

Mise en place Clé de support (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 RustDesk Server](#)
 - [Installation Debian](#)
 - [Création de la VM](#)
 - [Installation de Debian](#)
 - [Installation des applications](#)
 - [Installation de Tailscale](#)
 - [Configuration de Tailscale](#)
 - [Installation de RustDesk](#)
 - [Configuration de RustDesk](#)
 - [Installation de Chntpw](#)
 - [Installation de Gparted](#)
 - [Installation de memtest86+](#)
 - [Installation de BleachBit](#)
 - [Configuration de BleachBit](#)
- [Utilisation](#)

Pour Commencer

Nous avons dans l'entreprise KNCO, eu beaucoup de cas de mots de passes oubliés et avons déjà rencontré des problèmes de mémoire RAM défaillantes

C'est pour à l'avenir avoir un outil plus efficace et rapide que de récupérer l'ordinateur pour tester sa RAM dans le bureau IT ou de devoir récupérer le disque dur/SSD du poste qu'il a été décidé de créer deux clés de support externe

Le besoin est donc de pouvoir réinitialiser les mots de passes locaux et de tester la mémoire RAM. Mais nous devons également prévoir de l'installation d'autres outils sur la clé, que ce soit à distance pour régler un problème non prévu ou sur nos machines pour rajouter des solutions à de nouveaux problèmes

Nous partons 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

Nous n'avons pas à nous soucier d'une AD, car l'entreprise n'a pas de Domaine, la raison avancée étant que 90% des employés sont des représentants marketing dont le travail est de se déplacer d'opticiens en opticiens pour passer des commandes de branches de lunettes

Nous le ferons à l'aide d'un ordinateur annexe sous Windows, et de VMware Workstation 17, mais nous pourrions commencer avec un ordinateur sous Linux, et un autre outil de virtualisation permettant d'utiliser une clé USB comme volume pour les machines virtuelles
L'utilisation d'une machine virtuelle permet d'éviter le formatage non voulu d'un disque mais aussi de télécharger un pilote graphique et d'écran générique lors de l'installation, évitant des incompatibilités rares mais existante
Nous utilisons également une machine virtuelle pour des raisons de simplicité lorsqu'il est question de faire des mise à jour, de tests ou d'ajouter des fonctionnalités sur la clé

Prérequis

- [VmWare Workstation](#) pré-installé
- Clé/Stockage USB de 8Go minimum
- ISO de [Debian 11](#)
- Serveur Debian 11 pré-installé (Serveur RustDesk)

Installation RustDesk Server

1. Il faut tout d'abord installer et configurer ufw sur le serveur, pour cela, ouvrez un terminal (CTRL+T) et tapez les commandes suivantes :

```
sudo apt install ufw
sudo ufw allow 21115:21119/tcp
sudo ufw allow 8000/tcp
sudo ufw allow 21116/udp
sudo ufw enable
```

```
root@FTP-Entreprise:~#
sudo apt install ufw
sudo ufw allow 21115:21119/tcp
sudo ufw allow 8000/tcp
sudo ufw allow 21116/udp
sudo ufw enable
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ufw est déjà la version la plus récente (0.36-7.1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 6 non mis à jour.
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Firewall is active and enabled on system startup
root@FTP-Entreprise:~#
```

2. Installez le serveur RustDesk avec les commandes suivante :

```
wget https://raw.githubusercontent.com/techahold/rustdeskinstall/master/install.sh
chmod +x install.sh
./install.sh
```

The screenshot shows a terminal window titled "Terminal". The window contains the following text output from a shell script:

```
0 mis à jour, 2 nouvellement installés, 0 à enlever et 6 non mis à jour.
Il est nécessaire de prendre 540 ko dans les archives.
Après cette opération, 721 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 dnsutils all
1:9.16.44-1~deb11u1 [269 kB]
Réception de :2 http://security.debian.org/debian-security bullseye-security/main amd64 curl amd64 7.74.0-1.3+deb11u10 [271 kB]
540 ko réceptionnés en 0s (3 507 ko/s)
Sélection du paquet curl précédemment désélectionné.
(Lecture de la base de données... 192701 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../curl_7.74.0-1.3+deb11u10_amd64.deb ...
Dépaquetage de curl (7.74.0-1.3+deb11u10) ...
Sélection du paquet dnsutils précédemment désélectionné.
Préparation du dépaquetage de .../dnsutils_1%3a9.16.44-1~deb11u1_all.deb ...
Dépaquetage de dnsutils (1:9.16.44-1~deb11u1) ...
Paramétrage de dnsutils (1:9.16.44-1~deb11u1) ...
Paramétrage de curl (7.74.0-1.3+deb11u10) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
1) IP
2) DNS/Domain
Choose your preferred option, IP or DNS/Domain: 1
```

3. Il va être demandé quelques informations, la première est la préférence entre la connexion par IP ou par Domaine, nous choisirons ici l'IP (1)

```

Terminal
Fichier Édition Affichage Recherche Terminal Aide
Taille : 8517854 (8,1M) [application/octet-stream]
Sauvegarde en : « rustdesk-server-linux-amd64.zip »

rustdesk-server-lin 100%[=====] 8,12M 6,33MB/s ds 1,3s

2023-12-05 16:08:57 (6,33 MB/s) – « rustdesk-server-linux-amd64.zip » sauvegarde [8517854/8517854]

Archive: rustdesk-server-linux-amd64.zip
  inflating: amd64/hbbr
  inflating: amd64/hbbs
  inflating: amd64/rustdesk-utils
Creating /var/log/rustdesk
Created symlink /etc/systemd/system/multi-user.target.wants/rustdesksignal.service → /etc/systemd/system/rustdesksignal.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rustdeskrelay.service → /etc/systemd/system/rustdeskrelay.service.
Rustdesk Relay not ready yet...
Tidying up install
1) Yes
2) No
Please choose if you want to download configs and install HTTP server:

```

4. Il va ensuite être demandé si nous souhaitons installer un serveur HTTP pour récupérer les fichiers de configuration, nous choisirons ici "Non" (2)

```

Terminal
Fichier Édition Affichage Recherche Terminal Aide
dé [8517854/8517854]

Archive: rustdesk-server-linux-amd64.zip
  inflating: amd64/hbbr
  inflating: amd64/hbbs
  inflating: amd64/rustdesk-utils
Creating /var/log/rustdesk
Created symlink /etc/systemd/system/multi-user.target.wants/rustdesksignal.service → /etc/systemd/system/rustdesksignal.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rustdeskrelay.service → /etc/systemd/system/rustdeskrelay.service.
Rustdesk Relay not ready yet...
Tidying up install
1) Yes
2) No
Please choose if you want to download configs and install HTTP server:2
Your IP/DNS Address is
Your public key is NFHdVcoN48oIMKS2DVwUtvfMan1EfbZ3rMToI8IpNmc=
Install Rustdesk on your machines and change your public key and IP/DNS name to the above
Press any key to finish install

```

5. Copiez la clé publique, nous en aurons besoin plus tard

Your public key is NFHdVcoN48oIMKS2DVwUtvfMan1EfbZ3rMToI8IpNmc=

6. Installez ensuite Tailscale avec les commandes suivantes :

```
sudo apt install curl
curl -fsSL https://tailscale.com/install.sh | sh
```

```
support@Support: ~
Fichier Édition Affichage Recherche Terminal Aide
Après cette opération, 47,9 Mo d'espace disque supplémentaires seront utilisés.
Réception de :2 https://pkgs.tailscale.com/stable/debian bullseye/main all tails
cale-archive-keyring all 1.35.181 [3 082 B]
Réception de :1 https://pkgs.tailscale.com/stable/debian bullseye/main amd64 tai
lscalc amd64 1.54.1 [25,8 MB]
25,8 Mo réceptionnés en 4s (5 744 ko/s)
Sélection du paquet tailscale précédemment désélectionné.
(Lecture de la base de données... 148954 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../tailscale_1.54.1_amd64.deb ...
Dépaquetage de tailscale (1.54.1) ...
Sélection du paquet tailscale-archive-keyring précédemment désélectionné.
Préparation du dépaquetage de .../tailscale-archive-keyring_1.35.181_all.deb ...
Dépaquetage de tailscale-archive-keyring (1.35.181) ...
Paramétrage de tailscale-archive-keyring (1.35.181) ...
Paramétrage de tailscale (1.54.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/tailscaled.service →
 /lib/systemd/system/tailscaled.service.
+ [ false = true ]
+ set +x
Installation complete! Log in to start using Tailscale by running:

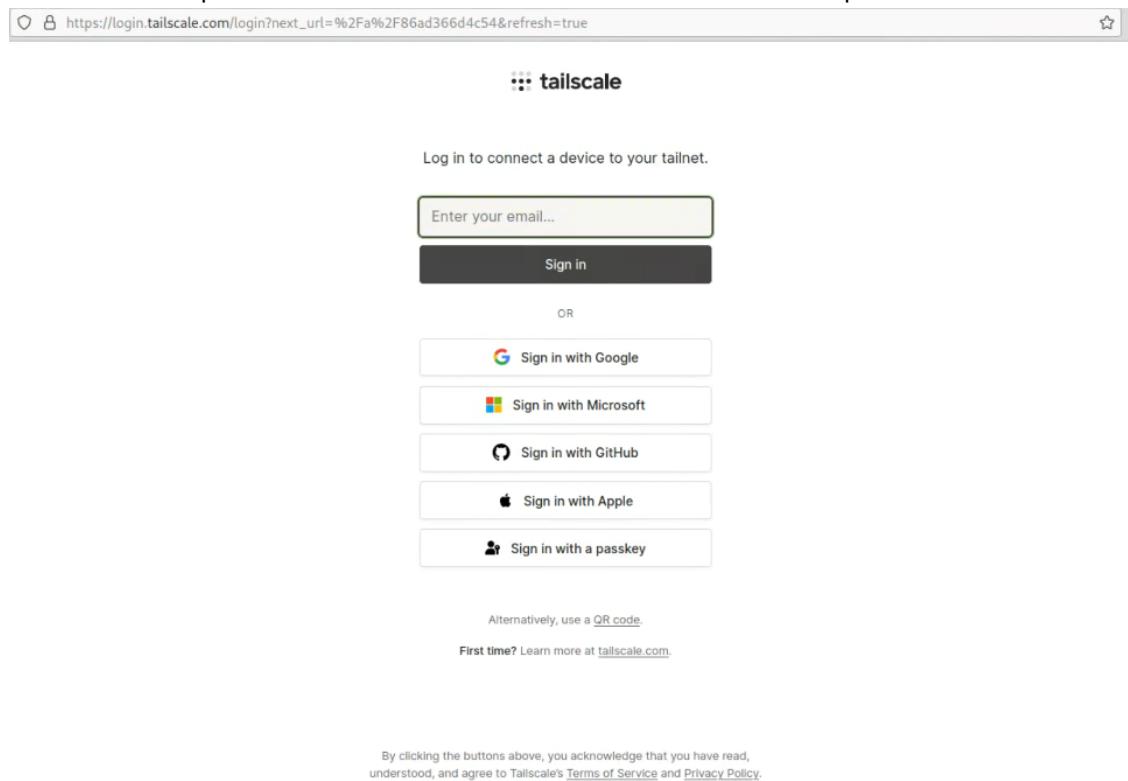
sudo tailscale up
support@Support:~$
```

7. Connectez vous à votre compte Tailscale en tapant la commande suivante dans un terminal (CTRL+T) :

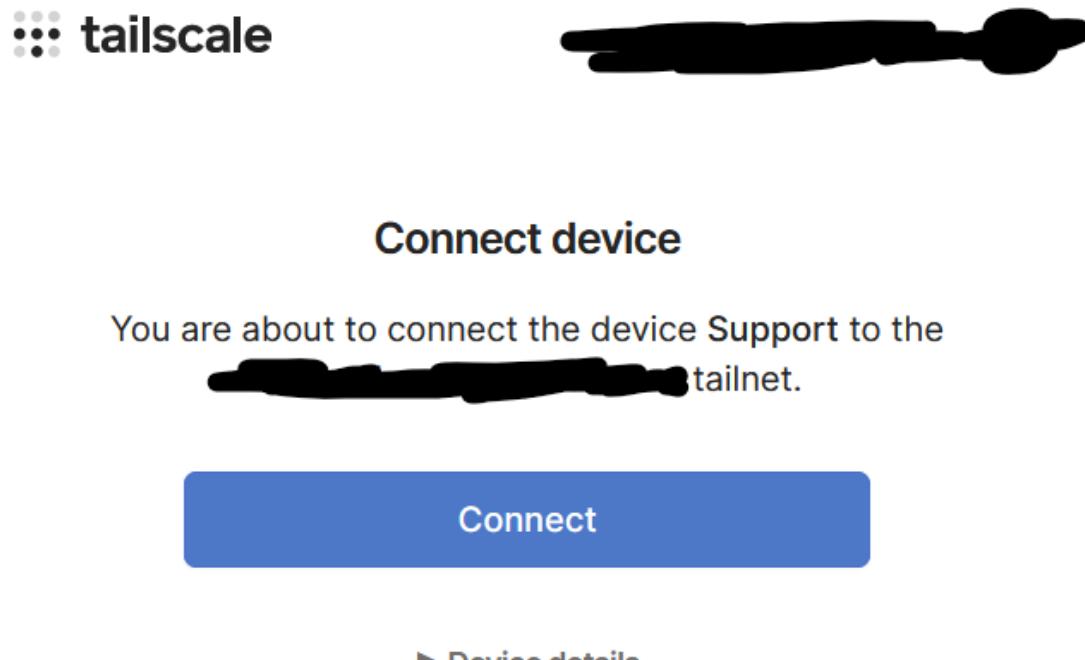
```
sudo tailscale up
```

```
support@Support:~$ sudo tailscale up
To authenticate, visit:
https://login.tailscale.com/a/86ad366d4c54
```

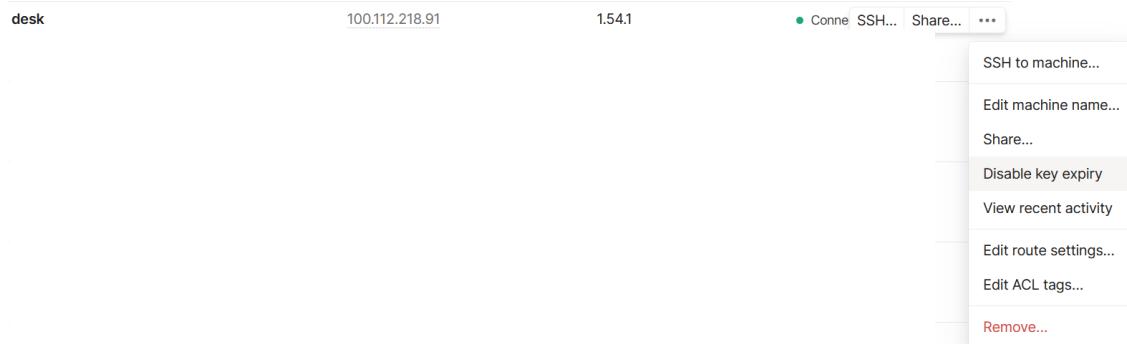
2. Allez sur le site pour vous connecter, et connectez vous à votre compte Tailscale



3. Cliquez sur "Connect" pour connecter le système à votre compte Tailscale



4. Désactivez l'expiration de la clé en cliquant sur "Disable key expiry" après avoir identifié le serveur nouvellement ajouté



5. Retournez sur le terminal et tapez la commande suivante :

```
sudo systemctl enable tailscaled  
sudo tailscale ip -4
```

```
~$ sudo systemctl enable tailscaled  
~$ sudo tailscale ip -4  
100.112.218.91
```

Notez l'adresse IP qui vous est donnée, nous en aurons besoin plus tard

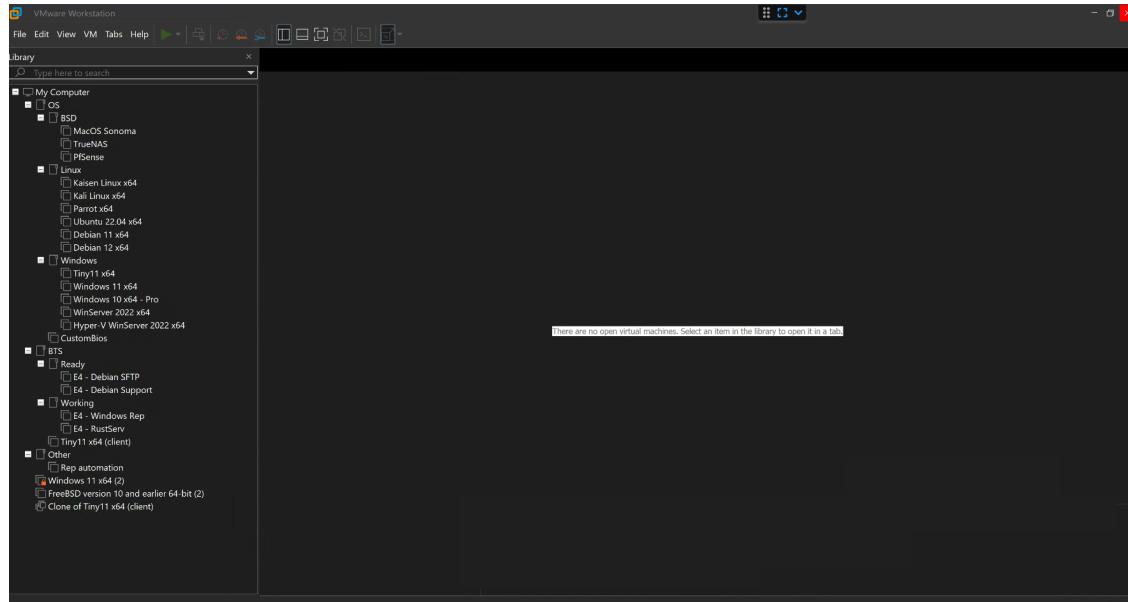
Installation Debian

Création de la VM

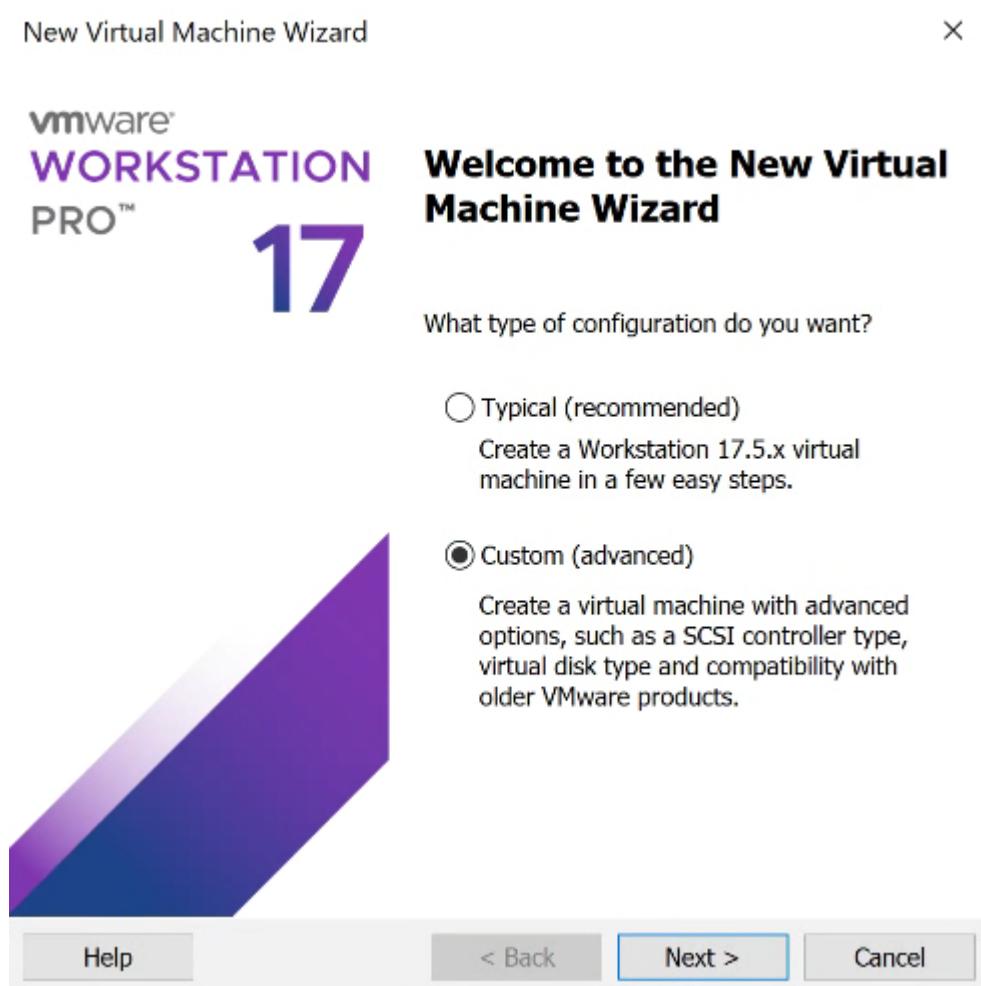
1. Téléchargez l'ISO de Debian 11 Ici nous utiliserons un ordinateur sous l'architecture Amd64 en netinst pour correspondre aux postes les plus communs, l'iso sera donc amd64 ou x86-64 mais le site propose également des iso d'architectures différentes tel que l'arm64 ou plus spécialisées [ici](#)

2. Branchez votre clé USB

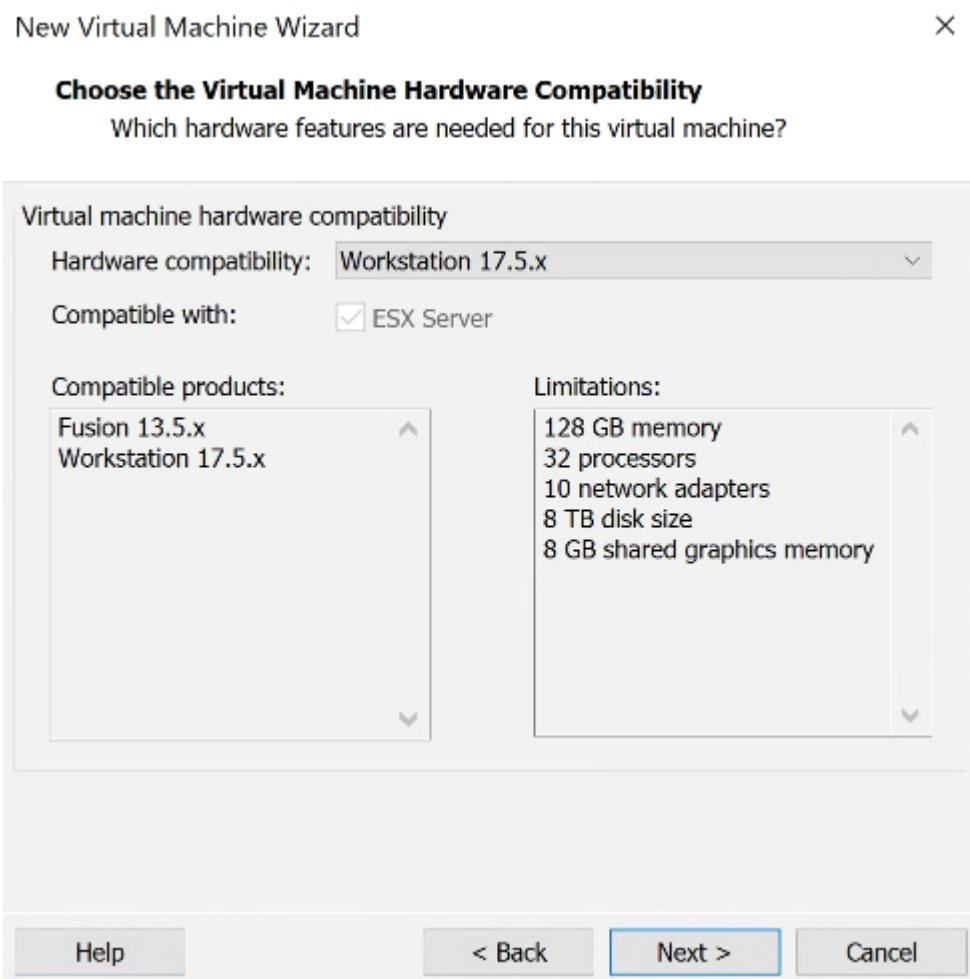
3. Ouvrez VmWare Workstation

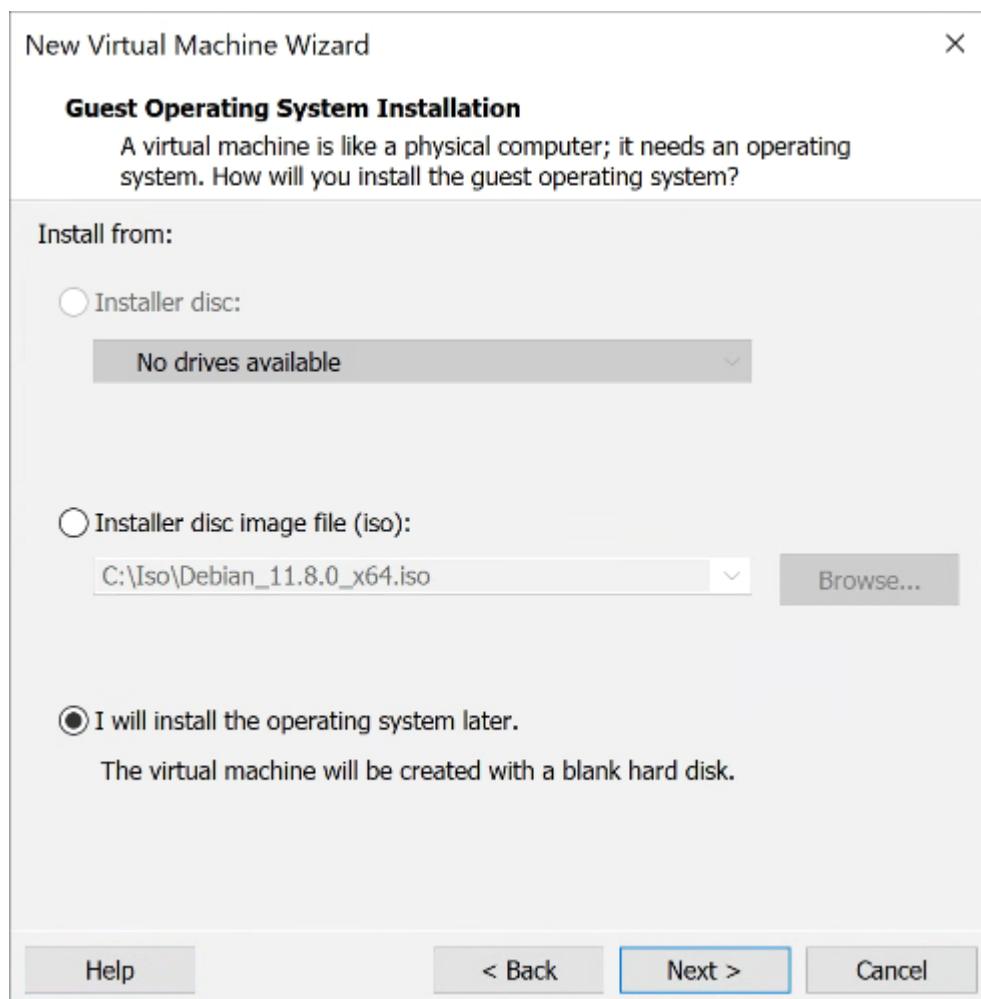


4. Créez une nouvelle machine virtuelle et sélectionnez « Custom »

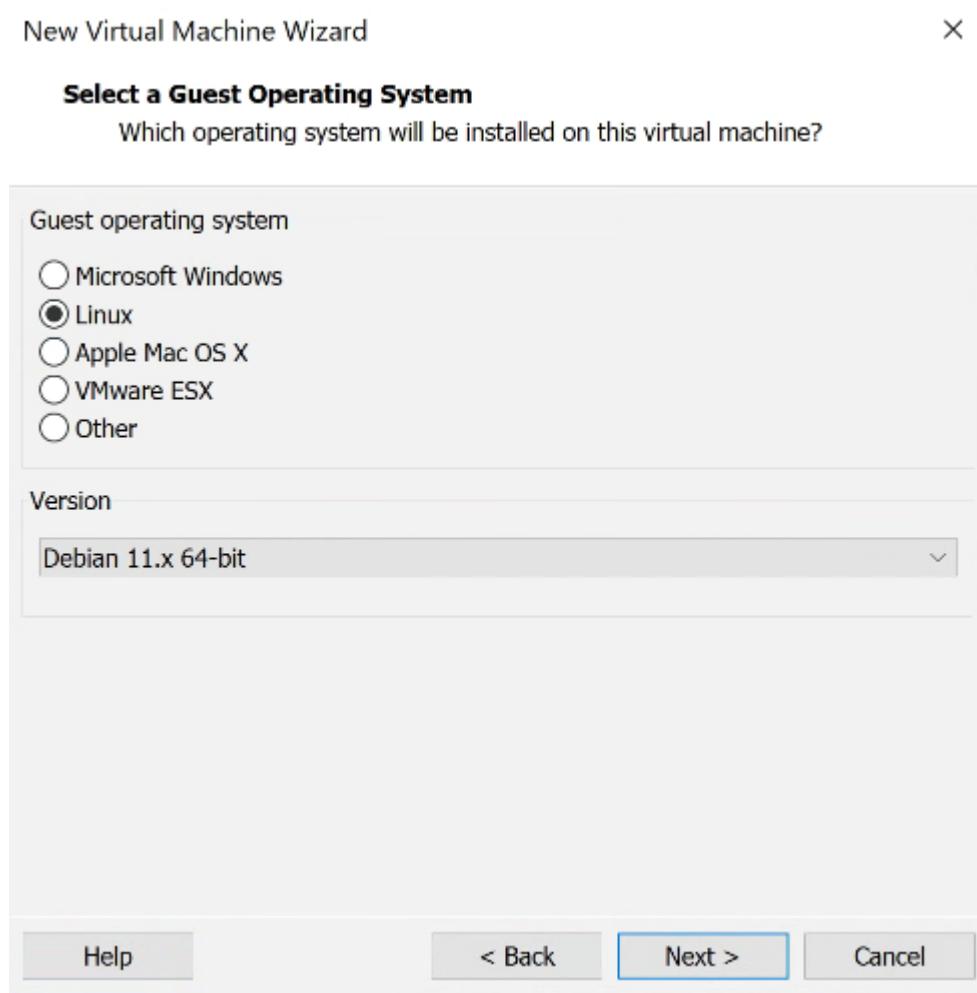


5. Faites next et encore next, puis sélectionnez « I will install the operating system later » et continuez

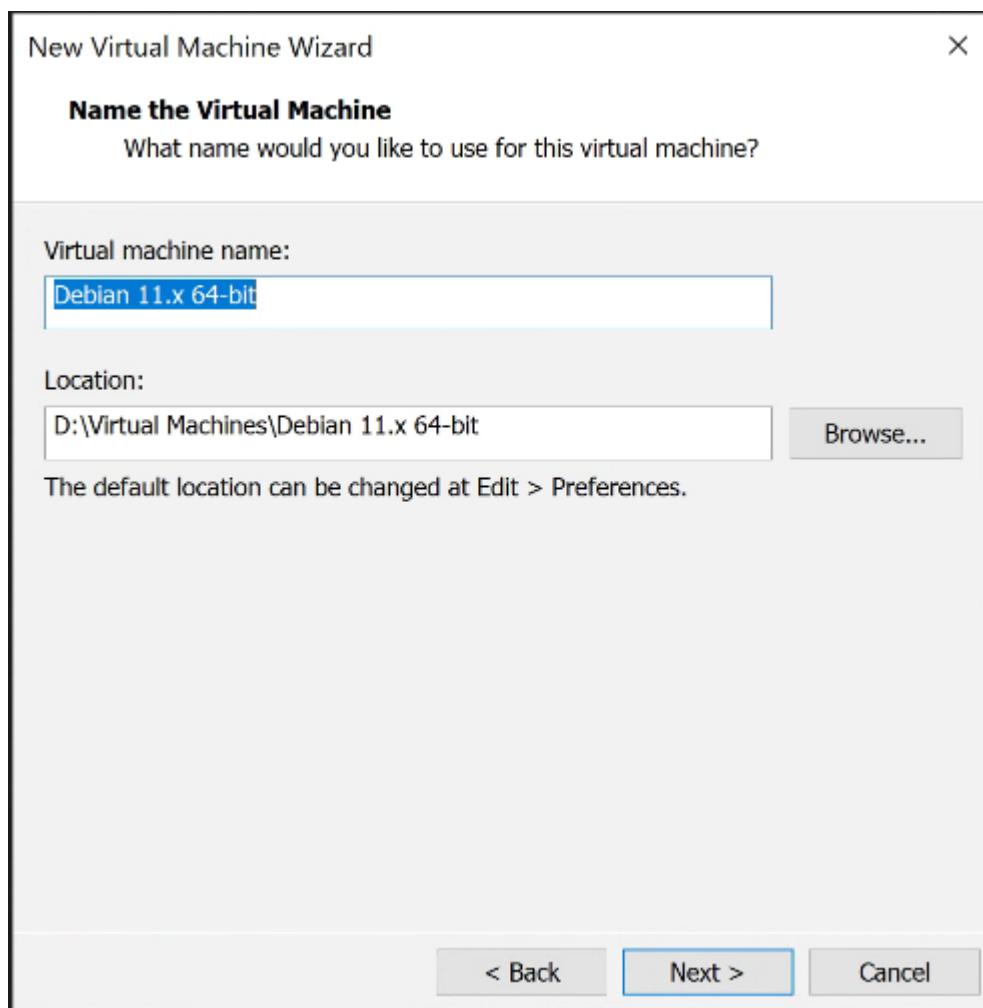




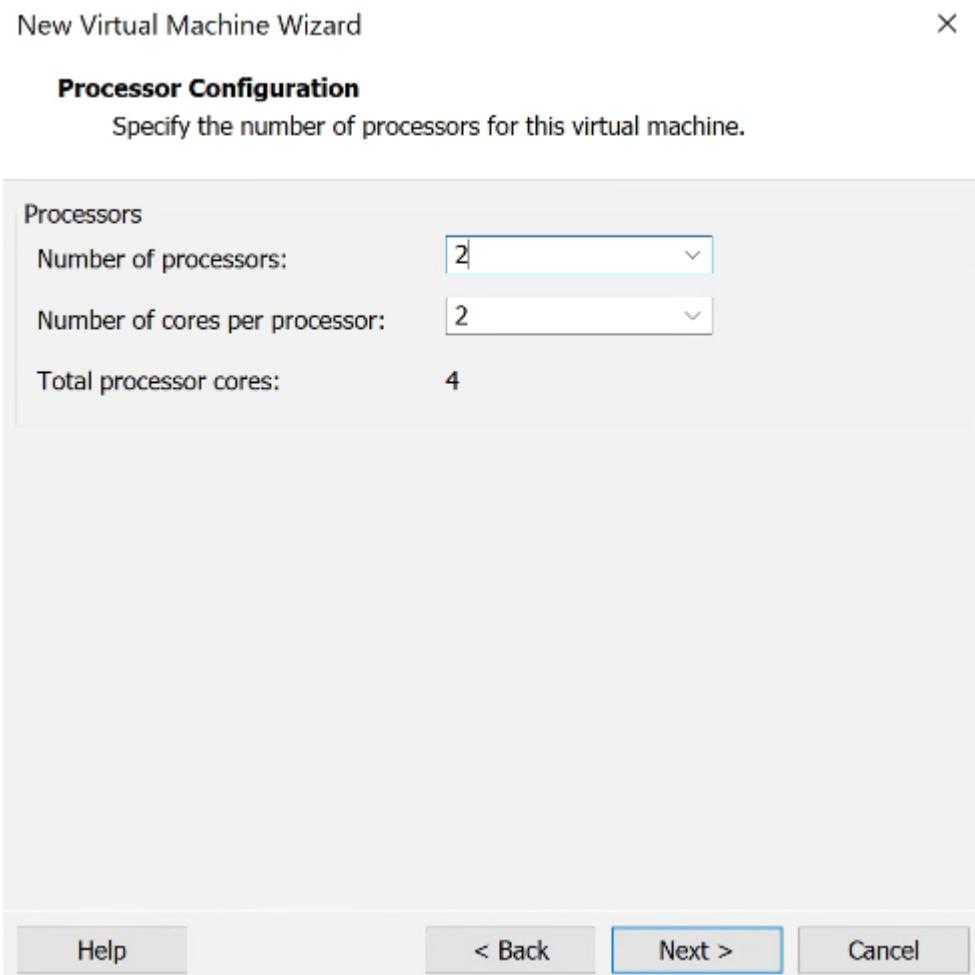
6. Sélectionnez « Linux » et cherchez « Debian 11.x 64-bit » avant de continuer

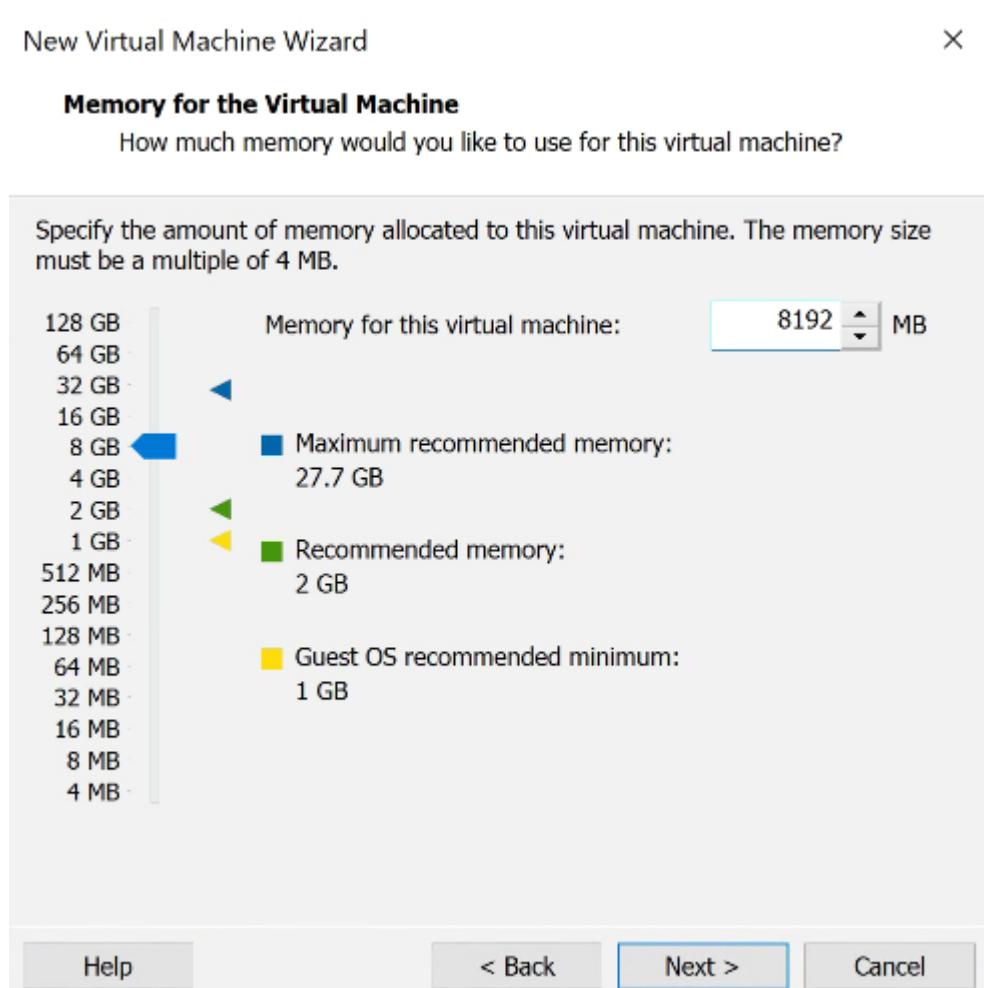


7. Nommez votre machine virtuelle et mettez là où des dossiers utilisateurs (dans C:/VM/nomdevm par exemple). Cela évitera des conflits de permissions avec VmWare

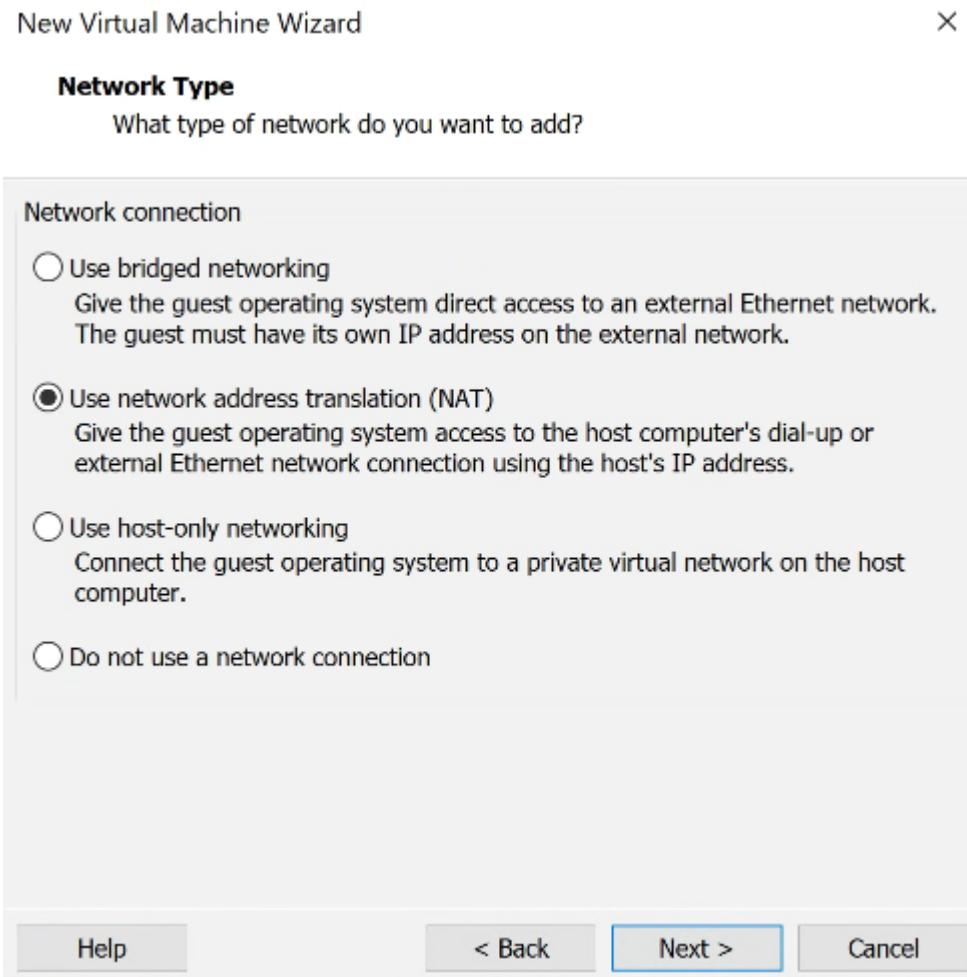


8. Faites next ou changez le nombre de coeurs pour la VM selon la configuration de votre ordinateur pour accélérer les installations, de même pour la RAM

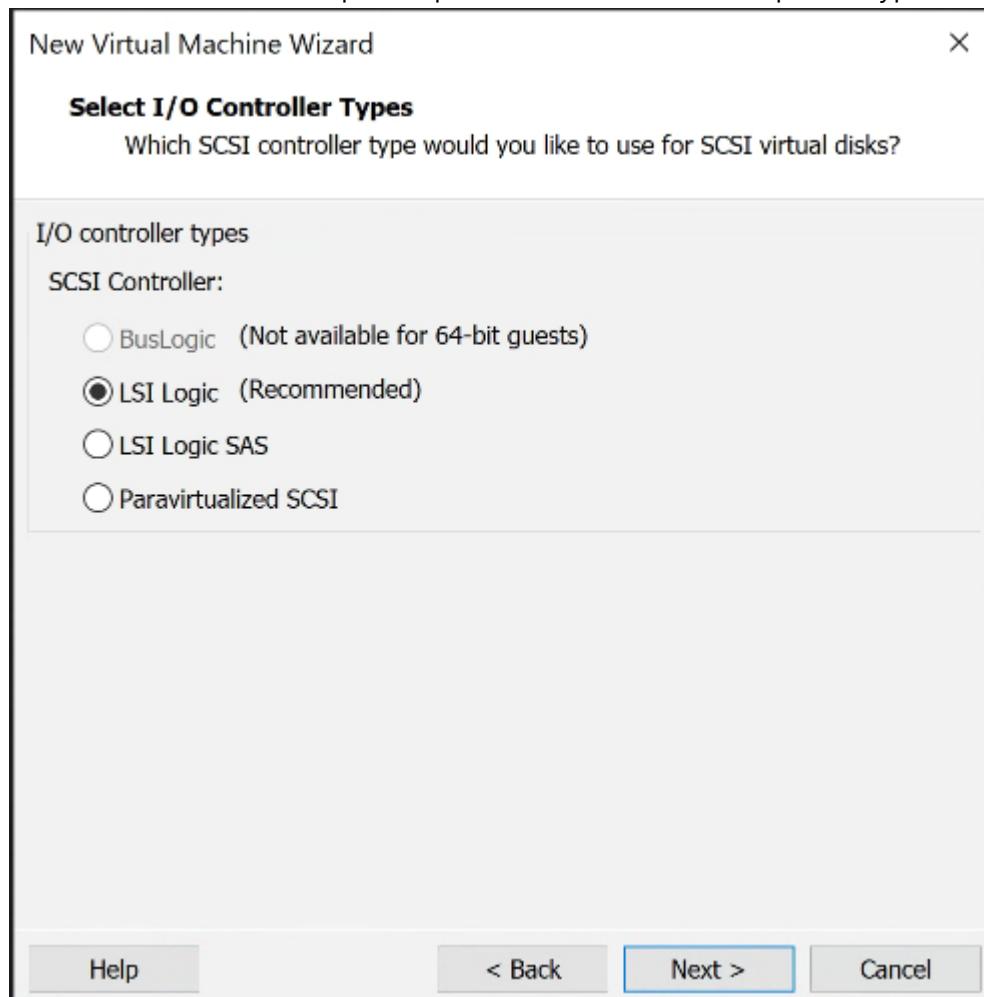


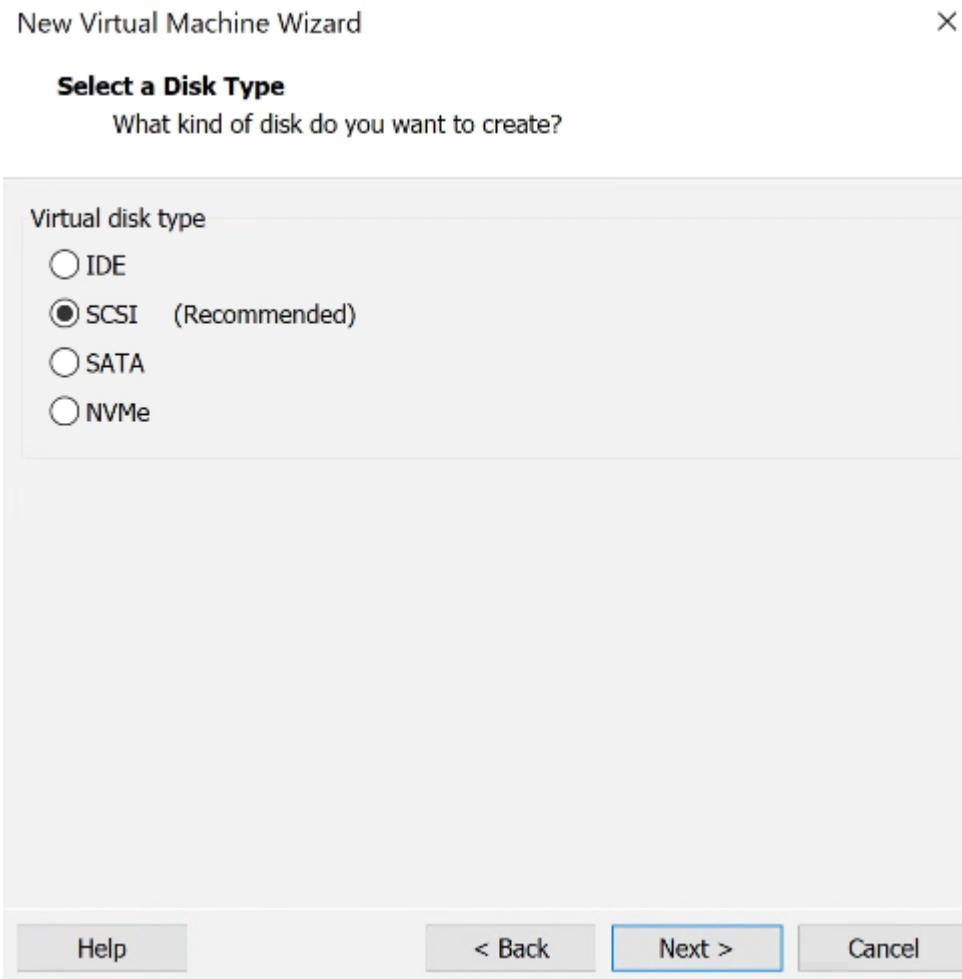


9. Laissez la carte réseau en NAT pour avoir un accès à internet lors de l'installation et continuez

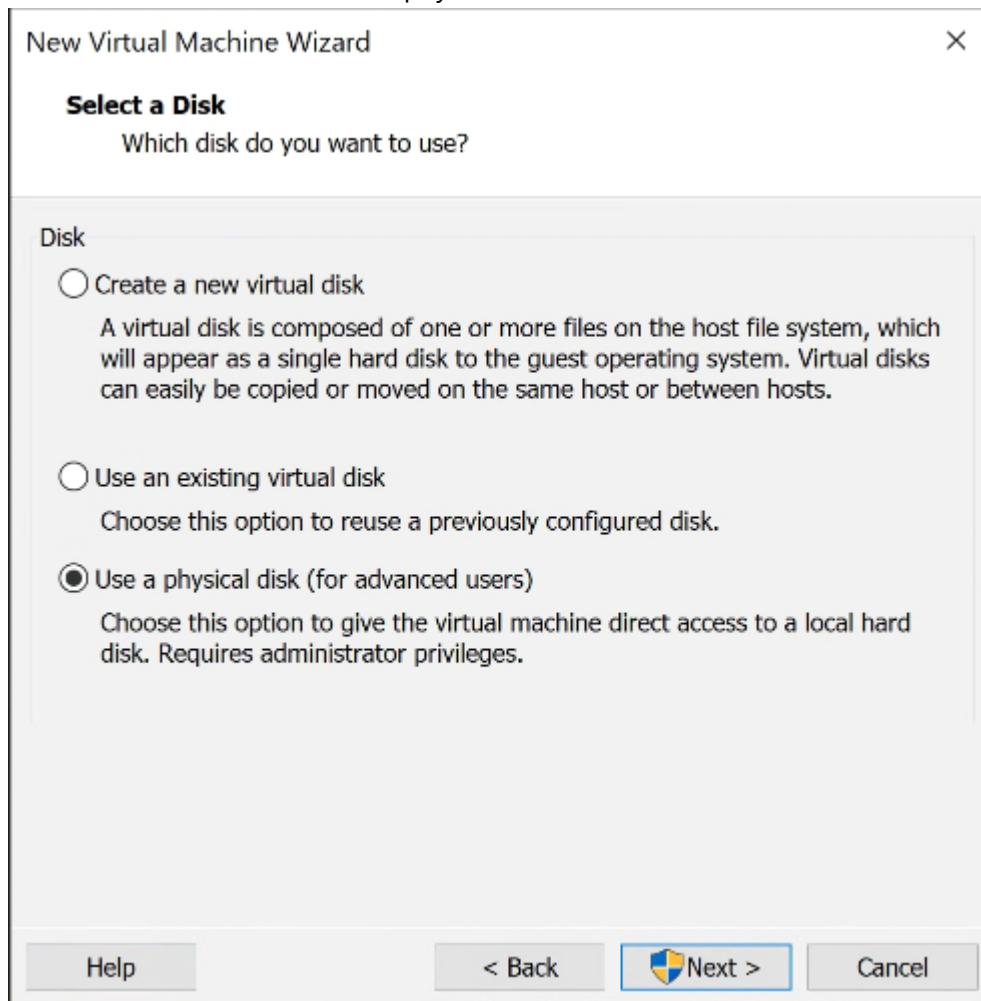


10. Laissez le controller de disque tel quel et continuez, de même pour le type de disque

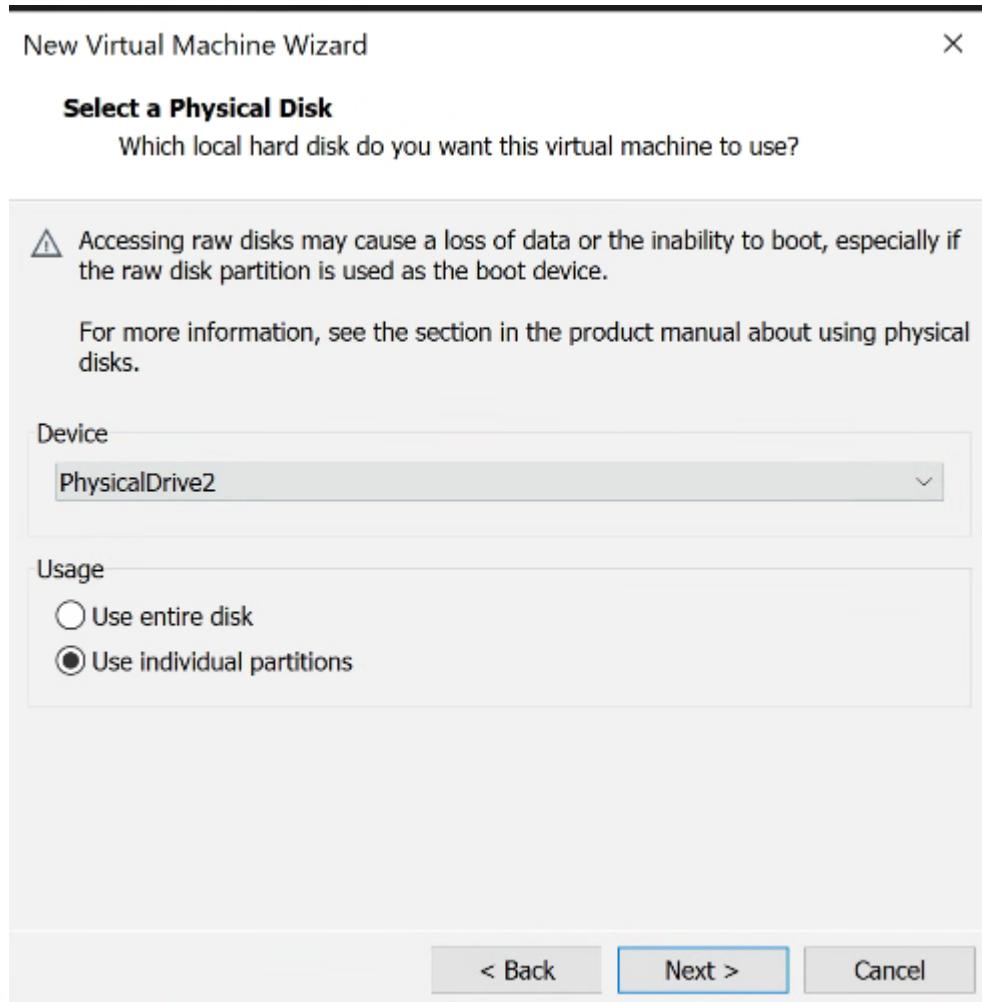


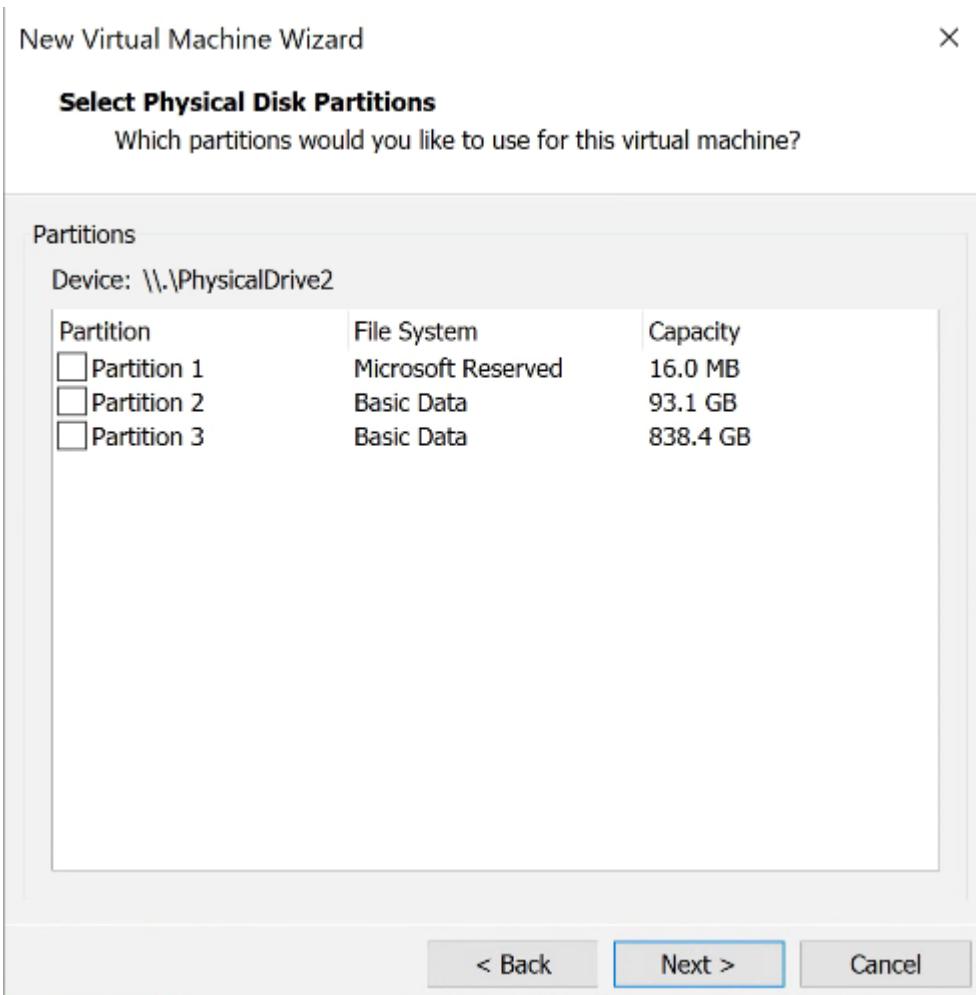


11. Continuez, sélectionnez « Use a physical disk »

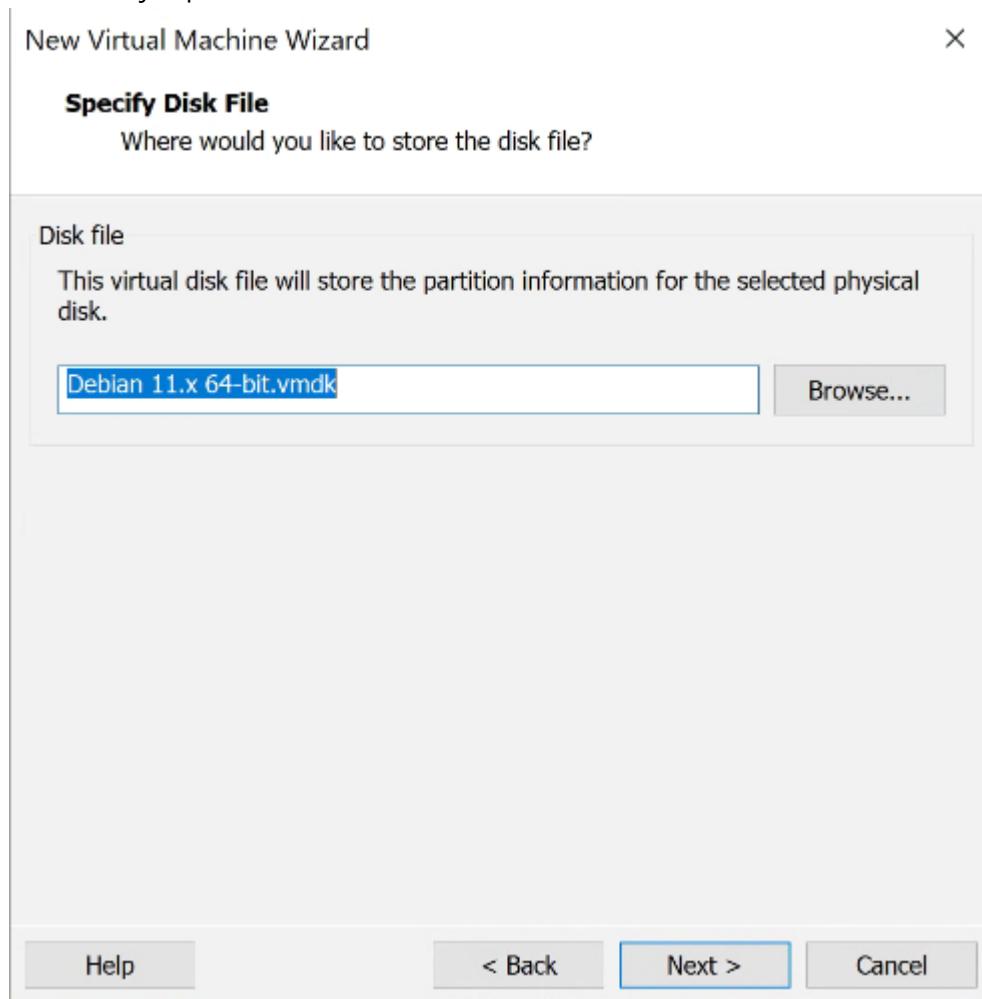


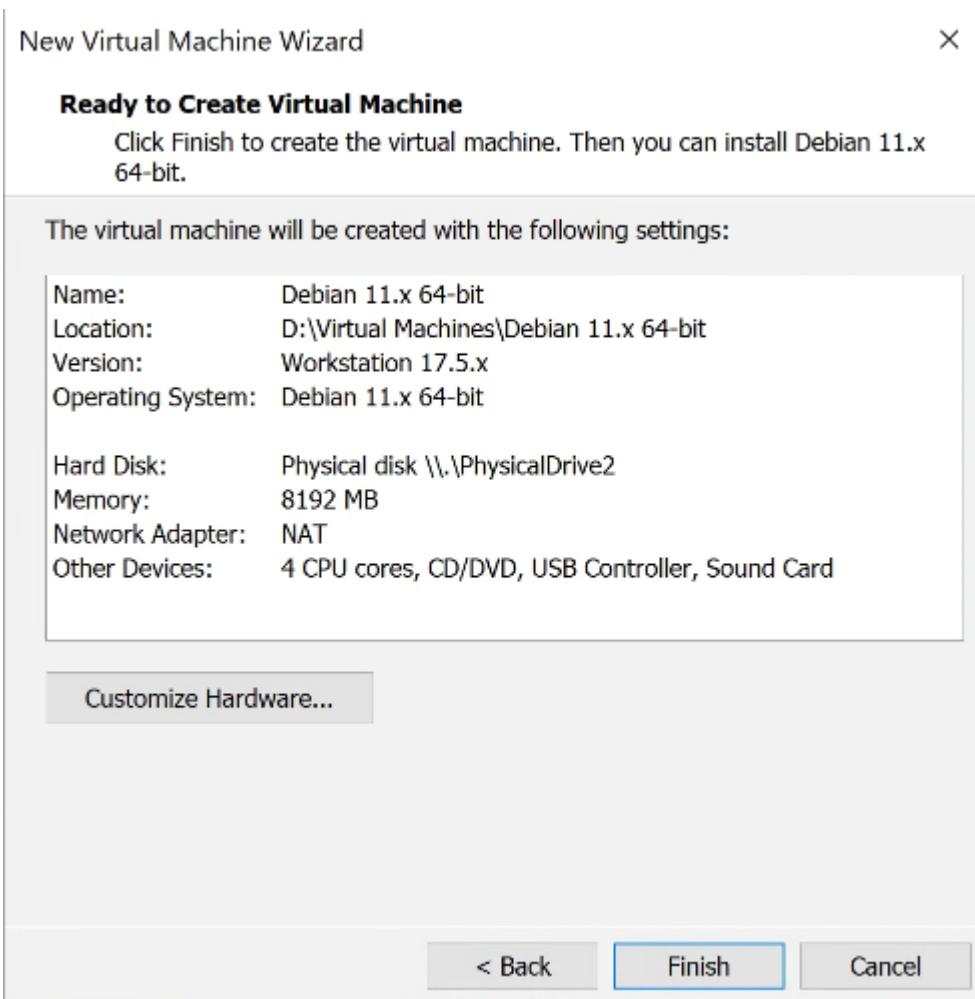
12. Sélectionnez votre clé USB et continuez. Si vous n'êtes pas sûr du disque à sélectionner, vous pouvez sélectionner "Use Individual partitions" et "Next" pour voir les partitions de votre disque. Retournez en arrière et remettez "Use entire disk" une fois que vous avez trouvé votre disque



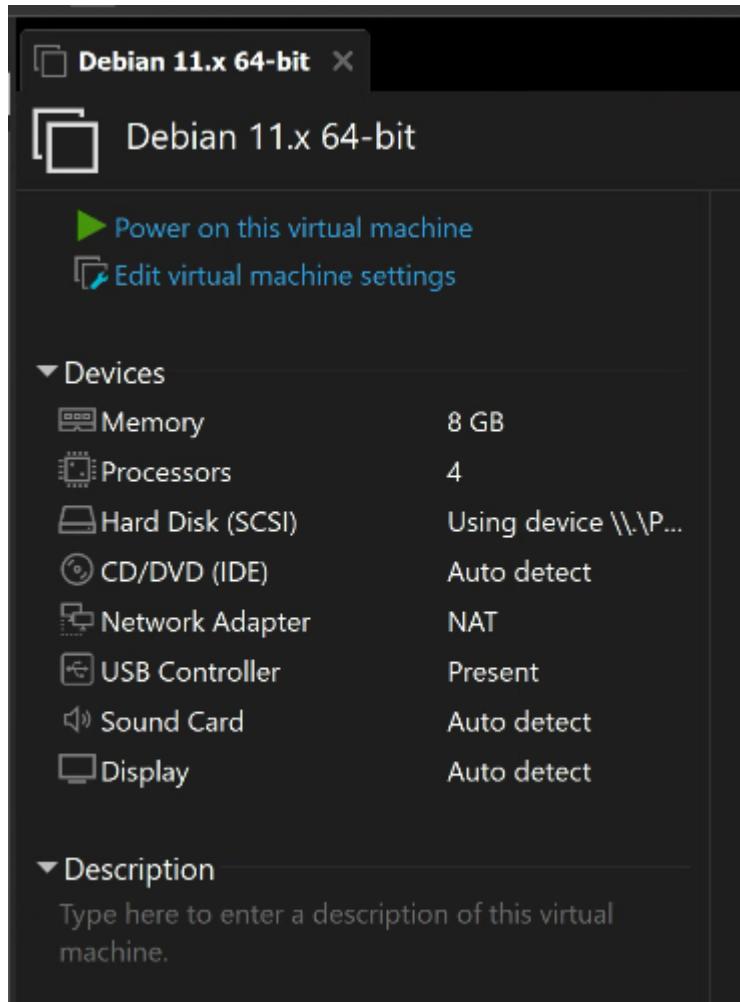


13. Continuez jusqu'à la fin de la création de la machine virtuelle

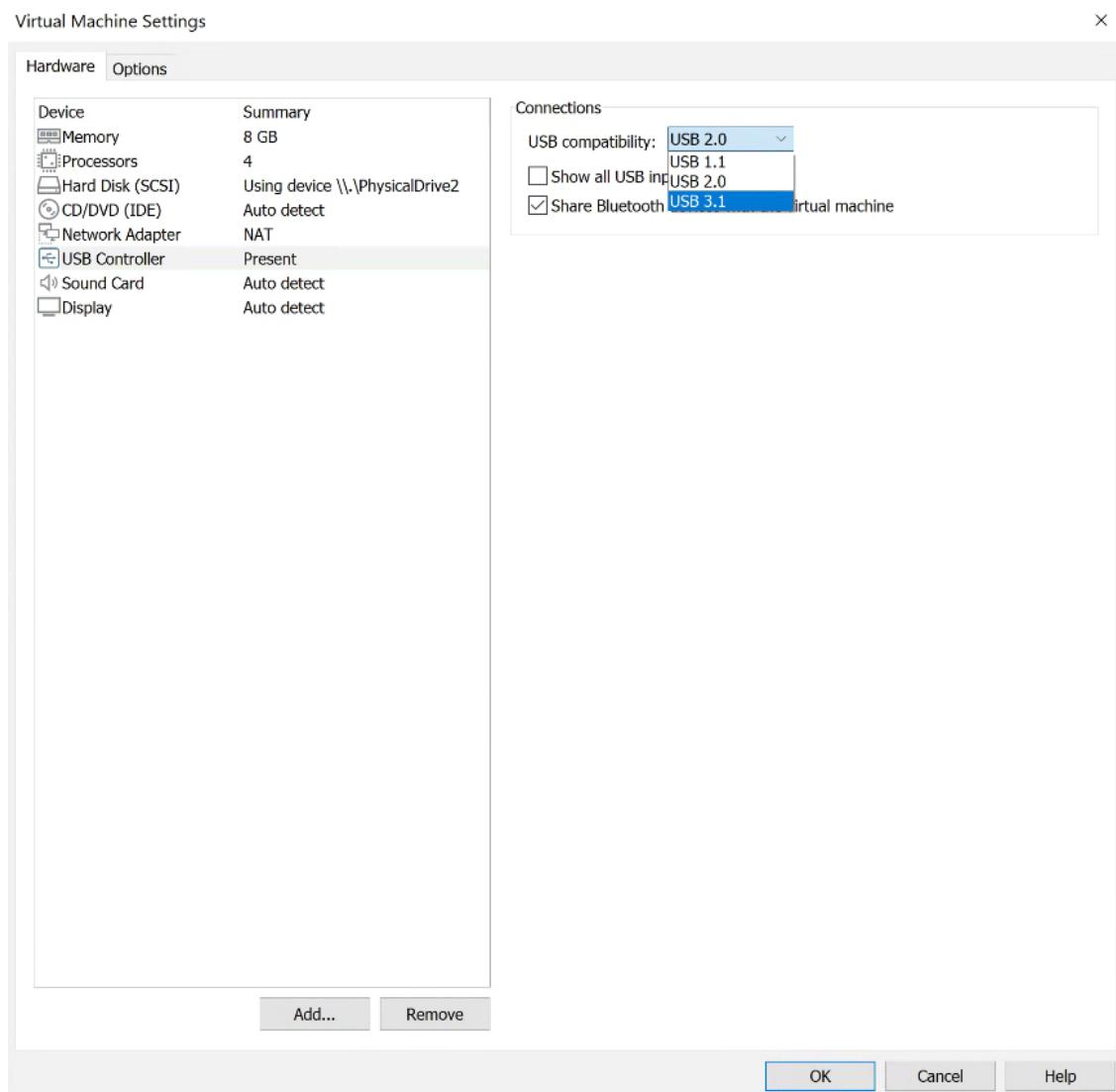




14. Une fois la machine virtuelle créée, allez dans les paramètres de la machine virtuelle et sélectionnez "USB Controller" dans la liste de gauche

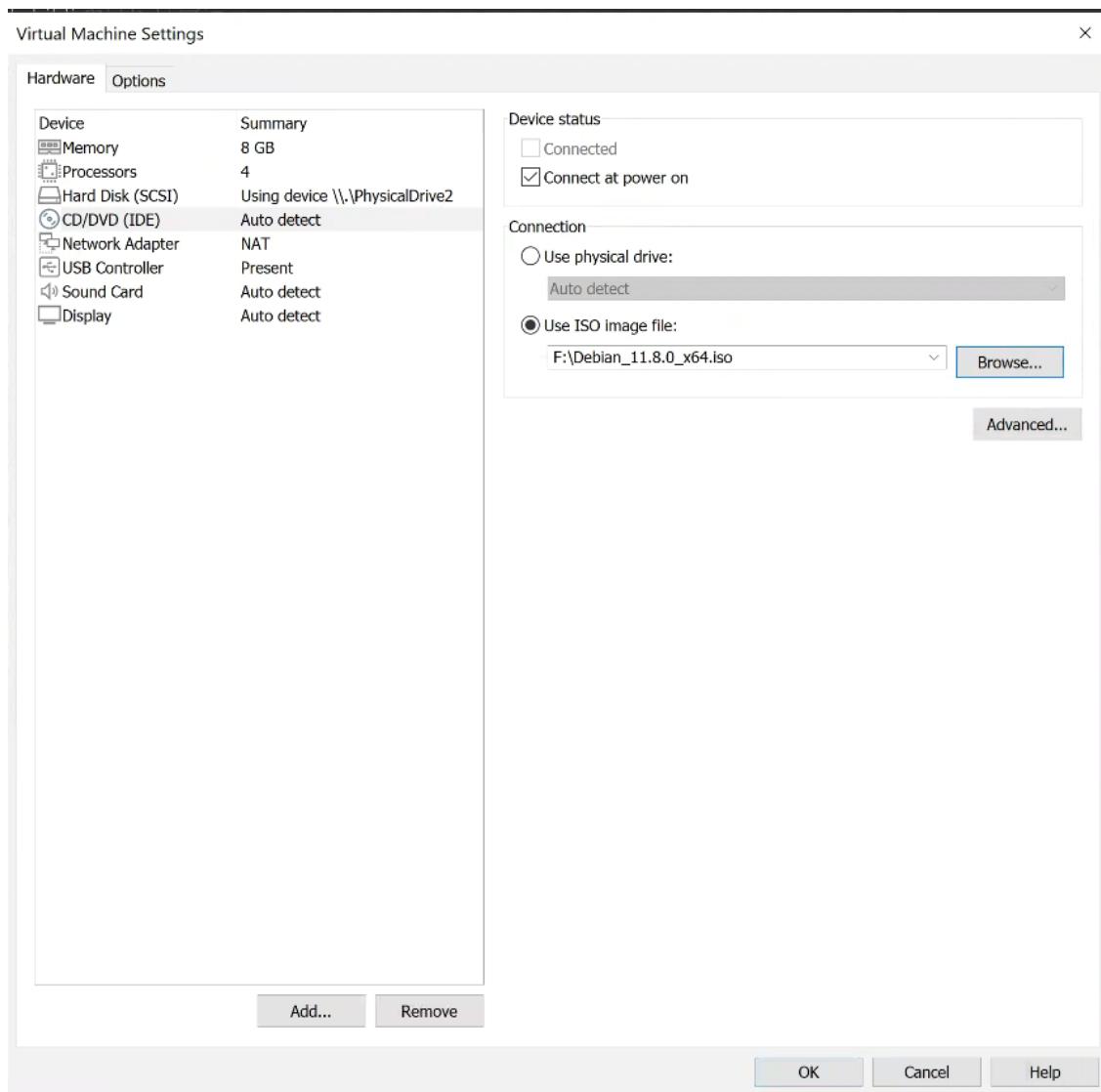


15. Sélectionnez "USB Compatibility" et sélectionnez "USB 3.1" dans la liste déroulante



16. Allez dans « CD/DVD (IDE) », sélectionnez « Use ISO image file : » et mettez l'Iso de Debian

11



17. Démarrez la machine virtuelle. Si une erreur apparaît, débranchez et rebranchez la clé, assurez-vous qu'elle ne soit pas utilisée d'une quelconque manière par votre ordinateur et relancer VMware Workstation en mode administrateur. Cela est dû à un problème de permissions avec la clé USB et de conflit d'utilisation avec VmWare



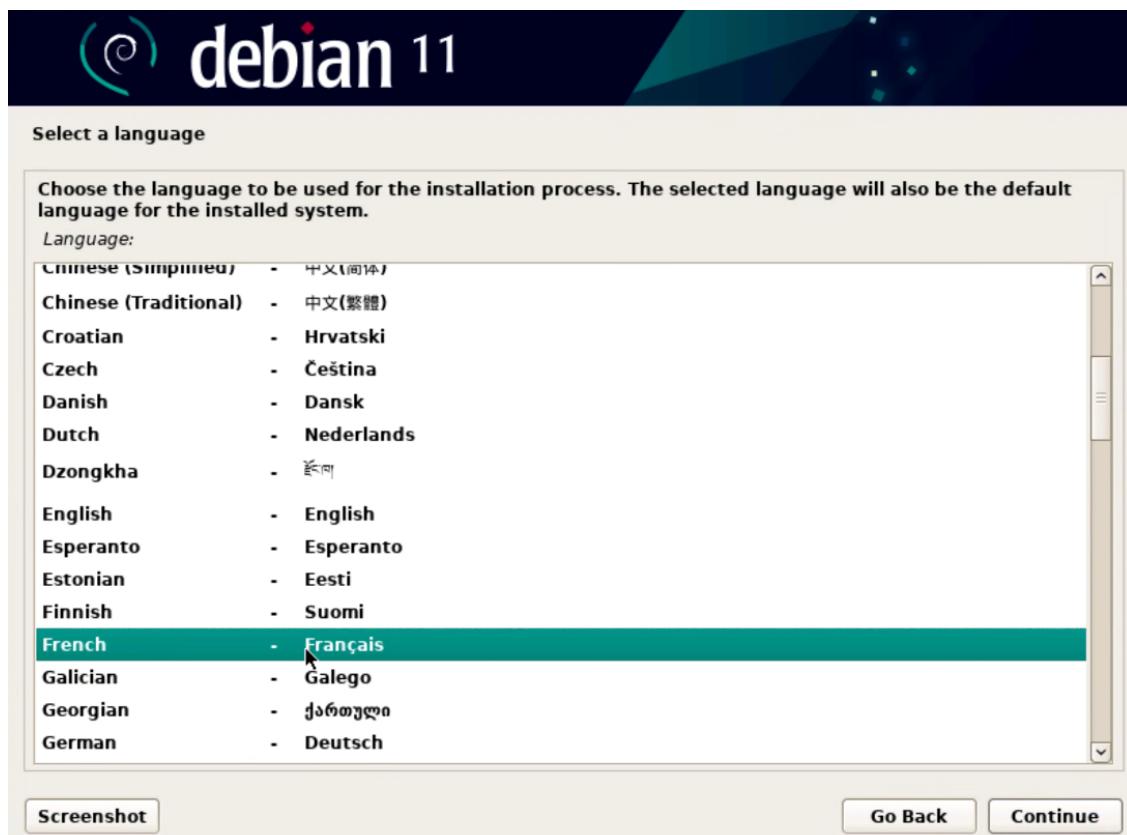
Système

1. Démarrez la Machine Virtuelle

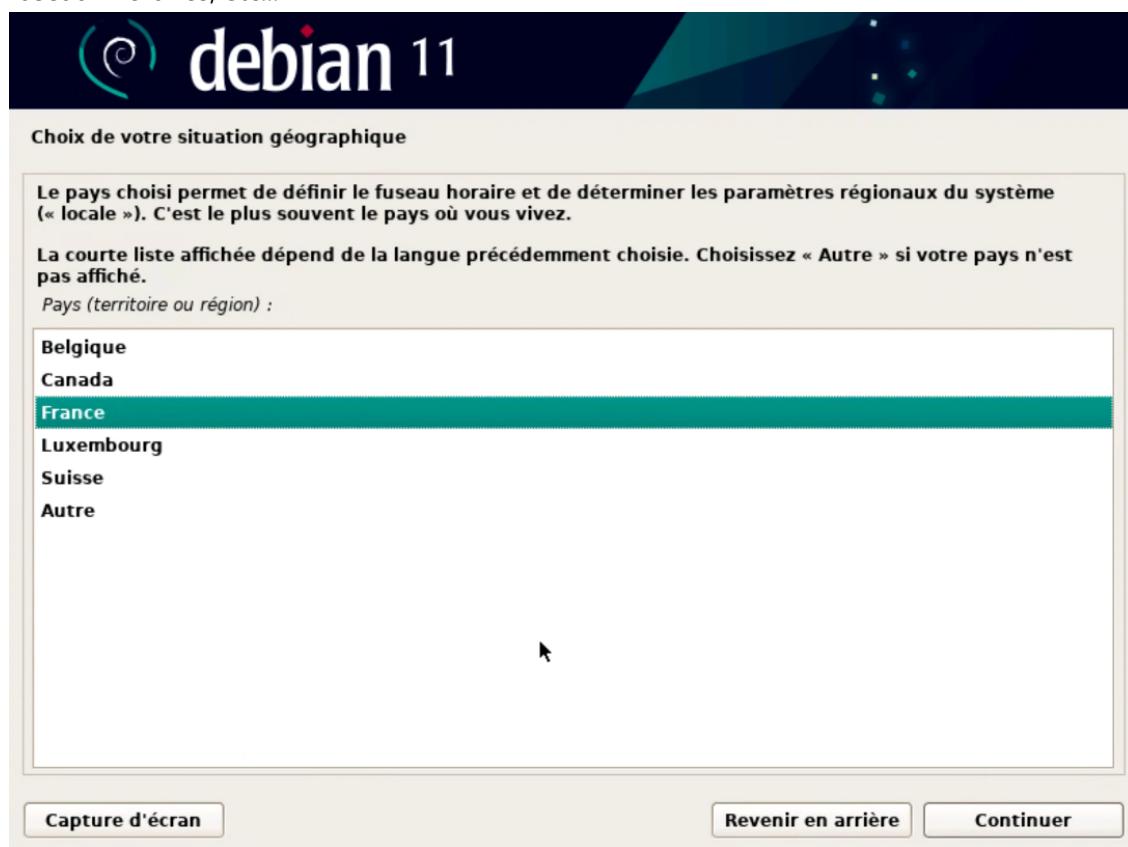
2. Sélectionnez, en faisant « entrer », la première option « Graphical install »



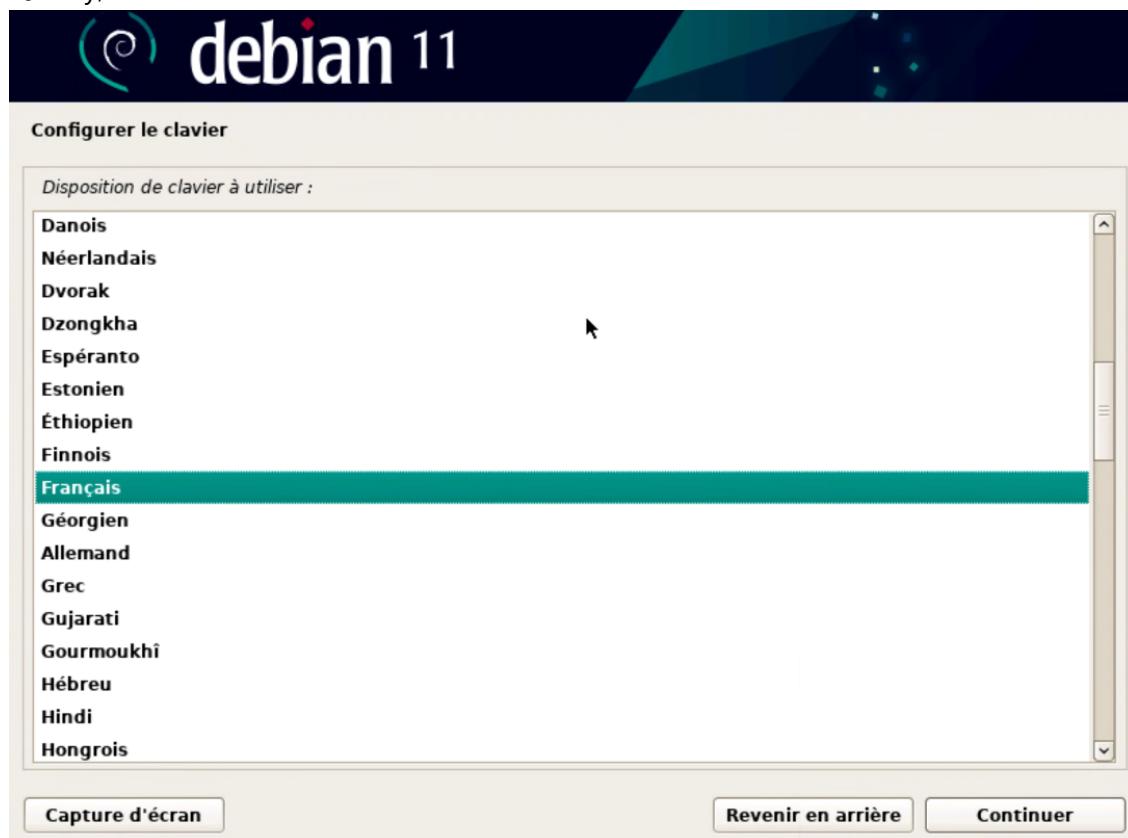
3. Sélectionnez ensuite la langue voulue (ici Français) en utilisant les flèches ou la souris puis entrer ou « continue ».



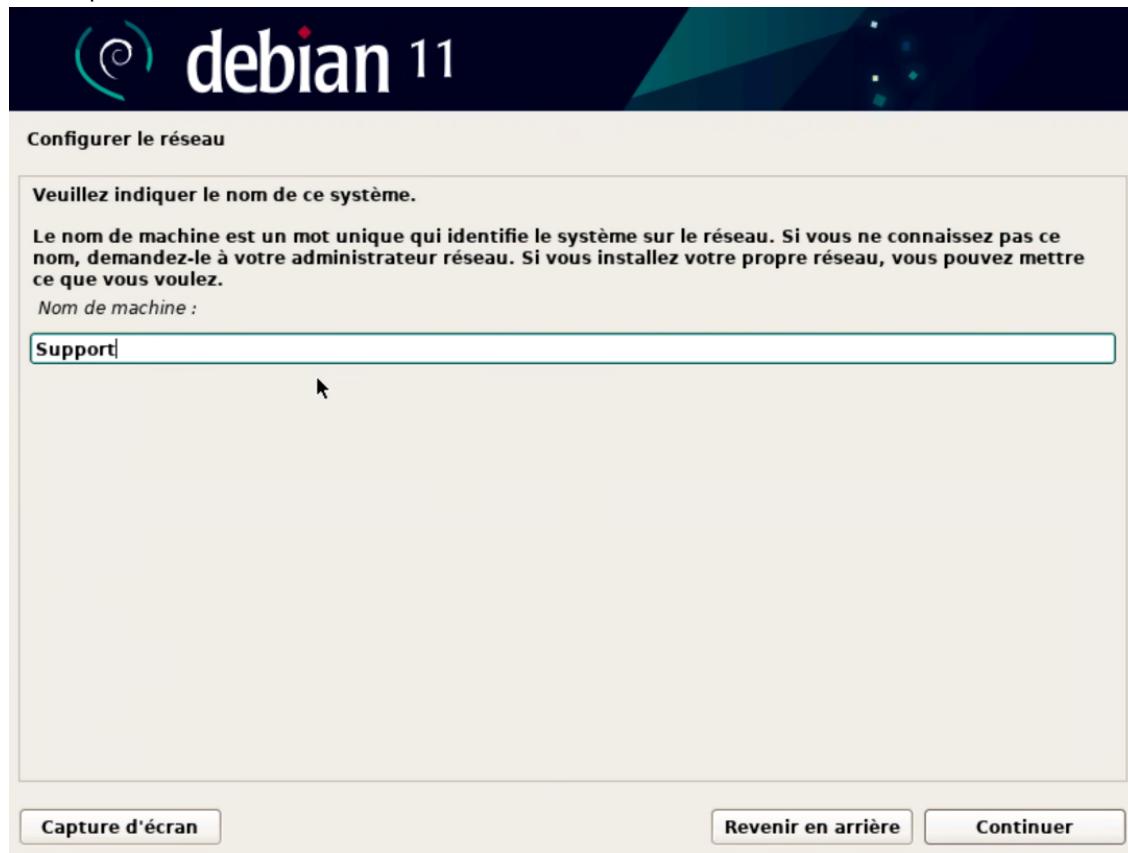
4. Sélectionnez votre pays (ici France) puis continuez. Cela impactera les configurations fuseaux horaires, etc...



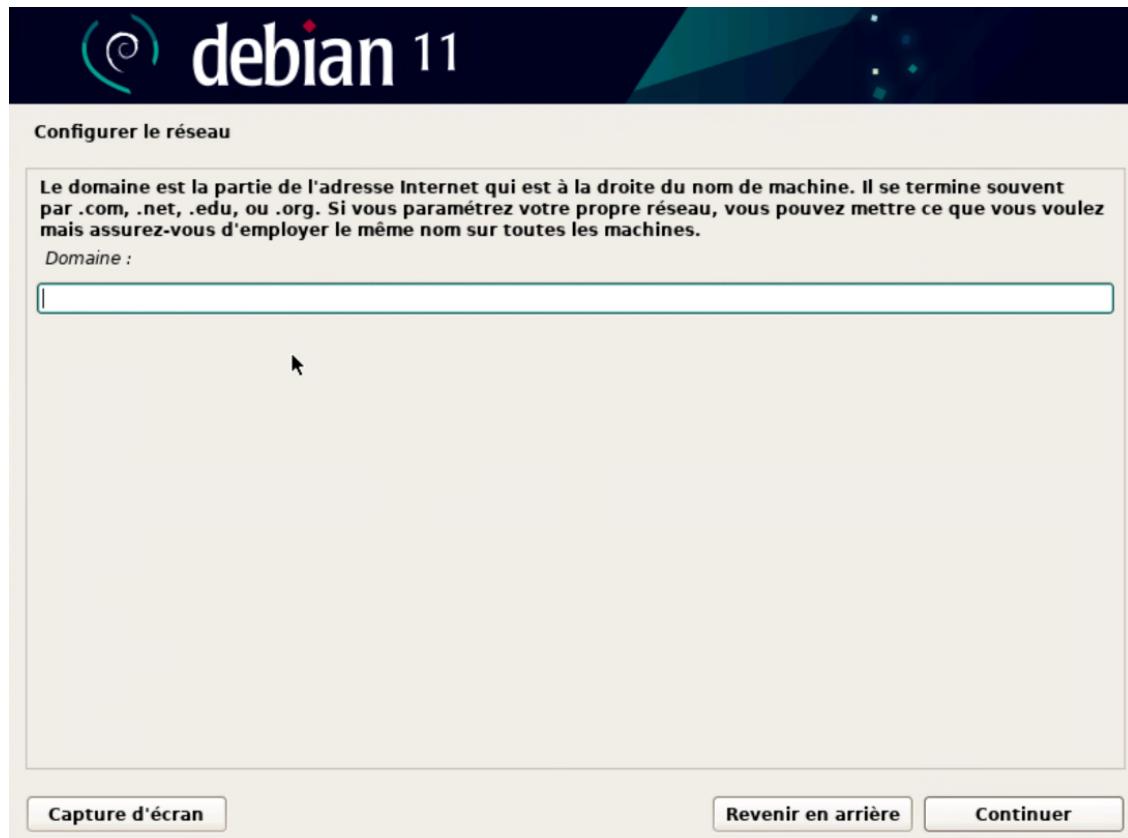
5. Sélectionnez votre disposition de clavier, un Azerty français sera « Français » ; pour un Qwerty, cela sera « Etats-Unis »



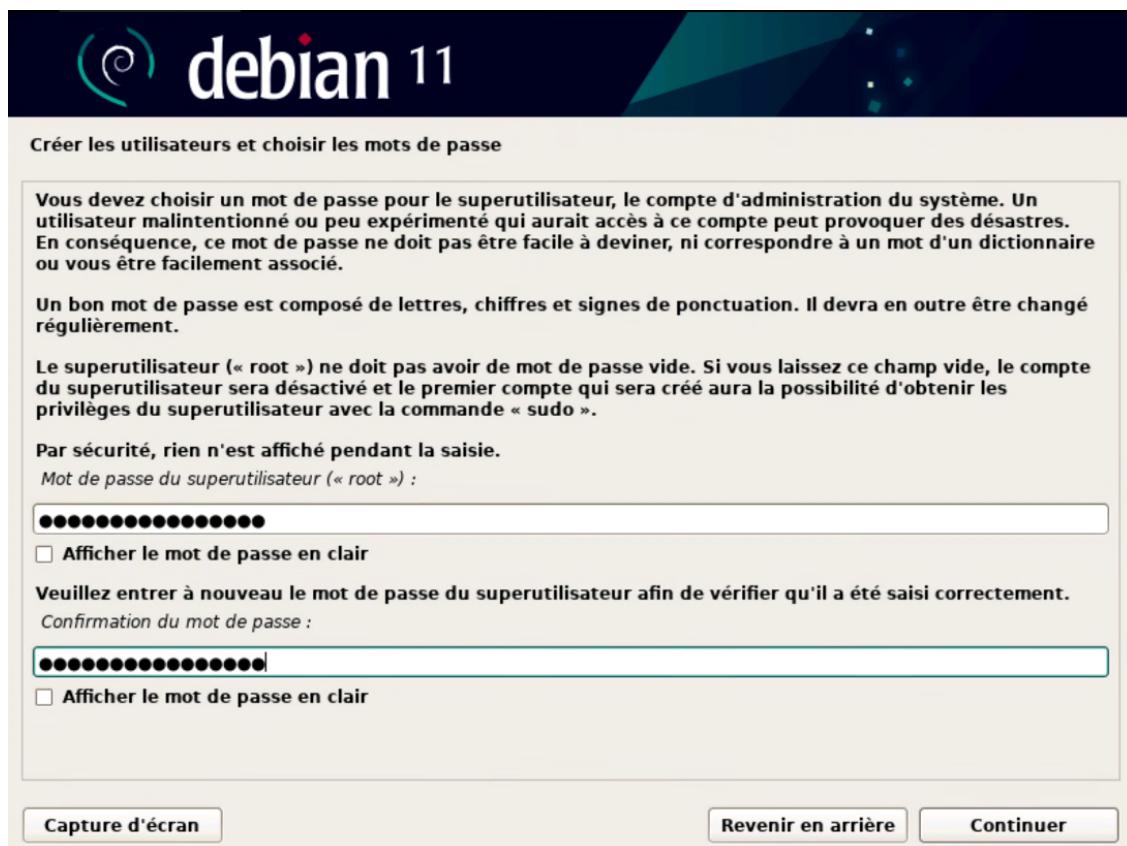
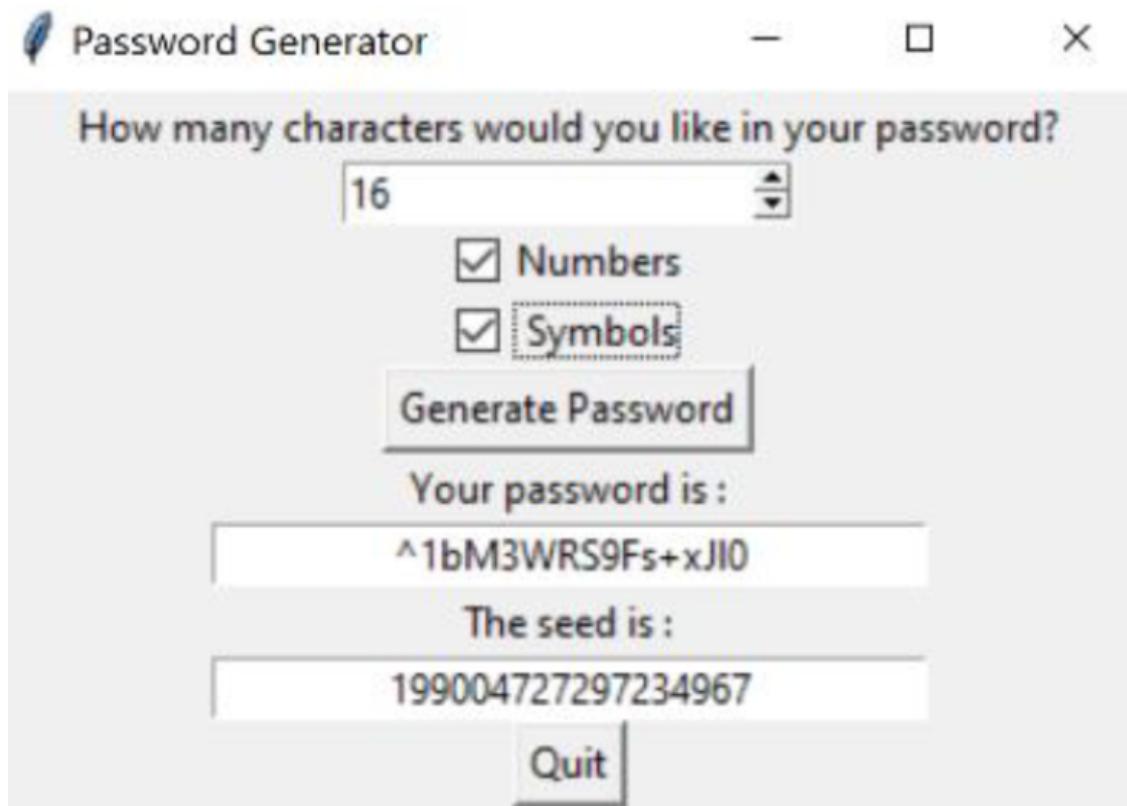
6. Nommez le serveur et faites « continuer » (nous l'appellerons ici « Support » pour l'exemple)



7. Laissez le domaine vide et continuez

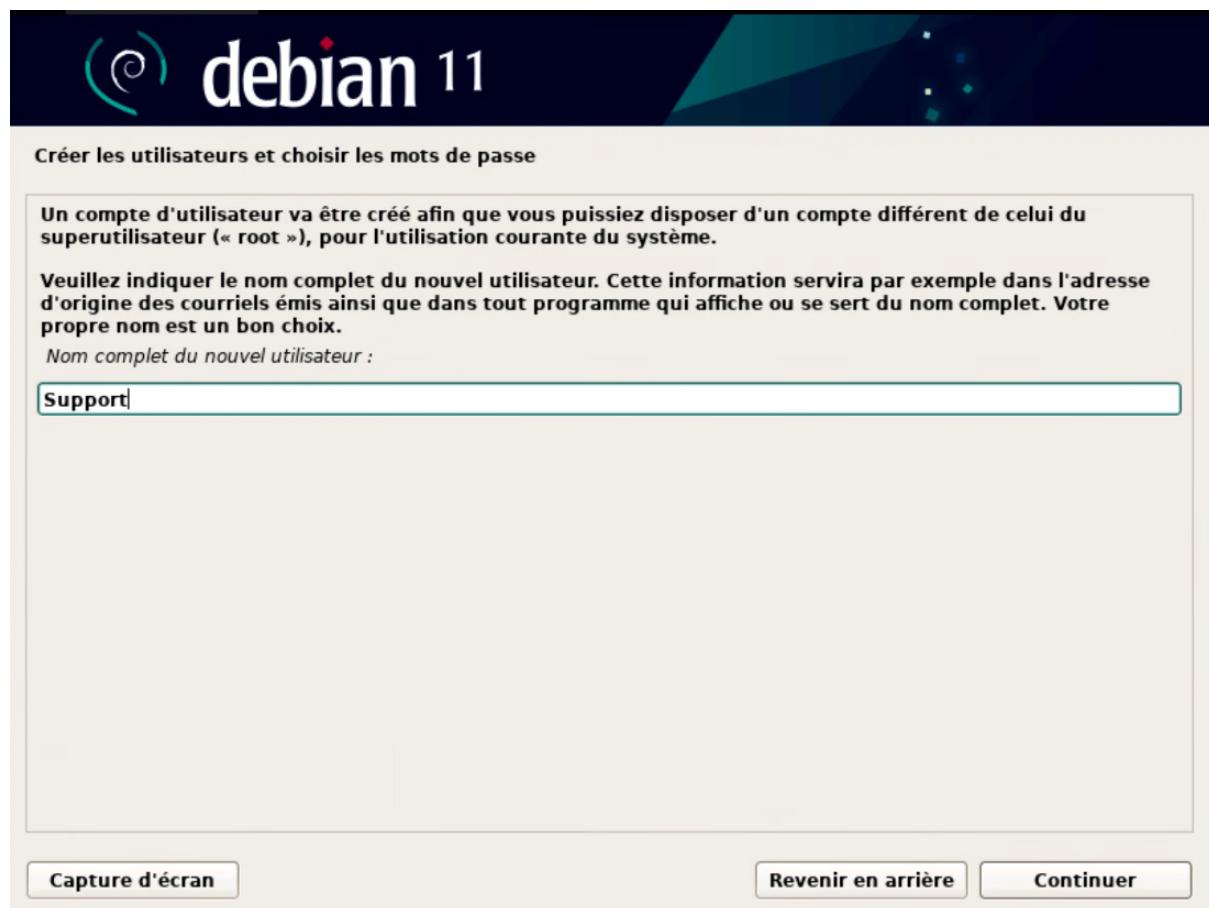


8. Choisissez ensuite un mot de passe sécurisé pour le superuser. J'utiliserais ici un programme Python disponible sur mon [Github](#) pour le générer



9. Confirmez le mot de passe et continuez

10. Choisissez ensuite un nom d'utilisateur (ici nous garderons le même que le nom de machine soit : « Support »)

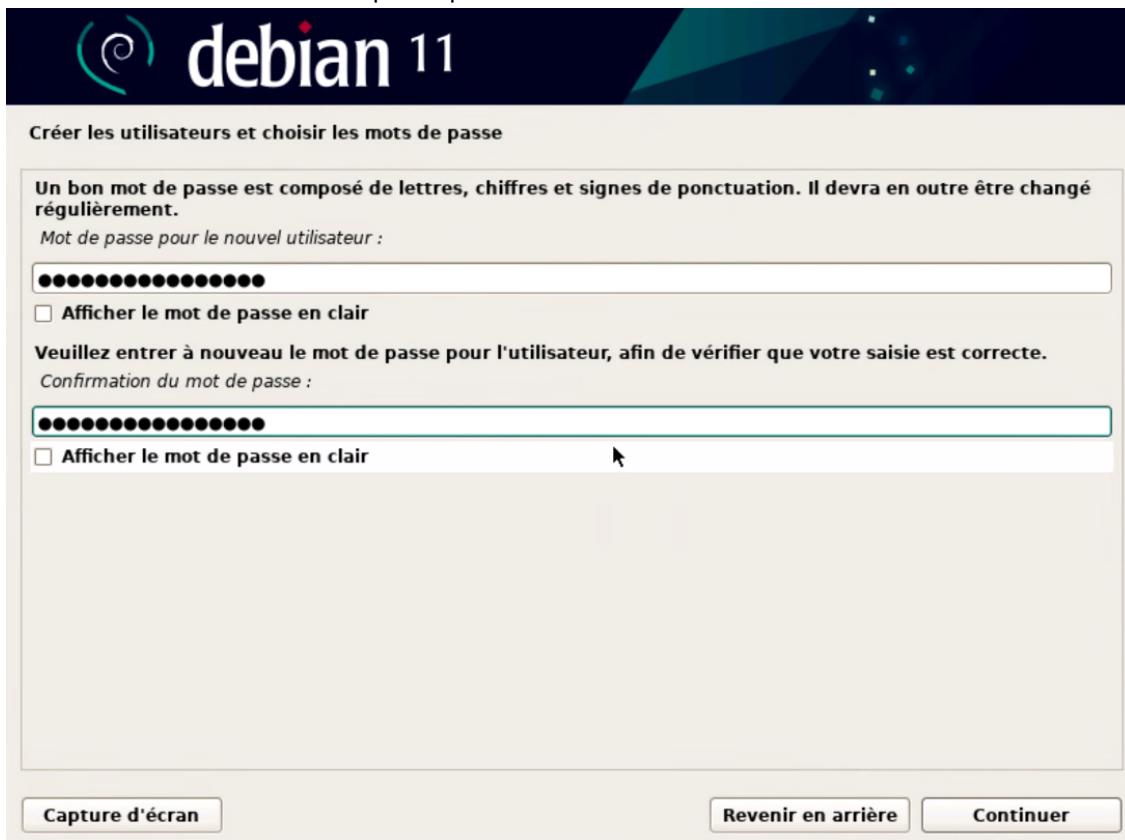


11. Nous ferons continuer directement (gardant le même nom pour l'utilisateur) après mais vous

pouvez changer ce qui est marqué pour l'identifiant (devenant différent du nom affiché à l'écran)

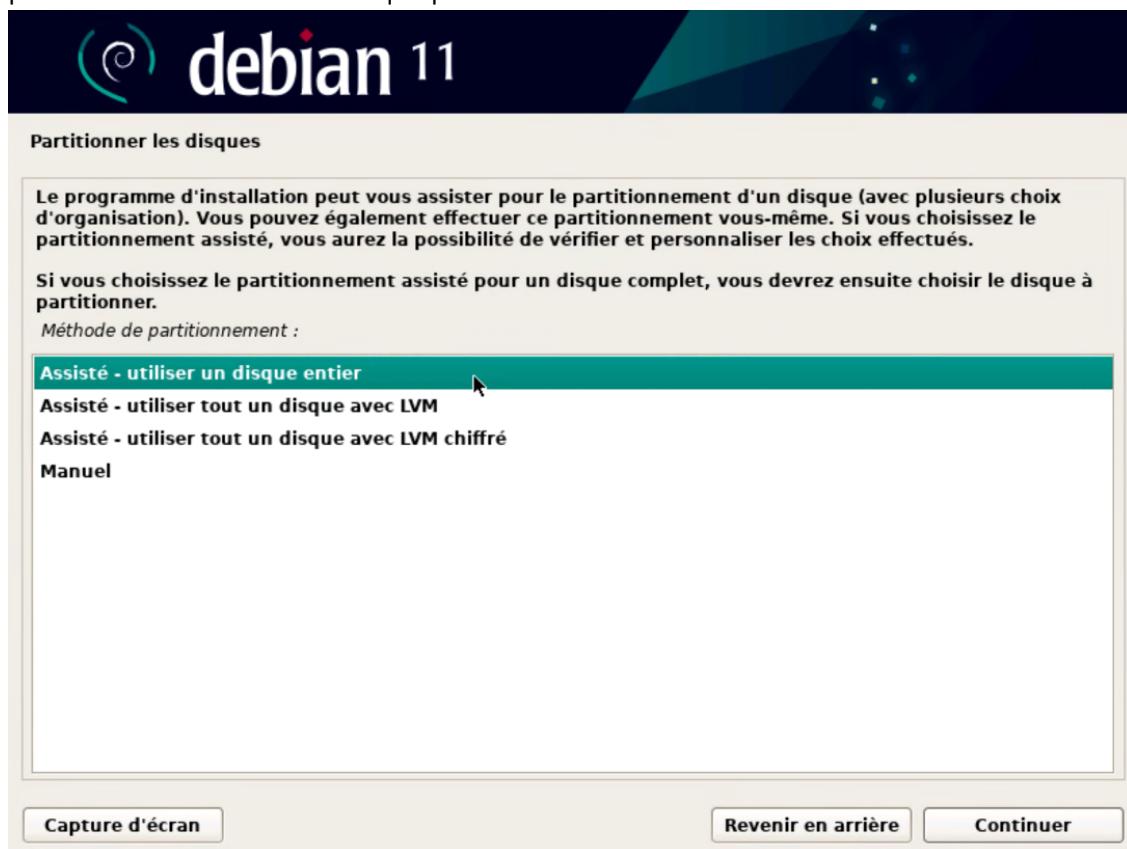


12. Choisissez ensuite un mot de passe pour l'utilisateur.

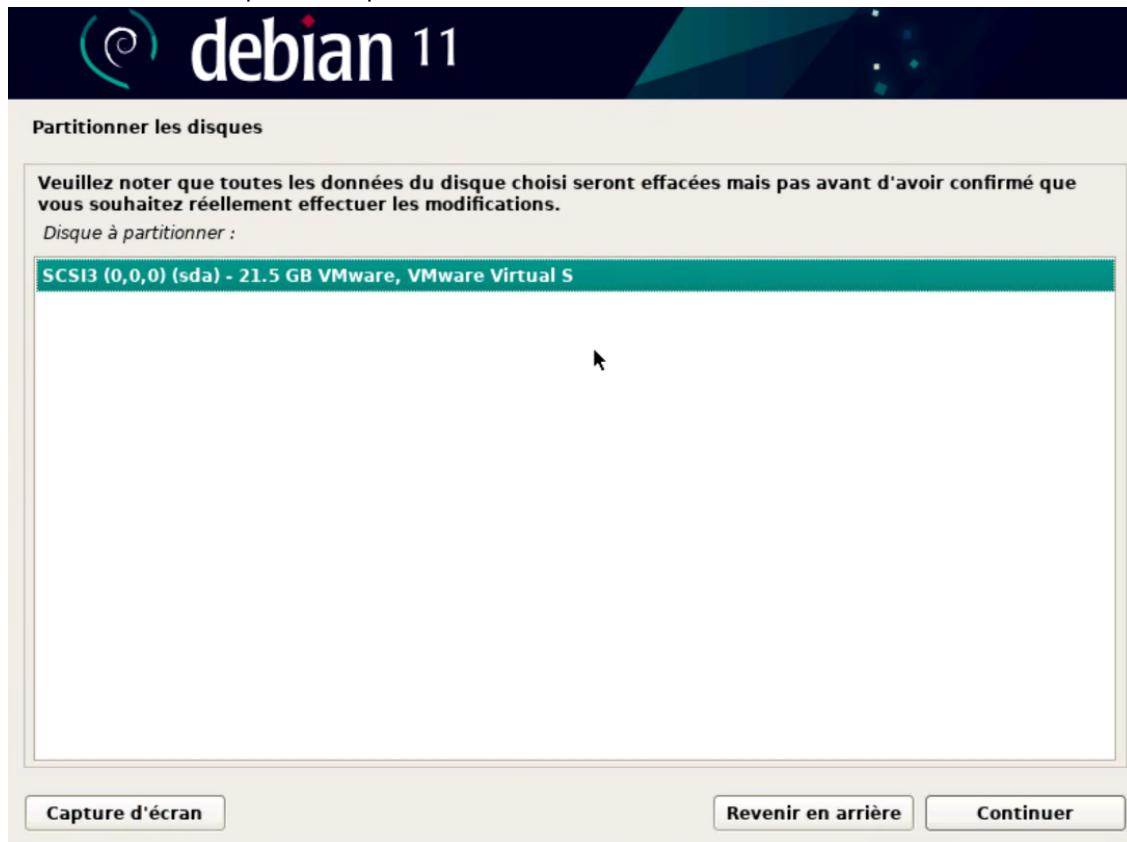


13. Confirmez le mot de passe et continuez

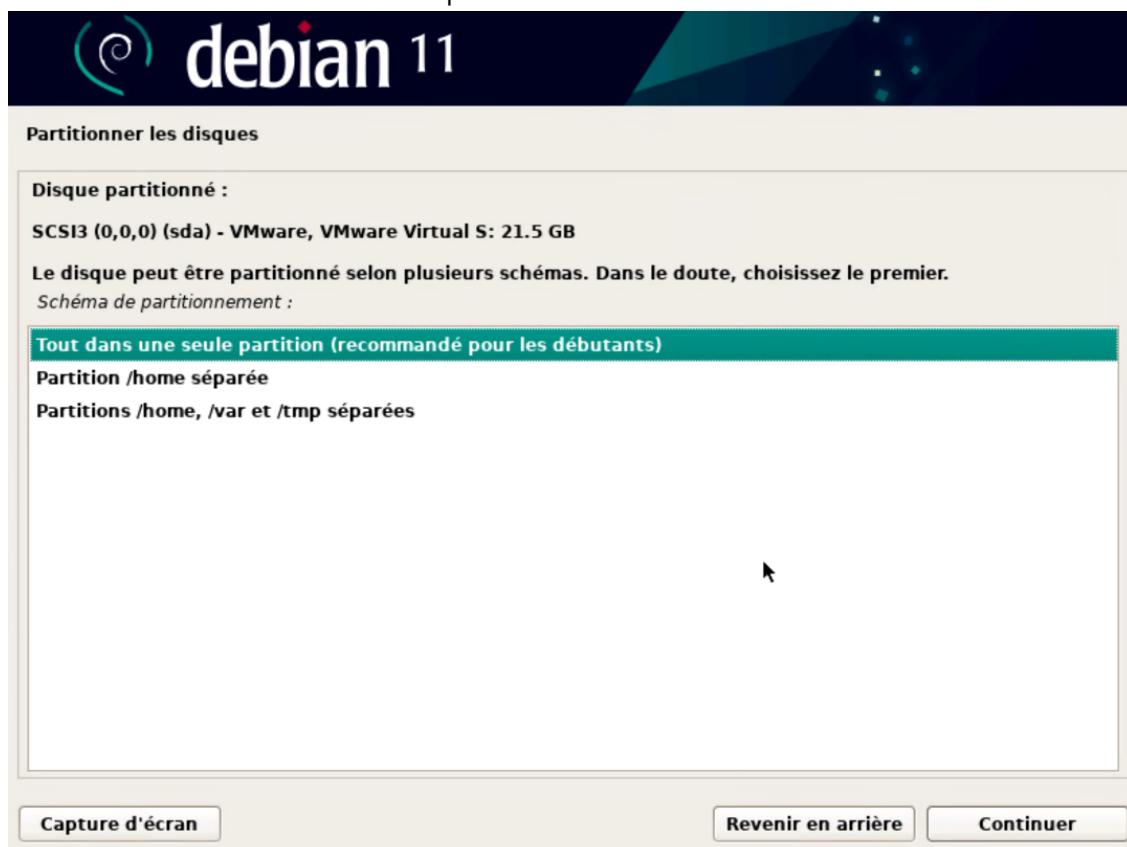
14. Sélectionnez « Assisté – utiliser un disque entier », n'ayant pas besoin de partitionnement particulier ou de chiffrer le disque pour l'utilisation de la clé



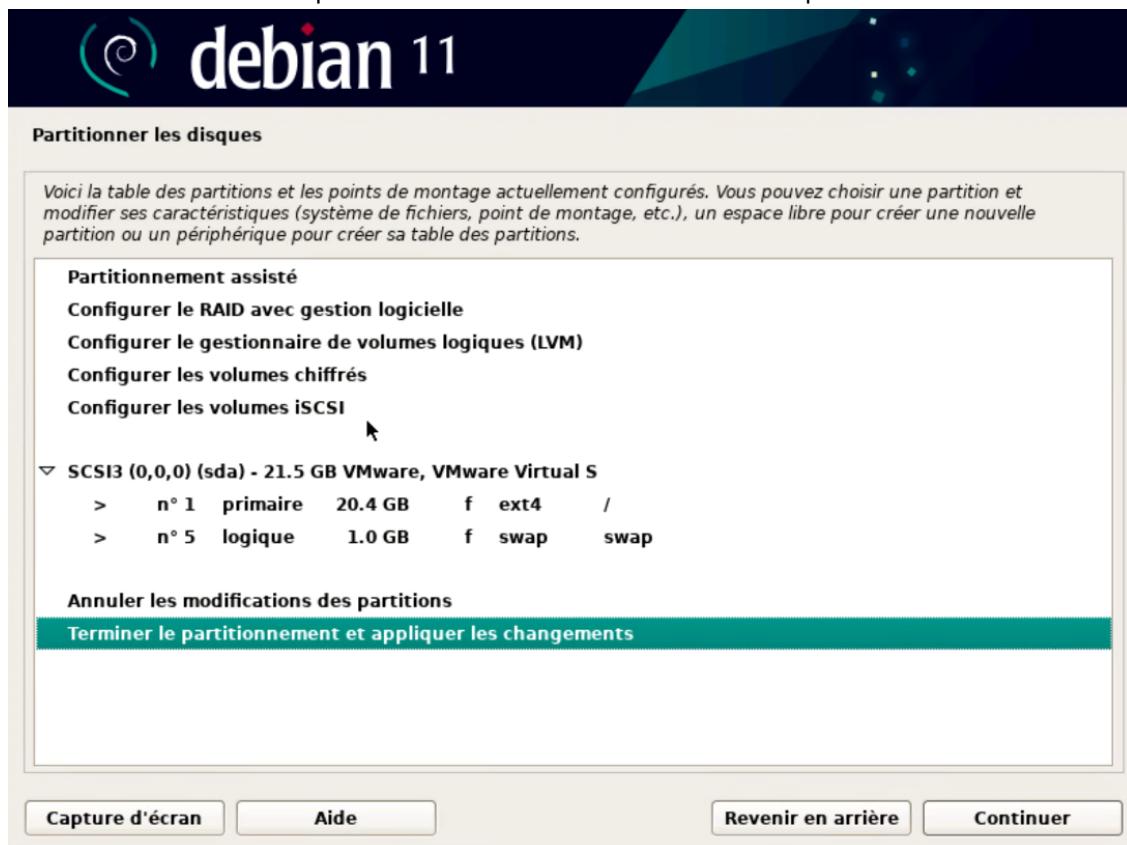
15. Sélectionnez le disque sur lequel vous souhaitez installer Debian (ici sda) et continuez



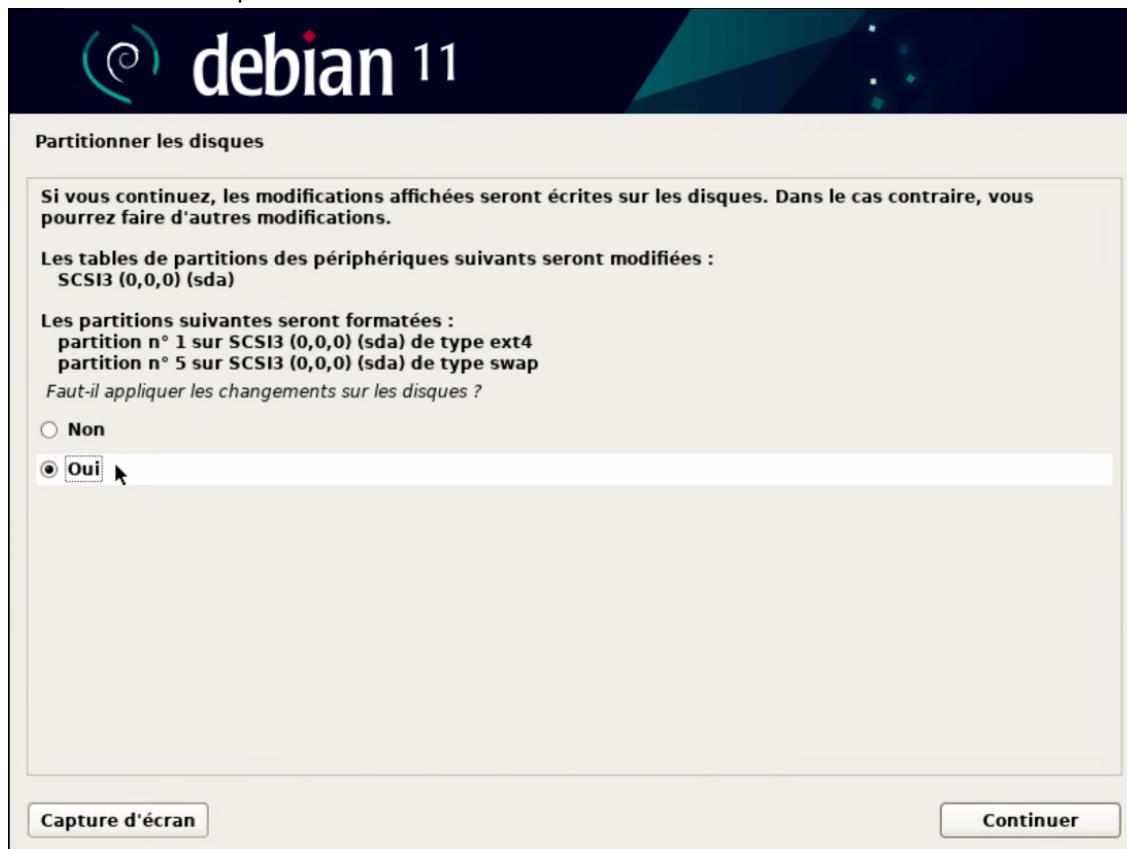
16. Sélectionnez « Tout dans une seule partition » et continuez



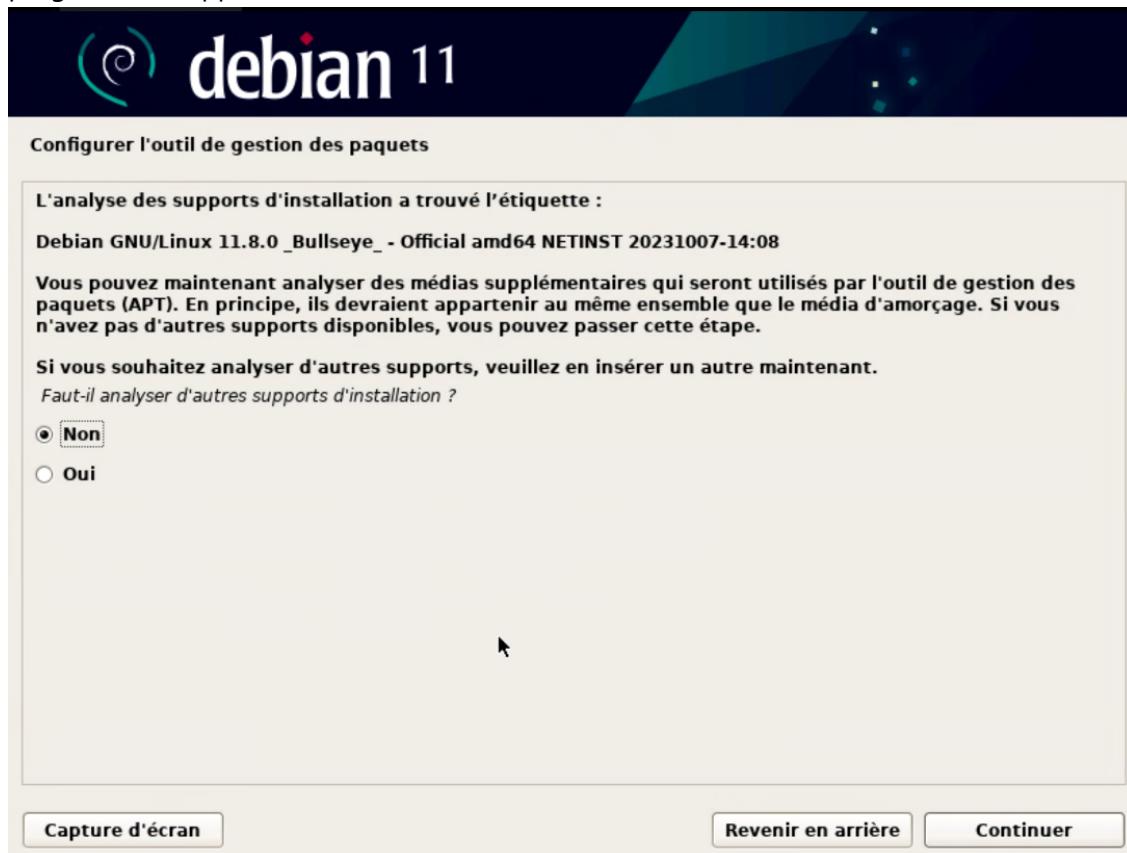
17. Choisissez « Continuer » pour valider les modifications sur le disque



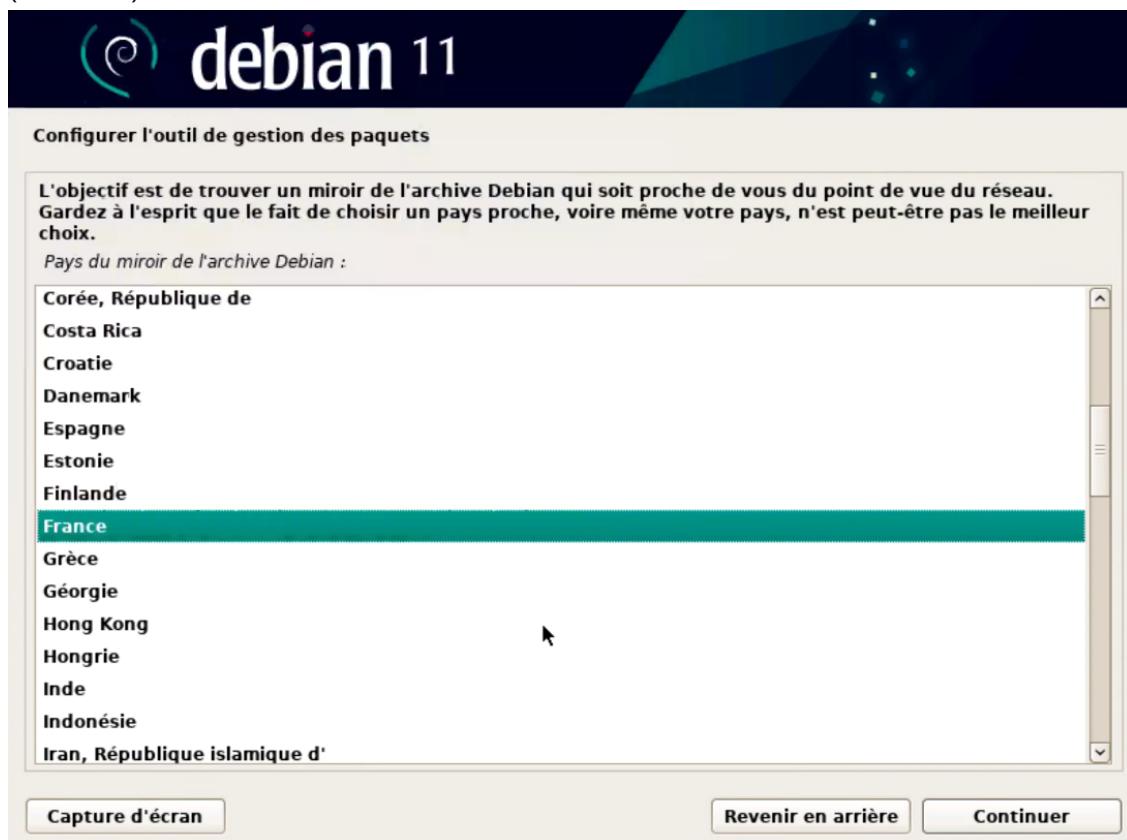
18. Choisissez « Oui » pour confirmer les écriture



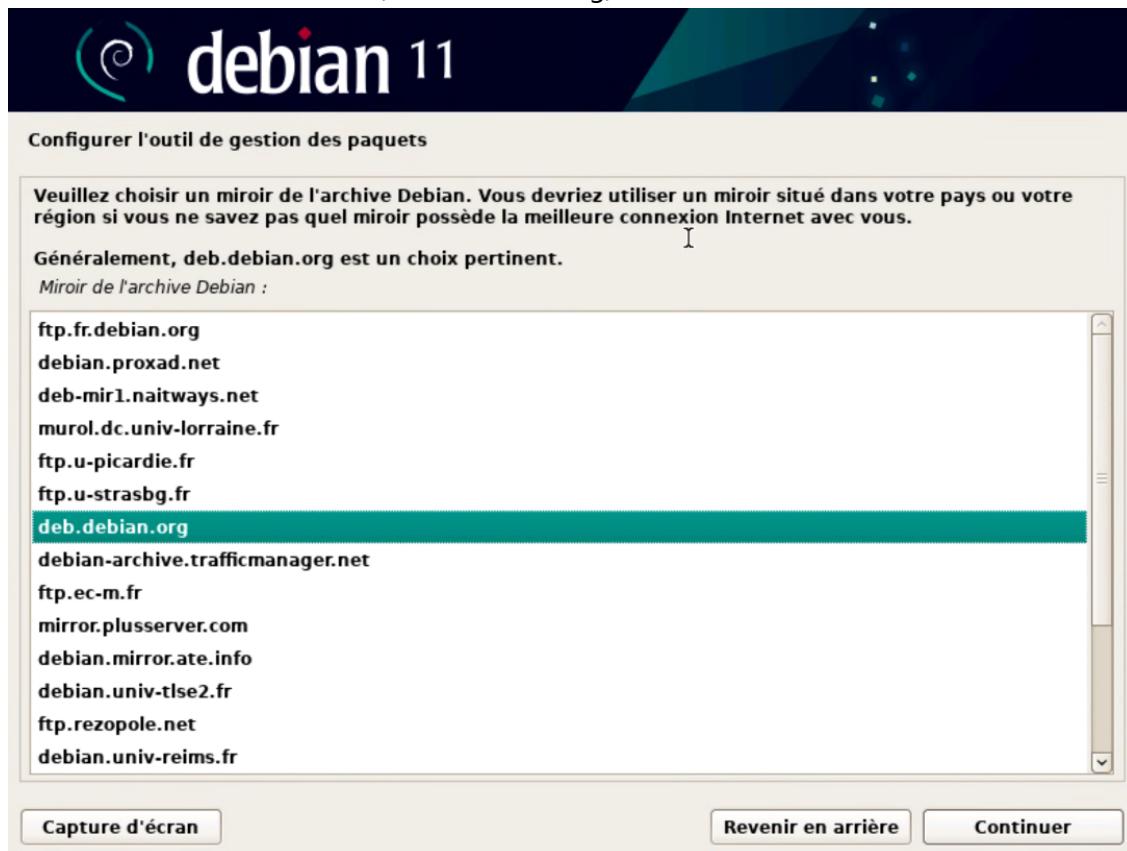
19. Si Debian vous demande si vous avez un autre support d'installation pour installer des programmes supplémentaires, cochez « non » et continuez



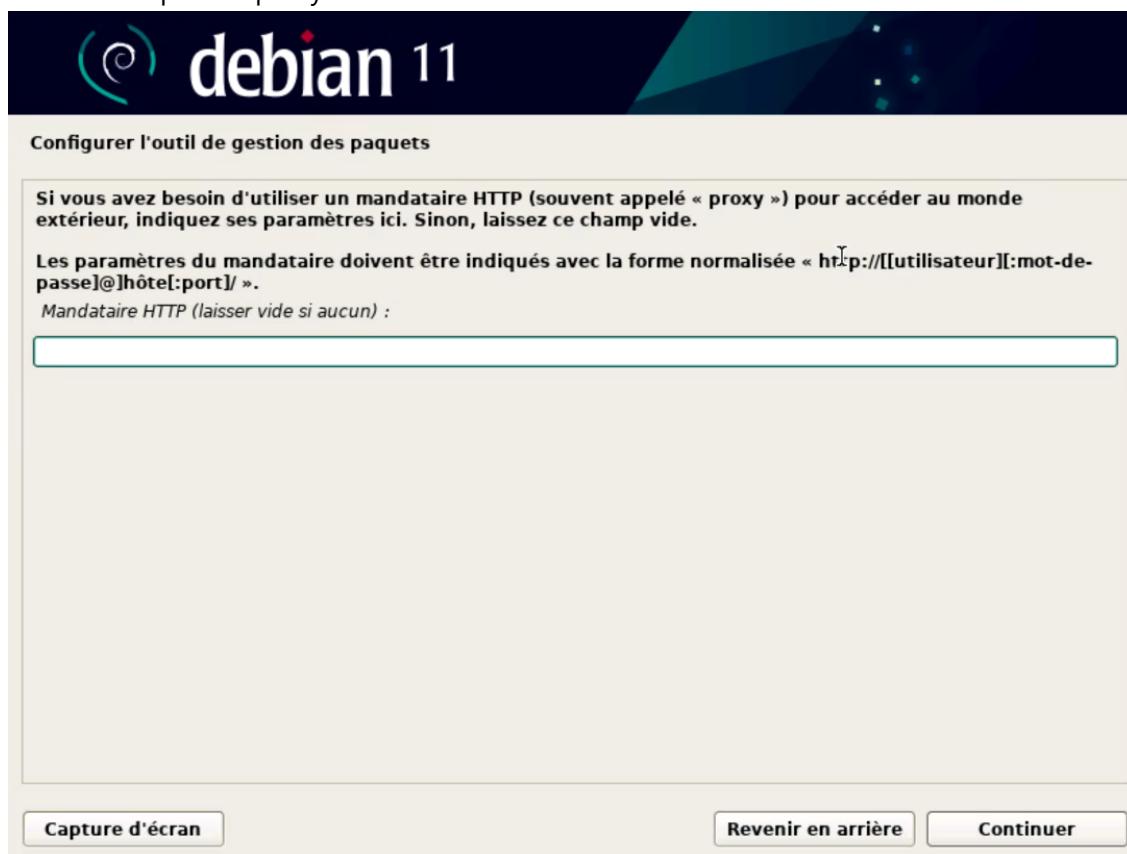
20. Faites continuer en sélectionnant le pays où est votre serveur l'outil de gestion des paquets
(ici France)



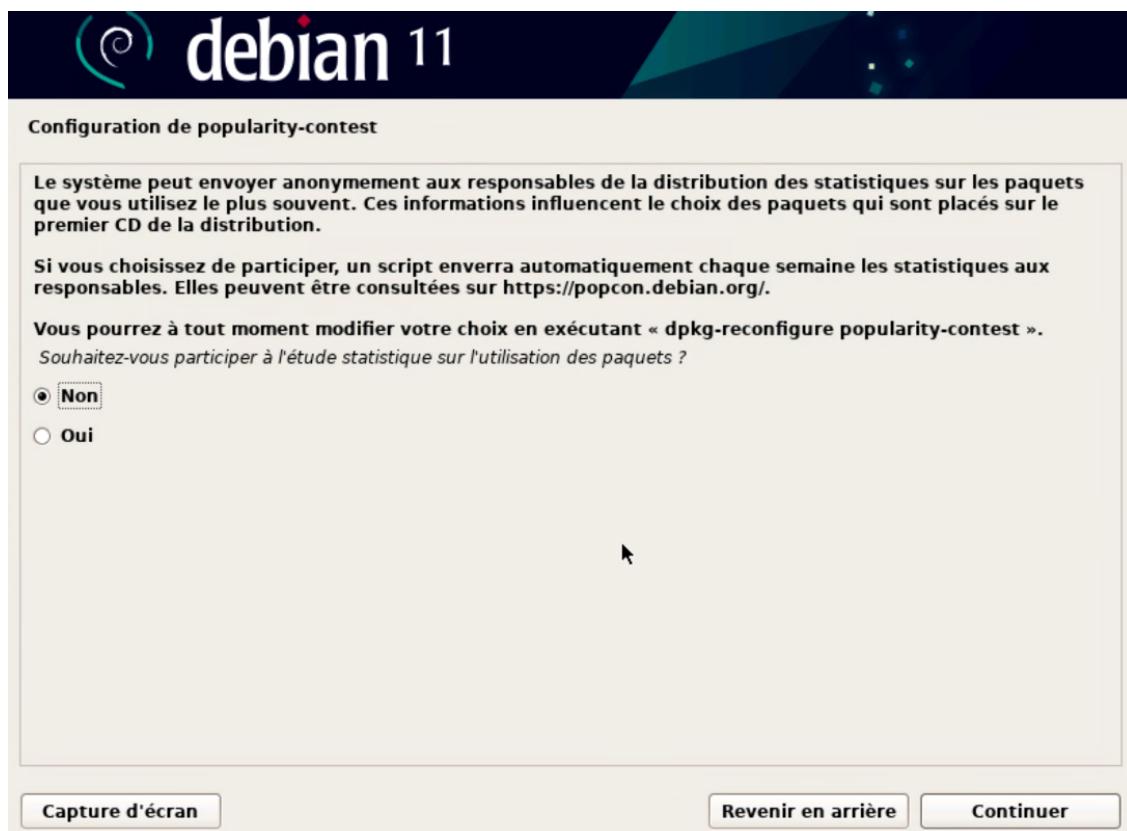
21. Sélectionnez le miroir Debian (ici deb.debian.org) et continuez



22. Laissez vide pour le proxy et continuez

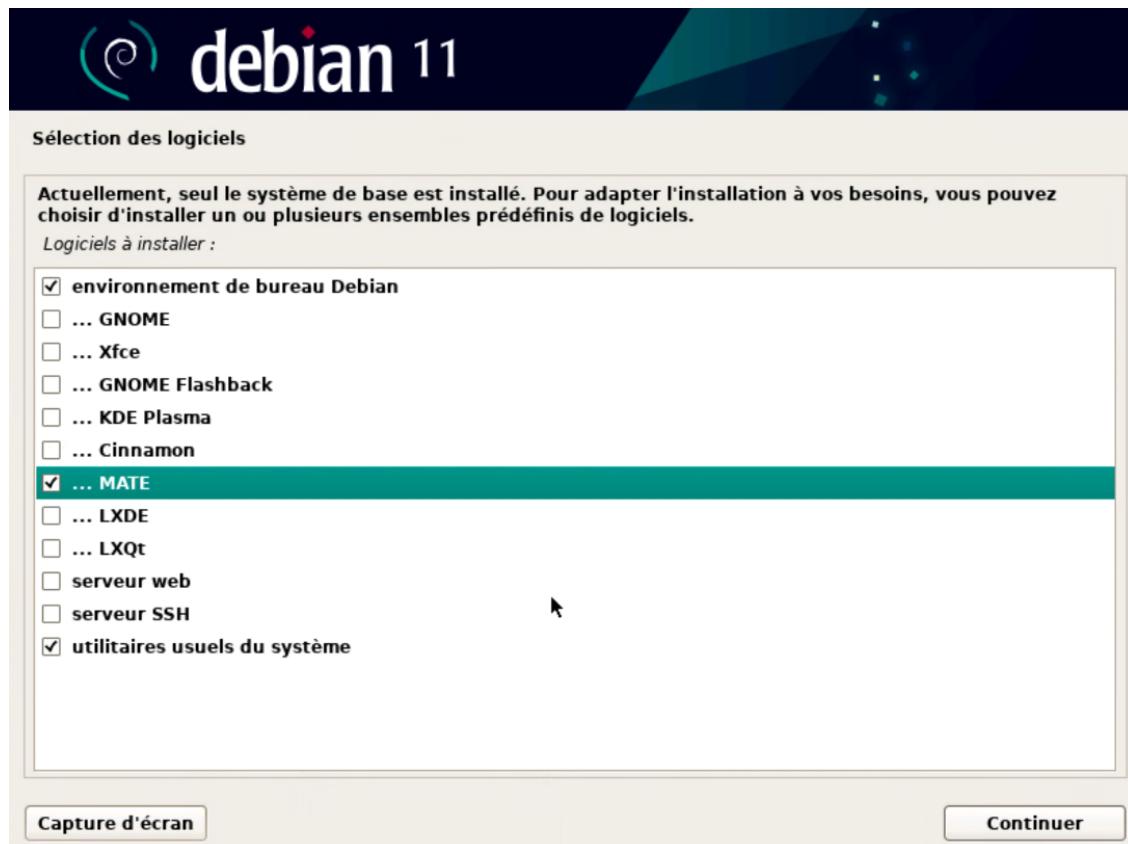


23. Si Debian vous demande si vous souhaitez participer à la « configuration popularity-contest » choisissez « non » et continuez



24. 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.

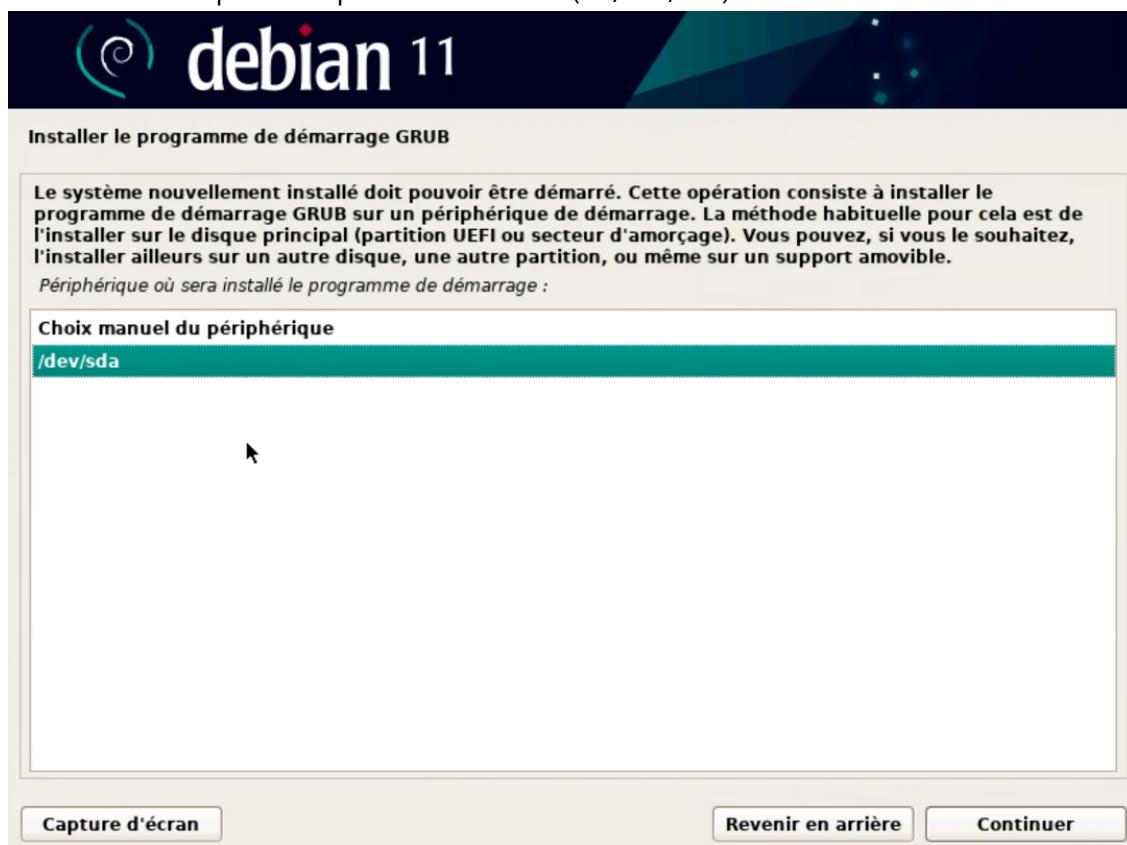


25. Faites continuer et patientez jusqu'à la fin de l'installation

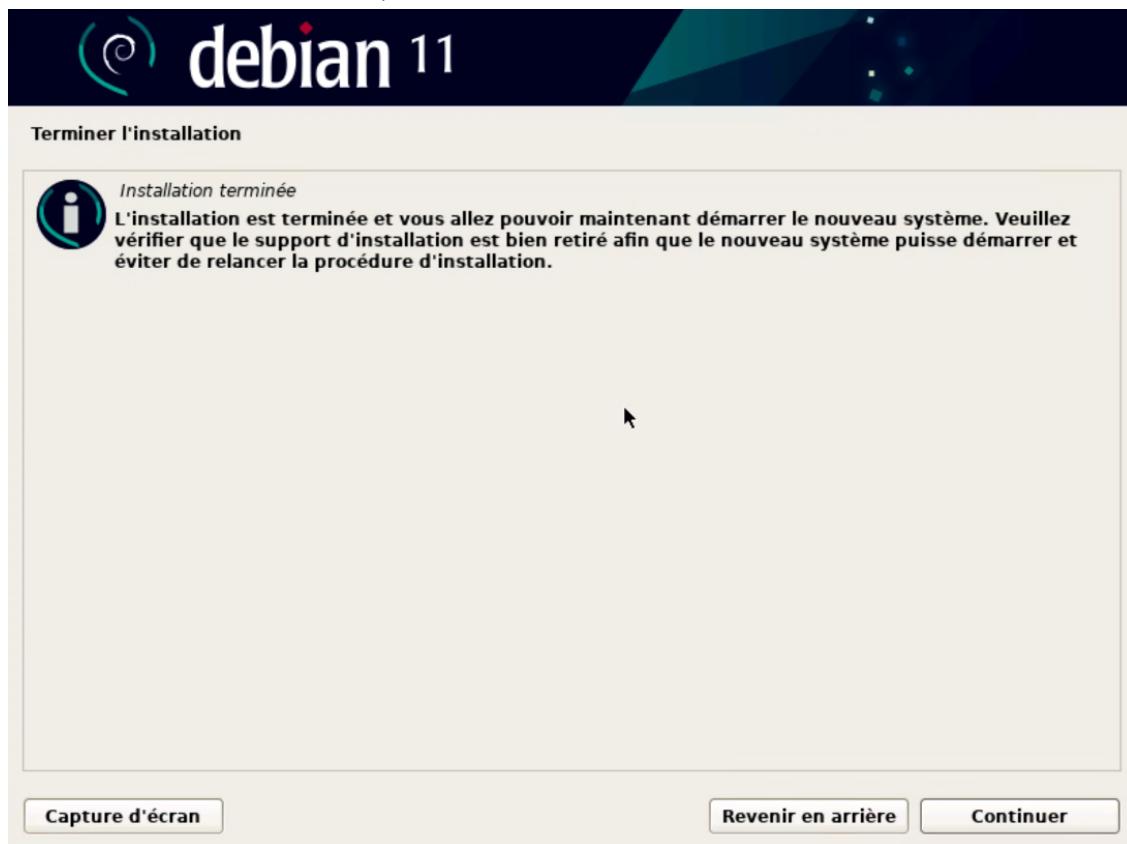
26. Une fois l'installation terminée, sélectionnez « Oui » pour installer le chargeur de démarrage GRUB sur la clé USB

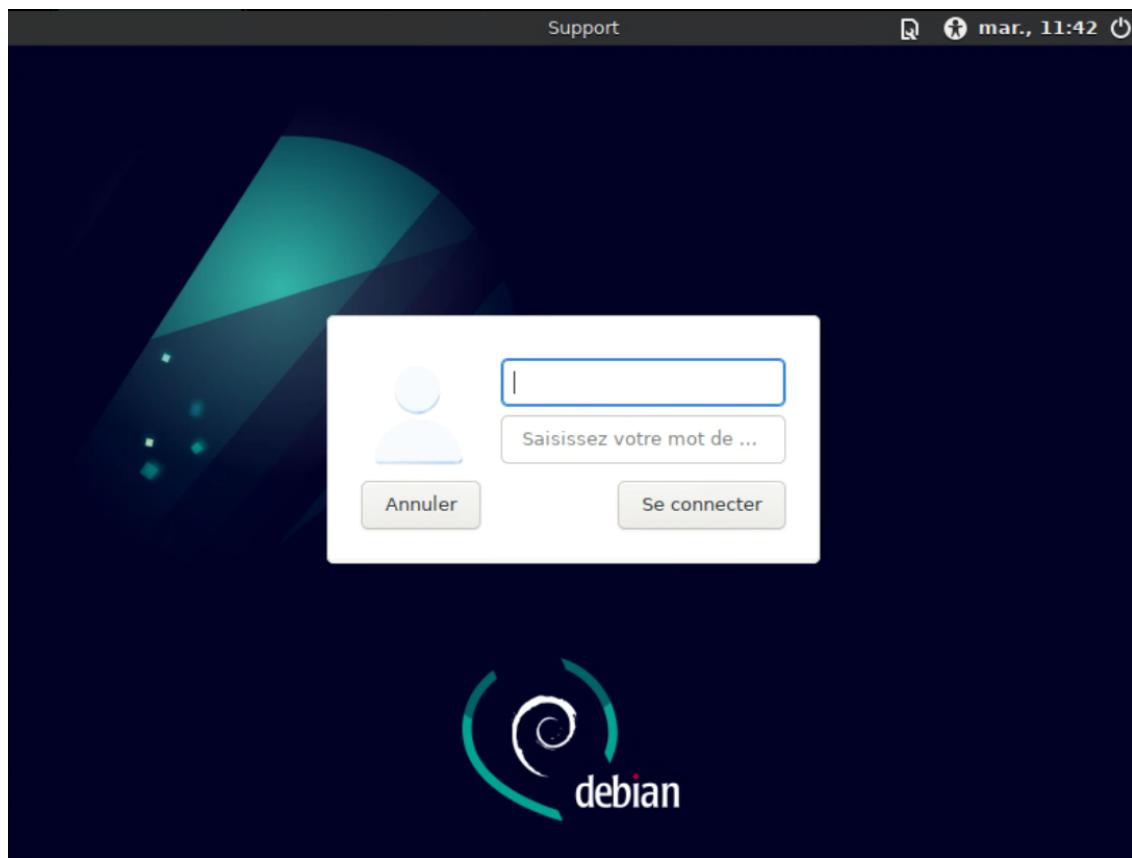


27. Choisissez le disque sur lequel installer GRUB (ici /dev/sda) et continuez



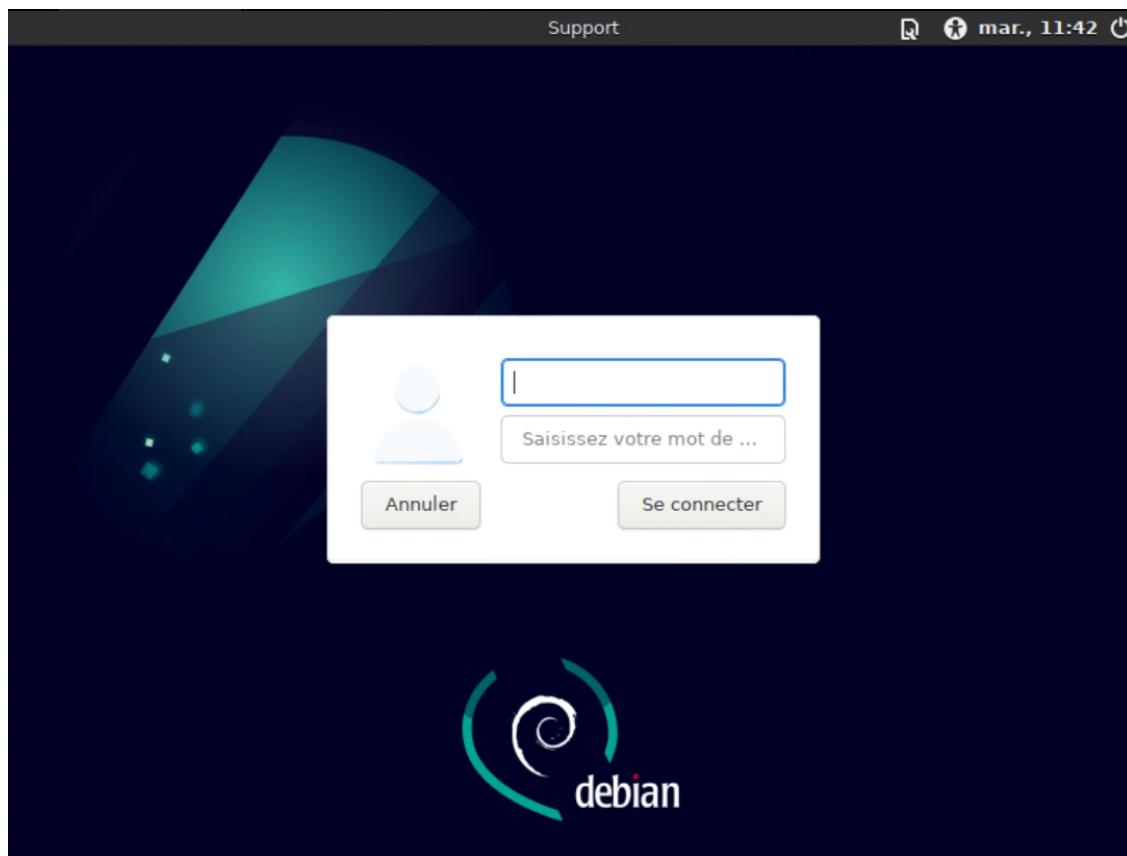
28. Une fois l'installation terminée, faites « Continuer » et retirez la clé USB une fois redémarré



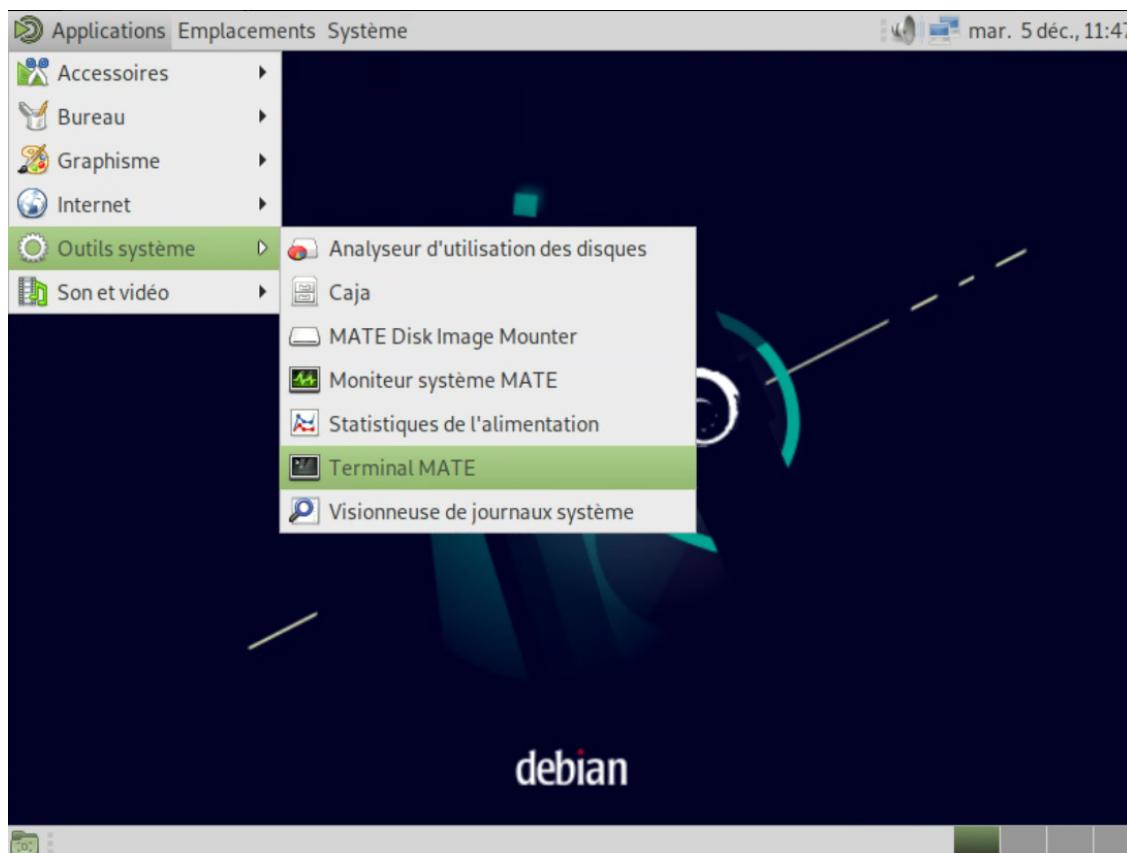


Installation des applications

1. Démarrez la Machine Virtuelle
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
```

The screenshot shows a terminal window titled "Terminal" with the following text output:

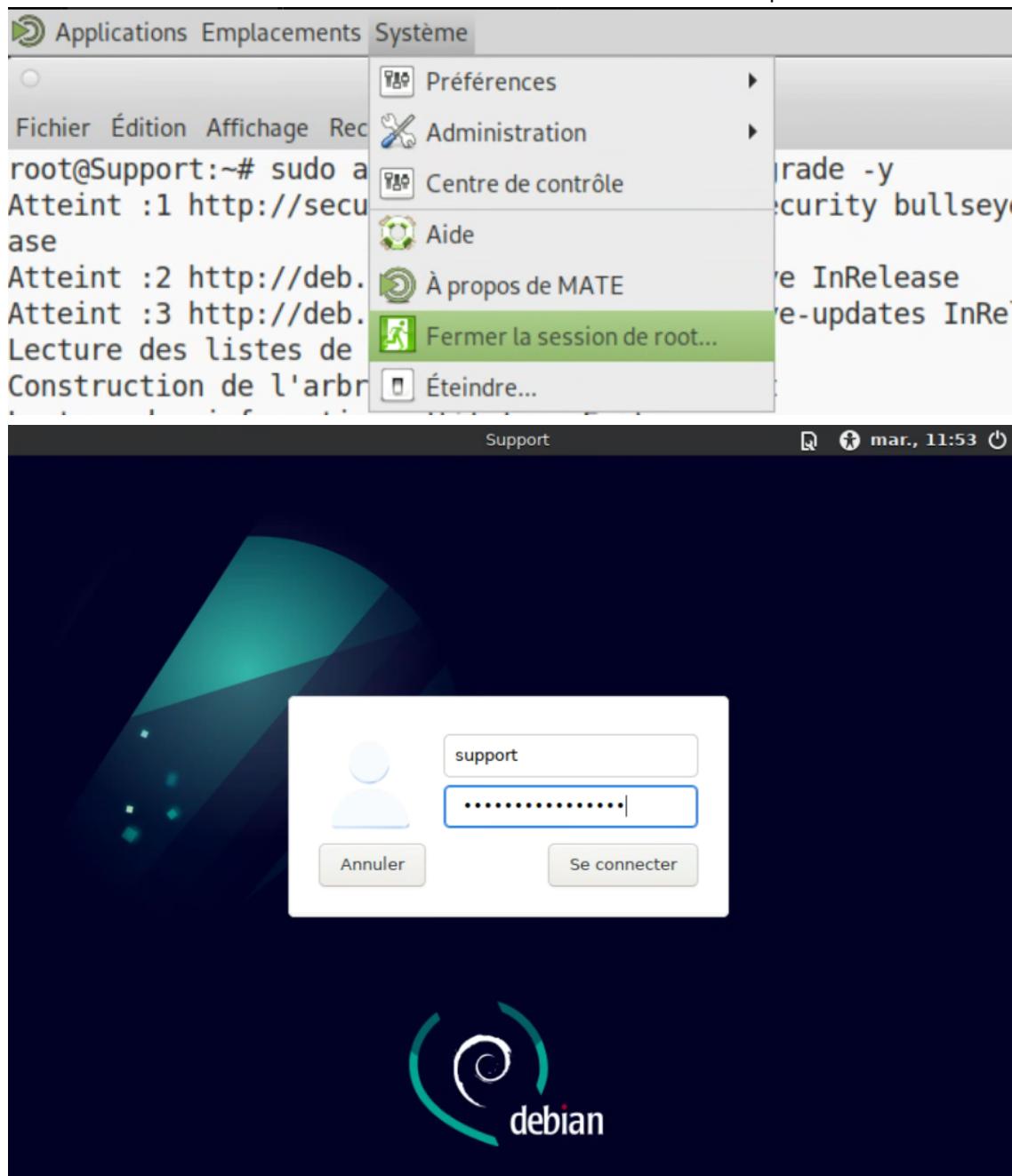
```
root@Support:~# sudo apt update && sudo apt upgrade -y
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
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@Support:~#
```

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@Support:~# sudo usermod -aG sudo support
root@Support:~# █
```

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



Installation de Tailscale

L'installation de Tailscale sur Debian 11 est assez simple, il suffit de lancez la commande suivante dans un terminal (CTRL+T) :

```
sudo apt install curl
curl -fsSL https://tailscale.com/install.sh | sh
```

```
support@Support: ~
Fichier Édition Affichage Recherche Terminal Aide
Après cette opération, 47,9 Mo d'espace disque supplémentaires seront utilisés.
Réception de :2 https://pkgs.tailscale.com/stable/debian bullseye/main all tails
cale-archive-keyring all 1.35.181 [3 082 B]
Réception de :1 https://pkgs.tailscale.com/stable/debian bullseye/main amd64 tai
lscalc amd64 1.54.1 [25,8 MB]
25,8 Mo réceptionnés en 4s (5 744 ko/s)
Sélection du paquet tailscale précédemment désélectionné.
(Lecture de la base de données... 148954 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../tailscale_1.54.1_amd64.deb ...
Dépaquetage de tailscale (1.54.1) ...
Sélection du paquet tailscale-archive-keyring précédemment désélectionné.
Préparation du dépaquetage de .../tailscale-archive-keyring_1.35.181_all.deb ...
Dépaquetage de tailscale-archive-keyring (1.35.181) ...
Paramétrage de tailscale-archive-keyring (1.35.181) ...
Paramétrage de tailscale (1.54.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/tailscaled.service →
 /lib/systemd/system/tailscaled.service.
+ [ false = true ]
+ set +x
Installation complete! Log in to start using Tailscale by running:

sudo tailscale up
support@Support:~$
```

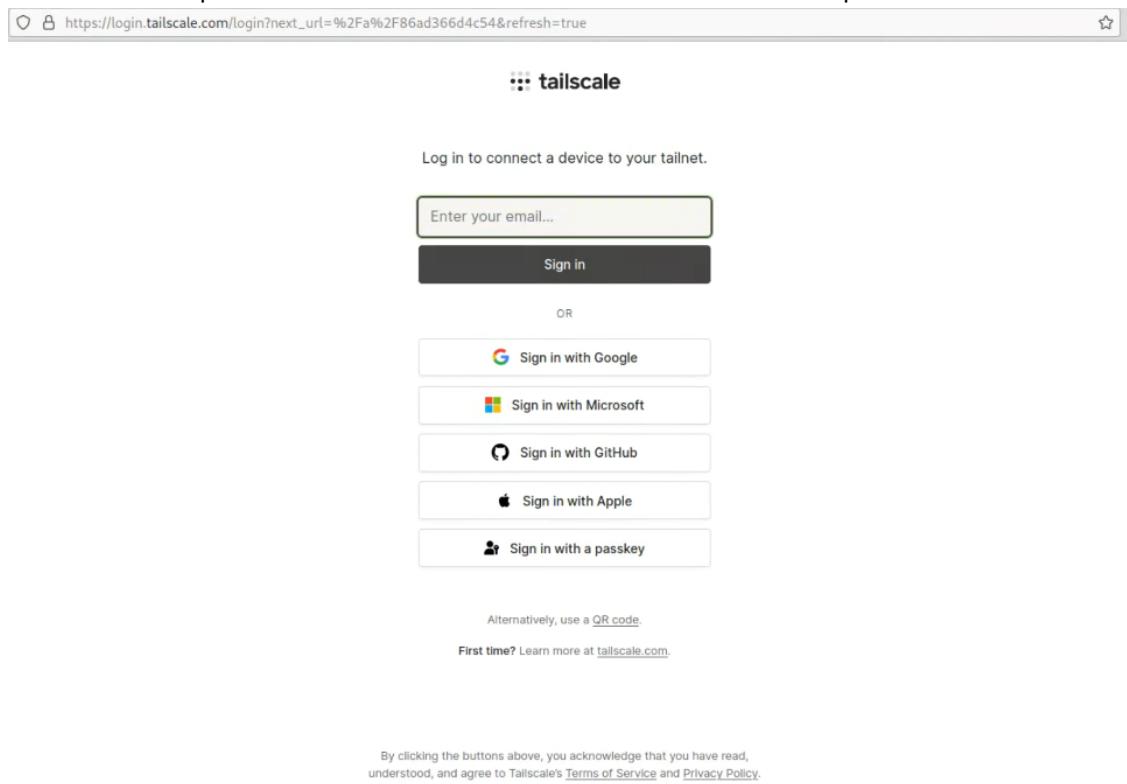
Configuration de Tailscale

1. Connectez vous à votre compte Tailscale en tapant la commande suivante dans un terminal (CTRL+T) :

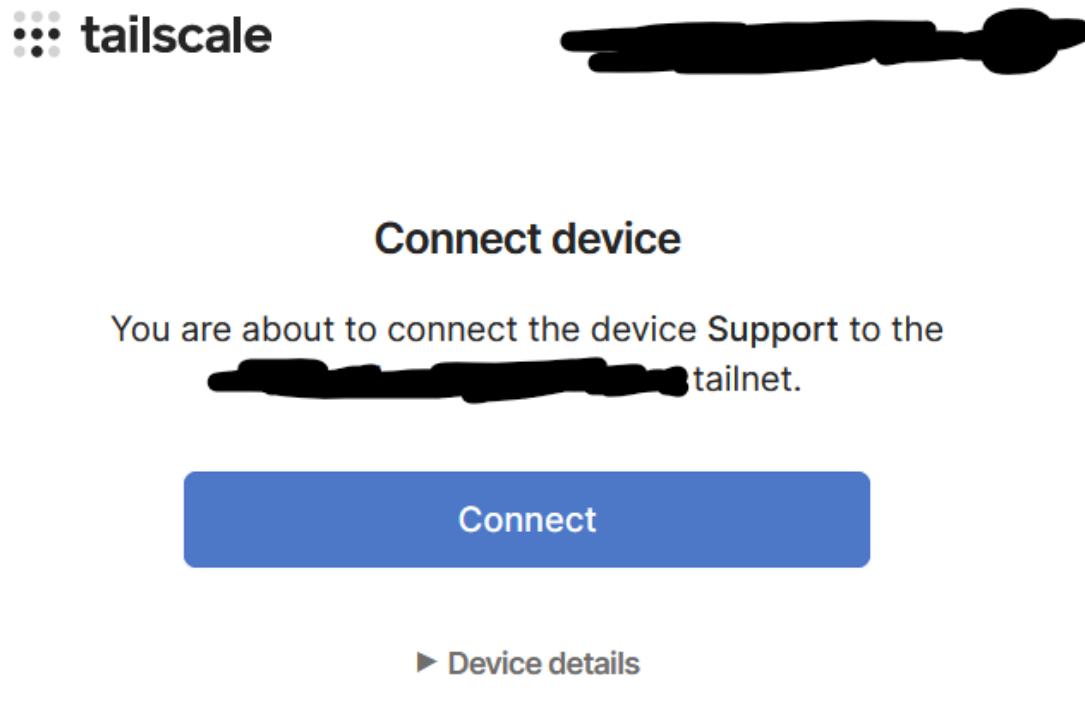
```
sudo tailscale up
```

```
support@Support:~$ sudo tailscale up
To authenticate, visit:
https://login.tailscale.com/a/86ad366d4c54
```

2. Allez sur le site pour vous connecter, et connectez vous à votre compte Tailscale



3. Cliquez sur "Connect" pour connecter le système à votre compte Tailscale



4. Désactivez l'expiration de la clé en cliquant sur "Disable key expiry" après avoir identifié le système nouvellement ajouté



5. Retournez sur le terminal et tapez la commande suivante :

```
sudo tailscale down
sudo tailscale up --ssh
sudo systemctl enable tailscaled
```

```
support@Support:~$ sudo tailscale up --ssh
support@Support:~$ sudo systemctl enable tailscaled
support@Support:~$
```

Cela nous permettra de connecter le système comme en VPN au serveur RustDesk et de pouvoir y accéder à distance via SSH dans le cas où RustDesk ne fonctionnerait pas

Installation de RustDesk

1. Téléchargez l'archive deb de RustDesk sur le [Github officiel](#)

The screenshot shows the GitHub repository page for 'rustdesk/rustdesk'. It highlights the '1.2.3' release. A prominent warning message in a red box reads: 'WARNING: YOU MAY BE BEING SCAMMED! If you are on the phone with someone you DON'T know AND TRUST who has asked you to install RustDesk, do not install and hang up immediately. They are likely a scammer trying to steal your money or other private information.' Below the release notes, it says 'Winget, FDroid update will come soon.' and provides download links for 'x86-64' (Windows, Ubuntu, Mac) and 'AArch64 (ARM64)' (Ubuntu, Android, Mac). There's also a link to 'More: check below please'.

2. Ouvrez un terminal (CTRL+T) et tapez les commandes suivantes :

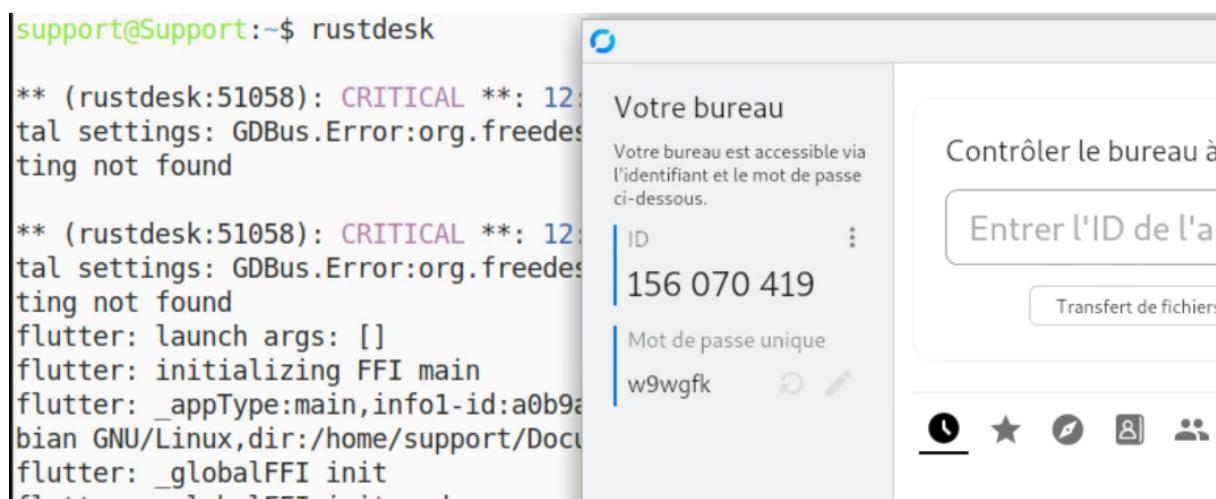
```
sudo apt install libxdo3 curl gstreamer1.0-pipewire
sudo dpkg -i ~/Téléchargement/NOM_DE_L_ARCHIVE.deb
sudo systemctl enable rustdesk
```

Cela installera les dépendances de RustDesk et RustDesk lui même, entrez votre mot de passe lorsque cela vous est demandé

```
support@Support: ~
Fichier Édition Affichage Recherche Terminal Aide
(Lecture de la base de données... 147996 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libxdo3_1%3a3.20160805.1-4_amd64.deb ...
Dépaquetage de libxdo3:amd64 (1:3.20160805.1-4) ...
Sélection du paquet curl précédemment désélectionné.
Préparation du dépaquetage de .../curl_7.74.0-1.3+deb11u10_amd64.deb ...
Dépaquetage de curl (7.74.0-1.3+deb11u10) ...
Sélection du paquet gstreamer1.0-pipewire:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../gstreamer1.0-pipewire_0.3.19-4_amd64.deb ...
Dépaquetage de gstreamer1.0-pipewire:amd64 (0.3.19-4) ...
Paramétrage de gstreamer1.0-pipewire:amd64 (0.3.19-4) ...
Paramétrage de libxdo3:amd64 (1:3.20160805.1-4) ...
Paramétrage de curl (7.74.0-1.3+deb11u10) ...
Paramétrage de rustdesk (1.2.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/rustdesk.service →
/lib/systemd/system/rustdesk.service.
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u7)
) ...
support@Support:~$ █
support@Support:~$ sudo dpkg -i ~/Téléchargements/rustdesk-1.2.3-x86_64.deb
Sélection du paquet rustdesk précédemment désélectionné.
(Lecture de la base de données... 147899 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../rustdesk-1.2.3-x86_64.deb ...
Failed to stop rustdesk.service: Unit rustdesk.service not loaded.
Dépaquetage de rustdesk (1.2.3) ...
Paramétrage de rustdesk (1.2.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/rustdesk.service →
/lib/systemd/system/rustdesk.service.
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1) ...
Traitement des actions différées (« triggers ») pour mailcap (3.69) ...
Traitement des actions différées (« triggers ») pour hicolor-icon-theme (0.17-2) ...
support@Support:~$
```

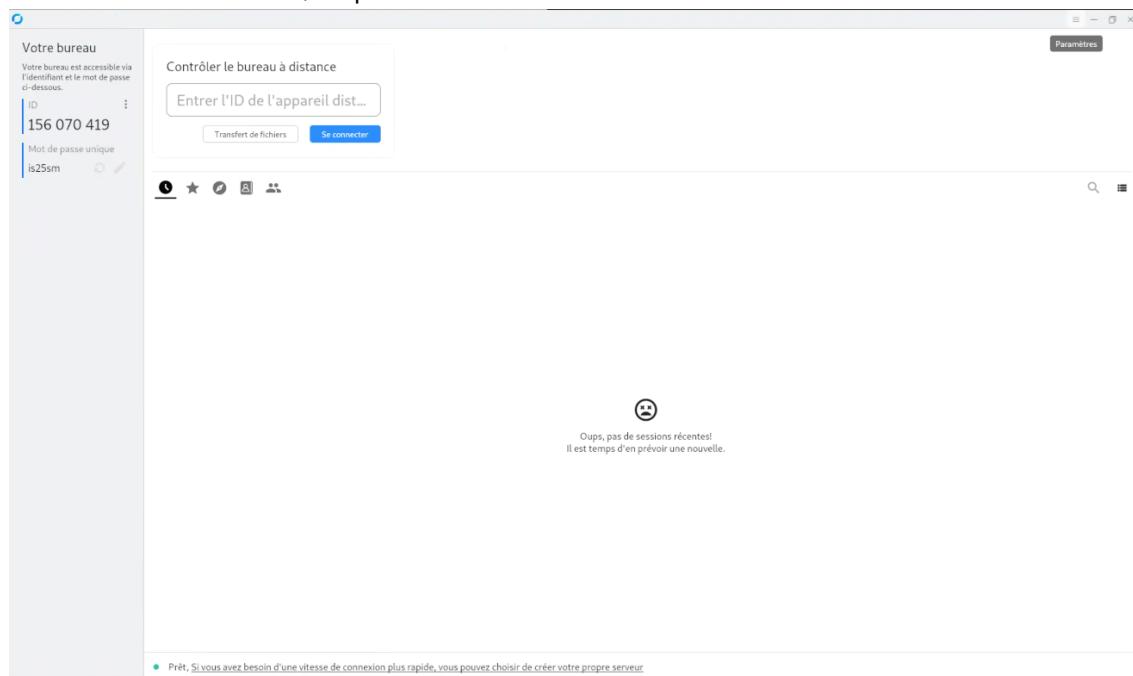
3. Lancez ensuite RustDesk en tapant la commande suivante dans un terminal (CTRL+T) :

```
rustdesk
```

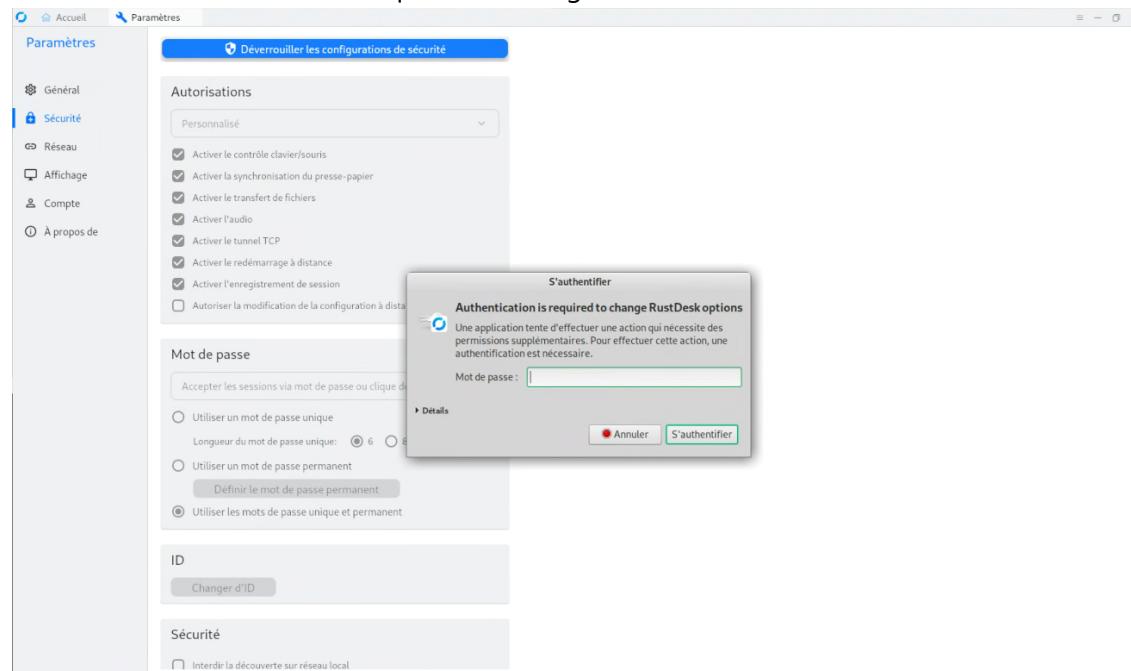


Configuration de RustDesk

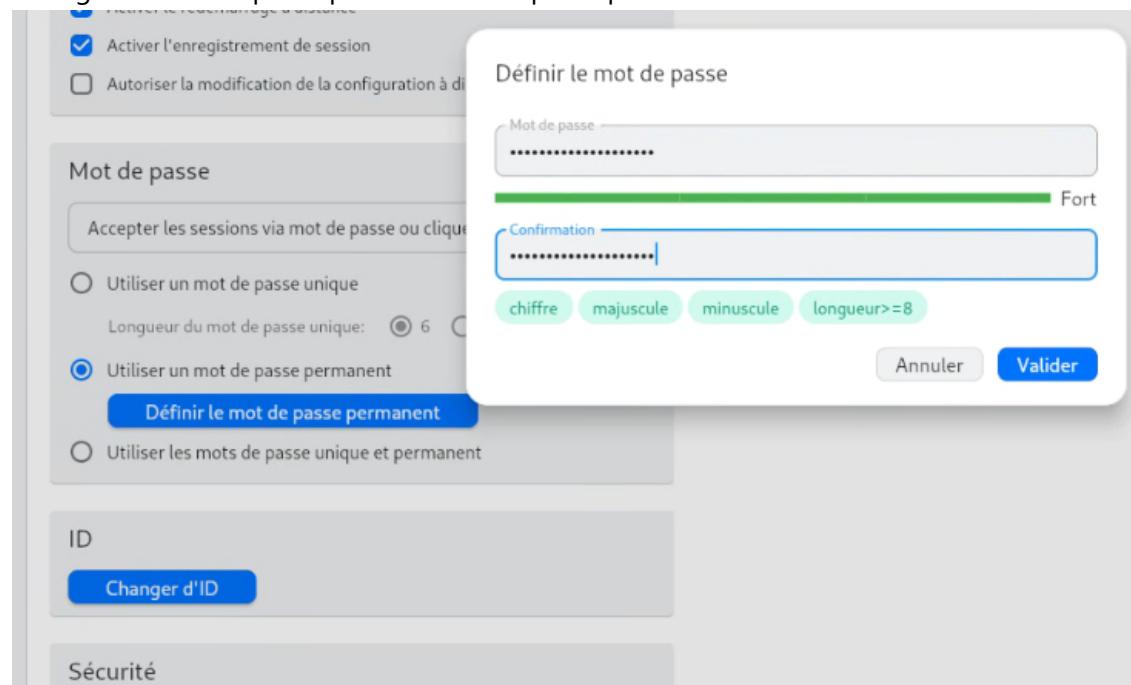
1. Une fois RustDesk lancé, cliquez sur les trois tirets en haut à droite



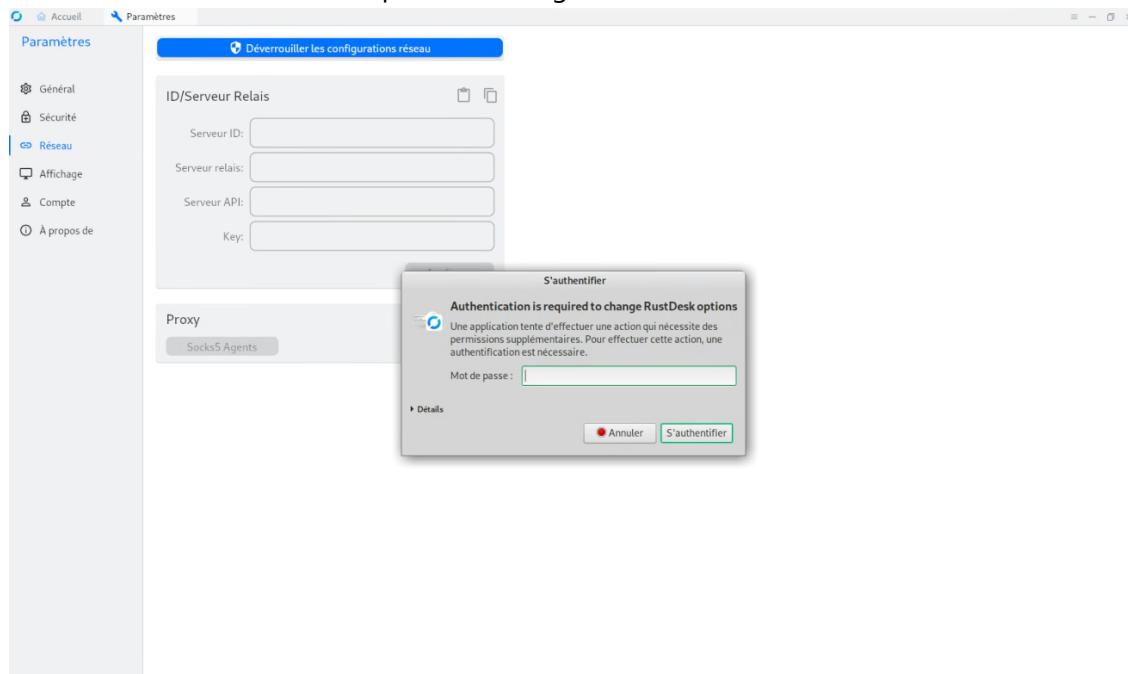
2. Allez dans "Sécurité" et "débloquez" les configurations de sécurité



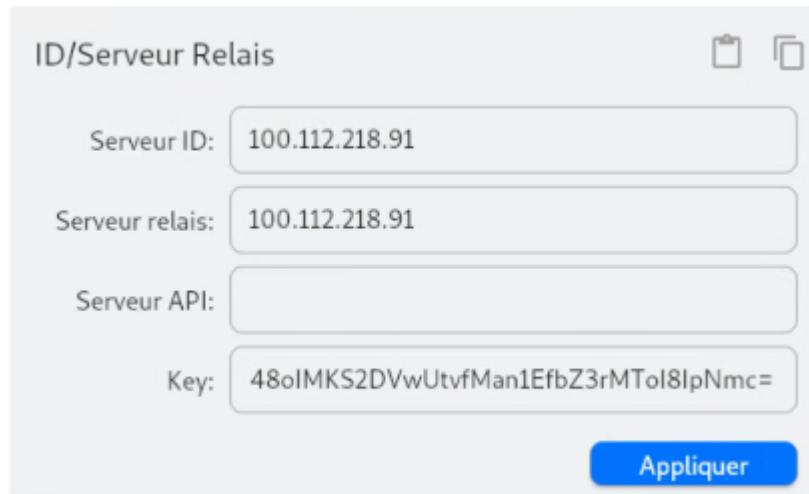
3. Changez le mot de passe pour un mot de passe permanent et définissez-le



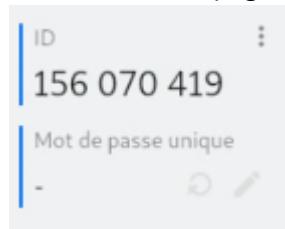
4. Allez dans "Réseau" et "débloquez" les configurations de réseau



5. Mettez dans "Serveur ID" et "Serveur Relay" l'adresse IP que vous avez noté lors de l'installation du serveur RustDesk ainsi que la clé publique que vous avez copié dans "Key" puis faites "Appliquer"



6. Revenez dans la page d'accueil et récupérez l'ID RustDesk du Debian



Vous pouvez désormais vous connecter à distance à votre Debian via RustDesk en utilisant l'ID que vous avez récupéré

Notez également que RustDesk se lancera automatiquement au démarrage de Debian, l'interface elle sera accessible en utilisant la commande `rustdesk` dans un terminal (CTRL+T)

Installation de Chntpw

- Ouvrez un terminal (CTRL+T) et tapez la commande suivante :

```
sudo apt install chntpw
```

```
support@Support:~$ sudo apt install chntpw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  filezilla-common libfilezillall libpugixml1v5 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  chntpw
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 91,9 ko dans les archives.
Après cette opération, 404 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 chntpw amd64 1.0-1.1 [91,9 kB]
91,9 ko réceptionnés en 0s (680 ko/s)
Sélection du paquet chntpw précédemment désélectionné.
(Lecture de la base de données... 148959 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../chntpw_1.0-1.1_amd64.deb ...
Dépaquetage de chntpw (1.0-1.1) ...
Paramétrage de chntpw (1.0-1.1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
support@Support:~$
```

- Vérifiez que l'installation s'est bien déroulée en tapant la commande suivante :

```
sudo chntpw -h
```

```
support@Support:~$ sudo chntpw -h
chntpw: change password of a user in a Windows SAM file,
or invoke registry editor. Should handle both 32 and 64 bit windows and
all version from NT3.x to Win8.1
chntpw [OPTIONS] <samfile> [systemfile] [securityfile] [otherreghive] [...]
-h      This message
-u <user> Username or RID (0x3e9 for example) to interactively edit
-l      list all users in SAM file and exit
-i      Interactive Menu system
-e      Registry editor. Now with full write support!
-d      Enter buffer debugger instead (hex editor),
-v      Be a little more verbose (for debugging)
-L      For scripts, write names of changed files to /tmp/changed
-N      No allocation mode. Only same length overwrites possible (very safe mode)
-E      No expand mode, do not expand hive file (safe mode)

Usernames can be given as name or RID (in hex with 0x first)

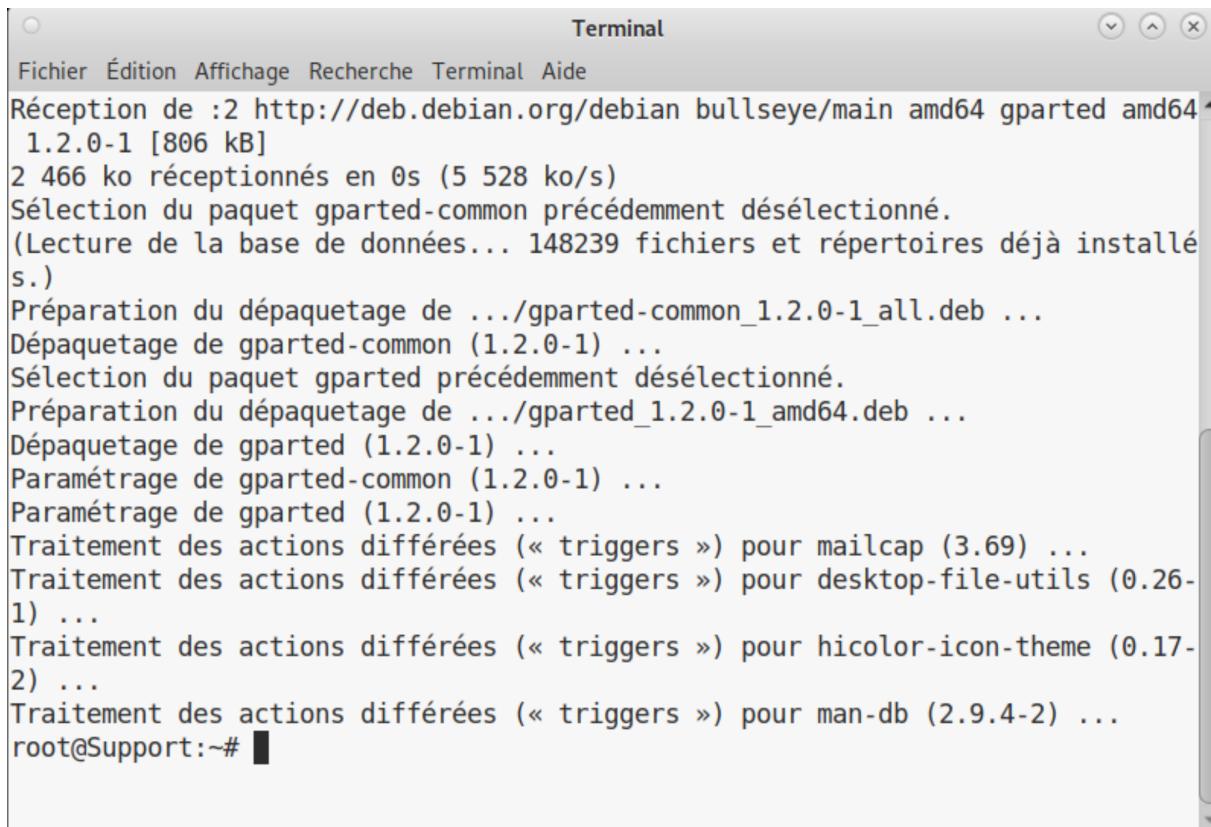
See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.
NOTE: This program is somewhat hackish! You are on your own!
support@Support:~$
```

Cela nous permettra de réinitialiser le mot de passe d'un utilisateur Windows si celui-ci est perdu

Installation de Gparted

1. Ouvrez un terminal (CTRL+T) et tapez la commande suivante :

```
sudo apt install gparted
```



```
Terminal
Fichier Édition Affichage Recherche Terminal Aide
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 gparted amd64 1.2.0-1 [806 kB]
2 466 ko réceptionnés en 0s (5 528 ko/s)
Sélection du paquet gparted-common précédemment désélectionné.
(Lecture de la base de données... 148239 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../gparted-common_1.2.0-1_all.deb ...
Dépaquetage de gparted-common (1.2.0-1) ...
Sélection du paquet gparted précédemment désélectionné.
Préparation du dépaquetage de .../gparted_1.2.0-1_amd64.deb ...
Dépaquetage de gparted (1.2.0-1) ...
Paramétrage de gparted-common (1.2.0-1) ...
Paramétrage de gparted (1.2.0-1) ...
Traitement des actions différées (« triggers ») pour mailcap (3.69) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1) ...
Traitement des actions différées (« triggers ») pour hicolor-icon-theme (0.17-2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@Support:~#
```

Cela nous permettra de monter plus facilement le disque Windows d'une machine sur lequel il faut intervenir

Installation de memtest86+

1. Ouvrez un terminal (CTRL+T) et tapez la commande suivante :

```
sudo apt install memtest86+
```

```
support@Support:~$ sudo apt install memtest86+
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  filezilla-common libfilezillall libpugixml1v5 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Paquets suggérés :
  hwtools memtester kernel-patch-badram memtest86 mtools
Les NOUVEAUX paquets suivants seront installés :
  memtest86+
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 77,8 ko dans les archives.
Après cette opération, 2 448 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 memtest86+ amd64 5.01-3.1 [77,8 kB]
77,8 ko réceptionnés en 0s (917 ko/s)
Préconfiguration des paquets...
Sélection du paquet memtest86+ précédemment désélectionné.
(Lecture de la base de données... 148973 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../memtest86+_5.01-3.1_amd64.deb ...
Dépaquetage de memtest86+ (5.01-3.1) ...
Paramétrage de memtest86+ (5.01-3.1) ...
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-5.10.0-26-amd64
Found initrd image: /boot/initrd.img-5.10.0-26-amd64
Found memtest86+ image: /boot/memtest86+.bin
Found memtest86+ multiboot image: /boot/memtest86+_multiboot.bin
Warning: os-prober will be executed to detect other bootable partitions.
Its output will be used to detect bootable binaries on them and create new boot entries.
done
support@Support:~$
```

Cela nous permettra de tester la RAM d'un ordinateur si celui-ci est lent ou si des erreurs apparaissent

Installation de BleachBit

1. Ouvrez un terminal (CTRL+T) et tapez la commande suivante :

```
sudo apt install bleachbit
```

```

support@Support:~$ sudo apt install bleachbit
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  filezilla-common libfilezilla11 libpugixml1v5 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  bleachbit
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 427 ko dans les archives.
Après cette opération, 2 439 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 bleachbit all 3.9.0-1 [427 kB]
427 ko réceptionnés en 0s (3 046 ko/s)
Sélection du paquet bleachbit précédemment désélectionné.
(Lecture de la base de données... 148990 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../bleachbit_3.9.0-1_all.deb ...
Dépaquetage de bleachbit (3.9.0-1) ...
Paramétrage de bleachbit (3.9.0-1) ...
/usr/share/bleachbit/bleachbit/_init__.py:260: SyntaxWarning: "is not" with a literal. Did you mean "!="?
  if msgctxt is not None and msgctxt is not "":
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour mailcap (3.69) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1) ...
support@Support:~$ 

```

2. Vérifiez que l'installation s'est bien déroulée en tapant la commande suivante :

```
sudo bleachbit -h
```

```

support@Support:~$ sudo bleachbit -h
chown for path /root aborted
chown for path /root aborted
Préservation automatique de la langue fr.
Préservation automatique de la langue fr.
Usage: utilisation : bleachbit [options] nettoyeur.option1 nettoyeur.option2

Options:
  -h, --help          show this help message and exit
  -l, --list-cleaners    lister les nettoyeurs
  -c, --clean          exécuter les nettoyeurs pour supprimer les fichiers et
                      réaliser d'autres modifications permanentes
  --debug             Régler le niveau de journalisation à verbeux
  --debug-log=DEBUG_LOG      enregistrer les messages de débogage dans un fichier
  -s, --shred          détruire des fichiers ou des dossiers spécifiques
  --sysinfo            afficher les informations système
  --gui                lancer l'interface graphique
  -p, --preview        prévisualiser les fichiers à supprimer et autres
                      modifications
  --preset             utiliser les options définies dans l'interface
                      graphique
  -W, --wipe-free-space    écraser l'espace libre dans les chemins d'accès donnés
  -v, --version         afficher les informations de version et quitter
  -o, --overwrite       écraser les fichiers pour masquer leur contenu
support@Support:~$ 

```

Cela nous permettra de nettoyer les fichiers temporaires du système Debian pour alléger la clé au maximum

Configuration de BleachBit

1. Lancez BleachBit en tant que root, soit dans le menu des applications, soit en tapant la commande suivante dans un terminal (CTRL+T) :

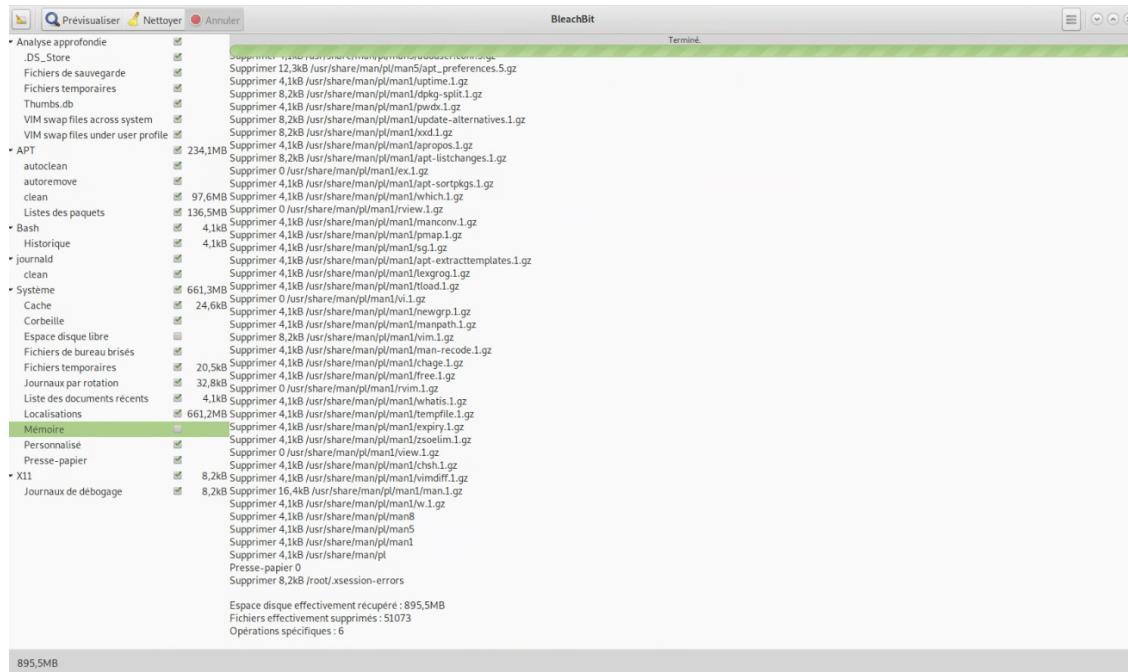
```
sudo bleachbit
```

```
support@Support:~$  
sudo bleachbit -h  
chown for path /root aborted  
chown for path /root aborted  
Préservation automatique de la langue fr.  
Préservation automatique de la langue fr.  
Usage: utilisation : bleachbit [options] nettoyeur.option1 nettoyeur.option2  
  
Options:  
-h, --help          show this help message and exit  
-l, --list-cleaners    lister les nettoyeurs  
-c, --clean         exécuter les nettoyeurs pour supprimer les fichiers et  
                   réaliser d'autres modifications permanentes  
--debug            Régler le niveau de journalisation à verbeux  
--debug-log=DEBUG_LOG      enregistrer les messages de débogage dans un fichier  
-s, --shred        détruire des fichiers ou des dossiers spécifiques  
--sysinfo          afficher les informations système  
--gui              lancer l'interface graphique  
-p, --preview      prévisualiser les fichiers à supprimer et autres  
                   modifications  
--preset           utiliser les options définies dans l'interface  
                   graphique  
-w, --wipe-free-space    écraser l'espace libre dans les chemins d'accès donnés  
-v, --version       afficher les informations de version et quitter  
-o, --overwrite     écraser les fichiers pour masquer leur contenu  
support@Support:~$
```

2. Fermez la pop-up et cochez toutes les cases excepté "Free disk space" et "Memory" puis cliquez sur "Supprimer"

Accéder au menu de l'application en cliquant sur l'icône empilement dans la barre de titre.

The screenshot shows the BleachBit application window. At the top, there's a toolbar with icons for Preview, Clean, and Cancel, followed by the application name 'BleachBit'. Below the toolbar is a status bar with three small icons. The main area contains two windows. The top window is a preferences dialog titled 'Préférences (au nom du superutilisateur)'. It has tabs for Général, Personnalisé, Lecteurs, Langues, and Liste blanche. The Général tab is selected, showing several checkboxes: 'Vérifier régulièrement les mises à jour sur Internet' (unchecked), 'Rechercher une nouvelle version bêta' (unchecked), 'Masquer les nettoyeurs inadéquats' (checked), 'Écraser le contenu des fichiers pour empêcher leur récupération' (unchecked), 'Quitter après le nettoyage' (unchecked), 'Confirmer avant de supprimer' (checked), 'Utiliser les préfixes CEI (1 Kio = 1024 octets) au lieu des préfixes SI (1 ko = 1000 octets)' (unchecked), 'Mode sombre' (checked), and 'Afficher les messages de débogage' (unchecked). A 'Fermer' button is at the bottom right. The bottom window is the main BleachBit interface. It shows a sidebar with categories like Analyse approfondie, APT, Bash, journald, Système, and X11, each with a list of items to clean. The 'Système' category is expanded, showing options like Cache, Presse-papier, Personnalisé, Fichiers de bureau brisés, Espace disque libre, Localisations, Mémoire, and Corbeille. The 'Corbeille' item under 'Système' is highlighted with a green selection bar. To the right of the sidebar, there's a detailed description of the selected item, such as 'Cache: Vider le cache' for Cache.



Utilisation

- RustDesk

Il est possible d'utiliser RustDesk pour se connecter à distance au Debian en utilisant son ID

- Tailscale

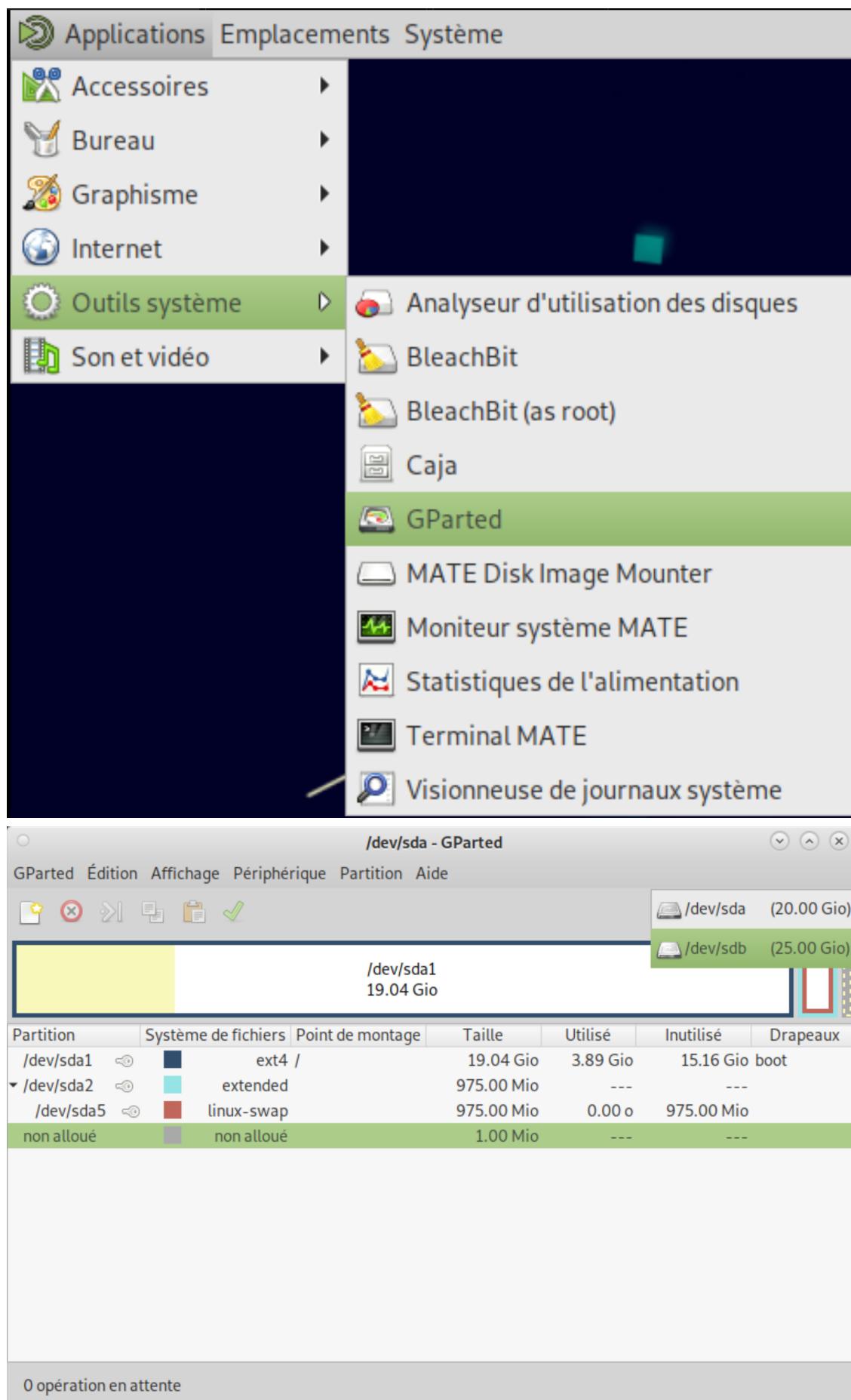
Tailscale est là pour faire une connexion directe sécurisée et externe au VPN de l'entreprise avec le serveur RustDesk, mais aussi pour permettre une connexion SSH à distance avec un appareil connecté au réseau Tailscale installé

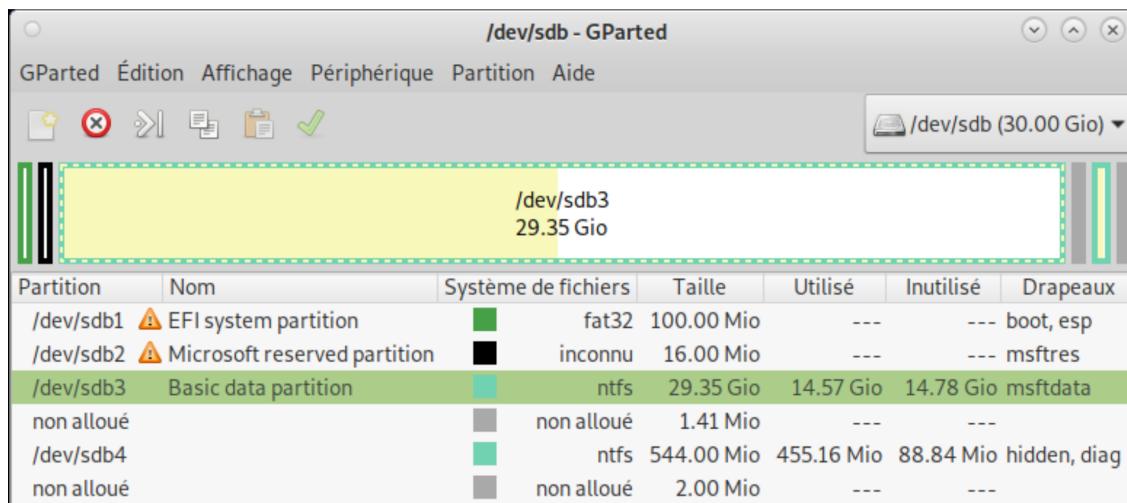
Pour cela il suffit de se connecter en SSH à l'IP Tailscale du Debian et d'utiliser les identifiants du debian

- Chntpw

Chntpw permet ici de réinitialiser le mot de passe d'un utilisateur en cas de besoin ou d'activer l'utilisateur Adminsitrateur/Administrator sur une machine Windows. Il est important de noter que son utilisation n'est fonctionnelle que sur les comptes locaux.

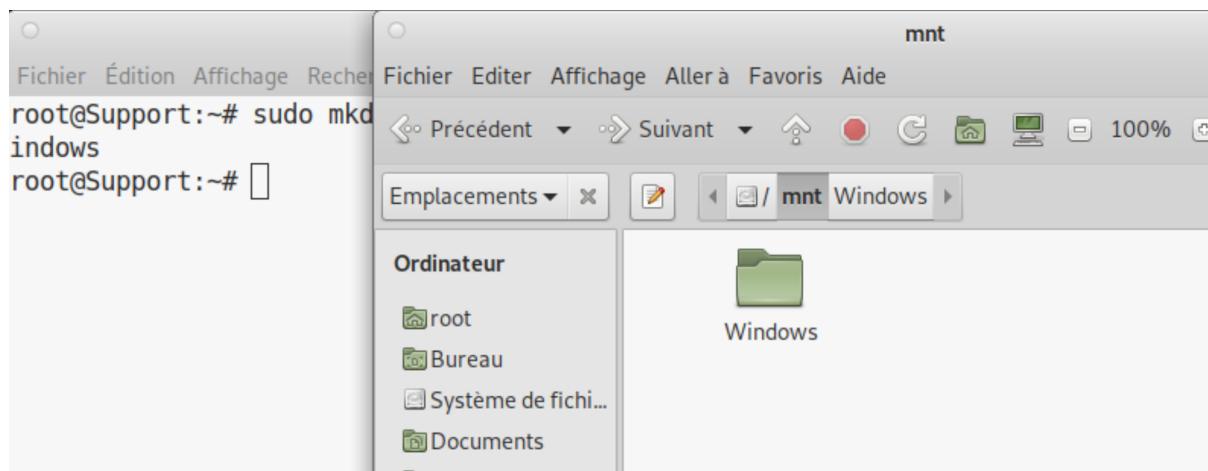
Pour l'utiliser, il faut monter le disque Windows, vous pouvez utiliser l'interface de Gparted pour identifier le disque.





Lancez le terminal et utilisez la commande (changez "/dev/sdb3" par la localisation affichée dans Gparted):

```
sudo mkdir /mnt/Windows ; sudo mount -t ntfs /dev/sdb3 /mnt/Windows
```



Une fois monté, utilisez les commandes suivantes pour aller accéder au fichier "SAM" et afficher les utilisateurs locaux :

```
cd /mnt/Windows/Windows/System32/config  
chntpw -l SAM
```

Usernames can be given as name or RID (in hex with 0x first)

See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.

NOTE: This program is somewhat hackish! You are on your own!
root@Support:/mnt/Windows/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 8 pages (+ 1 headerpage)
Used for data: 331/36576 blocks/bytes, unused: 34/20512 blocks/bytes.

RID - -----	Username -----	Admin? - Lock? --
01f4 Administrateur		ADMIN dis/lock
03ea Coucou		
01f7 DefaultAccount		dis/lock
01f5 Invit@		dis/lock
03e9 Nikki-Win10		ADMIN dis/lock
01f8 WDAGUtilityAccount		dis/lock

root@Support:/mnt/Windows/Windows/System32/config# █

Ici nous voulons supprimer le mot de passe de l'utilisateur "Coucou", nous ferons donc :

```
chntpw SAM -u Coucou
```

Tapez "1" pour supprimer le mot de passe puis "q" pour quitter, et enfin "y" pour sauvegarder

```
Select: [q] > 1
Password cleared!
===== USER EDIT =====

RID      : 1002 [03ea]
Username: Coucou
fullname:
comment :
homedir :

00000221 = Utilisateurs (which has 3 members)

Account bits: 0x0010 =
[ ] Disabled      | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act |
[ ] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10)   | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

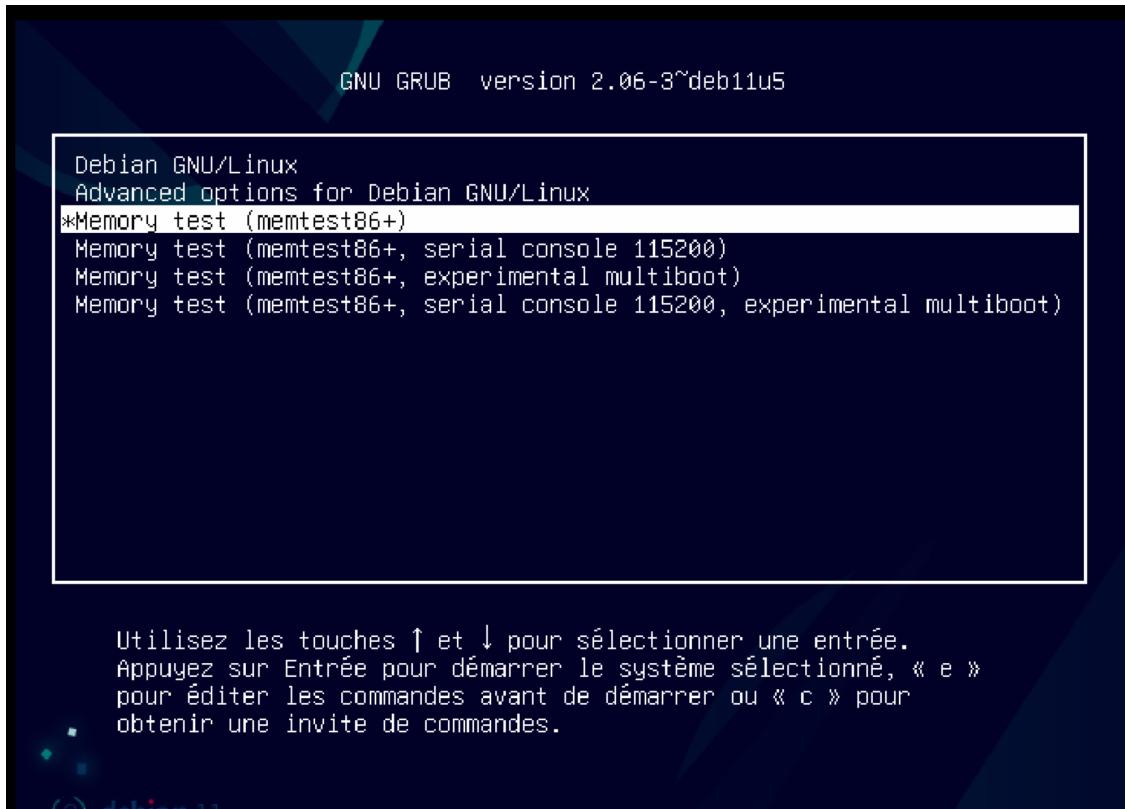
Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > q
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
#  Name
0  <SAM>
Write hive files? (y/n) [n] : y
```

- memtest86+

Lors d'un démarrage, avant que Debian se lance, sélectionnez "Memory test (memtest86+)" dans GRUB



Si une page bleue apparaît, Memtest86 s'est bien installé et fonctionne, pour l'utiliser, laissez passer le temps ou appuyez sur F1 pour accélérer le démarrage et attendre le retour de celui-ci

