Nextcloud



SOMMAIRE

Installation server Web Apache2	3
·	
Configuration du pare-feu	პ
Activation PHP	5
Mettre en place le serveur MariaDB	7
Créer une base de données et des utilisateurs	9
Configurer l'hôte Apache2	11
Site web Nextcloud	13

Installation server Web Apache2

Nous allons en premier temps mettre à jour la liste des paquets disponibles et leurs versions:

#sudo apt update

```
root@debian:~# sudo apt update
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Atteint :2 http://security.debian.org/debian-security bookworm-security InReleas
e
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
```

Ainsi qu'installer apache2:

sudo apt install apache2

```
root@debian:~# sudo apt install apache2
```

On vérifie l'état de service de Apache2

systemctl status apache2

```
    apache2.service - The Apache HTTP Server
        Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled Active: active (running) since Mon 2025-03-31 11:35:00 CEST; 54s ago
        Docs: https://httpd.apache.org/docs/2.4/
        Main PID: 4195 (apache2)
```

Le serveur Apache2 est actif, en cours d'exécution et configuré pour démarrer automatiquement.

Configuration du pare-feu

Installation de notre pare-feu

Sudo apt install ufw

```
root@debian:~# sudo apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  iptables libip6tc2
Paquets suggérés :
  firewalld rsyslog
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 ufw
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 548 ko dans les archives.
Après cette opération, 3 411 ko d'espace disque supplémentaires seront utilisés.
```

Réinstallation de OpenSSH

Sudo ufw allow OpenSSH sudo ufw enable

```
root@debian:~# sudo ufw allow OpenSSH
sudo ufw enable
```

Nous autorisons les ports 80/tcp (HTTP) 443/tcp (HTTPS)

Sudo ufw allow "www full"

```
root@debian:~# sudo ufw allow "WWW Full"
Rule added
Rule added (v6)
root@debian:~#
```

relancement du parefeu

Sudo ufw reaload

```
root@debian:~# sudo ufw reload
```

Nous vérifions que nos règles se sont bien activées

Sudo ufw status

```
root@debian:~# sudo ufw status
Status: active
Τo
                         Action
                                   From
                         -----
                                    ----
0penSSH
                         ALLOW
                                   Anywhere
                        ALLOW
WWW Full
                                    Anywhere
OpenSSH (v6)
                        ALLOW
                                    Anywhere (v6)
WWW Full (v6)
                         ALLOW
                                    Anywhere (v6)
```

Activation PHP

root@debian:~#

Lancement de l'installation de PHP

sudo apt install -y php php-curl php-cli php-mysql php-gd php-common php-xml php-json php-intl php-pear php-imagick php-dev php-common php-mbstring php-zip php-soap php-bz2 php-bcmath php-gmp php-apcu libmagickcore-dev

```
root@debian:~# sudo apt install -y php php-curl php-cli php-mysql php-gd php-com
mon php-xml php-json php-intl php-pear php-imagick php-dev php-common php-mbstri
ng php-zip php-soap php-bz2 php-bcmath php-gmp php-apcu libmagickcore-dev
```

Nous allons modifier dans le fichier apache php la timezone en Europe

sudo nano /etc/php/8.2/apache2/php.ini

Modifier la data.timezone

data.timezone = Europe/Amsterdam

Nous allons aussi modifier les paramètres ; memory_limit, upload_max_filesize, post-max_size et max_execution_time ; Ces modifications permettent à PHP de gérer des scripts plus lourds et d'accepter de gros fichiers envoyés par les utilisateurs.

```
memory_limit = 512M

upload_max_filesize = 500M

post_max_size = 600M

max_execution_time = 300
```

Les valeurs file_uploads, allow_url_fopen doivent etre en statu ON et les Valeurs display_errors, output_buffering en OFF comme ceci:

```
file_uploads = On
allow_url_fopen = On
display_errors = Off
output_buffering = Off
```

Ces réglages activent l'envoi de fichiers et l'accès distant tout en désactivant l'affichage des erreurs et le tampon de sortie pour plus de sécurité et de contrôle.

Vérifiez que zend_extension=opcache est bien activé, puis ajoutez les lignes suivantes pour optimiser les performances de PHP grâce à la mise en cache des scripts

```
opcache.enable = 1

opcache.interned_strings_buffer = 8

opcache.max_accelerated_files = 10000

opcache.memory_consumption = 128

opcache.save_comments = 1

opcache.revalidate_freq = 1
```

```
GNU nano 7.2
                             /etc/php/8.2/apache2/php.ini
;extension=snmp
;extension=soap
;extension=sockets
;extension=sodium
;extension=sqlite3
;extension=tidy
;extension=xsl
;extension=zip
;zend_extension=opcache
opcache.enable = 1
opcache.interned_strings_buffer = 8
opcache.max_accelerated_files = 10000
opcache.memory_consumption = 128
opcache.save_comments = 1
opcache.revalidate_freq = 1
; Module Settings ;
                           W Chercher ^K Couper
                                                     ^T Exécuter ^C Emplacement
^J Justifier ^/ Aller ligne
^G Aide
             ^R Lire fich.^\ Remplacer ^U Coller
```

Puis redémarrer Apache2

sudo systemctl restart apache2

Mettre en place le serveur MariaDB

Nextcloud utilise un serveur MariaDB comme base de données. Vous pouvez l'installer et le vérifier avec ces commandes :

Nous allons donc installer MariaDB sur notre machine:

Sudo apt install mariadb-server

```
root@debian:~# sudo apt install mariadb-server
```

Pour vérifier que MariaDB est bien installé et est bien en marche

- # sudo systemctl is-enabled mariadb
- # sudo systemctl status mariadb

```
mariadb.service - MariaDB 10.11.11 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enabled
Active: active (running) since Tue 2025-04-01 17:31:27 CEST; 2min 30s ago
```

Si le serveur fonctionne comme prévu, procédez à la sauvegarde du système. Ensuite, utilisez la commande suivante pour définir un mot de passe root, supprimer les utilisateurs anonymes et supprimer la base de données de test:

Sudo mariadb-secure-installation

Switch to unix socket authentication

Tapez n puis sur entrée

Cela garde l'authentification par mot de passe classique.

Change the root password?

Tapez n puis sur entrée

Tu gardes le mot de passe actuel.

Remove anonymous users?

Tapez y puis appuie sur Entrée

Cela supprime les utilisateurs anonymes.

Disallow root login remotely?

Tapez n puis appuie sur Entrée

Permet à root de se connecter à distance (utile selon le contexte).

Remove test database and access to it?

Tapez y puis appuie sur Entrée

Supprime la base de données de test accessible à tous.

Reload privilege tables now?

Tapez y puis appuie sur Entrée

Recharge les tables de privilèges pour appliquer les changements.

```
root@debian:~# sudo mariadb-secure-installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
       SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.
Enter current password for root (enter for none):
OK, successfully used password, moving on...
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.
You already have your root account protected, so you can safely answer 'n'.
Switch to unix_socket authentication [Y/n] n
 ... skipping.
You already have your root account protected, so you can safely answer 'n'.
Change the root password? [Y/n] n
 ... skipping.
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
     This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.
Remove anonymous users? [Y/n] y
 ... Success!
Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? [Y/n] n
 ... skipping.
By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.
Remove test database and access to it? [Y/n] v
 - Dropping test database..
- Removing privileges on test database...
By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.
Remove test database and access to it? [Y/n] y
```

By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? [Y/n] y

- Dropping test database...

... Success!

- Removing privileges on test database...

... Success!

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? [Y/n] y

... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB installation should now be secure.

Thanks for using MariaDB! root@debian:-#

Créer une base de données et des utilisateurs

Pour vous connecter au serveur MariaDB, utilisez cette commande et saisissez votre mot de passe root:

sudo mariadb -u root -p

```
Thanks for using MariaDB!
root@debian:~# sudo mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
Utilisez les commandes suivantes pour créer une nouvelle base de données, un utilisateur
associé ainsi que son mot de passe :
CREATE DATABASE nextcloud db;
      CREATE USER nextclouduser@localhost IDENTIFIED BY 'votremotdepasse';
      GRANT ALL PRIVILEGES ON nextcloud db.* TO nextclouduser@localhost;
      FLUSH PRIVILEGES;
      QUIT;
```

```
root@debian:~# sudo mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \gray{g}.
Your MariaDB connection id is 36
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> CREATE DATABASE nextcloud_db;
Query OK, 1 row affected (0,001 sec)
MariaDB [(none)]> CREATE USER nextclouduser@localhost IDENTIFIED BY '1234';
Duery OK, 0 rows affected (0,003 sec)
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO nextclouduser@localh
Query OK, 0 rows affected (0,002 sec)
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,002 sec)
MariaDB [(none)]>
```

SHOW GRANTS FOR 'nextclouduser'@'localhost';

Ensuite, allez dans le répertoire /var/www et téléchargez le code source le plus récent :

- # cd /var/www/
- # wget https://download.nextcloud.com/server/releases/nextcloud-31.0.2.zip

```
root@debian:~# wget https://download.nextcloud.com/server/releases/nextcloud-31.
0.2.zip
--2025-04-13 18:33:23-- https://download.nextcloud.com/server/releases/nextclou
d-31.0.2.zip
Résolution de download.nextcloud.com (download.nextcloud.com)... 5.9.202.145, 2a01
:4f8:210:21c8::145
Connexion à download.nextcloud.com (download.nextcloud.com)|5.9.202.145|:443... co
nnecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 266316946 (254M) [application/zip]
Sauvegarde en : « nextcloud-31.0.2.zip.1 »
nextcloud-31.0.2.zi 100%[===========] 253,98M 30,7MB/s
                                                                   ds 7,4s
2025-04-13 18:33:31 (34,2 MB/s) — « nextcloud-31.0.2.zip.1 » sauvegardé [2663169
46/266316946]
root@debian:~#
```

Une fois l'étape précédente terminée, décompressez le fichier, puis attribuez le répertoire à l'utilisateur www-data pour qu'il en ait la gestion:

unzip nextcloud.zip

Ensuite, changez le propriétaire du dossier afin que le serveur web puisse y accéder correctement :

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

Configurer l'hôte Apache2

Nous allons maintenant configurer un hôte virtuel Apache2. Pour cela, ouvrez le fichier de configuration avec la commande suivante :

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

Le fichier devrait ressembler à ceci :

```
<VirtualHost *:80>
```

ServerName nextcloud."votre.IP"(dans le cas de cette procédure: 192.168.208.219)

DocumentRoot /var/www/nextcloud/

```
# log files

ErrorLog /var/log/apache2/files.192.168.208.219-error.log

CustomLog /var/log/apache2/files.192.168.208.219-access.log combined

<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>

</VirtualHost>
```

```
/etc/apache2/sites-available/nextcloud.conf *
 GNU nano 7.2
<VirtualHost *:80>
    ServerName 192.168.208.219
    DocumentRoot /var/www/nextcloud/
   # log files
   ErrorLog /var/log/apache2/files.192.168.208.219-error.log
   CustomLog /var/log/apache2/files.192.168.208.219-access.log combined
    <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>
</VirtualHost>
```

Une fois les modifications enregistrées, quittez l'éditeur. Ensuite, activez la configuration en utilisant la commande suivante, puis vérifiez qu'elle fonctionne correctement :

- # sudo a2ensite nextcloud.conf
- # sudo apachectl configtest

Si le message « syntaxe OK » apparaît, redémarrez Apache2 pour appliquer la nouvelle configuration de l'hôte virtuel :

sudo systemctl restart apache2

Site web Nextcloud

En entrant http://[votre-ip] nous allons pouvoir configurer notre Nextcloud



Nous choisirons Calendrier pour planifier les rendez-vous, Contacts pour l'annuaire des salariés, et Talk pour la messagerie instantanée.



Et voilà, notre Nextcloud est prêt!

