TP n°5
Implémentation d'une Stratégie de compte et d'audit - Corrigé

Etudiant: Bouzara Zakaria

Matricule: 212138069681

RSD M1 groupe TP 3

A. Comment sont constitués les noms des comptes d'utilisateur ?

Les noms des comptes sont généralement composés d'un identifiant standardisé (par exemple, prénom.nom ou initiale+nom) pour assurer leur unicité.

B. Quelle stratégie allez-vous utiliser pour résoudre des conflits de noms de comptes d'utilisateurs ?

En cas de conflit, on ajoute un identifiant supplémentaire (numéro séquentiel, lettre ou département) afin de différencier les comptes identiques.

C. Qu'allez-vous utiliser comme suffixe UPN pour les comptes d'utilisateurs ?

On utilise comme suffixe UPN le domaine principal (par exemple, @nwtraders.msft) ou un suffixe spécifique défini par la localisation, tel que @Bab_ezzouar.

D. Quelle convention d'attribution de nom allez-vous utiliser pour les comptes de serveurs ?

Pour les serveurs, on adopte une convention avec un préfixe indicatif (ex : SRV) suivi du rôle ou de la fonction (par exemple, SRV-DB1).

E. Quelle convention d'attribution de nom allez-vous utiliser pour les ordinateurs clients ?

Les ordinateurs clients sont nommés avec un préfixe (comme PC ou WKS) suivi d'un identifiant unique ou d'un numéro, pour faciliter l'inventaire et la gestion.

F. Quels paramètres de stratégie de mot de passe allez-vous appliquer au domaine nwtraders.msft ?

Pour nwtraders.msft, la stratégie de mot de passe impose une longueur minimale, des caractères complexes, une expiration périodique et la conservation d'un historique pour éviter la réutilisation.

G. Quels paramètres de stratégie de mot de passe allez-vous appliquer au domaine corp.nwtraders.msft ?

Pour corp.nwtraders.msft, on applique des paramètres similaires voire plus stricts (longueur accrue, verrouillage renforcé) afin de renforcer la sécurité du domaine.

H. Quels paramètres d'audit des succès allez-vous inclure à votre plan ?

Le plan inclut l'audit des succès sur les connexions réussies, les modifications d'objets sensibles et l'accès aux ressources critiques.

I. Quels paramètres d'audit des échecs allez-vous inclure à votre plan ?

L'audit des échecs portera sur les tentatives de connexion infructueuses, les accès refusés et les modifications non autorisées d'objets.

J. Quelles sont les unités d'organisation créées ?

Les unités d'organisation créées comprennent généralement des OU pour les utilisateurs, les groupes, les serveurs et les ordinateurs clients.

K. Parmi les nouvelles unités d'organisation, lesquelles contiennent des comptes d'utilisateurs et de groupes ?

Les OU dédiées aux comptes d'utilisateurs et aux groupes sont celles nommées « Utilisateurs » ou « Personnel » et « Groupes ».

L. Quel est l'état du suffixe UPN *Votre_Ville* après l'avoir activé ?

Après activation, le suffixe UPN Votre_Ville apparaît comme configuré, mais il peut rester non routable s'il existe un conflit ou une mauvaise configuration.

M. Que pouvez-vous faire pour résoudre ce conflit de routage du suffixe UPN ?

Pour résoudre ce conflit de routage, il faut vérifier et corriger les configurations DNS et Active Directory, ou désactiver le suffixe en conflit.

N. Quels sont les éléments répertoriés pour les entrées objectGUID, objectSID et SIDHistory du groupe global G IT Admins ?

Le groupe global G IT Admins possède un objectGUID unique, un objectSID principal et un SIDHistory qui répertorie d'éventuels anciens SIDs issus d'une migration.

O. Quels sont les éléments répertoriés pour les entrées objectGUID, objectSID et sIDHistory du groupe global G IT Admins ?

Les entrées pour objectGUID, objectSID et SIDHistory du groupe sont identiques à celles mentionnées en N, assurant une continuité des identifiants.

P. L'une des entrées objectGUID, ObjectSID ou sIDHistory a-t-elle été modifiée suite au déplacement ?

Aucun des identifiants (objectGUID, objectSID ou SIDHistory) n'est modifié lors d'un déplacement, garantissant l'intégrité de l'objet.

Q. Est-ce que le groupe auquel vous avez accordé les autorisations pour ce dossier à l'étape 1 possède toujours des autorisations Contrôle total sur le dossier ? Expliquez pourquoi.

Le groupe conserve ses autorisations de contrôle total sur le dossier après le déplacement, car les permissions sont basées sur des SIDs qui restent inchangés dans Active Directory.