.local.
```

Testons un enregistrement de type A :

```
host -t A srv1.tux.local
```

Cette commande doit afficher :

```
Srv1.tux.local has address 192.168.8.70
```

## 8.9 Création de la zone de recherche inversée et de l'enregistrement PTR

Le DNS ne dispose pas encore de zone inversé (comme sous Windows), il faut donc la créer. J'utilise alors cette commande (il faut rentrer le nom du Serveur ainsi que les 3 premiers octets de votre réseau dans le sens inverse) :

```
samba-tool dns zonecreate 192.168.8.70 8.168.192.in-addr.arpa -U administrator
```

Ensuite on ajout un enregistrement PTR à la zone inversée 192.168.8.0/24 (70 est le dernier octet de notre adresse IP 192.168.8.**70**) :

```
samba-tool dns add srv1.tux.local 8.168.192.in-addr.arpa 70 PTR srv1.tux.local -U administrator
```





## 8.10 Test de notre zone inversée et de l'enregistrement PTR

Et maintenant place aux tests !! afin de vérifier que notre serveur Dns est bien configuré, tapé :

```
nslookup 192.168.8.70
nslookup tux.local
```

Cela doit afficher :

```
root@srv1:~# nslookup 192.168.8.70
70.8.168.192.in-addr.arpa      name = srv1.tux.local.

root@srv1:~#
root@srv1:~# nslookup tux.local
Server:      192.168.8.70
Address:     192.168.8.70#53

Name:   tux.local
Address: 192.168.8.70

root@srv1:~#
```

## 8.11 Test d'authentification Kerberos

Juste un petit test de plus pour être sûr que l'authentification Kerberos fonctionne. Entrez la commande suivante et le mot de passe du compte administrateur devrait être demandé :

```
kinit administrator
```

Devrait alors afficher :

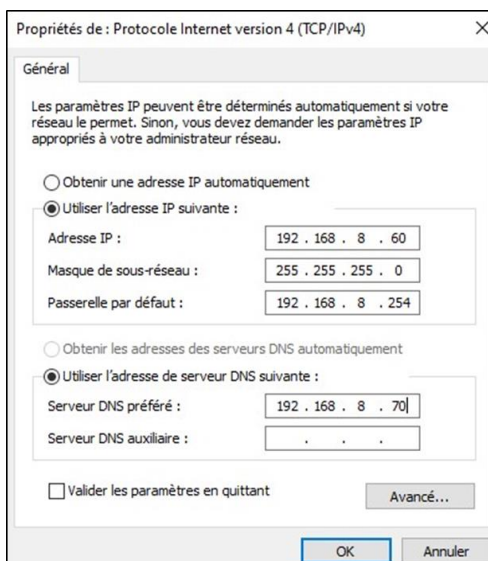
```
root@srv1:~# kinit administrator
Password for administrator@TUX.LOCAL:
Warning: Your password will expire in 41 days on ven. 28 janv. 2022 17:01:11
root@srv1:~# _
```

L'authentification fonctionne.

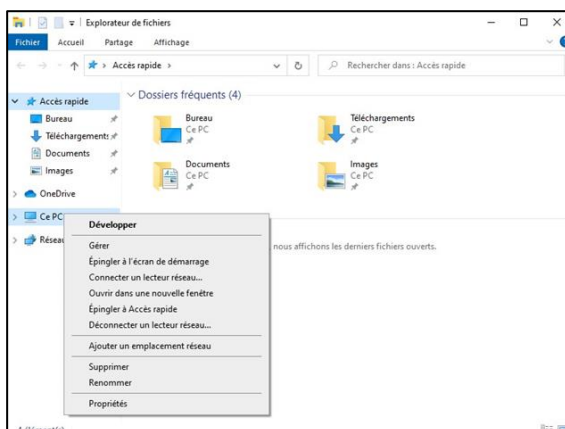


## 8.12 Relier un poste de travail Windows 10 à notre domaine tux.local

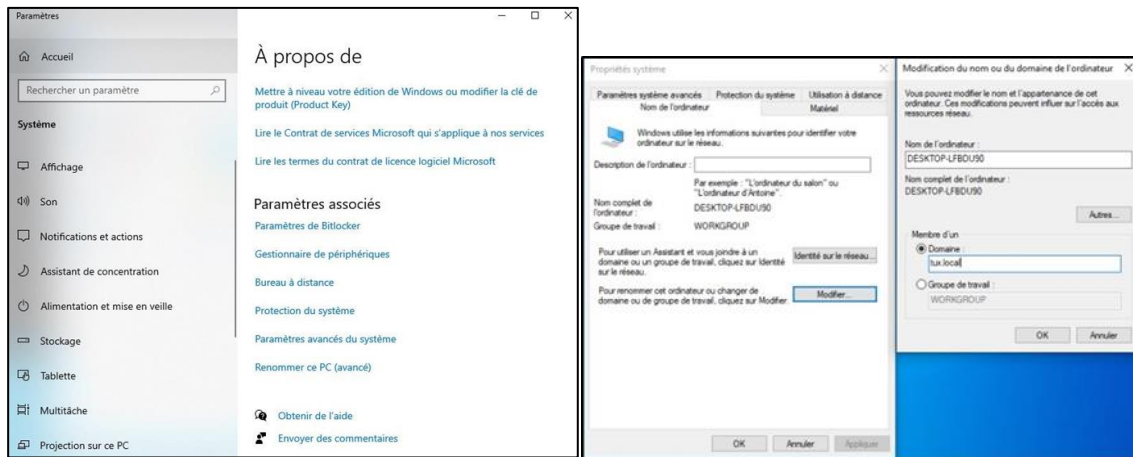
On va maintenant passer sur notre client Windows 10 afin de configurer son réseau. Si vous avez tout bien lu, je vous invite à installer un Windows 10 Pro. Pour le réseau du Windows 10, allons le mettre en Nat (Vmnet8) afin qu'il soit dans le même sous réseau que notre serveur Debian (192.168.8.0/24). Je ne détaille pas cette étape simple. Voici les paramètres que j'ai rentré :



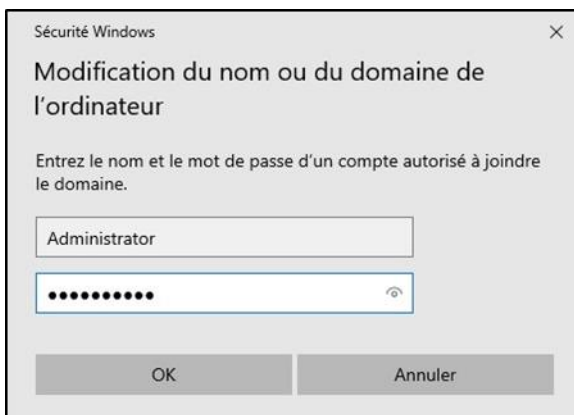
On intègre maintenant le Windows 10 dans le domaine tux.local. Je suppose que vous connaissez déjà la procédure mais je détaille au cas où. Sous Windows 10, on se rend dans le répertoire de fichier, on fait clique droite sur « Ce PC » et on sélectionne « Propriété ».



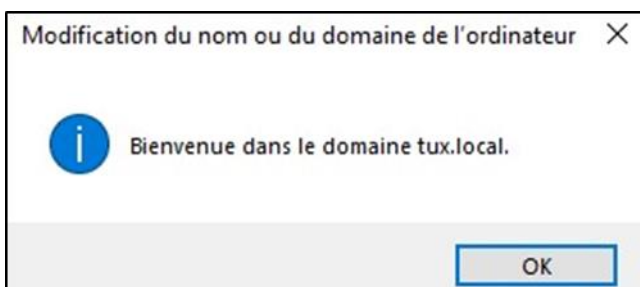
Ensuite tout en bas, on sélectionne « Renommer ce PC ». Dans propriété système, on sélectionne « modifier » et dans modification du nom ou du domaine de l'ordinateur, on sélectionne « Domaine » et on tape notre nom de domaine, à savoir tux.local, on clique sur « OK ».



Entrez alors les identifiants d'admin du domaine, soient administrator, puis Ok :



Votre client est alors admis dans le domaine :



Victoire ! Vous pouvez redémarrer Windows 10.

## 8.13 Installation du LAM



LDAP Account Manager (LAM) est une application web permettant de gérer simplement différents annuaires LDAP tels que OpenLDAP mais aussi l'Active Directory de Samba version 4.

Dans la section précédente, nous avons rattaché un poste Windows 10 à notre domaine tux.local.

Dans cette section, notre objectif sera de permettre l'ouverture de sessions Windows avec des comptes utilisateurs de notre Active Directory Samba version 4.

Nous allons commencer par installer LAM avec la commande suivante :

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

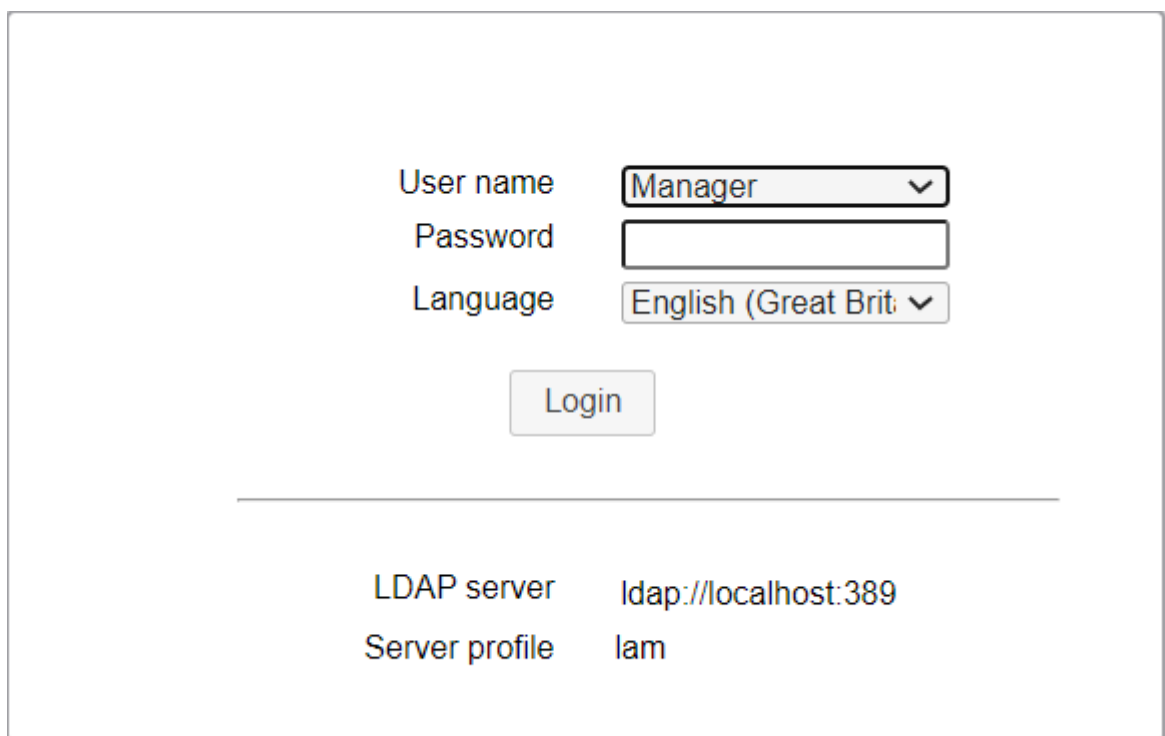
Note : cette commande installe également, si besoin, les paquets supplémentaires apache2 et php.

A l'issue de l'installation, utilisez votre navigateur web pour accéder à l'interface LAM, en tapant :

```
adresse-IP-du-serveur/lam
```

où adresse-IP-du-serveur est l'adresse IP de votre serveur.

Vous devriez obtenir une page web comme celle-ci-dessous :



User name	Manager ▼
Password	<input type="password"/>
Language	English (Great Brit) ▼
<input type="button" value="Login"/>	

---


LDAP server	ldap:///localhost:389
Server profile	lam



## 8.14 Configuration du LAM

### 8.14.1 Informations

Les illustrations suivantes sont extraites d'un LAM version 8.0.1, en langue anglaise.

Les champs de saisie sont accompagnés d'une explication accessible via l'icône  située à droite du champ.

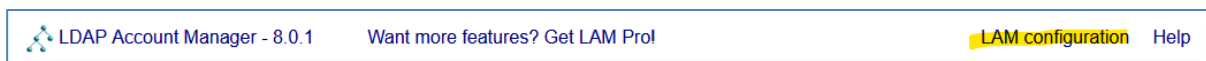
L'authentification sur LAM est réalisée selon deux niveaux :

- Un mot de passe pour la configuration générale (Master Configuration),
- Un mot de passe pour chaque profil serveur (Server Profile).

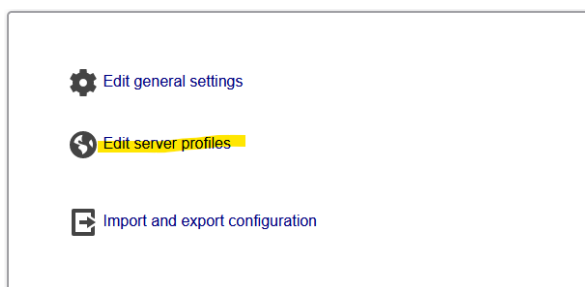
### 8.14.2 Création d'un profil serveur

En premier lieu, nous devons créer un profil de serveur LDAP compatible Samba version 4.

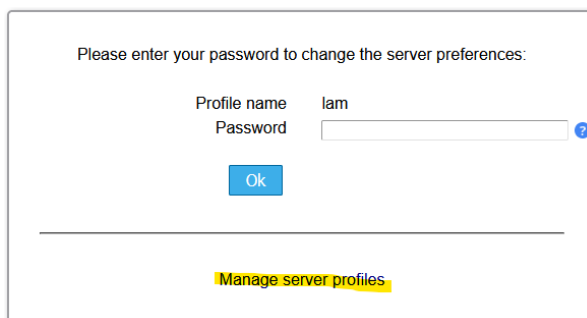
Pour ce faire, cliquez sur le champ « LAM configuration » apparaissant en haut et à droite de la page web.



Puis, sélectionnez « Edit server profiles » :



Puis, cliquez sur « Manage server profiles », afin de créer un nouveau profil LDAP.



Dans cette nouvelle page, saisissez les informations de la section « Add profile » avec la valeur « windows\_samba4 » comme Template, puis cliquez sur le bouton « Add ».



**Profile management**

**Add profile**

Profile name:

Profile password:

Reenter password:

Template:

Note : Le modèle de profil ‘windows-samba4’ est fourni avec une configuration adaptée à Samba version 4. Il va nous faciliter la tâche pour la configuration. Pour autant, il reste personnalisable selon nos besoins.

Enfin, confirmez l’ajout de notre profil, en saisissant le mot de passe d’administration de LAM qui est ‘lam’ par défaut.

**Add profile**

Master password:

**Master password**

Please enter the master configuration password. This is NOT your LDAP password. It is stored in your config.cfg file. If this is the first time you log in, enter "lam".

### 8.14.3 Configuration de notre profil serveur

La page de configuration présente 4 onglets : « General settings », « Account types », « Modules » et « Module settings ».

N’oubliez pas de sauvegarder à la fin de votre saisie.

#### **Onglet « General settings »**

Personnalisez les valeurs des champs en fonction de vos besoins.

Pour notre exemple, nous allons personnaliser les champs suivants :

Section	Champs	Exemple
Server settings	Server address	ldap://192.168.10.101
Tool settings	Tree suffix	dc=tux,dc=local
Security settings	List of valid users	cn=Administrator,cn=users,dc=tux,dc=local



Vous pouvez également personnaliser la langue par défaut, le fuseau horaire et éventuellement redéfinir le mot de passe de notre profil 'samba'.

N'hésitez pas à consulter les explications données pour chaque champ.

### Onglet « Account types »

Cet onglet est dépendant de l'onglet « Modules ». On y trouve les sections relatives aux modules.

Personnalisez les valeurs des champs en fonction de vos besoins.

Pour notre exemple, nous allons personnaliser les champs suivants :

Section	Champs	Exemple
Users	LDAP suffix	cn=Users,dc=tux,dc=local
Groups	LDAP suffix	cn=Users,dc=tux,dc=local
Hosts	LDAP suffix*	cn=Computers,dc=tux,dc=local

### Onglet « Modules »

Le modèle « windows\_samba4 » nous a facilité la tâche en prédéfinissant les modules propres à Samba version 4, à savoir « windowsUser », « windowsGroup » et « windowsHosts ».

Rien n'est à modifier, on conserve les modules proposés.

### Onglet « Module settings »

Pour notre exemple, nous allons personnaliser les champs suivants :

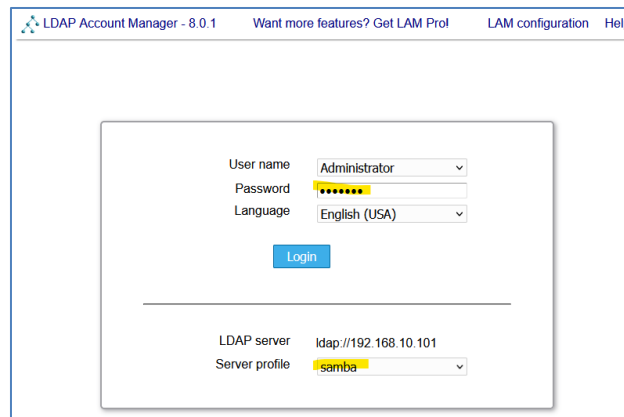
Section	Champs	Exemple
	Domains	tux.local

Il ne reste plus qu'à sauvegarder notre configuration en cliquant sur le bouton « Save ».



## 8.15 Accès à notre Active Directory LDAP

Depuis la page d'accueil de LAM, sélectionnez le compte d'administration du serveur Samba (ici, 'Administrator' ainsi que le mot de passe saisi lors de l'installation). Sélectionnez également votre profil serveur créé précédemment (ici 'samba'), puis cliquez sur le bouton « Login ».



Le message d'erreur suivant peut s'afficher :

**Cannot connect to specified LDAP server. Please try again.**

(8) LDAP error, server says: Strong(er) authentication required - BindSimple: Transport encryption required.

Il résulte d'une mise à jour de la sécurité à partir de la version 4.2.10, par l'ajout d'une authentification forte via le chiffage TLS (voir [https://wiki.samba.org/index.php/Updating\\_Samba#New\\_Default\\_for\\_LDAP\\_Connections\\_Requires\\_Strong\\_Authentication](https://wiki.samba.org/index.php/Updating_Samba#New_Default_for_LDAP_Connections_Requires_Strong_Authentication)).

La mise en place de TLS nécessite des certificats, ce qui dépasse le cadre de ce cours.

Nous allons donc désactiver cette sécurité, uniquement à titre pédagogique.

Encore une fois, dans le cadre de votre entreprise, vous devez conserver cette sécurité et mettre en place la gestion du TLS.

Ouvrez le fichier de configuration, « smb.conf », avec la commande suivante :

```
nano /etc/samba/smb.conf
```

Puis dans la section [global], ajoutez (ou modifiez) l'option suivante :

```
ldap server require strong auth = no
```





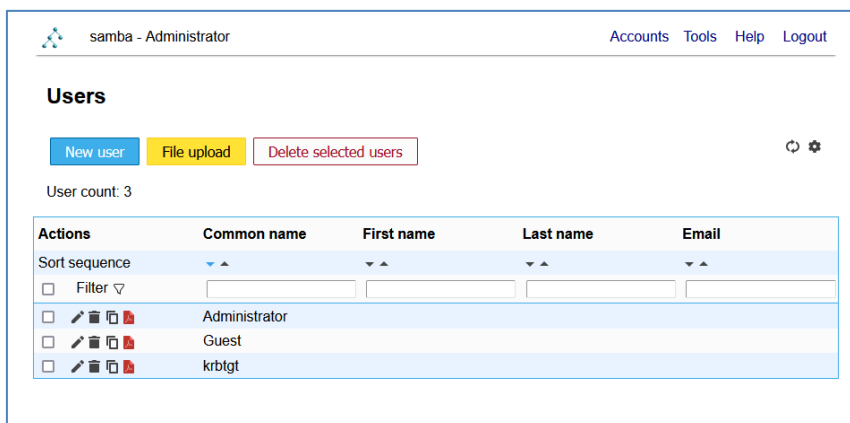
Exemple :

```
# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = DEBSRV
    realm = TUX.LOCAL
    server role = active directory domain controller
    workgroup = TUX
    idmap_ldb:use rfc2307 = yes
    ldap server require strong auth = no
```













Puis, redémarrez le service Samba, pour prendre en compte la modification réalisée :

```
systemctl restart samba-ad-dc.service
```

Vous devriez, désormais, pouvoir accéder à l'Active Directory LDAP :



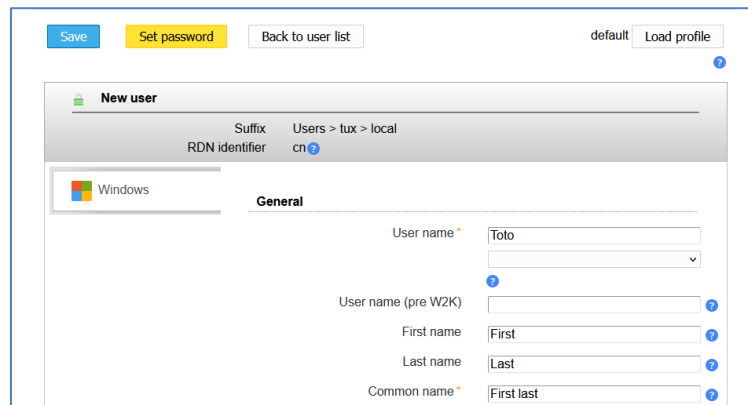
The screenshot shows the 'samba - Administrator' web interface. At the top, there are links for 'Accounts', 'Tools', 'Help', and 'Logout'. The main section is titled 'Users'. Below the title, there are three buttons: 'New user' (blue), 'File upload' (yellow), and 'Delete selected users' (red). Below these buttons, it says 'User count: 3'. There is a table with columns: 'Actions', 'Common name', 'First name', 'Last name', and 'Email'. The table contains three rows: 'Administrator', 'Guest', and 'krbtgt'. Each row has a checkbox and four icons (edit, delete, add, and another delete) in the 'Actions' column.

Actions	Common name	First name	Last name	Email
<input type="checkbox"/>    	Administrator			
<input type="checkbox"/>    	Guest			
<input type="checkbox"/>    	krbtgt			

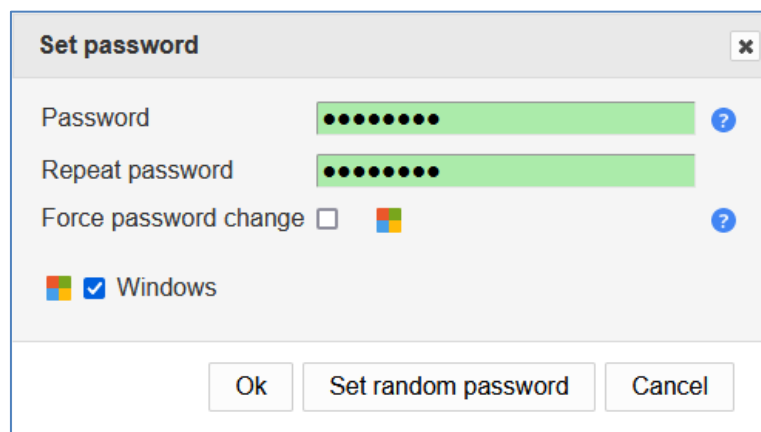


## 8.16 Création d'un utilisateur (Users)

Si ce n'est pas le cas, accédez à liste des utilisateurs via « Accounts > Users ».  
Cliquez sur le bouton « New user », et renseignez les champs selon vos besoins.  
Exemple :



Puis, cliquez sur le bouton « Set password » pour attribuer un mot de passe :



Et enfin, cliquez sur le bouton « save ».













Résultat : l'utilisateur a été créé.

### Users

New userFile uploadDelete selected users

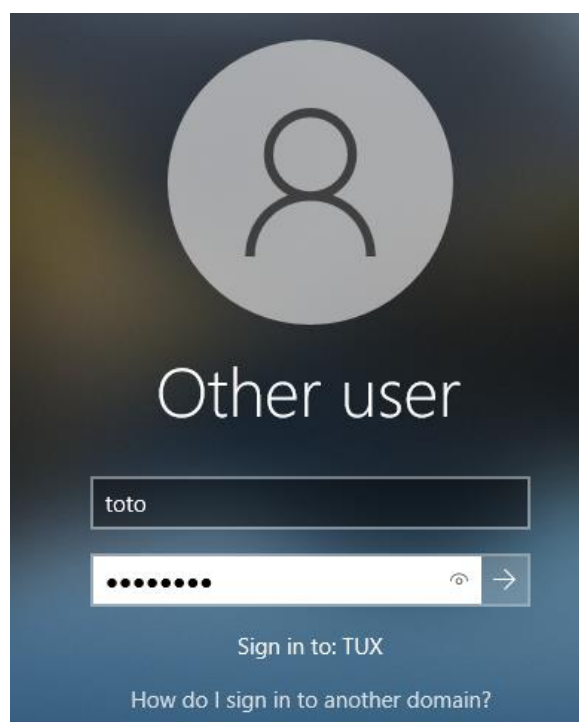
↺ ↻ ⚙

User count: 4

Actions	Common name	First name	Last name	Email
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>   	Administrator			
<input type="checkbox"/>   	Common	First	last	toto@tux.local
<input type="checkbox"/>   	Guest			
<input type="checkbox"/>   	krbtgt			

## 8.17 Test sur un poste Windows 10

L'utilisateur ainsi créé, est désormais opérationnel et peut accéder à notre domaine 'TUX' :



Après ouverture de la session

