BTS SIO – Option SISR
Media School Strasbourg

Déploiement d'une infrastructure Active Directory

Sous Windows Server 2022

Projet professionnel – Mise en situation d'entreprise (EXPERT-IT)

Réalisé par : Amir Tajik-Heulin
Professeur référent : Boris Malik
Année scolaire : 2025 – 2026

Table des matières

INTRODUCTION

Dans le cadre du BTS SIO option SISR, ce projet a pour objectif la mise en place d'une infrastructure informatique de type entreprise basée sur Windows Server 2022.

Inspiré d'un contexte professionnel réel (projet EXPERT-IT), ce travail consiste à concevoir, installer et configurer un environnement Active Directory permettant la centralisation des utilisateurs, la gestion des ressources réseau ainsi que l'application de politiques de sécurité adaptées.

L'infrastructure repose sur plusieurs machines virtuelles afin de simuler un environnement d'entreprise. Les services déployés incluent notamment Active Directory, DNS, DHCP, les stratégies de groupe (GPO), les partages réseau ainsi qu'un système de sauvegarde.

Ce document présente les différentes étapes de conception et de réalisation du projet, ainsi que les choix techniques retenus.

ANALYSE DES BESOINS

L'entreprise fictive étudiée dans le cadre de ce projet nécessite la mise en place d'une infrastructure informatique centralisée, sécurisée et facilement administrable.

Les principaux besoins identifiés sont les suivants :

• Centraliser l'authentification des utilisateurs au sein d'un domaine
• Gérer les comptes utilisateurs et ordinateurs de manière structurée
• Assurer une gestion centralisée des droits d'accès aux ressources réseau
• Mettre en place des règles de sécurité via des stratégies de groupe (GPO)
• Fournir automatiquement des adresses IP aux postes clients (DHCP)
• Garantir la disponibilité des services critiques
• Mettre en œuvre une solution de sauvegarde des données

Afin de répondre à ces exigences, une infrastructure basée sur Active Directory et les services Windows Server a été retenue.

ARCHITECTURE TECHNIQUE

L'infrastructure repose sur une architecture client/serveur virtualisée, composée de deux serveurs sous Windows Server 2022 et d'un poste client Windows.

Deux contrôleurs de domaine sont déployés afin d'assurer la redondance, la réplication Active Directory et la continuité de service en cas de défaillance de l'un des serveurs.

Machine	Système	Adresse IP	Rôle
DC1	Windows Server 2022	192.168.10.10	AD DS, DNS, DHCP
DC2	Windows Server 2022	192.168.10.11	Contrôleur de domaine secondaire
Client01	Windows 10/11	DHCP	Poste utilisateur

INSTALLATION ET CONFIGURATION DU CONTRÔLEUR DE DOMAINE (DC1)

1. Installation de Windows Server 2022

La première étape du projet a consisté à installer le système d'exploitation Windows Server 2022 sur une machine virtuelle destinée à devenir le contrôleur de domaine principal (DC1).

La machine virtuelle a été créée à l'aide de l'hyperviseur **(VMware)** avec les caractéristiques suivantes :

- 2 processeurs virtuels
- 4 Go de mémoire vive
- 60 Go d'espace disque

L'installation a été réalisée à partir de l'image ISO officielle de Windows Server 2022, en sélectionnant l'édition **Standard avec interface graphique (Desktop Experience)** afin de faciliter l'administration du serveur.

Après la copie des fichiers et le redémarrage du système, la configuration initiale a été effectuée (choix de la langue, définition du mot de passe administrateur et vérification du bon fonctionnement du serveur).

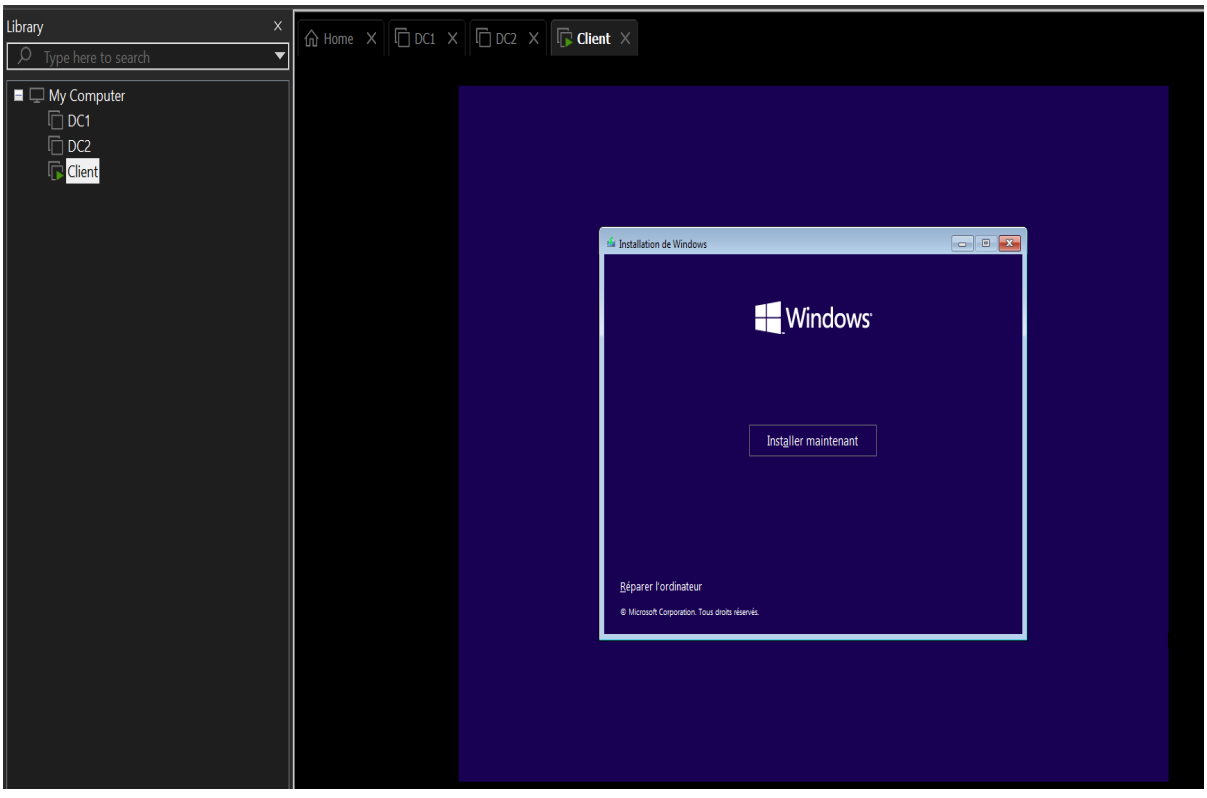


Figure 1 : Installation de Windows Server 2022 sur le serveur DC1

2. Configuration de l’adressage IP statique

Une adresse IP statique a été configurée sur le serveur DC1 afin de garantir la stabilité et la disponibilité des services réseau, notamment Active Directory et DNS.

Les paramètres réseau définis sont les suivants :

- **Adresse IP :** 192.168.10.10
- **Masque de sous-réseau :** 255.255.255.0
- **Passerelle par défaut :** 192.168.10.1
- **Serveur DNS préféré :** 127.0.0.1 (résolution locale du contrôleur de domaine)

L’utilisation d’une adresse IP fixe est indispensable pour un contrôleur de domaine, car elle permet d’assurer une résolution de noms fiable et un fonctionnement correct des services d’annuaire.

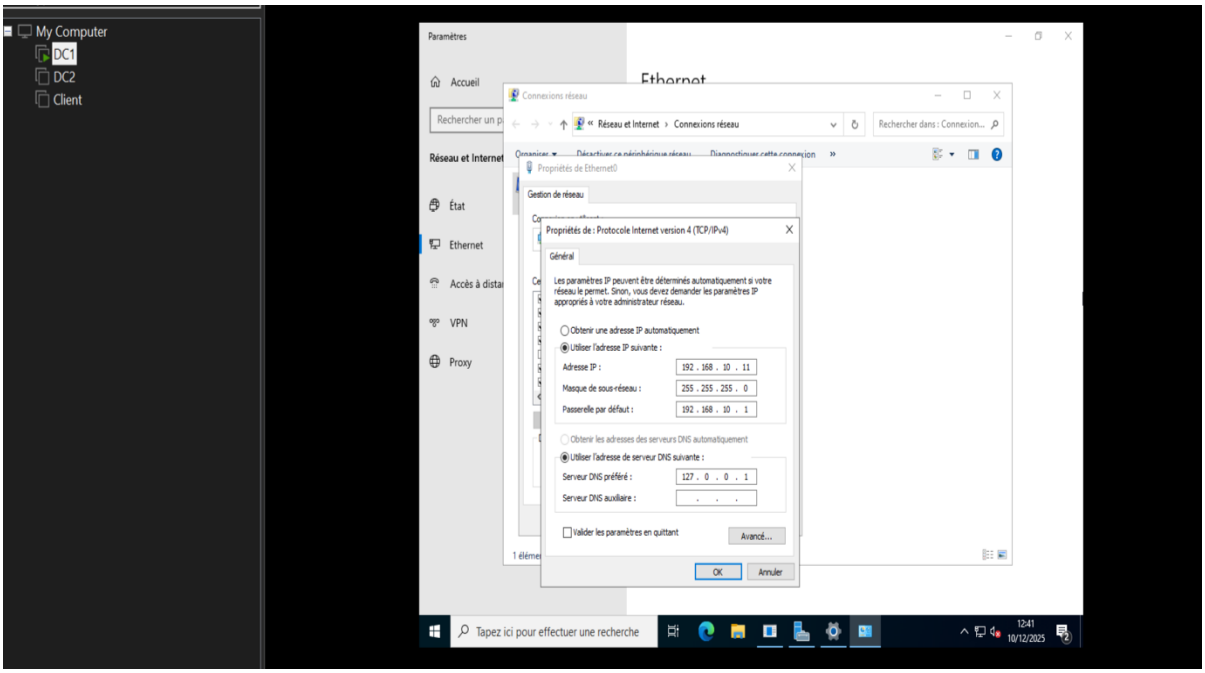


Figure 2 : Configuration de l’adresse IP statique sur le serveur DC1.

3. Installation des rôles Active Directory et DNS

Une fois le système installé et l'adressage IP configuré, les rôles **Active Directory Domain Services (AD DS)** et **DNS** ont été ajoutés sur le serveur DC1 à l'aide de l'assistant *Add Roles and Features* du gestionnaire de serveur.

Ces services sont indispensables pour permettre l'authentification centralisée des utilisateurs, la gestion des ressources du domaine ainsi que la résolution de noms au sein de l'infrastructure réseau.

Après l'installation des rôles, le serveur a été promu en **contrôleur de domaine** par la création d'une **nouvelle forêt Active Directory**. Un nom de domaine interne a été défini, et les chemins par défaut des dossiers **NTDS** et **SYSVOL** ont été conservés.

Un mot de passe de restauration des services d'annuaire (DSRM) a également été configuré, puis le serveur a été redémarré afin de finaliser la mise en place du contrôleur de domaine.

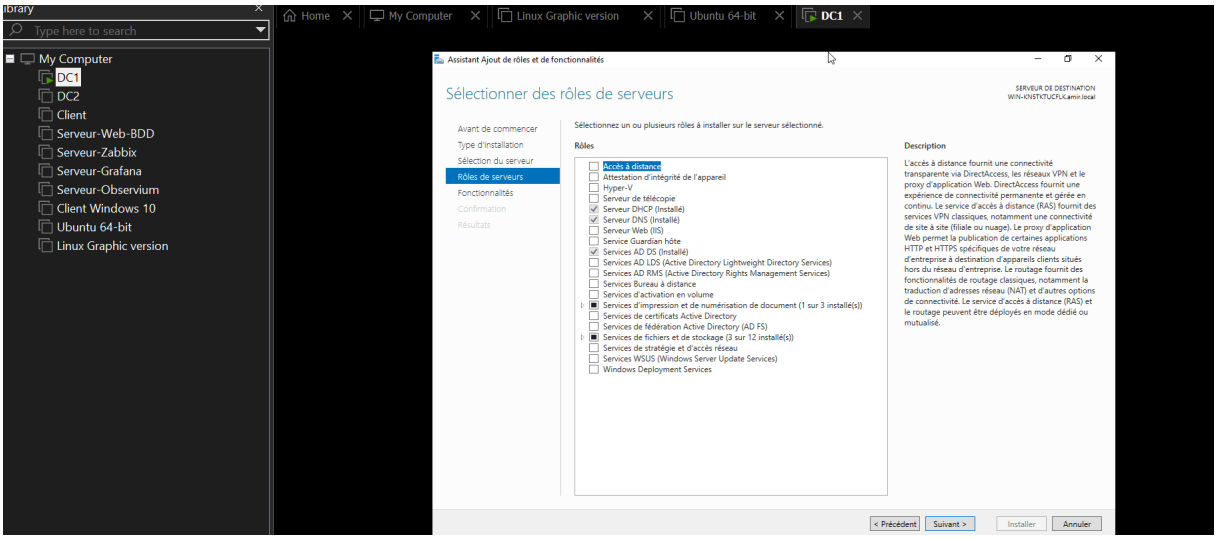


Figure 3 : Installation des rôles Active Directory Domain Services (AD DS) et DNS via le gestionnaire de serveur.

4. Création du domaine Active Directory

Le serveur DC1 a ensuite été promu en **contrôleur de domaine principal** par la création d'une **nouvelle forêt Active Directory**.

Un domaine interne nommé **expertv.local** a été défini. Le service DNS a été configuré automatiquement et intégré à Active Directory afin d'assurer la résolution de noms au sein du réseau.

Les niveaux fonctionnels par défaut ont été conservés, et un mot de passe de restauration des services d'annuaire (DSRM) a été spécifié lors de la procédure de promotion.

Après le redémarrage du serveur, le bon fonctionnement du domaine a été vérifié à l'aide de la console **Active Directory Users and Computers**, confirmant que le serveur DC1 est opérationnel en tant que contrôleur de domaine.

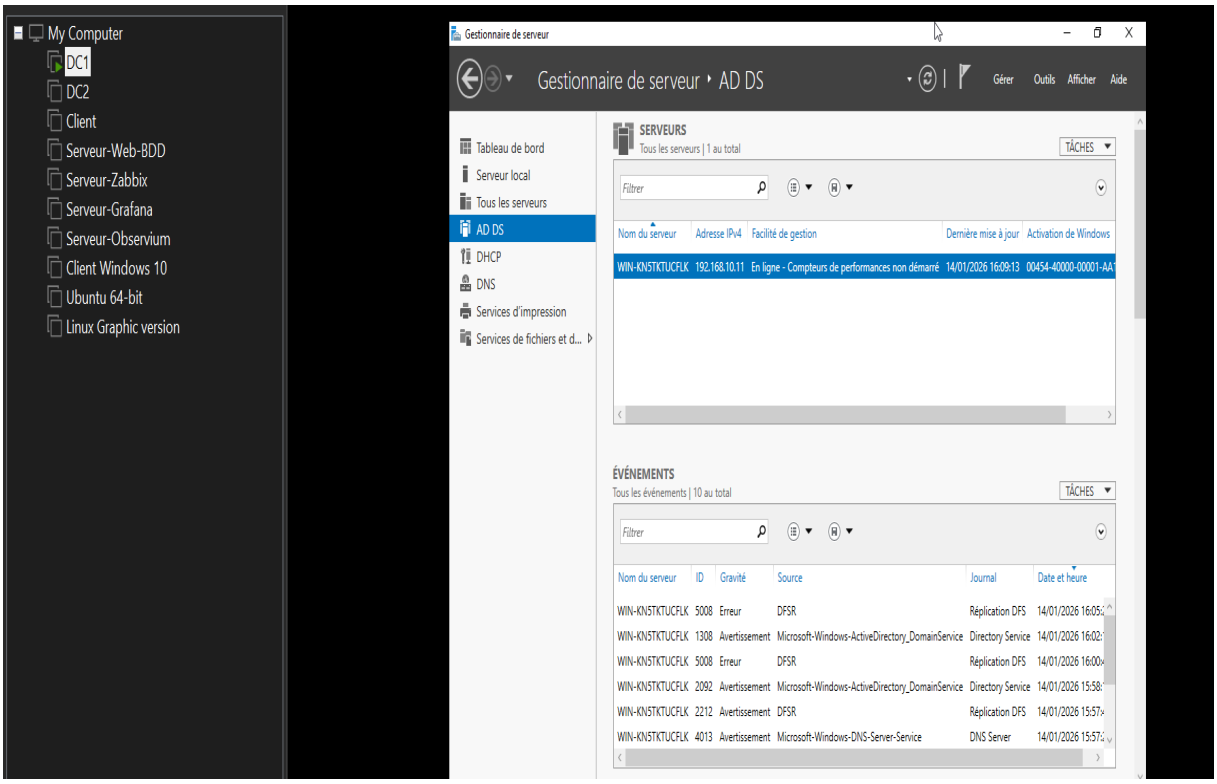


Figure 4 : Vérification de la création du domaine Active Directory et de la promotion du serveur DC1.

5. Création de la structure Active Directory

Après la création du domaine, une structure logique a été mise en place à l'aide d'**unités d'organisation (OU)** afin d'organiser les utilisateurs et les ordinateurs de manière hiérarchique.

Plusieurs OU ont été créées, notamment pour les services de l'entreprise (par exemple : **Direction**, **Informatique**, **Utilisateurs**, **Ordinateurs**). Cette organisation permet de faciliter l'administration du domaine et l'application ciblée des **stratégies de groupe (GPO)** selon les besoins de chaque service.

La mise en place de cette arborescence constitue une étape essentielle pour assurer une gestion centralisée, sécurisée et évolutive de l'infrastructure Active Directory.

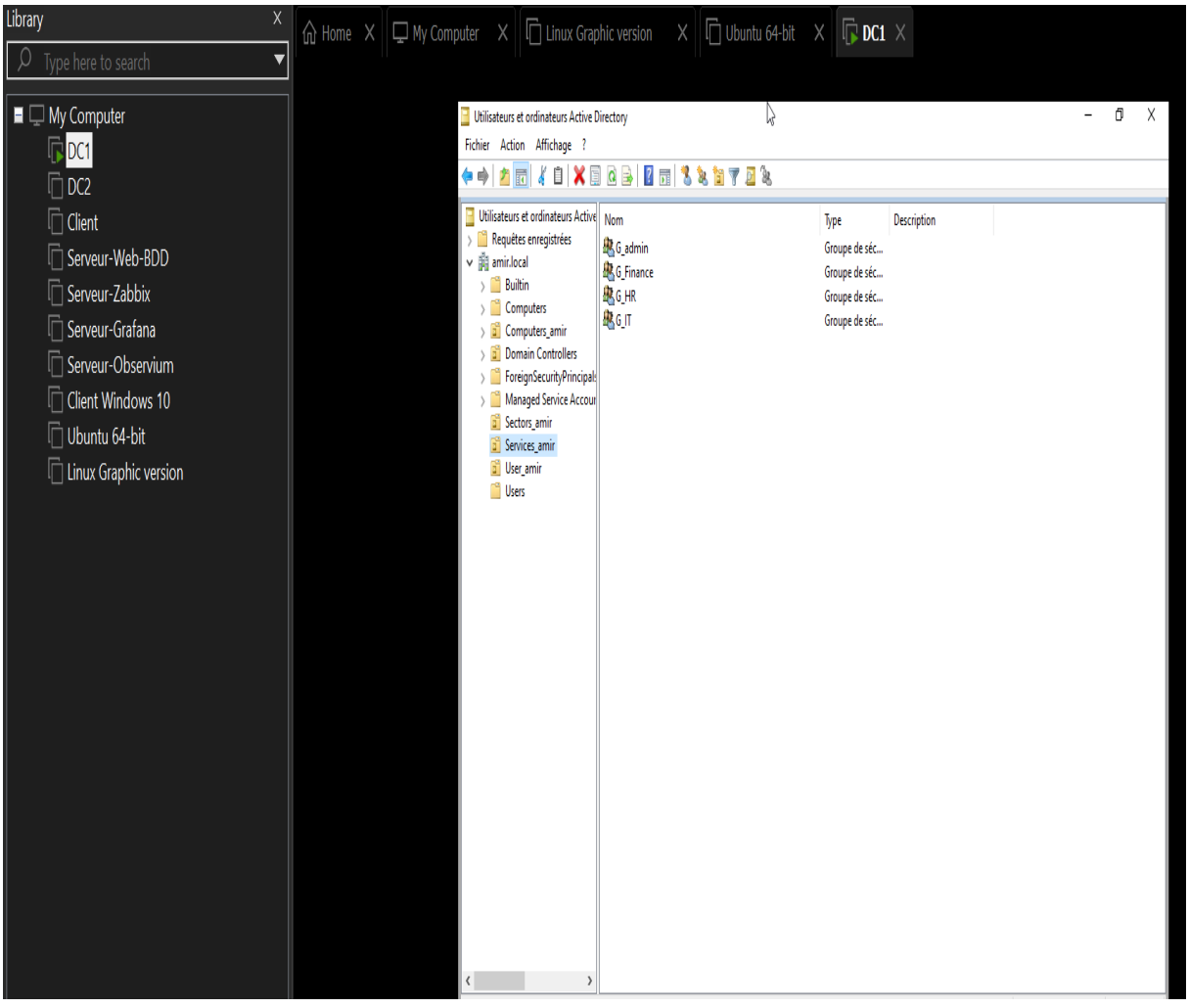


Figure 5 : Arborescence des unités d'organisation dans Active Directory.

AJOUT ET PROMOTION DU SECOND CONTRÔLEUR DE DOMAINE (DC2)

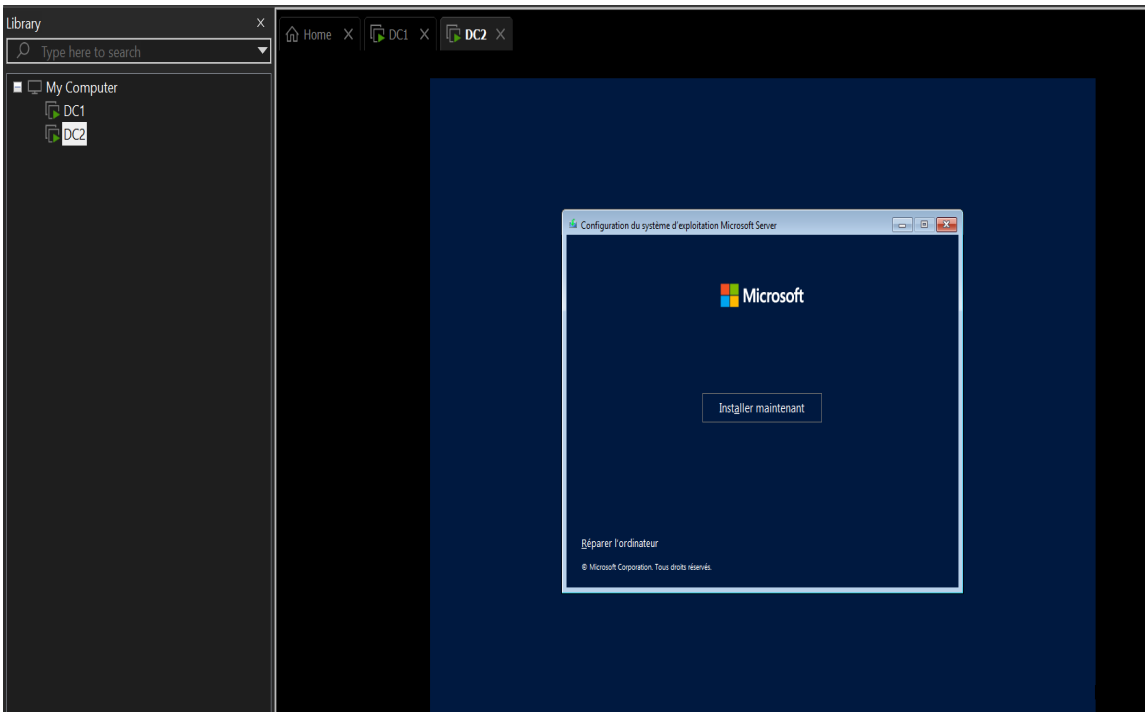
1. Installation et préparation du serveur DC2

Un second serveur sous **Windows Server 2022** a été déployé afin d'assurer la **redondance** des services Active Directory et DNS en complément du contrôleur de domaine principal.

Le système a été installé sur une machine virtuelle, puis une **adresse IP statique** a été configurée afin de garantir la stabilité des services réseau.

Le serveur DC2 a ensuite été **joint au domaine Active Directory existant** avant l'installation du rôle **Active Directory Domain Services (AD DS)**, préalable nécessaire à sa promotion en contrôleur de domaine supplémentaire.

Cette architecture permet d'assurer la **réplication des données Active Directory**, la tolérance aux pannes et la continuité de service en cas d'indisponibilité du serveur DC1.



2. Jonction de DC2 au domaine existant

Avant de pouvoir être promu en contrôleur de domaine, le serveur **DC2** a été joint au domaine Active Directory existant **expertv.local**. Cette étape permet au serveur d'intégrer l'infrastructure en place et de communiquer avec le contrôleur de domaine principal.

La jonction au domaine a été réalisée à l'aide des **identifiants administrateur du domaine**, puis le serveur a été redémarré afin de valider son intégration.

Des tests de connectivité ont ensuite été effectués (commande **ping** et résolution DNS) pour vérifier la communication correcte entre **DC1** et **DC2**, condition indispensable avant la promotion en contrôleur de domaine supplémentaire.

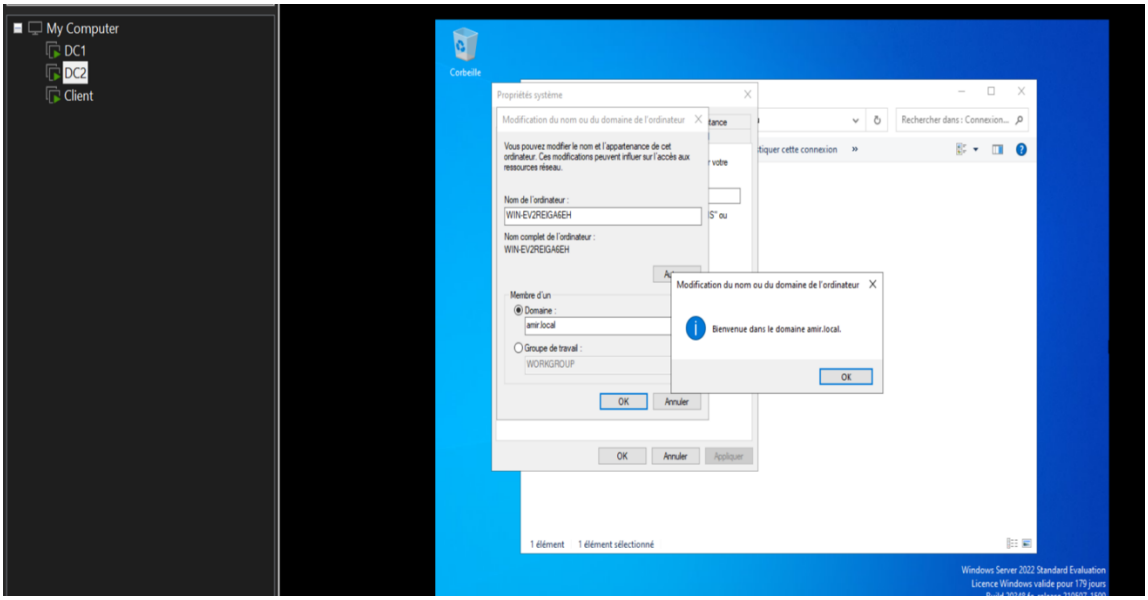


Figure : Jonction du serveur DC2 au domaine Active Directory existant.

3. Promotion de DC2 en contrôleur de domaine secondaire

Une fois joint au domaine, le serveur **DC2** a été promu en **contrôleur de domaine supplémentaire** par l'installation du rôle **Active Directory Domain Services (AD DS)**.

Lors de cette promotion, DC2 a été intégré dans la **forêt Active Directory existante** et configuré comme **Global Catalog**, permettant d'assurer la disponibilité des services d'authentification même en cas d'indisponibilité de DC1.

La **réplication automatique** des données Active Directory a été mise en place entre **DC1** et **DC2**. Des vérifications ont été réalisées à l'aide des outils d'administration (console *Active Directory Sites and Services* et commande **repadmin /replsummary**) afin de confirmer le bon fonctionnement de la synchronisation.

Cette architecture redondante garantit la **tolérance de panne**, la continuité de service et une meilleure résilience de l'infrastructure réseau.

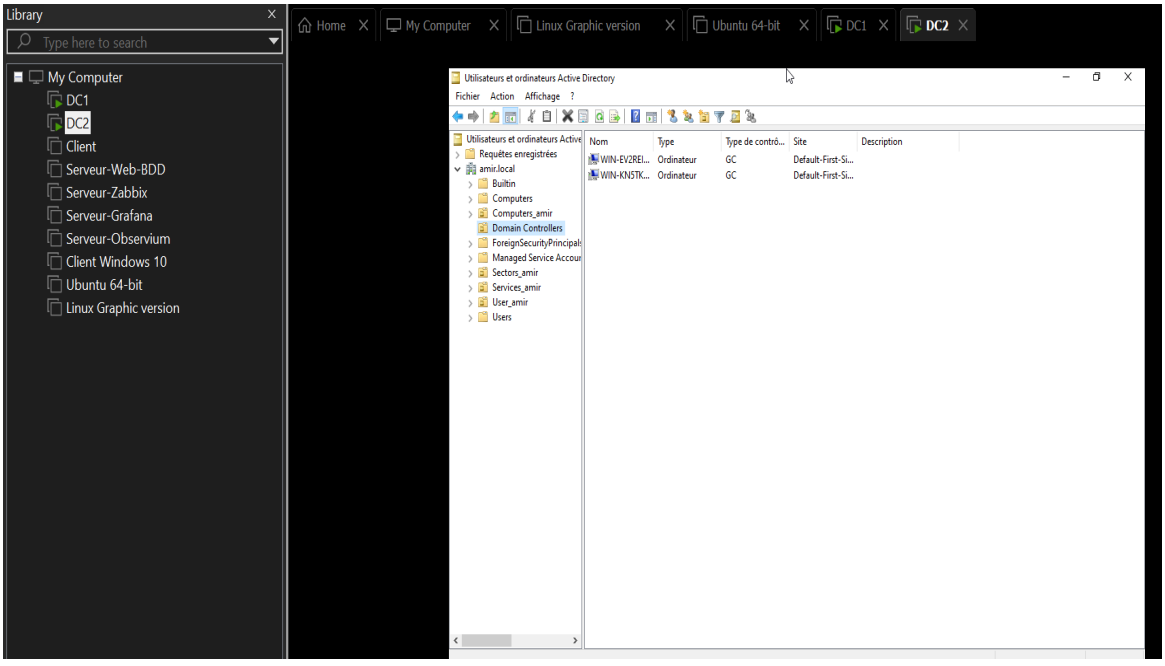


Figure : Présence des contrôleurs de domaine DC1 et DC2 dans l'unité d'organisation « Domain Controllers » du domaine.

4. Vérification de la réplication Active Directory

Après la promotion de DC2, la réplication des objets Active Directory a été vérifiée afin de s'assurer que les utilisateurs, groupes et unités d'organisation sont correctement synchronisés entre les deux contrôleurs de domaine.

Des contrôles ont été réalisés à l'aide des outils d'administration, notamment la console **Active Directory Sites and Services** ainsi que la commande **repadmin /replsummary**, permettant de confirmer l'absence d'erreurs de synchronisation.

La présence des contrôleurs de domaine **DC1** et **DC2** dans l'unité d'organisation **« Domain Controllers »** confirme le bon fonctionnement de la réplication Active Directory.

Cette réplication garantit la **continuité de service**, la **tolérance de panne** et la disponibilité de l'authentification même en cas d'indisponibilité de l'un des serveurs.

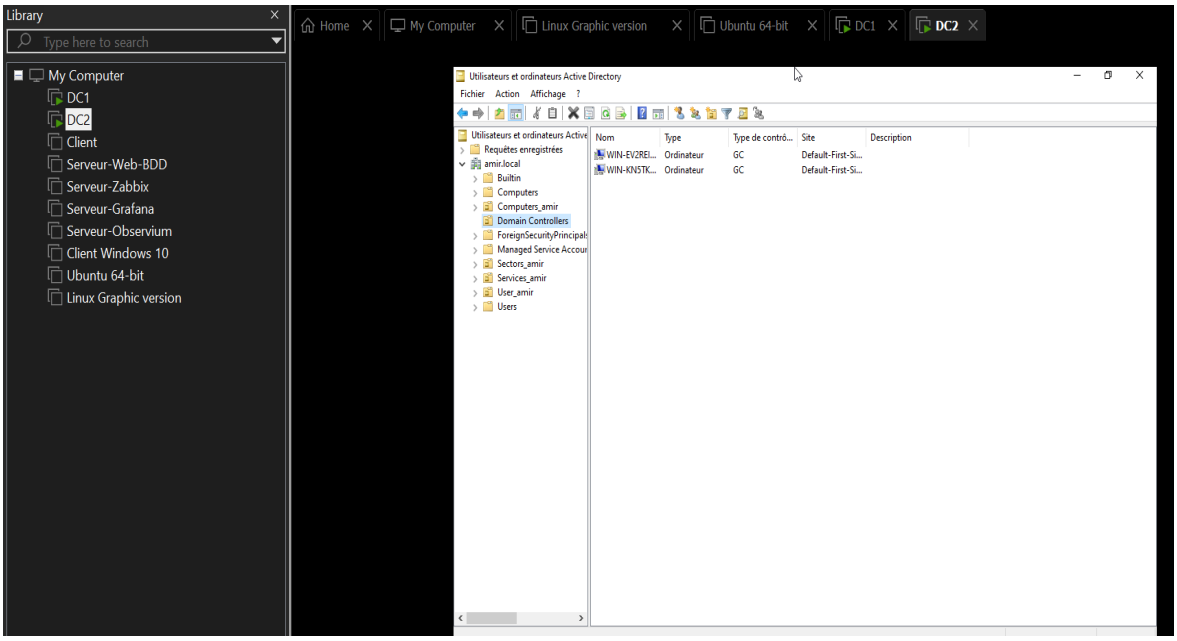


Figure : Vérification de la réplication Active Directory entre DC1 et DC2.

5. Justification du choix de deux contrôleurs de domaine

Le déploiement de deux contrôleurs de domaine permet d'assurer la **haute disponibilité** des services d'authentification et de résolution de noms.
En cas de panne du contrôleur de domaine principal, le second serveur peut continuer à fournir les services essentiels sans interruption pour les utilisateurs, garantissant ainsi la **continuité de service**.

MISE EN PLACE DU SERVICE DHCP

1. Installation du rôle DHCP

Afin d'automatiser l'attribution des adresses IP aux postes clients, le rôle **DHCP (Dynamic Host Configuration Protocol)** a été installé sur le serveur **DC1**.
Ce service permet de simplifier l'administration réseau en évitant la configuration manuelle des paramètres IP sur chaque poste client.

Après l'installation, une **plage d'adresses IP (scope)** a été créée en définissant :

- une plage d'adresses disponible pour les clients
- le **masque de sous-réseau**
- la **passerelle par défaut**
- le **serveur DNS du domaine**
- la **durée du bail DHCP**

Un test de connexion depuis un poste client a permis de vérifier l'obtention automatique d'une adresse IP valide et l'accès correct au domaine.

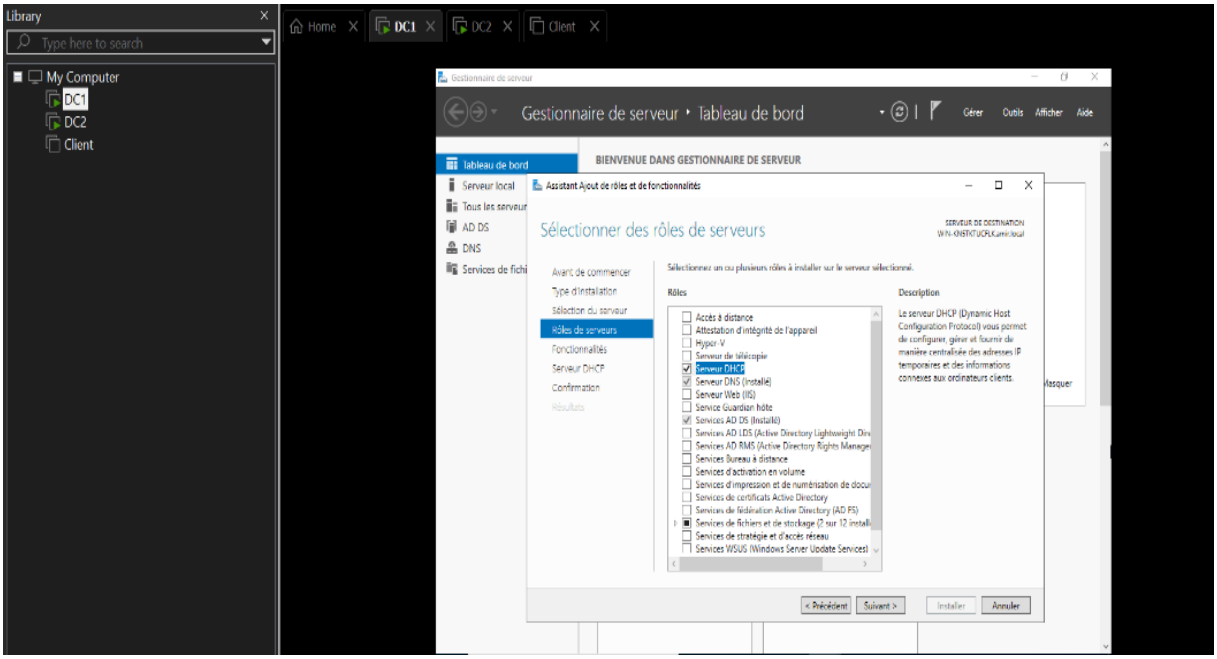


Figure : Installation du rôle DHCP dans le gestionnaire de serveur

2. Configuration de l'étendue DHCP

Une étendue DHCP a été créée pour le réseau interne de l'entreprise afin de définir la plage d'adresses IP attribuées automatiquement aux postes clients.

La plage configurée s'étend de **192.168.10.50** à **192.168.10.200**, en excluant les adresses réservées aux serveurs de l'infrastructure.

Le **masque de sous-réseau**, la **passerelle par défaut**, le **serveur DNS du domaine** ainsi que la **durée du bail DHCP** ont été définis afin d'assurer une configuration réseau cohérente pour l'ensemble des clients.

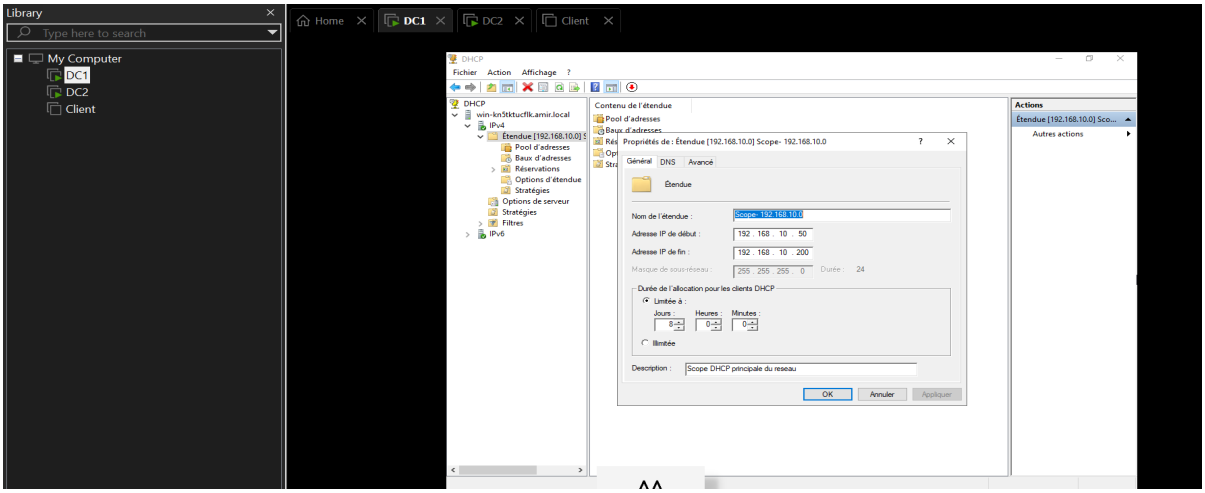


Figure : Configuration de l'étendue DHCP.

---

3. Configuration des options DHCP

Les options DHCP ont été configurées afin de fournir automatiquement aux postes clients les paramètres nécessaires à leur fonctionnement au sein du domaine Active Directory.

Le serveur DNS distribué correspond à l'adresse IP du contrôleur de domaine, permettant ainsi la **résolution des noms** et l'accès aux ressources du domaine.

Un test réalisé depuis un poste client à l'aide des commandes **ipconfig /renew** et **ipconfig /all** a permis de vérifier l'obtention correcte d'une adresse IP ainsi que la connectivité au domaine.

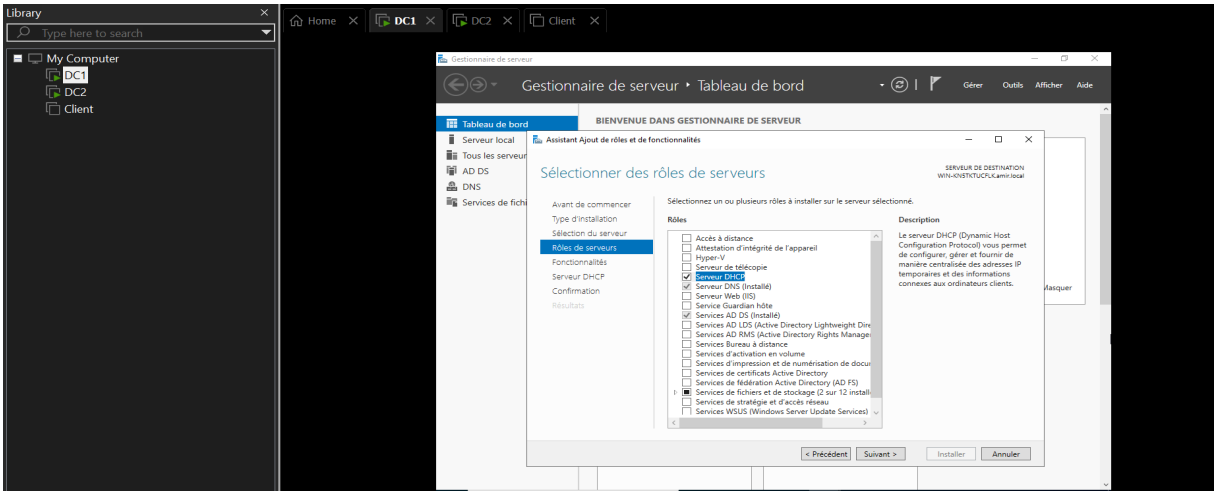


Figure : Configuration des options DHCP et test d'attribution d'adresse IP.

4. Vérification de l’attribution d’une adresse IP au client

Un poste client a été démarré sur le réseau afin de vérifier le bon fonctionnement du service DHCP.

L’obtention automatique d’une adresse IP appartenant à la plage configurée confirme le déploiement correct du service ainsi que la communication fonctionnelle avec l’infrastructure Active Directory.

Les commandes **ipconfig /renew** et **ipconfig /all** ont permis de vérifier la configuration réseau du poste client, notamment l’adresse IP attribuée, la passerelle par défaut et le serveur DNS du domaine.

Ces résultats valident l’intégration correcte du poste client au réseau de l’entreprise.

STRATÉGIES DE GROUPE (GPO) ET SÉCURITÉ

1. Mise en place des stratégies de groupe

Les stratégies de groupe (**Group Policy Objects – GPO**) ont été mises en place afin de centraliser la configuration et la sécurisation des postes et des utilisateurs du domaine **Active Directory**.
Les GPO permettent d'appliquer automatiquement des règles communes sans intervention manuelle sur chaque poste client.

2. GPO de sécurité

Des stratégies de sécurité ont été configurées afin de renforcer la protection des comptes utilisateurs et de limiter les risques liés aux mauvaises pratiques.

Les principales règles mises en place sont :

- Longueur minimale du mot de passe
- Historique des mots de passe
- Verrouillage du compte après plusieurs tentatives échouées
- Restriction de certaines fonctionnalités système

Ces paramètres contribuent à améliorer la **sécurité globale du domaine** et à protéger l'infrastructure contre les accès non autorisés.

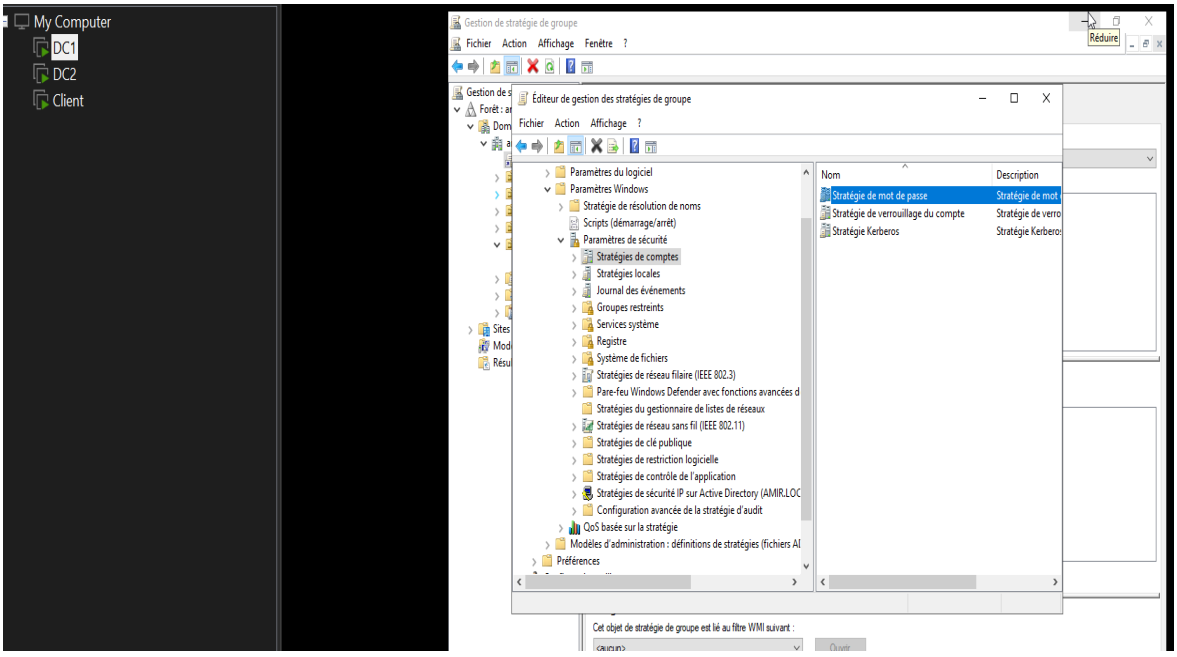


Figure : Paramètres de sécurité configurés via une GPO (mot de passe et verrouillage de compte).

3. GPO appliquées aux utilisateurs

Des **stratégies de groupe spécifiques aux utilisateurs** ont été mises en place afin de standardiser l'environnement de travail et de limiter certaines actions non autorisées.

Ces stratégies permettent notamment de **contrôler l'interface utilisateur**, de restreindre l'accès à certains paramètres système et d'assurer une configuration homogène sur l'ensemble des postes du domaine.

La mise en œuvre de ces GPO contribue à renforcer la **sécurité**, la **stabilité** et la **cohérence** de l'environnement informatique de l'entreprise.

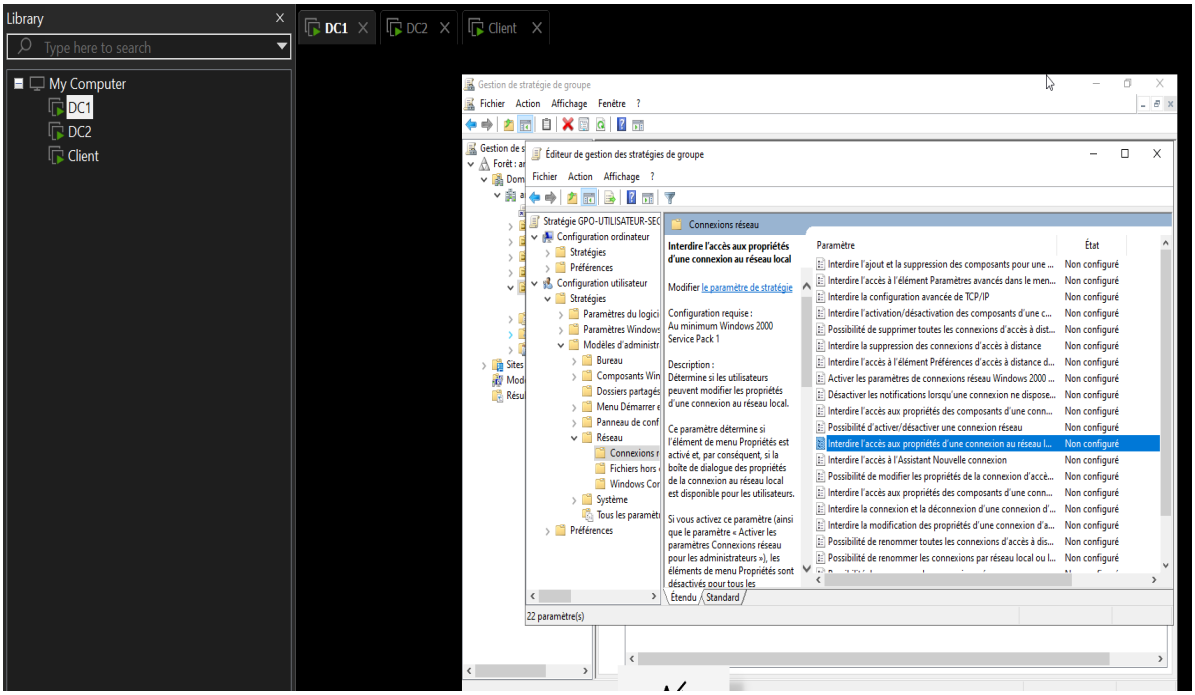


Figure : Exemple de GPO utilisateur appliquant des restrictions et des paramètres d'environnement.

4. Mappage des lecteurs réseau via GPO

Le mappage des lecteurs réseau a été configuré à l'aide des **stratégies de groupe (GPO)** afin de fournir automatiquement aux utilisateurs l'accès aux ressources partagées de l'entreprise.

Les lecteurs sont attribués en fonction des **droits des utilisateurs** et des **groupes Active Directory**, permettant de garantir un accès sécurisé et adapté aux besoins de chaque service. Par exemple, un lecteur réseau pointant vers le partage **\DC1\Partage** est monté automatiquement sous la lettre **Z:** lors de l'ouverture de session utilisateur.

Cette configuration simplifie l'accès aux données, améliore l'expérience utilisateur et assure une gestion centralisée conforme aux bonnes pratiques d'administration système.

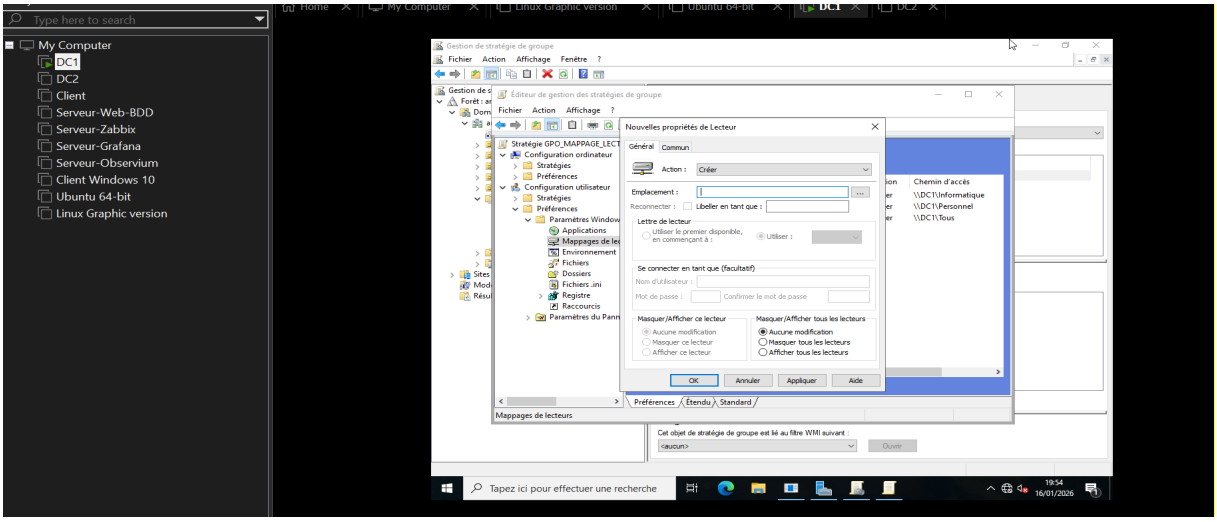


Figure : Mappage automatique d'un lecteur réseau via une stratégie de groupe.

5. Justification de l’utilisation des GPO

L’utilisation des **stratégies de groupe (GPO)** permet une administration centralisée du système d’information, réduit les erreurs de configuration et améliore le niveau global de sécurité.
Les GPO constituent ainsi un élément essentiel dans une infrastructure **Active Directory professionnelle**.

---

1. Mise en place des partages réseau

Afin de centraliser le stockage des données et de faciliter le travail collaboratif, des **partages réseau** ont été créés sur le serveur.

Ces partages permettent aux utilisateurs d’accéder aux ressources communes tout en respectant les règles de sécurité définies par l’entreprise, notamment grâce à l’utilisation des **droits NTFS**, des **autorisations de partage** et de l’appartenance aux **groupes Active Directory**.

Par exemple, un dossier partagé accessible via le chemin **\DC1\Commun** est attribué automatiquement aux utilisateurs autorisés grâce au **mappage des lecteurs réseau par GPO**.

Cette organisation garantit une gestion sécurisée, centralisée et cohérente des données de l’entreprise.

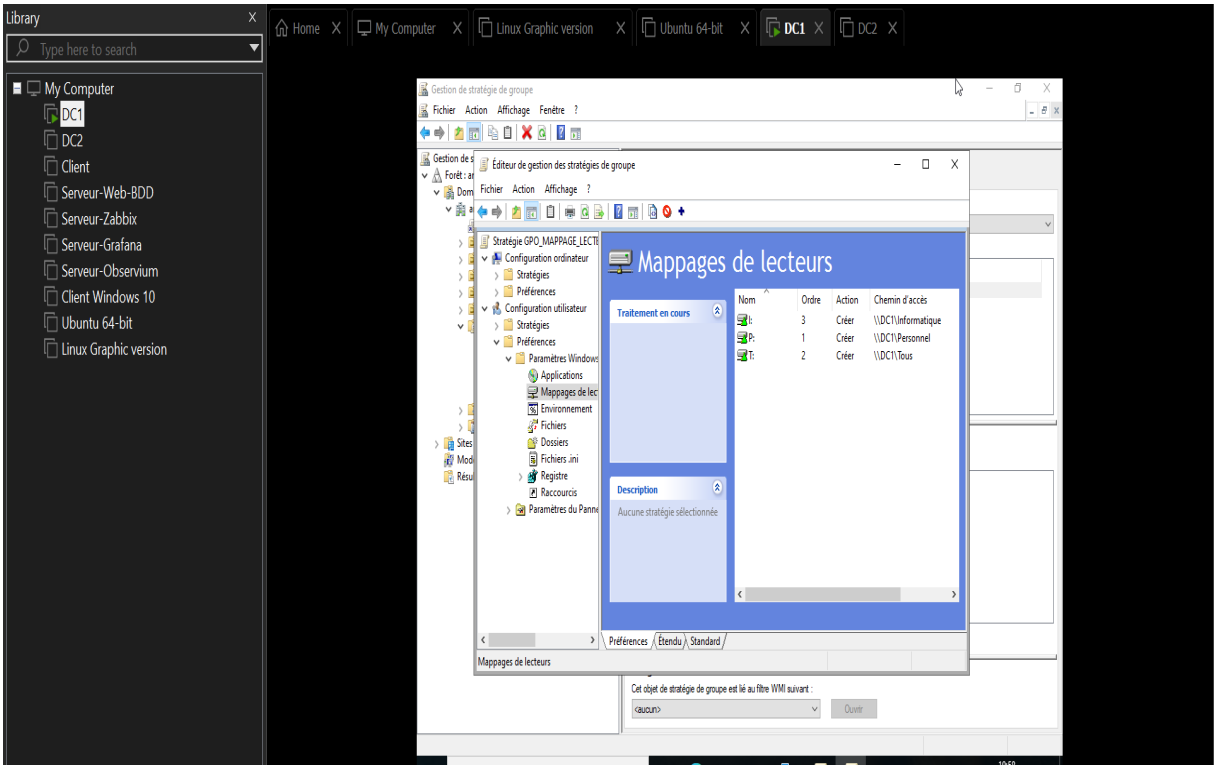


Figure : Dossiers partagés configurés sur le serveur Active Directory.

2. Gestion des droits d’accès (permissions NTFS)

Les **permissions NTFS** ont été configurées afin de contrôler précisément l’accès aux dossiers partagés du serveur.

Les droits ont été attribués en fonction des **groupes d’utilisateurs Active Directory**, permettant d’assurer une séparation claire des accès et une meilleure sécurité des données. Par exemple, un groupe d’utilisateurs standard dispose d’un droit de **lecture**, tandis que les administrateurs bénéficient d’un **contrôle total** sur les ressources concernées.

Cette organisation respecte le principe de **moindre privilège**, garantissant que chaque utilisateur ne possède que les droits strictement nécessaires à ses fonctions.

La combinaison des **permissions NTFS** et des **autorisations de partage** permet ainsi de mettre en place une gestion sécurisée, cohérente et conforme aux bonnes pratiques d’administration système.

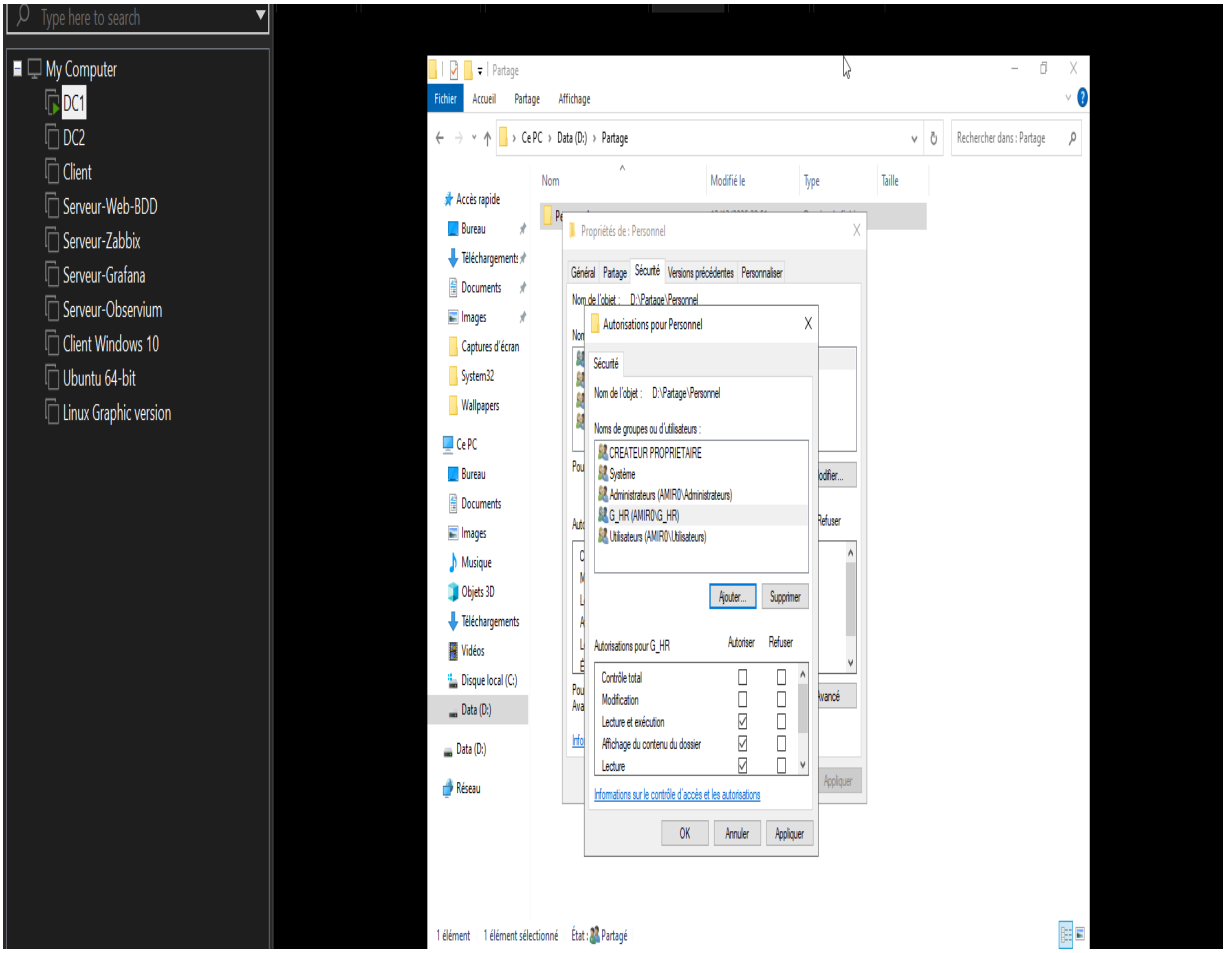


Figure : Permissions NTFS appliquées à un dossier partagé sur le serveur.

3. Mappage des lecteurs réseau sur les postes clients

Les lecteurs réseau ont été mappés automatiquement sur les postes clients via les **stratégies de groupe (GPO)** lors de l'ouverture de session des utilisateurs.

Cette méthode permet de fournir aux utilisateurs un accès direct, sécurisé et simplifié aux ressources partagées de l'entreprise, sans aucune intervention manuelle.
Les lecteurs affichés sur le poste client correspondent aux droits définis dans **Active Directory**, en fonction de l'appartenance aux groupes et des **permissions NTFS** appliquées sur les dossiers.

Ce mécanisme garantit une expérience utilisateur homogène tout en facilitant l'administration du système d'information grâce à une gestion centralisée.

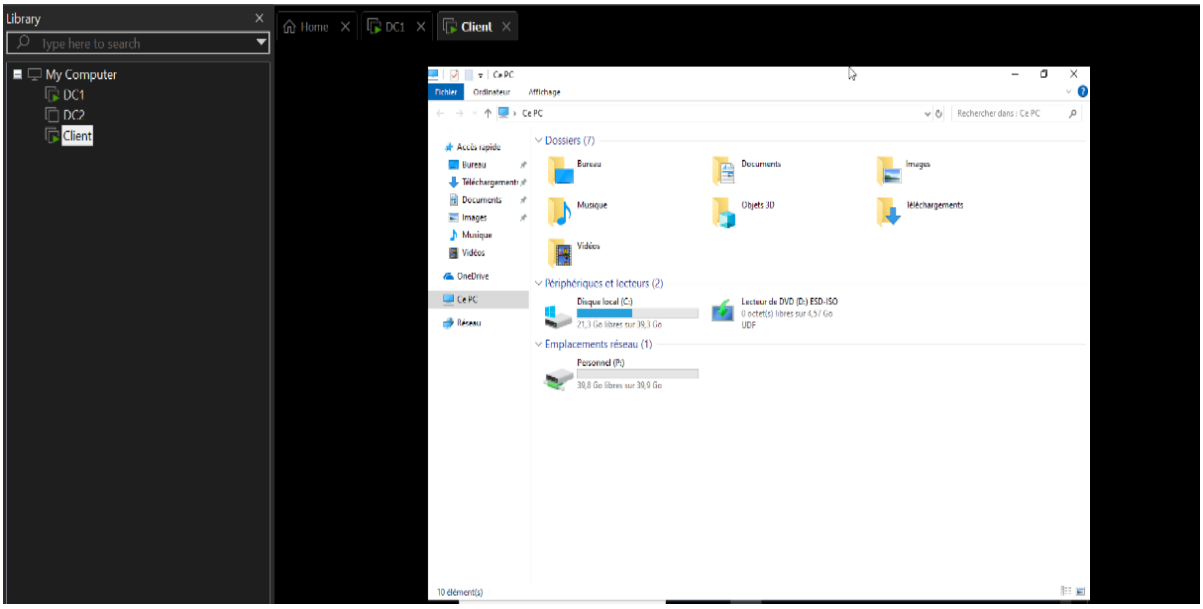


Figure : Lecteurs réseau automatiquement montés et visibles sur un poste client du domaine.

Mise en place de la sauvegarde des données

1. Objectif de la sauvegarde

La mise en place d'un système de sauvegarde est indispensable afin de garantir la **protection des données** et d'assurer la **continuité d'activité** en cas de panne, d'erreur humaine ou d'incident système.
L'objectif principal est de permettre une **restauration rapide et fiable** des données critiques.

2. Installation de l'outil de sauvegarde

Le service **Windows Server Backup** a été installé sur le serveur **DC1** afin de permettre la sauvegarde des données et des paramètres du système.
Cet outil natif de Windows Server offre une solution **simple, fiable et adaptée** aux infrastructures de petite et moyenne taille.

3. Configuration de la stratégie de sauvegarde

Une sauvegarde **complète quotidienne** a été configurée vers un support de stockage dédié.
Cette planification permet de sécuriser régulièrement les données tout en limitant l'impact sur les performances du serveur.

Un **test de restauration** a également été réalisé afin de vérifier l'intégrité des sauvegardes et de garantir la récupération effective des données en cas d'incident.

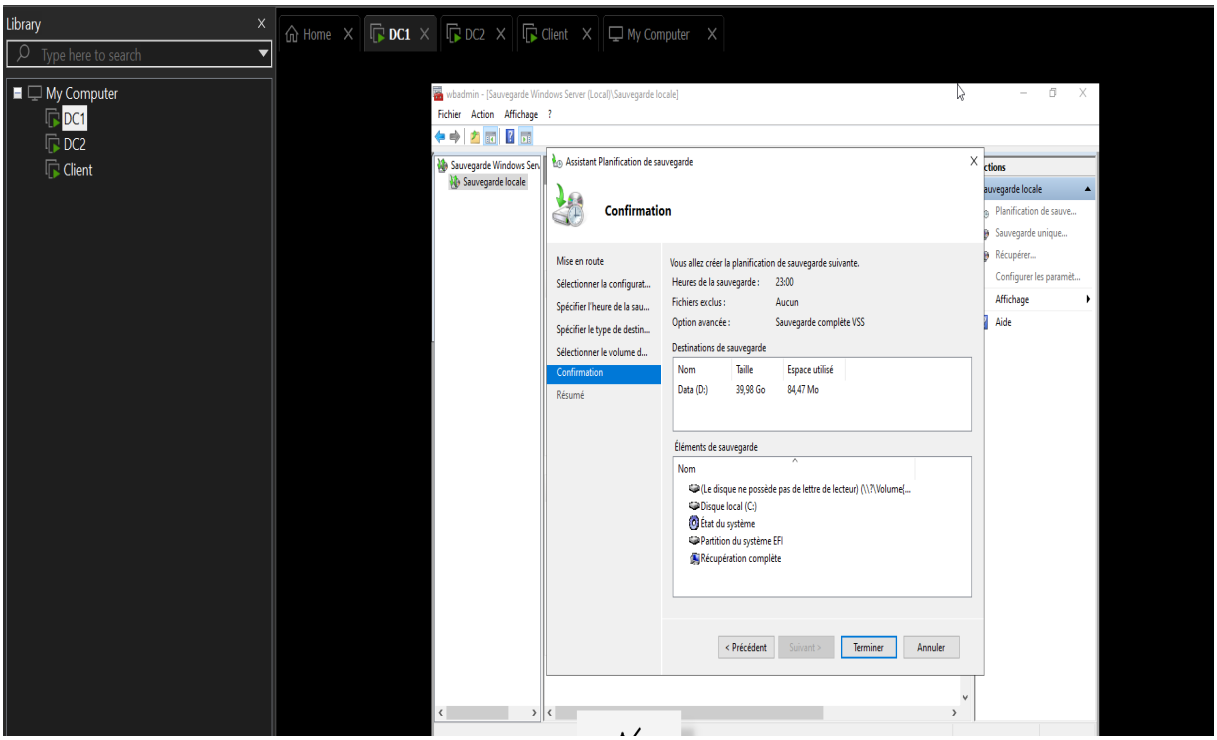


Figure : Interface d'installation et de configuration de Windows Server Backup.

3. Configuration de la sauvegarde planifiée

Une **sauvegarde planifiée** a été configurée afin d'automatiser la protection des données.
La sauvegarde s'exécute **quotidiennement à une heure définie** et est stockée sur un **support de stockage dédié**, permettant de conserver plusieurs versions des données et d'assurer leur disponibilité en cas d'incident.

Figure : Planification automatique de la sauvegarde avec Windows Server Backup.

---

4. Importance de la sauvegarde en entreprise

La sauvegarde régulière des données permet de **limiter les pertes en cas d'incident** et constitue un élément essentiel de la stratégie de sécurité du système d'information.
Elle contribue également à la **continuité d'activité**, à la **fiabilité des services** et à la **conformité aux bonnes pratiques de protection des données**.

Limites et améliorations possibles

1. Limites de l'infrastructure mise en place

L'infrastructure déployée dans le cadre de ce projet a été réalisée dans un **environnement virtualisé à des fins pédagogiques**.
Certaines limitations doivent donc être prises en compte :

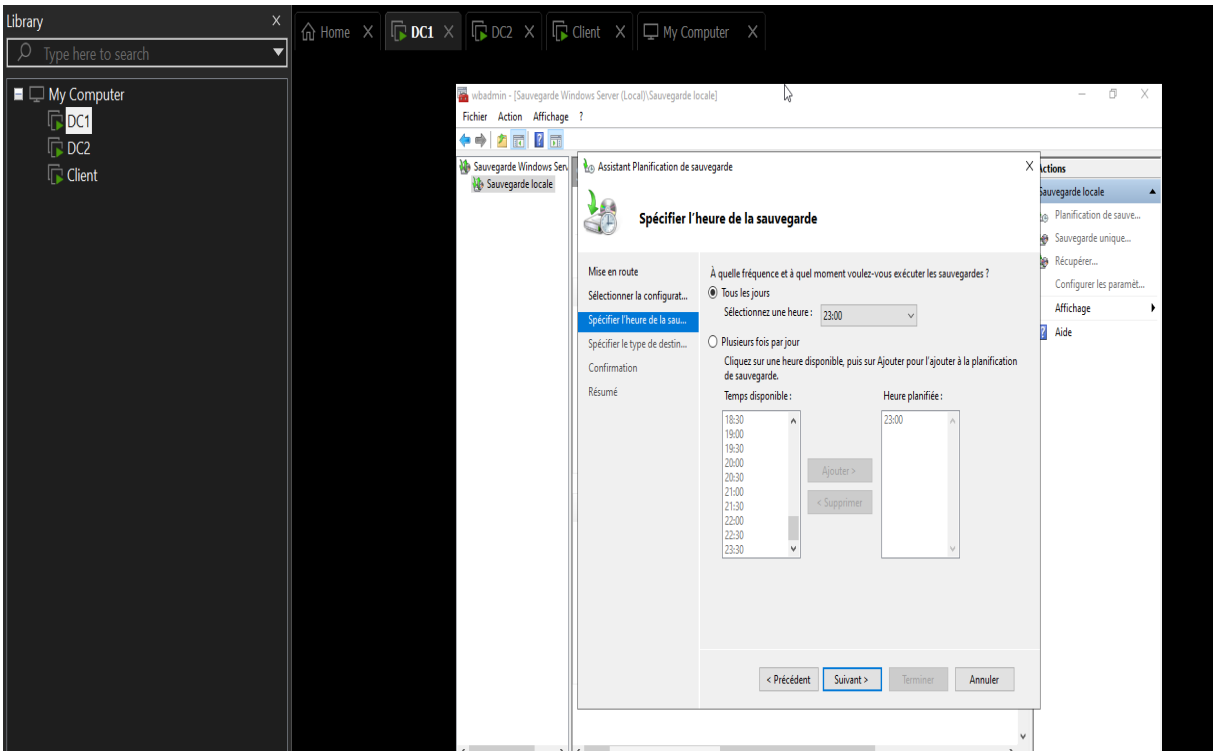
- Absence de **plan de reprise d'activité (PRA)** complet
- Sauvegardes stockées sur un **support unique**
- Absence de **solution de supervision des serveurs**
- Sécurité reposant principalement sur les **mécanismes natifs de Windows**

2. Améliorations envisageables

Afin de renforcer la robustesse de l'infrastructure, plusieurs évolutions pourraient être mises en œuvre :

- Mise en place d'un **PRA** et de sauvegardes **hors site**
- Déploiement d'une **solution de supervision** (type Centreon, Zabbix…)
- Renforcement de la **sécurité réseau** (pare-feu avancé, segmentation, journalisation)
- Automatisation supplémentaire de l'administration système

Ces améliorations permettraient d'atteindre un **niveau de sécurité et de disponibilité conforme aux exigences d'une infrastructure professionnelle**.



Conclusion générale

Ce projet a permis de mettre en œuvre une **infrastructure informatique de type entreprise** basée sur **Windows Server 2022** et **Active Directory**. L'ensemble des services essentiels a été déployé, notamment la **gestion centralisée des utilisateurs**, la **distribution automatique des adresses IP**, l'**application de stratégies de groupe**, la **gestion des partages réseau** ainsi que la **mise en place d'une solution de sauvegarde planifiée**.

La réalisation de cette infrastructure m'a permis de **renforcer mes compétences en administration systèmes et réseaux**, tout en développant une meilleure compréhension des enjeux liés à la **sécurité**, à la **disponibilité des services** et à la **gestion globale d'un système d'information** en environnement professionnel.

Les connaissances acquises au cours de ce projet constituent une **base solide pour une intégration en milieu professionnel**, notamment dans des fonctions d'**administrateur systèmes et réseaux** ou de **technicien SISR**, avec une capacité à déployer, sécuriser et maintenir une infrastructure d'entreprise fiable.

Enfin, les pistes d'amélioration identifiées (PRA, supervision, sécurité renforcée, MFA) ouvrent des perspectives d'évolution vers une **infrastructure plus résiliente et conforme aux bonnes pratiques professionnelles**.