

mis a jour des packages :

```
sudo apt update
```

```
sudo apt-get upgrade
```

Création du groupe :

```
sudo groupadd membres ( membres nom de groupe )
```

ajouter les membres dans le groupe membres :

```
sudo adduser amina membres
```

avec sudo adduser amina il demande de donner le mot de passe

vérifier les membre du group membres:

```
getent group membres ou Avec la commande: cd /home/
```

Mot de passe

faire des mot pour les utilisateurs avec la commande

```
sudo passwd amina
```

Créations des admins: Avec la commande:

```
sudo usermod -aG sudo amina: connexion avec un autre compte
```

la commande

```
/etc$ su (nom de membre)
```

```
/etc$ su amina
```

pour revient en admin on met exit

Configurations de SSH:

```
sudo nano /etc/ssh/sshd_config
```

echo "AllowUsers amina" >> /etc/ssh/sshd\_config' : pour écrire dans le fichier sshd\_config : AllowUsers amina pour Permettre à amina de se connecter via SSH. Et on refait la même chose pour les autres utilisateurs.

suppression

```
sudo deluser utilisateur
```

Configuration Fail2ban:

installation de Fail2ban:

- sudo apt install fail2ban : pour installer Fail2ban

le fichier.jail.conf

```
sudo cp /etc/fail2ban/jail.{conf,local} : Pour copier le fichier jail.conf dans un nouveau fichier jail.local
```

- Maintenant on peut ouvrir le fichier jail.local et le modifier avec:

```
sudo cp /etc/fail2ban/jail.{conf,local} :
```

```
sudo nano /etc/fail2ban/jail.local
```

```
sudo nano/etc/fail2ban/jail.local ( changer le bantime le findtime
```

Base de données :

Installation de mariadb-server

installation de la base de données avec la commande : sudo apt install mariadb-server

Configuration de BDD:

Pour entrer au fichier 50-server.cnf:

```
sudo vim /etc/mysql/mariadb.conf.d/50-server.cnf ( Vérifions que):
```

```
character-set-server=utf8mb4
```

```
collation-server=utf8mb4_general_ci)
```

Redémarrage :

```
sudo systemctl restart mariadb
```

.vérification du statut:

Pour vérifier le status mariadb ( active or deactivate) avec la commande:

```
sudo systemctl status mariadb
```

installation mysql\_secure\_installation

Pour installer mysql\_secure\_installation avec la commande: :sudo mysql\_secure\_installation

MYSQL: Pour accéder à mysql :

```
sudo mysql
```

et pour voir les base de données:

```
show databases
```

Création de la base de données

```
create database toeic;
```

Utilisation de la base toeic:

Accéder à la base données toeic avec la commande :

```
use toeic;
```

Création de deux tables Test

```
CREATE TABLE Test(id int(10) NOT NULL, niveau varchar (100) NOT NULL);
```

```
INSERT INTO Test(id, niveau) VALUES('1','facile');
```

Mise à jour des package

```
Sudo apt updat
```

```
Sudo apt upgrade
```

- Création des utilisateurs

```
sudo adduser
```

rendre l'utilisateur admin

```
sudo usermod -aG sudo aya
```

Tester la présence

“sudo cat /etc/group”: pour vérifier les membre du group sudo

et vérifier la présence des autres utilisateurs

Création d'un nouveau groupe:

```
sudo groupadd nom_groupe
```

Se localiser dans la racine : sudo su -

Affecter un nouveau mot de passe a admin: sudo passwd admin

ouvrir le fichier ssh et pouvoir le modifier

```
passwordAUTHENTICATION Yes
```

Tester la modification

```
sudo cat/etc/ssh/sshd_config
```

‘echo “AllowUsers aya” >> /etc/ssh/sshd\_config’: pour écrire dans le fichier

sshd\_config : AllowUsers amina pour Permettre à 'utilisateur' de se connecter via SSH

```
echo "AllowUsers nom_utilisateur" >> /etc/ssh/sshd_config
```

```
systemctl restart sshd
```

Connexion via ssh:

```
login as: nom_utilisateur
```

Permettre aux nouveaux utilisateurs de se connecter

via SSH

```
sudo echo "AllowUsers nom_des utilisateurs >> /etc/ssh/sshd_config"
```

```
systemctl restart sshd
```

### Configuration Fail2ban

Installation du Fail2ban pour limiter le nombre d'accès

Adresse ip privée

"Hostname -I"

On a besoin des adresses ip privée, pour cela on tape la commande suivante

Installation de Fail2ban

```
"sudo apt install fail2ban"
```

### Vérification du statut fail2ban

```
"sudo systemctl status fail2ban"
```

a configuration se trouve dans le fichier /etc/fail2ban/jail.conf ,il faut éviter de travailler directement sur ce package (écrasement lors des mises à jour), de ce fait

on va créer une copie sur un fichier d'extension .local

- Copie du fichier jail.conf dans un fichier jail.local

```
"sudo cp/etc/fail2ban/jail.{conf,local}"
```

- Ensuite ouverture du fichier jail.local et modification

```
"sudo nano /etc/fail2ban/jail.local"
```

### Les mises a jours

Sudo apt update

Sudo apt upgrade

### Installation des paquets pour le serveur web

Installation du serveur web avec php "sudo apt install apache2 php"

-vérifier que le serveur web fonctionne correctement( adresse publique sur google

### Création d'un dossier projet

```
"sudo mkdir /var/www/ws"
```

```
sudo mv /var/www/ws /var/www/projet
```

```
ls /var/www:
```

```
cd /var/www/projet
```

-Création d'une page html nommé index.html

Ouvrir le fichier index.html et y mettre du contenu

```
cd /var/www/projet
```

```
"sudo nano index.html"
```

Se positionner dans le dossier de configuration

```
"cd /etc/apache2/sites-available/"
```

Copier la configuration par défaut dans projet

```
"sudo cp 000-default.conf projet.conf"
```