LabInvent - ACLs

Droits des utilisateurs selon leur profil

Version : 17/12/18

Auteur : Etienne Pallier (IRAP)

URL de ce doc :
- short **:** http://tinyurl.com/labinvent2
- Long url

Nous décrivons ici le processus d'autorisation des utilisateurs, nommé "authorization" en anglais. Il s'agit d'expliquer la façon dont un utilisateur est autorisé à faire telle ou telle action selon son profil (ou rôle).

Lorsqu'un utilisateur s'authentifie (étape décrite précédemment), un profil lui est associé.
Par défaut, si l'utilisateur n'est pas présent dans la base de données (table "users"), le profil "Utilisateur" lui est associé, ce qui correspond au profil le moins privilégié.
D'autres profils offrent davantage de "pouvoirs". Il s'agit des profils "Responsable" et "Admin". Le profil le plus élevé est "SuperAdmin" et il ne doit être accordé qu'aux administrateurs et développeurs de l'application.

1. Principe général

(updated 17/12/18 - EP)

CakePHP3 n'intègre plus un composant pour un gérer les ACLs, un plugin est à disposition pour remplacer ce composant, hélas il n'est pas stable, et le fait qu'il utilise la base de données ralenti les applications, car le composant effectue beaucoup de requêtes.

De plus, il est conseillé pour des autorisations basiques d'utiliser la fonction isAuthorized($user) dans les controller.

Dans labinvent2, on utilise la fonction isAuthorized($user), qui définit les choses que les utilisateurs connecté peuvent faire et donne tous les droits au Super-Admin dans AppContoller.php.
Puis, dans chaque controller la fonction est redéclarer, on définit les actions possible pour chaque rôle.

Les autorisations sont gérées par la fonction **isAuthorized**()

1) **beforeFilter**() autorise les actions SANS connexion (pour les utilisateurs NON authentifiés)

2) puis, **isAuthorized**() autorise les actions APRES connexion (pour les utilisateurs authentifiés)

Comment définir qui a droit de faire quelles actions (c'est à dire qui a le droit d'accéder à quelles vues) ?

=> 1) **Régles générales par défaut** pour tous les contrôleurs : AppController.isAuthorized()
src/Controller/AppController.php/isAuthorized()
(héritage de Cake\Controller\Component\AuthComponent::isAuthorized(), c'est à dire
vendor/cakephp/src/Controller/Component/AuthComponent.php::isAuthorized())

(voir aussi https://book.cakephp.org/3.0/fr/controllers/components/authentication.html et
https://book.cakephp.org/3.0/fr/tutorials-and-examples/blog-auth-example/auth.html)

=> 2) **Régles pour un contrôleur donné** (ex: MaterielsController) : MaterielsController.isAuthorized()
src/Controller/MaterielsController.php/isAuthorized()

Une fois qu'on est dans une vue, comment définir qui a droit de voir quels éléments de la vue ?
=> src/Template/<Model>/nom_de_la_vue.ctp
ex : src/Template/Materiels/edit.ctp pour les règles concernant la vue "edit" des materiels

Procédure ajout d'une fonctionnalité :
- On ajoute la fonctionnalité dans le controller
- Si la fonctionnalité est accessible par tout le monde, il faut l'ajouter dans le isAuthorized($user) de l'AppController
- Sinon il faut ajouter la condition lié à l'action dans la fonction isAuthorized($user) du controller correspondant (1ère fonction de tous les controllers)
- Enfin lorsque vous réalisez la vue correspondante, il faut cacher les champs/boutons de votre fonctionnalité en fonction de vos droits, une variable "$role" est accessible dans toutes les vues, ainsi qu'une variable "$username" (nom de l'utilisateur, pas le login) pour tester la proriété d'un objet dans une vue.

* Si vous avez besoin de vérifier la propriété d'un objet pour un utilisateur, il faut utiliser la fonction "isOwnedBy" (déja défini dans materiels, suivis, emprunts)

* Exemple de la fonction provenant du controller Materiels :
```
public function isOwnedBy($id, $nomUtilisateur)
{
    return ($this->Materiels->exists(['id' => $id, 'nom_createur' => $nomUtilisateur]) || $this->Materiels->exists(['id' => $id, 'nom_responsable' => nomUtilisateur]));
}
```

* *Exemple 1 :* Ajout de la fonctionnalité désarchivé avec un bouton sur la view d'un matériel (pour les adminplus+)
* On se place dans le controller Materiels, on y définit la fonction correspondante "setStatusArchived($id)".
* Dans la fonction "isAuthorized($user)" du même controller, rajouter les lignes suivante :

```
if (in_array($action, ['setStatusArchived'])) {
    if (in_array($role, ['Administration Plus', 'Super Administrateur'])) {
            return true;
    }
}
```
* Puis on se place dans la view de materiels, et on affiche le bouton selon les mêmes conditions que l'action "setStatusArchived($id)" dans la fonction "isAuthorized($user)".

* *Exemple 2 :* Ajout d'une action "exportQrCode()" (pas très utile) pour tout le monde
* On se place dans la fonction "isAuthorized($user)" de l'AppController.
* Puis on ajoute l'action à la liste qui est autoriser à tout le monde

```
//Pour tout le monde
if (in_array($action, ['index', 'find', 'view', 'creer', 'add', 'exportQrCode'])) return true;
```

2. Tableau des ACLs (droits d'accès) selon les profils (et selon le contexte)

NB : ce tableau est encore incomplet, ne pas hésiter à l'enrichir…

Concernant les informations internes permettant de savoir qui a fait quoi (mises en place en février 2014), elles ne sont bien sûr pas modifiables puisque gérées automatiquement par le système, mais sont visibles par tous excepté le profil « utilisateur »

Conventions d'écriture :

- responsable+ = possible pour un « responsable » et plus (responsable, administration, et superadmin)
- admin+ = possible pour un « administration » et plus (administration et superadmin)

Légende :
- Acteur = la personne qui fait l'action
- **(M)** = Mandatory fields (champs obligatoires)
- **(H)** = Hidden fields (champs cachés)
- **(R)** = Read only fields (champs en lecture seule)
- **(C)** = Controles d'intégrité effectués sur les champs (ex : date livraison ≥ date achat)
- **(D)** = Valeur par Défaut d'un champ
- **(E)** = Emails envoyés

Dans le tableau ci-dessous, chaque ligne représente une **action** générale (login/logout…) ou spécifique sur les matériels/suivis/emprunts.
Pour chaque action, la ligne explicite :

- (**FROM**) : à partir de quelle vue elle est accessible (actionnable)
- (**TO**) : à quelle (nouvelle) vue elle conduit (une fois exécutée)
- pour chaque profil, s'il a accès à cette action et à quelle(s) condition(s)
- les **conséquences** de cette action

Par défaut, les droits de chaque profil prennent pour base les droits de la colonne « Par défaut » auquels ils peuvent éventuellement ajouter ou retrancher quelque chose

ACTION	VIEW		PROFILS					CONSEQUENCES	TESTÉ
	FROM	**TO**	**<Par défaut> (1)** *(valeurs par défaut **héritées par tous les profils**)*	**USER (2)** (utilisateur lambda, **authentifié** via LDAP ou via la BD)	**RESP (3)** (responsable du **groupe métier ou thématique** auquel le matériel est lié)	**ADMIN (4)**	**SUPER ADMIN (5)** (il a au moins les mêmes droits que **admin**)		X = tout (X) = partiel
GENERAL **Une personne quelconque NON AUTHENTIFIÉE n'a droit à rien**, sauf à voir les pages suivantes : ○ A propos (+ guide utilisateur) ○ Page de connexion (login) : c'est sa page d'accueil **L'acteur d'une action ne doit pas recevoir de mail pour cette action (inutile)**									**testUser10**
Login	**Login**	**Accueil**	O (Utilisateur non connecté, si dans LDAP ou dans table BD utilisateurs privilégiés)						**testUser20**
Logout		**Login**	O (utilisateur connecté)						**testUser30 (TODO)**
Aller à l'Accueil	login ou clic sur Accueil dans menu gauche	**Accueil** (pages/home)	« Voir les matériels à mon nom »		- « Voir les matériels **à valider** du/des groupe(s) dont je suis responsable » - « Voir **tous** les matériels du/des groupe(s) dont je suis responsable" - « Voir les **suivis** des matériels du/des groupe(s) dont je suis responsable »	- « Voir les matériels à **valider** (dont je suis gestionnaire) » - « Voir les matériels à **archiver** (sortir de l'inventaire) (dont je suis gestionnaire) » - « Voir **tous** les matériels dont je suis gestionnaire » ***NB**: uniquement les matériels dont il est le **gestionnaire de référence***		**N/A**	**testPage10**

Aller aux Outils	clic sur Outils dans menu gauche	**Outils** (pages/tools)	admin +	N	N	O	Options en plus : - Configuration générale de l'application - Gérer utilisa-teurs privilégiés - Passer en mode debug - Passer en mode install	**N/A**	**testPage20**

Table MATERIEL

(D) : owner = createur, … (**TODO**)
(M) : Nom, Domaine/Catégorie, Site, Propriétaire, Statut, prix (ssi matériel inventoriable), Technique/Inventoriable (seulement pour ADMN)…
(M) pour VALIDATION : infos administratives, prix, date commande et livraison
Ne pas pouvoir imprimer l'étiquette inventaire tant que le matériel n'est pas VALIDATED

Actions CRUD (Create, Read, Update, Delete) :

- **Utilisateur** : il ne peut que créer un matériel, un suivi, ou un emprunt, consulter, et modifier (uniquement ce qu'il a créé lui-même) ; ne doit pas pouvoir modifier le propriétaire, ni le statut, ni l'étiquette, ni les données admin d'un matériel (en mode Création comme Modification)
- **Responsable** : il est "responsable" d'un groupe (métier ou thématique) et a donc accès à (est responsable de) tous les matériels de ce groupe ; il a plus de droits qu'un "USER", mais pas accès à certains champs et certaines vues réservées à l'administration (admin) ; il ne doit pas pouvoir modifier le statut, ni les données admin d'un matériel (en mode Création comme Modification) ; il ne **peut pas valider un matériel** (même <800€, car validation = livraison) ; il ne **peut pas archiver** un matériel, mais **seulement demander l'archivage** (comme un « utilisateur »), et encore uniquement des matériels dont il est responsable
- **Administration** : il a presque tous les droits (y-compris sur les "données administratives") ; il peut modifier un matériel quelque soit son statut (y-compris TOBEARCHIVED et ARCHIVED), et peut notamment modifier le statut du matériel (pour le rétrograder) ; il est surtout le seul à pouvoir "valider" un matériel (pour dire qu'il a bien été livré).
- **Superadmin** : il a tous les droits, ceux de « admin » et certains droits supplémentaires pour lui permettre des corrections d'erreur et la configuration de l'application (notamment l'administration des utilisateurs, des catégories, des groupes…)
- **Matériel VALIDATED** : tout le monde peut les modifier ("user" et "resp" ne peuvent modifier que leurs matériels, "resp" peut aussi modifier les matériels du (ou des) groupe(s) dont il est responsable), sans toutefois pouvoir modifier leur NATURE (un ordinateur reste un ordinateur) ou le fait que le matériel est inventoriable ou pas, plus encore quelques autres éléments (par exemple, l'intitulé de l'équipement doit rester le même le plus possible, il peut être complété mais pas modifié intégralement) ; certains champs sont donc readonly (sur_categorie_id', 'categorie_id', 'materiel_administratif', 'materiel_technique', 'date_acquisition', 'nom_responsable', 'fournisseur', 'organisme', 'prix_ht') ; les seuls champs modifiables sont donc : (designation, sous_categorie, materiel_administratif, materiel_technique, description, etiquette, lieu_stockage, lieu_detail, numero_serie, groupes_thematique, groupes_metier)

• **Matériel TOBEARCHIVED ou ARCHIVED** : seul “admin” (et +) peut les modifier, mais UNIQUEMENT le champ "status" (pour pouvoir rétrograder à CREATED ou VALIDATED) • **Le seul moyen de modifier complètement un matériel VALIDATED, TOBEARCHIVED, ou ARCHIVED**, c'est de <u>rétrograder</u> son statut à CREATED (“admin”+ only) • **Gestionnaire de référence** : ce champ (facultatif) permet de désigner le gestionnaire (administratif) qui a complété ou validé la fiche (ou bien qui va le faire). Si c'est un Administratif qui crée la fiche matériel, c'est lui qui est désigné comme "gestionnaire de référence" par défaut. N’importe quel autre administratif peut modifier la fiche (ou la valider), mais il sera alors désigné comme nouveau gestionnaire.								
Read one (view)	**index**	**view**	***O*** ***responsable+ : voir*** *bouton « Imprimer Etiquettes » (sauf si CREATED)* ***(H)*** *: données admin*			+ données admin			testMat10
Read all (index)			**O** limiter aux **matériels actifs** (non archivés)		+ bouton “Exporter liste complète”	**Filtres** des matériels : **« tous** (par défaut, y-compris matériels archivés)», « à valider », « validés », « à sortir », « archivés » **Cases à cocher** pour faire une sélection de matériels **Boutons** pour « exporter » une liste de matériels (cochés) ou « changer leur statut »			testMat20
Create (add)	**view ou index**	**view** (vue détaillée du matériel créé)	***O*** ***(H)*** *statut, créateur, étiquette, donnés admin* ***(M) owner***	**(R)** owner = « self »		**(D)** gestionnaire = self		**Materiel.status = CREATED** *(la fiche matériel reste modifiable)*	**testMat30 (TODO: finaliser)**

			(C) *date livraison ≥ date achat, …* ***gestionnaire :*** *champ select parmi une liste de gestionnaires* ***numero_irap*** *: doit contenir l'année d'ACQUISITION du matériel (et non plus l'année de CREATION de la fiche comme avant)* ***date_acquisition*** *= date de la mise en service (service fait) qui déclenche la prise en charge de la facture et l'inventaire des tutelles*					Si acteur <> admin : afficher message "Vous devez maintenant imprimer cette fiche et l'amener à un gestionnaire pour qu'il passe la commande" (**E** ssi différent de l'acteur) : owner, resp	
Update (edit)	**view ou index**	**view** (vue détaillée du matériel modifié)	***(H)*** *statut (admin+), etiquette O/N (admin+), données admin (admin+)* ***(M)*** *(idem que pour « Create ») :* ***owner, gestionnaire*** ***(C)*** *idem « Create »* ***(R si VALIDATED)*** sur_categorie_id', 'categorie_id', 'materiel_administratif', 'materiel_technique', 'date_acquisition', 'date_livraison', 'nom_responsable', 'fournisseur', 'organisme', 'prix_ht'	**ssi owner** *ssi materiel.CREATED ou materiel.VALIDATED* **(R)** : + owner	**ssi owner ou responsable** *ssi materiel.CREATED OU [materiel.VALIDATED ET (owner ou (responsable et non inventoriable))]* si materiel.VALIDATED => ne doit pas pouvoir changer en un matériel « inventoriable »	**(D)** gestionnaire = self (**R** si VALIDATED+) : données admin (*date livraison et etiquette O/N doivent être modifiables ; afficher un warning si modif des infos comptables)* **(seul(s) champ modifiable(s)** si TOBEARCHIVED ou ARCHIVED) : statut	O	(**E** ssi différent de l'acteur) : owner, resp	**testMat40 (TODO:**

Delete	**view ou index**	**index** (après confirmation)	*ssi materiel.CREATED*	ssi owner	ssi responsable de ce matériel		O	Fiche matériel **supprimée de la BD** (**E** ssi différent de l'acteur) : owner, resp, admin de référence	
Autres actions :									
Rechercher (find)			limiter aux **matériels actifs** (non archivés)			voit TOUS les matériels (y-compris archivés) Case à cocher (non cochée par défaut) : "matériels actifs seulement (non archivés)"			
Valider (statusValidated) **= le matériel a été livré**	**view ou index**	reste dans la vue d'origine	***admin only*** *ssi materiel.CREATED* ***(M)** :* *données admin (centre financier, EOTP), date achat, date livraison (= date validation par défaut)*	**N**	**N**	**O** **(D)** gestionnaire = self	O	**Materiel.status = VALIDATED** *(désormais, seuls **certains champs** du matériel sont encore modifiables)* (E) : owner, resp	
Demander archivage (statusToBeArchived)	**view ou index**	reste dans la vue d'origine	responsable+ ssi materiel.VALIDATED	**N**	**O**	**O**	**O**	**Materiel.status = TOBEARCHIVED** *(désormais, la fiche matériel n'est **plus modifiable**)* (E) : ssi différent de l'acteur - owner - resp - admin de référence	

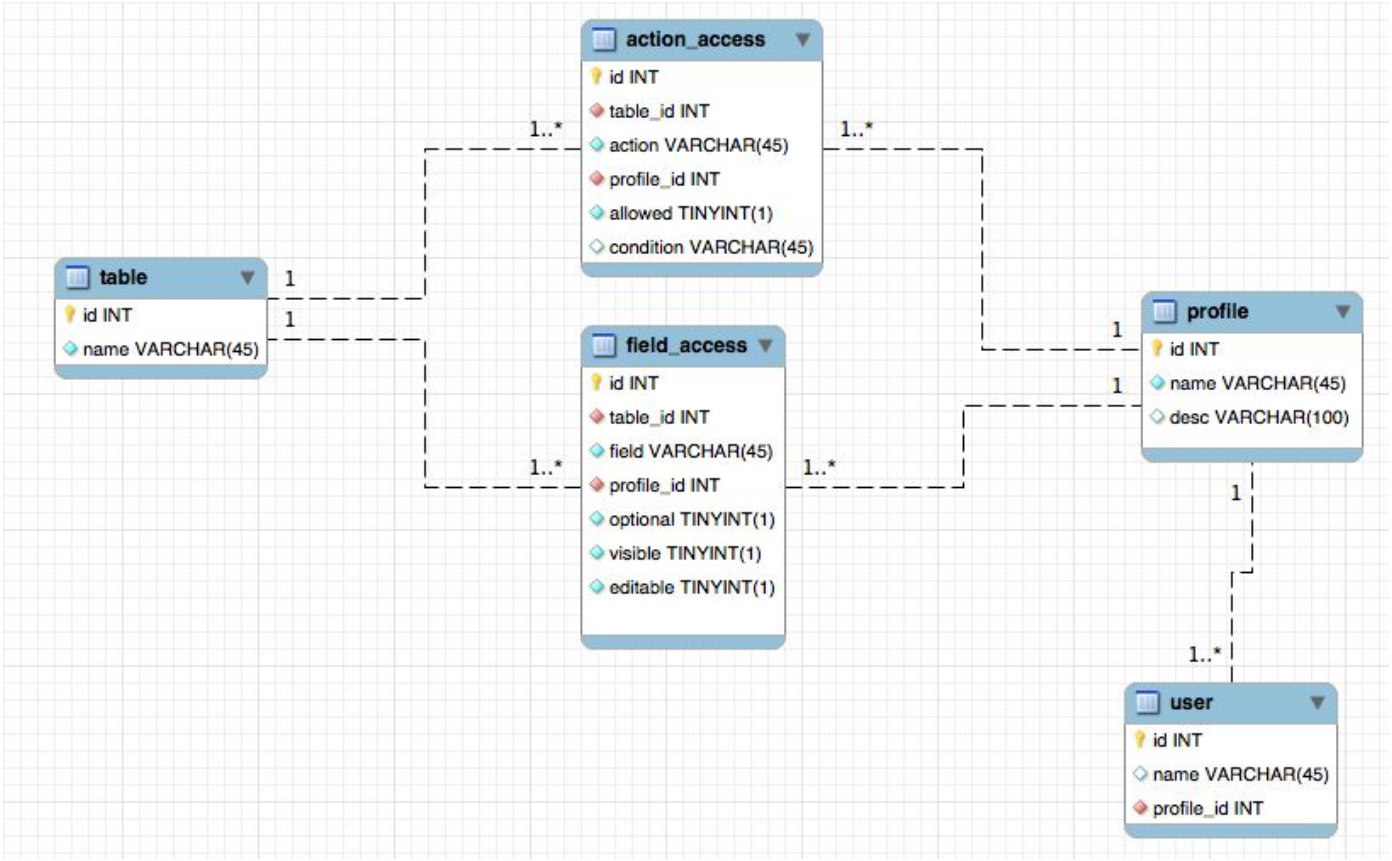
Archiver (statusArchived)	**view ou index**	reste dans la vue d'origine	admin+ Ssi materiel.TOBEARCHIVED	**N**	**N**	**O**	**O**	**Materiel.status = ARCHIVED** *désormais, la fiche matériel n'est **plus visible**, sauf par "admin")* (E) : - owner - resp	
Dé-valider (rétrograder le statut à CREATED)			admin+	**N**	**N**	**O**		**Materiel.status = CREATED**	
Exporter (csv)			responsable+	**N**	**O**	O	O		
Montée de statut groupée *augmenter (+1) le statut d'un groupe de matériels, depuis la vue « index »*			admin+	N	N	**O**	O	**Materiel.status = <nouveau statut>**	
Edition documents (**admin**+) : - **Doc d'admission** : ssi VALIDATED (quand on "VALIDE" un matériel "CREATED", le statut passe en « VALIDATED » et le document d'admission est automatiquement édité) ; **Bouton** "Doc admission" affiché seulement à partir du statut "VALIDATED" - **Doc de sortie** : **ssi TOBEARCHIVED ou ARCHIVED** (quand on "ARCHIVE" un document "TOBEARCHIVED", le statut passe en ARCHIVED et le document de sortie est automatiquement édité) ;				N	N	**O**	O		

Bouton "Doc Sortie" affiché seulement à partir du statut TOBEARCHIVED Le doc de sortie doit être couplé avec la liste des matériels a archiver (TOBEARCHIVED) quand il y a une demande de sortie									
Print Etiquette	**view ou index**		**ssi materiel VALIDATED**					**Etiquette imprimée** (et normalement collée sur le matériel)	
Attachement document : **- <u>creation</u>** **- modif** **- suppression**			**TODO**						
Tables SUIVI et EMPRUNT On ne doit pas pouvoir emprunter ou suivre un matériel CREATED ou ARCHIVED User a les droits C, R, U (si créateur), D (si créateur) Resp+ a les droits C, R, U, D									
- **Table SUIVI** Tout le monde peut rechercher un suivi (M) : Materiel, Statut, Date Intervention, Type d'intervention (D) : Statut = En cours									
Create (add)	**Materiel view**	**Suivi view**	ssi materiel.VALIDATED					**Suivi CREATED**	
Update (edit)	**Materiel view ou Suivi view**	**Suivi view**	o	Ssi createur					

Delete			o	Ssi createur	Ssi responsable de ce materiel			**Suivi supprimé de la BD**	
Read (view et index)			o						
Rechercher (find)			o						
- Table EMPRUNT **Droits d'un USER** : il peut modifier/supprimer un emprunt dont il est soit le créateur soit l'emprunteur. S'il créé un emprunt, il ne doit pas pouvoir changer le nom de l'emprunteur (par défaut, c'est lui). Ainsi, il pourra modifier/supprimer cette fiche au besoin plus tard. Par défaut donc, pour un user, emprunt.emprunteur=creator, materiel.owner=creator (M) : Matériel, Type emprunt, Date Emprunt, Date Retour, emprunteur (D) : type emprunt = interne, Date Emprunt = today, emprunteur = créateur									
Create (add)	**Materiel view**	**Emprunt view**	ssi materiel.VALIDATED	ssi acteur = materiel.owner OU emprunteur = acteur emprunteur (par défaut = createur) = createur si acteur <> materiel.owner	O	**O**	**O**	**Emprunt CREATED**	
Update (edit)	**Materiel view ou Emprunt view**	**Emprunt view**		Ssi acteur = (createur ou emprunteur ou materiel.owner) emprunteur = createur si acteur <> materiel.owner					
Delete				Ssi createur				**Emprunt supprimé de la BD**	
Read (view et index)				O	O	**O**	**O**		

AUTRES TABLES Par défaut, pour tous ces objets, superadmin a tous les droits, admin a tous les droits sauf « delete », et les autres profils n'ont que le droit de lecture (view et index)									
Tables Domaines, Catégories, Sous-catégories									
			Read only			+ Create/Update : O	CRUD : O		
Tables de Groupes (thématiques et métiers)									
			Read only				CRUD : O		
Autres tables ?									

3. Schéma de la BD pour les ACLs (authentication & authorization)



1) Table « table »

Nom de chaque table mysql (+ autres attributs si nécessaire)

id	name	desc
1	materiel	Table des matériels
2	suivi	Table des suivis de matériels
3	emprunt	Table des emprunts de matériels

2) Table « profile »

id	name	desc
1	default	Profil virtuel pour préciser les droits par défaut (valables pour tous les profils)
2	utilisateur	Utilisateur du LDAP
3	responsable	Responsable d'un groupe (thématique ou métier)
4	admin	Administratif (gestionnaire)
5	superadmin	Le roi du monde

3) Table « action_access »

Définition des droits associés aux profils, pour chaque action :
Qui (profil) a le droit de faire quoi (action) et sous quelle(s) condition(s)) ?
Attention :
- par défaut, une action non mentionnée dans cette table est accessible à tout le monde !
- les droits d'accès MINIMUM sont ceux donnés pour le profil 1 (= default) s'il est défini ; tous les autres profils (2 à 5) se basent sur le profil 0 et ils peuvent éventuellement ajouter des conditions supplémentaires.

id	table_id	action	profile_id	allowed	condition
1	1	edit	1	1	materiel.status = CREATED

					(par défaut, l'action « edit » (update) est accessible à tous, à condition que le statut du materiel soit « CREATED)
2	1	edit	2	Null	user_id = materiel.owner_id *(le profil « utilisateur » ajoute la condition « doit être propriétaire du matériel »)*
3	1	edit	3	Null	user_id = materiel.responsable_id *(le profil « responsable » ajoute la condition «doit être le responsable de CE materiel »)*
4	1	create	3	1	
5	1	validate	3	1	
...					

4) Table « field_access »

Définition des droits d'accès sur les champs et selon le profil utilisateur
Par défaut, un champ non mentionné dans cette table est :
- facultatif : **optional=True**
- visible : **visible=True**
- modifiable : **editable=True**

id	table_id	field	profile_id	optional	visible	editable
1	1	prix	1	0	1	1
2	1	date_achat	2	1	1	1
3	1	date_livraison	3	1	1	1
...						

La ligne 1 nous dit que pour un « utilisateur », le champ materiel.prix est optionnel, visible, et non editable

5) Page web de saisie des ACLs

- Saisie des autorisations sur les actions (table action_access) :

<SELECT-Table> «materiel»

<SELECT-Action> «edit»

<SELECT-Profile>	<autorisé ? (o/n)>	<Saisir condition>
« utilisateur »	« o »	« materiel.status = CREATED »

[**SUBMIT**]

- Saisie des autorisations sur les champs (table field_access) :

<SELECT-Table> « materiel »

<SELECT-field> «prix»

<SELECT-Profile>	<optionnel ?(o/n)>	<visible?(o/n)>	<editable?(o/n)>
« utilisateur »	« n »	« o »	« o »

[**SUBMIT**]

Plusieurs tableaux de synthèse s'affichent en dessous au fur et à mesure de la saisie (2 tableaux par table) :

Table «MATERIEL» :

- Autorisations sur les ACTIONS (trié par (table), puis action, puis profil) **:**

Action	Profil	Autorisé	Condition
create	utilisateur	o	
edit	utilisateur	o	materiel.status = CREATED
...			

- Autorisations sur les CHAMPS (trié par (table), puis champ, puis profil) :

Champ	Profil	Optionnel	Visible	Editable
prix	utilisateur	n	o	o
prix	responsable	n	o	o
date_achat	utilisateur	o	o	o
...				

Table «SUIVI» :

…

<u>Table «EMPRUNT »</u> :

…