

Fiche technique M2L



Réaliser par JOVANOVIC William / MILIC Daniel / SALANDINI Enzo

SOMMAIRE

Installation de PfSense	2
Configuration de base	3
Configuration des interfaces.	7
Configuration de l'IP LAN.	8
Installation de Windows.	10
Création serveur Active directory.....	15
Installation du rôle d'Active directory	15
Configuration des services de domaine Active directory.....	18
Configuration DHCP.....	20
Configuration DNS	25
Ajout dans le domaine	29
Gestion unité d'organisation et utilisateur.....	31
Création unités d'organisations	31
Création user.....	33
Déploiement d'une application via le GPO	34
On va créer un nouvel objet GPO	34

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...),

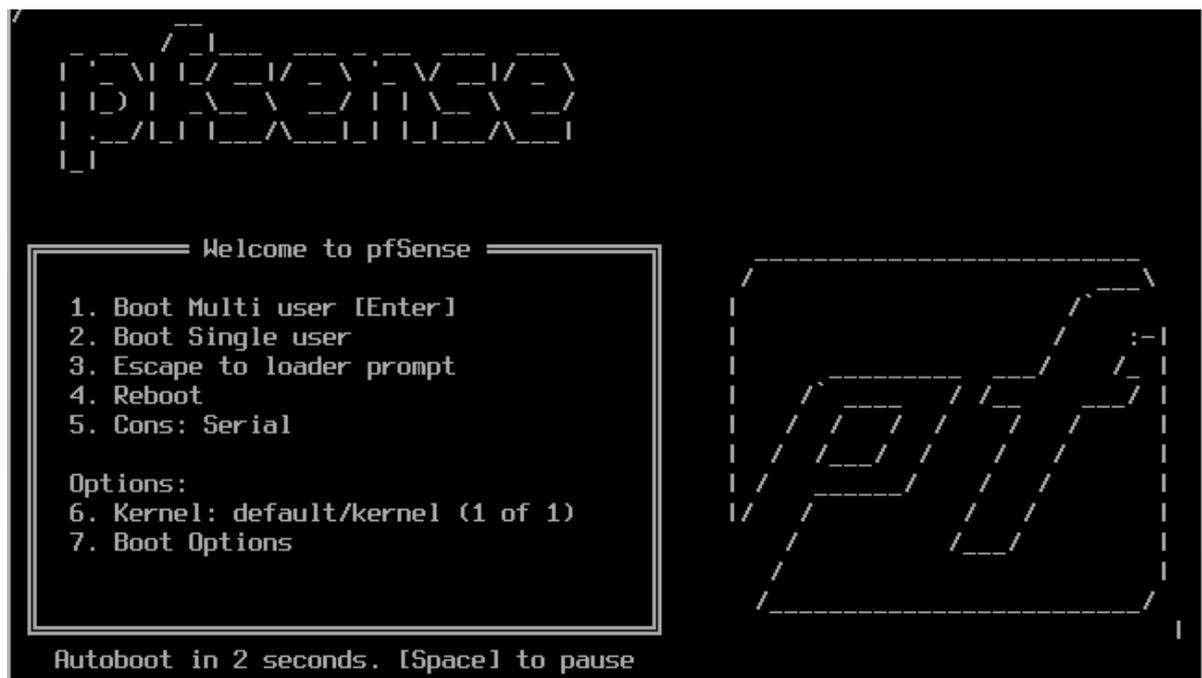
Déploiement automatisé de logiciels via des GPO,

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

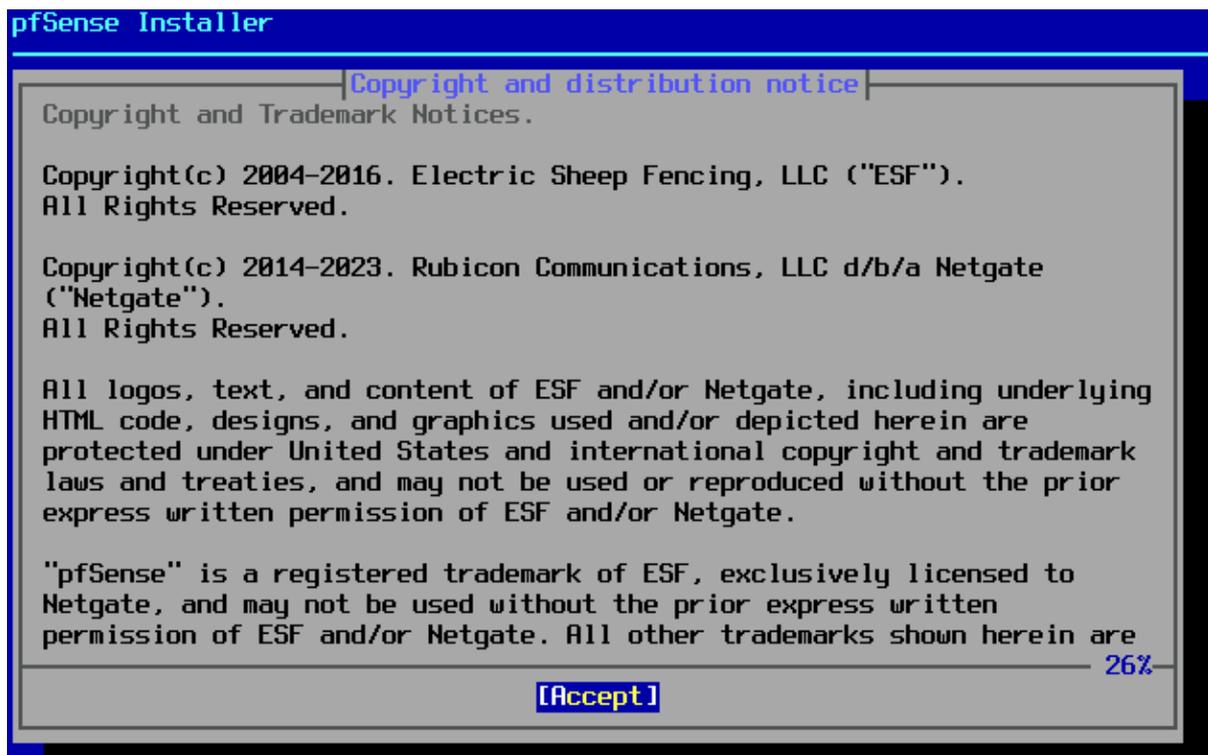
Ce projet a donc pour but de professionnaliser et sécuriser l'environnement informatique interne grâce à une infrastructure claire, centralisée, sécurisée et automatisée. Il facilitera l'administration du réseau tout en améliorant l'expérience utilisateur au sein de la structure.

Installation de PfSense

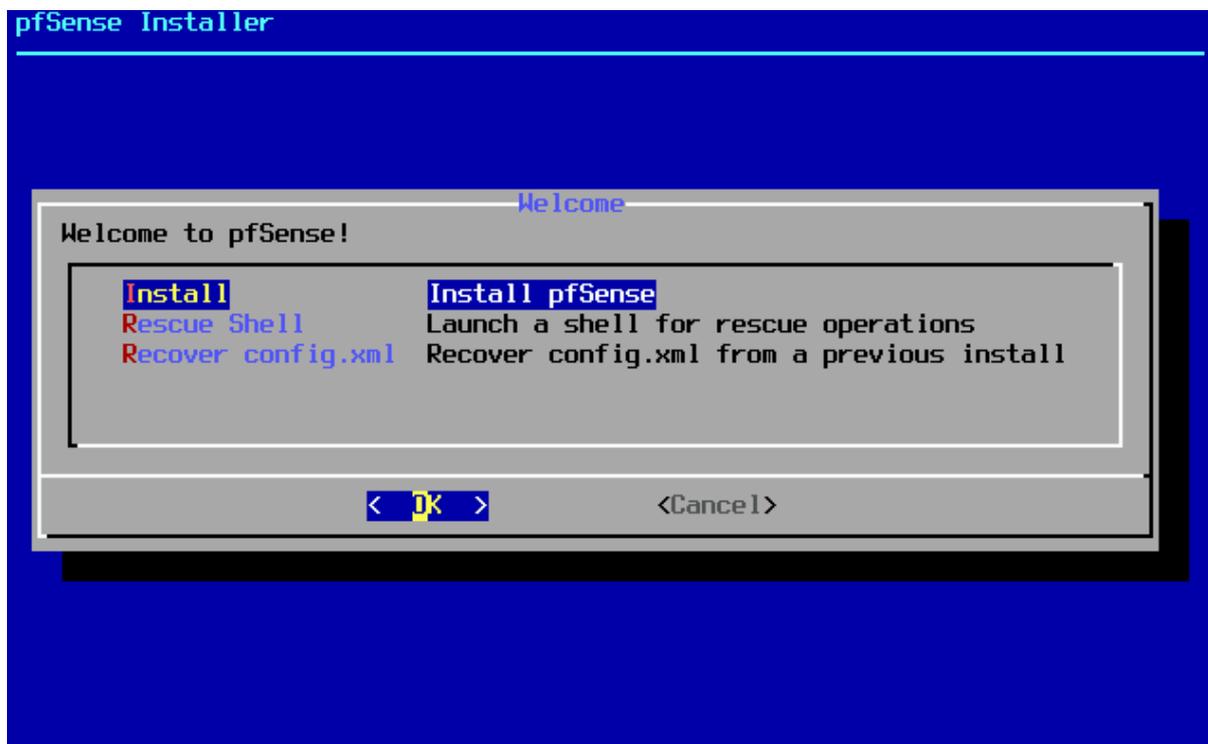
Configuration de base



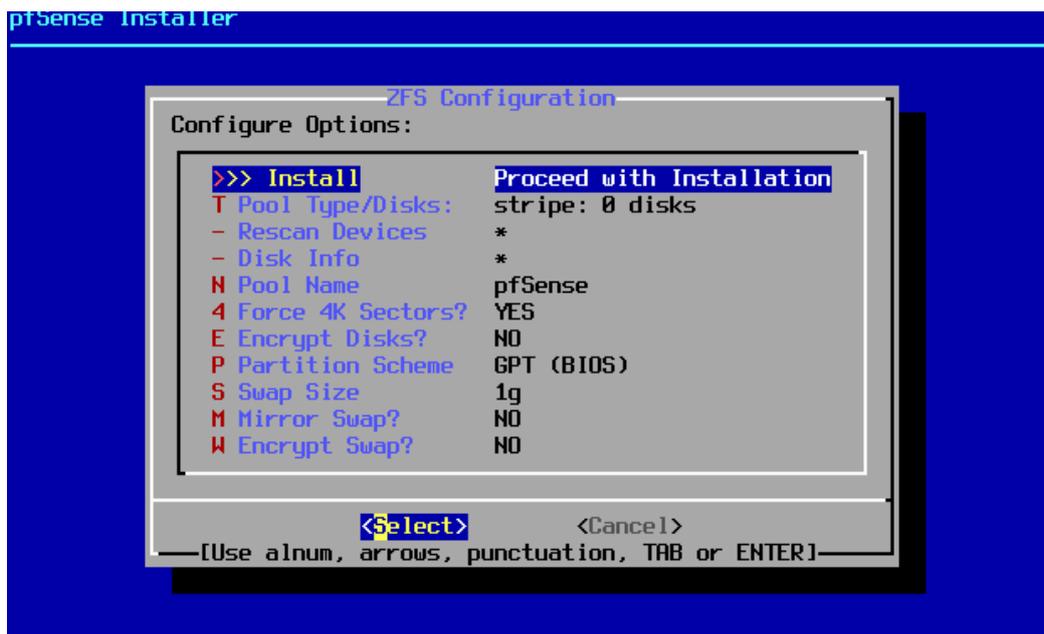
Sélectionné accept



Sélectionné Install pour commencer l'installation du pfsense



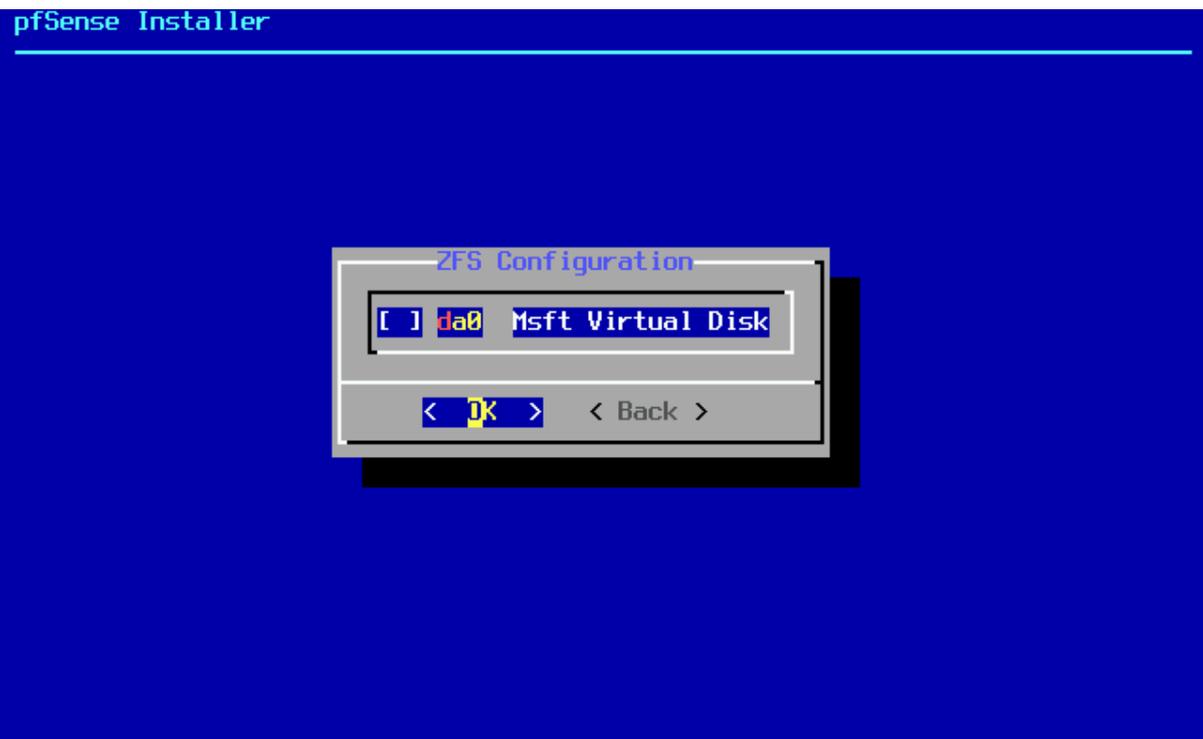
Installation guidée.



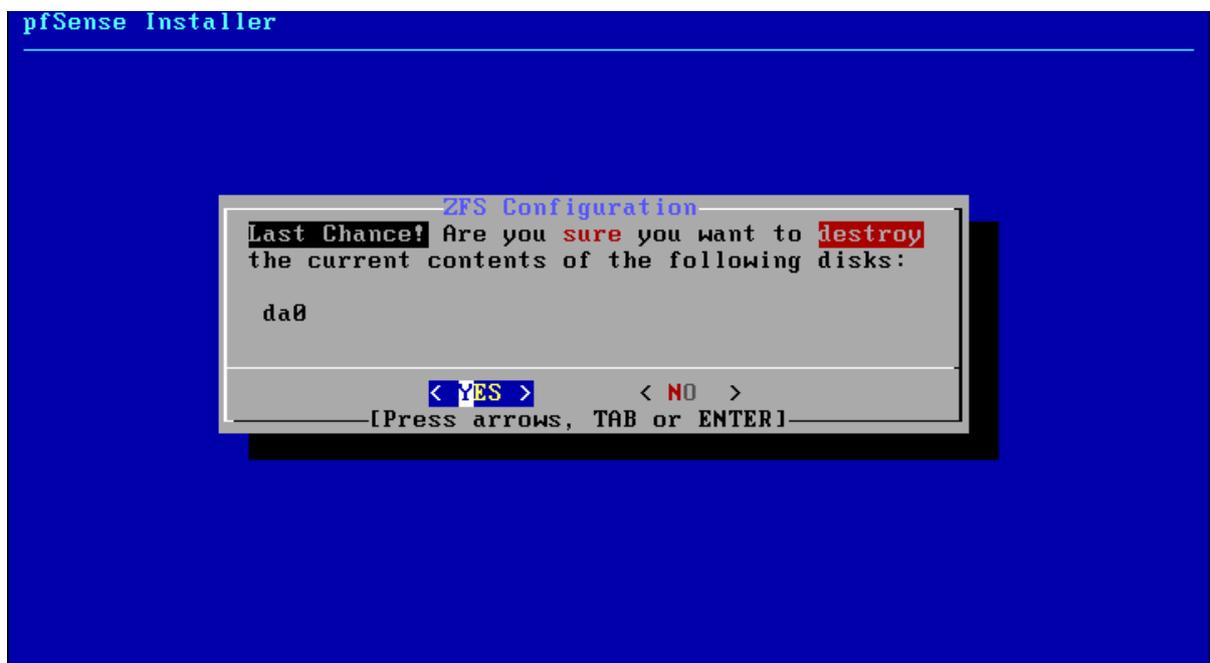
Sélectionner Stripe

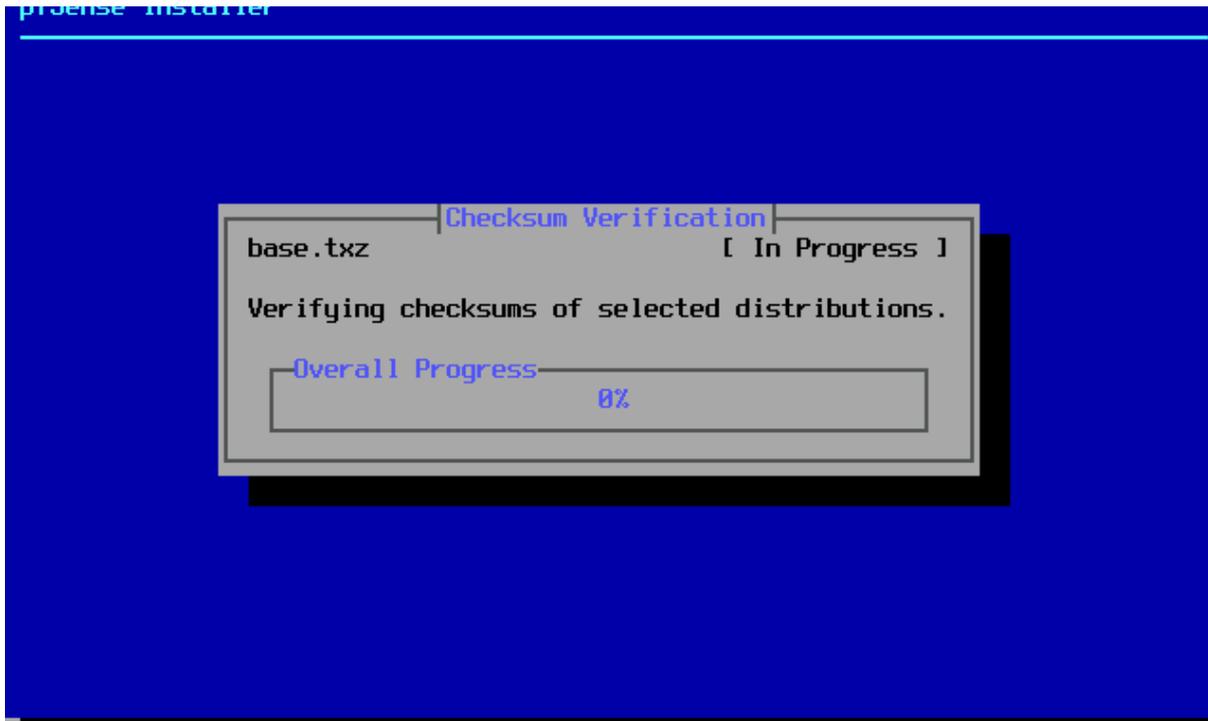


Choix du disque (appuyer sur espace puis entré)

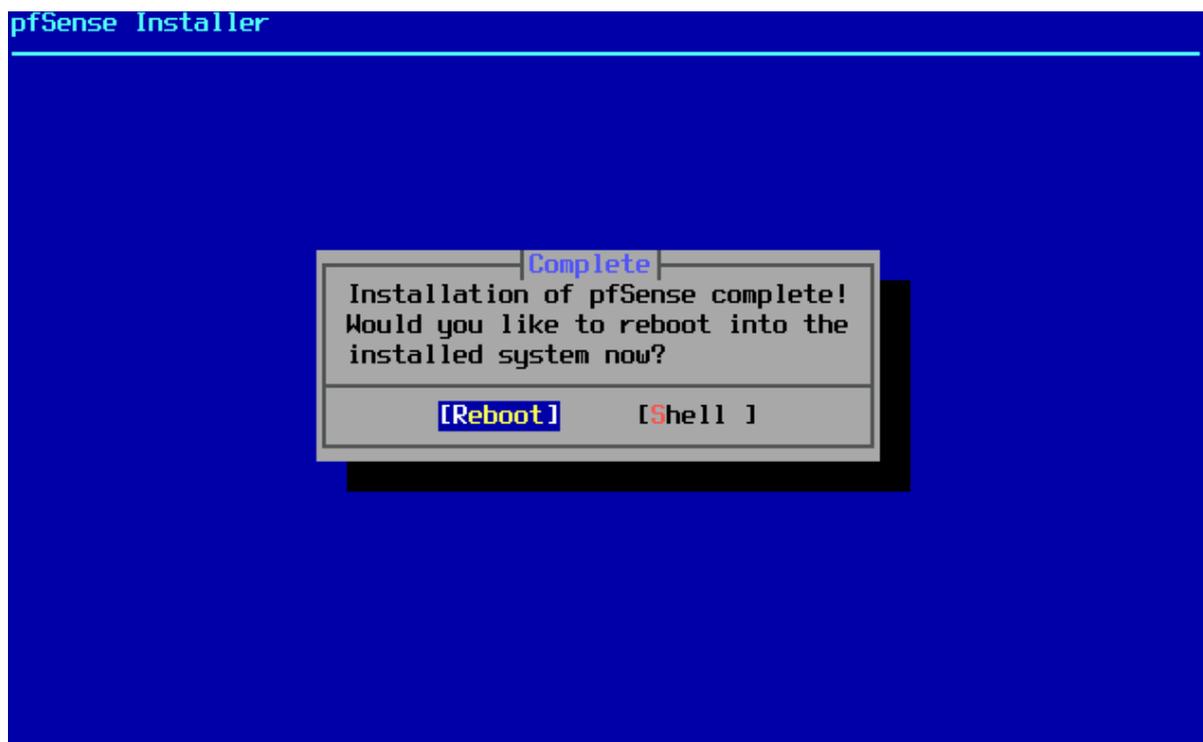


Confirmation



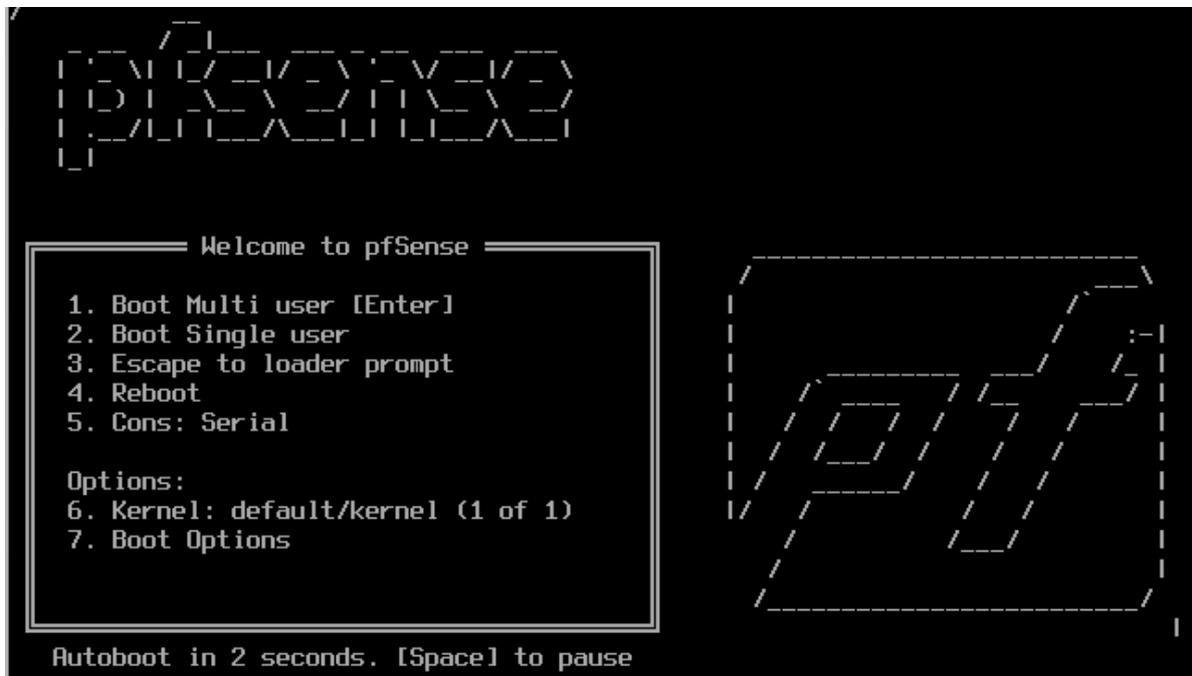


Faite entré sur reboot pour redémarrer votre machine



Penser à éjecter le disque.

Configuration des interfaces.



Pas de configuration de vlan

```
2025-02-23 14:26:06.723315+00:00 - php-fpm 379 - - /rc.linkup: Ignoring link event during boot sequence.
.....Migrating System Memory RRD file to new format
done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

hn0      00:15:5d:80:c2:1a (down) Hyper-V Network Interface
hn1      00:15:5d:80:c2:1b (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a):
```

Choix des interfaces.22

```
if the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): a

Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.

No link-up detected.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 a or nothing if finished): hn1

The interfaces will be assigned as follows:

WAN  -> hn0
LAN  -> hn1

Do you want to proceed [y|n]?
```

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.arp) (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.

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.10.10
Enter the end address of the IPv4 client address range: 192.168.10.30
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 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.10.1/

Press <ENTER> to continue.
```

```
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

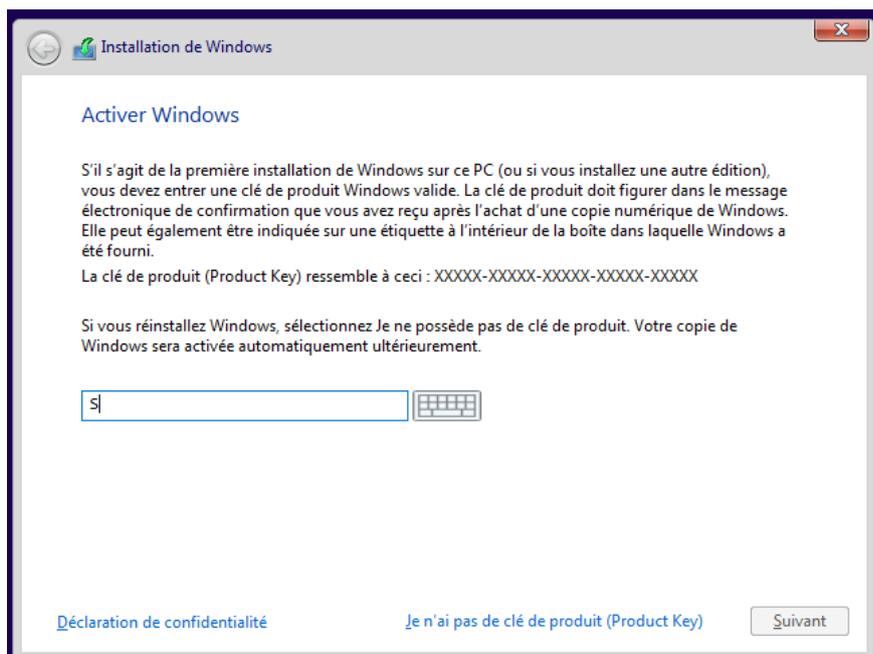
Enter an option: |
```

Installation de Windows.

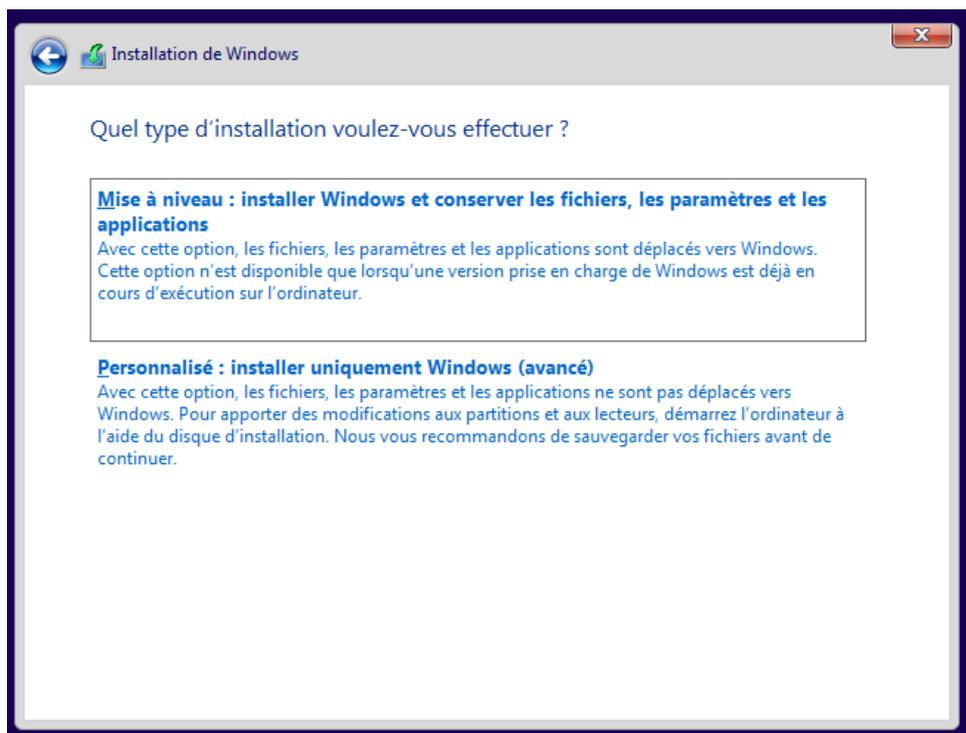
Choisir la langue du système



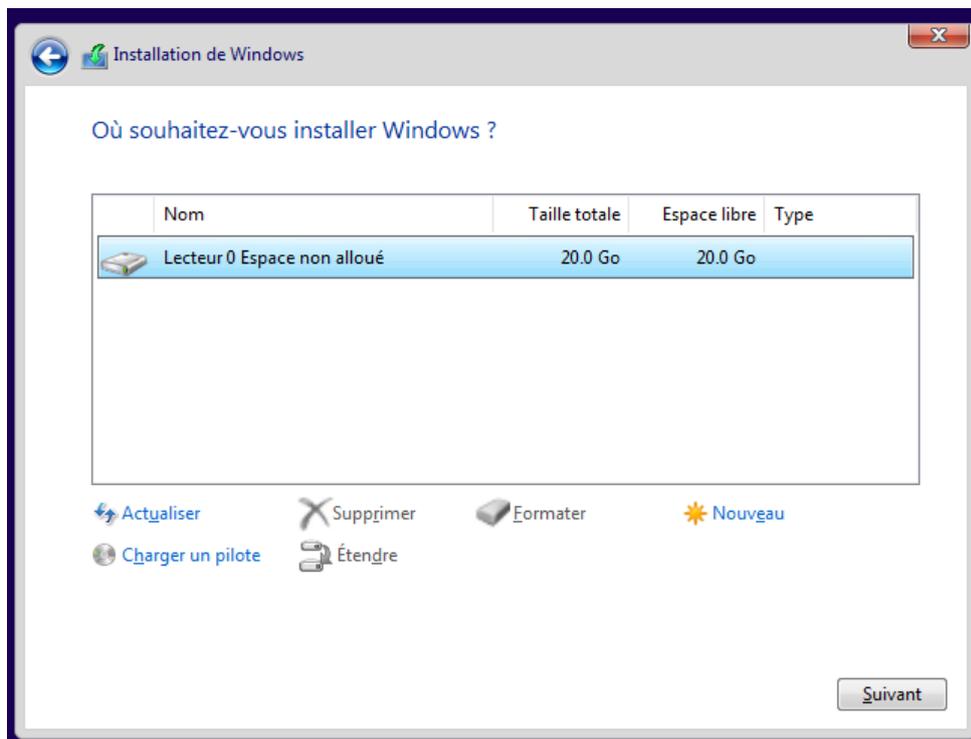
Renseigner une clé d'activation.



Choisir le type d'installation (ici personnalisé).



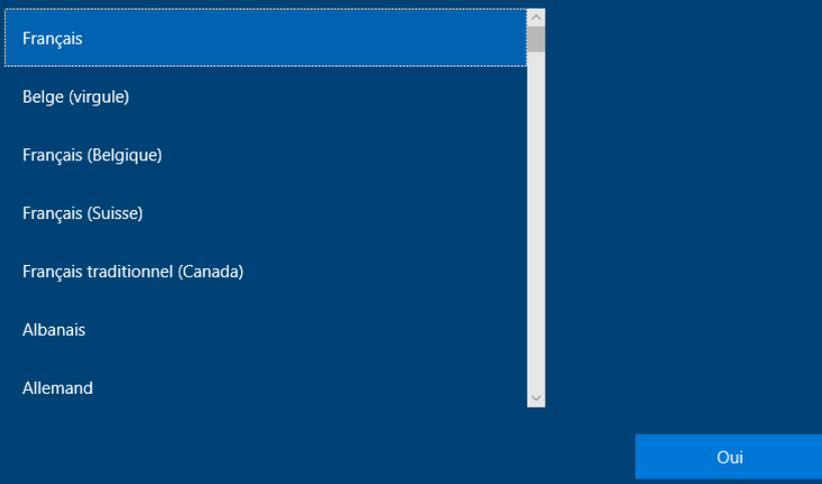
Sélectionner le disque d'installation.



Choisir la région du système et la disposition du clavier.

Est-ce la bonne disposition de clavier ?

Si vous utilisez également une autre disposition de clavier, vous pouvez l'ajouter après.



A screenshot of a Windows setup screen with a dark blue background. At the top, the text reads "Est-ce la bonne disposition de clavier ?" followed by "Si vous utilisez également une autre disposition de clavier, vous pouvez l'ajouter après." Below this is a list of keyboard layouts: Français (highlighted in blue), Belge (virgule), Français (Belgique), Français (Suisse), Français traditionnel (Canada), Albanais, and Allemand. A vertical scrollbar is on the right side of the list. At the bottom right, there is a blue button labeled "Oui".

Choisir la configuration (ici personnelle).

Comment souhaitez-vous configurer ?



Configurer pour une utilisation personnelle

Nous vous aiderons à effectuer une configuration avec un compte personnel Microsoft. Vous aurez un contrôle total sur cet appareil.



Configurer pour une organisation

Vous aurez accès aux ressources de votre organisation, notamment la messagerie électronique, le réseau, les applications et les services. Votre organisation disposera d'un contrôle total sur cet appareil.

Suivant

Choisir un type de compte (ici hors connexion)

Ajoutez votre compte

Un seul compte vous permet de connecter votre appareil aux applications et services Microsoft, comme Office, OneDrive, Microsoft Edge et le Microsoft Store.



Créer un compte
Connexion avec une clé de sécurité

Votre compte Microsoft est utilisé pour activer les fonctionnalités des applications et services Microsoft lorsque vous vous connectez, y compris la sauvegarde des données sur votre appareil au cas où vous deviez les remplacer ou les restaurer. Vos paramètres, votre historique de navigation, vos favoris, vos mots de passe, vos contacts, etc., sont également synchronisés entre vos appareils.

[Compte hors connexion](#) [Confidentialité et cookies](#) [Conditions d'utilisation](#) [Découvrir plus d'inform](#)

Suivant

Choisir un nom d'utilisateur

Qui sera amené à utiliser ce PC ?

Quel nom voulez-vous utiliser ?

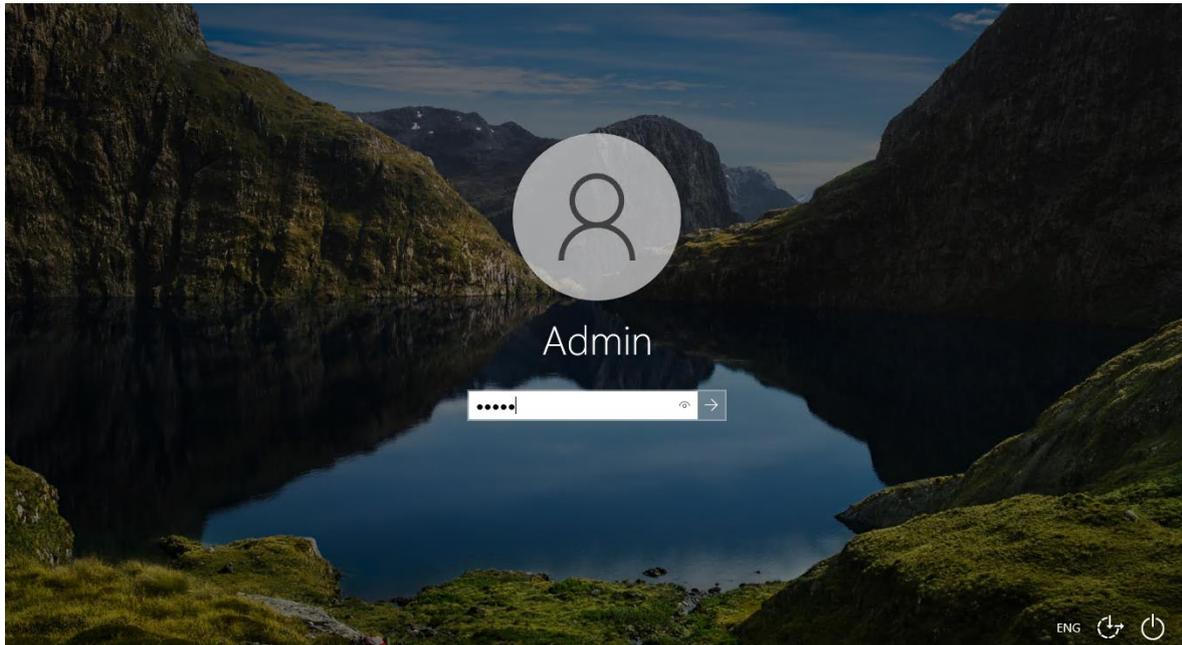


Ou, encore mieux, utilisez un compte en ligne

Suivant

Choisir un mot de passe

Personnaliser l'expérience utilisateur.

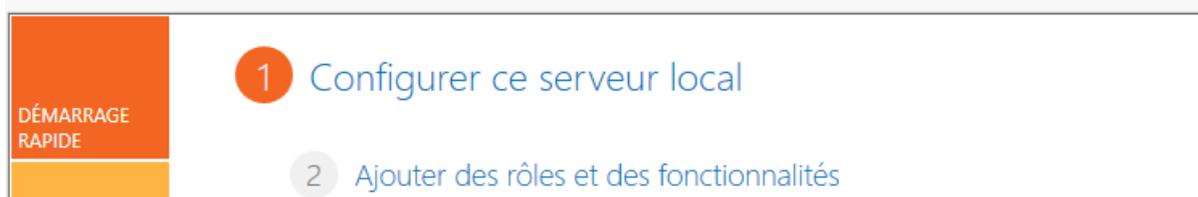


Procédure Active directory

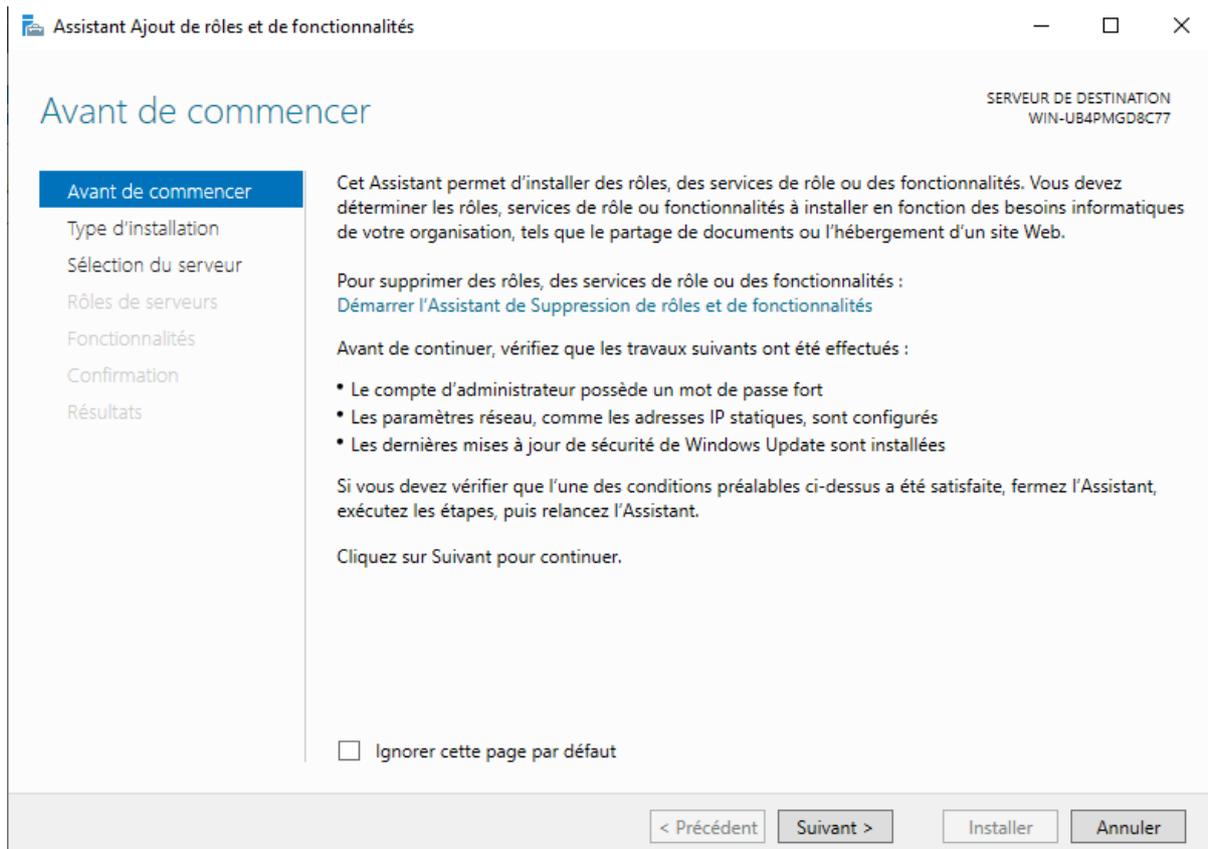
Création serveur Active directory

Installation du rôle d'Active directory

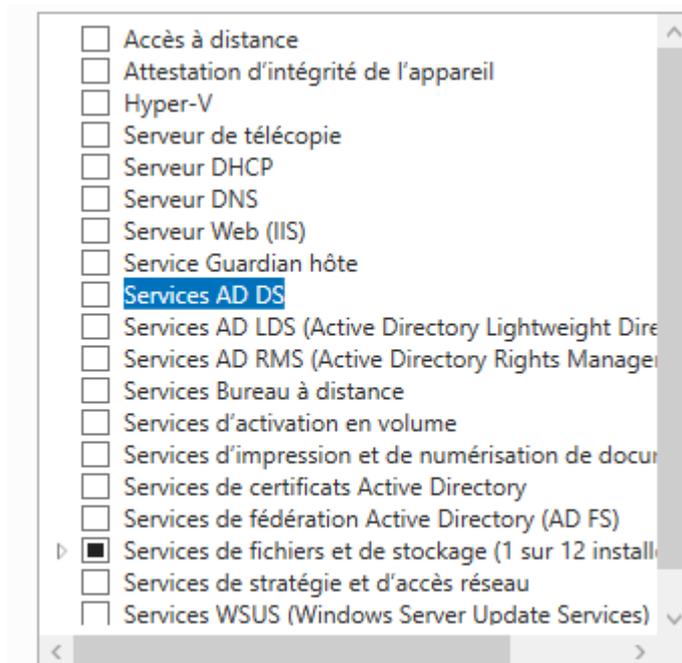
Commençons par cliquer sur 'ajouter des rôles et des fonctionnalités'



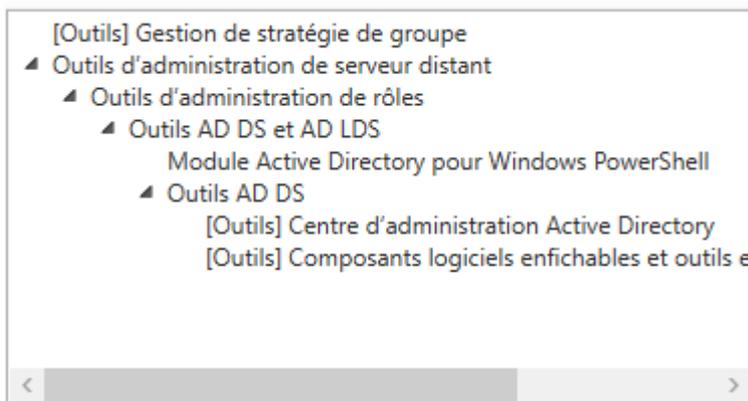
Depuis la page 'avant de commencer' poursuive jusqu'à 'rôle de serveurs' en cliquant sur le bouton "suivant"



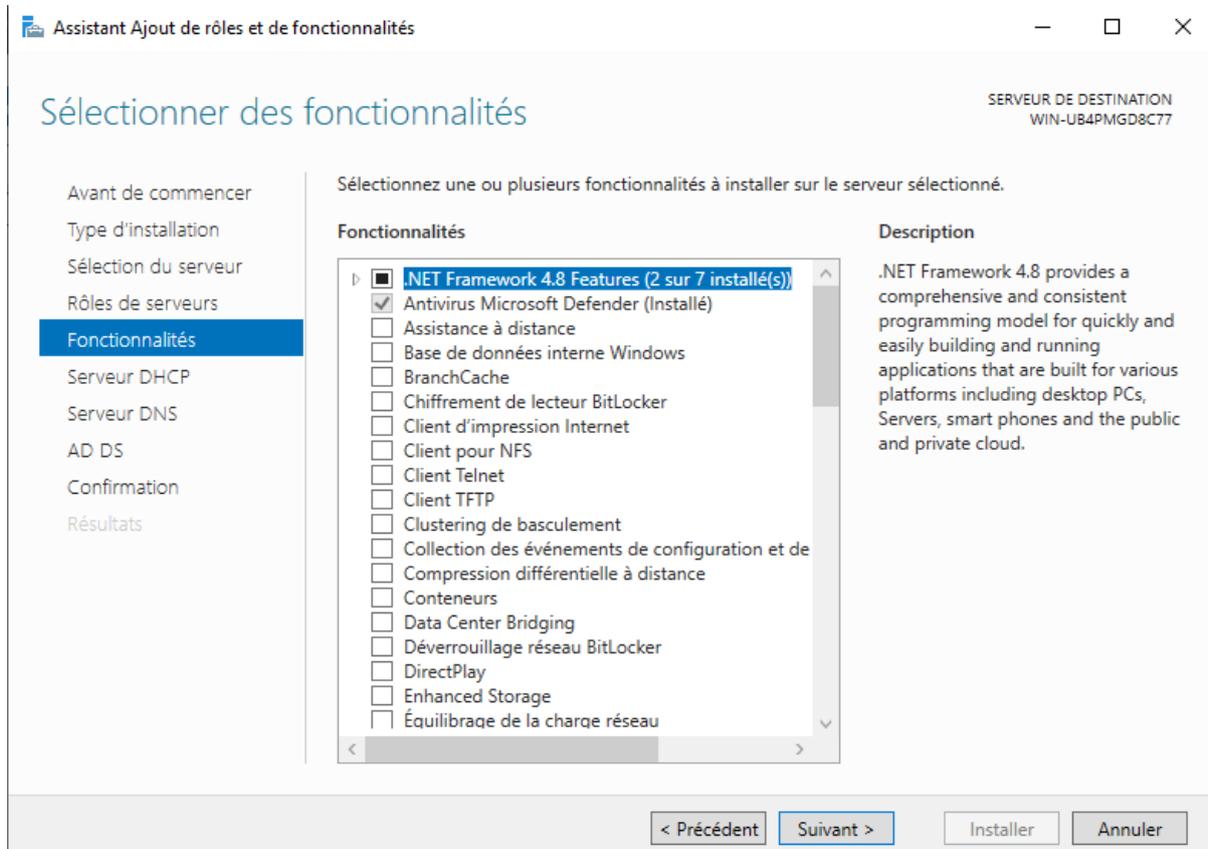
Selectionné le rôle désiré dans notre cas 'Service AD DS'



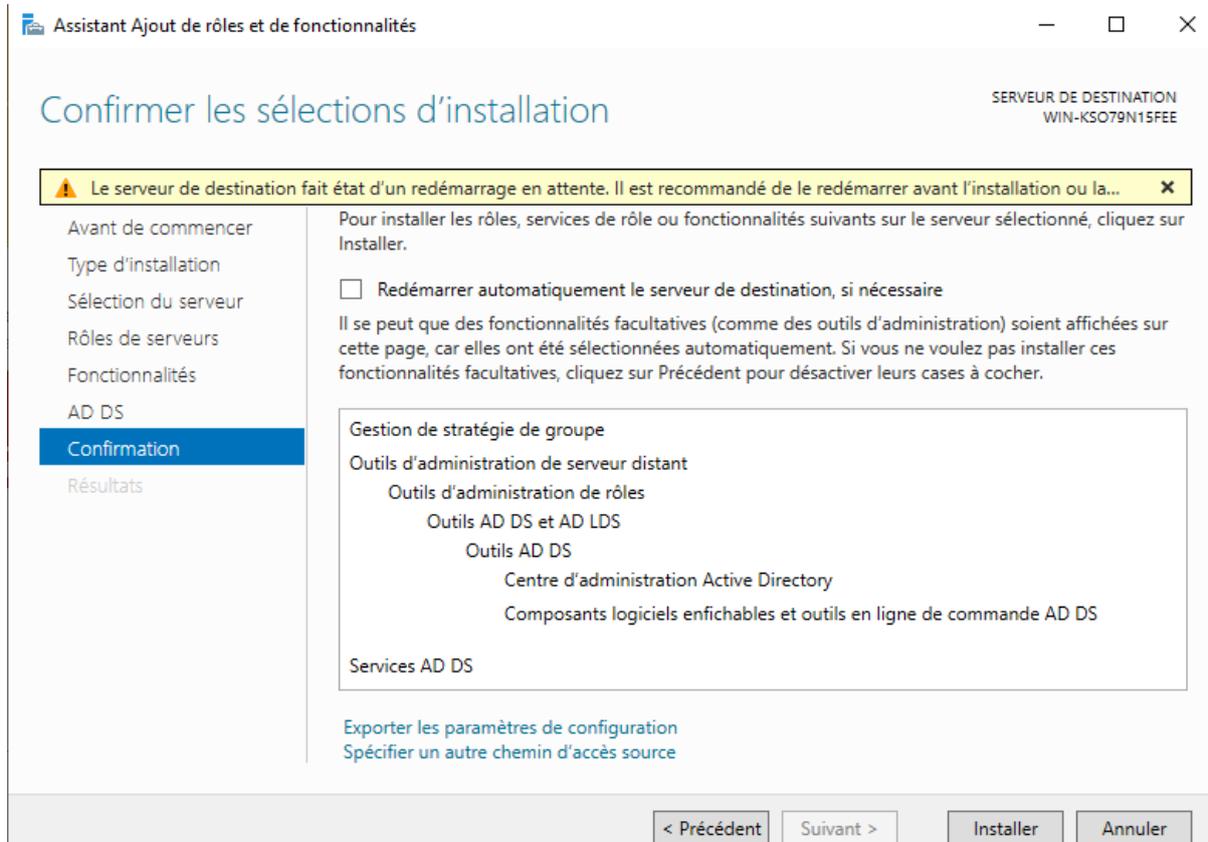
Accepté la page des fonctionnalités nécessaire qui vas s'ouvrir et cliqué ensuite sur suivant



Poursuivre jusqu'à confirmation

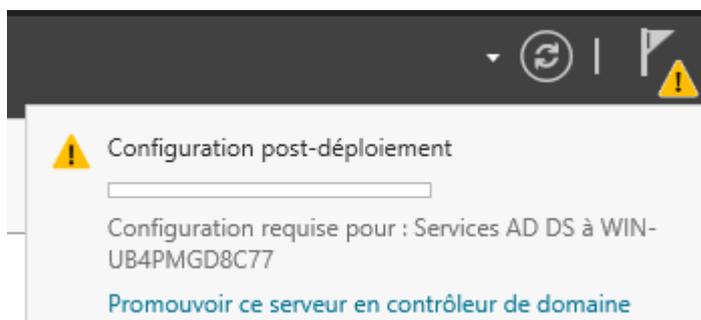


Puis cliqué sur installation.

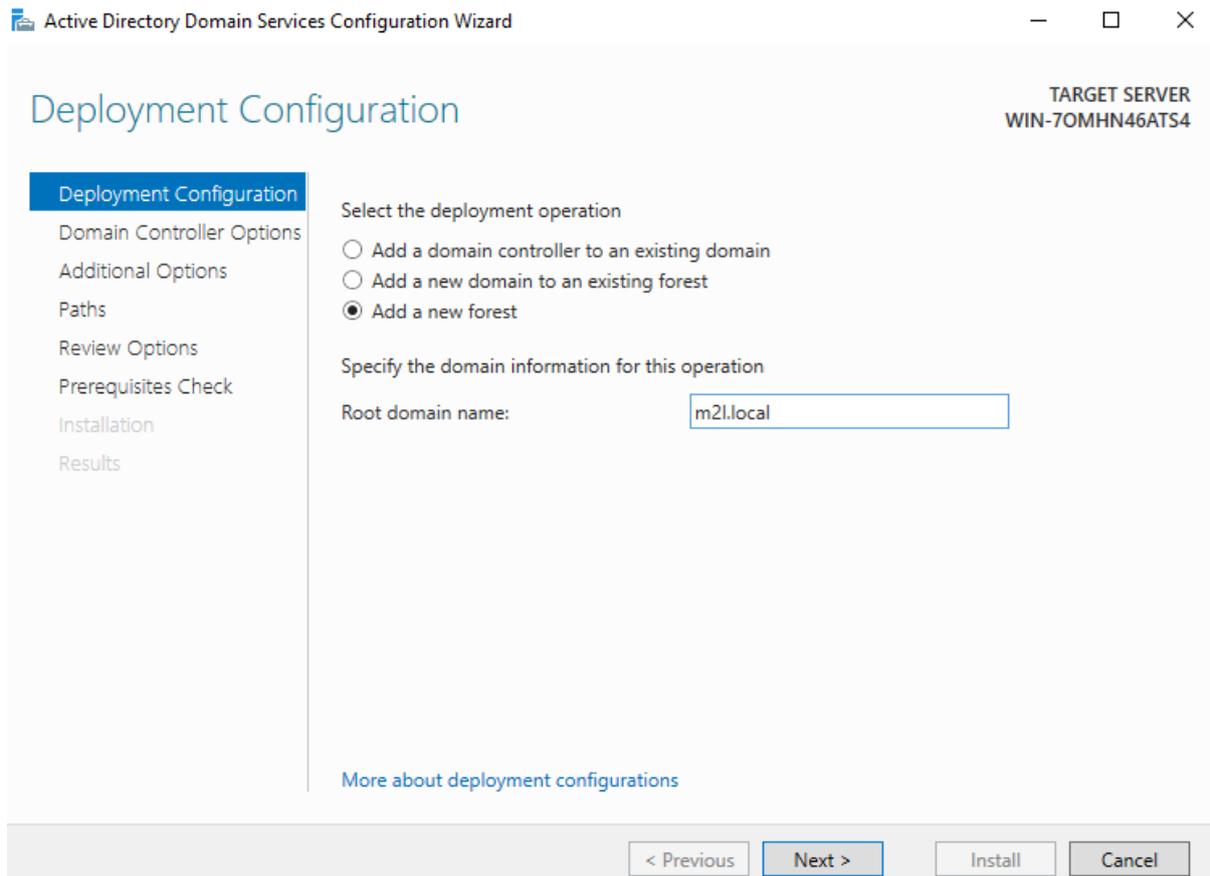


Configuration des services de domaine Active directory

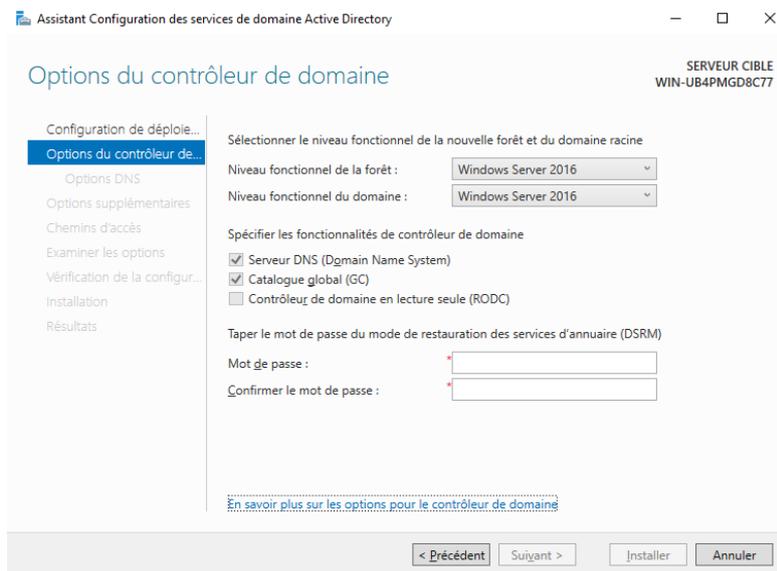
Lorsque l'installation se termine une notification en haut a droit va apparaître cliqué sur 'Promouvoir ce serveur en contrôleur de domaine.'



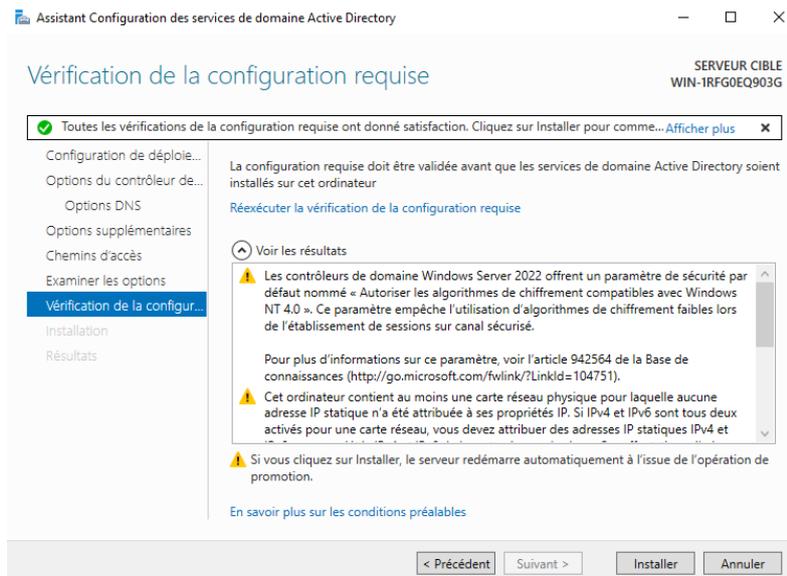
Coché la case Ajouté une nouvelle forêt puis donné un nom a cette dernierX.X



Donné un mot de passe à ce domaine

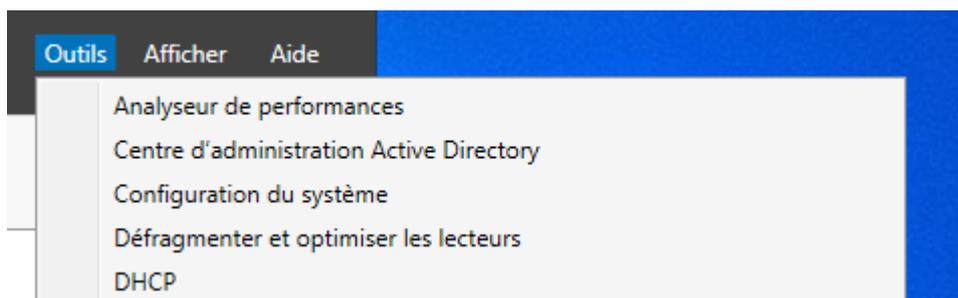


Poursuivé jusqu'à la page "vérification de la configuration" et cliqué sur installer

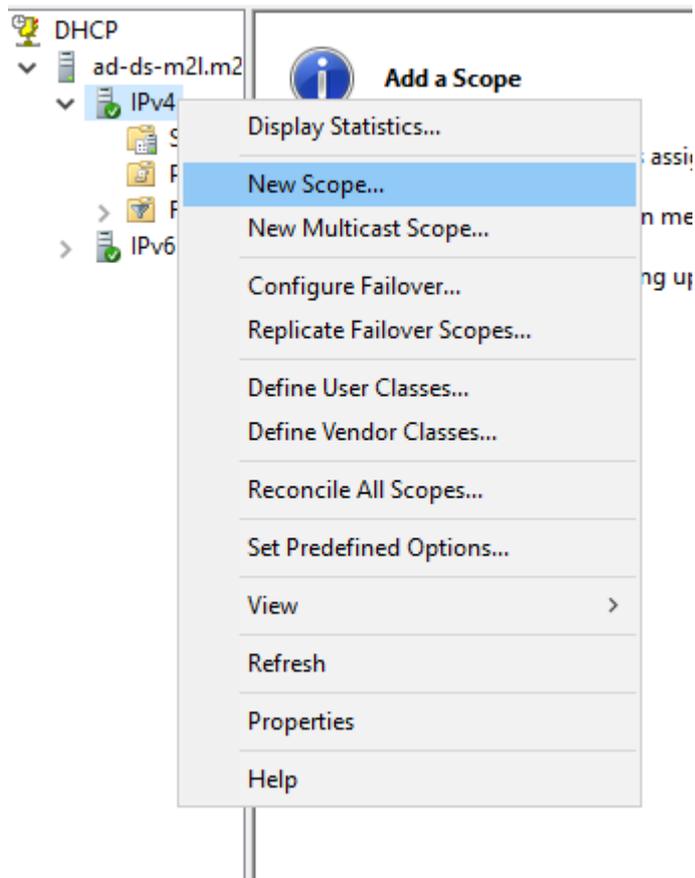


Configuration DHCP

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

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

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

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Choisir la durée du bail

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

Next >

Cancel

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

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

Choix du routeur par défaut

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

<input type="text"/>	Add
192.168.1.1	Remove
	Up
	Down

< Back Next > Cancel

Le Domain et DNS utilisé

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:
<input type="text"/>	<input type="text"/>
<input type="button" value="Resolve"/>	169.254.74.23
	<input type="button" value="Add"/>
	<input type="button" value="Remove"/>
	<input type="button" value="Up"/>
	<input type="button" value="Down"/>

< Back Next > Cancel

Activation de la nouvelle étendu

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

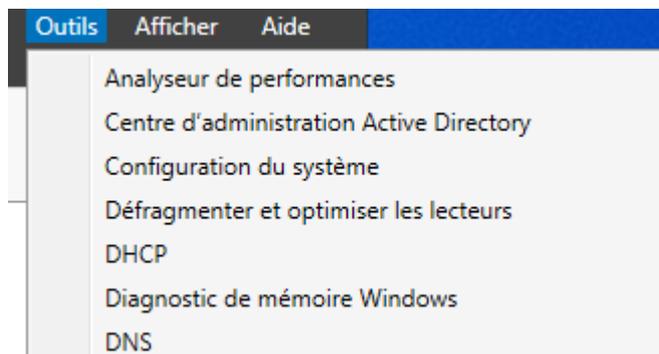
Yes, I want to activate this scope now

No, I will activate this scope later

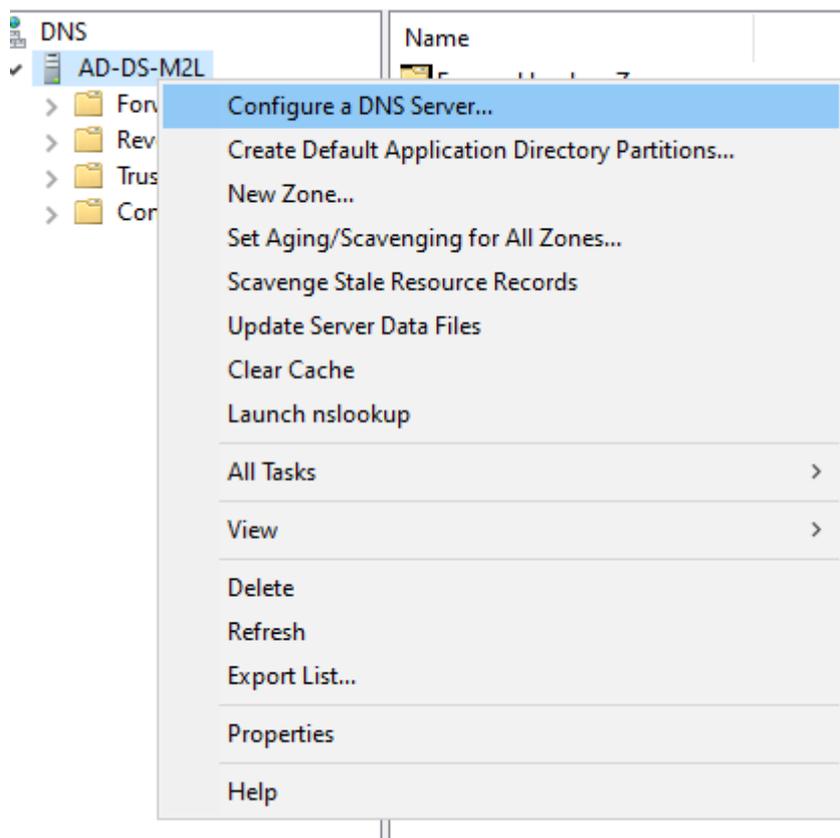
< Back Next > Cancel

Configuration DNS

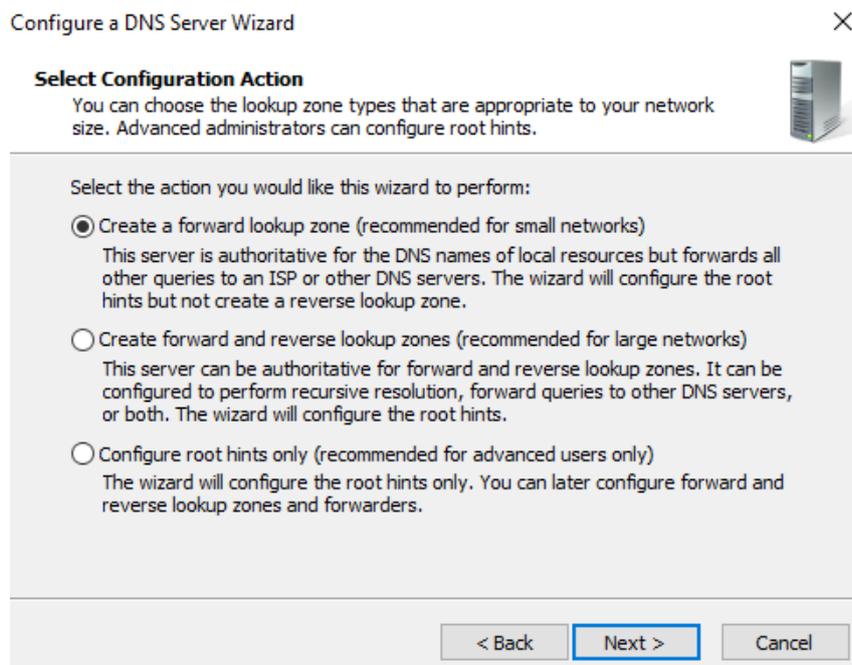
Allez dans l'onglet DNS en haut droite du gestionnaire de serveur dans outil



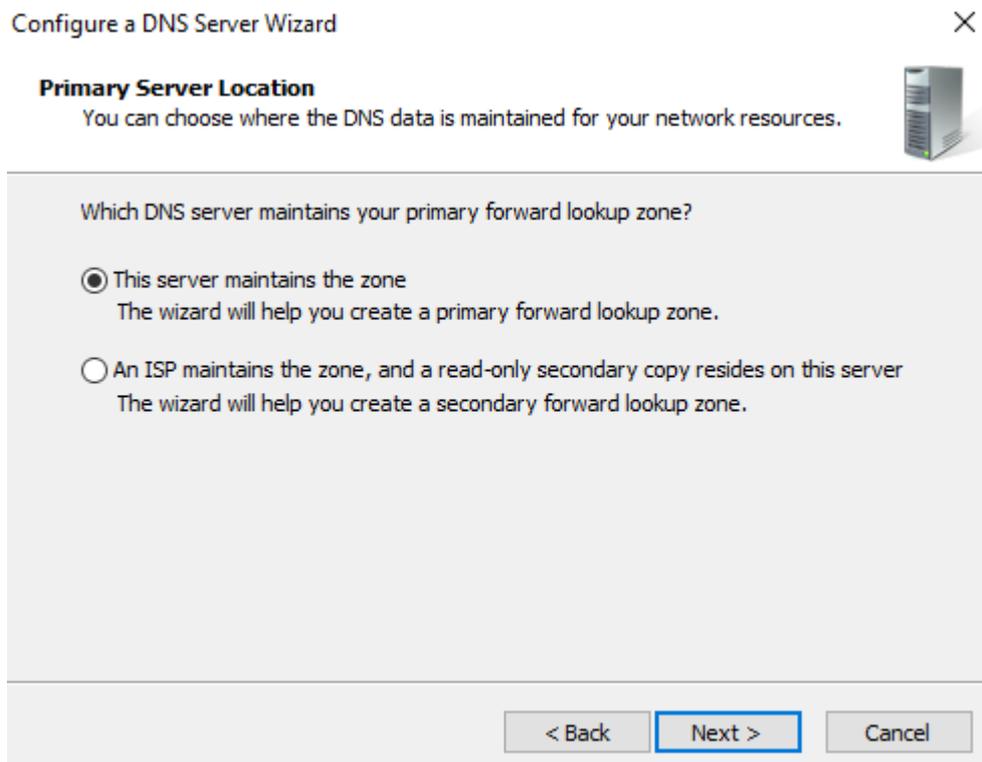
Faite clic droit sur le serveur ad et faite "configuration serveur DNS"



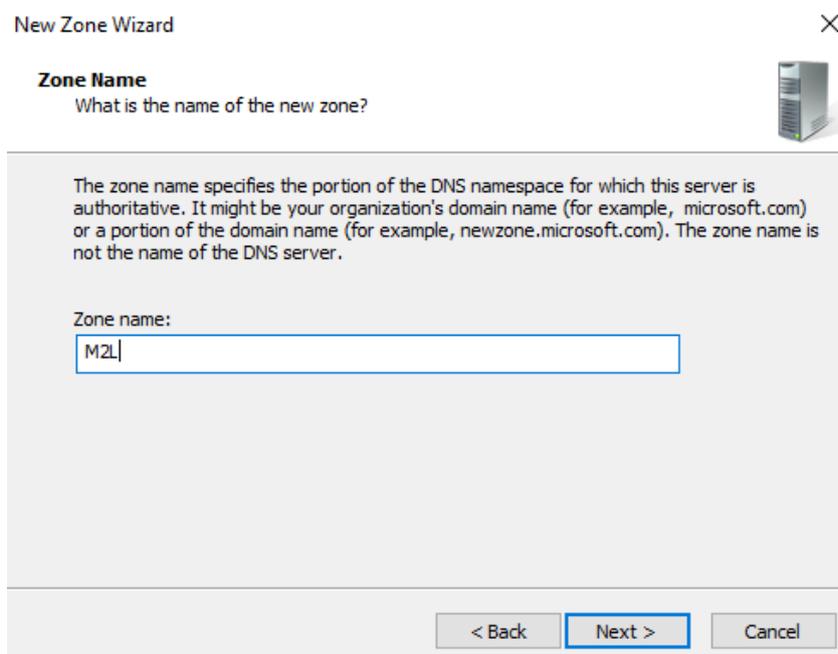
À l'étape "Select Configuration Action", sélectionnez "Create a forward lookup zone" afin de permettre à votre serveur DNS de résoudre les noms de domaine locaux en adresses IP dans un petit réseau.



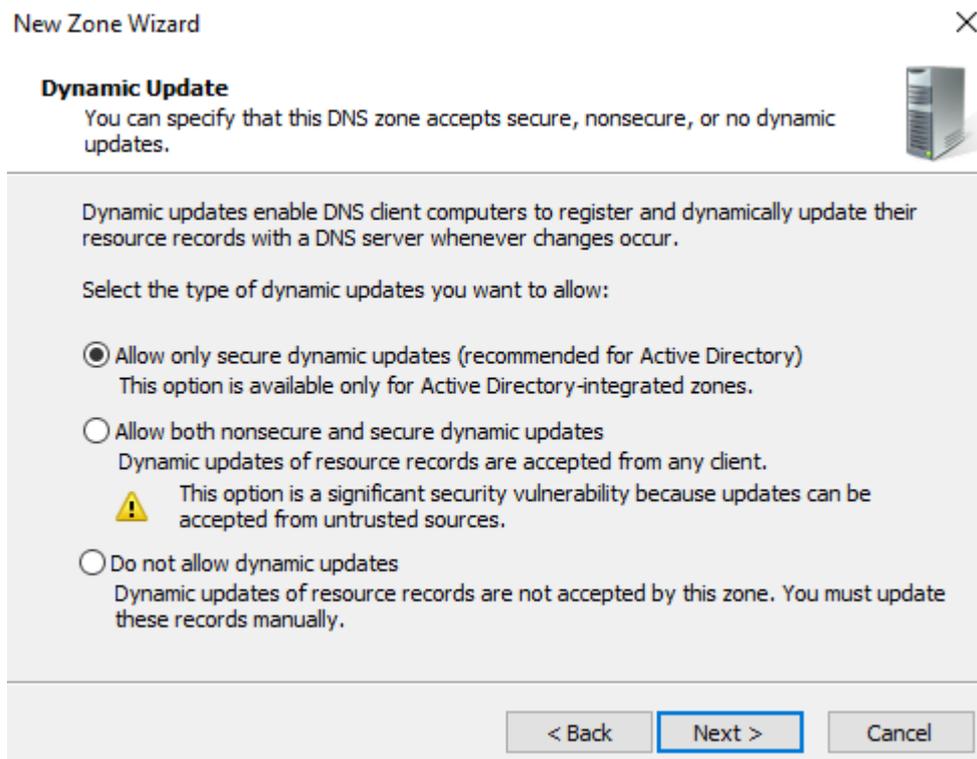
À l'étape "Primary Server Location", sélectionnez "This server maintains the zone" afin de créer une zone de recherche directe principale directement hébergée sur votre serveur DNS.



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"

Configure a DNS Server Wizard



Forwarders

Forwarders are DNS servers to which this server sends queries that it cannot answer.



Should this DNS server forward queries?

Yes, it should forward queries to DNS servers with the following IP addresses:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
8.8.8.8	<Attempting to r...	OK

Delete

Up

Down

No, it should not forward queries

If this server is not configured to use forwarders, it can still resolve names using root name servers.

< Back

Next >

Cancel

Terminer la configuration cliquer sur finir

Configure a DNS Server Wizard



Completing the Configure a DNS Server Wizard

You have successfully completed the Configure a DNS Server Wizard. When you click Finish, the following settings will be saved.

Settings:

DNS server to configure: AD-DS-M2L
Forward lookup zone to create: M2L
IP address of forwarder: 8.8.8.8

Configure the hosts that will use this DNS server to point to this DNS server for name resolution, and then verify name resolution using nslookup. If you added a new primary zone, add resource records to it for the hosts whose names need to be resolved by this DNS server.

To close this wizard, click Finish.

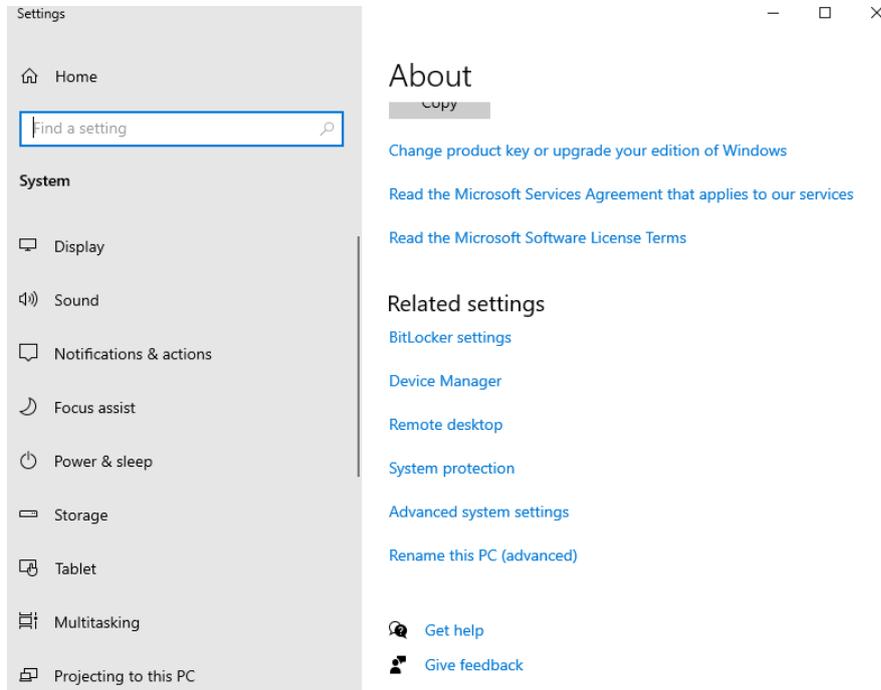
< Back

Finish

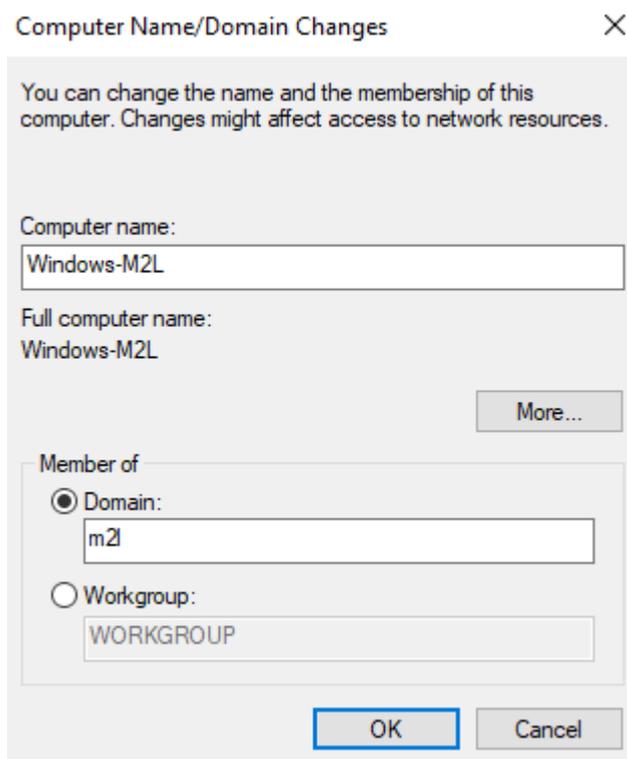
Cancel

Ajout dans le domaine

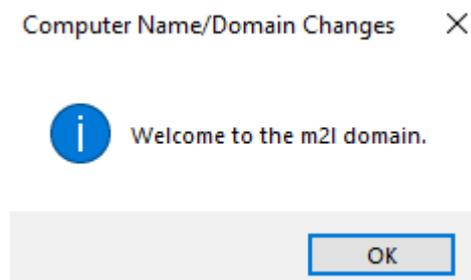
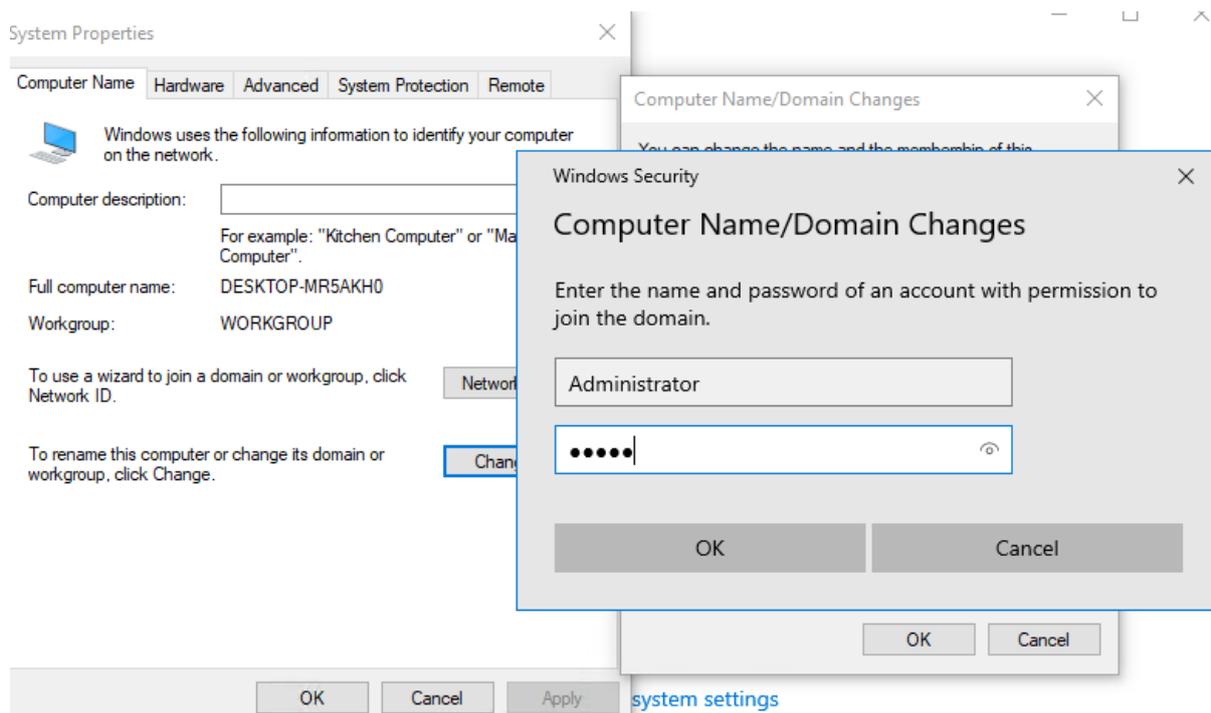
Se rendre dans les paramètres, puis rechercher nom et enfin cliquer sur Renommer ce pc (avancé)



Rentrer les informations



Se connecter avec l'administrateur



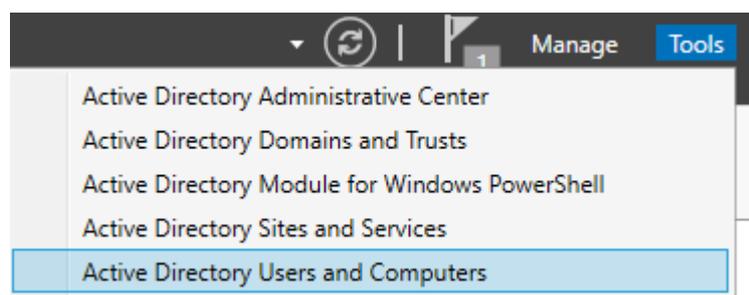
Si cela fonctionne, nous avons vérifié que le DNS et le DHCP fonctionnent.

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

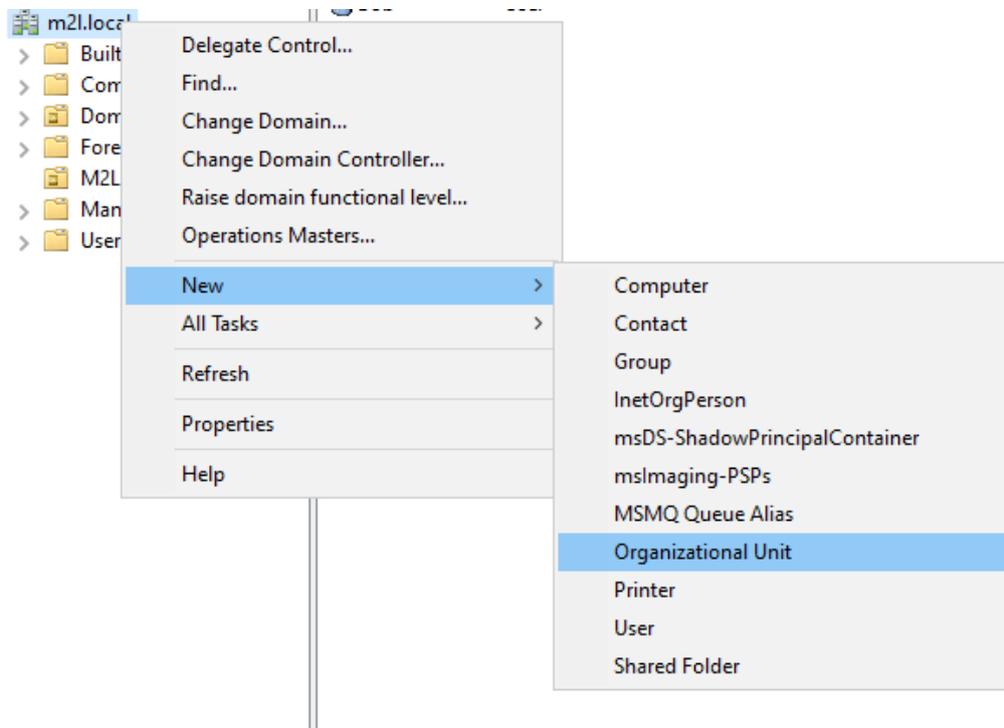
Gestion unité d'organisation et utilisateur

Création unités d'organisations

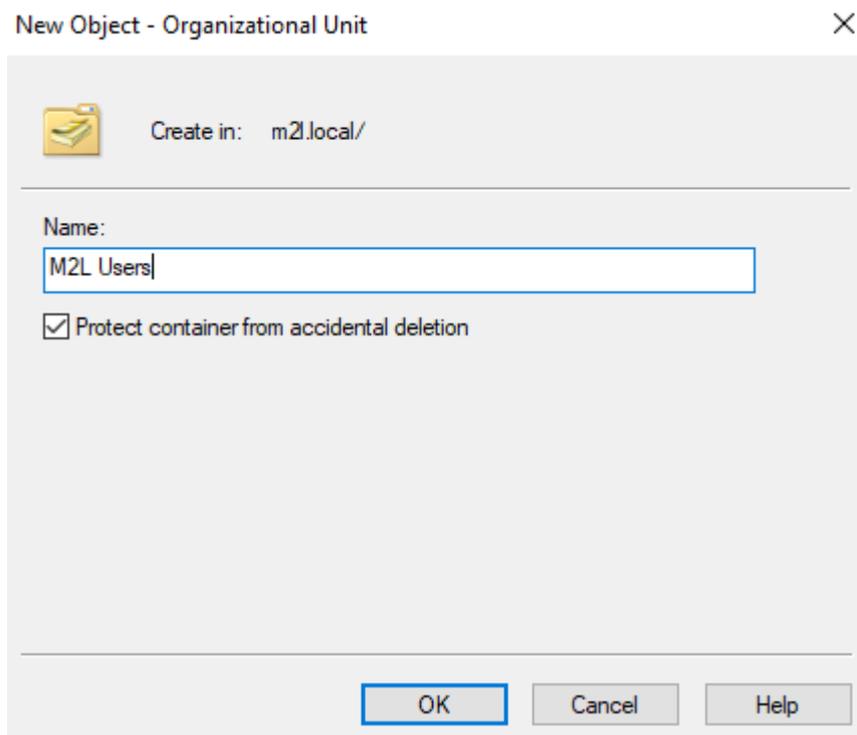
Tout d'abord nous allons nous rendre dans l'onglet 'Active directory Users and Computer'



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

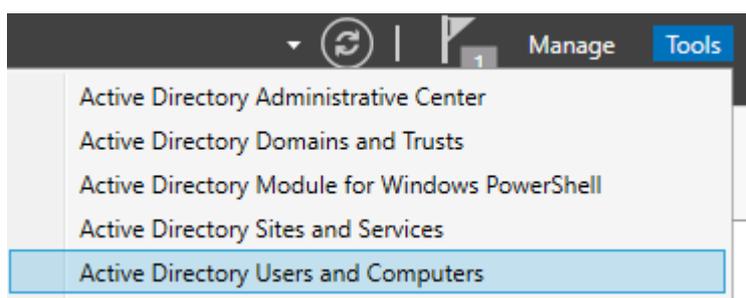


Créer votre unité d’organisation avec le nom désiré

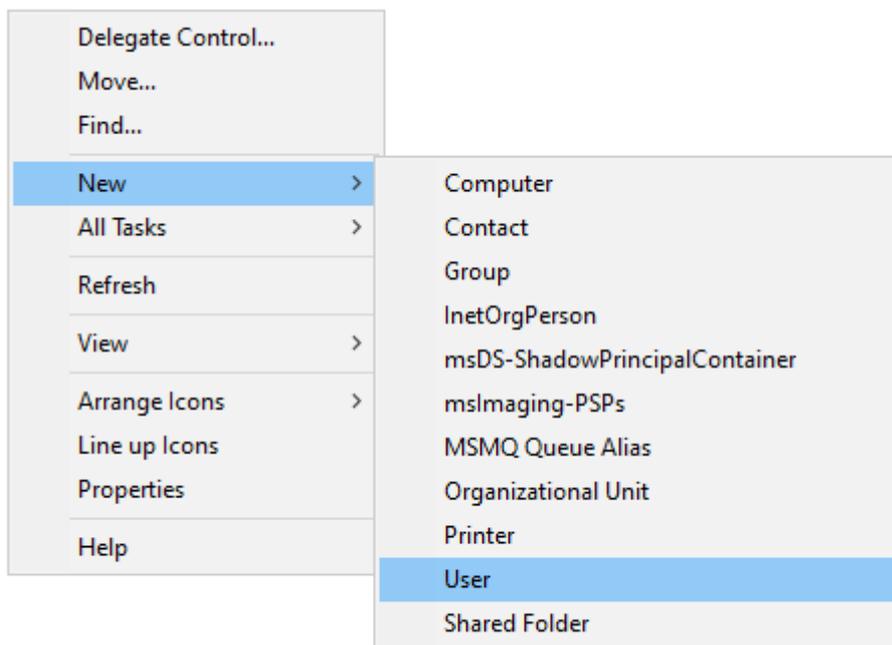


Création user

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



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



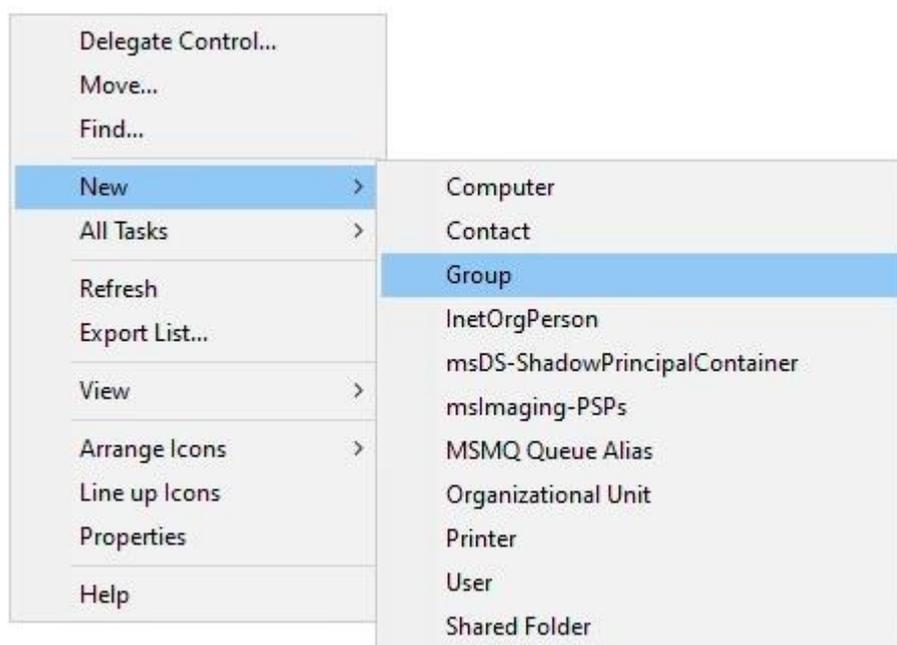
Puis suivez les indications en prenant soins de remplir les informations demandées

Création d'un groupe de sécurité.

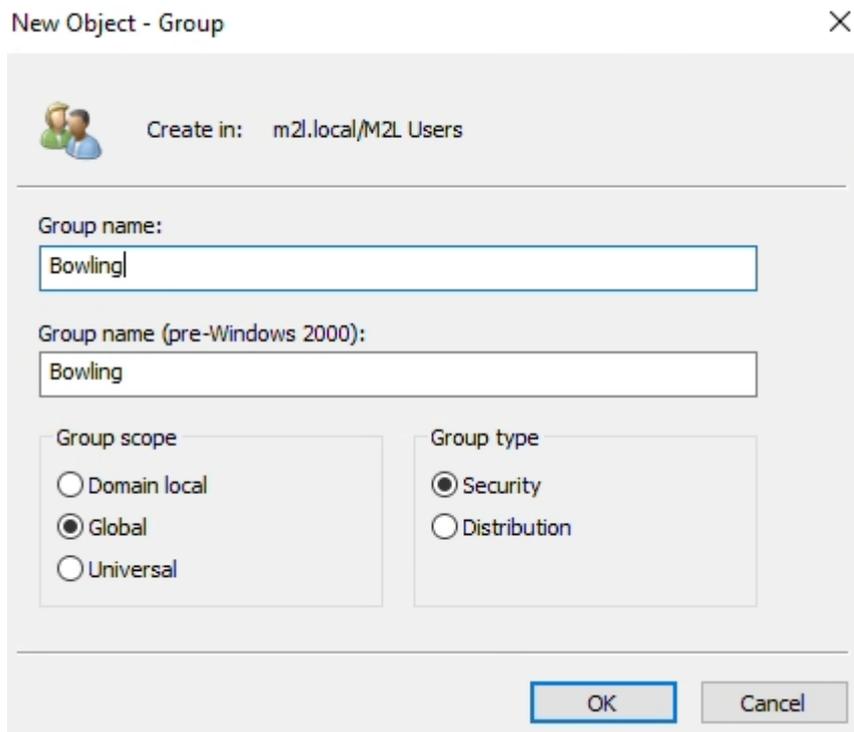
Tout d'abord nous allons nous rendre dans l'onglet "Active directory Users and Computer"



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

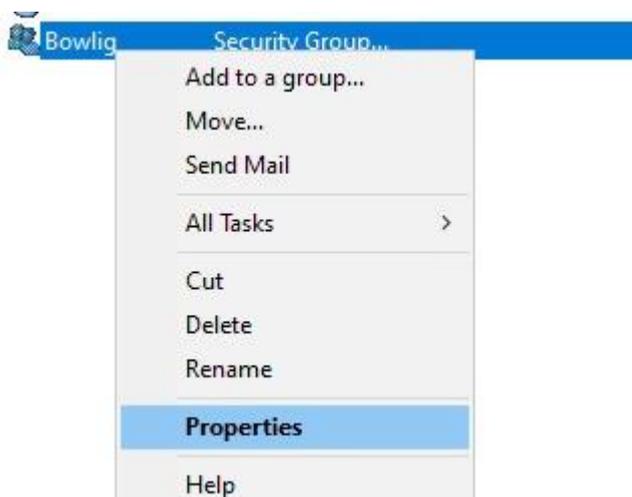


Puis suivez les indications en prenant soins de remplir les informations demandées

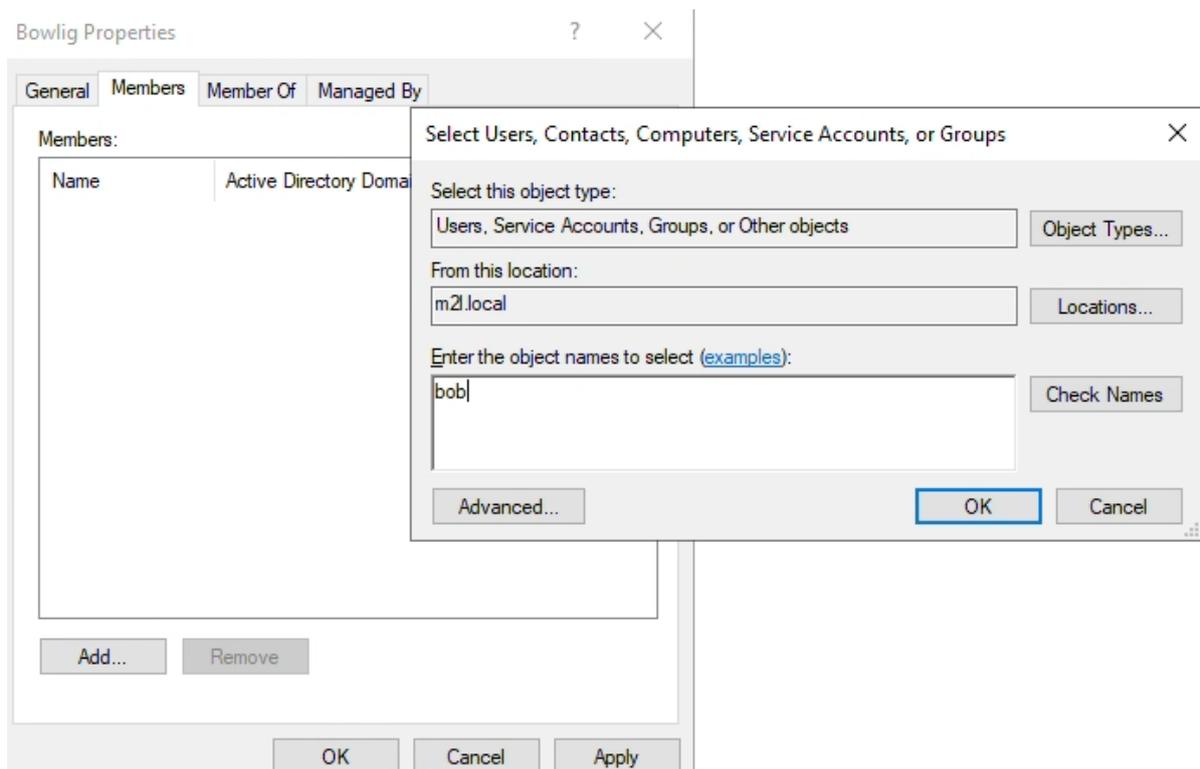


Ajout d'un utilisateur dans le groupe de sécurité.

Faite clic droit sur votre groupe et faite properties.



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



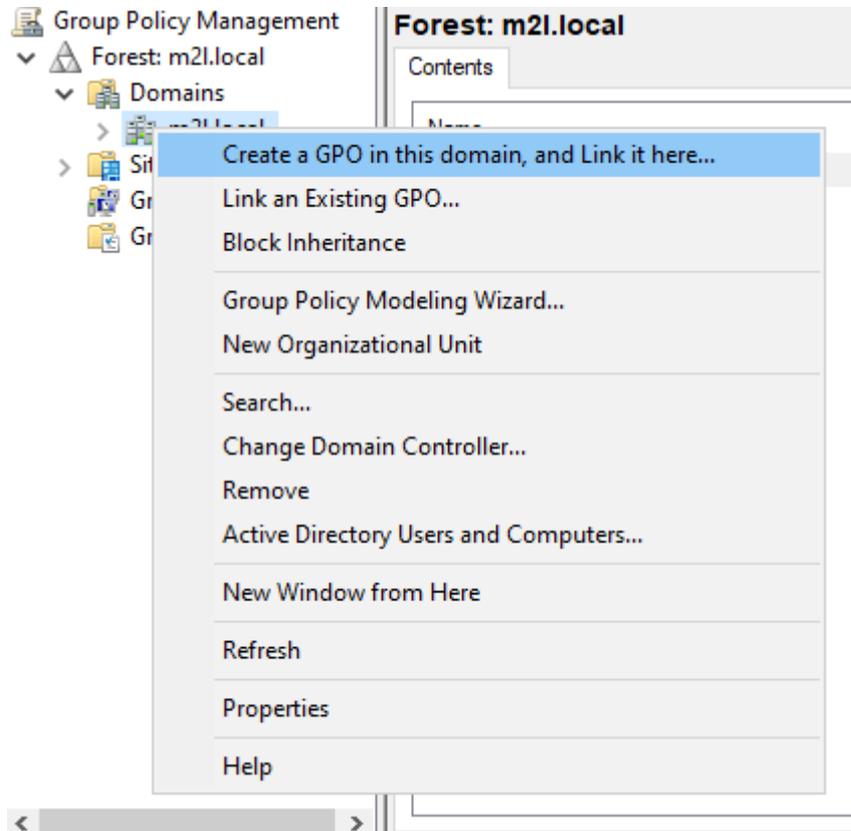
Déploiement d'une application via le GPO

Création d'un nouvel objet GPO

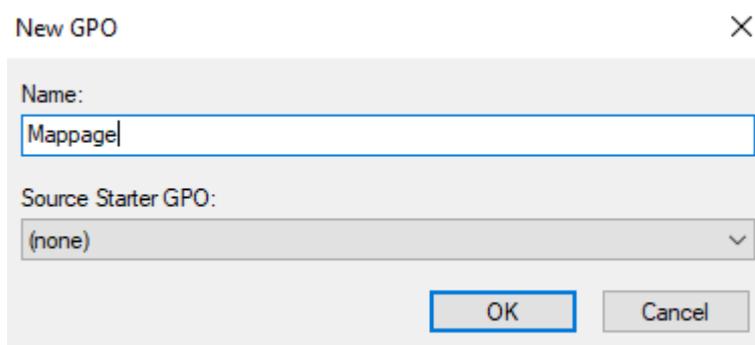
Allez dans l'onglet "Gestion de stratégie de groupe" en haut droite du gestionnaire de serveur dans outil

Gestion des stratégies de groupe

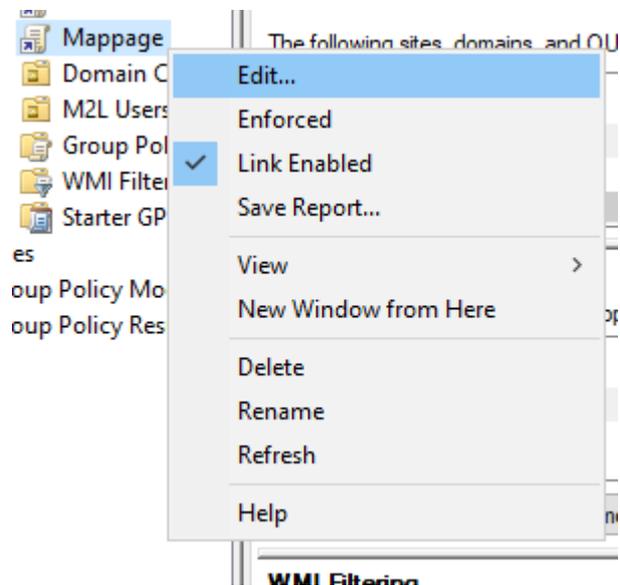
Créer une nouvelle GPO
Faites un clic droit sur le domaine, puis sélectionnez "Create a GPO in this domain, and Link it here..." pour créer et lier une stratégie de groupe.



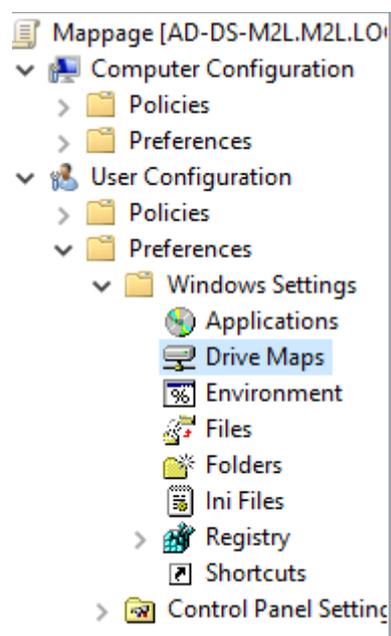
Choisir le nom de cette dernière



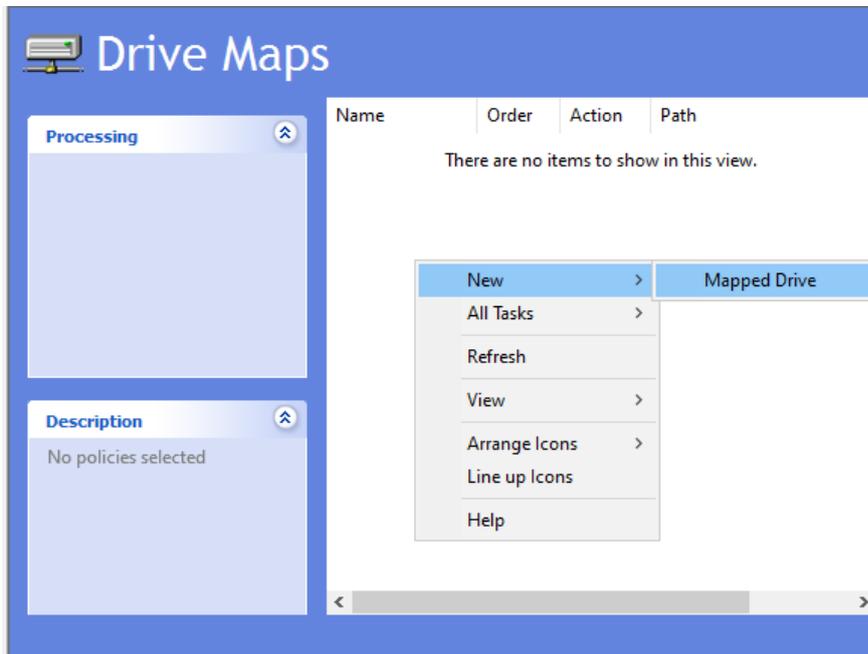
Faites un clic droit sur la GPO souhaitée puis sélectionnez **"Edit..."** pour modifier sa configuration.



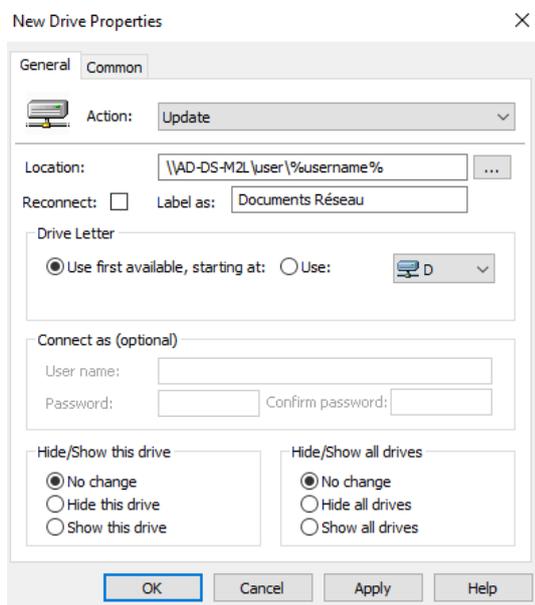
Dans l'éditeur de GPO, accédez à User Configuration > Preferences > Windows Settings > Drive Maps pour créer un lecteur réseau attribué aux utilisateurs.



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

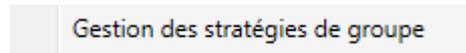


Une fois le lecteur créé, fermez l'éditeur de GPO, puis effectuez un gpupdate /force dans l'invite de commandes sur un poste client pour appliquer immédiatement la stratégie.

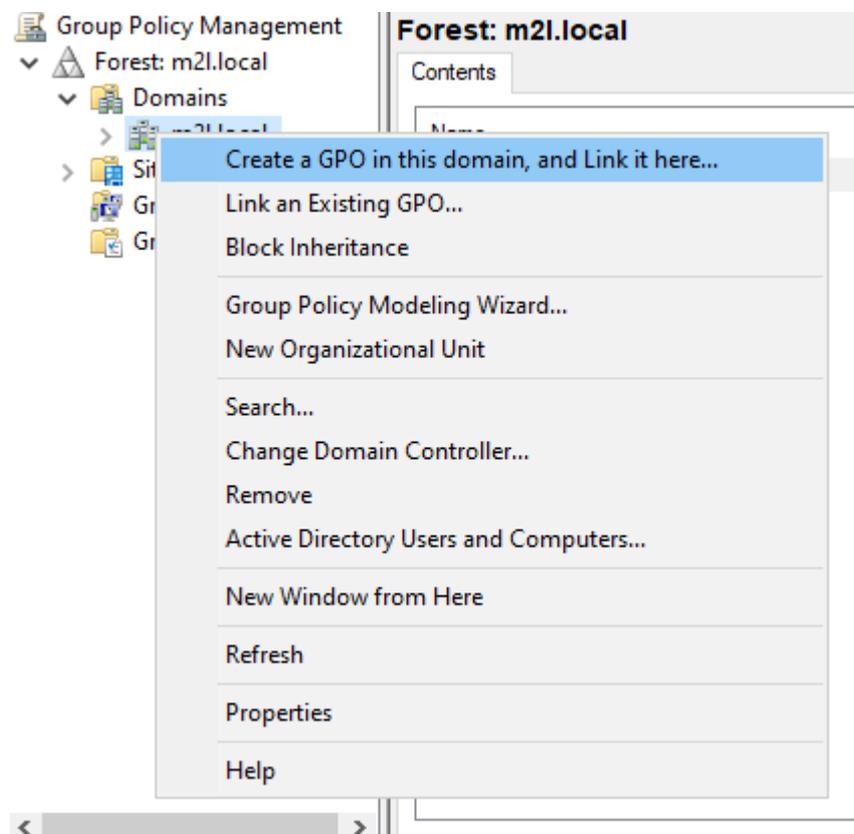
Création d'une gpo qui s'applique uniquement a un groupe de sécurité.

Création d'un nouvel objet GPO

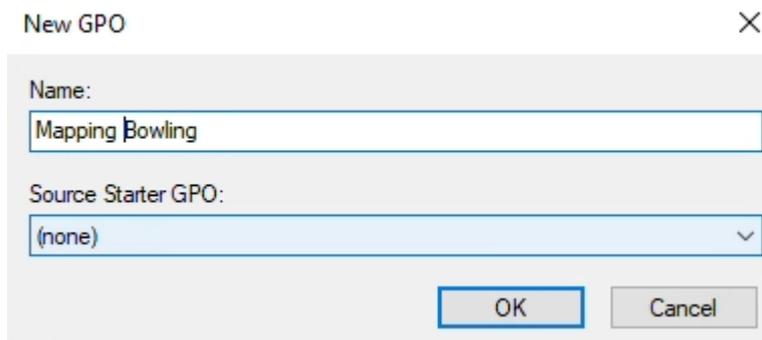
Allez dans l'onglet "Gestion de stratégie de groupe" en haut droite du gestionnaire de serveur dans outil



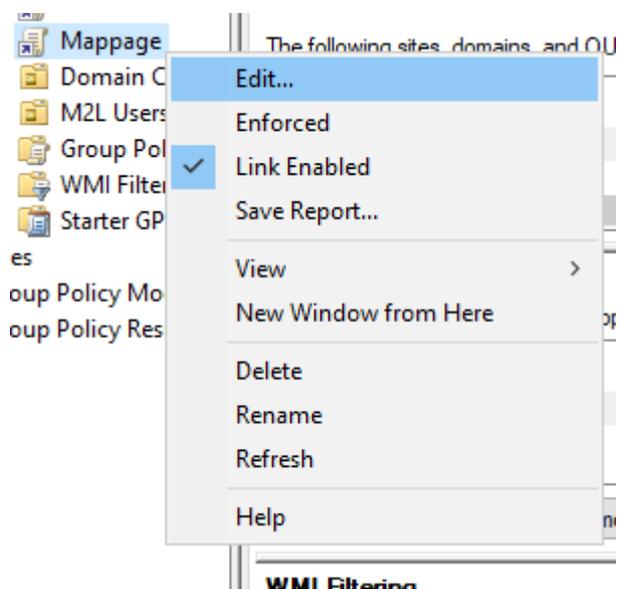
Créer une nouvelle GPOFaites un clic droit sur le domaine, puis sélectionnez "Create a GPO in this domain, and Link it here..." pour créer et lier une stratégie de groupe.



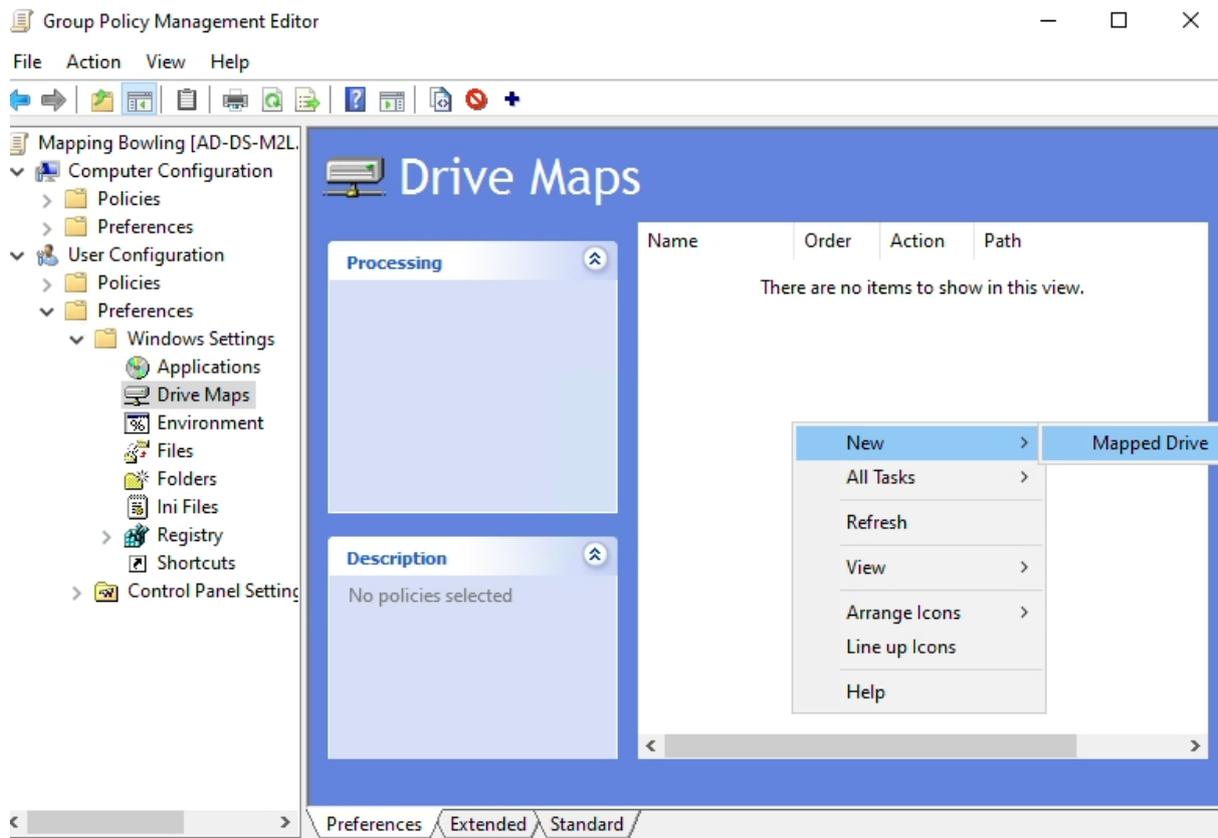
Choisir le nom de cette dernière



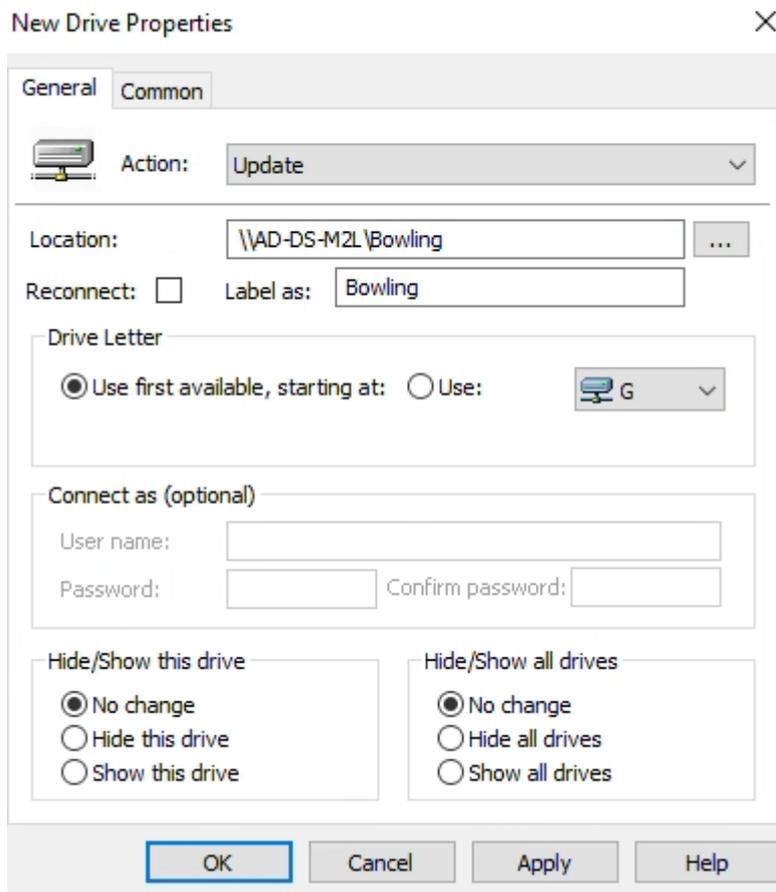
Faites un clic droit sur la GPO souhaitée puis sélectionnez "**Edit...**" pour modifier sa configuration.



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 :

Security Filtering

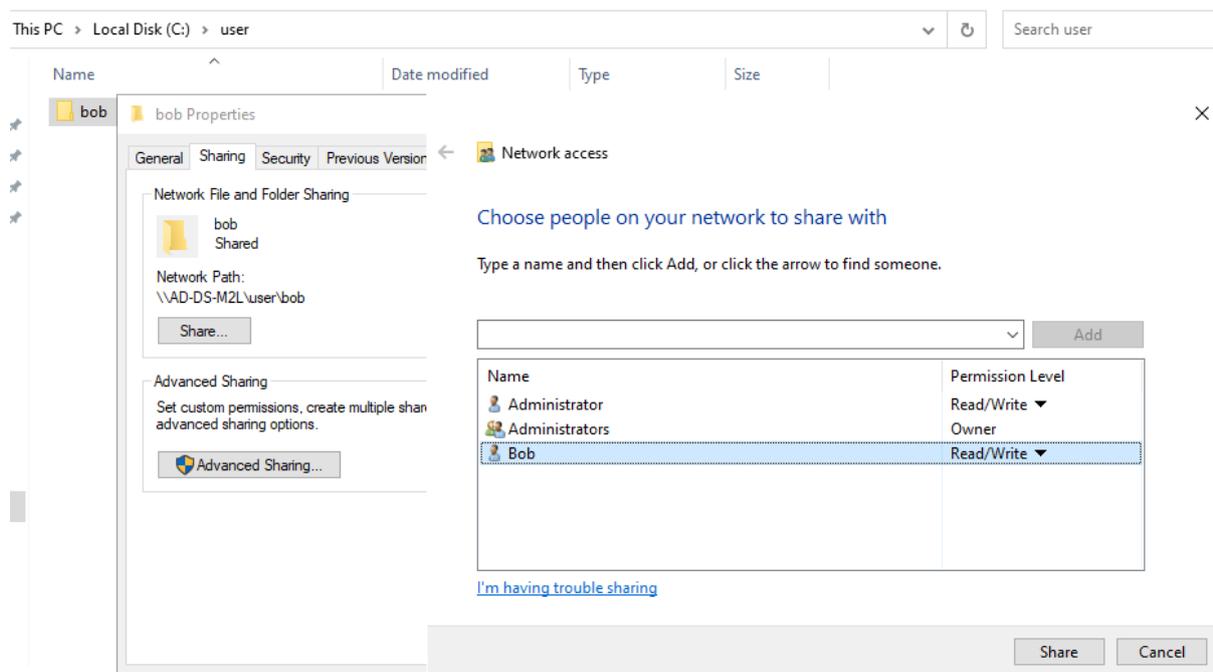
The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users
Bowling (M2L\Bowling)

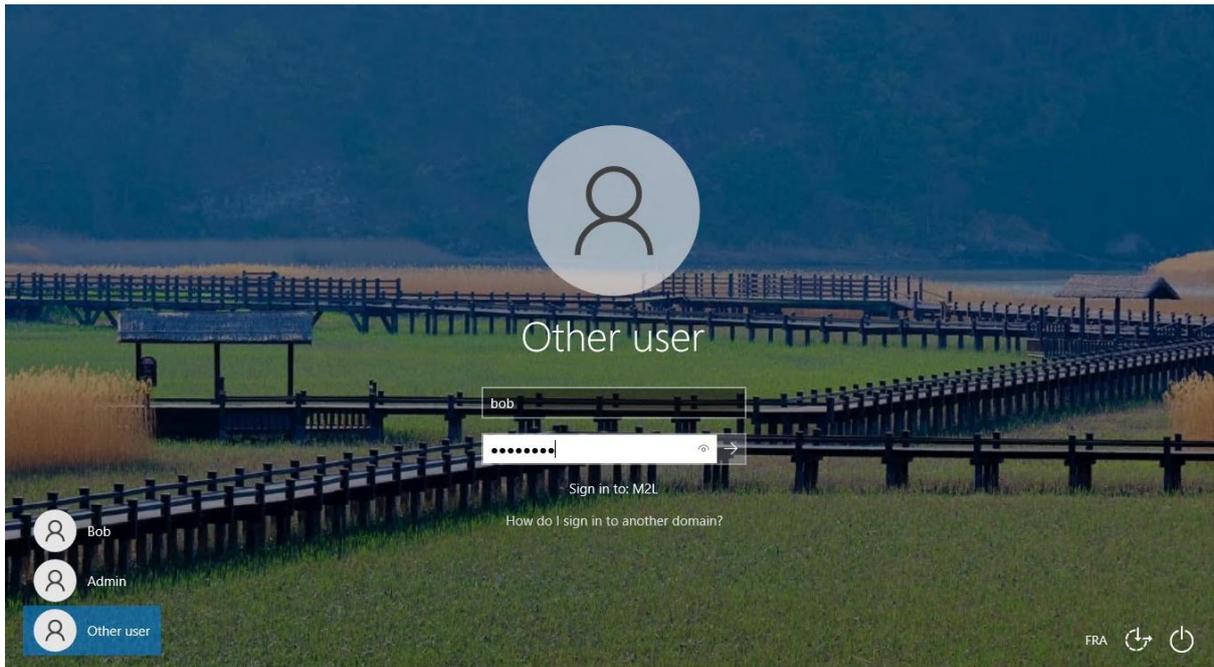
Buttons: Add... Remove Properties

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 vérifier 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

