

# GESTION DES DROITS ADMINISTRATEURS SUR LE PARTAGE DE DONNÉES

*Entreprise : PAPREC*

<b>Formation</b> BTS SIO - Option SISR	<b>Année scolaire</b> 2ème Année
<b>Mission réalisée</b> Création et gestion des groupes Active Directory	<b>Contexte</b> Acquisition d'une entreprise de recyclage

## 1. CONTEXTE ET BESOIN

---

### Contexte général

PAPREC a récemment fait l'acquisition d'une entreprise de recyclage qui disposait de sa propre infrastructure Active Directory et de ses serveurs de stockage. Cette acquisition nécessitait une intégration complète des systèmes d'information pour unifier la gestion des utilisateurs et des données.

Dans ce cadre, j'ai été missionné, en tant qu'alternant BTS SIO 2ème année, pour participer à la conception et à la mise en place de l'architecture de groupes Active Directory permettant de gérer les droits d'accès aux partages de données.

### Besoins identifiés

- Centralisation des accès : intégrer tous les utilisateurs dans l'AD PAPREC
- Sécurisation des données : appliquer les standards de sécurité PAPREC
- Gestion structurée des droits : différencier lecture et modification selon les profils
- Continuité d'activité : garantir l'accès aux données pendant et après la migration

## 2. OBJECTIFS

---

### Objectifs principaux

- Concevoir une architecture de groupes Active Directory adaptée à l'organisation
- Créer les groupes AD selon une nomenclature définie
- Configurer les droits d'accès (lecture / modification) sur les dossiers partagés
- Attribuer les groupes aux utilisateurs selon leurs fonctions

## Périmètre de ma mission

Ma contribution s'est concentrée sur la phase de création et de configuration des groupes Active Directory, ainsi que sur l'attribution des droits NTFS sur les dossiers. La migration effective des données a été réalisée par l'équipe système de PAPREC. J'ai pu constater que l'ensemble du processus a fonctionné correctement à l'issue de la migration.

## 3. CONTRAINTES

---

### Contraintes techniques

- Cohabitation temporaire de deux infrastructures Active Directory
- Préservation de l'intégrité des données existantes
- Compatibilité avec les applications métier existantes
- Nomenclature des groupes à respecter strictement

### Contraintes de délais

- Formation à réaliser en 2 semaines pour l'utilisation de Windows Server
- Projet délais 1 Mois

## 4. ENVIRONNEMENT TECHNIQUE

---

Composant	Détail
Systèmes serveurs	Windows Server 2019 / 2022
Postes de travail	Windows 11
Infrastructure AD	Multiplés domaines PAPREC + domaine acquis
Outil principal	ADUC (Active Directory Users and Computers)
Administration avancée	ADSI Edit, PowerShell
Synchronisation	OneDrive Entreprise

## 5. MA CONTRIBUTION PERSONNELLE

---

### Ce que j'ai réalisé

- Analyse de l'existant : audit des 100 comptes utilisateurs et de leurs droits
- Conception de l'architecture de groupes AD (40 groupes au total)
- Création des groupes selon la nomenclature définie
- Configuration des droits d'accès (lecture / modification) sur les dossiers partagés
- Attribution des groupes aux utilisateurs selon leurs fonctions
- Documentation des attributions et création d'une matrice des droits
- Tests de fonctionnement avec les utilisateurs finaux à l'issue de la migration

## Ce que j'ai observé et appris

Bien que la migration physique des données ait été effectuée par l'équipe système de PAPREC, j'ai pu suivre le processus et observer que les droits que j'avais configurés ont bien été appliqués. Tous les utilisateurs ont pu accéder à leurs dossiers conformément aux groupes qui leur avaient été attribués.

## Décisions prises

- Choix du type "Universel" pour les groupes : compatibilité avec les multiples domaines PAPREC
- Désactivation systématique de l'héritage des droits pour repartir sur une base propre
- Mise en place d'une nomenclature stricte et documentée pour les groupes
- Application du principe du moindre privilège pour chaque attribution

## 6. DÉMARCHE ET PLAN D'ACTION

Phase	Période	Actions
Phase 1 - Préparation	Semaine 1	Audit de l'existant, analyse des besoins, conception de l'architecture de groupes, planification, de plus apprentissage de l'utilisation de l'outil Active Directory
Phase 2 - Création des groupes	Semaine 2	Création des 40 groupes selon la nomenclature, configuration des droits de base, tests
Phase 3 - Attribution des droits	Semaine 3	Affectation des utilisateurs aux groupes, validation avec les responsables, documentation
Phase 4 - Suivi post-migration	Semaine 4	Observation du bon fonctionnement après la migration effectuée par l'équipe système, tests d'accès

## 7. MISE EN OEUVRE - ÉTAPES DE DÉPLOIEMENT

### Étape 1 : Conception de la nomenclature

Avant toute création, j'ai défini avec l'équipe la nomenclature des groupes à respecter :

**Format : Fr-[Entreprise]\_[Métier]\_[Niveau] - [Fonction]**

*Exemple : Fr-Lrb\_Metier\_1-Commerce*

- Type de groupe : Universel (compatibilité multi-domaines)
- Localisation : Unité d'organisation dédiée par région
- 40 groupes créés au total

### Étape 2 : Création des groupes dans ADUC

Via l'outil ADUC (Active Directory Users and Computers), j'ai créé les 40 groupes en respectant la nomenclature définie. Chaque groupe a été placé dans l'unité d'organisation (OU) correspondant à sa région.

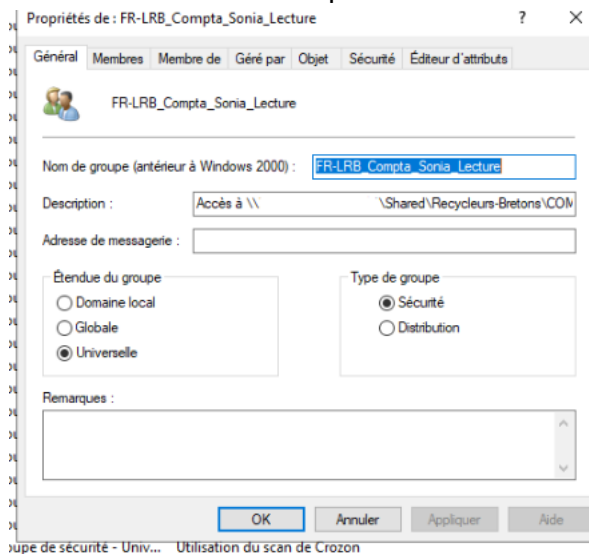
### Étape 3 : Configuration des droits d'accès

- Groupes lecture : droits de lecture uniquement sur les dossiers concernés
- Groupes modification : droits de lecture + écriture + modification
- Application du principe du moindre privilège : chaque utilisateur n'a que les droits nécessaires à son rôle

### Étape 4 : Désactivation de l'héritage

Pour chaque dossier partagé, j'ai désactivé l'héritage des droits existants afin de repartir sur une base propre et d'appliquer uniquement les nouveaux groupes PAPREC.

Chemin : Clic droit > Propriétés > Sécurité > Avancé > Désactiver l'héritage



### Étape 5 : Application des nouveaux droits

J'ai ensuite appliqué les groupes AD sur les dossiers partagés, en définissant le niveau d'accès approprié pour chaque groupe.

Chemin : Propriétés > Sécurité > Avancé > Ajouter > Sélection du groupe AD

FR-LRB_Scan_ComptaFact	Groupe de sécurité - Univ...	
FR-LRB_Compta_Karine_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Compta_Karine_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Compta_Sonia_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Compta_Sonia_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_10-ICPE_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_10-ICPE_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_11-CTHP_Usine_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_11-CTHP_Usine_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_12-Informatique_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_12-Informatique_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_13-SCI_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_13-SCI_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_14-Contrôle_de_gestion_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_14-Contrôle_de_gestion_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_15-NPI_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_15-NPI_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_1-Navaleo_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_1-Navaleo_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_2-Commerce_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_2-Commerce_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_3-Exploitation_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_3-Exploitation_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_4-Comptabilité_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_4-Comptabilité_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_5-Achats_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_5-Achats_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_6-Direction_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_6-Direction_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_7-RSE_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_7-RSE_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_8-Eco_Organismes_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_8-Eco_Organismes_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_9-Projet_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Metiers_9-Projet_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Photos_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Photos_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Publics_Lecture	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Publics_Modification	Groupe de sécurité - Univ...	Accès à \\\
FR-LRB_Users	Groupe de sécurité - Univ...	Groupe global des groupes d'utilisateurs LRB - NE PAS Y METTRE DE COMPTE UTILISATEURS
FR-LRB_Compta_Users	Groupe de sécurité - Univ...	Groupe global des groupes d'utilisateurs LRB accèdent au dossier COMPTA- NE PAS Y METTR...
FR-LRB_Metiers_Users	Groupe de sécurité - Univ...	Groupe global des groupes d'utilisateurs LRB accèdent au dossier METIERS - NE PAS Y METTR...
FR-LRB_Scan_CRZ	Groupe de sécurité - Univ...	Utilisation du scan de Crozon

## Étape 6 : Attribution aux utilisateurs

Chaque utilisateur a été ajouté dans les groupes correspondant à sa fonction et à son service, sur la base de l'audit réalisé en phase 1 et de la validation des responsables de service.

## 8. ARCHITECTURE DES GROUPES ET DROITS

### Répartition des groupes créés

Type de groupe	Droits accordés	Nombre
Lecture seule	Consultation de documents	25
Modification	Lecture + écriture + modification	15
TOTAL		40

### Principes de sécurité appliqués

- Moindre privilège : attribution minimale des droits nécessaires à chaque rôle
- Séparation des rôles : distinction claire entre groupes lecture et modification
- Traçabilité : documentation de toutes les attributions dans un tableau Excel

## 9. TESTS ET VALIDATION

---

### Plan de tests réalisés

- Tests d'accès par groupe d'utilisateurs : vérification que chaque groupe accède uniquement à ses dossiers
- Tests de refus d'accès : vérification que les utilisateurs ne peuvent pas accéder aux dossiers auxquels ils ne sont pas autorisés

### Résultats constatés

Critère de validation	Résultat
Accès aux dossiers pour les utilisateurs concernés	Fonctionnel
Refus d'accès pour les utilisateurs non autorisés	Fonctionnel
Droits lecture / modification correctement différenciés	Fonctionnel
Aucun incident de sécurité constaté post-migration	Confirmé

## 10. DOCUMENTATION PRODUITE

---

- Matrice des droits : tableau Excel listant chaque utilisateur, son groupe et son niveau d'accès

## Dossier Commun

**DOSSIERS INDIVIDUELS** => Lecture/Exécution sur ce dossier seulement Utilisateurs du domaine

**Dossiers nominatifs => Lecture/Modification de l'utilisateur associé**

## DOSSIERS METIERS

**1-Navaléo => OU Navaleo Déconstruction**

2-Commerce => OU Commerce

3-Exploitation => OU Exploit

4-Comptabilité => OU Comptabilité

5-Achats => OU Achats

6-Direction => OU Direction

7-RSE => OU RSE

8-Eco Organismes => OU Eco\_Organismes

9-Projet => OU Projet

10-ICPE-Environnement => OU ICPE

11-CTHP USINE => OU CTHP\_Usine

**12-Informatique** => OU Informatique

13-SCI => OU SCI

**14-Contrôle\_de\_gestion** => OU Contrôle de gestion

15-NPI => OU NPI

**DOSSIERS PARTAGE =>** Lecture/Exécution sur ce dossier seulement Utilisateurs du domaine

**Dossiers nominatifs => Contrôle total de l'utilisateur associé**

**DOSSIERS PUBLICS** => Lecture/Modification Utilisateurs du domaine

## Dossier Compta

Dossier [→ Lecture/Modification](#)

Dossier > Lecture/Modification

**Dossier Photos - Documents Commerciaux => Lecture/Modification**

=> Lecture/Exécution utilisateurs du domaine

**Dossier SCAN** => Lecture/Exécution sur ce dossier seulement Utilisateurs du domaine

**Dossiers nominatifs** => Lecture/Modification de l'utilisateur associé

[illegible]

- Nomenclature des groupes : règles de nommage et exemples de création
- Procédure de création d'un groupe AD : guide pas à pas pour les administrateurs
- Guide d'attribution des droits NTFS : procédure de désactivation de l'héritage et d'application des groupes

## 11. BILAN PERSONNEL

## Compétences acquises

- Maîtrise de l'outil ADUC pour la création et la gestion de groupes Active Directory

- Compréhension de la différence entre droits de partage et droits NTFS
- Application du principe du moindre privilège dans un environnement réel
- Capacité à concevoir une architecture de groupes cohérente avec les besoins métier
- Rédaction de documentation technique claire et exploitable

### Apprentissages personnels

Ce projet m'a permis de confronter les notions théoriques apprises en BTS SIO à une situation réelle en entreprise. J'ai compris l'importance de la planification et de la documentation dans un projet d'infrastructure, ainsi que la nécessité d'impliquer les responsables de service pour valider les attributions de droits.

Le fait d'avoir pu constater que la configuration des groupes que j'avais réalisée a bien fonctionné à l'issue de la migration a été très formateur et valorisant.

### Limites et points d'amélioration

- Je n'ai pas réalisé la migration des données moi-même : cette partie a été prise en charge par l'équipe système
- La création manuelle des 40 groupes aurait pu être automatisée via un script PowerShell
- La phase de tests aurait pu être plus formalisée avec des cas de tests documentés

## 12. EN BONUS :

J'ai appris en bonus comment justement créer ces fichiers dans les serveurs qui sont partagés :

One drive :

**Différence entre "envoyer" et "partager"**

- **Envoyer** : via WhatsApp, SMS, e-mail (copie locale)
- **Partager** : via OneDrive ou serveurs (accès en ligne sécurisé et synchronisé)

Share Dossier :

Il faut bien sur des groupes créer sur l'AD et des utilisateurs pour pouvoir créer ce type de dossier

Donc j'ai appris comment les reconnaître aussi car je ne savais pas différencier un fichier à un fichier partagé

Etapes pour y parvenir :

- 1- Créer un dossier
- 2- Click droit sur le nom, puis propriété
- 3- Partage avancé et cocher partager ce dossier
- 4- Cliquer sur autorisation pour les droits de partage de donnée

En plus la sécurité dans un dossier en termes de droit passe avant le partage.

Par exemple si je donne sur partage tous les droits au recycleur bretons et que sur sécurité je restreins tout cela alors le fichier sera restreint

Et donc ne pas oublier de mettre tous les droits dans partage pour ne pas avoir de restriction derrière en plus.



## 13. CONCLUSION

---

Ce projet m'a permis de contribuer concrètement à l'intégration d'une entreprise acquise par PAPREC, en prenant en charge la conception et la mise en place de l'architecture de groupes Active Directory. Même si je n'ai pas réalisé la migration des données moi-même, ma participation à la configuration des droits d'accès a été essentielle pour que la migration réalisée par l'équipe système se passe correctement.

Ce projet constitue une expérience significative dans le cadre de ma formation BTS SIO, me permettant de valider des compétences concrètes en admini