

# Article : NextCloud : Offre de Cloud privé pour les 5000 personnels de l'Université Grenoble Alpes

**Guenael Sanchez**

DGDSI Université Grenoble Alpes  
43 Rue des Mathématiques  
38400 Saint Martin d'Hères

## Résumé

*Face au constat de l'utilisation grandissante des outils de stockage de données dans le « cloud » proposés par des sociétés privées et souvent américaines. Et suite à la demande de certains chercheurs et personnels administratifs de pouvoir bénéficier d'un tel outil hébergé et administré localement, l'Université Grenoble Alpes a lancé, il y a 6 ans, une expérimentation sur l'outil OwnCloud.*

*Avec près de 400 utilisateurs pour environ 1 téra-octet de données, nous avons souhaité passer à l'échelle supérieure : Offrir au 5000 personnels de l'Université un espace de stockage « cloud » répondant aux caractéristiques suivantes :*

- Données hébergées à l'UGA,
- Quota suffisant pour faire « concurrence » aux outils privés,
- Simplicité d'utilisation et d'accès,
- Outils collaboratifs aboutis notamment face à la suite Google.

*Notre choix s'est porté sur les logiciels NextCloud & OnlyOffice, en offrant 50 giga-octets d'espace par utilisateur. Nous appuyant sur la plateforme de virtualisation grenobloise (WINTER) [1] et sur l'hébergement de données grenoblois lui aussi (SUMMER) [2], la solution se veut modulaire et « scalable » pour suivre l'évolution du nombre d'utilisateurs.*

*Après un an de test auprès de 1 200 utilisateurs pour environ 10 téra-octets de données stockées, la solution est maintenant en production et répond bien à différents besoins exprimés. D'un côté le chercheur souhaitant synchroniser ses données entre plusieurs postes, mais aussi le personnel administratif sur poste nomade souhaitant accéder et sauvegarder simplement ses données.*

*Vous retrouverez nos choix d'architecture technique sur notre poster, ainsi que les différents cas d'usages.*

## Mots-clefs

*Cloud privé, NextCloud, Outils collaboratifs, OnlyOffice, Clustering.*

## 1 Introduction & Contexte

L'Université Grenoble Alpes regroupe depuis 2016 les trois Universités historiques du bassin grenoblois. Bientôt, l'UGA, structurée en UI (Université Intégrée), regroupera les autres structures d'enseignement supérieur / recherche du bassin alpin comme Grenoble INP, etc.

De nombreux personnels et chercheurs utilisent à titre privé ou professionnel des solutions de stockage de données en ligne de type « cloud ». Des offres souvent gratuites, proposant un modèle payant pour obtenir plus de volumétrie et/ou de services. Ces solutions, majoritairement proposées par les géants du Net, sont, pour la plupart, hébergées en partie ou en totalité sur le sol américain. Cette localisation des données et la législation s'y rapportant n'est pas sans poser quelques problèmes.

Il est néanmoins difficile de reprocher à un utilisateur sa manière de gérer ses données quand on a rien de mieux à lui proposer. C'est pourquoi nous avons lancé, en 2013, un test sur l'outil OwnCloud. Avec 400 utilisateurs pour 1 téra-octet de données, les retours étaient très positifs !

L'authentification est simple, ne nécessite pas l'utilisation d'un client VPN, une application mobile permet un accès simple aux données, un client lourd permet la synchronisation entre dossiers locaux et dossiers dans le « nuage ». Enfin, il est facile de partager fichiers et/ou dossiers avec une personne en particulier, présente dans l'annuaire de l'établissement, ou de créer un lien de partage que l'on peut communiquer à l'extérieur.

L'architecture technique était monolithique, une seule machine virtuelle pour assurer l'ensemble des services. Peu « scalable », sensible aux variations de l'activité des utilisateurs, l'UGA, et ses potentiels 5500 utilisateurs nous obligent à voir plus grand.

Début 2018, voilà un an que NextCloud, branche issue du projet ownCloud, a démarré. La vivacité du projet NextCloud, et les retours d'autres Universités qui l'ont déployé nous convainquent de miser sur ce dernier.

Le projet de Cloud privé UGA sera donc basé sur la solution NextCloud.

## 2 Réponse technique

Notre retour d'expérience sur OwnCloud a permis de mettre en exergue les éléments cruciaux de la solution :

- Une base de données solide et performante, idéalement répartie en cluster afin de tolérer la panne d'un élément et de distribuer la charge,
- Une ferme d'instances php en mode FPM (FastCGI Process Manager) afin de tolérer la panne d'un élément et de distribuer la charge,
- Un frontal type HAProxy, idéalement doublé, afin de là aussi tolérer la panne d'un élément,
- Un serveur REDIS qui a un double but, stocker les sessions PHP des utilisateurs, et servir de cache à l'application NextCloud,
- Un stockage NFS performant pouvant stocker un grand nombre de fichiers, fourni par la plateforme SUMMER,
- Un annuaire LDAP performant pouvant supporter de multiples requêtes paginées.

Ce qui nous amène au schéma suivant :

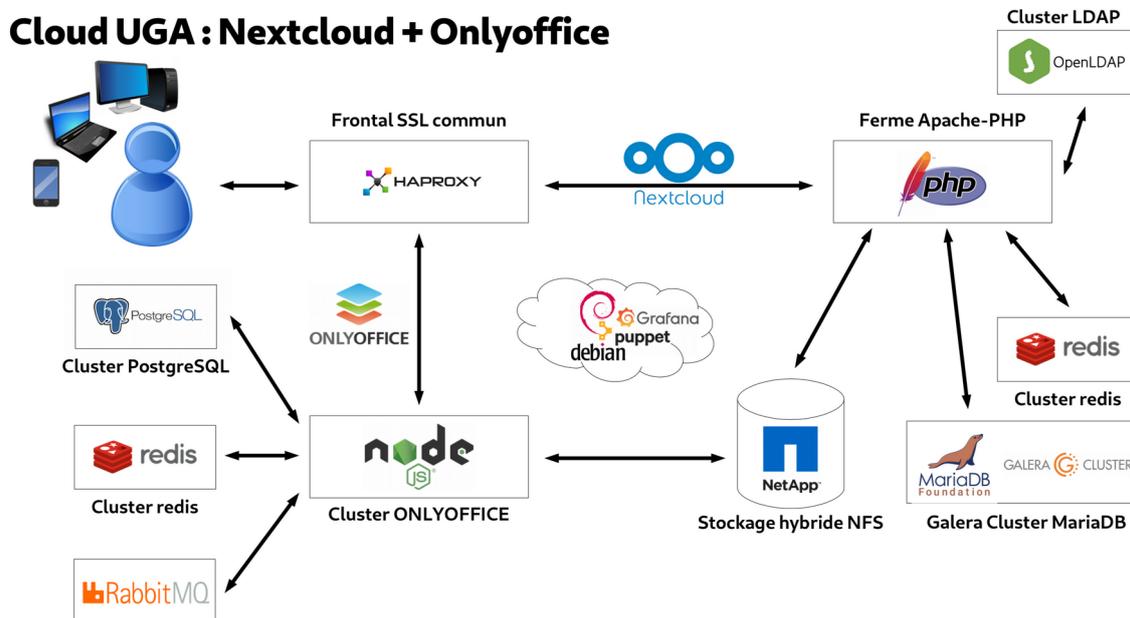


Figure 1: Architecture Nextcloud & Onlyoffice

L'ensemble sera constitué de machines virtuelles hébergées sur WINTER [1], la plateforme de virtualisation mutualisée de l'UGA.

## 2.1 Base de données

L'utilisation du moteur MariaDB est recommandé par NextCloud. Cependant, afin de durcir la solution, nous avons cherché à mettre ce moteur de base de données en cluster. Notre équipe a testé différents outils, et a retenu le duo MariaDB et GaleraCluster, pour sa simplicité de configuration et de reprise après incidents.

La documentation en ligne de NextCloud donne plusieurs conseils de configuration<sup>1</sup> pour MariaDB, et quelques conseils pour un fonctionnement en mode GaleraCluster.

Pour le moment, l'application NextCloud cible un nœud en particulier, nous sommes en phase de test d'un outil SQLProxy, qui permet, une répartition de charges entre les nœuds, et est également capable, d'analyser le type de requêtes SQL.

Cette analyse permet, par exemple de cibler toutes les requêtes "modifiantes" (INSERT/UPDATE/DELETE) vers un nœud en particulier, et de répartir les requêtes de lecture (SELECT) entre tous les nœuds. Cette configuration permet de résoudre certains problèmes d'écritures concurrentes qui peuvent apparaître lors de taux de charge très élevés.

## 2.2 Moteur d'exécution du code PHP

1. [https://docs.nextcloud.com/server/15/admin\\_manual/installation/server\\_tuning.html#using-mariadb-mysql-instead-of-sqlite](https://docs.nextcloud.com/server/15/admin_manual/installation/server_tuning.html#using-mariadb-mysql-instead-of-sqlite)

Le couple Apache/PHP n'est plus à présenter, mais peut fonctionner selon différents modes. L'approche FPM (FastCGI Process Manager) reste la méthode la plus légère et surtout prévisible.

Chaque nœud de la ferme est taillé pour un nombre précis de processus PHP lancés en parallèle. Cette limite s'obtient par une montée en charge générée manuellement, en mesurant la taille mémoire de chaque processus, et en augmentant le nombre de processus pour s'approcher d'une saturation mémoire idéal (90-95%).

Reste ensuite à multiplier les nœuds Apache-PHP-fpm en fonction de vos besoins, la couche HAProxy en frontale permettant de gérer cela facilement.

### **2.3 Répartiteur de charge**

Pour assurer une répartition de charge entre les moteurs PHP, nous avons opté pour le logiciel HAProxy. Petite spécificité nous concernant, nous l'utilisons en terminaison SSL. C'est donc HAProxy qui communique de manière chiffrée avec les clients, le reste des communications entre HAProxy et les nœuds Apache-Php restant en HTTP non chiffré.

Cette configuration nous permet d'utiliser le mode HTTP d'HAProxy, collectant ainsi des statistiques poussées en termes de code de retour HTTP, des URL demandées, etc.

De plus, grâce au protocole VRRP et au logiciel keepalived, une deuxième machine virtuelle configurée de manière identique est prête à prendre le relai en cas de défaillance, le duo keepalived-VRRP assurant le transfert de l'IP principale du service.

### **2.4 Stockage des sessions, cache applicatif et verrous de fichiers**

Les clients étant répartis entre les différents moteurs d'exécution PHP, il est impératif que ces moteurs mettent en commun les sessions des utilisateurs. De cette manière, un client peut basculer d'un moteur à l'autre de manière transparente.

NextCloud utilise également le moteur redis afin de stocker un certain nombre d'informations de cache, mais aussi la gestion des verrous de fichiers évitant ainsi les modifications d'un même fichier par 2 sources en simultané.

### **2.5 Stockage des données**

Nos amis de la plateforme SUMMER [2] nous fournissent un volume NFS sur du stockage hybride (cache SSD + stockage classique pour données refroidies). L'avantage du NFS est d'être élastique et peut être augmenté quand nécessaire.

Dans nos dernières statistiques d'utilisation, nous observons quelques pics d'échange de données autour de 2000/4000 IOPS avec une latence sous la milliseconde. En comparaison des autres usages NFS observés sur la plateforme SUMMER, il nous reste encore une large marge de progression.

### **2.6 Annuaire LDAP**

Pour authentifier les utilisateurs, plusieurs sources sont possibles. Nous avons opté pour un annuaire openLDAP redondé en temps réel (Maître/Esclave).

L'annuaire maître se synchronise toutes les heures auprès de nos référentiels.

Ces annuaires sont énormément sollicités en requête de recherche. En effet, NextCloud tient à jour en tâche de fond et en base de données, son propre annuaire des personnes. Le logiciel scrute donc constamment les changements d'informations et les répercutent dans sa propre base.

D'autre part, les utilisateurs peuvent générer de nombreuses requêtes lorsqu'ils utilisent la fonctionnalité de partage d'un fichier/dossier. Pour partager un fichier avec un utilisateur « Pierre Martin », les requêtes LDAP suivantes vont être émises au fur et à mesure que l'utilisateur tape au clavier : uid=p\* / uid=pi\* / uid=pie\* etc.

### 3 Phases de tests et de formation

Début 2018, nous avons déployé la première infrastructure de test, les machines virtuelles sont hébergées sur la plateforme mutualisée WINTER [1] et configurées à l'aide de l'outil Puppet, afin d'assurer une cohérence dans les configurations de chaque brique. L'infrastructure étant élastique pour s'adapter à la charge, il est important que toutes les briques (briques cluster MariaDB/GaleraCluster ou briques Apache/PHP) soient configurées de manière uniforme.

D'abord ouvert aux personnels de la DSI, puis aux anciens utilisateurs de la plateforme OwnCloud, et enfin à l'ensemble du personnel de l'UGA, cette montée en charge progressive nous a permis de surveiller le comportement de chaque brique logicielle, gérer les scénarios de mises à jour applicatives, créer la documentation utilisateur, etc.

Aujourd'hui, avec presque 2000 utilisateurs actifs, et 10 To de données stockées, le cloud UGA est en vitesse de croisière.

Nous avons choisi un accompagnement externe, revendeur et intégrateur du support officiel NextCloud. Notre partenaire nous assiste dans les phases de montée de version, ou de problématiques rencontrées. Il valide également nos choix techniques pour assurer une compatibilité avec les pré-requis & bonnes pratiques édités par NextCloud.

Le coût de la licence est lié au nombre d'utilisateurs potentiellement admissible sur la plateforme. Dans notre cas, l'authentification est liée à un annuaire LDAP des personnels UGA (au sens large) et contient plus de 20 000 entrées, dépassant ainsi largement le nombre « réel » de personnels présents au sein de l'UGA.

Cette différence s'explique par la présence de comptes liées à des personnes morales, des comptes en attente d'expiration, des étudiants vacataires, etc.

Nous avons donc créé un groupe LDAP restreint à deux populations :

- Les personnes qui ont utilisé au moins une fois la plateforme depuis sa mise en service,
- Les personnes qui ont exprimé (opt-in) leur souhait d'utiliser la plateforme via un formulaire de consentement.

Le coût pour 5 500 utilisateurs au tarif « académique » est en 2019 de 10 450 € HT.

### 4 Intégration OnlyOffice

Un des atouts de NextCloud est la possibilité d'inclure des applications tierces. Un des principaux usages que nos utilisateurs ont souhaité expérimenter est celui de pouvoir

collaborer en ligne sur des documents bureautiques ; Traitement de texte, tableur ou présentation.

Plusieurs options disponibles sur le marché, nos collègues testent en parallèle plusieurs plateformes intégrables à la suite Alfresco. Au final, notre choix se porte sur OnlyOffice.

OnlyOffice est disponible en version communauté sous licence GNU AGPL v3, ou en version d'intégration soumis à licence commerciale. Afin de nous assurer un support de la part de l'éditeur, nous optons pour le modèle soumis à licence.

La licence est basée sur le nombre de documents ouverts en parallèle. Dans notre configuration, nous avons opté pour une installation en mode cluster, permettant d'isoler les différents composants de l'application.

L'utilisation est assez simple. On parcourt en ligne son espace cloud, et on clique sur le document (formats .docx / .xlsx / .pptx supportés en édition) que l'on souhaite éditer. Pour le moment, la solution ne permet pas l'édition des documents au format OpenDocument (.odt/.ods/.odp) ou Office ancienne génération (.doc/.xls/.ppt), sauf à activer des fonctionnalités encore considérées comme expérimentales.

En attendant un support complet de ces formats de fichiers, OnlyOffice permet de convertir, directement dans le cloud de l'utilisateur, le fichier à éditer. L'éditeur « Ascensio System » n'a pour le moment, pas indiqué de date pour le support des formats « historiques ».

Un nouvel onglet s'ouvre alors avec le document ouvert en édition. Si ce document était partagé dans NextCloud avec d'autres personnes, et si ces personnes cliquent également sur le document qui est partagé avec eux, un onglet d'édition s'ouvre et la collaboration est activée, on voit les curseurs des autres participants, ainsi que leurs modifications en temps réel.

Pour 200 documents ouverts simultanément, le coût de la licence académique est de 2 600 € HT, auquel il faut ajouter, si on le souhaite, 1 309 € pour l'infrastructure de pré-production.

#### **4.1 Répartiteur de charge**

Nous utilisons la même instance HAProxy que pour NextCloud. En effet HAProxy est capable de gérer plusieurs "frontaux" avec des noms DNS différents, et des certificats SSL différents.

Cette brique étant déjà redondée, la partie OnlyOffice en profite également.

#### **4.2 Moteur OnlyOffice**

Basé sur NodeJS, l'installation d'OnlyOffice se fait via le gestionnaire de paquets de Debian « apt » ! Des instructions de configuration peuvent être spécifiées avec l'installation, permettant un déploiement en mode cluster. (voir Annexe avec commande de config à #TODO)

Par défaut, l'installation du paquet OnlyOffice considère que le fonctionnement est monolithique et entraîne l'installation et la configuration de tous les autres paquets en local.

### 4.3 Stockage des sessions

Les sessions, ainsi qu'un certain nombre d'informations de cache sont stockées dans un moteur Redis, lui-même redondé sur un mode Maître/Esclave.

Les données stockées sont volatiles et non vitales.

### 4.4 Gestionnaires de files d'attente de messages

OnlyOffice préconise l'utilisation du logiciel RabbitMQ pour la gestion, le stockage et la diffusion de messages/files d'attente, entre les briques du cluster, notamment concernant la licence d'utilisation, et le compteur de documents ouverts.

### 4.5 Moteur de base de données

OnlyOffice préconise l'utilisation de PostgreSQL. Nous avons pu nous appuyer sur notre équipe de base de données, qui nous fournit un moteur redondé pour PostgreSQL. Deux tables seulement sont nécessaires et stockent les données relatives aux modifications effectuées sur les documents en cours d'édition.

Lorsque le compteur de document ouvert revient à 0, les tables sont vides. La version de démonstration d'OnlyOffice permet d'ouvrir jusqu'à 20 documents en simultanément. Vu l'activité quasi-nulle mesurée lors de nos simulations, la charge est donc globalement assez faible en comparaison de celle que NextCloud, par exemple, impose à son moteur de base de données.

### 4.6 Stockage NFS

Enfin, un espace partagé en NFS est monté sur chaque instance OnlyOffice, et permet de partager un pot commun des fichiers de cache, à savoir les documents ouverts en cours de modification, et autres fichiers temporaires. Là aussi, lorsque les documents sont fermés, et après un délai d'expiration, ce cache est vidé.

## 5 Conclusion

L'offre est un réel succès ! Avec presque 2000 utilisateurs actifs (sur une population de 5500 personnels) l'UGA propose une vraie alternative crédible et viable face aux outils disponibles gratuitement sur Internet.

Le tout basé sur une solution de logiciel libre, nous continuons à sensibiliser et inviter les nouveaux arrivants et le reste du personnel à basculer petit à petit leurs usages sur cet outil.

Le fait de proposer un espace conséquent par utilisateur (50 giga-octets) aide probablement à la crédibilité de la solution. En effet, les différents acteurs gratuits disponibles sur Internet proposent des espaces entre 2 et 25 giga-octets.

On note que l'usage du client lourd est omniprésent, l'utilisation en ligne se développant plus timidement, notamment depuis l'intégration d'OnlyOffice dans la solution.

Les outils sont robustes, et l'accompagnement est un relai idéal avec les développeurs de la solution. Pour la suite, nous envisageons de développer la formation des

utilisateurs sur les produits de la solution, et nous évaluons la pertinence de déployer d'autres applications tierces comme Talk, une solution d'audio et vidéo-conférence. Vous pouvez retrouver les principaux éléments sur notre poster.

## Annexe

Les auteurs ajoutent, si nécessaire, une annexe avec une section non numérotée.

## Bibliographie

- [1] Guenael Sanchez et al. WINTER : virtualisation hyperconvergente Full-Flash multi-site. Dans Actes du congrès JRES2017, Montpellier, Novembre 2017 ; [https://conf-ng.jres.org/2017/document\\_revision\\_1923.html?download](https://conf-ng.jres.org/2017/document_revision_1923.html?download)
- [2] Dimitri Rapacchi et al. SUMMER : 4 ans de stockage mutualisé et réparti. Dans Actes du congrès JRES2017, Montpellier, Novembre 2017 ; [https://conf-ng.jres.org/2017/document\\_revision\\_2869.html?download](https://conf-ng.jres.org/2017/document_revision_2869.html?download)