Nextcloud dans la région

Centre - Val de Loire

Grégory Brousse Guillaume de Lafond Pierre Legay

Gip Recia

7 juin 2023

Contexte : Le GIP Recia

Le Groupement d'Intérêt Public Recia (Région Centre Interactive) associe plus de 500 structures publiques sur toute la Région Centre Val de Loire ;

- l'État (rectorat) ;
- La Région Centre Val de Loire
- les Conseils départementaux :
  - du Cher ;
  - de l'Indre-et-Loire ;
  - de l'Eure-et-Loir ;
  - de l'Indre ;
  - du Loir-et-Cher ;
  - et du Loiret
- les Universités de Tours et d'Orléans, l'INSA ;
- le CROUS ;
- Ciclic Centre-Val de Loire ;
- GIP e-santé Centre Val de Loire ;
- des communes et communautés de communes.

Contexte : Les activités du GIP Recia

- La maintenance informatique des Lycées, des collèges, des CFA, des EFSS ;
- Les ENT 1^{er} et 2^{nd} degrés.
- Le réseau régional haut débit (renater ReCOR) ;
- L'hébergement de données ;
- Aménagement numérique du territoire (conseil / réseaux d'initiative publique) ;
- Études, expertises, assistance, conseil, veille, animation, observatoire ;
- Économie numérique et programme transition numérique ;

Contexte : Les ENT des lycées et collèges de la région

ENT du 2^{nd} degrés de la région centre.

- multi-domaines :
  - 1 pour l'ENT des Lycées de la région ;
  - 6 pour les ENT des collèges de chaque département ;
  - 238 collèges + 101 lycées + ...
- Nombreux utilisateurs potentiels :

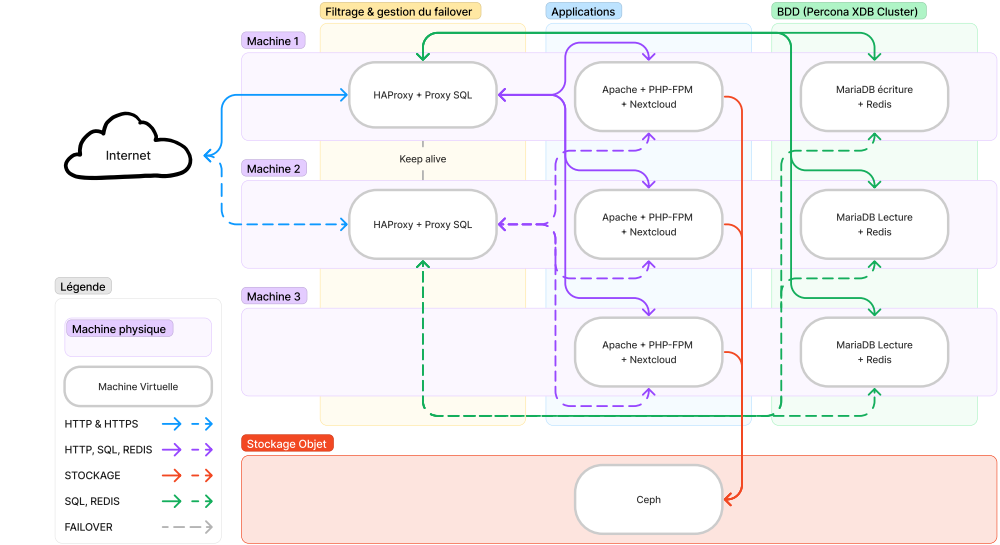
  187 000 comptes actifs ;
  192 000 Élèves ;
  16 700 Enseignants
- 61 000 Groupes : classe, groupe pédagogique, matière ...
- authentification SSO CAS.

Contexte : L'environnement applicatif

Infrastructure de production hébergée Aqua Ray Cloud for Humans (www.aquaray.com).

- OpenLdap ;
- Portail uPortal ;
- Authentification SSO CAS ;
- Grouper ;
- OnlyOffice ;
- Collabora.

Infrastructure : L'architecture



Recia

Infrastructure : Les instances de production

Deux instances de production sur la même infrastructure.

1. Pour l'ENT depuis mai 2020 (V18.0.3 ... V24.0.12)
   - 9 domaines (avec leurs CSS) ;
   - 372 établissements ;
   - 118 224 comptes actifs ;
   - 67 383 groupes ;
   - Création des comptes et groupes automatique depuis LDAP.
2. Pour le GIP Recia (V25.0.6) (extension aux collectivités locales ?)
   - Stockage NetApp ;
   - Création automatique des comptes, groupes et groupFolders.

Nos Adaptations : Plugins cssJsLoader
(Steamulo)

- Permet de charger nos propres JS et CSS ;
- Personnalisation en fonction du domaine de connexion ;
- Jusqu'en 2022 intégration en `iframe` dans le portail avec `postMessage_resize_iframe_in_parent.js` ;
- Depuis 2022 plus d'`iframe`, peut-être remplacé par l'utilisation de thème ?

Nos Adaptations : Plugins ldapImporter
(Steamulo)

- Est dérivé du plugin “CAS user and group backend” de Felix Rupp ;
- Permet l’importation des comptes à partir du LDAP ;
- Fait l’association des comptes et des groupes aux établissements ;

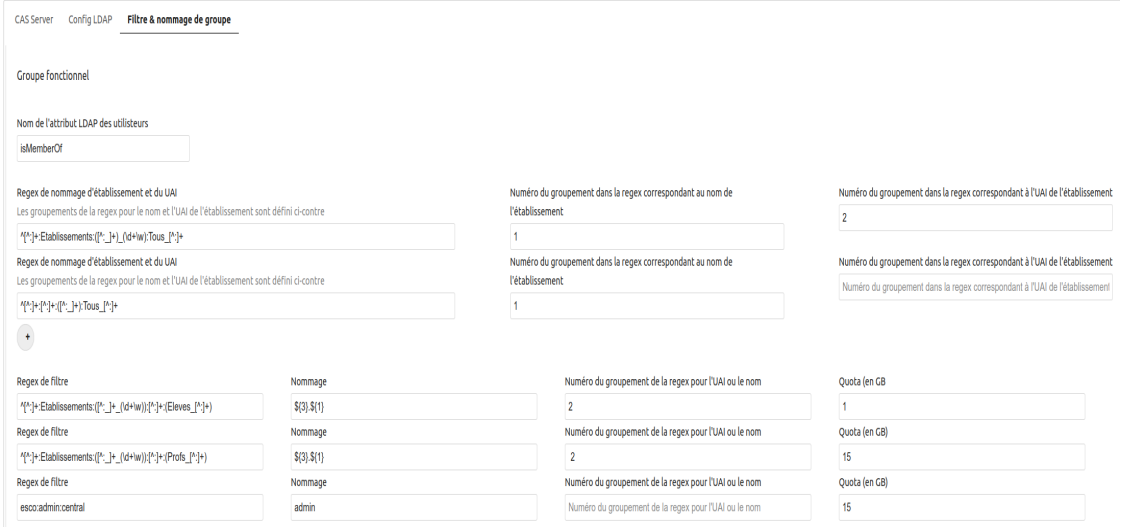
$$=> \textit{table etablissement}$$

- Filtre et traduit les groupes Grouper en groupes Nextcloud ;

$$=> \textit{table asso\_uai\_user\_group}$$

- Gère les quotas des utilisateurs en fonction des leurs groupes.

Nos Adaptations : Plugins ldapImporter



Nos Adaptations : Plugins ldapImporter

exemple de filtrage et renommage de groupe

Le groupe Grouper :

```
clg18:Etablissements:ALBERT CAMUS_0180592W:3EME:Eleves_3-2
```

satisfait la regex :

```
^[^:]+:Etablissements:([^:_]+_(\d+\w)):[^:]+:(Eleves_[^:]+)
|   ${3}.${1}  |  2
```

est réécrit pour Nextcloud en :

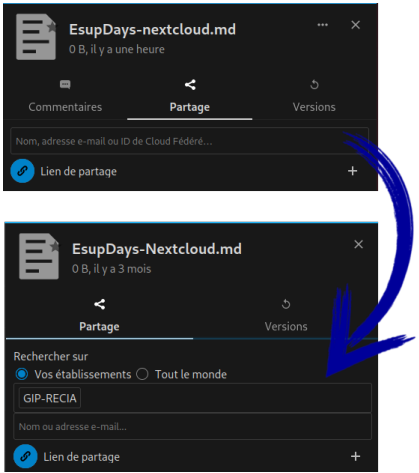
```
Eleves_3-2.ALBERT CAMUS_0180592W
```

et déduit l'appartenance de l'utilisateur à l'établissement :

```
ALBERT CAMUS_0180592W
```

Nos Adaptations : Plugin File sharing

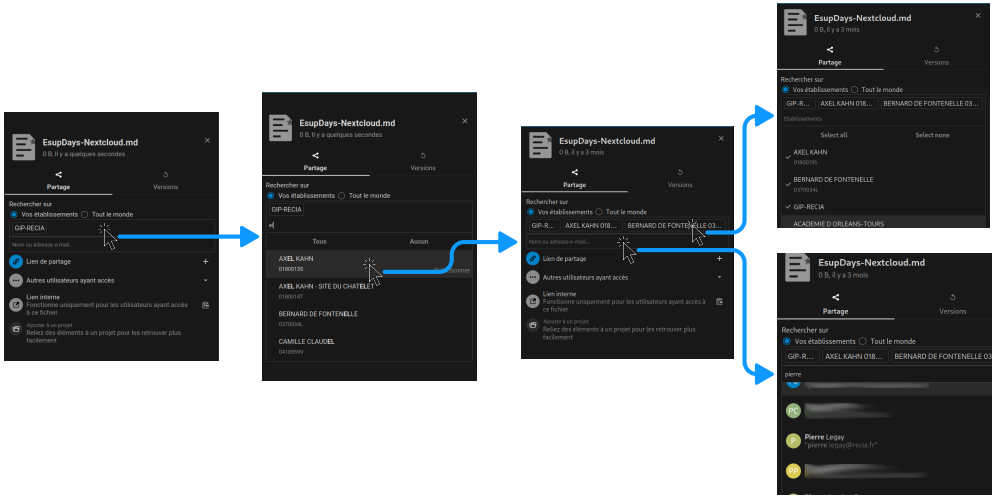
Présentation



- Facilité la recherche d'utilisateurs et de groupes pour le partage en permettant la recherche par établissement ;
- Fork de l'App File sharing de Nextcloud ;
- Backend PHP & frontend Vue JS.

Nos Adaptations : Plugin File sharing

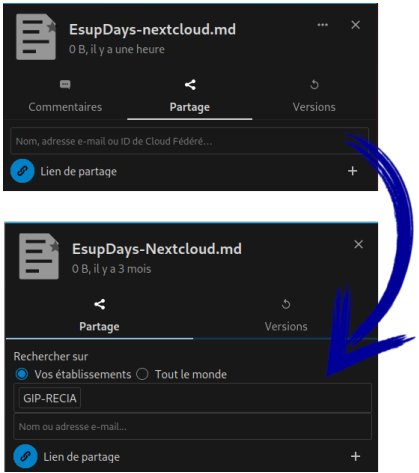
Utilisation



- 2 routes :
  - recherche d'établissements liés à l'utilisateur courant ;
  - recherche des utilisateurs et des groupes liés à un établissement.
- 1 contrôleur.

Nos Adaptations : Plugin File sharing

Frontend



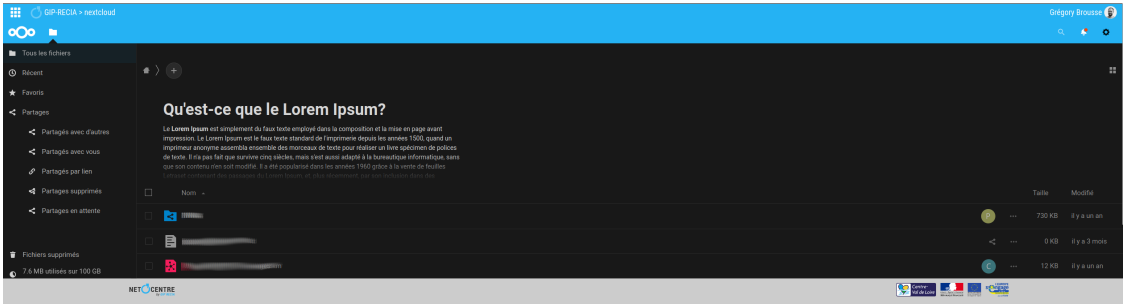
Remplacement dans la vue *SharingTab* du composant *SharingInput* par :

- boutons radios de sélection du type de recherche ;
- composant de recherche d'établissement basé sur le composant *NcMultiselect* ;
- composant dérivé du composant originel *SharingInput*.

Nos Adaptations : Bandeau ENT

Les navigateurs n'acceptant plus le cross-domaine sur les cookies de session (authentification CAS).

- Création d'un composant web simulant le portail (Extended uPortal Header) ;
- Intégration dans Nextcloud via un thème ;
- tenant compte du multi-domaine.



Les difficultés rencontrées : cluster SQL, Stockage Objet, UI ...

- Synchronisation du cluster SQL : Une lecture suivant immédiatement l'écriture peut échouer. Par exemple : A la 1^{re} connexion d'un utilisateur il y a création de son carnet d'adresse (CarDav) qui échoue parfois. $wsrep\_sync\_wait = 3$
- Le stockage objet (en V18) ; OpenIo recommandation de ne pas dépasser 500 000 objets par *bucket*. Obligation de sortir les *avatars* et les *previews* du *bucket* par défaut. (Résolut pour les *previews* dans les versions récentes `objectstore.multibucket.preview-distribution`).
- Avec le stockage objet pas de *snapshot*, comment se prémunir d'une attaque de type *ransomware* ; projet a l'étude avec Arawa.
- Le grand nombre de groupes génère un *timeout* à l'appel de la gestions des utilisateurs (pas de pagination sur les groupes)
- Pour le bandeau ENT. L'ajout d'un *header* et d'un *footer* n'est pas prévu, On est obligé de contrôlé la css de chaque page, pour le *footer*, la solution à été de le fixer et de le cacher quand on est dans la page.

Les Projets : Gestion des GroupFolders et ransomware

- Pour le Nextcloud du Recia, nous avons besoin de GroupFolders créés automatiquement à partir des groupes Grouper. Travail similaire a la gestion des groupes et utilisateurs (ldapImporter) mais en supprimant l'interface graphique mal commode pour la saisie des regexs.
- Une étude est lancée avec Arawa : comment nous prémunir des attaques du type ransomware avec le stockage Object (ceph).