

TP1

Objectifs principaux :

1. **Installer Windows Server 2008** et **Windows 7** sur des machines virtuelles (VM).
2. **Créer un réseau local** entre les deux machines virtuelles.
3. **Configurer Active Directory (AD)** pour gérer un domaine.
4. **Ajouter un ordinateur (Windows 7) au domaine.**

Étapes clés

1. Création des machines virtuelles (VMWare)

- **Windows Server 2008** (40 Go de disque) et **Windows 7** (20 Go).
- Choix de la méthode d'installation : **ISO** ou **CD-ROM**.
- Configuration du nom et de l'emplacement des fichiers VM.

2. Configuration du réseau local

- **Mode Host-Only** : Pour isoler les machines virtuelles entre elles.
- **Attribution des adresses IP manuelles** :
 - Serveur : **192.168.1.1** (avec DNS pointant vers lui-même).
 - Client : IP dans le même sous-réseau (ex: **192.168.1.2**).
- Vérification avec **ipconfig** dans l'invite de commandes (**cmd**).

3. Installation d'Active Directory (AD)

- Lancer **dcpromo** pour promouvoir le serveur en **contrôleur de domaine**.
- Création d'une **nouvelle forêt** avec le nom de domaine **DepInfo.to**.
- Choix du **niveau fonctionnel** : Windows Server 2008.
- Définition d'un **mot de passe** (ex: **DepInfo123**).
- Redémarrage pour finaliser l'installation.

4. Ajout d'un ordinateur au domaine

- Sur la machine **Windows 7**, configurer le DNS pour pointer vers le serveur (**192.168.1.1**).
- Joindre le domaine **DepInfo.to** via les propriétés système.

Concepts importants

- **Active Directory (AD)** : Service Microsoft pour la gestion centralisée des utilisateurs, ordinateurs et stratégies.
- **Forêt/Domaine** : Structure hiérarchique pour organiser les ressources réseau.
- **Host-Only vs NAT vs Bridged** :
 - **Host-Only** : Réseau isolé entre VMs.
 - **NAT** : Accès Internet partagé avec la machine hôte.

- **Bridged** : La VM agit comme un appareil indépendant sur le réseau physique.

TP2

Objectifs principaux :

1. **Créer des Unités d'Organisation (OU)** graphiquement et en ligne de commande.
2. **Gérer des utilisateurs** via l'interface graphique (**DSA.msc**) et la commande **DSADD**.
3. **Restreindre les horaires de connexion** pour un utilisateur.

Étapes clés

1. Création d'Unités d'Organisation (OU)

- **Graphiquement** (via **DSA.msc**) :
 - Créer une **OU "Etudiants"** avec des sous-OU (**L2, L3, M1, M2**).
 - Supprimer une OU : Clic droit → *Supprimer* (après activation des *Fonctionnalités avancées*).
- **En ligne de commande (DSADD)** :

`dsadd ou "OU=Enseignants,DC=DepInfo,DC=to"`

`dsadd ou "OU=Vacataires,OU=Enseignants,DC=DepInfo,DC=to"`

2. Création d'utilisateurs

- **Graphiquement (DSA.msc)** :
 - Exemple : Utilisateur **"Etudiant1"** dans l'OU **M1**.
 - Nom de connexion : **Etudiant1@DepInfo.to**
 - Mot de passe : **EtudiantM123\$\$** (désactiver *"Changer le mot de passe au prochain login"*).
- **En ligne de commande (DSADD)** :

`dsadd user "CN=Etudiant2,OU=M1,OU=Etudiants,DC=DepInfo,DC=to" -pwd P@ssw0rd -upn Etudiant2@DepInfo.to`

- **Création en masse** (exemple pour 3 utilisateurs) :
 - `for %i in (1 2 3) do dsadd user "CN=User-%i,OU=M2,OU=Etudiants,DC=DepInfo,DC=to" -pwd P@ssw0rd%i -upn User-%i@DepInfo.to`

3. Restrictions d'accès

- **Interdire les connexions** à un utilisateur (ex: *Etudiant1* le lundi) :
 - Propriétés de l'utilisateur → Onglet *Compte* → *Horaires d'accès* → Bloquer le lundi.

Concepts importants

- **Unités d'Organisation (OU)** : Structure hiérarchique pour organiser les utilisateurs/groupes (ex: par promotion, département).
 - **DSADD** : Commande PowerShell pour automatiser la gestion d'Active Directory.
 - **User Principal Name (UPN)** : Format de connexion moderne (`utilisateur@domaine`).
 - **Gestion des horaires** : Permet de contrôler les plages d'accès aux ressources.
-

TP3

Objectifs principaux :

1. **Créer des groupes (globaux et locaux)** graphiquement et via la commande `DSADD`.
2. **Administrer les membres des groupes** (ajout d'utilisateurs, imbrication de groupes).
3. **Affecter un responsable** à un groupe.

Étapes clés

1. Création de groupes

- **Graphiquement** (via `DSA.msc`) :
 - **Groupes globaux** dans l'OU *M1* :
 - `G_M1SI` (ex: pour les étudiants en Systèmes d'Information).
 - `G_M1CPI` (ex: pour les étudiants en Cyber-sécurité).
 - **Groupe local** dans l'OU *Ressources* :
 - `DL_Imprimante` (pour gérer les accès aux imprimantes).
- **En ligne de commande** (`DSADD`) :

Groupes globaux (scope g) :

```
dsadd group "CN=G_M1SI,OU=M1,OU=Etudiants,DC=DepInfo,DC=to" -scope g  
-secgrp yes
```

```
dsadd group "CN=G_M1RMSE,OU=M1,OU=Etudiants,DC=DepInfo,DC=to" -scope g  
-secgrp yes
```

Groupe local (scope l) :

```
dsadd group "CN=DL_Partage,OU=Ressources,DC=DepInfo,DC=to" -scope l  
-secgrp yes
```

2. Gestion des membres

- **Ajout d'utilisateurs :**
 - Etudiant1 et Etudiant2 dans G_M1SI.
 - Etudiant3 et Etudiant4 dans G_M1CPI.
- **Imbrication de groupes :**
 - Ajouter G_M1SI et G_M1CPI au groupe local DL_Imprimante (pour hériter des permissions).

3. Affectation d'un responsable

- Dans les propriétés d'un groupe (ex: G_M1SI), désigner un **responsable** (ex: un enseignant ou administrateur).

Concepts importants

- **Groupes globaux (scope g) :**
 - Utilisés pour organiser les utilisateurs par **rôles/fonctions** (ex: étudiants, enseignants).
 - Peuvent être membres d'autres groupes (y compris locaux).
- **Groupes locaux (scope l) :**
 - Utilisés pour **attribuer des permissions** (ex: accès à une imprimante, un dossier partagé).
- **Groupes de sécurité (-secgrp yes) :**
 - Permettent de gérer les droits d'accès (contrairement aux groupes de distribution).

TP4

Objectifs principaux :

1. **Configurer les permissions NTFS et de partage** sur un dossier local (Windows 7).
2. **Tester l'accès local et distant** avec des utilisateurs locaux et AD.
3. **Comprendre l'interaction** entre permissions NTFS et partage.

Étapes clés

1. Permissions NTFS et partage en local (Windows 7)

- **Création d'un utilisateur local :**

```
net user UserTest P@ssw0rd123 /add
```

Vérification du groupe de l'utilisateur :

```
net localgroup Utilisateurs # Vérifie les membres du groupe "Utilisateurs"
```

`net users UserTest` # Affiche les détails de l'utilisateur (type de compte)

- **Dossier test (C:\DossierTest) :**
 - **Permissions NTFS :** Autoriser *Lecture* mais refuser *Écriture* pour `UserTest`.
 - **Permissions de partage :** Donner *Contrôle total* à `UserTest`.
- **Test d'accès local :**
 - **Autorisé :** Ouvrir un fichier.
 - **Interdit :** Modifier/supprimer un fichier (priorité aux permissions NTFS).

2. Accès distant via Active Directory (Windows Server)

- **Scénario 1 :**
 - **Permissions de partage :** *Lecture* pour le groupe `G1-Test`.
 - **Permissions NTFS :** *Contrôle total* pour `G1-Test`.
 - **Résultat :** L'accès distant est limité à la *lecture* (la permission la plus restrictive s'applique).
- **Scénario 2 :**
 - **Permissions combinées :**
 - Partage : *Lecture + Modification*.
 - NTFS : *Contrôle total*.
 - **Résultat :** L'utilisateur peut *modifier* le fichier (la moins restrictive des deux prévaut).

3. Dossier caché

- **Syntaxe :** `\\NomDuServeur\DossierCache$` (le \$ masque le partage dans l'explorateur).

Concepts importants

- **Permissions NTFS :**
 - Gèrent les accès *locaux* aux fichiers/dossiers (ex: *Lecture*, *Écriture*).
- **Permissions de partage :**
 - Contrôlent l'accès *réseau* (ex: *Contrôle total*, *Modification*).
- **Règle de combinaison :**
 - **Accès local :** Seules les permissions NTFS s'appliquent.
 - **Accès distant :** La permission *la plus restrictive* entre NTFS et partage est retenue.

TP5

Objectifs Pédagogiques :

1. **Créer et lier des GPO** pour modifier l'environnement utilisateur.
2. **Configurer des restrictions** via les GPO (menu Exécuter, Corbeille, Panneau de configuration).

3. **Comprendre l'héritage des GPO** et le bloquer si nécessaire.
4. **Tester et vérifier** l'application des stratégies.

Étapes Clés

1. Préparation de la Structure Active Directory

- Création de deux utilisateurs :
 - **Etudiant3** dans l'OU **L3**.
 - **Etudiant4** dans l'OU **L2**.
 - Tous deux sous l'OU parente **Etudiants**.

2. Création et Liaison des GPO

- **Outil utilisé** : *GPMC (gpmc.msc)*.
- **GPO1** (liée à l'OU **Etudiants**) :
 - **Action** : Supprime le menu **Exécuter** du menu Démarrer.
 - Chemin :
Configuration utilisateur > Modèles d'administration > Menu Démarrer et barre des tâches > "Supprimer le menu Exécuter".
- **GPO2** (liée à l'OU **L3**) :
 - **Action** : Masque l'icône **Corbeille** du bureau.
 - Chemin :
Configuration utilisateur > Modèles d'administration > Bureau > "Supprimer l'icône Corbeille".
- **GPO3** (liée à l'OU **L2**) :
 - **Action** : Bloque l'accès au **Panneau de configuration**.
 - Chemin :
Configuration utilisateur > Modèles d'administration > Panneau de configuration > "Empêcher l'accès au Panneau de configuration".

3. Application et Vérification des GPO

- **Commande pour actualiser** :

`gpupdate /force`
- **Tests** :
 - **Etudiant3** (OU **L3**) :
 - Menu Exécuter **masqué** (GPO1 héritée).
 - Corbeille **masquée** (GPO2).
 - Panneau de configuration **accessible** (non affecté par GPO3).
 - **Etudiant4** (OU **L2**) :
 - Menu Exécuter **masqué** (GPO1 héritée, sauf si blocage).

- Panneau de configuration **bloqué** (GPO3).
- Corbeille **visible** (non affectée par GPO2).

4. Blocage de l'Héritage des GPO

- **Action** : Bloquer l'héritage sur l'OU **L2**.
 - **Conséquence** :
 - Les GPO parentes (ex: GPO1 sur **Etudiants**) ne s'appliquent **plus** à **L2**.
 - Seules les GPO directement liées à **L2** (ex: GPO3) restent actives.
 - **Exemple** :
Etudiant4 ne sera plus affecté par la GPO1 (menu Exécuter réapparaît).

Concepts Importants

- **GPO (Group Policy Object)** :
 - Permet de centraliser la gestion des paramètres utilisateur/ordinateur dans un domaine Active Directory.
- **Héritage** :
 - Par défaut, les GPO parentes s'appliquent aux OUs enfants (surchargeable).
- **Priorité** :
 - En cas de conflit, la GPO la plus **proche** de l'OU (ou avec l'option "*Forcer*") l'emporte.
- **Bonnes Pratiques** :
 - Tester les GPO dans un OU dédié avant déploiement large.
 - Utiliser **gpresult /r** pour vérifier les stratégies appliquées à un utilisateur/machine.

TP6

Objectifs Pédagogiques :

1. **Configurer une stratégie de mot de passe** via la *Default Domain Policy*.
2. **Bloquer les ports USB** via une GPO dédiée.
3. **Réinitialiser un mot de passe** utilisateur dans Active Directory.
4. **Maîtriser le filtrage de sécurité** pour cibler des GPO.

Étapes Clés

1. Stratégie de Mot de Passe

- **Modification de la *Default Domain Policy*** :
 - Chemin :
Configuration ordinateur > Stratégies > Paramètres de

sécurité > Stratégies de comptes > Stratégie de verrouillage de compte.

- **Paramètres clés :**
 - **Seuil de verrouillage :** Nombre d'échecs avant blocage (ex: 3 tentatives).
 - **Durée de verrouillage :** Réduite à **1 minute** (au lieu de 30 par défaut).
- **Application :**
gpupdate /force
- **Test :** Saisir 3 fois un mot de passe erroné pour vérifier le verrouillage temporaire.

2. Réinitialisation de Mot de Passe

- **Méthode :**
 - Dans *Utilisateurs et ordinateurs Active Directory* → Clic droit sur l'utilisateur → *Réinitialiser le mot de passe*.

3. GPO de Blocage des Ports USB

- **Création d'une GPO "Blocage_USB" :**
 - **Liaison** à l'OU L3.
 - **Paramétrage :**
Configuration ordinateur > Modèles d'administration > Système > Accès au stockage amovible > "Toutes les classes de stockage amovible" → **Désactivé**.
 - **Effet :** Empêche l'utilisation des clés USB sur les machines ciblées.

4. Filtrage de Sécurité

- **Principe :** Restreindre l'application d'une GPO à des utilisateurs/groupes spécifiques.
- **Méthode :**
 - Supprimer "*Utilisateurs authentifiés*" dans **Délégation > Avancé**.
 - Ajouter un **groupe de sécurité** (ex: **G_Admin**) pour limiter la GPO aux membres de ce groupe.

Concepts Importants

- **Default Domain Policy :**
 - Stratégie globale s'appliquant à **tout le domaine** (ex: politiques de mot de passe).
- **GPO USB :**
 - Utilise les **paramètres ordinateur** (agit sur la machine, pas l'utilisateur).
- **Filtrage de sécurité :**
 - Permet de **cibler finement** les GPO (ex: ne bloquer les USB que pour les étudiants, pas les profs).

TP7

Objectifs Pédagogiques :

1. **Déployer un logiciel** (ex: Google Chrome) via GPO en utilisant deux méthodes :
 - **Affectation** (installation forcée).
 - **Publication** (installation à la demande).
2. **Configurer un point de distribution réseau** pour héberger les packages logiciels.
3. **Tester et désinstaller** un logiciel déployé via GPO.

Étapes Clés

1. Préparation de l'Active Directory

- Création de deux **OUs** sous **M2** :
 - **M2_SI** → Utilisateur **Etudiant5**.
 - **M2_CPI** → Utilisateur **Etudiant6**.

2. Création du Point de Distribution

- **Dossier partagé** :
 - Chemin : **C:\Application** → Partage nommé **Applications\$** (masqué).
 - Permissions : Accès "**Lecture**" pour "*Tout le monde*".
- **Dépôt du package** :
 - Y placer le fichier **.MSI** du logiciel (ex: **chrome.msi**).

3. Déploiement par Affectation (Installation Forcée)

- **GPO liée à M2_SI** (nommée **GPO_Affectation**) :
 - Chemin GPO :
Configuration utilisateur > Stratégies > Installation de logiciels > Nouveau Package.
 - **Package** : Sélectionner le **.MSI** via le **chemin réseau** (ex: **\\Serveur\Applications\$\chrome.msi**).
 - Choisir "**Affecté**".
- **Effet** :
 - Le logiciel est **installé automatiquement** pour **Etudiant5** (raccourci dans *Démarrer > Tous les programmes*).

4. Déploiement par Publication (Installation à la Demande)

- **GPO liée à M2_CPI** (nommée **GPO_Publication**) :
 - Même chemin que l'affectation, mais choisir "**Publié**".

- **Effet :**
 - Etudiant6 peut installer le logiciel via :
Panneau de configuration > Programmes > Installer un logiciel réseau.

5. Désinstallation du Logiciel

- **Méthode :**
 - Supprimer le package de la GPO GPO_Publication → Actualiser avec `gpupdate /force`.
- **Effet :**
 - Le logiciel est **désinstallé** pour Etudiant6.

Concepts Importants

- **Affectation vs Publication :**
 - **Affectation** : Installation obligatoire (visible dès la connexion).
 - **Publication** : Installation facultative (via le Panneau de configuration).
- **Point de distribution :**
 - Doit être accessible en **lecture** par les machines cibles (utilisation d'un chemin UNC : `\\Serveur\Partage$`).
- **Format requis :**
 - Seuls les fichiers **.MSI** (Windows Installer) sont supportés pour le déploiement GPO.