**BTS SIO** **SISR: Windows Server / Active Directory**

## Contexte

Nous avons vu beaucoup de services, système, et autre gestions de sécurité sous environnement Linux. Nous allons maintenant voir leur "équivalent" sous Windows.

## Déroulement de la séance

00- L'image ISO de Windows Server 2019 à utiliser est sur le réseau R:\ETUDIANTS\Ressources\Windows\Serveurs.

01- Faire une VM avec 4Go RAM / 2CPU / 1 coeurs / 60Go DD / Pas de clé de licence / Carte réseau en Custom **VMNet2**. Installer **Windows Server 2019 (experience de Bureau).**

02- Dans la configuration réseau figer l'adresse IP en statique sur 192.168.1.1 / 255.255.255.0 DNS 192.168.1.1 et pas de passerelle. Renommer votre machine en **DC1**.

03- Définir le mot de passe Administrateur local à **sisr2025!**

04- Dans le gestionnaire de serveur, nous allons installer les roles suivants:
- Serveur DHCP
- Serveur DNS
- Serveur Web IIS
- Services AD DS

05- pour exploiter les services fournis par notre serveur, nous aurons besoin d'une VM Windows 10 sur le VMNet2. VM W10 Client.

06- Pour le service Active Directory, nous allons créer une nouvelle foret **sio.local**

07- Après le reboot du serveur, nous allons configurer le serveur DHCP pour notre VM W10.
-> Créer une étendue sur les adresses IP 50 à 99.

08- Démarrer votre VM Windows 10 sur le VMNet2, vérifier qu'elle possède bien l'IP attendue.

09- La faire rentrer sur le domaine SIO.local à l'aide du compte Administrateur

10- Sur votre serveur, tous les outils utiles pour gérer votre Domaine AD se trouvent dans **Démarrer / Outils d'administration**. Créer un utilisateur **test** sur le domaine SIO mot de passe **sisr2025!**, seconnecter sur le client avec cet utilisateur.

11- Sur le serveur, créer un répertoire C:\Partage, le partager pour l'utilisateur **test.**
Créer 2 fichiers textes **text.txt et text2.txt** dans ce dossier.

12- Sur le serveur, modifier le profil de l'utilisateur pour que s'execute un script **login.bat** au démarrage. Ajouter également un lecteur réseau X: \\DC1\Partage

13- Ecrire un script **login.bat** stocker dans **C:\Windows\SYSVOL\sysvol\sio.local\scripts**, qui va copier les fichiers text1 et text2 depuis X: sur le bureau de l'utilisateur.

14- Valider le bon fonctionnement du script en ouvrant une session **test** sur le client.

15- Sur votre Windows Serveur, ouvrir le gestionnaire DNS:
- Créer un alias (CNAME) **www** vers votre serveur dans la zone **sio.local**
- recharger la zone et tester la config précédente avec la commande **nslookup**

- Créer une zone inversée 192.168.1 avec les **PTR** correspondant aux IP de votre réseaux
- recharger la zone et tester la config précédente avec la commande **nslookup (www.sio.local et 192.168.1.1)**

- Créer une nouvelle zone principale **google.fr**, y créer un enregistrement A **www** vers **192.168.1.1**
- recharger la zone et effectuer un ping **www.google.fr** . Que penser du résultat ? Quelle utilité peut bien avoir une telle configuration ?

- Sur votre Client Windows 10, essayez d'accéder au site http://www.sio.local puis http://www.google.fr . Pourquoi ce résultat ?

16- Introduction aux GPOs (Voir PDF 02- gpos.pdf)

**Rappel des commandes utiles GPO:**
**gpupdate /force -> pour mettre a jour la liste des GPO sur le client**
**gpresult /r -> affiche la liste des GPO appliquées**
**rsop -> affiche le contenu des GPO appliquées**

17- Réalisation d'une Première GPO **Utilisateur** selon le tuto (désactivation de la console CMD):

https://www.it-connect.fr/chapitres/comment-creer-sa-premiere-gpo/

18- En se basant sur la GPO Précédente, créer une GPO **Utilisateur** de personnalisation
- empecher les utilisateurs du domaine (et non les Administrateurs) de modifier les fonds d'ecrans
- forcer un fond d'ecran de votre choix
- empecher les utilisateurs d'accèder à leur stockage amovible (clé usb)

19- En se basant sur la GPO Précédente, créer une GPO **Machine** pour déployer **Firefox**

https://www.it-connect.fr/comment-deployer-un-logiciel-au-format-msi-par-gpo/