PROJET E5 BTS SIO SISR :

INFRASTRUCTURE RÉSEAU NOTATECH

Documentation technique

REDOULES CLÉMENT

Contexte :

Dans le cadre de mon projet de BTS SIO SISR, j'ai conçu l'infrastructure réseau d'une entreprise fictive, Notatech. L'objectif était de créer un environnement sécurisé et performant, incluant un serveur Windows pour la gestion centralisée des utilisateurs (Active Directory, DNS, DHCP) et un pare-feu pfSense avec Suricata pour la sécurité réseau. Cette infrastructure permet une protection avancée grâce à la détection et la prévention des intrusions (IDS/IPS), garantissant ainsi la sécurité des données et des communications de l'entreprise.

Sommaire :

Configuration rôle AD DS

13-16

Création d'une nouvelle forêt AD

17-19

Sélection des rôles d'accès à distance :

18-24

Création de GPO :

25-29

Création des utilisateurs et des unités d'organisation :

30-32

Test sur une machine cliente :

33-44

Configuration du Serveur AD en redondance :

45-63

Activation et vérification de la redondance :

64-67

Création du pare feu PfSense :

68-77

Configuration DHCP et internet :

78-81

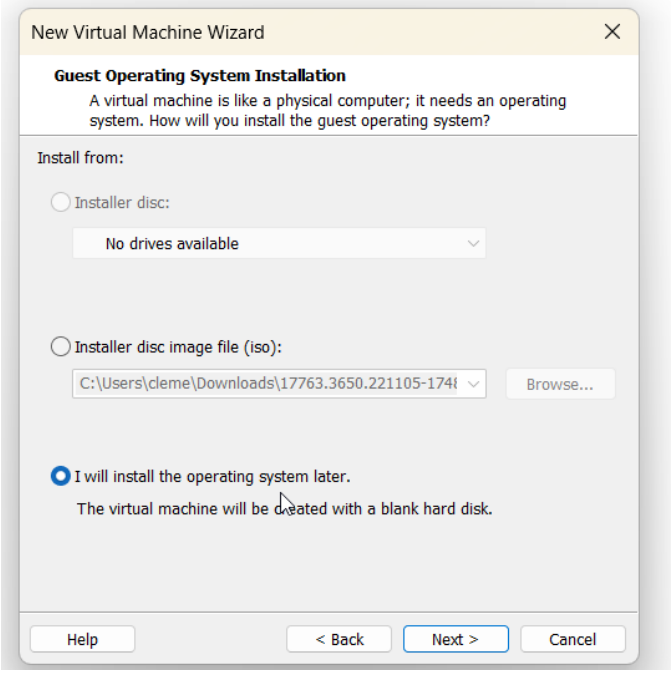
Configuration d'un IPS/IDS :

82-86

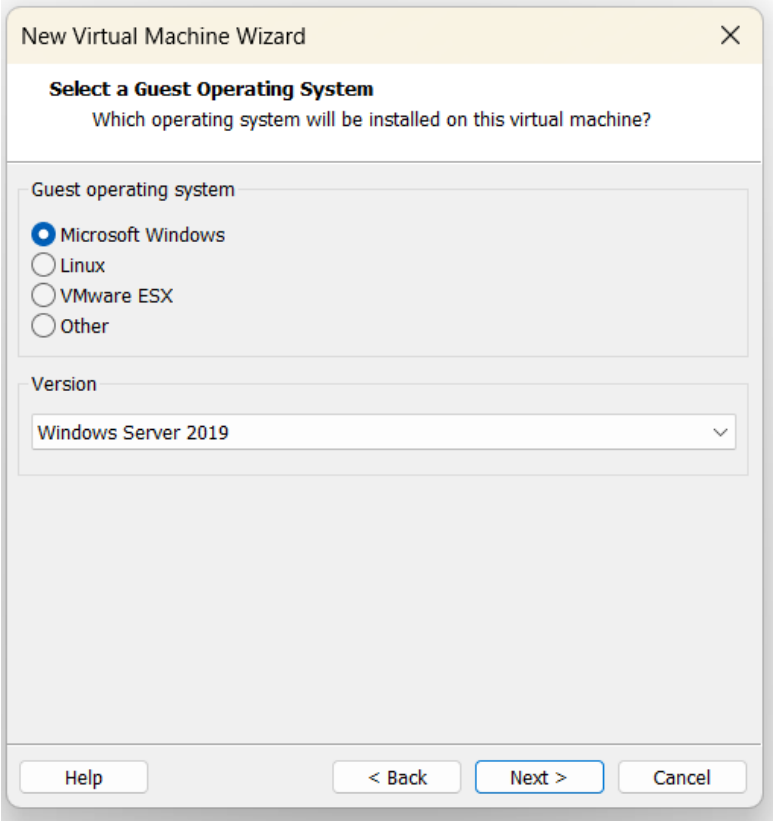
Création du serveur AD DS :

Je commence par cliquer sur « créer une machine virtuelle sur le logiciel VMWare Workstation, et choisis une configuration custom

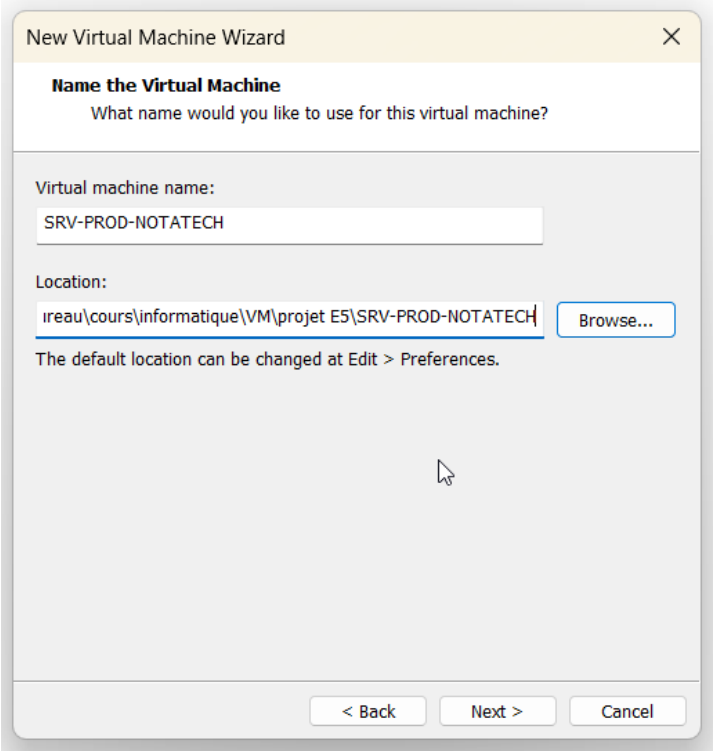
Ensuite je choisis d'installer l'iso de Windows server plus tard pour éviter d'avoir des soucis avec le compte microsoft



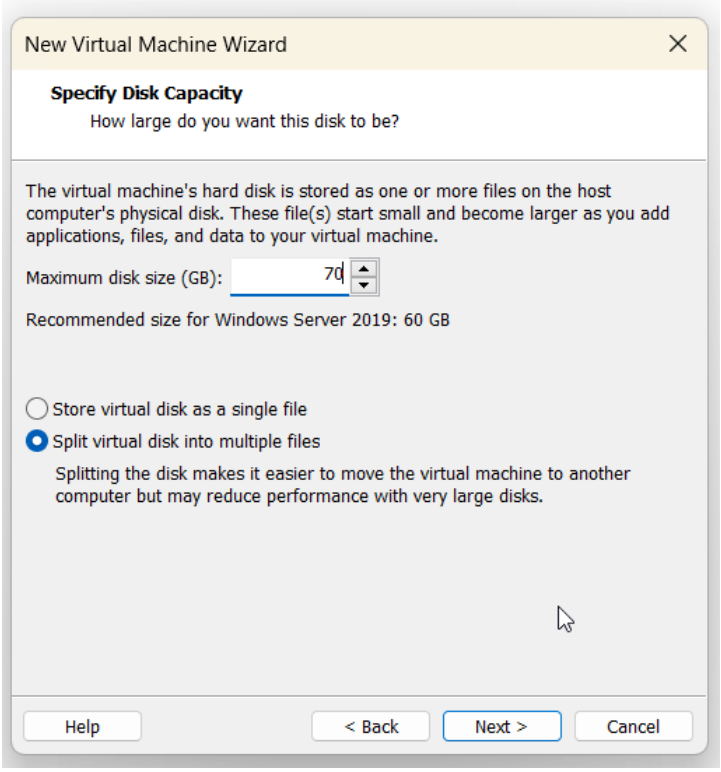
Ensuite je sélectionne « Microsoft Windows » comme système d'exploitation et sélectionne windows server 2019 pour la version



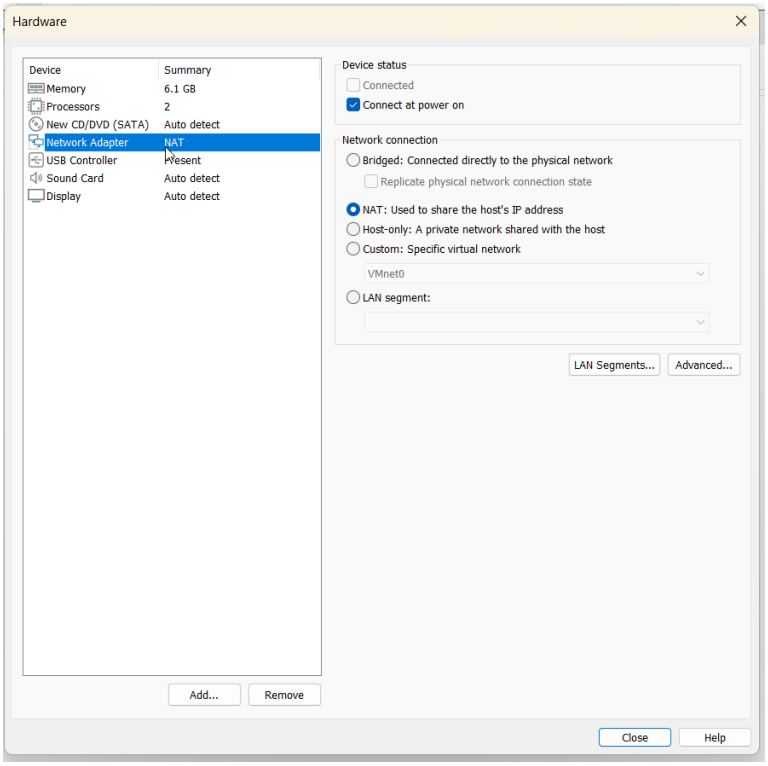
Je nomme ma machine virtuelle « SRV-PROD-NOTATECH » pour « serveur de production notatech »



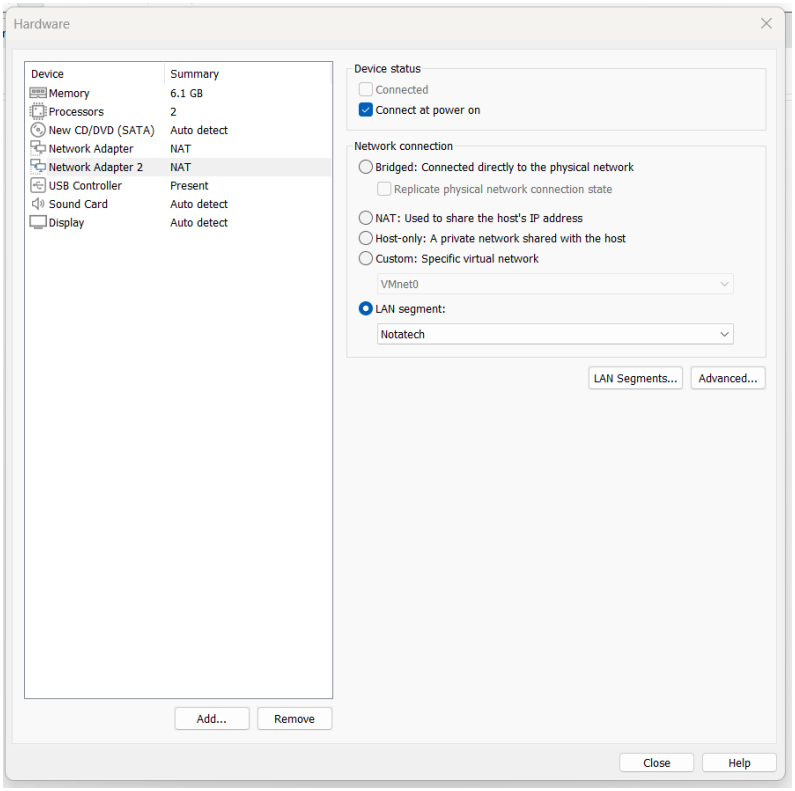
Je choisis ensuite de mettre 70GB d'espace disque pour ne pas avoir de soucis au niveau de l'espace de stockage suffisant



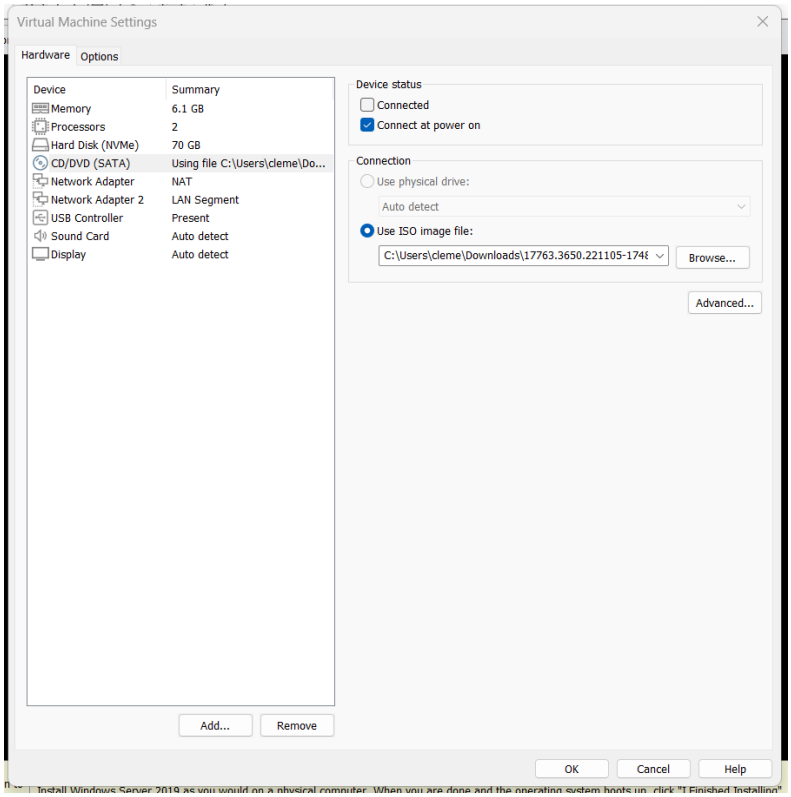
Ensuite je me rend dans les paramètres de la VM et met sa première carte réseau en NAT, pour avoir l'accès a internet



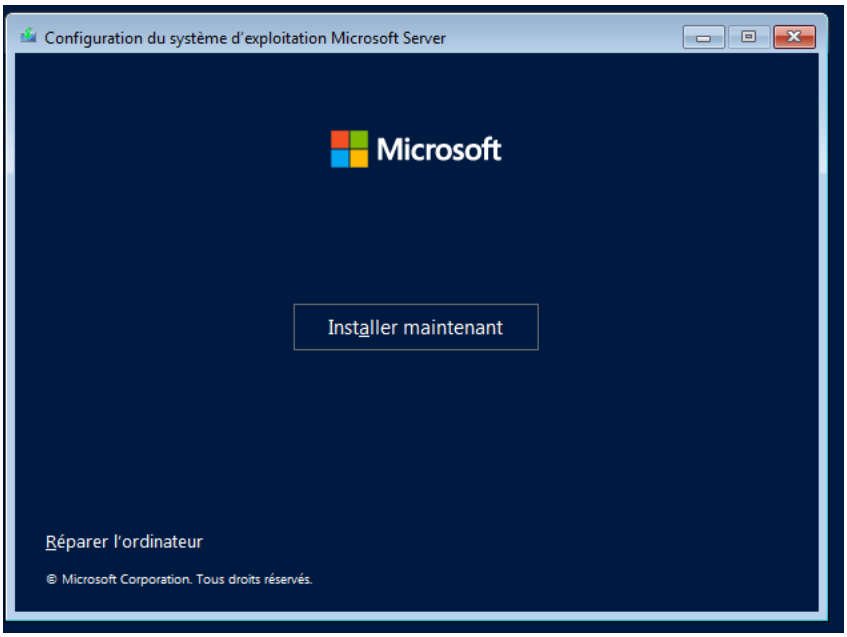
Et je rajoute ensuite une deuxième carte réseau a ma machine, cette fois ci sur un LAN segment appelé « notatech » créé spécialement pour lier les machines de l'infrastructure réseau facilement



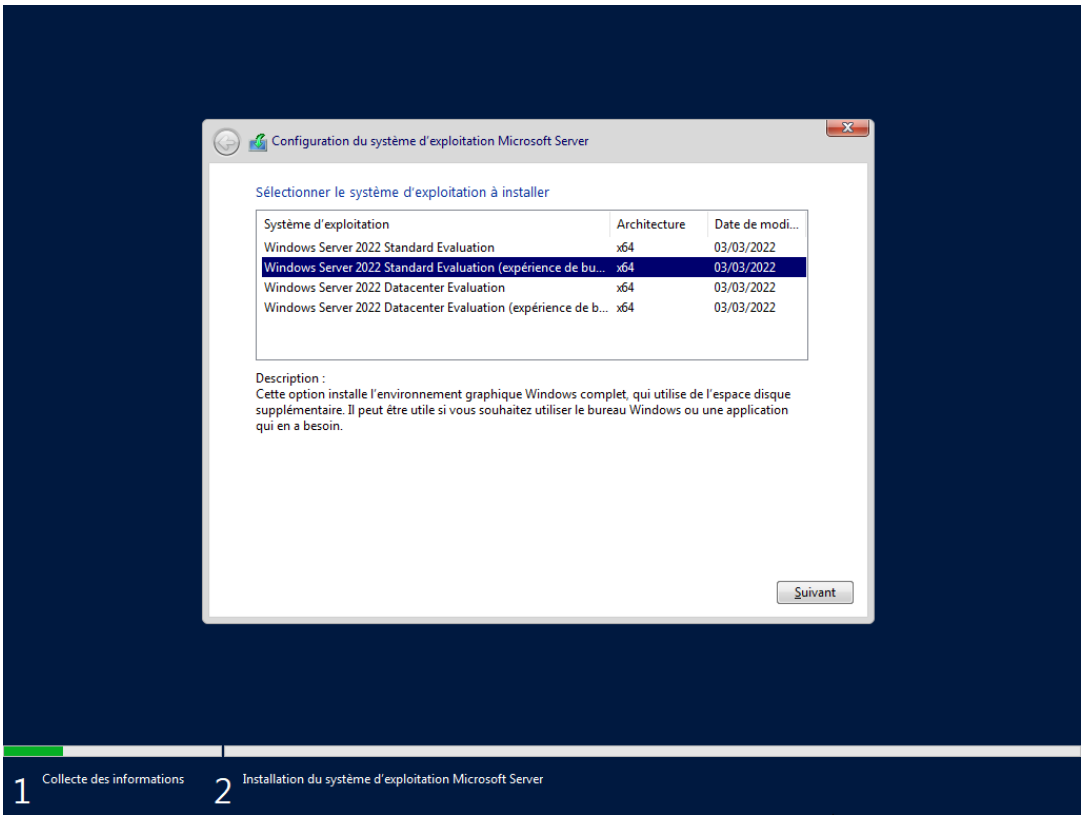
Ce qui nous donne donc finalement 2 cartes réseaux, une en NAT pour l'accès à internet et une en LAN segment pour facilement relier les prochaines machines



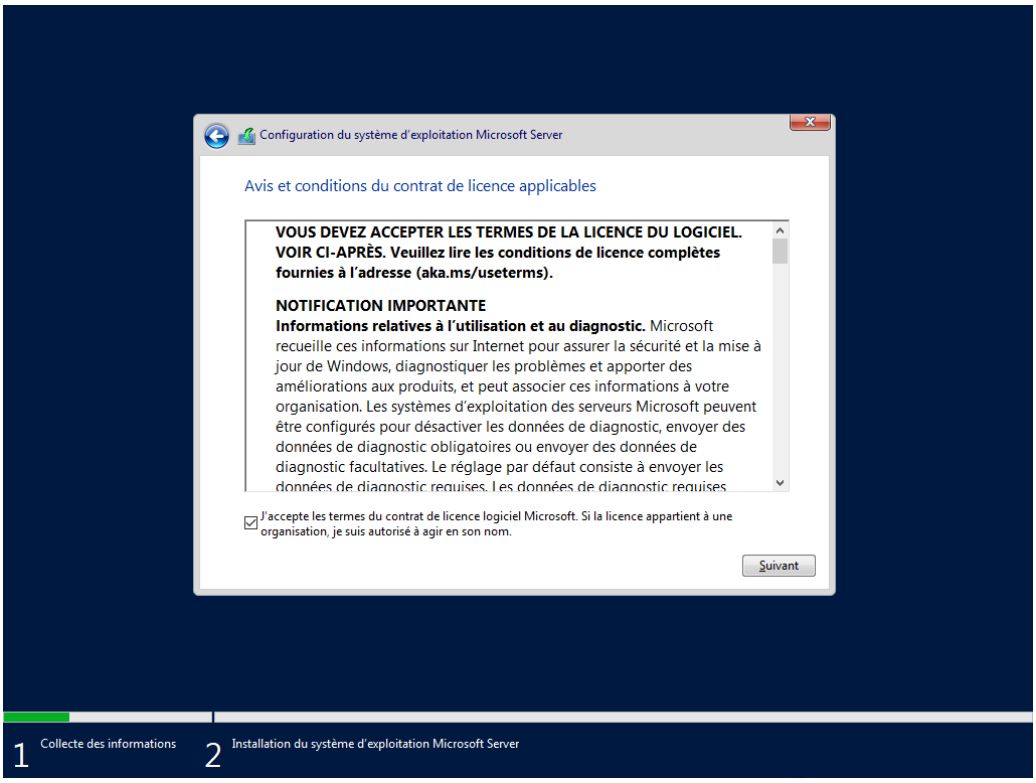
Ensuite je démarre donc ma machine virtuelle Windows server, j'arrive sur cette page je clique sur « installer maintenant »



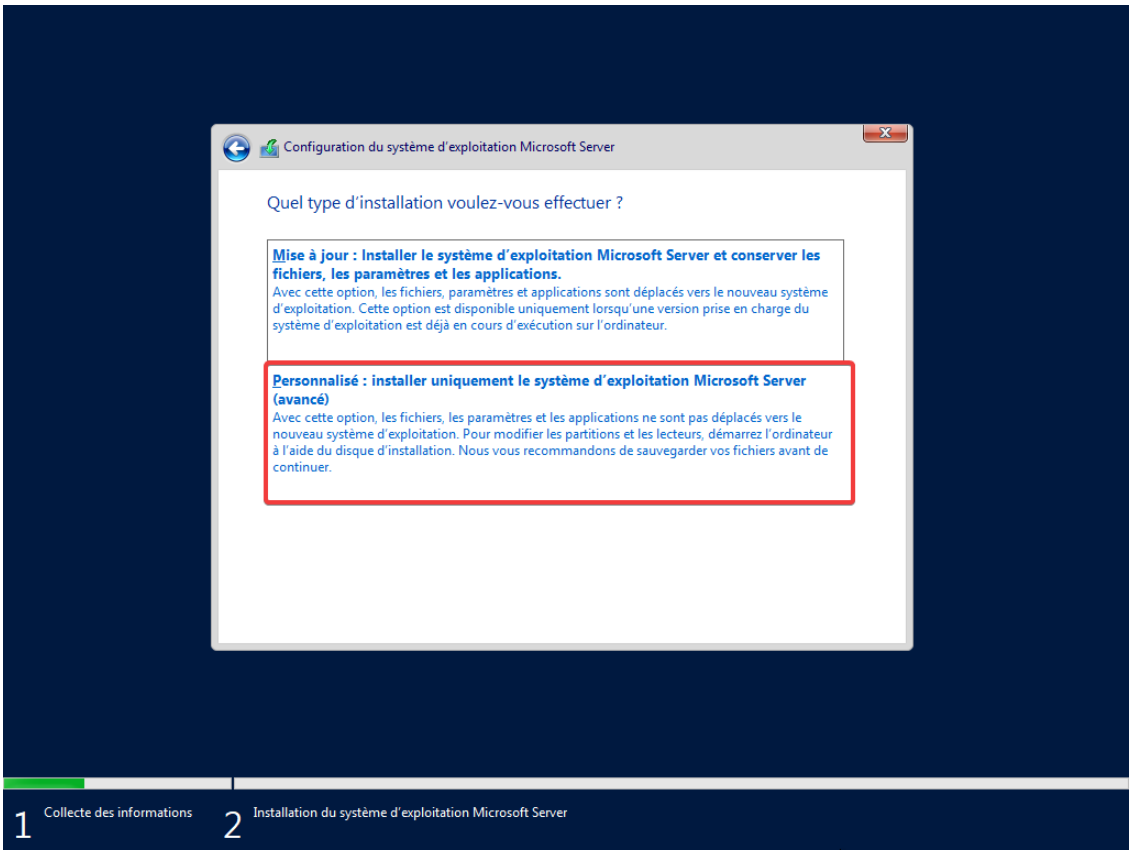
Je sélectionne ensuite la 2ème option « Windows server 2022 standard Evaluation (expérience de bureau)



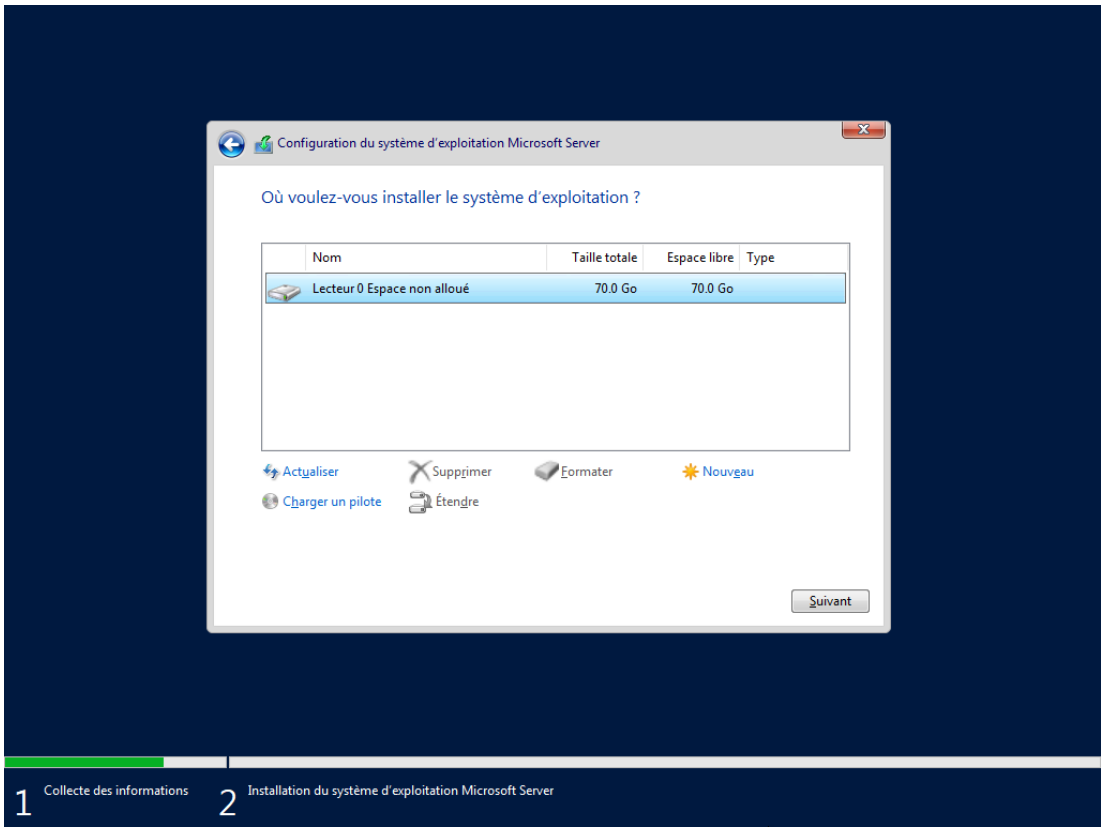
Ensuite les conditions d'utilisation apparaissent je coche donc « j'accepte les termes du contrat » et clique sur suivant



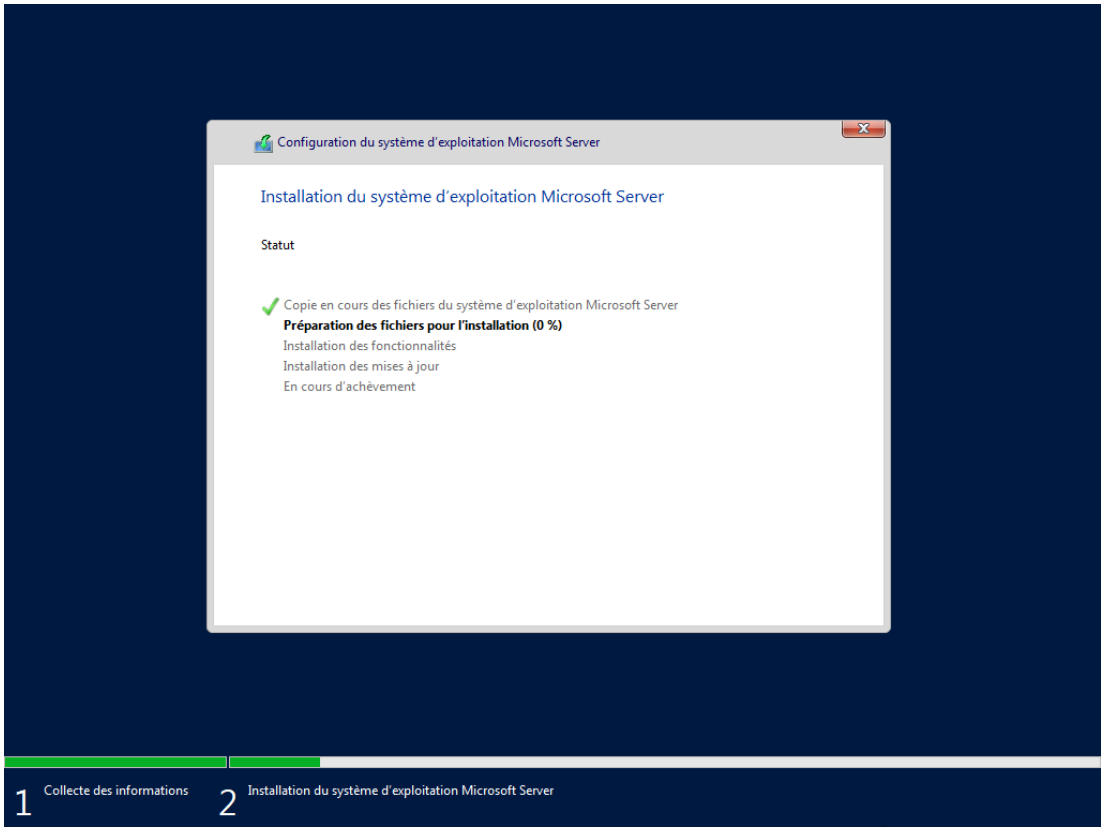
Pour le type d'installation je sélectionne **« personnalisé »** pour pouvoir sélectionner mon disque



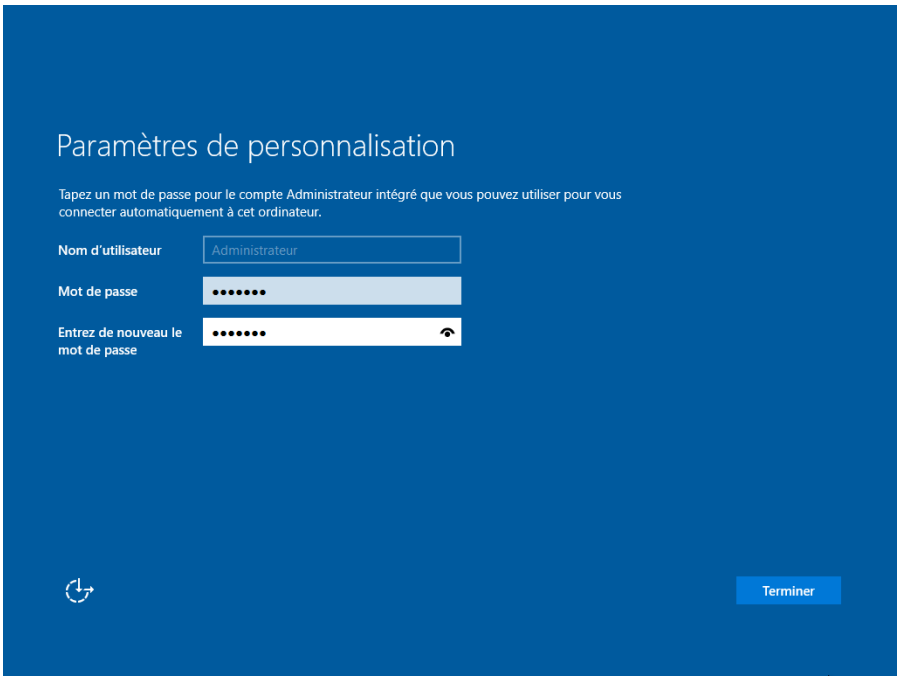
Je sélectionne donc mon disque et clique sur suivant



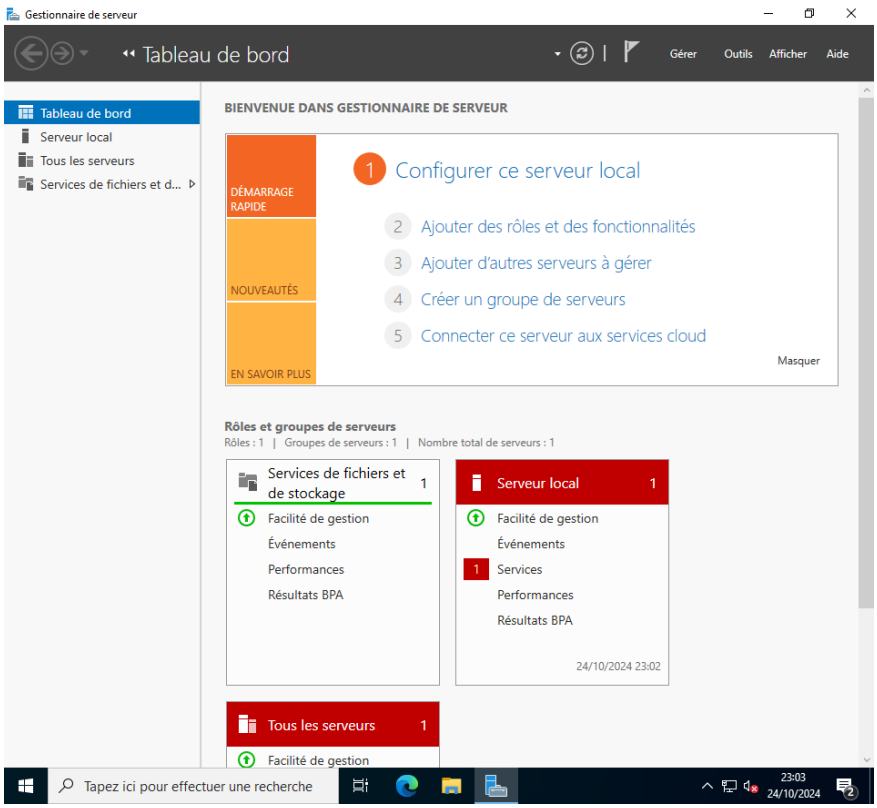
Et l'installation va finalement se lancer



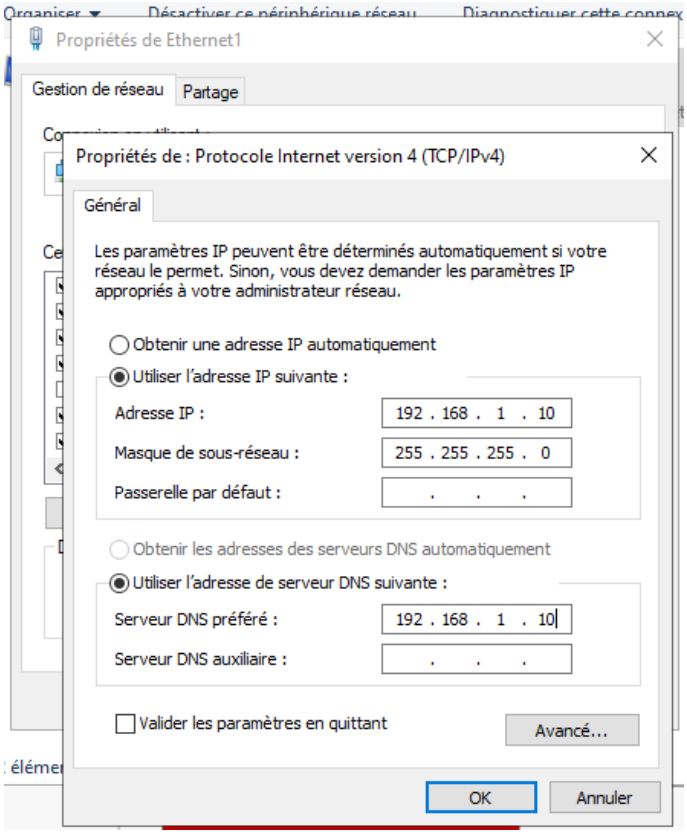
Une fois installé cette page apparaitra, nous demandant de renseigner les identifiants pour le compte administrateur de notre Windows server, je mets donc le mot de passe et clique sur « terminer »



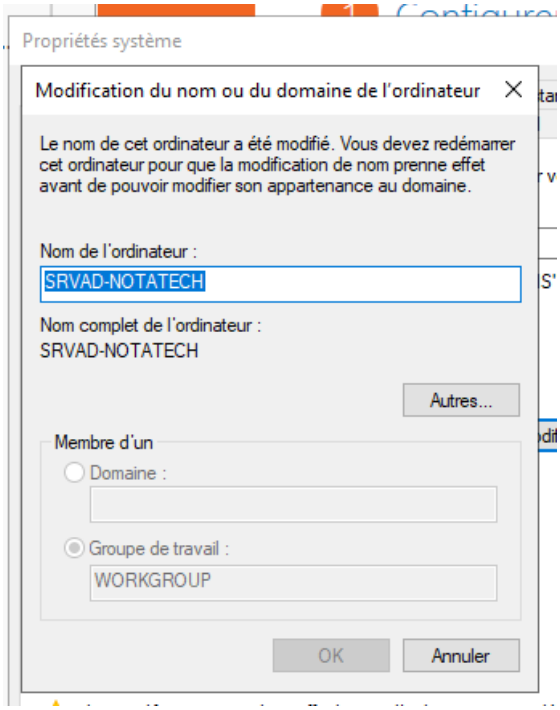
Et enfin cette page qui est le Server manager s'ouvrira et on pourra configurer notre serveur



Tout d’abord je commence par configurer une IP fixe pour mon serveur, pour nous faciliter la suite de la configuration

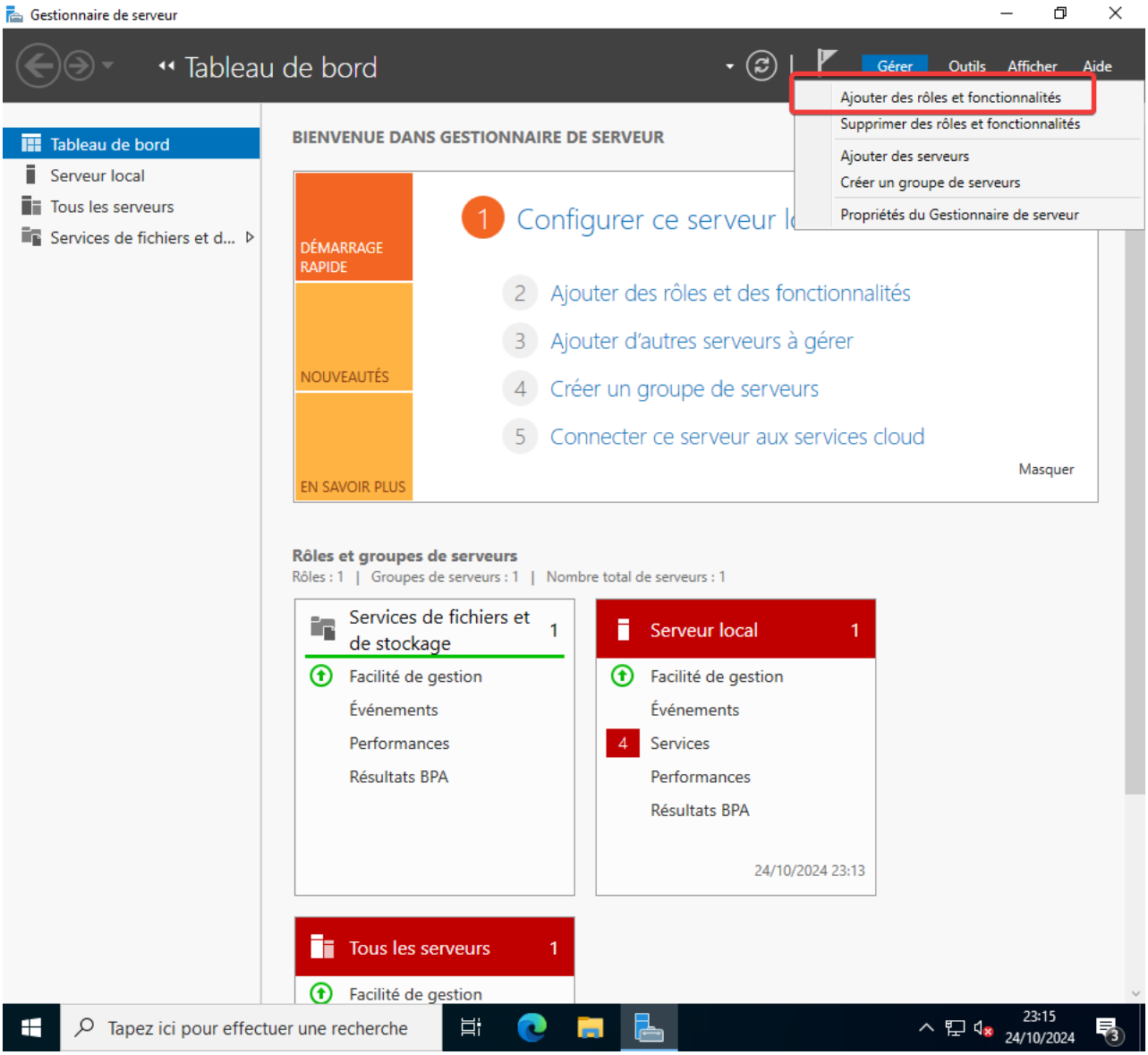


Et ensuite je renomme ma machine en « SRVAD-NOTATECH » pour qu’elle soit identifiable facilement

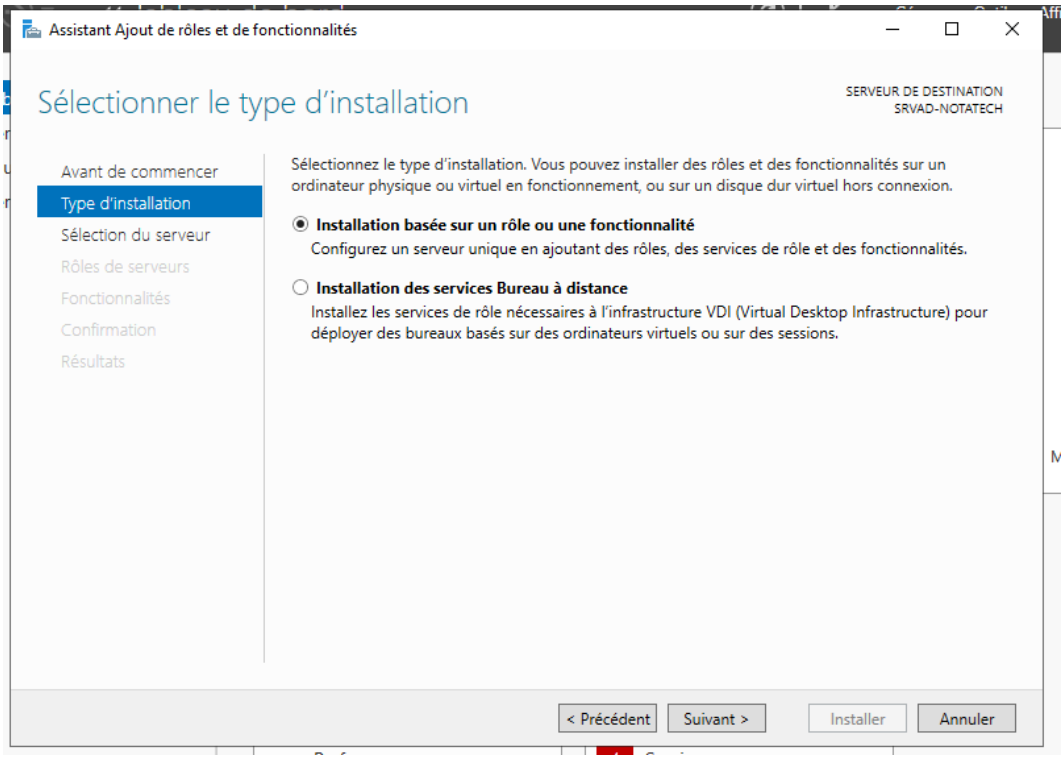


Configuration rôle AD DS

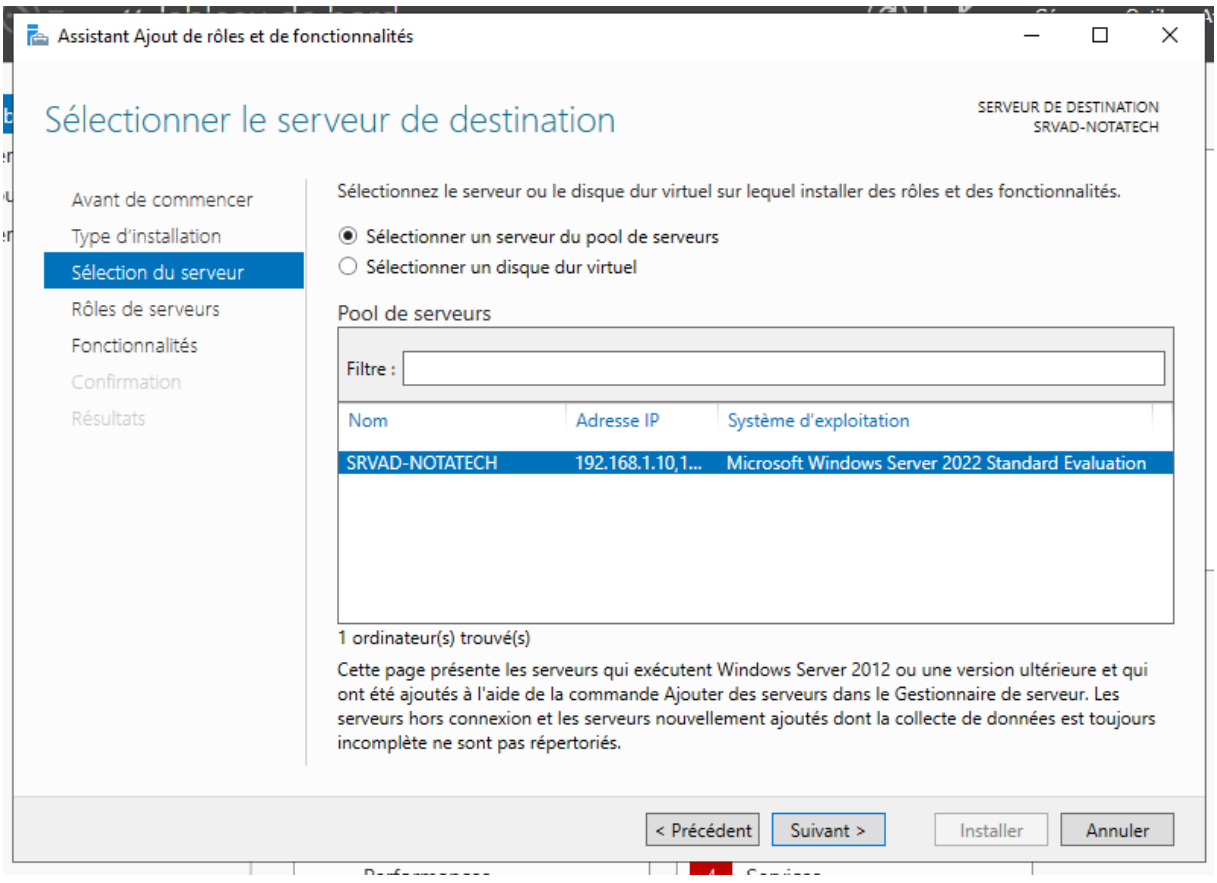
Tout d'abord pour l'ajout de ce rôle, je me rends dans « gérer » sur le tableau de bord du server manager et je clique sur « ajouter des rôles et fonctionnalités »



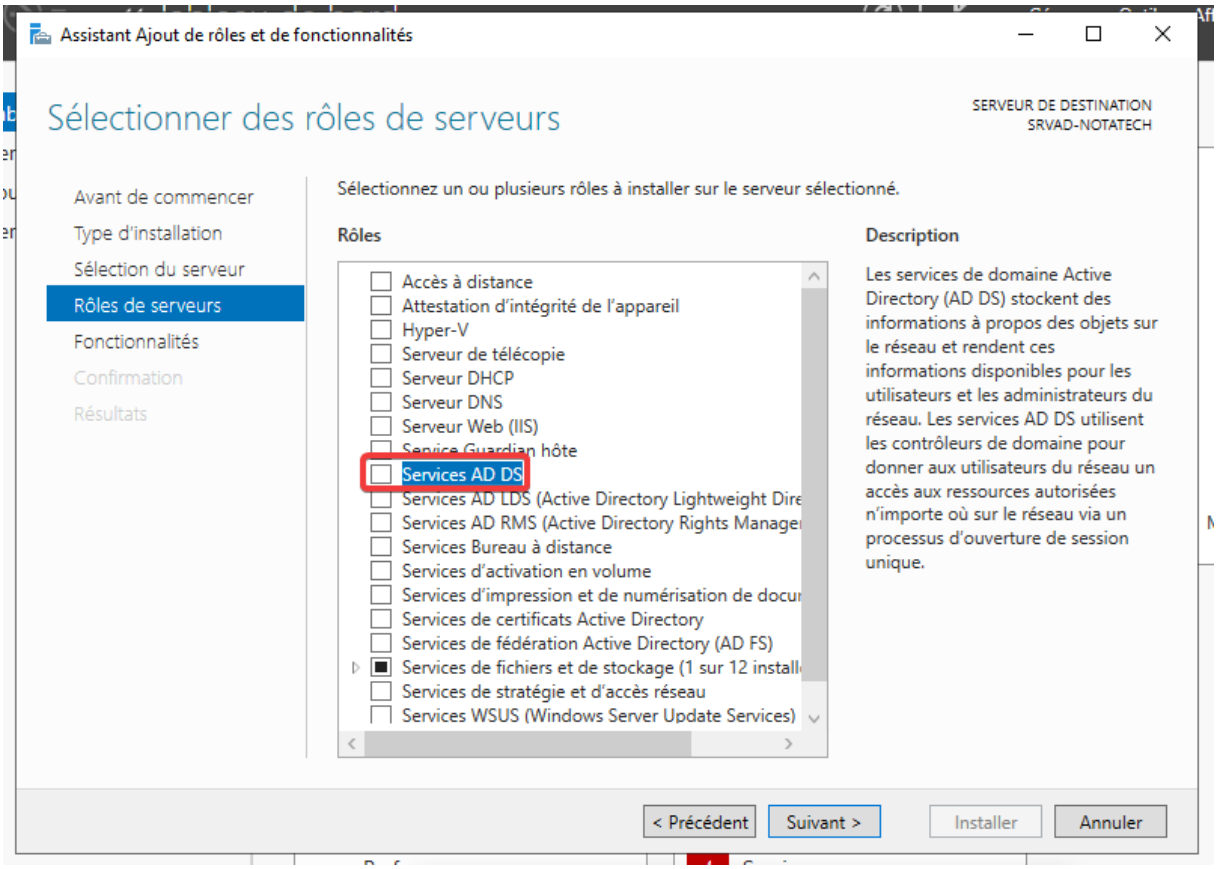
Ensuite arrivé sur cette page je clique sur « installation basée sur un rôle ou une fonctionnalité » et je clique sur suivant



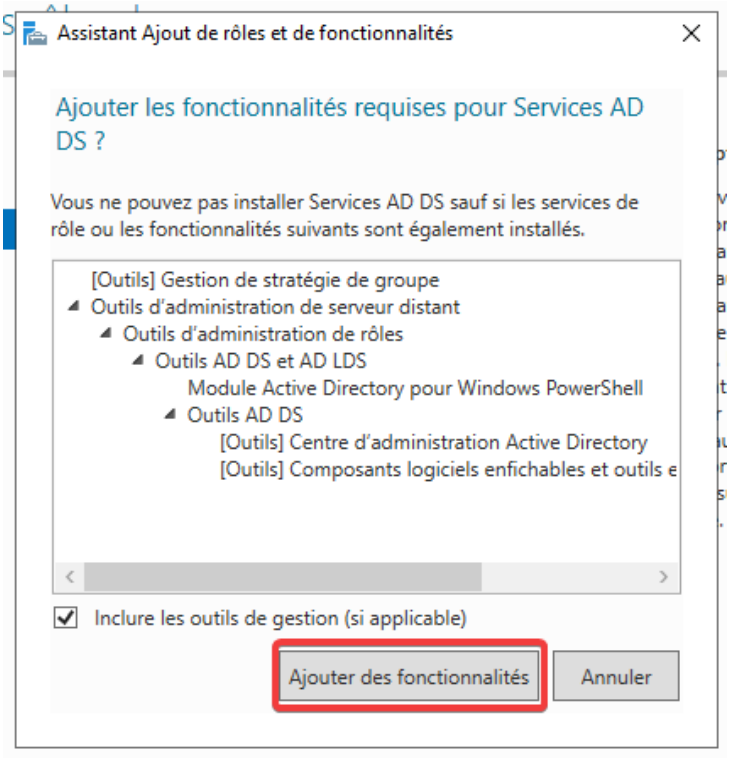
Ensuite pour la sélection du serveur je sélectionne mon serveur et clique sur suivant



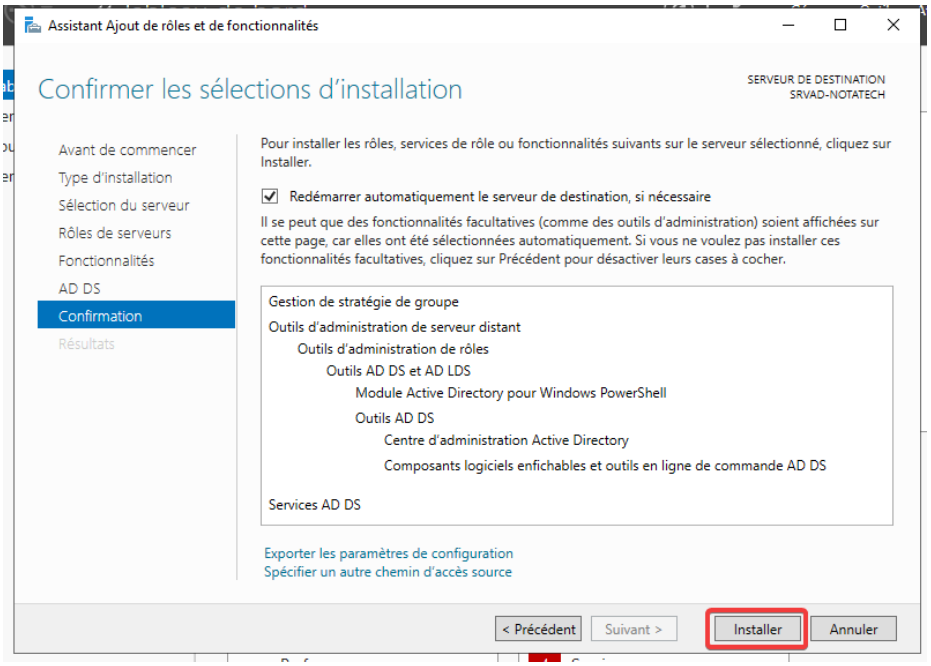
Pour les rôle de serveur je sélectionne « serveur AD DS »



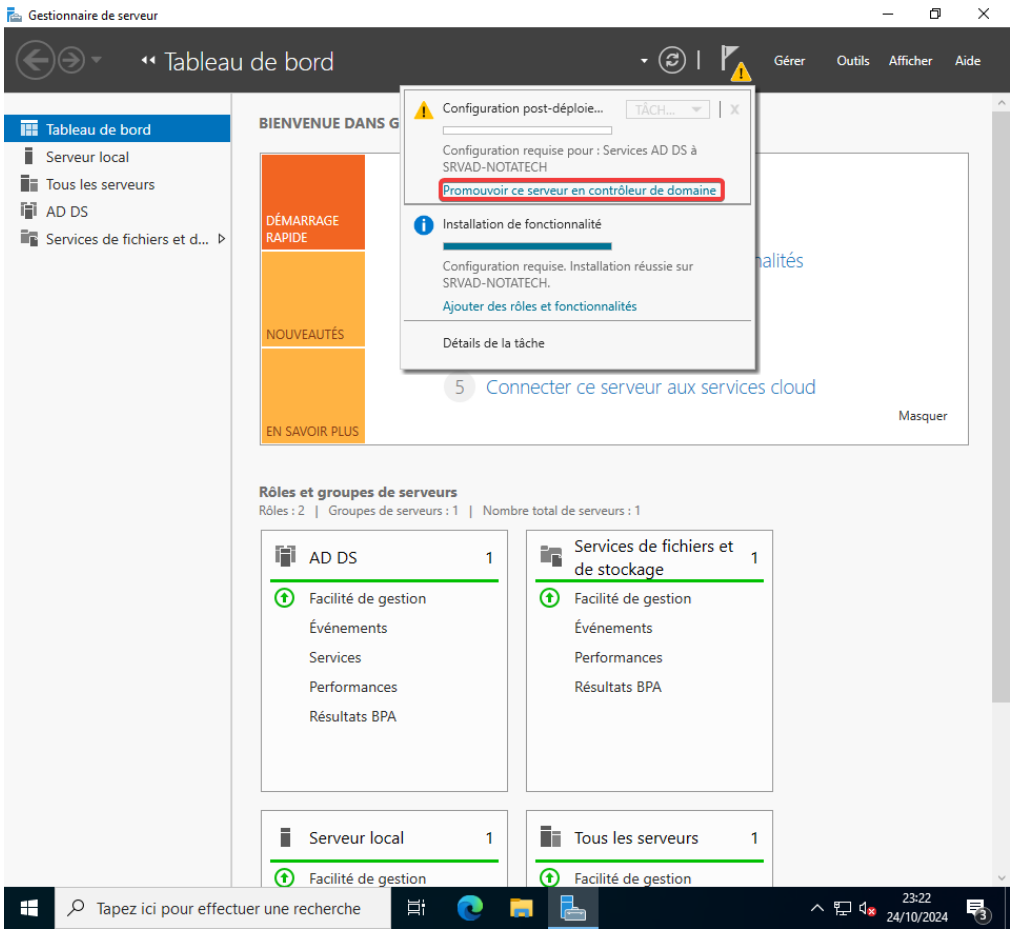
Cette page apparait je clique sur le bouton « ajouter des fonctionnalités » et je fais « suivant »



Ensuite pour ce qui est du reste je laisse les paramètres par défaut et je clique finalement sur « installer »

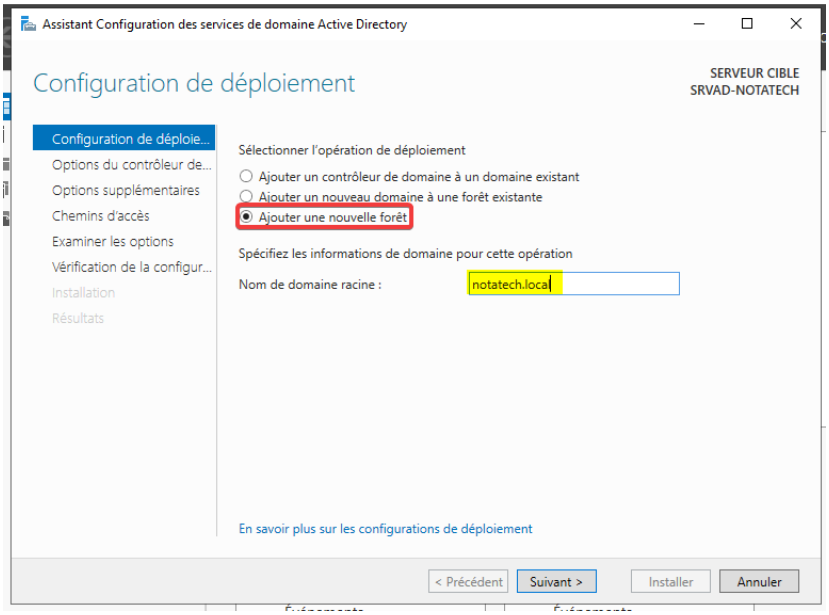


Ensuite une fois installé je clique sur le drapeau et je clique sur promouvoir ce serveur en contrôleur de domaine

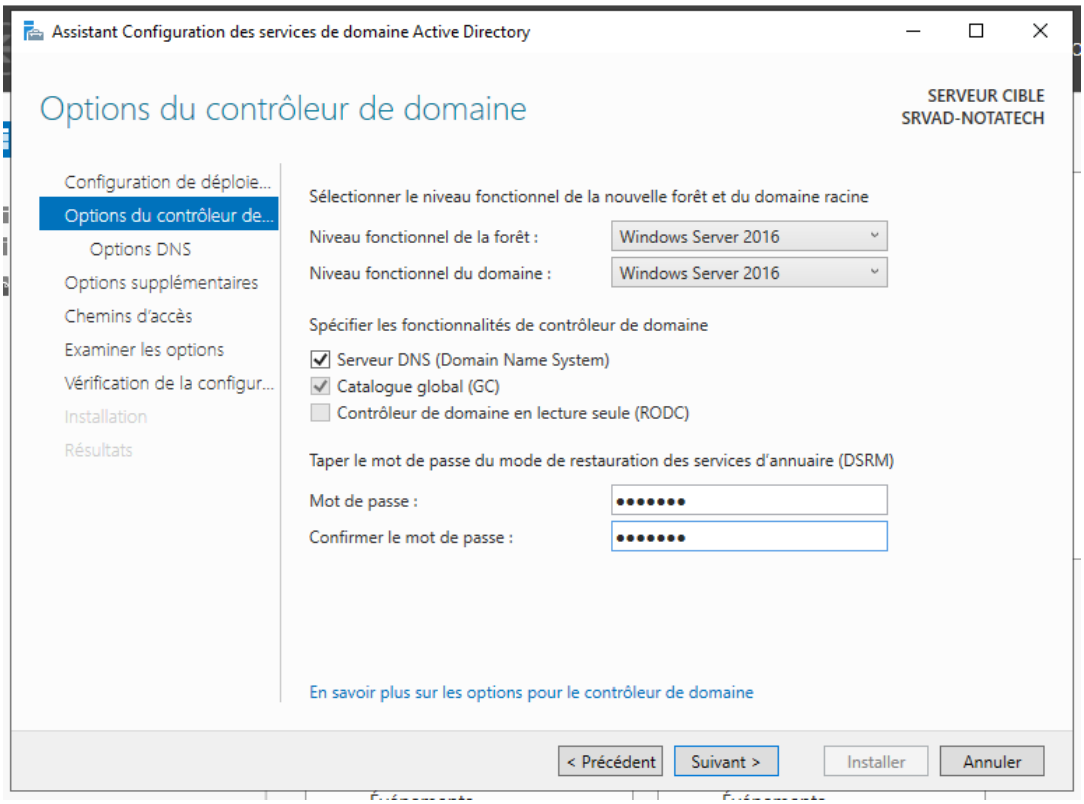


Création d'une nouvelle forêt AD

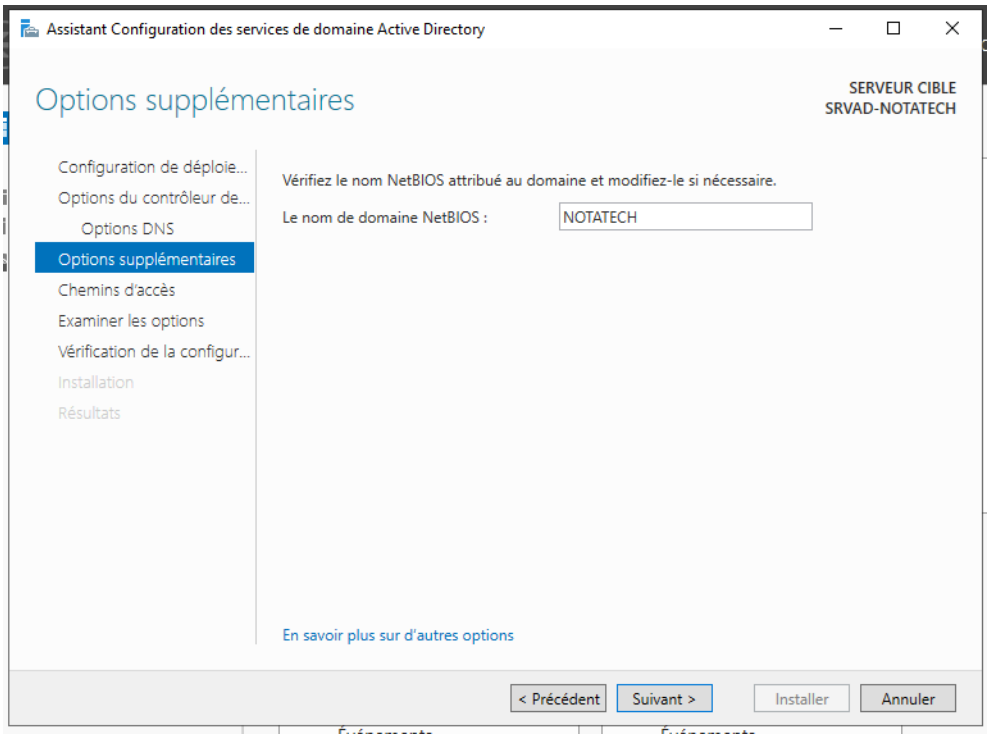
Je commence ici à créer une infrastructure Active Directory (AD) en définissant une nouvelle forêt avec le domaine racine notatech.local. C'est une étape essentielle pour centraliser la gestion des utilisateurs, des groupes, et des politiques réseau.



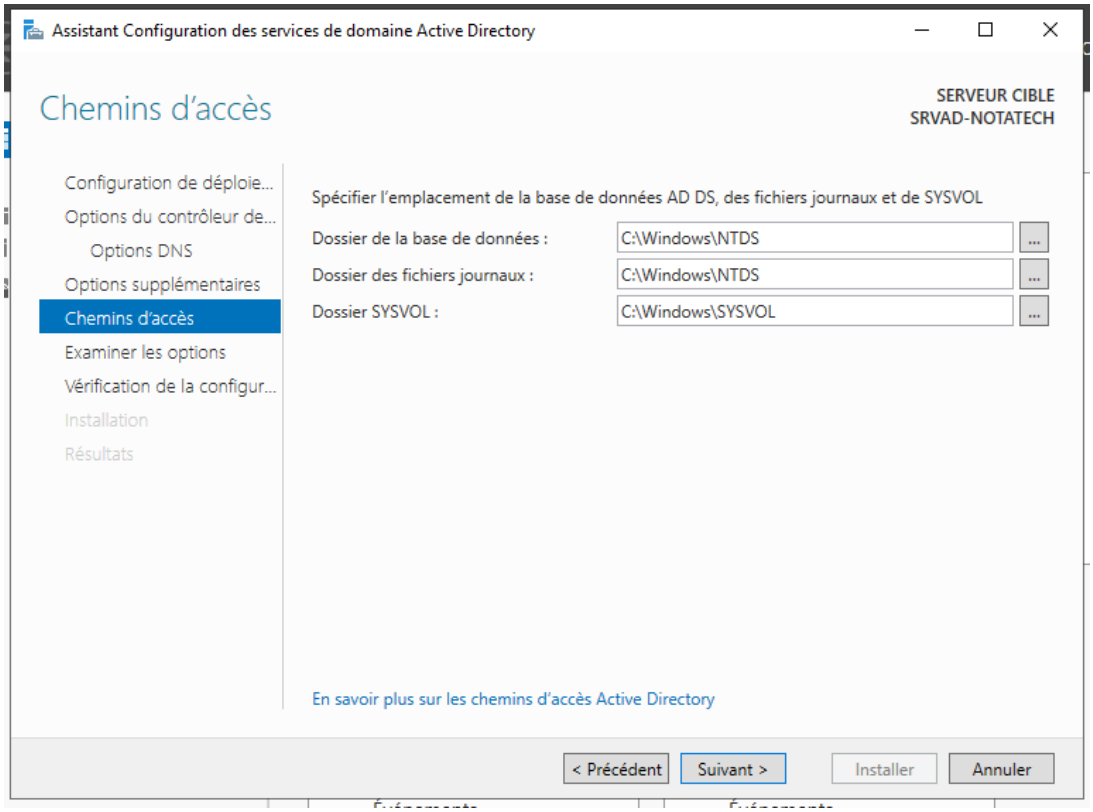
J'ai choisi le niveau fonctionnel Windows Server 2016 pour garantir une compatibilité avec les fonctionnalités nécessaires. Le rôle DNS et le Catalogue Global sont activés pour permettre une gestion efficace des authentifications et des résolutions de noms dans le domaine.



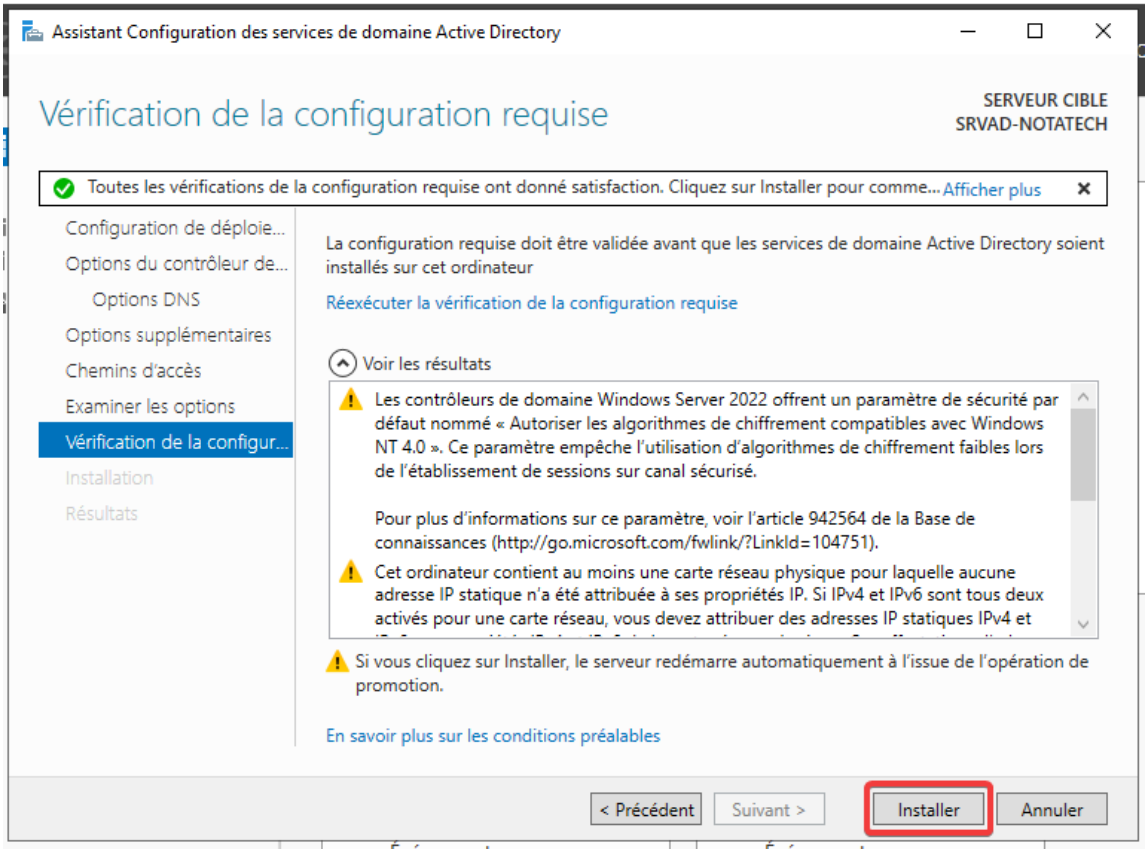
À cette étape, j'ai confirmé le nom NetBIOS NOTATECH pour simplifier les identifications réseau.



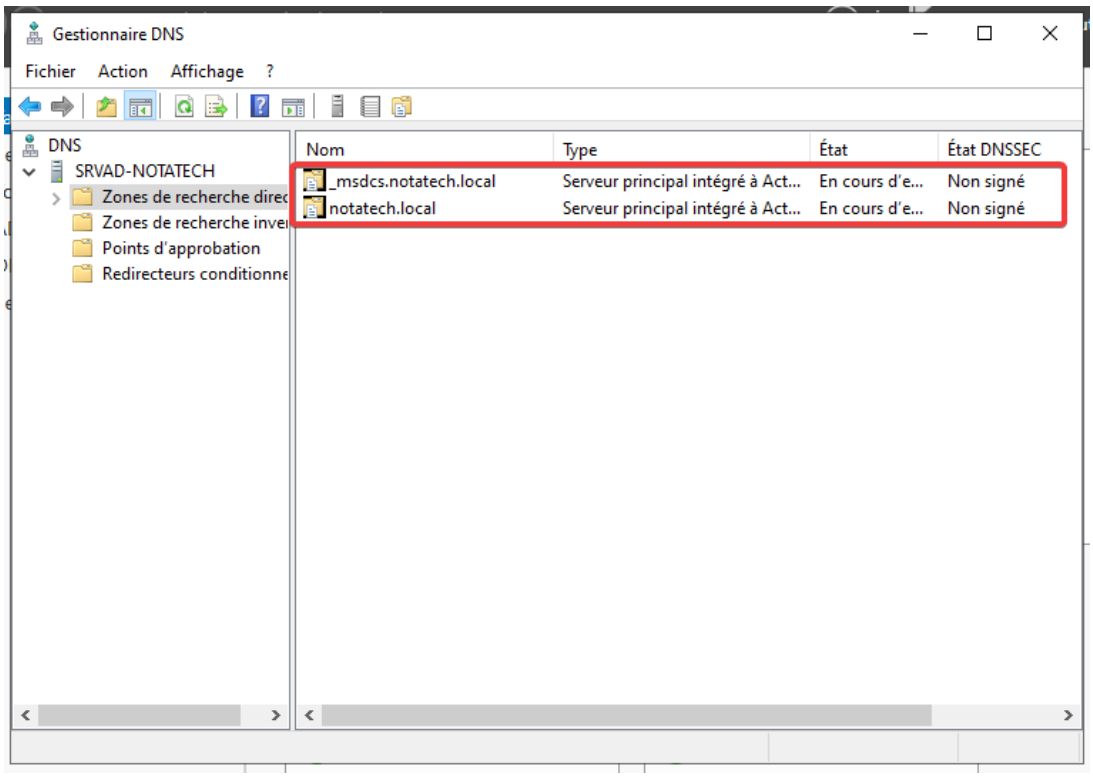
J'ai également validé les chemins d'accès par défaut pour les fichiers critiques de l'Active Directory.



Avant l'installation, j'ai vérifié que toutes les configurations étaient correctes. Cette étape garantit que le serveur est prêt à fonctionner comme contrôleur de domaine principal.

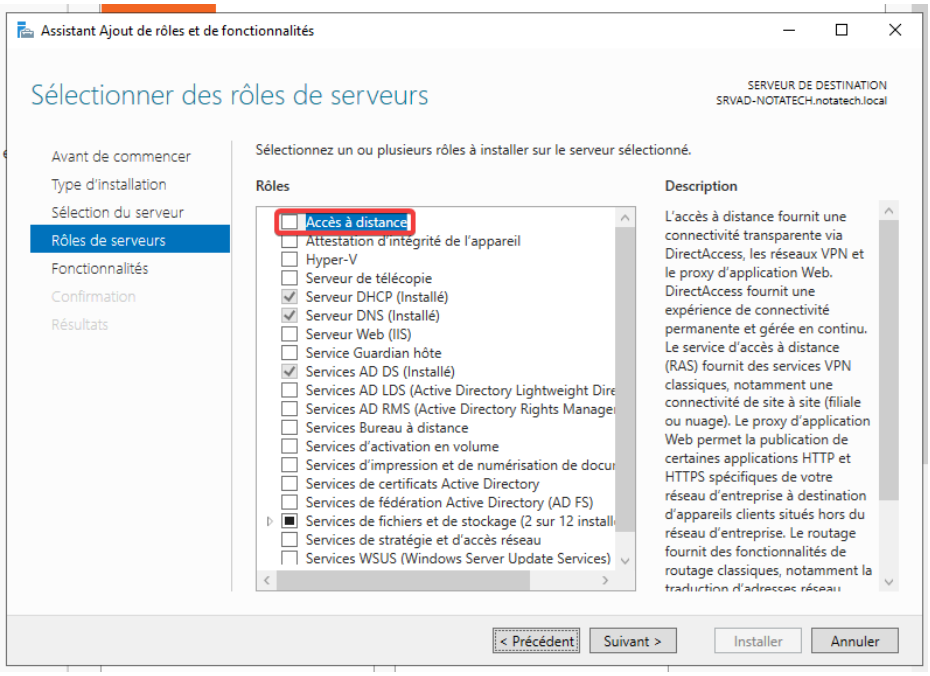


Je vérifie ensuite que les zones de recherches directes se sont bien crées

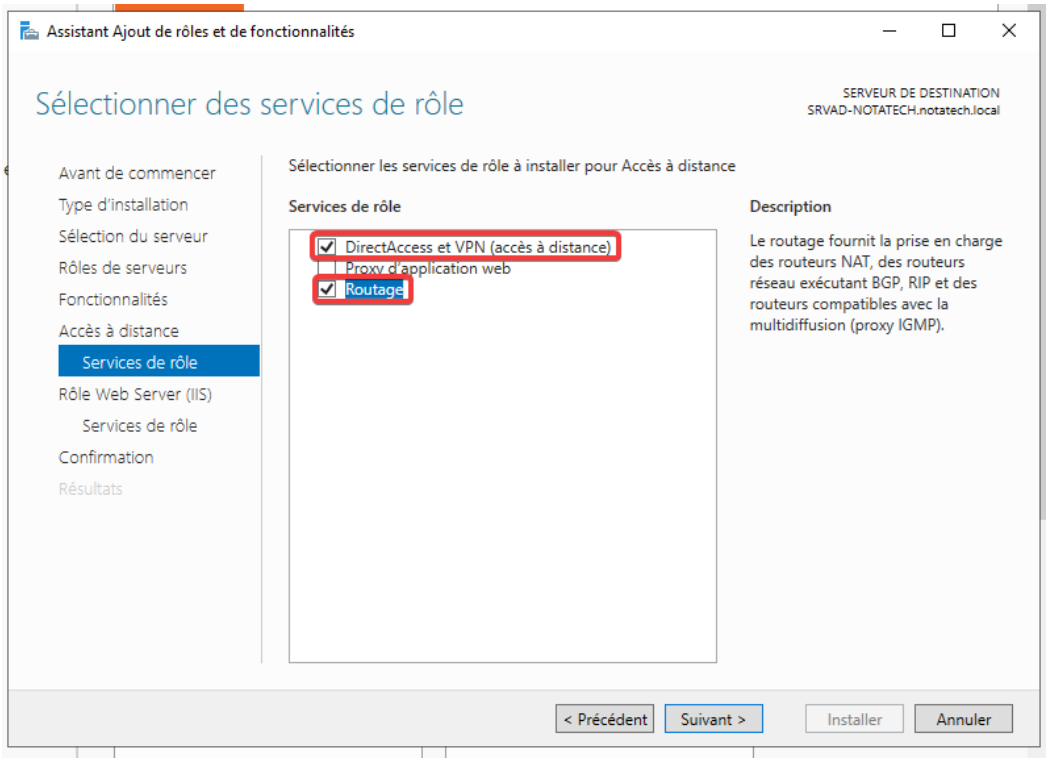


Sélection des rôles d'accès à distance :

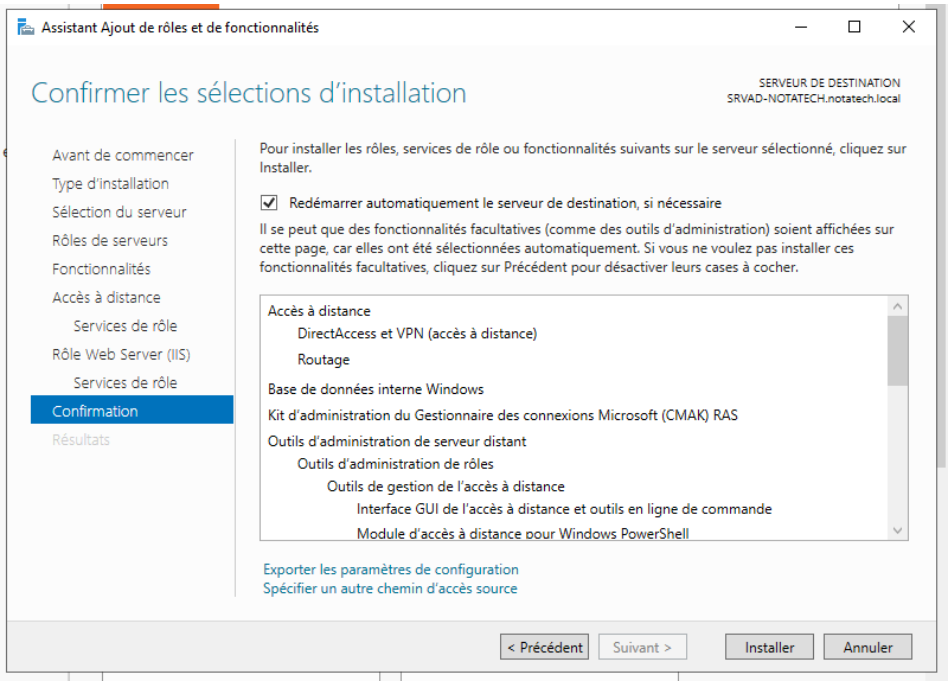
Pour permettre le routage et l'accès distant, j'ai ajouté les rôles « Accès à distance » par l'ajout de rôles et de fonctionnalités



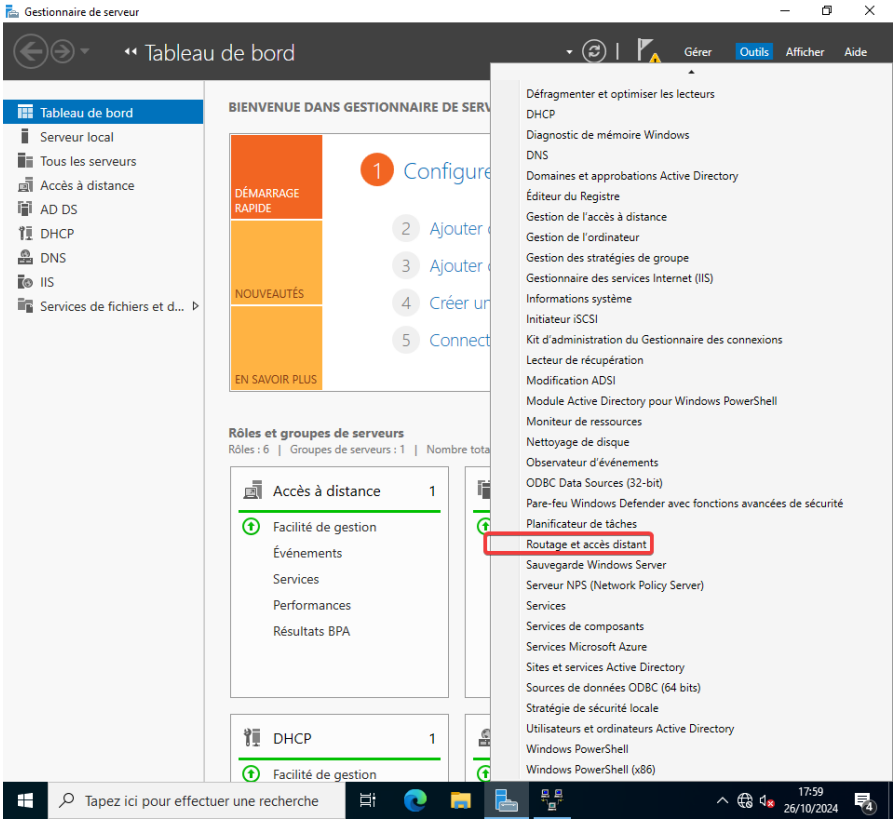
Ensuite je sélectionne direct Access et VPN (qui nous servira plus tard). Ces fonctionnalités assureront que les utilisateurs pourront se connecter au réseau de manière sécurisée.



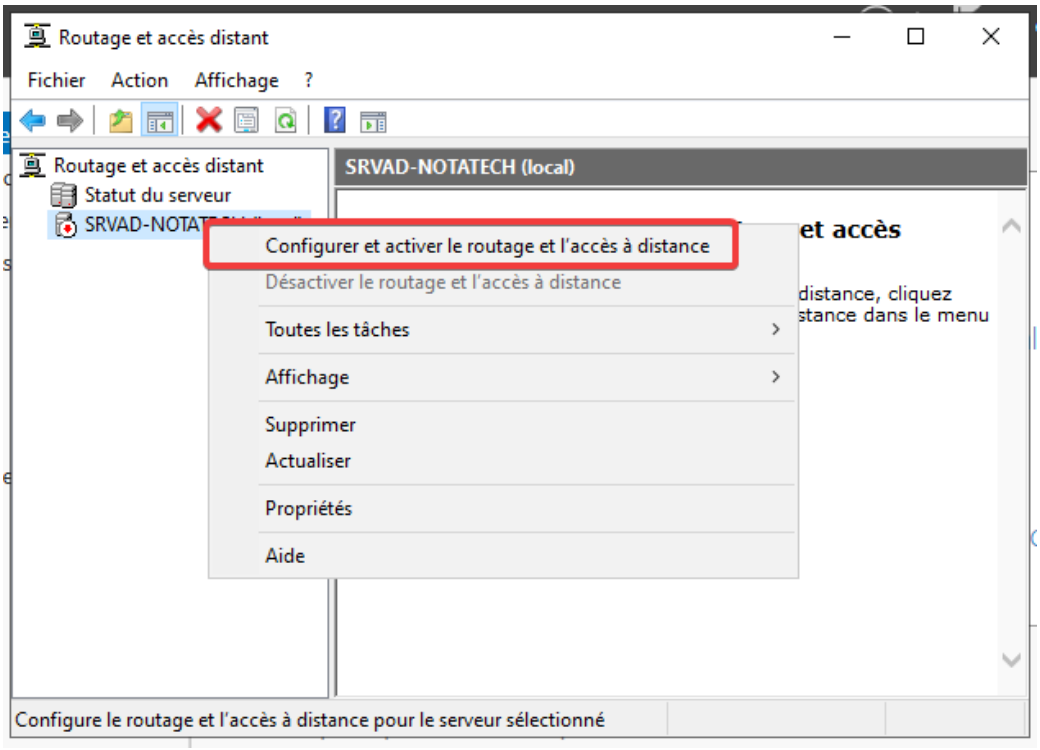
J'ai confirmé l'installation des services comme le routage NAT et DirectAccess. Ces services permettront de gérer les connexions VPN et d'assurer la sécurité des communications entre les machines.



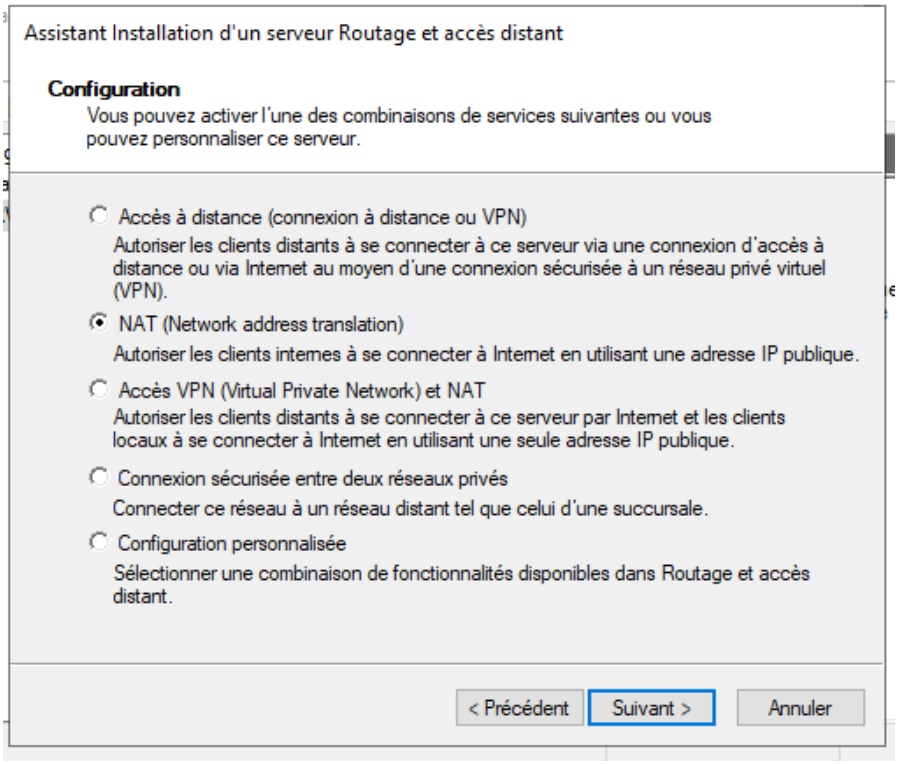
Après l'installation, j'ai ouvert l'outil "Routage et accès distant" pour configurer les paramètres NAT. Cela permettra à mes machines internes d'accéder à Internet tout en maintenant une protection grâce au pare-feu.



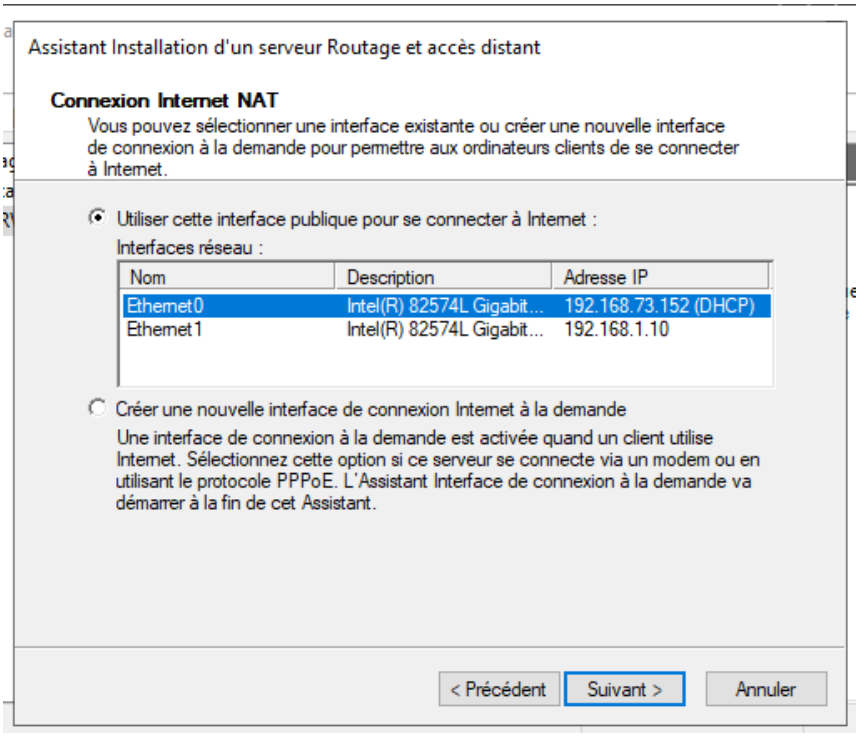
Enfin, j'ai activé la fonction NAT sur le serveur pour qu'il puisse rediriger le trafic entre mon réseau interne et Internet. Pour ce faire, sur la fenêtre qui vient de s'ouvrir je fais une clique droit sur mon serveur et je clique sur « configurer et activer le routage et l'accès à distance »



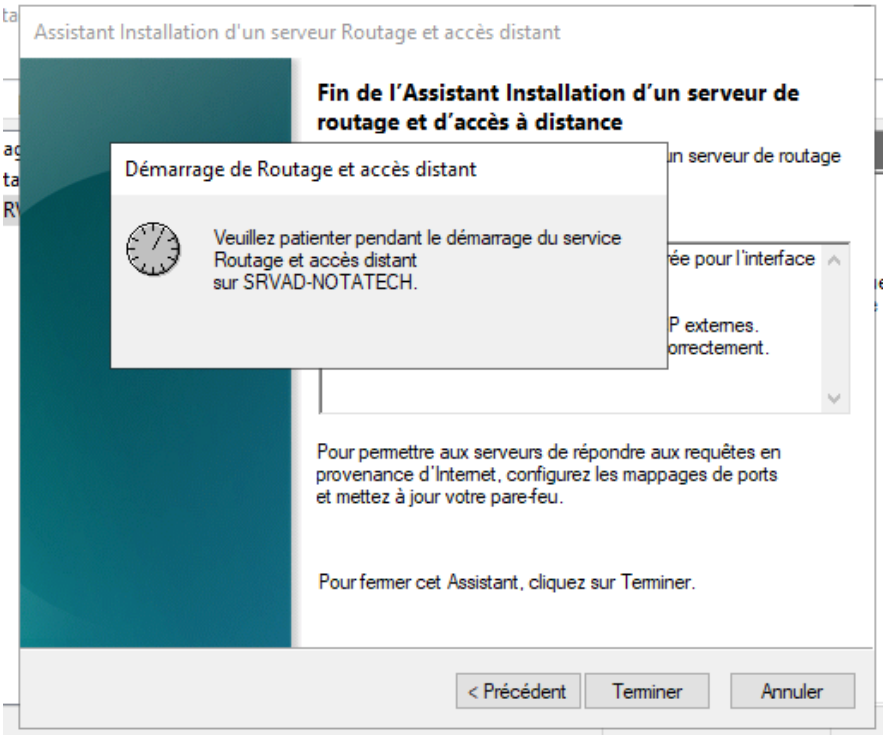
Dans cette étape, j'ai choisi l'option "NAT (Network Address Translation)" pour permettre aux machines de mon réseau interne d'accéder à Internet à travers une adresse publique.



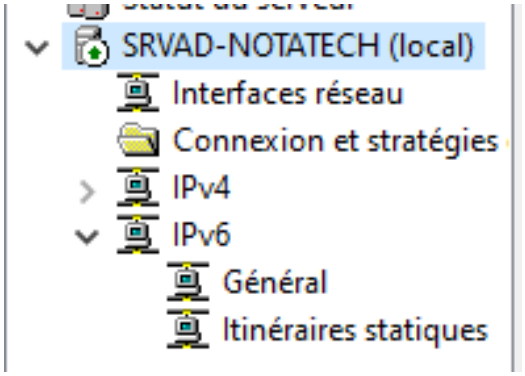
J’ai sélectionné l’interface réseau correspondant à ma carte NAT, associée à l’adresse IP fournie par le DHCP (192.168.73.152). Cette interface sera utilisée comme passerelle pour rediriger le trafic Internet.



L’installation et la configuration du rôle "Routage et accès distant" sont terminées. Le démarrage du service se lance.



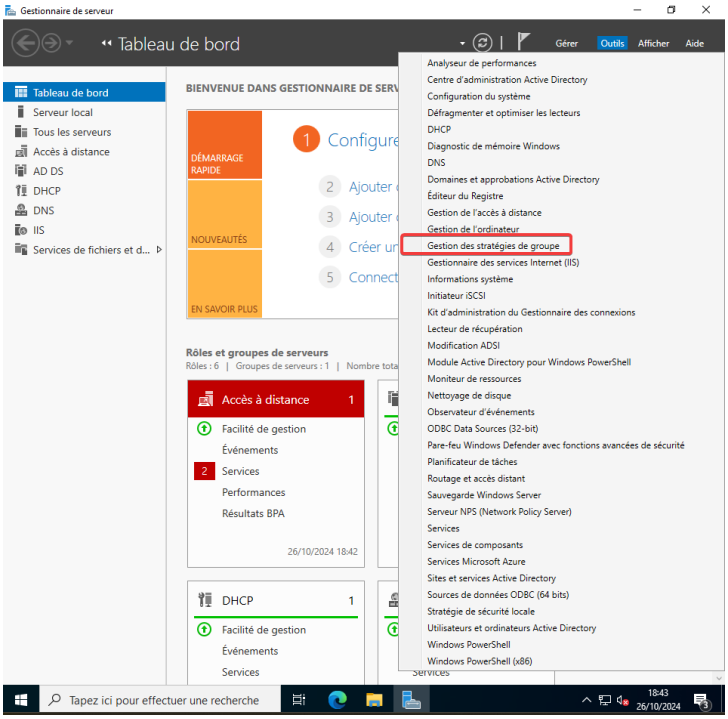
L’installation finalement terminée je vérifie qu’il est bien actif, il l’est bien donc l’installation et la configuration du rôle "Routage et accès distant" sont terminées. Le serveur est maintenant prêt à gérer le trafic NAT pour permettre l’accès à Internet depuis le réseau interne.



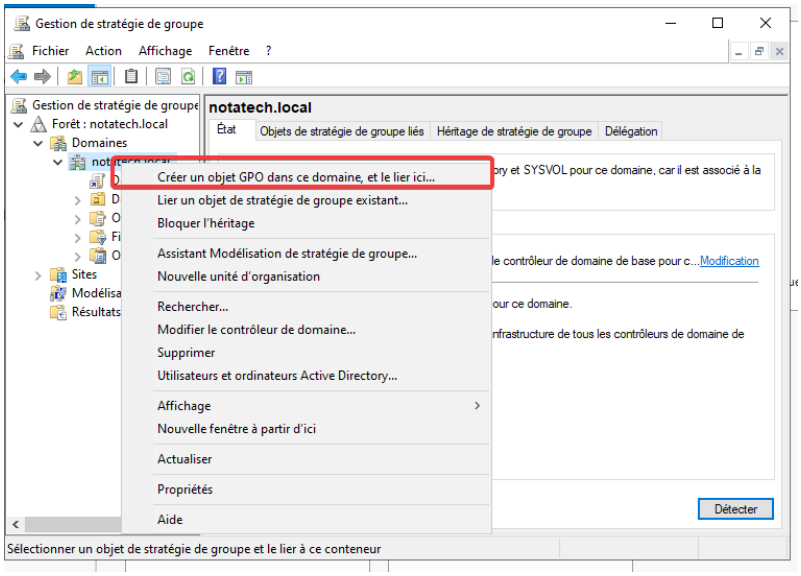
Création de GPO :

Dans cette partie nous allons voir comment j'ai configuré mes GPO pour les exigences de mot de passe

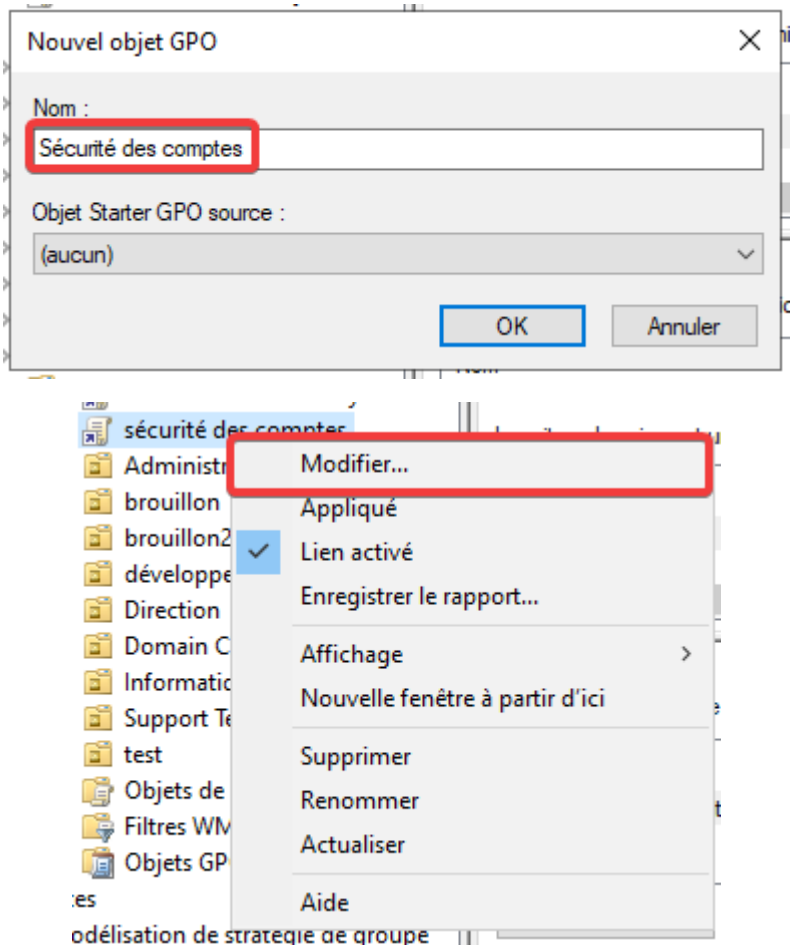
Dans le tableau de bord du serveur, je clique sur Outils, puis sur Gestion des stratégies de groupe pour ouvrir la console GPO.



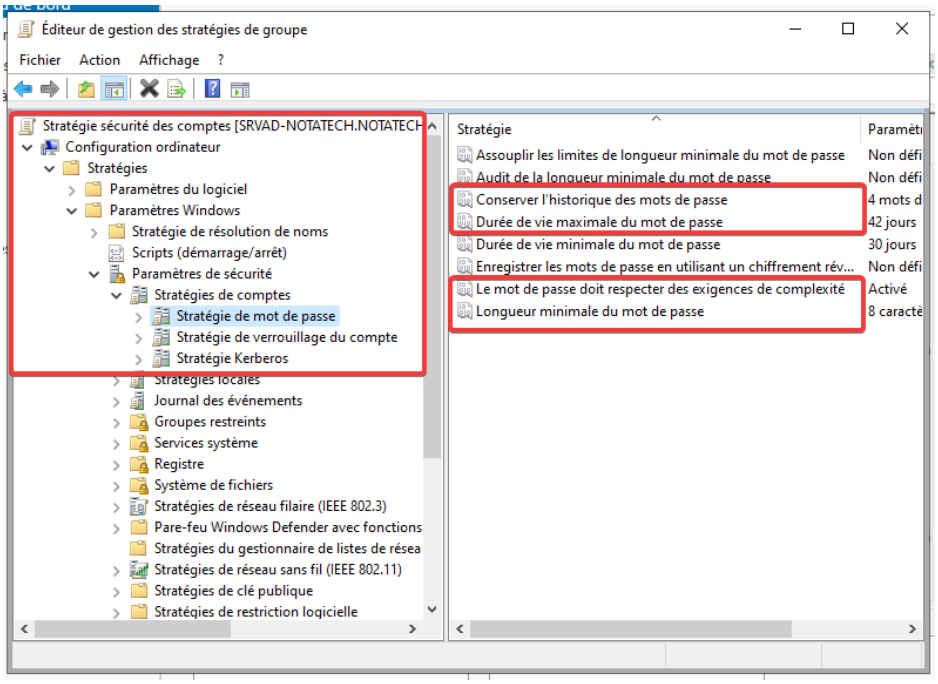
Dans la console **Gestion des stratégies de groupe**, je fais un clic droit sur le domaine **notatech.local**, puis je sélectionne **Créer un objet GPO dans ce domaine et le lier ici**.



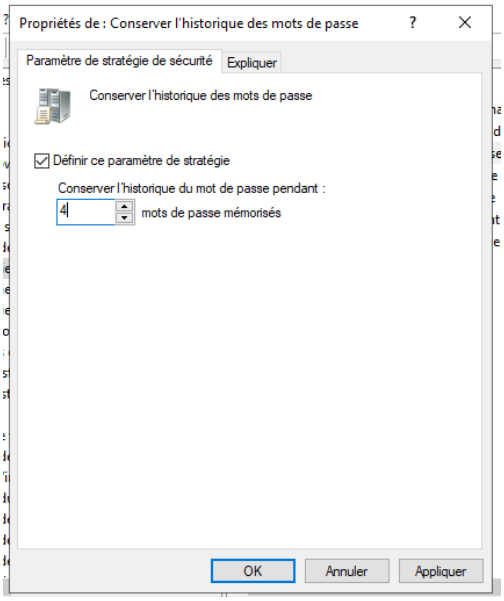
Je donne un nom explicite à la GPO, comme ici "**Sécurité des comptes**". Et je fais un clic droit « modifier »



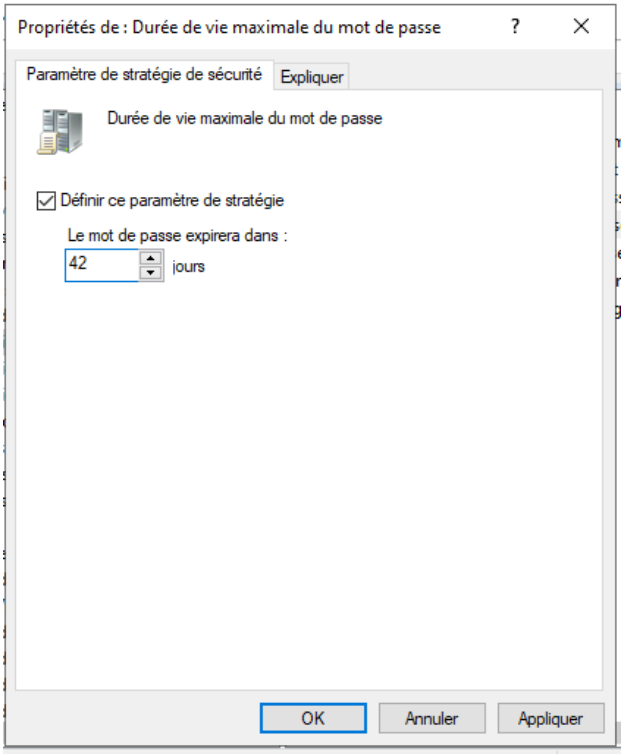
Je me rends donc ensuite au chemin « **configuration ordinateur > paramètres Windows > paramètres de sécurité** » dans cette fenêtre je repère ces paramètres et je vais cliquer dessus pour les modifier



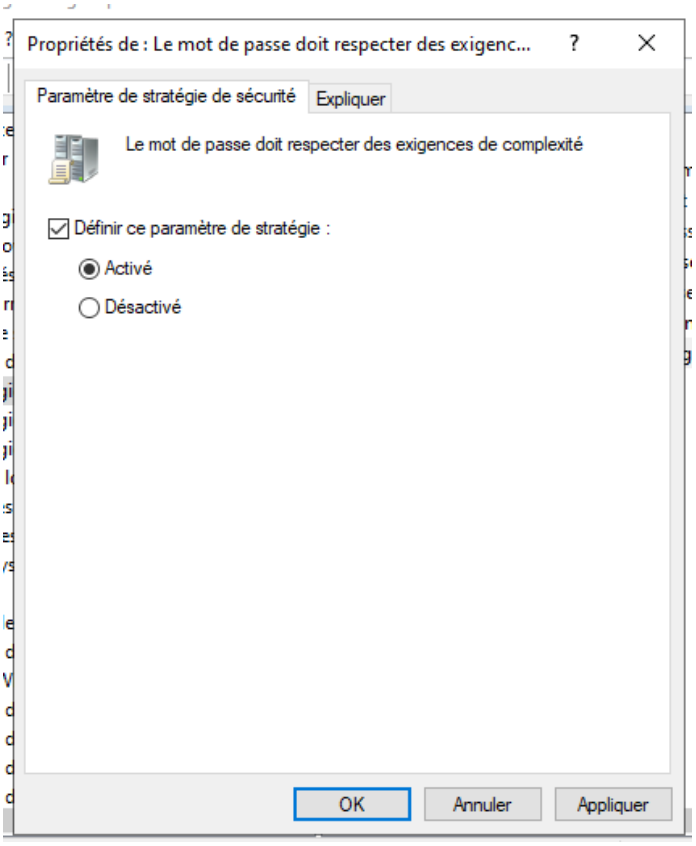
Je choisis tout d'abord de conserver un historique de au moins 4 mots de passe



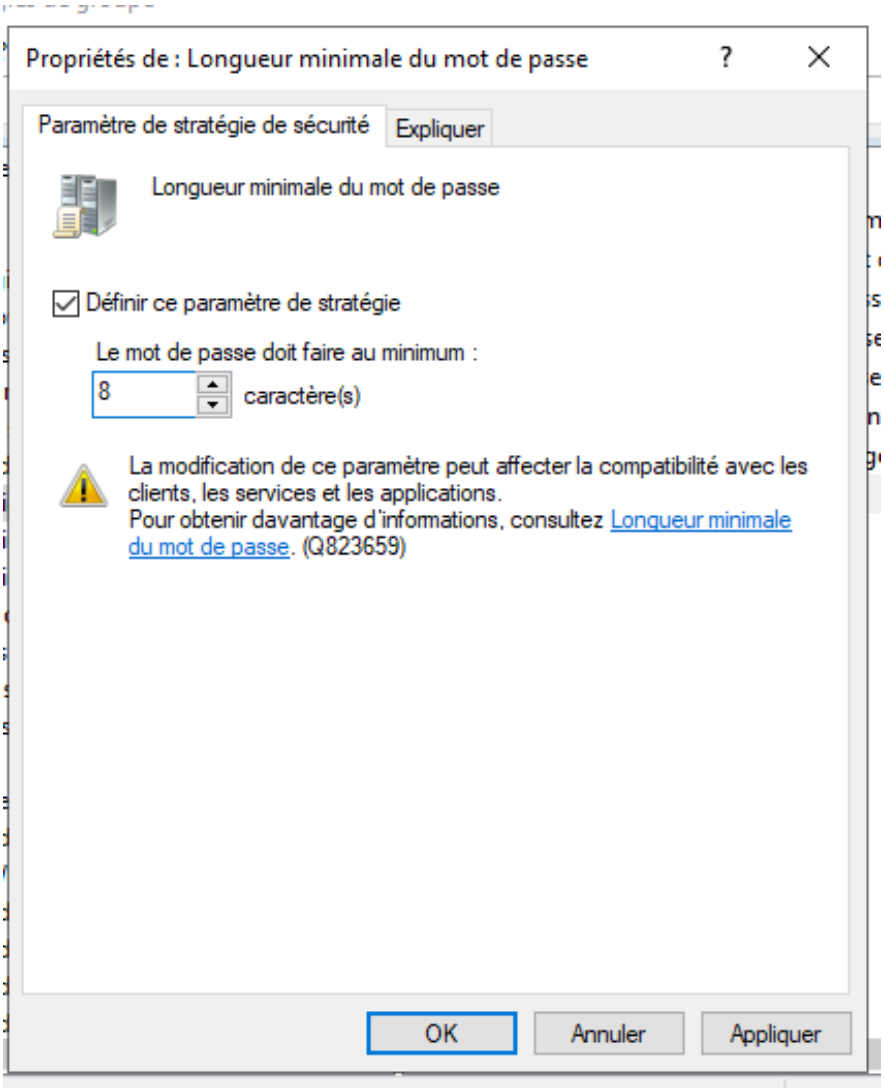
Ensuite je sélectionne la durée de vie maximale pour un mot de passe de 42 jours



Pour les exigences des mots de passe je clique sur le paramètre en question et sélectionne activer et « définir ce paramètre de stratégie »

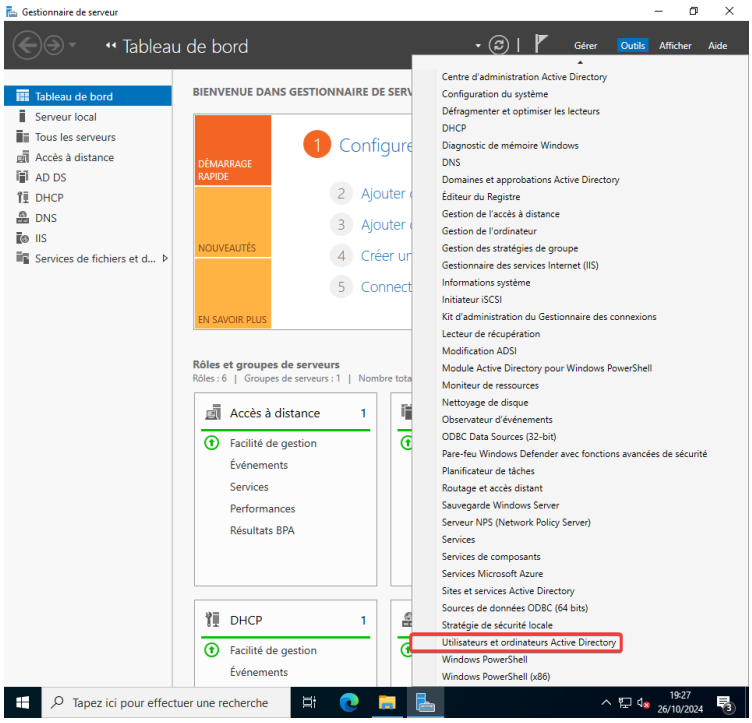


Et finalement pour la longueur minimale des mots de passe, je saisi un minimum de 8 caractères

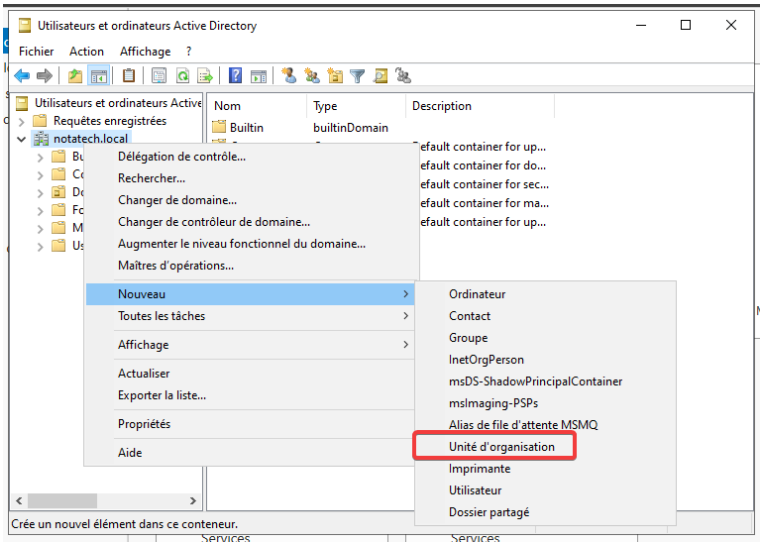


Création des utilisateurs et des unités d'organisation :

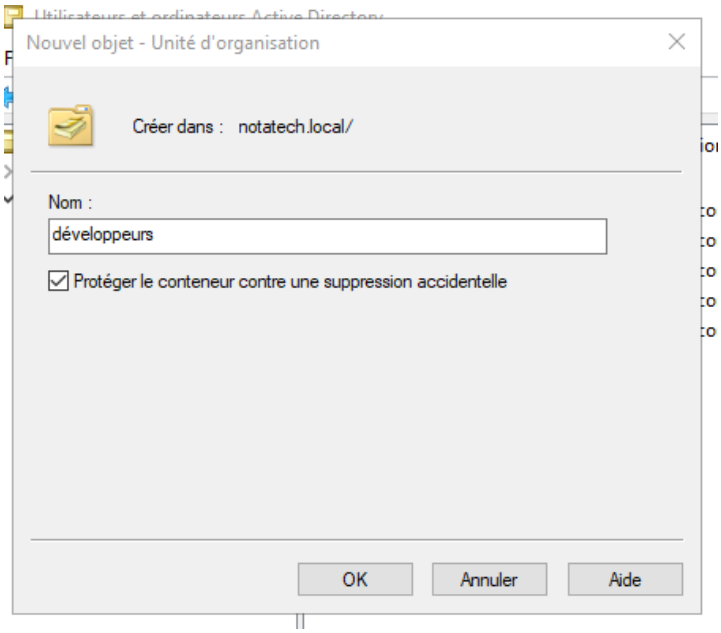
Pour commencer la création, je me rends tout d'abord dans « utilisateurs et ordinateurs Active Directory » dans les outils de Windows server



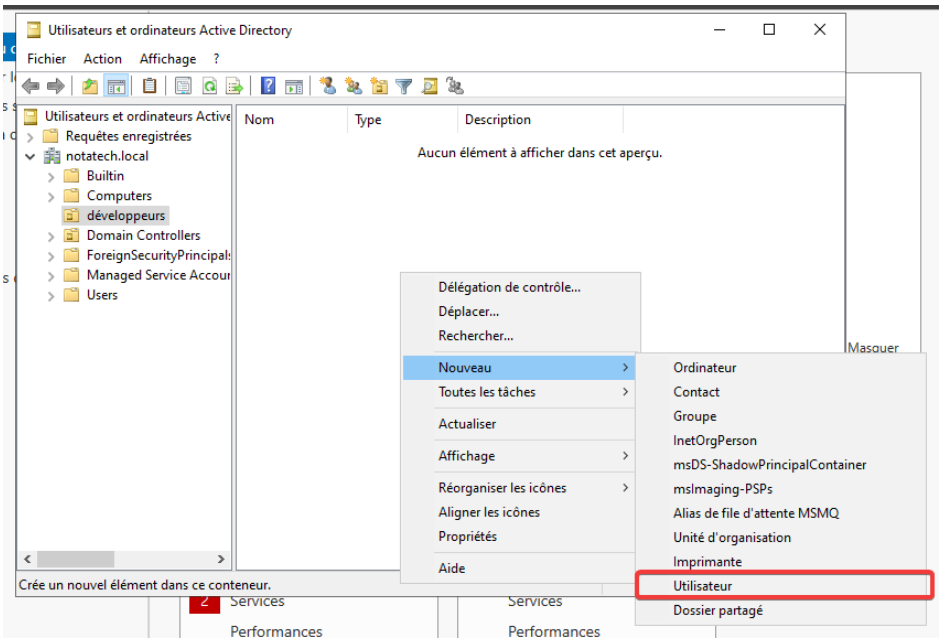
Ensuite une fois dans cette fenêtre je fais un clic droit, nouveau et sélectionne « unité d'organisation » pour commencer a créer une unité d'organisation



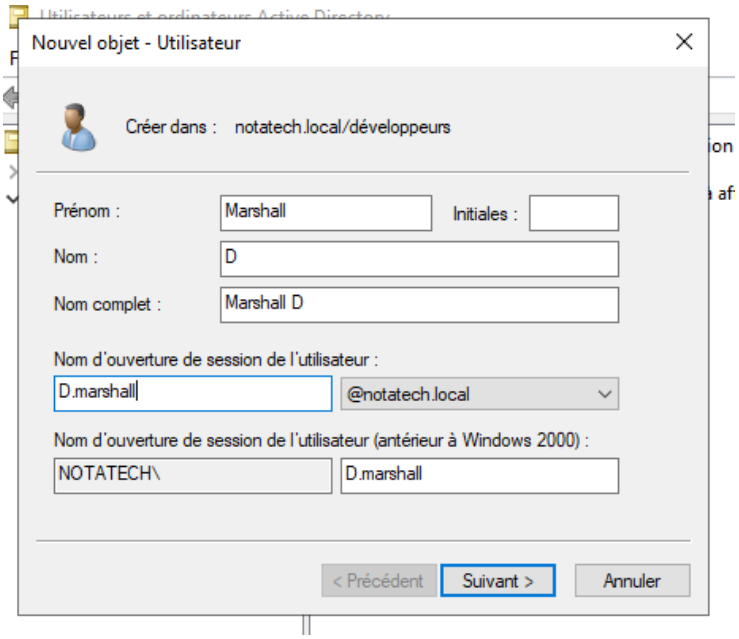
Je nomme cette unité d'organisation « développeurs », elle regroupera tous les utilisateurs de développeurs



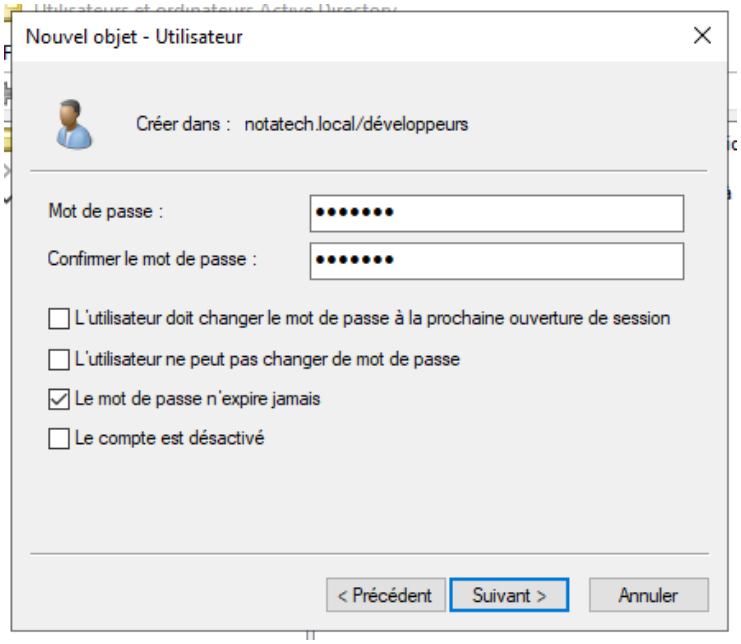
Une fois créé je fais un clic droit, nouveau et sélectionne « utilisateur » pour créer un nouvel utilisateur dans cette unité d'organisation



Je créer cet utilisateur se nommant « Marshall D », il se connectera avec l'identifiant « D.marshall »



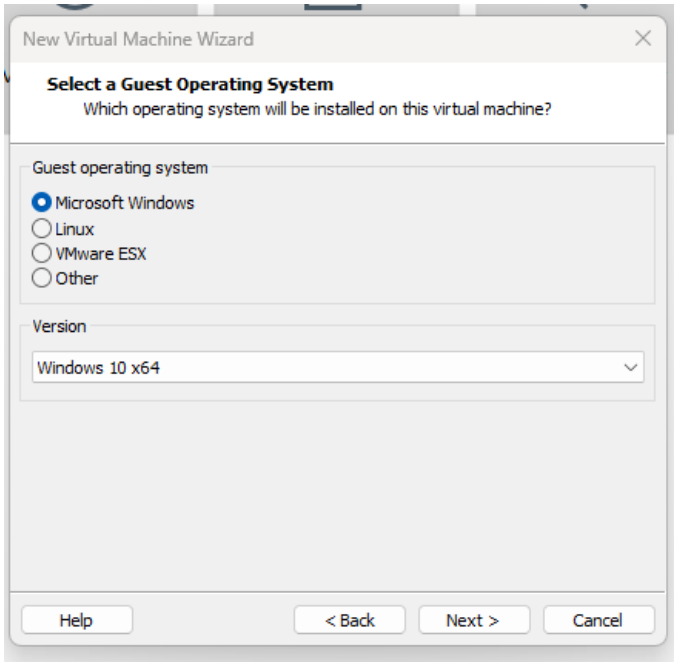
Ensuite je définis un premier mot de passe pour cet utilisateur qui pourra le changer plus tard (je ne l'active pas pour l'instant pour faciliter la suite des tests)



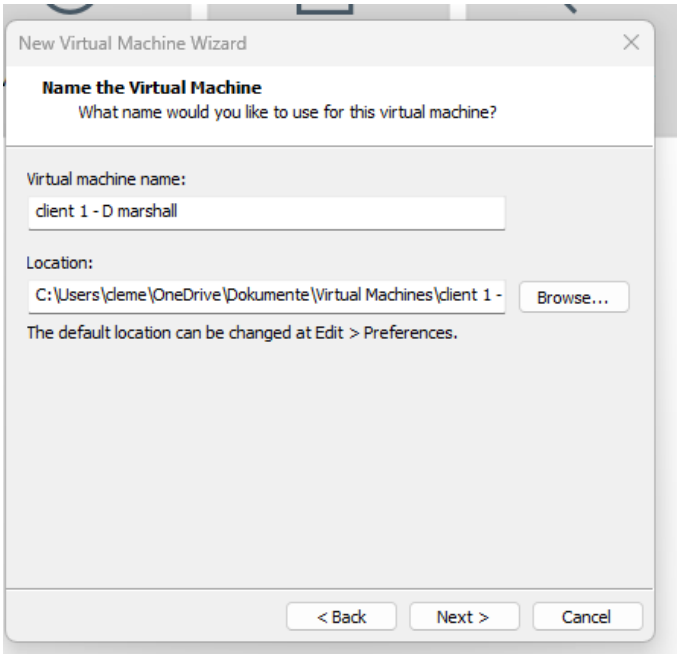
Test sur une machine cliente :

Nous allons maintenant creer une machine windows 10 cliente pour pouvoir tester le nouvel utilisateur

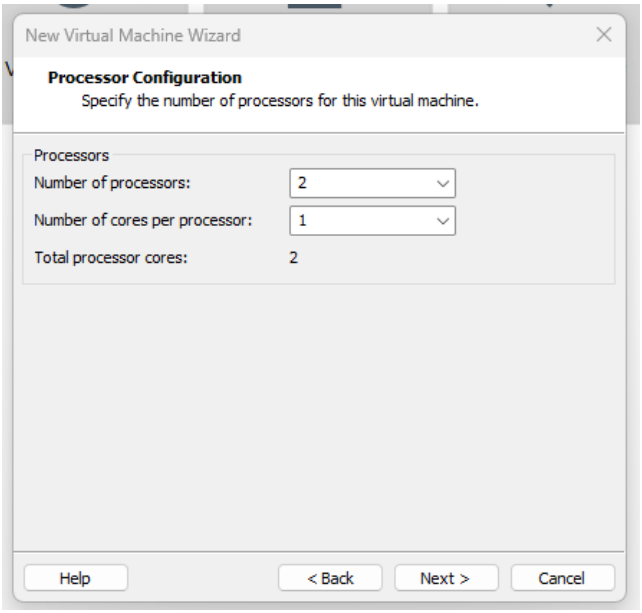
Je commence par créer une nouvelle machine virtuelle et sélectionne Windows 10



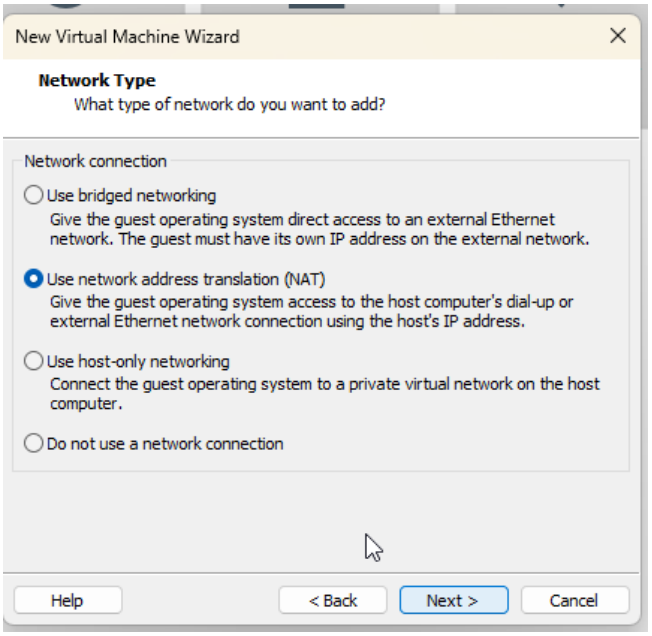
Je donne à ma machine le nom de « client 1 – D marshall »



Je sélectionne seulement ce nombre de processeurs car ce sera largement suffisant pour les tests que nous allons effectuer

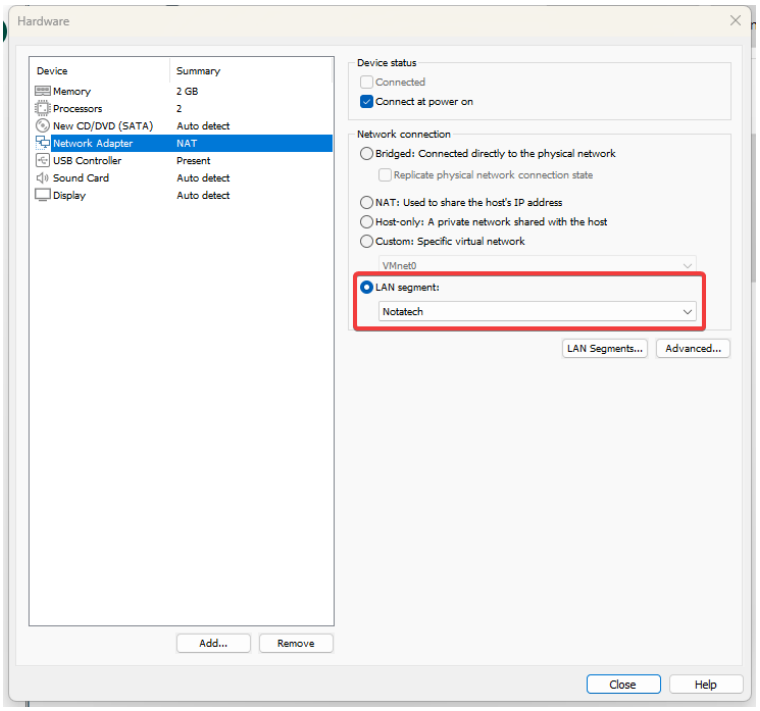


Je choisis ensuite une connexion NAT (par défaut) que nous allons changer ensuite pour utiliser la connexion LAN segment « notatech » pour se connecter au même LAN que le serveur

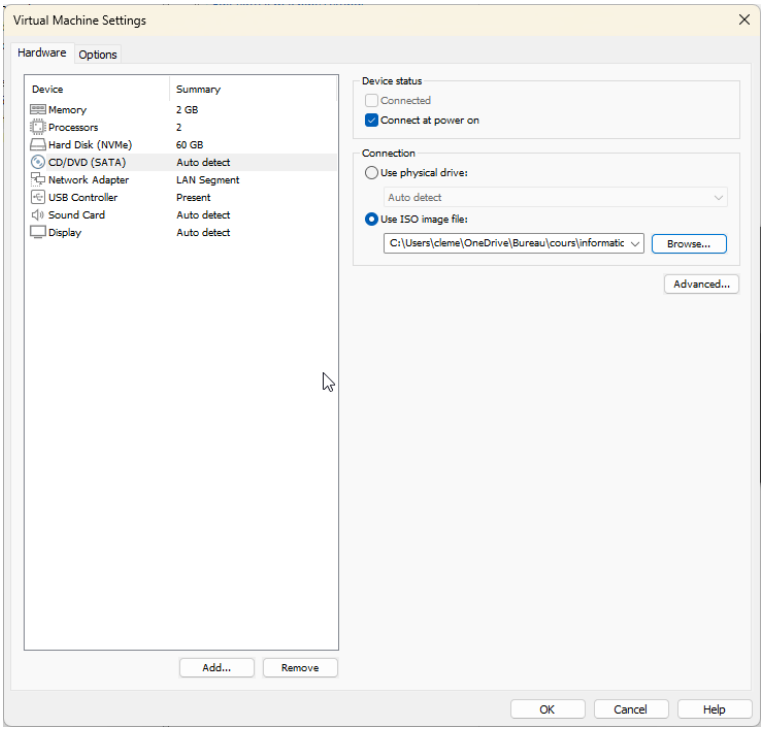


Et ensuite je laisse les paramètres par défaut pour le reste de la configuration

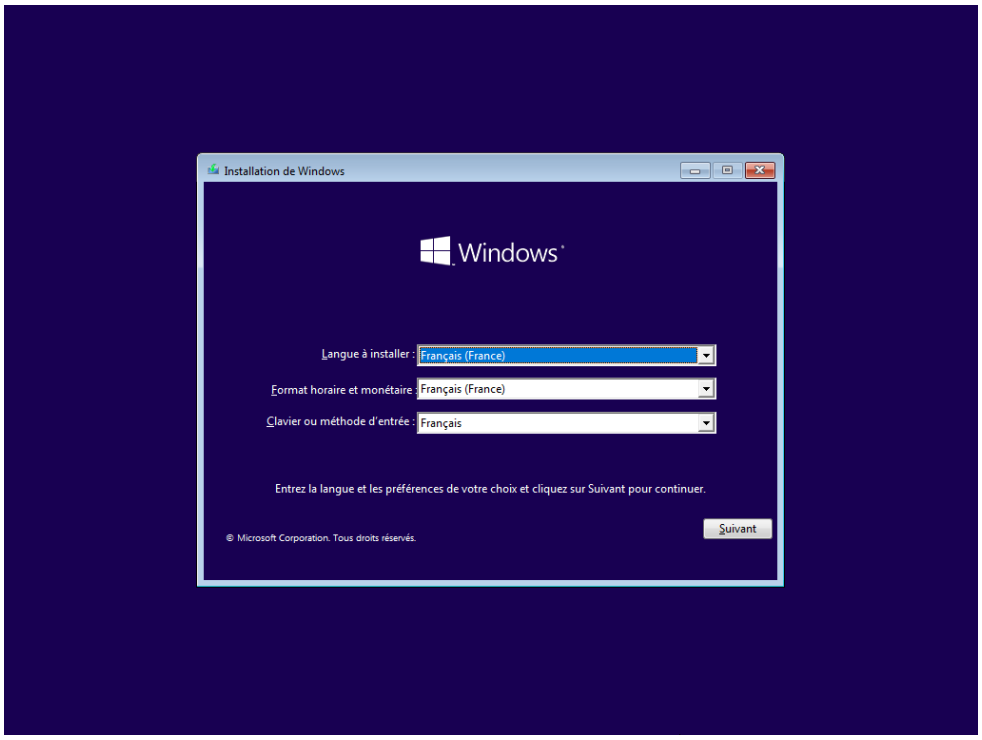
Ensuite je me rends dans la configuration hardware de la machine et change la connexion réseau a « LAN segment » et sélectionne mon LAN segment précédemment créer pour le réseau Notatech



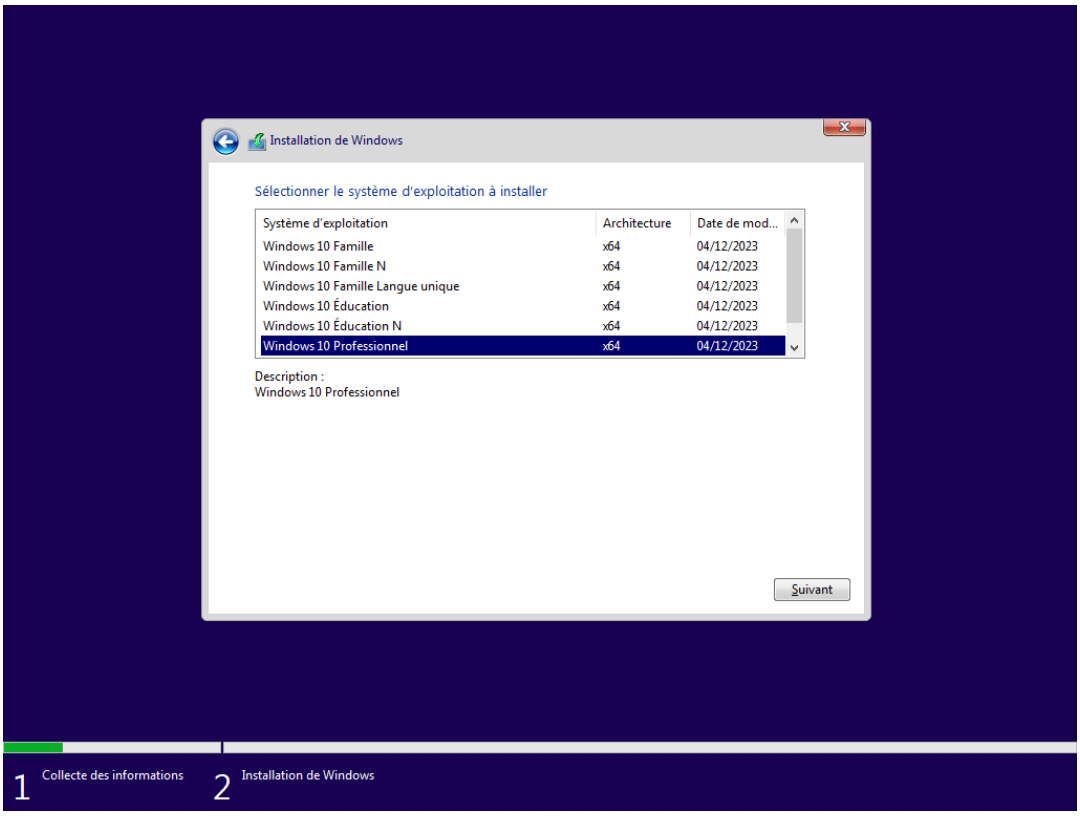
Et je me rends finalement dans « CD/DVD », sélectionne « Use ISO image file » et sélectionne mon ISO de Windows 10 classique



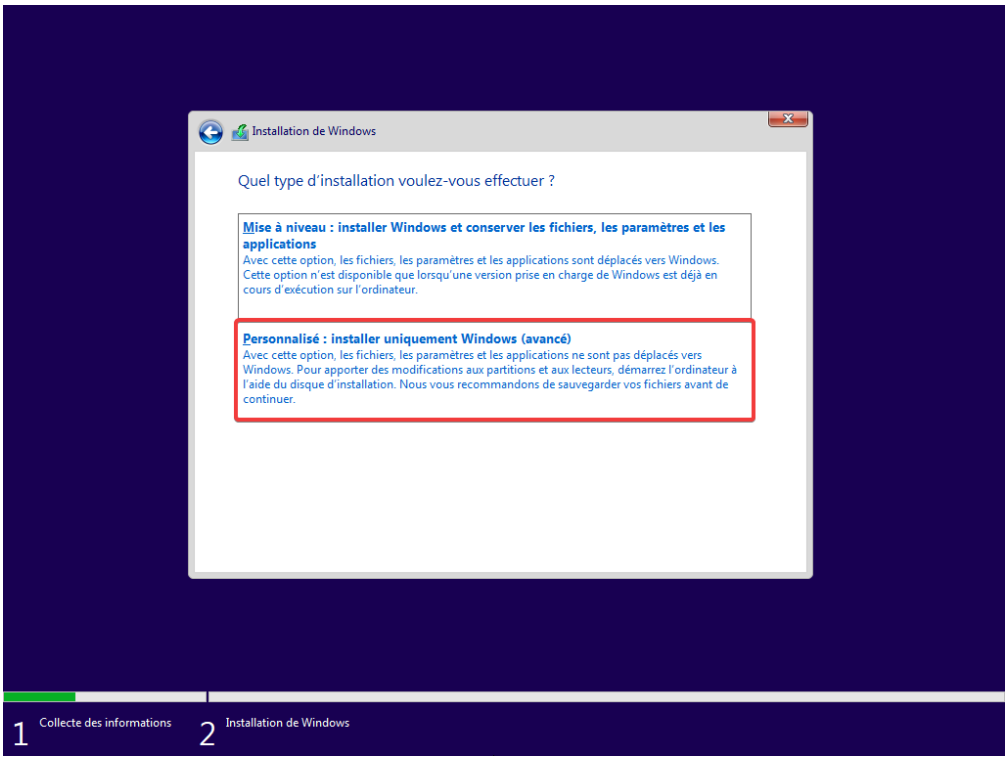
Ensuite je lance donc ma machine virtuelle, arrivé sur cet écran je clique sur « suivant »



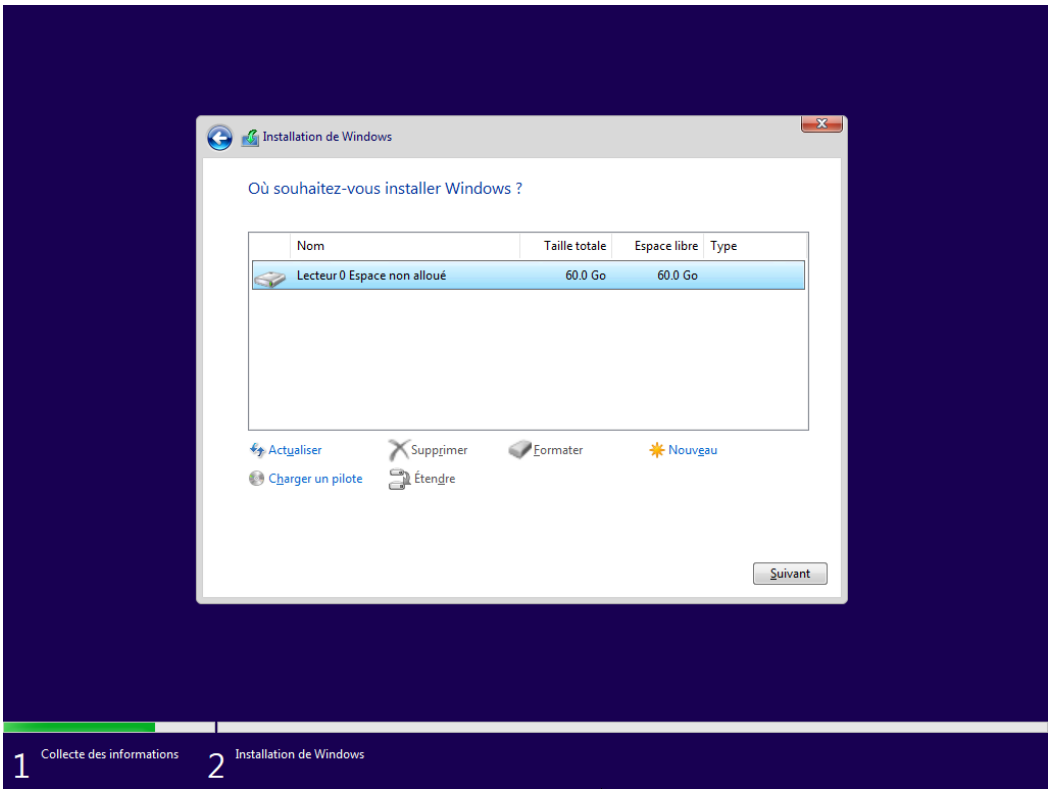
Je sélectionne ici « Windows 10 professionnel »



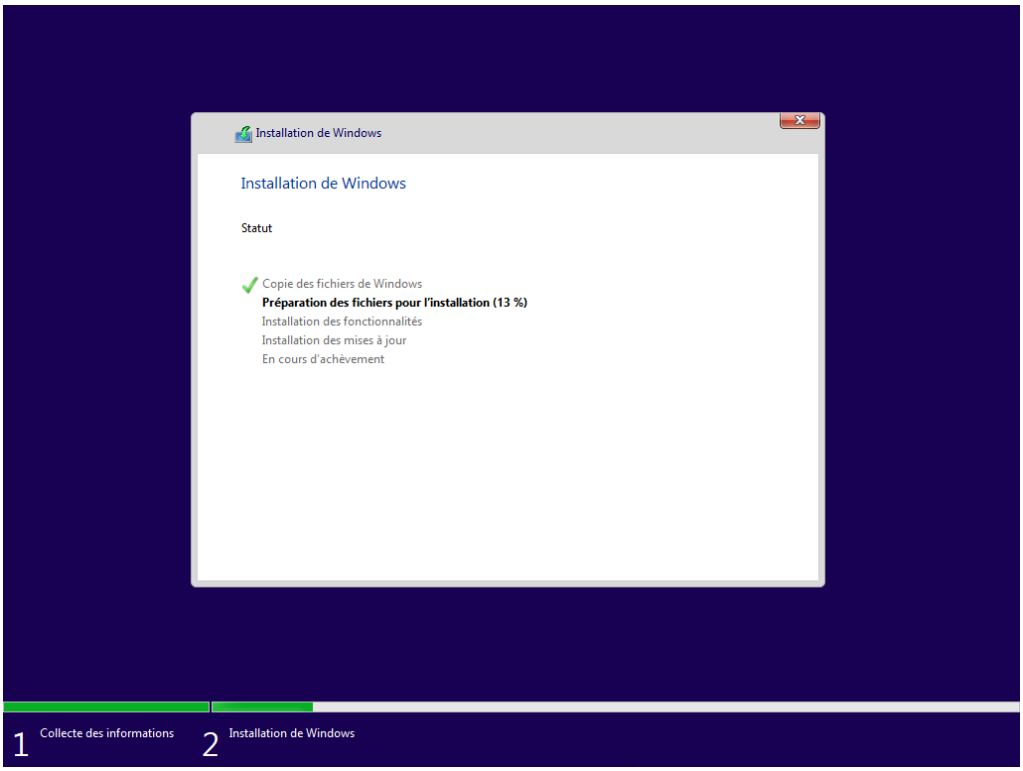
Pour le type d'installation je sélectionne « **personnalisé** »



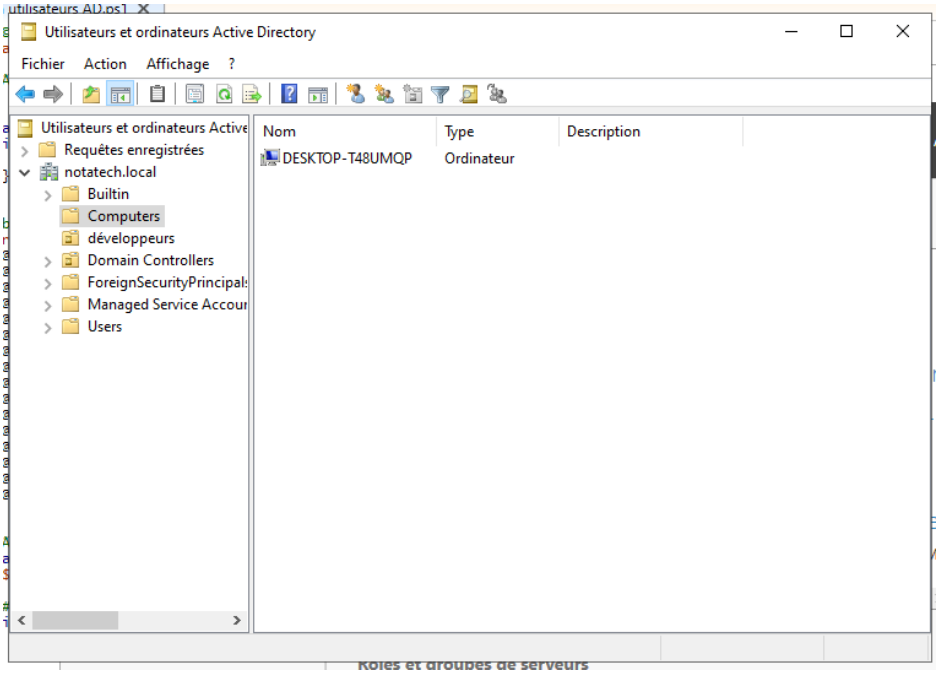
Ici je sélectionne simplement mon disque



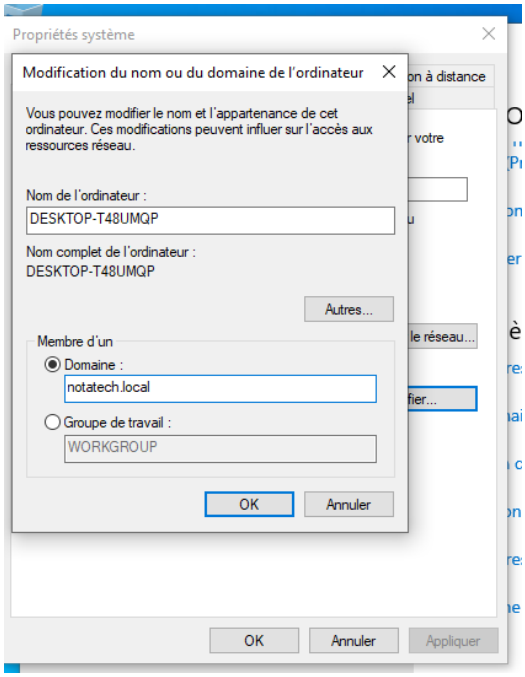
L’installation va donc se lancer avant de pouvoir finalement lancer la machine cliente



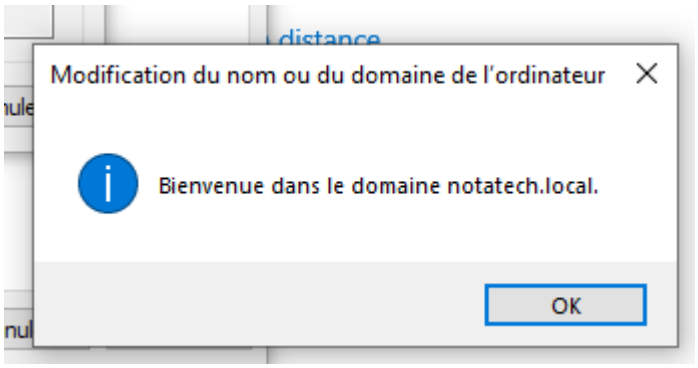
Avant de pouvoir me connecter avec cette machine je dois l'ajouter a mon domaine sur mon windows server, je récupère donc le nom de ma machine et l'ajoute dans la section « computers » de mon Active directory



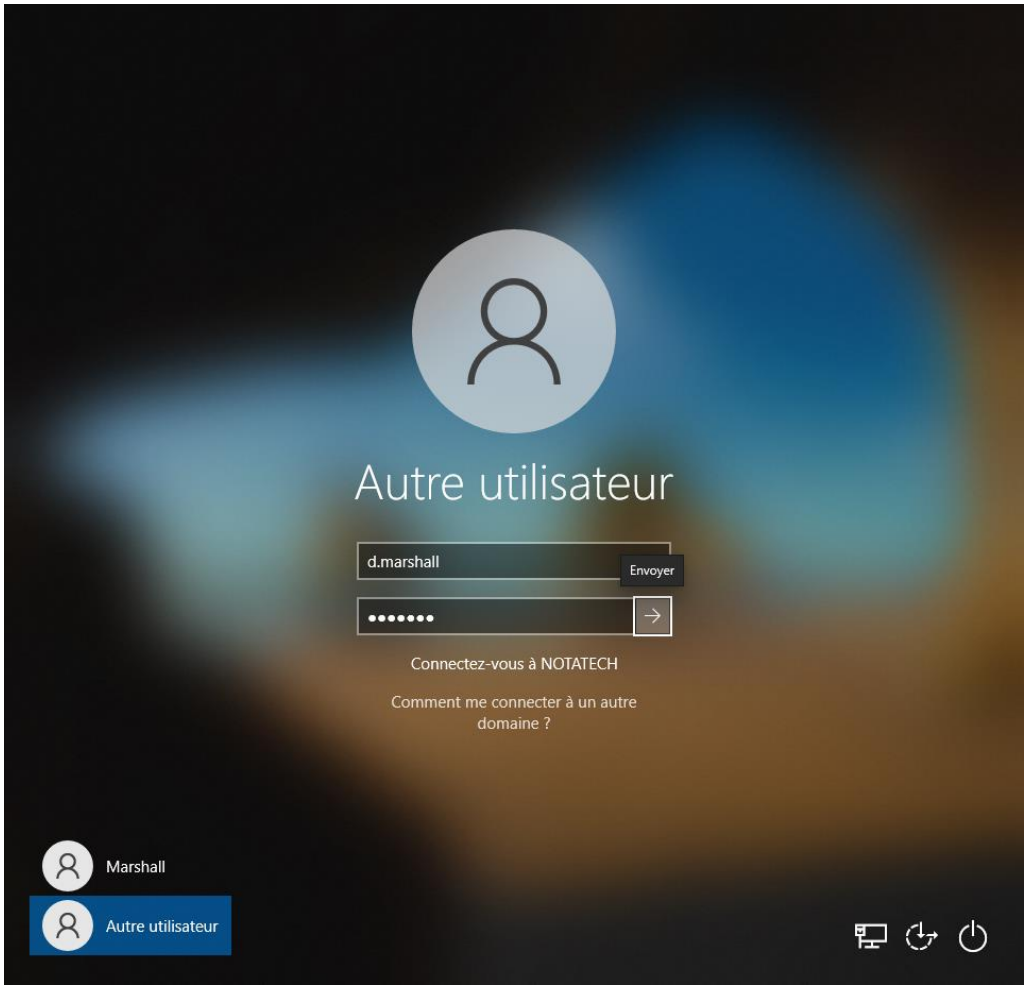
Ensuite sur ma machine cliente, une fois connecté je l'ajoute au domaine que j'ai créer précédemment « notatech.local ».



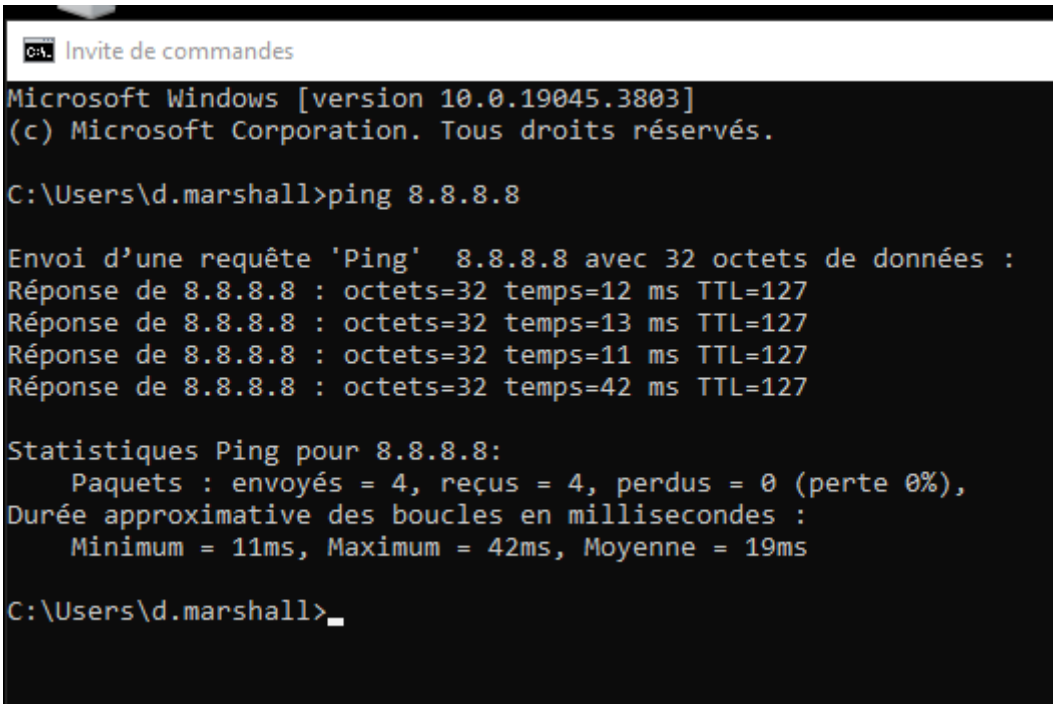
Ce message apparaitra finalement, on est donc maintenant bien lié au domaine



Ensuite je me deconnecte de la session et me connecte avec la session que j'ai créer précédemment



Je suis bien connecté, je verifie que la connexion a internet fonctionne bien, ping OK tout est bon au niveau de ça



Nous allons maintenant créer les autres utilisateurs mais je vais utiliser un script PowerShell pour aller plus rapidement. L'entreprise m'a fourni ce tableau à respecter

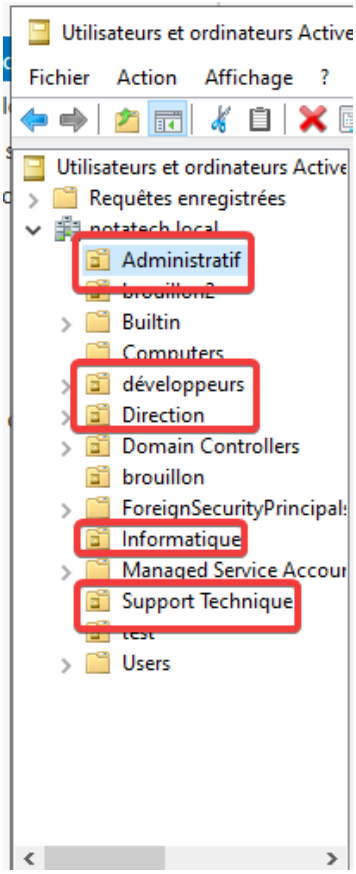
Nom	Poste	Secteur	Nom d'utilisateur
Pierre Duval	PDG	Direction	pduval
Clara Dupuis	Développeur	Informatique	cdupuis
Antoine Lambe	Développeur	Informatique	alambert
Laura Martine	Développeur	Informatique	lmartine
Julien Moreau	Développeur	Informatique	jmoreau
Nadia Girard	Développeur	Informatique	ngirard
Isabelle Lemoi	Secrétaire	Administratif	ilemoine
Marc Beaulieu	Secrétaire	Administratif	mbeaulieu
Sophie Thibaul	Secrétaire	Administratif	sthibault
Camille Perrin	Secrétaire	Administratif	cperrin
Éric Roy	Secrétaire	Administratif	eroy
Luc Durand	Technicien Sup	Support Technique	ldurand
Sarah Bernard	Technicien Sup	Support Technique	sbernard
Kevin Fournier	Technicien Sup	Support Technique	kfournier
Hélène Petit	Technicien Sup	Support Technique	hpetit
Jean Fabre	Technicien Sup	Support Technique	jfabre

Voici mon script, ce script va me permettre de créer tous les utilisateurs et mes unités d'organisation en respectant le tableau mentionné avant, tout en activant l'option **l'utilisateur devra changer de mot de passe** et désactivant l'option **le mot de passe n'expire jamais**

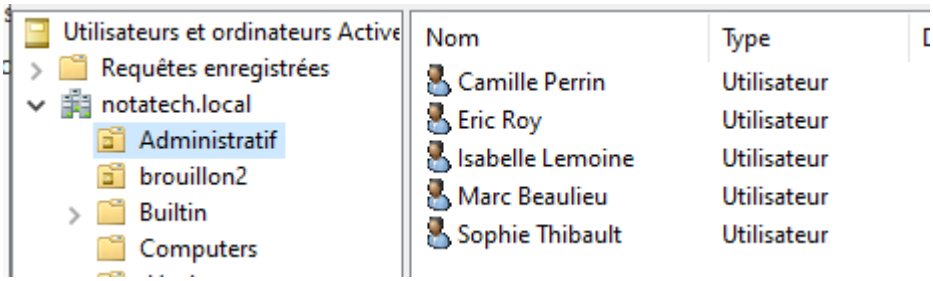
script création utilisateurs AD.ps1*

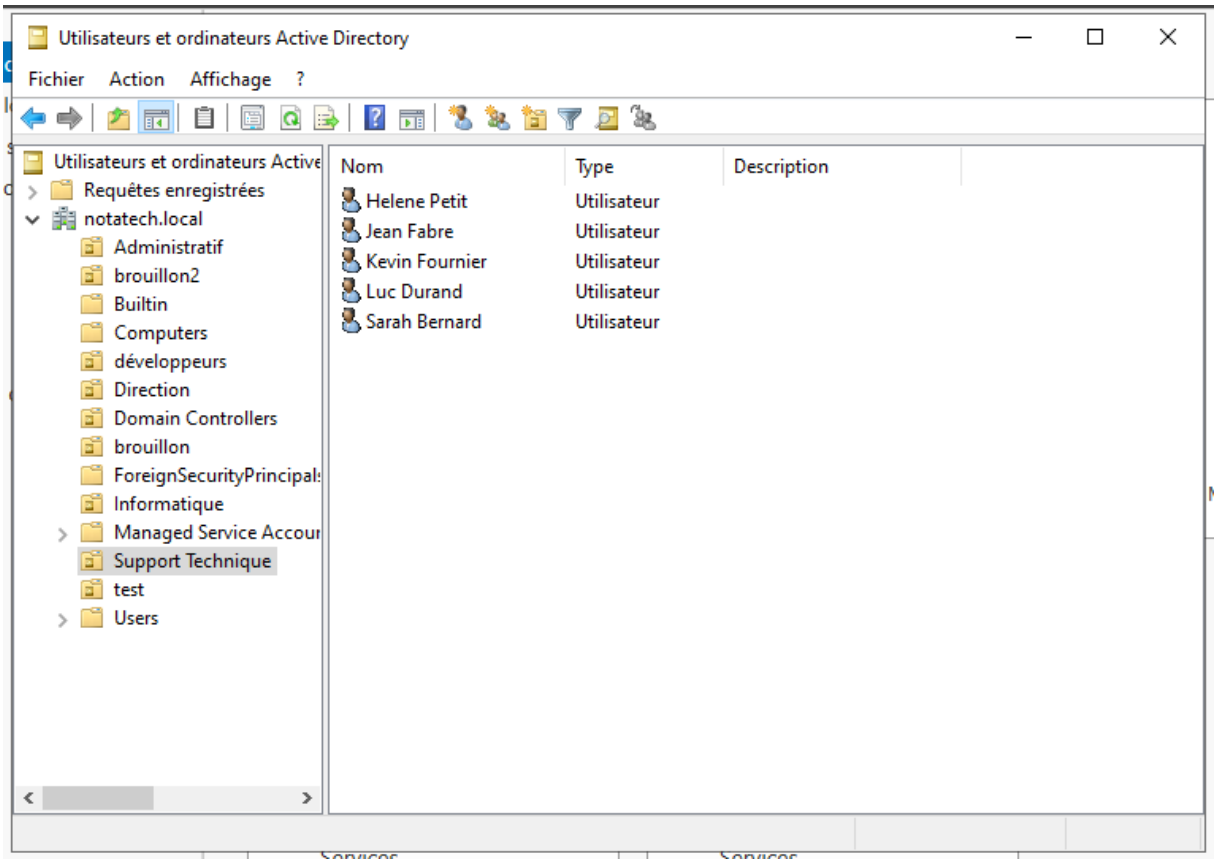
```powershell
# Definir le nom du domaine
$domain = "notatech.local"

# Creer les unites d'organisation (OU)
$ous = @("Direction", "Informatique", "Administratif", "Support Technique")

foreach ($ou in $ous) {
    if (-not (Get-ADOrganizationalUnit -Filter "Name -eq '$ou'" -ErrorAction SilentlyContinue)) {
        New-ADOrganizationalUnit -Name $ou -Path "DC=notatech,DC=local"
    }
}

# Tableau des utilisateurs a creer
$users = @(
    @{ Nom = "Pierre Duval"; Poste = "PDG"; Secteur = "Direction"; NomUtilisateur = "pierre.duval" },
    @{ Nom = "Clara Dupuis"; Poste = "Developpeur"; Secteur = "Informatique"; NomUtilisateur = "clara.dupuis" },
    @{ Nom = "Antoine Lambert"; Poste = "Developpeur"; Secteur = "Informatique"; NomUtilisateur = "antoine.lambert" },
    @{ Nom = "Laura Martine"; Poste = "Developpeur"; Secteur = "Informatique"; NomUtilisateur = "laura.martine" },
    @{ Nom = "Julien Moreau"; Poste = "Developpeur"; Secteur = "Informatique"; NomUtilisateur = "julien.moreau" },
    @{ Nom = "Nadia Girard"; Poste = "Developpeur"; Secteur = "Informatique"; NomUtilisateur = "nadia.girard" },
    @{ Nom = "Isabelle Lemoine"; Poste = "Secretaire"; Secteur = "Administratif"; NomUtilisateur = "isabelle.lemoine" },
    @{ Nom = "Marc Beaulieu"; Poste = "Secretaire"; Secteur = "Administratif"; NomUtilisateur = "marc.beaulieu" },
    @{ Nom = "Sophie Thibault"; Poste = "Secretaire"; Secteur = "Administratif"; NomUtilisateur = "sophie.thibault" },
    @{ Nom = "Camille Perrin"; Poste = "Secretaire"; Secteur = "Administratif"; NomUtilisateur = "camille.perrin" },
    @{ Nom = "Eric Roy"; Poste = "Secretaire"; Secteur = "Administratif"; NomUtilisateur = "eric.roy" },
    @{ Nom = "Luc Durand"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "luc.durand" },
    @{ Nom = "Sarah Bernard"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "sarah.bernard" },
    @{ Nom = "Kevin Fournier"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "kevin.fournier" },
    @{ Nom = "Helene Petit"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "helene.petit" },
    @{ Nom = "Jean Fabre"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "jean.fabre" }
)

# Creer les utilisateurs
foreach ($user in $users) {
    $ouPath = "OU=$($user.Secteur),DC=notatech,DC=local"

    # Verifier si l'utilisateur existe deja
    if (-not (Get-ADUser -Filter "SamAccountName -eq '$($user.NomUtilisateur)'" -ErrorAction SilentlyContinue)) {
        New-ADUser -Name $user.Nom -GivenName $user.Nom.Split(" ")[0] -Surname $user.Nom.Split(" ")[1] `
            -SamAccountName $user.NomUtilisateur -UserPrincipalName "$($user.NomUtilisateur)@$domain" `
            -Path $ouPath -AccountPassword (ConvertTo-SecureString "Root123" -AsPlainText -Force) `
            -Enabled $true `
            -ChangePasswordAtLogon $true `
            -PasswordNeverExpires $false
    } else {
        Write-Host "L'utilisateur $($user.Nom) existe deja."
    }
}
```

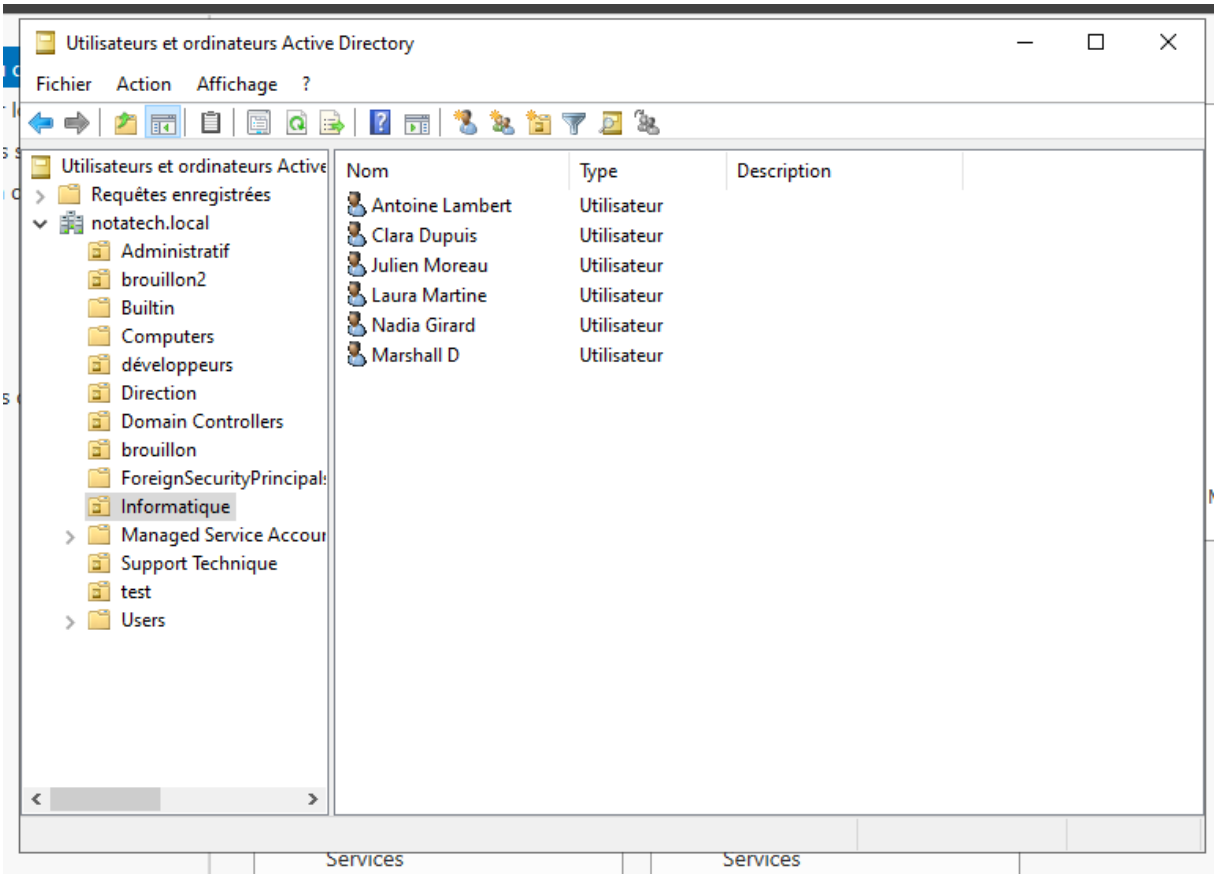
Ici on voit que mes unités d’organisation se sont bien créées



Et les utilisateurs correspondant aussi




Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
notatech.local
Administratif
brouillon2
Builtin
Computers
développeurs
Direction
Domain Controllers
brouillon
ForeignSecurityPrincipals
Informatique
Managed Service Accour
Support Technique
test
Users
Nom
Type
Description
Helene Petit Utilisateur
Jean Fabre Utilisateur
Kevin Fournier Utilisateur
Luc Durand Utilisateur
Sarah Bernard Utilisateur

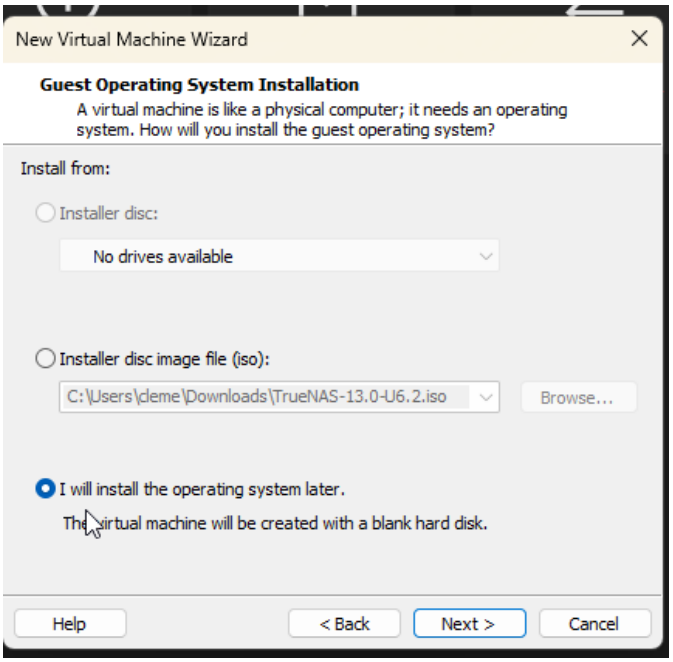

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
notatech.local
Administratif
brouillon2
Builtin
Computers
développeurs
Direction
Domain Controllers
brouillon
ForeignSecurityPrincipals
Informatique
Managed Service Accour
Support Technique
test
Users
Nom
Type
Description
Antoine Lambert Utilisateur
Clara Dupuis Utilisateur
Julien Moreau Utilisateur
Laura Martine Utilisateur
Nadia Girard Utilisateur
Marshall D Utilisateur
Services
Services

Serveur AD en redondance :

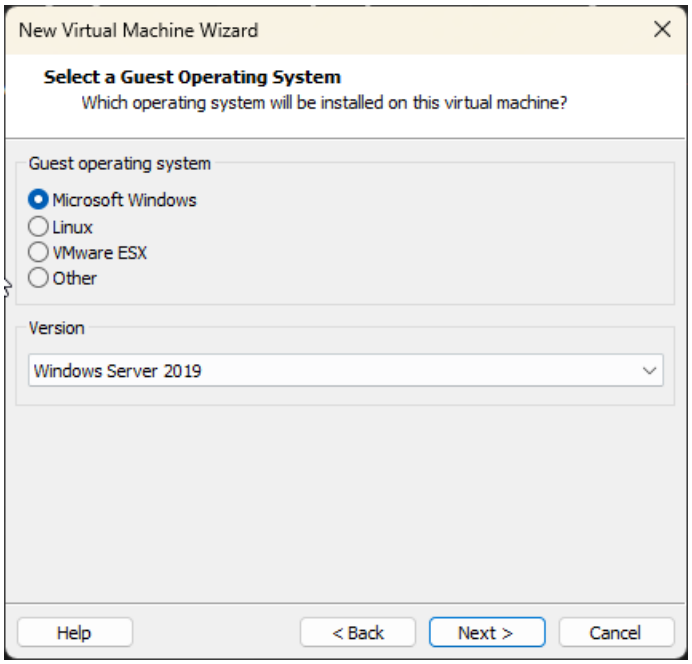
Dans cette partie-là je vais vous montrer comment j'ai mis mon serveur AD en **redondance**.

Tout d'abord je commence par créer une nouvelle machine virtuelle Windows server pour la redondance. Ici je sélectionne **custom**

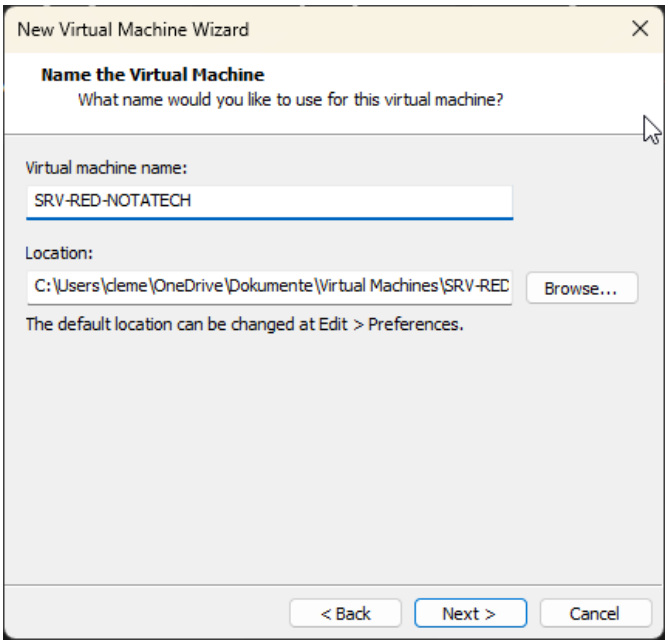
Ensuite comme mon premier serveur j'installerai l'iso plus tard



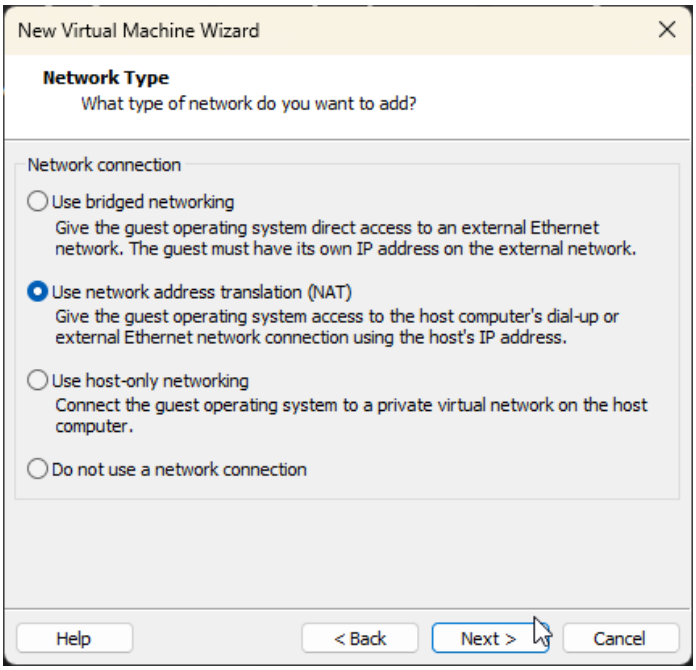
Ici je sélectionne **Windows Server 2019**



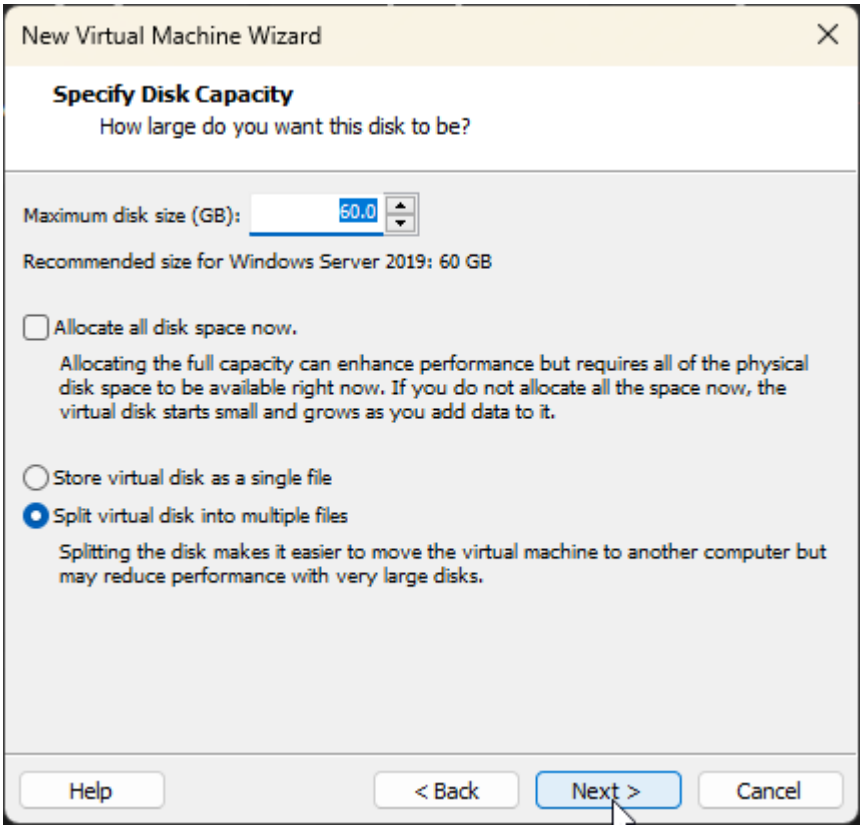
Ensuite ici je nomme mon serveur **SRV-RED-NOTATECH** pour spécifier que c'est mon serveur de redondance



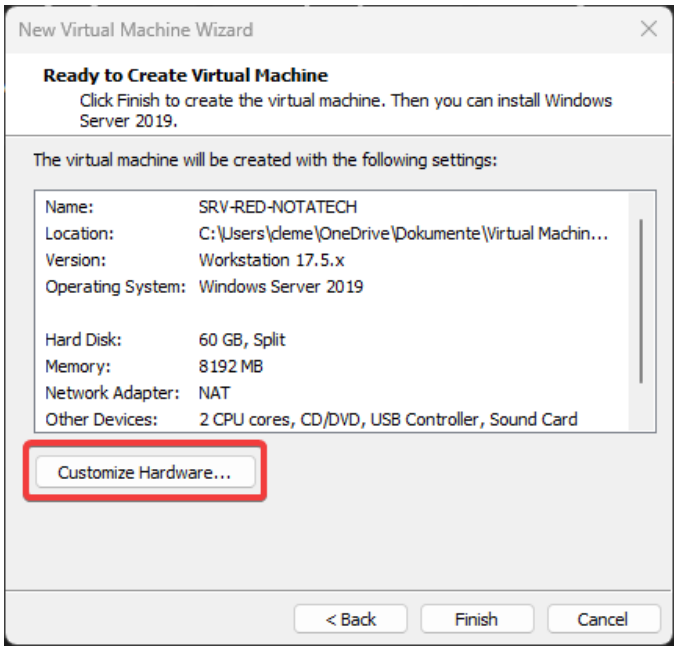
Pour le reste je laisse les options par défaut et ici je sélectionne **NAT**, on en configurera une deuxième plus tard en **LAN segment**



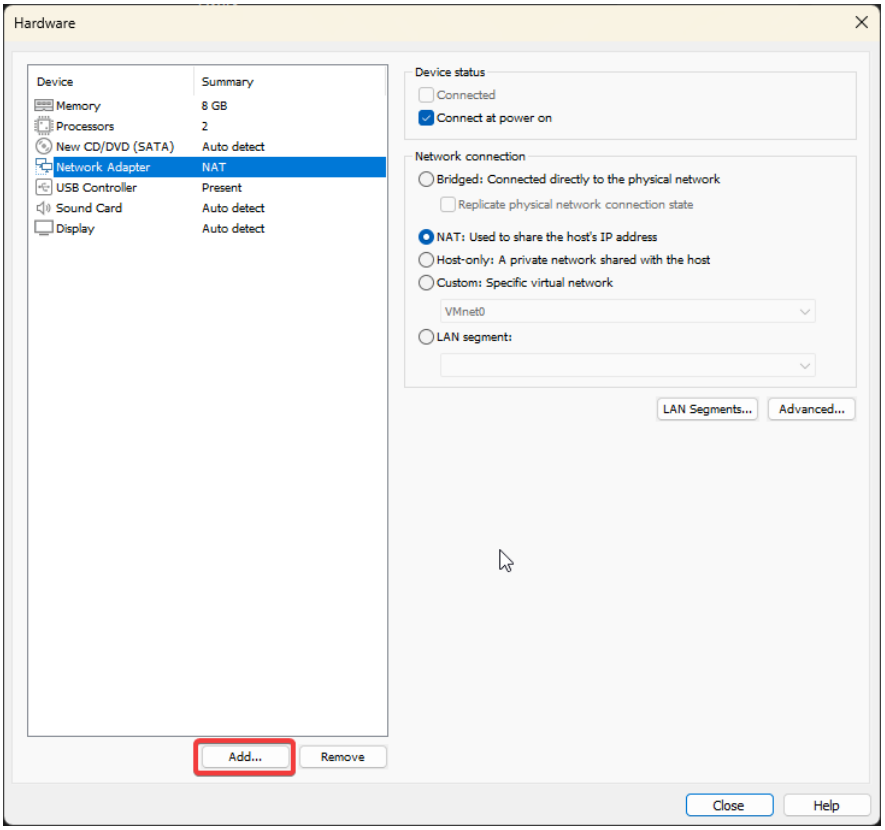
Ici je sélectionne **60GB** pour l'espace disque, ce qui suffira amplement



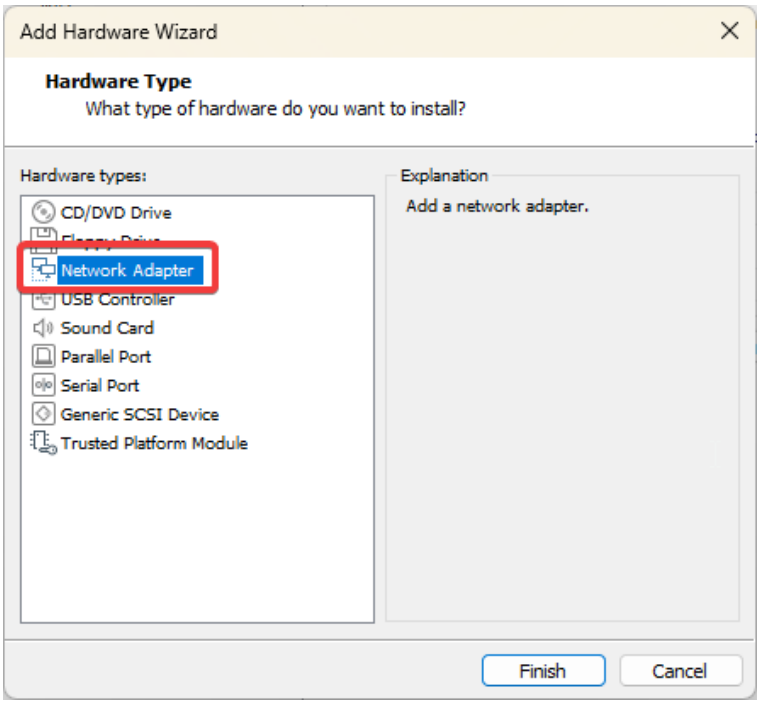
Ensuite étape très importante, ici je sélectionne **Customize Hardware** pour ajouter une autre carte réseau



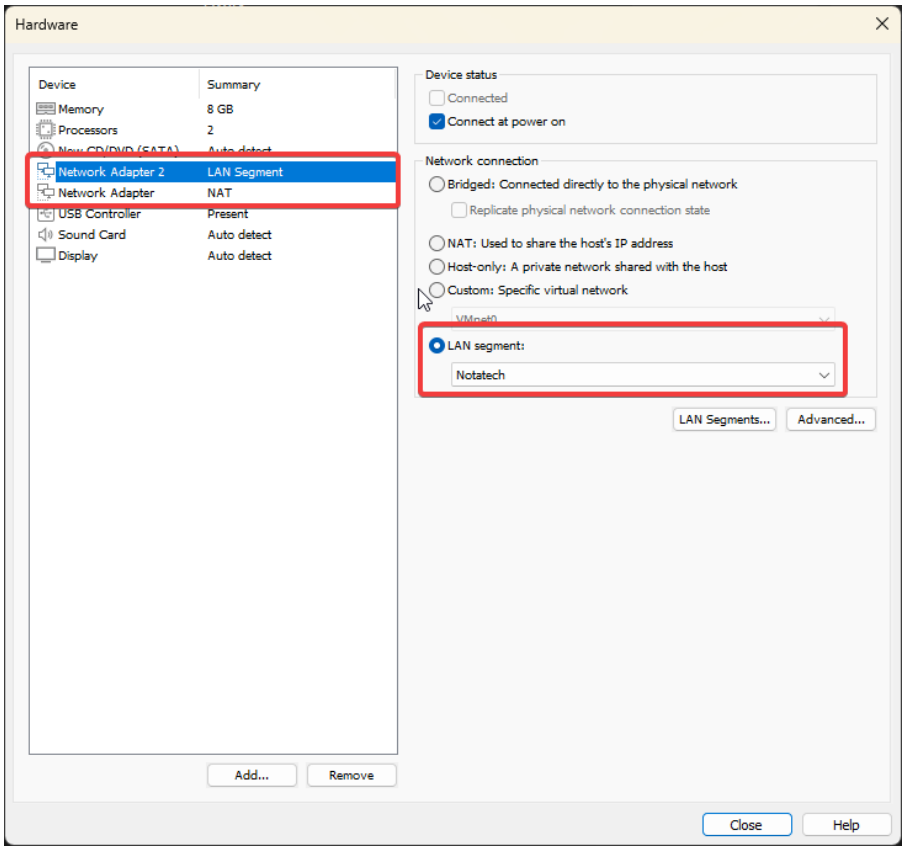
Ensuite ici je clique sur **Add**



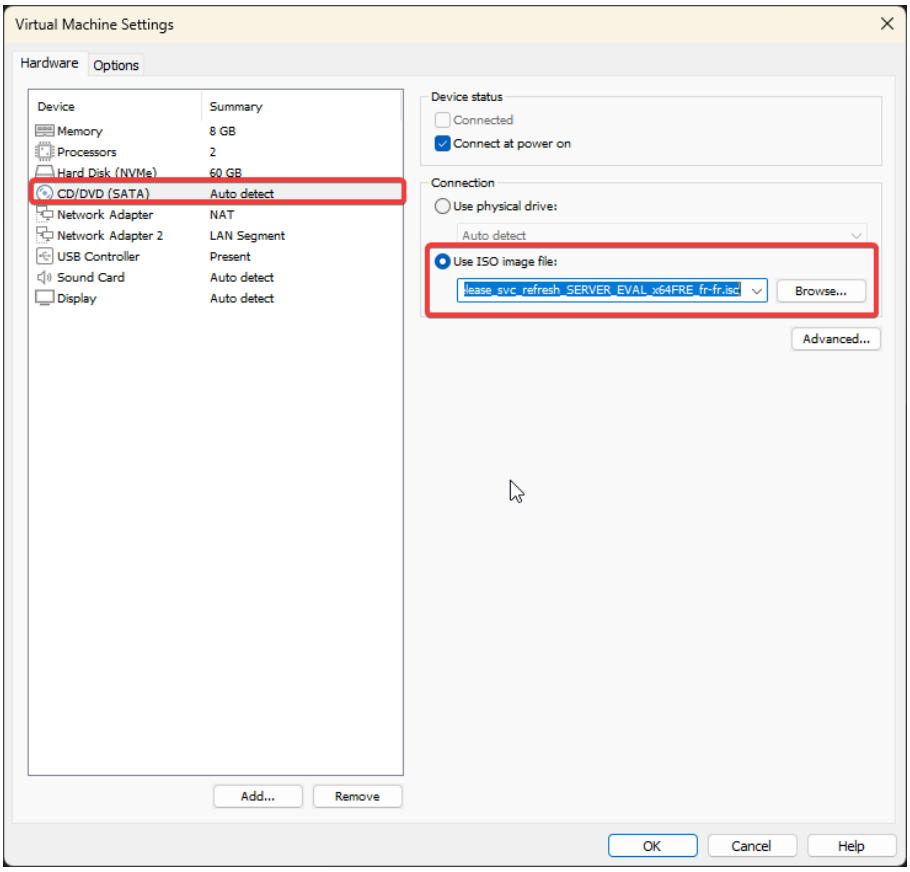
Je sélectionne **Network Adapter** pour ajouter une autre carte réseau a mon serveur



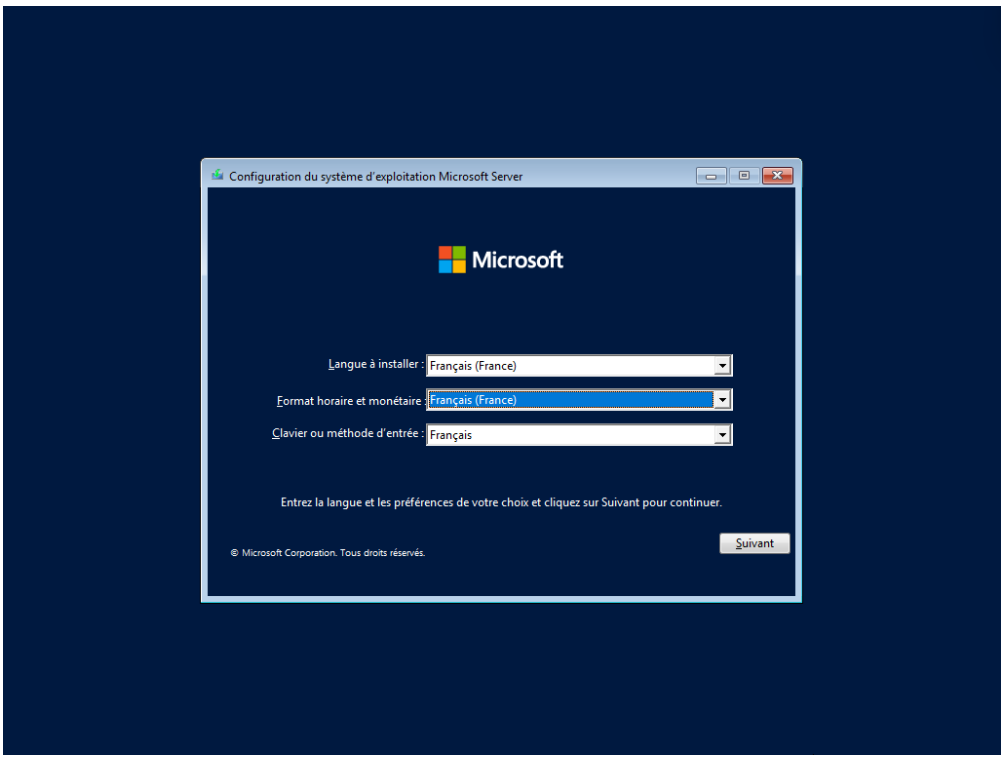
Et je met cette carte en **LAN Segment** et je la met sur le segment **Notatech**, pour que la machine soit directement liée a mon réseau



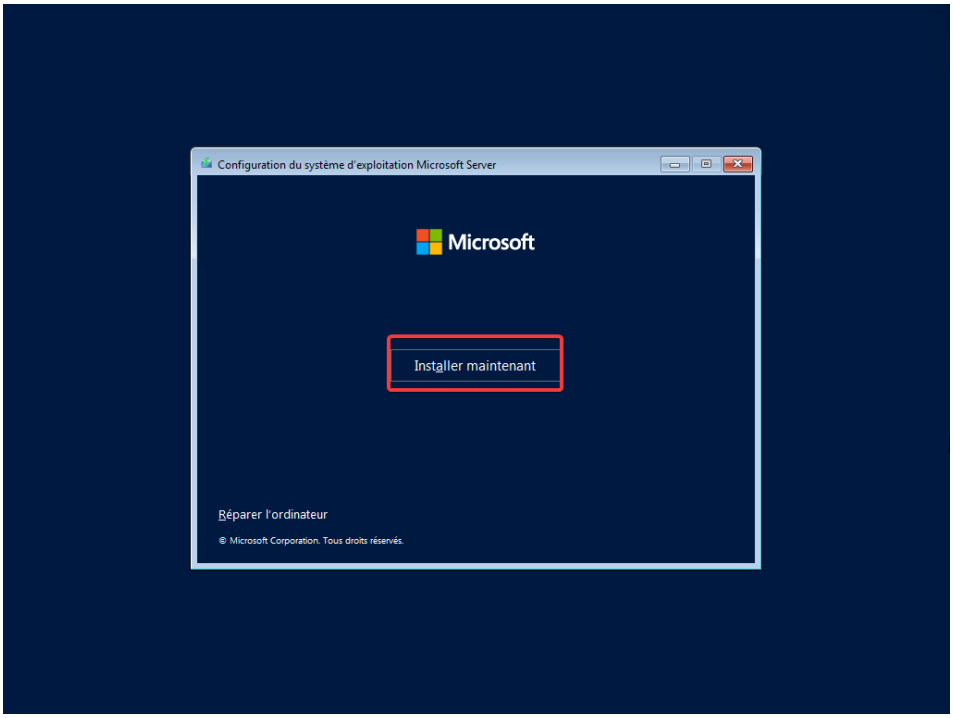
Et finalement je sélectionne l'Iso de mon **Windows server** et démarre ma machine pour débuter l'installation.



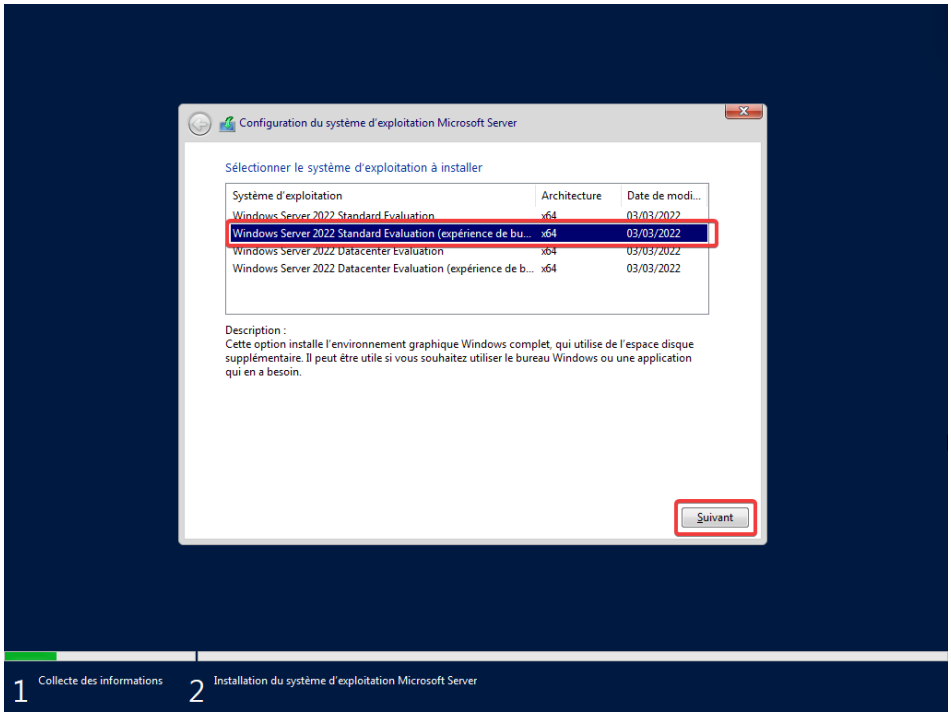
Je démarre donc mon 2ème serveur et suis ces étapes comme nous l'avons fait toute à l'heure



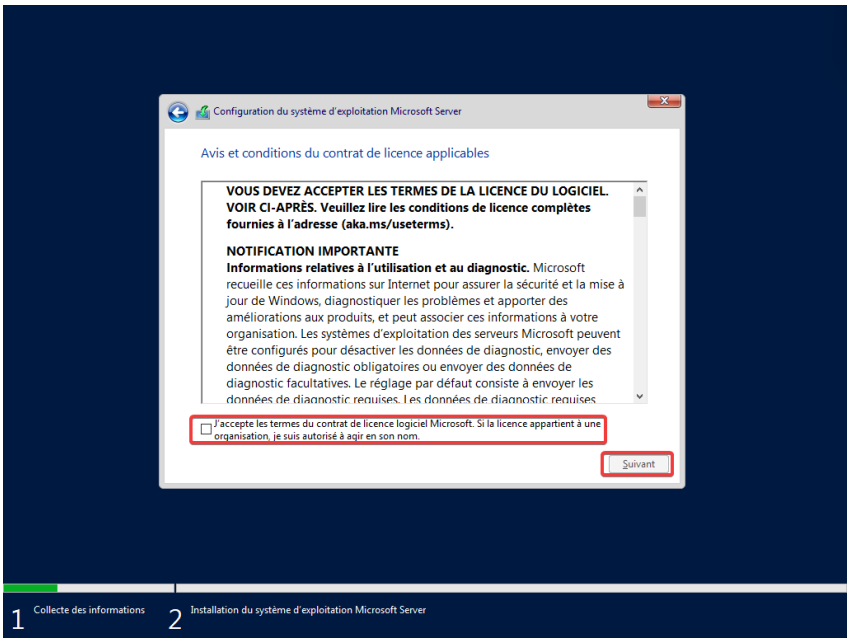
Je clique ici sur **« installer maintenant »**



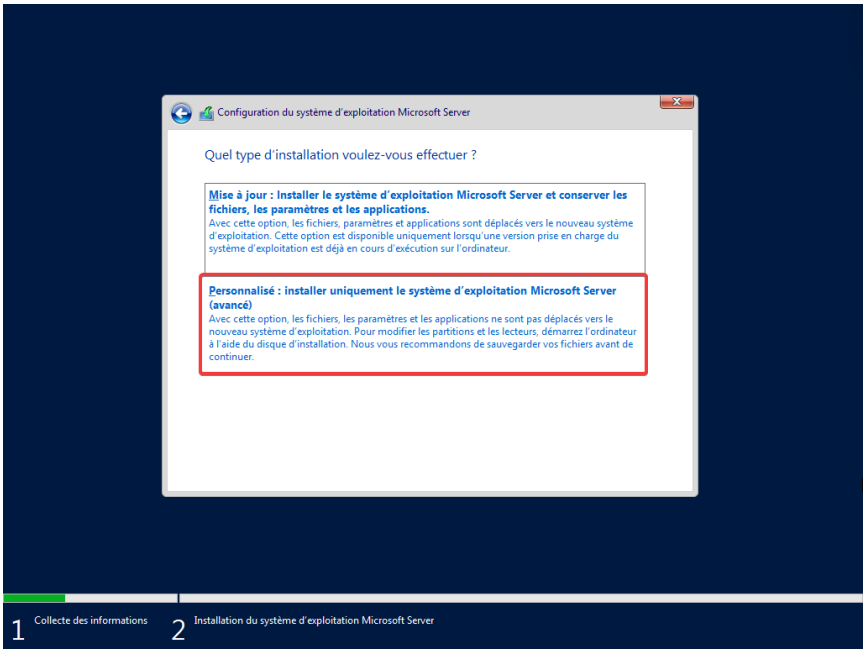
Pour ce qui est du système d'exploitation je sélectionne la 2ème option comme mon premier serveur, Windows server 2022 standard (expérience de bureau)



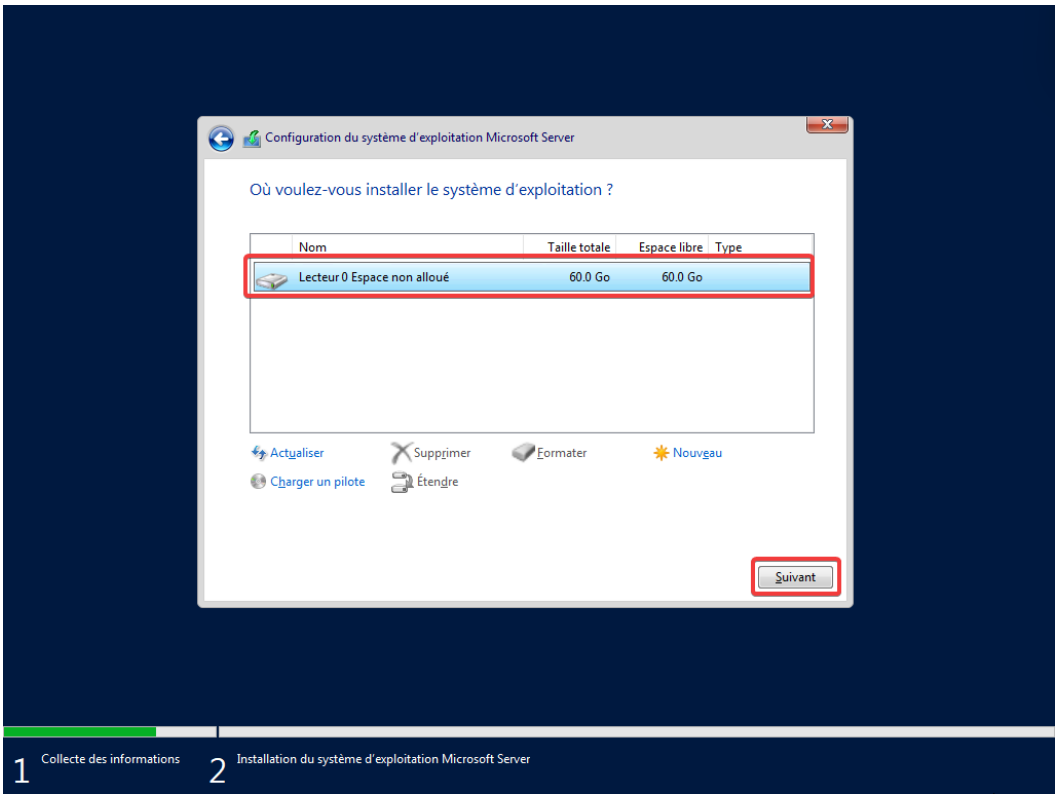
Ensuite j'accepte les conditions d'utilisation de l'applicable



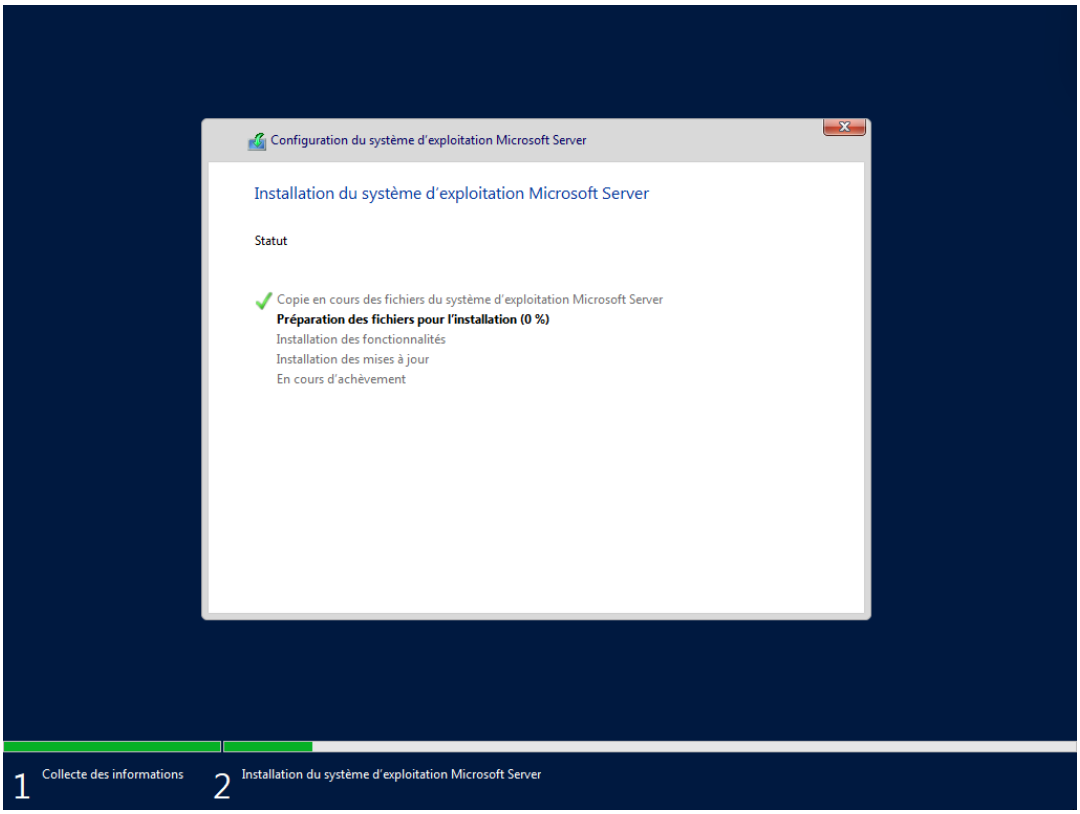
Pour le type d'installation je sélectionne « personnalisé »



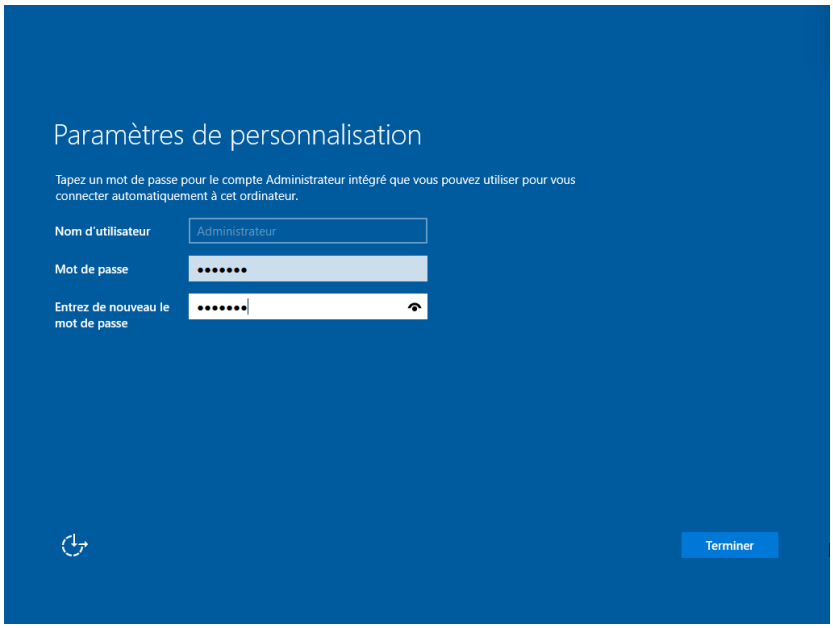
Je sélectionne mon disque et clique sur suivant

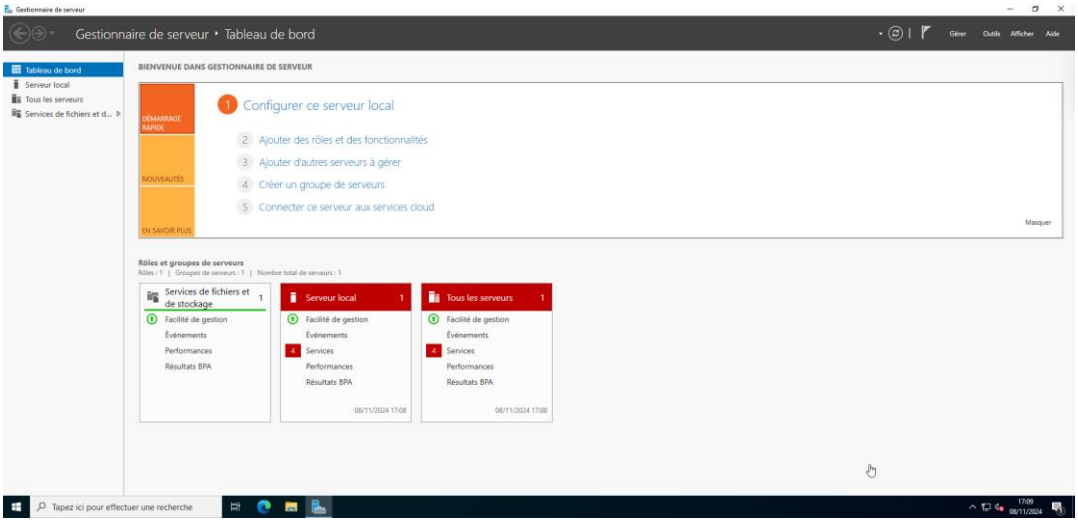


Et l'installation de notre système va finalement se lancer



Ensuite une fois la machine installée je créer le compte administrateur de la machine



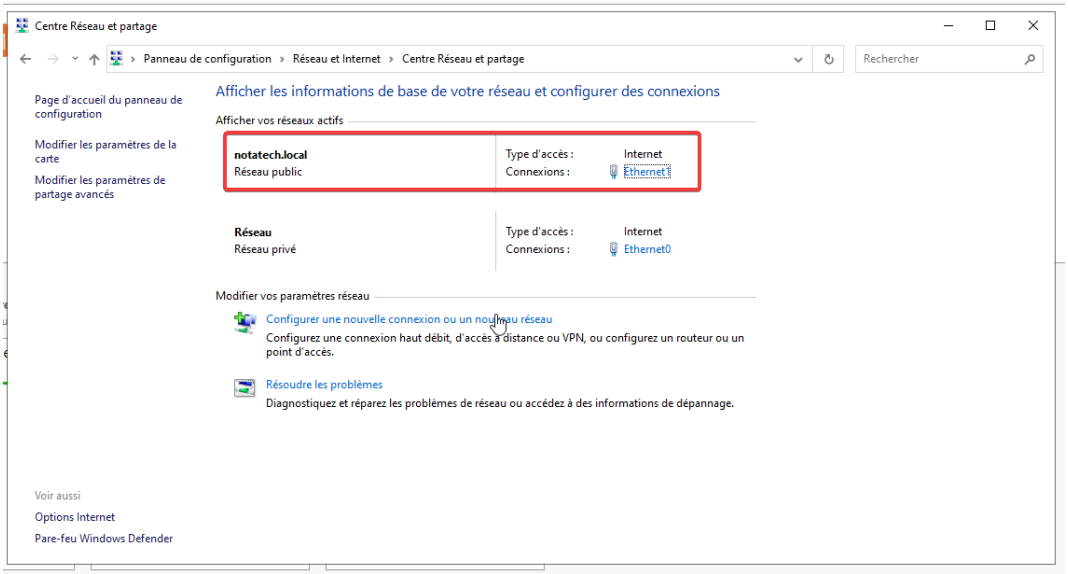


Et voilà nous avons finalement notre 2ème machine de créé et prête à être configurée

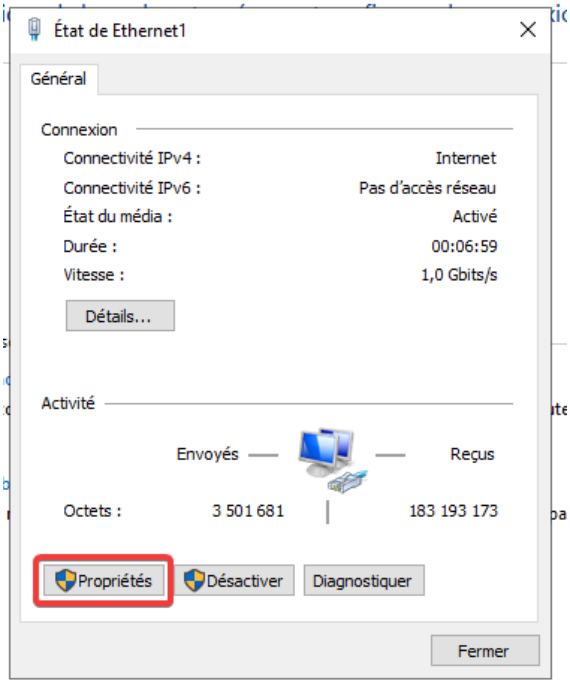
Configuration du 2ème Windows server :

Dans cette étape nous allons commencer la configuration de notre 2ème serveur pour ensuite configurer la redondance de celui-ci

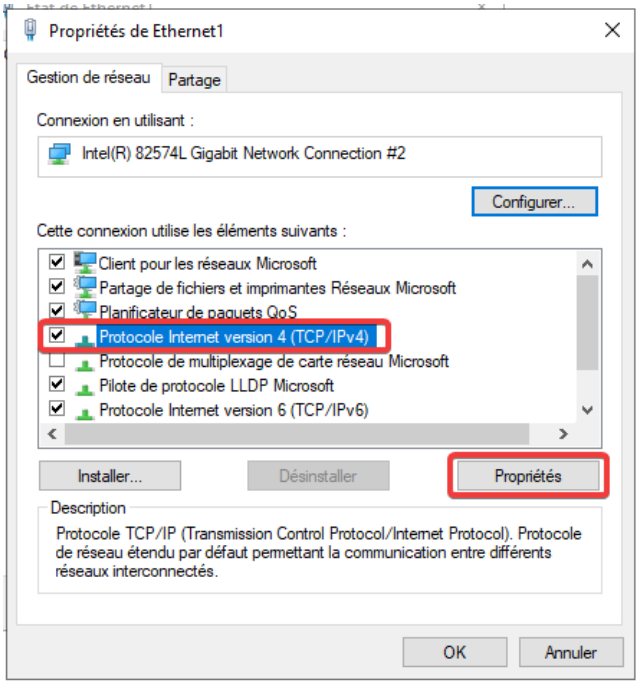
Je commence tout d'abord par configurer mon Windows server en IP fixe, pour cela je me rend dans le panneau de configuration, centre réseau et partage et je clique ici sur ma carte en LAN sur « Ethernet 1 »



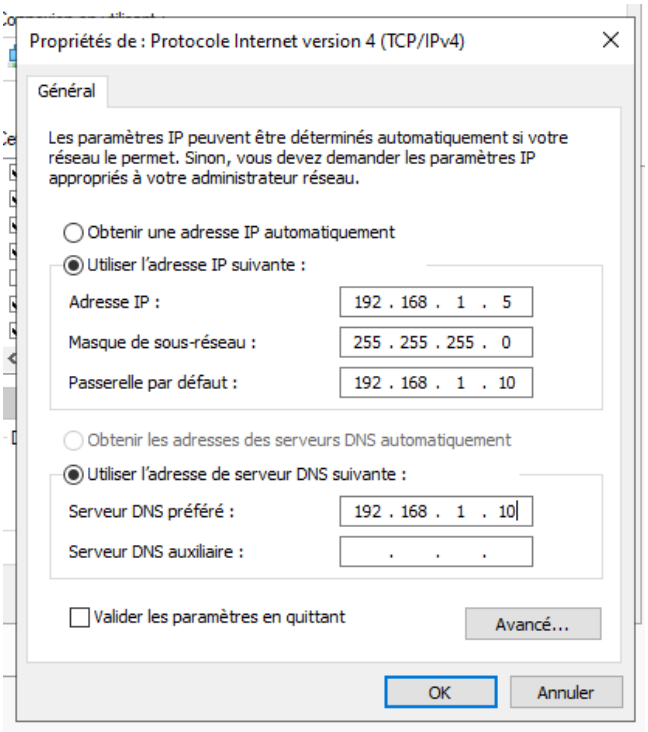
Ensuite je clique sur propriétés pour configurer mon IP fixe



Je clique ici sur « protocole internet version 4 (TCP/IPV4) et propriétés



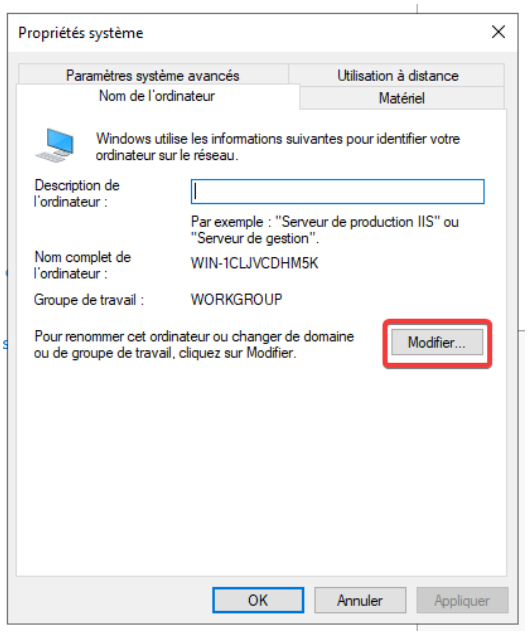
J'arrive finalement sur cette page ou je sélectionne « utiliser l'adresse IP suivante » et je configure mon serveur en 192.168.1.5/24 avec la passerelle 192.168.1.10 qui correspond a l'adresse de mon premier serveur



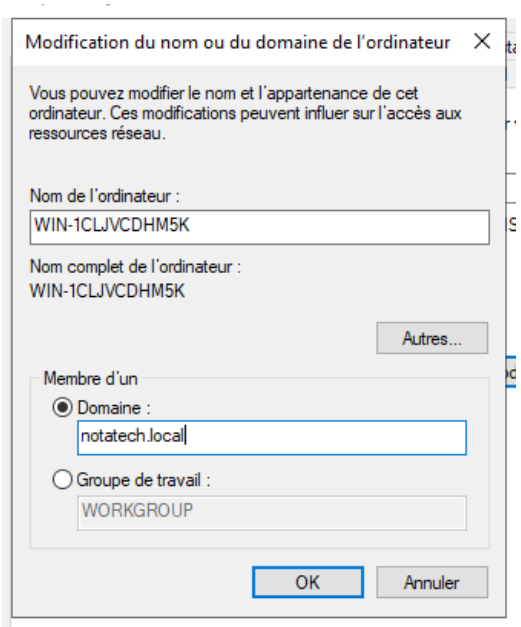
Changement du nom et intégration dans le domaine :

Comme pour la configuration de ma machine cliente ici on va l'intégrer au domaine « notatech.local »

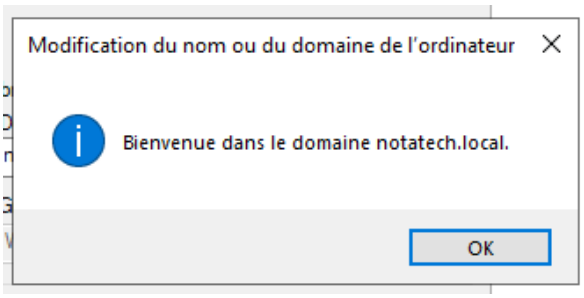
Pour ce faire je me rends dans les propriétés système je clique ici sur « modifier »



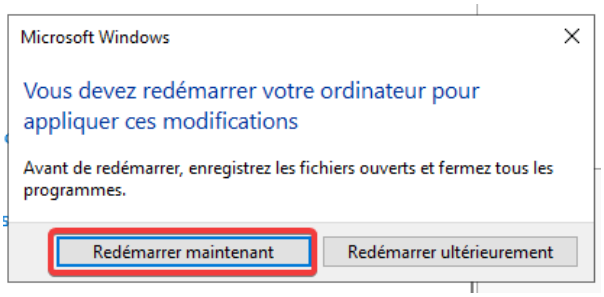
Ici dans domaine je rentre « notatech.local » et je clique ensuite sur OK



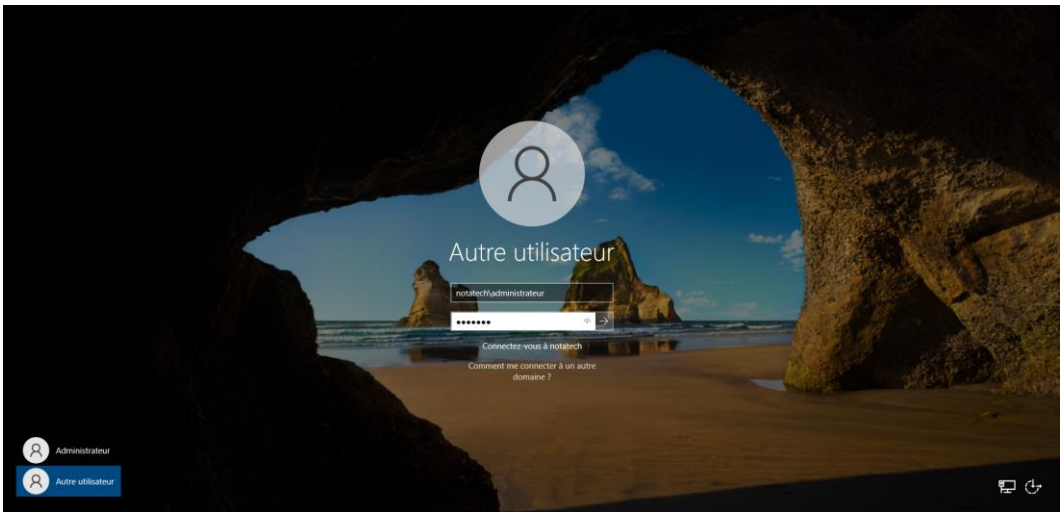
Ce message apparait m'indiquant que ma machine est bien intégrée au domaine donc tout est bon



Ensuite je clique sur « redémarrer maintenant » pour redémarrer mon serveur et qu'il prenne bien en compte les modifications apportées



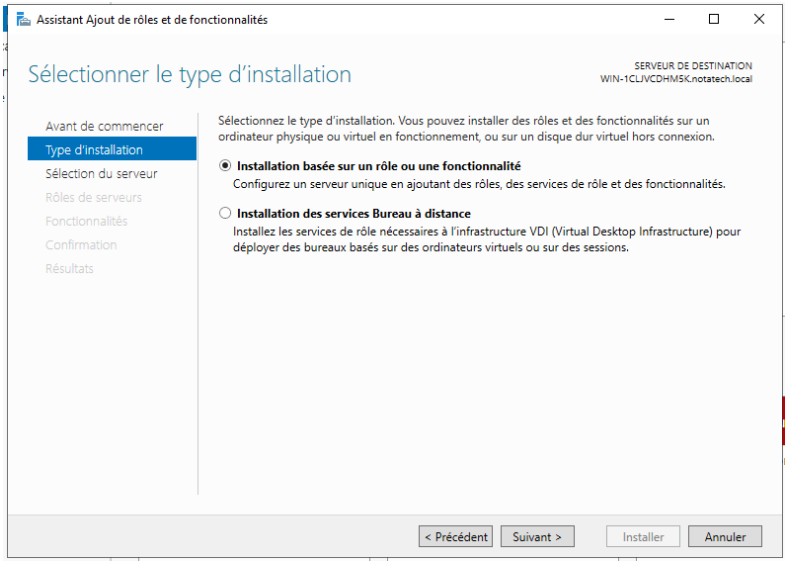
Je peux bien me connecter avec mon domaine, donc tout est bon au niveau de la liaison avec le domaines



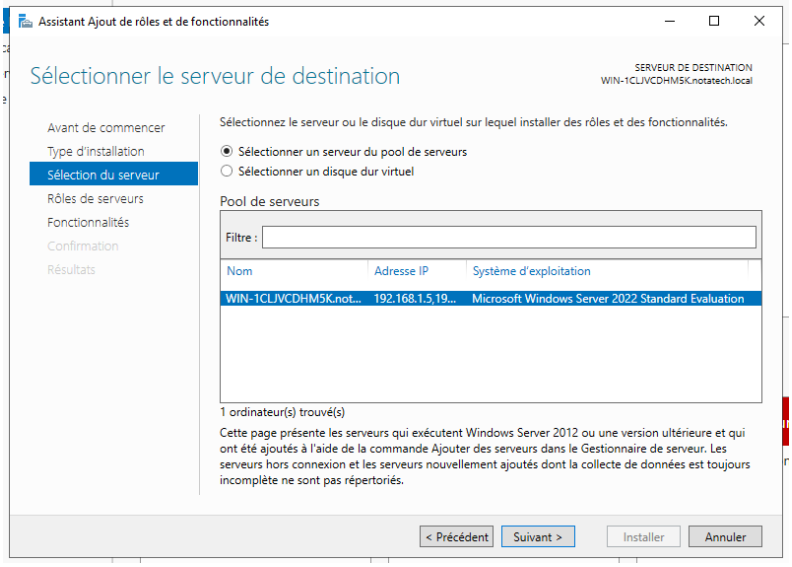
Installation des rôles AD DS sur le 2ème serveur :

Pour commencer cette installation je me rend d'abord sur le gestionnaire de serveur et vais dans « gérer » et clique sur « ajouter des rôles et fonctionnalités »

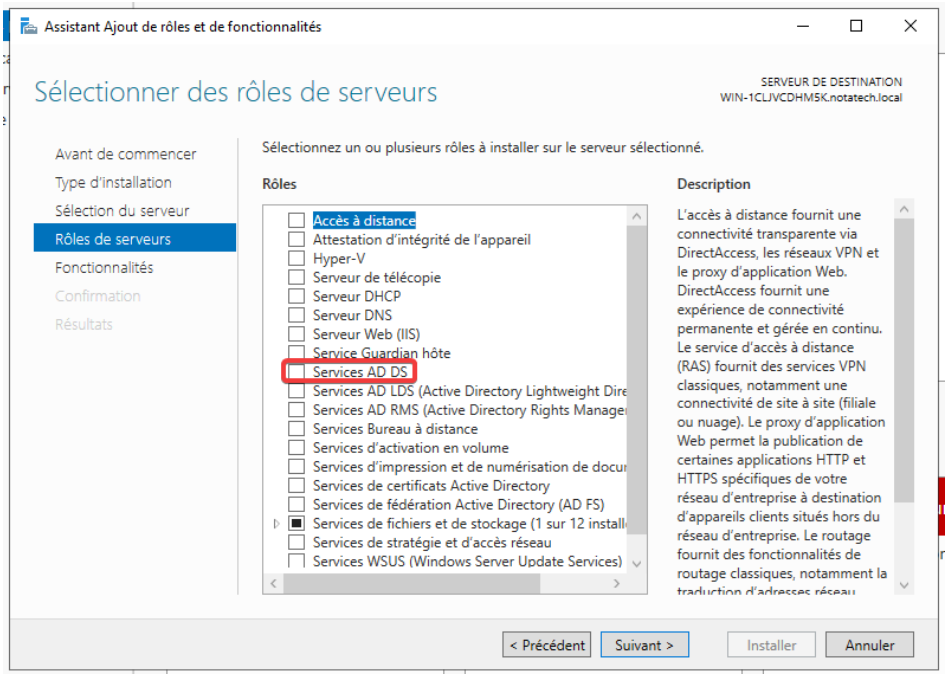
Ici je sélectionne « installation basée sur un rôle ou une fonctionnalité », suivant



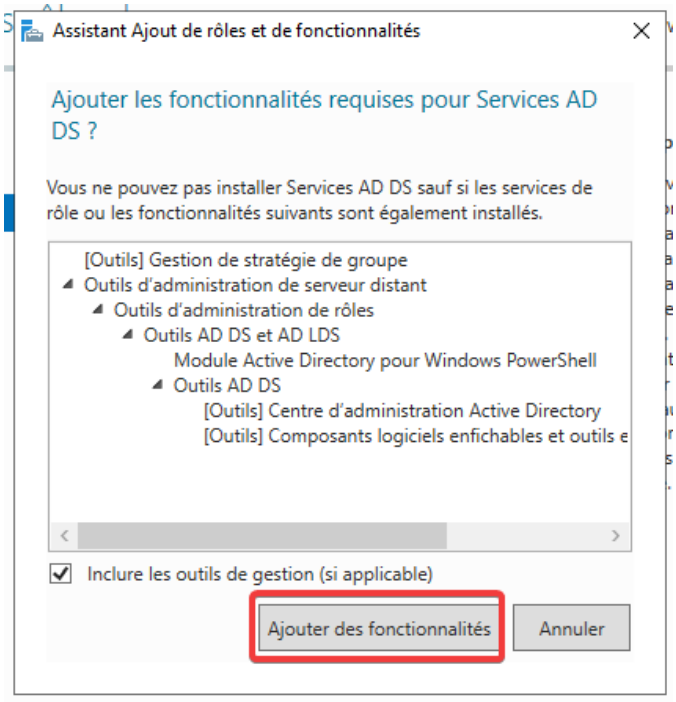
Ici je sélectionne donc mon serveur et fait suivant



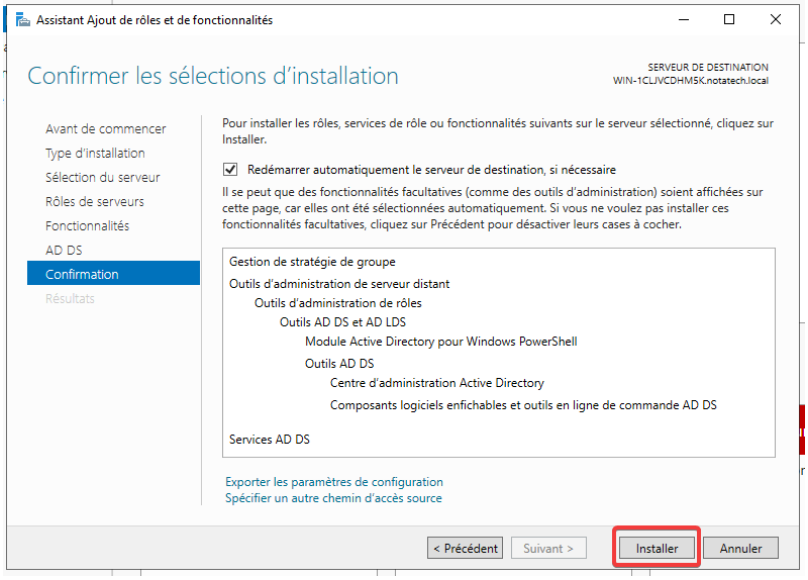
Pour les rôles de serveurs je sélectionne « Services AD DS »



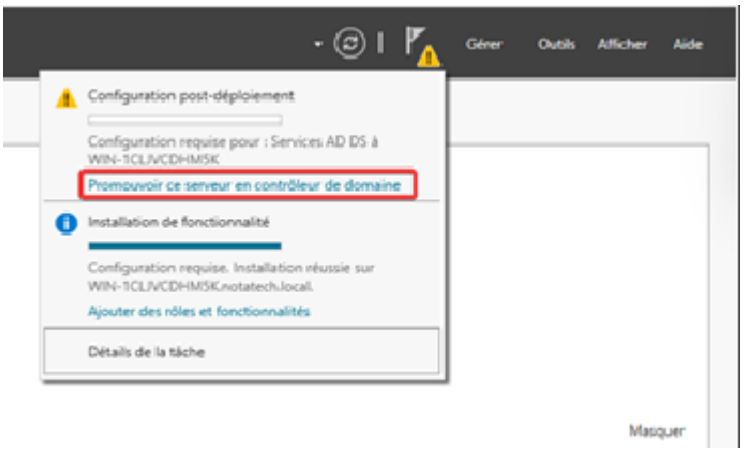
Je clique ici sur « Ajouter des fonctionnalités » et passe a la suite



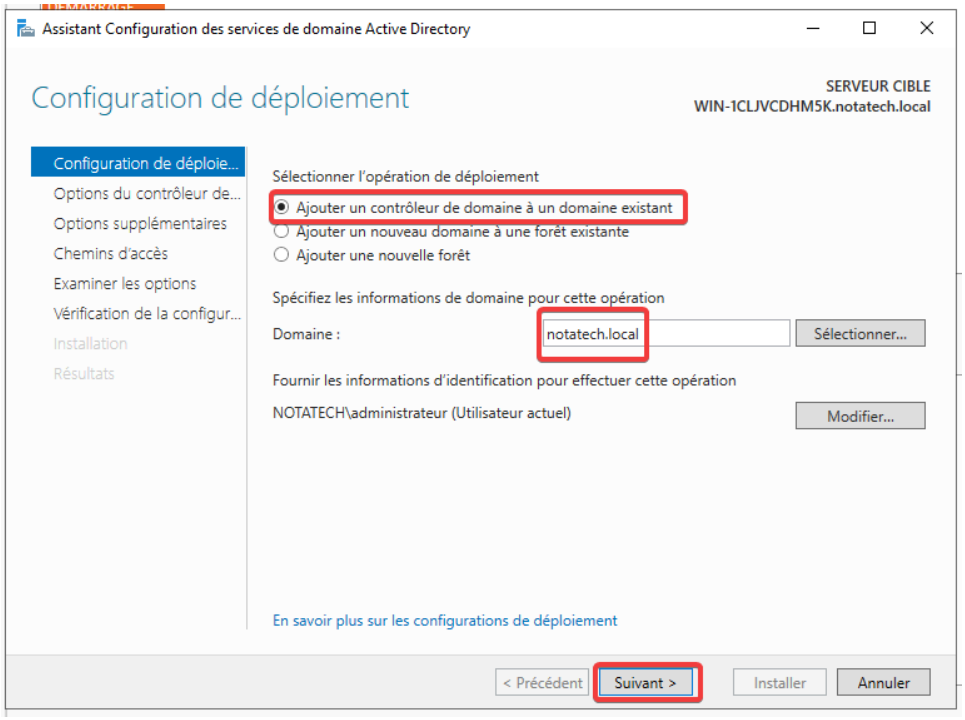
Ensuite je laisse les paramètres par défaut pour la suite et démarre l'installation



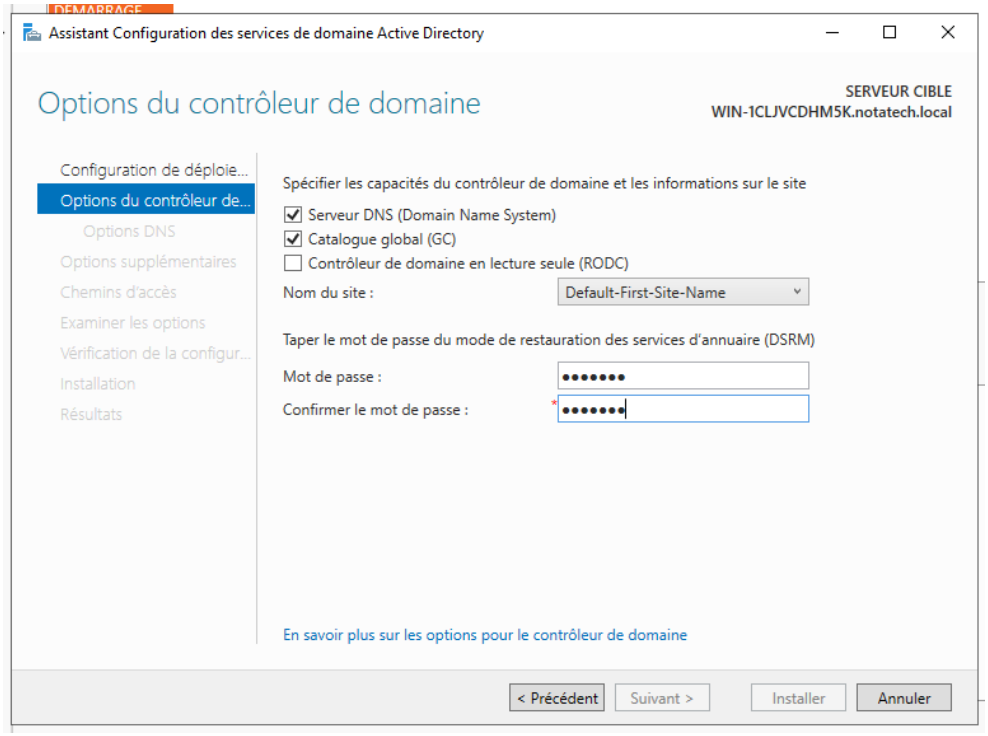
Ensuite une fois ceci installé, je vais **promouvoir ce serveur en contrôleur de domaine**, pour ce faire sur le tableau de bord je clique sur le drapeau, on voit cette notification qui nous propose de promouvoir ce serveur en contrôleur de domaine, je clique donc sur « promouvoir ce sevreur en controleur de domaine »



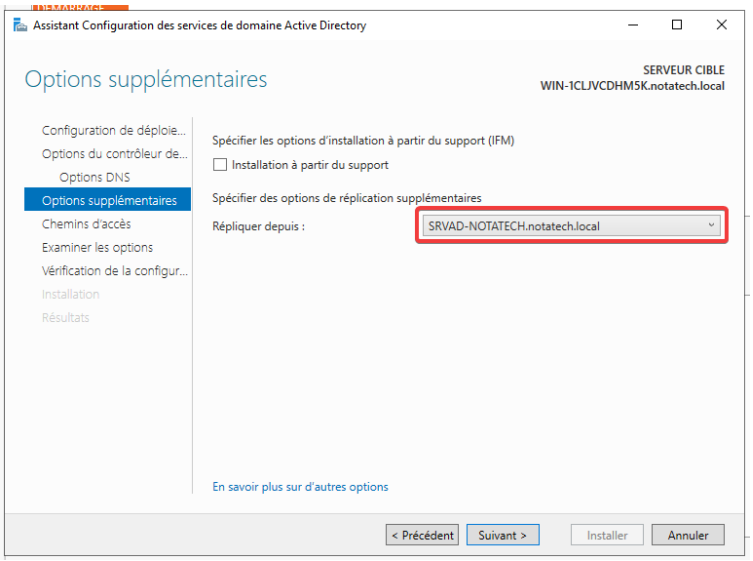
Ensuite ici vu qu'on configure notre 2ème serveur notre forêt est déjà créé, donc nous allons tout simplement ajouter notre contrôleur de domaine au domaine **notatech.local,** je sélectionne donc « ajouter un contrôleur de domaine à un domaine existant et j'écris **notatech.local.**



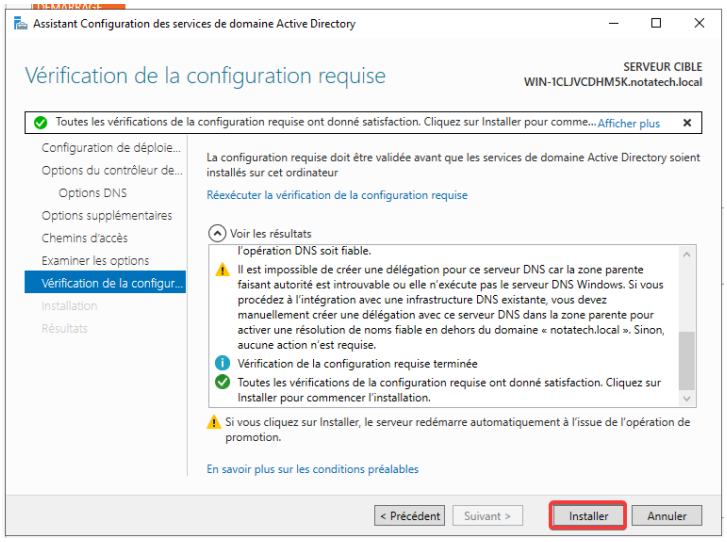
Ici je sélectionne un mot de passe pour le **mode de restauration des services d'annuaires**.



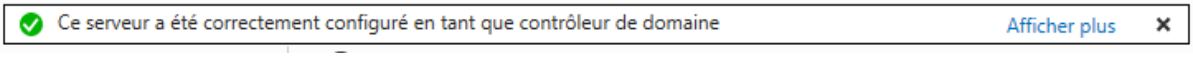
Ici arrivé à la section « options supplémentaires » je fais attention a bien **sélectionner mon premier serveur** car c'est grâce a ce paramètre que la réplication va se faire.



J'arrive finalement au dernier paramètre et je clique sur **installer**.



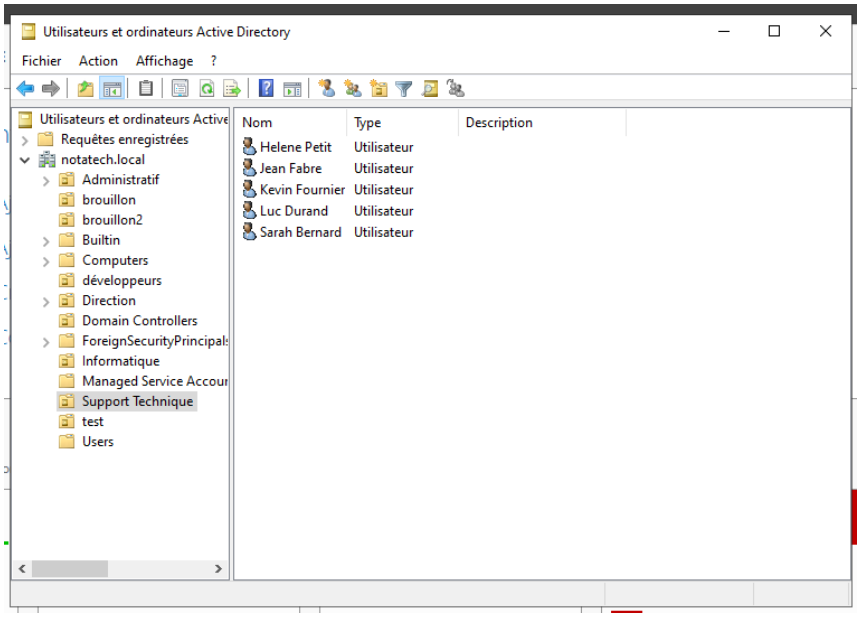
Cette petite banderole va finalement apparaitre et nous confirme que le serveur a été **correctement configuré en tant que contrôleur de domaine**.



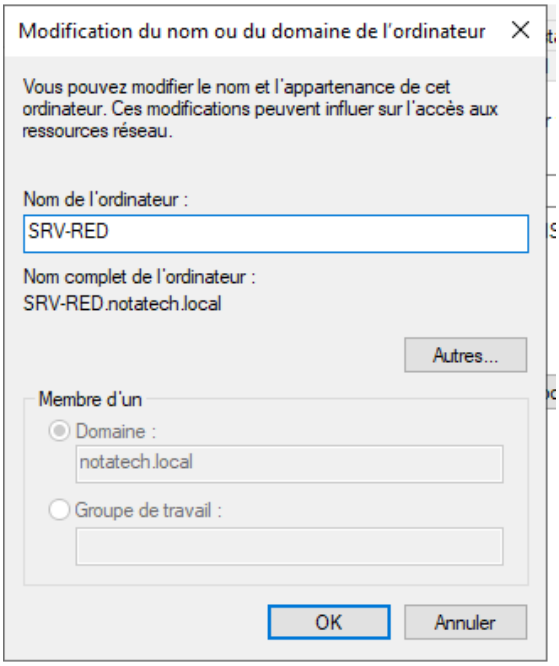
Activation et vérification de la redondance :

Ici dans cette partie je vais faire la réplication et les vérifications que ma redondance fonctionne bien

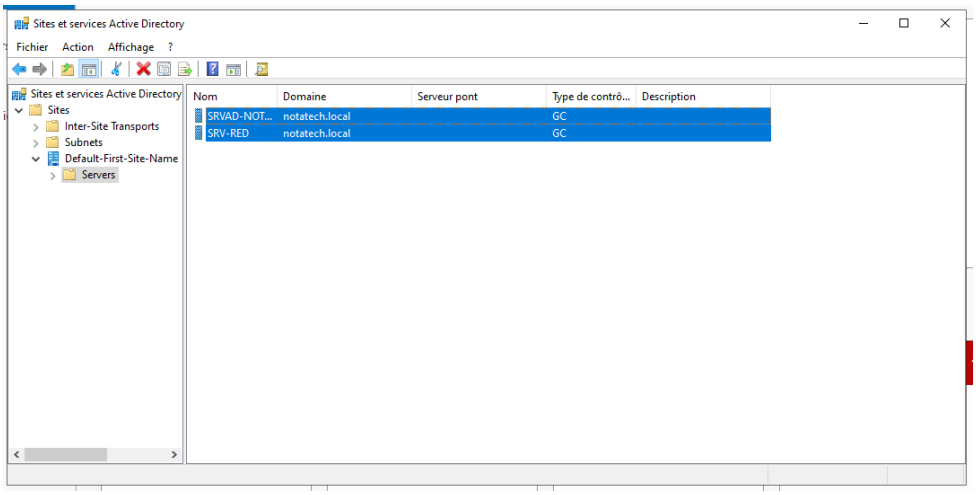
Je commence d'abord par vérifier dans ma console d'utilisateurs et ordinateurs Active Directory que mes utilisateurs et unité d'organisation ont bien été répliqués, c'est bien le cas comme nous pouvons le voir.



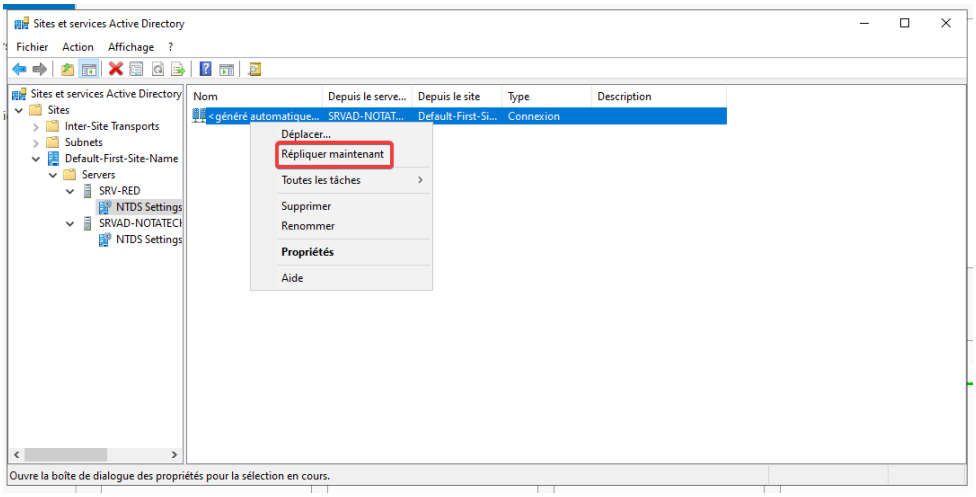
Je commence d'abord par **renommer mon serveur**, je le renomme ici en **« SRV-RED »** pour l'identifier facilement lors de la réplication.



Nous allons maintenant faire la **réplication**, je me rend dans **« Sites et services Active Directory »** je vérifie que je vois bien mon serveur AD principal et celui prévu pour la redondance



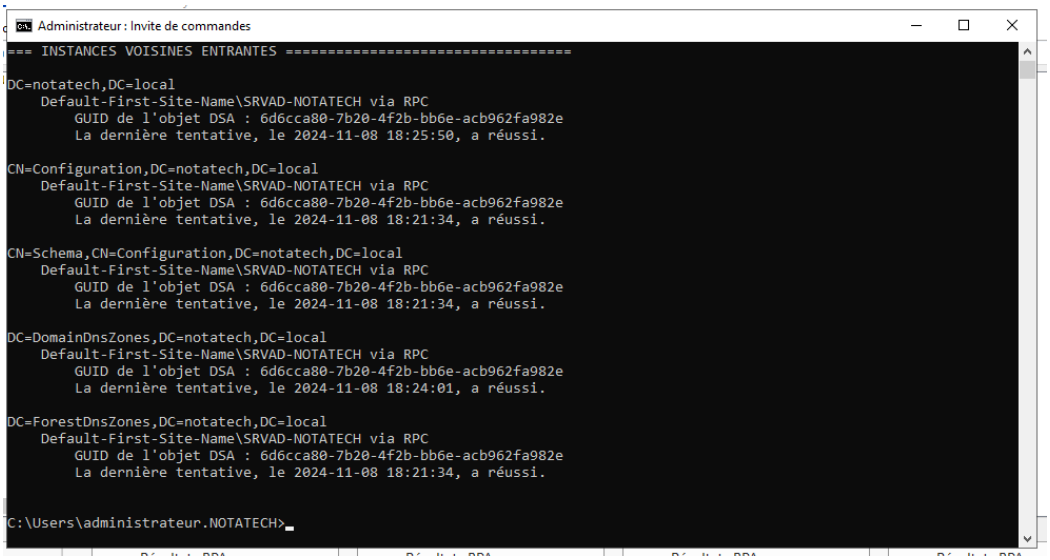
Je me rends ensuite dans **servers > NTDS settings** et je fais un clique droit sur la connexion affichée et clique sur **répliquer maintenant**



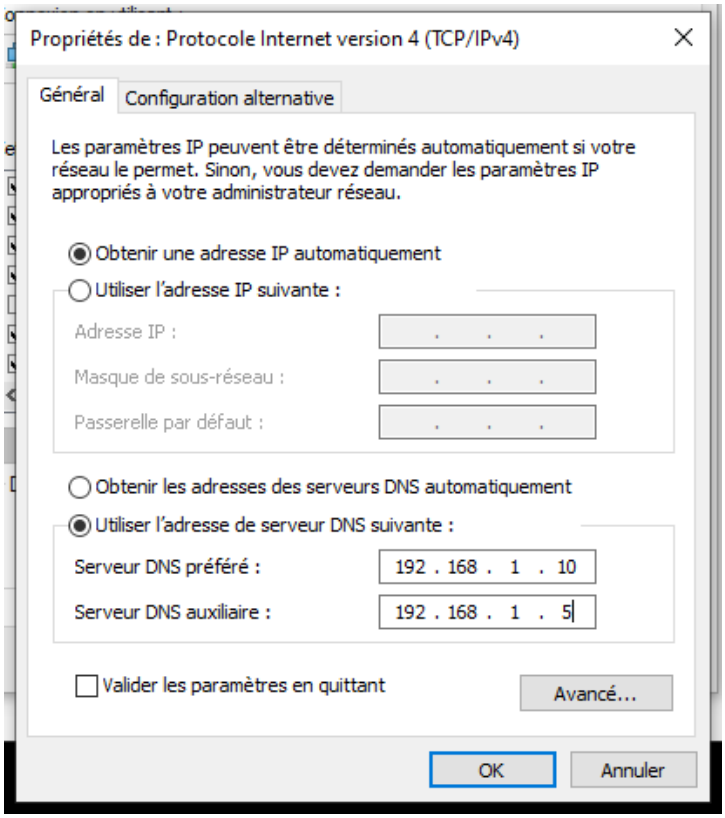
La réplication devrait maintenant fonctionner. Je fais donc cette commande **« repadmin /showrepl »** qui permettra d'afficher l'état de la réplication Active Directory entre les contrôleurs de domaine, indiquant les connexions établies

```
C:\Users\administrateur.NOTATECH>repadmin /showrepl
```

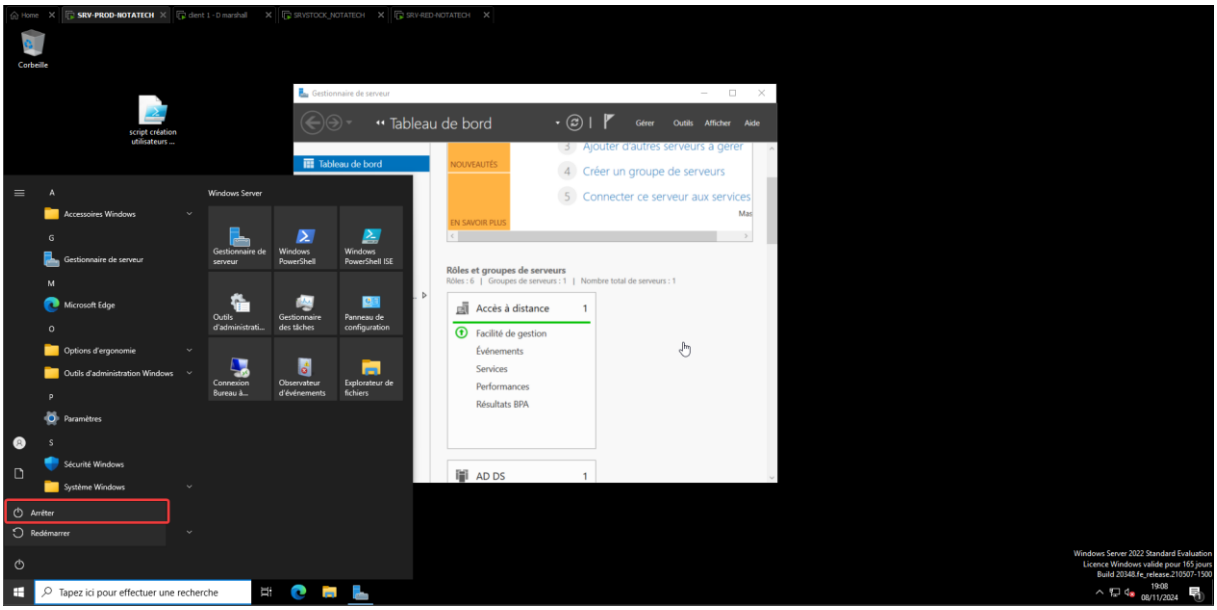
Ceci affichera ces lignes qui nous montre bien que la réplication fonctionne.



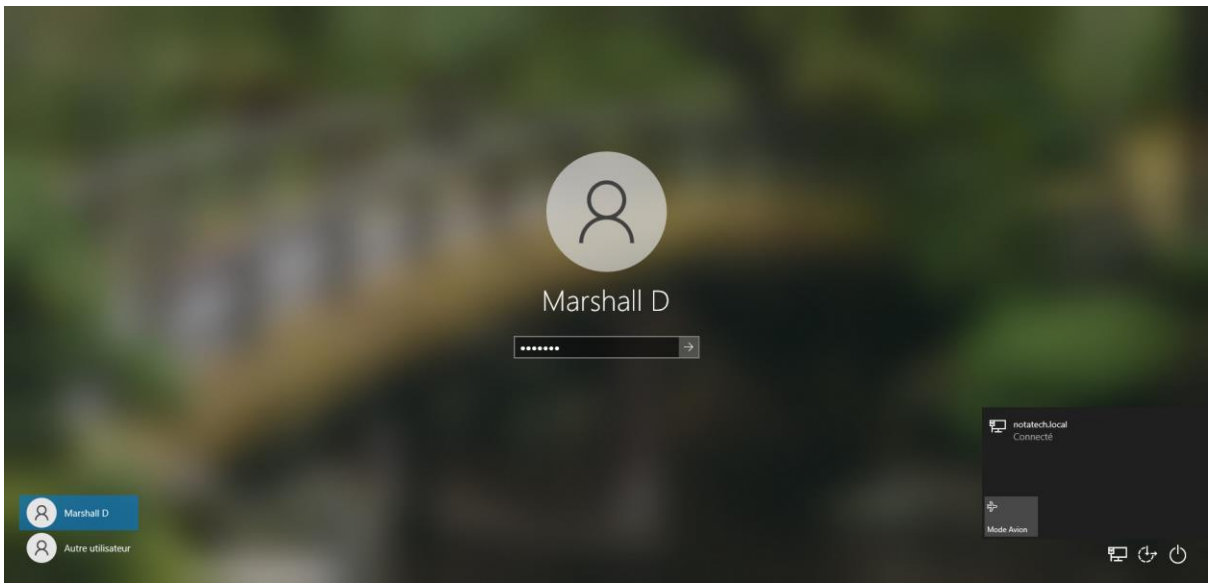
Et finalement nous allons faire le test final pour voir si la réplication fonctionne bien, nous allons éteindre le serveur AD principal **SRV-PROD-NOTATECH** et ensuite je vais essayer de me connecter avec mon ordinateur client a l'utilisateur **D Marshall,** avant ça il faut que je rajoute l'adresse DNS du serveur de redondance en **DNS Auxiliaire**, pour qu'il soit reconnu par les postes (on le rajoutera dans le DHCP plus tard)



Ensuite j'éteins donc mon serveur AD principal **SRV-PROD-NOTATECH**



Ensuite je me connecte donc a ma machine cliente, déjà on voit que la machine a bien récupérée le réseau et reconnait bien le domaine **notatech.local**



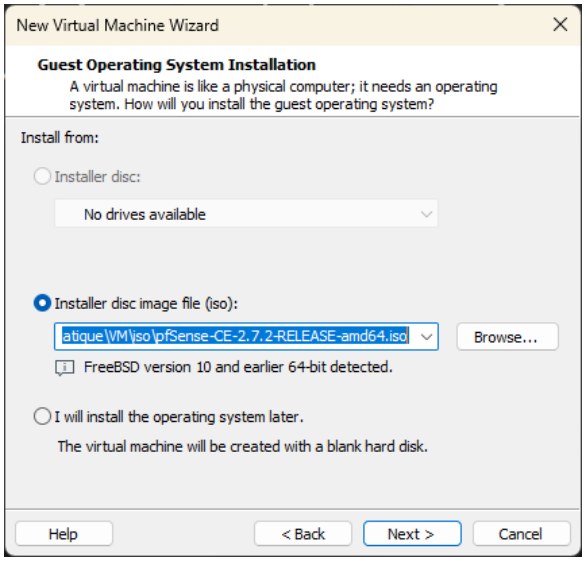
Création du pare feu PfSense :

Dans cette partie nous allons voir la création du pare feu PfSense, qui nous permettra de sécuriser notre réseau en mettant en place un IDS et des ACL

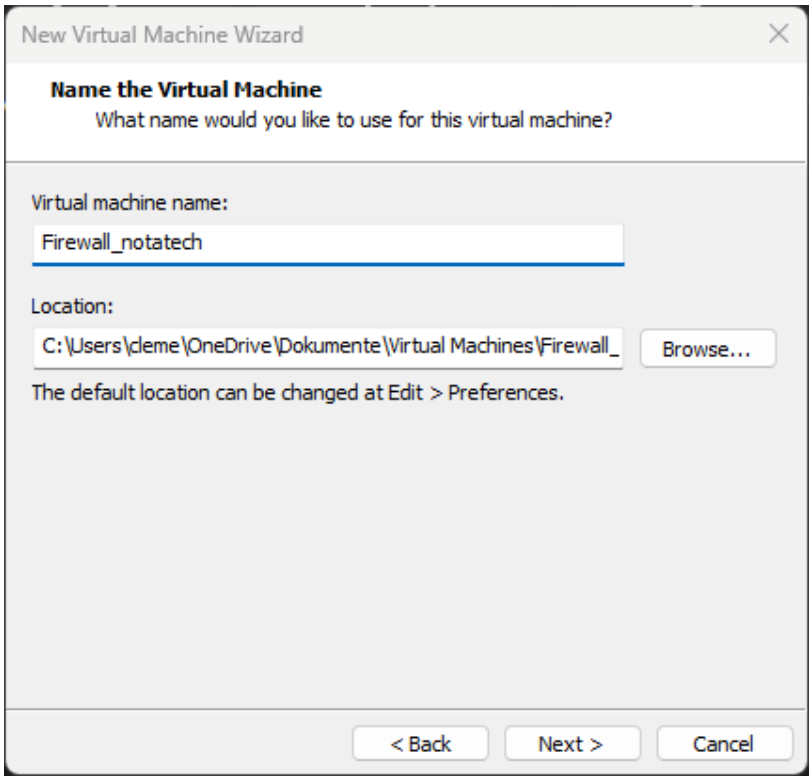
1ère étape : création du pfsense :

Tout d'abord il va falloir créer la VM Pfsense, comme pour les autres machines je me rend sur vmWare et clique sur créer une nouvelle machine et sélectionne « custom »

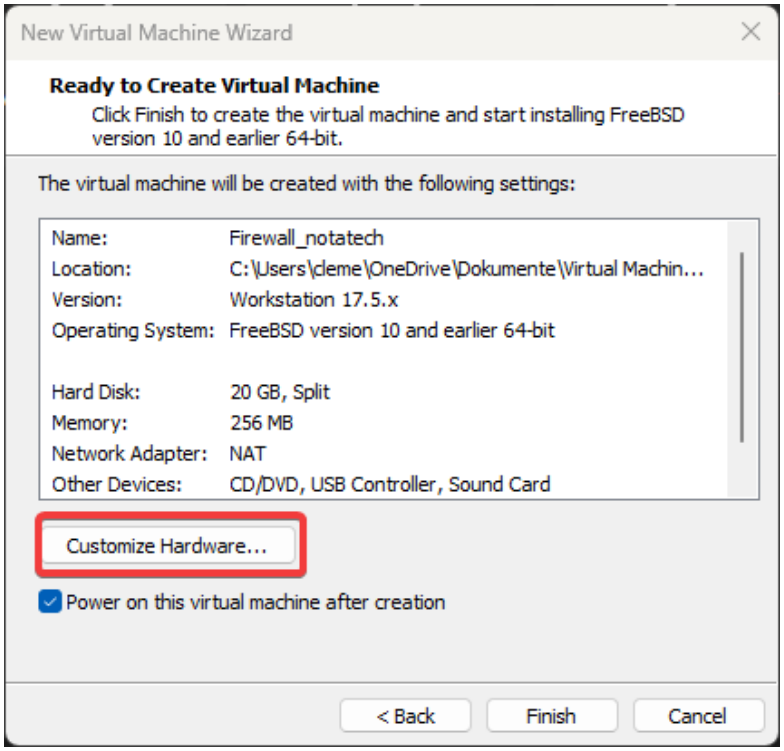
Ensuite ici je sélectionne mon ISO de pfsense et clique sur **suivant**



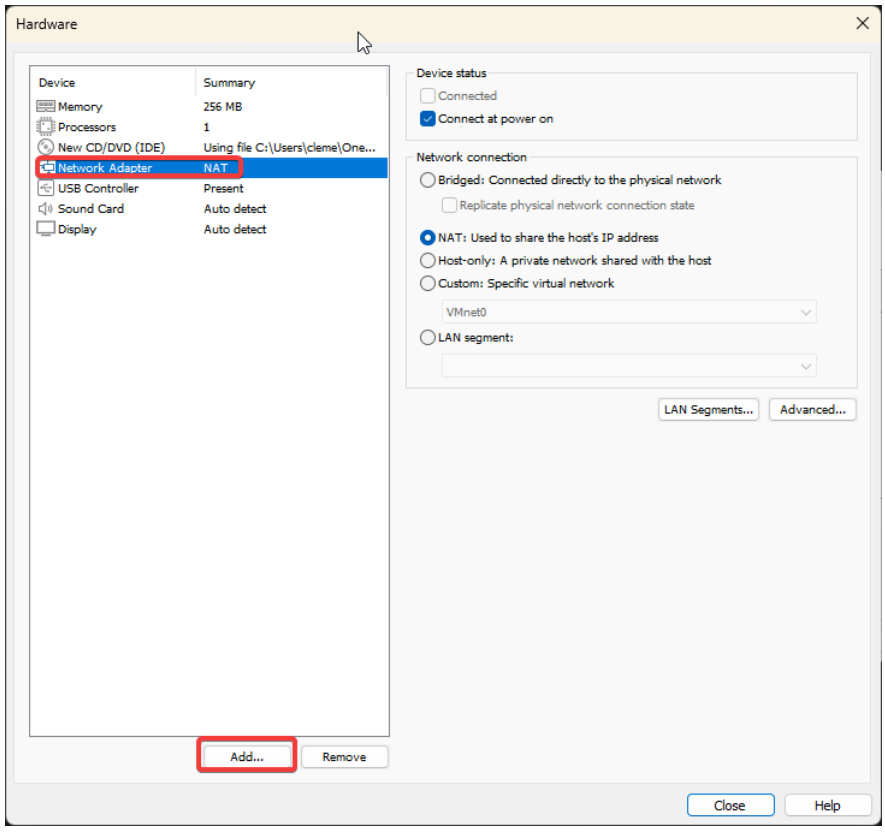
Ensuite, vu que nous sommes en train de faire un pare feu, je nomme ma machine « **Firewall_notatech** »



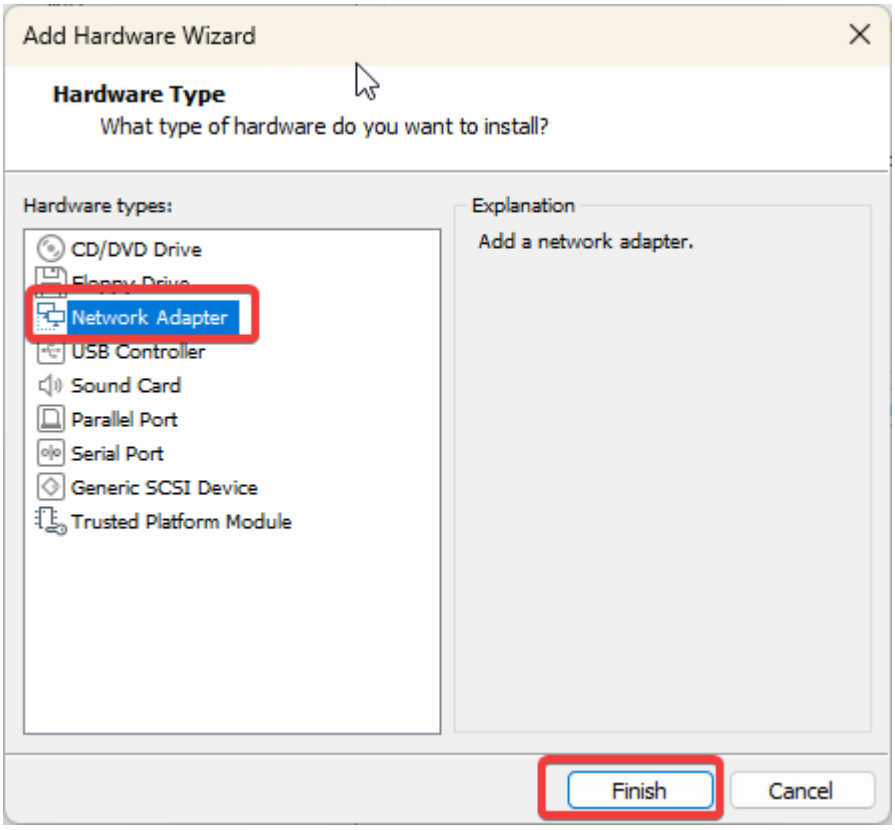
Pour les autres paramètres je les laisse par défaut et arrivé ici je clique sur **« customize hardware »** ici on va ajouter une deuxième carte réseau de manière a en avoir une en NAT et une en LAN segment



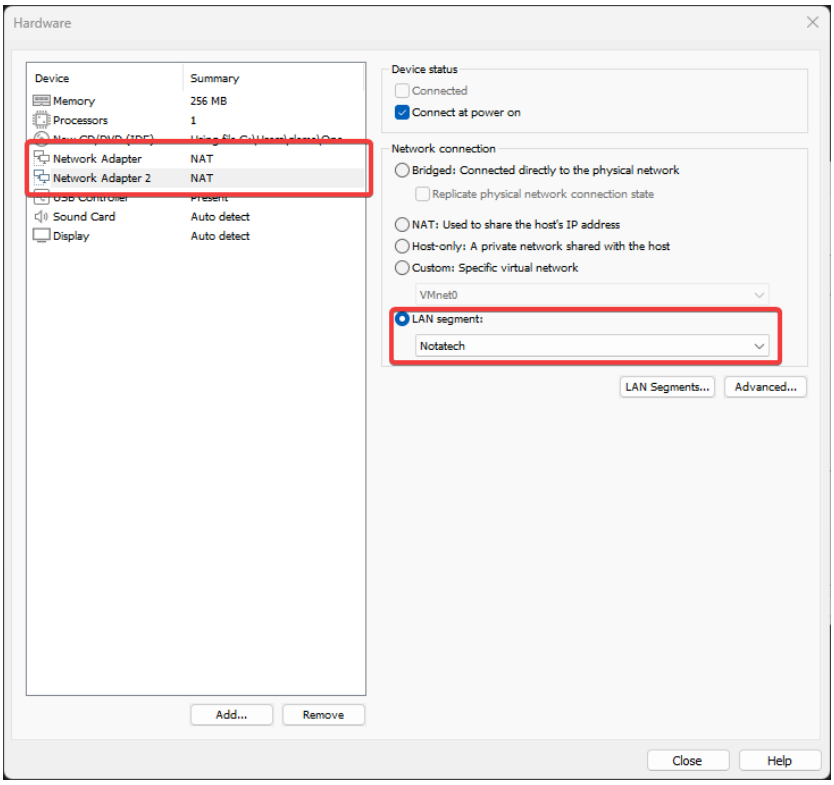
Ici je clique sur « **Add** » pour ajouter un équipement



Ensuite cette page s'ouvrire ou je sélectionne « **network adaptater** » puis **finish**

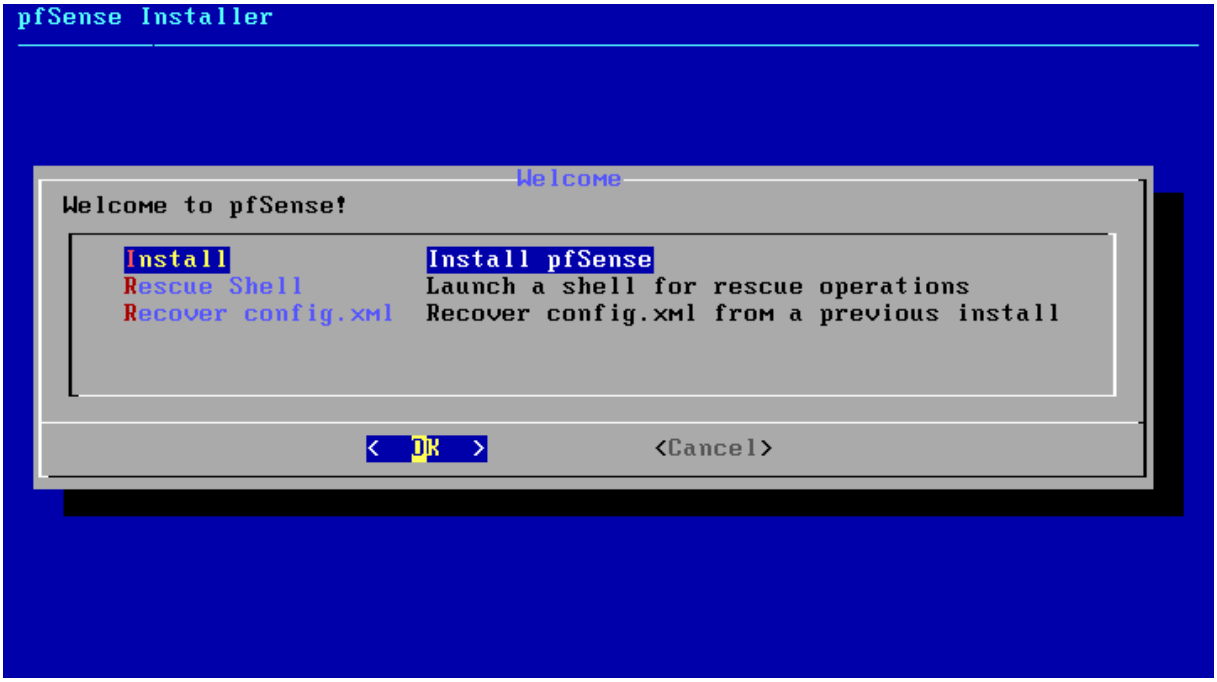


Et finalement je configure cette 2ème carte réseau en LAN segment et la met sur le segment **Notatech**

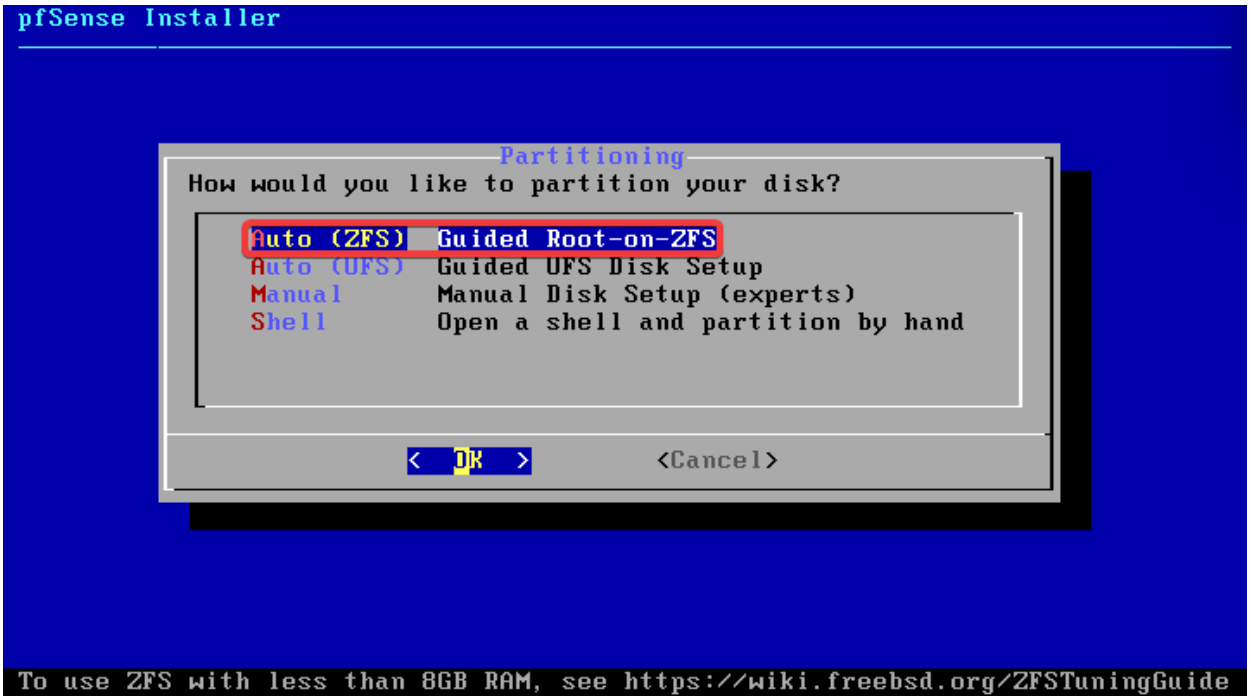


Installation du PfSense :

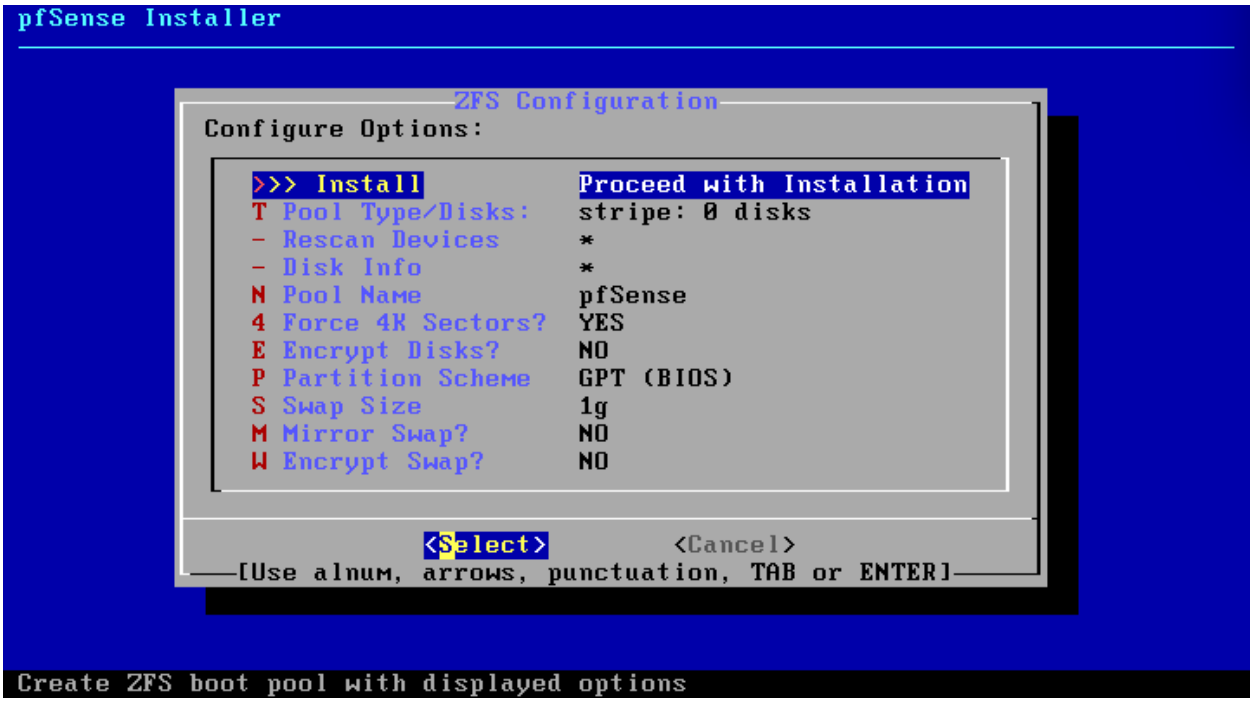
Ici on va passer a la partie installation du système pfsense. Arrivé sur cette première page, je sélectionne **« install PfSense »**



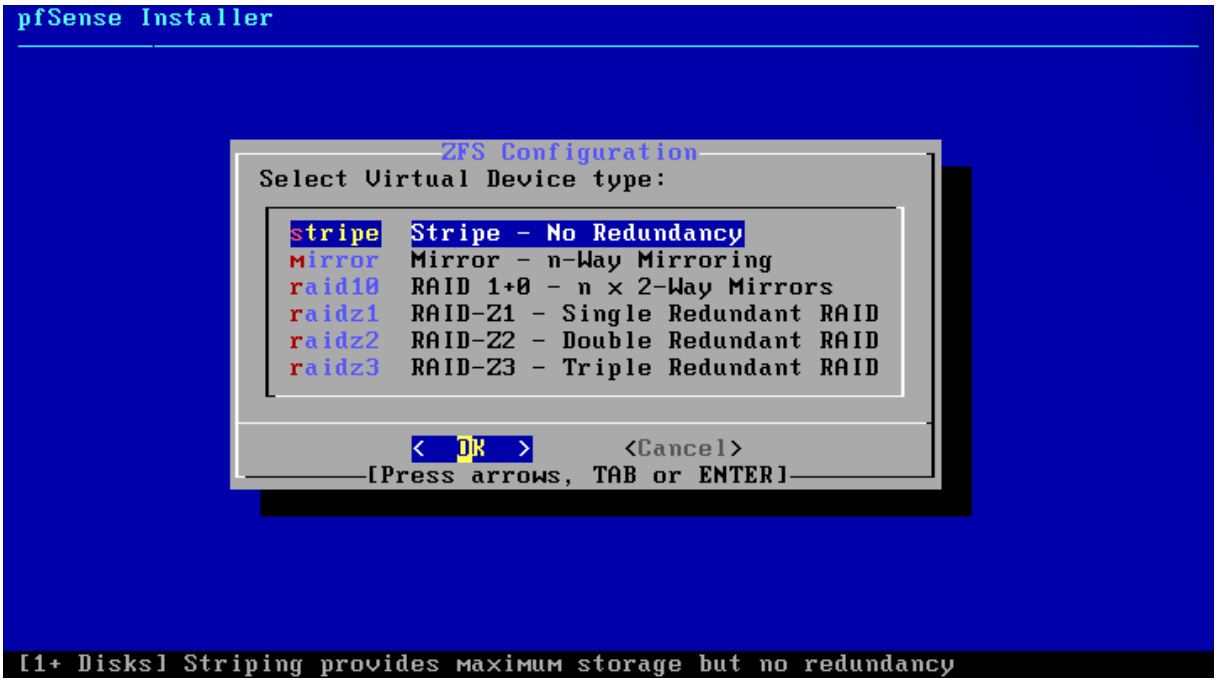
Ici je prend la 1ère option : **« Auto ZFS »**



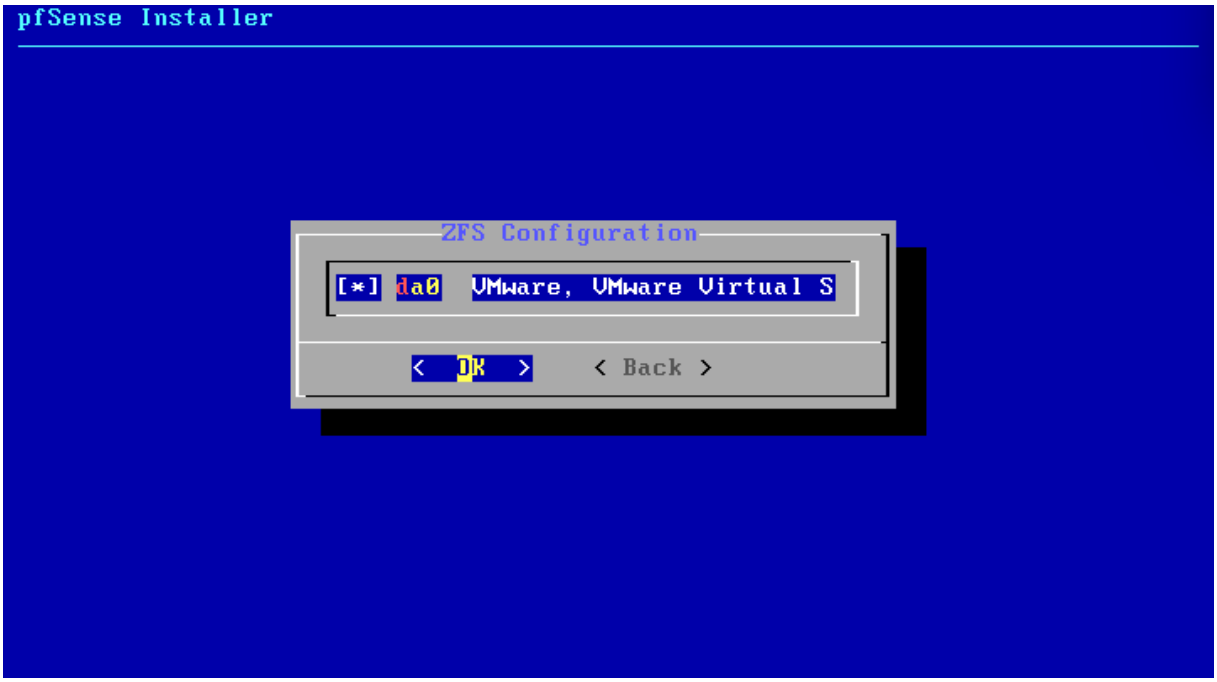
Ici je sélectionne **Install** et fait **Select**



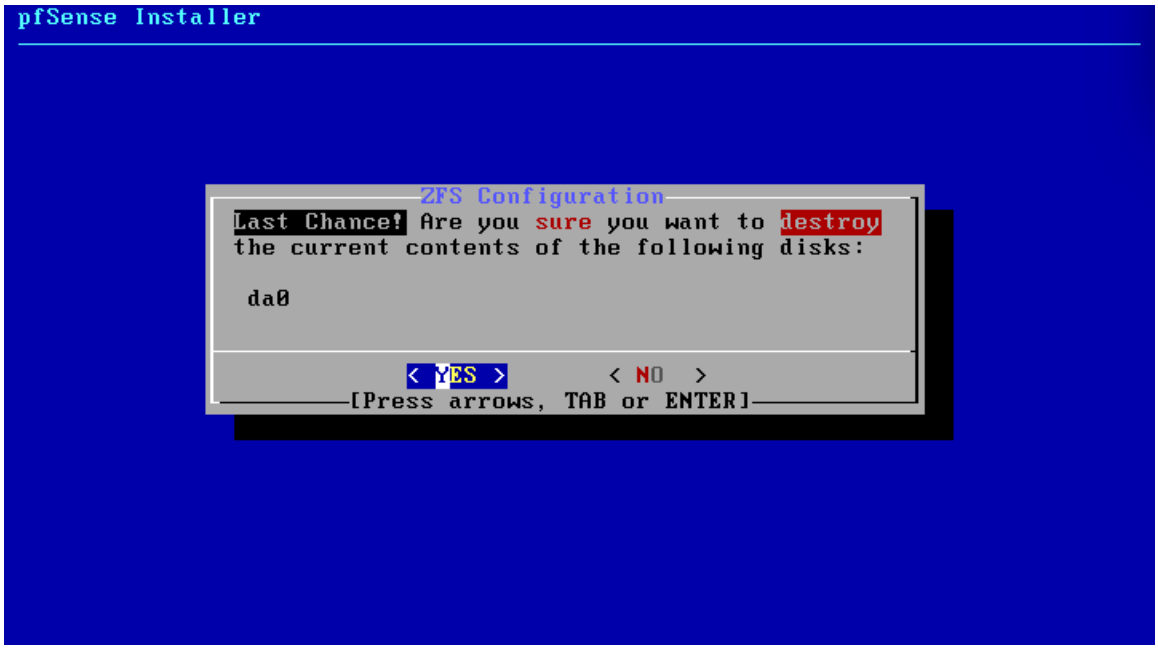
Ici je sélectionne **Stripe** car je ne souhaite pas configurer de redondance pour le moment



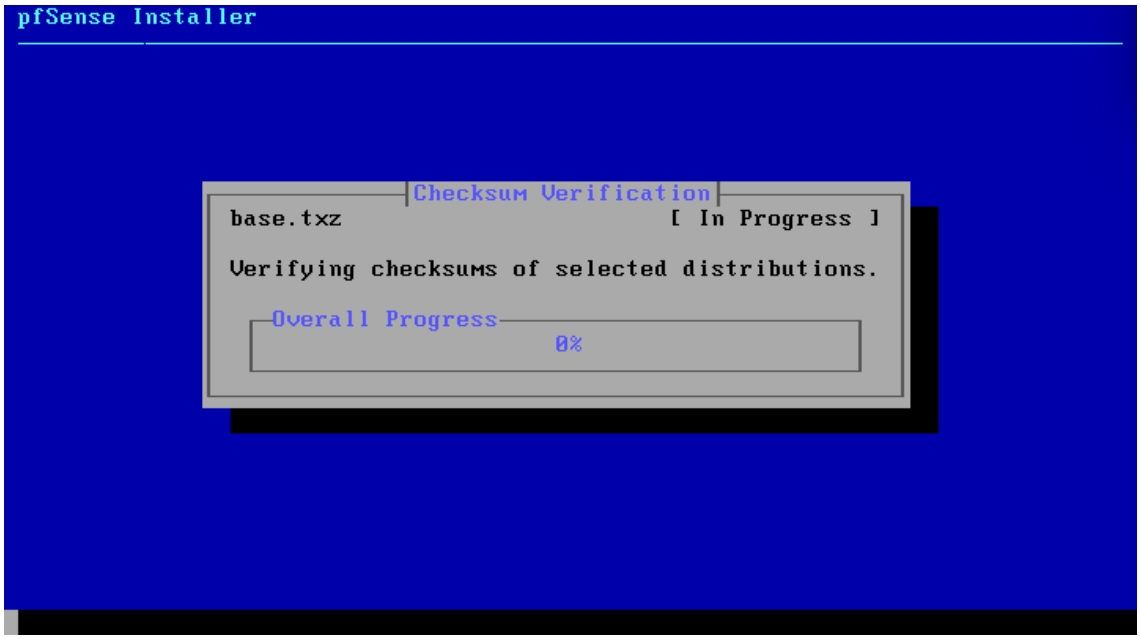
Ensuite je sélectionne mon disque ici et clique sur **OK**



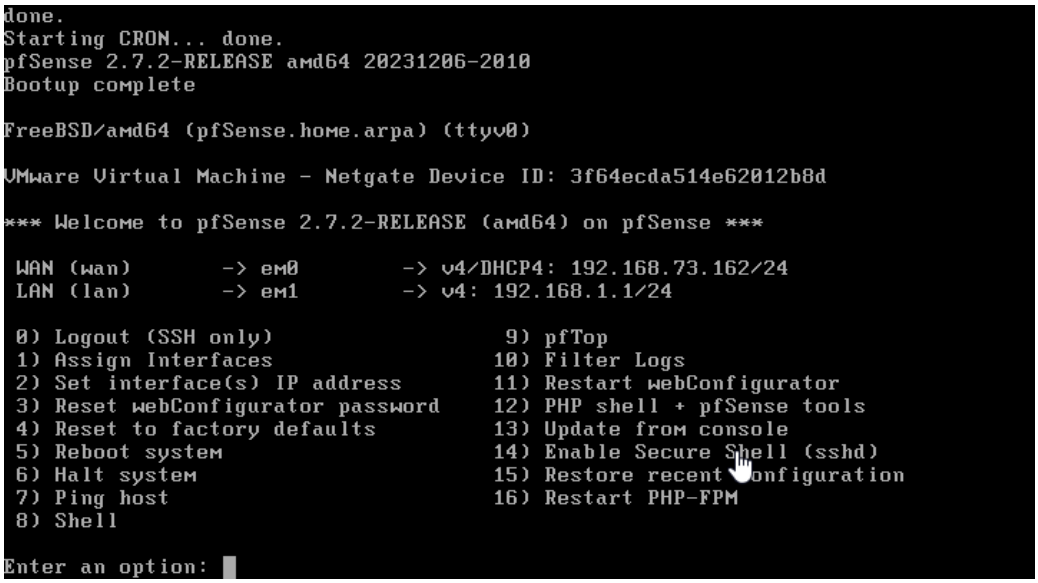
Ce message m'indique que les données sur le disque « da0 » vont être supprimés, je n'y fait pas attention car je n'ai rien sur le disque en question



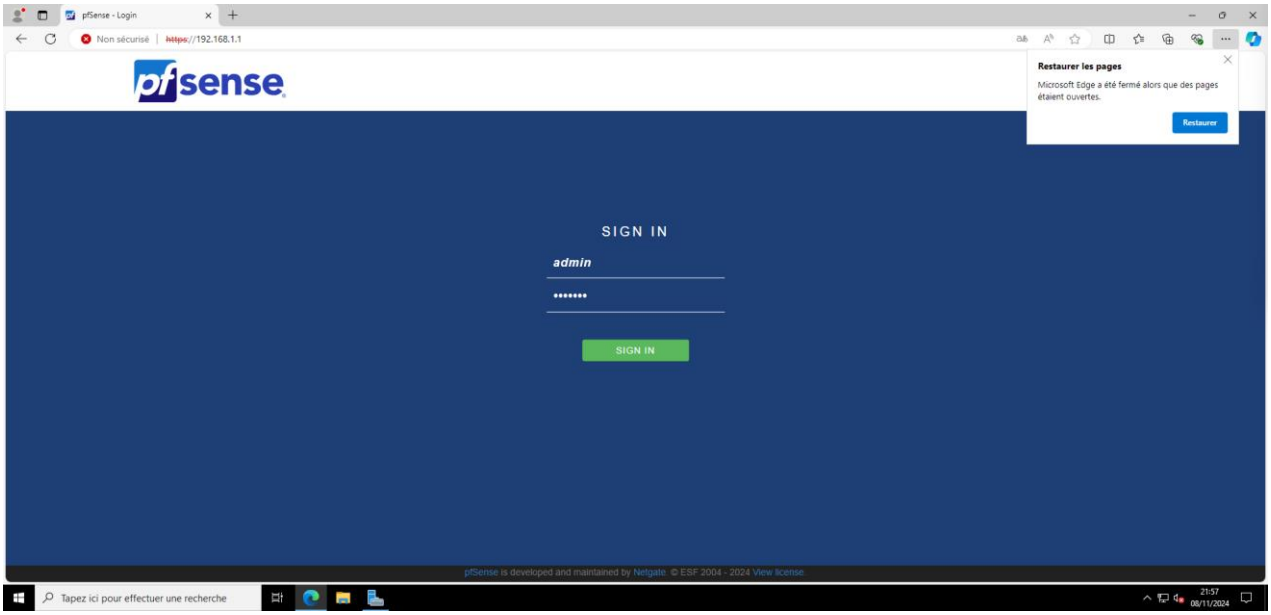
Et ensuite PfSense va finalement s'installer, il nous faudra juste redémarrer notre machine a la fin de cette progression



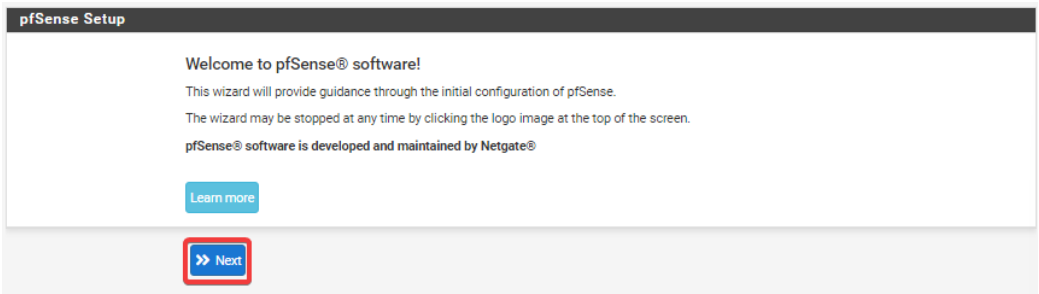
Ensuite une fois bien installé et redemarré, le PfSense nous affiche une page comme celle-ci, nous indiquant les IP des différentes interfaces et les options de paramètre



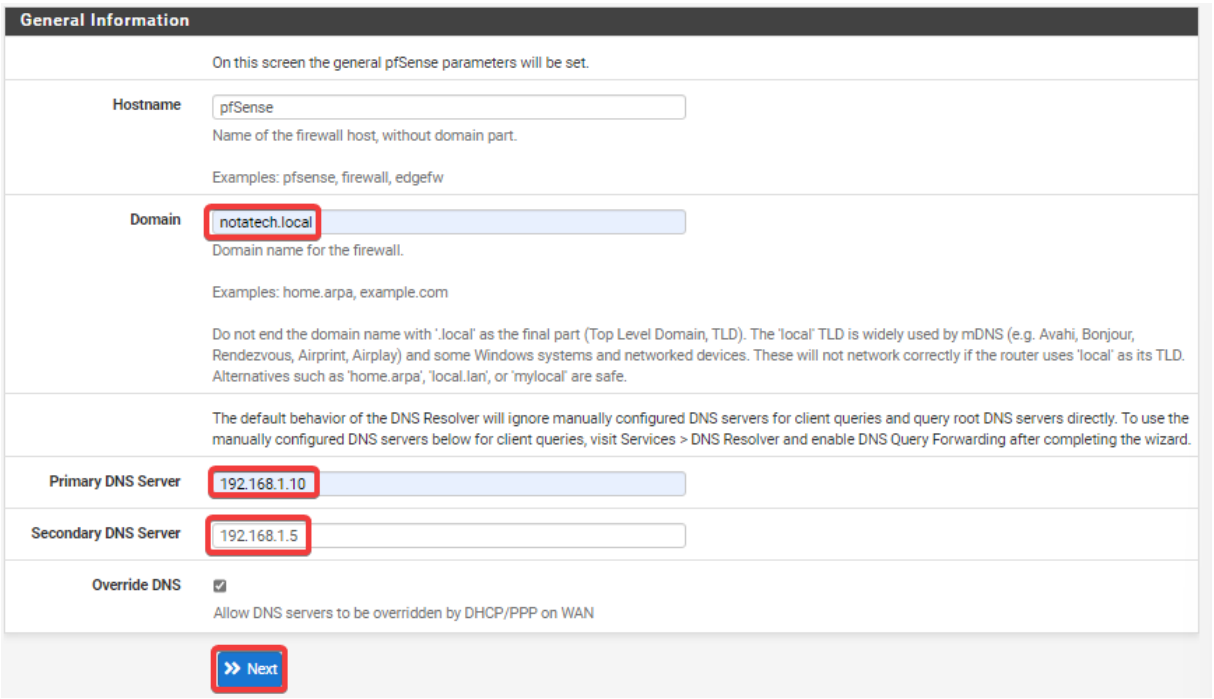
Nous n'allons pas rester plus sur la machine PfSense, nous allons juste la laisser demarrée et la configurer par l'interface web, en marquant l'IP LAN de notre PfSense dans une barre de recherche sur une machine du réseau. Je me connecte ici avec les identifiants génériques Admin Pfsense



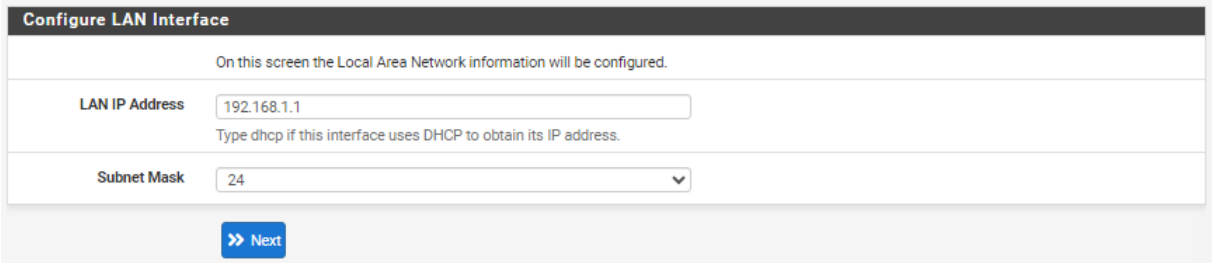
Ensuite nous allons rentrer dans la configuration de notre **PfSense**, je clique donc simplement sur **Next**



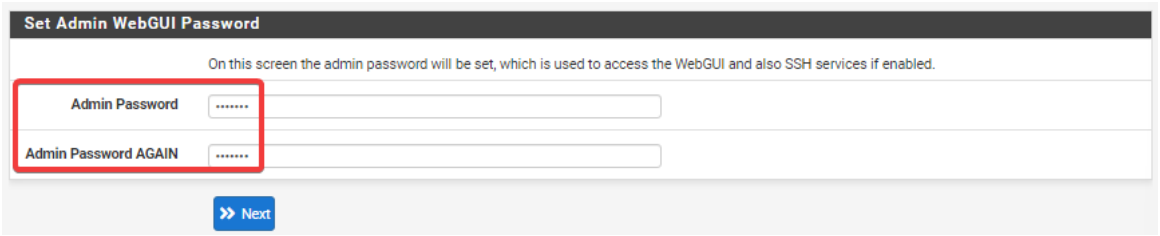
Ici pour le **Hostname** je laisse **PfSense**, pour ce qui est du domaine je rentre mon nom de domaine **Notatech.local**, pour le serveur DNS primaire je rentre l'IP de mon serveur AD principal **192.168.1.10** et pour le second je rentre celui de mon serveur en redondance **192.168.1.5**



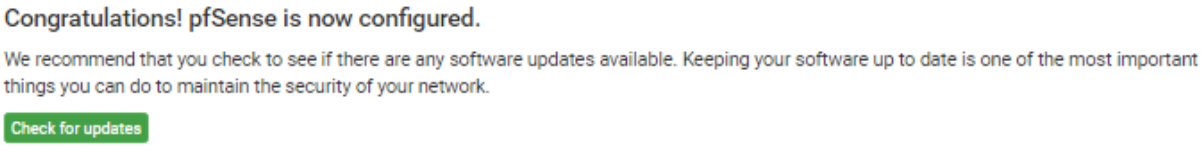
Ici on me demande l'adresse IP LAN, je rentre l'adresse de mon PfSense **192.168.1.1**



Ici je modifie mes identifiants de connexion a mon interface WEB PfSense



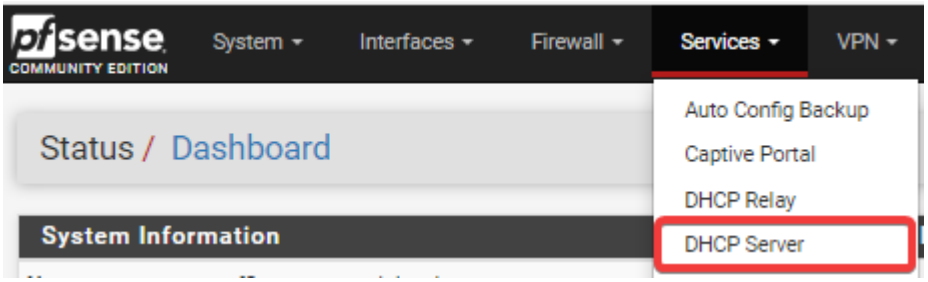
Et la configuration principale de notre PfSense est terminée !



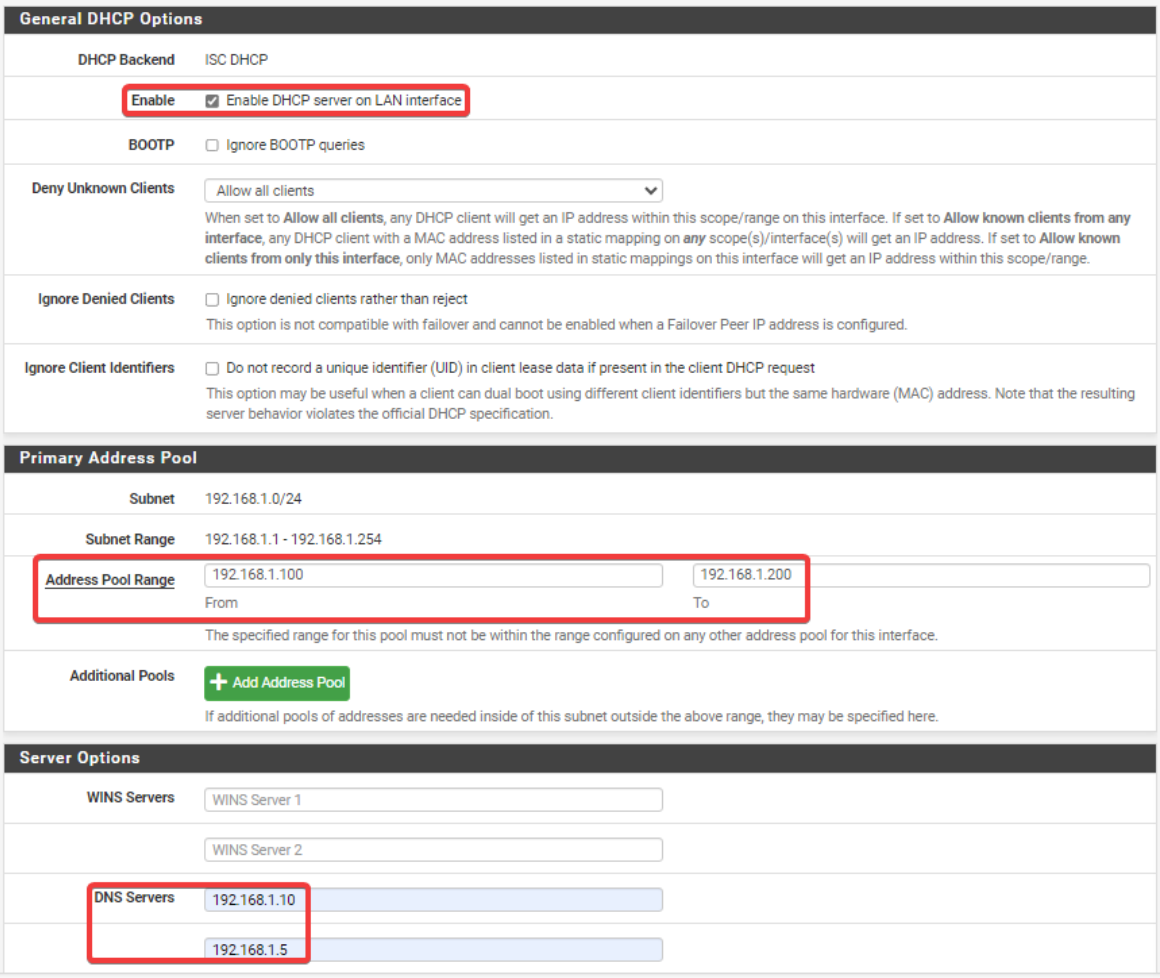
Configuration DHCP :

Ici même si nous avons déjà configuré le DHCP sur le serveur, il faudra le configurer aussi sur le PfSense, car la passerelle par défaut deviendra l'adresse du PfSense et non celle du serveur

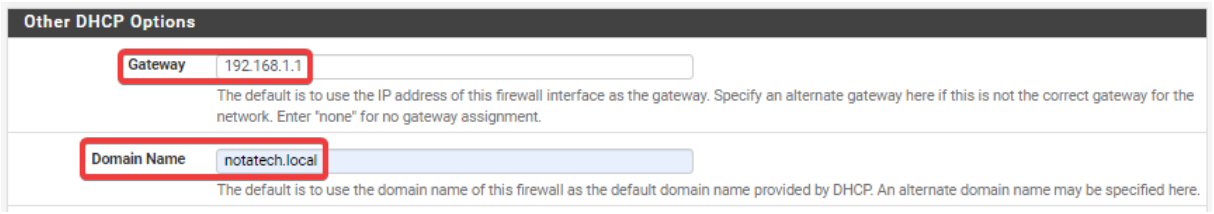
Je commence donc tout d'abord par me rendre dans **Services > DHCP Server**



Ici je coche **« Enable DHCP server on LAN interface »**, je définis mon **Pool Range** de **192.168.1.100** jusqu'à **192.168.1.200** et finalement je renseigne l'IP de mes 2 serveurs AD dans les **Server Options**



Et finalement dans **Other DHCP Options**, je renseigne l'adresse de ma passerelle qui est donc l'adresse de mon PfSense, **192.168.1.1** et je renseigne mon nom de domaine **notatech.local**

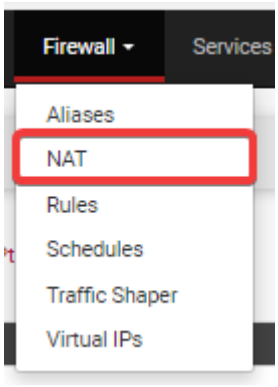


Je sauvegarde et applique et voilà **la configuration de notre DHCP est terminée**

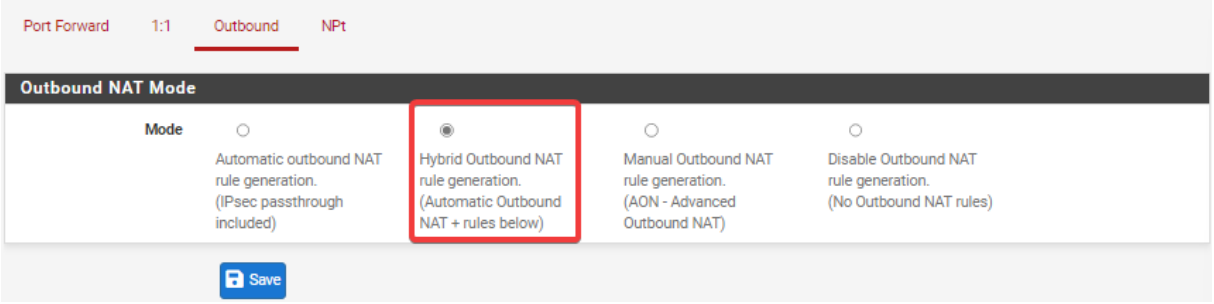
Configuration internet pour les clients :

Dans cette partie nous allons configurer le PfSense pour qu'il diffuse la connexion internet aux utilisateurs dans le réseau

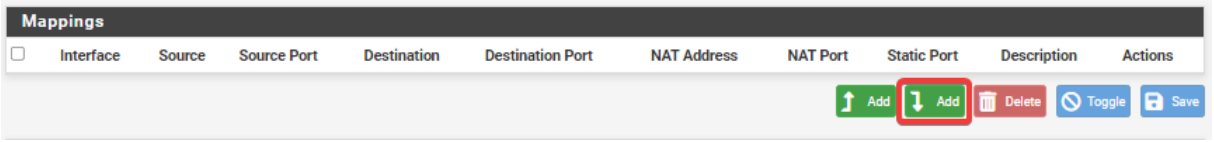
Dans un premier temps, dans l'interface web du PfSense je clique sur **Firewall > NAT**



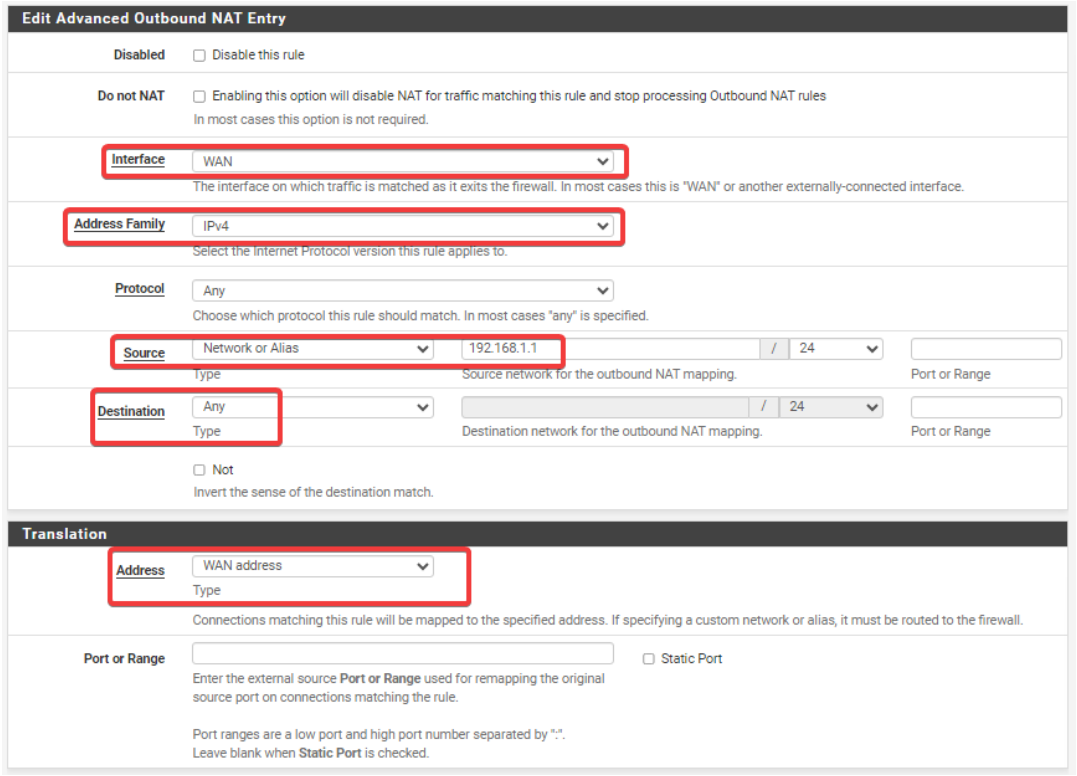
Ensuite ici je sélectionne **Hybrid Outbound NAT**



Ici je clique sur **Add** pour ajouter une nouvelle règle



Ensuite cette page apparaît, ici pour l'interface je sélectionne **WAN** car c'est l'interface qui peut communiquer avec internet, pour la famille d'adresse je sélectionne **IPV4** car nous n'avons pas besoin de configurer d'IPV6, en source je sélectionne **Network or Alias** et rentre l'adresse **192.168.1.1** car c'est notre adresse **LAN**

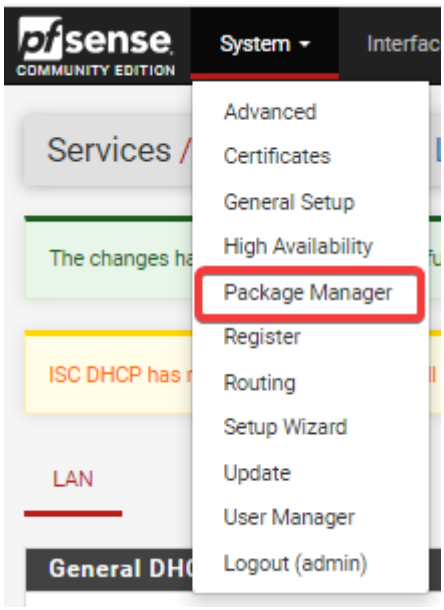


Ensuite je sauvegarde ces paramètres, les applique et les machines pourront se connecter à internet.

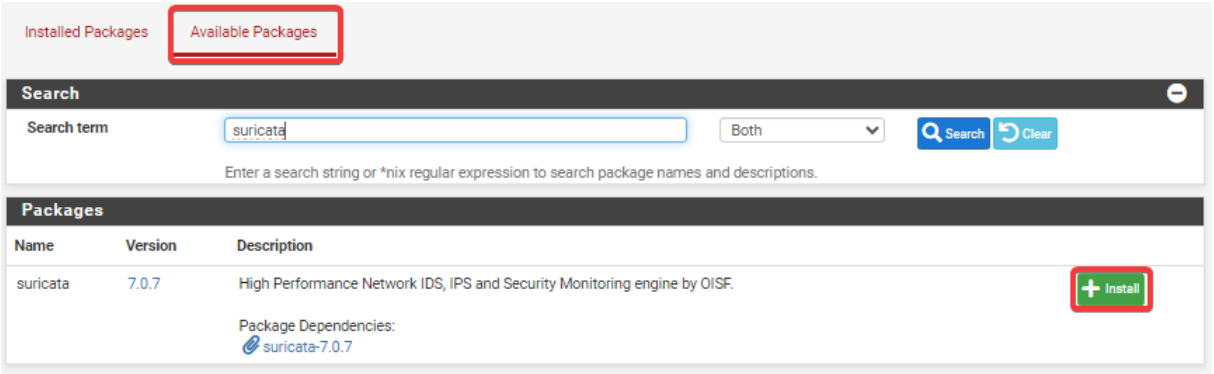
Configuration d'un IPS/IDS :

Dans cette partie nous allons voir comment j'ai configuré l'IDS/IPS avec le suricata sur mon PfSense pour améliorer la sécurité de mon réseau. Qui est un programme qui permet de surveiller notre réseau

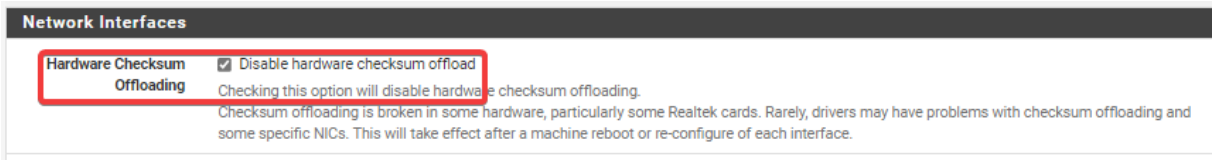
Je commence tout d'abord par me rendre dans **System > Package Manager** sur l'interface web de mon PfSense



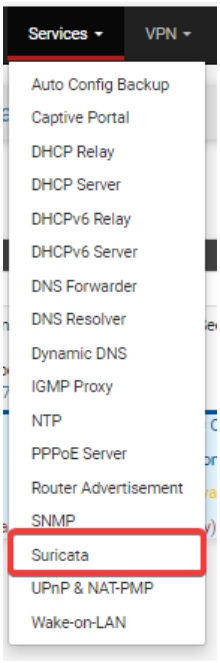
Ensuite je clique sur **Available Packages** et je recherche **Suricata** et je clique sur **Install**



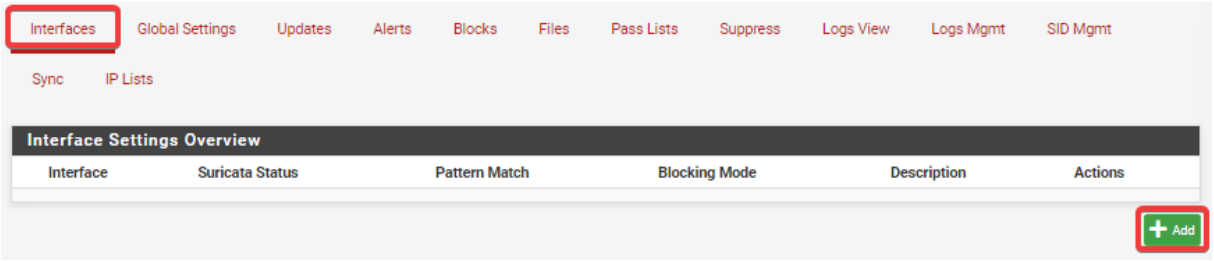
Pour que le Suricata fonctionne bien il faudra tout d'abord désactiver cette option dans **System > Advanced > Networking**



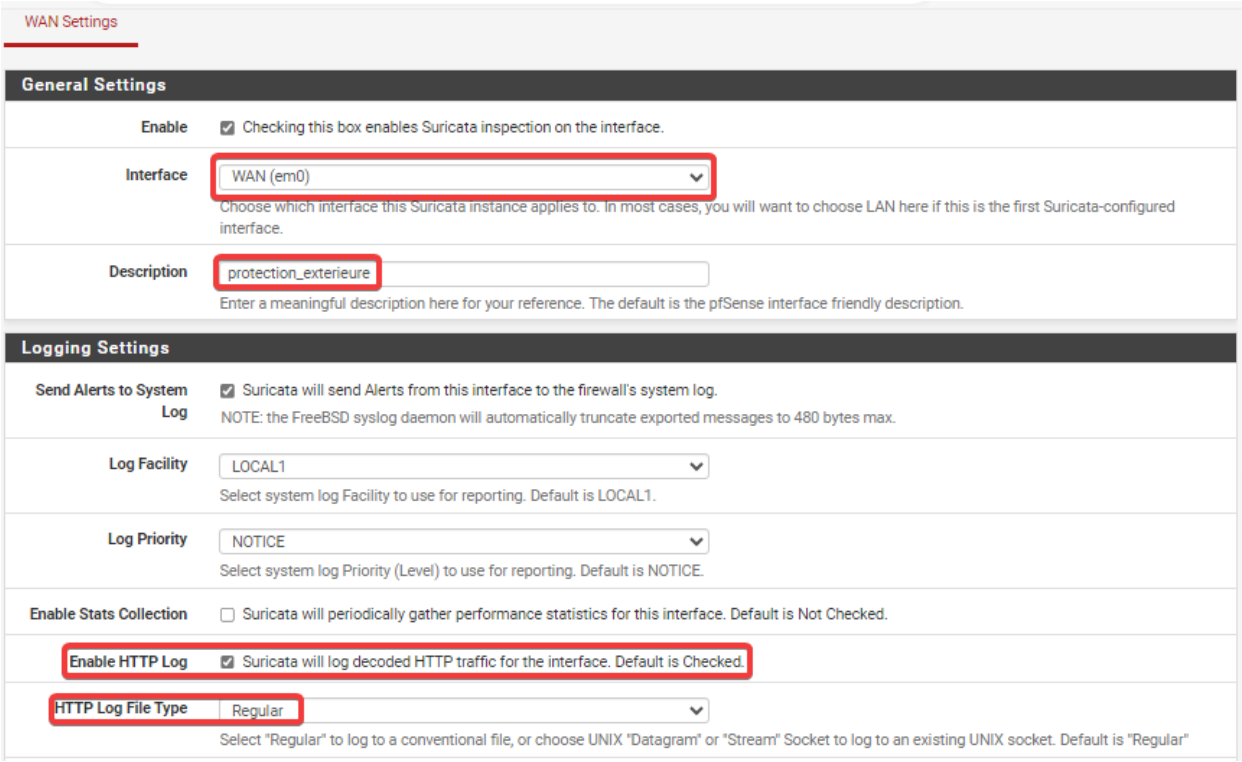
Ensuite on va maintenant le configurer, je me rends dans **Services > Suricata**



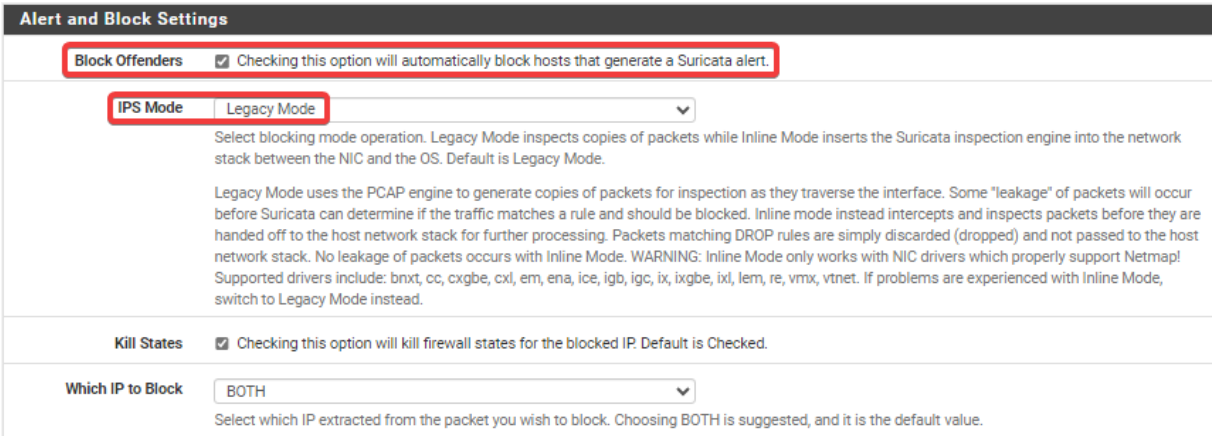
Ensuite dans **Interfaces** je clique sur **Add** pour ajouter une nouvelle interface



Arrivé sur cette page je sélectionne l'interface **WAN** pour détecter les intrusions venant de l'extérieur, ensuite je donne la description **protection_exterieure**, ensuite je coche **Enable HTTP Log**, pour recevoir des journaux d'événements des événements http et je laisse **Regular** pour le type de log

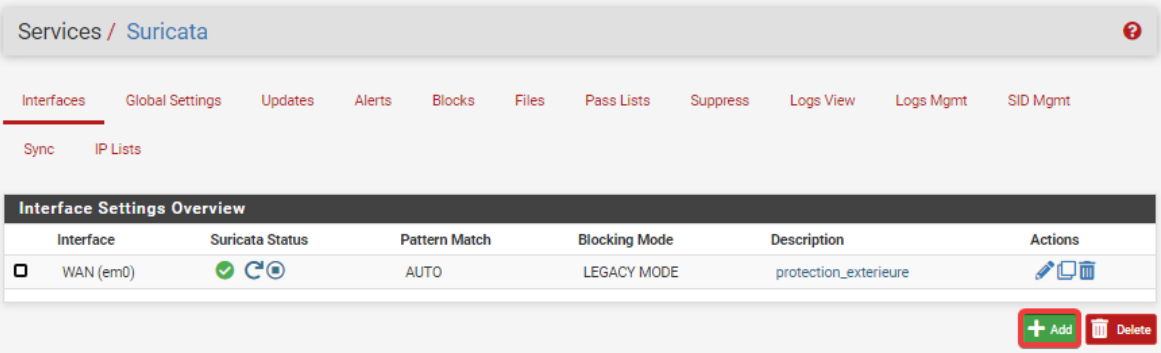


Ensuite dans **Alert and Block Settings** je coche **Block Offenders** pour automatiquement bloquer les hôtes ayant générés des alertes Suricata

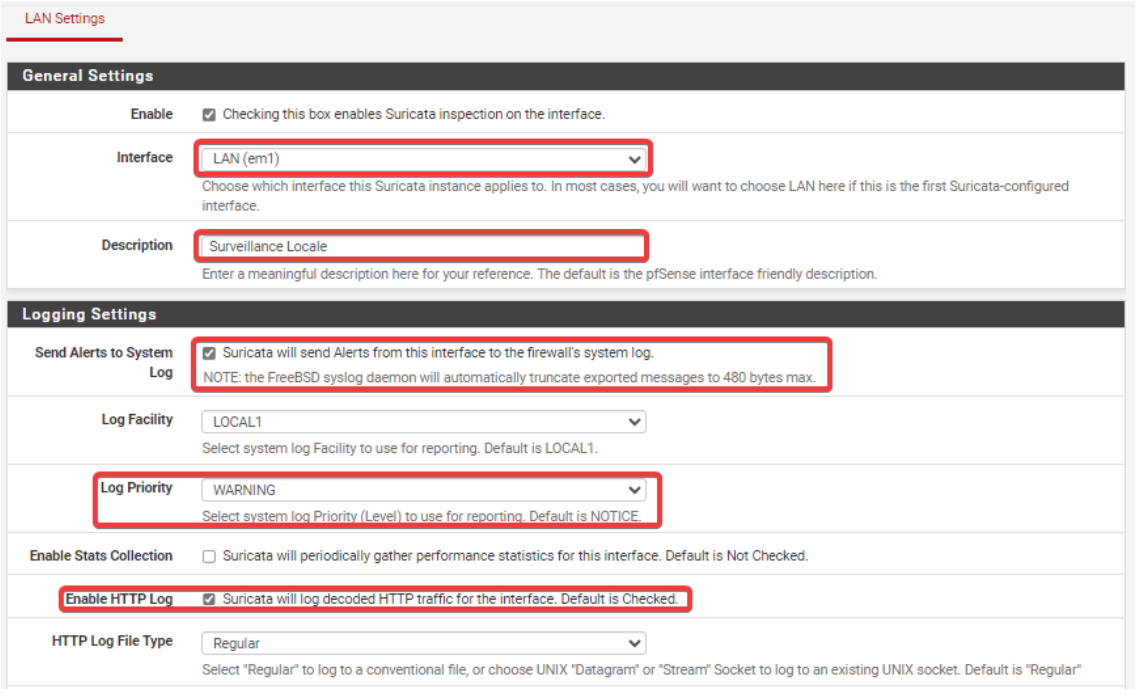


Et ensuite pour la suite je laisse les paramètres par défaut.

Ensuite nous allons aussi surveiller l'interface **LAN,** pour ce faire je commence par retourner sur la page de mon **Suricata** et sur la page **interfaces** et ici je clique sur **Add**

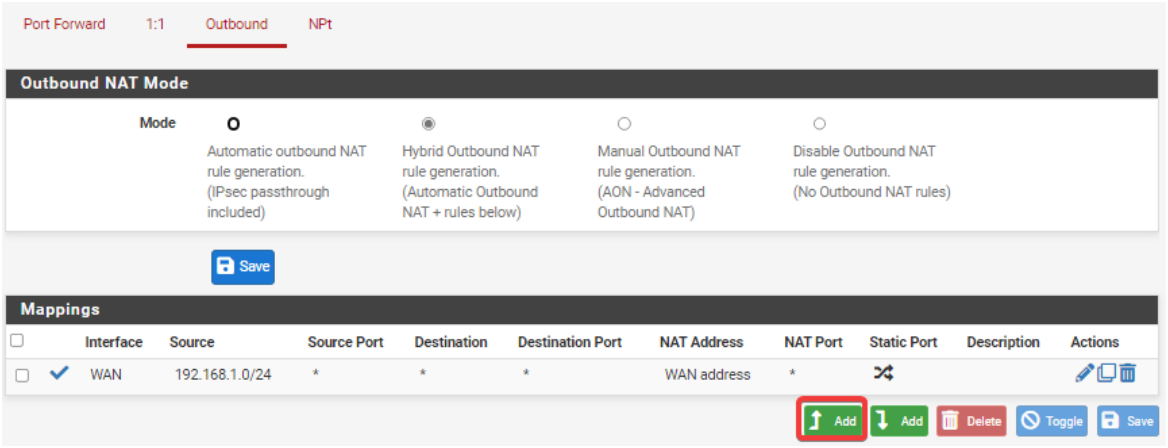


Ensuite sur cette fenêtre je rentre ces informations, je sélectionne **LAN** car c'est l'interface qu'on veut surveiller, je la nomme **« surveillance locale »** je coche ensuite **Send Alerts to system Log** pour être alerter de ce qui se passe sur mon interface et je laisse les autres options par défaut

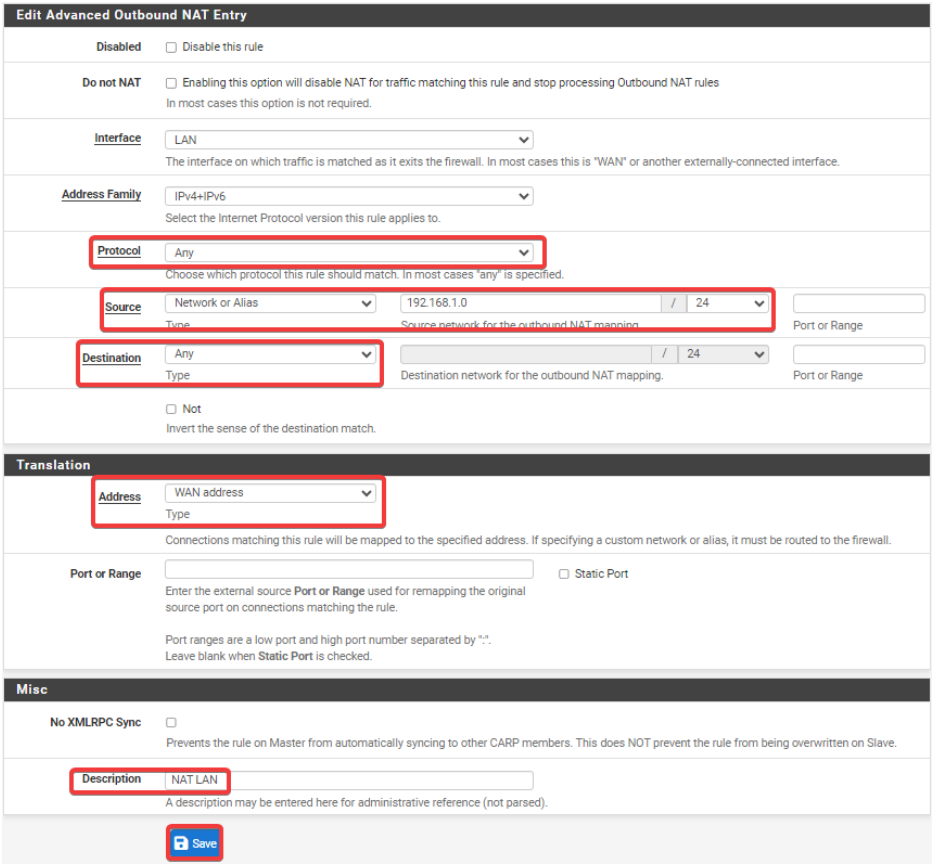


Et ensuite je laisse les autres options par défaut et je sauvegarde et applique la configuration.

Ensuite comme pour le WAN, je me rends dans **Firewall > Outbound** et clique ici sur **Add**



Ensuite cette page s'ouvre, et je sélectionne ces paramètres, sauvegarde et applique



Et voila la configuration de mon IDS est terminée