esup portail

apereo Aix*Marseille université Initiative d'excellence

Groupie, une alternative à Grouper

Peggy Fernandez-Blanco – Aix Marseille Université
Dominique LALOT – Aix Marseille Université

Historique Grouper aux EsupDays

Gestion de groupes :

Auparavant, pas trop de solutions hormis les groupes PAGS mais liés à uPortal, et accessibles via un web service

Puis Grouper, projet Internet2, est apparu (présentation RECIA 2010?)

Aux ESUP days

- 10 (2010) Généralisation ESUP V3, évolution Grouper et ESUP-Commons V2
- 12 (2011) Atelier Grouper
- 16 (2013) Atelier Grouper
- 20 (2015) Installation de Grouper v2
- 22 (2015) Retour sur l'utilisation de Grouper
- 25 (2018) ESUP's recipe: How to easily install Grouper

Historique Grouper AMU

Avant 2012

- 3 universités
  - Pas de gestion de groupes

2012 création d'Aix Marseille Université

- Fusion des 3 universités
  - ENT unique
  - LDAP unique

Arnaud Deman responsable atelier ESUP Grouper est parmi nous

- On installe Grouper (1.6.2)
- Le nouvel ENT est configuré avec Grouper. On va jusqu'à enlever les groupes PAGS

Grouper

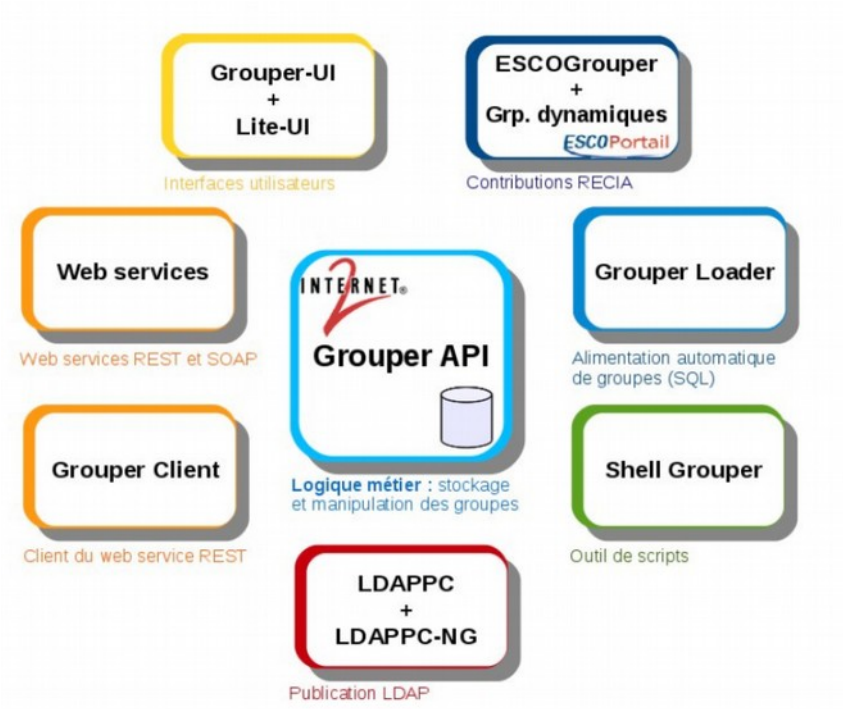
Gestion des groupes
- Arborescence de groupes
- Inclusion de groupes
- Délégation sur des répertoires ou des groupes

2 interfaces web
- Internet2
- ESCOGrouper

Alimentation des groupes
- Manuelle
- À partir de filtres LDAP

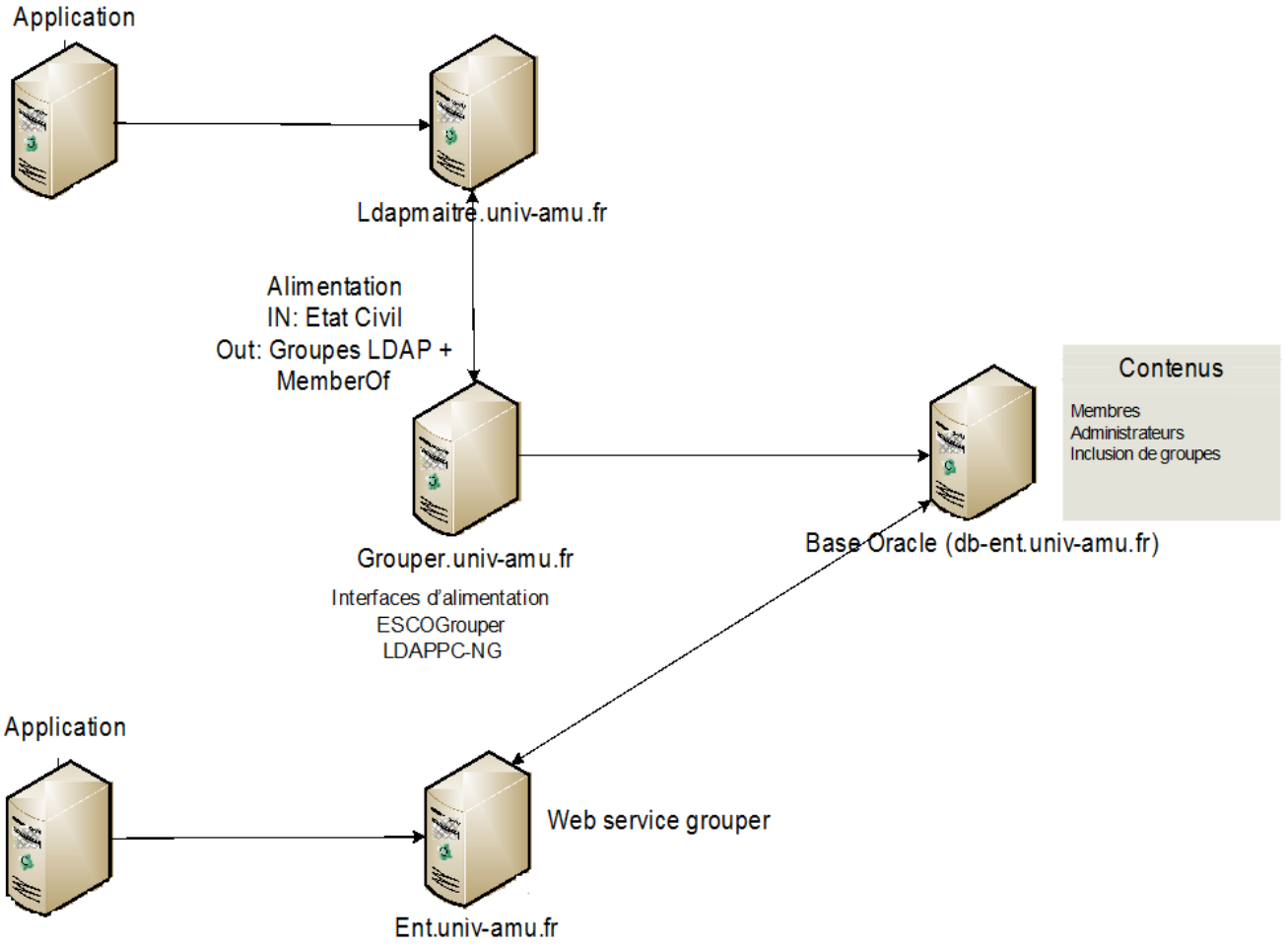
Export des groupes
- LDAP
- AD

Grouper



- Grouper API : composant de base
  Appli java
- Grouper-UI : interface utilisateur internet2
  Très complète, orientée administrateur
- ESCOGrouper : interface graphique développée par le RECIA
  Plus ergonomique
- Web services :
  REST et SOAP
- Shell grouper :
  Permet d'écrire des scripts pour manipuler des groupes
- LDAPPC et LDAPPC-NG :
  Outil de publication dans le LDAP

Grouper AMU Architecture



Mais alors, tout va bien ?

Grouper AMU : des interrogations…

Notre expert nous quitte (mutation)

- Et l'architecture n'est pas simple à maintenir ou à faire évoluer

Inconvénients de Grouper:

- Deux outils pour administrer
- L'outil du RECIA avait quelques faiblesses pour les utilisateurs
- Gestion d'une base Oracle. On a eu des plantages et là, il faut être DBA..
  - Et tout plante → retour par sécurité aux groupes PAGS dans uPortal
- Modifications différées dans le LDAP
- Uportal groupStore Grouper pas adapté si l'utilisateur a plusieurs centaines de groupes (plus d'une minute pour se connecter)

Et au final, le GT ESUP ENT conseille l'usage du groupStore SmartLDAP !

Et si on faisait plus simple ?

Grouper AMU : des interrogations…

Au final :

Choix entre une migration de Grouper, coûteuse en temps humain

Ou trouver / développer un outil qui gère des groupes LDAP

On l’a fait, et il s’appelle GROUPIE

Groupie

« Make it simple ! »

Groupie : feuille de route 1

Tout dans le LDAP (openLDAP) avec overlay memberOf (références inverses)

- Pas de base SQL

- Simplicité
  - Les membres peuvent voir qui est membre
  - Un groupe peut avoir plusieurs administrateurs
    - Il peut juste ajouter / supprimer des membres
    - Et éventuellement ne pas être membre

- Rester compatible avec Grouper sur le nommage et faciliter la migration
  - Simuler l'arborescence Grouper avec les : et les groupes sont dans ou=groups

Groupie : feuille de route 2

- Ajouter des filtres sur les groupes
- Faire des groupes de groupes
- Ajouter un utilisateur qui n'est pas dans le filtre dans un groupe à filtre
- Synchroniser les groupes dans l'Active Directory
  Pas de métadonnées à exporter. Juste recopier à l'identique dans ou=groups mais uniquement cn et member
- Groupes personnels
  - Développés mais pas utilisés (limités en nombre de groupes)
    dans une sous « ou » de groups : ou=perso,ou=groups

Groupie : attributs LDAP

Les attributs sont préfixés amu (historique maison)

- **amuGroupAdmin**
  - DN de l'administrateur du groupe
  - On va basculer vers supannGroupeAdminDN (merci Pascal Rigaux...)
- **amuGroupFilter**
  - Filtre LDAP ou SQL (compatible Perl dbi)
    - dn: cn=amu:ufr:odontologie:ldap:enseignants,ou=groups,dc=univ-amu,dc=fr

      amuGroupFilter: (&(amudatevalidation=*)(amuComposante=odontologie)(eduPersonAffiliation=faculty))
    - dn: cn=amu:app:grp:limesurvey:gestionnaires,ou=groups,dc=univ-amu,dc=fr

      amuGroupFilter: dbi:mysql:host=xx.univ-amu.fr;port=3306;database=Limesurvey_Prod|lime_user_read|$pass|select users_name from limesurvey_users

      amuGroupFilter: dbi:Oracle:host=yy;port=1530;sid=APPLIP|DEV_ADE|$PASS|SELECT login FROM V_USERS_ADE

Groupie : attributs LDAP

- **amuGroupOfGroup** (TRUE) Le filtre cherche dans les groupes
  - dn: cn=amu:app:grp:nemesis:tousgroupes,ou=groups,dc=univ-amu,dc=fr
    cn: amu:app:grp:nemesis:tousgroupes
    amuGroupOfGroup: TRUE
    amuGroupFilter: cn=amu:app:grp:nemesis:*

- **amuGroupMember**
  - DN d'un utilisateur. Sert à ajouter un utilisateur manuellement dans un groupe à filtre. On exécute le filtre puis on ajoute ce membre en member

Groupie : développement

- PHP Symfony pour le frontend
  - Version 2.7
  - PHP 5 ou plus
  - ~3000 lignes de code

- PERL pour le backend filtres + synchros AD
  - 200 lignes pour les filtres SyncAllGroups.pl
  - 294 lignes pour SyncADGroups.pl

Groupie AMU : migration

Exportation de tous les groupes

- « *Grouper m'a tuer* » :-(DDOS du LDAP
  - → Réécriture de la synchro grouper pour basculer
    - Exportation des admins, et des membre de groupes. A l'époque, un peu de JAVA et de PERL. *Schéma de la base SQL grouper très complexe* :-(

Réécriture des applications qui utilisaient le web service Grouper

- Nos applications utilisaient le web service :-)
- Les autres (moodle, nextcloud,uPortal, ...) ne font que du LDAP :-)))

6 mois ont été nécessaires avant de basculer. Peut être plus facile maintenant.

Groupie AMU : migration finie

Au final, toutes les métadonnées sont dans du LDAP

- Répliquées
- Robustes
- Modifiables simplement via Groupie ou un simple phpLdapAdmin
- Pas de stress sur les mises à jour (schémas SQL, arrêts de bases etc..)
- Une seule interface minimaliste et simple
- Un système humainement compréhensible et maintenable

Tout est dans le cn du groupe

Groupie : opérations

Pour le moment (2019), un seul groupe autorisé à créer les groupes

- Nom / Description / Filtre

Admin de groupes (350 gestionnaires pour 1250 groupes)

- Voir mes groupes
  - Ajout / Suppression de membres
- Chercher si un utilisateur est dans un de ses groupes

Utilisateur

- Voir mes appartenances (lister les groupes dont je suis membre)

Pour les deux

- Recherches sur groupes

Groupie AMU

Liste de mes groupes

Nom	Description	Gérer groupe
amu		
app		
grp		
ecandidat		
users	Utilisateurs eCandidat	
pacbo		
deve		
autresresp	Groupe pour certains rapports PACBO auquels ont accés les responsables de scolarité	
projet		
users	Utilisateurs plateforme projets redmine	
sesame		
admin	Groupe des administrateurs de sesame	
webmindns	Gestion des zones DNS par Webmin	
svc		
deve		
respscolantennes	Responsables de Scolarité Antennes	
dosi		
poleen	pole-environnement-numerique	
sdn31	Test des solutions de groupware	
drv		
dirlab		
allsh	Dirlab Secteur allsh	
dsp	Dirlab secteur drot sciences politiques	
eg	Dirlab secteur economie gestion	
sante	Dirlab secteur santé	
sciences	Dirlab secteur sciences	
ed		
direction	Direction	
presidence		
gouvernance	gouvernance	

Groupie AMU

Nombre d'administrateurs du groupe : 1

Afficher 10 éléments Recherche

Nom complet	Mail	Téléphone
LALOT Dominique	dominique.lalot@univ-amu.fr	+33413941850

Affichage éléments 1 à 1 sur 1 éléments Précédent 1 Suivant

Nombre de membres du groupe : 5

Afficher 10 éléments Recherche

Nom complet	Type	Affectation principale
FERNANDEZ BLANCO Peggy	employee	YDOSI
LALOT Dominique	employee	YDOSI
PUCELLE David	employee	YDOSI
TEST dom	researcher	FAMU
TRUCY Gregory	employee	YDOSI

Affichage éléments 1 à 5 sur 5 éléments Précédent 1 Suivant

Groupie AMU

Ajout d'utilisateur au groupe AMU:SVC:DOSI:POLEEN

Recherche individuelle

Veuillez indiquer l'identifiant ou le nom de la personne à rechercher.

Identifiant

Nom Recherche exacte ☑

Rechercher Annuler

L'autocomplétion fournit un maximum de 20 résultats.

Si vous ne trouvez pas dans la liste la personne que vous recherchez, tapez le nom dans le formulaire puis cliquez sur le bouton "Rechercher".

Retour

Ajout de personnes en masse

Pour ajouter plusieurs membres en même temps, cliquez sur ce bouton.

Ajouts multiples

Ajout d'utitlisateurs en masse

Recherche d'utilisateurs

Ajout de personnes en masse

Saisissez une liste d'identifiants ou d'emails (un par ligne).

Liste d'identifiants ou de mails

Ajouter Annuler

Retour

Groupie AMU

Modification des droits d'un utilisateur

Modifications pour l'utilisateur : FERNANDEZ BLANCO Peggy

Afficher 10 éléments Recherche

Nom du groupe	Membre	Administrateur
amu:app:grp:sesame:admin	☑	☑
amu:app:grp:sesame:gestioncomptesiep	☐	☑
amu:app:grp:sesame:gestioncomptesifsi	☐	☑
amu:app:grp:sesame:gestioncomptesmanuels	☑	☑
amu:app:grp:sesame:gestioncomptessalles	☐	☑
amu:app:grp:sesame:gestioncompteswifi	☐	☑
amu:app:grp:sesame:labos:ciae	☐	☐
amu:app:grp:sesame:labos:cpyth	☐	☐
amu:app:grp:sesame:labos:cscie	☐	☐
amu:app:grp:sesame:labos:iep	☐	☑

Affichage éléments 1 à 10 sur 18 éléments Précédent 1 2 Suivant

Valider les changements de droit Annuler

Retour à l'utilisateur

Groupie : conclusion

Au final, un outil maison simple

- Peu d'assistance aux administrateurs de groupes
- Robuste et stable
- Mis en place en 2015
- On peut l'améliorer si ça intéresse la communauté
- Vous pouvez aussi y participer

https://github.com/amu-dosi-polen/groupie

- Certains établissements l'ont déjà utilisé, comme Paris 1

Université Paris 1

Grouper 2.1 (2012) puis 2.2 (2015)

Avec export **complet** dans LDAP avec grouper **psp**

- notamment supannGroupeLecteurDN (utilisé pour les binds applicatifs)
- Seul l'historique (l'audit) est uniquement disponible dans grouper

On ajoute des attributs dans LDAP car pas facile/faisable dans grouper 2.2 :

- mail : pour les comptes de fonction
- homeDirectory : pour les dossiers partagés NAS

Automatisation de la création de groupes via **gsh**

Grouper à l'université Paris Panthéon-Sorbonne

Tentative de migration en Grouper 2.4 (2018)

Pas mal de changements :

- "new UI" remplace complètement "lite UI" et "admin UI" (bye bye "struts")
- **gsh** passe de BeanShell à Groovy
  - nécessite l'adaptation de notre automatisation de création de groupes
- suppression à terme de **psp**, remplacé par **pspng**
  - psp était horrible mais puissant
  - pspng est simple, mais a encore des bugs et ne semble pas pouvoir gérer supannGroupeLecteurDN

Université Paris Panthéon-Sorbonne

On teste Groupie

- fonctionne au bout d'une demi-journée comme gestionnaire de groupe manuel.
- réutilise les droits supannGroupeAdminDN (exportés par grouper **psp**)

Super !

Améliorations de Groupie

La liste de courses pour Paris1

- Pouvoir modifier la "description" et ajouter "ou"
- Utiliser "." à la place de ":" comme séparateur dans le "cn" (pour l'utilisation UNIX/POSIX, ex NSS)
- Gérer l'inclusion de groupes dans l'UI et améliorer la vitesse de propagation des modifications d'un groupe inclus
- Autoriser les groupes dans l'attribut "supannGroupeAdminDN" et les gérer
- Gérer supannGroupeLecteurDN

  exemple : le groupe "applications.zabbix.users" a supannGroupeLecteurDN "cn=zabbix,ou=admin,dc=univ-paris1,dc=fr" autorisant ce bind a voir les membres du groupe "applications.zabbix.users"