TP SISR — Annuaire d’établissement : AD DS, DNS, DHCP & GPO (PowerShell)

Contexte

Vous mettez en place l’infrastructure d’un établissement scolaire.
Environnement recommandé (minimum) :

- **SRV-DC1** (Windows Server 2022) : **AD DS**, **DNS**, **DHCP** (contrôleur de domaine).
- **SRV-FS1** (Windows Server 2022, membre du domaine) : **serveur de fichiers** (dossiers personnels, quotas).
- **CL-W10/11** (client, membre du domaine) pour tests utilisateurs.

Les serveurs auront des **IP fixes** hors du pool DHCP. Le client obtiendra son adresse via DHCP.

Objectifs

1. Déployer le domaine **mediaschool.local** avec **AD DS** et **DNS** intégrés.
2. Fournir des adresses IP via **DHCP** (pool 192.168.100.50–200, bail 6 h) et options adaptées.
3. Structurer l’annuaire (OU, groupes, comptes).
4. Créer et **lier des GPO uniquement via PowerShell** (module **GroupPolicy**) :
    - Politique de **quotas** appliquée aux dossiers personnels (déployés sur SRV-FS1).
    - **Horaires de connexion** différents selon le groupe (Administration / Profs / Élèves).
5. Vérifier le fonctionnement (adhésion domaine, attribution IP, application GPO, quotas, restrictions horaires).

Contraintes & Prérequis

- Windows Server 2022 (éval), Windows 10/11 pour le poste client.
- Accès **PowerShell** (exécuter en **élevé**).
- Rôles/Features à installer selon besoin : **AD-Domain-Services**, **DNS**, **DHCP**, **File Services**, **FSRM** (File Server Resource Manager) sur **SRV-FS1**.
- NTP cohérent sur tous les hôtes.
- Pare-feu : autoriser le trafic AD/DNS/DHCP/SMB entre hôtes.

Livrables

1. **Schéma logique** : noms d'hôtes, IP, masque, passerelle, DNS, rôle par machine.
2. **Arborescence AD** (OU), **groupes**, et **règles de nommage** retenues.
3. **Scripts PowerShell** (.ps1) utilisés pour :
    - Création/Liaison des **GPO**,
    - Affectation des **horaires de connexion** par groupe,
    - (optionnel) Création d'utilisateurs, groupes, OU.
4. **Captures d'écran** :
    - DHCP (scope actif, bail de 6 h, options),
    - DNS (zone directe/reverse, enregistrements),
    - GPMC (liaisons GPO),
    - FSRM (quotas effectifs),
    - Session refusée/acceptée selon horaires,
    - Poste client avec IP du pool et appartenance au domaine.
5. **Procédure de test** détaillée + **analyse** (1 page max).

Travaux à réaliser

A. Plan d’adressage & DNS

1. Fixer les IP des serveurs (exemple à adapter) :
    - **SRV-DC1** : 192.168.100.10/24, GW 192.168.100.1, DNS = 192.168.100.10
    - **SRV-FS1** : 192.168.100.20/24, GW 192.168.100.1, DNS = 192.168.100.10
2. Installer **AD DS** et promouvoir **SRV-DC1** en **contrôleur de domaine** du **nouveau domaine** : `mediaschool.local`.
3. Vérifier la **zone DNS** `mediaschool.local` et créer la **zone reverse** (192.168.100.0/24).
4. S’assurer que l’enregistrement DNS de **SRV-FS1** s’enregistre correctement.

B. DHCP (sur SRV-DC1)

1. Installer et **autoriser** le rôle **DHCP** dans AD.
2. Créer un **scope** :
    - Nom : `SCOPE-SALLE-INFO`
    - Pool : **192.168.100.50** → **192.168.100.200**
    - **Bail : 6 heures**
    - Exclusions : réserver une plage pour futurs serveurs si nécessaire.
3. **Options** du scope :
    - **003 Router** = 192.168.100.1
    - **006 DNS Servers** = 192.168.100.10
    - **015 DNS Domain Name** = mediaschool.local
4. Activer les **mises à jour dynamiques DNS** sécurisées par DHCP.

5. Vérifier sur le **poste client** l'obtention d'une adresse du pool et la résolution DNS.

C. Modélisation Active Directory

1. Créer l'OU racine : **ECOLE**.
2. Sous-OU : **Comptes-Utilisateurs** (avec **Administration**, **Profs**, **Eleves**), et **Comptes-Ordinateurs**.
3. Créer **3 groupes de sécurité globaux** :
    - `MS-Administration`, `MS-Profs`, `MS-Eleves`.
4. Créer au minimum **2 utilisateurs par groupe** (nommage clair).
5. Joindre **SRV-FS1** et **CL-W10/11** au domaine.

D. Partages & Dossiers Personnels (SRV-FS1)

1. Créer un volume **D:\Donnees** (ou équivalent) et un partage **\SRV-FS1\Homes**.
2. Déployer des **dossiers personnels** par utilisateur (ex. `\\SRV-FS1\Homes\%USERNAME%`), ACL appropriées (propriétaire exclusif).
3. Installer **FSRM** et préparer des **modèles de quotas** :
    - **Administration** : 10 Go, alerte 85%
    - **Profs** : 5 Go, alerte 85%
    - **Eleves** : 1 Go, alerte 85%
4. Appliquer les **quotas** sur les dossiers personnels (ciblage par groupe).

Les **quotas sont configurés sur SRV-FS1** (FSRM). La GPO servira à **déployer/monter** le lecteur perso (GPP) et à **normaliser** des paramètres ; la **limitation d'espace** est assurée par FSRM.

E. GPO (création & liaison exclusivement en PowerShell)

1. **Créer** une GPO **par public** (3 GPO minimales) et les **lier** aux OU concernées :

- `GPO-ADM-Poste` (Administration),
- `GPO-PROF-Poste` (Profs),
- `GPO-ELEVE-Poste` (Élèves).

2. **Contenu attendu** (exemples non exhaustifs) :
   - **Montage du lecteur personnel H:** via **Preferences** → **Drive Maps** (chemin `\\SRV-FS1\Homes\%USERNAME%`).
   - Stratégies de **sécurité** de base (écran de veille forcé, délai, redirection dossiers si souhaité).
   - Activer : **Network security: Force logoff when logon hours expire** (sécurité → options).
3. **Règle** : toute opération GPO (création, configuration, liaison, enforcement, filtrage sécurité si utilisé) doit être réalisée **via PowerShell** (module **GroupPolicy**).

Livrer les scripts `.ps1` correspondants.

F. Horaires de connexion (différenciés par groupe)

Définir et appliquer (via **PowerShell** sur les comptes AD) les **plages horaires** suivantes :

- **Administration** : **Lun–Ven 07:00–19:00**
- **Profs** : **Lun–Ven 07:00–20:00** et **Sam 08:00–12:00**
- **Élèves** : **Lun–Ven 08:00–18:00**, **interdit** le week-end

Exigences :

1. Affecter automatiquement ces **logon hours** à **tous les membres** des groupes `MS-Administration`, `MS-Profs`, `MS-Eleves`.
2. Documenter la logique (matrice 7×24, fuseau horaire).
3. Vérifier le **refus de session** hors créneau sur le poste client (message d'erreur ou déconnexion forcée selon politique).

Remarque : les **horaires de connexion** sont une **propriété du compte AD** (pas un paramètre GPO). L'activation de « **Force logoff when logon hours expire** » dans la GPO de domaine aide à l'application côté sessions réseau.

G. Vérifications & Tests

1. **DHCP** : le client reçoit une IP du **pool** ; le **bail** indique **6 h** ; DNS suffix = mediaschool.local.
2. **DNS** : résolutions directes et inverses (ping SRV-DC1 / SRV-FS1 par nom & IP).
3. **Quotas** : tenter de dépasser la limite dans le dossier personnel → blocage attendu.
4. **GPO** : le lecteur **H:** est monté ; paramètres de sécurité appliqués.
5. **Horaires** :
    - Créer un scénario de connexion **interdite** (ex. élève un samedi) → **connexion refusée**.
    - Connexion **autorisée** dans la fenêtre prévue → **succès**.
6. Capturer journaux pertinents (**Event Viewer**, **FSRM**, **DHCP**, **DNS**, **GPResult**/`gpupdate`).

Questions de réflexion (à rendre)

1. Expliquez le **rôle** de chaque composant (AD DS, DNS, DHCP, GPO, FSRM) et le **chemin** d'une authentification domaine jusqu'au montage du lecteur.
2. Comparez **NTFS quotas** vs **FSRM quotas** pour ce cas d'usage. Pourquoi choisir FSRM ?
3. Quels risques si le **DHCP** n'actualise pas correctement **DNS** ? Quelles bonnes pratiques ?
4. Proposez **2 améliorations** de sécurité et **2** d'exploitabilité (sauvegardes, modèles GPO, délégation, WMI filtering…).

TP SISR - Partie 2 WSUS & Masterisation (UI ou PowerShell)

Contexte (rappel)

Environnement minimal :

- **SRV-DC1** (Windows Server 2022) : **AD DS**, **DNS**, **DHCP** (bail 6 h, pool 192.168.100.50–200, domaine **mediaschool.local**).
- **SRV-FS1** (Windows Server 2022, joint au domaine) : **serveur de fichiers (FSRM/quotas)**, **MDT/WDS**, **WSUS**.
- **CL-W10/11** (poste client joint au domaine) pour tests.

Les IP des serveurs sont fixes (hors pool). DNS client = SRV-DC1.
DHCP sur SRV-DC1 ; MDT/WDS et **WSUS** centralisés sur **SRV-FS1** (stockage).

Objectifs (complétés)

1. Déployer **AD DS + DNS + DHCP** (pool 192.168.100.50–.200, bail **6 h**).
2. Structurer l'annuaire (OU/groupes) et créer des **GPO via PowerShell** (lecteur perso, sécurité).
3. Mettre en place des **quotas** par public (FSRM sur SRV-FS1).
4. **Horaires de connexion** distincts (Administration / Profs / Élèves) et application.
5. **WSUS** : centraliser et **automatiser** les mises à jour, avec ciblage en **anneaux** (Pilote → Production).
6. **Masterisation** : capturer et déployer une image Windows **via MDT/WDS**, configurable **en UI ou PowerShell**.

Livrables (complétés)

1. Schéma logique (rôles/hostnames/IP/ports) + justification des placements (pourquoi WSUS/MDT sur SRV-FS1).

2. Arborescence AD (OU), groupes, comptes (règle de nommage).

3. **GPO** : scripts PowerShell **.ps1** (création/liaison/paramétrage) + `gpresult`.

4. **WSUS** :

    - **Si UI** : captures des étapes clés (produits/classifications, synchro, groupes Pilote/Production, règles d'approbation auto, rapport de conformité).

    - **Si PowerShell** : scripts `.ps1` (install, config, produits/classifications, synchro, approbations, ciblage) + sortie de commande/rapport.

    - Copie des paramètres GPO WSUS (modèle administratif).

5. **Masterisation** :

    - **Si UI (MDT/WDS)** : captures (installation ADK/WinPE, Deployment Share, Task Sequence, boot images, WDS, options DHCP 66/67, capture/déploiement).

    - **Si PowerShell** : scripts `.ps1` MDT/WDS (création DS, import OS, TS, génération boot, ajout WDS) **ou** workflow Sysprep + DISM (capture .wim) + déploiement.

6. Procédure de tests et résultats :

    - WSUS (détection, téléchargement, installation, redémarrage planifié, conformité Pilote→Prod).

    - Masterisation (PXE, exécution TS, jonction domaine, premier logon, GPO appliquées).

7. Analyse (1 page max) : risques, bonnes pratiques (staging updates, maintenance, image lifecycle).

Travaux à réaliser

A. Rappels AD/DNS/DHCP (inchangé, synthèse)

- Domaine **mediaschool.local** (SRV-DC1).

- DHCP : Scope `SCOPE-SALLE-INFO`, **192.168.100.50–200**, **bail 6 h**, options 003=GW, 006=DNS=SRV-DC1, 015=DNS suffix.
- AD : OU **ECOLE** → **Comptes-Utilisateurs** (Administration/Profs/Eleves), **Comptes-Ordinateurs**.
- Groupes globaux : `MS-Administration`, `MS-Profs`, `MS-Eleves`.
- SRV-FS1 : partage `\\SRV-FS1\Homes`, dossiers perso, **FSRM quotas** (Adm 10 Go, Profs 5 Go, Élèves 1 Go).

B. GPO (toujours PowerShell uniquement)

- 3 GPO par public (+ GPO domaine si nécessaire).
- Contenus attendus : lecteur H:, options sécurité (écran veille, force logoff at logon hours), etc.
- **Scripts .ps1 fournis en livrables.**

C. WSUS — Automatisation des mises à jour (UI ou PowerShell)

C1. Architecture & installation

- **Rôle WSUS** sur **SRV-FS1** (stockage local `D:\WSUS` recommandé).
- Base WID (par défaut) ou SQL si dispo (au choix, justifier).
- Synchronisation avec Microsoft Update (proxy si nécessaire).
- **Produits** : Windows 10/11, Windows Server 2022 (au minimum).
- **Classifications** : Security Updates, Critical Updates, Definition Updates, Feature Packs (justifier vos choix).

Livrable : choix Produits/Classifications + justification pédagogique.

C2. Groupes WSUS & ciblage des postes

- Créer **deux anneaux** : `WSUS-Pilote` (petit échantillon) et `WSUS-Production` (reste des postes).
- Choisir une méthode de **ciblage** :
    - **Client-side targeting** : via GPO (`Target group name`) selon OU, **recommandé**.
    - **Server-side** : affectation manuelle dans la console (toléré pour le labo).

C3. GPO Windows Update (obligatoire, configurée via GPMC)

- Paramètres **Configuration ordinateur → Modèles admin → Composants Windows → Windows Update** :
    - **Spécifier l'emplacement du service de mise à jour Microsoft** : `http://SRV-FS1:8530` (intranet WSUS) pour **détection** et **statistiques**.
    - **Configurer Mises à jour auto** : mode 4 (téléchargement auto et planification de l'installation) + planification (ex. tous les jours 12:00).
    - **Ne pas redémarrer auto si un utilisateur est connecté** (selon politique).
    - **Ciblage côté client** : `WSUS-Pilote` **ou** `WSUS-Production` selon OU.
- **Preuve d'application** : `gpresult /h` sur un poste de chaque anneau.

C4. Automatisation des approbations et de la conformité

- Mettre en place un **processus d'approbation** :
    - **Auto-approval** pour **Security/Definition** vers `WSUS-Pilote`.
    - Après validation (tests OK), **approbation vers `WSUS-Production`** (documenter la procédure : manuelle planifiée **ou** script PowerShell).
- Générer un **rapport de conformité** par groupe (captures ou export).

UI ou PowerShell : vous choisissez, mais **joignez** soit les **captures** des étapes (UI), soit les **scripts `.ps1`** (PowerShell).

C5. Tests WSUS

- Forcer la détection sur un client de chaque anneau (méthode au choix), vérifier :
    - Apparaît dans WSUS, groupe correct, état **Needed/Installed**.
    - Téléchargement/installation selon fenêtre planifiée, redémarrage le cas échéant.
- Mesurer le **délai** entre approbation Pilote et disponibilité sur Production ; commenter.

D. Masterisation — MDT/WDS (UI ou PowerShell)

D1. Pré-requis

- Installer **Windows ADK** + **WinPE add-on** sur **SRV-FS1**.
- Installer **MDT** et **WDS** sur **SRV-FS1**.
- Créer un dossier `D:\MDT` (Deployment Share).
- DHCP (SRV-DC1) :
    - Même VLAN : configurer **Option 66** (nom/IP de SRV-FS1) et **Option 67** (bootfile) :
        - BIOS/Legacy : `\Boot\x64\wdsnbp.com`
        - UEFI x64 : `\Boot\x64\wdsmgfw.efi`
    - *Ou* routeur avec **IP Helper** vers WDS.

D2. UI — Scénario demandé

1. **Créer le Deployment Share** (MDT) et **importer l'OS** (install.wim de l'ISO).
2. Créer une **Task Sequence** standard (déploiement client, jonction domaine, apps/paramètres).
3. **Update Deployment Share** pour générer les **Boot Images** (LiteTouch).
4. Ajouter les **Boot Images** dans **WDS**.

5. **Capture** : préparer un poste de référence (Sysprep & Capture via TS dédiée) → obtenir un `.wim` personnalisé.

6. **Déploiement** : démarrer **PXE** sur le client, exécuter la TS de déploiement, vérifier jonction domaine, GPO, lecteur H:, quotas.

D3. PowerShell — Scénario demandé

- Utiliser le **module MDT** :
    - Créer le **Deployment Share**, **importer** l'OS, **créer** la **Task Sequence**, **mettre à jour** le Share (génération des boot images).
- Utiliser les **cmdlets WDS** pour **ajouter les boot/install images** au serveur WDS.
- Alternative **DISM/Sysprep** :
    - `sysprep /generalize /oobe /shutdown` sur la ref,
    - **capturer** la partition avec DISM pour produire un `.wim`,
    - **déployer** via WDS (Install Image) et post-config (GPO/Domain join automatisés via unattend/MDT).

Livrables : soit **scripts** `.ps1` (MDT/WDS/ DISM), soit **captures** UI (toutes les étapes). Fournir **CustomSettings.ini** et **Bootstrap.ini** si MDT utilisé.

D4. Tests Masterisation

- **PXE** : le client boote bien sur l'image LiteTouch.
- **Déploiement complet** :
    - Jonction automatique au domaine,
    - Profil local clean (sysprep),
    - GPO appliquées (lecteur H:),
    - Drivers et apps de base présents,
    - Horloge/DNS corrects.
- **Rejouer** l'installation sur un second poste pour valider la **répétabilité**.

E. Vérifications globales (fin de TP)

1. **DHCP/DNS** : IP du pool, bail **6 h**, résolution directe/inverse OK.
2. **AD/GPO** : `gpresult` montre les GPO du public ; restrictions **horaires** effectives.
3. **FSRM** : dépassement quota impossible (preuve).
4. **WSUS** :
    - Poste **Pilote** reçoit/installe une mise à jour approuvée,
    - Migration vers **Production** validée/documentée,
    - Rapport de conformité fourni.
5. **Masterisation** : image déployée avec succès via PXE, poste opérationnel et conforme.

Questions de réflexion (ajout)

1. Quels avantages/inconvénients de **WSUS** vs **Windows Update for Business/Intune** dans un contexte on-prem d'école ?
2. Pourquoi segmenter en **anneaux Pilote/Production** ? Quels critères de promotion ?
3. Comparez **MDT/WDS (image-centré)** et **Autopilot/Intune (policy-centré)** pour un parc pédagogique.
4. Quelles **mises à jour** ne faut-il **pas** auto-approuver sans test ? Justifiez.
5. Comment maintenir votre **image de référence** (drivers, apps, cumulative updates) avec un **cycle mensuel** ?