Projet EXPERTY 2 – Mise en place de l'infrastructure serveurs

BTS SIO – Option SISR

Atelier de professionnalisation

SOMMAIRE

Glossaire

Définitions des termes techniques utilisés :

AD DS : Active Directory Domain Services
DNS : Domain Name System
GPO : Group Policy Object
AGDLP : Account → Global group → Domain Local group → Permissions
RAID : Redundant Array of Independent Disks
DFS : Distributed File System (Serveur de fichiers)
OU : Organizational Unit
DHCP : Dynamic Host Configuration Protocol

1. Présentation générale du projet

1.1 Contexte

L'entreprise EXPERTY est un cabinet d'expertise comptable fondé en 2012 par Monsieur Bernard SIMON. Elle compte aujourd'hui environ 80 employés répartis sur un site unique situé à Strasbourg.
Grâce à sa croissance rapide et à l'augmentation de son portefeuille clients, le PDG a décidé de faire construire un nouveau bâtiment dans la banlieue ouest de Strasbourg afin d'accompagner ce développement.

Jusqu'à présent, l'entreprise disposait d'une infrastructure informatique basique, composée d'un réseau local récemment modernisé lors d'un précédent projet (refonte du câblage, installation de nouveaux équipements réseau et déploiement d'une image Windows pour les postes clients).
Aujourd'hui, le besoin se déplace vers la mise en place d'une infrastructure serveurs complète, permettant de centraliser la gestion des utilisateurs et des ressources, d'assurer la sécurité des données et de garantir la continuité de service.

Ce projet s'inscrit donc dans la phase d'évolution du système d'information d'EXPERTY, afin d'offrir une architecture plus professionnelle, sécurisée et adaptée à la taille de l'entreprise.

1.2 Objectif du projet

L'objectif principal de ce projet est de concevoir et déployer l'infrastructure serveurs du nouveau bâtiment d'EXPERTY, en appliquant les bonnes pratiques Microsoft et les recommandations de l'ANSSI.

De manière plus détaillée, les objectifs sont les suivants :

- Mettre en place un domaine Active Directory nommé experty.local pour centraliser l'authentification et la gestion des comptes utilisateurs.
- Déployer deux contrôleurs de domaine redondants, assurant la tolérance de panne et la disponibilité du service.
- Configurer les rôles essentiels :
    - DNS / DHCP redondés (répartition 80/20)
    - Serveur de fichiers (DFS) avec structure AGDLP et quotas utilisateurs
    - Service d'impression partagé et gestion via GPO
    - Sauvegardes automatisées et rotation des supports

- Mettre en place des stratégies de groupe (GPO) pour uniformiser les postes clients : fond d'écran, mappage des lecteurs, verrouillage, sécurité, etc.

- Créer des profils itinérants pour faciliter la mobilité des utilisateurs.
- Garantir une administration centralisée et sécurisée grâce à Windows Admin Center et aux consoles MMC.

Ce projet a donc pour finalité d'apporter à EXPERTY une infrastructure stable, redondée, sécurisée et évolutive, tout en respectant les contraintes matérielles et logicielles imposées.

1.3 Contraintes et périmètre

Contraintes techniques

- Les serveurs doivent être physiques, installés sur site (aucune solution Cloud n'est autorisée).
- Tous les services critiques doivent être redondés (Active Directory, DNS, DHCP, fichiers).
- Application stricte des bonnes pratiques Microsoft pour la répartition des rôles et la gestion de la sécurité.
- Respect des préconisations de l'ANSSI pour la politique de mot de passe et la sécurité des comptes.
- Mise en œuvre d'une infrastructure testable en maquette (4 machines virtuelles minimum).
- Respect de la structure AGDLP pour la gestion des permissions.

Périmètre du projet

Inclus :

- Conception et déploiement de l'infrastructure serveurs
- Configuration complète des rôles Windows Server (AD DS, DNS, DHCP, DFS, Impression, Sauvegarde)
- Création des GPO, profils itinérants et dossiers personnels
- Définition du plan d'adressage IP
- Proposition de matériel et plan de déploiement
- Documentation technique (procédures, schémas, annexes)

Exclus :

- Câblage et équipements réseau (déjà réalisés)
- Téléphonie et ERP
- Antivirus, VPN, et sécurité physique des locaux
- Solutions Cloud
- Normes environnementales (DEEE)
- Renouvellement des postes clients

2.Analyse des besoins

2.1 Structure et effectif de l'entreprise

L'entreprise **EXPERTY** regroupe environ **80 employés** répartis sur un seul site, selon la structure suivante :

Service	Effectif	Fonction principale
Direction	1	PDG
Assistante de direction	2	Gestion administrative
Informatique	3	Responsable, admin, alternant
Accueil	2	Standard
Administratif	5	Support interne
Comptabilité	65	Gestion clients, compta

2.2 Analyse fonctionnelle

Besoins généraux

- Authentification centralisée via un domaine Active Directory.
- Gestion hiérarchisée des utilisateurs et des permissions selon les services (modèle AGDLP).
- Accès simplifié aux fichiers partagés, avec distinction entre dossiers communs et personnels.
- Sauvegarde automatique et sécurisée des données critiques.
- Gestion des impressions via un serveur centralisé, avec priorités selon les postes.
- Uniformisation de la configuration des postes grâce à des stratégies de groupe (GPO).
- Disponibilité et redondance pour éviter toute interruption de service.
- Mobilité interne via des profils itinérants pour que les utilisateurs puissent se connecter depuis n'importe quel poste.
- Administration simplifiée depuis un point central (Admin Center ou consoles MMC).

Besoins des utilisateurs

Catégorie d'utilisateur	Besoins principaux

Direction	Accès complet, haute disponibilité, sécurité renforcée
Assistantes / Administratif	Accès aux dossiers partagés, imprimante par défaut, quotas de stockage
Comptables	Accès aux dossiers clients, partages internes sécurisés
Informatique	Accès total à l'AD, aux serveurs et à la console d'administration
Accueil	Accès restreint au réseau et aux applications internes

Contraintes d'usage

- Les collaborateurs doivent pouvoir se connecter du lundi au vendredi de 7h à 20h.
- Les élèves stagiaires (si présents) ont des plages horaires restreintes : 9h à 16h30.
- Les responsables de service ont un accès illimité (24/7).

2.3 Analyse technique

L'analyse technique définit les éléments informatiques à mettre en œuvre pour répondre aux besoins identifiés.

Rôles et fonctionnalités à déployer

Rôle / Service	**Objectif**	**Détails techniques attendus**
Active Directory (AD DS)	Centraliser la gestion des comptes utilisateurs et des groupes	Domaine *experty.local* avec 2 DC redondants
DNS	Résolution de noms interne / externe	Zones *intranet.experty.local* et *www.experty.local*
DHCP	Attribution automatique des adresses IP	Configuration redondée 80/20 sur les 2 DC
DFS	Stockage et partage sécurisé des données	Namespace « partage », quotas 1 Go par utilisateur
Service d'impression	Centraliser la gestion des imprimantes réseau	Installation automatique via GPO, NB recto-verso
Sauvegarde	Protection des données de l'entreprise	Sauvegarde journalière, politique de rotation

GPO	Standardiser la configuration des postes clients	Fond d'écran, mappage lecteurs, restrictions
Profils itinérants	Mobilité des utilisateurs	Sauvegarde du profil sur le serveur de fichiers
Outils d'administration	Gérer les serveurs à distance	Windows Admin Center, MMC, Server Manager

Infrastructure matérielle prévue

- 2 serveurs physiques (pour DC1 et DC2)
- 1 serveur dédié aux fichiers et sauvegardes (DFS)
- 1 serveur pour les impressions
- 1 client Windows 10/11 pour les tests de la maquette
- Onduleur et support de sauvegarde local (disque ou bande)

Exigences de sécurité

- Mots de passe conformes aux préconisations ANSSI (longueur, complexité, durée de vie).
- Application stricte de la méthode AGDLP pour les permissions.
- Dossiers personnels sécurisés accessibles uniquement à l'utilisateur et au service informatique.
- Limitation des privilèges utilisateurs (pas d'administrateurs locaux).
- Blocage des accès sensibles (cmd, gestion réseau).

3.Étude et conception de la solution

3.1 Architecture logique

Afin de répondre aux besoins de l'entreprise EXPERTY et d'assurer la haute disponibilité des services, une infrastructure à trois serveurs principaux et un poste client a été conçue.
Cette architecture respecte les bonnes pratiques Microsoft tout en restant compatible avec les contraintes matérielles de la maquette.

Nom de la machine	Rôles principaux	Description
DC1	Active Directory, DNS, DHCP (primaire)	Contrôleur de domaine principal hébergeant les rôles

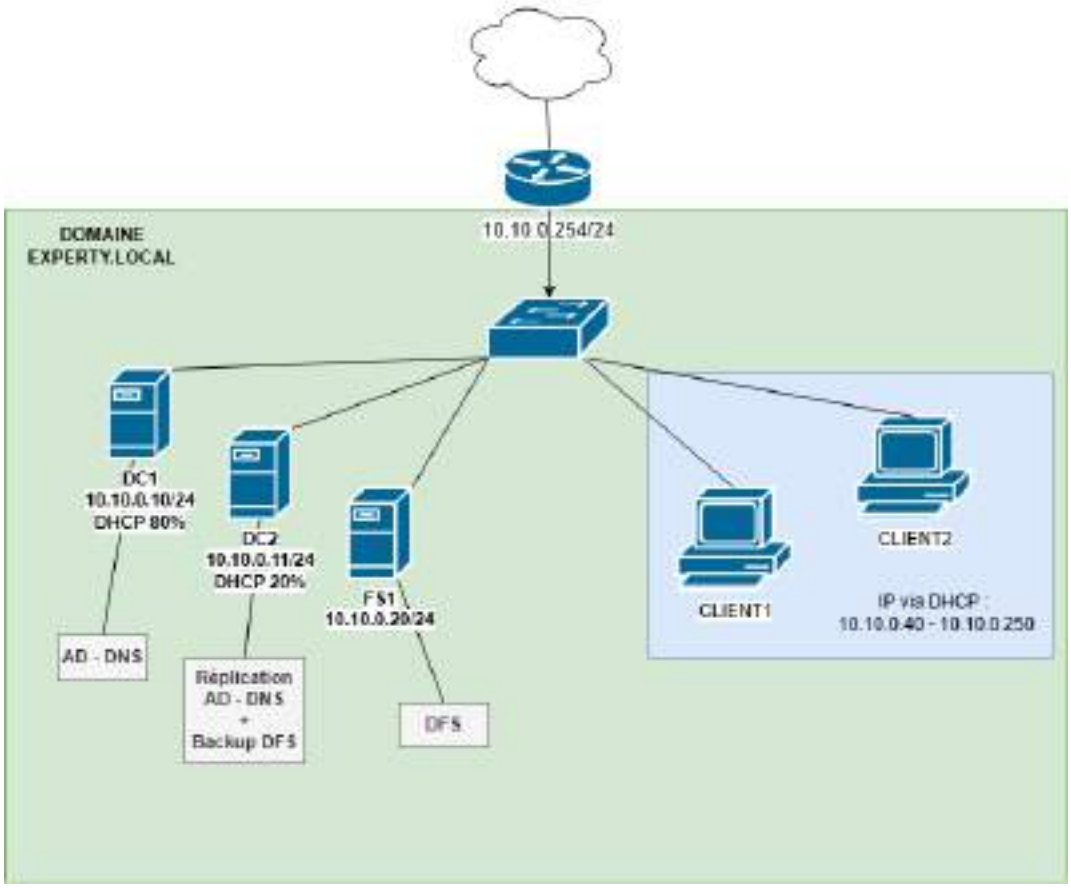
		d’authentification et de résolution de noms
DC2	Active Directory, DNS, DHCP (secondaire)	Contrôleur de domaine secondaire pour la redondance et la reprise d’activité
FS1	Serveur de fichiers, DFS, impression, sauvegarde	Centralisation des données utilisateurs et des impressions
CLIENT1	Poste utilisateur Windows 10/11	Poste client intégré au domaine pour les tests fonctionnels

L’ensemble de ces machines virtuelles sera hébergé sur un poste physique à l’aide de **VMware Workstation**, dans le cadre de la maquette.

Fonctionnement global

- Les utilisateurs s’authentifient sur le domaine experty.local via AD DS.
- Le DNS interne assure la résolution des noms locaux.
- Le DHCP distribue dynamiquement les adresses IP aux clients.
- Les données sont stockées sur le serveur de fichiers FS1, avec un DFS Namespace nommé partage.
- Une sauvegarde journalière protège les données critiques.
- Les imprimantes réseau sont déployées automatiquement par GPO.

Schéma logique



3.2 Plan d'adressage IP

L'adressage IP a été conçu pour offrir une gestion simple et éviter les conflits.
Le réseau interne de l'entreprise utilise une plage **10.10.0.0/24**, adaptée à la taille du site et compatible avec les besoins actuels.

Machine	Adresse IP	Masque	Passerelle	Services
DC1	10.10.0.10	255.255.255.0	10.10.0.254	DNS et DHCP primaire
DC2	10.10.0.11	255.255.255.0	10.10.0.254	DNS et DHCP secondaire (20%)
FS1	10.10.0.20	255.255.255.0	10.10.0.254	DFS, impression et sauvegarde
CLIENT1	DHCP	255.255.255.0	10.10.0.254	Poste client test

Répartition DHCP (80/20)

- DC1 (primaire) : 10.10.0.40 → 10.10.0.250 (80%)
- DC2 (secondaire) : 10.10.0.40 → 10.10.0.250 (20%)
- Réservation des adresses fixes pour les serveurs et les périphériques réseau.

Avantages

- Plan clair, simple à maintenir et à documenter.
- Redondance assurée par la double configuration DHCP et DNS.
- Possibilité d'évolution future (sous-réseaux par service si extension).

3.3 Arborescence Active Directory

Une organisation logique de l'annuaire Active Directory a été définie afin de faciliter la gestion des utilisateurs et des stratégies de sécurité.
L'arborescence respecte les principes du modèle **AGDLP** (Account → Global Group → Domain Local Group → Permissions).

Structure des OU (Organizational Units)

OU	**Contenu**	**Description**
Utilisateurs	Comptes utilisateurs de chaque service	Classés par sous-OU
├── Direction	Compte du PDG et de l'assistante	Accès total au partage Direction
├── Informatique	Admin réseau et techniciens	Accès complet à tous les serveurs
├── Comptabilité	Responsables et collaborateurs comptables	Accès au partage "Comptabilité"
├── Administratif	Gestion RH et secrétariat	Accès restreint
├── Accueil	Standardistes	Accès limité aux dossiers communs
Ordinateurs	Objets des postes clients	Affectés par service
Groupes	Groupes globaux et locaux	Gestion des permissions AGDLP
Serveurs	Objets des serveurs du domaine	DC1, DC2, FS1

Principe AGDLP appliqué

- **A (Accounts)** → Comptes utilisateurs (ex. u.martin)
- **G (Global Groups)** → Groupes par service (GG_Compta, GG_Admin)
- **DL (Domain Local Groups)** → Groupes par ressource (DL_PartageCompta)
- **P (Permissions)** → Droits NTFS sur les dossiers partagés

3.4 Politiques de sécurité (GPO)

Les **stratégies de groupe** permettent de centraliser et d'uniformiser la configuration des postes clients du domaine.
Elles ont été définies selon les recommandations de l'**ANSSI** et les besoins d'**EXPERTY**.

Nom de la stratégie	Objectif	Paramètres principaux
Sécurité_MotDePasse	Appliquer une politique de mot de passe forte	Min. 10 caractères, majuscules, chiffres, symboles, renouvellement 90j
FondEcran_Experty	Uniformiser le fond d'écran	Logo EXPERTY, modification interdite
LecteursReseaux	Mappage automatique des lecteurs	T: "Tous" / P: "Personnel" / I: "Informatique"
Restriction_Utilisateur	Renforcer la sécurité	Blocage invite de commande, panneau de config et carte réseau
MiseEnVeille	Gestion de l'énergie	Écran en veille après 15 minutes
Navigateur	Uniformisation navigateur Firefox	Page d'accueil : *intranet.experty.local*
Imprimante_Réseau	Déploiement imprimante par défaut	Noir et blanc, recto-verso

Ces stratégies sont appliquées à des **OU spécifiques** (ex. *Utilisateurs\Comptabilité*) ou à l'ensemble du domaine selon leur portée.

Avantages

- Sécurité renforcée et postes conformes à la politique interne.
- Administration simplifiée et homogène.
- Réduction des erreurs utilisateur et meilleure maintenance à distance.

4. Choix techniques et justification

4.1 Choix de l'OS serveur

L'infrastructure d'EXPERTY repose sur le système Windows Server 2022, dernière version du système d'exploitation serveur de Microsoft.
Ce choix se justifie par sa stabilité, sa compatibilité étendue avec les rôles demandés (AD DS, DNS, DHCP, DFS, impression, sauvegarde), et sa prise en charge de la gestion moderne via Windows Admin Center.

Nous utiliserons la version avec l'interface graphique complète qui est plus intuitive et simplifie l'administration AD/DNS/DHCP et la formation des utilisateurs. Mais aussi pour les démonstrations lors de la soutenance.

4.2 RAID

Dans le cadre de la maquette, le choix du RAID 1 a été retenu pour l'ensemble des serveurs.
Ce mode de redondance, appelé "miroir", consiste à dupliquer les données sur deux disques identiques, assurant une tolérance de panne simple et efficace.

Ce choix se justifie par :

- la simplicité de configuration dans un environnement virtuel VMware,
- la sécurité des données en cas de défaillance d'un disque,
- une cohérence technique entre tous les serveurs de l'infrastructure.

Bien que d'autres configurations telles que le RAID 5 offrent de meilleures performances et une meilleure utilisation de la capacité disque, le RAID 1 reste le plus adapté pour une maquette pédagogique, où la stabilité et la clarté de la démonstration priment sur les performances.

4.3 Sauvegarde

L'objectif de la stratégie de sauvegarde mise en place pour la société EXPERTY est de garantir la sécurité, la disponibilité et la récupération rapide des données critiques de l'entreprise en cas de panne, de suppression accidentelle ou d'incident matériel.
Elle vise à assurer la continuité d'activité tout en respectant les bonnes pratiques de l'ANSSI et les politiques internes de l'entreprise.

Types de données à sauvegarder
Les éléments suivants sont considérés comme critiques et doivent être inclus dans la politique de sauvegarde :

- Données stockées sur les serveurs de fichiers (lecteurs partagés, profils utilisateurs, DFS).
- Données des répertoires personnels (lecteurs P:).
- Données administratives internes et documents comptables.
- Paramètres de configuration et bases de données des serveurs (Active Directory, DNS, DHCP, GPO).
- Scripts, procédures et fichiers de configuration du service informatique.

Méthode de sauvegarde retenue
La sauvegarde sera effectuée quotidiennement, à l'aide d'un logiciel de sauvegarde automatisé tel que **Windows Server Backup**.

Deux niveaux de sauvegarde sont prévus :
- **Sauvegarde complète hebdomadaire** : l'intégralité des données est copiée sur le support de sauvegarde.
- **Sauvegarde incrémentielle quotidienne** : seules les modifications depuis la dernière sauvegarde sont enregistrées.

Planification

Type de sauvegarde	Fréquence	Heure d'exécution	Support	Rétention
Complète	Chaque week-end (samedi 22h)	Nuit	Disque dur externe / NAS	1 mois
Incrémentielle	Tous les jours ouvrés (20h)	Nuit	Disque dur externe / NAS	7 jours

Supports de sauvegarde
Les sauvegardes seront stockées sur disques externes dédiés connectés aux serveurs de fichiers.
Un roulement de supports sera mis en place (exemple : 3 disques étiquetés Semaine 1 / Semaine 2 / Semaine 3) afin de prévenir toute perte simultanée.

Un NAS interne pourra également être utilisé comme destination intermédiaire, avant l'export sur disque externe pour conservation hors site.

Sauvegarde dans la maquette VMware
Dans la maquette de démonstration, une sauvegarde simplifiée sera mise en place afin d'illustrer le fonctionnement du service :

- Utilisation de Windows Server Backup pour effectuer une sauvegarde manuelle du volume D: (partages).
- Sauvegarde stockée dans un dossier simulant un disque externe (ex. E:\Sauvegardes).

4.4 Redondance

La tolérance de panne et la continuité de service sont des éléments essentiels pour une infrastructure d'entreprise.
L'objectif est d'assurer que les services critiques restent disponibles même en cas de défaillance d'un serveur.

Mécanismes de redondance mis en place

Service	Type de redondance	Implémentation
Active Directory (AD DS)	Réplication entre 2 DC	DC1 et DC2 hébergent chacun une copie complète du domaine *experty.local*
DNS	Secondaire intégré à AD	Zones DNS répliquées automatiquement entre DC1 et DC2
DHCP	Redondance 80/20	DC1 (80%) et DC2 (20%) via protocole Failover
Fichiers (DFS)	Espace de noms unique + réplication	Serveur FS1 héberge l'espace "partage" avec possibilité de répliquer sur un second volume
Sauvegarde	Multi-supports et copies externes	Rotation quotidienne des disques et externalisation hebdomadaire

Bénéfices de la redondance

- Haute disponibilité : les utilisateurs restent connectés même en cas de panne d'un serveur.
- Réduction des interruptions de service : basculement automatique DHCP/DNS.
- Sécurité accrue : données du domaine et profils utilisateurs préservés.
- Souplesse de maintenance : possibilité de redémarrer un serveur sans impacter le réseau.

5.Déploiement et configuration

5.1 Installation et configuration des serveurs

L'infrastructure de la société EXPERTY repose sur trois serveurs Windows Server 2022 et un poste client Windows 11 Pro, tous virtualisés sous VMware Workstation.

Étapes de déploiement :

Création des machines virtuelles

- Chaque serveur a été créé avec 2 processeurs, 4 Go de RAM et deux disques virtuels configurés en RAID 1 (miroir).
- Les fichiers ISO de Windows Server 2022 et Windows 11 Pro ont été montés pour l'installation initiale.
- Le type de carte réseau sélectionné est VMnet8 (NAT), configuré sur le sous-réseau 10.10.0.0/24.

Paramétrage réseau

Les adresses IP statiques ont été définies comme suit :

Machine	Adresse IP	Masque	Passerelle	DNS primaire	DNS secondaire
DC1	10.10.0.10	255.255.255.0	10.10.0.254	10.10.0.10	10.10.0.11
DC2	10.10.0.11	255.255.255.0	10.10.0.254	10.10.0.11	10.10.0.10
FS1	10.10.0.20	255.255.255.0	10.10.0.254	10.10.0.10	10.10.0.11
CLIENT1	DHCP	255.255.255.0	10.10.0.254	Automatique	Automatique

Installation des rôles et fonctionnalités

- Installation de Active Directory Domain Services (AD DS) sur DC1 puis promotion en contrôleur de domaine avec le nom de domaine experty.local.
- Installation de DNS et DHCP sur DC1 et DC2 pour assurer la redondance (80/20).
- Installation de DFS, impression et sauvegarde sur FS1.
- Intégration du poste CLIENT1 dans le domaine experty.local.

Configuration RAID

- Tous les serveurs utilisent une configuration RAID 1 simulée sur deux disques virtuels.
- Objectif : assurer la redondance et simplifier la maintenance.

Tests initiaux

- Ping entre chaque machine.
- Vérification de la résolution DNS (nslookup experty.local).
- Attribution d'adresse IP via DHCP sur le poste client.

5.2 Mise en place des rôles

Active Directory (AD DS)

- Création du domaine experty.local sur DC1.
- Ajout de DC2 en second contrôleur de domaine pour assurer la réplication automatique des objets et la tolérance de panne.
- Mise en place d'une arborescence d'unités d'organisation (OU) :
    - Utilisateurs
    - Ordinateurs
    - Groupes
    - Sous-OU : Direction, Informatique, Comptabilité, Administratif, Accueil

DNS

- Zone principale *experty.local* créée automatiquement avec AD DS.
- Zones supplémentaires :
    - *intranet.experty.local* → hébergé sur FS1 (page d'accueil Intranet).
    - *www.experty.local* → redirigé vers le même serveur.
- Réplication DNS activée entre DC1 et DC2.

DHCP

- DC1 : plage 10.10.0.50 à 10.10.0.200 (80%)
- DC2 : plage 10.10.0.201 à 10.10.0.250 (20%)
- DHCP Failover configuré en mode Load Balance 80/20.
- Options configurées :
    - Passerelle : 10.10.0.254
    - DNS : 10.10.0.10, 10.10.0.11
    - Domaine : experty.local

DFS (Distributed File System)

- Installation du rôle sur FS1.
- Création d'un espace de noms unique nommé \\experty.local\partage.
- Arborescence :
    - *experty.local**partage**Direction*
    - *experty.local**partage**Comptabilité*
    - *experty.local**partage**Informatique*
    - *experty.local**partage**Administratif*
    - *experty.local**partage**Accueil*

- Droits NTFS appliqués selon la méthode AGDLP :
    - Groupes globaux par service (GG_Compta, GG_Admin, etc.)
    - Groupes locaux (DL_Compta, DL_Admin, etc.)
    - Attribution des permissions (Lecture / Modification / Contrôle total).

Service d'impression

- Rôle Print and Document Services installé sur FS1.
- Ajout d'une imprimante virtuelle "Microsoft Print to PDF" simulant l'imprimante réseau.
- Partage sous le nom \\FS1\Imprimante_Reseau.
- Déploiement via GPO :
    - Imprimante ajoutée automatiquement pour tous les utilisateurs.
    - Impression par défaut en noir et blanc recto-verso.
    - Priorité donnée aux responsables de service.

Service de sauvegarde

- Installation de Windows Server Backup sur FS1.
- Création d'une tâche planifiée :
    - Type : Sauvegarde complète quotidienne.
    - Source : Partages DFS + dossiers de profils.
    - Destination : Deuxième disque virtuel (E:).
    - Heure : 23h00.
- Politique de rotation : 7 jours de rétention minimum.

Profils itinérants

- Dossier partagé : *FS1**Profils*
- Chemin de profil défini dans les propriétés des comptes utilisateurs AD : *FS1**Profils**%username%*
- Permissions :
    - Utilisateur : Contrôle total sur son dossier.
    - Administrateurs : Lecture seule.

5.3 Configuration des quotas utilisateurs

Pour éviter la saturation du stockage, un quota de 1 Go a été défini pour chaque dossier personnel utilisateur.

Étapes :

1 - Activation de la gestion des quotas sur FS1 (fsrm.msc).
2 - Application d'un modèle de quota :

- Limite : 1 Go par utilisateur.

- Alerte : 90% (mail ou notification locale).

3 - Surveillance automatique via l'outil File Server Resource Manager (FSRM).

Ce mécanisme permet d'optimiser l'espace disque tout en avertissant les utilisateurs avant dépassement.

5.4 Profils itinérants

Les profils itinérants ont été déployés afin que chaque utilisateur retrouve son environnement personnel depuis n'importe quel poste du domaine.

Étapes de mise en place :

1 - Création du partage *\\FS1\Profils* avec droits :
- Administrateurs : Lecture seule.
- Chaque utilisateur : Contrôle total sur son propre dossier.

2 - Dans Active Directory, configuration du chemin de profil :
\\FS1\Profils\%username%

3 - Vérification du fonctionnement :
- Connexion d'un utilisateur depuis CLIENT1.
- Création automatique du dossier utilisateur sur FS1.
- Test de déconnexion/reconnexion depuis un autre poste (persistance du profil).

Avantages :
- Les données utilisateur sont centralisées et sécurisées sur le serveur.
- Simplifie la maintenance des postes clients.
- Compatible avec les quotas et les sauvegardes quotidiennes.

6. Matériel et coûts estimatifs

L'objectif de cette partie est d'évaluer le matériel nécessaire à la mise en place de la nouvelle infrastructure serveurs de l'entreprise EXPERTY.

L'étude prend en compte :
- Les besoins en performance (80 utilisateurs)
- La tolérance de panne (RAID, redondance, sauvegardes)
- La pérennité du matériel (prévision sur 5 ans d'utilisation)
- Le rapport coût / performance / fiabilité

L’entreprise souhaite disposer de serveurs physiques sur site (pas de Cloud) et de systèmes redondés pour garantir la continuité de service.

L’infrastructure proposée
L’architecture repose sur trois serveurs physiques principaux, complétés par un système de sauvegarde et un onduleur pour la protection électrique.
Le matériel proposé correspond à des équipements professionnels d’entrée/milieu de gamme, adaptés à une PME de 80 employés.

Détail du matériel

Équipement	Modèle	Spécifications principales	Quantité	Prix unitaire (€)	Total (€)
Serveur DC1	Dell PowerEdge R350	Xeon Silver, 32 Go RAM, 2×1 To SSD en RAID 1	1	2 500 €	2 500 €
Serveur DC2	Dell PowerEdge R350	Xeon Silver, 32 Go RAM, 2×1 To SSD en RAID 1	1	2 500 €	2 500 €
Serveur FS1 (fichiers / DFS / sauvegarde)	Dell PowerEdge R550	Xeon Silver, 64 Go RAM, 4×2 To HDD en RAID 1	1	3 000 €	3 000 €
Baie de stockage / Rack 12U	StarTech 12U	Support serveurs, ventilation intégrée	1	800 €	800 €
Onduleur (UPS)	APC Smart-UPS 1500VA	Autonomie ~15 min, protection électrique	2	400 €	800 €
Disques de sauvegarde externes	Seagate Exos 4 To	Rotation de 7 disques (1 par jour ouvré)	7	100 €	700 €
Switch Gigabit (24 ports)	Netgear ProSAFE GS324	Administration simple, VLAN support	1	150 €	150 €
Câblage, accessoires et ventilation	–	Baie + alimentation + organisation câbles	–	250 €	250 €

Sous-total matériel = 10 700 €

Logiciels et licences

Élément logiciel	Type	Détails / Justification	Prix unitaire (€)	Total (€)
Windows Server 2022 Standard Lien	Licence serveur	3 licences (DC1, DC2, FS1)	800 €	2 400 €
Windows Server CAL (Client Access License) Lien	Licence utilisateur	80 utilisateurs	30 €	2 400 €

Total estimé licences = 4 800 €

Justification des choix

- Performances
  Les serveurs choisis disposent de processeurs Xeon et de 32 à 64 Go de RAM, largement suffisants pour un domaine de 80 utilisateurs.
  Le RAID 1 assure la redondance tout en maintenant une bonne performance de lecture/écriture.

- Fiabilité
  L'utilisation de matériels Dell et APC garantit une qualité professionnelle, avec des composants conçus pour fonctionner en continu (24h/24, 7j/7).

- Sécurité
  - Onduleurs pour protéger contre les coupures électriques.
  - RAID 1 pour la tolérance de panne disque.
  - Sauvegardes quotidiennes sur supports multiples.

- Évolutivité
  La baie permet d'ajouter facilement de nouveaux serveurs ou volumes DFS à l'avenir, sans modification majeure de l'infrastructure.

Résumé global des coûts

Catégorie	Montant estimé (€)
Matériel serveurs et stockage	10 700 €
Licences logicielles	4 800 €
Total général estimé TTC	**15 500 €**

Le coût global estimé de 15 500 € TTC pour la mise en place de l'infrastructure EXPERTY est cohérent avec la taille et les besoins de l'entreprise.

7. Planning de déploiement

Le déploiement de la nouvelle infrastructure a été planifié sur une période de 4 semaines, en tenant compte des phases de préparation, d'installation, de configuration et de validation.
Ce planning a été conçu de manière réaliste, tout en restant adapté à la taille du projet et aux ressources disponibles.

Il comprend la mise en place complète des serveurs (Active Directory, DNS, DHCP, DFS, sauvegardes), la configuration du stockage RAID, ainsi que la documentation technique et la formation du personnel informatique.

Étape	Tâche	Responsable	Durée estimée	Commentaire
Phase 1 – Préparation (Semaine 1)				
1.1	Étude des besoins et validation du plan d'adressage IP	Équipe projet	1 jour	Inclut validation avec le service informatique
1.2	Commande du matériel (serveurs, disques, licences)	Responsable info	2 jours	Phase administrative
1.3	Réception et vérification du matériel	Technicien	1 jour	Contrôle des serveurs reçus
Phase 2 – Installation (Semaine 2)				
2.1	Installation physique des serveurs	Technicien	1 jour	Montage en baie, câblage
2.2	Installation de Windows Server sur chaque machine	Technicien	2 jours	Configuration IP, renommage, mises à jour
2.3	Configuration du RAID et partitionnement	Technicien	1 jour	RAID 1 pour système, RAID 5 pour données

Phase 3 – Configuration des rôles (Semaine 3)				
3.1	Mise en place des contrôleurs de domaine (AD DS, DNS, DHCP)	Administrateur	2 jours	Redondance DHCP 80/20
3.2	Création des OU, utilisateurs et GPO	Administrateur	2 jours	Application AGDLP + GPO ANSSI
3.3	Installation et configuration du DFS	Administrateur	1 jour	Création des partages + droits
3.4	Configuration du serveur de sauvegarde	Technicien	1 jour	Planification sauvegarde complète / incrémentielle
Phase 4 – Validation et documentation (Semaine 4)				
4.1	Tests fonctionnels (authentification, DFS, sauvegarde)	Équipe projet	2 jours	Vérification des redondances
4.2	Rédaction de la documentation technique	Équipe projet	2 jours	Procédures + schémas
4.3	Présentation et transfert de compétences	Responsable info	1 jour	Formation du service interne

8. Conclusion

Le projet **EXPERTY 2** avait pour objectif de concevoir et de déployer **une infrastructure serveurs complète et sécurisée** pour accompagner la croissance de l'entreprise EXPERTY.
L'enjeu principal était de mettre en place une solution fiable, centralisée et redondée, tout en respectant les bonnes pratiques Microsoft et les préconisations de l'ANSSI.

Au terme de ce projet, une maquette fonctionnelle composée de trois serveurs et d'un poste client a été réalisée.

Cette infrastructure intègre l'ensemble des rôles demandés :

- Active Directory pour la gestion centralisée des comptes utilisateurs et groupes,
- DNS et DHCP pour la gestion du réseau et la redondance des services,
- DFS pour le partage et la structuration des données,
- Sauvegarde automatisée pour la sécurité des informations,
- Profils itinérants et stratégies de groupe (GPO) pour assurer la cohérence et la personnalisation des postes utilisateurs,
- Service d'impression centralisé et déployé via GPO.

La solution mise en place permet à l'entreprise EXPERTY de bénéficier d'un système informatique stable, évolutif et facile à administrer.
Les mécanismes de redondance garantissent la continuité de service, tandis que la sauvegarde quotidienne et la gestion des quotas assurent la sécurité et l'intégrité des données.

Ce projet a également permis de mettre en pratique de nombreux savoirs techniques acquis durant la formation BTS SIO option SISR :

- gestion d'un domaine Windows Server,
- configuration des rôles réseaux,
- mise en œuvre d'une architecture redondée,
- administration via GPO et DFS,
- documentation technique complète.

En conclusion, la maquette EXPERTY démontre la faisabilité et la pertinence d'une telle infrastructure dans un environnement professionnel.
Elle répond pleinement aux besoins exprimés par l'entreprise : fiabilité, sécurité, accessibilité et centralisation.
Cette expérience a renforcé les compétences techniques et méthodologiques nécessaires à la gestion d'un projet d'infrastructure réseau d'entreprise.

9. Table des illustrations

À générer automatiquement dans Word.

Annexes

Les annexes ne comptent pas dans les 20 pages principales.

A.1 Procédures détaillées (avec captures d'écran)

Création domaine AD

Configuration GPO

DHCP redondé

DFS namespace

Mise en place de la sauvegarde planifiée

A.2 Scripts PowerShell éventuels

(Ex : création d'utilisateurs, GPO, mappage lecteurs)

A.3 Captures de la maquette (VirtualBox)

Vue réseau, configuration IP, tests ping

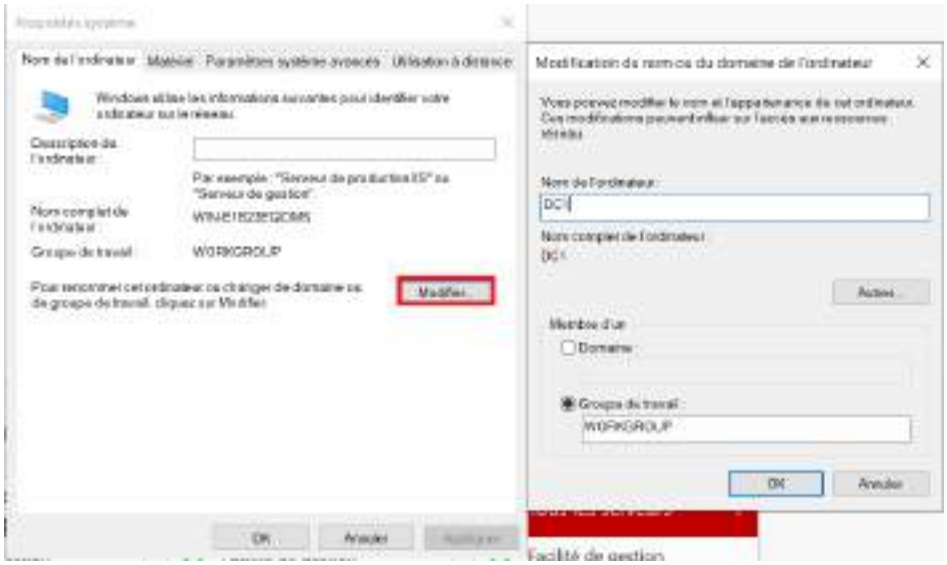
Capture Windows Admin Center ou Server Manager

Préparer une VM Windows Server 2022

Il faut de préférence 2CPU et 4Go de RAM. Si on utilise VMware, il faut penser à désactiver le DHCP VMware.
On privilégie la version graphique pour des facilités de paramétrages :

Une fois l'installation terminée, on configure une IP fixe.
Win + R → ncpa.cpl → Propriété de la carte réseau
On désactive IPv6 pour éviter les conflits et on configure IPv4 :

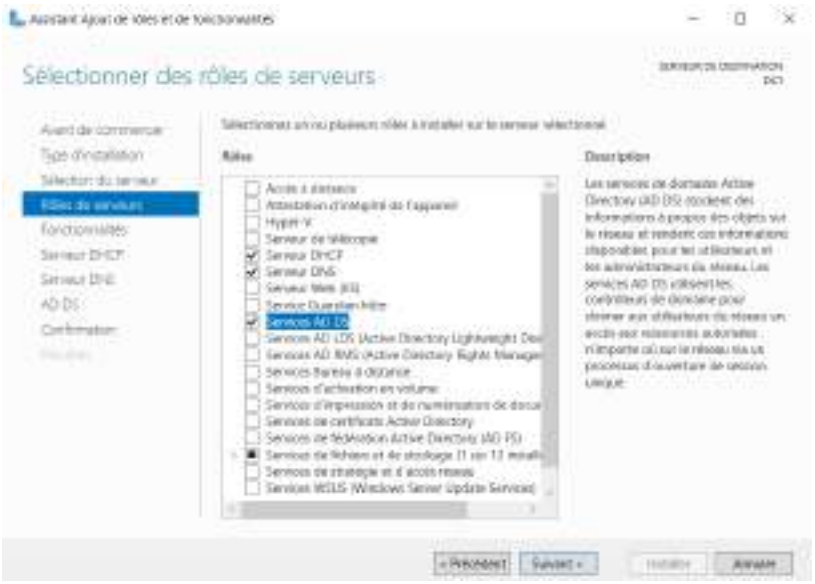
On renomme la machine aussi :
Win+R → sysdm.cpl
Nom de l'ordinateur → Modifier



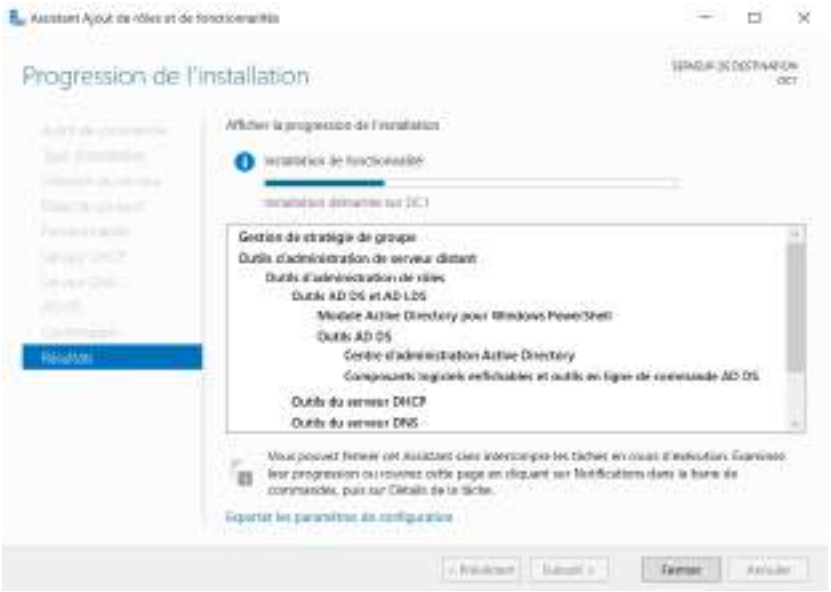
Autoriser le PING pour tester la connectivité :
Ouvrir un powershell
Enable-NetFirewallRule -Name FPS-ICMP4-ERQ-In

Création du domaine Active Directory & Configuration DNS

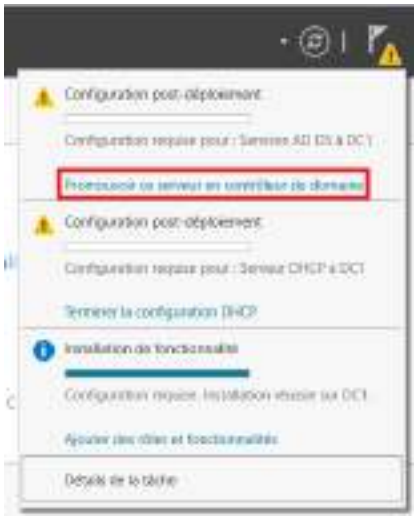
Il faut installer le **rôle AD** dans le **Gestionnaire de serveur**
Cliquez sur Gérer → Ajouter des rôles et fonctionnalités
Dans Rôles de serveurs on coche Services AD DS + Serveur DNS



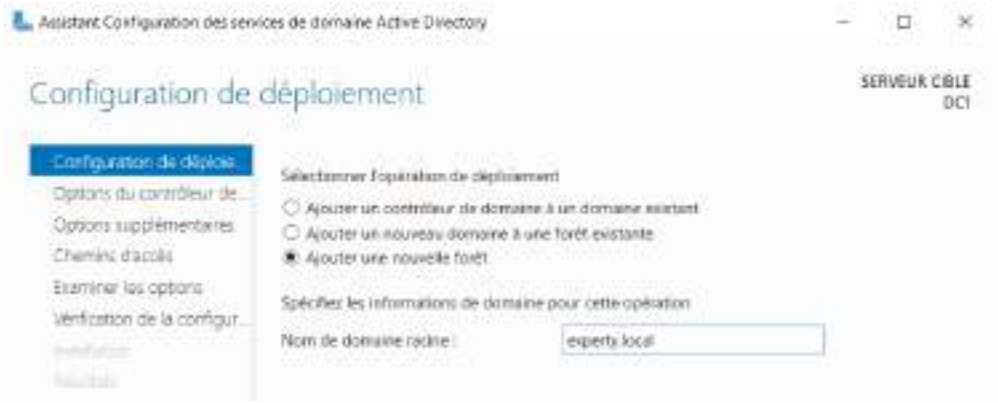
On peut laisser par défaut, faire Suivant et Installer

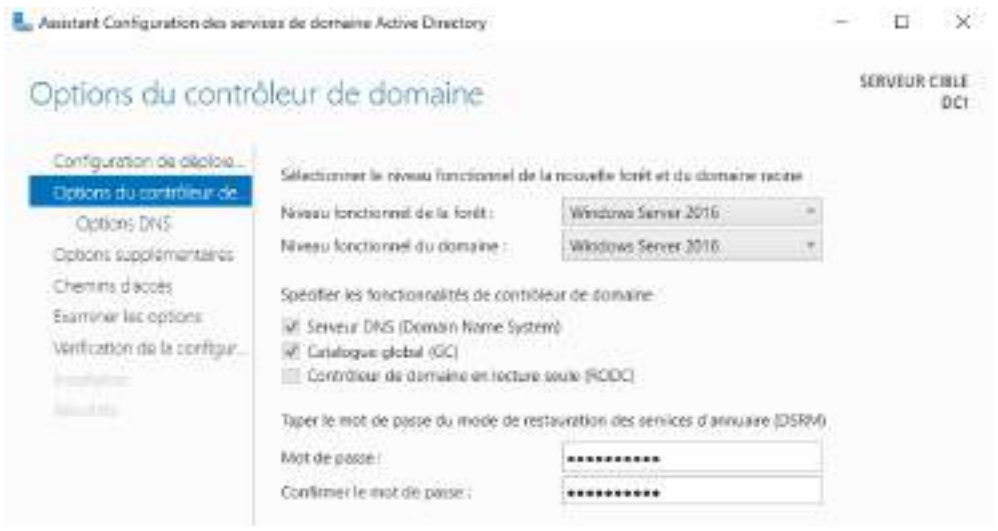


Il faut promouvoir le serveur en contrôleur de domaine.
On clique sur la notification drapeau jaune puis Promouvoir ce serveur en contrôleur de domaine.



On sélectionne :
Ajouter une nouvelle forêt
Nom du domaine racine : experty.local





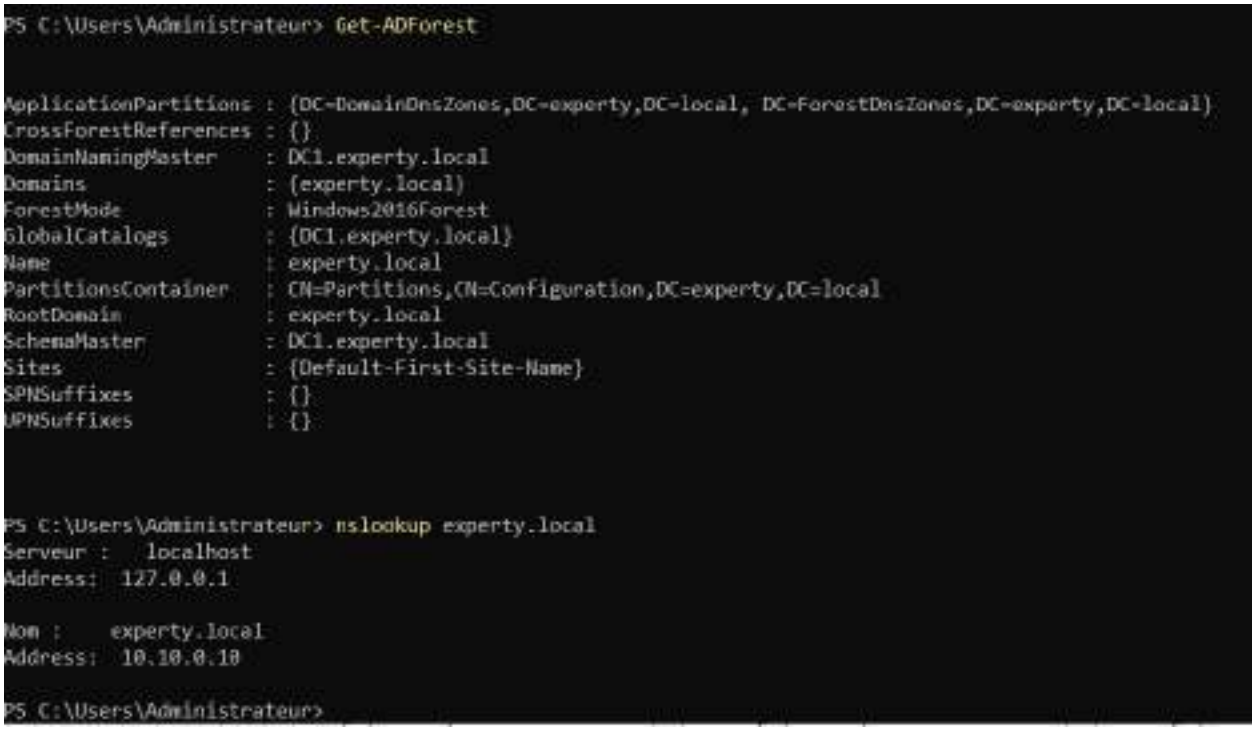
Niveau fonctionnel de la forêt : Windows Server 2016
Coche Serveur DNS

Configure le mot de passe
On laisse le reste des options par défaut → Installer

On redémarre puis on se connecte avec les identifiants du domaine :
Nom d'utilisateur : experty\Administrateur
Mot de passe : Admin@2022

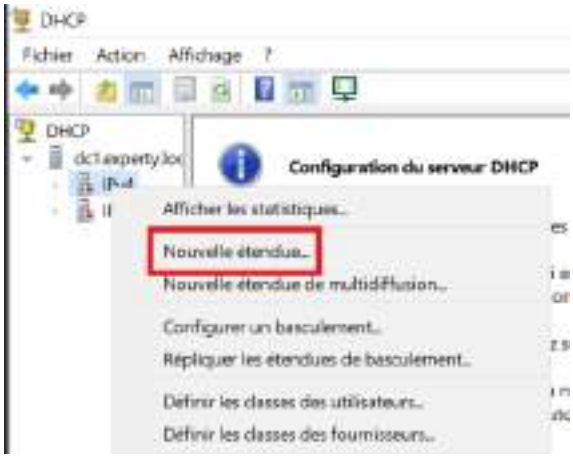
On peut vérifier dans PowerShell (on doit voir le domaine experty.local) :
Get-ADDomain
Get-ADForest

Vérification du DNS :
nslookup experty.local → 10.10.0.10



Configuration DHCP redondé (Failover 80/20)

Dans le Gestionnaire de serveur :
Outils → DHCP
Clique droit sur IPv4 → Nouvelle étendue (New Scope)



Dans l'assistant :

Voulez-vous configurer les options DHCP pour cette étendu maintenant ? → Oui, je veux configurer ces options maintenant

On configure notre scope :

Nom : LAN-EXPERTY
Plage d'adresses : 10.10.0.40 → 10.10.0.200
Masque : 255.255.255.0
Durée de bail : 8 jours

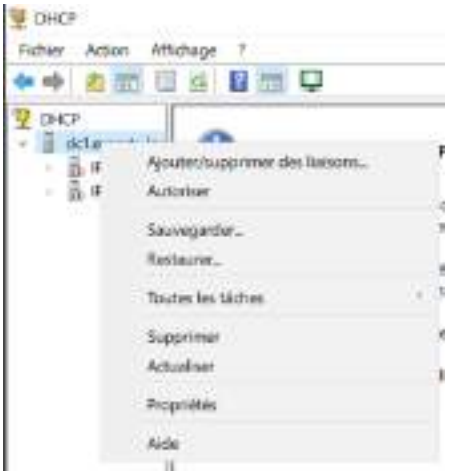
On ajoute notre routeur (passerelle par défaut) :

10.10.0.254

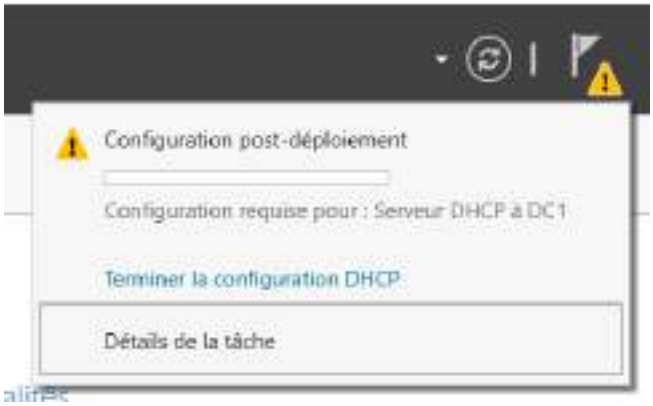
On renseigne le nom de domaine et serveur DNS :
Domaine parent : experty.local
DNS Adresse IP (adresse de DC1 et DC2) : 10.10.0.10, 10.10.0.11

Note : Serveur WINS à laisser vide
On peut finir l'installation de l'assistant.

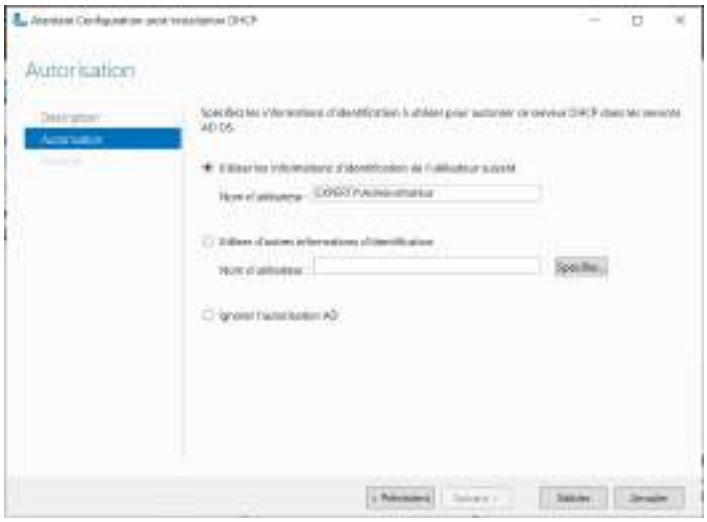
Ensuite on autorise le serveur DHCP :
Clique droit sur le nom du serveur DHCP → Autoriser



Retour dans le Gestionnaire de serveur :



On termine la configuration DHCP



Tests rapides sur le DC1 en powershell :

ping 10.10.0.254
nslookup experty.local
Get-Service DHCPServer

Pour la redondance DHCP → Voir Configuration d'un DHCP secondaire

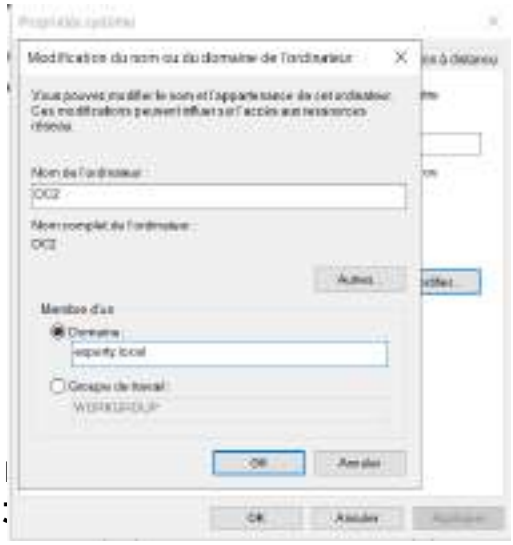
Configuration de la redondance avec un DC2

On configure une IP fixe : Win + R → ncpa.cpl

On pense à bien mettre en DNS préféré l'IP de DC1.
On peut ensuite tester la connexion avec un ping.

On peut maintenant rejoindre le domaine experty.local :

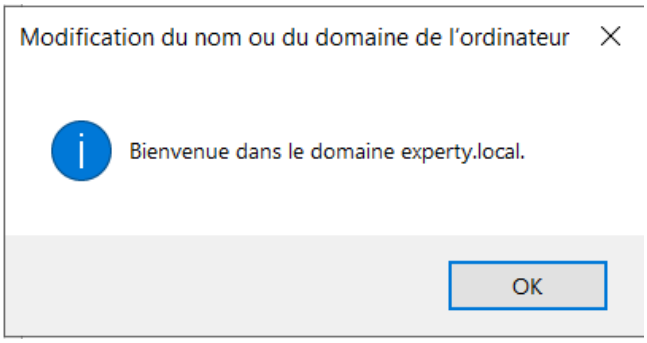
Win + R → sysdl.cpl → Modifier



Nom de l'ordinateur : DC2
Domaine : experty.local

On rentre après les identifiants admin :

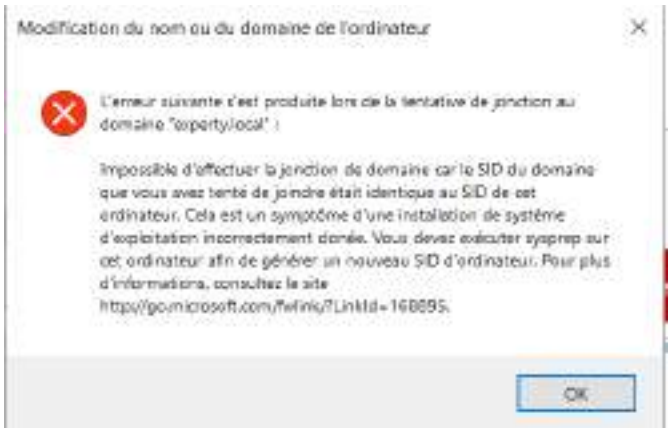
Administrateur
Admin@2022



Si tout fonctionne on nous renvoie ce message de Bienvenue

On peut alors redémarrer la VM et se connecter avec experty\Administrateur

Erreur fréquente si manipulation avec VM :



C'est à cause du clonage des VM. Pour corriger sans tout réinstaller

Win + R → sysprep

On lance sysprep.exe et on sélectionne :

Entrer en mode OOBE

Généraliser

Arrêter

On relance la machine et lors de la manipulation le message ne devrait plus s'afficher.

On peut maintenant ajouter les rôles sur le DC2 :

Gestionnaire de serveur → Gérer → Ajouter des rôles et des fonctionnalités

On sélectionne les rôles AD DS + DNS Server + DHCP

Comme sur le DC1, on promouvoit le DC2 en contrôleur de domaine

On sélectionne :

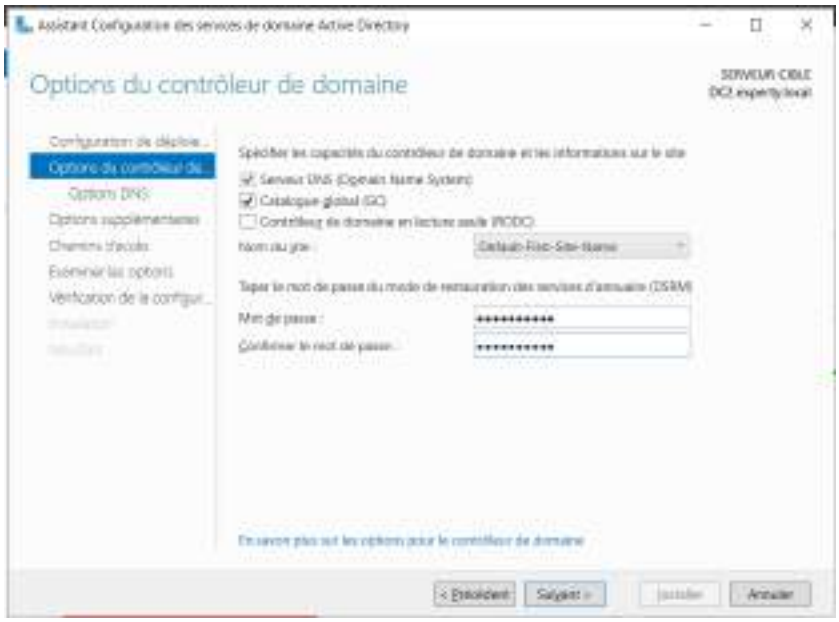
Ajouter un contrôleur de domaine à un domaine existant

Domaine : experty.local

Quand on clique sur Sélectionner, on doit trouver DC1.experty.local

On utilise les identifiants du domaine pour se connecter :

Administrateur / Admin@2022



Ensuite dans les options du contrôleur de domaine :

On coche Serveur DNS

Et on rentre le mot des passe DSRM d'auparavant.

On fait Suivant jusqu'à Installer

Pour vérification après redémarrage, on se connecte avec experty\Administrateur

Sur PowerShell :

Get-ADDomainController -Discorver -Service “PrimaryDC”

Get-ADReplicationPartnerMetadata -Target “DC2”

On doit voir DC1 comme partenaire de réplication.

Pour le DNS :

nslookup experty.local

On doit avoir un réponse depuis DC2

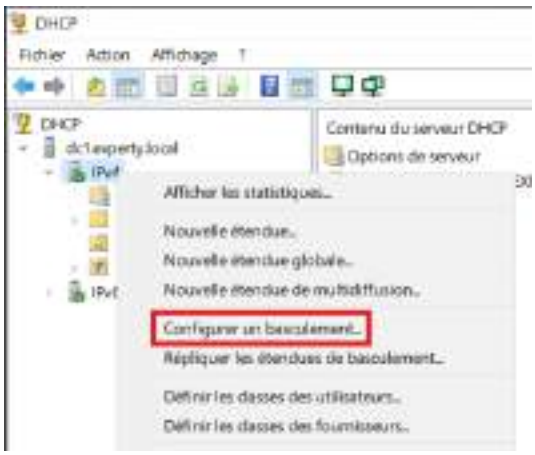
Pour la configuration DHCP secondaire :

Sur DC1 :

Gestionnaire de serveur → Outils → DHCP

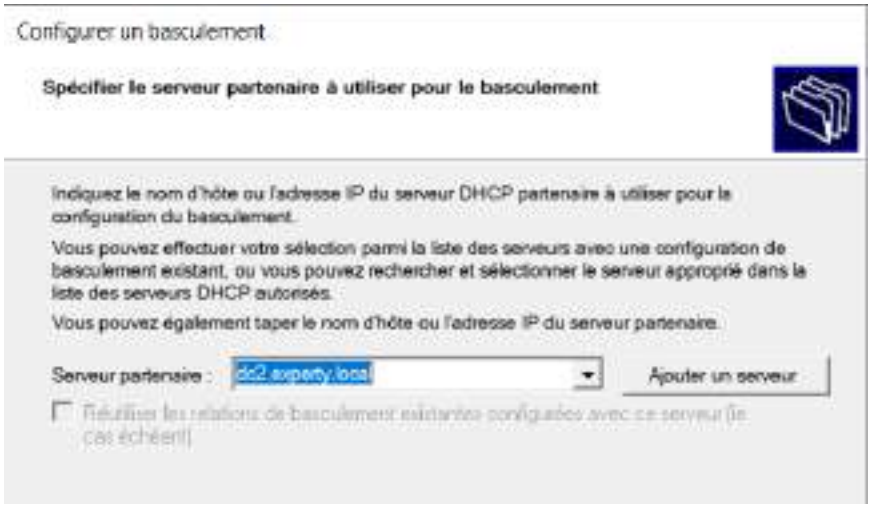
Clique droit sur IPv4 dans le serveur DHCP

“Configurer un basculement”



On sélectionne notre étendu :

On rentre notre serveur partenaire :



Et on configure un basculement :

Nom de la relation :
dc1.experty.local-dc2.experty.local

Mode :
Équilibrage de charge (80% - 20%)

Secret partagé : Experty2025!

On fait Suivant → Terminer

Serveur de fichier et DFS

Pensez à configurer une IP fixe (Win + R → ncpa.cpl)
Ajouter si besoin la machine au domaine experty.local :

Win + R → sysdl.cpl → Modifier
Domaine : experty.local
Identifiants : Administrateur / Admin@2022

On relance la machine et on se connecte avec experty\Administrateur

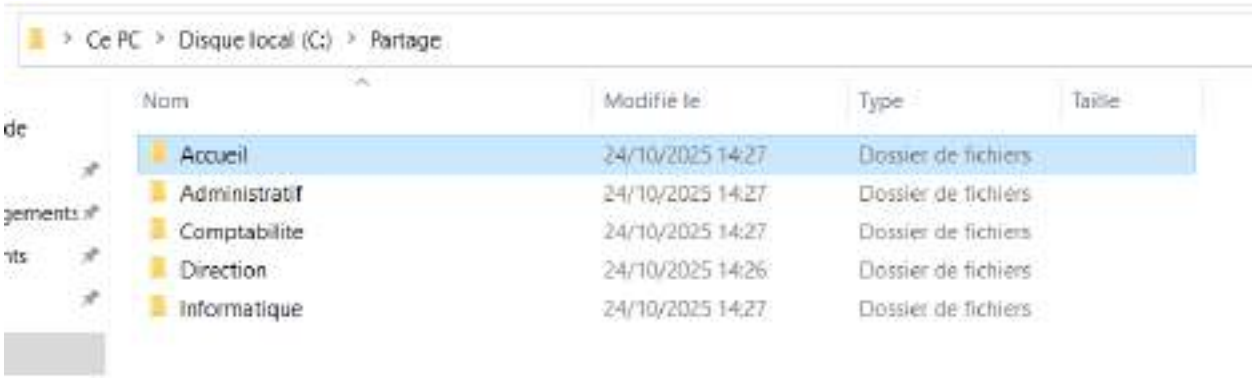
Installation du rôle DFS (Il faut que les contrôleurs de domaines soit allumés) :

Gestionnaire de serveur → Ajouter des rôles et fonctionnalités
On sélectionne le serveur FS1 avec les rôles suivant :
Services d'impression et de numérisation des de document
Services de fichier et de stockage
-> Services de fichiers et iSCSI
-> Serveur de fichier
-> Espaces de nom DFS
-> Gestionnaire de ressources du serveur de fichiers
-> Réplication DFS

Dans les fonctionnalités, on coche Sauvegarde Windows Server

On peut ensuite finir l'installation.

Création du namespace \\experty.local\\partage :
On se rend dans C:\
On crée un dossier Partage.
On crée des sous dossier par services.

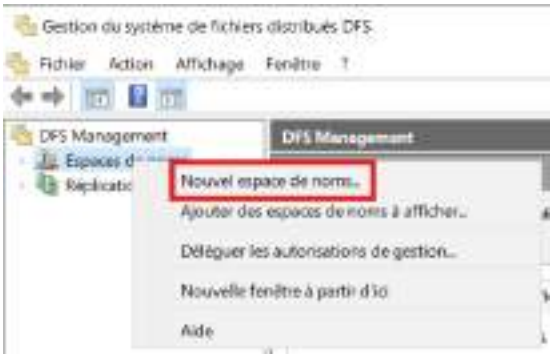


Sur chaque dossier :

Clique droit → Propriétés → Partage avancé :
Cocher "Partager ce dossier"
Nom du partage = même nom que le dossier
Cliquez sur "Autorisations"

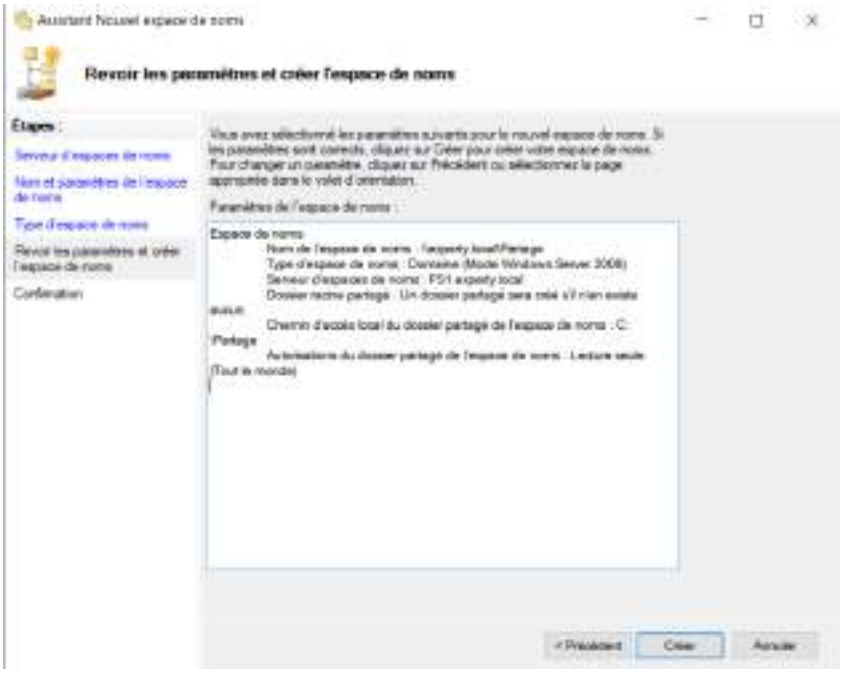
Supprime "Tout le monde"
Ajouter Administrateurs : Contrôle total

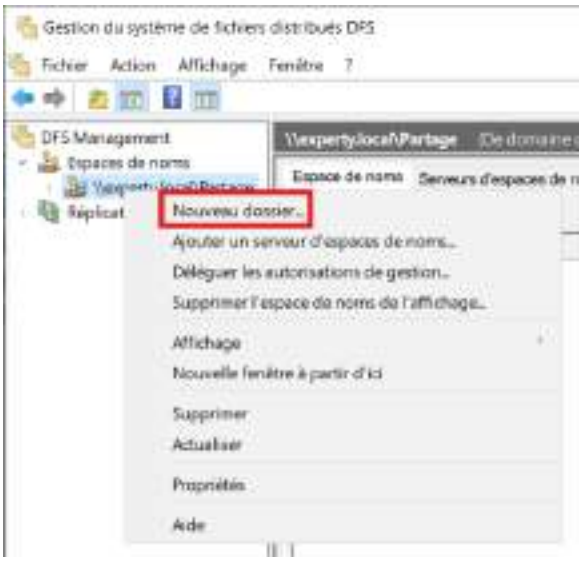
On crée maintenant l'espace DFS
Gestionnaire de serveur → Outils → Gestion DFS
Clique droit sur Espaces de nom → Nouvel espace de noms



On sélectionne le serveur FS1.experty.local (le serveur hôte)

Nom de l'espace de noms : Partage
Choisis le type : Espace de noms basé sur le domaine
(il deviendra alors accessible via \\experty.local\partage)

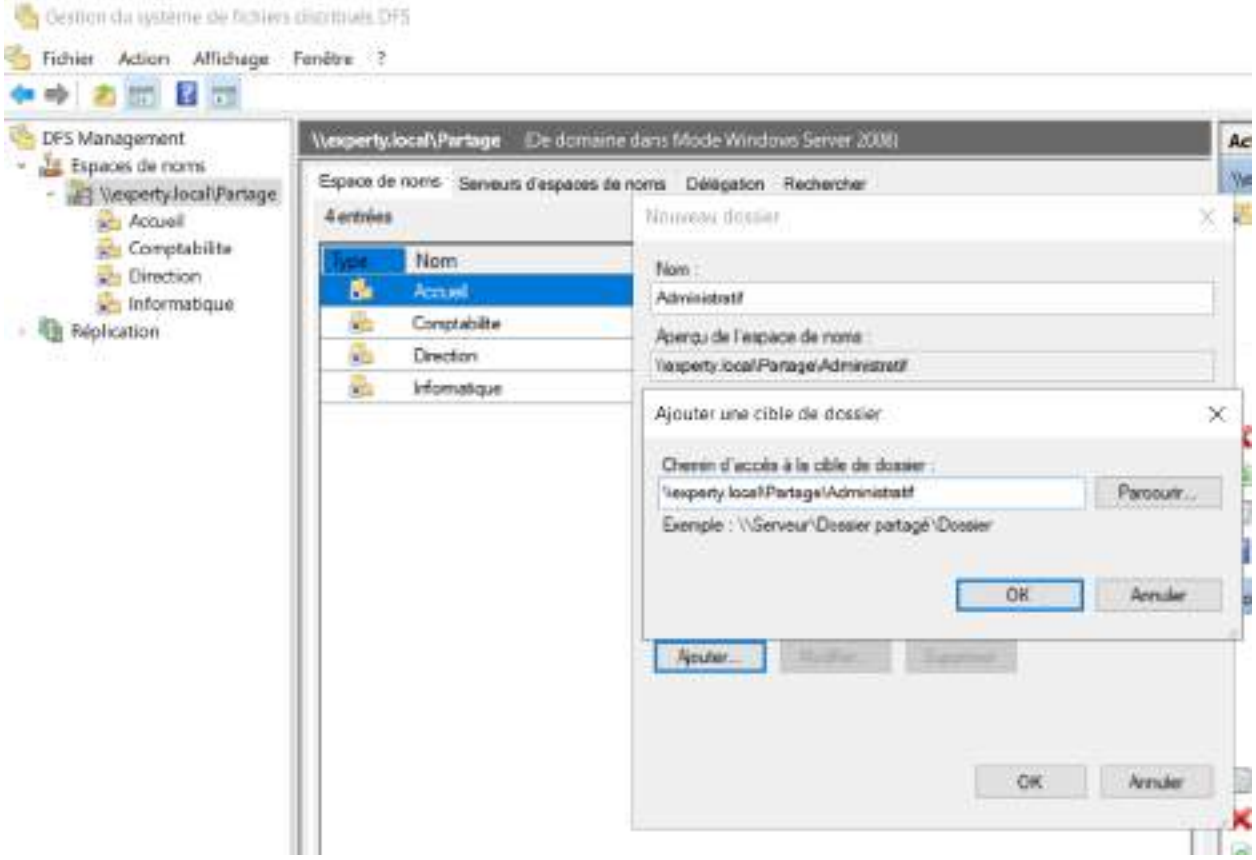




On ajoute les dossier créer dans notre espaces de noms :

Espaces de noms
Clique droit \\experty.local\Partage
Nouveau dossier...

Exemple pour le dossier Administratif :



L'espace DFS sera créé et visible à l'adresse :

\\experty.local\partage

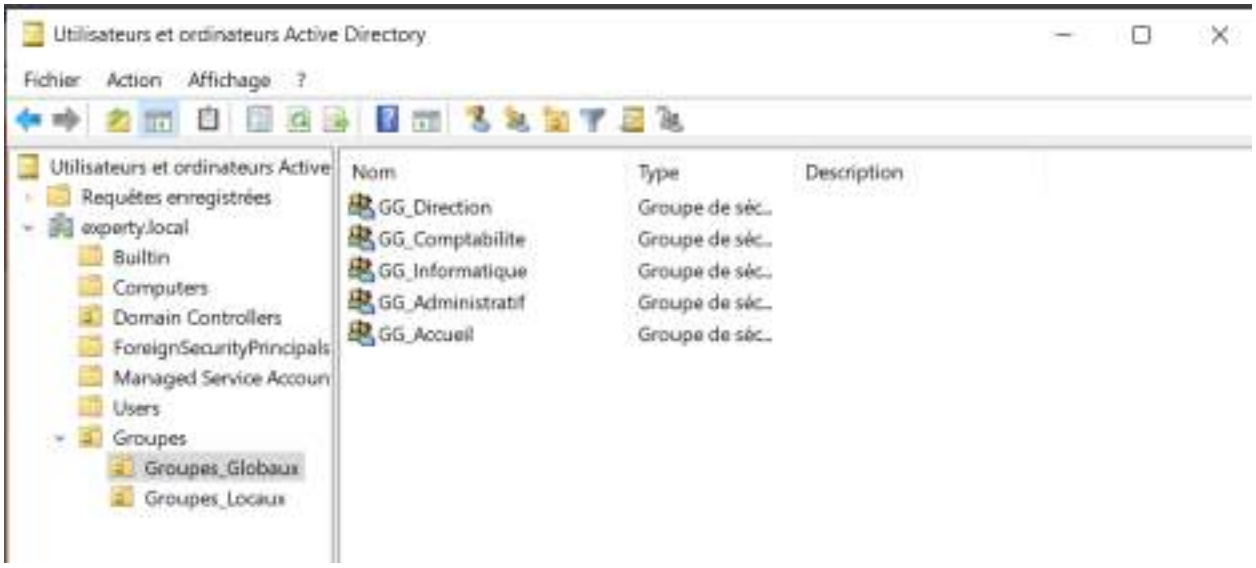
On va maintenant créer des Groupes pour limiter les accès. On utilise la **méthode AGDLP** qui est recommandée.

Sur DC1 :
Gestionnaire de serveur → Outils → Utilisateurs et ordinateurs Active Directory

Dans notre domaine experty.local :
Clique droit → Nouveau → Unité d'organisation

A l'intérieur, crée un sous-dossier "Groupes_Globaux" (Unité d'organisation)

Ensuite dans Groupes_Globaux, on peut créer les groupes respectifs à chaques dossier :



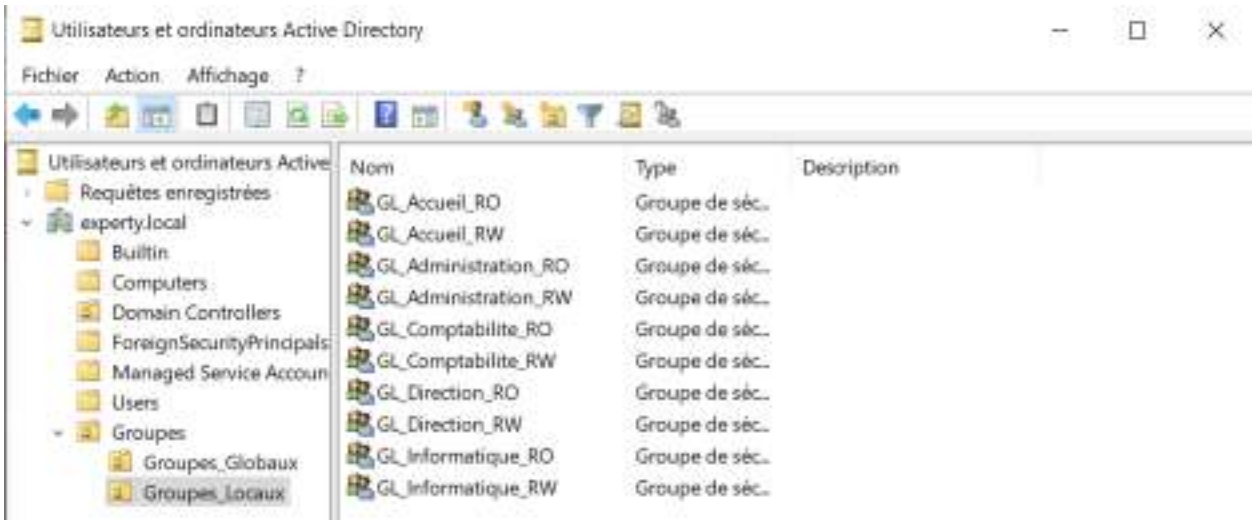
Dans ce groupe, Clique droit → Nouveau → Groupe
On remplit :

- Nom du groupe : GG_Direction (exemple)
- Type de groupe : Sécurité
- Étendu du groupe : Globale

Un fois les groupes créés, on maintenant créer les groupes locaux, ils vont servir de clés d'attribution de droits pour chaque service. On va alors créer deux clés par services, RW (accès lecture/écriture) et RO (accès lecture seule).

Pour les créer :
On crée un dossier “Groupes_Locaux” (Unité d’organisation)
Dans ce groupe, Clique droit → Nouveau → Groupe
On remplit :

- Nom du groupe : GL_Accueil_RO (exemple)
- Type de groupe : Sécurité
- Étendu du groupe : Local du domaine

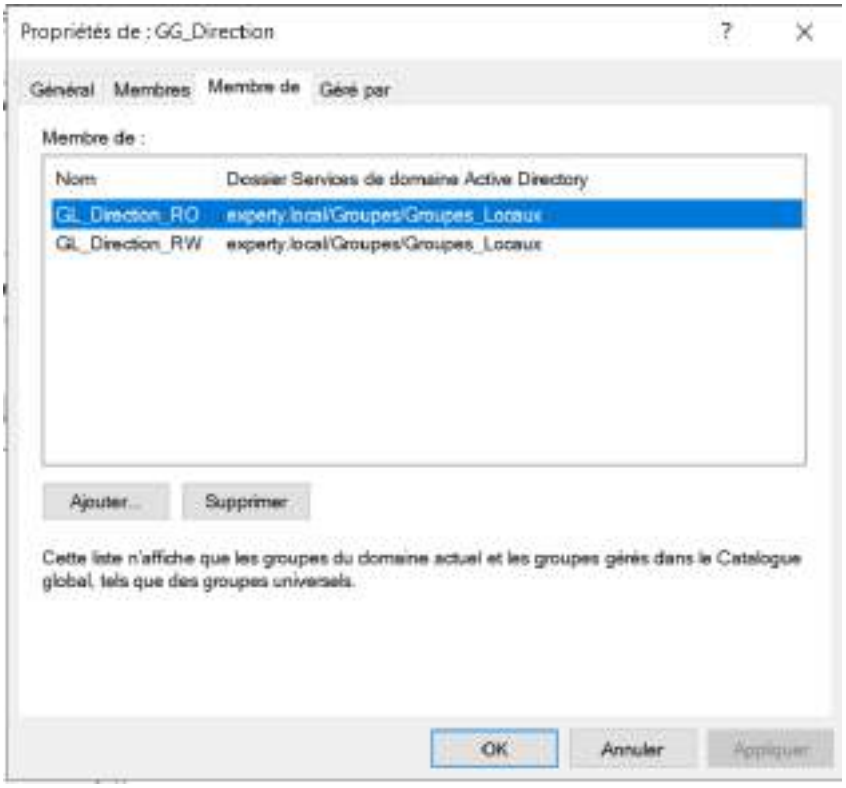


On va maintenant lier les groupes GG et GL entre eux, on choisit quels sont les accès qu’on souhaite donner à chaque GG.

Exemple, on veut que la direction ait accès à son dossier mais aussi à celui du service d’administration :
Dans GG_Direction on ajoute les clés GL_Direction_RW & GL_Administration_RO.

Pour cela :

- On double-clique sur le **GG_Direction**
- Onglet **Membres** → **Ajouter**
- Clique sur **Emplacements** → choisis le domaine (experty.local)
- Clique sur **Avancé** → **Rechercher maintenant**
- On selectionne GL_Direction_RW par exemple



Application des droits sur FS1 (NTFS)

Pour chaque dossier qu'on a précédemment créé :
1 - Clique droit sur le dossier (ex. C:\Partages\Comptabilite) → Propriétés → Sécurité → Modifier → Ajouter.

2 - Clique sur Emplacements → sélectionne experty.local.

3 - Ajoute le groupe correspondant :
- Dossier "Comptabilité" → GG_Comptabilite
- Dossier "Direction" → GG_Direction
- etc.

4 - Clique sur Autorisations :
- GG du service → "Modification"
- Administrateurs du domaine → "Contrôle total"
- Supprime "Tout le monde" s'il est présent.

5 - Clique sur Appliquer → OK.

Ce mécanisme lie chaque groupe à son espace de travail.

🔐 Étape 6 : Application des droits sur FS1 (NTFS)

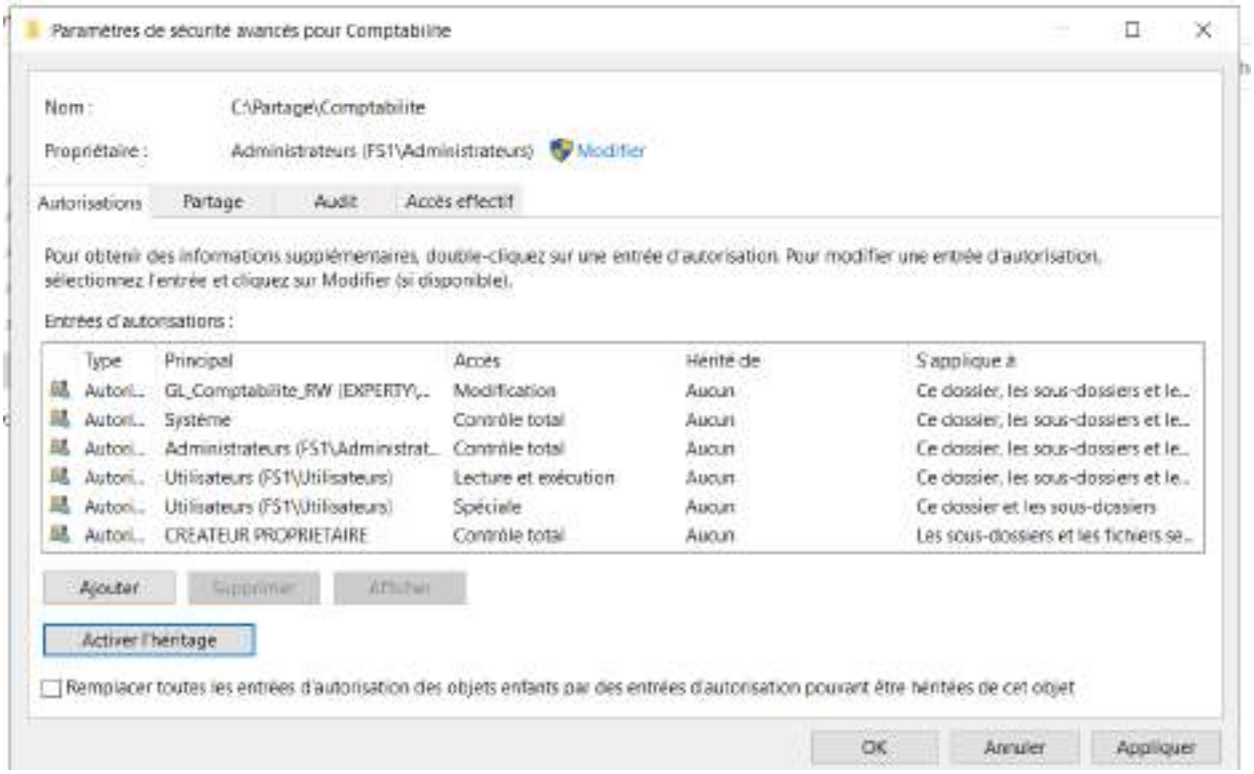
> Une fois les groupes globaux créés, tu reviens sur FS1 pour attribuer les bons droits aux dossiers.

Pour chaque dossier :

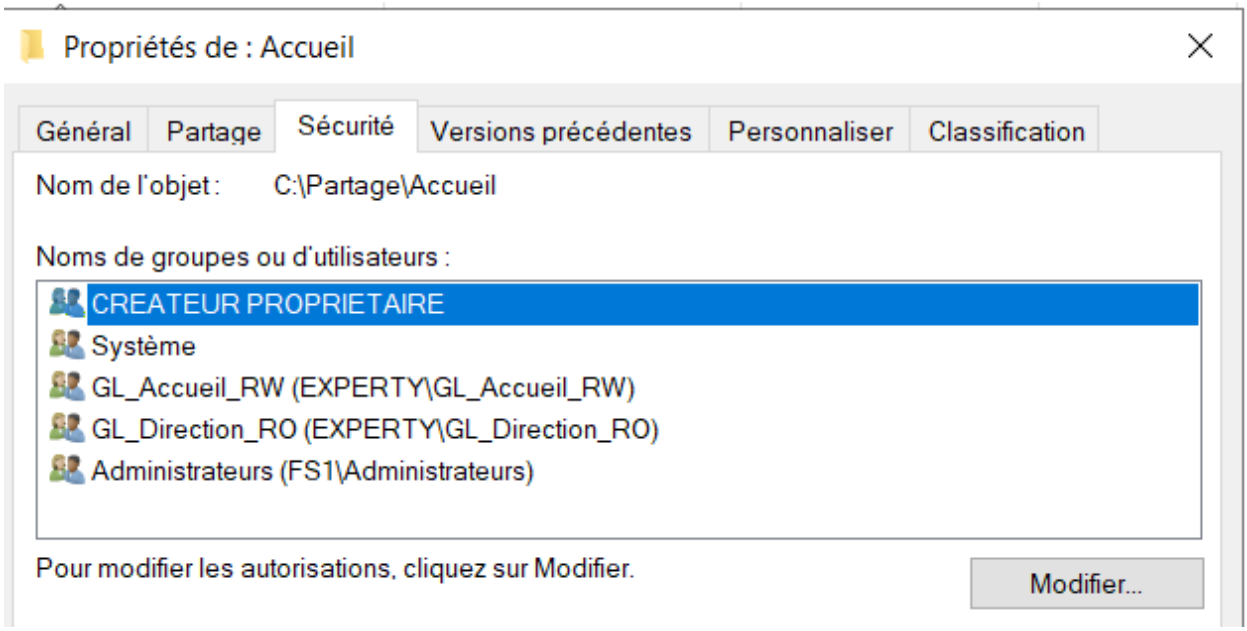
1. Clique droit sur le dossier (ex. `C:\Partages\Comptabilite`) → **Propriétés** → **Sécurité** → **Modifier** → **Ajouter**.
2. Clique sur **Emplacements** → sélectionne `experty.local`.
3. Ajoute le groupe correspondant :
   - Dossier "Comptabilite" → `GG_Comptabilite`
   - Dossier "Direction" → `GG_Direction`
   - etc.
4. Clique sur **Autorisations** :
   - **GG du service** → "Modification"
   - **Administrateurs du domaine** → "Contrôle total"
   - Supprime "Tout le monde" s'il est présent.
5. Clique sur **Appliquer** → **OK**.

💡 Ce mécanisme lie chaque groupe à son espace de travail.

On fait avec les GL à la place des GG



pener a desactiver l'héritage pour supprimer les profils utilisateurs et ajouter les bons



🧩 2️⃣ Application des bonnes pratiques AGDLPV

> 🎯 Objectif : sécuriser et organiser les permissions des dossiers partagés.

Tu as déjà commencé :

✅ les **Groupes Globaux (GG)** sont créés sur DC1.

Maintenant, il faut **appliquer la méthode complète AGDLPV** :

🧱 Création des utilisateurs dans l'Active Directory (AD)

Tu vas créer **1 ou 2 utilisateurs par service** (Direction, Comptabilité, Informatique, Administratif, Accueil).
Cela suffira largement pour ta démo.

⚙️ Étape 1 — Ouvrir la console Active Directory

1. Connecte-toi à **DC1**.
2. Clique sur **Démarrer → Outils d'administration → Utilisateurs et ordinateurs Active Directory**.
3. Dans le volet gauche, développe ton domaine :

```
lua                                                    Copier le code

experty.local
```

⚙️ Étape 2 — Créer les unités d'organisation (OU)

> C'est important pour garder ton AD bien structuré.

1. Clique droit sur ton domaine → **Nouveau → Unité d'organisation**.
   - Nom : `Utilisateurs`
2. Refais la même chose à l'intérieur de `Utilisateurs` :
   - `Direction`
   - `Comptabilite`
   - `Informatique`
   - `Administratif`

⚙️ Étape 2 — Créer les unités d'organisation (OU)

> C'est important pour garder ton AD bien structuré.

1. Clique droit sur ton domaine → **Nouveau** → **Unité d'organisation.**
   - Nom : `Utilisateurs`
2. Refais la même chose à l'intérieur de `Utilisateurs` :
   - `Direction`
   - `Comptabilite`
   - `Informatique`
   - `Administratif`
   - `Accueil`

✅ Tu auras maintenant une arborescence comme :

```
esperty.local
└── Utilisateurs
    ├── Direction
    ├── Comptabilite
    ├── Informatique
    ├── Administratif
    └── Accueil
```

⚙️ Étape 3 — Créer les utilisateurs

⚙️ Étape 3 — Créer les utilisateurs

> On crée des comptes de test réalistes (1 ou 2 par service).

Exemple :

Service Comptabilité

1. Clique droit sur `Comptabilite` → **Nouveau** → **Utilisateur**.
2. Renseigne :
   - **Prénom** : Julie
   - **Nom** : Martin
   - **Nom d'ouverture de session** : `j.martin`
   - → Suivant
3. Mot de passe :
   - `Test@2025`
   - Décoche "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session".
   - Coche "Le mot de passe n'expire jamais" (pour ta maquette).
   - → Terminer.

Répète pour d'autres services, par exemple :

Service	Prénom	Nom	Identifiant
Direction	Bernard	Simon	b.simon
Informatique	Enzo	Dubois	e.dubois
Administratif	Clara	Petit	c.petit
Accueil	Sarah	Lopez	s.lopez

💡 Tu peux te limiter à **5 utilisateurs au total** (un par service) — c'est suffisant pour tester GPO, droits et profils.

⚙️ Étape 4 — Ajouter les utilisateurs dans les groupes globaux (GG)

1. Va dans ton OU **Groupes → Groupes_Globaux** (que tu avais créée précédemment).
2. Ouvre un groupe (ex : `GG_Comptabilite`).
3. Onglet **Membres → Ajouter**.
   - Tape le nom de ton utilisateur : `j.martin` → OK.
4. Refais pour chaque service :
   - `b.simon` → `GG_Direction`
   - `e.dubois` → `GG_Informatique`
   - `c.petit` → `GG_Administratif`
   - `s.lopez` → `GG_Accueil`

✅ Résultat attendu :

Chaque utilisateur appartient à son groupe global, ce qui lui donnera automatiquement les bons droits sur FS1.

⚙️ Étape 5 — Vérification rapide

1. Ouvre une console PowerShell sur DC1.
2. Tape :

```powershell
Get-ADUser -Filter * | Select Name,SamAccountName
```

→ Tu verras la liste de tous les utilisateurs créés.

3. Tu peux aussi tester :

```powershell
Get-ADGroupMember GG_Comptabilite
```

Étape 7 : Mise en place de l'imprimante réseau

1. Ouvre **Outils → Gestion de l'impression**.
2. Ajoute une **nouvelle imprimante locale** :
   - Port : `FILE:` (Print to File)
   - Pilote : "Microsoft Print to PDF"
   - Nom : `Imprimante_Reseau`
3. Coche "Partager cette imprimante" sous le nom :

```
\\FS1\Imprimante_Reseau
```

4. Sur DC1, déploie-la via une GPO :
   - **Gestion des stratégies de groupe (GPMC)** → Crée une GPO `GPO_Imprimante`
   - Édite-la :
     - Configuration utilisateur → Stratégies → Paramètres Windows → Connexions d'imprimantes
     - Clique droit → "Nouvelle connexion" → entre `\\FS1\Imprimante_Reseau`

Mise en place complète de l'imprimante réseau (sur FS1)

Objectif

Tu vas :

1. Installer une **imprimante partagée** sur FS1 (ex. "Microsoft Print to PDF").
2. La **partager sur le réseau** sous le nom `Imprimante_Reseau`.
3. La **déployer automatiquement** sur les postes clients via une **GPO** (stratégie de groupe).

Étape 1 — Ouvrir la console de gestion d'impression

1. Sur **FS1**, ouvre le **Gestionnaire de serveur**.
2. En haut à droite, clique sur **Outils → Gestion de l'impression**.
   👉 Une console nommée **Gestion de l'impression** s'ouvre.
3. Dans le volet gauche, développe :

markdown — Copier le code

```
Gestion de l'impression
    └─ Serveurs d'impression
        └─ FS1 (ton serveur)
            ├─ Pilotes
            ├─ Ports
            └─ Imprimantes
```

Étape 2 — Ajouter l'imprimante

Option 1 : Simuler une imprimante avec Microsoft Print to PDF

C'est parfait pour une maquette.

1. Clique droit sur **Imprimantes** → **Ajouter une imprimante.**
2. L'assistant s'ouvre :
   - Sélectionne **Ajouter une imprimante locale ou réseau avec des paramètres manuels** → Suivant.
   - Choisis **Créer un nouveau port** → Type de port = **Port local** → Suivant.
   - Dans le champ du nom du port, entre :

     Copier le code

     ```
     \\FS1\Imprimante_Reseau
     ```

     → Clique sur **OK.**
   - Sélectionne le **pilote d'imprimante :**
     - Fabricant : **Microsoft**
     - Modèle : **Microsoft Print to PDF**
     - → Suivant.
   - Nom de l'imprimante :

     nginx — Copier le code

     ```
     Imprimante_Reseau
     ```

     → Suivant.
   - Choisis **Partager cette imprimante :**
     - Nom du partage : `Imprimante_Reseau`
     - Emplacement : `FS1`

- Nom du partage : `Imprimante_Reseau`
- Emplacement : `FS1`
- Commentaire : `Imprimante réseau par défaut`

→ Suivant, puis **Terminer**.

💡 Tu peux tester en imprimant un document : cela générera un fichier PDF (puisqu'on simule une imprimante réelle).

🧪 Étape 3 — Vérifier le partage réseau

1. Ouvre **Explorateur de fichiers** sur FS1.
2. Dans la barre d'adresse, tape :

```
\\FS1
```

3. Tu dois voir ton imprimante listée sous le nom :

```nginx
Imprimante_Reseau
```

4. Si tu veux tester depuis ton **client Windows 11**, tape :

```
\\FS1
```

→ L'imprimante doit aussi apparaître.

✅ Cela confirme que le partage est bien visible sur le réseau.

Étape 4 — Déploiement via GPO (sur DC1)

Maintenant, tu vas la faire apparaître **automatiquement** sur les postes clients du domaine.

1. Sur **DC1**, ouvre le **Gestionnaire de serveur**.
2. Clique sur **Outils → Gestion des stratégies de groupe** (GPMC).
3. Clique droit sur ton domaine `experty.local` → **Créer un objet GPO dans ce domaine et le lier ici.**
   - Nom : `GPO_Imprimante_Réseau`.
4. Clique droit sur la nouvelle GPO → **Modifier**.

Dans l'éditeur de stratégie :

1. Va dans :

```
Configuration utilisateur
  → Stratégies
    → Paramètres Windows
      → Connexions d'imprimantes
```

2. Clique droit dans la zone blanche → **Nouvelle connexion.**
3. Dans le champ "Nom de l'imprimante" :

```
\\FS1\Imprimante_Reseau
```

4. Coche :
   - ✅ "L'imprimante est disponible dans le menu Imprimer"
   - ✅ "Rendre cette imprimante l'imprimante par défaut" *(si tu veux)*
5. Ferme la fenêtre et quitte l'éditeur.

Étape 5 — Actualiser la stratégie sur le client

Sur ton poste **CLIENT1** :

1. Ouvre une session avec un utilisateur du domaine (`test1` par exemple).
2. Ouvre **Invite de commandes** et tape :

```cmd
gpupdate /force
```

3. Attends le message "Les stratégies de groupe ont été mises à jour avec succès".
4. Va dans :

```cmd
Panneau de configuration → Périphériques et Imprimantes
```

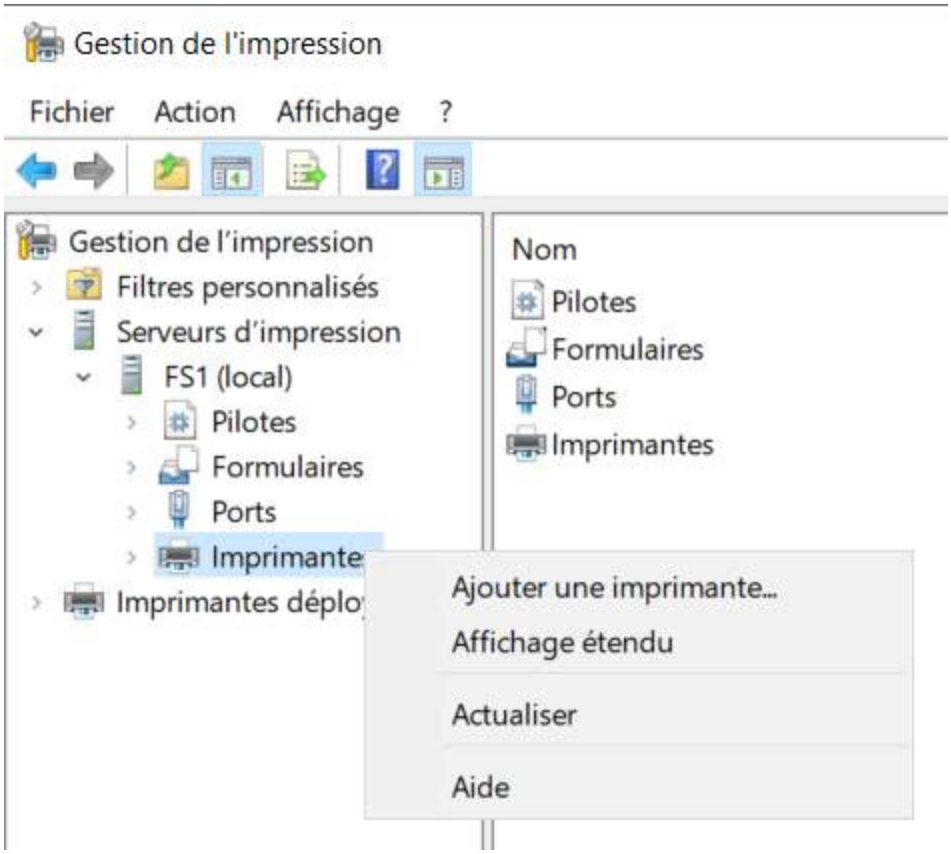
→ Tu dois voir apparaître ton **Imprimante_Reseau** automatiquement ✅

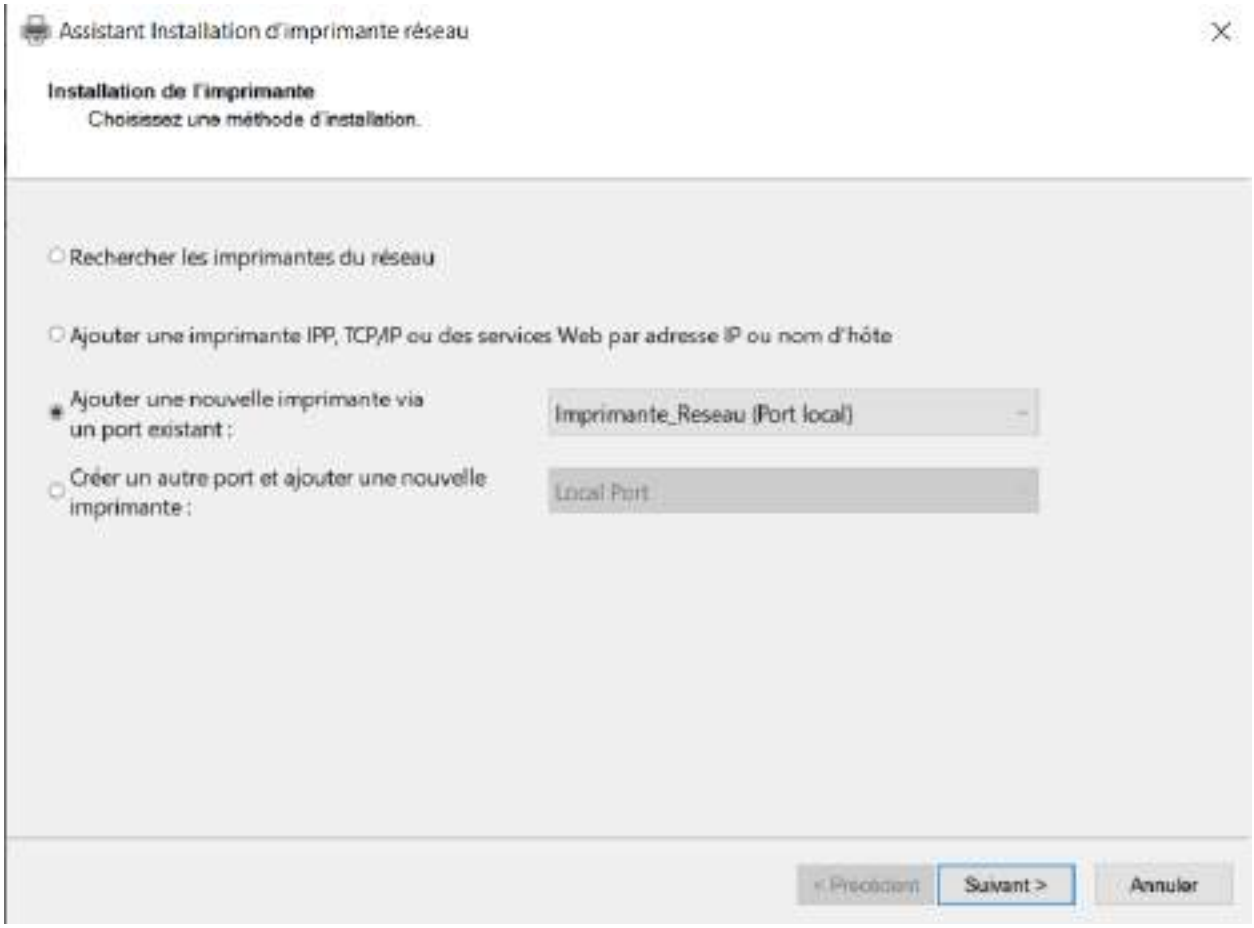
Étape 6 — Test

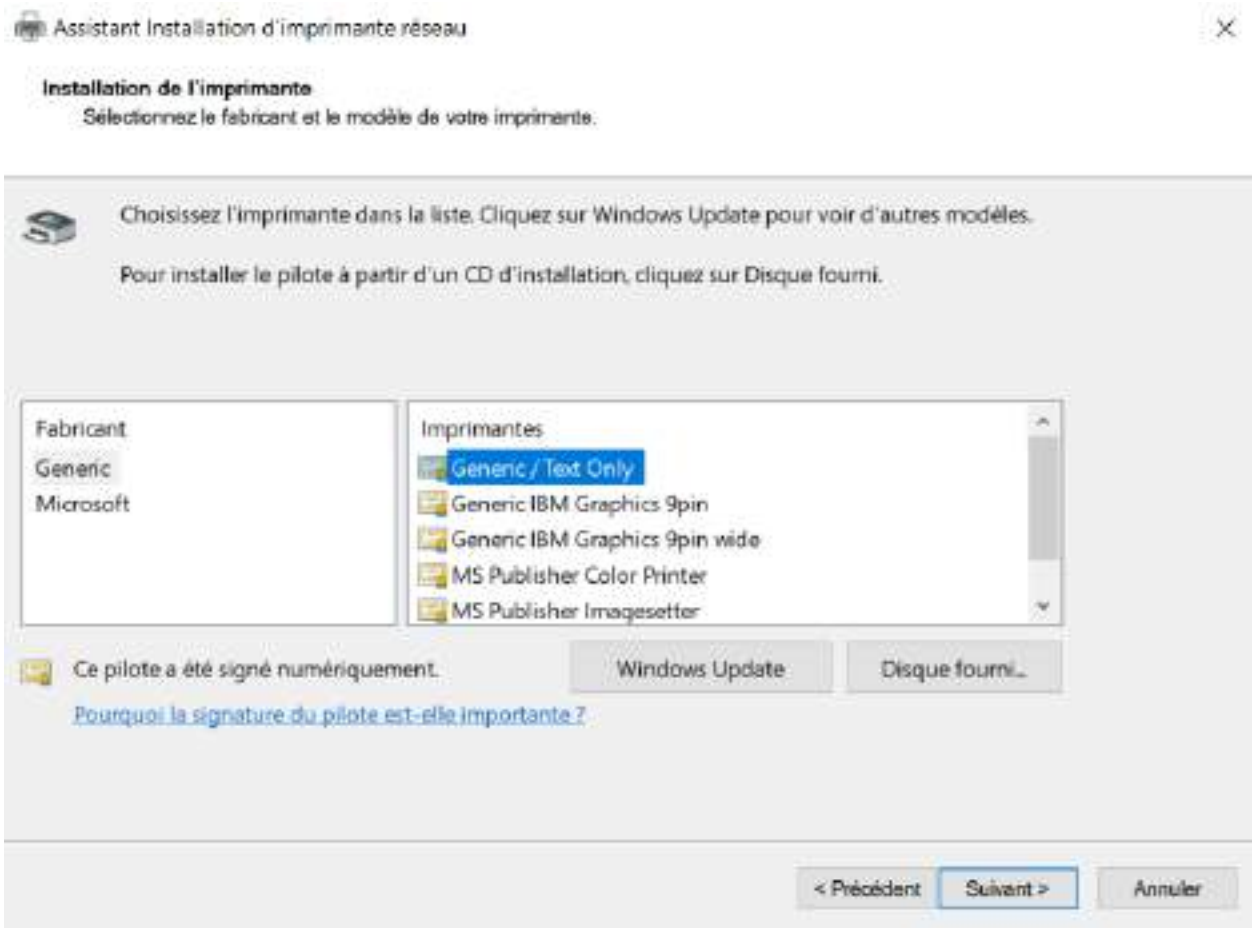
Depuis ton client :

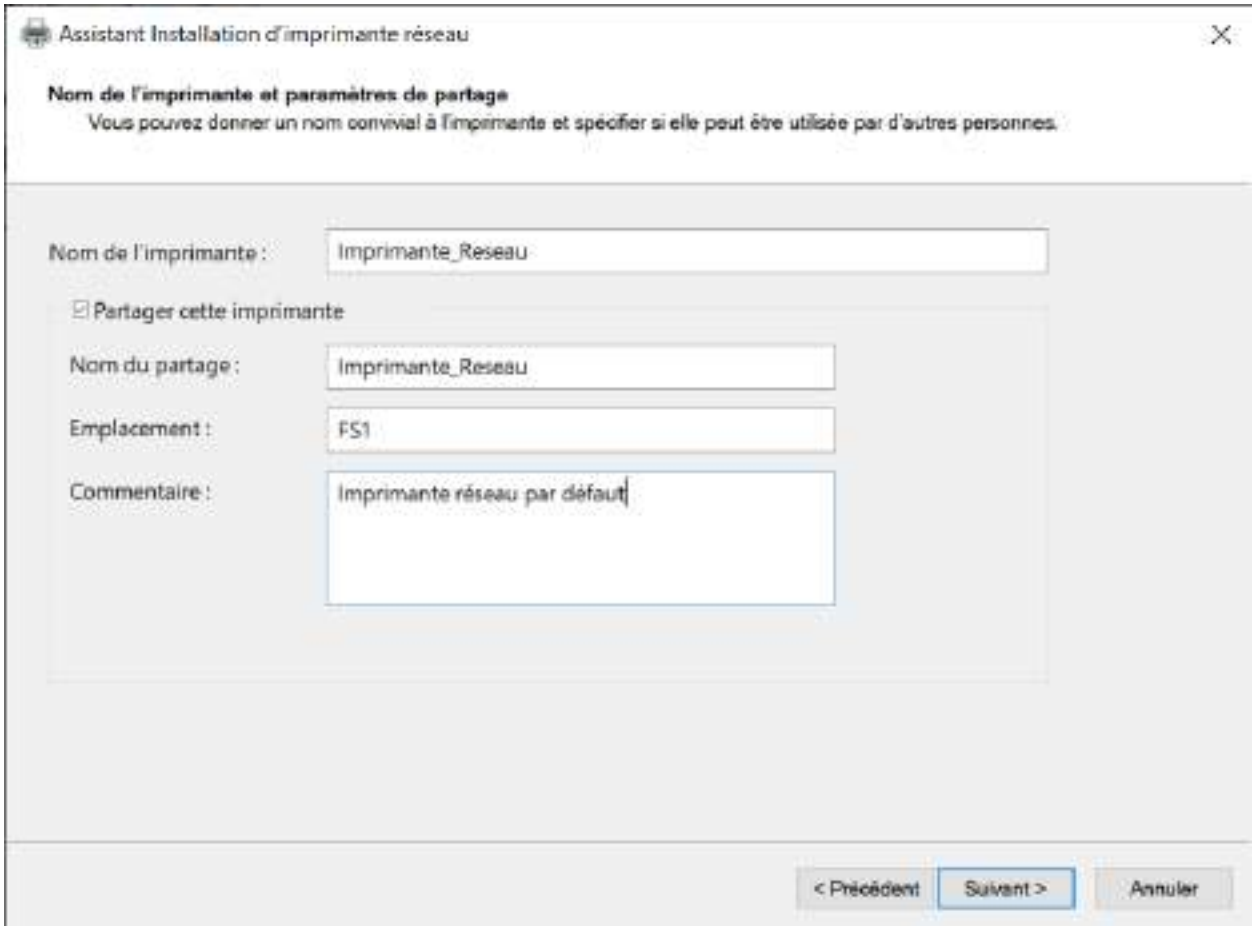
1. Ouvre **Word** ou **Bloc-notes**.
2. Fais **Fichier → Imprimer → Sélectionne Imprimante_Reseau → Imprimer**.
3. Si c'est une "Microsoft Print to PDF", elle te proposera d'enregistrer le document sur le bureau.

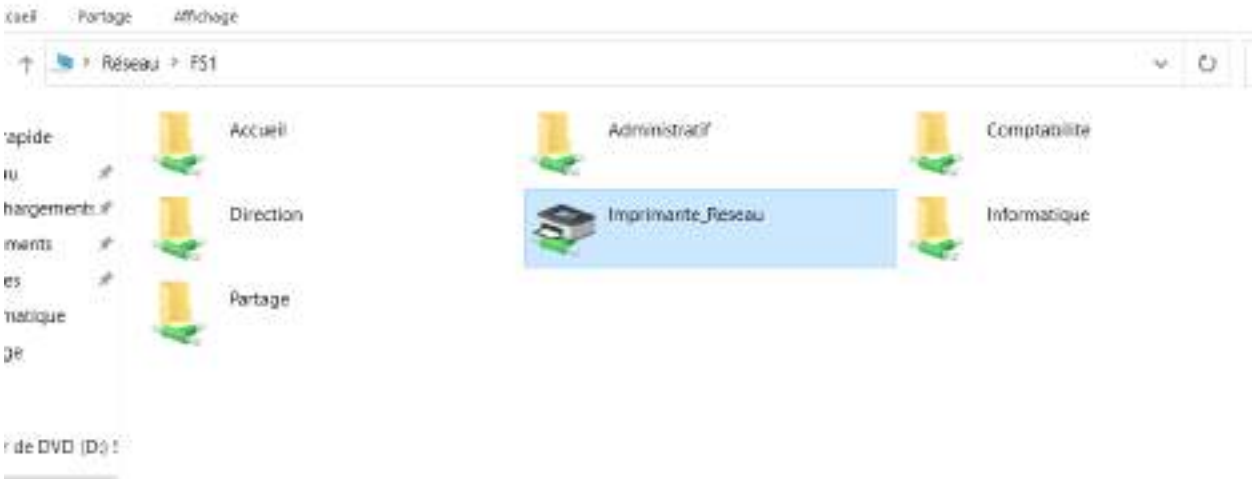
→ Test réussi 🎉

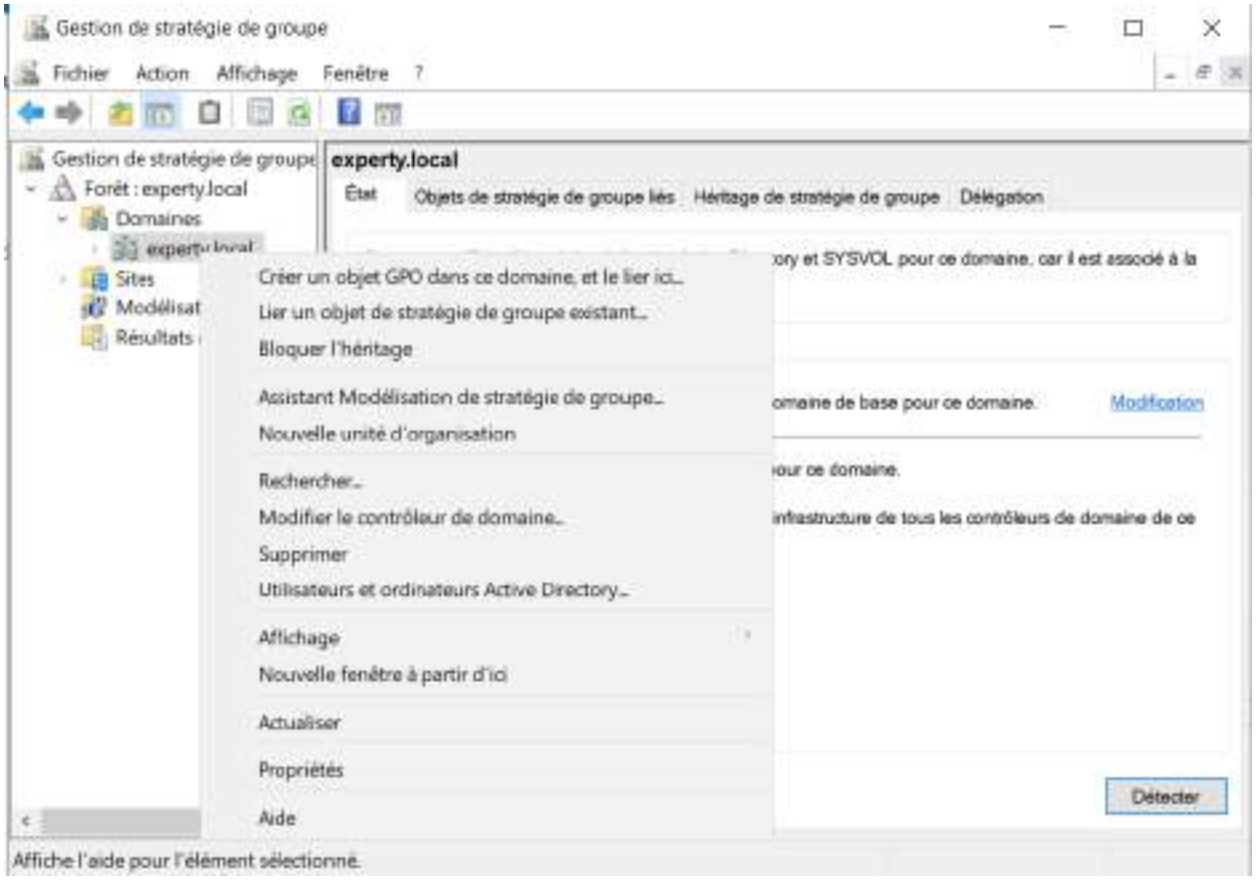

Gestion de l'impression
Fichier
Action
Affichage
?
Gestion de l'impression
Filtres personnalisés
Serveurs d'impression
FS1 (local)
Pilotes
Formulaires
Ports
Imprimante
Imprimantes déplo
Nom
Pilotes
Formulaires
Ports
Imprimantes
Ajouter une imprimante...
Affichage étendu
Actualiser
Aide

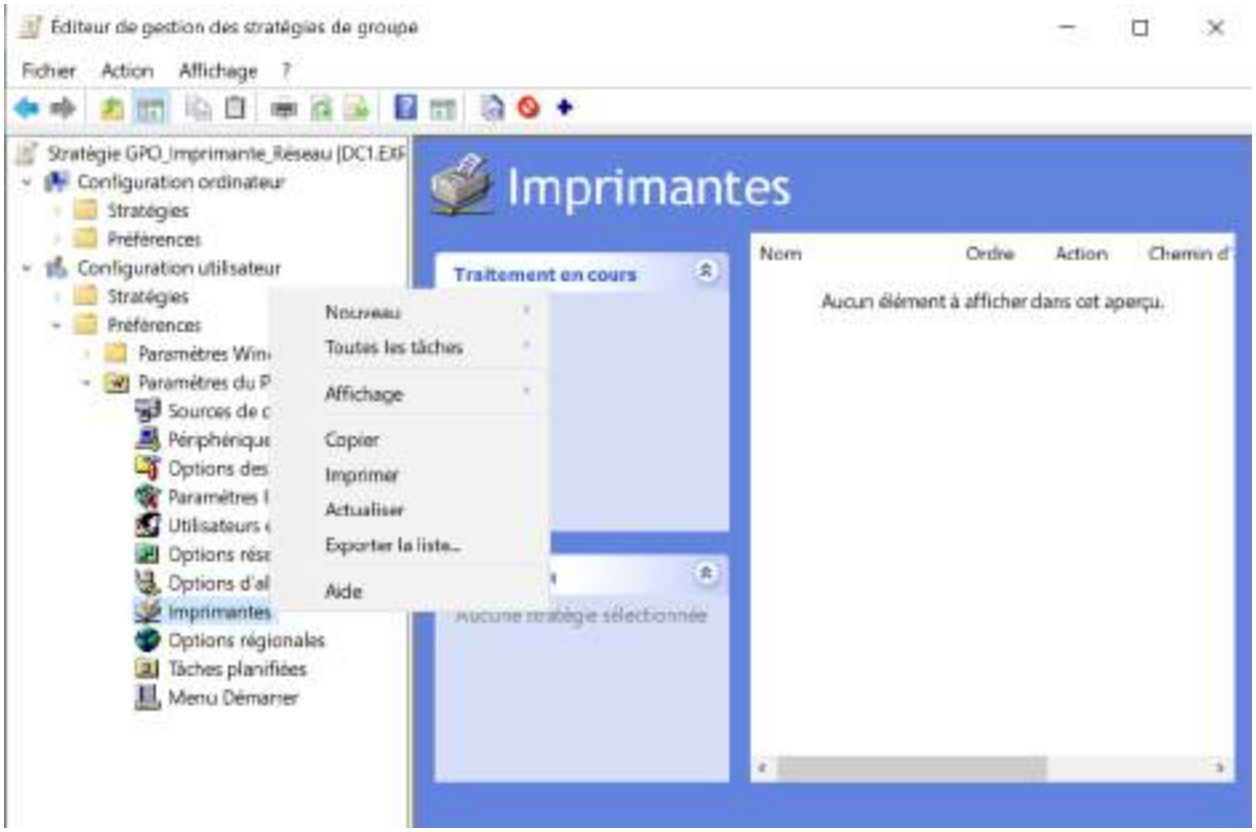

Assistant Installation d'imprimante réseau
Installation de l'imprimante
Choisissez une méthode d'installation.
Rechercher les imprimantes du réseau
Ajouter une imprimante IPP, TCP/IP ou des services Web par adresse IP ou nom d'hôte
Ajouter une nouvelle imprimante via un port existant :
Imprimante_Reseau (Port local)
Créer un autre port et ajouter une nouvelle imprimante :
Local Port
< Précédent
Suivant >
Annuler

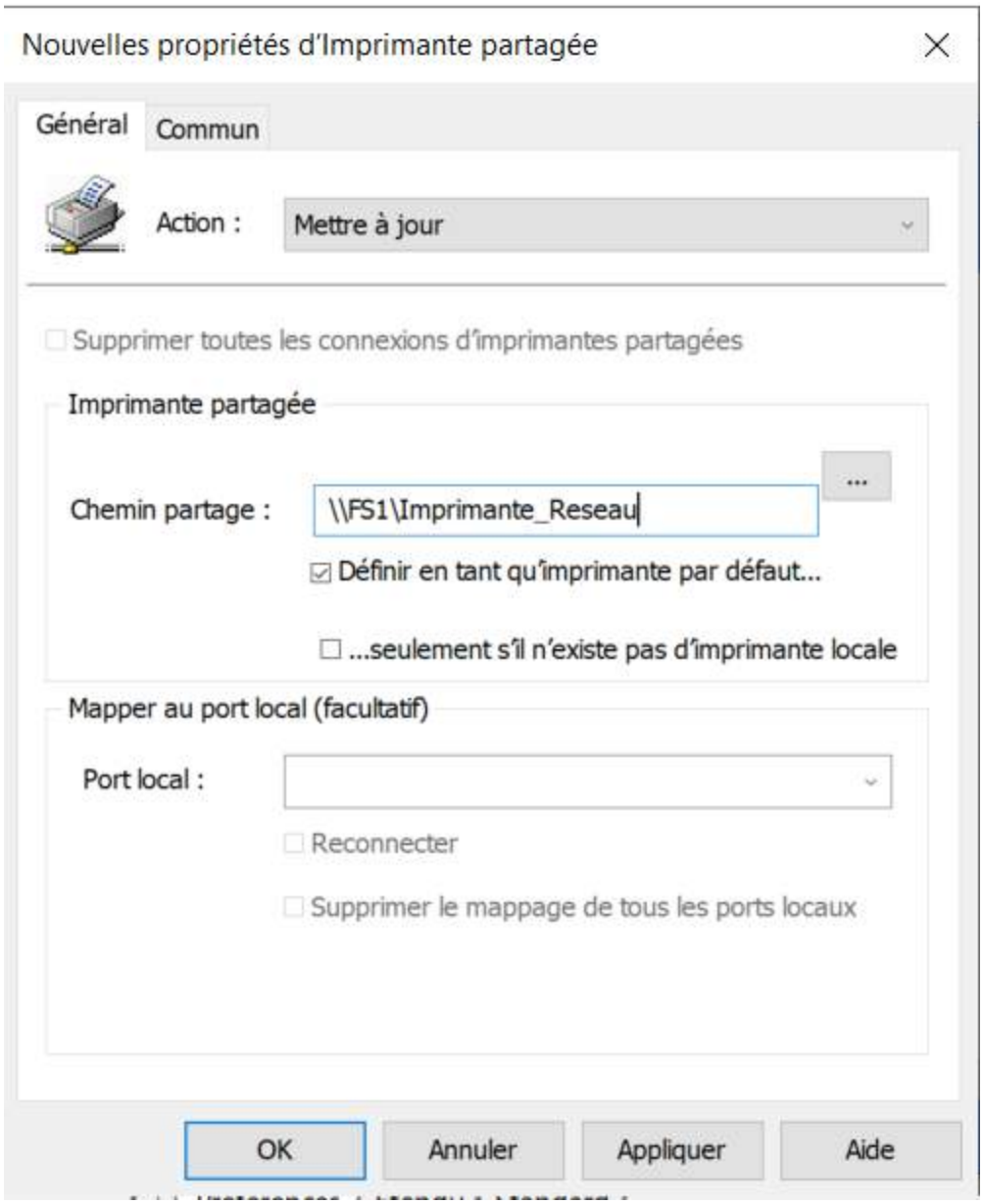

Assistant Installation d'imprimante réseau
Installation de l'imprimante
Sélectionnez le fabricant et le modèle de votre imprimante.
Choisissez l'imprimante dans la liste. Cliquez sur Windows Update pour voir d'autres modèles.
Pour installer le pilote à partir d'un CD d'installation, cliquez sur Disque fourni.
Fabricant
Generic
Microsoft
Imprimantes
Generic / Text Only
Generic IBM Graphics 9pin
Generic IBM Graphics 9pin wide
MS Publisher Color Printer
MS Publisher Imagesetter
Ce pilote a été signé numériquement.
Windows Update
Disque fourni...
Pourquoi la signature du pilote est-elle importante ?
< Précédent
Suivant >
Annuler


Assistant Installation d'imprimante réseau
Nom de l'imprimante et paramètres de partage
Vous pouvez donner un nom convivial à l'imprimante et spécifier si elle peut être utilisée par d'autres personnes.
Nom de l'imprimante :
Imprimante_Reseau
Partager cette imprimante
Nom du partage :
Imprimante_Reseau
Emplacement :
FS1
Commentaire :
Imprimante réseau par défaut
< Précédent
Suivant >
Annuler


Partage
Affichage
Réseau > FS1
Accueil
Direction
Partage
Administratif
Imprimante_Reseau
Comptabilité
Informatique


Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : experty.local
Domaines
Sites
Modélisat
Résultats
experty.local
État
Objets de stratégie de groupe liés
Héritage de stratégie de groupe
Délégation
ory et SYSVOL pour ce domaine, car il est associé à la
Créer un objet GPO dans ce domaine, et le lier ici...
Lier un objet de stratégie de groupe existant...
Bloquer l'héritage
Assistant Modélisation de stratégie de groupe...
omaine de base pour ce domaine.
Modification
Nouvelle unité d'organisation
Rechercher...
our ce domaine.
Modifier le contrôleur de domaine...
nfrastructure de tous les contrôleurs de domaine de ce
Supprimer
Utilisateurs et ordinateurs Active Directory...
Affichage
Nouvelle fenêtre à partir d'ici
Actualiser
Propriétés
Détecter
Aide
Affiche l'aide pour l'élément sélectionné.


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Imprimante_Réseau [DC1.EXF
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètres Win
Paramètres du P
Sources de c
Périphériqu
Options des
Paramètres I
Utilisateurs
Options rés
Options d'al
Imprimantes
Options régionales
Tâches planifiées
Menu Démarrer
Nouveau
Toutes les tâches
Affichage
Copier
Imprimer
Actualiser
Exporter la liste...
Aide
Imprimantes
Traitement en cours
Aucune stratégie sélectionnée
Nom
Ordre
Action
Chemin d'
Aucun élément à afficher dans cet aperçu.


Nouvelles propriétés d'Imprimante partagée
Général
Commun
Action :
Mettre à jour
Supprimer toutes les connexions d'imprimantes partagées
Imprimante partagée
Chemin partage :
\\FS1\Imprimante_Reseau
...
Définir en tant qu'imprimante par défaut...
...seulement s'il n'existe pas d'imprimante locale
Mapper au port local (facultatif)
Port local :
Reconnecter
Supprimer le mappage de tous les ports locaux
OK
Annuler
Appliquer
Aide

💾 Étape 8 : Configuration de la sauvegarde

1. Sur FS1 → **Outils** → **Sauvegarde Windows Server**
2. Crée une **sauvegarde planifiée** :
   - Type : "Sauvegarde complète (Full Server)"
   - Fréquence : quotidienne (23h00)
   - Destination : deuxième disque virtuel (E:) ou volume séparé
3. Laisse la planification s'exécuter.

⚙️ Étape 1 — Vérifier l'installation de l'outil "Sauvegarde Windows Server"

1. Sur **FS1**, ouvre le **Gestionnaire de serveur**.
2. Clique sur **Gérer → Ajouter des rôles et fonctionnalités**.
3. Clique sur **Suivant** plusieurs fois jusqu'à arriver à la section **Fonctionnalités**.
4. Coche :

```arduino
Sauvegarde Windows Server
```

5. Clique sur **Suivant → Installer**.
6. Attends la fin de l'installation (quelques secondes).

✅ Une fois installé, tu verras l'outil "Sauvegarde Windows Server" dans le menu **Outils**.

⚙️ Étape 2 — Préparer un disque ou un volume de sauvegarde

💡 Pour ta maquette VMware :

- Tu peux **ajouter un deuxième disque virtuel** à ta VM FS1 (20 à 40 Go).
  - VMware → Settings → Add → Hard Disk → Create a new virtual disk → 30 Go → OK.
- Démarre FS1.
- Ouvre le **Gestionnaire de disques** :
  - Clique droit sur le nouveau disque → **Initialiser le disque** → GPT → OK.
  - Clique droit sur l'espace non alloué → **Nouveau volume simple** → Suivant.
  - Attribue la lettre **E:**
  - Nom du volume :

```nginx
Sauvegarde
```

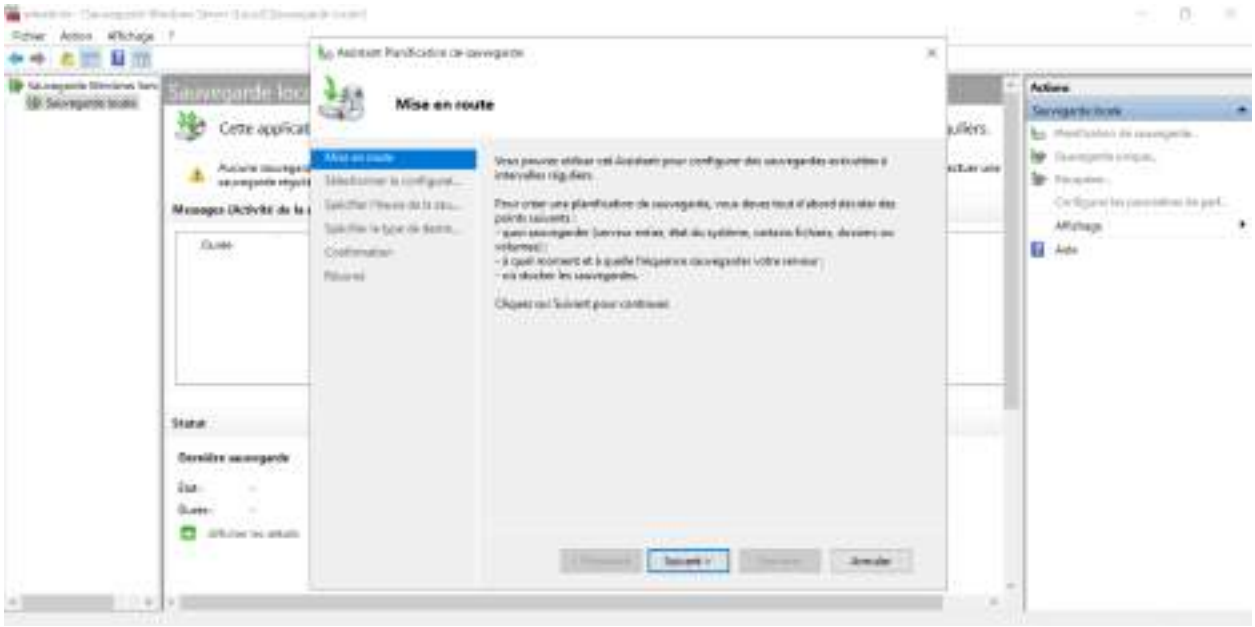
  - Termine l'assistant.

✅ Ton disque de sauvegarde est prêt et visible dans l'explorateur (`E:`).

⚙️ Étape 3 — Ouvrir l'outil de sauvegarde

1. Dans le **Gestionnaire de serveur**, clique sur **Outils → Sauvegarde Windows Server**.
2. Dans la fenêtre, choisis **Sauvegarde planifiée** (colonne de droite).

⚙️ Étape 4 — Configurer la planification



⚙️ Étape 4 — Configurer la planification

L'assistant de sauvegarde planifiée s'ouvre :

1 Configuration de la planification

- Choisis : **Sauvegarde complète du serveur (Full Server)** → Suivant.

  💡 Cela inclut tout : le système + les dossiers partagés.

  (Si tu veux cibler uniquement tes partages, coche "Personnalisée" → sélectionne `C:\Partages`)

2 Planification

- Choisis : **Tous les jours**
- Heure : **23:00** (23h00)
- Clique sur **Suivant**.

3 Destination de la sauvegarde

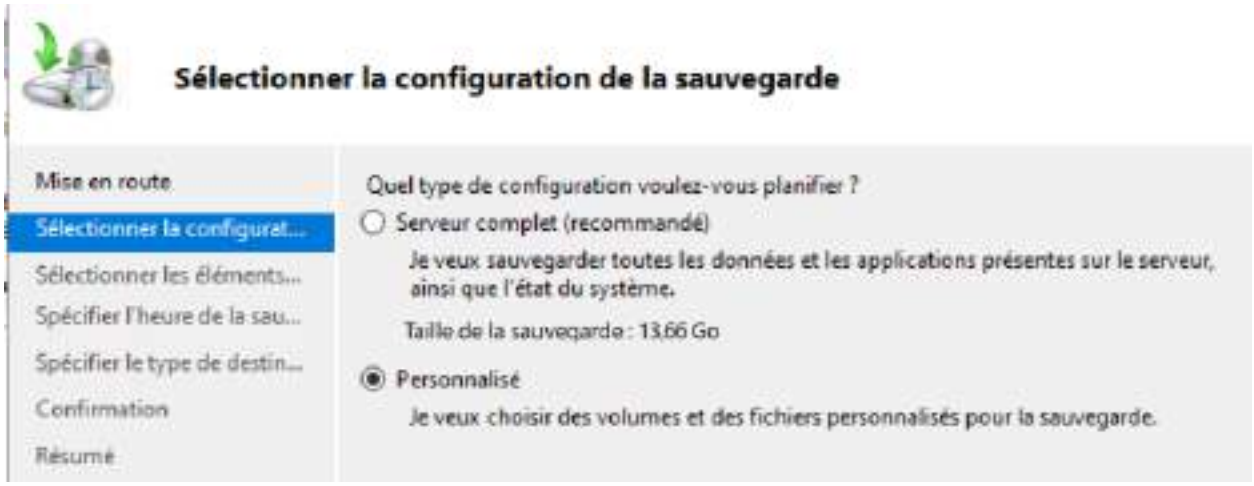
Tu as deux options :

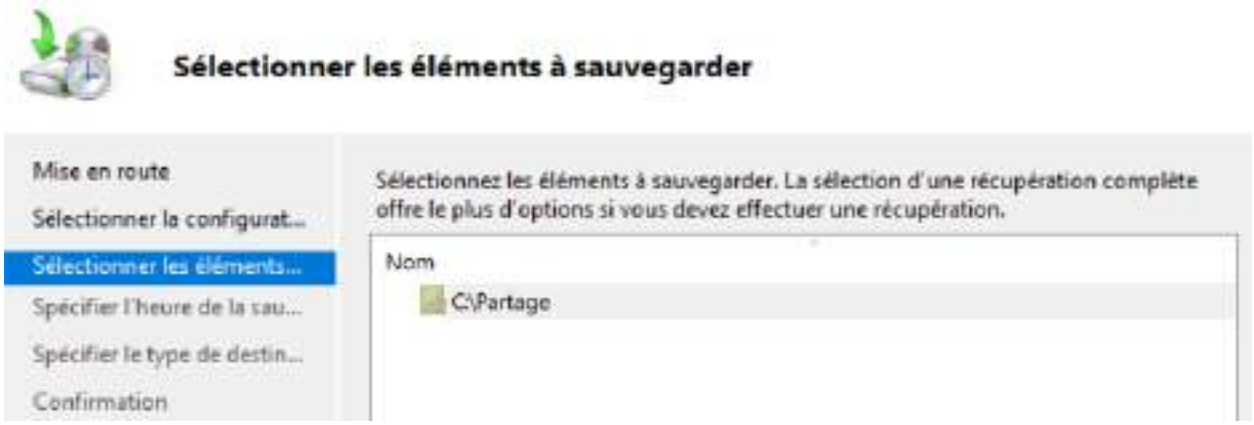
- **Disque dur dédié** (recommandé)
- **Volume ou dossier réseau** (optionnel pour toi)

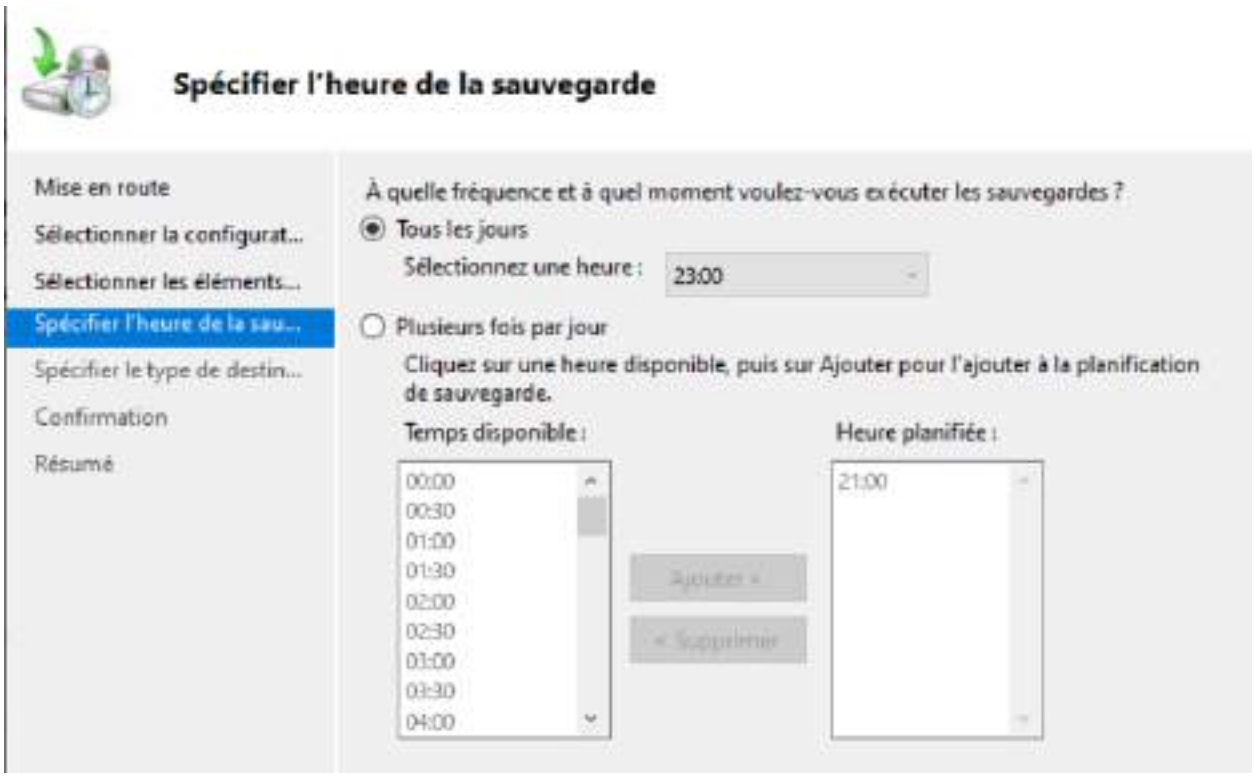
➡️ Choisis **Disque dur dédié**.

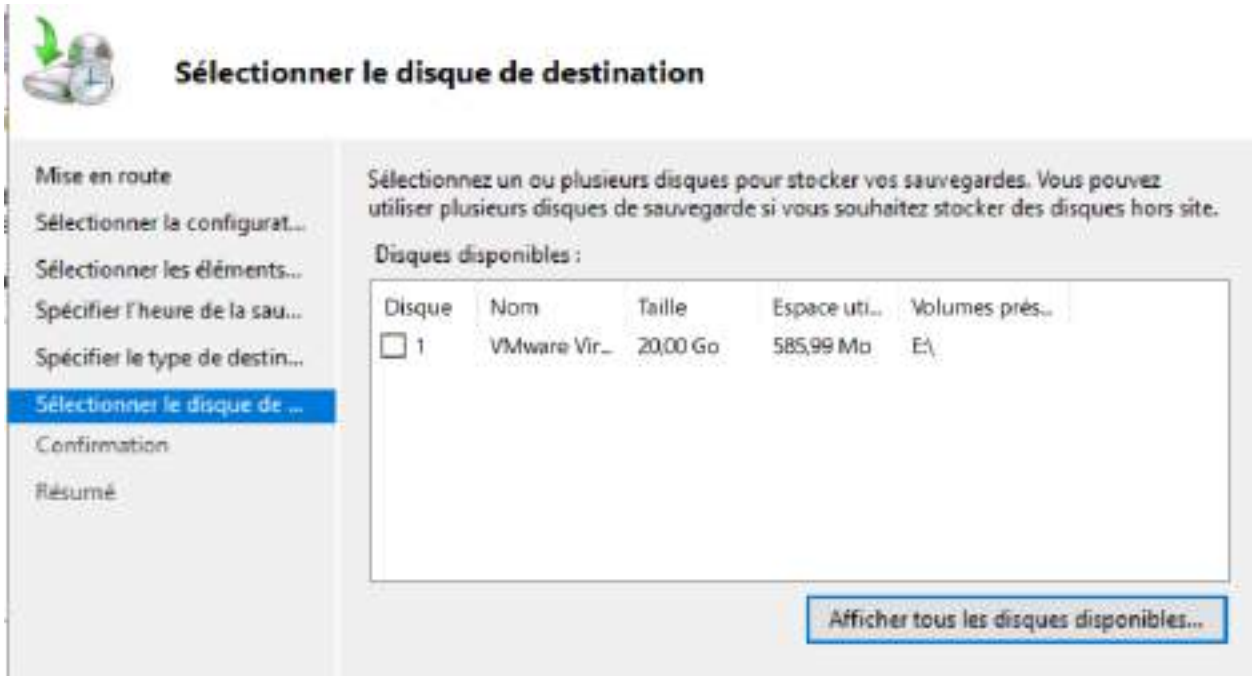
L'outil détecte ton disque `E:` → coche-le → Suivant.

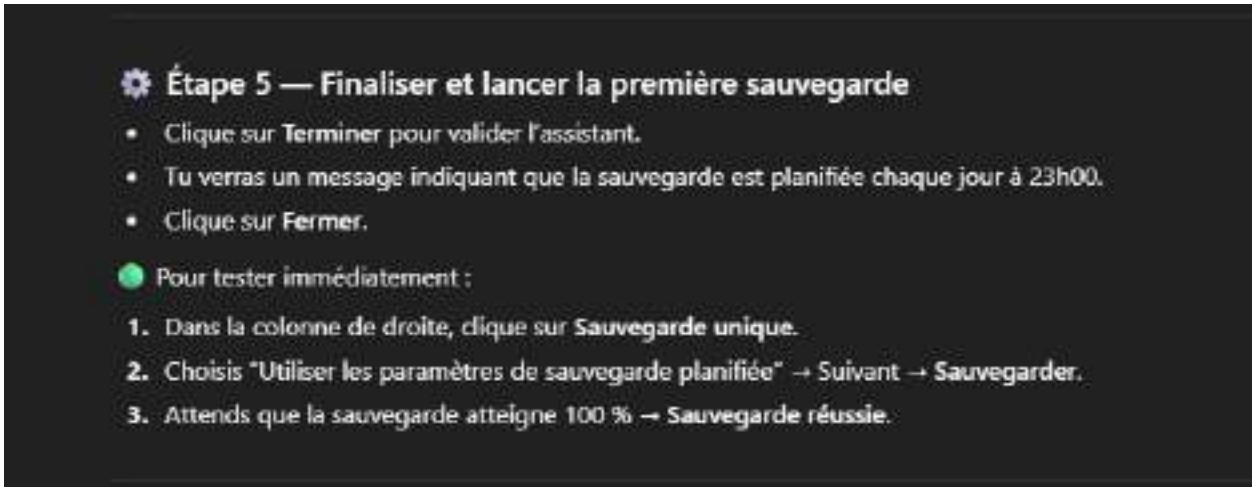
💡 L'outil va formater le disque pour en faire un disque de sauvegarde (il sera réservé aux sauvegardes).


Sélectionner la configuration de la sauvegarde
Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Confirmation
Résumé
Quel type de configuration voulez-vous planifier ?
Serveur complet (recommandé)
Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.
Taille de la sauvegarde : 13,66 Go
Personnalisé
Je veux choisir des volumes et des fichiers personnalisés pour la sauvegarde.


Sélectionner les éléments à sauvegarder
Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Confirmation
Sélectionnez les éléments à sauvegarder. La sélection d'une récupération complète offre le plus d'options si vous devez effectuer une récupération.
Nom
C:\Partage


Spécifier l'heure de la sauvegarde
Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Confirmation
Résumé
À quelle fréquence et à quel moment voulez-vous exécuter les sauvegardes ?
Tous les jours
Sélectionnez une heure :
23:00
Plusieurs fois par jour
Cliquez sur une heure disponible, puis sur Ajouter pour l'ajouter à la planification de sauvegarde.
Temps disponible :
00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
Ajouter >
< Supprimer
Heure planifiée :
21:00


Sélectionner le disque de destination
Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Sélectionner le disque de ...
Confirmation
Résumé
Sélectionnez un ou plusieurs disques pour stocker vos sauvegardes. Vous pouvez utiliser plusieurs disques de sauvegarde si vous souhaitez stocker des disques hors site.
Disques disponibles :
Disque
Nom
Taille
Espace uti...
Volumes prés...
1
VMware Vir...
20,00 Go
585,99 Mo
E:\
Afficher tous les disques disponibles...


Étape 5 — Finaliser et lancer la première sauvegarde
Clique sur Terminer pour valider l'assistant.
Tu verras un message indiquant que la sauvegarde est planifiée chaque jour à 23h00.
Clique sur Fermer.
Pour tester immédiatement :
1. Dans la colonne de droite, clique sur Sauvegarde unique.
2. Choisis "Utiliser les paramètres de sauvegarde planifiée" → Suivant → Sauvegarder.
3. Attends que la sauvegarde atteigne 100 % → Sauvegarde réussie.


Résumé
Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Sélectionner le disque de ...
Confirmation
Résumé
Statut : La planification de sauvegarde a bien été créée.
Votre première sauvegarde planifiée aura lieu à 24/10/2025 23:00.
Vérifiez que les disques utilisés pour stocker les sauvegardes planifiées sont connectés à cet ordinateur et accessibles.

✅ **Vérifie dans :**

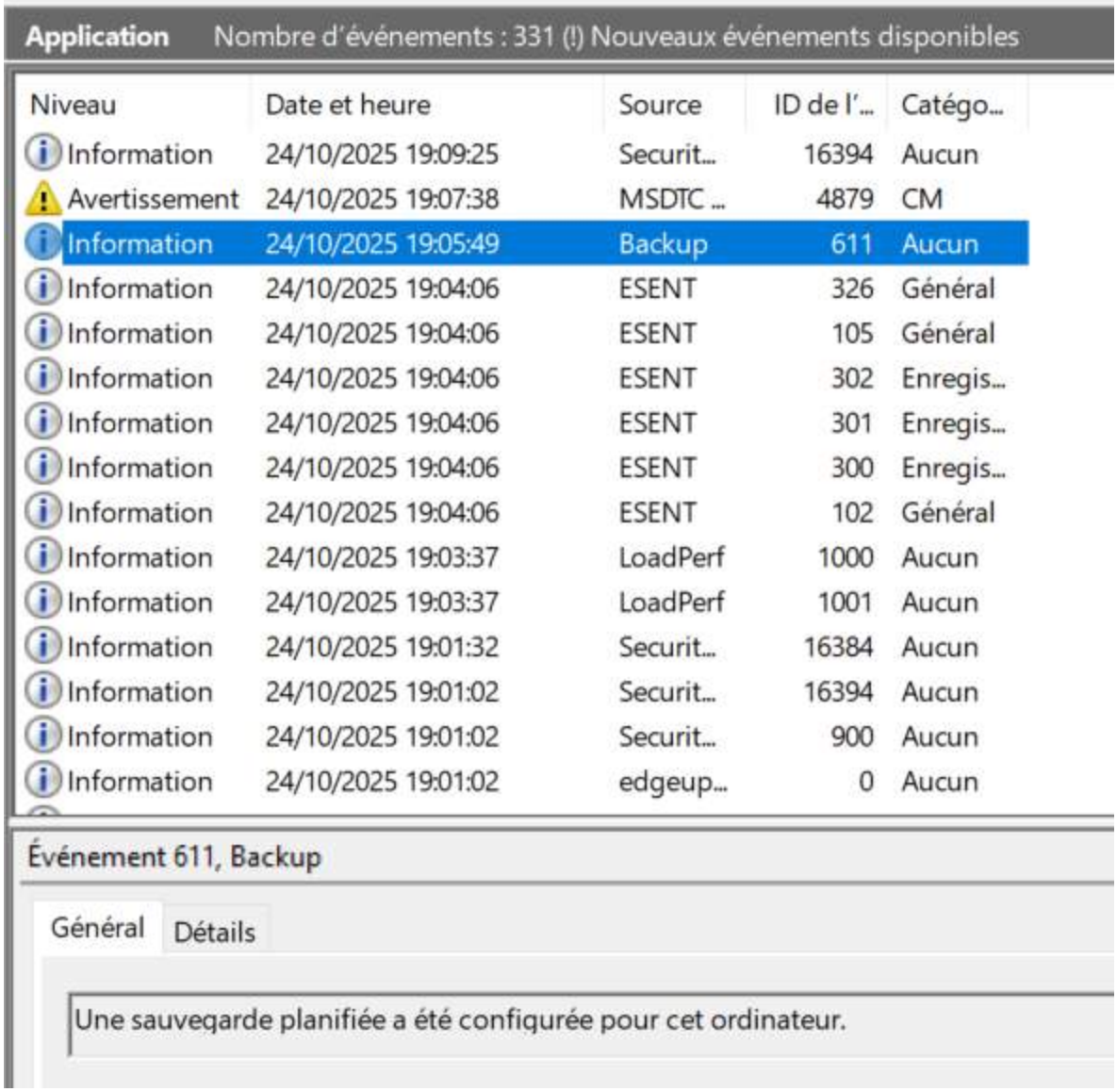
- `E:\WindowsImageBackup` → tu verras les fichiers de ta sauvegarde.
- Ouvre l'**Observateur d'événements** → Journaux Windows → **Applications** → tu verras une entrée "Backup completed successfully".

✅ **Test de restauration (facultatif pour la soutenance)**

1. Dans **Sauvegarde Windows Server**, clique sur **Restaurez**.
2. Choisis "Cette machine" → Sélectionne le volume ou le dossier `C:\Partages`.
3. Suis l'assistant pour restaurer un fichier supprimé.

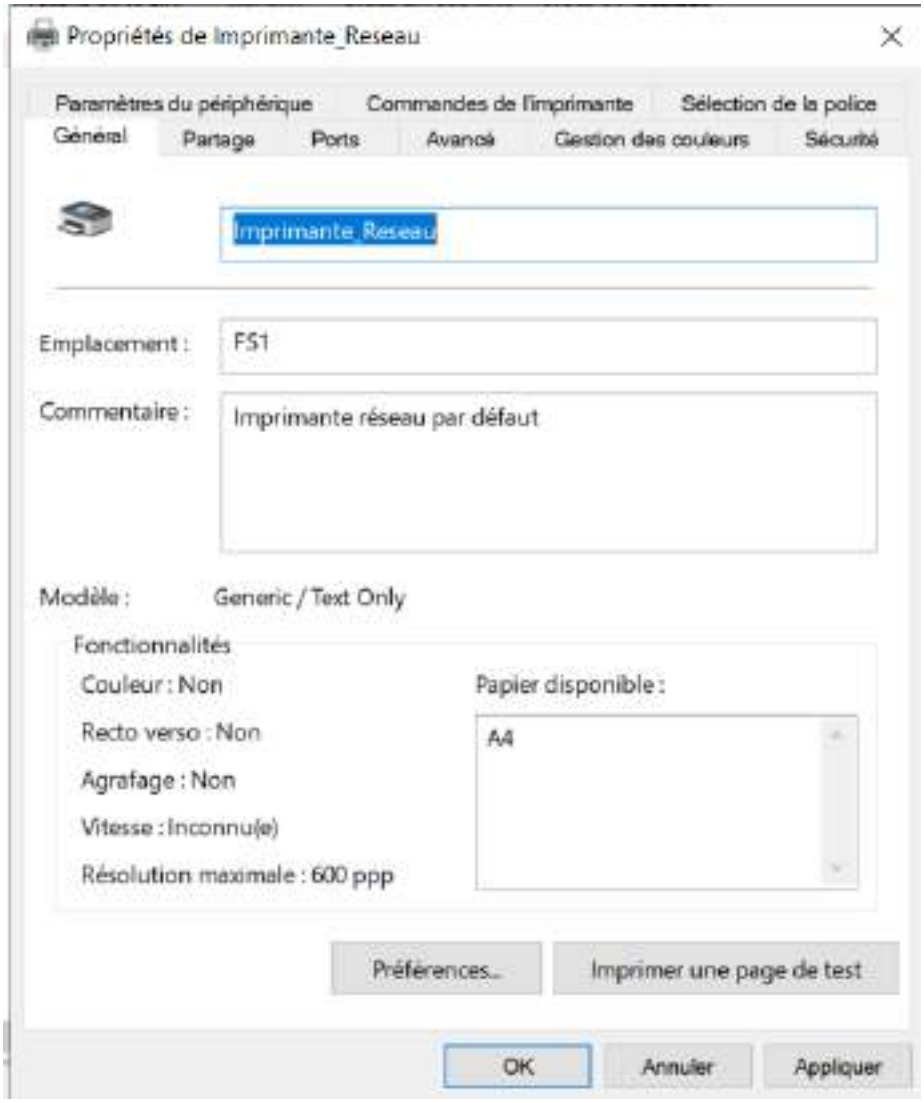
📄 **Exemple à écrire dans ton rapport :**

> Une **sauvegarde planifiée quotidienne** a été configurée sur le serveur FS1 à l'aide de l'outil **Sauvegarde Windows Server**.
> Elle s'exécute chaque soir à **23h00**, et enregistre une copie complète des données du répertoire `C:\Partages` sur un second disque virtuel (`E:`).
> En cas de perte de données ou de panne du serveur, cette configuration permet une **restauration rapide** des fichiers critiques.
> Pour la démonstration, une sauvegarde manuelle a été effectuée avec succès via l'outil "Sauvegarde unique".


Application Nombre d'événements : 331 (!) Nouveaux événements disponibles
Niveau Date et heure Source ID de l'... Catégo...
Information 24/10/2025 19:09:25 Securit... 16394 Aucun
Avertissement 24/10/2025 19:07:38 MSDTC ... 4879 CM
Information 24/10/2025 19:05:49 Backup 611 Aucun
Information 24/10/2025 19:04:06 ESENT 326 Général
Information 24/10/2025 19:04:06 ESENT 105 Général
Information 24/10/2025 19:04:06 ESENT 302 Enregis...
Information 24/10/2025 19:04:06 ESENT 301 Enregis...
Information 24/10/2025 19:04:06 ESENT 300 Enregis...
Information 24/10/2025 19:04:06 ESENT 102 Général
Information 24/10/2025 19:03:37 LoadPerf 1000 Aucun
Information 24/10/2025 19:03:37 LoadPerf 1001 Aucun
Information 24/10/2025 19:01:32 Securit... 16384 Aucun
Information 24/10/2025 19:01:02 Securit... 16394 Aucun
Information 24/10/2025 19:01:02 Securit... 900 Aucun
Information 24/10/2025 19:01:02 edgeup... 0 Aucun
Événement 611, Backup
Général Détails
Une sauvegarde planifiée a été configurée pour cet ordinateur.

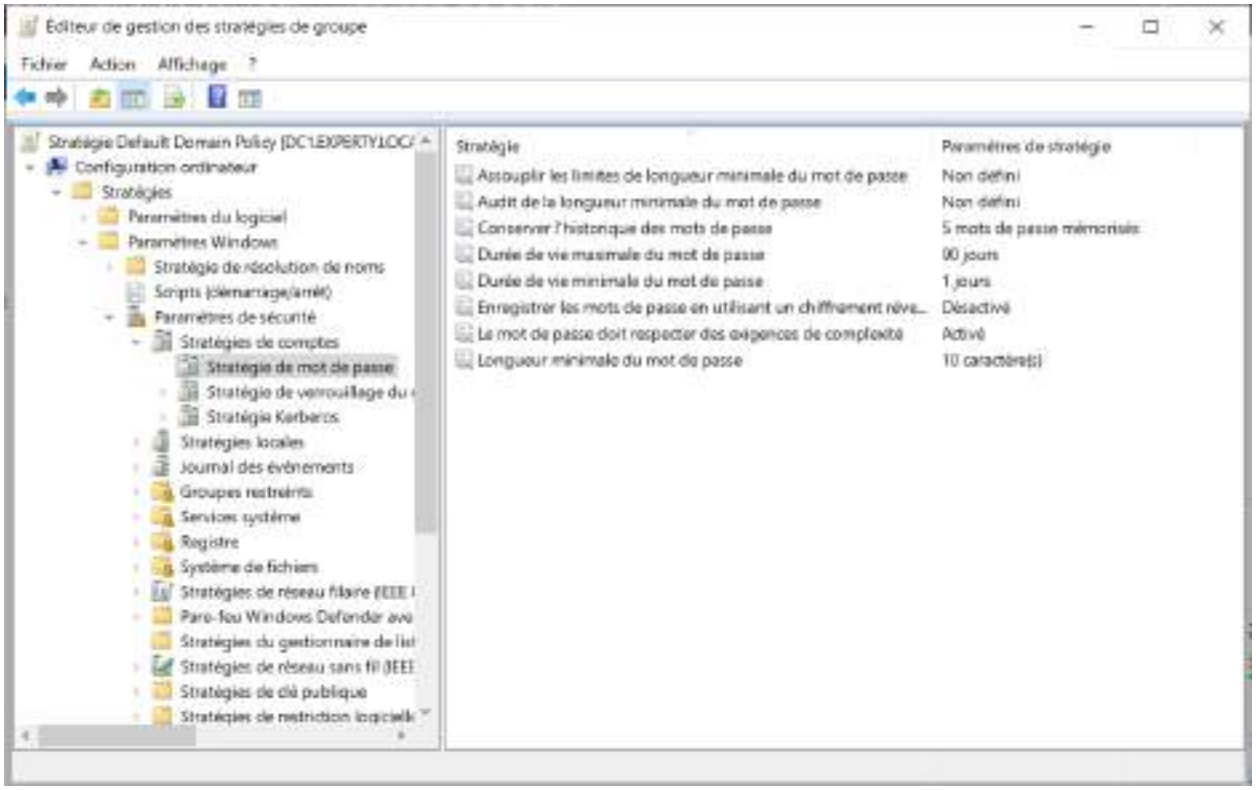
Service d'impression

Élément	État	Détails / Actions
Imprimante installée sur tous les postes via GPO	✅	Créée et déployée via `\\FS1\Imprimante_Reseau` + GPO sur DC1.
Paramétrage par défaut (NB recto-verso)	⚙	À vérifier → Propriétés de l'imprimante sur FS1 → onglet "Préférences" → activer "Noir et blanc" et "Recto-verso".



GPO


1 Politique de mots de passe (préconisation ANSSI)
Objectif : renforcer la sécurité du domaine selon les règles ANSSI.
Tu vas appliquer une politique de mot de passe via la stratégie de sécurité du domaine.
Tout se fait sur DC1.
Étapes exactes :
1. Sur DC1, ouvre :
Outils → Gestion des stratégies de groupe (GPMC)
2. Clique droit sur :
pgsql
Copier le code
Default Domain Policy
→ puis Modifier.
(C'est la stratégie qui s'applique à tout ton domaine.)
3. Dans l'éditeur :
markdown
Copier le code
Configuration ordinateur
→ Stratégies
→ Paramètres Windows
→ Paramètres de sécurité
→ Stratégies de compte
→ Stratégie de mot de passe
4. Configure ainsi (préconisations ANSSI adaptées à ton projet) :
Appliquer l'historique des mots de passe : 5
Durée de vie maximale du mot de passe : 90 jours
Durée de vie minimale du mot de passe : 1 jour
Longueur minimale du mot de passe : 10 caractères
Le mot de passe doit respecter les exigences de complexité : Activé
Stocker les mots de passe avec chiffrement réversible : Désactivé
5. Ferme l'éditeur → les changements sont enregistrés automatiquement.
6. Force l'application sur le domaine :
Poser une question



- Chaque utilisateur doit disposer d'un dossier personnel P : (limité à 1Go avec alerte en cas de dépassement 10%) accessible uniquement par lui et le service informa+tique.V

Création des dossiers personnels et quotas utilisateurs sur FS1

Étape 1 – Créer le dossier principal des profils et des données personnelles

1. Sur **FS1**, ouvre l'**Explorateur de fichiers**.
2. Dans ton disque principal (C:), crée un dossier :

```
maicefile                                                    Copier le code

C:\Profils
```

3. Clique droit sur ce dossier → **Propriétés** → **Partage** → **Partage avancé**.
   - Coche **Partager ce dossier**.
   - Nom du partage :

```
nginx                                                        Copier le code

Profils
```

   - Clique sur **Autorisations** → supprime "Tout le monde".
   - Clique sur **Ajouter** → tape `Tout le monde` → OK.
     - Coche **Lecture** uniquement (pour que tout le monde voie le partage, mais sans modifier).
   - Clique sur **Ajouter** → tape `Administrateurs` → OK.
     - Coche **Contrôle total**.
   - Clique sur **OK** → **Appliquer** → **OK**.

✅ Ton partage est accessible via :

```
                                                             Copier le code

\\FS1\Profils
```

⚙️ Étape 2 – Configurer le chemin du dossier personnel pour chaque utilisateur

> On fait ça sur DC1 (dans l'Active Directory).

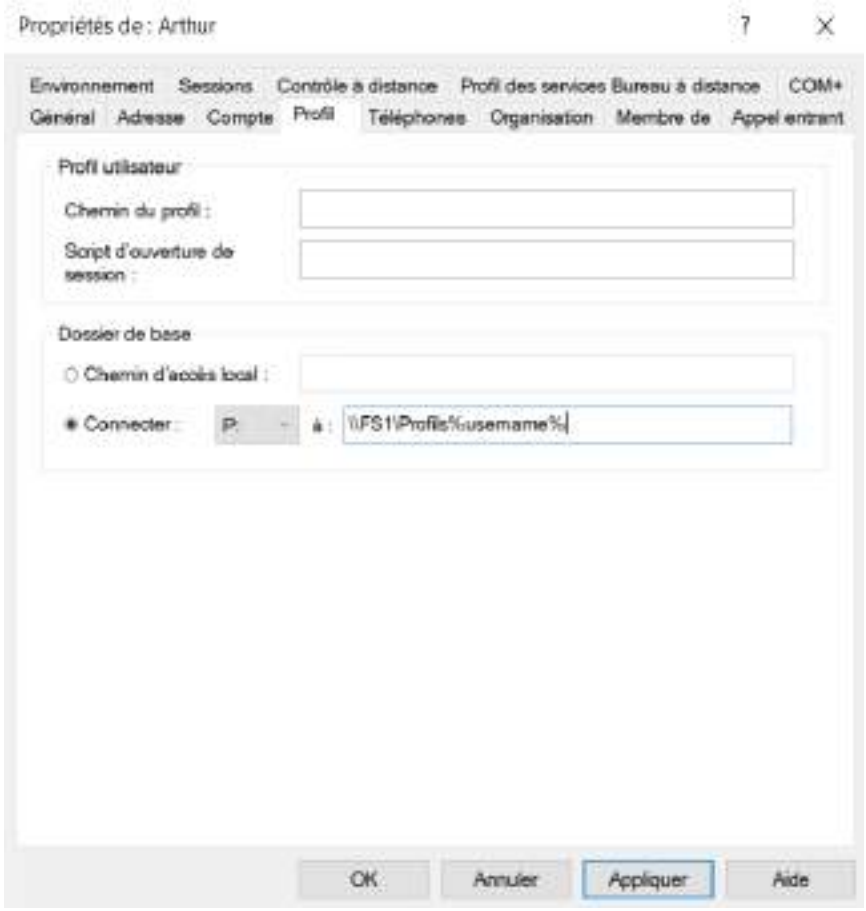
1. Ouvre **Outils → Utilisateurs et ordinateurs Active Directory**.
2. Ouvre l'OU `Utilisateurs` → puis le service, ex. `Comptabilite`.
3. Clique droit sur `j.martin` → **Propriétés**.
4. Onglet **Profil** :
   - Dans "Dossier personnel", coche :
     Connecter : P: à \FS1\Profils%username%
     (ou **\FS1\Profils\j.martin** si tu veux le définir manuellement).
   - Clique sur **Appliquer → OK**.

💡 Fais pareil pour chaque utilisateur.
→ Lorsqu'il se connectera, Windows créera automatiquement son dossier personnel sur FS1.

⚙️ Étape 3 – Vérifier les permissions des dossiers personnels

1. Sur FS1, ouvre `C:\Profils`.
2. Tu verras que des dossiers se créent pour chaque utilisateur (ex. `j.martin`, `b.simon`…).
3. Clique droit sur un dossier (ex. `j.martin`) → **Propriétés → Sécurité**.
   - L'utilisateur (`experty\j.martin`) doit avoir **Contrôle total**.
   - Les **Administrateurs** ont **Lecture / Exécution** seulement.
   - Aucun autre utilisateur ne doit avoir accès.

✅ Tu garantis que chaque dossier personnel est privé.



Étape 4 – Installer l'outil de gestion des quotas (FSRM)

1. Sur **FS1**, ouvre le **Gestionnaire de serveur**.
2. Clique sur **Gérer → Ajouter des rôles et fonctionnalités**.
3. Clique sur **Suivant** jusqu'à **Fonctionnalités**.
4. Coche :

```arduino
Gestionnaire de ressources du serveur de fichiers (File Server Resource Manager)
```

5. Clique sur **Suivant → Installer**.
6. Une fois terminé, redémarre FS1 si demandé.

Fonctionne

GPO Utilisateur :

🧱 PHASE 1 : LES GPO UTILISATEURS

Tout se fait depuis ton **DC1**, dans la console "Gestion des stratégies de groupe (GPMC)".

⚙️ Étape 1 — Ouvrir la console GPMC

1. Sur **DC1**, ouvre le **Gestionnaire de serveur**.
2. Clique en haut à droite sur **Outils → Gestion des stratégies de groupe**.
   👉 Tu verras ton domaine :

```
axperty.local
```

3. Clique droit sur **"Objets de stratégie de groupe" → Nouveau**.
   - Nom : `GPO_Utilisateurs_Experty`
     → Clique sur **OK**.
4. Clique droit sur cette GPO → **Modifier**.

⚙️ Étape 2 — Mappage des lecteurs réseau (lecteurs T:, P:, I:)

> On va créer les lecteurs T: (Tous), P: (Personnel) et I: (Informatique).
> Ces lecteurs apparaîtront automatiquement sur le poste client au démarrage.

Dans l'éditeur GPO :

1. Va dans :

```
Configuration utilisateur
  → Préférences
    → Lecteurs réseau
```

2. Clique droit → **Nouveau → Lecteur réseau**.

- **Lecteur T: (tous)**
- **Action :** Mettre à jour
- **Emplacement :**

```
\\axperty.local\partage
```

- **Lettre du lecteur :** T
- **Reconnecter :** coché

- **Lettre du lecteur :** T
- **Reconnecter :** coché
- Clique sur **OK**.

- **Lecteur P: (personnel)**
- Recommence :
  - **Action :** Créer
  - **Emplacement :**

```matlab
\\FS1\Profils\%username%
```

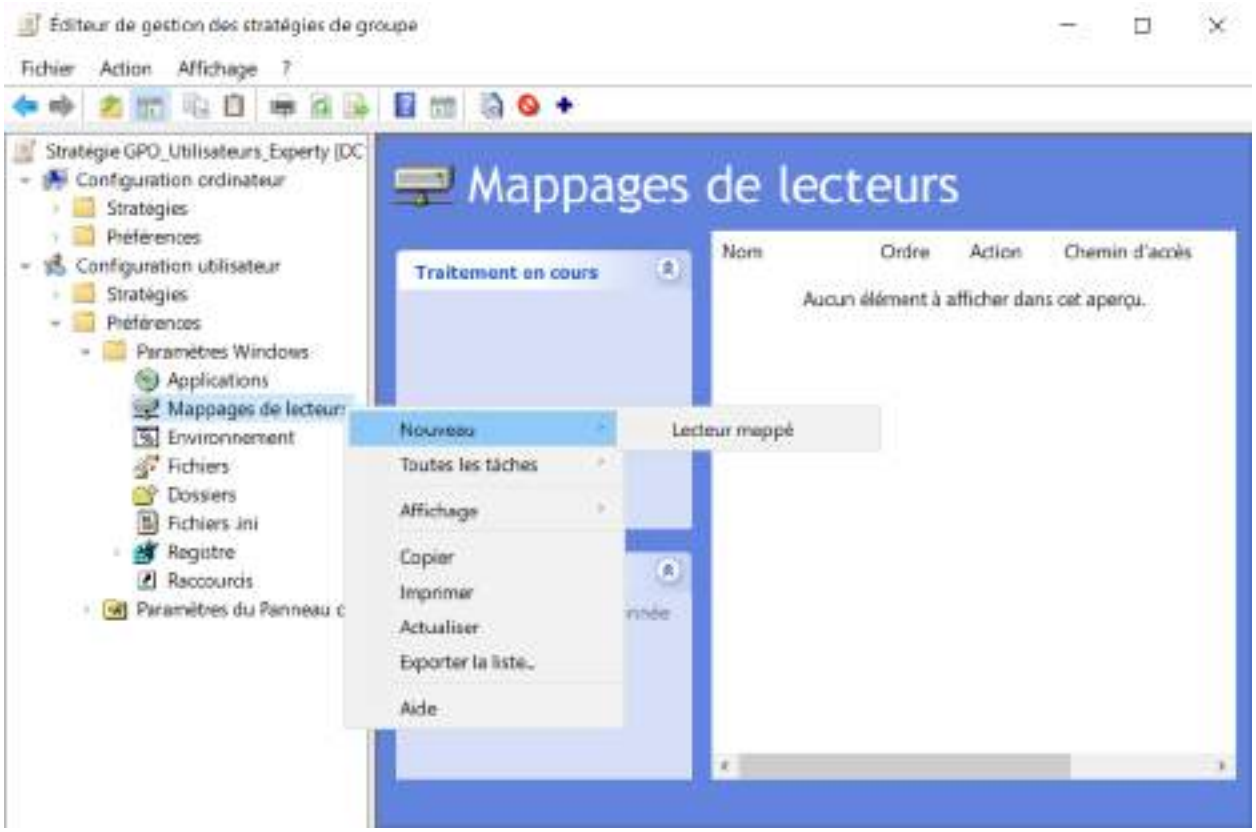
  - **Lettre du lecteur :** P
  - **Reconnecter :** coché
  - Clique sur **OK**.

- **Lecteur I: (informatique)**
- **Action :** Créer
- **Emplacement :**

```bat
\\exporty.local\partage\Informatique
```

- **Lettre du lecteur :** I
- **Reconnecter :** coché
- Clique sur **OK**.

Ferme la fenêtre.


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Utilisateurs_Experty [DC
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètres Windows
Applications
Mappages de lecteurs
Environnement
Fichiers
Dossiers
Fichiers ini
Registre
Raccourcis
Paramètres du Panneau c
Mappages de lecteurs
Traitement en cours
Nom
Ordre
Action
Chemin d'accès
Aucun élément à afficher dans cet aperçu.
Nouveau
Lecteur mappé
Toutes les tâches
Affichage
Copier
Imprimer
Actualiser
Exporter la liste...
Aide


Propriétés de : T:
Général
Commun
Action :
Mettre à jour
Emplacement :
\\experty.local\partage
...
Reconnecter :
Libeller en tant que :
Lettre de lecteur
Utiliser le premier disponible, en commençant à :
Utiliser :
T
Se connecter en tant que (facultatif)
Nom d'utilisateur :
Mot de passe :
Confirmer le mot de passe
Masquer/Afficher ce lecteur
Aucune modification
Masquer ce lecteur
Afficher ce lecteur
Masquer/Afficher tous les lecteurs
Aucune modification
Masquer tous les lecteurs
Afficher tous les lecteurs
OK
Annuler
Appliquer
Aide

⚙️ Étape 3 — Appliquer un fond d'écran "Experty" (logo)

Prépare ton image :

1. Copie ton image (ex. `logo_experty.jpg`) dans un dossier partagé accessible à tous :

```
\\FS1\Partages\Informatique\FondEcran
```

2. Vérifie que tous les utilisateurs ont **au moins les droits de lecture** dessus.

Dans l'éditeur GPO :

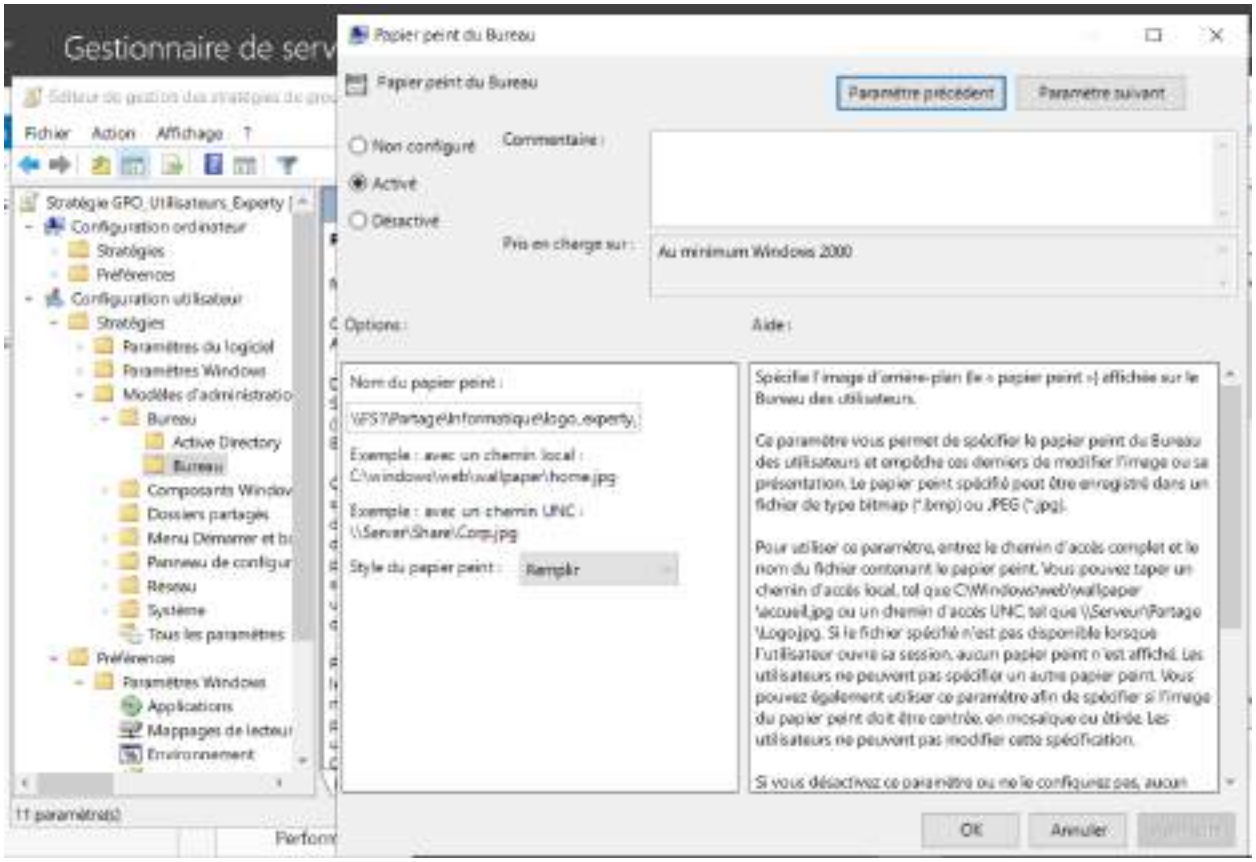
1. Va dans :

```
Configuration utilisateur
  → Stratégies
    → Modèles d'administration
      → Bureau
        → Bureau
```

2. Double-clique sur **"Papier peint du bureau"**.
   - Active cette stratégie.
   - Chemin d'accès au papier peint :

```
\\FS1\Partages\Informatique\FondEcran\logo_experty.jpg
```

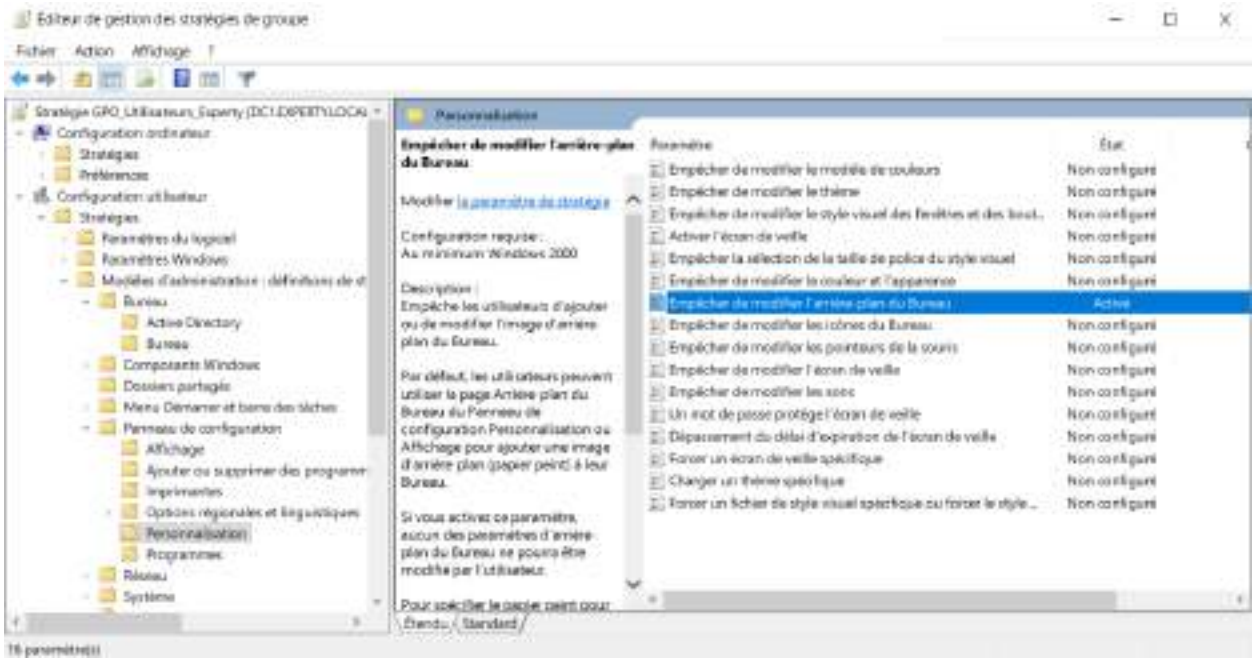
   - Style : **Rempli.**
   - Clique sur **Appliquer → OK.**
3. Toujours dans le même dossier "Bureau", double-clique sur :
   "Empêcher la modification du papier peint" → Active → OK.



Étape 1 — Le bon emplacement

Dans ton **Éditeur de gestion des stratégies de groupe (GPO)**, navigue ici :

```pgsql
Configuration utilisateur
   → Modèles d'administration
      → Panneau de configuration
         → Personnalisation
```



⚙ Étape 4 — Restreindre l'accès (sécurité des postes)

Dans l'éditeur GPO :

- **Bloquer l'accès à l'invite de commande :**

vbnet — Copier le code

```
Configuration utilisateur → Stratégies → Modèles d'administration → Système
```

- Double-clique sur "Empêcher l'accès à l'invite de commandes".
- Active la stratégie → coche "Oui" pour désactiver les scripts CMD.

- **Interdire la modification de la carte réseau :**

Copier le code

```
Configuration utilisateur → Stratégies → Modèles d'administration → Réseau → Connexions réseau
```

- Double-clique sur "Interdire aux utilisateurs de modifier les composants de la configuration réseau" → Active.

- **Mettre l'écran en veille après 15 minutes :**

```
pgsql
```

Copier le code

```
Configuration utilisateur → Préférences → Panneau de configuration → Options d'alimentation
```

- Clique droit → Nouveau → Options d'alimentation.
- Mets "Écran éteint après 15 minutes".

- **Définir la page d'accueil Firefox :**

> (si tu as Firefox installé sur les postes clients)

```
bash
```

Copier le code

```
Configuration utilisateur → Préférences → Paramètres du Registre
```

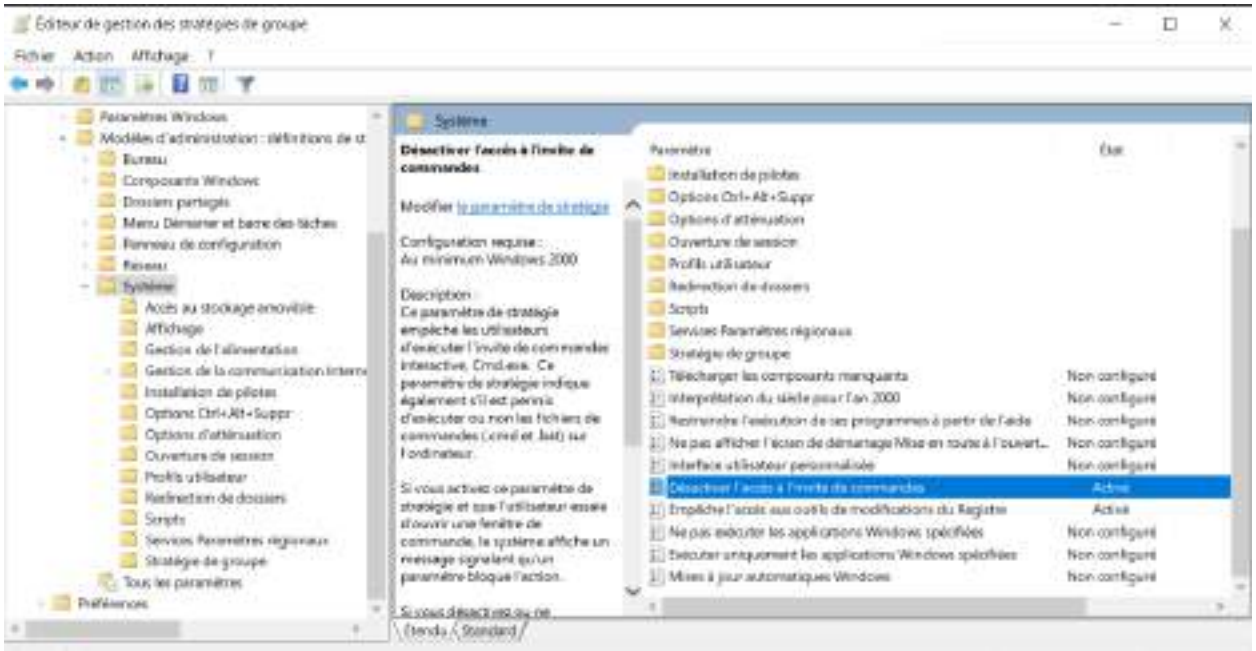
- Clique droit → Nouveau → Élément du registre.
- Clé :

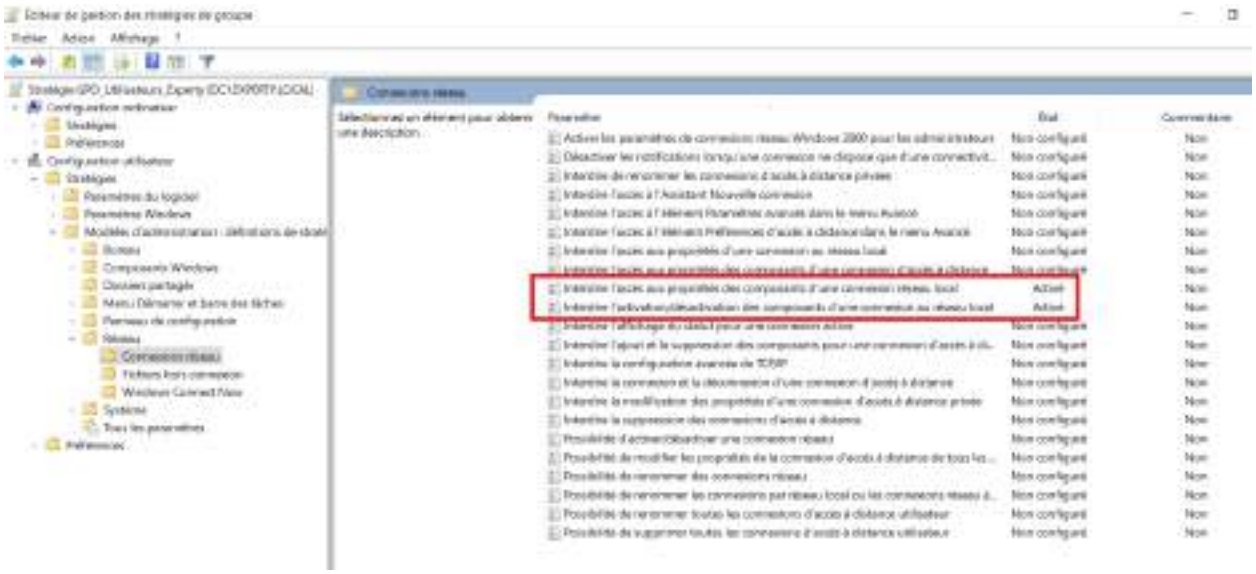
```
css
```

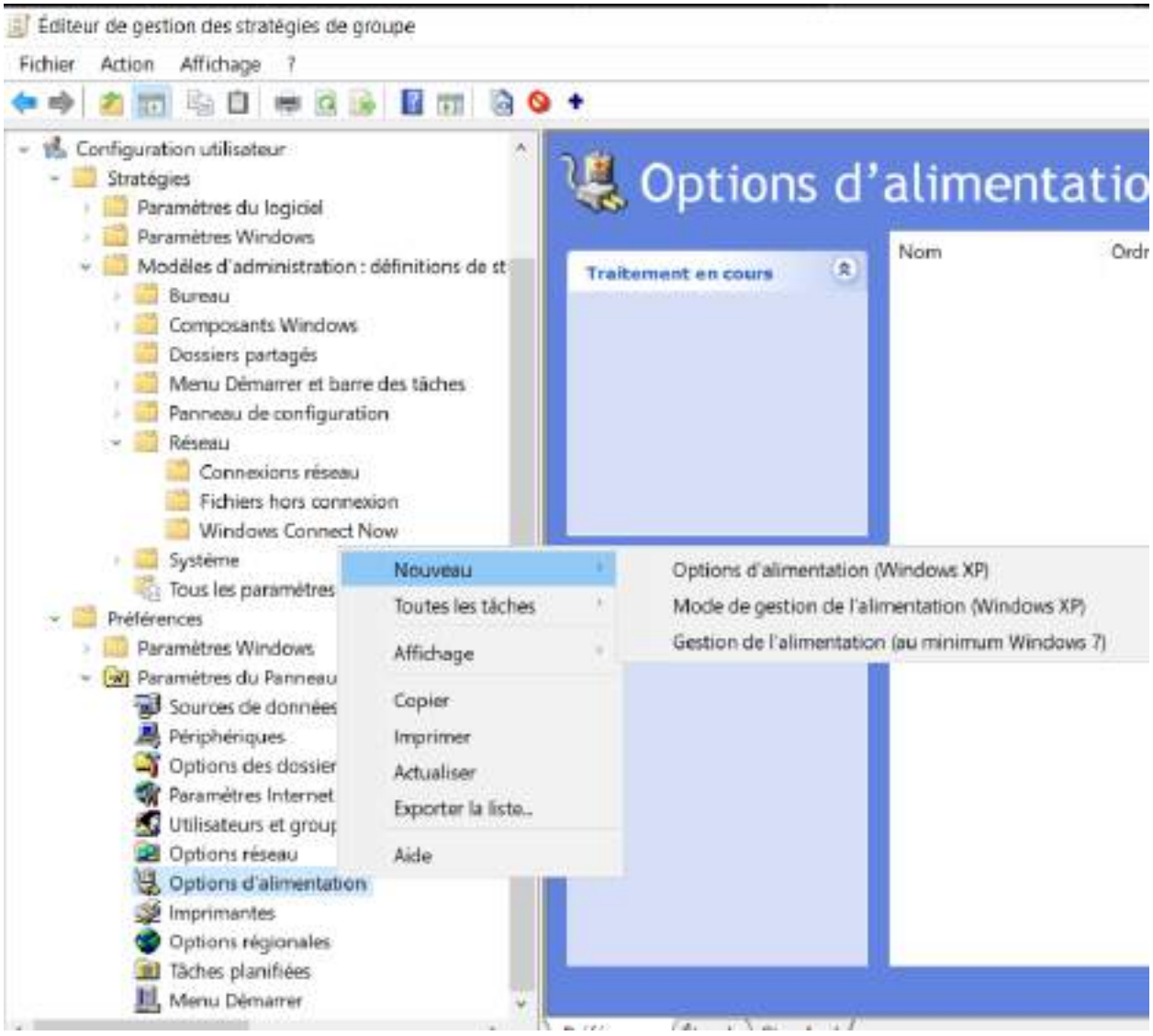
Copier le code

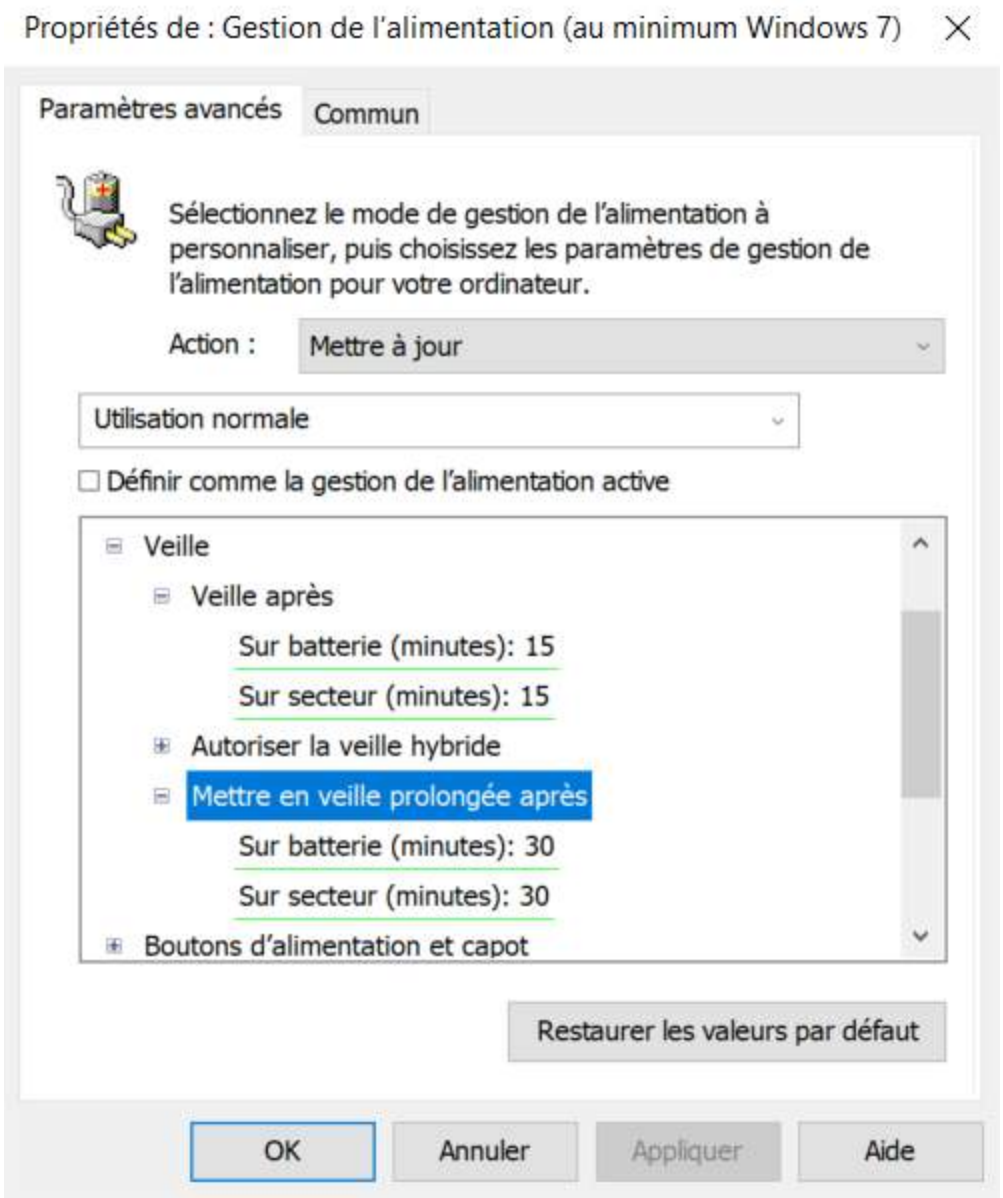
```
HKCU\Software\Mozilla\Firefox\Main
```

- Nom de valeur : `HomePage`
- Donnée : `http://intranet.experty.local`
- Type : REG_SZ.
- Clique sur OK.






Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Configuration utilisateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Modèles d'administration : définitions de st
Bureau
Composants Windows
Dossiers partagés
Menu Démarrer et barre des tâches
Panneau de configuration
Réseau
Connexions réseau
Fichiers hors connexion
Windows Connect Now
Système
Tous les paramètres
Préférences
Paramètres Windows
Paramètres du Panneau
Sources de données
Périphériques
Options des dossier
Paramètres Internet
Utilisateurs et group
Options réseau
Options d'alimentation
Imprimantes
Options régionales
Tâches planifiées
Menu Démarrer
Options d'alimentatio
Traitement en cours
Nom
Nouveau
Toutes les tâches
Affichage
Copier
Imprimer
Actualiser
Exporter la liste...
Aide
Options d'alimentation (Windows XP)
Mode de gestion de l'alimentation (Windows XP)
Gestion de l'alimentation (au minimum Windows 7)


Propriétés de : Gestion de l'alimentation (au minimum Windows 7)
Paramètres avancés
Commun
Sélectionnez le mode de gestion de l'alimentation à personnaliser, puis choisissez les paramètres de gestion de l'alimentation pour votre ordinateur.
Action :
Mettre à jour
Utilisation normale
Définir comme la gestion de l'alimentation active
Veille
Veille après
Sur batterie (minutes): 15
Sur secteur (minutes): 15
Autoriser la veille hybride
Mettre en veille prolongée après
Sur batterie (minutes): 30
Sur secteur (minutes): 30
Boutons d'alimentation et capot
Restaurer les valeurs par défaut
OK
Annuler
Appliquer
Aide


Oui ✅ tu dois installer Firefox sur ta machine cliente avant de pouvoir définir une page d'accueil via GPO, sinon la stratégie ne s'appliquera pas (puisque les paramètres Firefox n'existeront pas encore sur le poste).
🌟 Étapes complètes à suivre :
🖥️ 1. Installer Firefox sur la machine cliente
Télécharge Firefox ESR (version entreprise, plus stable pour les GPO) :
👉 https://www.mozilla.org/firefox/enterprise ↗
Installe-le manuellement sur ton client (ou par GPO si tu veux aller plus loin).
⚙️ 2. Préparer le modèle ADMX de Firefox sur ton DC
Pour gérer Firefox via GPO, il faut ajouter les modèles d'administration (ADMX) de Mozilla :
1. Télécharge les modèles :
👉 https://github.com/mozilla/policy-templates/releases ↗
2. Décompresse le dossier ZIP.
3. Copie les fichiers suivants :
firefox.admx → dans :
C:\Windows\PolicyDefinitions
Le dossier fr-FR (ou en-US selon ta langue) → dans :
C:\Windows\PolicyDefinitions\fr-FR
💡 Fais-le sur DC1 pour centraliser les modèles GPO.

3. Créer la GPO pour définir la page d'accueil

1. Ouvre la **console GPMC** (`gpmc.msc`) sur ton DC.
2. Clique droit sur ton OU "Utilisateurs" → **Créer un nouvel objet GPO** → nomme-le par exemple :
   👉 `GPO - Firefox Page Accueil`
3. Clique droit → **Modifier**.
4. Va dans :

```
vbnet                                                    Copier le code

Configuration utilisateur
└── Modèles d'administration
    └── Mozilla
        └── Firefox
```

5. Trouve et configure :
   - **Homepage** → "Définir la page d'accueil, la nouvelle fenêtre et la nouvelle session"
     → Active et mets ton URL (par exemple `http://intranet.experty.local`)
   - Facultatif : **Prevent changing homepage** → Active pour bloquer la modification.

---

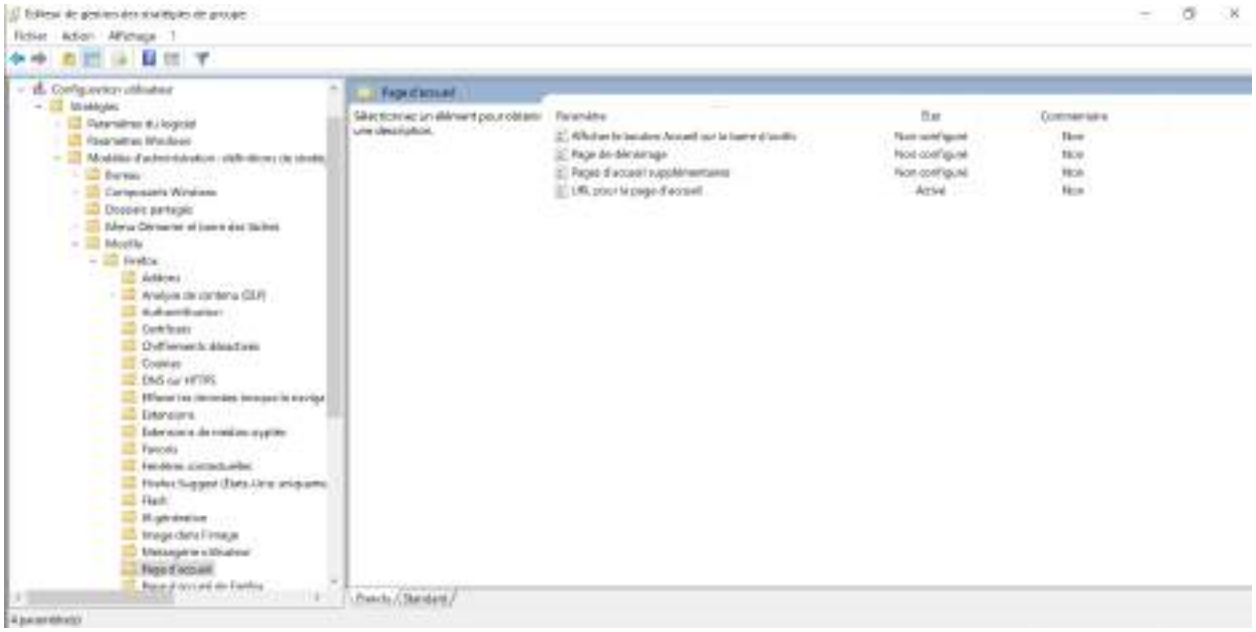
4. Appliquer et tester

1. Sur le client :
   - Ouvre une session avec un utilisateur du domaine.
   - Lance `cmd` → tape :

```
bash                                                     Copier le code

gpupdate /force
```

   - Redémarre si besoin.
2. Ouvre Firefox → Il doit s'ouvrir sur ton intranet expertv.local par défaut 🚀

Poser une question



. Ouvre une invite de commande en admi

```bash
gpupdate /force
```

🧱 Création des dossiers personnels et profils itinérants

(sur FS1 et DC1)

🎯 Objectif

Chaque utilisateur doit avoir :

- un **dossier personnel P:** (`\\FS1\Profils\%username%`), limité à 1 Go,
- un **profil itinérant**, pour retrouver son bureau et documents depuis n'importe quel poste,
- des **droits d'accès sécurisés** (lui seul + administrateurs du domaine).

⚙️ Étape 1 — Préparer la structure sur FS1

Sur **FS1**, fais ceci :

1. Ouvre **l'explorateur de fichiers**.
2. Va dans ton disque principal :

```makefile
C:\
```

3. Crée deux dossiers distincts :

```makefile
C:\Profils
C:\Personnels
```

💡 **Explication :**

- `C:\Profils` → pour les **profils itinérants** (AppData, bureau, etc.)
- `C:\Personnels` → pour les **dossiers personnels (lecteur P:)**

⚙️ Étape 2 — Partager les dossiers

On va partager ces dossiers sur le réseau pour qu'ils soient accessibles depuis le domaine.

🔹 **Partage du dossier Profils**

1. Clique droit sur `C:\Profils` → **Propriétés** → Onglet **Partage** → **Partage avancé**.
2. Coche **Partager ce dossier**.
3. Nom du partage :

```nginx
Profils
```

4. Clique sur **Autorisations** →
   - Supprime "Tout le monde".
   - Clique sur **Ajouter** → tape :

```nginx
Authenticated Users
```

   → Clique sur **OK**.
   - Donne-leur uniquement le droit **Modification** (pas contrôle total).
   - Clique sur **OK**.
5. Clique sur **Appliquer** → **OK** → **Fermer**.

⚙️ Étape 3 — Créer les dossiers utilisateurs automatiquement

On ne crée pas chaque dossier à la main : c'est Active Directory qui s'en charge.
On va configurer le chemin pour chaque utilisateur.

Sur **DC1** :

1. Ouvre **Outils → Utilisateurs et ordinateurs Active Directory**.
2. Va dans ton OU **Utilisateurs** (ou l'unité d'organisation correspondant à ton service).
3. Clique droit sur un utilisateur (ex. `test1`) → **Propriétés**.

Onglet Profil :

Tu verras 2 champs à remplir 👇

- **Profil itinérant :**

Chemin du profil :

```
matlab                                                    Copier le code

\\FS1\Profils\%username%
```

- **Dossier personnel (Lecteur P:)**

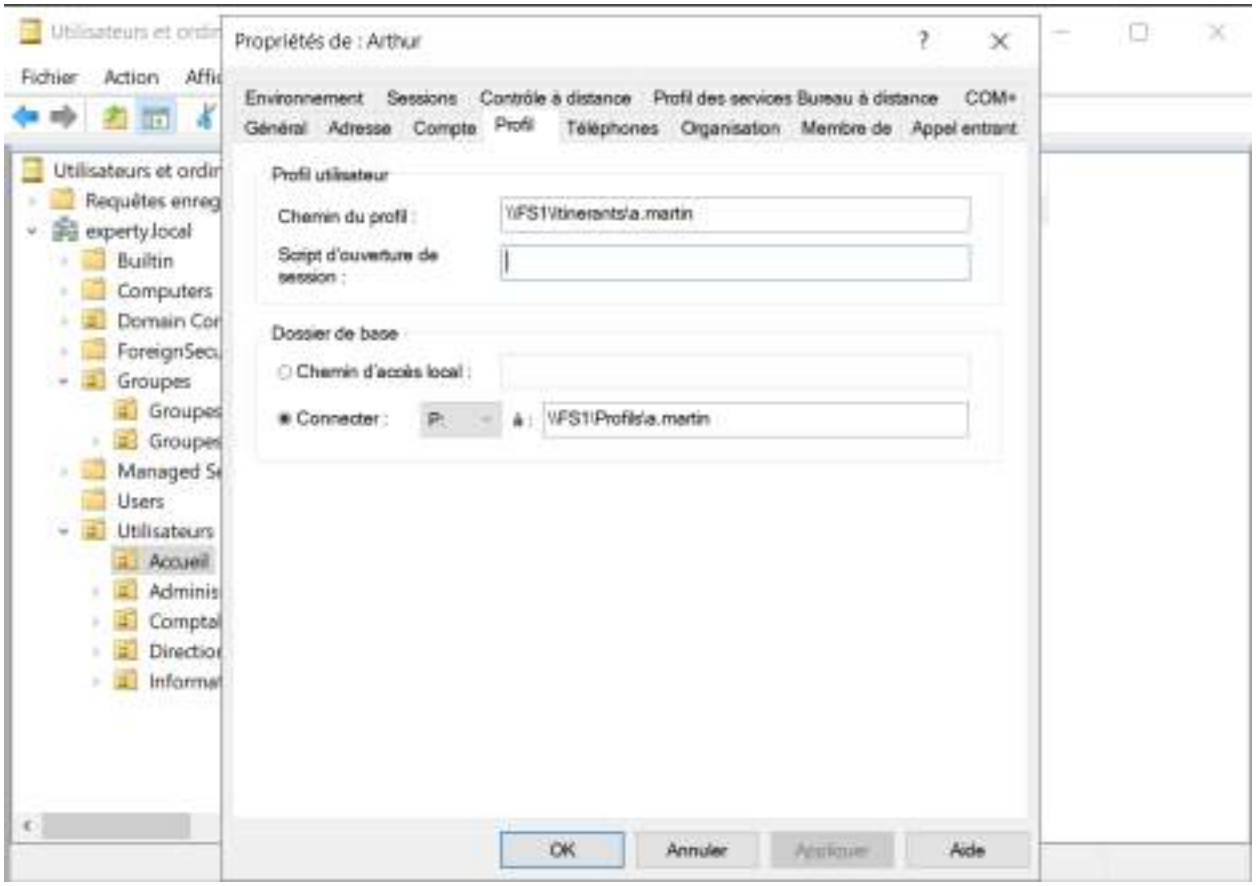
Choisis :

- **Connecter :** P:
- **À :**

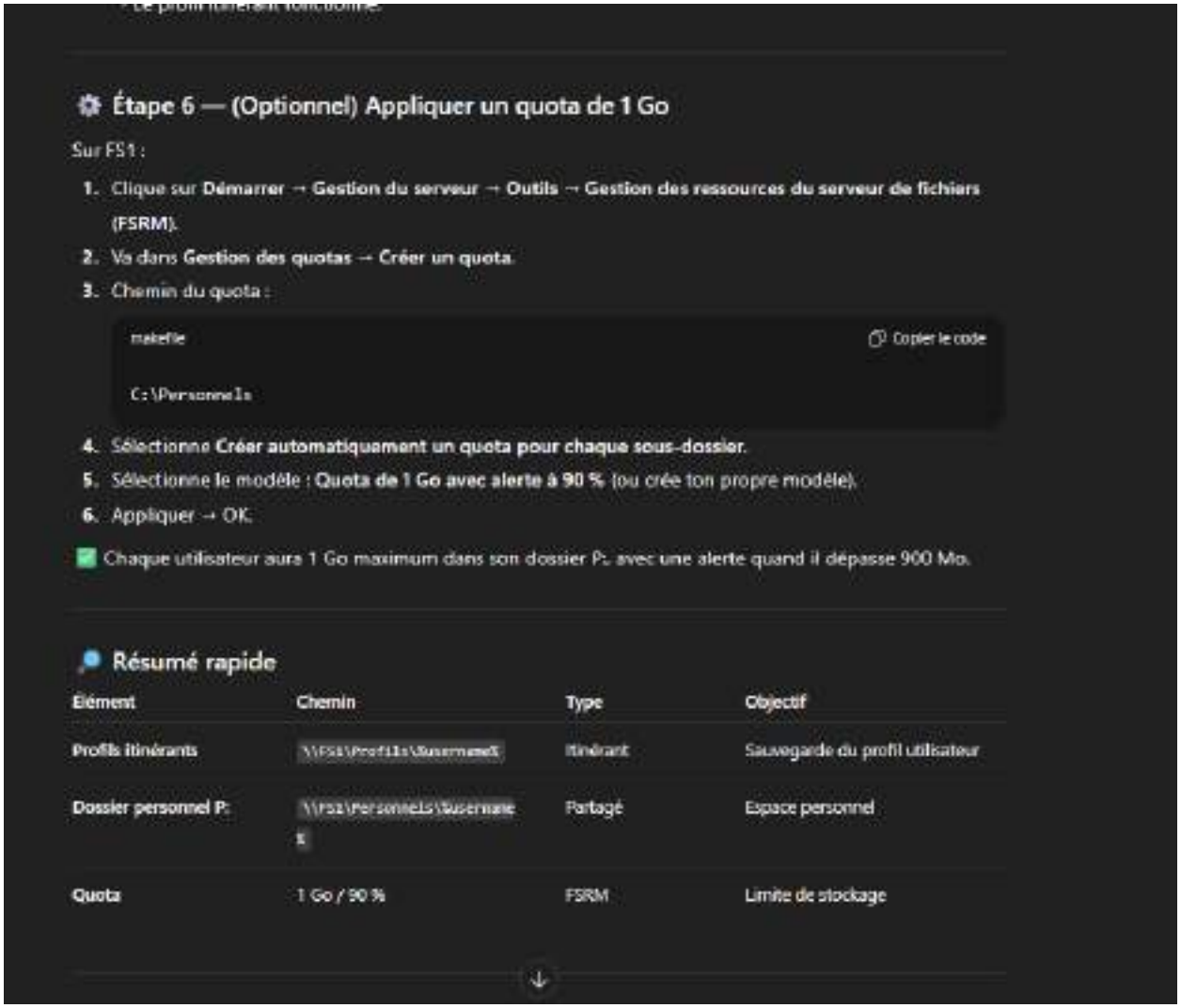
```
matlab                                                    Copier le code

\\FS1\Personnels\%username%
```

Clique sur **Appliquer → OK**.

💡 Quand l'utilisateur se connectera, le serveur FS1 créera automatiquement un dossier portant son nom (`\\FS1\Personnels\test1`) et configurera les droits [illegible] corrects (accès exclusif).


Propriétés de : Arthur
Environnement
Sessions
Contrôle à distance
Profil des services Bureau à distance
COM+
Général
Adresse
Compte
Profil
Téléphones
Organisation
Membre de
Appel entrant
Profil utilisateur
Chemin du profil :
\\FS1\Itinerants\a.martin
Script d'ouverture de session :
Dossier de base
Chemin d'accès local :
Connecter :
P:
à :
\\FS1\Profils\a.martin
OK
Annuler
Aide


Étape 4 — Vérification côté serveur
Après la connexion du premier utilisateur :
Sur FS1, regarde dans :
makefile
Copier le code
C:\PersonnelS
Tu verras un dossier test1.
Clique droit → Propriétés → Sécurité :
Propriétaire : test1
Autorisations :
test1 : Contrôle total
Administrateurs : Lecture seule
Parfait.
Étape 5 — Vérification côté client
Sur CLIENT1 :
1. Connecte-toi avec ton utilisateur (test1).
2. Ouvre Explorateur de fichiers → tu dois voir :
Lecteur P: pointant vers \\FS1\PersonnelS\test1
Bureau et données qui se chargent depuis \\FS1\Profils\test1
3. Crée un fichier sur le bureau → déconnecte-toi → reconnecte-toi → le fichier est toujours là
→ Le profil itinérant fonctionne.

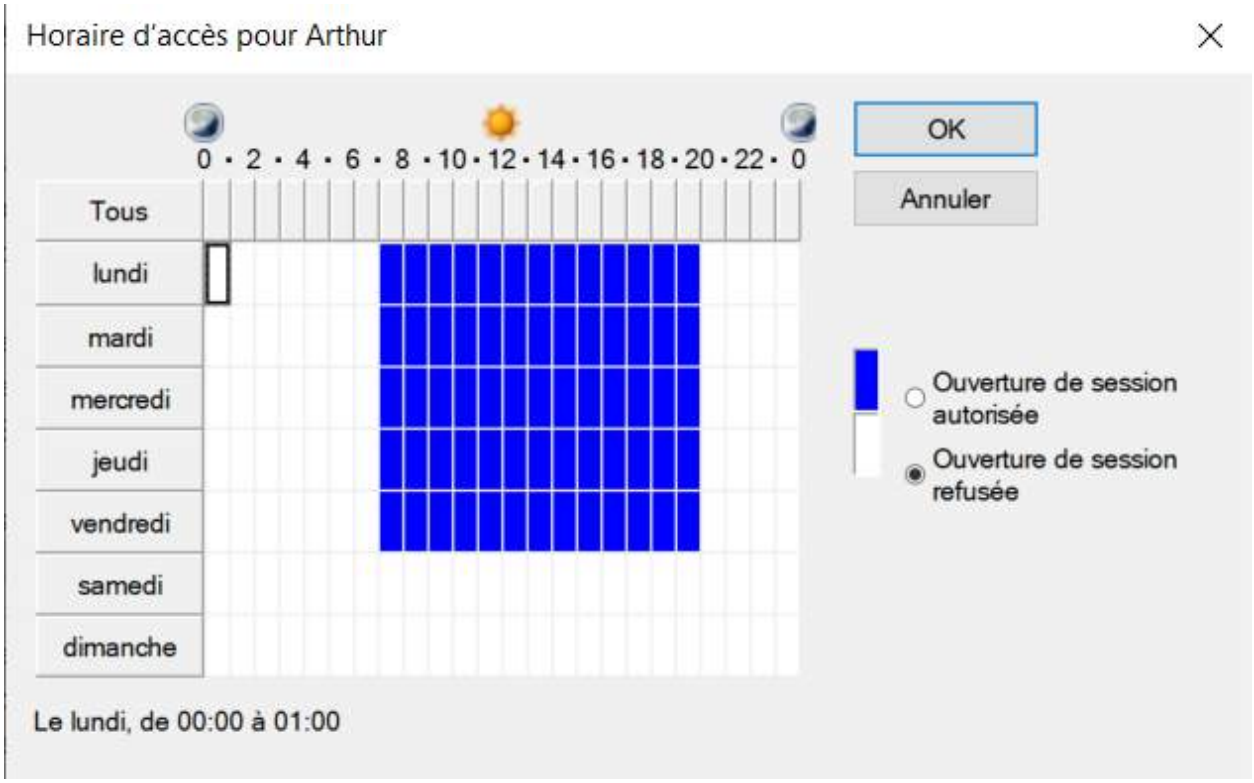

Étape 6 — (Optionnel) Appliquer un quota de 1 Go
Sur FS1 :
1. Clique sur Démarrer → Gestion du serveur → Outils → Gestion des ressources du serveur de fichiers (FSRM).
2. Va dans Gestion des quotas → Créer un quota.
3. Chemin du quota :
makefile
Copier le code
C:\Personnels
4. Sélectionne Créer automatiquement un quota pour chaque sous-dossier.
5. Sélectionne le modèle : Quota de 1 Go avec alerte à 90 % (ou crée ton propre modèle).
6. Appliquer → OK.
Chaque utilisateur aura 1 Go maximum dans son dossier P: avec une alerte quand il dépasse 900 Mo.
Résumé rapide
Elément
Chemin
Type
Objectif
Profils itinérants
\\FS1\Profils\%username%
Itinérant
Sauvegarde du profil utilisateur
Dossier personnel P:
\\fs1\Personnels\%username%
Partagé
Espace personnel
Quota
1 Go / 90 %
FSRM
Limite de stockage

Horaires de connexion

Élément	État	Détails / Actions
Responsables : 24/7	⚙	À faire via Active Directory (Propriétés utilisateur → Onglet "Compte").
Collaborateurs / élèves : horaires restreints	⚙	À faire pareil → on peut limiter les heures autorisées.

Procédure :

1. Sur DC1 → Outils → "Utilisateurs et ordinateurs Active Directory".
2. Clique droit sur un utilisateur → **Propriétés** → **Onglet "Compte"** → **Heures de connexion.**
3. Clique sur les cases :
   - Bleu = autorisé
   - Blanc = refusé
4. Exemples :
   - **Responsables** → tout bleu (7j/7, 24h/24).
   - **Collaborateurs** → Lundi–Vendredi, 7h00–20h00.
   - **Élèves** → Lundi–Vendredi, 9h00–16h30.
5. Clique sur **OK** → **Appliquer.**



Mise en place de la réplication DFS : FS1 (source) → DC2 (copie)

Principe

Le serveur **FS1** contient les dossiers partagés (`C:\Partages`)
et le serveur **DC2** va recevoir une **copie automatique** dans `C:\Partages_Backup` .

Grâce à DFS, tout ce que tu ajoutes/modifies/supprimes sur FS1 se synchronisera avec DC2.

Étape 1 — Préparer les dossiers sur DC2

1. Connecte-toi sur **DC2** avec ton compte `experty\Administrateur` .
2. Ouvre **l'explorateur de fichiers**.
3. Crée un dossier :

```
makefile                                                    Copier le code

C:\Partages_Backup
```

💡 Ce dossier sera la "copie miroir" du `C:\Partages` de FS1.

4. Pas besoin de le partager : DFS s'en charge.

Étape 2 — Sélectionner le rôle à installer

1. Dans la liste, développe :

```
nginx                                                       Copier le code

Services de fichiers et de stockage
  → Services de fichiers et iSCSI
```

2. Coche :
   - ✅ **Espaces de noms DFS**
   - ✅ **Réplication DFS**
3. Laisse les autres options par défaut.
4. Clique sur **Suivant** → **Installer**.

⚙ Étape 2 — Ouvrir la console "Gestion DFS"

1. Sur **FS1**, ouvre le **Gestionnaire de serveur**.
2. Clique en haut à droite sur **Outils → Gestion DFS**.
3. Dans le volet gauche, tu vois deux sections :
   - **Espaces de noms**
   - **Réplications**

⚙ Étape 3 — Créer un nouveau groupe de réplication

1. Clique droit sur **Réplications → Nouvelle réplication**.
2. Choisis **Réplication de dossiers → Suivant**.
3. Donne un nom :

```
nginx                                                    Copier le code

Partages_Redondance
```

4. Clique sur **Suivant**.

⚙ Étape 4 — Ajouter les serveurs membres

1. Clique sur **Ajouter**.
2. Entre le nom des serveurs :
   - **FS1**
   - **DC2**
3. Clique sur **Suivant**.

⚙ Étape 5 — Sélectionner le dossier à répliquer

1. Sélectionne **FS1** comme **serveur principal**.
2. Chemin du dossier à répliquer :

```
makefile                                                 Copier le code

C:\Partages
```

3. Clique sur **Suivant**.

⚙ Étape 6 — Choisir le dossier cible sur DC2

1. Sélectionne **DC2** → clique sur **Définir le dossier cible**.
2. Indique :

```
C:\Partages_Backup
```

3. Valide → clique sur **Suivant**.

⚙ Étape 7 — Type de topologie

1. Laisse le choix **Réplication complète en double sens (bidirectionnelle)**.

   💡 Cela veut dire que les fichiers seront synchronisés dans les deux sens (FS1 ↔ DC2).

   → Suivant.

⚙ Étape 8 — Planification et bande passante

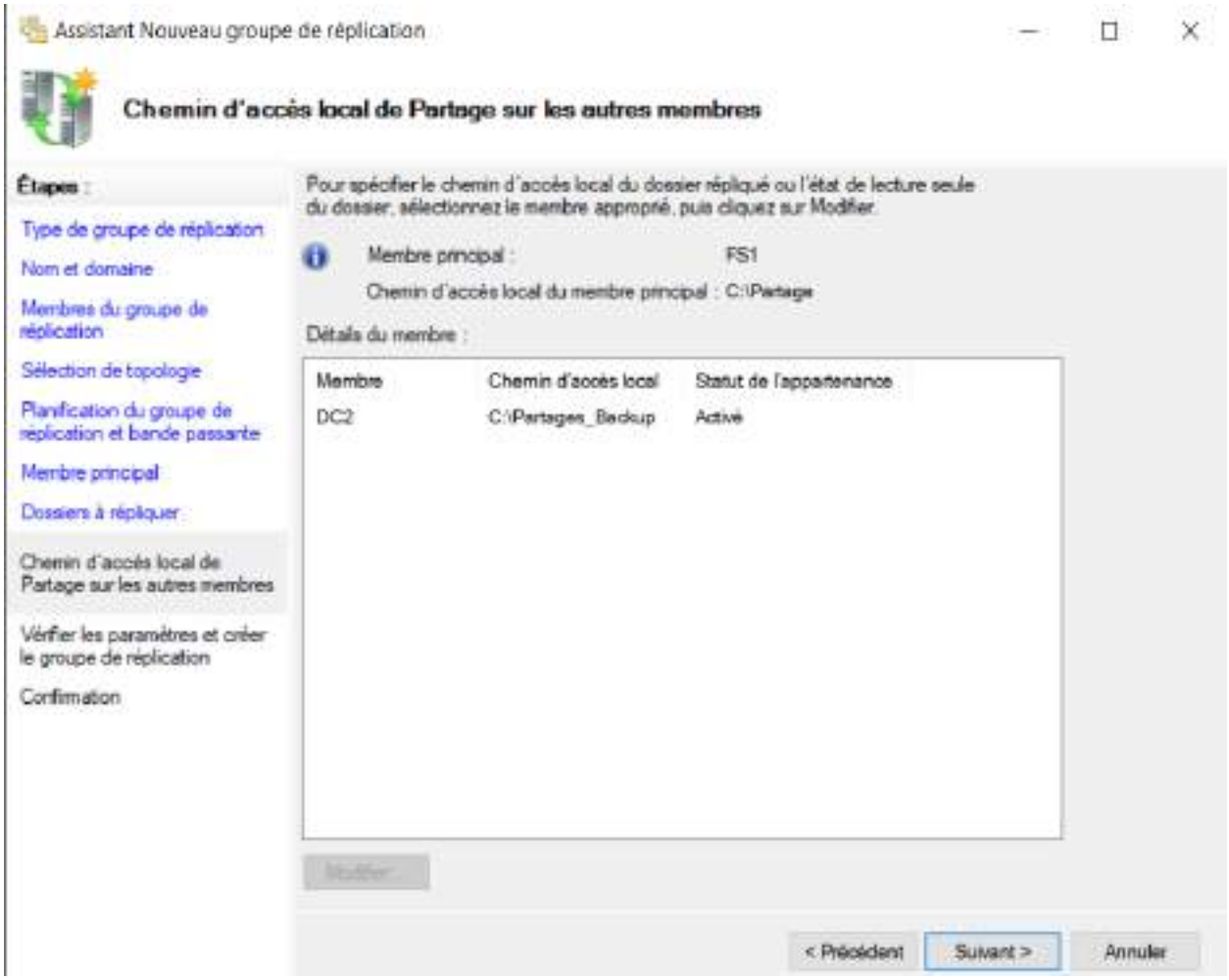
1. Laisse **Permanente (24 h/24)** et **Bande passante complète**.

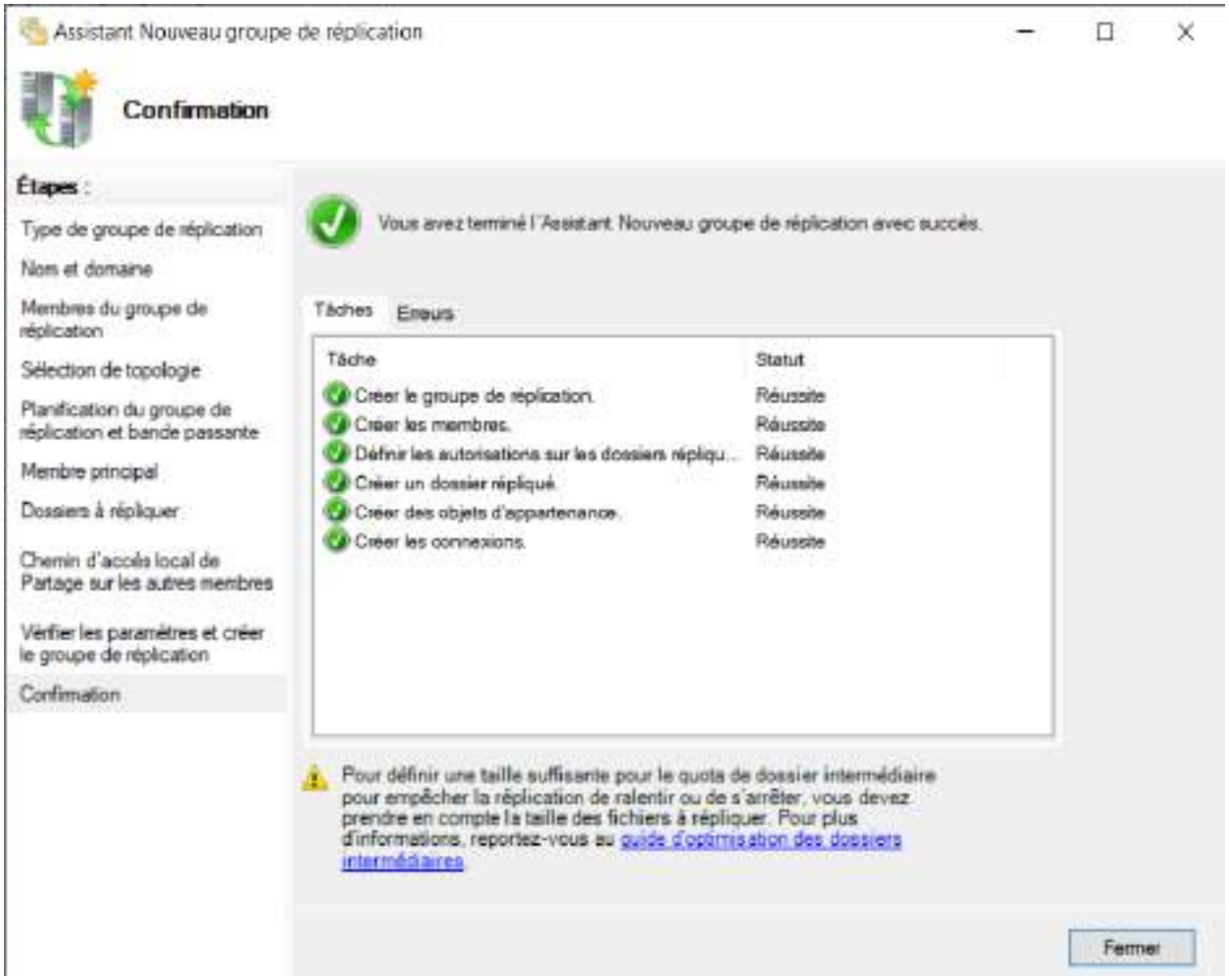
   → Suivant.

⚙ Étape 9 — Créer le groupe de réplication

1. Vérifie le récapitulatif.
2. Clique sur **Créer** → **Fermer**.

🕐 DFS mettra quelques minutes à initialiser le servi[illegible]e réplication sur les deux serveurs.


Assistant Nouveau groupe de réplication
Chemin d'accès local de Partage sur les autres membres
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Chemin d'accès local de Partage sur les autres membres
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Pour spécifier le chemin d'accès local du dossier répliqué ou l'état de lecture seule du dossier, sélectionnez le membre approprié, puis cliquez sur Modifier.
Membre principal : FS1
Chemin d'accès local du membre principal : C:\Partage
Détails du membre :
Membre
Chemin d'accès local
Statut de l'appartenance
DC2
C:\Partages_Backup
Activé
< Précédent
Suivant >
Annuler


Assistant Nouveau groupe de réplication
Confirmation
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Chemin d'accès local de Partage sur les autres membres
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Vous avez terminé l'Assistant Nouveau groupe de réplication avec succès.
Tâches
Erreurs
Tâche
Statut
Créer le groupe de réplication.
Réussite
Créer les membres.
Réussite
Définir les autorisations sur les dossiers répliqu...
Réussite
Créer un dossier répliqué.
Réussite
Créer des objets d'appartenance.
Réussite
Créer les connexions.
Réussite
Pour définir une taille suffisante pour le quota de dossier intermédiaire pour empêcher la réplication de ralentir ou de s'arrêter, vous devez prendre en compte la taille des fichiers à répliquer. Pour plus d'informations, reportez-vous au guide d'optimisation des dossiers intermédiaires
Fermer

⚙️ Étape 10 — Vérification

Sur FS1 :

1. Crée un dossier test :

```makefile
C:\Partages\Test_DFS
```

2. Attends 1 à 3 minutes (selon ta VM).

Sur DC2 :

1. Ouvre :

```makefile
C:\Partages_Backup
```

2. Tu dois voir apparaître le dossier `Test_DFS`. ✅

Si oui → ta réplication DFS est **fonctionnelle** 🎉

⚙️ Étape 11 — Vérification dans la console DFS

1. Dans la console "Gestion DFS", développe **Réplications → Partages_Redondance**.
2. Tu verras :
   - **FS1**
   - **DC2**
   - L'état de la synchronisation : "OK" ou "Initialisation".

↓

💾 Étape 12 — (Optionnel mais conseillé)

Dans ton **espace de noms DFS** (`\\experty.local\partage`),
tu peux ajouter **DC2 comme cible secondaire** :

1. Clique droit sur ton dossier DFS (ex. `Comptabilite`) → **Ajouter une cible**.
2. Indique le chemin :

```
\\DC2\Partages_Backup\Comptabilite
```

3. Ainsi, si FS1 tombe, les utilisateurs peuvent toujours accéder à leurs fichiers via DC2.
