Partie windows

Elements de correction: les éléments de correction ne sont pas un corrigé exhaustif. Ils se contentent de reprendre les points clefs de chaque exercice.

Question 1 : acces partage

Contexte: un domaine avec un contrôleur de domaine **cd1** et deux ordinateurs membres du domaine **station1** et **station2**. Il existe trois utilisateurs testAD2, testAD4 et testAD5 sur le domaine.

On souhaite partager un dossier nommé donnees situé à la racine de c:\ sur **station1** de façon à ce que deux utilisateurs testAD2 et testAD4 aient les accès suivants :

- en ouvrant une session sur **station1**, testAD2 a accès en contrôle total au partage; testAD4 y a accès en lecture/exécution/affichage du contenu du dossier
- en se connectant depuis une autre machine (**station2** par exemple) sur le partage, testAD2 et testAD4 ont un accès en lecture seule.

Précisez les opérations à effectuer pour mettre en place cette politique.

Votre chef vous demande maintenant que l'utilisateur testAD5 aie les même accès que testAD2. Que faites-vous ?

Votre chef vous demande maintenant que testAD2 perde ses accès au dossier donnees. Que faites-vous ?

Elements de correction:

Deux choses à mettre en évidence dans cet exercice :

- la différence entre les droits d'accès locaux (ntfs via Propriétés/sécurité) et via partage (Propriétés/Partage/autorisations). L'accès au partage à distance nécessite de satisfaire les deux. Le premier suffit à l'accès local.
- une gestion conforme aux bonnes pratiques du métier suppose de créer un groupe sur le domaine, de donner les autorisations à ce groupe et de mettre les utilisateurs dans ce groupe pour les leur donner, de les enlever du groupe pour les leur ôter.

Question 2 :

1. Sauvegarder un système en cours d'exécution peut poser des problèmes. Citer les plus courants. Quelles sont les solutions classiques permettant d'effectuer de telles sauvegardes en toute sécurité ?
2. Quelle différence y a-t-il entre des sauvegardes incrémentales et des sauvegardes différentielles ? Vous pourrez illustrer votre propos sur deux exemples de régime de sauvegarde
3. Certains codes d'acquittement d'un serveur smtp décrits dans la RFC 2821 sont de la forme 2XY, 4XY et 5XY. Indiquez la différence entre ces trois types de codes.
4. serveur de catalogue global dans une forêt windows 2000: quel rôle ? Peut-il y en avoir plusieurs dans la forêt ?
5. Sous windows 2000, on dit que les permissions sont cumulatives. Expliquez ce que l'on entend par ce terme et donnez l'algorithme permettant de déterminer si un utilisateur a la permission d'accéder à un objet.

Elements de correction:

- Q1 deux problèmes classiques:
  - accès impossible à des fichiers verrouillés par certaines applications

    - la sauvegarde prenant du temps, si une application maintient une cohérence entre plusieurs fichiers, cette cohérence peut ne pas être maintenue s'ils sont modifiés lors de la sauvegarde : l'un des fichiers pourrait avoir sa première version sauvée tandis qu'une autre aura sa version après modification de sauvée s'il est traité plus tard par la sauvegarde (cf cours).
    - les solutions classiques:
        - arrêter le système et les applications concernées
        - avoir un logiciel de sauvegarde adapté aux applications à sauver
        - créer un instantané (snapshot) de la partition à sauvegarder avant de faire la sauvegarde.
- Q2:une sauvegarde incrémentale sauvegarde tout ce qui a changé par rapport à la sauvegarde précédente. Une sauvegarde différentielle sauvegarde tout ce qui a changé depuis une sauvegarde de référence qui n'est pas forcément la précédente. Cela a deux conséquences : sur le volume à sauvegarder qui est plus faible pour la sauvegarde incrémentale et sur le nombre de sauvegardes à restaurer qui est plus élevé avec une sauvegarde incrémentale.
- Q3: 2XY: acquittement positif; 4XY: acquittement négatif temporaire; 5XY: acquittement négatif définitif.
- Q4: le catalogue global est une base de données hébergée par un ou plusieurs contrôleurs de domaine. Par défaut, le premier contrôleur de la forêt est serveur de catalogue global. Le catalogue globale contient les appartenance aux groupes universels ce qui le rend indispensable à l'ouverture de session des utilisateurs. Il contient aussi la localisation des objets de la forêt ce qui permet d'optimiser le traitement des requêtes dans la forêt.
- Q5: les droits d'accès d'un utilisateur sont l'union des droits d'accès des groupes auxquels il appartient et des seins propres. ex.: si le groupe G1 a un accès en écriture, si etu1 a un accès en lecture et s'il appartient à G1 alors étu1 a un accès en lecture et en écriture. L'algorithme est le suivant
    - si l'utilisateur ou l'un des groupes auxquel il appartient a un refus d'accès alors l'accès est refusé
    - si l'utilisateur ou l'un des groupes auxquel il appartient a une autorisation d'accès alors l'accès est autorisé
    - sinon l'accès est refusé

Question 3 : groupes et unités d'organisation

Qu'est-ce qu'un unité d'organisation ? A quoi cela peut-il être utilisé ? Quelle différence entre groupes et unités d'organisation ?

Elements de correction:

un groupe contient des utilisateurs et d'autres groupes. On les utilise dans la définition des permissions et droits d'accès comme par exemple tout ce qui est ACL NTFS.

Une unité d'organisation est un conteneur active directory. On peut le lien à des stratégies de groupes et faire de la délégation de contrôle sur les objets qu'elle contient.
On peut déléguer le contrôle sur une unité à un groupe ou à un utilisateur. Le contraire n'a pas de sens : on ne délégue pas de contrôle sur un groupe, on ne délégue pas de contrôle à une unité.

Question 4 :

Scénario : Dans un domaine windows 2000, parmis vos utilisateur, on trouve notamment des enseignants (ens1, ens2, …) et des étudiants (etu1, etu2, etu3, …). On souhaite imposer les choses suivantes :

- Un étudiant est autorisé à réinitialiser les mots de passe des autres étudiants
- Les étudiants ne peuvent pas changer leur mot de passe
- Aucun étudiant et aucun enseignant n'a de commande « exécuter » dans son menu « Démarrer »

Vous expliquerez les modalités de mise en place de cette politique (création de container, lesquels ?, pourquoi ? mise en place des limitations, …).

Elements de correction:

- créer une unité ueve dans le domaine
- créer dedans une unité ens et une unité étu
- mettre les comptes des enseignant dans ens et les comptes des étudiants dans eut
- créer un groupe chmdp dans le domaine et y mettre etu1
- déléguer le contrôle sur l'UO etu au groupe chmdp
- lier une stratégie de groupe (GPO) interdisant le changement de mot de passe à l'unité étu. Une solution alternative moins souple consiste à interdire le changement de mot de passe dans les propriétés des comptes étudiants
- lier à l'UO ueve, une stratégie de groupe interdisant l'item « exécuter »

Administration système: examen sur machine (durée 0h30)

Architecture :

Notre configuration de travail sera constituée de 4 ordinateurs:

- un ordinateur windows 2000 pro appelé **station1** situé sur le réseau R1 : 192.168.100.0/24
- un ordinateur windows 2000 pro appelé **station2** situé sur le réseau R3 : 192.168.150.0/24
- un ordinateur windows 2000 serveur appelé **cd1** situé sur le réseau R1 et d'adresse IP 192.168.100.10. **cd1** est contrôleur du domaine test.shayol.org et serveur dns.
- un ordinateur windows 2000 serveur appellé **passerelle1** ayant deux cartes réseau, une sur chaque réseau R1 et R2 (192.168.200.0/24) faisant office de passerelle.
- un ordinateur windows 2000 serveur appellé **passerelle2** ayant deux cartes réseau, une sur chaque réseau R2 (192.168.200.0/24) et R3 (192.168.150.0/24)faisant office de passerelle.

Du point de vue de vmware, R1 sera sur le commutateur virtue VMNET 5, R2 sera sur le commutateur virtuel VMNET6 et R3 sur VMNET7.

Exercice 1configuration IP

Faites en sorte

- qu'il soit possible de faire des « ping » entre l'ensemble de vos ordinateurs.
- que tous les ordinateurs aient des entrées correctes dans le dns

Elements de correction:

ping:

- chaque machine doit se voir affecter une adresse ip correcte, cd1 comme serveur dns. station1 et cd1 ont l'ip sur R1 de passerelle1 comme routeur par défaut. passerelle1 a l'ip de passerelle1 sur R2 comme routeur par défaut. passserelle1 a l'ip de passerelle2 sur R2 comme routeur par défaut. station2 a l'ip de passerelle2 sur R3 comme routeur par défaut.
- le routage est activé sur passerelle1 et sur passerelle2

dns:

- il faut créer une zone inverse pour R2 et pour R3 sur cd1
- il faut ajouter une entrée directe et inverse pour tous les ordinateurs qui n'en ont pas.

exercice 2 domaine test.shayol.org

Vous intégrerez **station1** et **station2** au domaine test.shayol.org

On vous demande de faire en sorte que **passerelle1** devienne un second contrôleur pour le domaine test.shayol.org.

Elements de correction:

par ordre de difficulté:

- ajouter station1 suppose simplement de lui avoir défini une adresse ip correcte (sur R1) et cd1 comme serveur dns. Rappel: les ordinateurs windows 2000 utilisent le dns pour repérer leur contrôleur de domaine.L'ajout au domaine se fait alors sans problème.

- faire que passerelle1 devienne controleur de domaine a les mêmes prérequis : ip correcte et cd1 comme serveur dns. On utilise ensuite dcpromo pour ajouter un nouveau contrôleur de domaine au domaine
- ajouter station2 suppose que la connectivité IP fonctionne et que station2 aie bien cd1 comme serveur dns.

exercice 3

Sur **station1**, créez les utilisateurs locaux test1, test2 et test3 ayant respectivement comme mot de passe passtest1, passtest2 et passtest3.
Ouvrez une session en tant que test1 et créez un répertoire **RepTest1** à la racine de C :. Dans Ce répertoire, créer deux répertoires **RepTest2** et **RepTest3**.
On vous demande d'obtenir l'état suivant :

- Test1 n'a que le droit lecture/exécution/affichage sur RepTest1 et Reptest3. Il n'a aucun droit sur Reptest2. Il ne peut se redonner des droits plus élevés.
- Test2 est CT sur tous les répertoires.
- Test3 a le droit lecture/exécution/affichage/écriture/modification sur RepTest1 et RepTest3; il n'a aucun droit sur RepTest2.
- L'administrateur est en CT sur les trois dossiers.

Qu'aurait apporté en plus le droit CT à test3 sur RepTest1 et RepTest3 ?

Elements de correction:

un exercice de base fait 70 fois en TD.

- pour que test1 ne puisse se redonner plus de droits, il faut qu'il ne soit plus propriétaire des dossiers. La solution la plus simple consiste à ouvrir une session en tant qu'administrateur et à s'approprier le dossier.
- une gaffe à éviter: il ne faut pas laisser le groupe « tout le monde » en control total sur les dossiers car les permissions sont cumulatives sous windows.

Exercice 4:

Les ouvertures de session ont-elles lieu sans problème sur **station1** et **station2** si **cd1** est arrêté ? Si oui, expliquez pourquoi et pour quels comptes. Si non, expliquez pour quels comptes et ce qu'il faut faire pour qu'elles aient lieu.

Elements de correction:

Aucun problème pour les comptes utilisateurs locaux.
Pour les comptes utilisateurs du domaine, on peut noter que l'on a un autre contrôleur de domaine mais ça ne suffit et il reste deux problèmes à régler :

- en tant que premier controleur de la forêt, cd1 est serveur de catalogue global. Le catalogue global est consulté lors de l'ouverture de session pour vérifier l'appartenance de l'utilisateur à des groupes universels et créé le jeton d'accès. Si le serveur de catalogue global est inaccessible, l'ouverture de session utilise les données en cache sur le poste de travail. Cela suppose que l'utilisateur y a déjà ouvert une session.

  pour résoudre ce problème, il suffit de déclarer que

passerelle1 est aussi serveur de catalogue global

- le second problème est lié en dns: les ordinateurs windows 2000 utilise le dns pour trouver les contrôleurs de domaine. Sans serveur dns, certains ordinateurs ne trouveront pas l'autre contrôleur de domaine et ne pourront vérifier le mot de passe de l'utilisateur.

  pour palier ça, il suffit d'installer un serveur dns esclave sur passerelle1 (ou tout autre ordinateur) et de l'indiquer comme dns en plus de cd1 dans la conf tcp/ip des postes de travail.