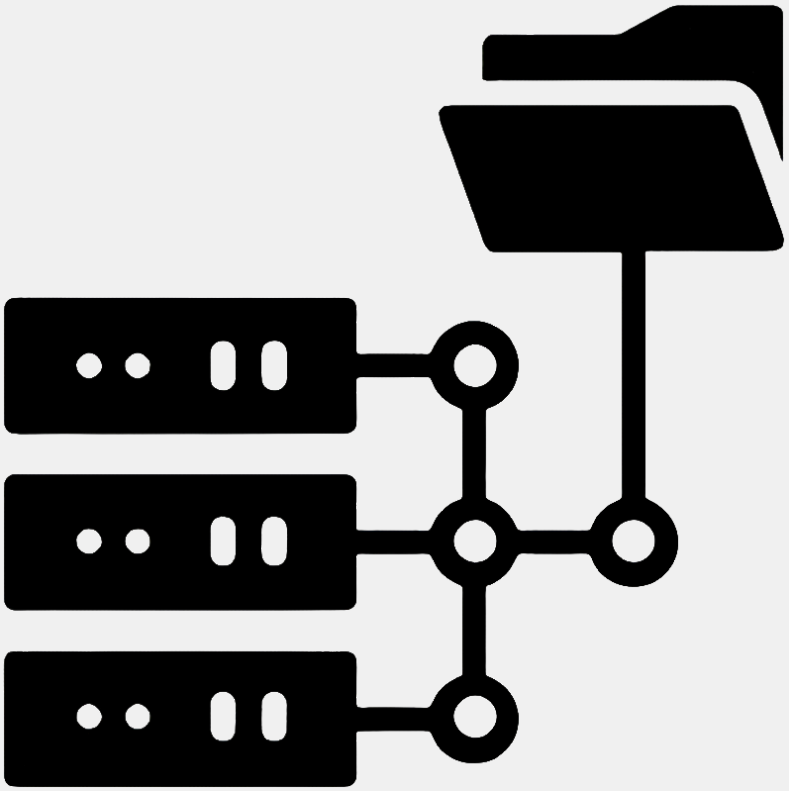
# DOCUMENTATION



ABELLA - ABDOUH - BACCAM

# SOMMAIRE

# NETWORK ATTACHED STORAGE (NAS)

## C’est quoi un NAS?

Un **NAS** (Network Attached Storage) est un **appareil de stockage connecté à un réseau**, qui permet de **stocker et de partager des fichiers** entre plusieurs utilisateurs. Il se compose d'**un ou plusieurs disques durs** installés dans un boîtier, connecté à un réseau local (LAN) ou à internet via un routeur. Le NAS est **équipé d'un système d'exploitation léger et d'une interface web** permettant de gérer les fichiers stockés, les droits d'accès, les sauvegardes, etc.

## Pourquoi utiliser un NAS?

L'utilisation d'un NAS offre **plusieurs avantages**, tels que le **partage de fichiers centralisé** et simplifié entre plusieurs utilisateurs, la **sauvegarde de données automatisée et sécurisée**, la **diffusion multimédia en continu** sur différents appareils, l'**accès à distance aux données stockées** depuis n'importe où dans le monde, la possibilité de **créer un cloud personnel**, la prise en charge de **plusieurs protocoles de transfert de fichiers**, la **flexibilité dans la gestion des droits** d'accès aux fichiers et la **possibilité d'étendre la capacité de stockage** en fonction des besoins. En somme, un NAS permet une **gestion centralisée, sécurisée et flexible des données**.

## Qui devrait utiliser un NAS?

Les personnes et les organisations qui ont besoin d'un **stockage centralisé, sécurisé et flexible pour leurs données** devraient envisager d'utiliser un NAS. Plus particulièrement, les utilisateurs suivants peuvent bénéficier de l'utilisation d'un NAS :

- Les **particuliers** qui souhaitent **stocker et partager des fichiers multimédias**, tels que des films, de la musique et des photos, **entre plusieurs appareils dans leur réseau domestique**.
- Les **petites et moyennes entreprises** qui ont besoin d'un **moyen simple et économique de stocker et de partager des fichiers importants** entre les employés, de sauvegarder les données de l'entreprise et de **fournir un accès à distance sécurisé aux données**.
- Les **professionnels de la création**, tels que les graphistes, les vidéastes et les photographes, qui ont besoin d'un **espace de stockage centralisé pour leurs fichiers volumineux et d'un moyen facile de collaborer avec les clients et les collègues**.
- Les **passionnés de technologie** qui cherchent à **construire leur propre cloud personnel** pour stocker et accéder à leurs données depuis n'importe où dans le monde.

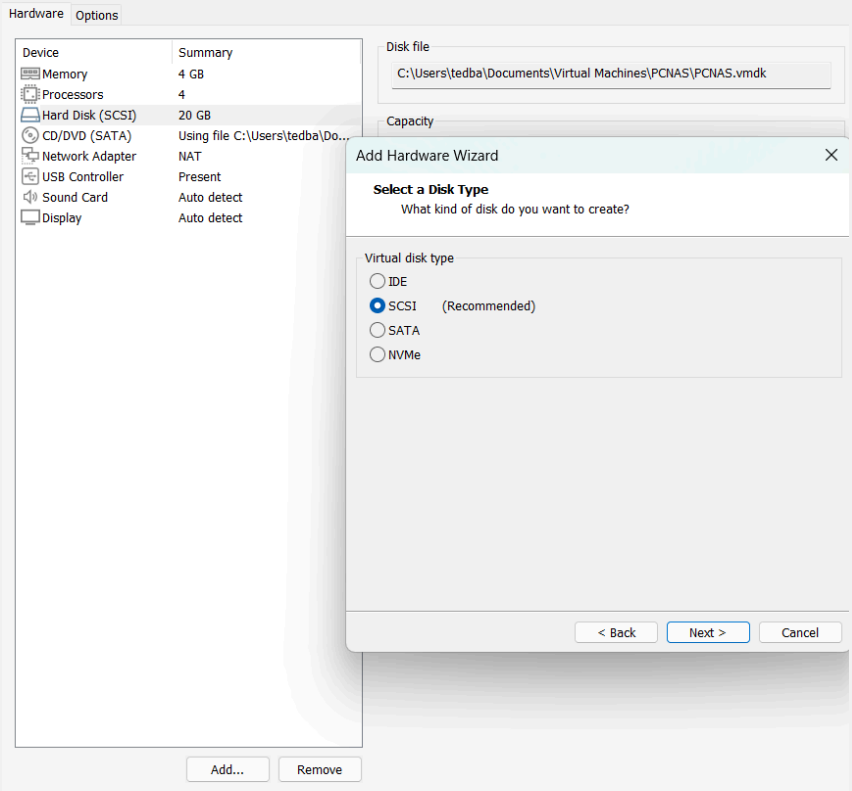
En fin de compte, tout utilisateur qui a **besoin d'un stockage de données fiable, sécurisé et évolutif** peut bénéficier de l'utilisation d'un NAS.

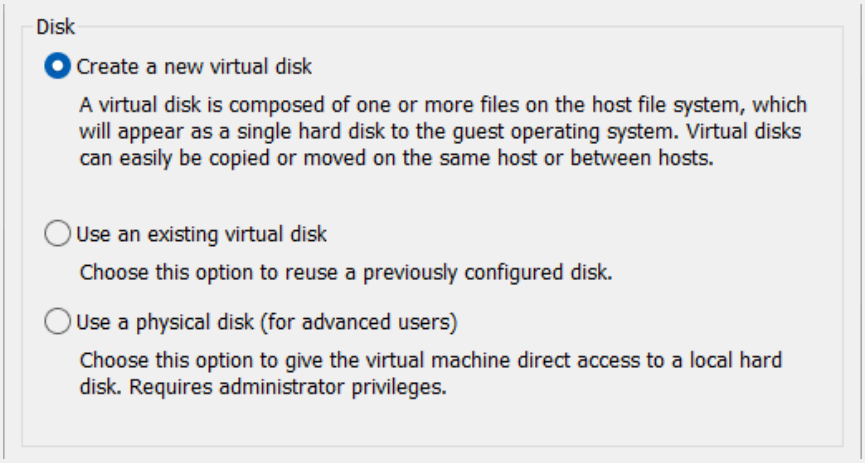
# MISE EN PLACE D'UN NAS

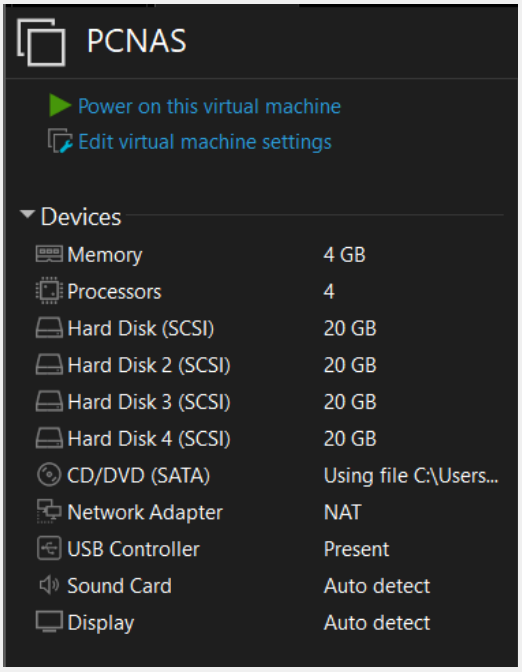
## Installation de la VM Debian

### Mise en place du RAID 5

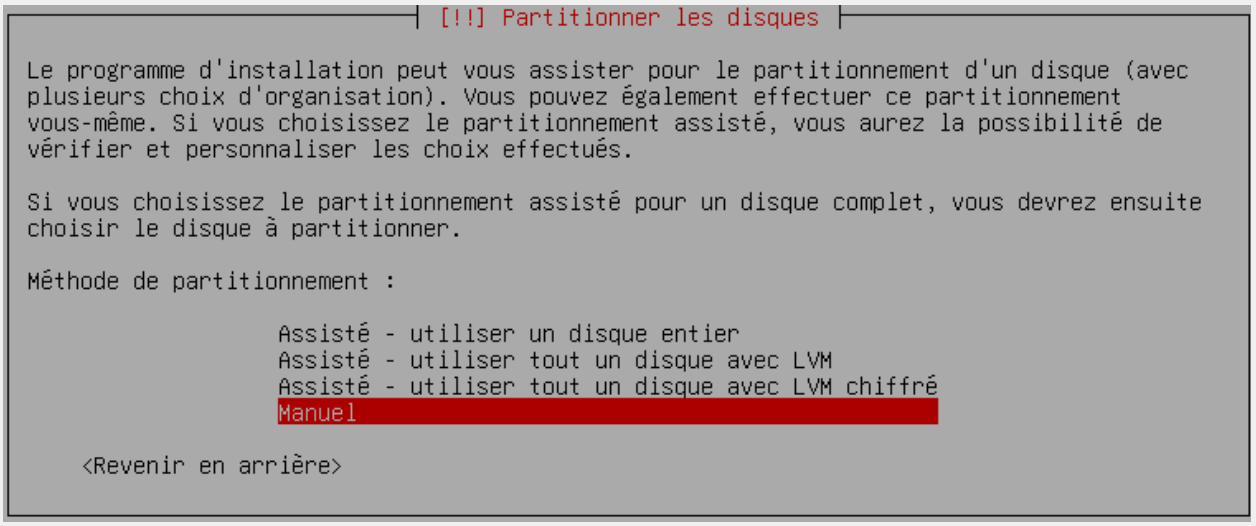
Pour configurer un RAID 5 avec VMware et Debian 12, commencez par **créer une nouvelle machine virtuelle** (VM) dans VMware en utilisant l'**image ISO d'installation de Debian 12**.





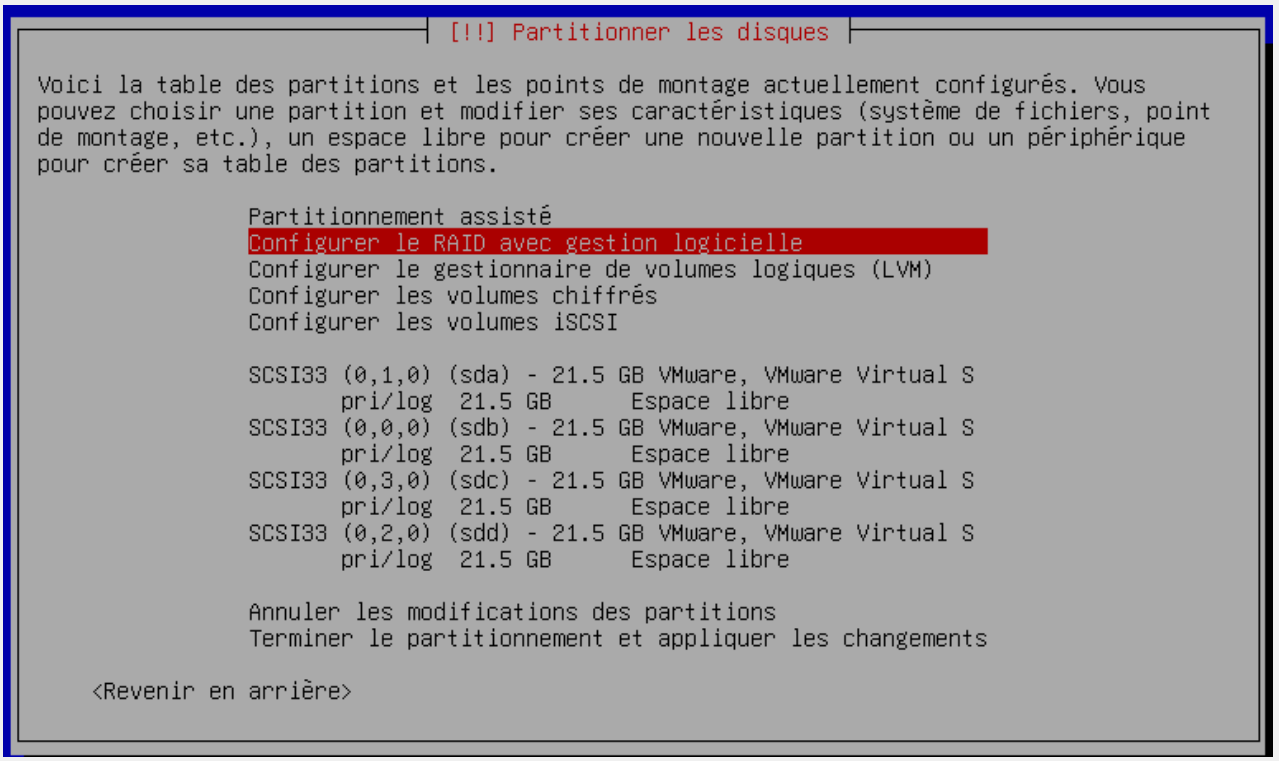



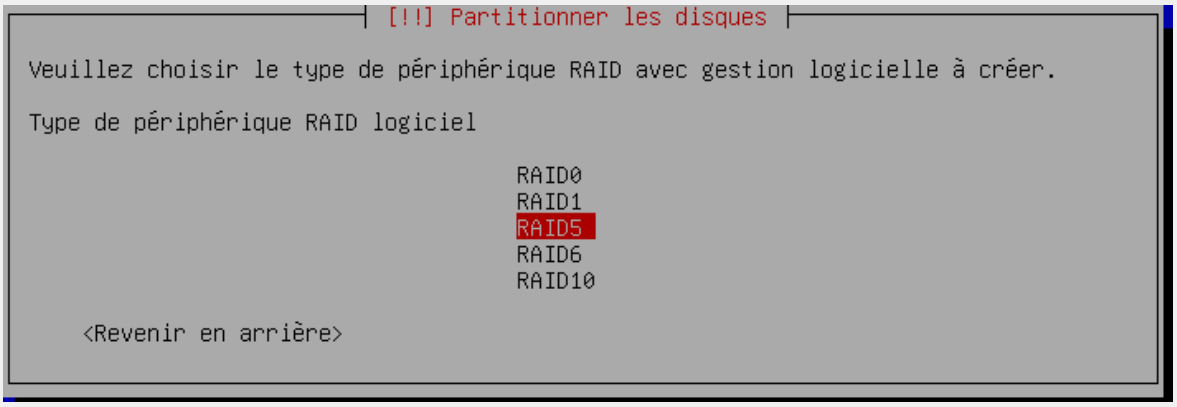

Une fois la VM en place, éditez-la pour y **ajouter trois disques durs supplémentaires**. Le **RAID 5** nécessite au moins trois disques pour fonctionner, car il **utilise la parité pour permettre la récupération des données en cas de défaillance d'un disque**. Le disque supplémentaire est utilisé comme **disque de secours**.



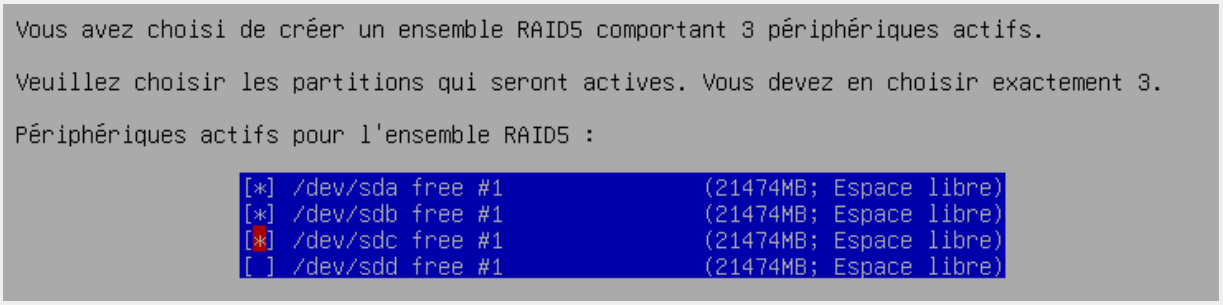

Procédez à l'installation de **Debian en mode non graphique**. Lorsque vous atteignez l'étape de partitionnement, sélectionnez "**Partitionnement manuel**".

À partir de là, vous devrez **créer une table de partitions pour chaque disque dur**. Puis, aller sur "**Configurer le RAID avec gestion logicielle**"

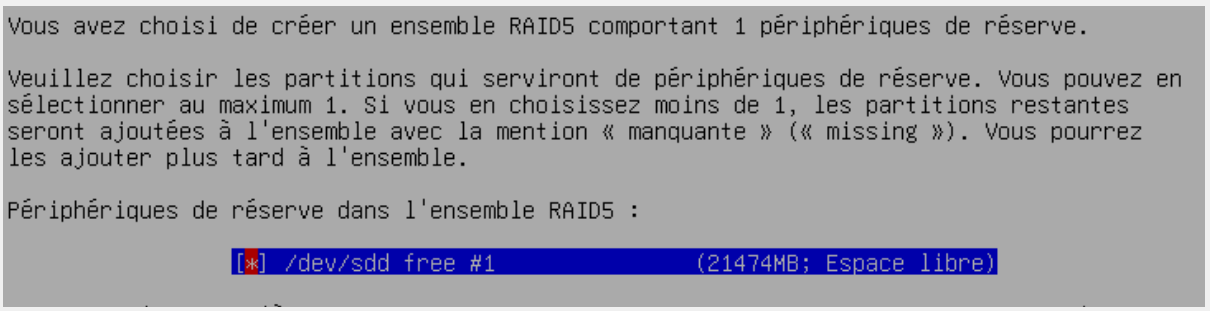




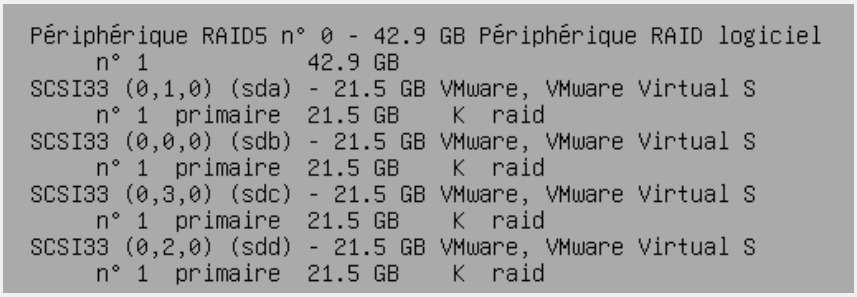

**Créez un nouveau volume RAID 5** en utilisant les partitions que vous venez de créer.




Lorsque vous êtes invité à sélectionner un périphérique de secours, **sélectionnez le quatrième disque dur que vous avez ajouté à la VM**.




Et voilà, notre RAID 5 est enfin mis en place. Il ne faut pas oublier de **procéder au partitionnement assisté sur le périphérique RAID 5** pour pouvoir continuer l'installation correctement



# Configuration du NAS

## SSH/SFTP

**Mettez à jour le système Debian** en utilisant les commandes suivantes :

```
sudo apt update
sudo apt upgrade
```

**Installez le serveur SSH (OpenSSH)** avec la commande suivante :

```
sudo apt install openssh-server
```

**Créez deux utilisateurs, 'nasuser1' et 'nasuser2'**, en utilisant la commande **'adduser'**. Vous serez invité à définir un mot de passe pour chacun :

```
sudo adduser nasuser1
sudo adduser nasuser2
```

**Créez les répertoires de base pour chaque utilisateur** et attribuez-leur les **permissions appropriées** :

```
sudo mkdir /home/nasuser1/nasdata
sudo mkdir /home/nasuser2/nasdata
sudo chown nasuser1:nasuser1 /home/nasuser1/nasdata
sudo chown nasuser2:nasuser2 /home/nasuser2/nasdata
```

**Créez un dossier public partagé**, accessible par les deux utilisateurs :

```
sudo mkdir /naspublicdata
sudo chown nasuser1:nasuser2 /naspublicdata
sudo chmod 770 /naspublicdata
```

**Modifiez le fichier de configuration SSH** pour restreindre les utilisateurs au répertoire SFTP et empêcher l'accès shell :

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

Ajoutez les lignes suivantes à la fin du fichier :

```
Match Group sftponly
    ChrootDirectory /home/%u
    ForceCommand internal-sftp
    AllowTCPForwarding no
    X11Forwarding no
```

**Créez un nouveau groupe 'sftponly'** et ajoutez les utilisateurs 'nasuser1' et 'nasuser2' à ce groupe :

```
sudo groupadd sftponly
sudo usermod -aG sftponly nasuser1
sudo usermod -aG sftponly nasuser2
```

**Ajustez les propriétés et les permissions** des répertoires home pour les utilisateurs 'nasuser1' et 'nasuser2' :

```
sudo chown root:root /home/nasuser1
sudo chown root:root /home/nasuser2
sudo chmod 755 /home/nasuser1
sudo chmod 755 /home/nasuser2
```

**Appliquez les modifications** en redémarrant le service SSH :

```
sudo systemctl restart ssh
```

**Créez des points de montage pour le dossier public partagé** à l'intérieur du répertoire de base de chaque utilisateur :

```
sudo mkdir /home/nasuser1/nasdata/public_mnt
sudo mkdir /home/nasuser2/nasdata/public_mnt
```

**Montez le dossier public partagé** sur les points de montage respectifs :

```
sudo mount --bind /naspublicdata /home/nasuser1/nasdata/public_mnt
sudo mount --bind /naspublicdata /home/nasuser2/nasdata/public_mnt
```

**Éditez le fichier '/etc/fstab'** pour que les montages soient **conservés après un redémarrage** :

```
sudo nano /etc/fstab
```

Ajoutez les lignes suivantes à la fin du fichier :

```
/naspublicdata /home/nasuser1/nasdata/public_mnt none bind 0 0
/naspublicdata /home/nasuser2/nasdata/public_mnt none bind 0 0
```

Les utilisateurs 'nasuser1' et 'nasuser2' peuvent désormais **se connecter au serveur via SFTP et accéder à leurs répertoires de base respectifs** ainsi qu'au dossier public partagé.

## SAMBA

Cette configuration permettra aux clients Windows, macOS et Linux de **se connecter et d'accéder aux fichiers partagés à l'aide du protocole SMB/CIFS**, en utilisant les mêmes utilisateurs et les mêmes dossiers que ceux utilisés pour le SFTP.

Commencez par **installer Samba et ses dépendances** :

```
sudo apt update
sudo apt install samba samba-common-bin
```

**Créez un fichier de configuration Samba** personnalisé :

```
sudo nano /etc/samba/smb.conf.custom
```

Ajoutez les lignes suivantes à ce fichier :

```
[global]
   workgroup = WORKGROUP
   server string = %h server
   log file = /var/log/samba/log.%m
   max log size = 1000
   syslog = 0
   panic action = /usr/share/samba/panic-action %d
   encrypt passwords = true
   passdb backend = tdbsam
   obey pam restrictions = yes
   unix password sync = yes
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully*
   pam password change = yes
   map to guest = bad user
   usershare allow guests = no

[nasuser1]
   path = /home/nasuser1/nasdata
   read only = no
   browseable = yes
   valid users = nasuser1

[nasuser2]
   path = /home/nasuser2/nasdata
   read only = no
   browseable = yes
   valid users = nasuser2

[public]
   path = /naspublicdata
   read only = no
   browseable = yes
   valid users = nasuser1, nasuser2
```

**Enregistrez et fermez le fichier** en appuyant sur `Ctrl + X`, puis `Y` et `Enter`.

**Remplacez le fichier de configuration Samba par défaut** par le fichier personnalisé :

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.backup
sudo mv /etc/samba/smb.conf.custom /etc/samba/smb.conf
```

**Ajoutez les utilisateurs Samba** :

```
sudo smbpasswd -a nasuser1
sudo smbpasswd -a nasuser2
```

Pendant la création des utilisateurs Samba, vous serez invité à **définir un mot de passe pour chacun**.

**Redémarrez le service Samba** :

```
sudo systemctl restart smbd
```

Désormais, vos clients Windows, macOS et Linux devraient **pouvoir se connecter à votre serveur NAS à l'aide du protocole SMB/CIFS** et **accéder aux dossiers partagés 'nasuser1', 'nasuser2' et 'public'** en utilisant les mêmes informations d'identification que celles utilisées pour le SFTP.

## WebDAV

Pour **mettre en place l'accès WebDAV** sur notre serveur NAS Debian sans SSL, nous allons **utiliser le serveur web Apache**. Toutefois, il est important de noter que **l'utilisation de WebDAV sans SSL n'est pas recommandée**, car les **données seront transmises en texte brut et pourront être interceptées**.

Suivez les étapes ci-dessous pour configurer l'accès WebDAV pour les utilisateurs 'nasuser1' et 'nasuser2' :

Commencez par **installer Apache et les modules WebDAV** requis :

```
sudo apt update
sudo apt install apache2
```

**Activez les modules Apache** nécessaires :

```
sudo a2enmod dav
sudo a2enmod dav_fs
```

**Créez un fichier de configuration Apache** personnalisé :

```
sudo nano /etc/apache2/conf-available/webdav.conf
```

Ajoutez les lignes suivantes à ce fichier :

```
Alias /nasuser1 /home/nasuser1/nasdata
Alias /nasuser2 /home/nasuser2/nasdata
Alias /public /naspublicdata

<Directory /home/nasuser1/nasdata>
    DAV On
    AuthType Basic
    AuthName "nasuser1 WebDAV"
    AuthUserFile /etc/apache2/webdav-passwd/nasuser1.passwd
    Require valid-user
</Directory>

<Directory /home/nasuser2/nasdata>
    DAV On
    AuthType Basic
    AuthName "nasuser2 WebDAV"
    AuthUserFile /etc/apache2/webdav-passwd/nasuser2.passwd
    Require valid-user
</Directory>

<Directory /naspublicdata>
    DAV On
    AuthType Basic
    AuthName "Public WebDAV"
    AuthUserFile /etc/apache2/webdav-passwd/public.passwd
    Require user nasuser1 nasuser2
</Directory>
```

**Enregistrez et fermez le fichier** en appuyant sur `Ctrl + X`, puis `Y` et `Enter`.

**Créez le répertoire pour les fichiers de mot de passe WebDAV** :

```
sudo mkdir /etc/apache2/webdav-passwd
```

**Créez les fichiers de mot de passe WebDAV** pour les utilisateurs **'nasuser1' et 'nasuser2'**, ainsi que pour le **dossier public** :

```
sudo htpasswd -c /etc/apache2/webdav-passwd/nasuser1.passwd nasuser1
sudo htpasswd -c /etc/apache2/webdav-passwd/nasuser2.passwd nasuser2
sudo htpasswd -c /etc/apache2/webdav-passwd/public.passwd nasuser1
sudo htpasswd /etc/apache2/webdav-passwd/public.passwd nasuser2
```

Pendant la création des fichiers de mot de passe, vous serez invité à **définir un mot de passe pour chaque utilisateur**.

**Activez la configuration Apache** personnalisée :

```
sudo a2enconf webdav
```

**Redémarrez le service Apache** :

```
sudo systemctl restart apache2
```

Désormais, vous devriez **pouvoir accéder à vos dossiers 'nasuser1', 'nasuser2' et 'public' via WebDAV** en utilisant l'adresse respectivement :

```
http://192.168.204.141/nasuser1
http://192.168.204.141/nasuser2
http://192.168.204.141/public
```

## Rsync

Pour **configurer la sauvegarde de votre serveur NAS sur un deuxième serveur à l'aide de rsync** et planifier la sauvegarde à l'aide de cron, commencez par **créer un autre serveur RAID 5 pour le backup**.

Suivez les étapes ci-dessous pour mettre en place la sauvegarde :

Installez rsync sur les deux serveurs :

Sur le serveur NAS (la source) :

```
sudo apt update
sudo apt install rsync
```

Sur le deuxième serveur (la destination) :

```
sudo apt update
sudo apt install rsync
```

Créez un utilisateur "backupnas" sur le deuxième serveur :

Lors de l'installation de la machine virtuelle de sauvegarde, **créez l'utilisateur "backupnas"**. Sinon, utilisez la commande suivante pour créer l'utilisateur "backupnas" sur le deuxième serveur :

```
sudo adduser backupnas
```

Pendant la création de l'utilisateur, vous serez invité à **définir un mot de passe** pour celui-ci.

Créez un répertoire de sauvegarde sur le deuxième serveur :

**Créez un répertoire de sauvegarde pour l'utilisateur "backupnas"** sur le deuxième serveur en utilisant les commandes suivantes :

```
sudo mkdir /home/backupnas/nasbackup
sudo chown backupnas:backupnas /home/backupnas/nasbackup
```

**Créez un script de sauvegarde** sur le serveur NAS :

**Créez un script de sauvegarde "nasbackup.sh" sur le serveur NAS** en utilisant l'éditeur de texte nano :

```
nano /home/laplateforme/nasbackup.sh
```

Ajoutez les lignes suivantes au script :

```
#!/bin/bash

SOURCE="/home/nasuser1/nasdata/ /home/nasuser2/nasdata/ /naspublicdata/"
DESTINATION="backupnas@<IP_ADDRESS_OF_SECOND_SERVER>:/home/backupnas/nasbackup"

rsync -avz --progress --delete --exclude=/nasdata/public_mnt/ $SOURCE $DESTINATION
```

Assurez-vous de **remplacer "<IP_ADDRESS_OF_SECOND_SERVER>" par l'adresse IP réelle du deuxième serveur**.

**Enregistrez et fermez le fichier**.

Rendez le script de sauvegarde exécutable :

**Utilisez la commande chmod pour rendre le script de sauvegarde exécutable** :

```
chmod +x /home/laplateforme/nasbackup.sh
```

Testez la sauvegarde :

**Exécutez le script de sauvegarde "nasbackup.sh" sur le serveur NAS** pour **tester la sauvegarde sur le deuxième serveur** :

```
sudo /home/laplateforme/nasbackup.sh
```

Vous devriez voir rsync synchroniser les fichiers et les répertoires entre le serveur NAS et le deuxième serveur.

Planifiez la sauvegarde à l'aide de cron :

Ouvrez le fichier de **configuration de cron** pour l'utilisateur "laplateforme" :

```
crontab -e
```

Ajoutez une nouvelle ligne au fichier de configuration de cron pour planifier la sauvegarde :

```
0 2 * * * /home/laplateforme/nasbackup.sh
```

Cette ligne **planifiera la sauvegarde pour qu'elle s'exécute tous les jours à 2h du matin**. Vous pouvez modifier l'heure et la fréquence en fonction de vos besoins.

**Enregistrez et fermez le fichier de configuration de cron**.

**La sauvegarde sera maintenant planifiée et exécutée automatiquement** en fonction de la configuration que vous avez définie. Vous pouvez vérifier les journaux de sauvegarde sur le deuxième serveur pour vous assurer que la sauvegarde s'est déroulée correctement.

## Webmin

Mise à jour du système

Commencez par **mettre à jour le cache des paquets de votre système** vers la dernière version en utilisant la commande suivante :

```
sudo apt update -y
```

Après avoir mis à jour le cache des paquets, **installez les autres dépendances requises** en utilisant la commande suivante :

```
sudo apt install gnupg2 curl -y
```

Une fois que toutes les dépendances requises sont installées, vous pouvez passer à l'étape suivante.

### Installation de Webmin

Le paquet Webmin n'est pas inclus dans le référentiel Debian 12 par défaut. Vous devrez donc **ajouter le référentiel Webmin à APT**.

Tout d'abord, **téléchargez et ajoutez la clé GPG** et **ajoutez le référentiel Webmin** avec les commandes suivantes :

```
cd /tmp
curl -o setup-repos.sh
https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh
```

Une fois le référentiel ajouté, **mettez à jour le référentiel et installez Webmin** avec la commande suivante :

```
sudo apt update -y
sudo apt install webmin --install-recommends -y
```

Une fois que Webmin est installé, vous pouvez passer à l'étape suivante.

### Configuration de systemd pour Webmin

Pour **configurer systemd pour gérer Webmin**, utilisez les commandes suivantes :

```
sudo systemctl enable webmin
sudo systemctl start webmin
sudo systemctl status webmin
```

La **commande "enable" active Webmin pour qu'il démarre automatiquement** au démarrage du système. La **commande "start" démarre manuellement le service Webmin**. La **commande "status" affichera l'état actuel du service Webmin**.

### Connexion à Webmin

Pour vous **connecter à Webmin, ouvrez votre navigateur web et entrez l'adresse IP de votre serveur suivie du port 10000**. Par exemple, si l'adresse IP de votre serveur est 192.168.1.100, vous entrerez "192.168.1.100:10000" dans la barre d'adresse de votre navigateur.

Lorsque vous vous connecterez pour la première fois, vous serez invité à **vous authentifier en utilisant les informations d'identification de l'utilisateur root**. Entrez le nom d'utilisateur "root" et le mot de passe que vous avez défini pour l'utilisateur root lors de l'installation de votre système d'exploitation.

Une fois que vous êtes connecté à Webmin, vous pouvez **utiliser l'interface graphique pour gérer votre serveur**.

# Client pour accéder au NAS

## Cyberduck

**Cyberduck est un client de transfert de fichiers populaire et gratuit qui offre une interface utilisateur graphique conviviale pour gérer les fichiers sur des serveurs distants**. Il prend en charge plusieurs protocoles de transfert de fichiers, notamment **SFTP, SAMBA et WebDAV**.

Avec Cyberduck, vous pouvez vous **connecter à votre serveur SFTP en utilisant vos informations d'identification et naviguer dans le système de fichiers de votre serveur**. Vous pouvez également **télécharger des fichiers de votre ordinateur local vers le serveur SFTP** et **téléverser des fichiers du serveur vers votre ordinateur local**.

En ce qui concerne SAMBA, **Cyberduck vous permet de vous connecter à des partages réseau SAMBA et de gérer les fichiers sur ces partages**. Vous pouvez **parcourir les fichiers et les dossiers partagés, télécharger des fichiers de votre ordinateur local vers le partage SAMBA** et **téléverser des fichiers du partage vers votre ordinateur local.**

Pour ce qui est de WebDAV, **Cyberduck vous offre la possibilité de vous connecter à des serveurs WebDAV et de gérer les fichiers stockés sur ces serveurs**. Vous pouvez **naviguer dans le système de fichiers du serveur WebDAV, télécharger des fichiers de votre ordinateur local vers le serveur et téléverser des fichiers du serveur vers votre ordinateur local**.

En somme, **Cyberduck est un outil pratique et polyvalent pour gérer les fichiers sur des serveurs distants en utilisant différents protocoles de transfert de fichiers**, tels que SFTP, SAMBA et WebDAV.

## Filezilla

De l'autre côté, nous avons **FileZilla, qui est également un client de transfert de fichiers populaire et gratuit, offrant une interface utilisateur graphique conviviale pour gérer les fichiers sur des serveurs distants**. Tout comme Cyberduck, FileZilla **prend en charge plusieurs protocoles de transfert de fichiers, notamment SFTP, FTP et FTPS**.

Avec FileZilla, vous pouvez vous **connecter à votre serveur SFTP en utilisant vos informations d'identification et naviguer dans le système de fichiers de votre serveur**. Vous pouvez également **télécharger des fichiers de votre ordinateur local vers le serveur SFTP** et **téléverser des fichiers du serveur vers votre ordinateur local**. FileZilla vous permet également de **reprendre les transferts de fichiers interrompus et de définir des limites de vitesse pour les transferts de fichiers**.

En ce qui concerne FTP et FTPS, FileZilla vous **offre la possibilité de vous connecter à des serveurs FTP et FTPS et de gérer les fichiers stockés sur ces serveurs**. Vous pouvez **naviguer dans le système de fichiers du serveur**, **télécharger des fichiers de votre ordinateur local vers le serveur et téléverser des fichiers du serveur vers votre ordinateur local**. FileZilla prend également en charge la **compression de fichiers et le transfert de fichiers volumineux**.

En somme, FileZilla est un autre **outil pratique et polyvalent pour gérer les fichiers sur des serveurs distants en utilisant différents protocoles de transfert de fichiers**, tels que SFTP, FTP et FTPS. Son **interface utilisateur graphique intuitive** et ses **fonctionnalités avancées** en font un choix populaire parmi les utilisateurs.

# Conclusion

Pour conclure, nous allons résumer les étapes et les choix technologiques que nous avons mis en œuvre pour créer un **serveur NAS (Network-Attached Storage) robuste, sécurisé et polyvalent**.

Dans un premier temps, nous avons opté pour l'**utilisation de SFTP (SSH File Transfer Protocol) pour assurer le transfert de fichiers sécurisé entre le serveur NAS et les clients. SFTP** offre un chiffrement des données pendant leur transfert, **garantissant ainsi la confidentialité et l'intégrité des informations**.

Ensuite, nous avons intégré **SAMBA (Server Message Block) pour faciliter le partage de fichiers entre les différents systèmes d'exploitation**, tels que Windows, macOS et Linux. SAMBA **simplifie la collaboration et l'échange de fichiers au sein d'un réseau local**.

Pour permettre l'**accès aux fichiers du serveur NAS via Internet**, nous avons mis en place WebDAV (Web-based Distributed Authoring and Versioning). **WebDAV est un protocole qui permet aux utilisateurs de modifier et de gérer des fichiers sur un serveur web à distance**, en utilisant un navigateur web ou un client WebDAV dédié.

En ce qui concerne la sauvegarde des données, nous avons choisi d'**utiliser rsync (Remote Sync) pour synchroniser et sauvegarder les fichiers du serveur NAS sur un autre serveur de sauvegarde**. Rsync est un **outil de synchronisation de fichiers efficace et flexible** qui minimise la quantité de données transférées en ne copiant que les modifications apportées aux fichiers.

Enfin, pour faciliter **la gestion et la configuration du serveur NAS**, nous avons installé **Webmin, une interface d'administration web basée sur un navigateur**. Webmin **simplifie la gestion du système en fournissant une interface utilisateur graphique intuitive** pour effectuer des tâches d'administration courantes, telles que la **gestion des utilisateurs, la configuration des services et la surveillance du système**.

En combinant les technologies **SFTP, SAMBA, WebDAV, rsync et Webmin**, nous avons créé un **serveur NAS sécurisé, polyvalent et facile à gérer**, répondant ainsi aux besoins variés des utilisateurs.