

Examen admin réseau W2K3

Tous documents de cours autorisés
durée 1h00

Nom :	Prénom :

Présentation :

Votre travail consiste à réaliser les tâches suivantes. On vous indique en général simplement ce que l'on souhaite obtenir sans vous imposer de méthodes pour l'obtenir.

Vous utiliserez 3 machines virtuelles vmware :

- **station1**: une machine windows 2000 pro avec une carte réseau sur NAT
- **serveur3**: une machine windows 2000 ou 2003 serveur avec une carte réseau sur NAT
- **serveur4**: une machine windows 2000 ou 2003 serveur avec une carte réseau sur NAT

Vous ferez en sorte que le nom des machines vmware (celui qui apparaît dans l'onglet) soit celui indiqué ci-dessus.

Ces ordinateurs devront avoir les adresses IP suivantes :

- **station1**: 192.168.10.1
- **serveur3**: 192.168.10.3
- **serveur4**: 192.168.10.4

Initialement, les machines n'auront pas de serveur dns configuré.

Les noms des onglets vmware doivent refléter le nom des machines.

Exercice 1: tcp/ip

Configurez tcp/ip sur ces machines de façon à ce qu'elles puissent se « ping » entre elles.

Exercice 2: Gestion des droits d'accès

Question 1: Ce TD est à faire sur **station1**.

Créez les utilisateurs locaux test1, test2 et test3 ayant respectivement comme mot de passe passtest1, passtest2 et passtest3. Créez le groupe local **compta**. test1 et test2 sont membres de compta mais pas test3.

Ouvrez une session en tant que test1 et créez un dossier **RepTest1** à la racine de C:\, un dossier **RepTest2** dans **RepTest1** et un dossier **RepTest3** dans **RepTest1**.

Ouvrez une session en tant qu'administrateur de la station.

On vous demande ensuite d'obtenir l'état suivant :

- Test1 a accès en lecture/lecture-exécution/affichage du contenu sur **RepTest1**, **RepTest2** et **RepTest3**.
- Test2 est CT sur **RepTest1**, **RepTest2** et **RepTest3**.
- Test3 a accès en lecture/lecture-exécution/affichage du contenu sur **RepTest1**, à **RepTest3** mais il n'a pas accès à **RepTest2**.
- Les membres du groupe compta ont accès en lecture, lecture-exécution, écriture et modification à **Reptest1** et **Reptest2**.
- l'administrateur local est en CT sur tous les dossiers.

Question 2: On souhaite que test1 n'ait plus accès à **RepTest1** et qu'il ne puisse se redonner les droits. On ne souhaite pas non plus utiliser d'interdictions. Expliquez par écrit succinctement comment faire (vous listez toutes les actions à faire mais

vous n'expliquez pas comment réaliser chaque action) Appliquez le ensuite sur machine.

Exercice 3: Création du domaine toto.fr

Le respect du nom du domaine est impératif. Si vous utilisez un nom de domaine différent, vous n'aurez aucun des points de la question.

On vous demande de créer le domaine toto.fr qui devra être géré par **serveur3**. **station1** devra être intégrée au domaine.

On suppose que votre parc ne comporte plus aucun contrôleur de domaine windows NT. Il comporte par contre des postes de travail windows 98, windows NT, windows 2000

L'état obtenu :

- **serveur3** gère le domaine toto.fr.
- la station w2k pro **station1** fait partie du domaine
- un utilisateur testAD1 existe sur le domaine
- aucune utilisateur local testAD1 n'existe sur la station de travail **station1**
- testAD1 peut utiliser **station1**

Exercice 4: second contrôleur pour toto.fr

Question 1: (**sur machine**): faites en sorte que **serveur4** soit un nouveau contrôleur de domaine pour le domaine **toto.fr**.

Question 2: (**sur papier**): en cas de panne de serveur3, on souhaite que serveur4 soit à même de permettre les ouvertures de session sur le domaine. Vous expliquerez ce qu'il faut faire pour que ça soit possible en justifiant brièvement vos propositions.

Question 3: (**sur machine**): mettez en place ce que vous avez décrit à la question 2 de façon à ce que **serveur4** puisse gérer le domaine en cas de panne de **serveur3**.

Exercice 5: profil itinérant

Faites en sorte que testAD1 ait un profil itinérant. Vous expliquerez sur papier votre démarche (les grandes étapes et l'endroit où aller vérifier ce que vous avez fait). Puis vous l'appliquerez sur machine.

Partie sur papier: durée 1h00, sans documents

Partie Unix

Question 1 : généralités

Q1-1: comment s'appelle l'outil traditionnel de planification de tâche sous unix ?

Q2-1: qu'est-ce que syslog ?

Q3-2: quelle commande tapez-vous pour afficher la table de routage d'une machine unix ?

Q4-2: quelle commande tapez-vous pour afficher les systèmes de fichiers montés ?

Q5-2: est-ce vraiment le mot de passe que l'on trouve dans le fichier /etc/passwd ou /etc/shadow ?

Q6-1: après avoir donné la signification de l'acronyme PAM, vous expliquerez le rôle de ce mécanisme ?

Q7-1: à quoi sert NSS (géré par le fichier /etc/nsswitch.conf)

Question 8 : nis et nfs

1. expliquez quels services rendent nfs et nis
2. on dit parfois que nis est un complément naturel à nfs. expliquez pourquoi.

Question 9 : ssh

1. expliquez ce qu'apporte ssh en matière de sécurité
2. un utilisateur toto souhaite se connecter depuis une machine nommée station1 sur une machine nommée station2 via ssh sans avoir à taper de mot de passe.
 - Expliquer sur quoi s'appuie alors l'authentification
 - indiquez ce que l'utilisateur doit faire en pratique pour que ça soit possible (fichier à créer, modifier, ...)
 - d'un point de vue sécurité, que pensez-vous de cette façon de procéder ? Sachant qu'il utilise cette connexion pour lancer une application fixe (mathematica) à distance depuis station1. Citez des améliorations possibles de la sécurité sans revenir à une authentification par mot de passe.
- Expliquez ce qu'est un tunnel ssh et décrivez de façon détaillée une utilisation concrète possible d'un tel tunnel.

Partie windows

Question 10 :

1. Qu'est-ce qu'un profil itinérant ? expliquez en le fonctionnement. quelle différence avec un simple partage ou un dossier de base ?
- 2.

Question 11 : groupes et unités d'organisation

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

Question 12 : tolérance de panne

1. un domaine windows peut être géré par plusieurs contrôleurs de domaine windows. Expliquez l'intérêt d'une telle possibilité
2. un domaine windows est géré par 2 contrôleurs de domaine windows. L'un des contrôleurs est débranché du réseau. Le second contrôleur peut-il prendre le relais :
 - o pour l'ouverture des sessions ?
 - o pour la création de comptes
 - o pour l'intégration de nouveaux postes dans le domaine ?
 - o ...

La majeure partie des points portent sur les explications accompagnant la réponse.