Prise en main et Sécurisation de Debian 13

Bienvenue chez Innov-Tech ! Votre mission : déployer srv-core01, un serveur ultra-sécurisé qui servira de socle à l'infrastructure critique de l'entreprise.

Debian 13 "Trixie" : Le Choix Stratégique

Noyau Linux 6.x

Support matériel amélioré et nouvelles fonctionnalités de sécurité au niveau du noyau.

Nftables par défaut

Le pare-feu moderne remplace iptables pour toute nouvelle infrastructure.

Logiciels à jour

Versions récentes offrant un compromis optimal entre nouveauté et stabilité.

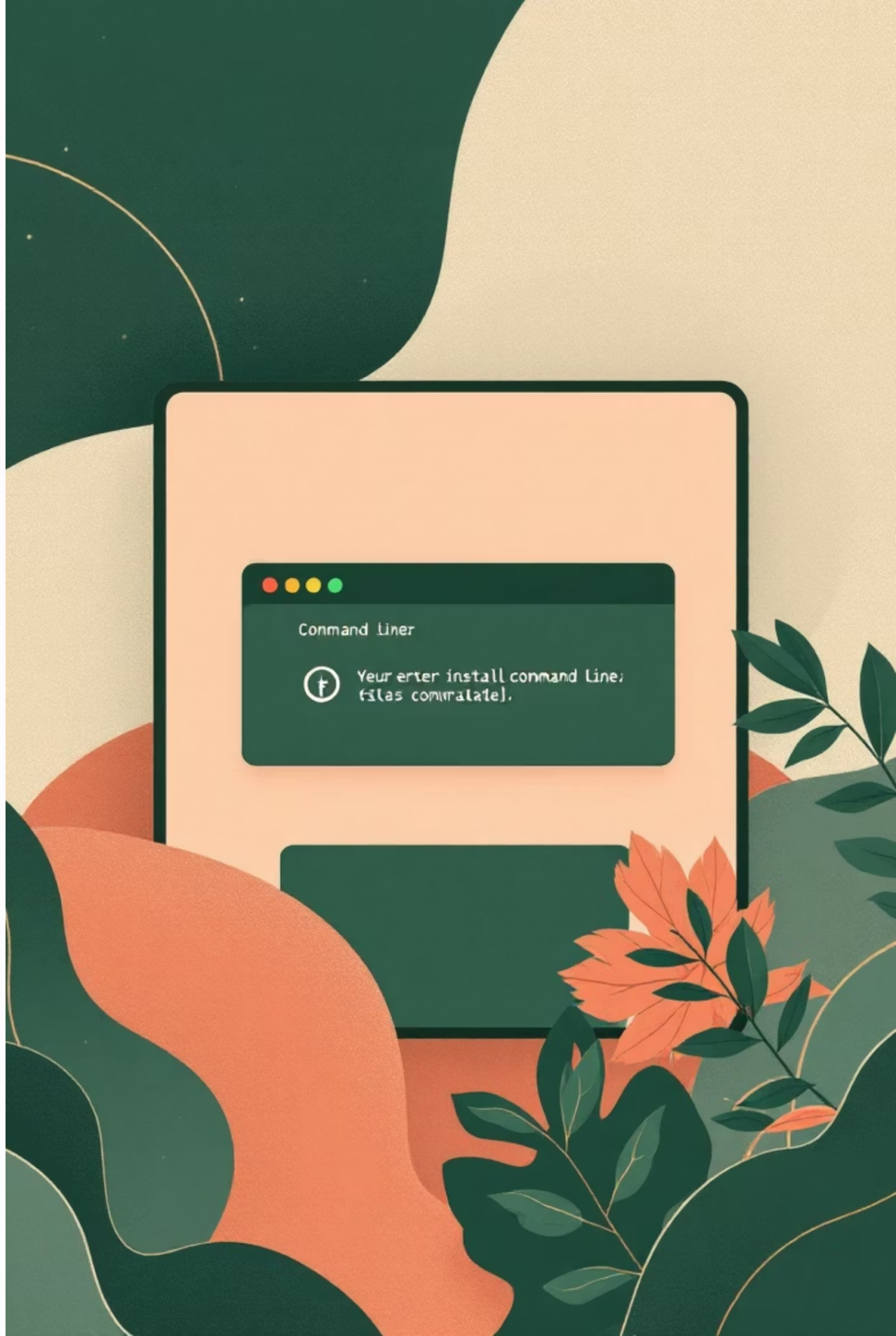
Installation Minimale : Surface d'Attaque Zéro

La Stratégie d'Entreprise

Chaque paquet installé représente une porte potentielle pour un attaquant. Moins de logiciels = moins de failles à exploiter.

- Image netinst (network install)
- Sélection minimale : serveur SSH + utilitaires système
- Aucun environnement de bureau
- Installation depuis les dépôts officiels

Principe clé : On part d'une feuille blanche et on installe uniquement ce qui est strictement nécessaire.



Partitionnement Stratégique

Concevoir les partitions comme les pièces d'un bâtiment : une pièce inondée ne doit pas noyer le reste.

1

/ (racine)

8-10 Go (ext4) - Le cœur du système

2

/home

5 Go (ext4) - Données utilisateurs isolées

3

/var

15 Go (ext4) - Logs, bases de données, sites web

4

/tmp

2 Go (ext4) - Fichiers temporaires avec noexec

5

swap

2-4 Go - Mémoire virtuelle

Les Avantages du Partitionnement

Sécurité Renforcée

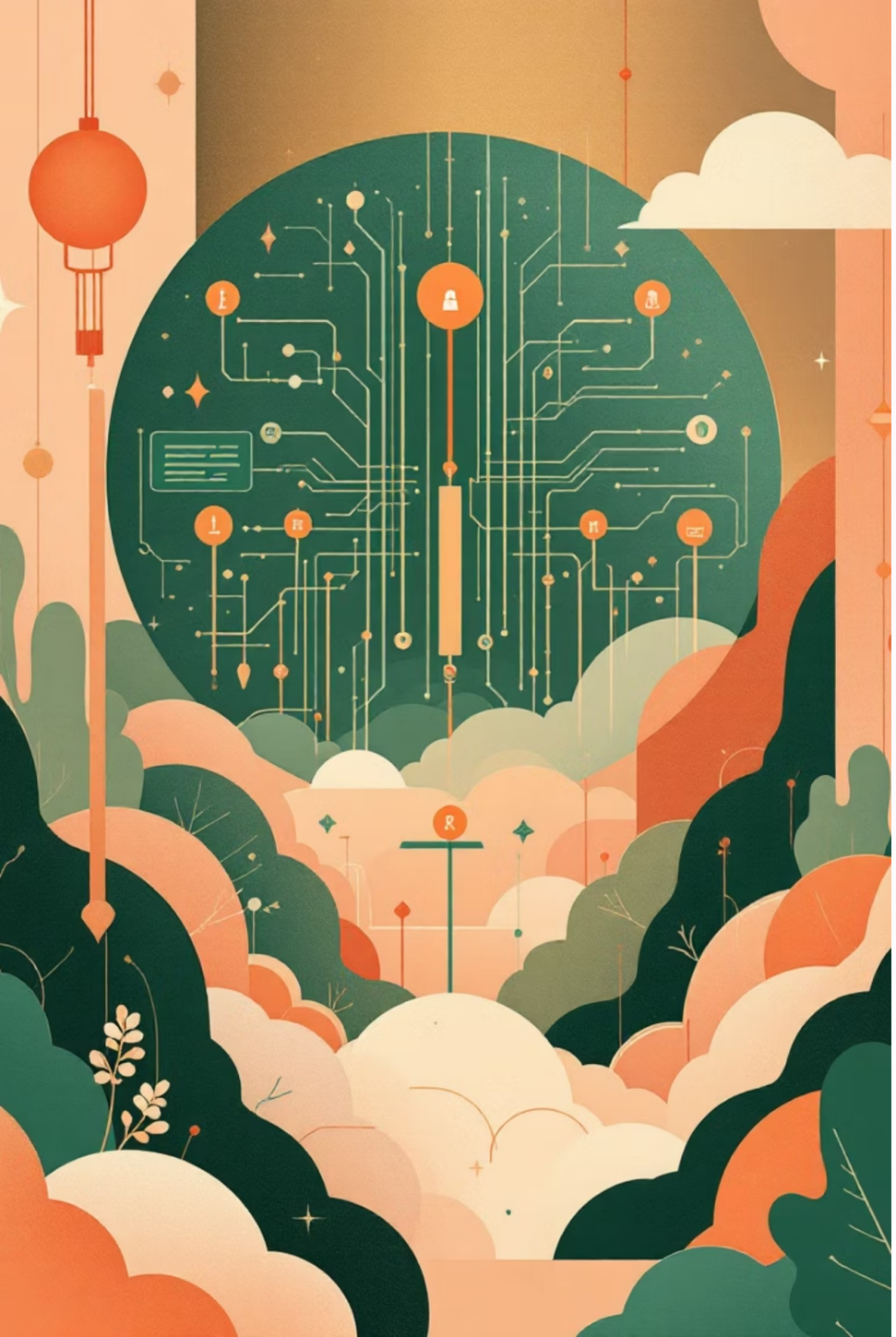
Options spécifiques par partition : interdire l'exécution depuis /tmp (noexec, nosuid, nodev).

Stabilité Garantie

Si /var sature de logs, le système racine continue de fonctionner normalement.

Performance Optimisée

Disques dédiés pour partitions critiques comme /var/lib/mysql.



SSH : La Porte d'Entrée Blindée

Configuration Sécurisée

Fichier : `/etc/ssh/sshd_config`

- **Port 2222** : Éviter les scans automatiques
- **PermitRootLogin no** : Jamais de connexion root directe
- **PasswordAuthentication no** : Clés SSH uniquement
- **AllowUsers** : Restriction par utilisateur et IP

L'authentification par clés SSH asymétriques, c'est remplacer une serrure standard par une serrure biométrique.

Outils de Sécurité Essentiels

sudo : Pouvoir Contrôlé

Délégation granulaire des privilèges. Exemple : autoriser uniquement le redémarrage d'Apache2 pour un technicien

```
techN1 ALL=(ALL) NOPASSWD:
/usr/sbin/systemctl restart apache2
```

Fail2ban : Gardien Automatique

Surveille les logs et bannit automatiquement les IP suspectes. Efficace contre les attaques par force brute sur SSH, FTP, web.

Nftables : Le Pare-feu Moderne

Stratégie d'entreprise : **"Tout interdire par défaut, sauf ce qui est explicitement autorisé"**

01

Trafic Loopback

Autoriser tout le trafic sur la machine elle-même

02

Connexions Établies

Autoriser les connexions initiées par le serveur (established, related)

03

Port SSH

Autoriser les nouvelles connexions sur le port SSH (2222)

04

Politique par Défaut

Tout le reste est jeté (drop)

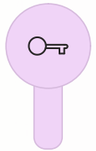
Travaux Pratiques : Déploiement srv-core01

Installation Minimale

Démarrer sur ISO netinst, partitionnement manuel, sélection SSH + utilitaires uniquement

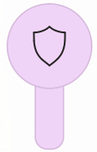
Configuration Initiale

Mise à jour système, installation sudo, création utilisateur admin



Clés SSH

Génération et déploiement de l'authentification par clé, configuration sshd_config



Fail2ban

Installation et configuration avec maxretry=3, bantime=1h

Nftables

Création /etc/nftables.conf, activation et tests de validation

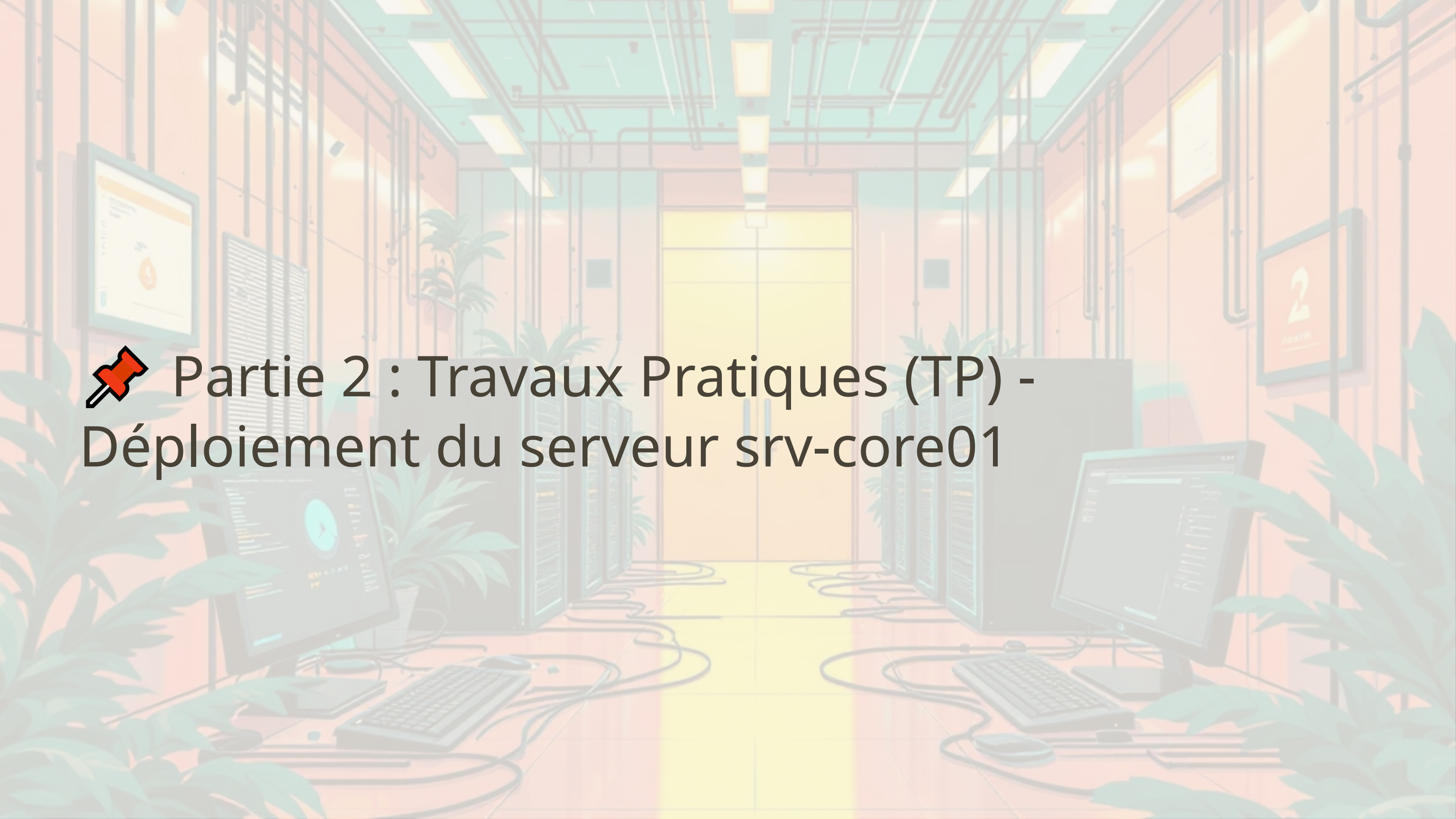
Compte-Rendu

Documentation complète pour la DSI avec schémas et résultats des tests

Mission Accomplie !

Vous avez déployé **srv-core01**, le premier maillon sécurisé de l'infrastructure d'Innov-Tech.

5	3	0
Partitions	Couches de Sécurité	Surface d'Attaque
Configurées pour sécurité et stabilité optimales	SSH durci, Fail2ban, Nftables	Installation minimale = risques minimaux



📌 Partie 2 : Travaux Pratiques (TP) - Déploiement du serveur srv-core01

Travaux Pratiques

Prise en Main & Sécurisation (Hardening) de Debian 13

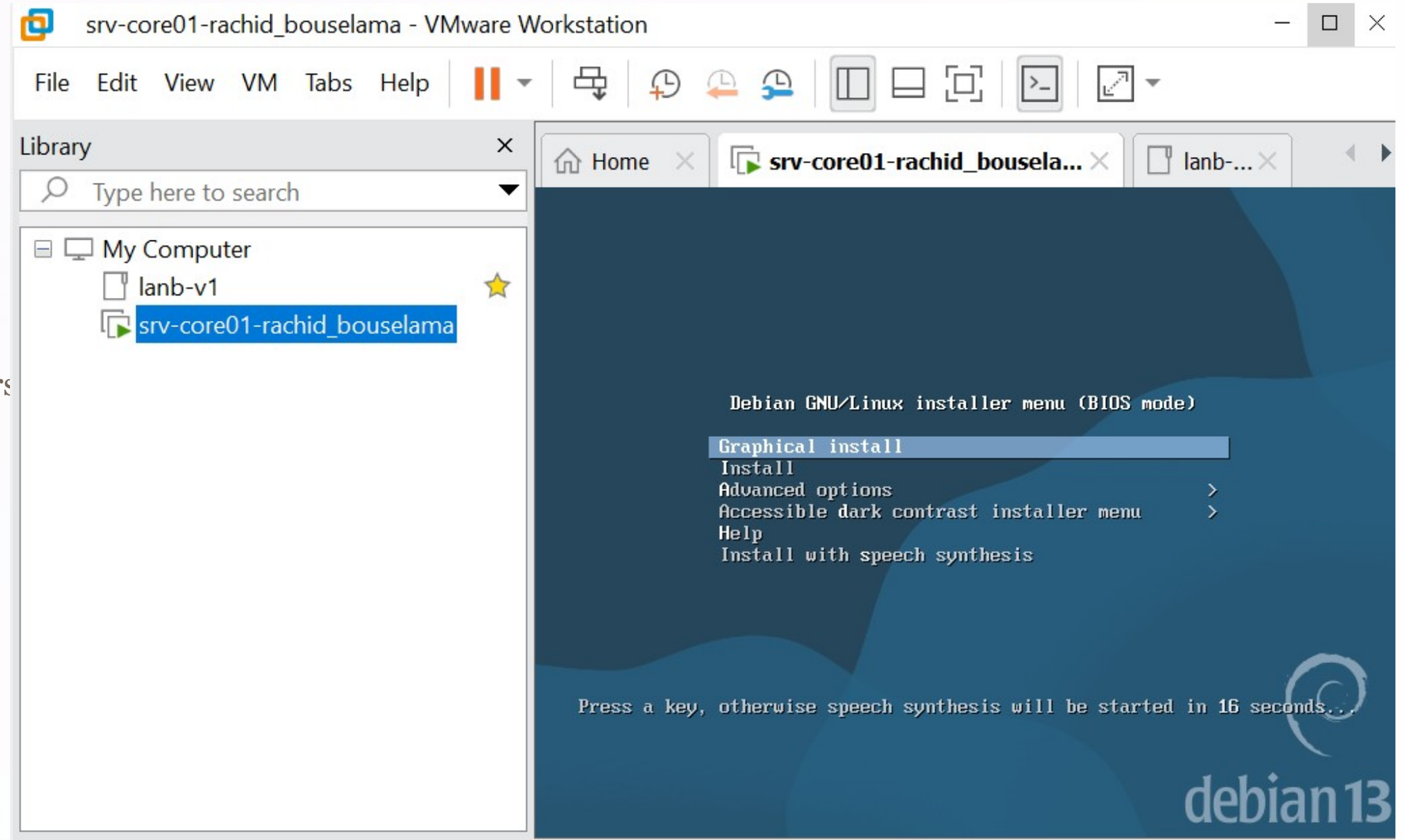
TP : Déploiement du serveur srv-core01

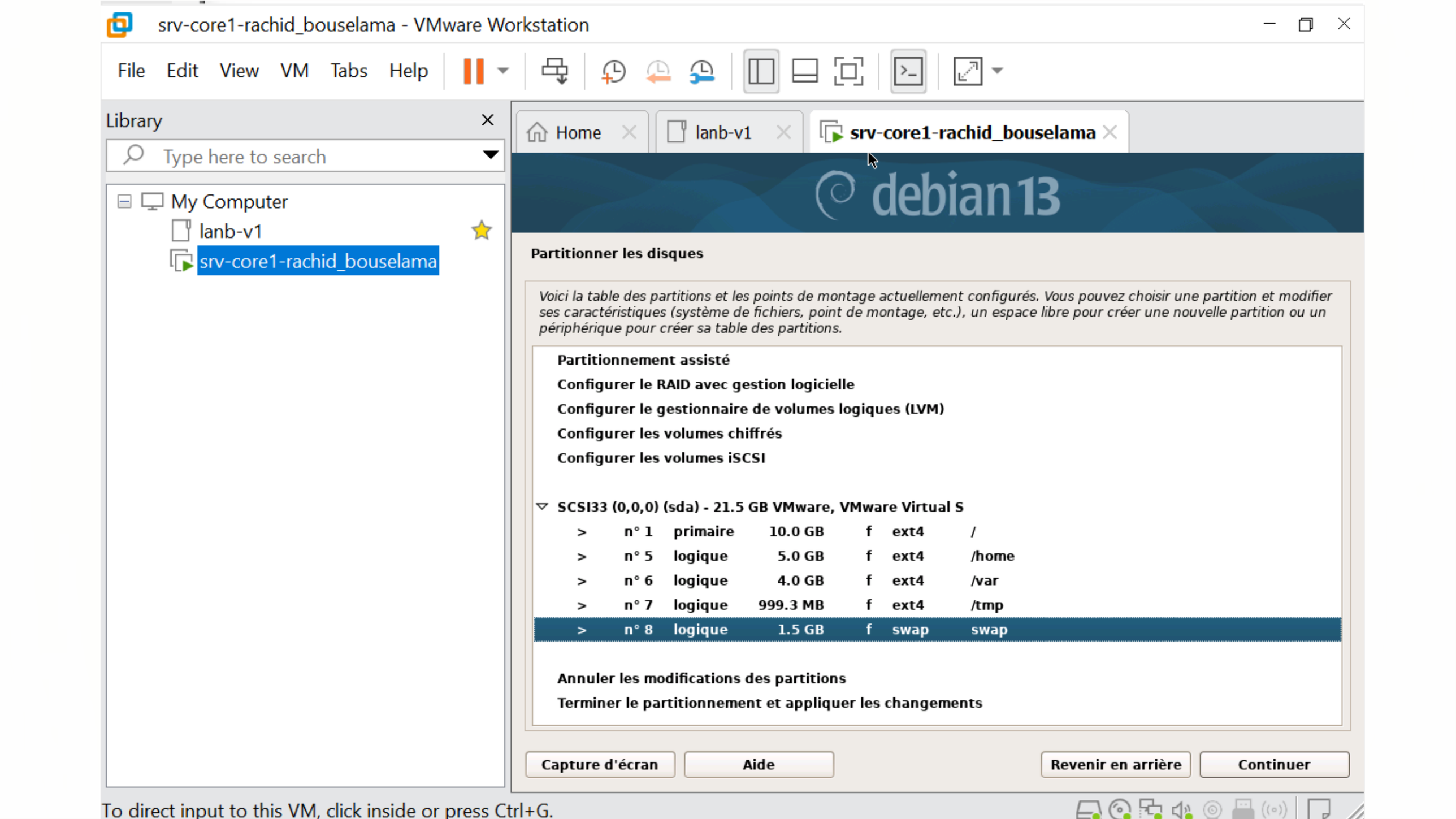
(Espace pour un logo ou une image)

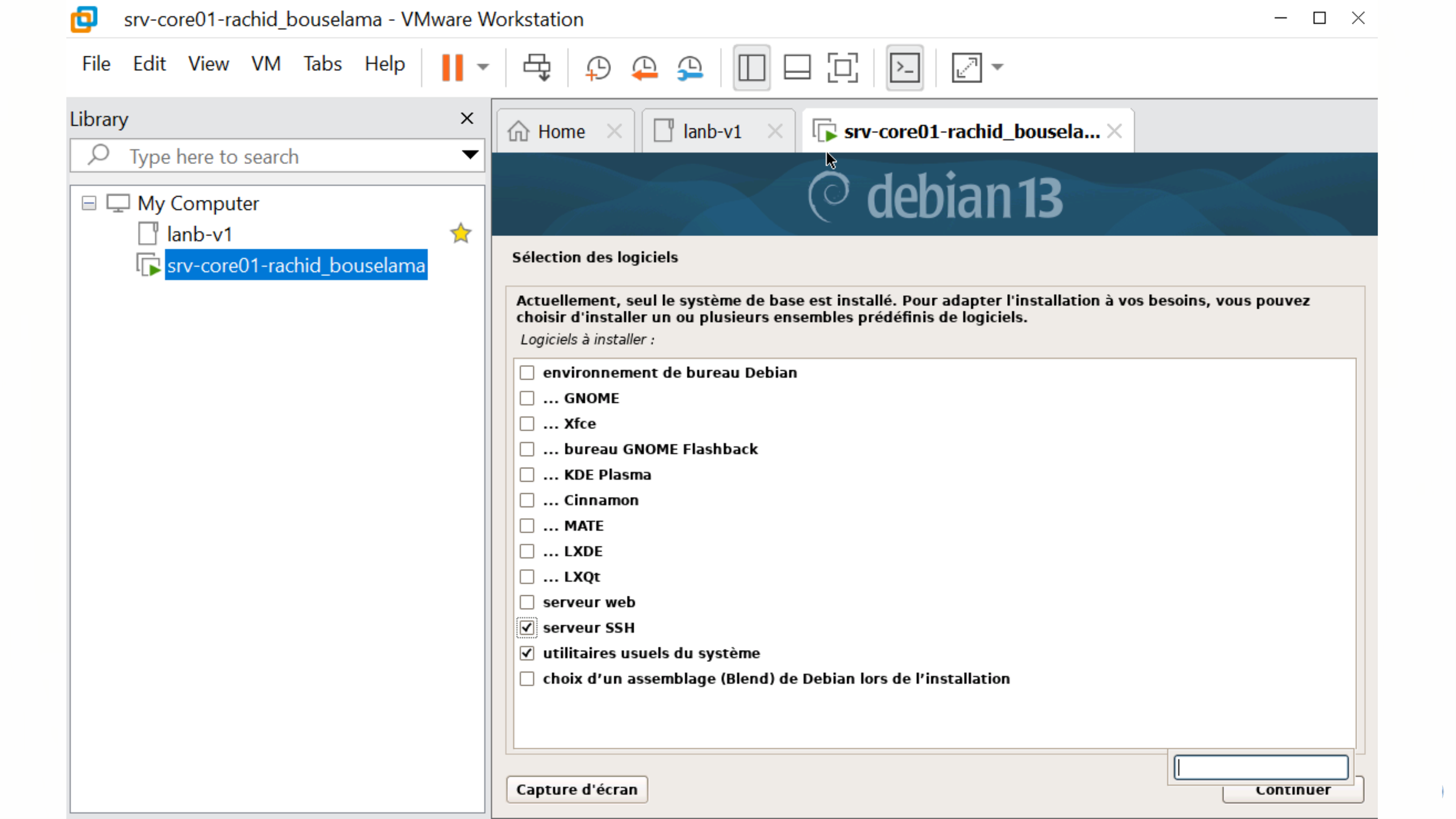
Étape 1 : Installation Minimale

Procédure d'installation

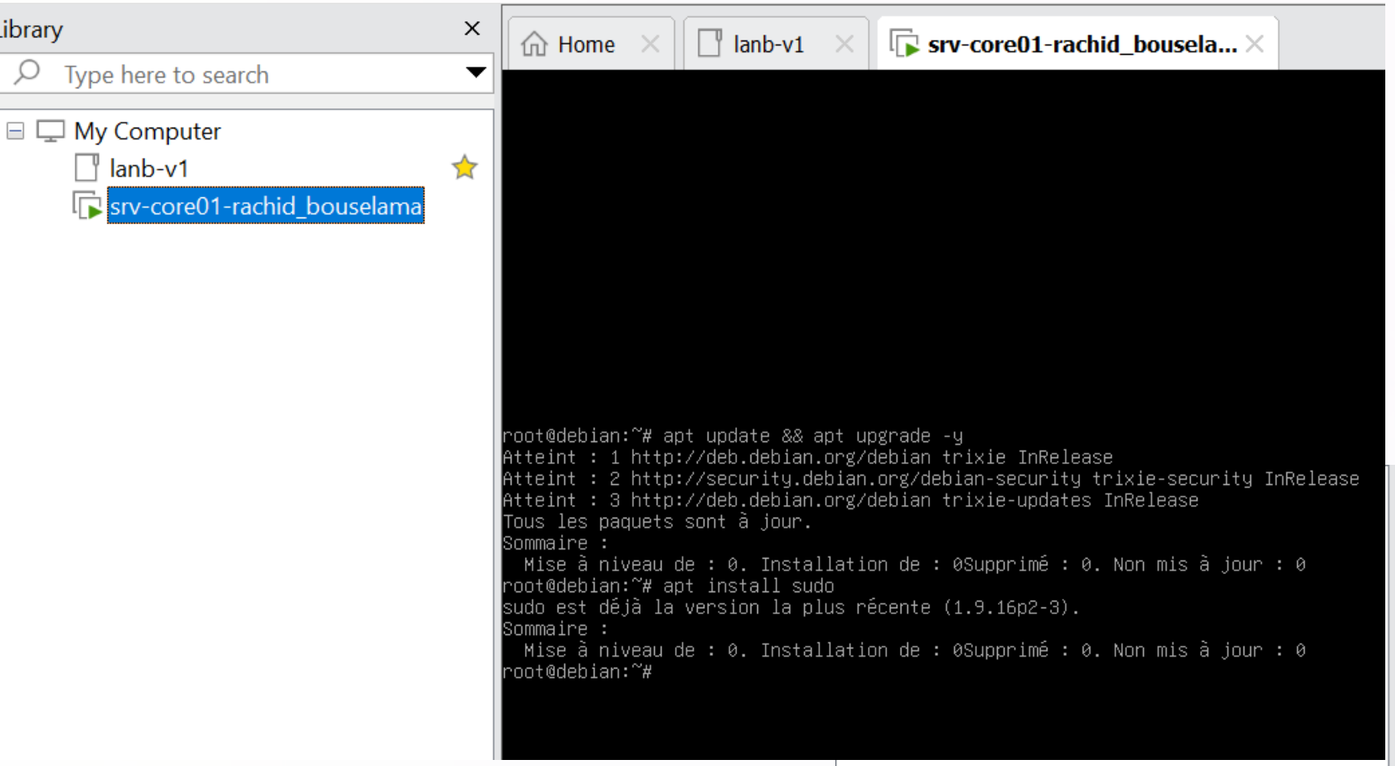
- Démarrer sur debian-13-netinst.iso
- Suivre l'installation en mode texte
- Choisir **partitionnement manuel**
- Créer les 5 partitions définies en cours
- Installer uniquement :
  - *Serveur SSH*
  - *Utilitaires usuels du système*

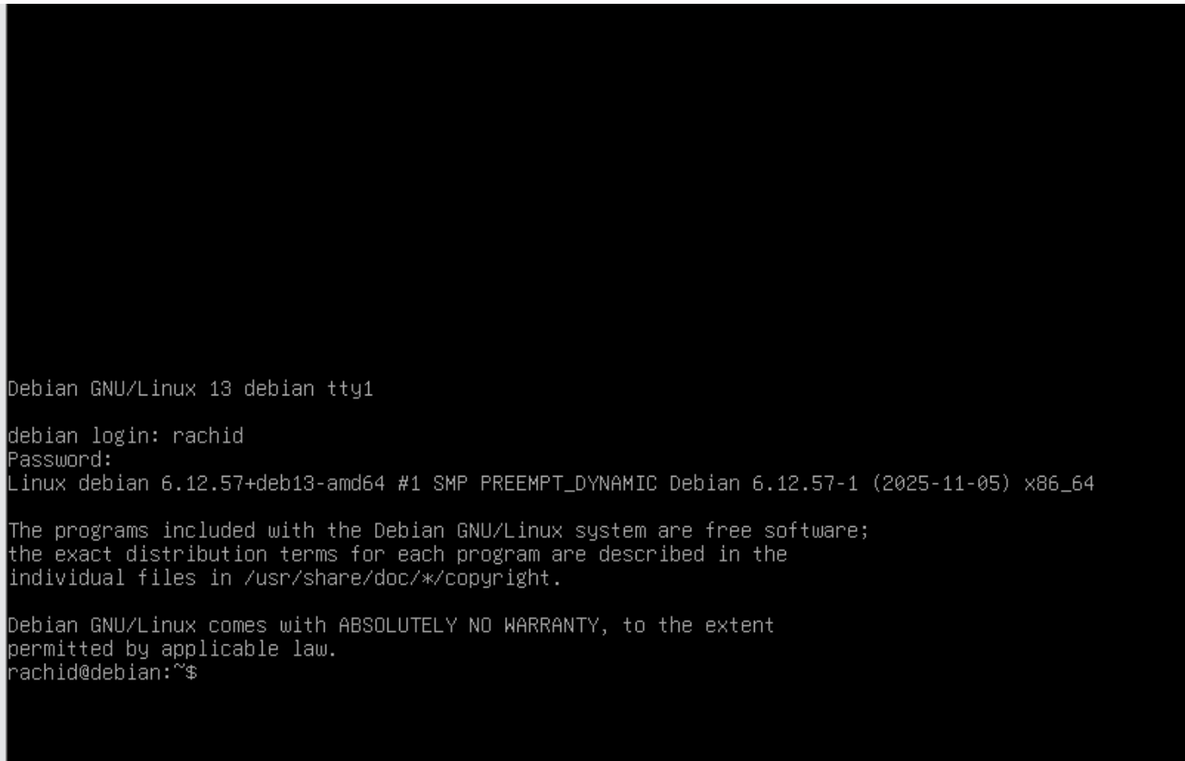



srv-core1-rachid_bouselama - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
lanb-v1
srv-core1-rachid_bouselama
Home
lanb-v1
srv-core1-rachid_bouselama
debian 13
Partitionner les disques
Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.
Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI
SCSI33 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
> n° 1 primaire 10.0 GB f ext4 /
> n° 5 logique 5.0 GB f ext4 /home
> n° 6 logique 4.0 GB f ext4 /var
> n° 7 logique 999.3 MB f ext4 /tmp
> n° 8 logique 1.5 GB f swap swap
Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
Capture d'écran
Aide
Revenir en arrière
Continuer
To direct input to this VM, click inside or press Ctrl+G.

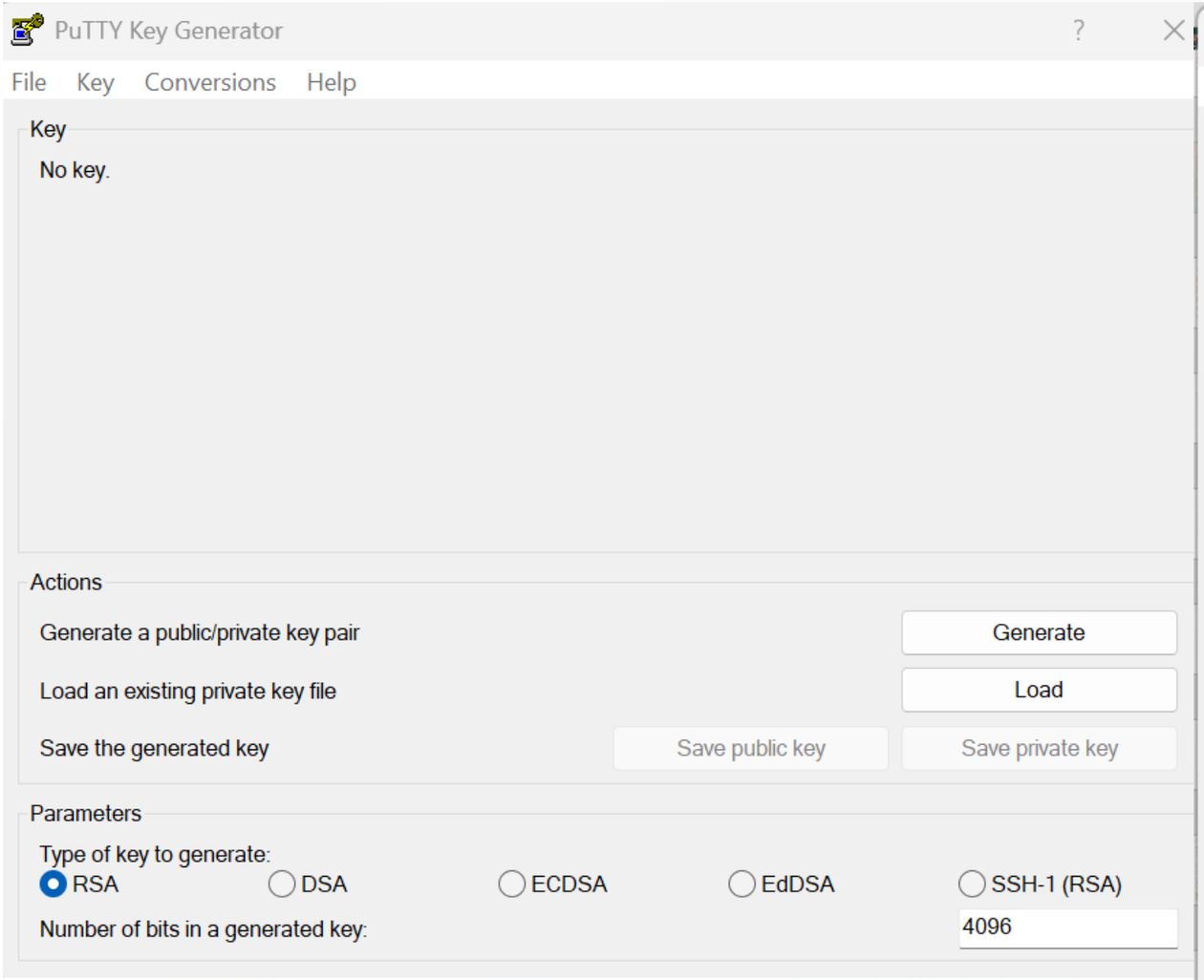

srv-core01-rachid_bouselama - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
lanb-v1
srv-core01-rachid_bouselama
Home
lanb-v1
srv-core01-rachid_bousela...
debian 13
Sélection des logiciels
Actuellement, seul le système de base est installé. Pour adapter l'installation 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
Capture d'écran
Continuer

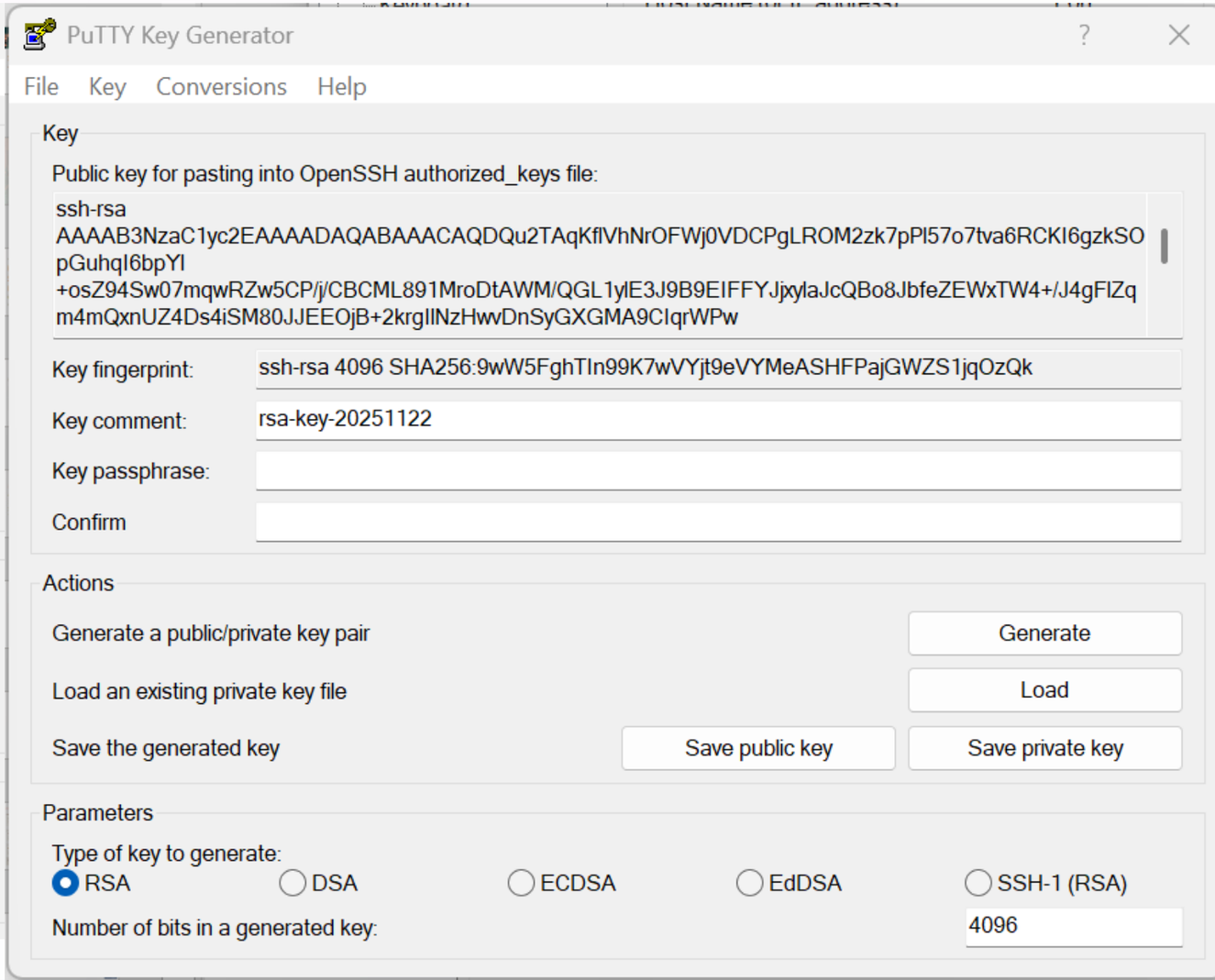
Étape 2 : Post-Installation

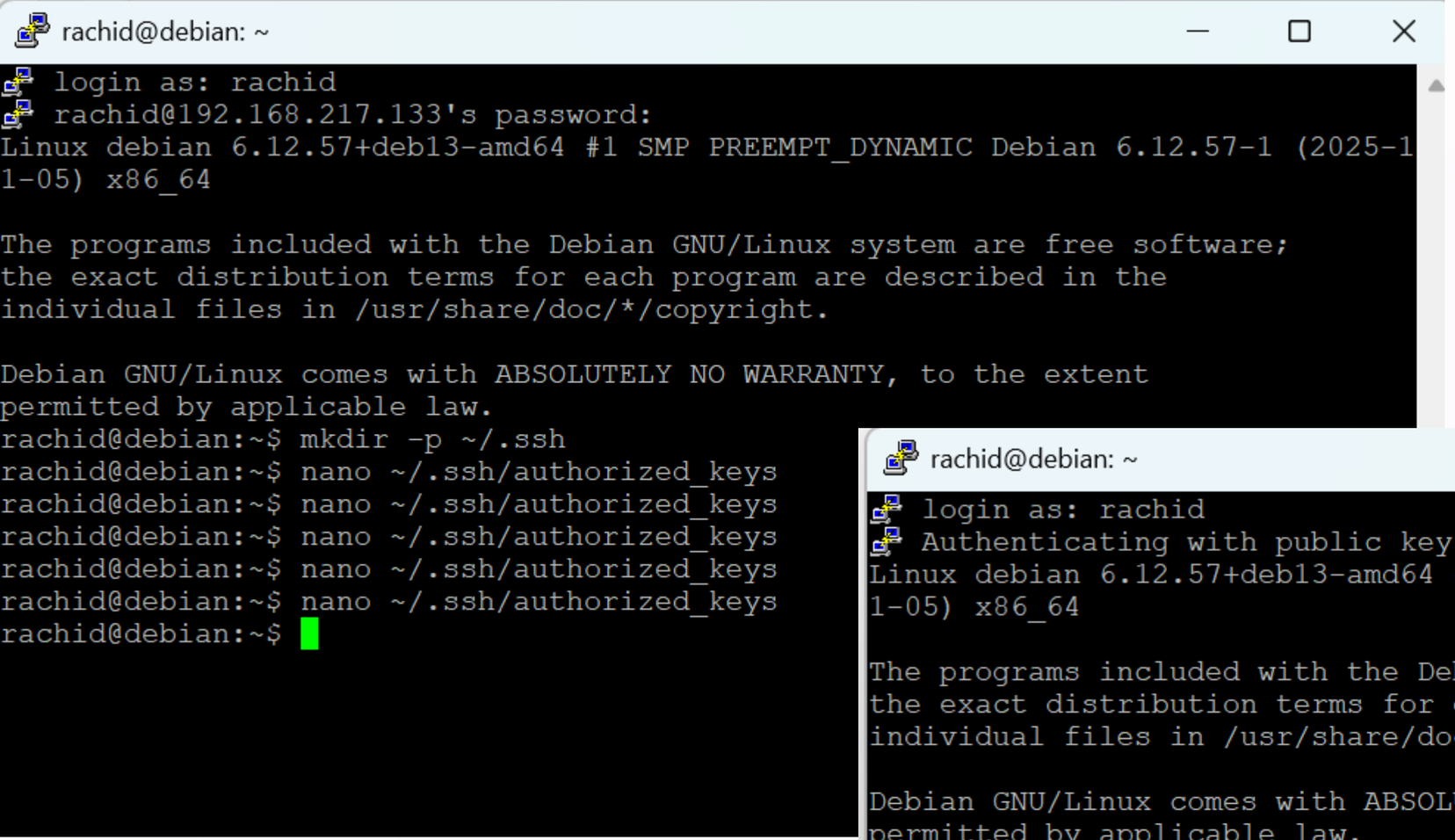


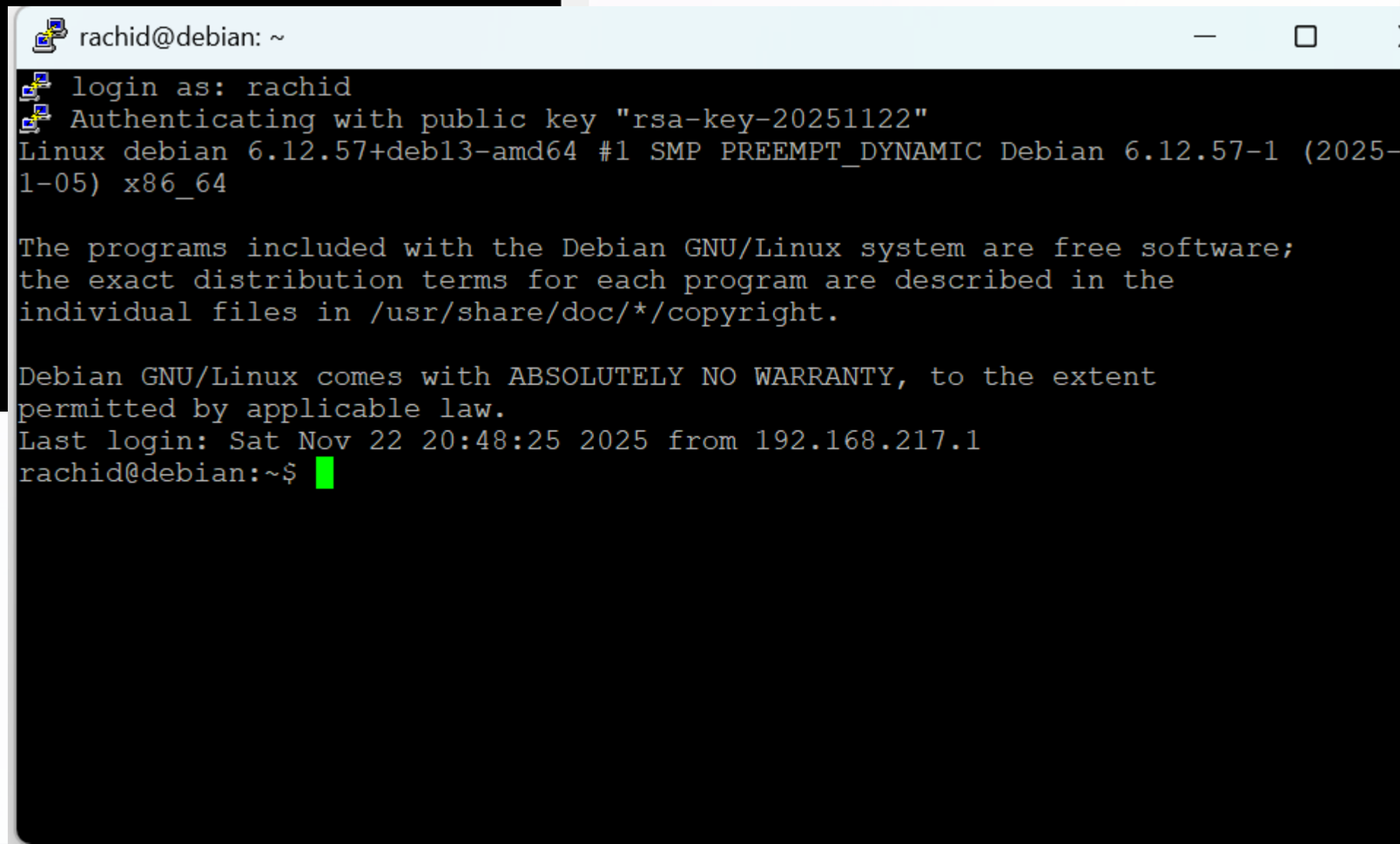


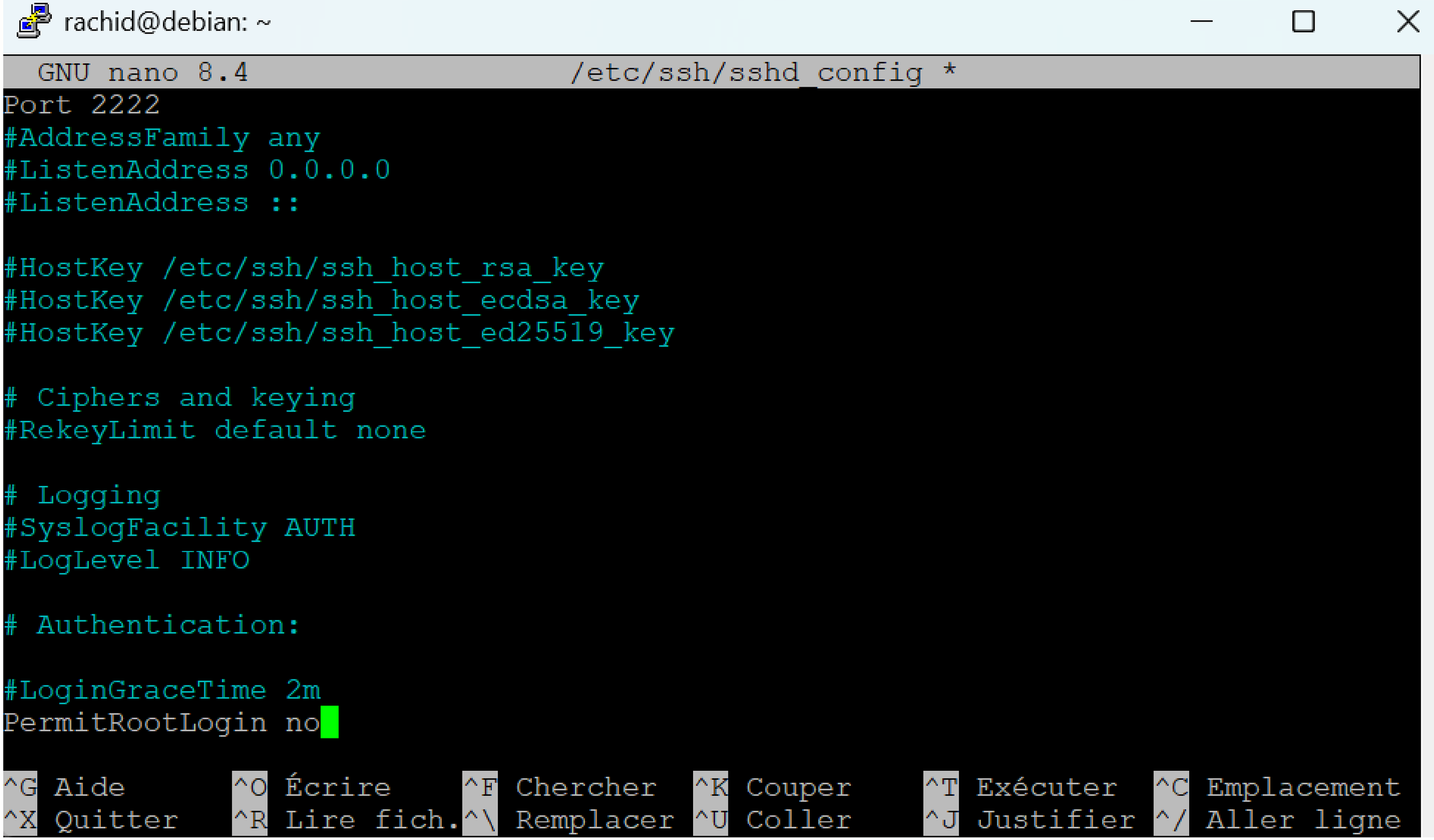
Étape 3 : Authentification SSH par clé



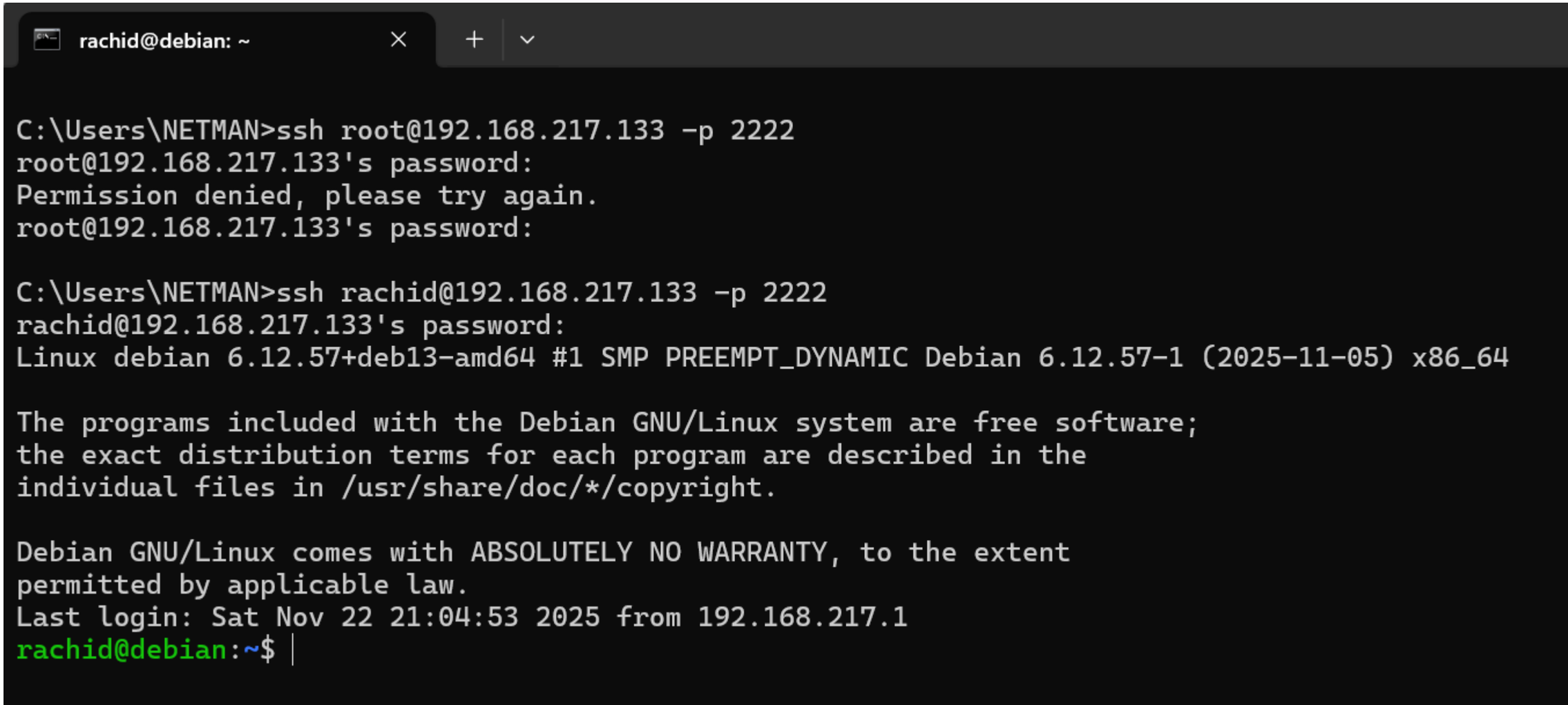



rachid@debian: ~
login as: rachid
rachid@192.168.217.133's password:
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
rachid@debian:~$ mkdir -p ~/.ssh
rachid@debian:~$ nano ~/.ssh/authorized_keys
rachid@debian:~$ nano ~/.ssh/authorized_keys
rachid@debian:~$ nano ~/.ssh/authorized_keys
rachid@debian:~$ nano ~/.ssh/authorized_keys
rachid@debian:~$ nano ~/.ssh/authorized_keys
rachid@debian:~$


rachid@debian: ~
login as: rachid
Authenticating with public key "rsa-key-20251122"
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) 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: Sat Nov 22 20:48:25 2025 from 192.168.217.1
rachid@debian:~$

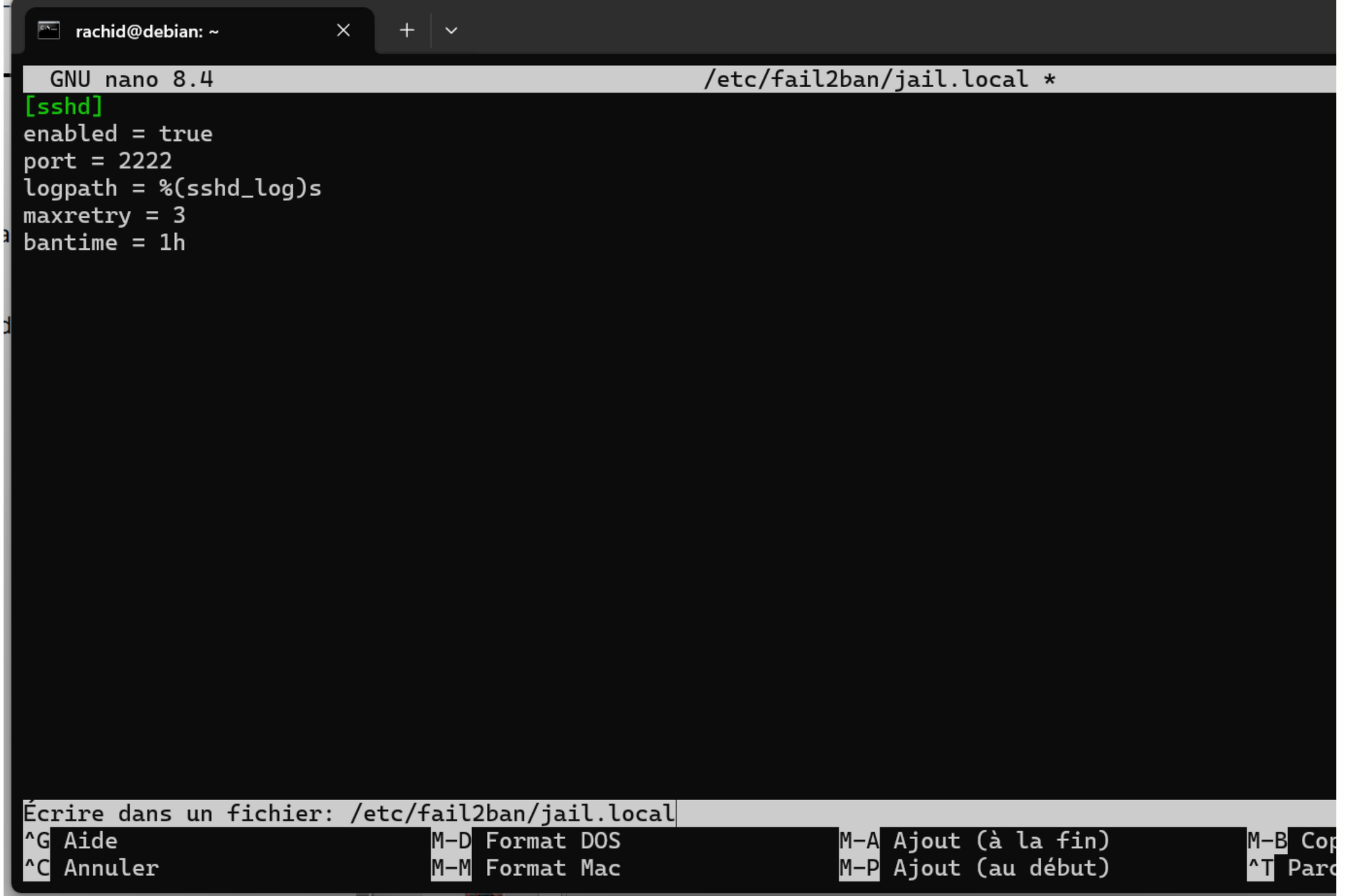

rachid@debian: ~
GNU nano 8.4 /etc/ssh/sshd_config *
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
Ciphers and keying
#RekeyLimit default none
Logging
#SyslogFacility AUTH
#LogLevel INFO
Authentication:
#LoginGraceTime 2m
PermitRootLogin no
^G Aide ^O Écrire ^F Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

Tests SSH


rachid@debian: ~
C:\Users\NETMAN>ssh root@192.168.217.133 -p 2222
root@192.168.217.133's password:
Permission denied, please try again.
root@192.168.217.133's password:
C:\Users\NETMAN>ssh rachid@192.168.217.133 -p 2222
rachid@192.168.217.133's password:
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) 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: Sat Nov 22 21:04:53 2025 from 192.168.217.1
rachid@debian:~$

Étape 4 : Mise en place de Fail2ban

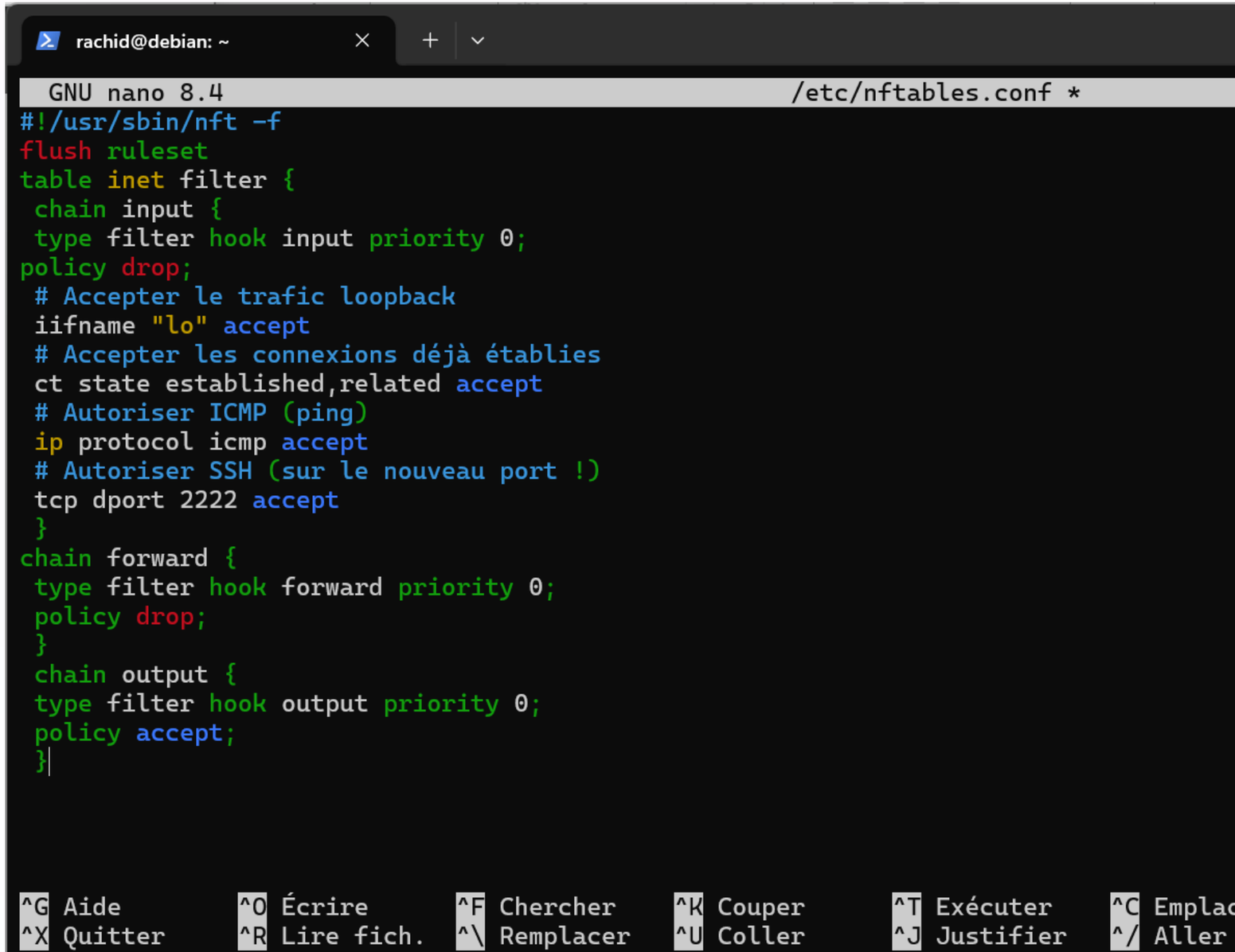
```
rachid@debian: ~
Mot de passe :
root@debian:/home/rachid# sudo apt install fail2ban
Installation de :
  fail2ban

Installation de dépendances :
  python3-autocommand       python3-jaraco.text     python3-pyinotify   python3-typing-extensions
  python3-inflect           python3-more-itertools  python3-setuptools  python3-zipp
  python3-jaraco.context    python3-pkg-resources   python3-systemd     whois
  python3-jaraco.functools  python3-pyasyncore      python3-typeguard

Paquets suggérés :
  mailx  system-log-daemon  monit  sqlite3  python-pyinotify-doc  python-setuptools-doc

Sommaire :
  Mise à niveau de : 0. Installation de : 16Supprimé : 0. Non mis à jour : 0
Taille du téléchargement : 1 861 kB
  Espace nécessaire : 9 106 kB / 17,7 GB disponible

Continuer ? [O/n] O
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 python3-systemd amd64 235-1+b6 [40,8 kB]
Réception de : 2 http://deb.debian.org/debian trixie/main amd64 fail2ban all 1.1.0-8 [466 kB]
Réception de : 3 http://deb.debian.org/debian trixie/main amd64 python3-autocommand all 2.2.2-3 [13,6 kB]
Réception de : 4 http://deb.debian.org/debian trixie/main amd64 python3-more-itertools all 10.7.0-1 [67,4 kB]
Réception de : 5 http://deb.debian.org/debian trixie/main amd64 python3-typing-extensions all 4.13.2-1 [90,5 k
Réception de : 6 http://deb.debian.org/debian trixie/main amd64 python3-typeguard all 4.4.2-1 [37,3 kB]
Réception de : 7 http://deb.debian.org/debian trixie/main amd64 python3-inflect all 7.3.1-2 [32,4 kB]
Réception de : 8 http://deb.debian.org/debian trixie/main amd64 python3-jaraco.functools all 4.1.0-1 [12,0 kB]
Réception de : 9 http://deb.debian.org/debian trixie/main amd64 python3-pkg-resources all 78.1.1-0.1 [224 kB]
```


rachid@debian: ~
GNU nano 8.4 /etc/fail2ban/jail.local *
[sshd]
enabled = true
port = 2222
logpath = %(sshd_log)s
maxretry = 3
bantime = 1h
Écrire dans un fichier: /etc/fail2ban/jail.local
^G Aide
M-D Format DOS
M-A Ajout (à la fin)
M-B Cop
^C Annuler
M-M Format Mac
M-P Ajout (au début)
^T Parc

```
déconnexion
Connection to 192.168.217.133 closed.
PS C:\Users\NETMAN> ssh rachid@192.168.217.133 -p 2222
rachid@192.168.217.133's password:
Permission denied, please try again.
rachid@192.168.217.133's password:
Permission denied, please try again.
rachid@192.168.217.133's password:
ssh_dispatch_run_fatal: Connection to 192.168.217.133 port 2222: Connection timed out
PS C:\Users\NETMAN>
PS C:\Users\NETMAN>
PS C:\Users\NETMAN>
PS C:\Users\NETMAN>
```

Étape 5 : Firewall nftables

Configuration du fichier /etc/nftables.conf



```
nov. 22 22:16:21 debian systemd[1]: Starting nftables.service - nftables...
nov. 22 22:16:21 debian nft[2540]: /etc/nftables.conf:24:1-1: Error: syntax error, unexpe
nov. 22 22:16:21 debian nft[2540]:  }
nov. 22 22:16:21 debian nft[2540]: ^
nov. 22 22:16:21 debian systemd[1]: nftables.service: Main process exited, code=exited, s
nov. 22 22:16:21 debian systemd[1]: nftables.service: Failed with result 'exit-code'.
nov. 22 22:16:21 debian systemd[1]: Failed to start nftables.service - nftables.
root@debian:/home/rachid#  sudo nano /etc/nftables.conf
root@debian:/home/rachid# sudo systemctl start nftables
root@debian:/home/rachid# sudo systemctl enable nftables
Created symlink '/etc/systemd/system/sysinit.target.wants/nftables.service' → '/usr/lib/s
.
root@debian:/home/rachid# sudo systemctl enable nftables
root@debian:/home/rachid#
```

```
PS C:\Users\NETMAN> ping 192.168.217.133

Envoi d'une requête 'Ping'  192.168.217.133 avec 32 octets de données :
Réponse de 192.168.217.133 : octets=32 temps<1ms TTL=64
Réponse de 192.168.217.133 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.217.133:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
PS C:\Users\NETMAN> ssh rachid@192.168.217.133 -p 2222
rachid@192.168.217.133's password:
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) 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: Sat Nov 22 22:13:21 2025 from 192.168.217.1
rachid@debian:~$
```

📝 Compte-Rendu – Déploiement et Sécurisation du Serveur srv-core01

1. Schéma de partitionnement choisi & justification

Partitionnement manuel avec 5 partitions :

Partition	Point de montage	Rôle	Justification
/	racine	Système principal	Séparer le système des données utilisateurs
/home	données users	Stockage des comptes	Protège les données en cas de problème système
/var	logs & services	Services, logs, paquets	Évite qu'un log trop gros remplisse /
/tmp	fichiers temporaires	Sécurité & nettoyage	Isolation des fichiers temporaires
swap	mémoire virtuelle	Gestion RAM	Améliore la stabilité si RAM saturée

✔ **Partitionnement sécurisé**

✔ **Prévention des débordements**

✔ **Séparation logique des données**

1. Mesures de sécurité SSH mises en place

1

Authentification par clé SSH

- Suppression de l'usage des mots de passe
- Ajout de la clé publique RSA 4096 bits
- Connexion protégée, impossible à brute-forcer

2

Changement du port SSH

- Port par défaut 22 → 2222
- Réduction des scans automatisés

3

Désactivation du login root

- PermitRootLogin no
- Empêche les attaques directes sur le compte root

4

Désactivation de PasswordAuthentication

- Seules les clés SSH sont autorisées
- Bloque toutes les attaques par mot de passe

5

Redémarrage et test du service SSH

✔ **SSH entièrement sécurisé**

✔ **Prévention brute-force + scans**

1. Configuration du firewall nftables (commentée)

Voici le fichier utilisé :

🔎 Explication rapide :

policy drop

Tout est bloqué par défaut

loopback

Nécessaire au fonctionnement interne

established,related

Permet les connexions déjà ouvertes

icmp

Autorise ping pour diagnostic

ssh 2222

Autorise votre accès administrateur

✔ **Firewall minimal, clair et sécurisé**

✔ **Surface d'attaque très réduite**

1. Résultats des tests de validation

Test SSH (clé uniquement)

- Connexion sans mot de passe → OK
- Connexion root → Refusée (OK)
- Connexion port 2222 → OK

Test Fail2ban

Actions réalisées :

- 3 tentatives SSH invalides
- Fail2ban détecte → ban de l'IP

Vérification avec :

```
sudo fail2ban-client status sshd
```

→ L'IP apparaît dans la liste des bannis

Test nftables

- Connexion SSH toujours active → OK
- Ping serveur → OK
- Tout autre port → Bloqué (OK)

Conclusion

Le serveur srv-core01 est maintenant :

- correctement installé
- durci selon les bonnes pratiques
- protégé contre brute-force
- équipé d'un firewall efficace
- sécurisé via SSH + clés + Fail2ban

C'est le premier maillon sécurisé de l'infrastructure Innov-Tech.