

Auteur: P. Petit	Titre: TD Administration Active Directory niv. 2	Version: 1.3
Date: 05/12/2006	Licence: Gnu Free Documentation Licence	Durée: 1h00

Administration d'Active Directory

Objectifs

- Tolérance de panne
- création d'une arborescence
- audit

Configuration initiale

Ce TD est à réaliser avec une station de travail windows Xp pro et trois serveur windows 2003 server. Il peut probablement aussi être réalisé avec une station w2k pro et deux serveur w2k server. La station de travail sera appelée **station1**. Les serveurs seront appelés **serveur2**, **serveur3** et **serveur4**. **serveur2** sera contrôleur de domaine/serveur dns du domaine shayol.org. La station sera dans le domaine shayol.org.

D'un point de vue IP, ces machines seront sur le sous-réseau 192.168.10.0/24 sur vmnet3. Le dernier octet de l'adresse ip des machines sera leur numero. Pour gagner en performances sous vmware, **Serveur3** ne sera démarré qu'à l'exercice 3.

Prérequis

- Gestion des utilisateurs dans un domaine
- planification dans un domaine : unités d'organisation, forêt, arborescences
- planification des groupes

Exercice 1: Ajout d'un contrôleur de domaine à un domaine

On souhaite améliorer la tolérance de panne du domaine. Créez un utilisateur test4 sur le domaine et n'ouvrez pour l'instant aucune session sur **station1** avec. Ouvrez par contre une session **station1** avec test3. Dans vmware, déconnectez la prise réseau de **serveur2**. Tentez ensuite d'ouvrir une session sur **station1** en tant que test3 puis en tant que test4. Que remarquez-vous ? Expliquez.

Pour éviter ces problèmes, on décide d'installer un second contrôleur de domaine pour le domaine shayol.org. Utilisez **serveur4** pour cela. N'oubliez pas de reconnecter la carte réseau de **serveur2** avant.

Une fois le nouveau contrôleur de domaine installé, trouvez l'outil permettant de voir les deux contrôleurs et de lancer manuellement une réplication des données de ces contrôleurs de l'un sur l'autre. Ces répliquions doivent se faire automatiquement. Pour le tester, créez un utilisateur test5 sur le domaine depuis l'un des contrôleur et vérifiez qu'il est aussi visible sur l'autre contrôleur.

Nous allons maintenant tester la tolérance de panne : déconnectez la carte réseau vmware de **serveur2**. Tentez ensuite d'ouvrir des sessions sur **station1** en tant que test3, test4 et test5¹. Que constatez-vous ?

Le catalogue global est une structure de données qui permet aux machines du domaine de déterminer de façon efficace à quels groupes appartient un utilisateur. Son intérêt n'apparaît que dans une structure multidomaines car il évite d'interroger tous les domaines de la forêt. Il est aussi utilisé dans un domaine. Une station de travail qui ne peut contacter son serveur de catalogue global

¹ On suppose que vous n'avez jamais ouvert de session sur **station1** en tant que test5. Si vous l'avez fait, créez un utilisateur test6.

Auteur: P. Petit	Titre: TD Administration Active Directory niv. 2	Version: 1.3
Date: 05/12/2006	Licence: Gnu Free Documentation Licence	Durée: 1h00

ne peut déterminer les groupes auxquels appartient un utilisateur; Elle ne peut ouvrir de session qu'aux utilisateurs pour lesquels elle l'a déjà fait pas le passé grâce à un cache local mais pas aux utilisateurs qu'elle authentifie pour la première fois.

Reconnectez **serveur2**, faites en sorte que **serveur4** soit aussi serveur de catalogue global. Faites ensuite le test de tolérance de panne (créez un utilisateur test6, déconnectez la carte réseau de **serveur2** et testez l'ouverture de session sur **station1** en tant que test3, et test6).

Pour des questions de performances vmware, arrêtez **serveur4** pour faire la suite du TP.

Exercice 2: création d'un sous domaine

1. On souhaite créer un sous domaine nommé test.shayol.org. Vis à vis de shayol.org: appartiendra-t-il à la même arborescence ? à la même forêt ? Qu'en aurait-il été si le domaine s'était appelé norstralie.fr ?
2. D'un point de vue dns, la création du sous-domaine test.shayol.org impose-t-elle d'installer un serveur dns sur son contrôleur de domaine ?
3. **serveur2** peut-il être contrôleur de domaine de test.shayol.org ?
4. Intégrer **serveur3** au domaine shayol.org puis créer le sous-domaine test.shayol.org de façon à ce que **serveur3** en soit contrôleur de domaine.
5. modifiez la stratégie de sécurité du contrôleur de domaine de façon à ce que tous les utilisateurs authentifiés puissent ouvrir des sessions sur **serveur3**.
6. test1, test2 et test3 peuvent-ils ouvrir des sessions sur **serveur3** ?

Exercice 3: gestion des groupes

On souhaite que l'utilisateur test1 du domaine shayol.org soient administrateur du domaine test.shayol.org. Comment faire ? Appliquez le.

On souhaite remplacer test1 par test2 et test3. Comment faire ? appliquez le.