Installation et configuration de Nextcloud :

Au sein de notre projet nous devions trouver une équivalence à Dropbox, pour centraliser et contrôler les données de la clinique en interne. Nous avons choisi Nextcloud.

NextCloud permet de garder sous contrôle ses données et l'ensemble peut être relié à un serveur LDAP (Synchronisation avec notre Active Directory). Le partage de lien, la réplication inter-nextcloud et d'autres fonctionnalités présentent NextCloud comme l'une des meilleures alternative.

Installation des pré-requis :

Nous commencerons par installer paire par paire nos paquets :

```
apt-get install apache2 mariadb-server libapache2-mod-php5
```

```
apt-get install php5-gd php5-json php5-mysql php5-curl
```

```
apt-get install php5-intl php5-mcrypt php5-imagick
```

MariaDB

A l'installation de maria-server, nous avons dû créer un mot de passe root pour nous authentifier.

Nous l'utilisons pour nous connecter à la base de donnée :

```
mysql -u root -p
```

Créons la base "nextcloud" avec le compte "nextcloud" et le mot de passe : "monpassword" :

```
CREATE DATABASE IF NOT EXISTS nextcloud;
```

```
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost' IDENTIFIED BY 'monpassword';
```

Nous quittons désormais MariaDB :

```
quit
```

Nous avons configuré notre base de donnée MariaDB pour NextCloud (autre serveur de base de donnée compatible).

Apache2

Le serveur web a besoin d'être modifié :

```
nano /etc/apache2/sites-available/000-default.conf
```

Modifiez la ligne "DocumentRoot" en :

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

Le chemin par défaut sur lequel pointera notre serveur web sera dans le dossier "nextcloud". (Afin de le rendre visible sur une page web).

Installation de NextCloud :

Téléchargez NextCloud au format .zip :

```
wget https://download.nextcloud.com/server/releases/nextcloud-13.0.4.zip
```

Unzip est un programme à rajouter sur votre distribution Debian :

```
apt-get install unzip
```

Dézippez NextCloud :

```
unzip nextcloud-13.0.4.zip
```

Renommez le répertoire :

```
mv nextcloud-13.0.4.zip nextcloud
```

Copiez-le ensuite vers l'emplacement "/var/www/" :

```
cp -r nextcloud /var/www/html/
```

Donnez les droits à l'utilisateur et au groupe www-data au répertoire nextcloud :

```
chown -R www-data:www-data nextcloud
```

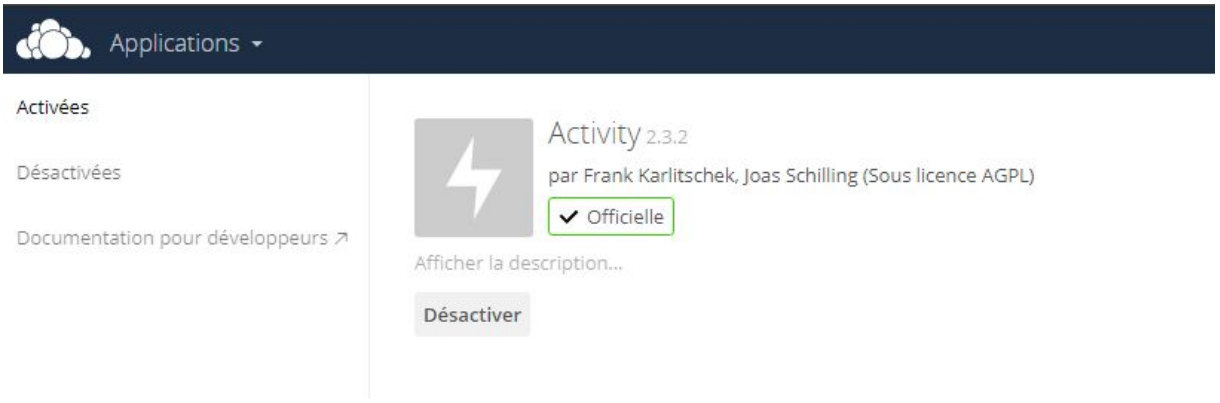
Configuration de NextCloud

Pour configurer notre nextcloud, rendons nous sur l'adresse IP du serveur dans notre cas :

http://172.17.252.70/nextcloud

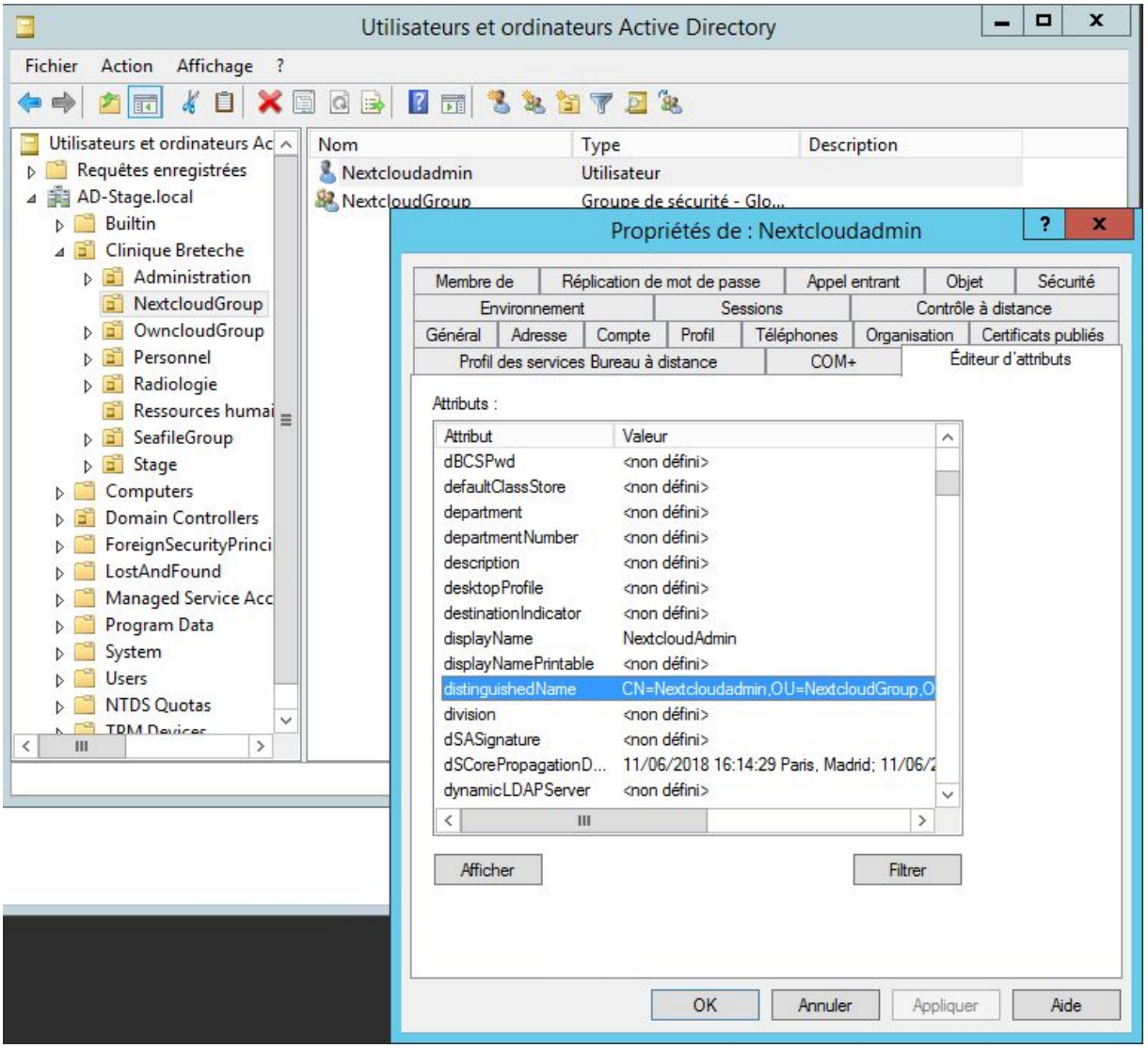
Nous avons besoin de notre nom d'utilisateur dans notre cas Localhost (l'admin du nextcloud), d'un mot de passe sécurisé.

Nous retrouvons en bas les paramètres d'identification de la base de données précédemment créée (MariaDB). Une fois tous les champs remplis, cliquez sur "Finish Setup" pour se connecter au Nextcloud.



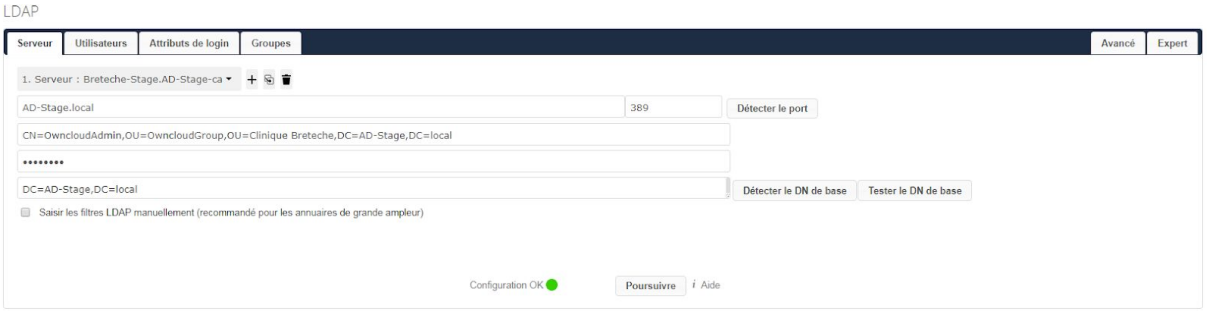
Allez dans le menu “Applications” en haut à gauche et activez tous les services qui sont désactivés dont le service LDAP pour se connecter à l’Active Directory.

Récupération du chemin pour connecter nextcloud à l’AD :

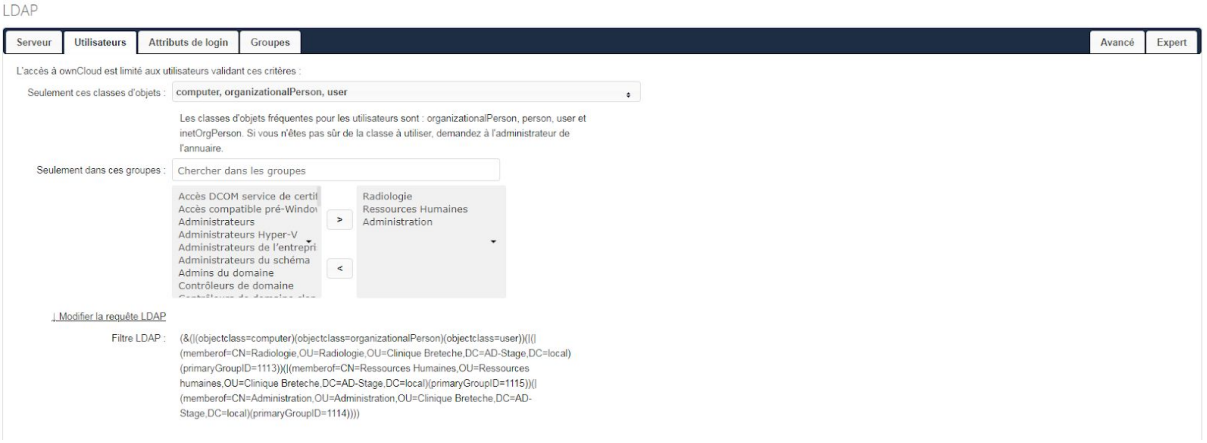


Le **DN** (*Distinguished Name*) d'un objet est un moyen d'identifier de façon unique un objet dans la hiérarchie. Un DN se construit en prenant le nom relatif de l'élément (RDN -*Relative Distinguished Name*), et en lui ajoutant l'ensemble des noms relatifs des entrées parentes. Le DN d'un élément est donc la concaténation de l'ensemble des RDN de ses ascendants hiérarchiques.

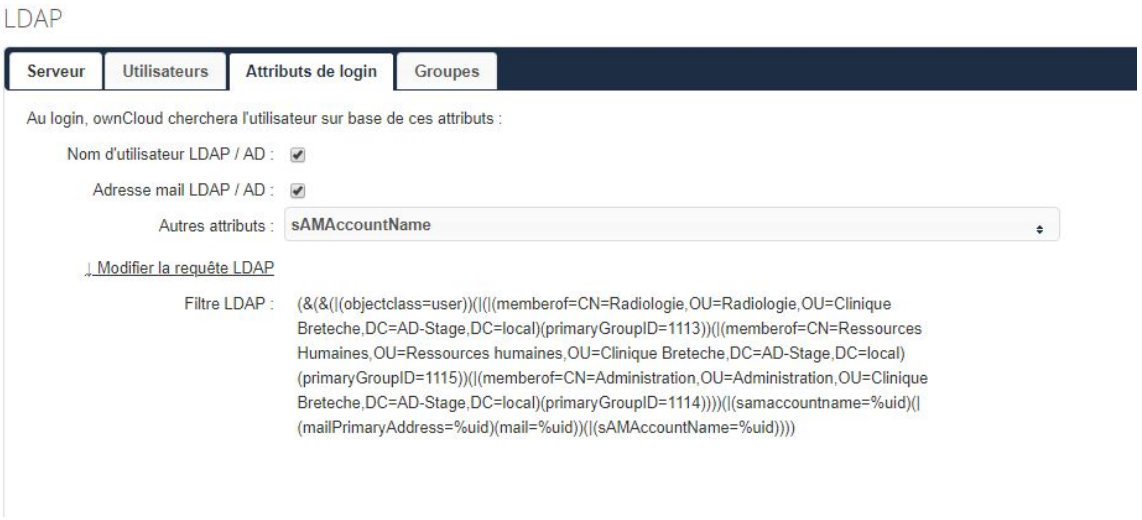
Connection à l'AD depuis nextcloud :



Nous avons ensuite autorisé l'accès à certains groupes d'utilisateurs :

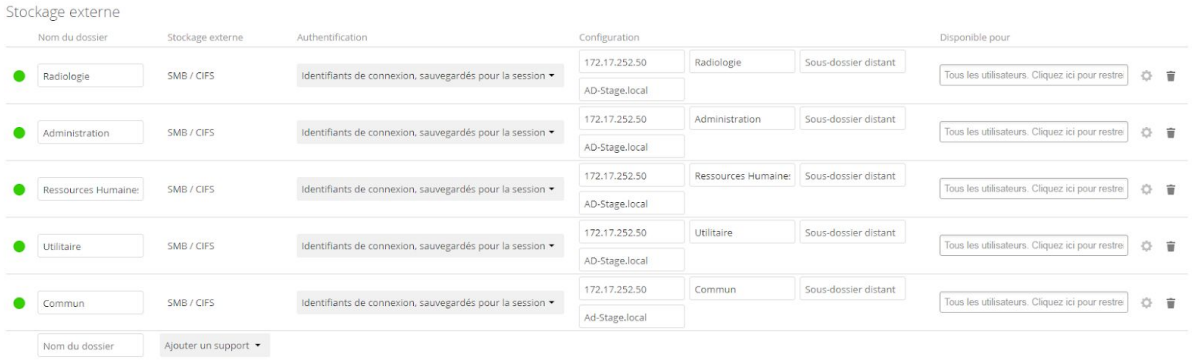


Dans "Attributs de login" ne pas oublier de cocher les cases "Nom d'utilisateur LDAP / AD :" et "Adresse mail LDAP / AD :" afin que les informations de connexion comme l'identifiant soit synchronisé

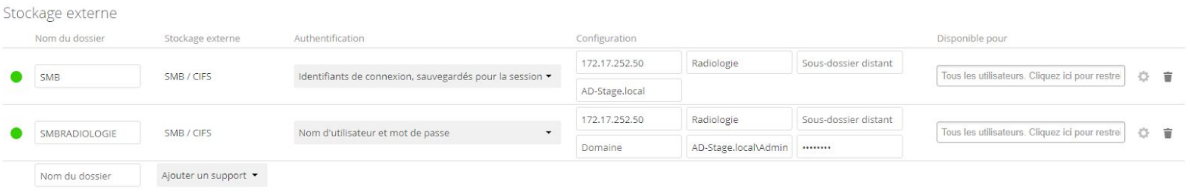


Le filtre suivant recherche des entrées dont l'attribut ID utilisateur sAMAccountName correspond à l'ID utilisateur qui a été utilisé pour se connecter au système. Ce filtre ne recherche que les entrées contenues dans les classes d'objets organizationalPerson et person.

Nous avons configuré le stockage externe, cela nous a permis de récupérer tous les dossiers partagés du Windows Server 2012 :



Les erreurs à ne pas faire:

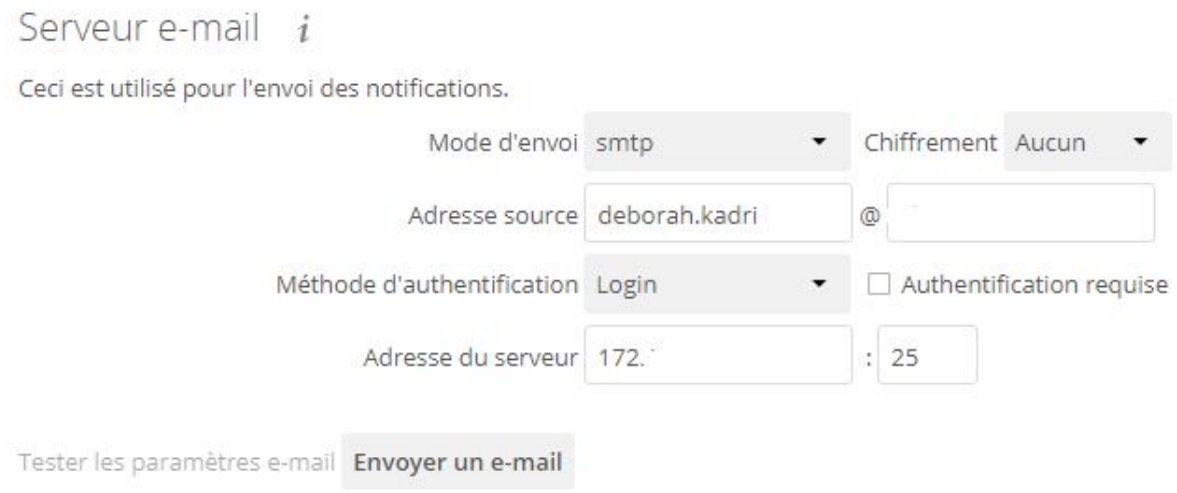


SMB: Dans ce premier cas, lorsque l'on choisi l'authentification "Identifiant de connexion, sauvegardés pour la session" les identifiants de connexion pour se connecter à nextcloud seront utilisés pour se connecter aux dossiers du domaine, les autorisations d'accès seront alors conservées. (Ce que nous voulons en terme de sécurité et de protection des données).

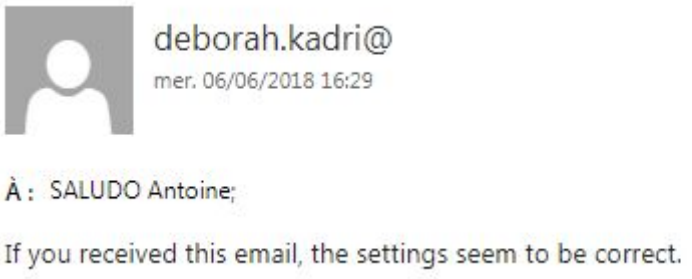
SMBRADIOLOGIE: Dans le cas second, si l'on choisit le mode d'authentification "Nom d'utilisateur et mot de passe" nous devons rentrer les identifiants pour accéder au fichier ce qui va alors donner les droits de ce compte à tous les utilisateurs. En effet, pour accéder à ce fameux dossier ils prendront les identifiants entrés dans la configuration. (pas de protection des données).

Nous pouvons voir que nos dossiers ont bien été synchronisés via l'AD:

Nous avons ensuite configuré le serveur de notification par mail:



Lors du test des paramètres le mail a bien été reçu:



Nous allons maintenant sécuriser notre nextcloud afin d'enlever les messages qui concerne la sécurité:

Comment créer un certificat SSL ?

Nous allons maintenant procéder à la mise en plus de notre page en HTTPS. Pour se faire, nous avons besoin d'un certificat SSL.

Le paquet openssl doit être installé par la commande :

```
sudo apt-get install openssl
```

Allons dans le répertoire /etc/ssl et créons la clé :

```
cd /etc/ssl
sudo openssl genrsa -out server.key 2048
```

Ensuite il faut générer un fichier de « demande de signature de certificat », en anglais CSR : Certificate Signing Request :

```
sudo openssl req -new -key server.key -out server.csr
```

Nous devions répondre à plusieurs questions. Nous avons mis notre nom de notre serveur (stagecloud.clinique-breteche.fr).

```
openssl req -text -noout -in server.csr
```

Nous récupérons le certificat auto-signé pour 1 an :

```
sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Nous avons été dans le fichier configuration default-ssl.conf :

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin stagecloud.clinique-breteche.fr
                ServerName stagecloud.clinique-breteche.fr
                SSLCertificateFile /etc/ssl/nextcloud/nextcloud.crt
                SSLCertificateKeyFile /etc/ssl/nextcloud/nextcloud.key
                DocumentRoot /var/www/html/nextcloud
```

Nous avons activé le module SSL avec la commande et redémarré le service apache2 :

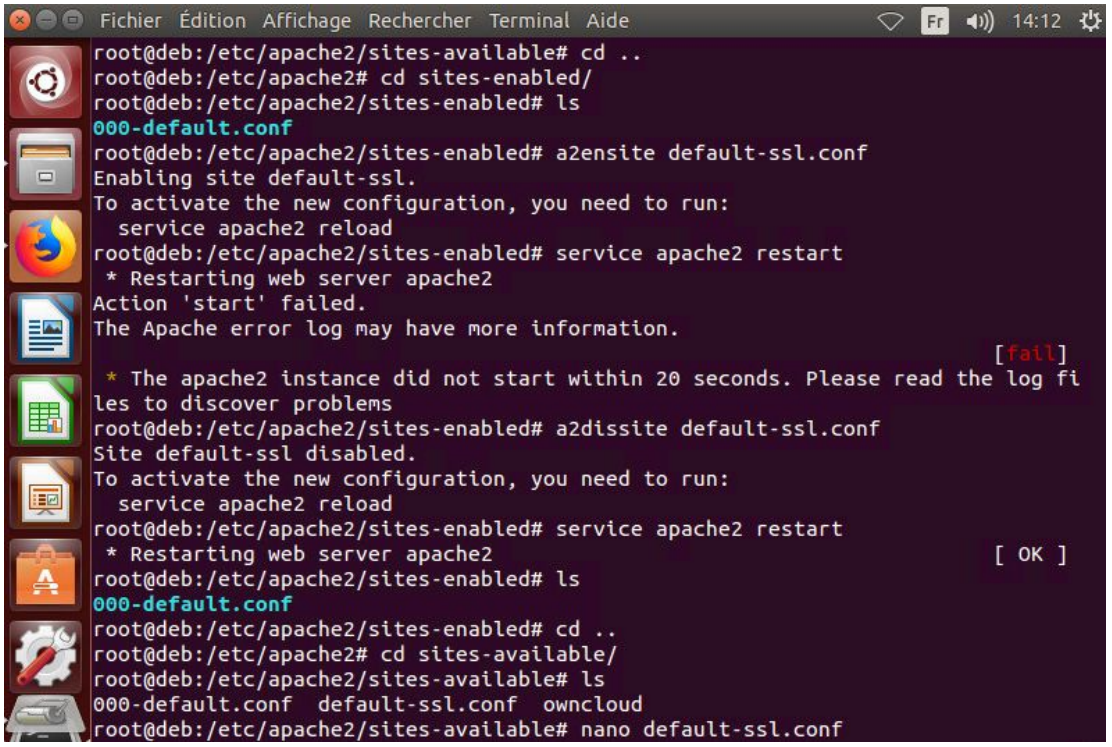
```
a2enmod ssl
```

Nous avons remarqué que notre service apache2 ne se redémarrait pas car le fichier de conf n'était pas activé et donc pas présent dans "sites-enabled" mais "sites-available". De ce fait, le module SSL ne pouvait pas s'activer.

Nous avons rentré dans "sites-enabled" la commande suivante pour activer le module SSL :

```
a2dissite default-ssl.conf
```

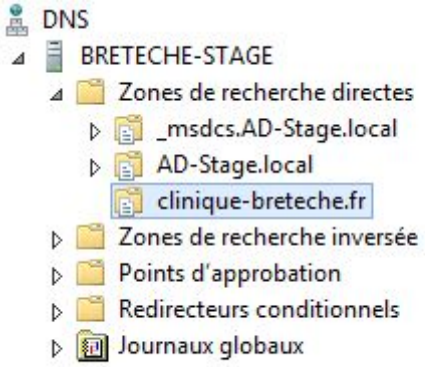
Et nous avons redémarré le service apache2, ceci nous as permis de passer notre site du protocole HTTP à HTTPS.



Ici notre service apache2 ne voulait pas redémarrer car dans le fichier default-ssl.conf car les options SSLCertificateFile et SSLCertificateKeyFile d'origines étaient non commentées alors que nous avions rajouté ces paramètres avec des valeurs personnelles.

```
root@deb:/home/deb# cd /etc/apache2/sites-available/
root@deb:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  owncloud
root@deb:/etc/apache2/sites-available# vi default-ssl.conf
root@deb:/etc/apache2/sites-available# a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@deb:/etc/apache2/sites-available# service apache2 restart
 * Restarting web server apache2                                          [ OK ]
root@deb:/etc/apache2/sites-available# vi default-ssl.conf
root@deb:/etc/apache2/sites-available#
```

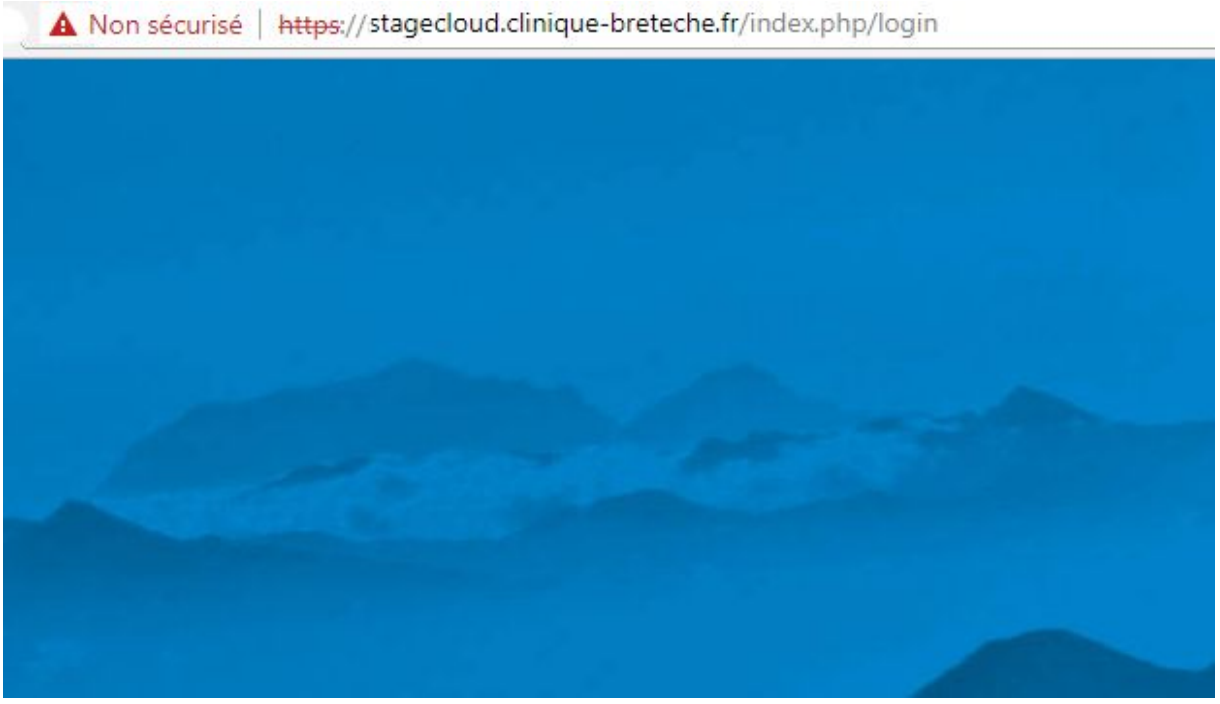
Nous avons ensuite créer une nouvelle zone de recherche directe dans le DNS, nous avons appelé cette zone clinique-breteche.fr :



Nous avons ensuite ajouté un hôte sur cette zone de recherche directe, à cet hôte nous avons donné un nom, stageloud, et son IP :

Une fois ceci effectué notre URL pour accéder au site nextcloud est passée de 172.17.252.70/nextcloud à stagecloud.clinique-breteche.fr .

Une fois notre nouvelle connexion sur le site nous pouvons voir que notre site est passé de http://172.17.252.70/nextcloud à https://stagecloud.clinique-breteche.fr



Le certificat est auto-signé et il déclenche des alertes de sécurité sur la plupart des serveurs web car il n'a pas été vérifié par une autorité de certification de confiance. Malgré cela, notre serveur web est bel et bien protégé.