BTS SIO · Option SISR ·
Bloc 2 « Administration des systèmes et des réseaux » · Bloc 3 « Cybersécurité des services informatiques »

Atelier Active Directory

Comptes, UGDLP, partages réseau et GPO — cas d'étude Maison des ligues - M2L (domaine m2l.lan)

SUJET ÉTUDIANT —— barème /20

info	**Comment utiliser ce document** • Les **cases jaunes** sont à remplir par vous : réponses, résultats observés, preuves. • Avancez **niveau par niveau** ; faites valider chaque niveau par le formateur (visa). • Dans tout le document, `<SERVEUR>` désigne le nom réel de votre serveur (à noter ci-dessus).

Nom et prénom	Raphaël Rosario et Théo Bricet
Groupe / date	BTS SIO SISR – atelier réalisé le 02/11/2026
Nom réel du serveur Windows Server 2022 (hostname)	WIN-IL2KT5724QT (contrôleur de domaine m2l.lan – 192.168.10.100)
Nom réel du poste Windows 11 (hostname)	CLI-THEO (le lab fournit un Windows 10 Professionnel 22H2, pas un Windows 11 – 192.168.10.10)
VMID Proxmox (serveur / poste)	VMID 104 (SRV-WIN2022) / VMID 101 (CLI-Theo)

Sommaire

1. Contexte et mission **3**
2. Infrastructure de travail **3**
3. Objectifs pédagogiques **3**
4. Déroulé et barème **4**
5. Données du projet **4**
5.1 Organisation et comptes à créer 4
5.2 Besoins d'accès (matrice métier) 5
5.3 Conventions de nommage 5
N0 — Préparer et sécuriser l'environnement **6**
N1 — Annuaire : OU, comptes et poste de travail **10**
N2 — Groupes et stratégie UGDLP **14**
N3 — Partages réseau et permissions NTFS **19**
N4 — Stratégies de groupe (GPO) **24**
N5 — Validation : tests et rapport **31**
Bonus — Défis facultatifs **37**
Annexe A — Glossaire **40**
Annexe B — Guide de diagnostic **41**
Annexe C — Grille de barème et auto-évaluation **42**

1. Contexte et mission

La **Maison des Ligues de Lorraine (M2L)** accueille les ligues sportives régionales et mutualise leurs services support. Son système d'information repose sur le domaine Active Directory **m2l.lan**, hébergé sur un serveur **Windows Server 2022**, dans l'infrastructure virtualisée **Proxmox VE** de la DSI.

La direction vient de valider une réorganisation en **quatre services** : Direction, Comptabilité, Communication et Informatique (DSI). Jusqu'à présent, tous les agents partageaient les mêmes dossiers et aucune règle de sécurité n'était appliquée aux postes de travail.

Votre mission (technicien(ne) SISR de la DSI) : structurer l'annuaire, créer les comptes, appliquer le modèle de droits **UGDLP**, publier des partages réseau sécurisés, déployer des **stratégies de groupe (GPO)**, puis **prouver par des tests** depuis un poste Windows 11 que l'ensemble fonctionne.

2. Infrastructure de travail

Élément	Rôle	Détails
Proxmox VE	Hyperviseur	Réseau LAN : pont `vmbr1` — 192.168.10.0/24
Windows Server 2022	Contrôleur de domaine m2l.lan	AD DS + DNS — 192.168.10.100 — vous y travaillez en **Administrateur du domaine**
Windows 11	Poste de test	Joint au domaine m2l.lan — 192.168.10.10 (ou DHCP selon l'état du lab)
OPNsense	Passerelle LAN / Internet	Déjà configuré — **ne pas modifier**

!

Contraintes de l'atelier

- Domaine : **m2l.lan** — nom NetBIOS : **M2L**.
- Aucun accent ni espace dans les noms d'OU, de groupes, de partages ni de logins.
- Ne pas supprimer ni modifier la `Default Domain Policy`. Ne pas toucher à OPNsense.
- Voie **graphique ou PowerShell au choix** (ou mixte) : seul le résultat est noté ; un script PowerShell propre et réutilisable est valorisé dans le critère « Méthode » de la qualité professionnelle (annexe C).

3. Objectifs pédagogiques

- Structurer un annuaire Active Directory (OU, objets, attributs) selon une logique d'exploitation.
- Appliquer le modèle **UGDLP** : Comptes → groupes **G**lobaux → groupes **D**omaine **L**ocal → **P**ermissions.
- Publier des partages SMB et sécuriser les accès avec les permissions NTFS.
- Déployer des GPO (stratégies et préférences) et comprendre leur portée, leur ordre et leur diagnostic.
- Valider une configuration par une démarche de **tests documentés**.

Compétences du référentiel BTS SIO (option SISR) mobilisées	Niveaux
Bloc 2 · Installer et configurer des éléments d'infrastructure	N1 – N4
Bloc 2 · Automatiser des tâches d'administration (PowerShell)	N1 – N4
Bloc 2 · Tester l'intégration et l'acceptation ; rédiger la documentation technique	N0, N5
Bloc 2 · Identifier, qualifier, évaluer et réagir face à un incident ou à un problème	N5, annexe B
Bloc 3 · Gérer les accès et les privilèges appropriés	N2 – N4
Bloc 3 · Identifier les menaces et mettre en œuvre les défenses appropriées	N4

4. Déroulé et barème

Niveau	Intitulé	Durée	Barème	Visa
N0	Préparer et sécuriser l'environnement	15 min	Qualité	
N1	Annuaire : OU, comptes et poste de travail	40 min	4 pts	
N2	Groupes et stratégie UGDLP	40 min	4 pts	
N3	Partages réseau et permissions NTFS	45 min	4 pts	
N4	Stratégies de groupe (GPO)	55 min	4 pts	
N5	Validation : tests et rapport	25 min	2 pts	
	Qualité professionnelle (transversal)	—	2 pts	
	Total (pauses et marge : 20 min)	**4 h**	**20 pts**	

★ **Bonus (hors barème de base)**
Cinq défis facultatifs (B1 à B5) en fin de document : ils valorisent l'appréciation finale, à hauteur de **+2 points maximum**, dans la limite de 20/20.

5. Données du projet

5.1 Organisation et comptes à créer

Mot de passe initial de **tous** les comptes : `Pa$$w0rd` —Pas de changement obligatoire à la première ouverture de session.
Saisissez noms, services et fonctions **exactement** comme dans le tableau, sans accents.

Nom complet	Login (SamAccountName)	Service	Fonction (attribut Title)
Claire Marchal	`c.marchal`	Direction	Directrice
Paul Henry	`p.henry`	Direction	Assistant de direction
Nadia Petit	`n.petit`	Comptabilite	Comptable
Karim Roux	`k.roux`	Comptabilite	Gestionnaire de paie
Lea Garnier	`l.garnier`	Communication	Chargee de communication
Theo Leroy	`t.leroy`	Communication	Community manager
Amine Benali	`a.benali`	Informatique	Administrateur systemes
Sarah Klein	`s.klein`	Informatique	Technicienne support

5.2 Besoins d’accès (matrice métier)

RW = lecture + écriture · **R** = lecture seule · **—** = aucun accès. Cette matrice est **la référence** : c’est à vous d’en déduire les groupes et les permissions.

Ressource (partage)	Direction	Comptabilité	Communication	Informatique
`DIR$ (C:\Partages\Direction)`	RW	—	—	—
`COMPTA$ (C:\Partages\Comptabilite)`	R	RW	—	—
`COM$ (C:\Partages\Communication)`	R	—	RW	—
`DSI$ (C:\Partages\Informatique)`	—	—	—	RW
`COMMUN (C:\Partages\Commun)`	RW	RW	RW	RW

5.3 Conventions de nommage

Objet	Convention	Exemple
Groupe global (GG)	`GG_<Service>`	`GG_Comptabilite`
Groupe global « tous les agents »	`GG_M2L_Tous`	`GG_M2L_Tous`
Groupe domaine local (DL)	`DL_<Ressource>_<R ou RW>`	`DL_DSI_RW`
GPO	`GPO_M2L_<Périmètre>_<Objet>`	`GPO_M2L_Postes_Securite`

N0 Préparer et sécuriser l'environnement

⏱ 15 min | Qualité

RAPPEL DE COURS

- Un **snapshot Proxmox** fige l'état d'une machine virtuelle : il permet de revenir en arrière en quelques secondes si une manipulation tourne mal. Ce n'est pas une sauvegarde : il est stocké avec la VM et disparaît avec elle.
- Un poste ne fonctionne dans le domaine que si son **DNS pointe vers le contrôleur de domaine** et que son **canal sécurisé** avec le domaine est valide.

MISSIONS

M0.1 — **Créer un point de retour avant d'agir**

Créez un snapshot de **chaque VM** (serveur et poste Windows 11) nommé `avant_atelier_ad`, **sans** la mémoire RAM. Notez le VMID de chaque VM sur la page de garde.

M0.2 — **Vérifier l'infrastructure**

Sur le serveur puis sur le poste Windows 11, contrôlez : adresses IP, serveur DNS utilisé, résolution du nom `m2l.lan` et appartenance au domaine. Sur le poste uniquement, dans PowerShell lancé en administrateur, vérifiez la validité du canal sécurisé (ce test ne s'applique pas à un contrôleur de domaine). Ouvrez une session sur le serveur en **Administrateur du domaine**.

M0.3 — **Vérifier les outils d'administration**

Sur le serveur, repérez et ouvrez : la console **Utilisateurs et ordinateurs Active Directory**, la console **Gestion des stratégies de groupe**, et une console **PowerShell en administrateur**. Vérifiez que les modules PowerShell `ActiveDirectory` et `GroupPolicy` sont disponibles.

BOÎTE À OUTILS

Domaine	Pistes
Proxmox	Onglet **Snapshots** de la VM · commande `qm snapshot` (shell Proxmox)
Réseau	`ipconfig /all` · `nslookup` · `ping` · `hostname`
Domaine	`Test-ComputerSecureChannel` · `Get-ADDomain` · `Get-CimInstance Win32_ComputerSystem`
Modules / consoles	`Get-Module -ListAvailable` · `dsa.msc` · `gpmc.msc`

POINTS DE CONTRÔLE

✓	Point de contrôle	Résultat / preuve (à compléter)
☐	Snapshots créés sur les 2 VM (noms et VMID)	Snapshot « avant_atelier_ad » (sans RAM) sur VMID 104 SRV-WIN2022 et VMID 101 CLI-Theo. Snapshots ajoutés ensuite : avant_corrections et apres_atelier_ad (figure 3).
☐	Adresse IP du serveur / adresse IP du poste Windows 11	Serveur : 192.168.10.100/24 (passerelle 192.168.10.1) / Poste : 192.168.10.10/24 – les 2 VM sur le pont LAN vmbr1
☐	Serveur DNS configuré sur le poste Windows 11	192.168.10.100 (le contrôleur de domaine) – m2l.lan est résolu en 192.168.10.100
☐	Résultat de la vérification du canal sécurisé	True – « Le canal sécurisé entre l'ordinateur local et le domaine m2l.lan fonctionne correctement » (Test-ComputerSecureChannel -Verbose)
☐	Nom NetBIOS du domaine	M2L-LAB (Get-ADDomain → NetBIOSName). Le sujet prévoyait M2L : nom choisi lors de la promotion du DC.
☐	Nombre d'OU déjà présentes dans l'annuaire avant l'atelier	0 OU créée par nous : seule l'OU par défaut « Domain Controllers » et les conteneurs (Users, Computers…)

CAPTURES D'ÉCRAN — PREUVES

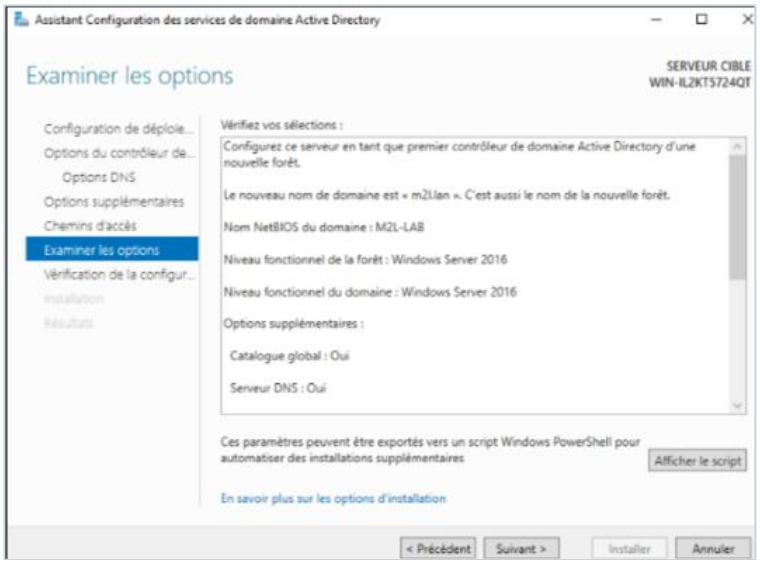


Figure 1 – Récapitulatif de la configuration de la nouvelle forêt (m2l.lan)

Aperçu des paramètres finaux : nom de domaine, nom NetBIOS (M2L-LAB), niveau fonctionnel et rôles DNS / Catalogue global.

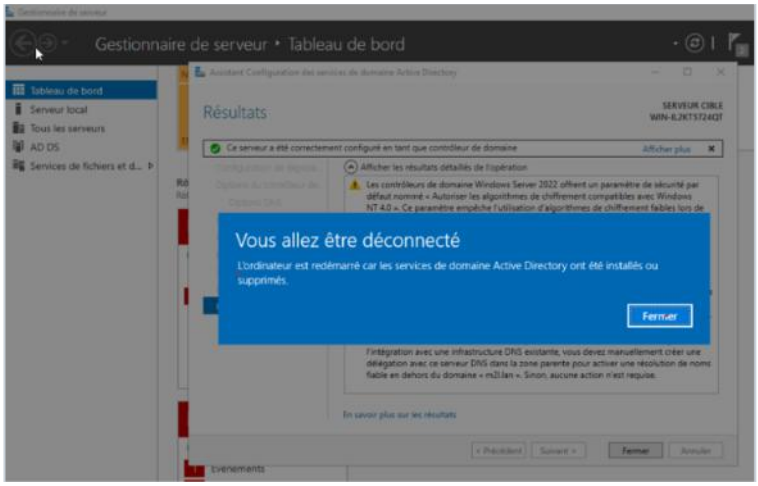


Figure 2 – Confirmation de l'installation et promotion du contrôleur de domaine

Message de fin de l'assistant AD DS confirmant la réussite de la configuration du domaine m2l.lan et le redémarrage automatique du serveur.

```
Shell Proxmox VE - noeud M2L (10.74.3.105)
root@M2L:~# qm listsnapshot 104   # SRV-WIN2022
`-> avant_atelier_ad            2026-10-28 11:44:40     no-description
 `-> avant_corrections          2026-10-29 17:14:09     Avant corrections et N3-N5 (29/10/2026)
  `-> apres_atelier_ad          2026-11-02 10:33:35     Fin atelier AD : N0-N5 + bonus B1-B5
   `-> current                                          You are here!
root@M2L:~# qm listsnapshot 101   # CLI-Theo
`-> avant_atelier_ad            2026-10-28 11:47:01     no-description
 `-> avant_corrections          2026-10-29 17:14:11     Avant corrections et N3-N5 (29/10/2026)
  `-> apres_atelier_ad          2026-11-02 10:33:37     Fin atelier AD : N0-N5 + bonus B1-B5
   `-> current                                          You are here!
```

Figure 3 – Snapshots Proxmox des deux VM (qm listsnapshot 104 / 101)

avant_atelier_ad = point de retour demandé en M0.1 ; avant_corrections et apres_atelier_ad encadrent nos corrections et la fin de l'atelier.

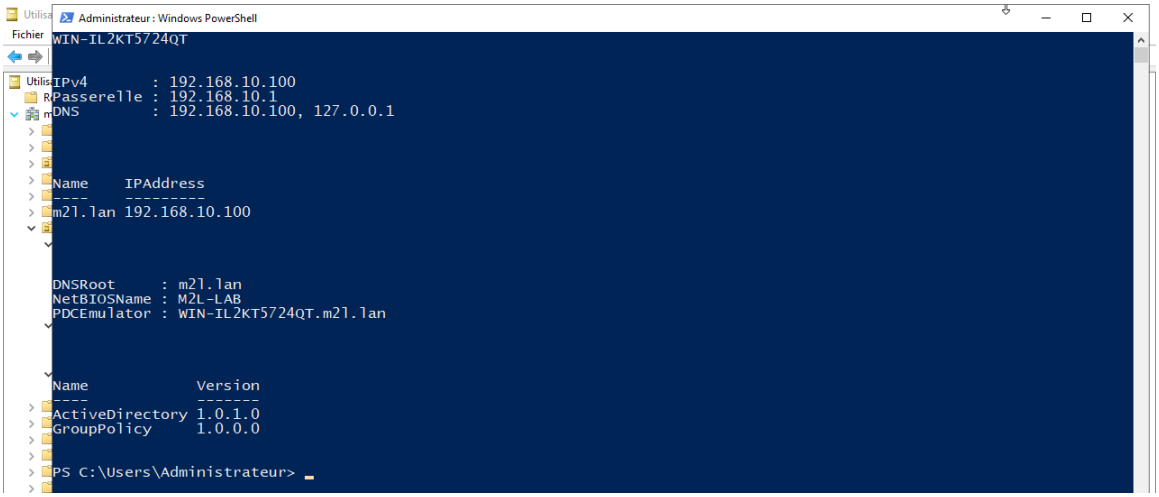


Figure 4 – Vérifications M0.2 / M0.3 sur le serveur WIN-IL2KT5724QT

IP 192.168.10.100, DNS 192.168.10.100 + 127.0.0.1, résolution de m2l.lan, nom NetBIOS M2L-LAB, modules ActiveDirectory et GroupPolicy disponibles.

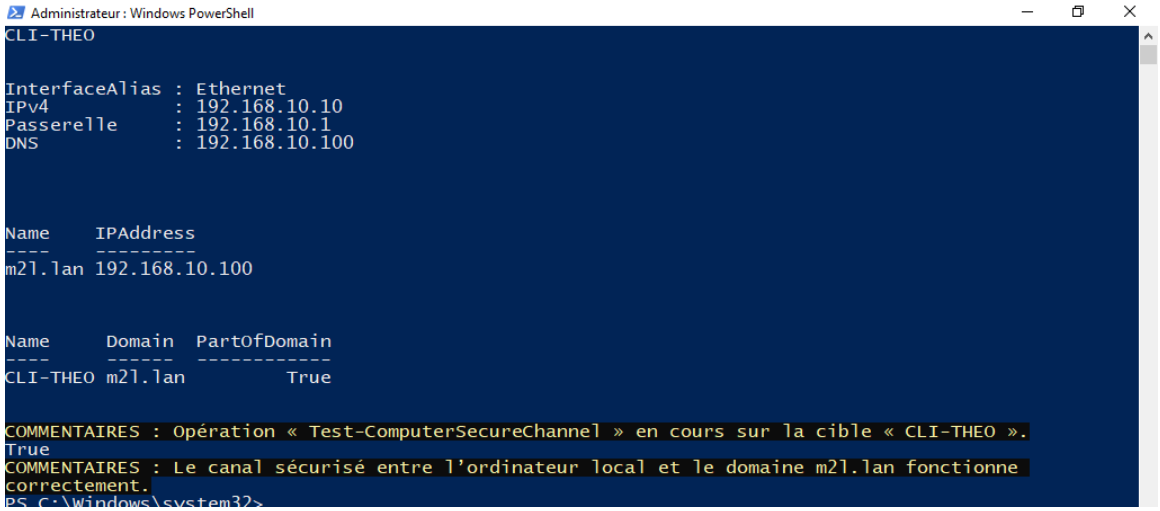


Figure 5 – Vérifications M0.2 sur le poste CLI-THEO (PowerShell administrateur)

IP 192.168.10.10, DNS 192.168.10.100, m2l.lan résolu, poste membre du domaine (PartOfDomain = True) et canal sécurisé valide (True).

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

N1 Annuaire : OU, comptes et poste de travail

⏱ 40 min | 4 pts

RAPPEL DE COURS

- Une **OU** est un conteneur administrable : on peut y **lier des GPO** et **déléguer** des droits. Les conteneurs par défaut (`CN=Users`, `CN=Computers`) ne permettent ni de lier une GPO ni de créer des sous-OU, et Microsoft déconseille d'y déléguer des droits.
- Bonne pratique : organiser **par type d'objet** (utilisateurs, groupes, ordinateurs), puis **par service**.
- **SamAccountName** : identifiant court (ancien format `M2L\login`) · **UPN** : `login@m2l.lan` (format e-mail). Le **DN** (Distinguished Name) est le chemin complet d'un objet dans l'annuaire.
- Une OU **protégée contre la suppression accidentelle** ne peut pas être supprimée tant que la protection n'est pas retirée.

MISSIONS

M1.1 Créer l'arborescence d'OU

Créez la structure ci-dessous directement sous la racine du domaine `m2l.lan`. **Toutes** les OU doivent être protégées contre la suppression accidentelle.

Arborescence attendue

```
m2l.lan
└── M2L
    ├── Utilisateurs
    │   ├── Direction
    │   ├── Comptabilite
    │   ├── Communication
    │   └── Informatique
    ├── Groupes
    │   ├── Globaux
    │   └── Domaine_Local
    └── Ordinateurs
        └── Postes
```

M1.2 Créer les 8 comptes utilisateurs

Créez les comptes du paragraphe 5.1, **chacun dans l'OU de son service** (sous `Utilisateurs`), avec :

- login = SamAccountName ; **UPN** = **`login@m2l.lan`** ;
- **prénom, nom, nom complet**, **service** (Department) et **fonction** (Title) renseignés ;
- mot de passe initial indiqué, **changement obligatoire** à la première connexion ;
- compte **activé**.

M1.3 Ranger le poste Windows 11

Le compte ordinateur du poste Windows 11 se trouve dans un conteneur par défaut. Déplacez-le dans l'OU **`Postes`**. Vous justifierez cette étape en Q4.2.

BOÎTE À OUTILS

Voie graphique	Voie PowerShell (cmdlets à explorer avec Get-Help -Examples)
Console **Utilisateurs et ordinateurs AD** (`dsa.msc`) : clic droit › Nouveau › Unité d'organisation / Utilisateur · menu Affichage › Fonctionnalités avancées	`New-ADOrganizationalUnit` · `New-ADUser` · `Get-ADComputer` · `Move-ADObject` · `Get-ADUser -SearchBase` · `Get-ADOrganizationalUnit`

✓ **Astuce de méthode**

Huit comptes identiques à créer : un tableau (`@(...)`) et une boucle `foreach` en PowerShell évitent les erreurs de saisie. Construisez-le à partir du tableau 5.1.

Mot de passe en PowerShell : écrivez-le entre guillemets simples, par ex. `ConvertTo-SecureString 'Pa$$w0rd' -AsPlainText -Force`. Entre guillemets doubles, `$$` et `$w0rd` seraient interprétés comme des variables : le mot de passe enregistré serait faux.

POINTS DE CONTRÔLE

✓	Point de contrôle	Résultat / preuve (à compléter)
☐	Nombre total d'OU sous `M2L` (racine incluse)	11 (M2L, Utilisateurs, Direction, Comptabilite, Communication, Informatique, Groupes, Globaux, Domaine_Local, Ordinateurs, Postes)
☐	Nombre d'utilisateurs dans chaque OU de service	Direction : 2 · Comptabilite : 2 · Communication : 2 · Informatique : 2 (8 comptes)
☐	DN complet du compte `c.marchal`	CN=Claire Marchal,OU=Direction,OU=Utilisateurs,OU=M2L,DC=m2l,DC=lan
☐	UPN du compte `a.benali`	a.benali@m2l.lan
☐	Protection contre la suppression accidentelle : comment l'avez-vous vérifiée ?	Console AD (Affichage › Fonctionnalités avancées) › Propriétés de l'OU › onglet Objet : case « Protéger l'objet contre une suppression accidentelle » cochée. Contrôle PowerShell : Get-ADOrganizationalUnit -Filter * -Properties ProtectedFromAccidentalDeletion → True pour les 11 OU.
☐	DN du compte ordinateur Windows 11 après déplacement	CN=CLI-THEO,OU=Postes,OU=Ordinateurs,OU=M2L,DC=m2l,DC=lan (avant le déplacement : CN=CLI-THEO,CN=Computers,DC=m2l,DC=lan – figure 10)

CAPTURES D'ÉCRAN — PREUVES

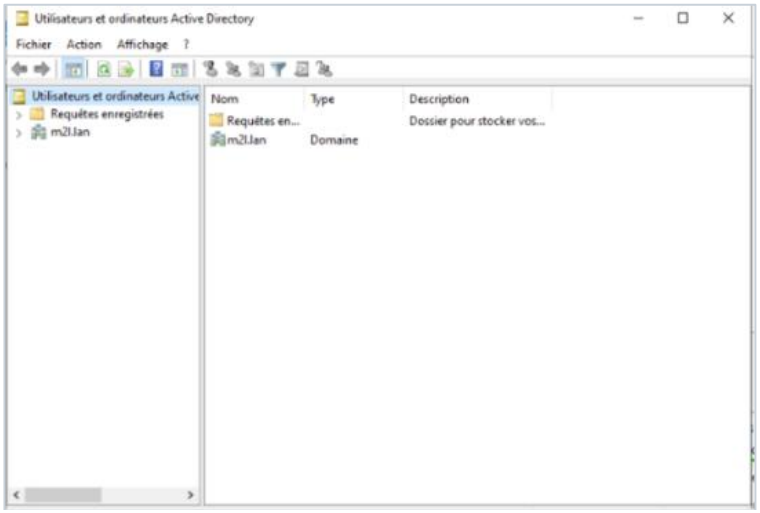


Figure 6 – Console Utilisateurs et ordinateurs Active Directory du domaine m2l.lan
Ouverture de la console d'administration et affichage de la structure par défaut du domaine.

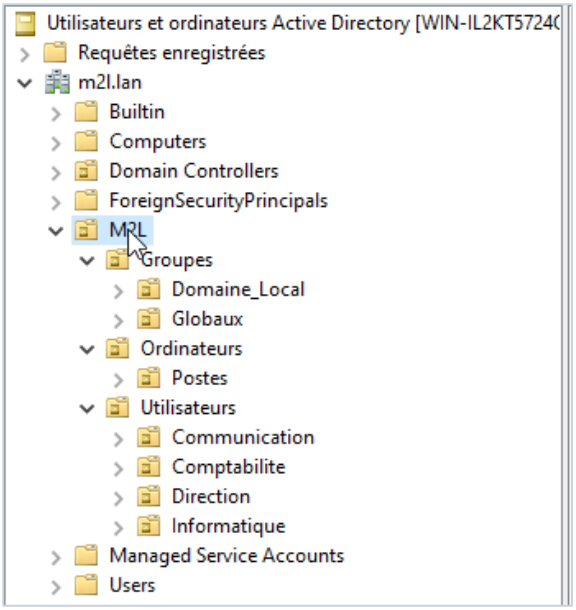


Figure 7 – Arborescence des OU du domaine m2l.lan
OU M2L : Groupes (Domaine_Local, Globaux), Ordinateurs (Postes) et Utilisateurs (4 OU de service).

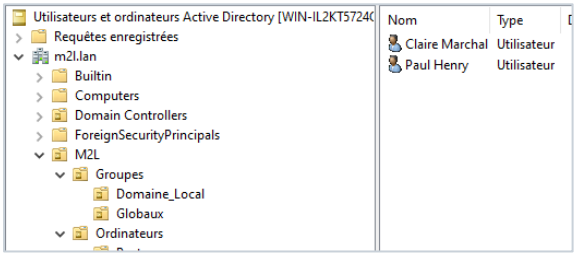


Figure 8 – Comptes de l'OU Utilisateurs\Direction
Claire Marchal (c.marchal) et Paul Henry (p.henry), créés par le script N1_Comptes.ps1.

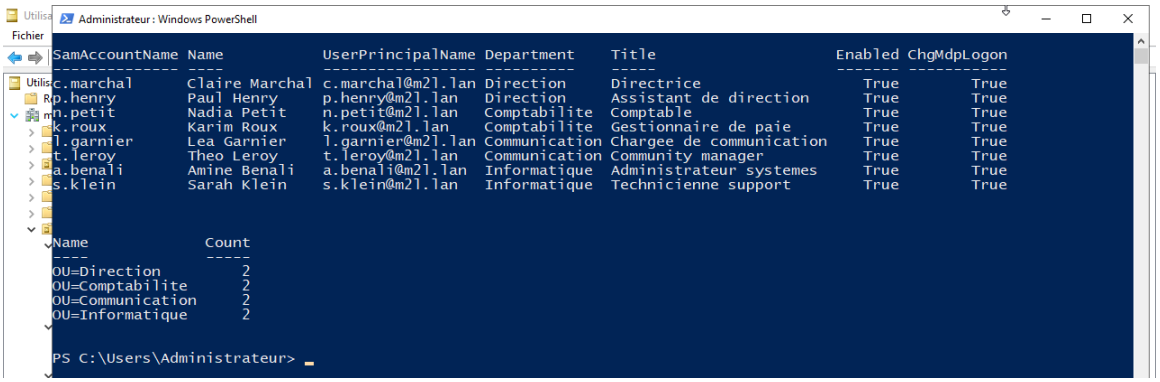


Figure 9 – Les 8 comptes créés (script PowerShell C:\Scripts\N1_Comptes.ps1)
Login, UPN, service, fonction, compte activé, changement de mot de passe obligatoire (pwdLastSet = 0) et répartition 2 comptes par OU de service.

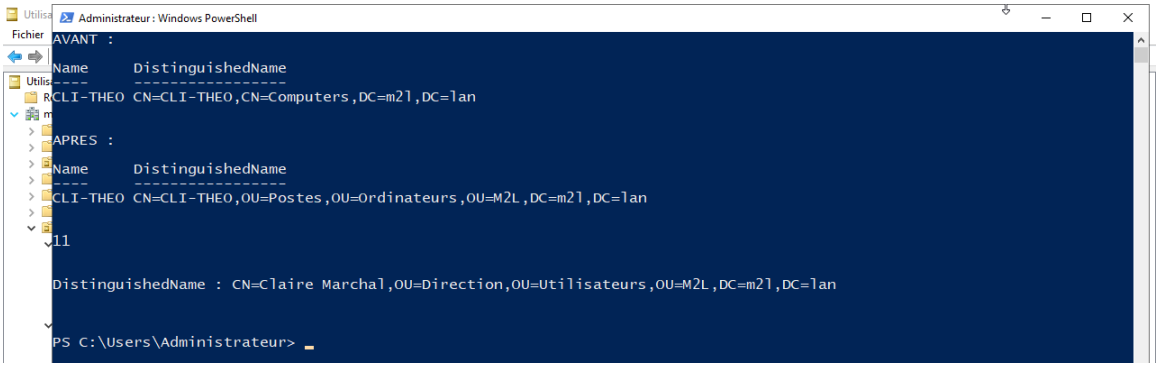


Figure 10 – M1.3 – Déplacement du poste CLI-THEO dans l'OU Postes
Avant : CN=Computers (conteneur par défaut, aucune GPO possible) ; après : OU=Postes,OU=Ordinateurs,OU=M2L. 11 OU sous M2L et DN de c.marchal.

QUESTIONS DE COMPRÉHENSION

Q1.1 — Quelle différence entre une OU et le conteneur `Users` ? Pourquoi ne pas ranger les comptes dans `Users` ?

Le conteneur Users ne permet pas d'appliquer des GPO (stratégies de groupe) ni de créer des sous-dossiers. Une OU permet d'organiser le domaine par service et d'y appliquer des GPO ciblées.

Q1.2 — Dans quels cas utilise-t-on le SamAccountName ? Dans quels cas l'UPN ?

SamAccountName (ex. M2L-LAB\c.marchal) : format court « pré-Windows 2000 » utilisé par les anciens systèmes, les commandes (net use, runas) et les accès réseau du type DOMAINE\login.

UPN (ex. c.marchal@m2l.lan) : format e-mail, unique dans la forêt, utilisé pour ouvrir une session sur les postes récents (c'est ce qu'on a utilisé en N5) et pour les services cloud (Microsoft 365, Entra ID).

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

N2 Groupes et stratégie UGDLP

⏱ 40 min | 4 pts

RAPPEL DE COURS

- **UGDLP** : les **Utilisateurs** (comptes) sont placés dans des groupes **G**lobaux (un par métier/service), qui sont placés dans des groupes **D**omaine **L**ocal (un par ressource et par niveau de droit), auxquels on attribue les **P**ermissions.
- On n'attribue **jamais** de permission directement à un utilisateur : l'arrivée ou le départ d'un agent ne doit modifier **que** son appartenance aux groupes globaux.
- Un groupe global ne contient que des comptes et des groupes globaux de son propre domaine ; un groupe domaine local est destiné à être utilisé dans les permissions des ressources du domaine.
- Les groupes peuvent être **imbriqués** : l'appartenance se propage (membership récursive).

MISSIONS

M2.1 — **Concevoir avant d'agir**

À partir de la matrice métier (5.2) et des conventions (5.3), **complétez le tableau de conception ci-dessous** avant toute création dans l'annuaire.
Un exemple est fourni. Faites-le vérifier au formateur.

Groupe domaine local (DL)	Ressource	Droit	Groupe(s) global(aux) membre(s)
`DL_DSI_RW`	DSI$	RW	GG_Informatique (exemple)
`DL_Direction_RW`	DIR$	RW	GG_Direction
`DL_Compta_RW`	COMPTA$	RW	GG_Comptabilite
`DL_Compta_R`	COMPTA$	R	GG_Direction
`DL_Com_RW`	COM$	RW	GG_Communication
`DL_Com_R`	COM$	R	GG_Direction
`DL_Commun_RW`	COMMUN	RW	GG_M2L_Tous

M2.2 — **Créer les groupes globaux**

Dans l'OU `Groupes\Globaux` : un groupe global de sécurité par service (`GG_<Service>`) contenant **les agents de ce service**, et `GG_M2L_Tous` contenant **les quatre groupes de service**.

M2.3 — **Créer les groupes domaine local**

Dans l'OU `Groupes\Domaine_Local` : les **7 groupes DL** de votre tableau de conception (portée **Domaine local**, type **Sécurité**), avec une description explicite.

M2.4 — **Appliquer l'imbrication**

Placez les groupes globaux dans les groupes domaine local conformément à votre conception.

M2.5 — **Contrôler la chaîne UGDLP**

À l'aide d'une requête **récursive**, listez **les utilisateurs qui obtiendront le droit RW sur COMMUN** puis **ceux qui obtiendront le droit R sur COMPTA$**. Vérifiez les groupes dont `c.marchal` est membre **direct**.

BOÎTE À OUTILS

Voie graphique	Voie PowerShell
Clic droit sur l'OU › Nouveau › Groupe (étendue + type) · Propriétés du groupe › onglet Membres › Ajouter	`New-ADGroup` (paramètres `-GroupScope` et `-GroupCategory`) · `Add-ADGroupMember` · `Get-ADGroupMember` (option `-Recursive`) · `Get-ADPrincipalGroupMembership`

POINTS DE CONTRÔLE

✓	Point de contrôle	Résultat / preuve (à compléter)
☐	Nombre de membres **directs** de `GG_M2L_Tous` et leur nature	4 membres directs, tous des groupes globaux de sécurité : GG_Direction, GG_Comptabilite, GG_Communication, GG_Informatique.
☐	Utilisateurs obtenus pour le droit RW sur COMMUN (liste)	Les 8 agents : a.benali, c.marchal, k.roux, l.garnier, n.petit, p.henry, s.klein, t.leroy (DL_Commun_RW ← GG_M2L_Tous ← 4 GG de service).
☐	Utilisateurs obtenus pour le droit R sur COMPTA$ (liste)	c.marchal (Claire Marchal) et p.henry (Paul Henry), via DL_Compta_R ← GG_Direction.
☐	Groupes dont `c.marchal` est membre direct	GG_Direction (+ « Utilisateurs du domaine », son groupe principal). Ses droits passent ensuite par GG_Direction → DL_Direction_RW, DL_Compta_R, DL_Com_R et GG_M2L_Tous → DL_Commun_RW.
☐	Portée et type du groupe `DL_Compta_R` (comment vérifié ?)	Portée : Domaine local · Type : Sécurité. Vérifié dans les propriétés du groupe (dsa.msc) et par Get-ADGroup DL_Compta_R (GroupScope = DomainLocal, GroupCategory = Security) – figure 18.

CAPTURES D'ÉCRAN — PREUVES

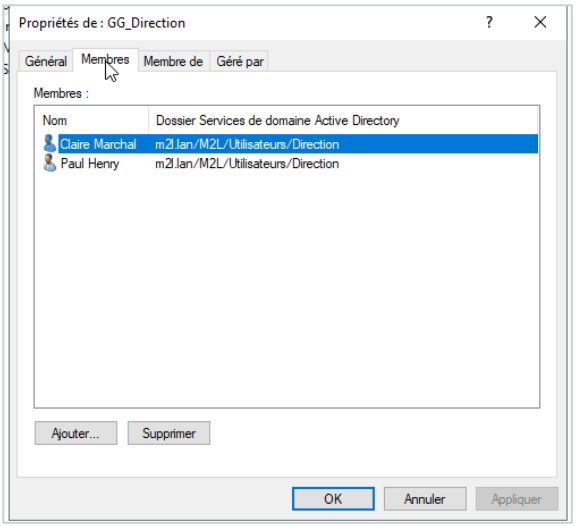


Figure 11 – Membres du groupe global GG_Direction
Claire Marchal et Paul Henry, rangés dans l'OU Utilisateurs/Direction.

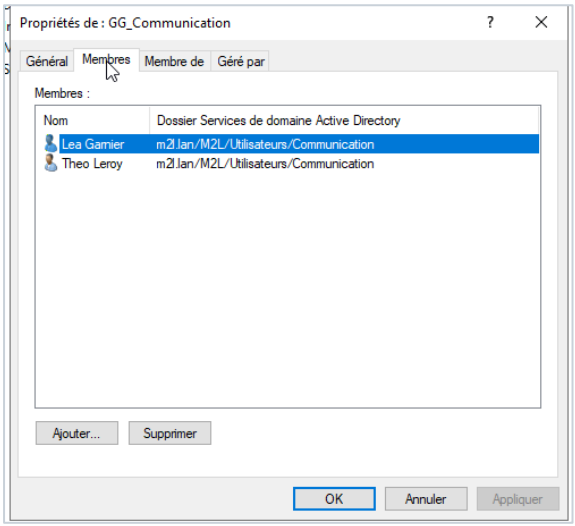


Figure 12 – Membres du groupe global GG_Communication
Lea Garnier et Theo Leroy, rangés dans l'OU Utilisateurs/Communication.

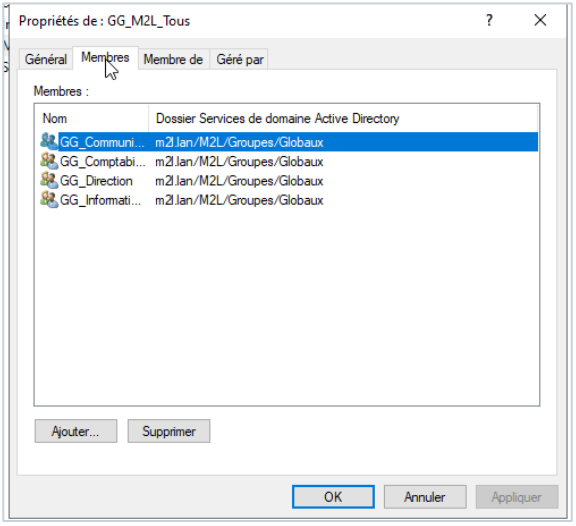


Figure 13 – Membres du groupe global GG_M2L_Tous
Les quatre groupes globaux de service sont imbriqués dans GG_M2L_Tous.

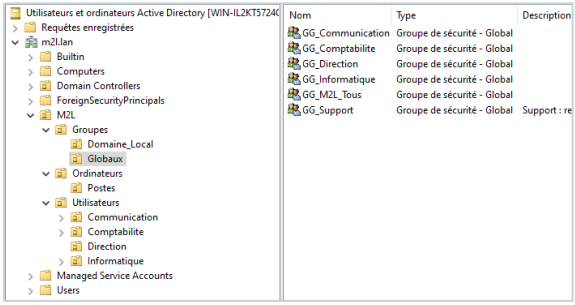


Figure 14 – Groupes globaux de l'OU Groupes\Globaux
GG_Communication, GG_Comptabilite (nom corrigé), GG_Direction, GG_Informatique, GG_M2L_Tous et GG_Support (bonus B3).

Nom	Type	Description
DL_Com_R	Groupe de sécurité - Domaine local	Lecture seule sur COM$ (C:\Partages\Communication)
DL_Com_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur COM$ (C:\Partages\Communication)
DL_Commun_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur COMMUN (C:\Partages\Commun)
DL_CommunDirection_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur COMMUN\Direction_Confidentiel
DL_Compta_R	Groupe de sécurité - Domaine local	Lecture seule sur COMPTA$ (C:\Partages\Comptabilite)
DL_Compta_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur COMPTA$ (C:\Partages\Comptabilite)
DL_Direction_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur DIR$ (C:\Partages\Direction)
DL_DSI_RW	Groupe de sécurité - Domaine local	Lecture/ecriture sur DSI$ (C:\Partages\Informatique)

Figure 15 – Groupes domaine local de l'OU Domaine_Local
Les 7 DL du sujet (portée Domaine local, type Sécurité) avec leur description, + DL_CommunDirection_RW créé pour le bonus B2.

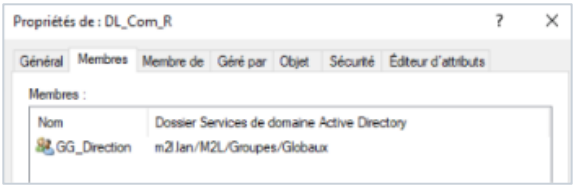


Figure 16 – Membres du groupe DL_Com_R
GG_Direction : accès en lecture de la Direction sur COM$.

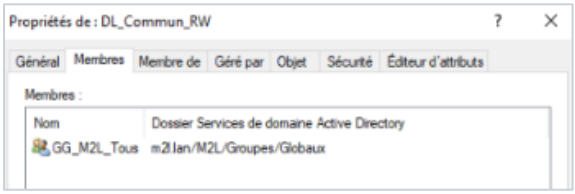


Figure 17 – Membres du groupe DL_Commun_RW
GG_M2L_Tous : accès en lecture/écriture de tous les services sur COMMUN.

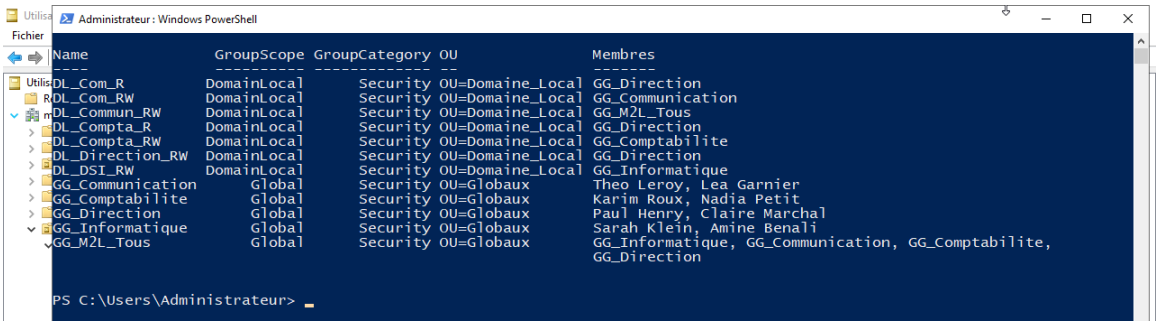


Figure 18 – Contrôle global des groupes GG / DL (portée, type, OU, membres)
Chaque DL ne contient que des groupes globaux, conformément au tableau de conception M2.1.

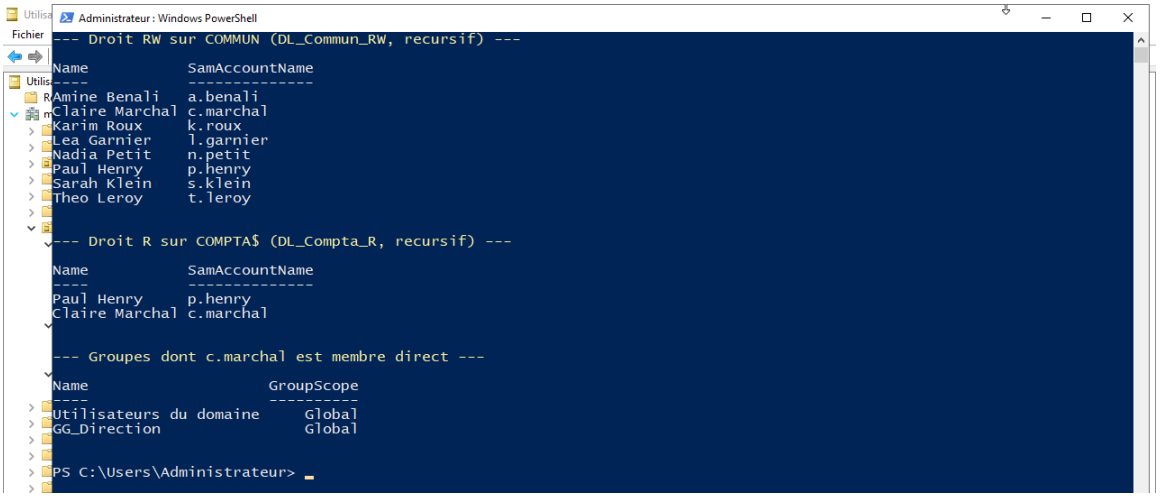


Figure 19 – M2.5 – Contrôle récursif de la chaîne UGDLP (script N2_Descriptions_Controle.ps1)
RW sur COMMUN : les 8 agents · R sur COMPTA$: p.henry et c.marchal · groupes directs de c.marchal : GG_Direction.

QUESTIONS DE COMPRÉHENSION

Q2.1 — Expliquez UGDLP avec vos mots, en prenant l'exemple de l'accès de la Direction en lecture à COMPTA$.

UGDLP permet d'attribuer des droits proprement :

1. Les utilisateurs de la Direction sont placés dans le groupe global **GG_Direction**.
2. Ce groupe global est ajouté au groupe domaine local **DL_Compta_R**.
3. La permission de lecture sur le dossier COMPTA$ est donnée à **DL_Compta_R**.

Aucun droit n'est donné directement à un utilisateur

Q2.2 — Un nouveau comptable est embauché : quelles opérations exactes réalisez-vous ? Quels objets ne touchez-vous pas ?

Opérations faites : Création de son compte dans l'OU Comptabilite et ajout au groupe global **GG_Comptabilite**.

Objets non touchés : On ne touche ni aux groupes DL_, ni aux partages, ni aux permissions NTFS. L'utilisateur hérite automatiquement de tous ses accès.

Q2.3 — Quel avantage à créer `GG_M2L_Tous` plutôt que d'ajouter les 8 utilisateurs à `DL_Commun_RW` ?

Cela respecte UGDLP et simplifie la gestion : un groupe DL reçoit des groupes globaux, pas des comptes. En imbriquant les 4 groupes de service dans GG_M2L_Tous, tout nouvel employé accède automatiquement au dossier COMMUN sans action supplémentaire.

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

N3 Partages réseau et permissions NTFS

⏱ 45 min | 4 pts

RAPPEL DE COURS

- Un accès à un dossier partagé traverse **deux niveaux de contrôle** : les autorisations de **partage** (SMB) puis les permissions **NTFS**. Le droit effectif est le **plus restrictif** des deux.
- Les permissions NTFS sont **héritées** du dossier parent. Un dossier créé à la racine d'un volume hérite de permissions génériques (groupes très larges) qui ne conviennent pas à des données sensibles.
- Un partage dont le nom finit par **$** est masqué dans la navigation réseau (il n'est **pas** protégé pour autant).
- Dans UGDLP, les ACL NTFS ne contiennent que : les **administrateurs**, **SYSTEM** et les **groupes domaine local**.

MISSIONS

Tableau de conception — avant M3.2, complétez la colonne ACL : pour chaque dossier, groupe(s) DL → droit NTFS (lecture et exécution ou modification).

Dossier	Nom du partage	ACL NTFS cible (à compléter : groupe → droit)
`C:\Partages\Direction`	`DIR$`	DL_Direction_RW → Modification
`C:\Partages\Comptabilite`	`COMPTA$`	DL_Compta_RW → Modification DL_Compta_R → Lecture et exécution
`C:\Partages\Communication`	`COM$`	DL_Com_RW → Modification DL_Com_R → Lecture et exécution
`C:\Partages\Informatique`	`DSI$`	DL_DSI_RW → Modification
`C:\Partages\Commun`	`COMMUN`	DL_Commun_RW → Modification

M3.1 Créer dossiers et partages

Créez `C:\Partages` et ses 5 sous-dossiers, puis publiez chacun sous le nom de partage du tableau. Choisissez les **autorisations de partage** de façon cohérente avec la stratégie UGDLP et **justifiez** votre choix (Q3.1).

M3.2 Sécuriser les ACL NTFS

Pour **chaque dossier** : couper l'héritage, retirer les groupes génériques (`Utilisateurs`, `Utilisateurs authentifiés`…), **conserver** Administrateurs et SYSTEM en contrôle total, puis attribuer les **groupes DL** avec le bon niveau : **lecture et exécution** pour un DL « R », **modification** pour un DL « RW ».

M3.3 Vérifier les droits effectifs

Sans ouvrir de session utilisateur, prouvez les droits de `c.marchal` sur `COMPTA$` et de `n.petit` sur `DIR$` (onglet **Accès effectif** : Propriétés › Sécurité › Avancé), qui tient compte des autorisations de partage. Conservez une capture d'écran.

BOÎTE À OUTILS

Voie graphique	Voie PowerShell / ligne de commande
Propriétés du dossier › **Partage** › Partage avancé › Autorisations · onglet **Sécurité** › Avancé › Désactiver l'héritage · onglet **Accès effectif**	`New-Item` · `New-SmbShare` · `Get-SmbShare` · `Get-SmbShareAccess` · `icacls` · `Get-Acl`

Pièges classiques

- Le groupe **Tout le monde** ne doit apparaître **nulle part**.
- Si vous oubliez de couper l'héritage, des groupes larges conservent un accès : testez-le !
- Ne donnez **jamais** de permission à un utilisateur ou à un groupe global directement.
- Un partage créé sans paramètre d'accès (`New-SmbShare`) ou par « Partage avancé » accorde par défaut **Lecture à Tout le monde** : remplacez cette entrée.

POINTS DE CONTRÔLE

✓	Point de contrôle	Résultat / preuve (à compléter)
☐	Liste des partages créés et chemins associés (sortie de commande)	COM$ → C:\Partages\Communication · COMMUN → C:\Partages\Commun · COMPTA$ → C:\Partages\Comptabilite DIR$ → C:\Partages\Direction · DSI$ → C:\Partages\Informatique (Get-SmbShare, figure 20)
☐	Autorisations de partage retenues (groupe → niveau)	Sur les 5 partages : BUILTIN\Administrateurs → Contrôle total ; AUTORITE NT\Utilisateurs authentifiés → Modifier. « Tout le monde » supprimé partout (Get-SmbShareAccess, figure 21).

☐	ACL NTFS finale d'un dossier de service (sortie `icacls` ou capture)	`icacls C:\Partages\Comptabilite (héritage coupé) :`
		`M2L-LAB\DL_Compta_R:(OI)(CI)(RX)`
		`M2L-LAB\DL_Compta_RW:(OI)(CI)(M)`
		`AUTORITE NT\Système:(OI)(CI)(F)`
		`BUILTIN\Administrateurs:(OI)(CI)(F)`

☐	Droits effectifs de `c.marchal` sur `COMPTA$`	Lecture seule : parcours, liste du dossier, lecture des attributs et des autorisations accordés ; création, écriture et suppression refusées (« limité par : Autorisations de fichiers »). Droit obtenu via GG_Direction → DL_Compta_R (RX) – figure 24.
☐	Droits effectifs de `n.petit` sur `DIR$`	Aucun accès : toutes les autorisations sont refusées (« limité par : Autorisations de fichiers ») car n.petit n'appartient à aucun groupe présent dans l'ACL de C:\Partages\Direction – figure 25.

CAPTURES D'ÉCRAN — PREUVES

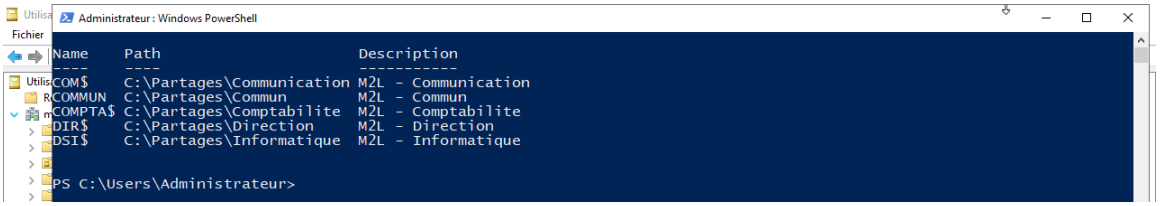


Figure 20 – M3.1 – Création des dossiers et des partages (script C:\Scripts\N3_Partages.ps1)
Les 5 partages et leur chemin ; les noms terminés par $ sont masqués dans la navigation réseau.

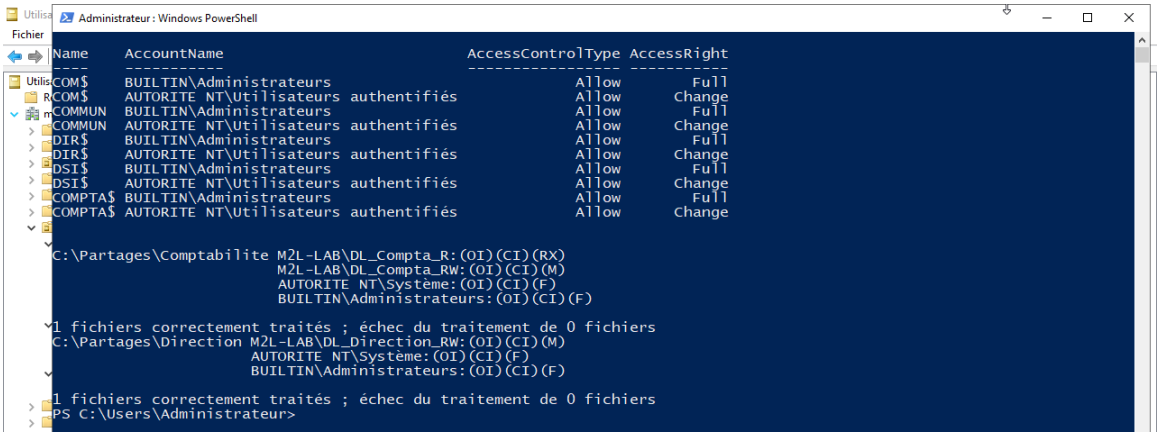


Figure 21 – Autorisations de partage et ACL NTFS finales

Partages : Administrateurs (Full) + Utilisateurs authentifiés (Change). NTFS de Comptabilite et Direction : héritage coupé, uniquement Admins, SYSTEM et groupes DL.

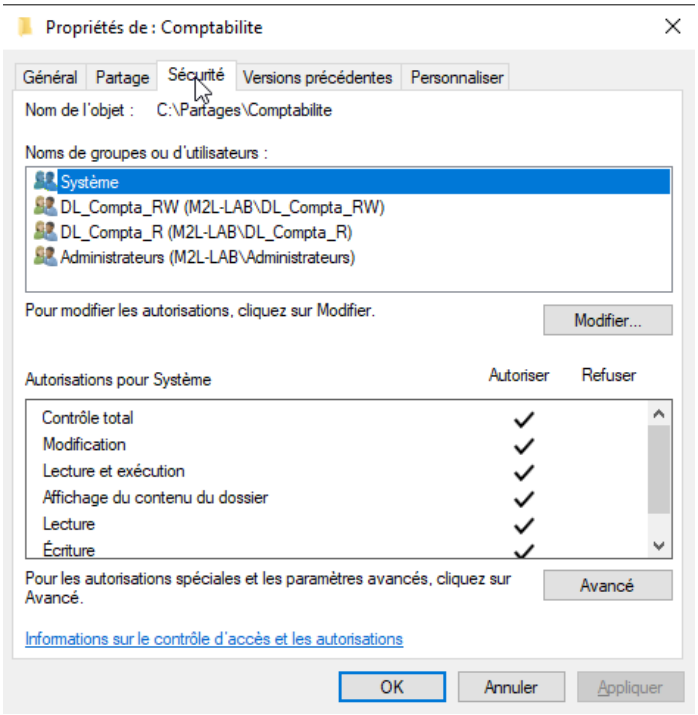


Figure 22 – Onglet Sécurité de C:\Partages\Comptabilite

Système, DL_Compta_RW, DL_Compta_R et Administrateurs : aucun groupe générique, aucun utilisateur ni GG.

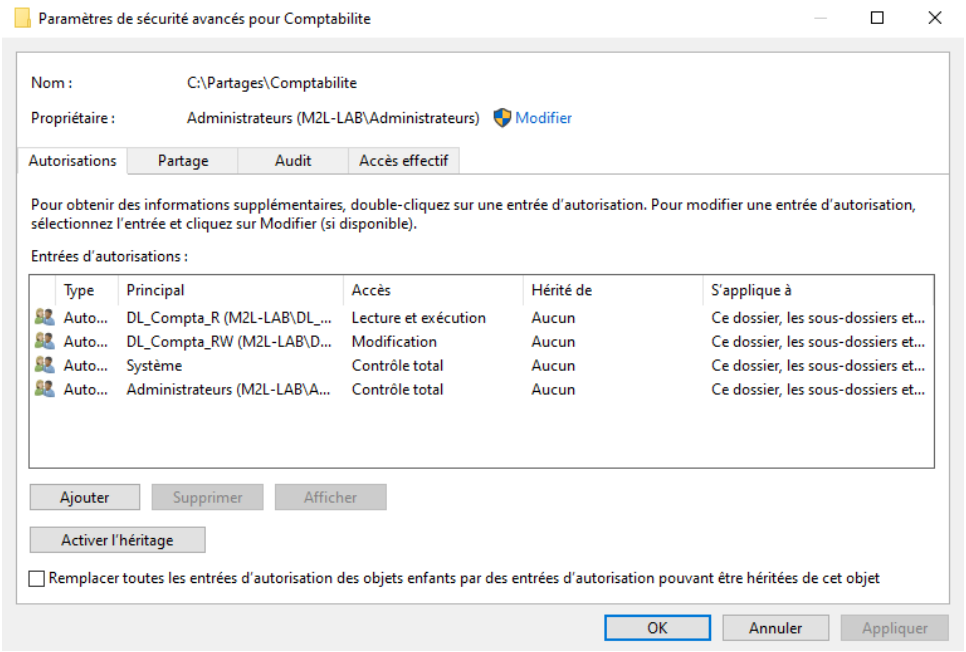


Figure 23 – Paramètres de sécurité avancés – héritage désactivé

Les 4 entrées sont « Hérité de : Aucun » : l'héritage de C:\ a bien été coupé.

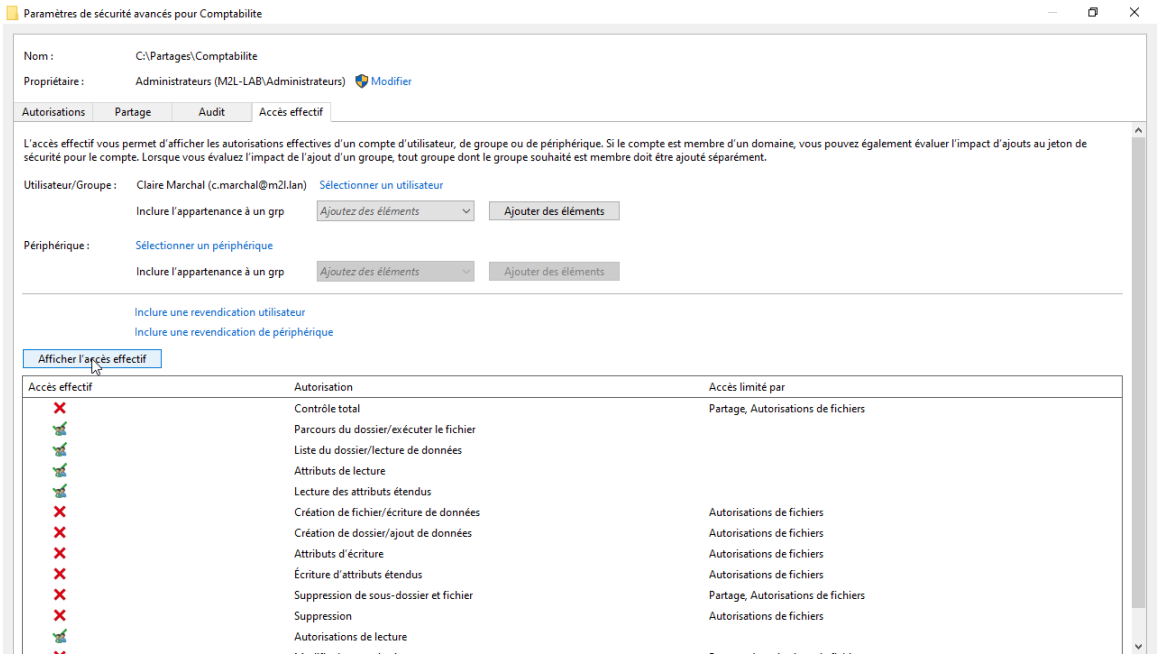


Figure 24 – M3.3 – Accès effectif de c.marchal sur COMPTA$

Lecture seulement : l'écriture et la suppression sont limitées par les autorisations de fichiers (DL_Compta_R = RX).

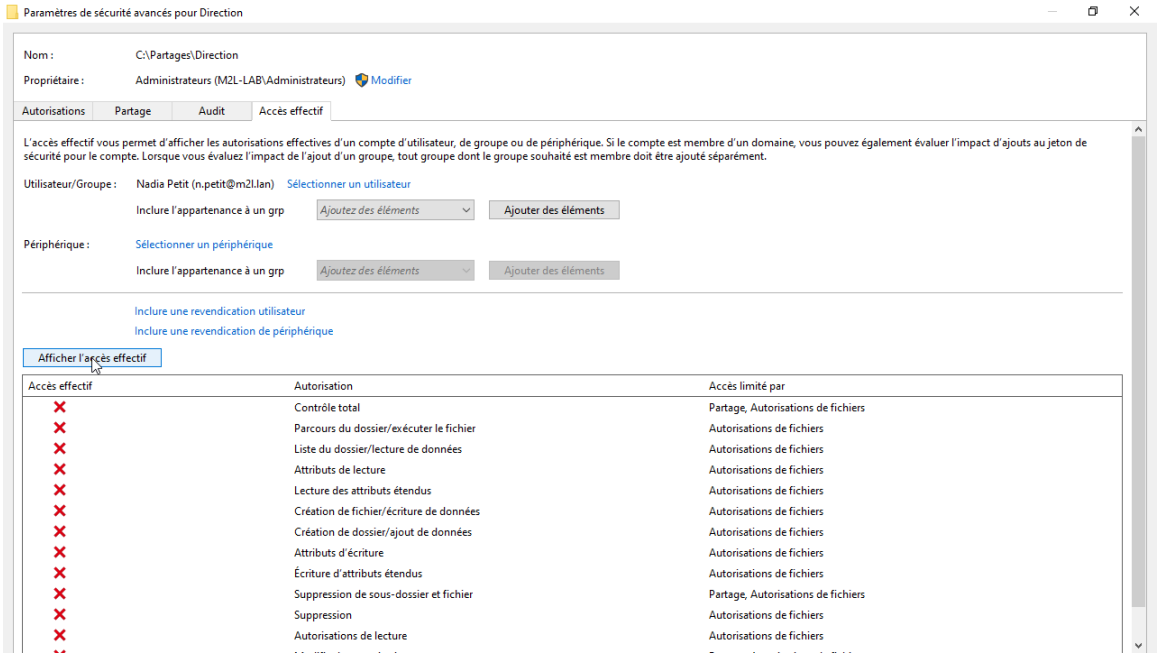


Figure 25 – M3.3 – Accès effectif de n.petit sur DIR$

Toutes les autorisations sont refusées : n.petit (Comptabilité) n'a aucun droit sur le dossier de la Direction.

QUESTIONS DE COMPRÉHENSION

Q3.1 — Quelles autorisations de partage avez-vous choisies et pourquoi ? Que se passe-t-il si partage et NTFS divergent ?

Autorisations de partage : Administrateurs → Contrôle total et Utilisateurs authentifiés → Modifier, « Tout le monde » supprimé. Le partage reste volontairement large (non bloquant) et c'est NTFS, avec les groupes DL, qui fait le filtrage fin : on n'a ainsi qu'un seul endroit à maintenir.

Si partage et NTFS divergent, le droit effectif est le plus restrictif des deux : par exemple partage en Lecture + NTFS en Modification = lecture seule à travers le réseau ; partage en Modifier + NTFS en Lecture et exécution = lecture seule aussi.

Q3.2 — Pourquoi attribuer le droit de lecture de la Direction sur COMPTA$ au groupe `DL_Compta_R` plutôt qu'à `GG_Direction` directement ?

Dans UGDLP, les permissions ne sont données qu'aux groupes domaine local, qui représentent « une ressource + un niveau de droit ». DL_Compta_R se lit tout seul (lecture sur COMPTA$) et l'ACL ne bouge plus jamais.

Si demain un auditeur ou un autre service doit lire COMPTA$, on ajoute simplement son groupe global dans DL_Compta_R, sans toucher au dossier. Les GG restent des groupes « métier » réutilisables (et un DL peut aussi recevoir des GG d'autres domaines approuvés).

Q3.3 — Le suffixe $ rend-il un partage sûr ? Justifiez.

Non. Le $ masque seulement le partage dans la navigation réseau (Voisinage réseau, net view) ; quiconque connaît le nom peut taper \\WIN-IL2KT5724QT\DIR$ et y accéder si ses droits le permettent.

La sécurité repose uniquement sur les autorisations de partage et NTFS (vérifiées en N3 et N5 : n.petit reçoit un refus sur DIR$). Le $ est une discrétion, pas une protection ; l'ABE (bonus B2) va plus loin en cachant les dossiers non autorisés.

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

N4 Stratégies de groupe (GPO)

⏱ 55 min | 4 pts

RAPPEL DE COURS

- Une GPO est un **objet** qui ne s'applique qu'une fois **liée** à un site, au domaine ou à une OU. Ordre d'application : **L**ocale → **S**ite → **D**omaine → **OU** (la plus proche de l'objet gagne), sauf option « Appliqué ».
- Une GPO contient une **configuration ordinateur** (appliquée au démarrage, selon l'OU de l'**ordinateur**) et une **configuration utilisateur** (appliquée à l'ouverture de session, selon l'OU de l'**utilisateur**).
- Les **stratégies de comptes** (mots de passe, verrouillage) des comptes de domaine ne sont prises en compte que si la GPO est liée **à la racine du domaine**.
- **Préférences** (GPP) : paramètres modifiables par l'utilisateur ou ciblables (ex. lecteurs réseau avec ciblage par groupe). **Stratégies** : paramètres imposés.
- Diagnostic : `gpupdate /force`, `gpresult`, rapports de GPO.

MISSIONS

M4.1 — GPO_M2L_Comptes_MDP — mots de passe et verrouillage

Créez cette GPO, **liez-la au bon niveau** (justifiez : Q4.1) en **position 1 de l'ordre des liens** (devant la Default Domain Policy), et configurez :

Paramètre	Valeur
Longueur minimale du mot de passe	10 caractères
Exigences de complexité	Activées
Durée de vie maximale / minimale	90 jours / 1 jour
Historique des mots de passe	5 mots de passe mémorisés
Seuil de verrouillage du compte	5 tentatives invalides
Durée de verrouillage / réinitialisation du compteur	15 minutes / 15 minutes

M4.2 — GPO_M2L_Utilisateurs_Bureau — environnement de travail

À lier sur l'OU `Utilisateurs` (tous les services) :

- **fond d'écran** imposé : `\\m2l.lan\NETLOGON\m2l_fond.jpg` (fichier déjà déposé par le formateur) ;
- lecteur **K:** vers `\\<SERVEUR>\COMMUN` pour **tous** ;
- lecteur **S:** vers le **partage du service** de l'utilisateur : un seul élément par service, **ciblé** sur le groupe global du service.

M4.3 — GPO_M2L_Utilisateurs_Restrictions — limiter les usages

Pour la **Direction, la Comptabilité et la Communication — mais pas l'Informatique** : interdire l'accès au **Panneau de configuration / Paramètres** et à l'**invite de commandes** (sans bloquer les scripts de connexion).

M4.4 — GPO_M2L_Postes_Securite — sécuriser les postes

Pour les **ordinateurs** du parc (OU `Postes`) : verrouillage de la session après **10 minutes** d'inactivité et **blocage de tous les supports de stockage amovibles**.

M4.5 — Contrôler l'application des GPO

Depuis le poste Windows 11 : forcez l'actualisation, listez les GPO appliquées pour un utilisateur et pour l'ordinateur, générez un **rapport HTML** de résultat de stratégie, et contrôlez les lecteurs réseau obtenus. L'invite de commandes étant bloquée pour la plupart des agents (M4.3), lancez `gpresult` depuis une console ouverte en administrateur sur le poste (options `/scope` et `/user`).

BOÎTE À OUTILS

Voie graphique	Voie PowerShell / ligne de commande
Gestion des stratégies de groupe (`gpmc.msc`) : Objets de stratégie de groupe › Nouveau · clic droit sur l'OU › Lier un objet GPO existant · Modifier › filtre sur les paramètres · Préférences › Paramètres Windows › Mappages de lecteurs	`New-GPO` · `New-GPLink` · `Set-GPRegistryValue` · `Get-GPInheritance` · `Get-GPOReport` · `Get-ADDefaultDomainPasswordPolicy` · sur le poste : `gpupdate /force` · `gpresult /r` · `gpresult /h` · `net use`

! **À savoir**

- Une stratégie **utilisateur** nécessite une **nouvelle ouverture de session** ; une stratégie **ordinateur** nécessite `gpupdate` puis parfois un **redémarrage**.
- Pour vos tests de mot de passe, rappelez-vous que le **verrouillage** s'applique aussi à vos essais : 5 erreurs = compte bloqué 15 minutes.
- La **première ouverture de session** d'un agent impose le changement de mot de passe : réalisez-y le test du mot de passe faible (Rapport 2), même si elle a lieu dès le N4 ; la durée de vie minimale (1 jour) bloquera ensuite tout nouveau changement.

POINTS DE CONTRÔLE

✓	Point de contrôle	Résultat / preuve (à compléter)
☐	Niveau et ordre de lien de `GPO_M2L_Comptes_MDP`	Liée à la racine du domaine m2l.lan, ordre de lien 1 (Default Domain Policy en 2), lien activé, non « Appliqué » – figure 27.
☐	Politique effective lue sur le domaine (valeurs obtenues)	Get-ADDefaultDomainPasswordPolicy : longueur 10, complexité True, durée max 90 j / min 1 j, historique 5, seuil 5, verrouillage 15 min, réinitialisation du compteur 15 min.
☐	GPO liées à chaque OU (sortie `Get-GPInheritance` ou capture GPMC)	Domaine : GPO_M2L_Comptes_MDP (1), Default Domain Policy (2) · OU Utilisateurs : GPO_M2L_Utilisateurs_Bureau OU Direction / Comptabilite / Communication : GPO_M2L_Utilisateurs_Restrictions · OU Informatique : aucune · OU Postes : GPO_M2L_Postes_Securite (figure 29) Après le bonus B5 : Restrictions n'a plus qu'un lien, sur l'OU Utilisateurs, avec refus pour GG_Informatique.
☐	GPO utilisateur appliquées à `c.marchal` (`gpresult`)	gpresult /r /scope user (session de c.marchal) : CN=Claire Marchal,OU=Direction,… → GPO_M2L_Utilisateurs_Restrictions, GPO_M2L_Utilisateurs_Bureau.
☐	GPO ordinateur appliquées au poste Windows 11	gpresult /scope computer /r (console administrateur sur CLI-THEO) : GPO_M2L_Postes_Securite, GPO_M2L_Comptes_MDP, Default Domain Policy.
☐	Lecteurs réseau obtenus par `c.marchal` et par `a.benali`	c.marchal : K: → \\WIN-IL2KT5724QT\COMMUN et S: → \\WIN-IL2KT5724QT\DIR$ · a.benali : K: → COMMUN et S: → \\WIN-IL2KT5724QT\DSI$

CAPTURES D'ÉCRAN — PREUVES

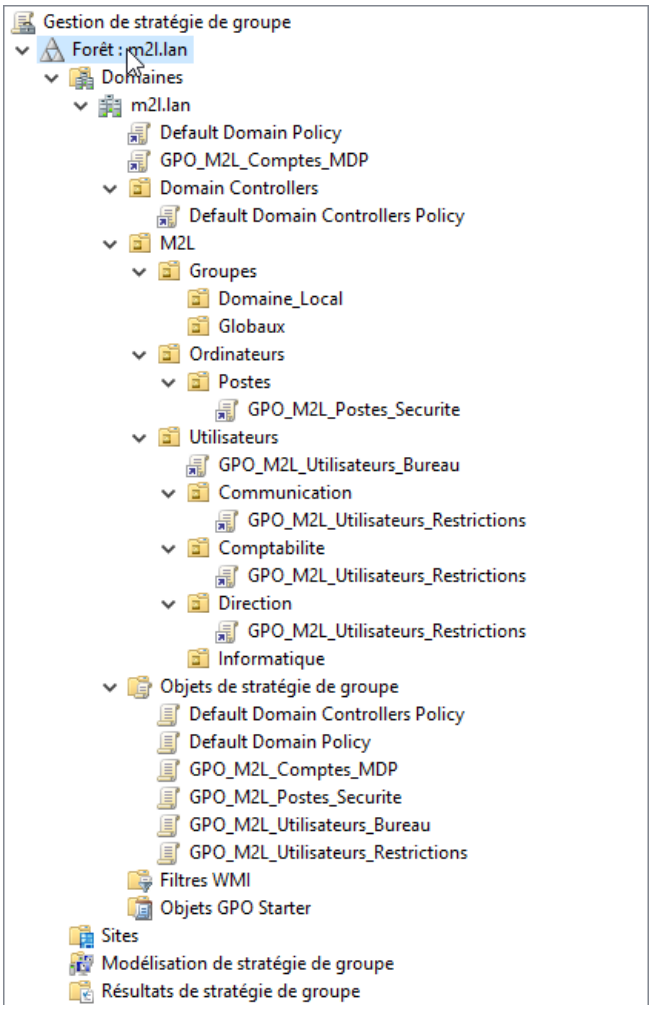


Figure 26 – Console GPMC : les 4 GPO M2L et leurs liens

Comptes_MDP sur le domaine, Postes_Securite sur Postes, Bureau sur Utilisateurs, Restrictions sur Communication, Comptabilite et Direction (Informatique exclue).

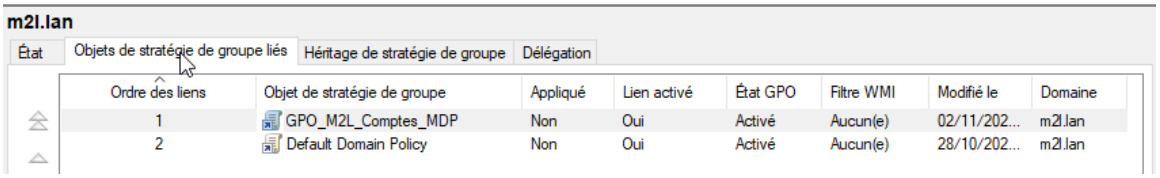


Figure 27 – M4.1 – Ordre des liens sur le domaine m2l.lan

GPO_M2L_Comptes_MDP en position 1, devant la Default Domain Policy (non modifiée).



Figure 28 – Politique de mots de passe effective sur le domaine

Valeurs lues avec Get-ADDefaultDomainPasswordPolicy après gpupdate : conformes au tableau M4.1.

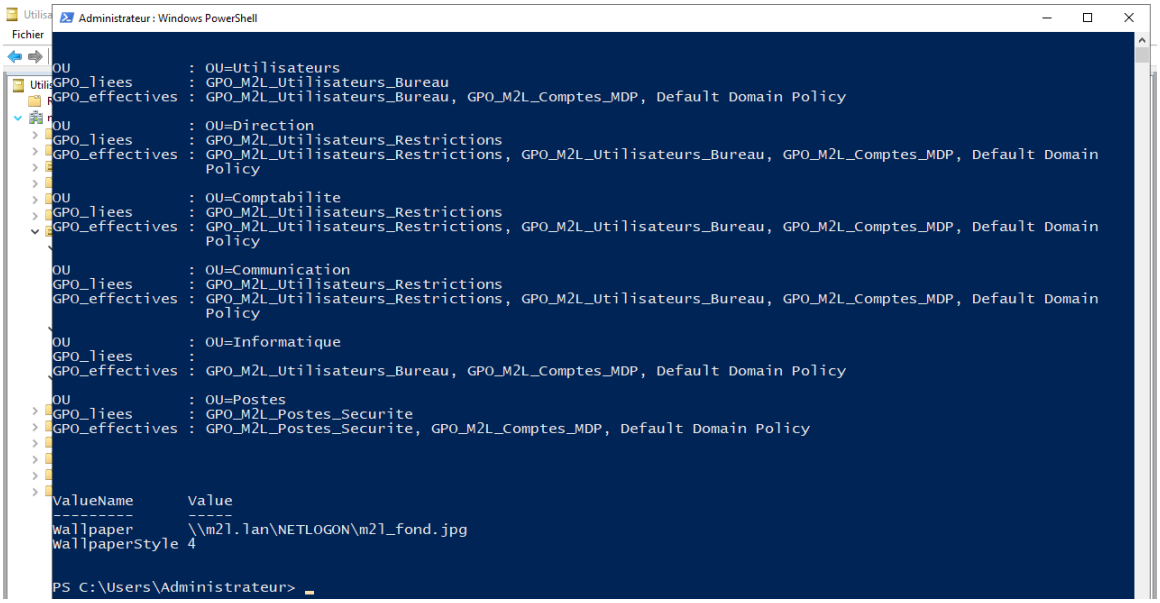


Figure 29 – GPO liées et GPO effectives par OU (Get-GPInheritance)
Valeur du fond d'écran imposé : \\m2l.lan\NETLOGON\m2l_fond.jpg (style Remplir).

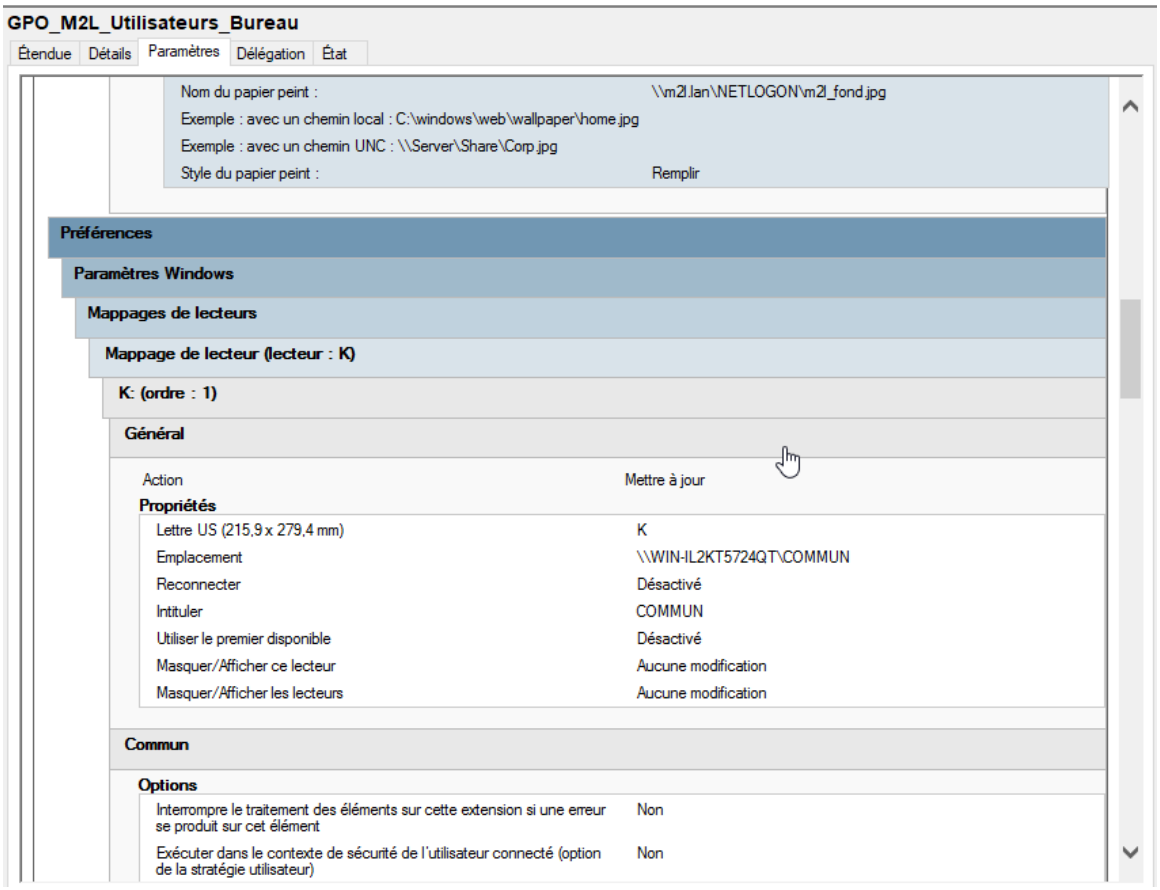


Figure 30 – M4.2 – GPO Bureau : fond d'écran et mappage du lecteur K:
Préférences › Mappages de lecteurs : K: → \\WIN-IL2KT5724QT\COMMUN pour tous les utilisateurs.

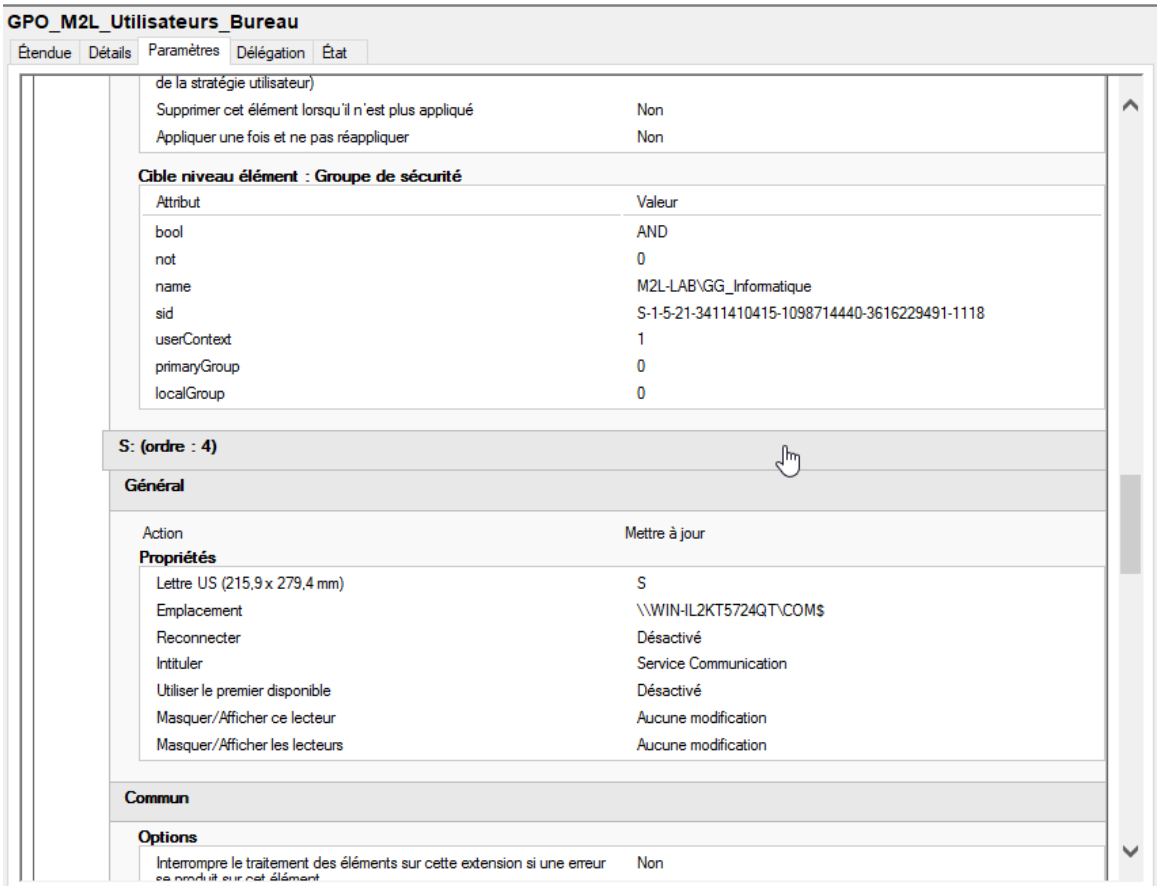


Figure 31 – M4.2 – Lecteur S: avec ciblage au niveau de l'élément

Un élément S: par service, ciblé sur le groupe global (ici GG_Informatique → DSI$, et S: → COM$ pour GG_Communication).



Figure 32 – M4.4 / M4.5 – GPO ordinateur appliquées à CLI-THEO

gpresult /scope computer : GPO_M2L_Postes_Securite ; InactivityTimeoutSecs = 600 et Deny_All = 1 dans le registre.

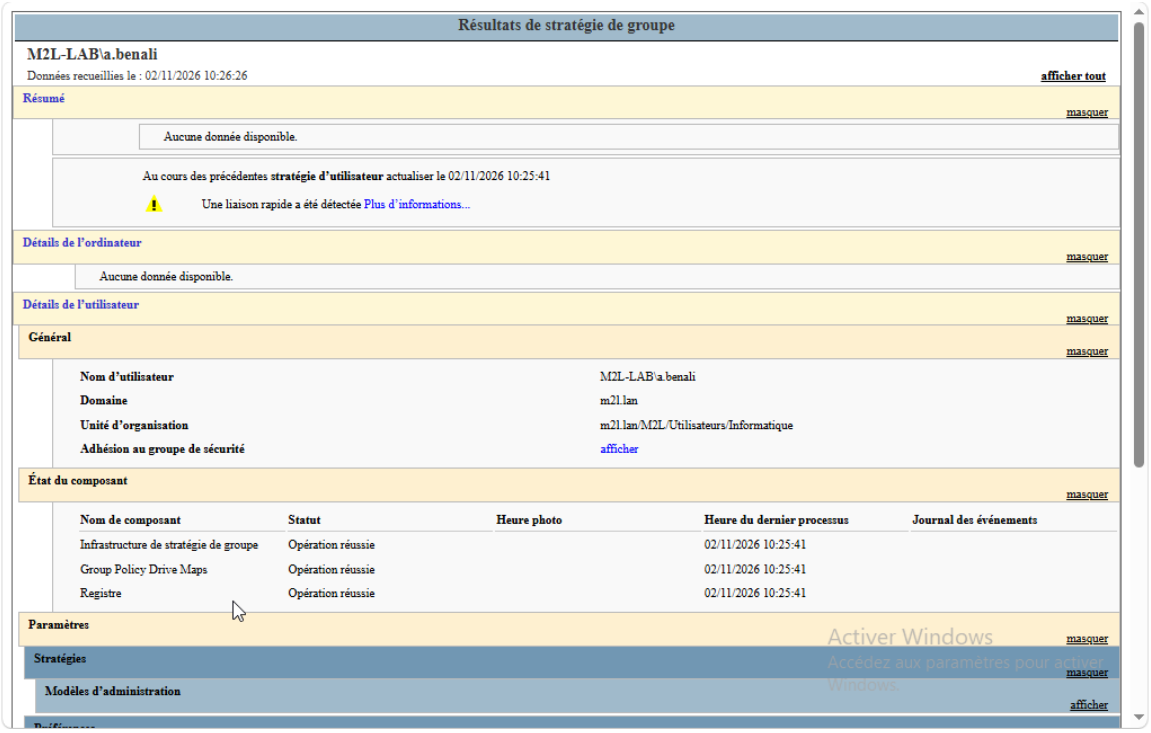


Figure 33 – M4.5 – Rapport HTML de résultat de stratégie (gpresult /h)
Rapport de a.benali : extensions Drive Maps et Registre traitées avec succès.

QUESTIONS DE COMPRÉHENSION

Q4.1 — Pourquoi la GPO de mots de passe doit-elle être liée au domaine et pas à l'OU `Utilisateurs` ?

Les stratégies de comptes (mot de passe, verrouillage) des comptes du domaine sont lues uniquement par les contrôleurs de domaine, dans les GPO liées à la racine du domaine : il n'y a qu'une politique de mots de passe par domaine.

Liée à l'OU Utilisateurs, la GPO ne s'appliquerait qu'aux comptes locaux des ordinateurs de cette OU (aucun ici) : elle n'aurait aucun effet sur les comptes AD. Pour une politique différente par groupe, on utilise un PSO (bonus B1).

Q4.2 — Pourquoi la GPO de sécurité des postes est-elle liée à l'OU `Postes` et non à une OU d'utilisateurs ? (lien avec M1.3)

Les paramètres de « Configuration ordinateur » (verrouillage après inactivité, supports amovibles) s'appliquent selon l'OU où se trouve l'objet ordinateur, au démarrage et au rafraîchissement. Liée à une OU d'utilisateurs, cette partie serait ignorée (sauf bouclage).

Lien avec M1.3 : le poste était dans CN=Computers, un conteneur où l'on ne peut pas lier de GPO. Il a fallu le déplacer dans OU=Postes pour qu'il reçoive GPO_M2L_Postes_Securite (vérifié par gpresult /scope computer).

Q4.3 — Bloquer `cmd.exe` empêche-t-il un utilisateur d'exécuter des commandes ? Quelles mesures complémentaires proposeriez-vous ?

Non. DisableCMD = 2 bloque seulement cmd.exe (les scripts de connexion restent autorisés). On l'a constaté en N5 : les agents bloqués pouvaient toujours lancer PowerShell, et d'autres moyens existent (PowerShell ISE, wscript/cscript, Gestionnaire des tâches › Exécuter, macros Office…).

Mesures complémentaires : AppLocker ou WDAC pour n'autoriser que les applications métier (et bloquer powershell.exe pour les non-admins), mode de langage contraint PowerShell, désactivation de Windows Script Host, pas de droits d'administrateur local (moindre privilège), journalisation PowerShell (Script Block Logging) remontée dans un SIEM.

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

N5 Validation : tests et rapport — ⏱ 25 min — 2 pts

Un administrateur ne livre pas une configuration sans **preuves de fonctionnement**.
Depuis le poste **Windows 11**, ouvrez une session avec chacun des 4 utilisateurs de test et renseignez les tableaux.

Procédure

- Première connexion de chaque utilisateur (en N4 ou en N5) : le changement de mot de passe est imposé. **Testez d'abord un mot de passe trop faible** (noter le message), puis un mot de passe conforme à la politique.
- Pour chaque partage, ouvrez `\\<SERVEUR>\<PARTAGE>` dans l'Explorateur, essayez de **lire**, puis de **créer** un fichier `test.txt`.
- Notation : **RW** (lecture + écriture) · **R** (lecture seule) · ✗ (accès refusé).

RAPPORT 1 — ACCÈS AUX PARTAGES (RÉSULTATS OBSERVÉS)

Utilisateur	DIR$	COMPTA$	COM$	DSI$	COMMUN
c.marchal (Direction)	RW	R	R	✗	RW
n.petit (Comptabilité)	✗	RW	✗	✗	RW
l.garnier (Communication)	✗	✗	RW	✗	RW
a.benali (Informatique)	✗	✗	✗	RW	RW

RAPPORT 2 — EFFETS DES GPO (OUI / NON, OU VALEUR OBSERVÉE)

Test	c.marchal	n.petit	l.garnier	a.benali
Fond d'écran M2L appliqué	Oui	Oui	Oui	Oui
Lecteur K: présent	Oui (COMMUN)	Oui (COMMUN)	Oui (COMMUN)	Oui (COMMUN)
Lecteur S: présent → vers quel partage ?	Oui → DIR$	Oui → COMPTA$	Oui → COM$	Oui → DSI$
Panneau de configuration bloqué	Oui	Oui	Oui	Non (DSI exclue)
Invite de commandes bloquée	Oui	Oui	Oui	Non (DSI exclue)
Mot de passe faible refusé (message)	Oui – message de la figure 34	Oui (même message)	Oui (même message)	Oui (même message) ; PSO DSI : 14 car. minimum (B1)

RAPPORT 3 — PARAMÈTRES DE L'ORDINATEUR

Test (compte administrateur sur le poste)	Résultat observé
Valeur d'inactivité de l'ordinateur appliquée (secondes) — où l'avez-vous lue ?	600 secondes (10 min) : HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System › InactivityTimeoutSecs. Constaté aussi en pratique : la session s'est verrouillée seule après 10 min sans activité.
Blocage des supports amovibles : preuve (clé de registre, gpresult…)	HKLM\Software\Policies\Microsoft\Windows\RemovableStorageDevices › Deny_All = 1, et GPO_M2L_Postes_Securite listée dans gpresult /scope computer (figure 32).

Analyse — Un test a-t-il échoué ? Quelle en était la cause et comment l'avez-vous corrigé ? (si aucun échec : quel test vous a paru le plus délicat et pourquoi ?)

Oui, trois tests ont échoué au premier essai :

1) Poste hors domaine : CLI-THEO était encore en WORKGROUP, sur vmbr0 (réseau de l'école) et avec 2 h de décalage horaire (bloquant pour Kerberos). Diagnostic : Get-CimInstance Win32_ComputerSystem, ipconfig. Correction : VM remises sur vmbr1, IP fixes 192.168.10.100 / .10, DNS vers le DC, heure corrigée, jonction au domaine puis M1.3.

2) Lecteurs K:/S: absents : les chemins UNC de la GPO Bureau avaient été saisis avec un seul « \ » (\m2l.lan au lieu de \\m2l.lan). Diagnostic : onglet Paramètres de la GPO dans la GPMC et Get-GPRegistryValue. Correction : script corrigé et relancé, versions AD/SYSVOL identiques (12/12).

3) Script de test refusé pour n.petit (stratégie d'exécution PowerShell). Correction : Set-ExecutionPolicy -Scope Process Bypass dans la session de test.

Le test le plus délicat a été le changement de mot de passe : la durée de vie minimale (1 jour) interdit de refaire un essai, et le PSO de la DSI exige 14 caractères pour a.benali. Remarque : le mot de passe initial réellement saisi dans le lab est Pa££w0rd (et non Pa$$w0rd), à cause de la disposition du clavier dans la console.

CAPTURES D'ÉCRAN — PREUVES

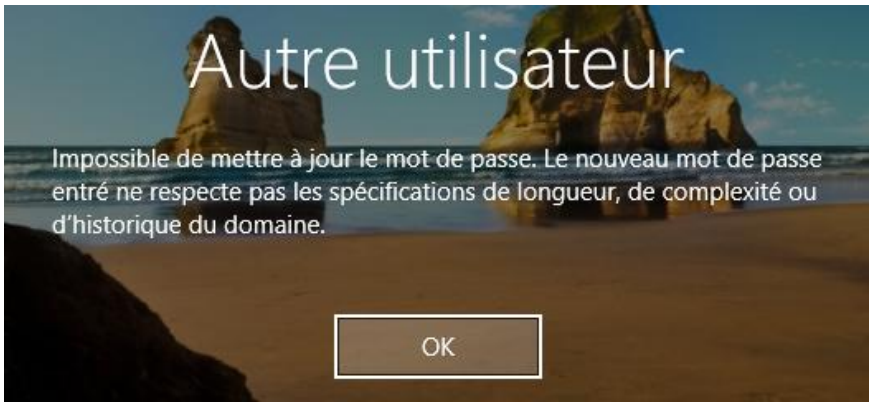


Figure 34 – Mot de passe faible refusé à la première connexion (c.marchal)

« azerty » est refusé : « Impossible de mettre à jour le mot de passe. Le nouveau mot de passe entré ne respecte pas les spécifications de longueur, de complexité ou d'historique du domaine. » (GPO_M2L_Comptes_MDP).

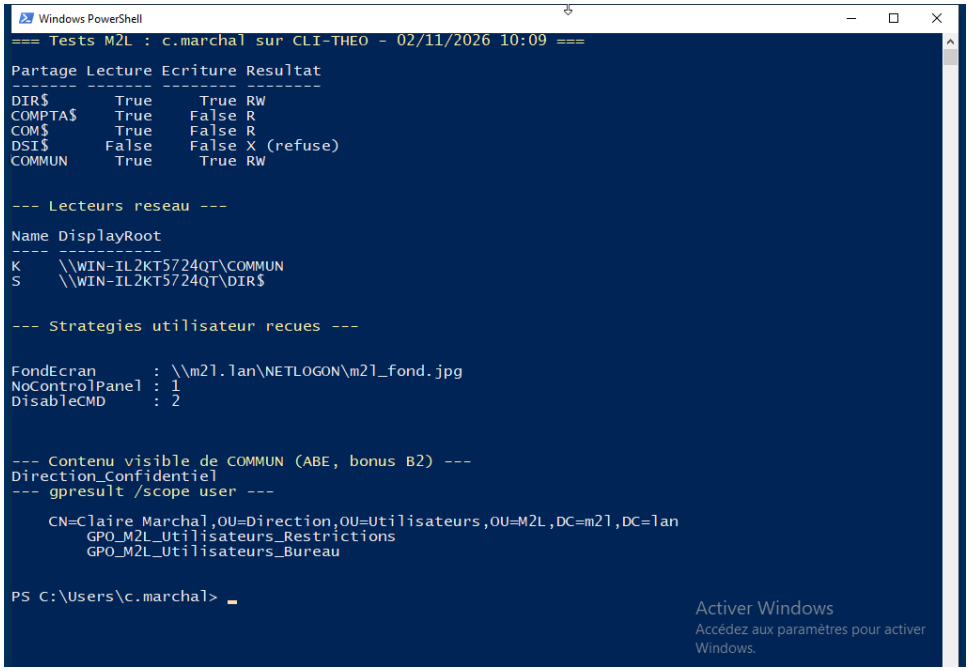


Figure 35 – Tests de c.marchal (Direction) – script \\m2l.lan\NETLOGON\Test-M2L.ps1

DIR$ RW, COMPTA$ R, COM$ R, DSI$ refusé, COMMUN RW ; K: et S: (DIR$), fond d'écran, NoControlPanel = 1, DisableCMD = 2 ; Direction_Confidentiel visible (B2).

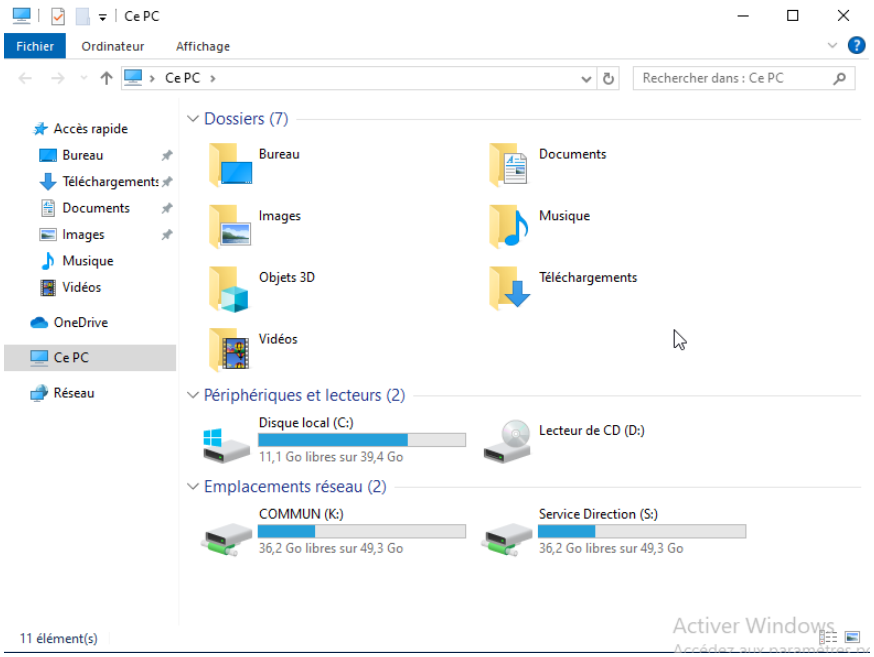


Figure 36 – Lecteurs réseau obtenus par c.marchal

COMMUN (K:) et Service Direction (S:) dans « Ce PC ».

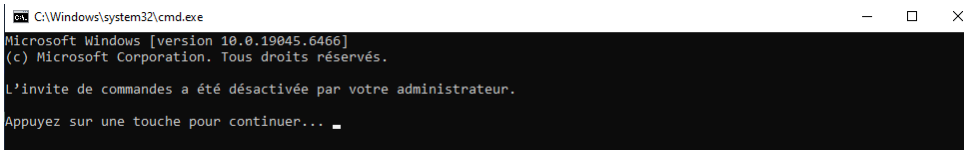


Figure 37 – Invite de commandes bloquée pour c.marchal

« L'invite de commandes a été désactivée par votre administrateur. »

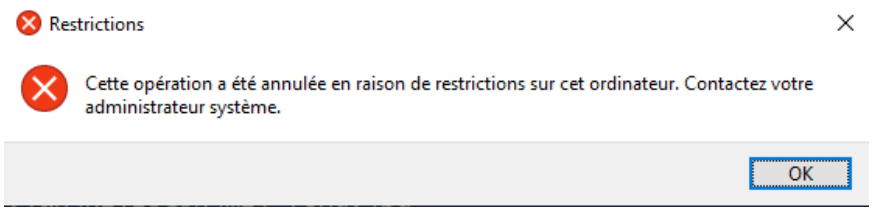


Figure 38 – Panneau de configuration bloqué pour c.marchal

« Cette opération a été annulée en raison de restrictions sur cet ordinateur. »

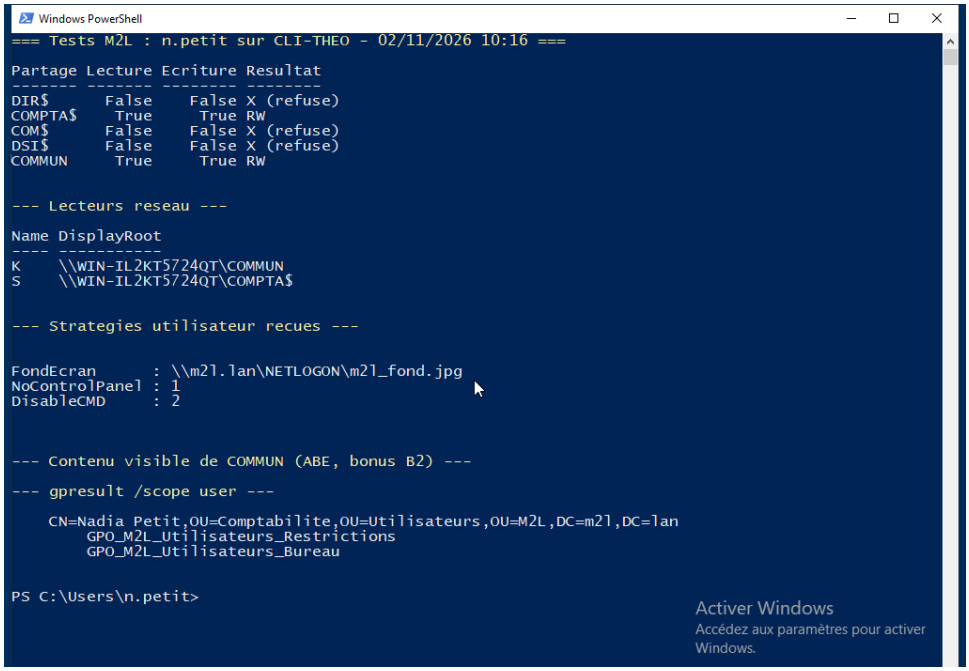


Figure 39 – Tests de n.petit (Comptabilité)

COMPTA$ et COMMUN en RW, le reste refusé ; S: → COMPTA$; restrictions appliquées ; Direction_Confidentiel invisible grâce à l'ABE (B2).

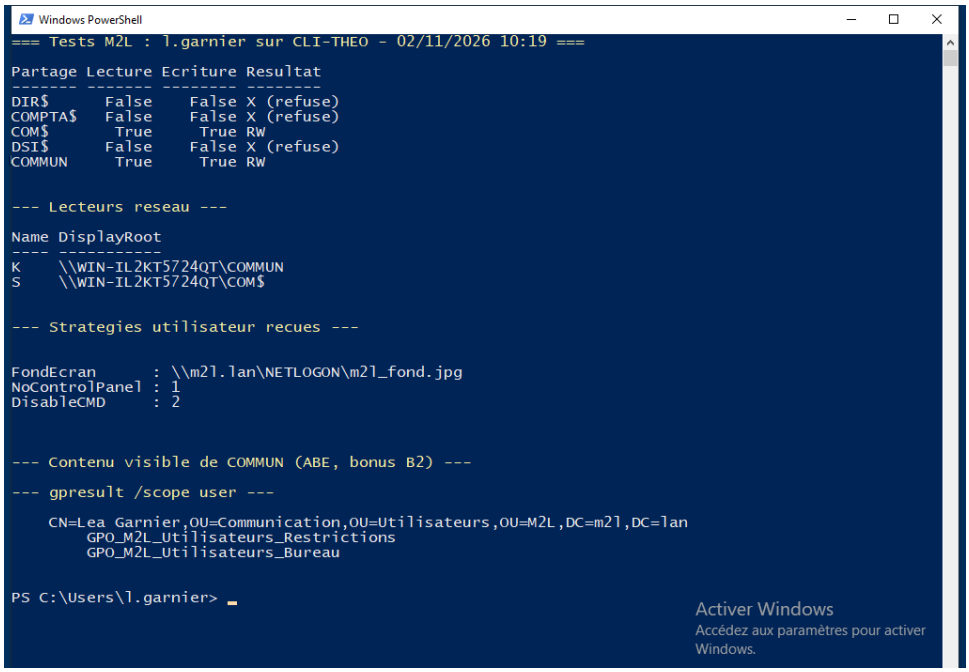


Figure 40 – Tests de l.garnier (Communication)

COM$ et COMMUN en RW, le reste refusé ; S: → COM$; restrictions appliquées.

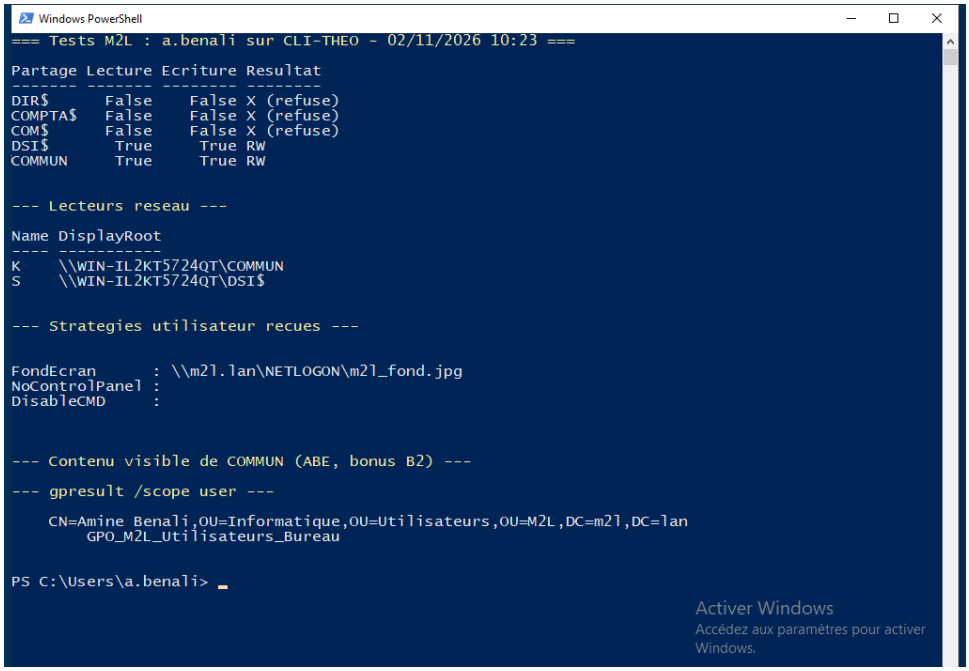


Figure 41 – Tests de a.benali (Informatique)

DSI$ et COMMUN en RW, le reste refusé ; S: → DSI$; aucune restriction (NoControlPanel et DisableCMD absents), seule la GPO Bureau s'applique.

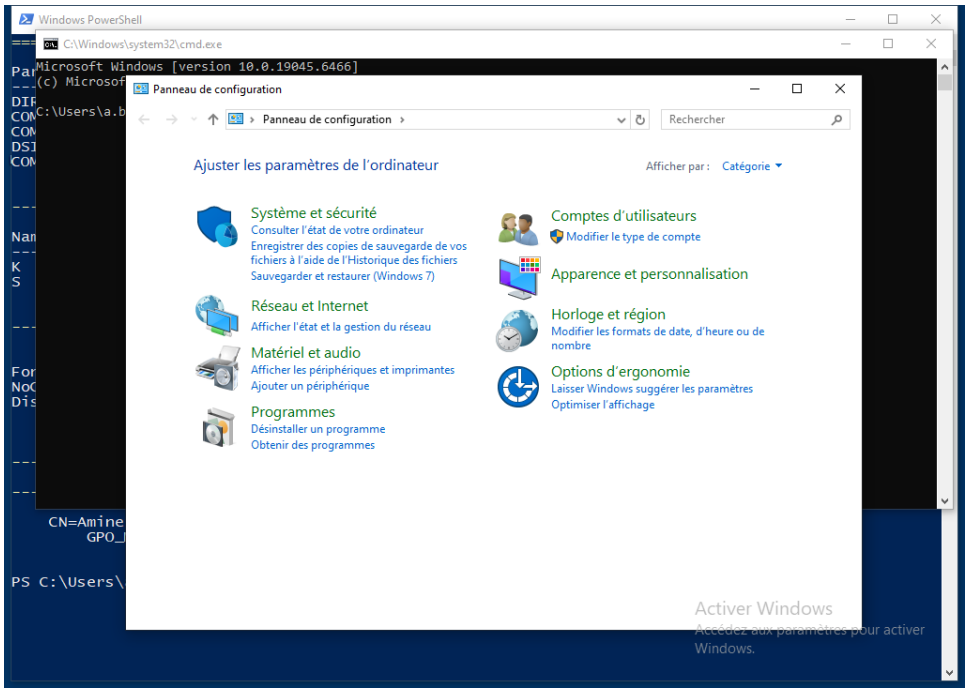


Figure 42 – Panneau de configuration et invite de commandes accessibles pour a.benali

La DSI n'est pas concernée par GPO_M2L_Utilisateurs_Restrictions.

★ **Défi du formateur (facultatif)**

Le formateur peut introduire **jusqu'à 3 incidents** dans votre configuration. Votre tâche : diagnostiquer avec méthode (symptôme → hypothèses → vérification → correction) et consigner chaque incident dans le journal ci-dessous.

JOURNAL DES INCIDENTS — DÉFI DU FORMATEUR

N°	Symptôme	Hypothèses	Vérification	Correction
1	Aucun incident introduit par le formateur à la date du rendu.			
2	—			
3	—			

Validation du niveau par le formateur : ☐ Validé ☐ À reprendre
Visa : _____ Heure : ____ h ____

Bonus — Défis facultatifs

Réalisables dès que les niveaux N1 à N4 sont validés. Chaque bonus réussi, **expliqué oralement au formateur**, valorise l'appréciation (+2 points maximum au total).

Défi	Énoncé	Pistes
B1 Mots de passe renforcés	Les comptes de la DSI (groupe GG_Informatique) doivent avoir une politique plus stricte que les autres agents : 14 caractères minimum, verrouillage après 3 erreurs. Sans toucher à la GPO du domaine.	Fine-Grained Password Policy (PSO) · `New-ADFineGrainedPasswordPolicy` · `Get-ADUserResultantPasswordPolicy`
B2 Énumération basée sur les accès	Créez dans COMMUN un sous-dossier réservé à la Direction. Faites en sorte que les autres services **ne le voient même pas**.	`Set-SmbShare` (mode d'énumération) · NTFS
B3 Délégation de contrôle	La technicienne support (`s.klein`) doit pouvoir **réinitialiser les mots de passe** des agents des trois autres services — rien d'autre. Appliquez le principe du moindre privilège : déléguez ce droit à un groupe dédié `GG_Support` ne contenant que s.klein (GG_Informatique inclut aussi a.benali).	Assistant « Déléguer le contrôle » · `dsacls`
B4 Administration à distance	Administrez l'annuaire et les GPO **depuis le poste Windows 11** sans ouvrir de session sur le serveur.	Outils RSAT (fonctionnalités facultatives Windows 11) · session avec un compte approprié
B5 Filtrage de sécurité	Remplacez les 3 liens de la GPO Restrictions par **un seul lien** sur l'OU `Utilisateurs`, en excluant l'Informatique par filtrage.	Onglet Délégation › Avancé · droit « Appliquer la stratégie de groupe »

Réalisation des bonus (scripts C:\Scripts\Bonus_B1_B2_B3.ps1 et Bonus_B5_Filtrage.ps1)

B1 – PSO_M2L_DSI

Fine-Grained Password Policy appliquée au groupe GG_Informatique : 14 caractères minimum, complexité, verrouillage après 3 erreurs pendant 15 min, priorité 10. La GPO du domaine n'est pas modifiée : Get-ADUserResultantPasswordPolicy renvoie PSO_M2L_DSI pour a.benali et rien pour c.marchal (politique du domaine).

B2 – Énumération basée sur l'accès

Sous-dossier COMMUN\Direction_Confidentiel : héritage coupé, Admins + SYSTEM + DL_CommunDirection_RW (← GG_Direction) en Modification ; FolderEnumerationMode = AccessBased sur COMMUN. Résultat N5 : c.marchal voit le dossier, n.petit, l.garnier et a.benali ne le voient pas.

B3 – Délégation de contrôle

Groupe GG_Support (s.klein uniquement) ; sur les OU Direction, Comptabilite et Communication (pas Informatique) : droit étendu « Reset Password » + écriture de pwdLastSet (forcer le changement) et lockoutTime (déverrouiller), sur les objets utilisateur uniquement (dsacls /I:S). Contrôle : 3 ACE par OU de service, 0 sur Informatique.

B4 – Administration à distance

RSAT installé sur CLI-THEO (Rsat.ActiveDirectory.DS-LDS.Tools, Rsat.GroupPolicy.Management.Tools). Depuis une session M2L-LAB\Administrateur sur le poste, l'annuaire et les GPO sont administrés sans ouvrir de session sur le serveur (PowerShell AD/GPO et console dsa.msc connectée à WIN-IL2KT5724QT).

B5 – Filtrage de sécurité

Les 3 liens de GPO_M2L_Utilisateurs_Restrictions sont remplacés par un seul lien sur l'OU Utilisateurs ; le droit « Appliquer la stratégie de groupe » est refusé à GG_Informatique (lecture conservée). Résultat : gpresult de a.benali indique « Filtrage : Refusé (Sécurité) », les 3 autres services restent restreints.



Figure 43 – Bonus B1, B2 et B3 – contrôles après exécution du script

PSO_M2L_DSI (14 car., 3 essais) pour a.benali ; COMMUN en AccessBased et ACL de Direction_Confidentiel ; 3 ACE GG_Support sur chaque OU de service, aucune sur Informatique.

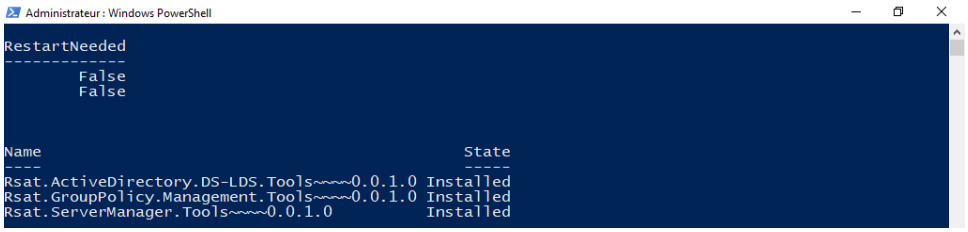


Figure 44 – Bonus B4 – installation des outils RSAT sur CLI-THEO

Outils AD DS / LDS et Gestion des stratégies de groupe installés (Add-WindowsCapability).

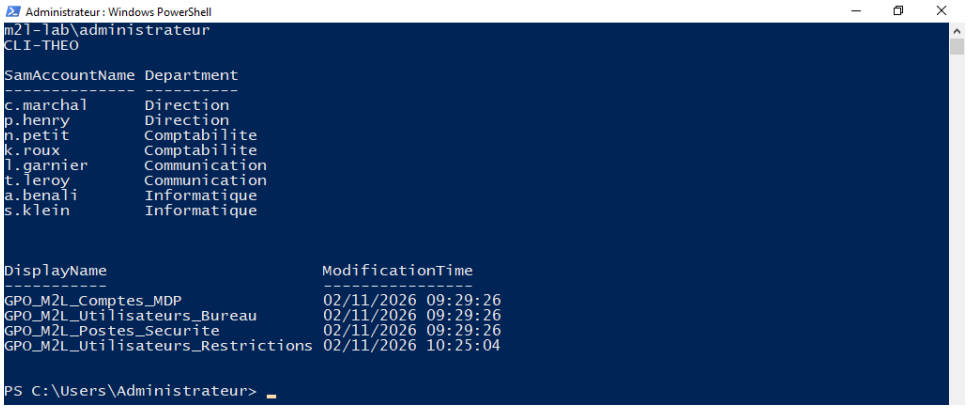


Figure 45 – Bonus B4 – administration de l'AD et des GPO depuis le poste

Session M2L-LAB\administrateur sur CLI-THEO : Get-ADUser et Get-GPO interrogent le DC à distance.

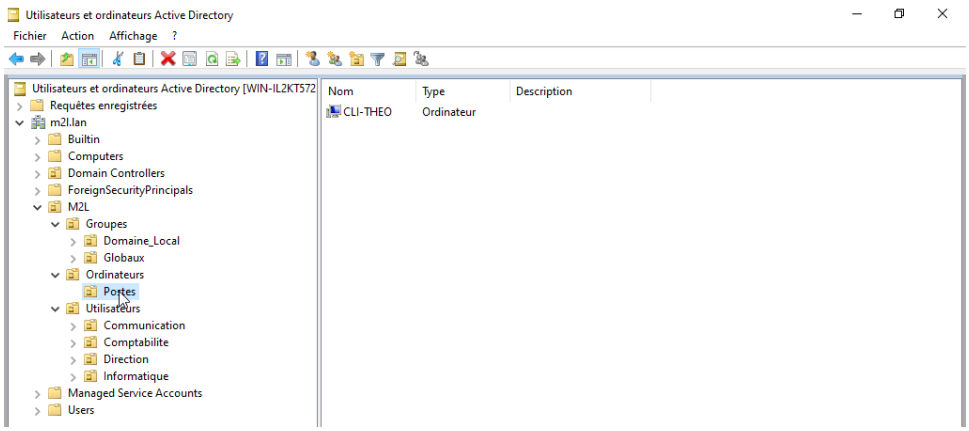


Figure 46 – Bonus B4 – console dsa.msc lancée sur le poste

La console, ouverte sur CLI-THEO, est connectée à WIN-IL2KT5724QT et montre le compte ordinateur CLI-THEO dans l'OU Postes.

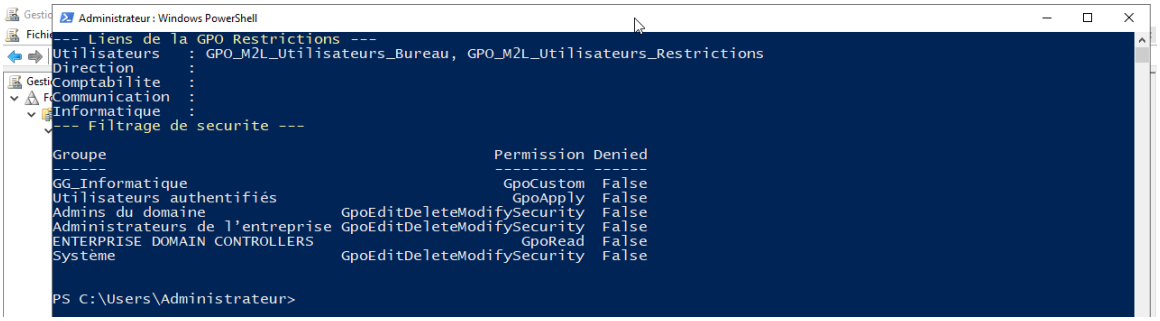


Figure 47 – Bonus B5 – un seul lien et refus pour GG_Informatique

GPO_M2L_Utilisateurs_Restrictions n'est plus liée qu'à l'OU Utilisateurs ; GG_Informatique a une permission personnalisée (refus de l'application).

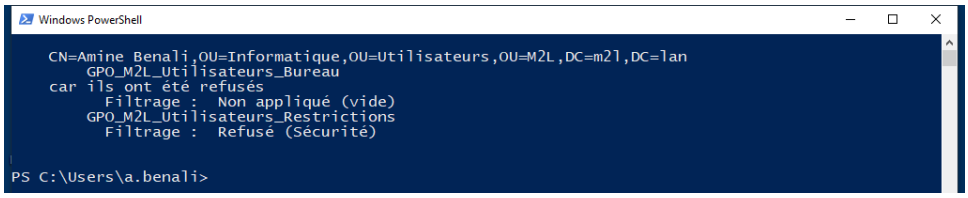


Figure 48 – Bonus B5 – vérification sur le poste avec a.benali

« GPO_M2L_Utilisateurs_Restrictions – Filtrage : Refusé (Sécurité) ».

Annexe A — Glossaire

Terme	Définition
ABE	Access-Based Enumeration (énumération basée sur l'accès) : masque à un utilisateur les dossiers d'un partage auxquels il n'a pas accès.
AD DS	Active Directory Domain Services : annuaire centralisant comptes, groupes, ordinateurs et stratégies.
UGDLP	Utilisateurs → Global → Domain Local → Permissions : modèle de gestion des droits.
Canal sécurisé	Liaison authentifiée (mot de passe du compte ordinateur) entre un poste membre et le domaine ; s'il est rompu, les ouvertures de session de domaine échouent.
DN / UPN / SamAccountName	Chemin complet d'un objet / identifiant de type e-mail / identifiant court de connexion.
DSI	Direction des systèmes d'information.
GG / DL	Groupe global (regroupe des comptes) / groupe domaine local (reçoit des permissions sur des ressources).
GPO / GPP	Objet de stratégie de groupe / préférences de stratégie de groupe (paramètres ciblables).
LSDOU	Ordre d'application : Local, Site, Domaine, OU.
NetBIOS (nom)	Nom court du domaine (ici M2L), utilisé dans le format d'ouverture de session M2L\login.
NETLOGON	Partage présent sur chaque contrôleur de domaine, destiné aux scripts et fichiers de connexion.
NTFS / ACL / ACE	Système de fichiers et ses permissions / liste de contrôle d'accès / une entrée de cette liste.
OU	Unité d'organisation : conteneur administrable (liens de GPO, délégation).
PSO	Password Settings Object : politique de mots de passe ciblée sur des utilisateurs ou groupes.
RSAT	Remote Server Administration Tools : consoles d'administration à distance installables sur Windows 11.
SMB / UNC	Protocole de partage de fichiers Windows / chemin réseau `\\serveur\partage`.
Snapshot	Instantané d'une VM Proxmox permettant un retour arrière rapide ; ce n'est pas une sauvegarde.
VMID	Identifiant numérique d'une machine virtuelle dans Proxmox VE.

Annexe B — Guide de diagnostic

Pistes de vérification — à vous de trouver la cause et la correction.

Symptôme	Pistes de vérification
Accès refusé alors que « le groupe est bon »	Session réouverte depuis la modification ? ACL réelle du dossier ?
Un utilisateur accède à un dossier qui ne le concerne pas	Héritage coupé ? Groupes génériques encore présents dans l'ACL ?
Une GPO ne s'applique pas	Lien actif et au bon endroit ? Objet (utilisateur / ordinateur) dans la bonne OU ? Configuration utilisateur ou ordinateur ? `gpresult` ?
Lecteur réseau absent	Chemin UNC joignable depuis le poste ? Ciblage au niveau de l'élément ? Nouvelle session ?
Création de compte refusée (mot de passe)	Une politique de mot de passe déjà appliquée ? Longueur et complexité du mot de passe initial ?
Le partage est inaccessible	DNS, résolution du nom du serveur, port 445, autorisations de partage ?
Compte bloqué pendant les tests	Politique de verrouillage : seuil et durée ?
Nouveau mot de passe conforme refusé	Durée de vie minimale (1 jour) ? Historique (5 mots de passe) ? Longueur (10) et complexité ?
gpresult impossible dans une session d'agent	Invite de commandes bloquée par une GPO ? Console administrateur et option /user ?

Annexe C — Grille de barème et auto-évaluation

Évaluez-vous honnêtement avant de présenter votre travail ; le formateur complétera la colonne de droite.

Niveau	Critère	Pts	Auto-éval.	Formateur
N1 Structure AD, comptes et poste	Arborescence d'OU conforme (11 OU)	1	1	
	8 comptes : login, UPN, comptes activés	0,75	0,75	
	Comptes dans la bonne OU de service	0,5	0,5	
	Attributs : nom complet, service, fonction	0,5	0,5	
	Mot de passe initial + changement obligatoire	0,25	0,25	
	Poste Windows 11 déplacé dans l'OU Postes	0,5	0,5	
	OU protégées contre la suppression accidentelle	0,5	0,5	
N2 Groupes et stratégie UGDLP	5 GG (portée Globale, type Sécurité, bonne OU)	0,75	0,75	
	Membres des GG conformes	0,75	0,75	
	7 DL (portée Domaine local, type Sécurité, bonne OU)	0,5	0,5	
	Imbrication GG → DL conforme à la matrice	1,5	1,5	
	Questions de compréhension UGDLP argumentées	0,5	0,5	
N3 Partages et permissions NTFS	5 dossiers + 5 partages (noms exacts, $ masqués)	1	1	
	Autorisations de partage non bloquantes	0,25	0,25	
	Justification partage / NTFS (cumul, plus restrictif)	0,25	0,25	
	NTFS : héritage coupé, Utilisateurs retiré, Admins + SYSTEM conservés	1	1	
	NTFS : bons DL avec les bons droits (RX / M)	1	1	
	Aucun utilisateur ni GG dans les ACL	0,5	0,5	
N4 Stratégies de groupe	GPO mots de passe liée au domaine, valeurs conformes	1	1	
	GPO Bureau : fond d'écran + lecteur K: + lecteurs S: ciblés	1,5	1,5	
	GPO Restrictions : 2 paramètres, liée aux 3 OU (DSI exclue)	0,75	0,75	
	GPO Postes : inactivité + stockage amovible, liée à l'OU Postes	0,75	0,75	
N5 Validation et rapport de tests	Matrice des tests d'accès renseignée et cohérente	1	1	
	Tests GPO + gpresult commentés	1	1	
Q Qualité professionnelle	Conventions de nommage respectées	0,5	0,5	
	Niveau 0 réalisé (snapshots + vérifications)	0,5	0,5	
	Méthode : contrôles au fil de l'eau, rapport clair	0,5	0,5	
	Autonomie et gestion du temps	0,5	0,5	
	TOTAL	**20**	20	