

Déploiement de ownCloud à la DT/INSU

Zouhir Hafidi

Division Technique de l'INSU La Seyne sur Mer

26 mars 2013

Pouvoir retrouver mes données et y accéder :

- A tout moment, quand j'en ai besoin
- De n'importe où
- Avec n'importe quel moyen
- Depuis un endroit unique
- De manière simple et flexible
- Aucune concession sur l'efficacité, la sécurité, la confidentialité, etc.

Solution : le Cloud

- Solution permettant un accès universel à ses fichiers via une interface web ou WebDAV
- Alternative open source à Dropbox & Cie
- « self hosted » donc pas de problèmes de confidentialité
- Projet initié en janvier 2010 par la communauté KDE (Frank Karlitschek), Développement actif
- Entité commerciale annoncée le 13 décembre 2011
- Ecrit en PHP / Javascript, supporte SQLite ou MySQL dans sa version community
- Multiplate-forme, Multilingue, AGPLv3

- Synchronisation de fichiers entre différents ordinateurs
- Stockage sécurisé
- Partage de fichiers entre utilisateurs ou publiquement
- Lecteur de musique en ligne
- Serveur de fichiers WebDAV
- Calendrier (CalDAV), Gestionnaire de Contacts (CardDAV)
- Éditeur de texte en ligne (proposant la coloration syntaxique)
- Visionneuse de documents en ligne (pdf, open document)
- Galerie d'images, qui permet de visualiser ses photos et de les classer en albums
- Drag and Drop dans l'interface web

- Stockage externe (montage Dropbox, etc.)
- Thématisation
- Restauration de fichiers effacés (Undelete)
- Moteur de recherche lucene (recherche sur noms et contenus de fichiers)
- Versionning
- Tâches, bookmarks, etc.
- Gestion des utilisateurs et des groupes (LDAP, AD)
- API publique
- Applications ownCloud (<http://apps.owncloud.com>)
- Infrastructure as a Service (IaaS)

	Community Edition	Business Edition	Enterprise Edition
ownCloud AGPL	✓	✓	✓
ownCloud licensed ⓘ	✗	✗	✓
Proprietary plug-in extensions	✗	✗	✓
Maintenance and Upgrades	✗	✓	✓
Certified by ownCloud Inc.	✗	✓	✓
Support	Community Forums only	via email	via email or phone
Support times	✗	5 days per week, business hours 9AM-6PM (US or GER)	5 days per week, 12 hours a day business hours 8AM-8PM (US or GER)
Reaction time	no SLA	1 business day	4 hours
Instances ⓘ	unlimited	Limited to one instance	Option for additional instances
Mobile Apps available	✓	✓	✓
Support for Mobile Clients	✗	✓	✓
Desktop Clients available	✓	✓	✓
Support for Desktop Clients	✗	✓	✓
Oracle Support ⓘ	✗	✓	✓
Logging Module ⓘ	✗	✓	✓
Dynamic User Storage ⓘ	✗	✗	✓
Unlimited number of incidents ⓘ	✗	✗	✓
Feature requests to ownCloud	✗	✗	✓
HA/Replication ⓘ	Yes, but unsupported/No	✗	✓
Branding	Web UI	Web UI	Web UI Optional for Desktop Clients and Mobile Apps
	more information	more information	more information

Demandes récurrentes de la part des utilisateurs :

- Pour les données stockées sur nos serveurs :
 - difficulté d'y accéder depuis l'extérieur (tunnels SSH, VPN, etc.)
- Pour les données stockées sur les portables :
 - pouvoir disposer d'un espace pour sauvegarder ses données afin de les retrouver en cas de perte, de vol ou de panne du portable
 - dépendance vis à vis du portable pour pouvoir accéder à ses données (pas de portable entre les mains = pas d'accès à ses données)

Mises en garde du service du FSD (Utilisation des ordinateurs portables et autres outils informatiques à l'étranger)

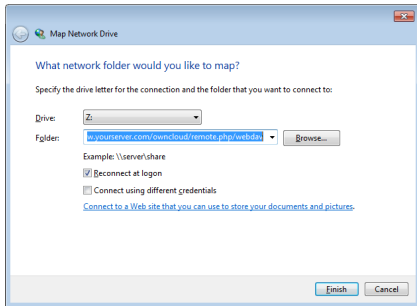
- Faire du cloud l'espace principal/unifié des répertoires de base des utilisateurs (données professionnelles uniquement)
- Offrir des fonctionnalités supplémentaires (partage, agenda, contacts, bookmarks, etc.)
- Recommandation : garder les données en local sur le portable en les couplant avec l'outil de synchronisation ownCloud (disponibilité, sauvegarde). La synchronisation se faisant dans les deux sens.

<https://owncloud.dt.insu.cnrs.fr>

- Interface web
- Accès, partage, synchronisation
- Versionning, undelete
- Couplage avec un stockage externe (Dropbox)
- Agenda, contacts, bookmarks, tâches, etc.

Côté client : accès WebDAV Windows

- En ligne de commande : `net use Z : https://owncloud.dt.insu.cnrs.fr/remote.php/webdav /user:youruser yourpassword /persistent`
- KB841215



- Via l'explorateur :
- En utilisant un logiciel tiers type cyberduck

- Dans Finder : Go > Connect to Server
- [https ://owncloud.dt.insu.cnrs.fr/files/webdav.php](https://owncloud.dt.insu.cnrs.fr/files/webdav.php)

- KDE/Dolphin : Add a Network Folder
- WebDAV
- Server = owncloud.dt.insu.cnrs.fr et Folder = /files/webdav.php

- GNOME/Nautilus : Connect to Server
- Secure WebDAV (HTTPS)
- Server = owncloud.dt.insu.cnrs.fr et Folder = remote.php/webdav

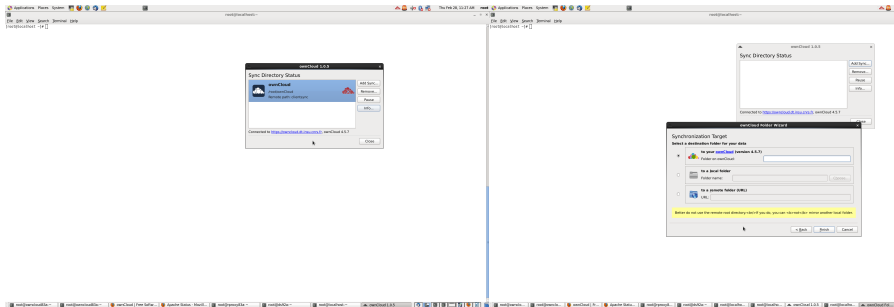
Côté client : accès WebDAV Linux (suite)

- Avec mount en tant que root : installer le package davfs2
- Mettre la chaîne terena (terena.pem) dans /etc/davfs2/certs/ (déplacer la troisième partie en tête du fichier sinon ça ne marche pas)
- Dans /etc/davfs2/davfs2.conf : servercert
/etc/davfs2/certs/terena.pem
- mount -t davfs
https://owncloud.dt.insu.cnrs.fr/remote.php/webdav/
/mnt/tmp/

- Avec mount en tant que user il faut passer par /etc/fstab
- https://owncloud.dt.insu.cnrs.fr/remote.php/webdav/
/home/user/webdav davfs rw,user,noauto 0 0
- En tant que root : usermod -aG davfs2 user
- mount /home/user/webdav
- Possibilité de mettre les credentials dans ~/.davfs2/secrets

- Mirall : Linux et Windows, portage Mac OS en cours
- <https://owncloud.org/sync-clients/>
- Possibilité de configurer plusieurs synchronisations
- Pour chaque synchronisation préciser un répertoire source et un répertoire destination
- La synchronisation se fait dans les 2 sens
- Méthode de synchronisation (server ≥ 4.5 et client ≥ 1.1) : File ID + Time Stamp
- Options - -logwindow, - -logfile
- $\sim/.local/share/data/ownCloud/$ et $\sim/.csync/$

Côté client : Synchronisation (suite)



- iOS : application iPhone et iPad, testée OK
- Android et WebOS : applications en cours de développement
- Autres applications : WebDAV Navigator pour Android, iPhone et BlackBerry

- VM CentOS 6.4, SELinux, LAMP (httpd, mod_ssl, mysql-server, php-ldap)
- 8Go de RAM, 2 coeurs, 2 interfaces réseau en bonding, stockage NetApp
- Adressage privé, derrière un reverse proxy NGINX (VM CentOS 6.4)

Installation et configuration de ownCloud en 10 mn chrono !

- `wget http://download.opensuse.org/repositories/isv:ownCloud:community/CentOS_CentOS-6/isv:ownCloud:community.repo`
- `yum -y install owncloud (/var/www/html/owncloud/, utilisé comme DocumentRoot avec AllowOverride ALL)`
- MySQL : `CREATE DATABASE owncloud;`
- MySQL : `GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud_user'@'localhost' IDENTIFIED BY 'XXXXXXXXX';`
- MySQL : `FLUSH PRIVILEGES;`
- `echo "test" > /var/www/html/owncloud/data/test.html`, si accès via navigateur alors problème de sécurité : le répertoire `data/` doit être bougé

ownCloud : installation (suite)

- `mkdir /var/www/owncloud/data`
- `chmod 750 /var/www/owncloud/`
- `chmod 770 /var/www/owncloud/data/`
- `chown root.apache /var/www/owncloud/`
- `chown apache.apache /var/www/owncloud/data/`
- `yum install polycoreutils-python`
- `semanage fcontext -a -t httpd_sys_rw_content_t
'/var/www/owncloud'`
- `restorecon '/var/www/owncloud'`
- `semanage fcontext -a -t httpd_sys_rw_content_t
'/var/www/owncloud/data/`
- `restorecon '/var/www/owncloud/data/`

ownCloud : installation (suite)

The screenshot shows the ownCloud installation wizard in a Mozilla Firefox browser window. The browser's address bar displays the URL `owncloud.dt.insu.cnrs.fr`. The page features the ownCloud logo at the top right. The main content area is a light gray form with the following sections:

- Create an admin account**: Two input fields. The first contains `owncloud_admin`. The second contains seven dots, representing a password.
- Advanced**: A dropdown menu is open, showing the **Data folder:** field with the value `/var/www/owncloud/data`.
- Configure the database**: Two radio buttons, **SQLite** and **MySQL**, with **MySQL** selected. Below are four input fields: `owncloud_user`, a field with seven dots, `owncloud`, and `localhost`.
- Finish setup**: A button at the bottom of the form.

At the bottom of the page, the text `ownCloud - web services under your control` is visible.

ownCloud : installation (suite)

Activation de « LDAP user and group backend » puis configuration (CentOS Directory Server)

Host	ds83a.dt.insu.cnrs.fr
Base DN	dc=dt,dc=insu,dc=cnrs,dc=fr
User DN	uid=owncloud,cn=config
Password	XXXXXXXXXX
User Login Filter	uid=%uid
User List Filter	objectClass=posixAccount
Group Filter	objectClass=posixGroup
Port	389
Base User Tree	ou=people,dc=dt,dc=insu,dc=cnrs,dc=fr
Base Group Tree	ou=Groups,dc=dt,dc=insu,dc=cnrs,dc=fr

- default quota = 10GB
- Maximum input size for ZIP files = 0 (unlimited)
- Ajout du thème DT/INSU (Merci Yannick Fitamant)
- Découverte des joies (peines) de ownCloud

- Matériel : serveur et réseau sous dimensionnés
- Logiciel : bugs owncloud (côté serveur et client)
 - Problèmes de synchronisation : messages d'erreur (Unknown transfer-coding in response), gonflement en mémoire et CPU côté client, fichiers non synchronisés, fichiers qui reviennent, rafraichissement, etc.
 - Problèmes suite MAJ : le 14 mars MAJ auto et passage en douleur de la 4.7 à la 5.0. ownCloud est resté en mode maintenance. Manque des tables dans MySQL. Il a fallu tout réinstaller
 - Problèmes client natif fedora : sous root OK mais pas en tant que user
 - Problèmes de partage : « Sharing 166099 failed, because the sharing backend for folder could not find its source »
 - Problèmes de conflit : apparition de fichiers dont le nom comporte le mot « conflict »
 - Problèmes dans le calendrier : après avoir ajouté un événement on ne le voit plus mais les autres users le voient !
 - En gros, des problèmes qui apparaissent, qui disparaissent, qui réapparaissent !
- Performance : montée en charge, big files
 - Plus un problème LAMP que ownCloud

- Pas encore mature mais très prometteur (inclus de base dans des distributions linux importantes)
- Déploiement récent (février 2013), tuning en cours
- Actuellement en expérimentation à la Seyne sur Mer uniquement (une vingtaine de personnes)
- Prochainement le service sera étendu aux autres sites de la DT/INSU
- Tests à venir avec NGINX au lieu de apache

- Le présenter aux utilisateurs comme un service expérimental (atténuer la pression)
- Commencer par ouvrir le service aux « power users »
- Étendre aux autres utilisateurs de manière progressive pour ne pas mettre à genou le serveur et être débordé par les évènements
- Faire une démo aux utilisateurs et leur fournir une documentation avec les « best practices »
- Ne pas activer trop d'applications au début, se focaliser sur la synchronisation qui implique beaucoup de « upload »
- Toujours utiliser les dernières versions surtout côté client

ownCloud : recommandations pour un déploiement réussi (suite)

- Ne pas hésiter au début à mettre des outils de stats/monitoring LAMP (ExtendedStatus On, server-status, server-info, check_httpd_limits.pl, autre ?)
- Ne pas se contenter de la config par défaut pour éviter les problèmes de performance : Mise en place d'un opcode cache (APC), paramétrage, Tuning LAMP en général
 - Tuning LAMP systems, Part 1 : Understanding the LAMP architecture (<http://www.ibm.com/developerworks/library/l-tune-lamp-1/index.html>)
 - Tuning LAMP systems, Part 2 : Optimizing Apache and PHP (<http://www.ibm.com/developerworks/library/l-tune-lamp-2/index.html>)
 - Tuning LAMP systems, Part 3 : Tuning your MySQL server (<http://www.ibm.com/developerworks/library/l-tune-lamp-3/index.html>)