**Configuration du stockage NAS**

* **Préparation des disques :**
  + Si vous utilisez plusieurs disques, configurez-les en RAID (Redundant Array of Independent Disks) pour la redondance des données.
  + Utilisez des outils comme mdadm pour configurer le RAID.
* **Création du système de fichiers :**
  + Créez un système de fichiers (par exemple, ext4 ou XFS) sur le volume RAID.
  + Montez le système de fichiers dans un répertoire approprié (par exemple, /media/nas).

**Gestion des utilisateurs et des dossiers**

* **Création des utilisateurs :**
  + Utilisez la commande adduser pour créer les utilisateurs qui auront accès au NAS.
  + Attribuez un mot de passe fort à chaque utilisateur.
* **Création des dossiers utilisateurs :**
  + Créez un dossier dédié pour chaque utilisateur dans le répertoire /media/nas.
  + Attribuez les droits d'accès appropriés à chaque dossier en utilisant chown et chmod. Par exemple :
    - mkdir /media/nas/utilisateur1
    - chown utilisateur1:utilisateur1 /media/nas/utilisateur1
    - chmod 700 /media/nas/utilisateur1
* **Session administrateur:**
  + S'assurer que l'utilisateur « root » a un mot de passe fort.
  + Créer un utilisateur administrateur avec la commande « adduser administrateur ».
  + Ajouter cette utilisateur au groupe « sudo » avec la commande « usermod -aG sudo administrateur ».

**Configuration de Samba**

* **Installation de Samba :**
  + Installez le serveur Samba en utilisant la commande apt install samba.
* **Configuration de Samba :**
  + Modifiez le fichier de configuration de Samba (/etc/samba/smb.conf) pour partager les dossiers utilisateurs.
  + Voici un exemple de configuration pour un dossier utilisateur :

[utilisateur1]

path = /media/nas/utilisateur1

valid users = utilisateur1

read only = no

browseable = yes

* + Redémarrez le service Samba avec la commande systemctl restart smbd.

**Sécurité et gestion des accès**

* **Pare-feu :**
  + Configurez un pare-feu (par exemple, ufw) pour autoriser uniquement les connexions nécessaires (SSH, Samba).
* **Mises à jour :**
  + Maintenez votre système Debian à jour avec les dernières mises à jour de sécurité.
* **Surveillance :**
  + Surveillez les journaux du système et de Samba pour détecter les activités suspectes.

# Tutoriel : Mise en Place d'un Serveur NAS Debian avec Gestion Multisessions

## Prérequis

* Une machine sous Debian (physique ou virtuelle)
* Accès root ou privilèges sudo
* Un disque de stockage pour le NAS
* Connexion réseau stable

## 1. Installation du Serveur NAS

### Mise à jour du système

sudo apt update && sudo apt upgrade -y

### Installation de Samba (pour le partage de fichiers)

sudo apt install samba -y

## 2. Configuration de la Gestion Multisessions

### Création des Dossiers des Utilisateurs

Chaque utilisateur aura un dossier dédié dans /srv/nas/users/.

sudo mkdir -p /srv/nas/users/

### Création des Comptes Utilisateurs

Créez un utilisateur pour chaque session :

sudo adduser nom\_utilisateur

Ajoutez l'utilisateur à Samba :

sudo smbpasswd -a nom\_utilisateur

### Configuration des Permissions

sudo chown -R nom\_utilisateur:nom\_utilisateur /srv/nas/users/nom\_utilisateur

sudo chmod 700 /srv/nas/users/nom\_utilisateur

## 3. Configuration de Samba

Modifiez le fichier de configuration de Samba :

sudo nano /etc/samba/smb.conf

Ajoutez les lignes suivantes en fin de fichier :

[users]

path = /srv/nas/users

browseable = yes

read only = no

guest ok = no

create mask = 0700

directory mask = 0700

valid users = %S

Redémarrez Samba :

sudo systemctl restart smbd

## 4. Mise en Place de la Session Administrateur

Création de l'utilisateur administrateur :

sudo adduser admin\_nas

sudo smbpasswd -a admin\_nas

Ajout aux privilèges root :

sudo usermod -aG sudo admin\_nas

Création d’un dossier d’administration :

sudo mkdir -p /srv/nas/admin

sudo chown admin\_nas:admin\_nas /srv/nas/admin

sudo chmod 770 /srv/nas/admin

Ajoutez cette section dans smb.conf :

[admin]

path = /srv/nas/admin

browseable = yes

read only = no

guest ok = no

valid users = admin\_nas

Redémarrez Samba :

sudo systemctl restart smbd

## 5. Tests et Validation

### Vérifier la Connectivité

Depuis un autre ordinateur sur le réseau, tapez :

smbclient -L //IP\_DU\_SERVEUR -U admin\_nas

Testez l’accès aux dossiers avec un client Samba ou via Windows (\IP\_DU\_SERVEUR\users).

## 6. Documentation et Maintenance

### Création d’une Documentation

Rédigez un guide utilisateur en incluant :

* Installation
* Accès aux fichiers
* Gestion des sessions
* Modification des permissions

### Automatisation des Sauvegardes

Ajoutez une tâche cron pour sauvegarder régulièrement les fichiers :

crontab -e

Ajoutez cette ligne pour une sauvegarde quotidienne :

0 2 \* \* \* tar -czf /backup/nas\_backup\_$(date +\%F).tar.gz /srv/nas/

## Conclusion

Ce tutoriel permet d’installer un serveur NAS Debian avec gestion multisessions et une administration efficace. Une bonne documentation assurera une utilisation optimale et une maintenance simplifiée.

### 1. ****Installation de Debian sans interface graphique****

* Téléchargez et installez **Debian minimal** sur votre VM.
* Configurez les dépôts et mettez à jour le système :

sudo apt update && sudo apt upgrade -y

### 2. ****Configuration du stockage et RAID****

* Installez **mdadm** pour la gestion du RAID :

sudo apt install mdadm -y

* Configurez un **RAID 5, 6 ou 10** selon vos besoins.

### 3. ****Installation et configuration des services****

#### a) ****SFTP (Secure File Transfer Protocol)****

* Vérifiez que **OpenSSH** est installé et activé :

sudo apt install openssh-server -y

* Configurez **SFTP** pour sécuriser l’accès et interdire SSH :
  + Éditez /etc/ssh/sshd\_config et ajoutez :

Match Group sftpusers

ChrootDirectory /home/%u

ForceCommand internal-sftp

X11Forwarding no

AllowTcpForwarding no

* + Créez un groupe et ajoutez des utilisateurs :

sudo groupadd sftpusers

sudo usermod -aG sftpusers LaPlateforme

#### b) ****WebDAV (Accès sécurisé via HTTPs)****

* Installez Apache et modifiez la configuration :

sudo apt install apache2 apache2-utils -y

sudo a2enmod dav dav\_fs ssl

* Ajoutez un utilisateur WebDAV et configurez /var/www/webdav comme répertoire partagé.

#### c) ****Partage Public (Samba ou NFS)****

* Installez et configurez **Samba** pour un accès réseau simple :

sudo apt install samba -y

* Ajoutez une section pour un dossier public dans /etc/samba/smb.conf :

[Public]

path = /srv/public

browsable = yes

read only = no

guest ok = yes

* Redémarrez Samba :

sudo systemctl restart smbd

### 4. ****Sauvegarde avec Rsync & Second Serveur****

* Installez rsync et configurez des sauvegardes automatiques sur un second serveur avec :

rsync -avz /data remote\_user@backup\_server:/backup

### 5. ****Virtualisation avec KVM/QEMU****

* Installez et configurez un hyperviseur pour gérer des VMs supplémentaires :

sudo apt install qemu-kvm libvirt-daemon-system virt-manager -y