Nom : Rhassef
Prénom : Ayoub

COMPTE RENDU D'ACTIVITÉ

AP2 - PROJET VALORELEC

10/02/2026-17/02/2026

SOMMAIRE

1. Résumé du contexte

La société **ValorElec**, PME spécialisée dans les installations électriques, connaît une croissance importante de son effectif. Jusqu'à présent, la gestion des données et des accès se faisait de manière artisanale.

Pour accompagner ce développement, l'entreprise a souhaité professionnaliser son infrastructure informatique afin de centraliser la gestion des utilisateurs, sécuriser le stockage des documents par service et automatiser le déploiement des outils de travail. Le projet repose sur l'implémentation d'une solution **Windows Server 2022**.

2. Objectifs et Missions à effectuer

Le projet a été découpé en quatre phases majeures :

- **Mise en place de l'annuaire :** Installation du rôle AD DS et configuration du DNS.
- **Gestion des identités :** Création de l'arborescence des Unités d'Organisation (OU) et application de la stratégie de groupes AGDLP.
- **Centralisation des données :** Mise en œuvre d'un espace de noms DFS, gestion des partages réseaux et mise en place de quotas de stockage.
- **Sécurisation du parc :** Déploiement automatisé de logiciels (MSI) et durcissement des postes clients via GPO (mots de passe, restrictions d'interface).

3. Présentation des Missions

3.1 M1-T1 Modélisation de l'architecture : Créer le schéma des OUs et groupes.

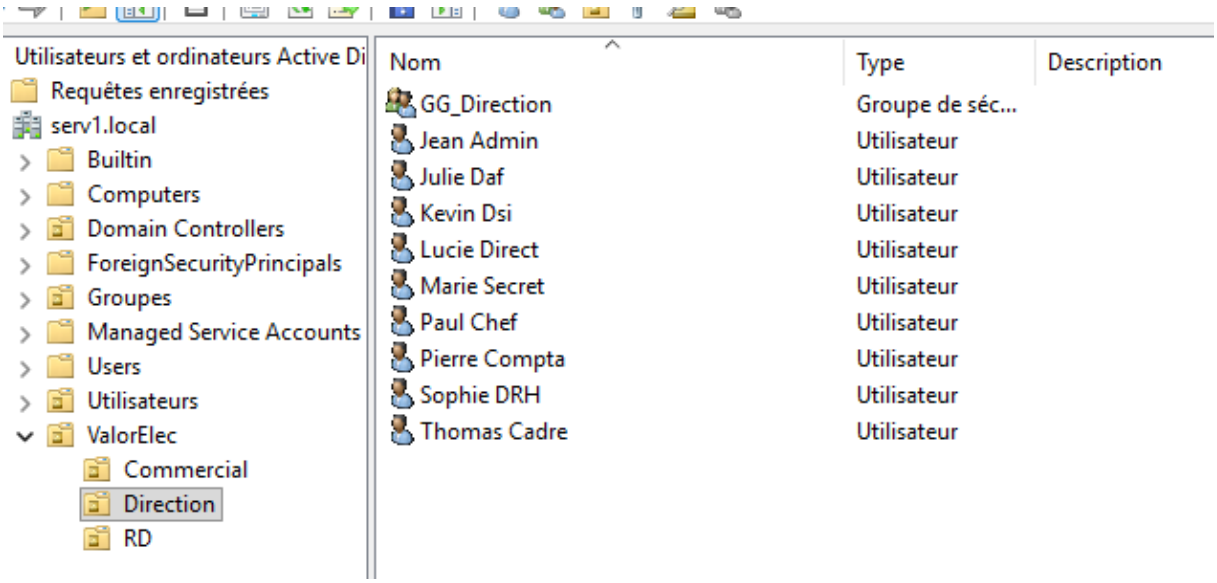
Cette étape consiste à concevoir l'arborescence Active Directory pour le client ValorElec afin d'organiser les 20 nouveaux collaborateurs par service. Cette structure est indispensable pour appliquer des politiques de sécurité spécifiques par métier (GPO).

Détails de l'organisation :

OU Racine : ValorElec (isolement du client).

Unités d'Organisation (OU) de niveau 2 : Direction, RD, Commercial.

Stratégie de Groupes : Création de groupes globaux pour chaque service (GG_Direction, GG_RD, GG_Commercial) afin de gérer les futures autorisations d'accès aux fichiers.



Dossier : Direction		Groupes Domaines Locaux (DL)		
		DL_Direction_L	DL_Direction_LM	DL_Direction_CT
Groupes Globaux	GG_Direction		X	
	GG_RD			
	GG_Commercial			

	Groupes Globaux (GG)		
	GG_Direction	GG_RD	GG_Commercial
Alain PROST	X		
Alice LEROY			X
Antoine LAVOISIER		X	
Blaise PASCAL		X	
David BECKHAM			X
Emma PETIT			X
Henri POINCARE		X	
Irène JOLIOT		X	
Jean DUPONT	X		
Julie MOREL			X
Lucas MARTIN		X	
Léon FOUCAULT		X	
Marc DUBOIS			X
Marie LEFEBVRE	X		
Nicolas BERNARD			X
Pierre AGUIAR		X	
Robert DE NIRO			X
Sarah CONNOR			X
Sophie CURIE		X	
Thomas DURAND		X	

Dossier : RD		Groupes Domaines Locaux (DL)		
		DL_RD_L	DL_RD_LM	DL_RD_CT
Groupes Globaux	GG_Direction	X		
	GG_RD		X	
	GG_Commercial			

	Groupes Globaux (GG)		
	GG_Direction	GG_RD	GG_Commercial
Alain PROST	X		
Alice LEROY			X
Antoine LAVOISIER		X	
Blaise PASCAL		X	
David BECKHAM			X
Emma PETIT			X
Henri POINCARE		X	
Irène JOLIOT		X	
Jean DUPONT	X		
Julie MOREL			X
Lucas MARTIN		X	
Léon FOUCAULT		X	
Marc DUBOIS			X
Marie LEFEBVRE	X		
Nicolas BERNARD			X
Pierre AGUIAR		X	
Robert DE NIRO			X
Sarah CONNOR			X
Sophie CURIE		X	
Thomas DURAND		X	

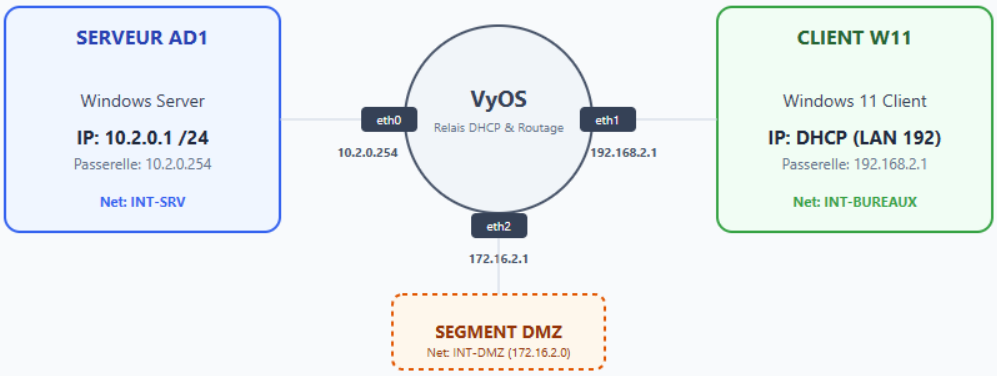
Dossier : Commercial		Groupes Domaines Locaux (DL)		
		DL_Commercial_L	DL_Commercial_LM	DL_Commercial_CT
Groupes Globaux	GG_Direction	X		
	GG_RD			
	GG_Commercial		X	

	Groupes Globaux (GG)		
	GG_Direction	GG_RD	GG_Commercial
Alain PROST	X		
Alice LEROY			X
Antoine LAVOISIER		X	
Blaise PASCAL		X	
David BECKHAM			X
Emma PETIT			X
Henri POINCARE		X	
Irène JOLIOT		X	
Jean DUPONT	X		
Julie MOREL			X
Lucas MARTIN		X	
Léon FOUCAULT		X	
Marc DUBOIS			X
Marie LEFEBVRE	X		
Nicolas BERNARD			X
Pierre AGUIAR		X	
Robert DE NIRO			X
Sarah CONNOR			X
Sophie CURIE		X	
Thomas DURAND		X	

Schémas Techniques : Projet ValorElec

Infrastructure Active Directory avec Routage VyOS (3 Segments) sous VirtualBox

1. Topologie Réseau et Configuration des Interfaces



Hôte Serveur

- Réseau interne : **INT-SRV**
- Promiscuité : Refuser
- IP : 10.2.0.1 / DNS : 10.2.0.1

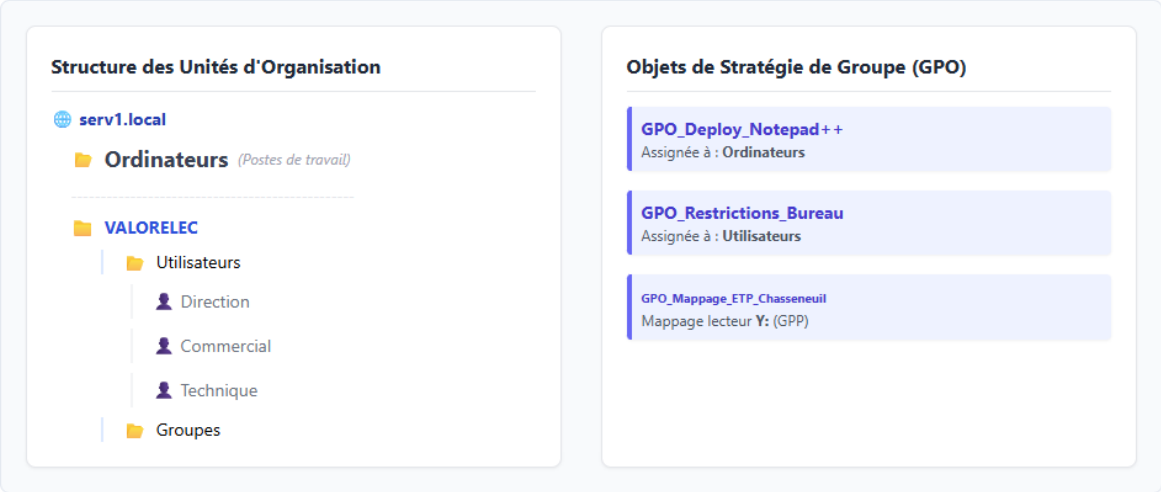
Hôte VyOS (3 NICs)

- Adapter 1 (eth0) : **INT-SRV**
- Adapter 2 (eth1) : **INT-BUREAUX**
- Adapter 3 (eth2) : **INT-DMZ**
- Promiscuité : **Tout autoriser**

Hôte Client

- Réseau interne : **INT-BUREAUX**
- Promiscuité : Refuser
- IP : Automatique (DHCP)

2. Organisation de l'Annuaire serv1.local



3. Centralisation des Données (DFS)

☑ Bilan de la mission — Objectif atteint. La structure de l'annuaire est en place, permettant une isolation claire du client et une organisation logique des ressources par service.

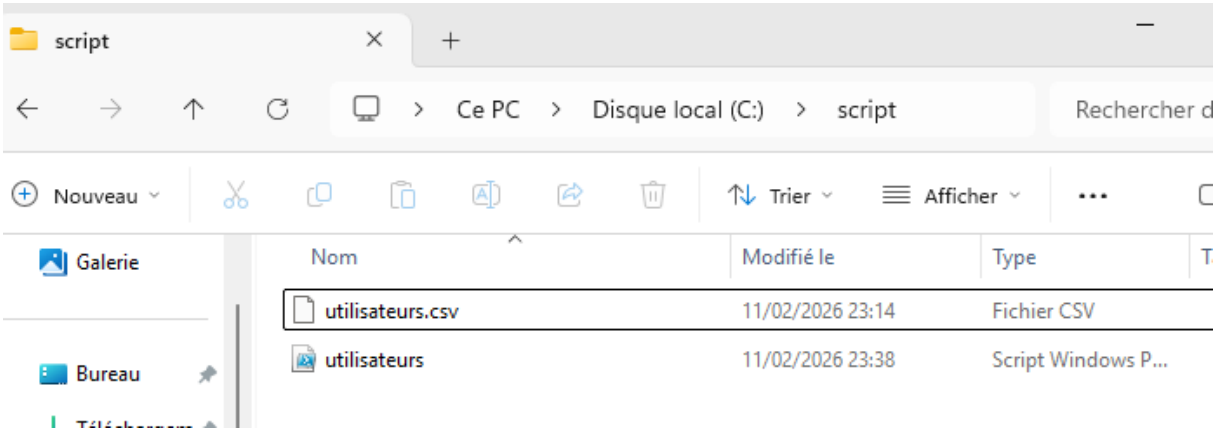
3.2 M1-T2 Automatisation et génération des accès utilisateurs

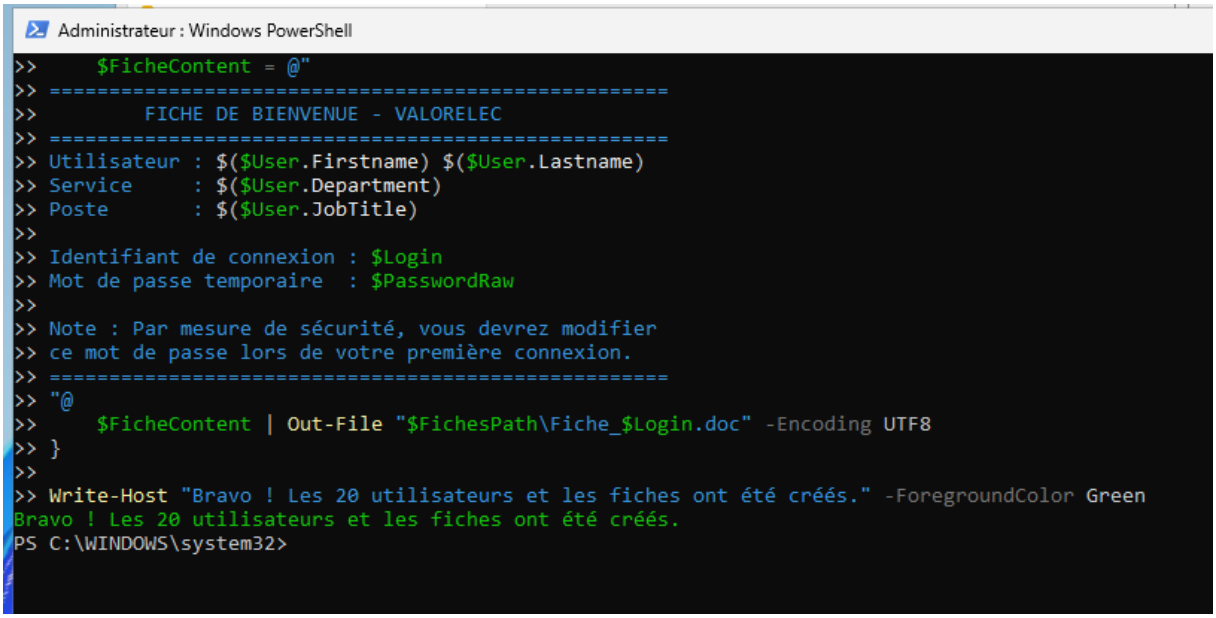
Cette tâche regroupe l'automatisation complète de la création des comptes et de la documentation utilisateur. L'objectif est de transformer le fichier CSV en objets Active Directory exploitables et de fournir les identifiants aux collaborateurs.

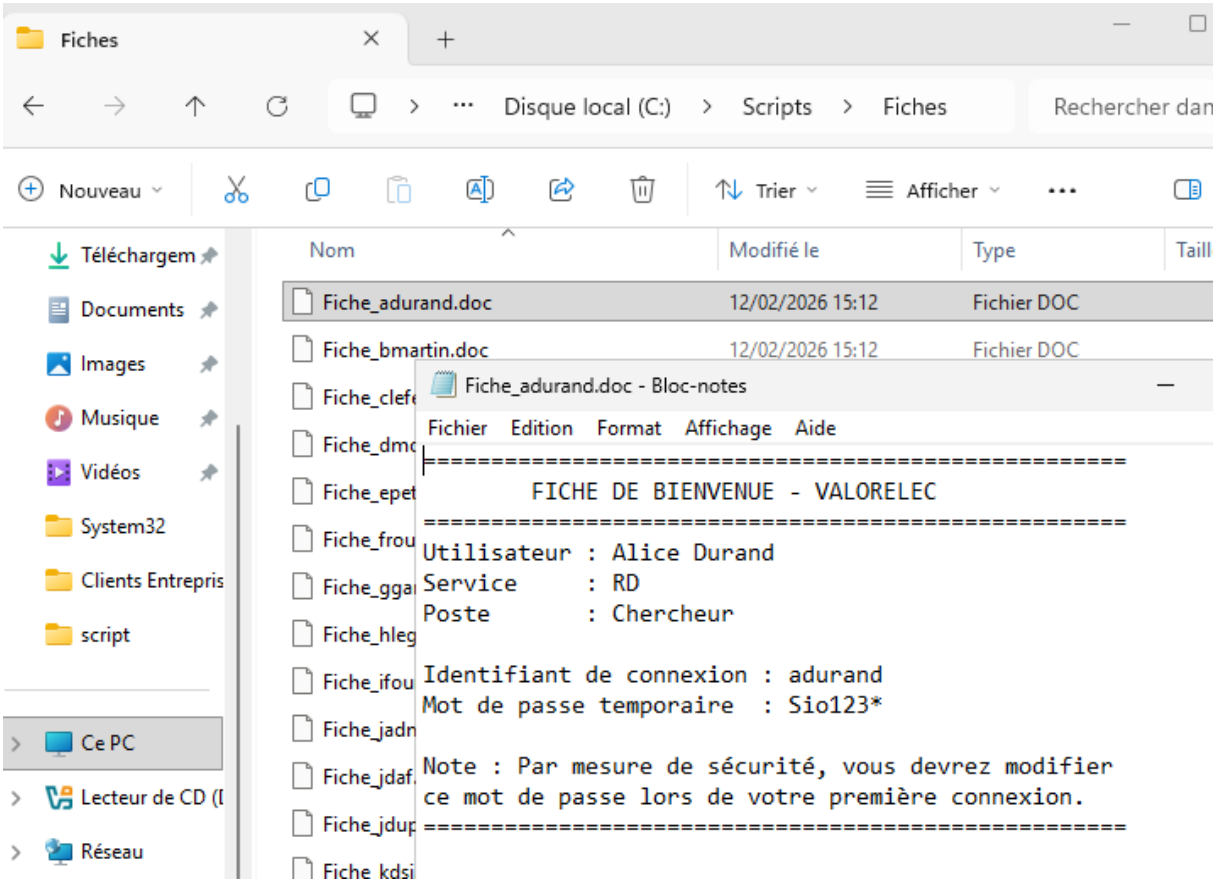
Actions automatisées :

- **Importation :** Lecture des 20 collaborateurs depuis C:\script\utilisateurs.csv.

- **Provisionnement :** Création des comptes avec mot de passe complexe (Sio123*) et ajout automatique dans les groupes de sécurité (GG_RD, GG_Direction, GG_Commercial).
- **Documentation :** Génération de 20 fiches de bienvenue individuelles (.doc) contenant les identifiants de connexion.







☑ Bilan de la mission — Objectif atteint. Le gain de temps est significatif grâce à l'automatisation. Les 20 comptes sont actifs et la documentation utilisateur est prête à être distribuée.

3.3 M2-T1 Configuration iSCSI : Mise en place du stockage (ex: TrueNAS) et connexion au serveur.

Déporter le stockage des données de l'entreprise ValorElec sur un serveur de stockage dédié (NAS) pour séparer le système et les données.

Étape 1 : Configuration du stockage sur TrueNAS

- Création d'un **Pool** de stockage nommé Pool_ValorElec en utilisant un disque physique.
- Création d'un **Zvol** (disque virtuel) de 20 Go pour accueillir les partages.

- Configuration du service **iSCSI** : création d'un Portail (Portal), d'une Cible (Target) et d'une Étendue (Extent) pour lier le Zvol au réseau.

Étape 2 : Connexion sur Windows Server

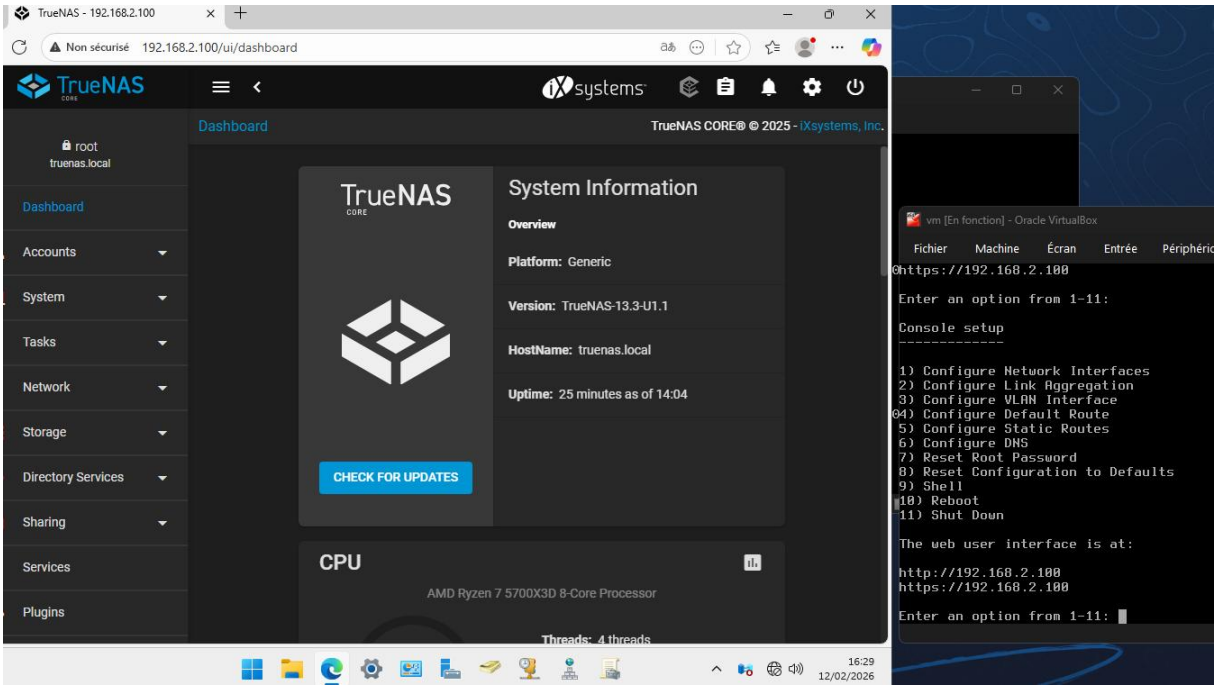
- Utilisation de l'**Initiateur iSCSI** pour lier le Windows Server au TrueNAS via l'IP 192.168.2.100.
- Authentification et connexion de la cible.

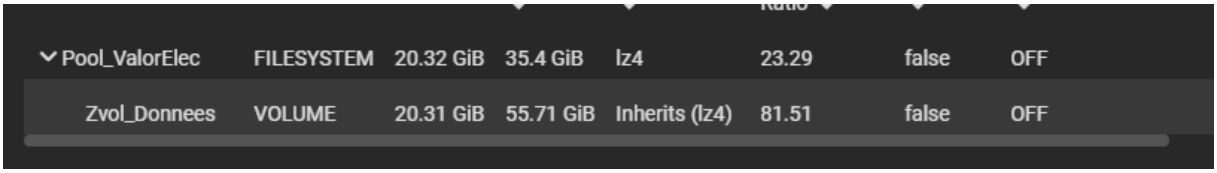
Étape 3 : Initialisation du disque

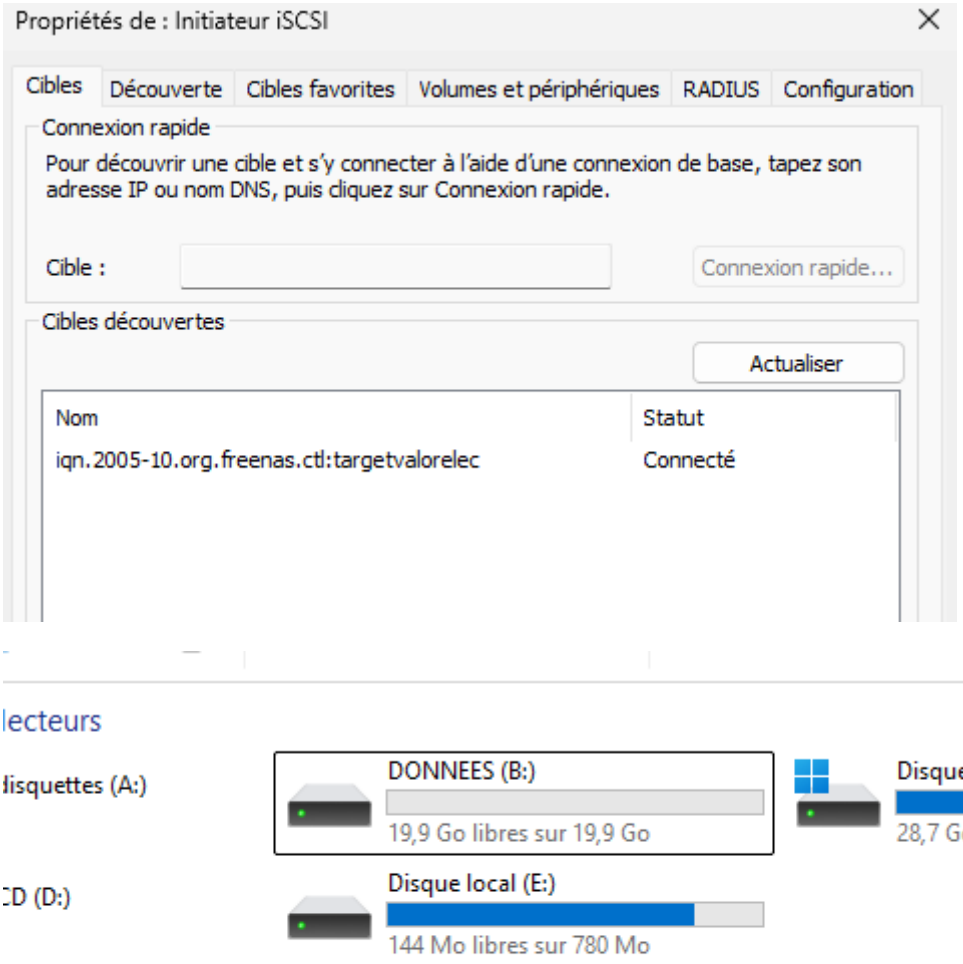
- Initialisation du nouveau disque détecté en mode **GPT**.
- Formatage du volume en **NTFS** avec l'étiquette DONNEES.

Incident rencontré: Lors du premier montage sur Windows Server, le disque virtuel (Zvol) affichait une taille erronée de seulement **16 Ko**.

Résolution : Après vérification sur l'interface TrueNAS, la taille du Zvol a été corrigée manuellement à **20 GiB**. Le disque a ensuite été réinitialisé en mode GPT et formaté en NTFS sur le serveur.







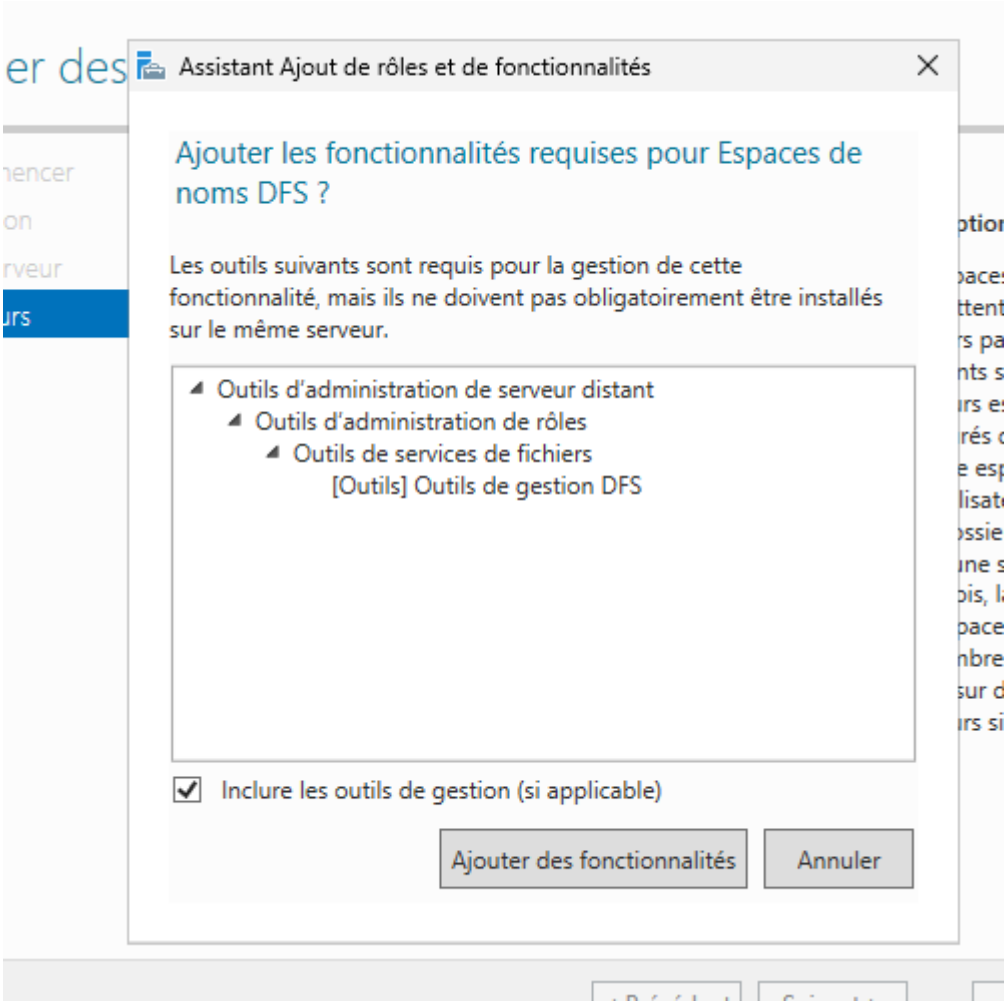
☑ Bilan de la mission — Objectif atteint. Le stockage est externalisé et sécurisé, offrant 20 Go d'espace dédié aux données de l'entreprise.

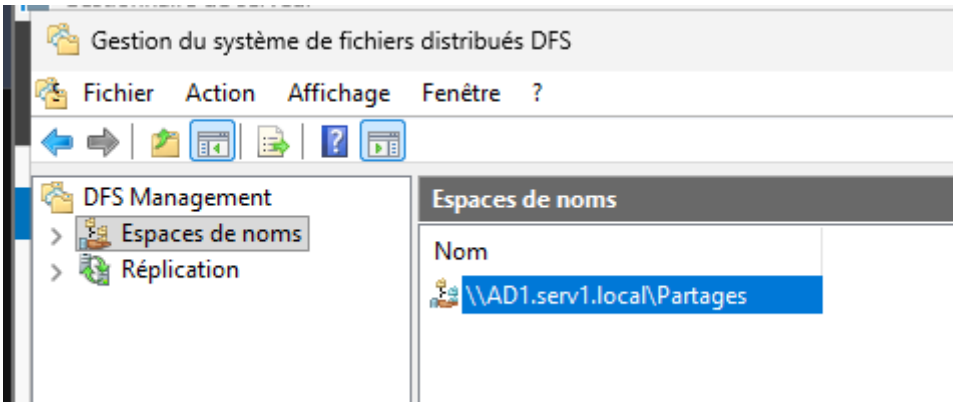
3.4 M2-T2 Étude et mise en œuvre de l'Espace de noms DFS

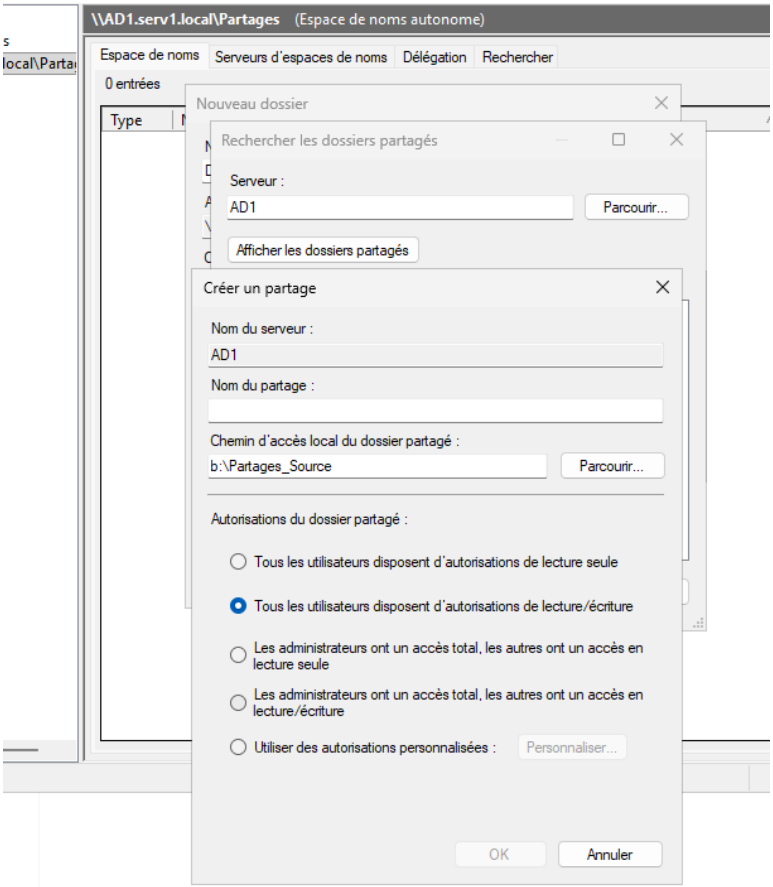
Mise en place d'une architecture de fichiers centralisée et sécurisée via le rôle **DFS (Distributed File System)**. Pour garantir la confidentialité, les dossiers physiques sur le serveur ont été configurés en **partages masqués**, rendant les ressources invisibles sur le réseau en dehors du point d'entrée unique DFS."

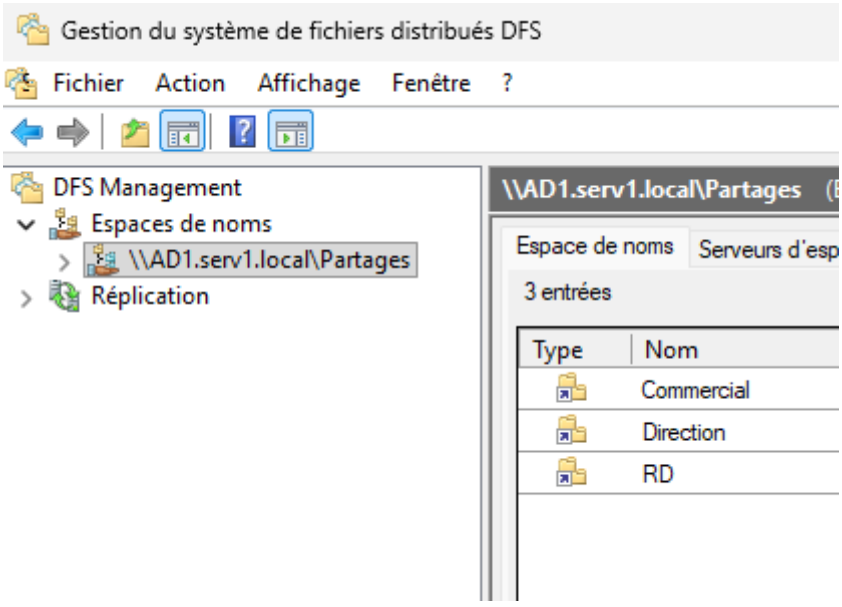
Détails techniques (Réalisation) :

1. **Création des partages masqués (Source) :**
    - Création des dossiers physiques sur le disque du serveur.
    - Partage de chaque dossier avec le symbole $ (ex: Commercial$, Direction$, RD$). Ces partages n'apparaissent pas dans le voisinage réseau classique.
2. **Configuration de l'Espace de noms DFS :**
    - Création de la racine de domaine : \\AD1.serv1.local\Partages.
3. **Liaison des dossiers :**
    - Création de dossiers logiques dans le DFS (ex: "Direction", "Commercial", "R&D").
    - Chaque dossier pointe vers sa **cible masquée** respective (ex: \\AD1.serv1.local\Direction$).
4. **Avantage Sécurité :** L'utilisateur ne peut passer que par le chemin DFS officiel. Les partages directs sont cachés, limitant ainsi les tentatives d'accès non autorisées par navigation réseau.


Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Espaces de noms DFS ?
Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de services de fichiers
[Outils] Outils de gestion DFS
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler


Gestion du système de fichiers distribués DFS
Fichier
Action
Affichage
Fenêtre
?
DFS Management
Espaces de noms
Réplication
Espaces de noms
Nom
\\AD1.serv1.local\Partages


\\AD1.serv1.local\Partages (Espace de noms autonome)
Espace de noms
Serveurs d'espaces de noms
Délégation
Rechercher
0 entrées
Type
Nouveau dossier
Rechercher les dossiers partagés
Serveur :
AD1
Parcourir...
Afficher les dossiers partagés
Créer un partage
Nom du serveur :
AD1
Nom du partage :
Chemin d'accès local du dossier partagé :
b:\Partages_Source
Parcourir...
Autorisations du dossier partagé :
Tous les utilisateurs disposent d'autorisations de lecture seule
Tous les utilisateurs disposent d'autorisations de lecture/écriture
Les administrateurs ont un accès total, les autres ont un accès en lecture seule
Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture
Utiliser des autorisations personnalisées :
Personnaliser...
OK
Annuler


Gestion du système de fichiers distribués DFS
Fichier
Action
Affichage
Fenêtre
?
DFS Management
Espaces de noms
\\AD1.serv1.local\Partages
Réplication
\\AD1.serv1.local\Partages
Espace de noms
Serveurs d'esp
3 entrées
Type
Nom
Commercial
Direction
RD

☑ Bilan de la mission — Objectif atteint. L'architecture de fichiers est simplifiée pour l'utilisateur final et sécurisée par l'utilisation de partages masqués (symboles $).

3.5 M3-T1 Matrice des droits (Excel) : Remplir le tableau des droits (Groupes Globaux vs Groupes Domaines Locaux).

Établir la matrice des droits d'accès pour les trois services de l'entreprise (Direction, RD, Commercial) en suivant la méthode AGDLP.

Structure mise en place :

1. **Comptes Utilisateurs** : Créés dans l'AD et affectés à leurs services respectifs.
2. **Groupes Globaux (GG)** : Un groupe par service (GG_Direction, GG_RD, GG_Commercial).
3. **Groupes Domaines Locaux (DL)** : Deux groupes par ressource pour gérer la granularité :
    - DL_NomDossier_L : Pour le droit de **Lecture**.
    - DL_NomDossier_LM : Pour le droit de **Lecture/Modification**.

Logique de sécurité appliquée :

- Le groupe global GG_RD est membre du groupe local DL_RD_LM (ils peuvent modifier leurs travaux).
- Le groupe global GG_Direction est membre du groupe local DL_RD_L (ils peuvent consulter la RD mais sans rien modifier).
- Les permissions NTFS sont appliquées uniquement sur les groupes **DL**.

☑ Bilan de la mission — Objectif atteint. La stratégie de droits est documentée et prête à être appliquée, garantissant une granularité fine (Lecture seule vs Modification).

3.6 M3-T2 Scripting Sécurité NTFS/Partage : Script PowerShell pour appliquer les droits NTFS(Script disponible sur le trello)

Automatiser la création de l'arborescence de sécurité AGDLP et appliquer les permissions NTFS sur le stockage iSCSI.

Actions réalisées :

- **Automatisation par script PowerShell** : Utilisation d'un script pour créer 9 groupes de sécurité (3 Globaux et 6 Locaux de Domaine).
- **Imbrication AGDLP** : Les Groupes Globaux (utilisateurs) sont intégrés dans les Groupes Locaux (accès aux ressources).
- **Sécurisation NTFS** : Application des droits sur le disque B: avec rupture de l'héritage pour garantir que chaque service n'accède qu'à ses propres données.
- **Supervision** : La Direction est ajoutée en "Lecture seule" sur les dossiers RD et Commercial via le groupe DL_RD_L et DL_Commercial_L.

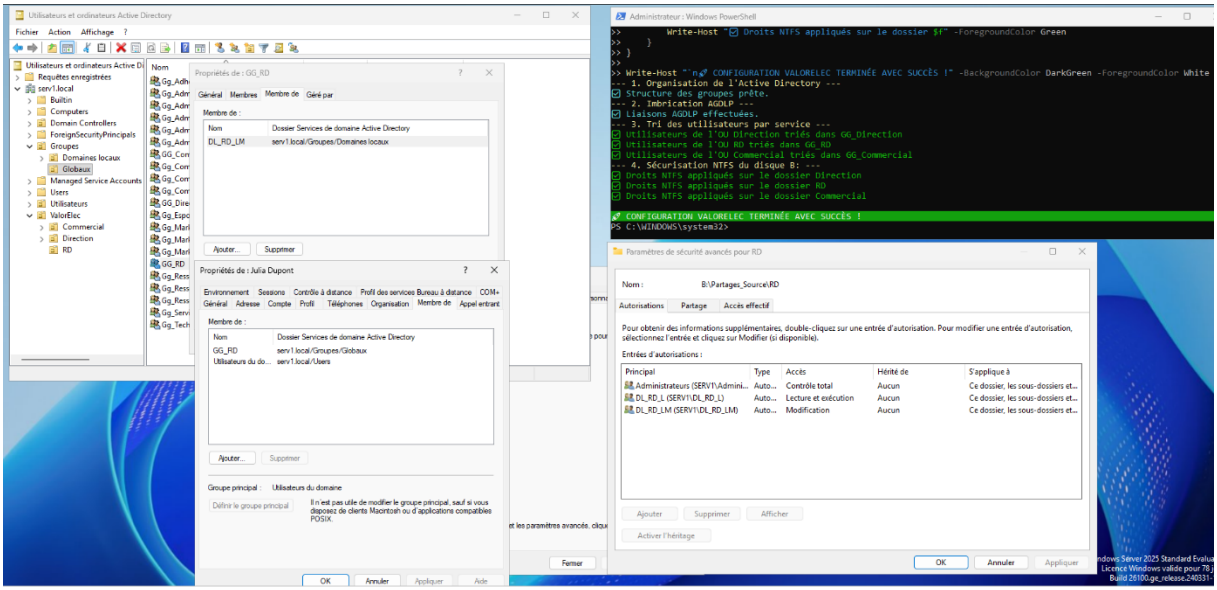
Problème rencontré : Échec immédiat du script avec un message **"Accès refusé"** lors de la création des Unités d'Organisation.

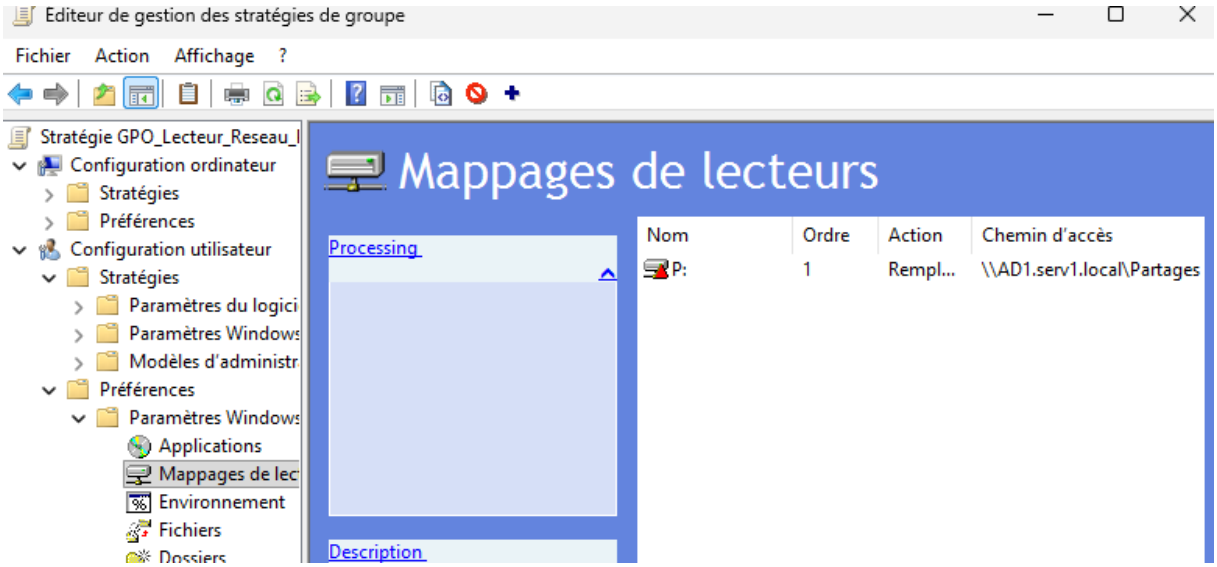
Résolution : L'erreur provenait de l'utilisation d'un **compte utilisateur standard** dépourvu de privilèges administratifs sur l'AD. La session a été relancée avec un **compte Administrateur du domaine**, ce qui a permis de finaliser la configuration.

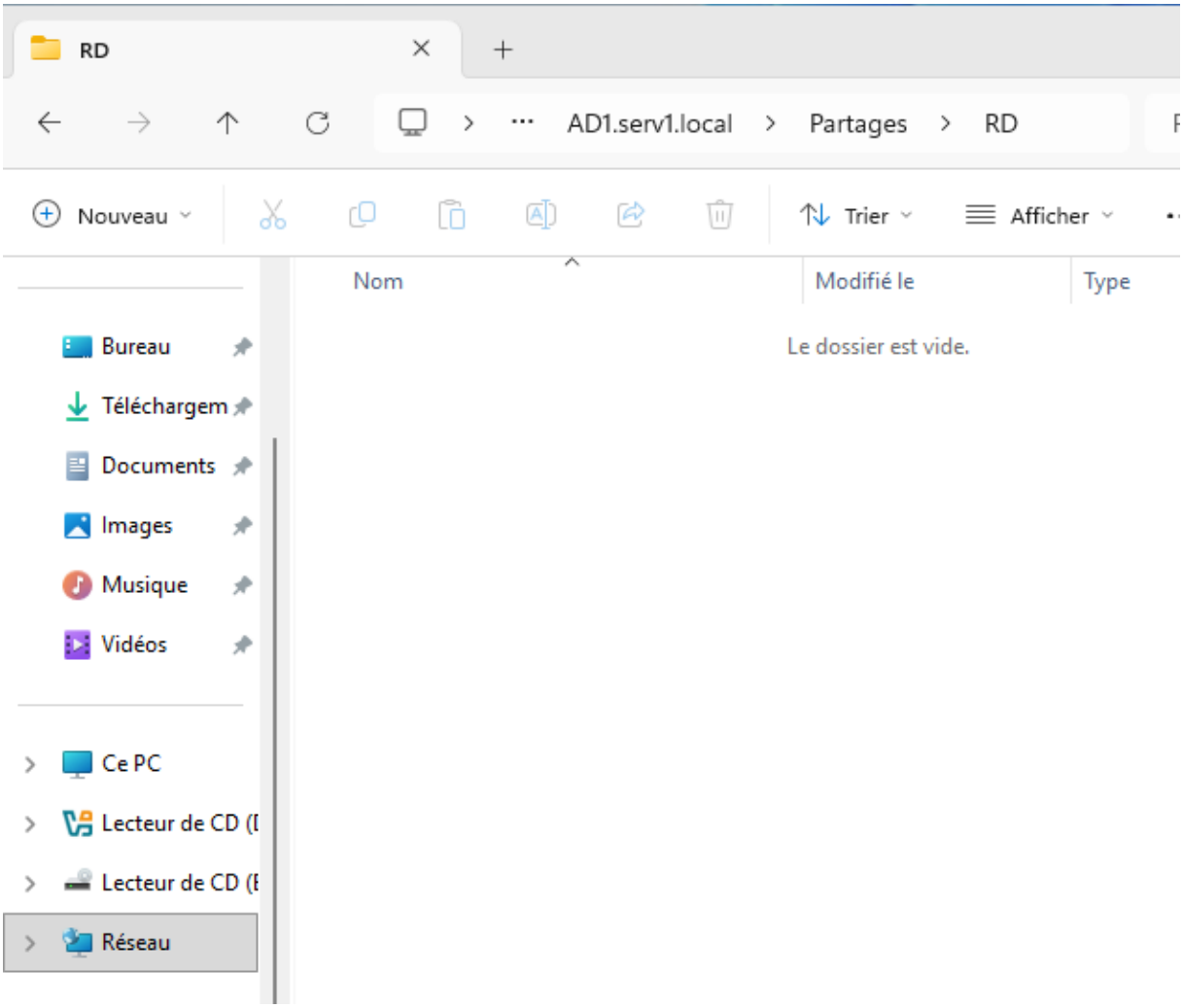
```
New-ADOrganizationalUnit : Accès refusé
Au caractère Ligne:1 : 1
+ New-ADOrganizationalUnit -Name "Groupes" -Path $Domain -ErrorAction S ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (OU=Groupes,DC=serv1,DC=local:String) [New-ADOrganiza
   tionalUnit], UnauthorizedAccessException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.Acti
   veDirectory.Management.Commands.NewADOrganizationalUnit
```

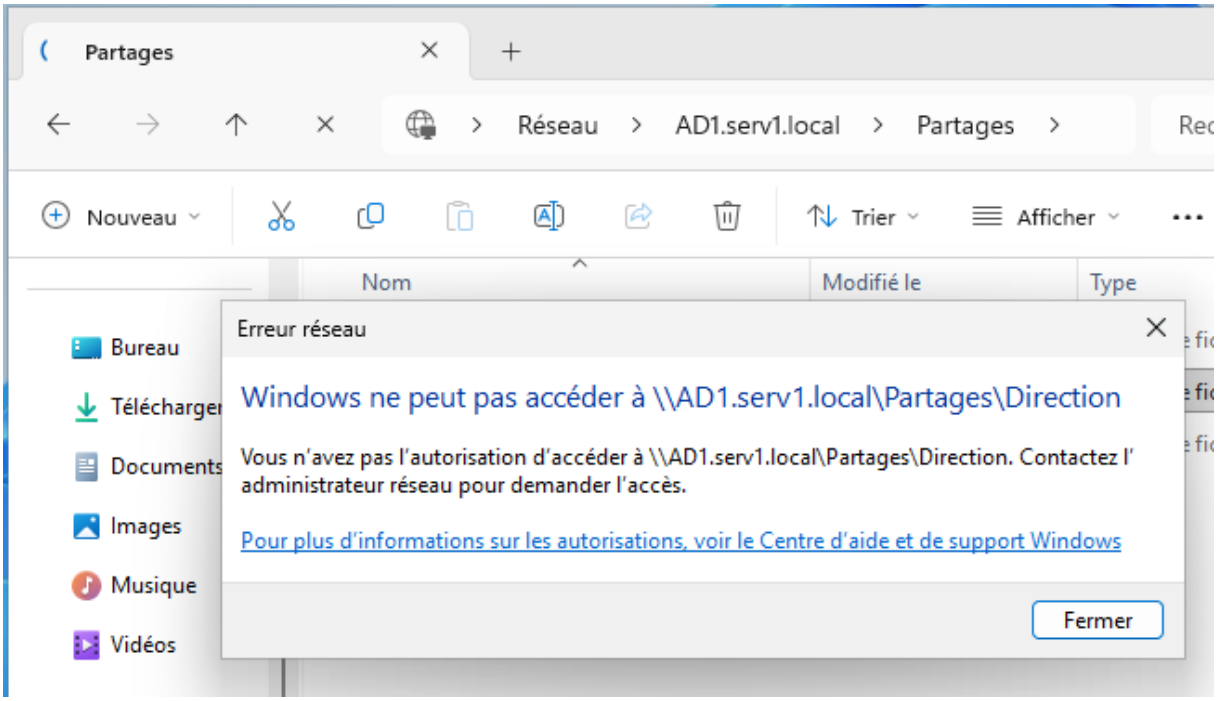
Résultat : Les 20 utilisateurs sont répartis et sécurisés. L'accès est désormais possible via le chemin DFS \\AD1.serv1.local\Partages ou directement via le lecteur P qui a était mappé.

Test effectuer : les tests on était fait un compte utilisateur de RD et on peut voir qu'on a bien accès au fichier RD mais pas aux autres fichiers ce qui montre que les droits fonctionnent bien.




Editeur de gestion des stratégies de groupe
Fichier
Action
Affichage
?
Stratégie GPO_Lecteur_Reseau_I
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Paramètres du logici
Paramètres Windows
Modèles d'administr
Préférences
Paramètres Windows
Applications
Mappages de lec
Environnement
Fichiers
Dossiers
Mappages de lecteurs
Processing
Description
Nom
Ordre
Action
Chemin d'accès
P:
1
Rempl...
\\AD1.serv1.local\Partages


RD
AD1.serv1.local
Partages
RD
Nouveau
Trier
Afficher
Nom
Modifié le
Type
Le dossier est vide.
Bureau
Téléchargem
Documents
Images
Musique
Vidéos
Ce PC
Lecteur de CD (
Lecteur de CD (
Réseau

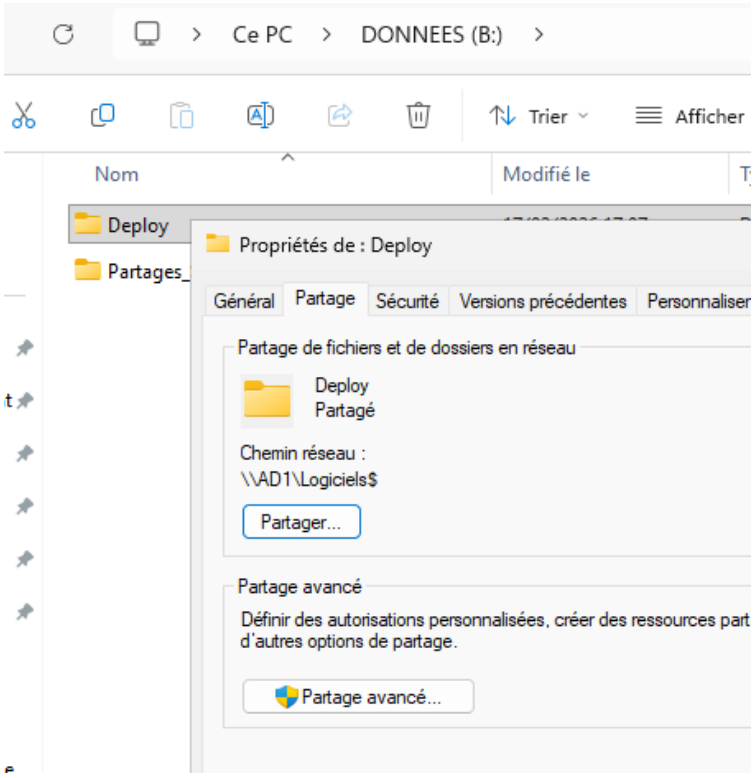

Partages
Réseau
AD1.serv1.local
Partages
Nouveau
Trier
Afficher
Nom
Modifié le
Type
Bureau
Télécharger
Documents
Images
Musique
Vidéos
Erreur réseau
Windows ne peut pas accéder à \\AD1.serv1.local\Partages\Direction
Vous n'avez pas l'autorisation d'accéder à \\AD1.serv1.local\Partages\Direction. Contactez l'administrateur réseau pour demander l'accès.
Pour plus d'informations sur les autorisations, voir le Centre d'aide et de support Windows
Fermer

☑ Bilan de la mission — Objectif atteint. Les droits NTFS sont appliqués et testés : un utilisateur du service RD peut accéder à ses fichiers mais se voit refuser l'accès au dossier Direction.

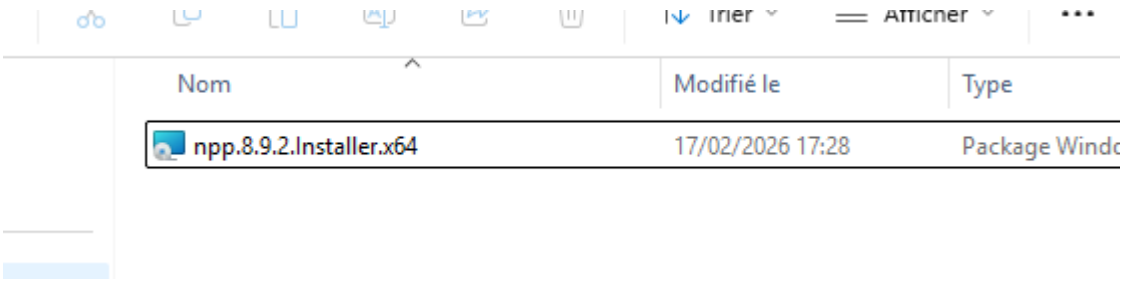
3.7 M4-T1 Déploiement logiciel : GPO d'installation automatique de NotePad++ (.msi).

Procédure de réalisation :

1. **Préparation du point de distribution :** Création d'un dossier C:\Deploy sur le serveur, partagé sous le nom Logiciels$. Les droits de partage sont accordés en **Lecture** au groupe **"Ordinateurs du domaine"** (car c'est la machine qui installe le logiciel au boot, pas l'utilisateur).

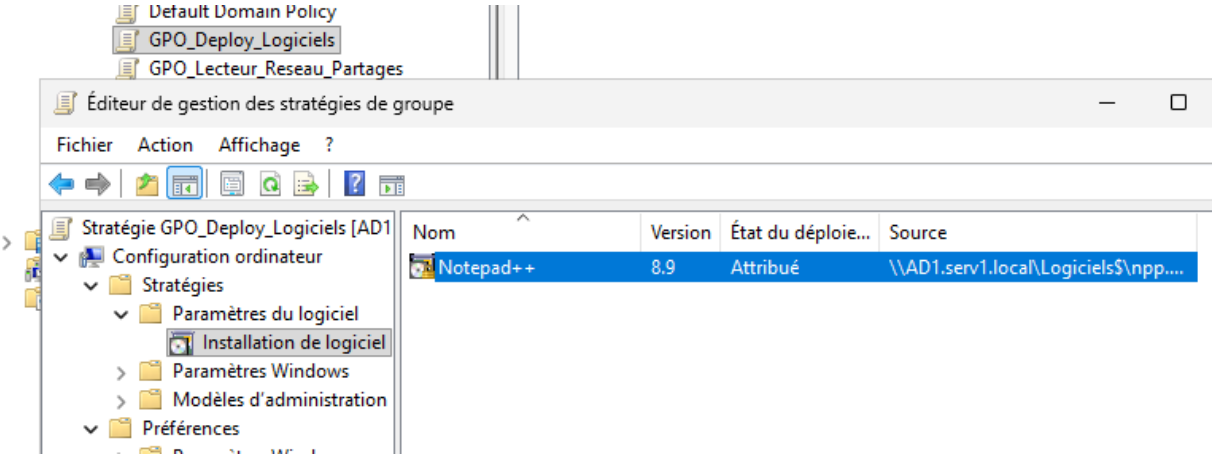


2. **Extraction du paquet :** Téléchargement du fichier .msi de NotePad++ (Windows Installer).

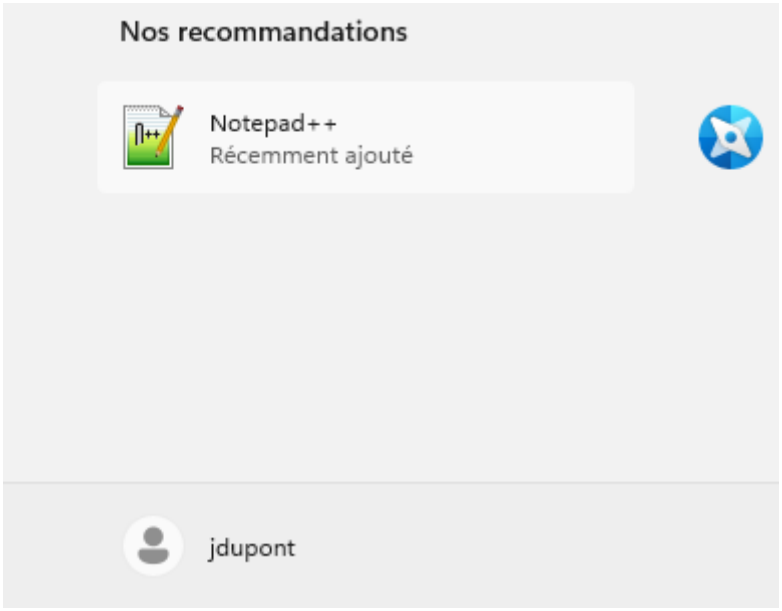


3. **Configuration de la GPO :** Création d'une GPO nommée GPO-Deploy-Logiciels.

   - Navigation vers : Configuration ordinateur > Politiques > Paramètres logiciels > Installation de logiciel.
   - Ajout d'un nouveau paquet en pointant impérativement sur le **chemin réseau UNC** (\\AD1\Logiciels$\npp.8.9.2.Installer.x64.msi) et non le chemin local.
   - Option choisie : **Assigné** (provoque l'installation automatique au prochain démarrage).



Application forcé de la GPO

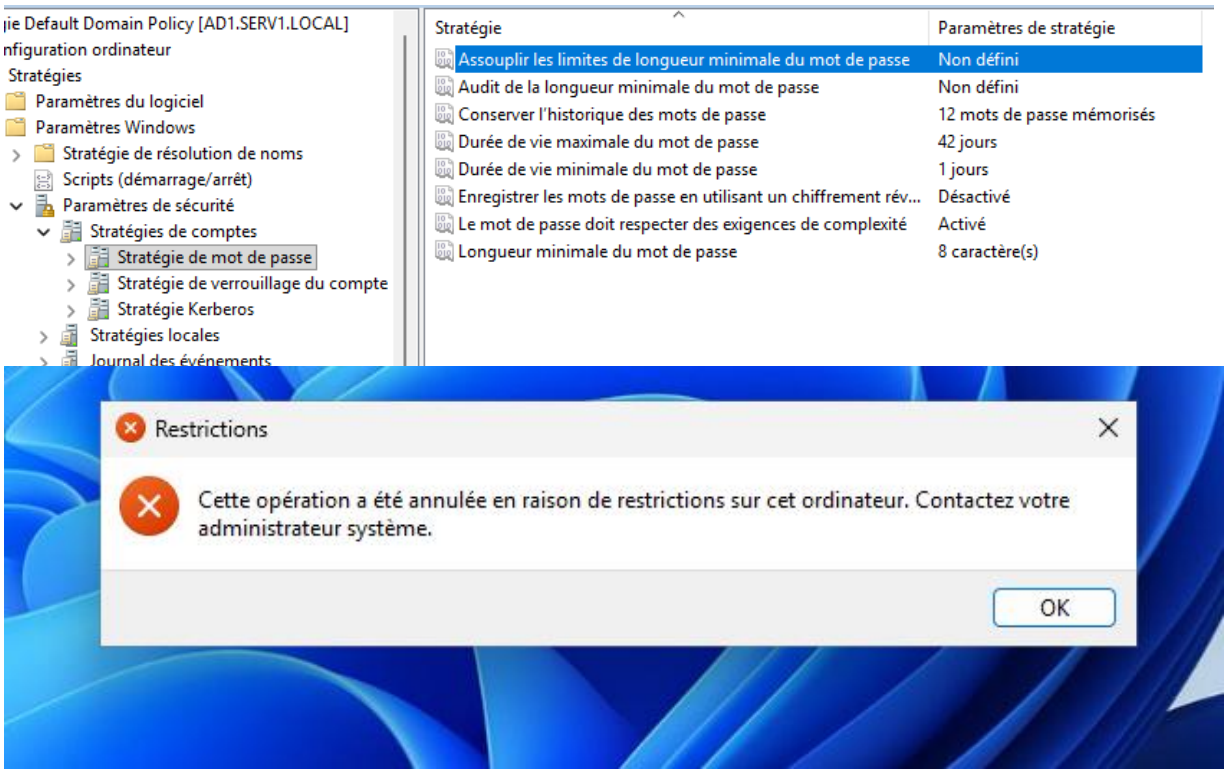


☑ Bilan de la mission — Objectif atteint. Le logiciel est déployé sans intervention humaine sur le parc informatique, facilitant la gestion logicielle..

3.8 M4-T2 GPO de restrictions : Paramétrage du panneau de configuration

Procédure de réalisation :

1. **Restriction du Panneau de Configuration :**
    - Édition d'une GPO USER-Restrictions-Standard.
    - Chemin : Configuration utilisateur > Modèles d'administration > Panneau de configuration.
    - Activation du paramètre : **"Interdire l'accès au Panneau de configuration et aux paramètres du PC"**.



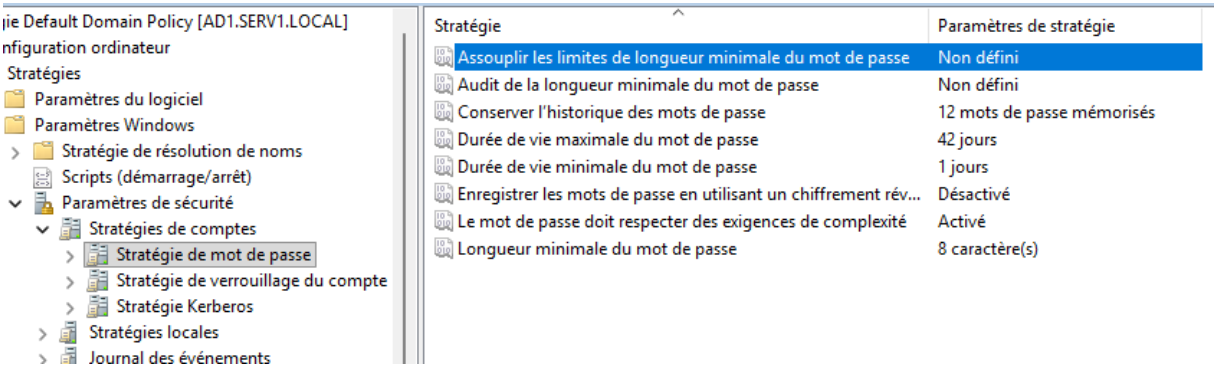
☑ Bilan de la mission — Objectif atteint. Le système est protégé contre les manipulations maladroites et les attaques par force brute (verrouillage de compte après 2 échecs). L'audit permet une traçabilité complète des événements de sécurité.

3.9 M4-T3 GPO d'Audit (Bonus) : Configuration de l'audit des logs de connexion.

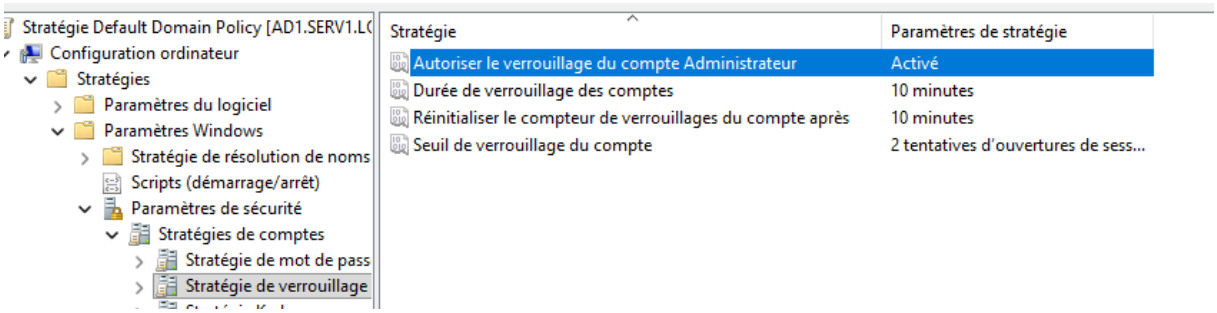
Mise en œuvre d'un durcissement (Hardening) du système pour protéger l'infrastructure contre les erreurs de manipulation des utilisateurs et les tentatives d'intrusion par force brute. Cette mission assure que seuls les administrateurs peuvent modifier les paramètres système et impose une politique de sécurité stricte sur les comptes."

Procédure technique (Réalisation) :

1. **Restriction de l'interface (GPO Utilisateur) :**
    - Création d'une GPO USER-Restrictions-Standard liée à l'OU des utilisateurs.
    - Activation du paramètre : *Configuration utilisateur > Modèles d'administration > Panneau de configuration > Interdire l'accès au Panneau de configuration*.
2. **Politique de mots de passe (GPO Domaine) :**
    - Modification de la Default Domain Policy.
    - Fixation de la longueur minimale à **8 caractères** avec exigence de complexité activée.
    - Paramétrage de l'historique sur **12 mots de passe** pour empêcher la réutilisation immédiate.

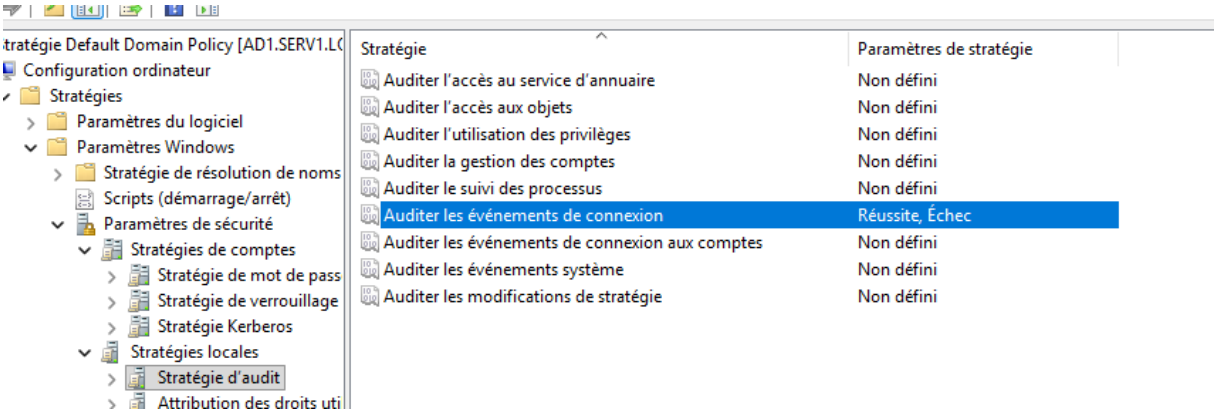


3. **Sécurité Anti Brute-Force :**
    - Configuration du **Seuil de verrouillage à 2 tentatives**.
    - Durée de verrouillage et réinitialisation du compteur réglées sur 10 minutes.

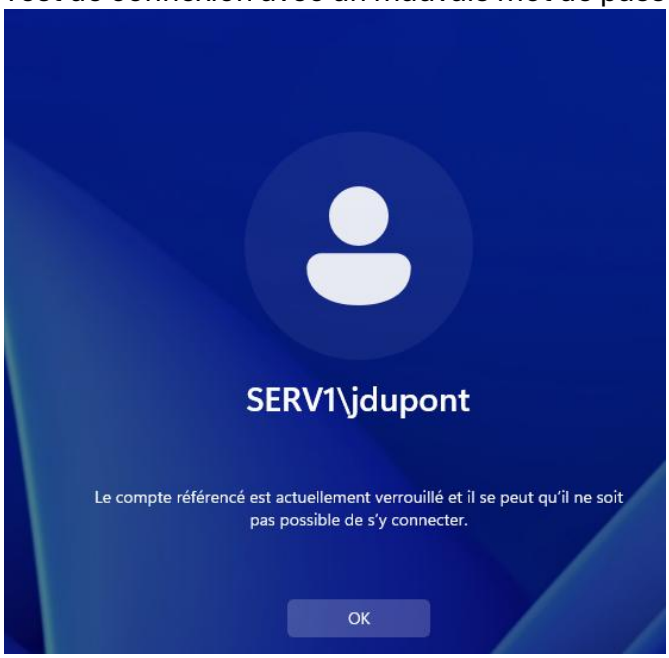


4. **Traçabilité (Audit) :**

   - Activation de l'audit des connexions (Réussites/Échecs) dans les stratégies locales de sécurité pour alimenter l'Observateur d'événements.



5. Test de connexion avec un mauvais mot de passe :



☑ Bilan de la mission — Objectif atteint. La structure de l'annuaire est en place, permettant une isolation claire du client et une organisation logique des ressources par service.

4. Scénario de démonstration

Étape de test	Manipulation à effectuer	Résultat attendu (Preuve)
1. Déploiement Logiciel	Vérifier la présence de Notepad++ sur le bureau ou le menu Démarrer.	Le logiciel est installé sans intervention manuelle.
2. Restriction GPO	Tenter d'ouvrir le Panneau de configuration.	Accès refusé par un message de restriction système.
3. Accès DFS	Ouvrir l'explorateur de fichiers sur le lecteur réseau **P:**.	Accès centralisé aux dossiers Direction, Commercial et RD.
4. Test des Quotas	Tenter de copier un fichier de 10 Go dans le dossier partagé.	Blocage de la copie par le gestionnaire FSRM.
5. Sécurité Compte	Saisir 3 mauvais mots de passe sur l'écran de verrouillage.	Verrouillage automatique du compte utilisateur.
6. Diagnostic GPO	Lancer la commande gpresult /r en invite de commande.	Affichage des GPO "Deploy" et "Restrictions" dans la liste.

5. Bilan Final

Le projet ValorElec est un succès technique. L'infrastructure mise en place répond aux exigences de confidentialité et de disponibilité de l'entreprise. L'utilisation du **DFS** permet une flexibilité totale sur le stockage physique des données, tandis que les **GPO** assurent une maintenance simplifiée du parc informatique. Les principales difficultés rencontrées (résolution DNS et cache DFS) ont été résolues par l'utilisation de noms de domaine pleinement qualifiés (FQDN), garantissant une stabilité optimale.

6. Liste des compétences couvertes (Référentiel SIO)

Ce projet valide les blocs de compétences suivants :

- **B1 : Support et mise à disposition de services informatiques**
    - Répondre aux incidents et aux demandes d'assistance.
    - Accompagner les utilisateurs dans l'utilisation de leur environnement numérique.
- **B2 : Administration des systèmes et des réseaux**
    - Concevoir une infrastructure réseau (AD, DNS).
    - Administrer et sécuriser les services (GPO, NTFS).
- **B3 : Gestion du patrimoine informatique**
    - Gérer des sauvegardes et assurer la continuité de service.
    - Vérifier le respect des règles d'utilisation (Quotas, Restrictions).