Création d'un serveur NAS sur Debian avec RAID 5

Introduction

La création d'un serveur NAS (Network Attached Storage) sur Debian avec un système RAID 5 offre une solution robuste et sécurisée pour le stockage et le partage de données au sein d'un réseau local. En combinant les fonctionnalités de stockage redondant offertes par le RAID 5 et les capacités de partage de fichiers fournies par des outils comme Samba, ainsi que la facilité d'accès offerte par SFTP et la réplication de données avec rsync, nous créons un environnement de stockage centralisé fiable et flexible.

Pour commencer, nous allons configurer un système RAID 5 avec trois disques, assurant ainsi la redondance des données et une meilleure tolérance aux pannes. En utilisant l'outil mdadm, nous allons créer, formater et monter le RAID, garantissant ainsi un accès sécurisé aux données.

Ensuite, nous installerons et configurerons Samba, ce qui nous permettra de partager facilement des fichiers avec d'autres systèmes d'exploitation sur le réseau. En définissant les autorisations appropriées et en configurant les paramètres de partage dans le fichier smb.conf, nous assurerons un accès contrôlé aux fichiers partagés.

Par la suite, nous mettrons en place un serveur SFTP (SSH File Transfer Protocol), permettant un transfert sécurisé de fichiers entre notre serveur et d'autres appareils via une connexion chiffrée SSH. En utilisant des clés SSH, nous éliminerons la nécessité de saisir un mot de passe lors de l'accès au serveur, garantissant ainsi une authentification sans tracas.

Enfin, nous explorerons la réplication de données avec rsync, une méthode efficace pour maintenir des copies synchronisées de nos données sur un emplacement distant. En automatisant ce processus à l'aide de tâches planifiées, nous assurerons une sauvegarde régulière et fiable de nos données.

À travers ces étapes, nous créerons un serveur NAS robuste et polyvalent sur Debian, répondant aux besoins de stockage et de partage de données au sein de notre réseau local.

1-Pour créer un RAID 5 avec nos trois disques (/home/alaa/sdb, /home/alaa/sdc, /home/alaa/sdd), nous pouvons suivre ces étapes :

1. **Installation de mdadm** : Assurons-nous d'avoir le logiciel mdadm installé sur notre système. Si ce n'est pas déjà le cas, nous pouvons l'installer en utilisant la commande suivante :

sudo apt-get update sudo apt-get install mdadm

2. **Création du RAID** : Utilisons la commande mdadm pour créer le RAID 5 en spécifiant les trois disques que nous souhaitons inclure. Assurons-nous de remplacer /dev/sdb, /dev/sdc et /dev/sdd par les chemins corrects vers nos disques :

sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /home/alaa/sdb /home/alaa/sdc /home/alaa/sdd

Cette commande crée un nouveau périphérique RAID appelé /dev/md0 avec un niveau RAID 5 utilisant les trois disques spécifiés.

3. **Vérification du statut du RAID** : Nous pouvons vérifier le statut du RAID en utilisant la commande suivante pour voir s'il est en cours de construction :

cat /proc/mdstat

4. **Formatage du RAID** : Une fois le RAID créé avec succès, nous devons formater le nouveau périphérique RAID avec le système de fichiers de notre choix. Par exemple, pour formater avec le système de fichiers ext4, utilisons la commande suivante :

sudo mkfs.ext4 /dev/md0

5. **Montage du RAID** : Enfin, montons le nouveau périphérique RAID dans le système de fichiers à un emplacement de notre choix. Par exemple, pour le monter dans /mnt/raid, utilisons la commande suivante :

sudo mkdir /home/alaa/raid5 sudo mount /dev/md0 /home/alaa/raid5

Assurons-nous de configurer le montage automatique du RAID au démarrage en ajoutant une entrée appropriée dans le fichier /etc/fstab.

sudo mdadm --detail --scan >> /etc/mdadm/mdadm.conf

Une fois ces étapes terminées, notre RAID 5 devrait être opérationnel et nous pourrons commencer à utiliser l'espace de stockage sécurisé et redondant qu'il offre.

Voici les étapes pour créer un RAID 5 avec nos trois disques sous forme de tableau :

Étape	Description	Commandes
1. Installation de mdadm	Assurons-nous d'avoir le logiciel mdadm installé sur notre système. Si ce	sudo apt-get update sudo apt-get install mdadm

	n'est pas déjà le cas, nous pouvons l'installer.	
2. Création du RAID	Utilisons la commande mdadm pour créer le RAID 5 en spécifiant les trois disques que nous souhaitons inclure.	sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /home/alaa/sdb /home/alaa/sdc /home/alaa/sdd
3. Vérification du statut du RAID	Nous pouvons vérifier le statut du RAID pour voir s'il est en cours de construction.	cat /proc/mdstat
4. Formatage du RAID	Une fois le RAID créé avec succès, nous devons formater le nouveau périphérique RAID avec le système de fichiers de notre choix.	sudo mkfs.ext4 /dev/md0
5. Montage du RAID	Montons le nouveau périphérique RAID dans le système de fichiers à un emplacement de notre choix.	sudo mkdir /home/alaa/raid5 sudo mount /dev/md0 /home/alaa/raid5 Configurer le montage automatique dans /etc/fstab si nécessaire **sudo mdadm --detail --scan >> /etc/mdadm/mdadm.conf**

2-Installer et configurer Samba

Pour installer et configurer Samba sur notre système, nous pouvons suivre les étapes suivantes :

1. Installation de Samba

Nous devons installer Samba avec la commande suivante :

sudo apt-get install samba

Cette commande installe le logiciel Samba, qui permet de partager des fichiers et des imprimantes entre différents systèmes d'exploitation.

2. Configuration de Samba

Une fois Samba installé, nous devons configurer le partage. Pour ce faire, nous allons éditer le fichier de configuration de Samba **smb.conf**. Ce fichier se trouve généralement dans **/etc/samba/**.

Ouvrons le fichier de configuration avec un éditeur de texte :

sudo nano /etc/samba/smb.conf

Ajoutons la configuration de base suivante pour partager un répertoire :

[Nas_raid5]

path = /chemin/vers/votre/raid

public = no

writable = yes

3. Redémarrer le service Samba

Après avoir modifié le fichier de configuration, nous devons redémarrer le service Samba pour appliquer les modifications

sudo service smbd restart

Cette commande redémarre le service Samba, appliquant ainsi les nouvelles configurations.

Pour vérifier que le service Samba fonctionne correctement, nous pouvons utiliser la commande suivante :

sudo systemctl status smbd.service

Cette commande affiche l'état actuel du service Samba, nous permettant de vérifier s'il est actif et fonctionne correctement.

4. Configuration des permissions sur le répertoire partagé

Nous devons nous assurer que le répertoire partagé a les bonnes permissions et appartient à l'utilisateur approprié.

Affichons les permissions actuelles du répertoire :

ls -l /home/alaa/raid5

Ensuite, changeons les permissions pour rendre le répertoire accessible :

sudo chmod -R 777 /home/alaa/raid5

Cette commande donne toutes les permissions (lecture, écriture, exécution) à tous les utilisateurs pour ce répertoire.

Si nous voulons restreindre légèrement les permissions, nous pouvons utiliser :

sudo chmod -R 775 /home/alaa/raid5

Cette commande donne des permissions complètes au propriétaire et au groupe, et des permissions de lecture et d'exécution aux autres.

Enfin, changeons le propriétaire du répertoire pour qu'il appartienne à l'utilisateur spécifié (par exemple, alaa) :

sudo chown -R alaa:alaa /home/alaa/raid5

Cette commande change le propriétaire et le groupe du répertoire et de tout son contenu.

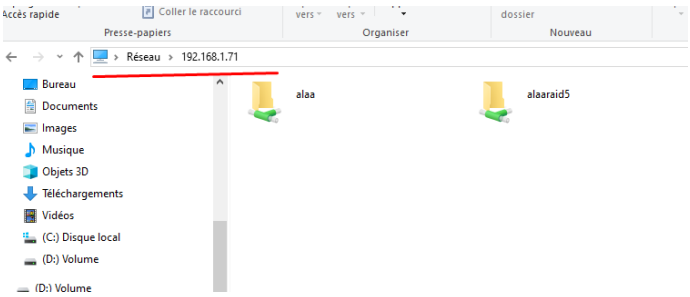
5. Accéder au partage Samba

Pour tester l'accès au partage Samba, nous pouvons utiliser la commande suivante :

smbclient //192.168.1.71/alaaraid5 -U alaa

Cette commande permet de se connecter au partage Samba spécifié sur l'adresse IP donnée avec le nom d'utilisateur **alaa**.

En suivant ces étapes, nous aurons installé et configuré Samba pour partager notre répertoire RAID 5. Assurons-nous de vérifier et de sauvegarder toutes nos configurations avant de procéder.



Voici les étapes pour installer et configurer Samba, présentées sous forme de tableau :

Étape	Description	Commandes

1. Installation de Samba	Installer le logiciel Samba pour partager des fichiers et des imprimantes entre différents systèmes d'exploitation.	**sudo apt-get install samba**
2. Configuration de Samba	Configurer le partage en éditant le fichier de configuration **smb.conf**.	**sudo nano /etc/samba/smb.conf**
	Ajouter la configuration suivante dans **smb.conf** :	**ini [NomDuPartage] path = /chemin/vers/votre/raid public = no writable = yes**
	- **NomDuPartage** : Nom du partage - **/chemin/vers/votre/raid** : Chemin d'accès réel à notre RAID 5	
3. Redémarrer le service Samba	Appliquer les modifications en redémarrant le service Samba.	**sudo service smbd restart**
	Vérifier que le service Samba fonctionne correctement.	**sudo systemctl status smbd.service**
4. Configuration des permissions sur le répertoire partagé	Vérifier les permissions actuelles du répertoire.	**ls -l /home/alaa/raid5**
	Changer les permissions pour rendre le répertoire accessible à tous les utilisateurs.	**sudo chmod -R 777 /home/alaa/raid5**
	Option pour restreindre légèrement les permissions.	**sudo chmod -R 775 /home/alaa/raid5**
	Changer le propriétaire du répertoire pour l'utilisateur spécifié (par exemple, alaa).	**sudo chown -R alaa:alaa /home/alaa/raid5**
5. Accéder au partage Samba	Tester l'accès au partage Samba avec la commande suivante.	**smbclient //192.168.1.71/alaaraid5 -U alaa**

3-installer et configurer un serveur SFTP sur Debian

Pour installer et configurer un serveur SFTP sur Debian ainsi que le client, suivons les étapes ci-dessous :

Installation du serveur SFTP (OpenSSH)

1. **Mettre à jour le système :**

sudo apt update

sudo apt upgrade

Installer le paquet OpenSSH :

sudo apt install openssh-server

Configurer le serveur SSH pour SFTP :

Ouvrons le fichier de configuration SSH :

sudo nano /etc/ssh/sshd_config

Ajoutons ou modifions les lignes suivantes pour configurer un sous-système SFTP :

Subsystem sftp internal-sftp

Ajouter un nouvel utilisateur (optionnel)

Si nécessaire, nous pouvons ajouter un nouvel utilisateur pour le SFTP en utilisant la commande suivante :

sudo adduser sftpuser

Cela crée un nouvel utilisateur nommé **sftpuser**.

Configuration du fichier sshd_config

Pour restreindre l'accès et définir des configurations spécifiques pour l'utilisateur **sftp_user**, nous pouvons éditer le fichier de configuration **sshd_config** avec les directives appropriées. Voici un exemple de configuration pour chrooter l'utilisateur **sftp_user** dans le répertoire **/home/alaa/raid5** :

Match User sftp_user

ChrootDirectory /home/alaa/raid5

ForceCommand internal-sftp

AllowTcpForwarding no

X11Forwarding no

Cela assure que l'utilisateur **sftp_user** est restreint au répertoire **/home/alaa/raid5** lorsqu'il se connecte via SFTP, sans possibilité de se déplacer dans d'autres répertoires ou d'exécuter des commandes Shell.

Connexion au SFTP

sftp alaa@192.168.1.71:/home/alaa/raid5

sftp sftp_user@192.168.1.71:/home/alaa/raid5

Voici les étapes pour configurer le SFTP, présentées sous forme de tableau :

Étape	Description	Commandes
1. Changer les permissions sur le répertoire	Assurer que les permissions sur le répertoire sont correctes.	**sudo chown alaa:alaa /home/alaa/raid5** **sudo chmod 755 /home** **sudo chmod 750 /home/alaa** **sudo chmod -R 755 /home/alaa/raid5**
2. Redémarrer le service SSH	Appliquer les changements en redémarrant le service SSH.	**sudo service ssh restart**
3. Changer le groupe du répertoire	Si nécessaire, changer le groupe du répertoire pour correspondre au groupe de l'utilisateur SFTP.	**sudo chown :sftp_user /home/alaa/raid5**
4. Ajouter l'utilisateur au groupe	Assurer que l'utilisateur a accès au répertoire en l'ajoutant au groupe approprié.	**sudo usermod -aG alaa sftp_user**
5. Vérifier l'appartenance au groupe	Vérifier si l'utilisateur est bien membre du groupe.	**groups sftp_user**
6. Ajouter un nouvel utilisateur (optionnel)	Créer un nouvel utilisateur pour le SFTP si nécessaire.	**sudo adduser sftpuser**
7. Connexion au SFTP	Se connecter au SFTP avec les utilisateurs appropriés.	**sftp alaa@192.168.1.71:/home/alaa/raid5** **sftp sftp_user@192.168.1.71:/home/alaa/raid5**

4-Réplication des données avec rsync depuis notre VM Debian vers un autre emplacement

1. Mise à jour du système

Nous devons d'abord mettre à jour notre système pour nous assurer que nous avons les dernières versions des paquets et des listes de paquets. Utilisons la commande suivante :

sudo apt update

Cette commande met à jour la liste des paquets disponibles et leurs versions.

2. Installation de rsync

Ensuite, nous devons installer l'outil rsync, qui est utilisé pour la synchronisation et la copie de fichiers entre différents systèmes. Utilisons la commande suivante :

sudo apt install rsync

Cette commande installe rsync sur notre système.

3. Synchronisation des données avec rsync

Pour synchroniser les données du répertoire **/home/alaa/raid5** vers un autre emplacement sur un serveur distant, nous pouvons utiliser la commande suivante :

rsync -avz /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup

- **-a** : Archive mode (copie les fichiers et les répertoires récursivement et préserve les permissions, les timestamps, les symboliques, etc.)
- **-v** : Mode verbeux (affiche les détails de la copie)
- **-z** : Compression des fichiers pendant le transfert pour économiser la bande passante
- **/home/alaa/raid5/** : Répertoire source
- **alaa@192.168.1.159:/home/alaa/raid5backup** : Répertoire de destination sur le serveur distant (adresse IP et chemin)

4. Exclusion de répertoires spécifiques

Si nous voulons exclure certains répertoires, comme **lost+found**, de la synchronisation, nous pouvons utiliser l'option **--exclude** :

rsync -avz --exclude=lost+found /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup

Cette commande exclut le répertoire **lost+found** de la synchronisation.

5. Automatisation de la synchronisation avec une tâche planifiée

Pour automatiser la synchronisation des données, nous pouvons créer une tâche planifiée à l'aide de cron. Utilisons la commande suivante pour éditer le crontab (planificateur de tâches) :

sudo crontab -e

Ajoutons la ligne suivante pour planifier la tâche de synchronisation :

* * * * * rsync -avz --exclude=lost+found /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup

- *** * * * *** : Planifie l'exécution de la commande chaque minute.
- La commande rsync est la même que précédemment, permettant une synchronisation automatique toutes les minutes.

En suivant ces étapes, nous aurons configuré la réplication des données avec rsync depuis notre VM Debian vers un autre emplacement, et nous aurons automatisé cette tâche pour qu'elle s'exécute régulièrement.

Voici les étapes pour la réplication des données avec rsync depuis notre VM Debian vers un autre emplacement, présentées sous forme de tableau :

Étape	Description	Commandes
1. Mise à jour du système	Mettre à jour la liste des paquets disponibles et leurs versions.	**sudo apt update**
2. Installation de rsync	Installer l'outil rsync pour la synchronisation et la copie de fichiers.	**sudo apt install rsync**
3. Synchronisation des données avec rsync	Synchroniser les données du répertoire **/home/alaa/raid5** vers un autre emplacement sur un serveur distant.	**rsync -avz /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup**

	- **-a** : Archive mode (copie les fichiers et les répertoires récursivement et préserve les permissions, les timestamps, les symboliques, etc.) - **-v** : Mode verbeux (affiche les détails de la copie) - **-z** : Compression des fichiers pendant le transfert pour économiser la bande passante	
4. Exclusion de répertoires spécifiques	Exclure certains répertoires, comme **lost+found**, de la synchronisation.	**rsync -avz --exclude=lost+found /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup**
5. Automatisation de la synchronisation avec une tâche planifiée	Créer une tâche planifiée à l'aide de cron pour automatiser la synchronisation des données.	**sudo crontab -e**
	Ajouter la ligne suivante pour planifier la tâche de synchronisation chaque minute :	*** * * * * rsync -avz --exclude=lost+found /home/alaa/raid5/ alaa@192.168.1.159:/home/alaa/raid5backup**

5-Utilisation du SSH sans mot de passe avec une clé RSA

Pour éviter que le système distant ne demande un mot de passe lors de l'exécution via cron, nous pouvons configurer l'authentification par clé SSH entre notre machine locale (notre VM Debian) et la machine distante. Cela permettra à la connexion SSH d'être établie automatiquement sans demander de mot de passe.

1. Génération d'une paire de clés SSH

Si nous n'avons pas déjà une paire de clés SSH sur notre VM Debian, nous devons en générer une. Utilisons la commande suivante :

ssh-keygen -t rsa

Cette commande génère une paire de clés SSH (privée et publique) de type RSA.

2. Copie de la clé publique vers le serveur distant

Ensuite, nous devons copier la clé publique générée vers le serveur distant. Utilisons la commande suivante :

ssh-copy-id alaa@192.168.1.159

Cette commande copie la clé publique vers le répertoire **~/.ssh/authorized_keys** sur le serveur distant, permettant ainsi une connexion sans mot de passe.

Une fois la clé publique copiée, nous devrions pouvoir nous connecter au serveur distant sans qu'il ne nous demande de mot de passe.

6-Installation et configuration de Webmin sur Debian

1. Mettre à jour le système

Avant d'installer Webmin, nous devons nous assurer que notre système Debian est à jour. Utilisons les commandes suivantes dans notre terminal :

sudo apt update

sudo apt upgrade

Ces commandes mettent à jour les listes de paquets disponibles et effectuent la mise à jour de tous les paquets déjà installés.

2. Télécharger le fichier d'installation

Comme Webmin n'est pas inclus dans les dépôts officiels de Debian, nous devons le télécharger depuis le site Web de Webmin. Utilisons wget pour télécharger le fichier d'installation directement sur notre système :

wget http://prdownloads.sourceforge.net/webadmin/webmin_1.973_all.deb

3. Installer Webmin

Une fois le fichier téléchargé, nous pouvons l'installer en utilisant dpkg (le gestionnaire de paquets Debian) :

sudo dpkg -i webmin_1.973_all.deb

Si des dépendances manquent, nous pouvons les installer en utilisant la commande suivante :

sudo apt-get install -f

4. Accéder à Webmin

Après l'installation, nous pouvons accéder à l'interface Web de Webmin en ouvrant notre navigateur Web et en visitant l'adresse suivante :

https://192.168.1.71:10000

Remplaçons **192.168.1.71** par l'adresse IP de notre serveur Debian.

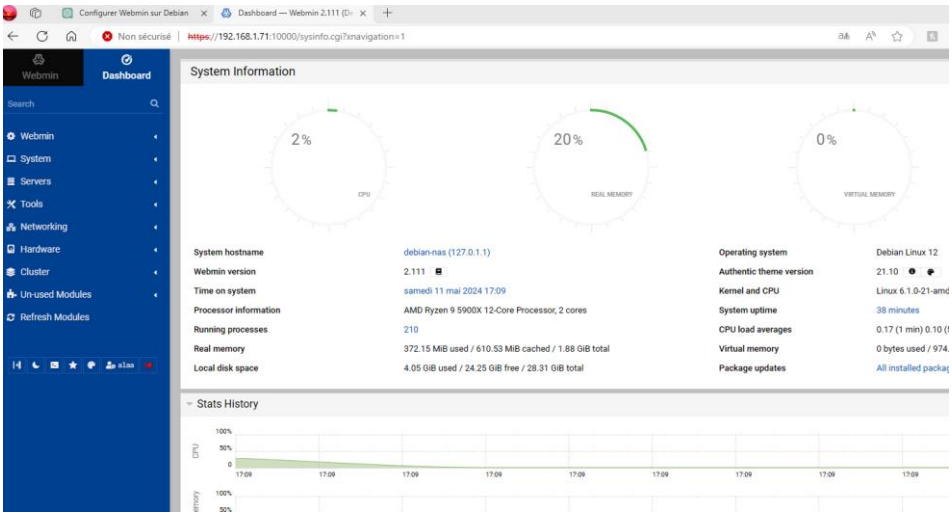
5. Connexion à Webmin

Nous utilisons nos identifiants d'administration système (par exemple, ceux de notre compte root) pour nous connecter à Webmin. Si nous rencontrons des problèmes de certificat SSL auto-signé, nous pouvons les ignorer ou accepter l'exception dans notre navigateur.

6. Configuration initiale

Une fois connectés, nous pouvons commencer à configurer Webmin selon nos besoins. Parcourons les différentes options de configuration pour sécuriser et personnaliser Webmin selon nos besoins spécifiques.

Ces étapes devraient nous permettre d'installer et de configurer Webmin avec succès sur notre serveur Debian. Si nous avons des questions ou rencontrons des problèmes, n'hésitons pas à demander de l'aide supplémentaire !



7-Installation et configuration de Nextcloud sur Debian

1. Installation des composants requis

Nous installerons Apache (le serveur web), MySQL/MariaDB (la base de données) et PHP (le langage de script côté serveur) un par un. Utilisons les commandes suivantes :

Composant	Commande d'installation
Apache	**sudo apt-get install apache2**
MySQL/MariaDB	Pour MySQL : **sudo apt-get install mysql-server** Pour MariaDB : **sudo apt-get install mariadb-server**
PHP	**sudo apt-get install php**

2. Configuration de la base de données pour Nextcloud

Après avoir installé MySQL/MariaDB, nous devons créer une base de données et un utilisateur pour Nextcloud. Suivons ces étapes :

1. Connectons-nous à MySQL en tant qu'utilisateur root :

sudo mysql -u root -p

2. Créons la base de données "nextcloud" :

CREATE DATABASE nextcloud;

3. Créons l'utilisateur "alaacloud" avec le mot de passe "alaa" et accordons-lui tous les privilèges sur la base de données "nextcloud" :

CREATE USER 'alaacloud'@'localhost' IDENTIFIED BY 'alaa';

GRANT ALL PRIVILEGES ON nextcloud.* TO 'alaacloud'@'localhost';

FLUSH PRIVILEGES;

EXIT;

3. Téléchargement et extraction de Nextcloud

Téléchargeons Nextcloud depuis le site officiel et extrayons-le dans le répertoire de destination :

wget https://download.nextcloud.com/server/releases/nextcloud-28.0.0.tar.bz2

tar -xvjf nextcloud-28.0.0.tar.bz2

sudo mv nextcloud /var/www/

sudo chown -R www-data:www-data /var/www/nextcloud/

4. Configuration d'Apache pour Nextcloud

Créons un fichier de configuration pour Nextcloud dans Apache :

sudo nano /etc/apache2/sites-available/nextcloud.conf

Puis, ajoutons les configurations suivantes dans le fichier :

```
Alias /nextcloud "/var/www/nextcloud/"
<Directory /var/www/nextcloud/>
   Options +FollowSymlinks
   AllowOverride All
   <IfModule mod_dav.c>
      Dav off
   </IfModule>
   SetEnv HOME /var/www/nextcloud
   SetEnv HTTP_HOME /var/www/nextcloud
</Directory>
```

5. Activation des configurations et modules Apache

Activons le site Nextcloud et les modules nécessaires dans Apache :

sudo a2ensite nextcloud.conf

sudo a2enmod rewrite headers env dir mime

sudo systemctl restart apache2

6. Configuration de Nextcloud

Modifions le fichier de configuration de Nextcloud pour spécifier le répertoire de stockage sur notre RAID 5 :

sudo nano /var/www/nextcloud/config/config.php

Et modifions le paramètre 'datadirectory' pour pointer vers le répertoire de notre RAID 5 :

'datadirectory' => '/home/alaa/raid5/',

En suivant ces étapes, nous avons installé et configuré Nextcloud sur notre serveur Debian, en lui permettant d'utiliser uniquement le répertoire spécifié sur notre RAID 5 pour le stockage de données, assurant ainsi la sécurité et l'isolation des données.