



Nextcloud dans la région

Centre - Val de Loire

Grégory Brousse Pierre Legay

Gip Recia

5 juin 2023

1 Contexte

Le GIP Recia

Les ENT des lycées et collèges de la région

L'environnement applicatif

2 Infrastructure Nextcloud

L'architecture

Les instances de production

3 Nos Adaptations

Plugins cssJsLoader, ladplImporter

Plugin files_sharing

Bandeau ENT

4 Les difficultés rencontrées

Stockage Object

UI groupes et intégration ENT

Le GIP Recia

Le Groupement d'Intérêt Public RECIA (Région Centre Interactive) associe :

- l'État (rectorat),
- plus de 500 structures publiques sur toute 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 Bourge,
- le CROUS,
- Ciclic Centre-Val de Loire,
- GIP e-santé Centre Val de Loire,
- des communes et communautés de communes.

Les activités du GIP Recia

- 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
- La maintenance informatique des Lycées, des collèges, des CFA, des EFSS
- Les ENT 1^{er} et 2nd degrés

Les ENT des lycées et collèges de la région

ENT du 2nd degrés de la région centre.

- multi-domaines

ENT des Lycées de la région.

1 ENT par départements de la région pour les collèges (6).

238 collèges + 101 lycées + ...

- Nombreux utilisateurs potentiels :


187 000 comptes actifs,

192 000 Élèves,

16 700 Enseignants

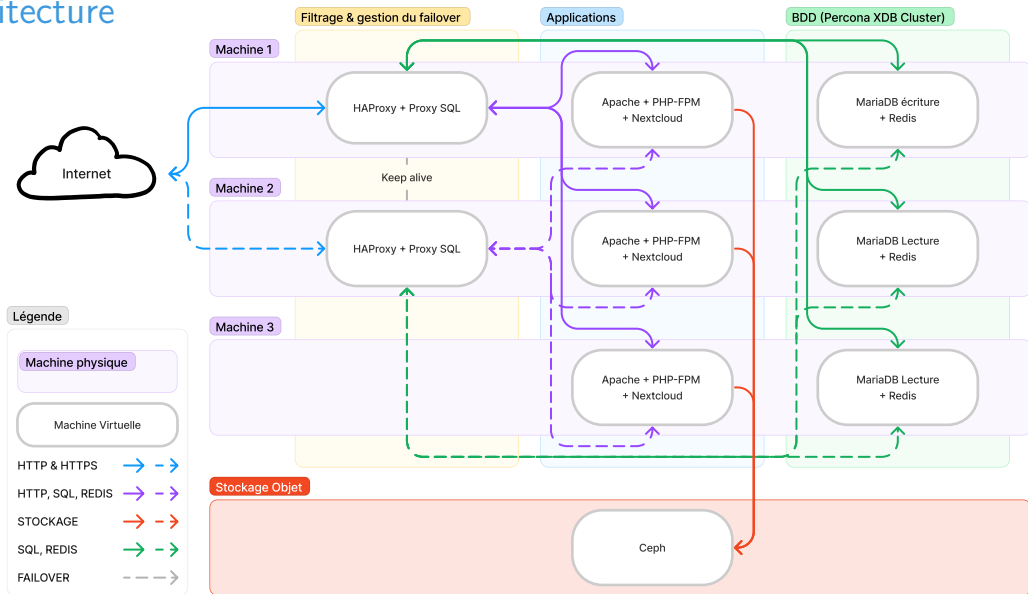
- 61 000 Groupes : classe, groupe pédagogique, matière ...
- authentification CAS

L'environnement applicatif

Infrastructure de production hébergé  AquaRay (www.aquaray.com).

- OpenLdap
- ENT UPortal
- Authentification SSO CAS
- Grouper
- OnlyOffice (via NC)
- Collabora (via NC)
- Moodle

L'architecture



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 groupFolder ;

Plugin 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 ?

Plugin 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 ;

=> *table etablisement*

- Filtre et traduit les groupes Grouper en groupes Nextcloud

=> *table asso_uai_user_group*

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

Plugin Idapimporter

CAS Server Config LDAP Filtre & nommage de groupe

Groupe fonctionnel

Nom de l'attribut LDAP des utilisateurs

isMemberOf

Regex de nommage d'établissement et du UAI

Les groupements de la regex pour le nom et l'UAJ de l'établissement sont défini ci-contre

`^{[^\-]*}+Etablissements:([^\-]*_)(d+lw).Tous_[^\-]*+`

Regex de nommage d'établissement et du UAI

Les groupements de la regex pour le nom et l'UAJ de l'établissement sont défini ci-contre

`^{[^\-]*}+{[^\-]*}+([^\-]*_).Tous_[^\-]*+`

+

Regex de filtre

`^{[^\-]*}+Etablissements:([^\-]*_)(d+lw);[^\-]*+.(Elevés_[^\-]*+)`

Regex de filtre

`^{[^\-]*}+Etablissements:([^\-]*_)(d+lw);[^\-]*+.(Profes_[^\-]*+)`

Regex de filtre

esco:admin:central

Nommage

`$(3).$(1)`

Nommage

`$(3).$(1)`

Nommage

admin

Numéro du groupement dans la regex correspondant au nom de l'établissement

1

Numéro du groupement dans la regex correspondant au nom de l'établissement

1

Numéro du groupement dans la regex correspondant à l'UAJ de l'établissement

2

Numéro du groupement dans la regex correspondant à l'UAJ de l'établissement

Numéro du groupement dans la regex correspondant à l'UAJ de l'établissement

Numéro du groupement de la regex pour l'UAJ ou le nom

2

Numéro du groupement de la regex pour l'UAJ ou le nom

2

Numéro du groupement de la regex pour l'UAJ ou le nom

Numéro du groupement de la regex pour l'UAJ ou le nom

Quota (en GB)

1

Quota (en GB)

15

Quota (en GB)

15

Plugin Idapimporter

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 Nexcloud en :

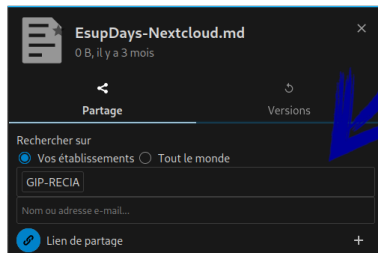
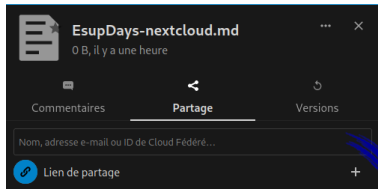
```
Eleves_3-2.ALBERT CAMUS_0180592W
```

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

```
ALBERT CAMUS_0180592W
```

Plugin files_sharing

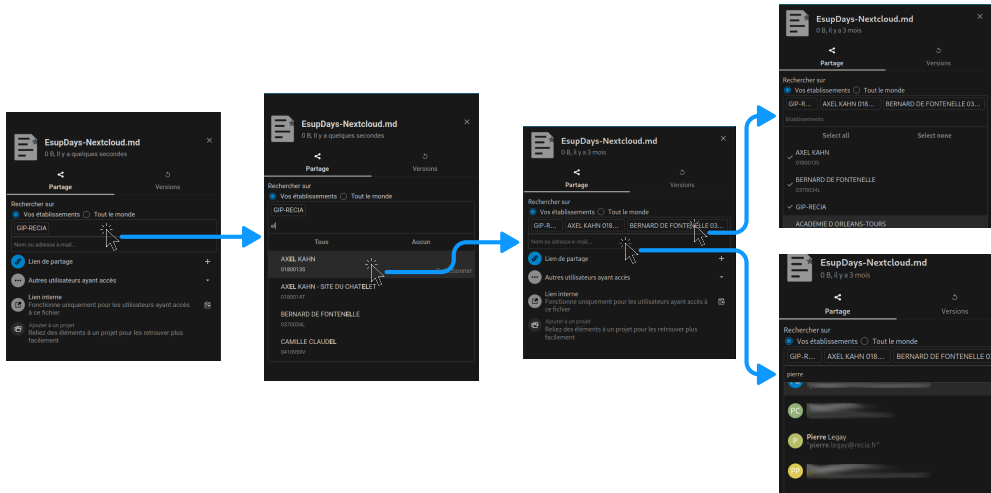
Présentation



- 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

Plugin files_sharing

Utilisation



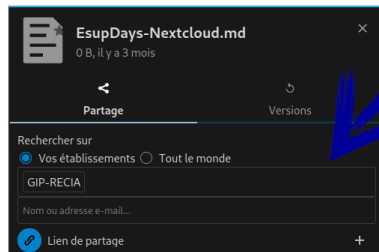
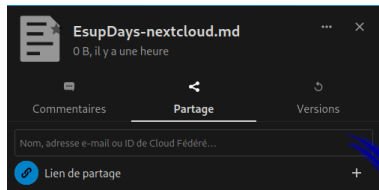
Plugin files_sharing

Backend

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

Plugin files_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*

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

- Création d'un composant web simulant le portail (à la prolongation_ent)
- Intégration dans NC via un thème.
- tenant compte du multi-domaines

Les difficultés rencontrées

- Le grand nombre de groupes génère un `jj time out` à l'appel de la gestion des utilisateurs (pas de pagination sur les groupes)
- Le stockage object (en V18); Openlo recommandation de ne pas dépasser 500 000 objets par "buckets". Obligation de sortir les "avatars" et "previews" du bucket par défauts. (Résolus pour les previews dans les versions récentes `jjobjectstore.multibucket.preview – distribution`).
- Avec le stockage object pas de `jjsnapshot`, comment se prémunir d'une attaque de type `jjransomware` = projet à l'étude avec Arawa.