Objet : Expression de besoin – Mise en place du DFS pour la continuité des partages réseau

Bonjour à vous,

Dans le cadre de la sécurisation et de l’amélioration de la résilience de notre infrastructure de fichiers, je vous propose la mise en place du service \*\*Distributed File System (DFS)\*\* sur nos serveurs Windows afin d’assurer une continuité de service optimale pour les partages réseau critiques.

**Objectifs de la mise en place du DFS :**

L’objectif est de garantir un accès transparent, redondant et sécurisé aux ressources partagées, même en cas de panne d’un serveur. Le DFS permettra également une administration centralisée des chemins d’accès et une réplication des données entre plusieurs sites ou serveurs.

**1. Mise en place de l’espace de noms DFS (DFS Namespace) :**

• Créer un espace de noms logique (ex. : \entreprise.local\partages) regroupant les dossiers partagés de manière centralisée.

• Masquer les chemins physiques aux utilisateurs et faciliter l’administration des accès.

**2. Installation d’un deuxième serveur de fichiers :**

• Installer un serveur de fichiers secondaire dans un site distant ou dans la même salle serveur, selon les besoins en tolérance de panne.

• Configurer les mêmes partages que sur le serveur principal.

**3. Réplication des données avec DFS-R (DFS Réplication) :**

• Activer la réplication des dossiers critiques entre les deux serveurs de fichiers.

• Choisir une topologie de réplication adaptée (hub and spoke ou full mesh).

• Utiliser des quotas et filtres pour limiter les réplications inutiles.

**4. Résilience et continuité d’accès :**

• En cas d’indisponibilité du serveur principal, les utilisateurs seront redirigés automatiquement vers le serveur secondaire via DFS.

• Le mappage des lecteurs réseau pourra être effectué via GPO sur le chemin d’espace de noms DFS unique.

**5. Sécurité et traçabilité :**

• Mettre en œuvre les bonnes pratiques de sécurité ANSSI :

- Utilisation exclusive de droits NTFS (jamais de droits utilisateurs directs).

- Chiffrement des volumes (BitLocker) sur les serveurs.

- Audit des accès aux fichiers via GPO et journalisation.

• Vérifier la cohérence des autorisations et la classification des données.

• Intégrer le suivi des réplications dans notre outil de supervision.

**6. PCA spécifique aux données partagées :**

• Documenter la configuration DFS et les stratégies de réplication.

• Intégrer DFS dans notre plan de continuité d’activité (PCA) global.

• Définir des procédures de restauration rapide des données partagées.

**7. Tests et validation :**

• Simuler l’arrêt du serveur principal pour valider la redirection automatique vers le serveur secondaire.

• Mesurer les délais de synchronisation et vérifier la cohérence des données.

• Sensibiliser les utilisateurs à l’utilisation du nouveau chemin d’accès DFS.

Cette solution nous permettra de garantir une disponibilité maximale des ressources partagées tout en renforçant la sécurité et la traçabilité des accès aux fichiers. Elle s’inscrit pleinement dans notre stratégie de cybersécurité et de conformité réglementaire (notamment RGPD).

Je reste à votre disposition pour toute précision complémentaire ou pour la mise en œuvre opérationnelle de cette solution.

Bien cordialement,

Fabien PICHON

DSI

Informatique