

PROCÉDURE D'INSTALLATION

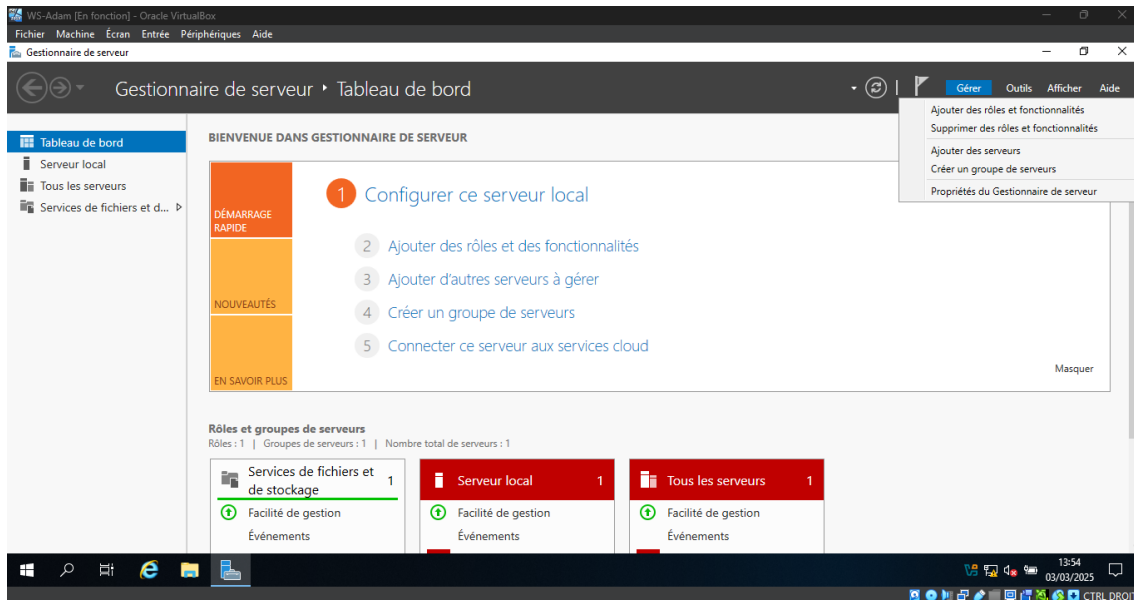
Active Directory Domain Services (AD DS)

Hyperviseur : VirtualBox | OS : Windows Server 2019 | Rôle : AD DS | Domaine : adam.lan

PARTIE 1 — Ajout du rôle AD DS via le Gestionnaire de serveur

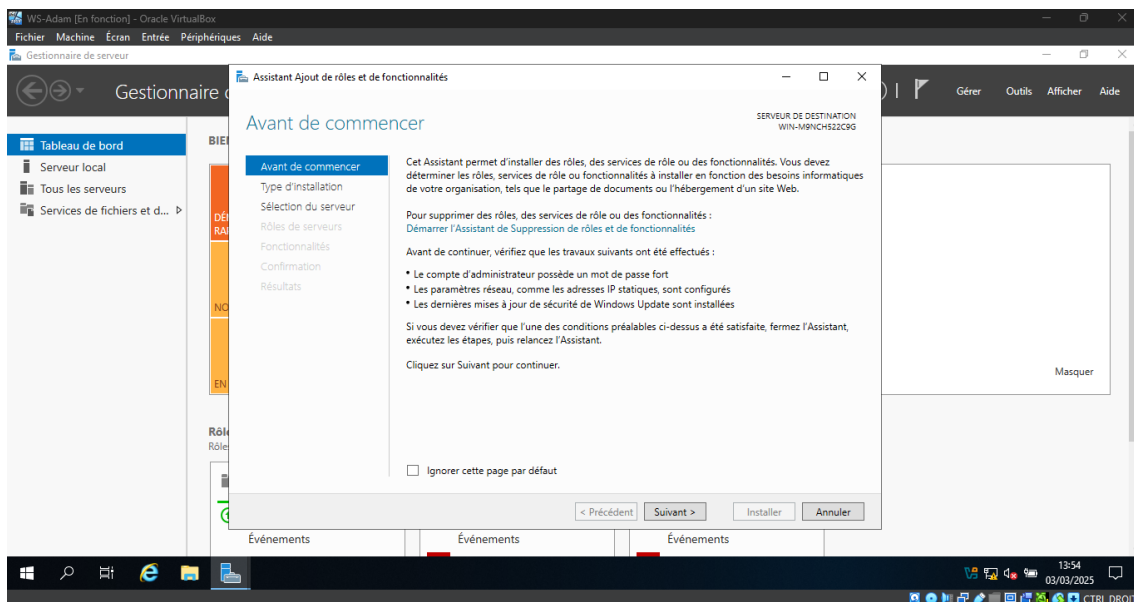
❗ Ces étapes s'effectuent dans le Gestionnaire de serveur (Server Manager) de Windows Server 2019, avant la promotion en contrôleur de domaine.

Étape 1 — Tableau de bord du Gestionnaire de serveur



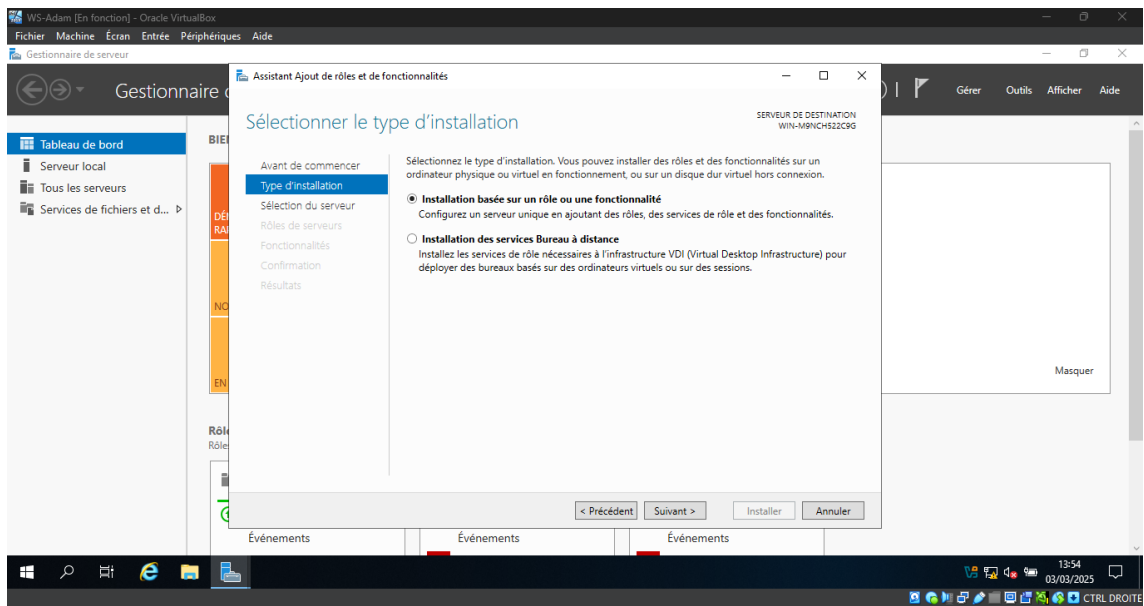
► Ouvrir le Gestionnaire de serveur. La fenêtre affiche un tableau de bord récapitulatif des rôles installés. Cliquer sur « Gérer » en haut à droite, puis sur « Ajouter des rôles et des fonctionnalités ».

Étape 2 — Assistant Ajout de rôles — Avant de commencer



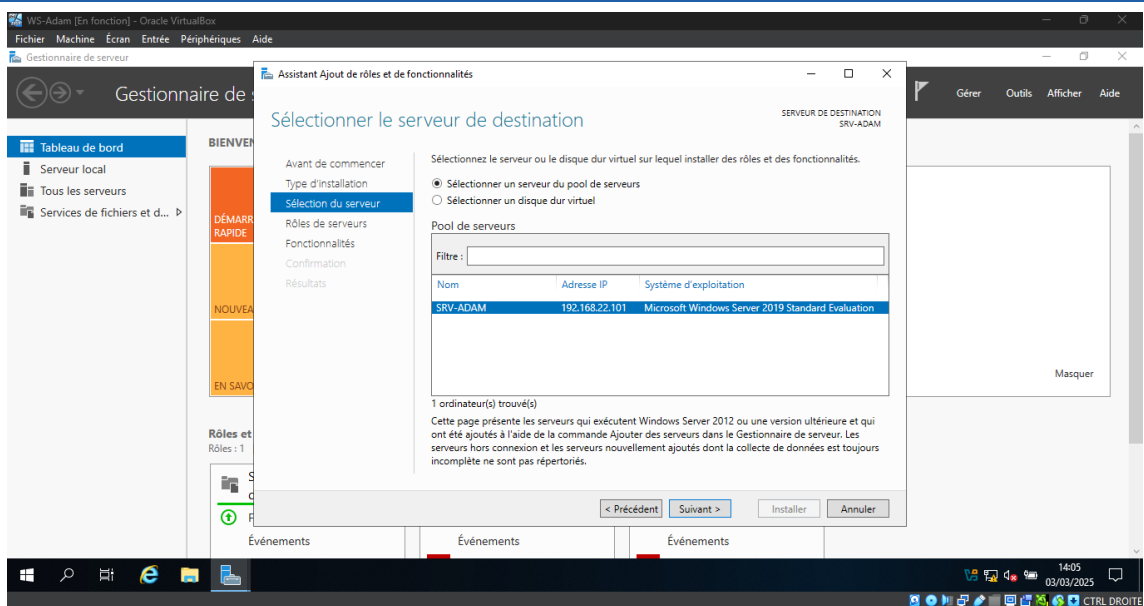
► L'assistant s'ouvre sur une page d'introduction. Lire les recommandations (compte Administrateur actif, IP statique configurée, mises à jour installées), puis cliquer sur Suivant.

Étape 3 — Type d'installation



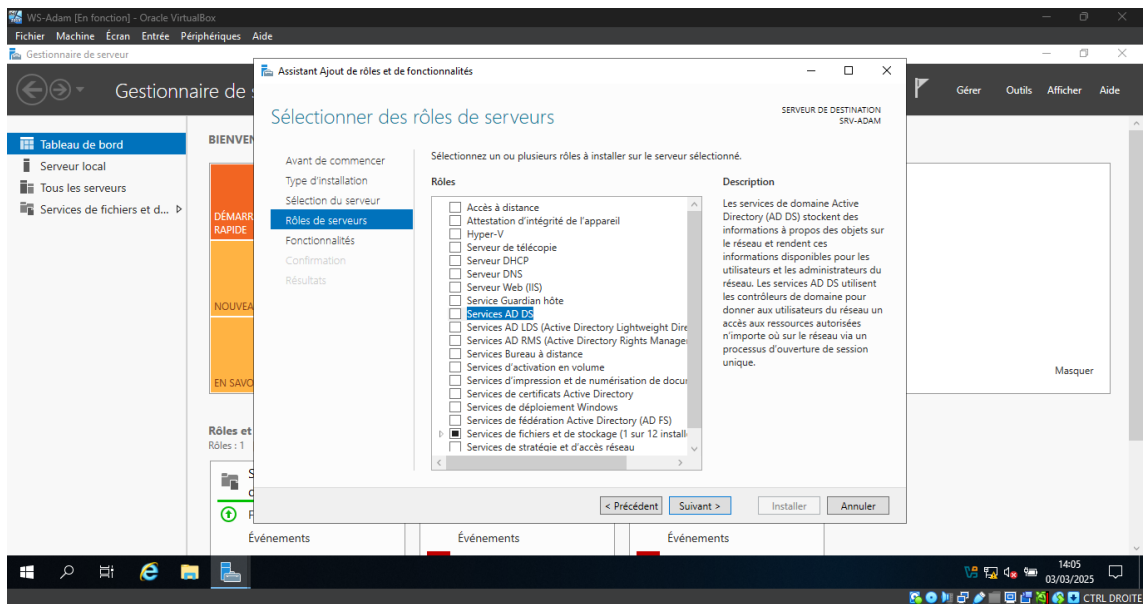
► Sélectionner « Installation basée sur un rôle ou une fonctionnalité », puis cliquer sur Suivant. Cette option installe les rôles directement sur le serveur local.

Étape 4 — Sélection du serveur de destination



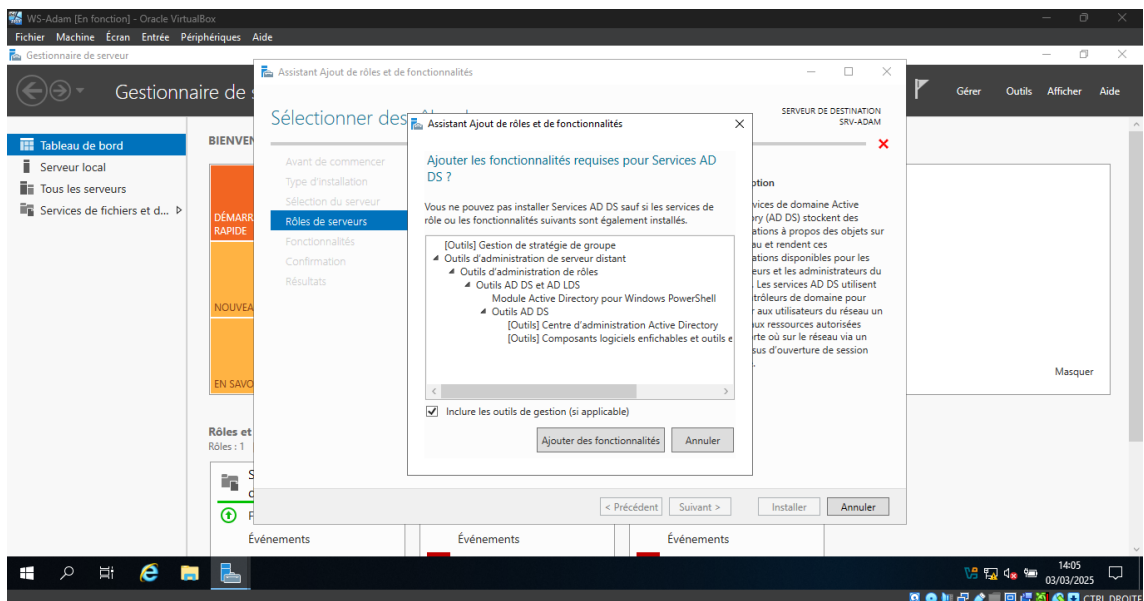
► Sélectionner le serveur local dans le pool de serveurs (il doit être le seul disponible dans un environnement de lab). Cliquer sur Suivant.

Étape 5 — Sélection des rôles de serveurs



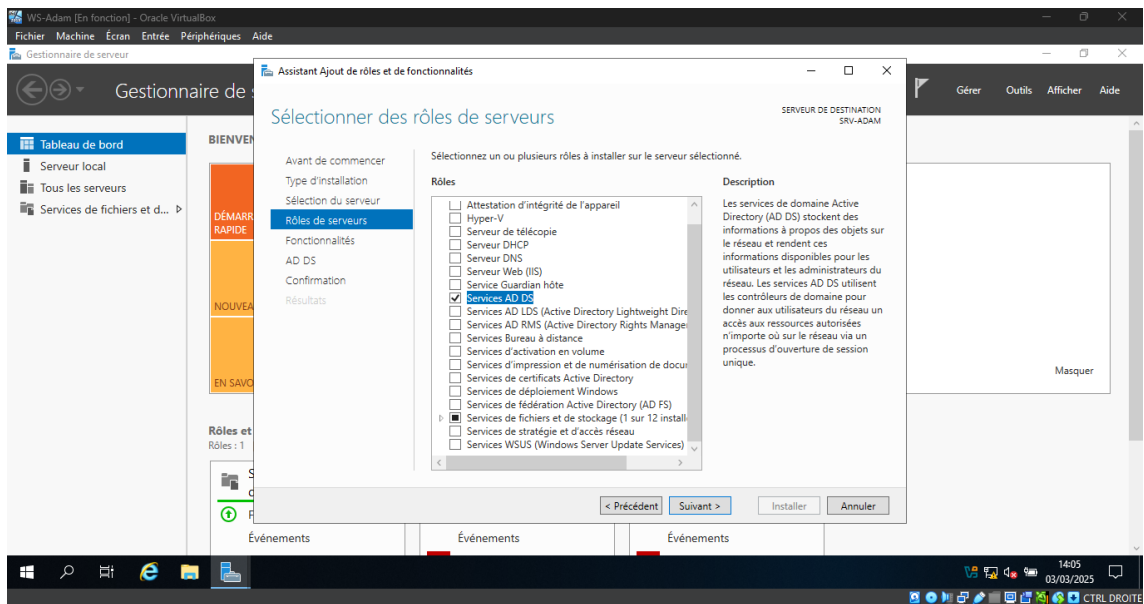
► Sur l'écran des rôles, défiler jusqu'à « Services de domaine Active Directory (AD DS) » et cocher la case correspondante. Une pop-up s'affiche pour proposer d'ajouter les fonctionnalités et outils d'administration requis.

Étape 6 — Ajout des fonctionnalités requises



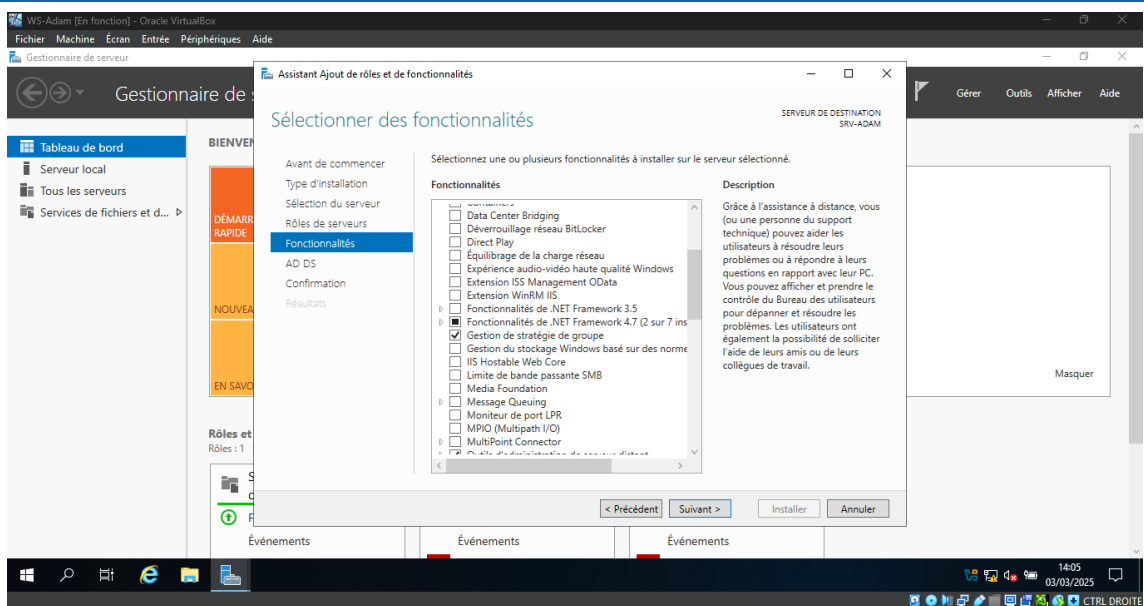
► Cliquer sur « Ajouter des fonctionnalités » dans la pop-up. Cela installe automatiquement les composants nécessaires à AD DS (PowerShell pour AD, outils RSAT, etc.). Cliquer ensuite sur Suivant.

Étape 7 — Fonctionnalités supplémentaires



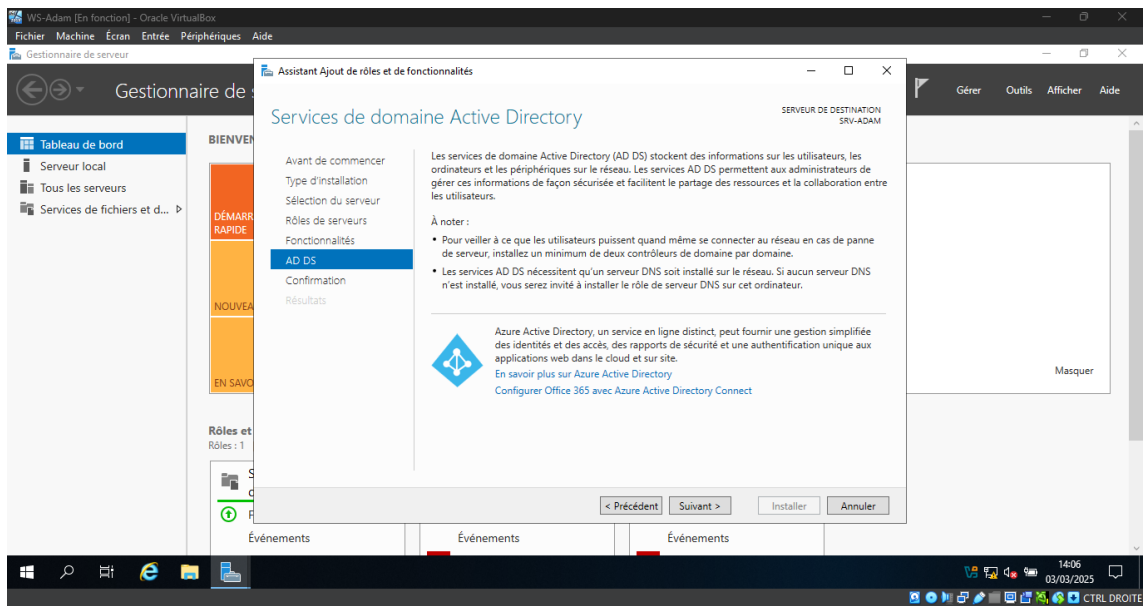
► Laisser les fonctionnalités par défaut cochées et cliquer sur Suivant. Des fonctionnalités comme .NET Framework 4.7 sont généralement déjà présélectionnées.

Étape 8 — Informations sur AD DS



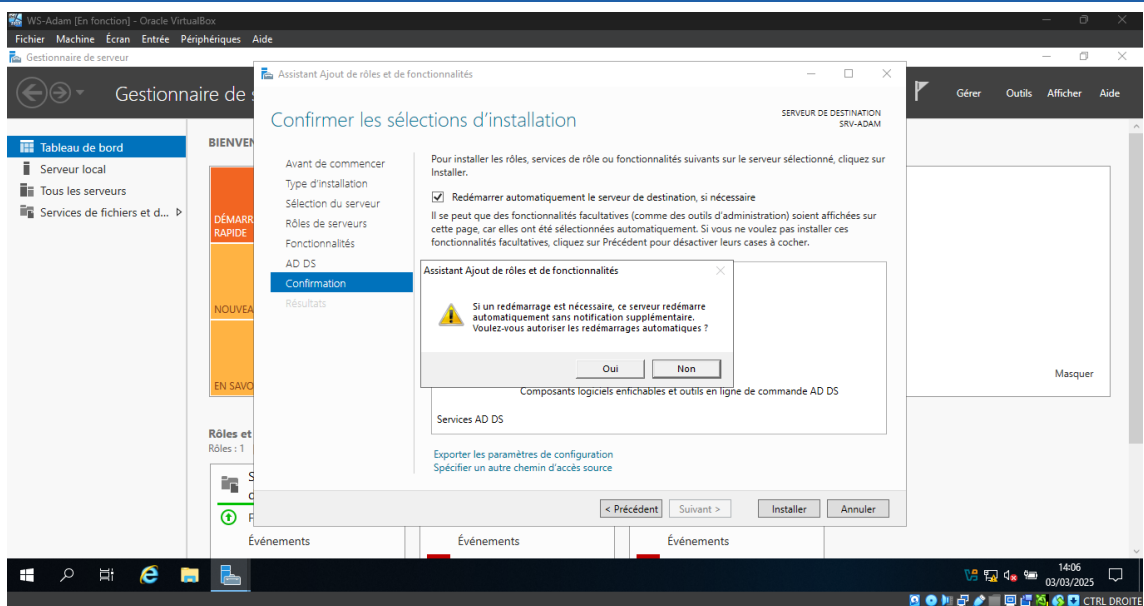
► Windows affiche une page descriptive sur AD DS : rôle, composants, prérequis. Lire ces informations pour comprendre ce qui va être installé, puis cliquer sur Suivant.

Étape 9 — Confirmation de l'installation



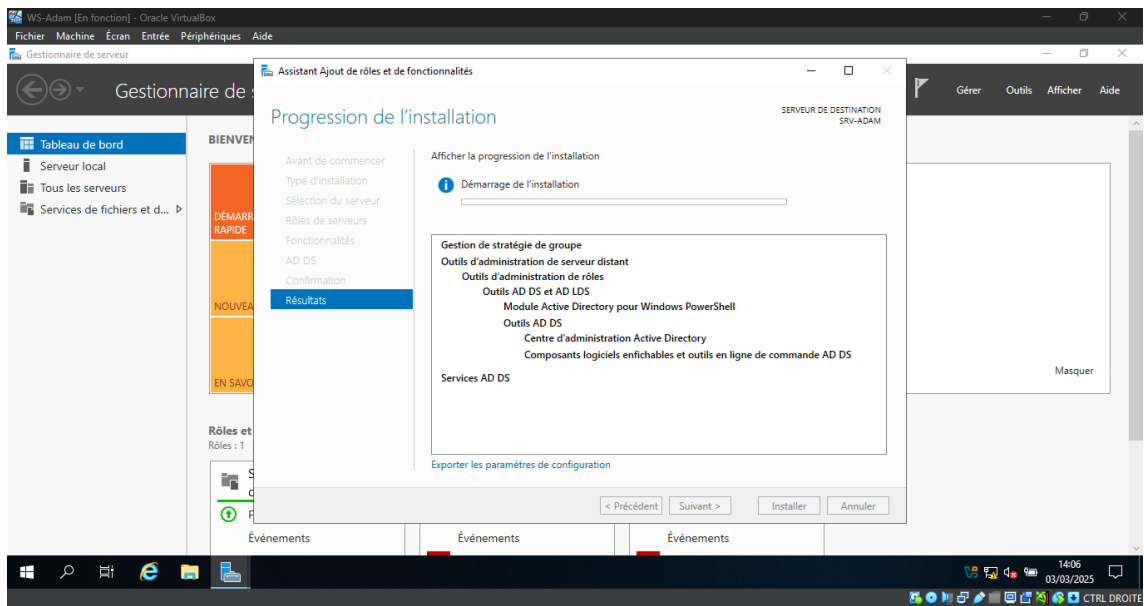
► Vérifier le récapitulatif des éléments à installer. Cocher si besoin « Redémarrer automatiquement si nécessaire ». Cliquer sur « Installer » pour lancer le processus.

Étape 10 — Installation en cours



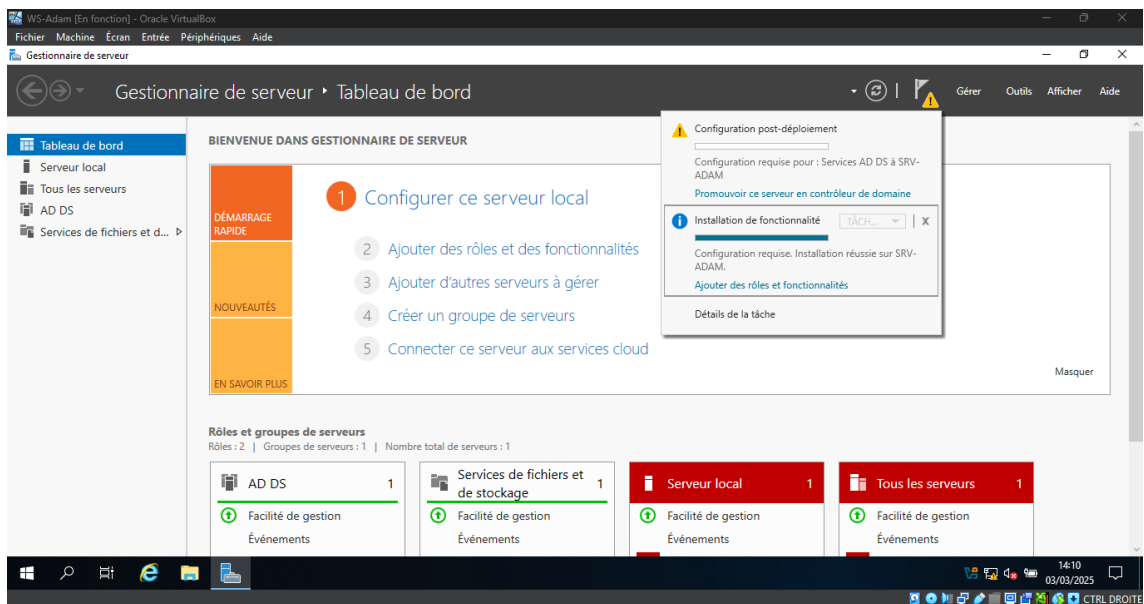
► L'installation du rôle AD DS est en cours. Une barre de progression indique l'avancement. Ne pas fermer la fenêtre ni éteindre le serveur durant cette phase.

Étape 11 — Installation terminée — Promotion requise



► Une fois l'installation terminée, un message indique qu'une « configuration supplémentaire est requise ». Le serveur doit maintenant être promu en contrôleur de domaine. Cliquer sur « Promouvoir ce serveur en contrôleur de domaine » via le drapeau d'alerte.

Étape 12 — Tableau de bord après installation

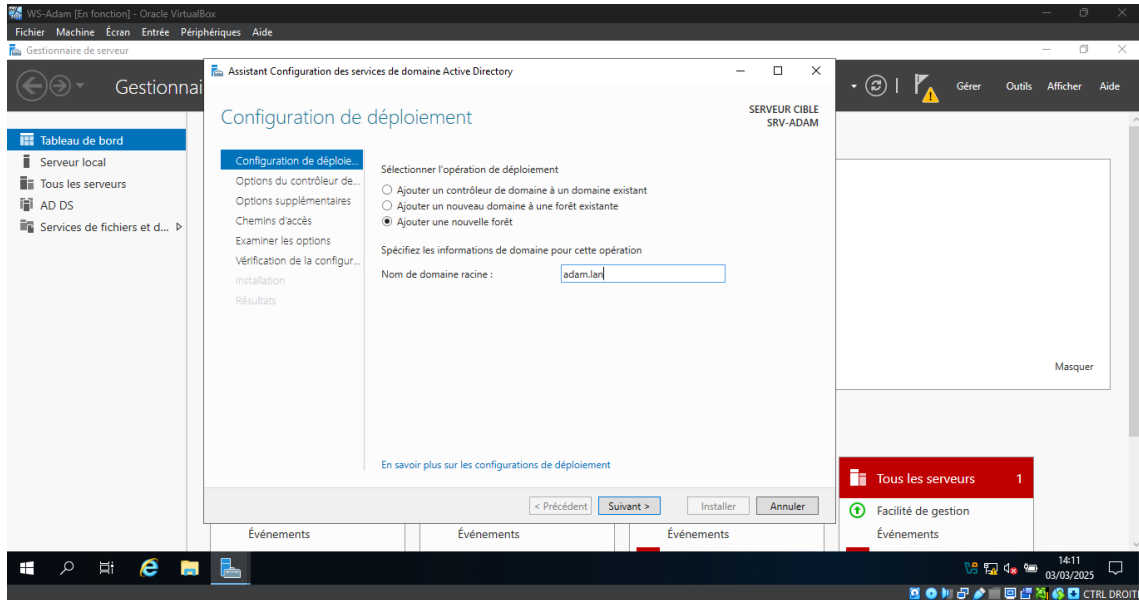


► Retourner au tableau de bord : le rôle AD DS apparaît maintenant dans la liste des rôles installés. L'alerte de configuration (drapeau jaune) est toujours visible — elle invite à terminer la promotion.

PARTIE 2 — Promotion en contrôleur de domaine

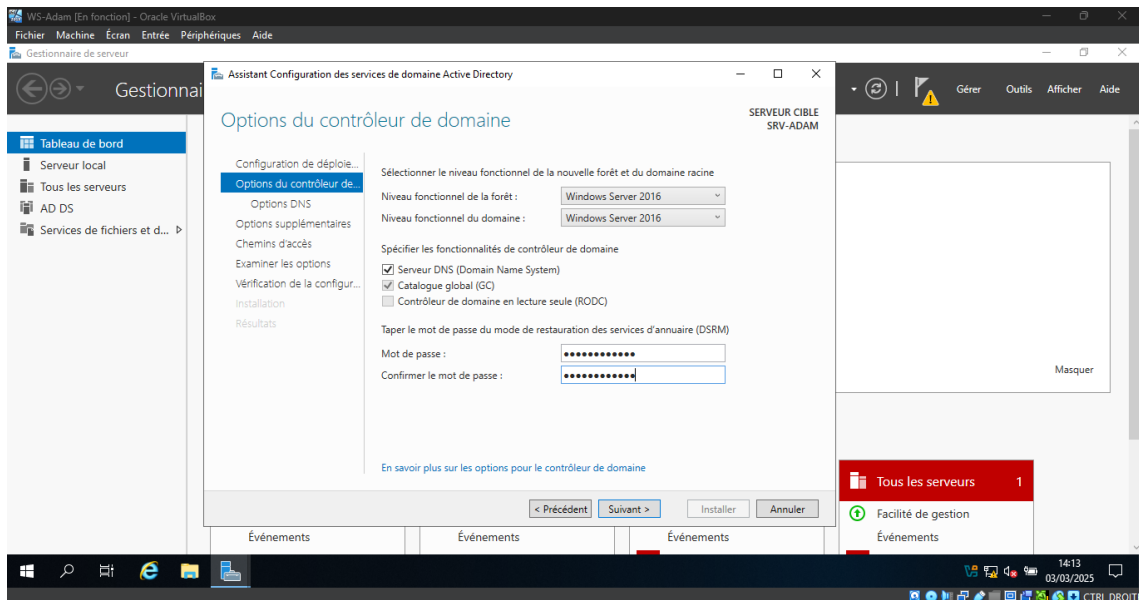
La promotion est l'étape qui transforme le serveur en contrôleur de domaine (DC). Elle crée la forêt et le domaine Active Directory. Cette opération est irréversible sans démontage complet du rôle.

Étape 13 — Lancer l'Assistant de configuration AD DS



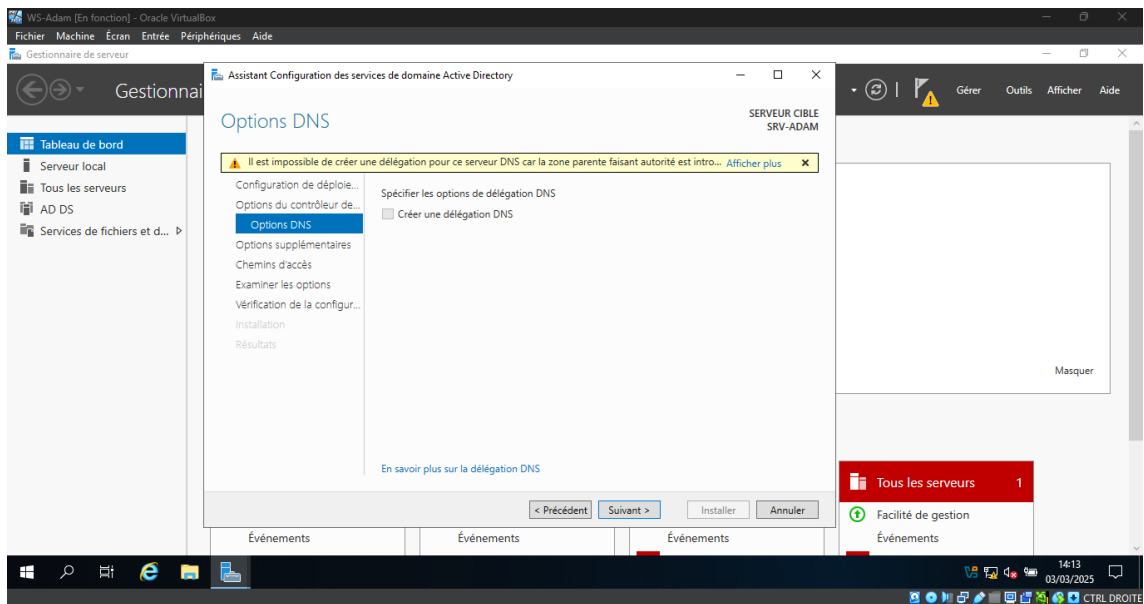
► Cliquer sur le drapeau d'alerte dans le Gestionnaire de serveur, puis sur « Promouvoir ce serveur en contrôleur de domaine ». L'Assistant de configuration AD DS s'ouvre.

Étape 14 — Ajout d'une nouvelle forêt



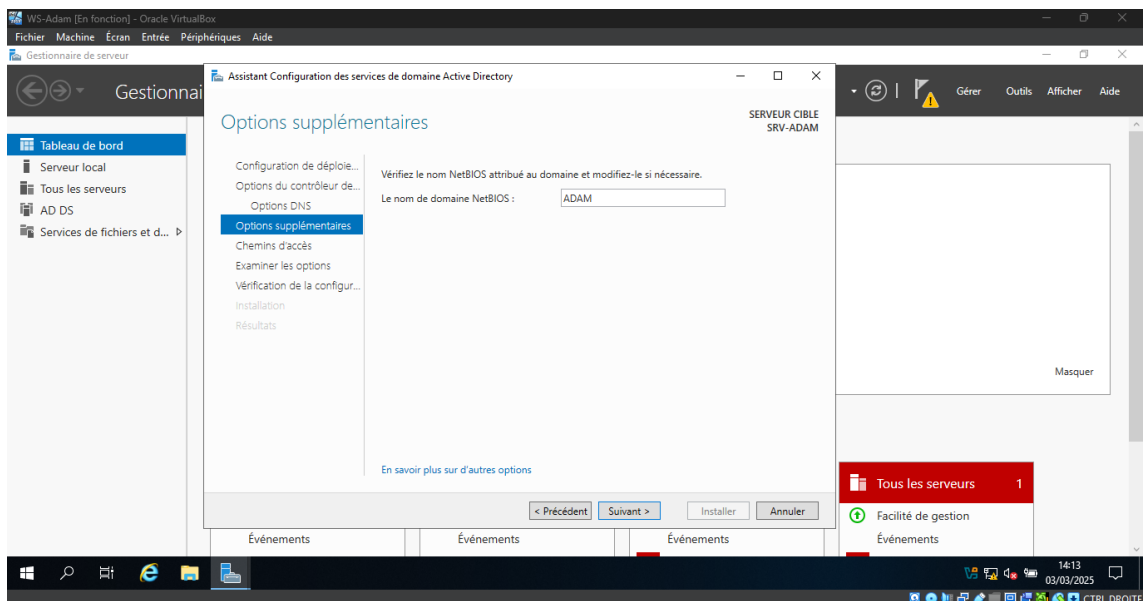
► Sélectionner « Ajouter une nouvelle forêt » et saisir le nom du domaine racine : adam.lan (ou le nom choisi pour votre domaine interne). Le suffixe .lan est utilisé pour les domaines non exposés sur Internet. Cliquer sur Suivant.

Étape 15 — Options du contrôleur de domaine



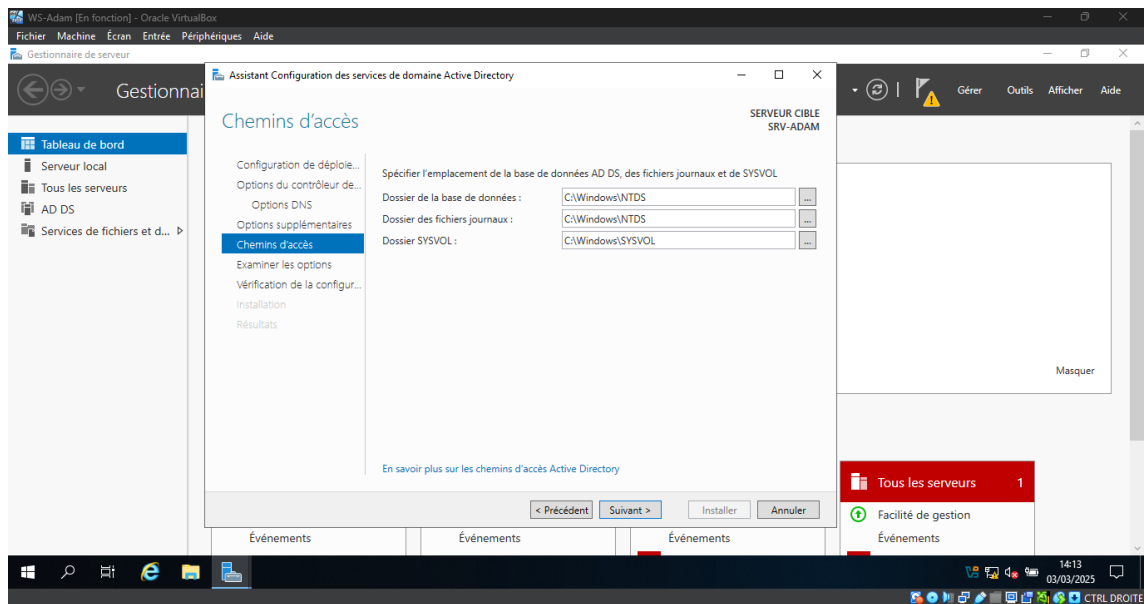
► Laisser le niveau fonctionnel à « Windows Server 2016 » (ou le plus récent disponible). S'assurer que les cases « Serveur DNS » et « Catalogue global (GC) » sont cochées. Définir un mot de passe DSRM (Directory Services Restore Mode) solide — ce mot de passe sert uniquement en cas de récupération d'urgence de l'AD.

Étape 16 — Options DNS



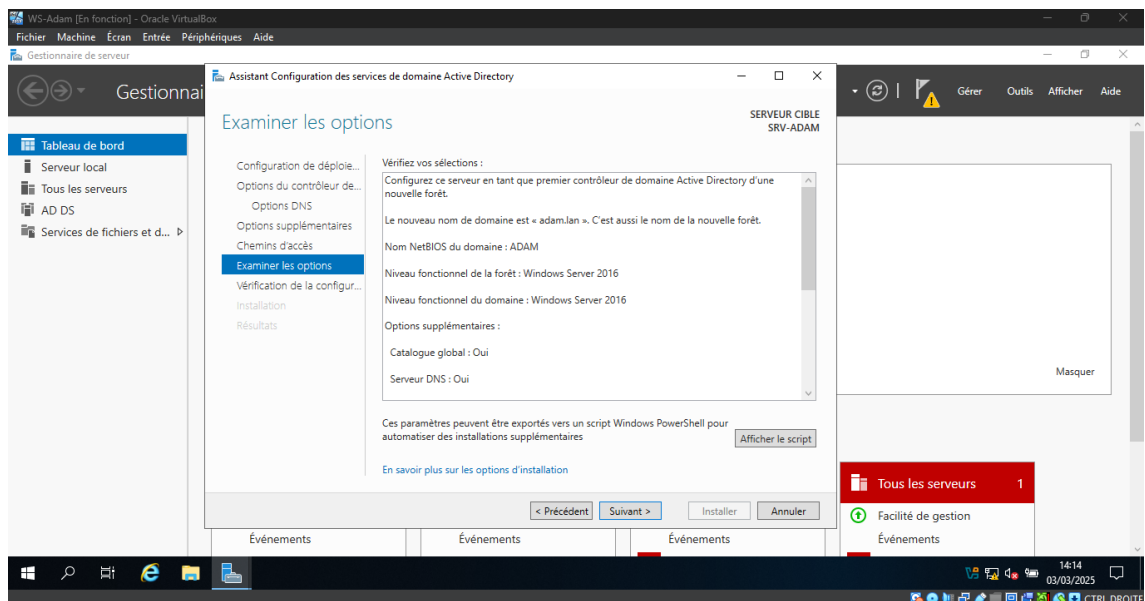
► Ne pas cocher la délégation DNS (non requise pour un domaine de lab). Si un avertissement sur la zone de délégation apparaît, l'ignorer. Cliquer sur Suivant.

Étape 17 — Nom NetBIOS du domaine



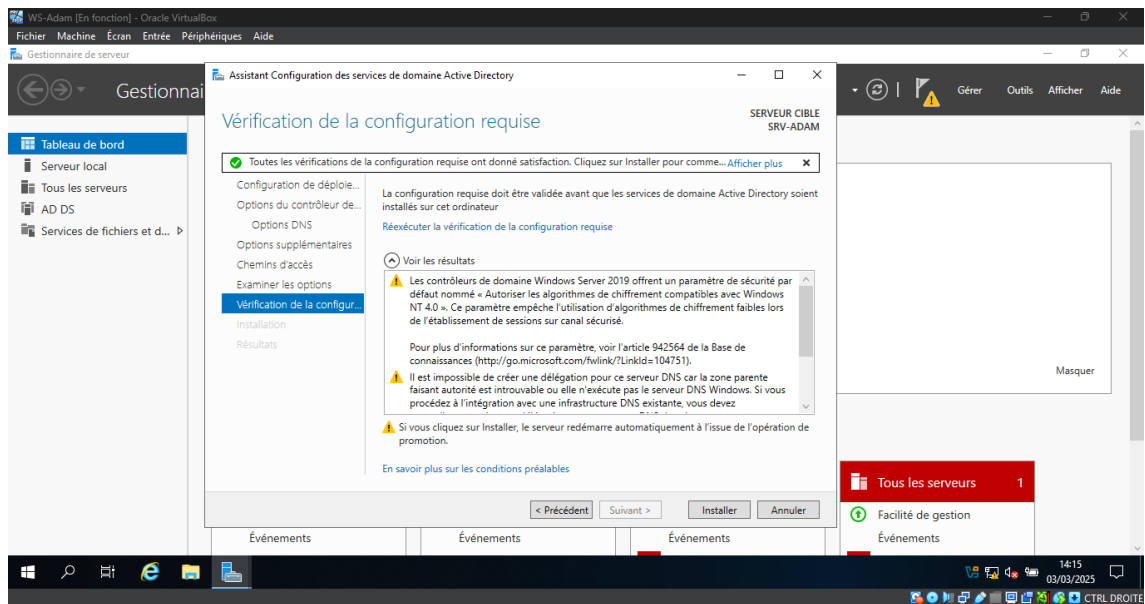
► Le nom NetBIOS est généré automatiquement à partir du nom de domaine (ex. ADAM pour adam.lan). Laisser la valeur proposée, elle est utilisée par les applications et systèmes plus anciens pour identifier le domaine. Cliquer sur Suivant.

Étape 18 — Chemins des dossiers AD



► Laisser les chemins par défaut pour la base NTDS (C:\Windows\NTDS), les journaux d'événements AD et le dossier SYSVOL (C:\Windows\SYSVOL). Ces emplacements sont standards pour un serveur de production ou de lab. Cliquer sur Suivant.

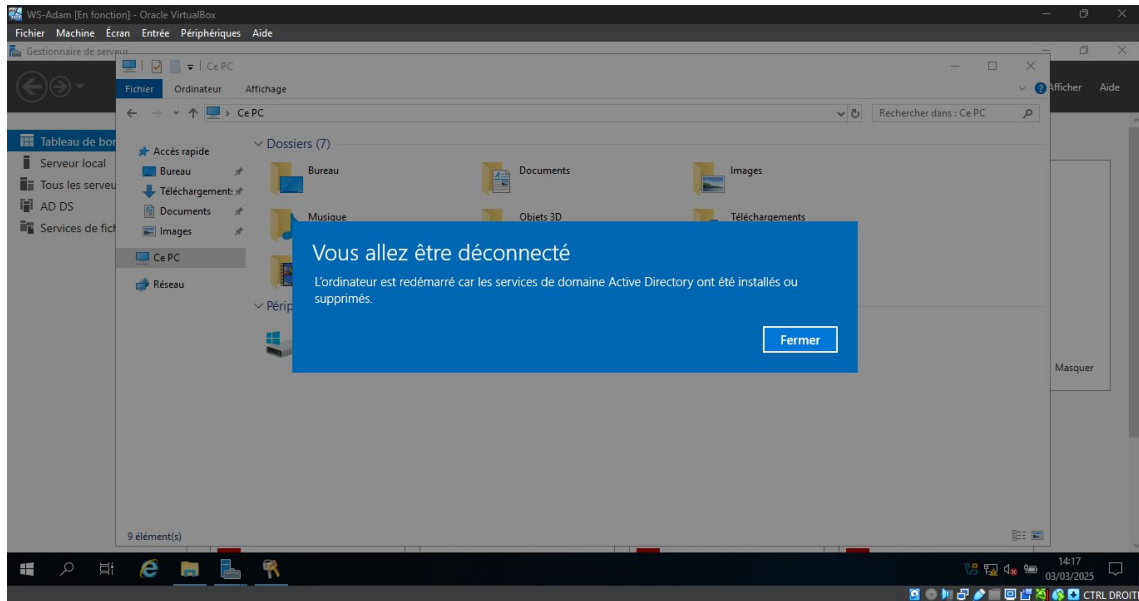
Étape 19 — Récapitulatif de la configuration



► L'assistant affiche le récapitulatif complet de la configuration qui sera appliquée. Vérifier attentivement le nom du domaine, le niveau fonctionnel et les chemins. Cliquer sur Suivant pour lancer la vérification des prérequis.

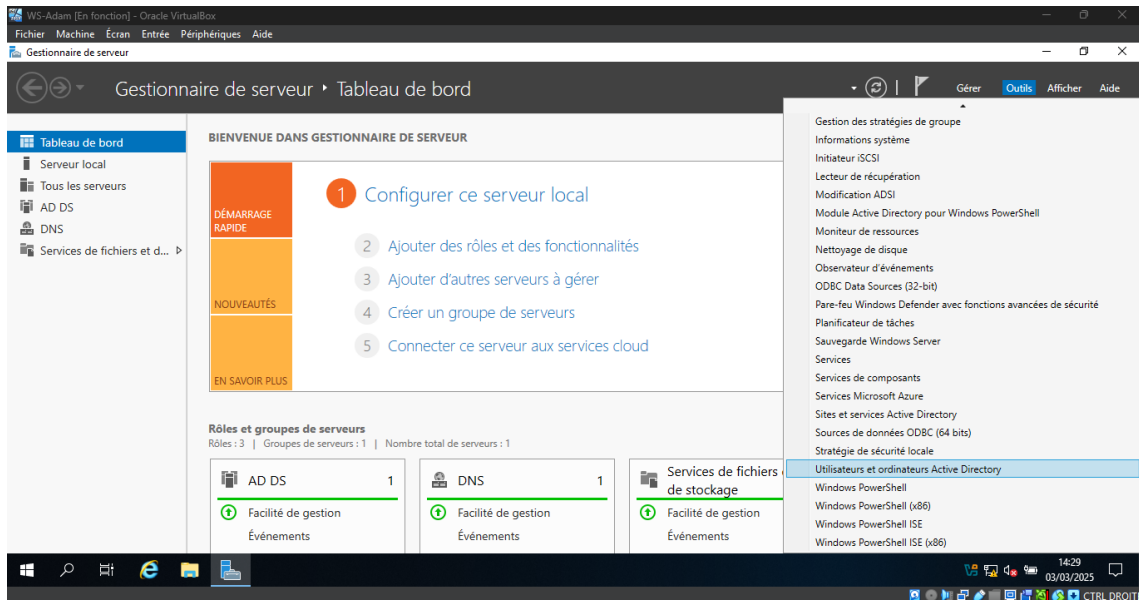
PARTIE 3 — Vérification des prérequis et finalisation

Étape 20 — Vérification des prérequis — Redémarrage



► Le serveur redémarre automatiquement après la vérification et l'installation. Attendre le redémarrage complet. À partir de ce moment, la connexion s'effectue avec le compte ADAM\Administrateur (domaine\utilisateur).

Étape 21 — Tableau de bord après promotion

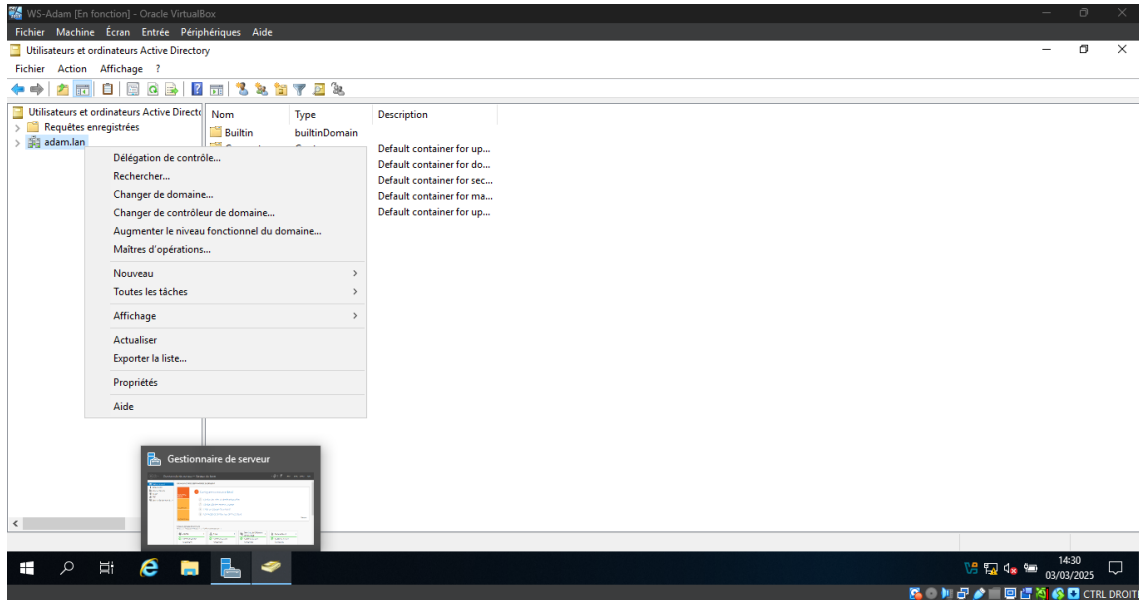


► Après reconnexion, le Gestionnaire de serveur affiche désormais les rôles AD DS et DNS actifs. Le serveur est maintenant un contrôleur de domaine pour adam.lan.

PARTIE 4 — Structure AD : Unités d'Organisation, Utilisateurs, Groupes

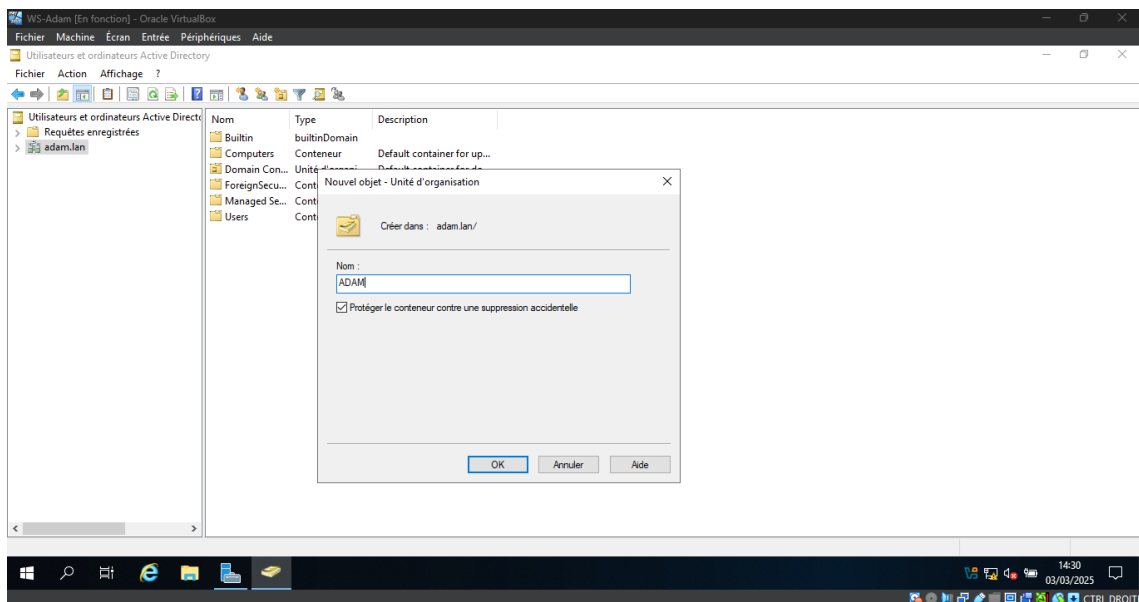
Les Unités d'Organisation (UO / OU) permettent de structurer l'AD et d'appliquer des GPO ciblées. La hiérarchie recommandée : Domaine → UO racine → UO par fonction (Admins, Ordinateurs, etc.).

Étape 22 — Ouvrir Utilisateurs et ordinateurs AD



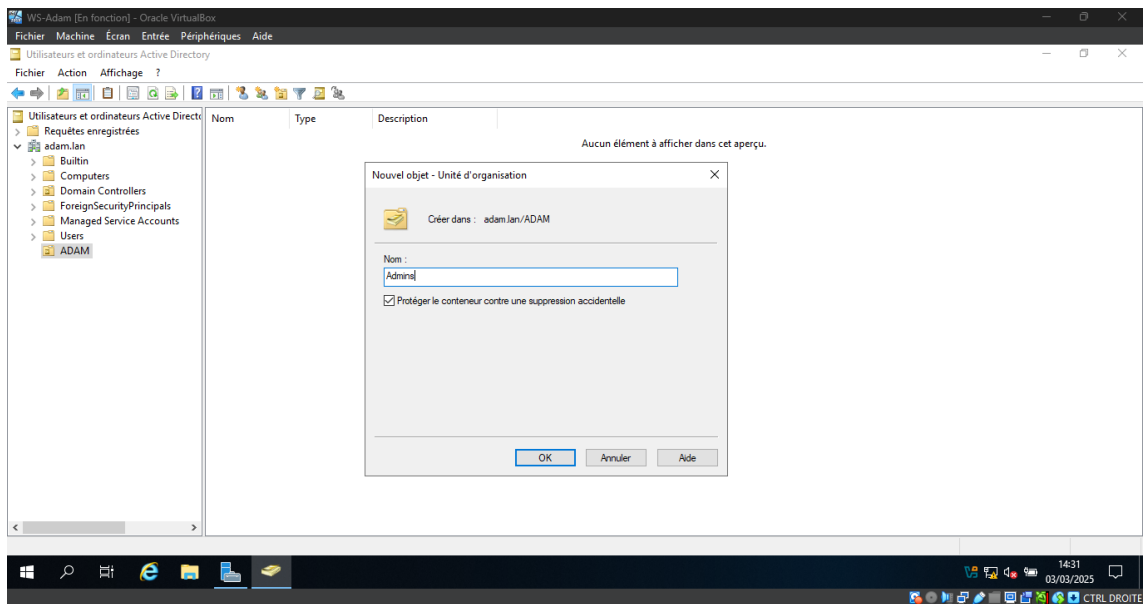
► Dans le Gestionnaire de serveur → Outils → « Utilisateurs et ordinateurs Active Directory ». Cet outil permet de gérer tous les objets du domaine (utilisateurs, groupes, UO, ordinateurs).

Étape 23 — Création de l'UO racine



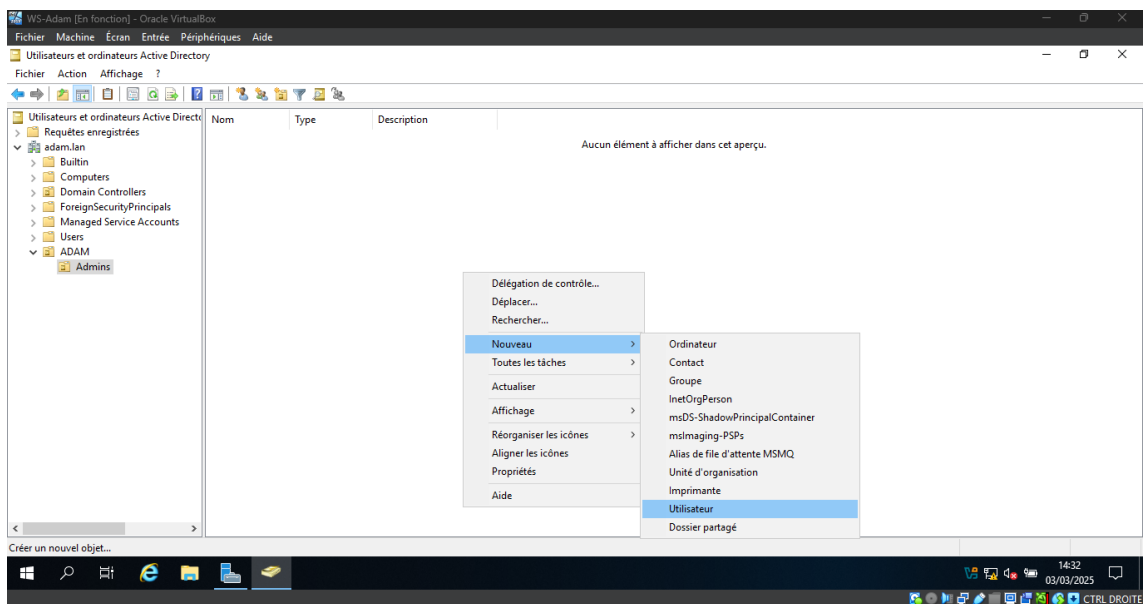
► Faire un clic droit sur le domaine (adam.lan) → Nouveau → Unité d'organisation. Nommer cette UO racine selon votre convention (ex. ADAM). Elle contiendra toutes les sous-UO.

Étape 24 — Nommage de l'UO racine



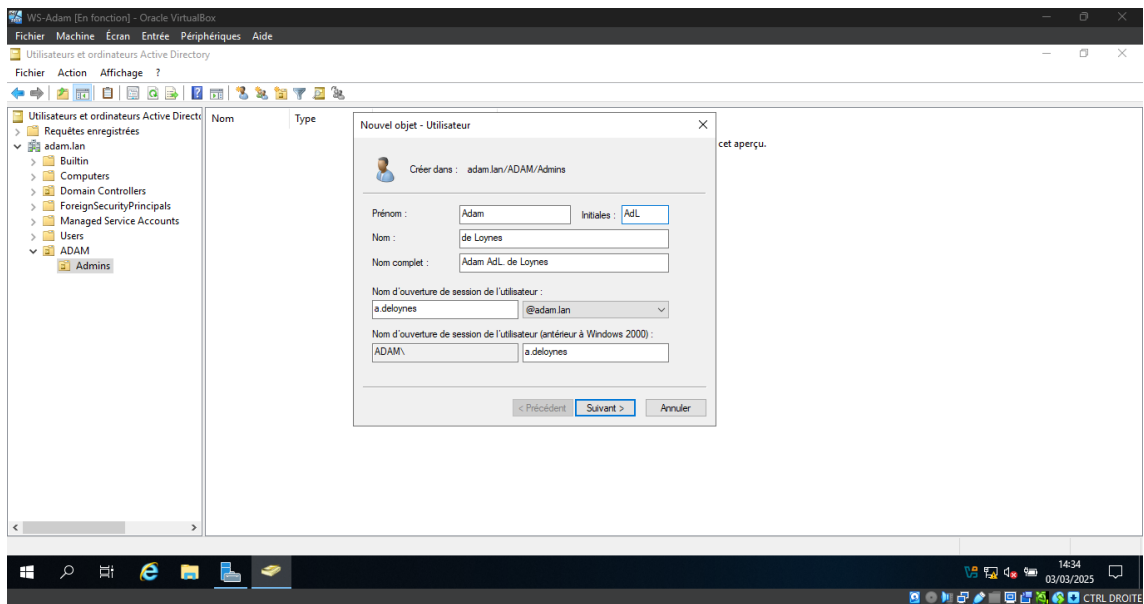
► Saisir le nom de l'UO (ex. ADAM). Laisser la case « Protéger le conteneur contre la suppression accidentelle » cochée — cela évite de supprimer l'UO par erreur. Cliquer sur OK.

Étape 25 — Arborescence AD créée



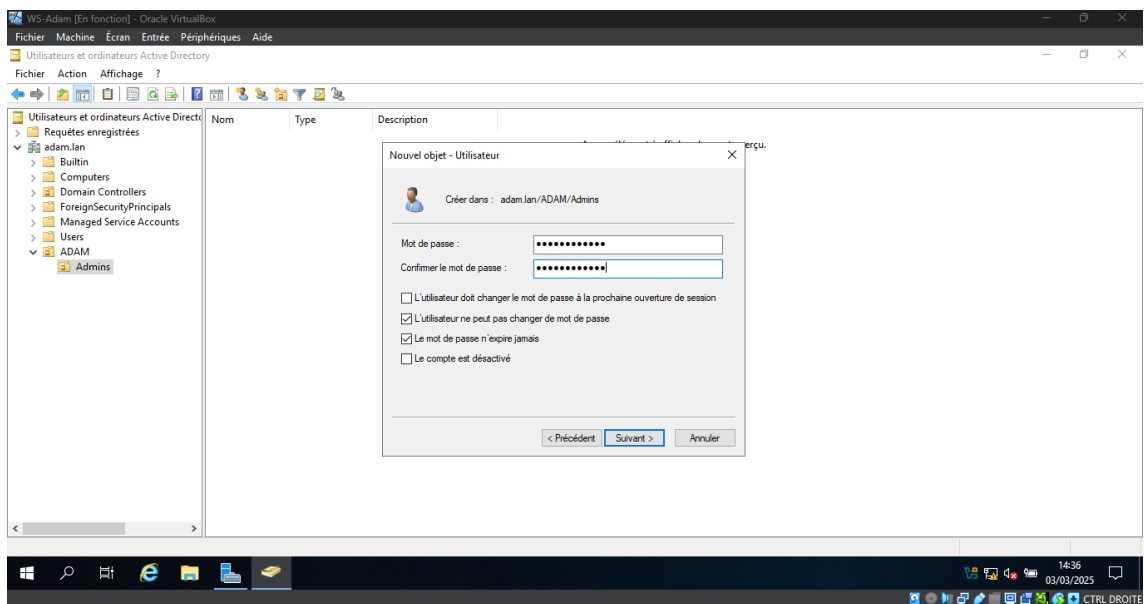
► L'UO racine apparaît dans l'arborescence sous adam.lan. Continuer en créant les sous-UO nécessaires à la structure du domaine.

Étape 26 — Création d'un utilisateur



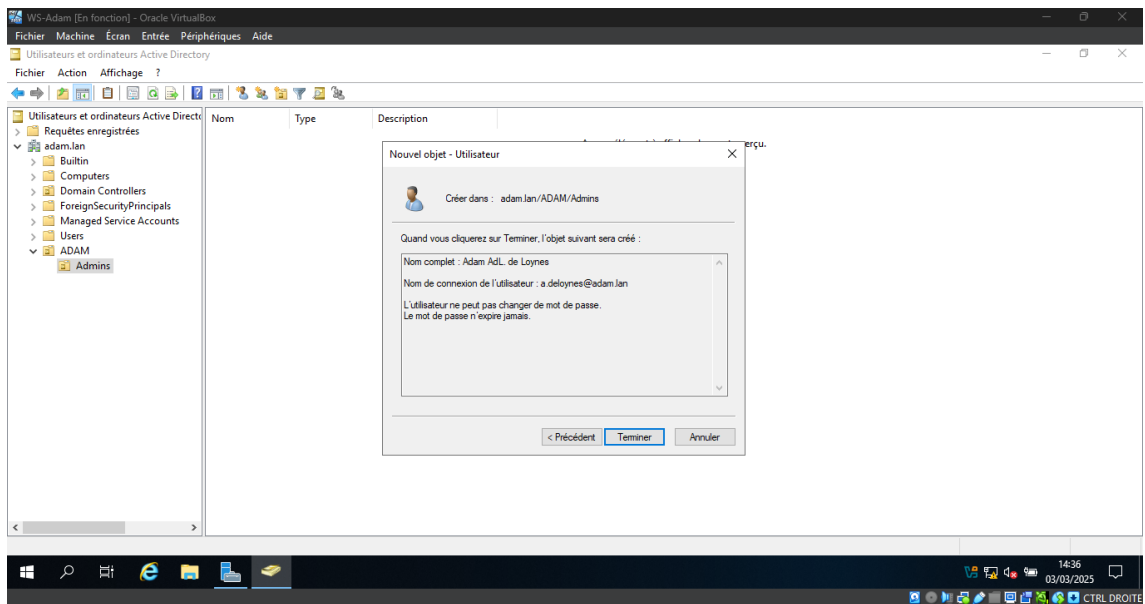
► Dans l'OU Admins (à créer de la même manière), faire un clic droit → Nouveau → Utilisateur. Renseigner le prénom, le nom et le nom d'ouverture de session (login, ex. a.nom).

Étape 27 — Mot de passe du compte



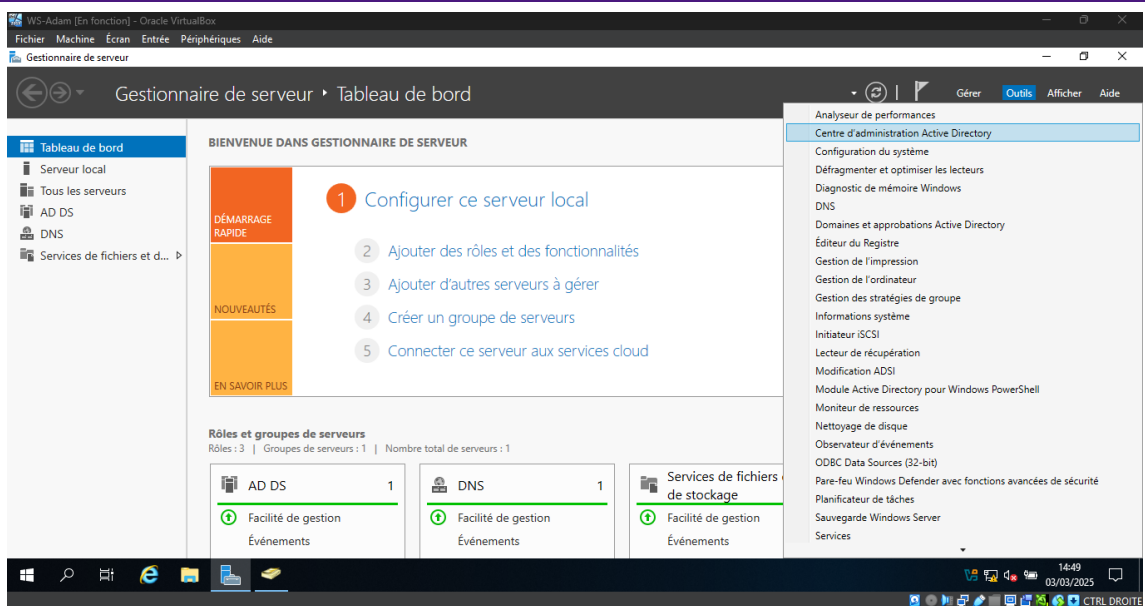
► Définir un mot de passe complexe pour le compte utilisateur. En environnement de production, décocher « Le mot de passe n'expire jamais » et cocher « L'utilisateur doit changer le mot de passe à la prochaine ouverture de session ».

Étape 28 — Confirmation de création



► Le résumé de création s'affiche avant de finaliser. Vérifier les informations et cliquer sur Terminer pour créer le compte.

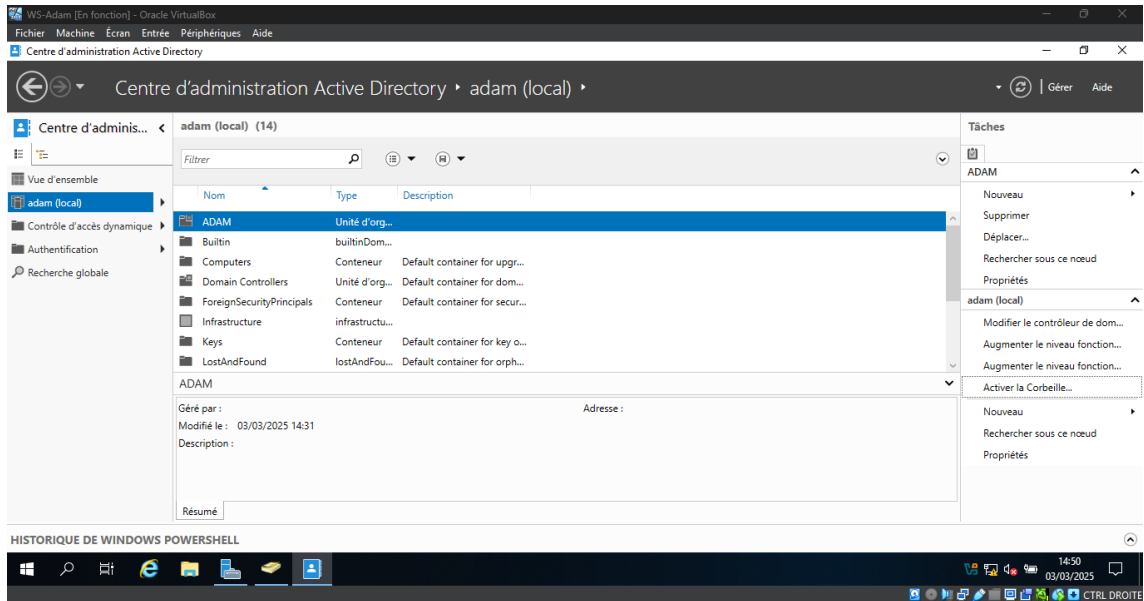
Étape 29 — Tableau de bord mis à jour



► Le Gestionnaire de serveur affiche maintenant les comptes et groupes créés. La structure AD est opérationnelle avec les utilisateurs correctement placés dans leurs UO respectives.

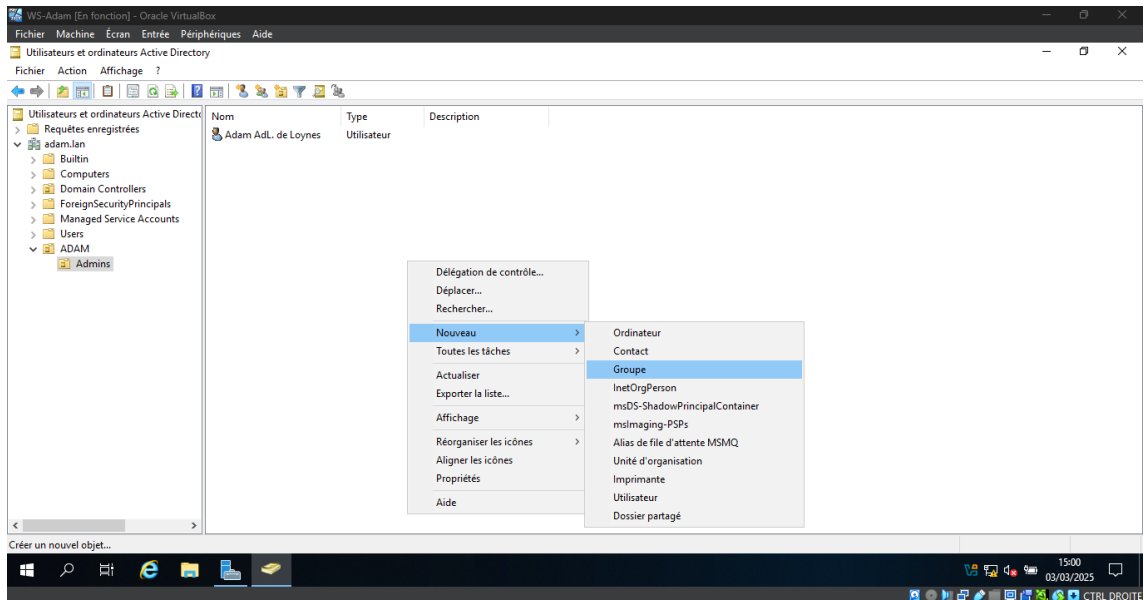
PARTIE 5 — Gestion des groupes et permissions

Étape 30 — Création d'un groupe



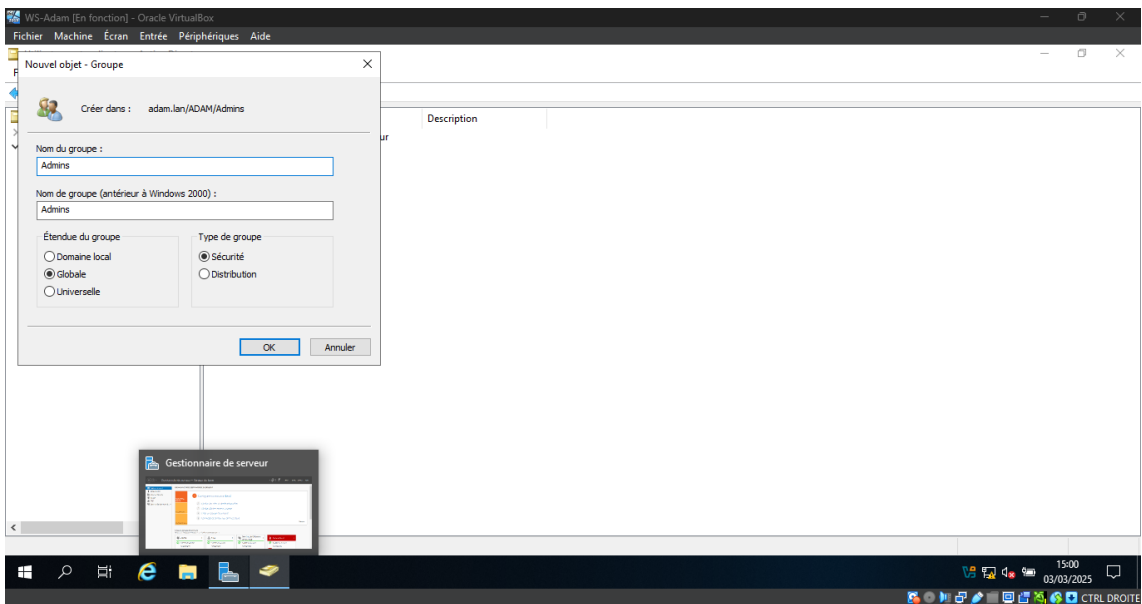
► Dans l'UO Admins, faire un clic droit → Nouveau → Groupe. Nommer le groupe « Admins ». Laisser l'étendue « Domaine local » et le type « Sécurité ». Les groupes de sécurité permettent d'attribuer des permissions à plusieurs utilisateurs simultanément.

Étape 31 — Ajouter un membre au groupe via clic droit



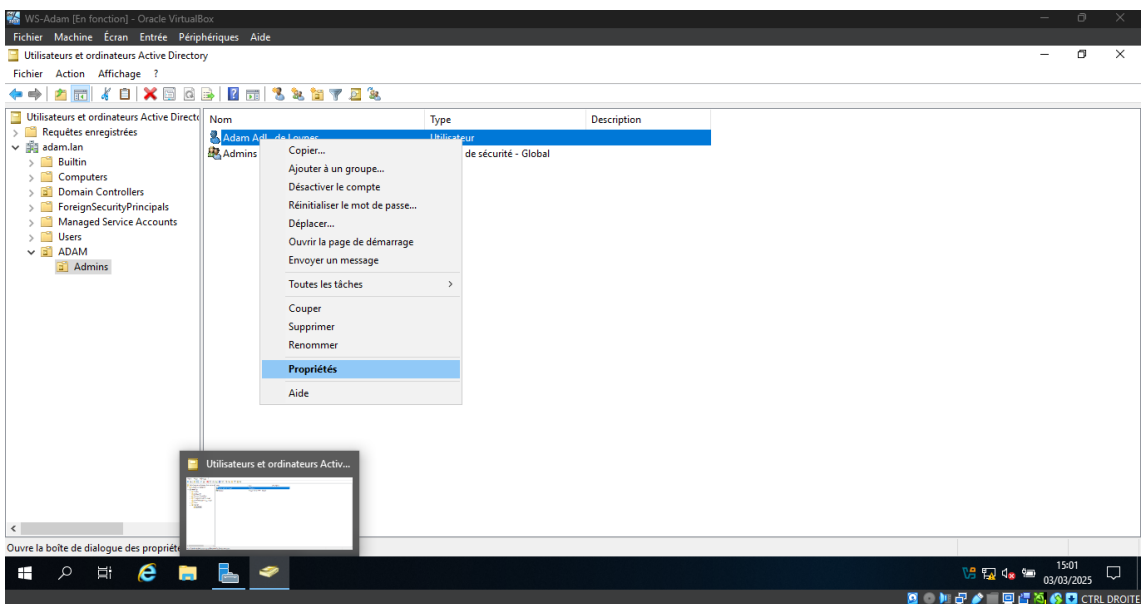
► Faire un clic droit sur le groupe Admins → Ajouter au groupe. Alternative : ouvrir les Propriétés de l'utilisateur → onglet « Membre de » → Ajouter.

Étape 32 — Propriétés du groupe — Nommage



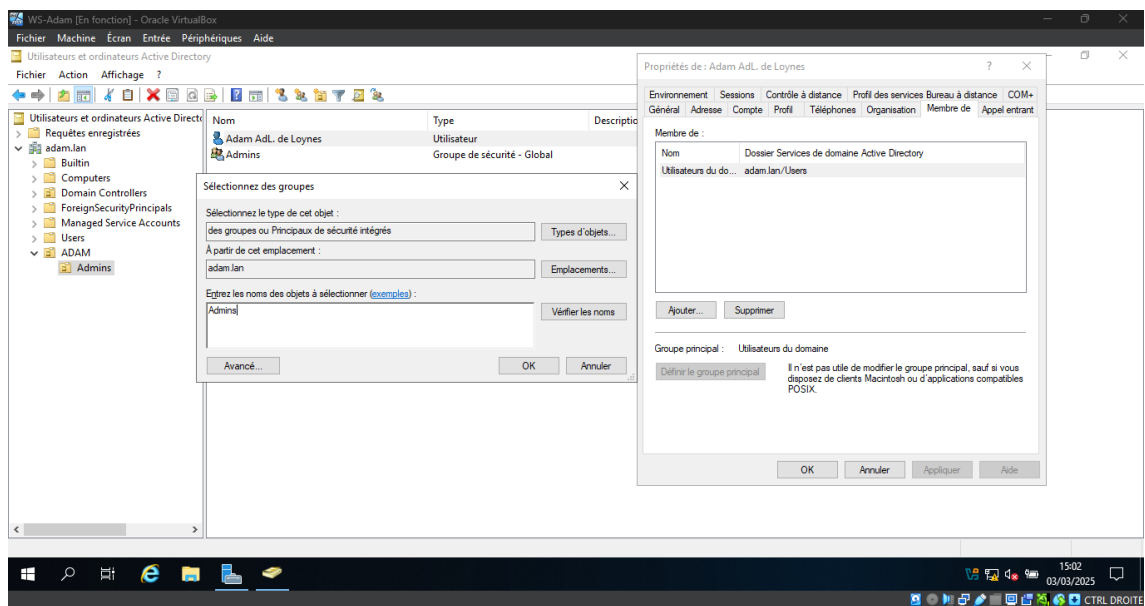
► Renseigner le nom du groupe (*Admins*), l'étendue (*Domaine local*) et le type (*Sécurité*). Ces paramètres déterminent la portée du groupe dans l'AD et ne sont pas facilement modifiables après création.

Étape 33 — Arborescence — Vue des objets créés



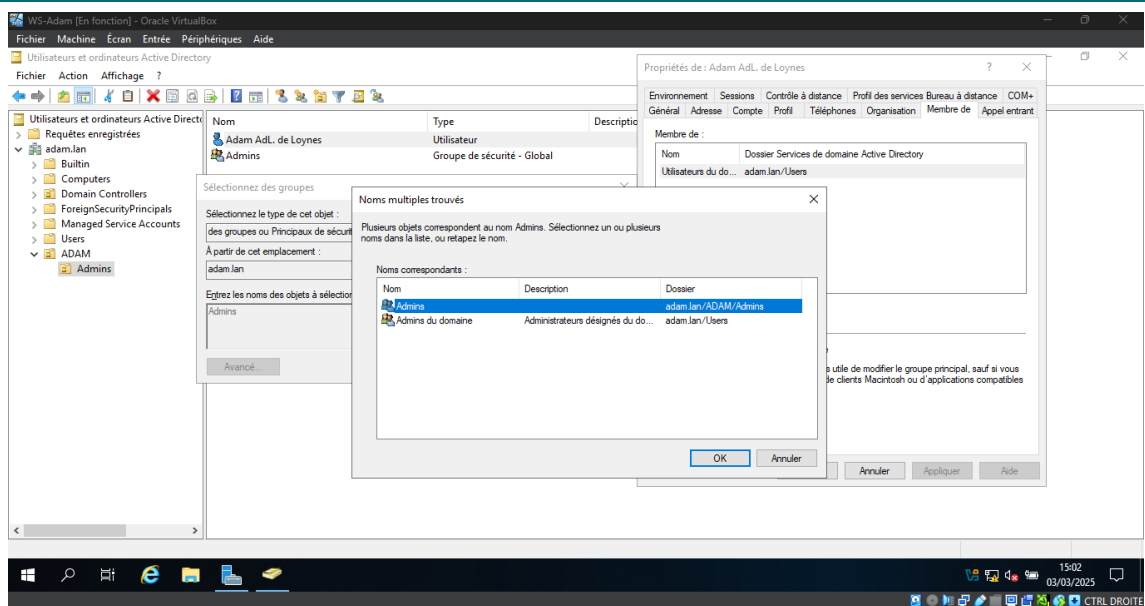
► L'arborescence AD montre maintenant les UO créées avec leurs objets (utilisateurs, groupes). La hiérarchie visuelle permet de confirmer la bonne organisation de la structure.

Étape 34 — Propriétés de l'utilisateur — Onglet Membre de



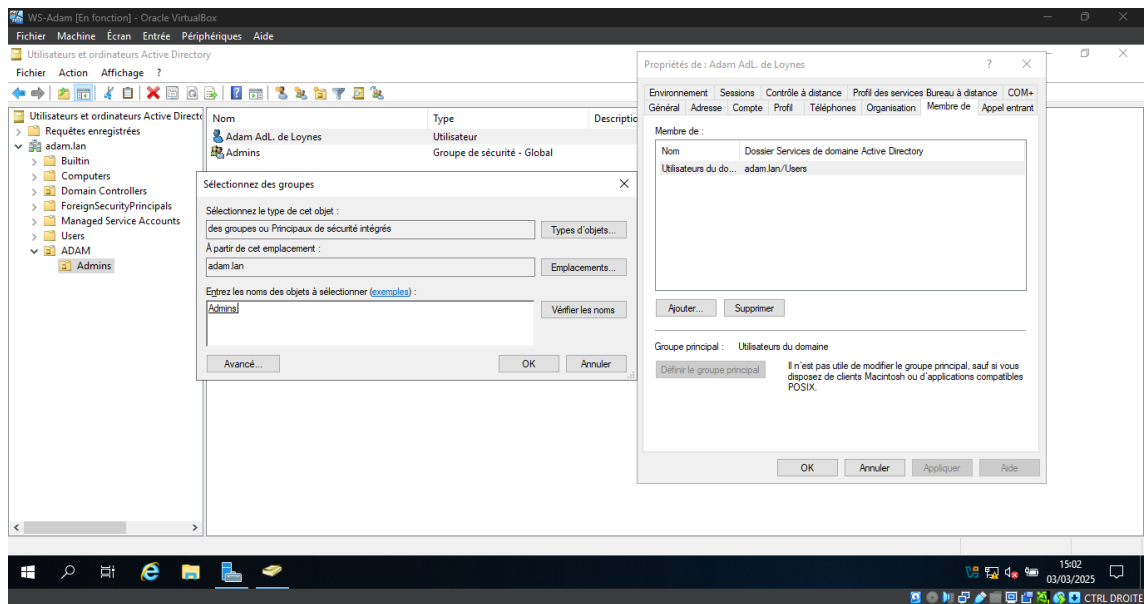
► Ouvrir les Propriétés de l'utilisateur admin → onglet « Membre de ». Cliquer sur « Ajouter » pour assigner l'utilisateur à un groupe AD.

Étape 35 — Recherche du groupe Admins du domaine



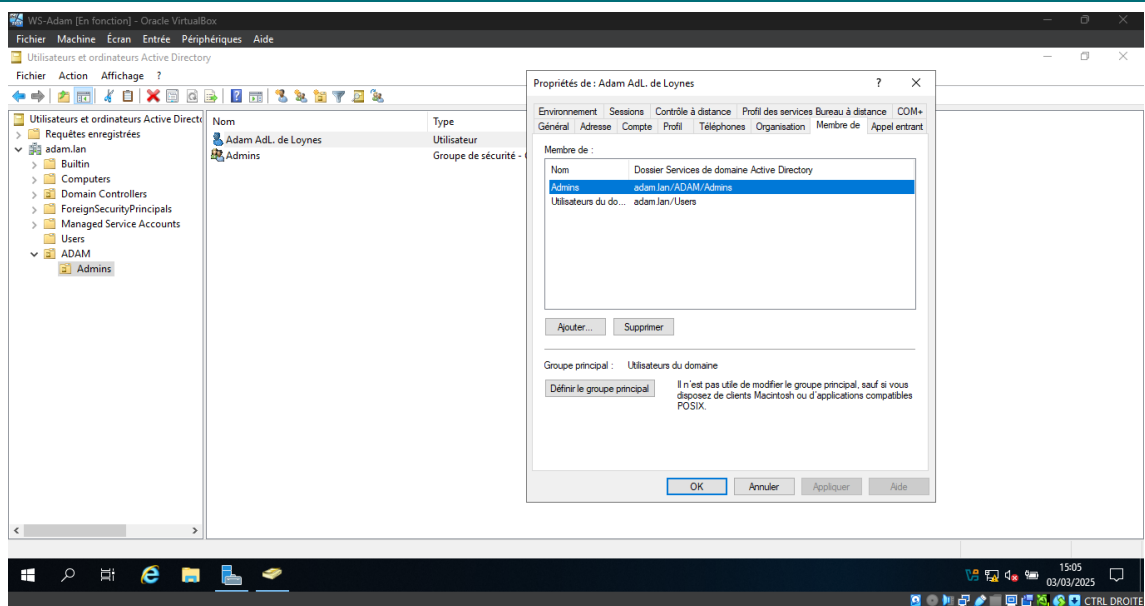
► Dans la fenêtre de sélection, taper « Admins du domaine » (ou « Domain Admins »), cliquer sur « Vérifier les noms » pour résoudre le nom, puis sur OK. Ce groupe donne des droits d'administration étendus sur tout le domaine.

Étape 36 — Confirmation de l'appartenance au groupe



► Le groupe « Admins du domaine » apparaît maintenant dans la liste des groupes de l'utilisateur. Confirmer en cliquant sur OK. L'utilisateur a maintenant les droits administrateur sur le domaine.

Étape 37 — Vérification dans la console AD

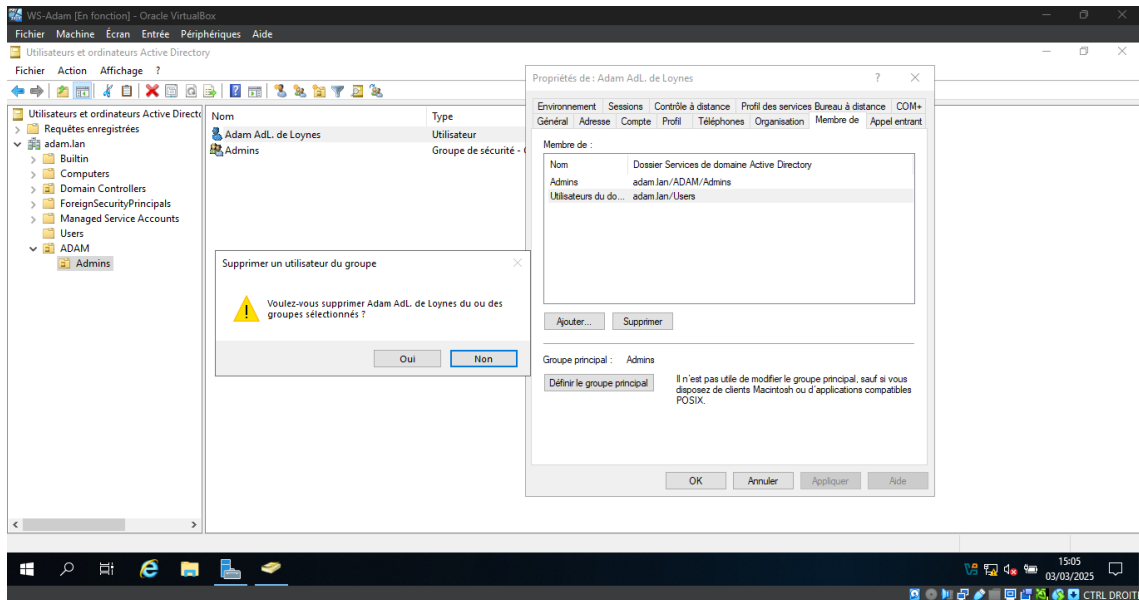


► Dans la console AD, vérifier que l'utilisateur apparaît bien dans les membres du groupe Admins du domaine. La modification est immédiatement active — aucun redémarrage n'est nécessaire.

PARTIE 6 — Activation de la Corbeille Active Directory

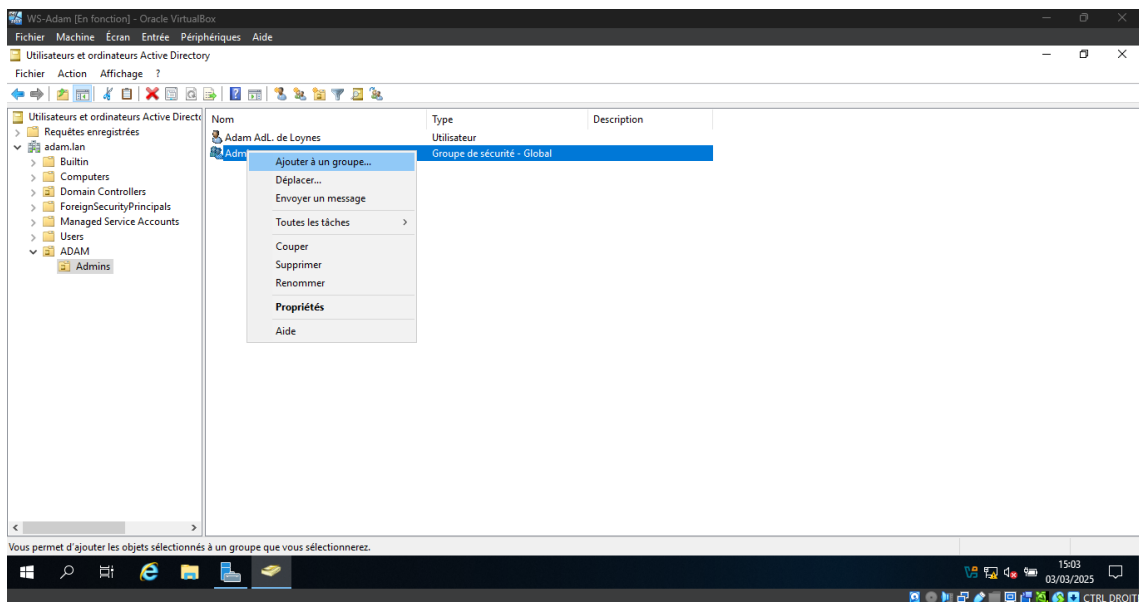
La corbeille AD permet de restaurer des objets supprimés (utilisateurs, UO, groupes) sans restaurer une sauvegarde complète. Elle doit être activée manuellement — l'opération est définitive et irréversible.

Étape 38 — Centre d'administration AD — Activation corbeille



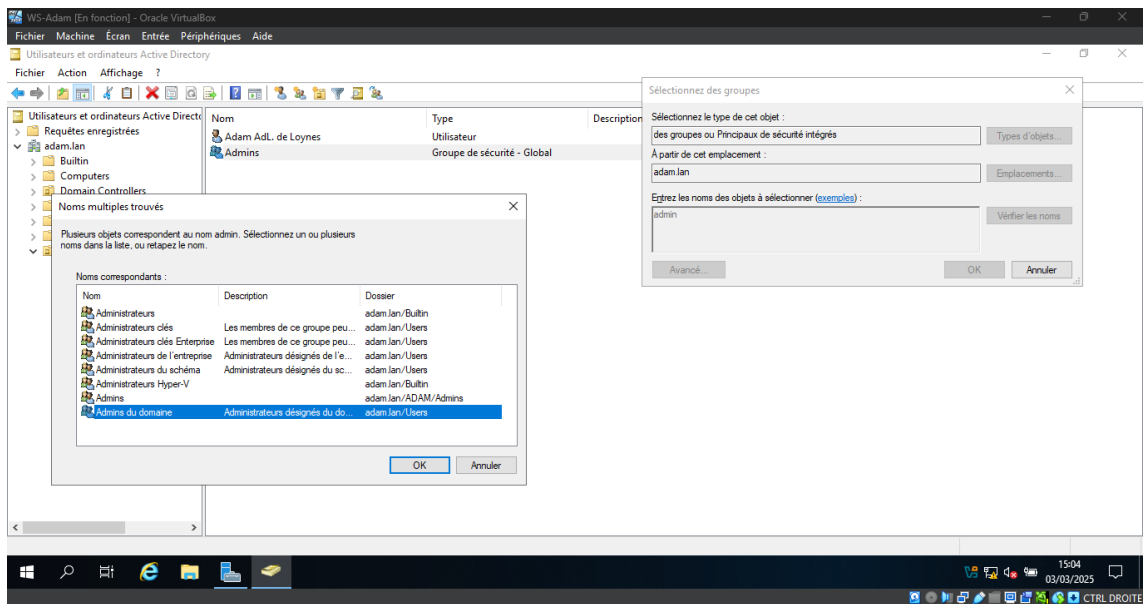
► Dans le Gestionnaire de serveur → Outils → « Centre d'administration Active Directory ». Dans le panneau de droite, cliquer sur « Activer la corbeille ».

Étape 39 — Confirmation de l'activation



► Une boîte de dialogue avertit que l'activation est irréversible. Cliquer sur OK pour confirmer. Après l'activation, actualiser la console (F5) pour voir apparaître le conteneur « Deleted Objects ».

Étape 40 — Vue de la console post-activation

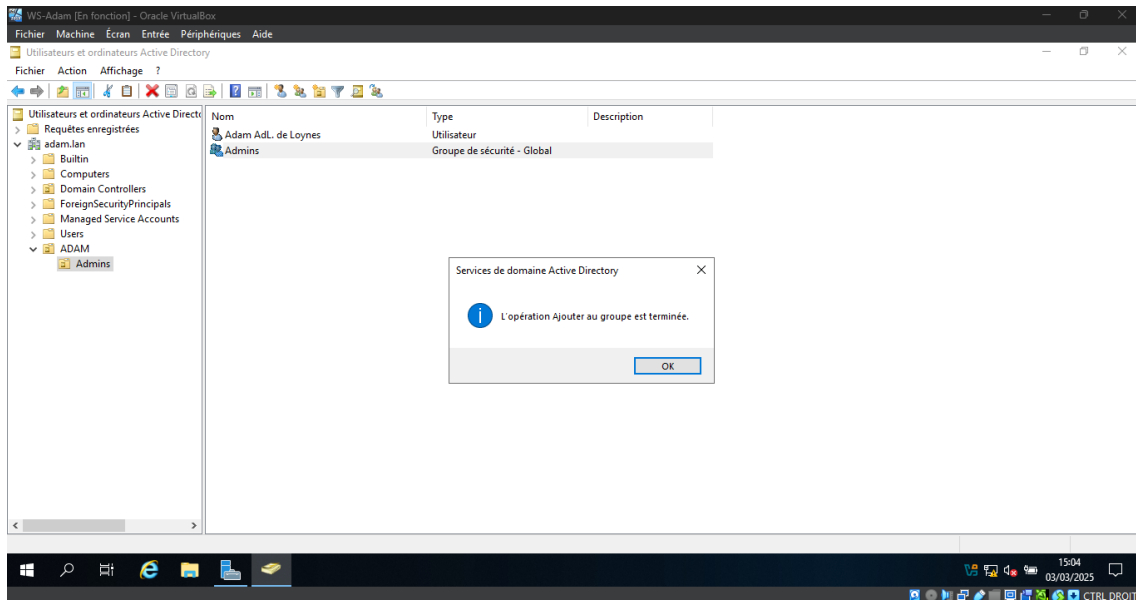


► Après actualisation, le conteneur « Deleted Objects » est visible dans l'arborescence du domaine. Tout objet supprimé sera désormais déplacé dans ce conteneur pendant une période de rétention (60 jours par défaut) avant suppression définitive.

PARTIE 7 — Création des sous-UO pour les Ordinateurs

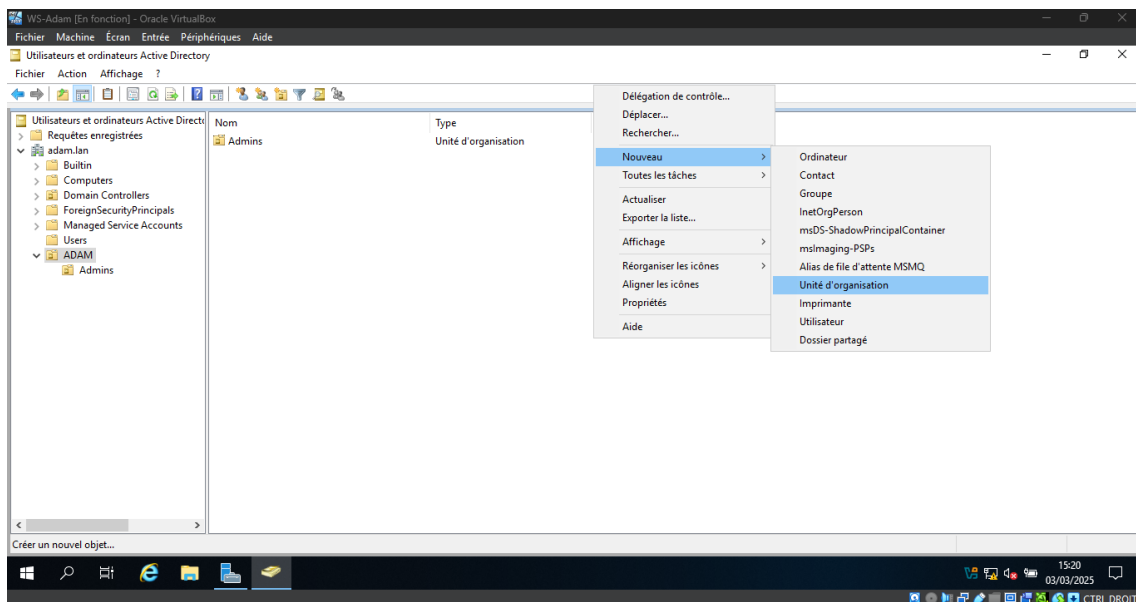
Les sous-UO permettent d'organiser les postes clients par service (Réseau, Direction, Compta, Labo) et d'appliquer des GPO spécifiques à chaque département.

Étape 41 — Création de l'UO Ordinateurs



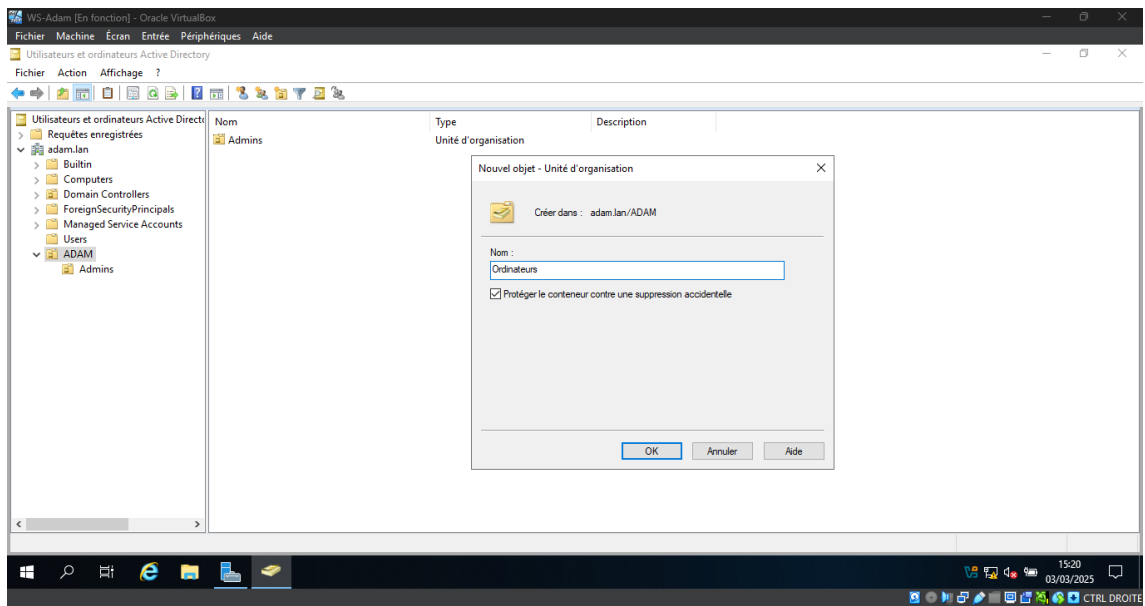
Dans l'UO racine (ADAM), créer une nouvelle UO nommée « Ordinateurs ». Elle servira de conteneur pour toutes les sous-UO par service.

Étape 42 — Confirmation (pop-up AD)



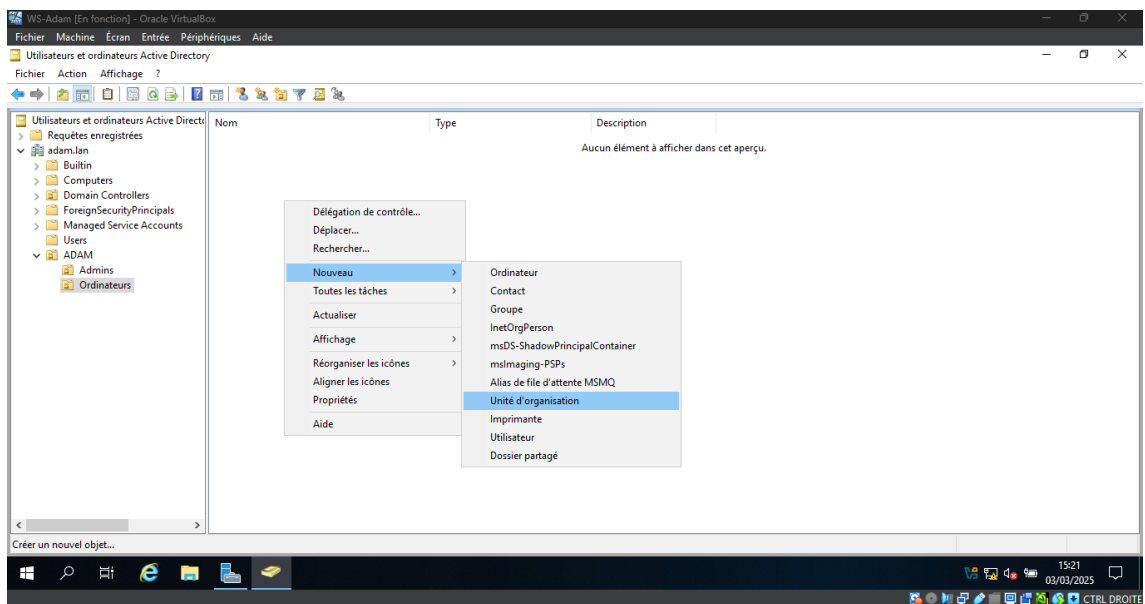
La pop-up de confirmation indique que l'objet a bien été créé. Cliquer sur OK pour fermer.

Étape 43 — Création de la sous-OU Direction



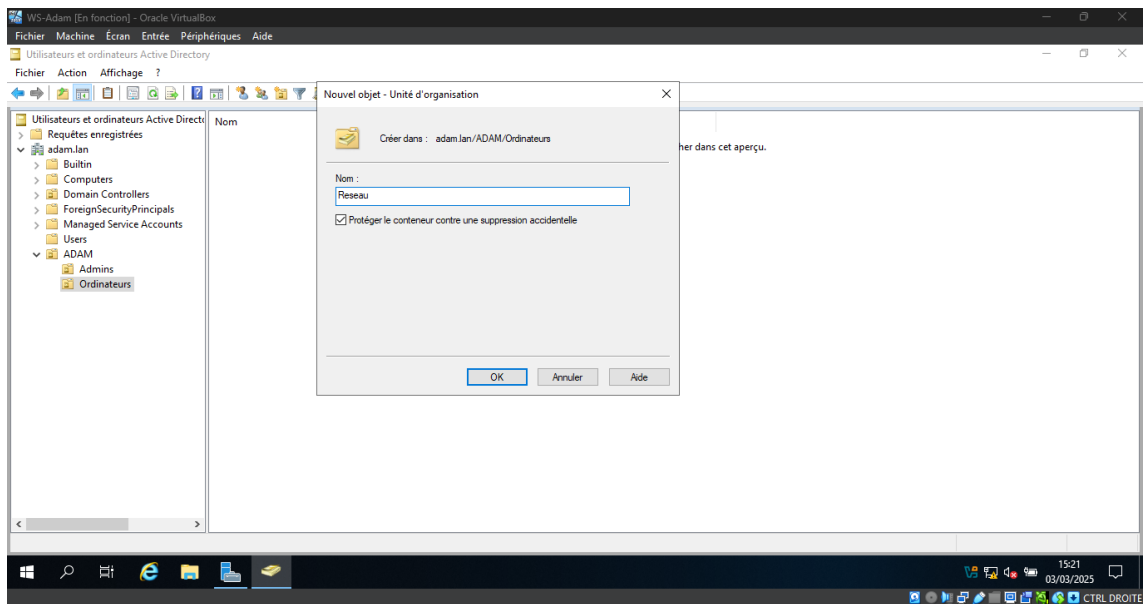
► Dans l'OU Ordinateurs, créer une sous-OU nommée « Direction ». Répéter cette opération pour chaque service : Réseau, Compta, Labo.

Étape 44 — Navigation dans l'arborescence



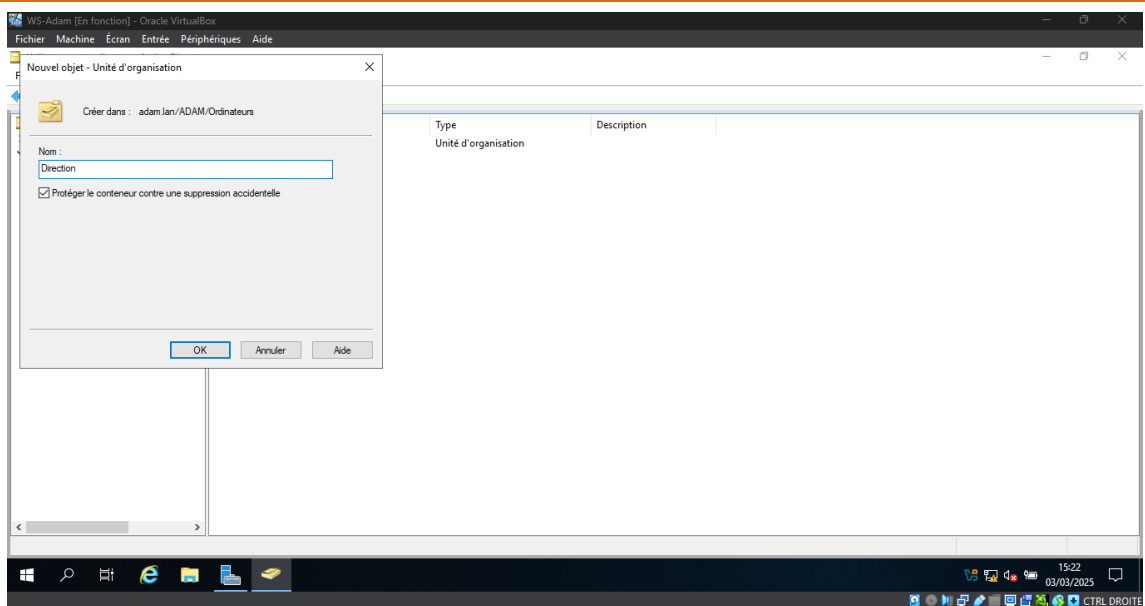
► En naviguant dans l'arborescence AD, vérifier que toutes les sous-OU sont correctement créées sous Ordinateurs. L'arborescence doit refléter la structure organisationnelle de l'entreprise ou du lab.

Étape 45 — Sous-VO Réseau



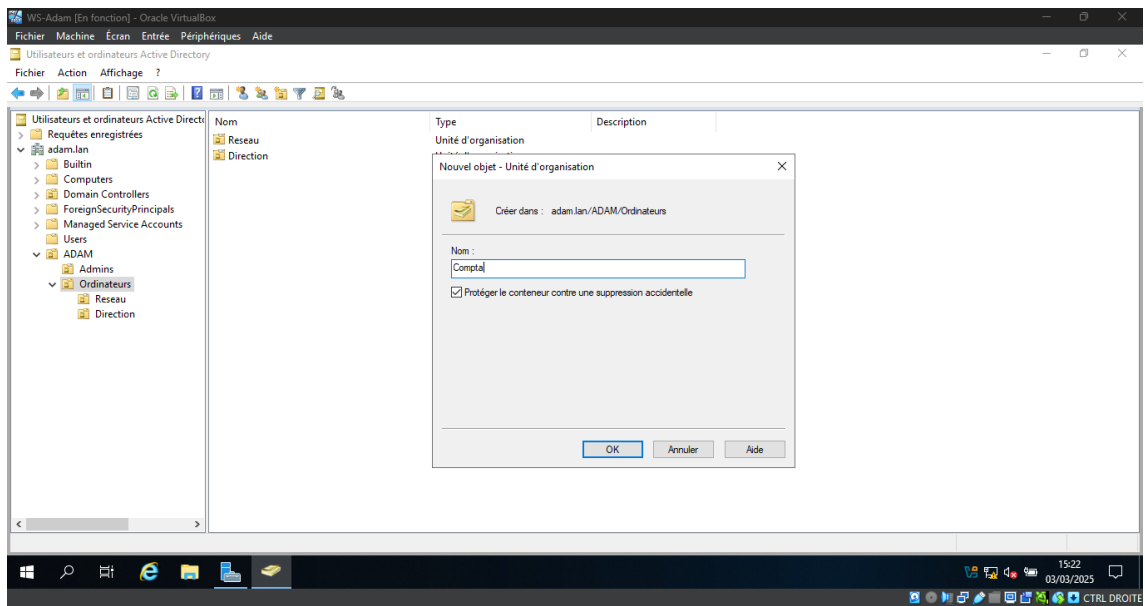
► Créer la sous-VO « Réseau » (sans accent pour éviter les problèmes de compatibilité dans les scripts PowerShell ou les outils tiers).

Étape 46 — Sous-VO Compta



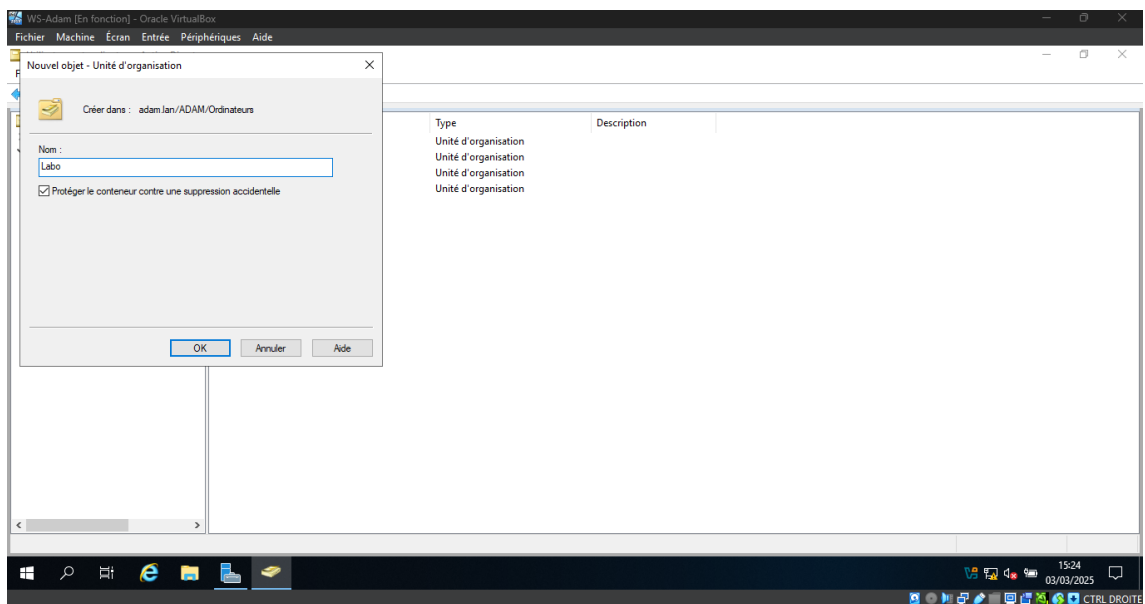
► Créer la sous-VO « Compta ». Ces VO seront utilisées pour affecter les postes clients lors de leur jonction au domaine.

Étape 47 — Sous-UO Labo



► Créer la sous-UO « Labo » pour les machines de test ou les postes d'atelier informatique. La structure finale sous Ordinateurs doit contenir : Direction, Réseau, Compta, Labo.

Étape 48 — Sous-UO Labo — Nommage

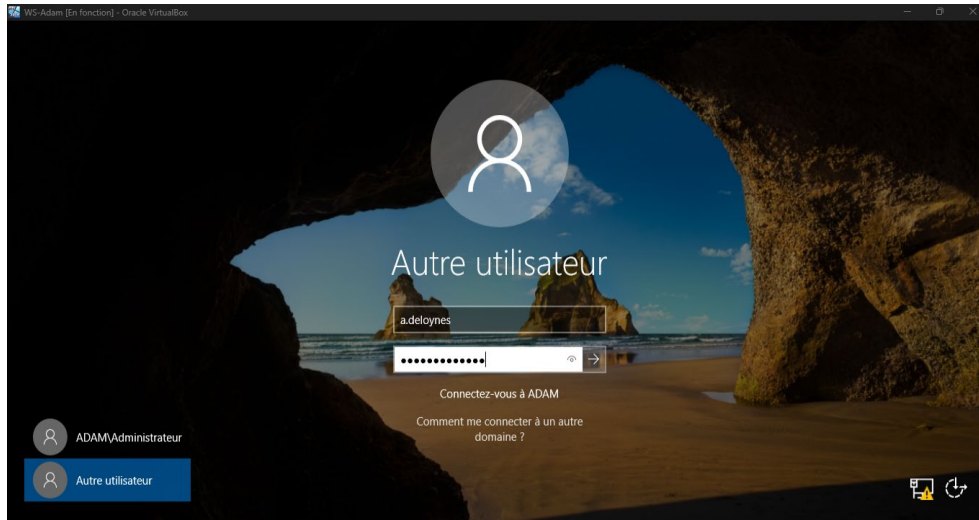


► Confirmer le nom « Labo » et cliquer OK. La structure des UO Ordinateurs est maintenant complète et prête à accueillir les postes clients du domaine.

PARTIE 8 — Dossier partagé Échanges et GPO de mappage lecteur

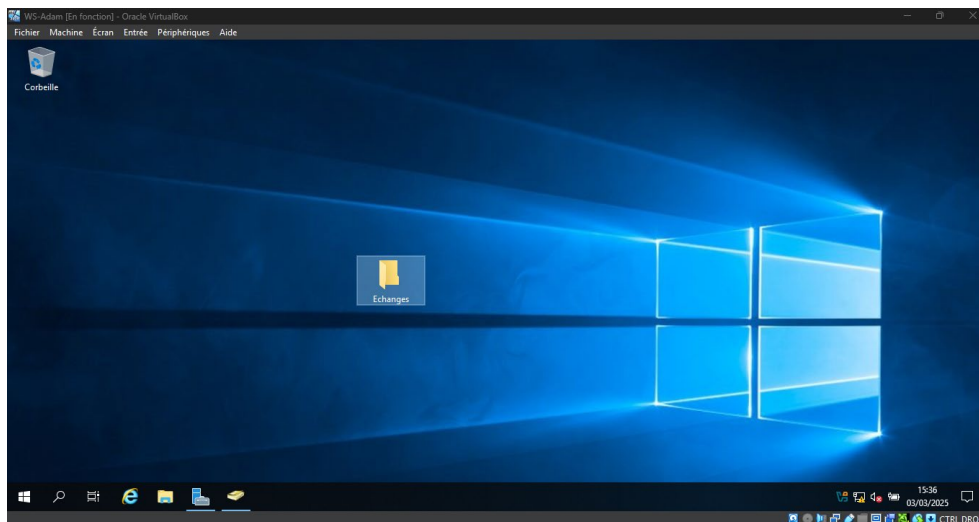
■ Cette section configure un dossier partagé réseau et une GPO pour monter automatiquement le lecteur Z: sur tous les postes membres du groupe Admins à l'ouverture de session.

Étape 49 — Connexion avec le compte admin



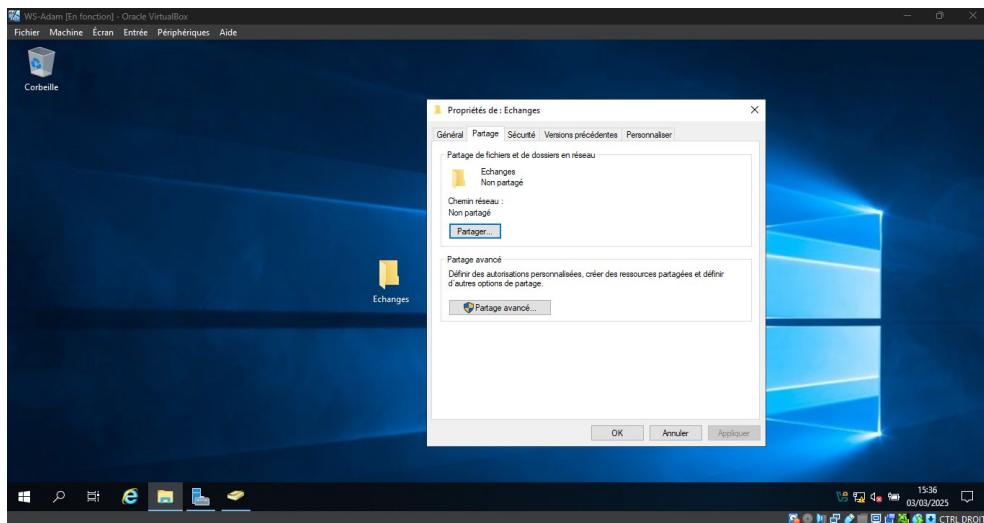
► Se déconnecter du compte Administrateur local et se connecter avec le compte admin du domaine (ex. ADAM\a.deloynes). Ce compte a été ajouté au groupe Admins du domaine — il a les droits nécessaires pour la suite des opérations.

Étape 50 — Création du dossier Echanges sur le bureau



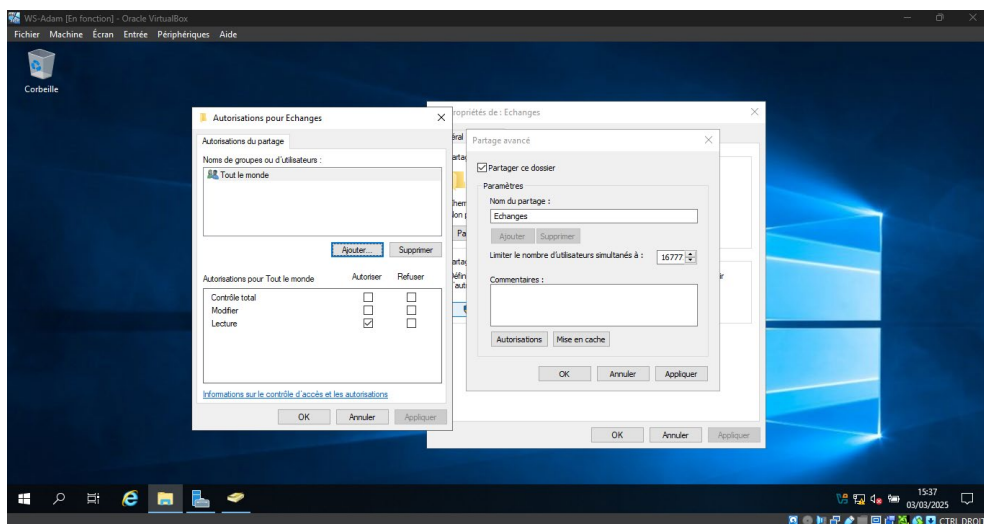
► Sur le bureau, créer un nouveau dossier nommé « Echanges » (sans accent de préférence pour la compatibilité réseau). Ce dossier sera partagé sur le réseau local du domaine.

Étape 51 — Propriétés du dossier — Onglet Partage



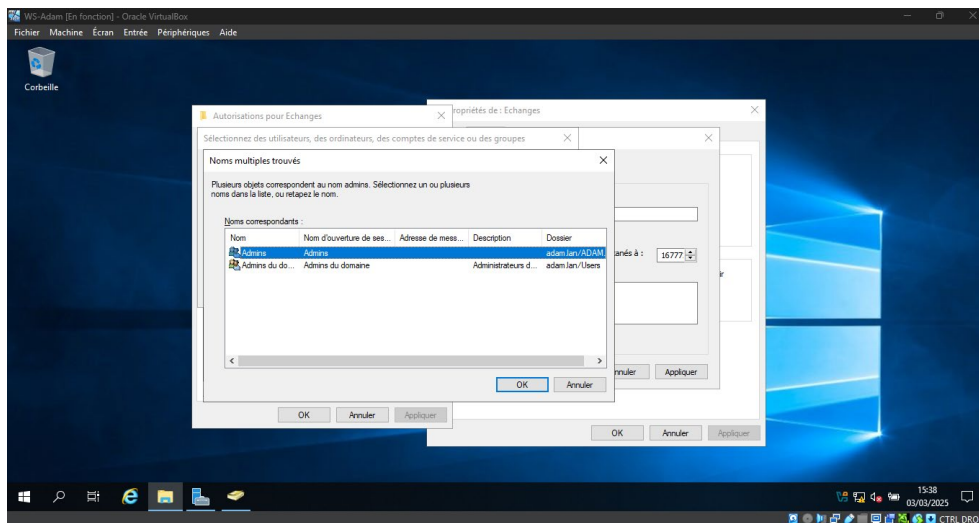
► Clic droit sur le dossier Echanges → Propriétés → onglet Partage → cliquer sur « Partage avancé ». Le partage avancé permet de contrôler précisément les autorisations d'accès au niveau du partage réseau.

Étape 52 — Configuration des autorisations — Ajout du groupe



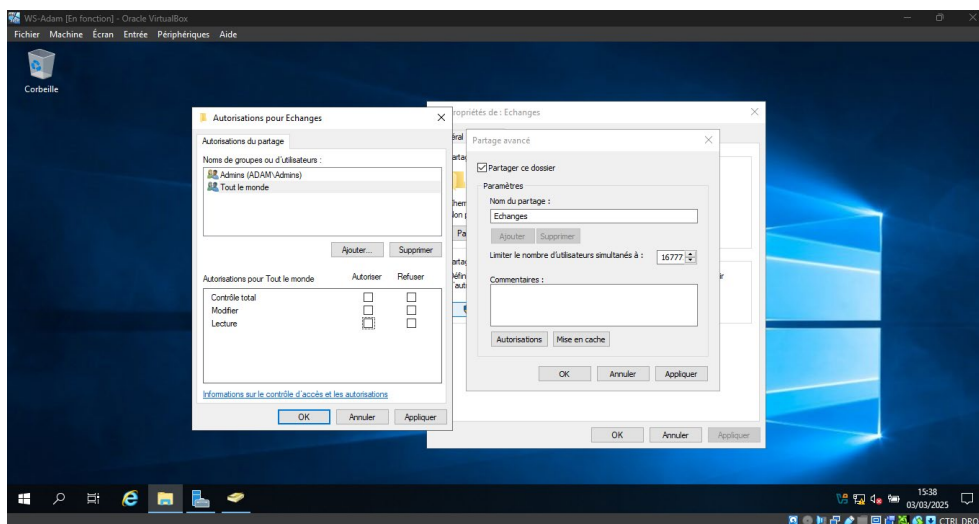
► Cocher « Partager ce dossier », cliquer sur « Autorisations » puis « Ajouter ». Dans la fenêtre de sélection, rechercher le groupe « Admins » du domaine et l'ajouter.

Étape 53 — Autorisations multiples — Sélection du groupe



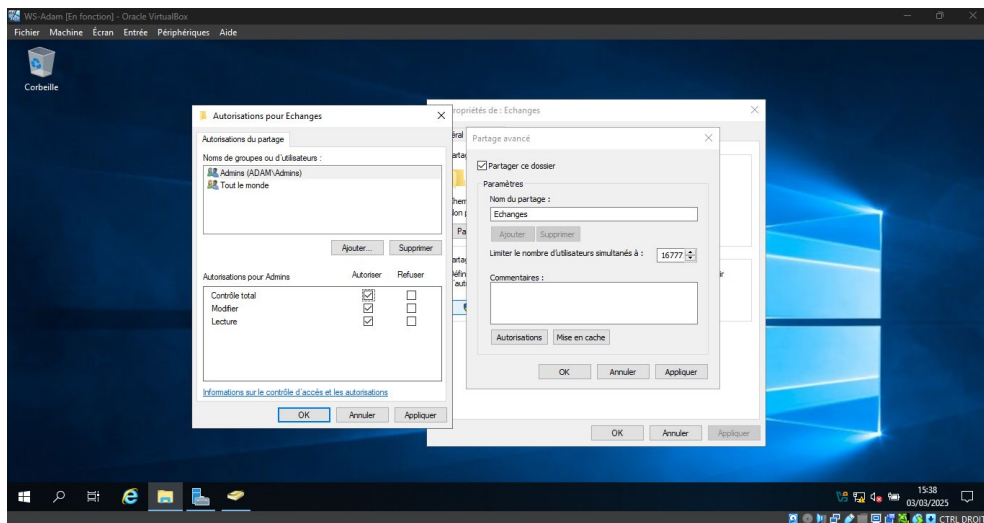
► Si plusieurs résultats correspondent (ex. Admins locaux vs Admins du domaine), sélectionner le groupe du domaine ADAM\Admins. Cliquer sur OK pour confirmer la sélection.

Étape 54 — Droits complets pour Admins



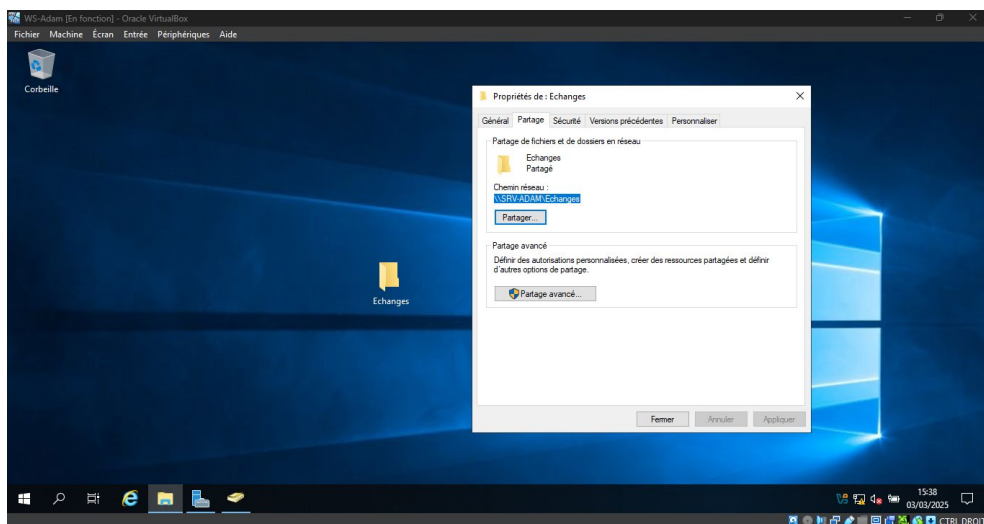
► Avec le groupe Admins sélectionné dans la liste, cocher « Contrôle total ». Cela accorde automatiquement Modification et Lecture également. Sélectionner « Tout le monde » et décocher toutes ses autorisations (ou le supprimer).

Étape 55 — Retrait des droits pour Tout le monde



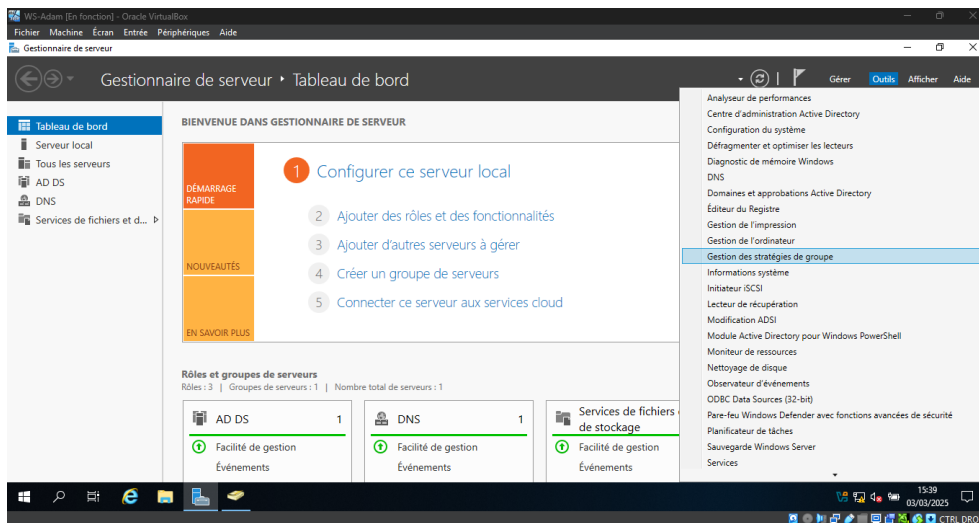
► Sélectionner « Tout le monde » et cliquer sur Supprimer pour retirer ce groupe de la liste des autorisations. Seul le groupe Admins doit avoir accès au dossier partagé.

Étape 56 — Chemin réseau du partage



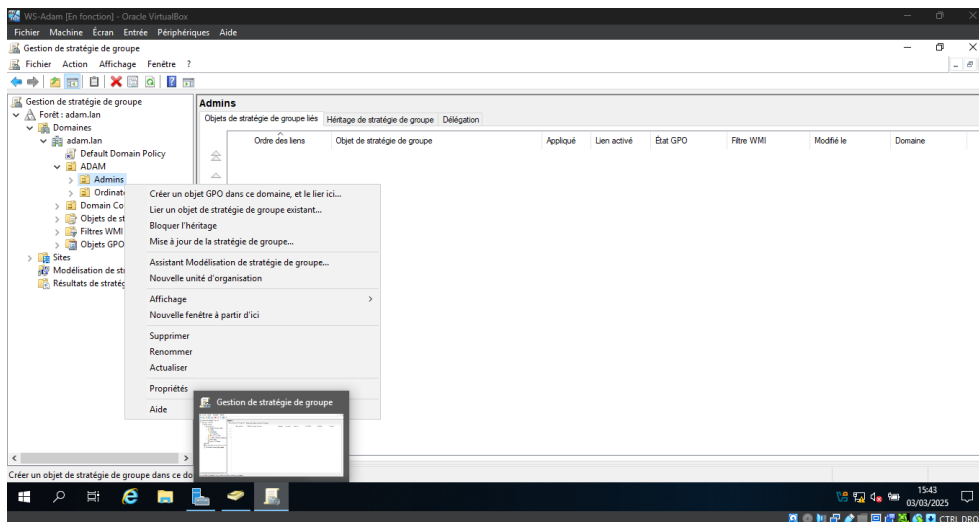
► Retourner dans l'onglet Partage des propriétés du dossier. Le chemin réseau (ex. \\SRV-ADAM\Echanges) est affiché. Noter ce chemin — il sera utilisé dans la configuration de la GPO.

Étape 57 — Gestionnaire de stratégie de groupe (GPMC)



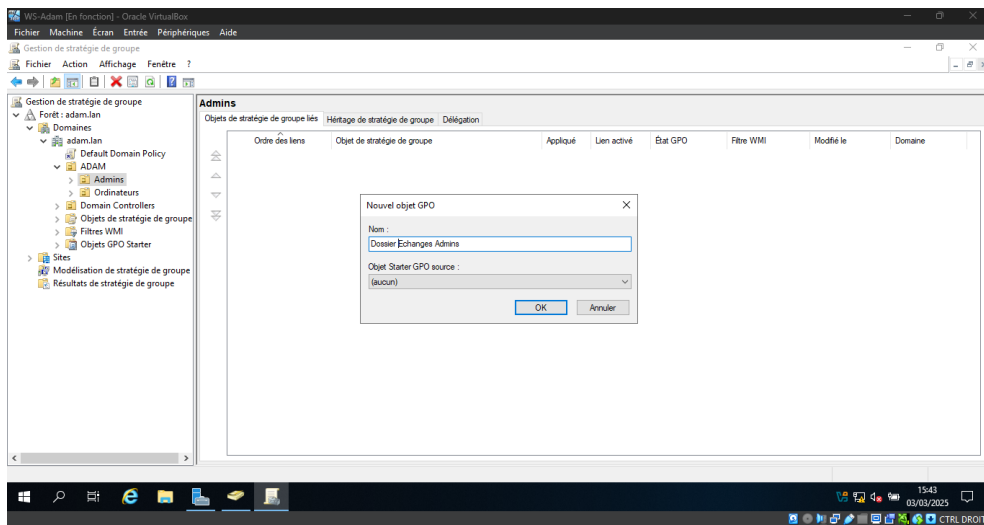
► Dans le Gestionnaire de serveur → Outils → « Gestionnaire de stratégie de groupe ». La console GPMC s'ouvre avec l'arborescence du domaine adam.lan.

Étape 58 — Créer un objet GPO dans l'UO Admins



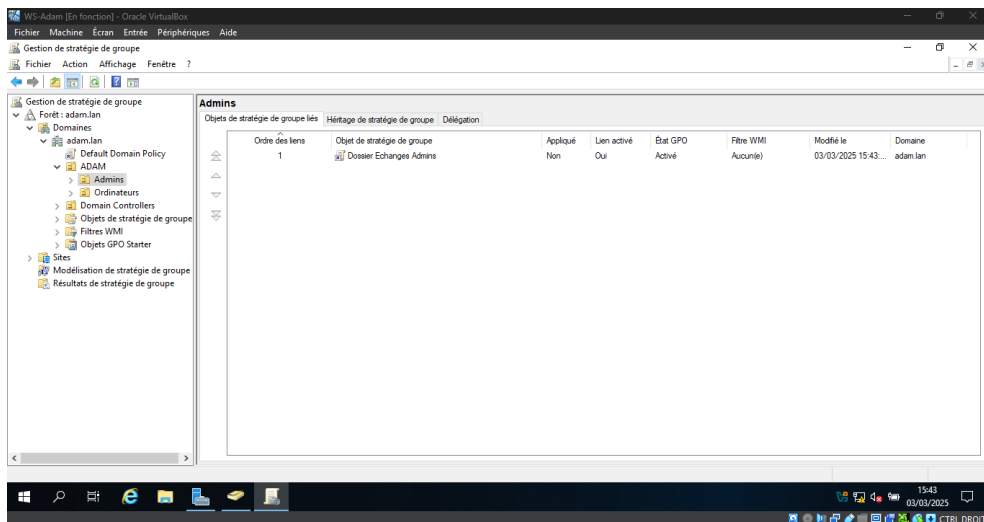
► Dans la console GPMC, naviguer vers l'UO Admins (adam.lan → ADAM → Admins). Faire un clic droit → « Créer un objet GPO dans ce domaine, et le lier ici ».

Étape 59 — Nommage de la GPO



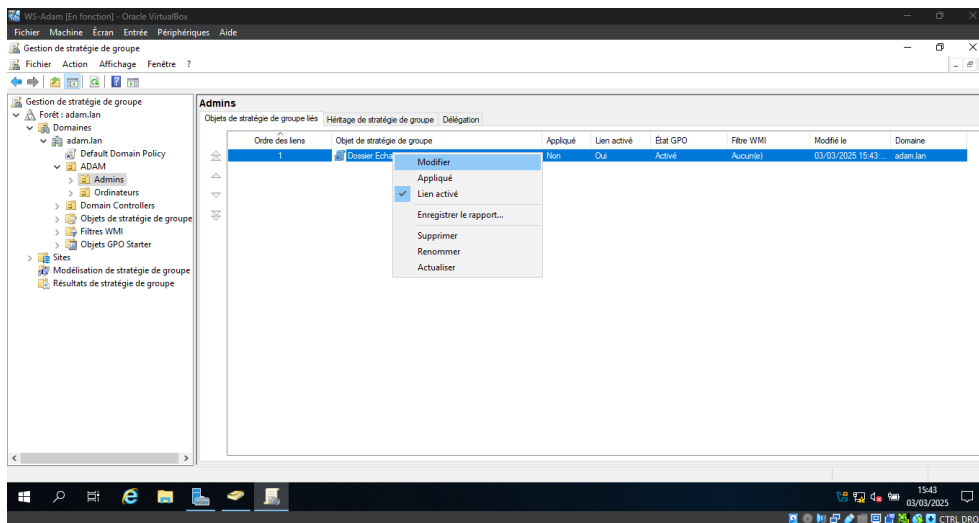
► Nommer la GPO « Dossier Echanges Admins » (ou tout nom explicite décrivant son rôle). Cliquer sur OK. La GPO est automatiquement liée à l'UO Admins.

Étape 60 — GPO créée — Modifier



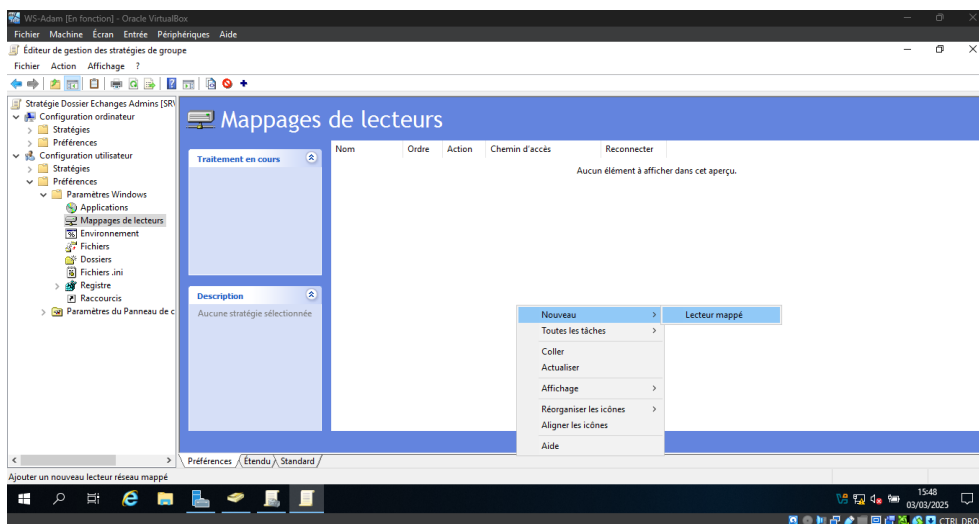
► La GPO apparaît dans la liste sous l'UO Admins. Faire un clic droit dessus → « Modifier » pour ouvrir l'éditeur de stratégie de groupe.

Étape 61 — Navigation dans l'éditeur — Mappage de lecteurs



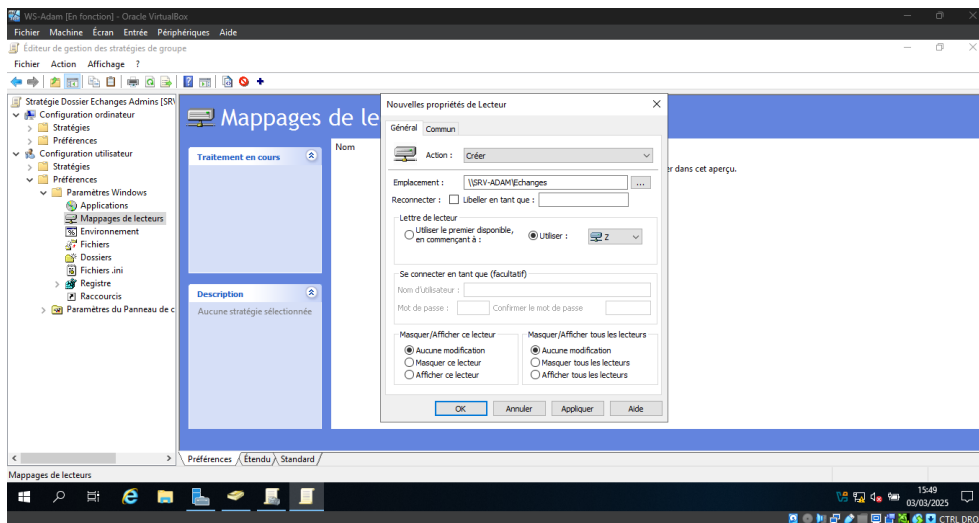
► Dans l'éditeur de GPO, naviguer vers : Configuration utilisateur → Préférences → Paramètres Windows → « Mappages de lecteurs ». Faire un clic droit dans le panneau de droite → Nouveau → Lecteur mappé.

Étape 62 — Configuration du lecteur mappé



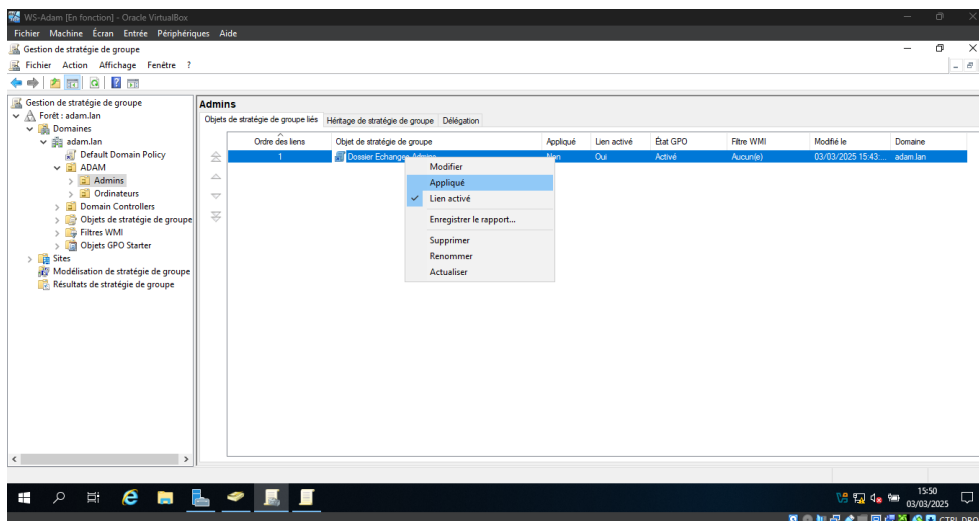
► Configurer le mappage : Action = Créer ; Emplacement = coller le chemin réseau (\\SRV-ADAM\Echanges) ; Étiquette = Echanges ; Lettre de lecteur = Z. La lettre Z est utilisée par convention pour les lecteurs réseau de fin d'alphabet, évitant les conflits avec les lecteurs locaux.

Étape 63 — Mappage de lecteur configuré



► Le mappage du lecteur Z: vers \\SRV-ADAM\Echanges est maintenant configuré dans la GPO. Fermer l'éditeur de GPO. La GPO sera appliquée automatiquement aux membres du groupe Admins à leur prochaine connexion.

Étape 64 — Mise à jour forcée des stratégies

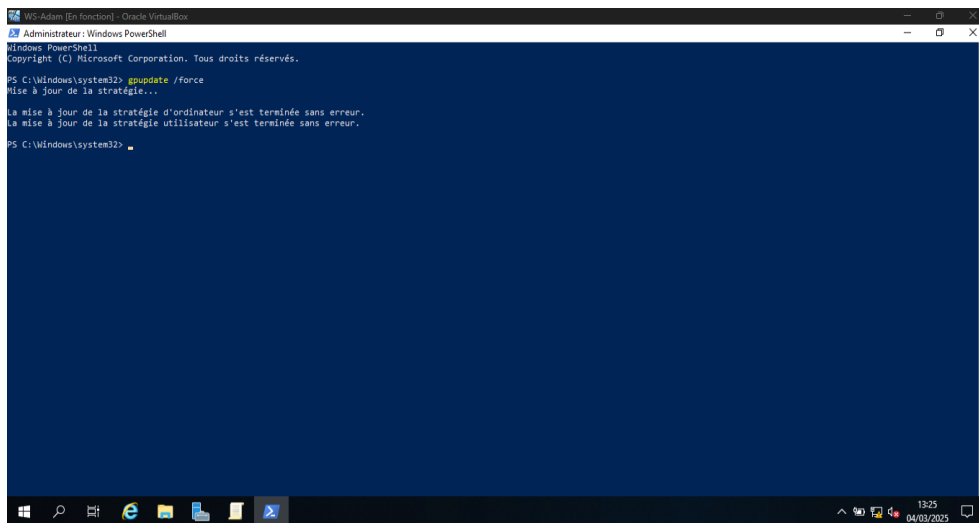


► Ouvrir PowerShell en tant qu'Administrateur et exécuter :

```
gpupdate /force
```

Cette commande force l'actualisation immédiate des GPO sans attendre le délai de rafraîchissement automatique (90 minutes par défaut). Vérifier que le résultat indique « La mise à jour de la stratégie d'ordinateur a réussi » et « La mise à jour de la stratégie utilisateur a réussi ».

Étape 65 — Vérification du lecteur réseau



```
WS-Adam [En fonction] - Oracle VM VirtualBox
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

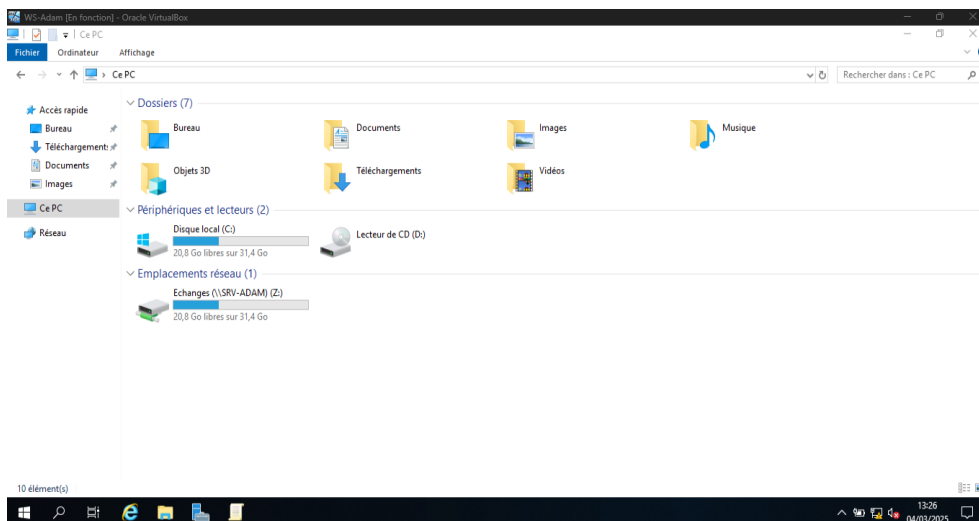
PS C:\Windows\system32> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Windows\system32>
```

► Ouvrir l'Explorateur de fichiers : le lecteur réseau Z: (Echanges) doit apparaître dans « Ce PC ». La GPO de mappage de lecteur est fonctionnelle. Les utilisateurs du groupe Admins trouveront ce lecteur monté automatiquement à chaque connexion.

Étape 66 — Structure finale du dossier partagé



► Vue finale de l'Explorateur de fichiers confirmant le lecteur Z: mappé et accessible. Le dossier Echanges est désormais disponible en partage réseau pour tous les membres du groupe Admins du domaine adam.lan.