Implantation et Sécurisation des Données

Optimisation de l'architecture, gestion des accès et politique de sauvegarde avancée

Choix du système de gestion des fichiers (SGF)

Nous avons opté pour Windows Server 2019 afin de bénéficier d'une gestion des permissions, d'une intégration transparente avec l'Active Directory (AD) et d'une administration facilitée grâce aux stratégies de groupe (GPO). Le protocole SMB est mis en œuvre pour garantir un accès réseau efficace et sécurisé aux différents répertoires.

1. Structuration des groupes et gestion des droits

La gestion des accès repose sur la création de groupes de sécurité dans l'Active Directory, permettant une attribution précise des droits :

- **G_service_administratif** : Claire Dubois
- **G_service_commercial** : Alice Martin, Julien Lefevre
- **G_service_logistique** : Marc Durand
- **G_service_rh** : Sophie Bernard
- **G_delegues_syndicaux** : Paul Morel
- **G_tous_les_utilisateurs**

Chaque groupe se voit attribuer des droits adaptés à ses besoins opérationnels, assurant à la fois confidentialité et collaboration.

2. Organisation de l'arborescence et gestion des permissions

La structure des dossiers, hébergée sur une partition dédiée (**E:\partages**), est conçue pour refléter l'organisation interne :

- E:\partages\administratif
- E:\partages\commercial\commandes
- E:\partages\logistique
- E:\partages\rh
- E:\partages\Syndicat
- E:\partages\utilisateurs\[nom utilisateur]

Les permissions NTFS sont configurées de façon à garantir que :

- Chaque service dispose d'un accès complet à son propre répertoire.
- Le service administratif bénéficie d'un accès en lecture sur l'ensemble des dossiers.
- Le service logistique a une lecture sur le dossier commercial et un accès total sur ses propres ressources.
- Les dossiers personnels sont strictement réservés à chaque utilisateur.
- Le dossier Syndicat est accessible à tous en lecture, avec modification réservée aux délégués syndicaux.

3. Automatisation des connexions via GPO

Pour simplifier l'accès aux ressources, une GPO spécifique est créée afin de monter automatiquement les lecteurs réseau selon l'appartenance aux groupes AD :

1. Lancement de la console GPMC.msc
2. Création d'une GPO nommée "lecteur_reseau"
3. Ajout des lecteurs mappés dans Configuration utilisateur > Préférences > Lecteurs mappés
4. Définition du ciblage en fonction des groupes AD

4. Politique de sécurité, gestion des quotas et sauvegardes

4.1 Sécurité et quotas

Le contrôle d'accès est strictement basé sur les groupes AD et renforcé par des quotas définis par service, limitant l'espace disque disponible afin de prévenir toute saturation.

4.2 Sauvegarde et restauration

La politique de sauvegarde actuelle concerne principalement les bases de données et les fichiers critiques des services. Cependant, des risques subsistent concernant les données personnelles, les fichiers de configuration et l'absence de redondance externe. Afin d'assurer la résilience du système, il est désormais recommandé d'inclure :

- Les répertoires personnels dans les sauvegardes régulières
- L'exportation fréquente des fichiers de configuration
- Des sauvegardes externalisées sur le Cloud ou un NAS distant
- **L'activation des snapshots réguliers sur le serveur de fichiers**, permettant de restaurer rapidement des fichiers ou dossiers supprimés ou altérés par erreur, offrant ainsi une couche de sécurité supplémentaire et une restauration quasi-instantanée en cas d'incident.

Conclusion

L’implantation des données sur un serveur centralisé, sécurisé et automatisé via GPO permet une gestion efficace, une traçabilité renforcée et une administration simplifiée. L’ajout d’une stratégie de sauvegarde complète, intégrant la gestion des snapshots, garantit la disponibilité et l’intégrité des données, assurant la pérennité des services informatiques de GSB.