

Bloc 1 - Procédure Groupe de sécurité



Yohan Ranson

Procédure Concrète : Gestion des Accès Dossiers

Note

Objectif : Chaque service accède uniquement à son dossier. Le service Informatique accède à tous les dossiers.

Prérequis :

- Serveur avec Active Directory.
- Dossiers de services partagés (ex: Achat, Direction).
- Compte administrateur.

Étape 1 : Créer les Groupes de Sécurité

1. Ouvrir "Utilisateurs et ordinateurs Active Directory" depuis le Gestionnaire de serveur.
2. Créez une Unité d'Organisation (OU) nommée Groupes_Securite pour plus de clarté.
3. Dans cette OU, faites un clic droit > Nouveau > Groupe.
4. Créez les groupes suivants (Type: Sécurité, Portée: Globale) :

- GRP_Achat_Acces
- GRP_Direction_Acces
- GRP_Production_Acces
- GRP_Informatique_Admin

6. Ajoutez les utilisateurs à leurs groupes respectifs (Clic droit sur l'utilisateur > Propriétés > Membre de > Ajouter...).

Étape 2 : Appliquer les Permissions aux Dossiers (Sécurité NTFS)

Répétez cette procédure pour chaque dossier de service. L'exemple ci-dessous est pour le dossier Achat.

1. Sur le serveur, faites un clic droit sur le dossier Achat > Propriétés.
 2. Allez sur l'onglet Sécurité puis cliquez sur Avancé.
 3. Cliquez sur Désactiver l'héritage, puis choisissez "Convertir les autorisations héritées...".
 4. Supprimez de la liste tous les groupes donnant des accès généraux comme Utilisateurs.
Conservez impérativement SYSTEM et Administrateurs (avec Contrôle total).
 5. Cliquez sur Ajouter :
 - Principal : GRP_Achat_Acces
 - Autorisations : Cochez Modification.
 - Validez avec OK.
 7. Cliquez à nouveau sur Ajouter :
 - Principal : GRP_Informatique_Admin
 - Autorisations : Cochez Contrôle total.
 - Validez avec OK.
 9. Cliquez sur Appliquer puis OK.
-

Étape 3 : Mapper le Lecteur Réseau Automatiquement (GPO)

Répétez cette procédure pour chaque service en l'appliquant à l'OU correspondante.

1. Ouvrez Gestion des stratégies de groupe.
2. Naviguez jusqu'à l'OU du service (ex: lyon/achat). Faites un clic droit > Créer un objet GPO dans ce domaine, et le lier ici....
3. Nommez la GPO (ex: GPO_Lecteur_Achat), puis faites un clic droit dessus > Modifier....
4. Naviguez vers : Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs.
5. Dans le panneau de droite, faites un clic droit > Nouveau > Lecteur mappé.
6. Configurez les champs suivants :
 - Action : Mettre à jour.
 - Emplacement : Le chemin du partage (ex: \DC1\Achat).
 - Reconnecter : Cochez la case.

- Lettre de lecteur : Cochez Utiliser et choisissez une lettre (ex: U:).

8. Cliquez sur Appliquer puis OK.

Étape 4 : Vérification et Dépannage

- Vérification : Connectez-vous avec un utilisateur Achat. Il doit voir le lecteur U: et ne doit PAS pouvoir accéder à \DC1\Direction. Connectez-vous avec un utilisateur Informatique, il doit pouvoir accéder à tous les dossiers.
- Dépannage : Si un lecteur n'apparaît pas, ouvrez l'Invite de commandes sur le poste client, tapez gpupdate /force et demandez à l'utilisateur de se déconnecter/reconnecter.