ÉCOLE D'INGÉNIEURS DU LITTORAL

Compte rendu du projet Administration réseau(Serveur BDD)

OUMENSKOU Youssef

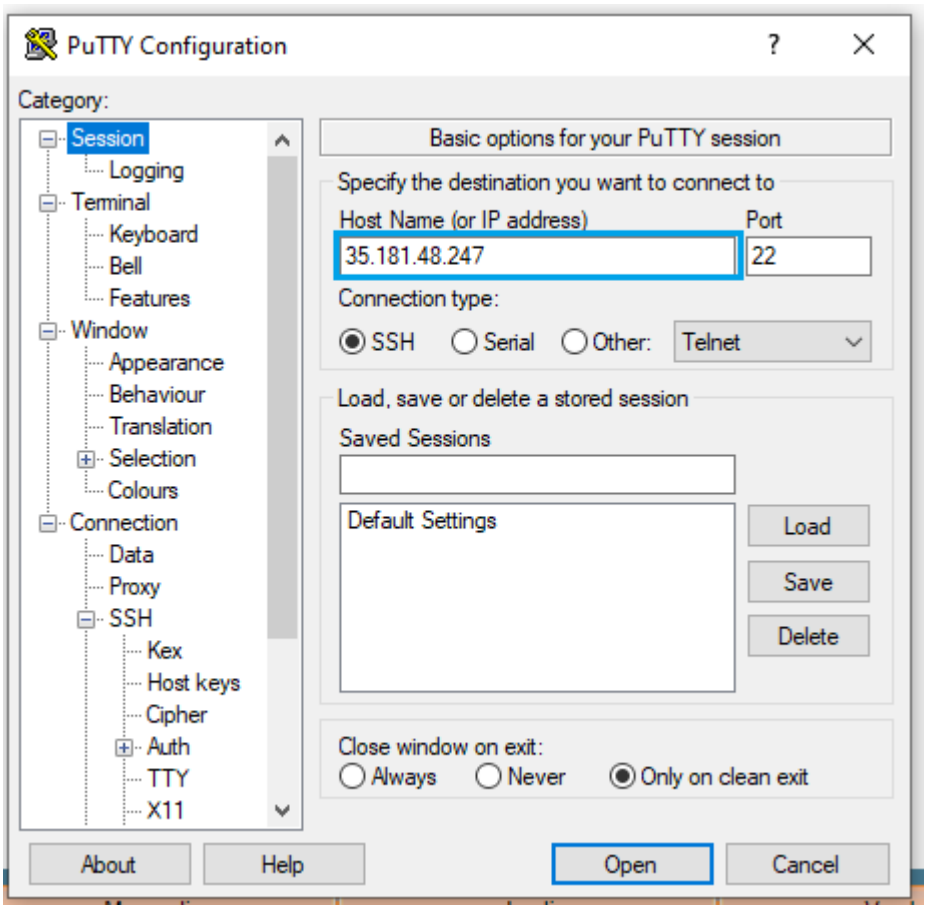
Sommaire:

I. PuTTy Configuration.
II. Mise à jour des packages.
III. création de groupes.
IV. création des utilisateurs.
V. configuration du ssh.
VI. configuration fail2ban.
VII. Installation et configuration de serveur BDD.

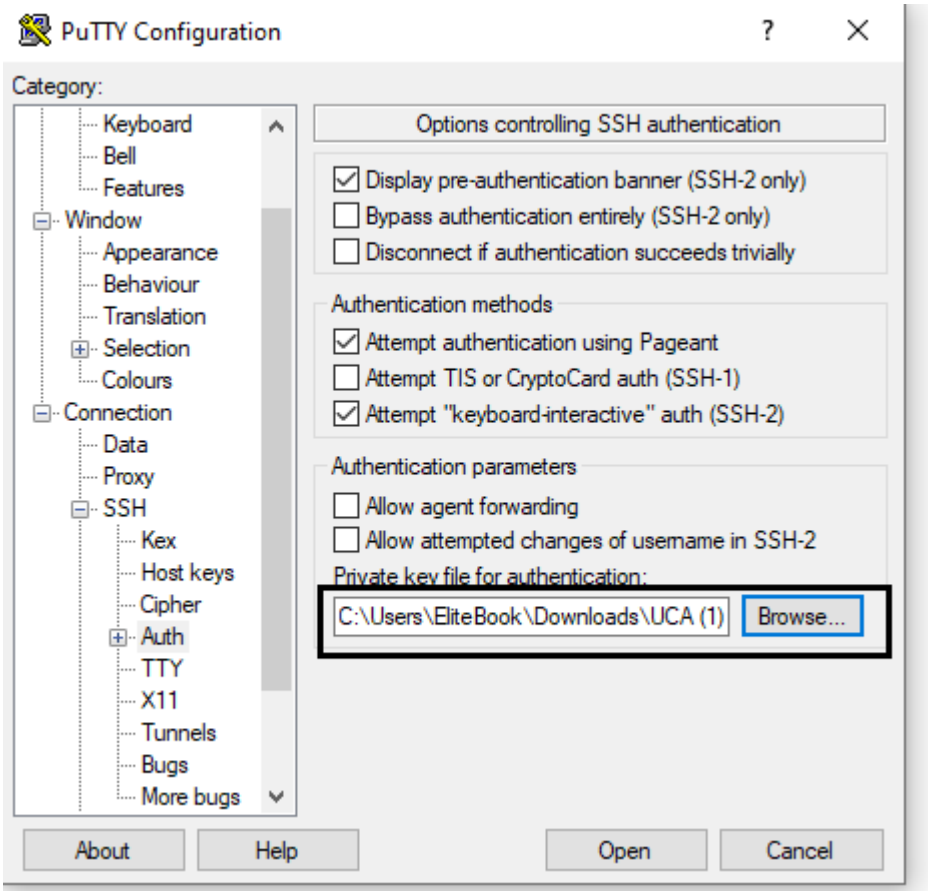
Team : UCA

PuTTy Configuration:

- ❖ l'adresse ip public



❖ On ajout ici la clé ssh



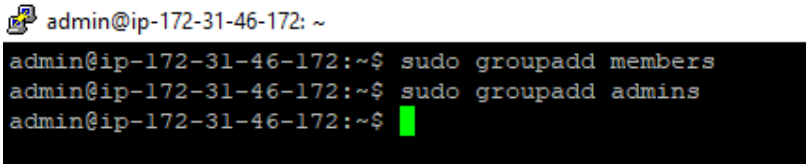
Mise à jour des packages:

- ❖ tout d'abord il faut faire la mise à jour des packages en utilisant les deux commandes suivantes:
  - ➢ "sudo apt-get update".
  - ➢ "sudo apt-get upgrade".

```
admin@ip-172-31-46-172:~$ sudo apt-get update
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://cdn-aws.deb.debian.org/debian bullseye InRelease
Hit:3 http://cdn-aws.deb.debian.org/debian bullseye-updates InRelease
Hit:4 http://cdn-aws.deb.debian.org/debian bullseye-backports InRelease
Hit:5 http://repo.mysql.com/apt/debian bullseye InRelease
```

```
admin@ip-172-31-46-172:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
```

1-)création des groupes:

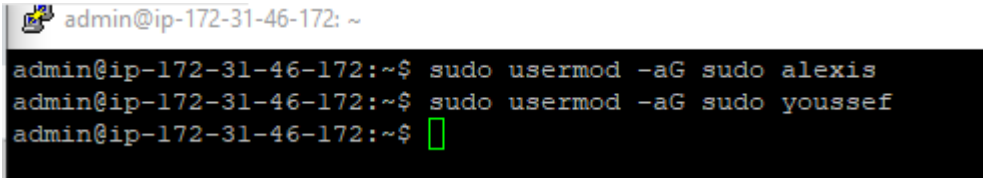


2-)création des utilisateurs:

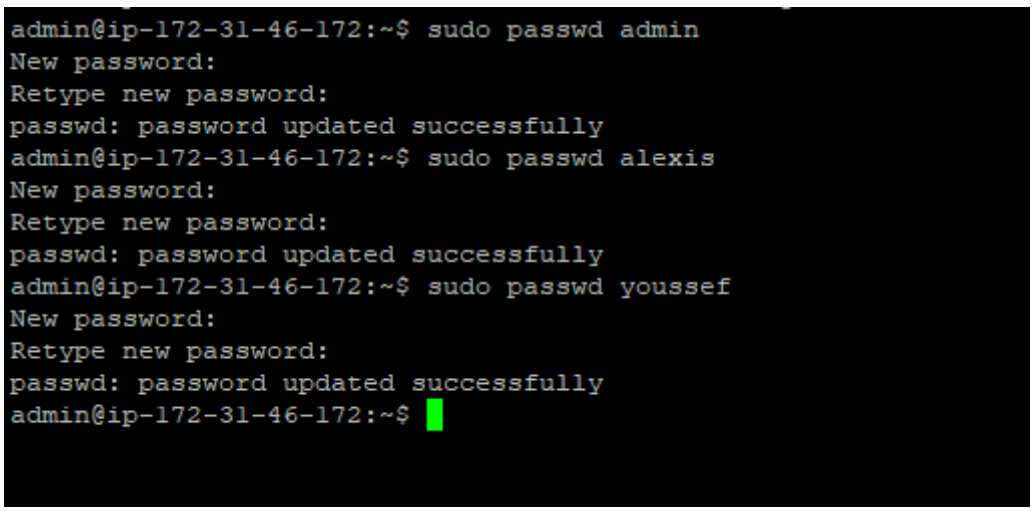
- pour créer les utilisateurs on utilise la commande “sudo adduser <username>”

```
admin@ip-172-31-46-172:~$ sudo useradd alexis -g admins -m
admin@ip-172-31-46-172:~$ sudo useradd youssef -g admins -m
admin@ip-172-31-46-172:~$ sudo useradd hamza -g members -m
admin@ip-172-31-46-172:~$ sudo useradd khaoula -g members -m
admin@ip-172-31-46-172:~$ sudo useradd oussama -g members -m
admin@ip-172-31-46-172:~$ sudo useradd hicham -g members -m
```

- Pour donner les droits d’administrateur aux utilisateurs(alexis et youssef) on utilise la commande “sudo usermod -aG”.



- Pour changer le password des utilisateurs on utilise la commande “sudo passwd <username>”:
  - Password de admin: admin*12345
  - Password de alexis: alexis_network



3-)configuration du ssh:

- Pour donner l'autorisation aux nouveaux utilisateurs et admin à connecter avec le mot de passe ,on va modifier le fichier “/etc/ssh/sshd_config” avec la commande “sudo vi /etc/ssh/sshd_config”:
  - ➢ On va changer “**no**” par “**yes**”

```
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

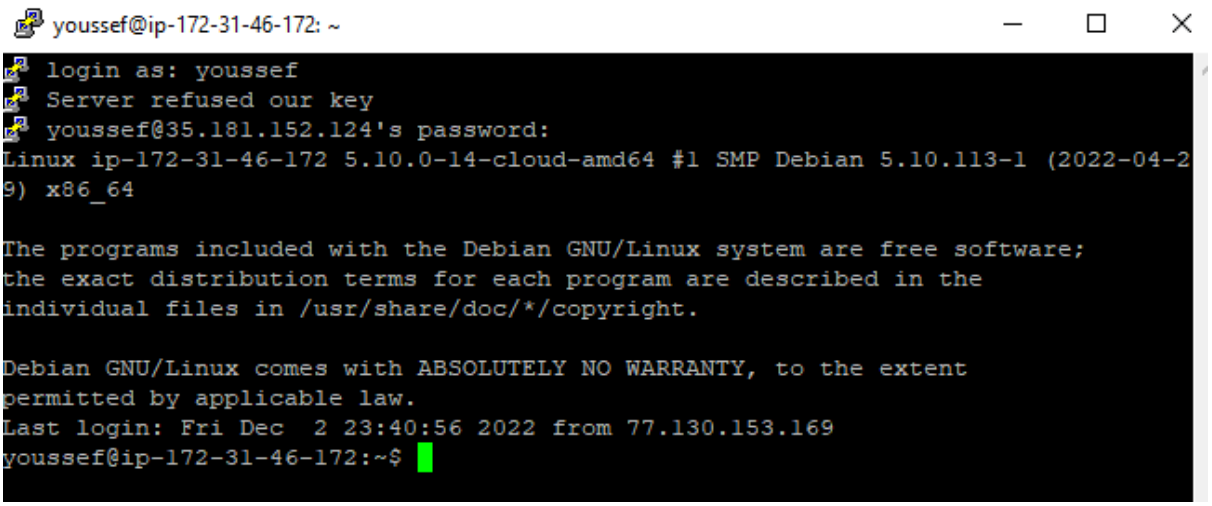
  - ➢ On va ajouter cette ligne a la fin de fichier “AllowGroups sudo members” pour permettre aux utilisateurs qui appartiennent à ces groupes de se connecter à la machine.

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
ClientAliveInterval 120
AllowGroups sudo members
```

  - ➢ Après on tappe la commande “sudo systemctl restart sshd”.

```
admin@ip-172-31-46-172:~$ sudo vi /etc/ssh/sshd_config
admin@ip-172-31-46-172:~$ sudo systemctl restart sshd
admin@ip-172-31-46-172:~$
```

  - ➢ pour se connecter à ssh on doit entrer le mot passe.



4-)configuration fail2ban:

- Installation de fail2ban via la commande “sudo apt-get install fail2ban”

```
admin@ip-172-31-46-172:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 1 not upgraded.
Need to get 596 kB of archives.
After this operation, 2819 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 fail2ban all 0.11.2-2 [451 kB]
Get:2 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 python3-pyinotify all 0.9.6-1.3
7.2 kB]
Get:3 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 python3-systemd amd64 234-3+b4 [
.4 kB]
Get:4 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 whois amd64 5.5.10 [81.1 kB]
Fetched 596 kB in 0s (4426 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 29607 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-2_all.deb ...
Unpacking fail2ban (0.11.2-2) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-1.3_all.deb ...
Unpacking python3-pyinotify (0.9.6-1.3) ...
Selecting previously unselected package python3-systemd.
Preparing to unpack .../python3-systemd_234-3+b4_amd64.deb ...
Unpacking python3-systemd (234-3+b4) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.10_amd64.deb ...
Unpacking whois (5.5.10) ...
Setting up whois (5.5.10) ...
Setting up fail2ban (0.11.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/sys
m/fail2ban.service.
Setting up python3-pyinotify (0.9.6-1.3) ...
Setting up python3-systemd (234-3+b4) ...
Processing triggers for man-db (2.9.4-2) ...
admin@ip-172-31-46-172:~$
```

- On affiche le statut de fail2ban via la commande “sudo systemctl status fail2ban”

```
admin@ip-172-31-46-172:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-11-21 14:56:04 UTC; 1min 14s ago
       Docs: man:fail2ban(1)
    Process: 15048 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
   Main PID: 15049 (fail2ban-server)
      Tasks: 5 (limit: 1123)
     Memory: 17.2M
        CPU: 250ms
     CGroup: /system.slice/fail2ban.service
             └─15049 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 21 14:56:04 ip-172-31-46-172 systemd[1]: Starting Fail2Ban Service...
Nov 21 14:56:04 ip-172-31-46-172 systemd[1]: Started Fail2Ban Service.
Nov 21 14:56:04 ip-172-31-46-172 fail2ban-server[15049]: Server ready
admin@ip-172-31-46-172:~$
```

- Faire une copie de fichier de configuration pour éviter de l'écraser lors de mise à jour de package.

```
admin@ip-172-31-46-172: ~
admin@ip-172-31-46-172:~$ sudo cp /etc/fail2ban/jail.conf  /etc/fail2ban/jail.local
admin@ip-172-31-46-172:~$
```

- On modifie le fichier de configuration via la commande “sudo vi /etc/fail2ban/jail.local”.
  - ➢ On ajoute les adresses ip privés des utilisateurs et l'adresse ip locale de la machine afin que fail2ban les ignore.

```
# "ignoreip" can be a list of IP addresses, CIDR m
# will not ban a host which matches an address in
# can be defined using space (and/or comma) separa
ignoreip = 127.0.0.1/8 ::172.31.46.172 172.31.33.1

# External command that will take an tagged argume
# and return true if the IP is to be ignored. Fals
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host i
bantime  = 3m

# A host is banned if it has generated "maxretry"
# seconds.
findtime  = 3m

# "maxretry" is the number of failures before a ho
maxretry = 3
```

- On redémarre le serveur fail2ban et on affiche son statut.

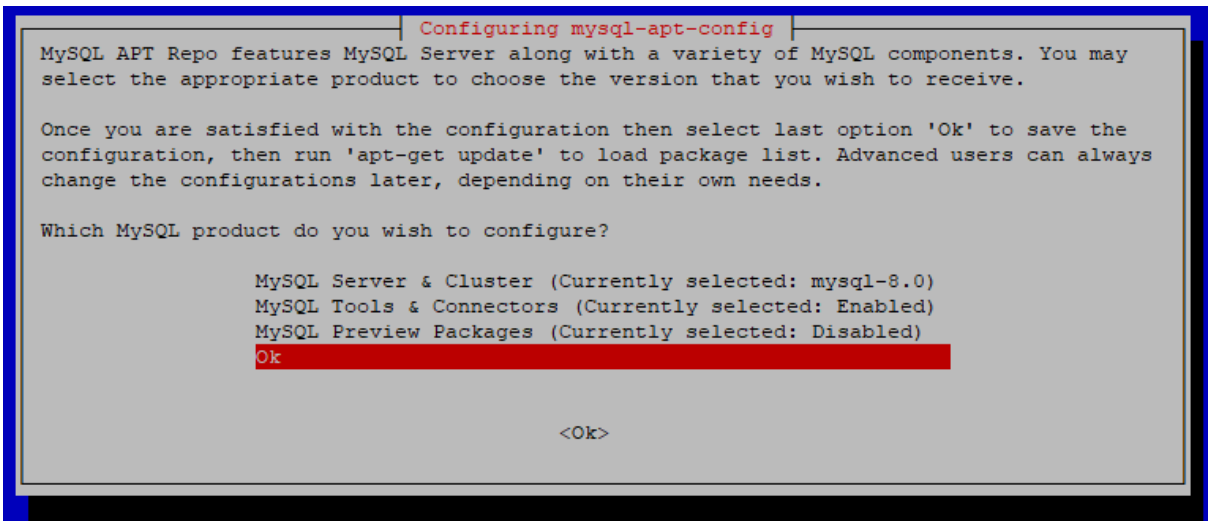
```
admin@ip-172-31-46-172:~$ sudo systemctl restart fail2ban.service
admin@ip-172-31-46-172:~$ sudo systemctl status fail2ban.service
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-12-02 21:04:49 UTC; 23s ago
       Docs: man:fail2ban(1)
    Process: 5438 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
   Main PID: 5439 (fail2ban-server)
      Tasks: 5 (limit: 1123)
     Memory: 13.4M
        CPU: 205ms
     CGroup: /system.slice/fail2ban.service
             └─5439 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 02 21:04:49 ip-172-31-46-172 systemd[1]: fail2ban.service: Succeeded.
Dec 02 21:04:49 ip-172-31-46-172 systemd[1]: Stopped Fail2Ban Service.
Dec 02 21:04:49 ip-172-31-46-172 systemd[1]: fail2ban.service: Consumed 3.350s CPU time.
Dec 02 21:04:49 ip-172-31-46-172 systemd[1]: Starting Fail2Ban Service...
Dec 02 21:04:49 ip-172-31-46-172 systemd[1]: Started Fail2Ban Service.
Dec 02 21:04:49 ip-172-31-46-172 fail2ban-server[5439]: Server ready
admin@ip-172-31-46-172:~$
```

5-) Installation et configuration de serveur BDD:

Etape 1:Ajout du référentiel de logiciels Mysql

- Mettre à jour des packages et installation de package gnupg .

```
admin@ip-172-31-46-172:/tmp$ sudo apt update
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://cdn-aws.deb.debian.org/debian bullseye InRelease
Hit:3 http://cdn-aws.deb.debian.org/debian bullseye-updates InRelease
Get:4 http://cdn-aws.deb.debian.org/debian bullseye-backports InRelease [49.0 kB]
Fetched 49.0 kB in 0s (118 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
admin@ip-172-31-46-172:/tmp$ sudo apt install gnupg
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dirmngr gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm
  libassuan0 libksba8 libnpth0 pinentry-curses
Suggested packages:
  dbus-user-session pinentry-gnome3 tor parcimonie xloadimage scdaemon pinentry-doc
The following NEW packages will be installed:
  dirmngr gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf
  gpgsm libassuan0 libksba8 libnpth0 pinentry-curses
0 upgraded, 14 newly installed, 0 to remove and 1 not upgraded.
Need to get 7665 kB of archives.
After this operation, 15.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 libassuan0 amd64 2.5.3-7.1 [50.
B]
```



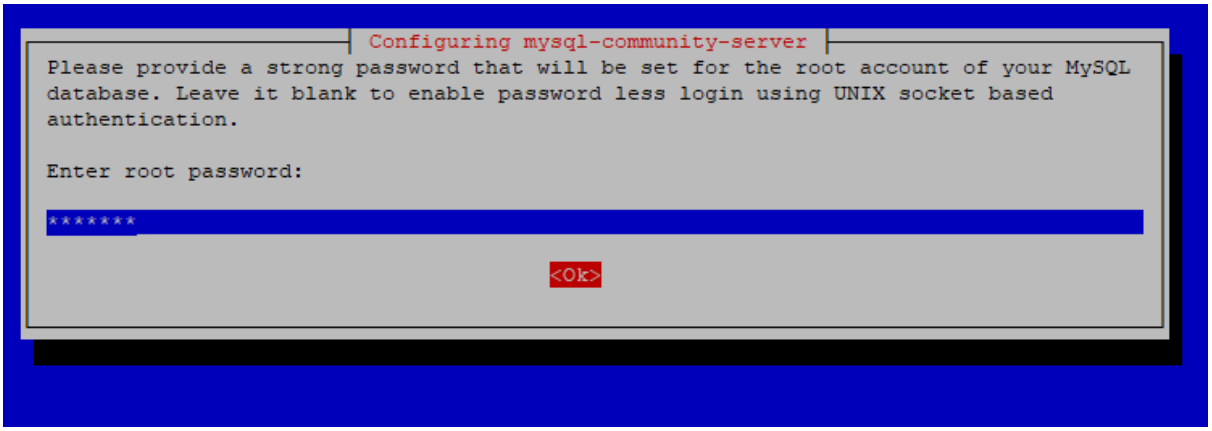
- On ajoute du référentiel de logiciels Mysql.

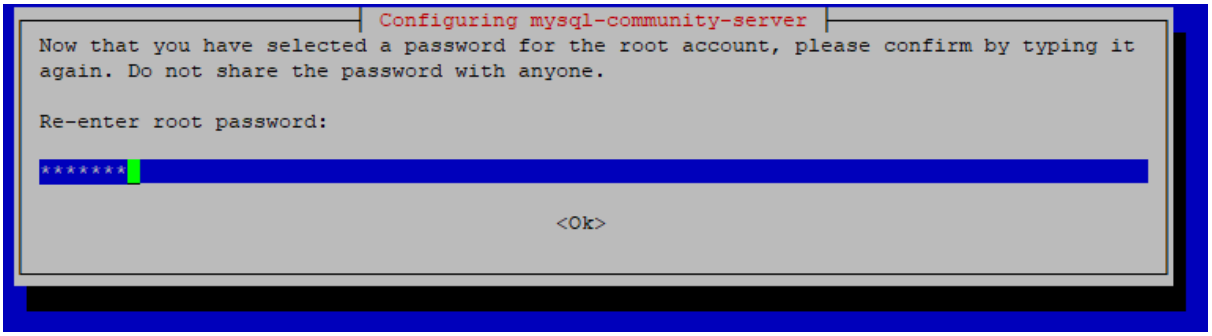
```
admin@ip-172-31-46-172:/tmp$ wget https://dev.mysql.com/get/mysql-apt-config_0.8.22-1_all.deb
--2022-11-21 15:14:44--  https://dev.mysql.com/get/mysql-apt-config_0.8.22-1_all.deb
Resolving dev.mysql.com (dev.mysql.com)... 23.217.254.70, 2a02:26f0:2b00:387::2e31, 2a02:26f0:2b0
0:3a2::2e31
Connecting to dev.mysql.com (dev.mysql.com)|23.217.254.70|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://repo.mysql.com//mysql-apt-config_0.8.22-1_all.deb [following]
--2022-11-21 15:14:44--  https://repo.mysql.com//mysql-apt-config_0.8.22-1_all.deb
Resolving repo.mysql.com (repo.mysql.com)... 184.50.240.231
Connecting to repo.mysql.com (repo.mysql.com)|184.50.240.231|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18012 (18K) [application/x-debian-package]
Saving to: 'mysql-apt-config_0.8.22-1_all.deb'

mysql-apt-config_0.8.22- 100%[=============================>]  17.59K  --.-KB/s    in 0s

2022-11-21 15:14:44 (204 MB/s) - 'mysql-apt-config_0.8.22-1_all.deb' saved [18012/18012]

admin@ip-172-31-46-172:/tmp$ sudo dpkg -i mysql-apt-config*
(Reading database ... 30355 files and directories currently installed.)
Preparing to unpack mysql-apt-config_0.8.22-1_all.deb ...
Unpacking mysql-apt-config (0.8.22-1) ...
Setting up mysql-apt-config (0.8.22-1) ...
Warning: apt-key should not be used in scripts (called from postinst maintainerscript of the pack
age mysql-apt-config)
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

Etape 2:installation de serveur MySQL

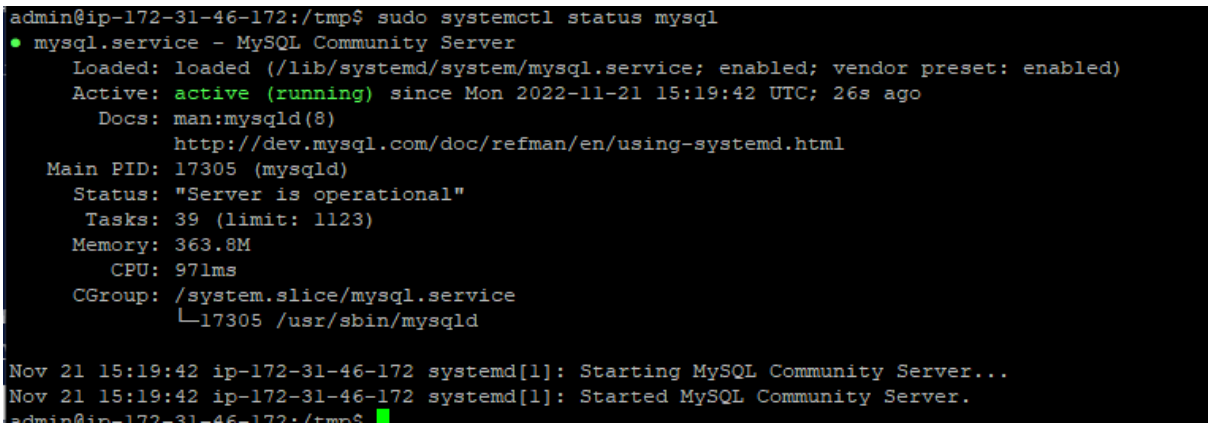
- Installation de serveur mysql via la commande “sudo apt install mysql-server”

```
172-31-46-172:/tmp$ sudo apt install mysql-server
ackage lists... Done
dependency tree... Done
tate information... Done
wing additional packages will be installed:
-compat4 libmecab2 libnuma1 libperl5.32 mecab-ipadic mecab-ipadic-utf8 mecab-utils
lient mysql-common mysql-community-client mysql-community-client-core
ommunity-client-plugins mysql-community-server mysql-community-server-core perl
dules-5.32
 packages:
c libterm-readline-gnu-perl | libterm-readline-perl-perl make
harness-archive-perl
wing NEW packages will be installed:
-compat4 libmecab2 libnuma1 libperl5.32 mecab-ipadic mecab-ipadic-utf8 mecab-utils
lient mysql-common mysql-community-client mysql-community-client-core
ommunity-client-plugins mysql-community-server mysql-community-server-core
erver perl perl-modules-5.32
d, 17 newly installed, 0 to remove and 1 not upgraded.
et 49.4 MB of archives.
s operation, 401 MB of additional disk space will be used.
nt to continue? [Y/n] Y
```





- Affiche le statut de mysql



Etape 3:sécurité

- Effectuer des mises à jour liées à la sécurité via la commande “mysql_secure_installation”.

```
admin@ip-172-31-46-172:/tmp$ mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.
Using existing password for root.

Estimated strength of the password: 25
Change the password for root ? ((Press y|Y for Yes, any other key for No) : N

 ... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
Success.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y
Success.
```

Étape 4:connexion à mysql,création de base de données, et tableau pour tester.

- On se connecte au serveur mysql via la commande “mysql -u root -p”.

```
admin@ip-172-31-46-172:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.31 MySQL Community Server - GPL

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database application
    -> ;
Query OK, 1 row affected (0.01 sec)

mysql> use application;
Database changed
mysql> show tables;
Empty set (0.00 sec)

mysql>
```

```
mysql>  CREATE TABLE CUSTOMERS(
    ->    ID   INT              NOT NULL,
    ->    NAME VARCHAR (20)     NOT NULL,
    ->    AGE  INT              NOT NULL,
    ->    ADDRESS  CHAR (25) ,
    ->    SALARY   DECIMAL (18, 2),
    ->    PRIMARY KEY (ID)
    -> );
Query OK, 0 rows affected (0.03 sec)
```

```
mysql> INSERT INTO CUSTOMERS (ID,NAME,AGE,ADDRESS,SALARY)
    -> VALUES (1, 'Ramesh', 32, 'Ahmedabad', 2000.00 );
Query OK, 1 row affected (0.01 sec)

mysql> select * from CUSTOMERS;
+----+--------+-----+-----------+---------+
| ID | NAME   | AGE | ADDRESS   | SALARY  |
+----+--------+-----+-----------+---------+
|  1 | Ramesh |  32 | Ahmedabad | 2000.00 |
+----+--------+-----+-----------+---------+
1 row in set (0.00 sec)
```