Procédure installation et configuration Windows Server 2025 + Active Directory

Partie 1 : Configuration de la VM Windows Server 2025

1.1 Création de la machine virtuelle

Ressources recommandées :

- ➔ RAM : 4 Go
- ➔ CPU : 2
- ➔ Disque dur : 50 Go
- ➔ ISO Windows Server 2025 : https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2025

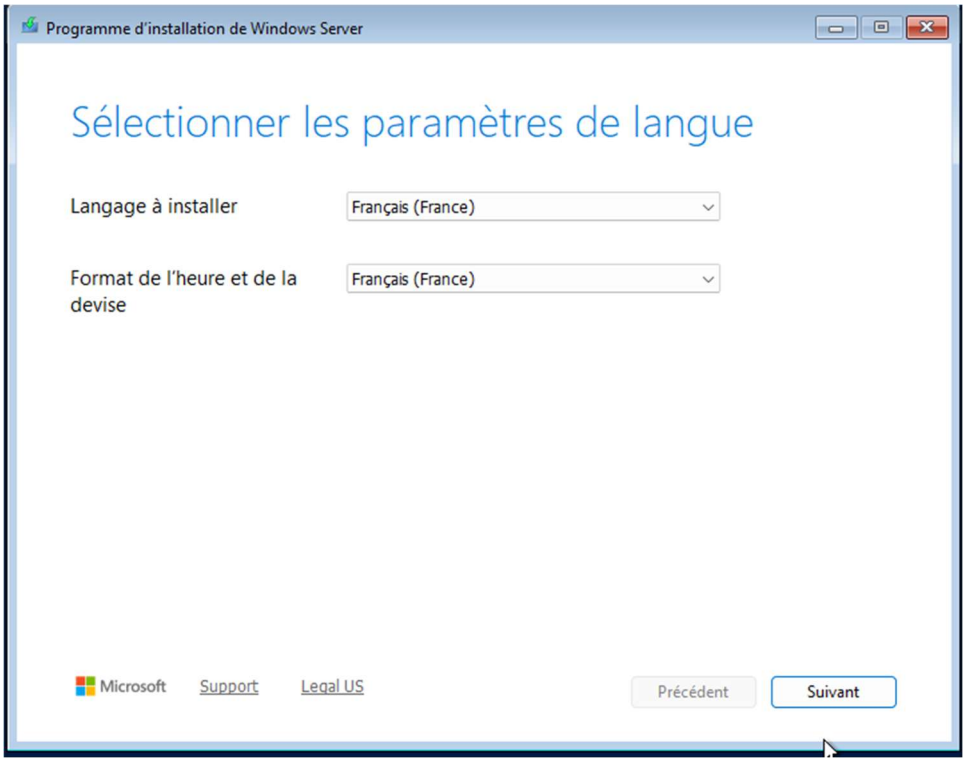
Configuration réseau :

1. Ajouter deux cartes réseau à la machine virtuelle
2. Première carte : Accès par pont (connexion au réseau hôte)
3. Deuxième carte : Réseau interne (isolé, pour le domaine)

1.2 Installation de la machine virtuelle

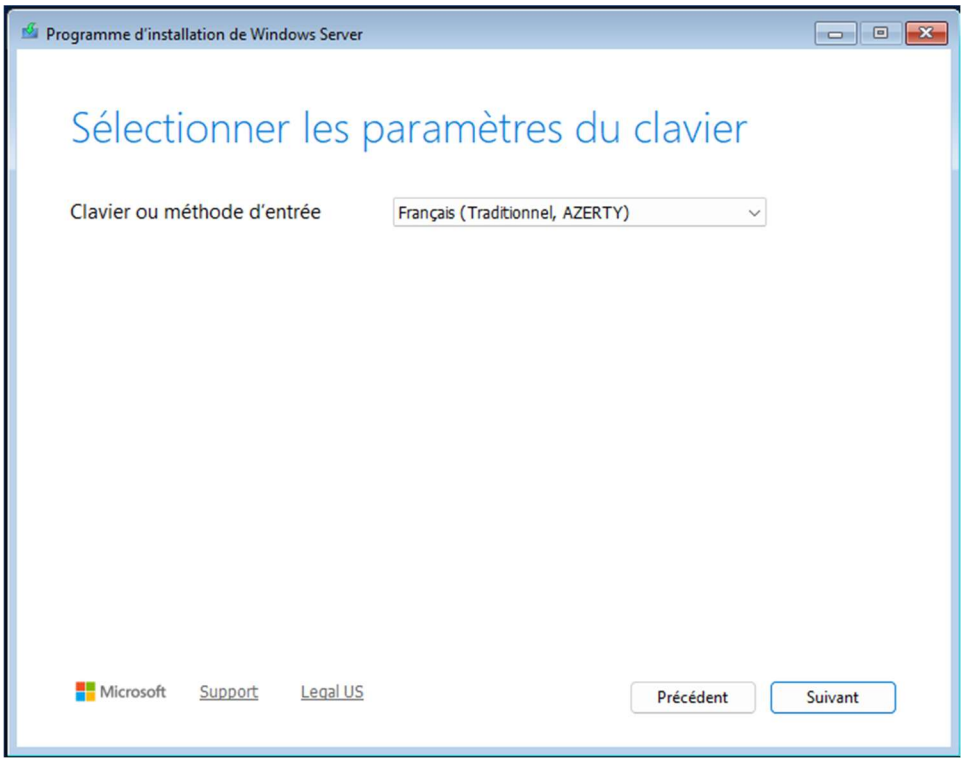
Avant démarrage de la VM, il faudra décocher « Skip unattented installation ».

Une fois la VM lancée, le choix de la langue est demandé



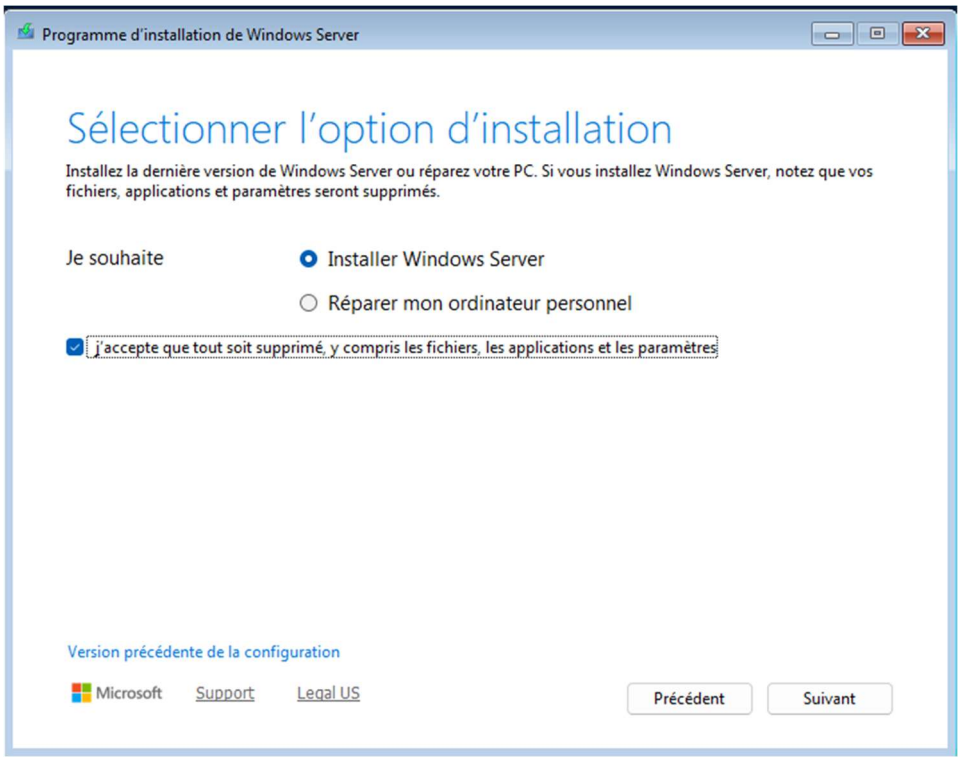
Il faudra dans ce cas renseigner « Français » pour le langage et le format de l'heure.

En cliquant sur « Suivant » la langue du clavier est demandée



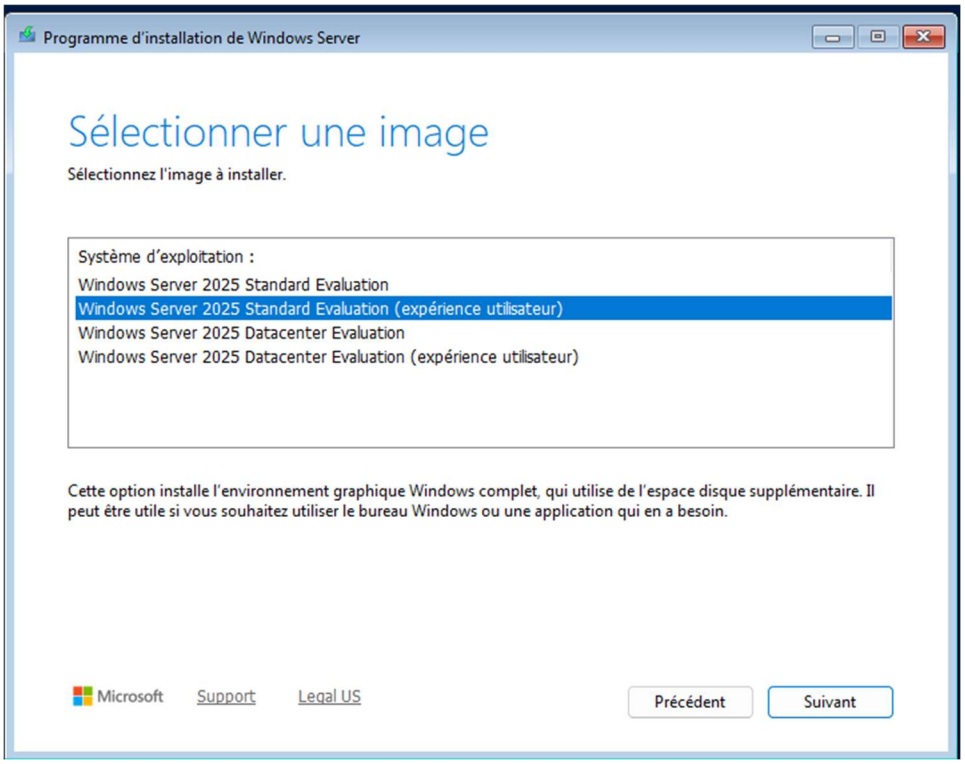
Il faudra aussi choisir « Français AZERTY ».

Ensuite, Windows demandera si l'on veut installer « Windows Server » ou « Réparer l'ordinateur personnel » :



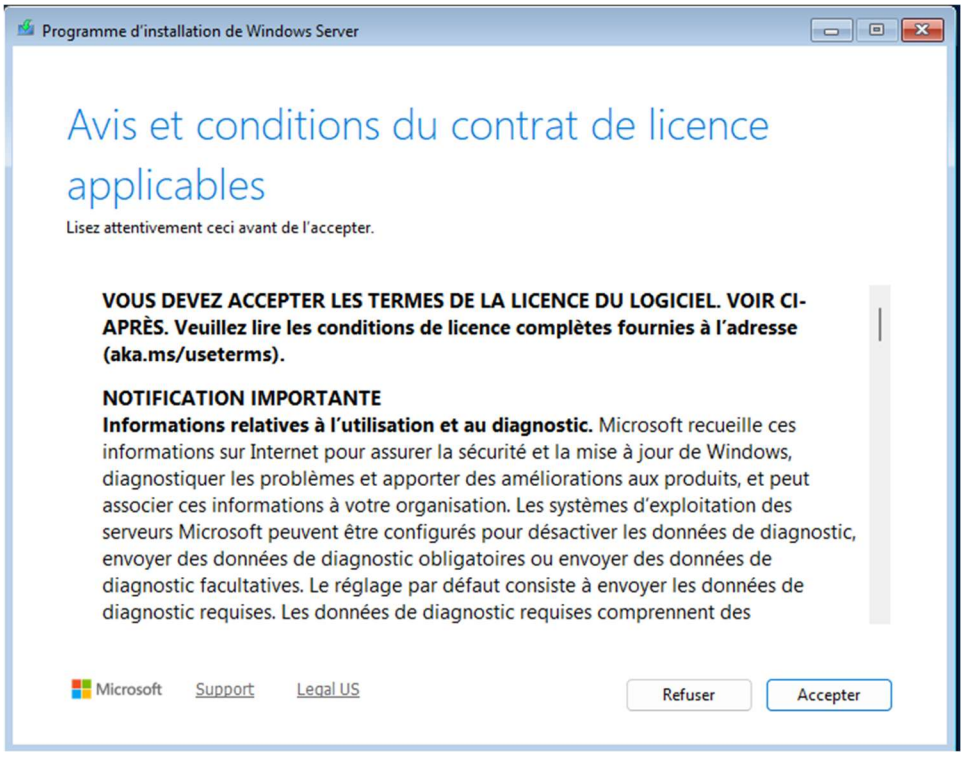
Dans ce cas, nous installons Windows Server en cochant bien la mention « *J'accepte que tout soit supprimé, y compris les fichiers, les applications et les paramètres* »

Ensuite, il faudra choisir l'image correspondante :

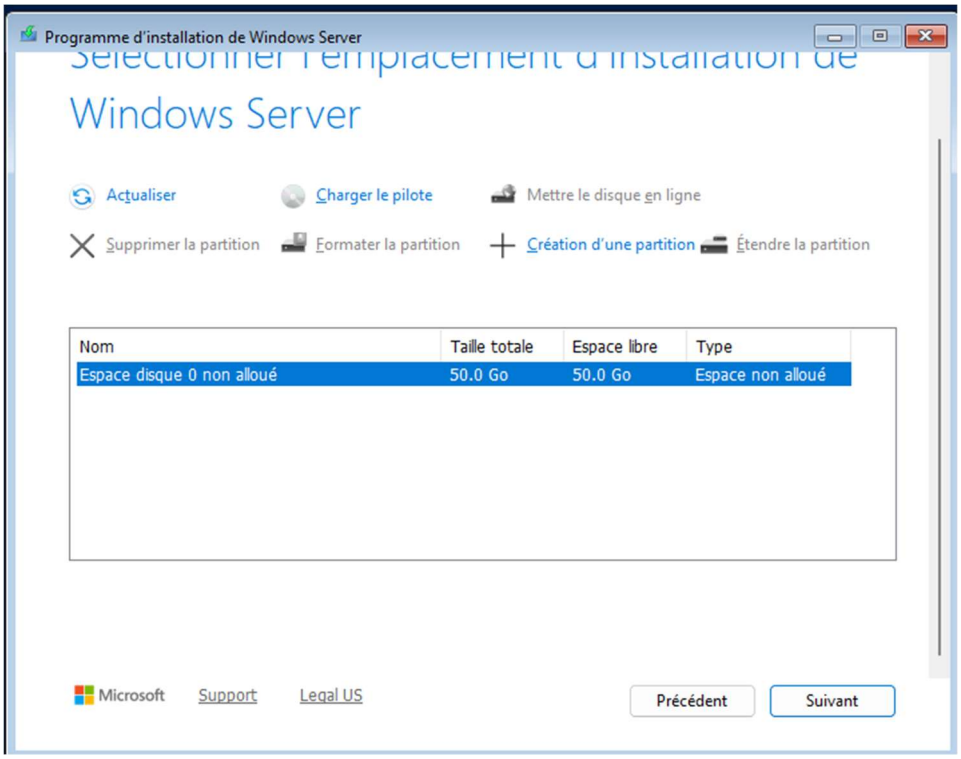


Dans le cas d'un Active Directory, il faudra choisir « Windows Server 2025 Standard Evaluation (expérience utilisateur) ».

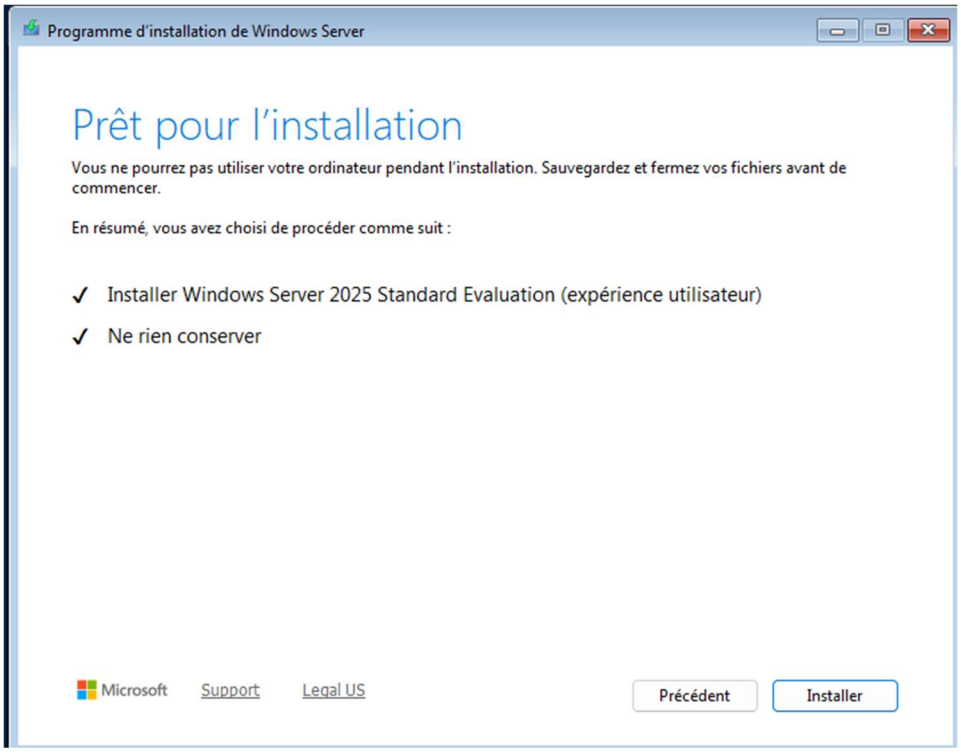
Ensuite il faut accepter les conditions du contrat de licence :



Pour le disque, il faudra choisir le disque dur ou installer Windows Server :

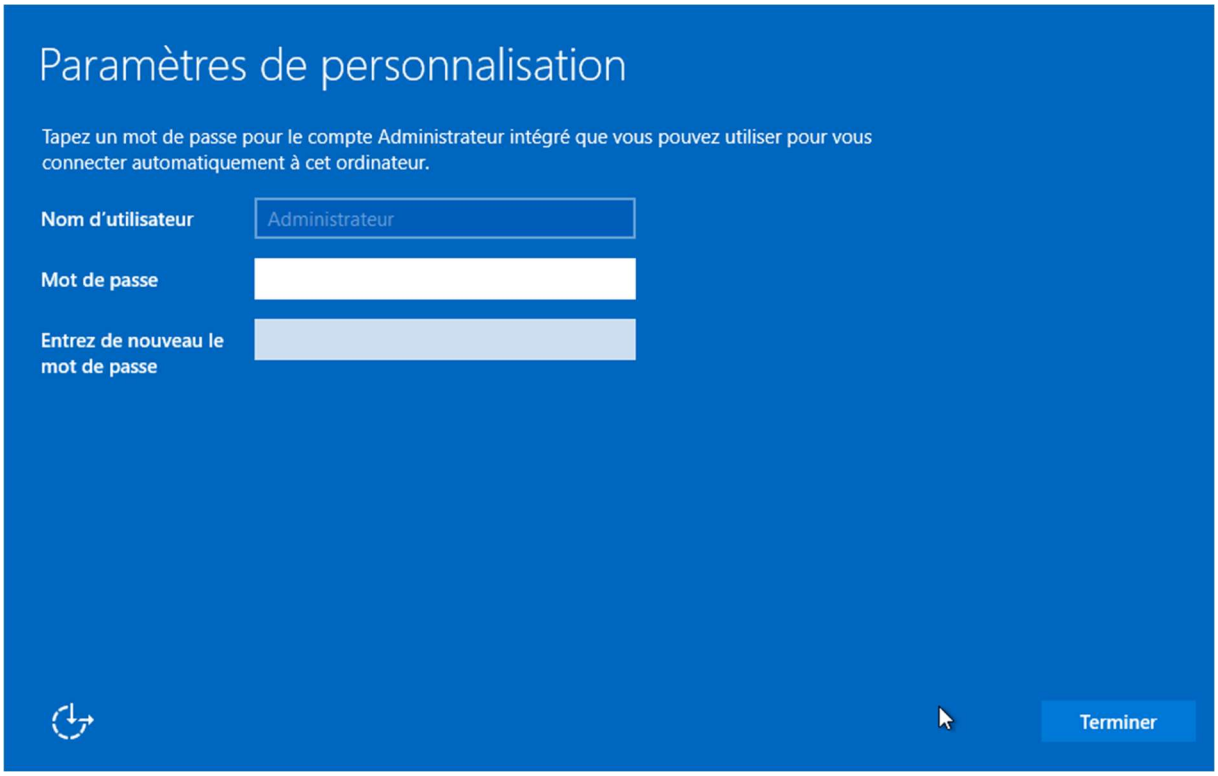


En cliquant sur « Suivant » une page de confirmation d'installation s'affiche



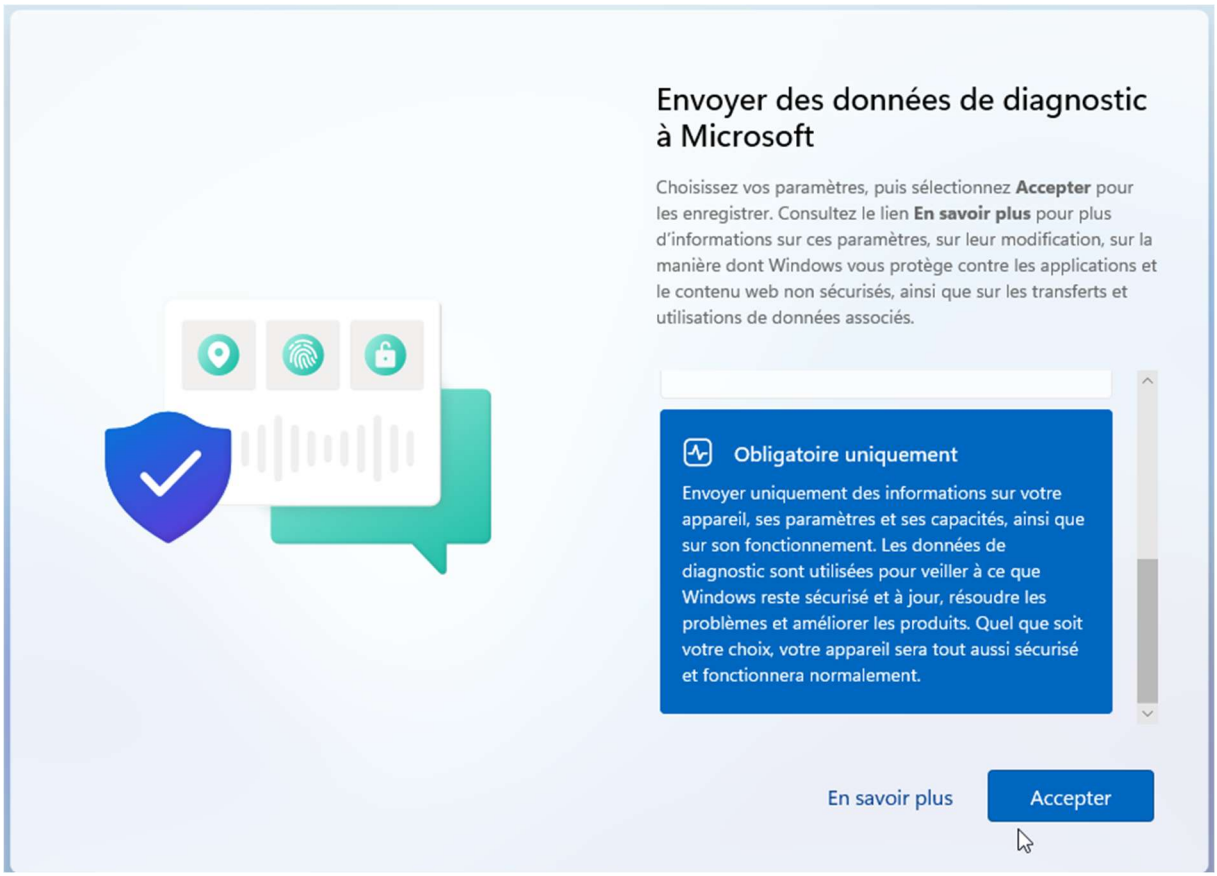
Il faudra cliquer sur « *Installer* » et attendre la fin de l'installation.

A la fin de l'installation, un mot de passe sera demandé :



Il faut utiliser un mot de passe de 7 caractères minimum avec caractères spéciaux.

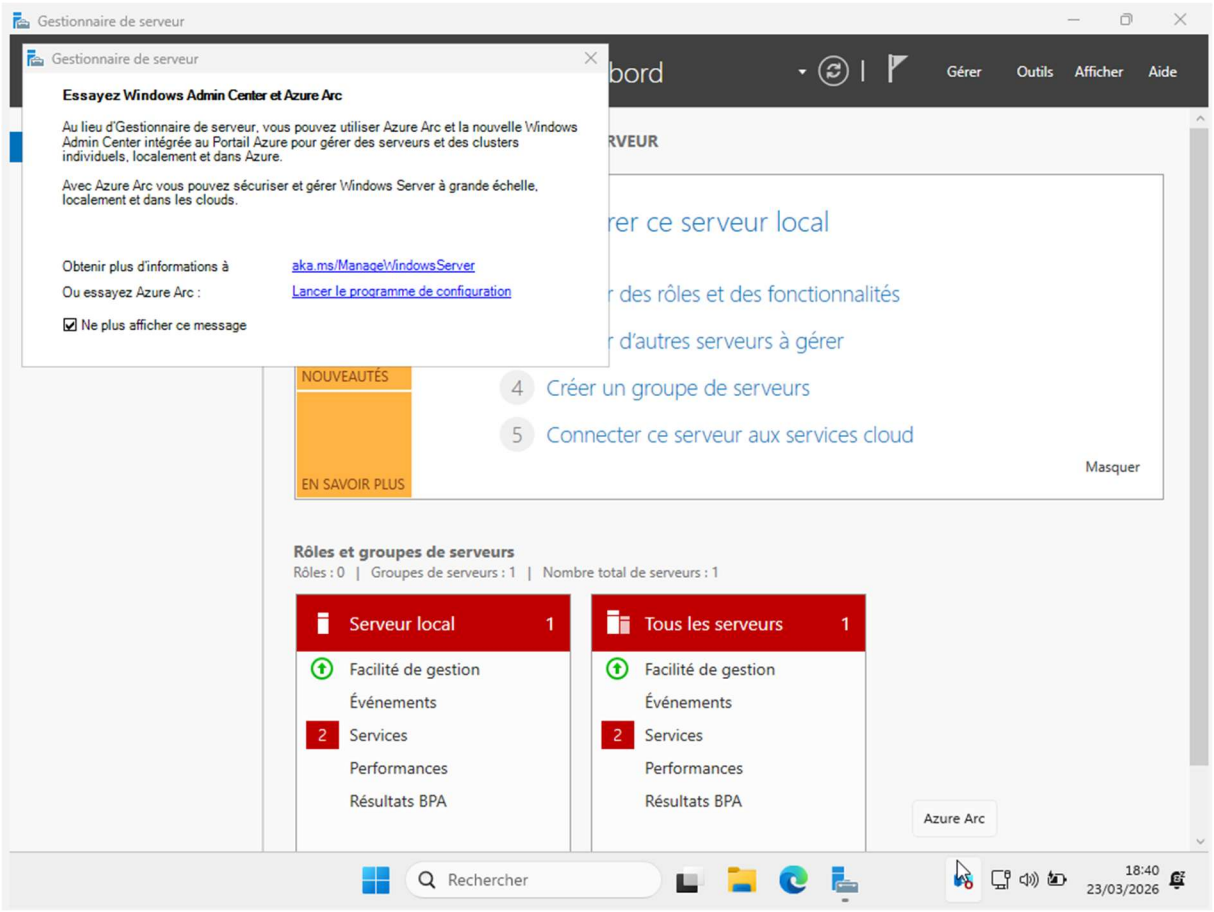
En cliquant sur « Terminer », Windows demandera à récupérer des informations :



Il faut choisir « Obligatoire uniquement » et Accepter.

Au redémarrage ou au verrouillage de la session, il faudra cliquer Ctrl+Suppr (droite) au lieu de Ctrl+Alt+Suppr pour déverrouiller la session.

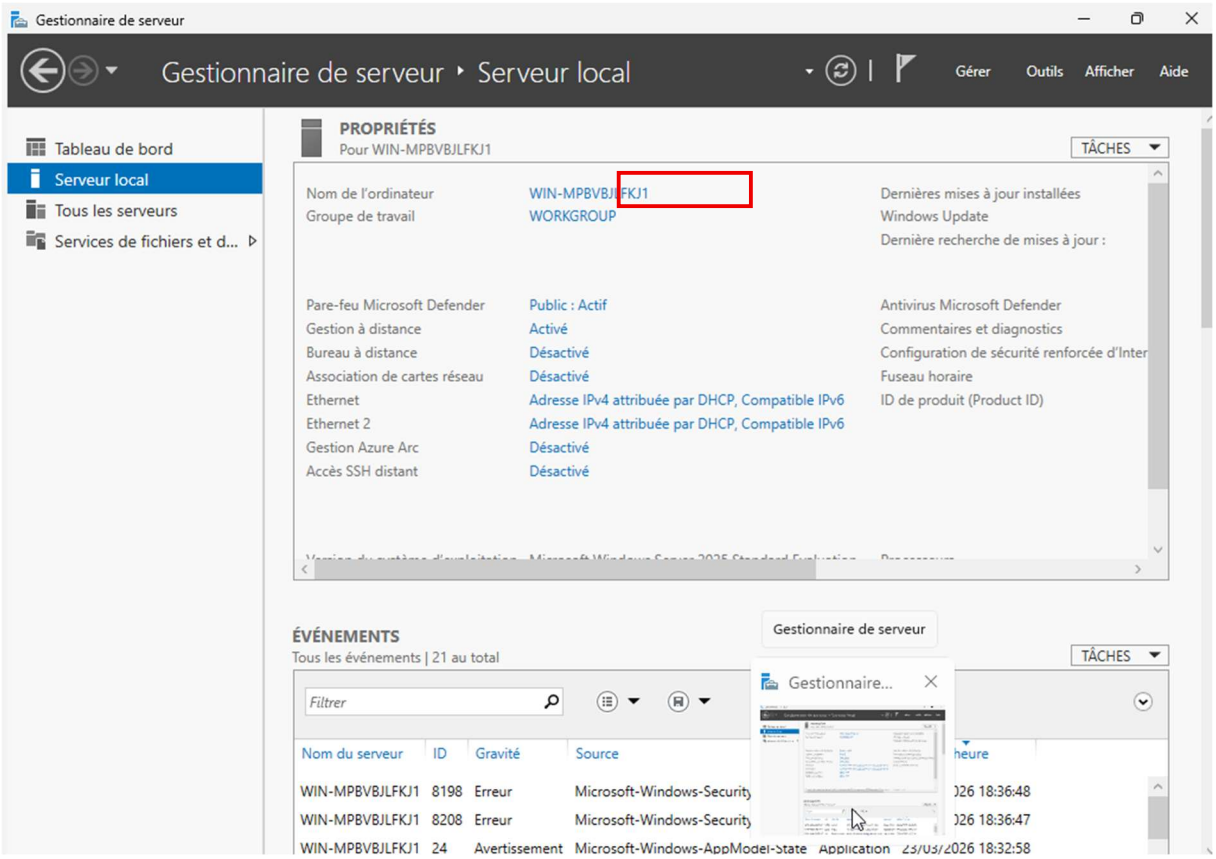
Une fois la session démarrée, il faudra ignorer les pop-ups Azure Arc et Windows Admin Center car c'est une publicité de Microsoft :



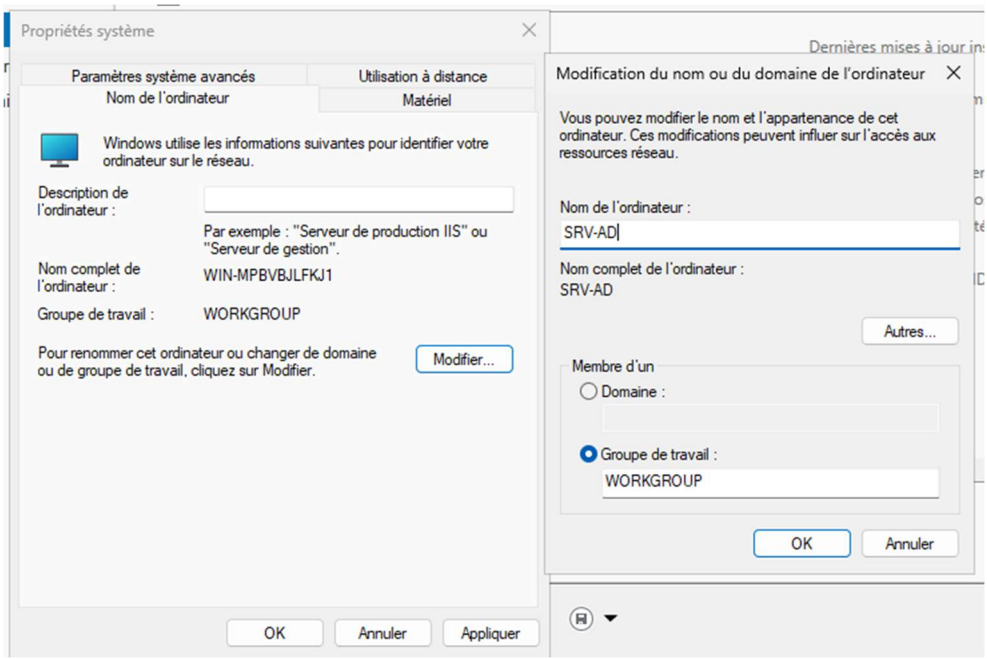
1.3 Renommer le serveur

Par défaut, Windows attribue un nom aléatoire (WIN-A7X9…). Le contrôleur de domaine doit avoir un nom fixe et significatif.

1. Ouvrir le **Gestionnaire de serveur**
2. Cliquer sur le **Serveur local** dans le menu de gauche
3. Dans la section Propriétés, cliquer sur le nom généré à côté de « Nom de l'ordinateur »



4. Cliquer sur le bouton **Modifier**...



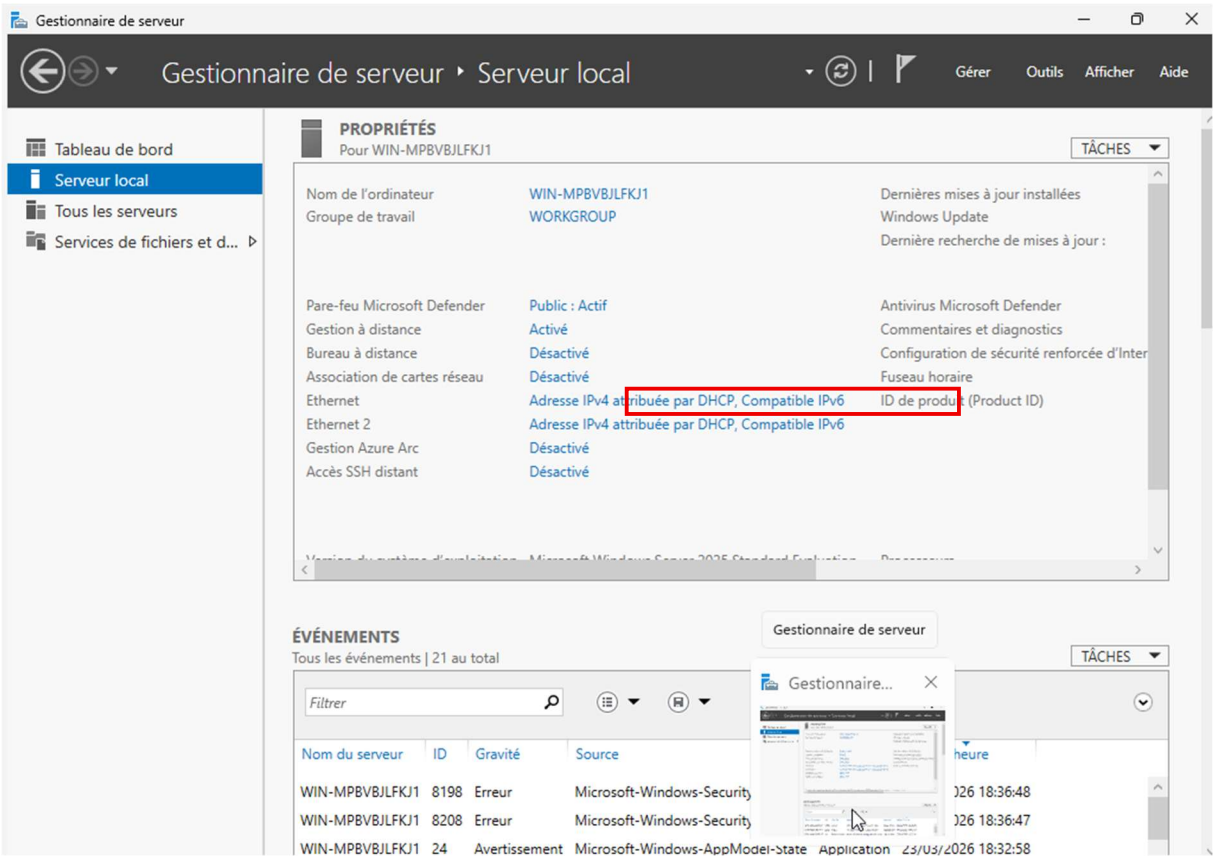
5. Entrer un nouveau nom (exemple : **SRV-AD** ou **SRV-GSB**)

6. Cliquer sur **OK**
7. Choisir **Redémarrer ultérieurement** (ne pas redémarrer immédiatement)

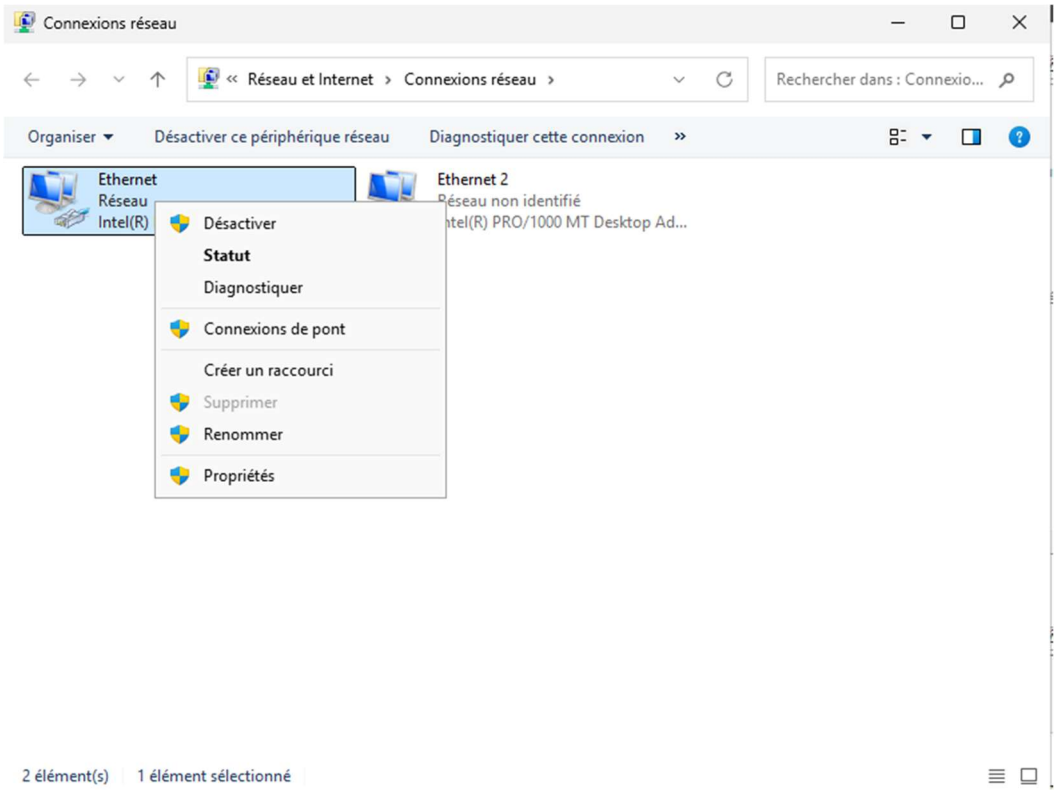
1.4 Configurer une adresse IP statique

Le serveur Active Directory doit avoir une IP fixe. Configuration en réseau par pont :

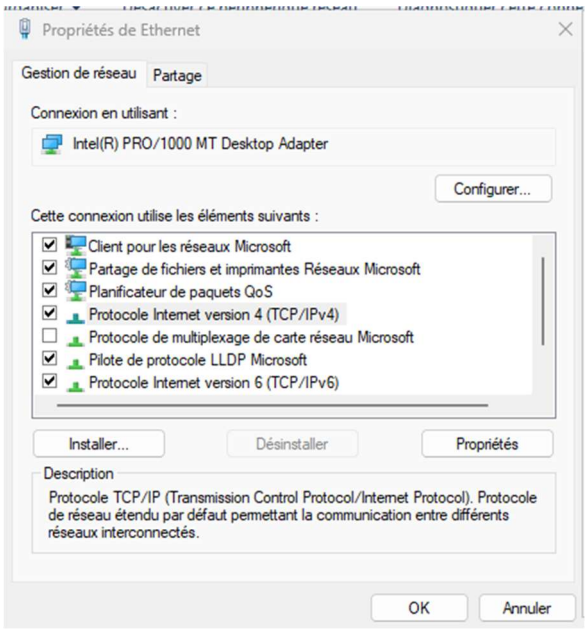
1. Dans le **Gestionnaire de serveur**, aller à **Serveur local**
2. Cliquer sur le lien bleu « Adresse IPv4 attribuée par DHCP » à côté d'« Ethernet »



3. Cela ouvre les connexions réseau
4. Faire un clic droit sur la carte « Ethernet » → **Propriétés**



5. Double-cliquer sur **Protocole Internet version 4 (TCP/IPv4)**



6. Cocher « Utiliser l'adresse IP suivante »
7. Remplir les champs (adapter selon le réseau, exemple en 192.168.1.X) :

a. Adresse IP : **192.168.1.190** (vérifier que cette IP est libre)

b. Masque de sous-réseau : **255.255.255.0**

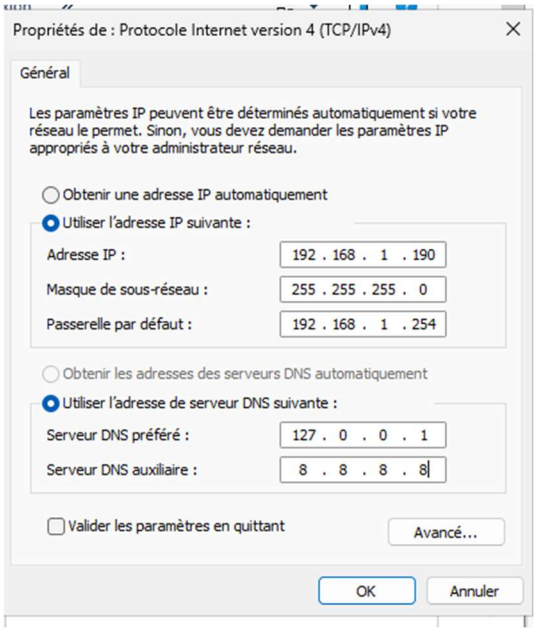
c. Passerelle par défaut : **192.168.1.254**

8. Configurer les serveurs DNS :

   a. Cocher « Utiliser l'adresse de serveur DNS suivante »

   b. Serveur DNS préféré : **127.0.0.1** (indispensable : le serveur s'interroge lui-même)

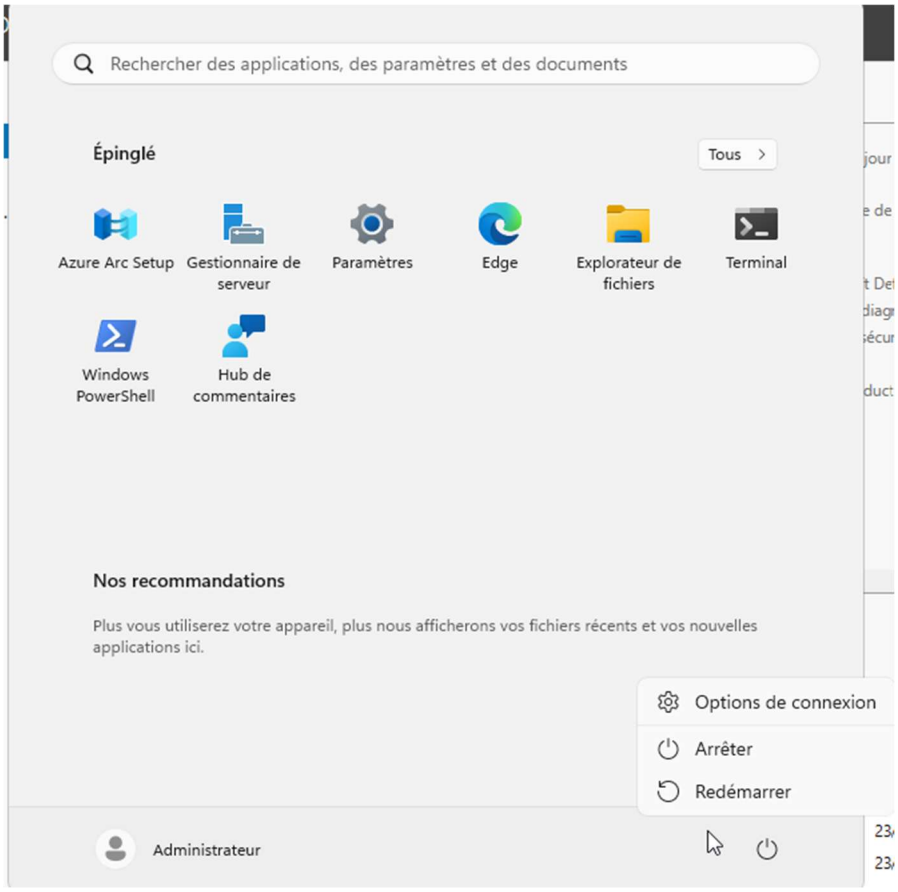
   c. Serveur DNS auxiliaire : **8.8.8.8** (Google)



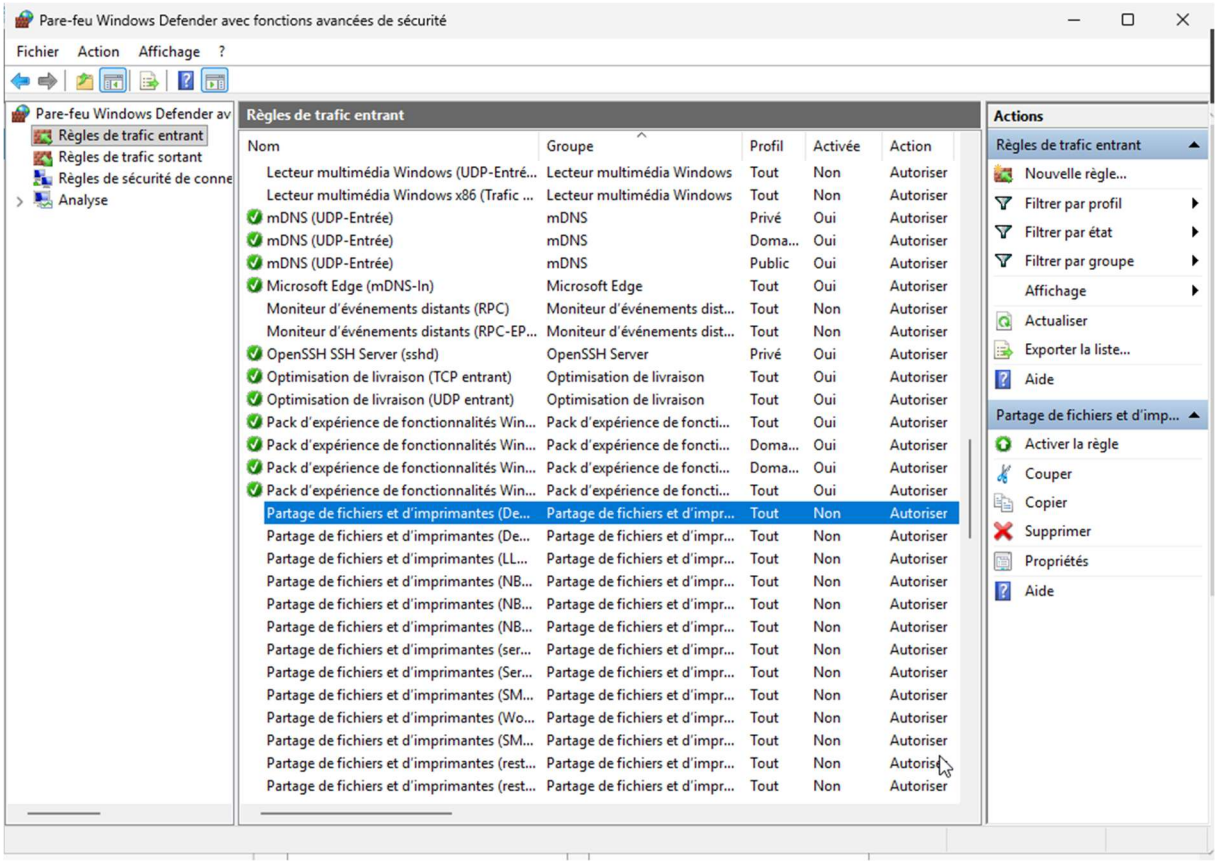
9. Cliquer sur **OK** deux fois

1.5 Redémarrer et tester la connectivité

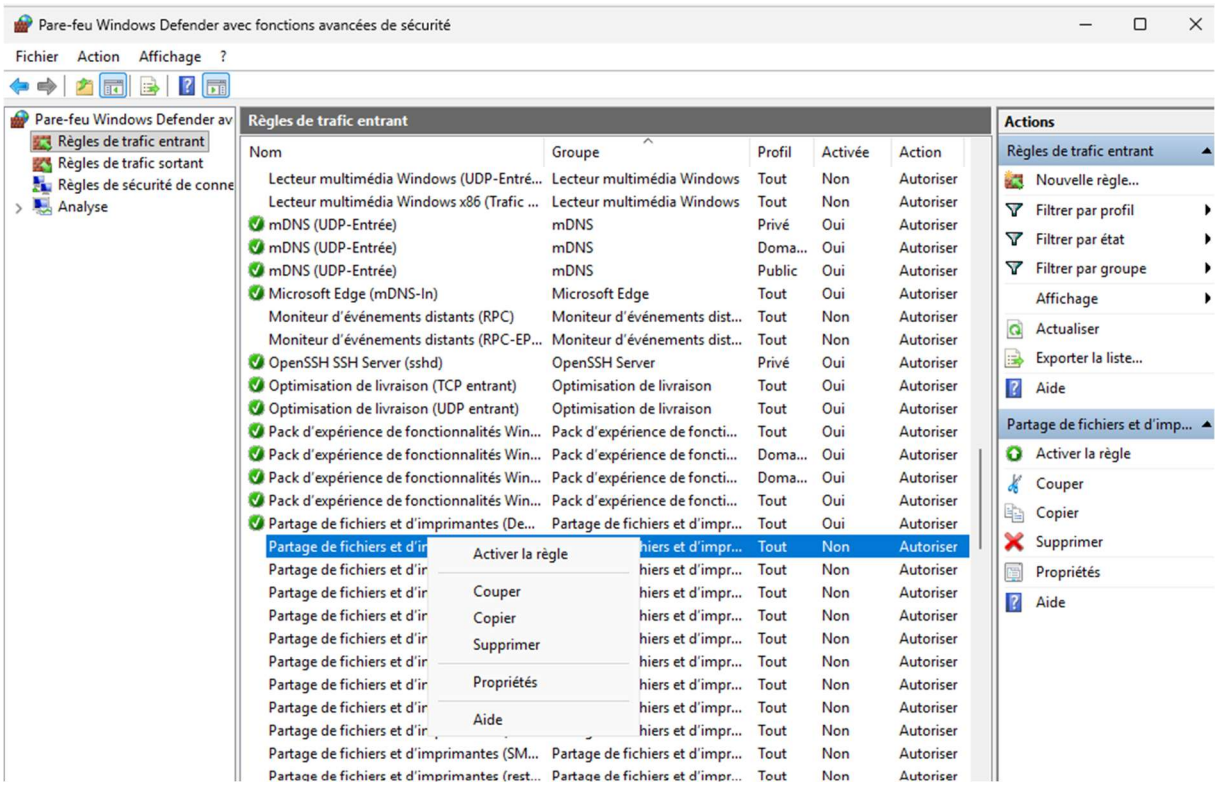
1. Clic droit sur le bouton Démarrer (logo Windows en bas) → **Arrêter ou se déconnecter** → **Redémarrer**



2. Une fois redémarré, ouvrir une invite de commandes et tester le ping
3. Si la réponse affiche « Délai d'attente de la demande dépassé » :
    a. Ouvrir le **Pare-feu Windows Defender avec fonctions avancées** (taper « pare-feu » dans le menu Démarrer)
    b. Cliquer sur **Règles de trafic entrant** dans le menu de gauche
    c. Chercher la règle **Partage de fichiers et d'imprimantes (Demande d'écho - ICMPv4 - Entrant)**



d. Faire un clic droit et cliquer sur **Activer la règle** (elle passe au vert)



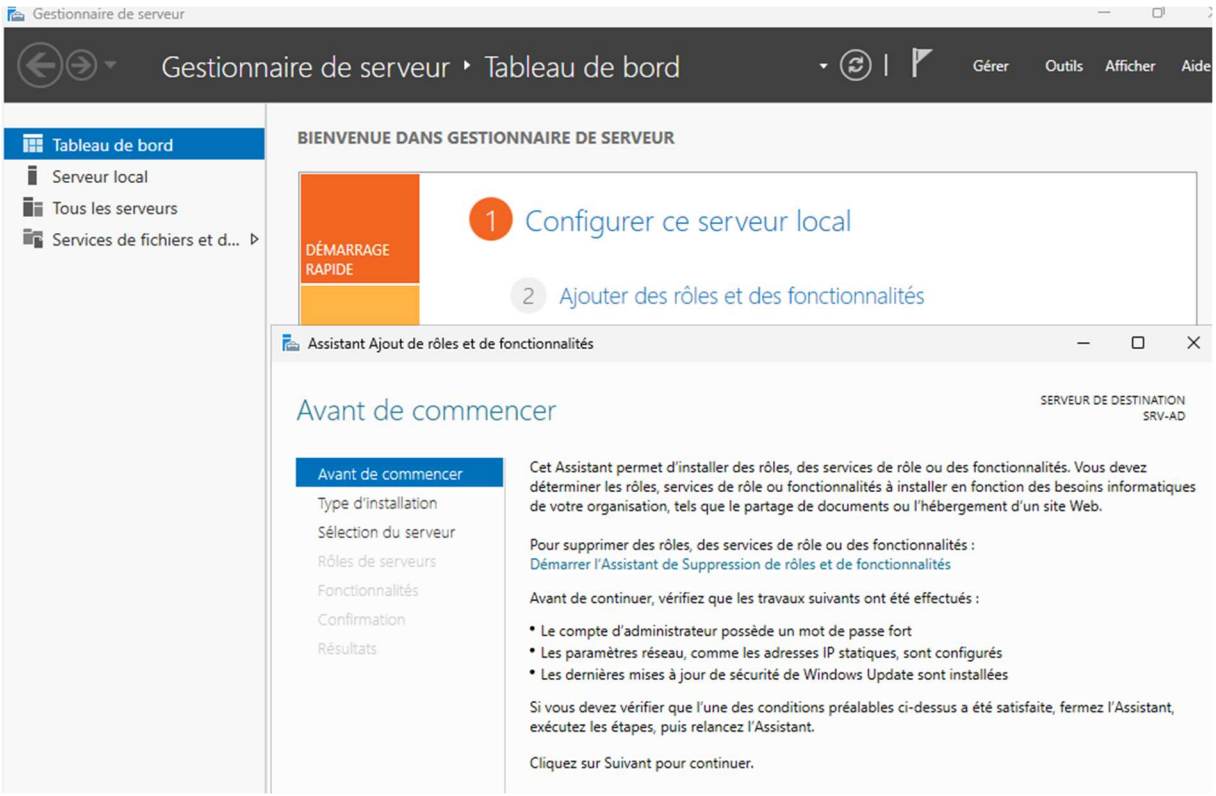
1.6 Problème potentiel : IP incorrect

Si l'IP n'est pas celle attendue, désactiver la deuxième carte réseau (Réseau interne) temporairement.

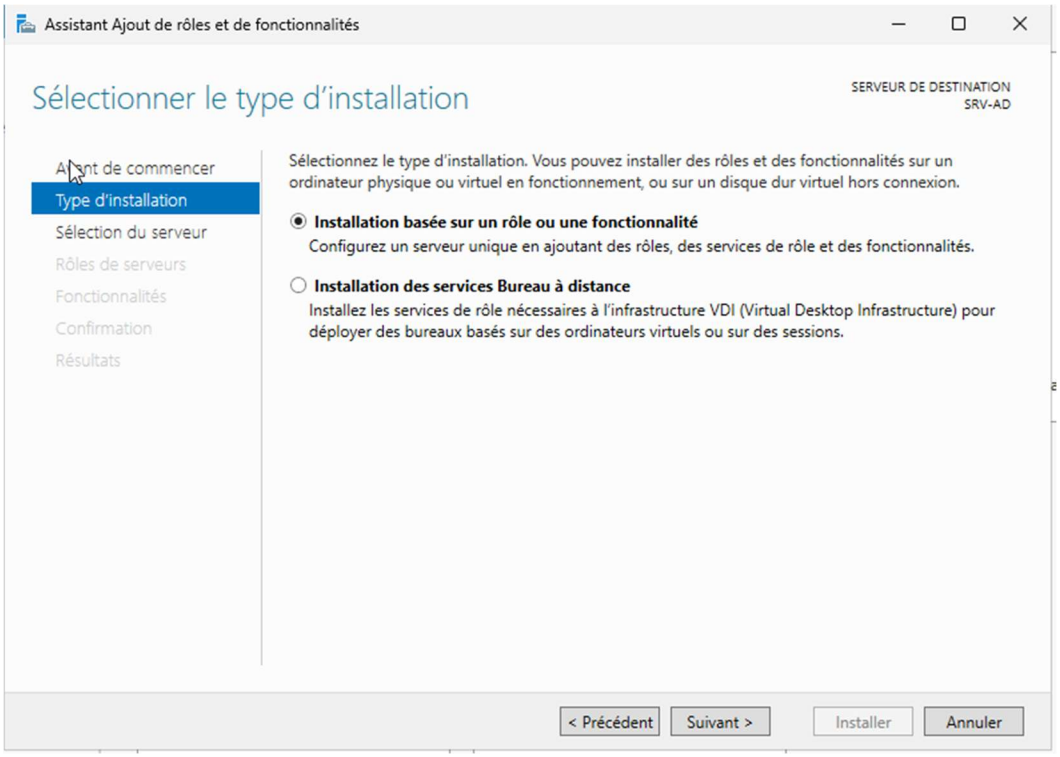
Partie 2 : Installation des rôles Active Directory

2.1 Installer le rôle AD DS

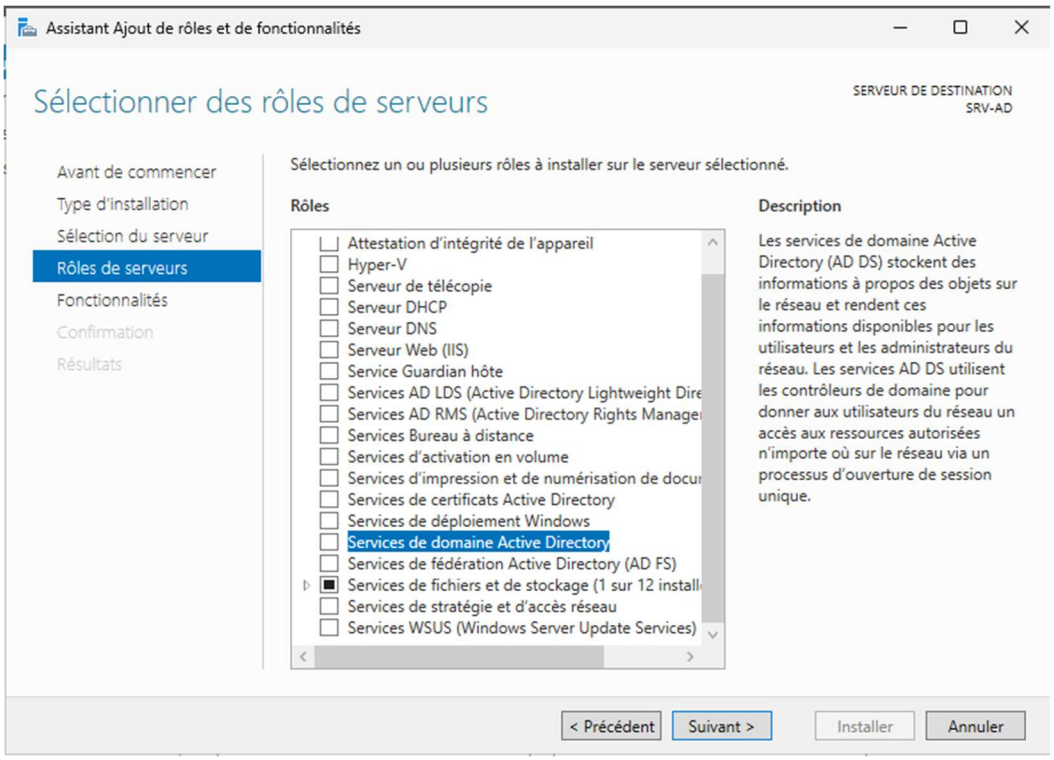
1. Ouvrir le **Gestionnaire de serveur**
2. Cliquer sur **Ajouter des rôles et des fonctionnalités** (lien 2 au centre)



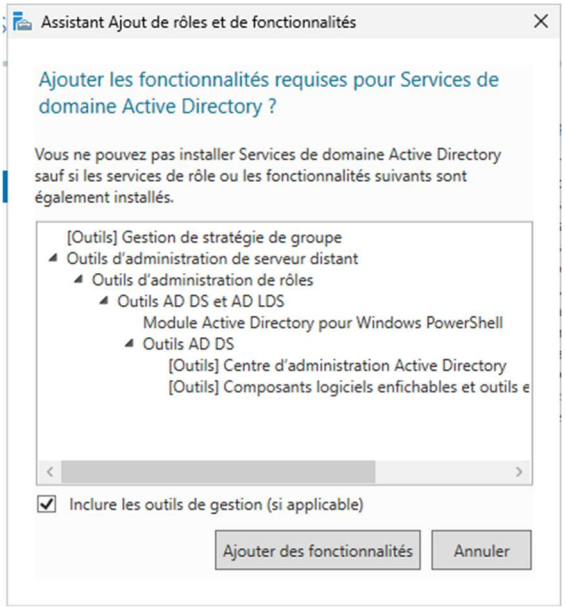
3. Suivre l'assistant jusqu'à l'écran de sélection des rôles



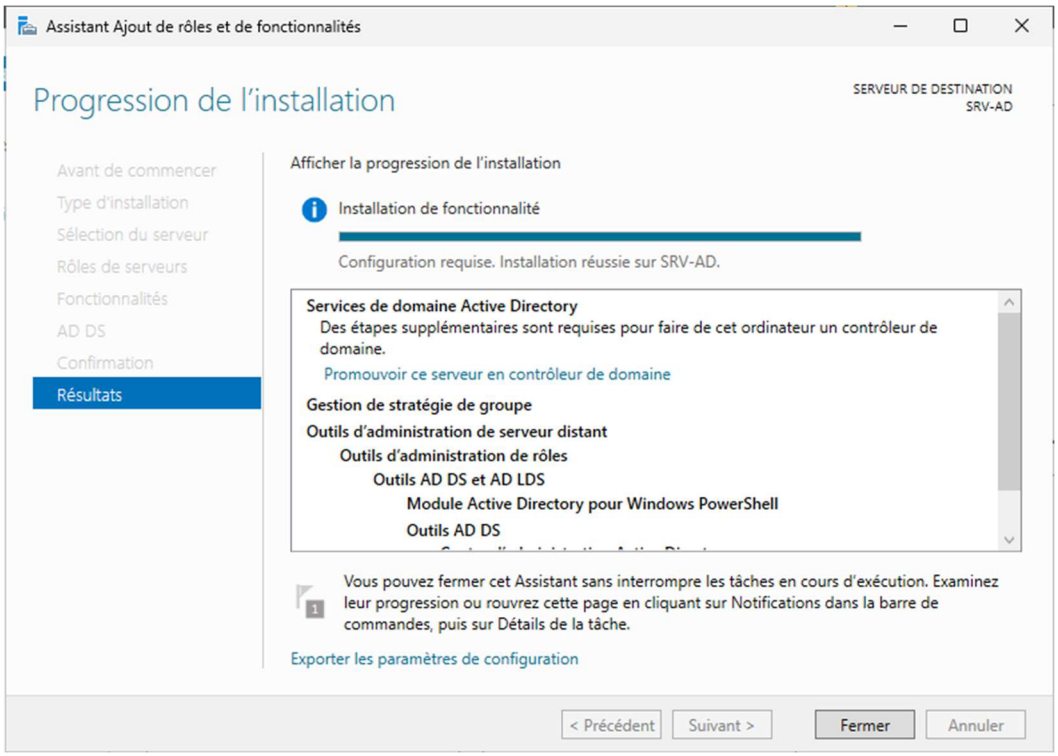
4. Cocher **Services de domaine Active Directory** (AD DS)



5. Un assistant propose d'ajouter les outils d'administration → cliquer sur **Ajouter des fonctionnalités**



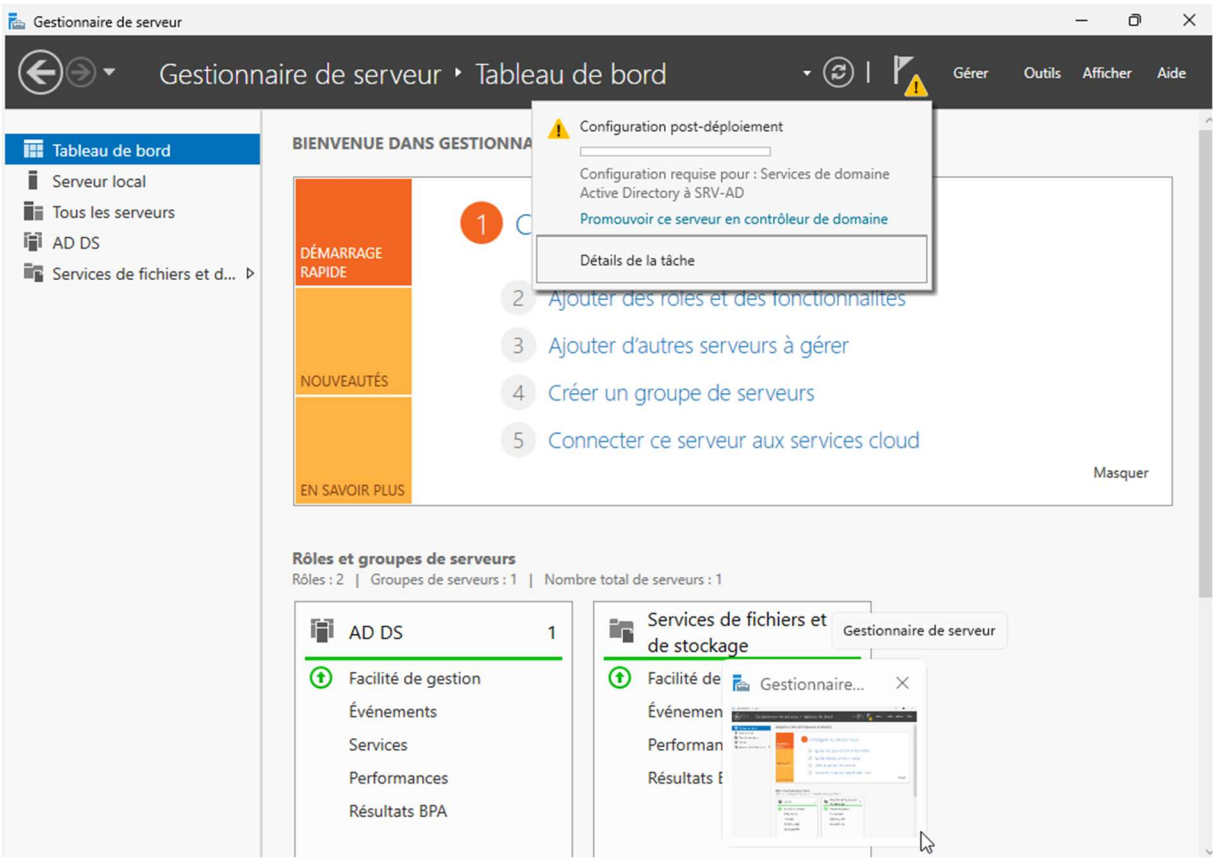
6. Cliquer sur **Suivant** jusqu'à la fin, puis cliquer sur **Installer**



Partie 3 : Installation des rôles Active Directory

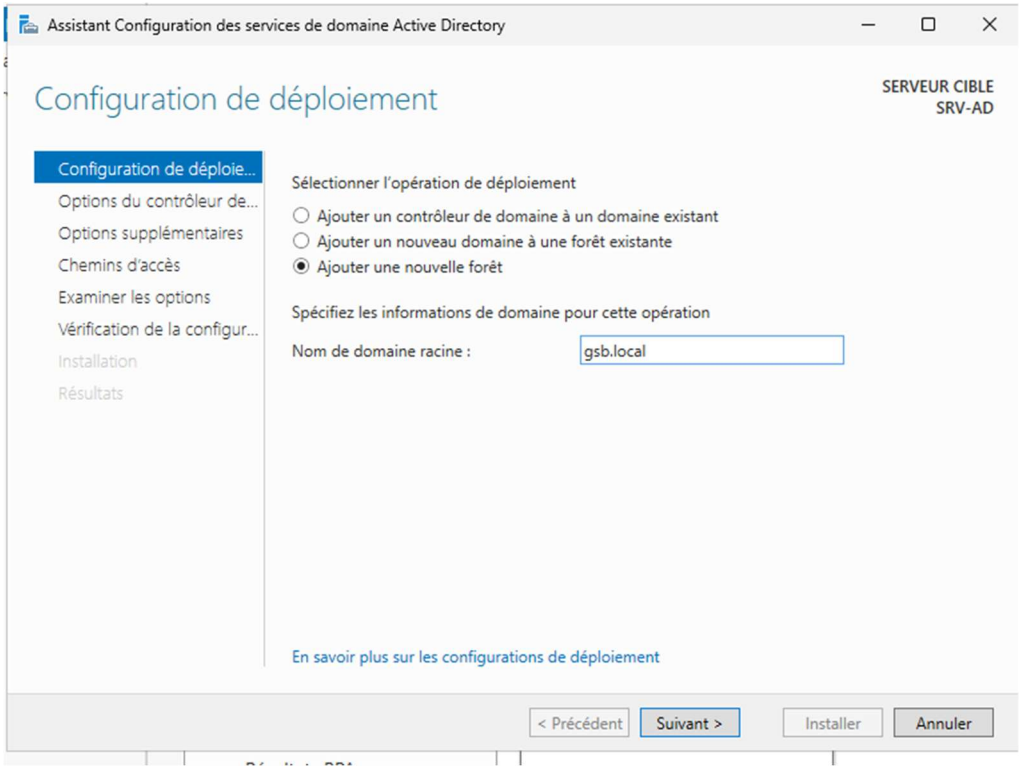
3.1 Lancer l'assistant de promotion

1. Dans le **Gestionnaire de serveur**, regarder tout en haut à droite
2. Cliquer sur l'icône du petit drapeau avec un point d'exclamation jaune
3. Un menu déroulant s'ouvre
4. Cliquer sur le lien bleu **Promouvoir ce serveur en contrôleur de domaine**



3.2 Créer une nouvelle forêt

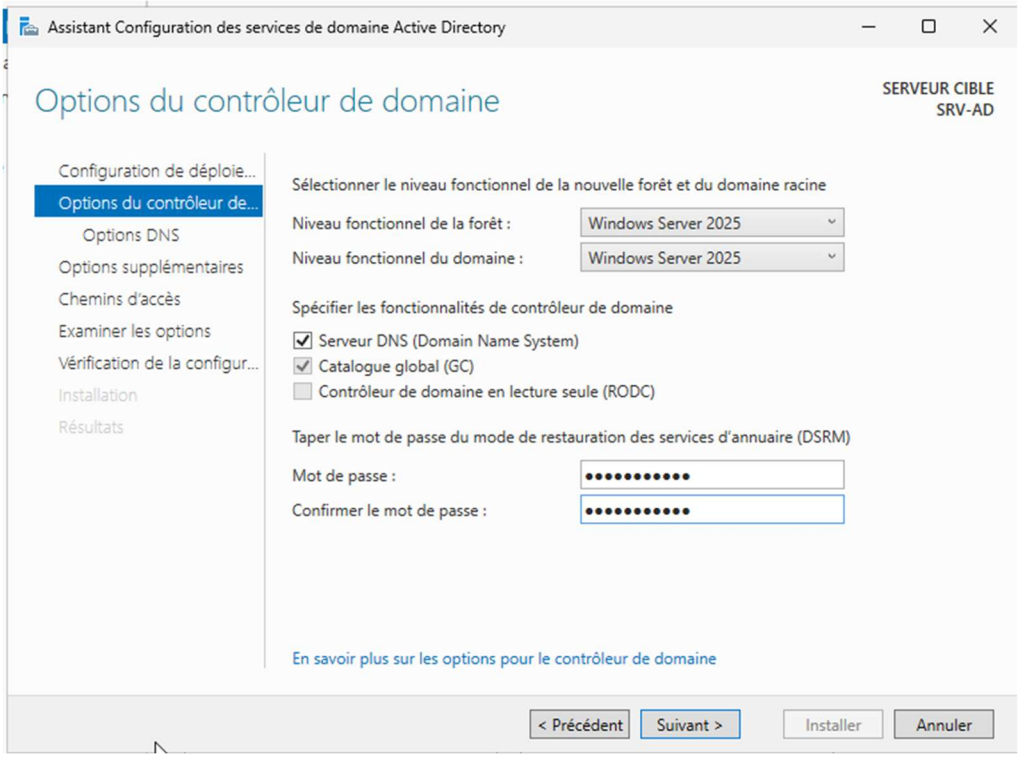
1. Sur l'écran « Configuration de déploiement », cocher la 3ème option : **Ajouter une nouvelle forêt**
2. Dans le champ Nom de domaine racine, entrer le nom du domaine (exemple : **gsb.local**)



3. Cliquer sur **Suivant**

3.3 Configurer les options et le mot de passe DSRM

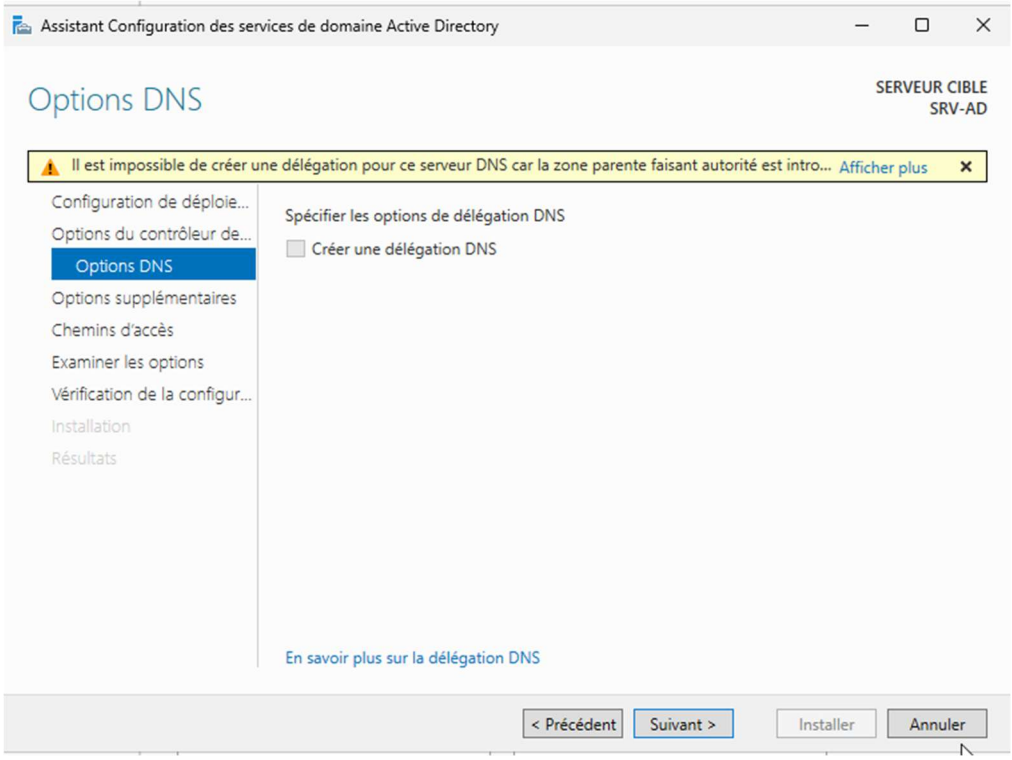
1. Sur l'écran des options :
    a. Laisser les niveaux fonctionnels par défaut (Windows Server 2025)
    b. S'assurer que la case **Serveur DNS (Domain Name System)** est cochée
2. Entrer un mot de passe de restauration des services d'annuaire (DSRM) complexe
3. Confirmer ce mot de passe dans le champ du dessous



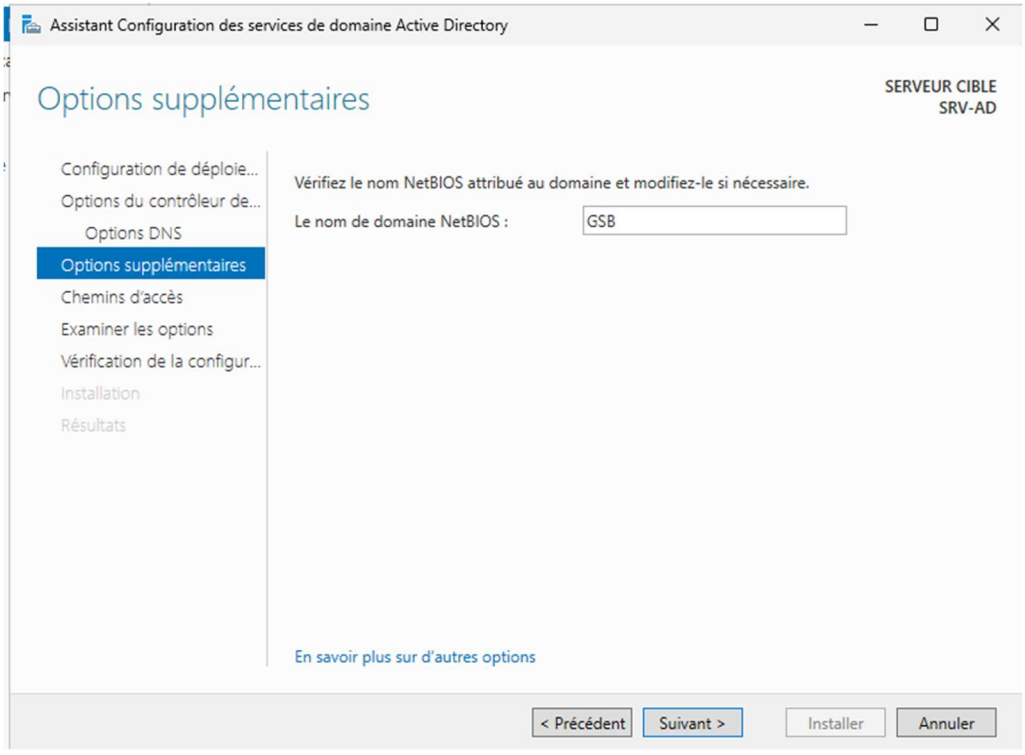
4. Cliquer sur **Suivant**

3.4 Finaliser l'installation

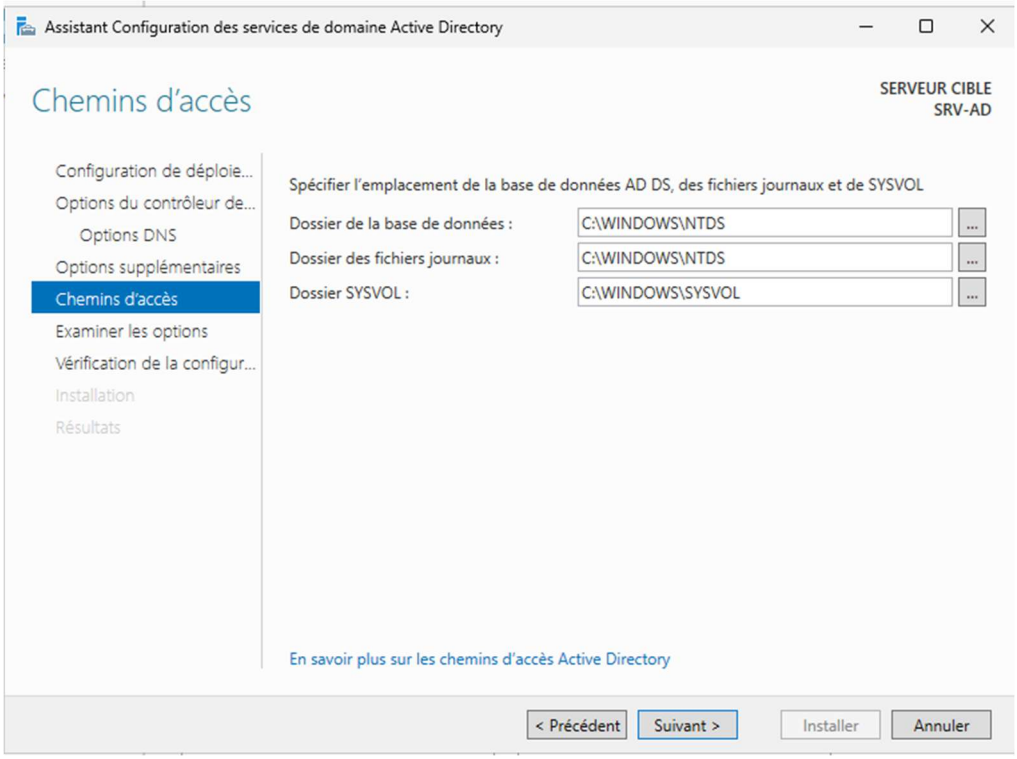
1. **Avertissement DNS** : Un message signale « Une délégation pour ce serveur DNS ne peut pas être créée ». C'est normal. Cliquer sur **Suivant**



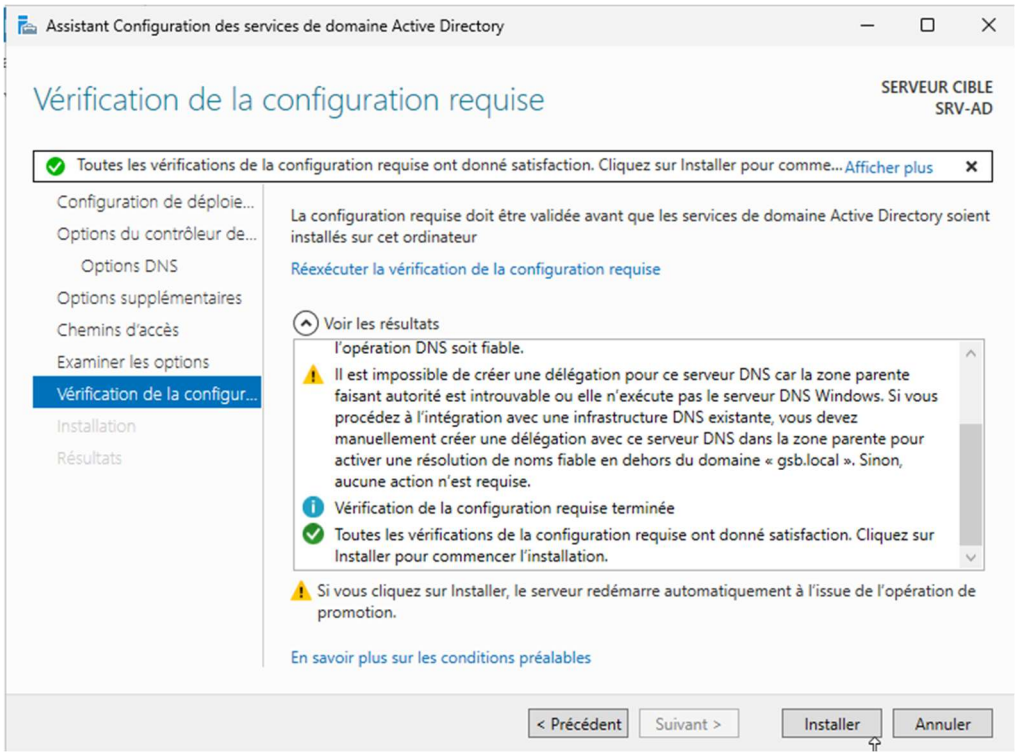
2. **Nom NetBIOS** : Le système affiche un nom calculé automatiquement (exemple : GSB). Laisser par défaut et cliquer sur **Suivant**



3. **Chemins d'accès** : Le système affiche où rangera la base de données AD (C:\Windows\NTDS). Laisser par défaut et cliquer sur **Suivant**



4. **Vérification de la configuration requise** : Quelques avertissements jaunes peuvent s'afficher (cryptographie, etc.). C'est normal
5. Vérifier qu'un **petit rond vert** apparaît en haut avec le message « Toutes les vérifications de la configuration requise ont donné satisfaction »



6. Cliquer sur **Installer**

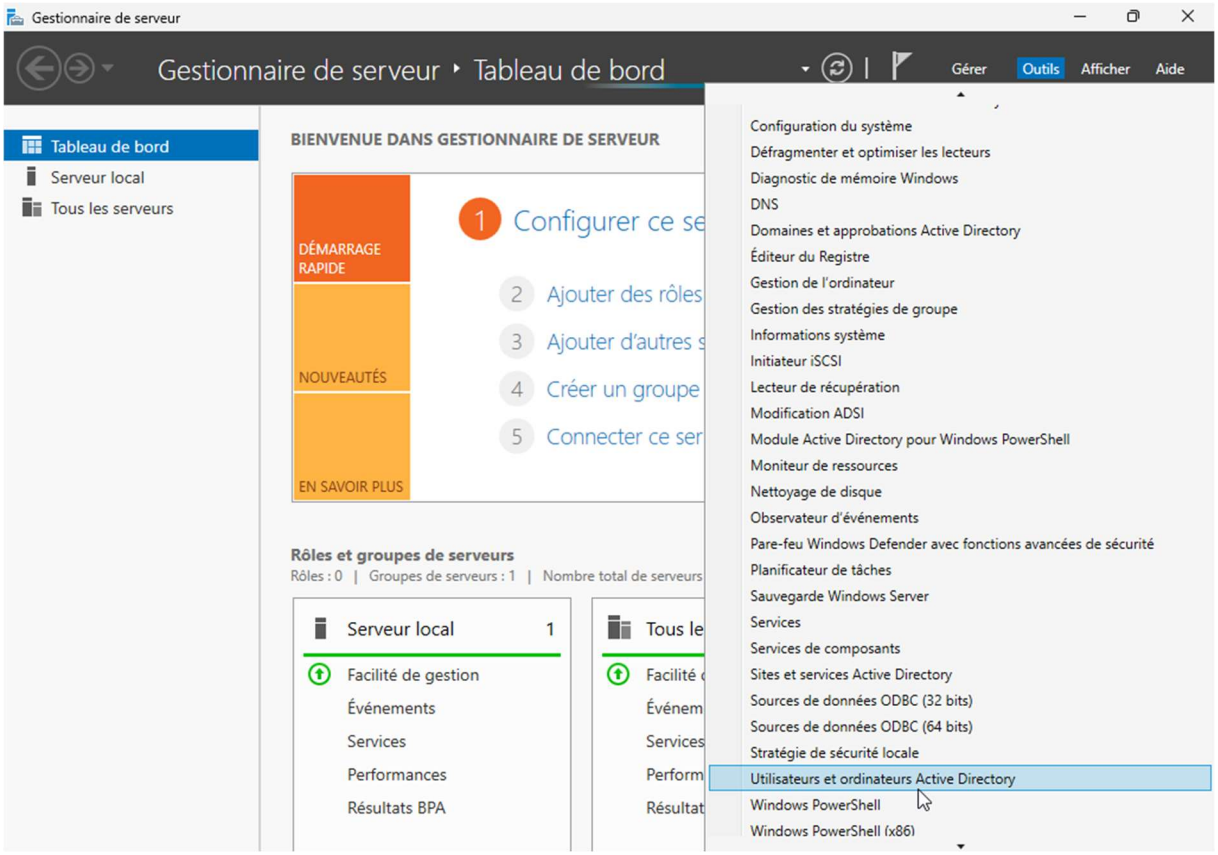
3.5 Redémarrage automatique

L'installation démarre. Le serveur va redémarrer automatiquement après quelques minutes. Laisser faire.

Partie 4 : Création d'un utilisateur test dans l'Active Directory

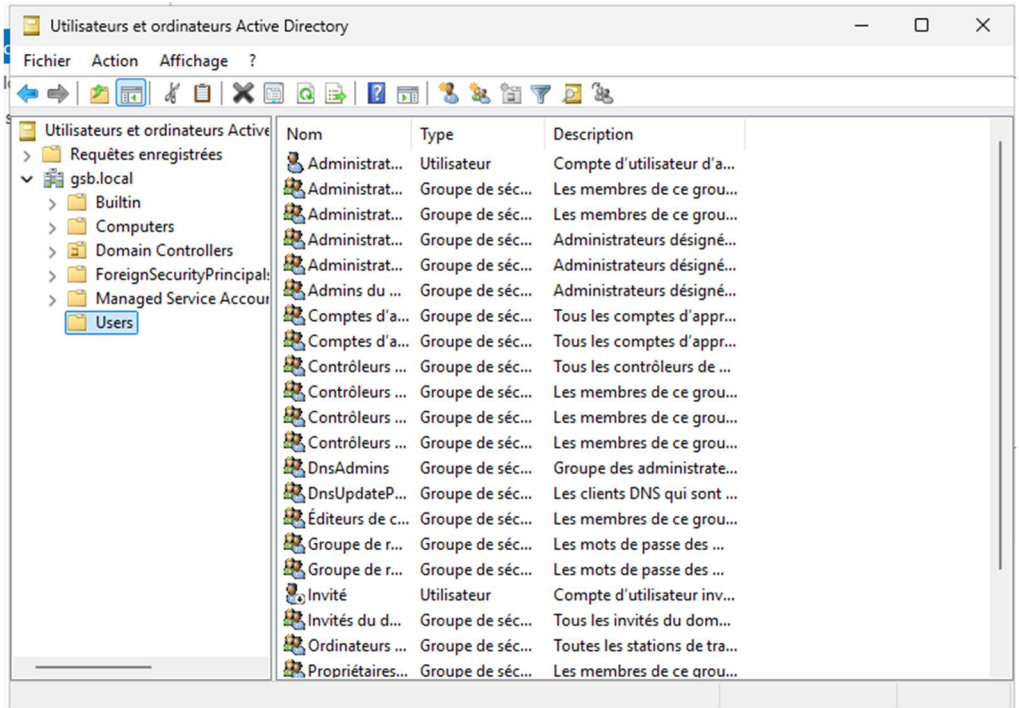
4.1 Accéder aux utilisateurs et ordinateurs Active Directory

1. Ouvrir le **Gestionnaire de serveur**
2. Cliquer sur le menu **Outils** en haut à droite
3. Sélectionner **Utilisateurs et ordinateurs Active Directory**

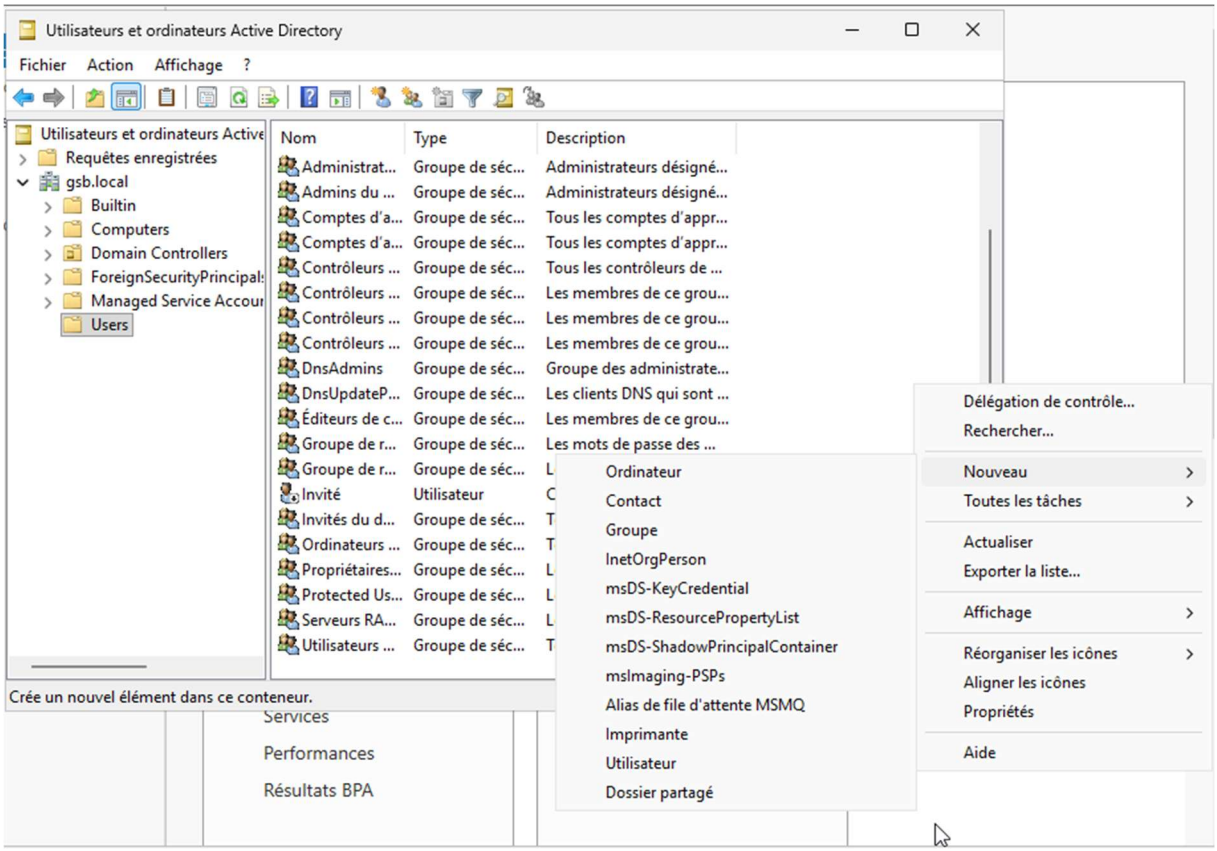


4.2 Créer un nouvel utilisateur

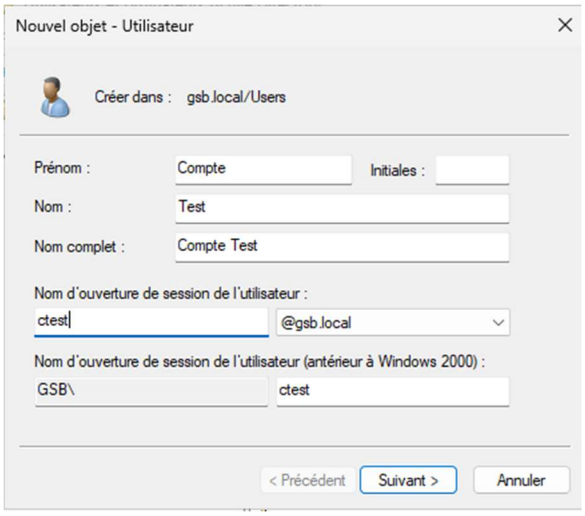
1. Dans la colonne de gauche, déployer le domaine (ex: gsb.local)



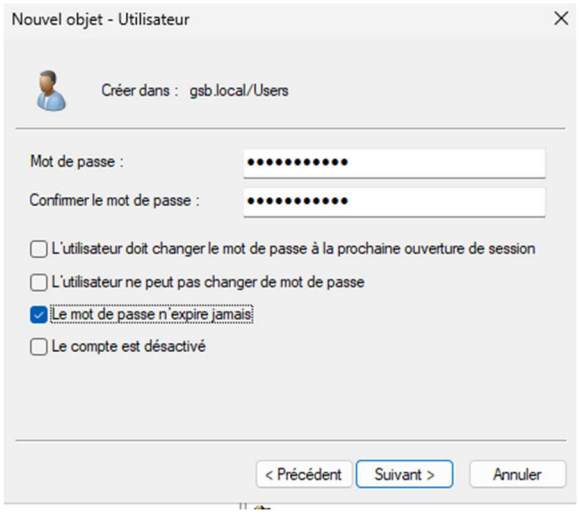
2. Cliquer sur le dossier jaune **Users**
3. Faire un clic droit dans la zone centrale → **Nouveau** → **Utilisateur**



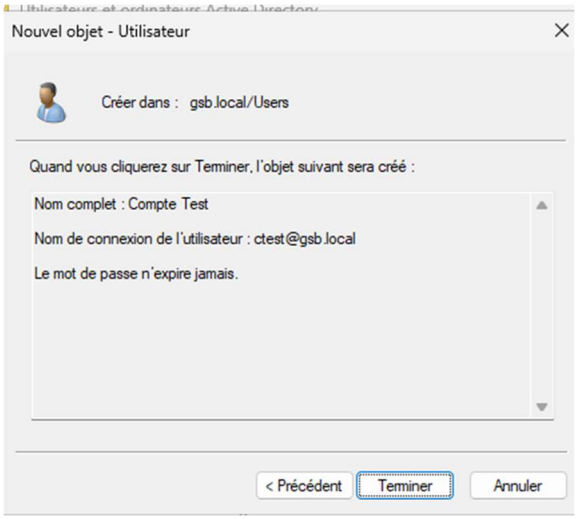
4. Remplir les champs :
    a. Prénom : **Compte**
    b. Nom : **Test**
    c. Nom d'ouverture de session : **ctest** (identifiant unique)
5. Cliquer sur **Suivant**



6. Entrer un mot de passe complexe
7. **Important** : Décocher « *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session* »
8. Cocher « *Le mot de passe n'expire jamais* »



9. Cliquer sur **Suivant**, puis sur **Terminer**

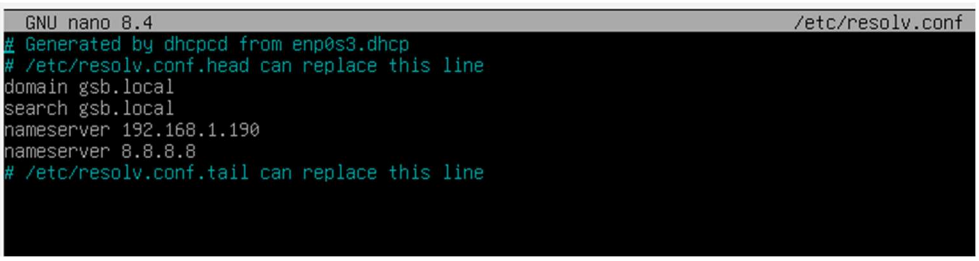


L'utilisateur est maintenant créé et disponible pour les tests.

Partie 5 : Configuration de Debian pour rejoindre le domaine

5.1 Configurer le fichier *resolv.conf*

Modifier le fichier /etc/resolv.conf sur le serveur Debian pour qu'il pointe vers le serveur AD :



domain gsb.local

search gsb.local

nameserver 192.168.1.190

nameserver 8.8.8.8

Remplacer 192.168.1.190 par l'adresse IP réelle du serveur Windows.

Partie 6 : Intégration de l'Active Directory à Symfony

6.1 Installer les prérequis sur Debian

Première étape : installer le support LDAP pour PHP et télécharger le composant Symfony.

Dans le terminal :

sudo apt update

sudo apt install php8.4-ldap

sudo systemctl restart apache2

Dans le dossier du projet Symfony (ex: /var/www/projet) :

composer require symfony/ldap

6.2 Configurer les variables d'environnement (.env)

Ouvrir le fichier .env (/var/www/projet/.env) et ajouter à la fin :

Connexion au serveur Active Directory :

LDAP_HOST=192.168.1.190

LDAP_PORT=389

LDAP_ENCRYPTION=none

Domaine décomposé (gsb.local -> DC = gsb, DC = local)

LDAP_BASE_DN="DC=gsb,DC=local"

Compte administrateur pour la recherche d'utilisateurs

LDAP_SEARCH_DN="CN=Administrateur,CN=Users,DC=gsb,DC=local"

LDAP_SEARCH_PASSWORD="MotDePasseAdministrateur"

Adapter les valeurs selon la configuration.

6.3 Configurer le service LDAP dans services.yaml

Ouvrir config/services.yaml et ajouter ce bloc à la fin :

Symfony\Component\Ldap\Ldap:

arguments: ['@Symfony\Component\Ldap\Adapter\ExtLdap\Adapter']

tags: ['ldap']

Symfony\Component\Ldap\Adapter\ExtLdap\Adapter:

arguments:

- host: '%env(LDAP_HOST)%'

port: '%env(int:LDAP_PORT)%'

encryption: '%env(LDAP_ENCRYPTION)%'

options:

protocol_version: 3

referrals: false

6.4 Configurer la sécurité (security.yaml)

L'objectif est de garder l'authentification gérée par Active Directory tout en utilisant l'entité App\Entity\Utilisateur pour les sessions et les rôles.

Remplacer le contenu du fichier config/security.yaml :

security:

password_hashers:

App\Entity\Utilisateur: 'auto'

providers:

 # Provider basé sur la base de données

app_user_provider:

entity:

class: App\Entity\Utilisateur

property: login

```
firewalls:
dev:
pattern: ^/(_(profiler|wdt)|css|images|js)/
security: false
main:
 lazy: true
 # Provider : entité Utilisateur en base de données
 provider: app_user_provider

 # Authentification LDAP contre Active Directory
 form_login_ldap:
  login_path: app_login
  check_path: app_login
  enable_csrf: true
  success_handler: App\Security\LoginSuccessHandler

  # Service LDAP
  service: Symfony\Component\Ldap\Ldap
  dn_string: '%env(resolve:LDAP_BASE_DN)%'

  # Chercher l'utilisateur dans l'AD par sAMAccountName
  query_string: '(&(sAMAccountName={user_identifier})(objectClass=person))'
  search_dn: '%env(resolve:LDAP_SEARCH_DN)%'
  search_password: '%env(resolve:LDAP_SEARCH_PASSWORD)%'

 logout:
  path: app_logout
  target: app_login
```

access_control:

 # Personnaliser selon les besoins

 # - { path: ^/admin, roles: ROLE_ADMIN }

 # - { path: ^/profile, roles: ROLE_USER }

when@test:

security:

password_hashers:

Symfony\Component\Security\Core\User\PasswordAuthenticatedUserInterface:

algorithm: plaintext

cost: 4

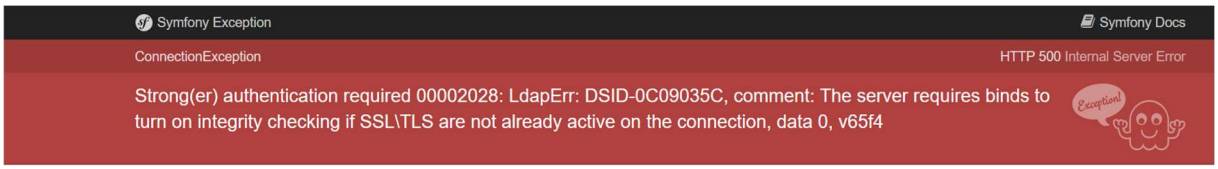
time_cost: 3

memory_cost: 10

Partie 7 : Résolution des erreurs courantes

7.1 Erreur : « Strong(er) authentication required »

Message d'erreur complet :



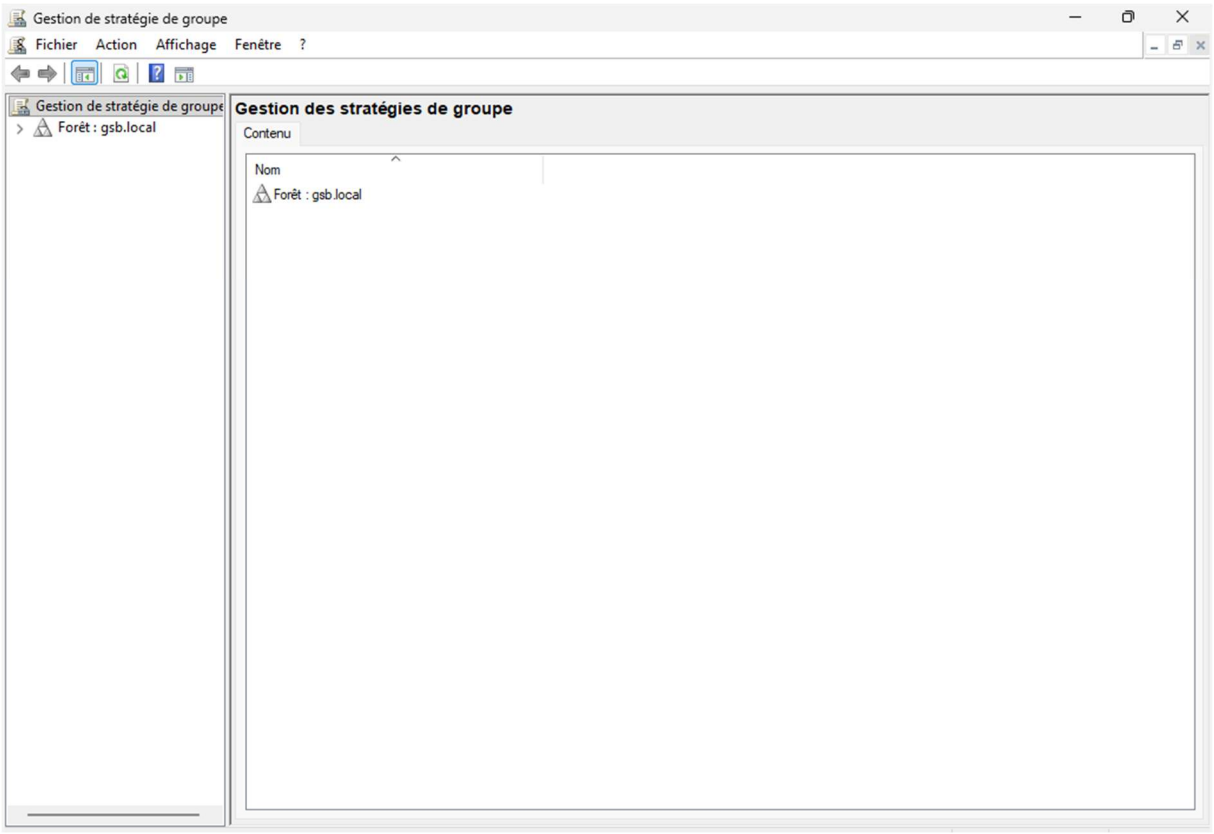
DSID-0C09035C, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v65f4

Cause : Windows Server 2025 refuse par défaut les connexions LDAP non sécurisées sur le port 389. Il exige une connexion chiffrée (LDAPS sur le port 636) ou la signature des paquets.

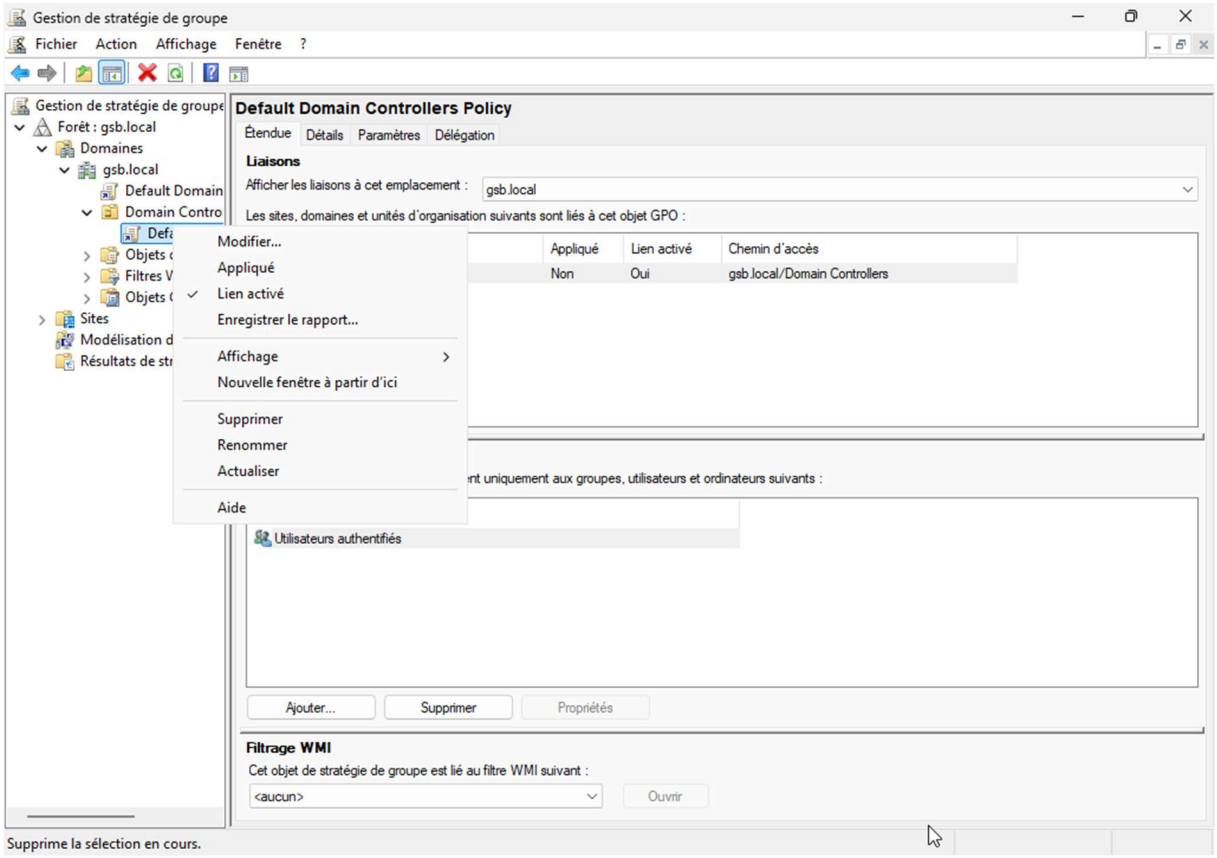
En environnement de test local (sans certificat SSL), la solution est de désactiver cette obligation de sécurité sur le serveur Active Directory.

7.2 Désactiver l'obligation LDAP signé sur Windows Server 2025

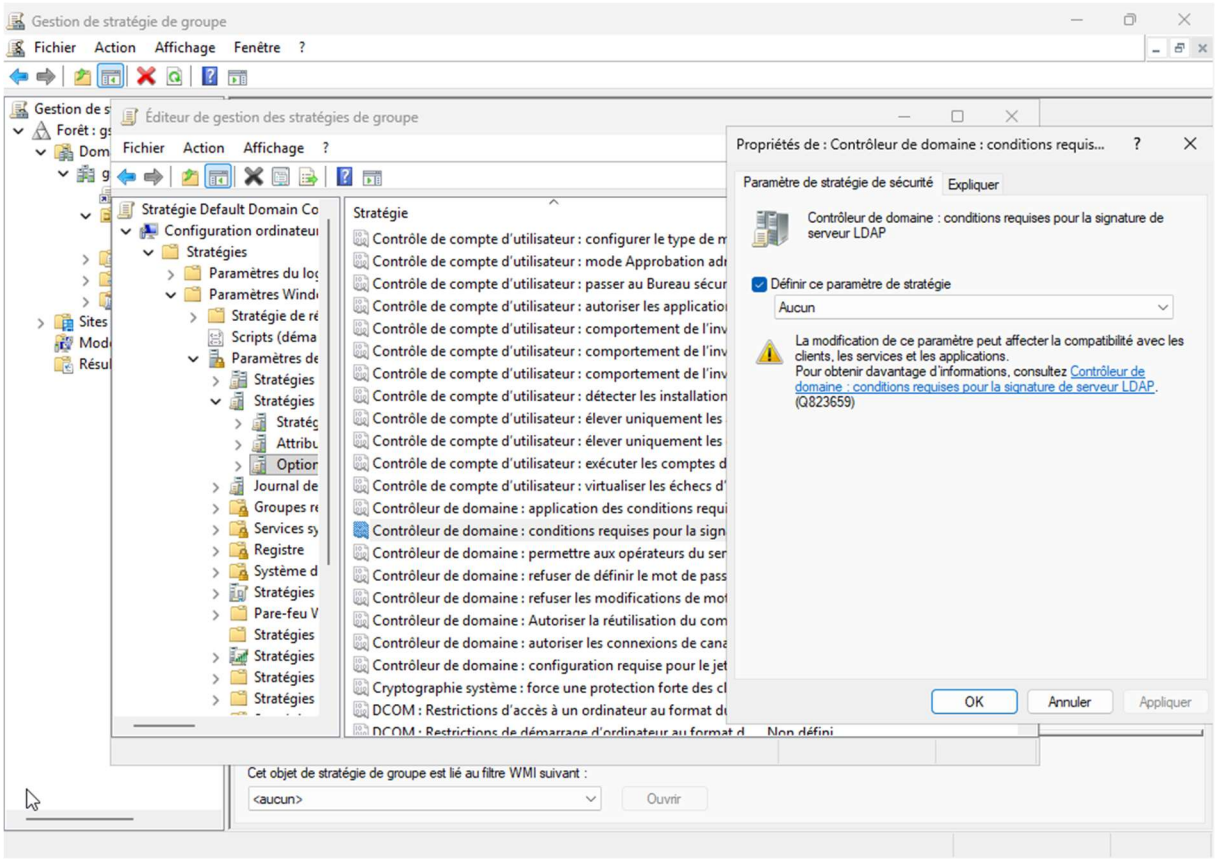
1. Sur le serveur Windows, ouvrir le menu Démarrer, taper **Group Policy** et ouvrir **Gestion de stratégie de groupe**



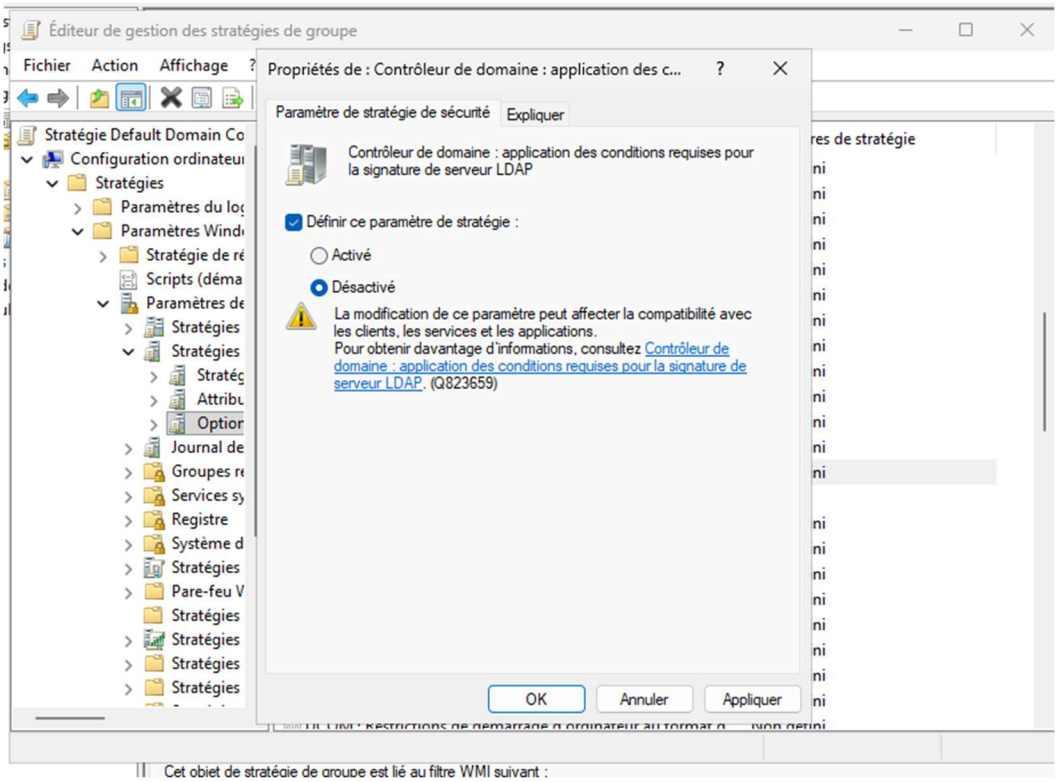
2. Dans l'arborescence de gauche, déployer :
    a. Forêt : gsb.local
    b. Domaines
    c. gsb.local
    d. Domain Controllers
3. Faire un clic droit sur **Default Domain Controllers Policy** et choisir **Modifier**



4. L'Éditeur de gestion des stratégies de groupe s'ouvre
5. Naviguer jusqu'au chemin :
    a. Configuration ordinateur
    b. Stratégies
    c. Paramètres Windows
    d. Paramètres de sécurité
    e. Stratégies locales
    f. Cliquer sur **Options de sécurité**
6. Chercher (en bas de la liste) la ligne : **Contrôleur de domaine : conditions requises pour la signature de serveur LDAP**
7. Double-cliquer, cocher « Définir ce paramètre de stratégie », et choisir **Aucun(e)**



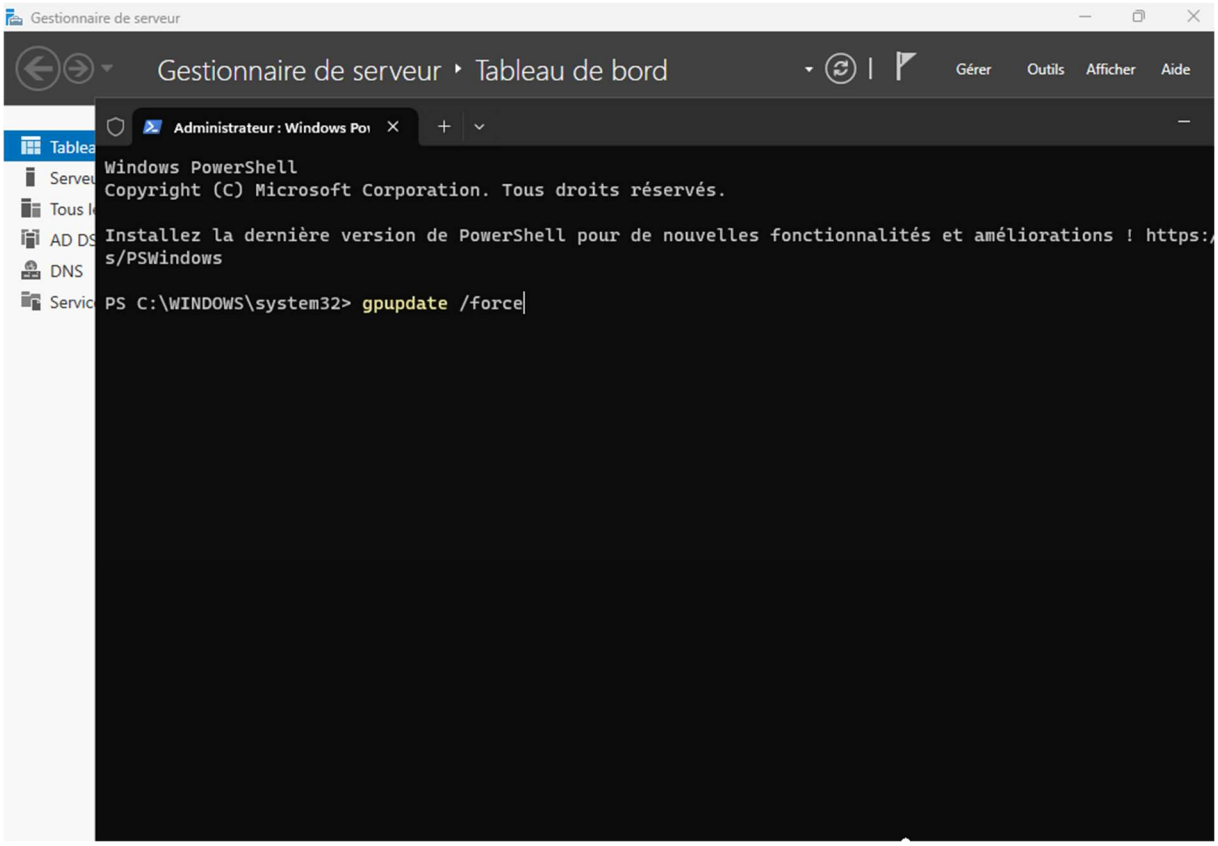
8. Chercher la ligne juste en dessous : **Contrôleur de domaine : application des conditions requises pour la signature de serveur LDAP**
9. Double-cliquer, cocher « Définir ce paramètre de stratégie », et choisir **Désactivé**



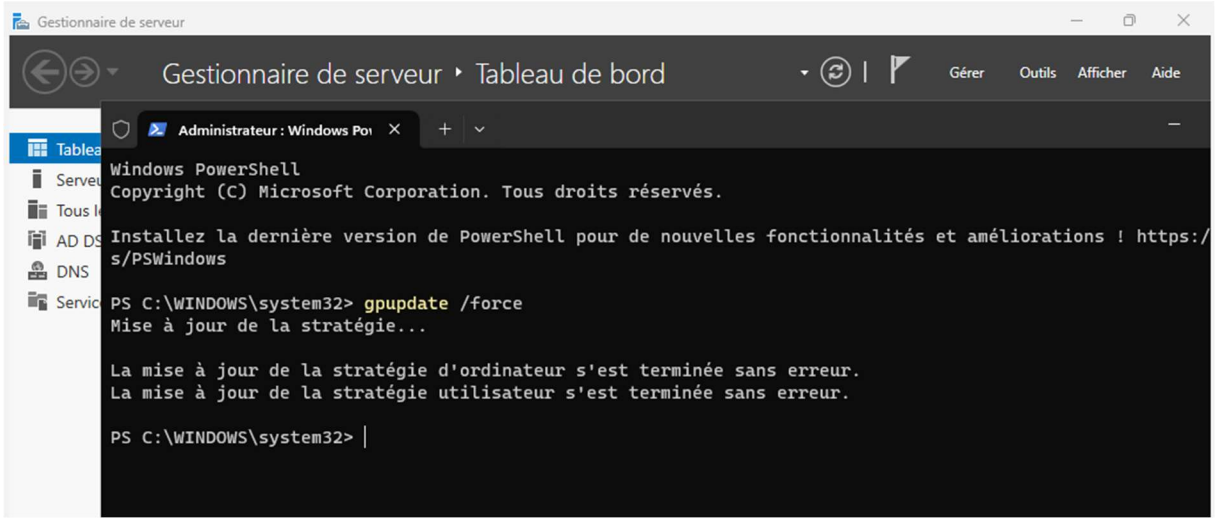
10. Cliquer sur **OK**

7.3 Appliquer les modifications sans redémarrage

1. Ouvrir une invite de commandes (clic droit sur le bouton Démarrer)
2. Taper la commande : *gpupdate /force*



3. Appuyer sur Entrée et attendre le message « La mise à jour de la stratégie d'ordinateur a réussi »



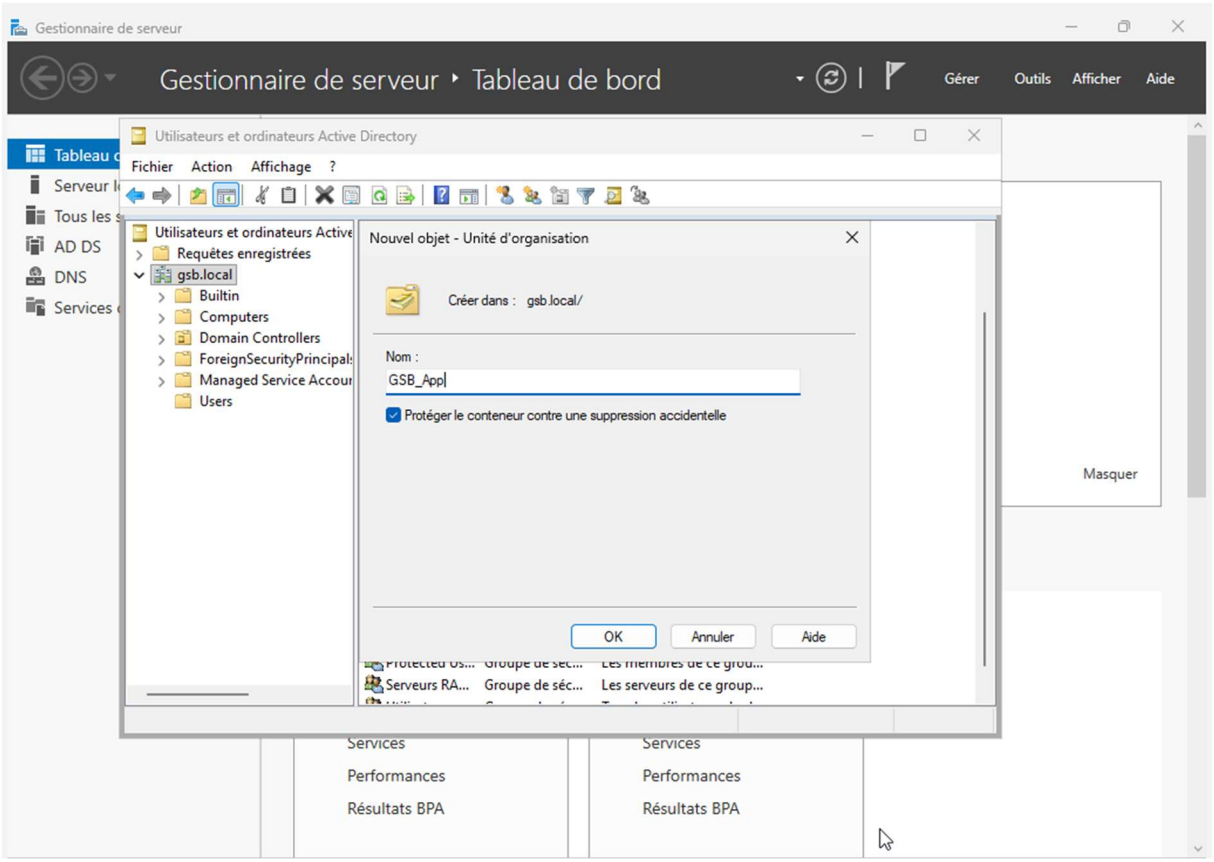
Une fois cela effectué, la connexion LDAP depuis Symfony devrait fonctionner sans erreur de sécurité stricte.

Partie 8 : Structuration de l’Active Directory

Création de l'Unité d'Organisation (OU) dédiée

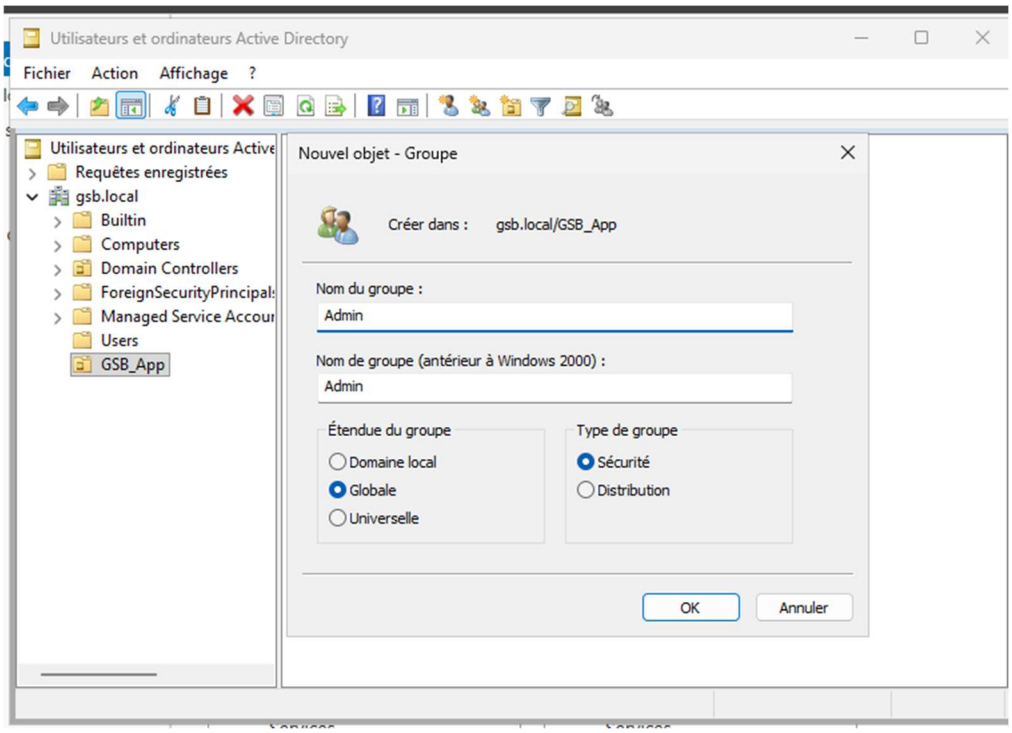
L’objectif est d’isoler les comptes générés par l’application web du reste des comptes d’administration ou de services, ceci pour des raisons de sécurité et de gestion des stratégies.

1. Sur le serveur Windows Server 2025, ouvrir la console **Utilisateurs** et **ordinateurs** Active Directory (accessible depuis le menu *Outils* du Gestionnaire de serveur).
2. Dans l'arborescence, effectuer un clic droit sur la racine du domaine (gsb.local).
3. Sélectionner **Nouveau** > **Unité d'organisation** et nommer cette entité GSB_App.



Création des groupes de sécurité métiers

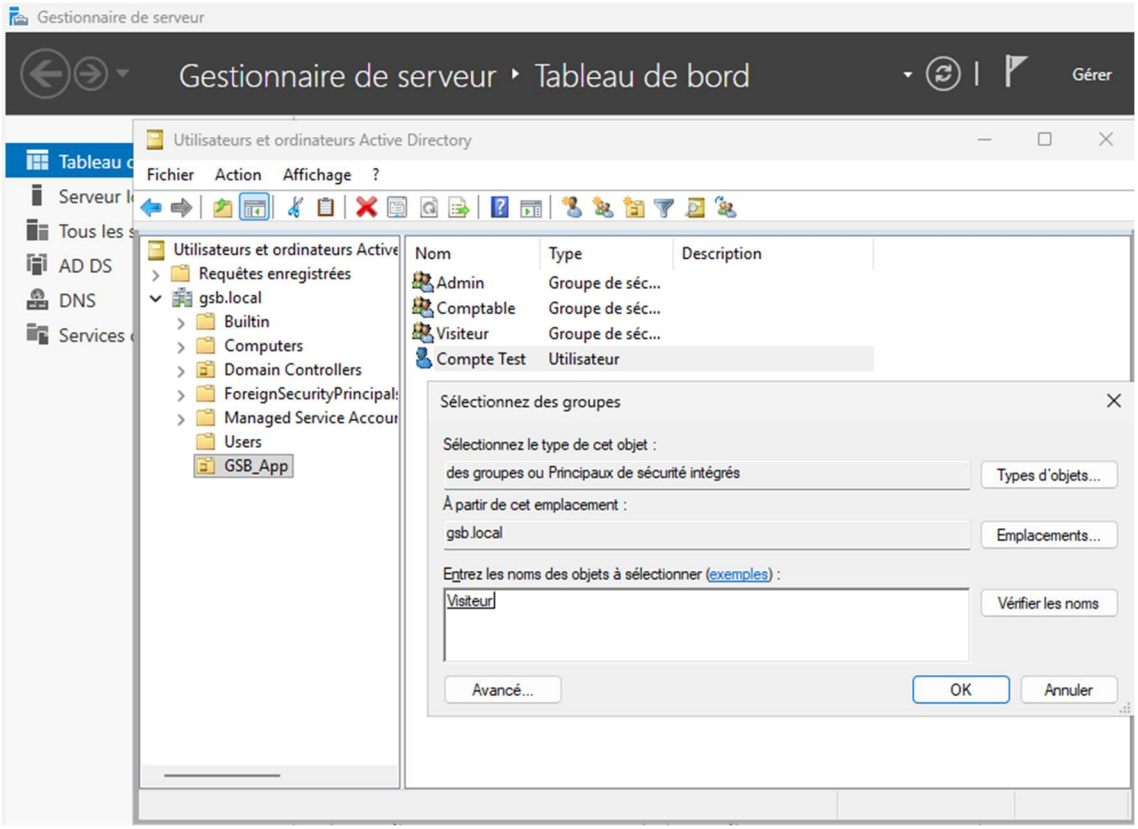
1. Dans l'OU GSB_App, effectuer un clic droit puis sélectionner Nouveau > Groupe.
2. Répéter l'opération pour créer trois groupes de type "Global" / "Sécurité" :
    - Admin
    - Comptables
    - Visiteur



Initialisation d'un compte de test

Afin de valider le futur algorithme de connexion (mapping des rôles), un compte utilisateur de test doit être mis en place.

1. Créer un nouvel utilisateur (ou déplacer un compte existant) nommé jtest à l'intérieur de l'OU GSB_App.



2. Accéder aux propriétés de cet utilisateur, se rendre dans l'onglet Membre de, et l'ajouter manuellement au groupe Comptables.