

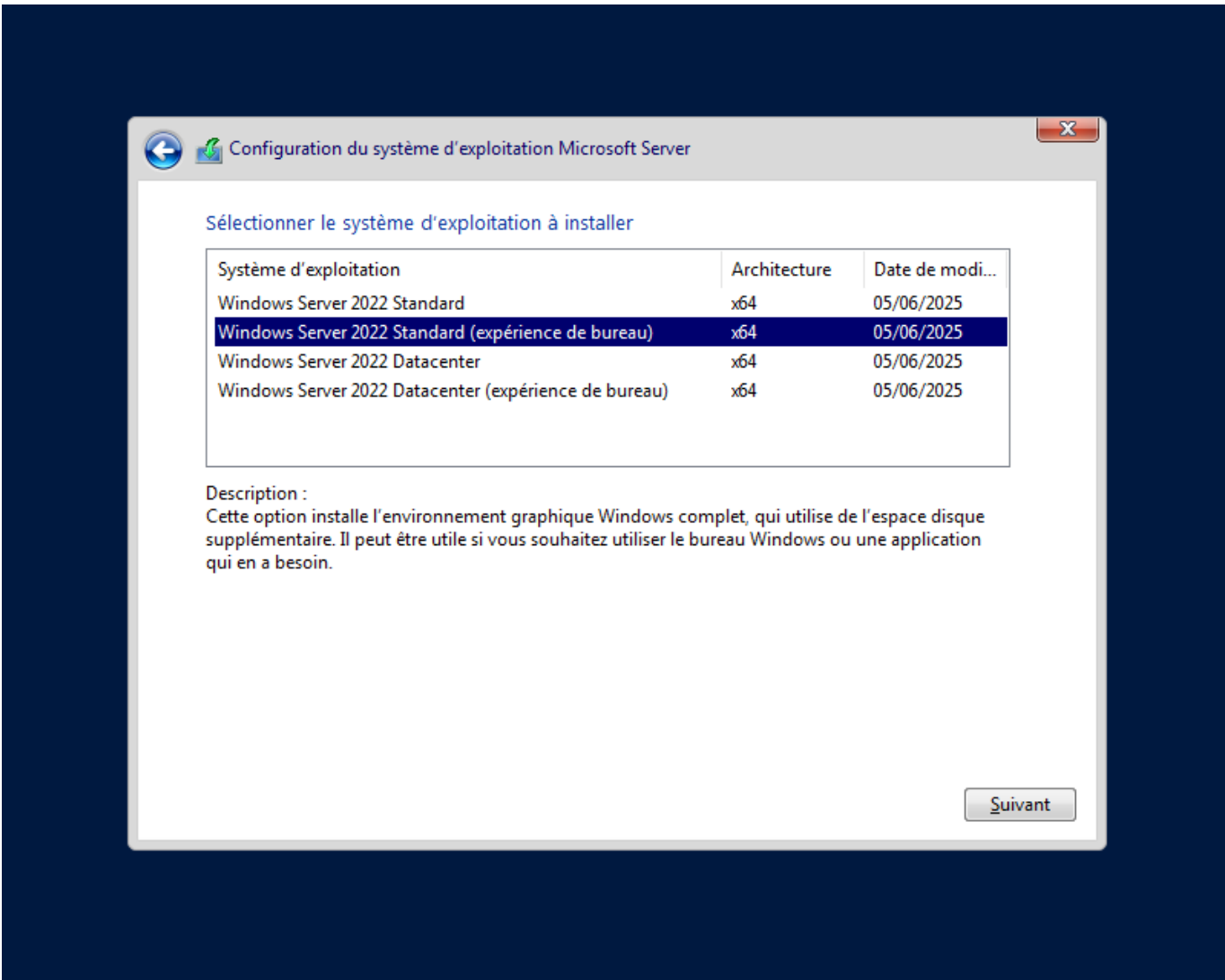
TP Installation Windows server & AD

Configurer un contrôleur de domaine avec Windows Server 2022

Je vais installer un contrôleur de domaine Active Directory sous Windows Server 2022. Ce serveur gère les connexions (authentification) des utilisateurs et ordinateurs. Il synchronise aussi les informations (réplication) entre les contrôleurs pour assurer la disponibilité et la tolérance aux pannes

Avant de commencer, je vérifie que j'ai :

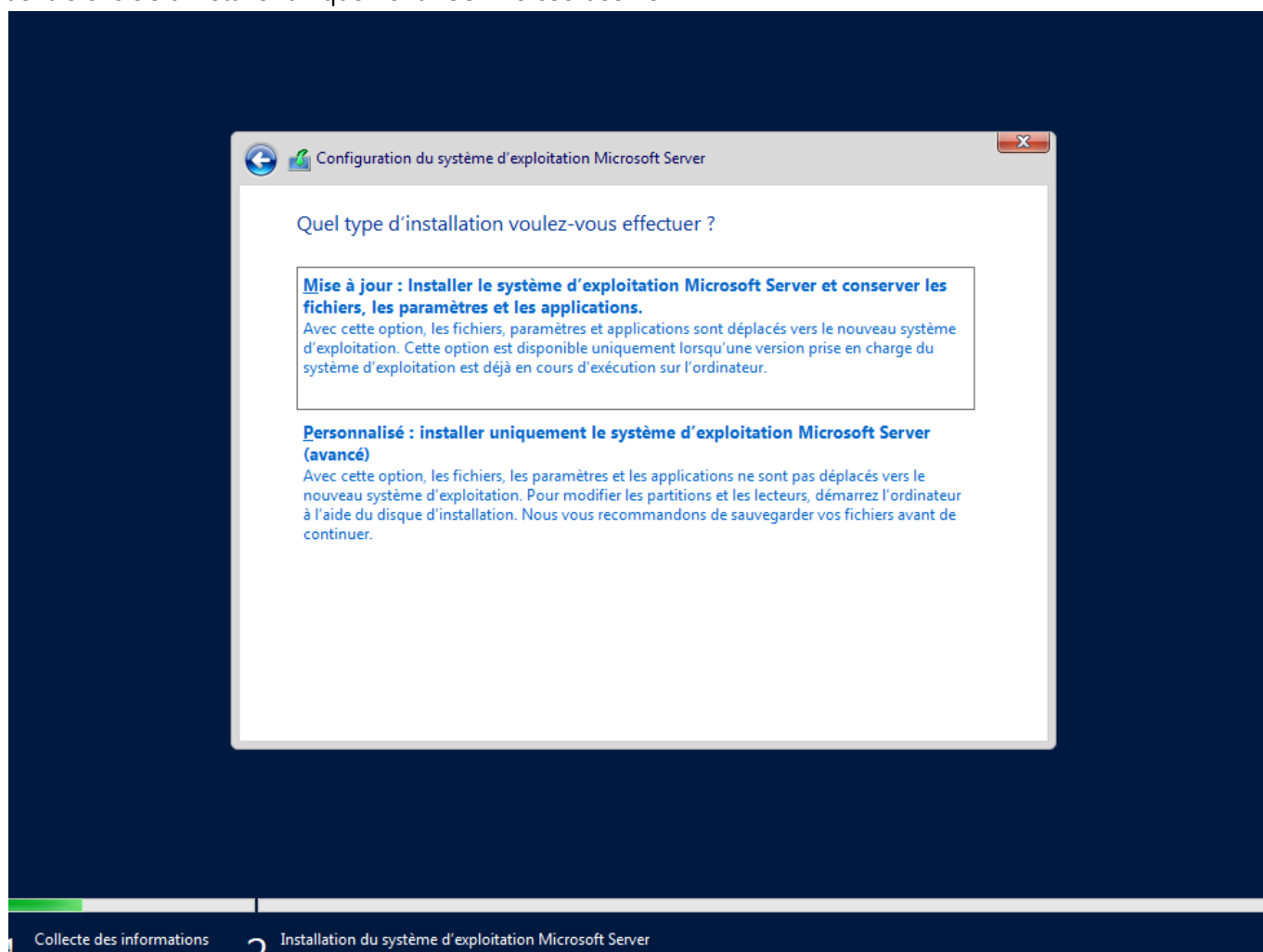
- Un serveur Windows Server 2022 à jour. Je lance l'installation sur ma VM, je me laisse guider par l'interface graphique. Je fais notamment attention à installer la version standard (expérience de bureau)



Édition / Type	Avec interface (GUI)	Sans interface (Core)	Nombre de VM Hyper-V	Fonctionnalités avancées (virtualisation, SDN, etc.)
-------------------	-------------------------	-----------------------------	-------------------------	---

Édition / Type	Avec interface (GUI)	Sans interface (Core)	Nombre de VM Hyper-V	Fonctionnalités avancées (virtualisation, SDN, etc.)
Standard	Standard Expérience de bureau	Standard	2 VM	Non
Datacenter	Datacenter Expérience de bureau	Datacenter	Illimité	Oui

Je fais choisie d'installer uniquement l'OS Microsoft server



Je configure le .compte admin

Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

Nom d'utilisateur

Administrateur

Mot de passe

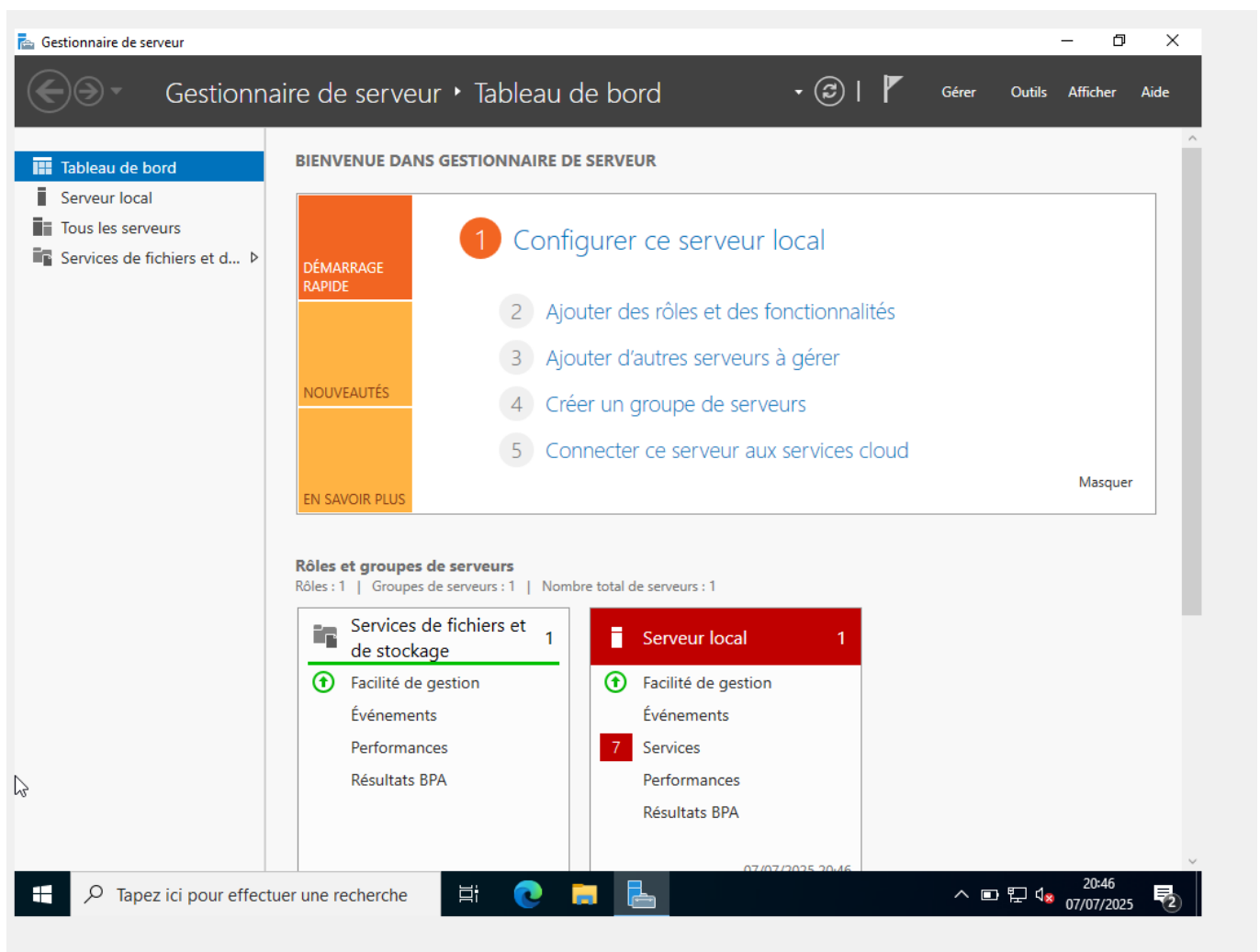
••••••••

Entrez de nouveau le mot de passe

••••••••



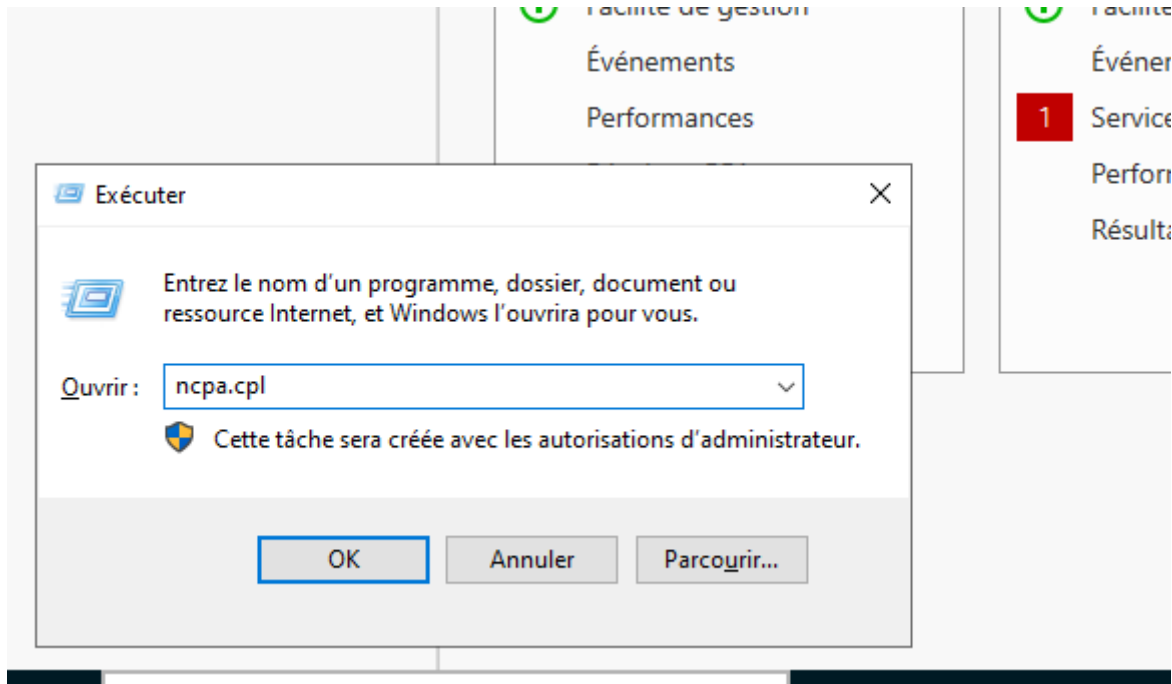
Maintenant que l'installation s'est terminée je passe à l'installation du AD DS.



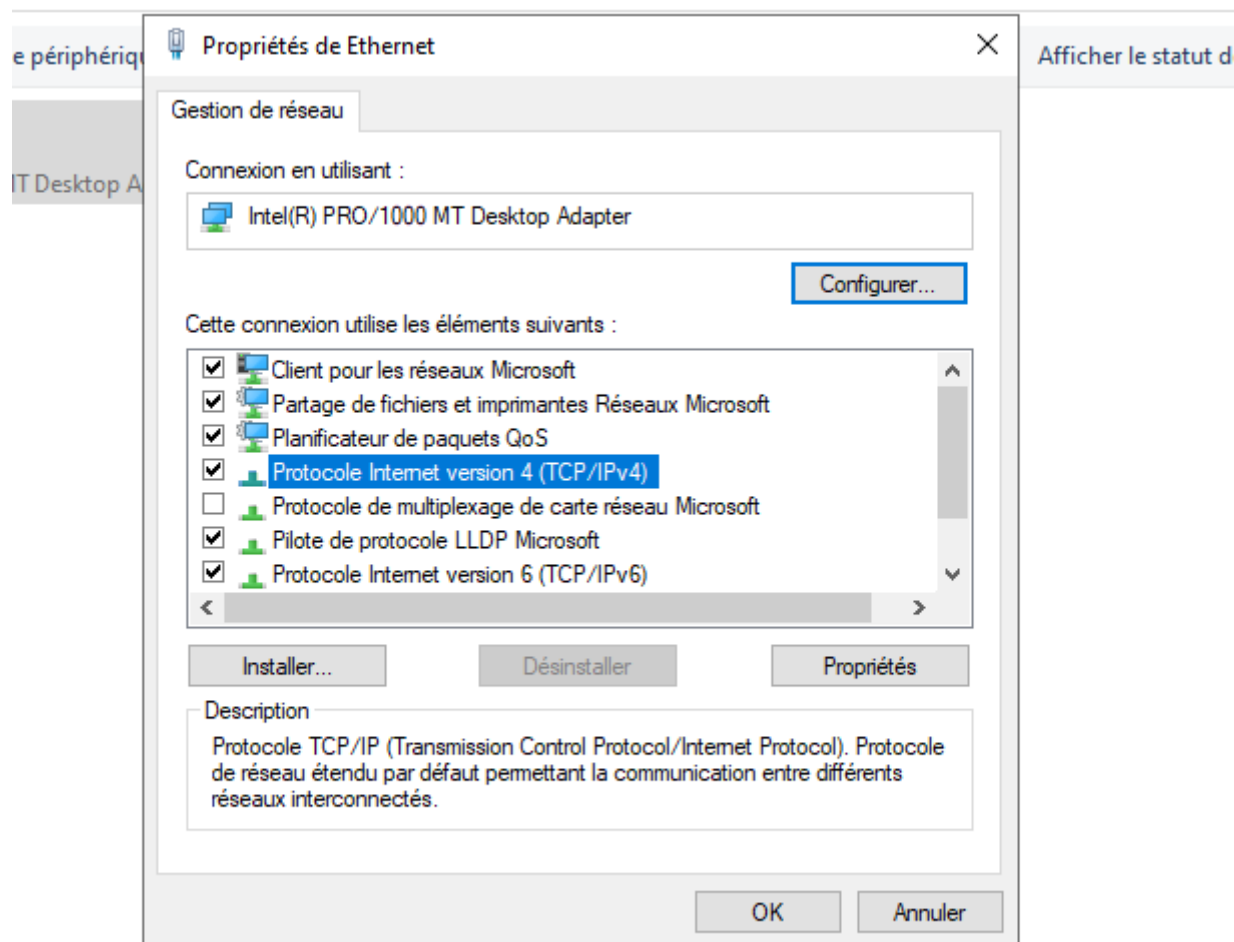
Installation du rôle Active Directory Domain Services

Configuration réseau

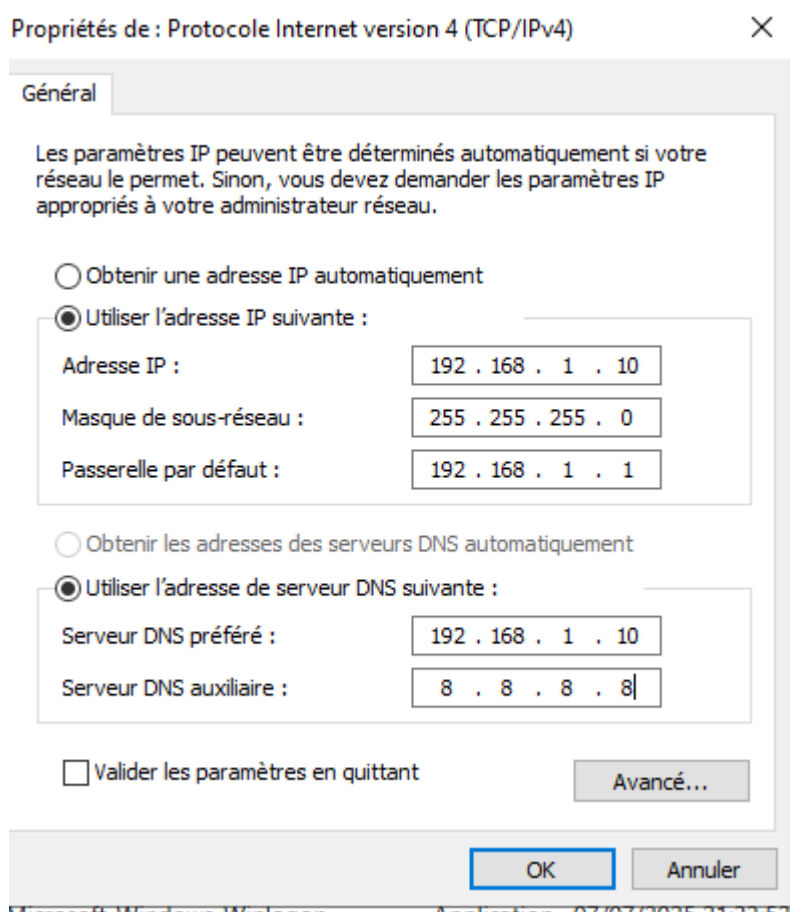
Je vais dans Paramètres > Réseau et Internet > Ethernet, je sélectionne ma carte réseau ou windows + r = ncpa.cpl



Puis dans Paramètres IPv4, je clique sur Modifier.



J'entre mon IP fixe, le masque, la passerelle et comme DNS : il est nécessaire de mettre son adresse de loopback afin de se joindre lui-même et de se fier à sa propre résolution puisque ce serveur sera délégué en tant que serveur de noms de domaine (DNS Server). Je peux aussi utiliser la commande `control.exe netconnections` pour modifier la carte réseau :



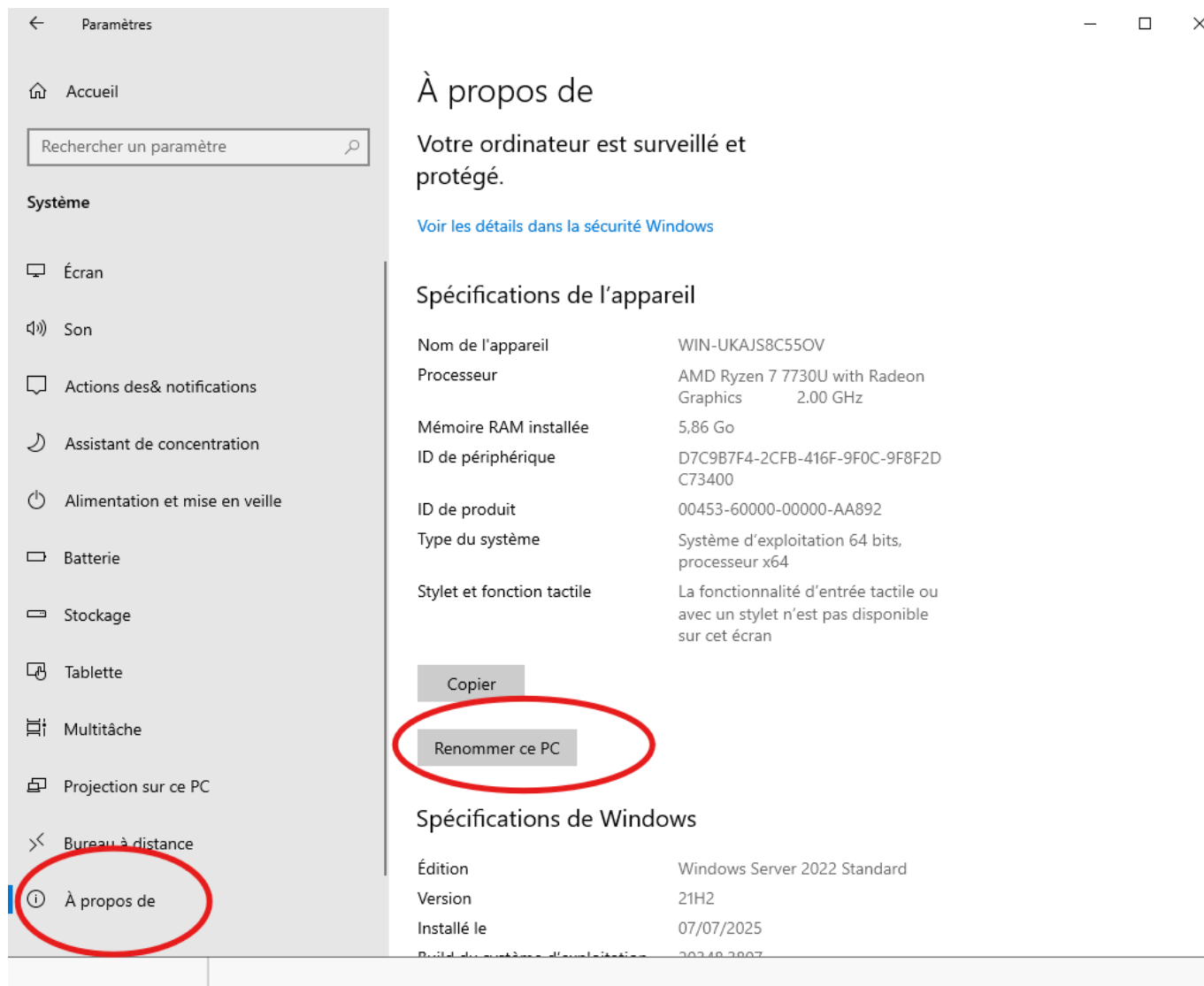
Pour résumer, les informations à renseigner sont :

- Adresse IP de la machine : 192.168.1.10
- Masque de sous réseau : 255.255.255.0
- Passerelle par défaut (accès à d'autres réseaux) : 192.168.1.1
- Serveurs DNS :
 - Adresse de loopback : 192.168.1.10
 - Eventuellement DNS public en auxiliaire 8.8.8.8.

Renommer le serveur

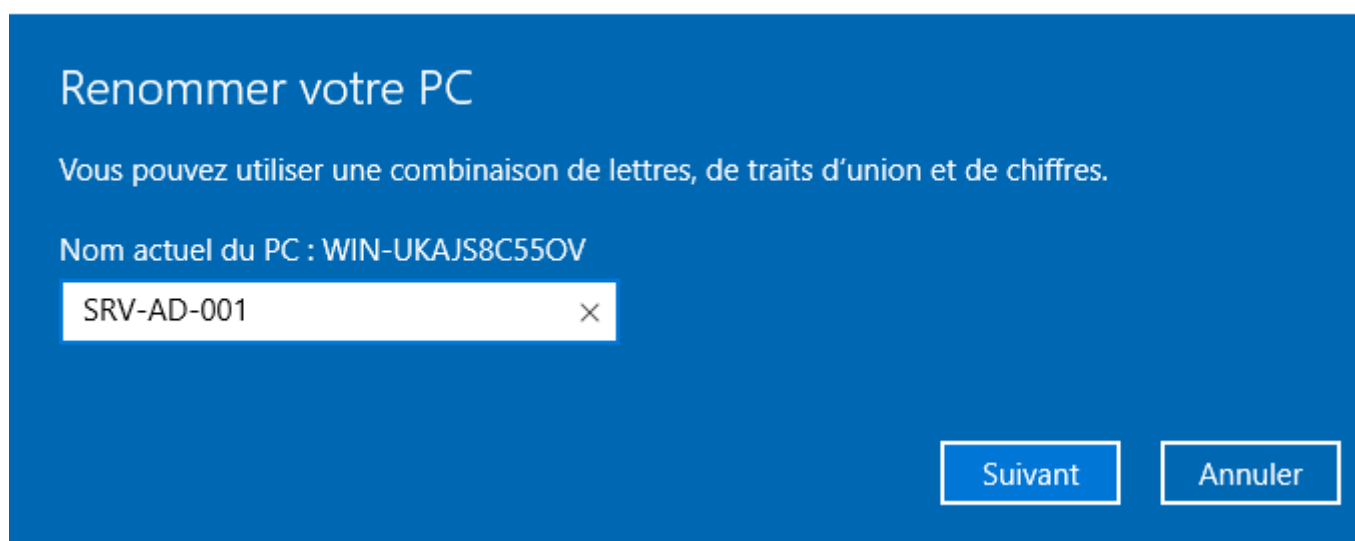
Avant l'installation je dois renommer le serveur de telle sorte à identifier clairement son rôle explicite.

Dans **Paramètres > Système > À propos de**, je clique sur **Renommer le PC**.



Je choisis un nom parlant, comme **SRV-AD-001**, puis je redémarre.

Renommer votre PC



Installer le rôle AD DS

Je me connecte en administrateur, j'ouvre le Gestionnaire de serveur, et je clique sur **Gérer > Ajouter des rôles et fonctionnalités**.

Gestionnaire de serveur > Tableau de bord

Gérer

Outils

Afficher

Aide

Tableau de bord

Serveur local

Tous les serveurs

Services de fichiers et d...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

NOUVEAUTÉS

EN SAVOIR PLUS

1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

5 Connecter ce serveur aux services cloud

Rôles et groupes de serveurs

Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

Services de fichiers et de stockage

1

Facilité de gestion

Événements

Performances

Résultats BPA

Serveur local

1

Facilité de gestion

Événements

Services

Performances

Résultats BPA

Tous les serveurs

1

Facilité de gestion

Événements

Services

Performances

Résultats BPA

Masquer

J'opte pour une installation basée sur un rôle ou une fonctionnalité, je sélectionne mon serveur.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SERVEUR DE DESTINATION
SRV-AD-001

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

☒ **Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

☐ **Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

Performances Services Services

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
SRV-AD-001

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
SRV-AD-001	192.168.10.1	Microsoft Windows Server 2022 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Performances Services Services

Je coche le rôle Services AD DS, j'accepte d'installer les outils associés.

Je passe les écrans suivants et lance l'installation

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
SRV-AD-001

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☐ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Gestion de stratégie de groupe

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS

Centre d'administration Active Directory

Composants logiciels enfichables et outils en ligne de commande AD DS

Services AD DS

[Exporter les paramètres de configuration](#)

[Spécifier un autre chemin d'accès source](#)

< Précédent

Suivant >

Installer

Annuler

Performances

Services

Services

Assistant Configuration des services de domaine Active Directory

Vérification de la configuration requise

SERVEUR CIBLE
SRV-AD-001

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... [Afficher plus](#) ✕

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

⬆ Voir les résultats

connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « beweb.local ». Sinon, aucune action n'est requise.

i Vérification de la configuration requise terminée

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

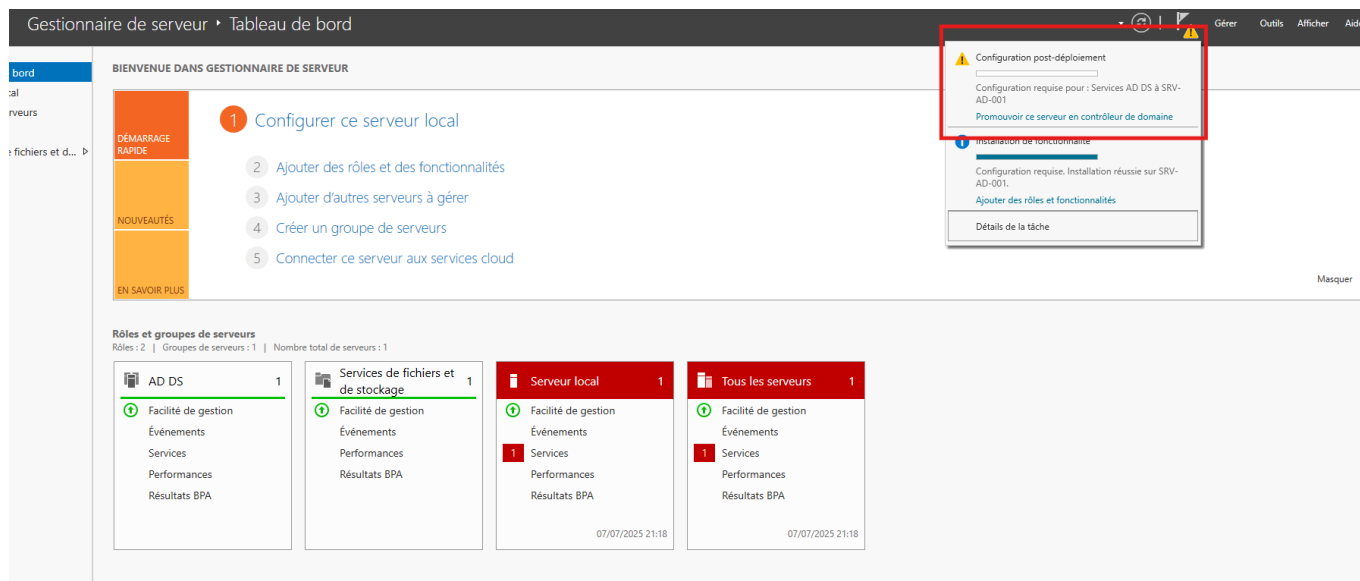
< Précédent

Suivant >

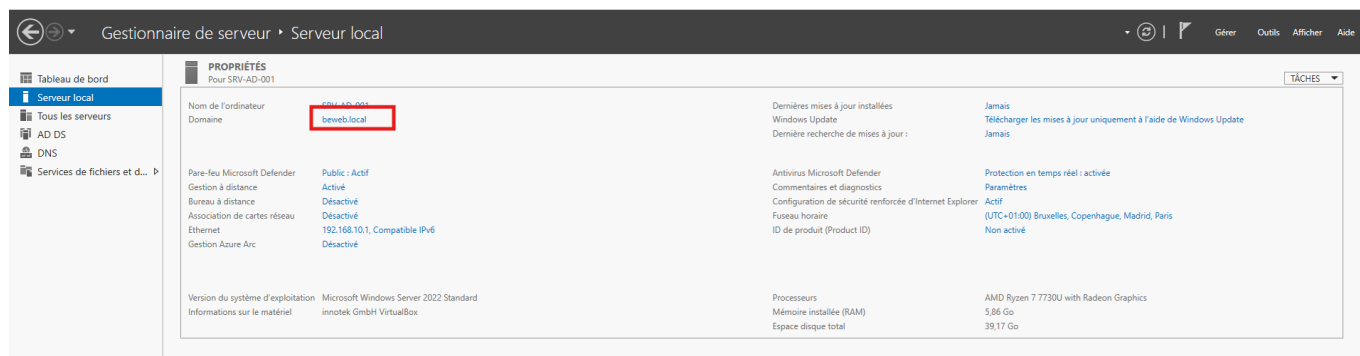
Installer

Annuler

Une fois l'installation finie, j'ai un message pour promouvoir le serveur en contrôleur de domaine : je clique dessus.



Je choisis Ajouter une nouvelle forêt, puis je définis mon domaine (**beweb.local**).



J'utilise un domaine local pour éviter les conflits avec un domaine public.

Ce domaine servira pour les connexions du type **prenom@beweb.local**

Je garde les niveaux de fonctionnement par défaut.

Je choisis un mot de passe robuste pour la restauration (DSRM).

Si l'assistant signale une erreur de délégation DNS, c'est normal car c'est un domaine local : je l'ignore.

Je laisse le nom NetBIOS généré par défaut.

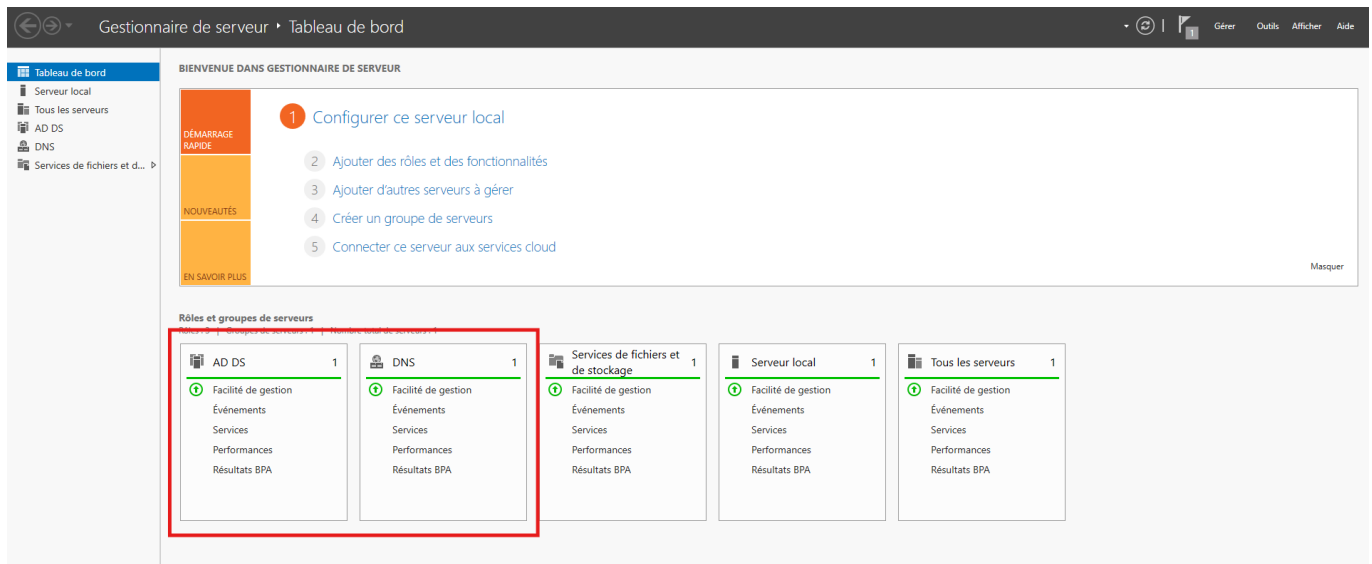
Je conserve les emplacements par défaut pour les dossiers NTDS et SYSVOL.

Je vérifie le résumé et clique sur Installer. Le serveur redémarre automatiquement

Finalisation de l'installation

Je me reconnecte, cette fois-ci avec le compte de domaine (**BEWEB\Administrateur**).

J'ouvre le Gestionnaire de serveur et je vérifie que AD DS et DNS sont bien actifs :



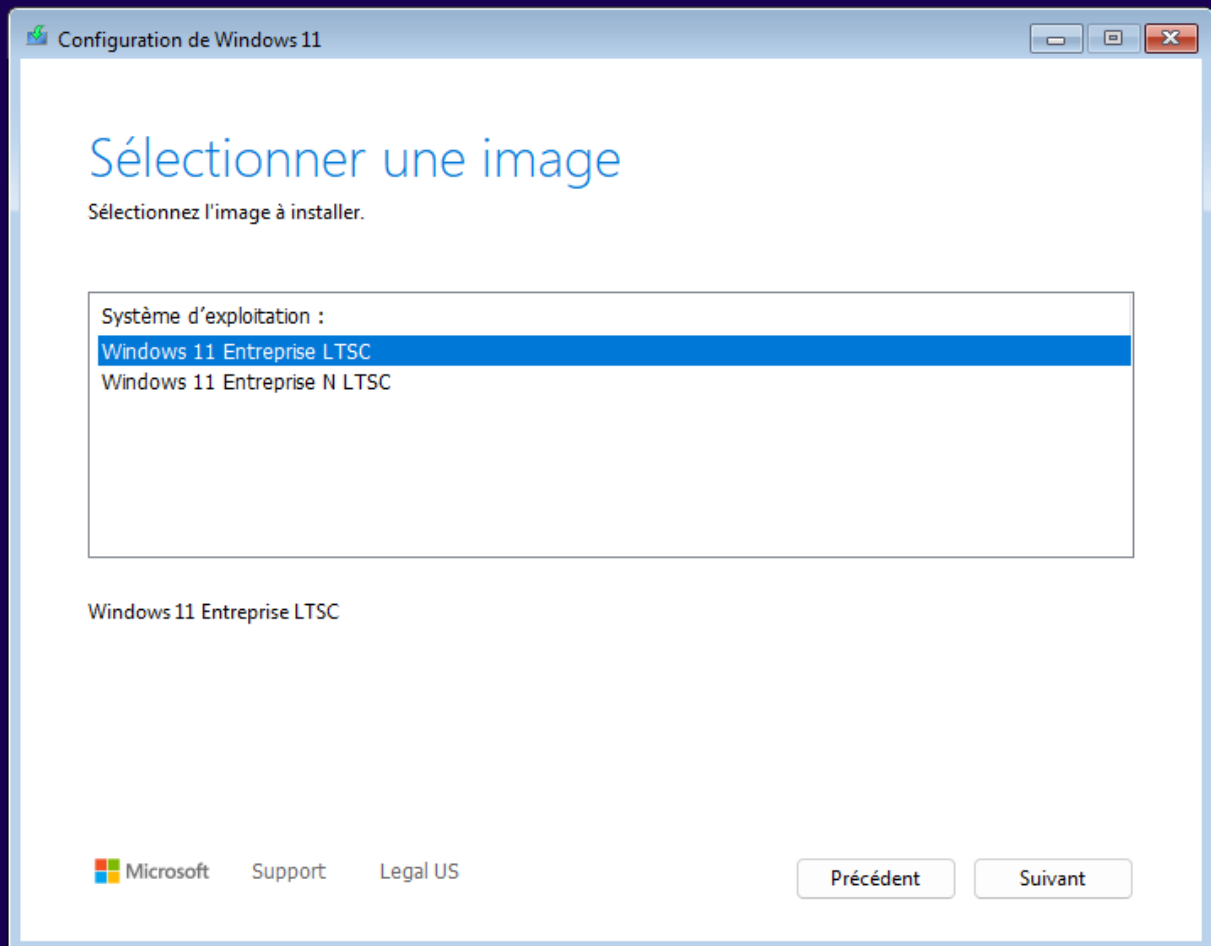
et que je suis connectée au bon domaine



J'ai maintenant mis en place un contrôleur de domaine Active Directory sur Windows Server 2022, en suivant toutes les étapes dans l'ordre. Cette procédure fonctionne aussi avec les versions 2012 à 2019. C'est un processus délicat mais bien balisé.

VM Client :

Je lance l'installation du client windows 11 entreprise, je fais notamment attention à installer la version **LTSC** (précisions sur N LTSC img)



Remarque :

- LTSC = version classique avec tous les outils multimédias inclus.
- N LTSC = version épurée, sans composants multimédias, pour respecter certaines législations.

2. Configurer IP VM

Sur Windows Client :

IP : 192.168.1.101
Masque : 255.255.255.0
Passerelle : 192.168.1.1
DNS : 192.168.1.10 (le serveur AD)

Et je renomme la machine client :

Renommer votre PC

Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.

Nom actuel du PC : DESKTOP-7VFFBQQ

PC-TSSR01



Suivant

Annuler

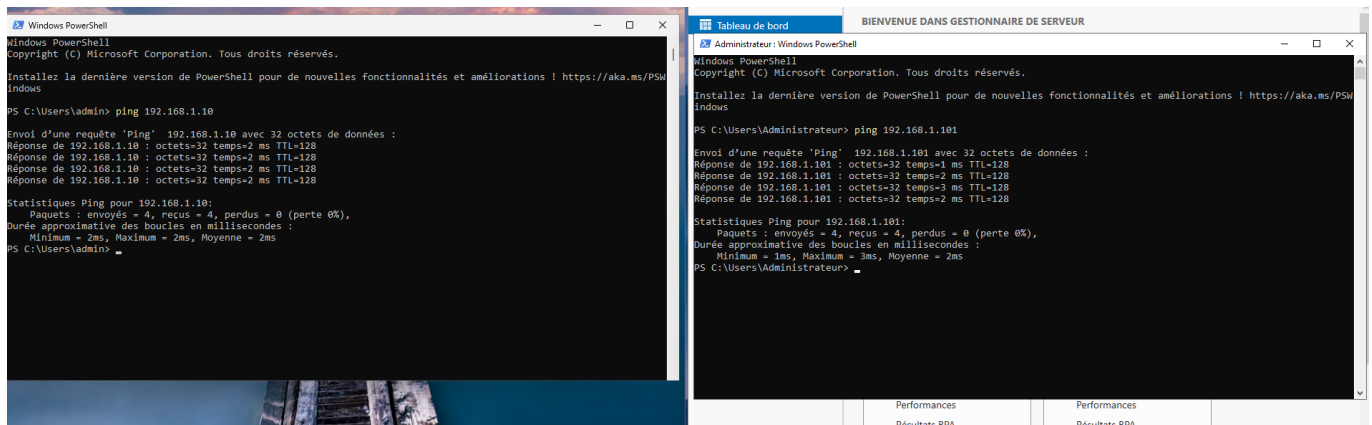
4. Test ping

Sur le Client :

```
ping 192.168.1.10
```

Sur le Server :

```
ping 192.168.1.101
```



Le contrôleur de domaine (SRV-AD-001) est bien fonctionnel (AD + DNS installés).

Le client peut pinguer le serveur AD et inversement.

Je vais rejoindre le domaine en mode GUI.

Je vais dans le **panneau de configuration** → **Système** → **Paramètres système avancés** ou plus simple :

Clic droit sur "Ce PC" → **Propriétés** → **Modifier les paramètres**

Modifier → **Sélectionner "Domaine"** → j'entre le nom du domaine (beweb.local).

← Paramètres

admin

Compte local

Rechercher un paramètre

Système

Bluetooth et appareils

Réseau et Internet

Personnalisation

Applications

Comptes

Heure et langue

Jeux

Accessil Démarrer

Système

Projection sur ce PC

Autorisations, PIN de couplage, détectabilité

Bureau à distance

Utilisateurs du Bureau à distance, autorisations de connexion

Presse-papiers

Historique de Couper et Copier, synchroniser, effacer

Composants système

Gérer les composants système préinstallés sur Windows

Fonctionnalités facultatives

Fonctionnalités supplémentaires pour votre appareil

Informations système

Spécifications de l'appareil, renommer l'ordinateur personnel, spécifications Windows

Rechercher

21:50

07/07/2025

← Paramètres

admin

Compte local

Rechercher un paramètre

Système

Bluetooth et appareils

Réseau et Internet

Personnalisation

Applications

Comptes

Heure et langue

Jeux

Accessibilité

Système > Informations système

Memoire RAM installée

5,84 Go

ID de périphérique

5AE13BB5-2C19-4CE0-9CD7-6334CCED9CBB

ID de produit

00425-00000-00002-AA987

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

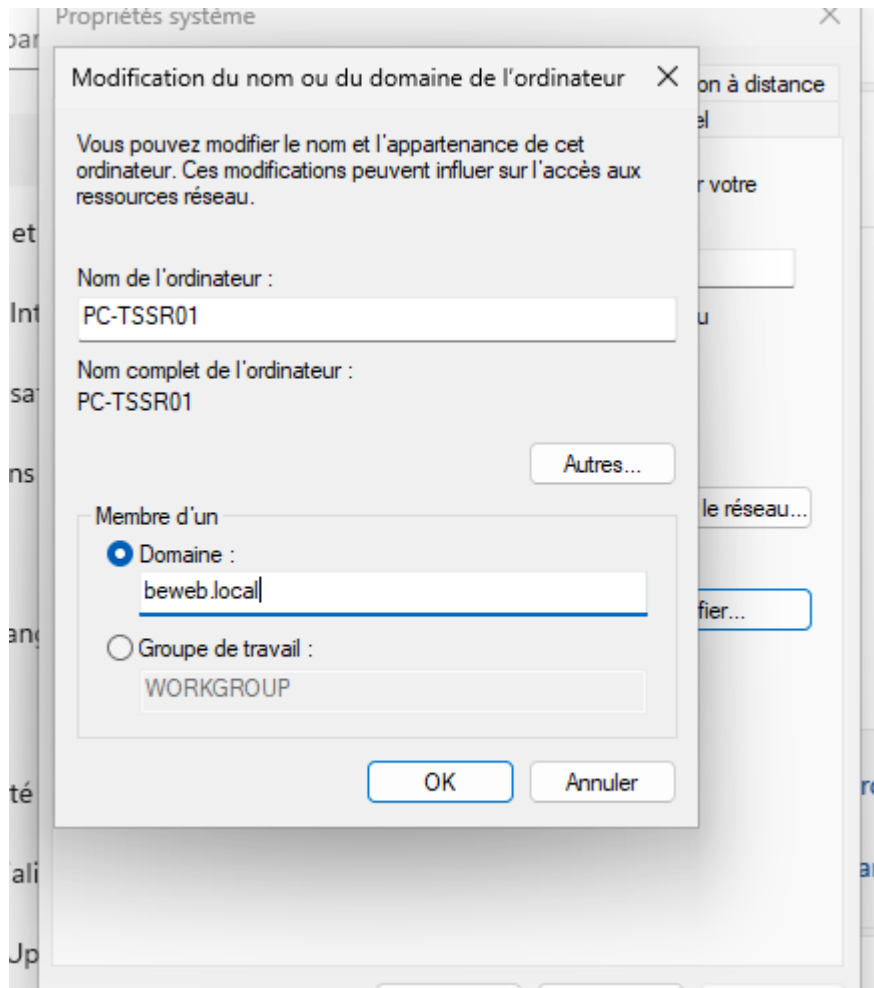
Spécifications de Windows

Copier

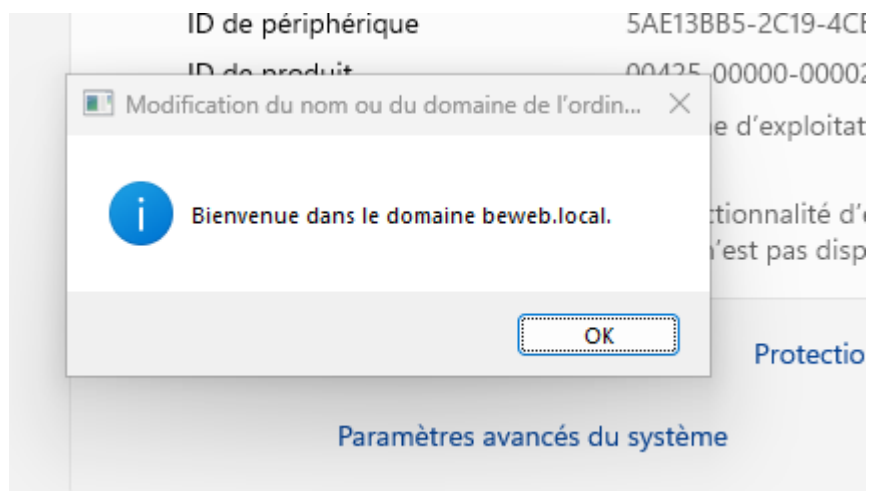
Rechercher

21:51

07/07/2025



J'entre les identifiants d'un compte administrateur du domaine (Administrateur du SRV-AD-001).



Je redémarre le client.

Après le redémarrage je peux me connecter au client avec un compte du domaine :

beweb\Administrateur

Création d'utilisateurs, groupes et dossier partagé

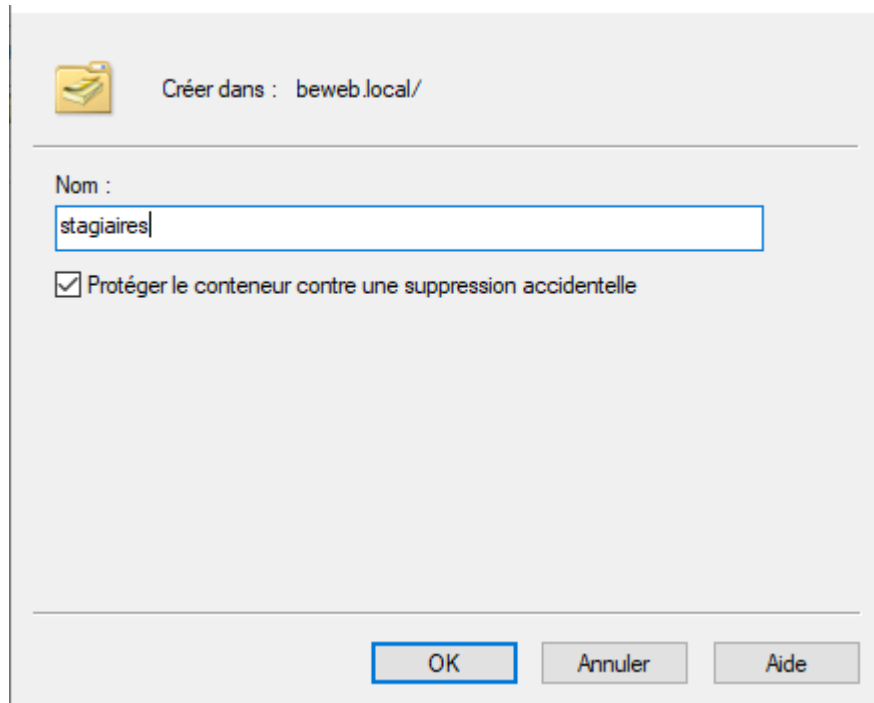
- Je crée une nouvelle unité d'organisation (OU)

Dans la console, je fais :

Clic droit sur **mon domaine** → **Nouveau** → **Unité d'organisation**,

Je nomme cette OU : **Stagiaires**.

Cette OU va me servir à regrouper facilement les comptes des stagiaires.



- Je crée deux comptes utilisateurs dans cette OU

Je fais clic droit sur l'OU **Stagiaires** → **Nouveau** → **Utilisateur**.

Je crée le premier utilisateur :

Nom d'utilisateur : **stagiaire01**

Je décoche l'option "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session" si besoin.

Puis je refais la même chose pour le second utilisateur :


Nom d'utilisateur : **stagiaire02**

Maintenant, mes deux stagiaires sont créés et regroupés dans l'OU Stagiaires.

Utilisateurs et ordinateurs Active	Nom	Type	Description
> Requetes enregistrees	Builtin	builtinDomain	
> beweb.local			

Délégation de contrôle...
Rechercher...
Changer de domaine...
Changer de contrôleur de domaine...
Augmenter le niveau fonctionnel du domaine...
Maîtres d'opérations...
Nouveau
Toutes les tâches
Affichage
Actualiser
Exporter la liste...
Propriétés
Aide

Ordinateur
Contact
Groupe
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur
Dossier partagé

 Créer dans : beweb.local/

Prénom : stagiaire01

Initiales :

Nom :

Nom complet : stagiaire01

Nom d'ouverture de session de l'utilisateur : stagiaire01

@beweb.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : BEWEB\

stagiaire01

< Précédent

Suivant >

Annuler



Créer dans : beweb.local/

Prénom : stagiaire02 Initiales :

Nom :

Nom complet : stagiaire02

Nom d'ouverture de session de l'utilisateur :

stagiaire02 @beweb.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

BEWEB\ stagiaire02

< Précédent

Suivant >

Annuler



Utilisateurs et ordinateurs Active
> Requetes enregistrees
> beweb.local

Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Domain Con...	Unité d'organi...	Default container for do...
ForeignSecu...	Conteneur	Default container for sec...
Managed Sem...	Conteneur	Default container for ma...
stagiaire01	Utilisateur	
stagiaire02	Utilisateur	
Users	Conteneur	Default container for up...

Utilisateurs et ordinateurs Active Directory		Nom	Type	Description
>	Requêtes enregistrées			
▼	beweb.local			
>	Builtin			
>	Computers			
>	Domain Controllers			
>	ForeignSecurityPrincipal:			
>	Managed Service Account			
>	Users			
>	stagiaires			
		stagiaire01	Utilisateur	
		stagiaire02	Utilisateur	

- Je crée un groupe AD pour gérer leurs droits

Je crée le groupe, toujours dans la console Active Directory, je fais :

Clic droit sur **OU Stagiaires** → **Nouveau** → **Groupe**.

Je nomme le groupe **G_Stagiaires**.

- Type de groupe : Sécurité
- Étendue : Globale.

Créer dans : beweb.local/

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe

☐ Domaine local
☒ Globale
☐ Universelle

Type de groupe

☒ Sécurité
☐ Distribution

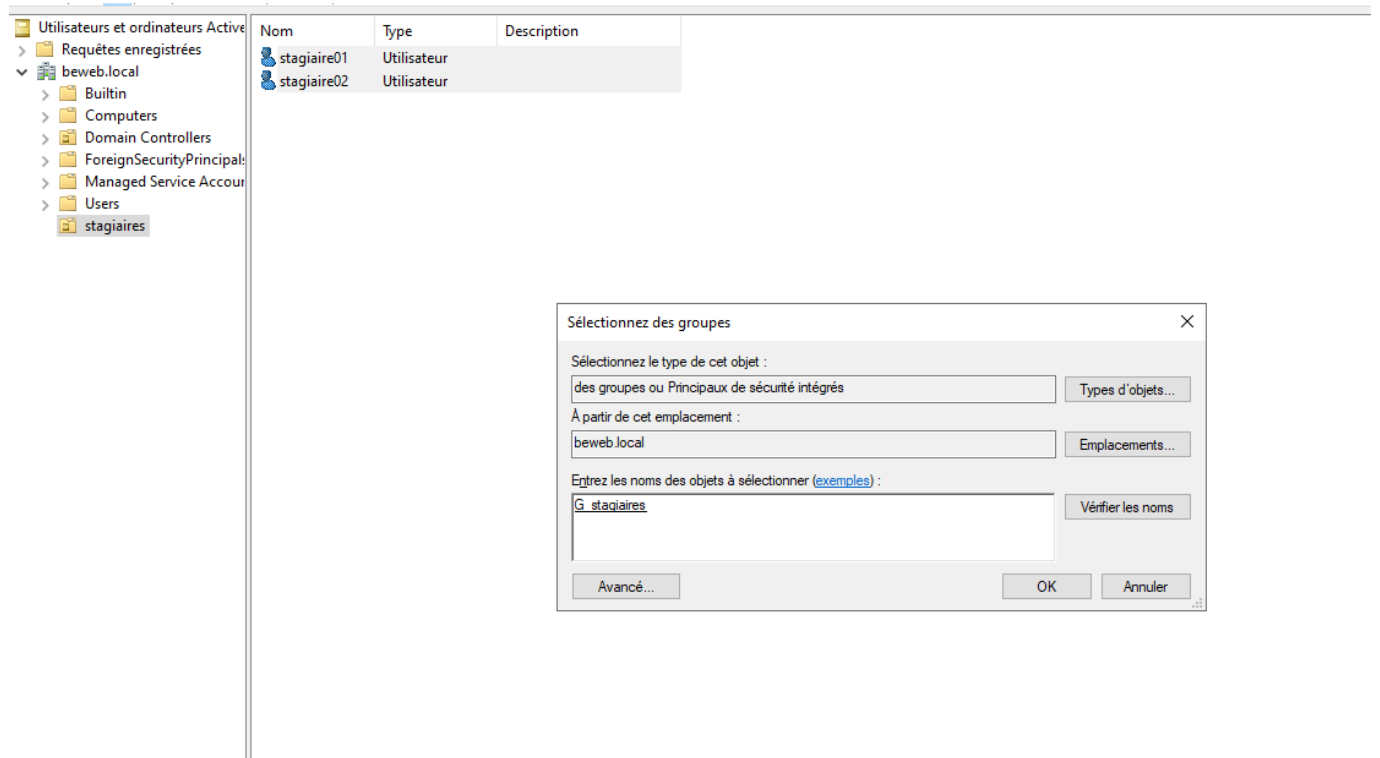
OK Annuler

- J'ajoute les utilisateurs au groupe

Je fais un double clic sur **G_Stagiaires** → **Membres** → **Ajouter...**

Je tape stagiaire01 et stagiaire02, puis je valide.

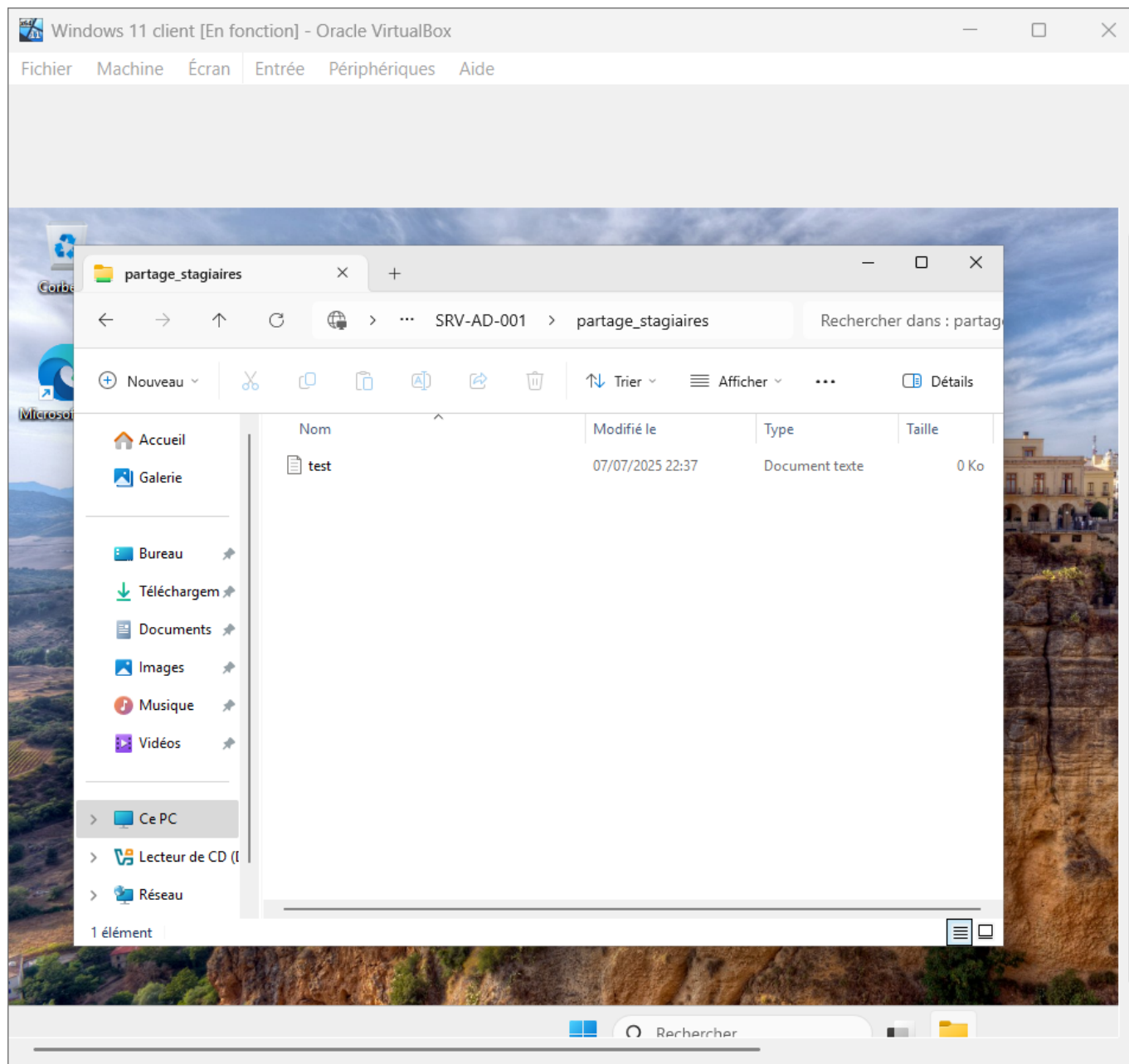
Ainsi, mes deux utilisateurs font désormais partie du groupe **G_Stagiaires**. Cela me permettra de leur attribuer des autorisations plus facilement.



- Je crée un dossier partagé et sécurisé sur le serveur

Sur mon serveur, je crée le dossier qui contiendra les fichiers partagés : Je vais dans le disque **C:**, puis je crée un dossier que je nomme :

C:\Partage_Stagiaires



Je configure le partage réseau, je fais clic droit sur le dossier > Propriétés > Partage > Partage avancé...

Je coche Partager ce dossier.

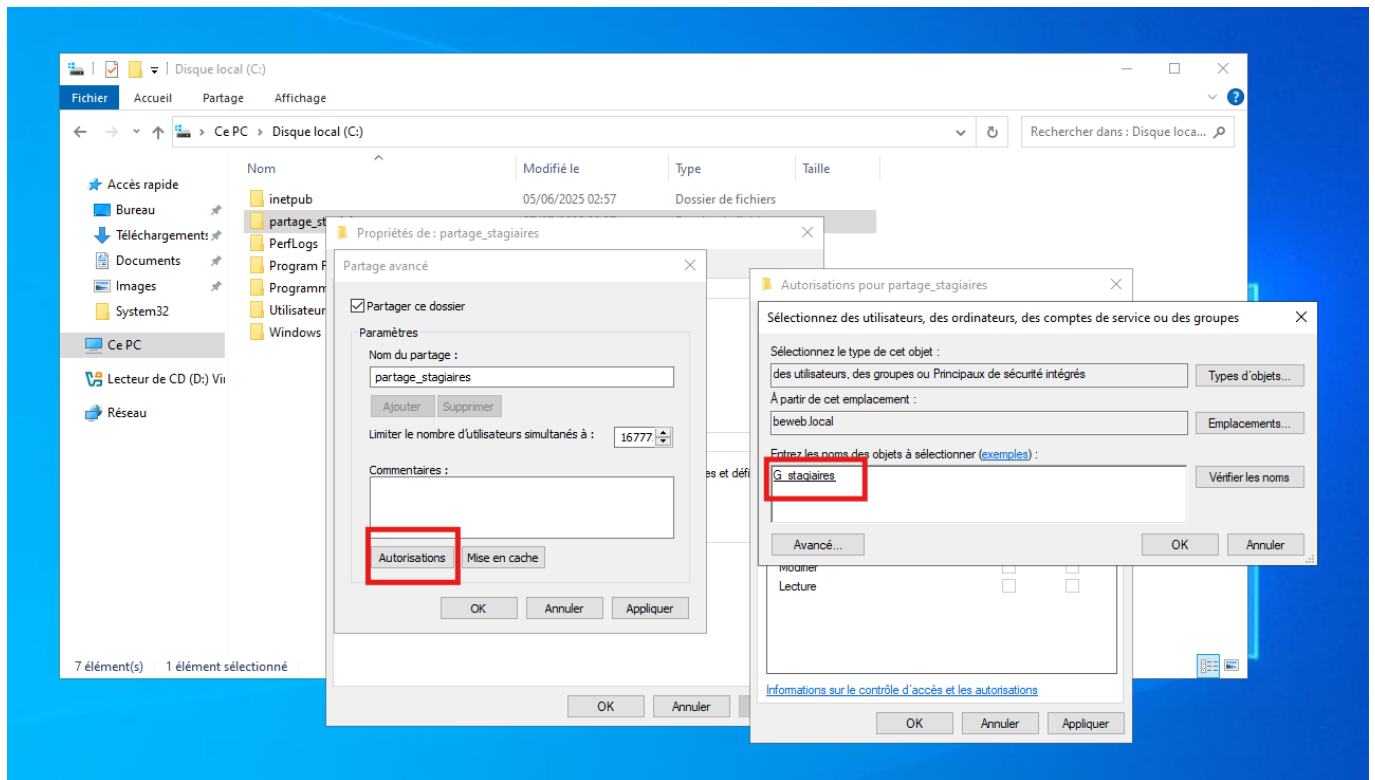
Je donne comme nom de partage :

partage_stagiaires

Puis je clique sur Autorisations.

Je supprime Tout le monde.

J'ajoute le groupe G_Stagiaires, à qui je donne Contrôle total.



- Je configure les permissions NTFS

Je vais ensuite dans l'onglet Sécurité.

Je clique sur Modifier...

Je supprime également Tout le monde si présent.

J'ajoute le groupe G_Stagiaires, et je lui donne les droits Lecture / écriture (Contrôle total facultatif selon le besoin).

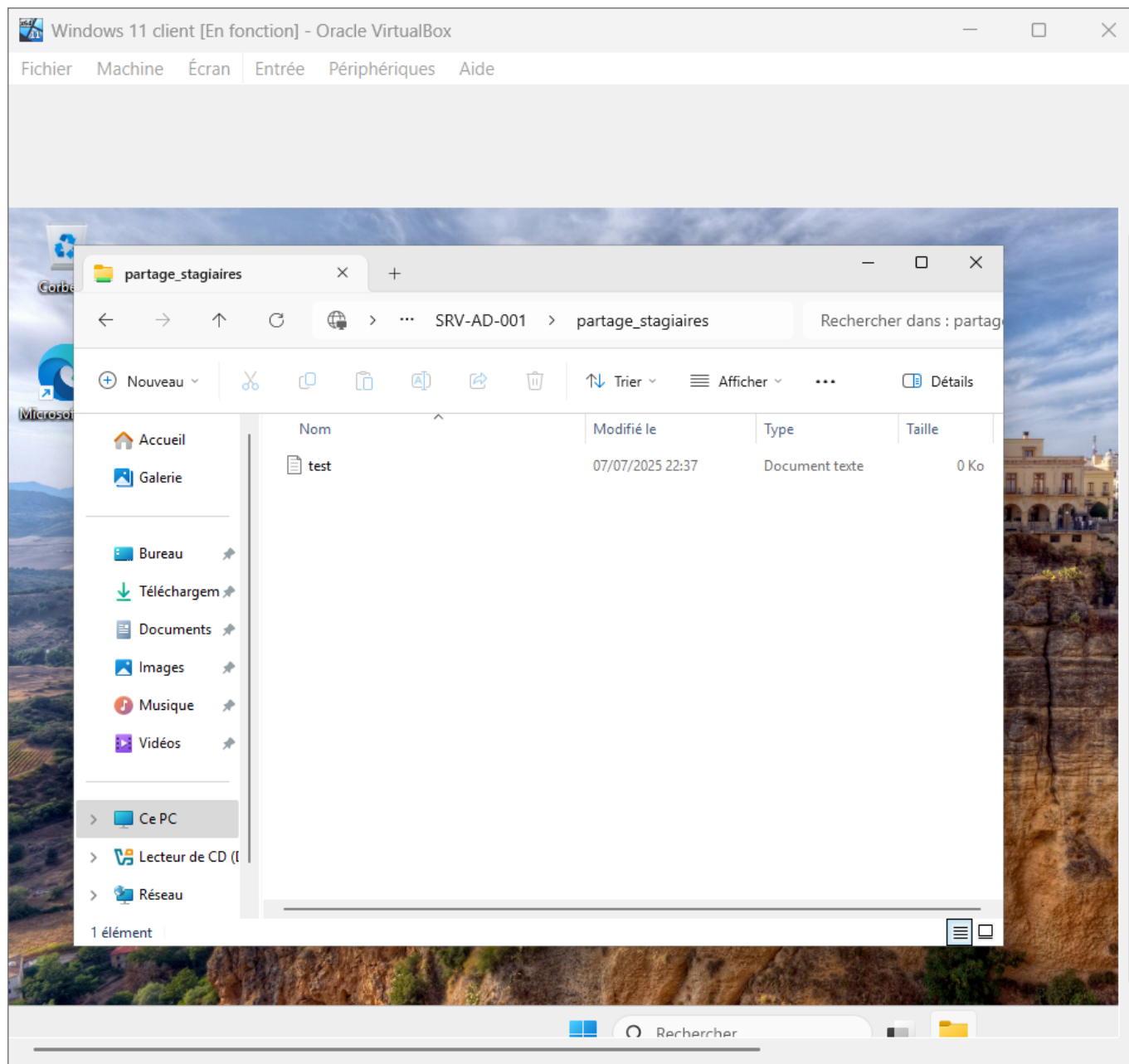
Maintenant, seuls les membres du groupe G_Stagiaires peuvent accéder à ce dossier partagé et y modifier des fichiers.

- Je teste le partage depuis un poste client

Sur un poste client Windows, je vérifie que tout fonctionne :

J'appuie sur Win + R, et je tape l'adresse réseau suivante (adaptée à mon serveur) :

\\SRV-AD-001\\partage_stagiaires



GPO ciblées sur un utilisateur

Dans cette partie, je vais apprendre à créer des stratégies de groupe (GPO) qui ne s'appliqueront qu'à un seul utilisateur précis. Pour cela, j'ai deux méthodes possibles :

- soit je passe par une Unité Organisationnelle (OU) dédiée,
- soit j'utilise le filtrage de sécurité directement sur la GPO.

Voici comment je procède dans les deux cas.

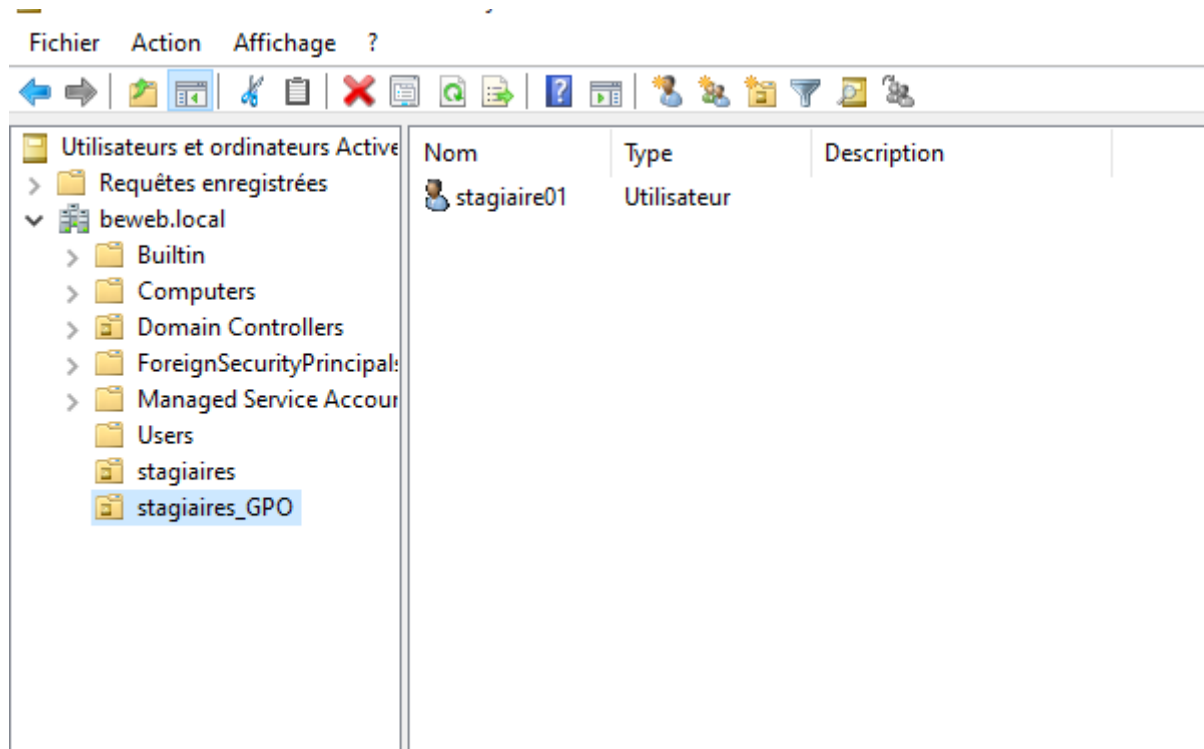
Option 1 : Créer une OU dédiée et y affecter la GPO

Je commence par créer une Unité Organisationnelle (OU) spécifique pour bien isoler l'utilisateur concerné.

→ Dans la console Utilisateurs et ordinateurs Active Directory, je crée une nouvelle OU que je nomme Stagiaires_GPO.

Je déplace ensuite l'utilisateur stagiaire dans cette OU.

→ Je sélectionne l'utilisateur stagiaire01, puis je le déplace dans l'OU Stagiaires_GPO pour que la GPO ne s'applique qu'à lui.

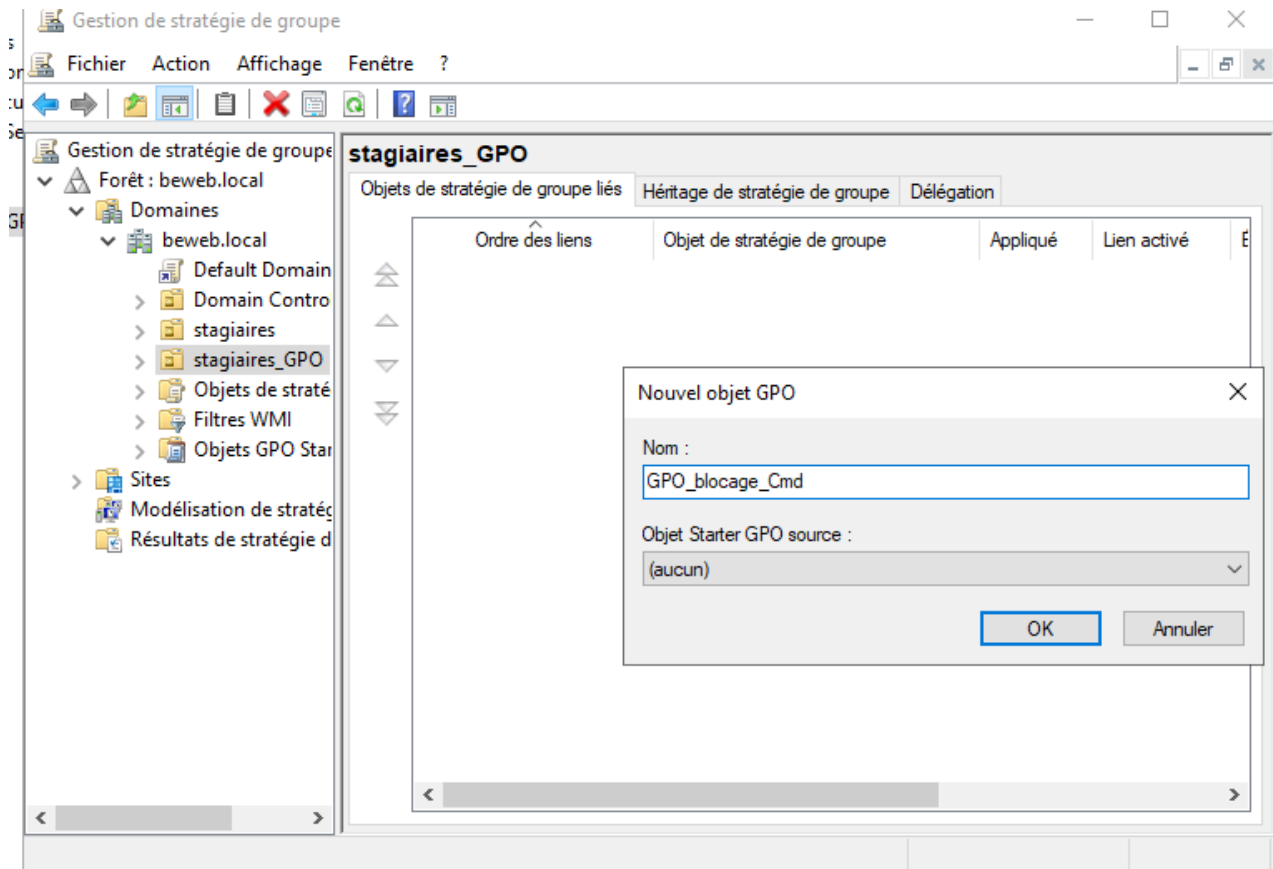


Dans la console de gestion des stratégies de groupe (GPMC - gpmc.msc), je crée la GPO.

→ Je crée une nouvelle GPO que je nomme : GPO_Blocage_Cmd.

Je lie cette GPO à l'OU Stagiaires_GPO.

→ Ainsi, seuls les utilisateurs présents dans cette OU, comme stagiaire01, seront concernés par les paramètres que je vais configurer dans cette GPO. Je vais dans configuration utilisateur, stratégies, modèles d'administration, système : désactiver l'accès à l'invite de commandes.



Option 2 : Utiliser le filtrage de sécurité pour cibler l'utilisateur

Si je ne souhaite pas déplacer l'utilisateur dans une OU spécifique, je peux appliquer la GPO à un conteneur plus large (comme tout le domaine ou une grande OU), et limiter son application grâce aux paramètres de sécurité. Voici comment je procède :

J'ouvre la GPO concernée dans GPMC et je vais dans l'onglet "Délégation".

Je retire le groupe "Authenticated Users".

→ Par défaut, toutes les personnes authentifiées héritent des GPO. Pour cibler seulement stagiaire01, je supprime ce groupe.

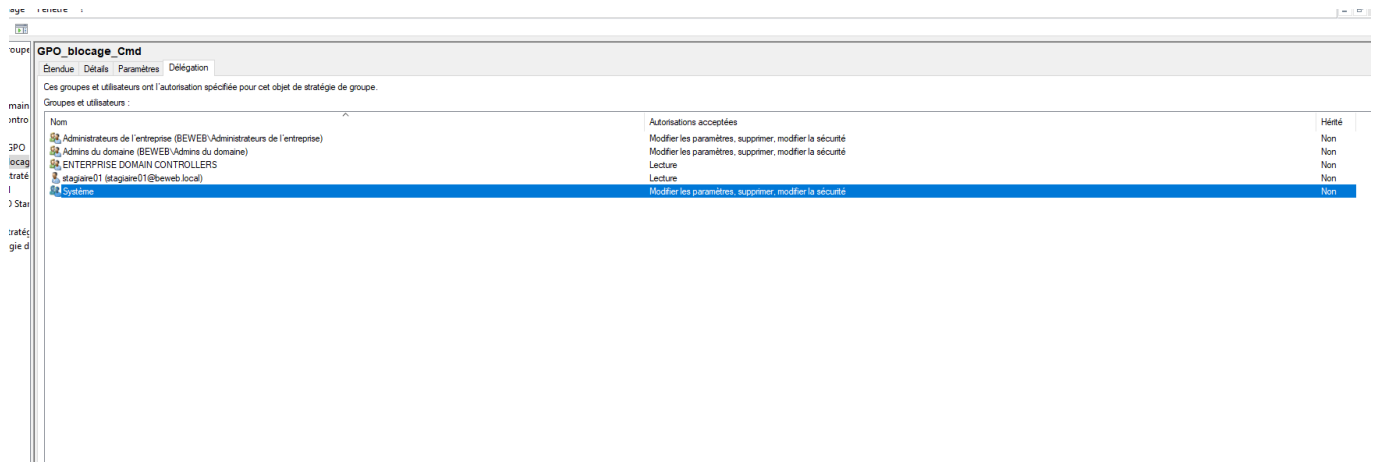
J'ajoute l'utilisateur stagiaire01 dans la liste.

→ Dans l'onglet Délégation, je clique sur Ajouter, je choisis l'utilisateur stagiaire01, puis je lui accorde le droit Lecture.

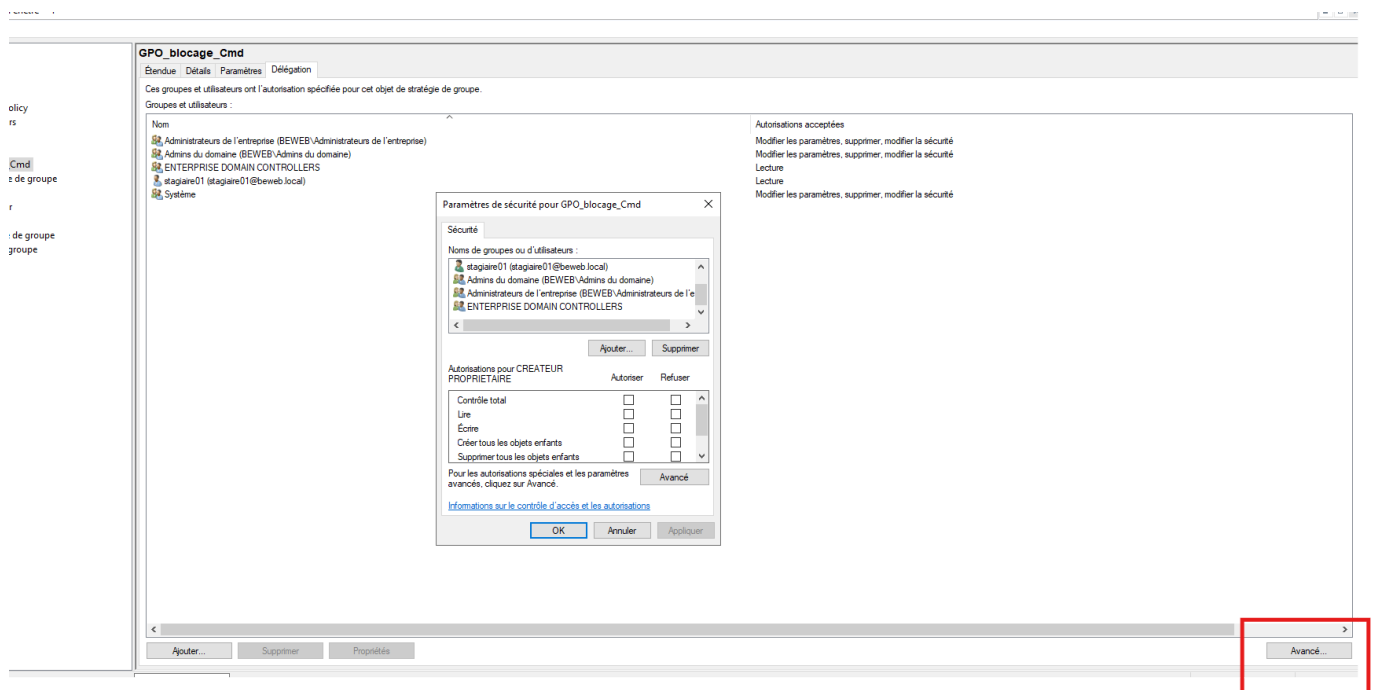
J'ouvre la console GPMC (gpmc.msc).

Je sélectionne ma GPO (par exemple : GPO_Blocage_Cmd).

Dans le volet de droite, je clique sur l'onglet « Délégation ».



En bas de la fenêtre, je clique sur le bouton "Options avancées..."



→ C'est ce bouton qui ouvre la fenêtre classique de gestion des permissions NTFS, qu'on appelle parfois l'onglet Sécurité.

Dans cette fenêtre des paramètres de sécurité avancés, je vois la liste des utilisateurs et groupes qui ont des droits sur la GPO.

Je vérifie qu'il n'y a pas d'autres groupes comme « Authenticated Users » ou « Domain Users » qui pourraient appliquer la GPO.

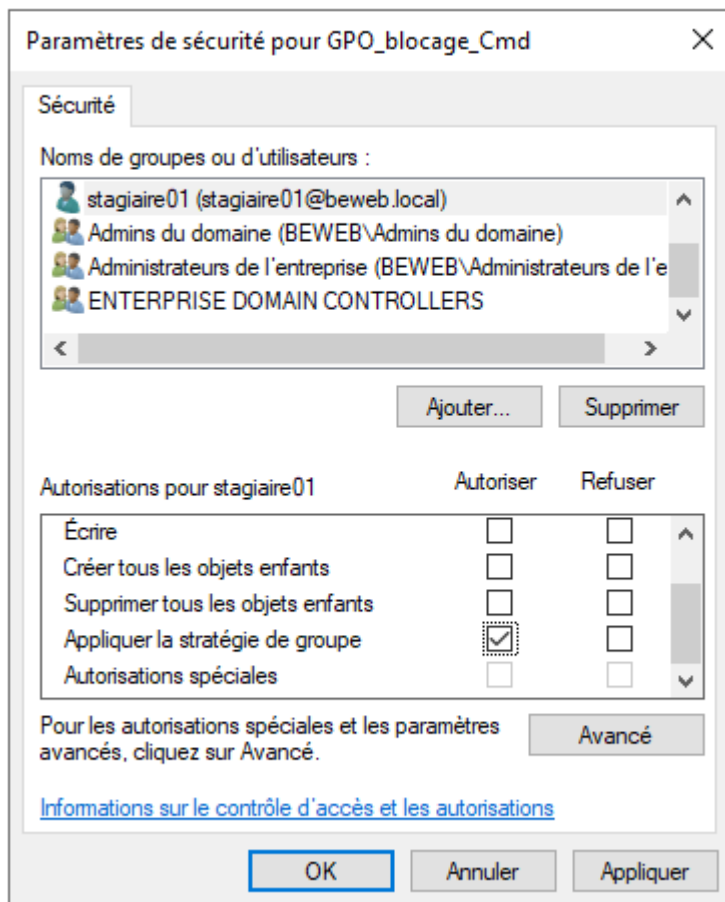
→ Si c'est le cas, je peux les supprimer pour restreindre la portée.

J'ajoute stagiaire01 s'il n'y est pas encore.

→ Je clique sur « Ajouter », je cherche stagiaire01, puis je valide.

Je sélectionne stagiaire01, puis je coche ces deux autorisations :

- Lecture
- Appliquer la stratégie de groupe



Si l'une de ces cases est décochée, la GPO ne s'appliquera pas correctement.

Je valide en cliquant sur OK.

Ensuite, je configure les différents paramètres que je souhaite imposer à cet utilisateur.

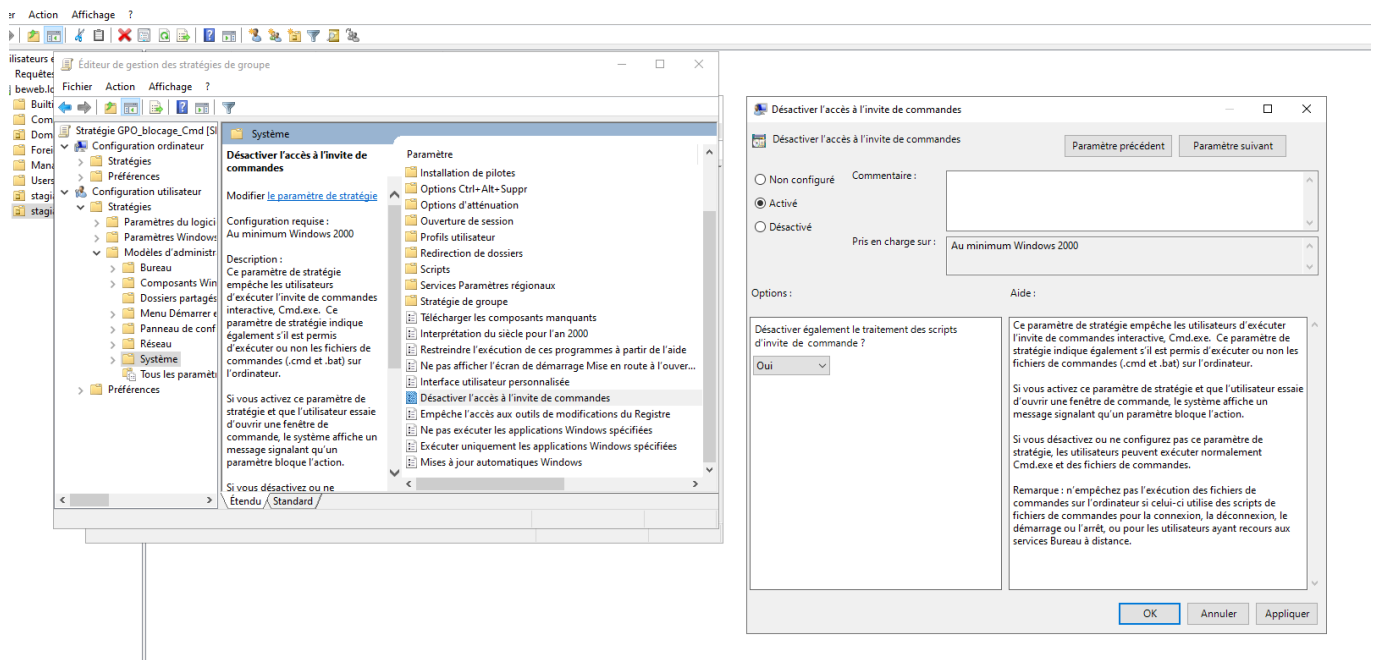
GPO 1 – Bloquer l'accès à l'invite de commandes (cmd)

Je me rends dans :

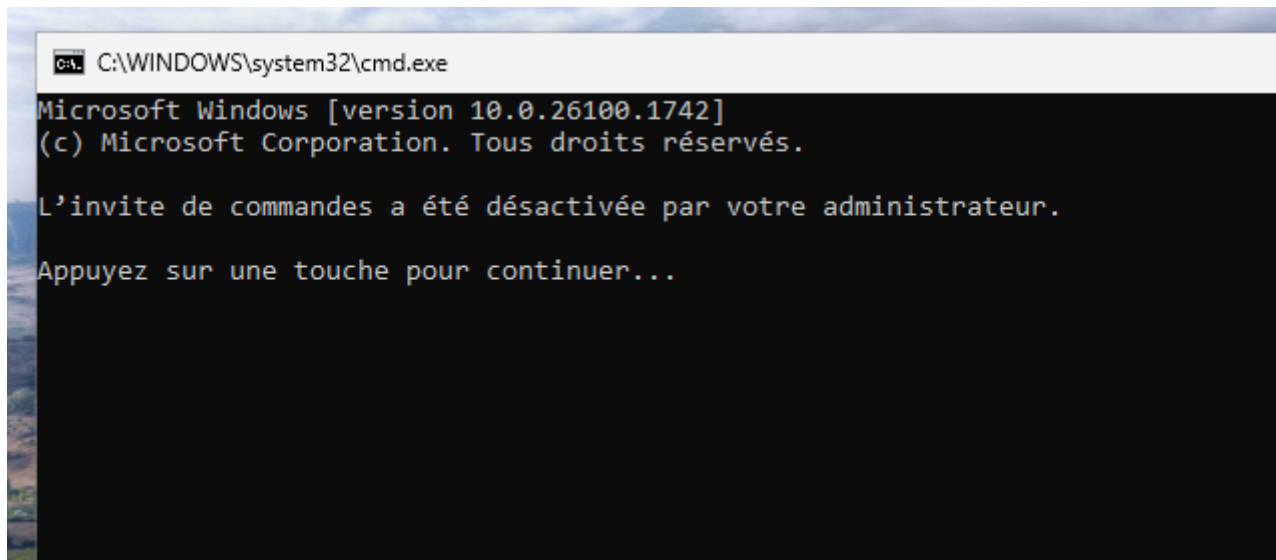
Configuration utilisateur > Modèles d'administration > Système

J'active la stratégie :

"Empêcher l'accès à l'invite de commandes"



Vérification sur la VM client :



GPO 2 – Masquer le Panneau de configuration

Je vais dans :

Configuration utilisateur > Modèles d'administration > Panneau de configuration

J'active la stratégie suivante :

“Interdire l'accès au Panneau de configuration et aux paramètres PC”



J'ouvre l'éditeur de gestion des stratégies de groupe (gpedit.msc pour tester localement, ou via GPMC pour modifier la GPO).

GPO 3 : Interdire accès aux périphériques de stockage amovibles

Je me rends dans la partie Configuration ordinateur (pas dans Configuration utilisateur) :

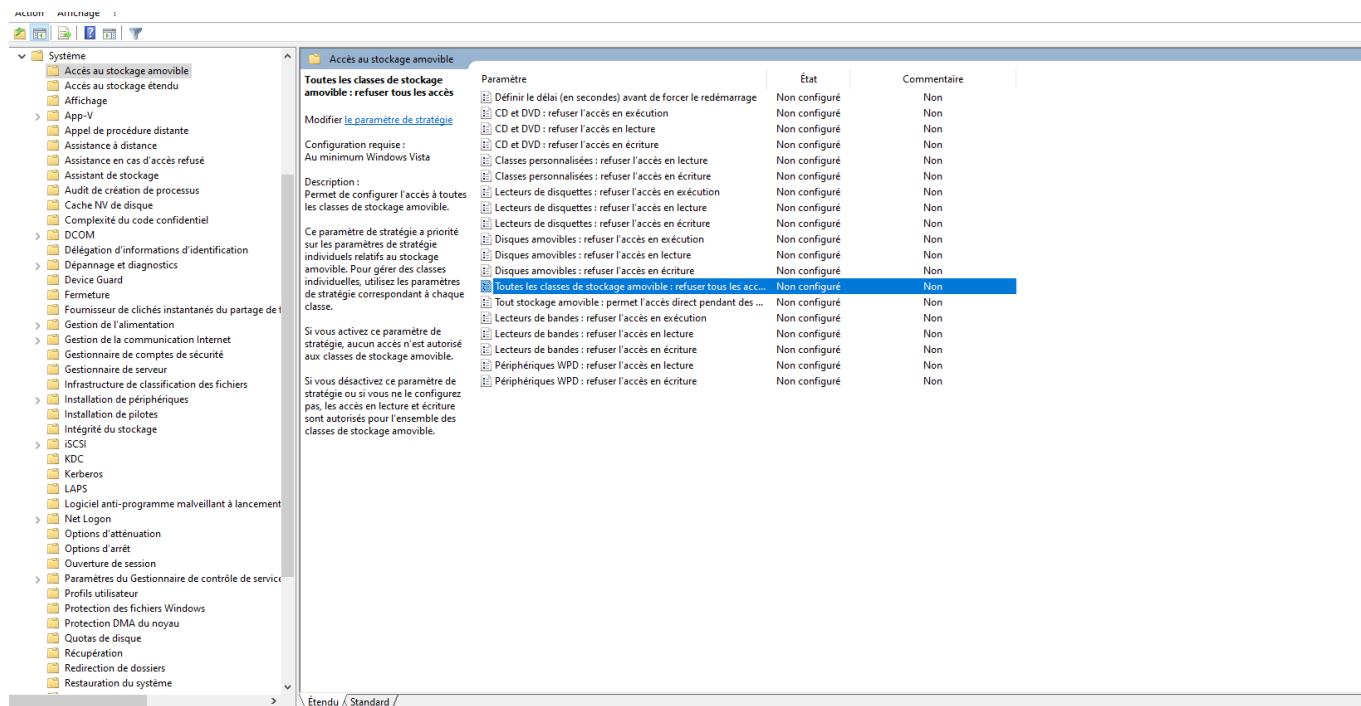
Configuration ordinateur └─ Modèles d'administration └─ Système └─ Accès aux périphériques de stockage amovibles

Dans le dossier "Accès aux périphériques de stockage amovibles", je retrouve plusieurs stratégies, dont celle-ci :

"Tous les types de supports de stockage amovibles : Refuser l'accès"

C'est celle-là que j'active (État : Activé).

Elle bloque l'accès en lecture et écriture à tous les périphériques de stockage amovibles, y compris les clés USB.



GPO 4 – Ajouter un script de connexion

J'ouvre la GPO dans la console GPMC (gpmc.msc), puis je fais clic droit → Modifier.

Je me rends dans cette arborescence :

Configuration utilisateur └─ Paramètres Windows └─ Scripts (ouverture de session/fermeture de session)

Je double-clique sur "Ouverture de session" (ou "Logon" si l'interface est en anglais).

Dans la fenêtre qui s'ouvre, je clique sur "Ajouter..."

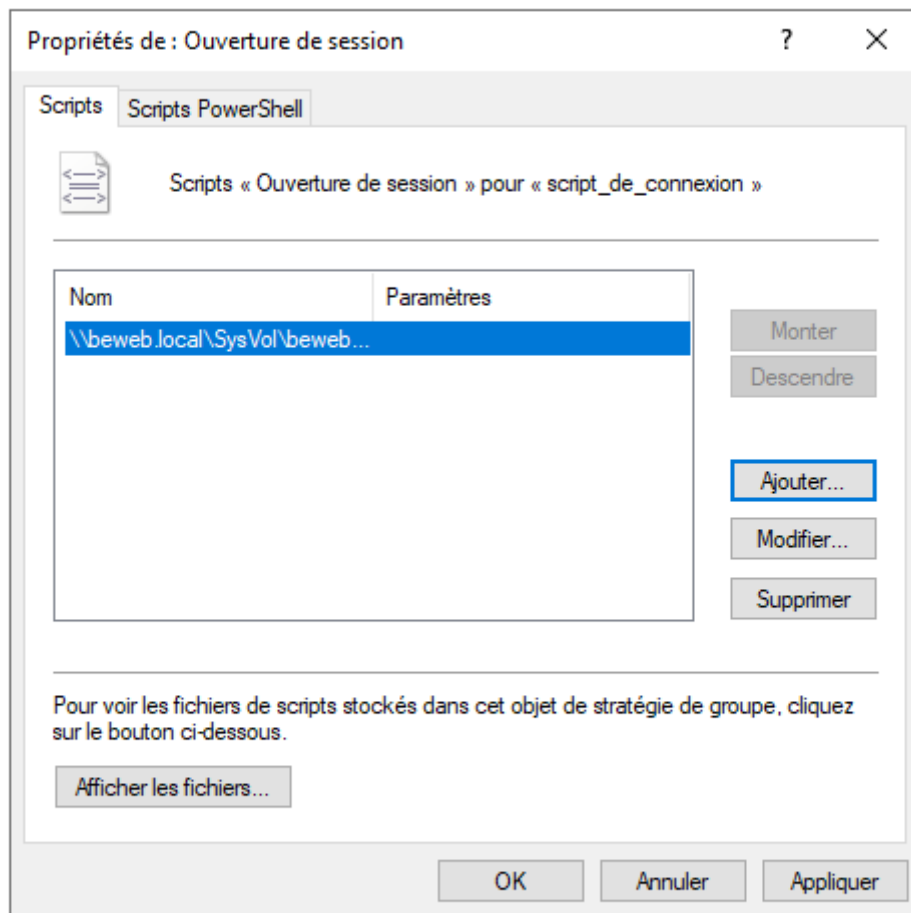
Dans la nouvelle fenêtre, je clique sur "Parcourir..." pour ouvrir le dossier où seront stockés les scripts de la GPO.

→ Par défaut, le chemin est quelque chose comme : \Nom_Domaine\SysVol\Nom_Domaine\Policies{ID-de-la-GPO}\User\Scripts\Logon

J'y dépose mon fichier batch (.bat), par exemple message.bat.

Je sélectionne mon script dans la liste, puis je valide.

: d'ouverture de
teur.



Comment créer un script batch (.bat)

1. J'ouvre le Bloc-notes (Notepad) J'appuie sur Windows + R, je tape notepad, puis j'appuie sur Entrée.
2. J'écris mes commandes batch Voici un exemple simple de script batch pour l'ouverture de session :

```
@echo off echo Bonjour, votre session est en cours de préparation... pause
```

Ce que fait ce script :

- @echo off : évite d'afficher les lignes de commande à l'écran.
- echo : affiche un message à l'écran.
- pause : demande à l'utilisateur d'appuyer sur une touche avant de fermer la fenêtre.

3. J'enregistre le fichier au format .bat

Je clique sur Fichier > Enregistrer sous...

Dans le champ Nom du fichier, j'écris par exemple :

script_logon.bat

Très important : dans Type, je choisis « Tous les fichiers (.) », sinon il s'enregistrera en .txt par erreur.

J'enregistre ce fichier dans un dossier temporaire (C:\Temp, par exemple), ou directement dans le partage SysVol de la GPO si je suis prête.

GPO 5 – Imposer un fond d'écran

1. J'ouvre la GPO dans la console GPMC

Je commence par ouvrir ma GPO dans la console GPMC (gpmc.msc), puis je fais clic droit > Modifier sur ma GPO (par exemple GPO_Blocage_Cmd).

2. Je navigue dans les paramètres de l'utilisateur

Ensuite, je me rends dans l'arborescence suivante :

Configuration utilisateur — Modèles d'administration — Bureau — Active Desktop

Si je ne vois pas ces options, il faut vérifier que les modèles d'administration sont bien chargés, ou que je suis sur une version de Windows compatible.

3. J'active la stratégie de fond d'écran

Dans le dossier Active Desktop, je double-clique sur la stratégie suivante :

« Papier peint du Bureau »

Je sélectionne l'option Activé.

Un champ "Nom du papier peint" apparaît.

4. Je renseigne le chemin du fichier image

Dans ce champ, je tape le chemin réseau complet vers l'image que je souhaite imposer comme fond d'écran. Exemple dans mon cas :

\\SRV-DC01\Stagiaires\fondcran.jpg

Le fichier fond.jpg doit être accessible en lecture pour l'utilisateur stagiaire01.

Je le place au préalable dans un dossier partagé du serveur (SRV-DC01), et je vérifie les permissions.

Je clique sur OK pour enregistrer la stratégie.

Papier peint du Bureau

Papier peint du Bureau

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé

Pris en charge sur : Au minimum Windows 2000

Options :

Nom du papier peint :

C:\Windows\Web\Wallpaper\fondecna.

Exemple : avec un chemin local :
C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC :
\\Server\Share\Corp.jpg

Style du papier peint : Ajuster

Aide :

Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

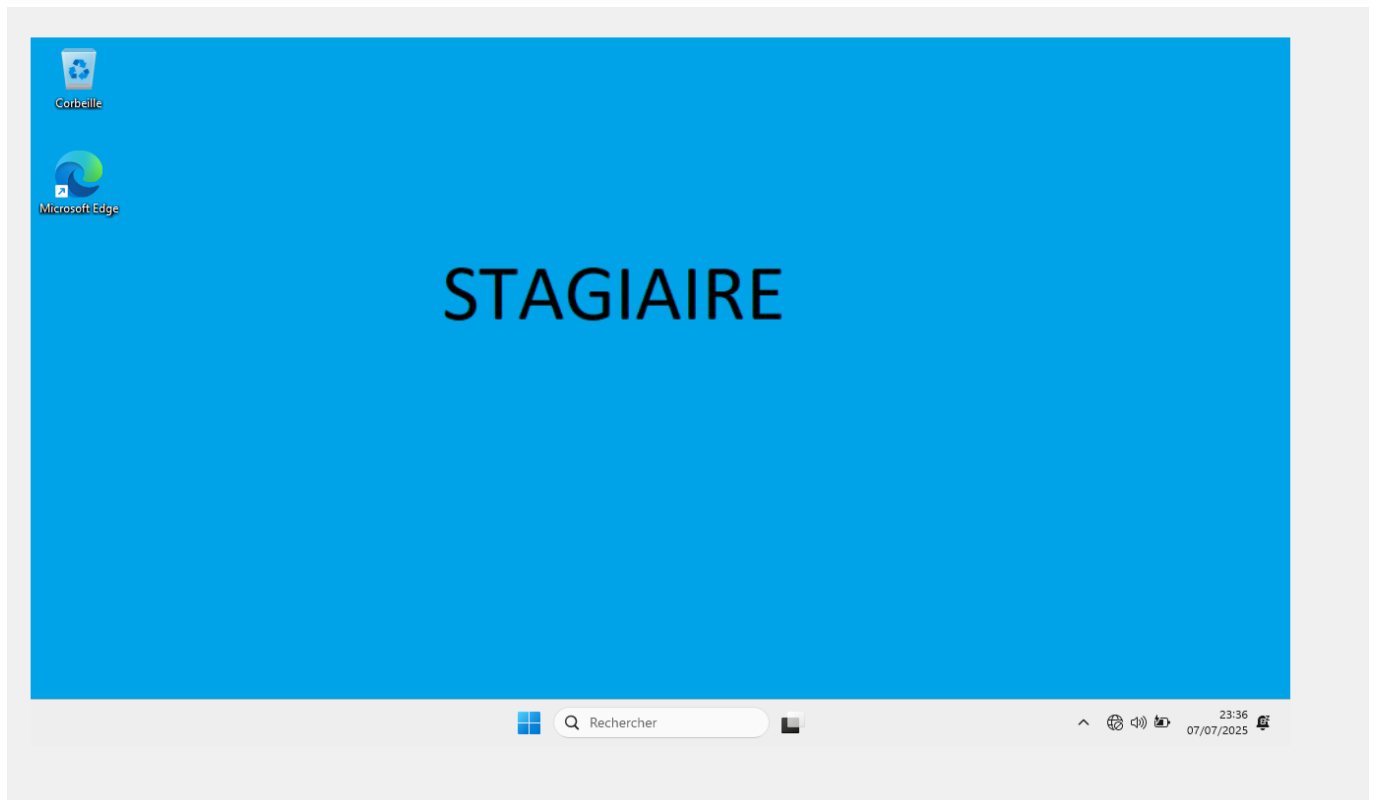
Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l'image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (*.bmp) ou JPEG (*.jpg).

Pour utiliser ce paramètre, entrez le chemin d'accès complet et le nom du fichier contenant le papier peint. Vous pouvez taper un chemin d'accès local, tel que C:\Windows\web\wallpaper\accueil.jpg ou un chemin d'accès UNC, tel que \\Serveur\Partage\Logo.jpg. Si le fichier spécifié n'est pas disponible lorsque l'utilisateur ouvre sa session, aucun papier peint n'est affiché. Les utilisateurs ne peuvent pas spécifier un autre papier peint. Vous pouvez également utiliser ce paramètre afin de spécifier si l'image du papier peint doit être centrée, en mosaïque ou étirée. Les utilisateurs ne peuvent pas modifier cette spécification.

Si vous désactivez ce paramètre ou ne le configurez pas, aucun

OK Annuler Appliquer

Vérification sur VM cliente :



Récapitulatif des actions

- J'ai créé une OU ou utilisé le filtrage pour cibler stagiaire01.
- J'ai appliqué cinq GPO précises pour restreindre son environnement de travail.
- Ces paramètres sont actifs dès la prochaine ouverture de session de stagiaire01, ou après avoir forcé l'application des GPO avec la commande gpupdate /force.

Sources :

- <https://www.vemotech.fr/tutorials/configurer-un-controlleur-de-domaine-avec-windows-server-2022-668999>
- <https://eole.ac-dijon.fr/documentations/2.8/completes/HTML/ModuleScribe/co/JoindreDomaine.html>