Proxmox - Installation et configuration

---

1. Télécharger Proxmox VE :

Afin de télécharger "Proxmox VE 8.4 ISO Installer", cliquez sur le lien :
Téléchargement de l'ISO Proxmox VE
ou rendez-vous sur :
Site Web de Proxmox - Section Download afin de vérifier qu'il s'agit bien de la dernière version disponible.

---

2. Réaliser une clé bootable de Proxmox VE :

À partir d'un utilitaire permettant de réaliser une clé bootable (Rufus, Balena ou Ventoy), créer une clé bootable contenant l'ISO de Proxmox VE.

---

3. Installation de Proxmox VE :

3.1. Identifier un ordinateur ayant la configuration requise :

- **CPU** : Intel 64 ou AMD64 avec Intel VT-d/AMD-Vi.
    - Mémoire **RAM** :
    - Minimum 2 GB pour l'OS Proxmox VE et les services ;
    - 1 à 8 GB par VM;
    - 1 GB de mémoire pour chaque TB de stockage utilisé par Ceph ou ZFS.
- Du **stockage** de type **SSD** de préférence :
    - **Stockage du système d'exploitation (OS)** :
        - **RAID matériel** avec une **mémoire cache d'écriture protégée par batterie (BBU)** ;
        - Ou **système sans RAID** utilisant **ZFS avec un cache SSD**.
    - **Stockage des machines virtuelles (VM)** :
        - Pour un **stockage local** : **RAID matériel avec cache d'écriture BBU** ;
        - Ou **système sans RAID avec ZFS**.
- **Cartes réseau (NIC)** : **Cartes réseau Gbit redondantes**, avec **cartes supplémentaires** selon technologie de stockage et configuration du cluster souhaitées.

3.2. Installer Proxmox :

- Insérer la clé USB sur la tour sélectionnée ;
- Démarrer l'ordinateur ;
- Booter sur la clé USB (UEFI) ;
- Suivre les instructions d'installation : [Documentation Proxmox VE - Installation]

---

4. Gestion des dépôts :

4.1. Se connecter en SSH :

- Ouvrir un terminal (Windows ou Linux) et exécuter la commande :

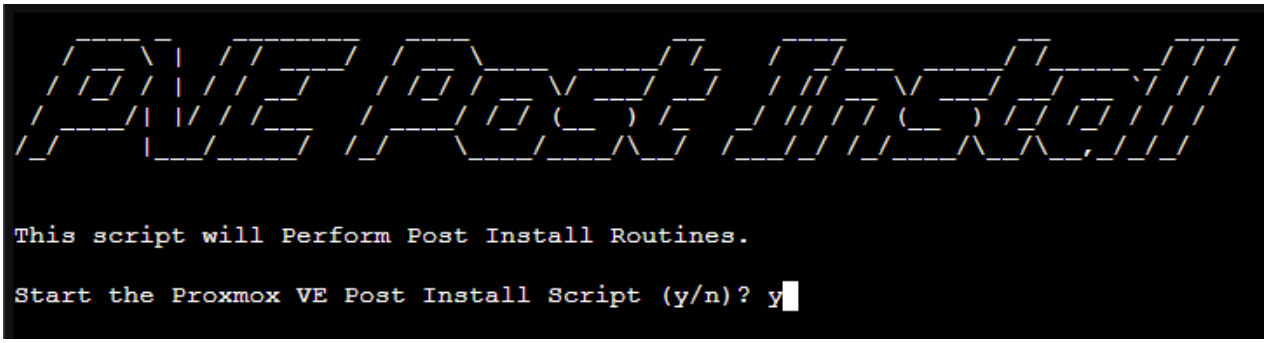
```
ssh root@<@ip_du_serveur>
```

4.2. Via le script **post-pve-install.sh** :

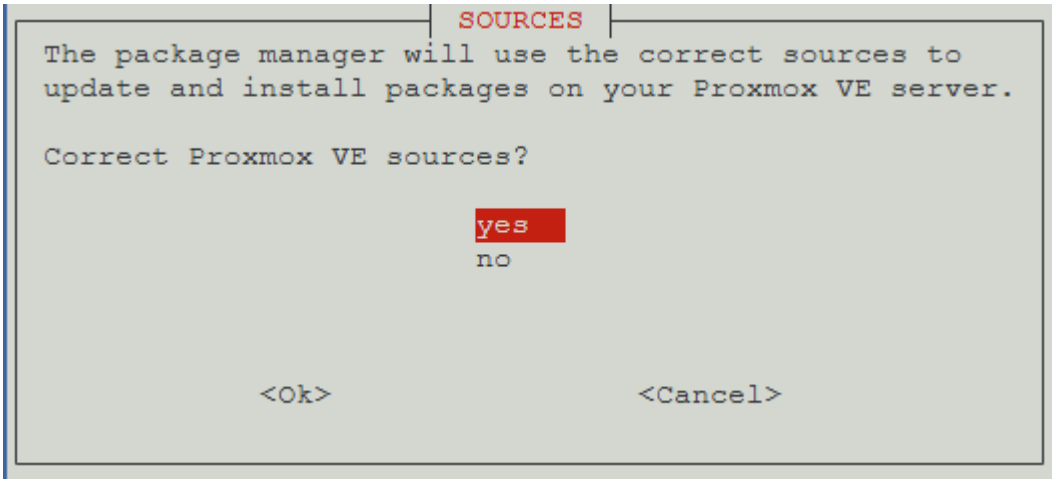
- Exécuter la commande :

```
bash -c "$(curl -fsSL [https://raw.githubusercontent.com/community-
scripts/ProxmoxVE/main/tools/pve/post-pve-install.sh]
(https://raw.githubusercontent.com/community-
scripts/ProxmoxVE/main/tools/pve/post-pve-install.sh))"
```

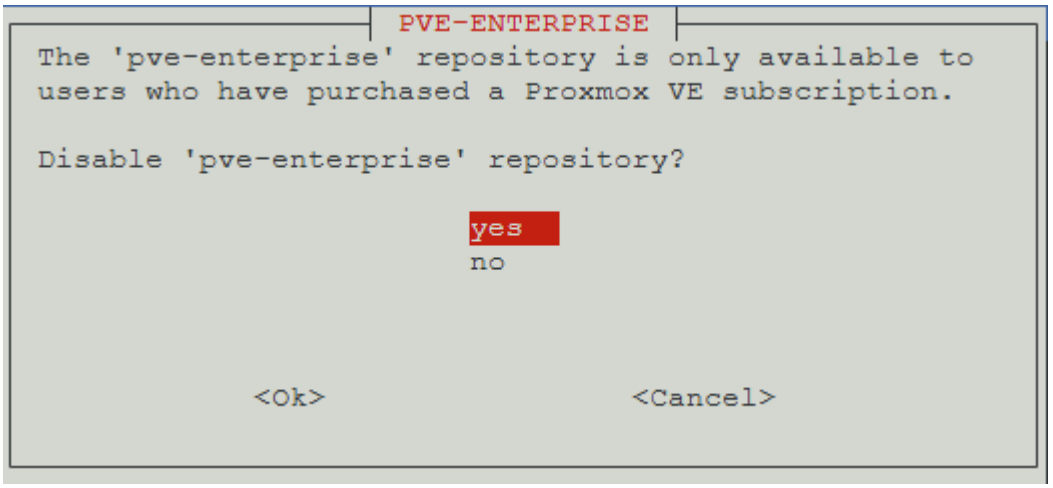
- Lancement de PVE Post Install :



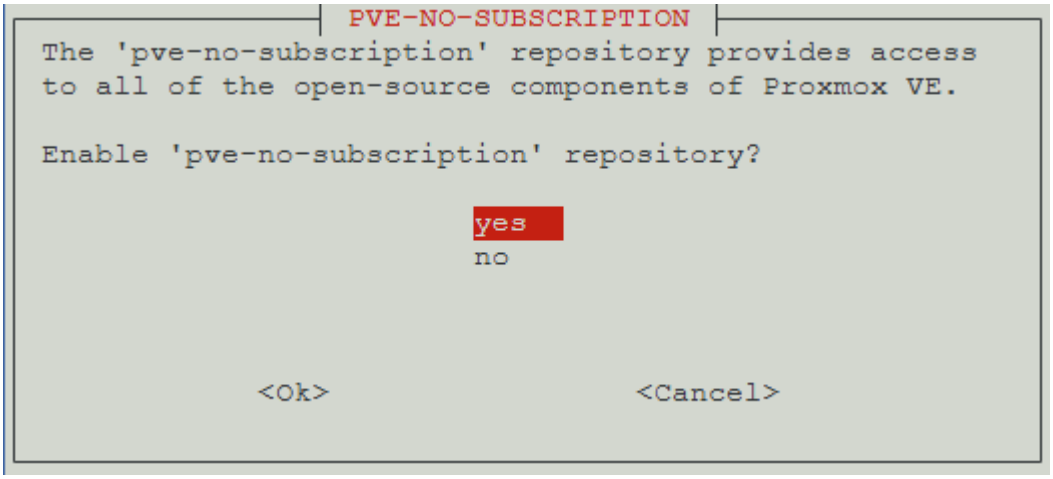
- Changer les sources :



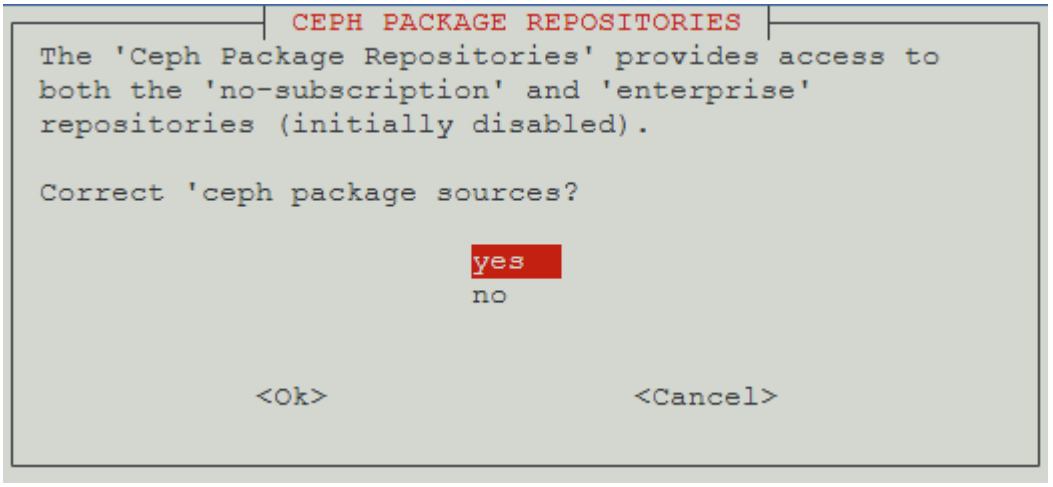
- Désactiver le dépôt entreprise :



- Activer le dépôt sans abonnement :

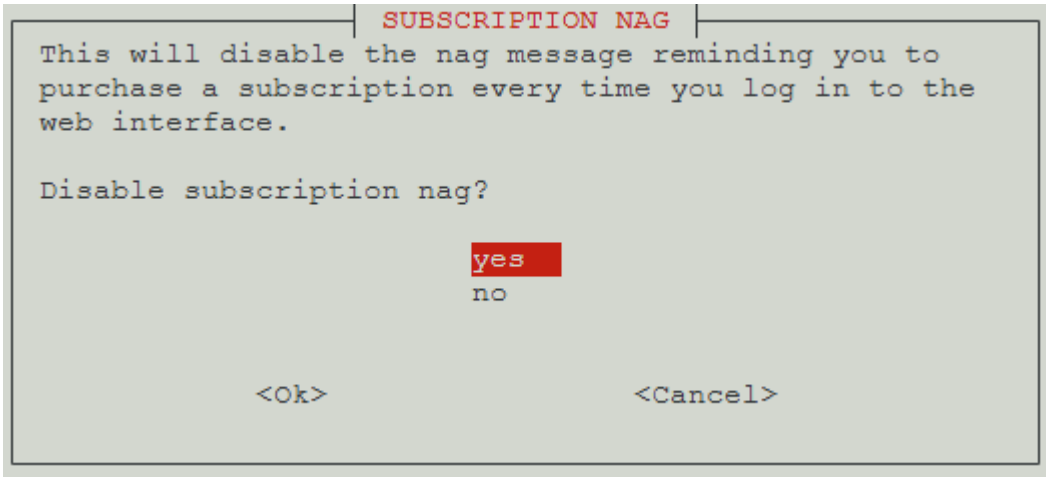


- Corriger le dépôt de ceph :



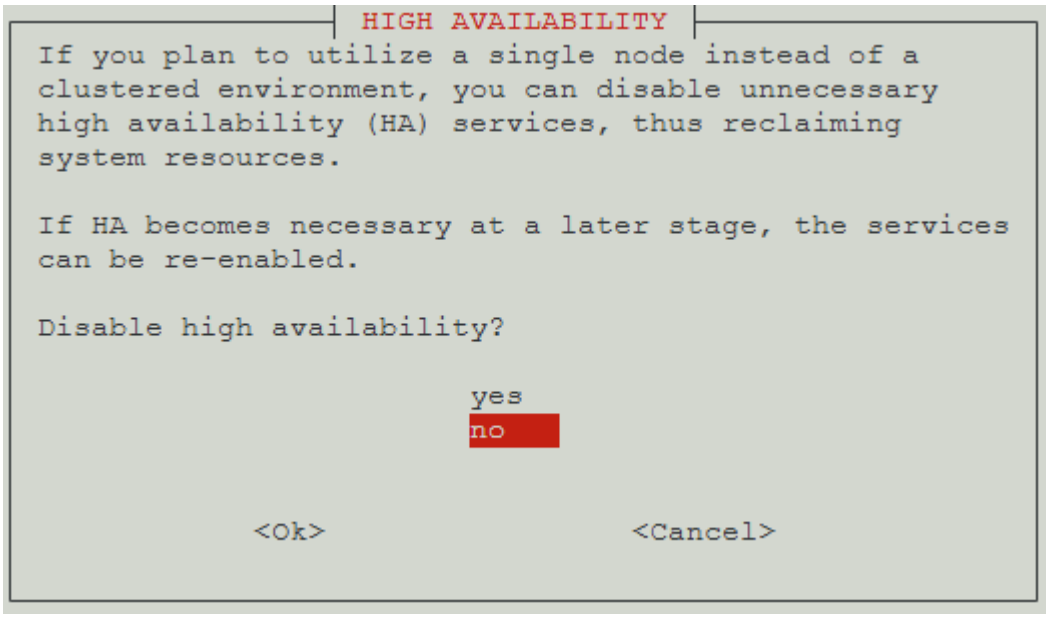
- Désactiver le dépôt de test :

- Désactiver le message à propos de la licence :

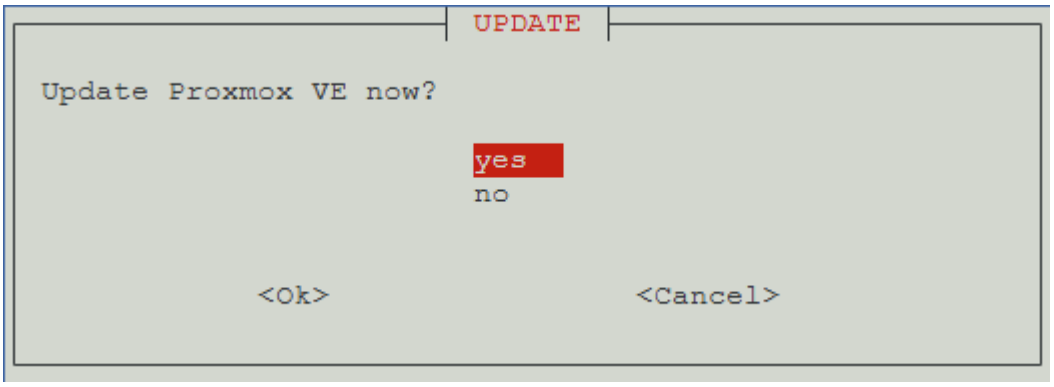


- Valider le choix précédent :

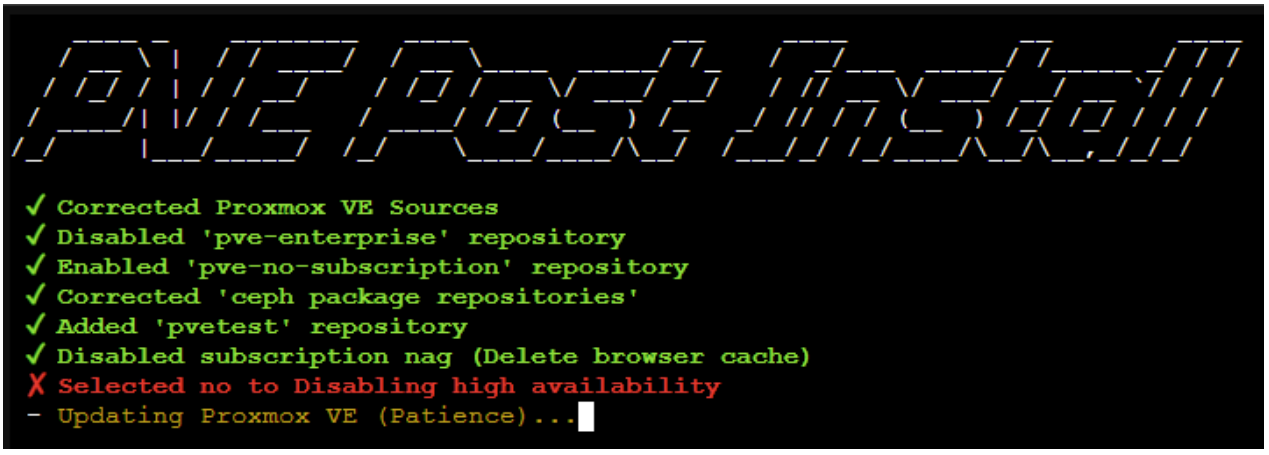
- Désactiver la haute disponibilité (cas d'un cluster) :



- Valider la mise à jour de Proxmox Backup Server :



- Exécution du script avec les opérations demandées :



- Redémarrer le server.

4.3. Via les fichiers de configuration :

4.3.1. Activer le dépôt "**no subscription" :

- Depuis l'interface "**root**" :
  - Cliquez sur le nœud concerné ;
  - Cliquez sur "**Updates**" ;
  - Cliquez sur "**Repositories**" ;
  - Cliquez sur "**Add**" ;
- Dans la fenêtre "**Add: Repository**" :
  - Dans le menu déroulant "**Repository**", sélectionnez "**No-Subscription**" ;
  - Cliquez sur "**Add**".

4.3.2. Désactiver les dépôts "pve-enterprise" et "ceph" :

- Éditer le fichier **ceph.list** :

```
nano /etc/apt/sources.list.d/ceph.list
```

- Commenter la ligne suivante :

```
#deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise
```

- Éditer le fichier **pve-enterprise.list** :

```
nano /etc/apt/sources.list.d/pve-enterprise.list
```

- Commenter la ligne suivante :

```
#deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
```

---

5. Administrer le serveur Proxmox depuis la machine :

5.1. Se connecter en SSH :

- Ouvrir un terminal (Windows ou Linux) et exécuter la commande :

```
ssh root@<@ip_du_serveur>
```

5.2. Créer un utilisateur "admin" non-root et l'ajouter au groupe sudo :

- Installer **sudo** :

```
apt-get update
apt-get install sudo
```

- Créer l'utilisateur :

```
useradd -m <admin_name> && usermod -aG sudo <admin_name> && passwd
<admin_name>
```

5.3. Mettre à jour Proxmox :

- Exécuter la commande :

```
apt-get update && apt-get upgrade && apt-get clean -y && apt-get autoremove
```

5.4. Configurer le fichier /etc/hosts :

- Éditer le fichier **/etc/hosts** :

```
nano /etc/hosts
```

- Modifiez le fichier comme suit :

```
127.0.0.1                   localhost
<ip_address>                <server_name>.<domain_name>.local pve<n°_noeud>
```

5.5. Sécuriser l'accès à Proxmox avec Fail2Ban :

5.5.1. Installer Fail2ban :

- Exécuter les commandes :

```
sudo apt-get update
sudo apt-get install fail2ban
```

5.5.2. Configurer Fail2Ban :

- Copier le fichier "**jail.conf**" vers "**jail.local**" :

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

- Éditer le fichier "**jail.local**" avec le commande :

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

- Compléter le fichier comme suit :

```
[proxmox]
enabled = true
port = https,http,8006
filter = proxmox
backend = systemd
maxretry = 3
findtime = 2d
bantime = 1h
ignoreip = 127.0.0.1/8 <local_networks>
```

- Éditer le fichier "**sshd.local**" avec la commande :

```
nano /etc/fail2ban/jail.d/sshd.local
```

- Compléter le fichier comme suit :

```
[sshd]
enabled = true
port = ssh
logpath = /var/log/auth.log
backend = systemd
ignoreip = 127.0.0.1/8 <local_networks>
```

- Créer le fichier "**proxmox.conf**" avec la commande :

```
nano /etc/fail2ban/filter.d/proxmox.conf
```

- Compléter le fichier comme suit :

```
[Definition]
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoregex =
journalmatch = _SYSTEMD_UNIT=pvedaemon.service
```

- Tester la configuration :

```
fail2ban-client -t
fail2ban-regex systemd-journal /etc/fail2ban/filter.d/proxmox.conf --print-all-matched
```

- Redémarrer le service :

```
systemctl restart fail2ban
```

- Consulter le statut de fail2ban avec la commande :

```
fail2ban-client status proxmox
```

5.6. Redémarrer le système :

- Exécuter la commande :

```
reboot
```

---

6. Administrer le serveur Proxmox depuis l'interface Web :

6.1. Se connecter à l'interface Web de Proxmox :

- Depuis le navigateur de votre choix, accéder à :

```
https://<server_address>:8006
```

6.2. Créer un cluster (le cas échéant) :

- Sélectionner la "**Vue serveur**" (*Server view*);
- Cliquer sur "**Centre de données**" (*Datacenter*);
- Cliquer sur "**Grappe de serveurs**" (*Cluster*);
- Cliquer sur le bouton "**Créer une grappe de serveurs**" (*Create Cluster*) ;
- Compléter la fenêtre en nommant le cluster et en indiquant l'IP du nœud "**maître**" (*Master*).

6.3. Ajouter un nœud au cluster (le cas échéant) :

6.3.1. Depuis le nœud "maître" :

- Cliquer sur "**Centre de données**" (*Datacenter*) ;
- Cliquer sur "**Grappe de serveurs**" (*Cluster*) ;
- Cliquer sur "**Informations de jonction**" (*Join Information*) ;
- Cliquer sur le bouton "**Copier l'information**" (*Copy Information*).

6.3.2. Depuis le nœud à joindre :

- Cliquer sur "**Centre de données**" (*Datacenter*) ;
- Cliquer sur "**Grappe de serveurs**" (*Cluster*) ;
- Cliquer sur "**Joindre la grappe de serveurs**" (*Join Cluster*);
- Dans la fenêtre affichée:
  - Coller les informations de jonction (du nœud "maître") ;
  - Saisisser le mot de passe "root" du nœud "maître" ;
  - Cliquer sur "**Joindre grappe de serveurs...**" (*Join Cluster*).

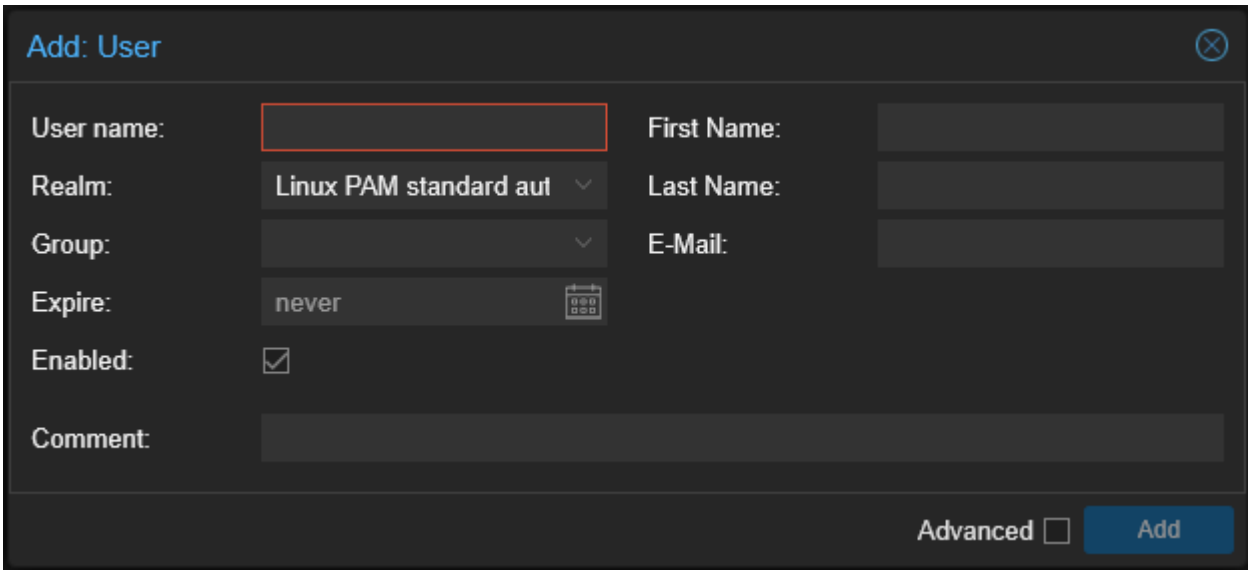
6.4. Sécuriser l'accès à Proxmox:

6.4.1. Gestion des utilisateurs :

6.4.1.1. Créer l'utilisateur "admin" non-root :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
  - Cliquer sur "**Centre de données**" (*Datacenter*) ;
  - Cliquer sur "**Permissions**" (*Permissions*) ;
  - Cliquer sur "**Utilisateurs**" (*Users*);

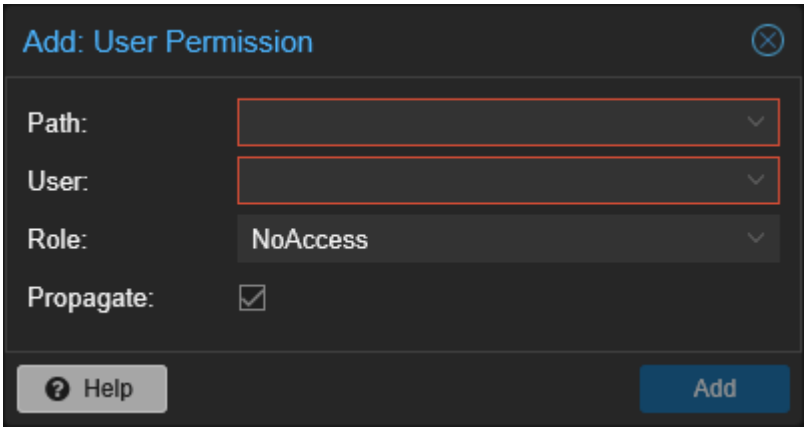
- Cliquer sur "**Ajouter**" (*Add*) et renseigner la fenêtre suivante :



avec "**Nom d'utilisateur : admin**" (*User name*) ; "**Royaume : pam**" (*Realm*).

6.4.1.2. Affectez des permission à l'utilisateur "admin" :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
  - Cliquer sur "**Centre de données**" (*Datacenter*) ;
  - Cliquer sur "**Permissions**" (*Permissions*) ;
  - Cliquer sur "**Ajouter**" (*Add*)
- Cliquez sur "Permissions de l'utilisateur" (*User Permission*) et renseignez la fenêtre suivante :



avec :

- le "**chemin d'accès de la source**" (*Path*) ;
- l'**utilisateur** concerné (*User*), ici **<admin_name>** ;
- le **rôle** (*role*), ici **PVEAdmin**.

6.4.2. Restriction d'accès :

6.4.2.1. Désactiver l'accès "root" en SSH sur le serveur Proxmox :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :

    - Cliquez sur le nœud Proxmox ("**pve**") ;
    - Cliquez sur "**Shell**".
- Éditer le fichier "**sshd_config**" :

```
nano /etc/ssh/sshd_config
```

- Commenter la ligne "**PermitRootLogin prohibit-password**" :

```
#PermitRootLogin prohibit-password
```

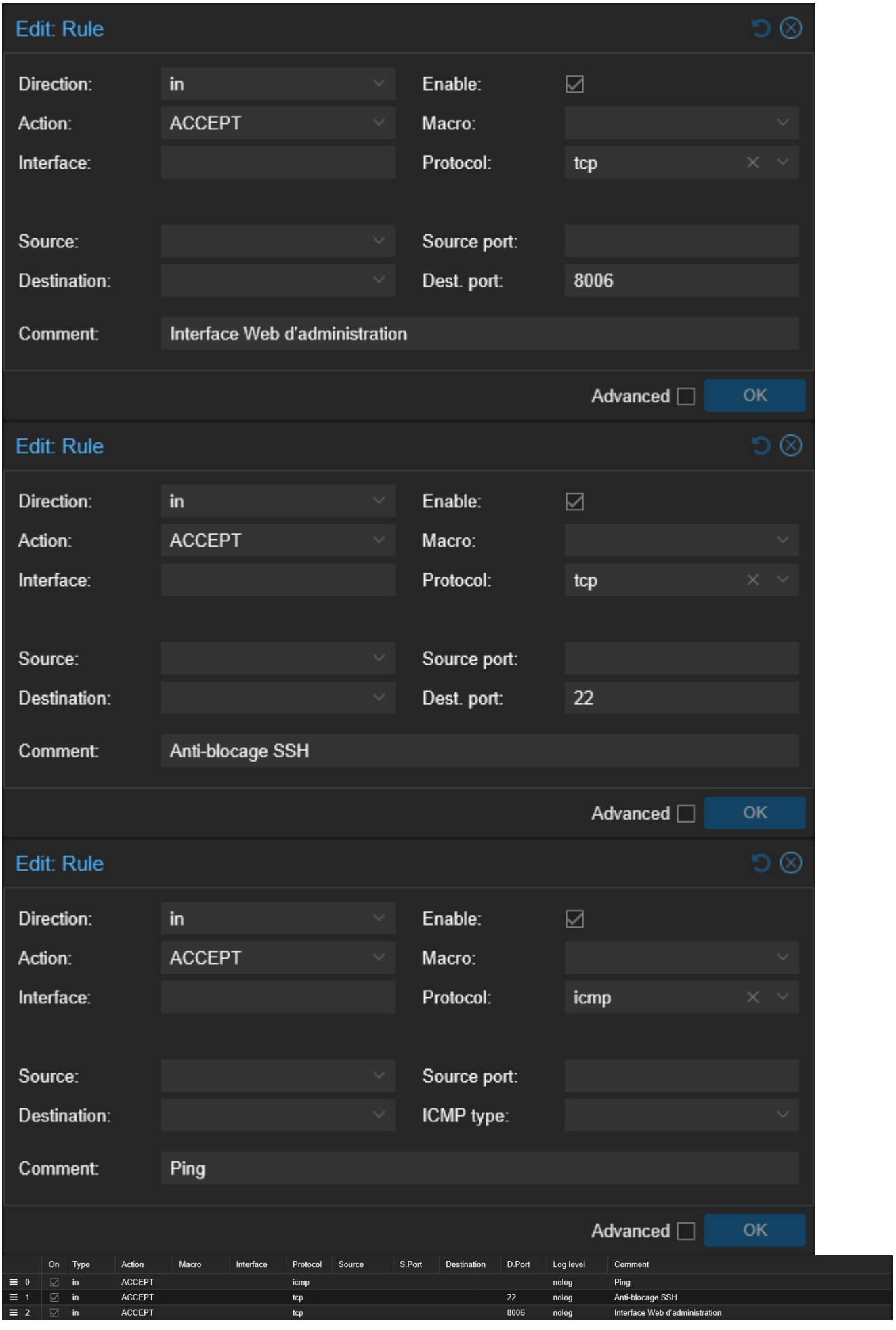
- Relancer le service SSH :

```
systemctl restart ssh
```

6.4.2.2. Configurer le pare-feu du Centre de données :

6.4.2.2.1. Créer les règles de pare-feu sur le Datacenter :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
    - Cliquer sur "**Centre de données**" (*Datacenter*) ;
    - Cliquez sur "**Pare-feu**" (*Firewall*) ;
    - Cliquez sur "**Ajouter**" (*Add*) ;
    - Ajoutez les règles de base suivantes :



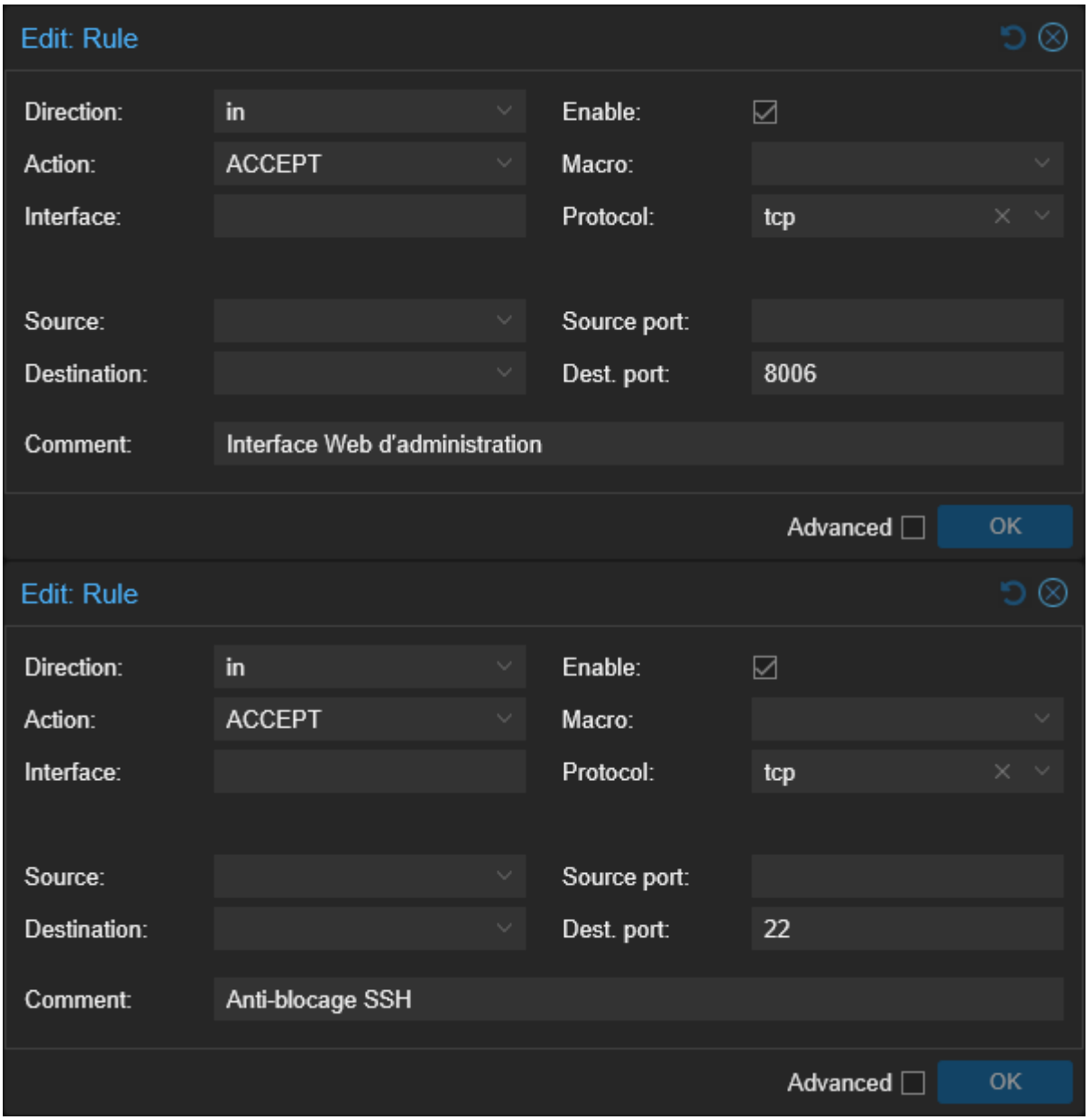
6.4.2.2.2. Activer le pare-feu du Datacenter :

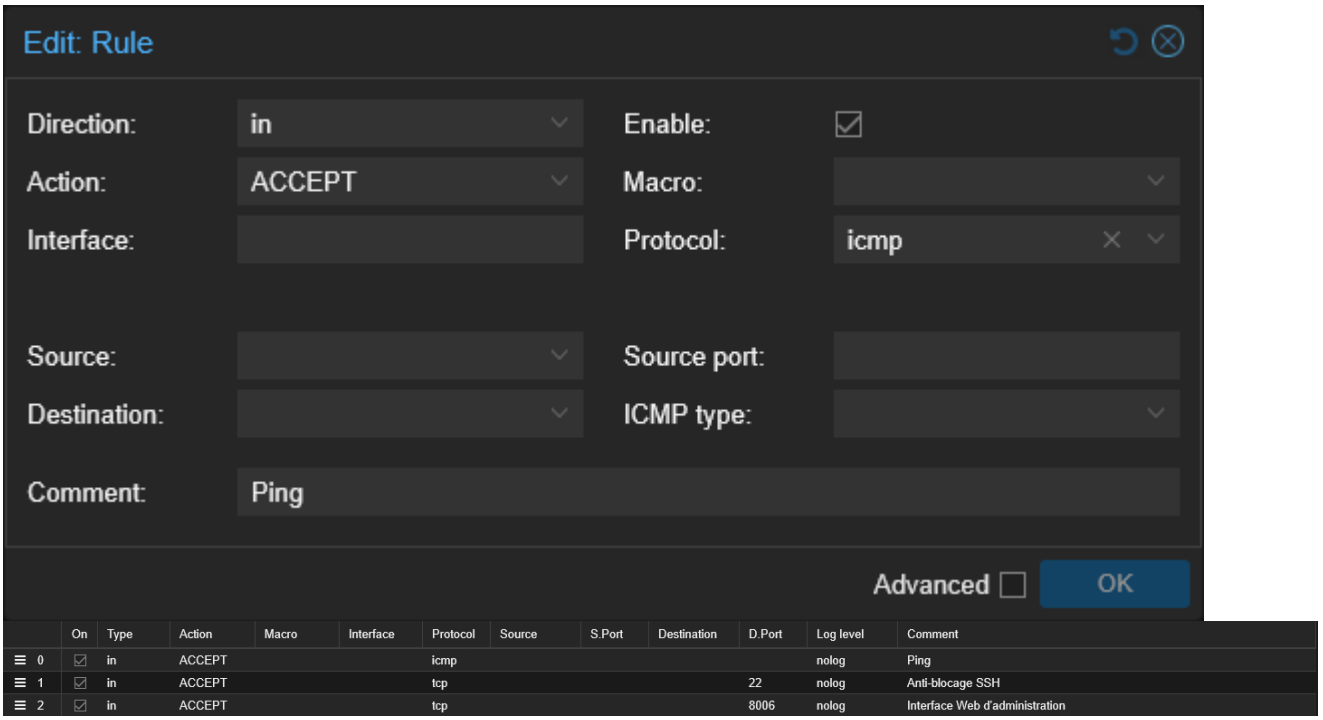
- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
  - Cliquer sur "**Centre de données**" (*Datacenter*) ;
  - Cliquez sur "**Pare-feu**" (*Firewall*) ;
  - Cliquez sur "**Options**" (*Options*) ;
  - Cliquez sur "**Éditer**" (*Edit*) ;
  - Cocher "**Pare-feu**" (*Firewall*).

6.4.2.3. Configurer le pare-feu des nœuds :

6.4.2.3.1. Créer les règles de pare-feu sur chaque nœud :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
  - Cliquez sur le nœud Proxmox ("**pve**") ;
  - Cliquez sur "**Pare-feu**" (*Firewall*) ;
  - Cliquez sur "**Ajouter**" (*Add*) ;
  - Ajoutez les règles de base suivantes :





6.4.2.3.2. Activer le pare-feu sur chaque nœud :

- Depuis l'interface "**root", en "Vue serveur**" (*Server View*) :
  - Cliquer sur "**Centre de données**" (*Datacenter*) ;
  - Cliquez sur "**Pare-feu**" (*Firewall*) ;
  - Cliquez sur "**Options**" (*Options*) ;
  - Cliquez sur "**Éditer**" (*Edit*) ;
  - Cocher "**Pare-feu**" (*Firewall*).