

# GROUPER

## Sommaire



- Grouper, pour quoi faire ?
- Pourquoi gérer des groupes ?
- Grouper d'un peu plus près...
- Architecture technique de Grouper
- Communauté Grouper
- Cas Lille1 avec publication dans l'annuaire Idap

# GROUPER

Pour quoi faire ?

Gérer des groupes ?

(ca doit être drôlement simple...m'enfin !)

 eh, méfies-toi quand même des choses qui paraissent simples...

# GROUPER

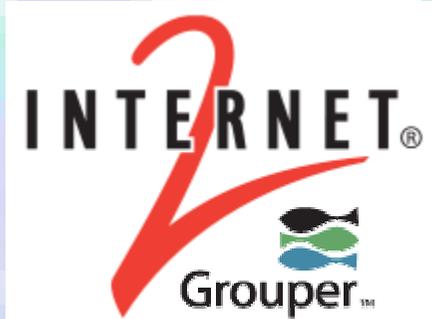
## Pour quoi faire ?



- Créer des groupes
- Les hiérarchiser dans une structure de répertoires
- Leur affecter des membres
- Les typer et leur ajouter des attributs
- Les combiner (groupes composites)
- Les exporter (liste tableur par ex) - les publier (dans ldap par ex)
- Déléguer leur gestion

# GROUPER

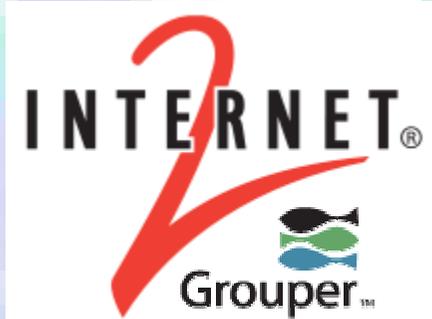
Pour quoi faire ?



- Partager les mêmes groupes, un référentiel unique pour éviter les oublis
- Ne pas refaire chaque groupe dans chaque application
- Donner la main aux usagers sur la gestion de leurs propres groupes.

# GROUPER

Pour quoi faire ?



Finalelement, gérer des groupes, cela paraît assez simple, non?...  
....enfin a priori...

Et une simple petite base de données,  
ce ne serait pas suffisant ?

 ou ne serait-ce pas comme gérer un agenda : cela semble simple et commun mais à la mise en oeuvre, ca se corse ???!!!!..)

# GROUPER

Pourquoi gérer des groupes ?

# GROUPER

## Pourquoi gérer des groupes ?



- Un certain nombre d'applications utilisent la notion de groupes
- Cependant, elles sont diverses et leur gestion des groupes aussi : redondances voire incohérences...
- Le projet Grouper mené au niveau global dans une université nécessite de tout remettre à plat et **établir un référentiel**. (moins efficace de ce point de vue, il peut aussi être mené partiellement (cf cas Lille1))
- Les applications pourront communiquer avec Grouper de différentes façons, par webservices par exemple, ou via l'annuaire ldap-supann dans le contexte universitaire français.

# GROUPER

## Pourquoi gérer des groupes ?



- La hiérarchie des groupes augmente et se complexifie au fur et à mesure que les services numériques augmentent
- Comment les ranger ?
- Qui a le droit d'administrer quelle branche ?
- Qui va maintenir et vérifier la cohérence des délégations de droit ?

# GROUPER

## Pourquoi gérer des groupes ?



- Un projet à part entière car
  - **Sensible** car derrière les groupes, il y a le **contrôle d'accès** à des applications et des informations qui peuvent être sensibles (confidentielles, financières, internes, etc)
  - Il constitue une **brique de base** du SI
  - Nécessite d'interagir avec nombre de personnes
  - **Projet technique**
  - Pas trivial à mettre en place
  - **Nouveau**
  - **Transversal**

# GROUPER

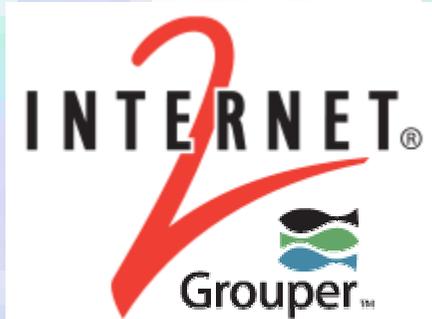
d'un peu plus près...

Oulala... ca commence un peu à me faire peur cht'histoire...

 eh, attends un peu de voir la suite mon gars...

# GROUPER

d'un peu plus près...

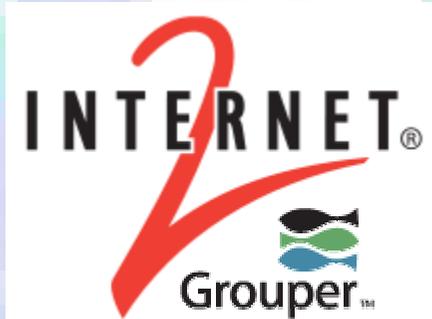


Faciliter la délégation grâce aux :

- Autorisations sur les répertoires / les groupes : create folder/create group
- Autorisations sur le groupe : admin/update/read/view/optin/optout
- Groupes composites : groupes dont les membres sont l'union/ l'intersection / complément de 2 autres groupes : ce qui permet de déléguer aux usagers adéquats sur la seule partie d'un groupe qui les concerne

# GROUPER

d'un peu plus près...



Des outils pour l'administrateur :

- Typage des groupes, un type peut porter un ou plusieurs attributs : technique qui permet une certaine indépendance par rapport à la hiérarchie des groupes / répertoires créés : travail sur les groupes de tel ou tel type quel que soit la branche.
- Auditer l'activité : permet de savoir qui a accès à quoi, qui a fait quoi sur quel groupe/répertoire.
- Point to time : savoir qui avait le droit sur quoi à un instant t (depuis la version 2.0)

EXEMPLES...

# GROUPER

d'un peu plus près...

Vous êtes actuellement sur :

 Root: 
  lille1: 
  utilitaires: 
  acces intranet TEST

<u>Name</u>	acces intranet TEST										
<u>Path</u>	lille1:utilitaires:acces intranet TEST										
<u>Description</u>	Ceux qui auront acces a l'intranet TEST										
<u>ID</u>	accesintranetest										
<u>ID Path</u>	lille1:utilitaires:accesintranetest										
<u>Alternate ID Path</u>											
<u>UUID</u>	bbb49b3180b94d5da96a875d512ff9a8										
<u>Types</u>	<table border="1"> <tr> <td>base</td> <td>members</td> <td>List field</td> </tr> <tr> <td>PortailEsup</td> <td>esup-groupKey</td> <td>IntranetTest</td> </tr> <tr> <td></td> <td>esup-groupName</td> <td>Groupe Intranet Test</td> </tr> </table>	base	members	List field	PortailEsup	esup-groupKey	IntranetTest		esup-groupName	Groupe Intranet Test	
base	members	List field									
PortailEsup	esup-groupKey	IntranetTest									
	esup-groupName	Groupe Intranet Test									

Groupe nommé « acces intranet TEST »

Exemple d'un type de groupe nommé « PortailEsup » portant 2 attributs de type string : esup-groupKey et esup-groupName

Voir qui a quel privilège sur le groupe

Regarder l'activité sur le groupe

Show entities with ADMIN privilege

[Delete](#)
[Add to Group workspace](#)
[Edit group](#)
[Edit attributes](#)
[Manage members](#)
[Add members](#)
[Manage members lite](#)
[Move group](#)
[Copy group](#)
[Audit log](#)

[View entity details](#)

# GROUPER

d'un peu plus près...

## Création d'un groupe composite

**Create composite group** ⓘ

Vous êtes actuellement sur :

📁 Root: 📁 lille1: 📁 utilitaires: 👤 EtudiantsNonDoctorants

Left group	<input type="text" value="lille1:utilitaires:Etudiants:TousLesEtudiantsComptesValides"/>
Type	<input type="text" value="not (complement)"/>
Right group	<input type="text" value="lille1:utilitaires:Etudiants:lesDoctoirants"/>

**Create composite group**

# GROUPER

d'un peu plus près...



Des outils pour l'administrateur :

- Un grouper-shell très puissant : permet de réaliser des opérations automatiques (ex : peupler un groupe SIFAC)
- L'API de Grouper disponible, par exemple :
  - `addMember(group, subject id)` : ajouter un membre à un groupe
  - `typeAdd(name)` : ajouter un type de groupe
  - `GroupFinder.findByAttribute(grouperSession, « nom_attribut », « valeur_attribut », booléen)`

```
.....
peuplerSifacCumul.gsh
.....
import java.io.*;

// pour surveiller ce qui est fait
final String outputFileName="/home/rester/Grouper/shellsLille1/resultPeuplerSifacCumul.txt";
PrintWriter output = new PrintWriter(new File(outputFileName));

// Ouverture d'une session grouper.
grouperSession = GrouperSession.startRootSession();

// selection du groupe sifac-cumul
g = GroupFinder.findByAttribute(grouperSession,"ustlRole","SIFAC-cumul-users",true);

InputStream ips=new FileInputStream("/home/rester/Grouper/shellsLille1/sifacroles.txt");
InputStreamReader ipsr=new InputStreamReader(ips);
BufferedReader br=new BufferedReader(ipsr);

while ((ligne=br.readLine())!=null) { try { uid=ligne.substring(2); sujet=SubjectFinder.findById(uid,true); action=ligne.substring(0,1); output.p
rintln(ligne); if (action.equals("A")) { g.addMember(sujet,false); } else { if (action.equals("S")) { g.deleteMember(sujet,false); } } } catch (E
xception e){ output.println(e.toString()); } } ;

br.close();
output.flush();
output.close();
```

WOR	Actuel
Position	100
Exes	6 / 430
Time	00:00:00
CON	1228 / 452
Mise en evidence	
Tags	
TAG	Reduction Inflation

# GROUPER

## Architecture technique

# GROUPER

## Architecture technique



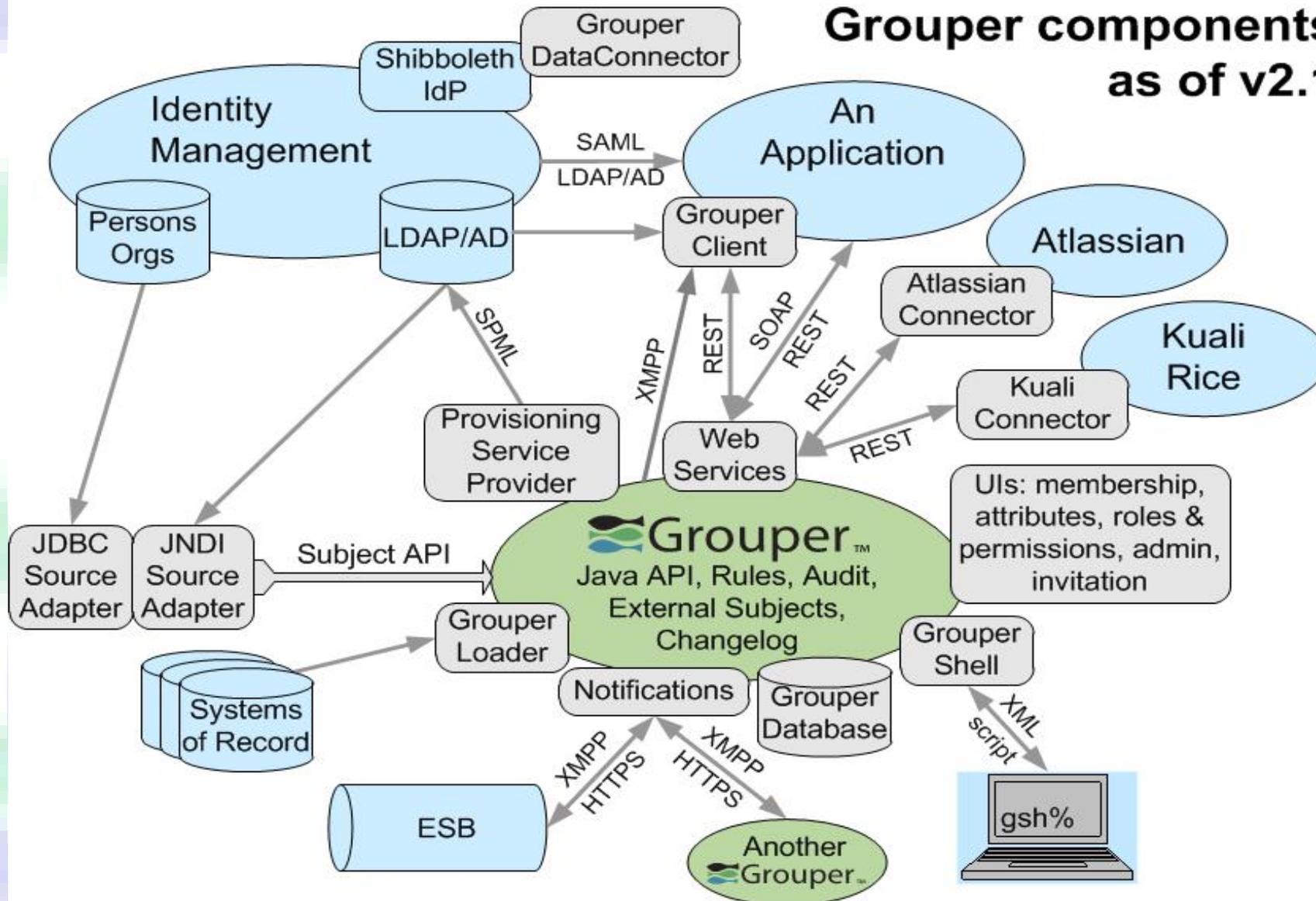
- Prérequis : java /database (postgresql, mysql, oracle, etc) (grouperAPI) / ant+servlet container (tomcat par ex)+webserver (apache par ex)
- Modularité : Grouper-API, Grouper-UI et lite-UI, web services, subjectAPI, etc
- Outils : grouper-shell, grouper-loader, grouper-client, Idappcng remplacé par psp (provisioning service provider)
- Beaucoup de notions à appréhender : stem, folder, group, include/exclude Group, requireGroup, privilege, subject, hook, composite, ...

# GROUPER

## Architecture technique

Comme au marché,  
Ne prenez que ce qui vous intéresse...

### Grouper components as of v2.1

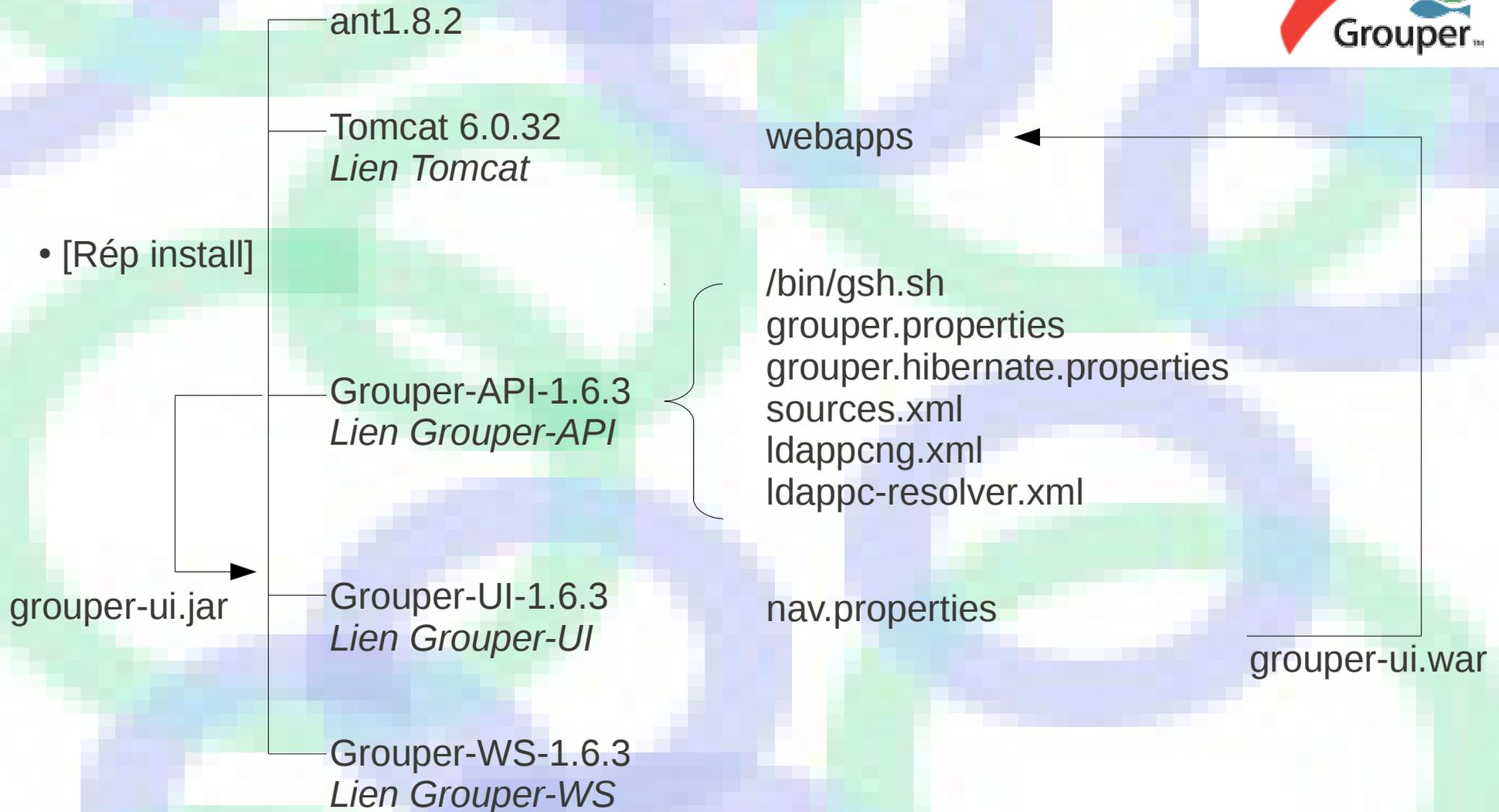


## 2 interfaces disponibles :

- AdminUI
  - Basé sur Struts
  - Réservé aux administrateurs
- LiteUI (démonstration)
  - Basé sur Ajax
  - Pour les utilisateurs

# GROUPER

## Architecture technique - Lille1



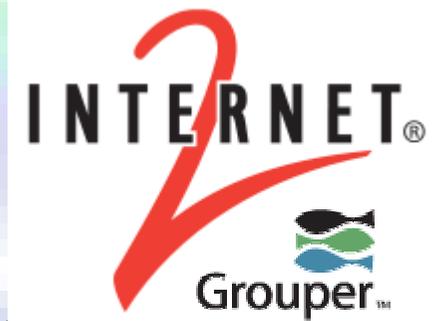
- /etc/apache2/sites-enabled/vh-grouper : AdminUI + Grouper-WS protégés par ip
- Base postgresql sur serveur dédié

# GROUPER

Communauté

# GROUPER

## Communauté



- Internet2 : consortium à but non lucratif créé en 1996
- Regroupant plus de 350 membres dont plus de 200 universités américaines
- Et des partenaires industriels et gouvernementaux
- 66000 institutions représentant plus de 50 pays
- Pour développer les technologies pour atteindre le très haut débit
- Mais aussi pour développer des applications pour l'apprentissage et la recherche
- les services InCommon pour fournir un espace de confiance sécurisé (Shibboleth et COrmanage).

# GROUPER

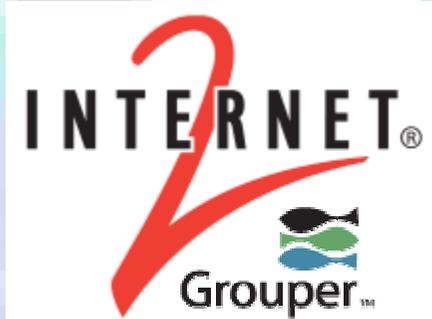
## Communauté



- Projet Grouper initié en juin 2001
- 24 institutions identifiées utilisent Grouper en production : des universités américaines, françaises, anglaises, allemandes, sud-africaines.
- 125 institutions ont téléchargé le logiciel Grouper depuis mars 2010
- Beaucoup de pays concernés : Canada, République Tchèque, Italie, Japon, Pays-bas, Pologne, Suède

# GROUPER

Communauté



- **Sa force est dans sa communauté !**
- Un wiki actif – une roadmap clairement indiquée
- Des ressources qui se développent : installateur, vidéos, retour d'expérience
- Une liste mail active et réactive, une communauté y compris les développeurs à l'écoute et qui évolue sans cesse.
- Des institutions parties prenantes (internet2, université de Chicago, université de Bristol, le NSF américain), ce qui garantit une non-commercialisation de l'outil.  
(fonctionnement bien différent des outils adossés à des sociétés...)

# GROUPER

## Cas Lille1

# GROUPER

## Cas Lille1

- Les services web offerts à nos étudiants et nos personnels se multiplient
- Les outils développés sont très diversifiés : relevé de notes, budget de la composante, gestion des congés, emplois du temps, etc
- Notre portail/ENT offre tous ces services mais il doit les cibler vers la sous-population concernée
- Il faut pouvoir déléguer l'administration de ces sous-populations

# GROUPER

## Cas Lille1



- La gestion électronique de documents amène à partager ces ressources entre groupes de travail
- Ces groupes de travail sont à géométrie variable et évolutifs dans le temps
- Là encore, il faut pouvoir déléguer la gestion de ces groupes et notamment leur peuplement/dépeuplement

# GROUPER

## Cas Lille1



- Projet Grouper mené d'avril à novembre 2011 par le pôle Web-ent du CRI
- Pour ses propres besoins qui devenaient urgents et dans l'attente d'une réflexion plus globale au niveau de l'université
- Ce qui a permis finalement de gagner en compétence sur le sujet et permettra de mieux appréhender une éventuelle généralisation
- Ne pas révolutionner l'existant...en tout cas, pas dans un 1er temps.

# GROUPER

## Cas Lille1



- 3 applications à servir :
  - portail (esup-portail)
  - CMS (infoglue)
  - GED (nuxeo)

La connexion directe applis ↔ Grouper plus tard

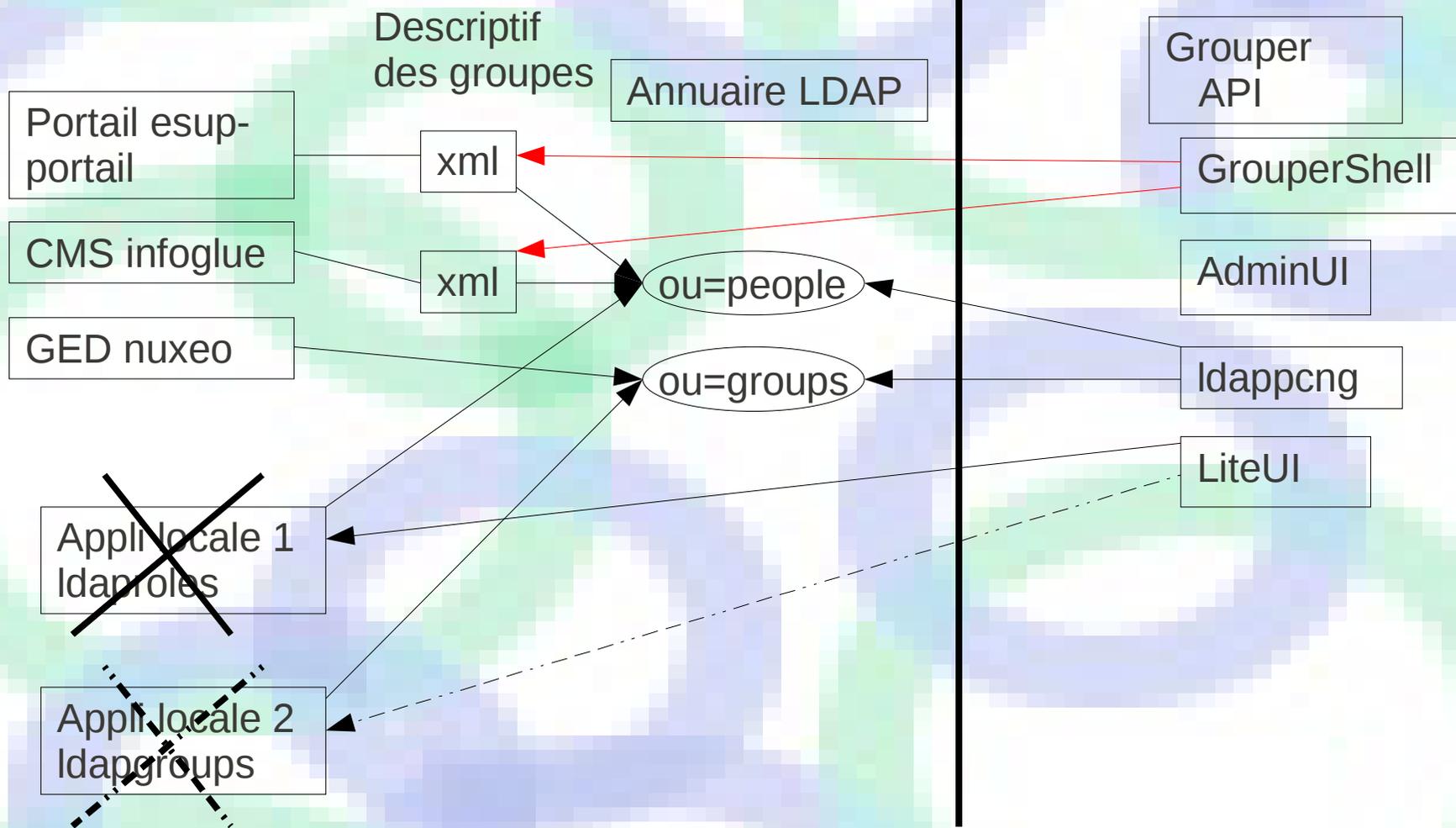
- 2 applications locales à remplacer :
  - « Gestion des rôles par le Idap »
  - « Idapgroup » pour gérer les groupes pour l'application gérant l'avancement des E/C -2e tps

# GROUPER

## Cas Lille1



### L'EXISTANT



# GROUPER

## Cas Lille1



- Configuration Idappcng : synchronisation Grouper vers l'annuaire Idap
- 2 fichiers principaux « pilotent » cette publication
- Publication 1 fois par heure en attendant psp (publication real-time et incrémentale (v2.1)) car Grouper interroge Idap pour faire un diff avant de publier → gourmand !
- Donc pas de publication de groupes volumineux (par ex, pas de généralisation de groupes d'étudiants... 20000 étudiants...) ;-(

- Exemple : publication des groupes portant un attribut « ustlRole » dans la branche ou=people
- Extrait ldappcng.xml :

```
<object id="member">
```

```
  <identifier ref="member-dn" baseId="{peopleOU}">  
    <identifyingAttribute name="objectClass" value="eduPerson" />  
  </identifier>  
  <attribute name="ustlRole" ref="memberIsMemberOf" />
```

```
</object>
```

- Extrait ldappc-resolver.xml :

```
<resolver:DataConnector id="MemberDataConnector"  
xsi:type="grouper:MemberDataConnector">
```

```
<grouper:GroupFilter xsi:type="grouper:ExactAttribute"  
name="PubLDAPPeople" value="ustlRole"/>
```

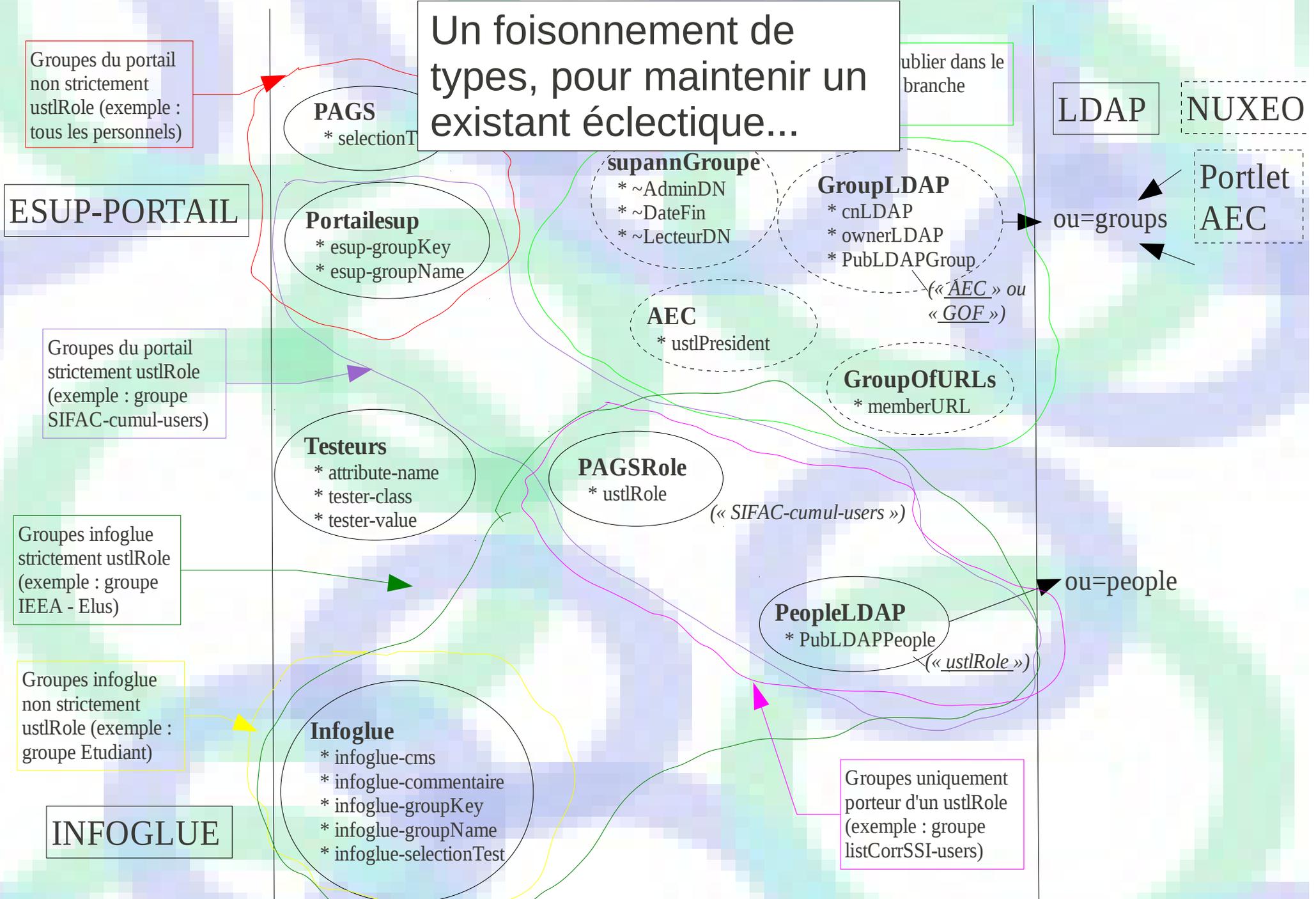
```
  <grouper:Attribute id="groups" />
```

```
</resolver:DataConnector>
```

Publication dans ldap : bien s'asseoir pour bien y réfléchir...

J'ai publié une page qui détaille et explique les publications ldappcng pas triviales...

# Un foisonnement de types, pour maintenir un existant éclectique...



**Notas** : Aucune dépendance entre les types – tous les attributs sont facultatifs (problèmes quand obligatoires) – être vigilant lors de la déclaration des types et de leurs attributs car pas de contrôle - « ... » : exemple de valeurs de l'attribut / « ... » : seules valeurs prises en compte actuellement par les scripts de publication dans le ldap. Ronds et rectangle en tiret : types non encore en exploitation, certains utilisés en ldap de test.

**tous les personnels du campus**

<b>Name</b>	tous les personnels du campus												
<b>Path</b>	lille1:utilitaires:Personnels:tous les personnels du campus												
<b>Description</b>	Tout le personnel du campus												
<b>ID</b>	tous												
<b>ID Path</b>	lille1:utilitaires:personnels:tous												
<b>Alternate ID Path</b>													
<b>UUID</b>	4ba01c34af424724afba983e1de70e3f												
<b>Types</b>	<table border="1"> <tr> <td><b>base</b></td> <td>members <i>List field</i></td> </tr> <tr> <td><b>PAGS</b></td> <td>selectionTest <i>List field</i></td> </tr> <tr> <td><b>GroupLDAP</b></td> <td> <b>cnLDAP</b> lille1:utilitaires:personnels:grouper-TousPers  <b>ownerLDAP</b>  <b>PubLDAPGroup</b> GOF         </td> </tr> <tr> <td><b>GroupOfURLs</b></td> <td> <b>memberURL</b> ldap://ldap.univ-lille1.fr/ou=people,dc=univ-lille1,dc=fr??sub?(&amp;(ntPassword=*)(&amp;(objectClass=ustlPerson)(!(objectClass=ustlExtPerson)(!(objectClass=ustlService))(objectClass=ustlAffilPerson)))         </td> </tr> <tr> <td><b>PortailEsup</b></td> <td> <b>esup-groupKey</b> TousPers  <b>esup-groupName</b> LDAP Tout le personnel         </td> </tr> <tr> <td><b>Infoglue</b></td> <td> <b>infoglue-cms</b> true  <b>infoglue-commentaire</b> Group 1: "Personnel" - PAGS - Role personnel  <b>infoglue-groupKey</b> 1  <b>infoglue-groupName</b> Personnel  <b>infoglue-selectionTest</b> <i>List field</i> </td> </tr> </table>	<b>base</b>	members <i>List field</i>	<b>PAGS</b>	selectionTest <i>List field</i>	<b>GroupLDAP</b>	<b>cnLDAP</b> lille1:utilitaires:personnels:grouper-TousPers <b>ownerLDAP</b> <b>PubLDAPGroup</b> GOF	<b>GroupOfURLs</b>	<b>memberURL</b> ldap://ldap.univ-lille1.fr/ou=people,dc=univ-lille1,dc=fr??sub?(&(ntPassword=*)(&(objectClass=ustlPerson)(!(objectClass=ustlExtPerson)(!(objectClass=ustlService))(objectClass=ustlAffilPerson)))	<b>PortailEsup</b>	<b>esup-groupKey</b> TousPers <b>esup-groupName</b> LDAP Tout le personnel	<b>Infoglue</b>	<b>infoglue-cms</b> true <b>infoglue-commentaire</b> Group 1: "Personnel" - PAGS - Role personnel <b>infoglue-groupKey</b> 1 <b>infoglue-groupName</b> Personnel <b>infoglue-selectionTest</b> <i>List field</i>
<b>base</b>	members <i>List field</i>												
<b>PAGS</b>	selectionTest <i>List field</i>												
<b>GroupLDAP</b>	<b>cnLDAP</b> lille1:utilitaires:personnels:grouper-TousPers <b>ownerLDAP</b> <b>PubLDAPGroup</b> GOF												
<b>GroupOfURLs</b>	<b>memberURL</b> ldap://ldap.univ-lille1.fr/ou=people,dc=univ-lille1,dc=fr??sub?(&(ntPassword=*)(&(objectClass=ustlPerson)(!(objectClass=ustlExtPerson)(!(objectClass=ustlService))(objectClass=ustlAffilPerson)))												
<b>PortailEsup</b>	<b>esup-groupKey</b> TousPers <b>esup-groupName</b> LDAP Tout le personnel												
<b>Infoglue</b>	<b>infoglue-cms</b> true <b>infoglue-commentaire</b> Group 1: "Personnel" - PAGS - Role personnel <b>infoglue-groupKey</b> 1 <b>infoglue-groupName</b> Personnel <b>infoglue-selectionTest</b> <i>List field</i>												

Exemple d'un groupe très typé (5 types) car utilisé dans beaucoup d'applications avec des noms parfois différents (maintenir l'existant)

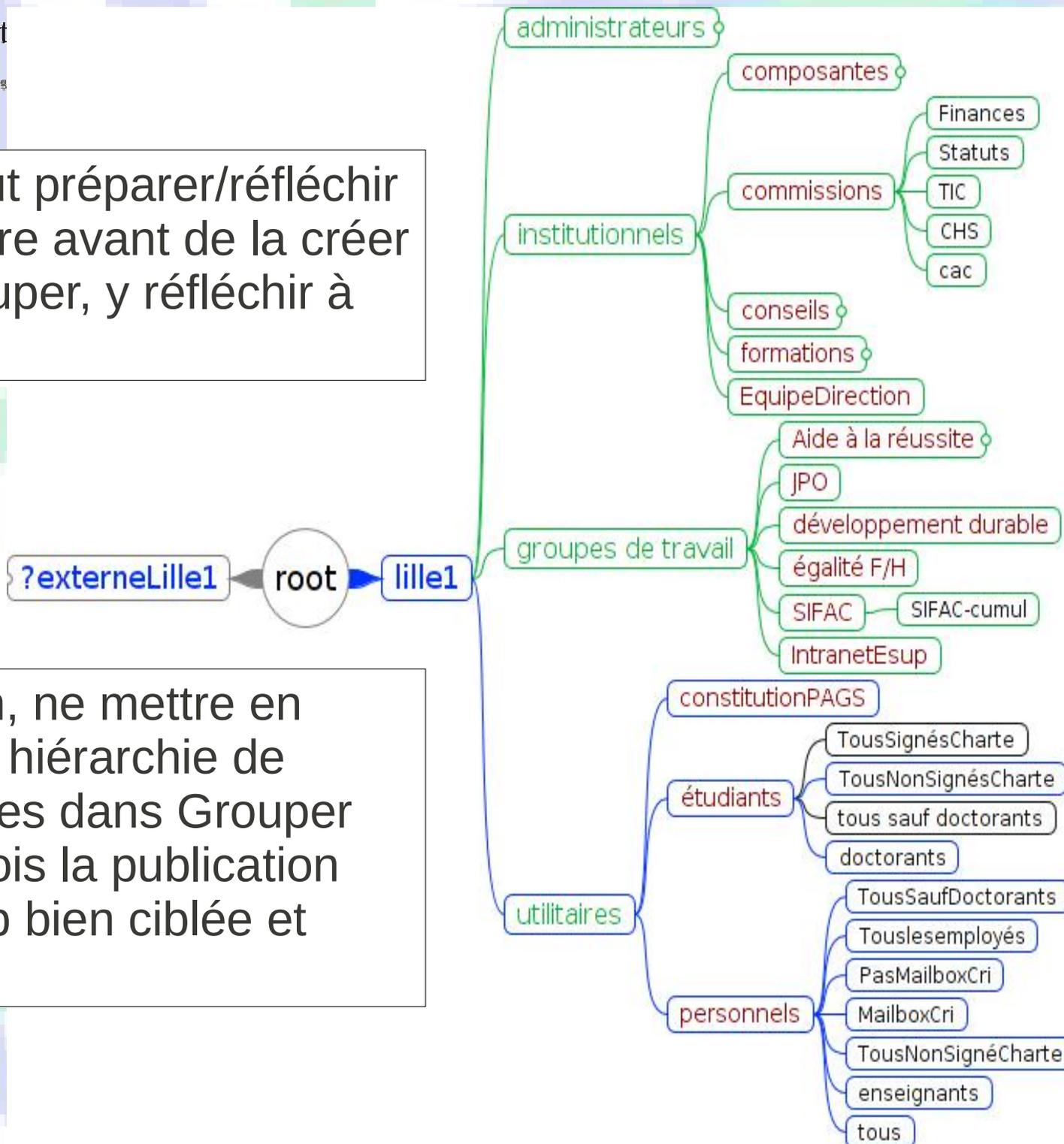
Pour GED

Pour portail

Pour CMS

Mieux vaut préparer/réfléchir sa structure avant de la créer dans Grouper, y réfléchir à plusieurs.

Attention, ne mettre en place sa hiérarchie de répertoires dans Grouper qu'une fois la publication vers Idap bien ciblée et testée !



 Andréa-Myrna Fernandez

Gérer (tous les droits)

 lille1:groupesdetravail:accesauxintranetsESUP:grouper-IntranetSUAIO

Lecture

Supprimer

## Ajouter une nouvelle règle

### Rechercher des utilisateurs

Pour lancer la recherche, veuillez taper au moins 3 caractère(s)

### Ajout manuel d'un utilisateur

#### Choix d'un groupe

-  administrators
- ▼  externe1
  - ▼  pres
    -  grouper-vppres
- ▼  lille1
  - ▼  administrateurs
    -  grouper-admin-espaces-nuxeo
    -  grouper-admin-nuxeo
  - ▼  groupesdetravail
    - ▼  accesauxintranetsESUP
      -  grouper-IntranetSUAIO
    -  grouper-egalitefh
  - ▼  liesaSIFAC
    -  grouper-SIFAC-cumul-users
  - ▼  institutionnels
    - ▼  composantes
      - ▼  servicescommuns
        - ▼  suaio
          -  grouper-TousSUAIO
      -  grouper-EquipeDirection
  - ▼  utilitaires
    - ▼  personnels
      -  grouper-TousPers
-  members

DANS LA GED NUXEO  
pour donner les droits sur  
des espaces de documents

Action

Accorder ▼

Permission

Lecture ▼

Ajouter

# Portail Lille 1

→ Bonjour Brigitte

Recherche



UNIVERSITÉ

VIE INSTITUTIONNELLE

VIE DOCTORALE

VIE DU CAMPUS

BIBLIOTHÈQUES

OUTILS D'ADMINISTRATION BW

MON UNIVERS

FINA

## Mon univers

➕ Ajouter une application

➔ Gestion des groupes (Grouper)

➔ Toutes les boîtes

## Utiles

👁 Mon univers

🔧 Outils

⊕ Assistance

A-Z Annuaire

🕒 Plans d'accès

☰ Index

🏠 Plan du site

## Gestion des groupes (Grouper)

### Mettre à jour les membres d'un groupe ⓘ

#### Gérer les groupes

Vous êtes actuellement sur: 📁 lille1: 📁 groupes de travail: 📁 acces aux Intranets ESUP: 👤 Présentation de la rentree [Trouver un autre groupe](#)

Nom	Présentation de la rentree
Adresse longue	lille1:groupes de travail:acces aux Intranets ESUP:Présentation de la rentree
Description	Présentation de la rentree

[Plus de choix...](#)

#### Ajouter un membre

Saisir les premiers caractères pour trouver un membre à ajouter - Merci de patienter car la recherche dans l'annuaire peut mettre un certain temps.

Ajouter un membre

#### Liste des membres

Les membres du groupe: 1-23 of 23 Taille de la page: 50

- ✖ Andréa-Myrna Fernandez - personnel ▾
- ✖ Brigitte Wallaert Taquet - personnel ▾
- ✖ Cécile Verbeke - personnel ▾

LiteUI dans le portail pour déléguer le peuplement des groupes

Alors  
**GROUPER**  
Pas si simple ?  
Qu'en pensez-vous ?

**MERCI pour votre attention !**