TP
Windows Server + Client AD

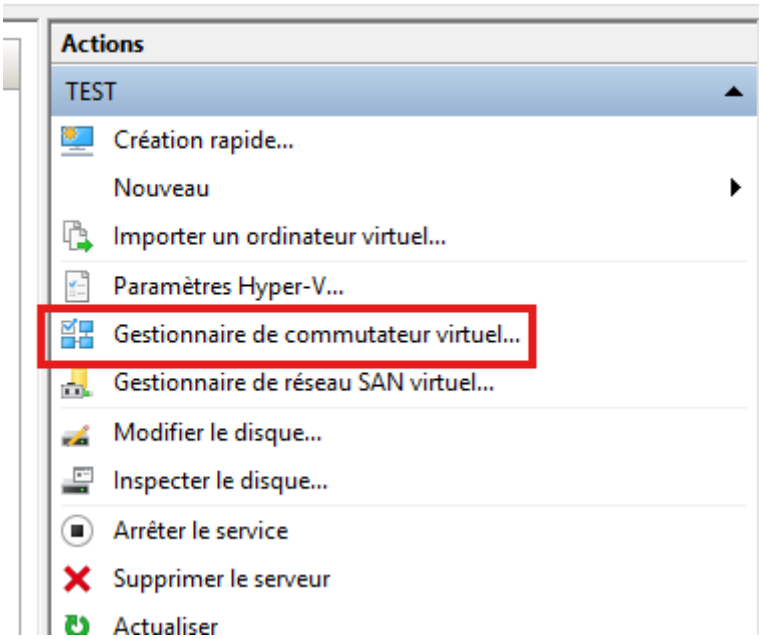
Sommaire

1. Création d'un réseau privé pour nos VM 2
2. Création de la VM « WinSrv2025 » avec interface graphique 4
3. Installation Windows Server 2025 13
4. Installation de Windows Server sans interface graphique 18
5. Installation Windows 11 20
6. Configuration IP et nom des différentes VM 20
7. Mise en place du rôle Active Directory (AD) 28
8. Intégration du poste client dans l'AD 39
9. Création des OU, utilisateurs et groupes dans Active Directory 46
10. Exercice GPO 56
11. Ajout ADMX 63

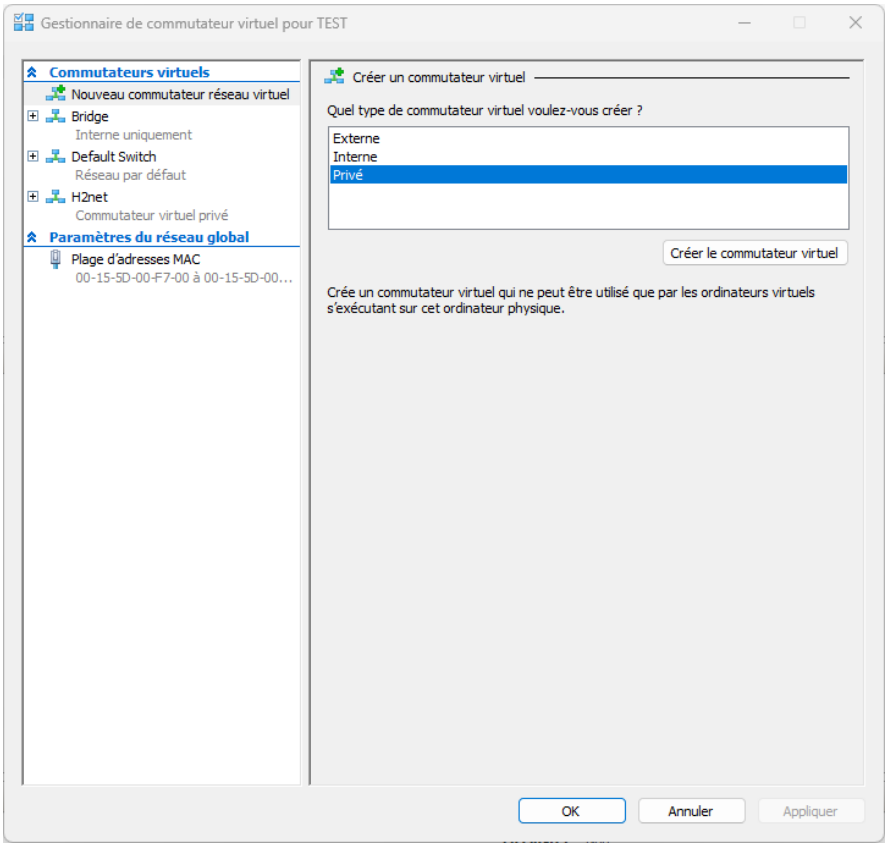
1. Création d'un réseau privé pour nos VM

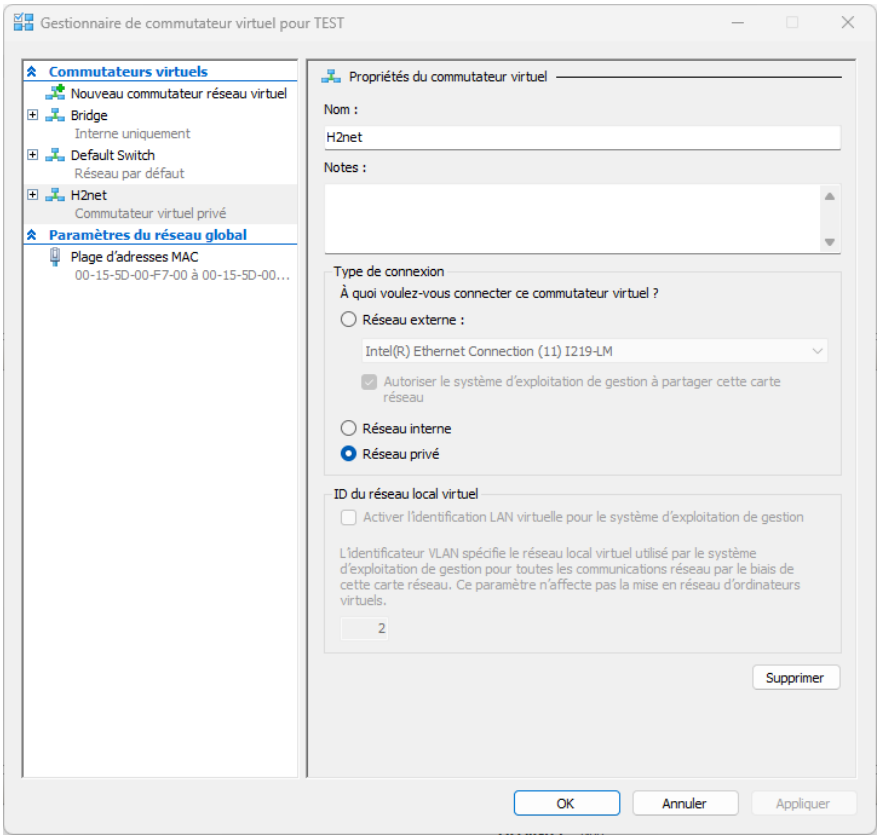
La première étape consiste à créer un commutateur privé pour nos 3 VM afin qu'elles puissent communiquer entre elles sur un sous réseau que nous allons créer par la suite (192.168.140.X avec comme masque 255.255.255.0).

Pour cela, il suffit de se rendre dans Hyper V puis dans le gestionnaire des commutateurs virtuels



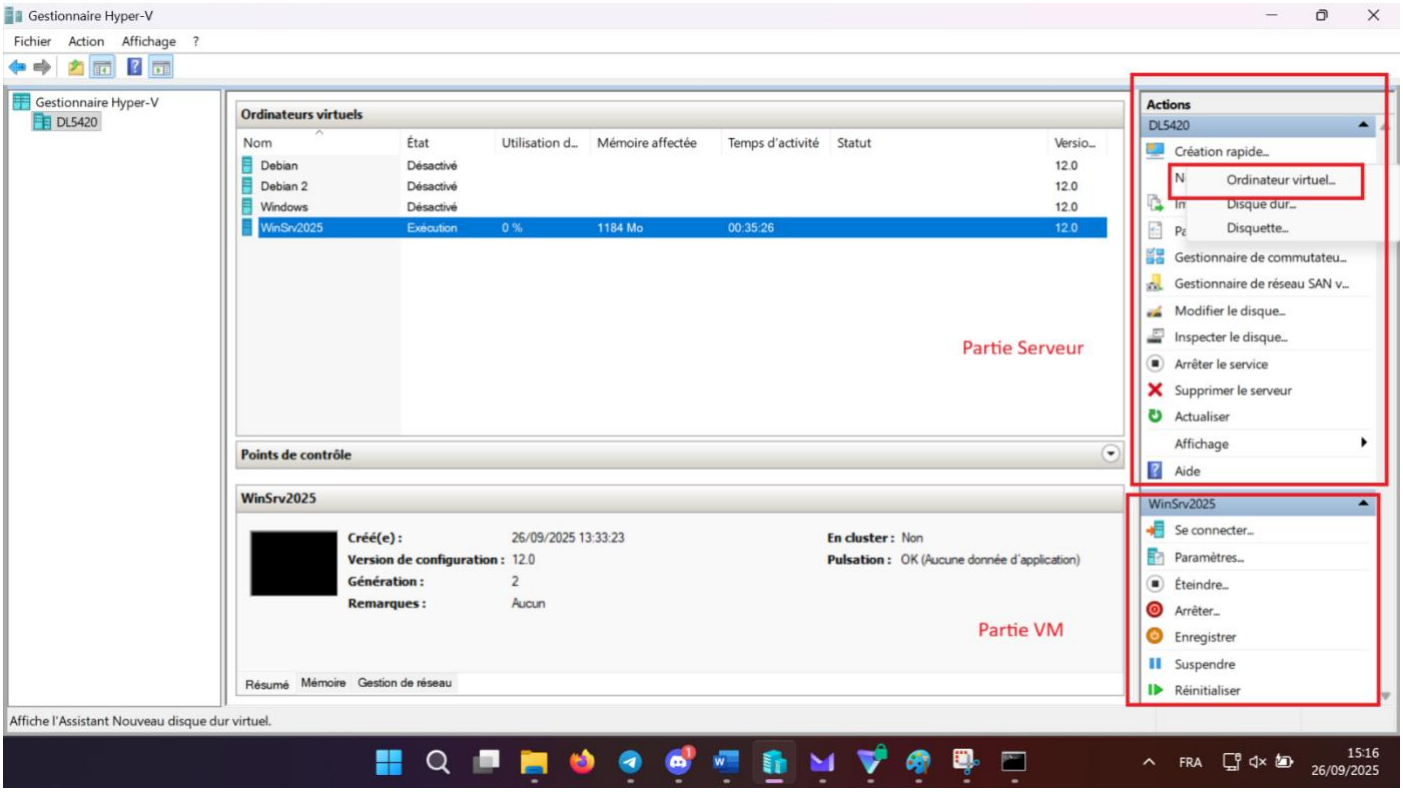
Une fois dans le gestionnaire de commutateur virtuel, nous allons ajouter un nouveau commutateur privé, nous pouvons lui donner le nom qu'on souhaite, ce dernier devra être sélectionné durant la configuration de la machine virtuelle :


Gestionnaire de commutateur virtuel pour TEST
Commutateurs virtuels
Nouveau commutateur réseau virtuel
Bridge
Interne uniquement
Default Switch
Réseau par défaut
H2net
Commutateur virtuel privé
Paramètres du réseau global
Plage d'adresses MAC
00-15-5D-00-F7-00 à 00-15-5D-00…
Créer un commutateur virtuel
Quel type de commutateur virtuel voulez-vous créer ?
Externe
Interne
Privé
Créer le commutateur virtuel
Crée un commutateur virtuel qui ne peut être utilisé que par les ordinateurs virtuels s'exécutant sur cet ordinateur physique.
OK
Annuler
Appliquer

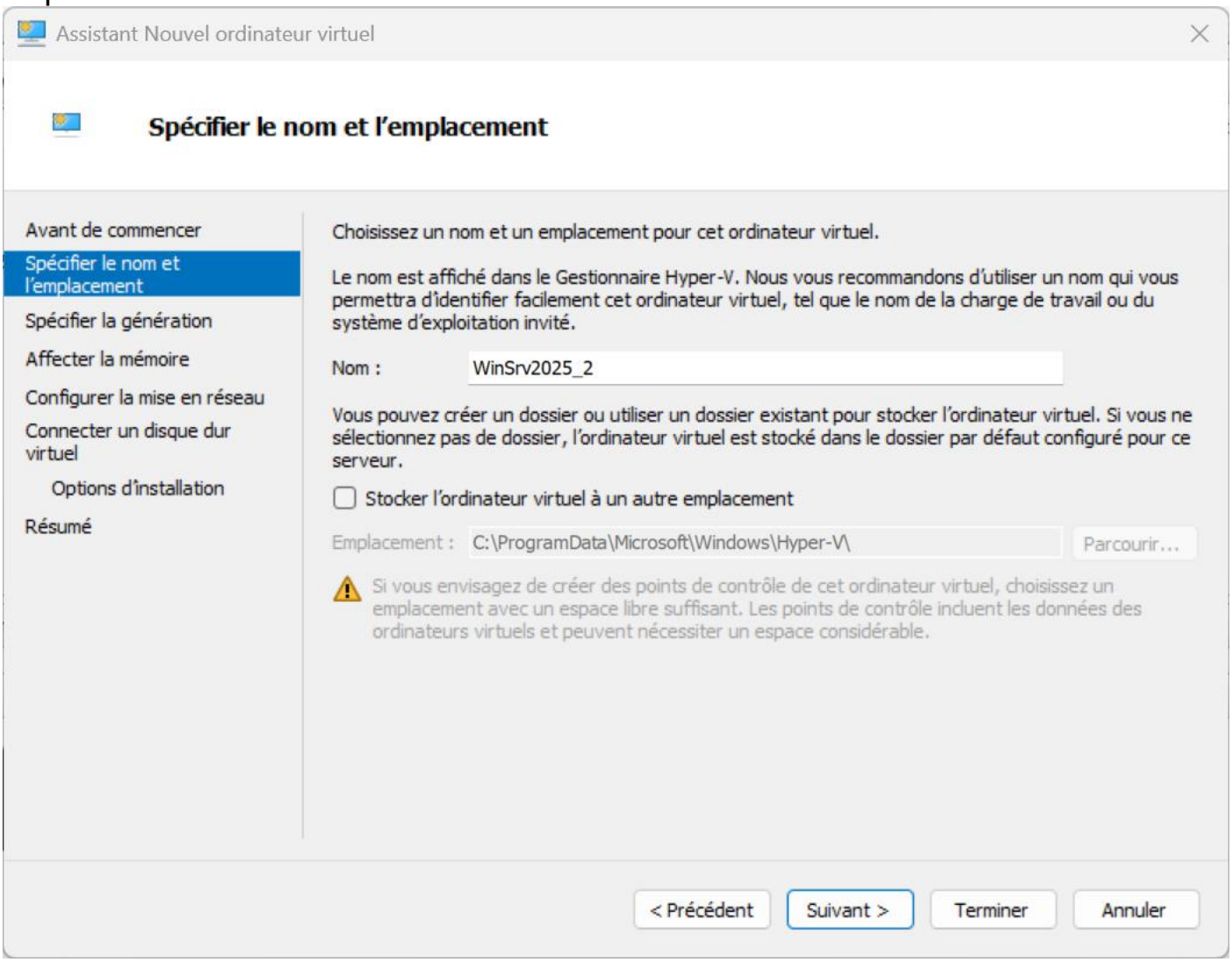

Gestionnaire de commutateur virtuel pour TEST
Commutateurs virtuels
Nouveau commutateur réseau virtuel
Bridge
Interne uniquement
Default Switch
Réseau par défaut
H2net
Commutateur virtuel privé
Paramètres du réseau global
Plage d'adresses MAC
00-15-5D-00-F7-00 à 00-15-5D-00…
Propriétés du commutateur virtuel
Nom :
H2net
Notes :
Type de connexion
À quoi voulez-vous connecter ce commutateur virtuel ?
Réseau externe :
Intel(R) Ethernet Connection (11) I219-LM
Autoriser le système d'exploitation de gestion à partager cette carte réseau
Réseau interne
Réseau privé
ID du réseau local virtuel
Activer l'identification LAN virtuelle pour le système d'exploitation de gestion
L'identificateur VLAN spécifie le réseau local virtuel utilisé par le système d'exploitation de gestion pour toutes les communications réseau par le biais de cette carte réseau. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs virtuels.
2
Supprimer
OK
Annuler
Appliquer

2. Création de la VM « WinSrv2025 » avec interface graphique

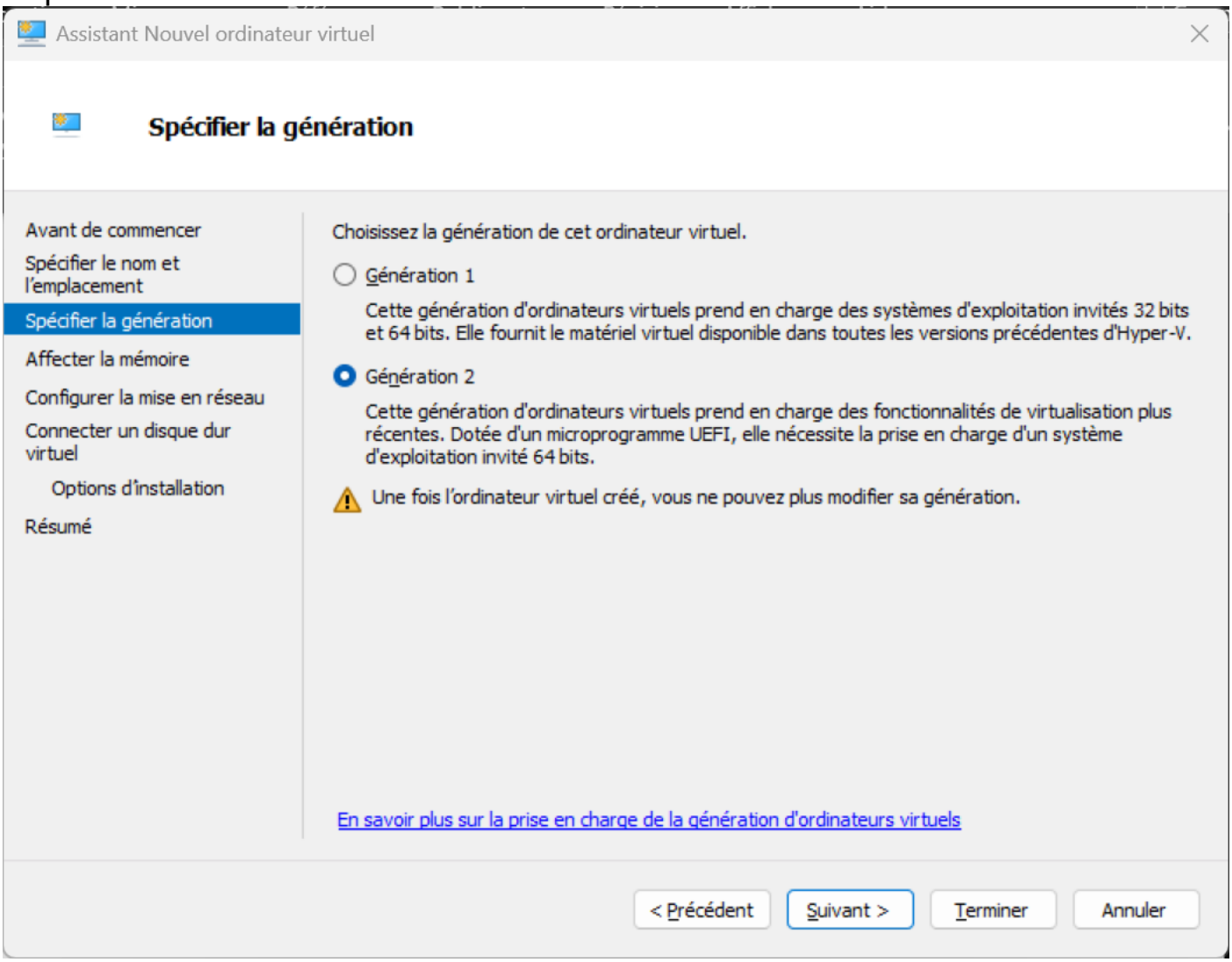
Pour créer notre VM, nous allons nous rendre sur gestionnaire Hyper V, puis dans la section pour gérer notre serveur, nous allons cliquer sur « Nouveau » puis « Ordinateur virtuel… »



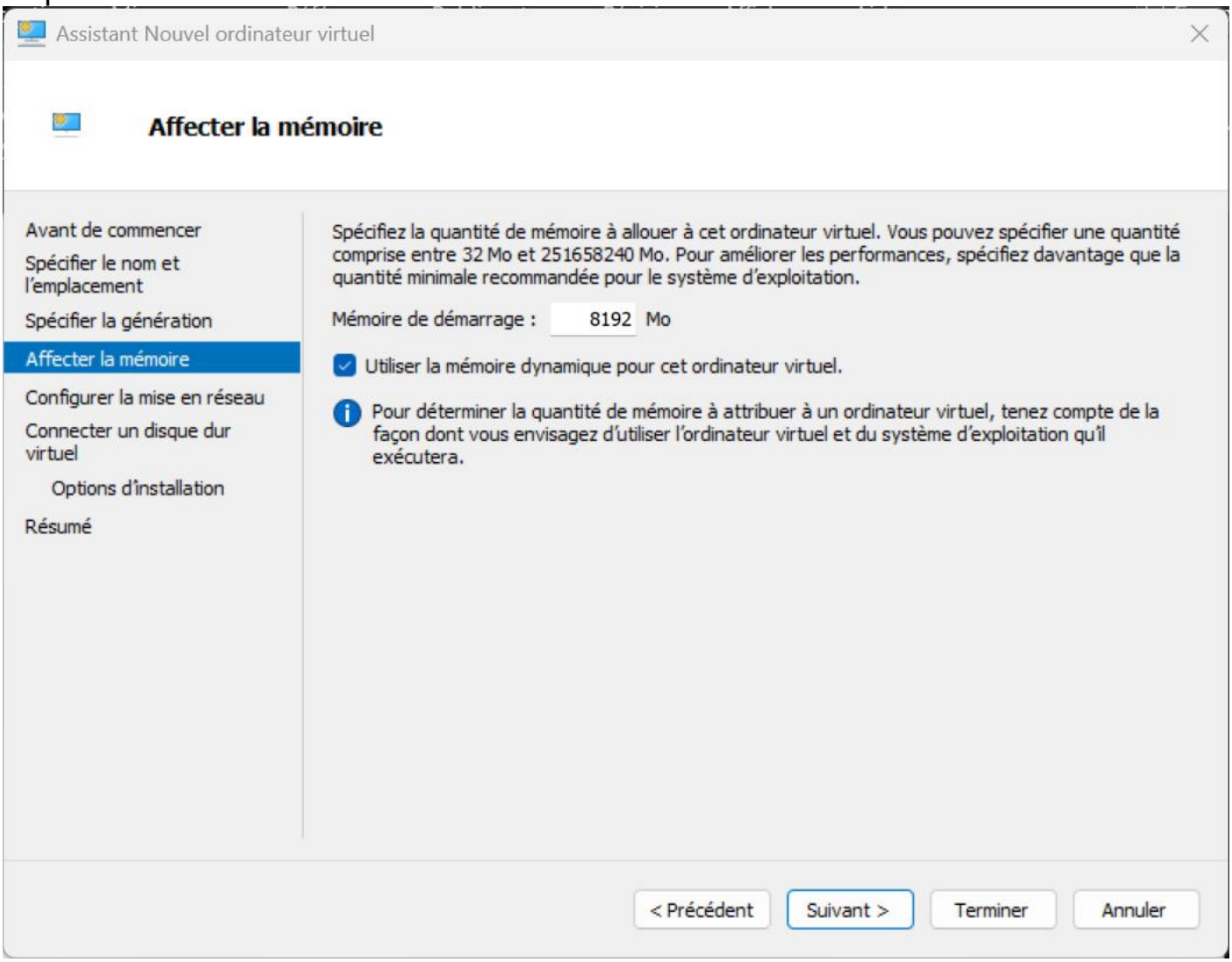
Nous allons donc créer un nouvel ordinateur virtuel



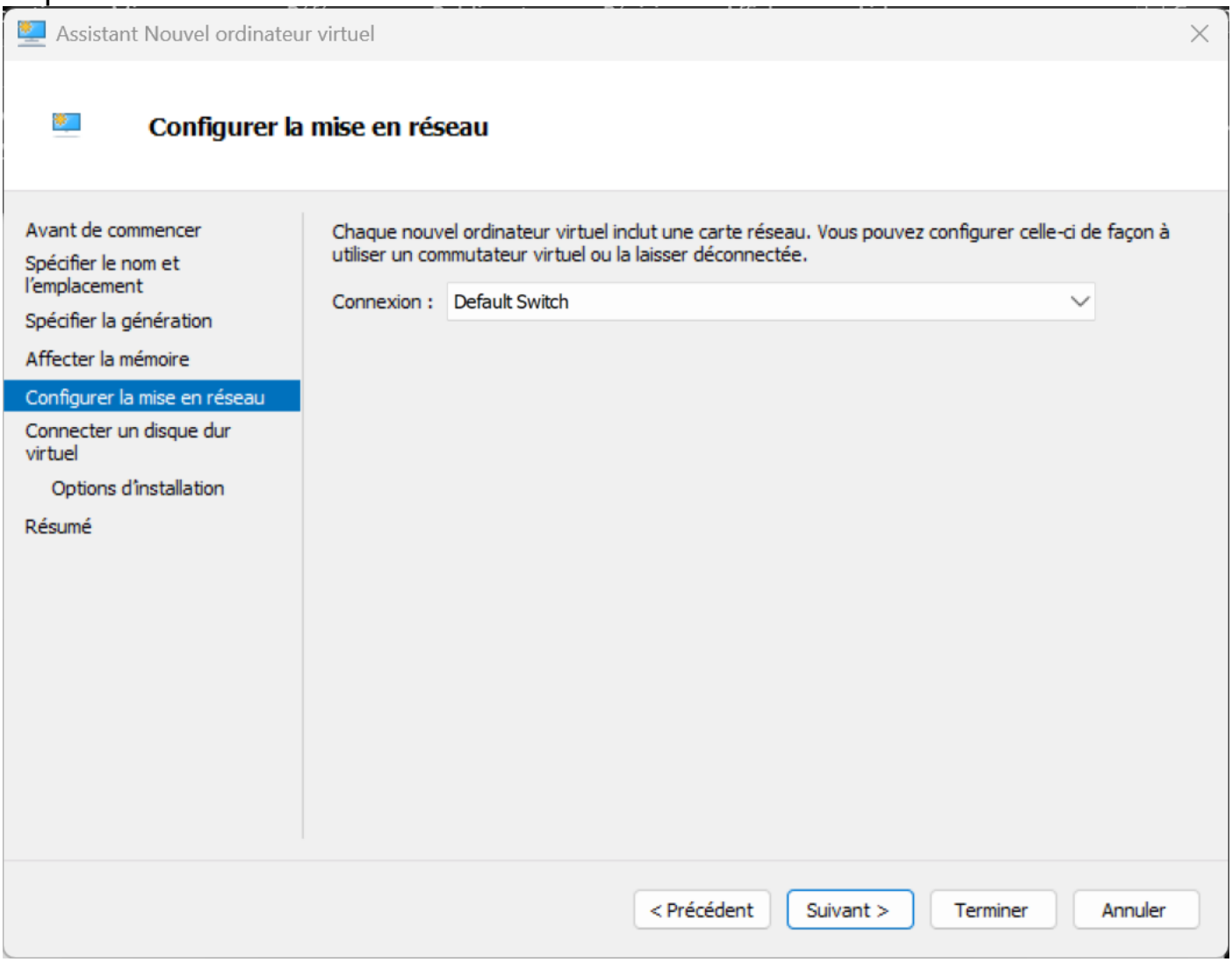
Une fois le nom de la VM définie, nous allons choisir la génération de cette dernière, pour un Windows Server 2025 (basé sur Windows 11), nous devons obligatoirement choisir la génération 2 avec UEFI/Secure boot :



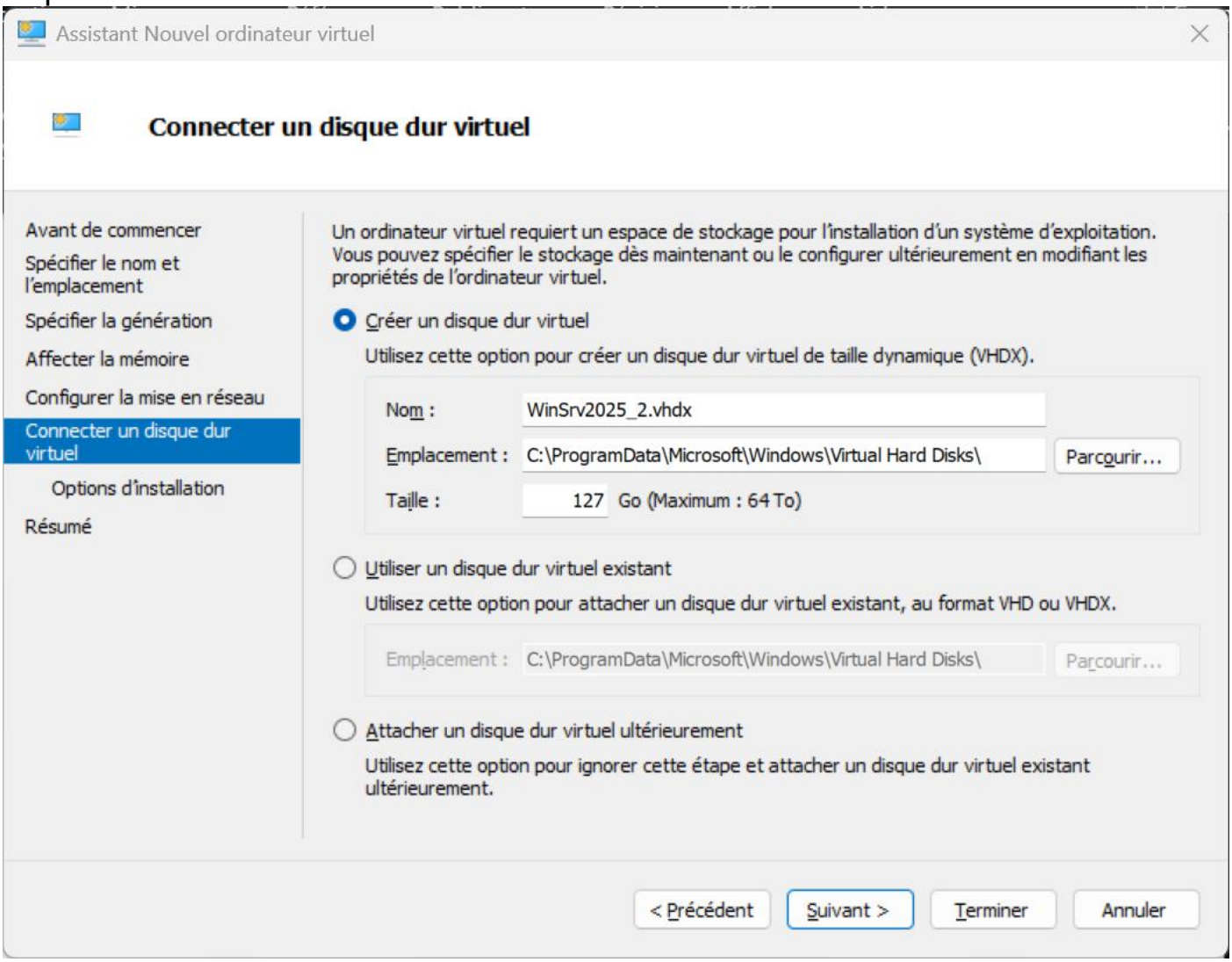
Maintenant, nous allons assigner la ram à notre VM, pour un Windows Server, il est recommandé de définir 8192 MB de ram (soit 8 Giga) :



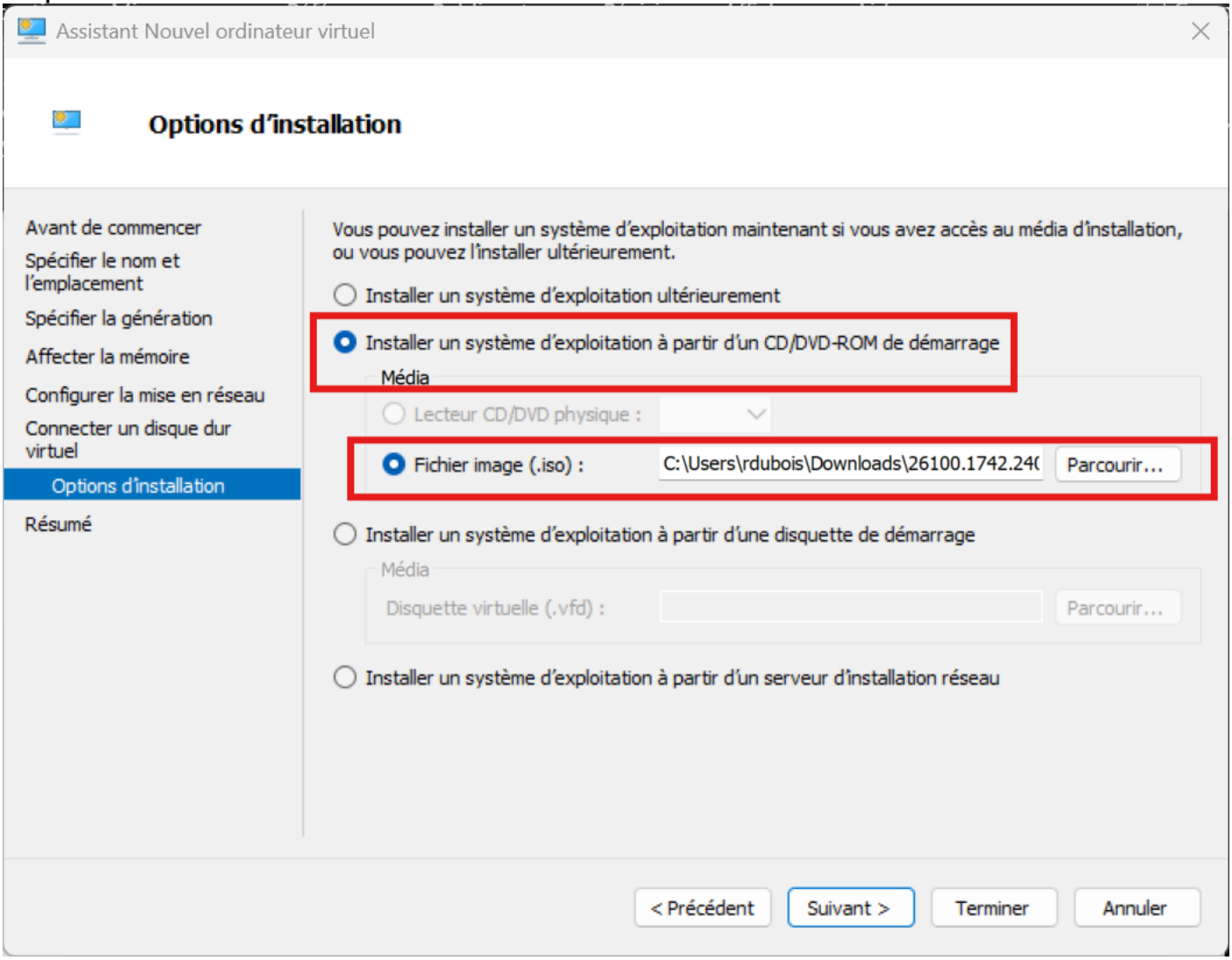
La prochaine étape est la configuration du réseau, pour avoir un accès à Internet, il faut sélectionner le réseau « Default Switch » présent par défaut sur Hyper V :



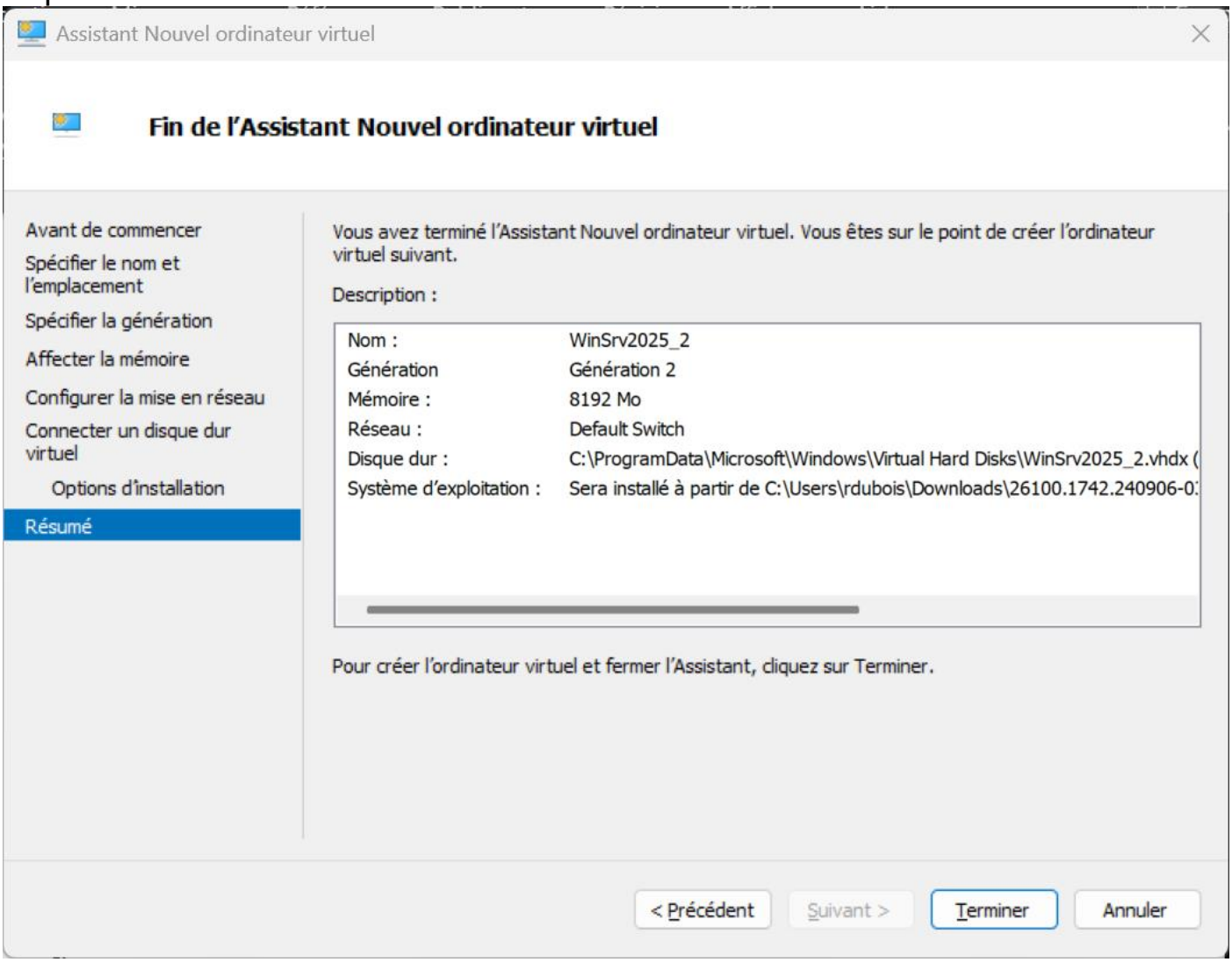
Dans la prochaine étape, nous allons définir le stockage et l'emplacement du disque pour notre VM, par défaut nous n'allons pas toucher à l'emplacement, cependant nous allons définir un disque assez grand (127 giga) pour pouvoir installer notre Windows Server :



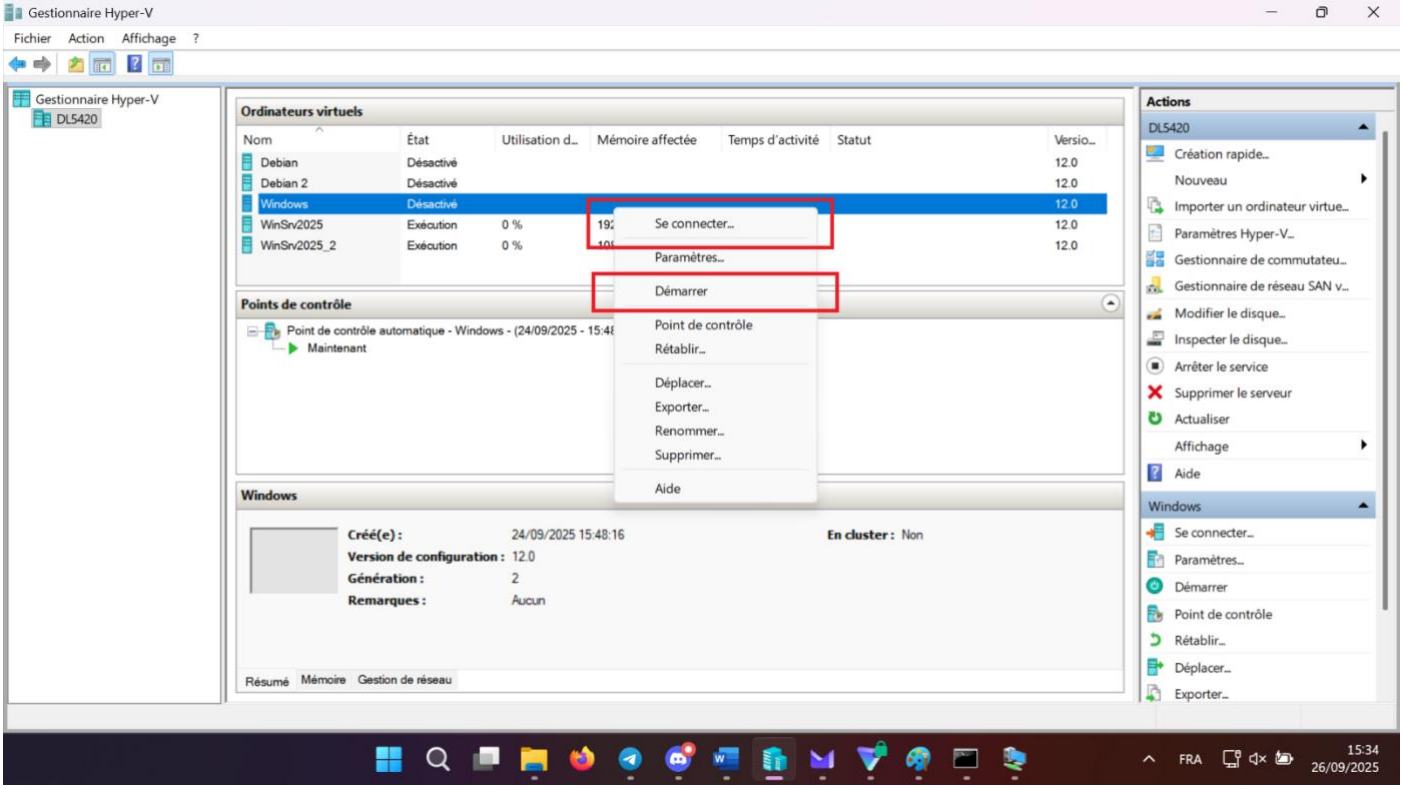
La dernière étape est de sélectionner l'image ISO que nous avons précédemment téléchargé :



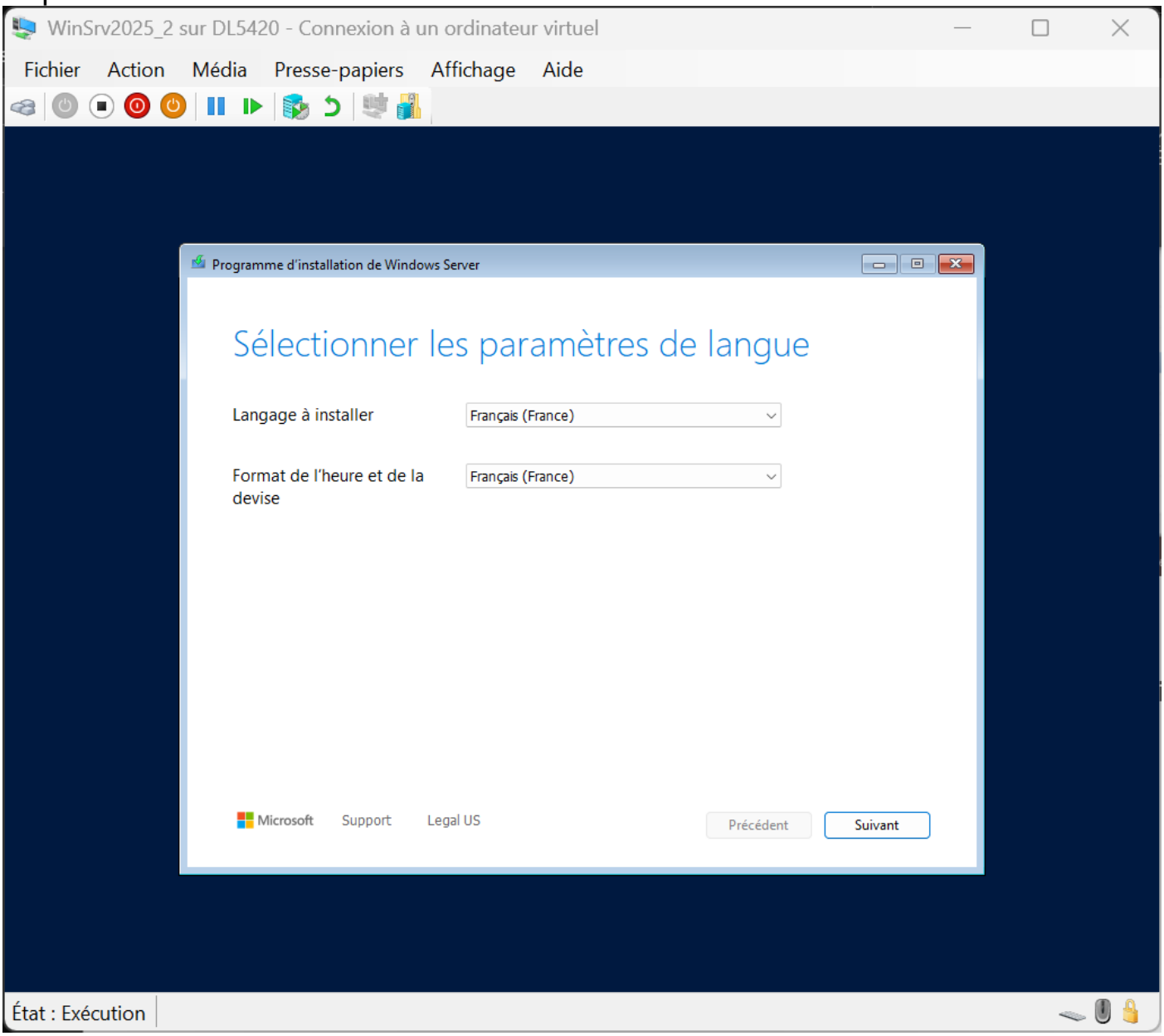
Une fois la configuration terminée, nous devons simplement valider les paramètres précédemment effectués puis cliquer sur « Terminer » :



Une fois notre VM créer, nous pouvons la démarrer en faisant clic droit, puis « Démarrer », puis nous allons pouvoir se connecter dessus en cliquant sur « Se connecter » :

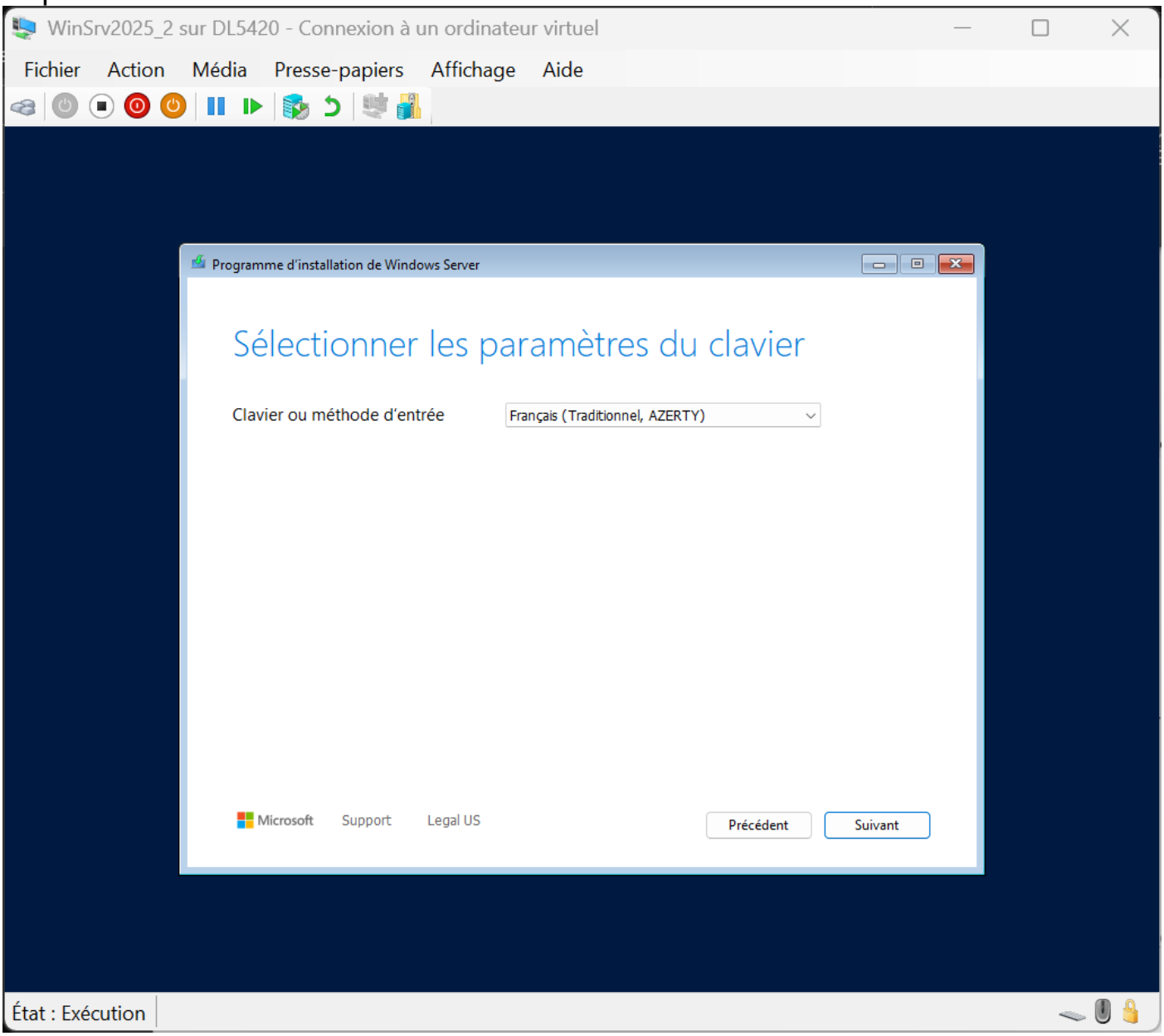


Une fois la VM démarré, nous allons pouvoir passer à l'installation de cette dernière :

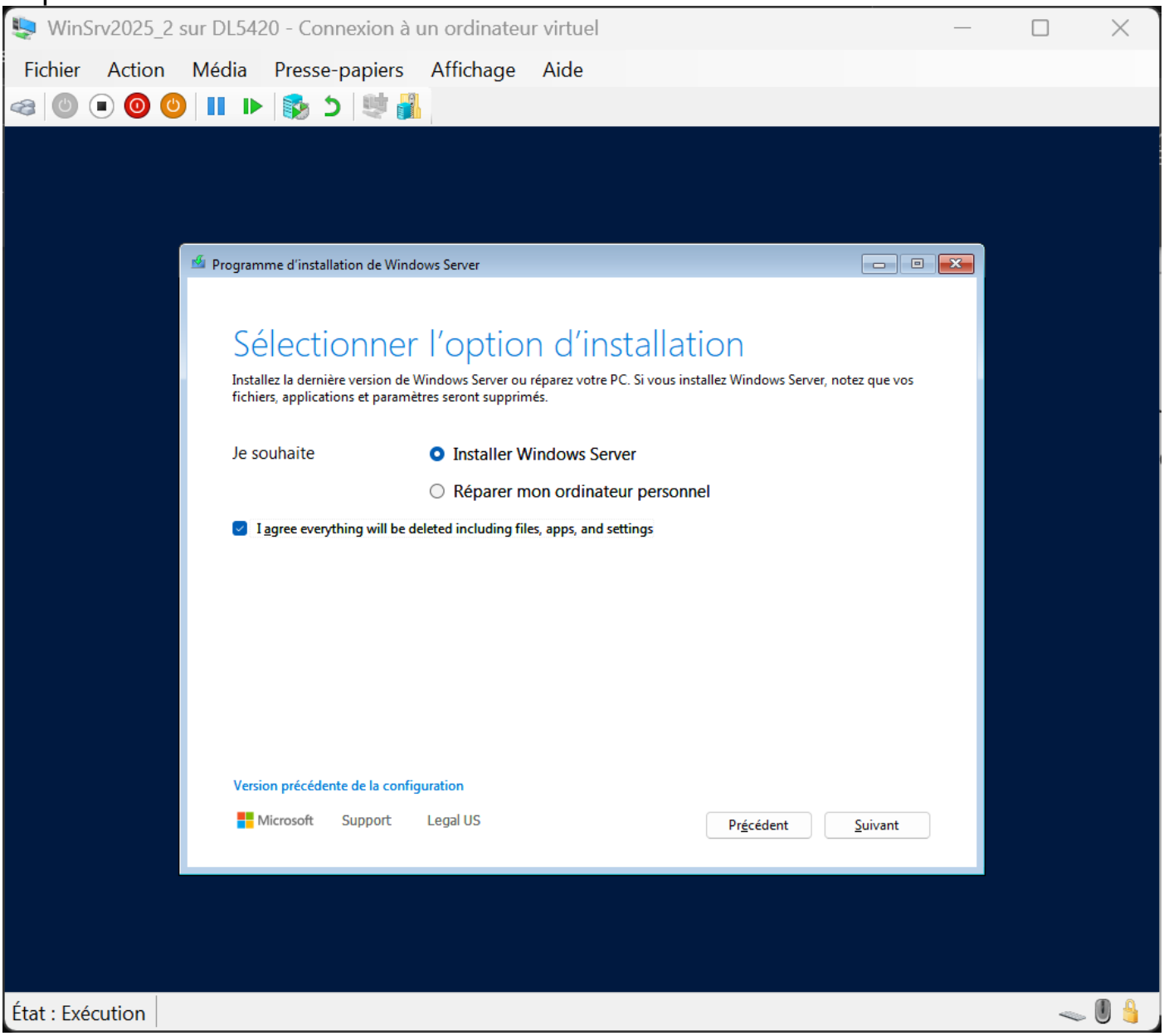


3. Installation Windows Server 2025

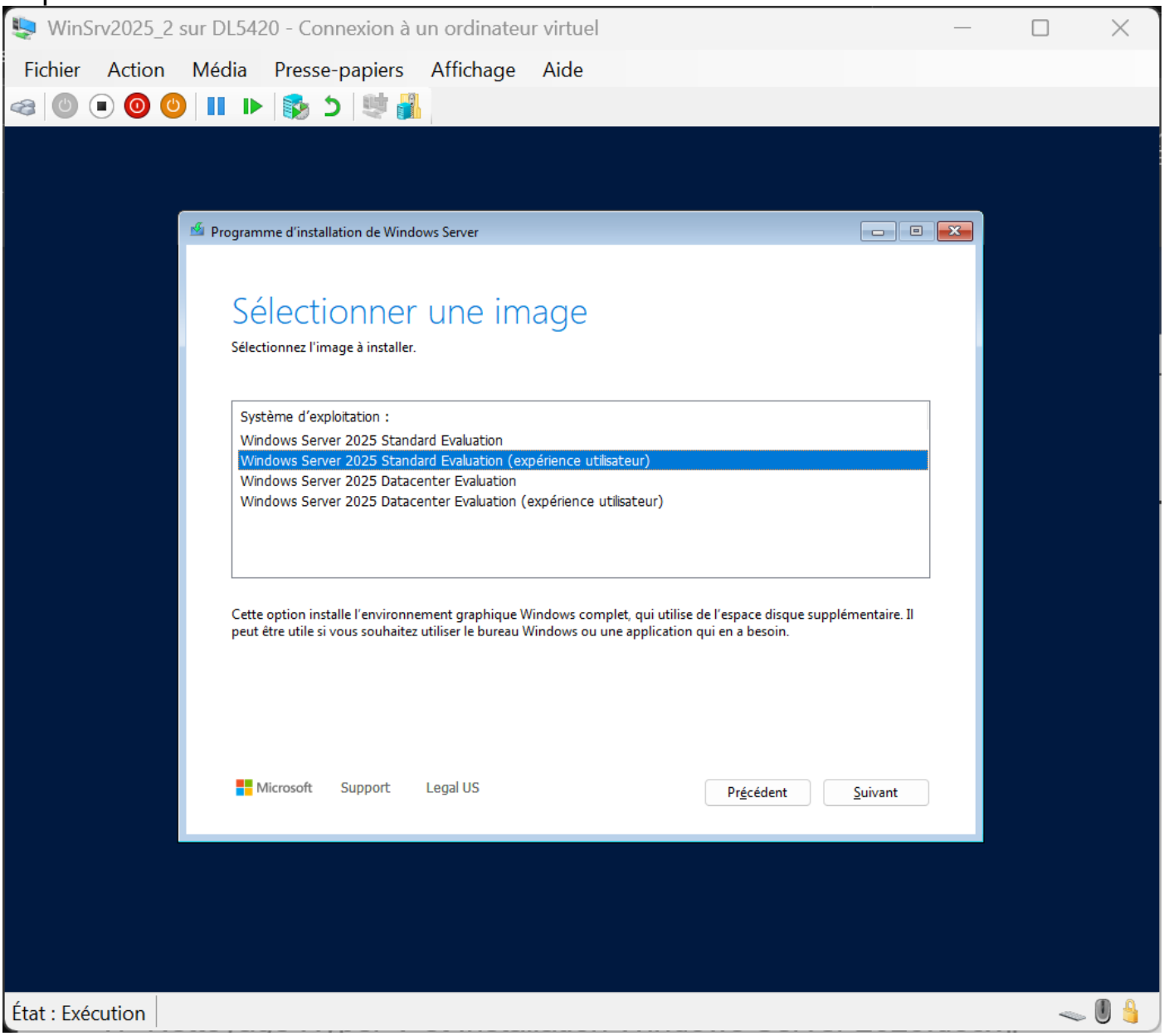
Une fois sur l'écran d'installation, nous allons laisser la langue et le format de l'heure en français, puis nous allons cliquer sur « Suivant » pour continuer l'installation. La disposition du clavier doit être défini en français puis nous pouvons cliquer sur « Suivant » :



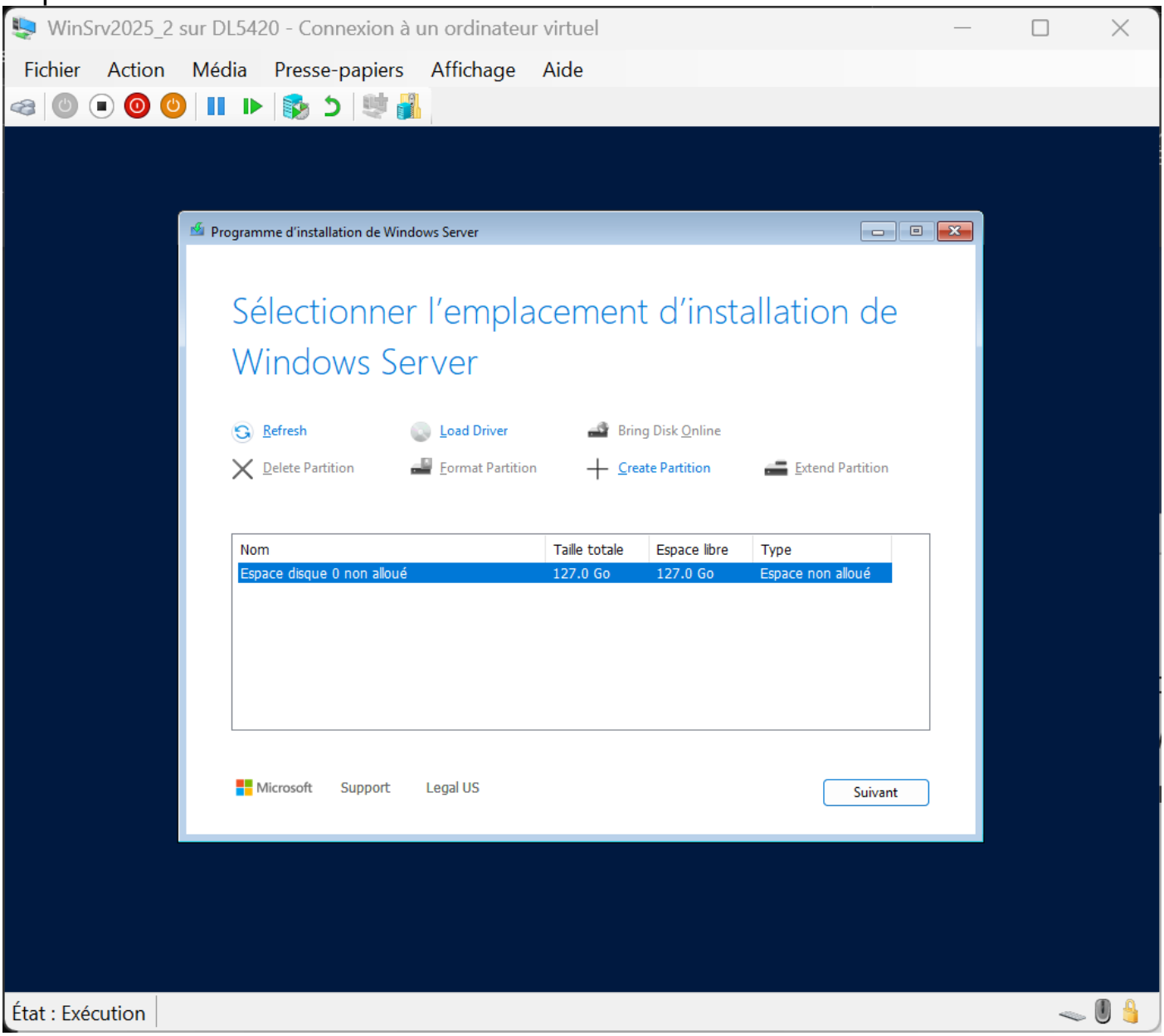
Une ceci défini, nous allons sélectionner « Installer Windows Server » et nous allons cocher l'option « I agree everything will be deleted including files, apps and settings » pour confirmer la suppression puis « Suivant » :



Une fois sur l'écran de sélection des éditions, nous allons sélectionner l'édition « Windows Server 2025 Standard Evaluation (expérience utilisateur) :



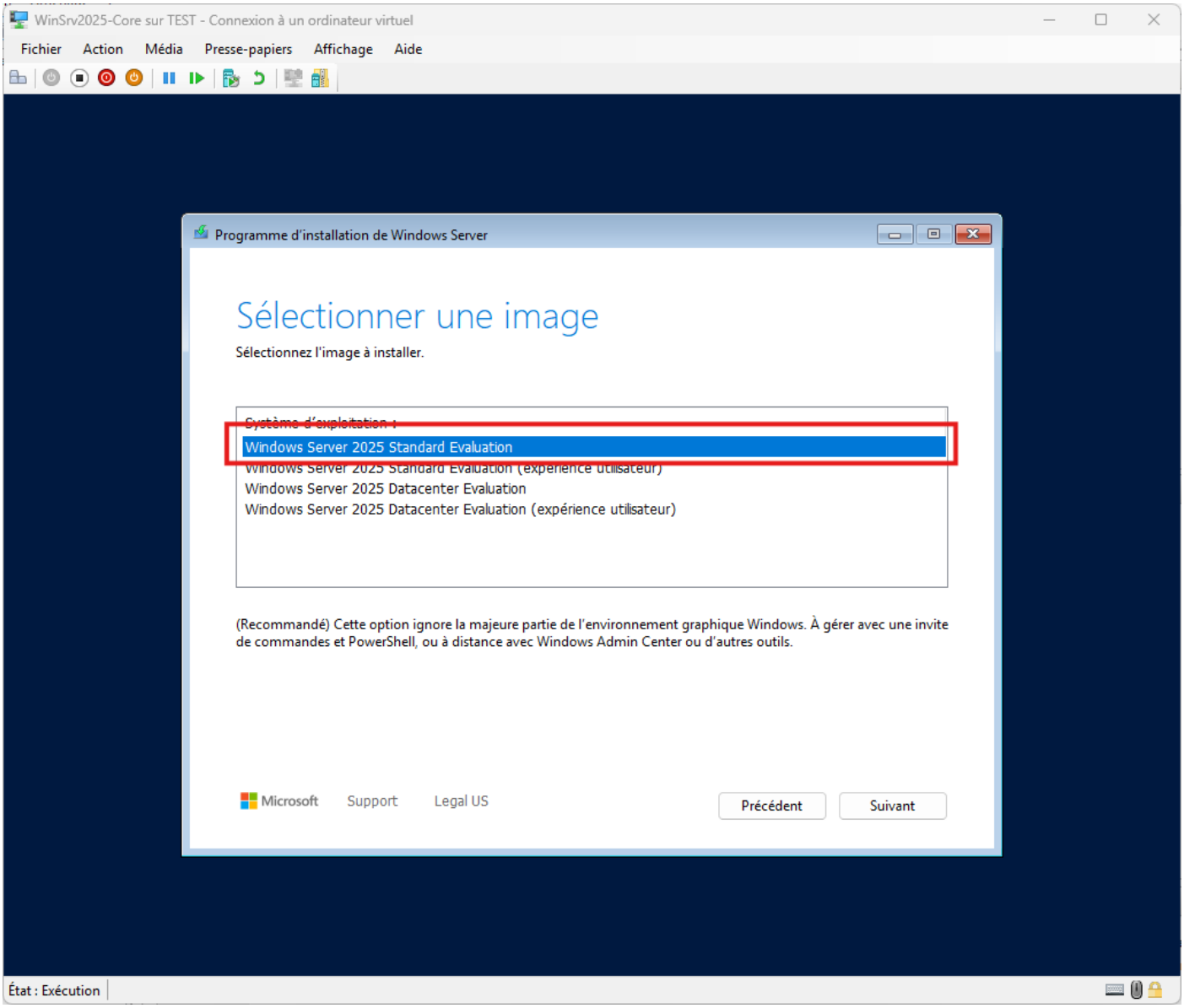
Une fois ceci fait, nous pouvons cliquer sur « Suivant », accepter les conditions d'utilisations de Microsoft, puis sélectionner le disque ou sera installé notre Windows 11. Dans notre cas, nous n'avons qu'un disque précédemment créer sur notre VM :



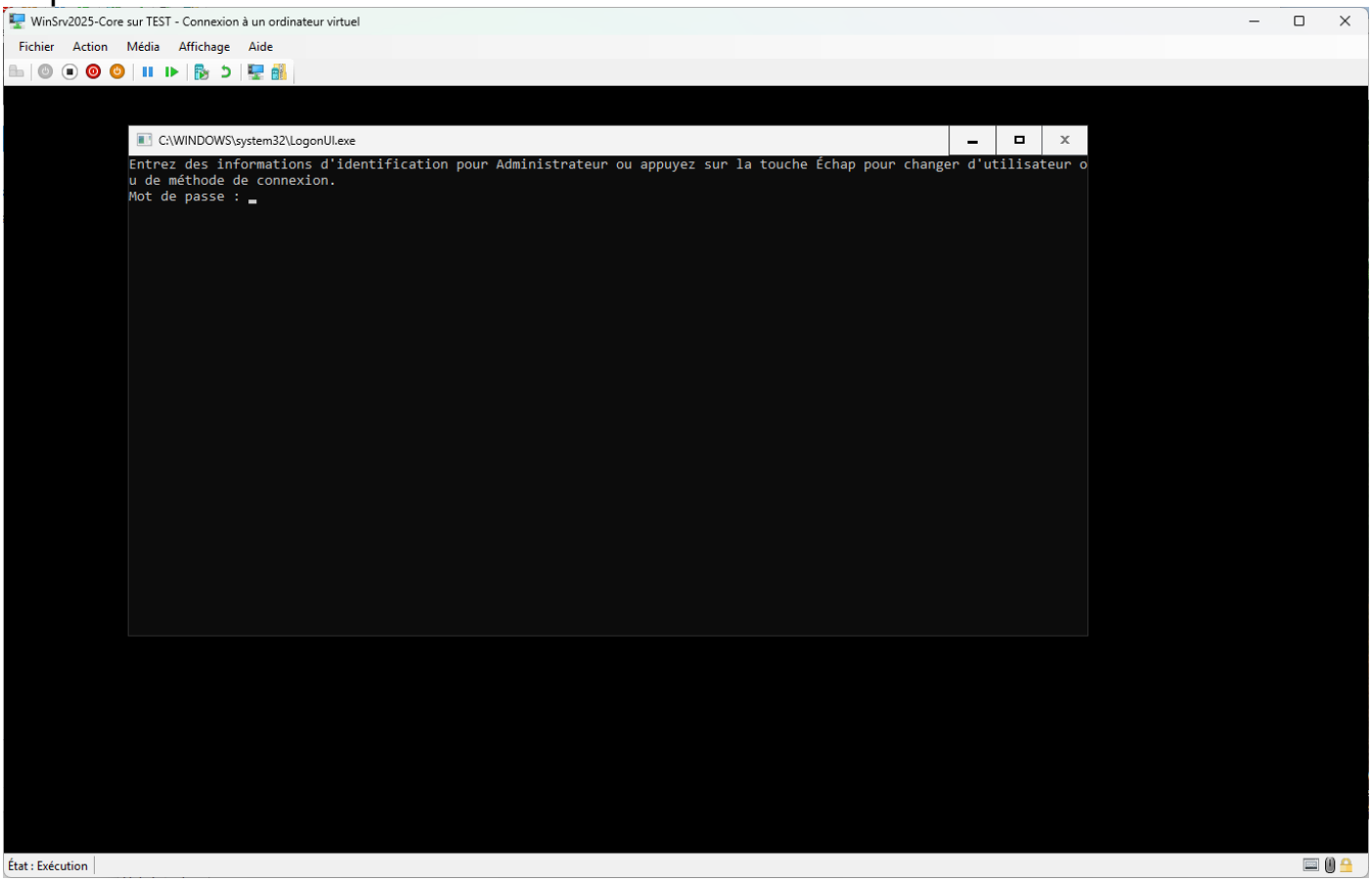
Une fois ceci fait, l'installation va débuter puis durer plusieurs minutes, il suffit de patienter. La VM va redémarrer à plusieurs reprises jusqu'à demander un mot de passe pour l'utilisateur « Administrateur ». Une fois ceci fait, il suffit de se connecter et notre installation de Windows Server est maintenant fini !

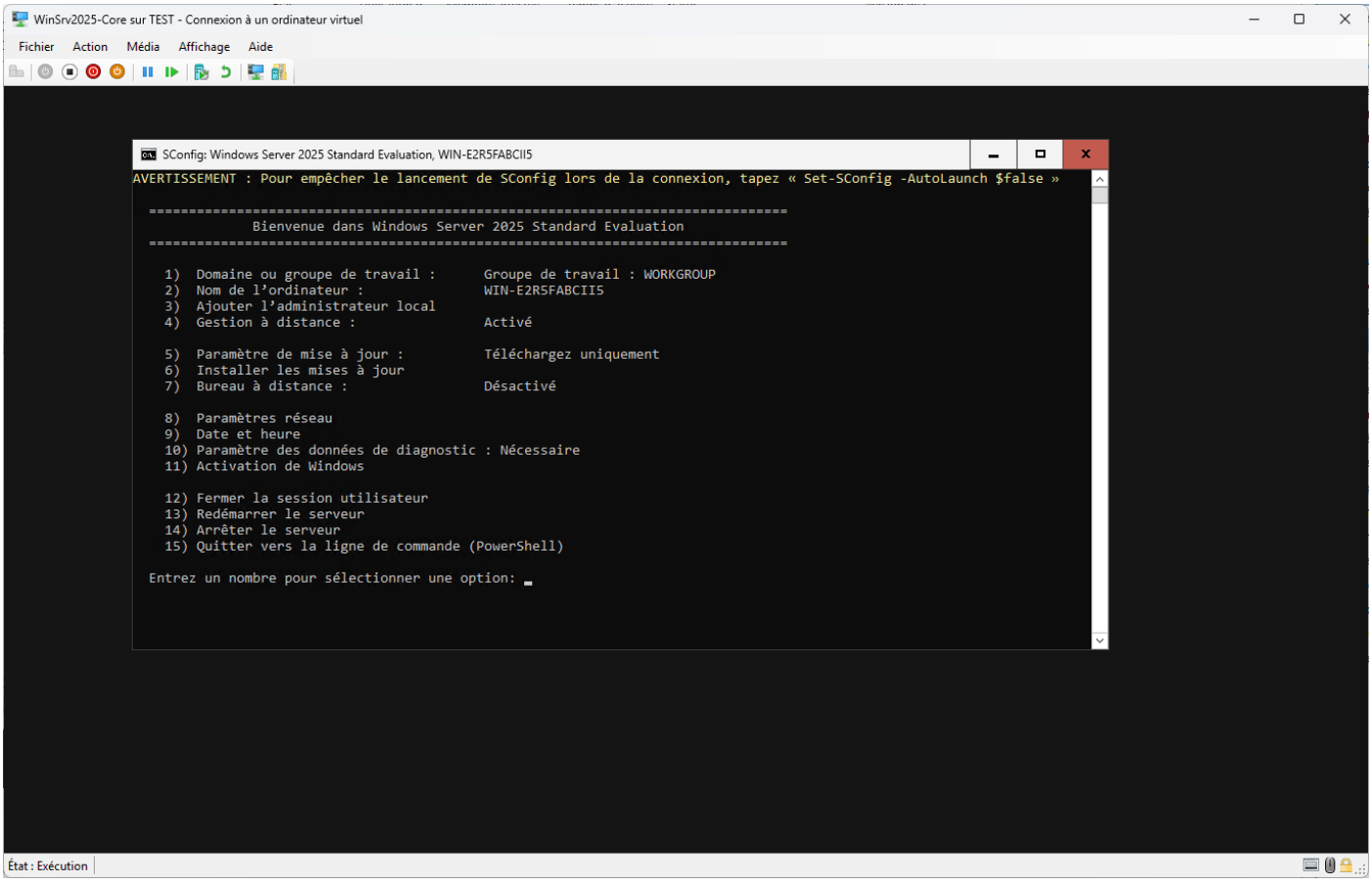
4. Installation de Windows Server sans interface graphique

Cette fois ci, nous allons installer la version sans interface graphique de Windows Server 2025. Les étapes sont similaires à celle effectué précédemment, cependant, pendant le choix de l'édition de Windows, il est important de sélectionner l'édition sans interface graphique :



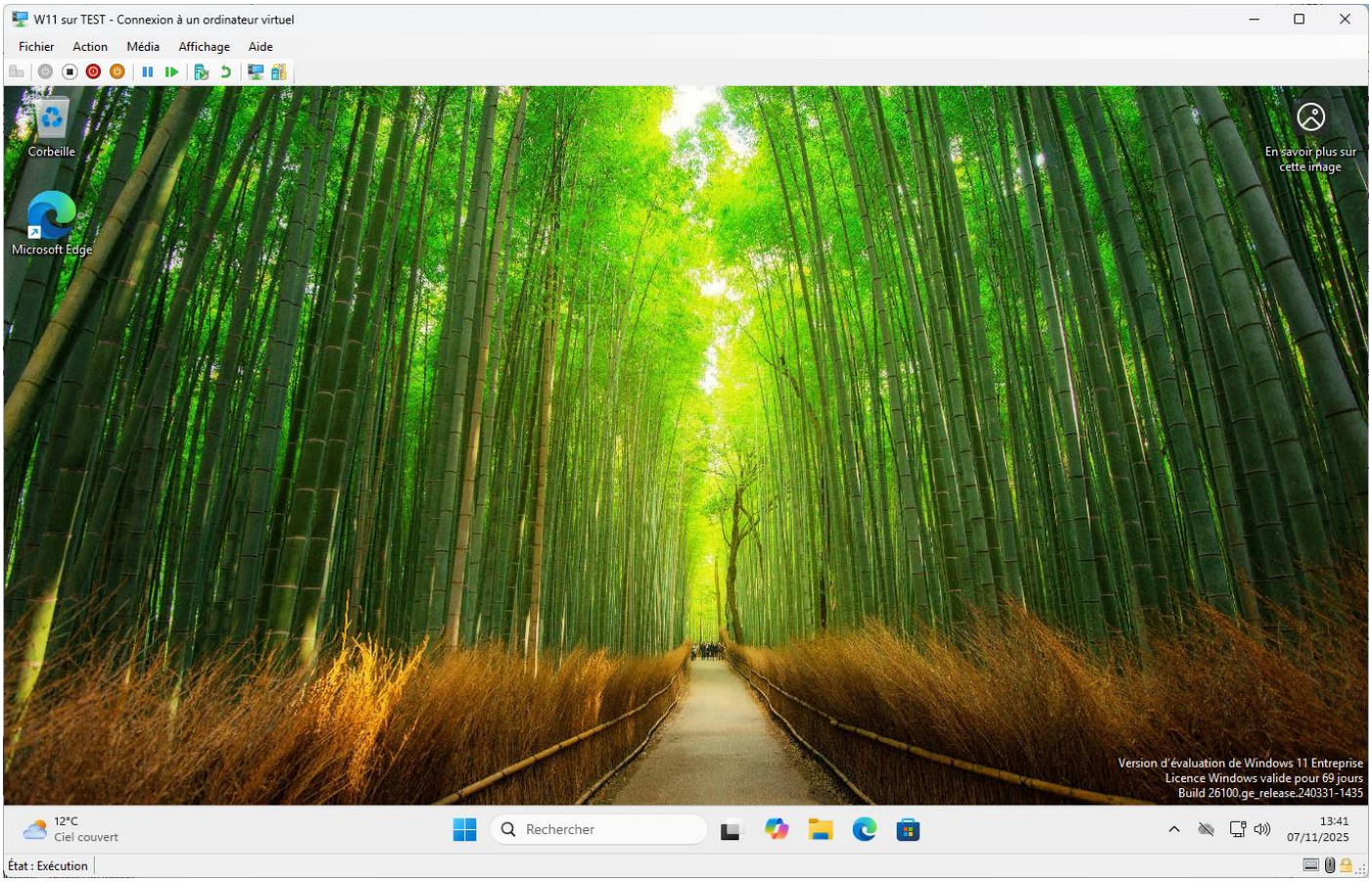
Une fois l'installation terminée, il faut définir un mot de passe, tout se réalise dans le terminal étant donné qu'aucune interface est présente sur le serveur


WinSrv2025-Core sur TEST - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
C:\WINDOWS\system32\LogonUI.exe
Entrez des informations d'identification pour Administrateur ou appuyez sur la touche Échap pour changer d'utilisateur o
u de méthode de connexion.
Mot de passe :
État : Exécution


WinSrv2025-Core sur TEST - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
SConfig: Windows Server 2025 Standard Evaluation, WIN-E2R5FABCII5
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig -AutoLaunch $false »
Bienvenue dans Windows Server 2025 Standard Evaluation
1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
2) Nom de l'ordinateur : WIN-E2R5FABCII5
3) Ajouter l'administrateur local
4) Gestion à distance : Activé
5) Paramètre de mise à jour : Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance : Désactivé
8) Paramètres réseau
9) Date et heure
10) Paramètre des données de diagnostic : Nécessaire
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)
Entrez un nombre pour sélectionner une option:
État : Exécution

5. Installation Windows 11

Les mêmes étapes sont réalisées avec Windows 11, cependant, il est important de bien utiliser l'ISO de Windows 11 dans Hyper-V. Les étapes sont similaires à celles réalisées sur Windows Server. Attention à bien sélectionner l'édition professionnel de Windows 11.



6. Configuration IP et nom des différentes VM

Avant de réaliser notre réseau, nous allons pré définir des IP entre les machines avec un nom d'hôte afin qu'on puisse les identifier plus facilement :

Commutateur virtuel : H2net (Commutateur privé)

WinSrv2025 (Serveur Graphique avec AD)

OS : Windows Server 2025

Adresse IP : 192.168.50.1

Masque : 255.255.255.0

Nom d'hôte : Server1

WinSrv2025Core (Serveur sans interface graphique)

OS : Windows Server 2025 Core

Adresse IP : 192.168.50.2

Masque : 255.255.255.0

Nom d'hôte : Server2

W11 (PC sous Windows 11)

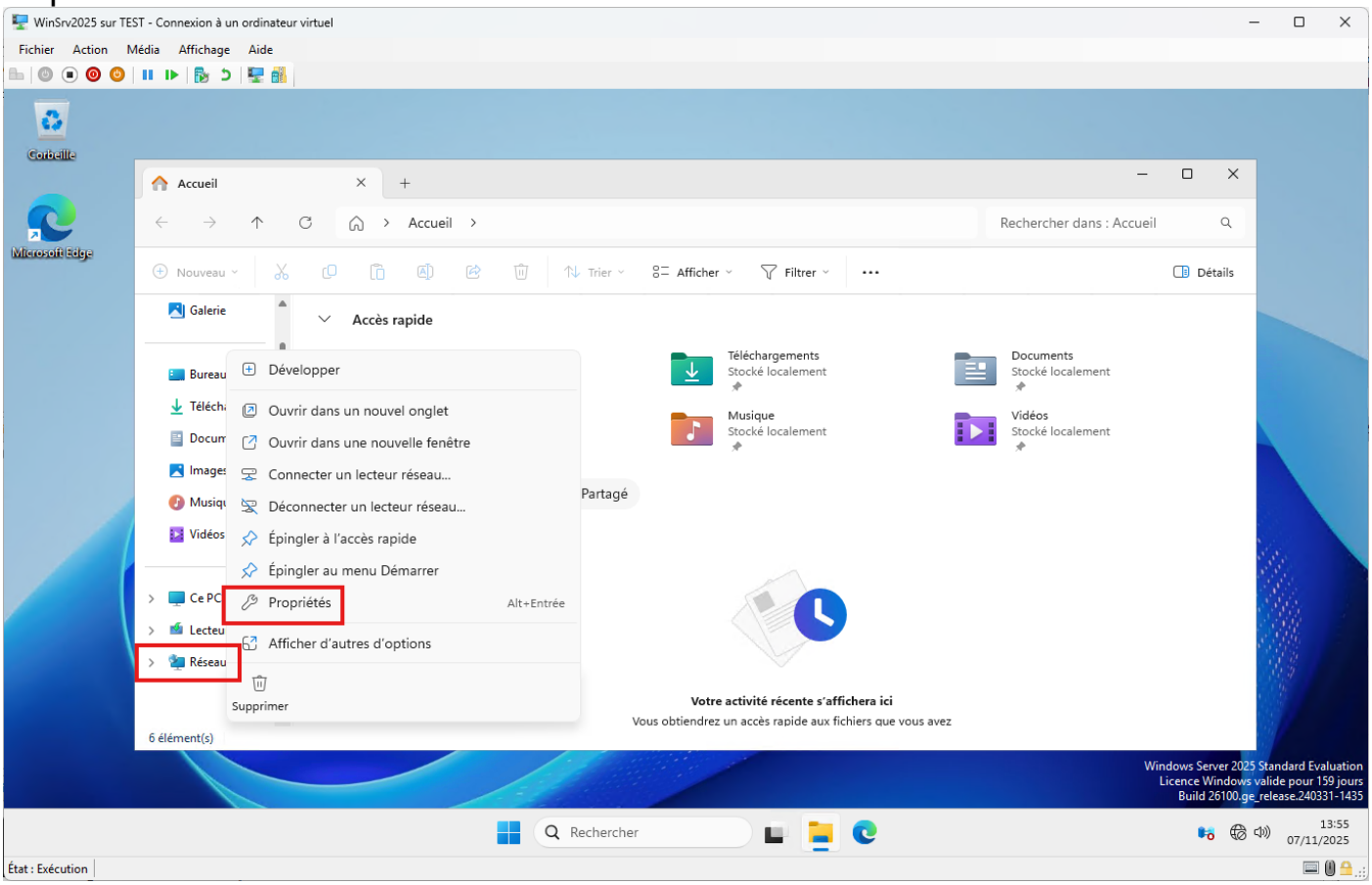
OS : Windows 11

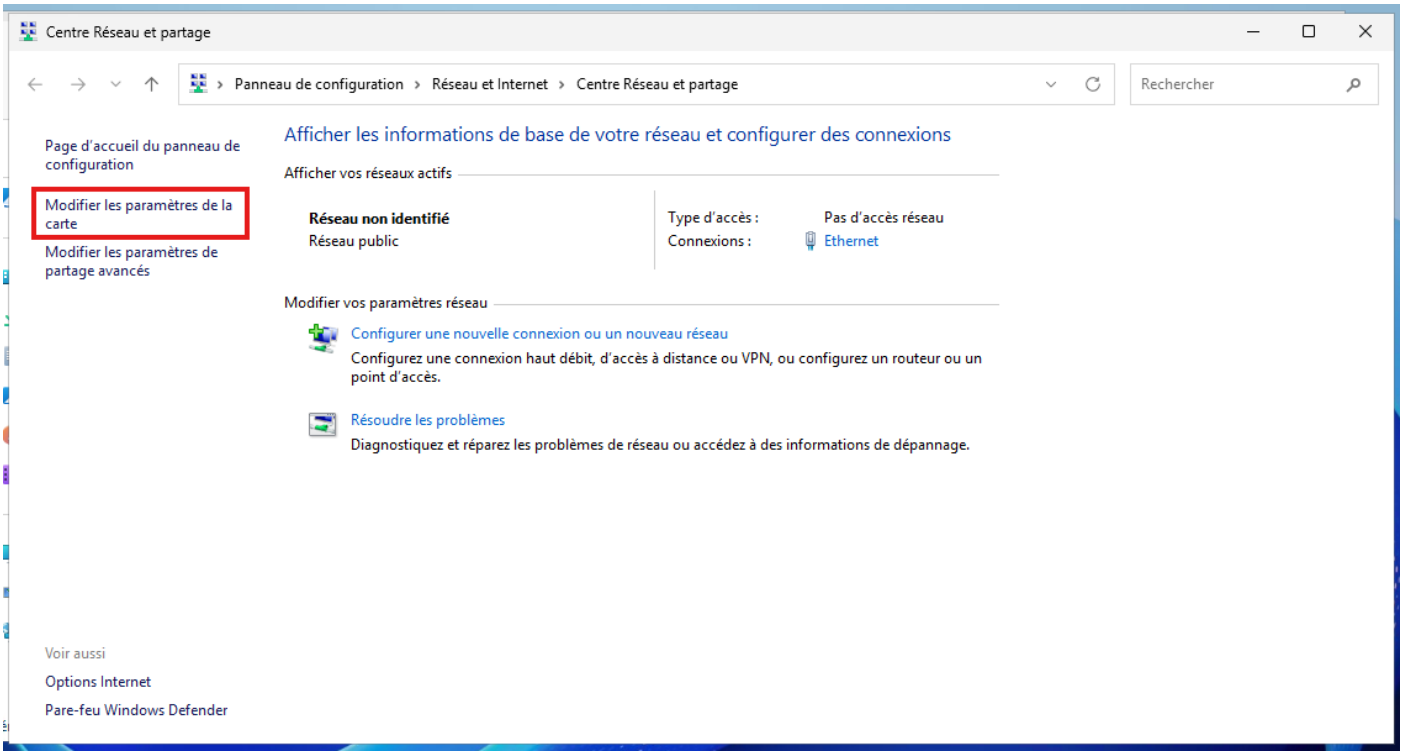
Adresse IP : 192.168.50.3

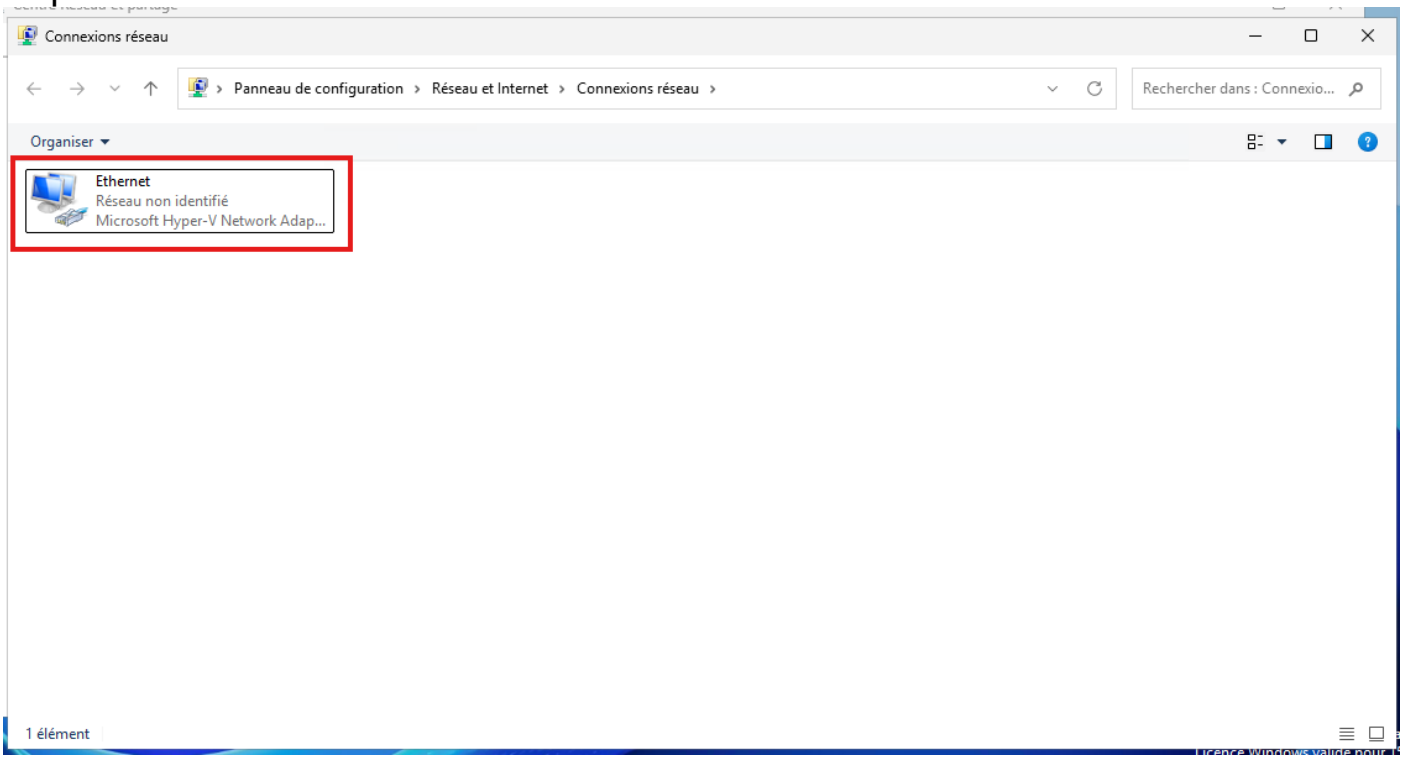
Masque : 255.255.255.0

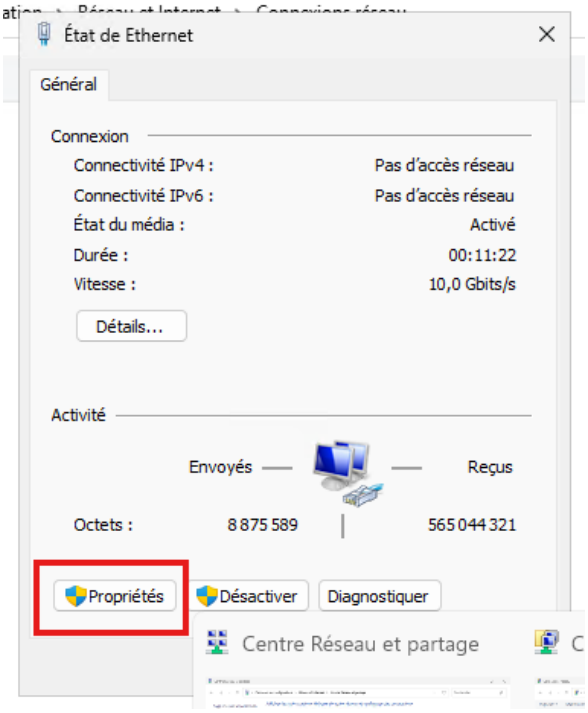
Nom d'hôte : PC1

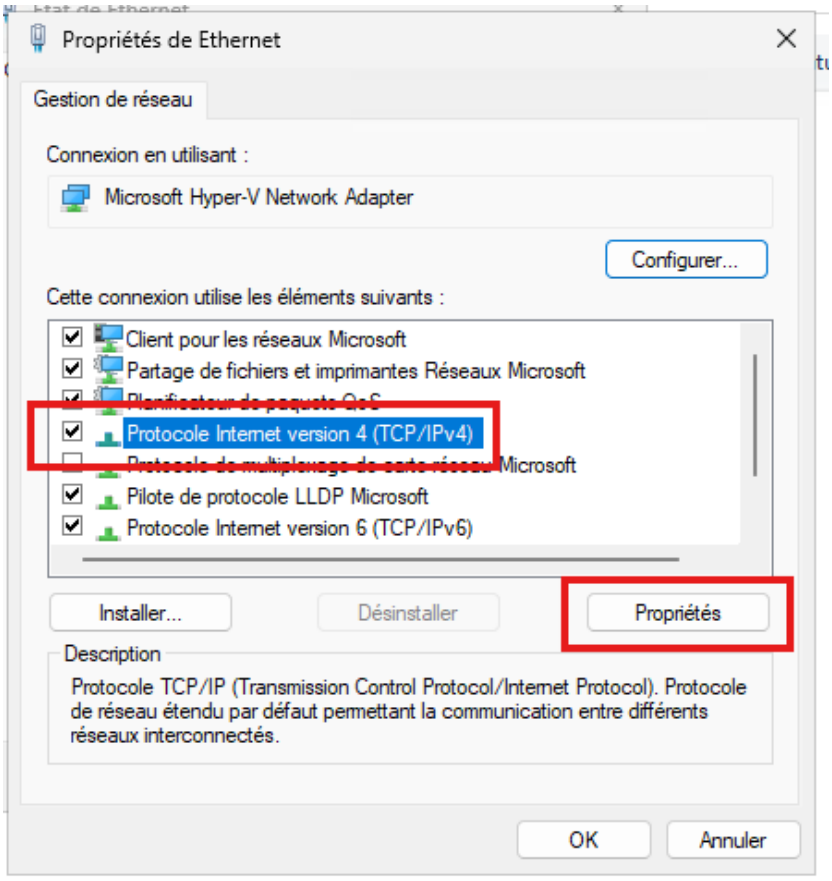
Pour modifier les paramètres IP, il suffit d'aller dans l'explorateur de fichier, de faire clic droit que réseau, propriétés, modifier les paramètres de la carte, ensuite il faut sélectionner la carte Hyper V, propriétés, puis enfin, Protocole Internet version 4 (TCP/IPv4) :


WinSrv2025 sur TEST - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Corbeille
Microsoft Edge
Accueil
Rechercher dans : Accueil
Nouveau
Trier
Afficher
Filtrer
Détails
Galerie
Accès rapide
Développer
Ouvrir dans un nouvel onglet
Ouvrir dans une nouvelle fenêtre
Connecter un lecteur réseau...
Déconnecter un lecteur réseau...
Épingler à l'accès rapide
Épingler au menu Démarrer
Propriétés
Alt+Entrée
Afficher d'autres d'options
Supprimer
Réseau
Partagé
Téléchargements
Stocké localement
Documents
Stocké localement
Musique
Stocké localement
Vidéos
Stocké localement
Votre activité récente s'affichera ici
Vous obtiendrez un accès rapide aux fichiers que vous avez
6 élément(s)
Windows Server 2025 Standard Evaluation
Licence Windows valide pour 159 jours
Build 26100.ge_release.240331-1435
Rechercher
13:55
07/11/2025
État : Exécution

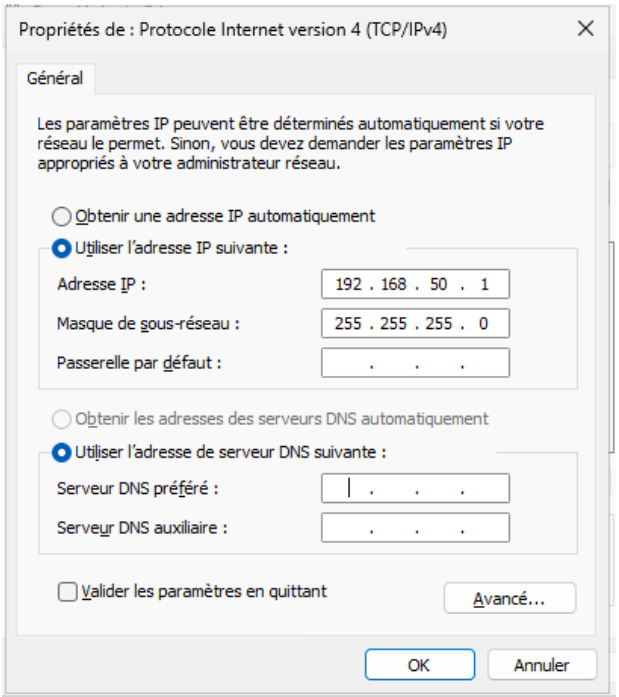

Centre Réseau et partage
Panneau de configuration › Réseau et Internet › Centre Réseau et partage
Rechercher
Page d'accueil du panneau de configuration
Modifier les paramètres de la carte
Modifier les paramètres de partage avancés
Afficher les informations de base de votre réseau et configurer des connexions
Afficher vos réseaux actifs
Réseau non identifié
Réseau public
Type d'accès : Pas d'accès réseau
Connexions : Ethernet
Modifier vos paramètres réseau
Configurer une nouvelle connexion ou un nouveau réseau
Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.
Résoudre les problèmes
Diagnostiquez et réparez les problèmes de réseau ou accédez à des informations de dépannage.
Voir aussi
Options Internet
Pare-feu Windows Defender


Connexions réseau
Panneau de configuration › Réseau et Internet › Connexions réseau ›
Rechercher dans : Connexio...
Organiser
Ethernet
Réseau non identifié
Microsoft Hyper-V Network Adap...
1 élément

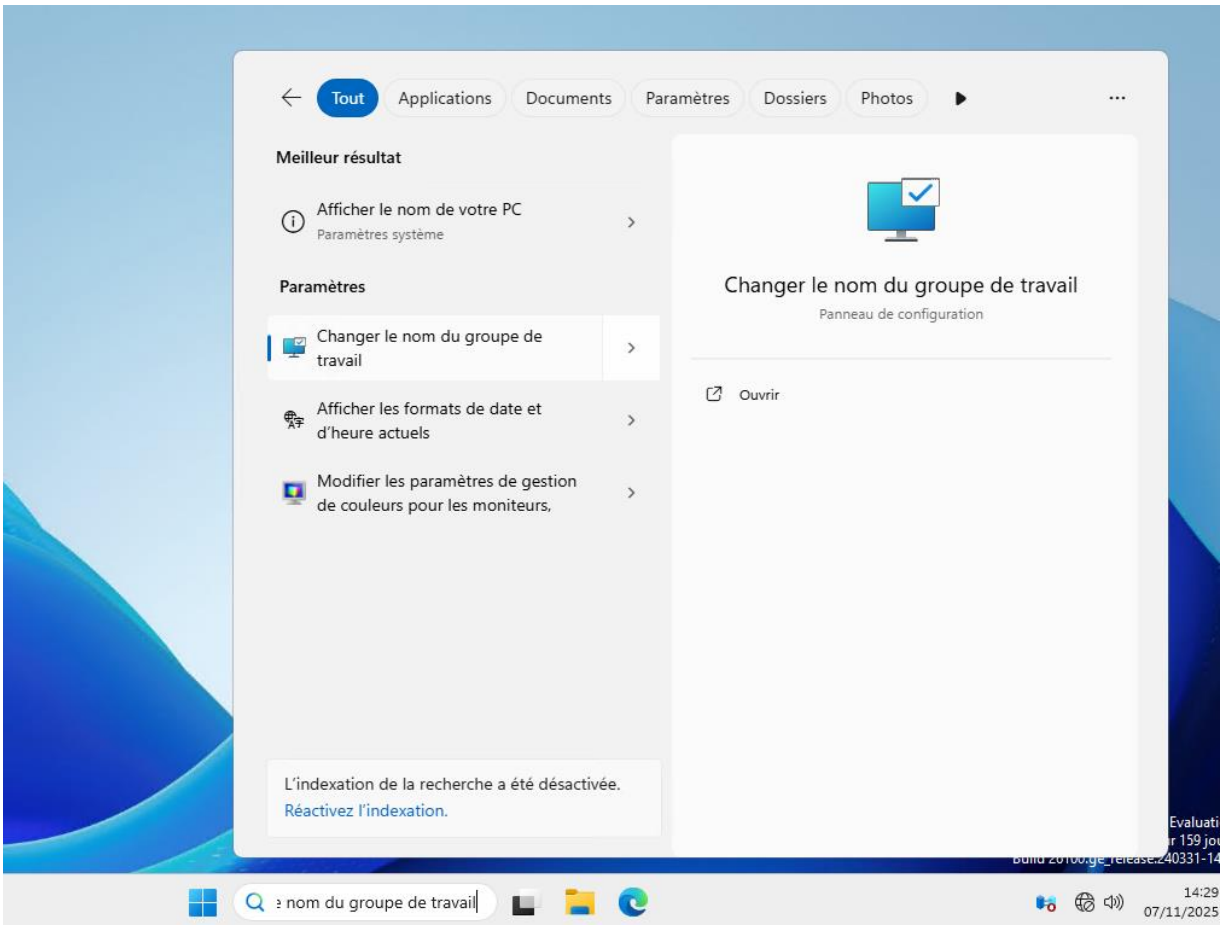

État de Ethernet
Général
Connexion
Connectivité IPv4 : Pas d'accès réseau
Connectivité IPv6 : Pas d'accès réseau
État du média : Activé
Durée : 00:11:22
Vitesse : 10,0 Gbits/s
Détails...
Activité
Envoyés
Reçus
Octets : 8 875 589 565 044 321
Propriétés
Désactiver
Diagnostiquer
Centre Réseau et partage



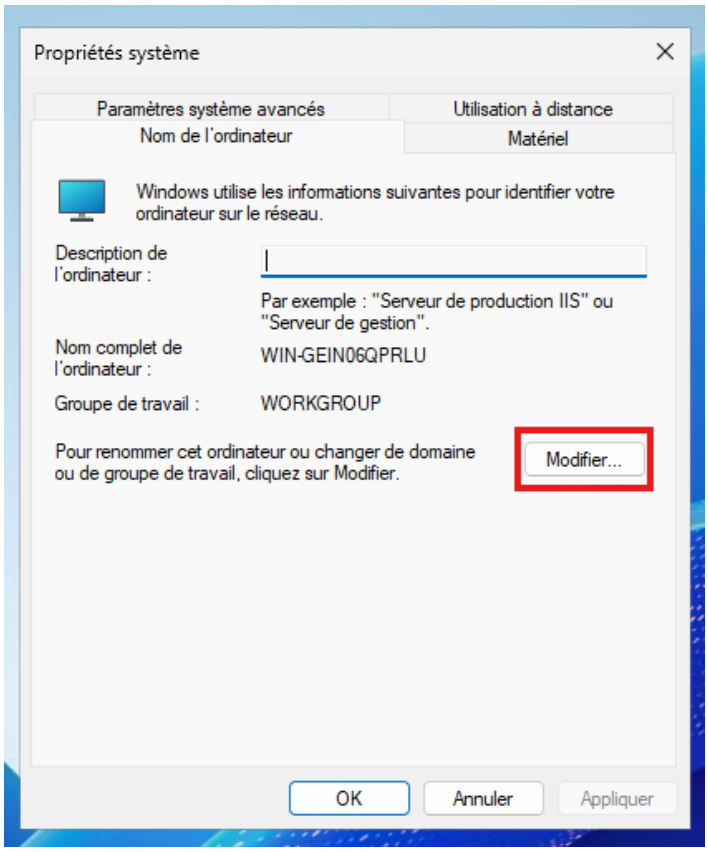
Une fois ceci fait, nous allons définir notre adresse IP manuellement avec le bon masque de sous réseau :

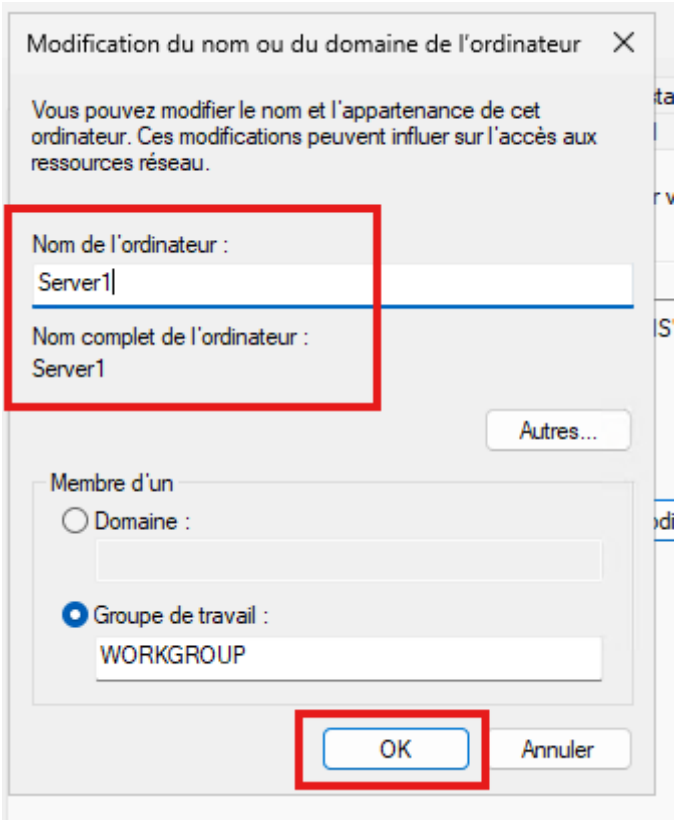


Pour modifier le nom de la machine, nous allons chercher « nom » dans la barre de recherche Windows, puis cliquer sur « changer le nom du groupe de travail » :



Une fois la fenêtre ouverte, nous allons cliquer sur modifier :

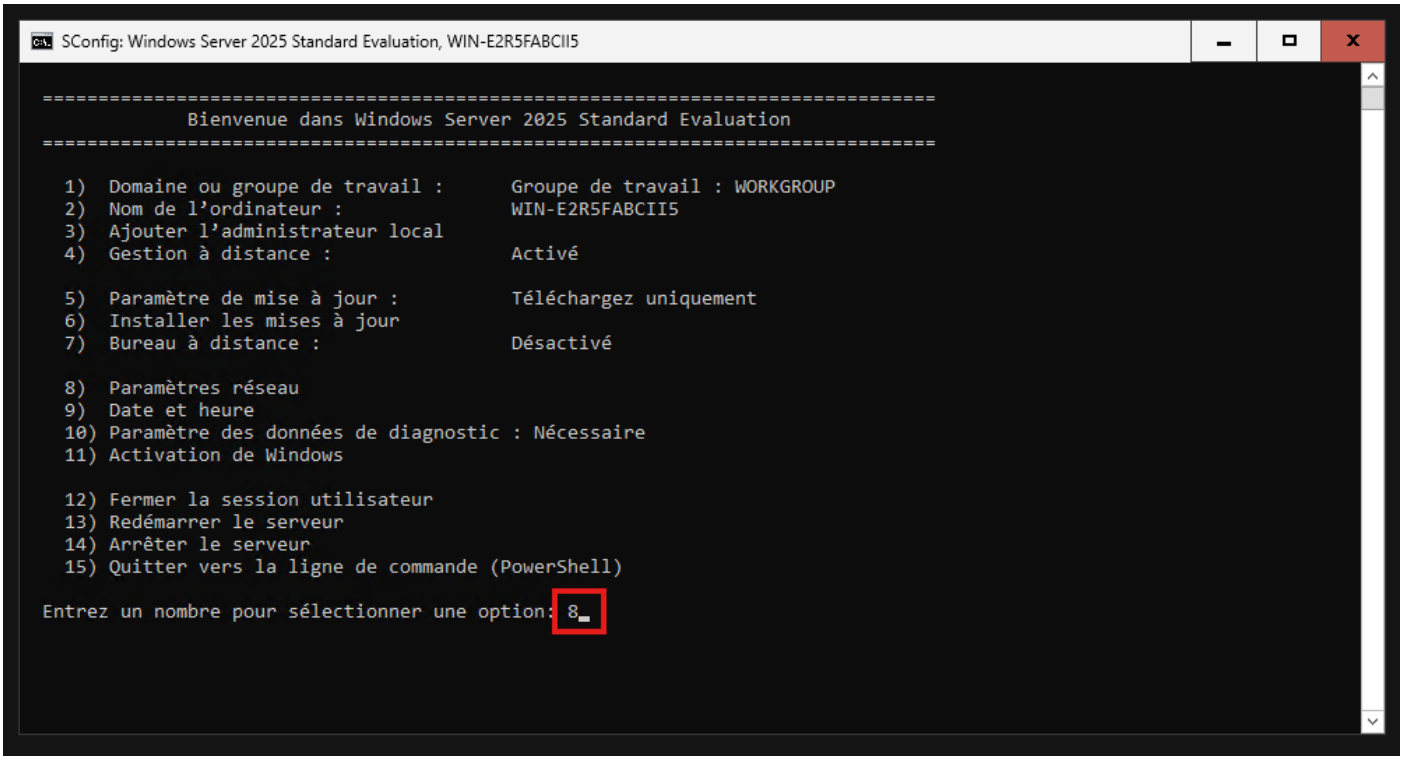

Propriétés système
Paramètres système avancés
Utilisation à distance
Nom de l'ordinateur
Matériel
Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.
Description de l'ordinateur :
Par exemple : "Serveur de production IIS" ou "Serveur de gestion".
Nom complet de l'ordinateur :
WIN-GEIN06QPRLU
Groupe de travail :
WORKGROUP
Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier.
Modifier...
OK
Annuler
Appliquer

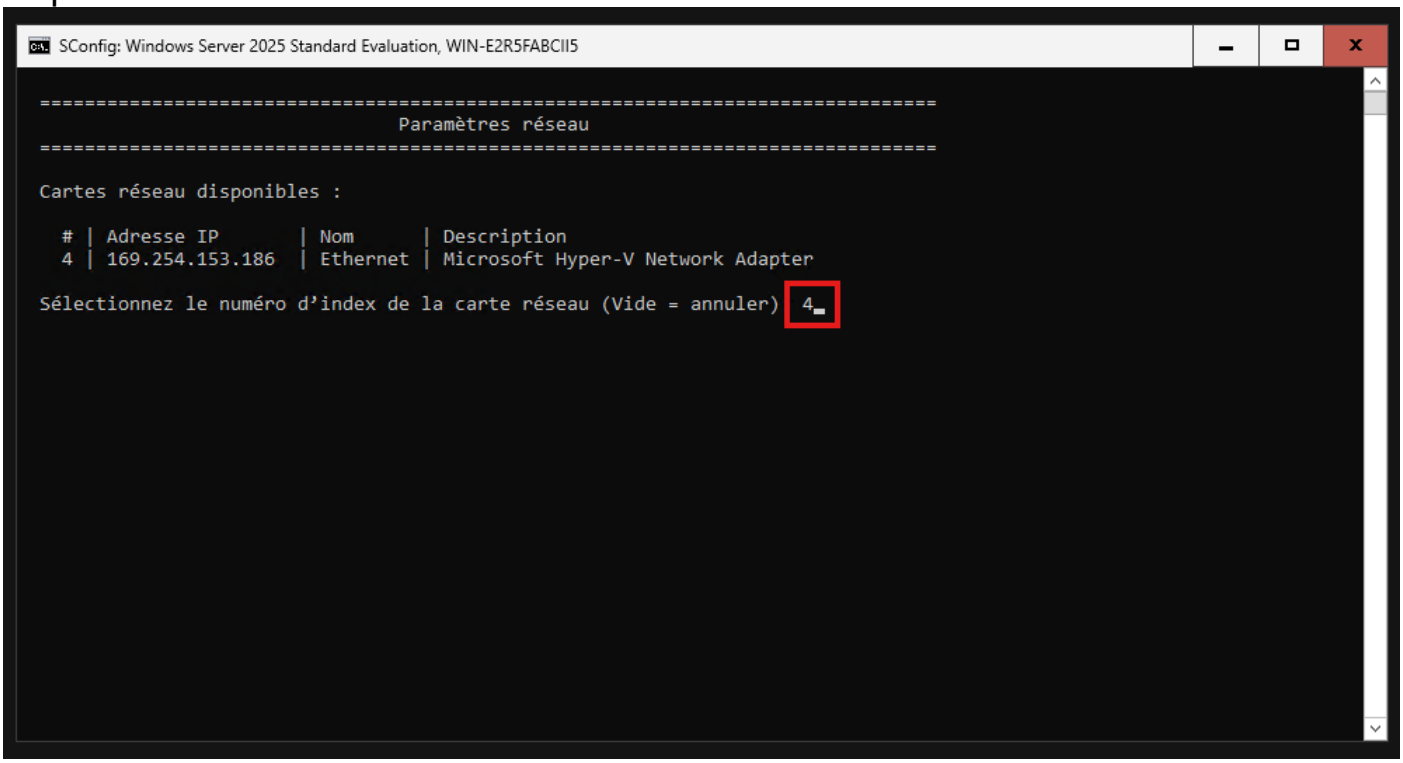

Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
Server1
Nom complet de l'ordinateur :
Server1
Autres...
Membre d'un
Domaine :
Groupe de travail :
WORKGROUP
OK
Annuler

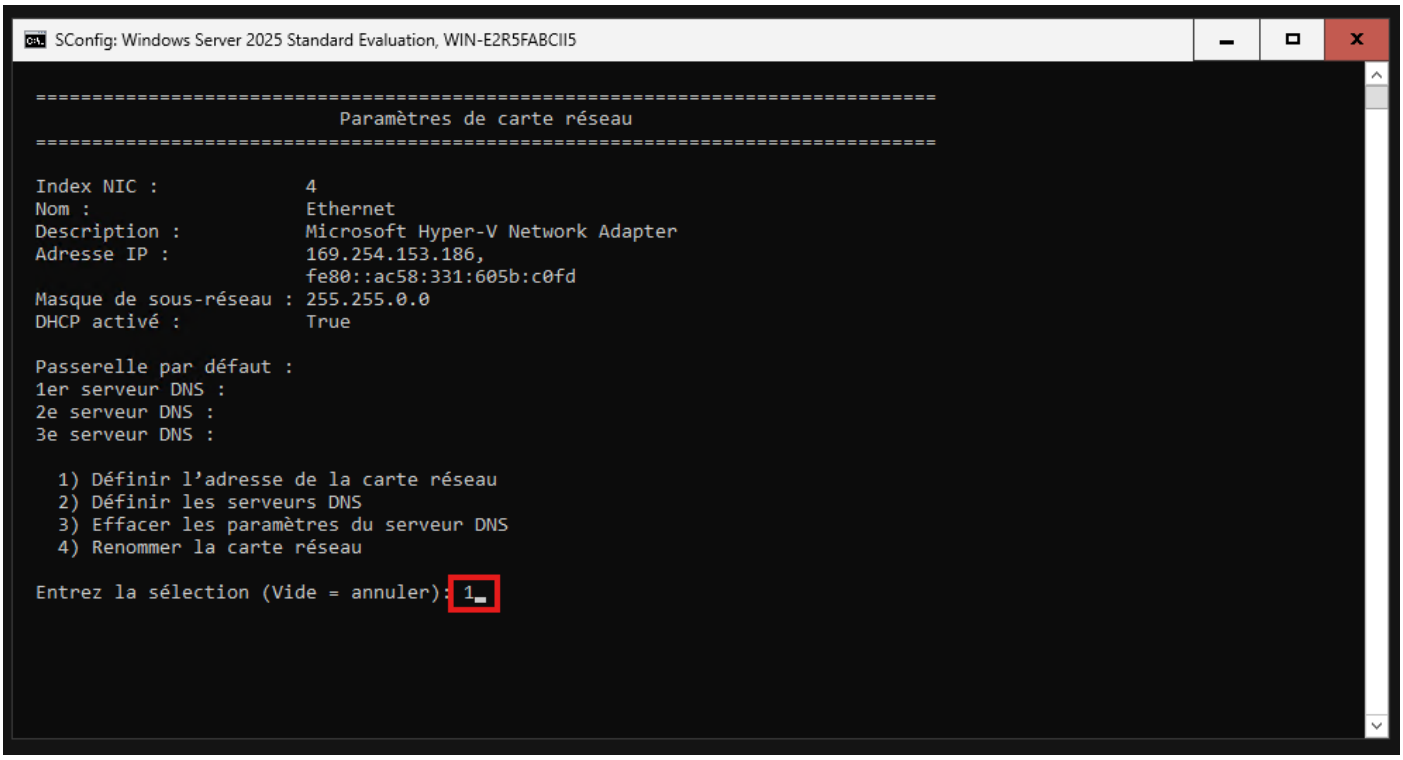
Une fois les modifications effectuées, un pop-up apparait pour redémarrer la machine, ce qui est nécessaire

(Manipulation WinSrv2025Core)

Pour configurer le réseau, il faut se rendre dans Paramètres réseau (option 8), ensuite il faut sélectionner l'interface que l'on souhaite paramétrer (en l'occurrence la 4). Puis, nous allons définir l'adresse IP (option 1) :



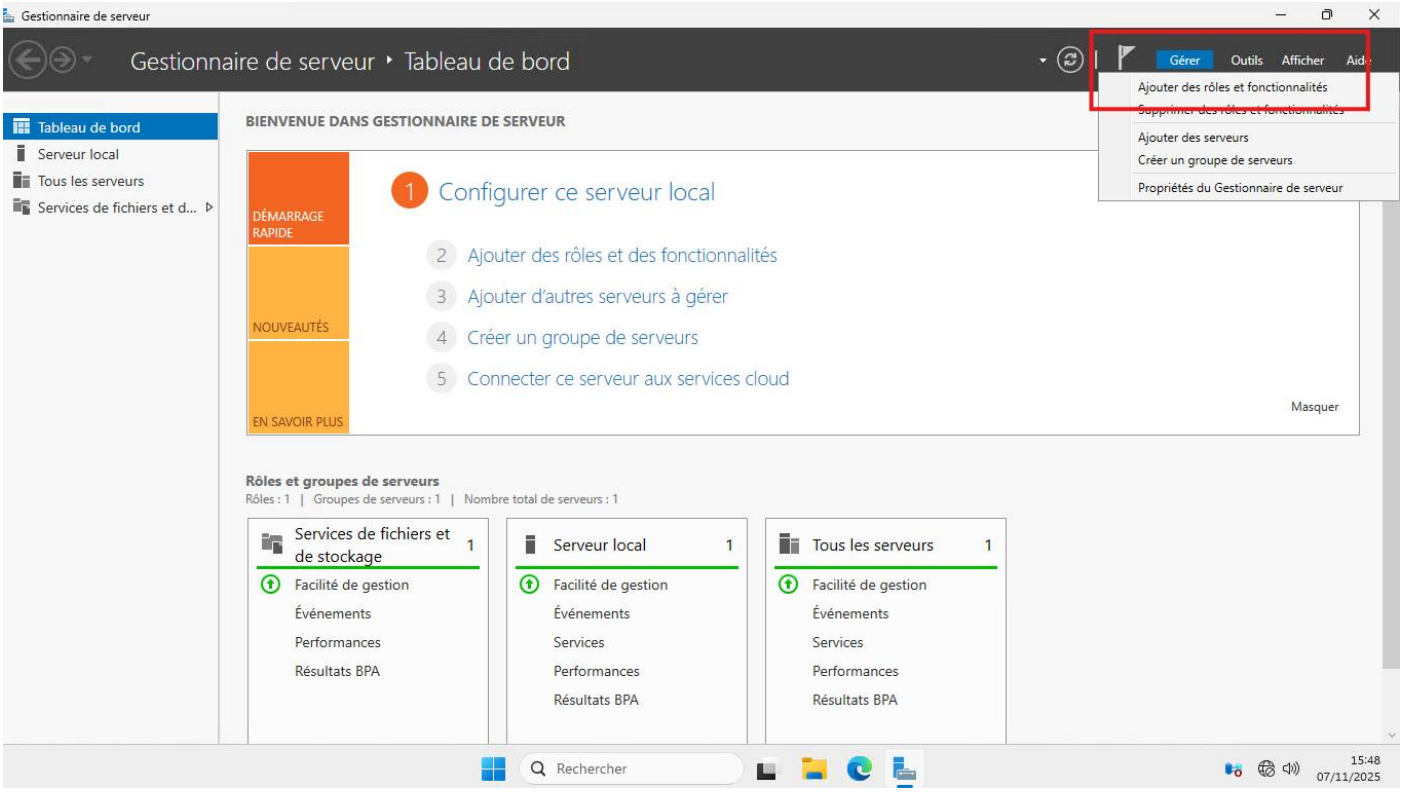




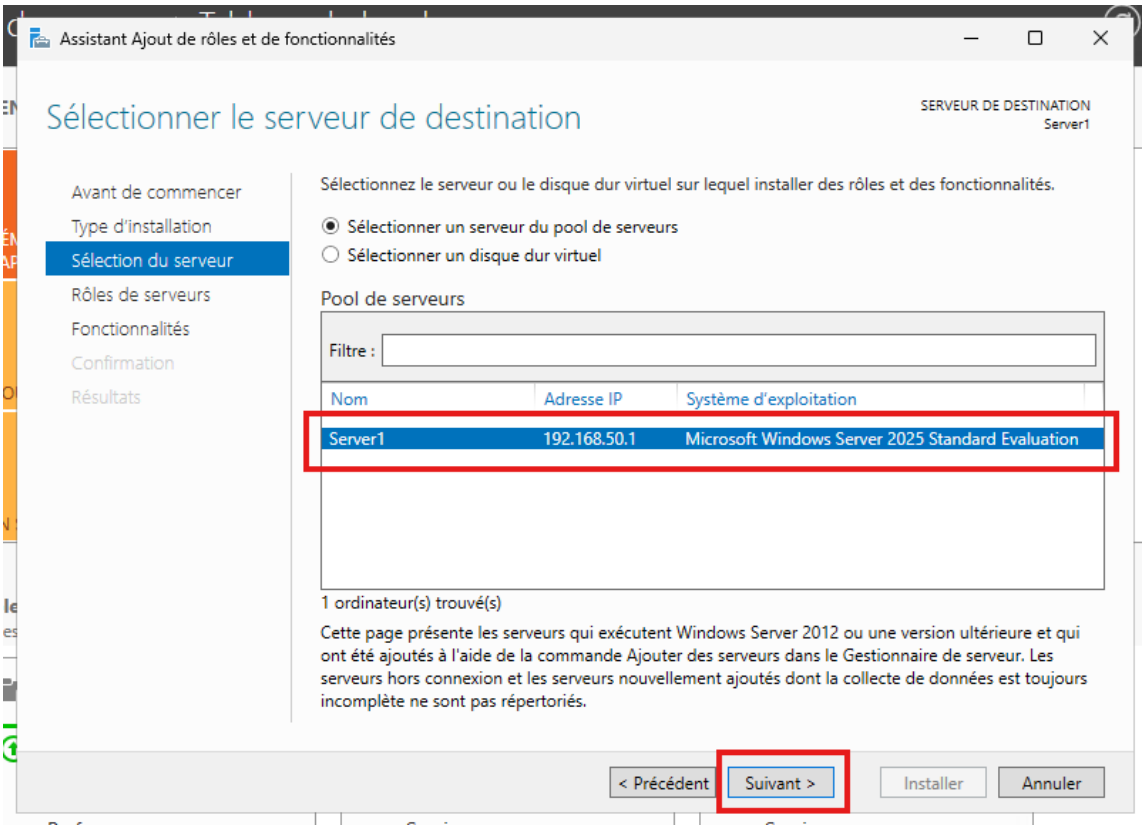
7. Mise en place du rôle Active Directory (AD)

A présent, nous allons activer le rôle Active Directory sur le serveur WinSrv2025 (version avec interface graphique). Pour cela, nous allons nous rendre dans le

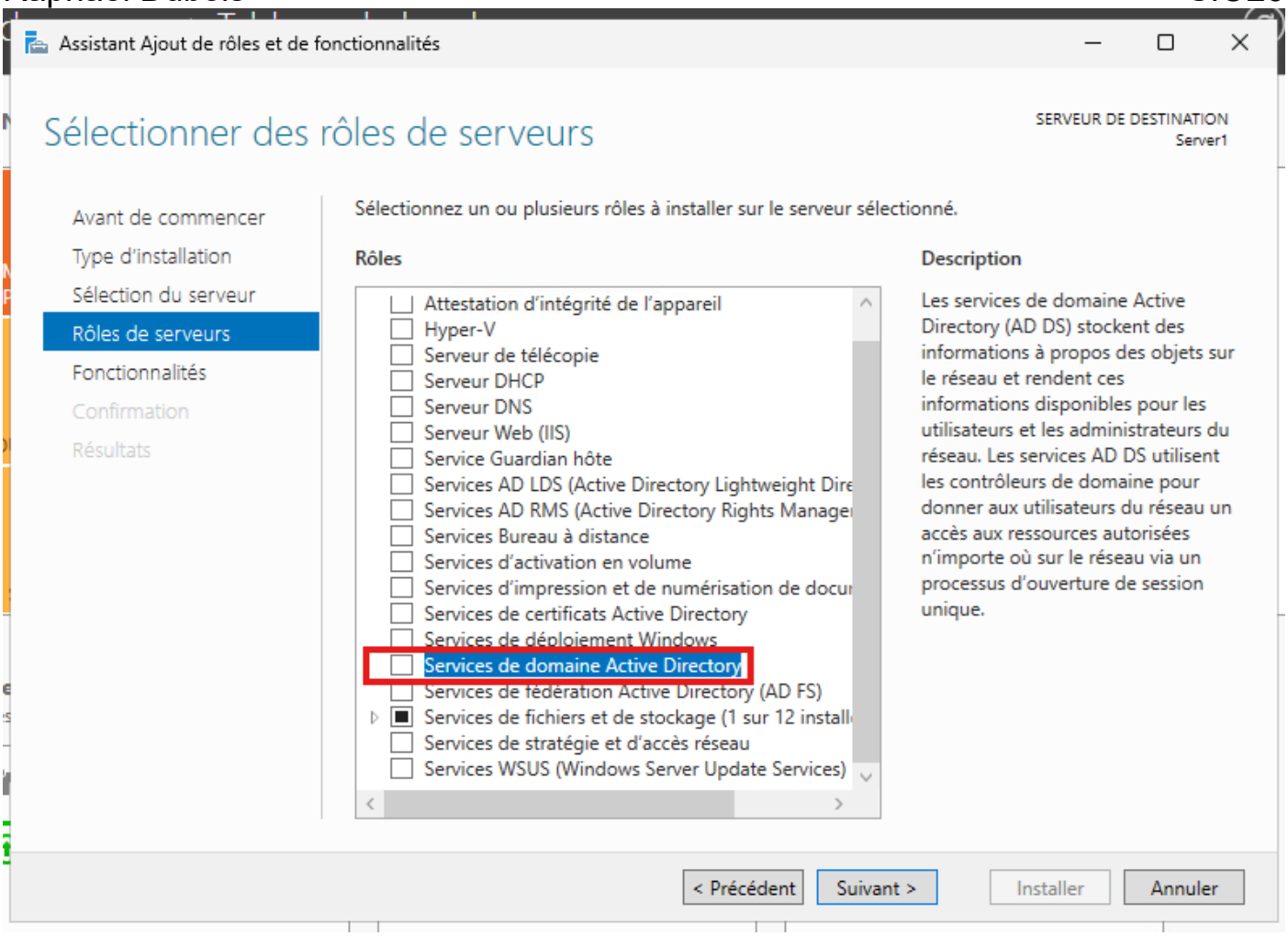
gestionnaire de serveur, puis nous allons aller dans « Gérer » puis « Ajouter des rôles et des fonctionnalités »

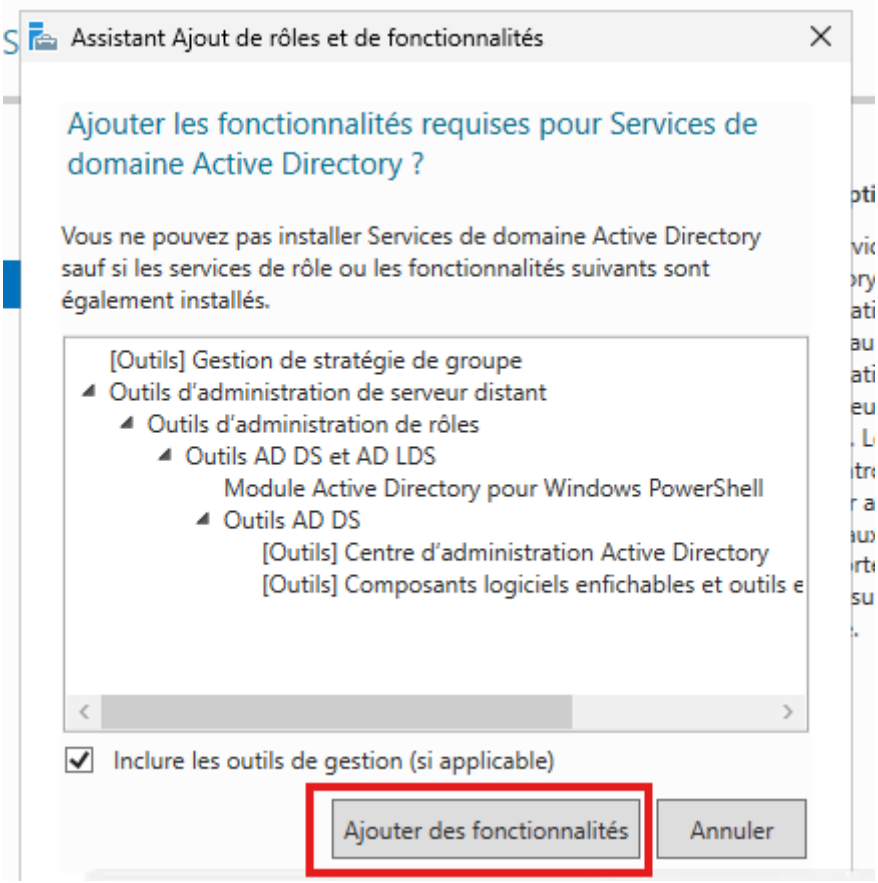


Une fois dans la configuration, nous pouvons faire suivant jusqu'à la sélection du serveur. Ici, on doit vérifier que notre serveur est bien sélectionné :

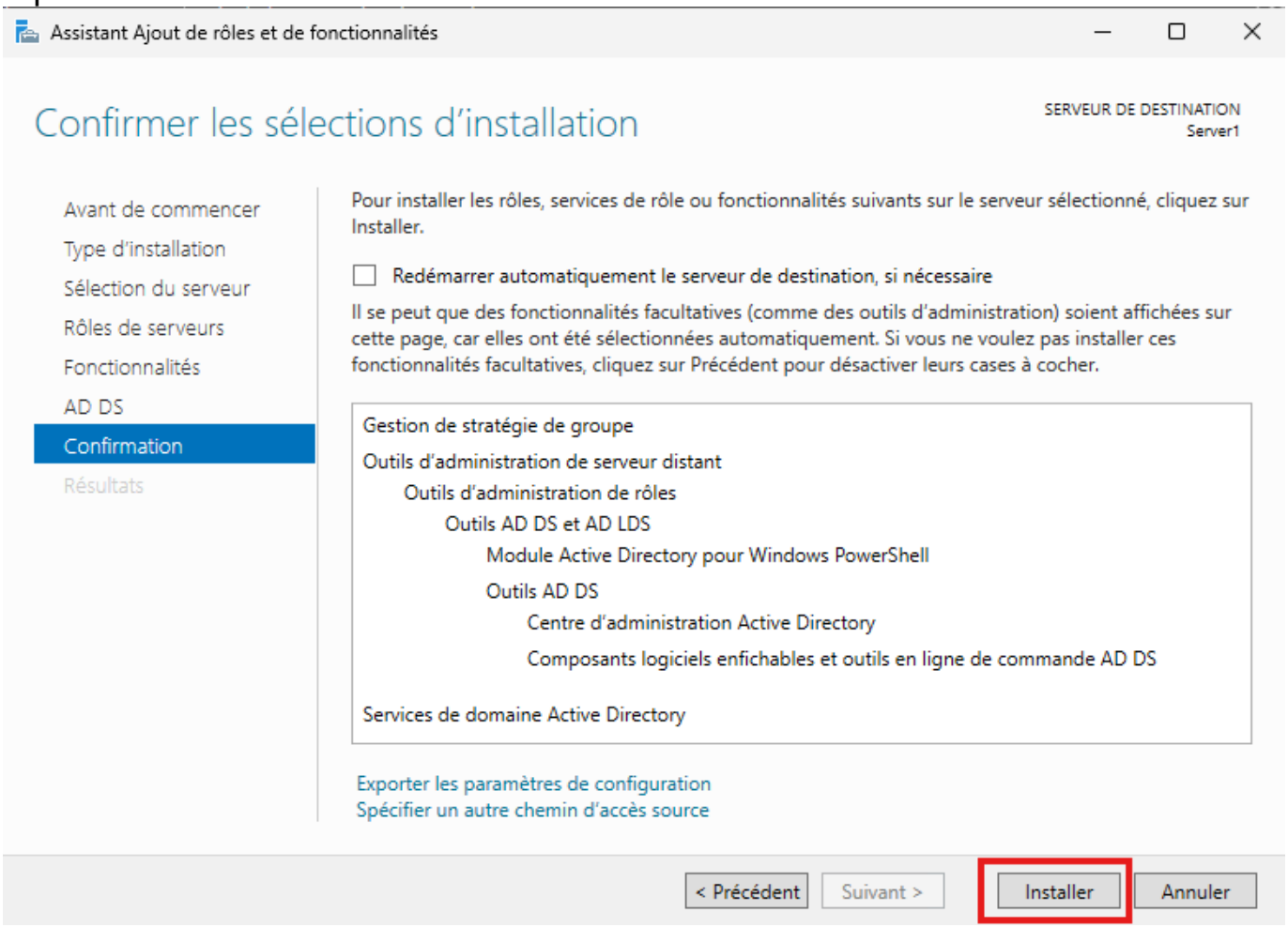


Ensuite, nous avons la liste des différentes fonctionnalités à installer, nous allons sélectionner « Services de domaine Active Directory » :

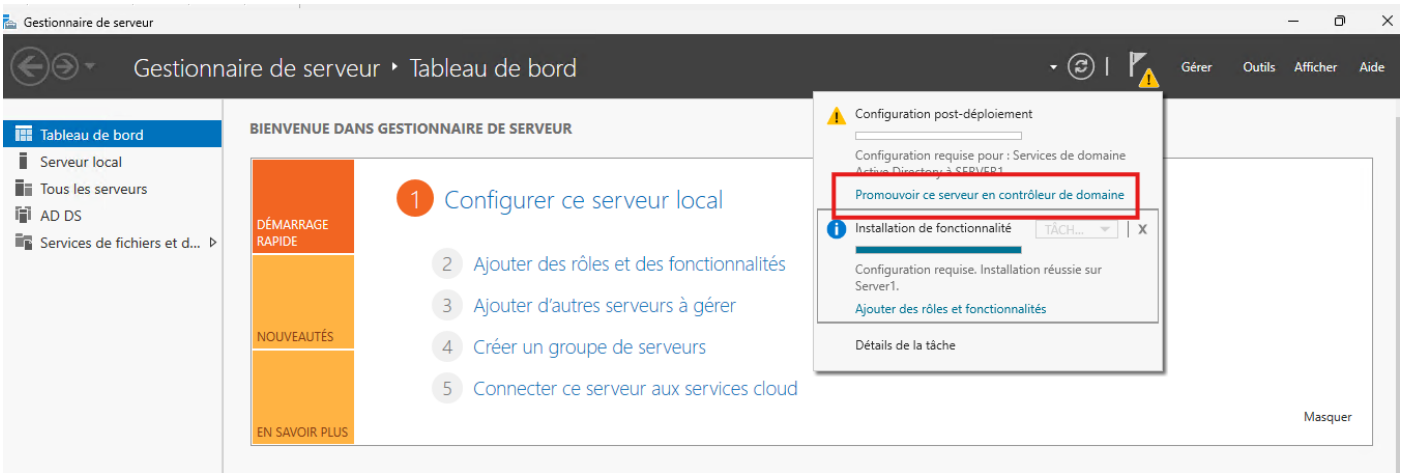

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
Server1
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Description
Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
< Précédent
Suivant >
Installer
Annuler



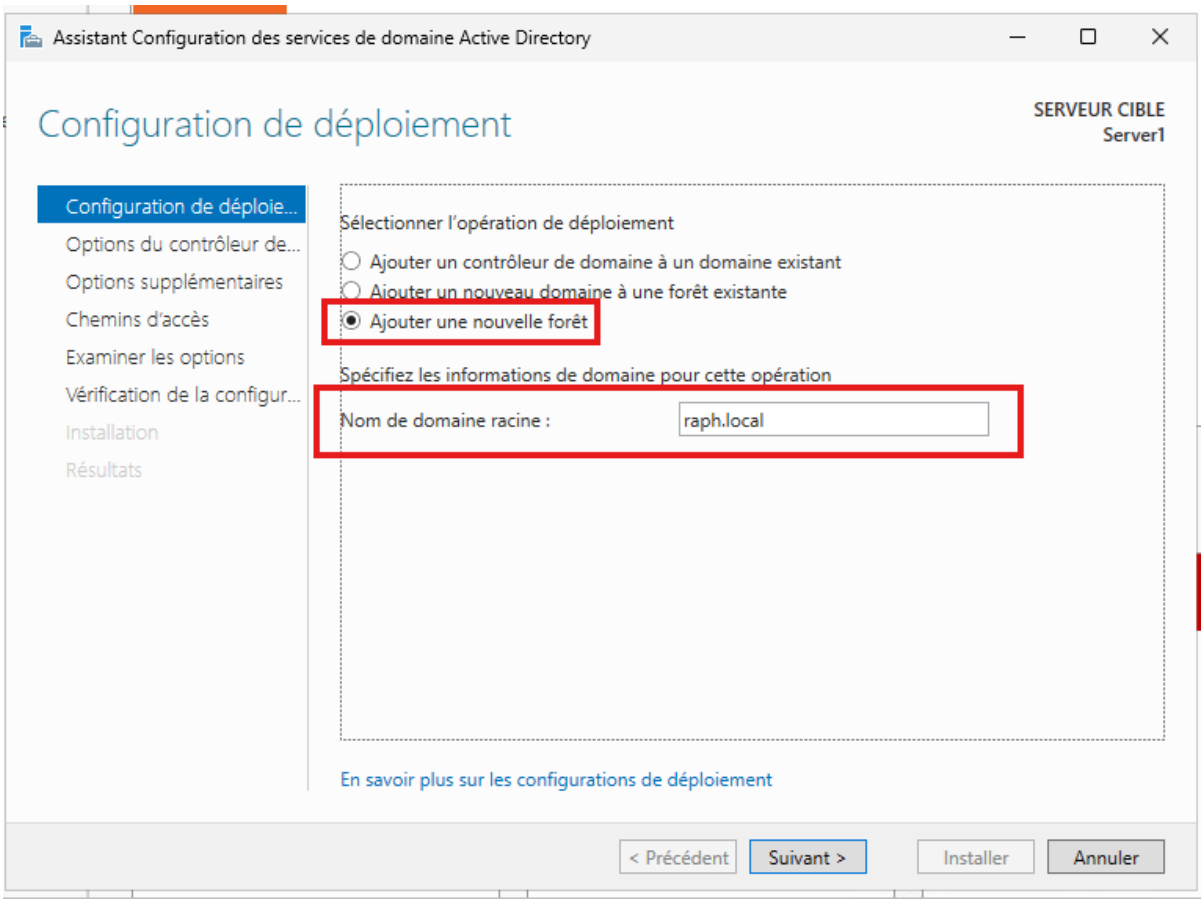
Une fois ceci coché, nous pouvons faire suivant, sélectionner aucune fonctionnalité et continuer à faire suivant jusqu'à tomber sur la page de confirmation :



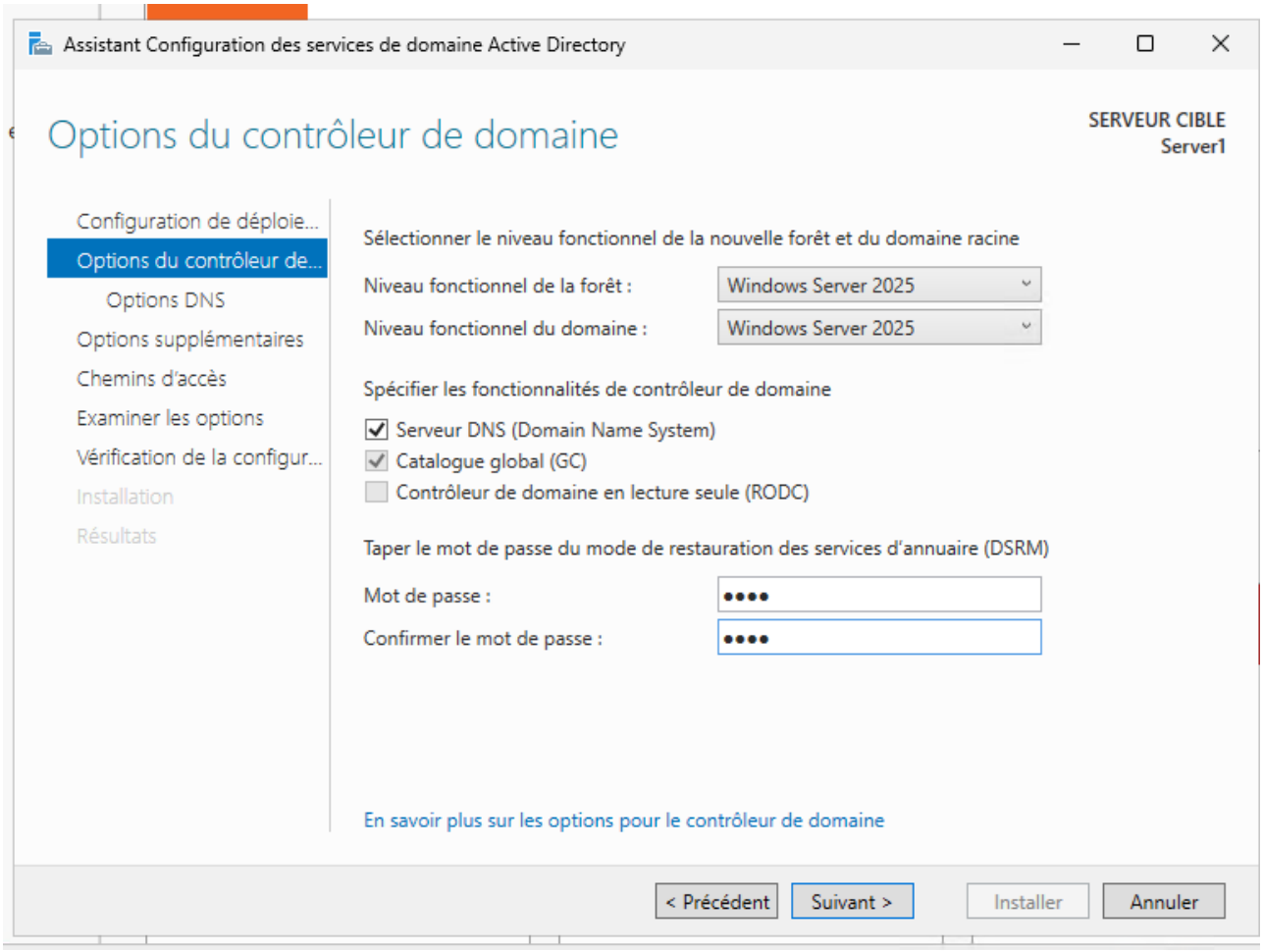
Une fois l'installation terminée, nous devons configurer le service, pour cela, il faut cliquer sur l'icône avec le drapeau, puis « Promouvoir ce serveur en contrôleur de domaine » :



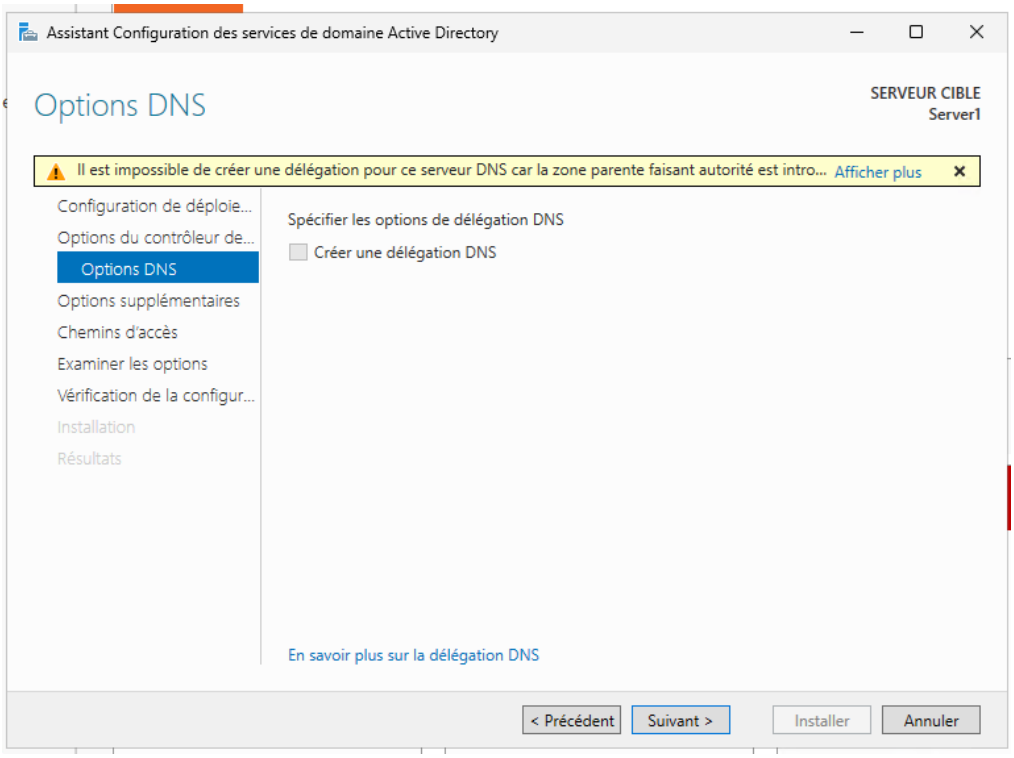
Dans la configuration, nous allons créer une nouvelle forêt avec le nom de domaine : raph.local



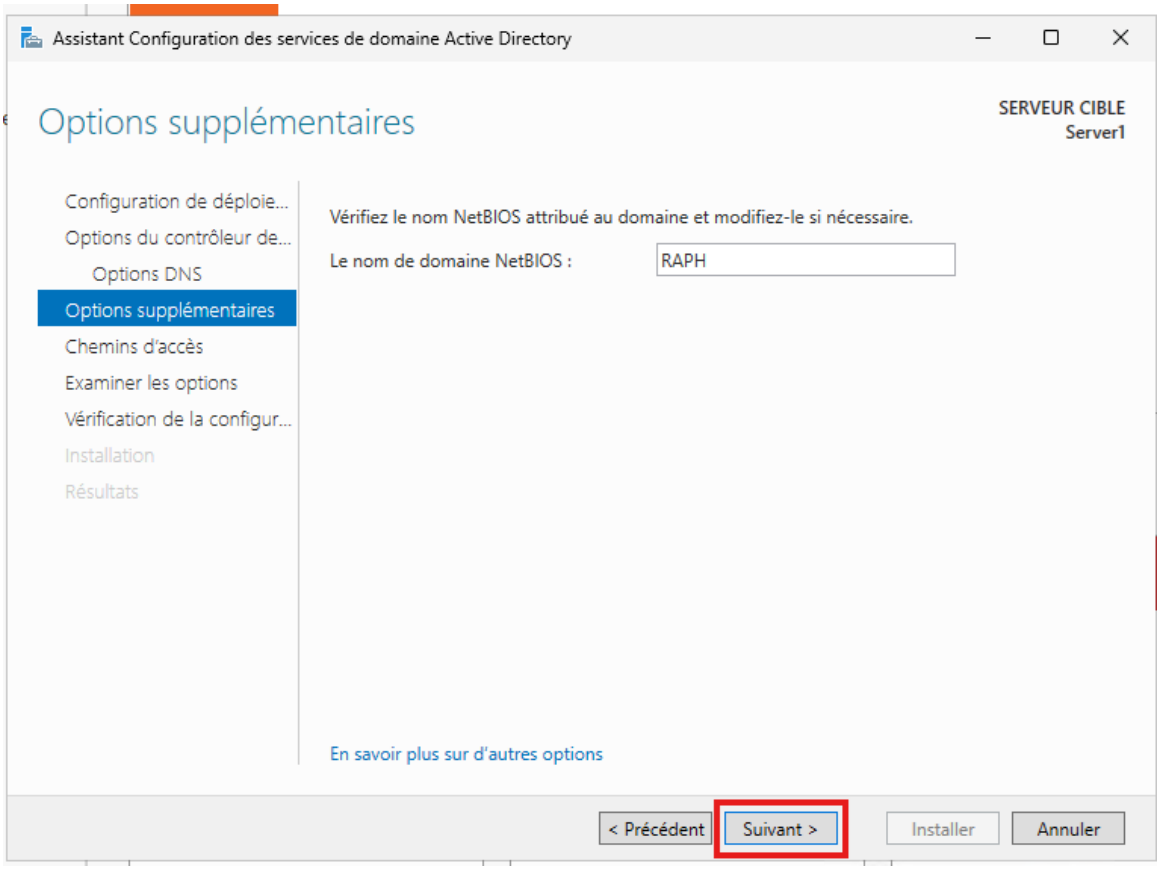
Ensuite, nous allons définir un mot de passe de restauration des services d'annuaires (DSRM) :



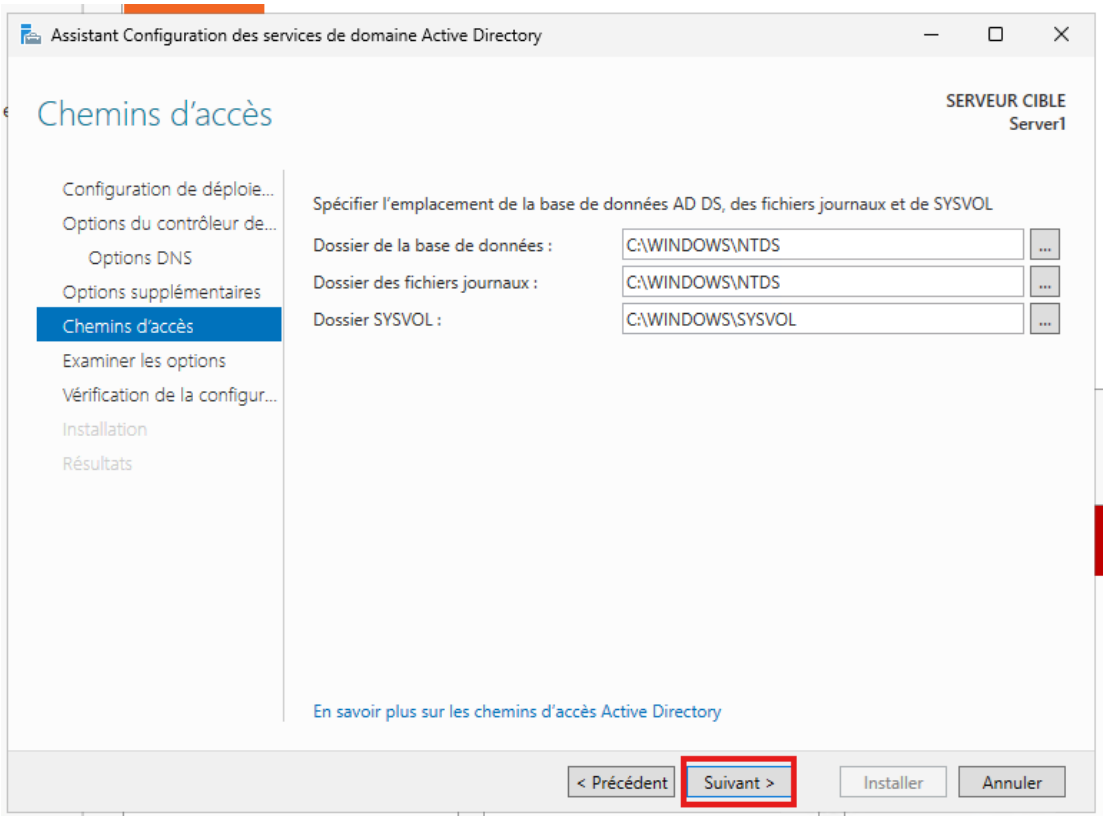
Ensuite, l'option « créer une délégation DNS » ne dois pas être coché :



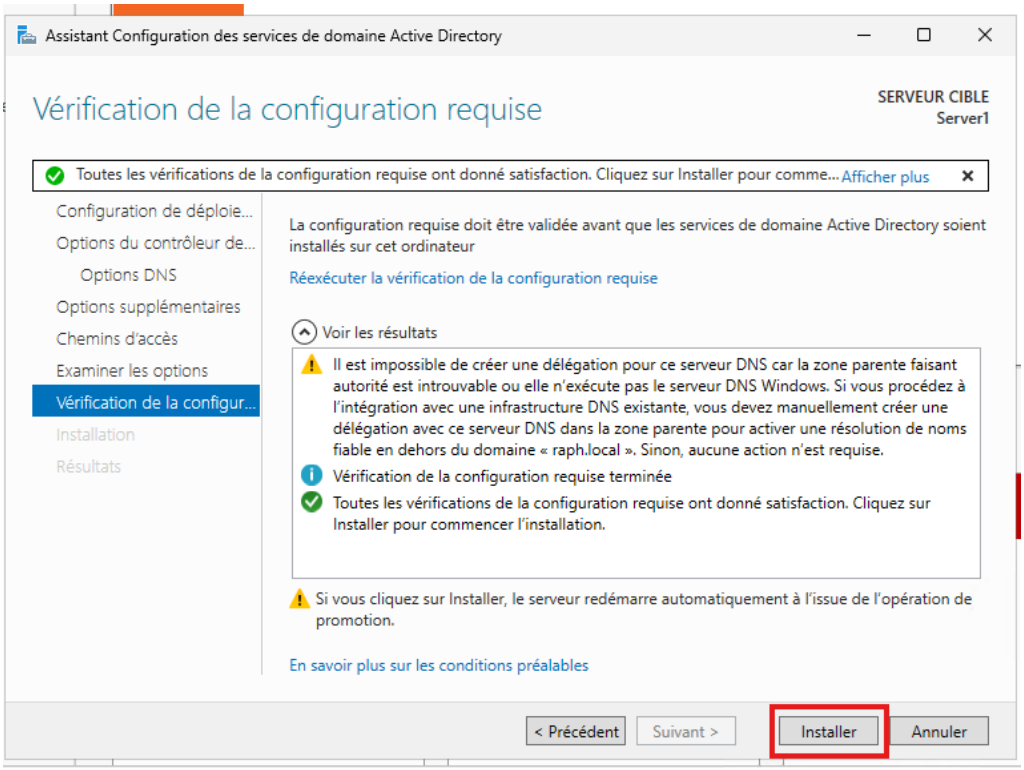
Le nom NETBIOS ne doit pas être modifié et doit être laissé par défaut :



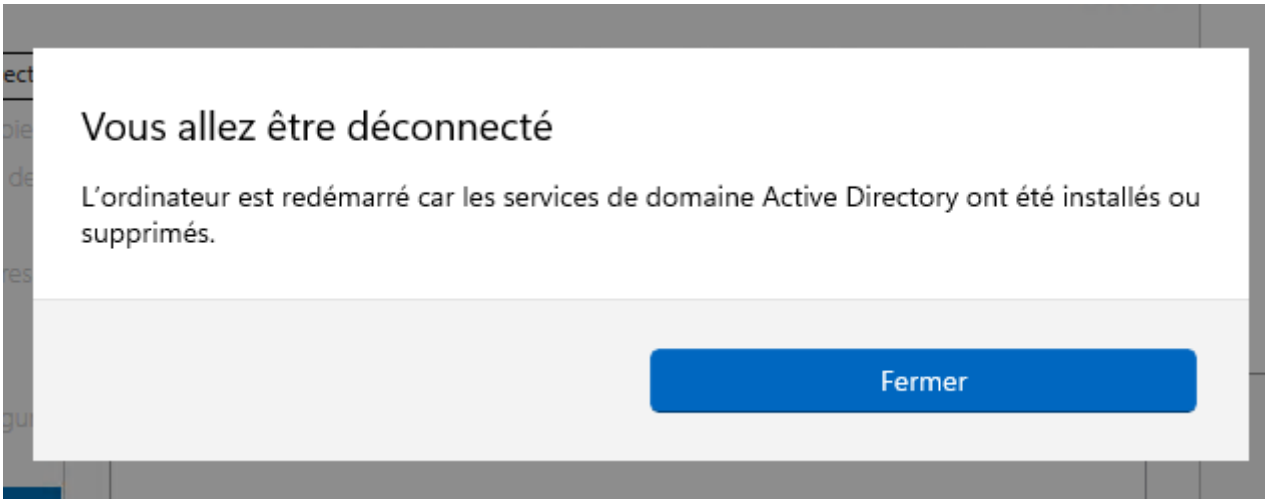
Les chemins d'accès (base de données, logs, sysvol) peuvent être laissé par défaut :

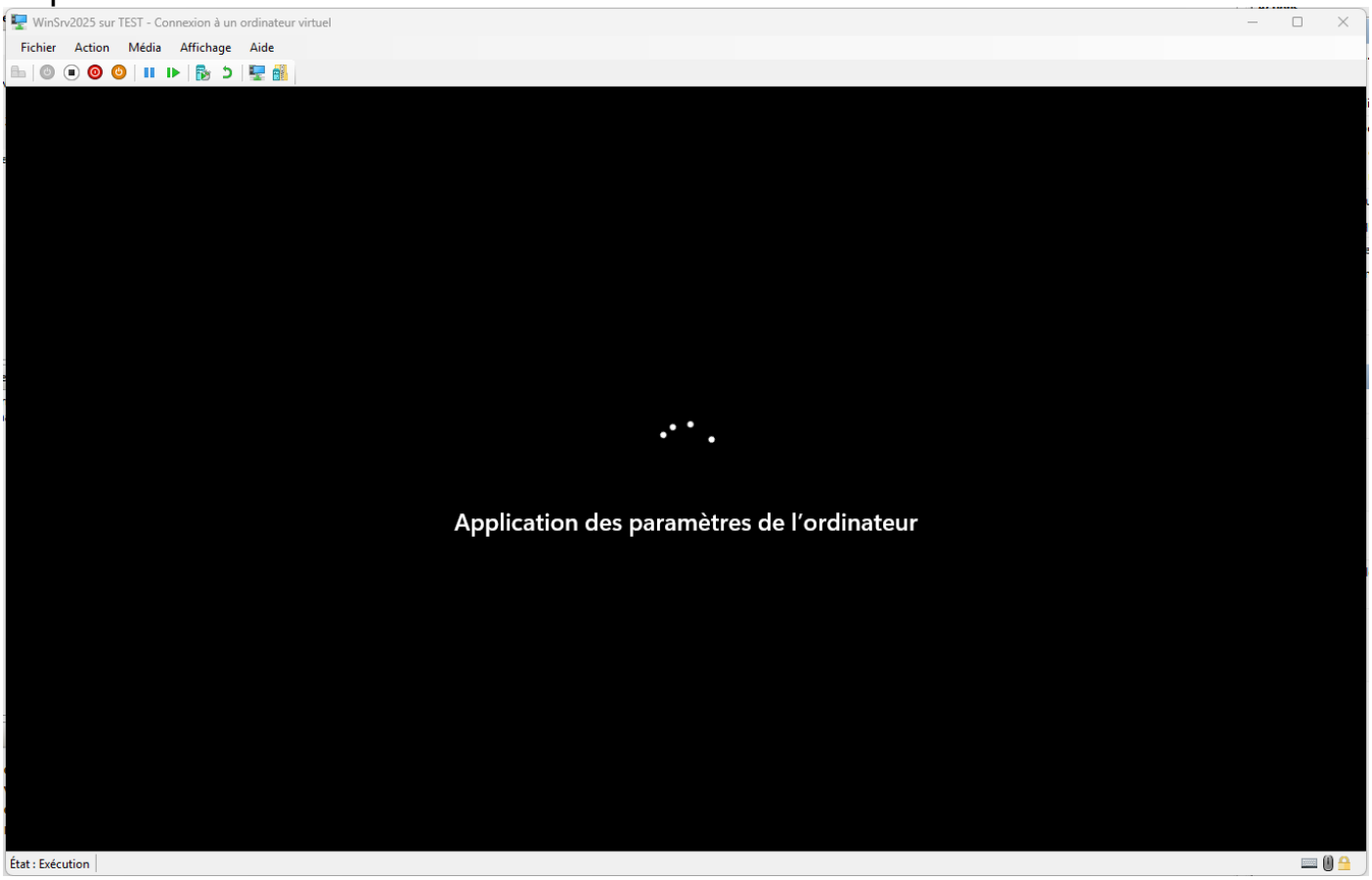


Une fois tout ceci fait, nous avons juste à confirmer les informations, faire suivant, puis installer :



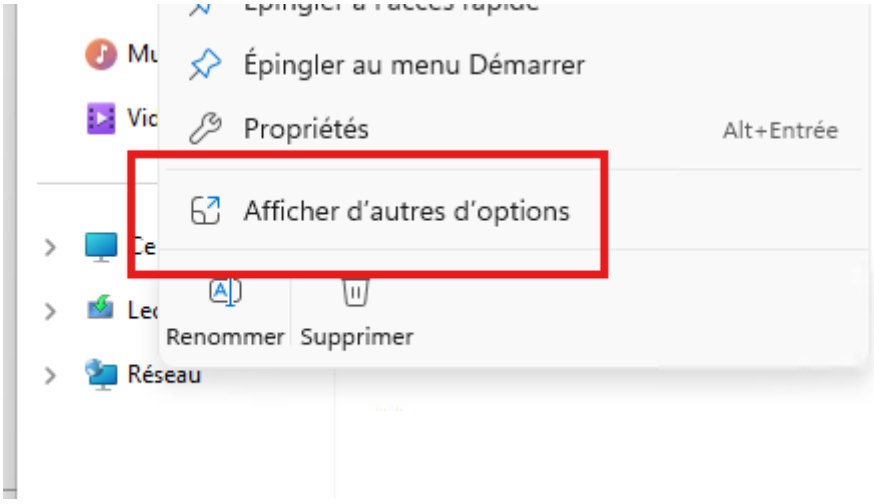
Une fois la configuration terminée, le serveur va redémarrer et ce configurer pour installer le service AD :

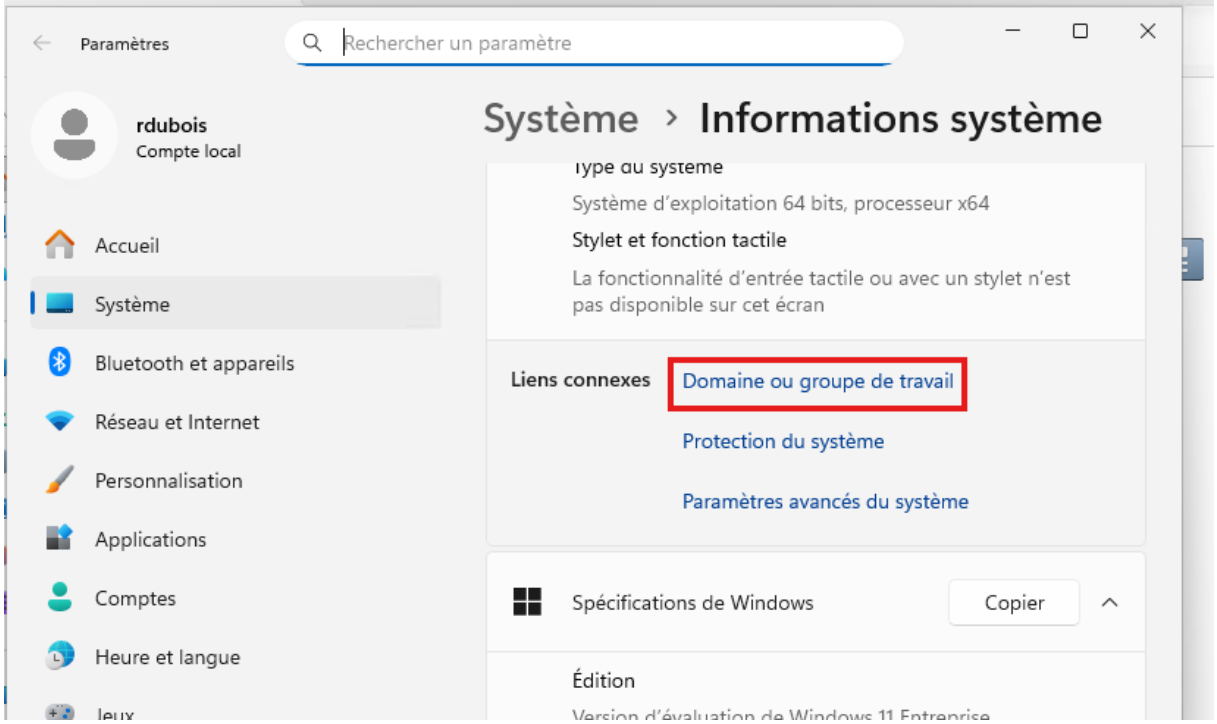


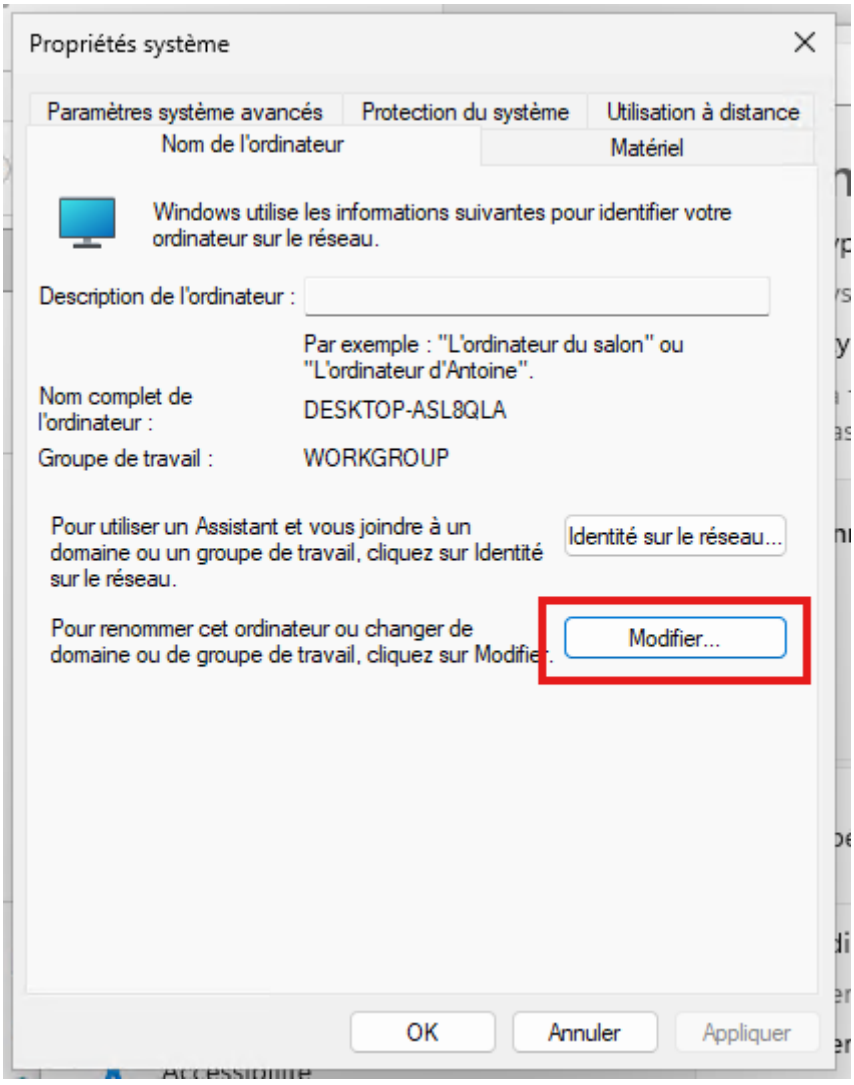


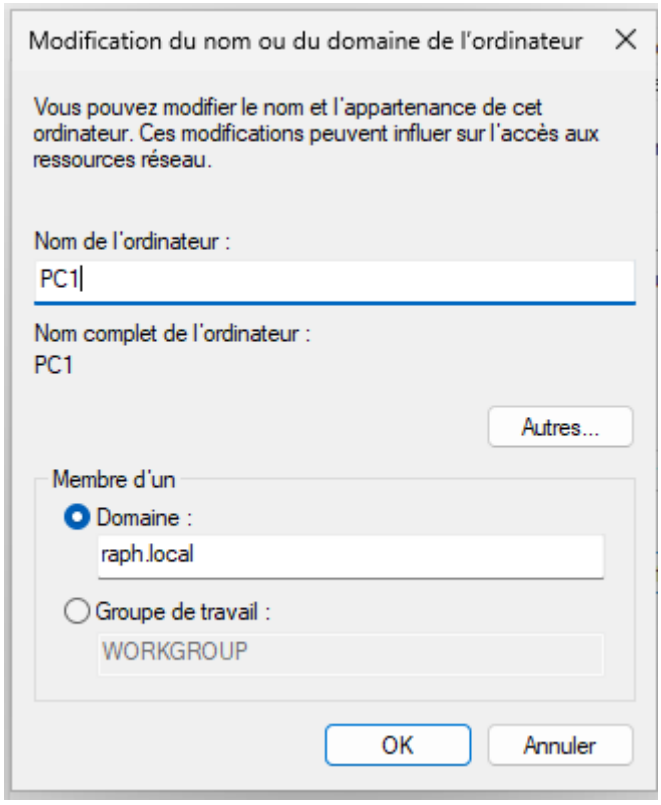
8. Intégration du poste client dans l'AD

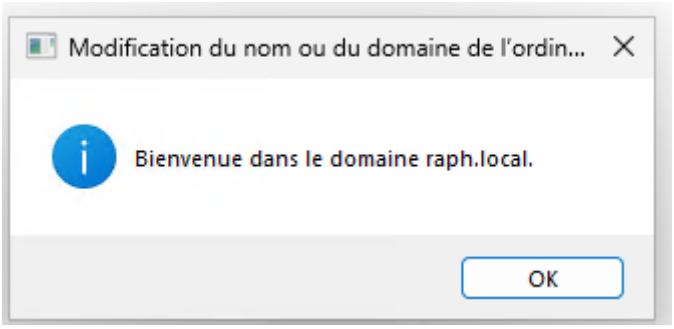
Pour intégrer notre poste Windows 11 Dans Active Directory, nous allons aller dans l'explorateur de fichier, puis clic droit sur « Ce PC » puis « Domaine ou groupe de travail », puis « Modifier » :



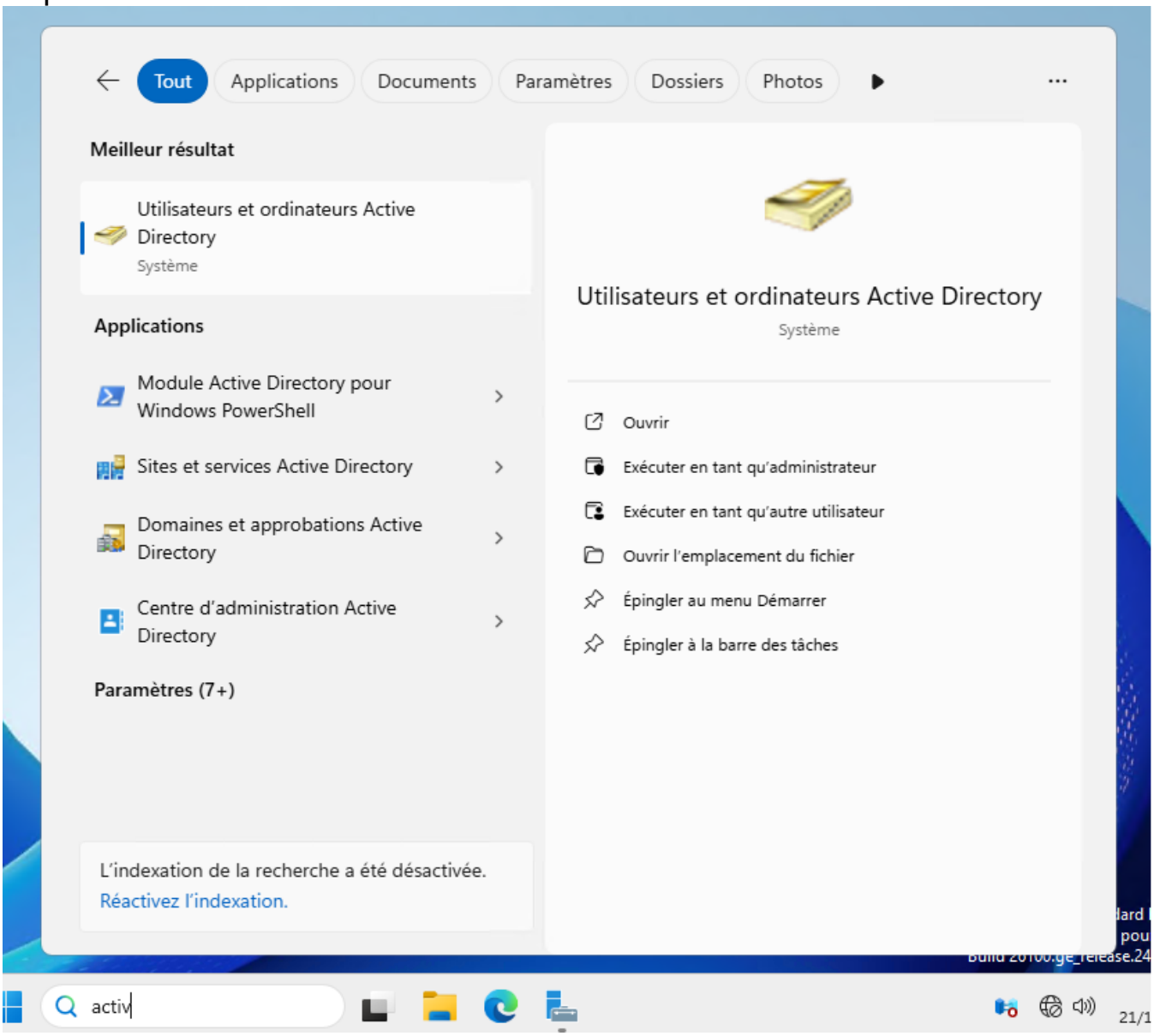

Paramètres
Rechercher un paramètre
rdubois
Compte local
Accueil
Système
Bluetooth et appareils
Réseau et Internet
Personnalisation
Applications
Comptes
Heure et langue
Jeux
Système › Informations système
Type du système
Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile
La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran
Liens connexes
Domaine ou groupe de travail
Protection du système
Paramètres avancés du système
Spécifications de Windows
Copier
Édition

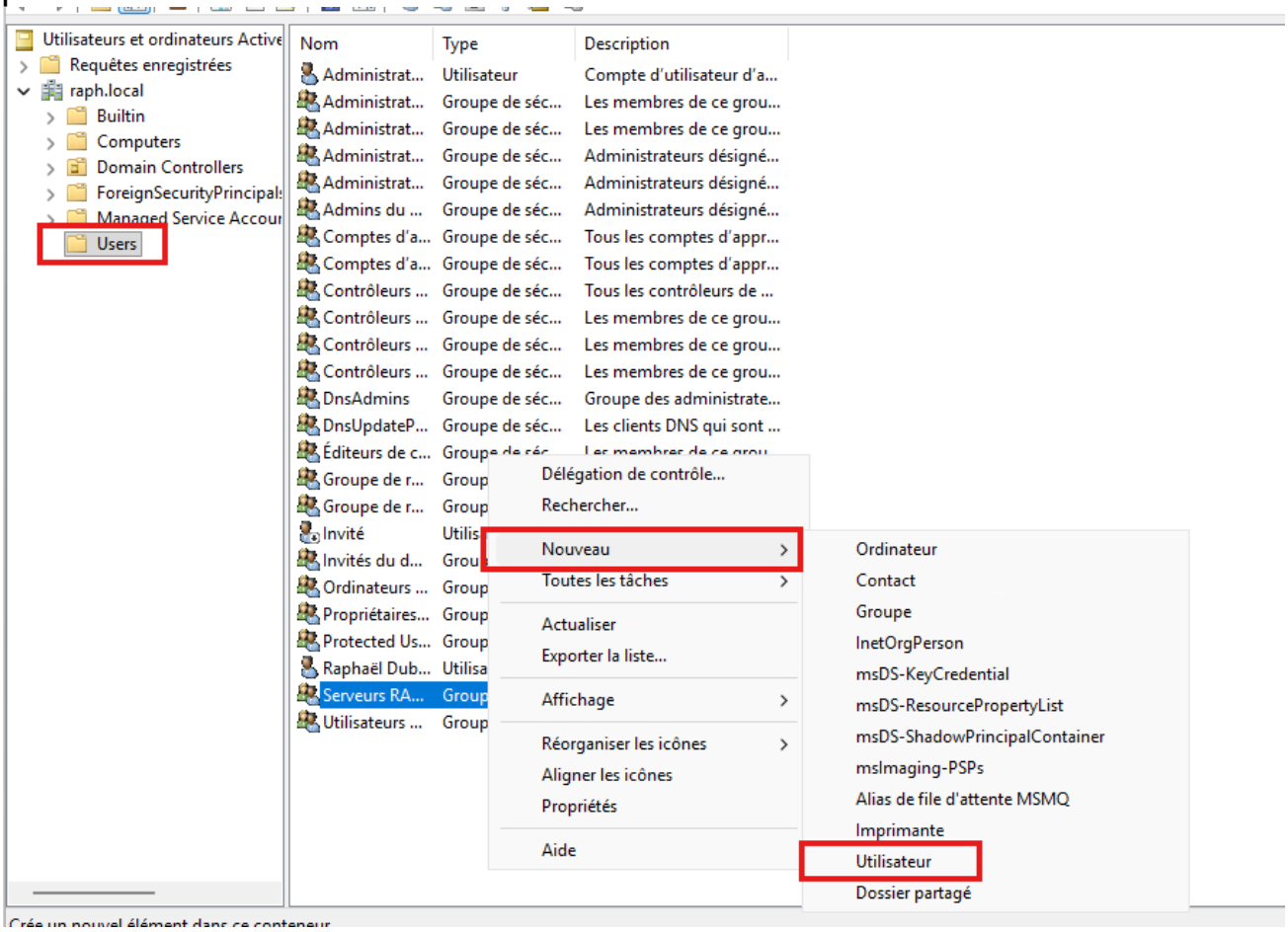

Propriétés système
Paramètres système avancés
Protection du système
Utilisation à distance
Nom de l'ordinateur
Matériel
Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.
Description de l'ordinateur :
Par exemple : "L'ordinateur du salon" ou "L'ordinateur d'Antoine".
Nom complet de l'ordinateur :
DESKTOP-ASL8QLA
Groupe de travail :
WORKGROUP
Pour utiliser un Assistant et vous joindre à un domaine ou un groupe de travail, cliquez sur Identité sur le réseau.
Identité sur le réseau...
Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier.
Modifier...
OK
Annuler
Appliquer

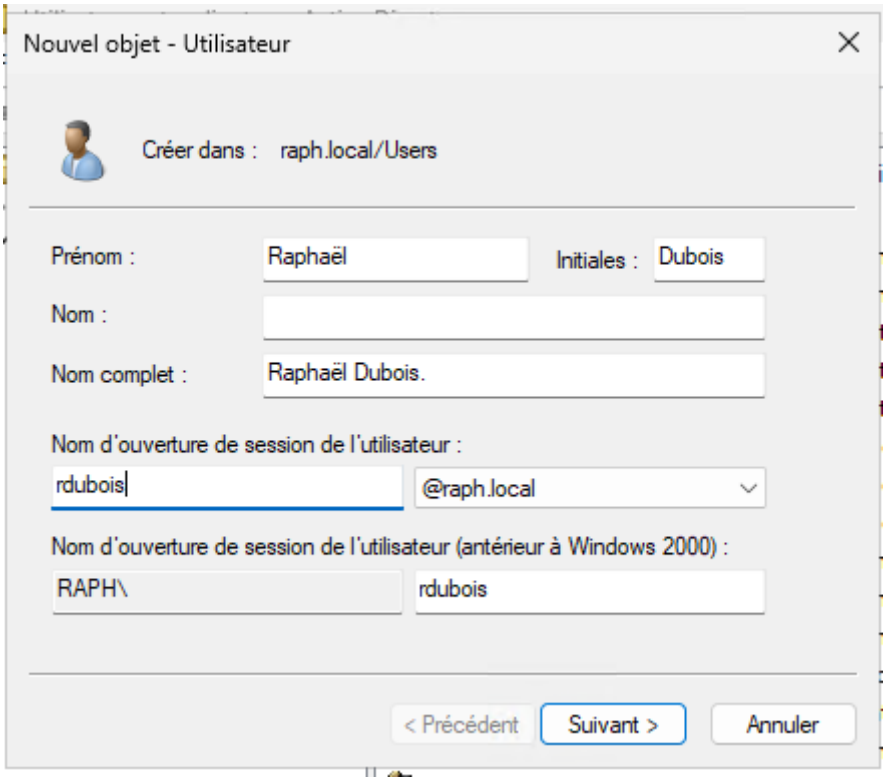




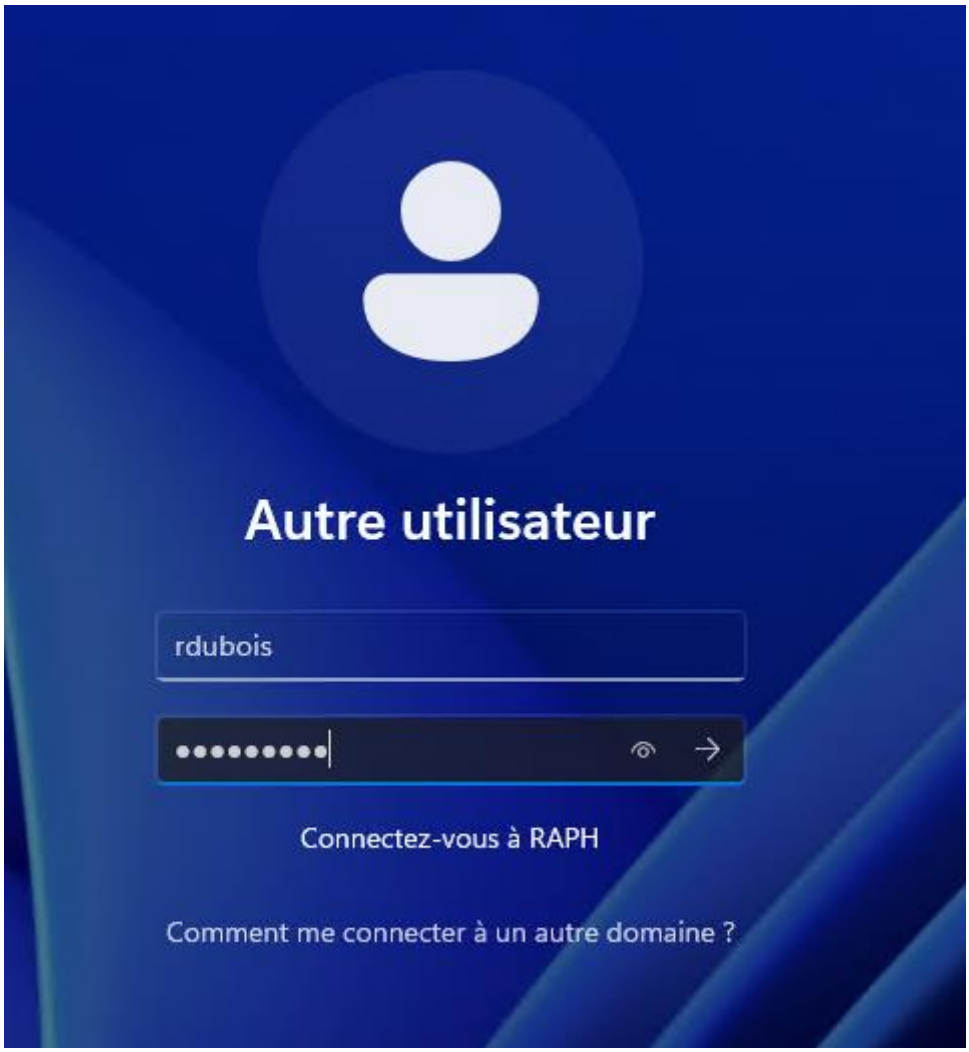
Une fois ceci fait, Windows va proposer de redémarrer le poste, après le redémarrage, il faudra créer un utilisateur sur l'active directory pour tester la connexion via un poste, pour cela, nous allons aller sur notre serveur, puis dans Utilisateurs et ordinateurs Active Directory :


Tout
Applications
Documents
Paramètres
Dossiers
Photos
Meilleur résultat
Utilisateurs et ordinateurs Active Directory
Système
Applications
Module Active Directory pour Windows PowerShell
Sites et services Active Directory
Domaines et approbations Active Directory
Centre d'administration Active Directory
Paramètres (7+)
L'indexation de la recherche a été désactivée.
Réactivez l'indexation.
Utilisateurs et ordinateurs Active Directory
Système
Ouvrir
Exécuter en tant qu'administrateur
Exécuter en tant qu'autre utilisateur
Ouvrir l'emplacement du fichier
Épingler au menu Démarrer
Épingler à la barre des tâches
activ



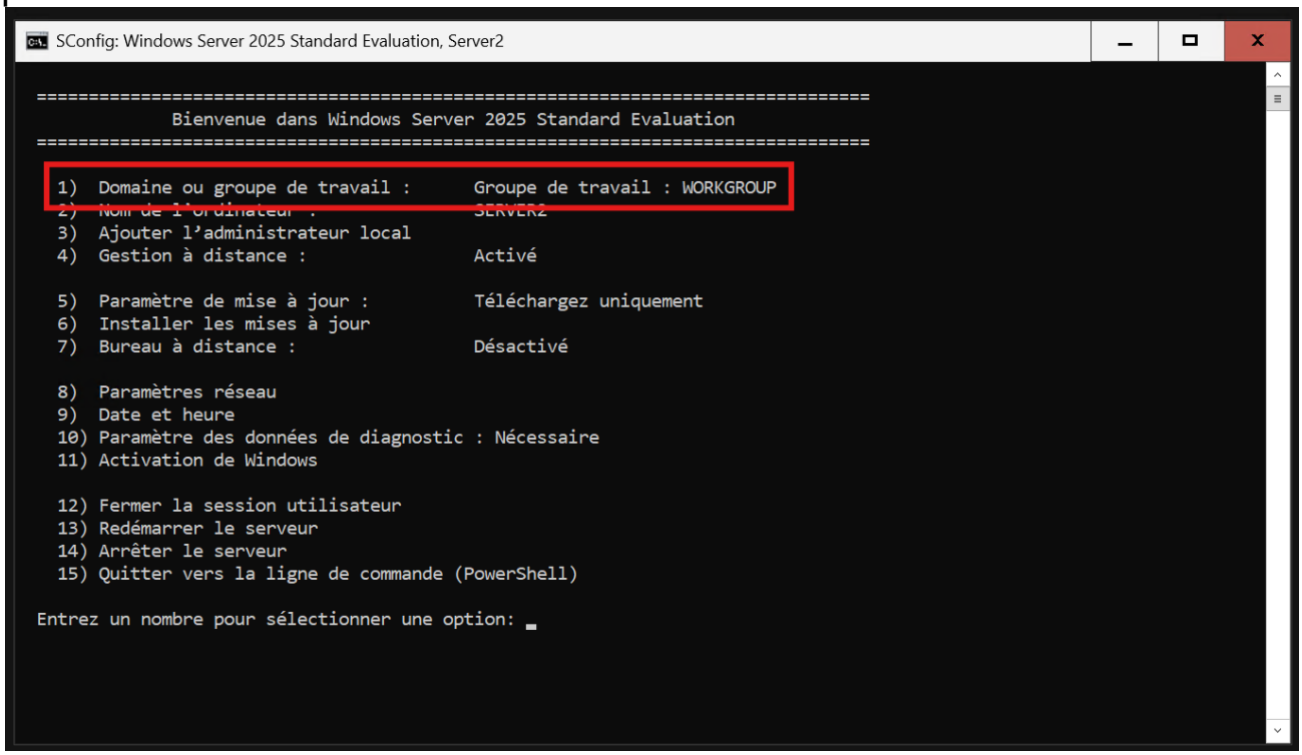


Une fois ceci fait, nous pouvons nous connecter sur le poste client :

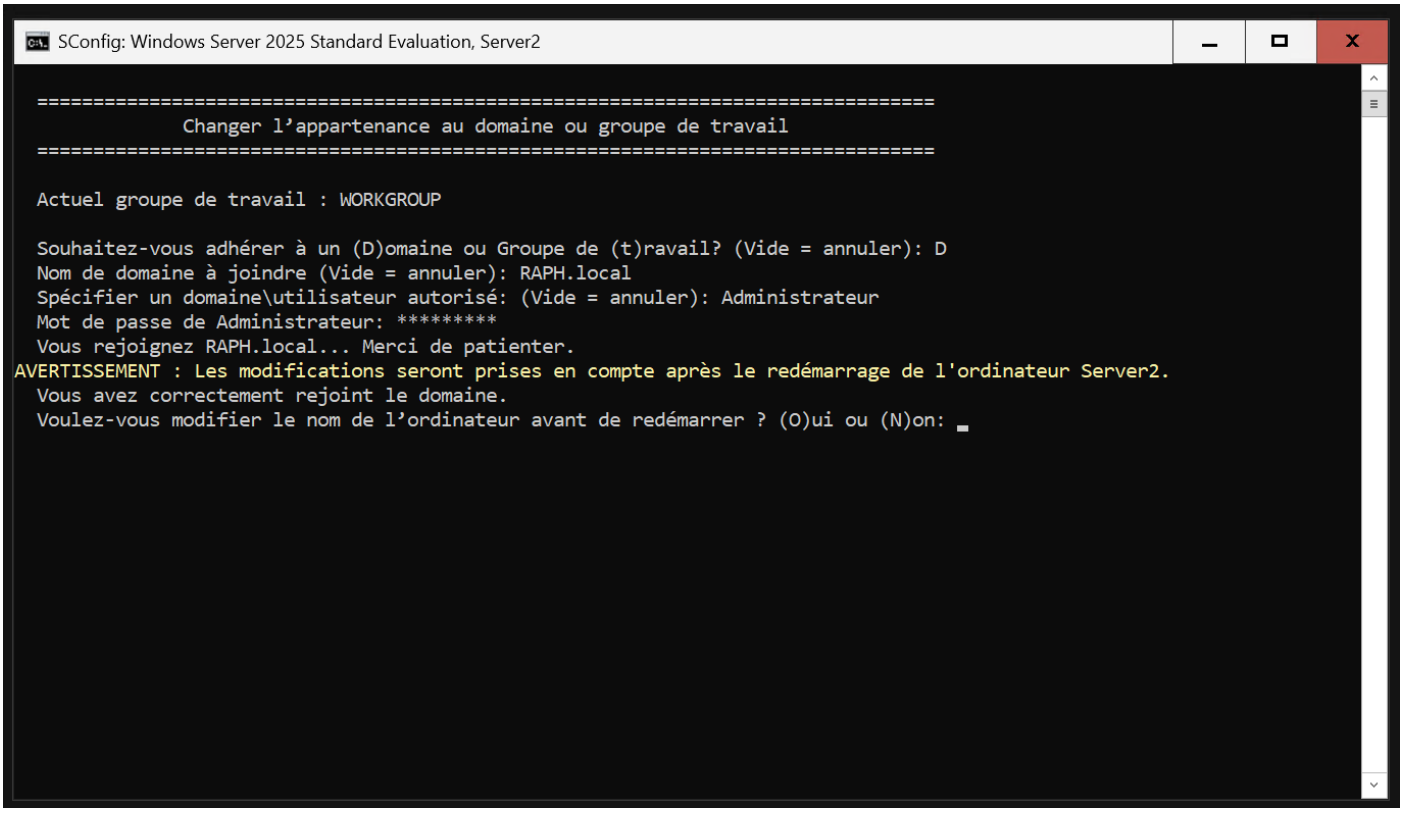


Une fois connecté, nous sommes enfin sur un compte utilisateur Active Directory !

Nous allons aussi intégrer le poste Windows Server Core dans l'AD, pour cela, nous allons sélectionner la première option dans sconfig (Domaine ou groupe de travail) :



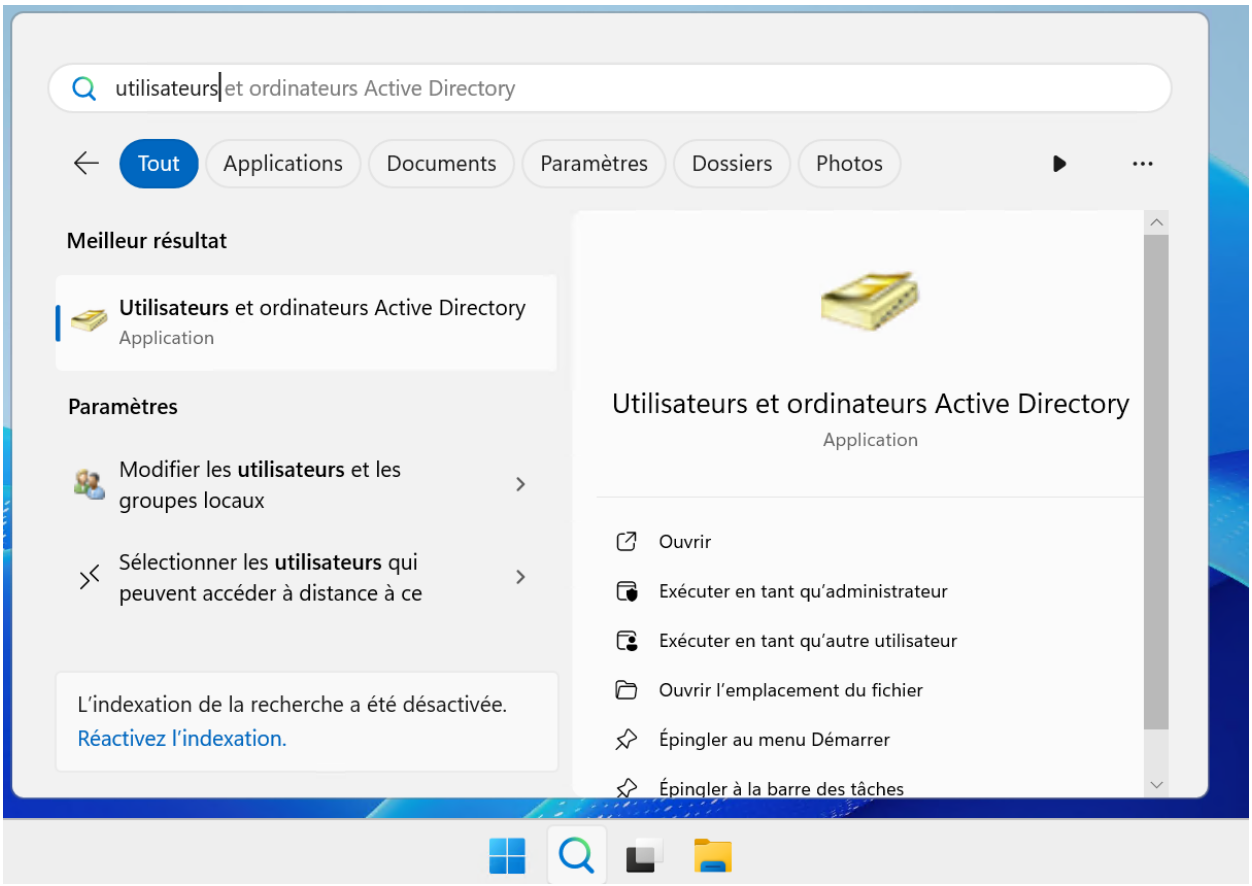
Maintenant, nous allons sélectionner l'option « D » pour choisir un domaine, puis nous allons indiquer notre nom de domaine avec son compte admin :



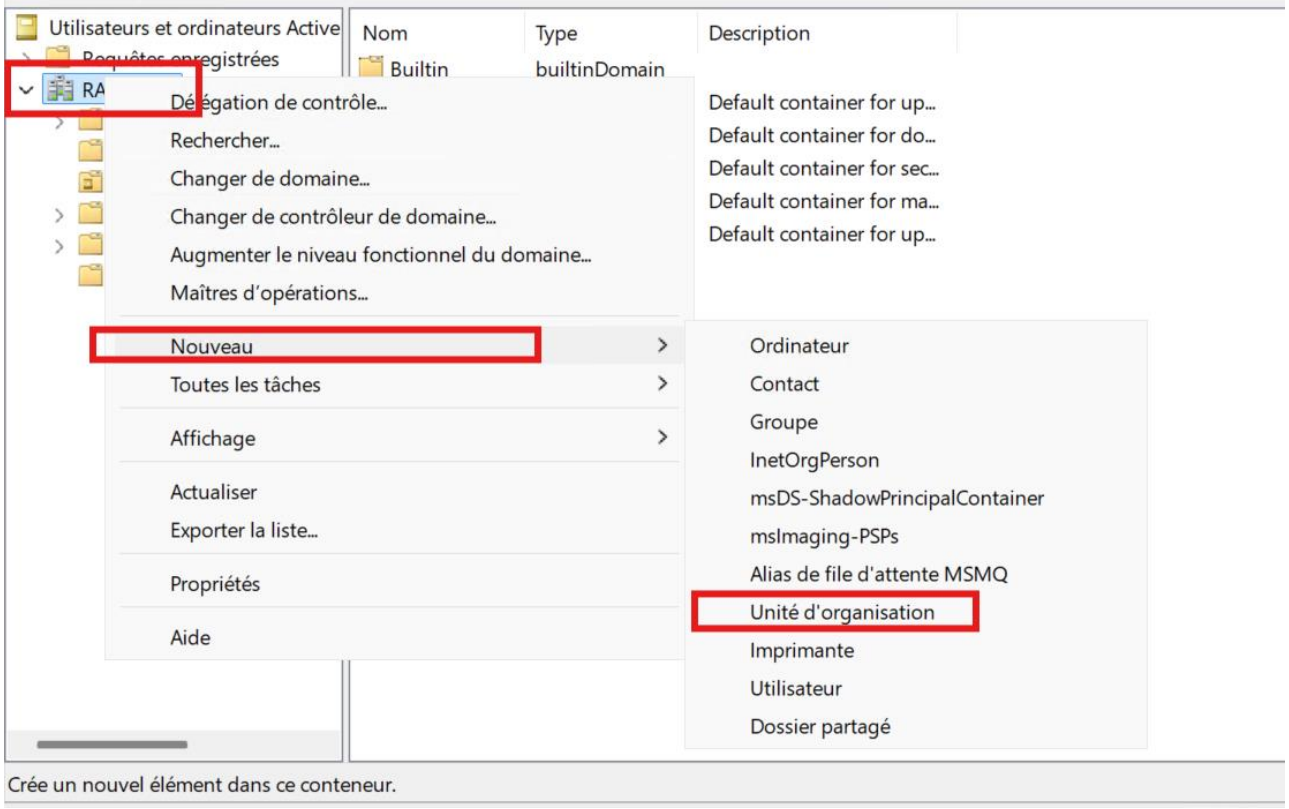
9. Création des OU, utilisateurs et groupes dans Active Directory

Maintenant que tout est en place, nous allons installer les utilisateurs suivants sur notre AD :

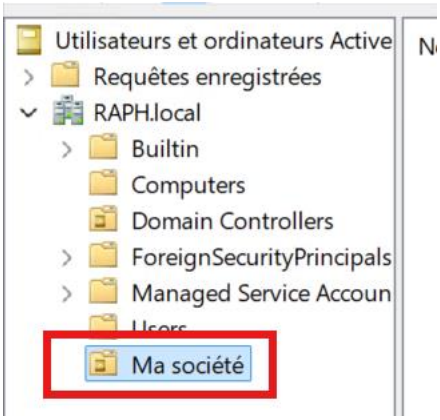
Premièrement, nous allons ouvrir le programme « Utilisateurs et ordinateurs Active Directory ». Pour cela, nous allons chercher dans la base de recherche Windows et l'ouvrir :



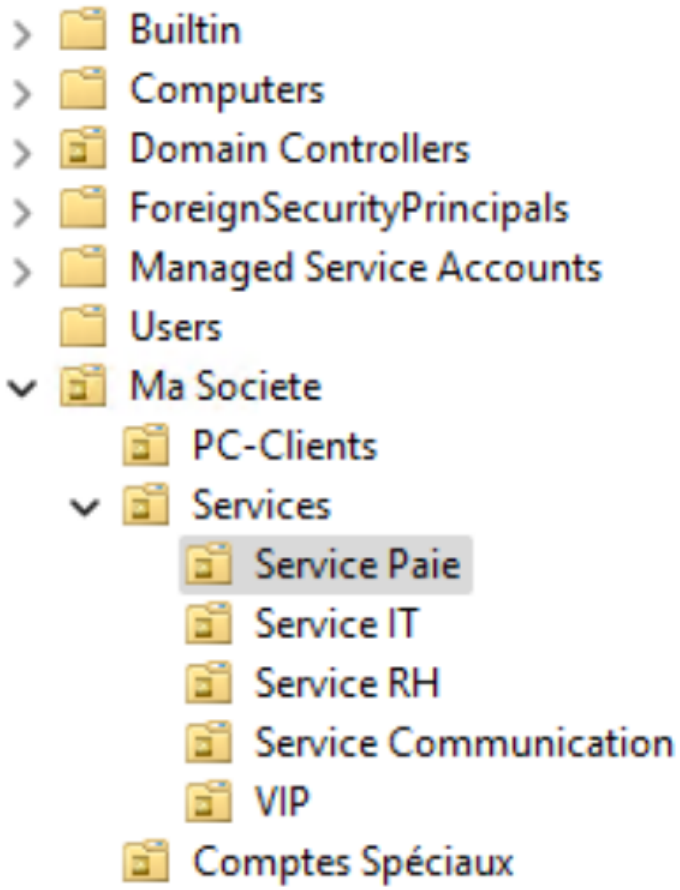
Une fois ceci fait, nous allons faire un clic droit sur « RAPH.local », puis nous allons faire « Nouveau » et enfin « Unité d'organisation » :



Cette dernière devra s'appeler « Ma société » :



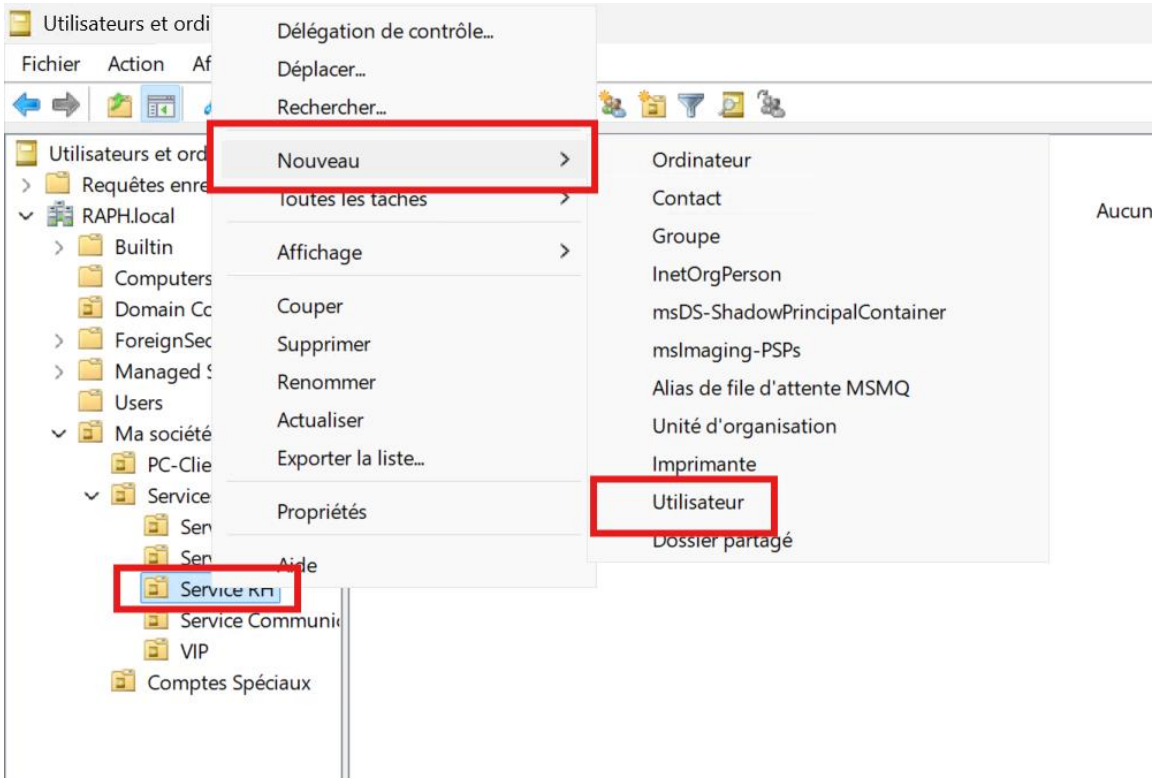
Maintenant, nous allons faire pareil, pour l'arborescence qui suit (avec tous les services présents dans notre entreprise) :



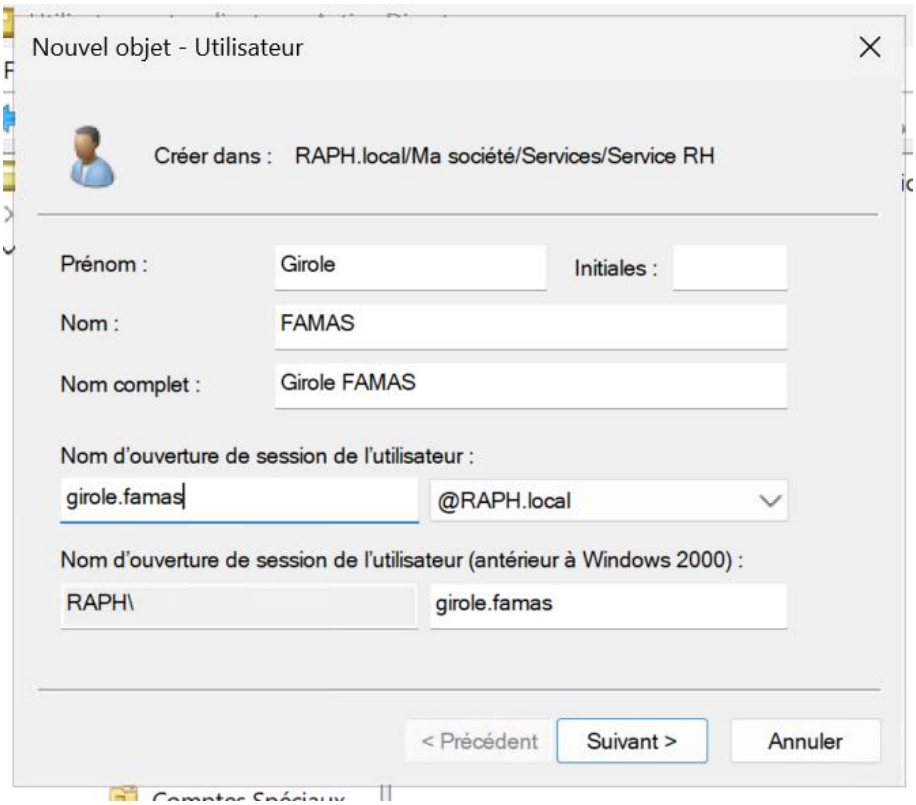
Les utilisateurs suivants doivent être crée :

NOM	Prénom	OU	Groupe	Mot de passe
XXIII	Jean	VIP	Grp_VIP	-qQqQ123..
SAINTDENIS	Benoit	IT	Grp_IT	-wWwW123..
CAMAT	Christine	Communication	Grp_COM	-JuJu456..
FAMAS	Girole	RH	Grp_RH	+HhHh159..
BOUK	Imen	PAIE	Grp_PAIE	+HhHh159..

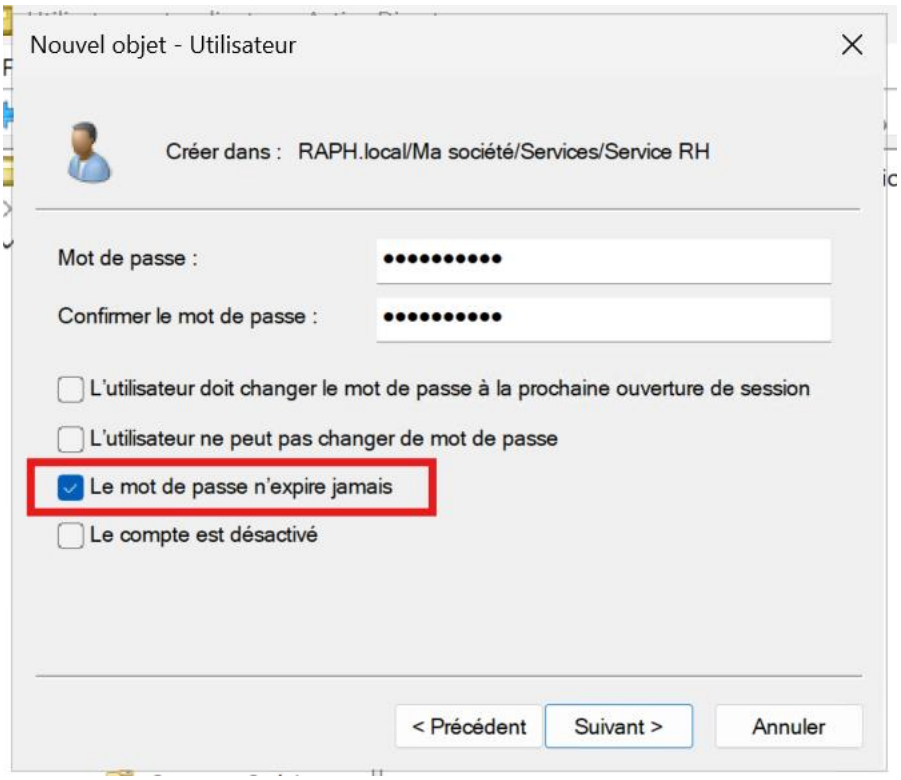
Pour cela, il suffit de se rendre dans un OU que nous avons créé (ici, nous allons prendre l'exemple du service RH), de faire clic droit, nouveau, puis, utilisateur :



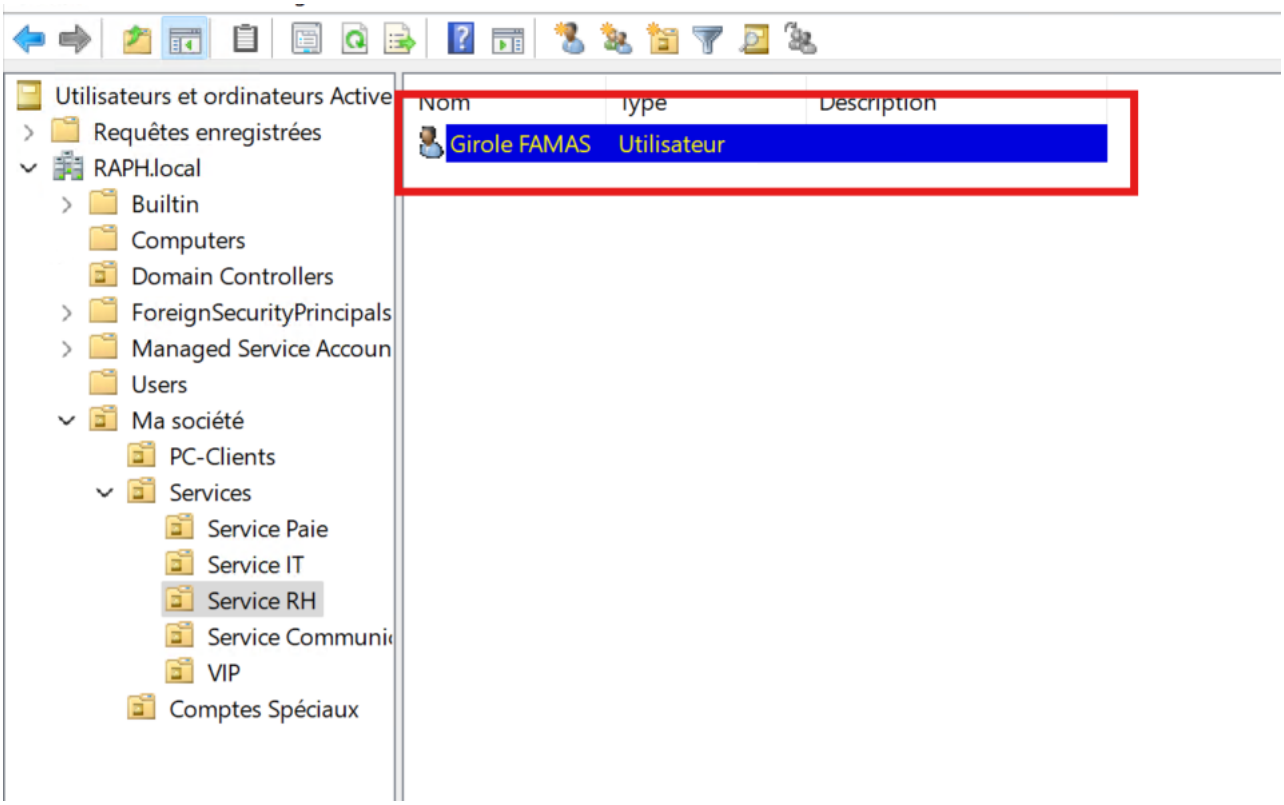
Puis, nous allons indiquer les informations de l'utilisateurs dans les différents champs :



Puis enfin, nous allons indiquer le mot de passe de l'utilisateur (en cochant bien l'option « Le mot de passe n'expire jamais ») :



Une fois créer, l'utilisateur est visible dans notre OU :

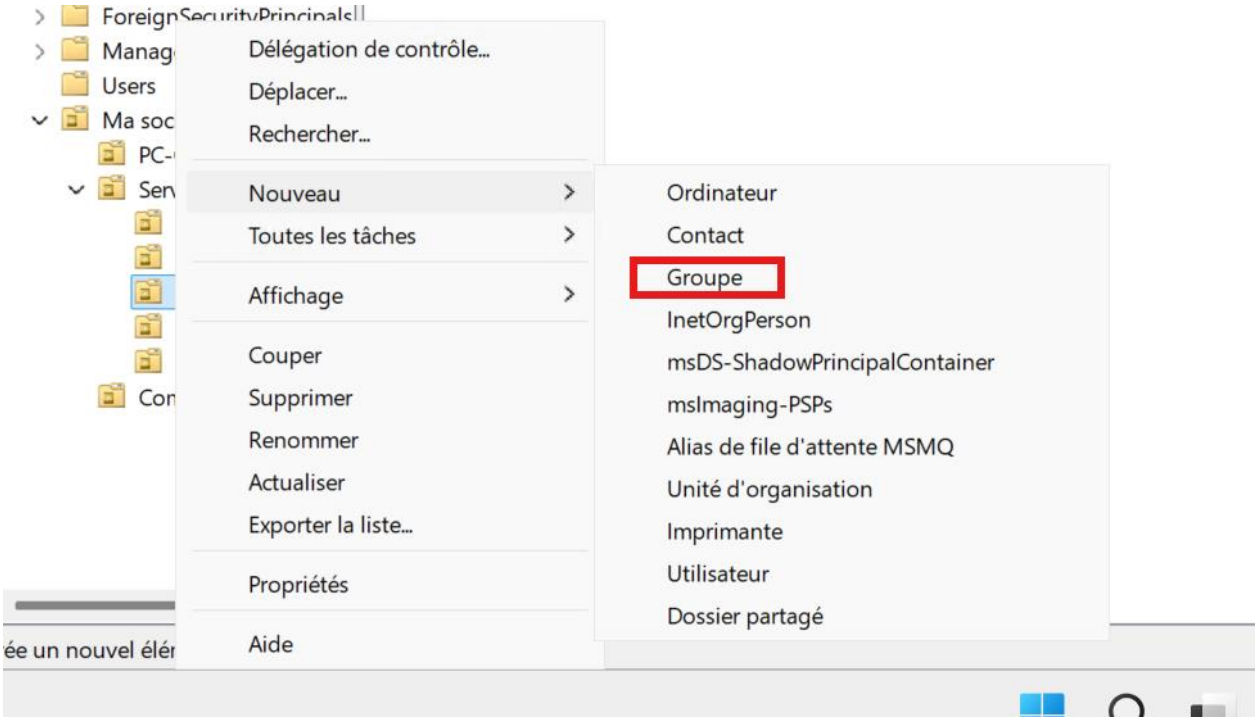


Maintenant, nous allons créer les différents groupes :

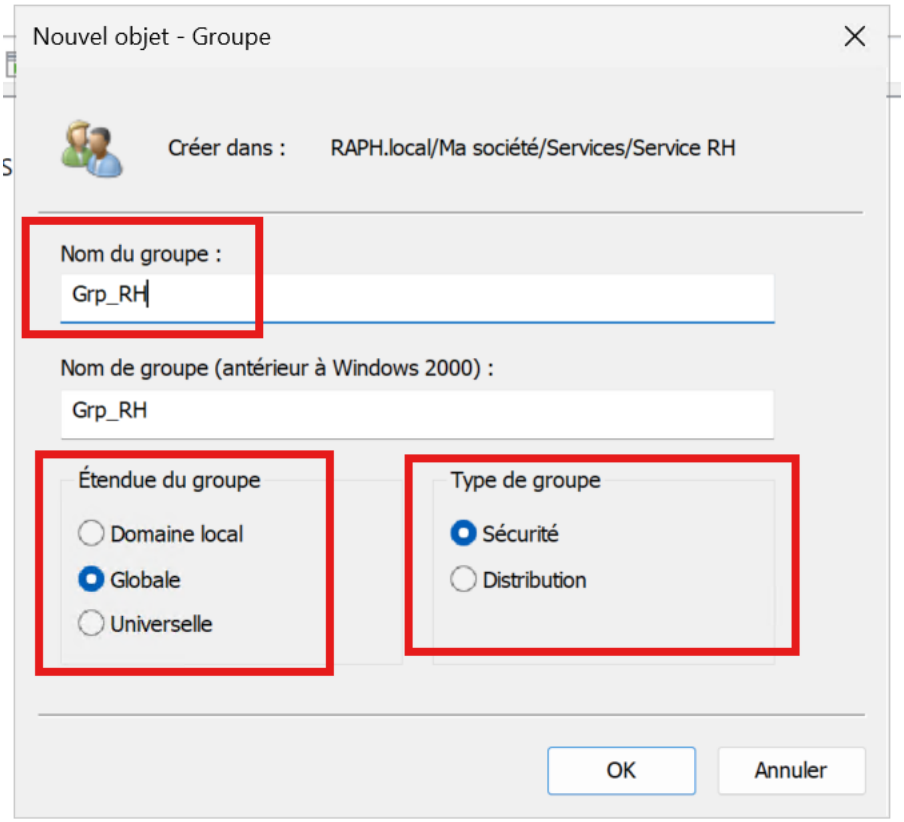
NOM	OU	Type	Etendue
Grp_IT	IT	Sécurité	Universelle
Grp_COM	Communication	Sécurité	Local
Grp_RH	RH	Sécurité	Local
Grp_Paie	PAIE	Sécurité	Local
Grp_VIP	VIP	Sécurité	Global

Exemple de création d'un groupe (groupe RH) :

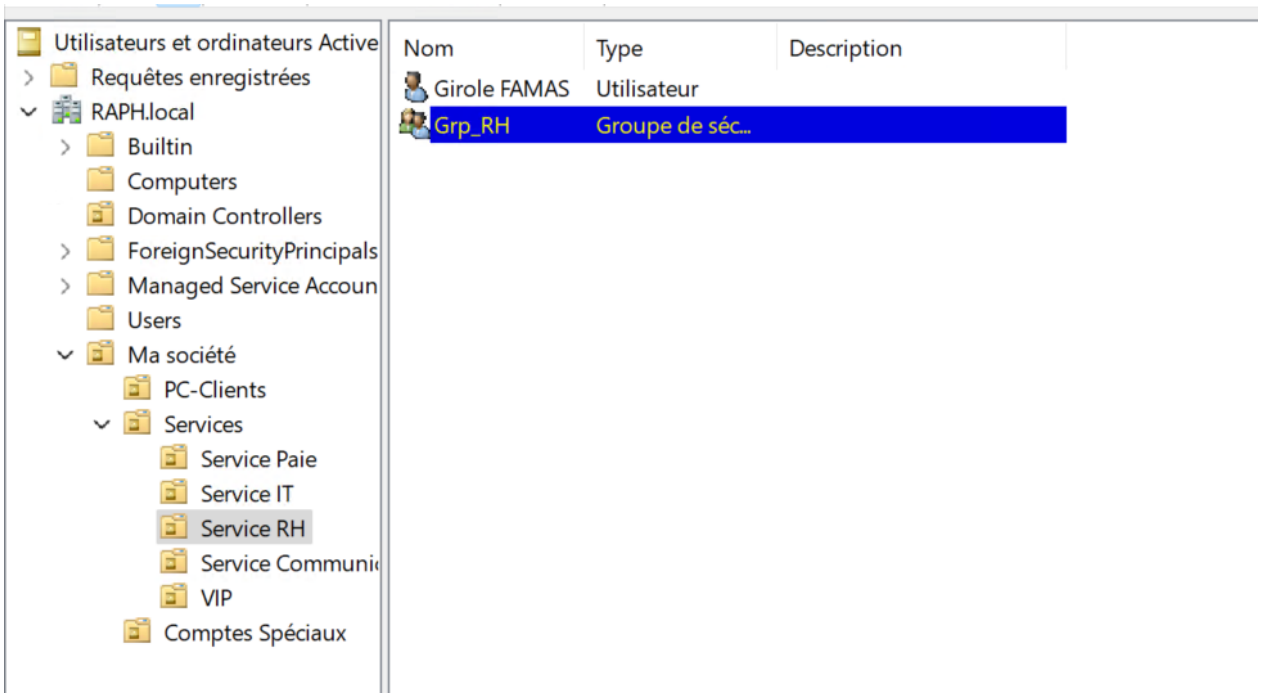
Premièrement, nous allons nous rendre sur notre OU, faire clic droit, nouveau, puis nouveau groupe :

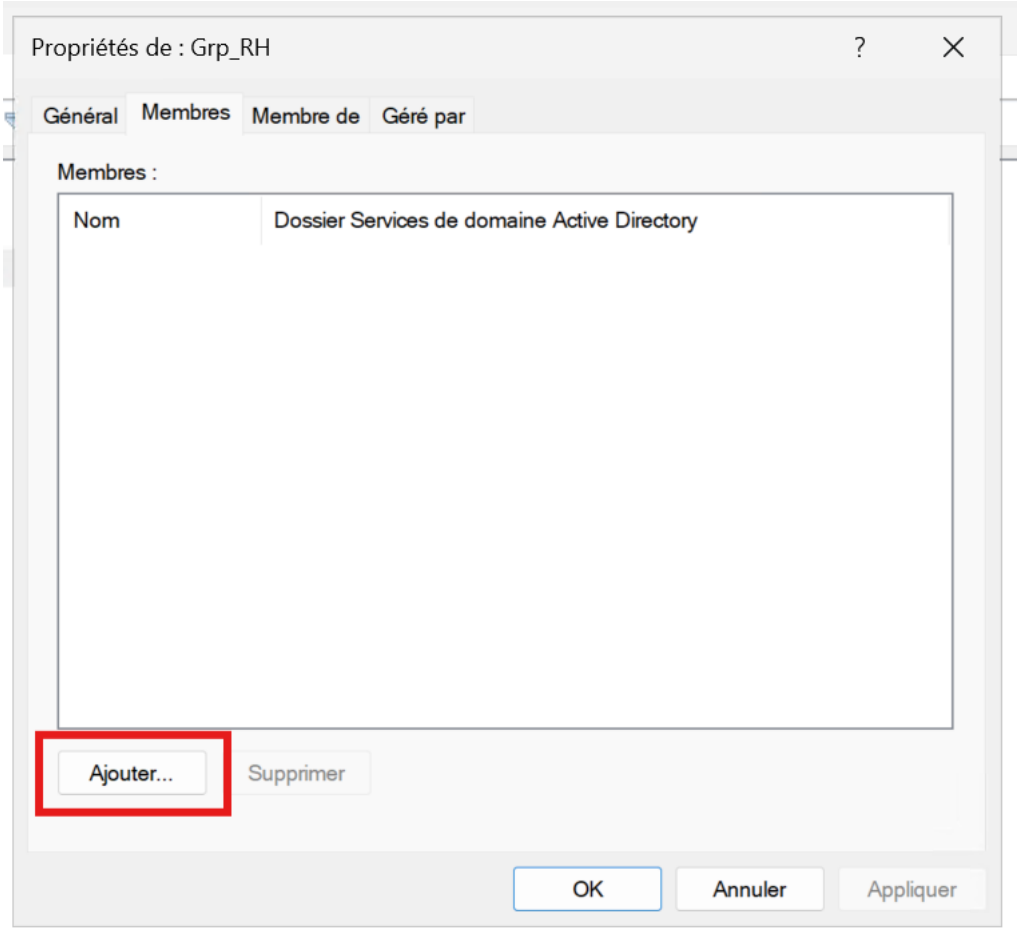


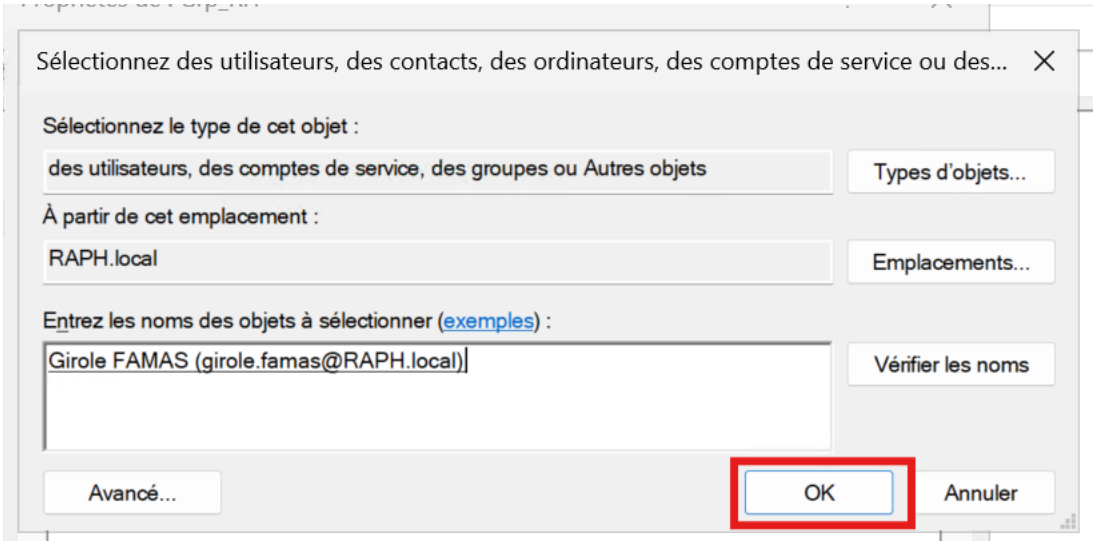
Une fois dans l'outil de création de groupe, nous allons entrer toute les infos (nom du groupe, étendue du groupe, type du groupe) puis nous pouvons confirmer :

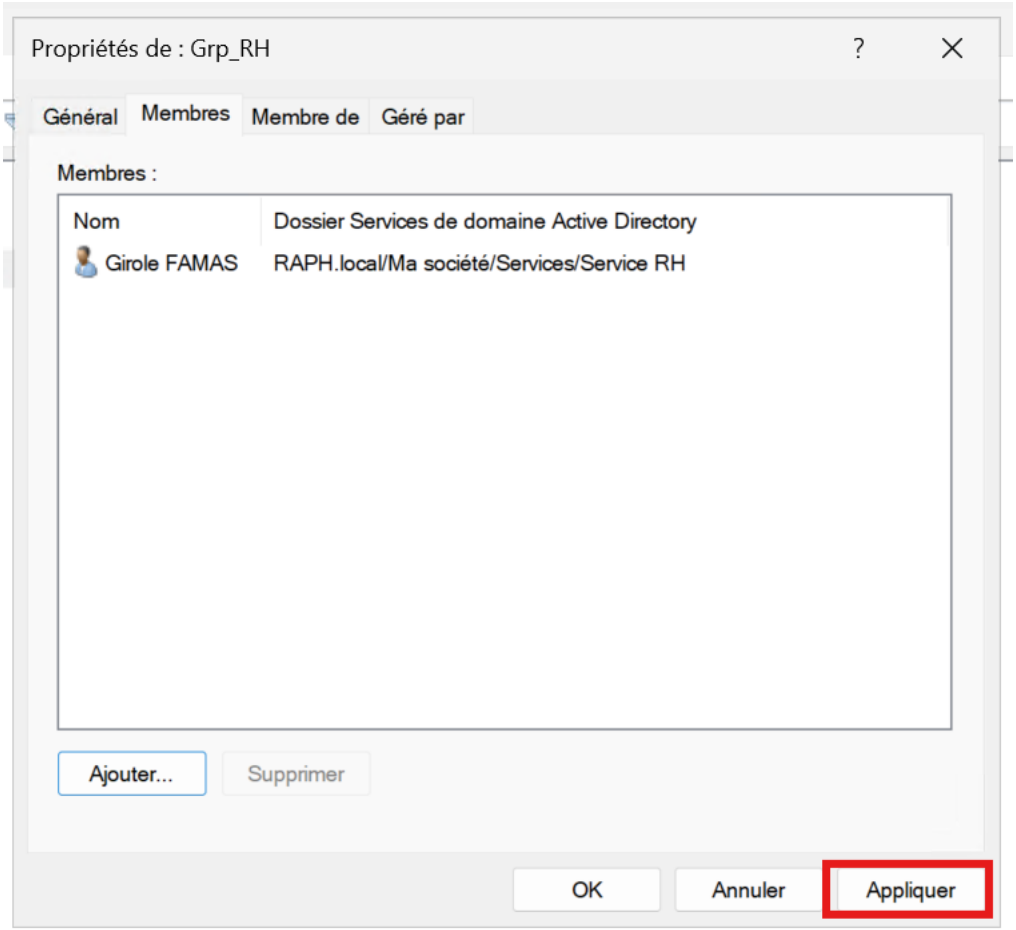


Une fois le groupe créer, nous allons double cliquer dessus, aller dans utilisateurs, nous nous allons ajouter l'utilisateur de notre service RH :









Une fois ceci fait, notre utilisateur est bien lié au groupe ! Les OU, utilisateurs et groupes ont été crée

Les types, étendues de groupe et GPO :

1. Les Types de groupes Il existe deux types distincts selon l'usage souhaité :

- Groupe de Sécurité : Possède un identifiant de sécurité (SID). Il sert à attribuer des permissions (ACL) sur des ressources (dossiers, imprimantes) et peut aussi servir pour la messagerie.
- Groupe de Distribution : Ne possède pas de SID de sécurité. Il est utilisé uniquement pour créer des listes de diffusion de courriels (ex: avec Exchange), sans gérer de droits d'accès.

2. Les Étendues de groupes (Scopes) L'étendue définit la portée du groupe dans l'architecture (domaine/forêt) :

- Groupe Global : Contient des objets du même domaine. On l'utilise pour regrouper les utilisateurs par rôle ou service (ex: G_Compta).
- Groupe de Domaine Local : Accepte des membres de toute la forêt mais n'est visible que dans son propre domaine. On l'utilise pour appliquer les droits d'accès sur les ressources locales (ex: DL_Imprimante_Etage1).
- Groupe Universel : Accepte des membres de n'importe quel domaine de la forêt. Il est stocké dans le Catalogue Global (utile pour les environnements multi-domaines).

3. Les GPO(Group Policy Object)

Différences entre Stratégie Ordinateur et Utilisateur La distinction principale réside dans la cible et le moment de l'application :

- **Configuration Ordinateur (Computer) :**
  - Cible : La machine physique (s'applique au registre HKLM).
  - Moment : S'applique au démarrage de l'OS (avant le login).

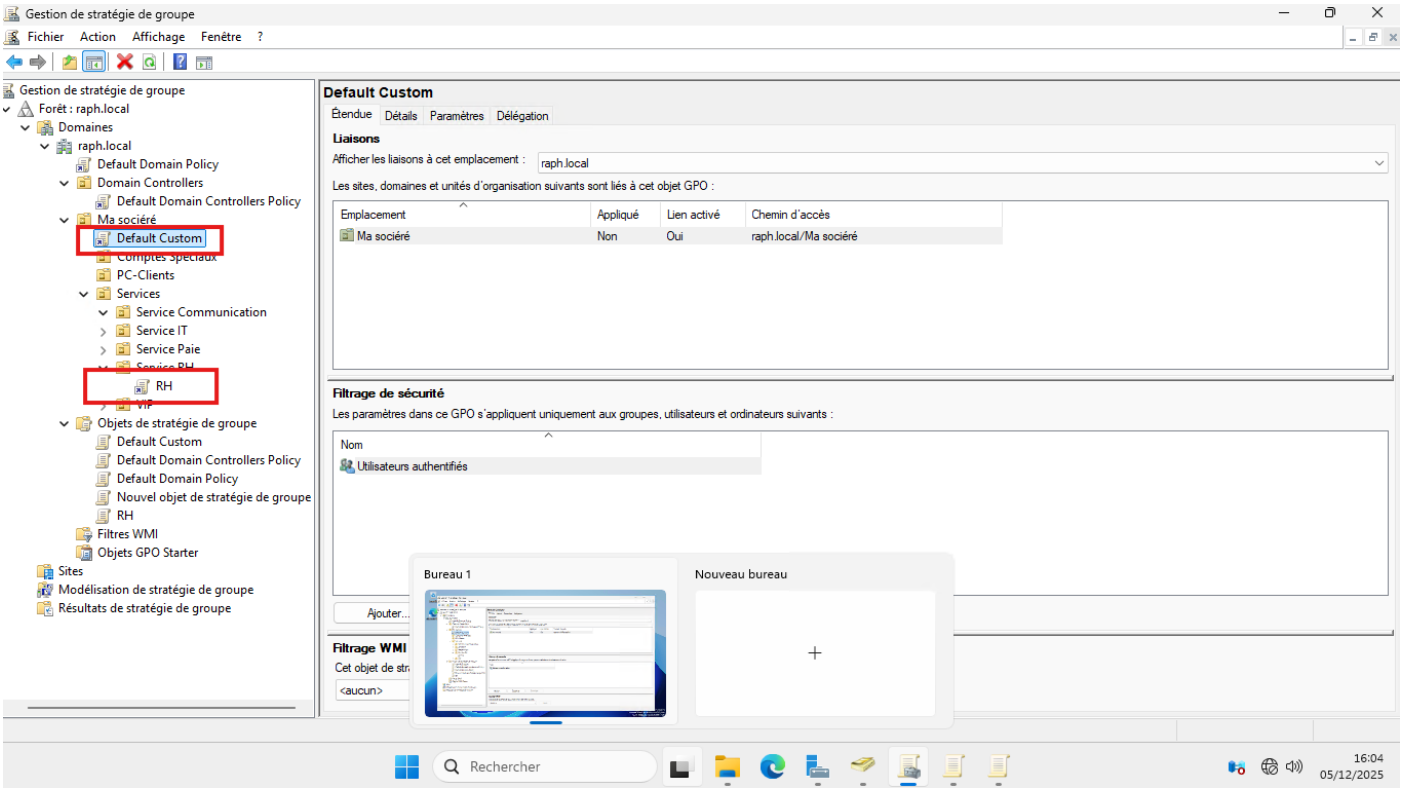
- Usage : Sécurité système, pare-feu, installation de logiciels MSI, scripts de démarrage.

- **Configuration Utilisateur (User) :**
  - Cible : Le compte utilisateur (s'applique au registre HKCU).
  - Moment : S'applique à l'ouverture de session (après le login).
  - Usage : Mappage de lecteurs réseau, imprimantes, fond d'écran, raccourcis bureau.

10. Exercice GPO

Exercice 1 : Appliquer un fond d'écran spécifique aux utilisateurs du service RH

Création de plusieurs GPO (une par défaut, et une pour le service RH)



1. Appliquer un fond d'écran spécifique (Utilisateur)

Ce paramètre force l'affichage d'une image pour l'utilisateur.

- **Emplacement** : Configuration utilisateur
- **Chemin** : Stratégies > Modèles d'administration > Bureau > Bureau
- **Paramètre à modifier** : **Papier peint du Bureau**
- **Action** : Mettre sur "Activé".
- **Important** : Dans le champ "Nom du papier peint", vous devez indiquer le chemin réseau (UNC) de l'image (ex: \\Serveur\Partage\image.jpg) et non un chemin local (C:...), sinon les autres postes ne pourront pas trouver l'image.

Image choisie : **C:\Windows\Web\Screen\img104.jpg (local)**

2. Désactiver l’accès aux clés USB (Ordinateur)

Le prompt mentionnant "pour tous les postes", il est préférable de le faire au niveau "Ordinateur" pour une sécurité maximale, quel que soit l'utilisateur connecté.

- **Emplacement** : Configuration ordinateur
- **Chemin** : Stratégies > Modèles d'administration > Système > Accès au stockage amovible
- **Paramètre à modifier : Toutes les classes de stockage amovible : Refuser tout accès**
- **Action** : Mettre sur "Activé".

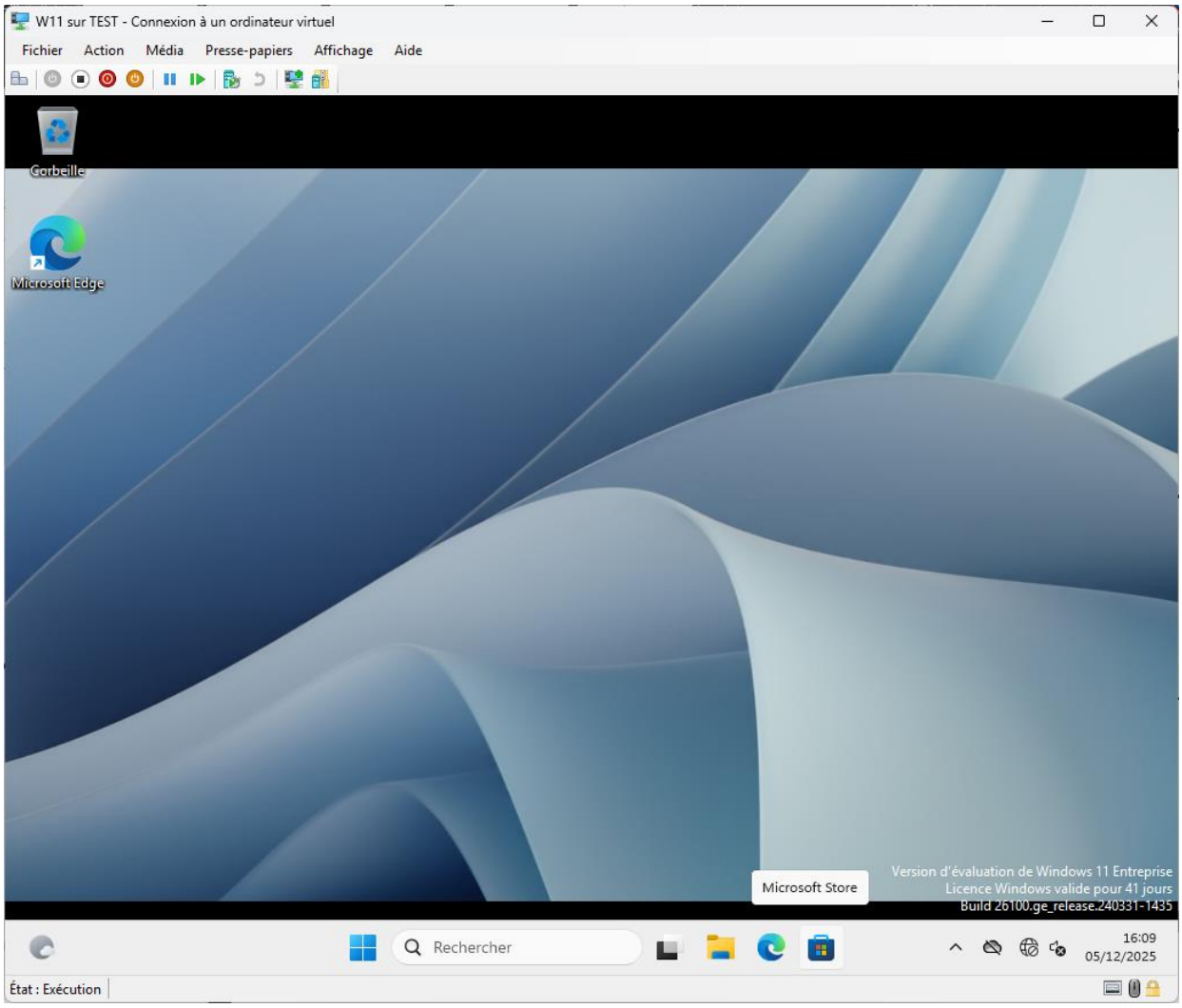
3. Bloquer le panneau de configuration (Utilisateur)

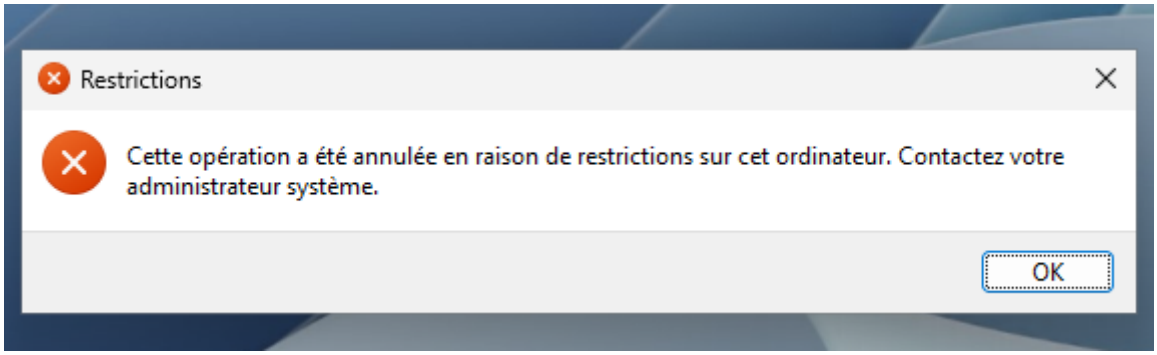
Cela empêche l'utilisateur d'accéder aux réglages sensibles.

- **Emplacement** : Configuration utilisateur
- **Chemin** : Stratégies > Modèles d'administration > Panneau de configuration

- **Paramètre à modifier : Interdire l'accès au Panneau de configuration et aux paramètres du PC**
- **Action** : Mettre sur "Activé".

Une fois ceci fait, nous pouvons nous connecter sur un utilisateur RH et vérifier si le fond d'écran et le blocage du panneau de contrôle est bien présent :





Exercice 2 : Déploiement de logiciel via GPO (7-Zip)

Le déploiement de logiciel par GPO se fait via la fonctionnalité **Installation de logiciel** (Software Installation).

1. Préparation du Fichier

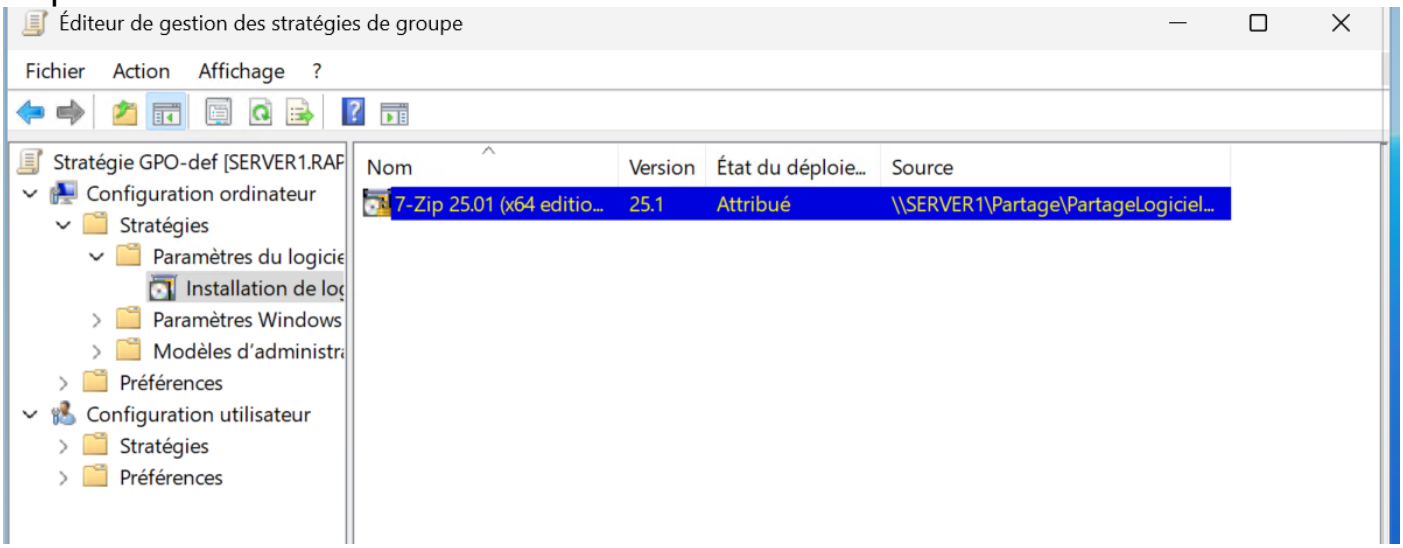
Le déploiement par GPO nécessite un package au format **MSI** (Windows Installer). Vous devez d'abord obtenir l'installeur MSI de 7-Zip.

Download 7-Zip 25.01 (2025-08-03) for Windows:

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip installer for Windows
Download	.exe	32-bit Windows x86	
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.7z	Windows x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager
Download	.tar.xz	64-bit Linux x86-64	7-Zip for Linux: console version
Download	.tar.xz	32-bit Linux x86	
Download	.tar.xz	64-bit Linux arm64	
Download	.tar.xz	32-bit Linux arm	
Download	.tar.xz	macOS (arm64 / x86-64)	7-Zip for MacOS: console version
Download	.7z	any / Windows	7-Zip Source code
Download	.tar.xz	any / Windows	7-Zip Source code
Download	.7z	any / Windows	LZMA SDK: (C, C++, C#, Java)
Download	.exe	Windows	7zr.exe (x86) : 7-Zip console executable

We recommend to use .exe type installer instead of .msi installer version

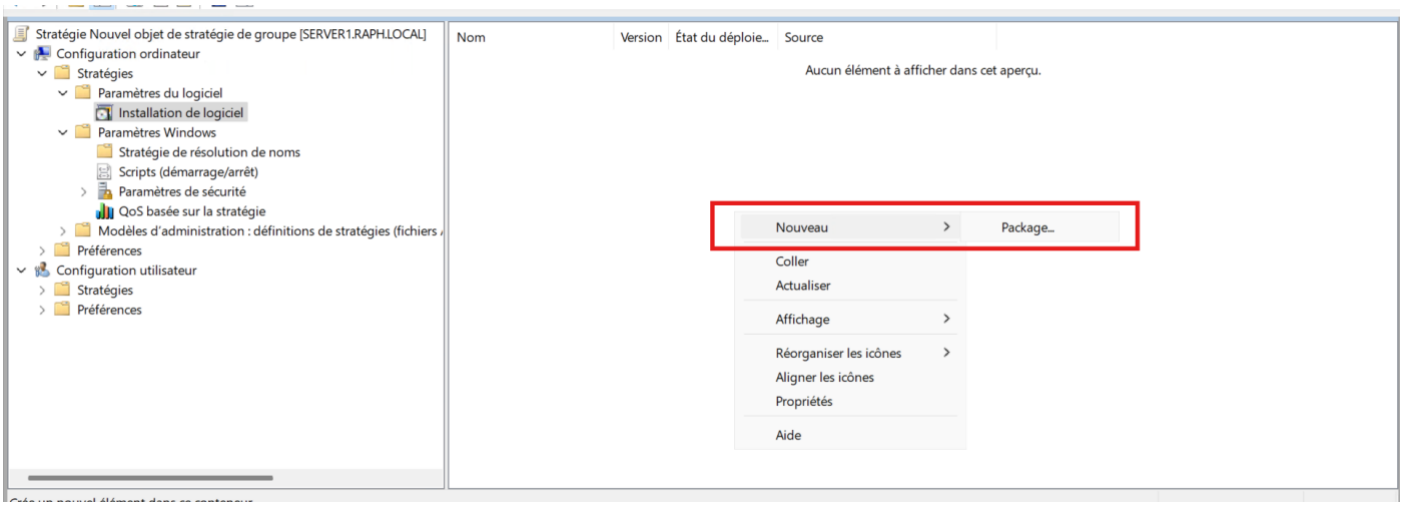
- **Partage réseau :** Placez le fichier MSI dans un **partage réseau** accessible en lecture par les ordinateurs cibles (ex: \\SERVER1\Partage\PartageLogiciel\7z.msi).



2. Création de la Stratégie

Ouvrez l'Éditeur de gestion des stratégies de groupe de la GPO liée à votre OU cible.

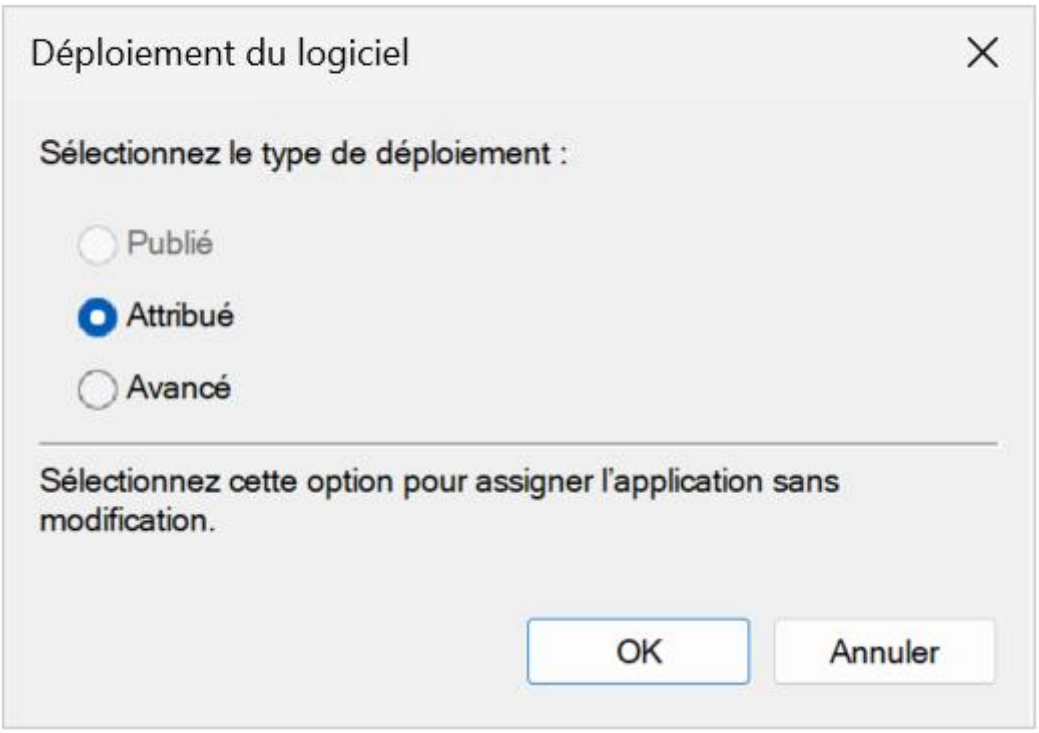
- **Emplacement** : Configuration ordinateur
- **Chemin** : Stratégies > Paramètres du logiciel > **Installation de logiciel**



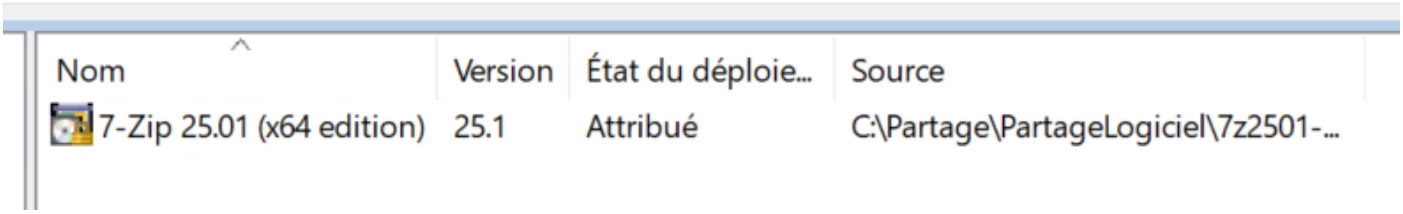
3. Déploiement

1. Faites un clic droit sur **Installation de logiciel**.
2. Sélectionnez **Nouveau** > **Package...**

3. Dans la fenêtre qui s'ouvre, naviguez jusqu'à l'emplacement réseau de votre fichier **MSI** (utilisez le chemin UNC, par exemple : \\Server1\Partage\PartageLogiciel\7z.msi).
4. Sélectionnez le fichier et cliquez sur **Ouvrir**.
5. Choisissez la méthode de déploiement :
   - **Publiée** : (Configuration utilisateur) L'utilisateur peut installer le logiciel depuis le Panneau de configuration.
   - **Attribuée** : (Configuration ordinateur) Le logiciel est **installé automatiquement** au redémarrage de l'ordinateur. C'est le choix standard pour un déploiement obligatoire.



Le logiciel sera installé automatiquement la prochaine fois que le poste client redémarrera et appliquera la stratégie.



Exercice 3 : Rapport d'application des GPO et analyse

Pour générer un rapport d'application des GPO sur un poste client, la commande la plus utile est **gpresult**.

1. Générer le rapport

Ouvrez une **Invite de commande (CMD)** ou **PowerShell** en tant qu'administrateur sur le poste client concerné et exécutez la commande suivante :

gpresult /h C:\RapportGPO.html /f

- **/h :** Indique que le rapport doit être généré au format **HTML** (plus lisible).
- **C:\RapportGPO.html :** Le chemin où le fichier sera enregistré.
- **/f :** Force l'écriture du fichier.

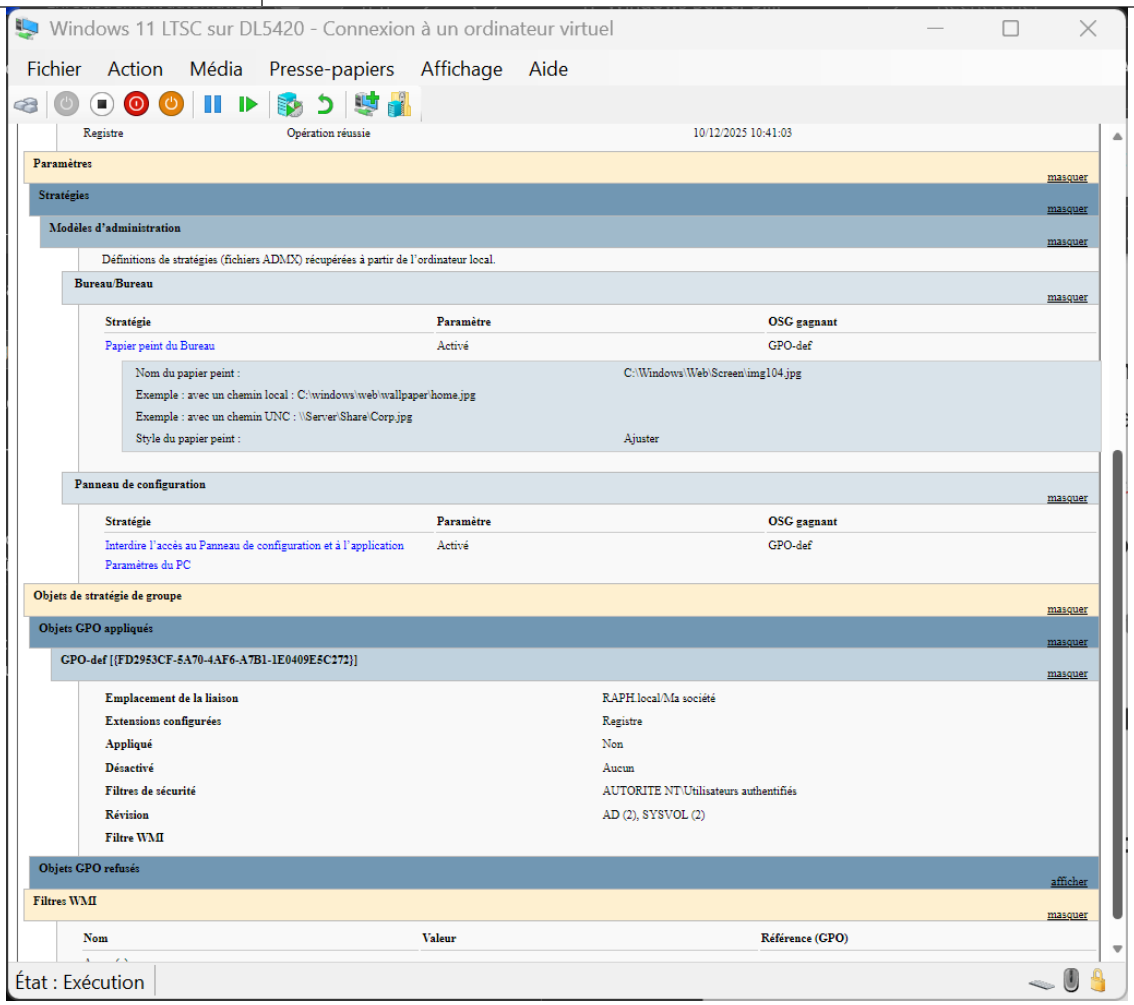
2. Analyser les résultats

Une fois la commande exécutée, ouvrez le fichier C:\RapportGPO.html dans un navigateur web. Le rapport est divisé en deux sections principales : **Détails de l'ordinateur** et **Détails de l'utilisateur**.

Les points clés à analyser sont :

Section du rapport	Que vérifier ?
GPO appliquées	Confirme la liste exacte des GPO (par nom) qui ont été appliquées.
GPO filtrées	Montre les GPO qui n'ont **pas** été appliquées et pourquoi (ex: filtrage de sécurité, désactivées, ...).
Détails de l'application de GPO	Indique la **dernière heure de mise à jour** des stratégies pour l'ordinateur et l'utilisateur.

Paramètres	Liste l'état final de chaque paramètre de stratégie (les réglages spécifiques comme le fond d'écran, l'accès USB, etc.).



11. Ajout ADMX

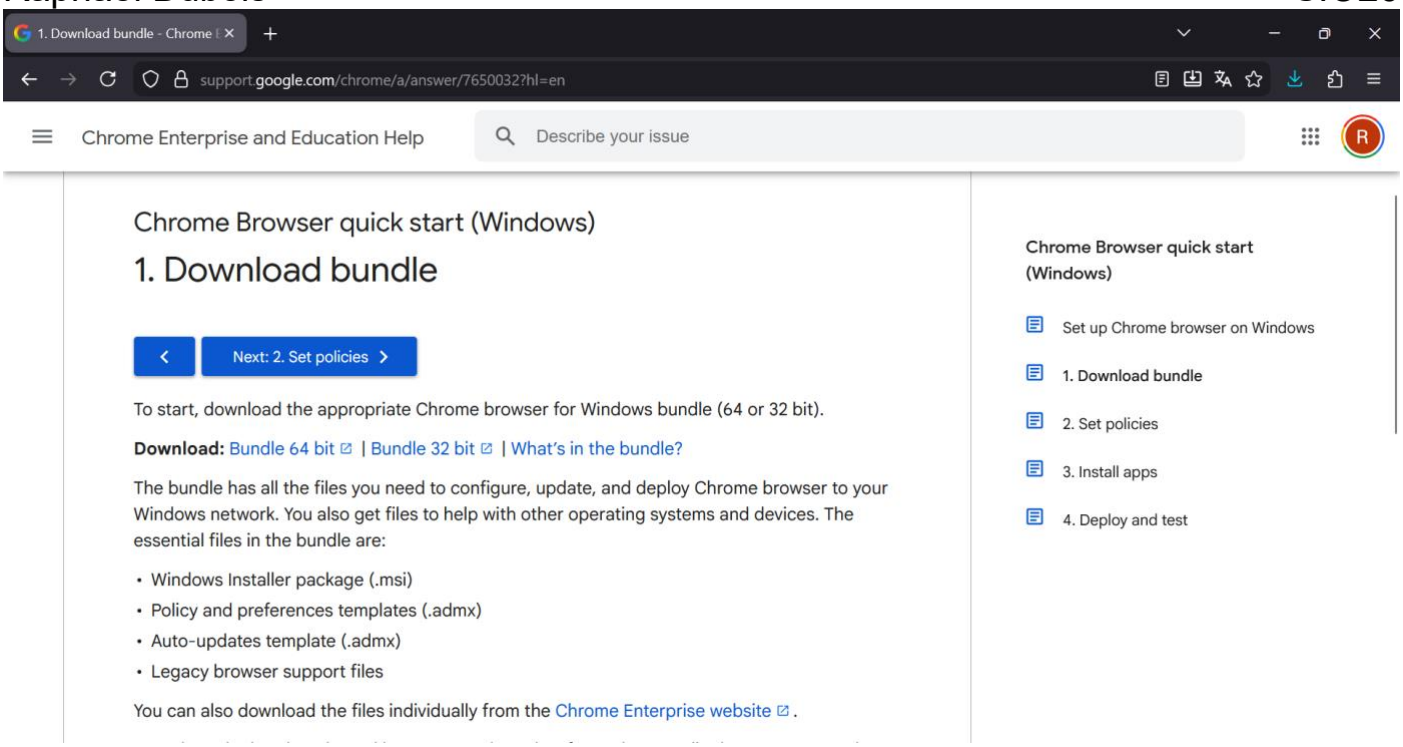
Voici les réponses aux exercices présentés dans les images, formulées directement.

Exercice 1 : Ajout d'un modèle ADMX personnalisé

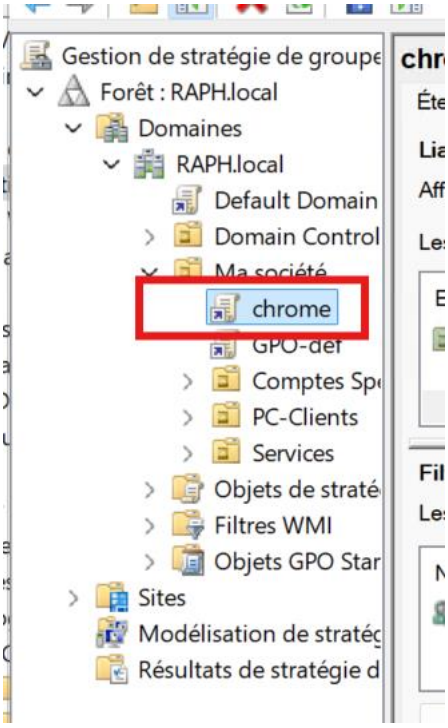
Pour gérer les paramètres de Google Chrome via GPO, voici la procédure à suivre :

1. **Préparation des fichiers :**

- Il faut télécharger le bundle "Google Chrome Enterprise" depuis le site officiel pour obtenir les fichiers .admx (structure) et .adml (langue).



- Une fois ceci fait, nous allons extraire le bundle, et créer une GPO

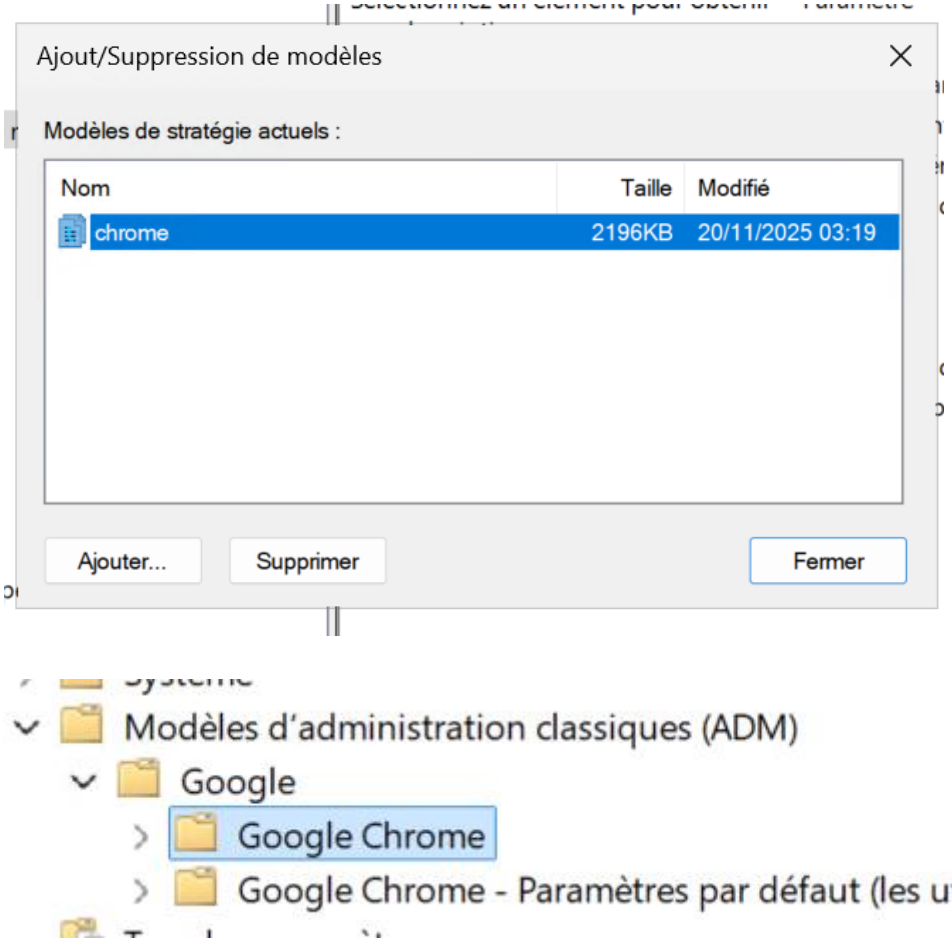


- Maintenant, nous allons modifier cette dernière, nous rendre dans **Configuration ordinateur > Stratégies > Modèle d'administration classiques** […] (fichiers

ADMX) et puis, nous allons faire clic droit dessus puis Ajout/Suppression de modèles

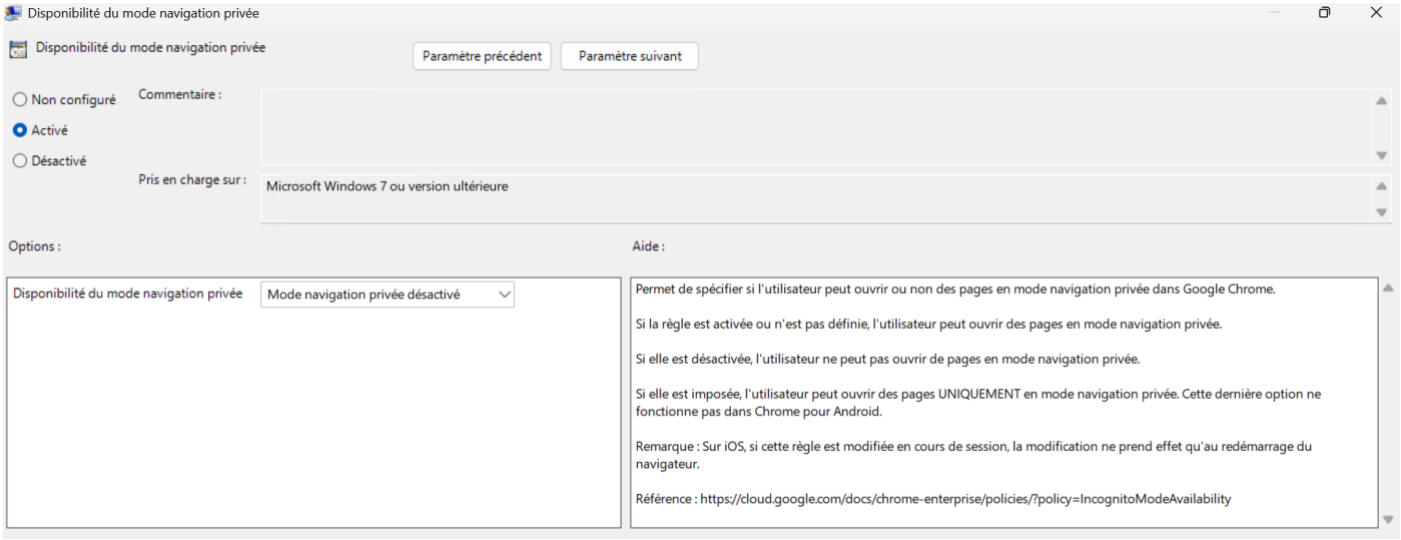


- Nous allons ajouter le modèle chrome.adm présent dans l'archive que nous avons décompressée (GoogleChromeEnterpriseBundle64\Configuration\adm\fr-FR\chrome.adm). Après avoir fait ceci, un peu plus bas, nous avons accès aux paramètres d'administration de Google Chrome

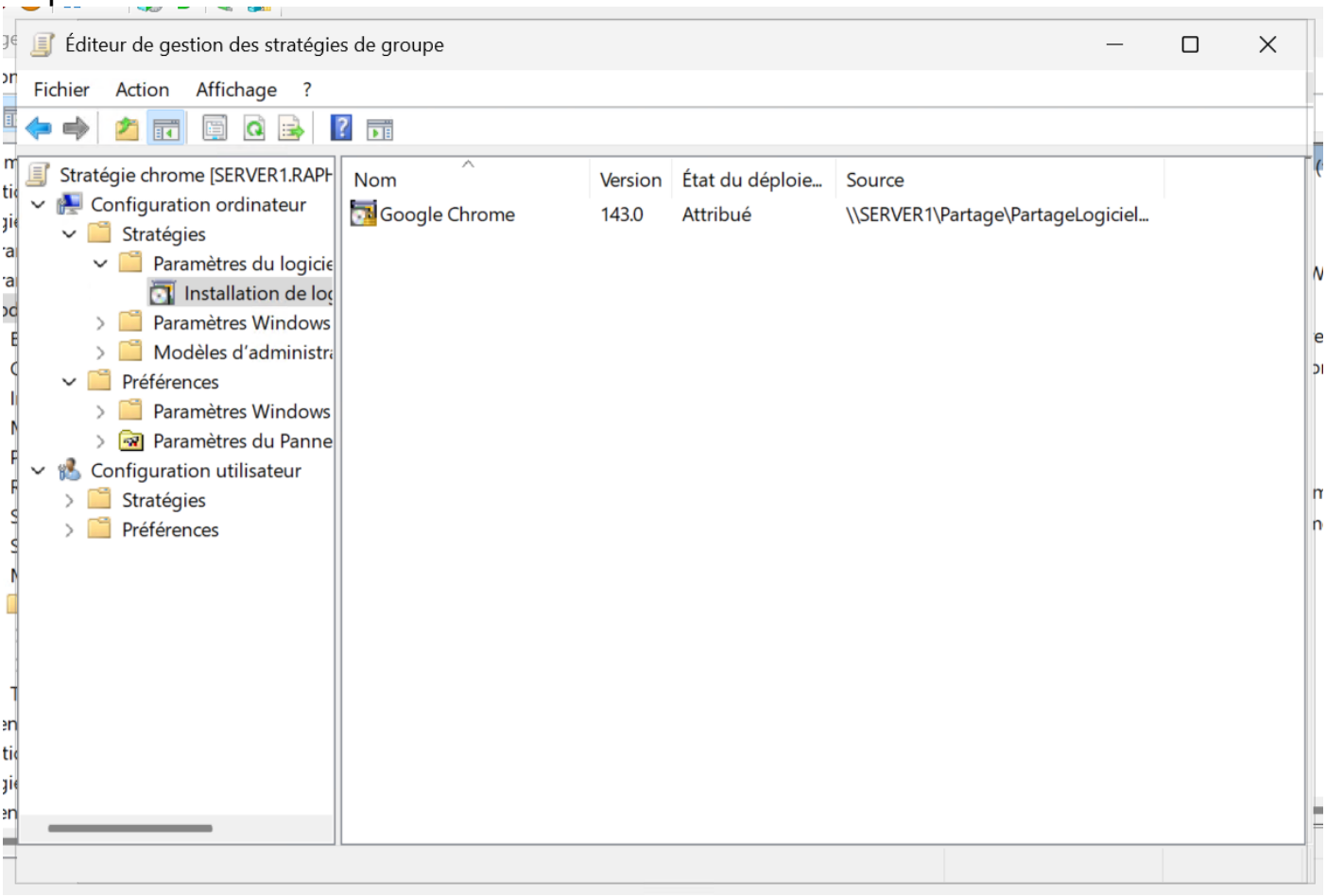


2. **Configuration de la GPO :**

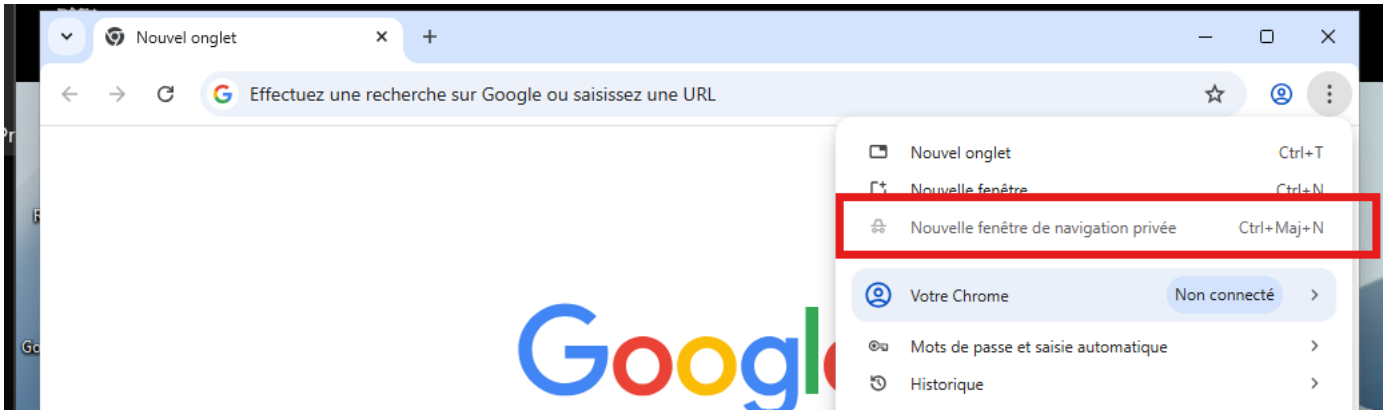
- Je navigue vers : Configuration ordinateur > Stratégies > Modèles d'administration > Google > Google Chrome.
- Pour le scénario demandé, je recherche le paramètre **"Disponibilité du mode navigation privée"** (Incognito mode availability) et je le passe sur **"Désactivé"** ou je force l'arrêt selon l'option précise pour empêcher l'utilisation du mode Incognito.



- Nous allons aussi ajouter le fichier « GoogleChromeStandaloneEnterprise64.msi » dans notre partage de logiciel dans \\SERVER1\Partage\PartageLogiciel\ GoogleChromeStandaloneEnterprise64.msi, et puis nous allons l'ajouter dans les logiciels à installer dans notre GPO



- Une fois ceci fait, nous pouvons se connecter sur la machine client, faire un gpupdate /force (redémarrer après), vérifier si chrome a bien été installé et le lancer pour voir si la navigation privée est bien présente :



Exercice 2 : Configuration de paramètres système via ADMX

Pour empêcher les utilisateurs de modifier les paramètres d'alimentation :

1. **Création de l'objet GPO :**

- Je crée une GPO nommée "GPO_Verrouillage_Alimentation".
- Cette stratégie s'appliquant à la machine, je la lie à une OU contenant les postes clients.

2. **Paramétrage :**

- Dans l'éditeur de gestion des stratégies de groupe, je vais dans :

Configuration ordinateur > Modèles d'administration > Système > Gestion de l'alimentation.

- Je sélectionne les paramètres de veille comme indiqué.
- Pour **interdire** la modification, il faut généralement passer le paramètre de restriction sur **"Activé"** (ex: "Empêcher les utilisateurs de modifier les paramètres de veille").

3. **Test :**

- Sur un poste client, j'exécute gpupdate /force pour appliquer la stratégie immédiatement et je vérifie que les options d'alimentation sont grisées.

Exercice 3 : Résolution de problèmes

Si les nouveaux paramètres ADMX ne s'affichent pas dans la console GPMC, voici les vérifications à effectuer :

1. **Vérification du Magasin Central :**

- Je vérifie que les fichiers ont bien été copiés dans le dossier PolicyDefinitions du SYSVOL et non dans le dossier local C:\Windows\PolicyDefinitions d'un seul serveur. La GPMC doit indiquer que les définitions sont "récupérées à partir du magasin central".

2. **Concordance des fichiers de langue (ADML) :**

- C'est une cause fréquente d'erreur : si j'ai copié le fichier .admx mais que le fichier .adml correspondant n'est pas dans le bon dossier de langue (ex: dossier fr-FR pour un serveur en français), le paramètre sera invisible ou affichera une erreur.

3. **Permissions et Réplication :**

- Je vérifie les permissions NTFS sur le dossier PolicyDefinitions pour m'assurer que les administrateurs ont bien le droit de lecture.
- Si l'infrastructure contient plusieurs contrôleurs de domaine, je vérifie que la réplication (DFS-R) s'est bien effectuée entre les serveurs.

4. **Journaux d'événements :**

- Je consulte l'Observateur d'événements (Event Viewer) dans la section "Stratégie de groupe" pour identifier d'éventuelles erreurs de parsing des fichiers XML (.admx).