Boumrah Samy

Active Directory - Chapitre 1 Activation AD DS / Création d'un Domain Controller.

Cette étape du projet de simulation de réseau d'entreprise détaille la procédure de déploiement d'un contrôleur de domaine au sein d'une infrastructure Active Directory, basée sur Windows Server 2022.

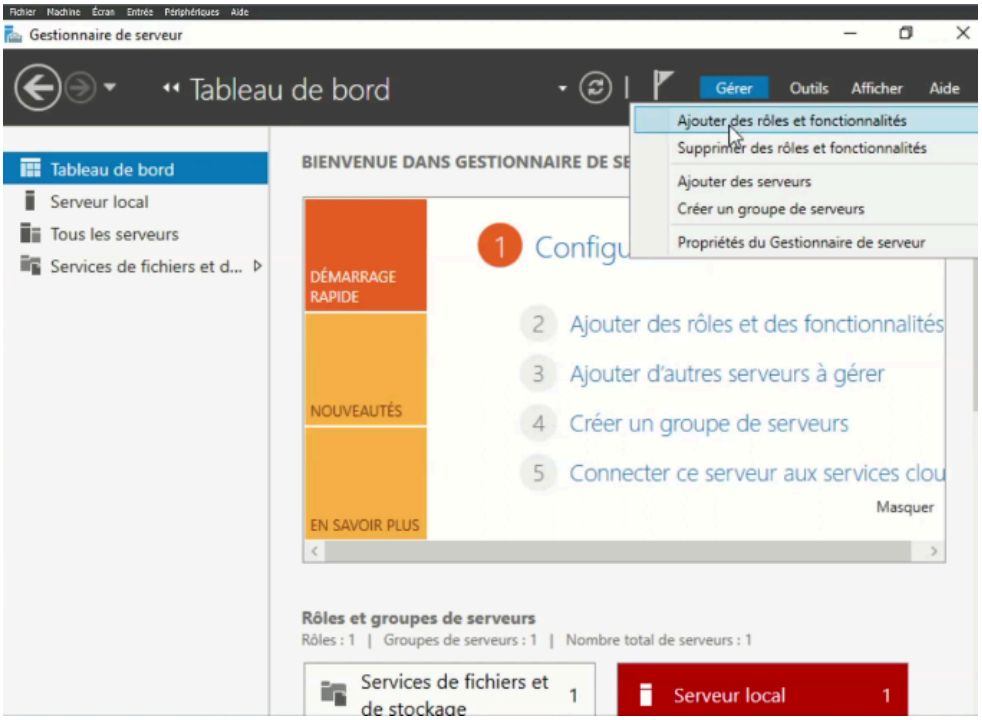
Prérequis techniques
Avant de procéder à l'installation, les configurations suivantes doivent être opérationnelles :

- Attribution d'une adresse IP statique au serveur Windows.
- Configuration du routeur pfSense assurant les services DHCP et DNS pour le réseau.

Procédure de déploiement

L'installation des services AD DS s'effectue via le Gestionnaire de serveur en suivant ces étapes :

1. Ouvrir le Gestionnaire de serveur.
2. Sélectionner l'option Ajouter des rôles et fonctionnalités pour lancer l'assistant de déploiement.



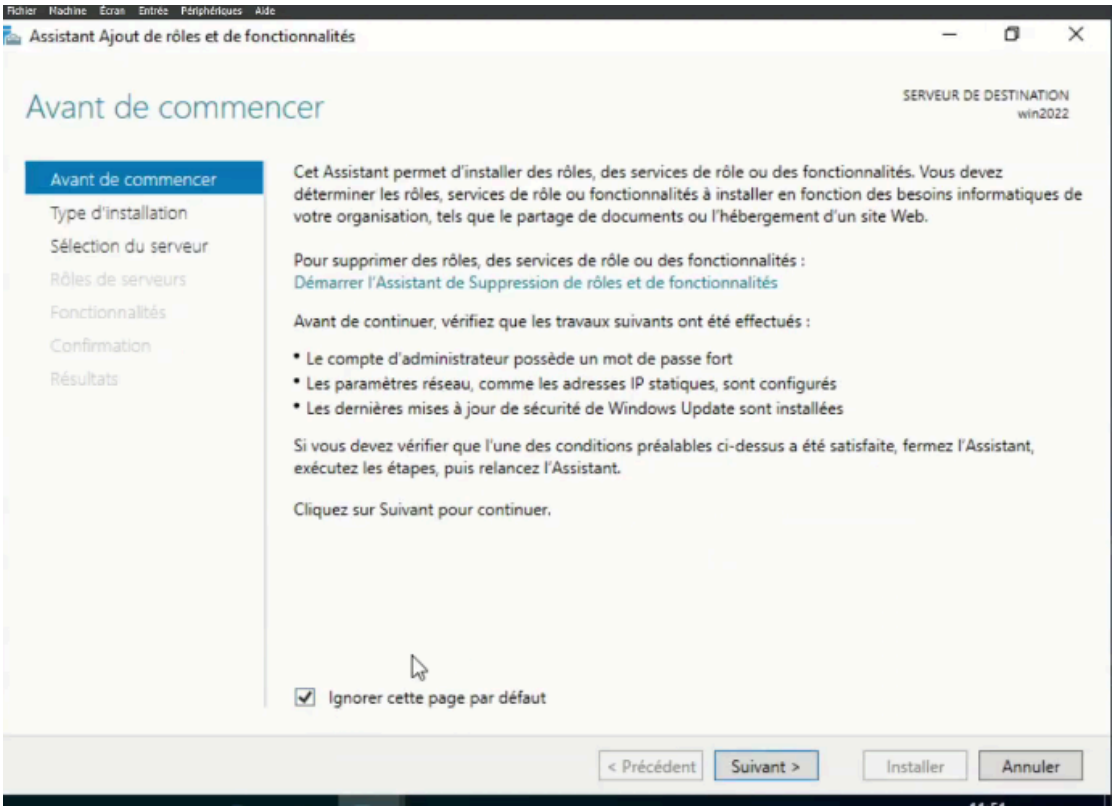
« Figure 1 : Lancement de l'assistant d'ajout de rôles et fonctionnalités »

Préparation de l'installation

Avant de poursuivre, il est impératif de valider les prérequis de sécurité du serveur. Bien que cette première page puisse être ignorée, il est recommandé de s'assurer que les conditions suivantes sont remplies :

- Sécurité des accès : Utilisation d'un mot de passe complexe pour le compte administrateur.
- Configuration réseau : Adresse IP statique correctement attribuée à la machine virtuelle.
- Maintenance : Installation des dernières mises à jour de sécurité via Windows Update.

Une fois ces vérifications effectuées, cliquez sur **Suivant** pour accéder aux étapes de configuration des rôles.

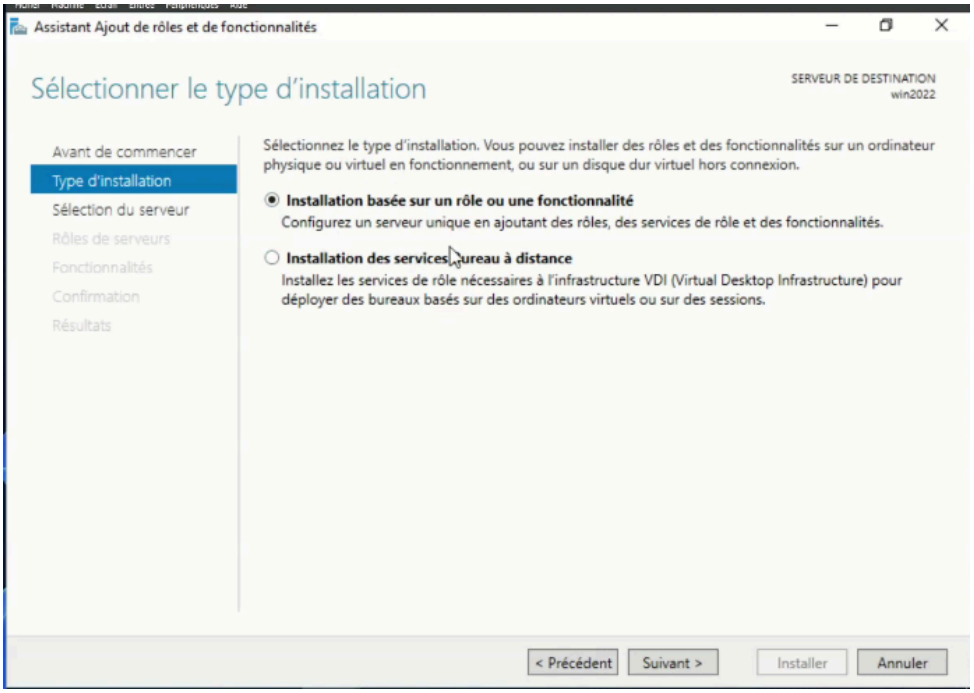


« Figure 2 : Validation des prérequis de sécurité avant l'ajout de rôles ».

Étape 2 : Sélection du type d’installation

Dans cette fenêtre de l’assistant, nous définissons le type d’installation requis. Pour ajouter les services Active Directory à notre serveur, nous conservons l’option Installation basée sur un rôle ou une fonctionnalité par défaut.

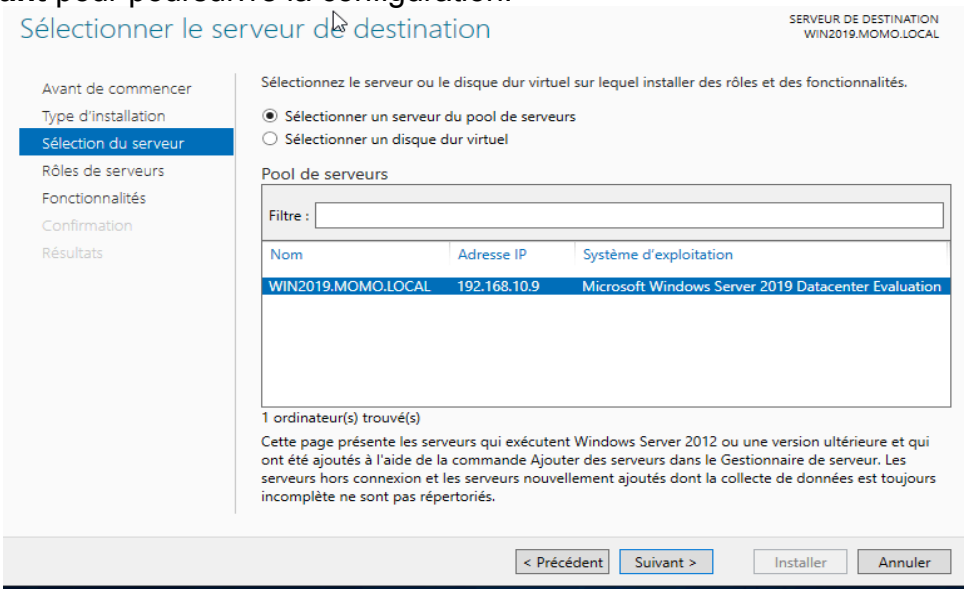
Cliquez sur **Suivant** pour valider ce choix et procéder à l’étape suivante de la configuration.



« Figure 3 : Sélection du type d'installation basée sur un rôle ou une fonctionnalité ».

Étape 3 : Sélection du serveur de destination

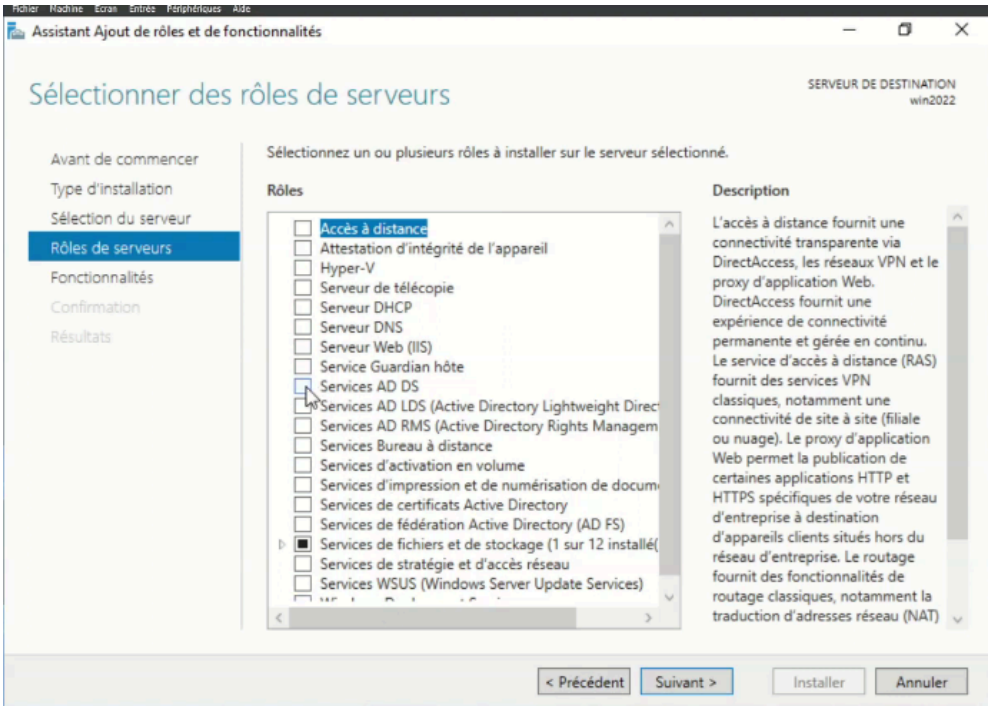
À cette étape, vérifiez que votre serveur apparaît correctement dans la liste des serveurs disponibles du pool. Une fois le serveur cible sélectionné, cliquez sur **Suivant** pour poursuivre la configuration.



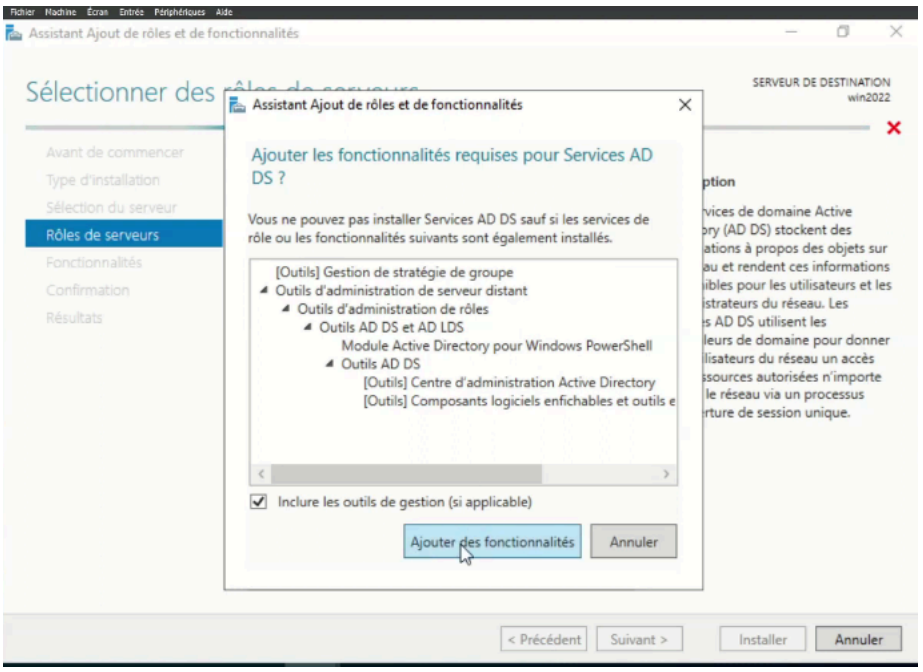
« Figure 4 : Sélection du serveur de destination dans le pool de serveurs ».

Étape 4 : Sélection des rôles serveur

Dans la liste des rôles disponibles, sélectionnez et cochez la case Services AD DS (Active Directory Domain Services). Une fenêtre contextuelle apparaîtra alors pour vous demander d'ajouter les outils d'administration associés ; validez en cliquant sur Ajouter des fonctionnalités, puis poursuivez en cliquant sur **Suivant**.



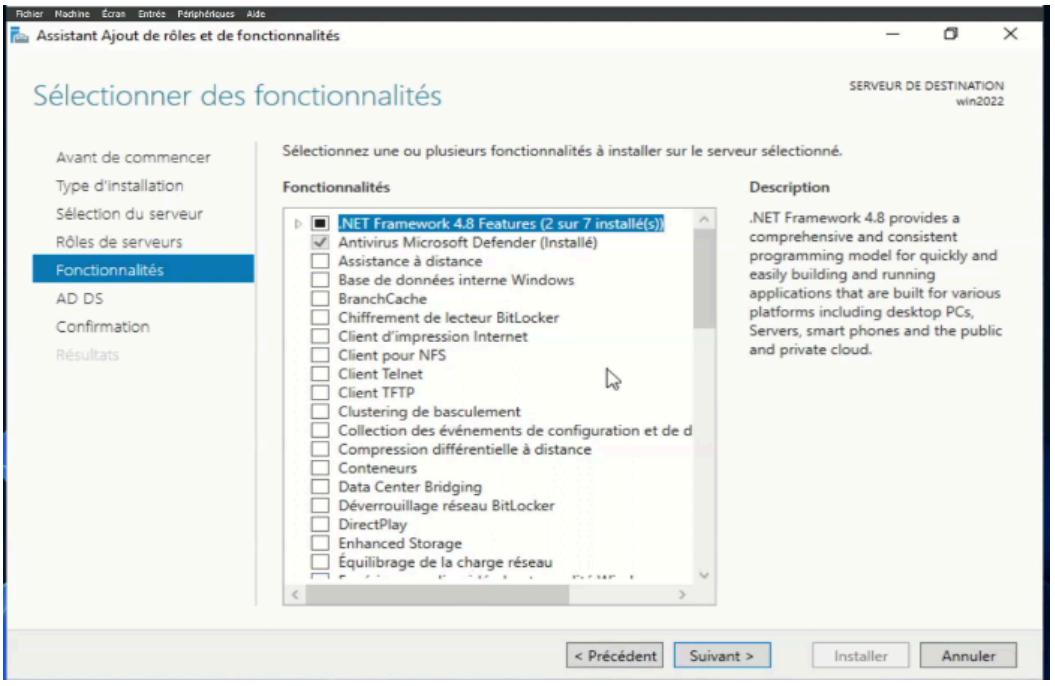
« Figure 5 : Sélection du rôle Services AD DS (Active Directory Domain Services) ».



Étape 5 : Sélection des fonctionnalités

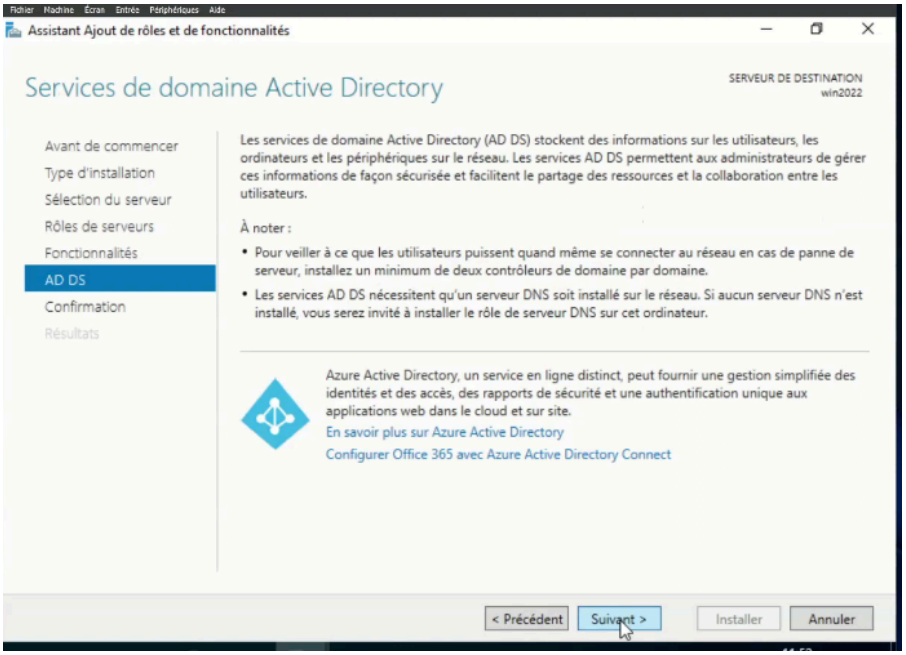
L'assistant propose ensuite d'ajouter des fonctionnalités complémentaires à votre serveur. Pour le bon déroulement de ce projet, nous conserverons les options par défaut, car celles-ci sont suffisantes pour l'installation des services AD DS. Il sera toujours possible d'ajouter des fonctionnalités ultérieurement selon les besoins de l'infrastructure.

Cliquez sur **Suivant** pour passer à l'étape suivante.



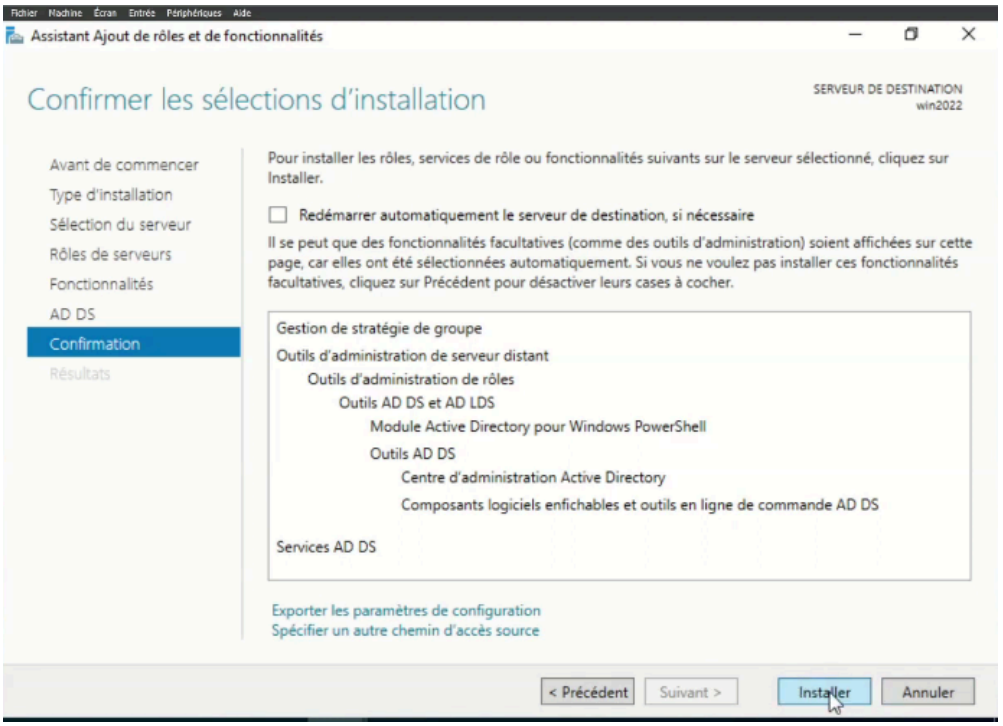
« Figure 6 : Sélection des fonctionnalités par défaut ».

On clique à nouveau sur **SUIVANT >**



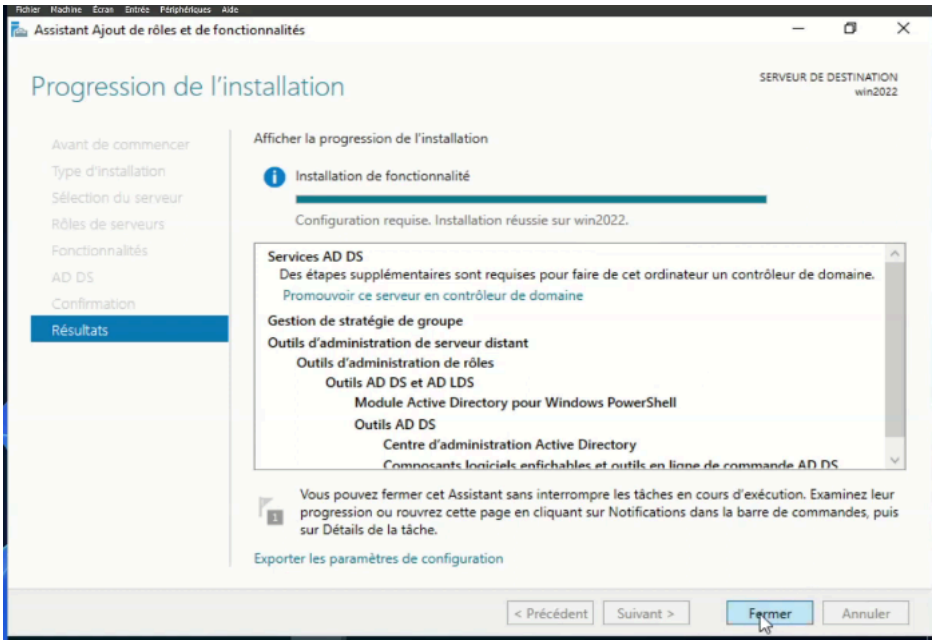
Étape 6 : Validation et installation des services

Une fois les étapes de configuration précédentes validées, l'assistant affiche un récapitulatif des choix effectués. Vous pouvez désormais lancer l'installation des **Services AD DS** en cliquant sur le bouton **Installer**. Le déploiement s'exécute alors en arrière-plan, et la progression peut être suivie directement dans la fenêtre de l'assistant.



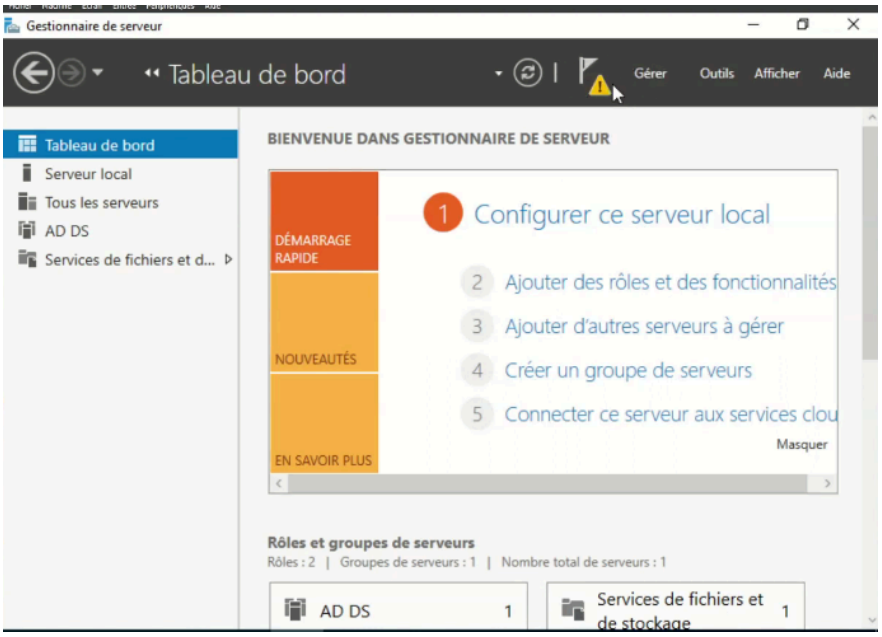
« Figure 7 : Lancement de l'installation des services AD DS ».

Une fois l'installation terminé on va passer à l'étape de configuration donc on va cliquer sur **FERMER.**



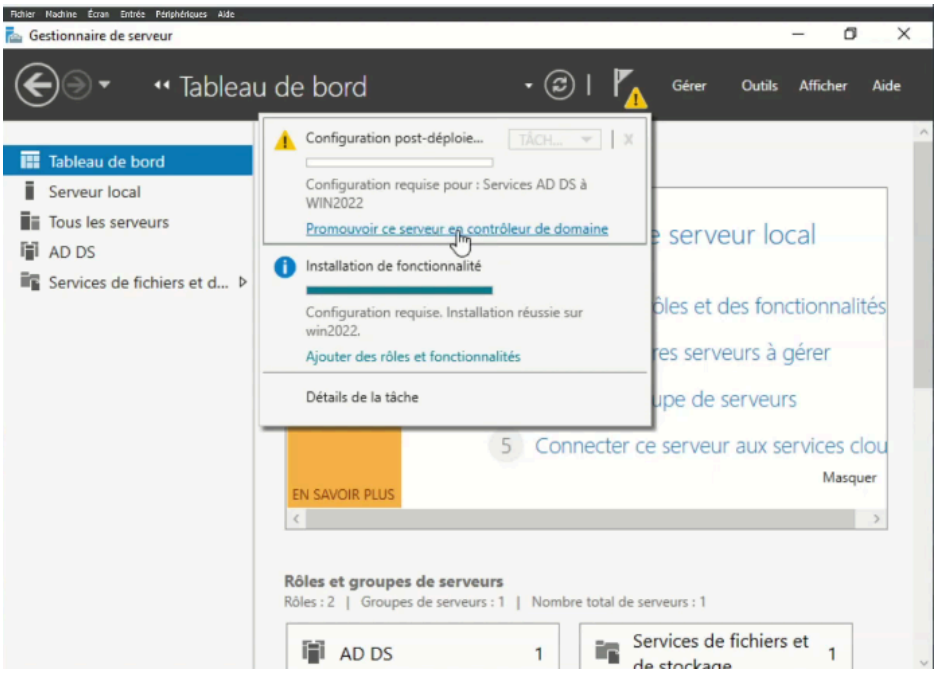
Étape 7 : Promotion du serveur en contrôleur de domaine

Une fois l'installation des rôles terminée, une notification d'avertissement apparaît dans la barre de titre du Gestionnaire de serveur. Celle-ci indique qu'une configuration post-déploiement est nécessaire pour finaliser l'installation.



« Figure 8 : Notification de configuration post-déploiement dans le Gestionnaire de serveur ».

Cliquez sur l'icône de notification (le drapeau avec un triangle jaune) pour afficher les détails des tâches en attente. Vous verrez alors une option permettant de **Promouvoir ce serveur en contrôleur de domaine.** Cliquez sur ce lien bleu pour ouvrir l'assistant de configuration Active Directory.

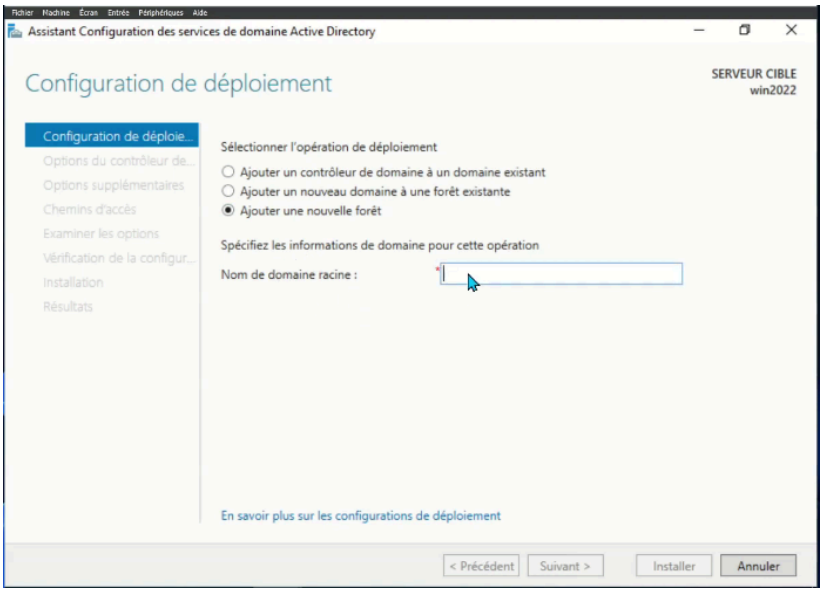


« Figure 9 : Lancement de l'assistant de promotion en contrôleur de domaine »

Étape 8 : Configuration de la forêt Active Directory

Étant donné qu'il s'agit du premier contrôleur de domaine de notre infrastructure, nous devons créer une nouvelle forêt. Dans l'assistant de configuration, sélectionnez l'option **Ajouter une nouvelle forêt.**

Saisissez ensuite le nom de votre domaine racine. Pour ma part, j'utiliserais l'appellation **MOMO.LOCAL** car ce projet m'a été suggéré par mon ami Mohamed**.** Une fois le nom défini, cliquez sur **Suivant** pour poursuivre la configuration des options du contrôleur de domaine.



« Figure 10 : Création d'une nouvelle forêt et définition du nom de domaine racine ».

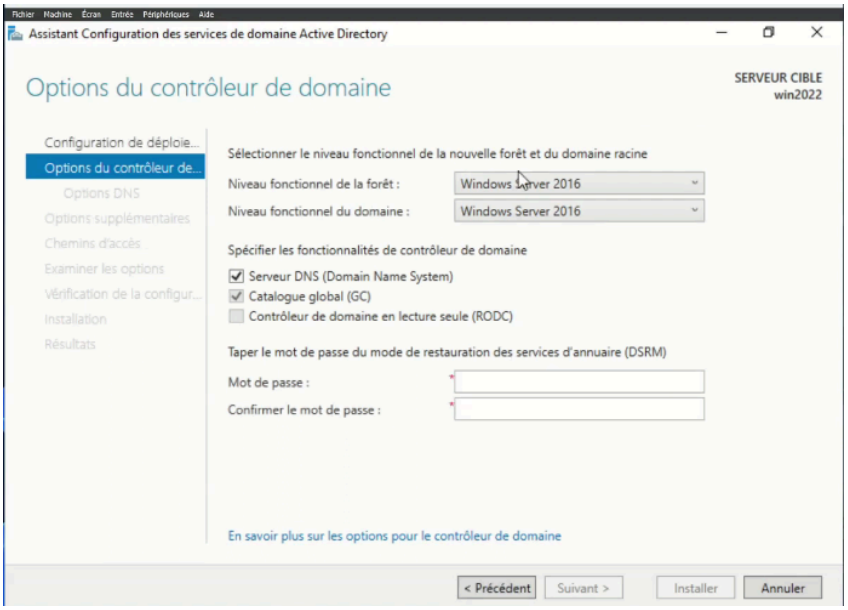
Boumrah Samy

Étape 9 : Options du contrôleur de domaine

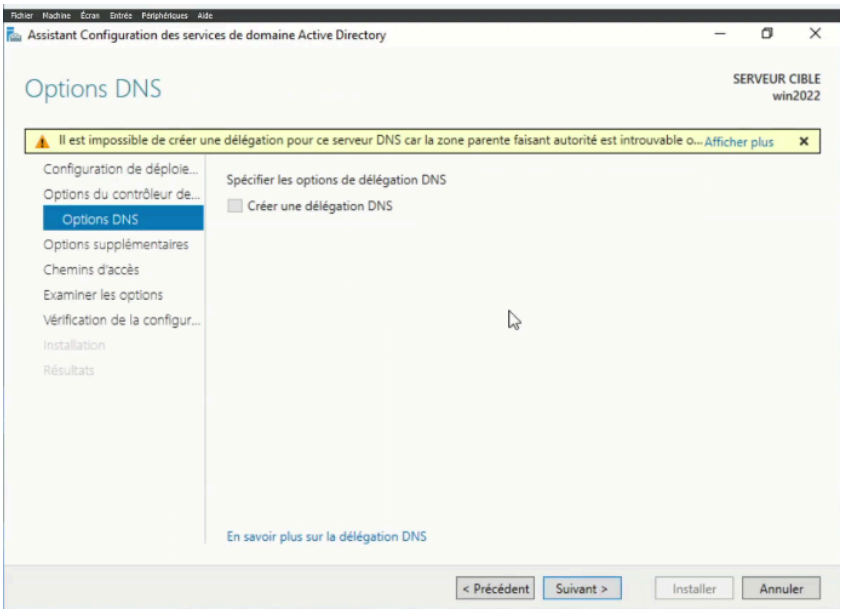
Dans cette section, nous définissons le niveau fonctionnel de la forêt et du domaine. Pour garantir la compatibilité et les fonctionnalités les plus récentes, nous conservons les valeurs par défaut (généralement Windows Server 2016 ou supérieur).

Il est indispensable de définir un **mot de passe de restauration des services d'annuaire (DSRM).** Ce mot de passe est critique, car il permet de restaurer l'annuaire Active Directory en cas de sinistre ou de corruption de la base de données.

Une fois le mot de passe saisi et confirmé, cliquez sur **Suivant**.

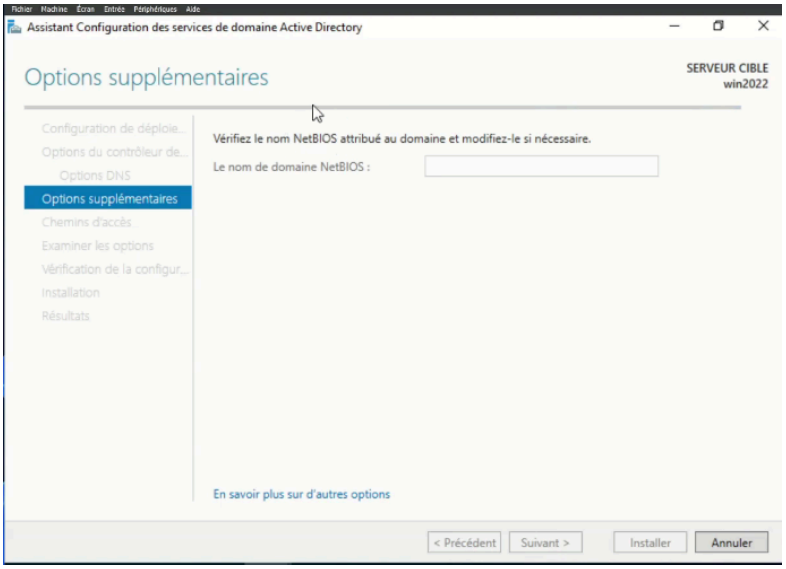


« Figure 11 : Définition du niveau fonctionnel et du mot de passe DSRM »



Étape 10 : Attribution du nom NetBIOS

À cette étape, l'assistant affiche automatiquement le nom NetBIOS correspondant au domaine racine défini précédemment (ex: **MOMO**). Vérifiez que ce nom est correctement généré, puis cliquez sur **Suivant** pour valider et poursuivre la configuration.

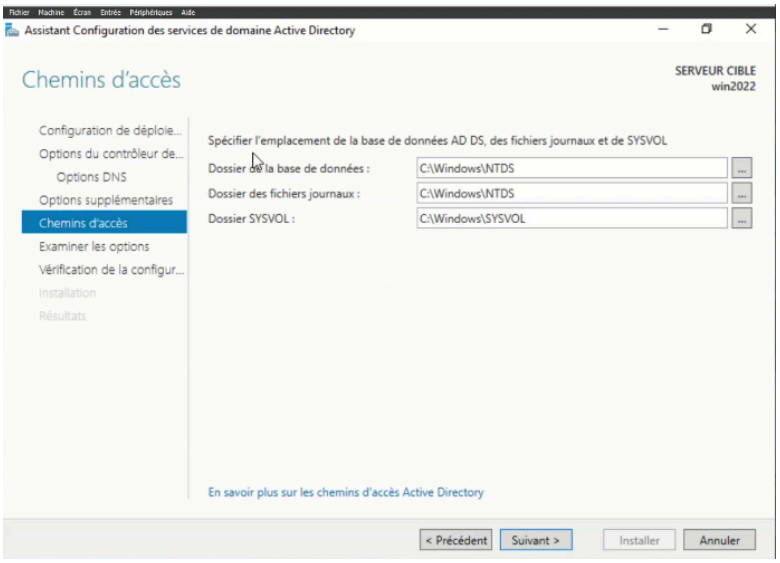


« Figure 12 : Vérification du nom NetBIOS du domaine ».

Étape 11 : Chemins d'accès des bases de données

L'assistant propose ensuite de définir l'emplacement de stockage des fichiers de la base de données Active Directory (NTDS), des fichiers journaux et du répertoire SYSVOL.

Pour cet environnement, nous conservons les répertoires par défaut suggérés par le système. Cliquez sur **Suivant** pour valider ces paramètres et continuer la configuration.

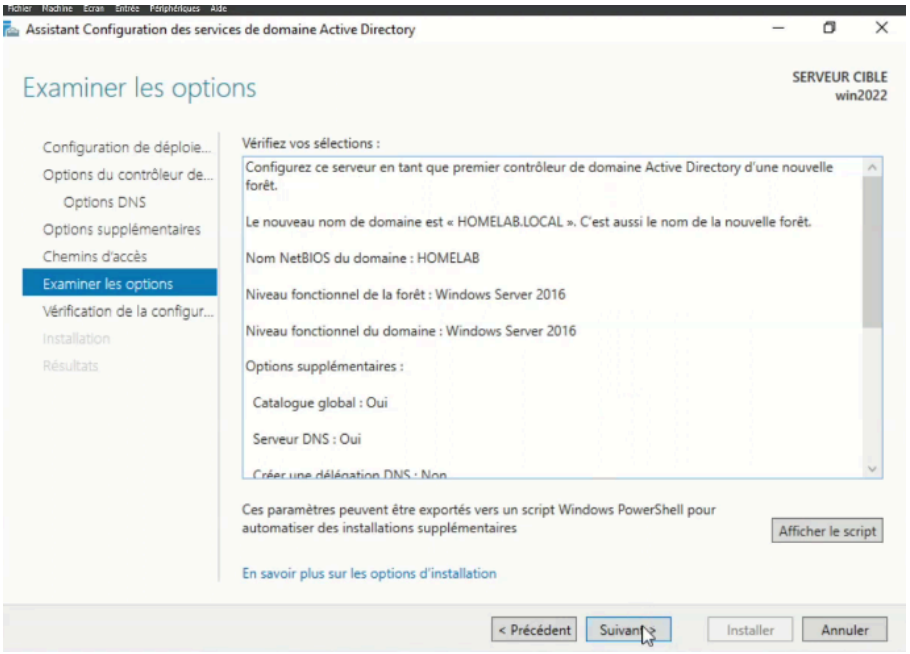


« Figure 13 : Configuration des emplacements de stockage des bases de données Active Directory »

Étape 12 : Récapitulatif et validation de la configuration

L'assistant affiche désormais une synthèse complète des options de configuration sélectionnées lors des étapes précédentes. Il est recommandé de vérifier attentivement ces informations pour assurer la conformité de l'installation avec les prérequis du projet.

Une fois les paramètres validés, cliquez sur **Suivant** pour passer à l'étape finale de contrôle des pré requis avant l'installation.



« Figure 14 : Synthèse des options de configuration de l'Active Directory ».

Étape 13 : Vérification des prérequis et installation

Une fois le récapitulatif validé, le système procède à une analyse automatique de la configuration afin de vérifier que tous les prérequis sont respectés. Si le message « Toutes les vérifications de la configuration requise ont réussi » s'affiche, vous pouvez finaliser le déploiement en cliquant sur **Installer**.

L'installation des services Active Directory débute alors, et le serveur procédera automatiquement à un redémarrage une fois la promotion terminée.

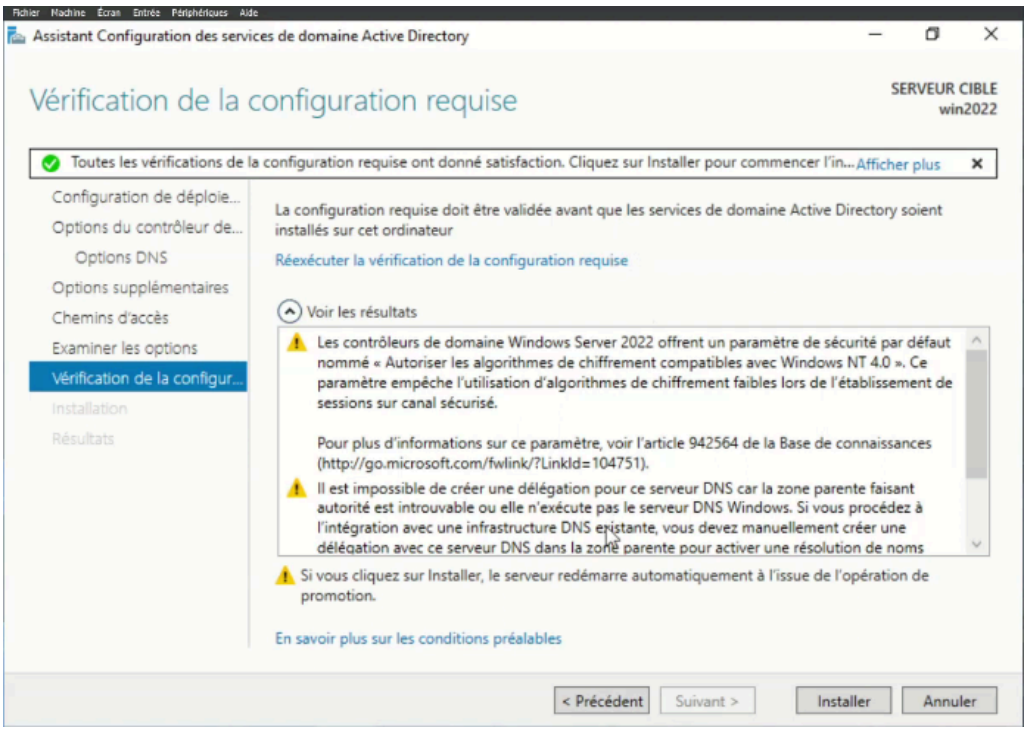
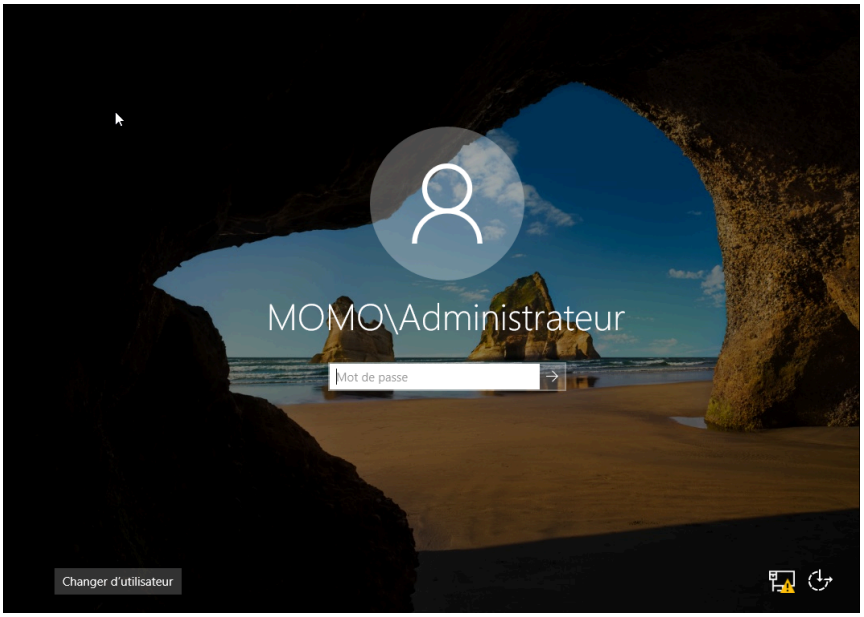


Figure 15 : Validation finale des prérequis avant l'installation du contrôleur de domaine ».

Étape 14 : Finalisation du déploiement et redémarrage

L'installation des services AD DS nécessite quelques minutes afin de finaliser la création du contrôleur de domaine et de structurer l'annuaire par défaut. Durant ce processus, le serveur redémarrera automatiquement pour appliquer les nouvelles configurations.

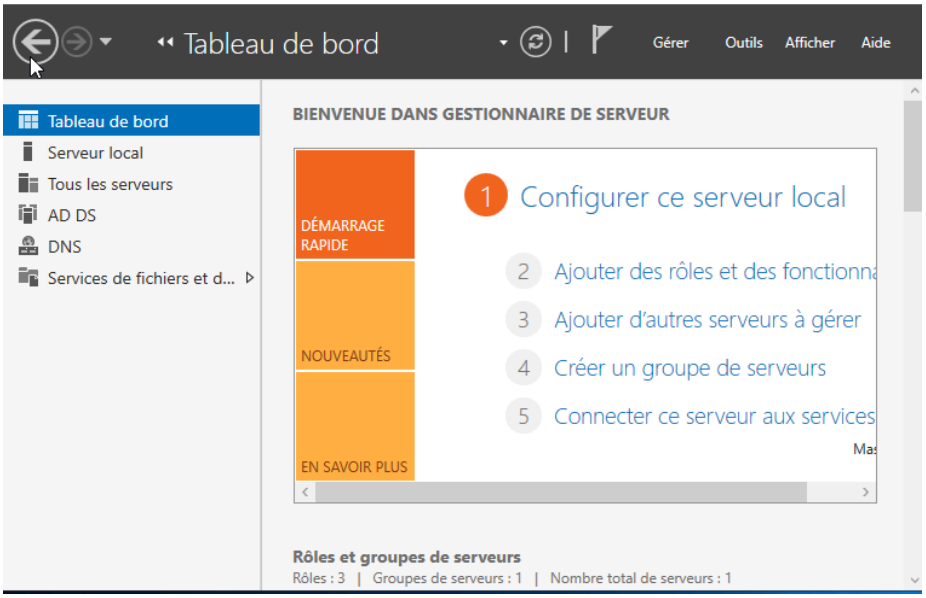
Une fois le redémarrage effectué, vous observerez le premier changement visuel sur l'écran d'ouverture de session : le nom de domaine précède désormais le compte utilisateur (ex: MOMO\Administrateur), confirmant que le serveur est bien promu en contrôleur de domaine.



: « *Figure 16 : Confirmation de la promotion du serveur après redémarrage ».*

Étape 15 : Vérification de l'installation

Une fois connecté, ouvrez le **Gestionnaire de serveur**. Vous constaterez que l'interface a été mise à jour : le rôle **AD DS** est désormais actif et votre domaine (**MOMO.LOCAL**) apparaît clairement dans le volet de navigation situé à gauche. Ce changement confirme que votre infrastructure est opérationnelle et prête à être administrée.



Conclusion du Chapitre 1

Le déploiement des services Active Directory Domain Services (AD DS) est désormais finalisé. Votre serveur Windows 2022 est officiellement promu en tant que contrôleur de domaine, constituant ainsi la pierre angulaire de votre infrastructure réseau. La base de l'annuaire est en place, permettant désormais la gestion centralisée des identités, la sécurisation des accès et le déploiement des futures politiques de groupe (GPO).

Fin du Chapitre 1.

Boumrah Samy

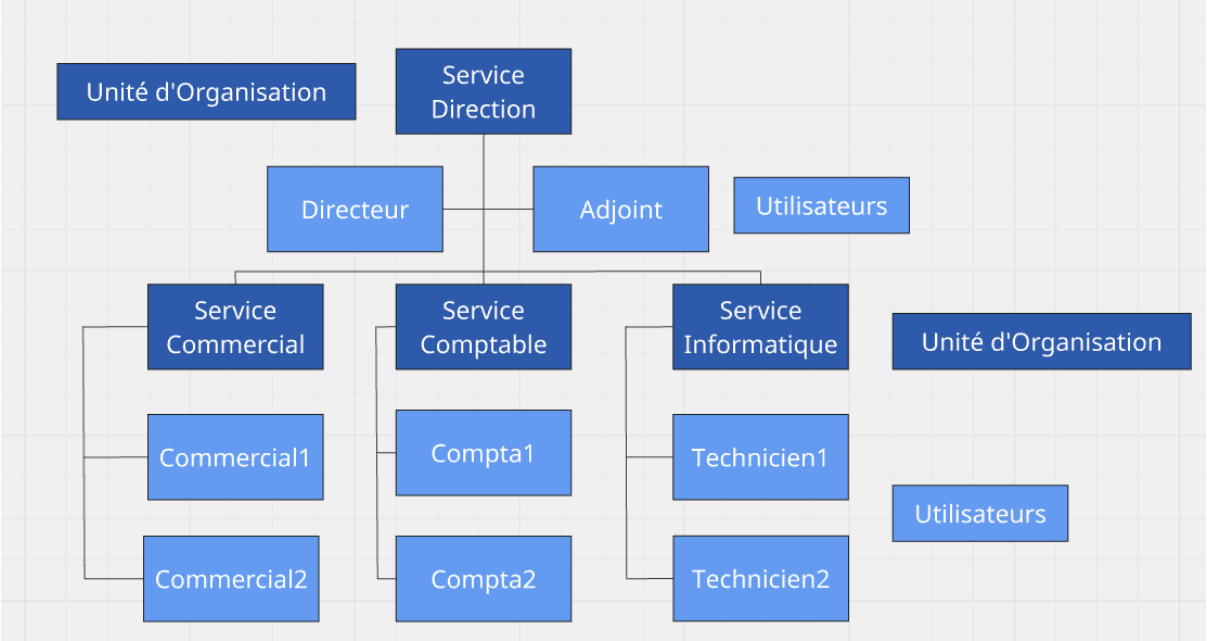
Active Directory - Chapitre 2 : Structuration de l'Active Directory

Objectif de la structuration

La structuration de l'annuaire Active Directory est une étape déterminante pour assurer une gestion cohérente, sécurisée et évolutive des ressources du système d'information. Elle consiste à organiser les objets (utilisateurs, ordinateurs, groupes) au sein d'Unités d'Organisation (UO) pour faciliter l'administration, la délégation de droits et l'application ciblée des politiques de groupe (GPO).

Architecture logique proposée

Pour ce laboratoire, nous adopterons une hiérarchie inspirée des bonnes pratiques d'administration système. Cette organisation s'articule autour de l'organigramme technique suivant, permettant de séparer distinctement les rôles, les responsabilités et les types d'objets.



« Figure 18 : Arborescence logique des Unités d'Organisation du domaine MOMO.LOCAL »

Organisation des ressources

Nous avons identifié quatre départements principaux : **Direction**, **Commercial**, **Comptabilité** et **Informatique**. Chaque département regroupe les comptes utilisateurs associés à ces pôles d'activité.

Afin de garantir une terminologie précise tout au long de ce projet, les concepts suivants seront utilisés :

- **Unité d'Organisation (UO) :** Conteneur logique permettant de structurer l'annuaire, correspondant ici aux différents services de l'entreprise. Les UO sont essentielles pour la délégation d'administration et l'application granulaire des stratégies de groupe.
- **Utilisateurs :** Objets identitaires représentant les membres des différents services, dont les accès et les droits seront administrés via leur appartenance à ces UO.

Lancement de l'administration

Pour débuter la mise en œuvre de cette structure, assurez-vous que votre contrôleur de domaine Windows Server est opérationnel et que les services AD DS sont correctement démarrés.

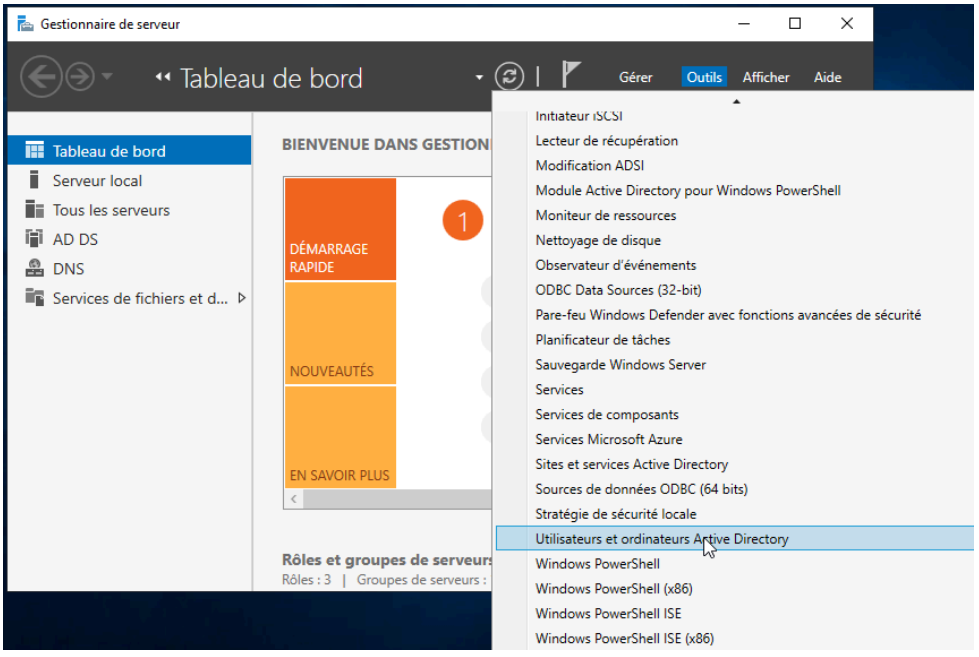
Étape 1 : Accès à la console d'administration

Pour entamer la structuration de votre annuaire, vous devez accéder à la console d'administration **Utilisateurs et ordinateurs Active Directory** (ADUC).

Depuis le **Gestionnaire de serveur**, procédez comme suit :

1. Cliquez sur le menu **Outils** situé dans la barre de navigation supérieure.
2. Dans le menu déroulant, sélectionnez **Utilisateurs et ordinateurs Active Directory**.

Note : Vous pouvez également accéder rapidement à cette console en saisissant la commande dsa.msc dans la fenêtre "Exécuter" (Windows + R).



« Figure 19 : Console d'administration des Utilisateurs et ordinateurs Active Directory »

Étape 2 : Analyse de l'arborescence par défaut

Lors de l'activation des services AD DS, le système génère automatiquement une structure de dossiers par défaut. Il est important de bien comprendre le rôle de chacun de ces conteneurs :

- **Builtin :** Contient les groupes de sécurité par défaut du domaine.
- **Computers :** Regroupe par défaut les ordinateurs joints au domaine.
- **Domain Controllers :** Contient les serveurs ayant le rôle de contrôleur de domaine.
- **Users :** Contient les comptes utilisateurs et groupes créés initialement lors du

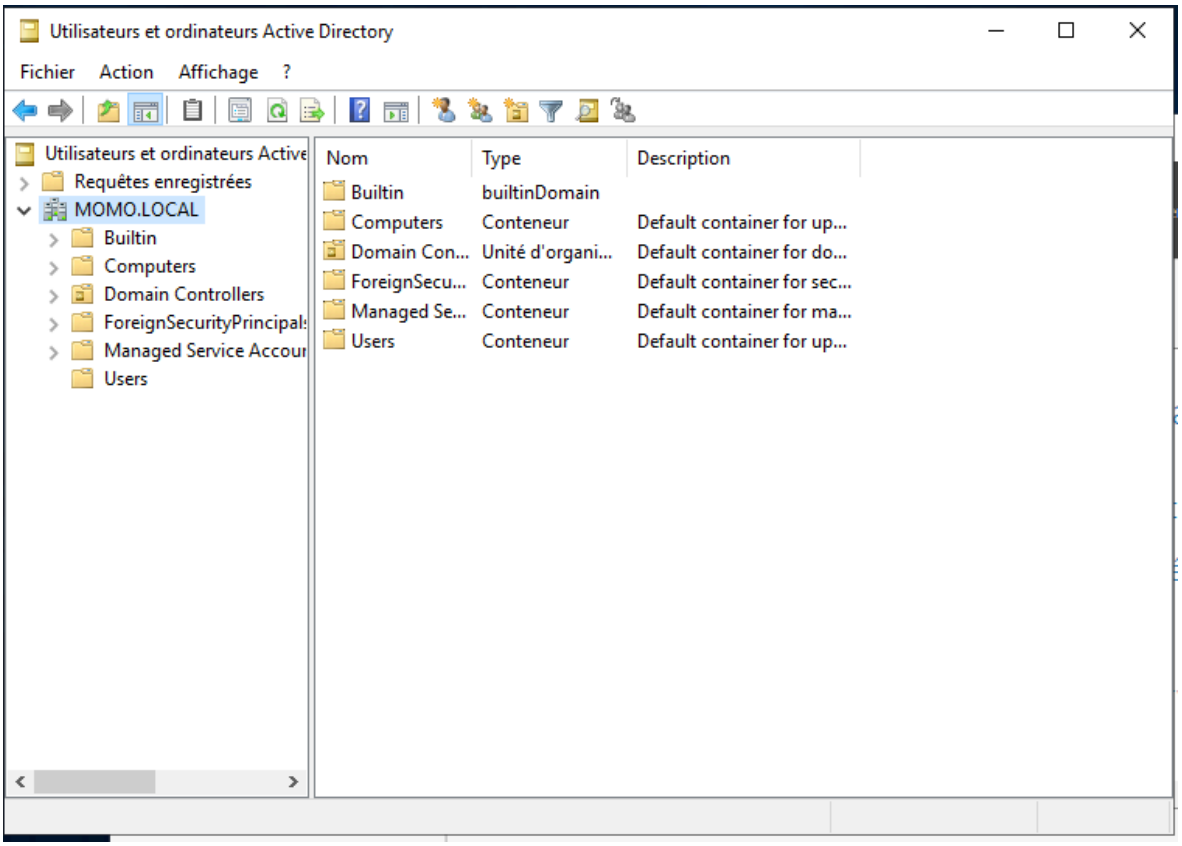


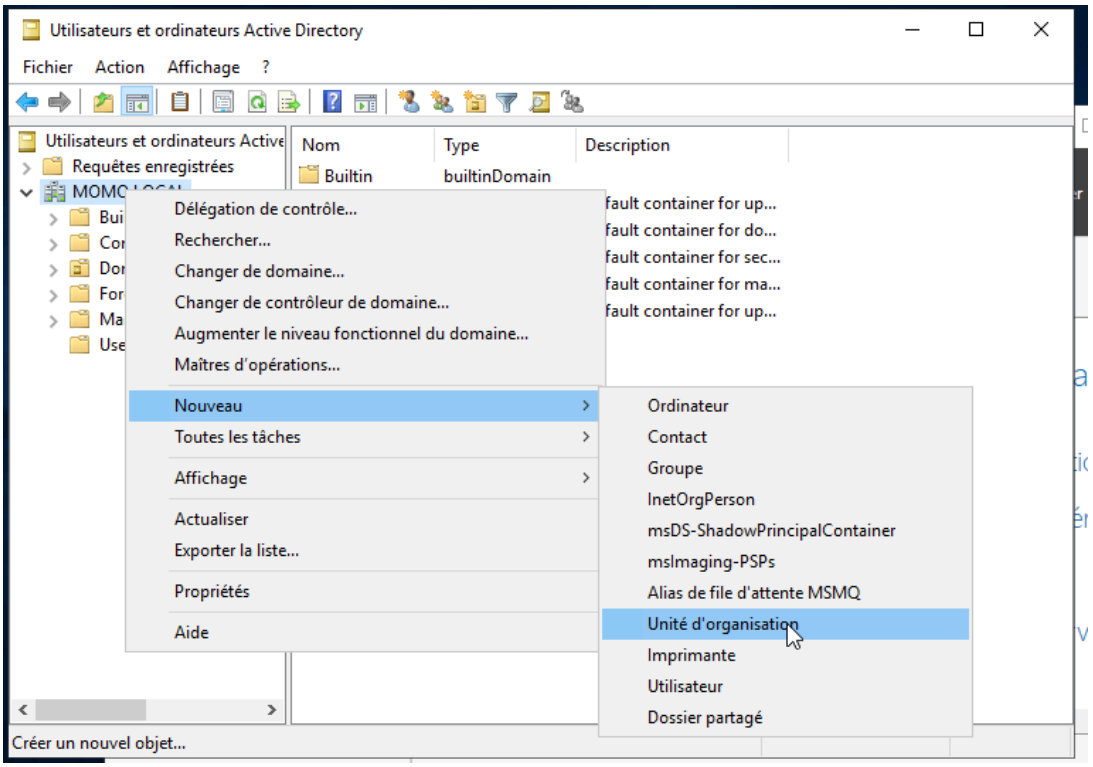
Figure 20 : Arborescence par défaut des conteneurs Active Directory »

Étape 3 : Création des Unités d'Organisation (UO)

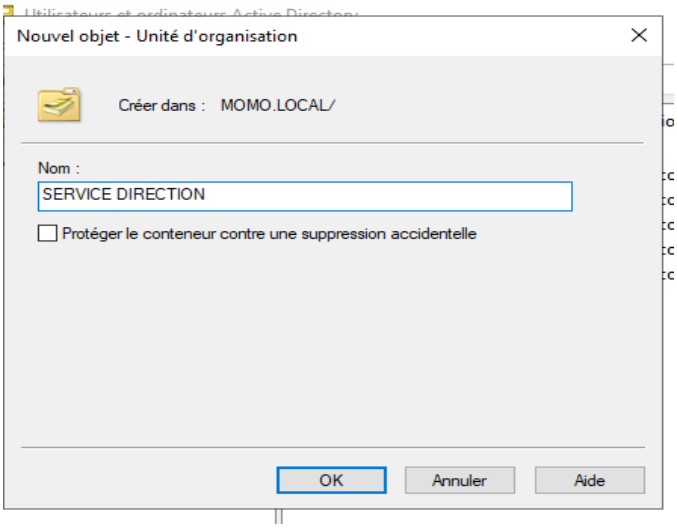
Afin d'implémenter l'arborescence définie dans notre organigramme et d'assurer une gestion rigoureuse de notre infrastructure, nous devons créer des Unités d'Organisation dédiées. Cette segmentation est indispensable pour appliquer des stratégies de groupe (GPO) spécifiques à chaque service.

Pour créer votre première unité d'organisation au sein de l'annuaire :

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, effectuez un clic droit sur votre nom de domaine (ex: MOMO.LOCAL).
2. Pointez sur **Nouveau**, puis sélectionnez **Unité d'organisation**.
3. Saisissez le nom du service correspondant (ex: *Direction*, *Commercial*, *Comptabilité* ou *Informatique*) et validez en cliquant sur **OK** pour finaliser la création de votre **UO**.

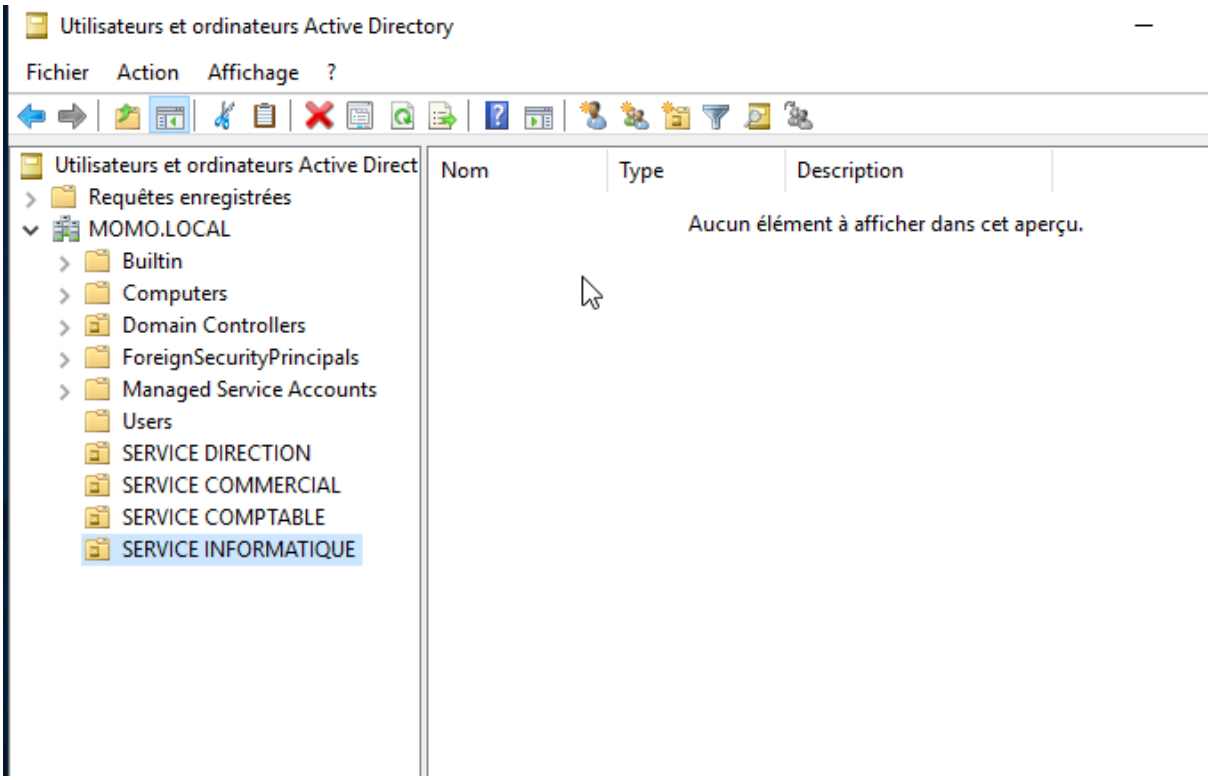


« Figure 21 : Procédure de création d'une nouvelle unité d'organisation »



NB : Vous pouvez décocher la case pour pouvoir supprimer vos UO plus tard sans soucis ou la garder cocher pour sécuriser vos d'une suppression accidentelle.

Une fois la première unité d'organisation créée, elle apparaît dans la console **Utilisateurs et ordinateurs Active Directory** sous le nom que vous avez défini. Cela confirme que la structure de base de l'annuaire est bien en place et que la première UO a été créée avec succès.



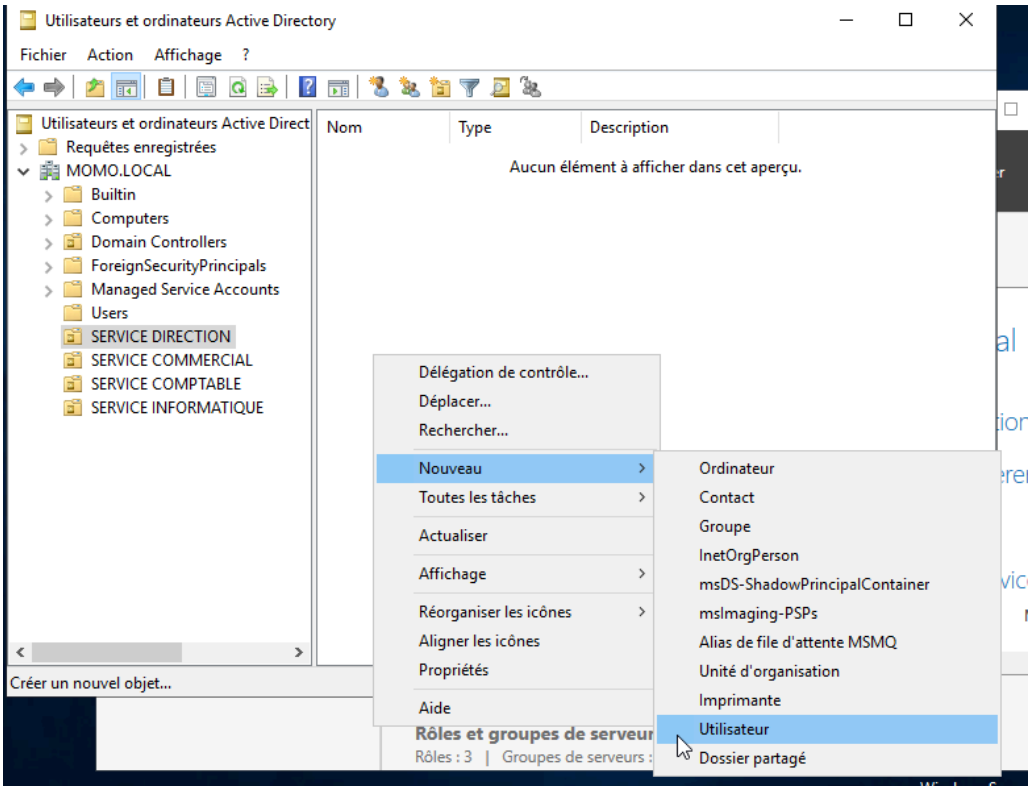
« Figure 22 : Création réussie de la première unité d'organisation »

Nous allons ensuite répéter cette opération afin de créer l'ensemble des unités d'organisation prévues dans l'organigramme du projet. Une fois les **quatre UO** créées, nous pourrons passer à l'étape suivante, qui consiste à créer les utilisateurs au sein de chaque service.

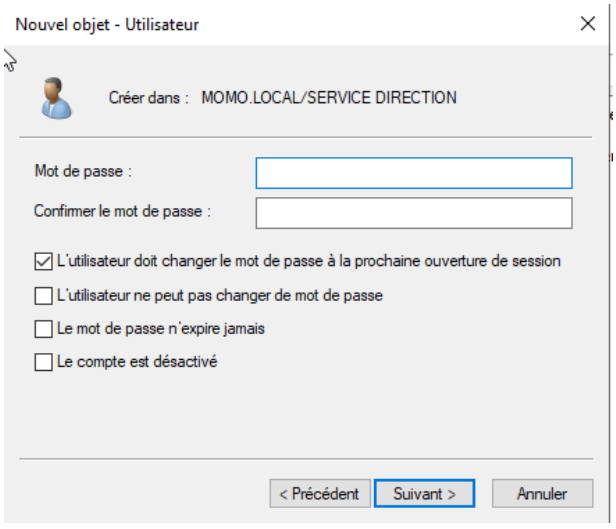
Étape 4 : Création des comptes utilisateurs

Une fois les Unités d'Organisation structurées, vous pouvez procéder à la création des comptes utilisateurs au sein de chaque service. Pour ce faire, suivez cette procédure :

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, naviguez jusqu'à l'unité d'organisation souhaitée (par exemple, le dossier SERVICE DIRECTION).
2. Effectuez un clic droit sur l'unité d'organisation.
3. Pointez sur **Nouveau**, puis sélectionnez **Utilisateur**.



« Figure 23 : Interface de création d'un nouvel utilisateur dans une UO »



Remplissez le formulaire de création avec les informations de l'utilisateur (Prénom, Nom, Nom de connexion), puis cliquez sur **Suivant** pour définir le mot de passe initial.

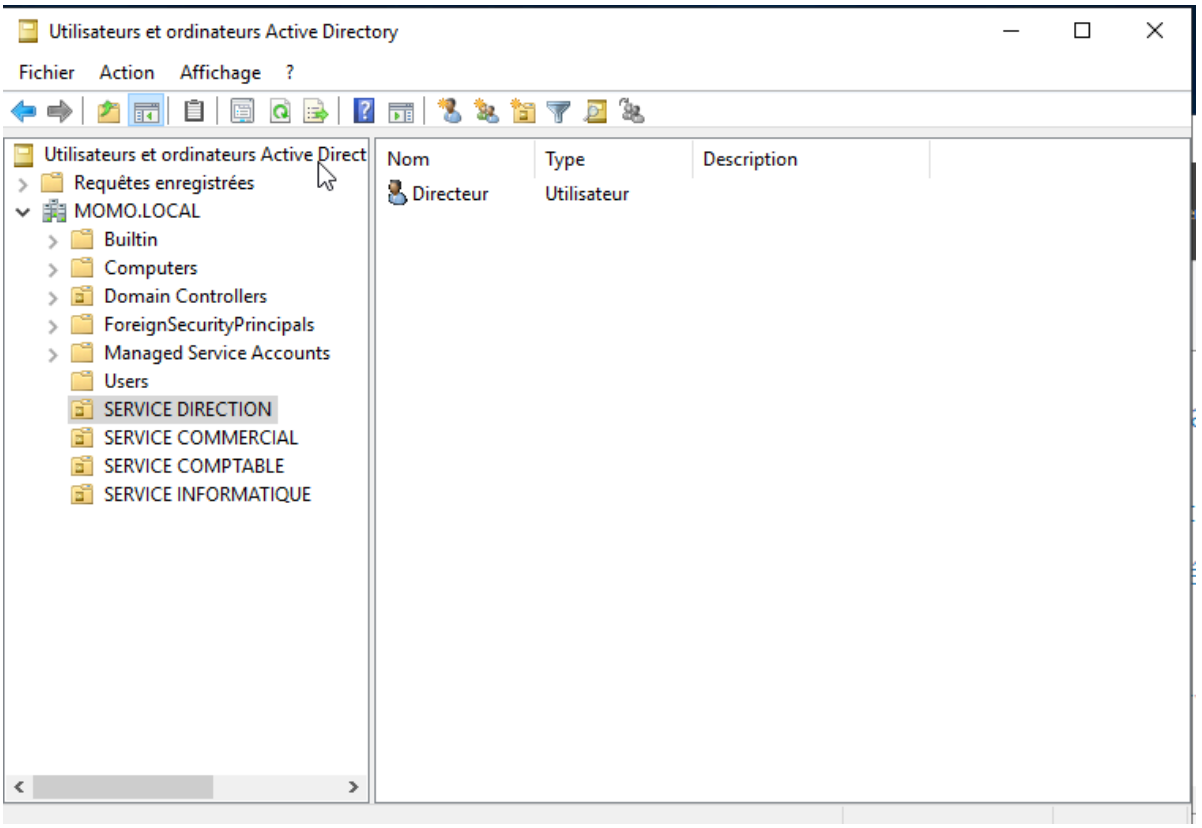
« Figure 24 : Configuration des options de mot de passe du compte utilisateur ».

Une fois les paramètres de sécurité définis selon vos besoins, cliquez sur **Terminer**. Votre premier utilisateur est alors créé et rattaché à l'unité d'organisation sélectionnée.

Note : Bien que ces configurations soient adaptées à un environnement de laboratoire, veillez à respecter les standards de sécurité de Microsoft en utilisant des mots de passe robustes (complexité, longueur et absence d'informations personnelles).

Gestion des objets

La console **Utilisateurs et ordinateurs Active Directory** offre une grande flexibilité dans l'administration de vos objets. Si un compte utilisateur a été créé par erreur dans une mauvaise unité d'organisation, il est possible de le déplacer simplement en le sélectionnant et en le faisant glisser (« drag-and-drop ») vers l'unité d'organisation cible.



« Figure 25 : Utilisateur correctement rattaché à son Unité d'Organisation »

Vous pouvez ensuite répéter l'opération pour créer tous les utilisateurs dans leurs UO comme présenté dans l'organigramme !

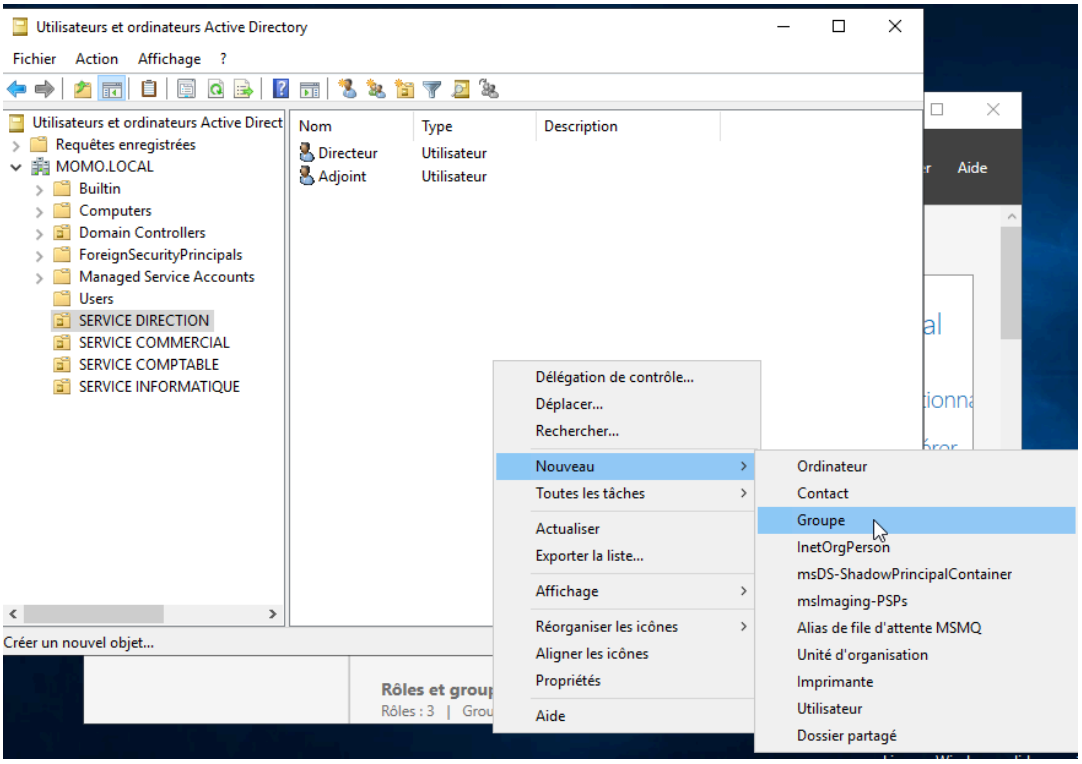
Étape 5 : Gestion des groupes d'utilisateurs

La création de groupes au sein des Unités d'Organisation (UO) est une pratique essentielle pour optimiser la gestion des accès et le partage de ressources au sein du réseau. En regroupant les utilisateurs par fonction ou par besoin métier, l'administration devient plus efficace, notamment lors de l'attribution de permissions sur des dossiers ou des applications.

Il est particulièrement simple de créer ces groupes au sein de vos UO et d'y intégrer les utilisateurs correspondants, facilitant ainsi la gestion centralisée des droits d'accès.

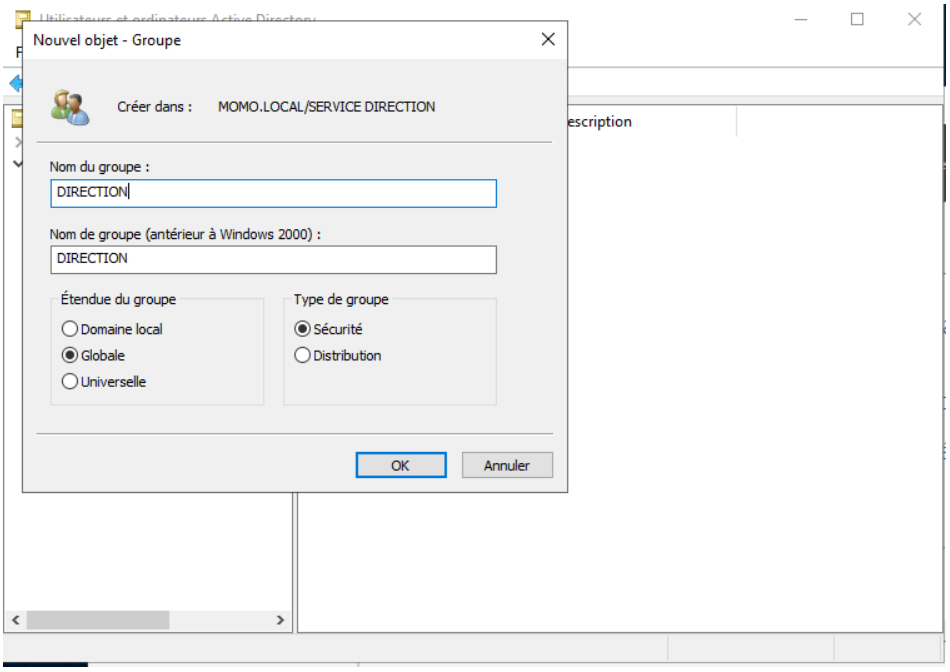
La création de groupes au sein d'une unité d'organisation permet de rationaliser l'administration des accès. La procédure est similaire à celle de la création d'utilisateurs :

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, effectuez un clic droit sur l'unité d'organisation ciblée (par exemple, SERVICE DIRECTION).
2. Pointez sur **Nouveau**, puis sélectionnez **Groupe**.



« Figure 26 : Procédure de création d'un groupe de sécurité dans une unité d'organisation »

1. Dans la fenêtre qui s'affiche, saisissez le **Nom du groupe**.
2. Conservez les paramètres par défaut pour l'étendue (Généralement « Global ») et le type de groupe (« Sécurité »), puis validez en cliquant sur **OK**.

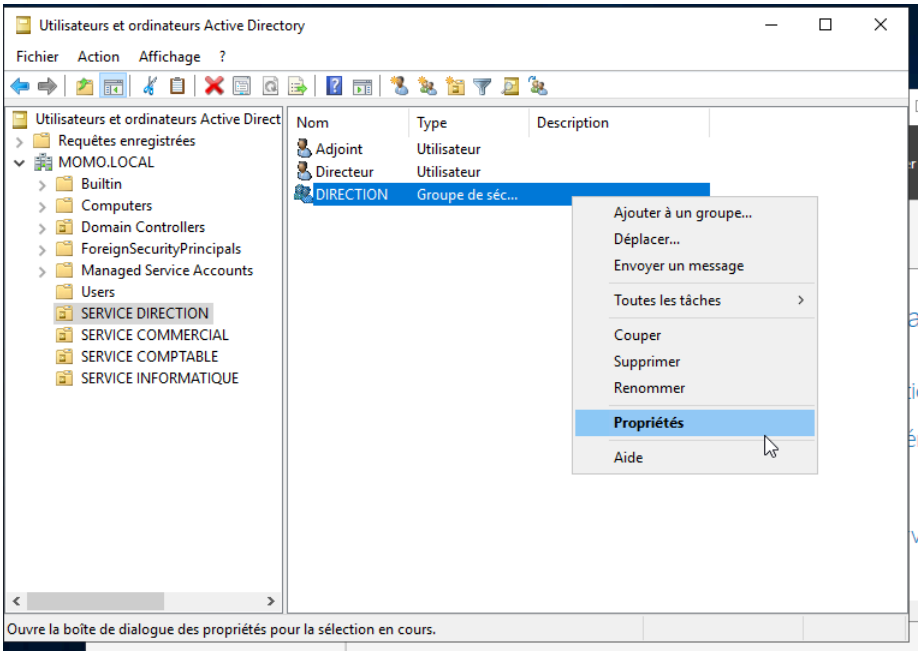


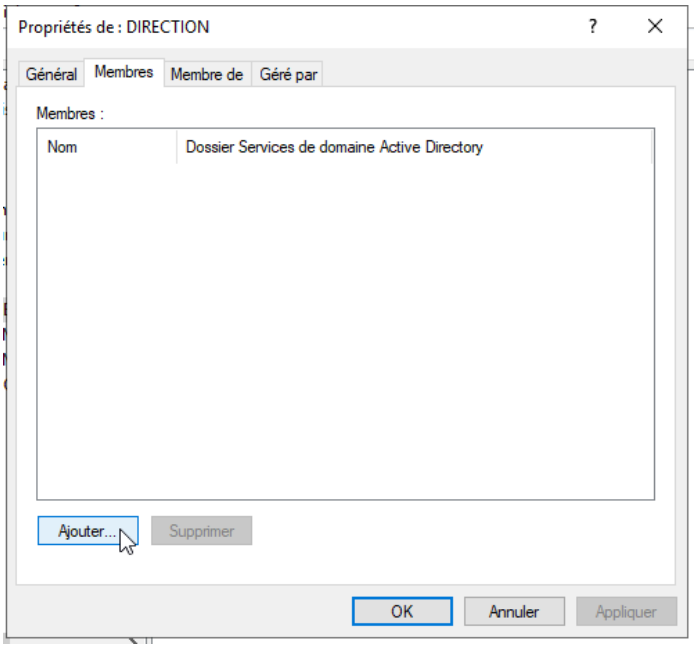
« Figure 27 : Création d'un nouveau groupe de sécurité »

Étape 7 : Ajout des membres au groupe

Une fois le groupe **DIRECTION** créé au sein de l'unité d'organisation correspondante, vous pouvez y intégrer les collaborateurs souhaités. Pour gérer la composition du groupe, procédez comme suit :

1. Effectuez un clic droit sur le groupe nouvellement créé.
2. Sélectionnez **Propriétés** dans le menu contextuel.

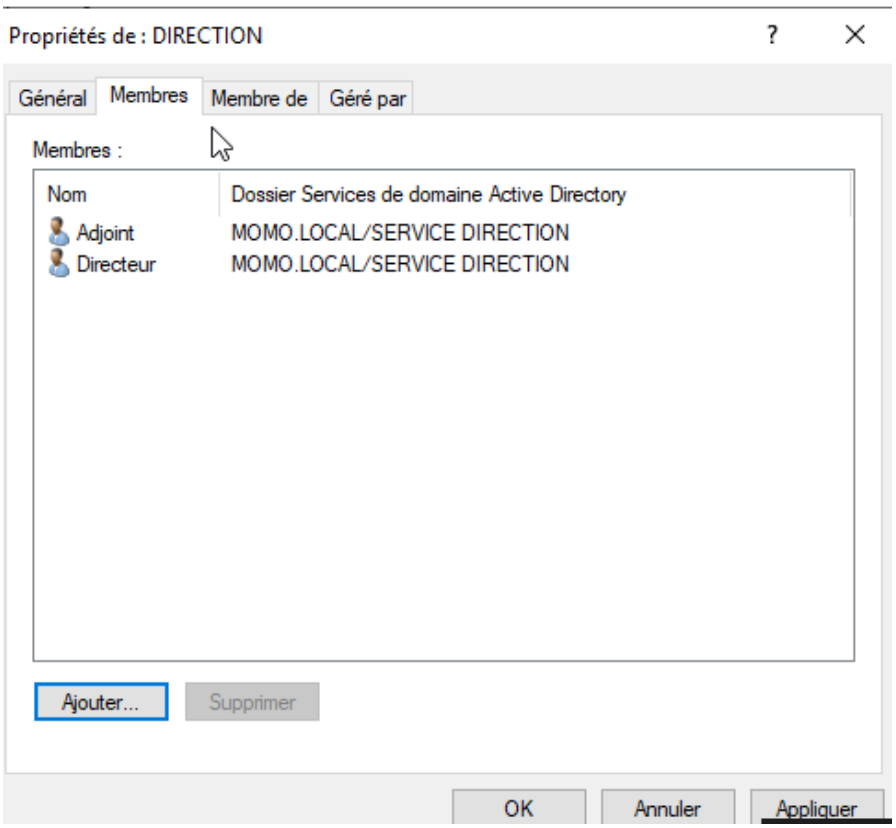




Cliquez sur **Ajouter**, saisissez le nom de l'utilisateur ou des utilisateurs que vous souhaitez intégrer, puis validez par **OK** pour l'intégrer dans le groupe sélectionné.

« Figure 28 : Ajout d'utilisateurs dans le groupe de sécurité »

Une fois que vous avez ajouté les utilisateurs souhaités, ceux-ci apparaissent désormais dans la liste de l'onglet **Membres**. Pour valider les modifications apportées à la composition du groupe, cliquez sur le bouton **Appliquer** situé en bas à droite de la fenêtre, puis sur **OK** pour fermer les propriétés. La configuration est alors immédiatement prise en compte par le contrôleur de domaine.



« Figure 29 : Confirmation de l'intégration des utilisateurs dans le groupe de sécurité »

Conclusion du Chapitre 2

Cette méthodologie peut être appliquée à l'ensemble des unités d'organisation et des utilisateurs prévus dans votre organigramme. En reproduisant ces étapes avec rigueur, vous garantissez la cohérence de votre arborescence Active Directory, assurant ainsi une administration structurée et évolutive de votre infrastructure. La base logique de votre domaine **MOMO.LOCAL** est désormais parfaitement établie et prête à supporter les futures configurations de sécurité et de déploiement.

Note : Bien que cette méthode manuelle soit idéale pour comprendre le fonctionnement de l'annuaire, elle peut devenir chronophage dans des contextes de déploiement massif. Pour une gestion industrielle, l'automatisation de la création d'objets (UO, utilisateurs, groupes) via des scripts PowerShell est fortement recommandée pour gagner en efficacité et réduire les risques d'erreurs humaines. Cette approche automatisée fera l'objet d'un chapitre complémentaire dédié dans ce laboratoire.

Fin du Chapitre 2.

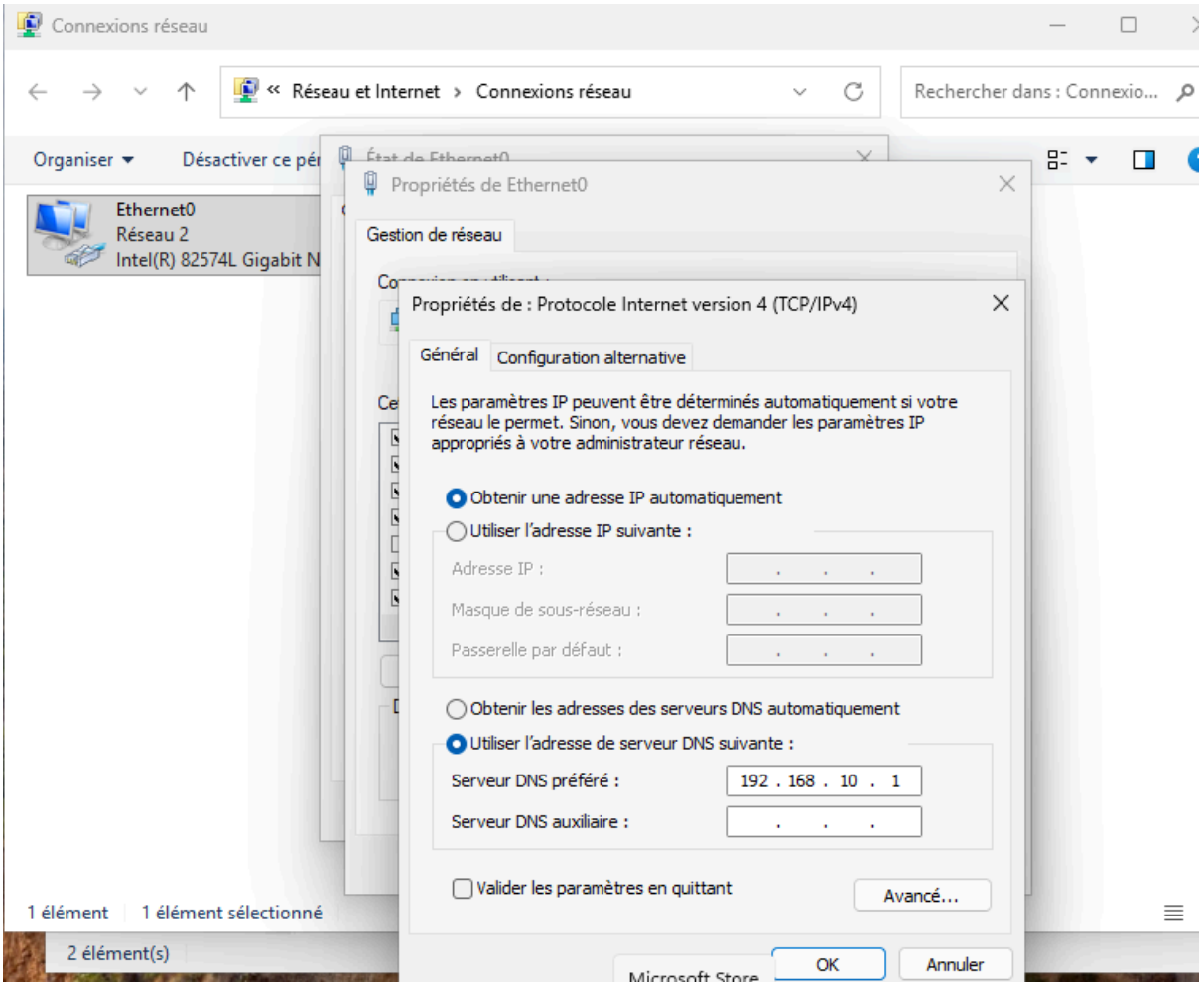
Boumrah Samy

Active Directory - Chapitre 3 : Intégrer Windows 11 Pro dans son Domaine

Cette étape consiste à joindre un poste client sous Windows 11 Pro à l'infrastructure Active Directory. Cette intégration permettra de bénéficier d'une gestion centralisée du poste et d'appliquer les politiques de groupe (GPO) définies sur le contrôleur de domaine.

Prérequis techniques

- **Installation du système :** Disposer d'une machine virtuelle équipée de l'édition **Windows 11 Professionnel**.
- **Configuration réseau :** Avant toute tentative de jonction, il est impératif que le poste client puisse communiquer avec le serveur. Assurez-vous que la configuration **DNS** de la carte réseau du client pointe exclusivement vers l'adresse IP de votre Windows Server (votre contrôleur de domaine).

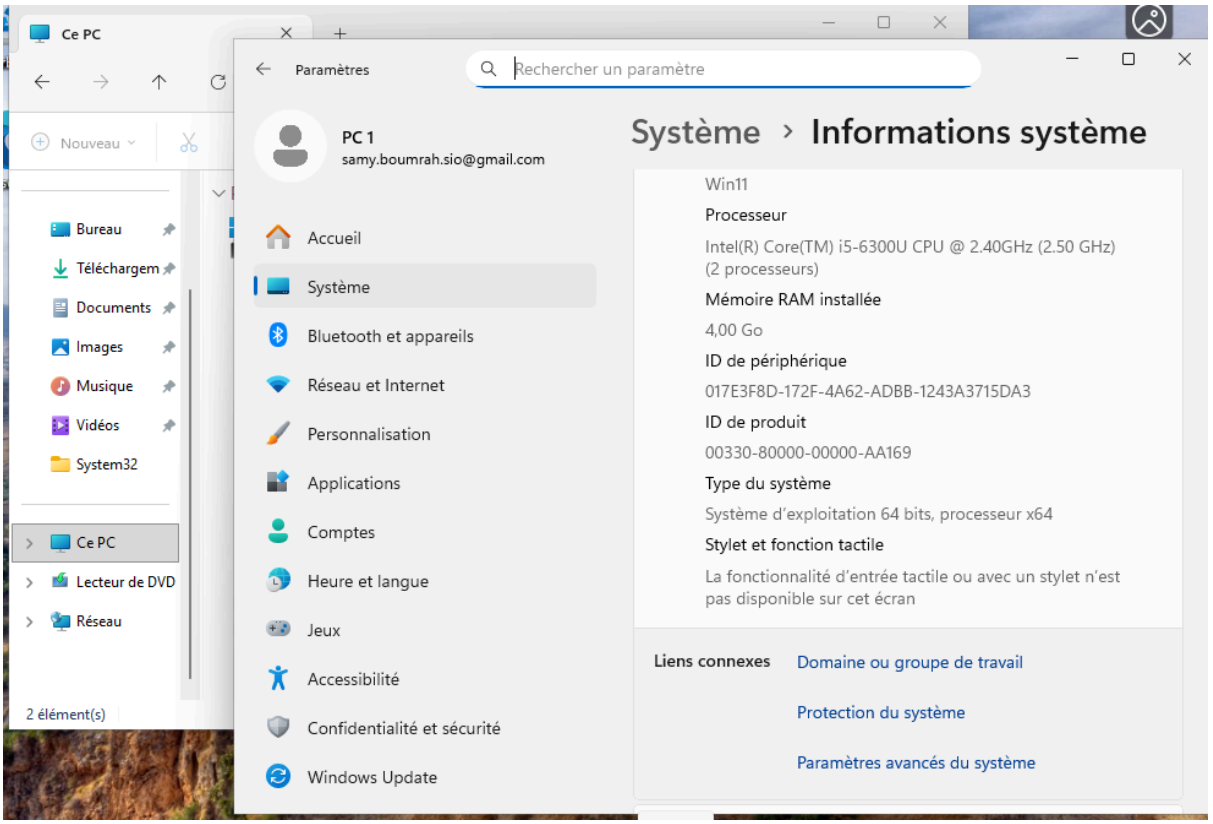


« Figure 30 : Configuration de l'adresse DNS du poste client ».

Étape 1 : Accès aux paramètres système

Une sur votre poste Windows 11 avec évidemment la configuration réseau validée, nous allons procéder à l'intégration du poste au domaine. Pour accéder aux paramètres d'identification de la machine, ouvrez l'explorateur de fichiers, effectuez un clic droit sur **Ce PC**, puis sélectionnez **Propriétés**.

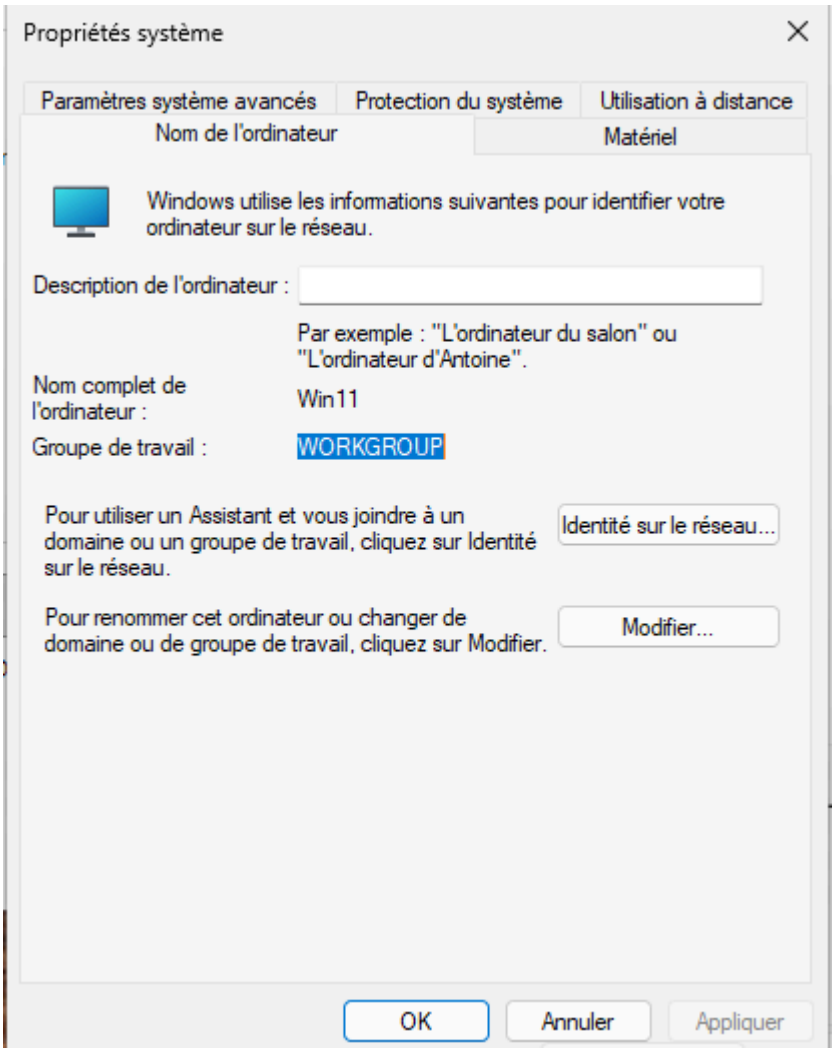
Cette manipulation vous permettra d'accéder à la page d'informations système affichée ci-dessous :



« Figure 31 : Accès aux propriétés du système pour la gestion du domaine »

Étape 2 : Configuration du domaine de rattachement

Sur la page des propriétés système, recherchez la section relative aux **liens connexes** ou aux **paramètres avancés** pour accéder à la gestion du domaine. Cliquez sur le lien **Domaine ou groupe de travail** (ou sur **Renommer ce PC (avancé)** selon votre version de Windows), ce qui ouvrira une nouvelle fenêtre contextuelle intitulée « Propriétés système ».



« Figure 32 : Ouverture de la boîte de dialogue Propriétés système pour la jonction au domaine »

Étape 3 : Jonction au domaine

Dans la fenêtre « Propriétés système » qui s'est ouverte, vous constaterez que votre poste est actuellement membre du groupe de travail par défaut (**WORKGROUP**).

Pour intégrer le poste au domaine Active Directory :

1. Cliquez sur le bouton **Modifier**.
2. Dans la section **Membre de**, sélectionnez l'option **Domaine**.
3. Saisissez le nom de votre domaine racine (dans notre cas, **MOMO.LOCAL**), puis cliquez sur **OK**.

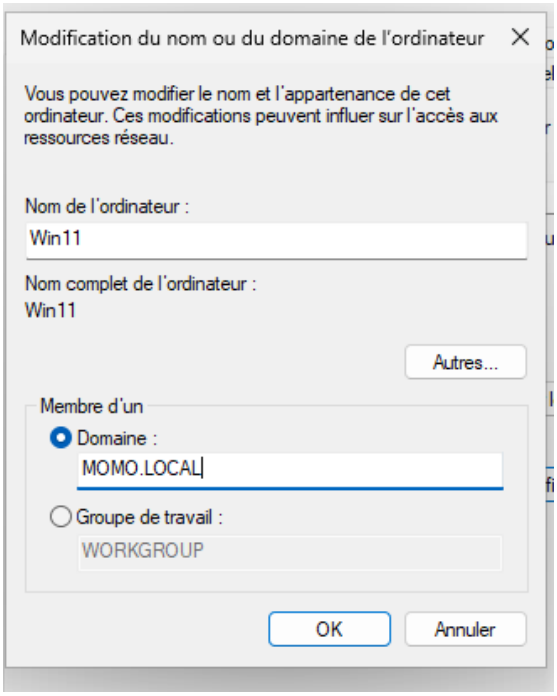
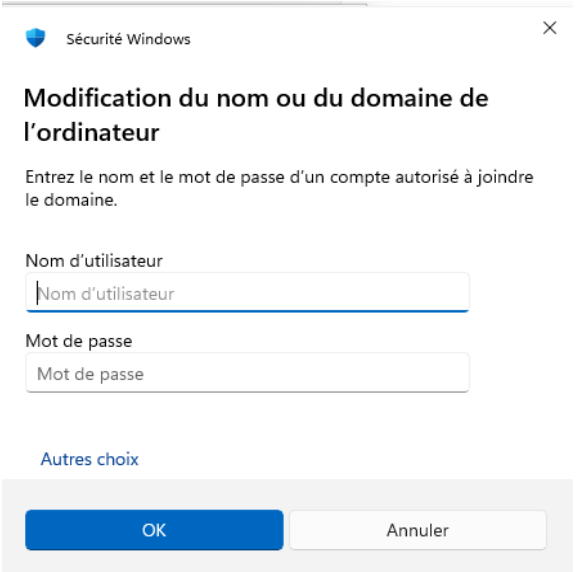


Figure 33 : Configuration de la jonction au domaine MOMO.LOCAL ».

Étape 4 : Authentification et finalisation

Une fois le nom du domaine saisi, une fenêtre d'authentification s'ouvrira. Vous devrez alors renseigner les identifiants d'un compte disposant des droits nécessaires (tel que votre compte administrateur du domaine créé précédemment) pour valider l'intégration.



Si la procédure est correctement configurée, un message de bienvenue confirmera la réussite de l'opération après quelques secondes : **« Bienvenue dans le domaine MOMO.LOCAL ».**

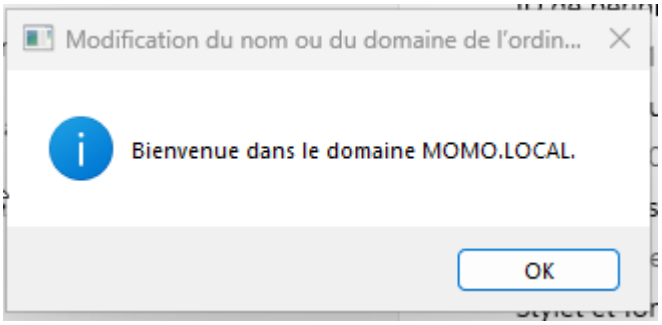
Note : En cas d'erreur de connexion, vérifiez systématiquement que votre poste client communique bien avec le serveur DNS et que l'adresse IP du serveur est correctement configurée en tant que serveur DNS préféré sur votre interface réseau.

« Figure 34 : Confirmation de l'intégration réussie dans le domaine »

Étape 5 : Finalisation de la jonction

Une fois vos identifiants renseignés, le système procède à la validation de la jonction au domaine **MOMO.LOCAL**. Si la configuration est correcte, une fenêtre contextuelle de confirmation, telle que celle illustrée ci-dessous, apparaîtra après quelques secondes, vous souhaitant la bienvenue dans le domaine.

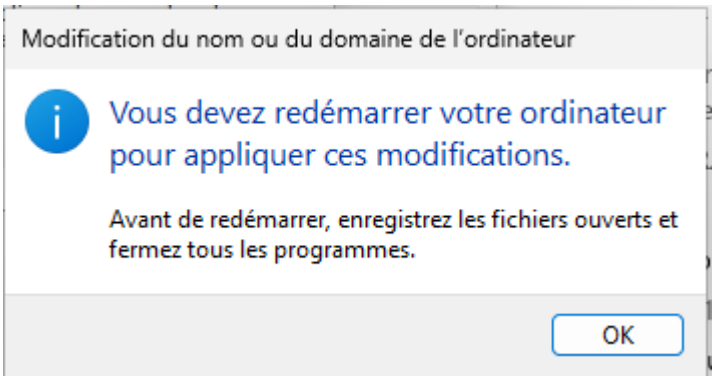
Il est alors impératif de **redémarrer votre poste client** pour finaliser l'intégration et appliquer les changements de stratégie de sécurité. Lors de la prochaine ouverture de session, vous pourrez sélectionner **« Autre utilisateur »** pour vous connecter avec n'importe quel compte utilisateur préalablement créé dans votre Active Directory.



« Figure 35 : Confirmation du message de bienvenue dans le domaine MOMO.LOCAL ».

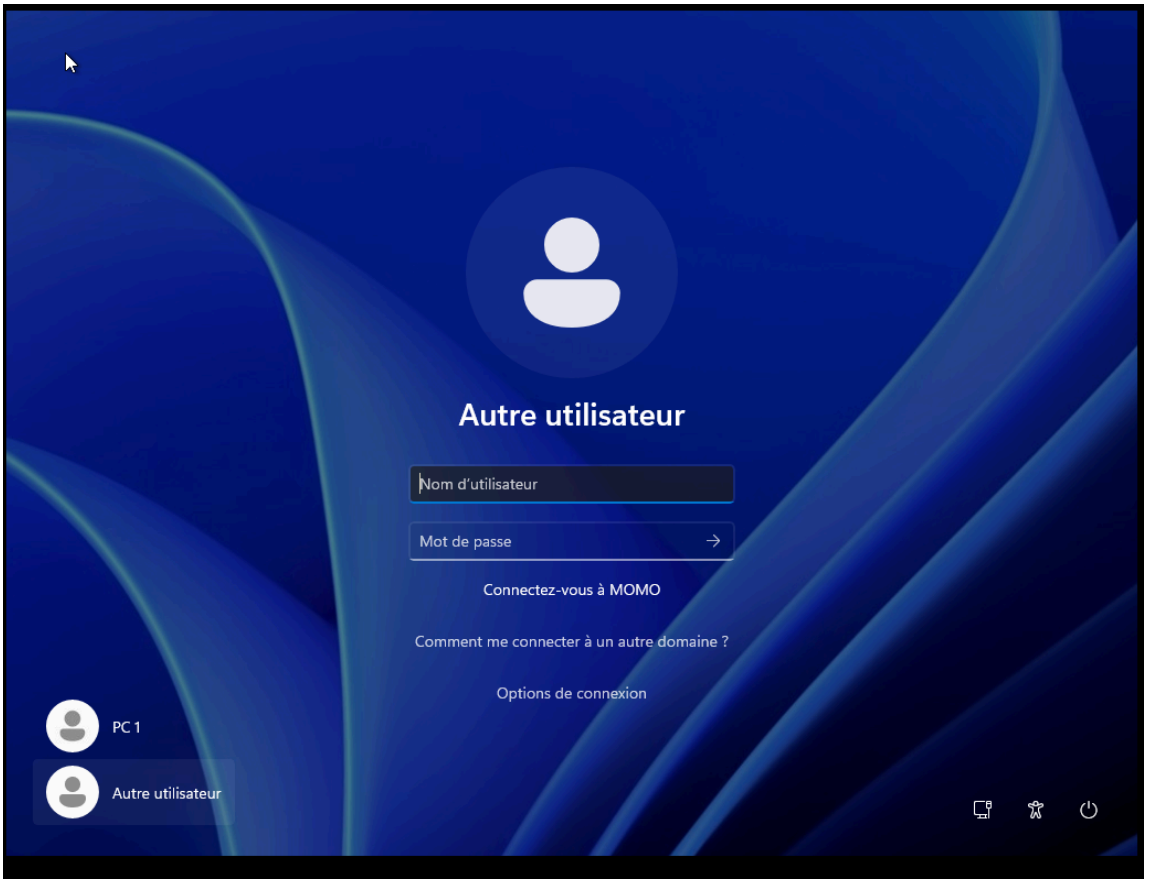
Étape 6 : Redémarrage final

Une fois le message de bienvenue validé, le système vous notifiera qu'un redémarrage est impératif pour finaliser l'application des modifications. Cliquez sur **OK** pour accepter le redémarrage, puis fermez les fenêtres de configuration restantes.



« Figure 36 : Notification système invitant au redémarrage pour finaliser l'intégration ».

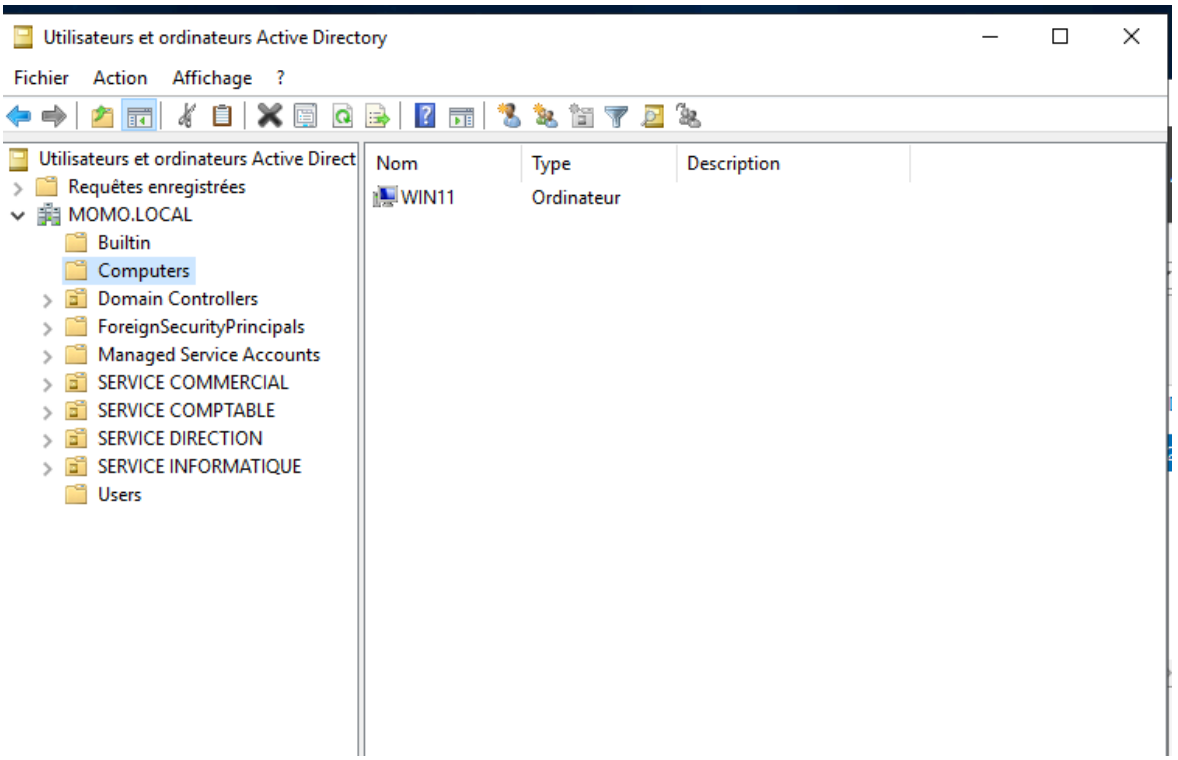
Lors de la prochaine séquence de démarrage, Windows 11 reconnaîtra son appartenance au domaine **MOMO.LOCAL** et vous invitera à vous connecter en utilisant les identifiants de votre compte de domaine.



Étape 7 : Vérification côté serveur

Une fois la session ouverte avec un compte utilisateur du domaine sur votre poste client, vous pouvez confirmer l'intégration depuis votre contrôleur de domaine **Windows Server 2022**.

Dans la console **Utilisateurs et ordinateurs Active Directory**, développez le conteneur **Computers** (ou l'Unité d'Organisation dans laquelle vous avez potentiellement déplacé l'objet). Vous devriez y voir apparaître le nom de votre machine **Windows 11**. La présence de cet objet confirme que la machine est correctement enregistrée et authentifiée au sein du domaine **MOMO.LOCAL**.



« Figure 37 : Confirmation de l'objet ordinateur dans la console AD ».

Conclusion du Chapitre 3

L'intégration de votre poste client Windows 11 au domaine est désormais effective. Cette étape marque une avancée majeure, car elle permet désormais de gérer ce poste de manière centralisée, de déployer des politiques de groupe et de sécuriser l'accès aux ressources du réseau via des comptes utilisateurs nominatifs. Votre infrastructure client-serveur est maintenant fonctionnelle.

Fin du Chapitre 3.

Boumrah Samy

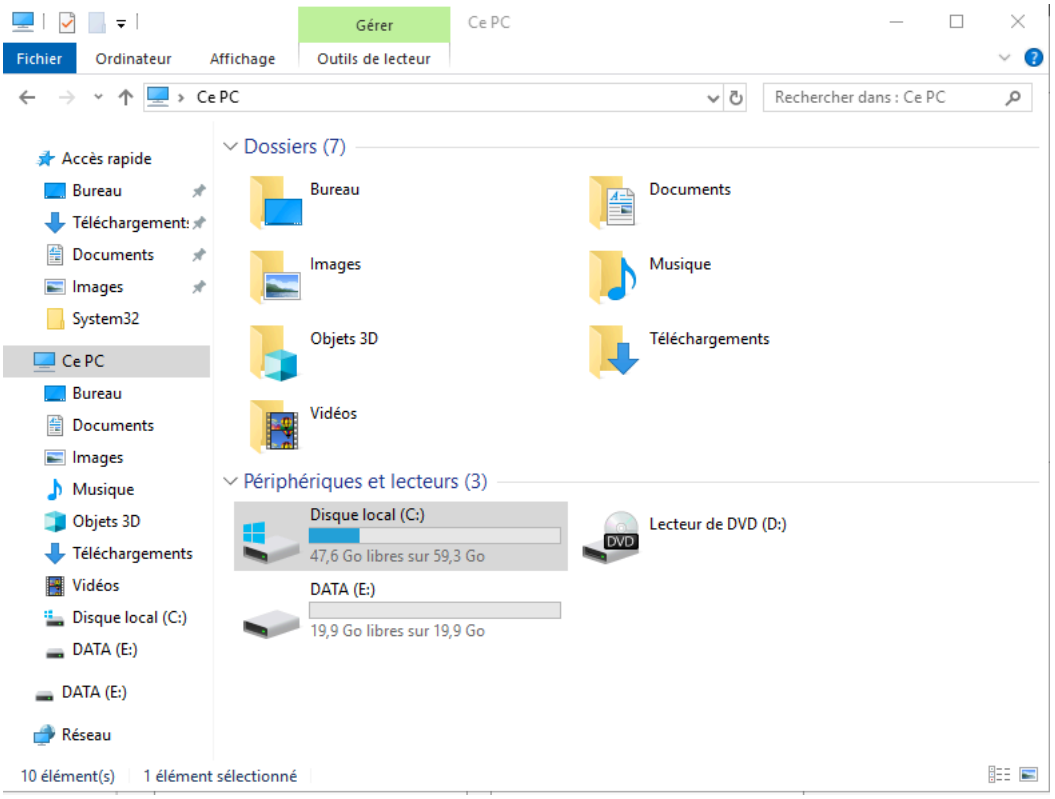
Active Directory - Chapitre 4 Connecter des lecteurs réseau avec stratégie GPO

Une fois l'annuaire Active Directory structuré et les comptes utilisateurs opérationnels, l'étape suivante consiste à mettre en place des lecteurs réseau. Cette solution permet de centraliser le stockage des données professionnelles sur le serveur, offrant ainsi une meilleure sécurisation et une sauvegarde facilitée des informations, tout en évitant le stockage local sur les postes clients, souvent plus vulnérables.

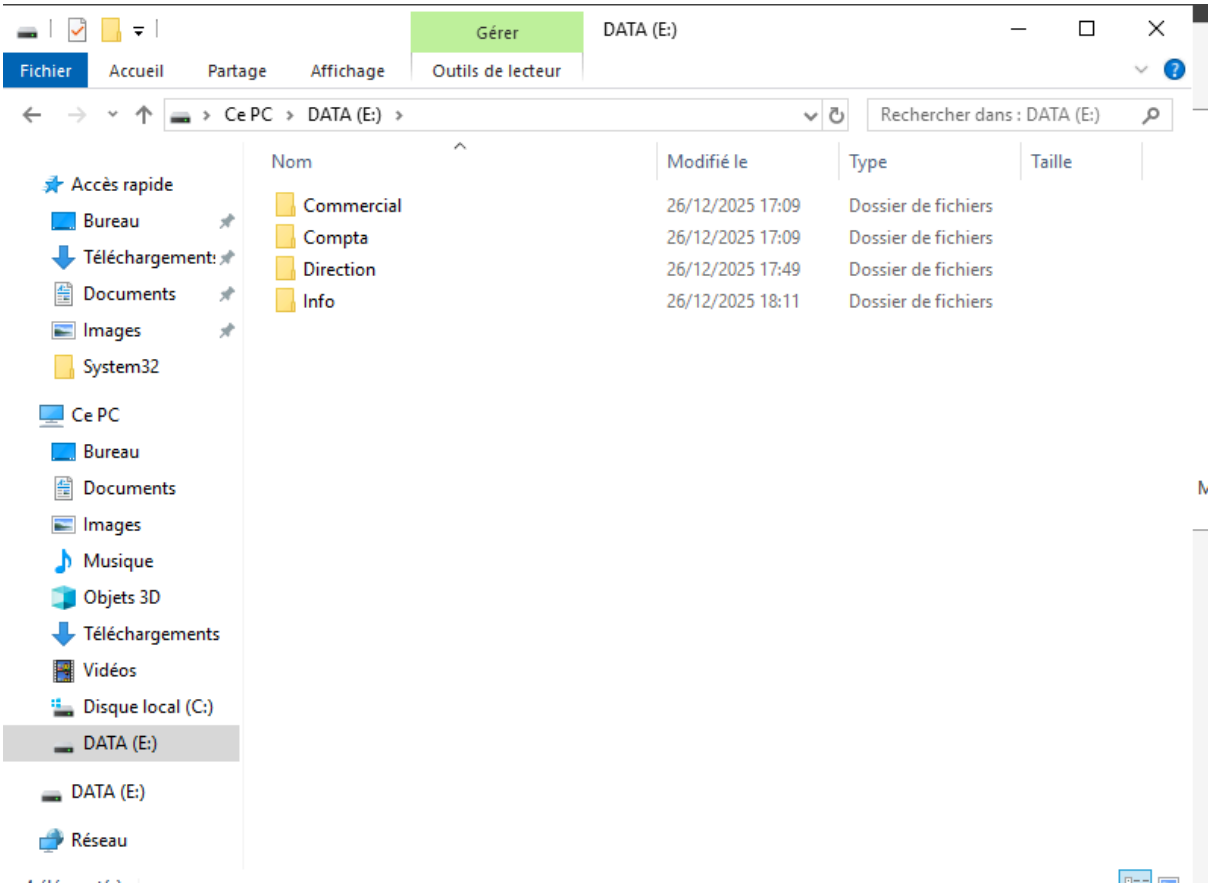
Étape 1 : Préparation de l'espace de stockage

La configuration s'effectue directement depuis votre serveur Windows hébergeant le service Active Directory.

- **Initialisation du volume de données :** Si un disque dédié (ex: disque DATA) n'est pas encore présent, éteignez la machine virtuelle et ajoutez un nouveau disque dur virtuel via les paramètres de la VM. Une fois redémarré, initialiser et formater ce disque via l'outil « Gestion des disques » (clic droit sur le menu Démarrer > Gestion des disques).



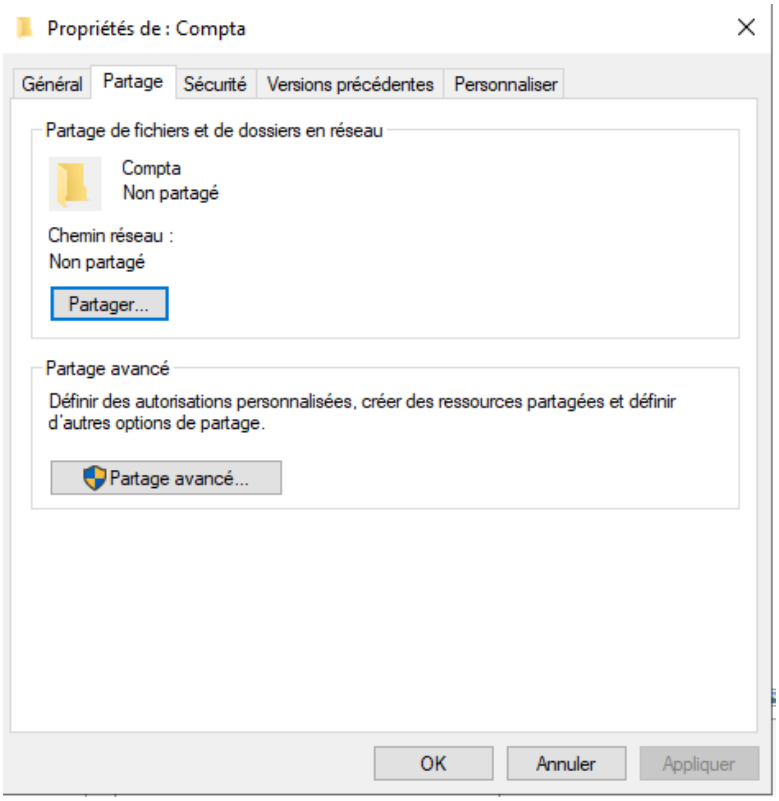
- **Création des répertoires :** Une fois le volume prêt, créez à la racine du disque les dossiers destinés à chaque service (ex: `\Direction`, `\Commercial`, etc.) qui accueilleront les données des utilisateurs.



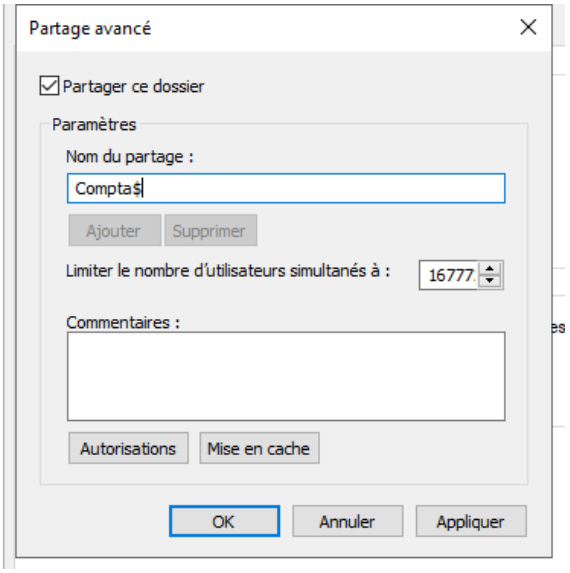
« Figure 38 : Préparation des répertoires de données sur le volume dédié »

Étape 2 : Autorisations de partage

Dans l'onglet **Partage** des propriétés du dossier, cliquez sur **Partage avancé** afin d'accéder aux paramètres détaillés du partage réseau. Dans la fenêtre qui s'affiche, cochez l'option **Partager ce dossier** pour activer la mise à disposition du répertoire sur le réseau.



Dans la fenêtre qui s'affiche, cochez l'option **Partager ce dossier** pour activer la mise à disposition du répertoire sur le réseau.

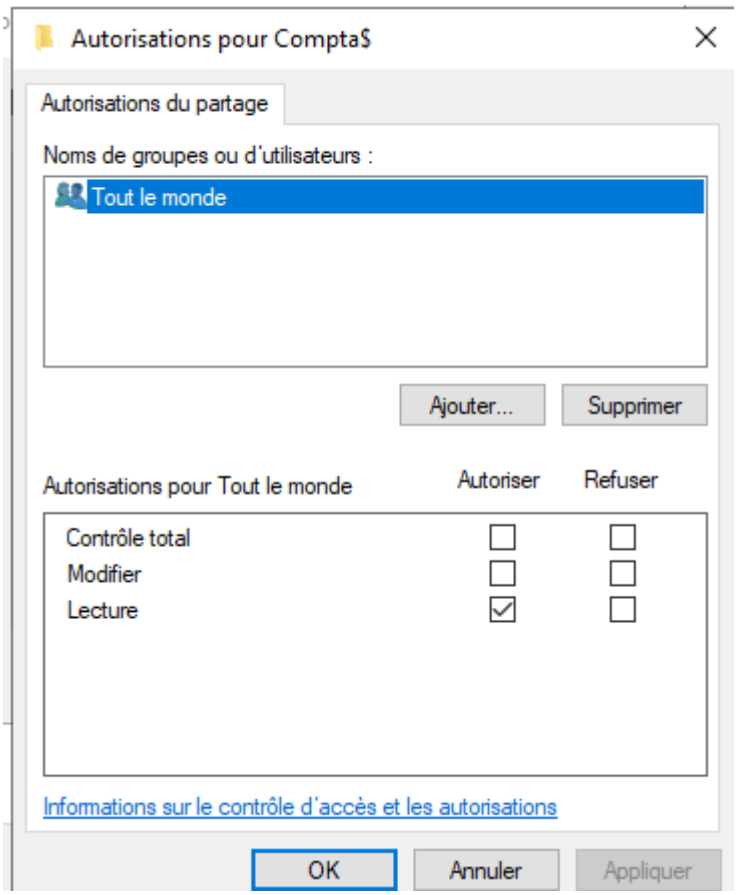


Afin de masquer ce partage aux utilisateurs lors de la navigation réseau, ajoutez le caractère **$** à la fin du nom du partage. Cette convention permet de créer un partage caché, accessible uniquement si l'on connaît son nom exact.

« Figure 40 : Activation du partage avancé et création d'un partage caché ».

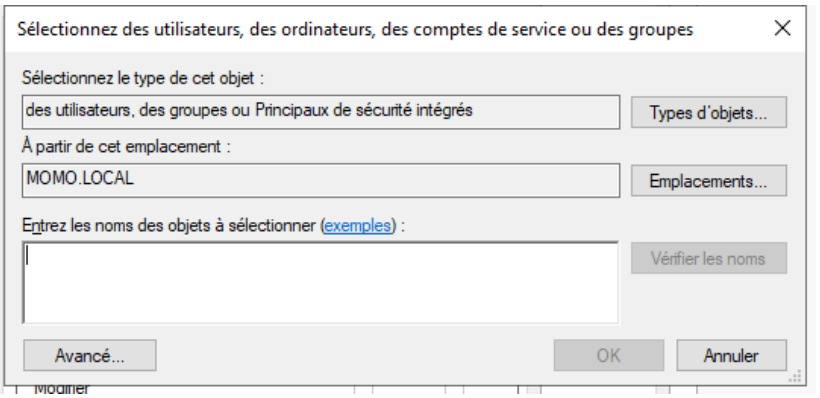
Étape 3 : Configuration des autorisations de partage

Dans la fenêtre des autorisations de partage, vous remarquerez que le groupe **Tout le monde** est généralement présent par défaut. Afin de restreindre l'accès au partage de manière plus précise et plus sécurisée, nous allons supprimer cette autorisation.



« Figure 40 : Suppression du groupe Tout le monde des autorisations de partage ».

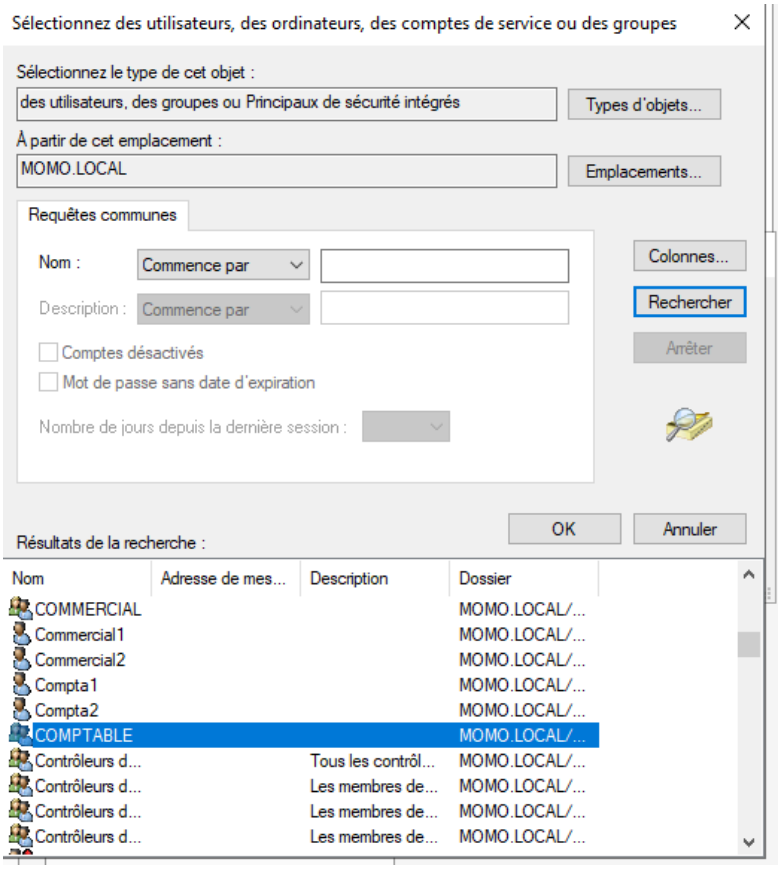
On clique donc ensuite sur ajouter et une nouvelle fenêtre va s'ouvrir. Nous pourrons ensuite ajouter uniquement les groupes ou utilisateurs concernés par l'accès à ce dossier.



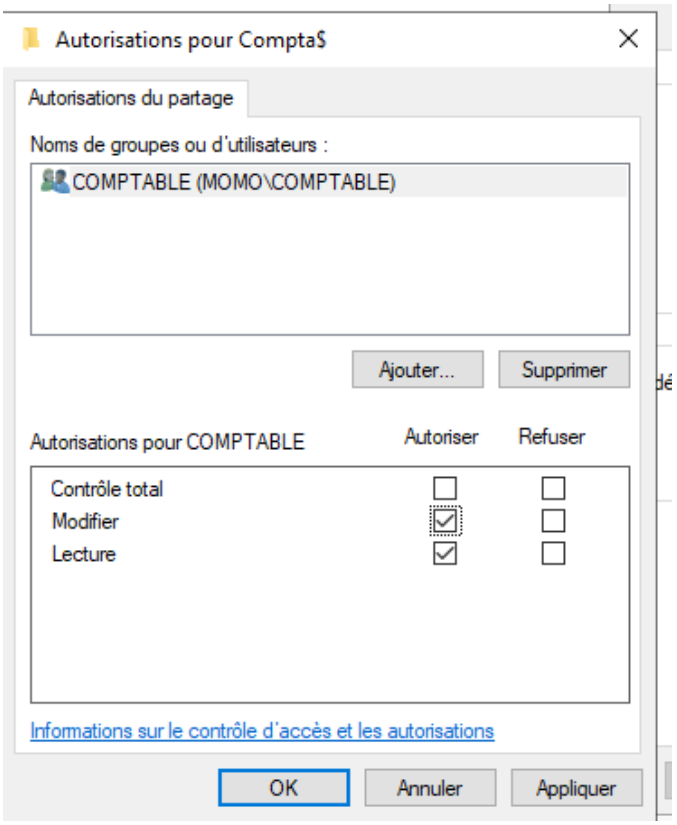
Étape 4 : Attribution des autorisations au groupe

Pour simplifier l'administration des accès, nous attribuons les droits non pas à chaque utilisateur individuellement, mais à un **groupe de sécurité**. Dans mon cas, je sélectionne le groupe **COMPTABLE**, car il regroupe les utilisateurs concernés par le lecteur réseau du service comptabilité. Ainsi, tous les membres de ce groupe, comme **Compta1** et **Compta2**, hériteront automatiquement des mêmes autorisations.

Une fois le groupe ajouté, il suffit de définir ses permissions sur le partage concerné, puis de valider les modifications en cliquant sur **Appliquer** et **OK**.

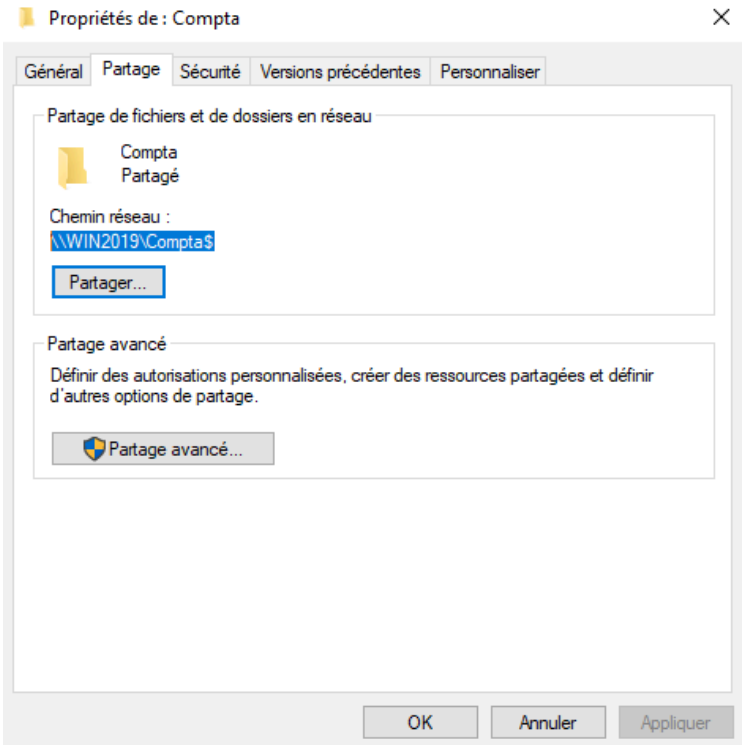


« Figure 41 : Attribution des droits de partage au groupe COMPTABLE ».



Étape 5 : Récupération du chemin réseau

Une fois les modifications appliquées et validées par **OK**, vous revenez à la fenêtre précédente, où Windows affiche le chemin réseau du partage créé. Il est conseillé de copier ce chemin, car il servira ultérieurement lors du mappage du lecteur réseau sur les postes clients.

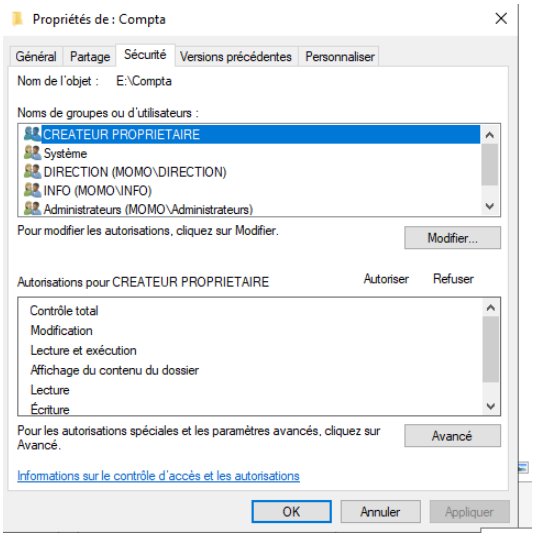


« Figure 42 : Affichage du chemin réseau du dossier partagé ».

Étape 6 : Configuration de la sécurité NTFS

Nous allons maintenant configurer les autorisations **NTFS** afin de contrôler précisément l'accès au dossier partagé. Cette étape est essentielle, car elle permet de restreindre l'accès aux seuls utilisateurs ou groupes autorisés, tout en empêchant les comptes non concernés d'accéder aux données du service.

Contrairement aux permissions de partage, les permissions NTFS s'appliquent directement au système de fichiers et offrent un contrôle plus fin sur les accès aux dossiers et sous-dossiers.



Après avoir cliqué sur l'onglet sécurité du fichiers, on peut directement continué sur l'option **paramètres avancé** ce qui nous amènera ici :

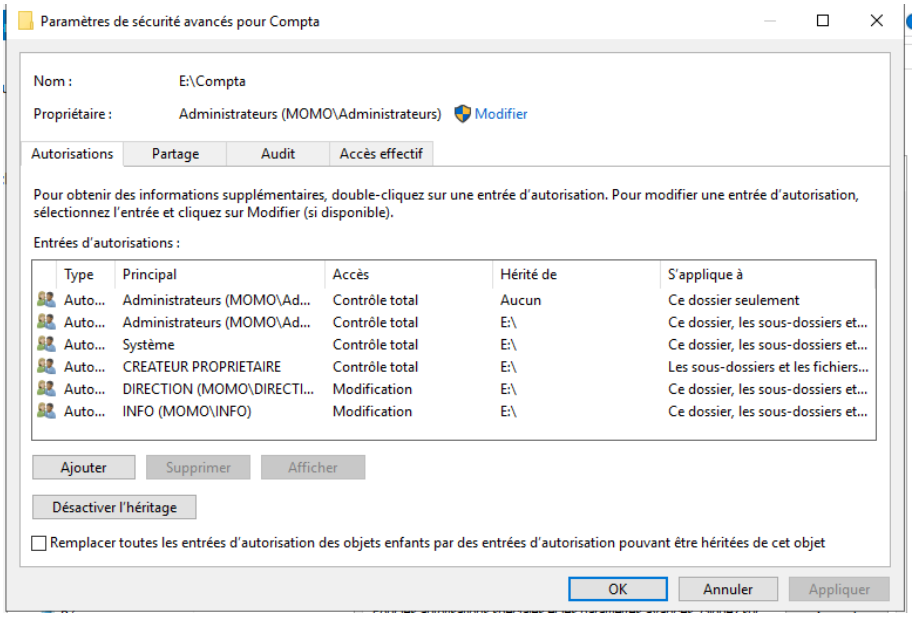
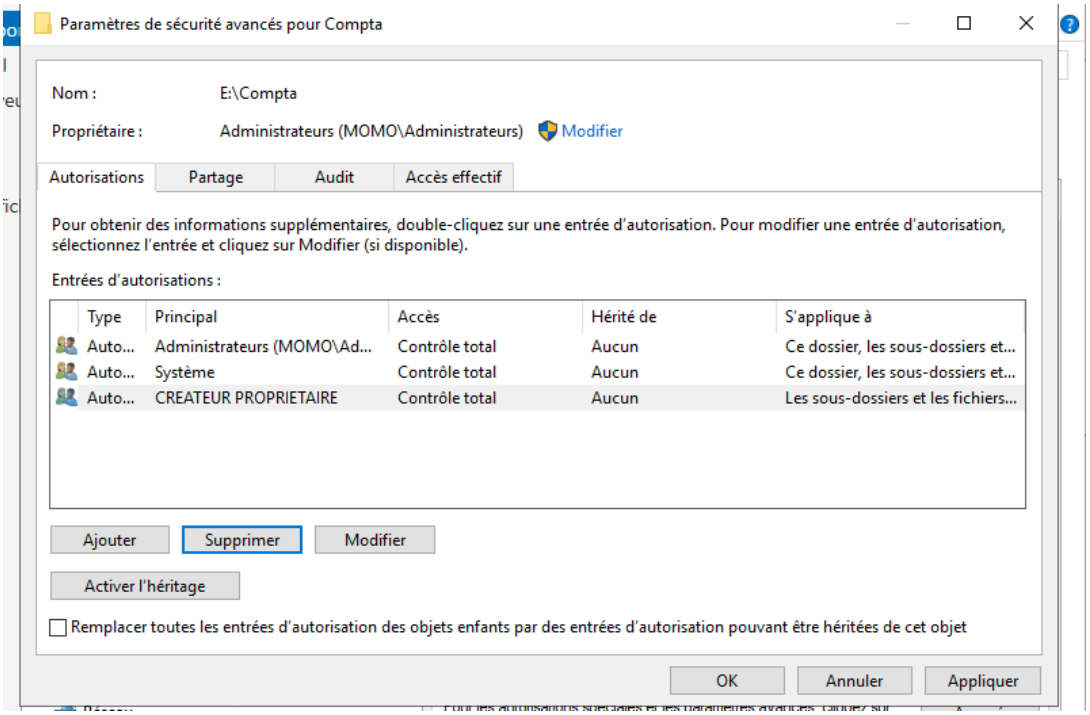


Figure 43 : Configuration des autorisations NTFS du dossier partagé ».

Étape 7 : Désactivation de l'héritage

Par défaut, le dossier hérite de plusieurs autorisations provenant du système ou du répertoire parent. Afin de maîtriser précisément les droits d'accès, nous allons **désactiver l'héritage** puis choisir l'option **Convertir les autorisations héritées en autorisations explicites**. Cela permet de conserver la base existante tout en gardant le contrôle sur les accès attribués.

Une fois cette opération effectuée, nous pourrons supprimer les groupes ou utilisateurs qui ne sont pas nécessaires afin de ne conserver que les autorisations utiles à notre configuration.



« Figure 44 : Désactivation de l'héritage des autorisations NTFS ».

Nous allons maintenant ajouter le groupe de sécurité correspondant au service concerné. Dans mon cas, je sélectionne le groupe **COMPTABLE**, puisque ce partage est destiné au dossier de la comptabilité. L'intérêt d'utiliser un groupe est simple : tous les utilisateurs membres de ce groupe, comme **Compta1** et **Compta2**, hériteront automatiquement des mêmes droits d'accès.

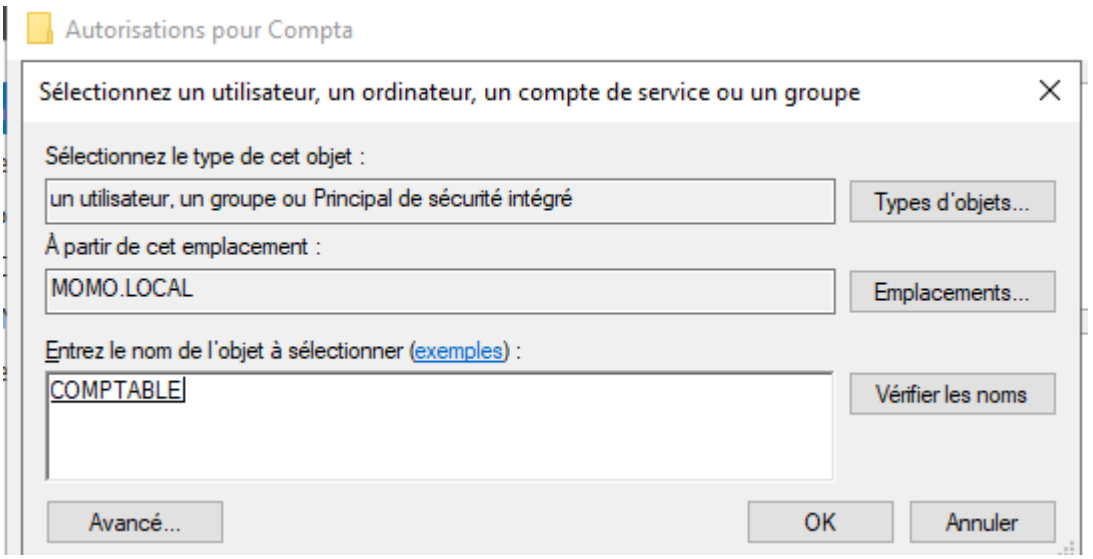
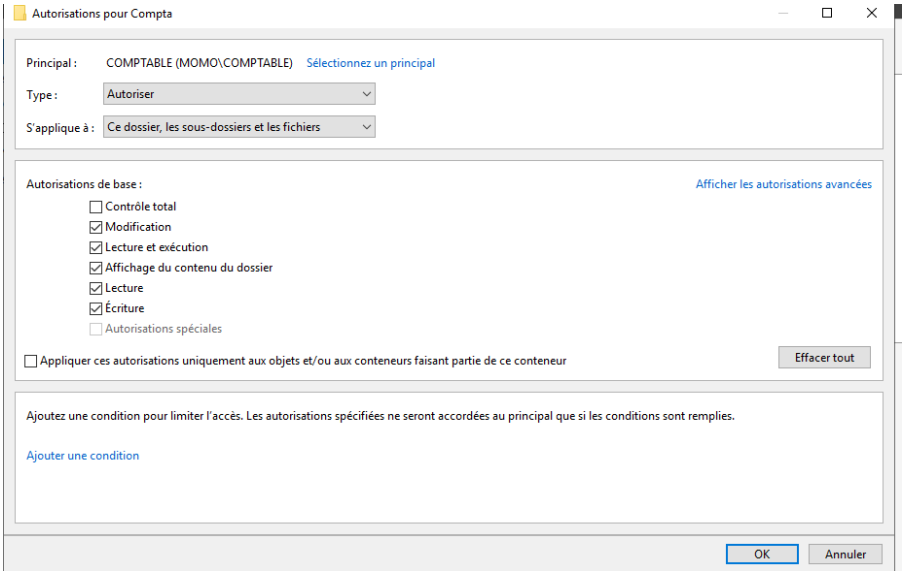


Figure 45 : Ajout du groupe COMPTABLE aux autorisations NTFS ».

Cliquez sur **Ajouter**, puis sur **Sélectionnez un principal** afin de rechercher et sélectionner à nouveau le groupe souhaité. Une fois le groupe trouvé et validé, vous pourrez lui attribuer les autorisations nécessaires, puis cliquer sur **Appliquer** et **OK** pour enregistrer la configuration.



« Figure 46 : Validation finale des autorisations NTFS pour le groupe COMPTABLE ».

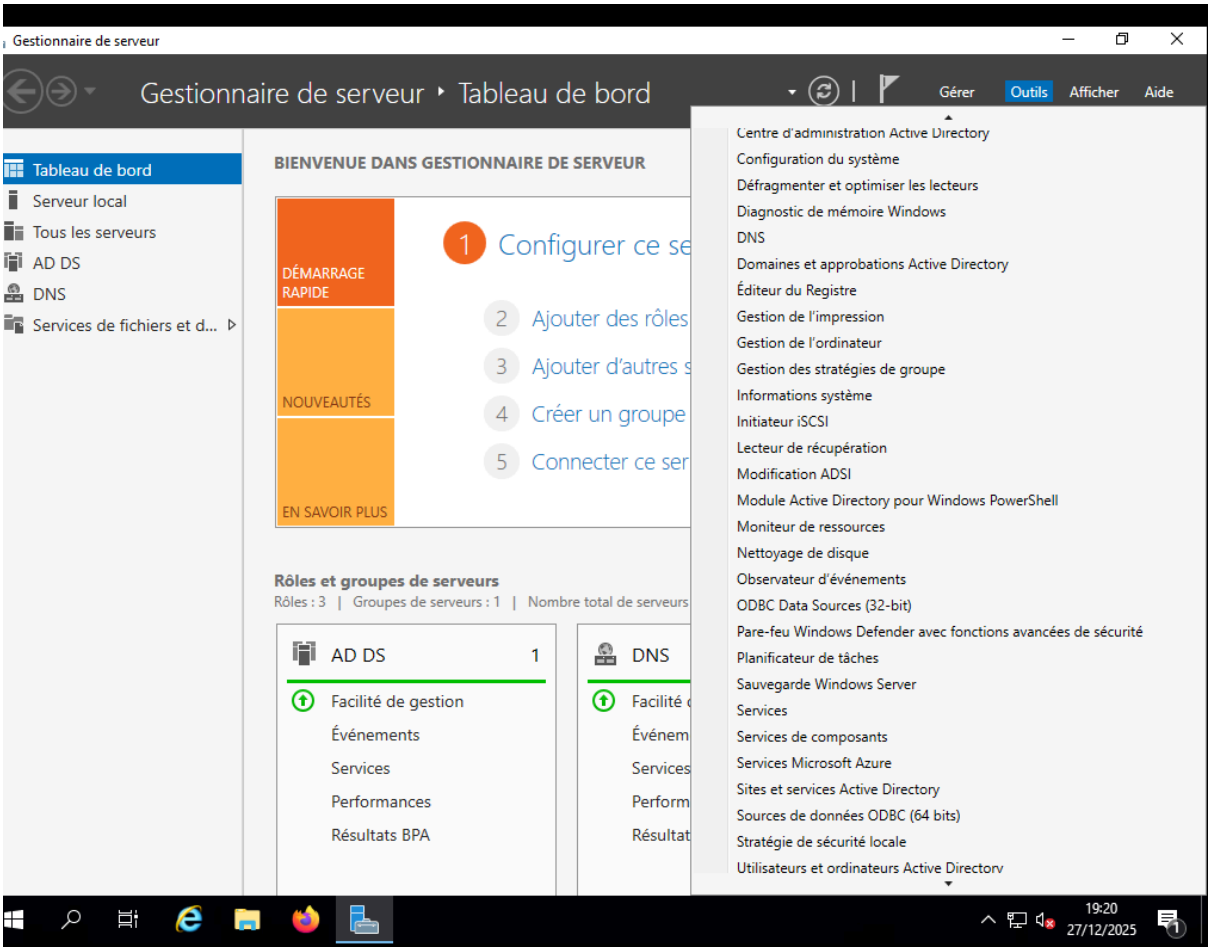
Une fois le groupe ajouté, il apparaît dans la liste des **entrées d'autorisations**. Il ne reste plus qu'à valider la configuration en cliquant sur **Appliquer**, puis sur **OK** pour enregistrer les changements.

Cette étape permet de finaliser les droits attribués au dossier partagé et de sécuriser l'accès selon les besoins définis au préalable.

Étape 8 : Création de l’objet de stratégie de groupe

Une fois la structure des dossiers partagés mise en place, nous pouvons créer l’objet de stratégie de groupe qui servira à déployer automatiquement le lecteur réseau sur les postes clients.

Pour cela, ouvrez le **Gestionnaire de serveur**, puis accédez à **Outils** et sélectionnez **Gestion des stratégies de groupe**. Cette console, également appelée **GPMC**, permet de créer, modifier et lier des objets de stratégie de groupe (GPO) au sein du domaine.

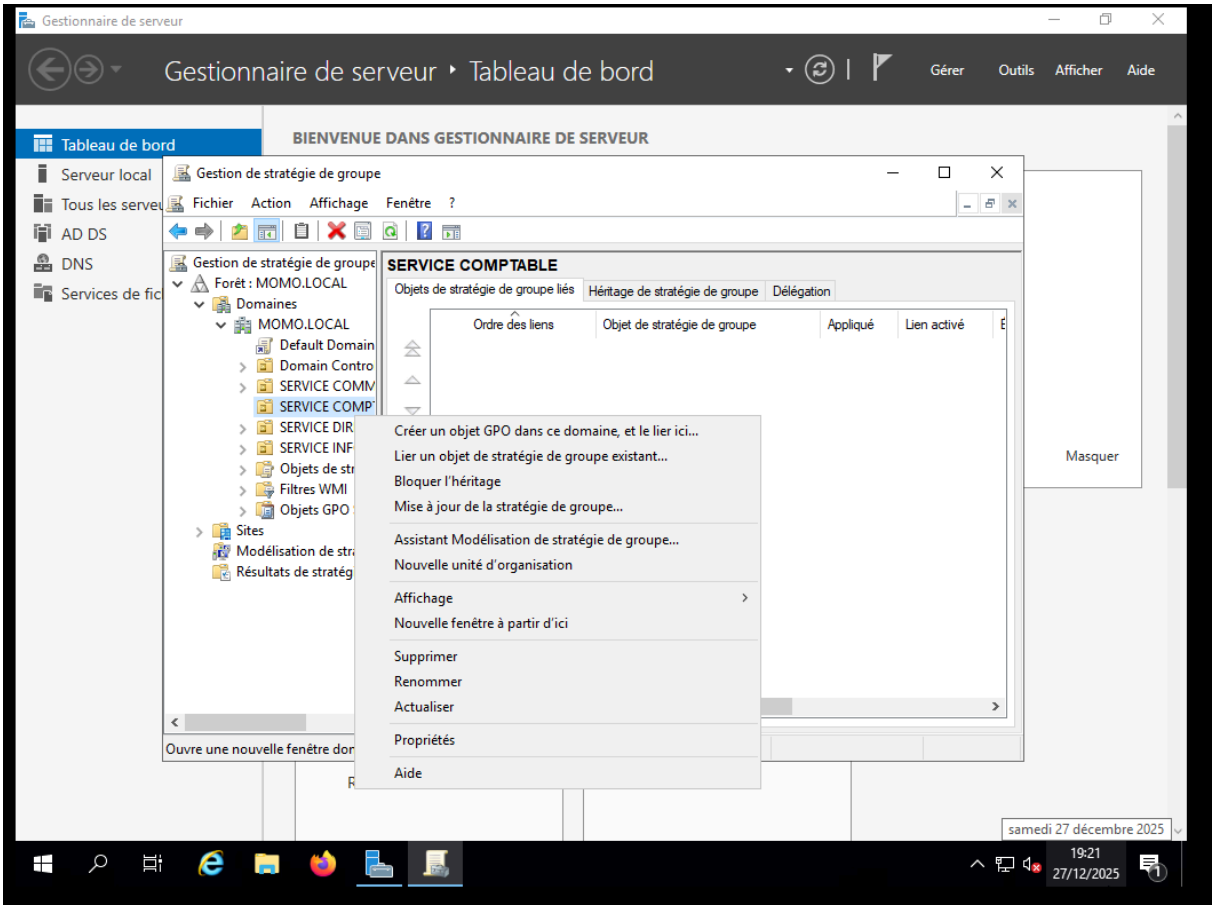


« Figure 47 : Accès à la console de gestion des stratégies de groupe (GPMC) »

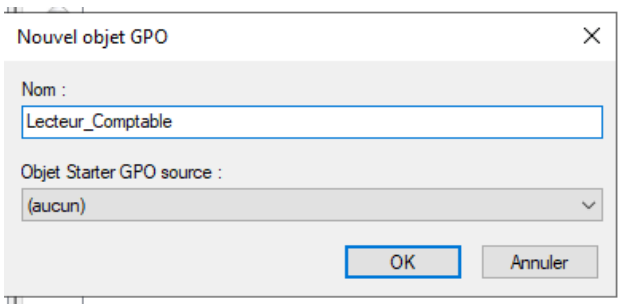
Étape 9 : Création et liaison de la GPO

Dans la console **Gestion des stratégies de groupe**, développez votre forêt puis votre domaine afin d'afficher les unités d'organisation créées précédemment. Effectuez ensuite un clic droit sur l'**UO** concernée, puis sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici**. Cette action permet de créer simultanément l'objet de stratégie de groupe et de l'associer directement à l'unité d'organisation ciblée.

Une fenêtre de création s'ouvre alors afin de vous permettre de nommer la stratégie en fonction de son usage, par exemple pour le déploiement d'un lecteur réseau.

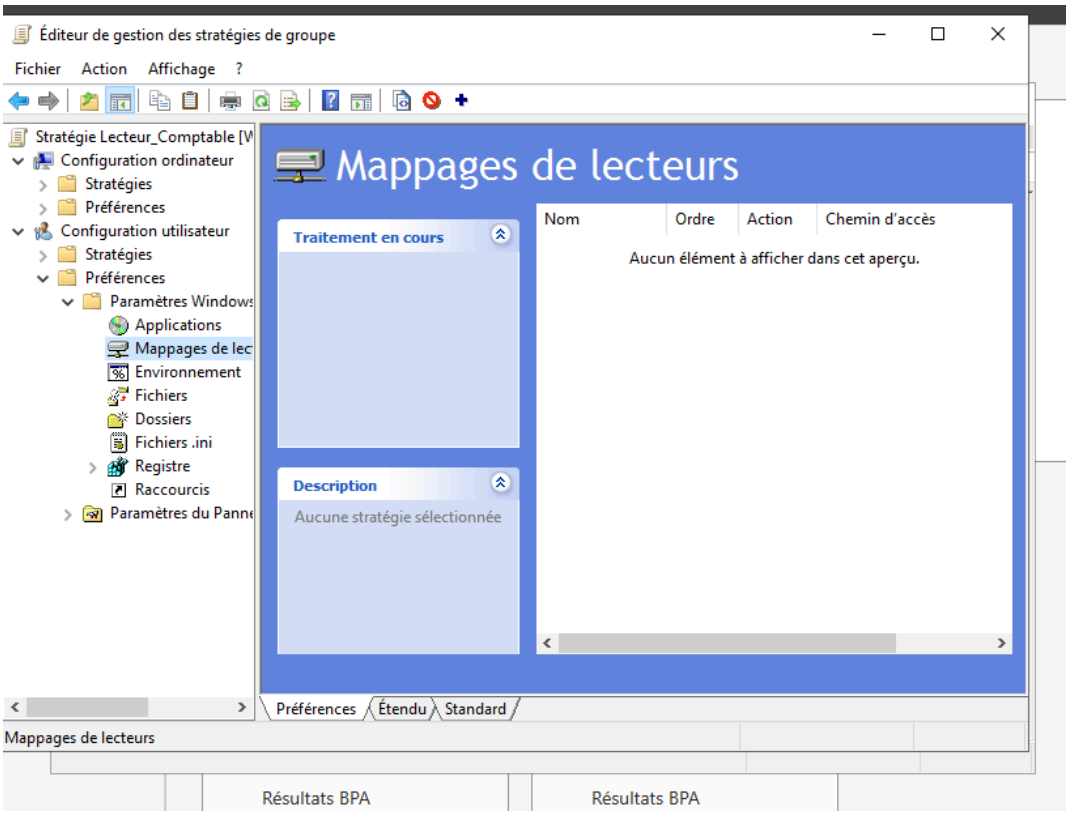


« Figure 48 : Création et liaison d'une GPO à une unité d'organisation ».



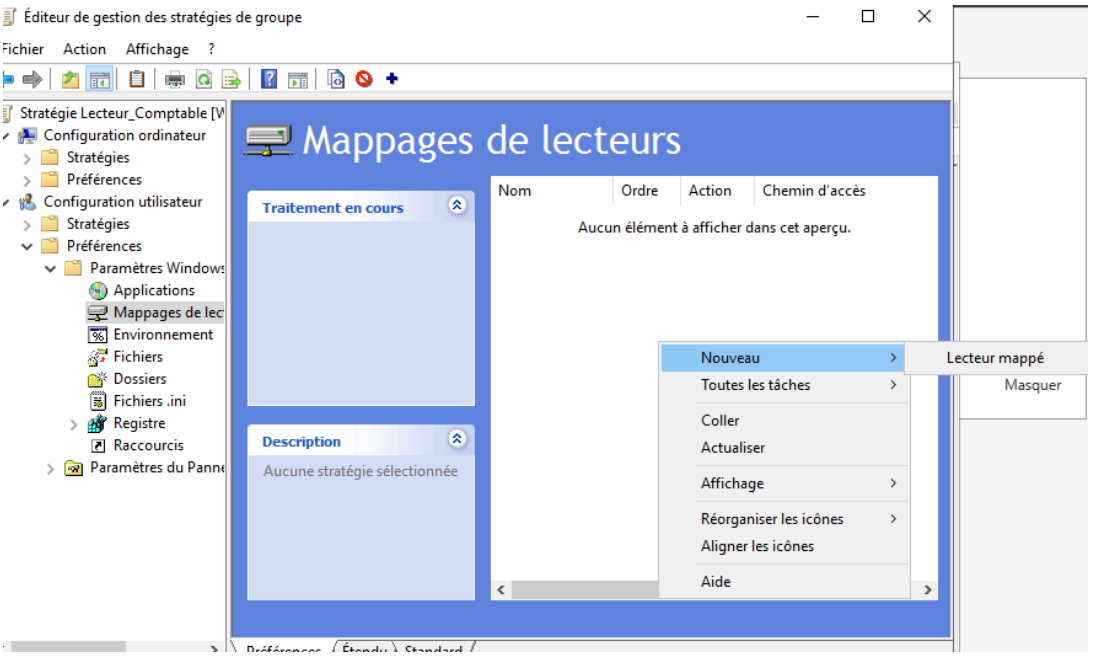
Une fois la fenêtre de création affichée, nous choisissons un nom pour la nouvelle GPO. Dans notre cas, nous la nommons **Lecteur_Comptable**, puis nous validons en cliquant sur **OK**.

L'objet apparaît ensuite sous votre **UO** ; effectuez alors un clic droit dessus, puis choisissez **Modifier**. Dans la fenêtre d'édition de la GPO, rendez-vous dans **Préférences**, puis **Paramètres Windows**, et enfin **Mappages de lecteurs**.

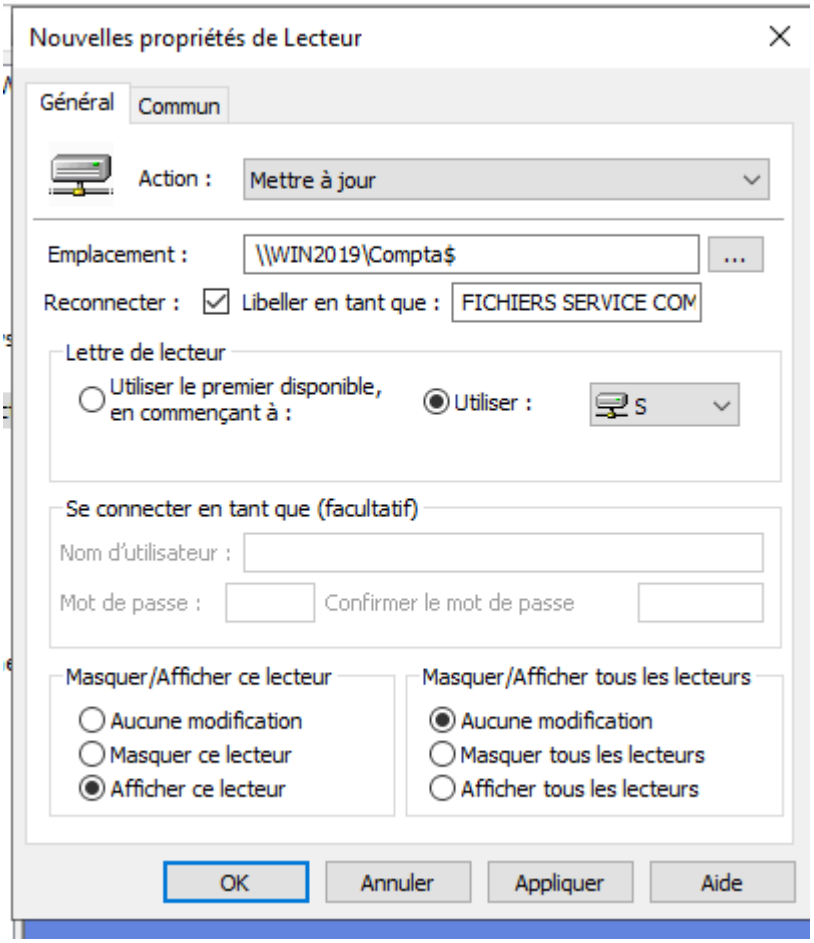


« Figure 49 : Mappages de lecteurs à l'aide d'une GPO ».

Clique droit dans la partie blanche a droite => Nouveau => Lecteur mappé



Une nouvelle page apparaît, dans laquelle vous pouvez renseigner l'emplacement du lecteur. Il suffit d'y coller le **chemin réseau** copié précédemment dans le champ prévu à cet effet.

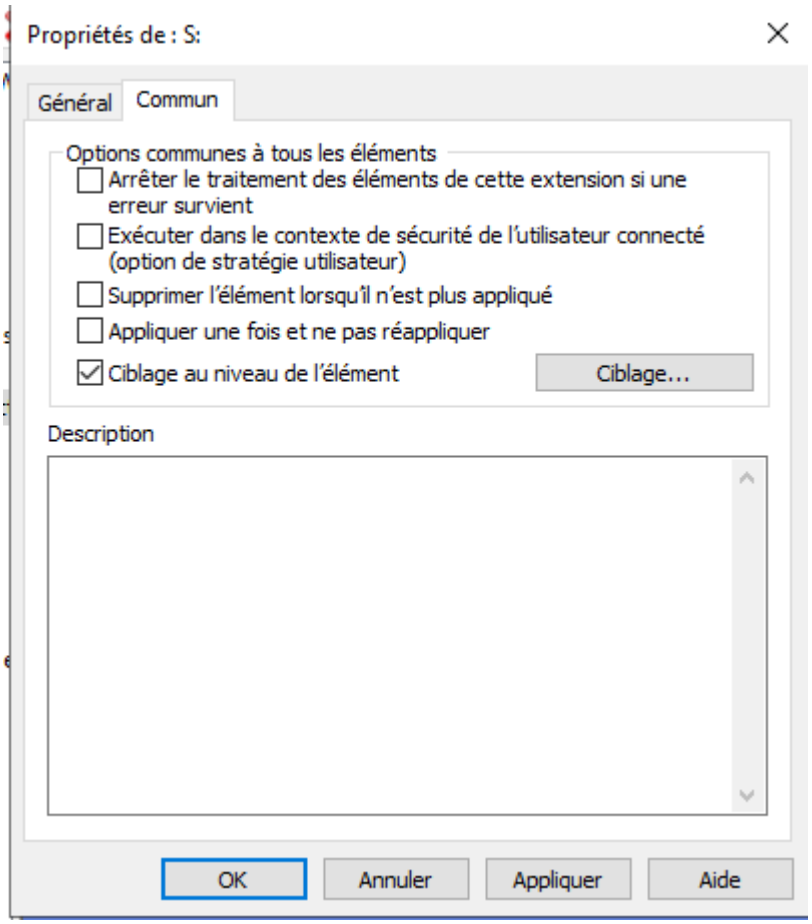


Vous pouvez cocher la case **Reconnecter** afin que le lecteur soit restauré à chaque ouverture de session. Dans le champ de libellé, nous renseignons **FICHIERS SERVICE COMPTABLE**, puis nous sélectionnons une lettre de lecteur choisie manuellement, en privilégiant une lettre basse dans l'alphabet pour éviter tout conflit avec d'autres lecteurs réseau.

« Figure 50: Paramétrage du lecteur réseau via la GPO ».

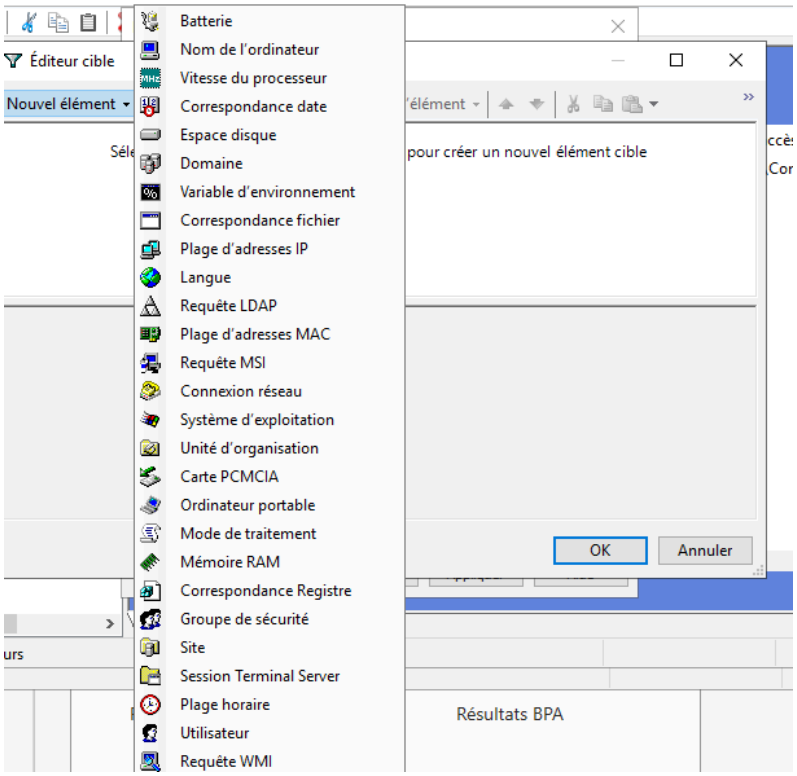
Une fois ces premiers paramètres renseignés, le lecteur peut être affiché puis valider en cliquant sur **Appliquer**.

On se dirige ensuite dans l'onglet **Commun** et on coche la case **Ciblage au niveau de l'élément** afin de cibler uniquement notre groupe **COMPTABLE**. Cette option permet de restreindre l'application du mappage aux utilisateurs concernés seulement.

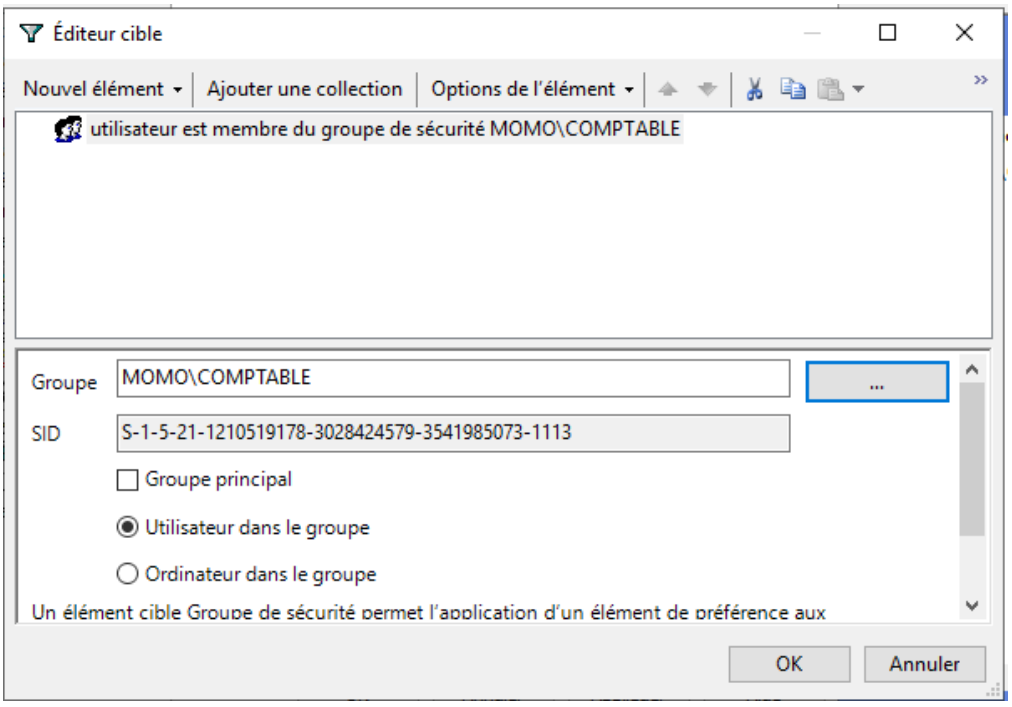


« Figure 51 : Activation du ciblage au niveau de l'élément pour le groupe COMPTABLE »

Dans la fenêtre de ciblage, cliquez sur **Nouvel élément**, puis sur **Groupe de sécurité**.



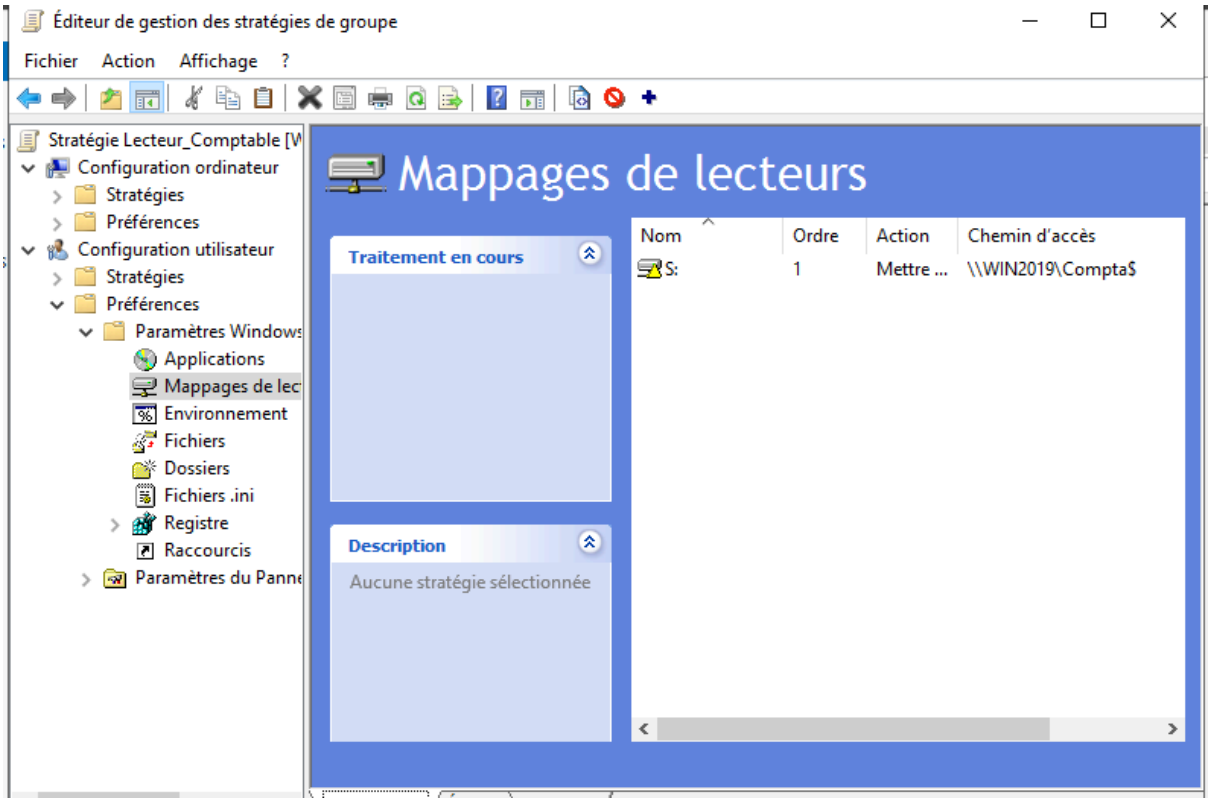
Une nouvelle page s'ouvre alors : cliquez sur les **trois points** pour parcourir l'annuaire, puis sur **Avancé** afin d'accéder à la recherche Active Directory. Vous pouvez ensuite cliquer sur **Rechercher** et sélectionner le groupe **COMPTABLE**, ou bien saisir directement son nom dans le champ prévu à cet effet.



« Figure 52 : Sélection du groupe de sécurité COMPTABLE dans le ciblage de l'élément »

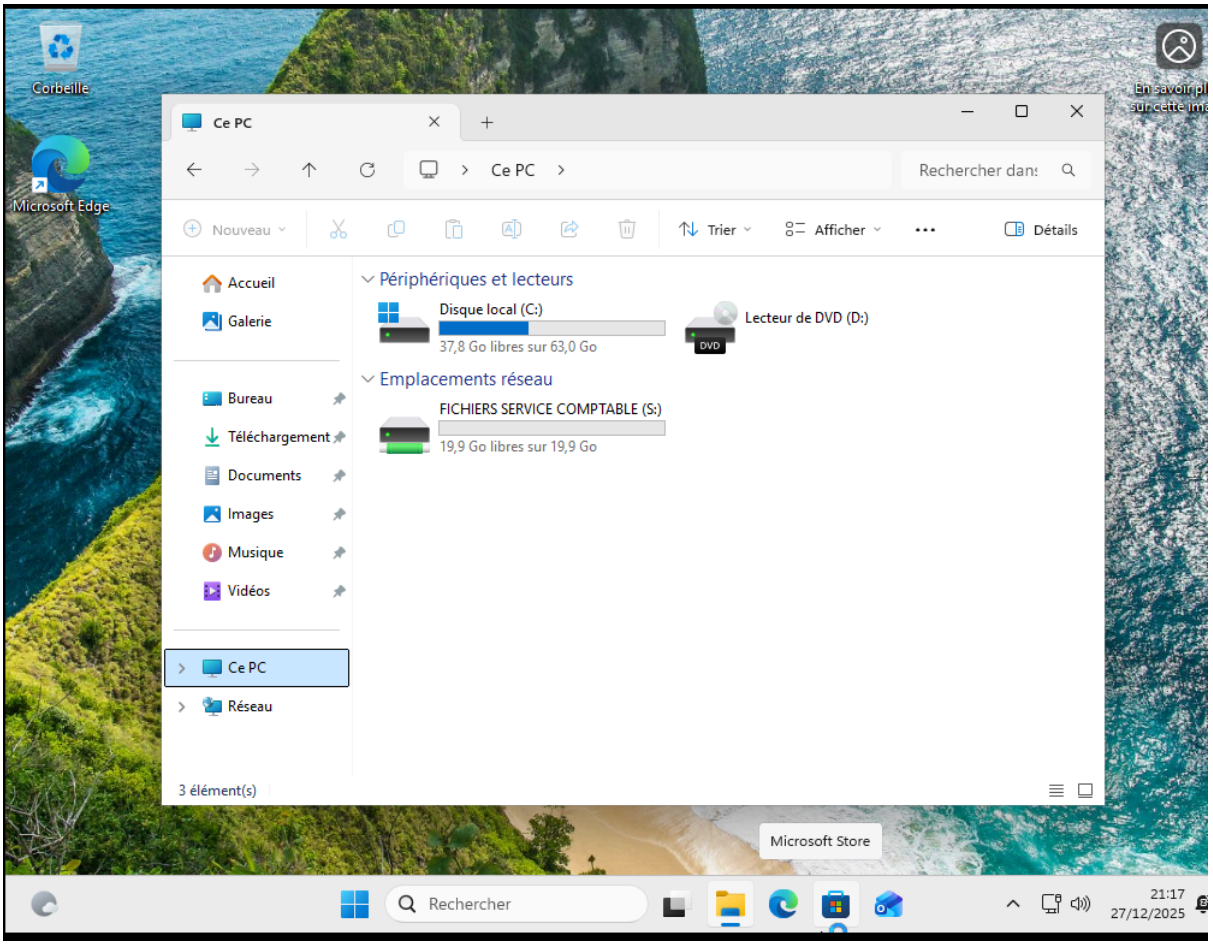
Étape 11 : Vérification du lecteur réseau

Une fois la configuration terminée, il suffit de se connecter sur la machine **Windows 11** avec un utilisateur appartenant à l'unité d'organisation ciblée, ici le groupe **COMPTABLE**. Après ouverture de session, rendez-vous dans **Fichiers**, puis dans **Ce PC** pour vérifier que le lecteur réseau **FICHIERS SERVICE COMPTABLE** s'affiche bien.



Pour confirmer que les droits ont été correctement appliqués, vous pouvez ouvrir ce lecteur et tenter d'y créer un dossier ou un fichier texte. Si l'opération réussit, cela signifie que les autorisations ont été configurées correctement.

*Note : Si le lecteur n'apparaît pas immédiatement, un redémarrage de **Windows 11** peut suffire à forcer l'application de la stratégie de groupe et l'affichage du lecteur.*



« Figure 53 : Vérification du lecteur réseau FICHIERS SERVICE COMPTABLE sur Windows 11 »

Conclusion du chapitre 4

Nous avons terminé la mise en place du lecteur réseau destiné au service comptable. Après avoir créé le partage, configuré les droits NTFS puis déployé la GPO, le lecteur FICHIERS SERVICE COMPTABLE a pu être appliqué aux utilisateurs du groupe COMPTABLE.

La vérification sur une machine Windows 11 a permis de confirmer que le lecteur apparaissait bien dans l'explorateur de fichiers. Ce travail montre l'intérêt d'une gestion centralisée des accès, qui simplifie l'administration et garantit une répartition cohérente des ressources dans le domaine.

Fin du chapitre 4