

Active Directory et DNS

1- Introduction et préparation

Partez du principe qu'il s'agit d'installer un contrôleur de domaine pour une entreprise qui n'en possédait pas auparavant.

A la fin de chaque partie, faites valider votre travail par le formateur.

Votre numéro de serveur est : X =

1. Adresse IP du client : **DHCP**
2. Adresse IP du serveur : 192.168.2.20X
3. Nom du serveur : serveurX
4. Nom du domaine AD : bookticX.lan

1. Supprimez tous les rôles installés sur votre Windows Server à l'exception du rôle Hyper-V.
2. Supprimez tous les partages

2- Questions sur Active Directory

1. Quelles sont les paramètres à modifier avant l'installation d'un contrôleur de domaine Active Directory ?
2. Quels protocoles peuvent gérer les noms de machines dans un domaine Windows ? Parmi ces protocoles lesquels sont obligatoires/facultatifs ?
3. Les comptes présents dans Windows avant l'installation d'Active Directory sont-ils copiés dans l'annuaire ?
4. Expliquez la composition d'un chemin UNC et comparez-la à celle d'un chemin URL.
5. Expliquez le principe de fonctionnement des GPO (stratégies de groupe).

3- Pratique sur Active Directory

- Créer un contrôleur de domaine pour le domaine **bookticX.lan** (le X sera donné par le formateur).
- Tous les mots de passe seront **Azerty77**
- Créer un utilisateur nommé **admin** appartenant au mêmes groupes que l'administrateur.
- Désactivez le compte de l'administrateur.
- Permettre à **admin** la prise en main à distance de votre serveur.
- Créer une première stratégie de groupe s'appliquant à tout le domaine pour permettre les mots de passe simples (minimum 5 caractères, pas de complexité).
- Créer les trois unités d'organisation suivantes : **Développement ; Réseau ; Système**.
- Dans l'unité d'organisation Développement, créer le **groupe Développeurs** et les **utilisateurs J. Ava et P. Ython** qui doivent être membres de ce groupe.
- Dans l'unité d'organisation Réseau, créer le **groupe Netadmins** et les utilisateurs **C. Isco et J. Uniper** qui doivent être membres de ce groupe.
- Dans l'unité d'organisation Système, créer le **groupe Sysadmins** et les utilisateurs **G. Nu et L. Inux** qui doivent être membres de ce groupe.

Trouvez une méthode permettant de prouver que les comptes utilisateurs sont opérationnels.

4- Profils et GPO

- Les sysadmins ne doivent pouvoir se connecter qu'**entre 8h et 20h**.
- Pour les sysadmins, interdire l'accès au menu exécuter dans le menu démarrer
- Pour les sysadmins, Interdire l'accès au panneau de configuration
- Pour les questions suivantes, vous définirez les partages et les droits NTFS nécessaires
- Les netadmins doivent utiliser des **profils itinérants** (stockés sur le serveur dans c:\share\profils\nomdelutilisateur)
- Tous les utilisateurs doivent avoir :
 - un **lecteur réseau personnel** P: (stocké sur le serveur dans c:\share\p\nomdelutilisateur)
 - un **lecteur de groupe** Q: (stocké sur le serveur dans c:\share\q\nomdugroupe)
 - un **lecteur réseau commun** à toute l'entreprise R: (stocké sur le serveur dans c:\share\commun)
- Déployer le **logiciel MBSA** automatiquement sur tous les postes clients.

Trouvez une méthode permettant de prouver que toutes vos GPO ont fonctionné.

5- Questions sur DNS

1. Qu'est-ce que le cache DNS ? Où le trouve-t-on ?
2. Qu'est-ce qu'une racine DNS ? Un serveur principal peut-il fonctionner sans indications de racines ?
3. Qu'est-ce qu'un redirecteur DNS ? Un serveur principal peut-il fonctionner sans indications de redirecteurs ?
4. Qu'est-ce qu'un transfert de zone ? Pourquoi est-ce risqué en terme de sécurité ?

6- Pratique sur DNS

Créer un nouveau domaine DNS nommé greta77.lan
Associer les noms suivants aux adresses IP correspondantes :

- serveur hôte pour votre IP
- ad alias de serveur
- ns1 alias de serveur
- monitoring alias de serveur
- inventaire alias de serveur
- routeur hôte pour votre passerelle
- imprimante hôte pour 192.168.2.150
- serveur serveur de mail pour le domaine greta77.lan

Trouvez une méthode permettant de prouver que votre zone greta77.lan est opérationnelle.

Créez un serveur DNS secondaire pour le domaine greta77.lan hébergé sur le serveur 192.168.2.2

Trouvez une méthode permettant de prouver que votre serveur DNS secondaire est opérationnel.