BTS SIO — Option SLAM

ADMINISTRATION DES HABILITATIONS ODOO

Gestion des utilisateurs, des groupes de sécurité et de la politique des droits d'accès

Établissement	Aristée
Période	Octobre 2025
Technologie	Odoo ERP / Mode Développeur Odoo / RBAC (Role-Based Access Control)
Candidat	COUR Cyrille

SOMMAIRE

1. Contexte Applicatif et Objectifs Sécurité

Durant le mois d'octobre 2025, dans le cadre de mes fonctions au sein du service informatique, j'ai été désigné responsable du déploiement opérationnel et de la maintenance de la politique de sécurité sur notre ERP Odoo. Cet outil centralise la majeure partie des flux d'information de notre organisation (CRM, facturation, inventaire, RH).

Mon objectif technique consistait à implémenter un modèle de contrôle d'accès basé sur les rôles (RBAC - Role-Based Access Control) afin de garantir la confidentialité des données et d'appliquer le principe du moindre privilège : chaque collaborateur ne doit accéder qu'aux fonctionnalités strictement nécessaires à l'exercice de sa fonction.

2. Activation des Fonctionnalités d'Administration Avancées

Pour manipuler les groupes de sécurité natifs et configurer finement les droits d'accès d'Odoo qui dépassent le simple choix par défaut, il est indispensable de basculer sur les droits d'administration de bas niveau.

- Se connecter avec un compte possédant les privilèges d'administrateur système.
- Naviguer dans le panneau des Paramètres (Settings).
- Faire défiler la page jusqu'au bloc d'outils techniques et cliquer sur le lien : « Activer le mode développeur » (Activate the developer mode).

3. Gestion et Création des Comptes Utilisateurs

L'intégration d'un nouveau collaborateur ou la modification d'un profil suit un flux d'approbation géré par l'IT via le menu Utilisateurs et Sociétés (Users & Companies) :

- Sélectionner l'option 'Utilisateurs' puis cliquer sur le bouton 'Créer'.
- Renseigner l'identité du collaborateur (Nom, Adresse e-mail professionnelle qui servira d'identifiant de connexion).
- Définir son niveau d'accès initial pour les différentes applications métier installées.

4. Structuration des Groupes et Configuration des Droits (RBAC)

4.1 Définition des Rôles Métiers

Le mode développeur activé fait apparaître le sous-menu masqué nommé « Groupes ». Les groupes agissent comme des conteneurs de sécurité. Au lieu d'assigner des droits individuels fastidieux à chaque utilisateur, on configure les droits sur un groupe (ex : 'Service Achat - Consultation', 'Comptabilité - Écriture') et on y associe les utilisateurs.

- Accéder à Configuration > Technique > Sécurité > Groupes.
- Créer un nouveau groupe sur-mesure ou éditer un groupe existant.

4.2 Application des Règles de Sécurité Avancées

À l'intérieur de la configuration d'un groupe, le service informatique intervient sur deux onglets hautement critiques pour le cloisonnement de la base de données :

- **Droits d'accès (Access Rights) :**

Permet de définir des autorisations de type CRUD (Création, Lecture/Read, Écriture/Write, Suppression/Unlink) sur des tables de données entières (les objets Odoo).

- **Règles sur les enregistrements (Record Rules) :**

Permet d'appliquer des filtres dynamiques (en langage Python/domaines Odoo). Par exemple, faire en sorte qu'un commercial puisse lire la table des clients, mais UNIQUEMENT les clients qui lui sont personnellement rattachés.

 Point d'attention Sécurité : Le droit de 'Suppression' (Unlink) doit être retiré de la quasi-totalité des groupes utilisateurs standards afin de prévenir toute perte de données ou sabotage accidentel de la base de données de production.

5. Conclusion et Validation de l'Infrastructure

La mise en place de cette politique de gestion d'accès durant le mois d'octobre 2025 a sécurisé l'usage de l'ERP Odoo au sein de l'entreprise. Cette démarche méthodique est totalement alignée avec les exigences de la gestion des habilitations demandées dans le référentiel du BTS SIO.

Grâce à l'utilisation rigoureuse des groupes et des règles d'enregistrements, l'administration est centralisée, grandement simplifiée, et l'entreprise est protégée contre les fuites de données internes.