Windows Server 2025: Sécurité des Fichiers et Partage

Introduction aux Permissions NTFS et au Partage de Fichiers

- Windows Server gère les fichiers et dossiers avec deux couches de sécurité :
  - Permissions NTFS : Liées au système de fichiers.
  - Permissions de Partage : Liées à l'accès réseau.
- Objectifs :
  - Contrôler finement l'accès aux données.
  - Distinguer les permissions locales et réseau.
  - Sécuriser les fichiers sensibles.

Permissions NTFS

- Les permissions NTFS s'appliquent aux fichiers et dossiers sur les volumes formatés en NTFS.
- Permissions de Base :
  - Lecture
  - Écriture
  - Lecture et Exécution
  - Liste du Contenu du Dossier
  - Modification
  - Contrôle Total
- Permissions Spéciales (Granulaires) : Assignées via 'Sécurité' > 'Avancé'.
- Héritage : Les permissions peuvent être héritées du dossier parent, ou bloquées pour des configurations spécifiques.

Permissions de Partage

- Les permissions de partage s'appliquent uniquement via l'accès réseau.
- Niveaux de Permissions :
  - Lecture
  - Modification
  - Contrôle Total
- Règle Cumulative : Permissions effectives = Permissions NTFS ∩ Permissions de Partage. Les permissions les plus restrictives s'appliquent.
- Exemple :
  - Partage : Contrôle Total
  - NTFS : Lecture Seule
  - Résultat Effectif : Lecture Seule

Mise en Place d'un Serveur de Fichiers

- Installer le rôle 'Serveur de fichiers et de stockage'.
- Créer des dossiers partagés (ex : \SRV-DATA\collaboratif$).
- Appliquer les permissions NTFS selon les groupes AD.
- Utiliser les GPO pour mapper les lecteurs automatiquement.
- PowerShell :
  - `Install-WindowsFeature -Name FS-FileServer`
  - `New-SmbShare -Name "collaboratif" -Path "D:\partages\collaboratif" -FullAccess "GroupeCollaboratif"`

Sécurisation des Données : Chiffrement et Bonnes Pratiques

- EFS (Encrypting File System) :
  - Chiffre les fichiers/dossiers NTFS pour un utilisateur spécifique. Non recommandé pour les données partagées.
- BitLocker :
  - Chiffre le volume entier (disque). Recommandé pour les serveurs mobiles ou les sauvegardes locales.
- Recommandations de Cybersécurité :
  - Utiliser les groupes AD pour l'attribution des permissions. Ne jamais assigner de permissions à des utilisateurs individuels.
  - Activer l'audit des accès aux fichiers sensibles (journaux de sécurité).
  - Restreindre l'accès aux partages administratifs (C$, ADMIN$).

DFS (Distributed File System)

- DFS regroupe plusieurs partages physiques en un seul arbre logique.
- Types de DFS :
  - DFS Namespace : Arbre logique (ex : \\entreprise.local\docs) qui masque les chemins physiques.
  - DFS Replication (DFS-R) : Réplication automatique des dossiers entre plusieurs serveurs.
- Avantages :
  - Haute disponibilité des données, meilleure distribution géographique et transparence pour l'utilisateur.
- Implémentation :
  - Installer les rôles DFS Namespace + DFS-R. Créer un espace de noms. Ajouter les dossiers cibles et configurer la réplication.

Plan de Continuité d'Activité (PCA) pour le Serveur de Fichiers et DFS

- Objectifs :
  - Continuer à servir les données en cas de panne du serveur principal. Distribuer les charges et les lieux d'accès.
- Stratégies :
  - Réplication DFS-R entre deux serveurs (ex : SRV-FICHIERS1 et SRV-FICHIERS2).
  - Déploiement via un espace de noms DFS redondant (espace de noms hébergé sur plusieurs serveurs).
  - Mapping via GPO du chemin DFS (ex : \\entreprise.local\partages).
- Bonnes Pratiques :
  - Définir une topologie de réplication appropriée (Hub and Spoke ou Full Mesh). Utiliser des quotas et des filtres pour la réplication. Tester régulièrement le basculement.

Cybersécurité et Audit des Partages

- Limiter la Surface d'Attaque :
  - Désactiver les anciens protocoles (SMBv1). Bloquer les partages inutilisés.
- Activer l'Audit des Accès aux Fichiers :
  - GPO > Audit > Activer 'Auditer l'accès aux fichiers'. Examiner les événements de sécurité 4663.
- Utiliser des Outils comme 'AccessChk' de Sysinternals :
  - Pour analyser les permissions effectives.
- Étiqueter et Classer les Données Sensibles :
  - Intégration avec Microsoft Information Protection (MIP). Formation de sensibilisation des utilisateurs.
- Surveillance en Temps Réel des Partages :
  - Intégration avec un SIEM. Détection des anomalies comportementales.

Conclusion

- Le serveur de fichiers, combiné avec NTFS et DFS, est un outil puissant pour centraliser et sécuriser les données d'entreprise.
- L'application des meilleures pratiques en matière de permissions, de chiffrement, d'audit et de PCA garantit une infrastructure robuste, performante et conforme aux exigences de cybersécurité.

Fin du Cours