**TP n°5**

**Implémentation d’une**

**Stratégie de compte et d’audit - Corrigé**

1. **Comment sont constitués les noms des comptes d’utilisateur ?**

* La longueur maximale du nom est de 20 caractères en majuscules ou minuscules. La casse n'est pas prise en compte.
* Certains caractères sont interdits    **/ \** **[ ] : ; , +** **\*** **, < >.**
* Noms d'utilisateurs uniques : Il peut exister 2 **noms** **relatifs** dans un même domaine, mais pas dans une même **UO**. Par contre, il ne peut pas y avoir 2 **noms uniques** dans un même annuaire.
* Noms uniques (WIN, WIN-2) et noms uniques relatifs (WIN User, WIN-2 User).
* (Pour les comptes créés dans le domaine père (nwtraders.local) les noms suivent la syntaxe suivante : nom\_Ordinateur**User.** Pour les comptes créés dans le domaine fils (fei.nwtraders.local) les noms suivent la syntaxe suivante : prenomUser**NomUser).**

1. **Quelle stratégie allez-vous utiliser pour résoudre des conflits de noms de**

**Comptes d’utilisateurs ?**

* Utiliser des préfixes et suffixe.
* On peut coder dans une entreprise suivant un identifiant unique suivit du nom et prénom ou d’autre informations par exemple.

1. **Qu’allez-vous utiliser comme suffixe UPN pour les comptes d’utilisateurs ?**

* L’UPN ou *User Principal Name* est l’identifiant par défaut pour l’ouverture de session Active Directory. Son format ressemble à une adresse email avec la présence du caractère « @ ».
* Le suffixe UPN correspond à ce qui se trouve après le @ dans le nom des compte d’utilisateur.
* Il correspond au nom du domaine DNS où il se trouve par défaut et dans notre cas c’est : @nwtraders.local pour les utilisateurs se trouvant dans le domaine parent et @fei.nwtraders.local pour les utilisateurs se trouvant dans le domaine fils.
* On peut changer le UPN lors de la création d’un utilisateur dans «  Domain et approbations Active Directory -> Domaines et approbations -> Propriétés ».
* Cette forme permet à tous d’ouvrir une session avec le nom qu’ils utilisent pour leur compte de messagerie.

1. **Quelle convention d’attribution de nom allez-vous utiliser pour les comptes de serveurs ?**

* Quelques lettres du sites (pays,ville,ect…) hébergeant le serveur, quelques caractères du type service (application fournie par le serveur), et le numéro de série identifiant le serveur avec les autres éléments.

1. **Quelle convention d’attribution de nom allez-vous utiliser pour les ordinateurs clients ?**

* *« PC-nom\_user » si il y a un nombre limité et minime d’ordinateurs et rajouter un numéro pour identifier chacun.* Sinon, On peut utiliser le nom du compte utilisateur et un numéro incrémentiel : *user001, user002.*

1. **Quels paramètres de stratégie de mot de passe allez-vous appliquer au domaine nwtraders.msft ? (nwtraders.local)**

Stratégie de mot de passe qu’on va utiliser dans le domaine nwtraders.local pour notre cas sont :

* Mettre un délai de renouvellement de mot de passe (Durée minimum de réinitialisation de mot de passe = 7 Jour, durée maximum d’utilisation = 15 à 30,40 jusqu’à 60 jours).
* Un mot constitué Des caractères alphanumériques (majiscule,minuscule,chiffre).
* ne contenant pas d’informations personnelles.
* court (8 caractères et 12 caractères).
* facile à retenir (on choisit un mot et en remplaçant a par @, i par 1, le e par 3 par exemple on peut rajouter le moi avec un caractère redondant).
* *Conserver l’historique des mots de passe 24 mots de passe mémorisés*. Cela permettra d'atténuer les vulnérabilités causées par la réutilisation des mots de passe.
* Utiliser un cryptage réversible pour enregistrer le mot de passe « désactiver ».Ce paramètre prend en charge les applications qui utilisent des protocoles qui nécessitent des mots de passe utilisateur pour l’authentification. Le stockage de mots de passe crypté de manière réversible signifie que les mots de passe crypté peuvent être déchiffrés. Ensuite, un attaquant qualifié qui peut pirater ce chiffrement peut utiliser le compte infecté pour se connecter aux ressources réseau.

1. **Quels paramètres de stratégie de mot de passe allez-vous appliquer au domaine corp.nwtraders.msft ? (fei.nwtraders.local)**

* Mettre un délai de renouvellement de mot de passe.
* Un mot constitué Des caractères alphanumériques (majiscule,minuscule,chiffre) et de caractères spéciaux.
* ne contenant pas d’informations personnelles.
* court (8 caractères et 12 caractères).
* facile à retenir (on choisit un mot et en remplaçant a par @, i par 1, le e par 3 par exemple on peut rajouter le moi avec un caractère redondant).

1. **Quels paramètres d’audit des succès allez-vous inclure à votre plan ?**

1. **Quels paramètres d’audit des échecs allez-vous inclure à votre plan ?**

1. **Quelles sont les unités d’organisation créées ?**

Les UO crée sont :

1. IT
2. Research
3. Accounting
4. **Parmi les nouvelles unités d’organisation, lesquelles contiennent des comptes d’utilisateurs et de groupes ?**

* L’unité IT contient deux groupes locaux (DL RessourcesAdmins,DL  AccountingAdmins) et un groupe global (G Admins).

1. **Quel est l’état du suffixe UPN *Votre\_Ville* après l’avoir activé ?**

1. **Que pouvez-vous faire pour résoudre ce conflit de routage du suffixe UPN ?**
2. **Quels sont les éléments répertoriés pour les entrées objectGUID, objectSID et SIDHistory du groupe global G IT Admins ?**
3. **Quels sont les éléments répertoriés pour les entrées objectGUID, objectSID et sIDHistory du groupe global G IT Admins ?**
4. **L’une des entrées objectGUID, ObjectSID ou sIDHistory a-t-elle été modifiée suite au déplacement :**

1. **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.**