

NOUVEAU

TUTORIEL PRATIQUE



INSTALLER ET CONFIGURER DEBIAN 13 TRIXIE

De l'installation de base aux premières manipulations

POINTS CLES DU TUTORIEL



Installation pas à pas



Configuration réseau



Sécurisation SSH



Commandes utiles et bonnes pratiques

Notes :

Ce tutoriel décrit l'installation de la version Debian 13 (appelée « Trixie ») parue le 10/8/2025. L'installation est présentée sous la forme d'une machine virtuelle créée à partir de l'hyperviseur © Proxmox. Pour plus d'informations sur la création des machines virtuelles, se référer aux tutoriels © Proxmox présents sur le site.

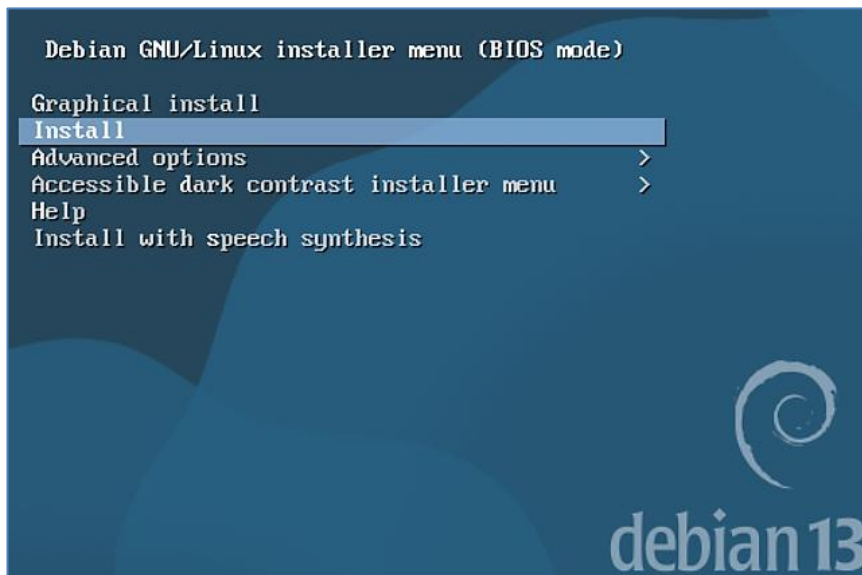
Dans ce tutoriel, nous supposons que notre machine virtuelle est reliée à un « vmbr » permettant d'obtenir une adresse IP dynamique et de l'Internet. Dans le cas contraire, il faudra configurer les adresses IP de manière manuelle.

La réalisation de ce tutoriel nécessite un fichier d'installation « iso » qui se trouve à cette adresse : <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-13.0.0-amd64-netinst.iso>

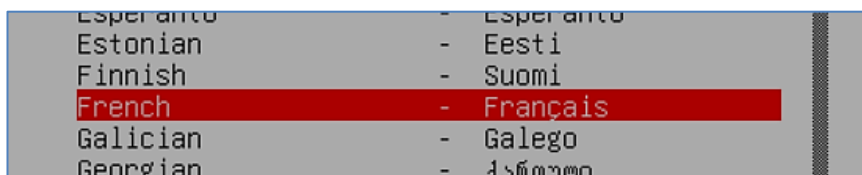
1 – LANCEMENT DE L'INSTALLATION DE DEBIAN 13 (TRIXIE)

Une fois la machine virtuelle créée et démarrée, on obtient cet écran d'installation :

- Sélectionnez l'installation en mode console en choisissant l'option « **Install** »
- Pressez la touche **Entrée** :



- Sélectionnez « **French** » et pressez la touche **Entrée** :



- Sélectionnez « **France** » et pressez la touche **Entrée** :



- Sélectionnez « **Français** » et pressez la touche **Entrée** :



- Saisissez un nom de machine et pressez la touche **Entrée** :

[!] Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

debian13

<Revenir en arrière> <Continuer>

- La saisie du nom de domaine n'est pas obligatoire ; vous pouvez juste presser la touche **Entrée** :

[!] Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

labo-sio.fr

<Revenir en arrière> <Continuer>

- Saisissez le mot de passe que vous souhaitez attribuer au compte « root » et pressez la touche **Entrée** :

[!!] Créer les utilisateurs et choisir les mots de passe

Un compte doit être paramétré pour disposer des privilèges administratifs de superutilisateur. Le mot de passe pour ce compte doit être quelque chose qui ne peut pas être deviné.

Pour autoriser une connexion directe du superutilisateur (« root ») par mot de passe, saisissez ici son mot de passe.

Autrement, vous pouvez bloquer le mot de passe du superutilisateur en laissant ce champ vide. À la place, vous pourrez utiliser le premier utilisateur créé par le système (à la prochaine étape) pour obtenir des privilèges d'administration. Cela sera effectué en ajoutant le premier utilisateur créé au groupe « sudo ».

Remarque : ce que vous saisirez ici sera caché (à moins de choisir de l'afficher).

Mot de passe du superutilisateur (« root ») :

[] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

- Saisissez à nouveau le mot de passe du compte « root », pour le confirmer, et pressez la touche **Entrée** :

[[!]] Créer les utilisateurs et choisir les mots de passe

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

[] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

- Saisissez le nom du compte utilisateur que vous souhaitez créer et pressez la touche **Entrée** :

[[!]] Créer les utilisateurs et choisir les mots de passe

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

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

Nom complet du nouvel utilisateur :

debian

<Revenir en arrière> <Continuer>

- Pressez la touche **Entrée** pour valider l'identifiant du compte utilisateur :

[[!]] Créer les utilisateurs et choisir les mots de passe

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

Identifiant pour le compte utilisateur :

debian

<Revenir en arrière> <Continuer>

- Saisissez le mot de passe du compte utilisateur et pressez la touche **Entrée** :

[[!]] Créer les utilisateurs et choisir les mots de passe

Assurez-vous de choisir un mot de passe suffisamment robuste pour qu'il ne puisse pas être deviné.

Mot de passe pour le nouvel utilisateur :

[] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

- Saisissez à nouveau le mot de passe du compte utilisateur, pour le confirmer, et pressez la touche **Entrée** :

[[!]] Créer les utilisateurs et choisir les mots de passe

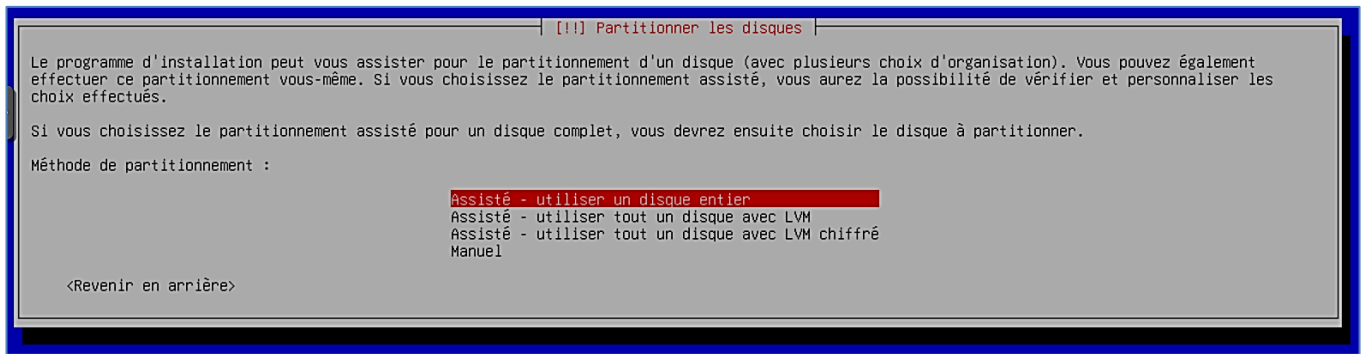
Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

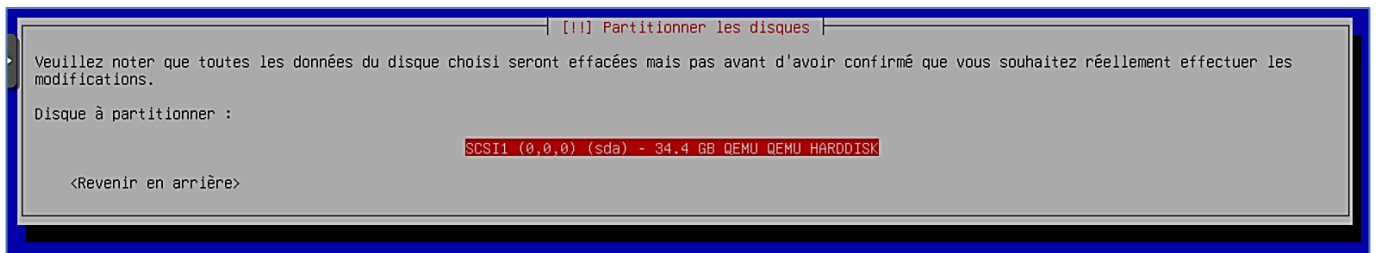
[] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

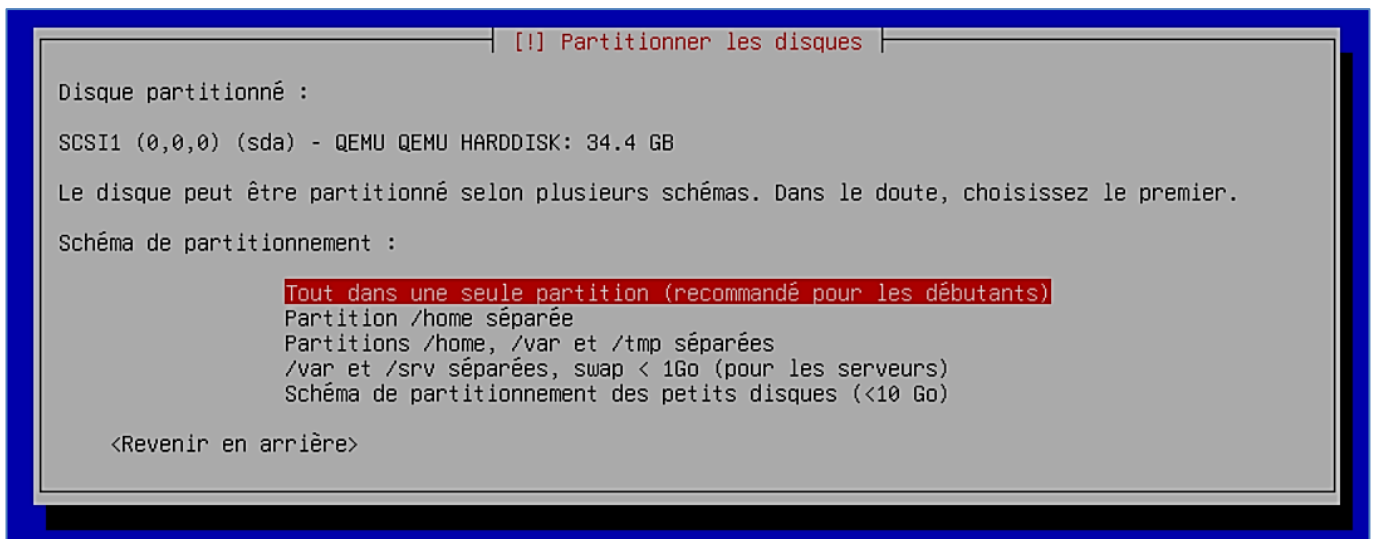
- Conservez le mode « **Assisté – un disque entier** » et pressez la touche **Entrée** :



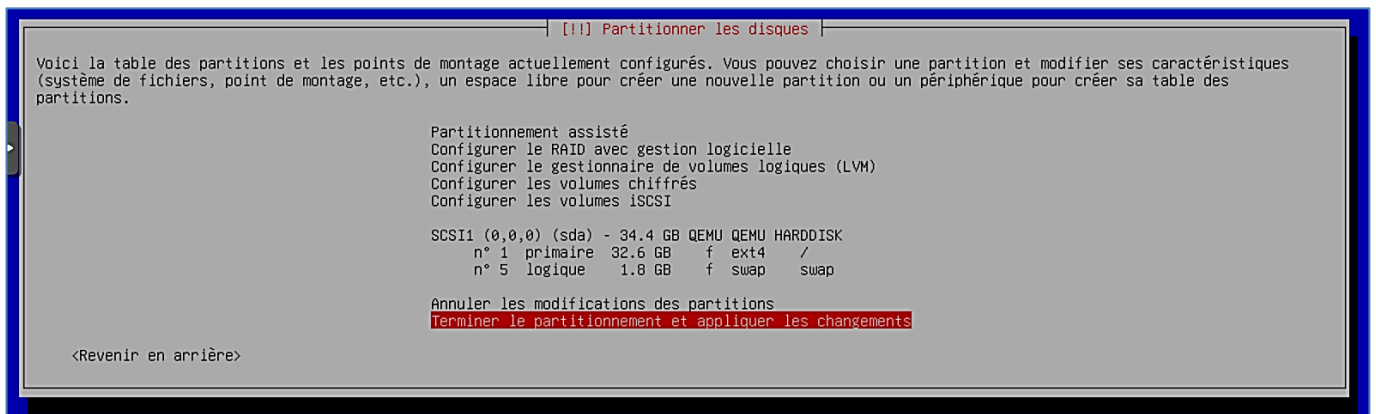
- Le disque de la machine virtuelle est sélectionné automatiquement ; pressez la touche **Entrée** :



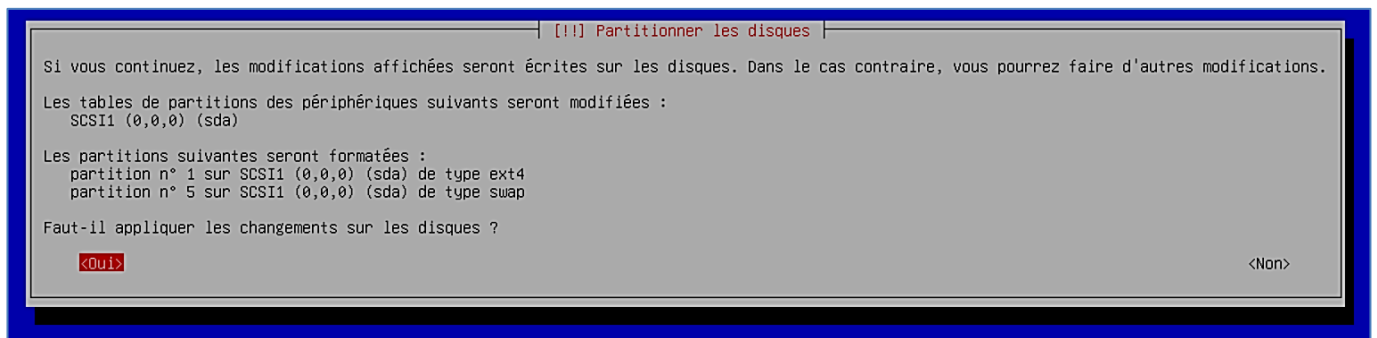
- Conservez « **Tout dans une seule partition (recommandé)** » et pressez la touche **Entrée** :



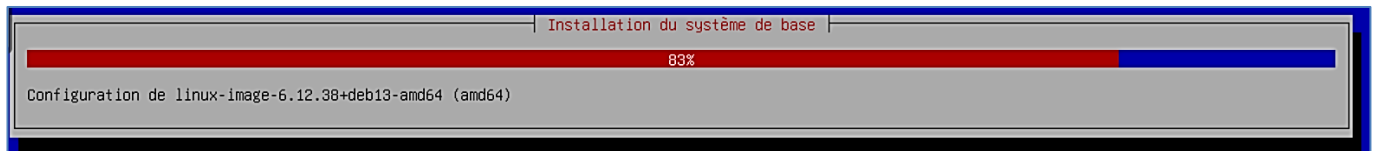
- Conservez « **Terminer le partitionnement et appliquer les changements** » ; pressez la touche **Entrée** :



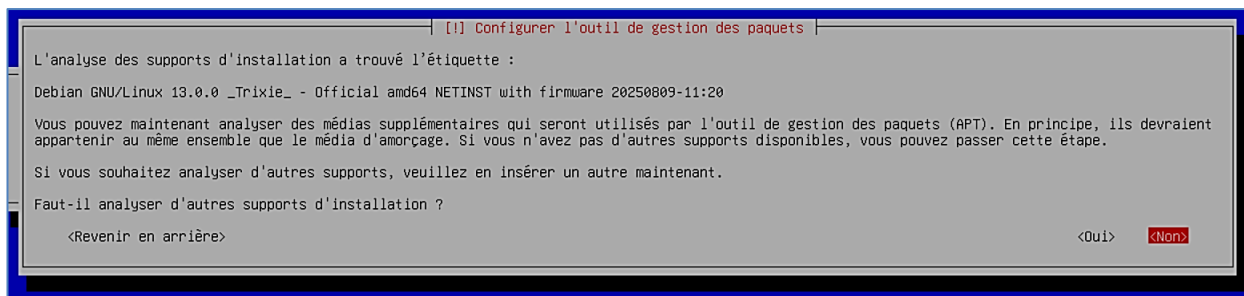
- Sélectionnez « **Oui** » et pressez la touche **Entrée** :



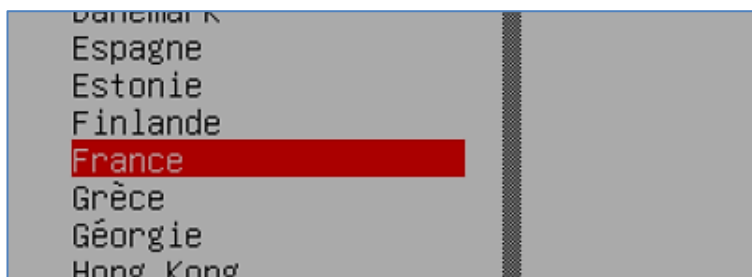
- Patientez pendant l'installation du système de base :



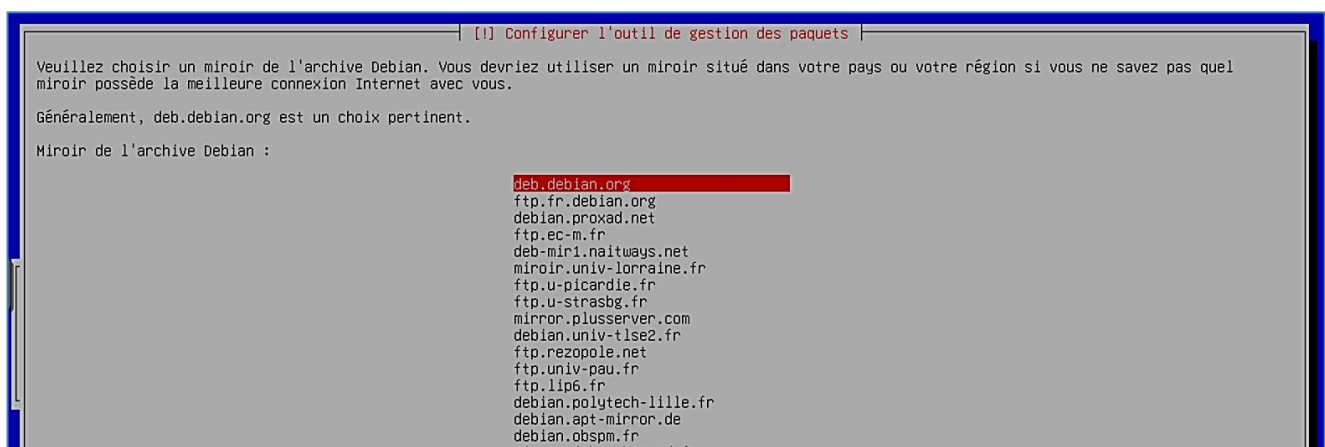
- Conservez l'option « **Non** » et pressez la touche **Entrée** :



- Sélectionnez « **France** » et pressez la touche **Entrée** :



- Conservez le 1^{er} miroir sélectionné et pressez la touche **Entrée** :



- Ne rien saisir ici (pas de serveur Proxy) et pressez la touche **Entrée** :

[!] Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée « http://[[utilisateur]:[mot-de-passe]@hôte[:port]]/ ».

Mandataire HTTP (laisser vide si aucun) :

<Revenir en arrière> <Continuer>

- Conservez l'option « **Non** » sélectionnée et pressez la touche **Entrée** :

[!] Configuration de popularity-contest

Le système peut envoyer anonymement aux responsables de la distribution des statistiques sur les paquets que vous utilisez le plus souvent. Ces informations influencent le choix des paquets qui sont placés sur le premier CD de la distribution.

Si vous choisissez de participer, un script enverra automatiquement chaque semaine les statistiques aux responsables. Elles peuvent être consultées sur <https://popcon.debian.org/>.

Vous pourrez à tout moment modifier votre choix en exécutant « dpkg-reconfigure popularity-contest ».

Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?

<Oui> <Non>

- **Décochez les 2 premières cases afin de ne pas installer d'interface graphique** : déplacez-vous jusqu'à l'option « **Serveur SSH** » et pressez la barre d'espace pour l'activer puis pressez la touche **Entrée** :

[!] Sélection des logiciels

Actuellement, seul le système de base est installé. Pour adapter l'installation à vos besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de logiciels.

Logiciels à installer :

- ☐ environnement de bureau Debian
- ☐ ... GNOME
- ☐ ... Xfce
- ☐ ... bureau GNOME Flashback
- ☐ ... KDE Plasma
- ☐ ... Cinnamon
- ☐ ... MATE
- ☐ ... LXDE
- ☐ ... LXQt
- ☐ serveur web
- ☒ serveur SSH
- ☒ utilitaires usuels du système
- ☐ choix d'un assemblage (blend) de Debian lors de l'installation

<Continuer>

- Sélectionnez l'option « **Oui** » et pressez la touche **Entrée** :

[!] Configuration de grub-pc

Il semble que cette nouvelle installation soit le seul système d'exploitation existant sur cet ordinateur. Si c'est bien le cas, il est possible d'installer le programme de démarrage GRUB sur le disque principal (partition UEFI ou secteur d'amorçage).

Attention : si le programme d'installation ne détecte pas un système d'exploitation installé sur l'ordinateur, cela empêchera temporairement ce système de démarrer. Toutefois, le programme de démarrage GRUB pourra être manuellement reconfiguré plus tard pour permettre ce démarrage.

Installer le programme de démarrage GRUB sur le disque principal ?

<Revenir en arrière> <Oui> <Non>

- Sélectionnez votre disque virtuel (**important**) et pressez la touche **Entrée** :

[!] Configuration de grub-pc

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible.

Périphérique où sera installé le programme de démarrage :

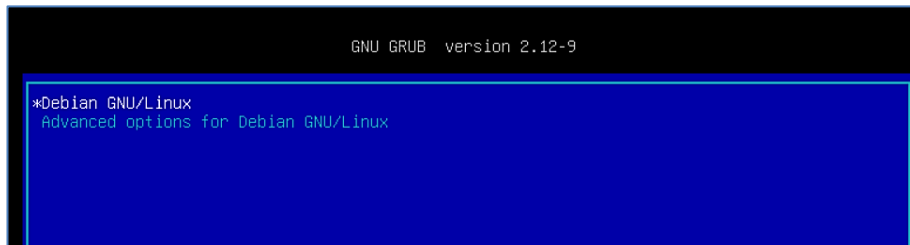
Choix manuel du périphérique
/dev/sda (scsi-0QEMU_QEMU_HARDDISK_drive-scsi0)

<Revenir en arrière>

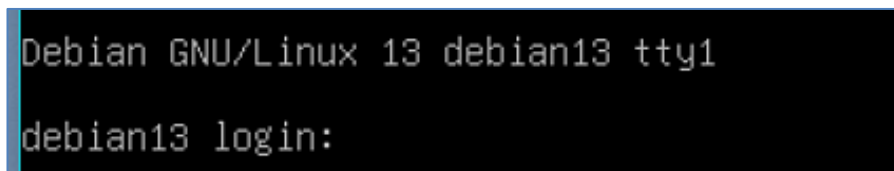
- Conservez l'option « **Continuer** » et pressez la touche **Entrée** :



Le système a été installé et redémarre automatiquement :



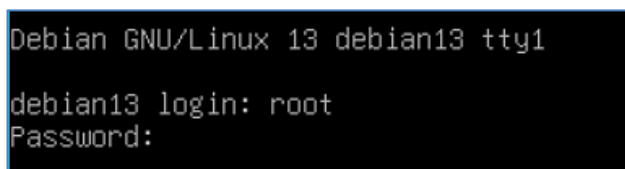
Le système est prêt ; la fenêtre d'authentification s'affiche :



2 – CONNEXION A LA SESSION « ROOT » - VERIFICATION ADRESSAGE IP ET TESTS DE PING

CONNEXION A LA SESSION AVEC L'UTILISATEUR « root »

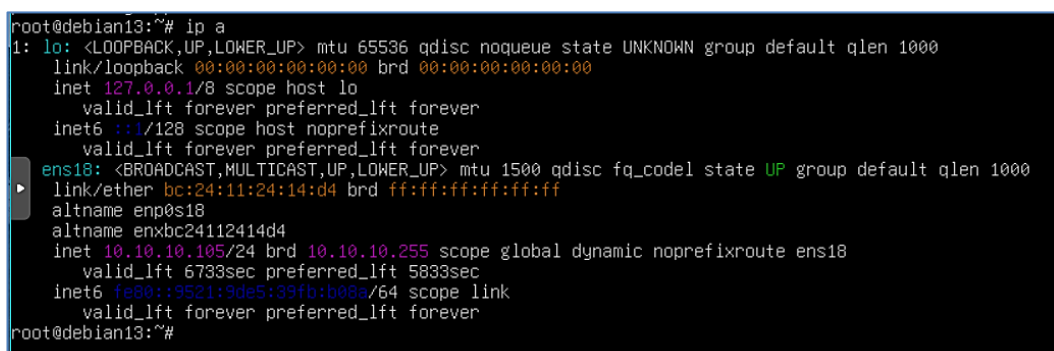
- Saisissez « **root** » et pressez la touche **Entrée**
- Saisissez le mot de passe qui a été défini lors de l'installation et pressez la touche **Entrée** :



VERIFICATION DE L'ADRESSE IP DYNAMIQUE ALLOUEE LORS DE L'INSTALLATION

- Saisissez la commande « **ip a** » :

ip a



L'adresse IP dynamique obtenue s'affiche dans la section correspondant à la carte réseau virtuelle de la machine nommée ici « ens18 ».

TEST DE LA CONNEXION INTERNET

- Saisissez la commande « **ping -c 4 1.1.1.1** » :

ping -c 4 1.1.1.1

```
root@debian13:~# ping -c 4 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=2.11 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=1.90 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=1.87 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=57 time=1.63 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.631/1.878/2.108/0.169 ms
root@debian13:~#
```

Note :

ping -c 4 : on envoie une requête « ping » mais on souhaite qu'elle s'arrête après 4 paquets « ECHO_REQUEST ».

Si la commande « **ping 1.1.1.1** » est saisie sans le paramètre « **-c 4** », on obtient une réponse continue. Dans ce cas, pour la stopper, il faudra presser les touches CTRL + C

```
root@debian13:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=2.04 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=1.95 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=2.10 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=57 time=2.13 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=57 time=2.63 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=57 time=2.08 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=57 time=2.10 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=57 time=1.94 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=57 time=1.91 ms
^C
--- 1.1.1.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 1.911/2.097/2.632/0.202 ms
root@debian13:~#
```

DECONNEXION DE LA SESSION

- Pour vous déconnecter de la session, vous avez plusieurs possibilités parmi lesquelles :
 - Saisissez « **exit** » et pressez la touche **Entrée** ; la session est déconnectée :

exit (ou CTRL + D)

```
root@debian13:~# exit
```

La session est déconnectée.

MISE A JOUR DES PAQUETS SYSTÈME

Tout comme une machine Windows, il est important de mettre à jour, régulièrement, les « paquets » de votre système à l'aide des commandes suivantes :

apt update

```
root@debian13:~# apt update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Réception de : 2 http://deb.debian.org/debian trixie-updates InRelease [47,1 kB]
Atteint : 3 http://security.debian.org/debian-security trixie-security InRelease
47,1 ko réceptionnés en 0s (268 ko/s)
Tous les paquets sont à jour.
```

apt full-upgrade -y

```
root@debian13:~# apt full-upgrade -y
mmaire :
► Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 0
```

Note : la variable « -y » permet de valider automatiquement la commande après avoir pressé la touche Entrée. Dans notre cas, il n'y a pas de mises à jour car nous avons installé la machine à partir du dernier fichier « iso » disponible.

INSTALLATION DE SUDO

« **root** » est le nom du compte d'utilisateur le plus puissant sur un système d'exploitation de type Unix, y compris **Debian 13**. C'est l'équivalent de l'administrateur système sur Windows. Le compte root a des permissions illimitées et peut exécuter n'importe quelle commande, modifier n'importe quel fichier ou paramètre, et accéder à toutes les parties du système.

Pourquoi utiliser sudo et un utilisateur standard ?

Travailler en tant qu'utilisateur « root » en permanence est extrêmement dangereux pour plusieurs raisons :

- **Sécurité** : Si un programme malveillant ou une erreur de commande est exécuté par l'utilisateur root, il peut causer des dommages irréversibles au système. Le simple fait de se tromper d'une lettre dans une commande de suppression peut effacer des fichiers système essentiels.
- **Vulnérabilités** : En étant connecté en tant que root, les failles de sécurité potentielles des applications que vous utilisez peuvent être exploitées pour prendre le contrôle total de votre système.
- **Risque d'erreurs** : Une simple faute de frappe peut avoir des conséquences désastreuses, comme l'effacement de fichiers importants.

Pour atténuer ces risques, il est fortement recommandé de travailler avec un compte utilisateur standard que l'on affectera à un groupe nommé « sudo » qui lui permettra d'avoir des « privilèges root » temporaires.

« **sudo** » (pour **super user do**) est une commande qui permet à un utilisateur standard d'exécuter des commandes avec les privilèges de l'utilisateur root de manière temporaire. Cette commande offre :

- **Une sécurité accrue** : sudo vous permet de n'utiliser les droits de superutilisateur que lorsque c'est absolument nécessaire. Au lieu d'être connecté en tant que root en permanence, vous effectuez vos tâches administratives de manière ponctuelle et contrôlée.

- **Une responsabilité** : L'utilisation de sudo est enregistrée dans les journaux du système (/var/log/auth.log). Il est ainsi facile de savoir qui a exécuté une commande avec des privilèges élevés.
- **Une meilleure pratique** : C'est la méthode de travail standard et recommandée pour la gestion des systèmes Debian, et plus largement, de tous les systèmes Unix/Linux modernes.

L'installation de « sudo » s'effectue ainsi :

- Saisissez la commande « **apt install sudo -y** » et patientez pendant l'installation du paquet :

apt install sudo -y

```
root@debian13:~# apt install sudo -y
Installation de :
  sudo

Sommaire :
  Mise à niveau de : 0. Installation de : 1 Supprimé : 0. Non mis à jour : 0
  Taille du téléchargement : 2 087 kB
  Espace nécessaire : 6 865 kB / 29,1 GB disponible

Réception de : 1 http://deb.debian.org/debian trixie/main amd64 sudo amd64 1.9.16p2-3 [2 087 kB]
2 087 ko réceptionnés en 0s (60,9 Mo/s)
Sélection du paquet sudo précédemment désélectionné.
(Lecture de la base de données... 30607 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../sudo_1.9.16p2-3_amd64.deb ...
Dépaquetage de sudo (1.9.16p2-3) ...
Paramétrage de sudo (1.9.16p2-3) ...
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.41-12) ...
root@debian13:~#
```

- Ajoutez au groupe « sudo » votre utilisateur standard (ici nous ajoutons l'utilisateur « debian », créé lors de l'installation, au groupe « sudo ») à l'aide de la commande suivante :

usermod -aG sudo debian

```
root@debian13:~# usermod -aG sudo debian
```

Note : la variable **-aG** signifie **ajouter au GROUPE sudo l'utilisateur debian**

- Vérifiez que l'utilisateur est bien dans le groupe « sudo » avec la commande « **groups nom_user** » :

groups debian

```
debian : debian cdrom floppy sudo audio dip video plugdev users netdev
```

SECURISATION SSH

Pour rappel, à la fin de l'installation de Debian 13 (voir page 7), nous avons coché la case « Serveur SSH » :

```
[ ] environnement de bureau Debian
[ ] ... GNOME
[ ] ... Xfce
[ ] ... bureau GNOME Flashback
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] serveur web
[*] serveur SSH
[*] utilitaires usuels du système
[ ] choix d'un assemblage (Blend) de Debian lors de l'installation
```

Il est important de sécuriser à minima les connexions SSH pour éviter le « brute-force » sur le port SSH (port « 22 » par défaut). Pour cela, nous pouvons effectuer les manipulations suivantes au niveau du fichier de configuration « sshd_config » ; ce fichier se trouve dans « /etc/ssh » :

- Connectez-vous en « root » sur la machine et éditez le fichier « sshd_config » avec la commande suivante :

nano /etc/ssh/sshd_config

- Décommentez la ligne « **#Port 22** » et modifiez le port SSH par défaut par un port non utilisé et **supérieur à 1024** (exemple ici, on a indiqué 2213) :

```
Port 2213
```

- Décommentez et modifiez la ligne « **PermitRootLogin** » en indiquant « **no** » :

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

- Redémarrez le service SSH avec la commande « **systemctl restart ssh** » :

systemctl restart ssh

```
root@debian13:~# systemctl restart ssh
```

- Vérifiez le statut du service SSH avec la commande « **systemctl status ssh** » ; le statut doit être affiché en **vert** avec l'indication du mode « **active (running)** » :

systemctl status ssh

```
root@debian13:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-08-10 20:17:36 CEST; 1min 18s ago
  Invocation: 6c29ee8ecf794f7eafb6d2a80e068226
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1652 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 1655 (sshd)
       Tasks: 1 (limit: 2302)
      Memory: 1.3M (peak: 1.8M)
         CPU: 25ms
    CGroup: /system.slice/ssh.service
            └─1655 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

août 10 20:17:35 debian13 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
août 10 20:17:36 debian13 sshd[1655]: Server listening on 0.0.0.0 port 2213.
août 10 20:17:36 debian13 sshd[1655]: Server listening on :: port 2213.
août 10 20:17:36 debian13 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

- Depuis votre machine Windows, ouvrez une console et testez la connexion SSH à votre machine Debian en tant que « root » ; logiquement, cette dernière ne doit pas aboutir et affiche le message « **Permission denied** ». Pour cela, saisissez la commande « **ssh root@IP_Debian -p 2213** » :

ssh root@IP_Debian -p 2213

```
PS C:\Users\pc> ssh root@21.....102 -p 2213
root@21.....102's password:
Permission denied, please try again.
root@21.....102's password: |
```

Note : pour quitter le processus, pressez les touches CTRL + C

- Refaites l'essai mais avec l'utilisateur « sudo » de votre machine en saisissant la commande « **ssh nom_user_sudo@IP_debian -p 2213** » ; en pressant la touche Entrée, le mot de passe de l'utilisateur est demandé ; saisissez-le et pressez la touche Entrée pour la connexion soit réalisée :

ssh nom_user_sudo@IP_debian -p 2213

```
PS C:\Users\pc> ssh debian@213.102 -p 2213
debian@213.102's password:
Linux debian13 6.12.38+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.38-1 (2025-07-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 10 20:05:14 2025 from 90.58.71.216
```

Note : pour quitter la session, vous pouvez fermer la fenêtre directement ou presser les touches CTRL + D ou saisir la commande « exit » et Entrée.

AUTHENTIFICATION SSH PAR CLE PUBLIQUE

La partie précédente a sécurisé, à minima, la connexion SSH mais il est fortement recommandé d'utiliser l'authentification par clé publique plutôt que par mot de passe. Pour cela, effectuez les manipulations suivantes :

Sur votre machine locale Windows, ouvrez une console.

- Saisissez la commande suivante qui vous permettra de générer vos clés (privée et publique) :

ssh-keygen -t ed25519 -a 100

Note : les clés sont enregistrées dans le dossier « c:\users\nom_utilisateur\.ssh »

```
Directory: C:\Users\pc\.ssh

Mode                LastWriteTime         Length Name
----                -
-a---              30/03/2025    08:47         411 id_ed25519
-a---              30/03/2025    08:47          97 id_ed25519.pub
```

- Copiez la clé publique (« .pub ») sur votre machine Debian à l'aide de la commande suivante :

```
cat ~/.ssh/id_ed25519.pub | ssh -p 2213 debian@213.102 "mkdir -p ~/.ssh && chmod 700 ~/.ssh && cat
>> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"
```

- Saisissez le mot de passe de votre utilisateur et pressez la touche **Entrée** ; la clé est copiée sur votre machine Debian :

```
PS C:\Users\pc\.ssh> cat ~/.ssh/id_ed25519.pub | ssh -p 2213 debian@213.102 "mkdir -p ~/.ssh && chmod 700 ~/.ssh
&& cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"
debian@213.102's password:
```

- Testez la connexion SSH à votre machine Debian ; vous n'avez plus besoin de saisir le mot de passe de l'utilisateur :

```
PS C:\Users\pc\.ssh> ssh debian@213.102.102 -p 2213
Linux debian13 6.12.38+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.38-1 (2025-07-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 10 20:24:23 2025 from 90.58.71.216
debian@debian13:~$
```

SECURISATION DU FICHER « sshd_config »

Une fois que la connexion par clé publique fonctionne, nous pouvons améliorer la configuration du fichier « sshd_config » en intervenant, notamment, sur les options suivantes du fichier « sshd_config » :

```
PasswordAuthentication no # force l'utilisation de clés SSH
PubkeyAuthentication yes # active authentification par clé publique
PermitEmptyPasswords no # interdit les mots de passe vides
MaxAuthTries 3 # limite tentatives avant blocage
```

- Editez le fichier « sshd_config » avec la commande suivante :

`sudo nano /etc/ssh/sshd_config`

```
debian@debian13:~$ sudo nano /etc/ssh/sshd_config
[sudo] Mot de passe de debian :
```

- Faites les modifications dans le fichier « sshd_config » qui a été édité :

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

PubkeyAuthentication yes
```

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

- Quittez et sauvegardez vos modifications : **CTRL + X + O** et pressez la touche **Entrée**
- Redémarrez le service SSH et assurez-vous que le statut est bien « actif » à l'aide des commandes :

`sudo systemctl restart ssh`

`systemctl status ssh`

Le service SSH est bien actif sur votre machine :

```

debian@debian13:~$ sudo systemctl restart ssh
debian@debian13:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-08-11 12:04:33 CEST; 8s ago
  Invocation: 88c4df1224414af9858d2cd868001c43
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 2677 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2680 (sshd)
    Tasks: 1 (limit: 2302)
   Memory: 1.3M (peak: 1.8M)
      CPU: 25ms
   CGroup: /system.slice/ssh.service
           └─2680 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
debian@debian13:~$ |

```

INSTALLER ET CONFIGURER FAIL2BAN

Fail2Ban est un outil de protection contre le brute-force. Il convient de l'installer sur notre machine Debian afin d'écarter les tentatives d'attaque sur SSH. Pour cela, effectuez les manipulations suivantes :

- Connectez-vous en SSH à votre machine Debian
- Installez l'outil Fail2Ban à l'aide de la commande suivante :

sudo apt install fail2ban -y

```

debian@debian13:~$ sudo apt install fail2ban -y
[sudo] Mot de passe de debian : |

```

- Activez Fail2Ban au démarrage de votre machine Debian afin que le service soit actif

sudo systemctl enable --now fail2ban

```

debian@debian13:~$ sudo systemctl enable --now fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban

```

- Créez un fichier « **jail.local** » dans le répertoire « **/etc/fail2ban** » contenant ceci :

sudo nano /etc/fail2ban/jail.local

[sshd]

```

enabled = true
port = 2213
filter = sshd
logpath = /var/log/fail2ban.log
backend = systemd
maxretry = 2
findtime = 300
banaction = iptables-allports
bantime = 86400
ignoreip = 127.0.0.1

```

- Quittez et sauvegardez le fichier avec **CTRL + X + O** et pressez la touche **Entrée**
- Redémarrez le service Fail2Ban et vérifiez que le statut est bien en mode « active » :

sudo systemctl restart fail2ban

systemctl status fail2ban

Vérifiez que le statut du service « Fail2ban » est bien en mode « **running** »):

```
debian@debian13:~$ sudo systemctl restart fail2ban
debian@debian13:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-08-11 12:18:58 CEST; 12s ago
     Invocation: f0efe8a994df4ac89f43e165fbc97948
       Docs: man:fail2ban(1)
    Main PID: 3233 (fail2ban-server)
      Tasks: 5 (limit: 2302)
     Memory: 12.1M (peak: 14.1M)
        CPU: 109ms
     CGroup: /system.slice/fail2ban.service
            └─3233 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

août 11 12:18:58 debian13 systemd[1]: Started fail2ban.service - Fail2Ban Service.
août 11 12:18:58 debian13 fail2ban-server[3233]: Server ready
```

COMMANDES UTILES FAIL2BAN

Bannir une IP

fail2ban-client set [nom du jail] banip [IP à bannir]

Enlever le ban d'une IP

fail2ban-client set [nom du jail] unbanip [IP concerné]

Lister les règles

fail2ban-client status

Afficher les détails d'une règle

fail2ban-client status sshd

Lister les tentatives de connexion

tail /var/log/fail2ban.log

Lister les tentatives de connexion (en temps réel)

tail -f /var/log/fail2ban.log

MODIFICATION DU MOT DE PASSE D'UN COMPTE UTILISATEUR

Vous pouvez modifier le mot de passe d'un compte utilisateur ainsi :

sudo passwd nom_utilisateur

```
debian@debian13:/var/log$ sudo passwd debian
Nouveau mot de passe : |
```