E5 - BTS Services Informatiques aux Organisations (SIO)
parcours SISR

C3 – MISE EN PLACE ET VERIFICATION DES NIVEAUX D'HABILITATION ASSOCIÉS À UN SERVICE

Présenté par:

MECHRAFI-LACROIX Steven

Année académique : 2024/2026

Objectifs du document

Ce document a pour objectif de présenter la **mise en place et la vérification des niveaux d'habilitation** associés à un service au sein de l'outil de gestion de parc **GLPI**. Il décrit la manière dont les droits d'accès sont attribués aux différents utilisateurs (administrateur, technicien, etc.) afin de garantir que chacun ne dispose que des permissions nécessaires à son rôle.

Il aborde notamment :

1. **La gestion des niveaux d'habilitation (droits) sur GLPI** : profils, rôles et permissions (administrateur, technicien…).
2. **La gestion des habilitations sur les ordinateurs de l'entreprise** : maîtrise des accès aux ressources du parc.

Principe des habilitations dans GLPI

Une **habilitation** correspond à l'ensemble des droits accordés à un utilisateur pour accéder à des fonctionnalités et des données de GLPI. L'objectif est d'appliquer le **principe du moindre privilège** : chaque utilisateur ne reçoit que les permissions strictement nécessaires à l'exercice de ses fonctions.

Dans GLPI, la gestion des habilitations repose sur trois notions complémentaires :

- **Les profils** : ils définissent un ensemble de droits (lecture, écriture, suppression…) sur les différents modules de GLPI (parc, assistance, gestion, administration). Exemples de profils : *Super-Admin*, *Admin*, *Technicien*, *Self-Service*.
- **Les entités** : elles permettent de cloisonner les données par périmètre (site, service, agence). Un utilisateur n'accède qu'aux entités qui lui sont rattachées.
- **Les utilisateurs et groupes** : chaque utilisateur se voit attribuer un ou plusieurs profils, éventuellement limités à certaines entités.

Gérer les niveaux d'habilitation (droits) sur GLPI

La gestion des droits s'effectue depuis le menu **Administration**, qui regroupe les utilisateurs, les groupes, les entités, les profils et les règles.

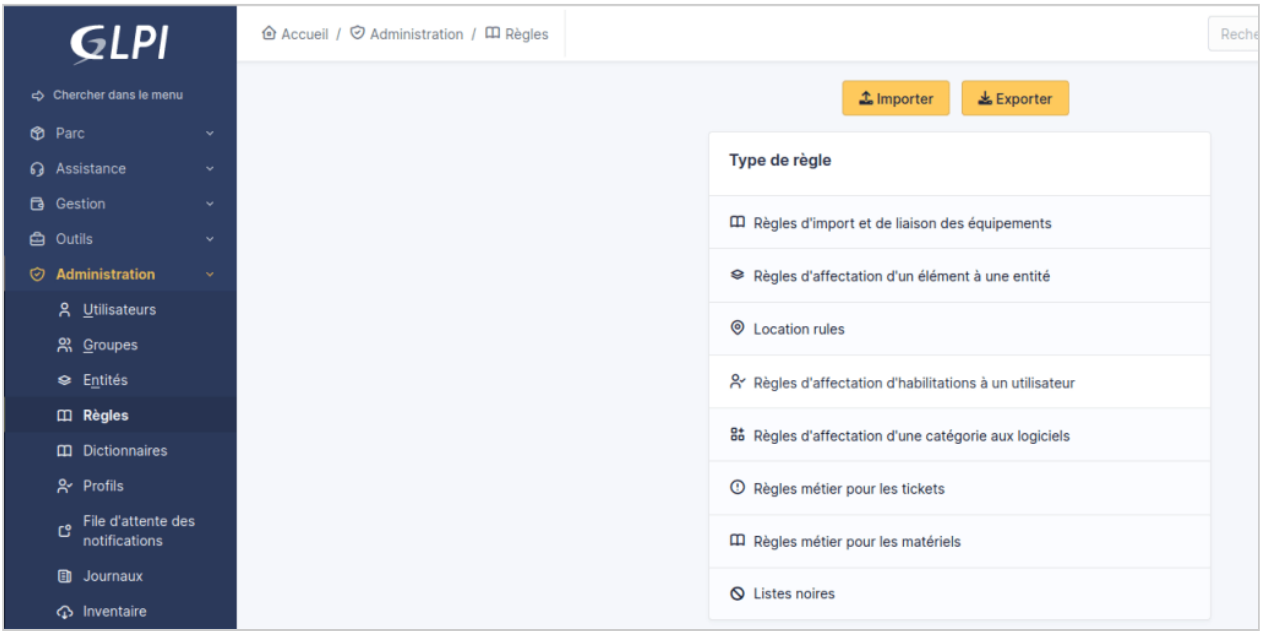
Les principaux profils

Profil	Rôle	Droits typiques
Super-Admin	Administration complète	Accès total, configuration du système
Admin	Administration courante	Gestion du parc, des utilisateurs, des tickets
Technicien	Support et exploitation	Traitement des tickets, gestion du matériel
Self-Service	Utilisateur final	Création et suivi de ses propres demandes

Étapes de configuration

1. **Création ou sélection d'un profil** : dans *Administration* > *Profils*, définir les droits accordés module par module (consulter, ajouter, modifier, supprimer).
2. **Création de l'utilisateur** : dans *Administration* > *Utilisateurs*, créer le compte et renseigner ses informations.
3. **Attribution de l'habilitation** : associer à l'utilisateur le profil correspondant à son rôle, en le limitant à l'entité concernée si nécessaire.
4. **Automatisation par les règles** : dans *Administration* > *Règles*, il est possible de définir des règles qui attribuent automatiquement un profil et une entité à un utilisateur selon des critères (par exemple lors d'un import depuis l'annuaire LDAP/Active Directory).

L'écran **Administration > Règles** permet de centraliser ces différents types de règles, dont les **règles d'affectation d'habilitations à un utilisateur**.



Écran GLPI « Administration > Règles » présentant les différents types de règles, dont les règles d'affectation d'habilitations à un utilisateur.

Vérification des habilitations

Après attribution, il est essentiel de **vérifier** que les droits sont corrects :

- Consulter la fiche de l'utilisateur pour contrôler le profil et l'entité associés.
- Se connecter avec un compte de test pour valider que seules les fonctionnalités prévues sont accessibles.
- Vérifier régulièrement la cohérence des habilitations (revue des accès) afin de retirer les droits devenus inutiles.

Gérer les niveaux d'habilitation sur les ordinateurs de l'entreprise

Au-delà de l'accès à l'outil GLPI lui-même, les habilitations permettent de **maîtriser qui peut consulter ou modifier les informations relatives aux ordinateurs** du parc.

Cloisonnement par entité

Chaque ordinateur est rattaché à une **entité** (site, service, agence). Un technicien affecté à une entité ne voit et ne gère que les ordinateurs de son périmètre, ce qui évite les modifications non autorisées sur le matériel d'un autre service.

Droits sur les actifs matériels

Selon son profil, un utilisateur peut disposer de droits différents sur les ordinateurs :

- **Consultation seule** : visualiser la fiche d'un ordinateur (caractéristiques, logiciels, historique) sans pouvoir la modifier.
- **Modification** : mettre à jour les informations (affectation, statut, localisation).
- **Création / suppression** : ajouter ou retirer un ordinateur du parc.

Bonnes pratiques

- Attribuer aux techniciens un profil limité à leur entité et aux actions nécessaires.
- Réserver les droits de suppression aux profils d'administration.
- Tracer les modifications grâce à l'historique de GLPI, qui enregistre les actions réalisées sur chaque ordinateur.

Synthèse

La mise en place des niveaux d'habilitation dans GLPI repose sur la combinaison des **profils** (droits par fonctionnalité) et des **entités** (cloisonnement par périmètre). Cette organisation garantit que chaque utilisateur — administrateur, technicien ou utilisateur final — n'accède qu'aux ressources et aux ordinateurs qui le concernent, conformément au principe du moindre privilège.

La **vérification régulière** des habilitations (revue des accès et tests de connexion) complète le dispositif et assure le maintien d'un niveau de sécurité conforme aux besoins de l'organisation.