Réussir la mise en place des ACL sur son projet Joomla

Joomla!™ **2.5 / 3.0**

Marc STUDER – Joomgroupe Lyon

Sommaire

1. ACL késako ?
2. Rappel : Les ACL en Joomla 1.5
3. Les ACL avec Joomla 2.5+
4. Les ACL basées sur les Rôles
5. Méthode de mise en place
6. Astuces et Hidden secrets !

ACL késako ?

- ACL = Access Control List
  - Origine : fichiers texte UNIX de listes des personnes autorisées à accèder a l'OS UNIX.
- Plus largement les ACL représentent une organisation de personnes :
  - regroupées dans des groupes, avec des permissions, et des niveaux d'accés
- Chaque ressource de l'entreprise est protégée :
  - par un niveaux pour y accèder, par des permissions d'action

- *Si un projet cible plus de 1 personne,*
  alors il faut prévoir une organisation basée sur les ACL.

Joomla 1.5 et avant : le passé fixe !

- Organisation des ACL figée !
- Contraintes J 1.5 :
  - Besoin de roles particuliers sur l'admin d'un composant.
    - Pas de choix possible → groupe Administrateur
    - Sensible et inimaginable en entreprise !
  - Solution de contournement :
    - utiliser des extensions qui nécessitaient quasi-toutes de "hacker" Joomla!

Les ACL avec Joomla 2.5+

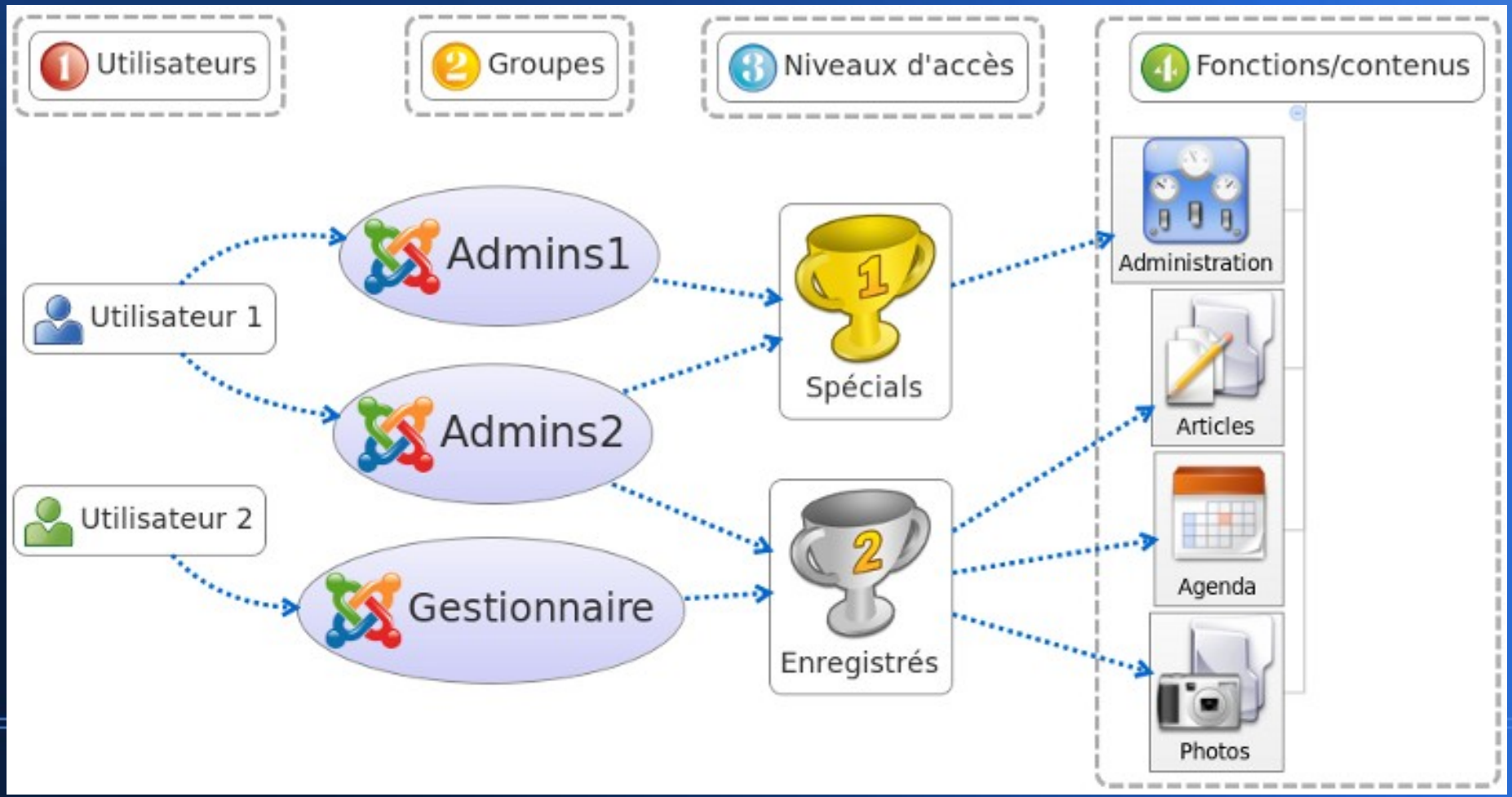
- Plus de limitation(!), ACL personnalisables.
  - nouvelle approche des ACL basées sur les rôles des utilisateurs (différent de J1.5)
  - personnalisation des ACL en J2.5+
    - ouverture de Joomla comme cible des projets corporate (idem Multi-DB)

Hélas de nombreux projets organisent encore les ACL en se basant sur la structure des ACL de J1.5.

- et pourtant ...

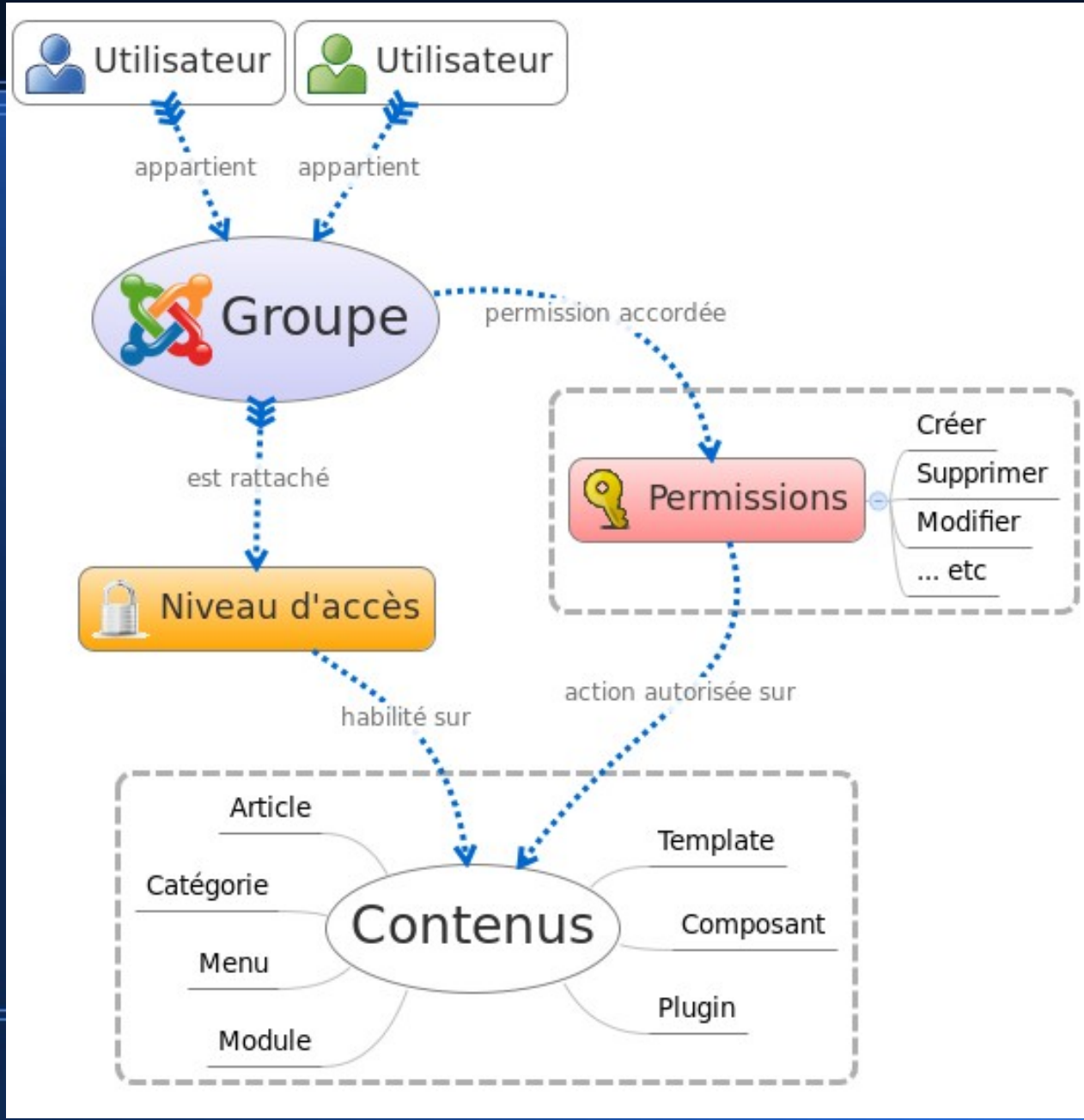
Groupes, niveaux d'accès, permissions !

- Rappel sur les groupes et les niveaux d'accès en J!2.5+



Groupes, niveaux d'accès, permissions !

- Rappel sur les permissions en J!2.5+



Les ACL basées sur les Rôles

- *Pourquoi s'éloigner du modèle de Joomla 1.5 et se compliquer la vie ?*
  - Nos clients attendent plus de simplicité dans la gestion des droits et permissions
  - vous éviterez de vous retrouvez dans des "*impasses*" lors de la phase d'intégration des extensions Joomla
- Un rôle ?
  - une tache logique
  - Une responsabilité au sein d'une organisation
- *Il doit être défini par le metier du client et doit être clairement compréhensible par ce même client.*

Les ACL basées sur les Rôles

- Organisation des rôles d'une entreprise
  - salariés du service “Achats”
    - passer des commandes, expéditions, gestion de stocks...
  - mais il faudra un autre rôle "Marketing" :
    - pour renseigner les fiches produits, les promos sur le site ...
  - ainsi qu'un autre rôle "Comptable" :
    - pour accèder a l'information financiere des ventes ...

un utilisateur pourra être affecté a un ou plusieurs de ces rôles !

- *Objectif : distribuer un CMS à nos clients qui représente son organisation et qu'il peut comprendre facilement !*

Les ACL basées sur les Rôles

- Principe des “**moindres privilèges**”
  - Un rôle permet d'accèder à une fonctionnalité et fourni les permissions pour effectuer une tâche ou un ensemble de tâches connexes.

- Principe de la “**séparation des tâches**”
  - Les tâches et les responsabilités d'un rôle sont **isolées** (et généralement ne se chevauchent pas avec ceux des autres rôles).

Les ACL basées sur les Rôles

- Un rôle représente la combinaison des domaines d'un métier du client
  - Une personne peut être affectée à plus d'un rôle.
  - Plusieurs personnes peuvent partager le même rôle.
  - Un rôle peut être facilement ajouté, supprimé ou transféré entre les utilisateurs.
  - Un rôle correspond au nom et aux compétences de la fonction métier de ce «rôle».

Organisation basée sur les Rôles

- Flexibilité sur les mouvements du personnel et leur responsabilités dans le CMS !
- 3 avantages :
  - L'attribution des rôles aux utilisateurs est intuitive et simple (idem terminologie interne)
  - Libre affectation pour refléter la réalité de l'organisation du personnel
  - Niveaux d'accès basés sur les rôles

    = backend adapté à chaque tâche

STOP ! ... Synthèse mémo.

- Role ?
  - = groupe Joomla
  - Correspond à une tache, une fonction, un service du client ...
- Principes ?
  - Limiter et séparer les permissions
- Objectif ?
  - Administrable simplement par le client

Les ACL dans Joomla 2.5+

- Joomla 2.5+ permet de mettre en place ce type d'architecture (Rôles)
- Il propose de base la structure des groupes de J1.5, mais dans un projet d'entreprise, il vaut mieux effacer ses groupes et recommencer à zéro

“Même les Groupes Gestionnaire et Administrateur peuvent être supprimés si l'organisation de vos ACL est correctement basée sur les rôles.”

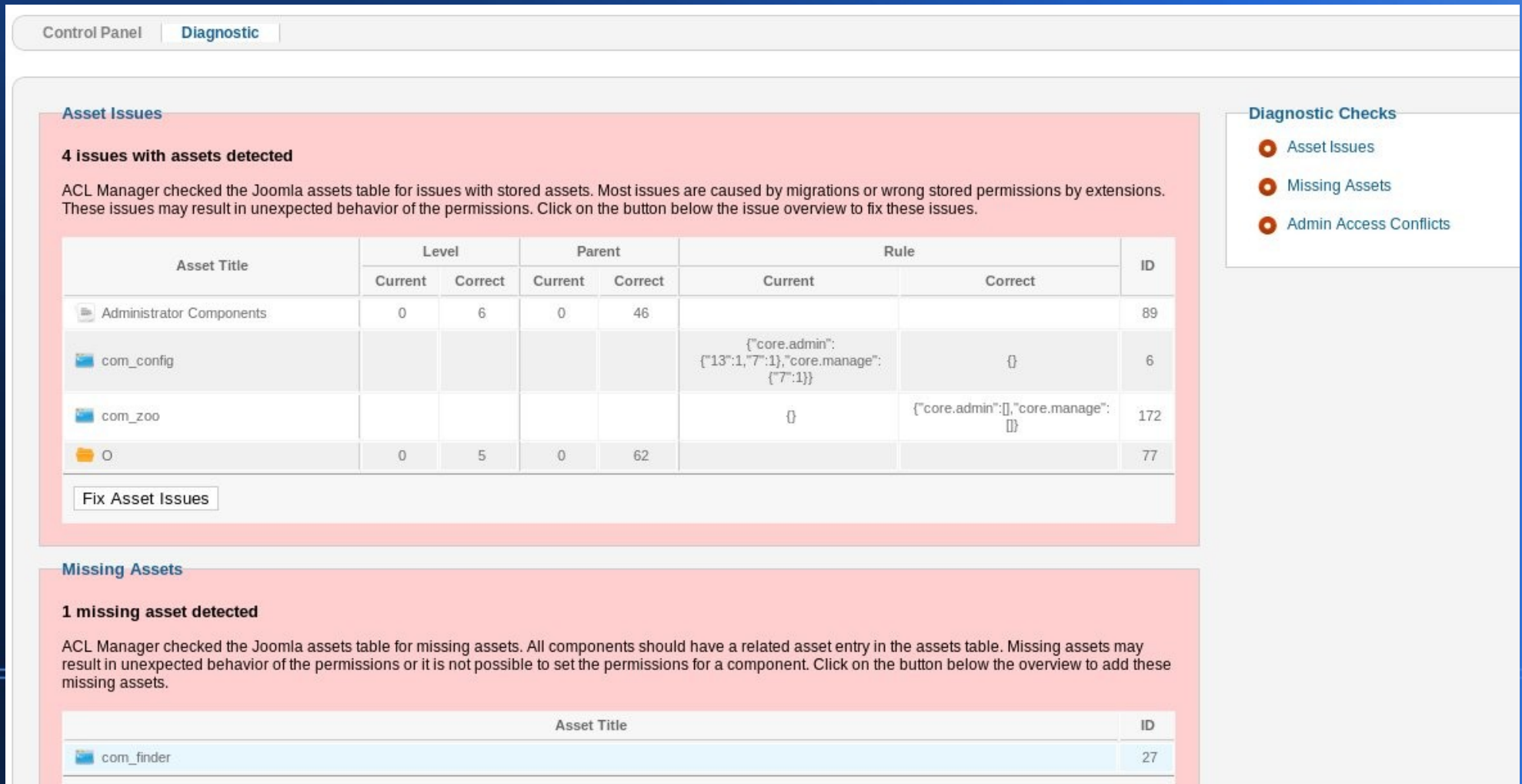
dixit Sander POTJER, développeur de ACL Manager

Et si je rencontre un conflit ?

- Des produits comme **ACL Manager** …
  vous permettent de voir rapidement la cartographie de vos permissions et groupes, et vous fournis de même un diagnostic sur les problèmes possibles.
  - group manager
  - permissions utilisateurs
  - diagnostic

Et si je rencontre un conflit ?

- Diagnostic par **ACL Manager**



Control Panel | Diagnostic

Asset Issues

4 issues with assets detected

ACL Manager checked the Joomla assets table for issues with stored assets. Most issues are caused by migrations or wrong stored permissions by extensions. These issues may result in unexpected behavior of the permissions. Click on the button below the issue overview to fix these issues.

Asset Title	Level		Parent		Rule		ID
	Current	Correct	Current	Correct	Current	Correct	
Administrator Components	0	6	0	46			89
com_config					{"core.admin":{"13":1,"7":1},"core.manage":{"7":1}}	{}	6
com_zoo					{}	{"core.admin":[],"core.manage":[]}	172
O	0	5	0	62			77

Fix Asset Issues

Missing Assets

1 missing asset detected

ACL Manager checked the Joomla assets table for missing assets. All components should have a related asset entry in the assets table. Missing assets may result in unexpected behavior of the permissions or it is not possible to set the permissions for a component. Click on the button below the overview to add these missing assets.

Asset Title	ID
com_finder	27

Diagnostic Checks

- Asset Issues
- Missing Assets
- Admin Access Conflicts

Méthode de mise en place

1. identifier les rôles dont votre client a besoin
   - comprendre l'organisation du client
   - affecter des rôles aux fonctionnalités
     - 1 rôle pour une fonctionnalité
     - 1 rôle pour plusieurs fonctionnalités
     - 1 rôle pour une partie des fonctionnalités d'un composant

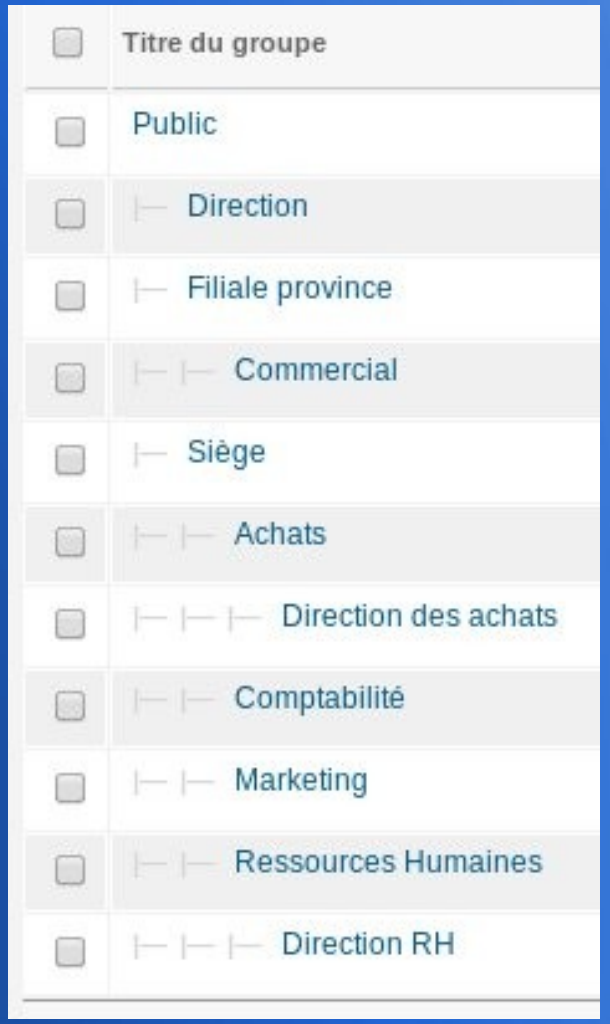
Méthode de mise en place

2. Créer un groupe pour chaque rôle
   - utilisez les **groupes** d'utilisateur pour définir un rôle
     - si vous identifiez 12 rôles, alors créez 12 groupes !
   - les **niveaux d'accès** et les **permissions** doivent être regroupés de facon unique dans un rôle
   - le **nom du groupe** doit correspondre au rôle
     - même s'il est constitué de plusieurs mots

Méthode de mise en place

3. *Aplatir* la hiérarchie du groupe

- philosophie très différente de J1.5,
- groupes avec permissions indépendantes,
- groupe parent commun a tous,
- toutes les permissions communes sont stockées dans le groupe parent.



Méthode de mise en place

4. Affecter les permissions aux rôles

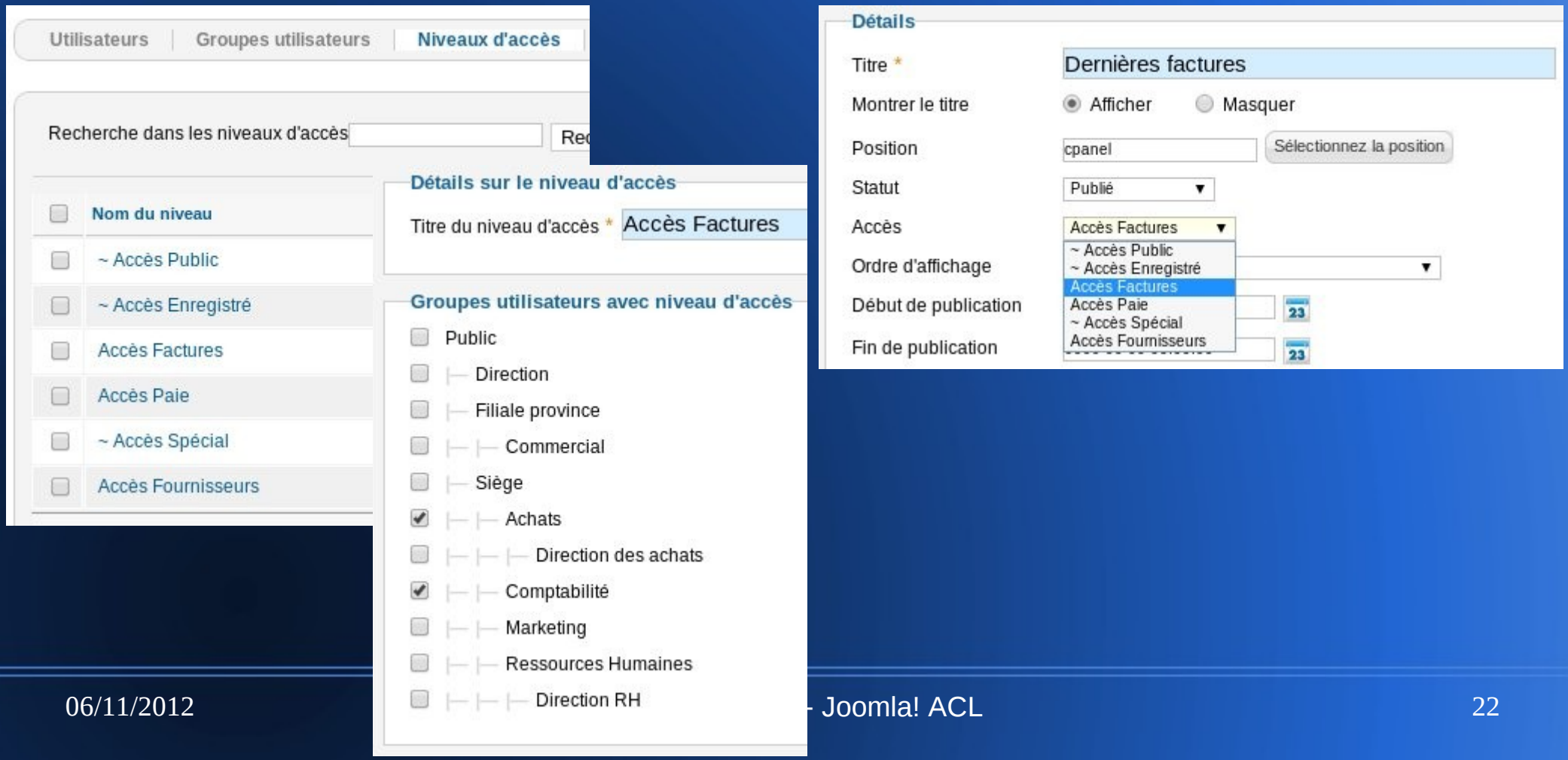
- définir des permissions par défaut dans la configuration générale
- 1 rôle est limité à tout ou partie d'un ou plusieurs composants

Méthode de mise en place

5. Créer des **niveaux d'accès** basés sur les rôles
   - les niveaux d'accès : attribuer une **autorisation d'accès** ! (module, menu, article ...) uniquement pour le simple fait d'accéder ou pas a l'info !
     - Exemple réel : les badges d'identification pour ouvrir des portes !
   - Régles de nommage :
     - 1) 1er niveau : prefixé par un tild : ~public, ~siège ... pour visuellement faciliter l'administration des niveaux d'accès
     - 2) ordonner dans l'ordre croissant des autorisations d'accès

Méthode de mise en place

5. Créer des niveaux d'accès basés sur les rôles



Méthode de mise en place

6. Configurer les permissions
   - 1) par défaut dans la configuration générale
   - 2) par défaut dans chaque composant
   - 3) pour chaque donnée de chaque composant

Méthode de mise en place

- Synthèse
  1. identifier les rôles du client
  2. Créer des groupes pour chaque rôle
  3. Organiser la hierarchie des groupes selon les permissions à gérer
  4. Affecter les permissions aux rôles
  5. Créer des niveaux d'accès selon les groupes et les fonctions installées (extensions …)
  6. Personnaliser les permissions pour chaque fonction

Joomla ACL Hidden Secrets

- Rapport des autorisations groupe /utilisateur
  - Dans la configuration générale, onglet Système
    - Activer le mode “Deboggage Système”
  - Gestion des utilisateurs ou des groupes utilisateurs
    - Bouton "Debug sur le rapport des autorisations"

Joomla ACL Hidden Secrets

- Rapport des autorisations groupe /utilisateur

Recherche dans les attributs | Rechercher | Réinitialiser | - Choisir un composant - | - Choisir le niveau initial - | - Choisir le niveau final -

Légende: [ ] Non applicable [-] Non autorisé [✓] Autorisé [✗] Interdit

Titre de l'attribut	Nom de l'attribut	Connexion au site	Connexion à l'administration	Accès hors-ligne	Super administrer	Accès à l'administration	Créer	Supprimer	Modifier	Modifier le statut	Modifier ses éléments	LFT	Id
Root Asset	root.1	✓	✓	-	-	✓	-	-	✓	-	✓	1 - 436	1
com_admin	com_admin	✓	✓	-	-	✓	-	-	✓	-	✓	2 - 3	2
com_banners	com_banners	✓	✓	-	-	✓	-	-	✓	-	✓	4 - 11	3
Non catégorisé	com_banners.category.10	✓	✓	-	-	✓	-	-	✓	-	✓	7 - 8	35
Bannières Exemples	com_banners.category.15	✓	✓	-	-	✓	-	-	✓	-	✓	9 - 10	40
com_cache	com_cache	✓	✓	-	-	✓	-	-	✓	-	✓	12 - 13	4
com_checkin	com_checkin	✓	✓	-	-	✓	-	-	✓	-	✓	14 - 15	5
com_config	com_config	✓	✓	-	-	✓	-	-	✓	-	✓	16 - 17	6
com_contact	com_contact	✓	✓	-	-	✗	✓	✗	✓	-	✓	18 - 87	7
Non catégorisé	com_contact.category.11	✓	✓	-	-	✗	✓	✗	✓	-	✓	23 - 24	36
Exemples de contacts	com_contact.category.16	✓	✓	-	-	✗	✓	✗	✓	-	✓	25 - 86	41
Site des parcs	com_contact.category.34	✓	✓	-	-	✗	✓	✗	✓	-	✓	26 - 27	59

Astuce ACL Joomla

- Personnalisation tableau de bord Backend
  - Personnalisable selon les rôles de chaque personne (dont le menu d'administration)
    - duppliquer et personnaliser les modules selon le nombre de niveaux d'accès
    - les affecter aux niveaux d'accès souhaités

Prochains rendez-vous lyonnais !

- **4 décembre : JoomSession de “Cook self service”**

  (par son fondateur “Jocelyn Huard” himself)

  - **Nouveau lieu : adresse a venir (sur notre page FaceBook)**
- **8 janvier : Présentation du nouveau composant HikaM.....**
  - **par l'équipe Hikashop**

  + présentation d'un site Joomla par Annick
- **5 février : Atelier template override**
  - **par l'équipe Arwen**

- **Espace temporaire de partage des présentations du Joomgroupe de Lyon :**

  www.garstud.com/joomgroupe/lyon