

# Gestion des groupes dans ori-oai-workflow

<b>Sommaire</b>	<b>page</b>
Déclarer le LDAP à utiliser	2
Où paramétrer les groupes d'utilisateurs ?	2
Comment déclarer un groupe d'utilisateurs ?	3

---

## Déclarer le LDAP à utiliser

Si les groupes d'utilisateurs ORI-OAI s'appuient sur des informations du LDAP, il faut que le LDAP soit déclaré dans le fichier "commons-parameters.properties" du quick-install.

Dans les paramètres :

```
# Le nom du serveur sur lequel se trouve le LDAP de l'établissement
LDAP_ETABLISSEMENT=xxxxxx

# La base dn du LDAP de l'établissement
LDAP_BASE_DN=xxxxxxx
```

## Où paramétrer les groupes d'utilisateurs ?

Trois cas de figures se présentent :

Pour ...	Remarque
le groupe "super-admin"	Droit d'accès aux onglets "Import/Export" et "Administration" de l'interface
un workflow par défaut	Un des workflows fournis par défaut dans les sources du module workflow. (localisé dans "conf\properties\workflows")
un workflow personnalisé	Workflow personnalisé par l'exploitant ; ("custom\properties\workflows\contrib_xxxx" selon les bonnes pratiques)

Ils sont détaillés ci-dessous.

### ➤ Groupe "super-admin"

Dans le fichier "commons-parameters.properties" du quick-install.

Les membres de ce groupe doivent être déclarés dans le paramètre suivant :

**WORKFLOW\_GROUP\_ADMINS**

### ➤ Workflow par défaut

Dans le fichier "commons-parameters.properties" du quick-install.

Entre les lignes 500 et 720, il s'agit des paramètres : **WORKFLOW\_(xxxx)\_GROUP\_(xxxx)**

Exemple :

# Groupe des modérateurs

WORKFLOW\_DC-E\_GROUP\_MODERATORS=virtual:(&(objectClass=Person)(uid=xxxxxx))  
pour le workflow "DC easy" (géré dans le dossier "default\_dc\_easy").

### ➤ **Workflow personnalisé**

Dans le fichier "groups.xml" du dossier de personnalisation de l'exploitant "contrib\_xxxx".

## Comment déclarer un groupe d'utilisateurs ORI-OAI ?

Il existe différentes manières de déclarer un groupe d'utilisateurs ORI-OAI.

- s'appuyer sur des **groupes** définis dans le **LDAP** ;
- définir des **groupes** dit "**virtuels**", en s'appuyant sur des attributs LDAP ;
- il est aussi possible d'utiliser des **règles Shibboleth**.

Dans le tableau ci-dessous, (*mon\_groupe*) est à intégrer, selon le cas :

- dans "commons-parameters.properties" : WORKFLOW\_(xxxx)\_GROUP\_(xxxx)=(**mon\_groupe**) ;
- ou dans "groups.xml" : <value><![CDATA[(**mon\_groupe**)]]></value>.

Voir les exemples fournis pour le fichier "groups.xml" :

- "groups\_exemple-gpe-LDAP.xml" (groupes LDAP) ;
- "groups\_exemple-uid-LDAP.xml" (attributs LDAP).

## Appui sur des groupes LDAP

- (mon\_groupe) = ***ldap:pers\_ORI-OAI\_admins***  
pour désigner le groupe "pers\_ORI-OAI\_admins" défini dans le LDAP.

## Appui sur des attributs LDAP (groupes virtuels)

- (mon\_groupe) = ***virtual:(objectClass=Person)***  
pour désigner toutes les personnes définies dans le LDAP (plus précisément toutes les entrées du LDAP dont la classe d'objets est de type Person)  
Ici, le groupe virtuel est construit en s'appuyant sur l'attribut LDAP *objectClass*.

- (mon\_groupe) = ***virtual:(&(objectClass=Person)(uid=login\_admin))***  
pour désigner l'utilisateur défini par les attributs LDAP :  
*objectClass* dont la valeur est "Person" ;  
ET  
*uid* dont la valeur est "login\_admin".

- (mon\_groupe) =  
***virtual:(/(&(objectClass=Person)(uid=moder))(&(objectClass=Person)(uid=admin)))***  
pour désigner un groupe de 2 utilisateurs, dont l'attribut LDAP *uid* a comme valeur :  
"moder"  
OU  
"admin".

- (mon\_groupe) = ***virtual:(&(objectClass=Person)(departmentnumber=nnn))***  
pour désigner un groupe des personnes dont l'attribut LDAP *departmentnumber* a comme valeur "nnn".

- (mon\_groupe) = ***virtual:(/(&(eduPersonAffiliation=faculty)(ustlRole=orioai-rp-auteurs)))***  
pour désigner un groupe d'utilisateurs dont :  
- soit l'attribut LDAP *eduPersonAffiliation* a comme valeur "faculty" ;  
- soit l'attribut LDAP *ustlRole* a comme valeur "orioai-rp-auteurs"

## Appui sur des règles Shibboleth

- (mon\_groupe) = ***shib:shibAttrsMap.get("Shib-InetOrgPerson-mail").equals("administrateur@mon-etabl.fr")***  
pour désigner l'utilisateur défini par l'@ email "administrateur@mon-etabl.fr".