



Direction des systèmes d'information

## Projet ownCoRe

JoSy "Cloud privé dans l'enseignement et la recherche"

-  
19 mai 2014

Pour plus d'information sur ce support, contacter :

- [eric.gervasoni@dr20.cnrs.fr](mailto:eric.gervasoni@dr20.cnrs.fr) (MOA)
- [paulo.moradefreitas@dr2.cnrs.fr](mailto:paulo.moradefreitas@dr2.cnrs.fr) (MOA)
- [david.rousse@dsi.cnrs.fr](mailto:david.rousse@dsi.cnrs.fr) (chef de projet/MOE)
- [gilian.gambini@dsi.cnrs.fr](mailto:gilian.gambini@dsi.cnrs.fr) (expertise MOE)





P. 2

# Plan

- ❑ **Contexte du projet**
- ❑ **Étude d'architecture**
- ❑ **Étude du dimensionnement**
- ❑ **Architecture cible détaillée**
- ❑ **Le suite du projet, les questions**

# Contexte du projet ownCore – Offre De Services du CNRS

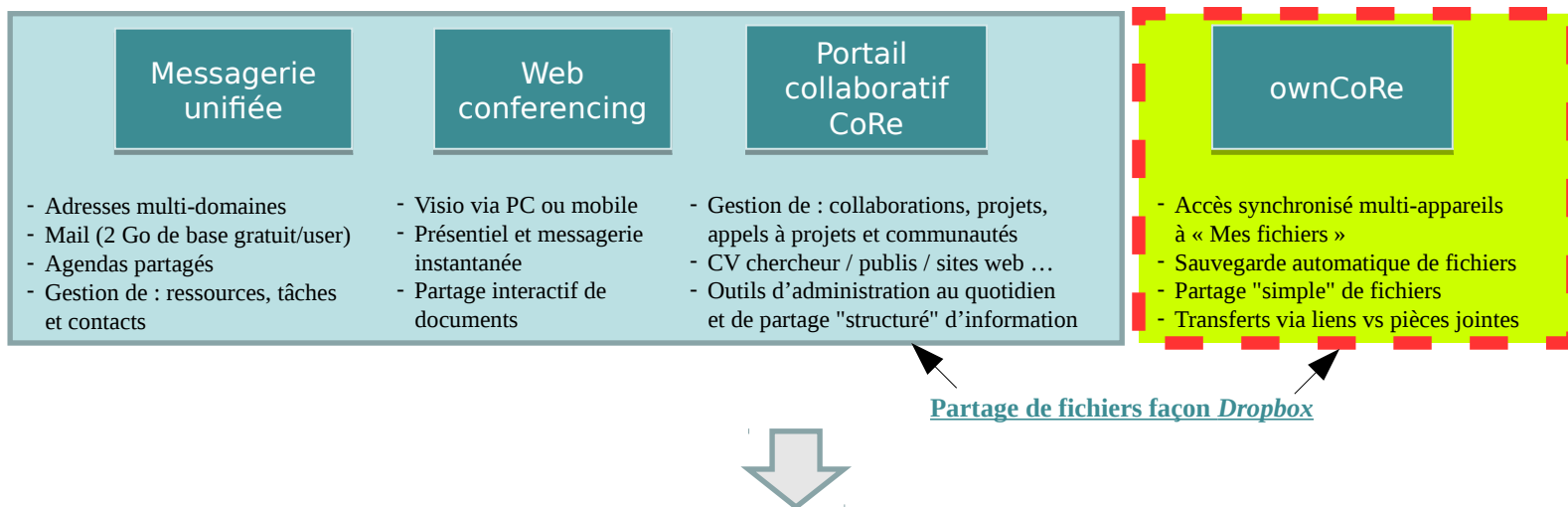
P. 3

## Objectifs des ODS :

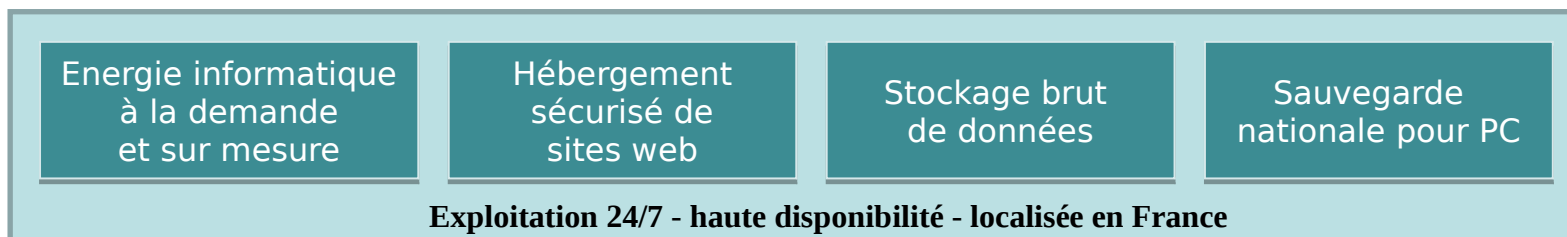
Simplifier et sécuriser le quotidien des laboratoires<sup>(\*)</sup> :

- proposer des outils adaptés aux métiers de la recherche et à leurs contraintes de sécurité
- permettre aux unités de se décharger au besoin de certaines tâches « techniques »

### Environnement utilisateurs : intégration native des outils → simplicité d'utilisation



### Socle infrastructures : mutualisation sur Cloud privatif → économies d'échelle



### Support

Equipes SI des  
Délégations  
Régionales



Support  
de proximité

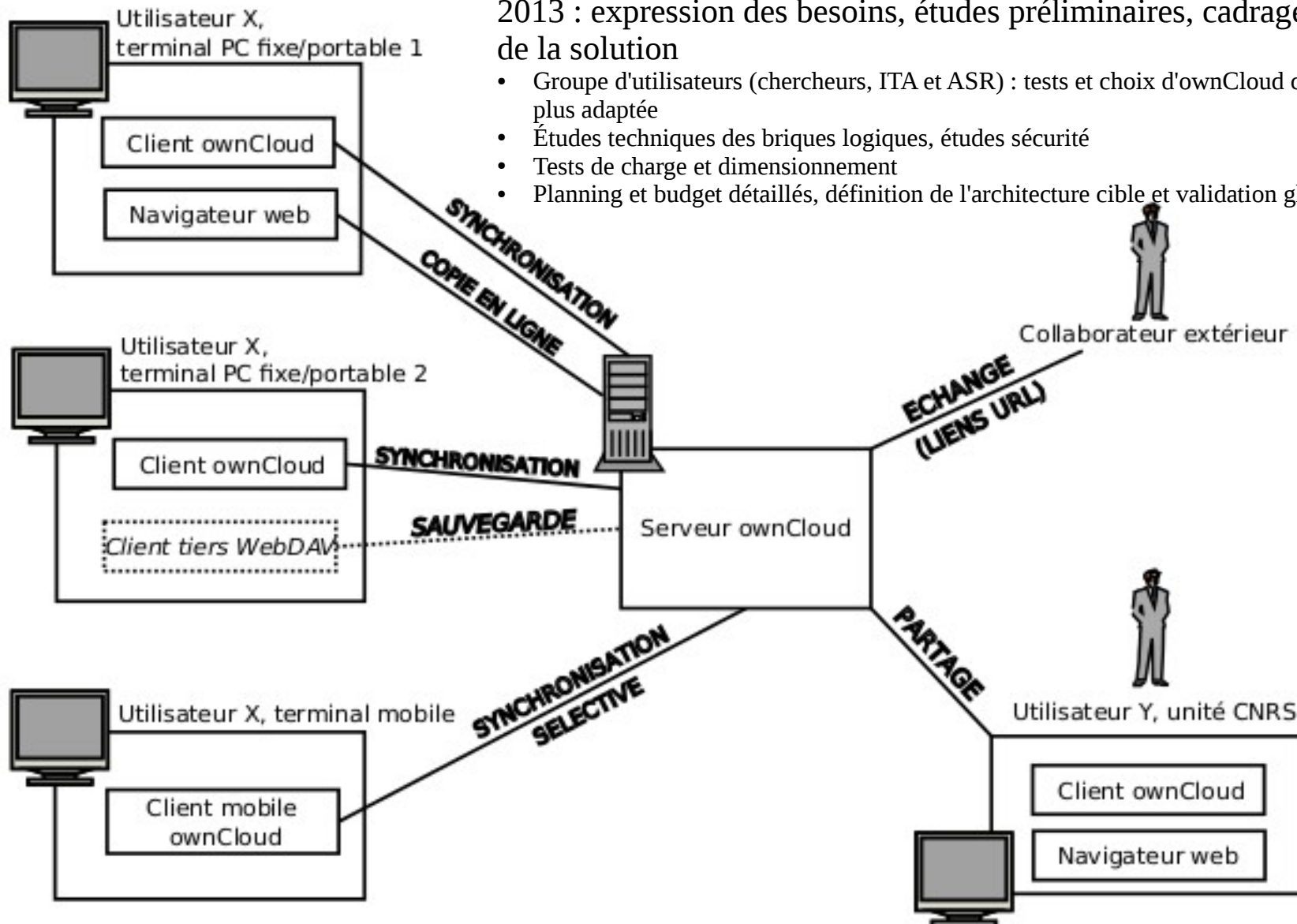
(conseil & accompagnement à la mise en œuvre des services)

(\*) Les entités administratives et fonctionnelles peuvent également bénéficier de ces services

# Contexte du projet ownCore

- **Objectifs spécifiques d'ownCoRe**

- Service de **partage et de synchronisation de fichiers** de travail
- **100 000 utilisateurs** potentiels / **10 Go** par utilisateur
- « Pré-projet » de janvier 2013 à septembre 2013, et projet depuis octobre 2013 : expression des besoins, études préliminaires, cadrage et validation de la solution
  - Groupe d'utilisateurs (chercheurs, ITA et ASR) : tests et choix d'ownCloud comme la solution la plus adaptée
  - Études techniques des briques logiques, études sécurité
  - Tests de charge et dimensionnement
  - Planning et budget détaillés, définition de l'architecture cible et validation globale

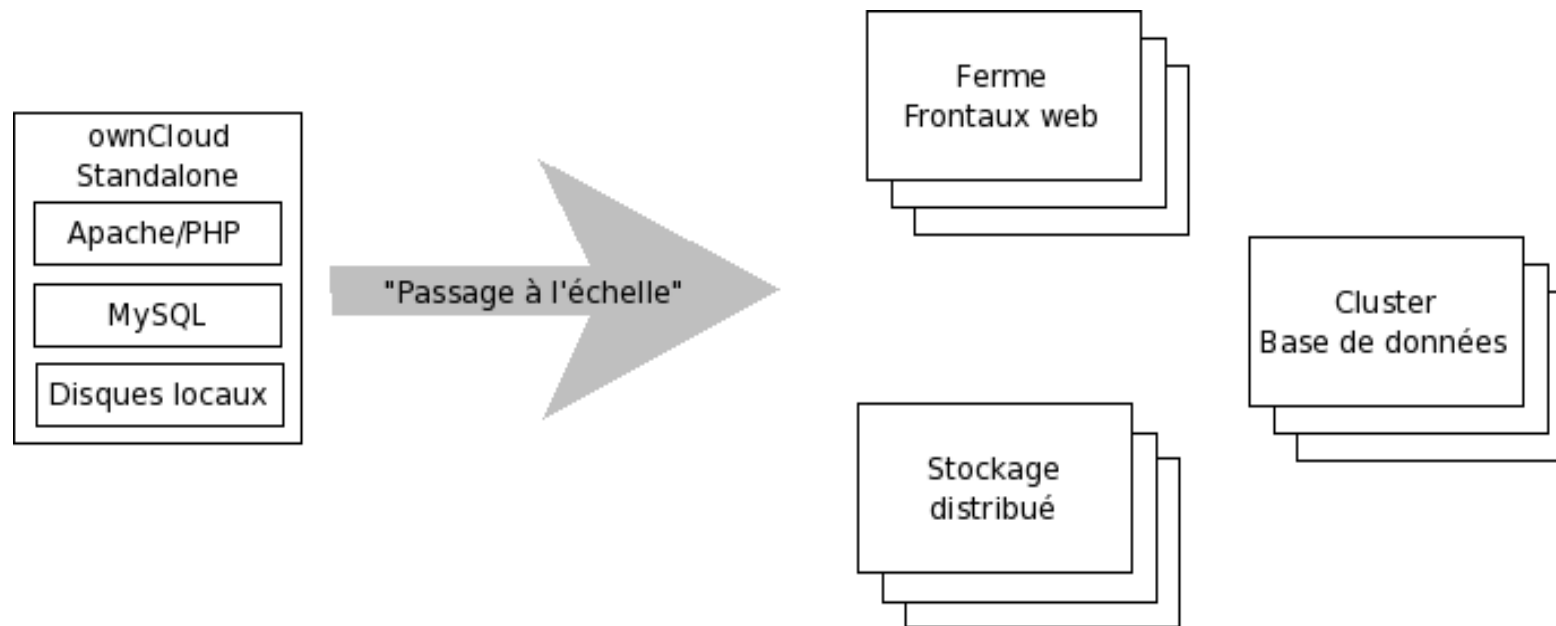




# Plan

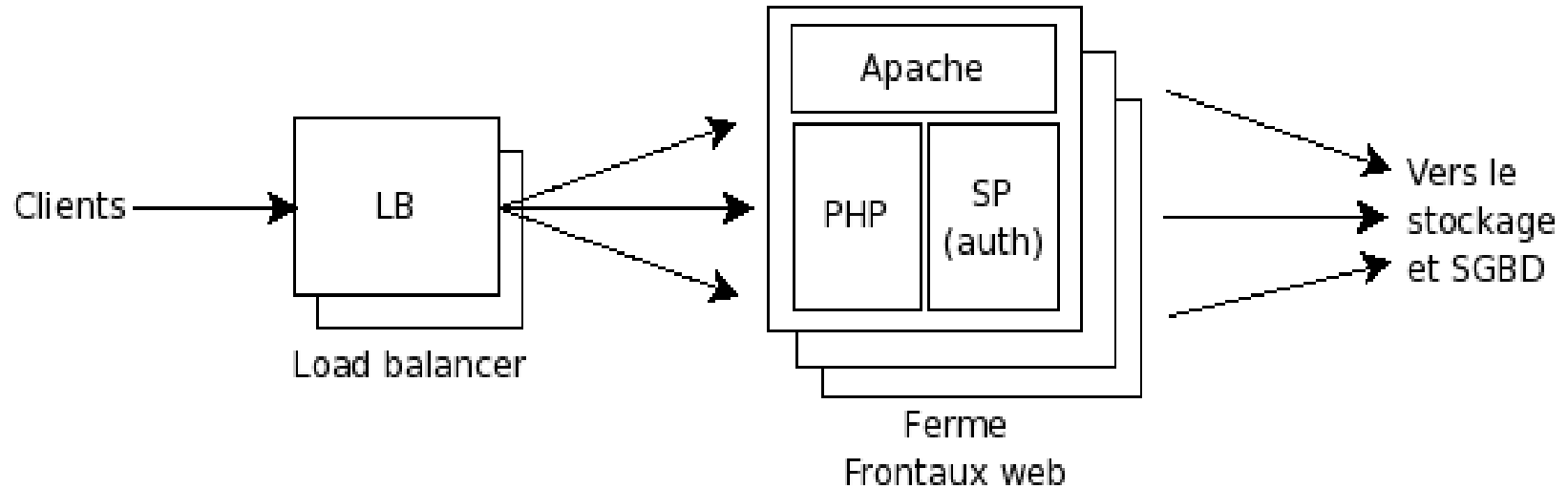
- ❑ **Contexte du projet**
- ❑ **Étude d'architecture**
  - ✓ Briques logiques
  - ✓ Scalabilité des frontaux web
  - ✓ Scalabilité de la base de données
  - ✓ Scalabilité du stockage
  - ✓ Sécurisation de la solution
- ❑ **Étude du dimensionnement**
- ❑ **Architecture cible détaillée**
- ❑ **Le suite du projet, les questions**

# Architecture – Briques logiques



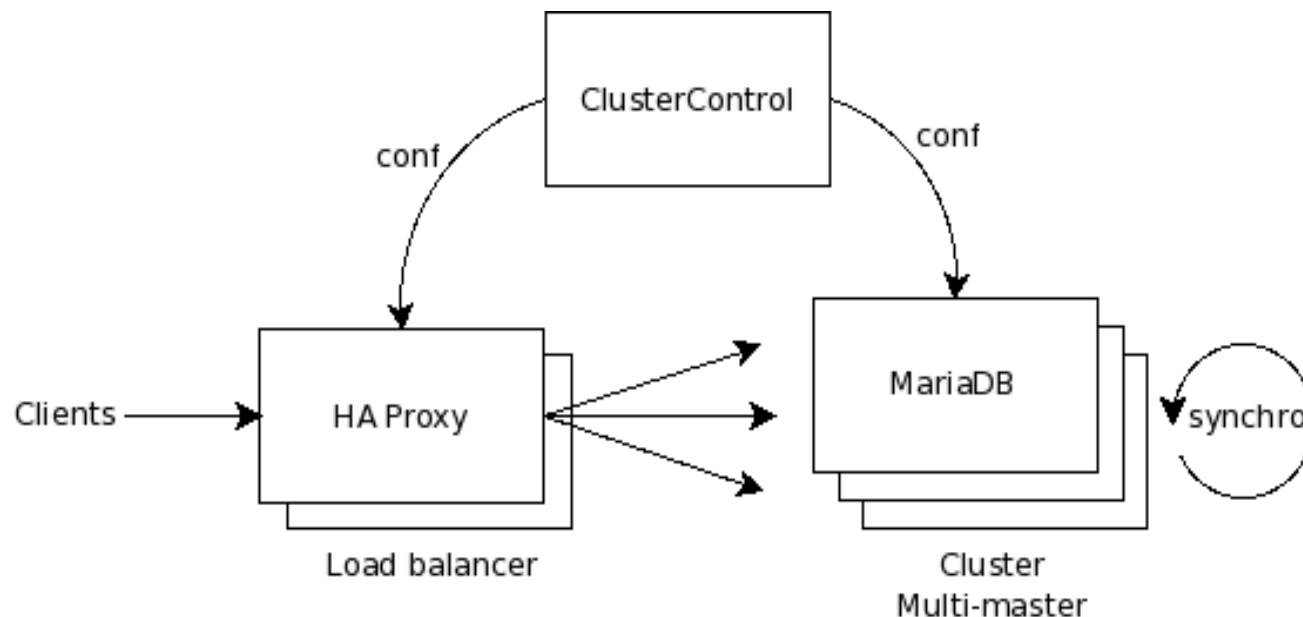
- Le service est divisé en 3 briques logiques
- Chaque brique doit être « **scalable** » et hautement **disponible**
- Garantir et maintenir la **sécurité** du système d'information au bon niveau, en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité

## Architecture – Scalabilité des frontaux web



- Nœud web autonome, identique et standard
- Scalabilité et HA assurées par les load balancers
- Limitations :
  - Besoin d'avoir un unique file system
  - Défaillance d'un nœud = ré-authentification SSO

- Nos contraintes :
  - SGBD supporté par ownCloud
  - HA et scalable
  - Coût raisonnable
  - Privilégier MariaDB à MySQL
- Solution retenue : **MariaDB Galera Cluster**
  - Logiciel déjà retenu à la DSI pour d'autres services
  - Exploitation facilitée avec **ClusterControl**



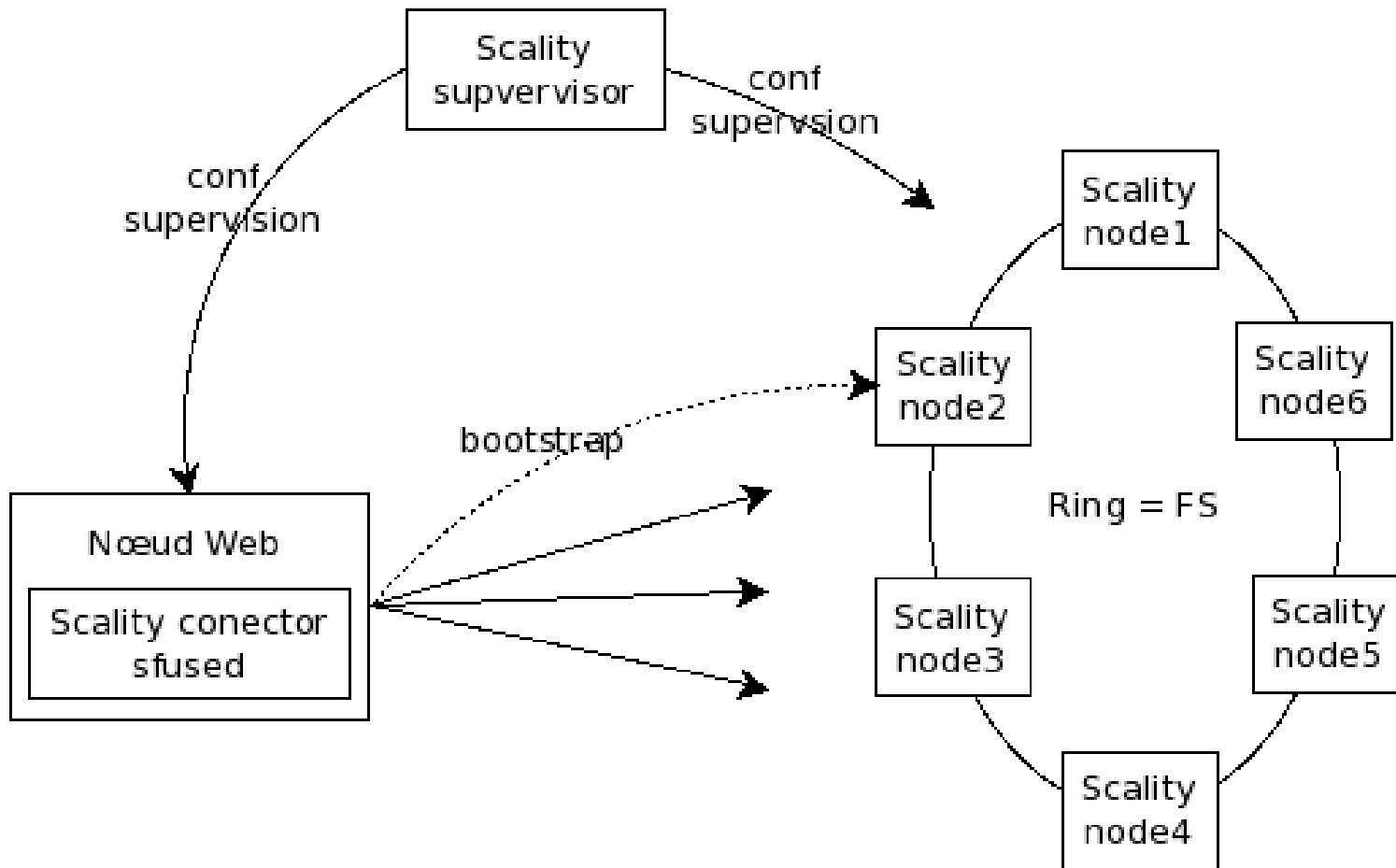




# Architecture – Scalabilité du stockage

- Notre besoin :
  - Présenter un filesystem unique d'1 Po utile, voire plus
  - Forte résilience car pas de sauvegarde du filesystem
  
- Les solutions répondant à notre besoin :
  - Dell **Compellent** (+ tête NAS FluidFS) → résilience et volumétrie limitées
  - EMC **Isilon** → solution matérielle et logicielle propriétaire
  - **Scality** → solution logicielle de stockage distribuée
  
- Solution retenue : **Scality**
  - Souplesse dans le choix du matériel
  - Exploitation simple
  - Perspective intéressante → géo-distribution, volumétrie, types de connecteurs

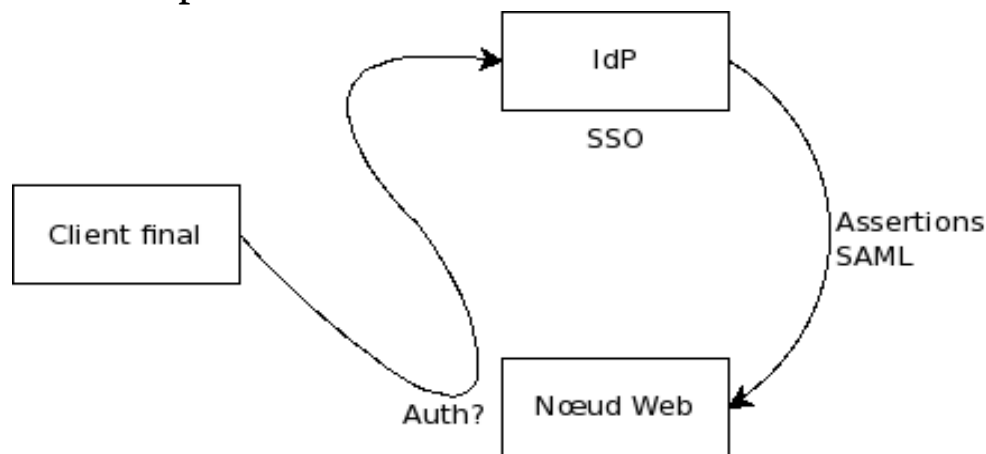
# Architecture – Scalabilité du stockage



# Architecture – Sécurisation de la solution

- **Authentification via le SSO Janus**

- Pas de base de comptes locale
- Provisionning des comptes automatique
- Ouverture à des partenaires CNRS possible



- **Limitations**

- L'IdP est une brique critique
- Utilisation d'un plugin = l'app user\_shibboleth
- Changement statu ou labo. d'un agent dans l'annuaire
- Shibbolethisation du client lourd (dispo. depuis la 1.5.\*)

- **Sécurisation** de la solution avec l'application de la PSSI du CNRS

- **Audit de code** d'ownCloud (coté serveur) effectué = possible car logiciel open source, résultats très satisfaisant
- **Étude de risque** sur le service ownCoRe effectuée = résultats satisfaisant, possibilité d'intégration de besoins spécifiques CNRS car logiciel open source
- **Audit technique** de sécurité et **tests d'intrusion** prévus

# Plan

- ❑ Contexte du projet
- ❑ Étude d'architecture
- ❑ Étude du dimensionnement
  - ✓ Démarche utilisée
  - ✓ Dimensionnement estimé
- ❑ Architecture cible détaillée
- ❑ Le suite du projet, les questions

# Dimensionnement – Démarche utilisée

- **Hypothèses fonctionnelles** d'usage du service
  - Population (cible haute) = **100000 utilisateurs**
  - Pourcentage d'utilisation du service = **entre 15% et 50%**
  - Quota = **10 Go** par utilisateur
  - Nombre de fichiers = **1000 fichiers par utilisateur**
  - Taille moyenne des fichiers = **5 Mo**
  - Nombre de mises à jour de fichiers = **50 par utilisateur**
  - Nombre de terminaux par utilisateur = **3**
  - Hypothèse de partage des fichiers d'un utilisateur = **15%** de ses fichiers, à **5** autres personnes
  - Durée de travail quotidienne des utilisateurs = **6 heures**
  - Durée de la plage d'authentification quotidienne des utilisateurs = **1 heure**
- **Dimensionnement théorique** basé sur ces hypothèses
  - Étude fine du fonctionnement d'**ownCloud**
  - Capacité de tenue de charge pour **MariaDB** (8 cœurs, 16Go de RAM) :
    - SELECTs : max **3857** / sec
    - INSERTs : max **22000** / sec
    - UPDATEs : max **3857** / sec
  - Capacité de tenue de charge pour **Apache** (8 cœurs, 16Go de RAM) : **530** requêtes simultanées gérées
- **Tests de charge** pour valider la théorie
  - Avec une **architecture simple**, **ci-dessous**, et l'**outil Tsung** pour simuler les usages fonctionnels :
    - 2 serveurs load balancer (Piranha)
    - 2 serveurs reverse proxies (Apache/mod\_proxy)
    - 2 serveurs web (Apache/ownCloud 6)
    - 1 serveur MariaDB
    - 1 serveur NFS exposant un espace de stockage unique



# Dimensionnement – Résultat

P. 14

- Serveurs **MariaDB** :

SQL servers		Number of SQL nodes (~ VM) for the estimated SQL load (8 cores/16GB RAM per node)						
	Number of users (N)							
% of active users	1	1000	5000	30000	50000	70000	100000	
5,00%	1	1	1	3	5	7	10	
10,00%	1	1	1	6	9	12	18	
15,00%	1	1	2	8	13	18	25	
20,00%	1	1	2	11	18	24	35	
30,00%	1	1	3	16	27	38	54	
50,00%	1	1	3	18	30	41	59	

- Serveurs **Apache/ownCloud** :

Web servers		Number of web nodes for the estimated load (8 cores/16GB RAM per node)						
	Number of users (N)							
% of active users	1	1000	5000	30000	50000	70000	100000	
5,00%	1 serv	1 serv	1 serv	3 serv	5 serv	7 serv	10 serv	
10,00%	1 serv	1 serv	1 serv	6 serv	10 serv	14 serv	19 serv	
15,00%	1 serv	1 serv	2 serv	9 serv	15 serv	20 serv	29 serv	
20,00%	1 serv	1 serv	2 serv	12 serv	19 serv	27 serv	38 serv	
30,00%	1 serv	1 serv	3 serv	17 serv	29 serv	40 serv	57 serv	
50,00%	1 serv	1 serv	5 serv	29 serv	48 serv	67 serv	95 serv	

- Bande passante **réseau** :

Total DL		Network bandwidth simulation for download [Sync own+Sync share] (global ownCoRe architecture)						
	Number of users (N)							
% of active users	1	1000	5000	30000	50000	70000	100000	
5,00%	0 mb/s	13 mb/s	64 mb/s	382 mb/s	637 mb/s	891 mb/s	1 273 mb/s	
10,00%	0 mb/s	25 mb/s	127 mb/s	764 mb/s	1 273 mb/s	1 782 mb/s	2 546 mb/s	
15,00%	0 mb/s	38 mb/s	191 mb/s	1 146 mb/s	1 910 mb/s	2 674 mb/s	3 819 mb/s	
20,00%	0 mb/s	51 mb/s	255 mb/s	1 528 mb/s	2 546 mb/s	3 565 mb/s	5 093 mb/s	
30,00%	0 mb/s	76 mb/s	382 mb/s	2 292 mb/s	3 819 mb/s	5 347 mb/s	7 639 mb/s	
50,00%	0 mb/s	127 mb/s	637 mb/s	3 819 mb/s	6 366 mb/s	8 912 mb/s	12 731 mb/s	

Total UL		Network bandwidth simulation for upload [Sync own+Sync share] (global ownCoRe architecture)						
	Number of users (N)							
% of active users	1	1000	5000	30000	50000	70000	100000	
5,00%	0 mb/s	5 mb/s	23 mb/s	139 mb/s	231 mb/s	324 mb/s	463 mb/s	
10,00%	0 mb/s	9 mb/s	46 mb/s	278 mb/s	463 mb/s	648 mb/s	926 mb/s	
15,00%	0 mb/s	14 mb/s	69 mb/s	417 mb/s	694 mb/s	972 mb/s	1 389 mb/s	
20,00%	0 mb/s	19 mb/s	93 mb/s	556 mb/s	926 mb/s	1 296 mb/s	1 852 mb/s	
30,00%	0 mb/s	28 mb/s	139 mb/s	833 mb/s	1 389 mb/s	1 944 mb/s	2 778 mb/s	
50,00%	0 mb/s	46 mb/s	231 mb/s	1 389 mb/s	2 315 mb/s	3 241 mb/s	4 630 mb/s	

Dimensionnement prévu pour la phase pilote CNRS

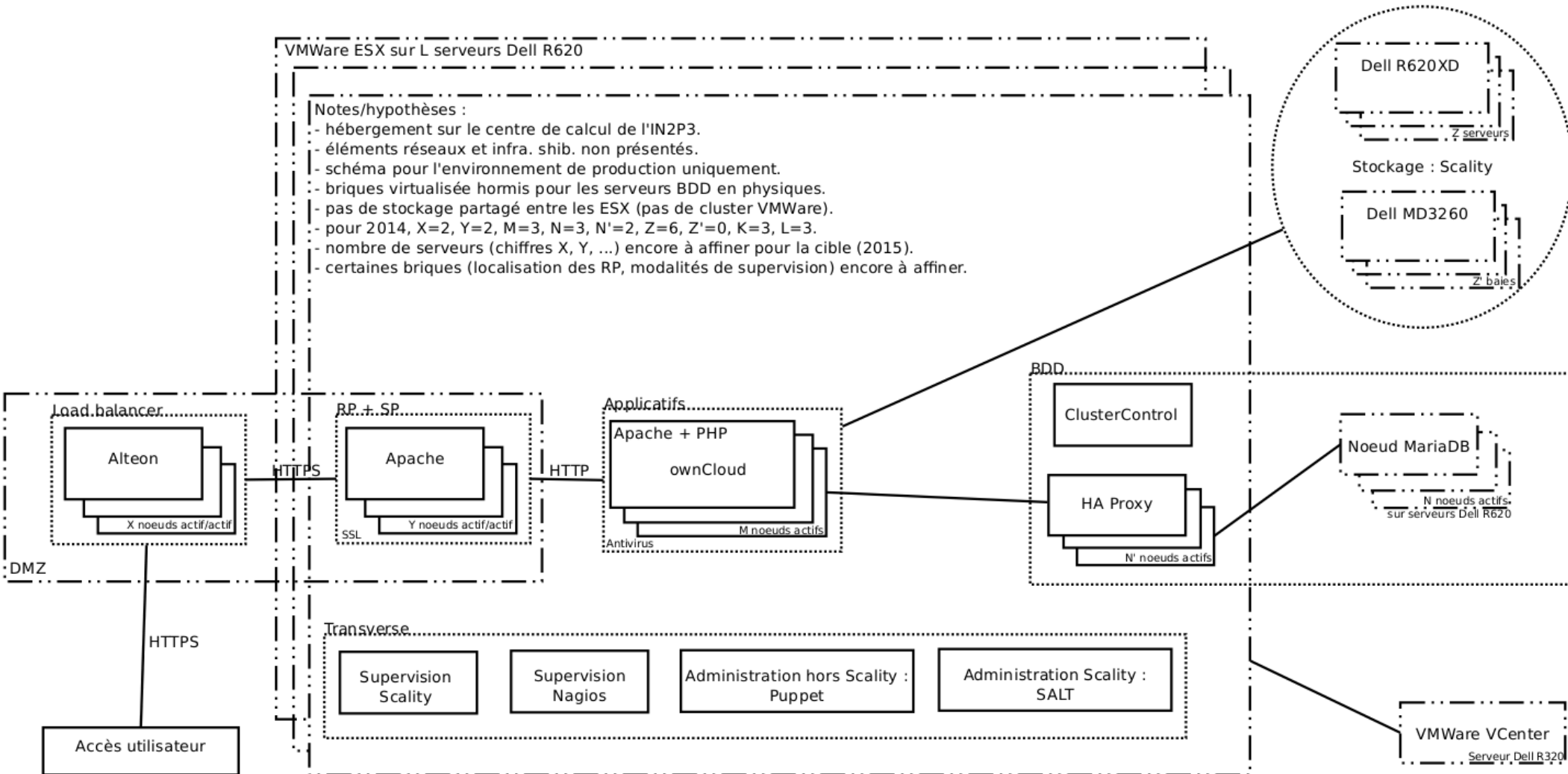
→ Ces chiffres sont issus d'un travail CNRS-LINAGORA. **Affiner les hypothèses d'usage et réaliser des optimisations matérielles et/ou logicielles** feront évoluer ce dimensionnement. La **méthode de travail** et les résultats détaillés seront rendus publics prochainement



# Plan

- ❑ Contexte du projet
- ❑ Étude d'architecture
- ❑ Étude du dimensionnement
- ❑ **Architecture cible détaillée**
- ❑ Le suite du projet, les questions

# Architecture cible détaillée







# Plan

- ❑ Contexte du projet
- ❑ Étude d'architecture
- ❑ Étude du dimensionnement
- ❑ Architecture cible détaillée
- ❑ Le suite du projet, les questions



## La suite du projet

- P. 18
- **Hébergement** de l'infrastructure au CC IN2P3 et **exploitation** assurée par BULL (prestataire assurant déjà l'exploitation d'autres briques de l'offre de services)
  - Déploiement d'un **service pilote** afin de valider les hypothèses d'usage du service, le dimensionnement prévisionnel, l'architecture proposée et le budget cible : lancer - ou non - un déploiement généralisé sur l'architecture telle que présentée
  - **Calendrier** prévisionnel
    - Juin 2014 : recette et conduite du changement
    - Juillet à septembre 2014 : **pilote** sur **2000 utilisateurs**
    - Octobre 2014 et jusqu'à fin 2014 : 1° déploiement sur **30000 utilisateurs**
    - En 2015 : objectif de déploiement sur **100000 utilisateurs**
  - **Échanger** avec la « communauté »
    - Via le web pour partager les travaux techniques réalisés en interne par la DSI jusqu'à présent (chiffres de dimensionnement, outil de tests de charge, ...)
    - Avec d'autres organismes (CERN, universités d'Aix-Marseille, de Lille3, de Nantes, de Lorraine, ...) pour confronter projets et démarches
    - Avec les personnels CNRS et de la communauté ESR, comme lors de cette journée



P. 19

# Les questions ?



*Logo prévisionnel de l'Offre De Service*

Merci de votre attention !



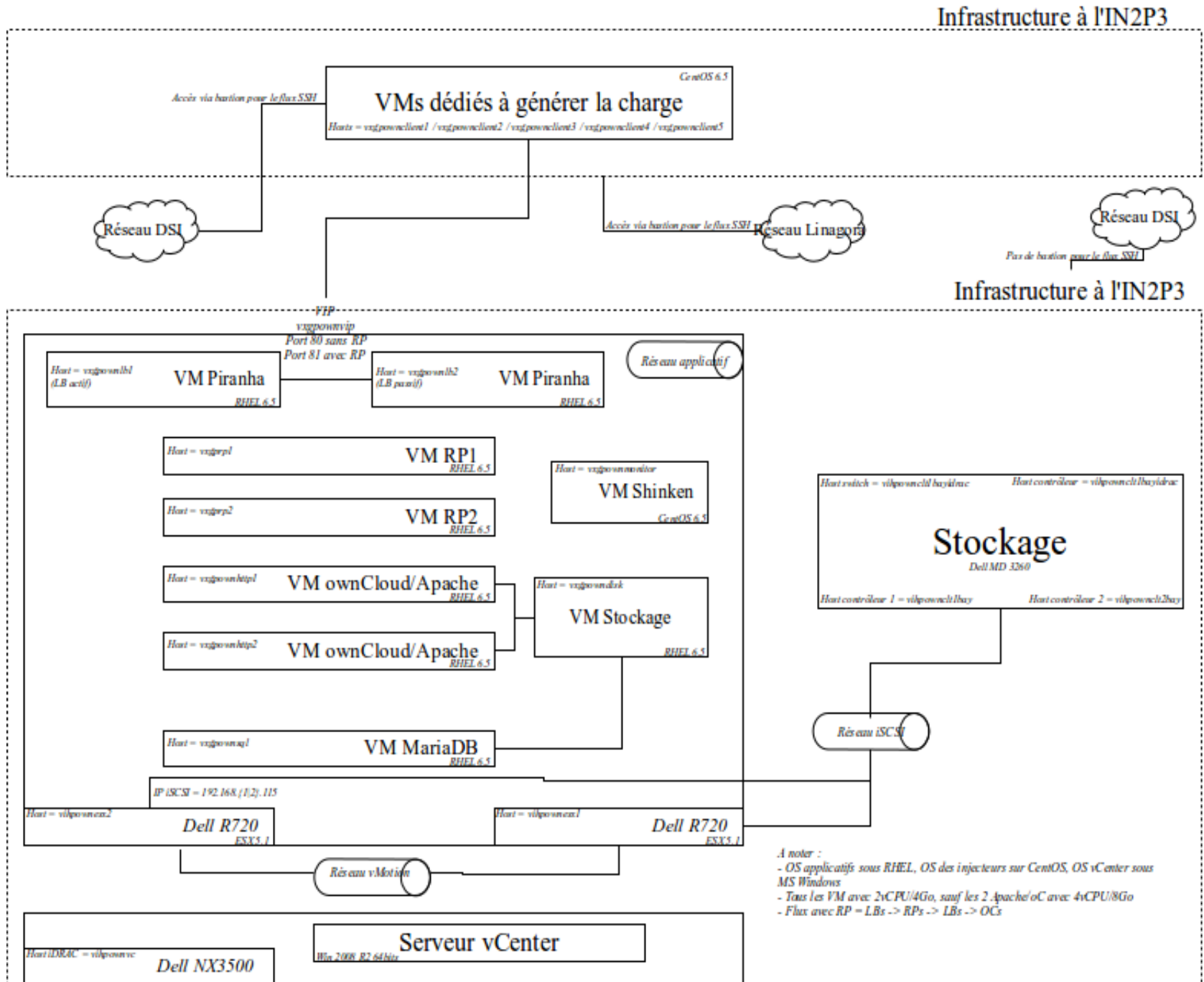
## Plan des annexes

- ❑ **Détail du contexte du projet**
- ❑ **Infrastructure des tests de charges**
- ❑ **Détails des tests de charge, basé sur Tsung**
- ❑ **Outillage de tests de charges, basé sur Tsung**
- ❑ **Pistes d'améliorations d'ownCloud**
- ❑ **Quelques liens utiles autour d'ownCloud**
- ❑ **ownCloud versus Dropbox**

## Annexe – Détail du contexte du projet

- **Nouvelle Offre De Services, ownCoRe**
  - **Objectifs**
    - Répondre à un besoin existant et identifié d'une ODS sécurisée de **partage et de synchronisation de fichiers** de travail
    - Proposer cette ODS aux membres des unités CNRS, **100 000 utilisateurs** potentiels, avec **10 Go** de volume utile par utilisateur
  - **Intérêts**
    - ODS « **anti-Dropbox** » : offre sur un cloud souverain CNRS permettant de réduire les risques d'exploitation d'informations de recherche inhérentes à des solutions « Dropbox-like »
    - ODS qui facilitera le **nomadisme**
- **Macro-étapes prévisionnelles du projet**
  - **Janvier 2013 août 2013** : expression des besoins et études préliminaires
    - *Choix d'ownCloud comme solution la plus adaptée*
  - **Septembre 2013 à avril 2014** : cadrage et validation de la solution
    - *Études des briques logiques*
    - *Tests de charge et dimensionnement*
    - *Planning et budget détaillés, définition de l'architecture cible et validation globale*
  - **Avril 2014 à juin 2014** : conception, mise en œuvre et mis en exploitation
  - **Juin 2014** : recette et conduite du changement
  - **Juillet 2014 à septembre 2014** : pilote sur 2000 utilisateurs
    - *Hébergement = CC IN2P3 - Exploitation = BULL*
  - **Octobre 2014 et jusqu'à fin 2014** : 1<sup>o</sup> déploiement sur 30000 utilisateurs
    - *Hébergement = CC IN2P3 - Exploitation = BULL*
  - **En 2015** : déploiement sur 100000 utilisateurs
    - *Hébergement = CC IN2P3 - Exploitation = BULL*

# Annexe - Infrastructure des tests de charges

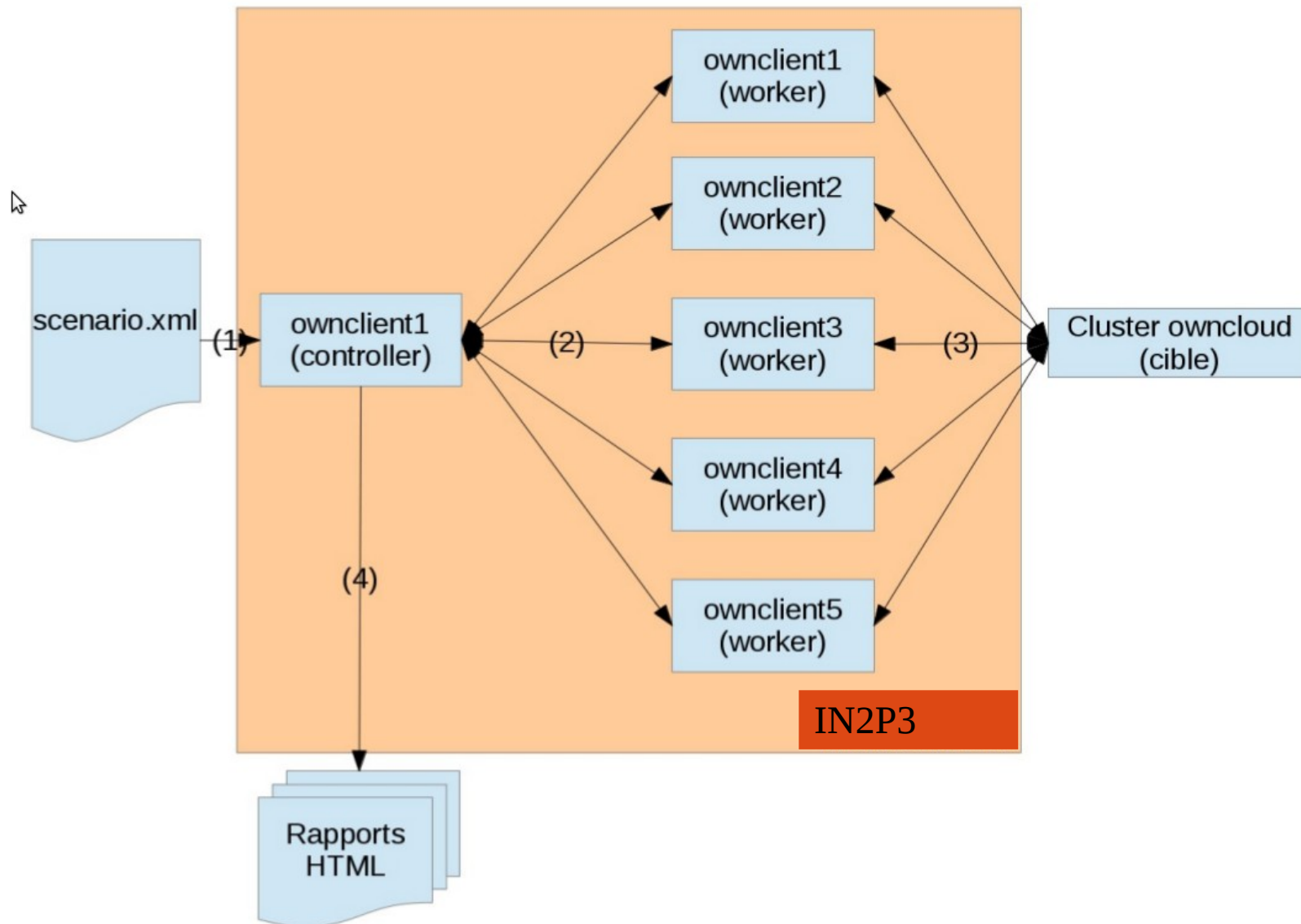


# Annexe – Détails des tests de charge, basé sur Tsung

- **Principe** des tests de charges :
  - Théoriquement, 100 serveurs Apache et 60 serveurs MariaDB sont nécessaires pour 50000 utilisateurs
  - Sur la plate-forme de tests de charges, les serveurs sont 2 fois moins puissants par rapport aux hypothèses théoriques (4 cœurs, 8Go de RAM)
  - Donc la limite pour 2 serveurs Apache et 1 serveur MariaDB devraient être de 500 utilisateurs
  
- **Scénario** des tests de charges :
  - Scénario réalisé avec l'outil **Tsung**
  - Scénario pour un fichier : **1 upload** et **4 download (5 Mo par fichier)**
  - 1 utilisateur génère 50 scenarii par jour, donc **0,0006 scenario / sec**
  
  - Donc la limite sur la plate-forme de tests devrait être : **0,3 scénario / sec**
  
- **Résultat** des tests de charges :
  - Scénario moyen par seconde : 0,261

Campaign	Shot	Theoretical limit	Result (scenario/sec)	Errors (limit reached)
1	1	0,075	N/A	Yes
1	2	0,075	0,067	No
1	3	0,075	0,108	Yes
2	1	Between 0,225 et 0,300	0,261	Yes

→ Ces tests de charges, réalisés conjointement par le CNRS et LINAGORA, confirment l'approche théorique. Optimiser le dimensionnement pourrait passer par un tuning du hardware et des évolutions du software.





# Annexe – Pistes d'améliorations d'ownCloud

- **Limitations actuelles d'ownCloud<sup>(\*)</sup>, et pistes d'améliorations**
  - **Corbeille et versionning** actuellement dépendant de l'espace de stockage restant de l'utilisateur, ce qui peut fonctionnellement être mal compris
    - amélioration possible : avoir un quota utilisateur dédié pour les fichiers mis en corbeille ou en versions N-x
  - **Optimisation des performances** via diverses pistes
    - amélioration en mettant les **métadonnées** relatives aux fichiers dans le filesystem (piste du CERN) en non en BDD
    - utiliser une BDD **NoSQL** (Cassandra, MongoDB)
    - réduire la charge liée aux **requêtes PROFIND** des clients lourds ownCloud (prévu dans la roadmap d'ownCloud)
  - **Optimisation** de la partie **LDAP** qui génère de la charge supplémentaire sur la BDD (x 1,5 environ) quand ownCloud est connecté à un annuaire LDAP
    - amélioration par ownCloud dans les versions futures ?
  - Implémentation de l'authentification **shibboleth sur le client lourd** (disponible en v1.5 mais qui semble bugguée ?)
    - tests détaillés en cours sur ownCoRe
  - Solution interne d'**antivirus** non incluse dans le cœur applicatif
    - ou faire confiance à la sécurité locale du poste ?
  - **Sécurisation** de l'outil, avec notamment ces actions
    - sécuriser le partage de liens, notamment pour les liens en écriture (par exemple aux seuls comptes authentifiés, et/ou en forçant un délai d'expiration du partage)
    - inclure une possibilité de chiffrement dans le client ownCloud
    - ne pas permettre de synchroniser un dossier géré par le client ownCloud avec d'autres outils équivalents
    - améliorer la traçabilité dans l'outil, par exemple en faisant évoluer l'app Activity
    - utiliser l'app user\_shibboleth plutôt que user\_servervars pour l'intégration à un SSO basé sur Shibboleth
    - mettre en place un flux HTTPS pour les accès, ce qui n'est pas natif par défaut dans l'outil
  - Certaines fonctions de l'**interface web** sont à améliorer : avancement de l'état lors de l'upload multiple de fichiers, suppression de gros volumes de données via le web
  - Interface de **gestion des utilisateurs** non adaptée pour une forte population
    - amélioration par ownCloud dans les versions futures de la page d'administration actuelle, ou en développer une app dédiée ? Avec une présentation par groupe, un outil de recherche

# Annexe – Quelques liens utiles autour d'ownCloud

- Offre De Services du CNRS

- Point d'entrée = <http://www.offres-de-services-unites.net/>

- Autour d'ownCloud<sup>(\*)</sup>

- Tutoriel ownCloud v5 et Shibboleth par la DSI = <https://aresu.dsi.cnrs.fr/spip.php?article187>
- Tutoriel d'installation d'ownCloud v4.5 par la DSI = <https://aresu.dsi.cnrs.fr/spip.php?article183>
- ownCloud au CERN, CERNbox = <http://indico.cern.ch/event/214784/material/slides/0?contribId=82&sessionId=6>
- Framework de tests d'ownCloud initié par le CERN = <https://github.com/opensmashbox/smashbox/blob/master/README.md>
- ownCloud à la DT INSU = <http://www.mathrice.fr/IMG/pdf/owncloud.pdf>
- ownCloud à l'IRCELYON = <http://aramis.resinfo.org/wiki/lib/exe/fetch.php?media=pleniaires:besson-l-aramis-17-04-2014.pdf>
- ownCloud à Lille3 = [http://www.min2rien.fr/wp-content/uploads/2014/02/Cedric\\_Foll\\_13022014\\_Owncloud.pdf](http://www.min2rien.fr/wp-content/uploads/2014/02/Cedric_Foll_13022014_Owncloud.pdf)
- Fiche PLUME sur ownCloud = <https://www.projet-plume.org/fiche/owncloud>
- ownCloud versus d'autres outils équivalents = <http://obtenir.cnrs.fr/images/formation/anf2013/obtenir-ANF2013-serviceenligne.pdf>
- Communauté française ownCloud = <http://www.owncloud.fr>
- ownCloud à Switch, modèle d'installation et documentation = <https://github.com/switch-ch/owncloud-ansible> et <https://github.com/switch-ch/cloudservice-owncloud>



## Annexe – ownCloud versus Dropbox

P. 27

Fonction		Dropbox	ownCloud
Synchronisation de données multi plate-formes et nomades		oui	oui
Sauvegarde (réplication de données asynchrone)		oui	oui
Partage de fichiers entre :	utilisateurs de la plate-forme	lecture	oui
		modification	oui
	extérieur à la plate-forme	lecture <sup>1</sup>	oui
		modification	oui <sup>2</sup>
groupe d'utilisateurs de la plate-forme		non	oui <sup>4</sup>
D'autres synchronisations possibles	Agendas	partiel <sup>5</sup>	oui <sup>6</sup>
	Contacts	partiel <sup>5</sup>	oui <sup>6</sup>
	Bookmarks	partiel <sup>5</sup>	oui <sup>6</sup>

1) Partage en lecture via l'envoi d'une URL, avec option mot de passe et date d'expiration.

2) Implémenté dans les faits dans Dropbox puisque devenir membre est ouvert à tous et gratuit.

3) ownCloud permet de partager des répertoires en écriture via envoi d'une URL, avec option mot de passe et date d'expiration.

4) Notion native dans ownCloud, mais la gestion de groupes d'utilisateurs reste à préciser (décorrélé des groupes de "contacts").

5) Possible via synchronisation de fichiers, mais non intégré sur le portail Web.

6) Moyennement l'installation de modules complémentaires sur le serveur et des add-ons côté clients, dont certains encore perfectibles.