Fiche technique M2L

Réaliser par JOVANOVIC William / MILIC Daniel / SALANDINI Enzo

Session 2024-2025

SOMMAIRE

Introduction

La Maison des Ligues de Lorraine souhaite moderniser son infrastructure réseau afin d'améliorer la gestion des utilisateurs, centraliser l'administration des machines et renforcer la sécurité de son système informatique.

Actuellement, l'absence d'une gestion centralisée complexifie l'administration, freine l'organisation et nuit à la sécurisation des postes. Pour répondre à cette problématique, le projet vise à mettre en place une infrastructure réseau complète, fondée sur les éléments suivants :

Installation de PfSense en tant que pare-feu pour filtrer les flux entrants/sortants et sécuriser l'environnement réseau,

Déploiement de Windows Server 2022 pour héberger un contrôleur de domaine Active Directory, accompagné des services DNS et DHCP pour une configuration réseau automatique et centralisée,

Ajout des postes clients dans le domaine, pour une gestion unifiée des utilisateurs et des machines,

Création d'unités d'organisation (OU) et gestion des comptes utilisateurs selon les services (RH, Compta, Informatique...),

Déploiement automatisé de logiciels via des GPO,

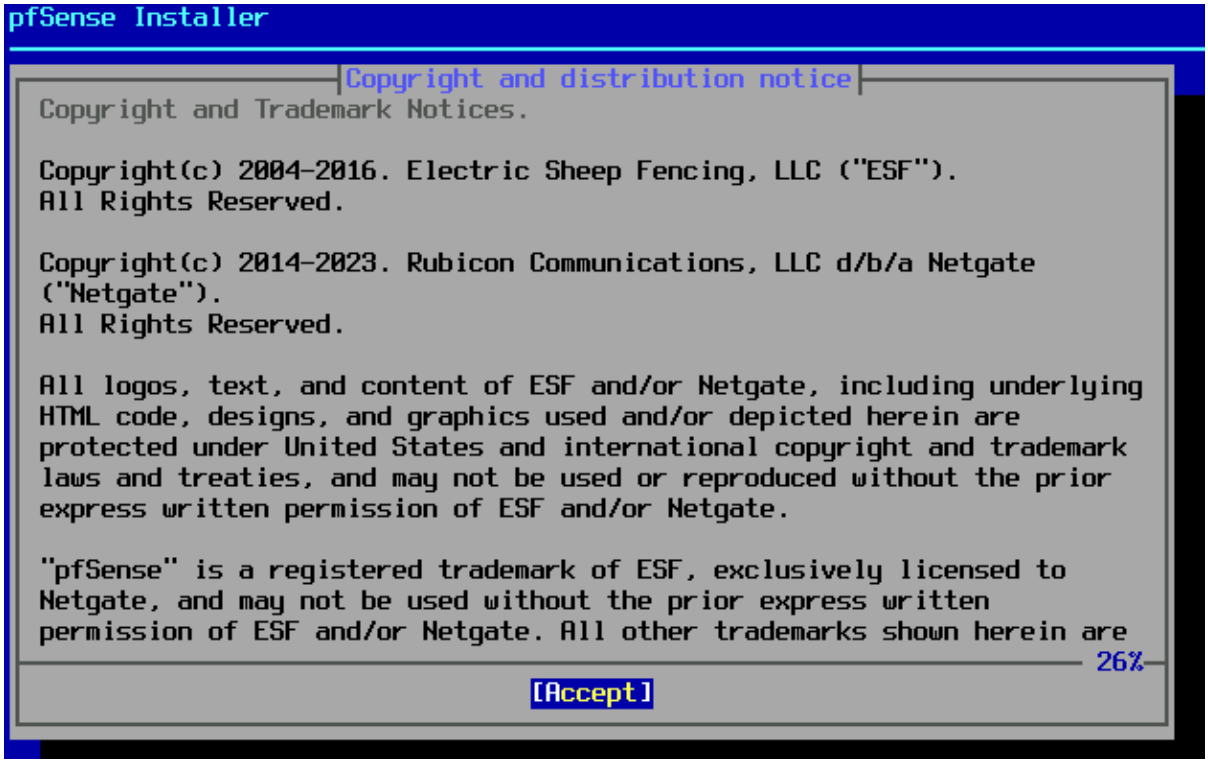
Création de répertoires partagés mappés automatiquement en fonction du service auquel appartient chaque utilisateur.

Ce projet a donc pour but de professionnaliser et sécuriser l'environnement informatique interne grâce à une infrastructure claire, centralisée, sécurisée et automatisée. Il facilitera l'administration du réseau tout en améliorant l'expérience utilisateur au sein de la structure.

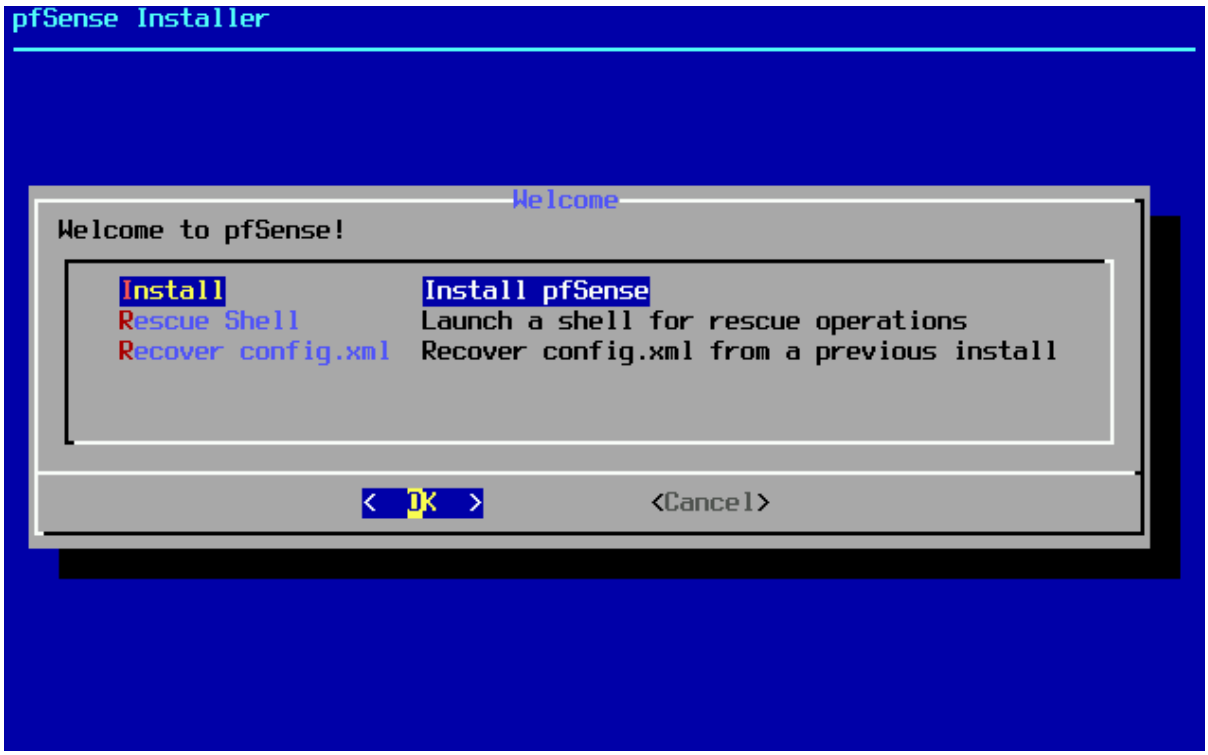
Installation de PfSense

Configuration de base

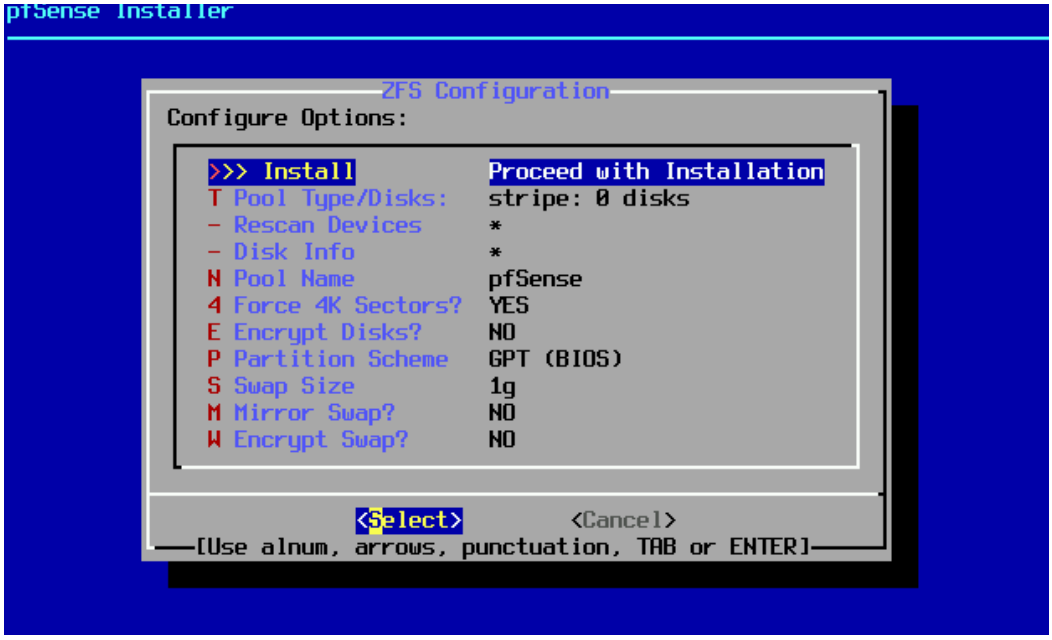
Sélectionné accept



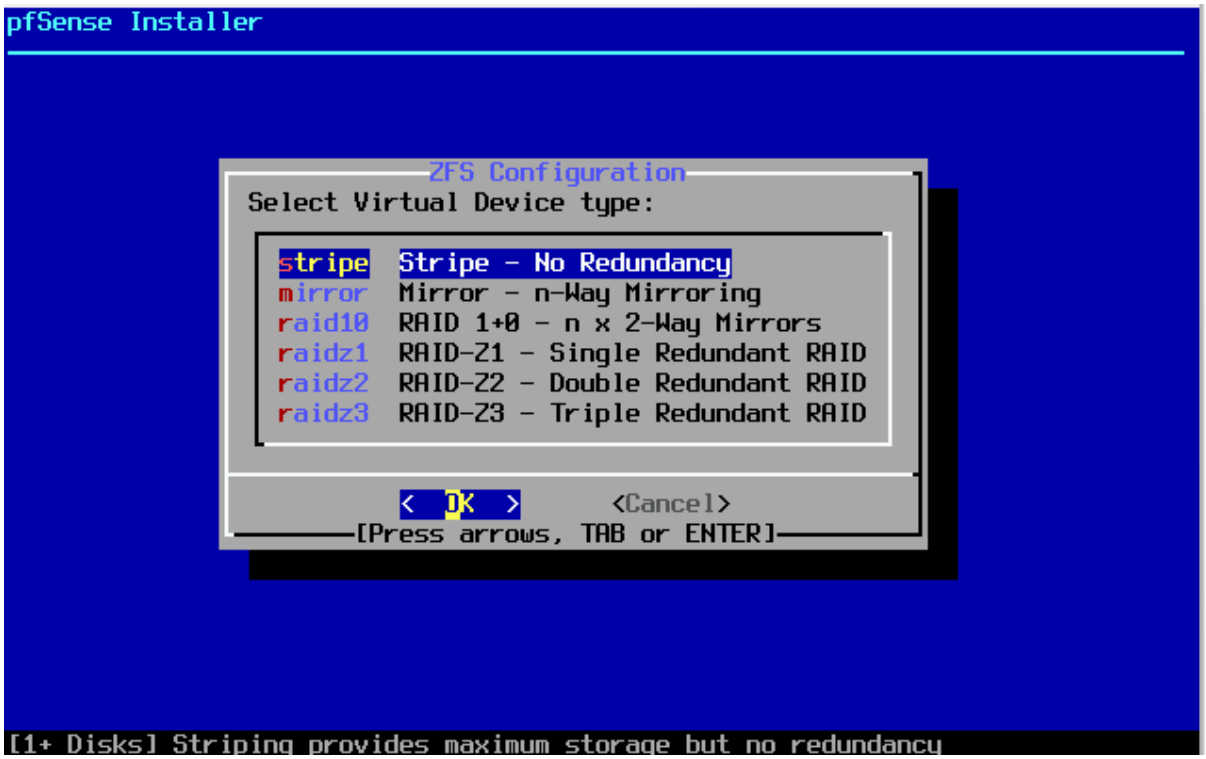
Sélectionné Install pour commencer l'installation du pfsense



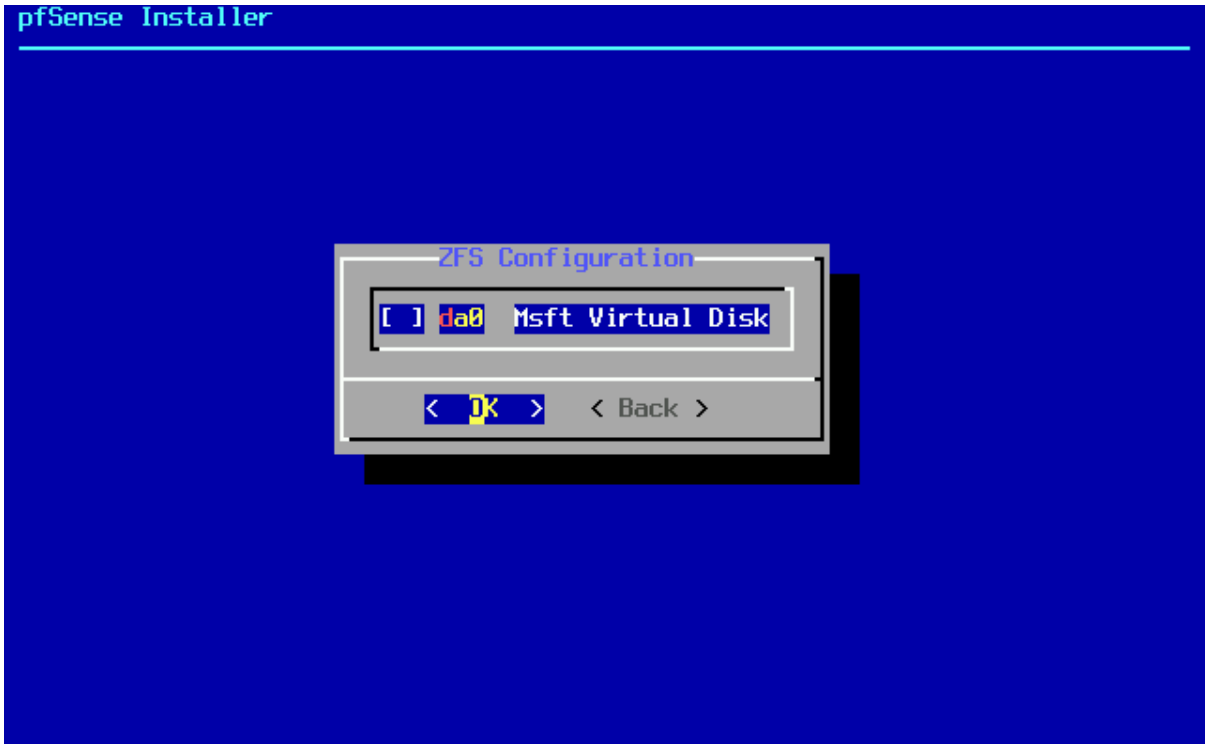
Installation guidée.



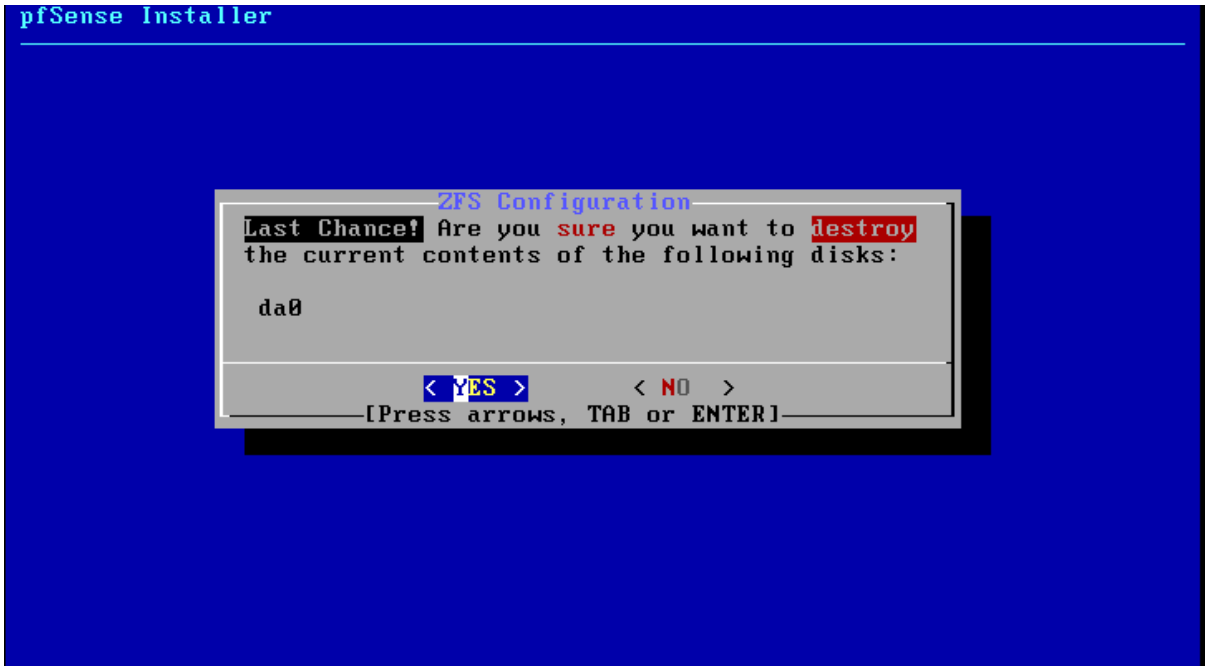
Sélectionner Stripe

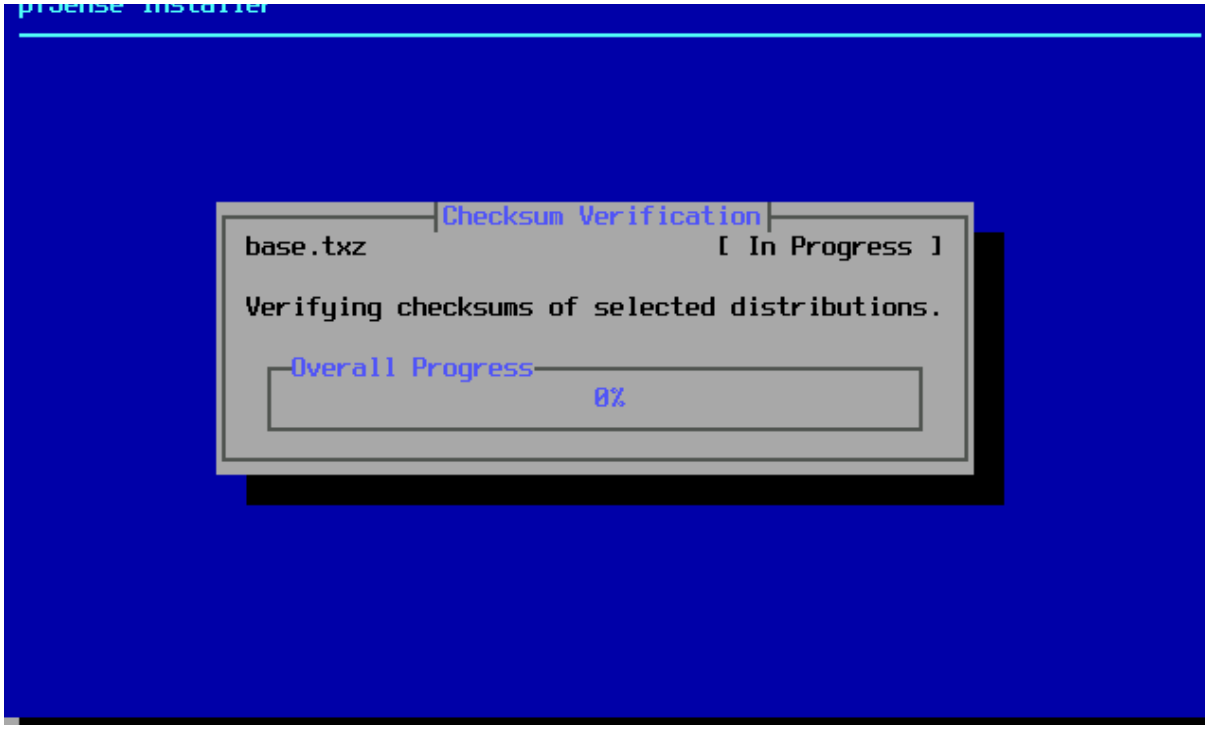


Choix du disque (appuyer sur espace puis entré)

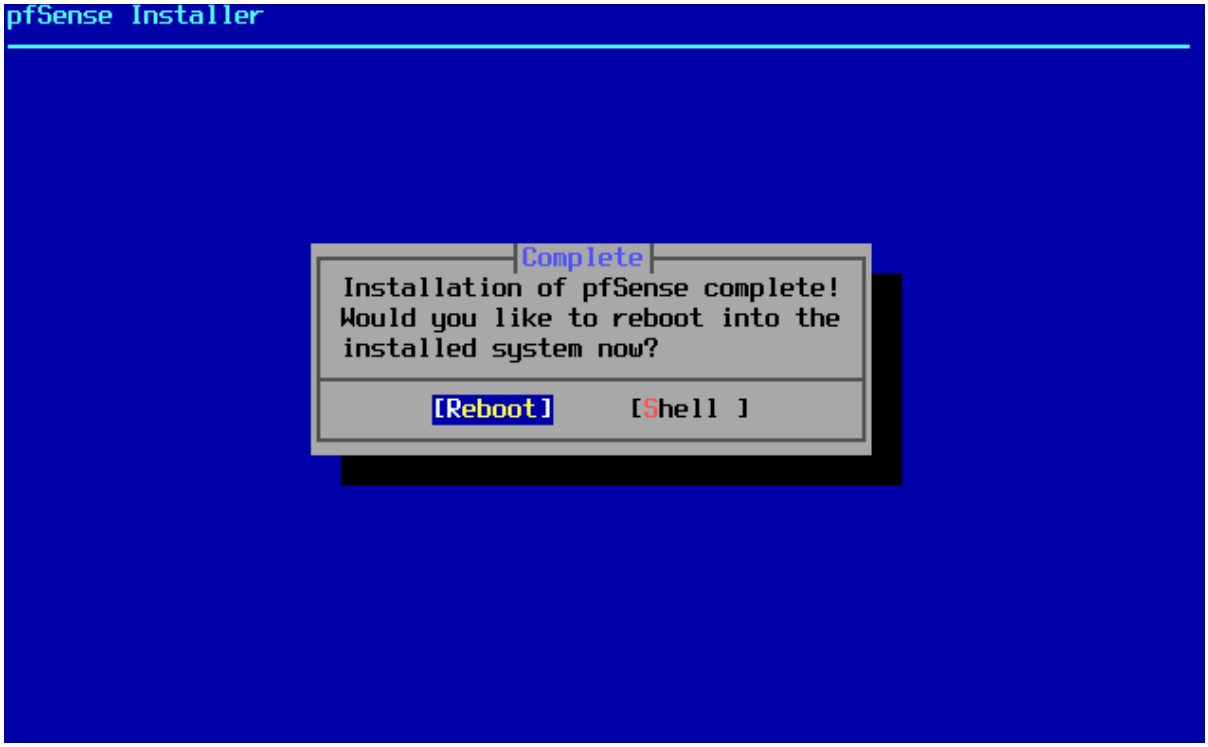


Confirmation



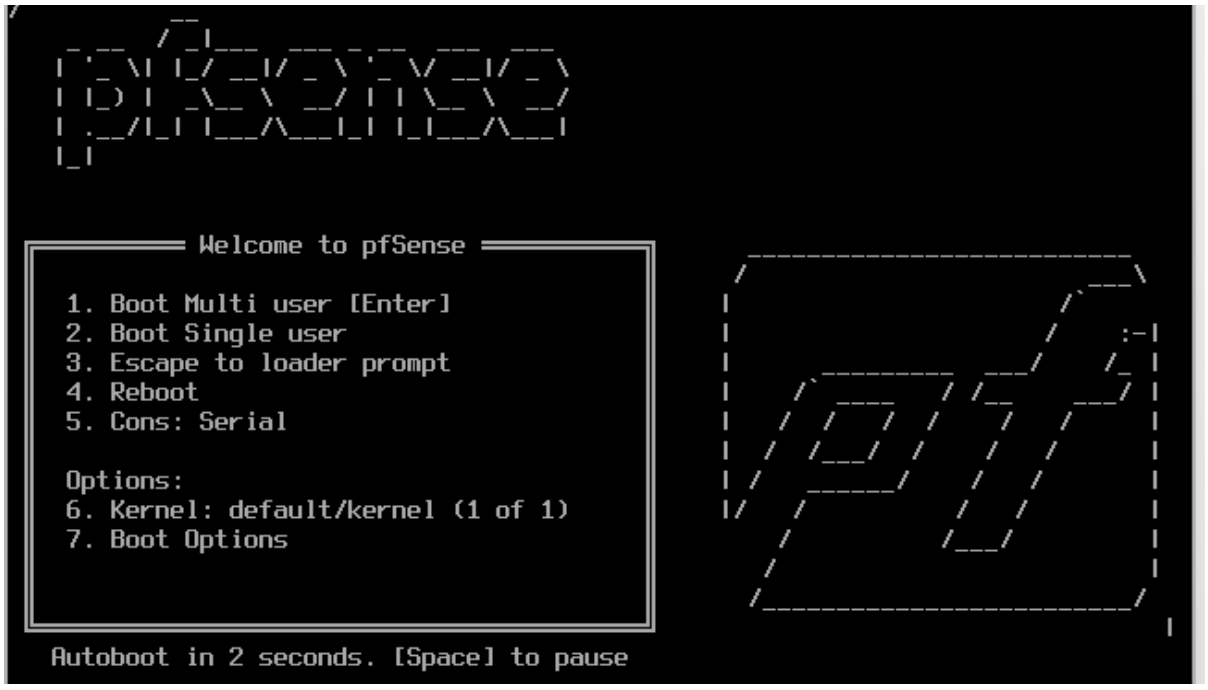


Faite entré sur reboot pour redémarrer votre machine

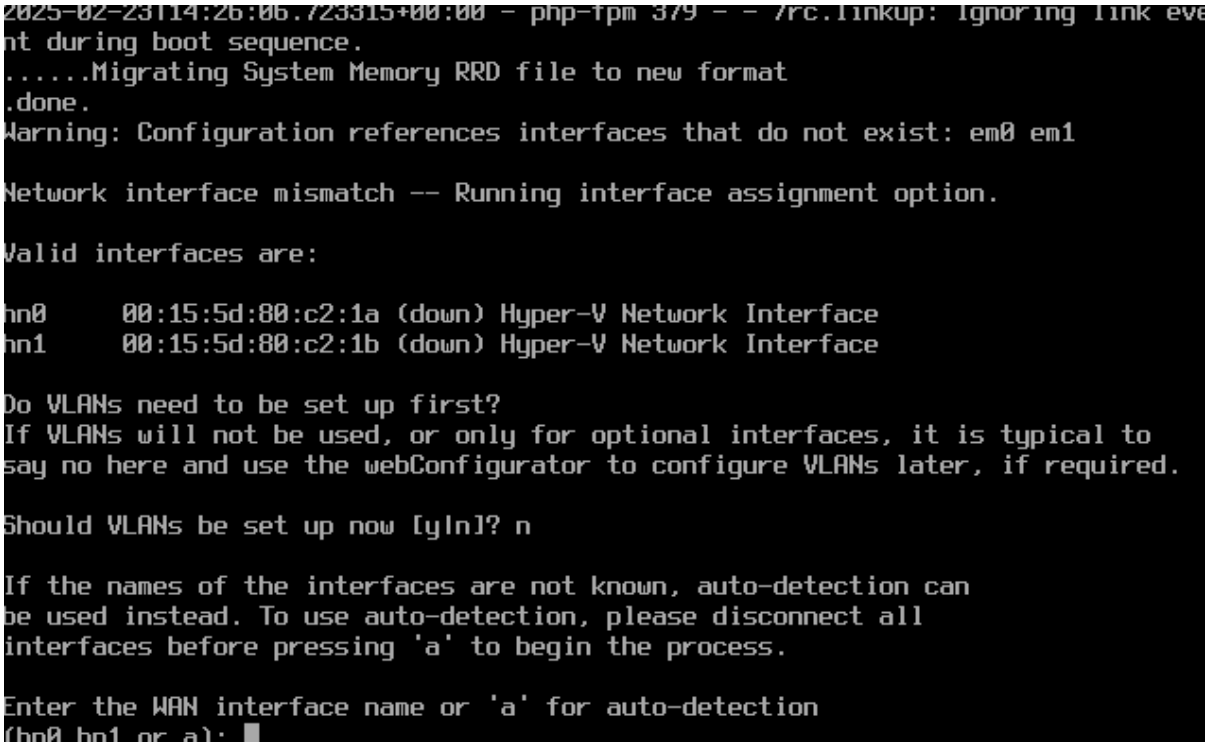


Penser à éjecter le disque.

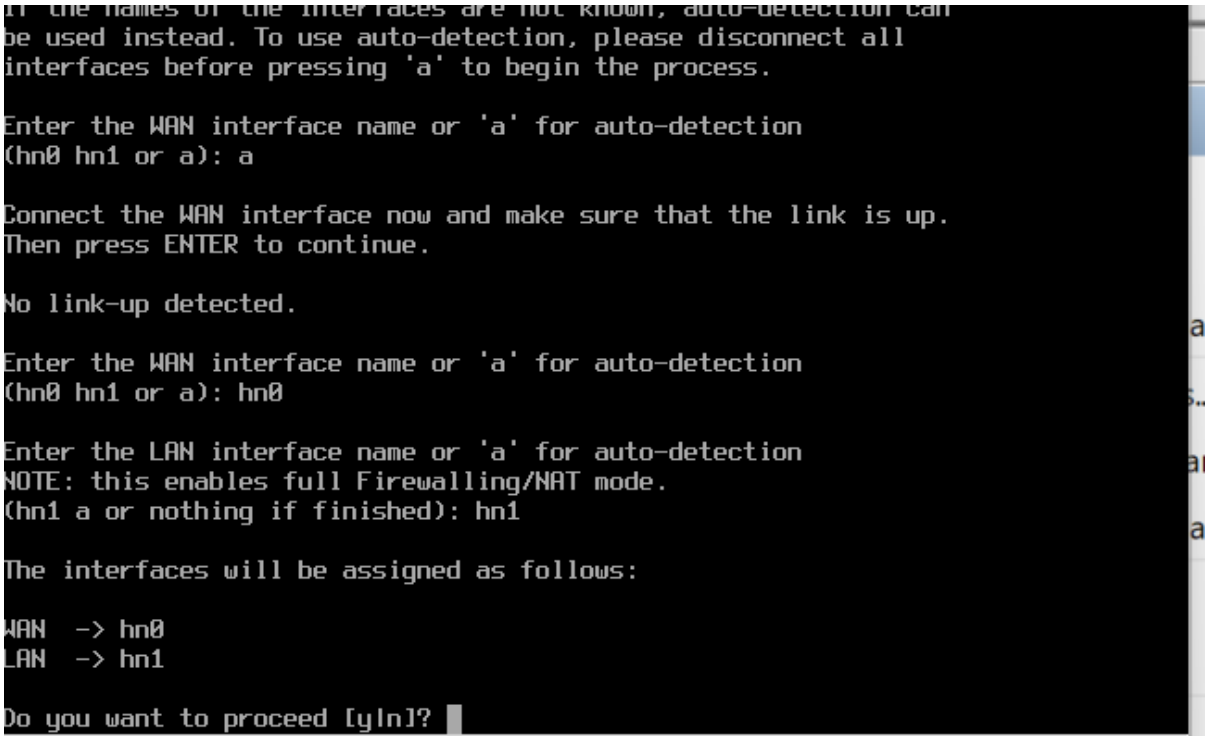
Configuration des interfaces.



Pas de configuration de vlan



Choix des interfaces.22



Configuration de l'IP LAN.

Choisir l’option 2

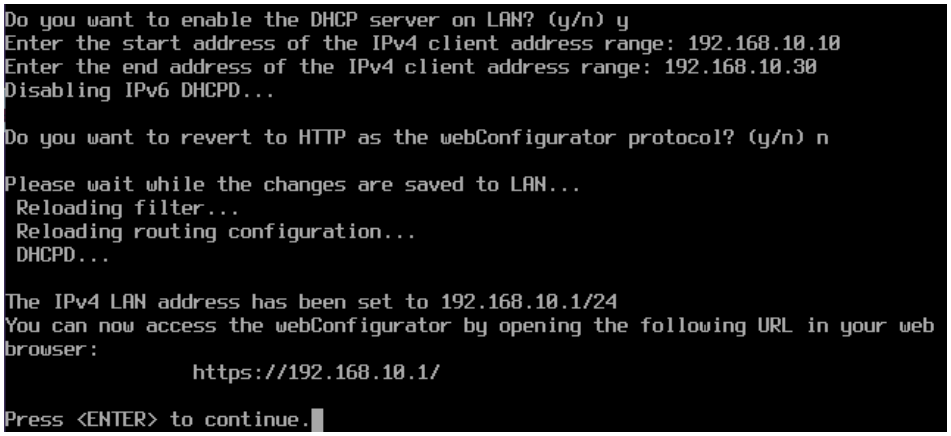
```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

Microsoft Azure - Netgate Device ID: d2c56c44dcd05faa0b84

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP4: 172.19.43.48/20
 LAN (lan)       -> hn1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

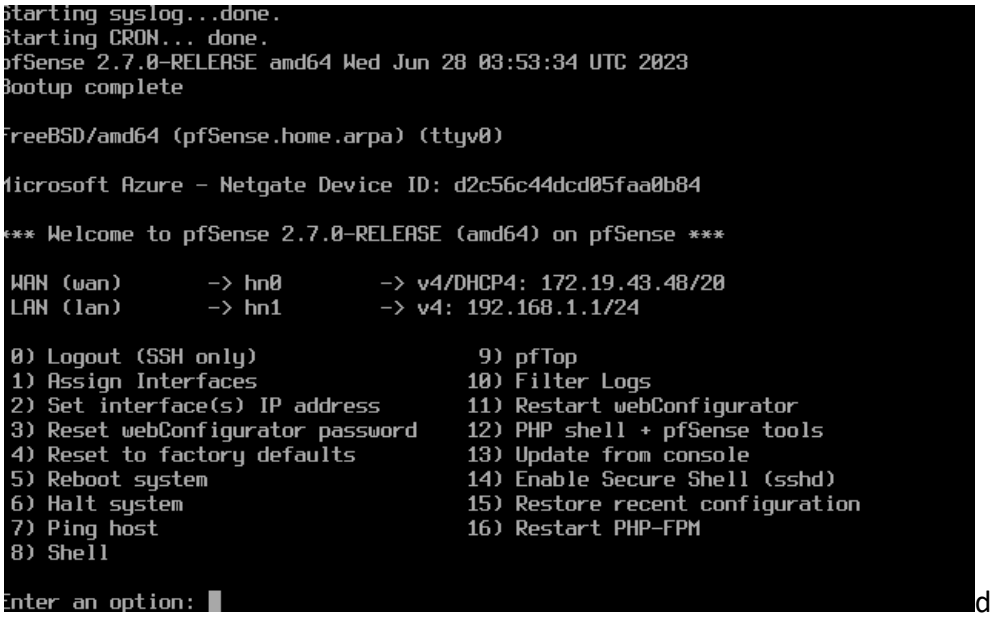
Paramétrage de l'interface LAN, Lorsque vous y êtes invité, tapez-y pour activer le serveur DHCP sur l'interface LAN.

```
Enter an option: 2

Available interfaces:

1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - 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:
> 192.168.10.1/24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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) y
```

Tapez n lorsqu’il vous est demandé si vous souhaitez revenir à HTTP pour l’interface web — cela permet de conserver une connexion sécurisée via HTTPS.

Puis appuyez sur Entrée pour continuer.

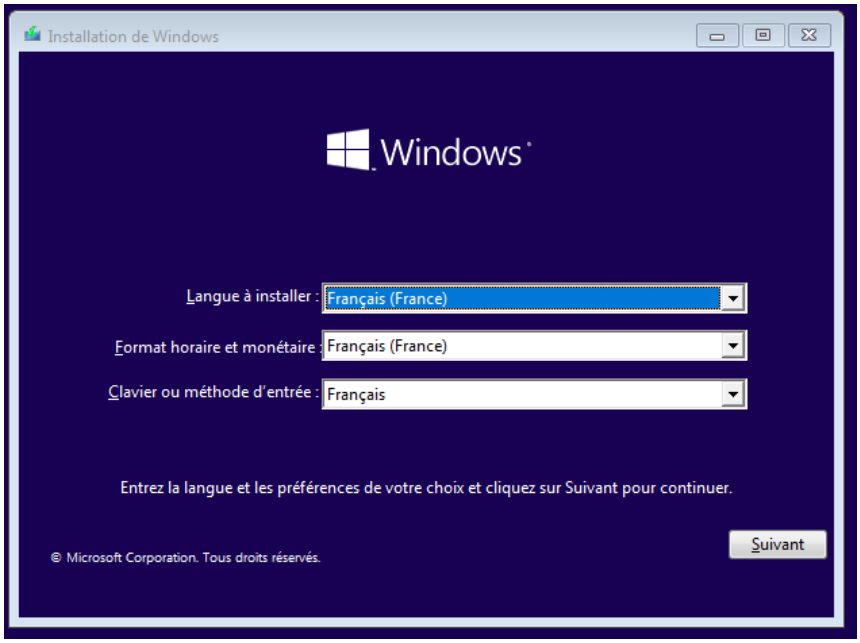




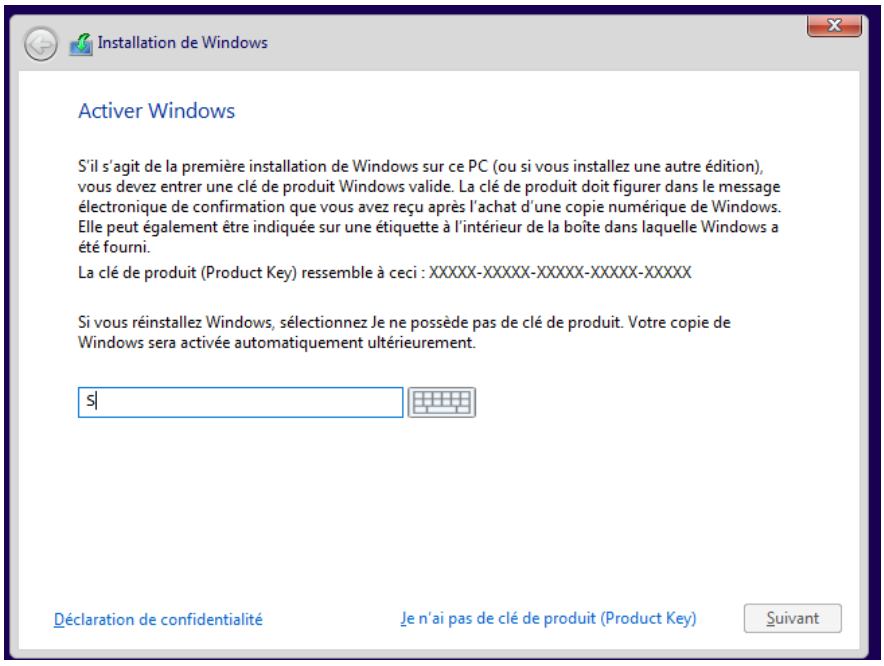
d

Installation de Windows.

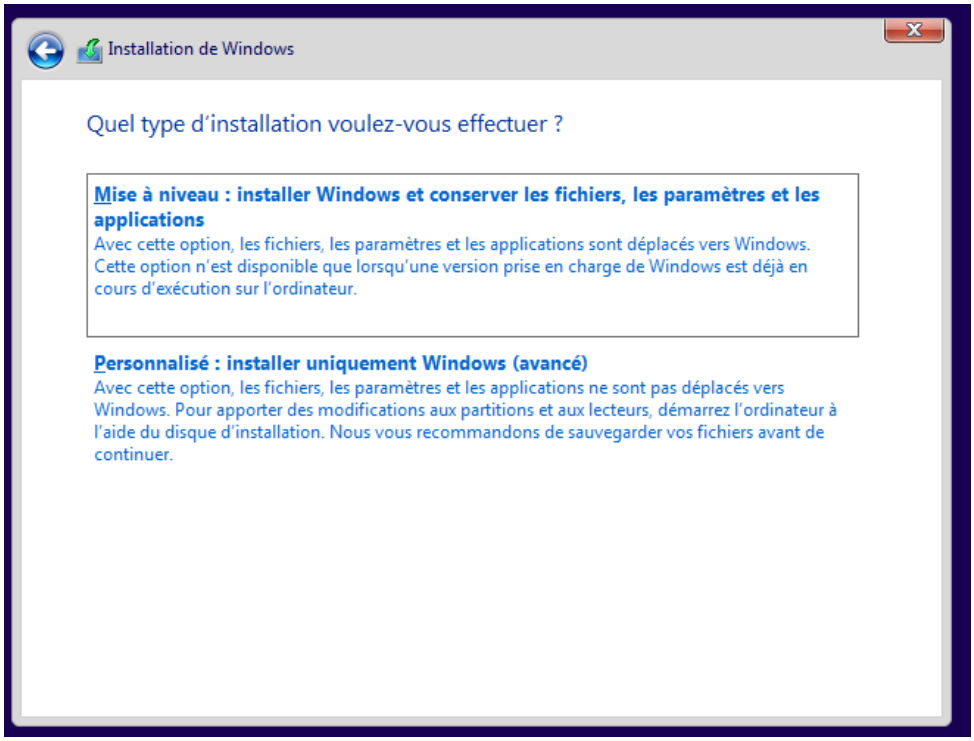
Choisir la langue du système



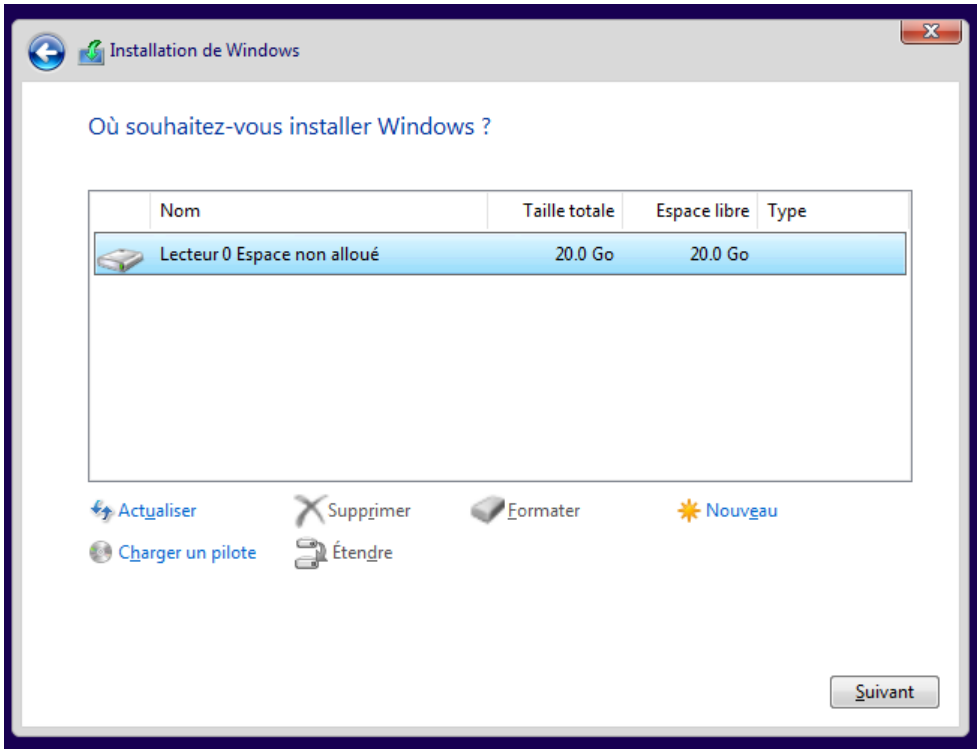
Renseigner une clé d'activation.



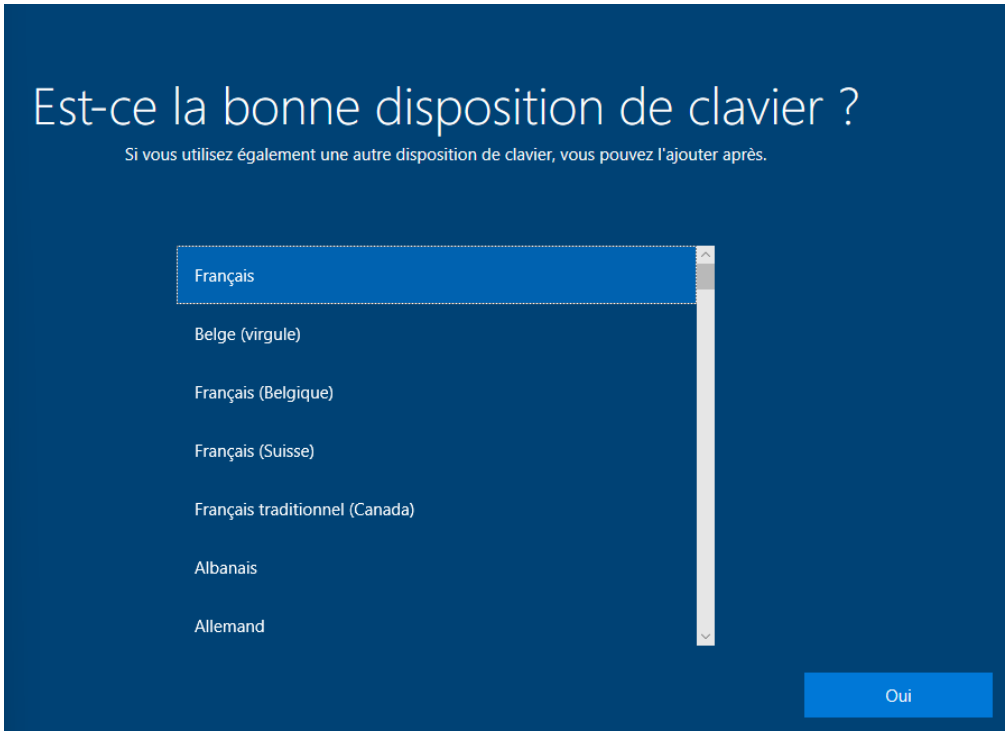
Choisir le type d'installation (ici personnalisé).



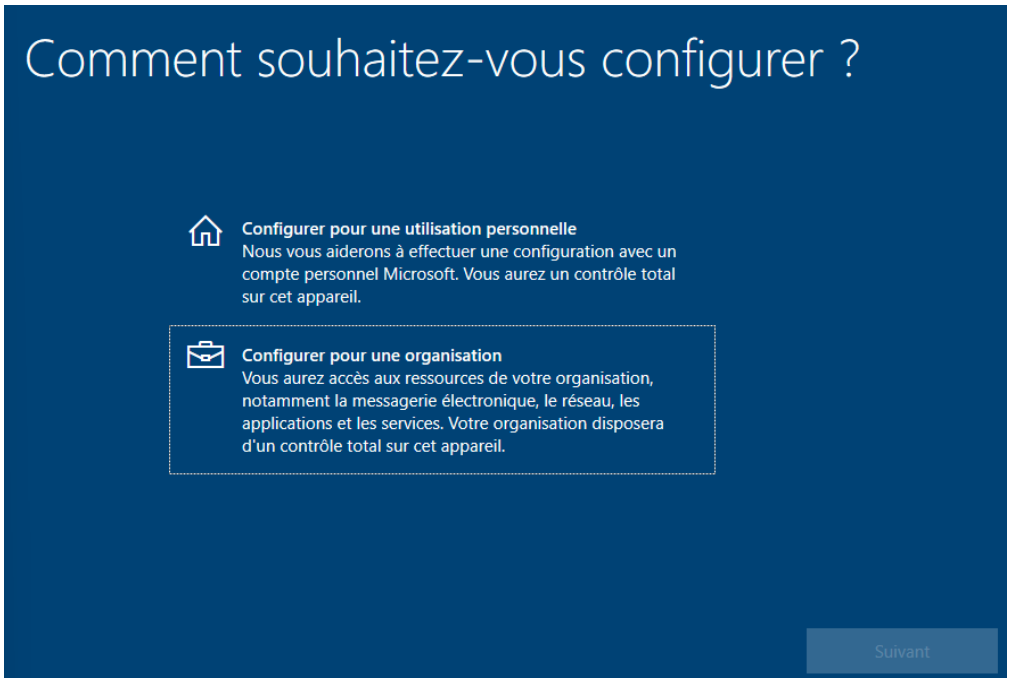
Sélectionner le disque d'installation.



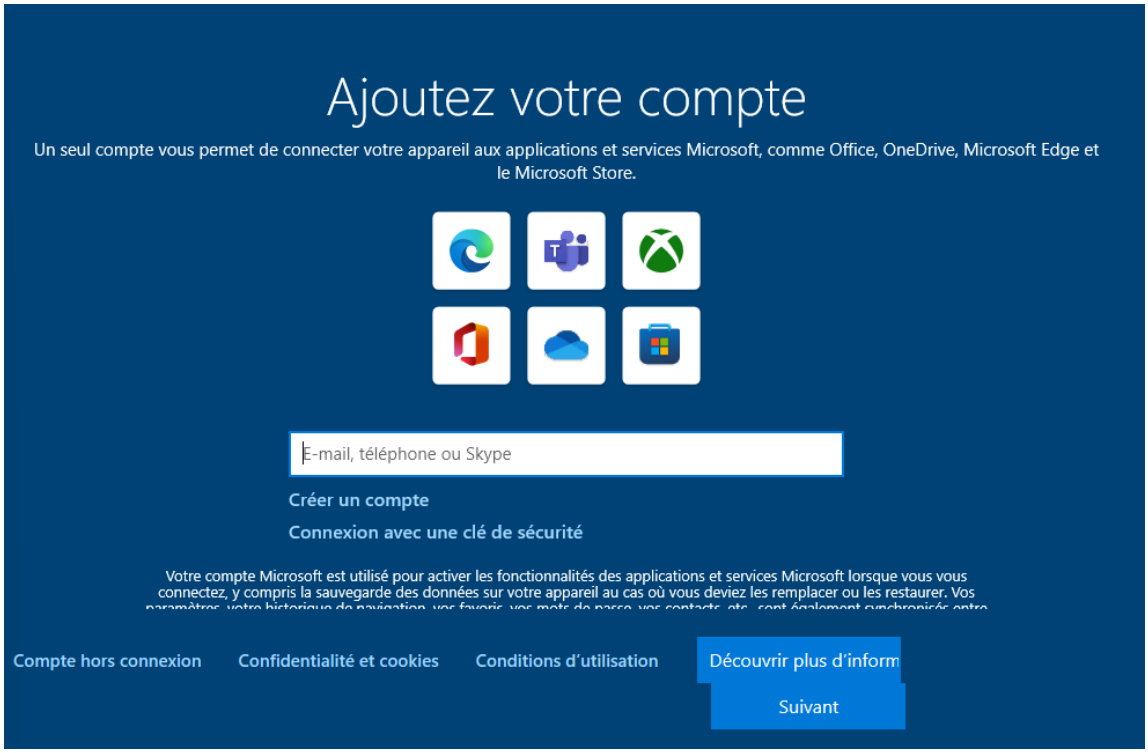
Choisir la région du système et la disposition du clavier.



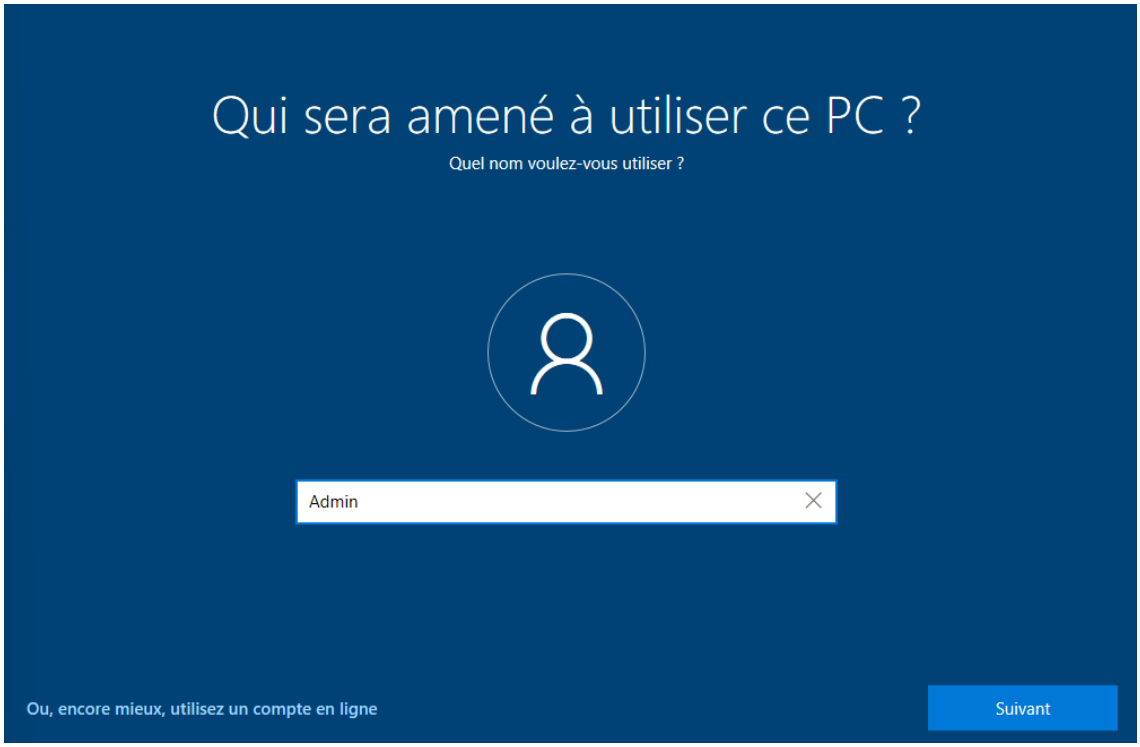
Choisir la configuration (ici personnelle).



Choisir un type de compte (ici hors connexion)

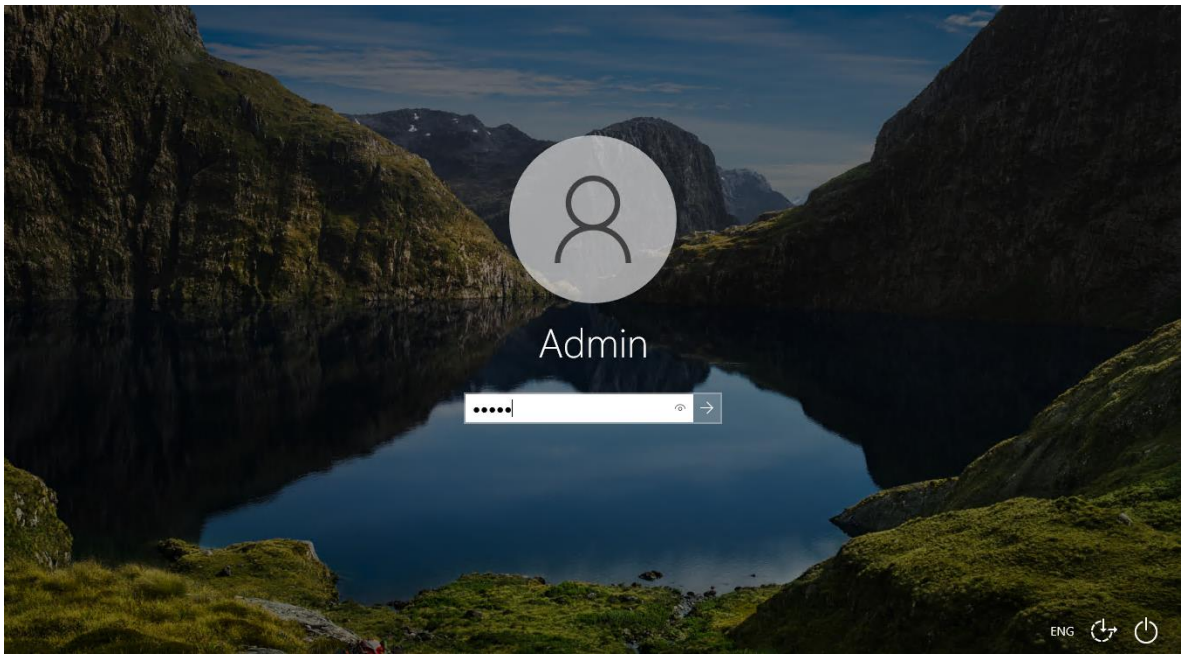


Choisir un nom d'utilisateur



Choisir un mot de passe

Personnaliser l’expérience utilisateur.

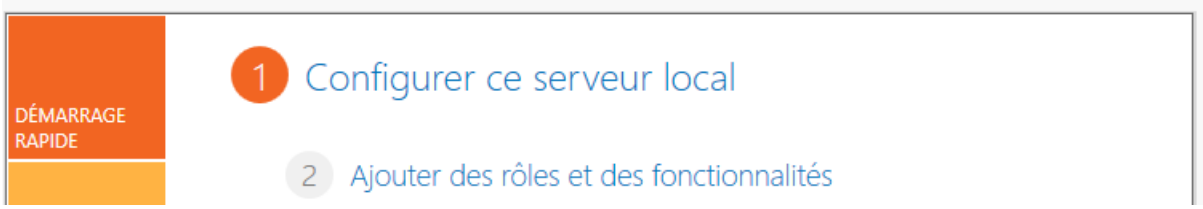


Procédure Active directory

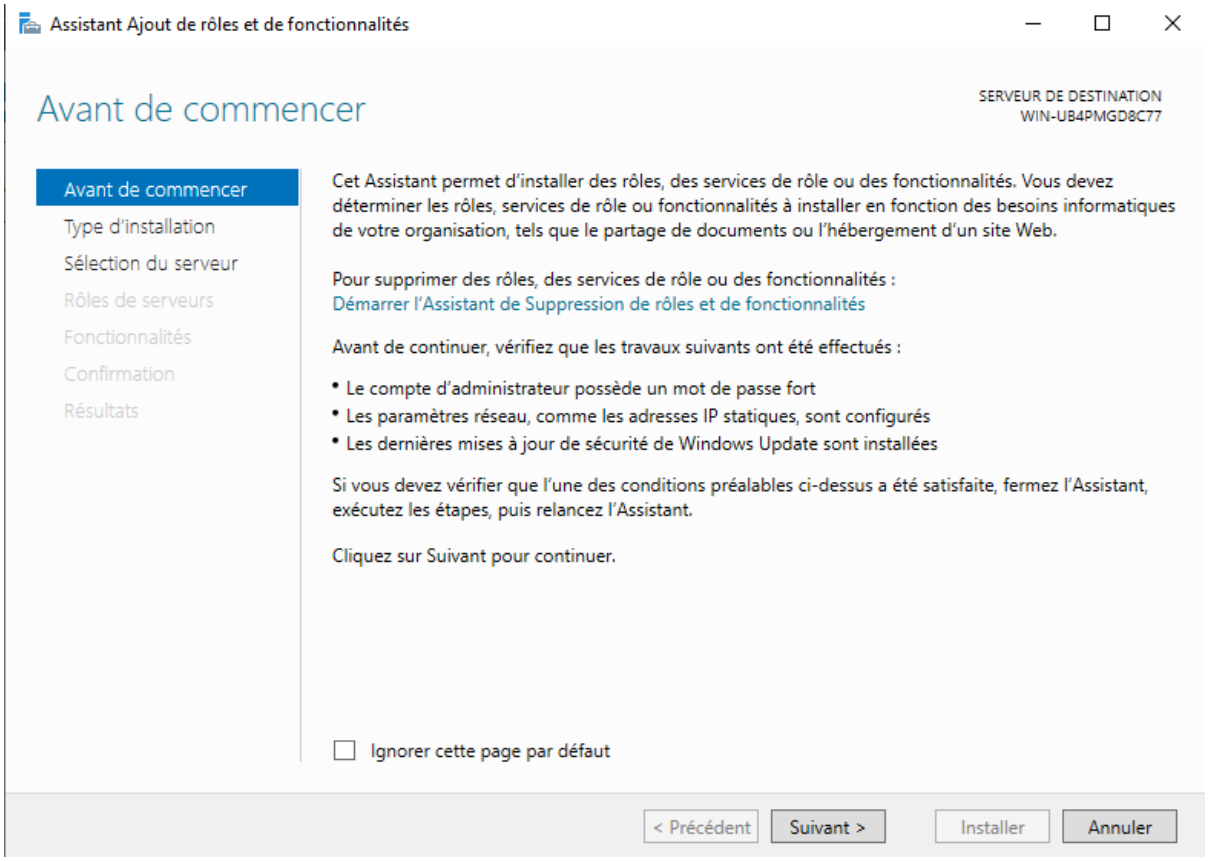
Création serveur Active directory

Installation du rôle d’Active directory

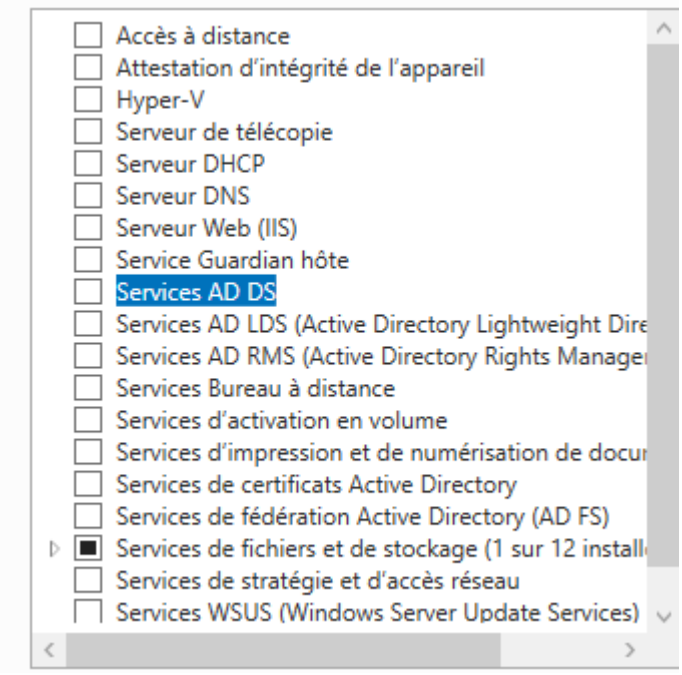
Commençons par cliquer sur ‘ajouter des rôles et des fonctionnalités’



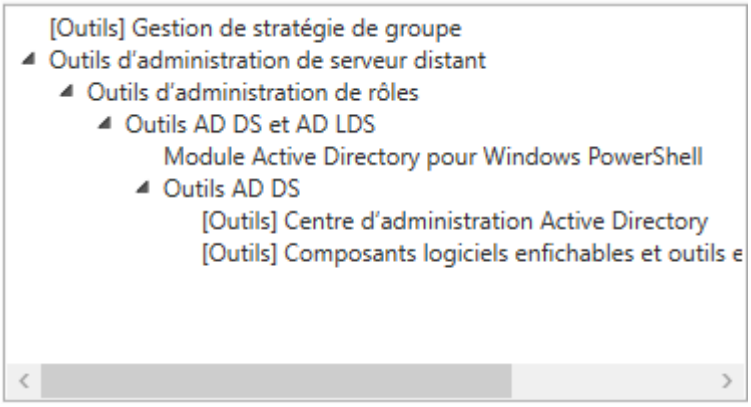
Depuis la page ‘avant de commencer’ poursuive jusqu'à ‘rôle de serveurs’ en cloquant sur le bouton “suivant”



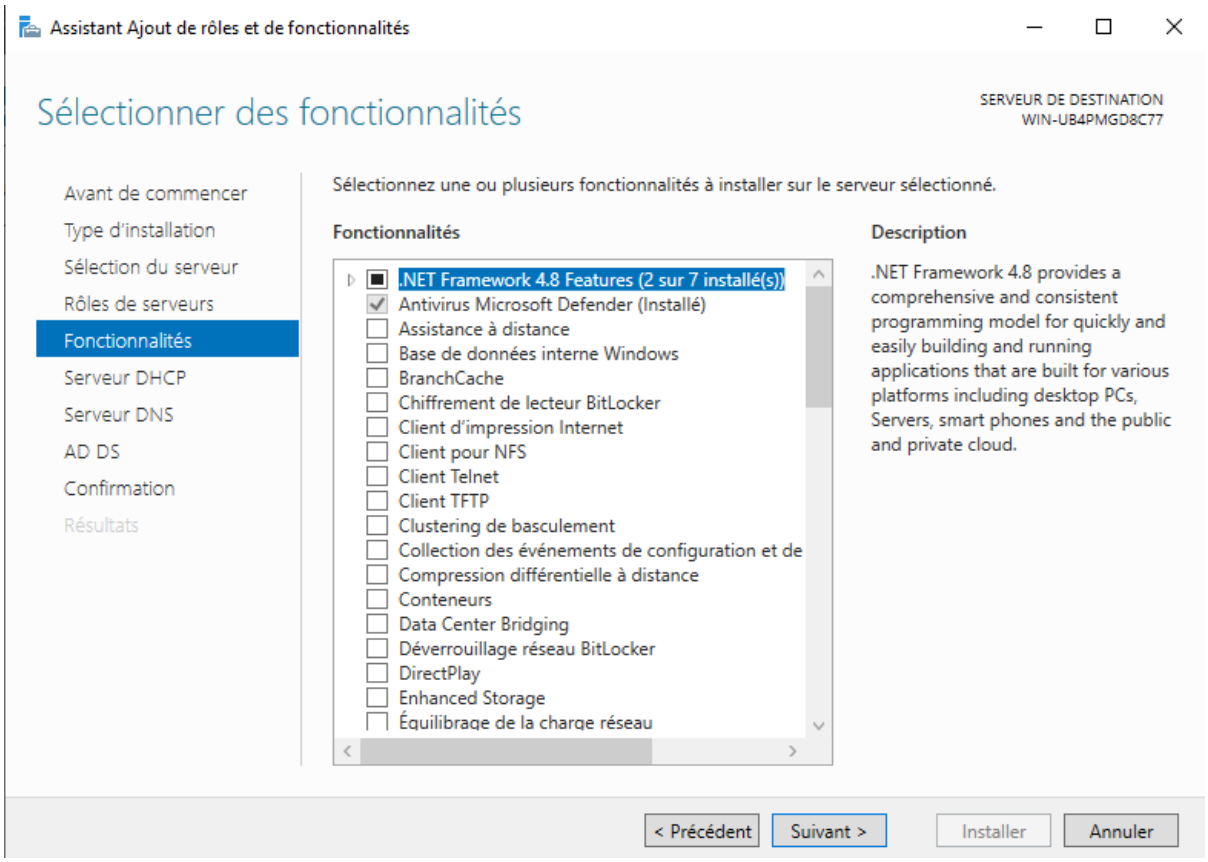
Selectionné le rôle désiré dans notre cas ’Service AD DS’



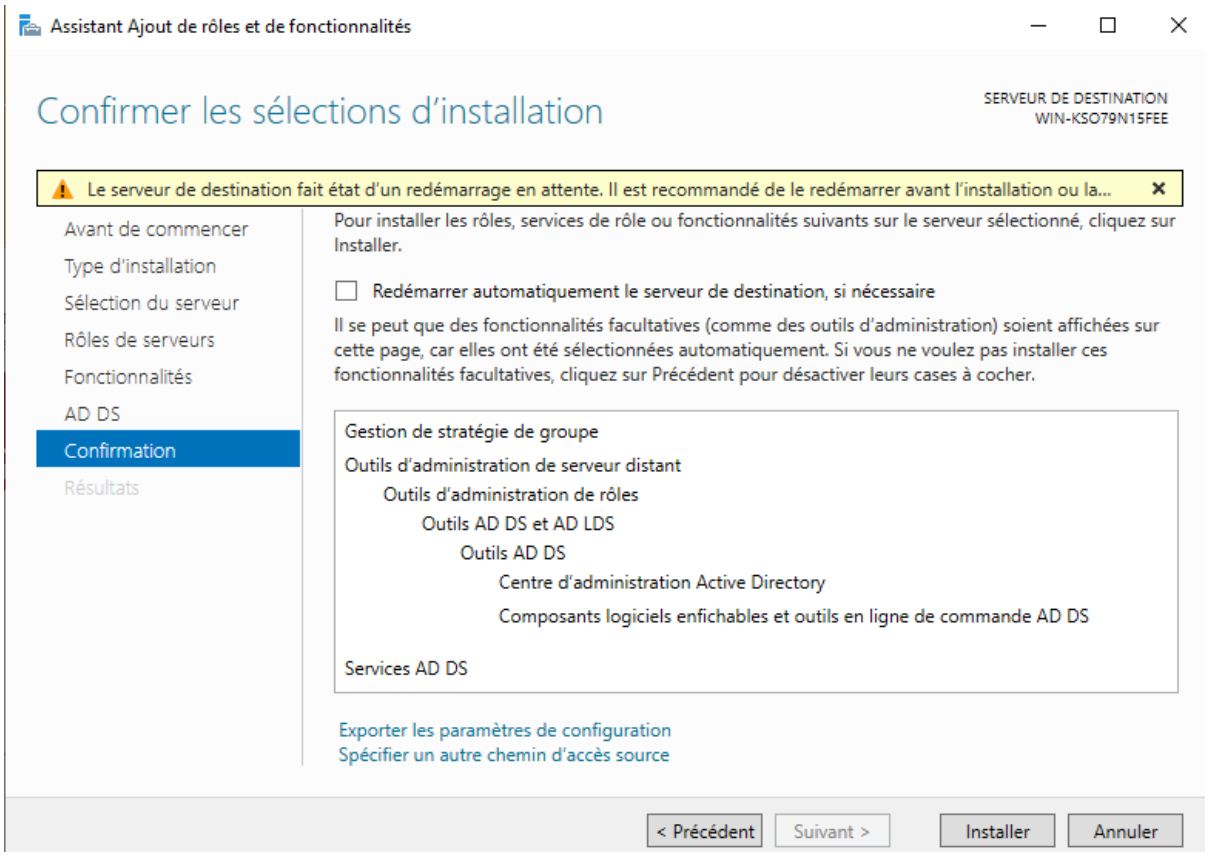
Accepté la page des fonctionnalités nécessaire qui vas s’ouvrir et cliqué enssuite sur suivant



Poursuivre jusqu'à confirmation

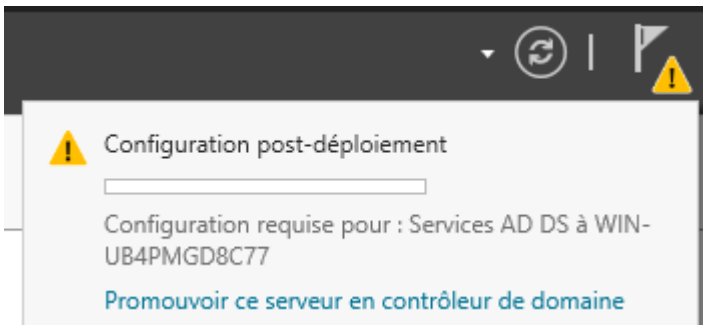


Puis cliqué sur installation.

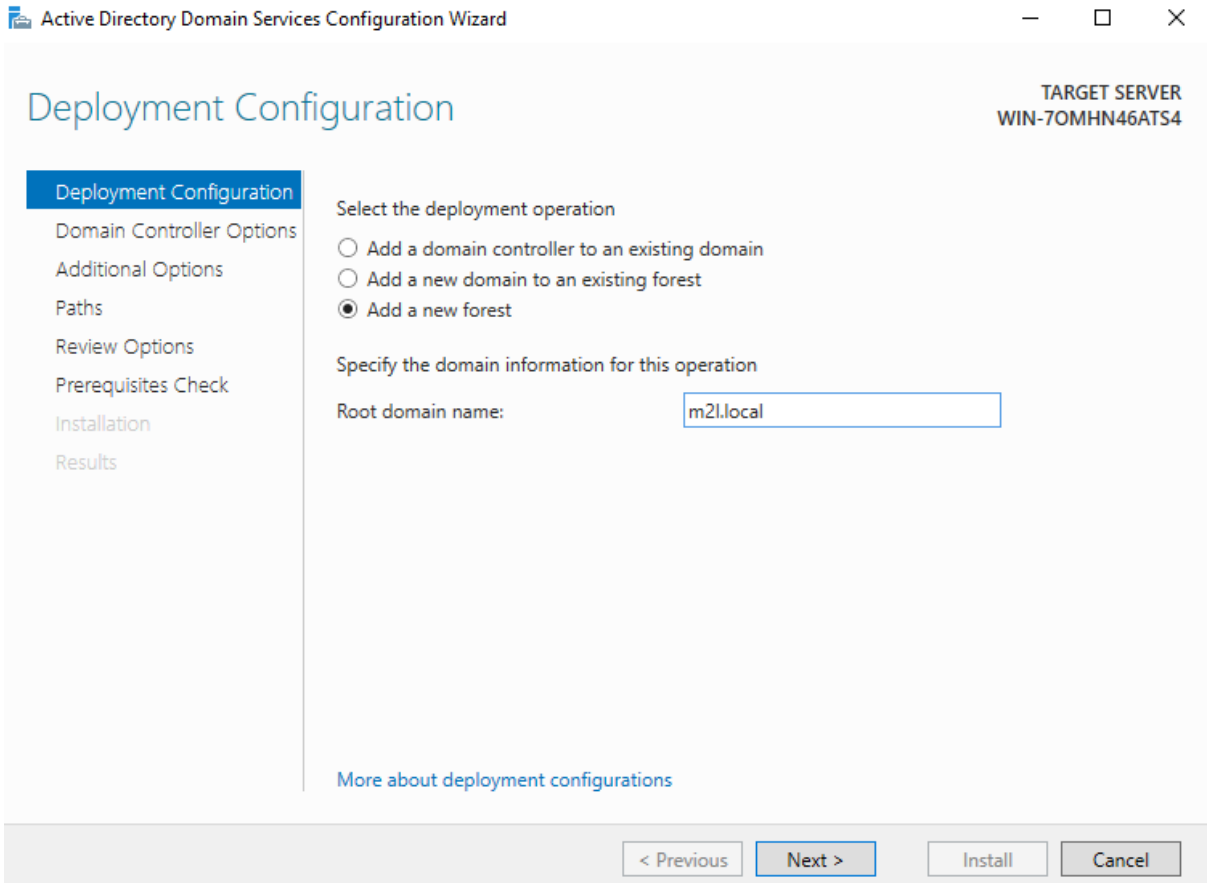


Configuration des services de domaine Active directory

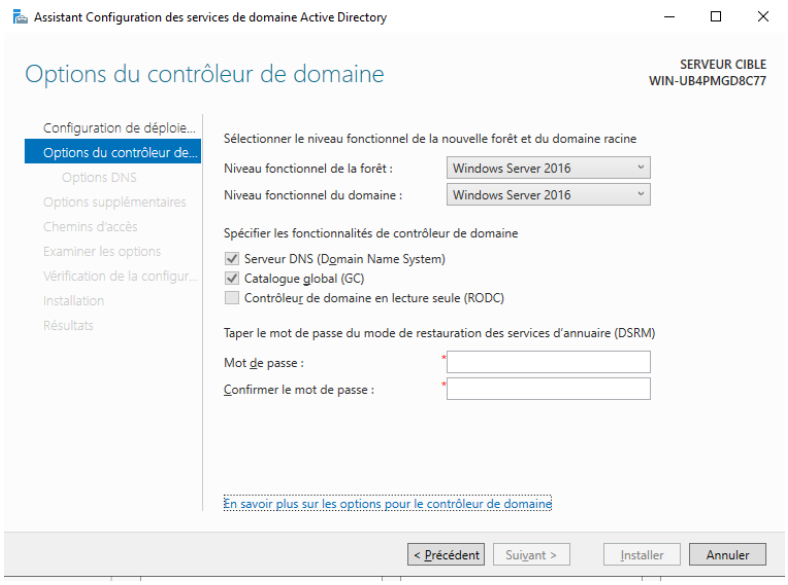
Lorsque l'installation se termine une notification en haut a droit va apparaître cliqué sur 'Promouvoir ce serveur en contrôleur de domaine.'



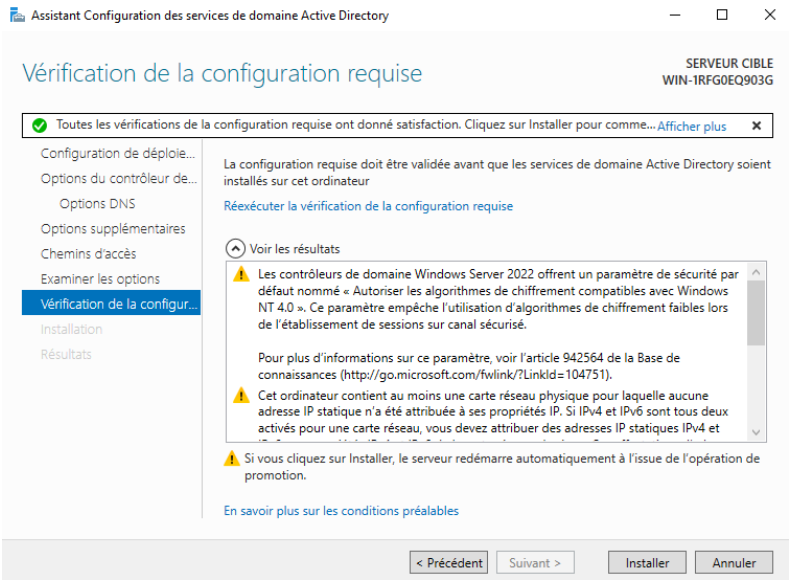
Coché la case Ajouté une nouvelle forêt puis donné un nom a cette dernierX.X



Donné un mot de passe à ce domaine

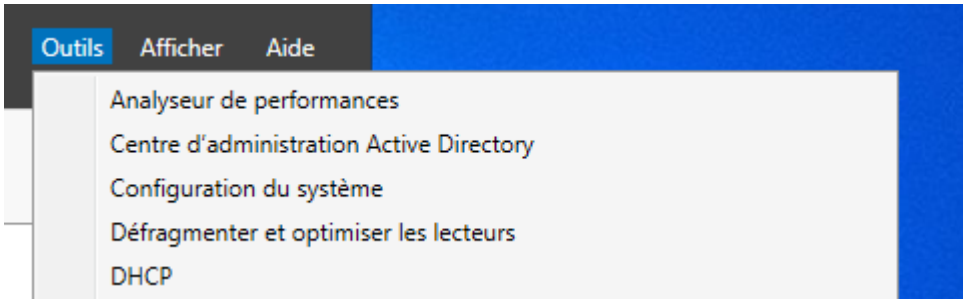


Poursuivé jusqu’à la page ”vérification de la configuration” et cliqué sur installer

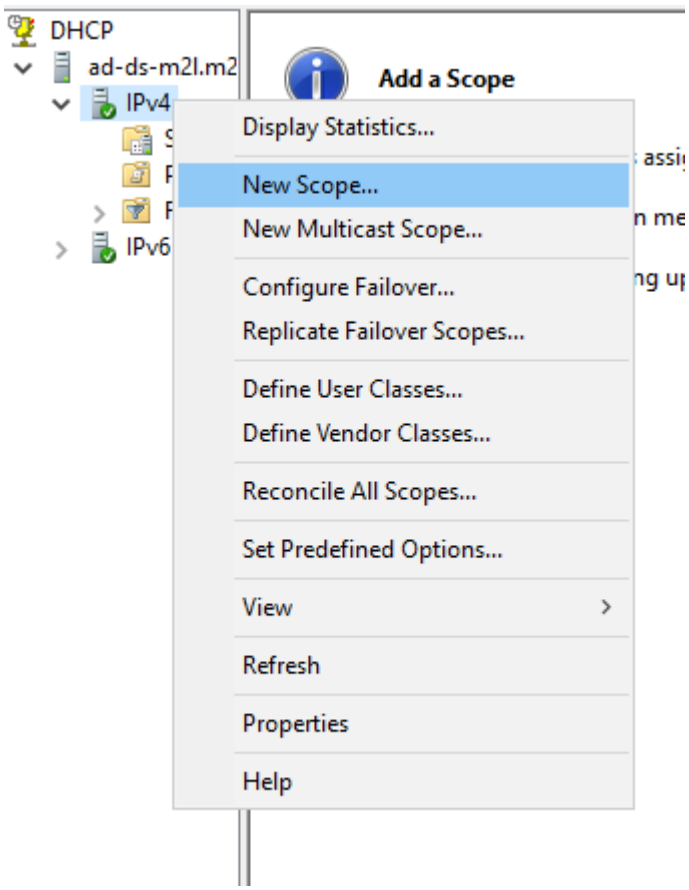


Configuration DHCP

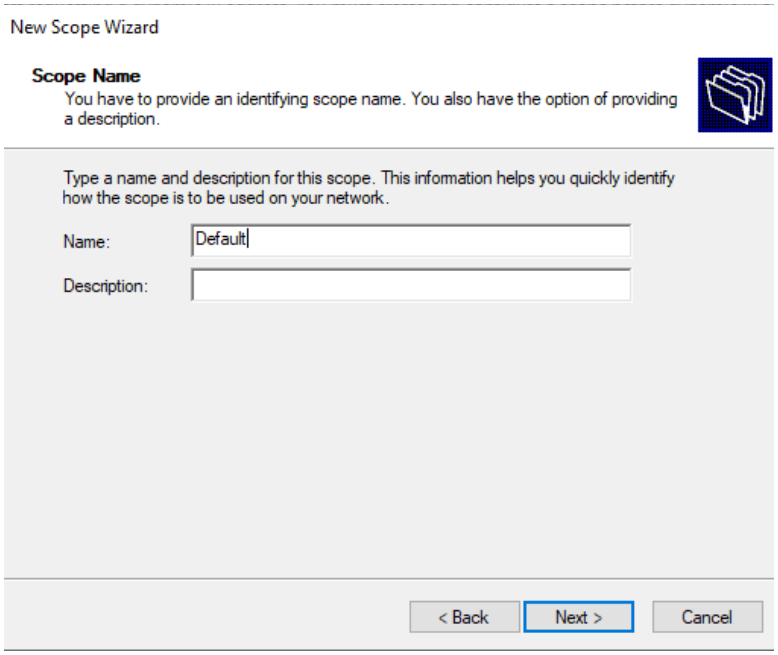
Allez dans l’onglet DHCP en haut droite du gestionnaire de serveur dans outil



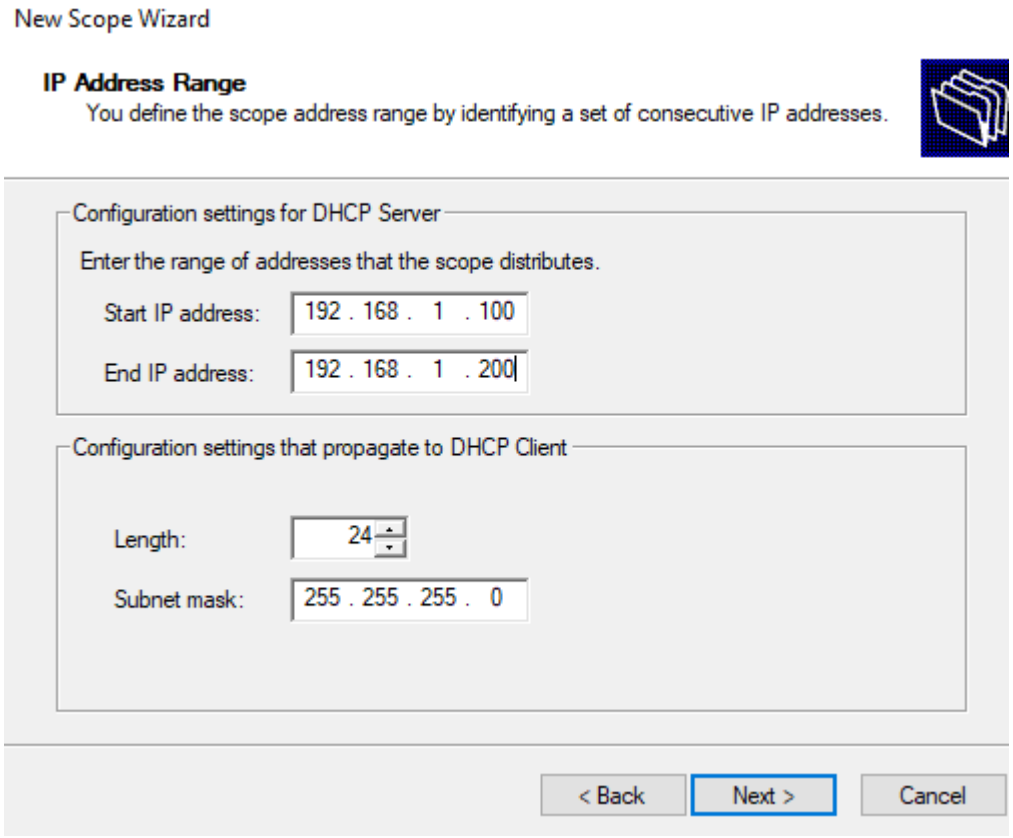
Faite clic droit sur l'IPV4 et faite nouvel étendu



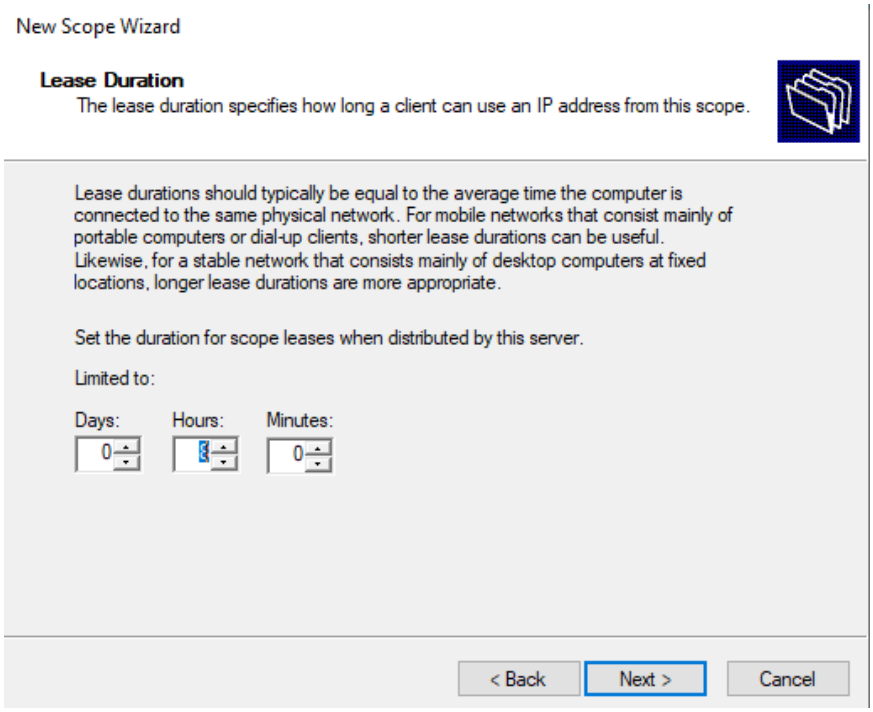
Entré le nom de votre nouvelle étendu



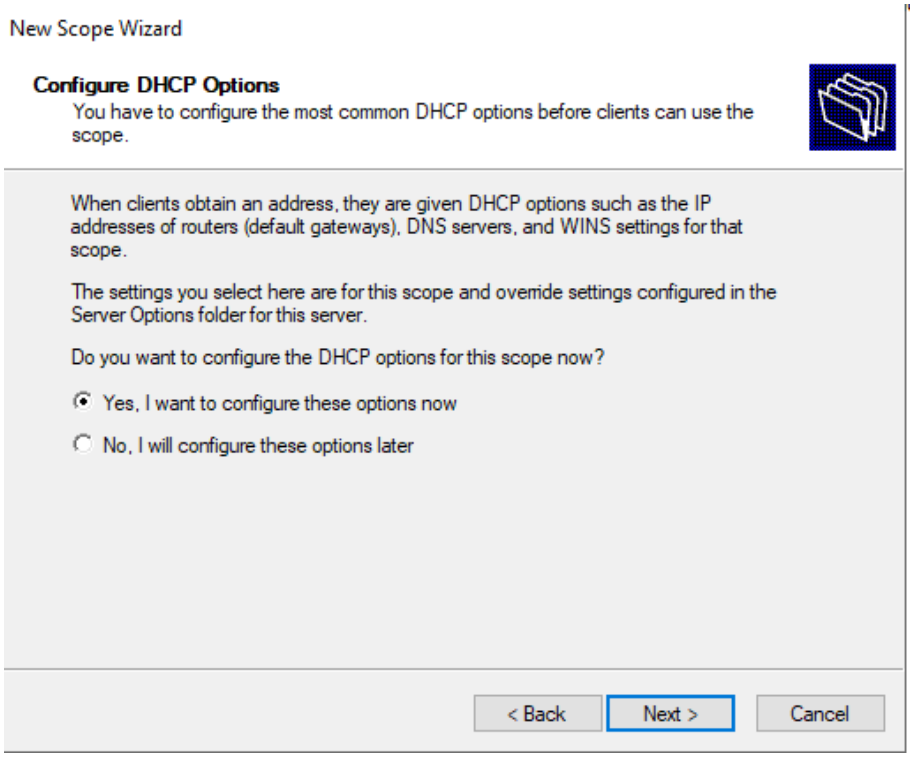
Configuré la plage IP que votre DHCP va attribuer dans ce cas-là le DHCP attribueras une adresse IP aux appareils entrant entre 192.168.1.100 à 192.168.1.200



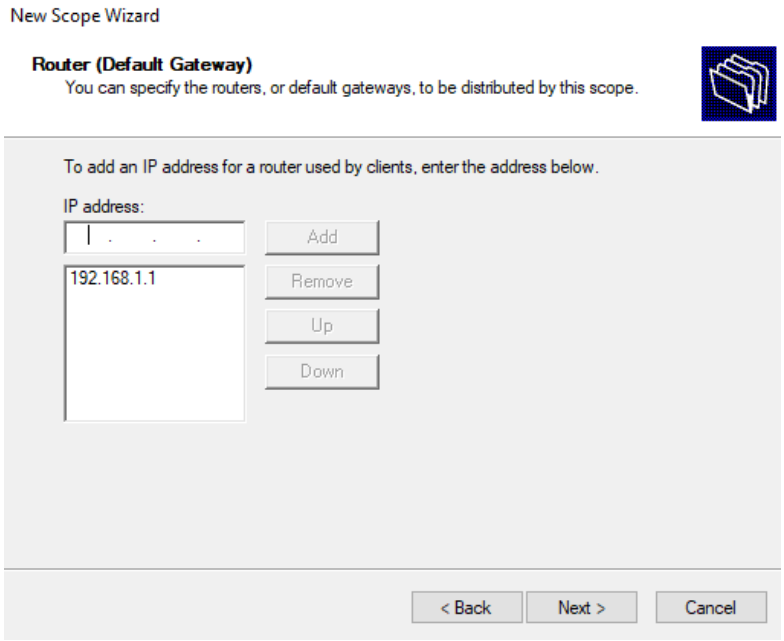
Choisir la durée du bail



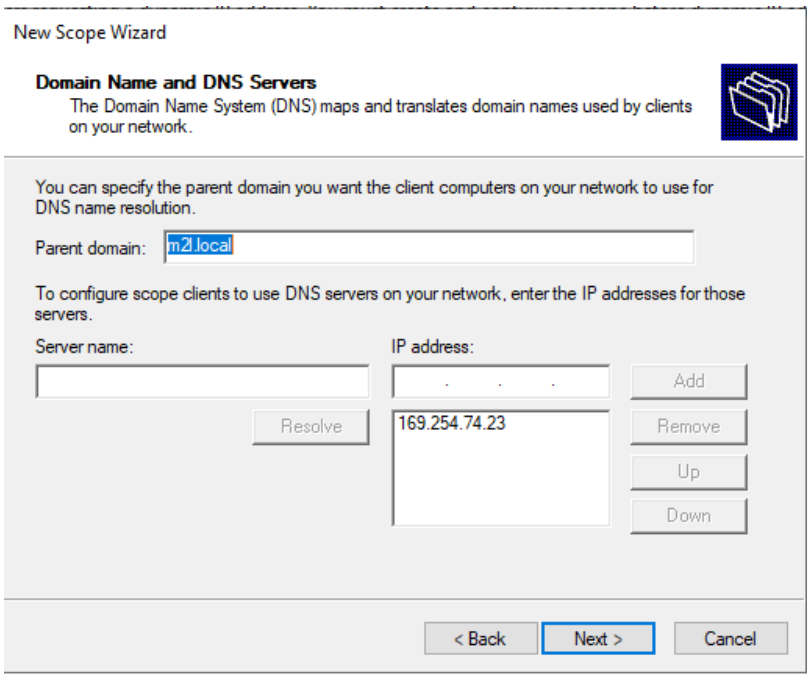
Accepté de configurer le routeur que vous attribuer par défaut le domaine et DNS qui seras utiliser et d'appliqué cette plage maintenant



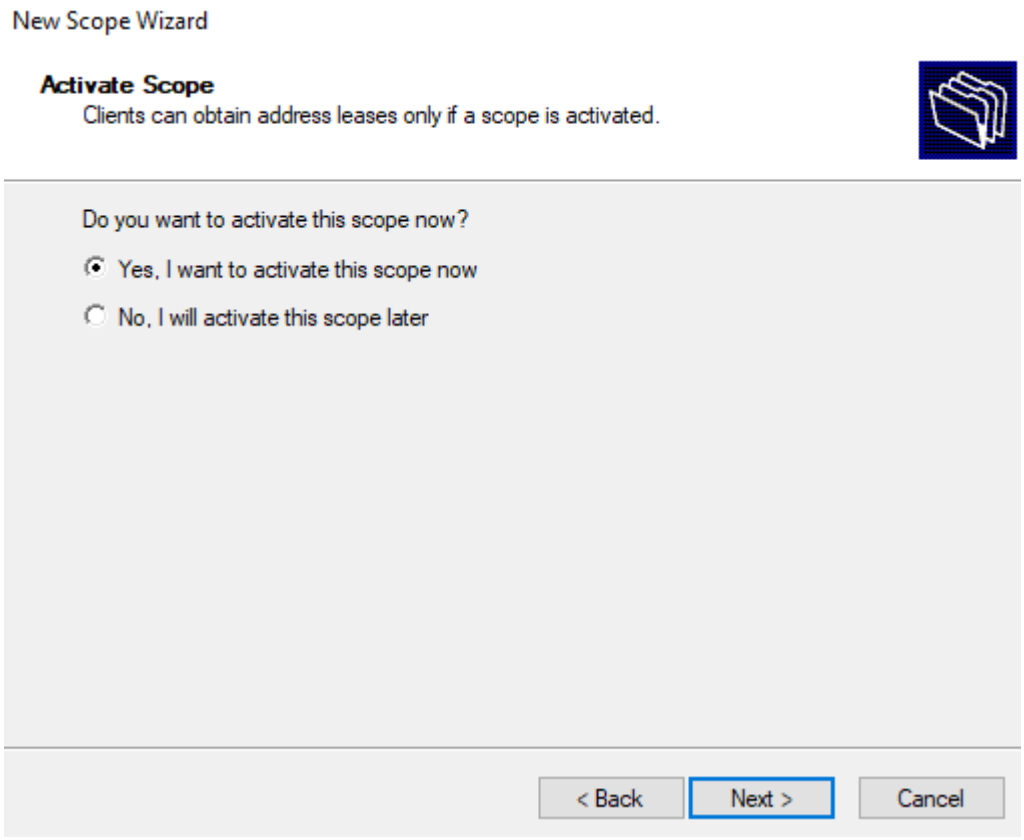
Choix du routeur par défaut



Le Domain et DNS utilisé

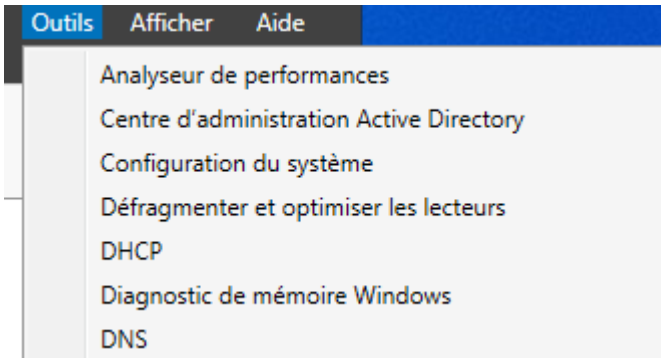


Activation de la nouvelle étendu

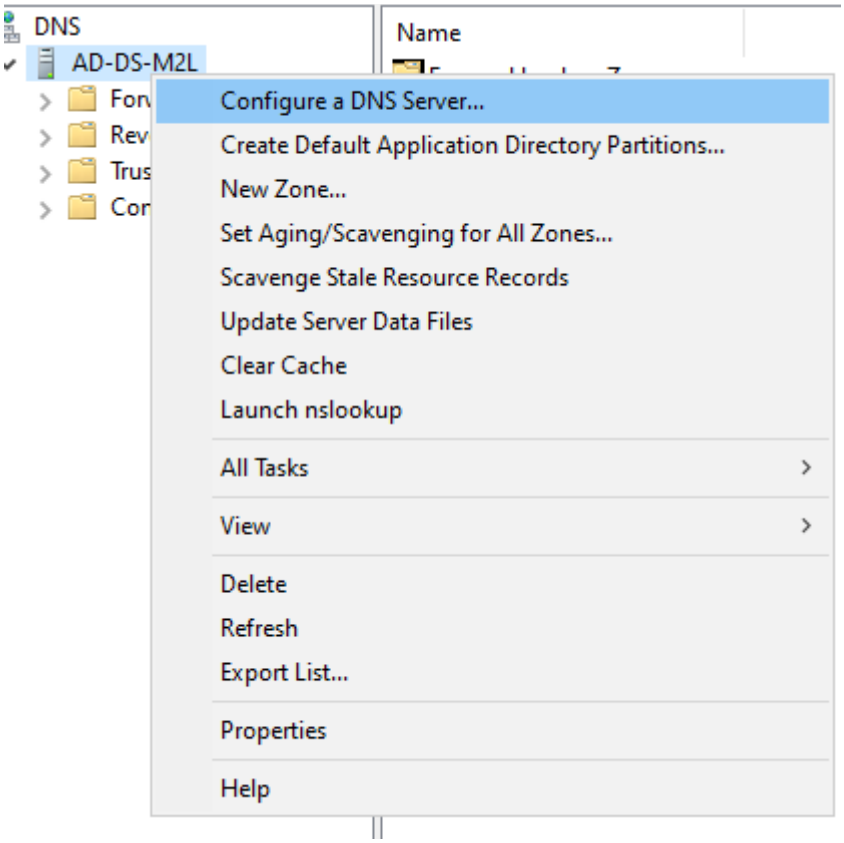


Configuration DNS

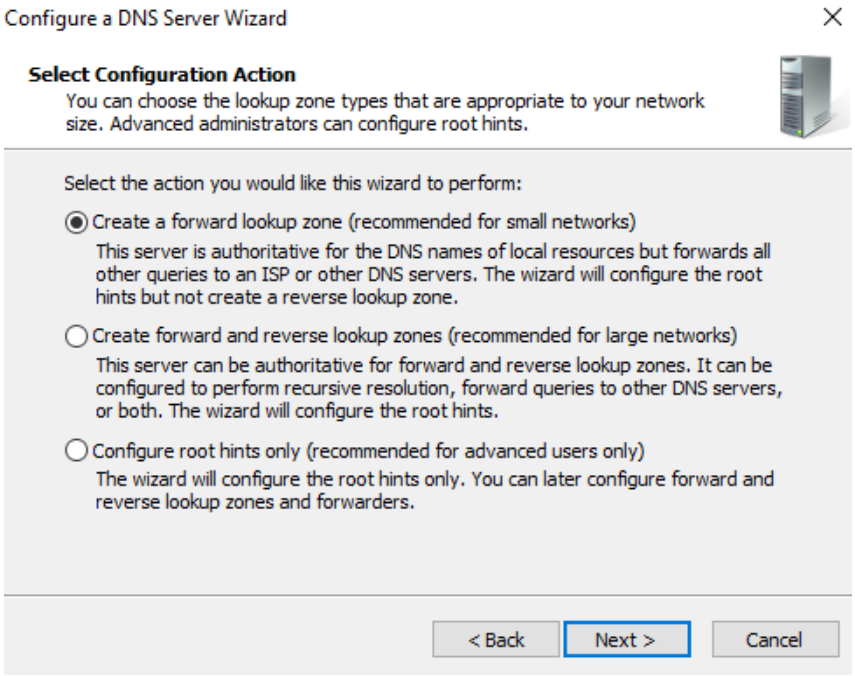
Allez dans l'onglet DNS en haut droite du gestionnaire de serveur dans outil



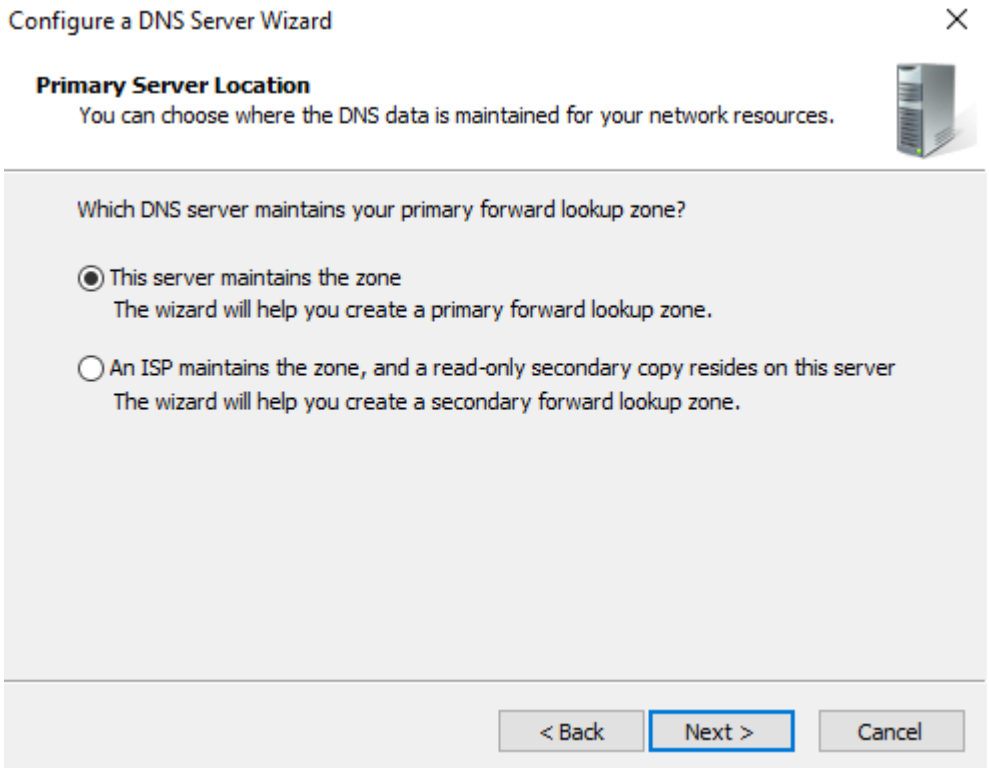
Faite clic droit sur le serveur ad et faite "configuration serveur DNS"



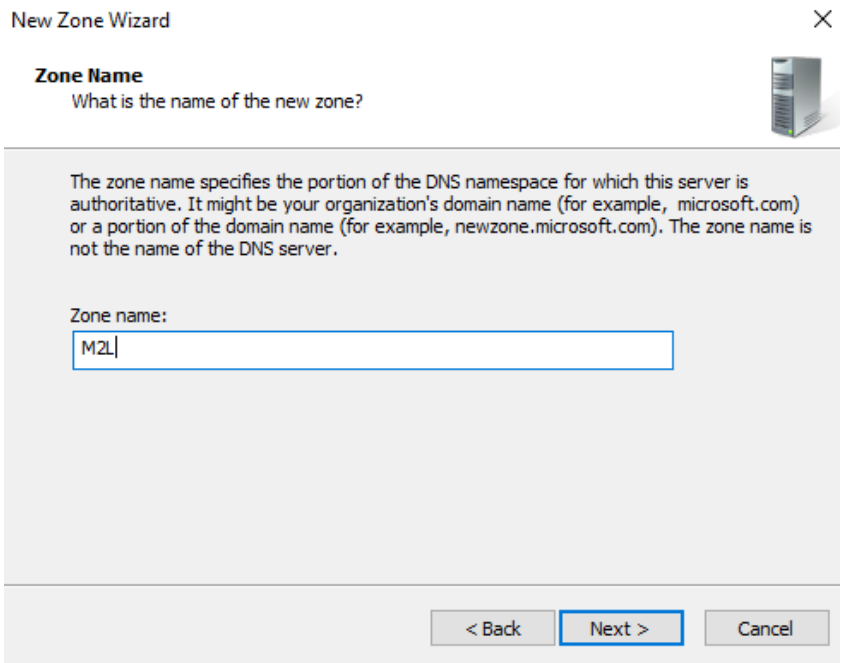
À l'étape "Select Configuration Action", sélectionnez "Create a forward lookup zone" afin de permettre à votre serveur DNS de résoudre les noms de domaine locaux en adresses IP dans un petit réseau.



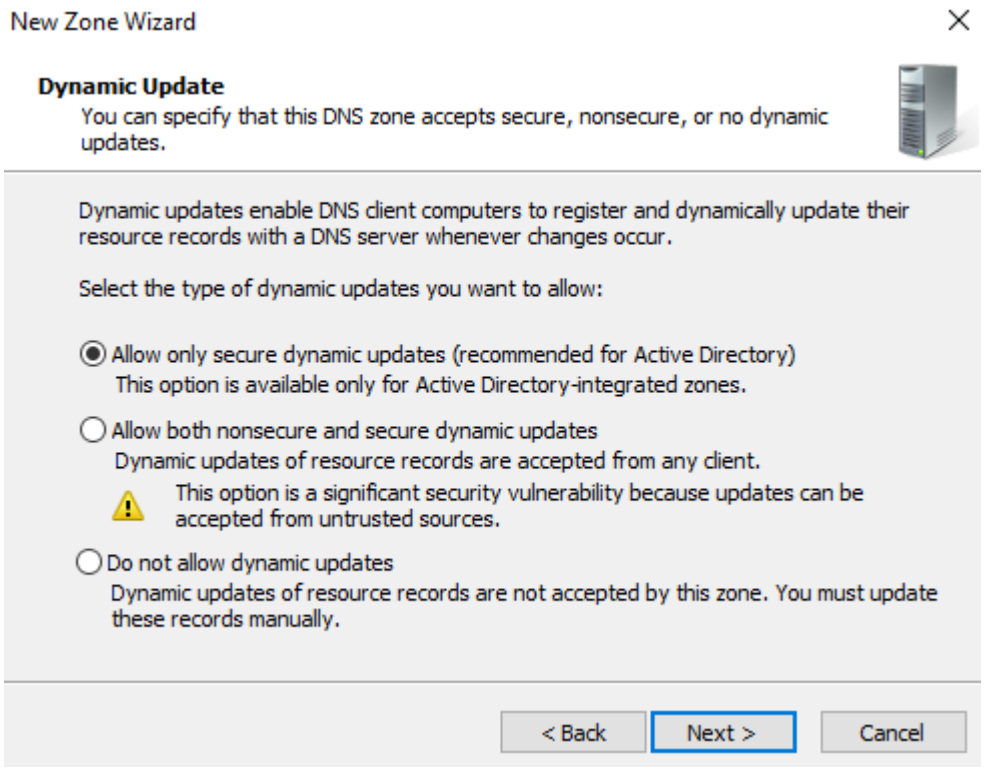
À l’étape "Primary Server Location", sélectionnez "This server maintains the zone" afin de créer une zone de recherche directe principale directement hébergée sur votre serveur DNS.



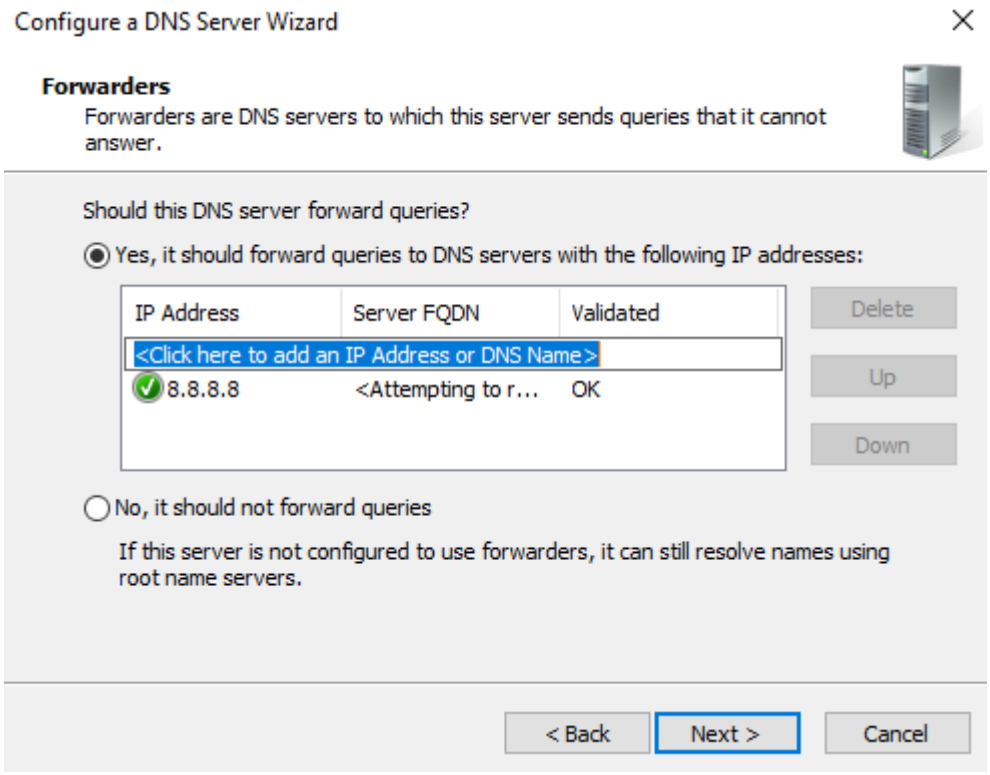
Choisir le nom de la nouvelle zone de recherche



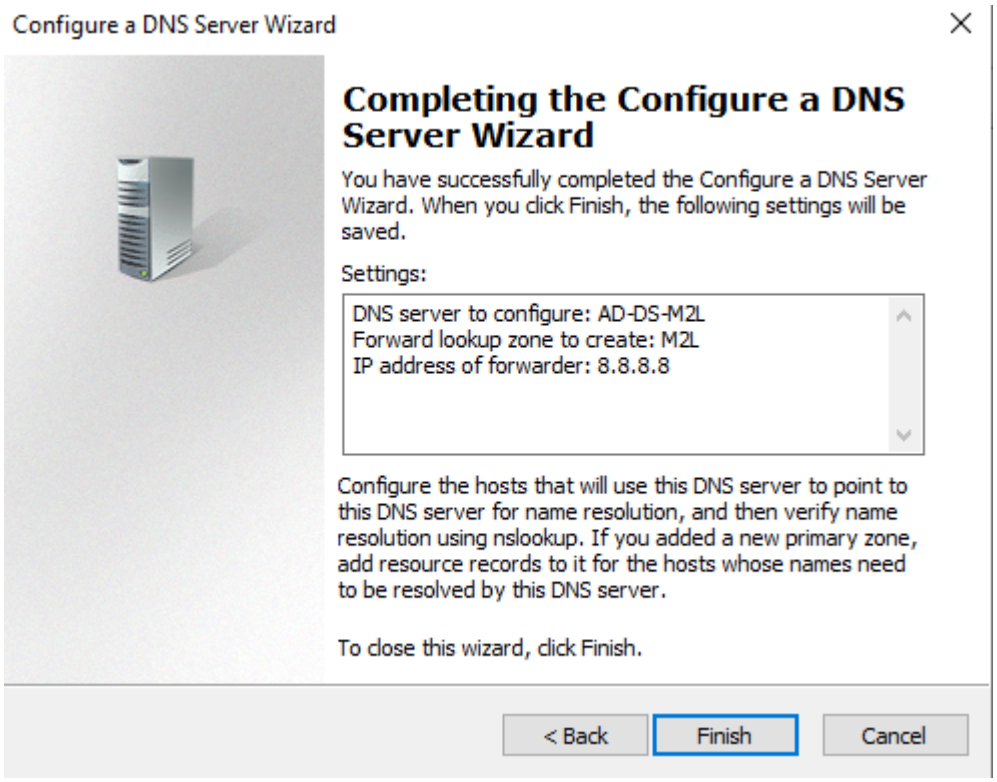
À l’étape "Dynamic Update", sélectionnez "Allow only secure dynamic updates" pour sécuriser les mises à jour DNS via Active Directory.



Cochez "Oui", ajoutez l’adresse IP d’un serveur DNS (ex. : 8.8.8.8), puis cliquez sur "Suivant"

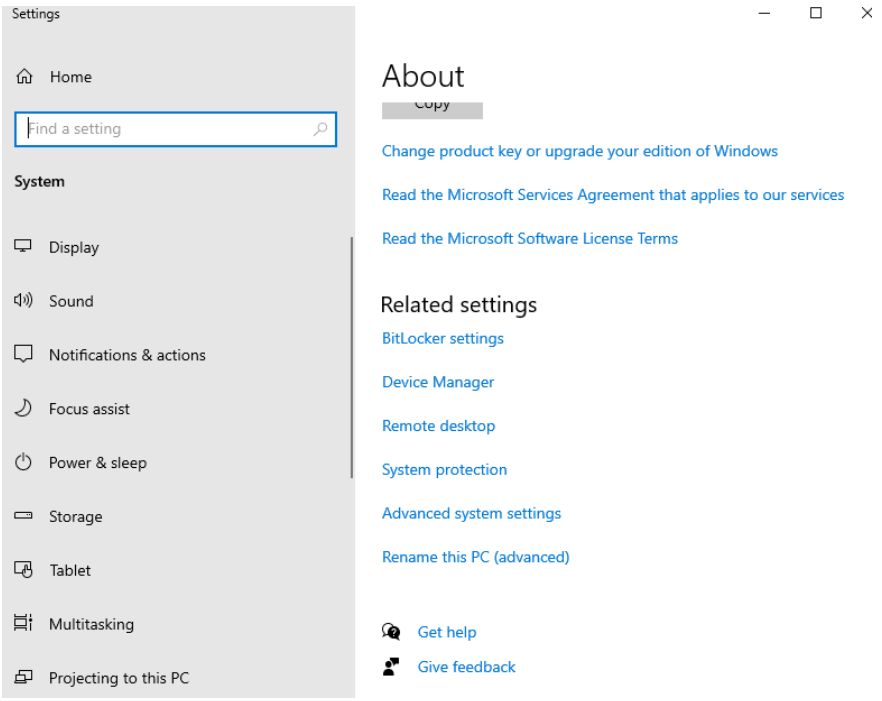


Terminer la configuration cliquer sur finir

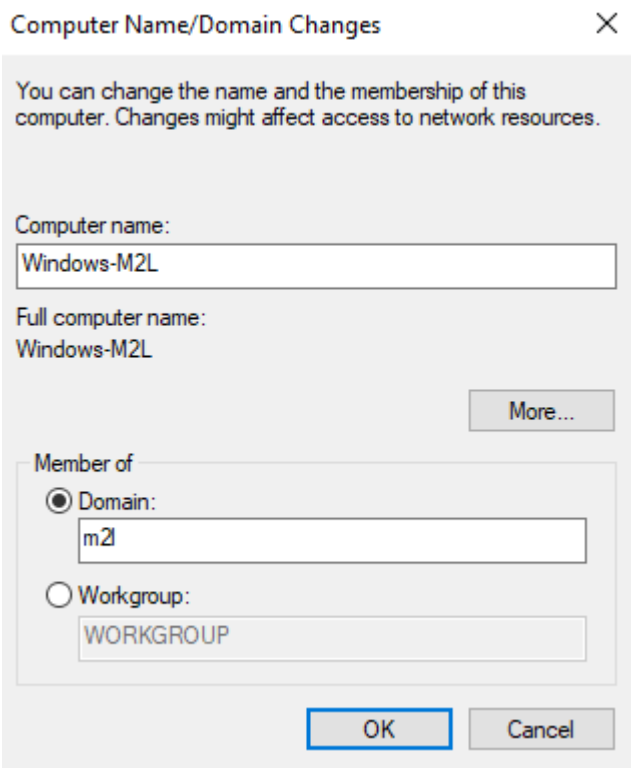


Ajout dans le domaine

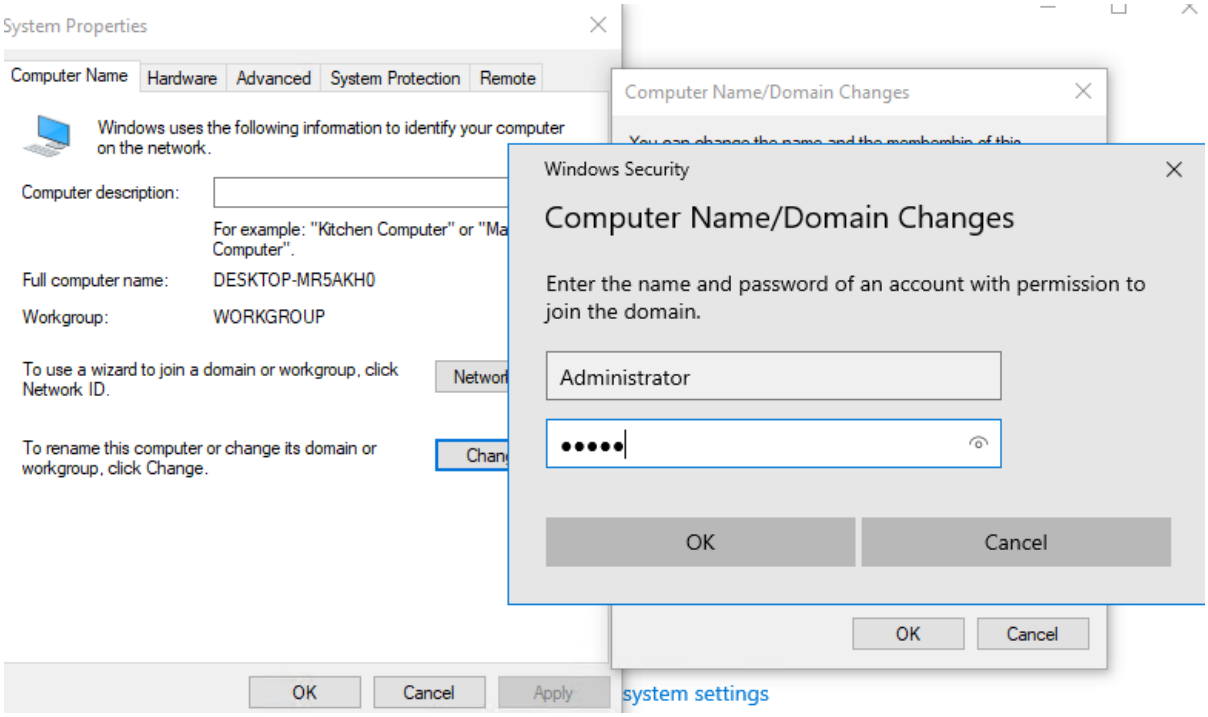
Se rendre dans les paramètres, puis rechercher nom et enfin cliquer sur Renommer ce pc (avancé)

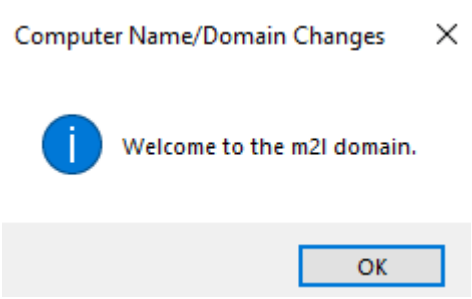


Rentrer les informations



Se connecter avec l'administrateur





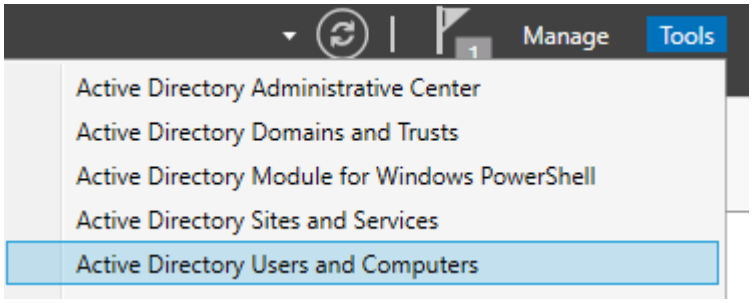
Si cela fonctionne, nous avons vérifié que le DNS et le DHCP fonctionnent.

Après avoir redémarré le pc, nous pouvons nous connecter avec l'utilisateur que l'on a créé précédemment.

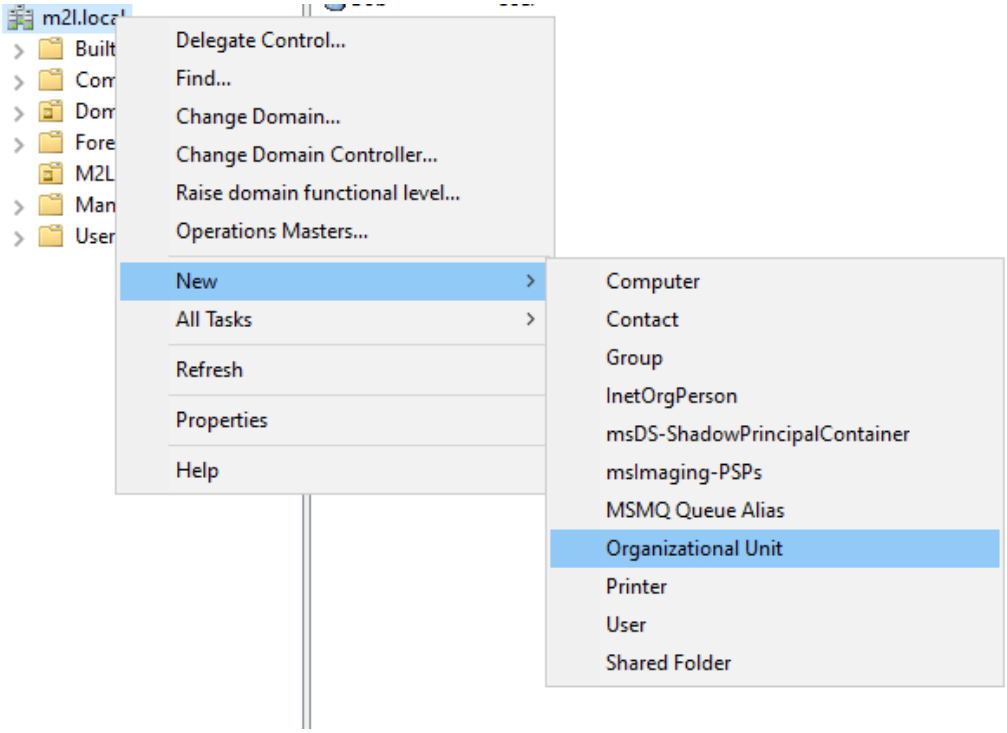
Gestion unité d'organisation et utilisateur

Création unités d'organisations

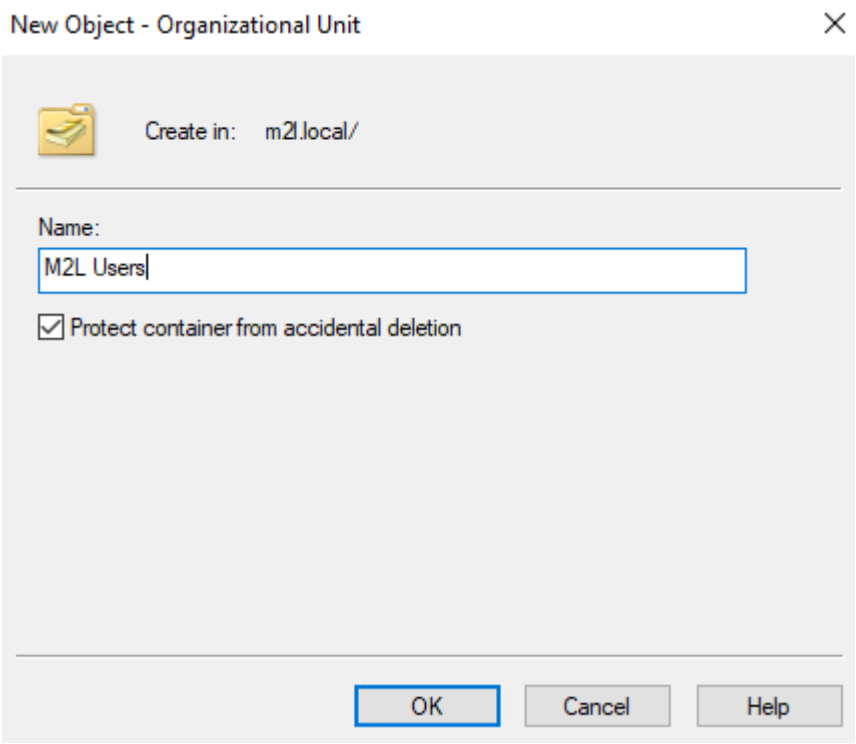
Tout d'abord nous allons nous rendre dans l'onglet 'Active directory Users and Computeur'



Puis faite clic droit sur votre active directory dans notre cas m2l.local et faite “new” puis “organizationnal unit”

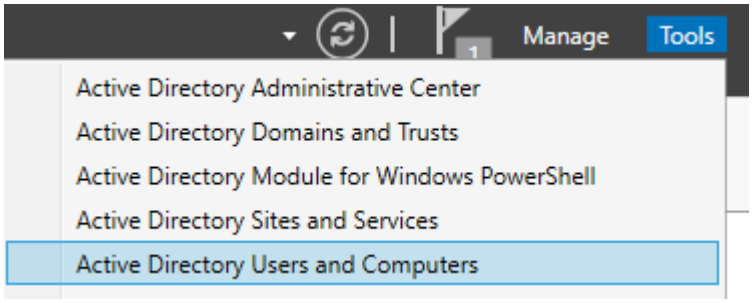


Créer votre unité d’organisation avec le nom désiré

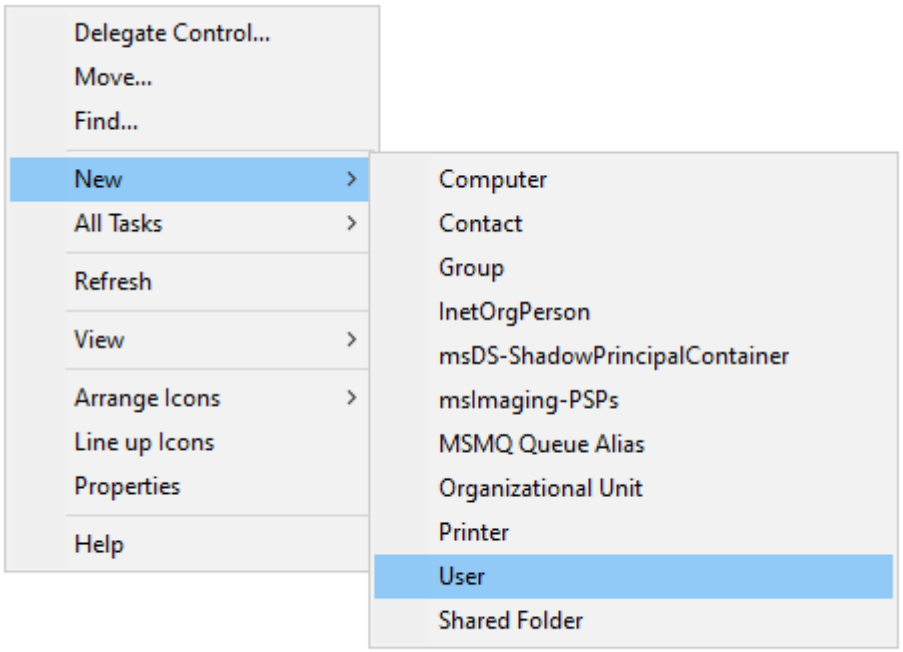


Création user

Afin de créer un nouvel utilisateur vous devez aussi vous rendre dans l'onglet "Active directory Users and Computeur"



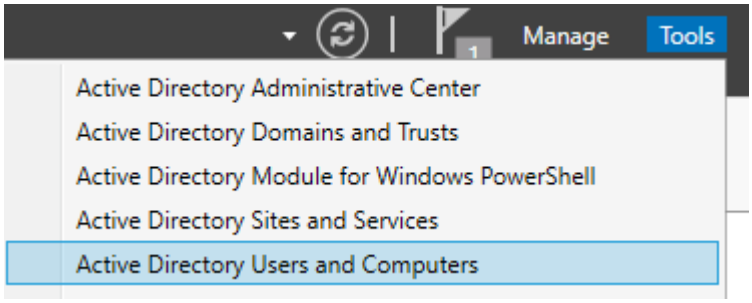
Puis faite clic droit sur votre active directory et faite “new” puis “User”



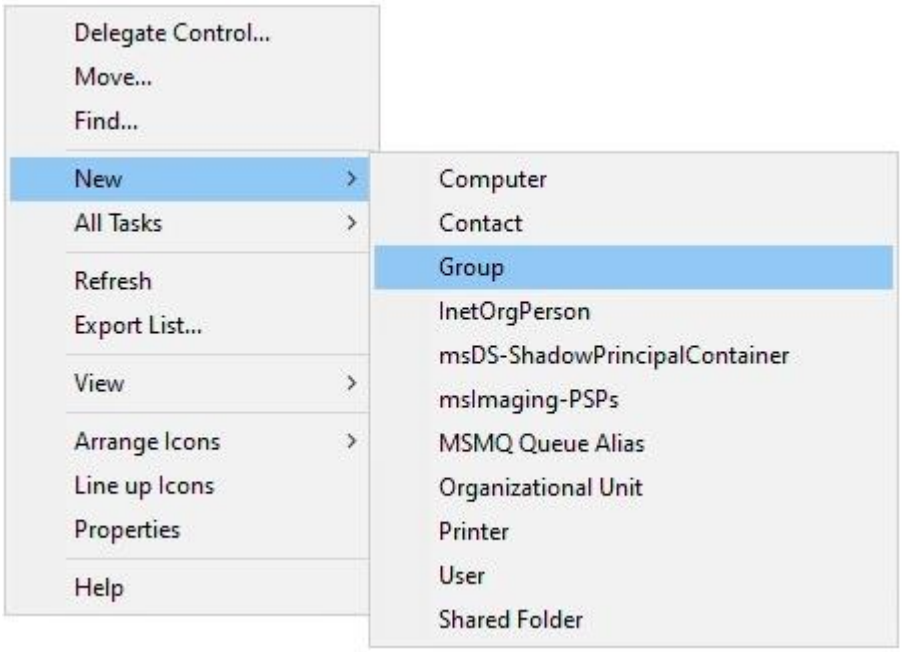
Puis suivez les indications en prenant soins de remplir les informations demandées

Création d’un groupe de sécurité.

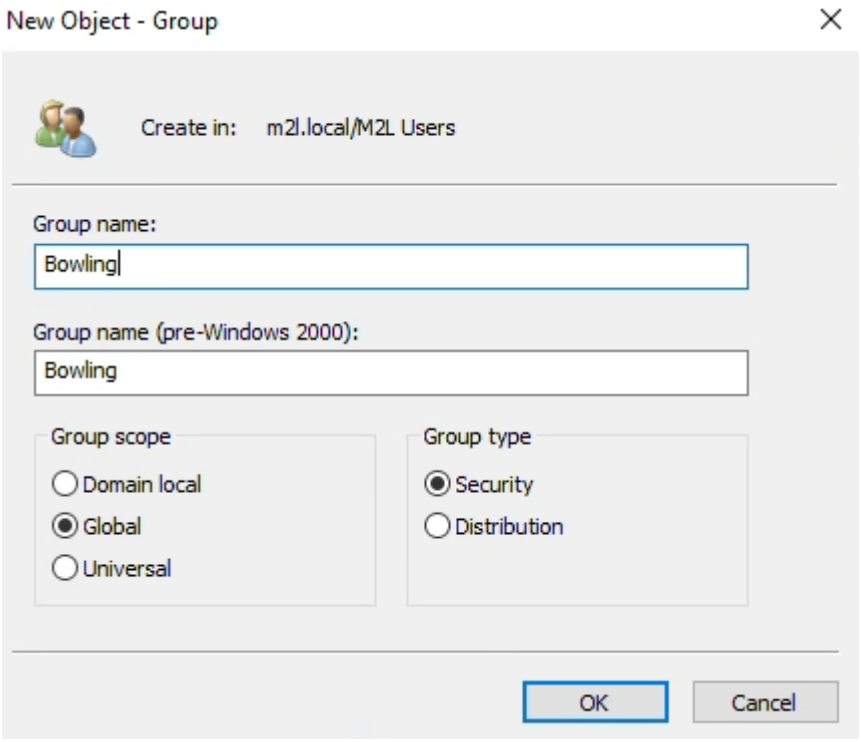
Tout d’abord nous allons nous rendre dans l’onglet “Active directory Users and Computeur”



Puis faite clic droit sur votre active directory et faite “new” puis “Group”

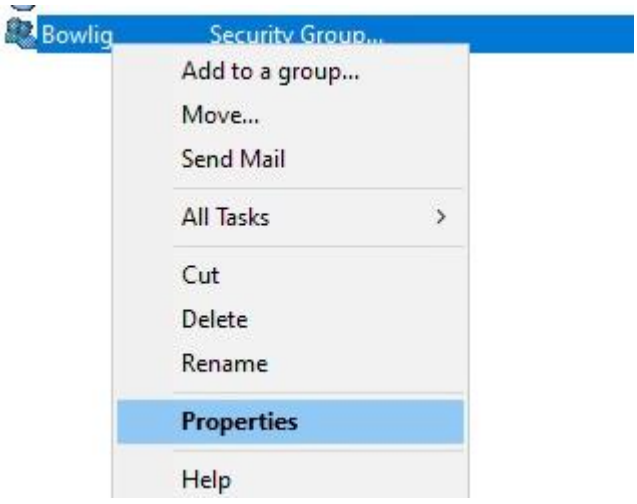


Puis suivez les indications en prenant soins de remplir les informations demandées

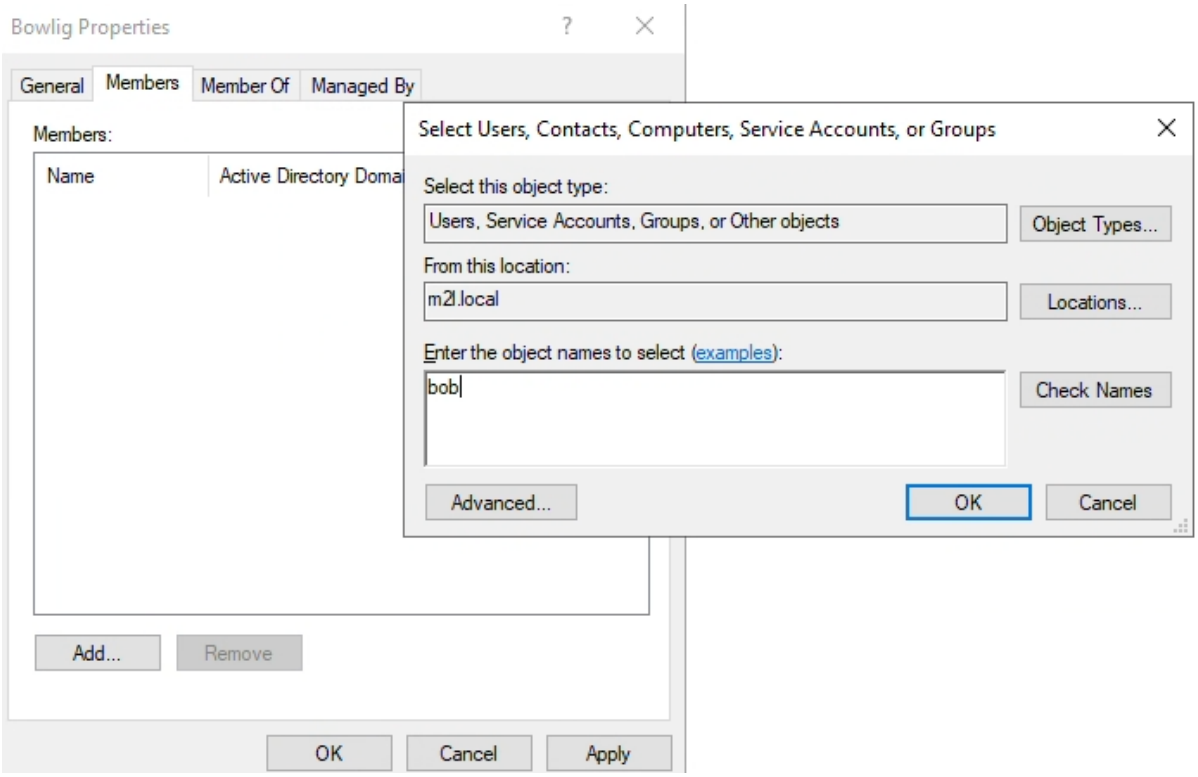


Ajout d'un utilisateur dans le groupe de sécurité.

Faite clic droit sur votre groupe et faite properties.



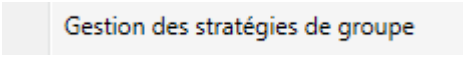
Puis dans l'onglet "Members" cliquez qur "Add" et renseignez l'utilisateur a rajouter.



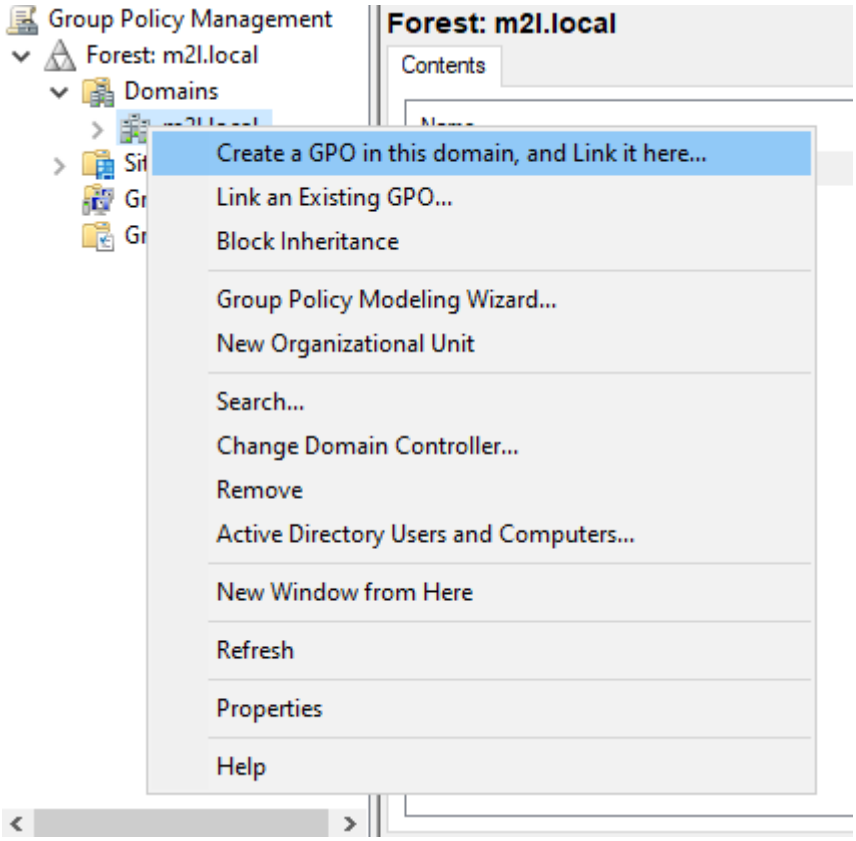
Déploiement d’une application via le GPO

Création d’un nouvel objet GPO

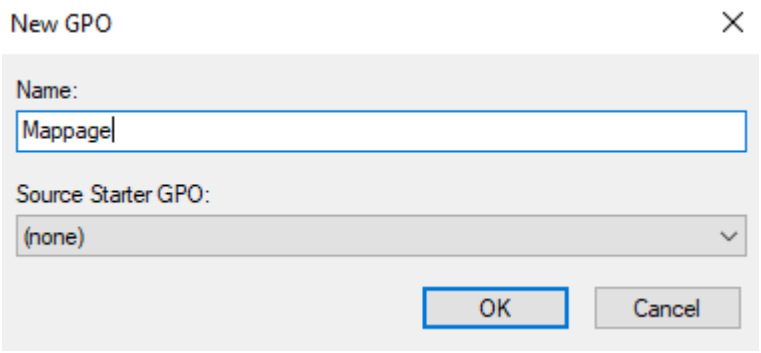
Allez dans l’onglet "Gestion de stratégie de groupe” en haut droite du gestionnaire de serveur dans outil



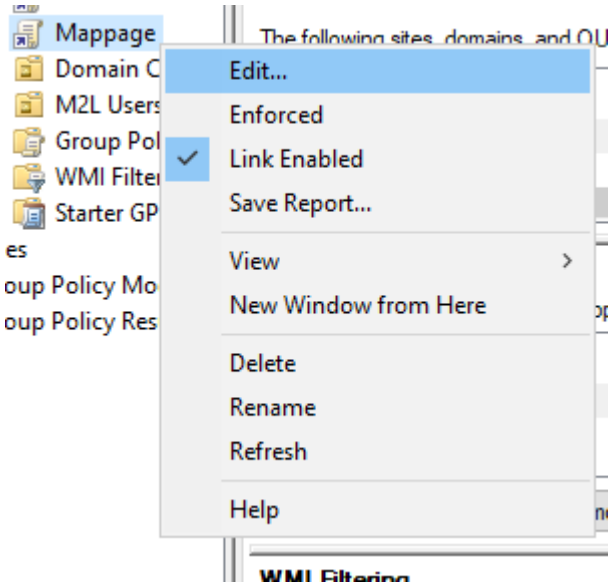
Créer une nouvelle GPOFaites un clic droit sur le domaine, puis sélectionnez "Create a GPO in this domain, and Link it here..." pour créer et lier une stratégie de groupe.



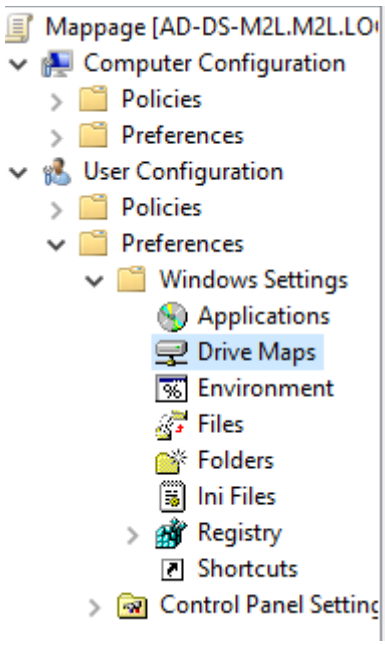
Choisir le nom de cette dernière



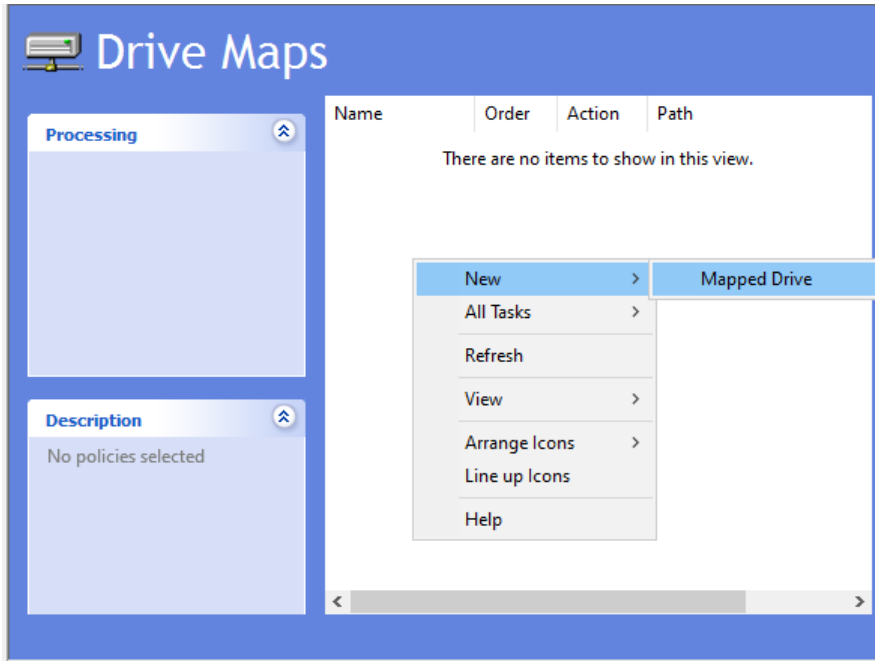
Faites un clic droit sur la GPO souhaitée puis sélectionnez **"Edit..."** pour modifier sa configuration.



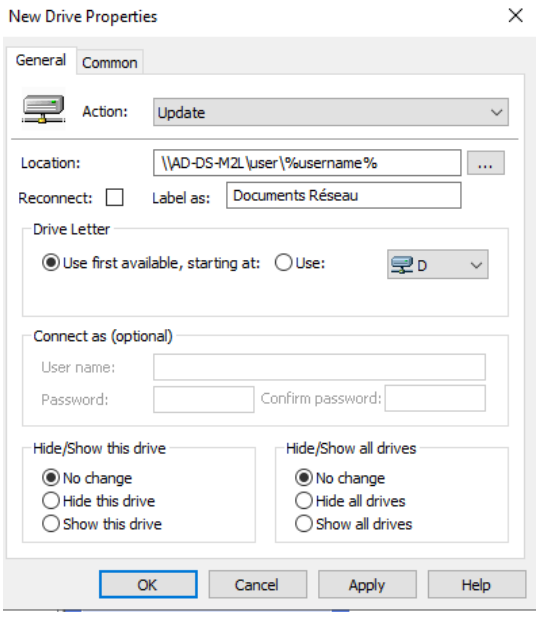
Dans l'éditeur de GPO, accédez à User Configuration > Preferences > Windows Settings > Drive Maps pour créer un lecteur réseau attribué aux utilisateurs.



Faites un clic droit sur Drive Maps, puis sélectionnez New > Mapped Drive afin de configurer un nouveau lecteur réseau pour les utilisateurs.



Dans la fenêtre New Drive Properties, remplissez les champs



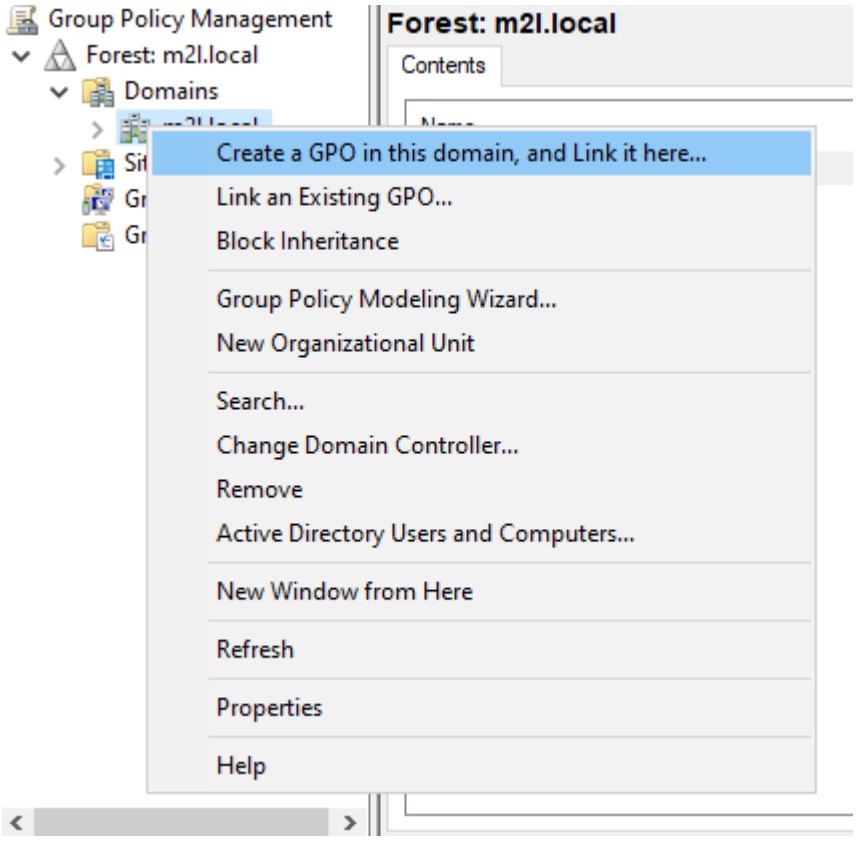
Une fois le lecteur créé, fermez l'éditeur de GPO, puis effectuez un gpupdate /force dans l'invite de commandes sur un poste client pour appliquer immédiatement la stratégie.

Création d’une gpo qui s’applique uniquemet a un groupe de sécurité.

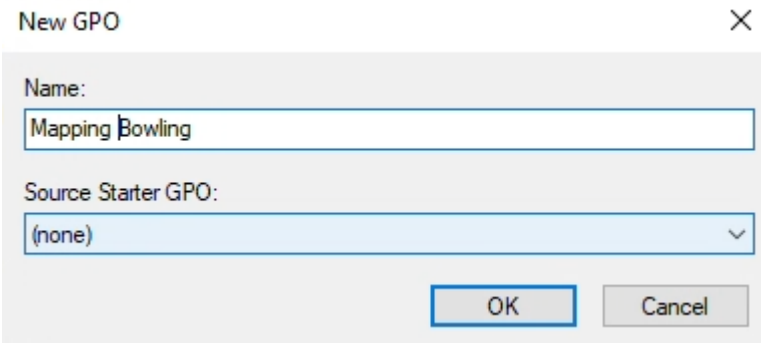
Création d’un nouvel objet GPO

Allez dans l’onglet "Gestion de stratégie de groupe” en haut droite du gestionnaire de serveur dans outil

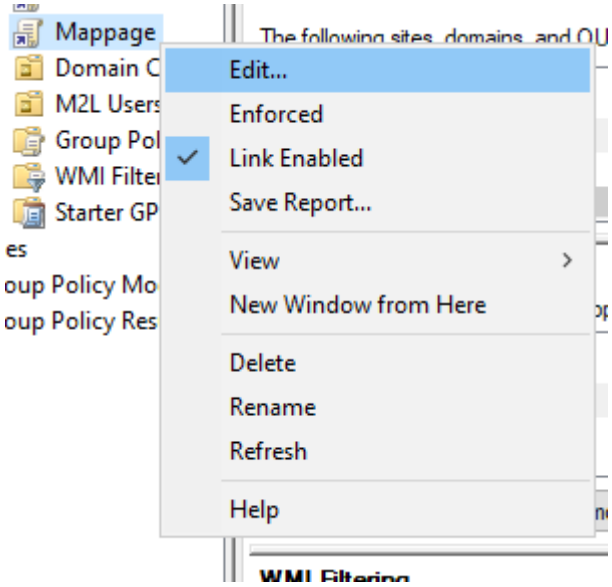
Créer une nouvelle GPOFaites un clic droit sur le domaine, puis sélectionnez "Create a GPO in this domain, and Link it here..." pour créer et lier une stratégie de groupe.



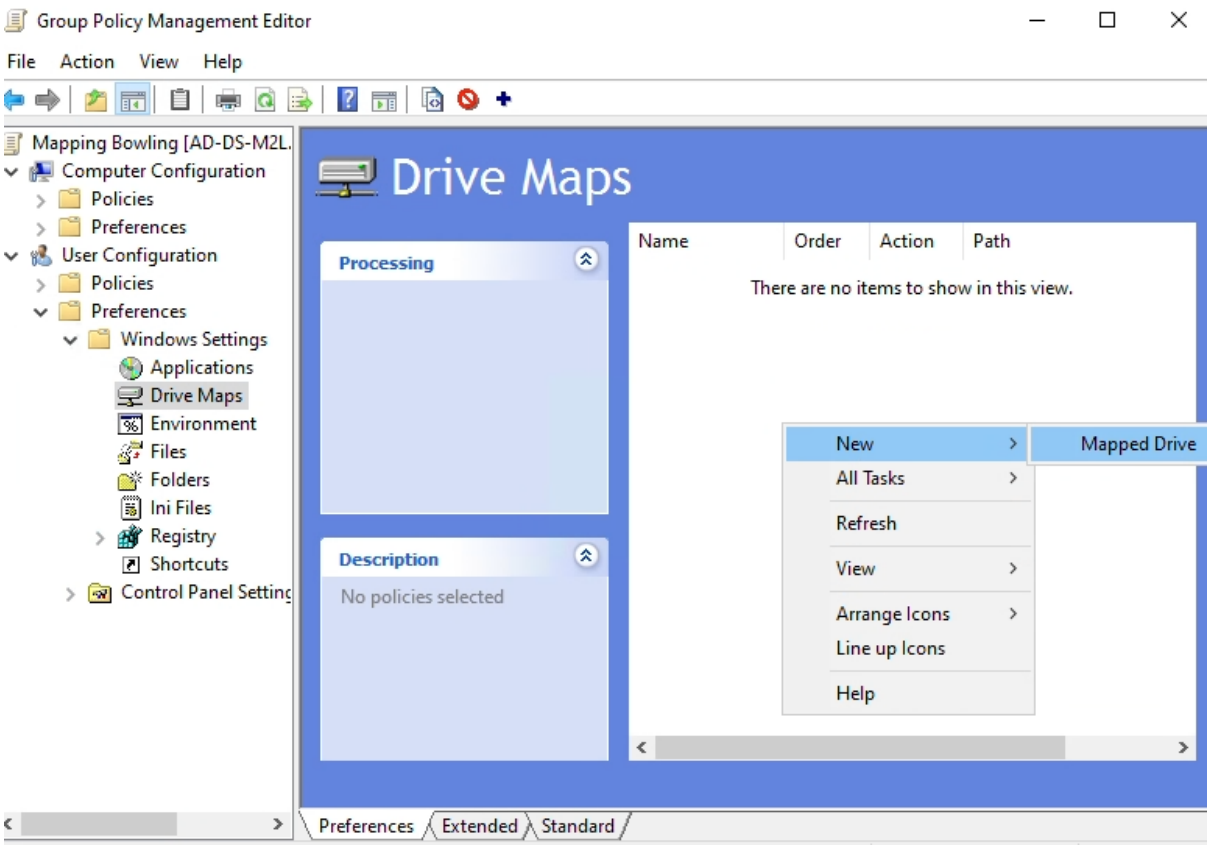
Choisir le nom de cette dernière



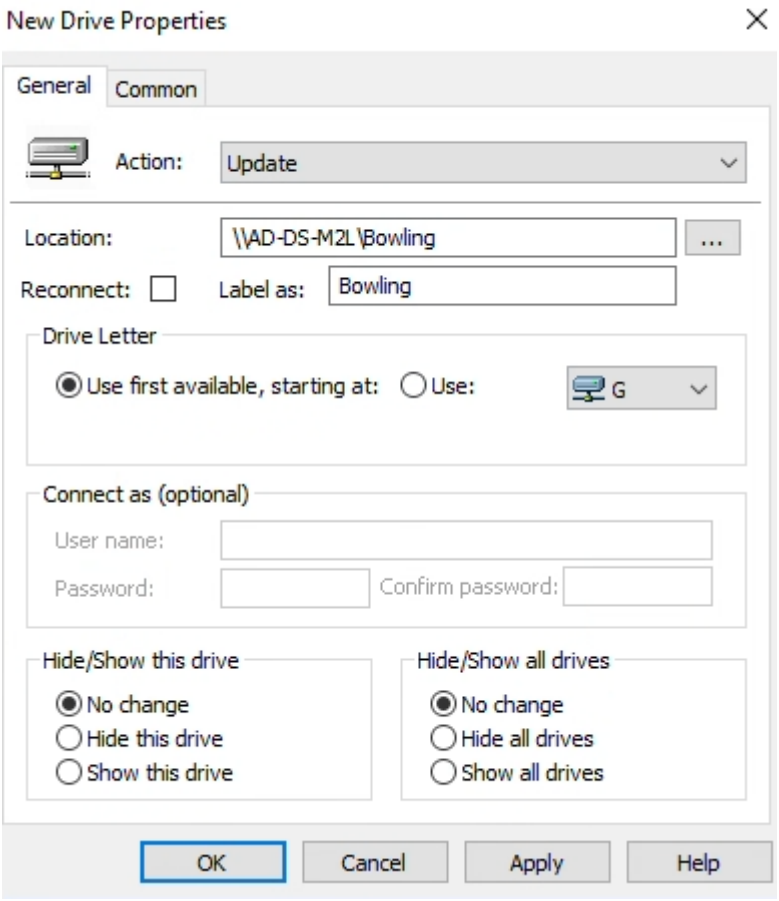
Faites un clic droit sur la GPO souhaitée puis sélectionnez **"Edit..."** pour modifier sa configuration.



Dans l'éditeur de GPO, accédez à User Configuration > Preferences > Windows Settings > Drive Maps, faites un clic droit sur Drive Maps, puis sélectionnez New > Mapped Drive afin de configurer un nouveau lecteur réseau pour les utilisateurs.

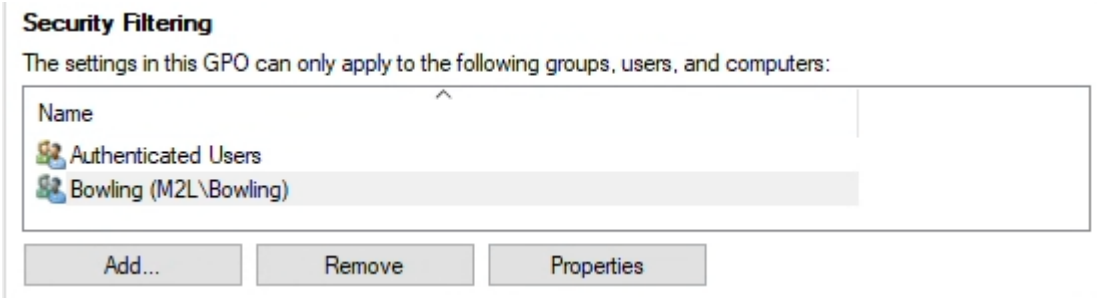


Dans la fenêtre New Drive Properties, remplissez les champs



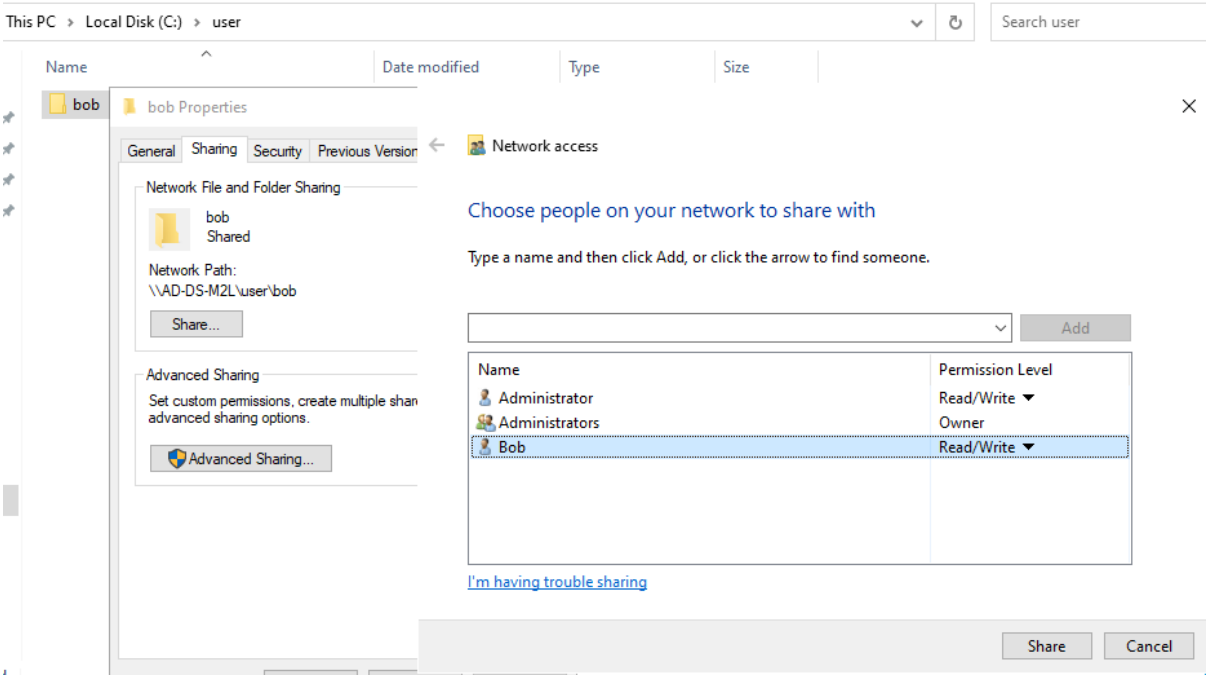
Dans l'onglet "Security Filtering" ajoutez le groupe "bowling"

Après l'ajout, ce dernier devrait ressembler à :

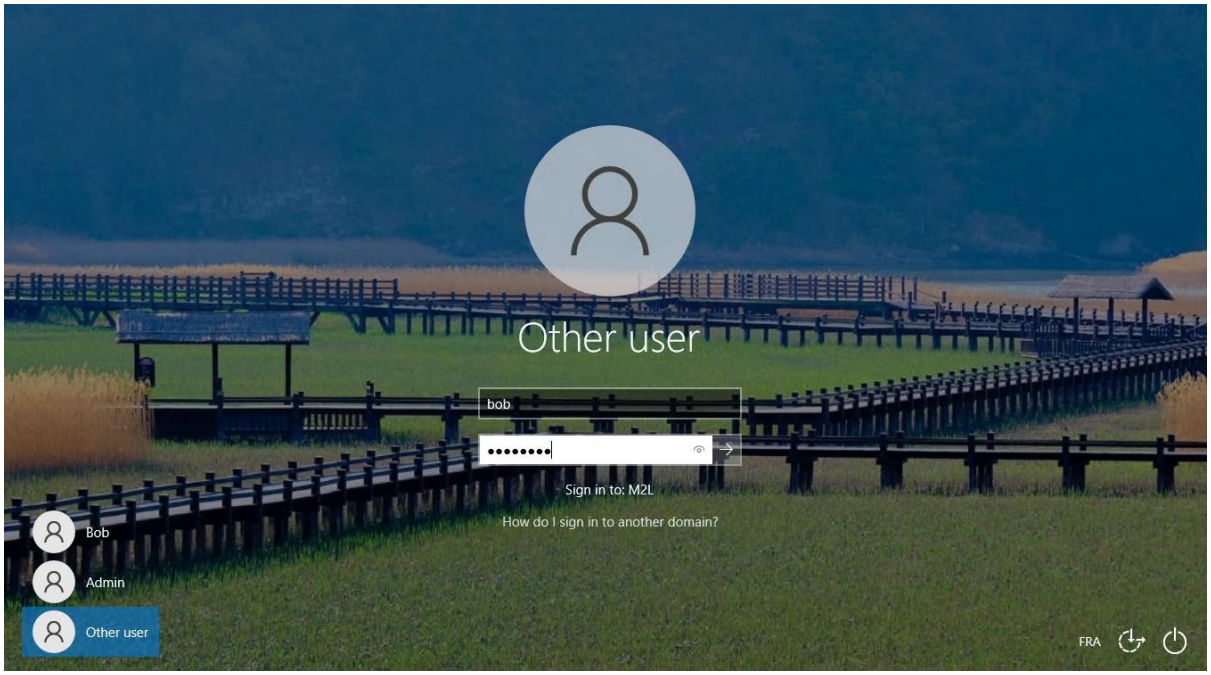


Une fois ces étapes terminées, fermez l'éditeur de GPO, puis effectuez un gpupdate /force dans l'invite de commandes sur un poste client pour appliquer immédiatement la stratégie.

Choisir un dossier à partager dans le mappage réseau puis lui attribuer des utilisateur qui y auront accès



Pour verifier le fonctionnement des configurations, connectez vous avec l'utilisateur créé.



Si tout se passe bien vous devriez avoir une page similaire en ouvrant un explorateur de fichier