

TP RESEAUX N°5 :

Modification des autorisations sur les objets Active Directory

Objectif

Pour répartir la charge entre les administrateurs, votre entreprise souhaite que chaque administrateur puisse créer et supprimer des comptes ordinateurs et réinitialiser les mots de passe utilisateur. Ces tâches spécifiques sont effectuées dans les unités d'organisation qui lui sont affectées.

Dans ce TP, vous allez effectuer les tâches suivantes :

- ✓ Déléguer le contrôle des unités d'organisation.
- ✓ Tester les autorisations déléguées. XP => stratégie de securite de domaine
Local => stratégie de securite de controleur de domaine

Exercices 1 : Préparer Creation de +eurs administrateurs la délégation de contrôle de l'unité d'organisation

1. Créer deux comptes utilisateurs Amar.Benaissa, Rayan.Touati, ces utilisateurs doivent pouvoir ouvrir une session locale sur la machine serveur. Réfléchissez à une solution qui leur permet cet accès. Pour accorder ce type d'accès (au serveur), a Amar et Rayan, il faut que les deux users soit membre d'un grp système qui a ce privilège et il vont l'avoir par le principe d'heritage, le group sys est :Operateur de serveurs
2. Créer une unité d'organisation UO_RH, dans cette unité d'organisation créer deux autres unités Users et Computers.
3. Dans l'unité d'organisation Users, créer un compte utilisateur Nassima.Lamouri.

On vous demande de répartir les tâches administration de l'unité d'organisation UO_RH entre les utilisateurs Amar.Benaissa et Rayan.Touati. Donc, déléguer le contrôle de l'unité d'organisation Users à l'utilisateur Amar.Benaissa et le contrôle de l'unité d'organisation Computers à l'utilisateur Rayan.Touati.

Exercices 2 : Déléguer le contrôle de l'unité d'organisation Deleguer le controle dans une seul unite wela kima nhabo

1. Déléguer le contrôle de l'unité Users à l'utilisateur Amar.Benaissa de telle sorte de lui attribuer le droit de réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session au sein de UO_RH :

- a. Sur le serveur, ouvrir une session en tant qu'administrateur.
- b. Cliquer avec le bouton droit sur l'unité d'organisation Users, puis cliquer sur Délégation de contrôle.
- c. Dans la page Bienvenue de l'Assistant Délégation de contrôle, cliquer sur Suivant.
- d. Dans la page Utilisateurs ou groupes, sélectionner Amar.Benaissa, puis cliquer sur Suivant.
- e. Dans la page Tâches à déléguer, Délégez les tâches courantes suivantes : « Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session »
- f. Cliquer sur Suivant, puis sur Terminer.

2. Déléguer le contrôle de l'unité Computers à l'utilisateur de telle sorte de lui attribuer le droit de Créer, supprimer et gérer les comptes ordinateurs au sein de UO_RH.

- a. En tant qu'administrateur, cliquer avec le bouton droit sur l'unité d'organisation Computers, puis cliquer sur Délégation de contrôle.
- b. Dans la page Bienvenue de l'Assistant Délégation de contrôle, cliquer sur Suivant.
- c. Dans la page Utilisateurs ou groupes, sélectionner Rayan.Touati, puis cliquer sur Suivant.
- d. Dans la page Tâches à déléguer cliquez sur Créer une tâche personnalisée à déléguer, puis cliquez sur Suivant.
- e. Dans la page Type d'objet Active Directory, cliquer sur Seulement des objets suivants dans le dossier, puis activez la case à cocher Objets Ordinateur.
- f. Activer les cases à cocher Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier, puis cliquez sur Suivant.
- g. Dans la page Autorisations, activez la case à cocher Générales.
- h. Sous Autorisations, activez les cases à cocher Lire et Écrire, puis cliquez sur Suivant.
- i. Dans la page Fin de l'Assistant Délégation de contrôle, cliquez sur Terminer.

3 Tester les autorisations de l'unité d'organisation

- a. Fermer la session de l'administrateur et ouvrir une session en tant que Amar.Benaissa.
- b. Accéder à l'unité d'organisation Users.
- c. Essayer de supprimer le compte d'utilisateur Nassima.Lamouri. Qu'est-ce que vous remarquez. on peut pas.....
- d. Essayez d'activer ou de désactiver ce compte d'utilisateur. Qu'est-ce que vous remarquez. on peut pas.....
- e. Réinitialisez le mot de passe de Nassima.Lamouri. Que remarquez-vous ? on peut car user Amar a été délégué pour ce contrôle.....

.....
.....
.....

f. Fermer la session et ouvrir une session en tant que Rayan.Touati.

g. Créer un compte d'ordinateur dans l'unité d'organisation Computers. Que remarquez-vous ?

.....
user Rayan, devrait pouvoir crée un compte d'ordinateur dans l'unité d'organisation computer
.....
.....

Exercices 3 : Bloquez l'héritage entre objets Active Directory (retour aux commandes)

1. Déconnectez-vous et ouvrez une session avec l'administrateur.

2. Dans UO_RH, bloquez l'héritage pour que l'UO Users n'hérite pas des droits délégués à UO_RH.

3. Ouvrez une session avec le user du Amar.Benaissa et essayez de réinitialiser le mot de passe de Nassima.Lamouri. Que remarquez-vous ?

Amar peut reinisialiser le mdp car cette autorisation n'est pas hérite du UO RH.....
.....
.....

Rappel sur comment supprimer les autorisations héritées

1. Dans la boîte de dialogue **Propriétés** de l'unité d'organisation, dans l'onglet **Sécurité**, cliquez sur **Paramètres avancés**.

2. Dans l'onglet **Autorisations** de la boîte de dialogue **Paramètres de sécurité avancé**, désactivez la case à cocher **Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants. Cela inclut les objets dont les entrées sont spécifiquement définies ici**.

3. Dans la boîte de dialogue **Sécurité**, cliquez sur **Supprimer**.

4. Dans la boîte de dialogue **Paramètres de sécurité avancé**, cliquez sur **OK**.

5. Affichez les paramètres de sécurité de votre unité d'organisation en effectuant les actions suivantes :

a. Cliquez avec le bouton droit sur votre unité d'organisation, puis cliquez sur **Propriétés**.

b. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Sécurité**.

6. Indiquez les noms d'utilisateur ou de groupe qui disposent d'autorisations héritées ou explicites