Guide de Configuration : Serveur Cloud Personnel Sécurisé avec Nextcloud sur Raspberry Pi

David .T

1. Matériel nécessaire

Pour configurer ton cloud sécurisé avec Nextcloud, tu auras besoin du matériel suivant:

- **Raspberry Pi 5** (ou Raspberry Pi 4 si tu n'as pas accès au 5)
- **Carte microSD** (32 Go ou plus, classe 10 ou supérieure)
- **Disque dur externe ou SSD** pour le stockage (connecté via USB)
- **Câble d’alimentation pour le Raspberry Pi**
- **Clavier et écran pour la configuration initiale**
- **Routeur compatible** (pour la configuration réseau, Ethernet recommandé)
- **Connexion Internet** pour télécharger les paquets et certificats SSL.

2. Préparation du Raspberry Pi

2.1. Installation de Raspberry Pi OS

(Raspberry Pi OS est le système d'exploitation qui permettra au Raspberry Pi de fonctionner. La version "Lite" sans interface graphique est choisie car elle économise des ressources et est idéale pour un serveur qui ne nécessite pas d'interface utilisateur lourde.)

1. **Télécharge** l'utilitaire **Raspberry Pi Imager** sur ton ordinateur.
2. **Installe Raspberry Pi OS Lite** (version sans interface graphique) sur ta carte microSD.
    - Cette version légère est idéale pour économiser des ressources.
3. **Insère** la carte microSD dans le Raspberry Pi, connecte-le à un clavier et un écran, puis démarre-le.

2.2. Mise à jour du système

(Les mises à jour garantissent que tous les logiciels installés sont à jour et contiennent les derniers correctifs de sécurité. Cela renforce la sécurité et la stabilité de ton syst)

Après le démarrage du Raspberry Pi, ouvre le terminal et exécute les commandes suivantes pour mettre à jour ton système :

```
sudo apt update
```

```
sudo apt upgrade -y
```

Cela garantit que tous les paquets sont à jour.

2.3. Partitionnement et chiffrement (LUKS)

(Le chiffrement via LUKS protège les données stockées sur le disque dur externe ou le SSD. Même si quelqu'un parvient à accéder physiquement à ton disque, il ne pourra pas lire tes fichiers sans la clé de chiffrement. Cela améliore la confidentialité et la sécurité de tes données.)

Pour une meilleure sécurité des données stockées sur ton disque dur externe ou SSD, tu peux configurer le chiffrement avec **LUKS**.

4. **Installer Cryptsetup** (utilitaire pour gérer LUKS) :

```
sudo apt install cryptsetup
```

5. **Chiffrer ton disque externe** avec LUKS :

```
sudo cryptsetup luksFormat /dev/sdX
```

Remplace /dev/sdX par l'emplacement de ton disque. Cette commande va formater et chiffrer le disque.

6. **Ouvrir le disque chiffré** :

```
sudo cryptsetup luksOpen /dev/sdX mon_disque_chiffre
```

7. **Formater le disque** :

```
sudo mkfs.ext4 /dev/mapper/mon_disque_chiffre
```

8. **Monter le disque** pour que Nextcloud puisse y accéder :

```
sudo mount /dev/mapper/mon_disque_chiffre /mnt/nextcloud_data
```

3. Installation de Nextcloud

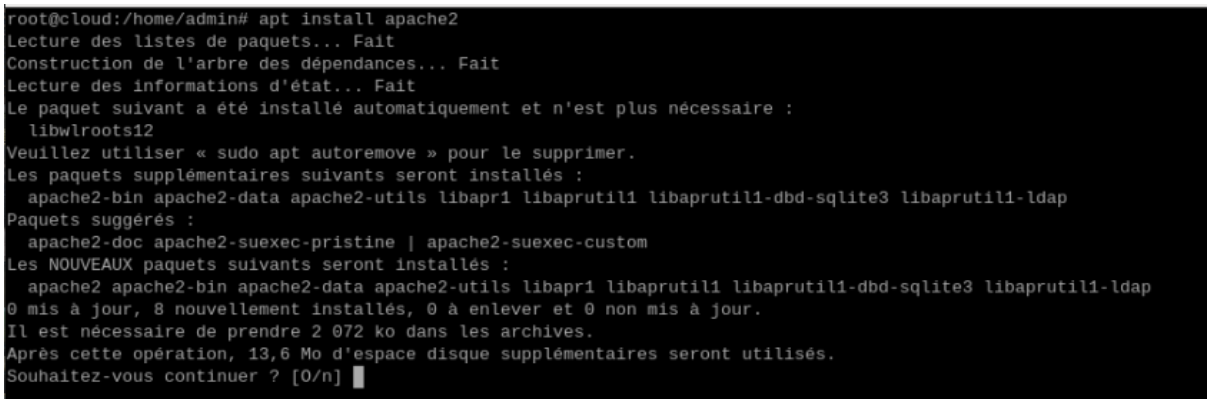
3.1. Installation d'Apache, MariaDB et PHP

(Apache est le serveur web qui permet aux utilisateurs d'accéder à l'interface Nextcloud via un navigateur.
MariaDB est le système de gestion de base de données qui stocke toutes les informations de Nextcloud, comme les utilisateurs et les fichiers.
PHP est le langage de programmation utilisé par Nextcloud pour fonctionner. Les modules supplémentaires (comme php-mysql ou php-gd) sont nécessaires pour certaines fonctionnalités comme la gestion des bases de données ou le traitement des images.)

Pour héberger Nextcloud, nous avons besoin d'un serveur web, d'une base de données et de PHP.

9. **Installer Apache** :

sudo apt install apache2 –y



10. **Installer MariaDB** (base de données) :

sudo apt install mariadb-server –y

```
root@cloud:/home/admin# apt install mariadb-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  libwlroots12
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  galera-4 gawk libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mariadb-perl
  libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl
  libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmariadb3
  libregexp-ipv6-perl libsigsegv2 libterm-readkey-perl libtimedate-perl liburi-perl liburing2 mariadb-client
  mariadb-client-core mariadb-common mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4
  mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo mariadb-plugin-provider-snappy mariadb-server-core
  mysql-common pv socat
Paquets suggérés :
  gawk-doc libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl
  libbusiness-isbn-perl libwww-perl mailx mariadb-test netcat-openbsd doc-base
Les NOUVEAUX paquets suivants seront installés :
  galera-4 gawk libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mariadb-perl
  libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl
  libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmariadb3
  libregexp-ipv6-perl libsigsegv2 libterm-readkey-perl libtimedate-perl liburi-perl liburing2 mariadb-client
  mariadb-client-core mariadb-common mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4
  mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo mariadb-plugin-provider-snappy mariadb-server
  mariadb-server-core mysql-common pv socat
0 mis à jour, 39 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 17,7 Mo dans les archives.
Après cette opération, 195 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

11. **Installer PHP et les modules nécessaires** :

sudo apt install php libapache2-mod-php php-mysql php-zip php-dom php-curl php-gd php-xml php-mbstring php-intl php-imagick php-bcmath php-gmp –y

```
root@cloud:/home/admin# sudo apt install php libapache2-mod-php php-mysql php-zip php-dom php-curl php-gd php-xml php-
mbstring php-intl php-imagick php-bcmath php-gmp -y
```

3.2. Configuration de MariaDB

(Cette étape configure la base de données pour Nextcloud. Une base de données dédiée à Nextcloud est créée, avec un utilisateur spécifique et des permissions appropriées pour gérer les données de manière sécurisée.)

12. Sécuriser MariaDB :

sudo mysql_secure_installation

Suis les instructions pour définir un mot de passe root sécurisé et désactiver les options non nécessaires.

13. **Configurer la base de données pour Nextcloud** :
    - Connecte-toi à MariaDB :
    -

sudo mysql -u root -p

- Crée une base de données et un utilisateur pour Nextcloud :

CREATE DATABASE nextcloud;

```
MariaDB [(none)]> CREATE DATABASE nextcloud;
Query OK, 1 row affected (0,000 sec)
```

CREATE USER 'nextclouduser'@'localhost' IDENTIFIED BY 'mot_de_passe_securise';

```
MariaDB [(none)]> CREATE USER 'neo'@'localhost' IDENTIFIED BY 'Jlachfe&lq';
Query OK, 0 rows affected (0,007 sec)
```

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

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud.* TO 'neo'@'localhost';
Query OK, 0 rows affected (0,007 sec)
```

FLUSH PRIVILEGES;
EXIT;

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> EXIT;
Bye
```

3.3. Téléchargement et installation de Nextcloud

(Tu télécharges et installes Nextcloud sur le Raspberry Pi. C'est l'application qui permet de gérer, partager et stocker tes fichiers, similaire à Google Drive ou Dropbox, mais hébergé chez toi.)

14. **Télécharger** Nextcloud
    wget https://download.nextcloud.com/server/releases/nextcloud-26.0.2.zip

```
root@cloud:/home/admin# wget https://download.nextcloud.com/server/releases/nextcloud-26.0.2.zip
--2024-12-27 23:46:38--  https://download.nextcloud.com/server/releases/nextcloud-26.0.2.zip
Résolution de download.nextcloud.com (download.nextcloud.com)… 2a01:4f8:210:21c8::145, 5.9.202.145
Connexion à download.nextcloud.com (download.nextcloud.com)|2a01:4f8:210:21c8::145|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 186134550 (178M) [application/zip]
Sauvegarde en : « nextcloud-26.0.2.zip »

nextcloud-26.0.2.zip          100%[=============================================>] 177,51M  7,66MB/s    ds 24s

2024-12-27 23:47:02 (7,42 MB/s) – « nextcloud-26.0.2.zip » sauvegardé [186134550/186134550]
```

15. **Décompresser** et déplacer le dossier Nextcloud dans le répertoire Apache :

unzip nextcloud-26.0.2.zip

sudo mv nextcloud /var/www/html/

```
  inflating: nextcloud/config/.htaccess
root@itak:/home/admin# mv nextcloud /var/www/html/
```

Et suppression du fichier zip

```
root@cloud:/home/admin# ls
Bookshelf  Desktop  Documents  Images  Modèles  Musique  nextcloud-26.0.2.zip  Public  Téléchargements  Vidéos
root@cloud:/home/admin# rm nextcloud-26.0.2.zip
root@cloud:/home/admin# ls
Bookshelf  Desktop  Documents  Images  Modèles  Musique  Public  Téléchargements  Vidéos
```

16. **Attribuer les permissions correctes** :

sudo chown -R www-data:www-data /var/www/html/nextcloud/config
sudo chown -R www-data:www-data /var/www/html/nextcloud/apps

sudo chmod -R 750 /var/www/html/nextcloud/config
sudo chmod -R 750 /var/www/html/nextcloud/apps

```
root@itak:/home/admin# chown -R www-data:www-data /var/www/html/nextcloud/apps
root@itak:/home/admin# chmod -R 750 /var/www/html/nextcloud/apps
root@itak:/home/admin# systemctl restart apache2
```

Création du dossier data (installation des apps nextcloud

```
root@itak:/var/www/html/nextcloud# mkdir data
root@itak:/var/www/html/nextcloud# chown -R www-data:www-data data
root@itak:/var/www/html/nextcloud# chmod -R 750 data
root@itak:/var/www/html/nextcloud# systemctl restart apache2
```

3.4. Configuration d'Apache pour Nextcloud

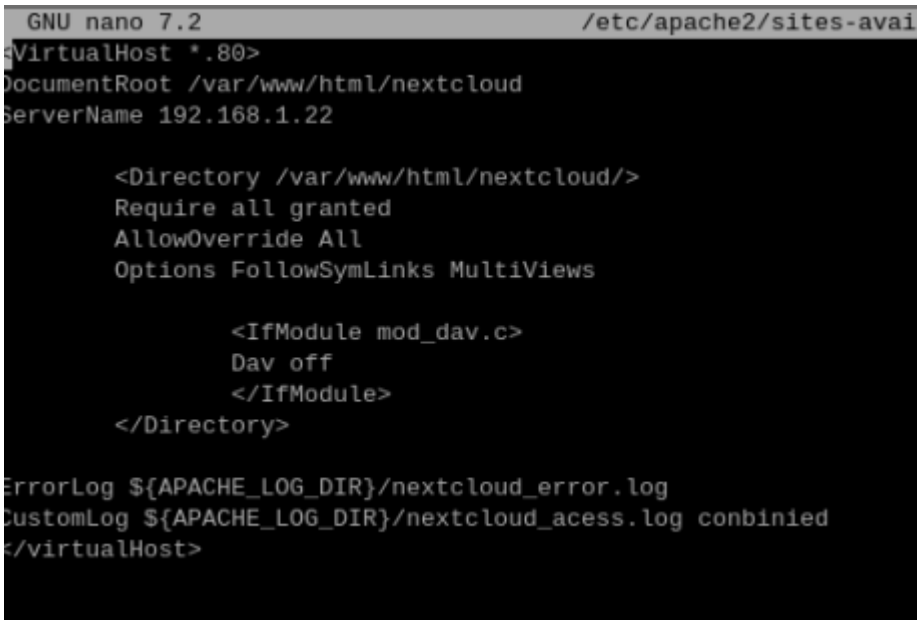
(Tu configures Apache pour qu'il serve correctement Nextcloud à partir de son répertoire d'installation. Cela permet à ton serveur web de comprendre comment traiter les requêtes vers Nextcloud, comme les connexions des utilisateurs ou l'accès aux fichiers.)

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

17. **Ajouter la configuration** suivante :

```
<VirtualHost *:80>
  DocumentRoot /var/www/html/nextcloud
  ServerName ton_domaine_ou_adresse_ip

  <Directory /var/www/html/nextcloud/>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
      Dav off
    </IfModule>
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
  CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
```

</VirtualHost>



<VirtualHost *:443>
  ServerName cloud-neo.duckdns.org
  DocumentRoot /var/www/html/nextcloud

  <Directory /var/www/html/nextcloud/>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
      Dav off
    </IfModule>
  </Directory>

  SSLEngine on
  SSLCertificateFile /etc/letsencrypt/live/cloud-neo.duckdns.org/fullchain.pem
  SSLCertificateKeyFile /etc/letsencrypt/live/cloud-neo.duckdns.org/privkey.pem

  ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
  CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>

```
<VirtualHost *:443>
  ServerName cloud-neo.duckdns.org
  DocumentRoot /var/www/html/nextcloud

  <Directory /var/www/html/nextcloud/>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
      Dav off
    </IfModule>
  </Directory>

  SSLEngine on
  SSLCertificateFile /etc/letsencrypt/live/cloud-neo.duckdns.org/fullchain.pem
  SSLCertificateKeyFile /etc/letsencrypt/live/cloud-neo.duckdns.org/privkey.pem

  ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
  CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>
```

18. **Activer le site et les modules nécessaires** :

sudo a2ensite nextcloud.conf

sudo a2enmod rewrite headers env dir mime

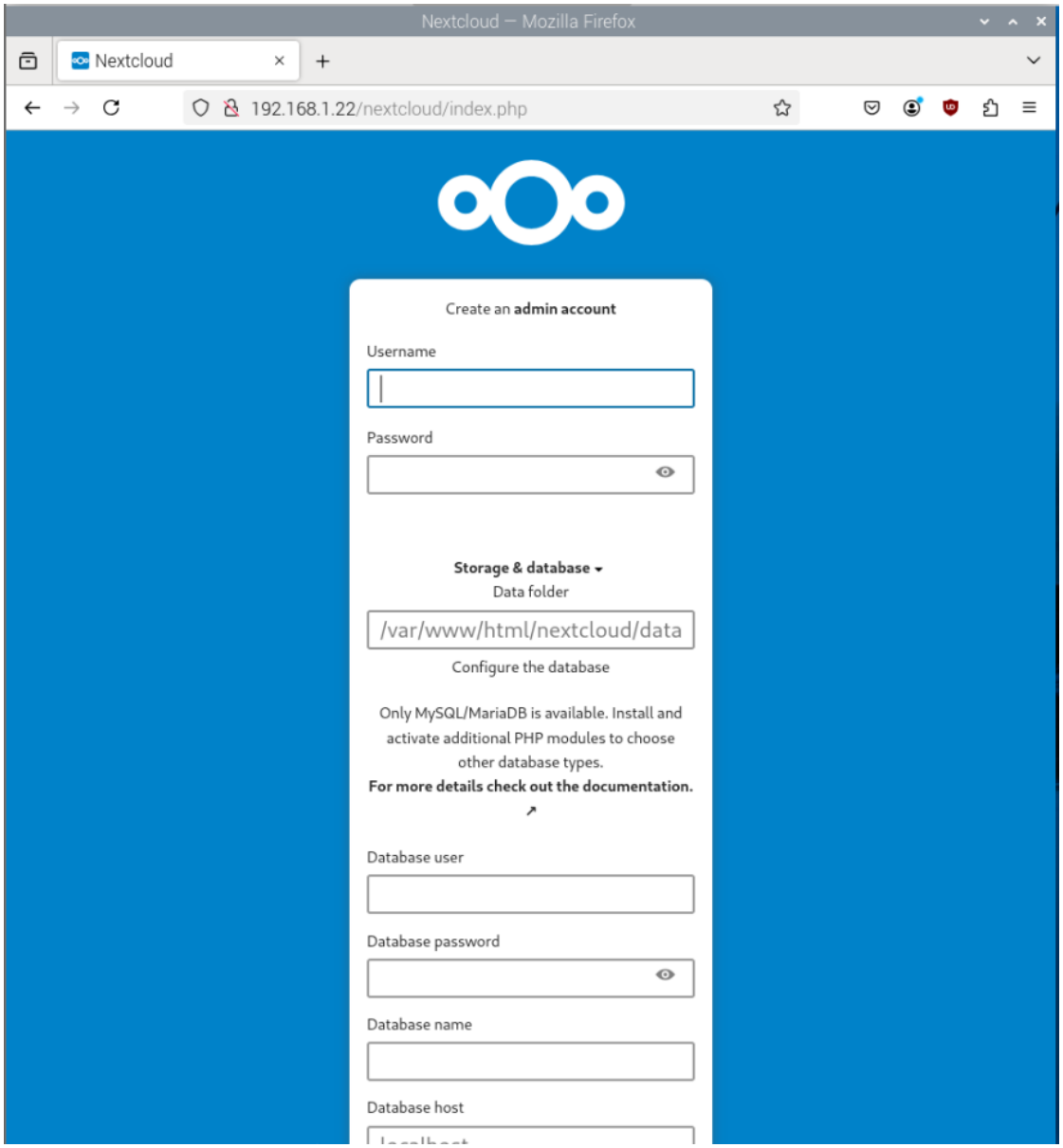
sudo systemctl restart apache2cd

3.5. Finalisation de l'installation

(C'est ici que tu termines l'installation via ton navigateur. Nextcloud configure les paramètres initiaux et commence à utiliser la base de données créée dans l'étape précédente.)

19. Ouvre ton navigateur et accède à l’adresse de ton Raspberry Pi ou à ton nom de domaine :

http://ton-ip/nextcloud



20. **Suis les instructions** pour terminer l'installation en utilisant la base de données que tu as créée.

4. Sécurisation du serveur

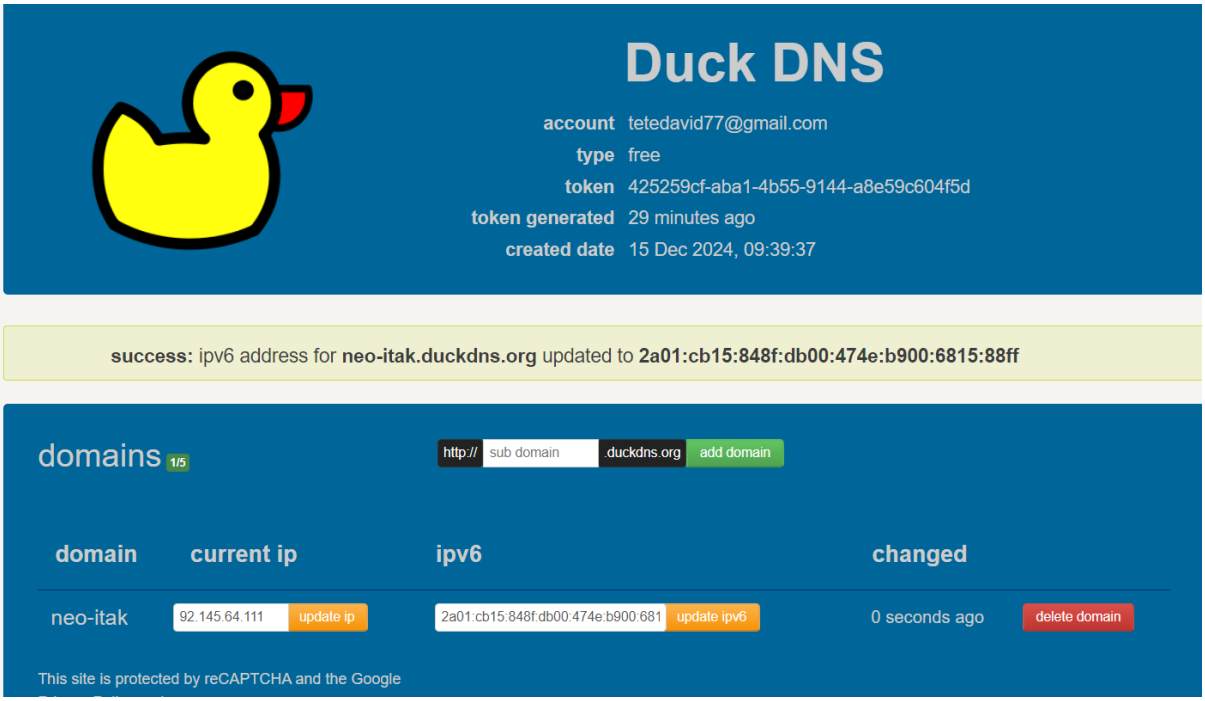
4.1. HTTPS avec Let's Encrypt

(Let's Encrypt permet d'obtenir gratuitement un certificat SSL, qui chiffre les communications entre les utilisateurs et ton serveur. Cela protège contre l'interception des données (comme les mots de passe ou fichiers) lors des connexions à Nextcloud.)

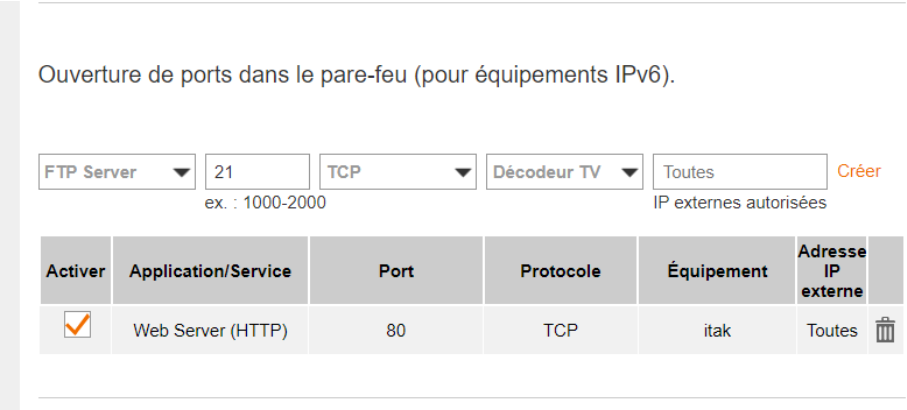
Pour sécuriser les connexions avec SSL :

Dans un premier temp il faut penser à se créer un nom de domaine.

Exemple : DuckDNS qui nous permet d’avoir un Nom de Domaine gratuitement.



Autoriser les connexions au port 80 depuis l'extérieur depuis l'interface Admin de la BOX



Modifier le nom du serveur dans le fichier de conf

```
  GNU nano 7.2
<VirtualHost *.80>
DocumentRoot /var/www/html/nextcloud
ServerName neo-itak.duckdns.org

        <Directory /var/www/html/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews

                <IfModule mod_dav.c>
                Dav off
                </IfModule>
        </Directory>

ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
CustomLog ${APACHE_LOG_DIR}/nextcloud_acess.log conbinied
RewriteEngine on
RewriteCond %{SERVER_NAME} =neo-itak.duckdns.org
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

```
root@cloud:/var/www/html/nextcloud/config# nano /var/www/html/nextcloud/config/config.php
```

```
  array (
    0 => '192.168.1.22',
    1 => 'neo-itak.duckdns.org',
  ),
  'datadirectory' => '/var/www/html/nex
```

21. **Installer Certbot** pour obtenir des certificats SSL :

sudo apt install certbot python3-certbot-apache -y

22. **Obtenir un certificat SSL** :

sudo certbot –apache

```
root@itak:/home/admin# certbot --apache -d neo-itak.duckdns.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Certificate not yet due for renewal

You have an existing certificate that has exactly the same domains or certificate name you requested and isn't close to expiry.
(ref: /etc/letsencrypt/renewal/neo-itak.duckdns.org.conf)

What would you like to do?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Attempt to reinstall this existing certificate
2: Renew & replace the certificate (may be subject to CA rate limits)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Deploying certificate
Successfully deployed certificate for neo-itak.duckdns.org to /etc/apache2/sites-available/nextcloud-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://neo-itak.duckdns.org

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

23. Suis les instructions pour configurer HTTPS.

4.2. Configuration du pare-feu (UFW) et SSH

(Le pare-feu UFW protège ton serveur en bloquant les connexions non autorisées. Il permet uniquement les connexions HTTP/HTTPS (sécurisées) et SSH (pour la gestion à distance). De plus, désactiver l'authentification par mot de passe pour SSH empêche les attaques de force brute et renforce la sécurité.)

24. **Configurer le pare-feu** UFW pour restreindre les connexions non sécurisées :

sudo apt install ufw –y

sudo ufw allow OpenSSH

```
root@itak:/home/admin# ufw allow OpenSSH
Rules updated
Rules updated (v6)
```

sudo ufw allow 'Apache Full'

```
root@itak:/home/admin# ufw allow 'Apache Full'
Rule added
Rule added (v6)
```

sudo ufw enable

- Cette configuration permet uniquement les connexions HTTP/HTTPS et SSH.

25. **Désactiver l'authentification par mot de passe SSH** :
    - Ouvre le fichier de configuration SSH :

sudo nano /etc/ssh/sshd_config

- Modifie les lignes suivantes :

PasswordAuthentication no
PermitRootLogin no

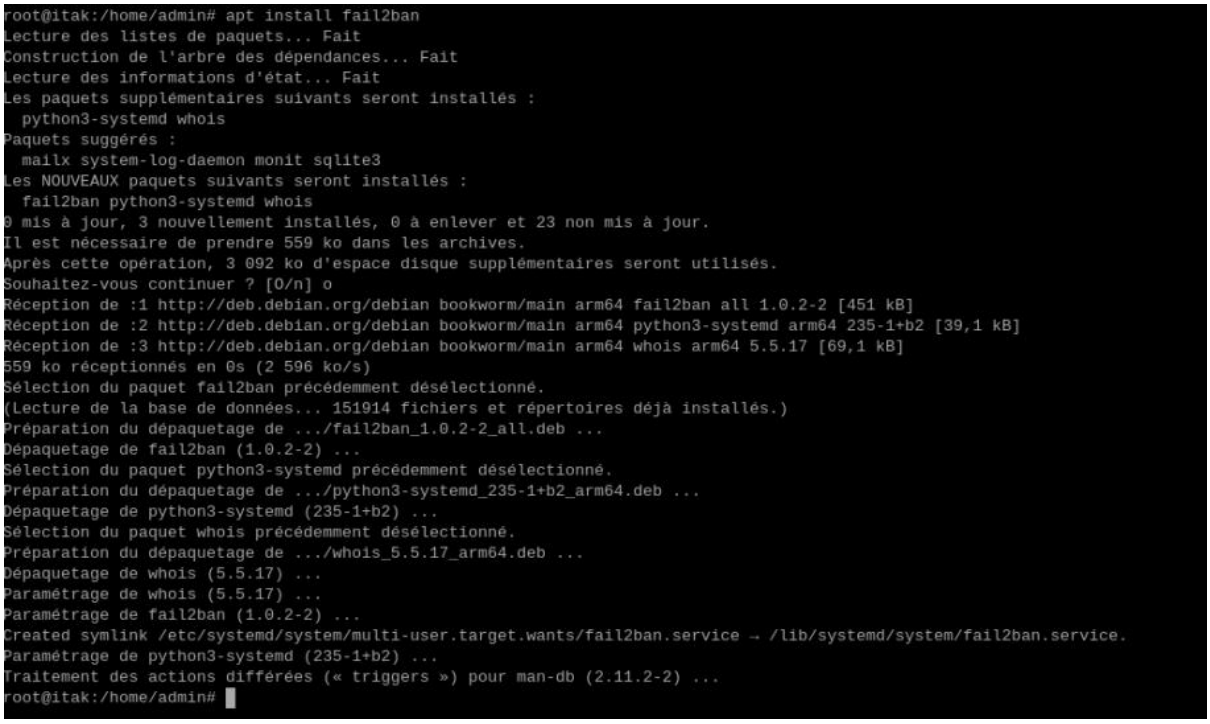
```
PasswordAuthentication no
PermitRootLogin no

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- Redémarre le service SSH :

sudo systemctl restart ssh

26. **Installer Fail2ban** pour protéger contre les attaques par force brute :

sudo apt install fail2ban



27. **Configurer Fail2ban pour SSH** :

sudo nano /etc/fail2ban/jail.local

- Ajoute ceci :

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3

4.3. Activation du chiffrement des données

(Cette étape assure que toutes les données stockées dans Nextcloud sont chiffrées. Même si une personne accède au serveur de fichiers, elle ne pourra pas lire les données sans la clé de chiffrement.)

28. Active le chiffrement dans les paramètres de sécurité de Nextcloud.

5. Accès externe sécurisé avec OpenVPN

5.1. Installation et configuration d'OpenVPN

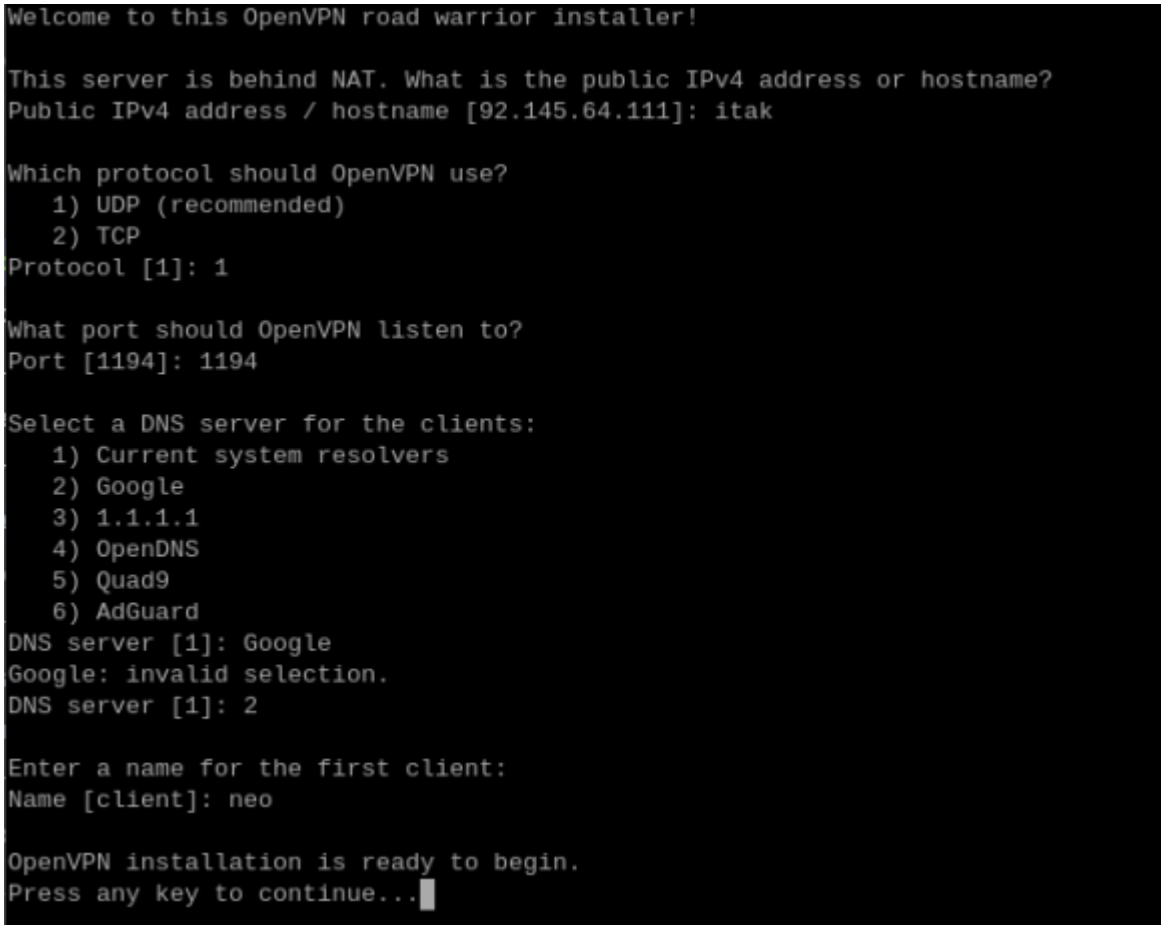
(OpenVPN permet un accès à distance sécurisé à ton serveur depuis l'extérieur de ton réseau local. En chiffrant le trafic via un VPN, cela protège les communications même sur des réseaux non sécurisés (comme le Wi-Fi public))

29. **Installer OpenVPN** :

sudo apt install openvpn -y

30. **Configurer OpenVPN** en suivant les instructions du script d'installation :

wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh



Une fois l'installation terminée, le script génère un fichier `.ovpn` pour le client que vous avez nommé (dans votre cas, `neo`). Ce fichier est crucial pour vous connecter au serveur OpenVPN.

Ce fichier sera situé dans le répertoire personnel de l'utilisateur qui a exécuté le script, généralement dans :

`/root/neo.ovpn`

Si vous ne trouvez pas le fichier ou si vous souhaitez générer un autre fichier client : `basopenvpn-install.sh`

Sélectionnez l'option "Add a new client" et entrez un nom

Copiez se fichier pour le mettre sur le poste client.

Télécharger OpenVPN Connect et ajoutez le fichier que vous avez copiez. Afin que la connexion puisse se faire.

6. Gestion des utilisateurs et droits d'accès

(Nextcloud permet de gérer plusieurs utilisateurs. Cela est utile si tu souhaites partager ton serveur avec d'autres personnes, en leur attribuant des permissions spécifiques (comme la lecture seule ou l'édition). L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire.)

31. **Activer l'authentification à deux facteurs (2FA)** dans les paramètres de Nextcloud.
32. **Créer des utilisateurs** avec des permissions spécifiques selon leurs besoins.
33. **Vérifier régulièrement les journaux d'accès** pour détecter des comportements anormaux.

7. Surveillance et mises à jour

7.1. Mises à jour automatiques

(Les mises à jour automatiques assurent que le système d'exploitation et les logiciels installés (comme Apache, MariaDB ou Nextcloud) reçoivent les dernières corrections de sécurité sans que tu aies besoin de les appliquer manuellement.)

Pour garder ton système à jour :

sudo apt install unattended-upgrades –y

sudo dpkg-reconfigure unattended-upgrades

7.2. Monitoring

(Le monitoring permet de surveiller les journaux de ton serveur pour détecter toute activité suspecte ou des erreurs système. Cela t'aide à prévenir et résoudre les problèmes potentiels avant qu'ils ne deviennent critiques.)

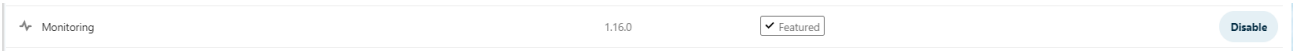
Surveille régulièrement les journaux Apache et Nextcloud.

7.3. Monitoring du système via l'application Nextcloud

(Nextcloud propose une application intégrée qui permet de surveiller l'état de ton serveur directement depuis l'interface Nextcloud. Voici comment l'installer et l'utiliser.)

7.3.1. Installation de l'application Server Info

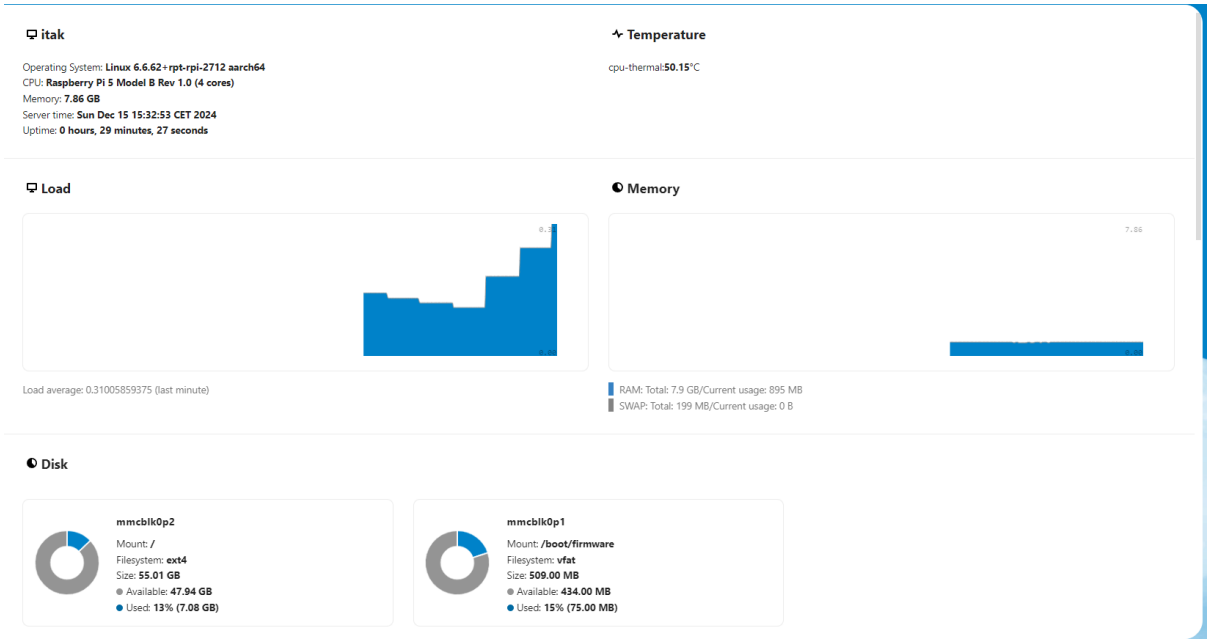
34. Connecte-toi à ton instance Nextcloud avec un compte administrateur.
35. Accède à l'onglet **Applications** :
    - Dans la barre latérale gauche, clique sur ton icône de profil, puis sélectionne **Applications** dans le menu déroulant.
36. Dans la barre de recherche en haut de la page, tape **Server Info** (ou **System Monitoring**).



37. Installe l'application **Server Info**.
    - Une fois installée, l'application sera automatiquement activée.

7.3.2. Accéder aux informations du serveur

38. Après l'installation, va dans **Paramètres** :
    - Clique sur ton icône de profil, puis sélectionne **Paramètres**.
39. Dans la barre latérale gauche, cherche la section **Information sur le serveur** sous l'onglet **Administration**.
40. Tu verras alors les informations suivantes :
    - **Utilisation du CPU** : Cela affiche la charge de travail actuelle du processeur.
    - **Utilisation de la RAM** : Cela indique la quantité de mémoire vive utilisée par le serveur.
    - **Espace disque disponible** : Cela montre la quantité d'espace de stockage disponible sur le disque utilisé par Nextcloud.
    - **Activité réseau** : Données concernant le trafic réseau sur le serveur.



Ces informations te permettent de suivre l'état général de ton serveur Nextcloud en temps réel et d'identifier rapidement les éventuels problèmes de performance.

7.3.3. Avantages de l'application Server Info

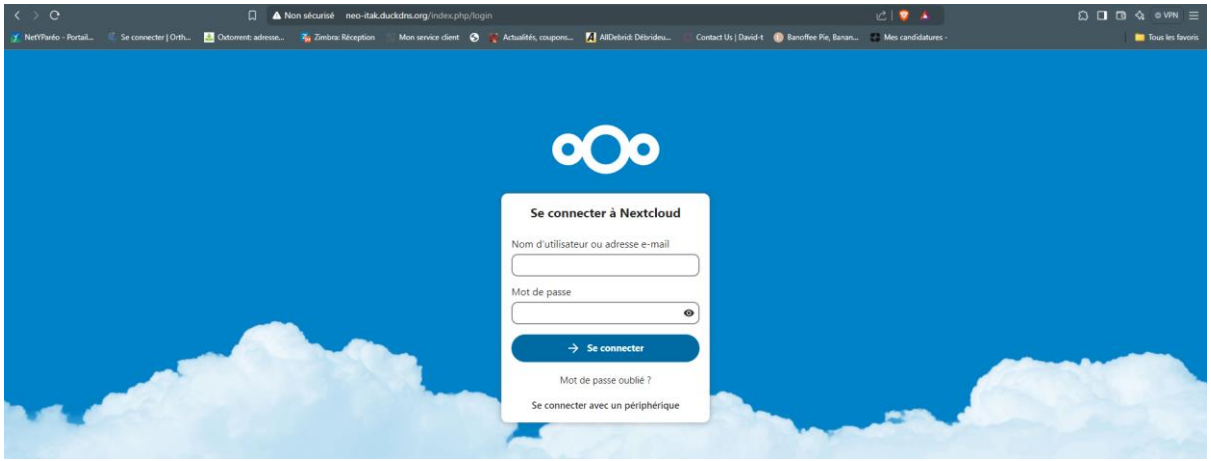
- **Facilité d'utilisation** : Aucune configuration avancée n'est nécessaire. L'application est installée et prête à l'emploi.
- **Surveillance en temps réel** : Elle fournit des données instantanées sur l'état du serveur.
- **Intégration native à Nextcloud** : Elle fait partie intégrante de l’interface Nextcloud, donc tout est centralisé.

8. Utilisation de Nextcloud

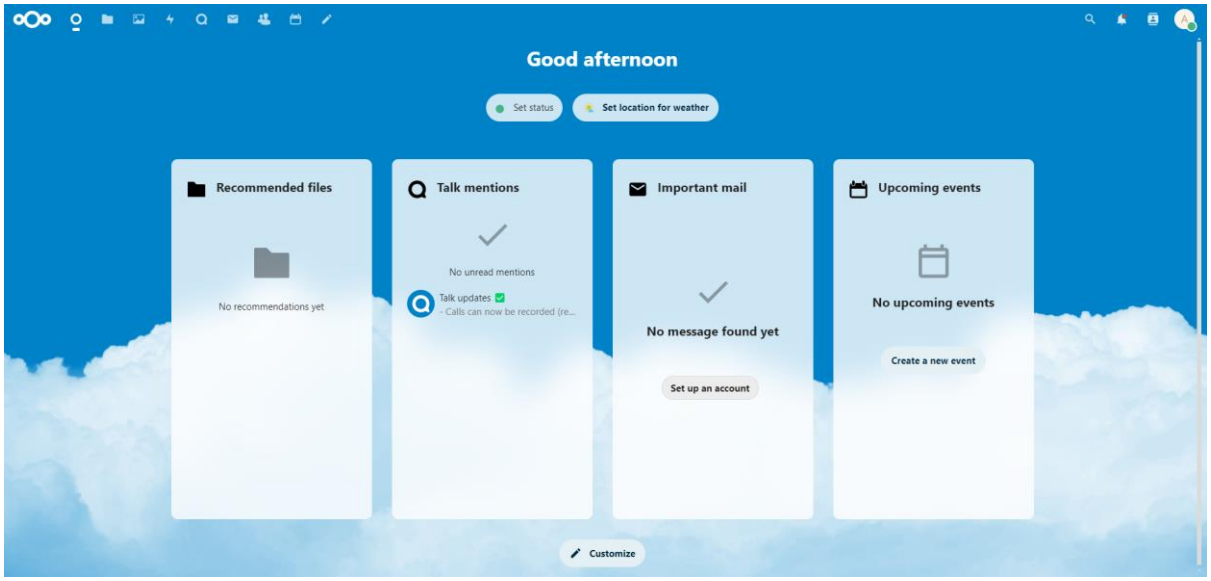
8.1. Connexion à Nextcloud

(Tu accèdes à Nextcloud via un navigateur web en entrant l'adresse IP ou le nom de domaine que tu as configuré. Tu te connectes avec tes identifiants administratifs pour accéder aux fonctionnalités de Nextcloud.)

41. **Ouvre un navigateur web** et accède à l'URL de ton Nextcloud : http://ton-ip/nextcloud ou https://ton-domaine.



42. **Connecte-toi avec tes identifiants** administratifs que tu as créés lors de l'installation.



8.2. Configuration initiale

(Une fois connecté, il est important de sécuriser davantage ton compte administrateur en modifiant le mot de passe et en configurant des options comme le stockage externe (par exemple, ton disque dur/SSD). Cela garantit que ton serveur est prêt à l'emploi.)

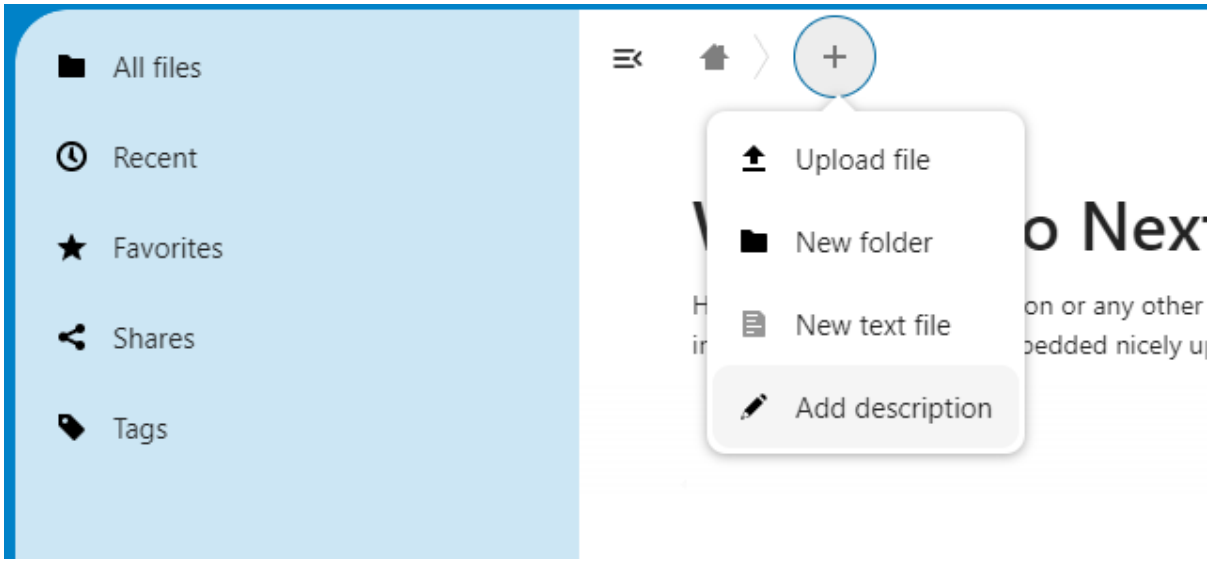
43. **Change le mot de passe administrateur** pour un mot de passe plus sécurisé.
44. **Configure les paramètres de stockage** dans les paramètres de Nextcloud (dans Paramètres > Administration > Stockage externe) pour inclure ton disque dur externe ou SSD si nécessaire.
45. **Vérifie la configuration du chiffrement** et active-le dans Paramètres > Sécurité.

8.3. Gestion des fichiers

(Nextcloud te permet de télécharger, organiser et partager des fichiers. Tu peux gérer des dossiers et fichiers comme sur un cloud traditionnel (Google Drive ou Dropbox), mais avec un contrôle total sur la sécurité et la confidentialité des données.)

46. Télécharger des fichiers :

- Clique sur le bouton Téléverser pour ajouter des fichiers depuis ton ordinateur.
- Tu peux également glisser-déposer des fichiers directement dans l'interface web.

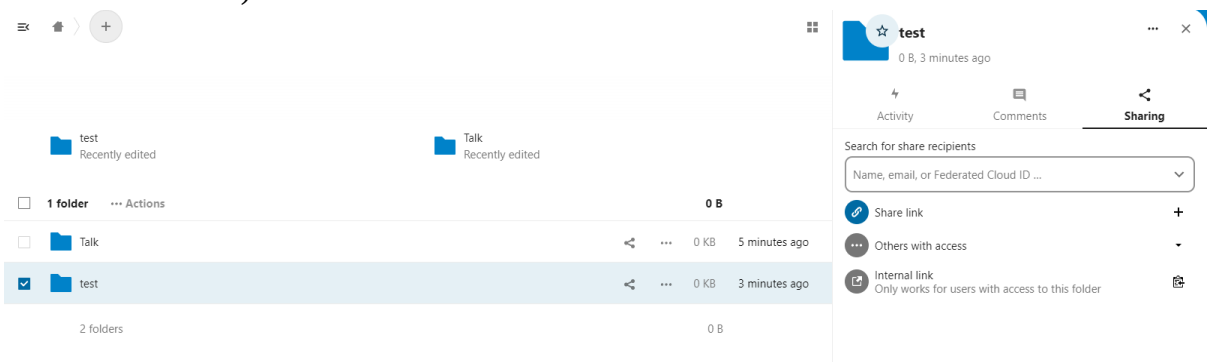


47. Organiser tes fichiers :

- Crée des dossiers pour classer tes fichiers.
- Utilise le moteur de recherche intégré pour retrouver rapidement des fichiers.

48. Partage de fichiers :

- Sélectionne un fichier ou un dossier, clique sur l'icône de partage, et génère un lien de partage.
- Configure les permissions pour les utilisateurs (lecture seule, modification, etc.).

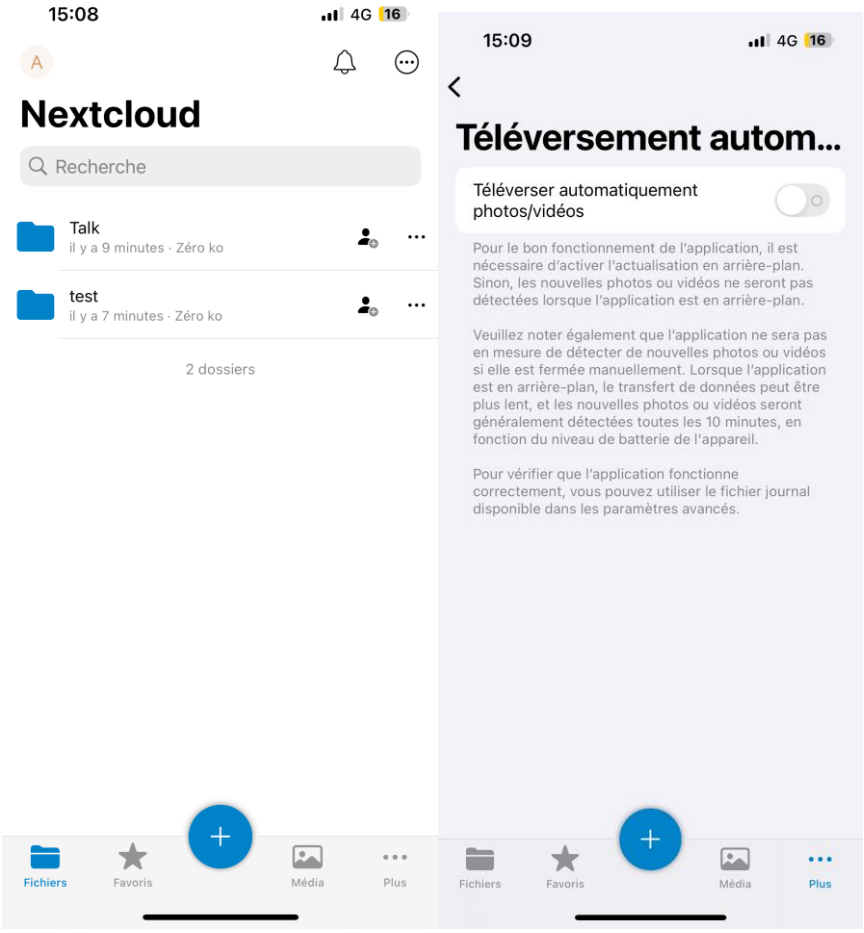


8.4. Application mobile

(L'application mobile Nextcloud permet de synchroniser et d'accéder à tes fichiers depuis un smartphone ou une tablette, où que tu sois.)

49. **Télécharge l'application Nextcloud** pour iOS ou Android depuis les boutiques d'applications.
50. **Connecte-toi avec tes identifiants** pour accéder à tes fichiers sur ton appareil mobile.

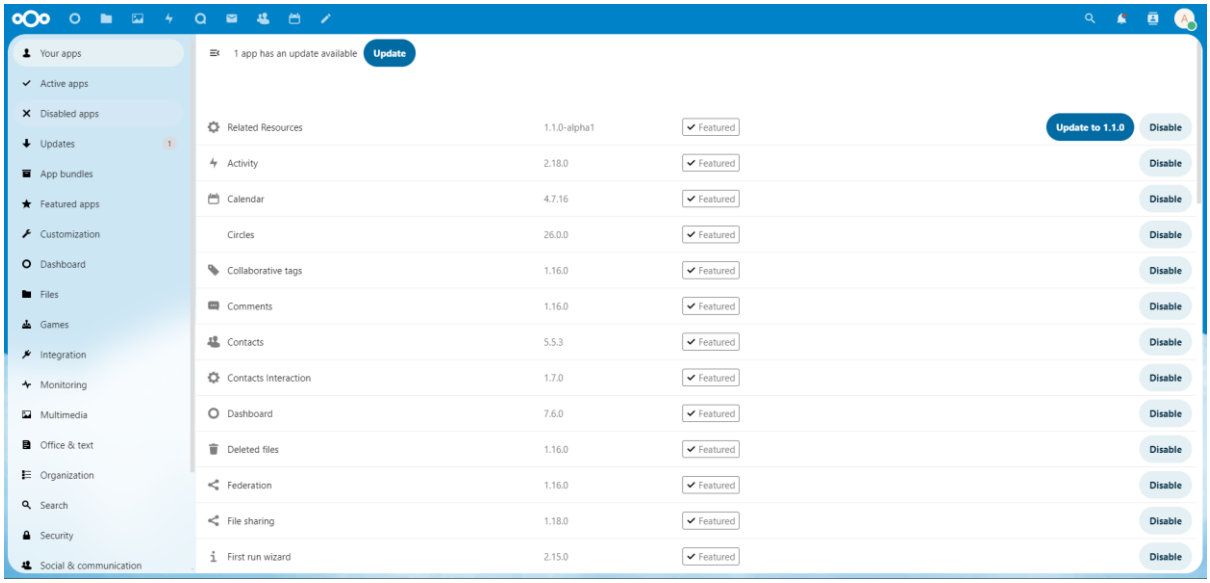
51. **Active la synchronisation automatique** pour garder tes fichiers à jour sur tous tes appareils.



8.5. Intégration d'applications

(Nextcloud offre un marché d'applications pour ajouter des fonctionnalités supplémentaires (comme un calendrier ou des outils de collaboration). Cela rend ton cloud encore plus polyvalent et utile.)

52. **Explore le marché d'applications de Nextcloud** pour ajouter des fonctionnalités supplémentaires (calendrier, contacts, etc.).
53. **Installe les applications désirées** via l'interface d'administration sous Applications.



8.6. Sécurité et maintenance

(Des sauvegardes régulières garantissent que tu peux restaurer tes données en cas de problème. Vérifier les mises à jour de Nextcloud garantit que tu restes protégé contre les nouvelles vulnérabilités.)

54. **Effectue des sauvegardes régulières** de ton serveur Nextcloud et de la base de données.
55. **Vérifie les mises à jour** de Nextcloud dans Paramètres > Administration > Mises à jour.