TP3 : Réseau Client-Serveur

Objectifs du TP

- Comprendre et configurer un réseau client-serveur dans un environnement Windows.
- Joindre un ordinateur à un domaine et utiliser des comptes utilisateurs de domaine.
- Accéder aux ressources partagées sur un serveur.
- Tester les privilèges des comptes utilisateurs.
- Utiliser et configurer la connexion au bureau à distance.

Tutoriel pour la Mise en Place de l'Environnement Réseau Client-Serveur

1. Préparation des Machines Virtuelles

1. **Créer des Machines Virtuelles :**
   - Utilisez un hyperviseur comme VMware, VirtualBox, ou Hyper-V pour créer deux machines virtuelles :
     - **Client** : Windows 10
     - **Serveur** : Windows Server (2016, 2019, ou 2022)
2. **Installer les Systèmes d'Exploitation :**
   - Suivez les instructions de l'installateur pour chaque système d'exploitation.

2. Configuration du Réseau

1. **Configurer les Adresses IP :**
   - **Serveur :**
     - IP : 192.168.55.2XY (où X est le numéro de votre baie et Y le numéro de votre PC)
     -
     - Masque de sous-réseau : 255.255.255.0 (/24)
   - **Client :**
     - IP : 192.168.55.XY (où X est le numéro de votre baie et Y le numéro de votre PC)
     - Masque de sous-réseau : 255.255.255.0 (/24)

   Questions :

   - Pourquoi est-il important que le client et le serveur soient sur le même sous-réseau ?

     Lorsque le client et le serveur sont sur le même subnet, ils peuvent communiquer directement sans passer par un router, ce qui réduit la latence, simplifie la configuration, optimise les performances et évite les complications liées au routage ou aux filtres de sécurité.

2. **Configurer les Paramètres Réseau :**
   - **Windows 10 :**

- Ouvrez les Paramètres → Réseau et Internet → Modifier les options de l'adaptateur.
- Faites un clic droit sur votre connexion réseau → Propriétés.
- Sélectionnez Protocole Internet Version 4 (TCP/IPv4) → Propriétés.
- Entrez les paramètres IP.

- **Windows Server :**
  - Ouvrez le Gestionnaire de serveur → Local Server.
  - Cliquez sur l'adresse IP pour configurer les paramètres réseau.
- **Pour information la commande PowerShell :**

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.55.XY -PrefixLength 24 -DefaultGateway 192.168.55.1
```

3 **Tester la Connectivité Réseau :**

- **Commande de Test de Configuration :**
  - Utilisez `ipconfig` pour vérifier les paramètres IP.
- **Commande de Test de Connectivité :**
  - Utilisez `ping 192.168.55.250` pour tester la connexion entre le client et le serveur.

Questions :

Quelles autres commandes peuvent être utilisées pour diagnostiquer les problèmes de réseau ?

En plus de ipconfig et ping, on peut utiliser des commandes comme :

- tracert pour tracer le chemin des paquets,

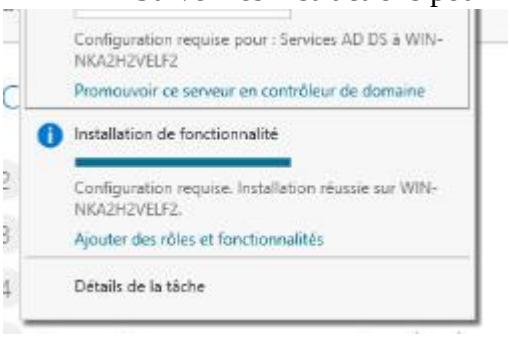
- nslookup pour vérifier la résolution DNS,

- netstat pour examiner les connexions actives.

D'autres outils comme arp, telnet, et route permettent d'approfondir l'analyse en vérifiant la configuration des routes et la communication au niveau des ports.

3. Configuration du Serveur Active Directory

1 **Installer Active Directory :**
   - Sur le serveur :
     - Ouvrez le Gestionnaire de serveur → Ajouter des rôles et fonctionnalités.
     - Sélectionnez Rôle basé ou installation de fonctionnalités → Serveur Active Directory.
     - Suivez les instructions pour installer les rôles nécessaires.



2 **Promouvoir le Serveur en Contrôleur de Domaine :**
   - Après l'installation, dans le Gestionnaire de serveur, cliquez sur Promouvoir ce serveur en contrôleur de domaine.
   - Sélectionnez Ajouter une nouvelle forêt et entrez un nom de domaine, par exemple, **VotreNom.local**.
   - Suivez les instructions pour configurer le domaine, définir le mot de passe DSRM, et redémarrez le serveur.

AD

Points de Sécurité :

   - Assurez-vous que le mot de passe DSRM est fort et conforme aux politiques de sécurité de votre organisation.

3 **Active Directory :**
   - Qu'est-ce qu'un domaine dans Active Directory ?

Un domaine dans Active Directory est un regroupement logique d'objets (utilisateurs, ordinateurs, groupes) partageant une même base de données et des règles de sécurité centralisées. Il permet la gestion des ressources et des permissions au sein d'un réseau.

   - Quelles informations peut-on trouver dans Active Directory ?

Dans AD, on peut trouver des informations sur les utilisateurs, groupes, ordinateurs, imprimantes et autres objets réseau, ainsi que leurs attributs, comme les noms, mots de passe, adresses, et permissions associées.

   - Qu'est-ce qu'un utilisateur dans Active Directory et quelles sont ses principales propriétés ?

Un utilisateur dans Active Directory est un objet représentant une personne ou un compte de service avec des droits d'accès au réseau. Ses principales propriétés incluent le nom d'utilisateur, mot de passe, adresse e-mail, appartenance à des groupes, et autorisations d'accès aux ressources.

- Que signifie "authentification" et comment cela fonctionne-t-il dans AD ?

L'authentification est le processus de vérification de l'identité d'un utilisateur. Dans Active Directory, elle fonctionne via des protocoles comme NTLM, où l'utilisateur fournit ses identifiants pour accéder aux ressources du réseau en prouvant son identité.

- Comment Active Directory aide-t-il à gérer les mots de passe des utilisateurs ?

AD gère les mots de passe des utilisateurs en appliquant des politiques de sécurité, comme la complexité, la durée de validité, et le verrouillage après plusieurs échecs. Ca permet aussi aux administrateurs de définir des règles spécifiques et de forcer la réinitialisation des mots de passe si nécessaire.

- Qu'est-ce qu'un groupe dans Active Directory et pourquoi est-il important ?

Un groupe dans AD est un ensemble d'utilisateurs , ordinateurs ou autres objets, permettant de simplifier la gestion des autorisations. Il est important car il facilite l'attribution de droits d'accès aux ressources, en appliquant des permissions à plusieurs objets à la fois.

- Quels sont les rôles des unités organisationnelles (OU) dans Active Directory ?Les unités organisationnelles (OU)permettent de regrouper et d'organiser les objets comme les utilisateurs, groupes, et ordinateurs de manière hiérarchique. Elles facilitent la gestion des permissions, l'application de stratégies de group et la délégation de tâches administratives spécifiques.

4. Configuration du Client pour Joindre le Domaine

1. **Créer un Nouveau Utilisateur sur AD :**
   - Utilisez le Gestionnaire d'Active Directory pour créer un utilisateur avec les droits nécessaires.
2. **Joindre le Domaine :**
   - Sur le client Windows 10 :
     - Ouvrez Paramètres → Système → Informations système.
     - Cliquez sur Modifier les paramètres → Modifier dans la section Nom de l'ordinateur, domaine et groupe de travail.
     - Sélectionnez Domaine et entrez **VotreNom.local**.
     - Entrez les informations d'identification d'un utilisateur ayant les droits pour ajouter des ordinateurs au domaine.

Questions :

- Quel rôle jouent les informations d'identification lors de la connexion au domaine ?

Les informations d'identification, comme le nom d'utilisateur et le mot de passe, sont essentielles pour vérifier l'identité de l'utilisateur lors de la connexion au domaine. Elles permettent à Active Directory de valider l'accès et d'accorder les permissions appropriées aux ressources réseau.

- Quels privilèges sont requis pour ajouter un ordinateur au domaine ?

  Pour ajouter un ordinateur au domaine, un utilisateur doit disposer des privilèges d'administrateur ou d'un rôle spécifique dans AD ; Cela permet de garantir que seules les personnes autorisées peuvent effectuer cette action, assurant ainsi la sécurité du réseau.

3. **Redémarrer le Client :**
   - Redémarrez l'ordinateur pour appliquer les changements.

5. Configuration des Ressources Partagées sur le Serveur

1. **Créer et Partager un Dossier :**
   - Sur le serveur :
     - Créez un dossier, par exemple **C:\Partage**.
     - Faites un clic droit sur le dossier → Propriétés → Partage → Partager.
     - Sélectionnez "Tout le monde" pour un partage ouvert, ou un groupe spécifique selon vos besoins.
     - Configurez les permissions (Lecture/Écriture) selon les besoins.

   Points de Sécurité :

   - Évitez de partager des dossiers avec "Tout le monde" si ce n'est pas nécessaire. Privilégiez des groupes spécifiques pour un meilleur contrôle d'accès.
2. **Configurer les Paramètres de Partage Avancés :**
   - Dans la section Partage avancé du dossier :
     - Activez le partage du dossier et définissez des permissions supplémentaires si nécessaire.
     -

6. Accès aux Ressources Partagées

1. **Accéder au Dossier Partagé :**
   - Sur le client Windows 10 :
     - Ouvrez Explorateur de fichiers.
     - Tapez `\\192.168.55.2XY` dans la barre d'adresse et appuyez sur Entrée.
     - Vous devriez voir le dossier partagé **Partage**.

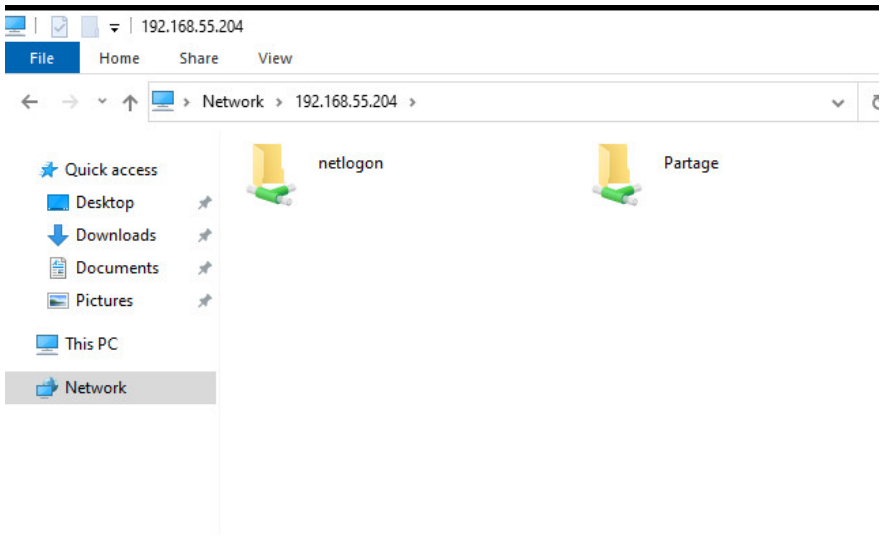
   Questions :

   - Comment la sécurité est-elle gérée lors de l'accès à un dossier partagé ?

La sécurité lors de l'accès à un dossier partagé est gérée via des permissions basées sur les utilisateurs et groupes dans Active Directory. Les administrateurs définissent des autorisations spécifiques (lecture, écriture, modification) pour contrôler l'accès aux dossiers, assurant ainsi que seuls les utilisateurs autorisés peuvent accéder ou modifier les fichiers.

- Que se passe-t-il si les permissions ne sont pas correctement configurées ?

  Si les permissions ne sont pas correctement configurées, cela peut entraîner des accès non autorisés à des ressources sensibles ou, à l'inverse, empêcher des utilisateurs légitimes d'accéder aux fichiers et dossiers nécessaires à leur travail. Cela crée donc des vulnérabilités de sécurité et des interruptions de service pouvant affecter la productivité.



7. Gestion des Utilisateurs et Mots de Passe

1 Modifier le Mot de Passe :

- **Via PowerShell :**

```
$username = "prenom.nom"
$newPassword = "NouveauMotDePasse!"
$securePassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Set-LocalUser -Name $username -Password $securePassword
```

2 Modifier le Mot de Passe via l'Invite de Commande :

- Ouvrez Invite de Commande en tant qu'administrateur.
- Utilisez la commande suivante :

```
net user prénom.nom NouveauMotDePasse! /domain
```

3 Points de Sécurité :

- Assurez-vous que les mots de passe respectent les politiques de complexité de l'organisation.

8. Configuration du Bureau à Distance

1 **Activer le Bureau à Distance :**
   - Sur le serveur ou le client Windows 10 :
     - Ouvrez Paramètres → Système → Bureau à distance.
     - Activez "Activer le Bureau à distance".

Points de Sécurité :

- Vérifiez que seules les personnes autorisées peuvent accéder à distance. Limitez l'accès en configurant les utilisateurs autorisés dans les paramètres de Bureau à distance.

2 **Se Connecter au Bureau à Distance :**
   - Depuis le client ou une autre machine :
     - Ouvrez Connexion Bureau à distance (Tapez `mstsc` dans le menu Démarrer).
     - Entrez l'adresse IP du serveur et cliquez sur Connecter.
     - Entrez vos informations d'identification pour vous connecter.

Questions :

- Quels sont les principaux avantages d'utiliser la connexion Bureau à distance dans un environnement professionnel ?

Les avantages de la connexion Bureau à distance incluent l'accès à distance aux ressources, la centralisation des applications, et une meilleure flexibilité pour les employés, facilitant ainsi le télétravail et réduisant les coûts de maintenance.

- Quels sont les risques associés à l'utilisation de la connexion Bureau à distance, et comment peut-on les atténuer ?

Les risques associés à l'utilisation de la connexion Bureau à distance incluent les attaques par force brute, les accès non autorisés et les fuites de données. Pour les atténuer, il est recommandé d'utiliser des mots de passe forts, d'activer l'authentification à deux facteurs, et de restreindre les adresses IP autorisées à se connecter.

Réflexion sur la Sécurité :

- La connexion Bureau à distance offre une flexibilité et un accès facile aux ressources d'une machine distante, ce qui est particulièrement utile pour le télétravail et l'assistance technique. Cependant, elle expose également les systèmes à des menaces de sécurité. Il est crucial de mettre en œuvre des mesures de sécurité, telles que l'utilisation de mots de passe forts, l'activation de l'authentification à deux facteurs, et la limitation des accès à des adresses IP spécifiques pour protéger les machines contre les accès non autorisés.

9. Vérification et Validation

1. **Tester la Connexion au Domaine :**
   - Connectez-vous au client avec votre compte de domaine.
   - Vérifiez l'accès aux ressources partagées sur le serveur.
2. **Tester les Partages :**
   - Assurez-vous que vous pouvez accéder aux dossiers partagés depuis le client et que les permissions sont correctement appliquées.
3. **Tester le Bureau à Distance :**
   - Assurez-vous que vous pouvez accéder à la machine distante via le Bureau à distance.

Conclusion

Ce TP vous permet de configurer un réseau client-serveur avec Active Directory, vous familiarisant avec les concepts essentiels et les compétences pratiques nécessaires pour gérer un environnement Windows. En intégrant des questions théoriques et des points de sécurité, ce TP vous aide à développer une compréhension plus approfondie des enjeux liés à la sécurité dans un environnement réseau.

N'oubliez pas de documenter vos étapes pour alimenter votre portfolio !