

BTS SIO 2025

Support & mise à disposition de service informatique

(E5)

PAGE DE PRÉSENTATION DU DOSSIER

N° d'inscription¹ : **2444891196**

NOM :DIALLO.....

PRENOM :Kadiatou Laetitia-Marie.....

date de passage ¹ : 12/06/2025	Heure de passage ¹ : 8h00
---	--------------------------------------

ÉTABLISSEMENT DE PASSAGE
LYC ECOLE NATIONALE DE COMMERCE 70 BOULEVARD BESSIERES 75017 PARIS

CATEGORIE CANDIDAT ² (UNE CASE A COCHER)	
<ul style="list-style-type: none">- Scolaire- <input checked="" type="checkbox"/> Apprentie- Formation professionnelle continue- Expérience professionnelle 3 ans	<ul style="list-style-type: none">• Ex-scolaire• Ex-apprenti• Ex-formation professionnelle continue

¹ Informations communiquées sur votre convocation envoyée courant mars 2024 sur votre compte **Cyclades**

² Informations communiquées sur votre confirmation d'inscription.

Tampon de L'établissement

SIEC – maison des examens

7 rue Ernest Renan 94749
ARCUEIL CEDEX
Tél : 01 49 12 23 00



Plan de la situation

Le cahier des charges.....	3
L'expression des besoins.....	3
La description de l'existant.....	3
L'analyse des choix.....	3
Les offres du marché.....	4
Le choix de la différence avec une solution open source.....	4
Mise en œuvre.....	5
Installation d'un serveur web avec« LAMP ».....	5
Installation de OwnCloud 6.....	7

Le cahier des charges

L'expression des besoins

Une entreprise souhaite renforcer la sécurité des données et des ressources informatiques en implémentant un système de **Listes de Contrôle d'Accès (ACLs)**. L'objectif est de garantir que seules les personnes autorisées aient accès aux informations sensibles et aux ressources critiques, tout en permettant une gestion fine des droits d'accès pour chaque utilisateur ou groupe d'utilisateurs.

La description de l'existant

L'entreprise utilise actuellement un système de gestion des accès basé principalement sur des permissions simples attribuées au niveau des fichiers et répertoires, sans recours aux Listes de Contrôle d'Accès (ACLs). L'accès aux ressources informatiques (fichiers, répertoires, applications) est principalement géré via des mécanismes d'authentification basés sur des utilisateurs et des groupes, mais sans granularité spécifique concernant les droits d'accès à des fichiers ou répertoires particuliers.

L'analyse des choix

L'objectif de cette analyse est d'évaluer les différentes solutions disponibles pour implémenter un système de gestion des droits d'accès basé sur les ACLs, tout en répondant aux besoins spécifiques identifiés dans la description de l'existant. Cela inclut la sécurité, la granularité des permissions, la facilité de gestion et l'intégration avec l'infrastructure existante.

Offres du marché

Solution	Fonctionnalités clés	Avantages	Limites	Coût
Windows ACLs (NTFS)	Gestion des droits détaillés (lecture, écriture, exécution), intégration avec Active Directory.	Solution intégrée, interface graphique conviviale, support natif dans Windows.	Limité aux environnements Windows, nécessite des connaissances sur les permissions NTFS.	Inclus (Windows).
ACLs POSIX	Gestion des	Gratuit, intégré	Interface en	Inclus (Linux).

(Linux)		droits (rwx) pour utilisateurs et groupes via setfacl et getfacl.	dans Linux, flexible.	ligne de commande, complexité accrue dans des environnements hétérogènes.	
FreeIPA (Open Source)		Centralisation des utilisateurs et ACLs, intégration Kerberos, interface web.	Gratuit, adapté aux environnements Linux, gestion centralisée avancée.	Complexité d'installation et de configuration, moins adapté à Windows.	Gratuit.
OpenLDAP		Gestion des ACLs avec centralisation des permissions, extensible avec d'autres outils open-source.	Flexible, mature, support communautaire actif.	Configuration complexe, principalement en ligne de commande.	Gratuit.
AWS IAM		Gestion des rôles et des politiques d'accès, contrôle d'accès aux services AWS via JSON.	Granularité élevée, intégration native avec AWS, évolutif.	Limité à AWS, nécessite des compétences spécifiques pour écrire les politiques JSON.	Payant (usage).
Azure Active Directory (AAD)		Gestion des accès cloud et sur site, contrôle basé sur les rôles (RBAC), intégration avec les services Microsoft.	Intégré avec les services Microsoft, gestion unifiée, support avancé.	Dépendance à Azure, coût variable.	Payant (usage).
Google Cloud IAM		Gestion des permissions sur Google Cloud, contrôle basé sur les rôles et les ACLs.	Simplicité d'utilisation, intégration avec Google Cloud, bonne granularité.	Limité aux environnements Google Cloud.	Payant (usage).

Le choix de la différence avec une solution open source

Les **Windows ACLs (Access Control Lists)**, intégrées au système de fichiers **NTFS (New Technology File System)**, permettent de gérer précisément les droits d'accès aux fichiers, dossiers et autres ressources dans un environnement Windows. Elles offrent un contrôle détaillé pour les utilisateurs et groupes, intégrées avec Active Directory pour une gestion centralisée.

Mise en œuvre

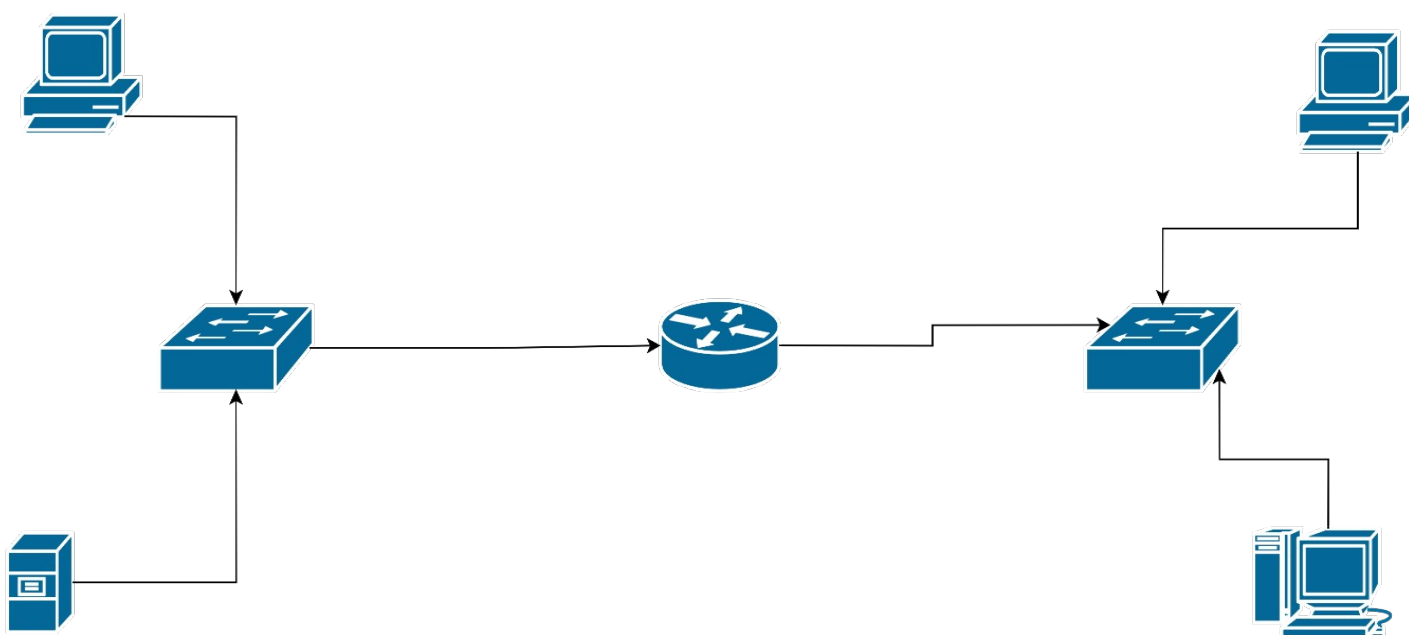
La mise en œuvre des **ACLs (Access Control Lists)** dans **Cisco Packet Tracer** permet de simuler le filtrage et le contrôle du trafic réseau en configurant des routeurs et des commutateurs. Voici un guide étape par étape pour mettre en place des ACLs sur Cisco Packet Tracer.

Scenario

Réseau 1 : Le réseau des employés, où chaque poste de travail a une adresse IP unique (par exemple, 192.168.1.10).

Réseau 2 : Le réseau réservé aux serveurs, où se trouve un serveur d'applications critiques utilisé pour la gestion des projets (adresse IP en 2: 192.168.2.10).

L'objectif est de **limiter les accès au serveur** de manière stricte, car il contient des informations sensibles et stratégiques pour l'entreprise. **Seul le poste de travail du responsable des projets, situé dans le Réseau 1, doit pouvoir accéder à ce serveur.**



Chaque pc représente ici un département spécifique de l'entreprise :

PC	Département	Rôle	Accès réseau autorisé	Restrictions
PC1	Ressources Humaines	Gestion des employés	Serveur RH uniquement	Bloqué pour les données financières.
PC2	Comptabilité	Gestion des finances	Serveur financier uniquement	Bloqué pour les données RH.
PC3	Informatique (IT)	Maintenance du réseau	Accès complet au serveur et gestion du réseau	Pas de restrictions.
PC4	Marketing ou Commercial	Relation client et projets	Serveur marketing ou CRM	CRM Bloqué pour les données RH et financières.

Cette structure simplifie l'administration des ACLs tout en assurant la séparation des responsabilités et la sécurité des données.

Mise en place du serveur DHCP

Le serveur DHCP attribue automatiquement des adresses IP aux appareils dans chaque département. Cela simplifie la gestion des adresses IP et garantit que chaque appareil obtient une adresse sans conflit. Cependant, Lorsqu'un réseau est divisé en VLANs, chaque VLAN agit comme un sous-réseau distinct, ce qui nécessite une configuration spécifique pour que le serveur DHCP puisse attribuer des adresses IP à chaque VLAN. Telle est le cas dans notre réseau.

La première étape consiste à attribuer une adresse IP statique au serveur, afin qu'il puisse distribuer correctement les adresses IP aux autres appareils du réseau. Pour ce faire, effectuez un clic droit sur le serveur, accédez à l'onglet **Desktop**, puis configurez les paramètres réseau en saisissant l'adresse IP, le masque de sous-réseau et la passerelle par défaut (gateway).

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.254

DNS Server: 0.0.0.0

Ajout des VLANs

Une fois cela fait, accédez à l'onglet **Services**, où il faudra configurer tous les sous-réseaux présents dans le réseau (VLAN).

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☐ On ☒ Off

Pool Name: Vlan 3

Default Gateway: 192.168.3.254

DNS Server: 0.0.0.0

Start IP Address: 192.168.3.0

Subnet Mask: 255.255.255.0

Maximum Number of Users: 256

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add, Save, Remove

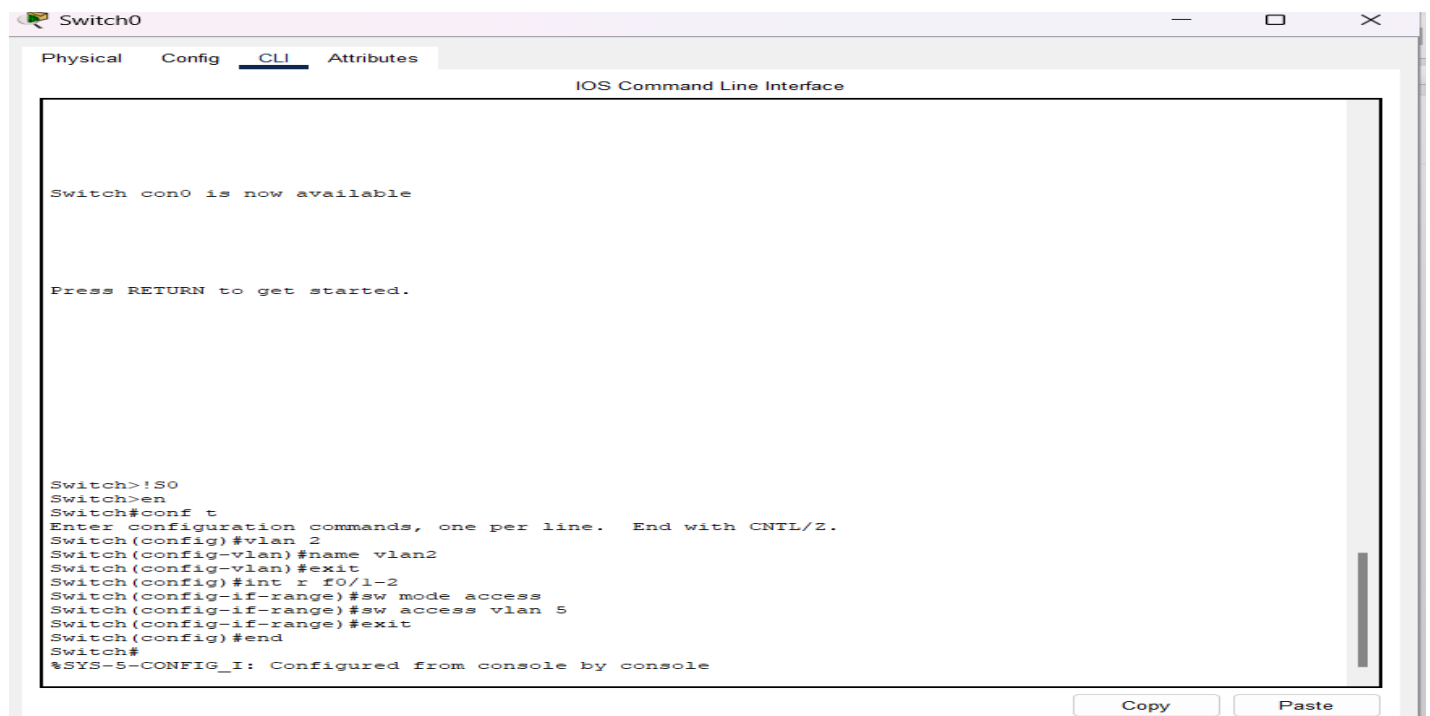
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Vlan 3	192.168.3.254	0.0.0.0	192.168.3.0	255.255.255.0	256	0.0.0.0	0.0.0.0
Vlan 2	192.168.2.254	0.0.0.0	192.168.2.0	255.255.255.0	256	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

Configuration des Switchs

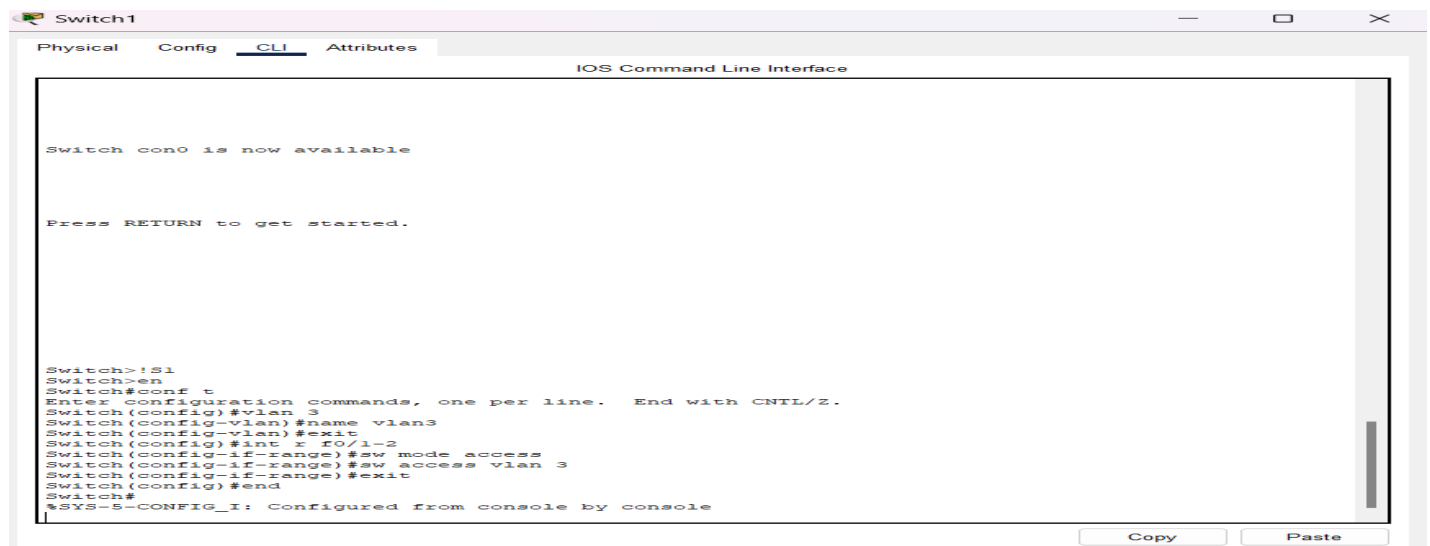
On configure les switchs en saisissant les lignes de commandes suivantes dans l'interface CLI :

```
!S0
en
conf t
vlan 2
name vlan2
exit
```

```
int r f0/1-2
sw mode access
sw access vlan 5
exit
end
```



On refait la même opération pour l'autre switch



Configuration de routeur

Apache

Après l'installation, nous lançons mysql de la façon suivante : mysql

```
-u root -p
```

```
Enter password : *****
```

Ensuite, nous allons simplement créer un utilisateur, une base avec l'accès à notre utilisateur :

```
CREATE DATABASE owncloud;  
CREATE USER 'ownclouduser'@'localhost' IDENTIFIED BY 'p4ssw0rd' GRANT  
ALL PRIVILEGES ON owncloud.* TO ownclouduser'@'localhost';
```

OU

```
CREATE USER 'ownclouduser'@'localhost' IDENTIFIED BY 'p4ssw0rd';  
CREATE DATABASE IF NOT EXISTS owncloud;  
GRANT ALL PRIVILEGES ON owncloud.* TO ownclouduser'@'localhost' IDENTIFIED BY 'p4ssw0rd';
```

PHP-5

Pour que notre serveur comprenne le langage de programmation PHP il faut lui installer la version 5 et quelques dépendances :

```
apt-get install php5 php5-common php5-gd
```

Nous avons terminé l'installation du serveur web sous lamp, owncloud peut enfin être mis en place.

Installation de OwnCloud 6

Owncloud est une plateforme d'hébergement et de stockage libre. Il permet de synchroniser des fichiers sur un serveur afin de les partager sur plusieurs équipements comme le fait Dropbox et de partager les dossiers à d'autres utilisateurs ou de générer des liens publics avec une durée limitée dans le temps si nécessaire. Ses principaux avantages sont :

-Vous n'êtes pas soumises aux licences ou changement de licences sur les fichiers que vous déposez en ligne. Certains services s'approprient les fichiers mis en ligne.

-Pas d'espionnage ou de pistage utilisateurs. Avec Owncloud vous gérez vos propres serveurs ce qui permet de choisir la localisation et donc la législation qui va avec. Vous limitez la récupération de données à des fins marketing ou l'espionnage industrielle..

-Maîtrise des données. Vous ne passez pas par un serveur tiers et donc vous maîtrisez entièrement vos données.

-Moins onéreux. Le coût de stockage au To est moins onéreux pour un service d'hébergement personnelle. Il faut toutefois prendre en compte le coût de la maintenance.

Afin de pouvoir récupérer owncloud, il nous faut le dépôt de owncloud dans notre source.list :

```
echo 'deb http://download.opensuse.org/repositories/isv:/ownCloud:/community/
Debian_7.0/ /' >> /etc/apt/sources.list.d/owncloud.list
```

Il est conseillé de récupérer la clé du dépôt pour éviter des problèmes et de l'ajouter à linux :

```
wget
http://download.opensuse.org/repositories/isv:/ownCloud:/community/Debian_7.0/Release.key
apt-key add - < Release.key
```

Puis, on lance une synchronisation des dépôts de notre source.list :

```
apt-get update
```

Ensuite nous installons owncloud :

```
apt-get install owncloud
```

L'installation est rapide, ensuite il faut se rendre dans le répertoire de owncloud et définir le groupe **“wwwdata”** en tant que groupe propriétaire sur les répertoires utiles au fonctionnement d'ownCloud :

```
cd /var/www/owncloud
mkdir data
chgrp www-data data -R
chgrp www-data config -R
chgrp www-data apps -R
```

Modification des permissions sur les différents répertoires (avec récursivité)

```
chmod 770 data -R
chmod 770 config -R
chmod 770 apps -R
```

Activons les modules rewrite et headers d'Apache2 :

Le Rewrite permet la réécriture d'URL, et, headers permet de gérer les en-têtes des requêtes/réponses HTTP.

```
a2enmod rewrite
a2enmod headers
```

Modifier notre « DocumentRoot » et « Directory » dans notre vhost par défaut d'Apache2 :

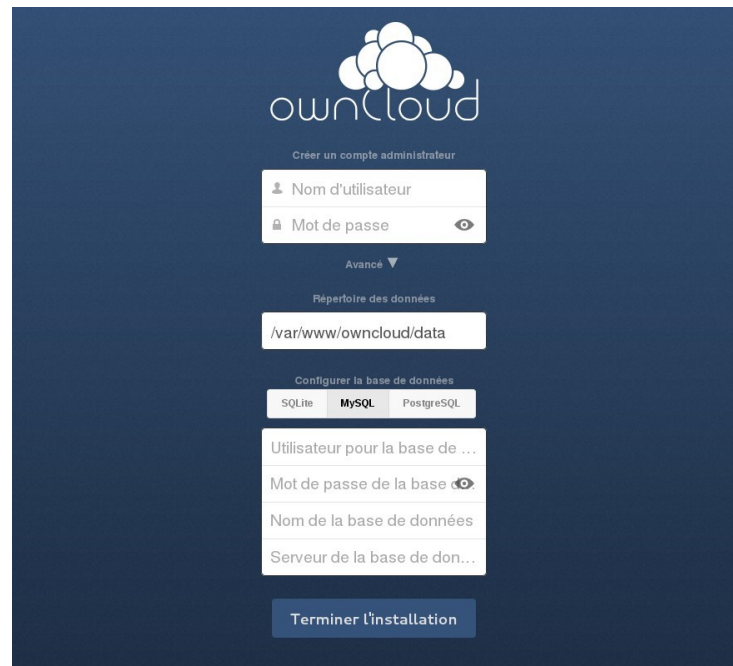
Le serveur web pointe désormais par défaut dans le repertoire de owncloud.

```
nano /etc/apache2/sites-available/default
DocumentRoot /var/www/owncloud/
Directory /var/www/owncloud/
```

Pour terminer l'installation de notre owncloud, nous redémarrons notre serveur Apache2 :

```
/etc/init.d/apache2 restart
```

Le serveur Owncloud est désormais accessible, et fonctionnel via son adresse IP ou son nom DNS :

The image shows the OwnCloud installation wizard on a dark blue background. At the top is the OwnCloud logo. Below it, the text "Créer un compte administrateur" is displayed. There are two input fields: "Nom d'utilisateur" and "Mot de passe" with an eye icon for toggling visibility. Below these is an "Avancé" dropdown menu. The next section is "Répertoire des données" with a text input field containing "/var/www/owncloud/data". Below that is "Configurer la base de données" with three radio buttons: "SQLite", "MySQL" (which is selected), and "PostgreSQL". There are four more input fields: "Utilisateur pour la base de ...", "Mot de passe de la base" (with an eye icon), "Nom de la base de données", and "Serveur de la base de don...". At the bottom is a blue button labeled "Terminer l'installation".

Désormais OwnCloud apparaît avec son Nuage blanc, il nous permet de créer un compte administrateur :

- ffonaisak
- p4ssw0rd

Laissons le repertoire par défaut pour les données : `/var/www/owncloud/data`

La configuration de la base de données est bien "MySQL"

Les derniers champs ont été précédemment configurés dans notre base de données MySQL :

- ownclouduser
- p4ssw0rd
- owncloud
- 127.0.0.1

Après avoir cliqué sur : « Terminer l'installation », nous voici connecté à Owncloud :

