

# Mise en place SFTP Debian 11

Fait en entreprise et dans le cadre de l'épreuve E4 du BTS SIO 2022-2024

[Télécharger en PDF](#)

## Sommaire

- [Pour Commencer](#)
  - [Prérequis](#)
  - [Installation](#)
    - [Formatage de la clé USB](#)
    - [Système](#)
    - [Installation des applications](#)
      - [Installation SFTP](#)
      - [Configuration SFTP](#)
  - [Sécurité](#)
  - [Utilisation](#)

## Pour Commencer

Nous avons dans l'entreprise KNCO le besoin de partager des fichiers entre les employés  
Cela passe par des excels contenant les bilans de chaque représentants (commerciaux se déplaçant chez les opticiens) ou encore les photos des produits utilisés par les représentants, le SAV mais aussi le service marketing

Le besoin est donc de pouvoir partager des fichiers entre les employés de l'entreprise, de manière sécurisée et simple d'utilisation

Nous partons également du postulat que les employés sont tous sur le même réseau, que ce soit en local ou en VPN, celui-ci étant déjà configuré par une autre entreprise

## Prérequis

- [Rufus](#), [Balena Etcher](#) ou tout autre logiciel du genre
- Clé/Stockage USB de 4Go minimum
- ISO de [Debian 11](#)
- Un serveur prêt à être installé

## Installation

### **Formatage de la clé USB**

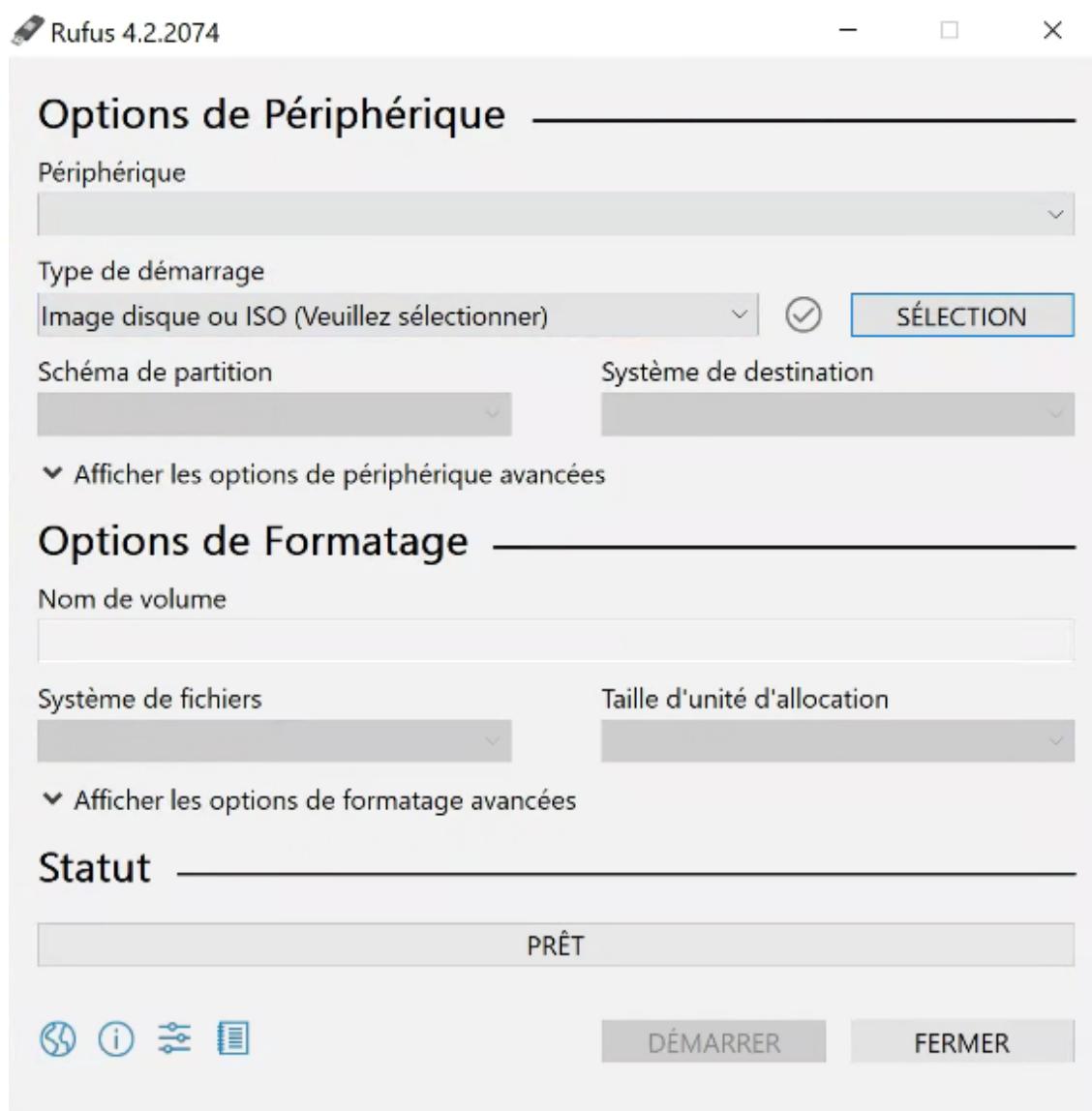
1. Téléchargez l'ISO de [Debian 11](#)

2. Téléchargez [Rufus](#)

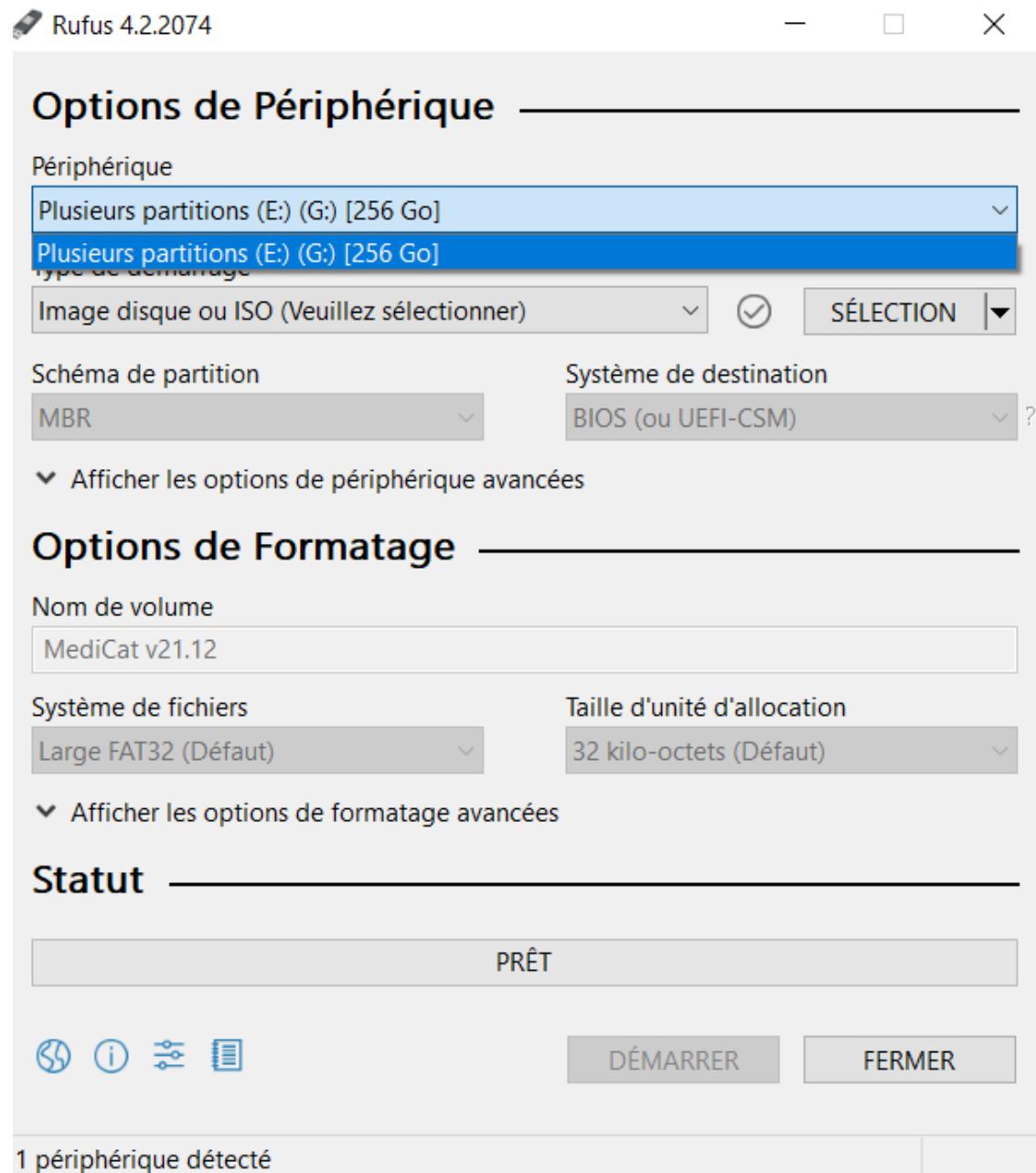
 [Rufus Website](#)

3. Branchez la clé USB sur le PC

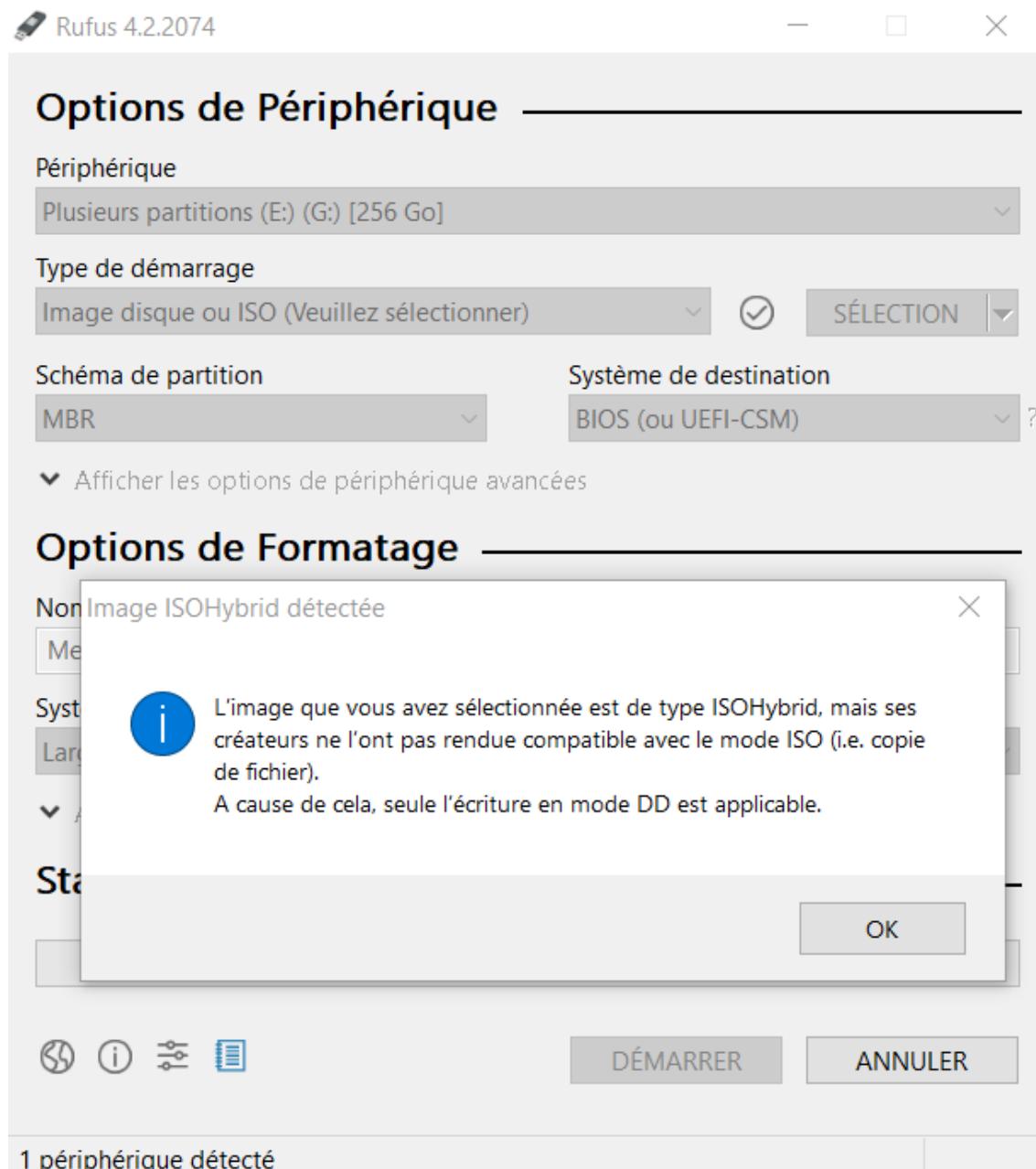
4. Ouvrir Rufus



5. Sélectionnez la clé USB



6. Sélectionnez l'ISO de Debian 11, continuez si vous avez une erreur "ISOHybrid"

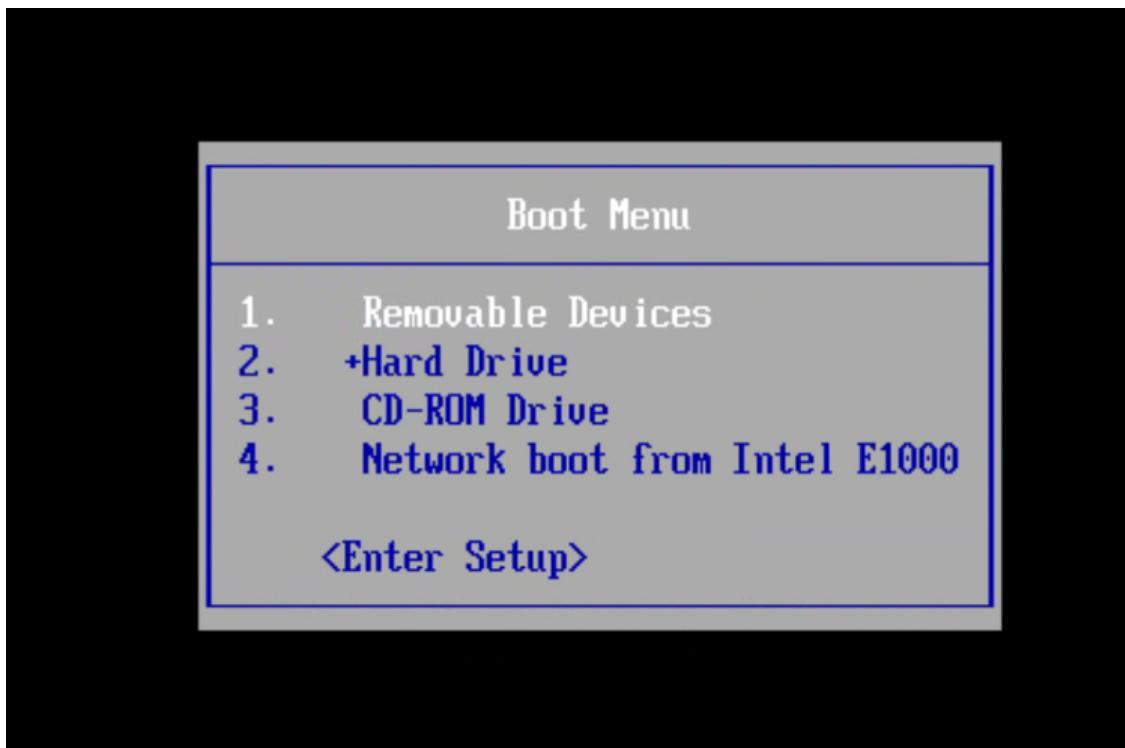


7. Lancez le formatage

## Système

1. Branchez la clé USB sur le serveur
2. Démarrez le serveur
3. Appuyez sur F11 pour accéder au boot menu

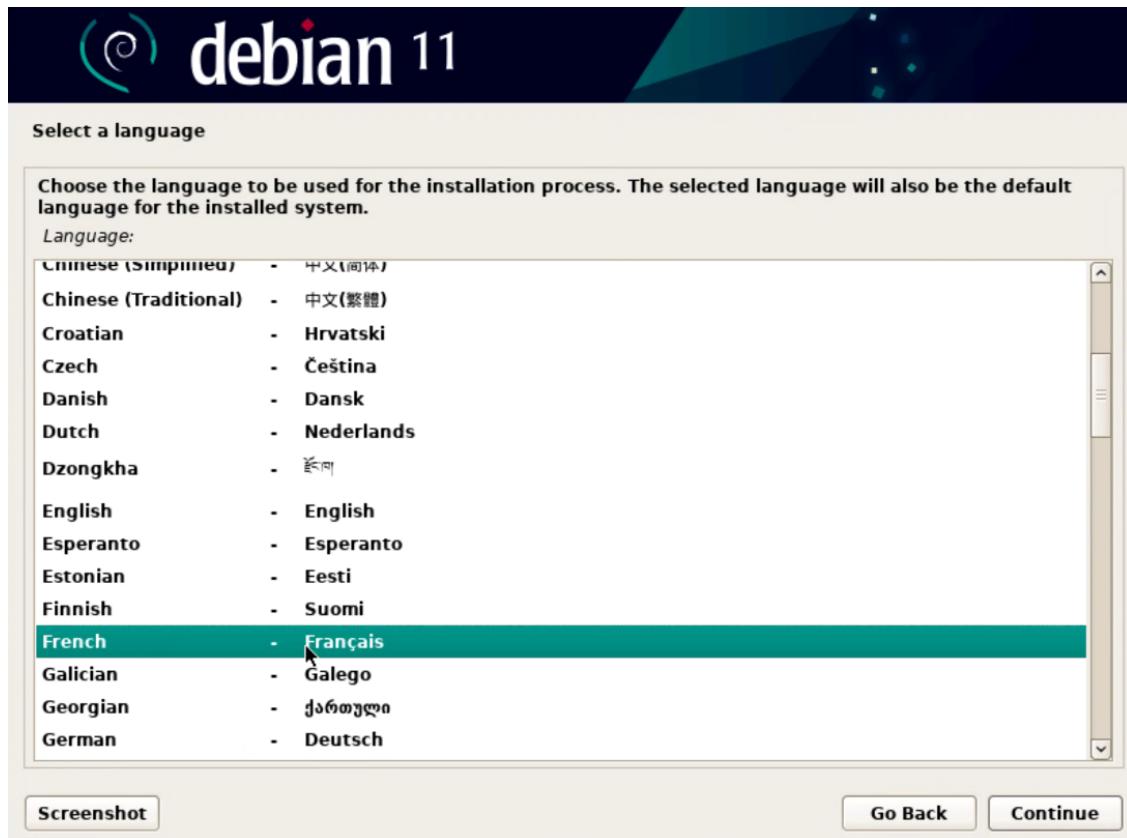
4. Sélectionnez la clé USB et faites entrer



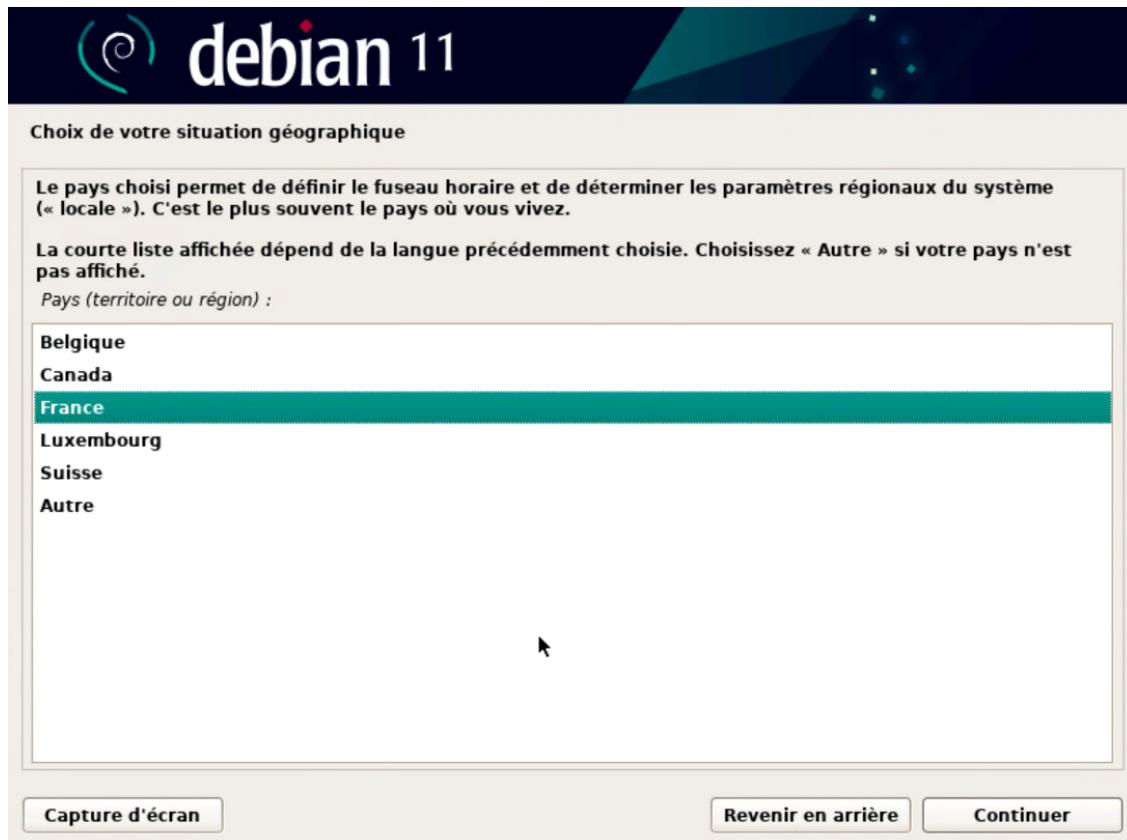
5. Un nouveau menu apparaît, sélectionnez "Graphical Install" et faites entrer



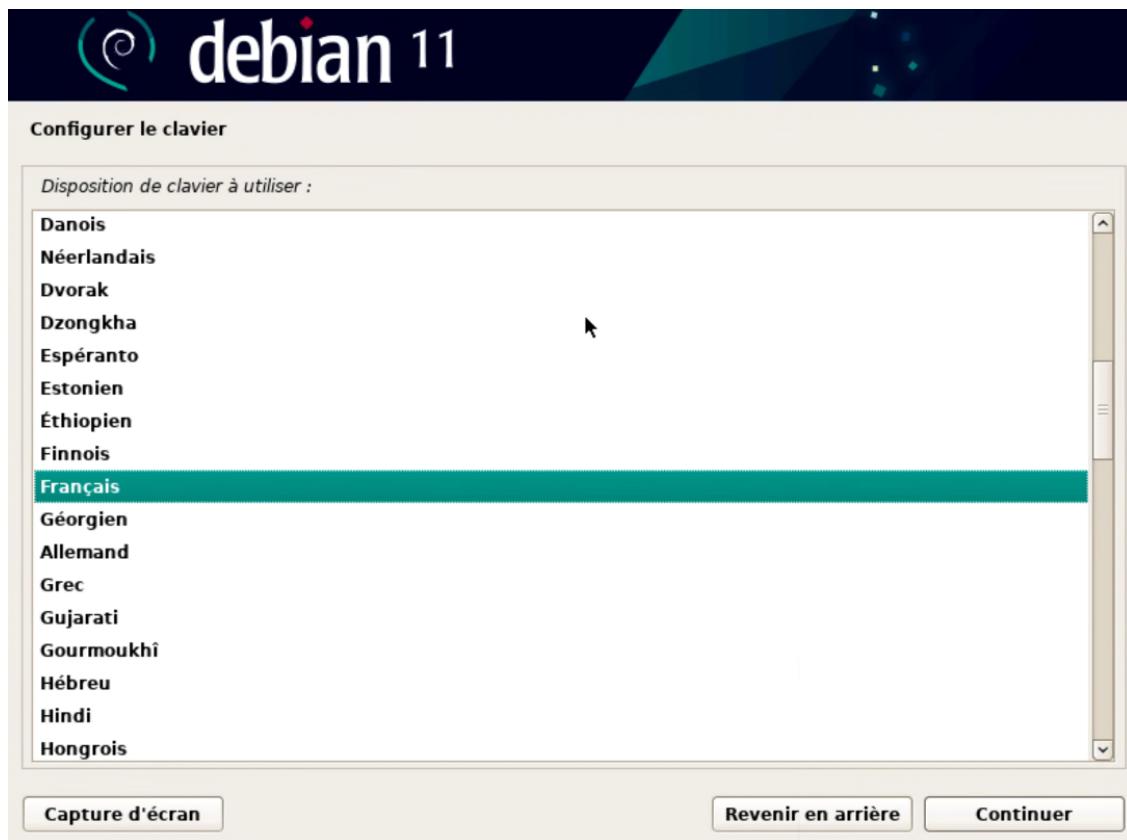
6. Sélectionnez ensuite la langue voulue (ici Français) en utilisant les flèches ou la souris puis entrer ou "continue".



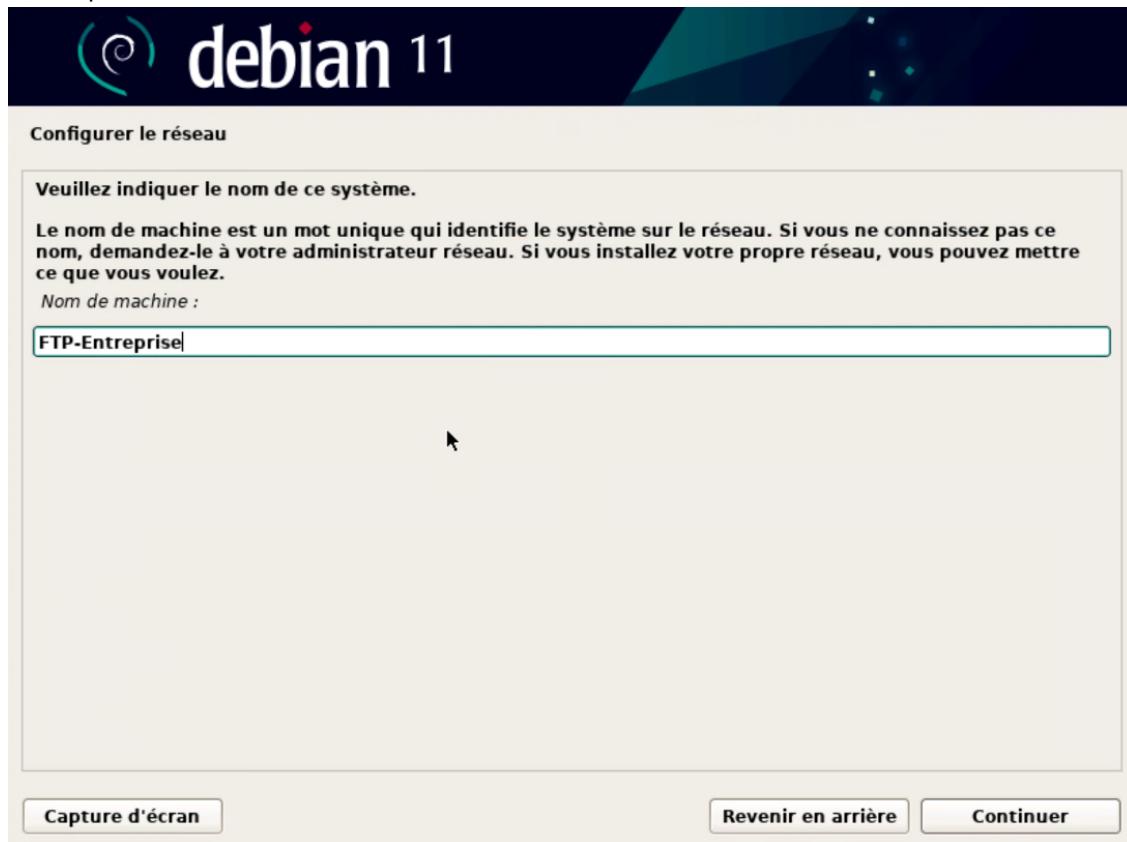
7. Sélectionnez votre pays (ici France) puis continuez. Cela impactera les configurations fuseaux horaires, etc...



8. Sélectionnez votre disposition de clavier, un Azerty français sera "Français" ; pour un Qwerty, cela sera "Etats-Unis"



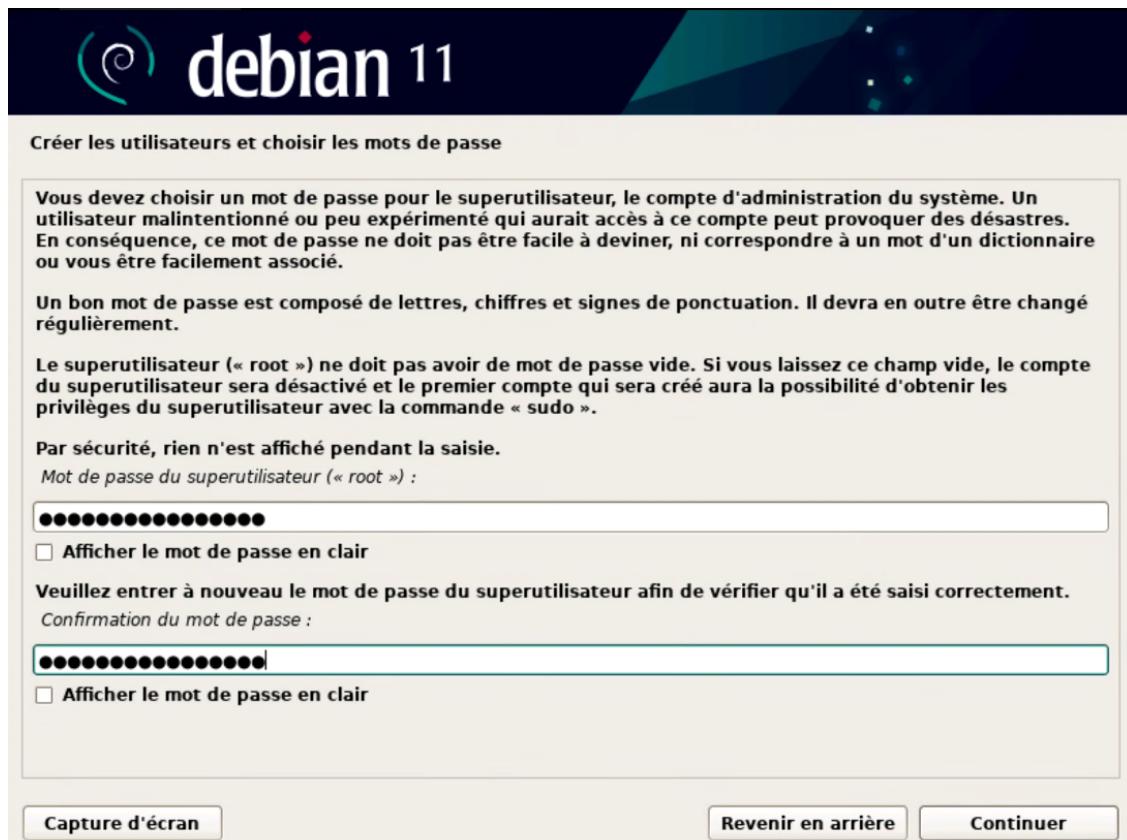
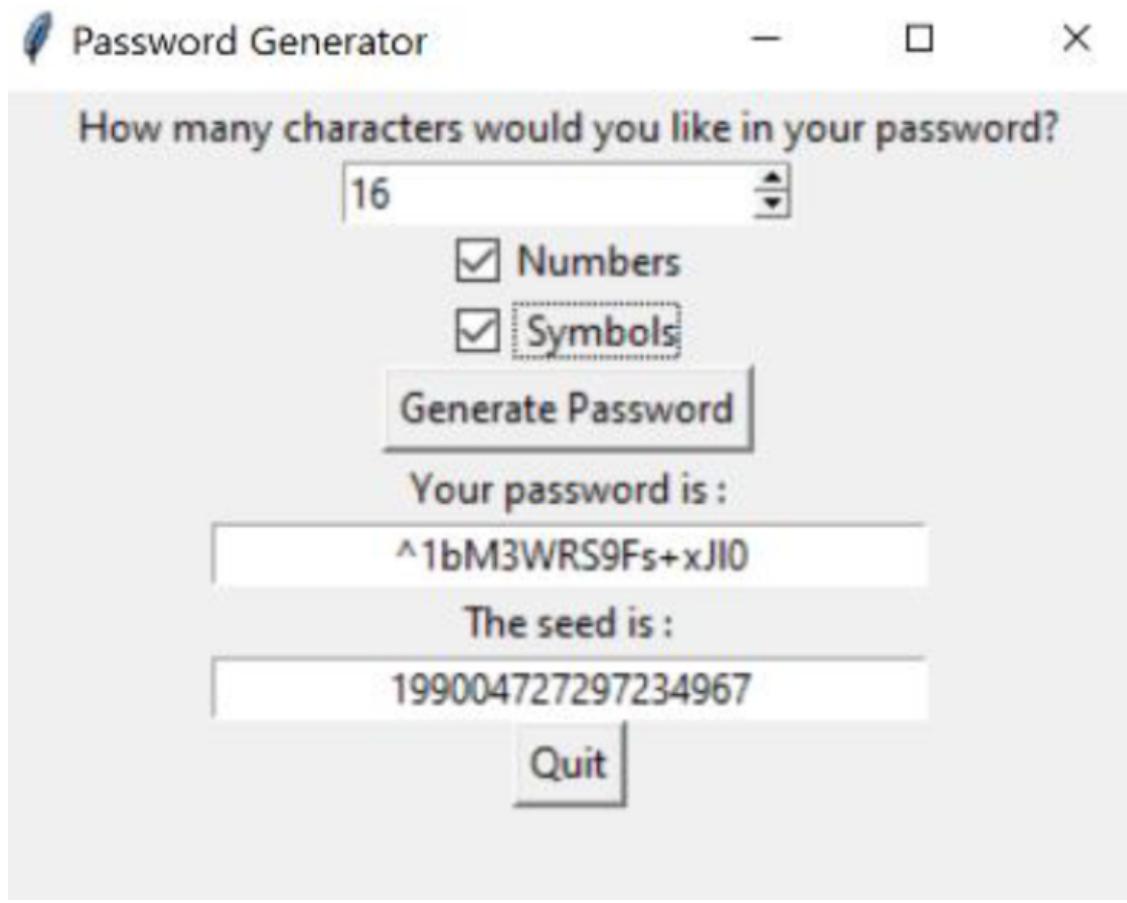
9. Nommez le serveur et faites "continuer" (nous l'appellerons ici "FTP-Entreprise" pour l'exemple)



10. Laissez le domaine vide et continuez

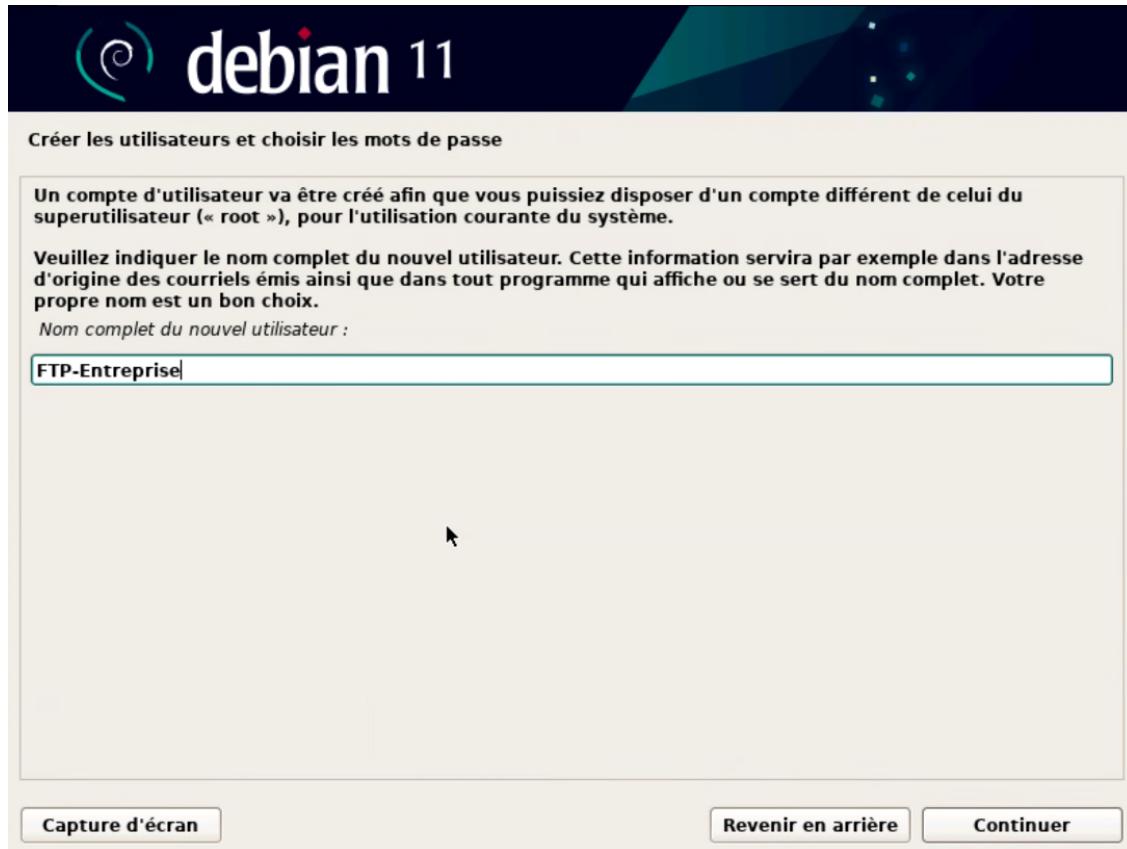


11. Choisissez ensuite un mot de passe sécurisé pour le superuser. J'utiliserais ici un programme Python disponible sur mon [Github](#) pour le générer



12. Confirmez le mot de passe et continuez

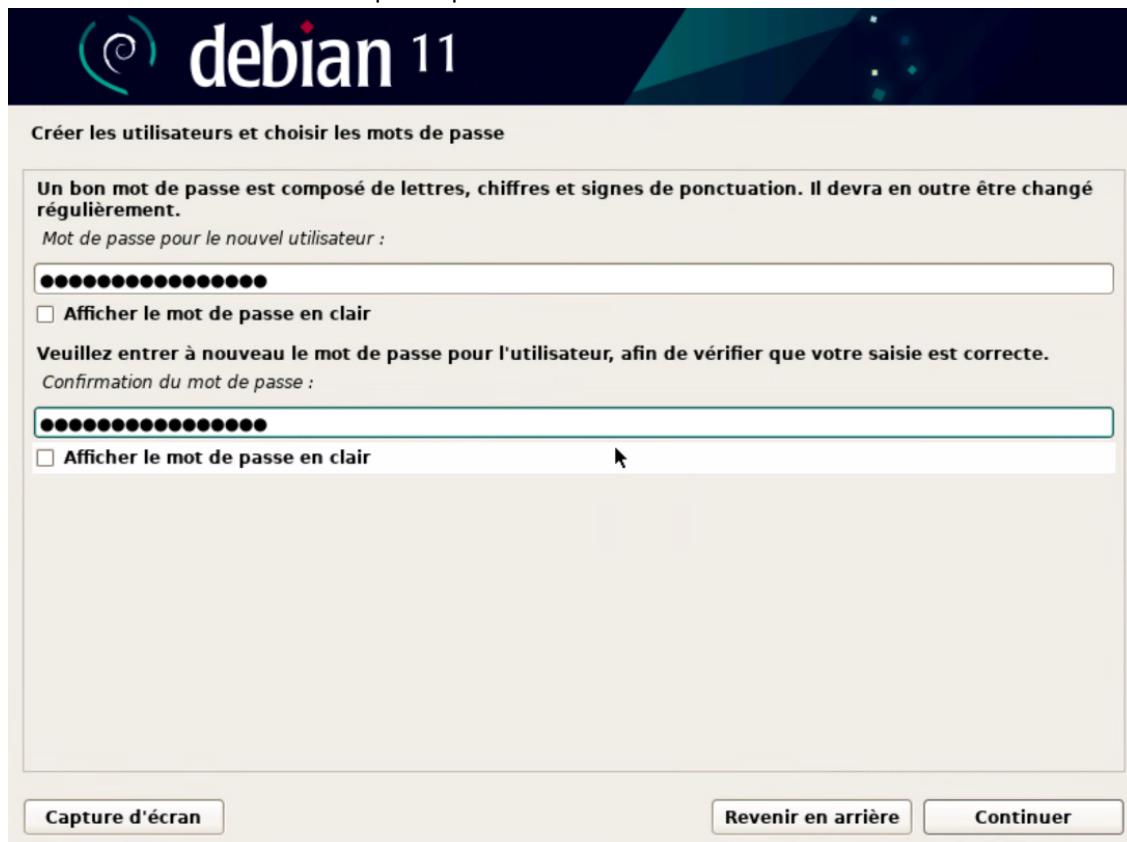
13. Choisissez ensuite un nom d'utilisateur (ici nous garderons le même que le nom de machine soit : "FTP-Entreprise")



14. Nous ferons continuer directement (gardant le même nom pour l'utilisateur) après mais vous pouvez changer ce qui est marqué pour l'identifiant (devenant différent du nom affiché à l'écran)

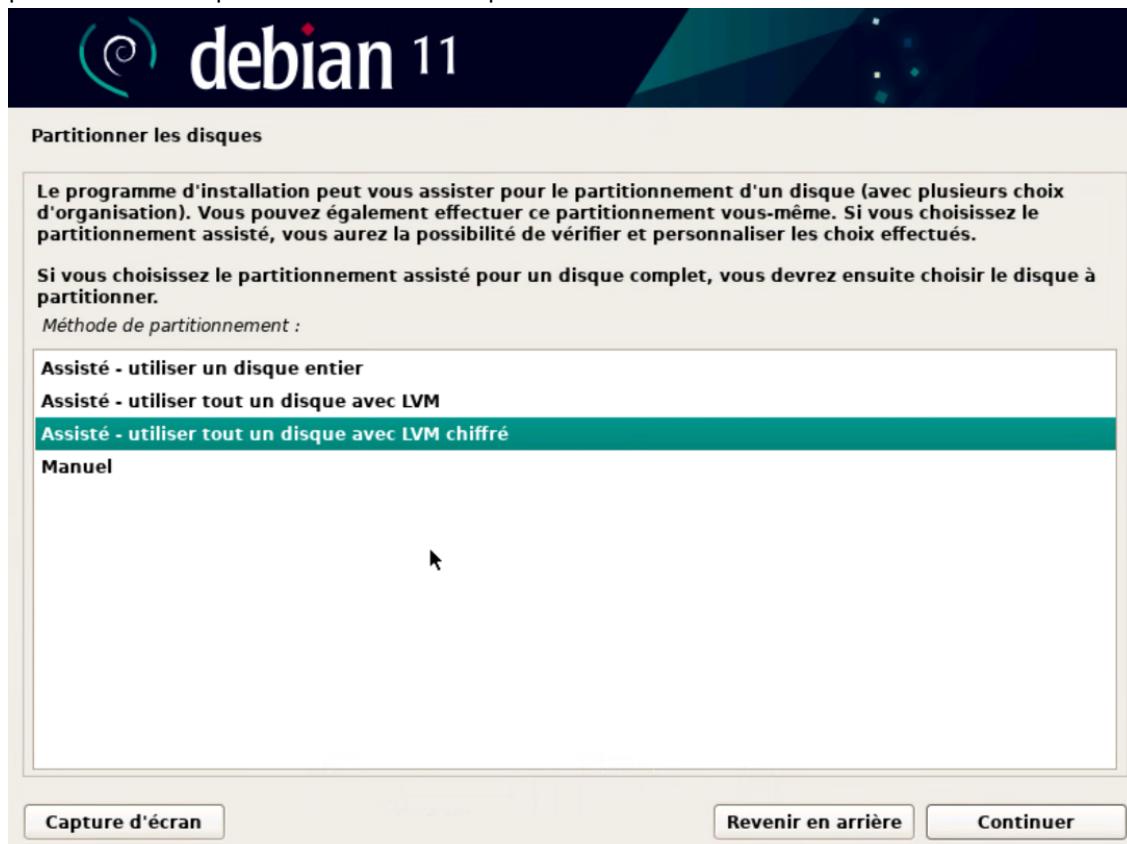


15. Choisissez ensuite un mot de passe pour l'utilisateur.

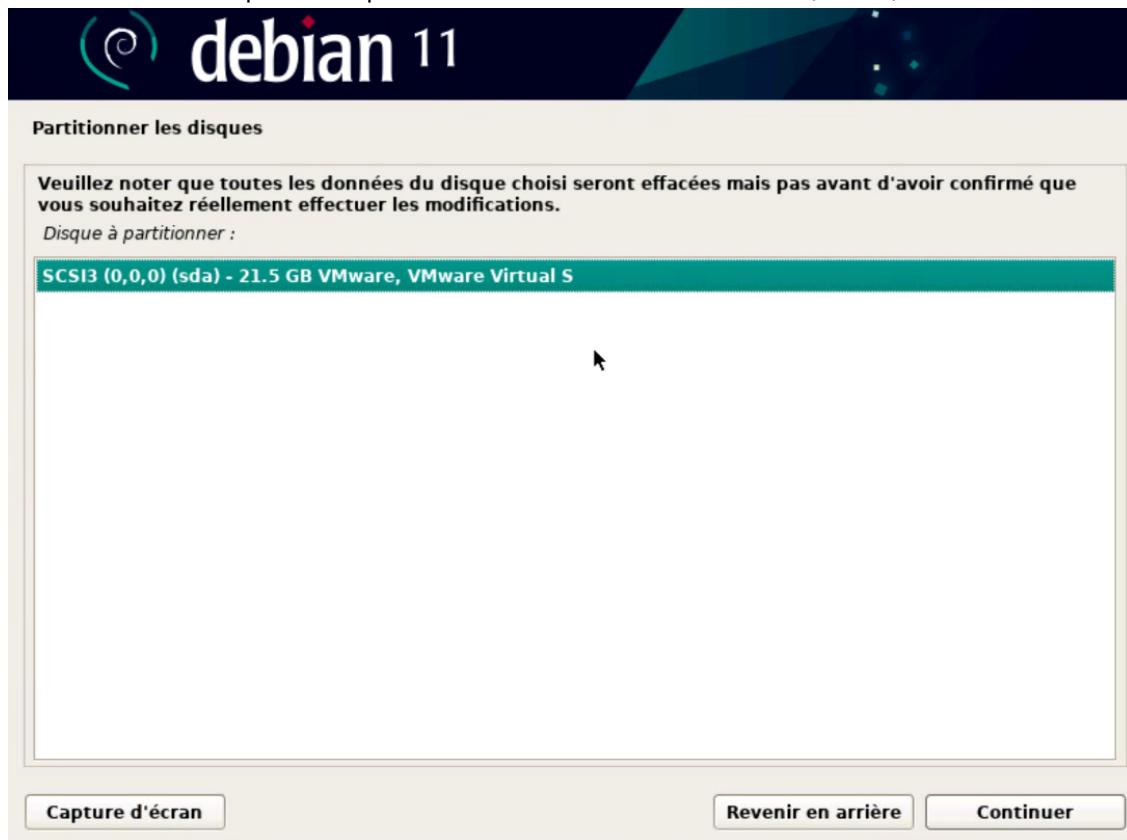


16. Confirmez le mot de passe et continuez

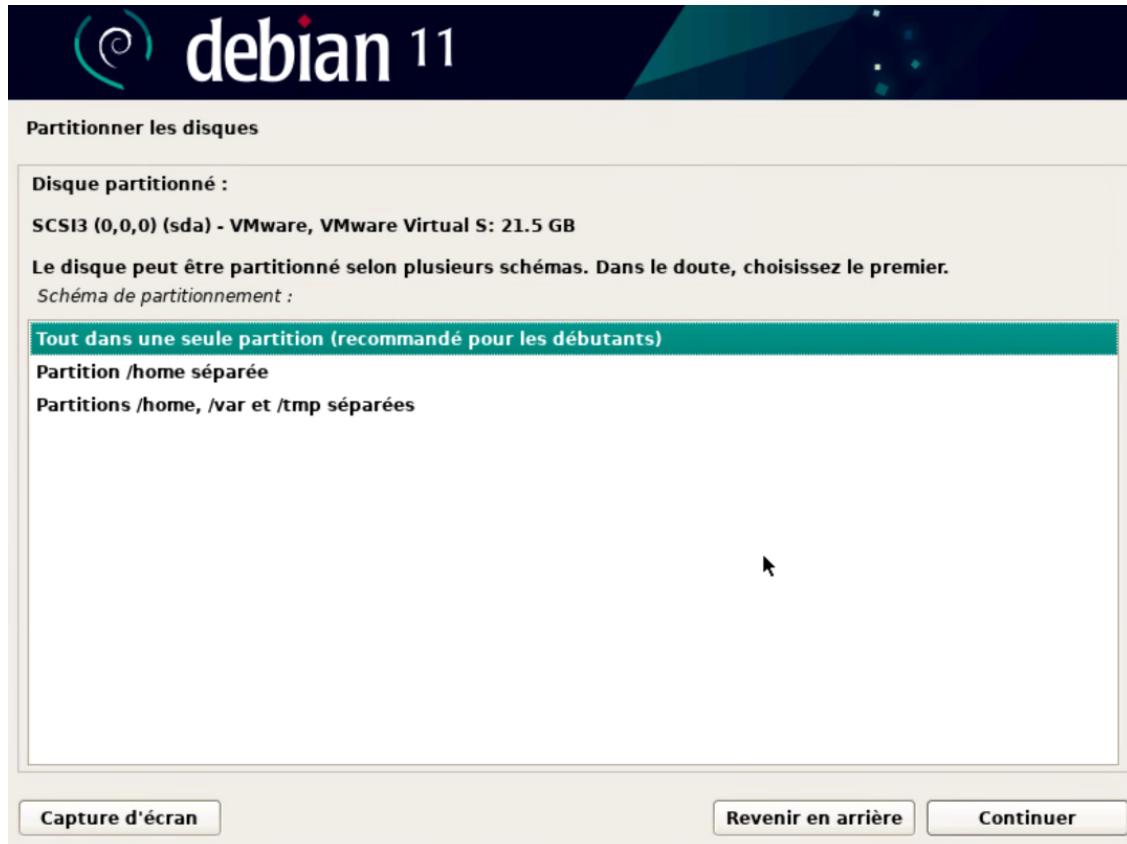
17. Sélectionnez "Assisté – utiliser tout un disque avec LVM chiffré", n'ayant pas besoin de partitionnement particulier mais d'une protection des données



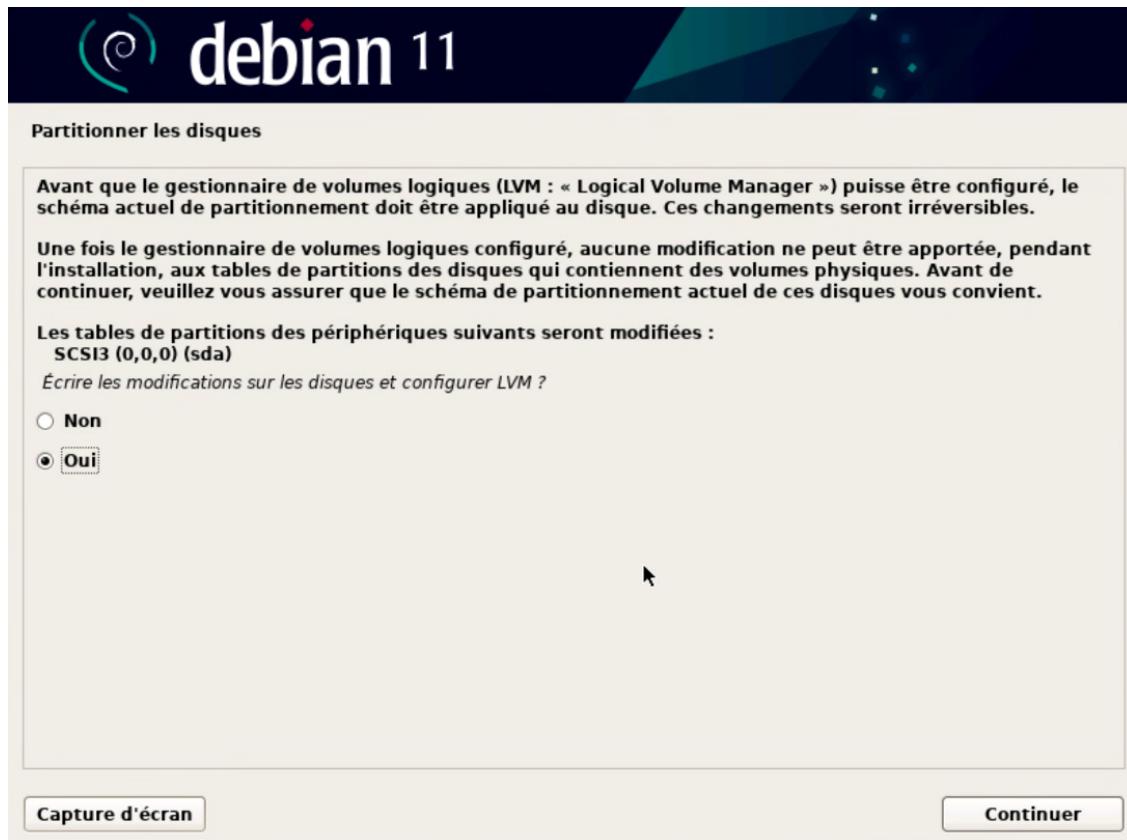
18. Sélectionnez le disque sur lequel vous souhaitez installer Debian (ici sda) et continuez



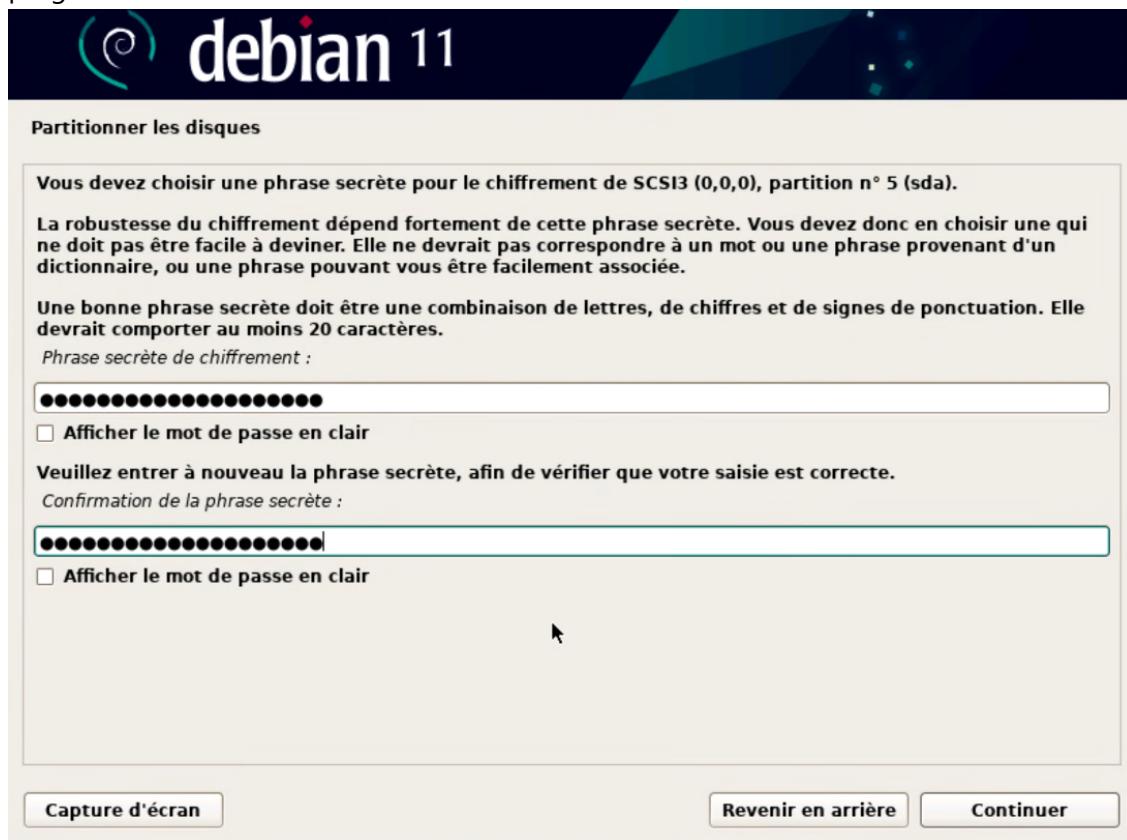
19. Sélectionnez "Tout dans une seule partition" et continuez



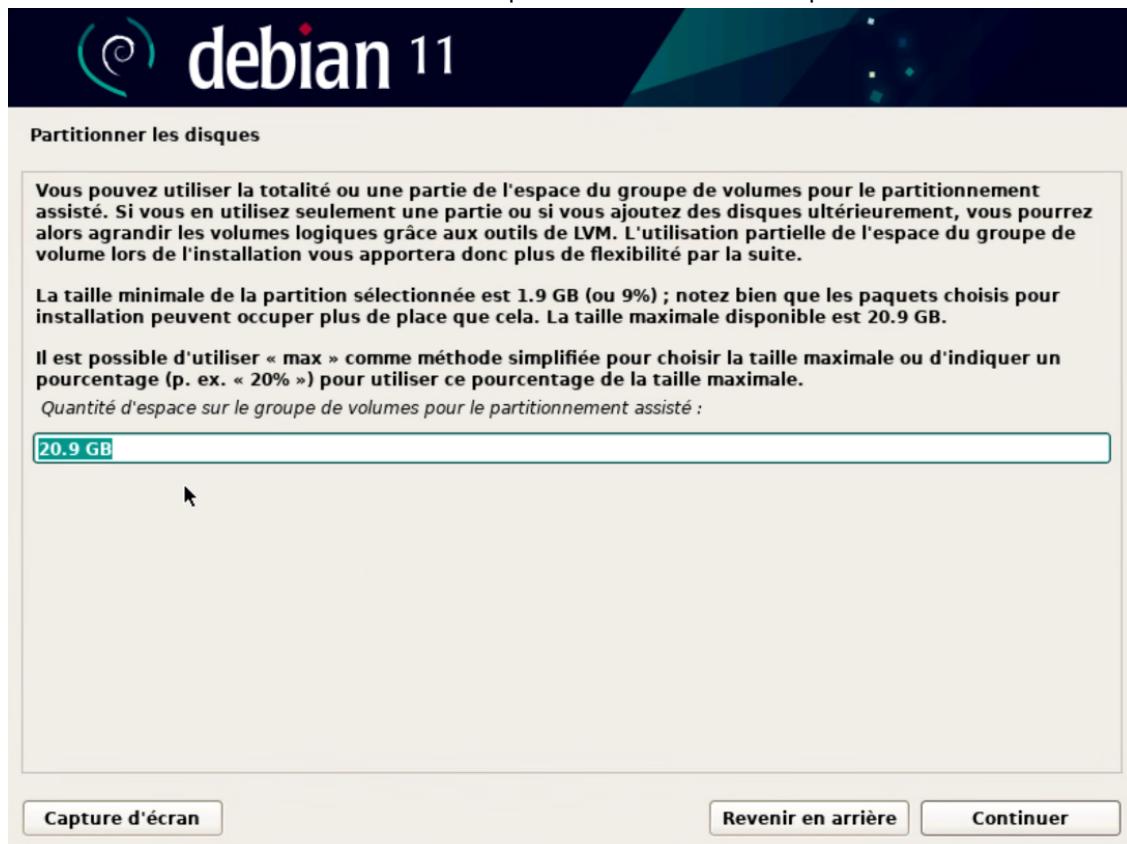
20. Faites les modifications sur le disque en choisissant "Continuer" dans la page suivante et continuez



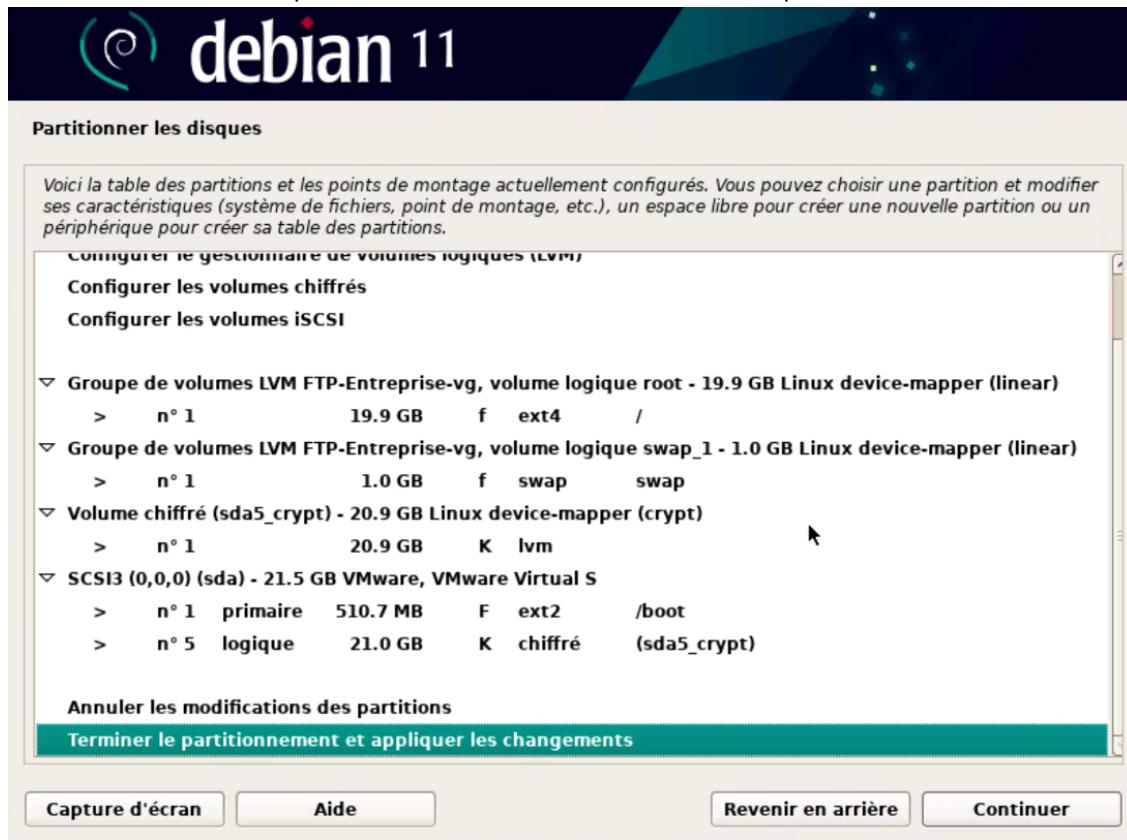
21. Choisissez la phrase de chiffrement pour le disque et continuez, j'utilise ici mon programme une nouvelle fois



22. Il est maintenant demandé la taille de la partition, laissez la taille par défaut et continuez



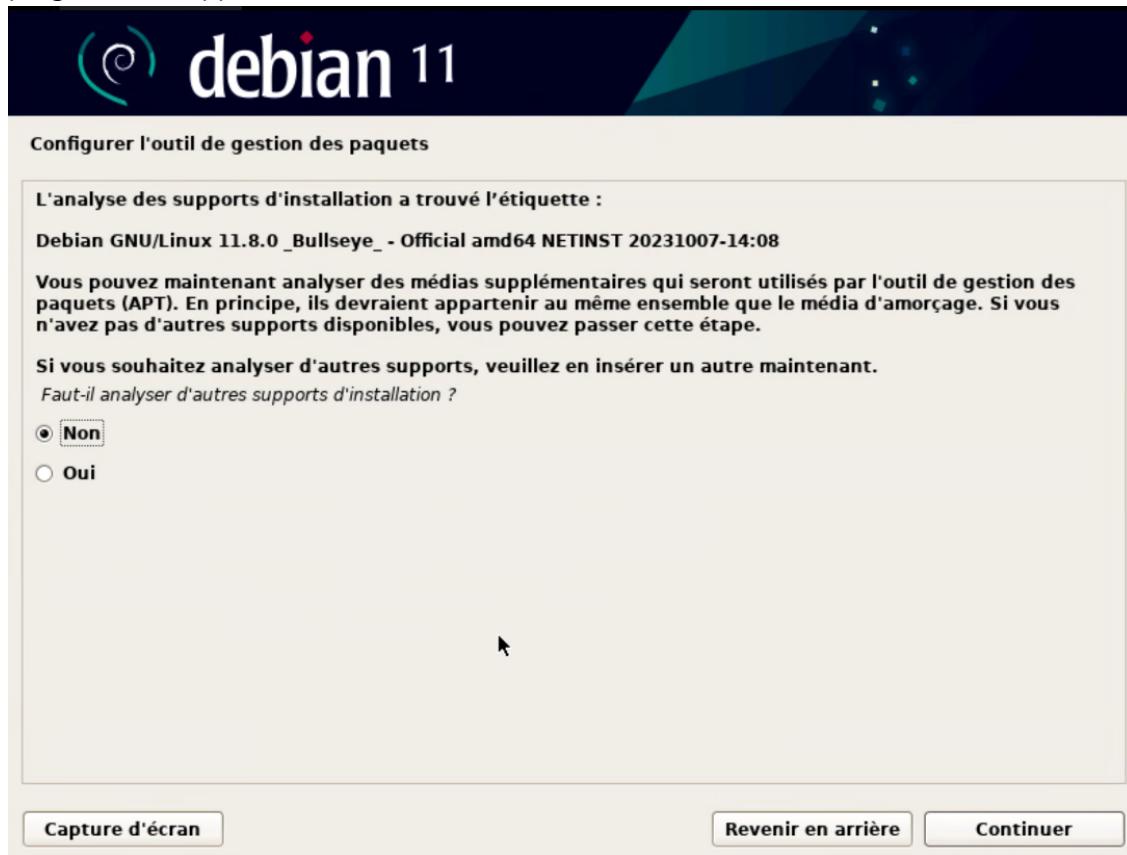
23. Choisissez "Continuer" pour valider les modifications sur le disque



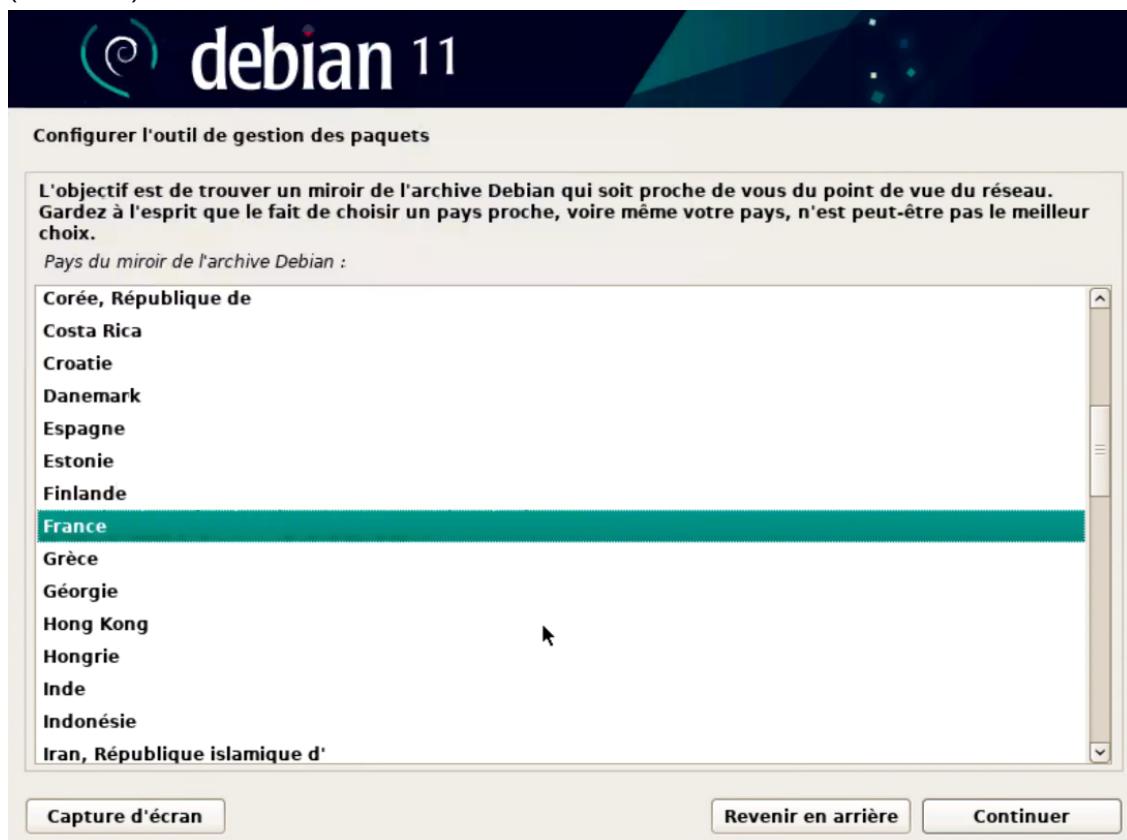
24. Choisissez "Oui" pour confirmer les écritre



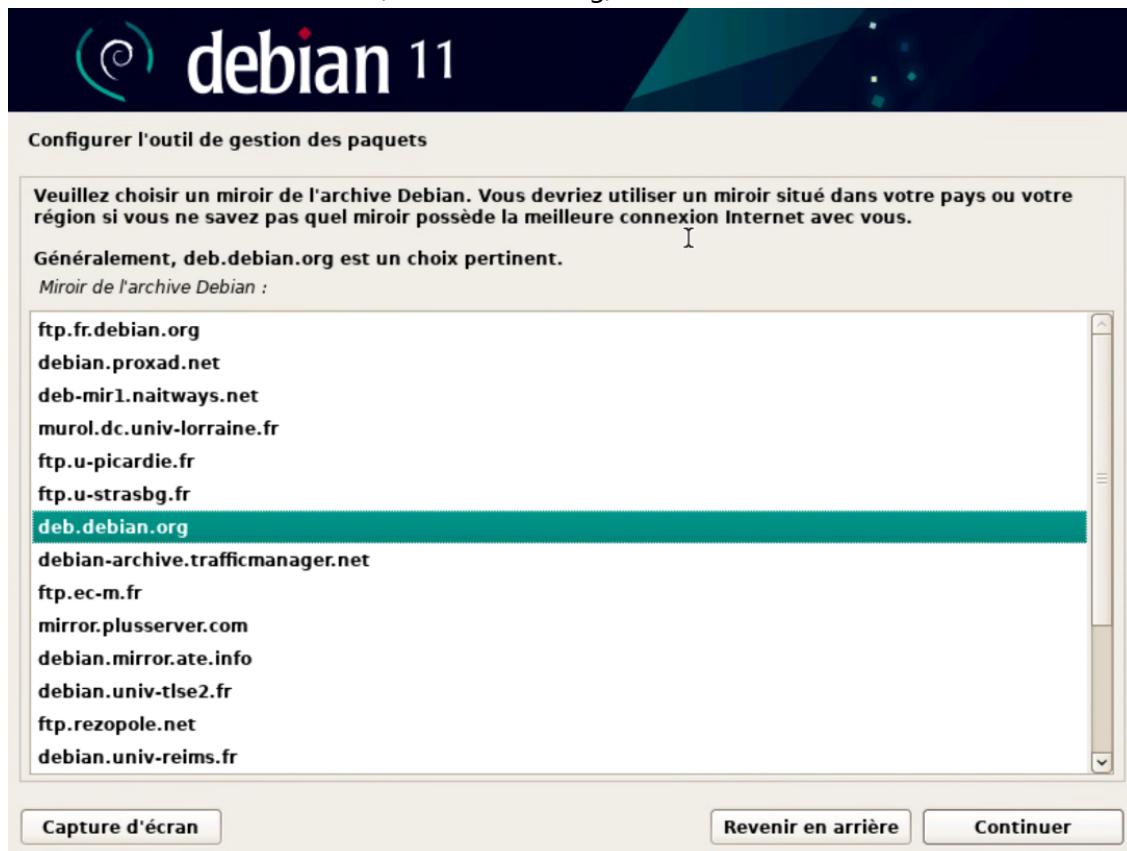
25. Si Debian vous demande si vous avez un autre support d'installation pour installer des programmes supplémentaires, cochez "non" et continuez



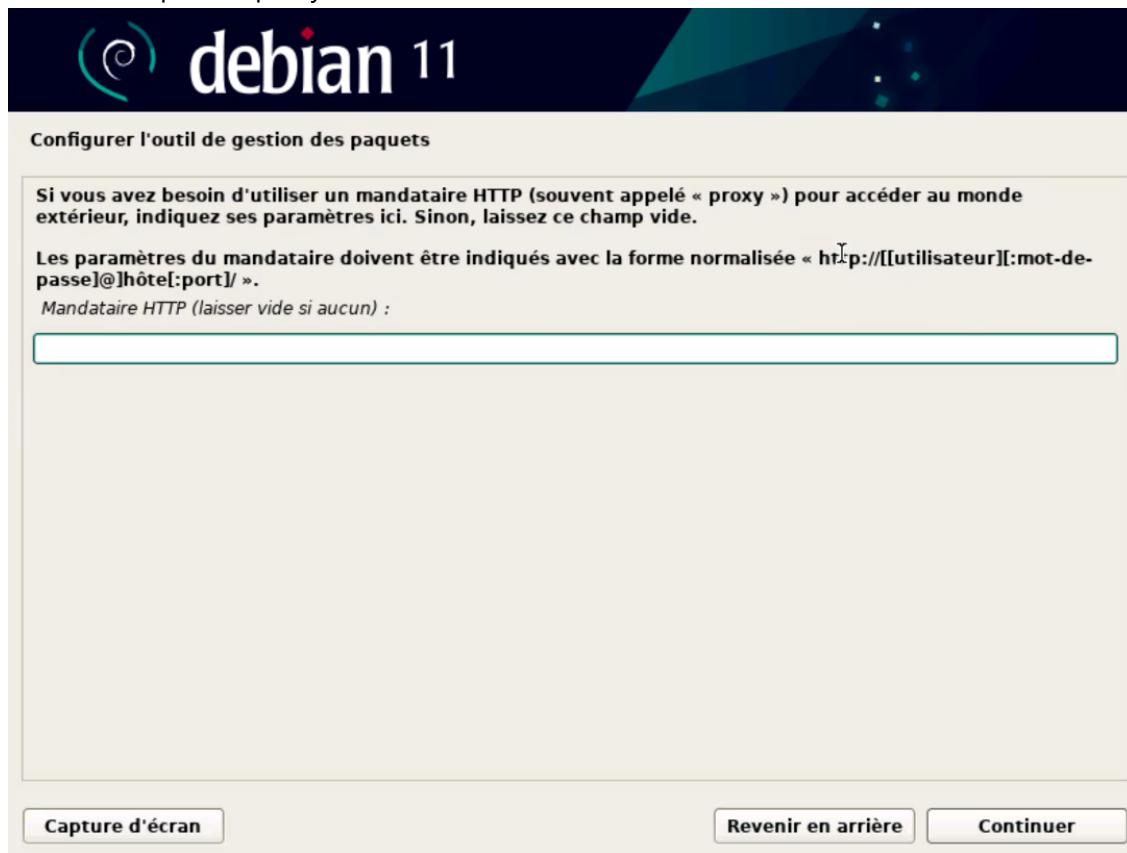
26. Faites continuer en sélectionnant le pays où est votre serveur l'outil de gestion des paquets  
(ici France)



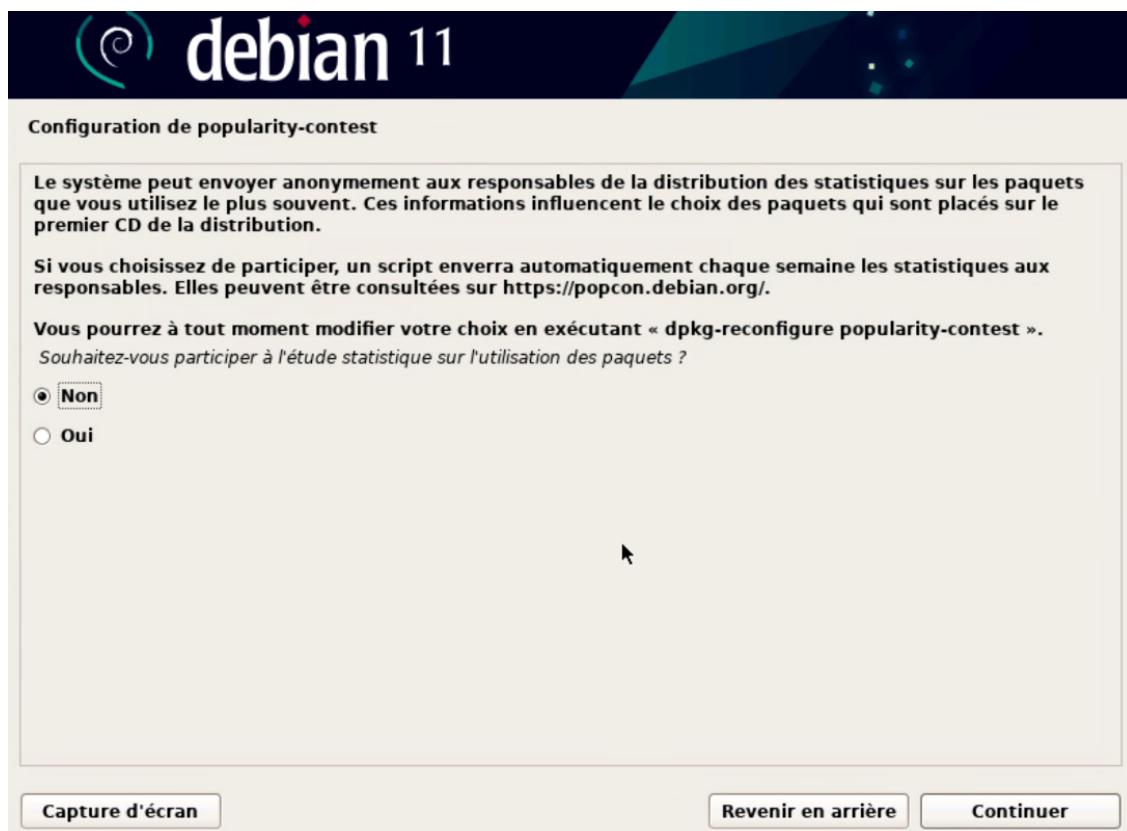
27. Sélectionnez le miroir Debian (ici deb.debian.org) et continuez



28. Laissez vide pour le proxy et continuez

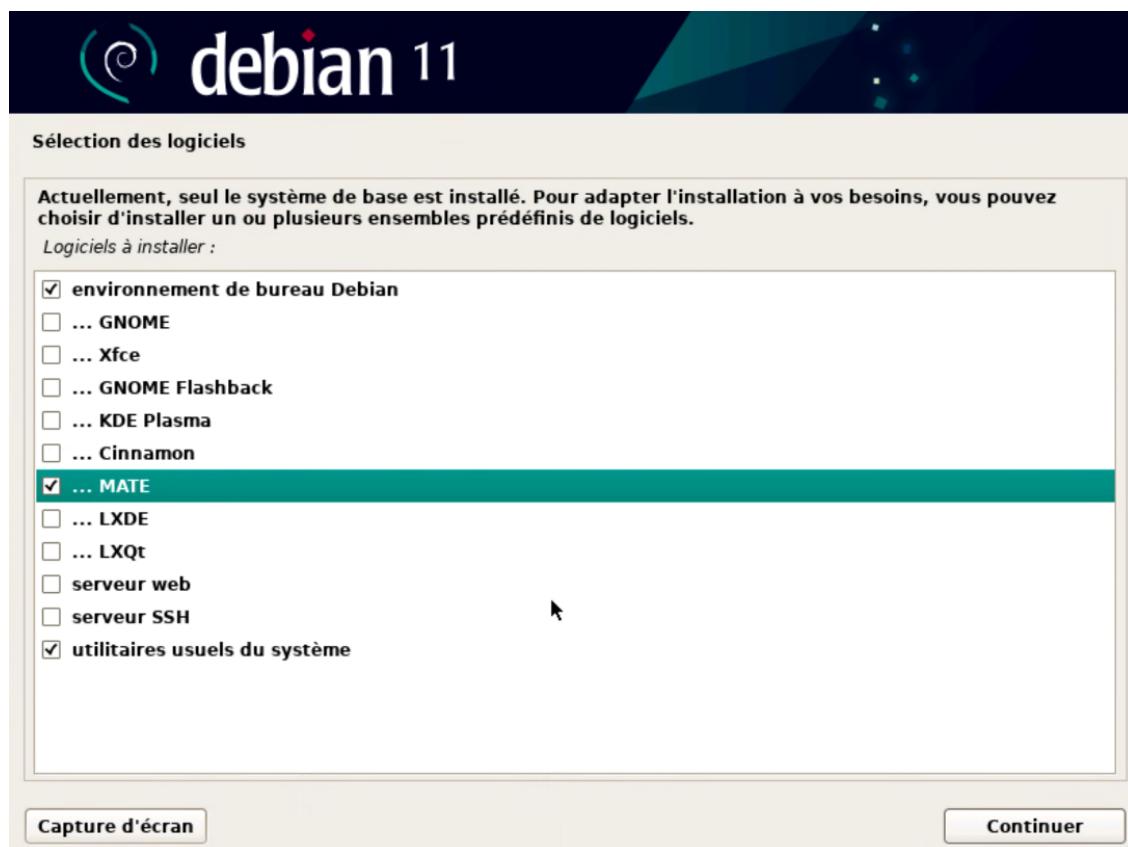


29. Si Debian vous demande si vous souhaitez participer à la "configuration popularity-contest" choisissez "non" et continuez



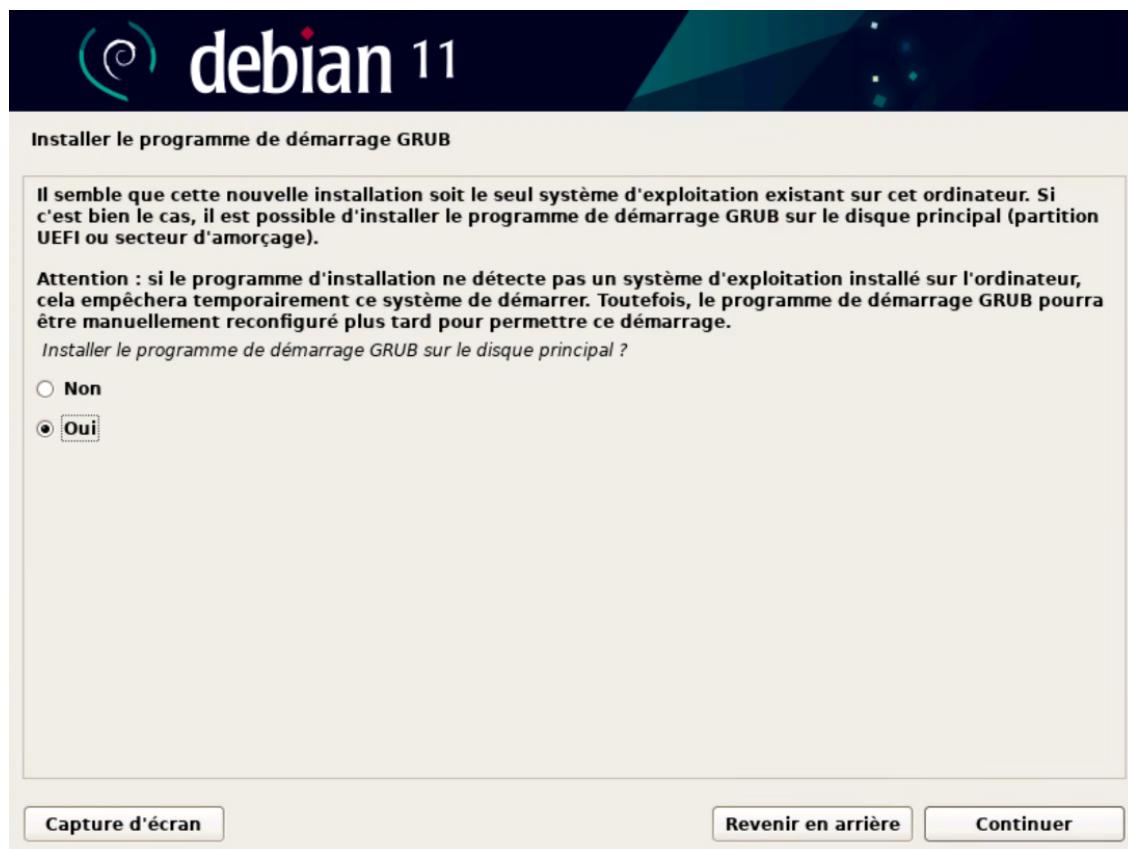
30. Patientez et une fois l'apparition de la "selection des logiciels", sélectionnez "Environnement de bureau Debian", "...MATE" et "utilitaires usuels du système", décochez

le reste.

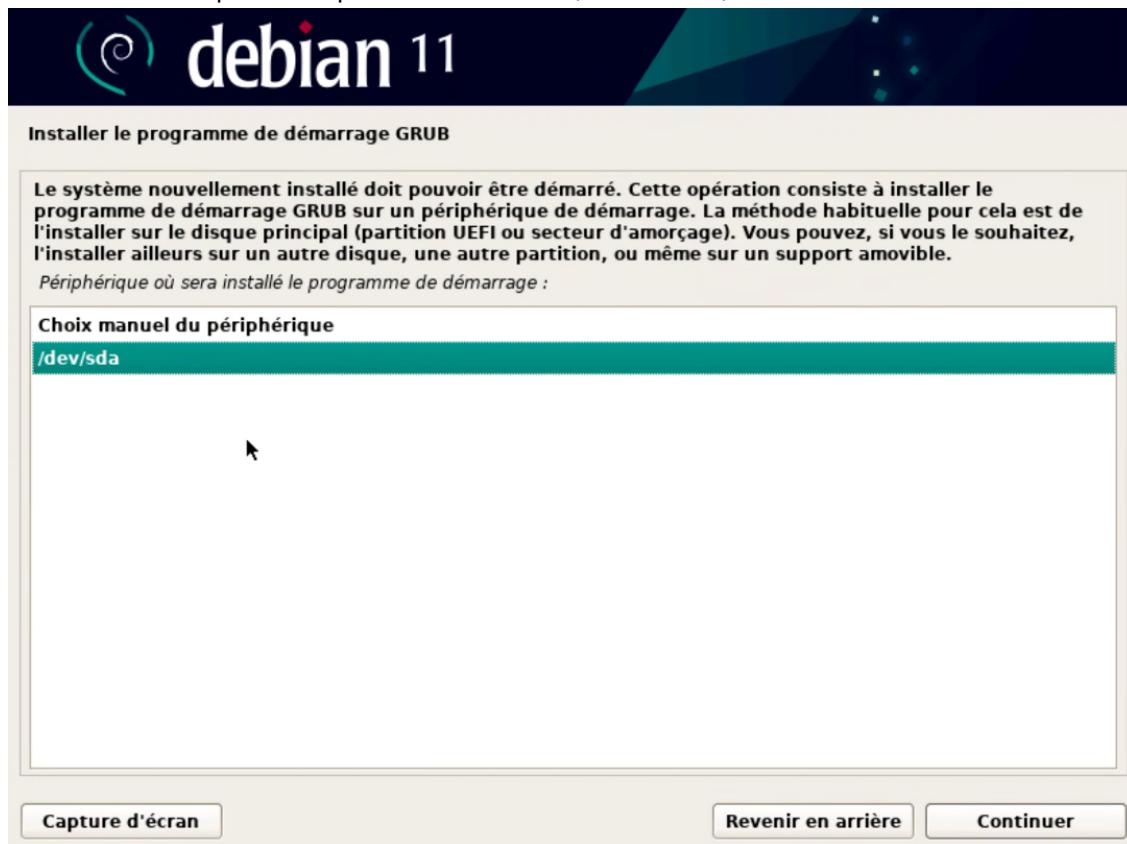


31. Faites continuer et patientez jusqu'à la fin de l'installation

32. Une fois l'installation terminée, sélectionnez "Oui" pour installer le chargeur de démarrage GRUB sur la clé USB



33. Choisissez le disque sur lequel installer GRUB (ici /dev/sda) et continuez



34. Une fois l'installation terminée, faites "Continuer" et retirez la clé USB une fois le serveur redémarré



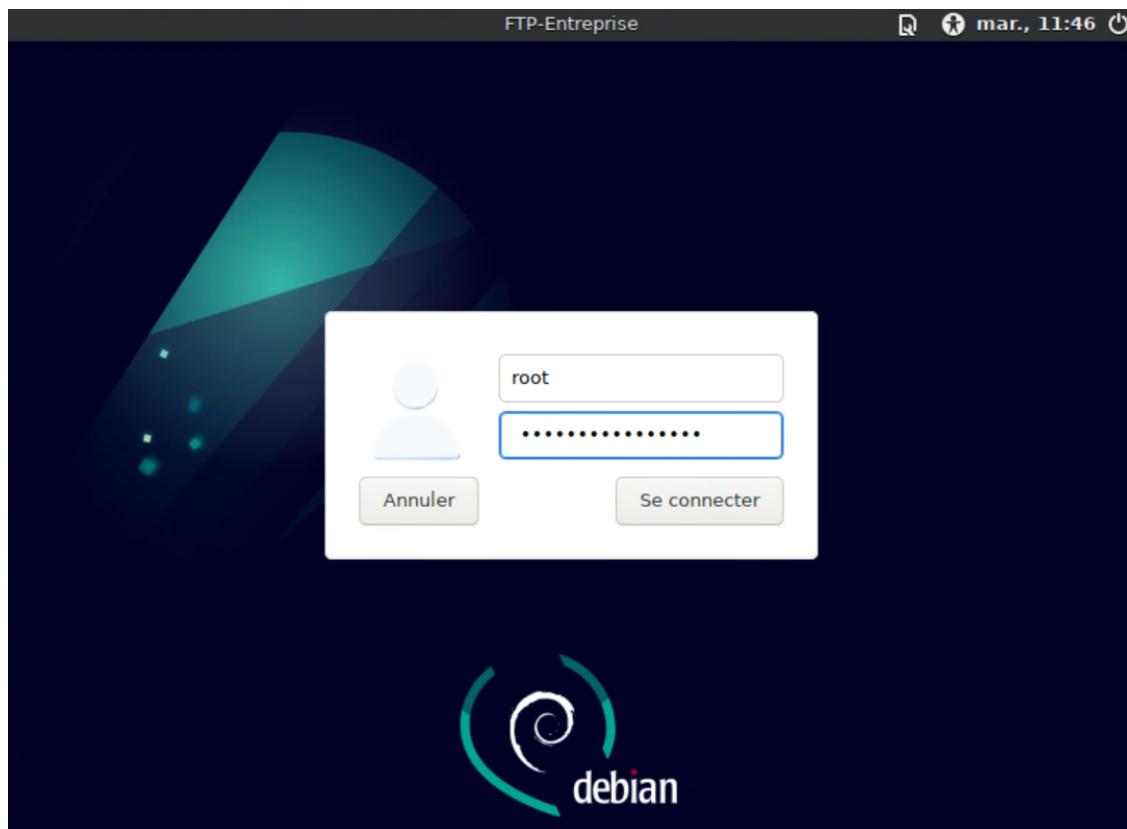
## Installation des applications

1. Démarrez le serveur, vous devriez arriver sur un écran noir avec quelques lignes de texte, entrez la clé de chiffrement que vous avez choisi lors de l'installation

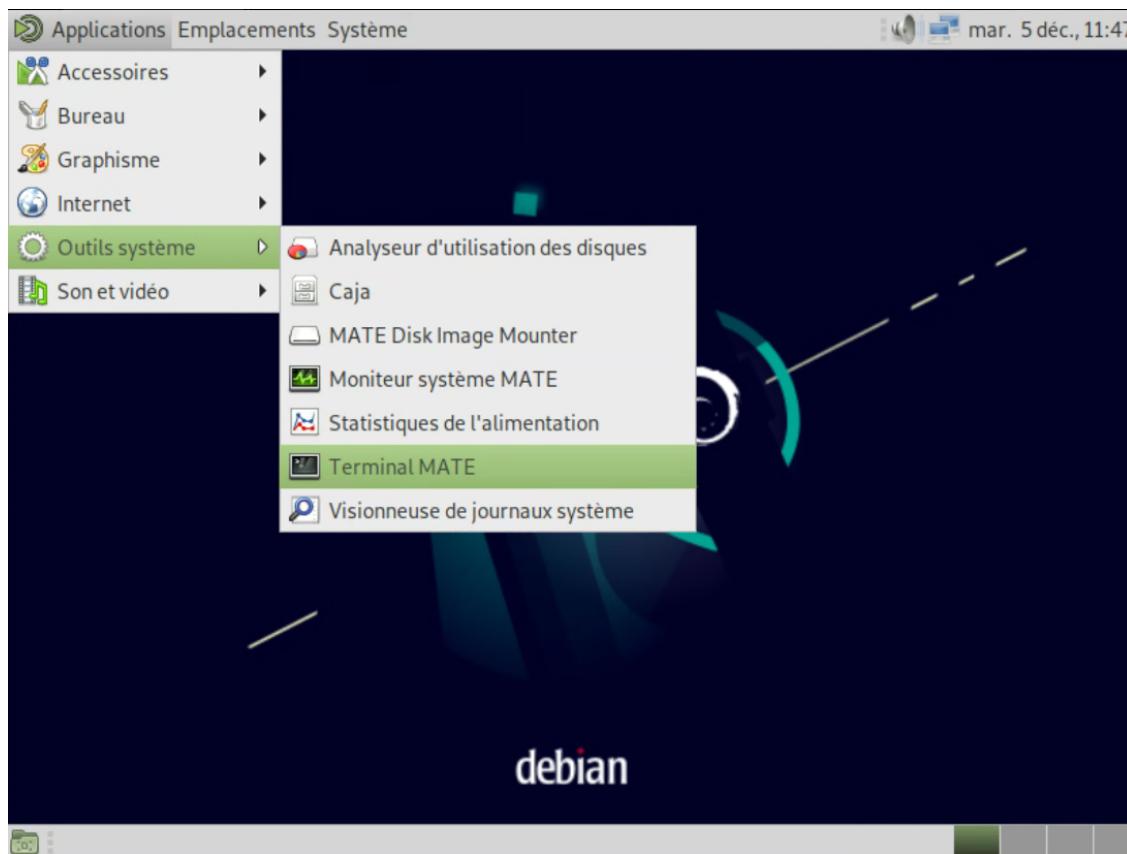
```
[ 1.012624] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
[ 1.626260] sd 2:0:0:0: [sda] Assuming drive cache: write through
Volume group "FTP-Entreprise-vg" not found
Cannot process volume group FTP-Entreprise-vg
Volume group "FTP-Entreprise-vg" not found
Cannot process volume group FTP-Entreprise-vg

Please unlock disk sda5_crypt:_
```

2. Avant de commencer, connectez-vous sur le Debian avec le compte root et le mot de passe que vous avez choisi lors de l'installation



3. Nous allons mettre à jour Debian. Pour cela, ouvrez un terminal (CTRL+T) ou lancez le Terminal MATE



4. Tapez la commande suivante :

```
sudo apt update && sudo apt upgrade -y
```

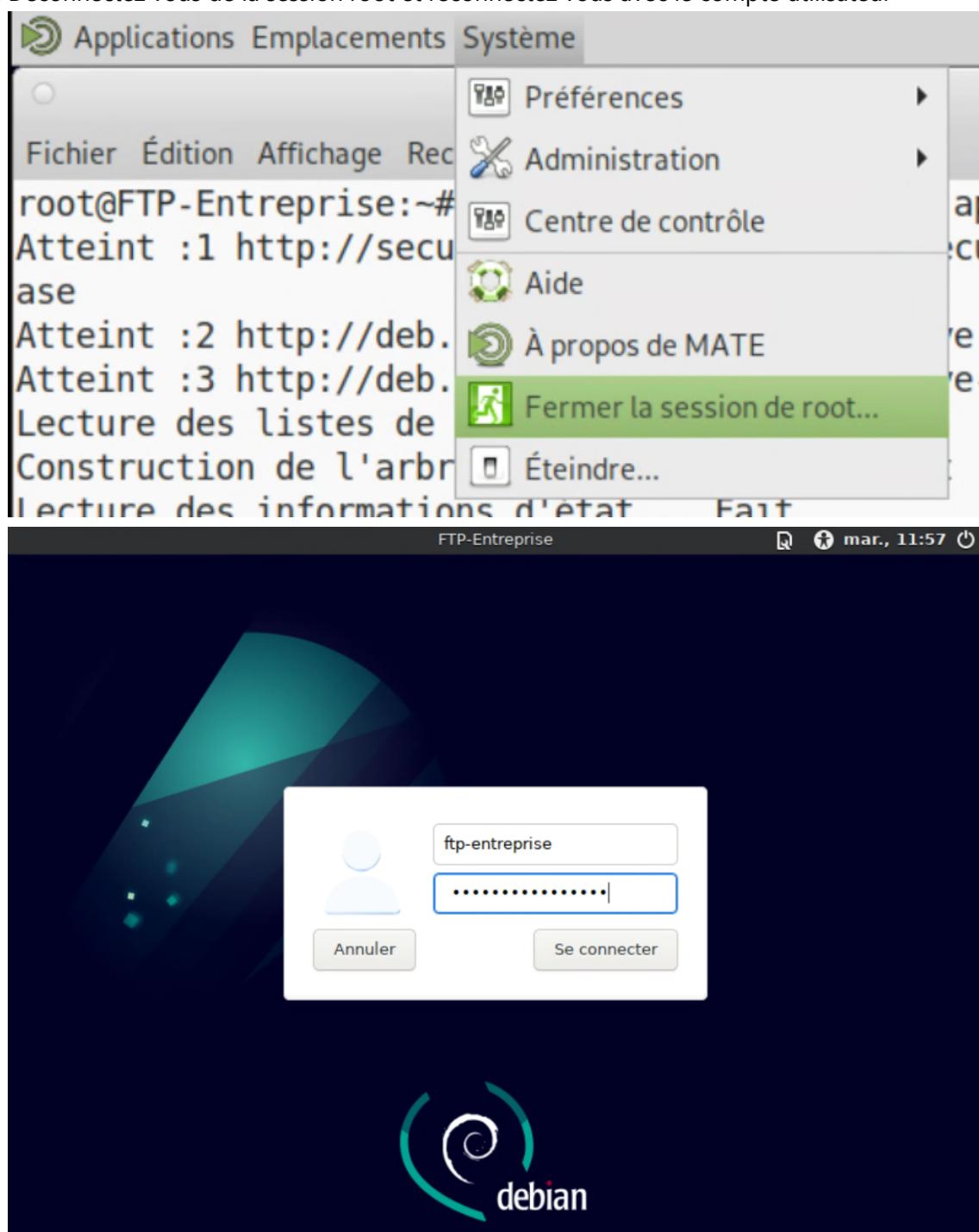
```
Fichier Édition Affichage Recherche Terminal Aide
root@FTP-Entreprise:~# sudo apt update && sudo apt upgrade -y
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@FTP-Entreprise:~#
```

5. Nous allons ensuite ajouter l'utilisateur au groupe sudo. Pour cela, ouvrez un terminal (CTRL+T) et tapez la commande suivante :

```
sudo usermod -aG sudo NOM_DE_L_UTILISATEUR
```

```
root@FTP-Entreprise:~# sudo usermod -aG sudo ftp-entreprise
root@FTP-Entreprise:~#
```

6. Déconnectez vous de la session root et reconnectez vous avec le compte utilisateur



#### Installation SFTP

2. Installez SFTP et démarrez SFTP

```
sudo apt install openssh-server  
sudo systemctl start sshd
```

```
s à jour.
Il est nécessaire de prendre 385 ko dans les archives.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 openssh-server amd64 1:8.4p1-5+deb11u2 [385 kB]
385 ko réceptionnés en 0s (2 121 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 149768 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../openssh-server_1%3a8.4p1-5+deb11u2_amd64.deb ...
Dépaquetage de openssh-server (1:8.4p1-5+deb11u2) sur (1:8.4p1-5+deb11u2) ...
Paramétrage de openssh-server (1:8.4p1-5+deb11u2) ...
rescue-ssh.target is a disabled or a static unit, not starting it.
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour ufw (0.36-7.1) ...
ftp-entreprise@FTP-Entreprise:~$
```

3. Vérifiez que SFTP est bien démarré

```
sudo systemctl status sshd
```

```
ftp-entreprise@FTP-Entreprise:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2023-12-05 15:07:33 CET; 1min 15s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 1708 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1709 (sshd)
     Tasks: 1 (limit: 9429)
    Memory: 1.1M
      CPU: 10ms
     CGroup: /system.slice/ssh.service
             └─1709 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

déc. 05 15:07:33 FTP-Entreprise systemd[1]: Starting OpenBSD Secure Shell server...
déc. 05 15:07:33 FTP-Entreprise sshd[1709]: Server listening on 0.0.0.0 port 22...
déc. 05 15:07:33 FTP-Entreprise sshd[1709]: Server listening on :: port 22.
déc. 05 15:07:33 FTP-Entreprise systemd[1]: Started OpenBSD Secure Shell server.
lines 1-17/17 (END)
```

Notez que pour sortir de la commande status, vous pouvez appuyer sur la touche Q ou CTRL+C

### Configuration SFTP

1. Créez l'utilisateur ou les utilisateurs

```
sudo adduser <username>
```

Donnez les informations demandées

```
ftp-entreprise@FTP-Entreprise:~$ sudo adduser design
Ajout de l'utilisateur « design » ...
Ajout du nouveau groupe « design » (1001) ...
Ajout du nouvel utilisateur « design » (1001) avec le groupe « design » ...
Création du répertoire personnel « /home/design »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for design
Enter the new value, or press ENTER for the default
    Full Name []: Design KNC0
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []
Cette information est-elle correcte ? [0/n]o
ftp-entreprise@FTP-Entreprise:~$
```

2. Installez ufw (un pare-feu logiciel) et ouvrez le port 22 (Port SSH, uniquement en TCP) :

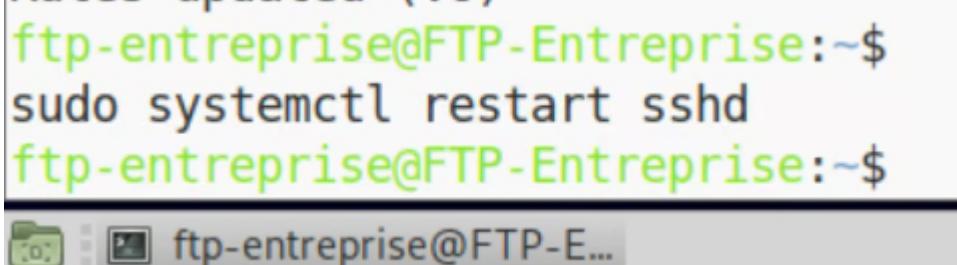
```
sudo apt install ufw
sudo ufw allow 22/tcp
```

The screenshot shows a terminal window titled "ftp-entreprise@FTP-Entreprise: ~". The window contains the following text:

```
Fichier Édition Affichage Recherche Terminal Aide
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ufw
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 167 ko dans les archives.
Après cette opération, 857 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 ufw all 0.36-7.1 [167 kB]
167 ko réceptionnés en 0s (1 364 ko/s)
Préconfiguration des paquets...
Sélection du paquet ufw précédemment désélectionné.
(Lecture de la base de données... 149675 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../archives/ufw_0.36-7.1_all.deb ...
Dépaquetage de ufw (0.36-7.1) ...
Paramétrage de ufw (0.36-7.1) ...
Traitement des actions différées (« triggers ») pour rsyslog (8.2102.0-2+deb11u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Rules updated
Rules updated (v6)
ftp-entreprise@FTP-Entreprise:~$
```

### 3. Redémarrez SFTP

```
sudo systemctl restart sshd
```



```
ftp-enterprise@FTP-Enterprise:~$ sudo systemctl restart sshd
ftp-enterprise@FTP-Enterprise:~$
```

The screenshot shows a terminal window with a black background and white text. The prompt is 'ftp-enterprise@FTP-Enterprise:~\$'. The user types 'sudo systemctl restart sshd' and presses Enter. The terminal then displays the command again followed by a new prompt 'ftp-enterprise@FTP-Enterprise:~\$'. Below the terminal window, there is a small icon bar with a folder icon, a square icon, and the text 'ftp-enterprise@FTP-E...'. The window has a light gray border.

### Installation fail2ban

#### 1. Installez et démarrez Fail2Ban

```
sudo apt install fail2ban
sudo systemctl start fail2ban
```

#### 3. Activez Fail2Ban au démarrage

```
sudo systemctl enable fail2ban
```

```
ftp-entreprise@FTP-Entreprise: ~
Fichier Édition Affichage Recherche Terminal Aide
Dépaquetage de fail2ban (0.11.2-2) ...
Sélection du paquet python3-pyinotify précédemment désélectionné.
Préparation du dépaquetage de .../python3-pyinotify_0.9.6-1.3_all.deb ...
Dépaquetage de python3-pyinotify (0.9.6-1.3) ...
Sélection du paquet python3-systemd précédemment désélectionné.
Préparation du dépaquetage de .../python3-systemd_234-3+b4_amd64.deb ...
Dépaquetage de python3-systemd (234-3+b4) ...
Sélection du paquet whois précédemment désélectionné.
Préparation du dépaquetage de .../whois_5.5.10_amd64.deb ...
Dépaquetage de whois (5.5.10) ...
Paramétrage de whois (5.5.10) ...
Paramétrage de fail2ban (0.11.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service →
 /lib/systemd/system/fail2ban.service.
Paramétrage de python3-pyinotify (0.9.6-1.3) ...
Paramétrage de python3-systemd (234-3+b4) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
ftp-entreprise@FTP-Entreprise:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/sys-
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
ftp-entreprise@FTP-Entreprise:~$
```

4. Vérifiez que Fail2Ban est bien démarré

```
sudo systemctl status fail2ban
```

```
ftp-entreprise@FTP-Entreprise:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
    Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pr>
    Active: active (running) since Tue 2023-12-05 13:55:37 CET; 43s ago
      Docs: man:fail2ban(1)
   Main PID: 80575 (fail2ban-server)
     Tasks: 5 (limit: 9429)
    Memory: 18.3M
       CPU: 106ms
      CGroup: /system.slice/fail2ban.service
              └─80575 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

déc. 05 13:55:37 FTP-Entreprise systemd[1]: Starting Fail2Ban Service...
déc. 05 13:55:37 FTP-Entreprise systemd[1]: Started Fail2Ban Service.
déc. 05 13:55:37 FTP-Entreprise fail2ban-server[80575]: Server ready
lines 1-14/14 (END)
```

Configuration fail2ban

### 1. Créez le fichier de configuration

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

### 2. Ajoutez les lignes suivantes à la fin du fichier

```
[sftp]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
```

The screenshot shows a terminal window titled "ftp-entreprise@FTP-Entreprise: ~". The title bar also displays "Fichier Édition Affichage Recherche Terminal Aide". The menu bar shows "GNU nano 5.4" and the file path "/etc/fail2ban/jail.local \*". The main area of the window contains the configuration code shown above. At the bottom, there is a toolbar with various keyboard shortcuts for file operations like "Aide" (Help), "Quitter" (Exit), "Écrire" (Write), "Lire fich." (Read file), "Chercher" (Search), "Remplacer" (Replace), "Couper" (Cut), "Coller" (Paste), "Exécuter" (Execute), and "Justifier" (Justify). The status bar at the bottom left shows "ftp-entreprise@FTP-E...".

### 3. Redémarrez Fail2Ban

```
sudo systemctl restart fail2ban
```

```
ftp-entreprise@FTP-Entreprise:~$ sudo systemctl restart fail2ban
ftp-entreprise@FTP-Entreprise:~$
```

## Sécurité

L'utilisation d'ufw et de fail2ban permet de sécuriser le serveur contre les attaques de type brute-force et de bloquer les ports non utilisés

Les connexions sont aussi limitées aux utilisateurs inscrits dans le serveur et sont donc sécurisé à la hauteur de la sécurité du mot de passe de l'utilisateur

On peut également noter que de par sa nature, le sftp ouvre la possibilité de se connecter au serveur avec un client SSH comme Putty pour un accès à distance au sein du réseau local

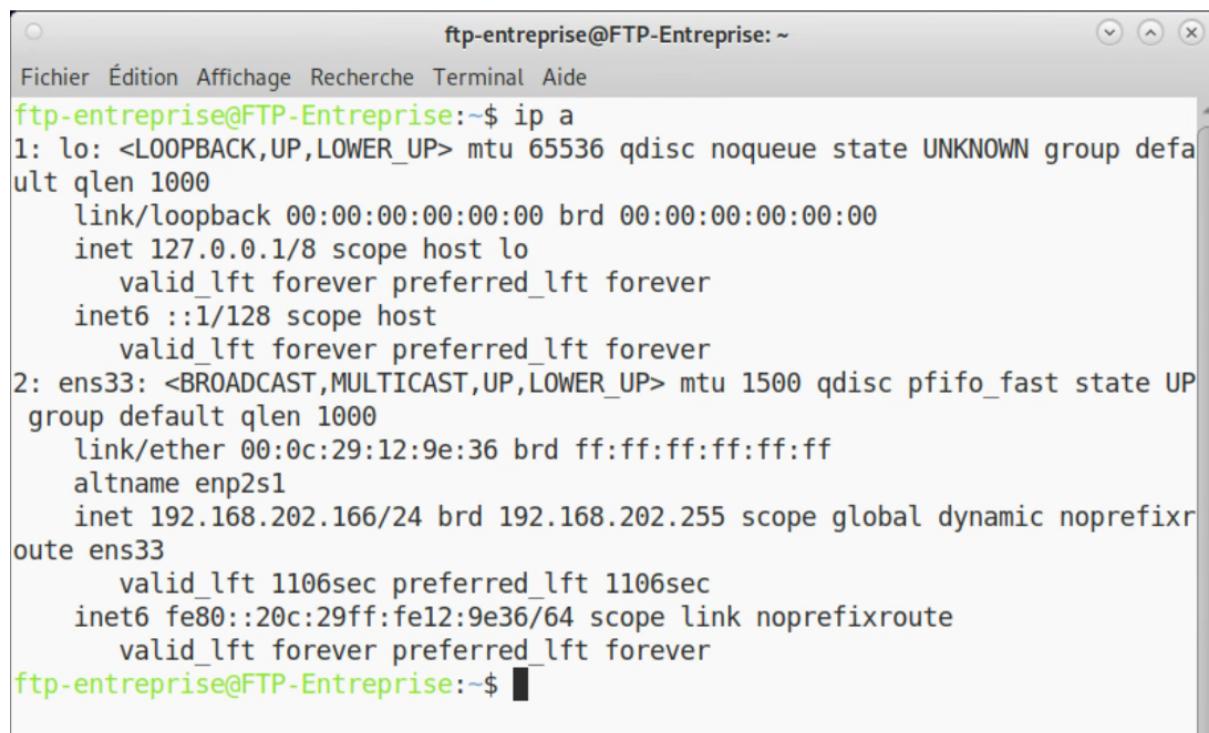
Il est aussi important de noter que le serveur n'est normalement pas accessible en dehors du réseau local, ce qui limite les risques d'attaques extérieures

## Utilisation

Pour utiliser le serveur, il vous suffit de vous connecter avec un client FTP (FileZilla, WinSCP, etc...) avec l'adresse IP du serveur, le nom d'utilisateur et le mot de passe de l'utilisateur

Pour savoir quelle est l'adresse IP du serveur, vous pouvez utiliser la commande suivante :

```
ip a
```



```
ftp-entreprise@FTP-Entreprise: ~
Fichier Édition Affichage Recherche Terminal Aide
ftp-entreprise@FTP-Entreprise:$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:12:9e:36 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.202.166/24 brd 192.168.202.255 scope global dynamic noprefixroute ens33
        valid_lft 1106sec preferred_lft 1106sec
    inet6 fe80::20c:29ff:fe12:9e36/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ftp-entreprise@FTP-Entreprise:$
```

Notez que l'adresse IP ici est 192.168.202.166

Nous allons ici prendre l'exemple de FileZilla

1. Ouvrez FileZilla
2. Entrez l'adresse IP du serveur dans "Hôte"
3. Entrez le nom d'utilisateur dans "Identifiant"
4. Entrez le mot de passe dans "Mot de passe"

5. Entrez le port 22 dans "Port"
6. Cliquez sur "Connexion rapide"
7. Acceptez le certificat

