

Exercice 1 : Comparaison matériel Server PC (**PAS A L'EXAMEN**)

Exercice 2 : Mise en place d'une infrastructure virtuelle

- Adresse IP dans même segment
- Désactiver Pare-feu
- Ping OK

Exercice 3 : Installation et configuration d'un service DHCP

- Option DHCP d'étendue différence option serveur
 - o Option étendu c'est spécifique à cette étendue
 - o Option serveur c'est pour toutes les étendues
- Renouvellement du bail de DHCP après moitié du temps puis après 87.5% de ce temps
- Ipconfig /release permet de désaffecter l'adresse IP actuelle
- Ipconfig /renew permet de demander une nouvelle adresse IP au premier server DHCP disponible
- Si pas DHCP Dispo alors APIPA de type 169.254.XXX.XXX /16 Classe B
- 4 pc distant pas de serveur DHCP un agent Relay fait le Relay vers l'entreprise où se trouve server DHCP

Exercice 4 : Installation et configuration d'un service DNS

- Mode dynamique permet au client de s'enregistrer tout seul auprès du DNS
-

Types d'enregistrement DNS :

- **NS** (Name Server) : Utilisé pour transferts de zone ainsi que délégations de zones
 - **A** (Hôte) : Mapper le nom d'hôte d'une machine à une adresse IP
 - **PTR** (Pointeur) : L'inverse d'un enregistrement A c'est-à-dire, Mapper une adresse IP à un nom FQDN
 - **SOA** (Start of Authority) : c'est le premier enregistrement créé à la création d'une zone, il indique quel server est server principal, gérer le mécanisme de transfert de zone.
-

- Option 006 [Serveur DNS] = fournir adresse IP du Server DNS au client DHCP
- Vérifier que DNS est actif sur client = NSLookup
- Un serveur DNS secondaire est une copie en lecture seulement.
- 2 serveurs DNS soient Lecture/écriture il suffit de configurer les zones des deux serveurs DNS en type intégré AD
- Pour avoir un autre nom sur la machine (atteindre www.rienafouttre.ch) on utilise un alias (Cname).
- Réplication immédiate de la zone sur les serveurs DNS
- Si server DNS 1 est down le server 2 DNS tente un nouvel essai de transfert de zone après 10 minutes par défaut.

- Ipconfig /RegisterDNS permet de forcer le réenregistrement du nom d'hôte et de l'IP du client auprès du server DNS

Exercice 5 : Installation et configuration Active Directory (AD)

- Installer un AD : Nouvelle forêt, nouveau domaine, Domaine AD de type : Zyrtech.local, une partition S : pour NTDS et SYSVOL
 - DHCP se désactive quand on met AD en place il faut le réactiver
-

Les 5 rôles FSMO :

- **Maitre des noms de schéma** : Unique dans la forêt garantie la définition de la base de donnée (schéma)
 - **Maitre des noms de domaine** : Unique dans la forêt gère le nom de domaine de la forêt et garanti l'unicité
 - **Maitre d'infrastructure** : Unique dans un domaine garantie la cohésion des noms et des appartenances des objets AD
 - **Gestionnaire du pool RID** : Unique par domaine distribue des tranches de RID au Contrôleur de domaine pour qu'il puisse créer ses SID unique
 - **Contrôleur de domaine principale** : Unique par domaine émule un Contrôleur de domaine principal pour les clients NT 4.0.
-
- Toujours allumer le server avant de se connecter avant le client.
 - Pas d'autorisation équivalente au DHCP
 - Pas de maximum de contrôleurs de domaine
 - 2 contrôleurs de domaine : Redondance et performance
 - LDAP = Accès à l'annuaire
 - Kerberos = Sécurité d'authentification

Exercice 6 : Gestion des consoles d'administration

- Console mmc fonctionne avec des logiciels enfichables
- Afin de rendre la console mmc active il faut la poser sur la machine client et se loguer sur la machine client en administrateur de la station de travail (pas en admin du domaine).
- Installer outils AD DS et AD LDS
- Console pour utilisateur (ex :Fred), créer une nouvelle console, ajouter un composant enfichable (ex : utilisateur et ordi de l'AD), dans Menu cliquer sur Action puis délégation de contrôle – ajouter > mettre le groupe/la personne ayant les droits, cocher les taches a déléguer puis terminer enregistrer.
- Il suffit de créer une console délégué avec en affichage ce que l'on souhaite donner comme possibilités à l'utilisateurs.

Exercice 7 : Gestion des comptes utilisateurs

- Mettre en place un système de nommage:
Utilisateur de domaine : (1ere lettre du prénom, 1ere et dernière lettre du nom)
Administrateur de domaine : Nom d'utilisateur d'au-dessus + _ADMIN
Alain Levrat :
Utilisateur de domaine (ALT) / Administrateur de domaine (ALT_ADMIN)
- Compte **guest** désactivé sur Serveur Win2K16-1
- Mot de passes de compte sensible dans enveloppe cacheté puis dans un coffre anti-feu.
- M.Sautter absent 6 Semaines M.Ditter demande les identifiants de Sautter, **il faut demander une confirmation écrite au RH ou chef de service de Sautter**

Exercice 8 : Structure de dossiers

- Les profils aides les utilisateurs à retrouver un enviro. De travail particulier composer par le bureau, menu démarrer...
- **Profil local** : utilisateur retrouve son enviro. uniquement sur la machine sur laquelle il à configurer on enviro.
Profil itinérant : utilisateur retrouve son enviro. Même s'il se déplace de poste en poste.
- **UNC (Universal Naming Convention)** : un chemin de type [\\WIN2K16-1\profiles\%username%](#)
- Rendre accessible dossier sur le réseau on crée **partage**. On gère sécurité grâce aux **autorisation de partage** (CT,M ou L)
- Le \$ mis après le nom d'un dossier permet de cacher le dossier en question sur le réseau.
- Partage spécifique aux contrôleurs de domaine comme : **NETLOGON** contient les scripts utilisateurs, **SYSVOL** permet synchronisation entre les contrôleurs de domaine
- sécurité du système de fichiers **NTFS**
- **Cas particulier d'entreprise dépend de l'entreprise ex : Directeur et responsable vente travaille sur projet commun P_Rach.**
- **Organigramme**
- **Conception d'une arborescence de dossiers en fonction du cas particulier d'au-dessus.**

Exercice 9 : Gestion des groupes de sécurité

- Comptes locaux stockés dans base de sécurité **SAM** elle est présente sur clients et sur Serveurs si serveur promu en contrôleur de domaines comptes et groupes stockés dans **Active Directory** dans fichier **ntds.dit**
- Utilisateur est identifié sur domaine avec un **SID unique**
- Accès a base SAM (Poste de travail – gérer – utilisateurs et groupes globaux)
- Groupes d'utilisateur permet de simplifier l'administration.
- Conseiller de créer un groupe même pour une seul personne
- Le renommage n'affecte pas l'appartenance d'un compte à un groupe car SID unique
- Les groupes ont aussi un **SID**
- **Groupe global** : peut être utilisé sur tous les pc appartenant à n'importe quel domaine d'une forêt (on nomme g_Direction)
- **Domaine locaux** : Utilisable que dans domaine où ils résident. (On nomme dl_Direction_M si on projette un droit de modifier))
- Tableau des personnes appartenant à SON groupe global

- Les utilisateurs vont dans les groupes globaux et les groupes globaux vont dans les domaines locaux : Users -> g_Direction -> dl_Direction_M

Exercice 10 : Gestion des droits de partage et NTFS

- Partages ne sont applicables qu'aux dossiers pas aux fichiers.
- Le partage Exécuter existe pas.
- Sécurité : Aucunes autorisations pour le groupe « tout le monde ».
- Si doit éteindre serveur « Gestion de l'ordinateur » on peut visualiser les fichiers ouverts.
- Droit lecture ne permet que d'ouvrir mais pas de modifier ou de supprimer
- Sécurité obligatoirement passer par NTFS
- Droit NTFS pour supprimer c'est le droit modifier M
- CT à AUCUN UTILISATEUR
- Tableau à remplir d'autorisation de partage (CT,M,L,)
- Tableau à remplir de droit NTFS (CT,M,LX,E,L,A)

Exercice 11 : Implémentation de la structure de répertoires

- Les domaines d'une forêt partagent :le même schéma, la même config et le même catalogue
 - 2 domaines partagent même espace de nom = enfant **sinon** = nouvelle arborescence
 - Unités organisationnelle : structurer hiérarchiquement un domaine
 - Les sites de l'AD s'intéressent a la structure physique pour optimiser le trafic.
 - Partition D : 3Go pour contenir arborescence de l'exercice 8 / Partition E : contiendra données des applications
 - Appliquer les bon droits NTFS aux dossiers
 - Kixstart dans NETLOGON du serveur
 - Appliquer script pour utilisateurs il suffit d'aller dans son profils sur utilisateur de l'AD puis de mettre le nom du script.
-

Script Kixstart :

```
USE H:/delete
```

```
USE H: "\\WIN2K16SRV-1\Utilisqteurs$\%USERNAME%"
```

```
USE S:/delete
```

```
IF INGROUP("g_Direction")=1
```

```
USE S: "\\WIN2K16SRV-1\Services\Direction"
```

```
END IF
```

```
USE P:/delete
```

```
USE P: "\\WIN2K16SRV-1\Projet"
```