Projet AD Stadium Company

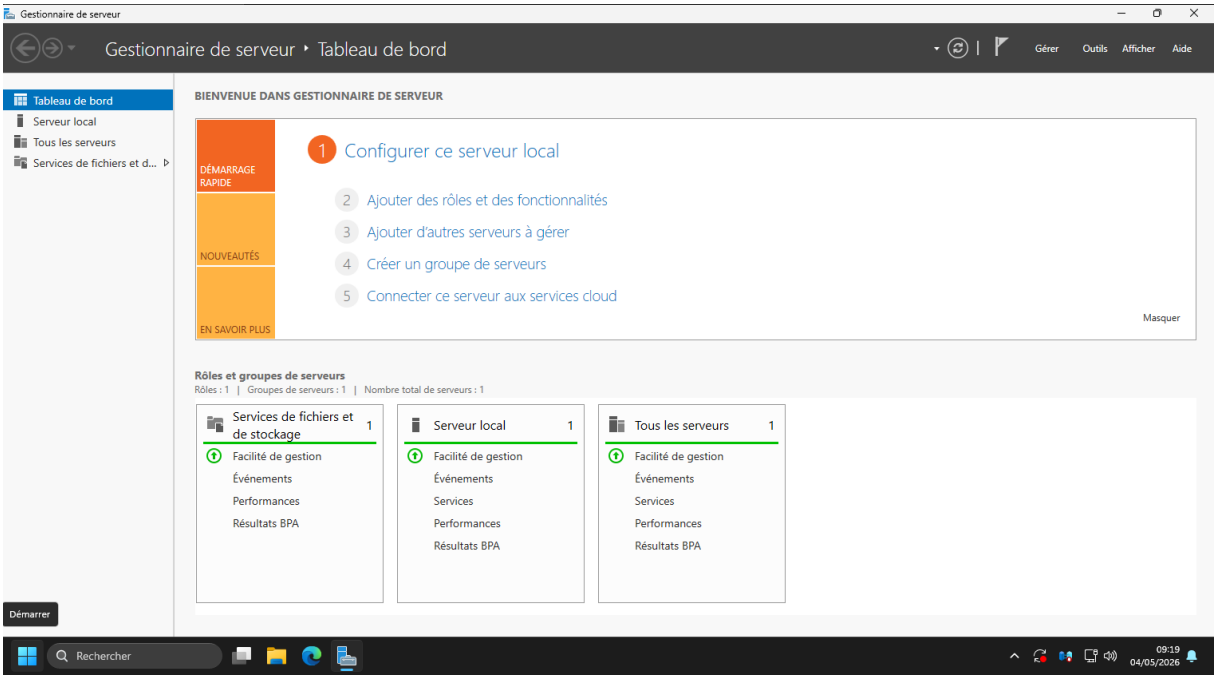
U5

SPINELLI Dylan
BTS SIO SISR | PARIS YNOV CAMPUS

Table des matières

1- Introduction à Windows Server

Windows Server est un système d'exploitation permettant l'administration d'un réseau informatique :



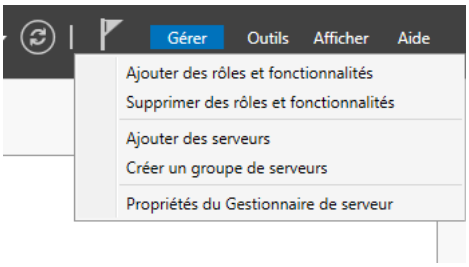
Plusieurs services sont disponibles dans Windows Server tels que DHCP, DNS, Stockage de fichiers, Contrôleur de Domaine

Nous allons installer un domaine Active Directory ainsi que plusieurs de ces fonctionnalités durant ce TP

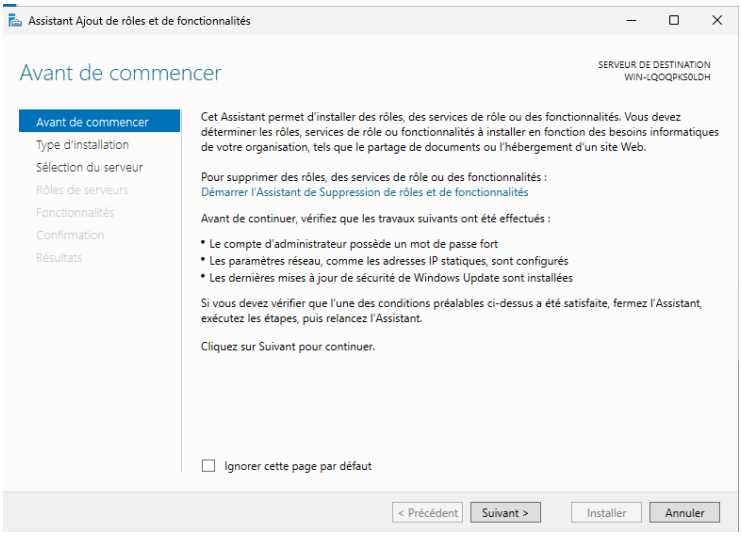
2-Installation d’un serveur DNS

2.1 - Installation du rôle DNS

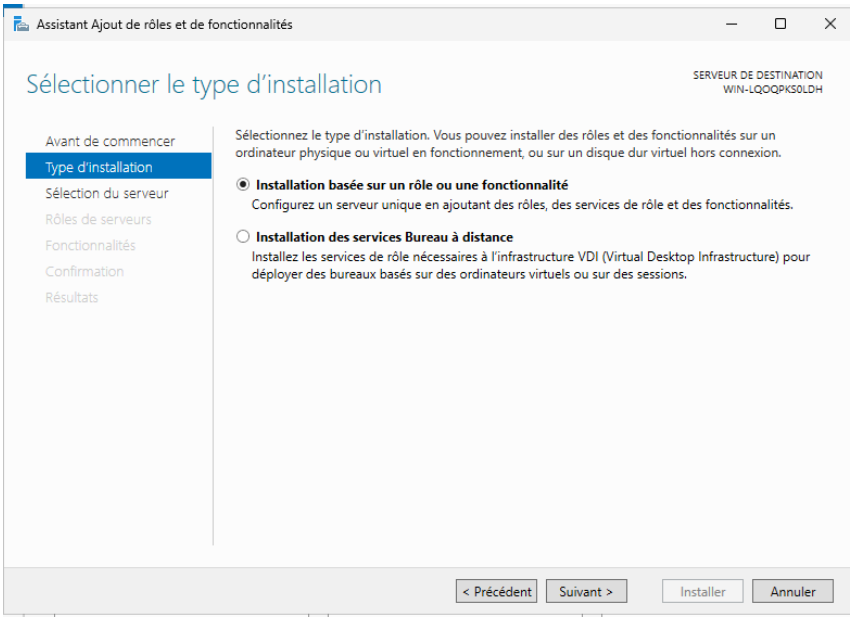
On commence par cliquer sur « ajouter des rôles ou fonctionnalités » :



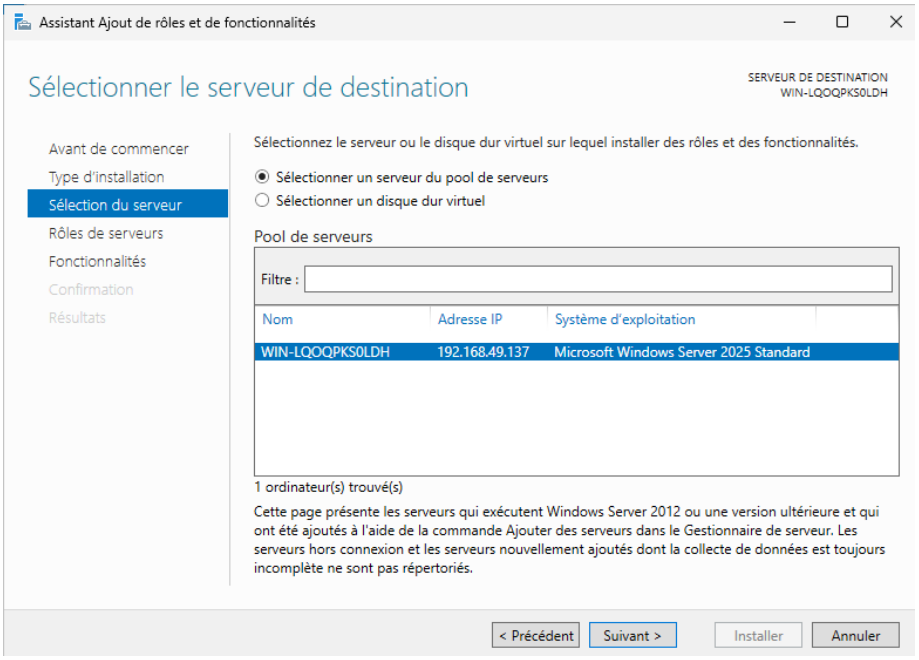
La fenêtre suivante s’ouvre :



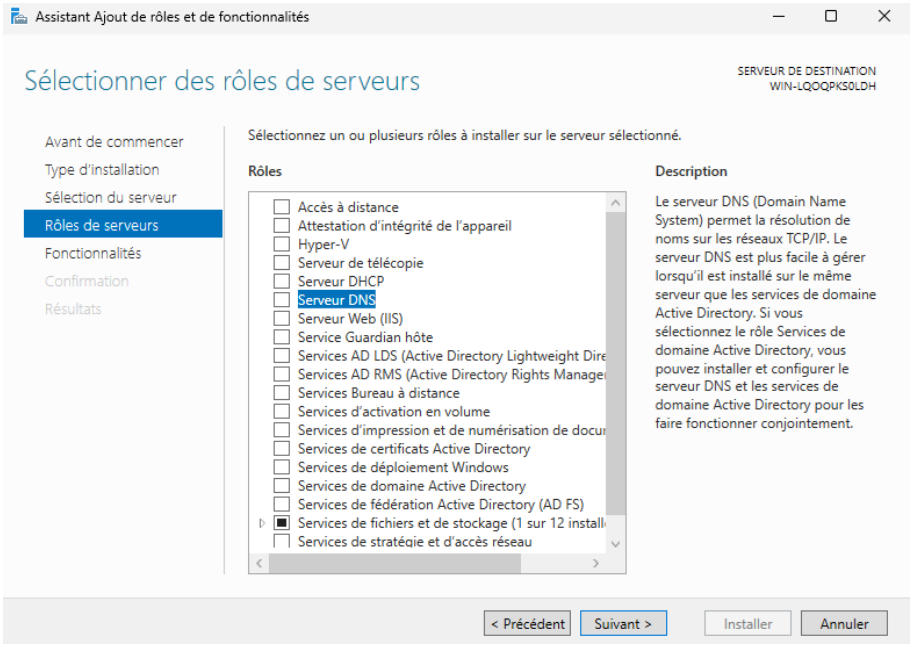
On renseigne le type d’installation :



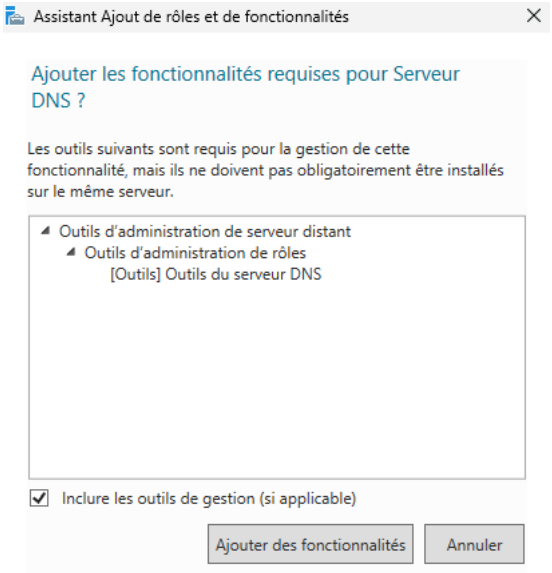
Le serveur de destination est notre VM Windows Server :



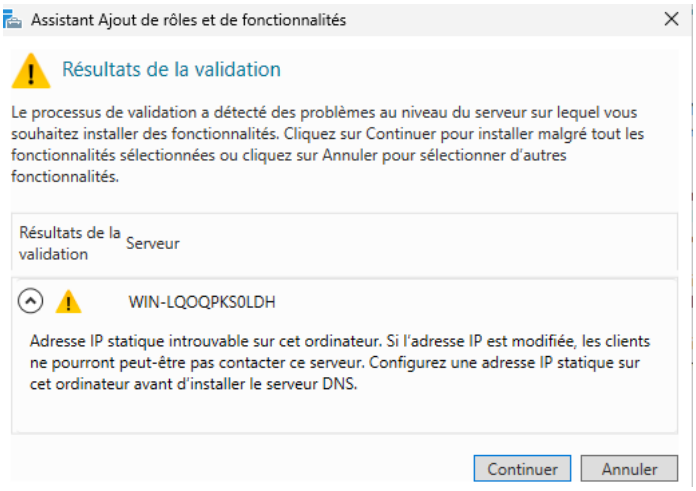
Dans la fenêtre « Rôles », on clique sur « serveur DNS » :


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
WIN-LQOQPKS0LDH
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
Accès à distance
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
Description
Le serveur DNS (Domain Name System) permet la résolution de noms sur les réseaux TCP/IP. Le serveur DNS est plus facile à gérer lorsqu'il est installé sur le même serveur que les services de domaine Active Directory. Si vous sélectionnez le rôle Services de domaine Active Directory, vous pouvez installer et configurer le serveur DNS et les services de domaine Active Directory pour les faire fonctionner conjointement.
< Précédent
Suivant >
Installer
Annuler

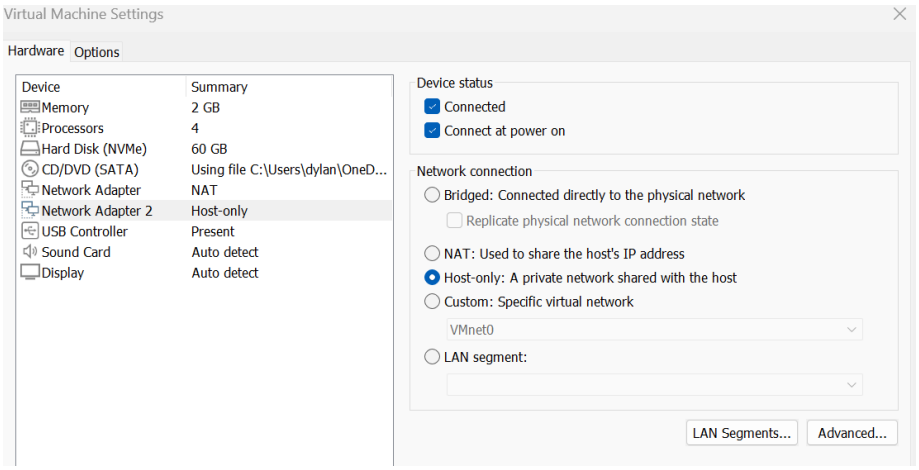
On installe les fonctionnalités requises :

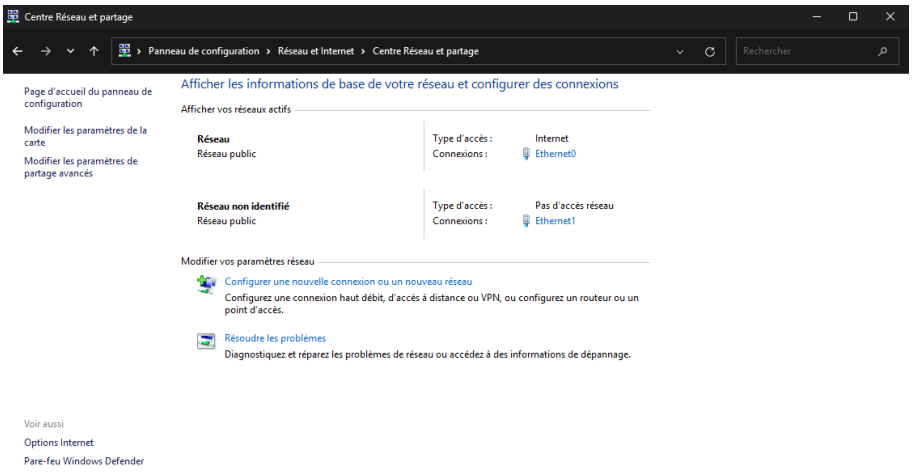


Une erreur apparait à l'écran :

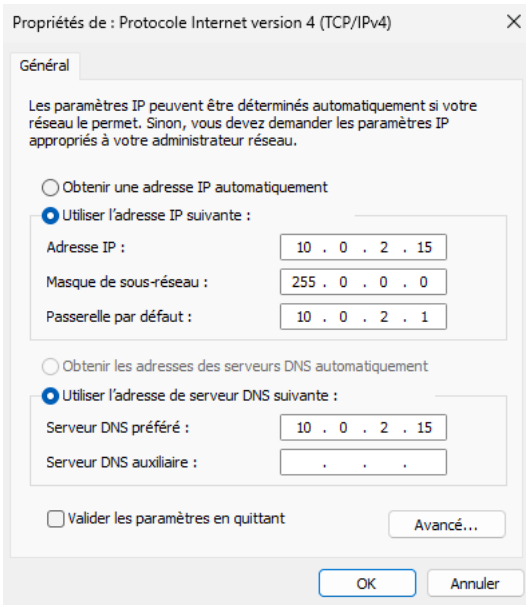


Il faut configurer une adresse IP statique pour notre serveur. On procède à la configuration d'une seconde carte réseau en mode statique sur notre serveur :



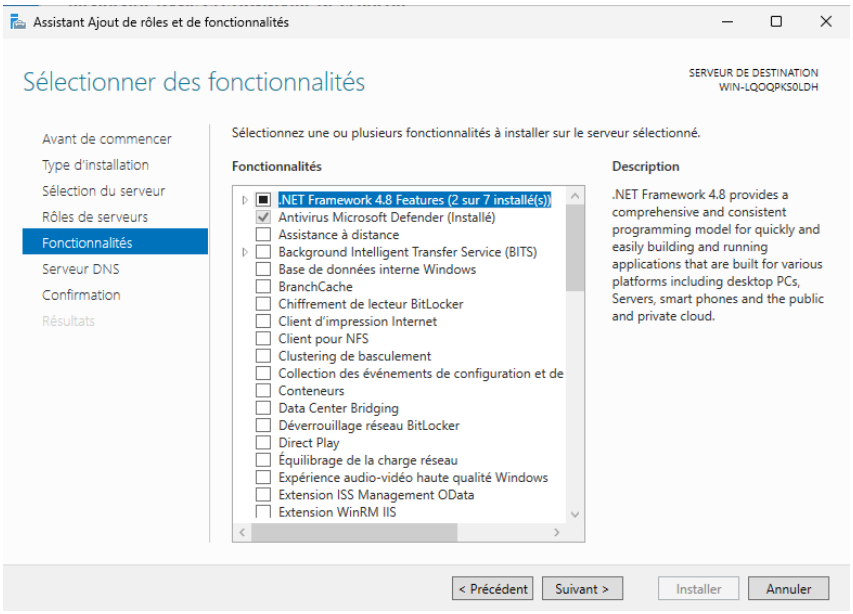


Nous avons désormais 2 cartes réseau. L'une en dynamique connectée à internet, l'autre en statique pour notre serveur DNS :

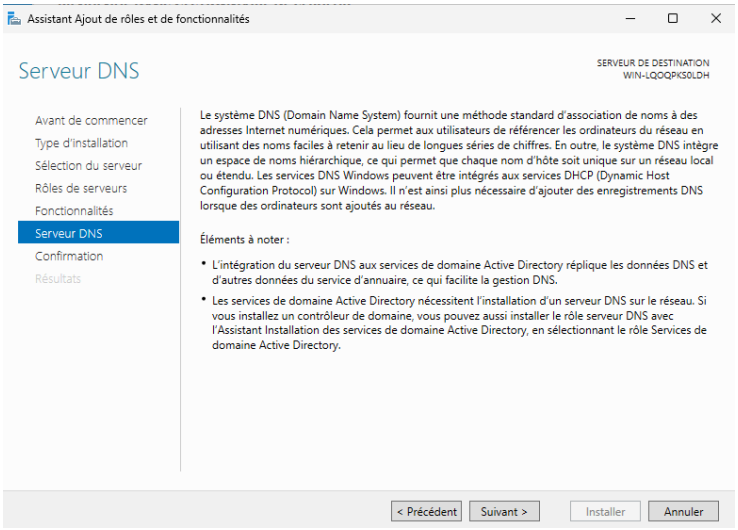


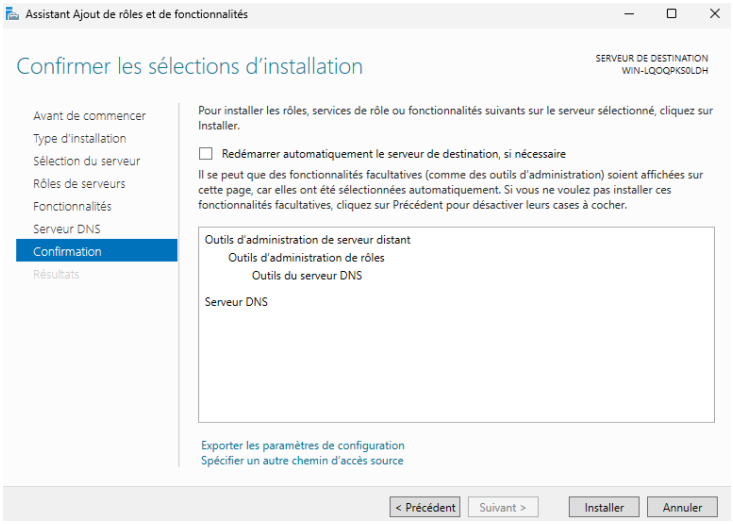
L'adresse IP de notre serveur DNS sera donc 10.0.2.15

On passe ensuite sur l'écran « fonctionnalités » :

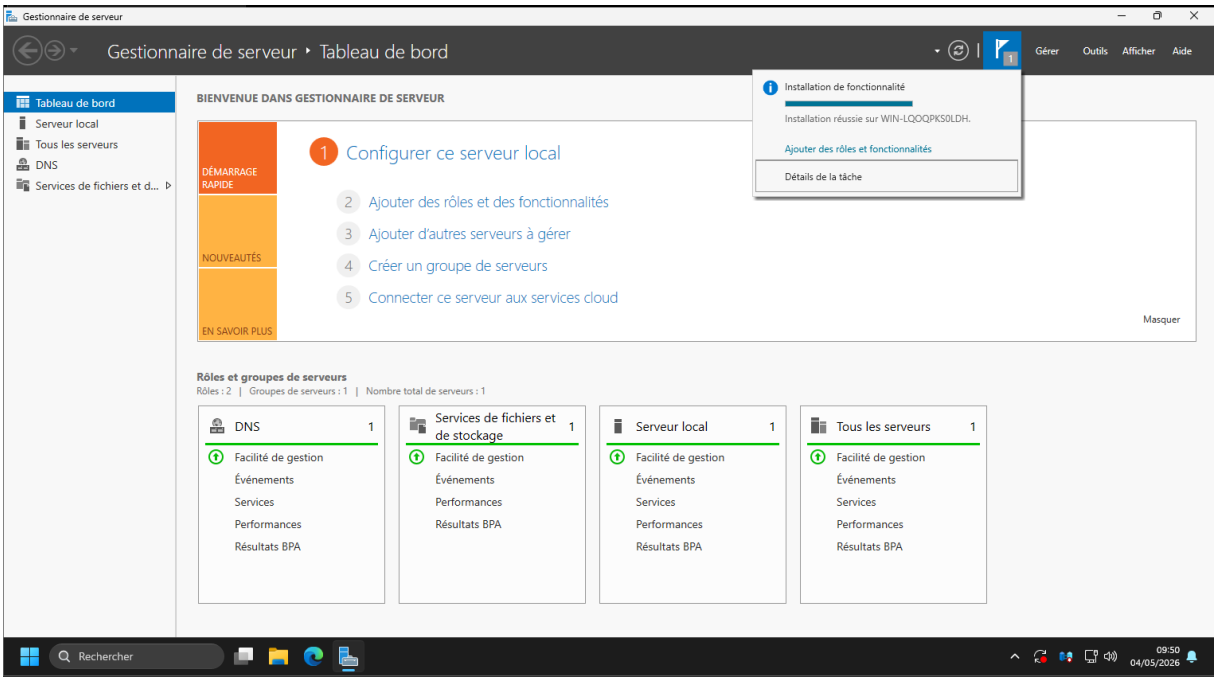


Nous pouvons ensuite procéder à l'installation du serveur DNS :





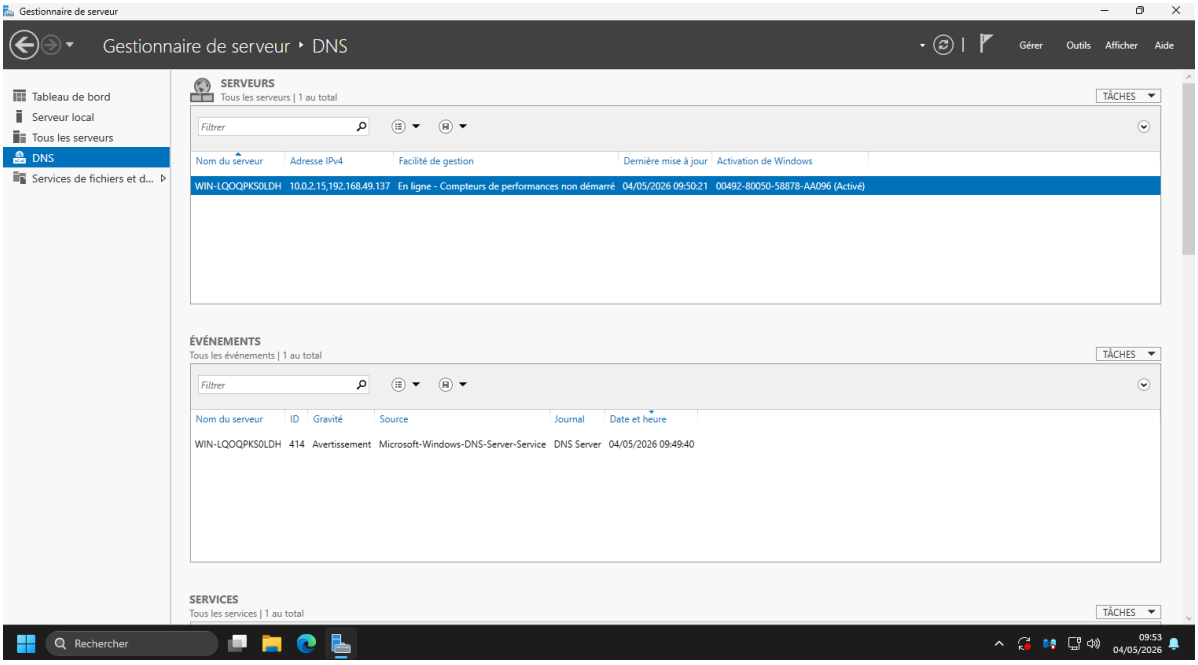
Notre serveur DNS à bien été installé :



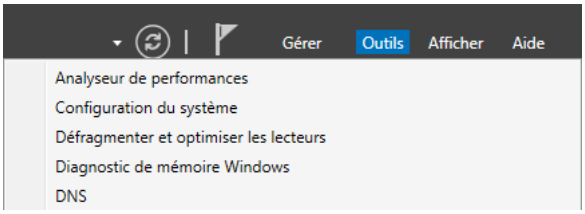
Nous pouvons désormais passer à la configuration du serveur

2.2 - Configuration du serveur DNS

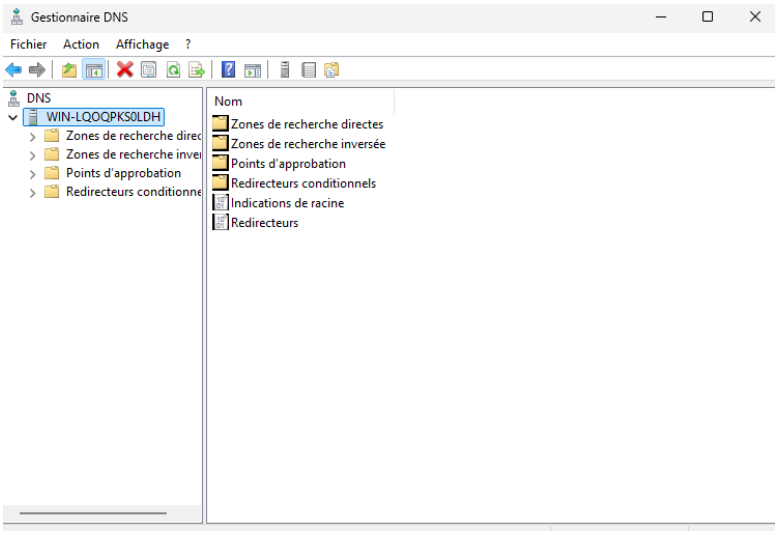
Maintenant que le service DNS est installé, on le voit bien apparaitre dans le gestionnaire de serveur :



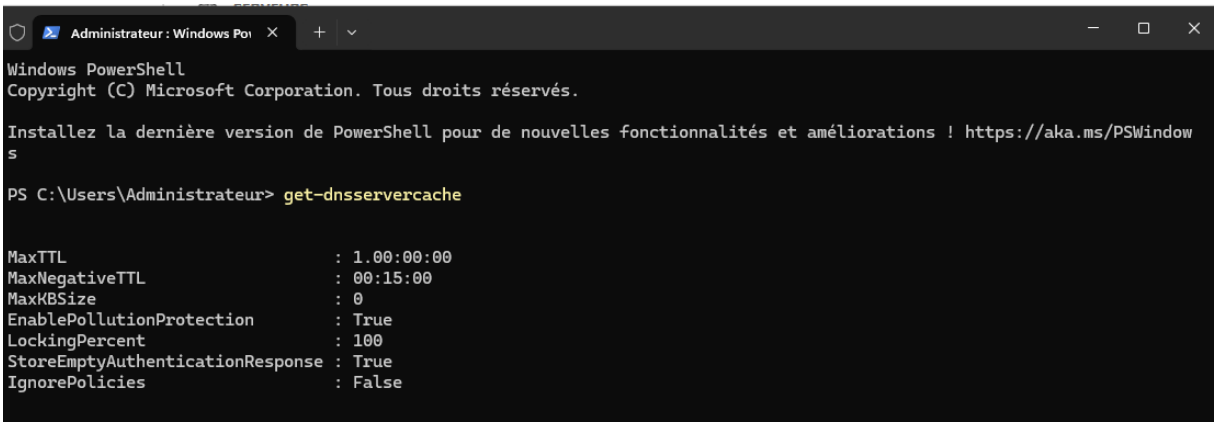
Allons dans « outils », « DNS » :



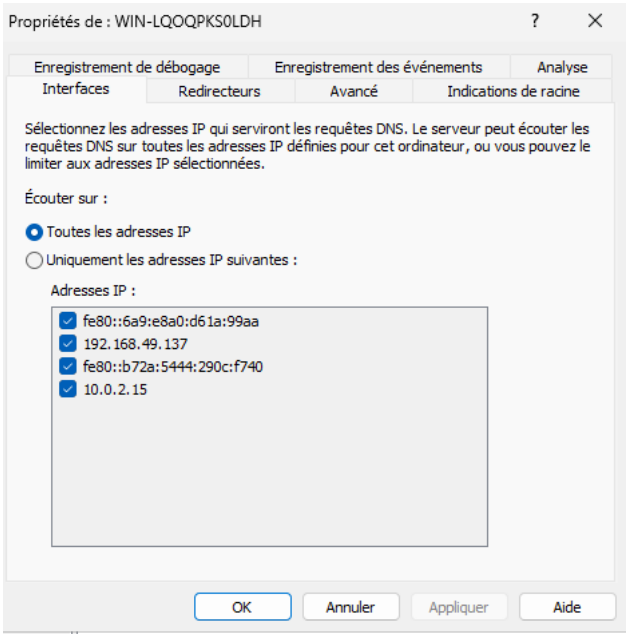
Une fenêtre « gestionnaire DNS » s'ouvre :



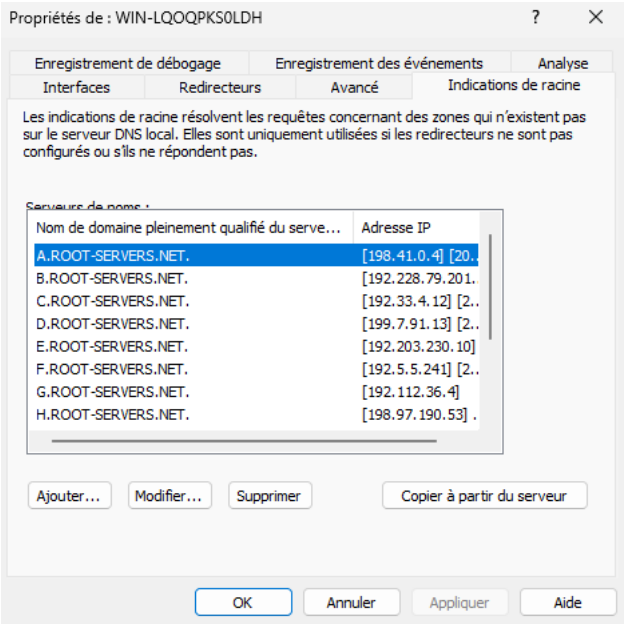
On peut vérifier la configuration du cache DNS dans powershell :



Dans les propriétés de notre serveur DNS, on vérifie que le DNS soit configuré sur toutes les adresses IP :

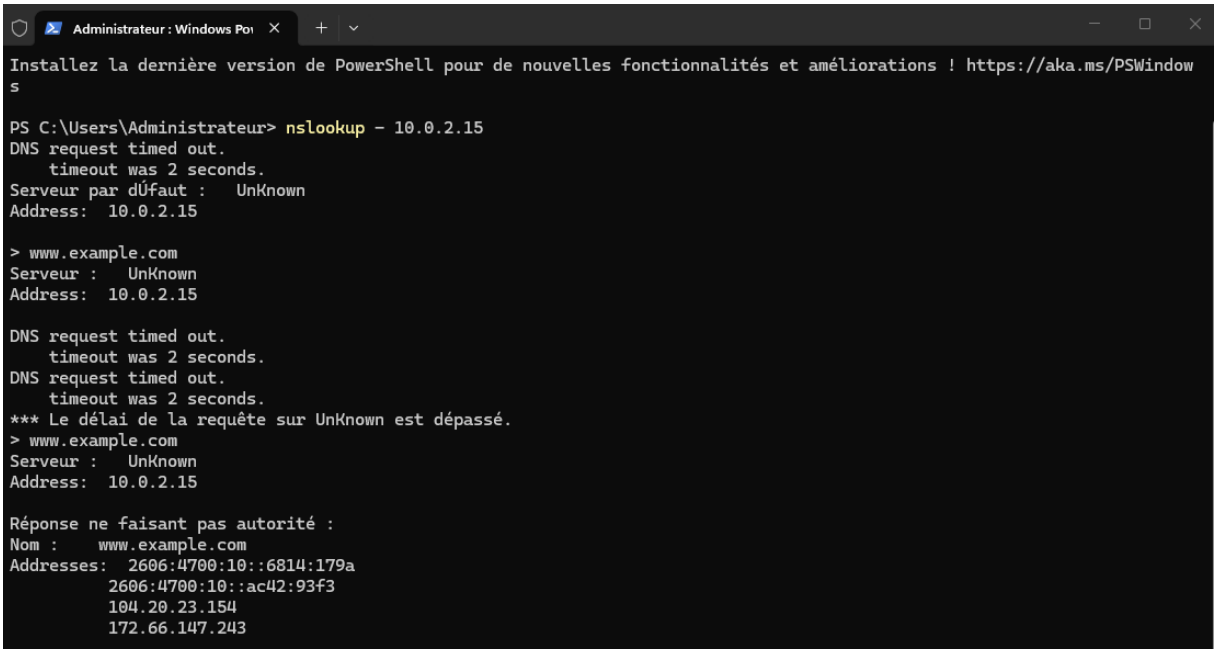


On vérifie également que les serveurs DNS racine sont bien configurés :



Les serveurs racines seront sollicités par notre serveur DNS lors des requêtes

Testons désormais notre serveur DNS avec www.example.com :



Le domaine www.example.com n'est pas configuré dans notre serveur. Notre serveur va donc interroger les serveurs racine jusqu'à trouver le domaine example.com

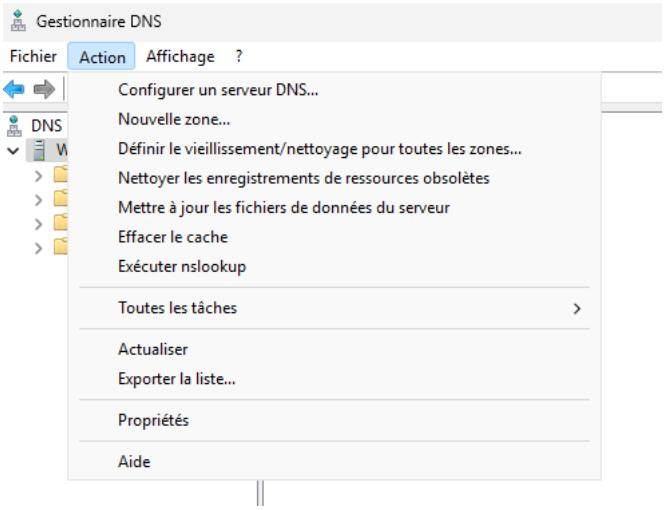
La réponse de notre serveur est donc « non-autoritaire » car elle provient d'un autre serveur.

Pour obtenir des réponses fiables, il faut configurer une zone DNS

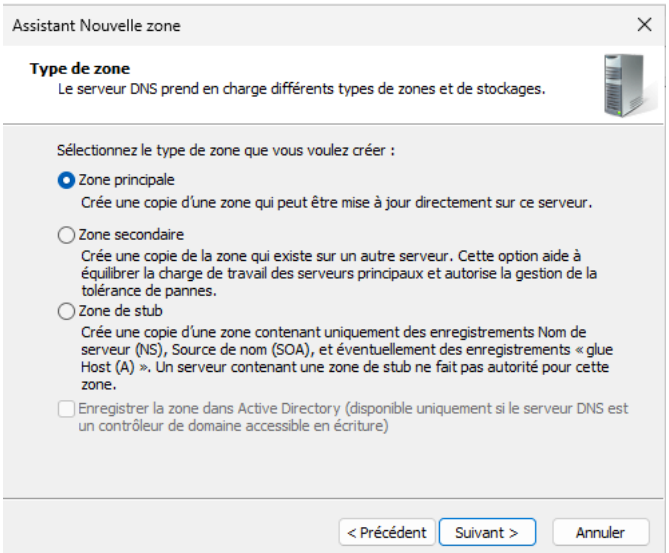
2.3 - Configuration d'une zone DNS

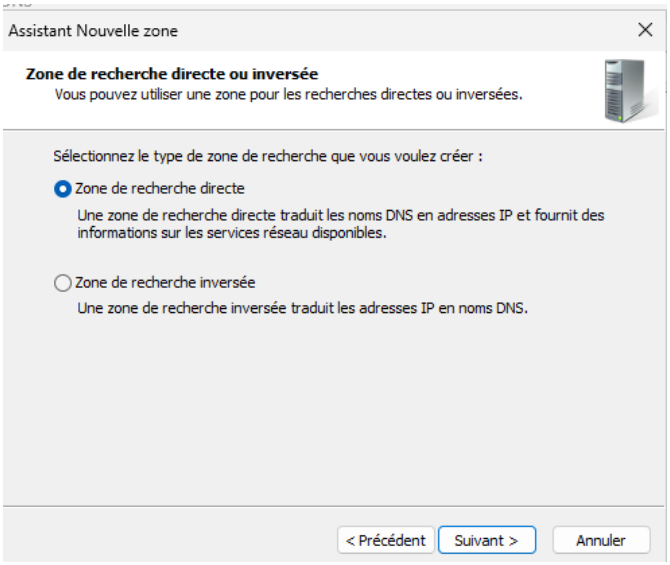
Une zone de transfert permet d'associer un nom à une adresse IP. Les noms de domaine sont plus simples à retenir que les adresses IP. De plus, les adresses IP peuvent être amenées à changer au fil du temps.

Commençons donc la configuration d'une nouvelle zone. On clique sur « action », « nouvelle zone » :

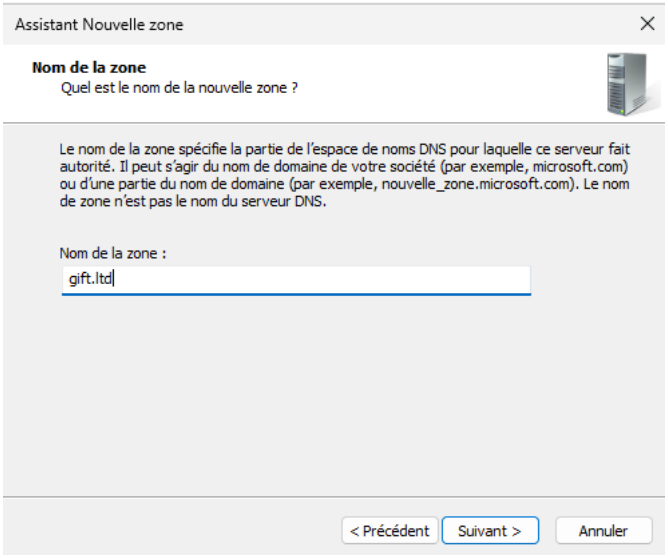


On configure une zone principale :

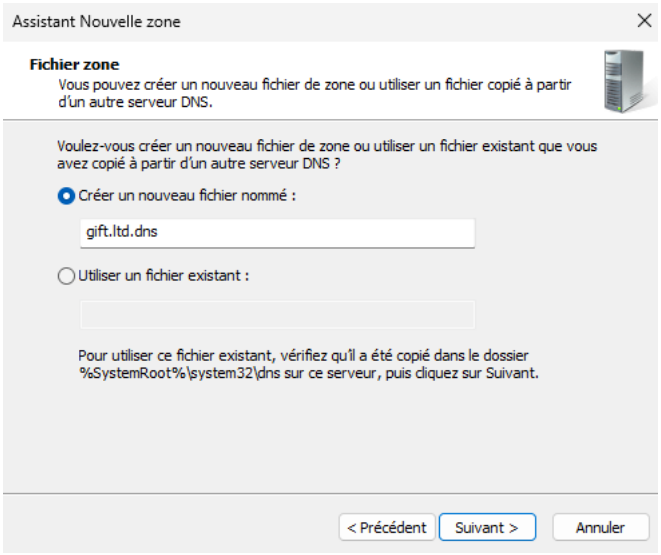




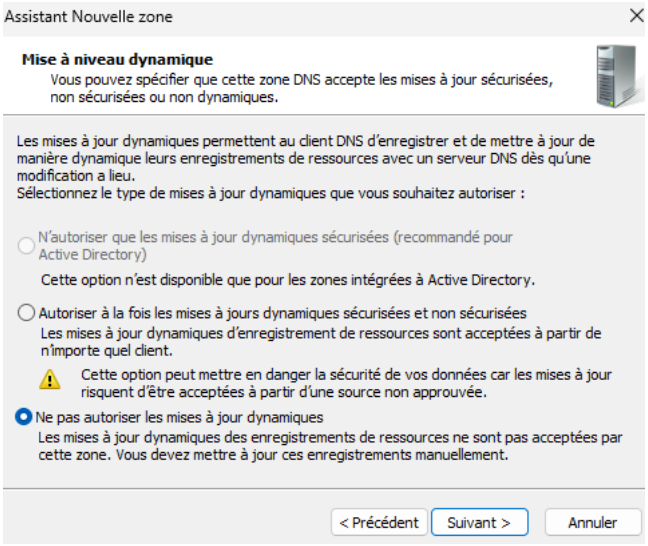
On nomme la zone « gift.ltd » :



On crée donc un nouveau fichier de zone pour notre DNS :

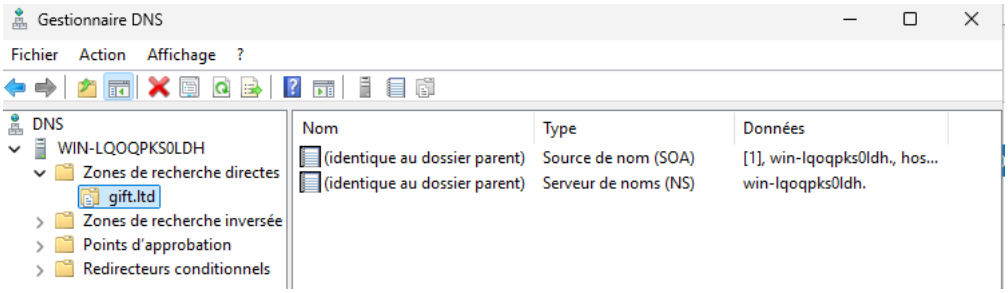


On désactive les MAJ dynamiques :

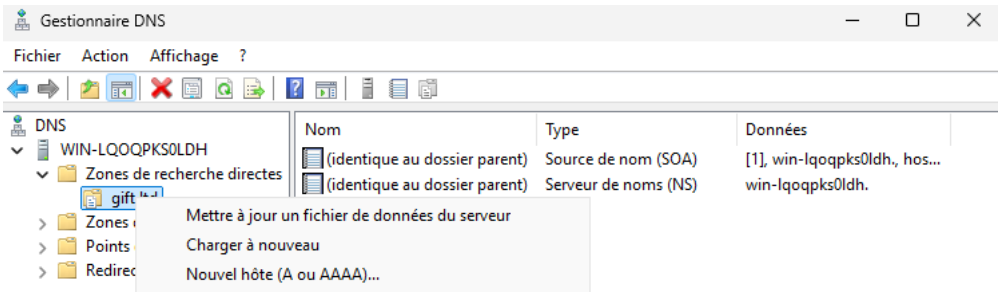


Laisser les MAJ dynamiques activées permet aux utilisateurs de modifier les adresses IP enregistrées. Un utilisateur malveillant pourrait donc modifier la configuration pour faire rediriger le DNS vers un autre serveur. Par mesure de sécurité, on préfère donc désactiver l'option.

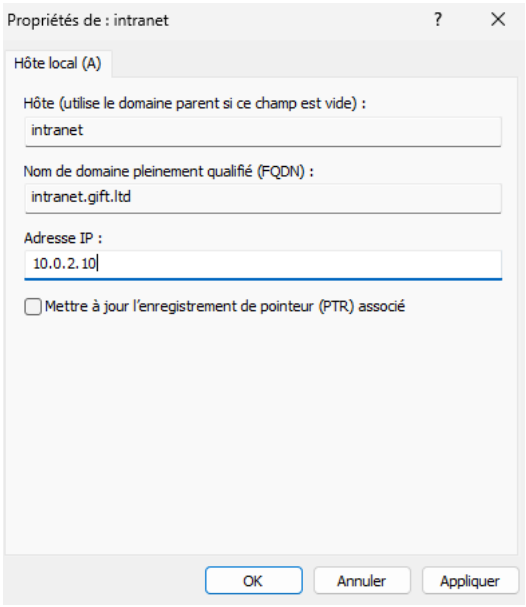
Nous avons terminé la configuration de notre zone :

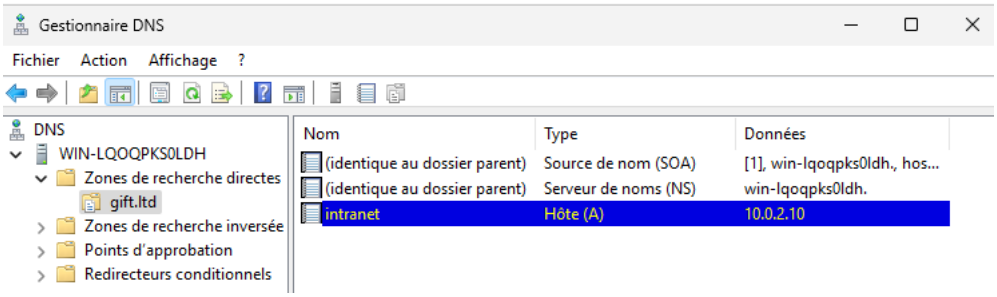


Il nous reste à ajouter l'enregistrement DNS dans notre zone. Pour cela, on choisit l'option « nouvel hôte » :



On renseigne ensuite le nom de domaine ainsi que l'adresse IP associée :





Nous avons désormais attribué un nom de domaine « intranet » à l'adresse IP 10.0.2.15

Vérifions cela depuis powershell :

```
PS C:\Users\Administrateur> nslookup intranet.gift.ltd  10.0.2.15
Serveur :   UnKnown
Address:  10.0.2.15

Nom :    intranet.gift.ltd
Address:  10.0.2.10
```

L'enregistrement DNS fonctionne correctement

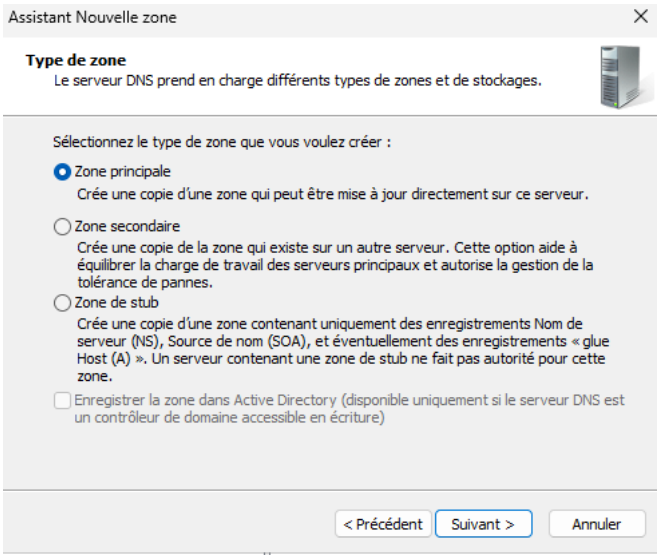
2.4 - Configuration d’une zone inverse DNS

La zone inverse associe une adresse IP à un nom. C’est l’inverse d’une zone forward. Elle permet de confirmer que le nom choisi dans une zone forward est bien associé à l'adresse IP, et d'interroger un DNS sur une adresse IP.

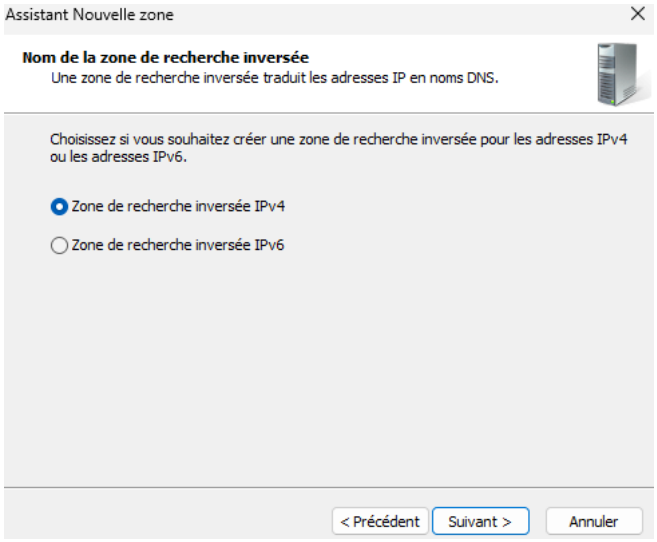
En effet, lorsque l’on ping 10.0.2.10, il ne reconnait pas son nom :

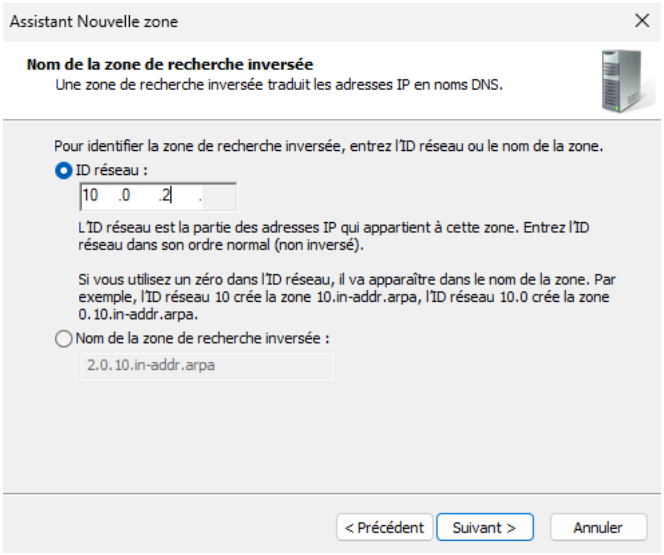
```
PS C:\Users\Administrateur> ping 10.0.2.10

Envoi d’une requête 'Ping'  10.0.2.10 avec 32 octets de données :
```

On crée donc une nouvelle zone principale :

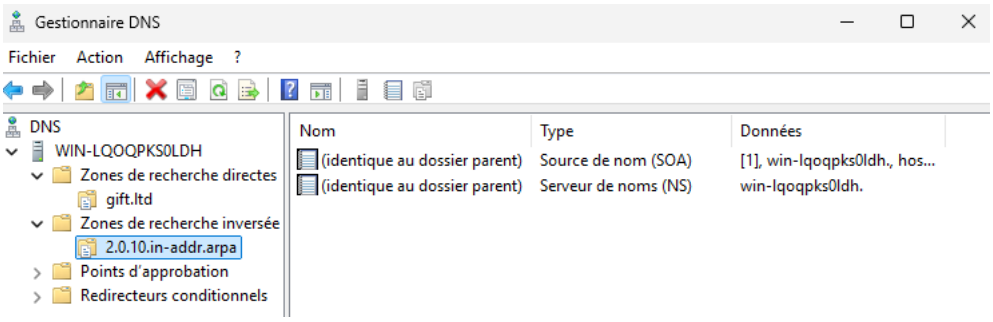


IPv4 :

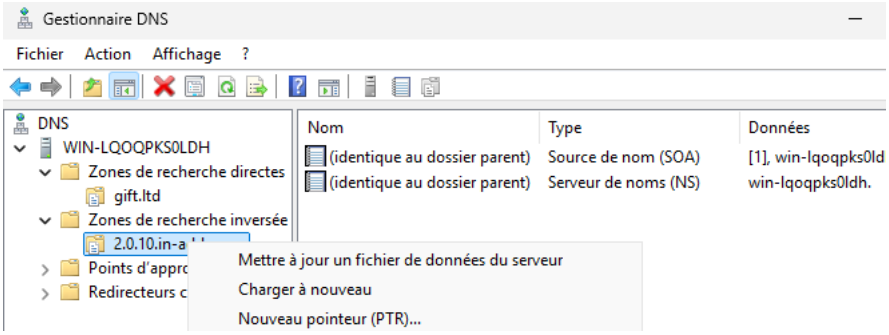




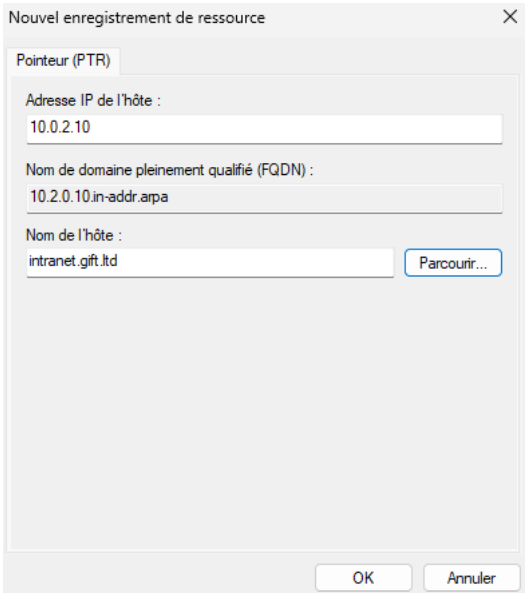
La nouvelle zone inversée est créé :

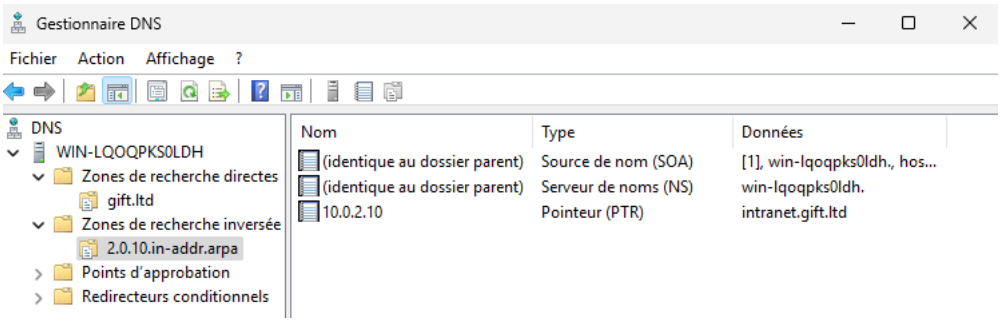


On ajoute ensuite un pointeur PTR :



On enregistre le nom « intranet » :





Vérifions désormais que nous pouvons identifier le nom « intranet » à partir de 10.0.2.10 :

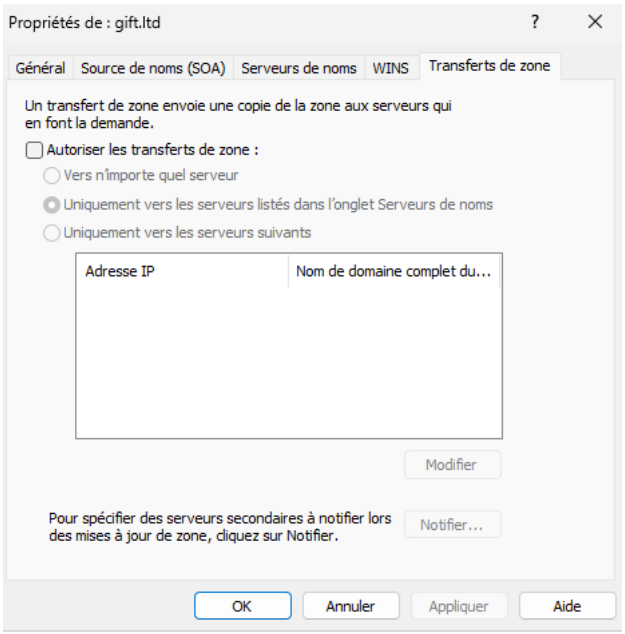
```
PS C:\Users\Administrateur> ping -a 10.0.2.10

Envoi d'une requête 'ping' sur intranet.gift.ltd [10.0.2.10] avec 32 octets de données :
```

Désormais, nous pouvons retrouver le nom intranet depuis 10.0.2.10

2.5 - Transfert de zone

Le transfert de zone est une fonctionnalité qui permet l'envoi d'une copie de la zone vers un autre serveur. Cette fonctionnalité est utile si plusieurs serveurs DNS sont présents dans le réseau. Cependant, elle représente également une vulnérabilité face au risque de cyberattaque.

Nous allons donc vérifier la configuration du transfert de zone :



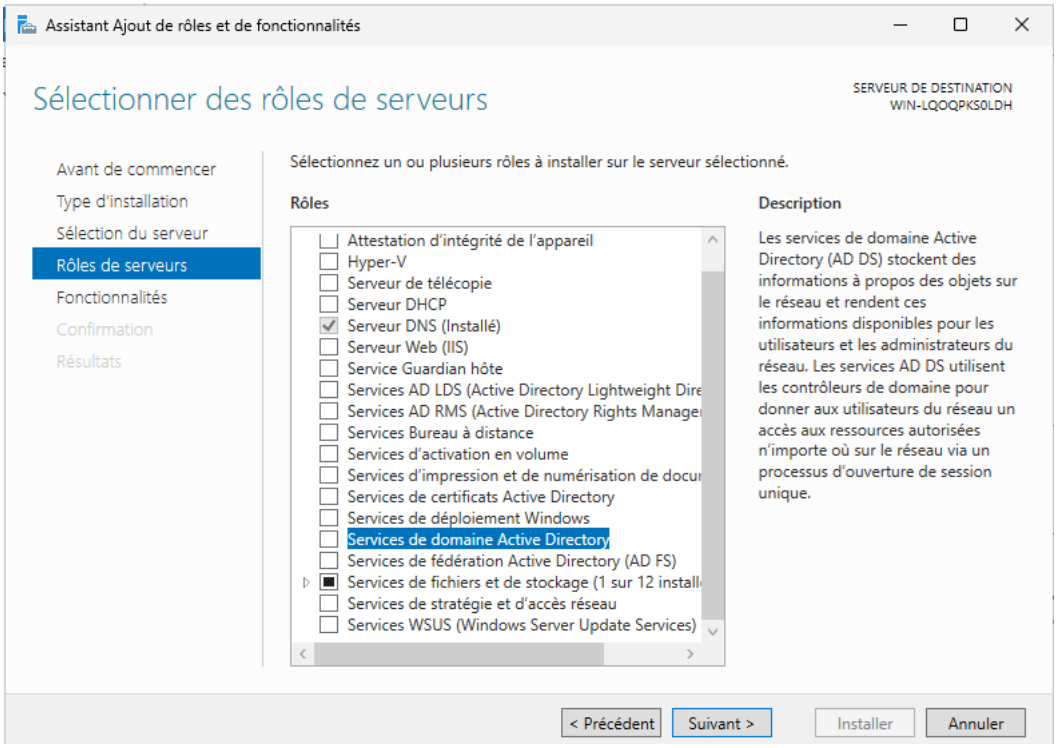
On préfèrera désactiver la fonctionnalité.

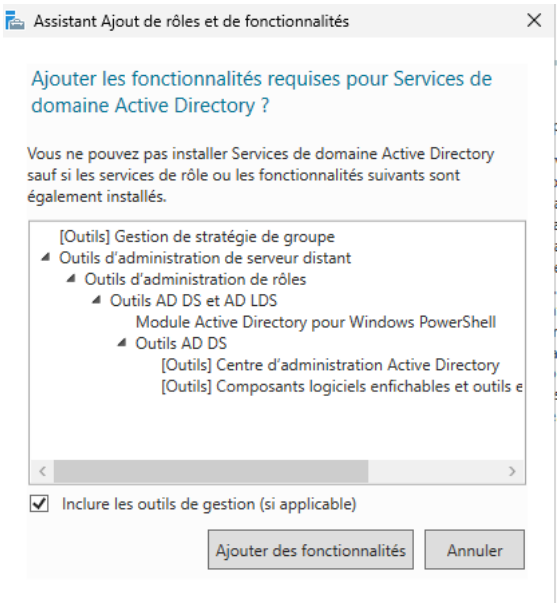
La configuration du serveur DNS est désormais terminée

3-Installation du contrôleur de domaine

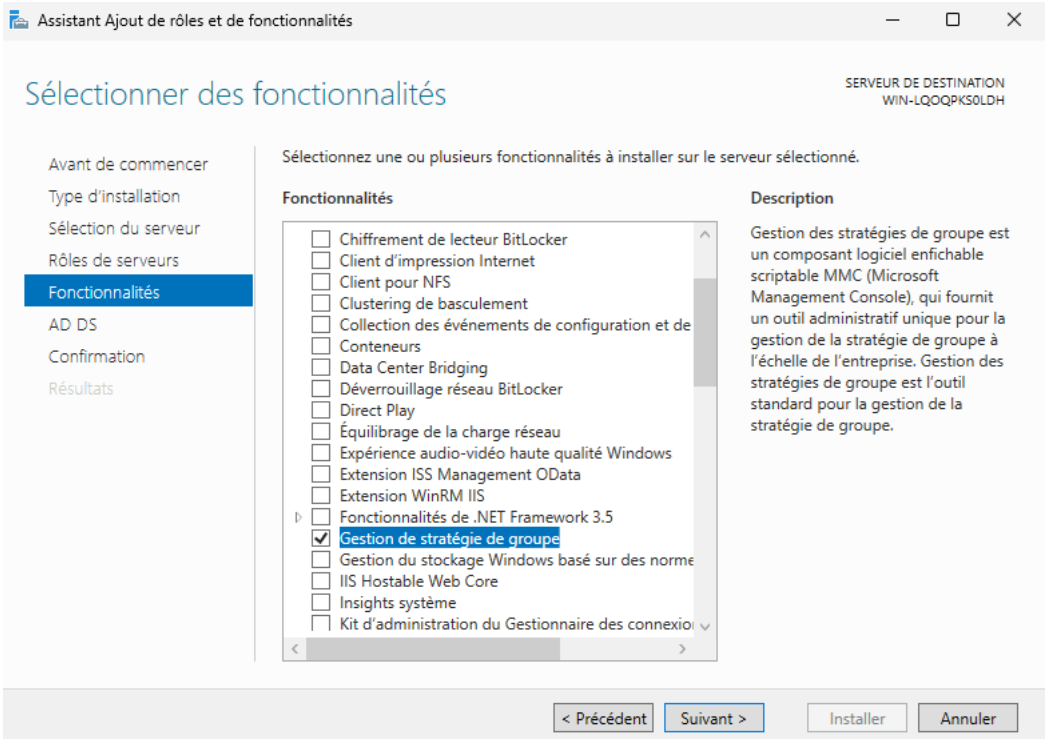
3.1 – Installation du rôle ADDS

Nous allons maintenant installer un contrôleur de domaine. Pour cela, on commence par installer le rôle ADDS (Active Directory Domain Services) :

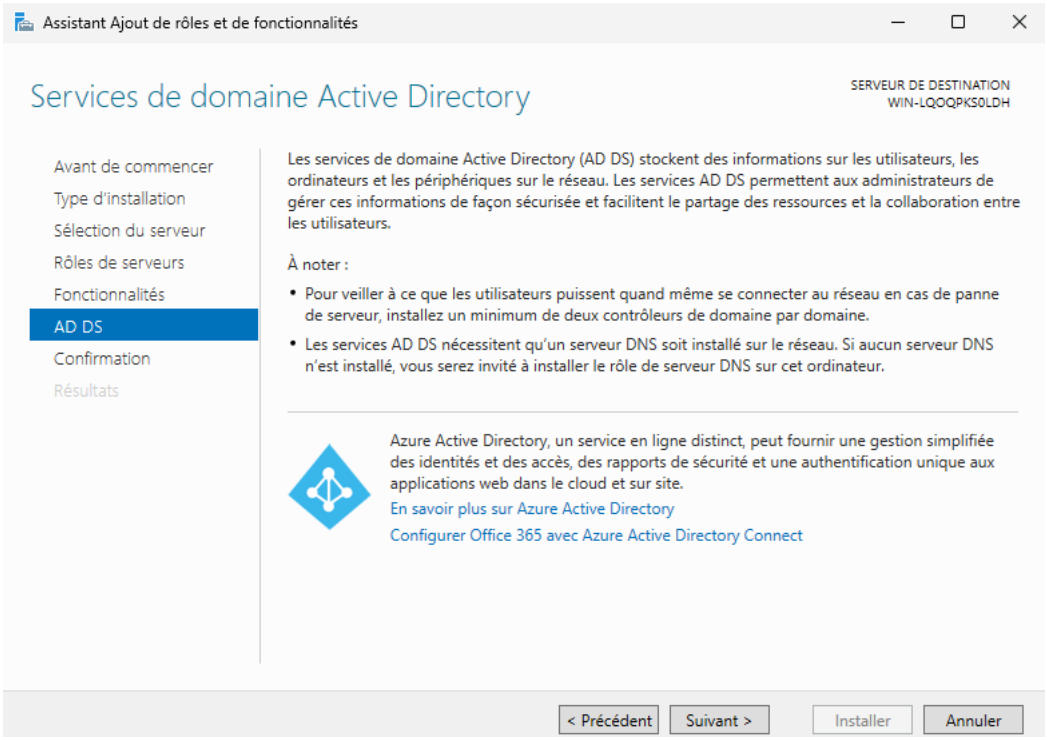




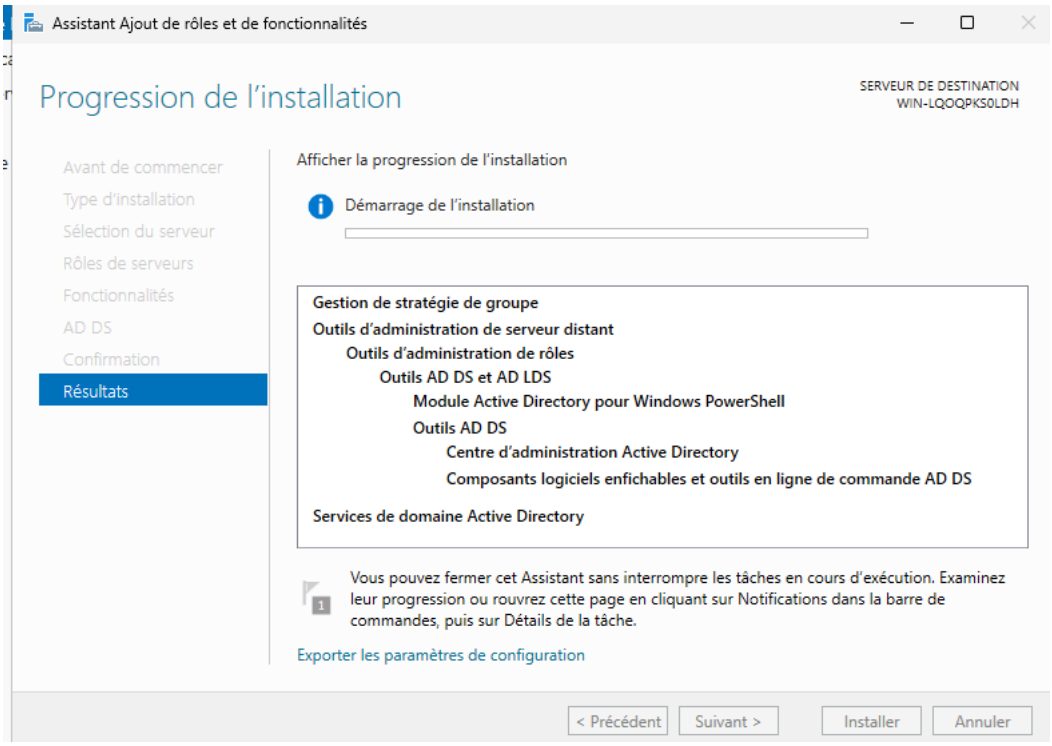
Pour les fonctionnalités, on vérifie que la fonctionnalité « Gestion de stratégie de groupe » est bien activée :

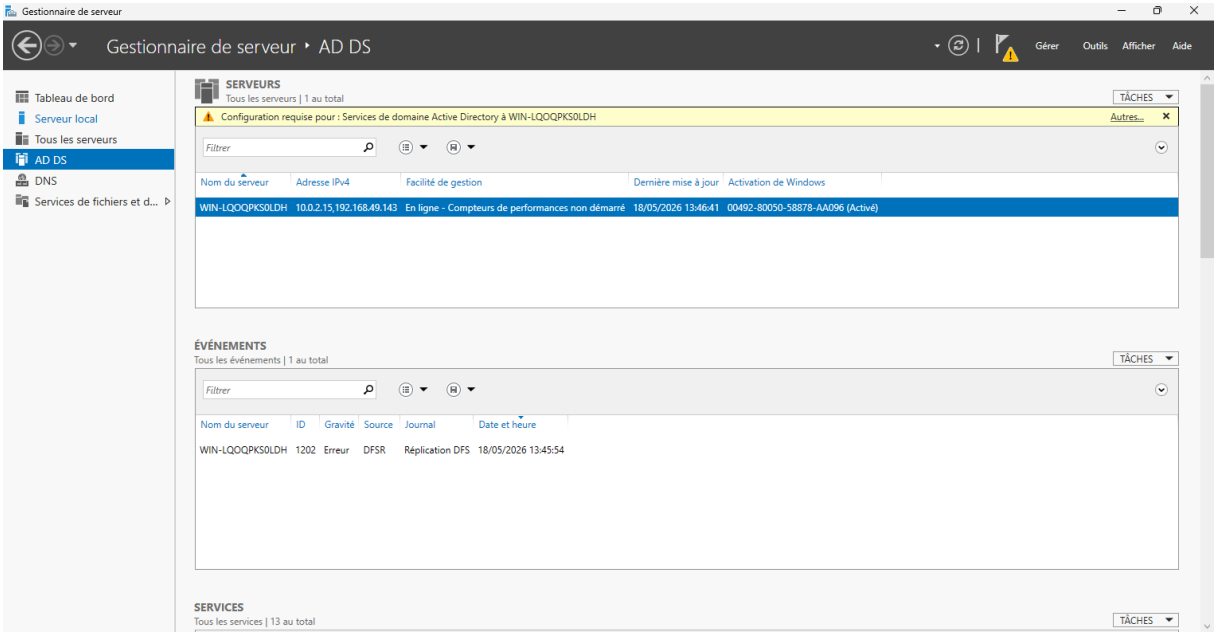


L'utilisation de ADDS requiert un serveur DNS. Celui-ci a été installé précédemment :



On peut ensuite commencer l'installation :

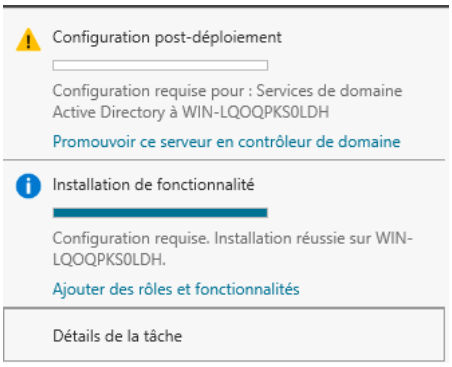




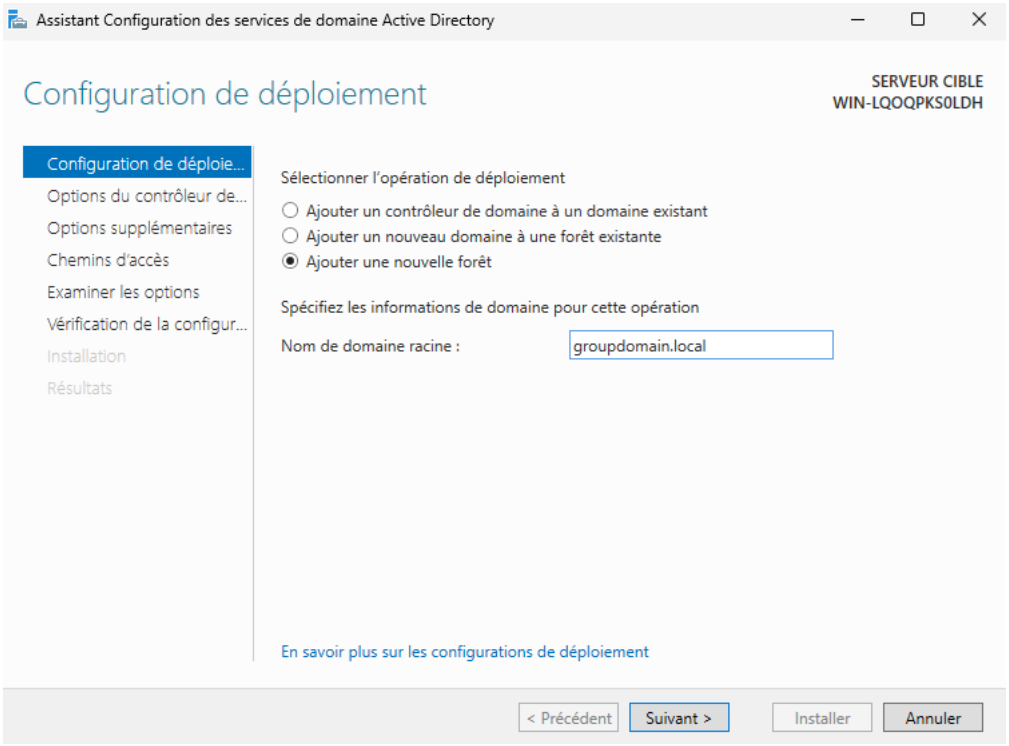
Notre contrôleur de domaine est désormais installé. Nous allons maintenant le configurer.

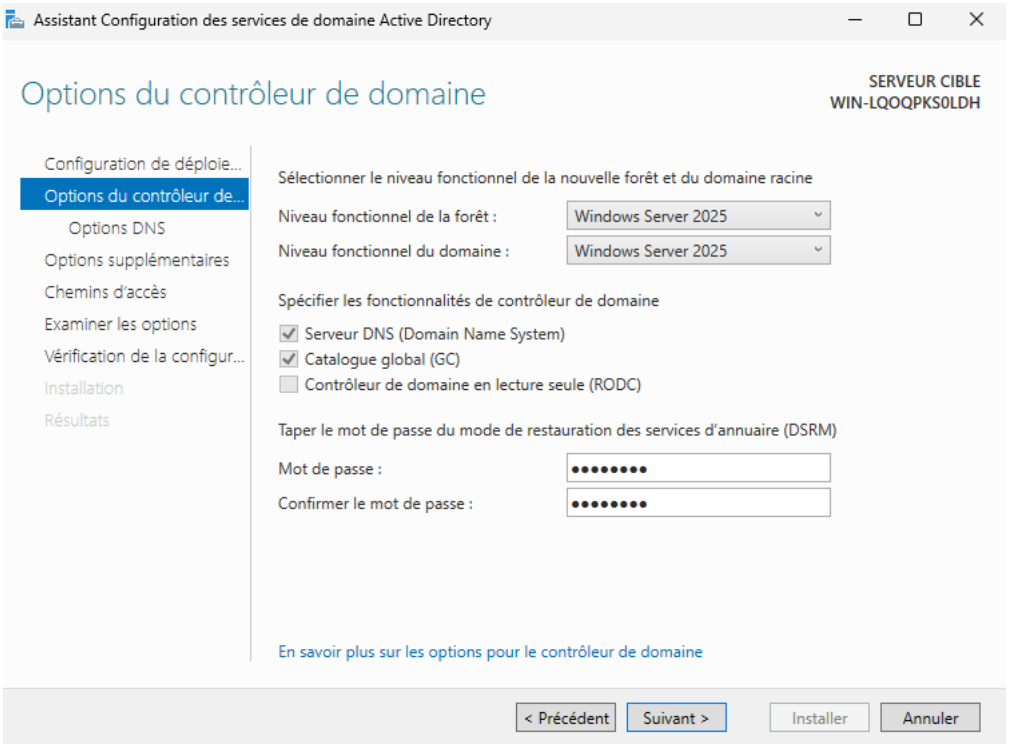
3.2 – Configuration du contrôleur de domaine

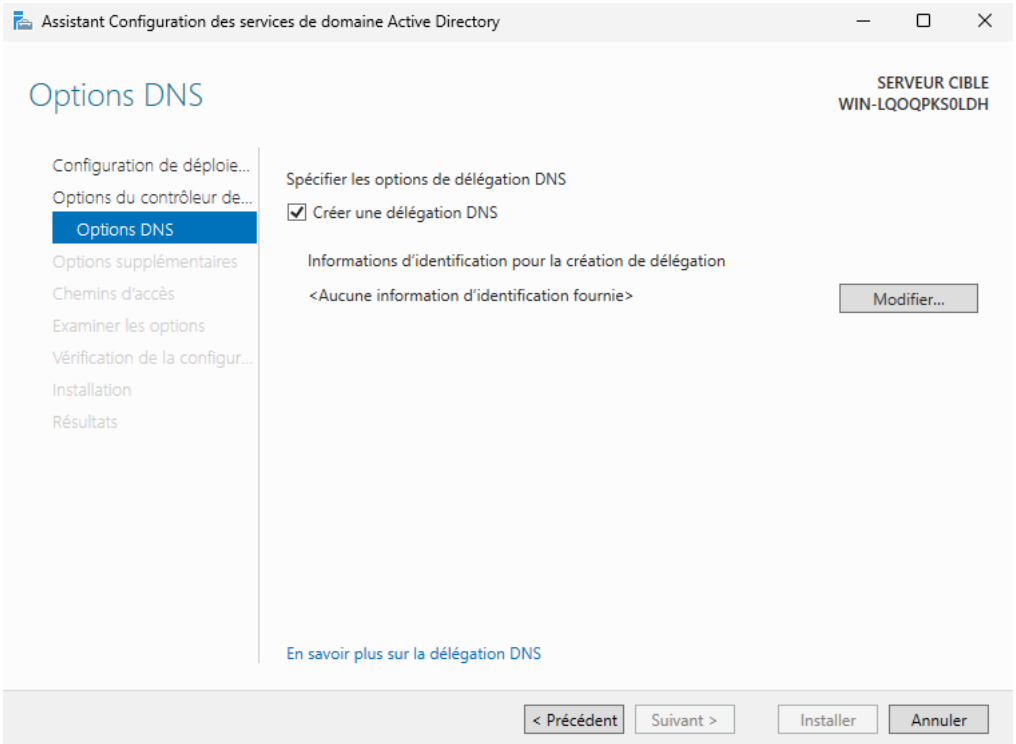
Nous devons définir notre serveur en tant que « contrôleur de domaine » :

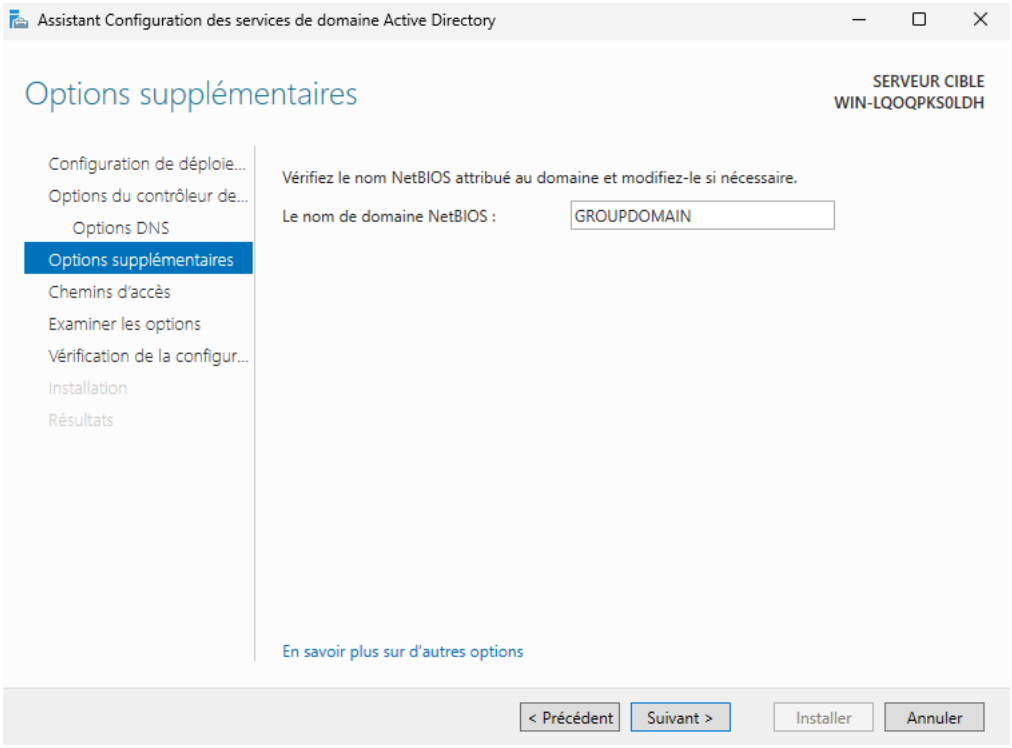


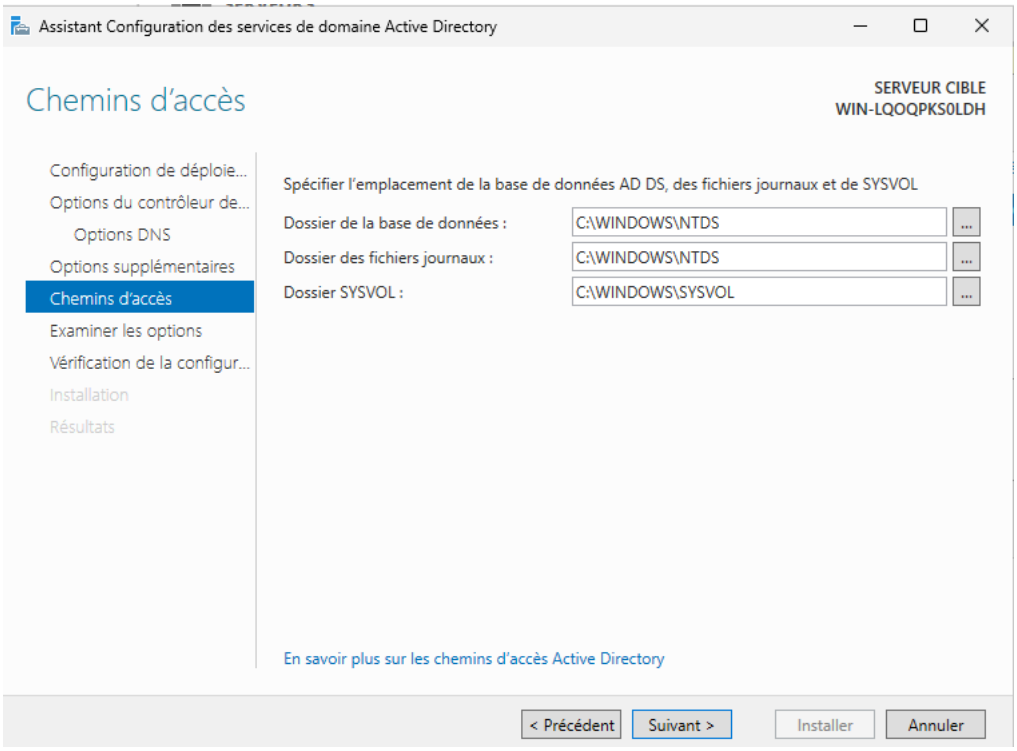
On crée une nouvelle forêt « groupdomain.local » :



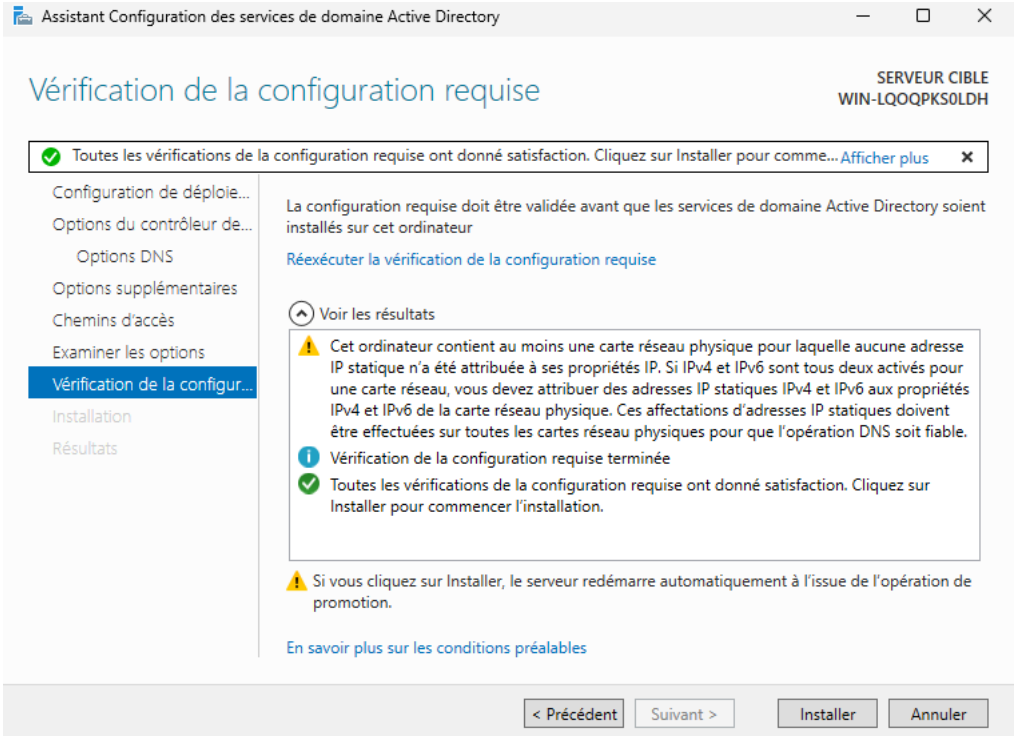

Assistant Configuration des services de domaine Active Directory
Options du contrôleur de domaine
SERVEUR CIBLE
WIN-LQOQPKS0LDH
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine
Niveau fonctionnel de la forêt :
Windows Server 2025
Niveau fonctionnel du domaine :
Windows Server 2025
Spécifier les fonctionnalités de contrôleur de domaine
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :
En savoir plus sur les options pour le contrôleur de domaine
< Précédent
Suivant >
Installer
Annuler

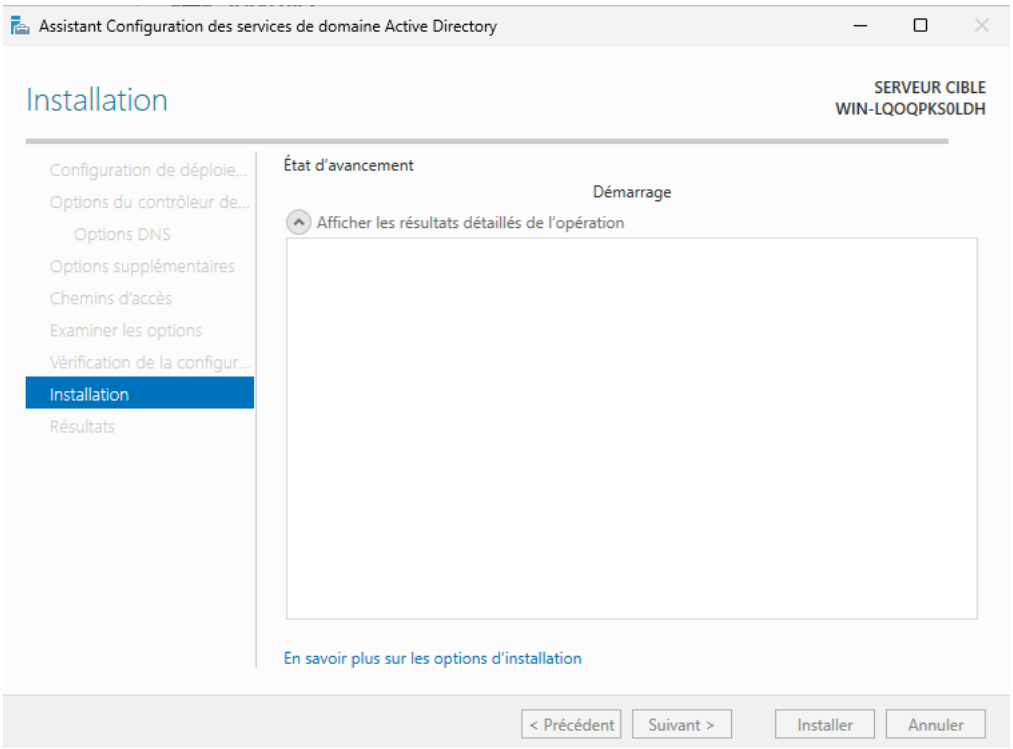

Assistant Configuration des services de domaine Active Directory
Options DNS
SERVEUR CIBLE
WIN-LQOQPKS0LDH
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier les options de délégation DNS
Créer une délégation DNS
Informations d'identification pour la création de délégation
<Aucune information d'identification fournie>
Modifier...
En savoir plus sur la délégation DNS
< Précédent
Suivant >
Installer
Annuler

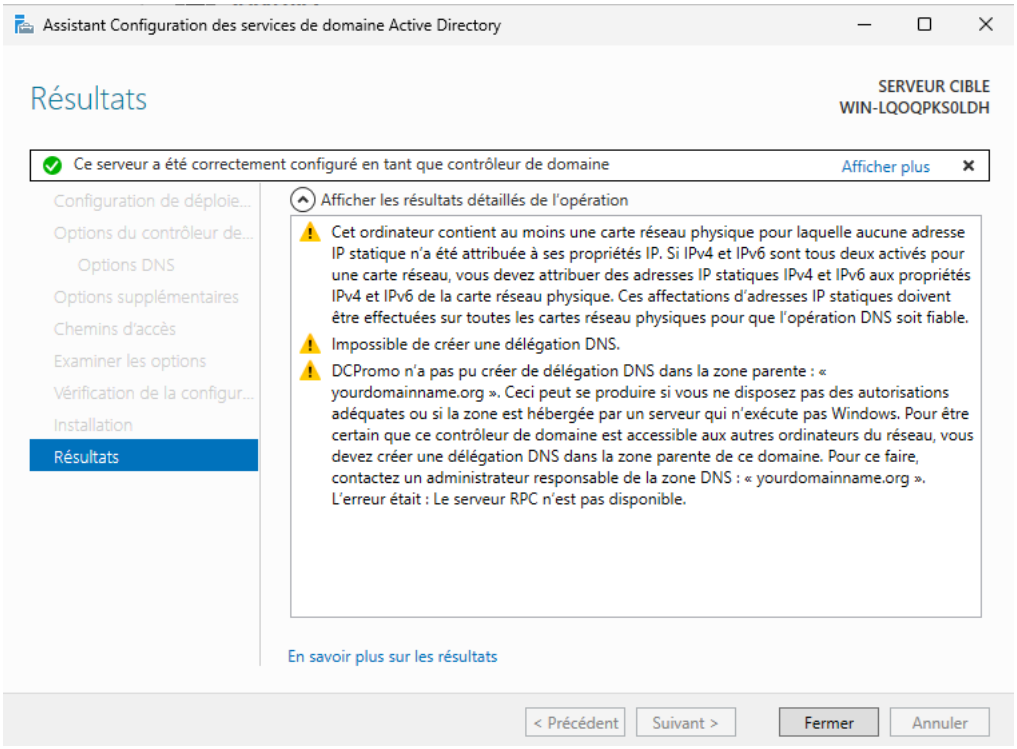

Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
WIN-LQOQPKS0LDH
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
GROUPDOMAIN
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Chemins d'accès
SERVEUR CIBLE
WIN-LQOQPKS0LDH
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL
Dossier de la base de données :
C:\WINDOWS\NTDS
Dossier des fichiers journaux :
C:\WINDOWS\NTDS
Dossier SYSVOL :
C:\WINDOWS\SYSVOL
En savoir plus sur les chemins d'accès Active Directory
< Précédent
Suivant >
Installer
Annuler

On peut débuter l'installation :

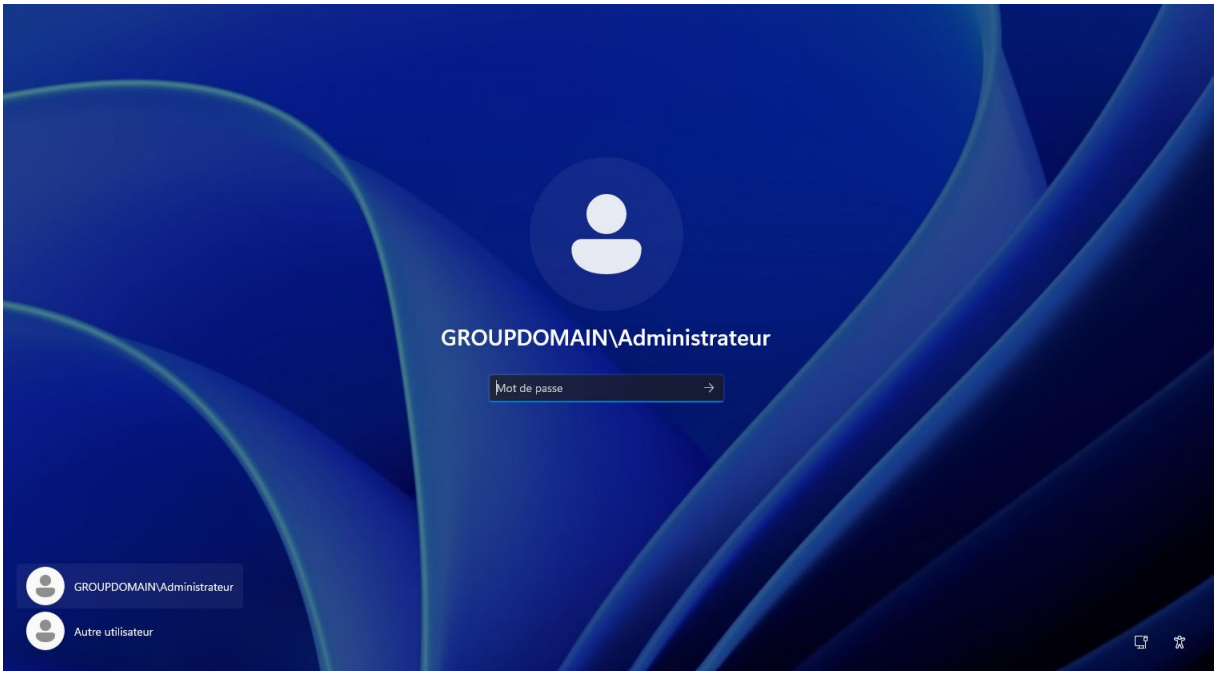






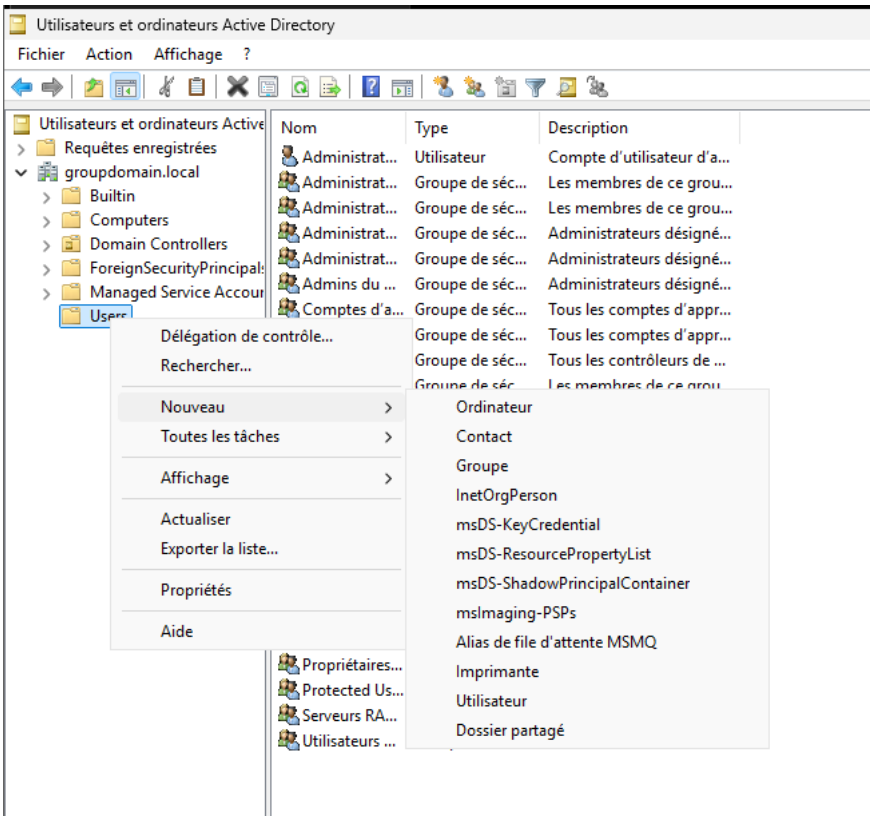
L'installation est terminée

Désormais, notre PC est bien dans le domaine :

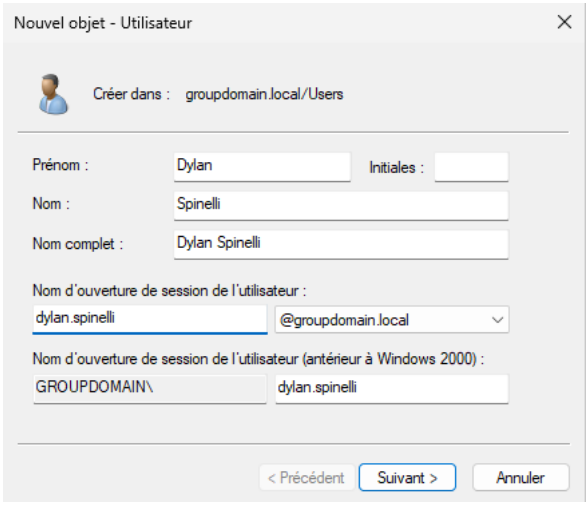


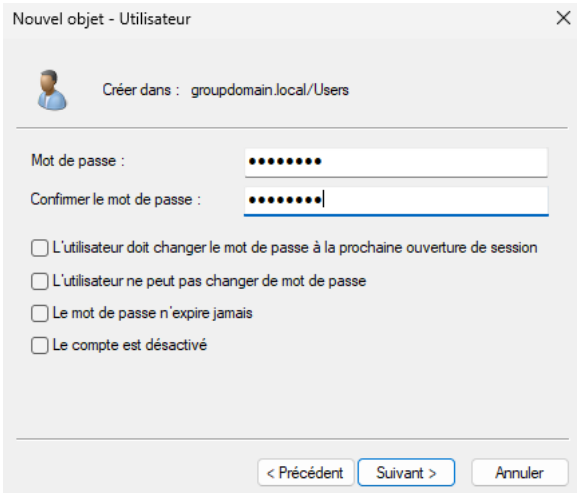
4 – Ajout d'un utilisateur dans le domaine

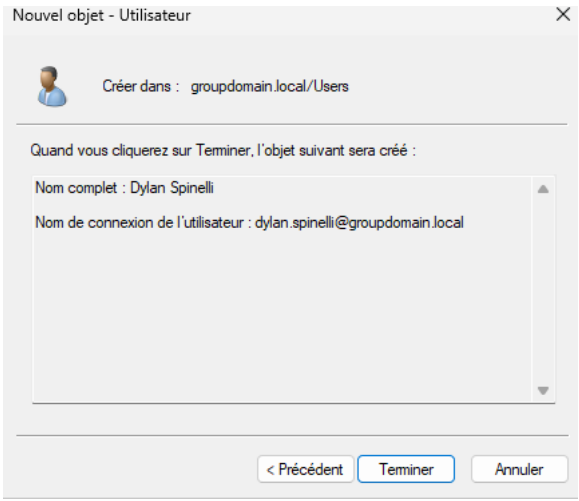
Nous allons maintenant rajouter un utilisateur dans le domaine :

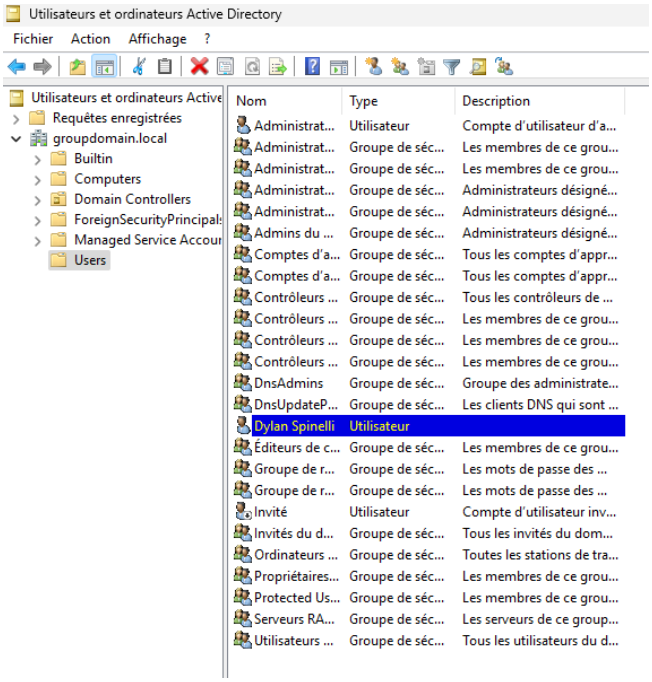


On définit le nom, prénom, le nom de la session ainsi qu'un mot de passe :





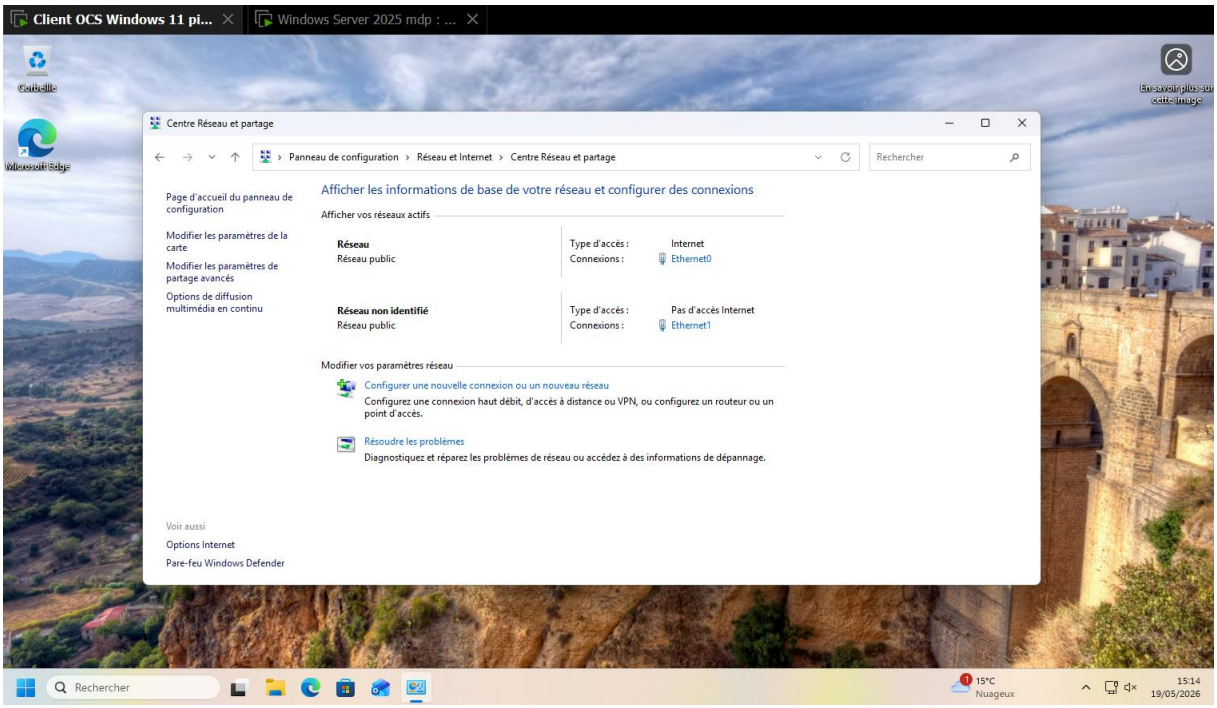




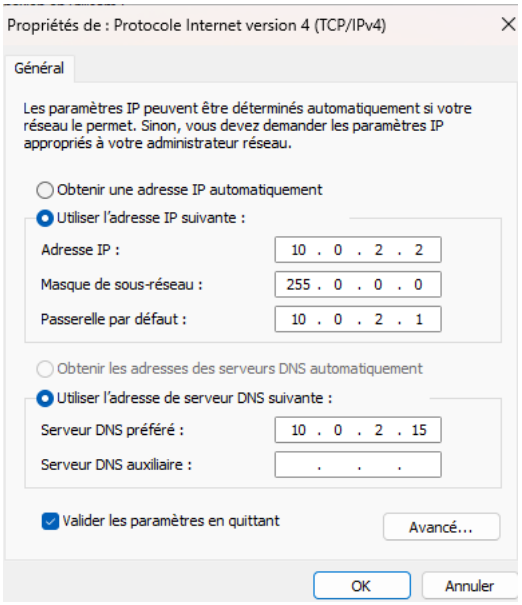
L'utilisateur a bien été crée dans le domaine.

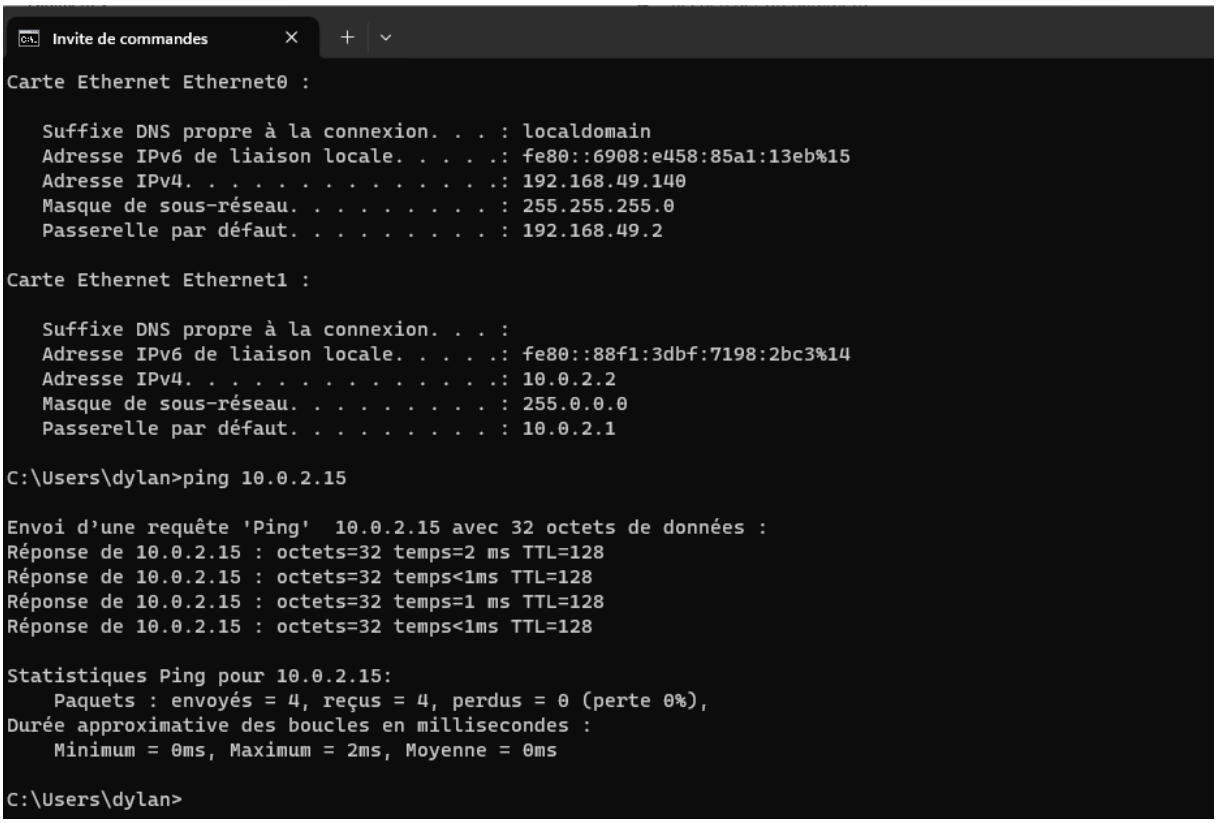
5 – Ajout d’un PC dans le domaine

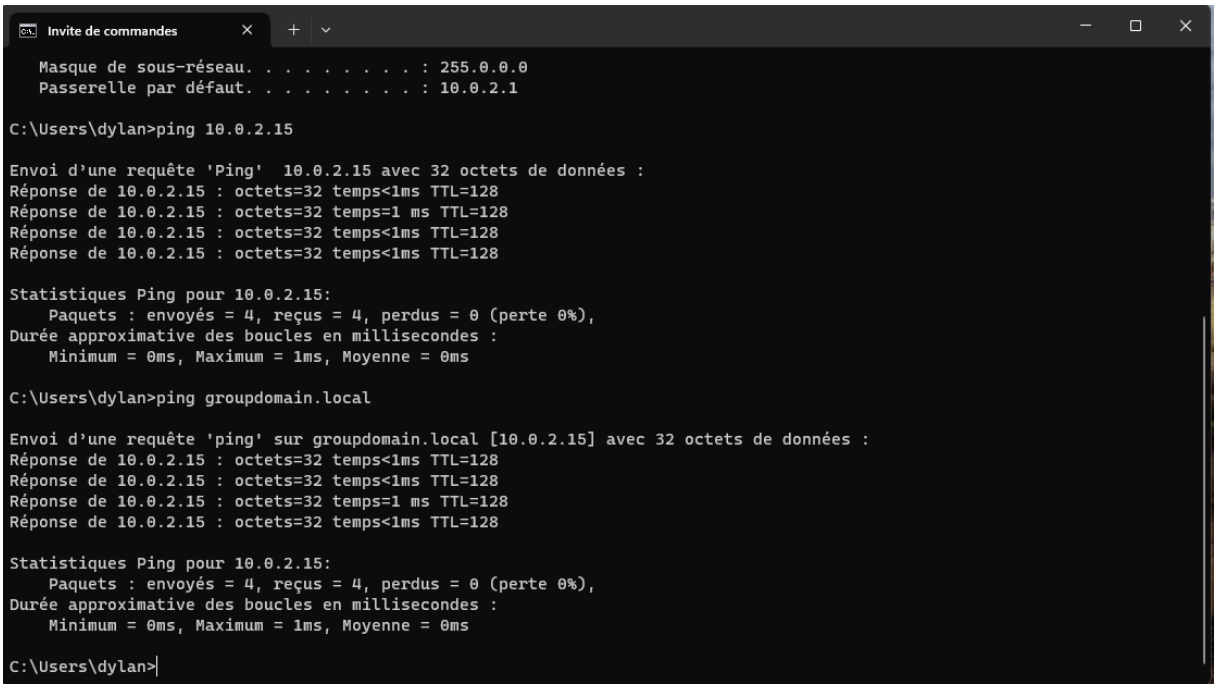
On ajoute sur notre machine cliente Windows 11 une carte réseau :



On lui configure une adresse IP dans le réseau de notre domaine :

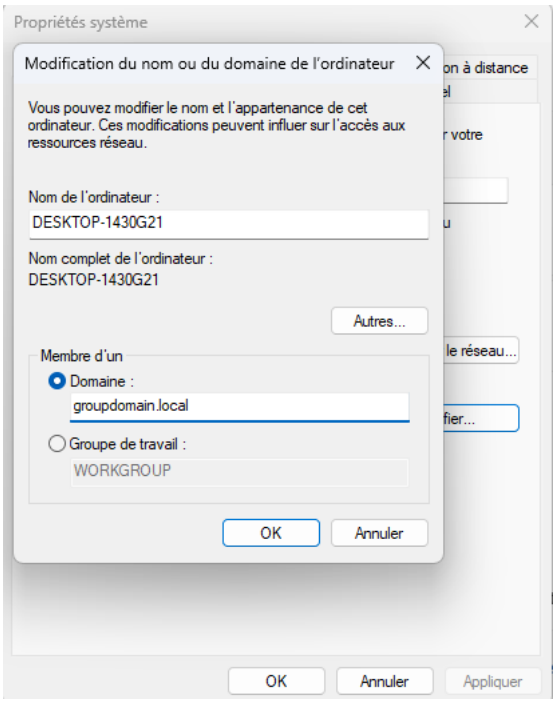




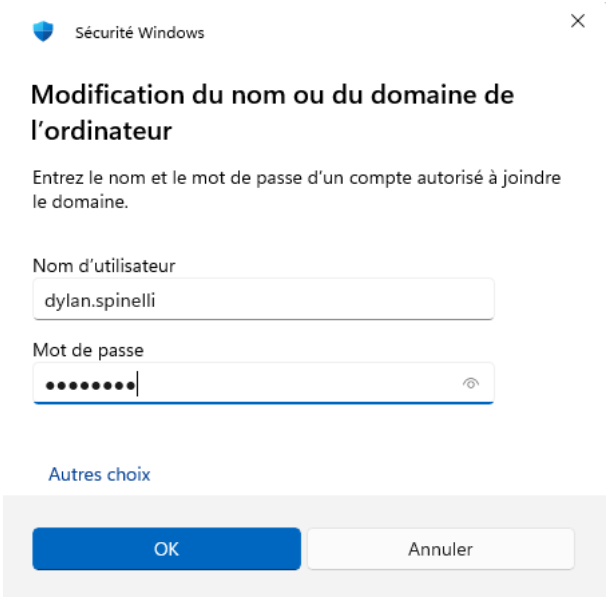


Notre machine est bien dans le même réseau que notre contrôleur de domaine. Nous pouvons donc désormais l'ajouter au domaine.

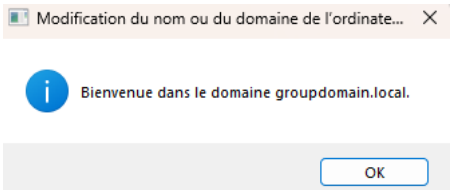
On renseigne le domaine « groupdomain.local » :



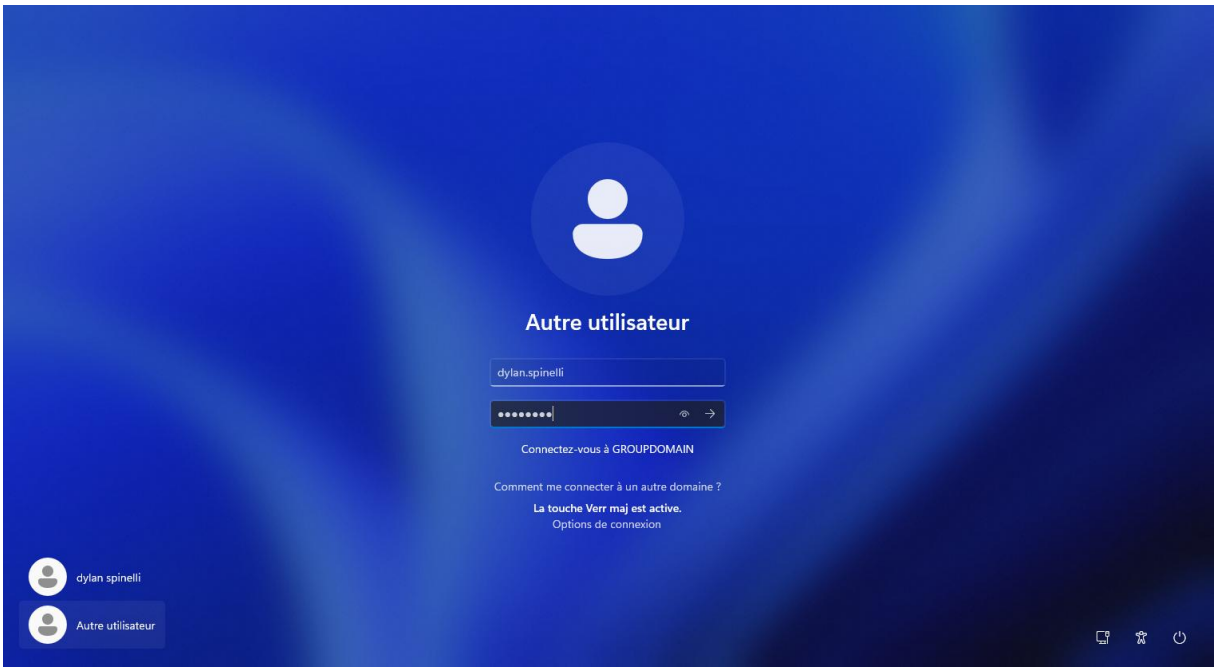
On se connecte avec notre profil crée précédemment :



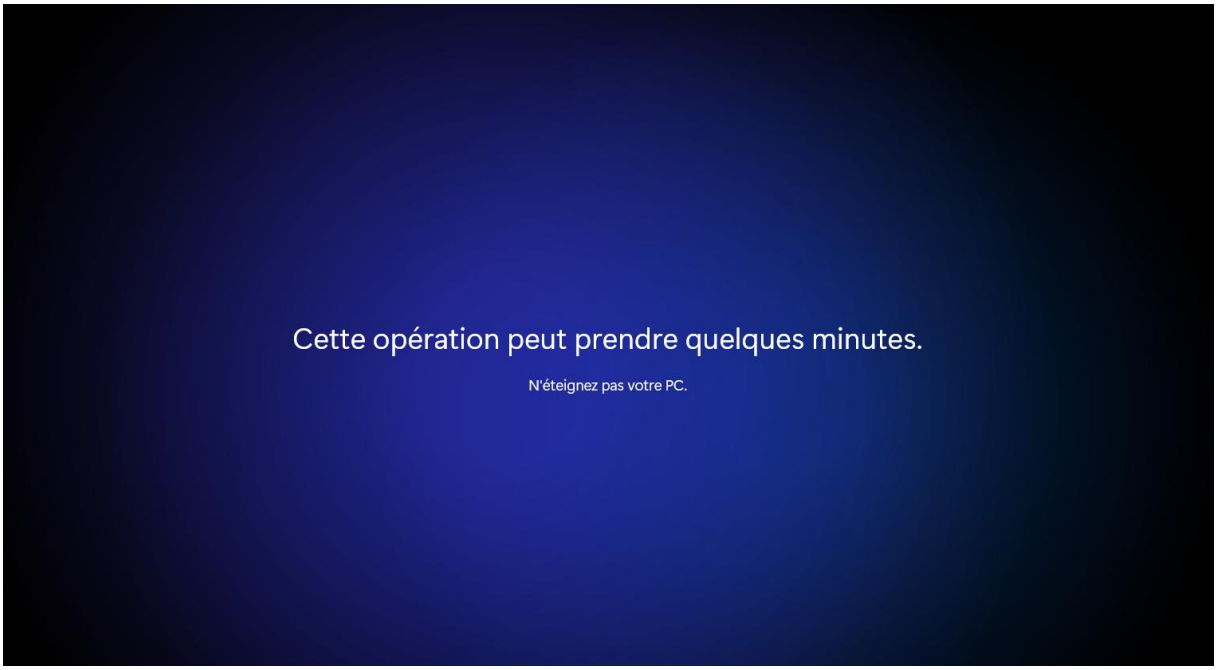
Le PC est désormais dans le domaine :

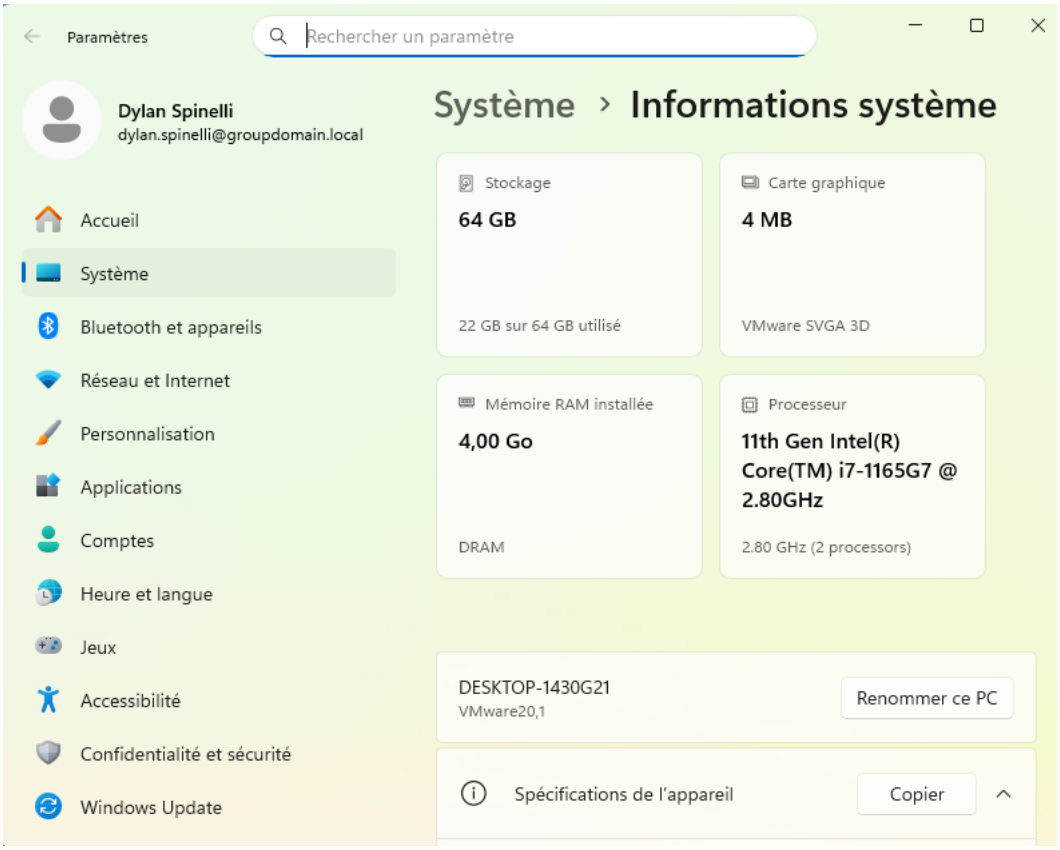


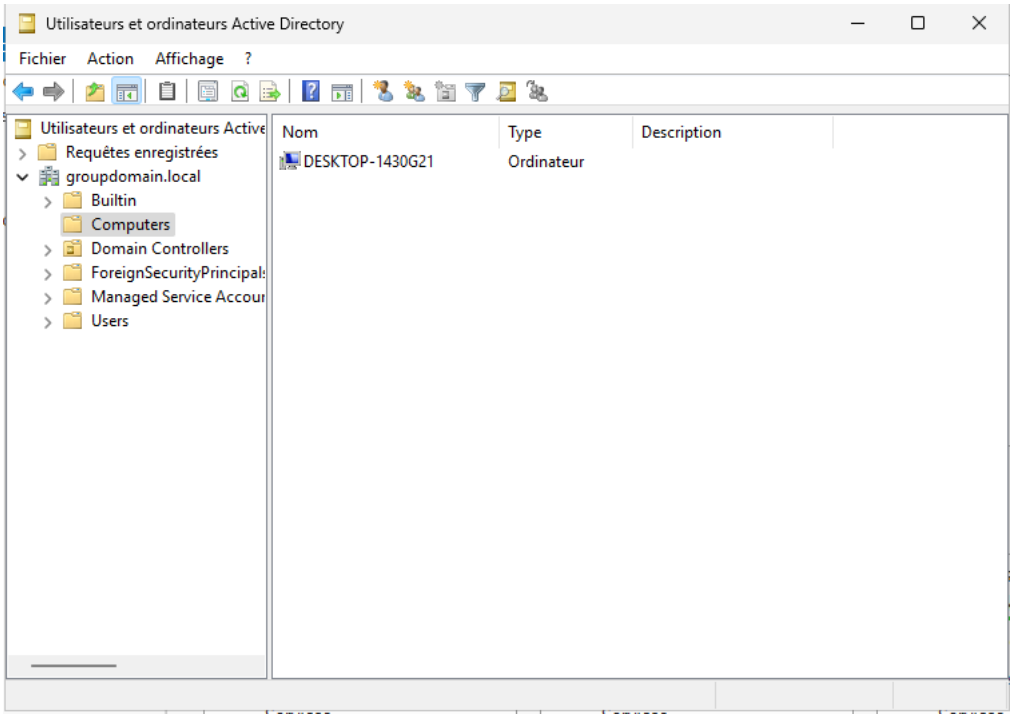
Après redémarrage, essayons de nous connecter à notre profil sur le domaine :



Notre session s'ouvre correctement :





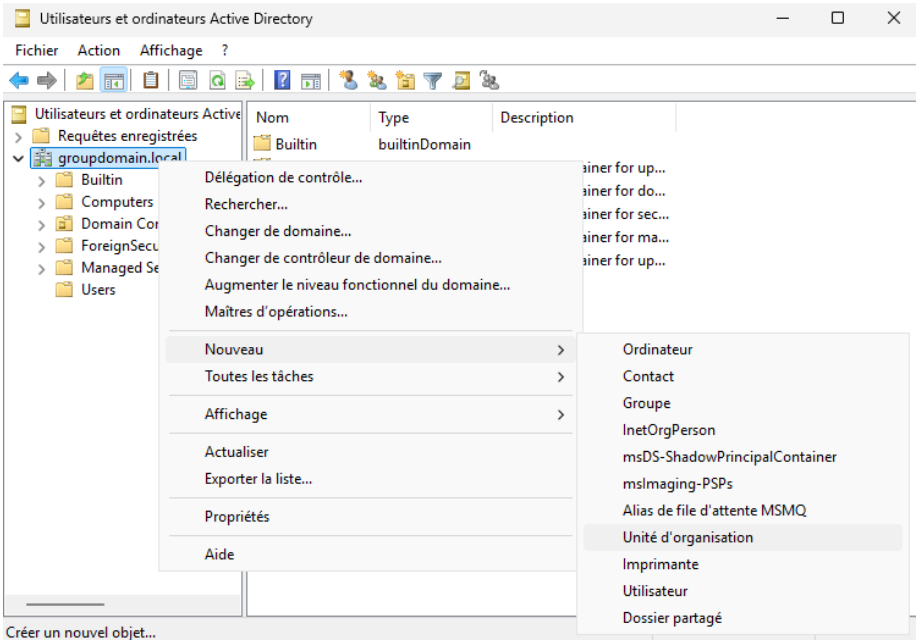


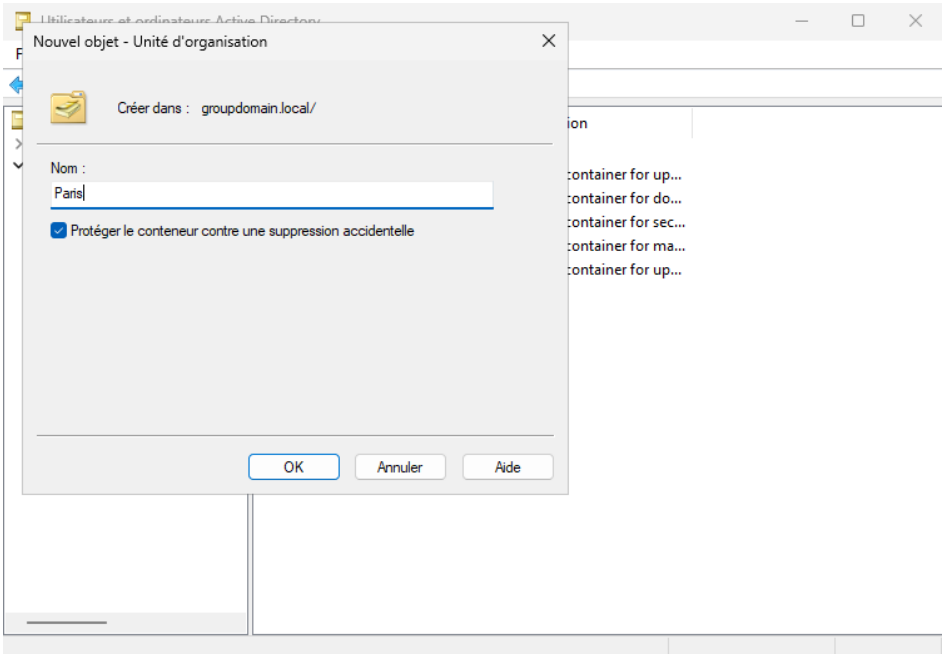
On retrouve bien notre PC dans le domaine Active Directory.

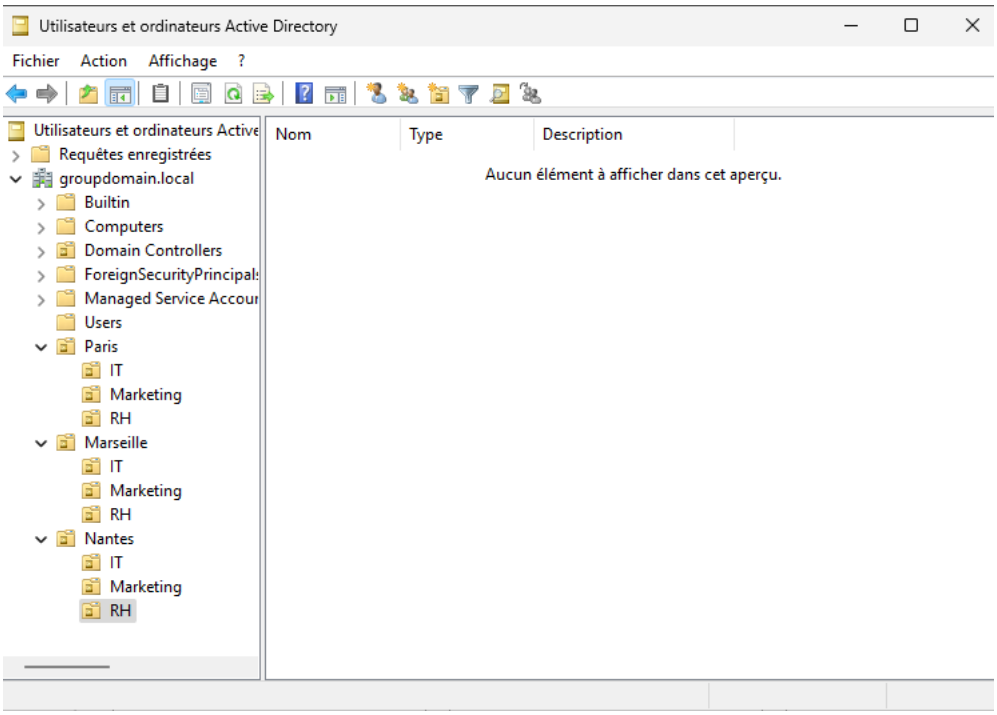
6 – Ajout des Unités d'organisation (UO)

On peut créer des unités d'organisation dans Active Directory afin d'organiser nos ressources selon la configuration d'une entreprise.

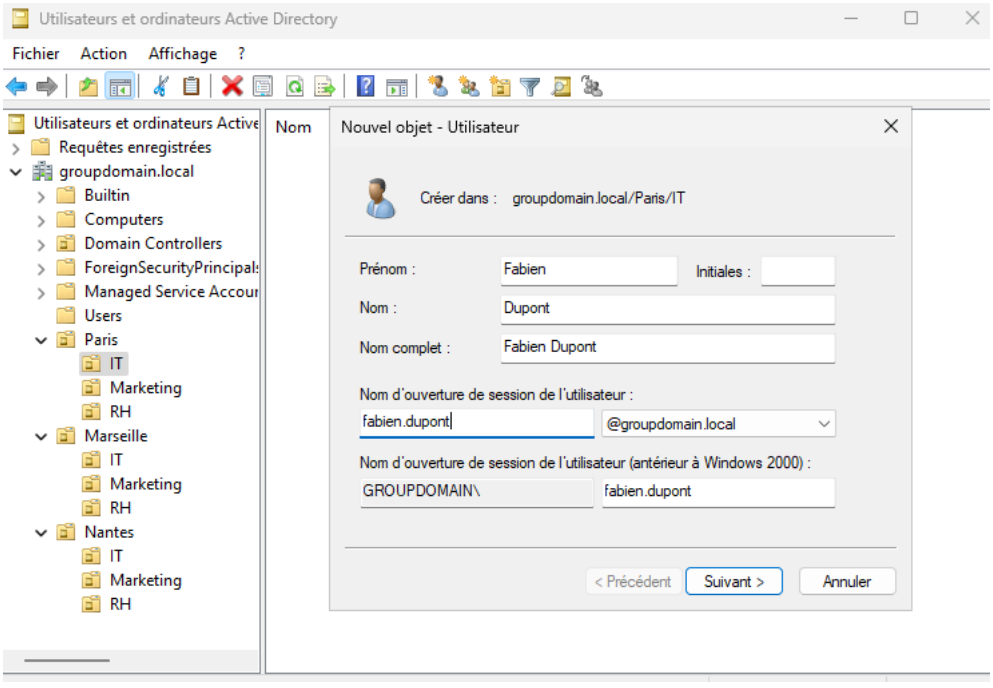
Pour ce projet, nous allons créer des unités d'organisation pour 3 sites : Paris, Marseille et Nantes ainsi que 3 services : IT, Marketing et RH

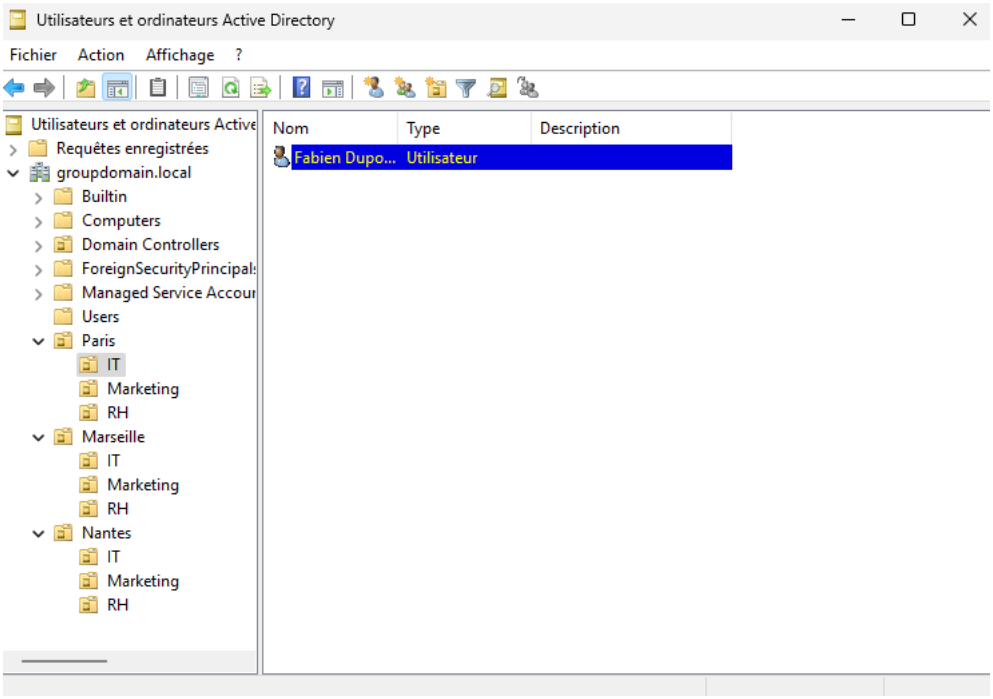






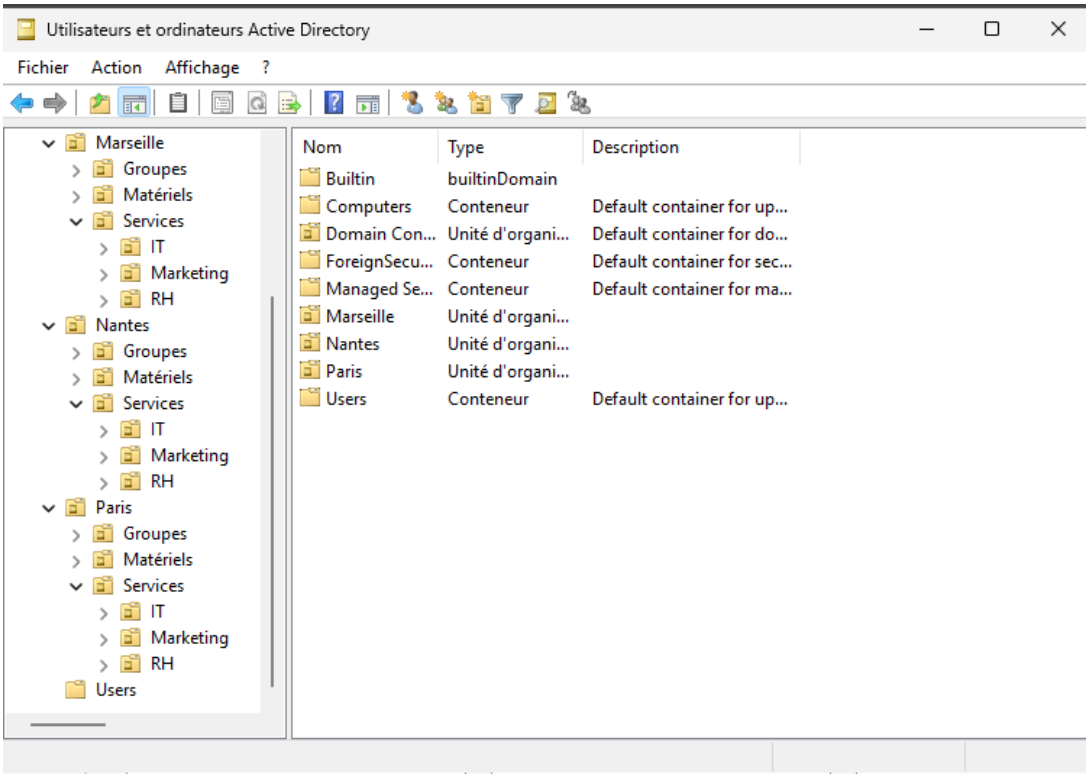
On peut désormais créer des utilisateurs dans ces groupes. Par exemple, créons un utilisateur dans le service IT de Paris :





L'utilisateur est désormais créé.

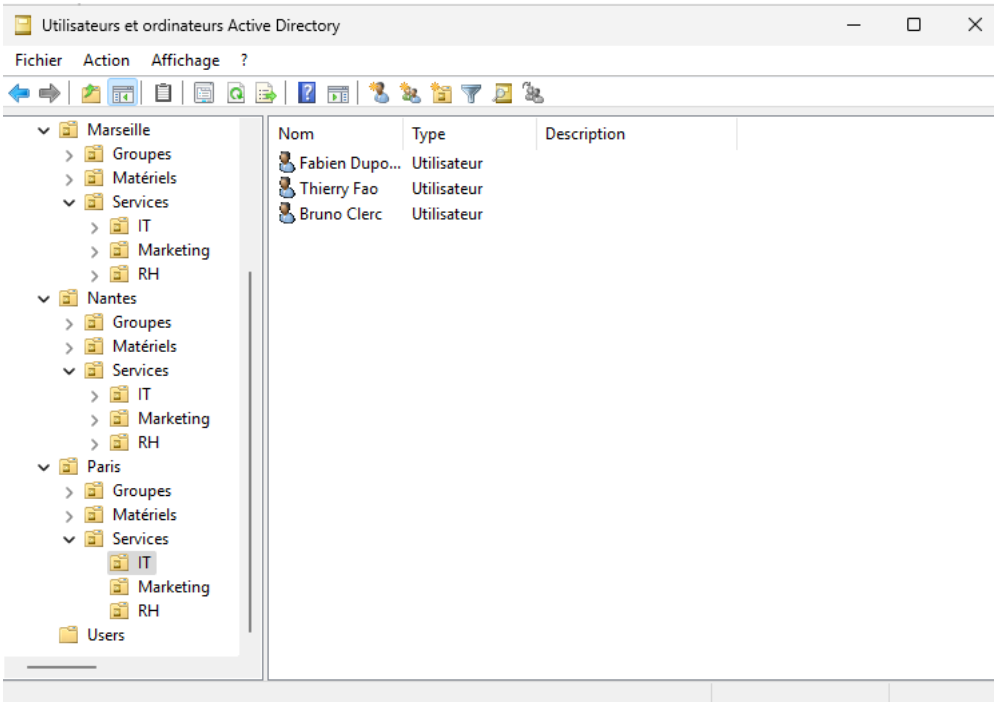
On décide de rassembler les différents services dans une UO « services » et de créer pour chaque site les unités d'organisation « groupes » et « matériels » :

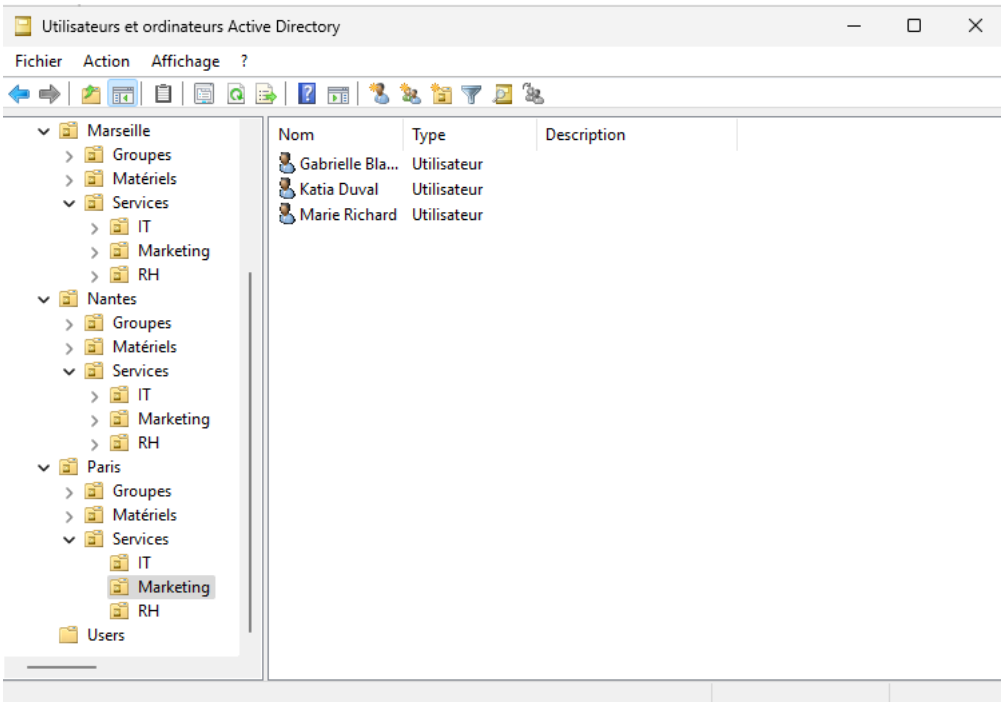


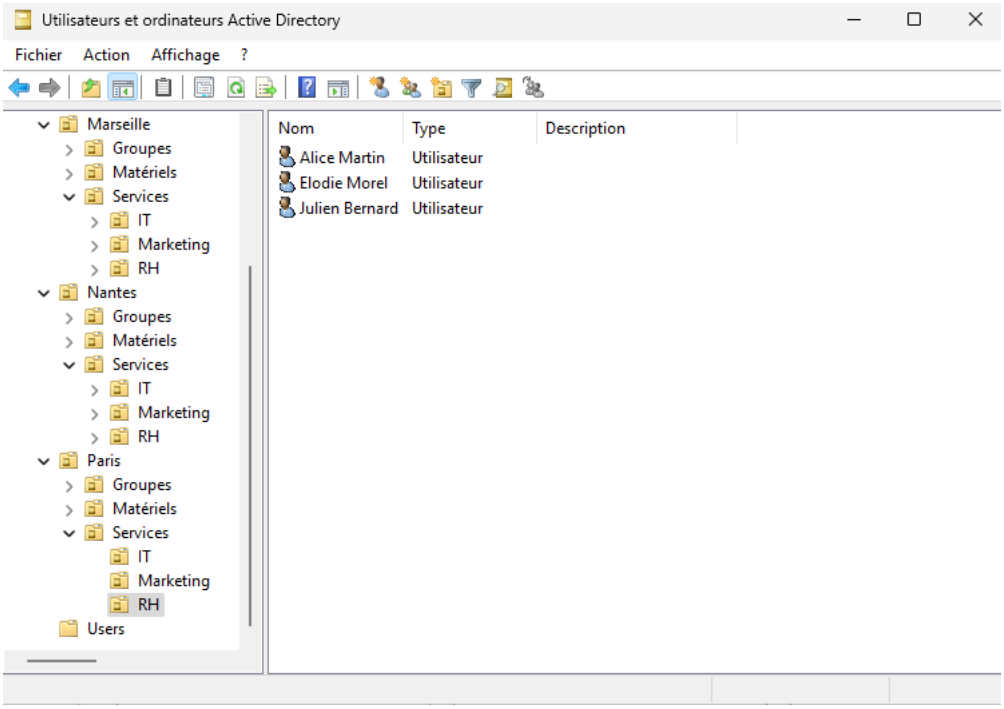
7- Ajout de groupes d’utilisateurs

7.1 – Création des groupes globaux

Concentrons-nous sur le site de Paris. Des utilisateurs ont été ajoutés pour chaque service :

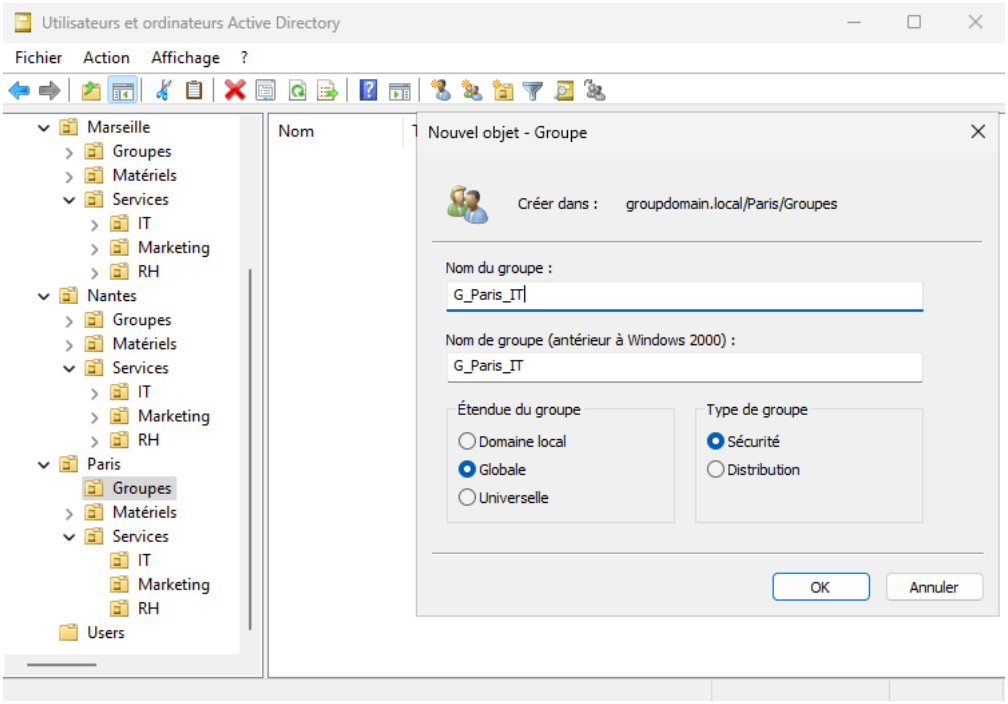


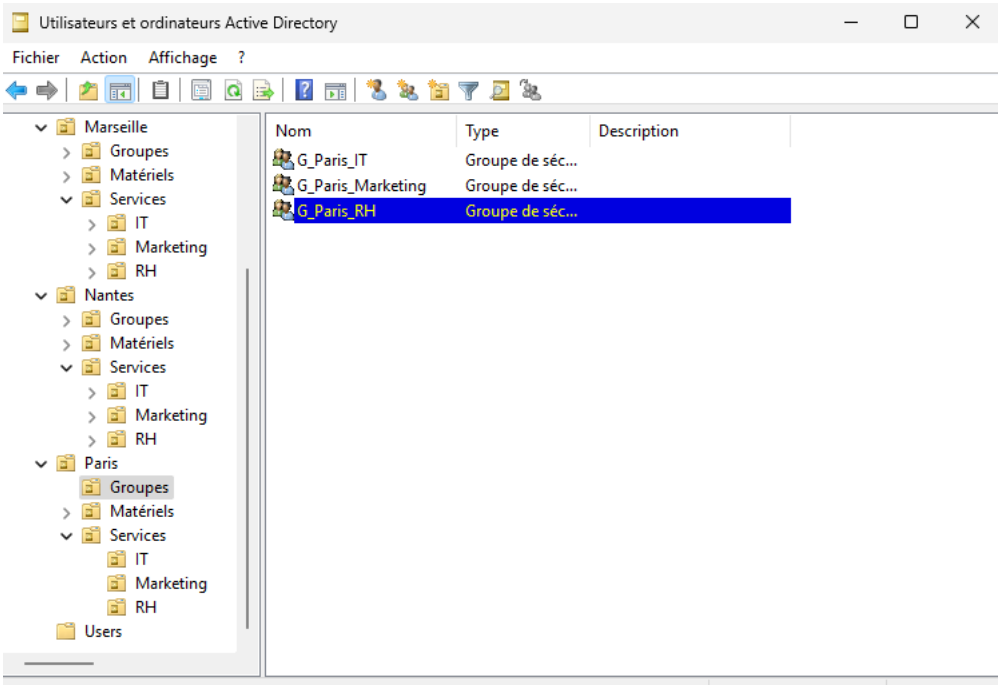




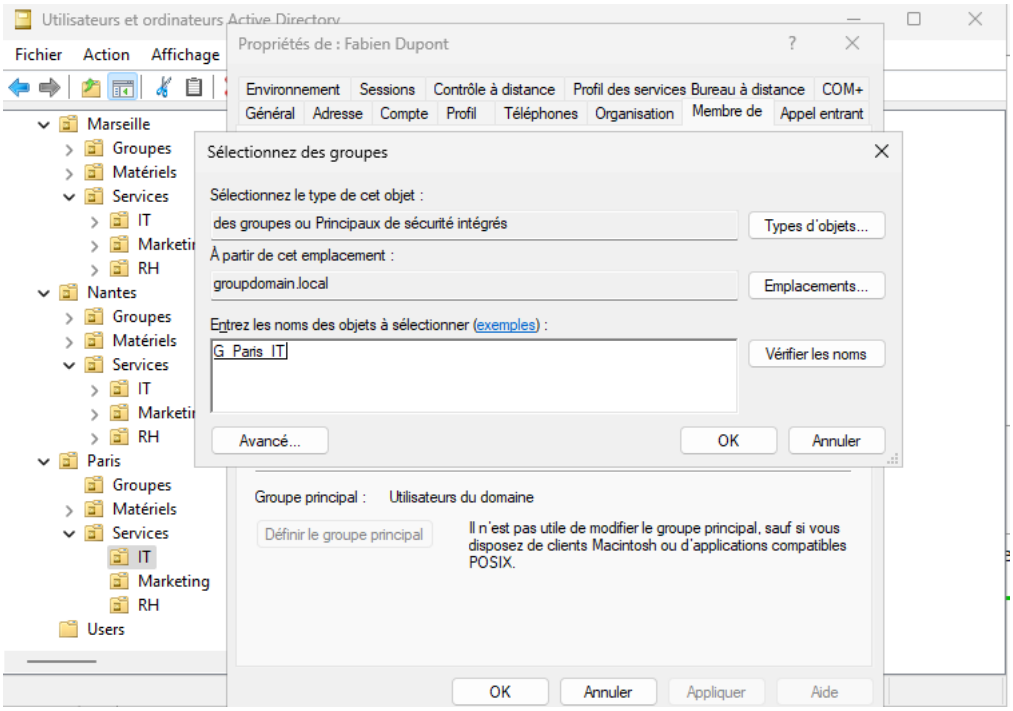
Nous allons donc regrouper ces utilisateurs dans des groupes qui correspondent à leur service.

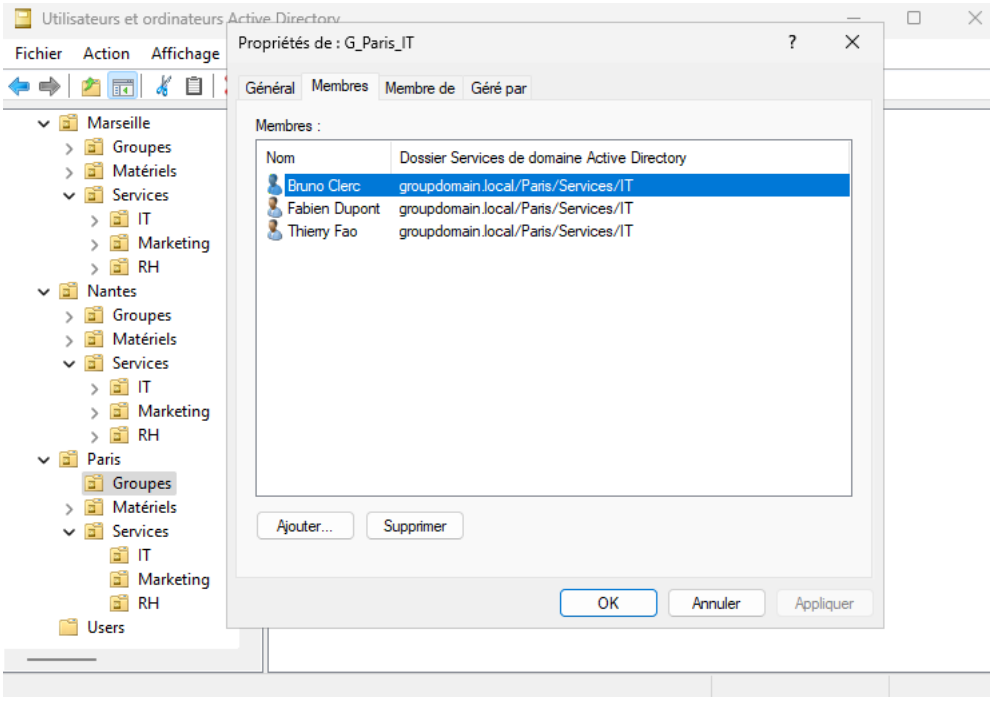
On crée des groupes de type global pour regrouper nos utilisateurs :





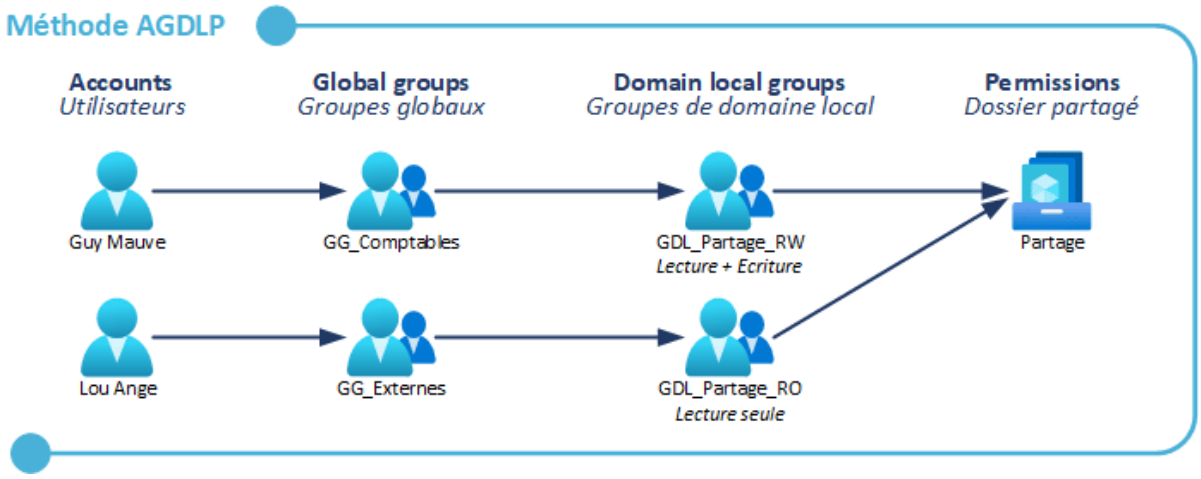
On peut ensuite ajouter les utilisateurs dans chaque groupe correspondant :




Utilisateurs et ordinateurs Active Directory
Fichier
Action
Affichage
Marseille
Groupes
Matériels
Services
IT
Marketing
RH
Nantes
Groupes
Matériels
Services
IT
Marketing
RH
Paris
Groupes
Matériels
Services
IT
Marketing
RH
Users
Propriétés de : G_Paris_IT
Général
Membres
Membre de
Géré par
Membres :
Nom
Dossier Services de domaine Active Directory
Bruno Clerc
groupdomain.local/Paris/Services/IT
Fabien Dupont
groupdomain.local/Paris/Services/IT
Thierry Fao
groupdomain.local/Paris/Services/IT
Ajouter...
Supprimer
OK
Annuler
Appliquer

7.2 – Ajout des droits AGDLP

Voici la méthode AGDLP :

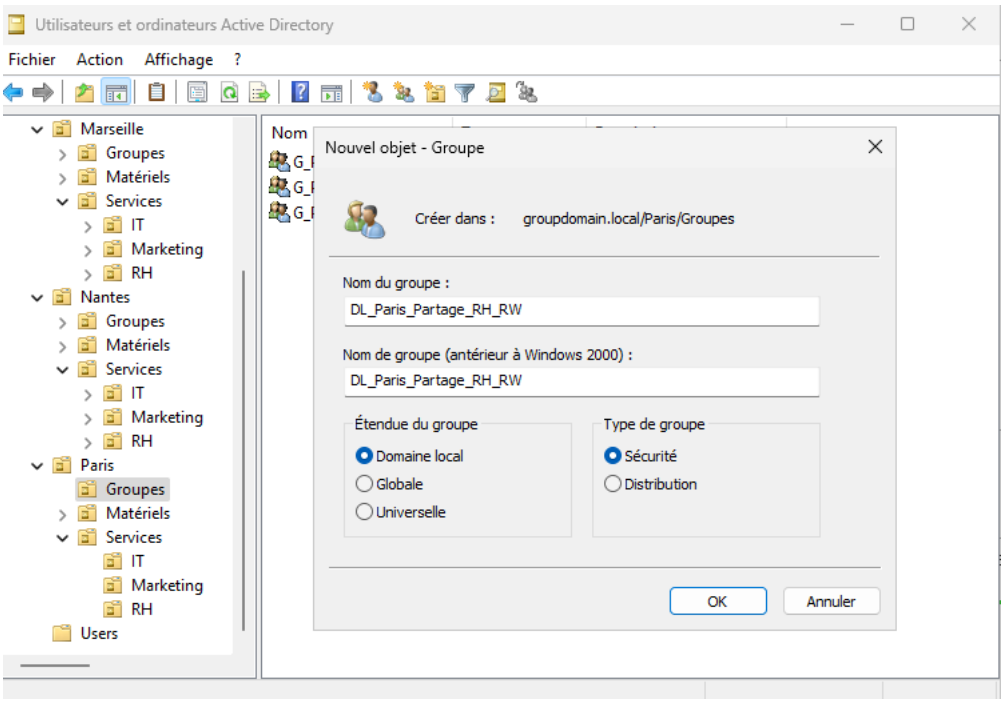


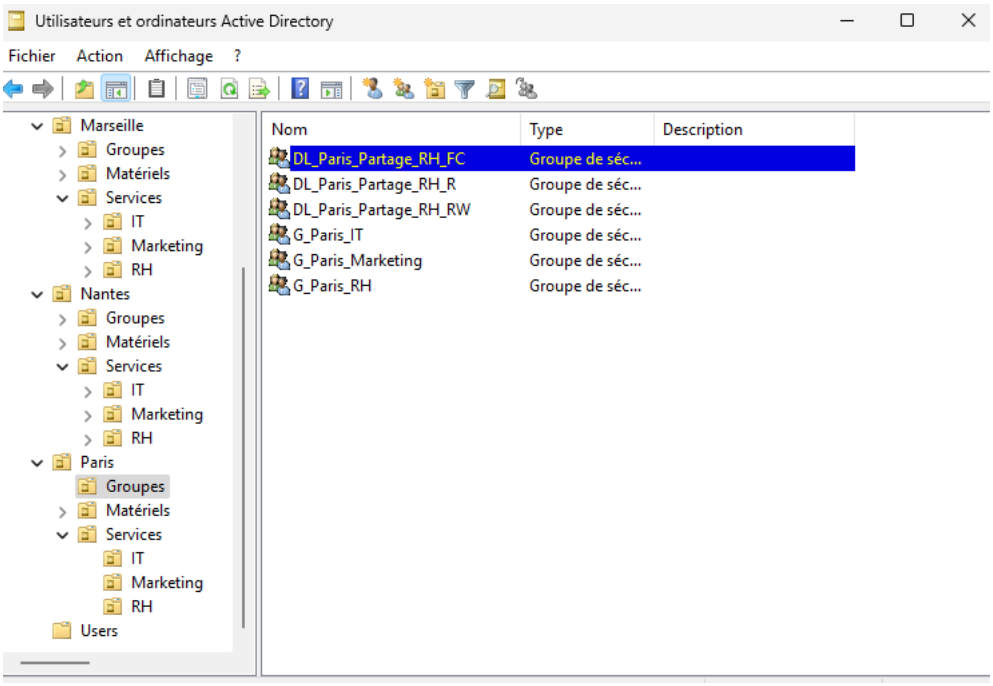
Nous avons créé des groupes globaux précédemment.

Nous allons donc désormais créer des fichiers partagés ainsi que des groupes de domaine local. Les groupes de domaine local permettent de définir les autorisations sur les ressources.

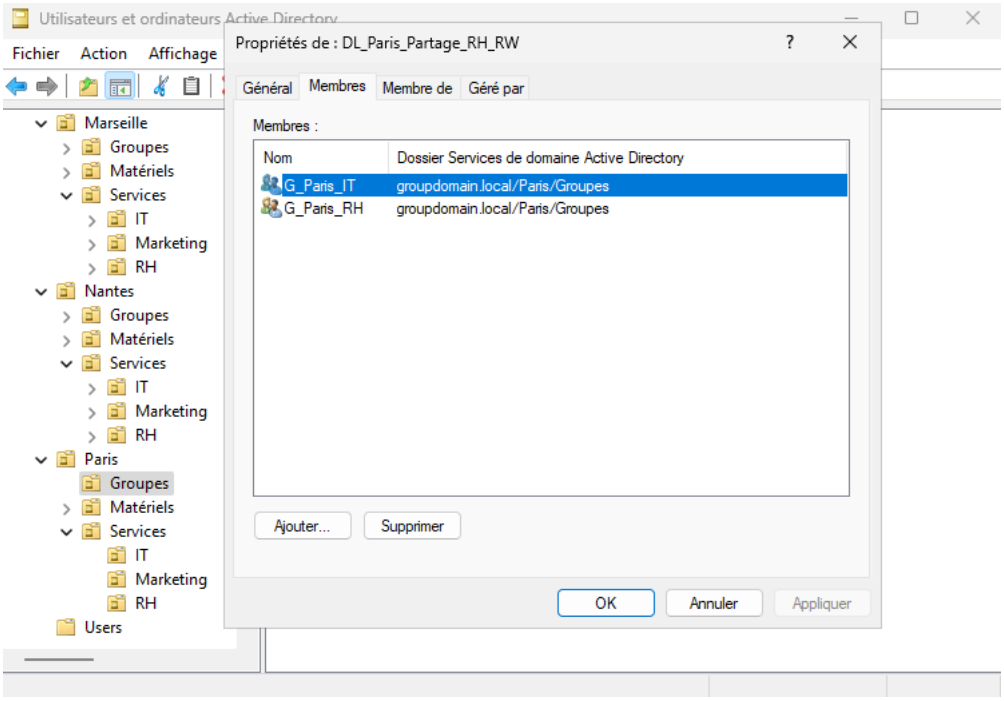
3 groupes de domaine local seront donc crées afin de définir les permissions aux utilisateurs sur le dossier partagé « Partage_RH » :

- RW : Permissions de lecture et écriture
- R : Permissions de lecture
- FC : Contrôle total

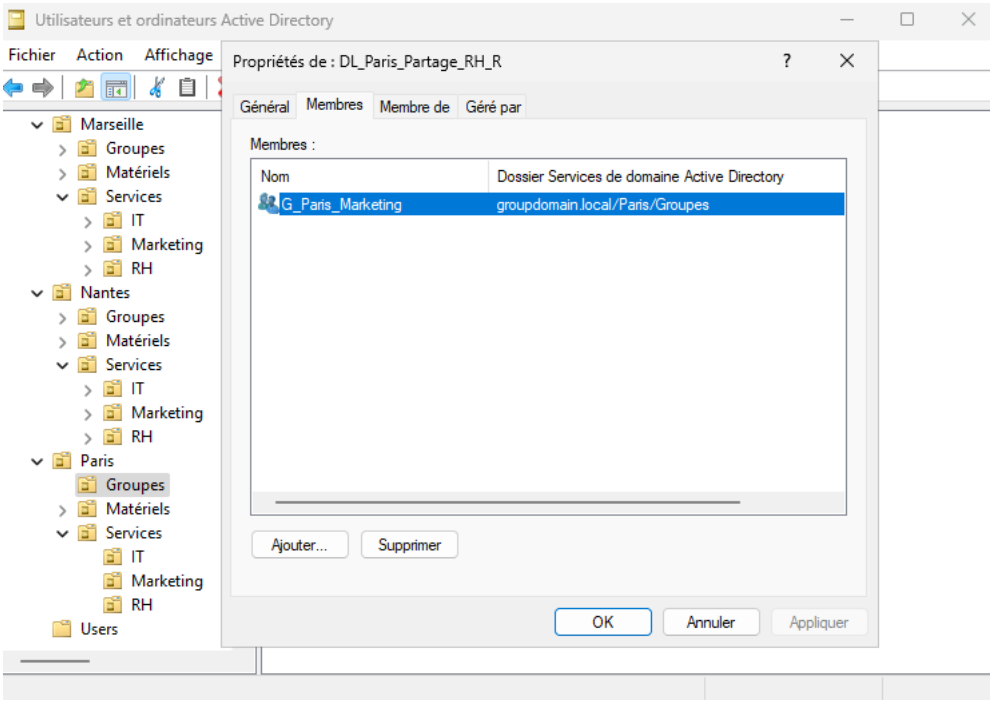




On inclut les groupes globaux IT et RH dans le groupe domaine local RW pour leur donner les permissions en lecture et écriture :

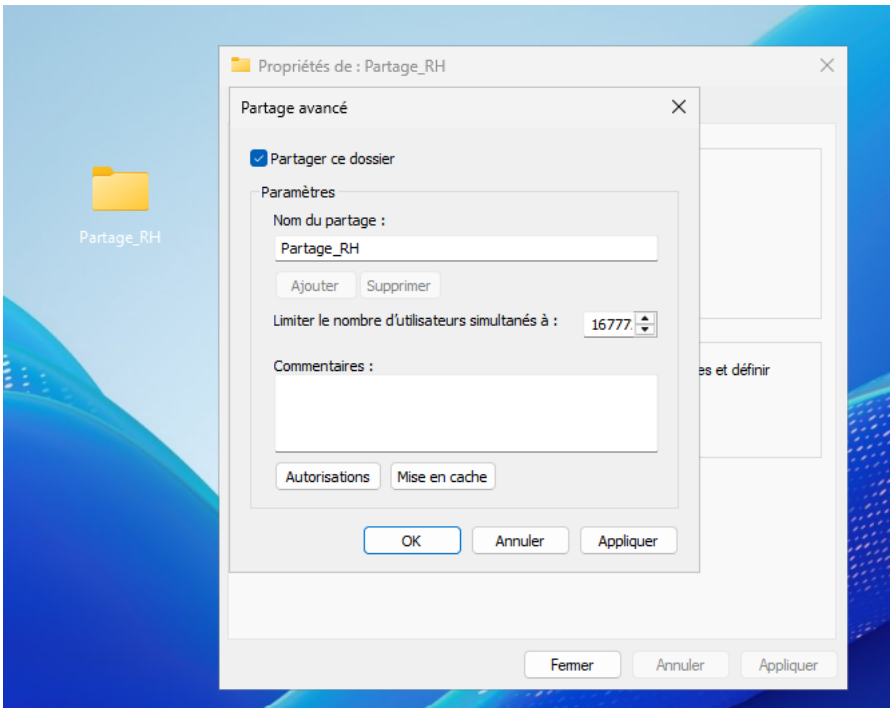


On inclut dans le groupe de domaine local R le service Marketing car nous souhaitons leur donner des permissions de lecture uniquement :

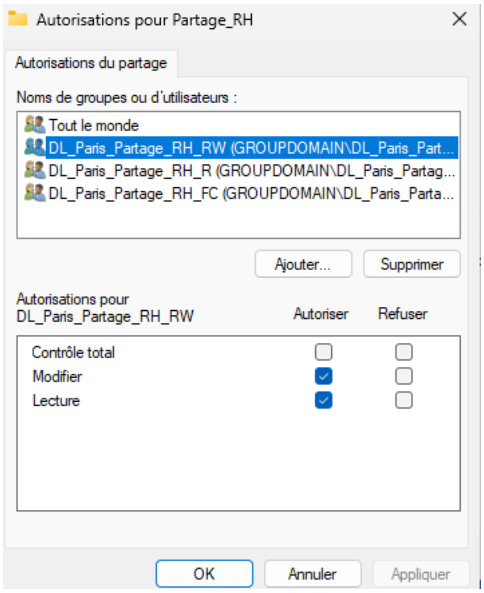


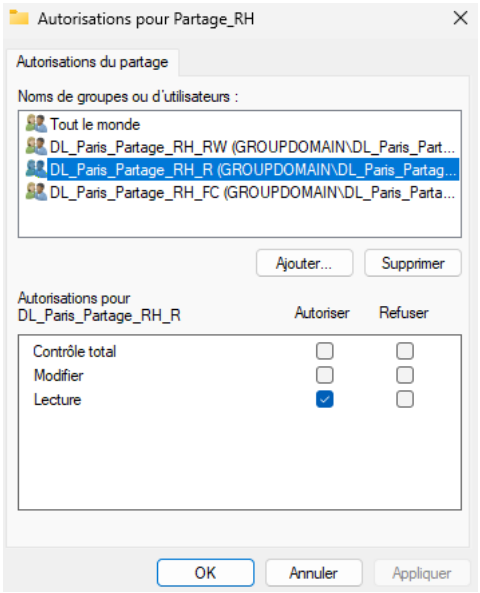
7.3 – Création du dossier partagé avec les droits AGDLP

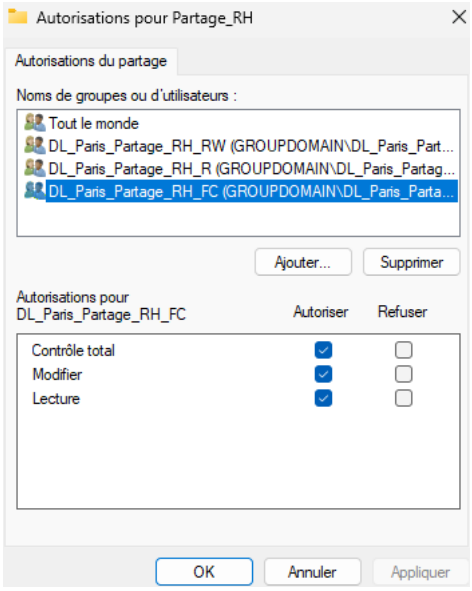
On crée désormais le dossier partagé sur le réseau Partage_RH :



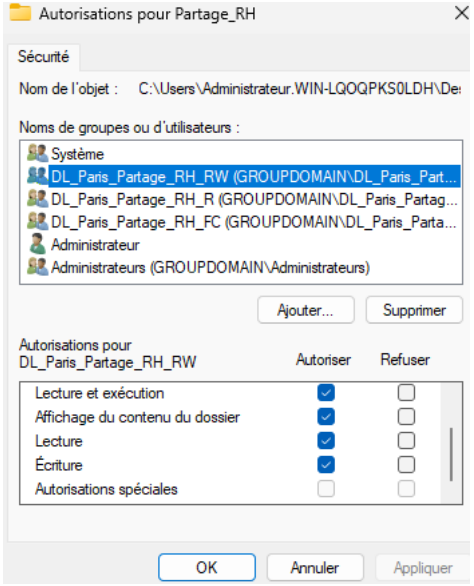
On définit les permissions pour les 3 groupes de domaine local :

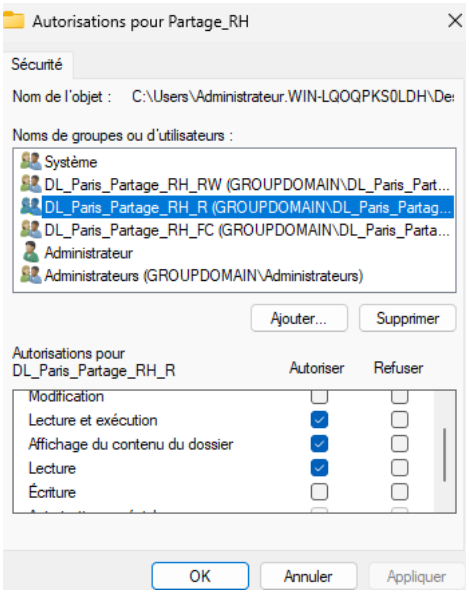


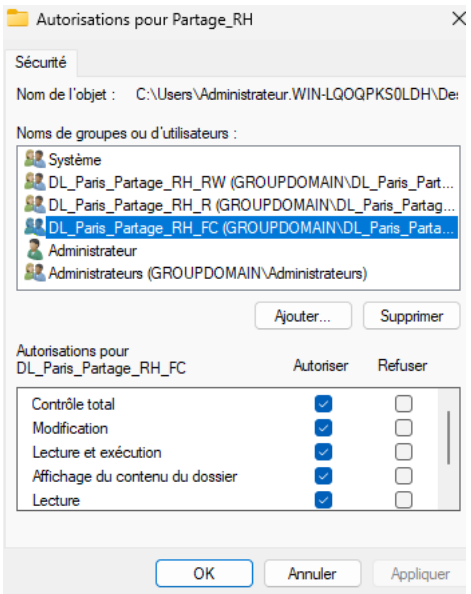

Autorisations pour Partage_RH
Autorisations du partage
Noms de groupes ou d'utilisateurs :
Tout le monde
DL_Paris_Partage_RH_RW (GROUPDOMAIN\DL_Paris_Part...
DL_Paris_Partage_RH_R (GROUPDOMAIN\DL_Paris_Partag...
DL_Paris_Partage_RH_FC (GROUPDOMAIN\DL_Paris_Parta...
Ajouter...
Supprimer
Autorisations pour DL_Paris_Partage_RH_R
Autoriser
Refuser
Contrôle total
Modifier
Lecture
OK
Annuler
Appliquer


Autorisations pour Partage_RH
Autorisations du partage
Noms de groupes ou d'utilisateurs :
Tout le monde
DL_Paris_Partage_RH_RW (GROUPDOMAIN\DL_Paris_Part...
DL_Paris_Partage_RH_R (GROUPDOMAIN\DL_Paris_Partag...
DL_Paris_Partage_RH_FC (GROUPDOMAIN\DL_Paris_Parta...
Ajouter...
Supprimer
Autorisations pour DL_Paris_Partage_RH_FC
Autoriser
Refuser
Contrôle total
Modifier
Lecture
OK
Annuler
Appliquer

On définit également les permissions dans l'onglet sécurité :

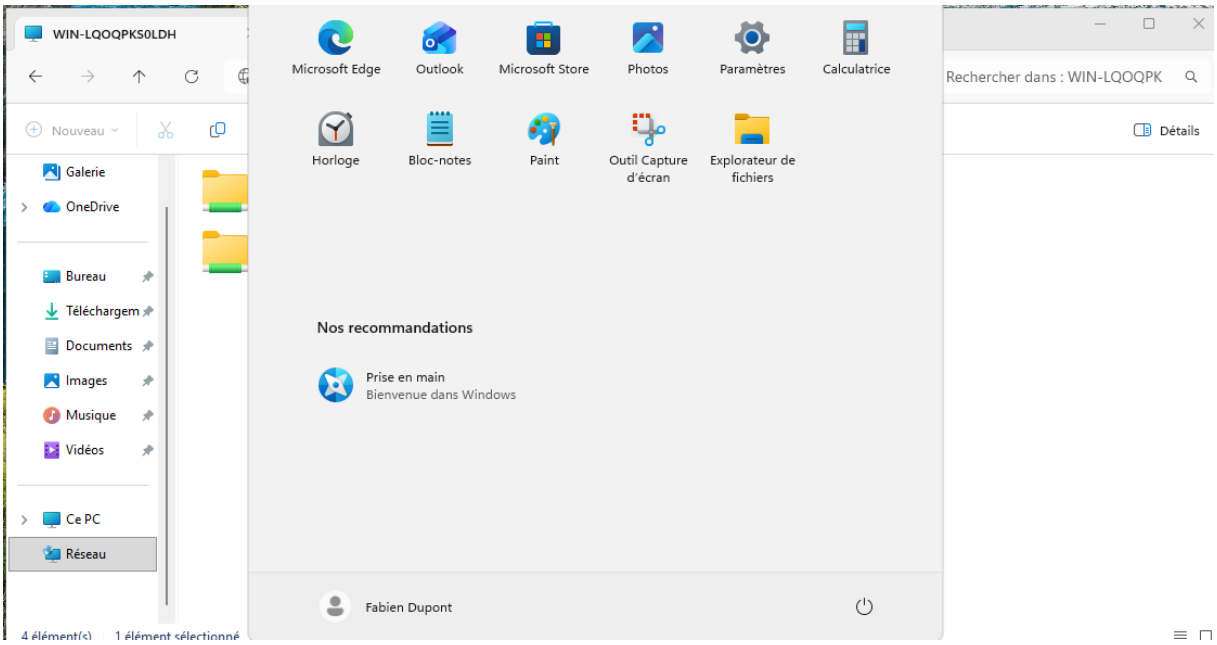


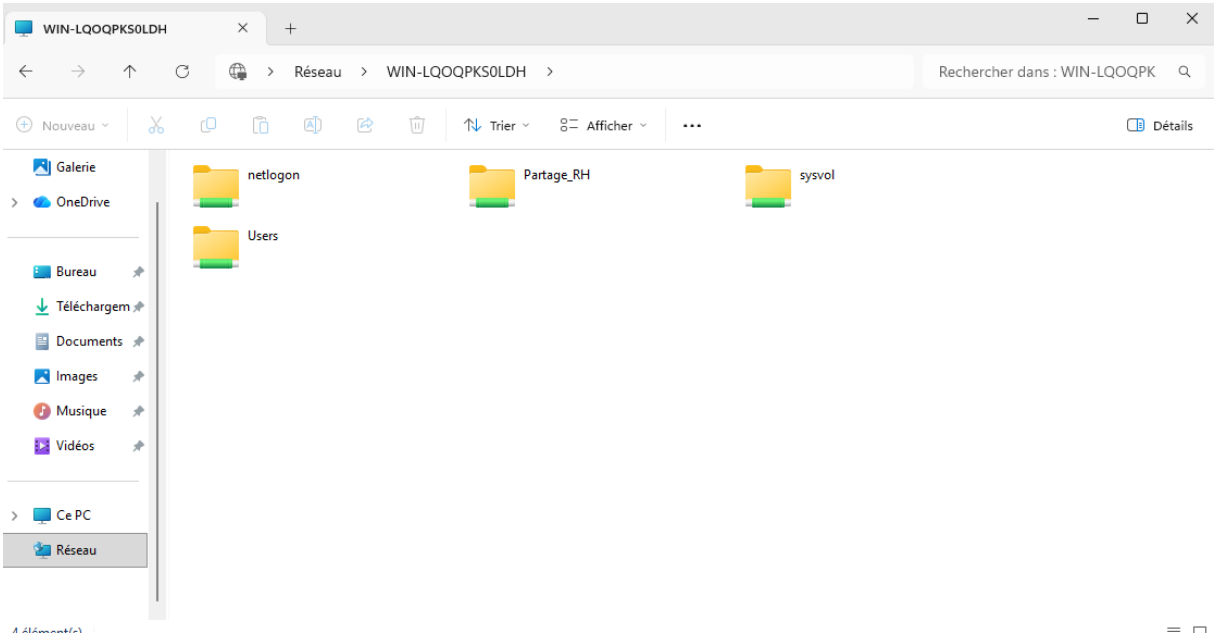




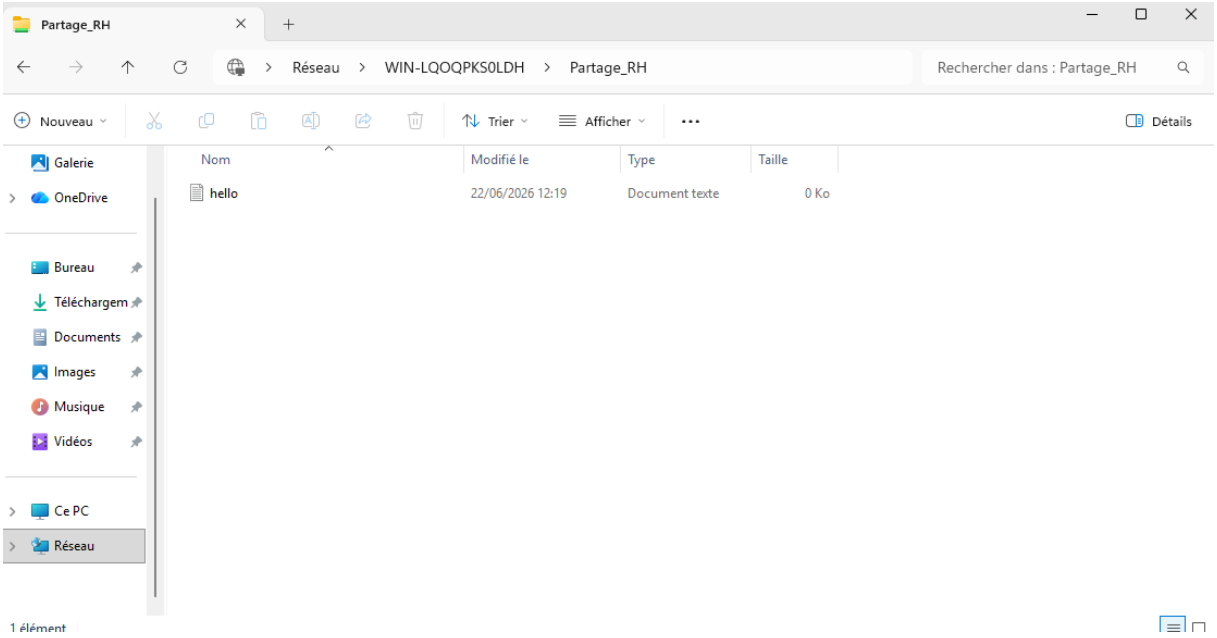
7.4 – Vérification des droits d’accès

Essayons d’accéder au dossier depuis la session d’un membre IT : Fabien Dupont

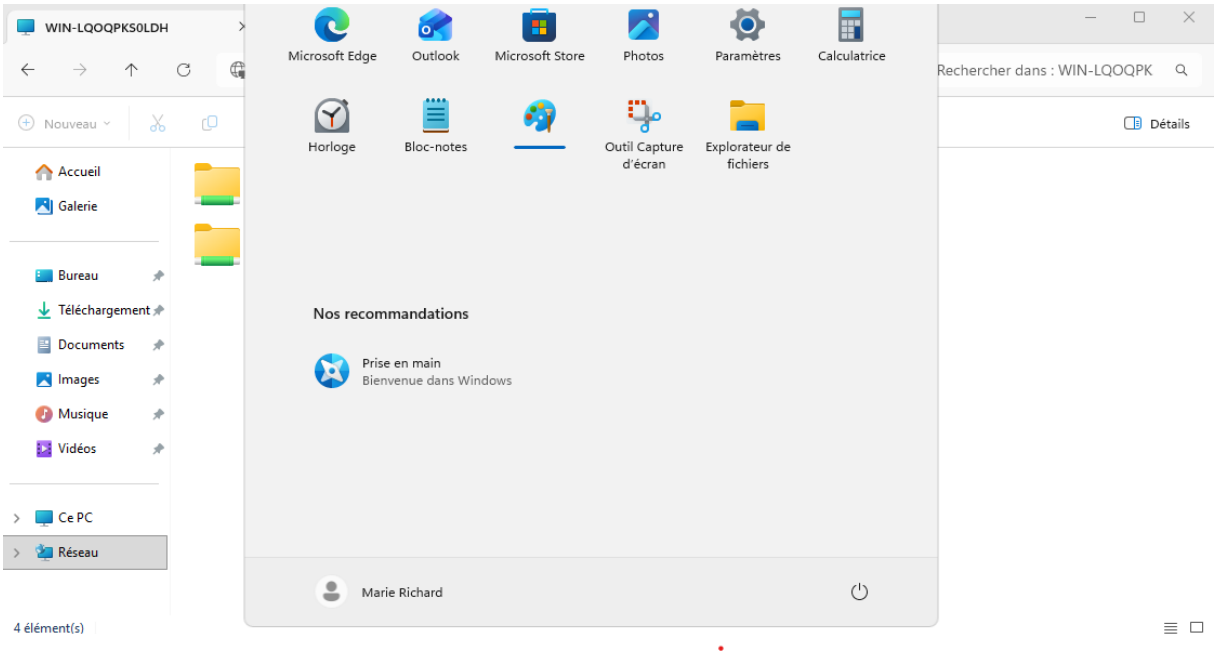


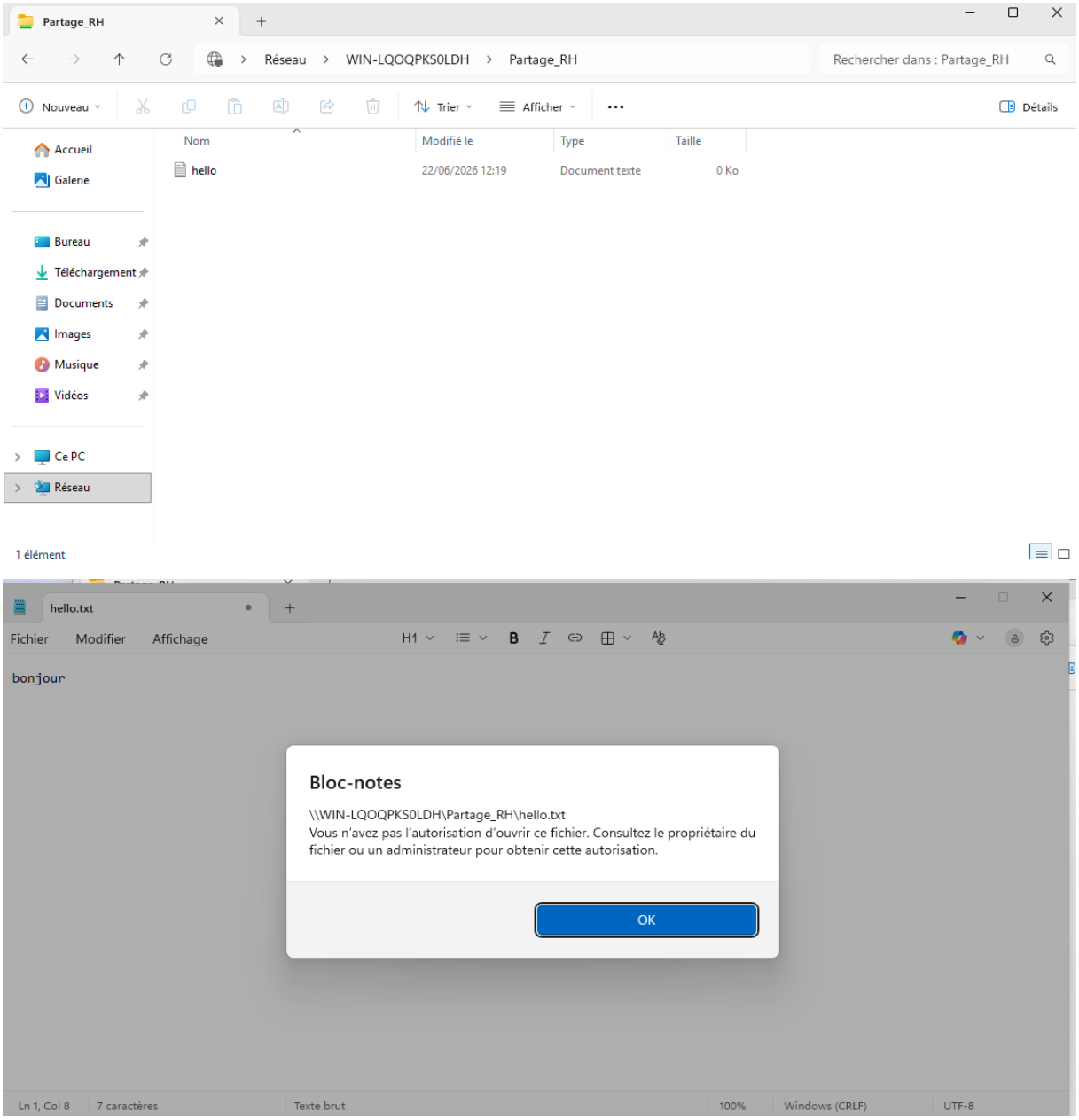


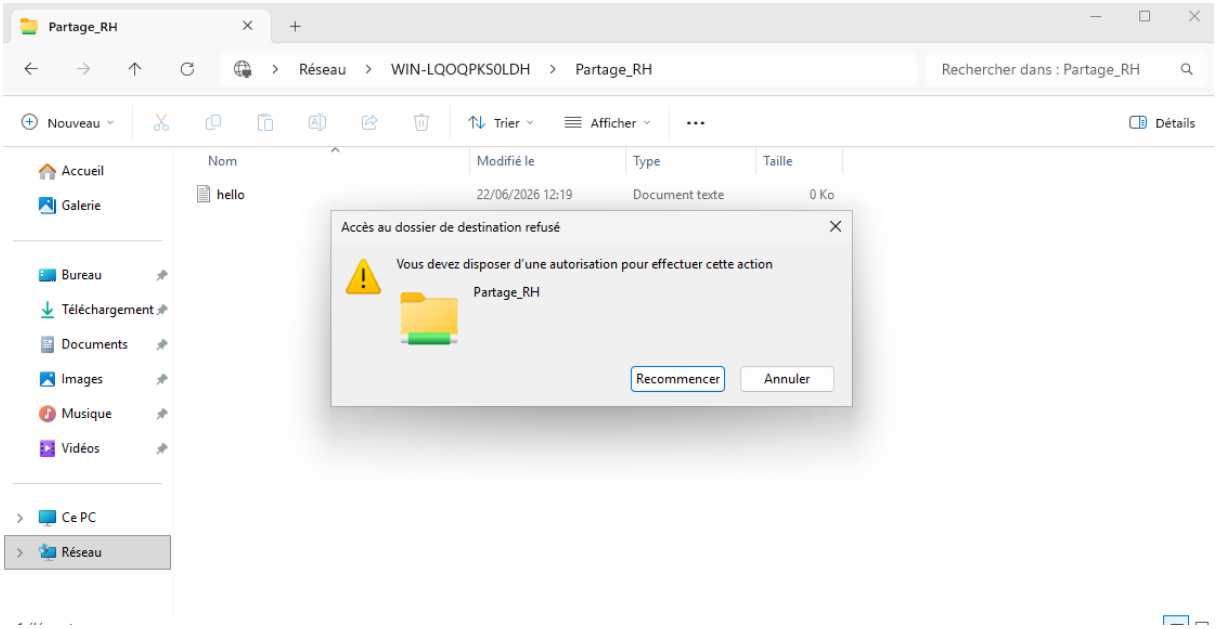
On peut bien accéder au dossier et modifier le contenu. On crée un fichier texte :



Connectons-nous maintenant depuis la session d'un utilisateur du service Marketing : Marie Richard




Partage_RH
Réseau
WIN-LQOQPKS0LDH
Partage_RH
Rechercher dans : Partage_RH
Nouveau
Trier
Afficher
Détails
Accueil
Galerie
Bureau
Téléchargement
Documents
Images
Musique
Vidéos
Ce PC
Réseau
Nom
Modifié le
Type
Taille
hello
22/06/2026 12:19
Document texte
0 Ko
1 élément
hello.txt
Fichier
Modifier
Affichage
H1
bonjour
Bloc-notes
\\WIN-LQOQPKS0LDH\Partage_RH\hello.txt
Vous n'avez pas l'autorisation d'ouvrir ce fichier. Consultez le propriétaire du fichier ou un administrateur pour obtenir cette autorisation.
OK
Ln 1, Col 8
7 caractères
Texte brut
100%
Windows (CRLF)
UTF-8

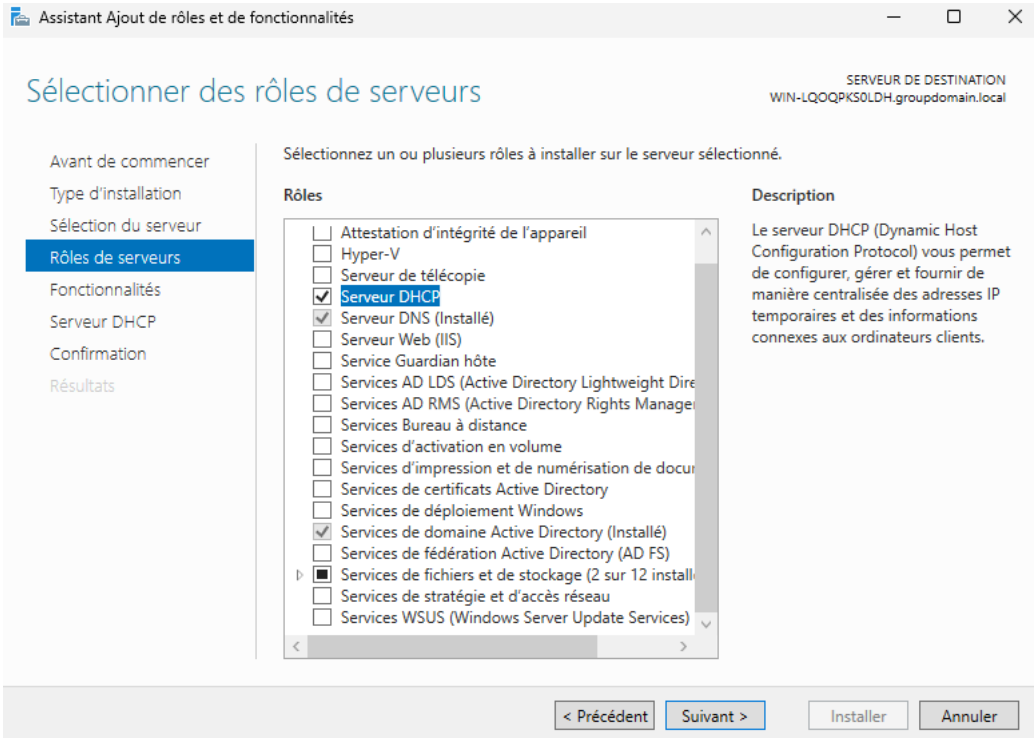


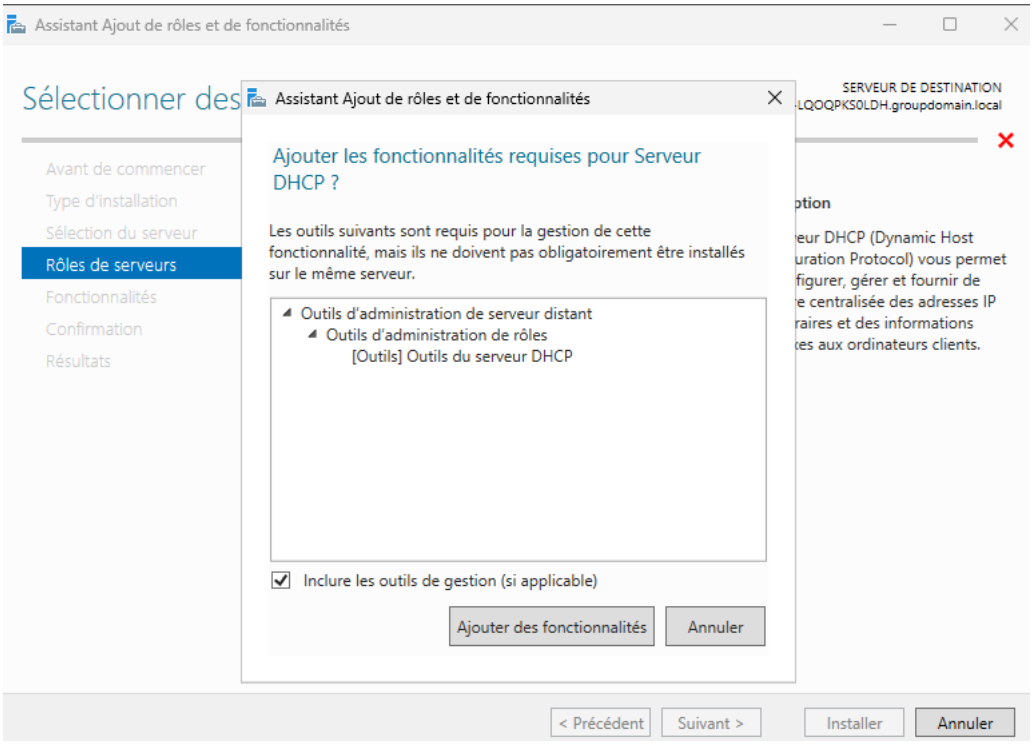
Nous pouvons bien accéder au dossier et consulter son contenu mais il est impossible de le modifier

8-Ajout du DHCP

8.1- Installation du rôle DHCP

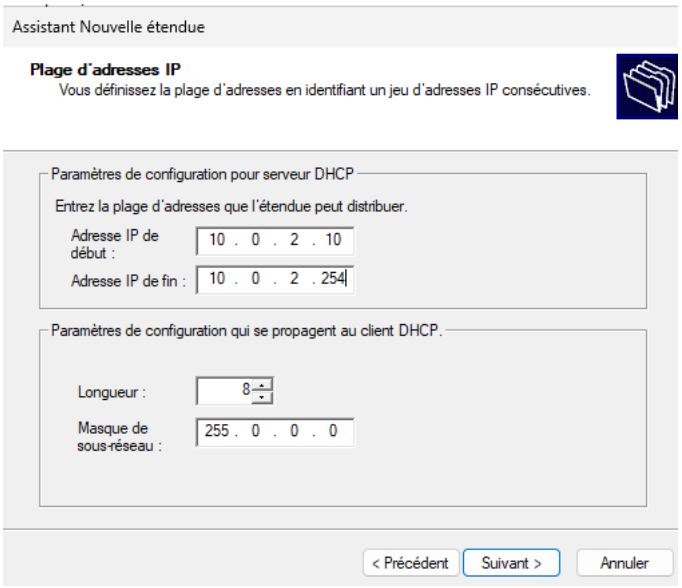
Nous allons désormais ajouter le rôle DHCP sur notre serveur :

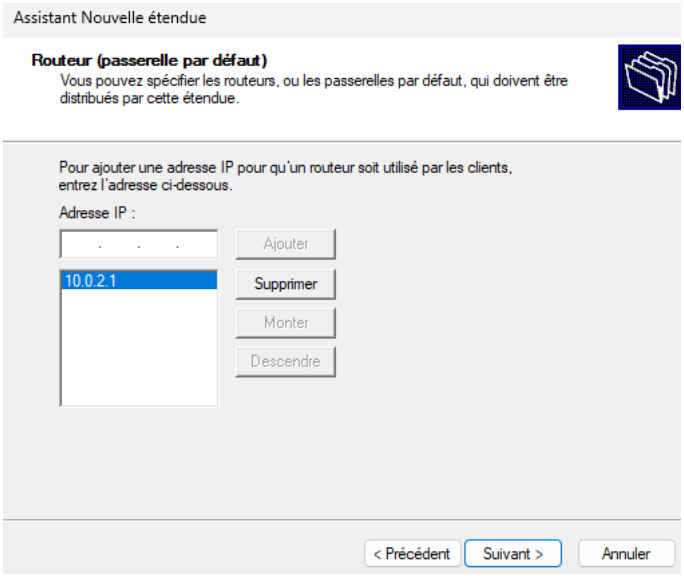


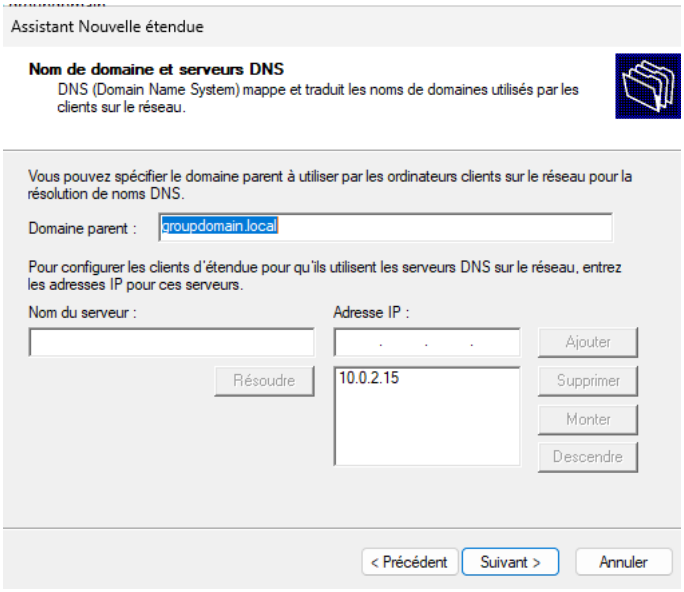


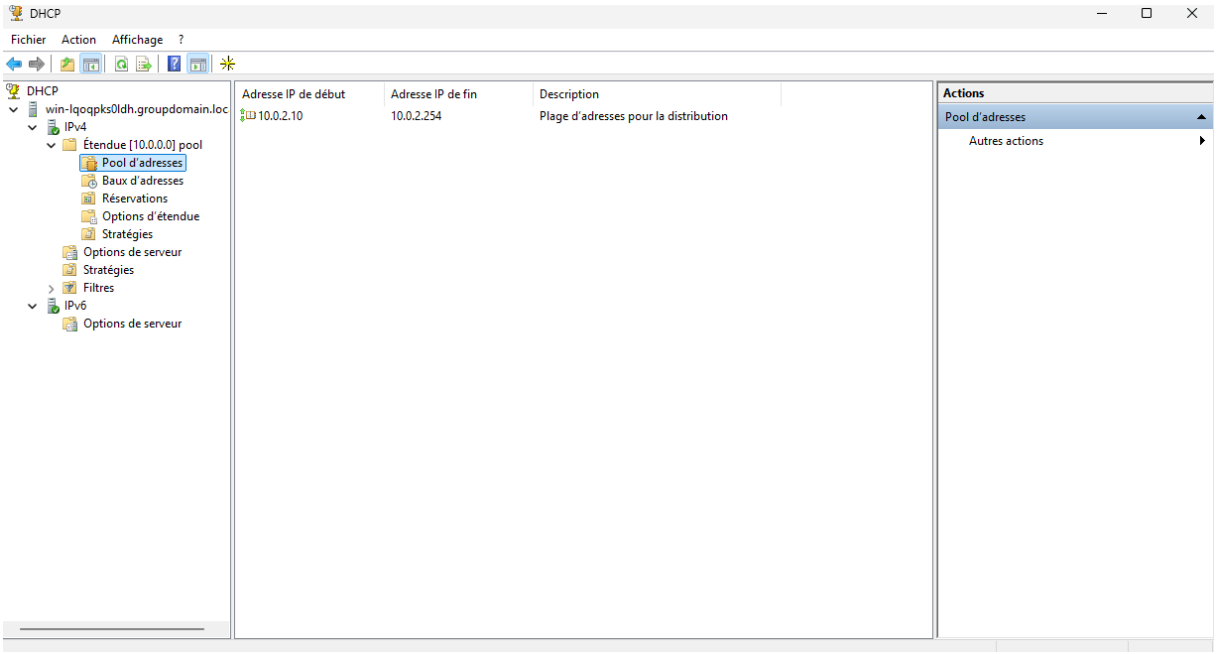
8.2 – Création de la plage d’adresses IP

Nous allons maintenant paramétrer le service DHCP pour qu’il attribue des adresses IP dans notre plage 10.0.2.10 - 254 :



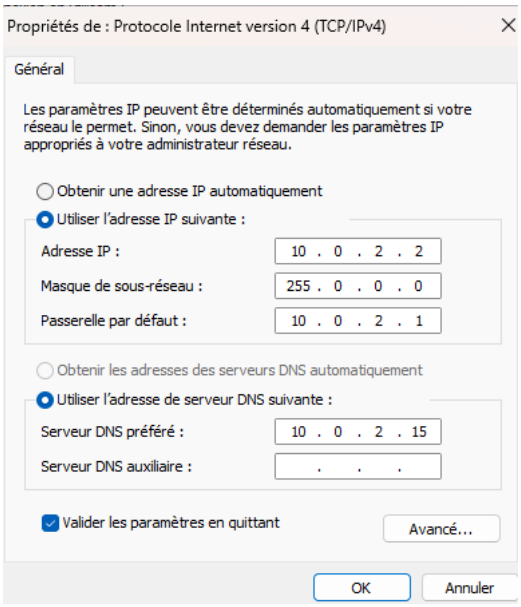


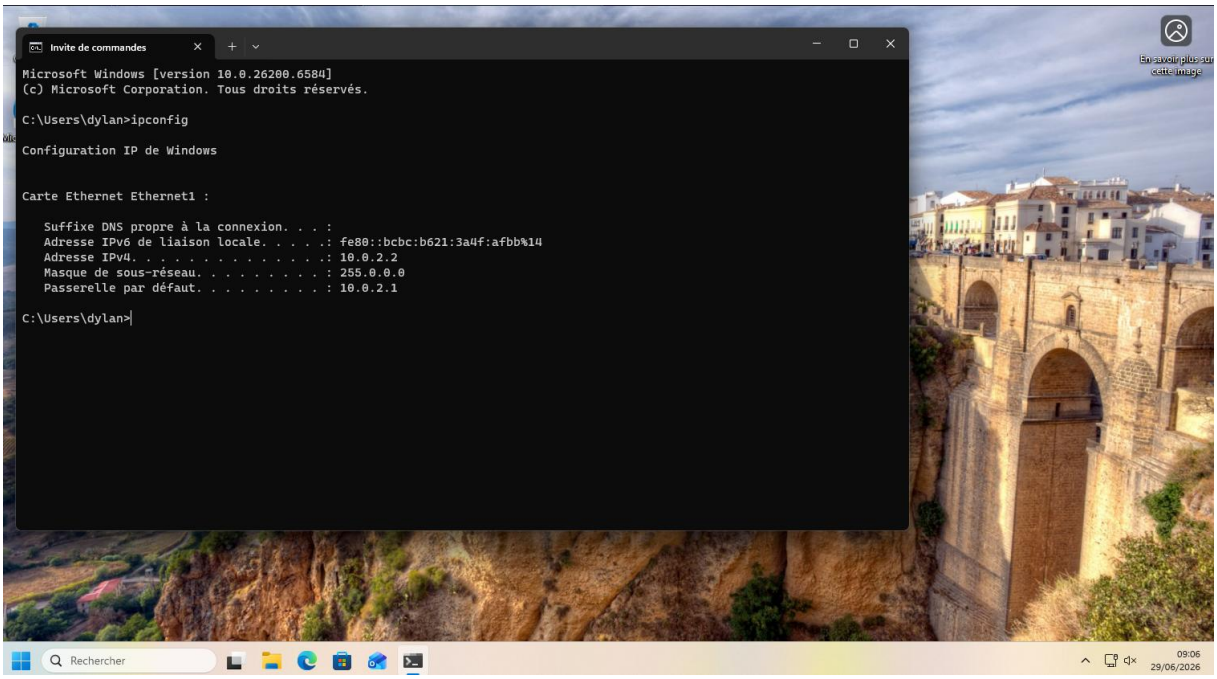

Assistant Nouvelle étendue
Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.
Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.
Domaine parent :
groupdomain.local
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.
Nom du serveur :
Adresse IP :
Ajouter
Résoudre
10.0.2.15
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler


DHCP
Fichier Action Affichage ?
DHCP
win-lqoqpks0ldh.groupdomain.loc
IPv4
Étendue [10.0.0.0] pool
Pool d'adresses
Baux d'adresses
Réservations
Options d'étendue
Stratégies
Options de serveur
Stratégies
Filtres
IPv6
Options de serveur
Adresse IP de début
Adresse IP de fin
Description
10.0.2.10
10.0.2.254
Plage d'adresses pour la distribution
Actions
Pool d'adresses
Autres actions

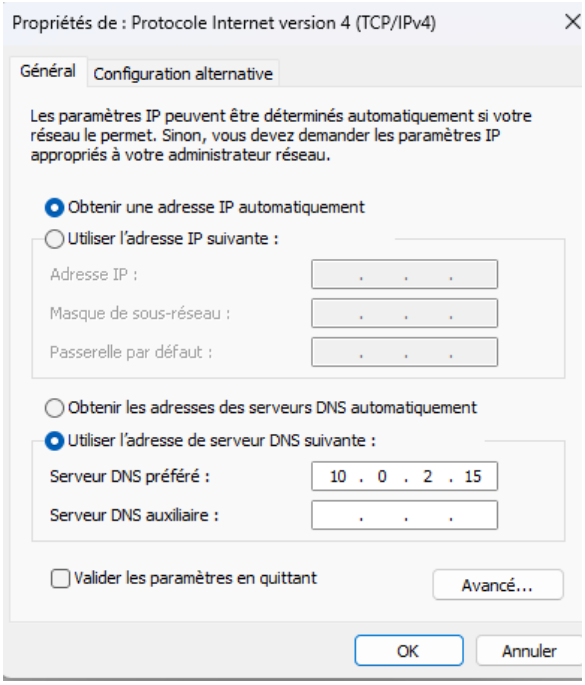
8.3 – Vérification du fonctionnement du DHCP

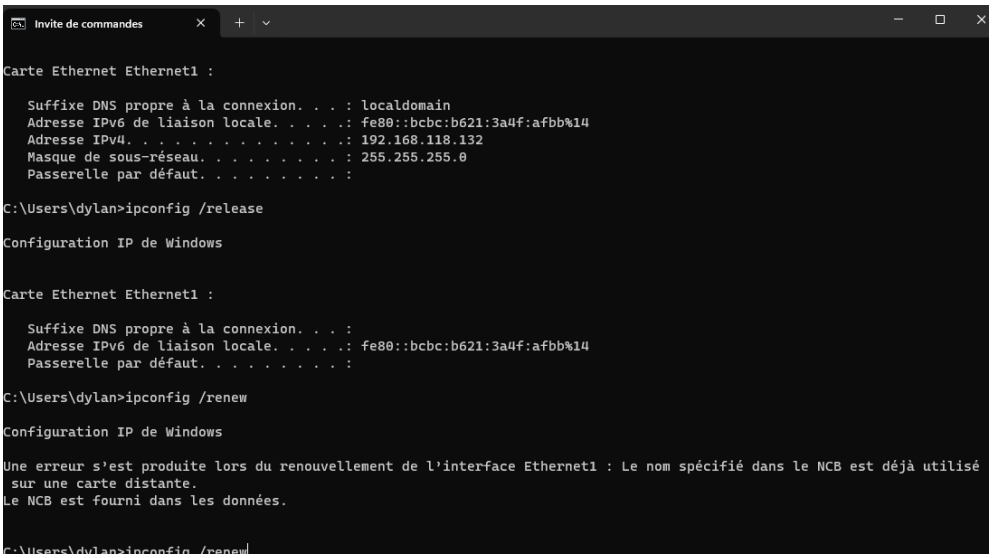
On rappelle l'adresse IP configurée précédemment sur notre PC client windows 11 :





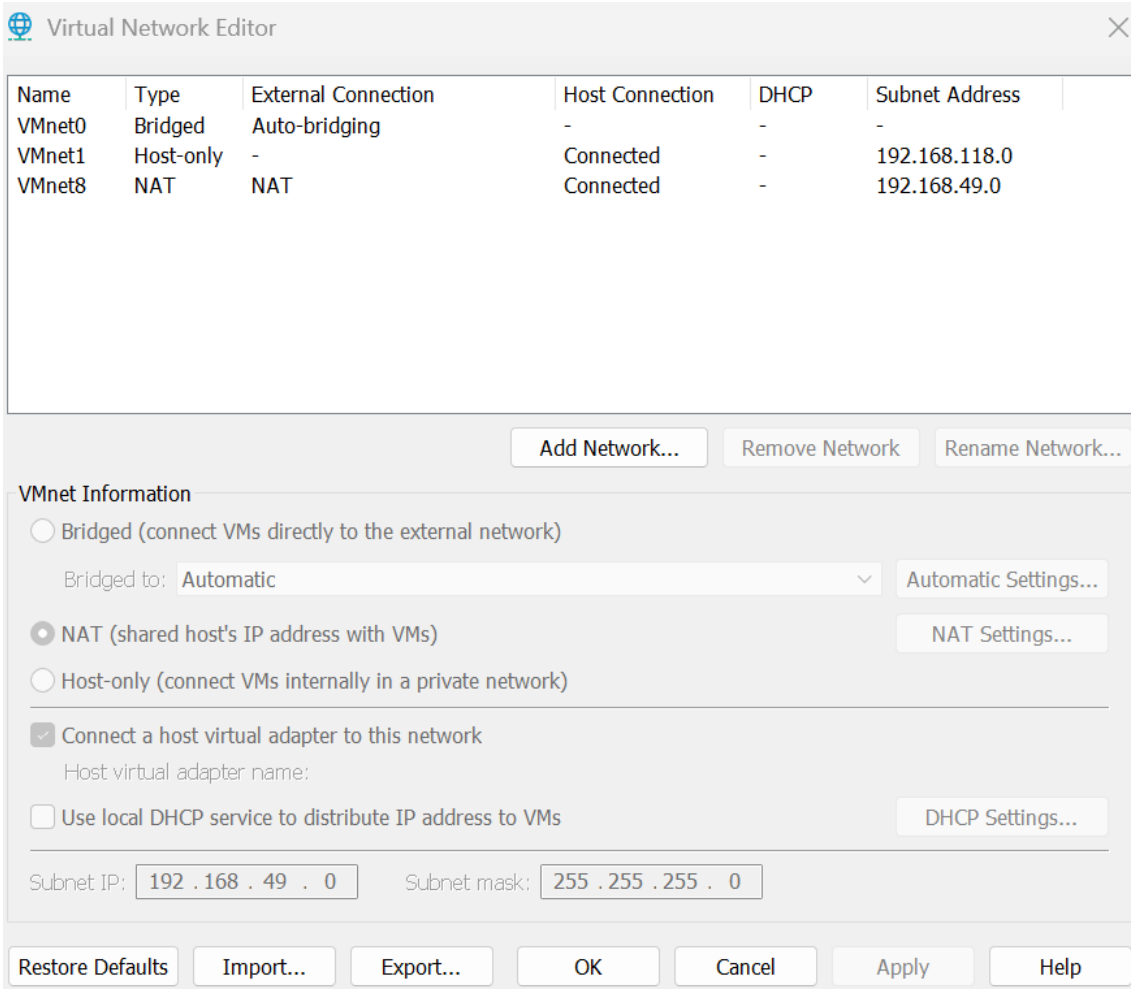
On paramètre l'attribution d'adresses IP en dynamique :

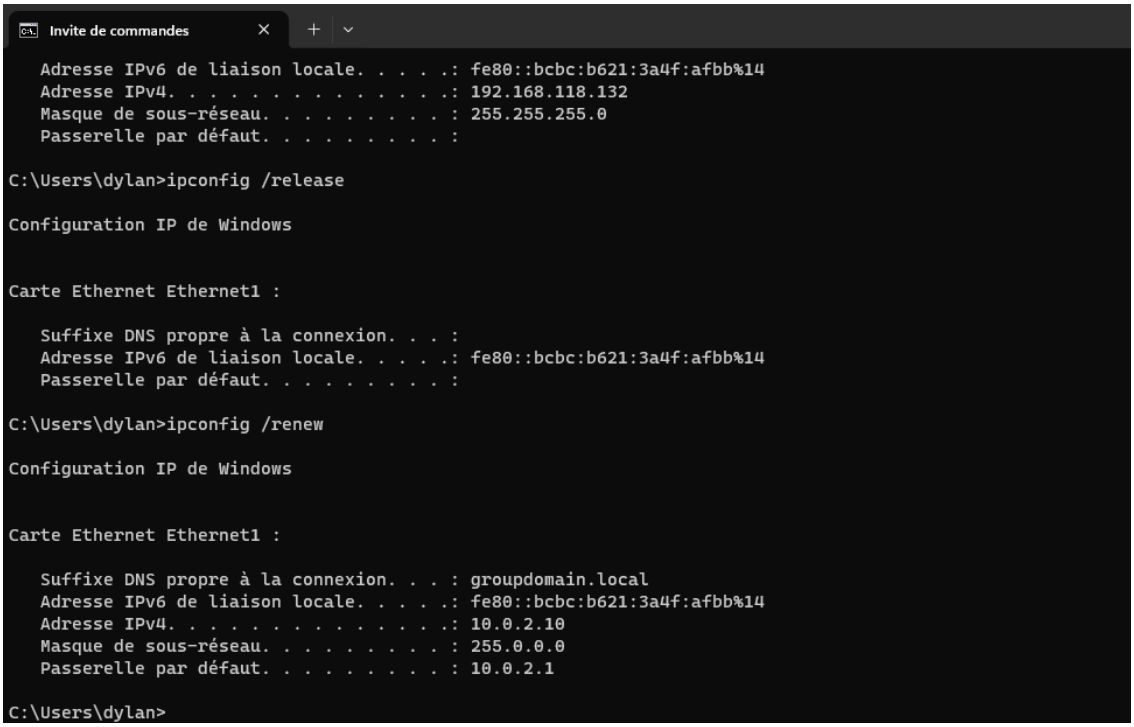




On s'aperçoit qu'un message d'erreur apparait et une adresse IP 192.168.118.132 a été attribuée par le DHCP de VMware.

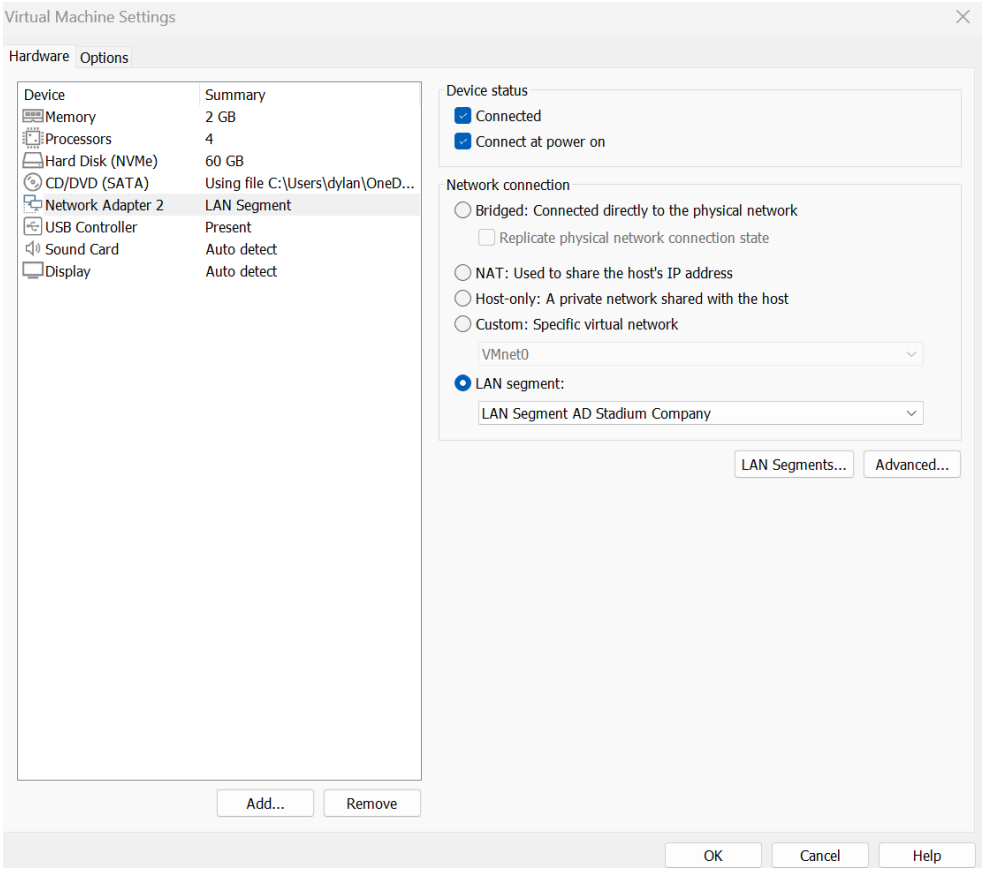
Nous allons donc désactiver le DHCP de VMware et refaire l'attribution DHCP :





Désormais, l'adresse IP 10.0.2.10 a été correctement attribuée à notre PC Windows.

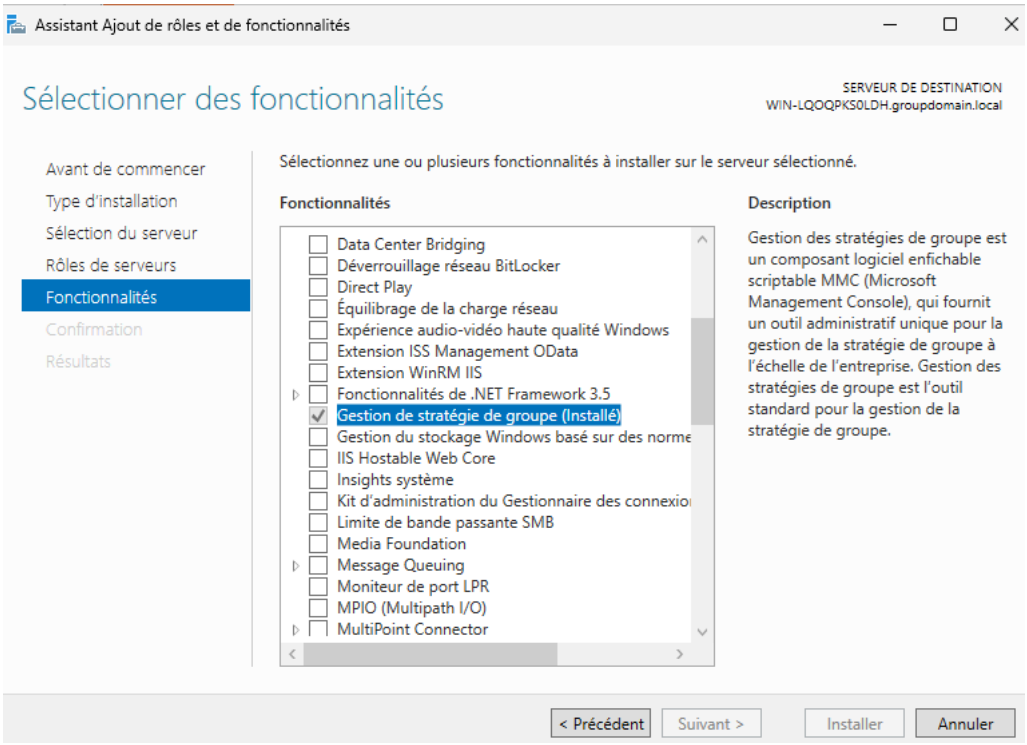
Pour pouvoir réactiver le DHCP dans VMware, on peut utiliser un LAN Segment dans le réseau :



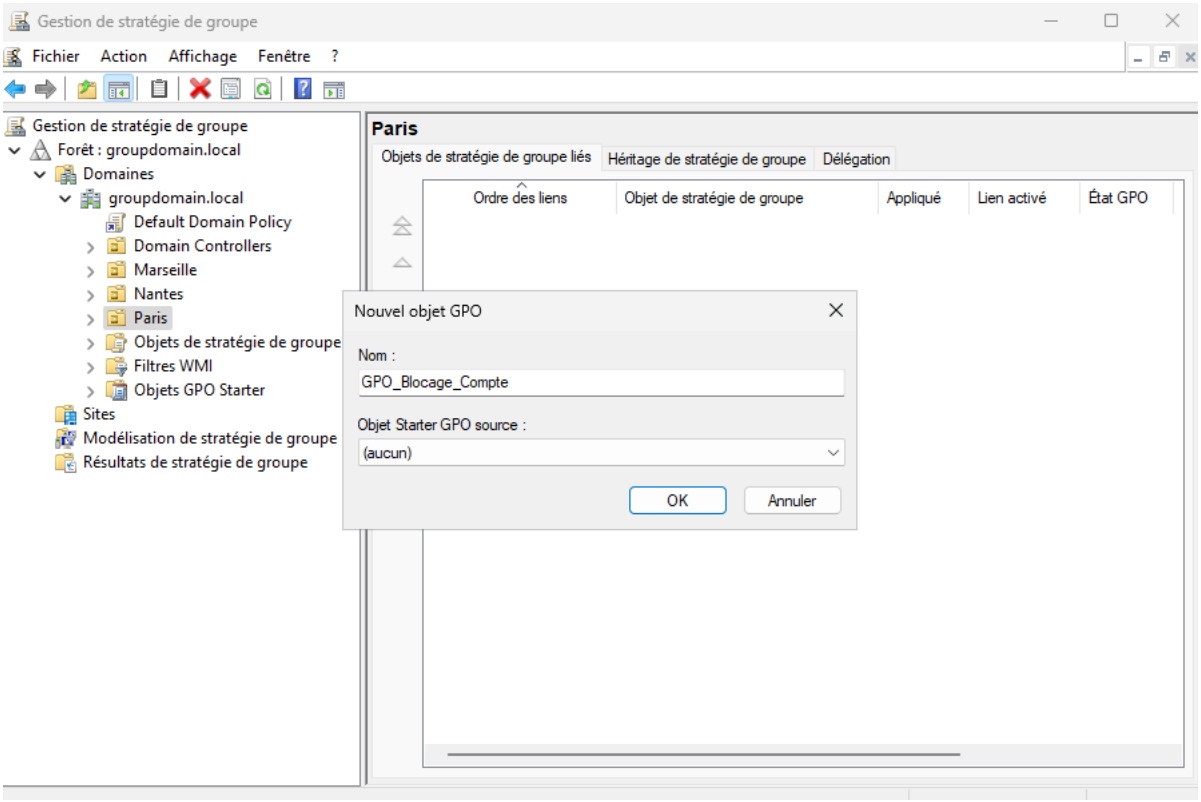
9-Ajout des Group Policy Objects (GPO)

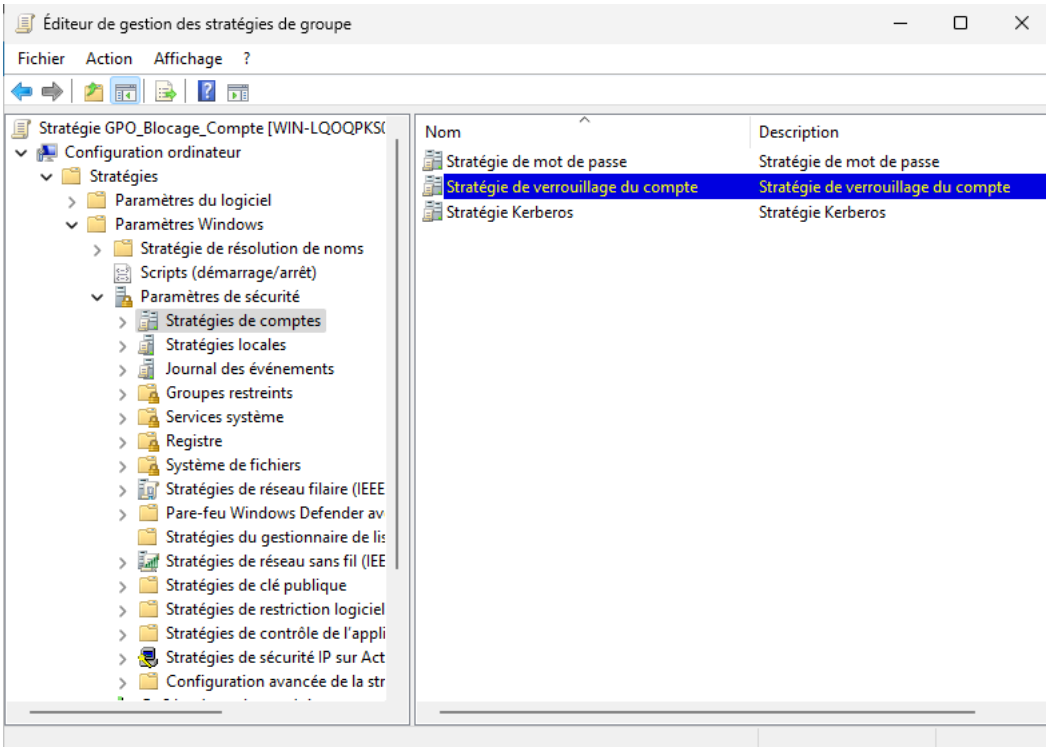
9.1 – Création des GPO

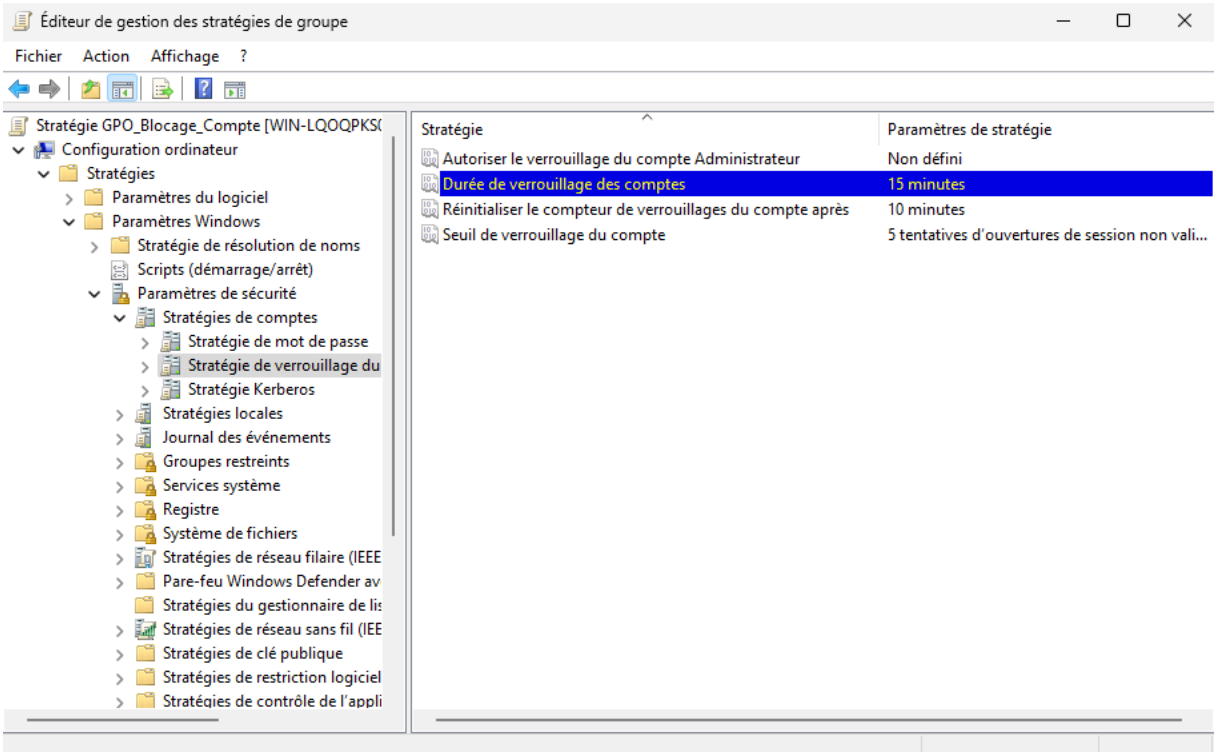
Le rôle « Stratégies de groupes » est déjà installé par défaut :



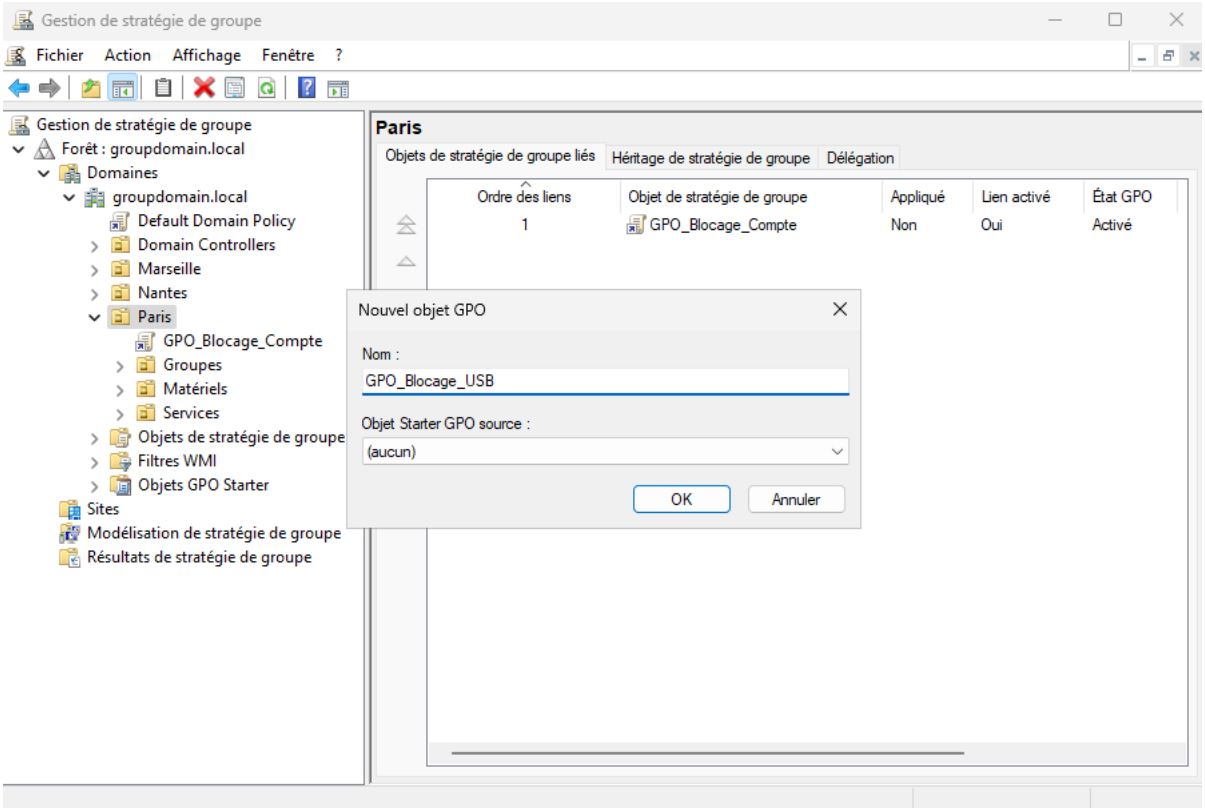
On crée un première GPO afin de bloquer les comptes utilisateurs lorsque un mauvais mot de passe est renseigné plusieurs fois :

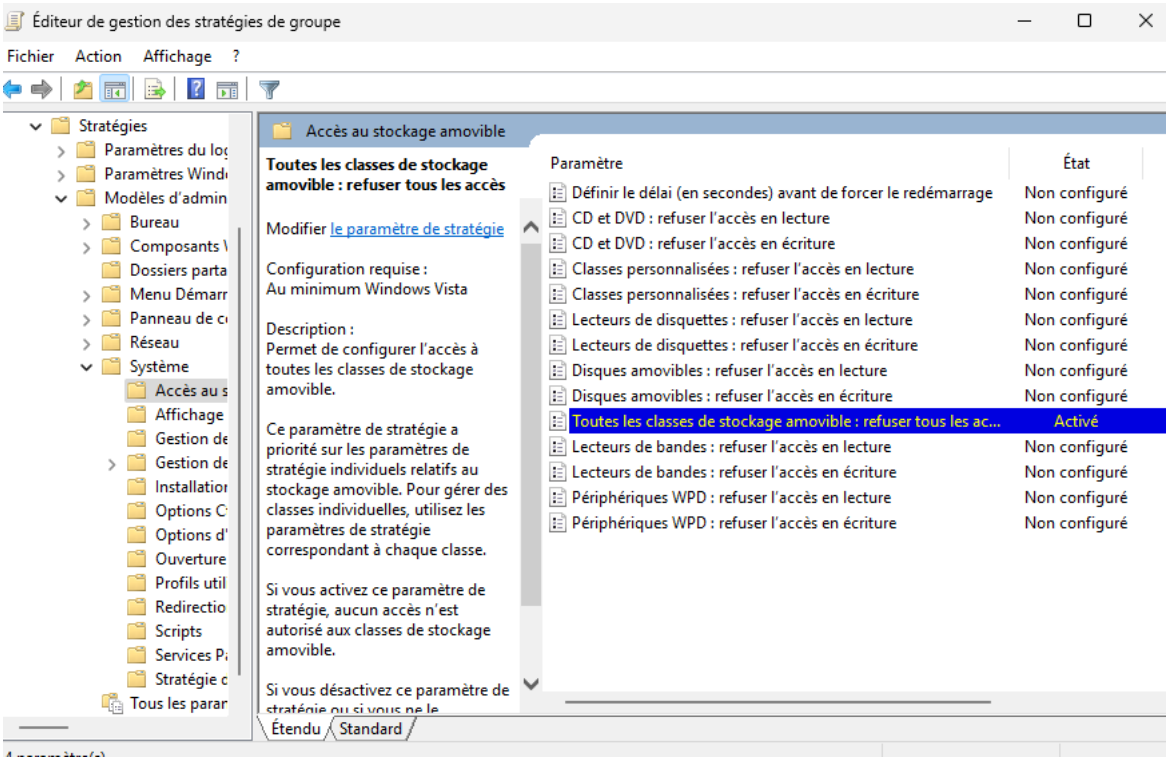

Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : groupdomain.local
Domaines
groupdomain.local
Default Domain Policy
Domain Controllers
Marseille
Nantes
Paris
Objets de stratégie de groupe
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
Paris
Objets de stratégie de groupe liés
Héritage de stratégie de groupe
Délégation
Ordre des liens
Objet de stratégie de groupe
Appliqué
Lien activé
État GPO
Nouvel objet GPO
Nom :
GPO_Blocage_Compte
Objet Starter GPO source :
(aucun)
OK
Annuler

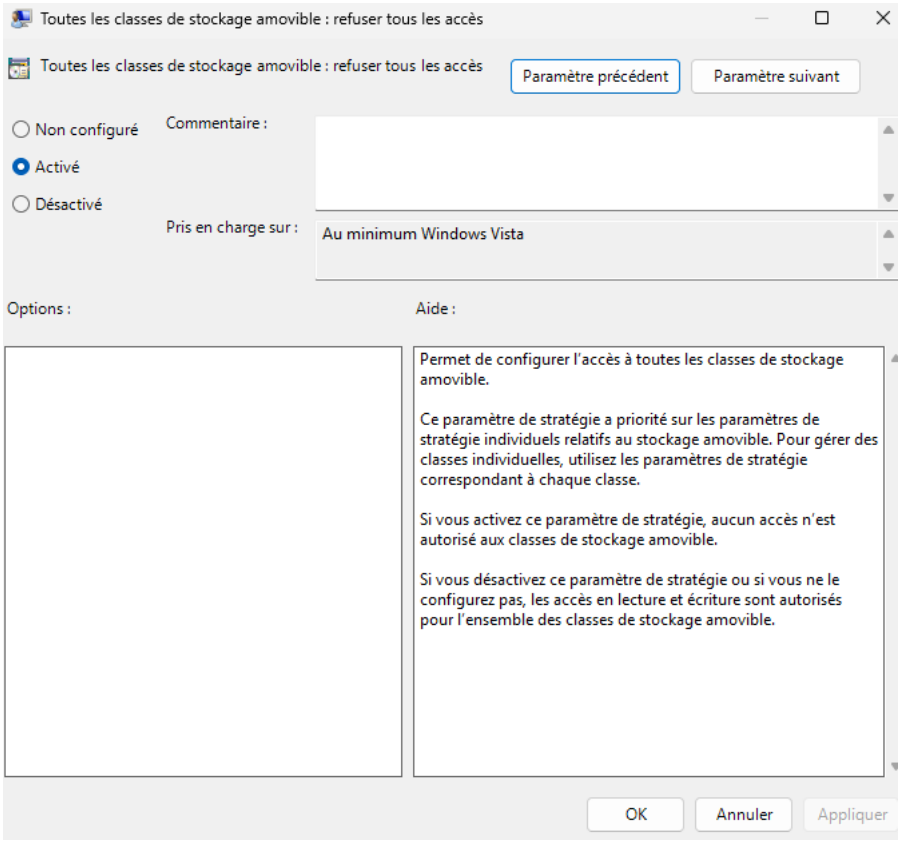

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Blocage_Compte [WIN-LQOQPKS(
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE
Pare-feu Windows Defender av
Stratégies du gestionnaire de lis
Stratégies de réseau sans fil (IEE
Stratégies de clé publique
Stratégies de restriction logiciel
Stratégies de contrôle de l'appli
Stratégies de sécurité IP sur Act
Configuration avancée de la str
Nom
Description
Stratégie de mot de passe
Stratégie de mot de passe
Stratégie de verrouillage du compte
Stratégie de verrouillage du compte
Stratégie Kerberos
Stratégie Kerberos


Éditeur de gestion des stratégies de groupe
Fichier
Action
Affichage
?
Stratégie GPO_Blocage_Compte [WIN-LQOQPKS(
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégie de mot de passe
Stratégie de verrouillage du
Stratégie Kerberos
Stratégies locales
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE
Pare-feu Windows Defender av
Stratégies du gestionnaire de lis
Stratégies de réseau sans fil (IEE
Stratégies de clé publique
Stratégies de restriction logiciel
Stratégies de contrôle de l'appli
Stratégie
Paramètres de stratégie
Autoriser le verrouillage du compte Administrateur
Non défini
Durée de verrouillage des comptes
15 minutes
Réinitialiser le compteur de verrouillages du compte après
10 minutes
Seuil de verrouillage du compte
5 tentatives d'ouvertures de session non vali...

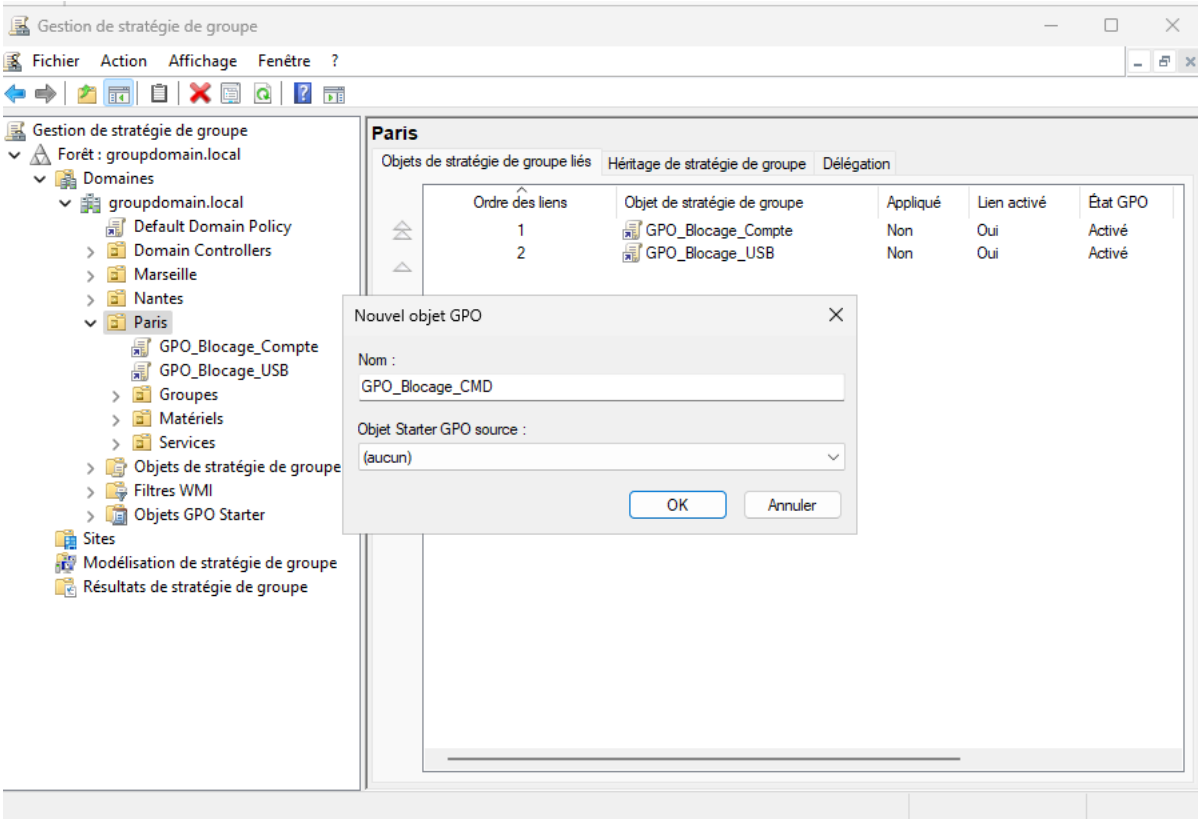
On crée une seconde GPO afin de bloquer les ports USB sur tous les PC de Paris :

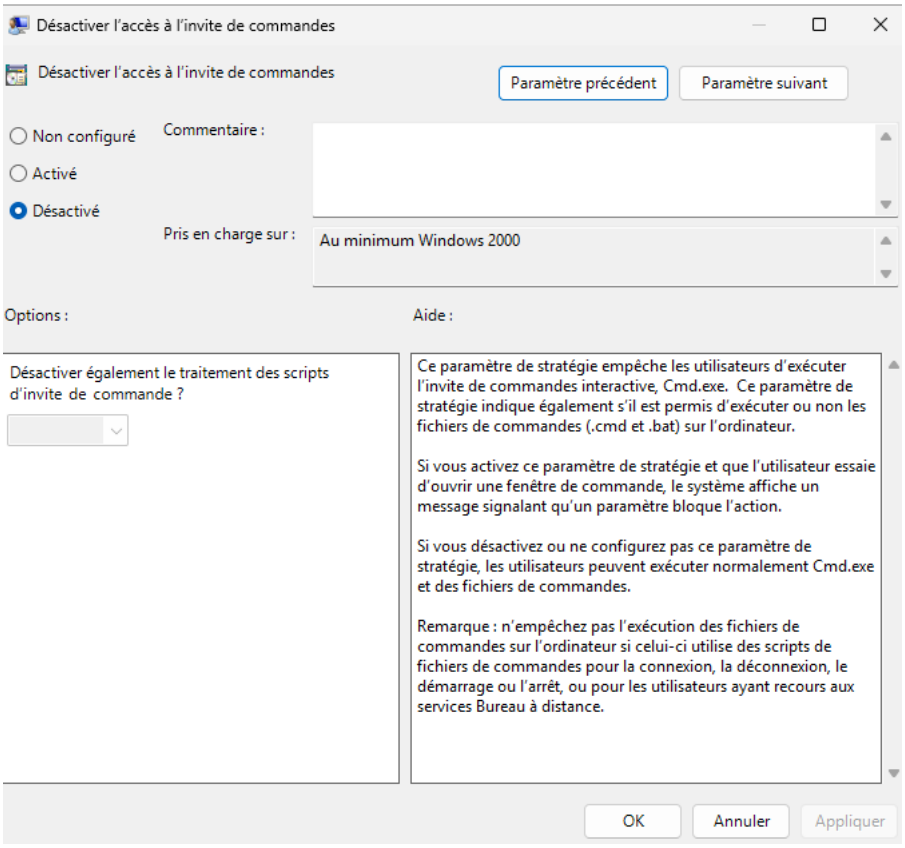


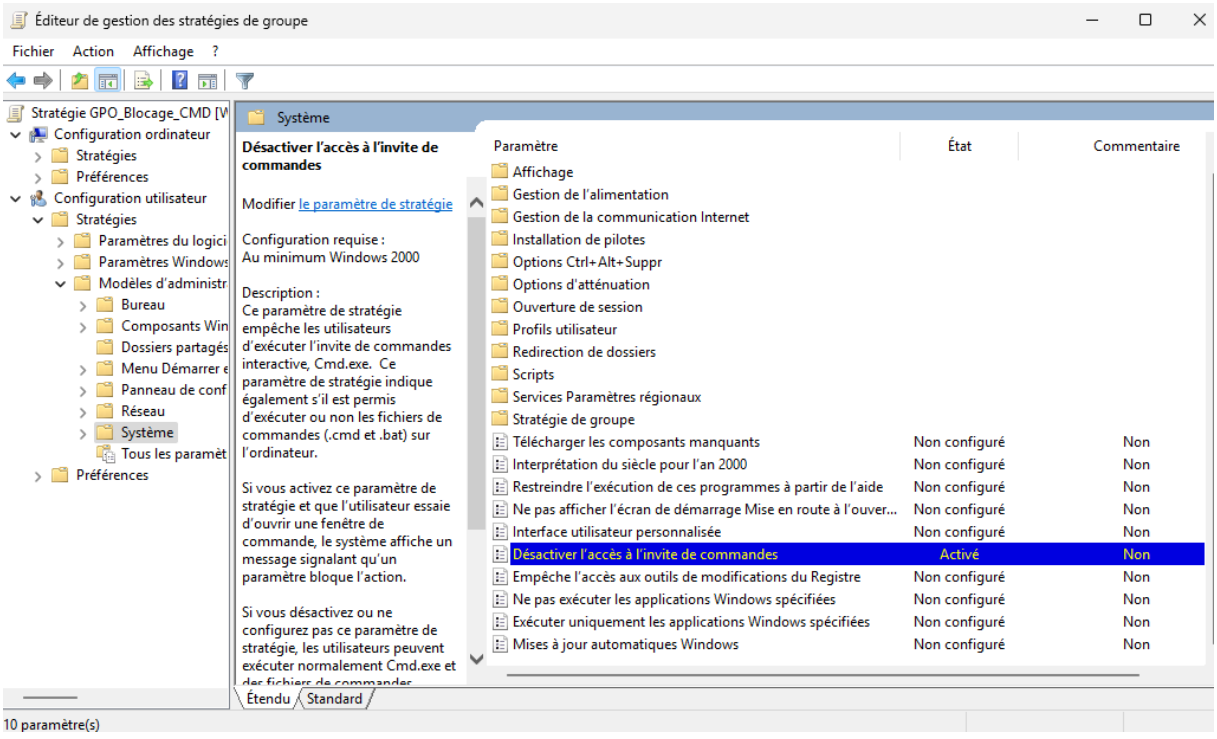




On rajoute un blocage de l'accès au CMD pour tous les comptes qui ne sont pas administrateurs :

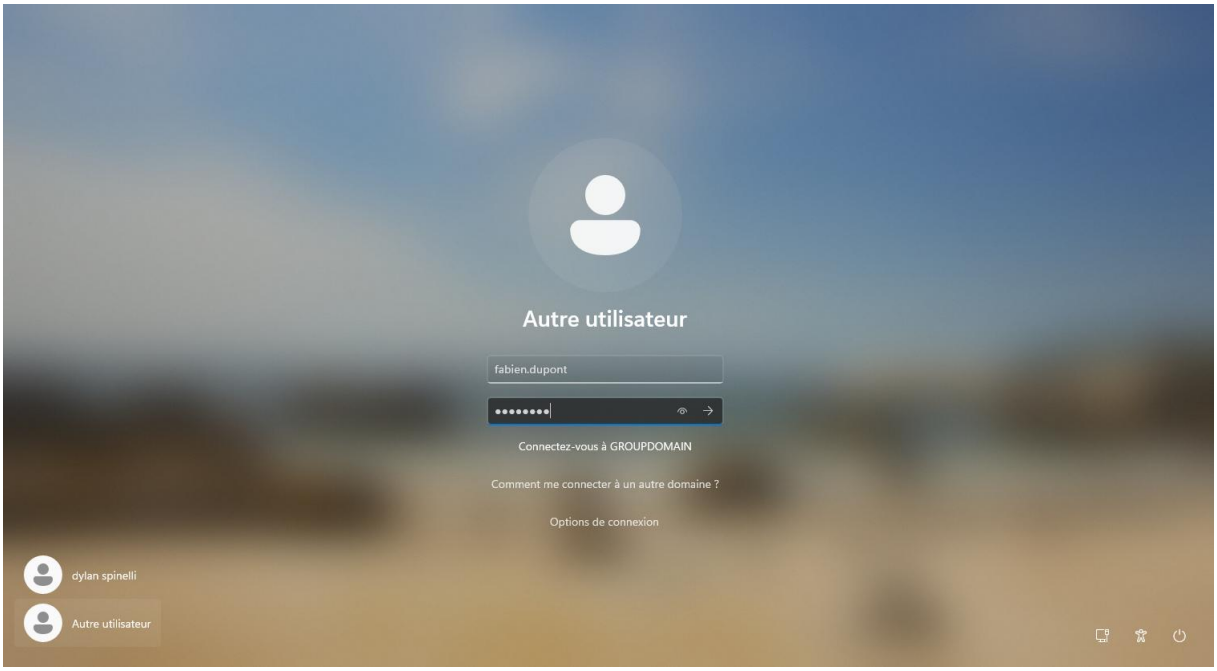



Désactiver l'accès à l'invite de commandes
Désactiver l'accès à l'invite de commandes
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows 2000
Options :
Aide :
Désactiver également le traitement des scripts d'invite de commande ?
Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.
Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.
Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et des fichiers de commandes.
Remarque : n'empêchez pas l'exécution des fichiers de commandes sur l'ordinateur si celui-ci utilise des scripts de fichiers de commandes pour la connexion, la déconnexion, le démarrage ou l'arrêt, ou pour les utilisateurs ayant recours aux services Bureau à distance.
OK
Annuler
Appliquer

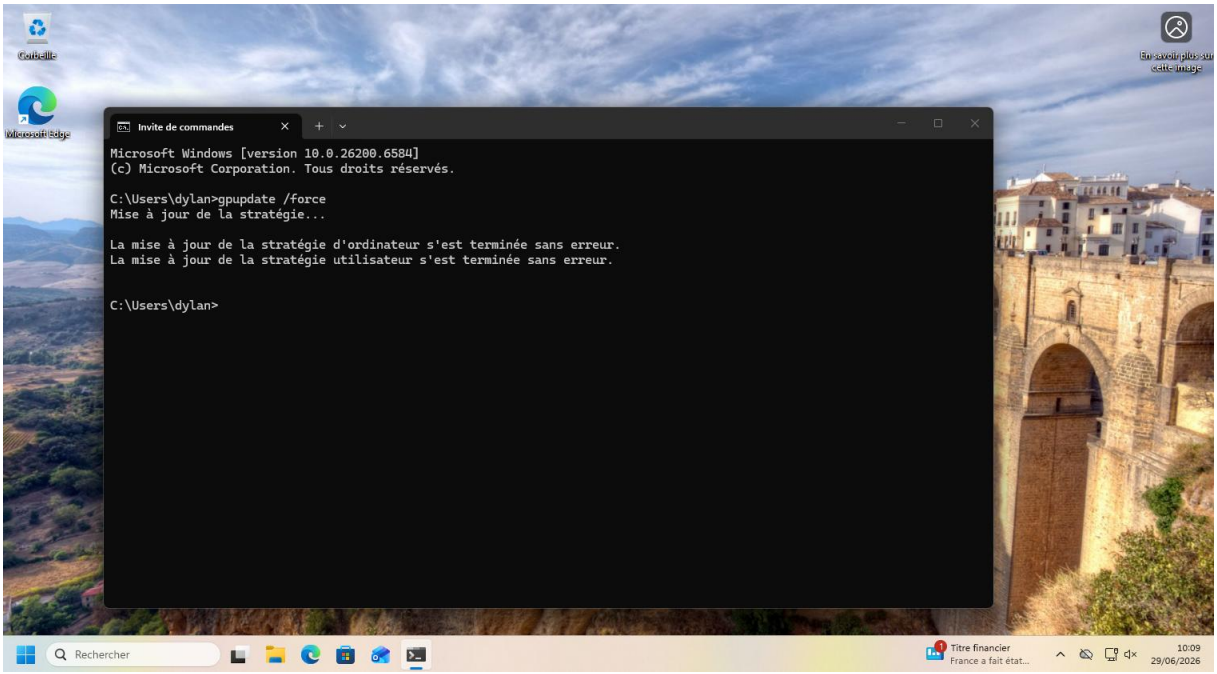

Éditeur de gestion des stratégies de groupe
Fichier
Action
Affichage
?
Stratégie GPO_Blocage_CMD [W
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Paramètres du logici
Paramètres Windows
Modèles d'administr
Bureau
Composants Win
Dossiers partagés
Menu Démarrer e
Panneau de conf
Réseau
Système
Tous les paramèt
Préférences
Système
Désactiver l'accès à l'invite de commandes
Modifier le paramètre de stratégie
Configuration requise :
Au minimum Windows 2000
Description :
Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.
Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.
Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et
Paramètre
État
Commentaire
Affichage
Gestion de l'alimentation
Gestion de la communication Internet
Installation de pilotes
Options Ctrl+Alt+Suppr
Options d'atténuation
Ouverture de session
Profils utilisateur
Redirection de dossiers
Scripts
Services Paramètres régionaux
Stratégie de groupe
Télécharger les composants manquants
Non configuré
Non
Interprétation du siècle pour l'an 2000
Non configuré
Non
Restreindre l'exécution de ces programmes à partir de l'aide
Non configuré
Non
Ne pas afficher l'écran de démarrage Mise en route à l'ouver...
Non configuré
Non
Interface utilisateur personnalisée
Non configuré
Non
Désactiver l'accès à l'invite de commandes
Activé
Non
Empêche l'accès aux outils de modifications du Registre
Non configuré
Non
Ne pas exécuter les applications Windows spécifiées
Non configuré
Non
Exécuter uniquement les applications Windows spécifiées
Non configuré
Non
Mises à jour automatiques Windows
Non configuré
Non
Étendu
Standard
10 paramètre(s)

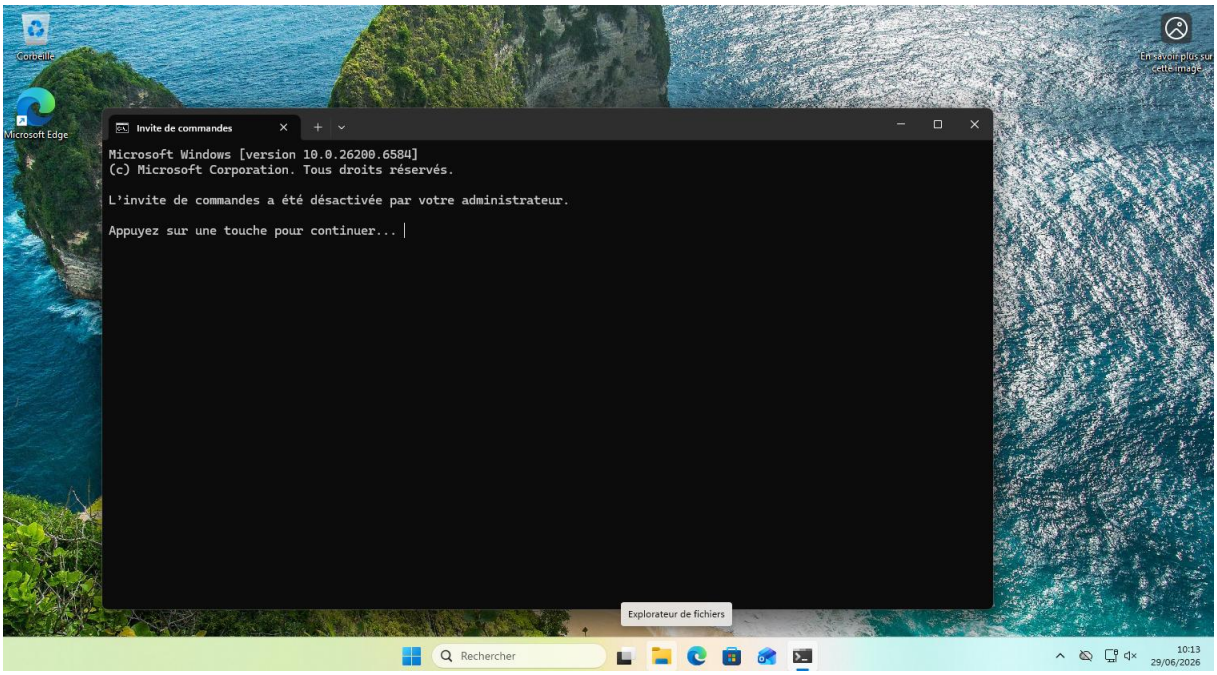
9.2 – Test des GPO

On se connecte sur la session d'un utilisateur de Paris :



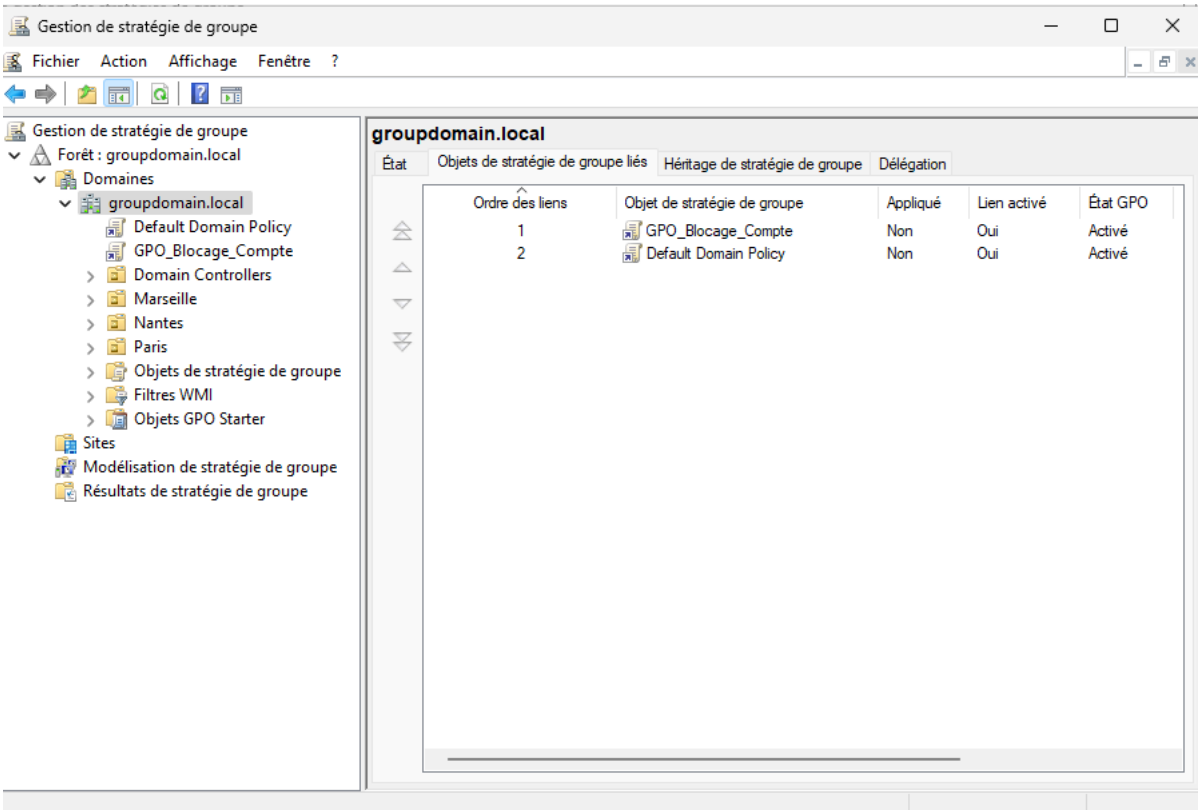
On force la mise à jour des GPO :

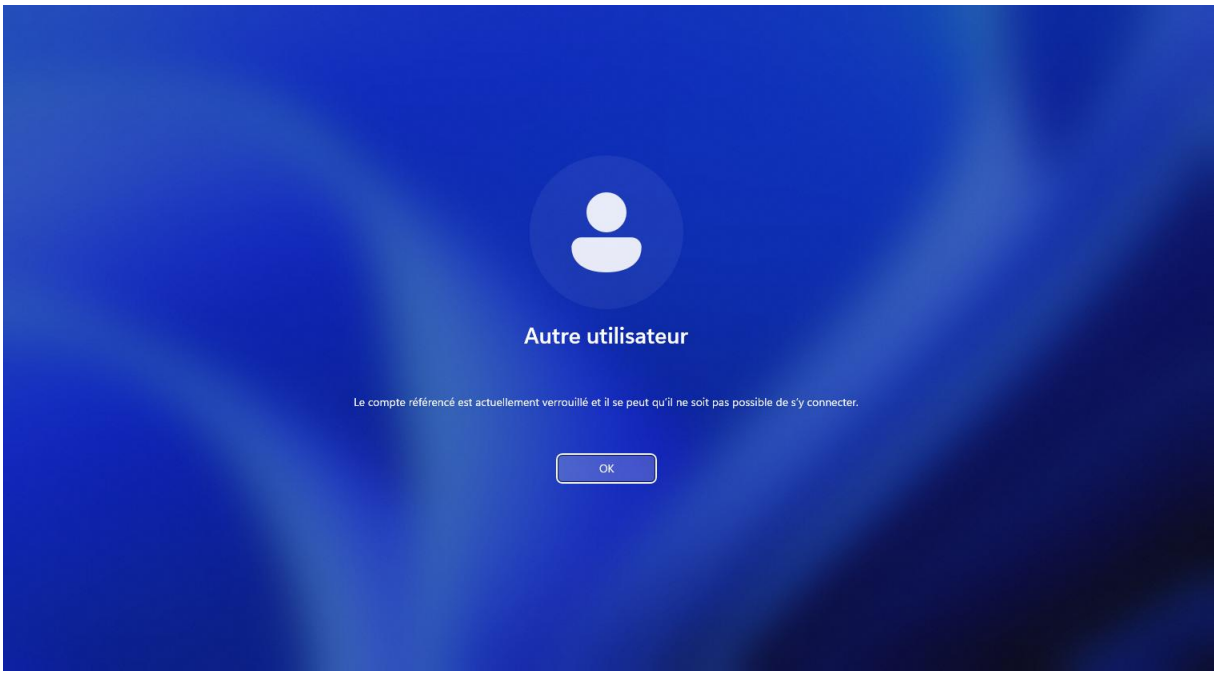




Le CMD est bien inaccessible

Pour la GPO concernant les blocages de comptes, il faut la lier à la racine du domaine et la mettre en priorité 1 :



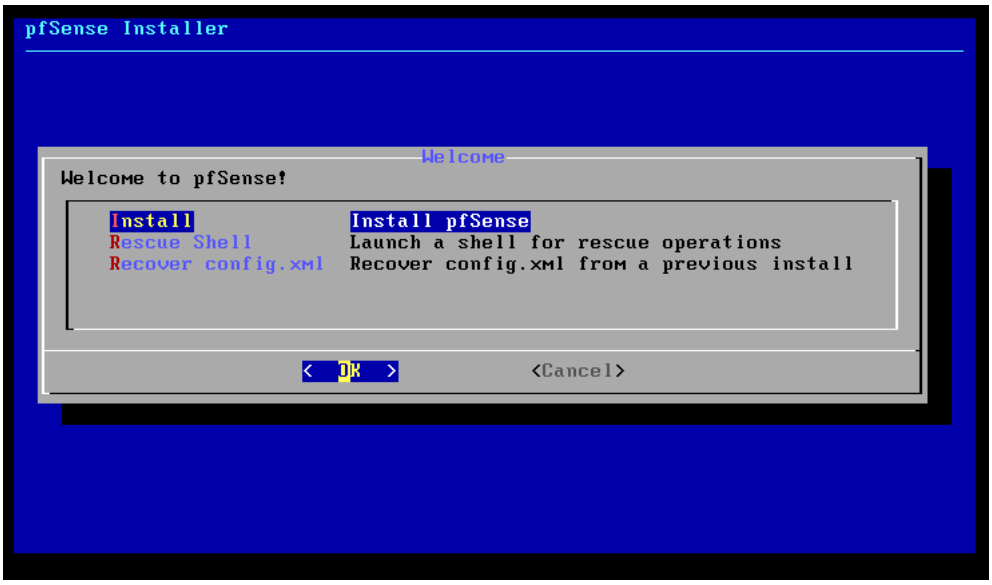


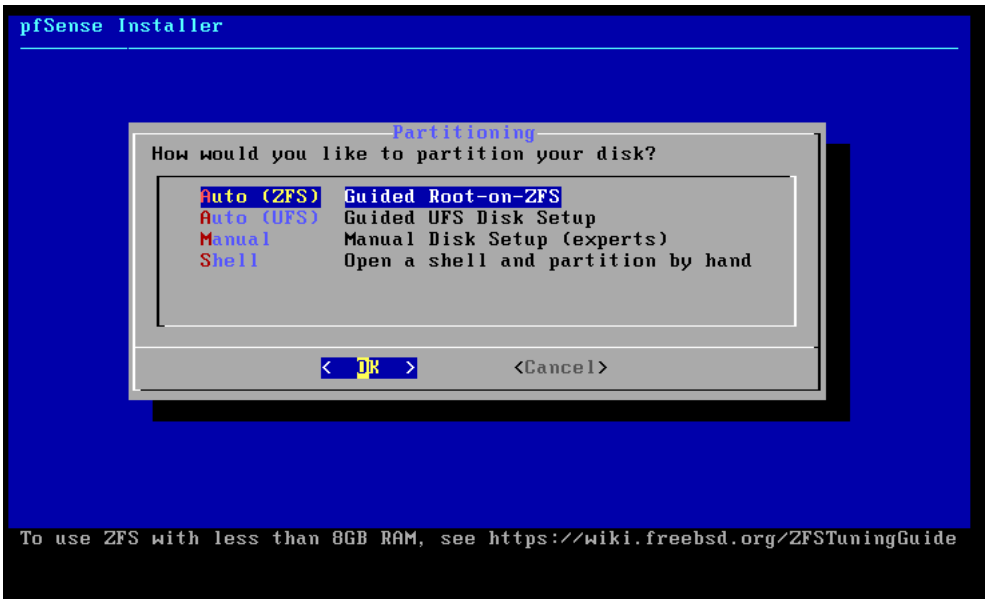
Désormais, les comptes sont bien bloqués lors de nombreuses tentatives de connexion échouées.

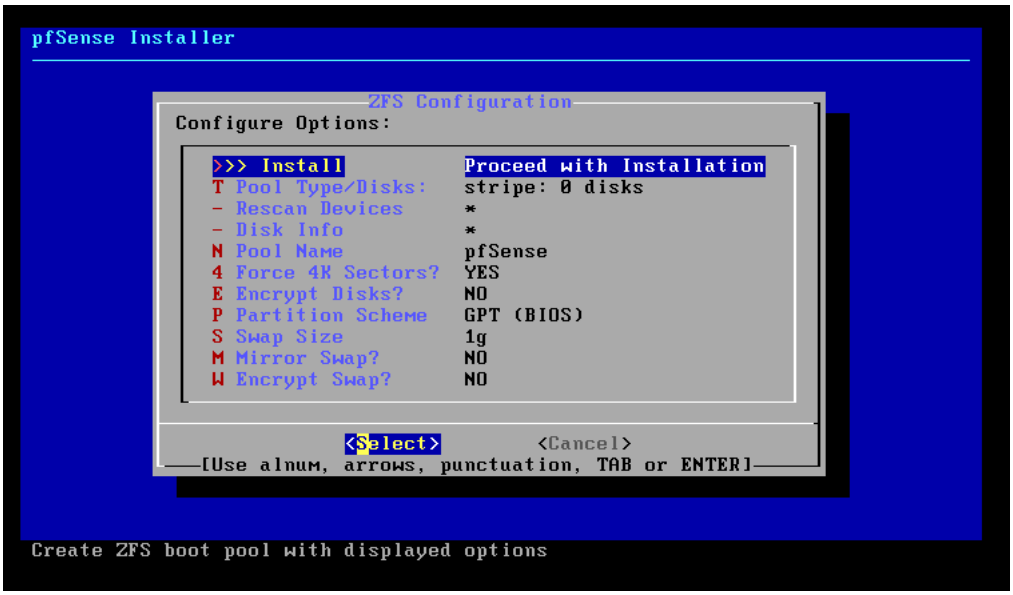
10- Ajout d’un pare-feu pfSense dans le domaine

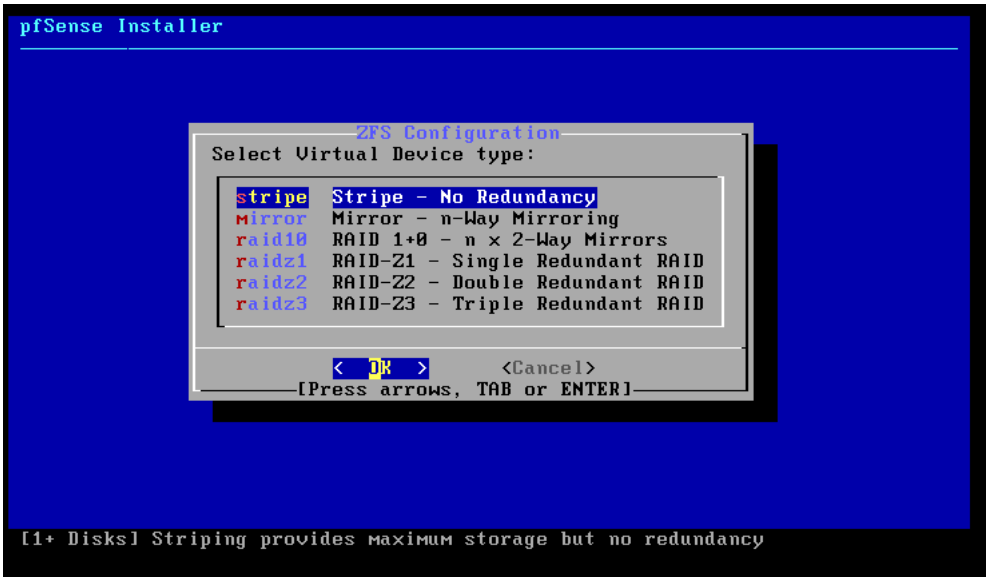
10.1 - Installation d’une VM pfSense

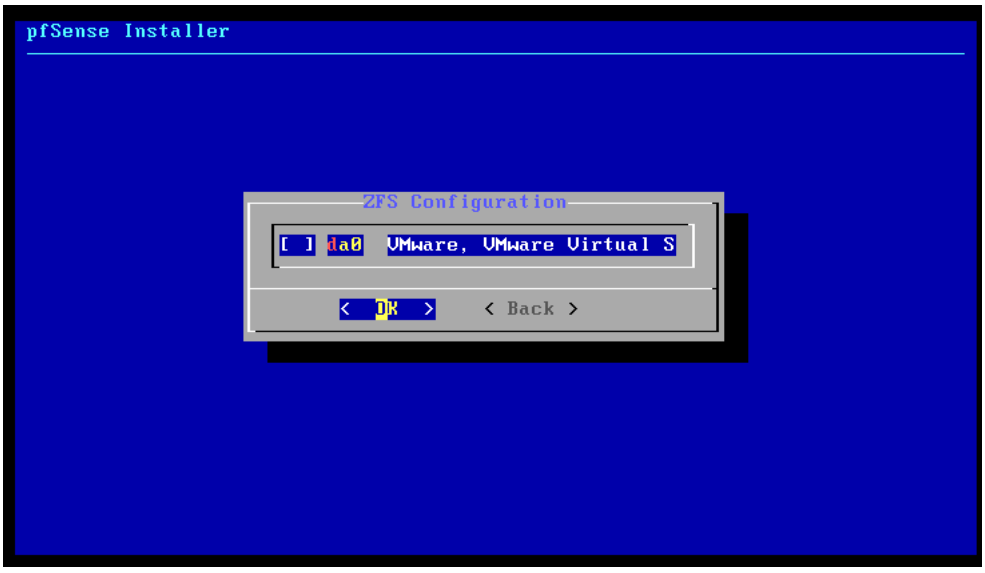
Nous allons désormais installer notre VM pfSense. Voici les différentes étapes de l’installation :

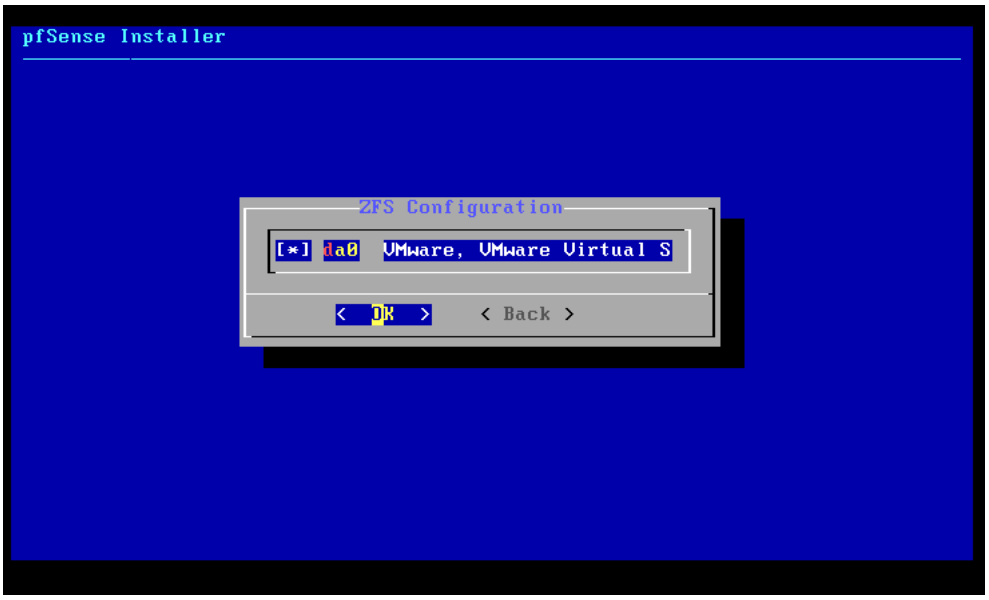


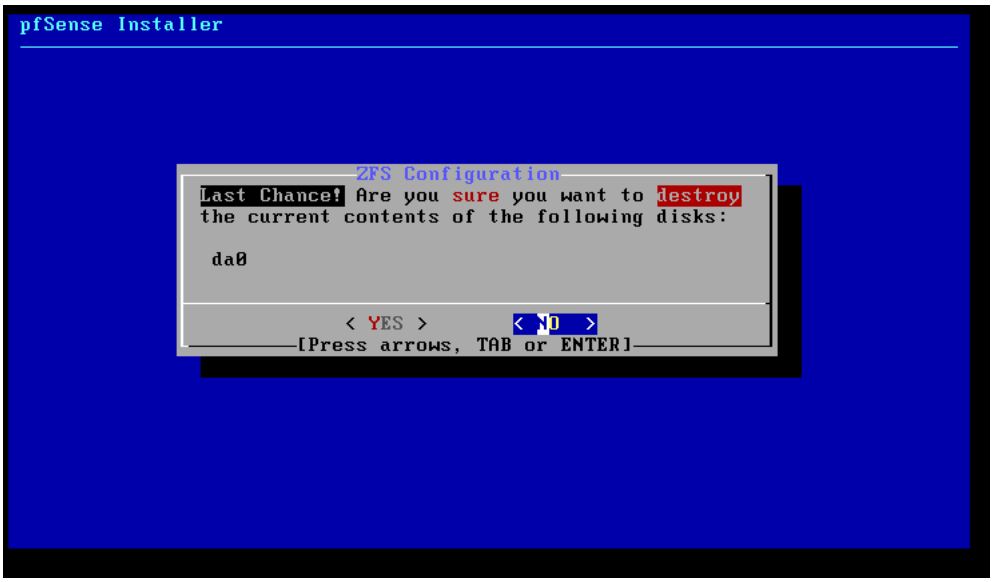



pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options

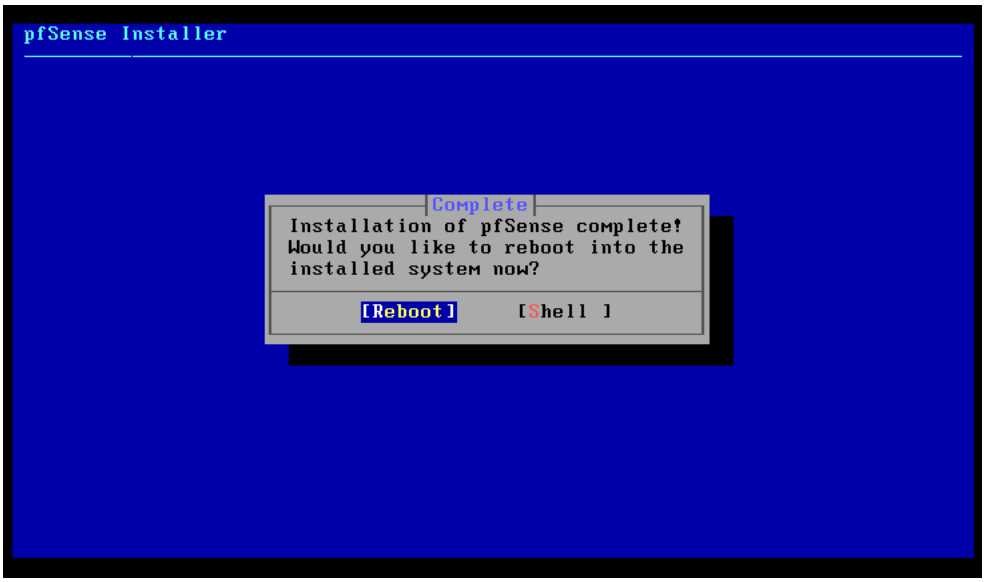

pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy


pfSense Installer
ZFS Configuration
[ ] da0 VMware, VMware Virtual S
< OK > < Back >


pfSense Installer
ZFS Configuration
[*] da0 VMware, VMware Virtual S
< OK >
< Back >

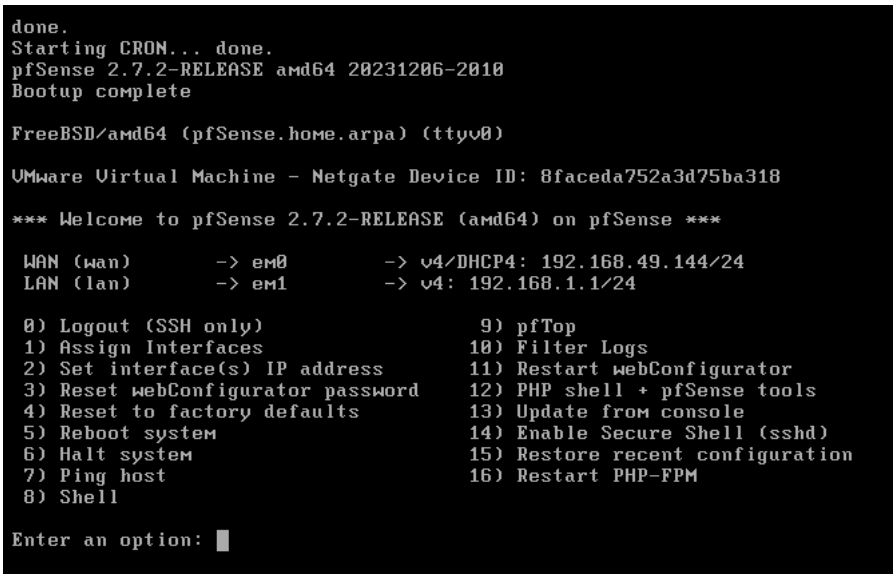

pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
da0
< YES >
< NO >
[Press arrows, TAB or ENTER]


pfSense Installer
Archive Extraction
base.txz [50%]
Extracting distribution files...
Overall Progress
50%
24561 files read @ 1754.4 files/sec.



L'installation de pfSense est désormais terminée.

Voici l'affichage de pfSense après redémarrage :



On configure l'IP statique du pfSense avec l'adresse de la passerelle de notre réseau 10.0.2.1/8 :

```
 6) Halt system                      15) Restore recent configuration
 7) Ping host                        16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.2.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 8
```

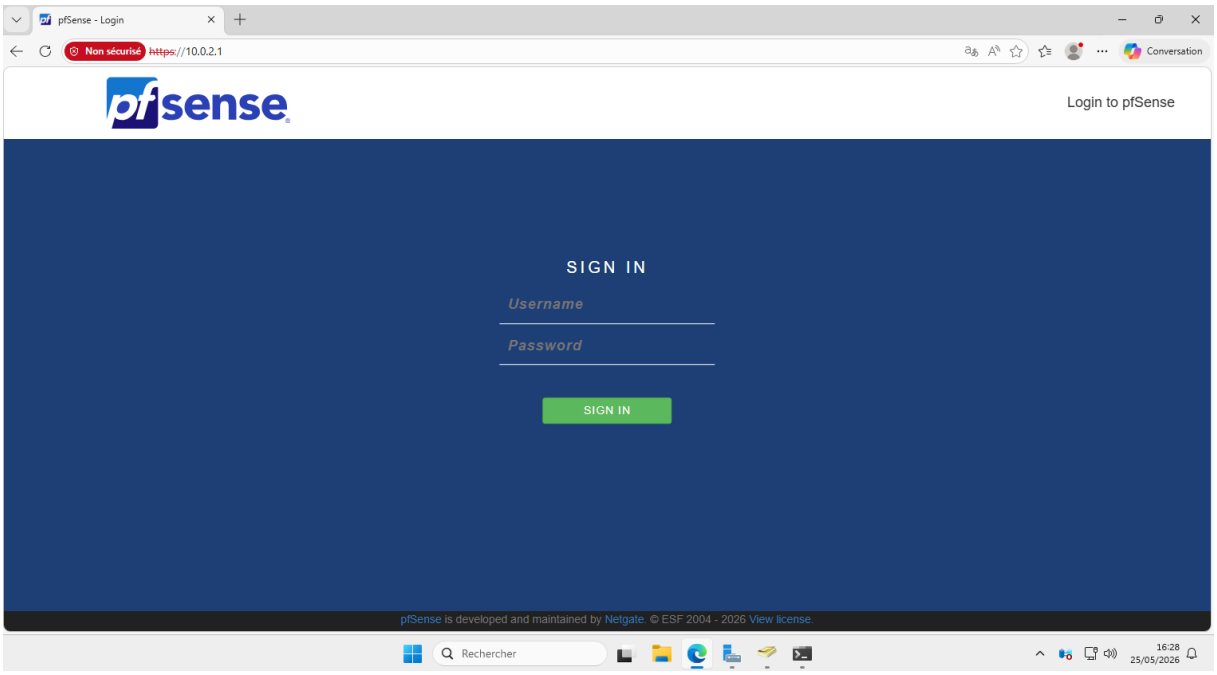
```
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n)

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 10.0.2.1/8
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.0.2.1/

Press <ENTER> to continue.
```

On fait un tracert sur notre windows server :

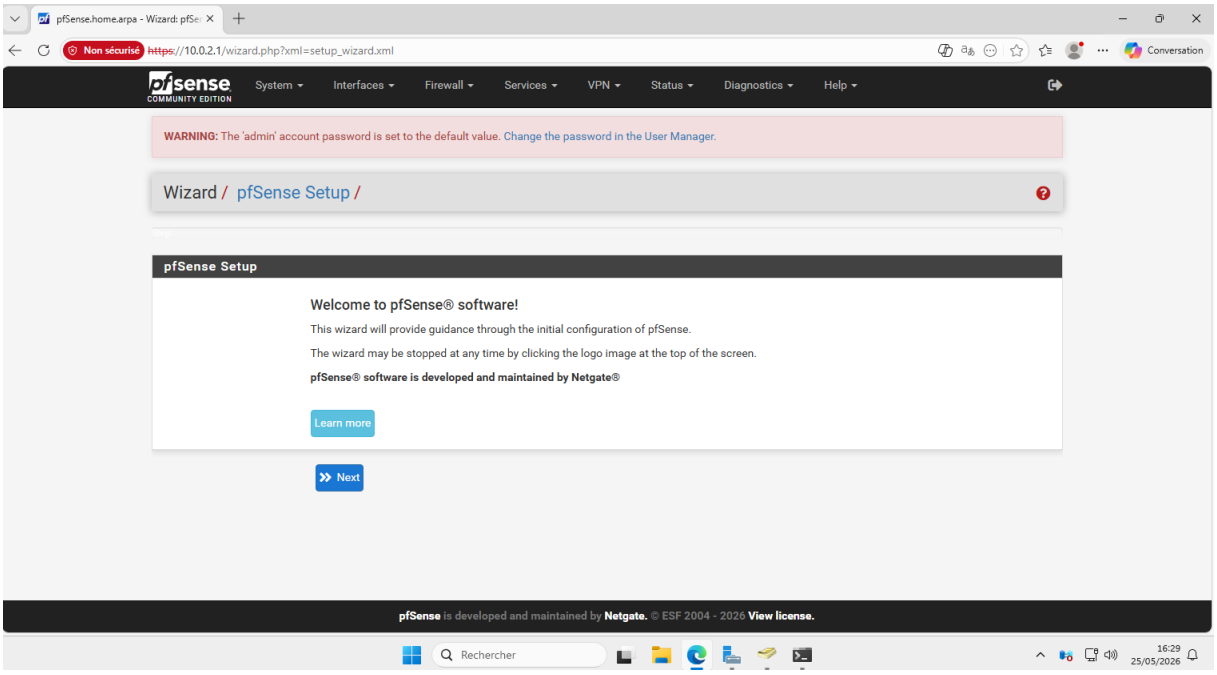
```
Administrateur : Command Pr
Microsoft Windows [version 10.0.26100.1742]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.WIN-LQOQPKS0LDH>tracert 8.8.8.8

Détermination de l'itinéraire vers 8.8.8.8 avec un maximum de 30 sauts.

  1     2 ms     1 ms     1 ms  10.0.2.1
  2     *        *        *     Délai d'attente de la demande dépassé.
  3     *        *     ^C
C:\Users\Administrateur.WIN-LQOQPKS0LDH>
```

Notre pare-feu pfSense est désormais la passerelle par défaut de notre réseau.

Essayons de nous connecter à pfSense depuis notre Windows server à l'adresse 10.0.2.1 :



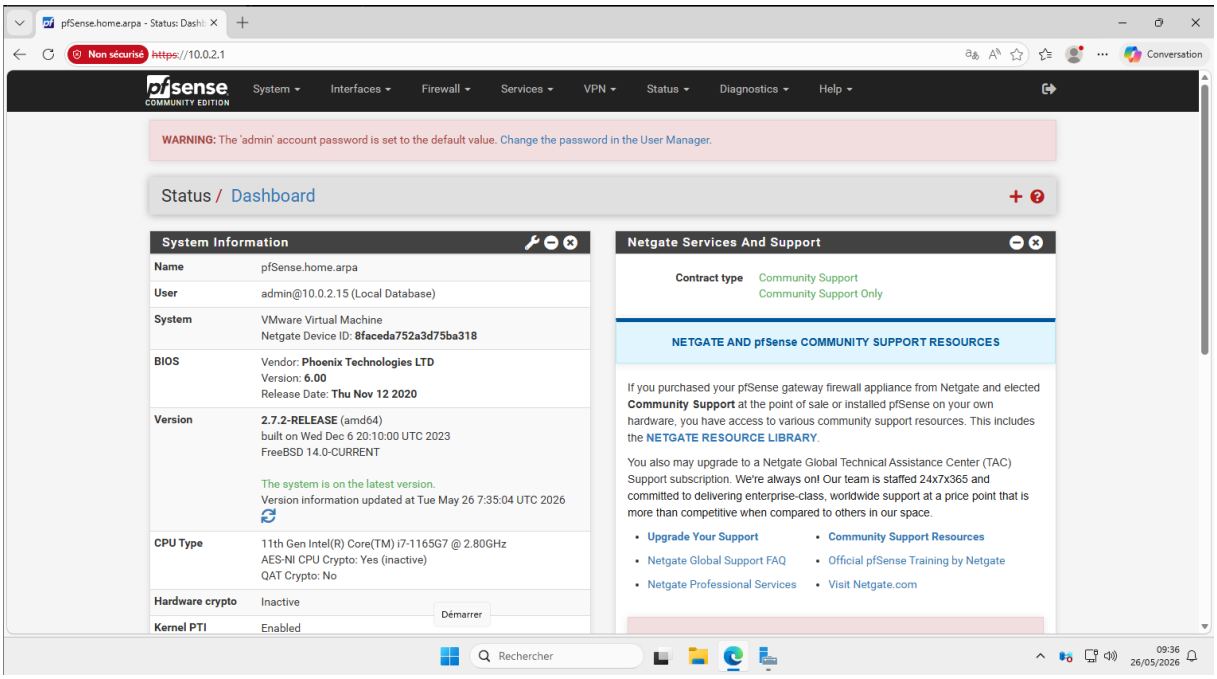
Les logins sont : admin/pfsense



Nous pouvons désormais procéder à la configuration du pare-feu pfSense.

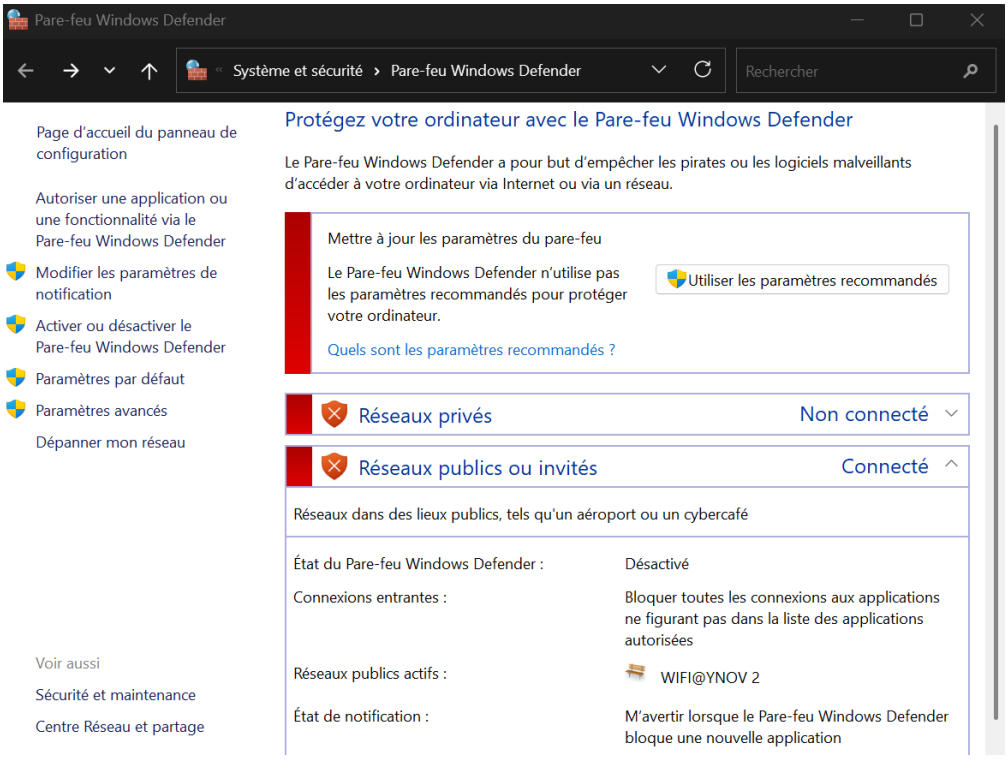
10.2 – Configuration de pfSense

Voici le tableau de bord de pfSense :



Nous allons essayer de nous y connecter depuis notre machine physique.

On désactive les pares-feux :



On ping notre PC depuis le pfSense :

```
Enter a host name or IP address: 192.168.49.1

PING 192.168.49.1 (192.168.49.1): 56 data bytes
64 bytes from 192.168.49.1: icmp_seq=0 ttl=128 time=0.485 ms
64 bytes from 192.168.49.1: icmp_seq=1 ttl=128 time=0.667 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=128 time=0.756 ms

--- 192.168.49.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.485/0.636/0.756/0.113 ms

Press ENTER to continue.
```

Dans l'autre sens, cela ne fonctionne pas (on ping l'adresse IP WAN du pfSense) :

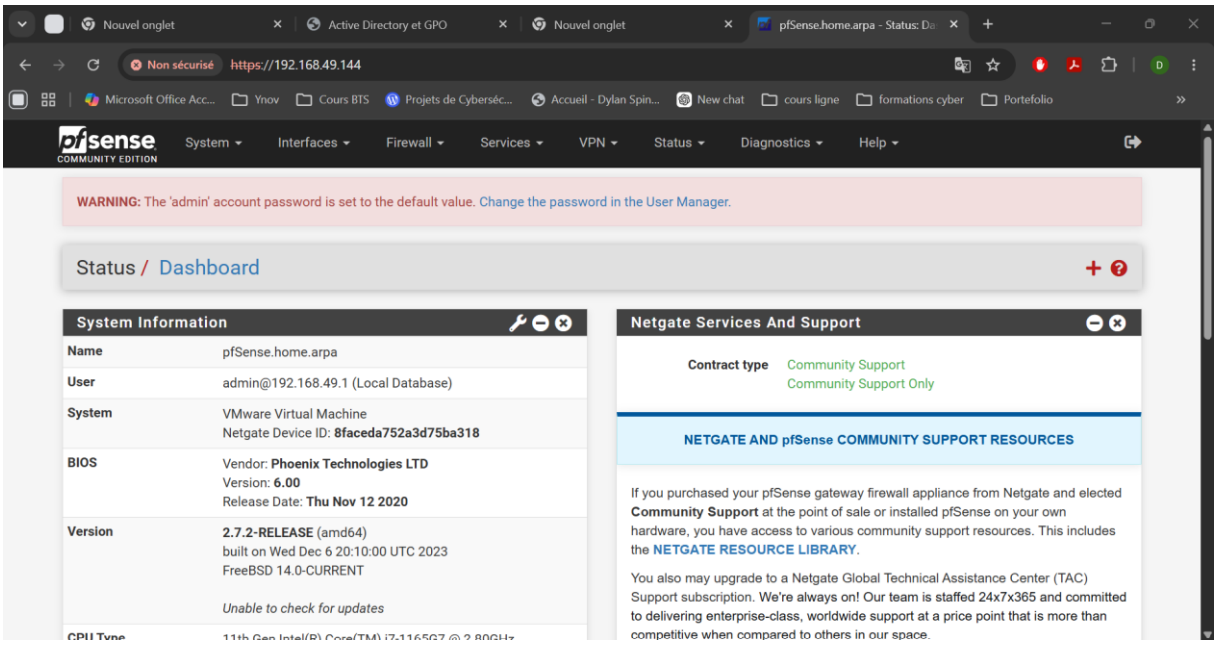
```
C:\Users\dylan>ping 192.168.49.144

Envoi d'une requête 'Ping'  192.168.49.144 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.49.144:
    Paquets : envoyés = 3, reçus = 0, perdus = 3 (perte 100%),
Ctrl+C
^C
```

On désactive également les pares-feux du pfSense :

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
```

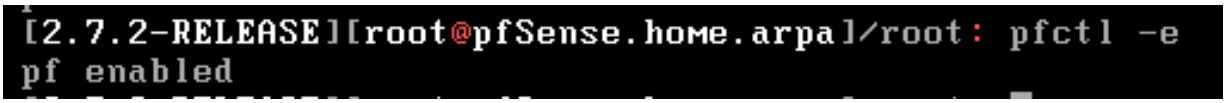
```
Enter a host name or IP address: 192.168.49.1

PING 192.168.49.1 (192.168.49.1): 56 data bytes
64 bytes from 192.168.49.1: icmp_seq=0 ttl=128 time=0.584 ms
64 bytes from 192.168.49.1: icmp_seq=1 ttl=128 time=0.635 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=128 time=0.405 ms

--- 192.168.49.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.405/0.541/0.635/0.099 ms

Press ENTER to continue.
```

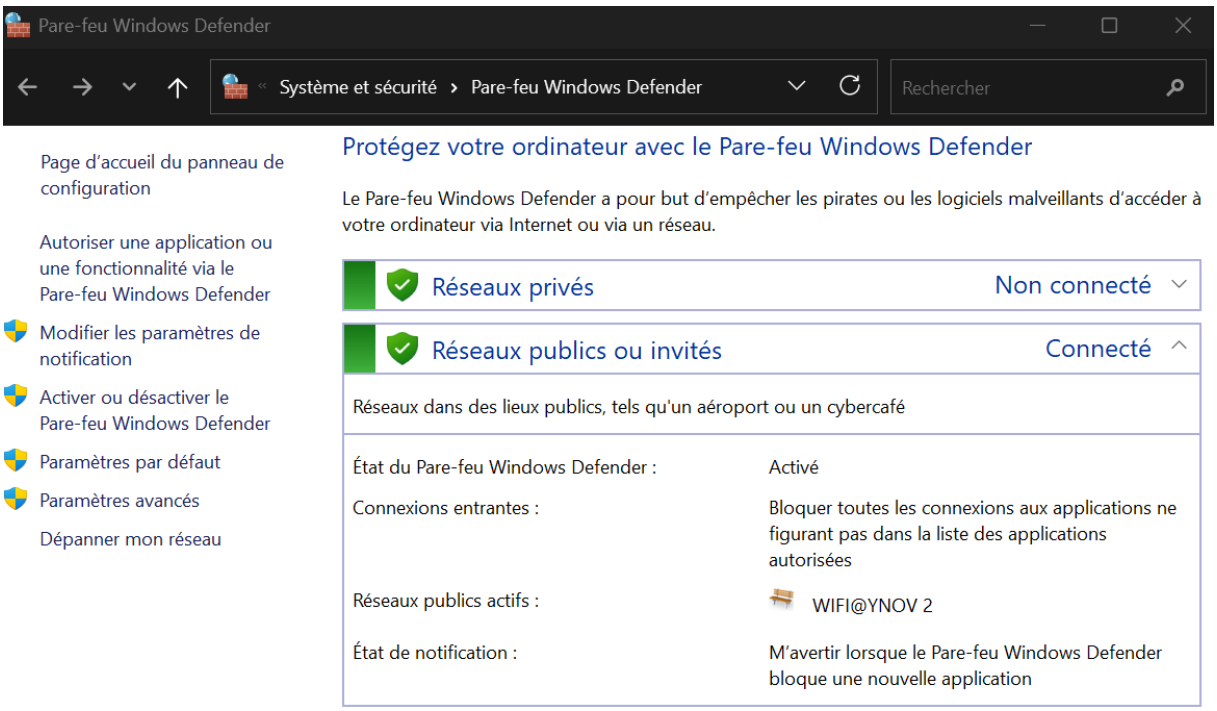
```
C:\Users\dylan>ping 192.168.49.144

Envoi d'une requête 'Ping'  192.168.49.144 avec 32 octets de données :
Réponse de 192.168.49.144 : octets=32 temps<1ms TTL=64
Réponse de 192.168.49.144 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.49.144 : octets=32 temps<1ms TTL=64
Réponse de 192.168.49.144 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.49.144:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 0ms
```



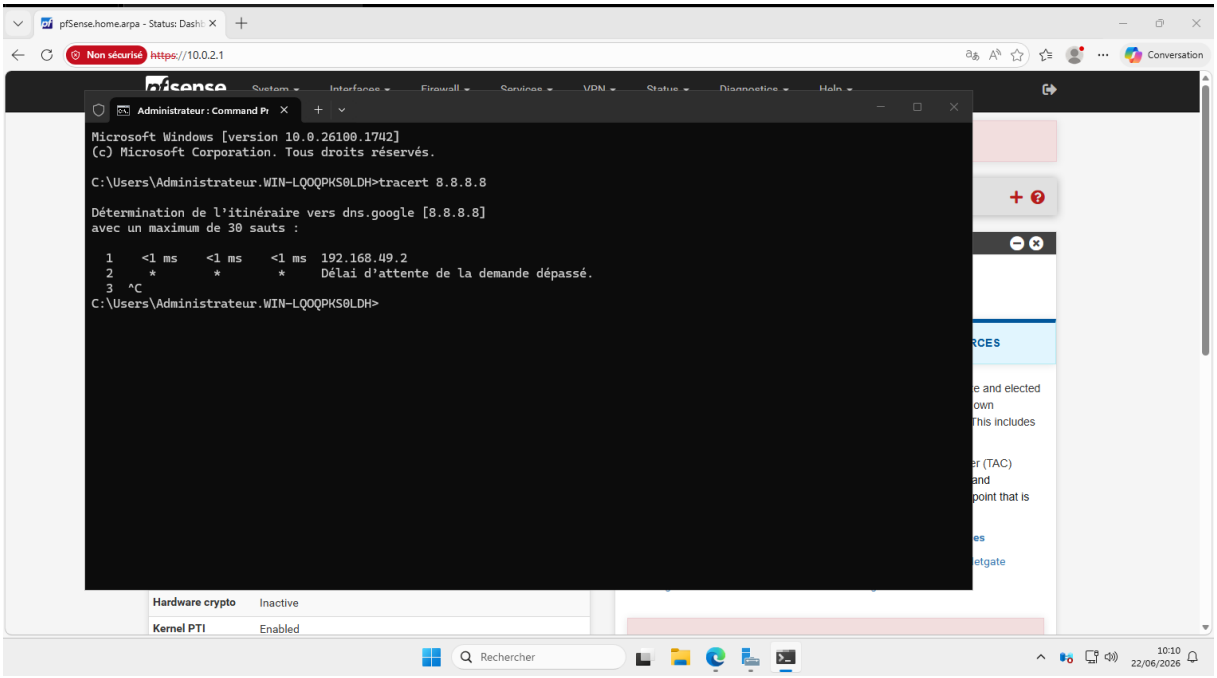
On arrive bien à se connecter au pfSense sur notre machine physique

On réactive ensuite l'ensemble des pares-feux :

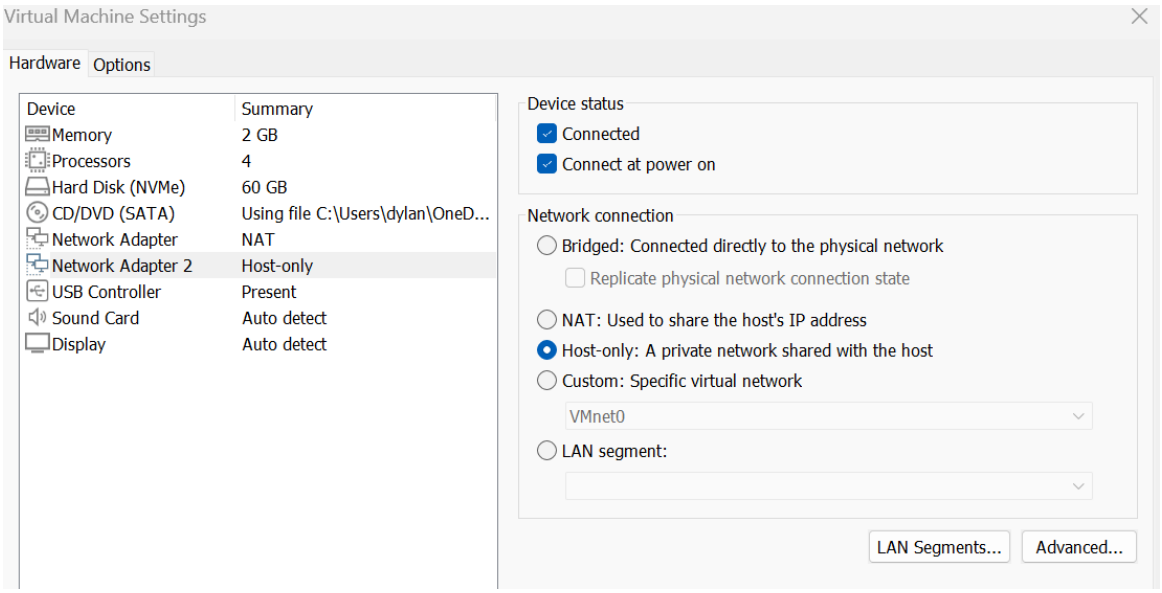




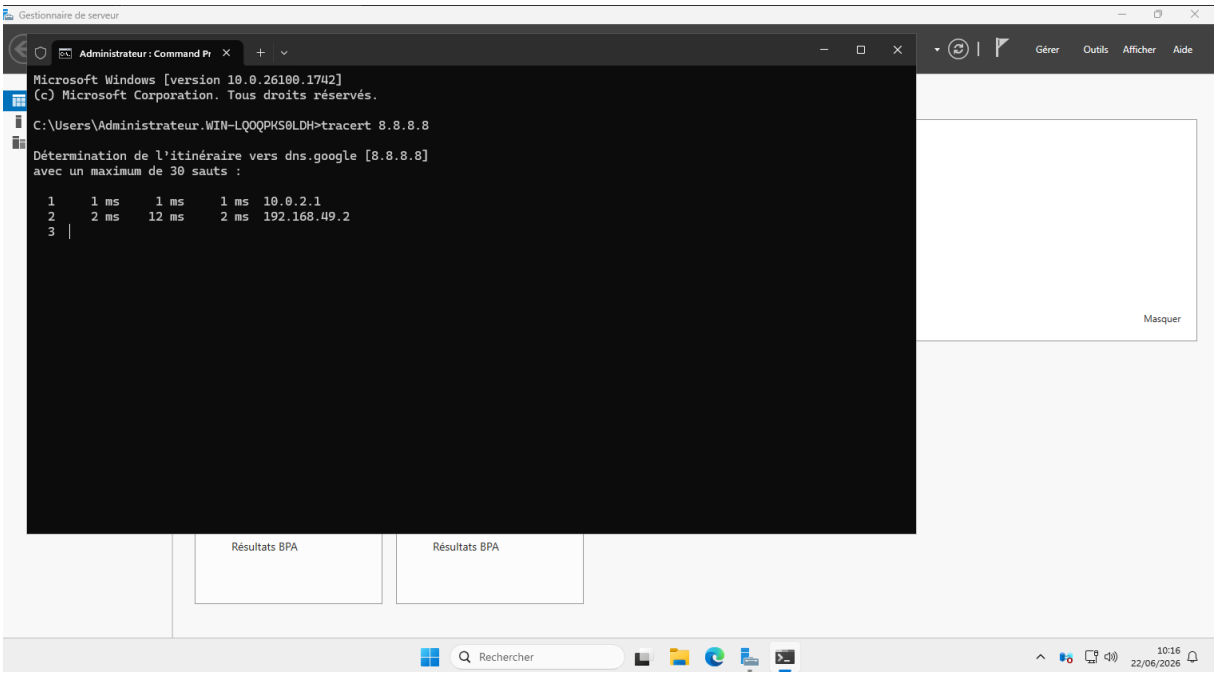
On s’aperçoit également que le trafic depuis le serveur contourne le pare-feu pfSense :



On retire donc la carte réseau NAT précédemment configurée :



On vérifie que le trafic passe bien par notre pare-feu :



On voit apparaitre l'adresse IP de notre pfSense : 10.0.2.1

Le trafic est donc bien redirigé vers notre pare-feu.