TRAVAIL PRATIQUE 1

DÉPLOIEMENT D'UN DOMAINE AD

ECE-PA-ING4-WINSRV

Objectifs pédagogiques

- Installer un **contrôleur de domaine** (AD DS + DNS) dans une **nouvelle forêt**
- Organiser l'annuaire : **OU, utilisateurs, groupes**, poste client
- Déployer des **GPO** de sécurité et de poste de travail
- Mettre en place un **partage SMB** avec droits NTFS et mapping par GPO
- Tester et valider le bon fonctionnement (DNS, authentification, journaux, gpresult)

Contraintes et livrables

- **Contraintes de nommage** :
  - DC : `SRV-DC-GPXX`
  - Client : `CLI-GPXX`
  - Domaine : `gpXX.lab.ece`
  - Comptes : `user1.gpXX` , `user2.gpXX` , `admin.gpXX`
  - Groupes : `Grp-GPXX-Utilisateurs` , `Grp-GPXX-Admins` , etc

  où XX correspond au numéro de votre groupe

- **Livrables du groupe (un fichier PDF unique)** :
  - Captures d'écran annotées des étapes clés
  - Réponses à **toutes les questions** de chaque partie
  - Tableau des tests réalisés (gpresult, nslookup, etc.)

- **Livrable individuel (un fichier PDF par étudiant)** :
  - Réponse à **1 seule question** parmi les 4 de fin de TP (**pas de doublon** dans un groupe)
  - Conclusion personnelle : difficulté rencontrée, point clé appris, bonne pratique

Travail collectif

Partie 1 - Installation du DC

1. Renommez le serveur en **SRV-DC-GPXX**.
2. Configurez une adresse IP statique et indiquez comme DNS l'adresse IP du DC.
3. Installez le rôle **AD DS** via Server Manager et promouvez le serveur en DC :
   - Nouvelle forêt : `gpXX.lab.ece`

- Choisissez un mot de passe DSRM robuste
- Laissez le rôle DNS s'installer automatiquement

4. Redémarrez et connectez-vous avec le compte `Administrateur@gpXX.lab.ece`.
5. Vérifiez la zone DNS `gpXX.lab.ece` et les enregistrements SRV (`_ldap`, `_kerberos`).
6. Lancez un **dcdiag** et notez les éventuelles anomalies.

📌 **Captures attendues** :

- Résumé de l'assistant de promotion
- Zone DNS + enregistrements SRV
- Résultats dcdiag (extrait)

❓ **Questions** :

1. Pourquoi `gpXX.lab.ece` est-il préférable à `.local` ?
2. À quoi servent les enregistrements SRV `_ldap._tcp` et `_kerberos._tcp` ?
3. Que vérifier en priorité si `dcdiag` remonte une erreur DNS ?
4. Quel est l'intérêt de configurer des redirecteurs DNS (forwarders) ?

Partie 2 - Organisation de l'annuaire

1. Créez 2 OU : `Utilisateurs-GPXX` et `Ordinateurs-GPXX`.
2. Créez les comptes :
   - `user1.gpXX` et `user2.gpXX` (mot de passe fort, changement au 1er logon)
   - `admin.gpXX`
3. Créez deux groupes de sécurité (Globaux) :
   - `Grp-GPXX-Utilisateurs` → ajoutez `user1` et `user2`
   - `Grp-GPXX-Admins` → ajoutez `admin.gpXX`
4. Déplacez les objets dans les OU correspondantes.
5. Vérifiez l'appartenance aux groupes avec la commande :

```
whoami /groups
```

📌 **Captures attendues** :

- Structure des OU
- Propriétés d'un compte
- Membres des groupes

❓ **Questions** :

1. Pourquoi organiser les objets dans des OU avant de déployer des GPO ?

2. Quel est l'intérêt d'utiliser des groupes plutôt que d'attribuer des droits aux utilisateurs directement ?
3. Proposez une organisation OU adaptée à une entreprise ayant 2 sites (Paris, Lyon) et 3 services (RH, IT, Finance).
4. Quels risques si tous les objets sont laissés à la racine du domaine ?

Partie 3 - Intégration du poste client

1. Renommez le client en **CLI-GPXX**.
2. Configurez le DNS du client pour qu'il pointe sur le DC.
3. Rejoignez le domaine `gpXX.lab.ece` et redémarrez.
4. Connectez-vous avec `user1.gpXX` puis `admin.gpXX` . Comparez les différences.
5. Vérifiez les stratégies appliquées :

```
gpresult /R
```

6. Consultez l'observateur d'événements et identifiez au moins :
   - un événement 4624 (connexion réussie)
   - un événement 4625 (connexion échouée)

📌 **Captures attendues** :

- Écran de jonction au domaine
- Résultat `gpresult /R`
- Événements 4624 et 4625

❓ **Questions** :

1. Pourquoi le client doit-il utiliser le DNS du DC avant de rejoindre le domaine ?
2. Que se passe-t-il si vous configurez 8.8.8.8 comme DNS du client ?
3. Que prouvent les événements 4624 et 4625 dans les journaux de sécurité ?
4. Quelles différences avez-vous constatées entre `user1.gpXX` et `admin.gpXX` ?

Partie 4 - GPO

1. Modification de la GPO `Default Domain Policy` :
   - Longueur minimale : 10
   - Complexité activée
   - Historique : 5 derniers mots de passe
   - Verrouillage après 5 tentatives pendant 15 minutes
2. Créez une nouvelle GPO `GPO-Securite-GPXX` appliquée à `Ordinateurs-GPXX` :

- Message de logon personnalisé
- Interdiction d'accès au Panneau de configuration
- Fond d'écran imposé :
  - Créez `C:\Shares\Public\Wallpapers\corp.jpg` sur le DC
  - Partagez `\\SRV-DC-GPXX\Public$`
  - Configurez la GPO pour appliquer ce fond d'écran
- Blocage d'exécutables dans Téléchargements :
  - SRP (Professional) ou AppLocker (Enterprise)
  - Règle : interdiction de `%USERPROFILE%\Downloads\*.exe`

3. Forcez l'application :

```
gpupdate /force
```

4. Testez tous les paramètres (mot de passe, logon, panneau de config, fond d'écran, blocage exe).

📌 **Captures attendues** :

- Paramètres GPO (extraits)
- Fond d'écran appliqué
- Panneau de configuration bloqué
- Exécutable bloqué dans Téléchargements

❓ **Questions** :

1. Pourquoi faut-il tester une GPO avant un déploiement global ?
2. Quelles sont les différences majeures entre SRP et AppLocker ? Quel choix avez-vous fait ici ?
3. Où serait-il préférable de stocker le fond d'écran pour plus de robustesse et pourquoi ?
4. Donnez un exemple de mauvaise GPO et ses conséquences possibles.

Partie 5 - Partage SMB et droits NTFS

1. Créez `C:\Data\Compta` sur le DC et partagez-le en **Compta$**.
2. Créez deux groupes supplémentaires :
   - `GG-Compta-Users-GPXX` (Global) → ajoutez `user2.gpXX`
   - `DL-Compta-RW-GPXX` (Domain Local) → membre = `GG-Compta-Users-GPXX`
3. Appliquez les droits NTFS sur `C:\Data\Compta` :
   - `DL-Compta-RW-GPXX` : Modify
   - Administrators/SYSTEM : Full
   - Pas d'accès pour les autres
4. Configurez une GPO pour monter le partage en lecteur **H:** pour `Utilisateurs-GPXX`

5. Connectez-vous avec `user2.gpXX` → doit créer/modifier des fichiers
6. Connectez-vous avec `user1.gpXX` → accès limité

📌 **Captures attendues** :

- ACL NTFS et propriétés du partage
- Configuration GPO
- Tests avec `user2.gpXX` et `user1.gpXX`

❓ **Questions** :

1. Expliquez le principe **AGDLP** utilisé ici
2. Pourquoi séparer Groupes Globaux (utilisateurs) et Domain Local (droits) ?
3. Quelle est la différence entre droits NTFS et droits de partage (et lequel prime) ?
4. Quelle preuve avez-vous produit pour montrer que la configuration fonctionne ?

Travail individuel

Chaque étudiant doit répondre à **une seule question** parmi les 4 suivantes (pas de doublon dans un même groupe) :

1. Imaginez qu'une mauvaise GPO ait été appliquée au niveau du domaine et qu'elle bloque toutes les connexions utilisateurs. Quelles sont les étapes pour corriger la situation sans aggraver les choses ?
2. Vous devez préparer un Active Directory pour une entreprise de 500 utilisateurs qui prévoit de doubler sa taille dans 2 ans. Proposez une organisation d'OU et de groupes qui facilite l'évolutivité et la gestion future.
3. Un utilisateur se plaint de ne pas recevoir les GPO attendues. Quels outils et méthodes utilisez-vous pour identifier l'origine du problème (DNS, réplication, permissions, filtres…) et comment le résoudre ?
4. Vous êtes chargé d'expliquer à la direction générale pourquoi l'Active Directory reste une cible privilégiée des attaquants. Rédigez un argumentaire clair et non technique, basé sur son rôle central dans l'entreprise.

En plus de répondre à l'une des quatre questions proposées, chaque étudiant doit rédiger une **conclusion personnelle** (10 à 15 lignes) sur ce TP.

Commandes utiles

- `dcdiag /v` : diagnostic DC

- `nslookup` , `ping` , `ipconfig /all` : tests réseau/DNS
- `gpresult /R` ou `/H rapport.html` : GPO appliquées
- **Événements** Sécurité :
  - 4624 = logon réussi
  - 4625 = échec logon
  - 4728/4732 = ajout groupe
  - 4738 = modif compte