

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 :

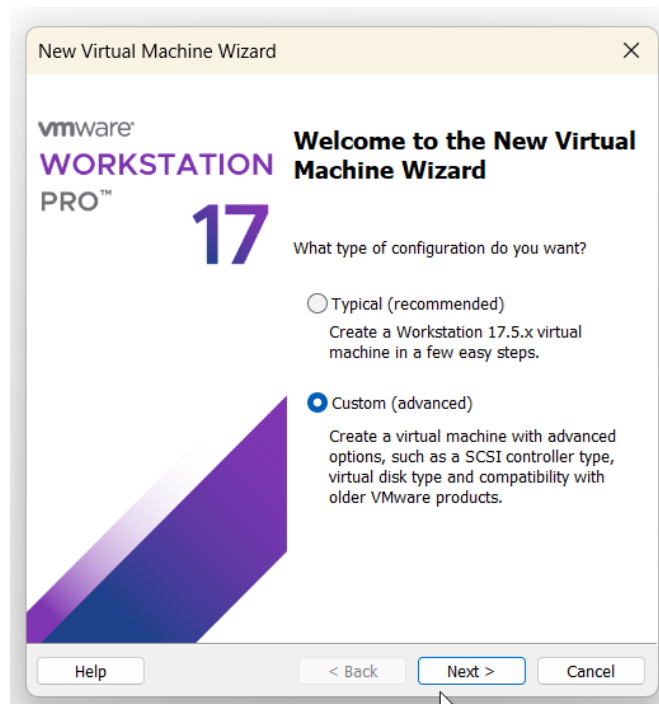
78-81

Configuration d'un IPS/IDS :

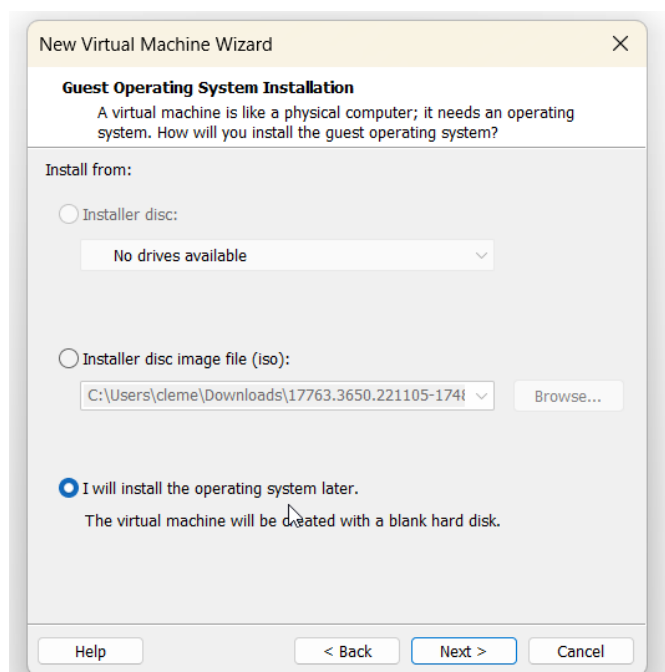
82-86

Création du serveur AD DS :

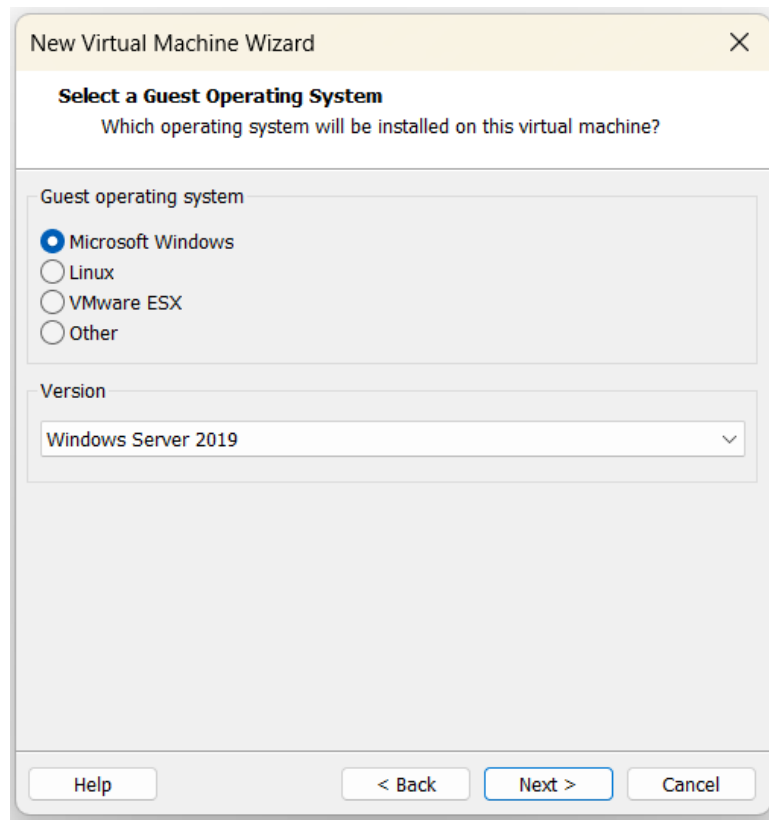
Je commence par cliquer sur « créer une machine virtuelle sur le logiciel VMWare Workstation, et choisis une configuration custom



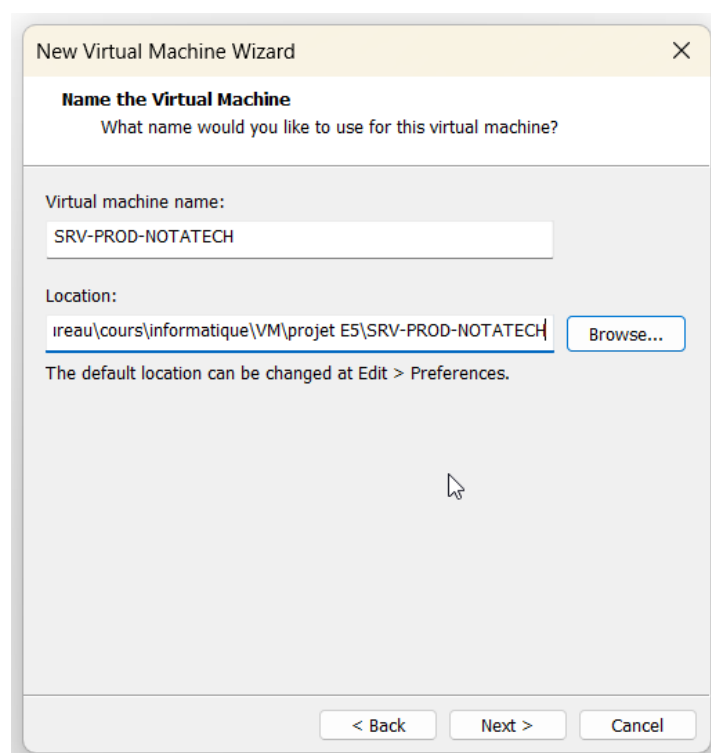
Ensuite je choisis d'installer l'iso de Windows server plus tard pour éviter d'avoir des soucis avec le compte microsoft



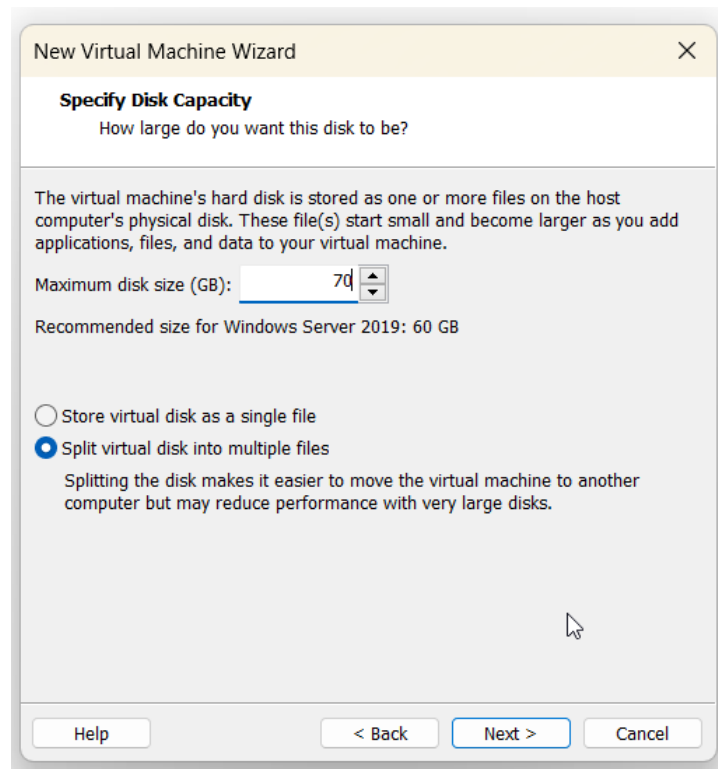
Ensuite je sélectionne « Microsoft Windows » comme système d'exploitation et sélectionne windows server 2019 pour la version



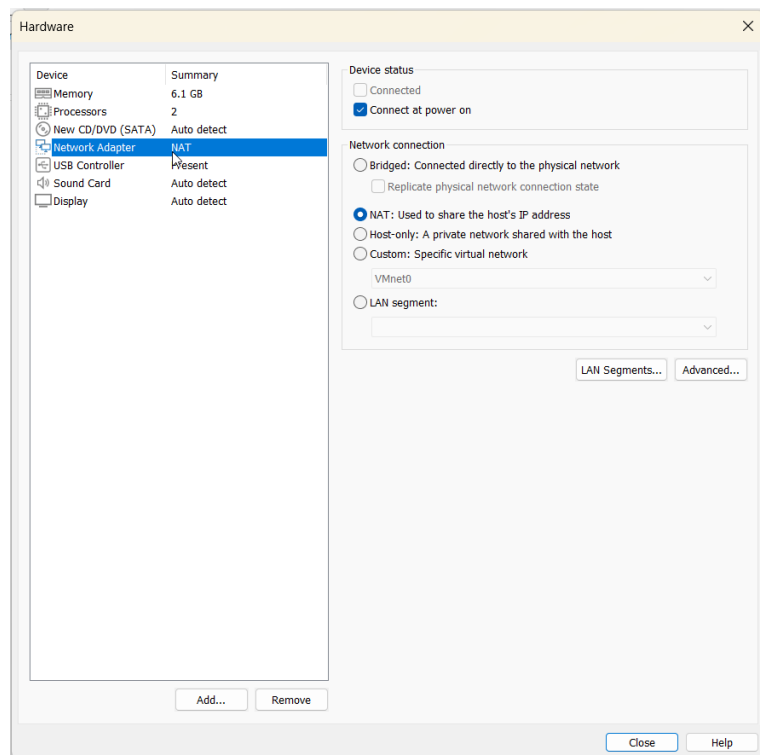
Je nomme ma machine virtuelle « SRV-PROD-NOTATECH » pour « serveur de production notatech »



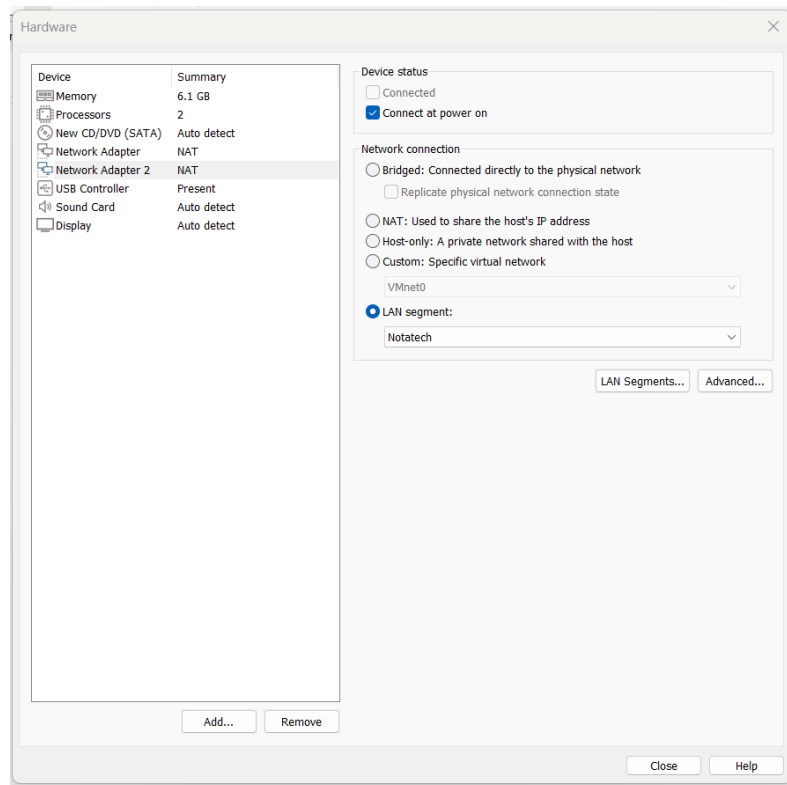
Je choisis ensuite de mettre 70GB d'espace disque pour ne pas avoir de soucis au niveau de l'espace de stockage suffisant



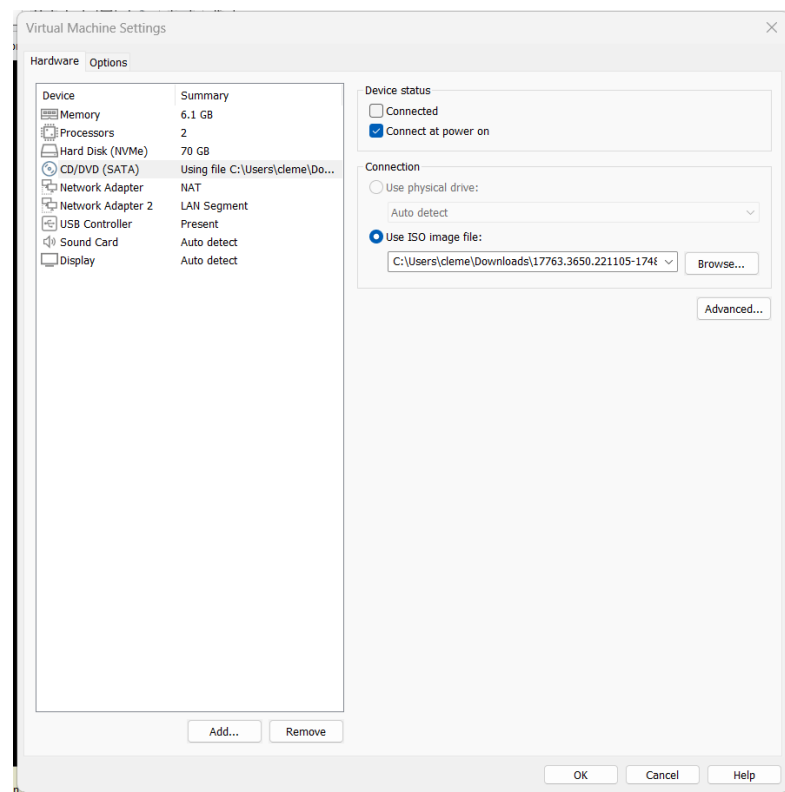
Ensuite je me rend dans les paramètres de la VM et met sa première carte réseau en NAT, pour avoir l'accès a internet



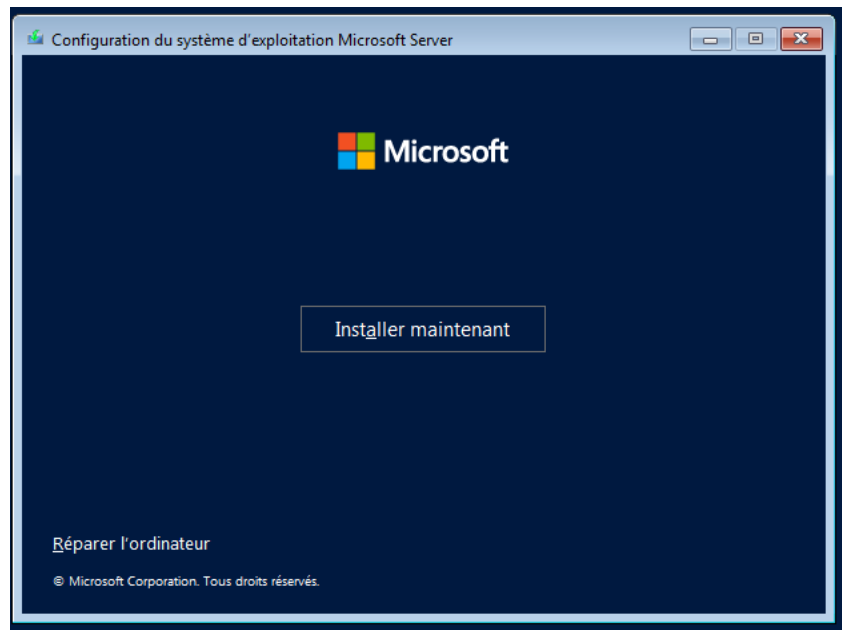
Et je rajoute ensuite une deuxième carte réseau a ma machine, cette fois ci sur un LAN segment appelé « notatech » créé spécialement pour lier les machines de l'infrastructure réseau facilement



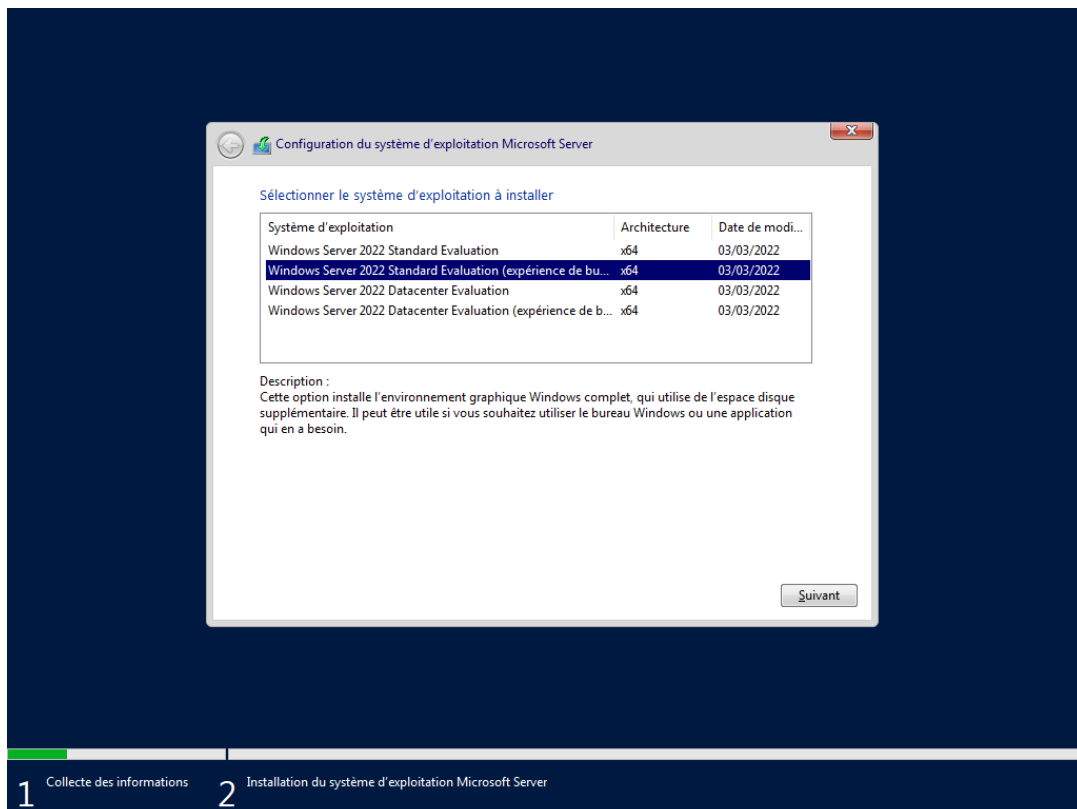
Ce qui nous donne donc finalement 2 cartes réseaux, une en NAT pour l'accès à internet et une en LAN segment pour facilement relier les prochaines machines



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



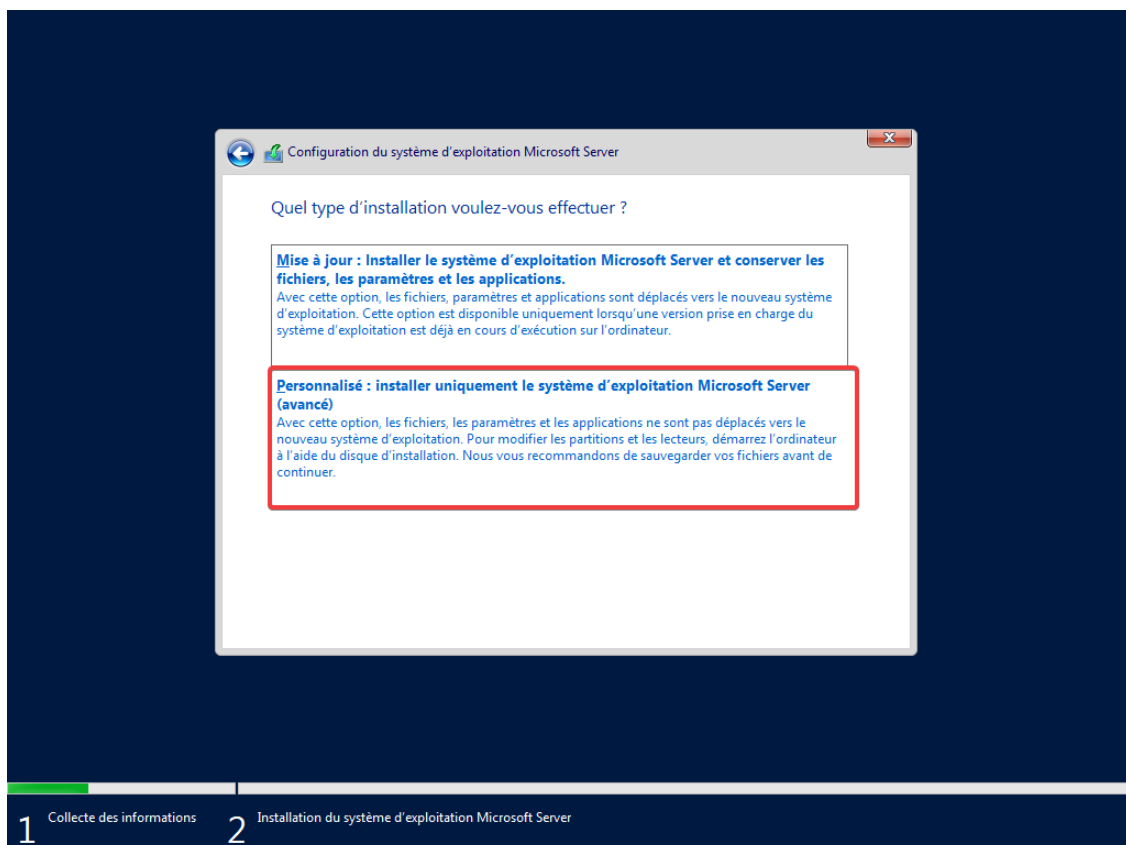
Je sélectionne ensuite la 2^{ème} option « Windows server 2022 standard Evaluation (expérience de bureau) »



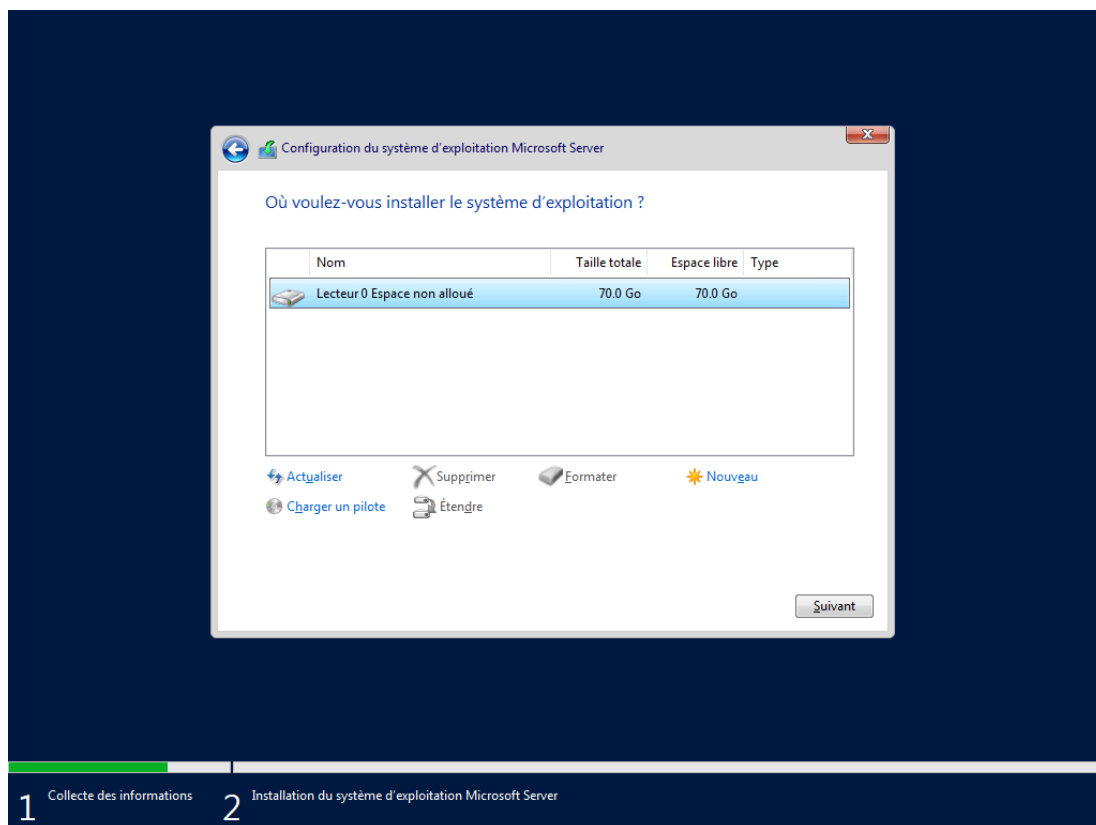
Ensuite les conditions d'utilisation apparaissent je coche donc « j'accepte les termes du contrat » et clique sur suivant



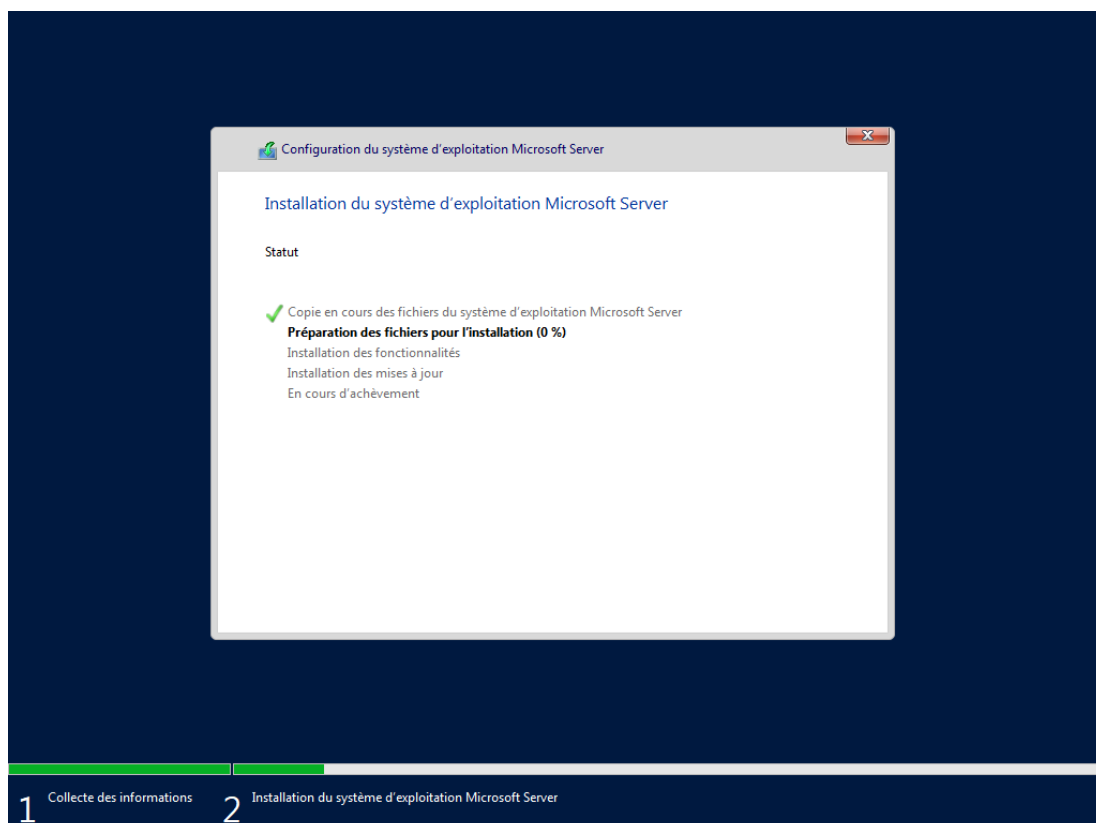
Pour le type d'installation je sélectionne « **personnalisé** » pour pouvoir sélectionner mon disque



Je sélectionne donc mon disque et clique sur suivant



Et l'installation va finalement se lancer



Une fois installé cette page apparaîtra, 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 »

Paramètres de personnalisation

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

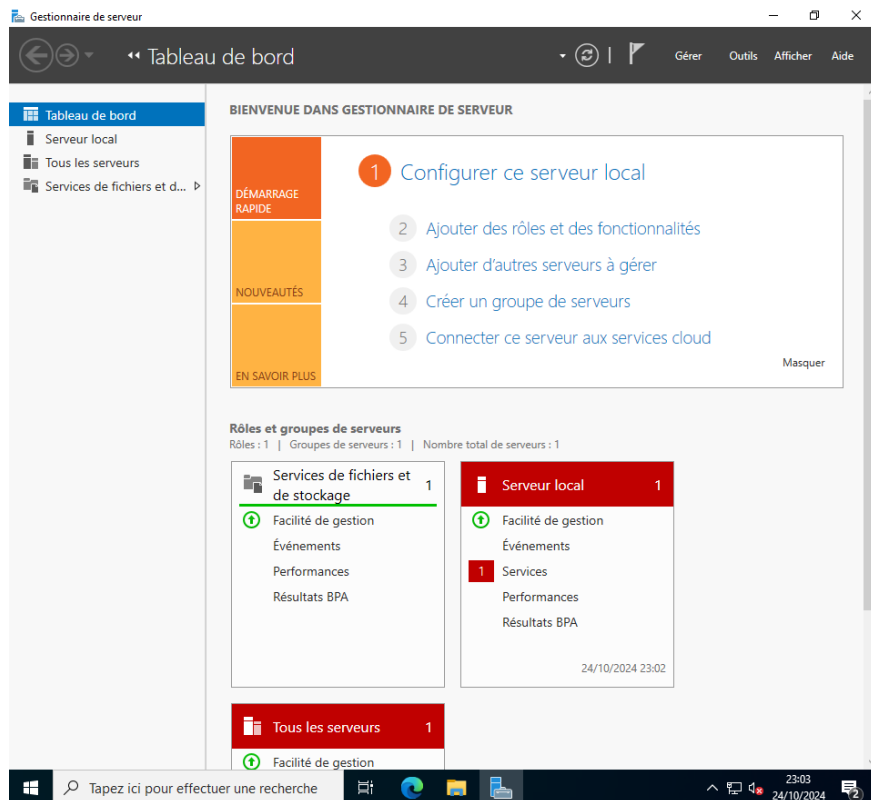
Nom d'utilisateur: Administrateur

Mot de passe:

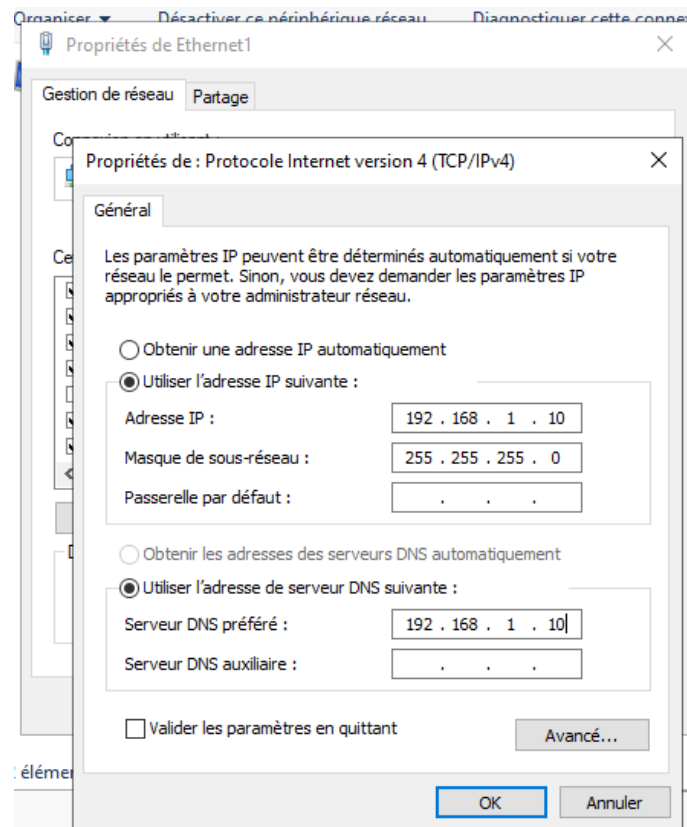
Entrez de nouveau le mot de passe: 🔍

Terminer

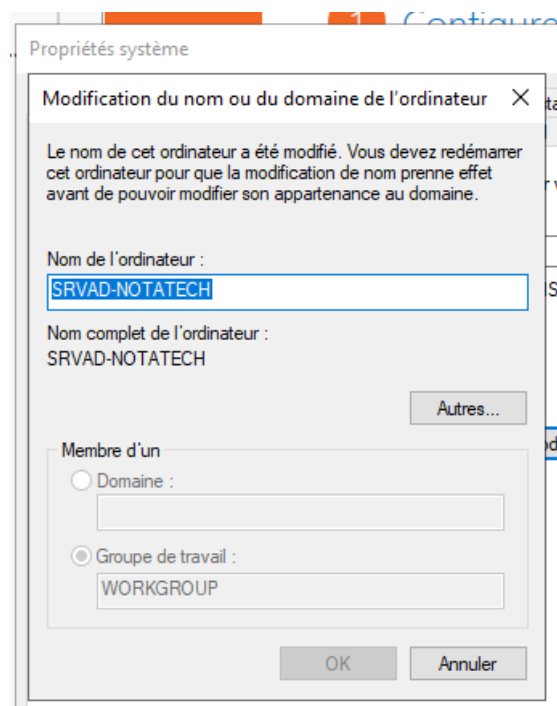
Et enfin cette page qui est le Server manager s'ouvrira et on pourra configurer notre serveur



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

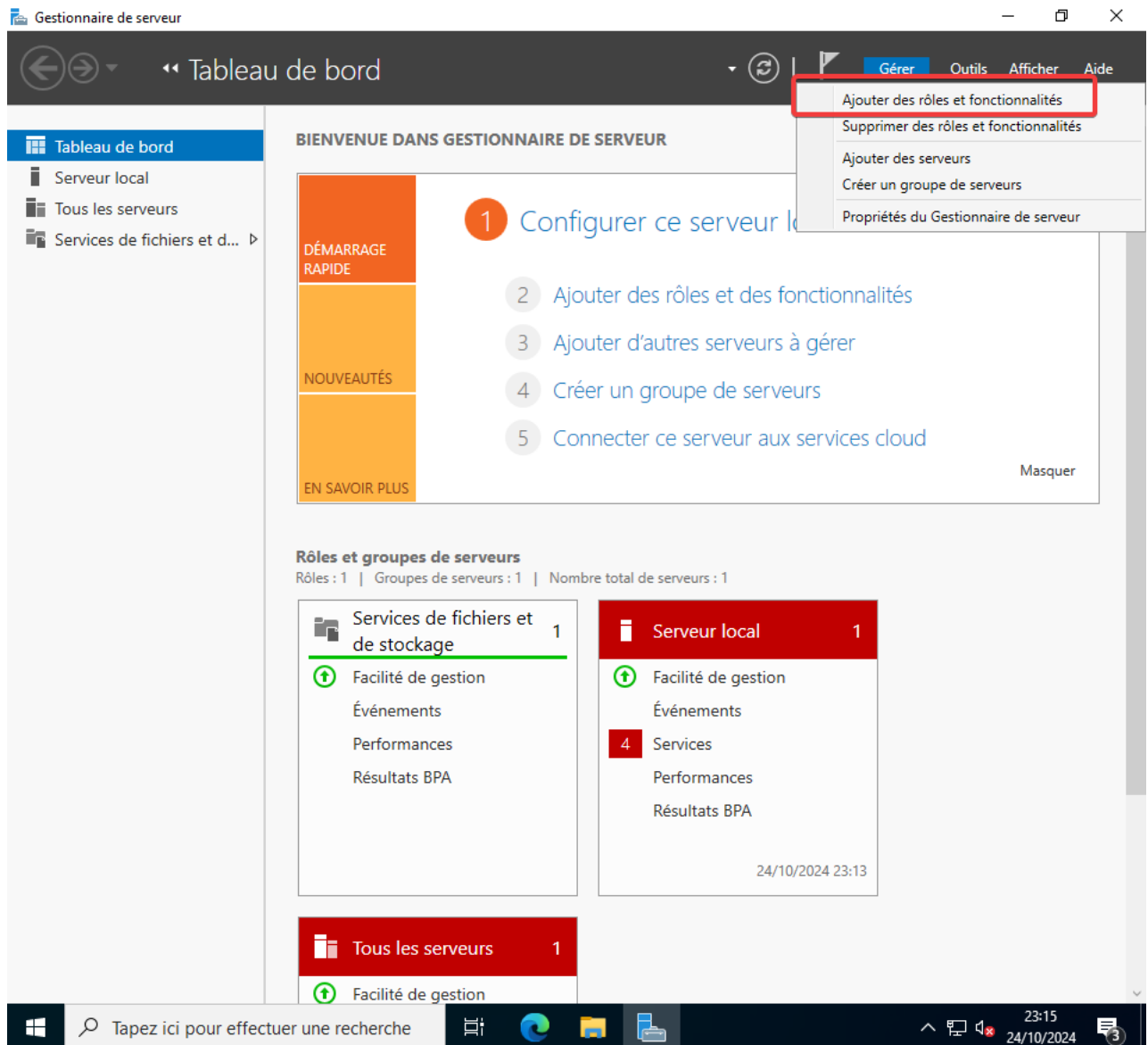


Et ensuite je renomme ma machine en « SRVAD-NOTATECH » pour qu'elle soit identifiable facilement

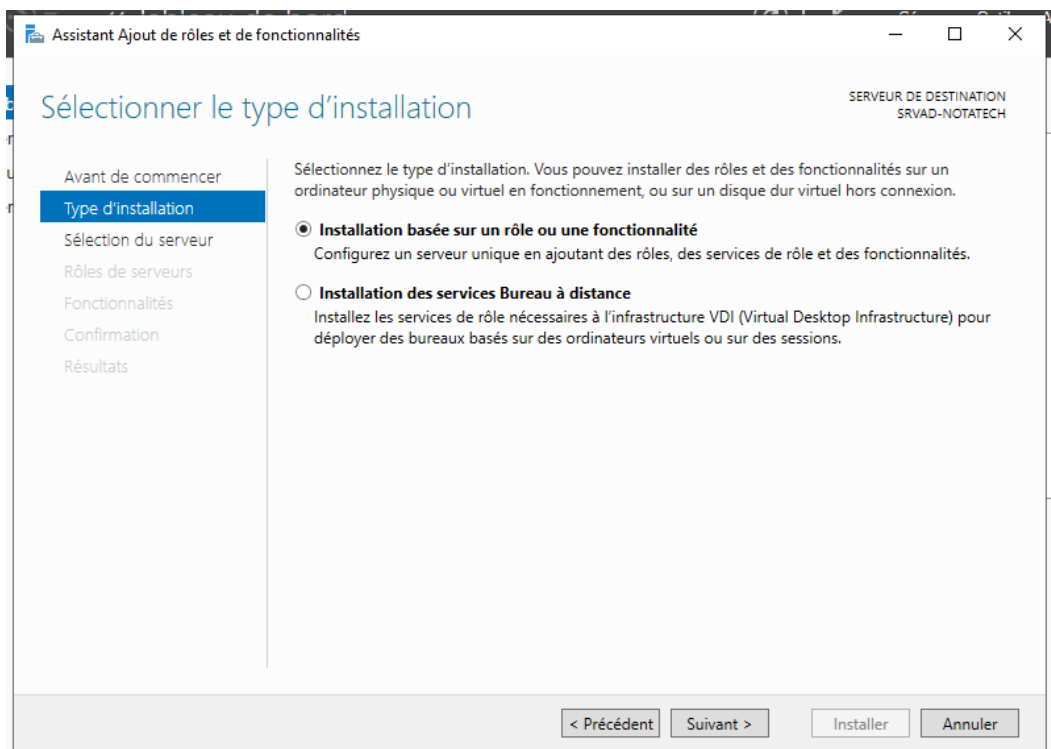


Configuration rôle AD DS

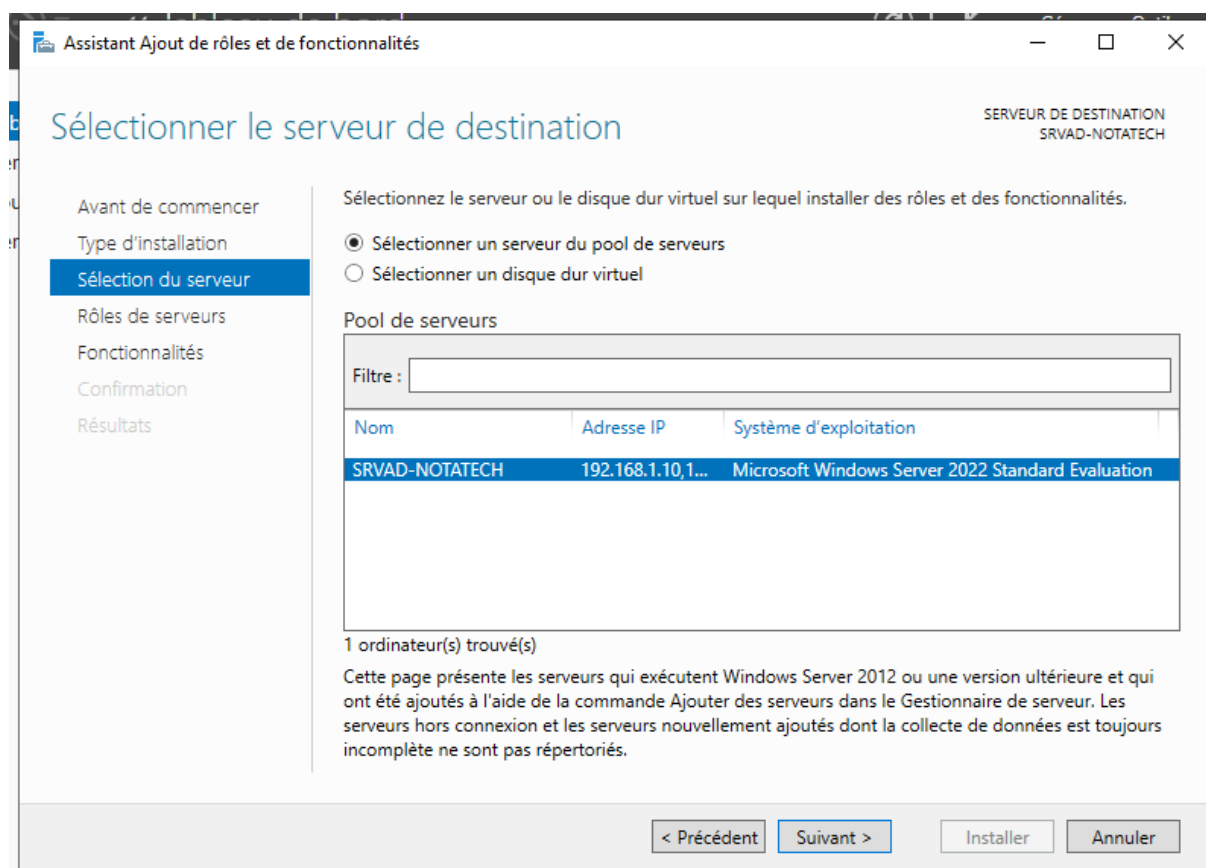
Tout d'abord pour l'ajout de ce rôle, je me rends dans « gérer » sur le tableau de bord du server manager et je clique sur « ajouter des rôles et fonctionnalités »



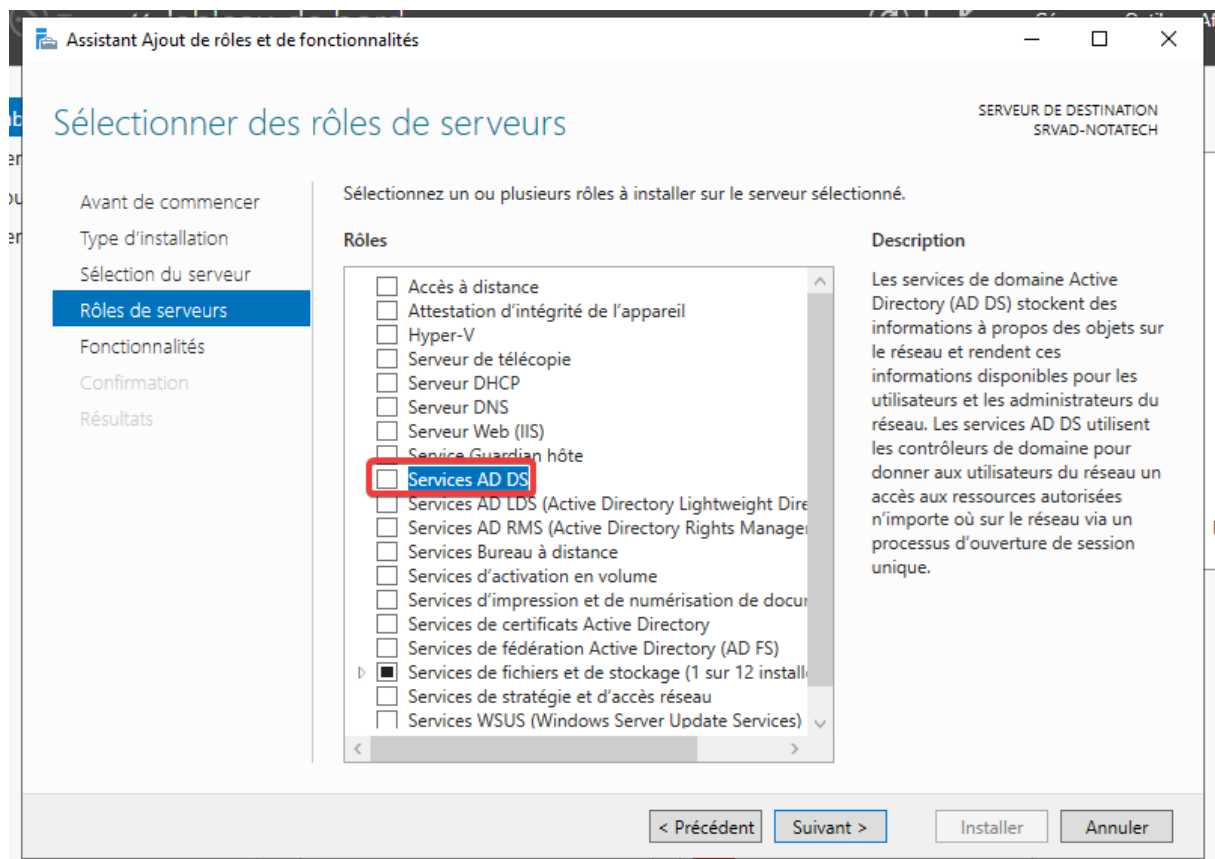
Ensuite arrivé sur cette page je clique sur « installation basée sur un rôle ou une fonctionnalité » et je clique sur suivant



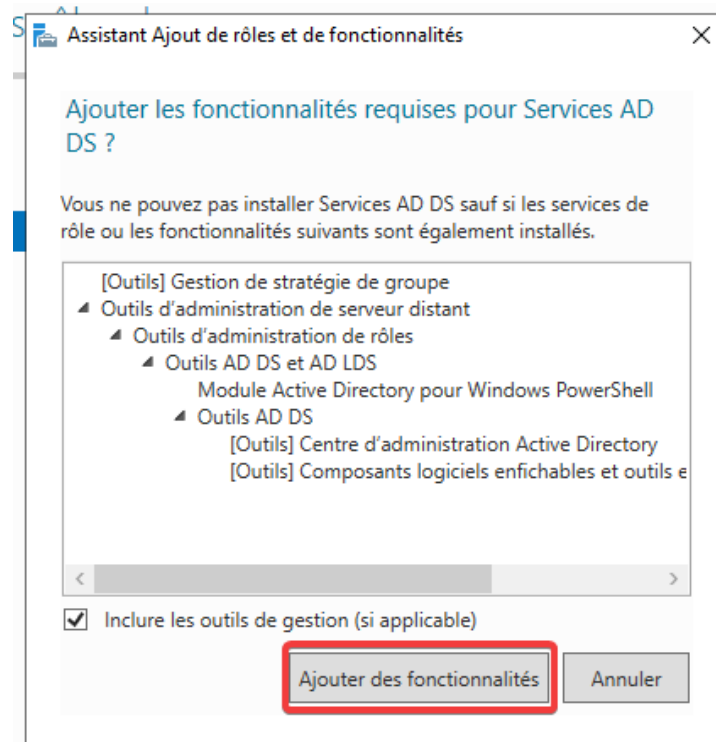
Ensuite pour la sélection du serveur je sélectionne mon serveur et clique sur suivant



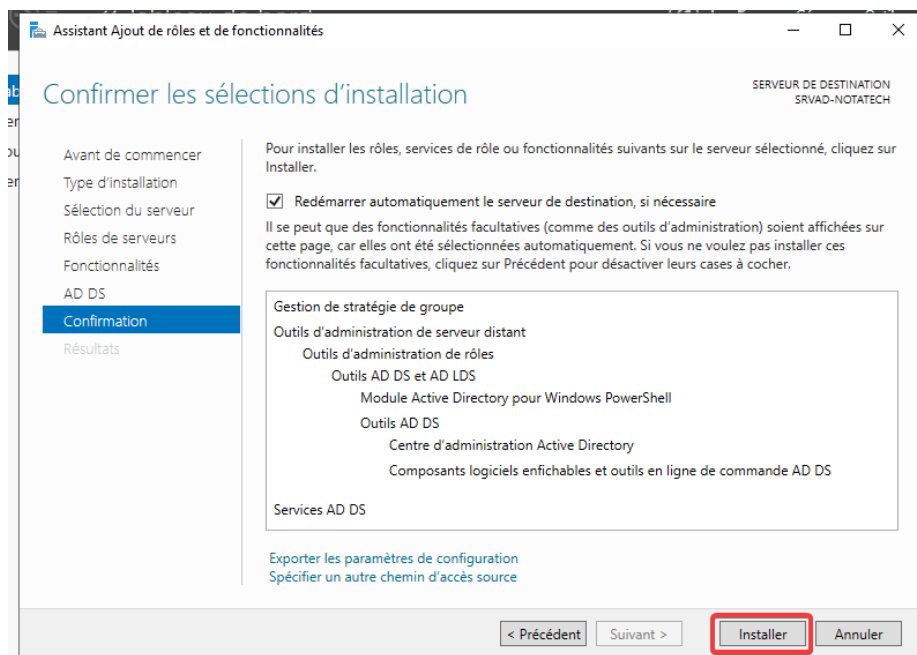
Pour les rôle de serveur je sélectionne « serveur AD DS »



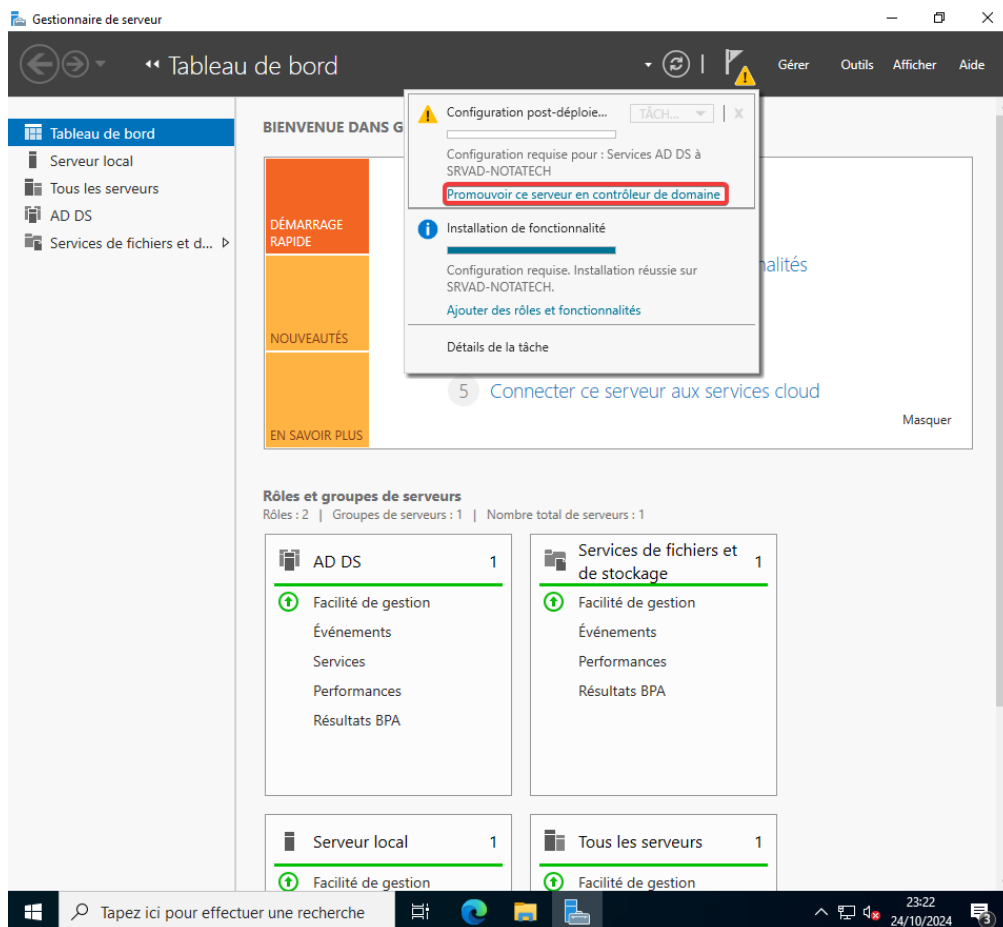
Cette page apparaît je clique sur le bouton « ajouter des fonctionnalités » et je fais « suivant »



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

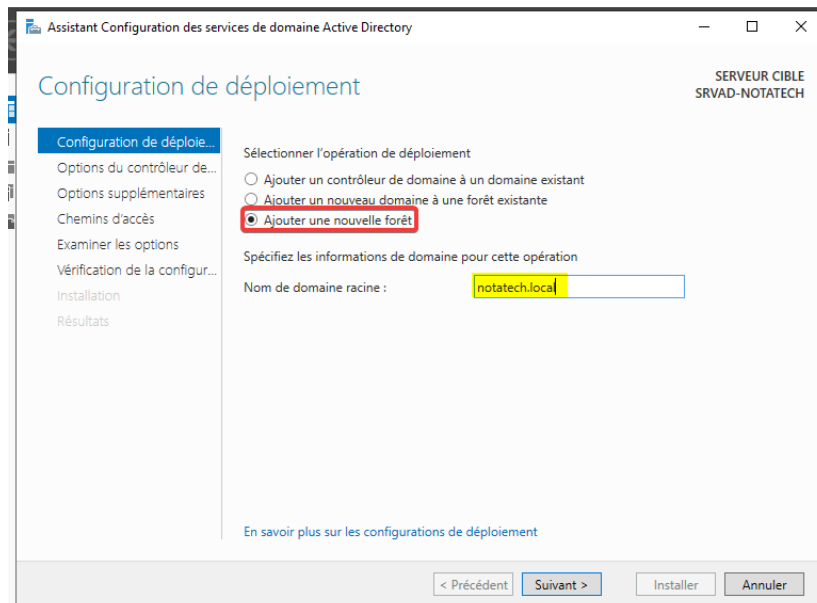


Ensuite une fois installé je clique sur le drapeau et je clique sur promouvoir ce serveur en contrôleur de domaine

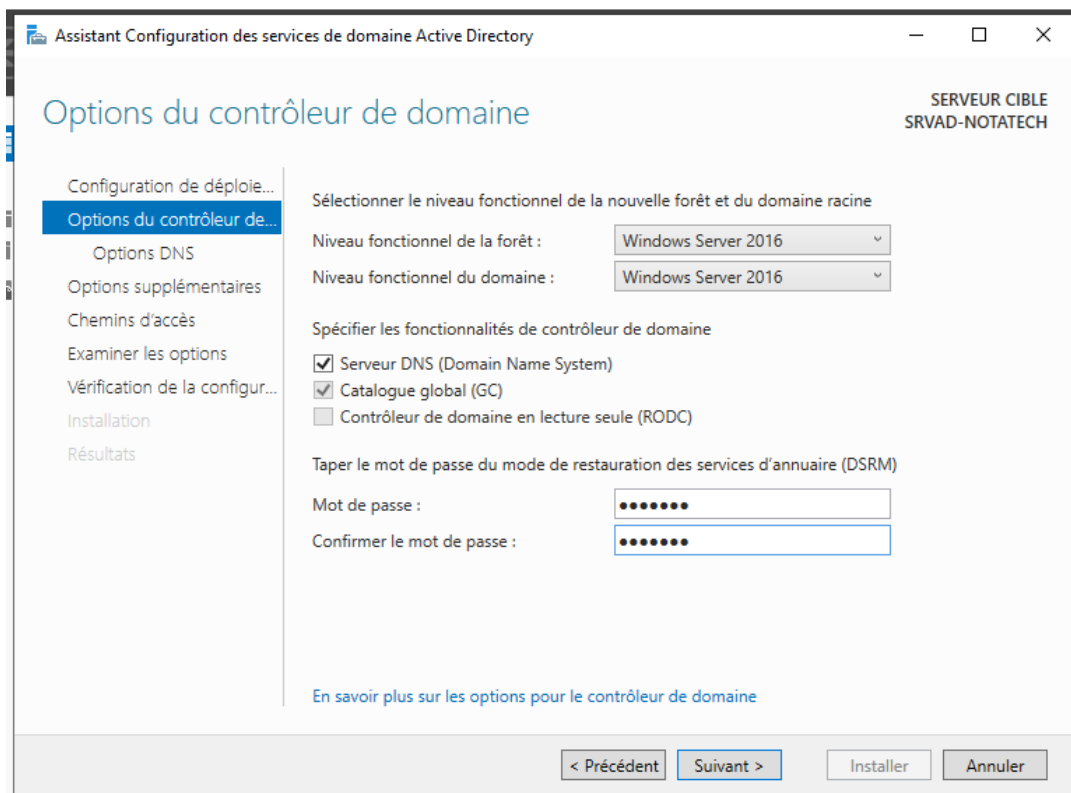


Création d'une nouvelle forêt AD

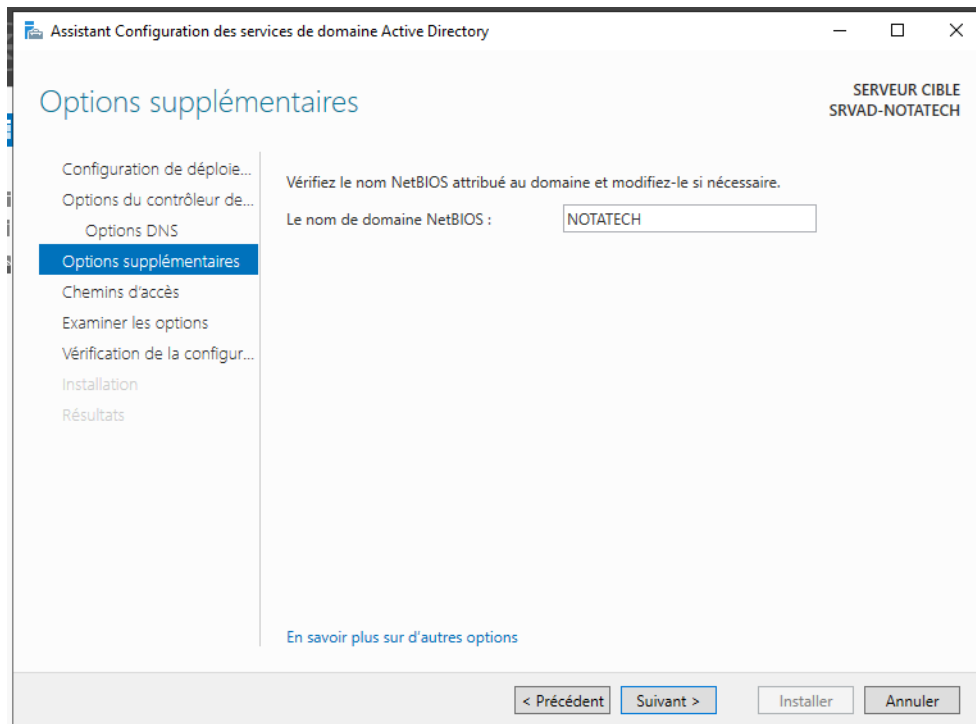
Je commence ici à créer une infrastructure Active Directory (AD) en définissant une nouvelle forêt avec le domaine racine notatech.local. C'est une étape essentielle pour centraliser la gestion des utilisateurs, des groupes, et des politiques réseau.



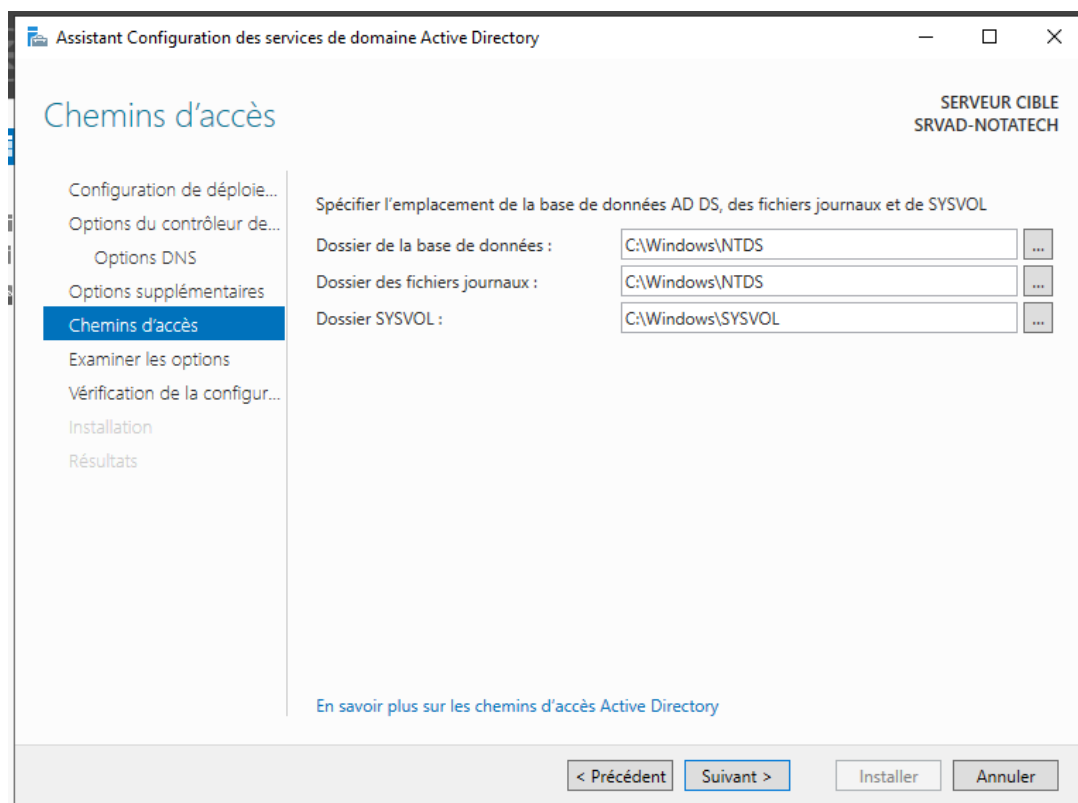
J'ai choisi le niveau fonctionnel Windows Server 2016 pour garantir une compatibilité avec les fonctionnalités nécessaires. Le rôle DNS et le Catalogue Global sont activés pour permettre une gestion efficace des authentifications et des résolutions de noms dans le domaine.



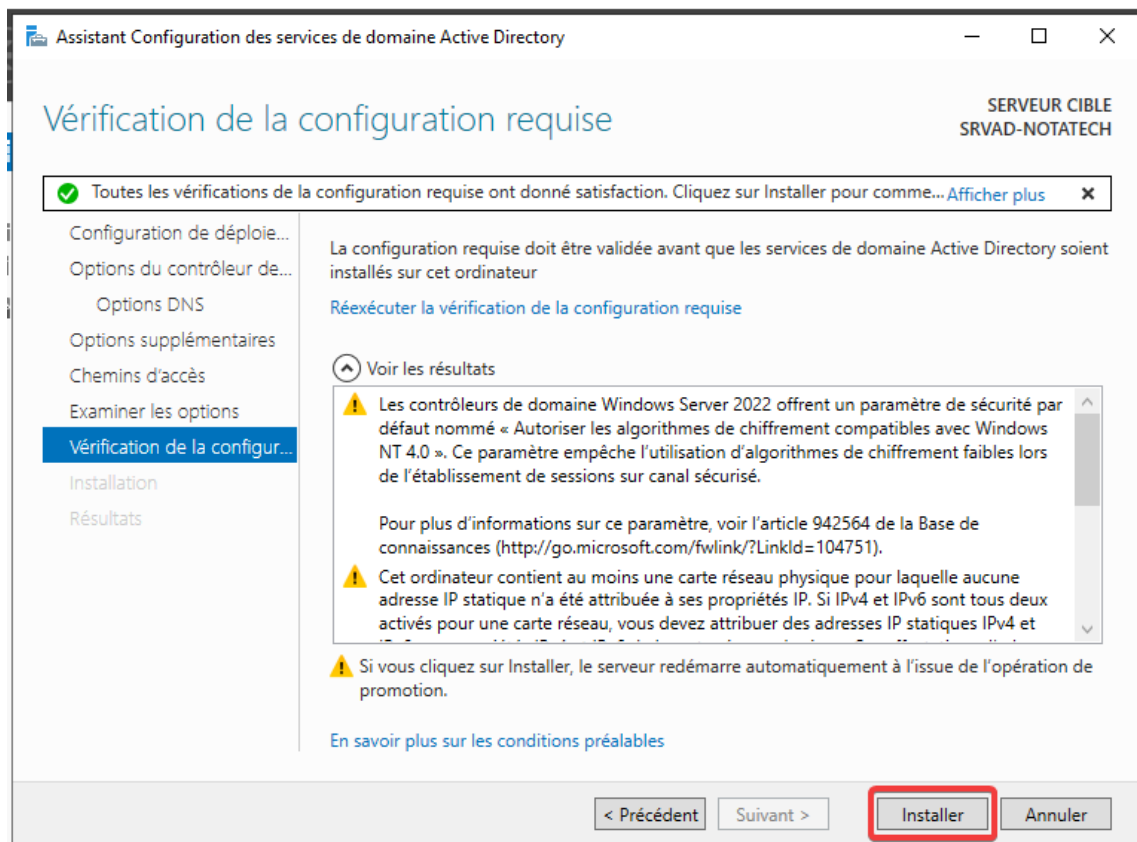
À cette étape, j'ai confirmé le nom NetBIOS NOTATECH pour simplifier les identifications réseau.



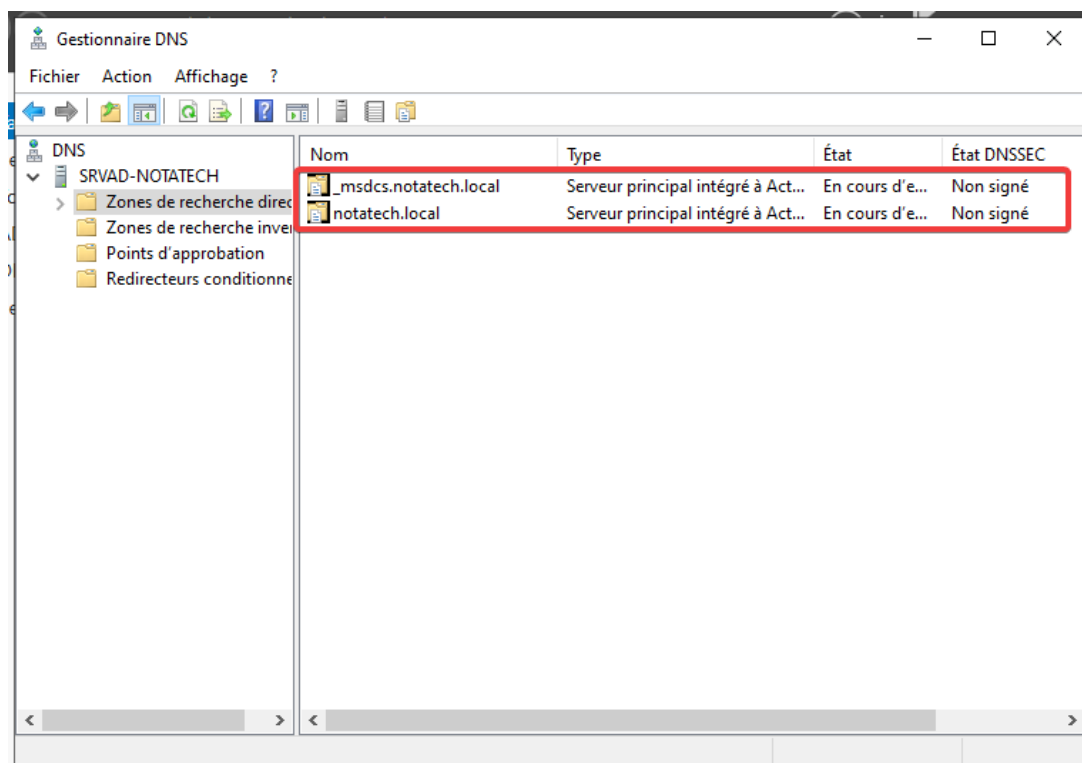
J'ai également validé les chemins d'accès par défaut pour les fichiers critiques de l'Active Directory.



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.

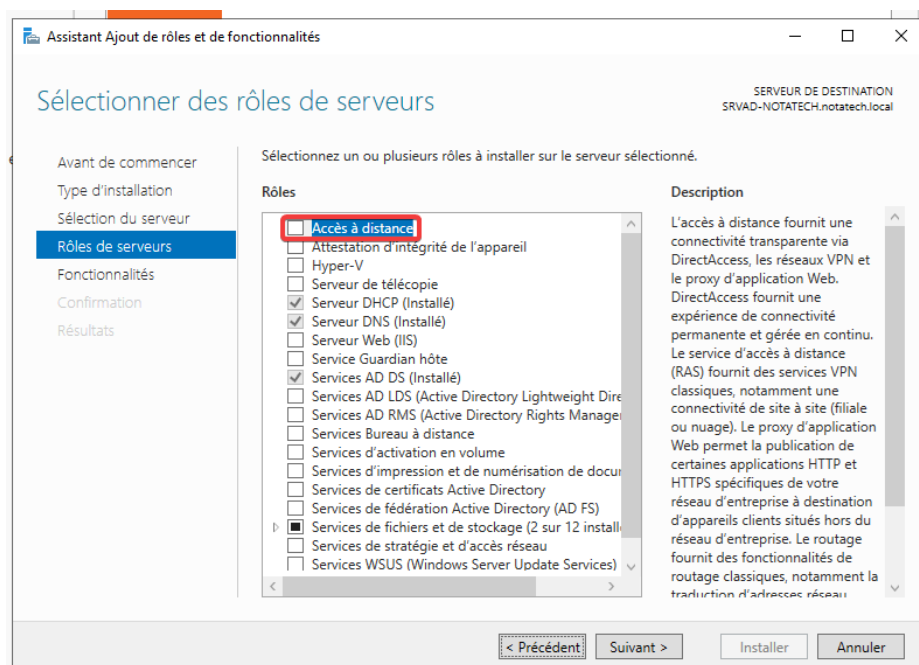


Je vérifie ensuite que les zones de recherches directes se sont bien créées

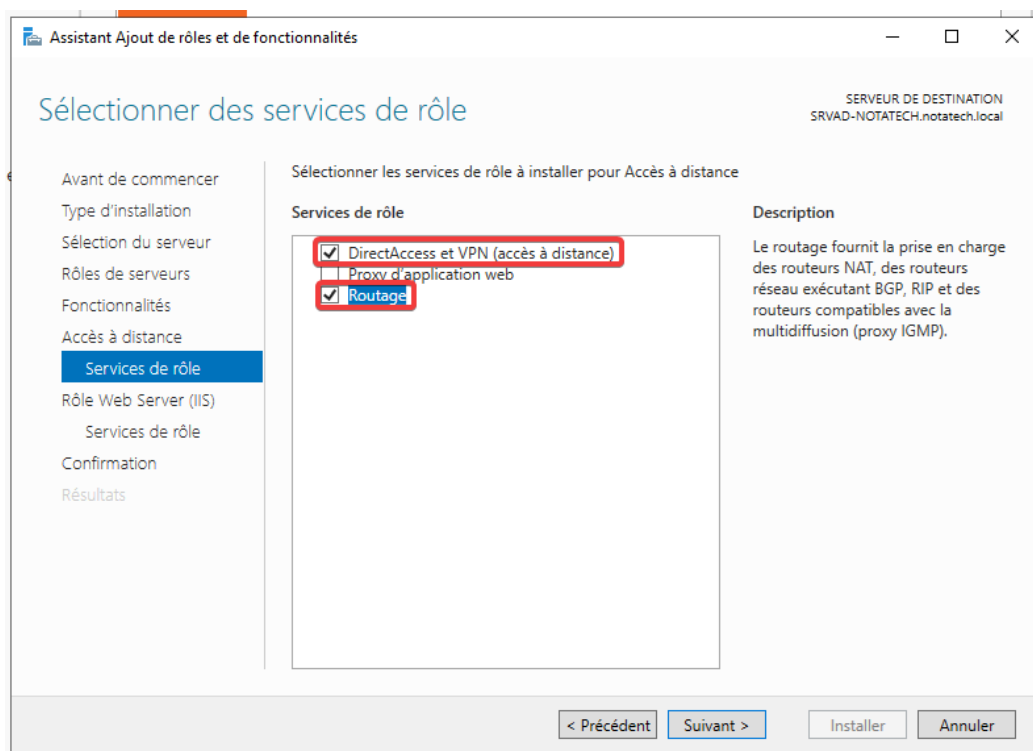


Sélection des rôles d'accès à distance :

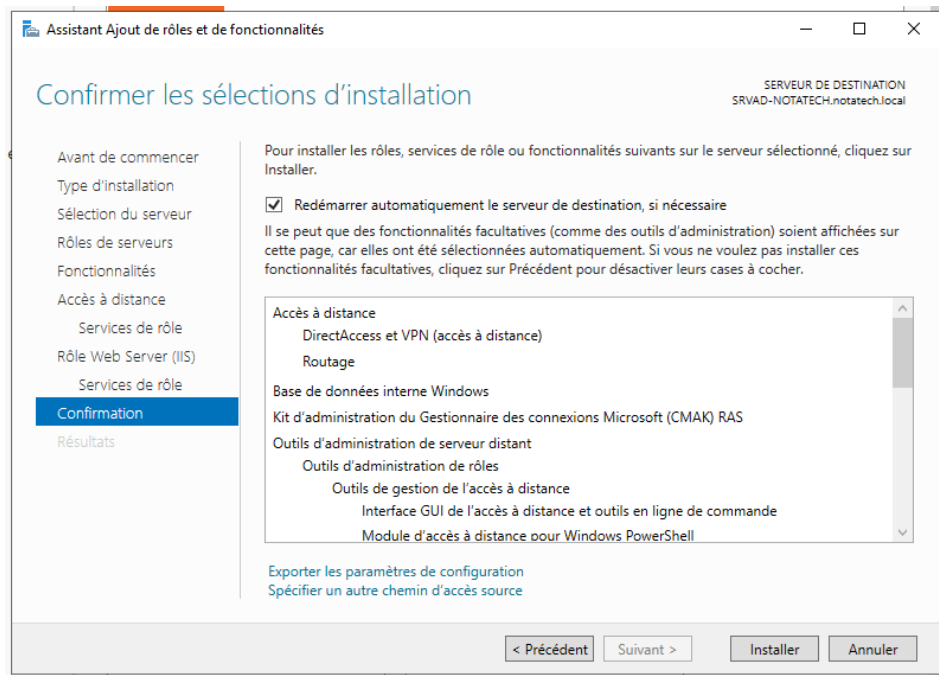
Pour permettre le routage et l'accès distant, j'ai ajouté les rôles « Accès à distance » par l'ajout de rôles et de fonctionnalités



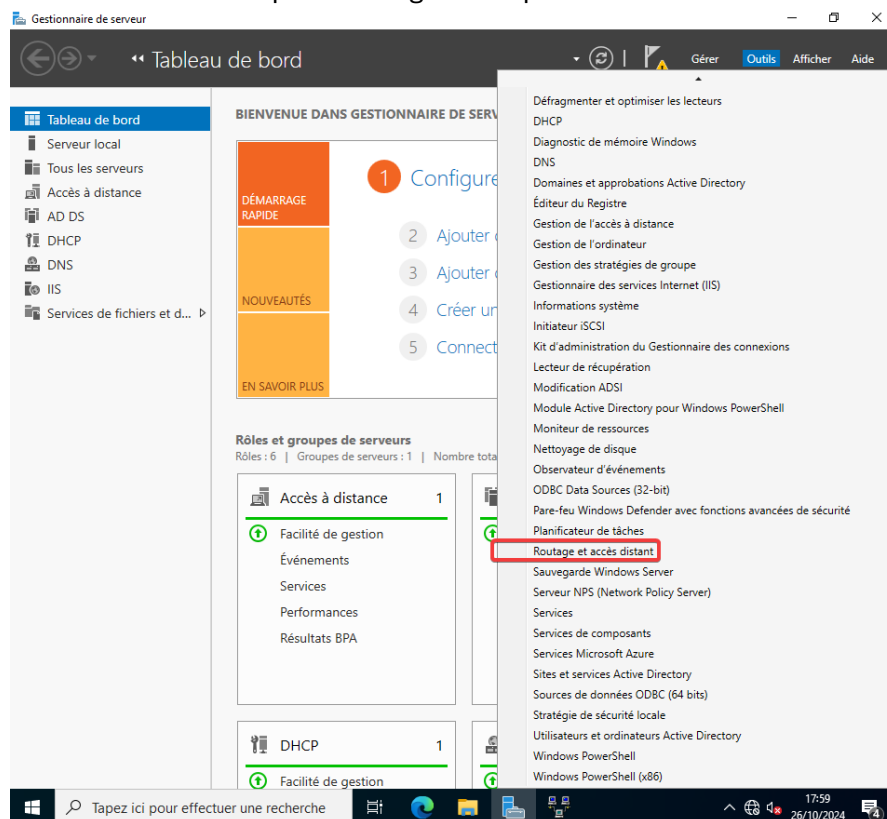
Ensuite je sélectionne direct Access et VPN (qui nous servira plus tard). Ces fonctionnalités assureront que les utilisateurs pourront se connecter au réseau de manière sécurisée.



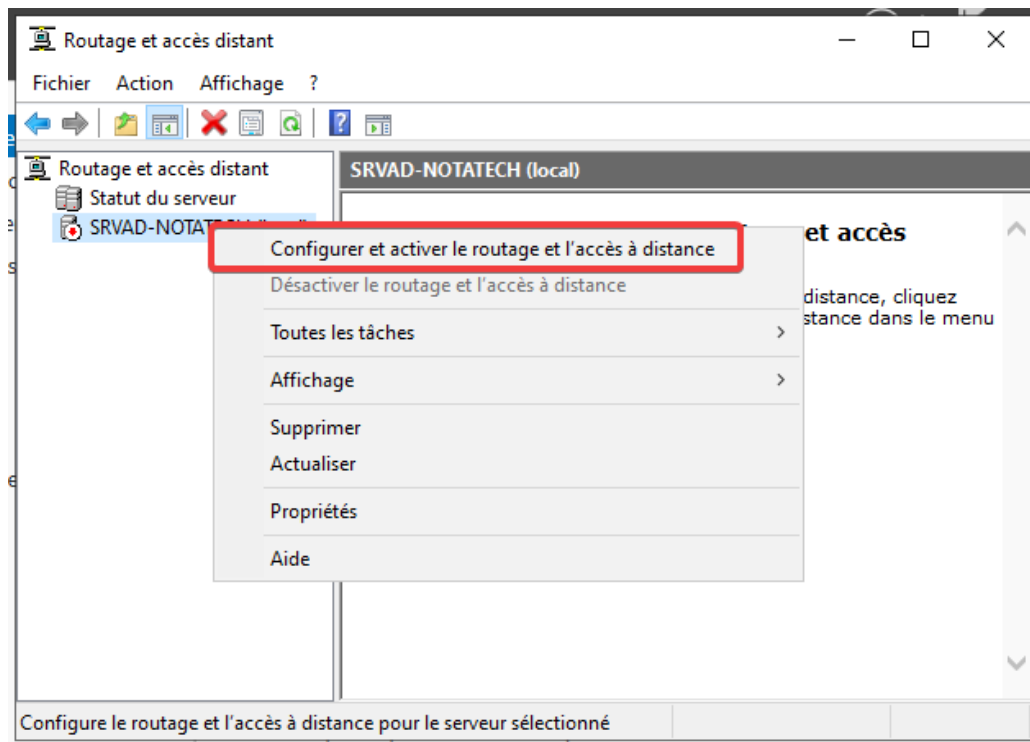
J'ai confirmé l'installation des services comme le routage NAT et DirectAccess. Ces services permettront de gérer les connexions VPN et d'assurer la sécurité des communications entre les machines.



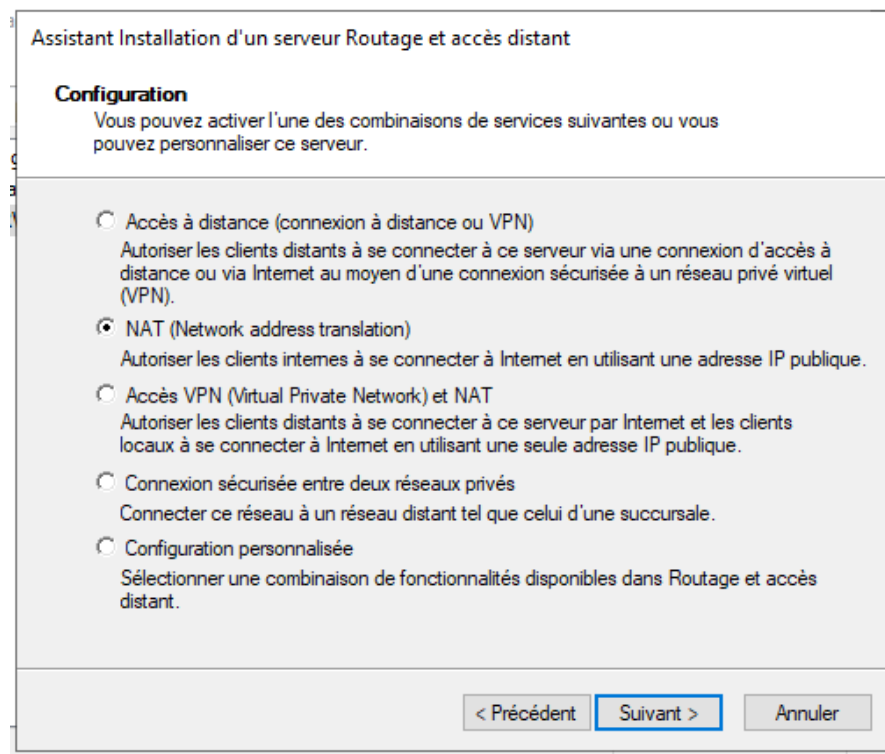
Après l'installation, j'ai ouvert l'outil "Routage et accès distant" pour configurer les paramètres NAT. Cela permettra à mes machines internes d'accéder à Internet tout en maintenant une protection grâce au pare-feu.



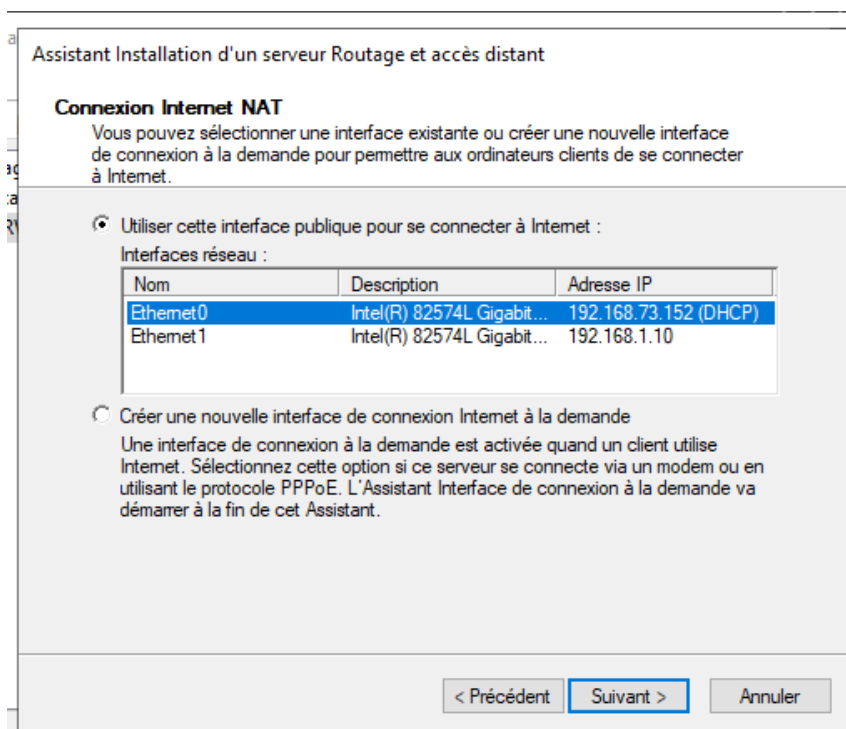
Enfin, j'ai activé la fonction NAT sur le serveur pour qu'il puisse rediriger le trafic entre mon réseau interne et Internet. Pour ce faire, sur la fenêtre qui vient de s'ouvrir je fais une clique droit sur mon serveur et je clique sur « configurer et activer le routage et l'accès à distance »



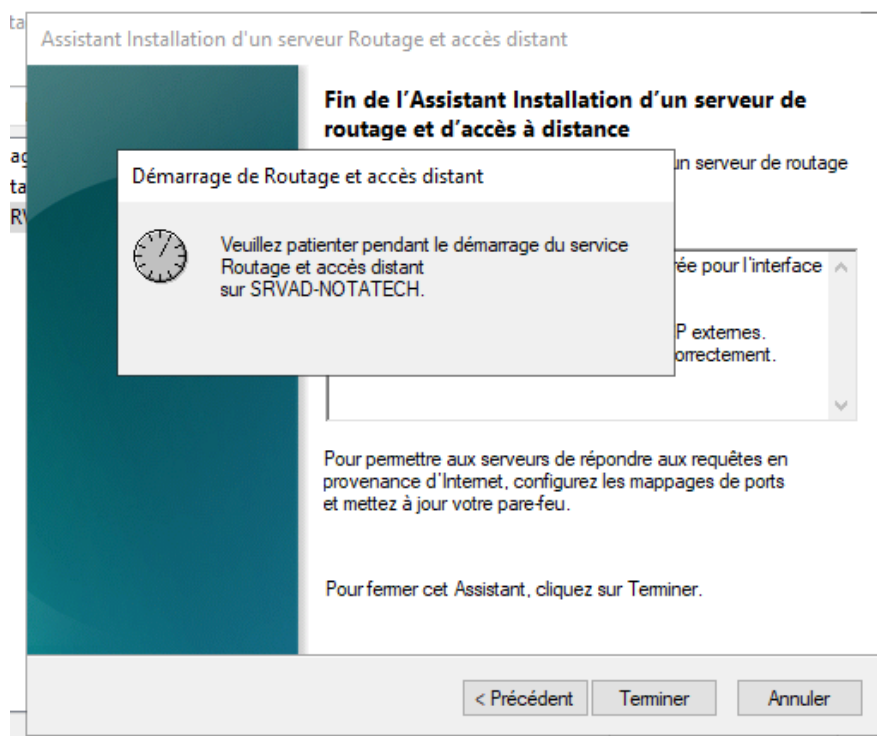
Dans cette étape, j'ai choisi l'option "NAT (Network Address Translation)" pour permettre aux machines de mon réseau interne d'accéder à Internet à travers une adresse publique.



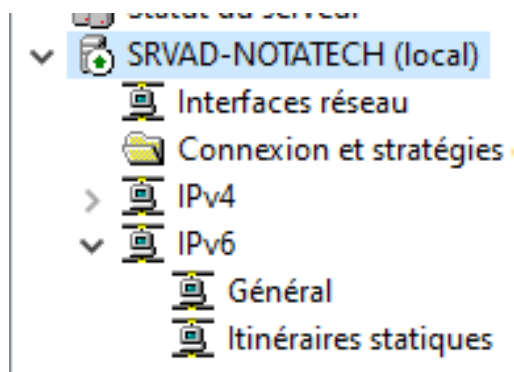
J'ai sélectionné l'interface réseau correspondant à ma carte NAT, associée à l'adresse IP fournie par le DHCP (192.168.73.152). Cette interface sera utilisée comme passerelle pour rediriger le trafic Internet.



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



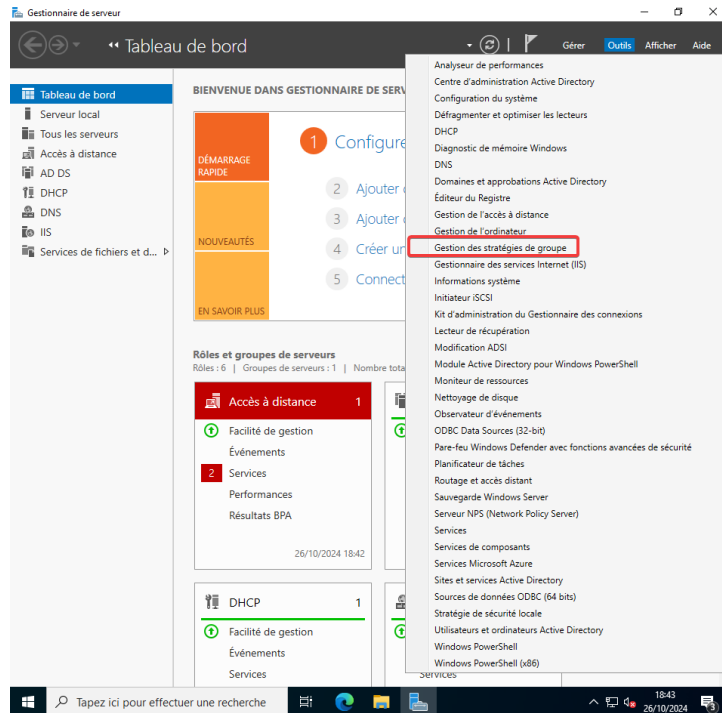
L'installation finalement terminée je vérifie qu'il est bien actif, il l'est bien donc l'installation et la configuration du rôle "Routage et accès distant" sont terminées. Le serveur est maintenant prêt à gérer le trafic NAT pour permettre l'accès à Internet depuis le réseau interne.



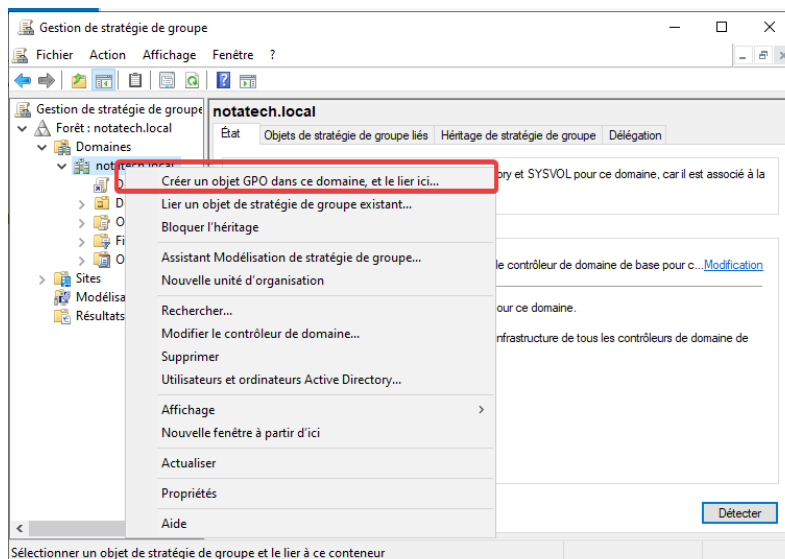
Création de GPO :

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

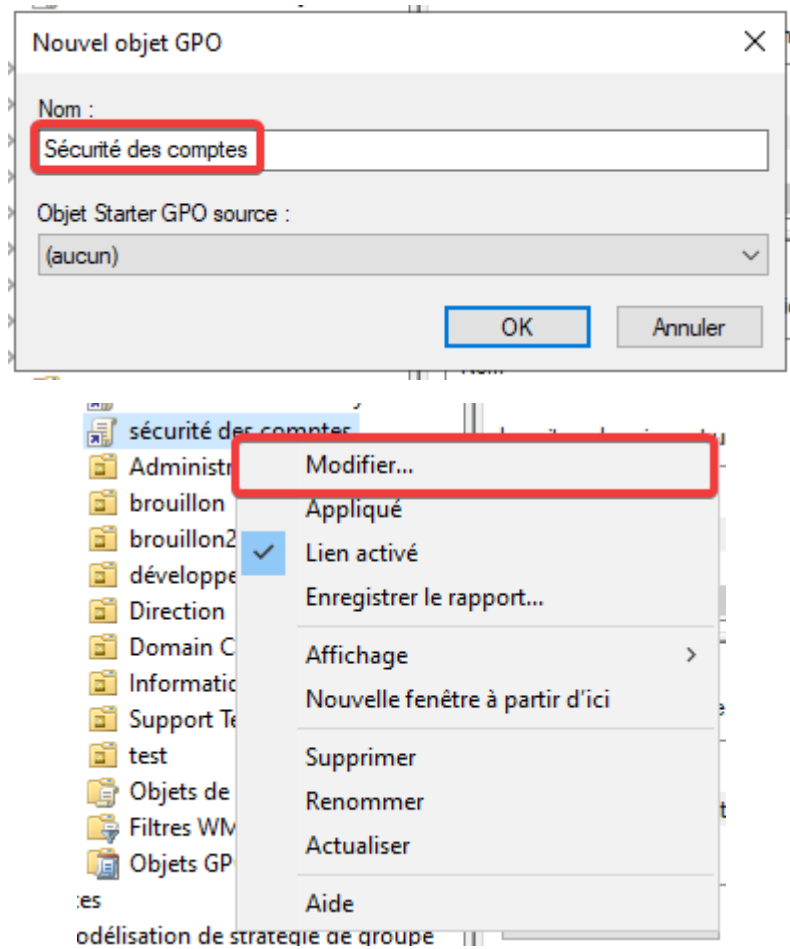
Dans le tableau de bord du serveur, je clique sur Outils, puis sur Gestion des stratégies de groupe pour ouvrir la console GPO.



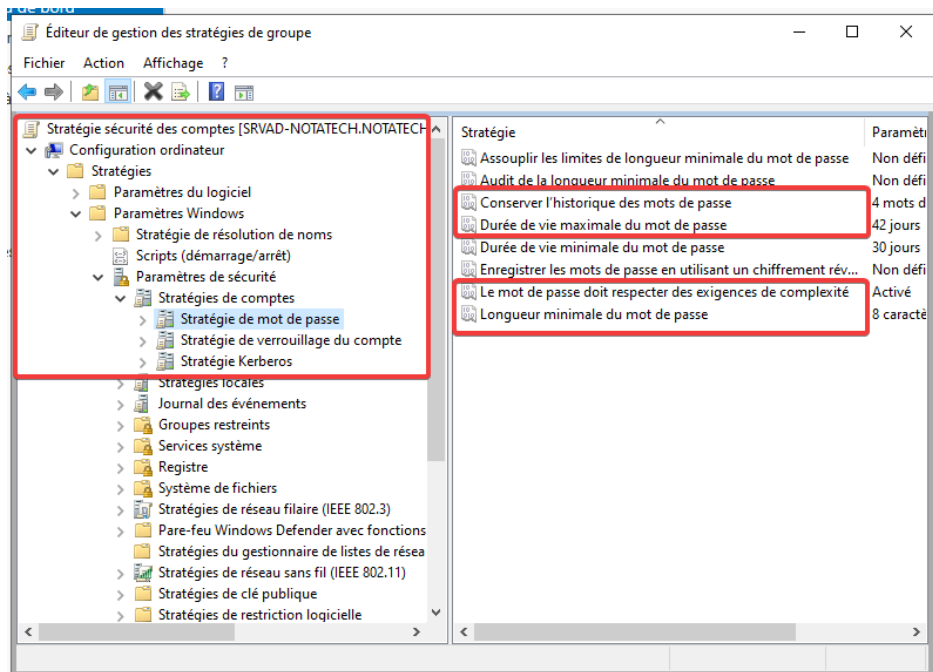
Dans la console **Gestion des stratégies de groupe**, je fais un clic droit sur le domaine **notatech.local**, puis je sélectionne **Créer un objet GPO dans ce domaine et le lier ici**.



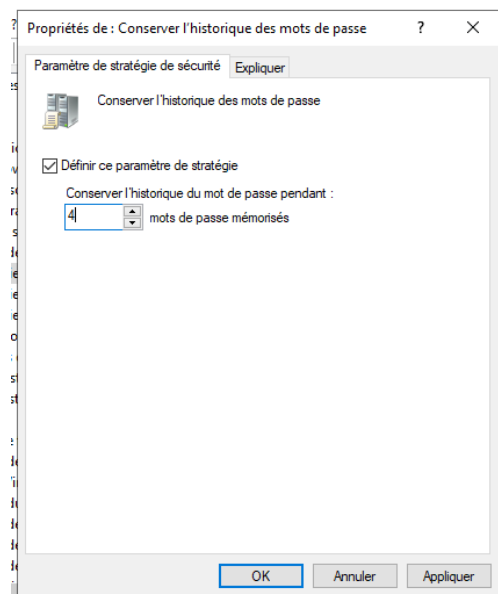
Je donne un nom explicite à la GPO, comme ici "**Sécurité des comptes**". Et je fais un clic droit
« modifier »



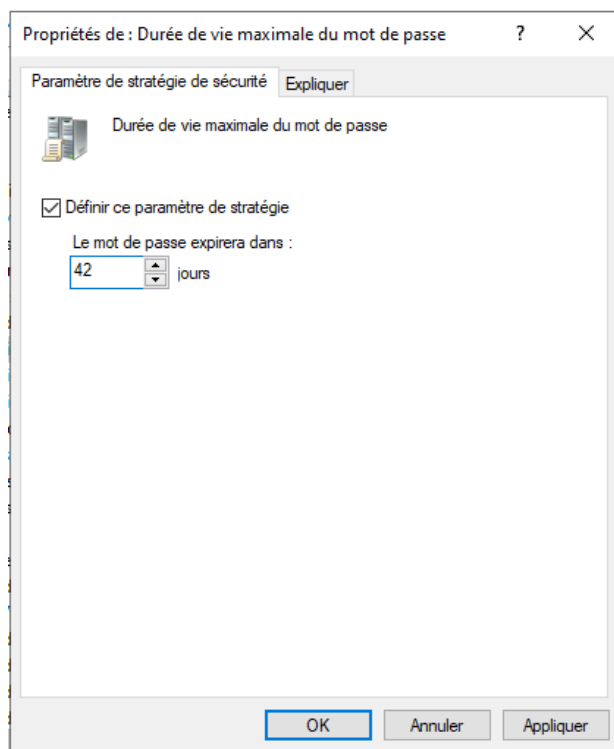
Je me rends donc ensuite au chemin « **configuration ordinateur > paramètres Windows > paramètres de sécurité** » dans cette fenêtre je repère ces paramètres et je vais cliquer dessus pour les modifier



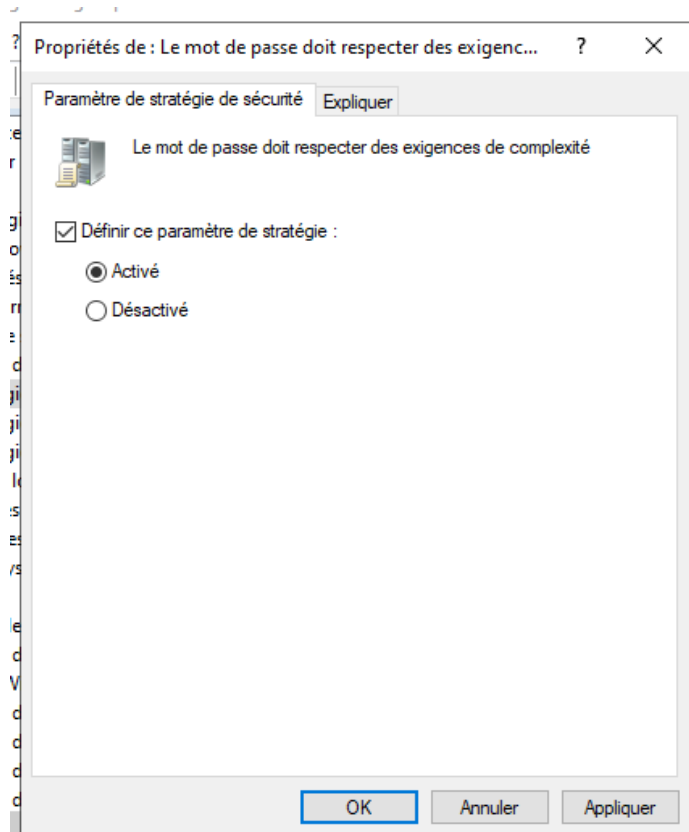
Je choisis tout d'abord de conserver un historique de au moins 4 mots de passe



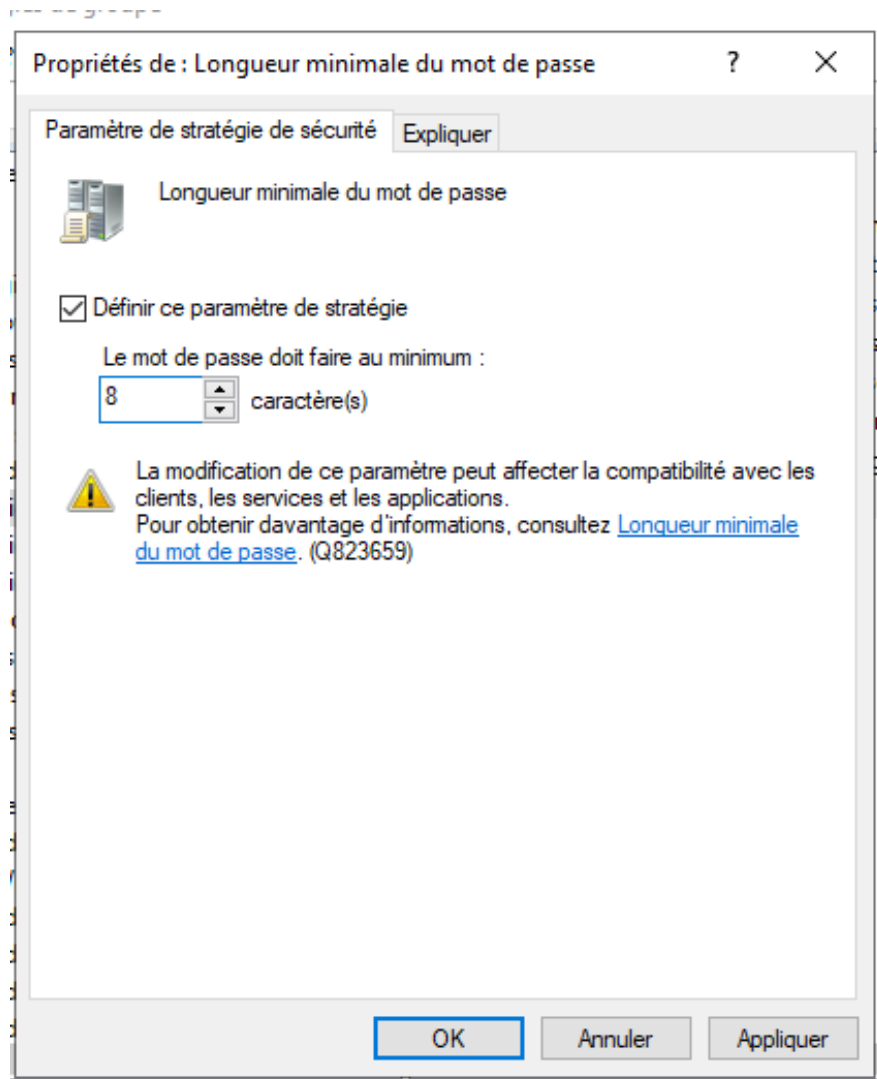
Ensuite je sélectionne la durée de vie maximale pour un mot de passe de 42 jours



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

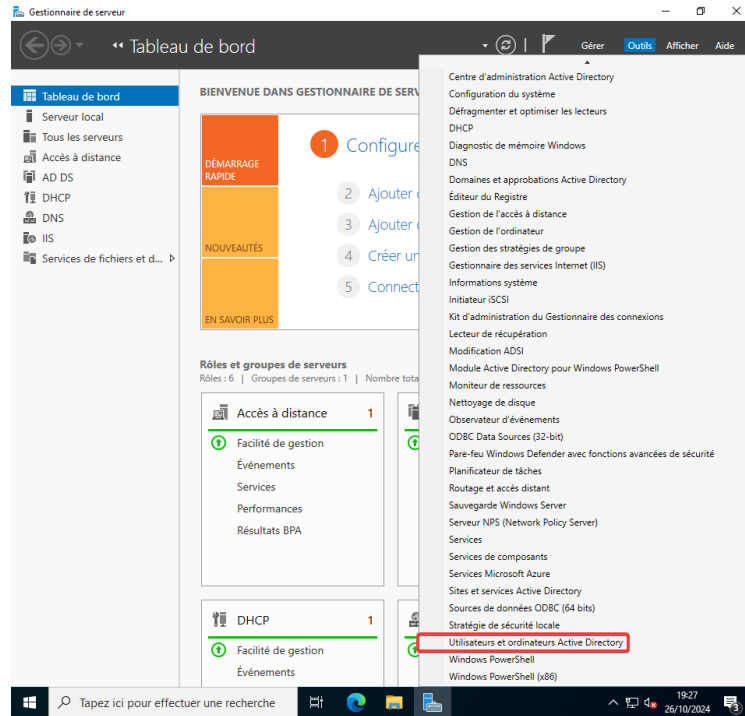


Et finalement pour la longueur minimale des mots de passe, je saisi un minimum de 8 caractères

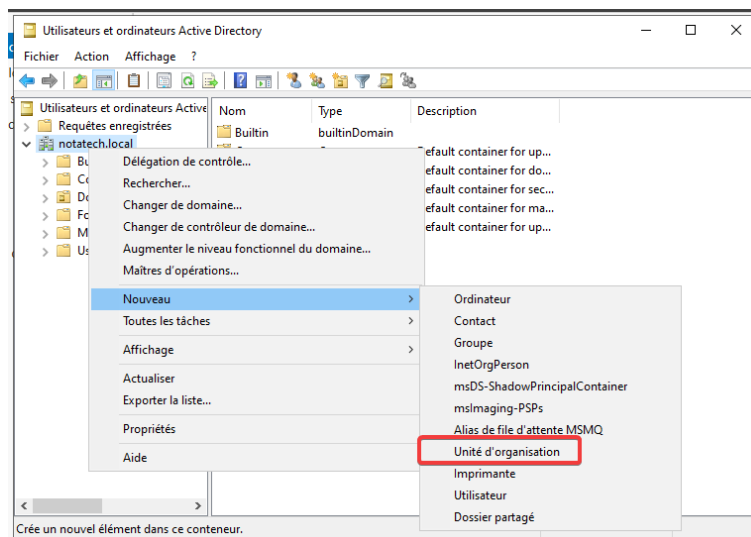


Création des utilisateurs et des unités d'organisation :

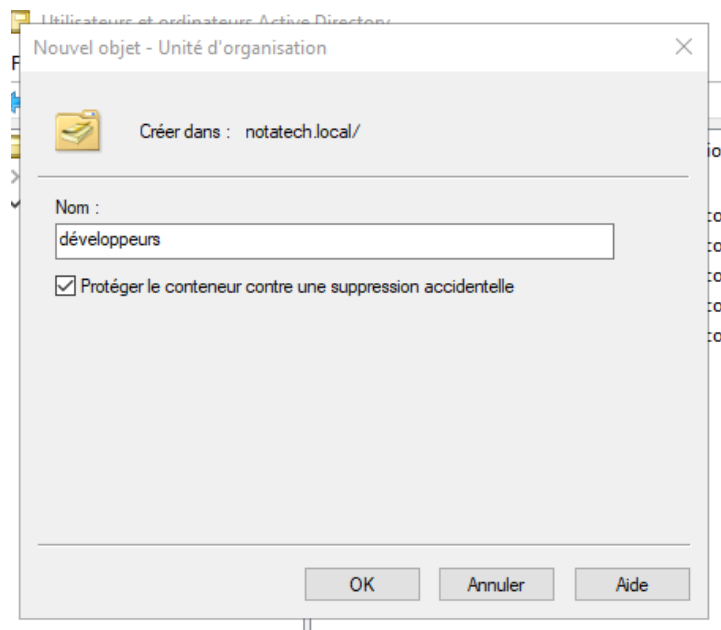
Pour commencer la création, je me rends tout d'abord dans « utilisateurs et ordinateurs Active Directory » dans les outils de Windows server



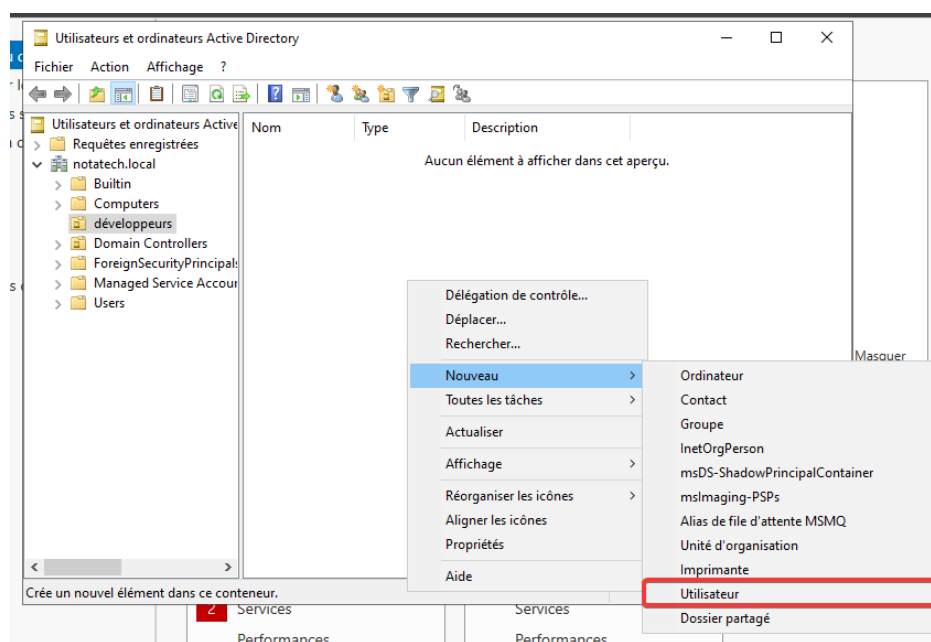
Ensuite une fois dans cette fenêtre je fais un clic droit, nouveau et sélectionne « unité d'organisation » pour commencer a créer une unité d'organisation



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 »

Nouvel objet - Utilisateur

Créer dans : notatech.local/développeurs

Prénom : Marshall Initiales :

Nom : D

Nom complet : Marshall D

Nom d'ouverture de session de l'utilisateur : D.marshall @notatech.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : NOTATECH\ D.marshall

< Précédent Suivant > Annuler

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)

Nouvel objet - Utilisateur

Créer dans : notatech.local/développeurs

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

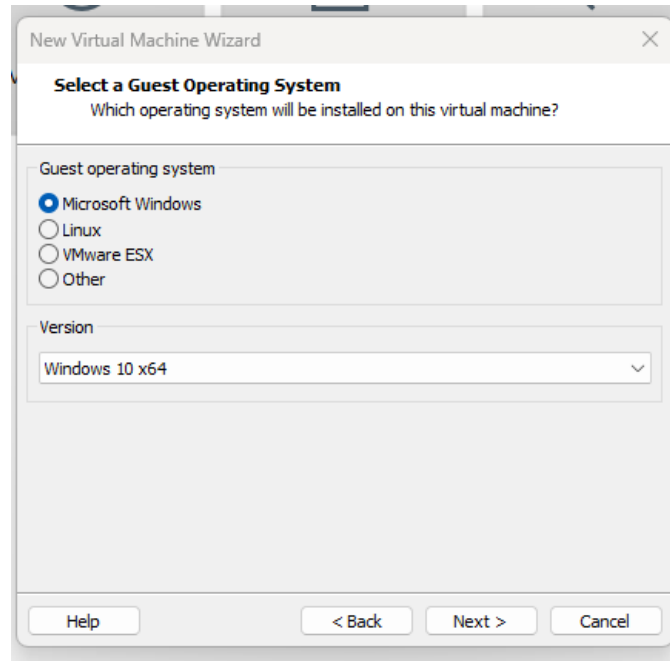
☐ Le compte est désactivé

< Précédent Suivant > Annuler

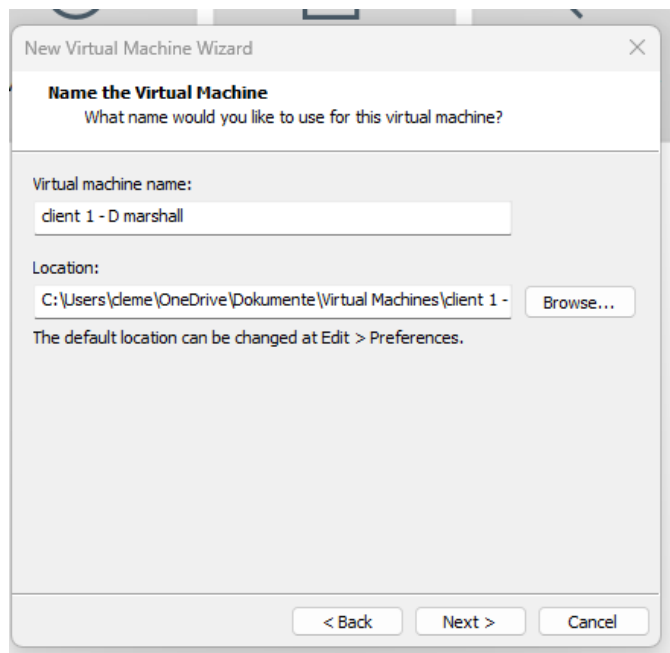
Test sur une machine cliente :

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

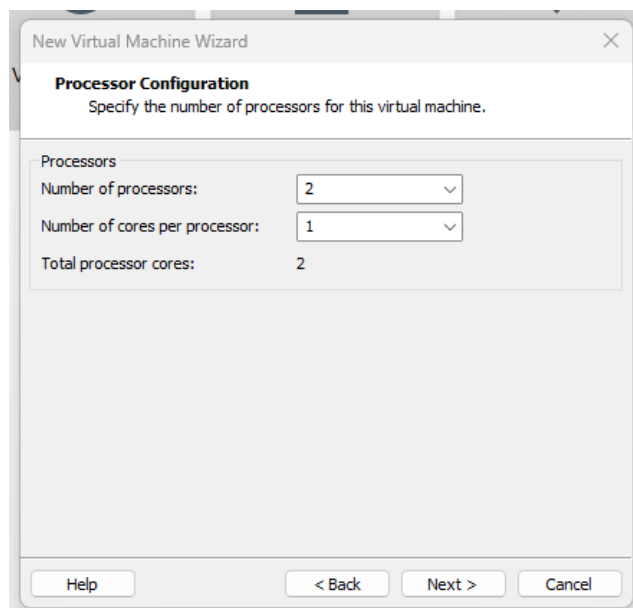
Je commence par créer une nouvelle machine virtuelle et sélectionne Windows 10



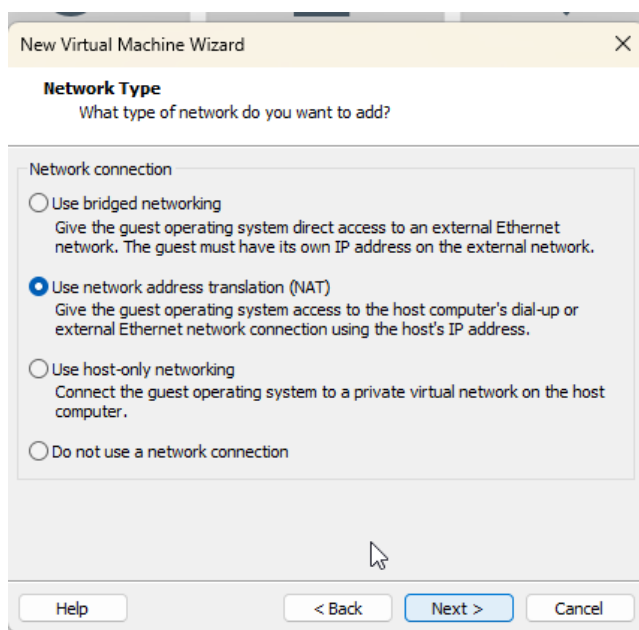
Je donne à ma machine le nom de « client 1 – D marshall »



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

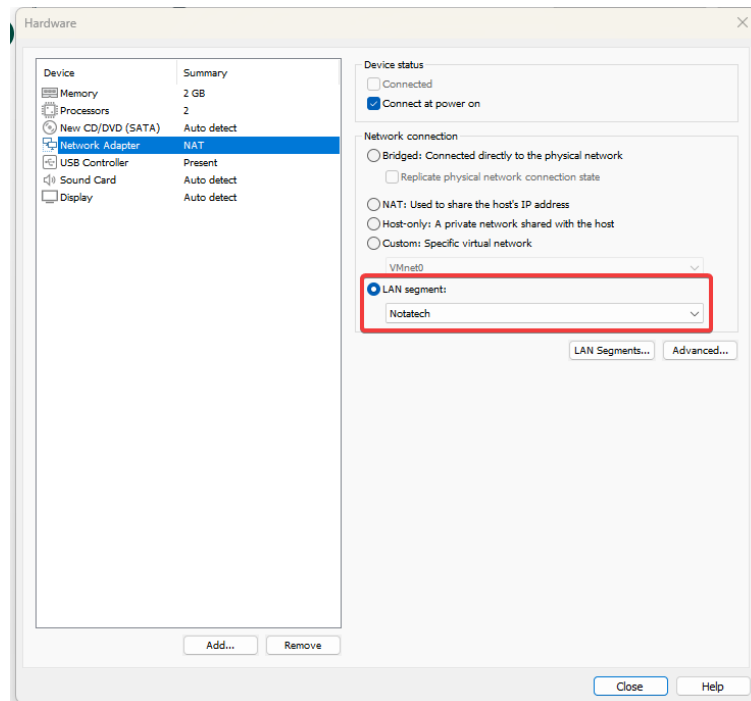


Je choisis ensuite une connexion NAT (par défaut) que nous allons changer ensuite pour utiliser la connexion LAN segment « notatech » pour se connecter au même LAN que le serveur

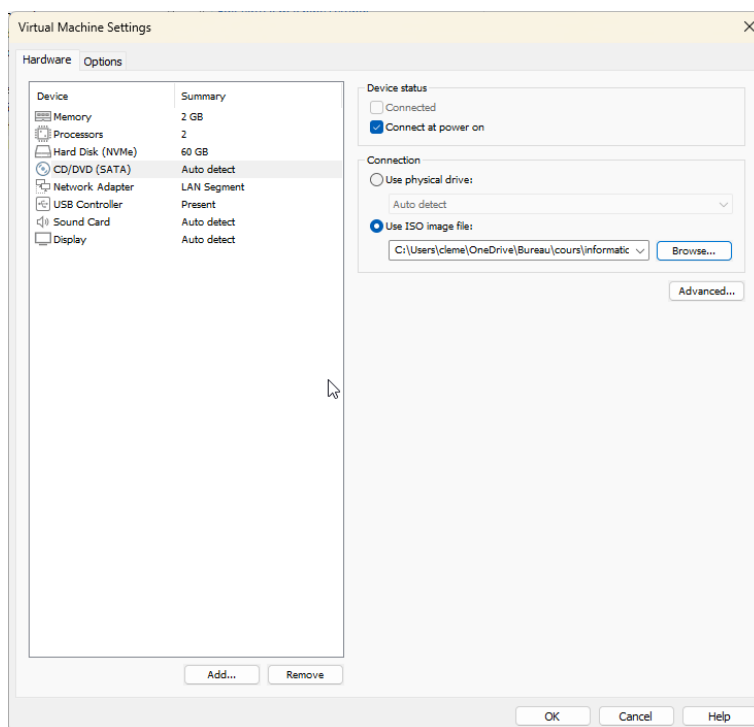


Et ensuite je laisse les paramètres par défaut pour le reste de la configuration

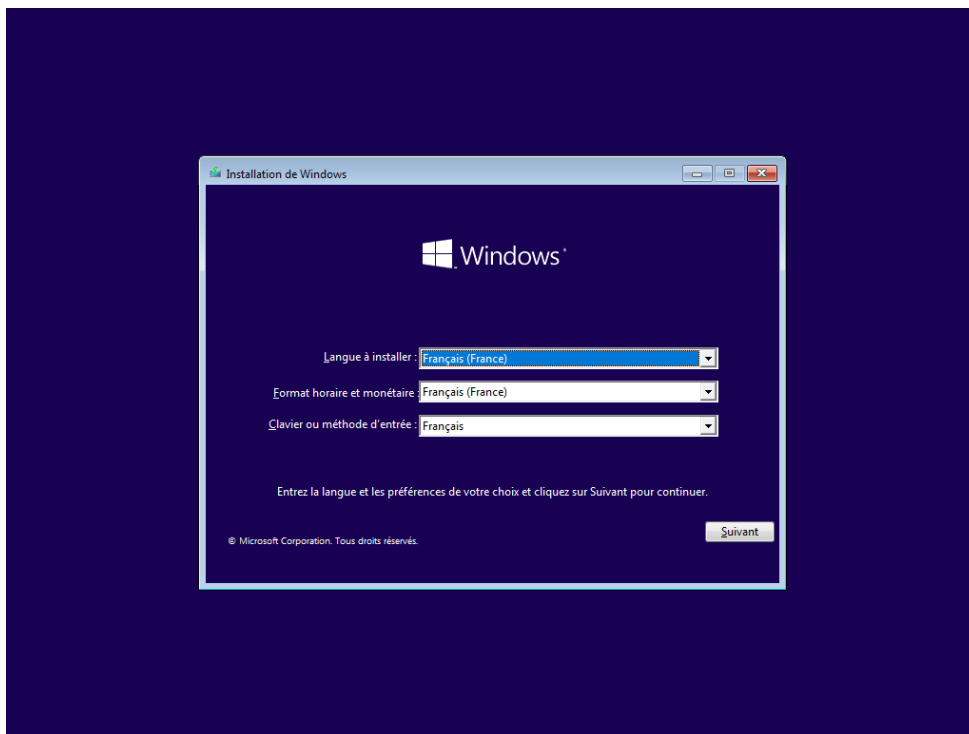
Ensuite je me rends dans la configuration hardware de la machine et change la connexion réseau a « LAN segment » et sélectionne mon LAN segment précédemment créer pour le réseau Notatech



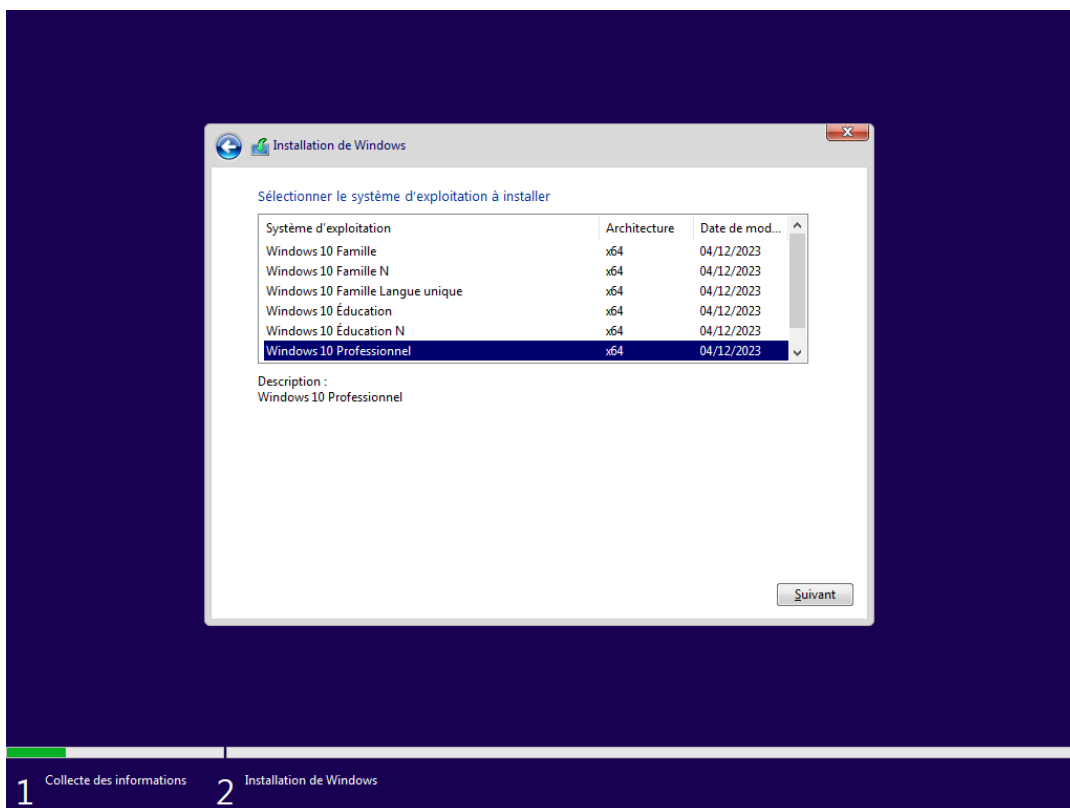
Et je me rends finalement dans « CD/DVD », sélectionne « Use ISO image file » et sélectionne mon ISO de Windows 10 classique



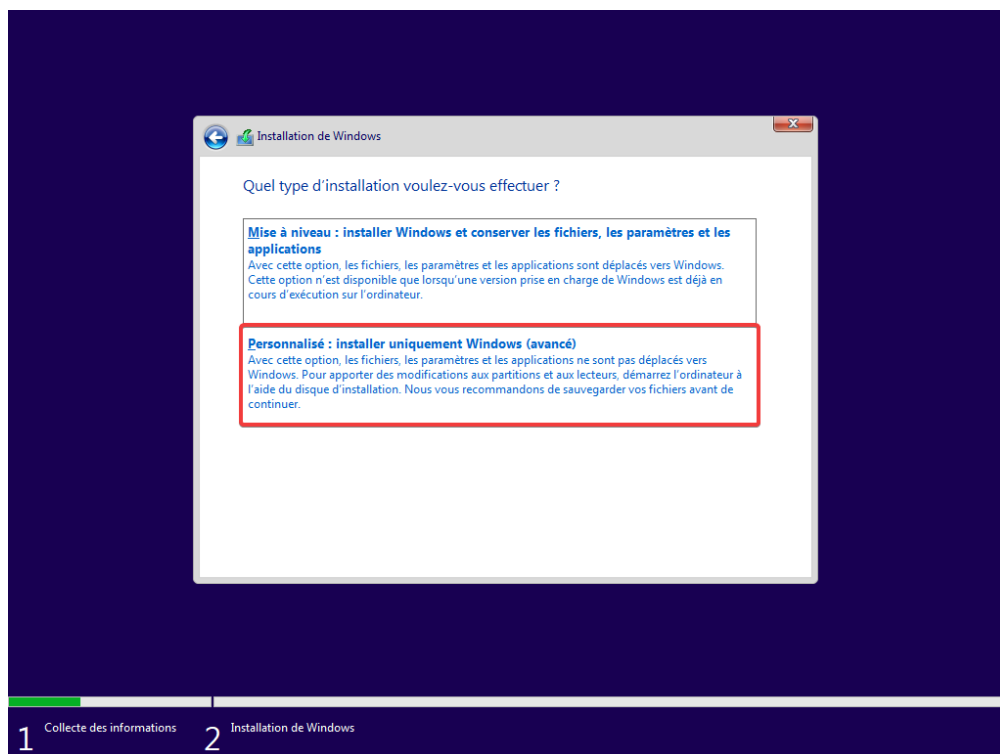
Ensuite je lance donc ma machine virtuelle, arrivé sur cet écran je clique sur « suivant »



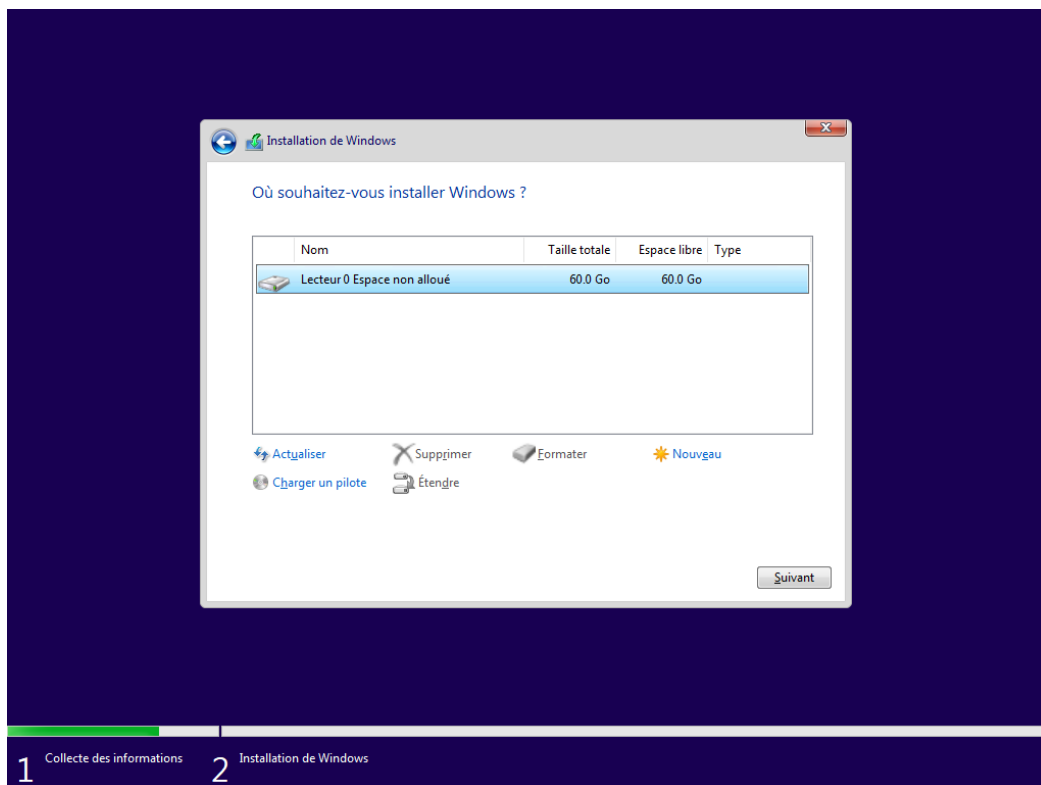
Je sélectionne ici « Windows 10 professionnel »



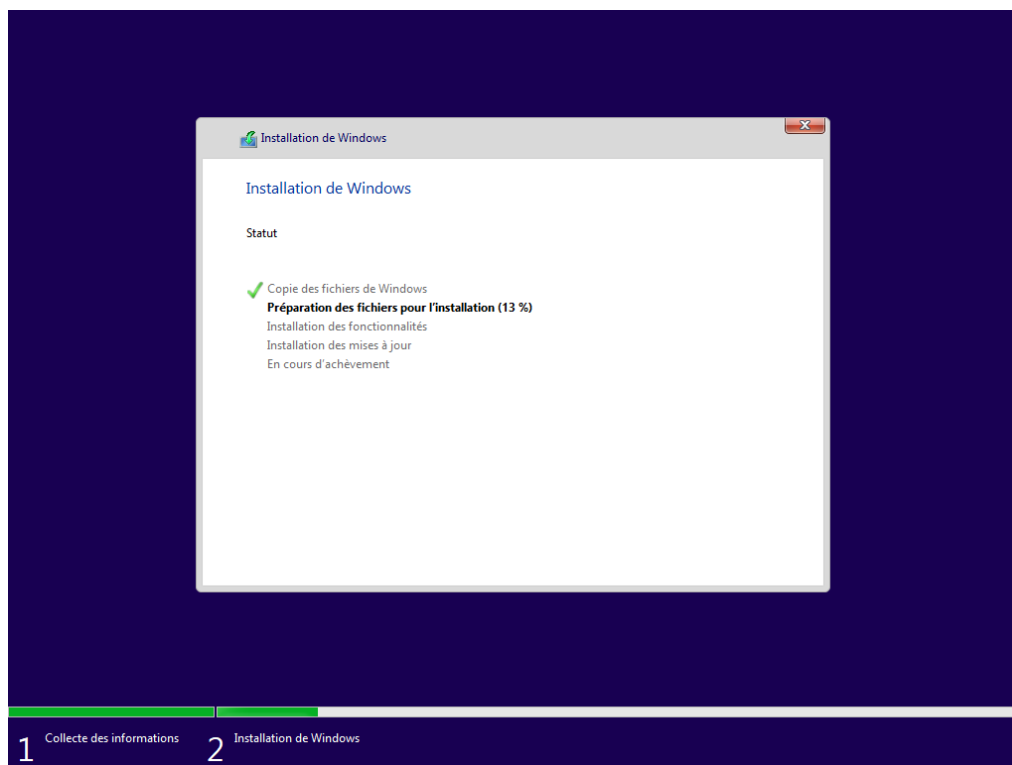
Pour le type d'installation je sélectionne « **personnalisé** »



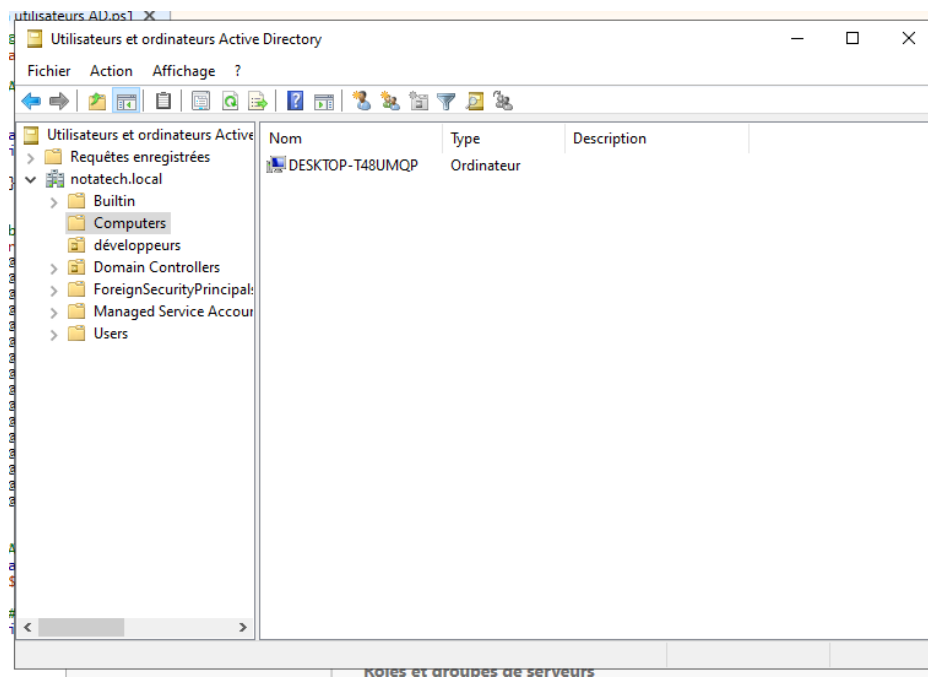
Ici je sélectionne simplement mon disque



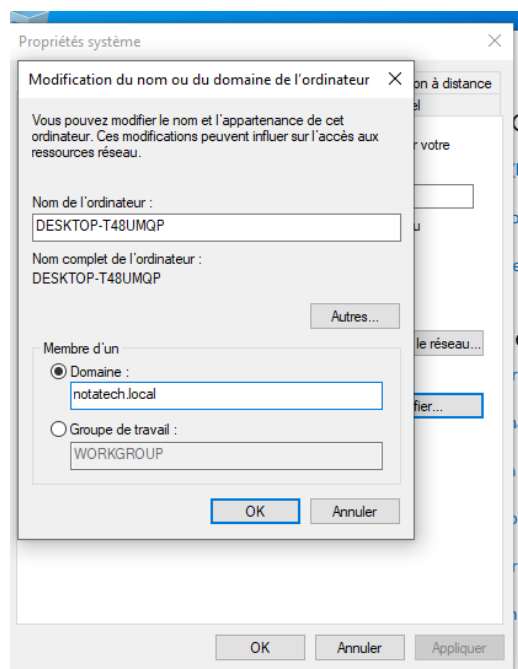
L'installation va donc se lancer avant de pouvoir finalement lancer la machine cliente



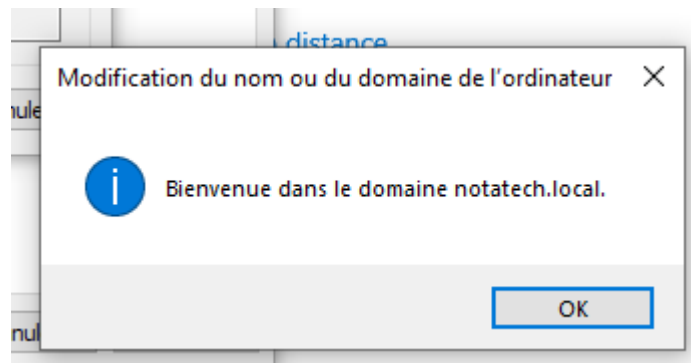
Avant de pouvoir me connecter avec cette machine je dois l'ajouter a mon domaine sur mon windows server, je récupère donc le nom de ma machine et l'ajoute dans la section « computers » de mon Active directory



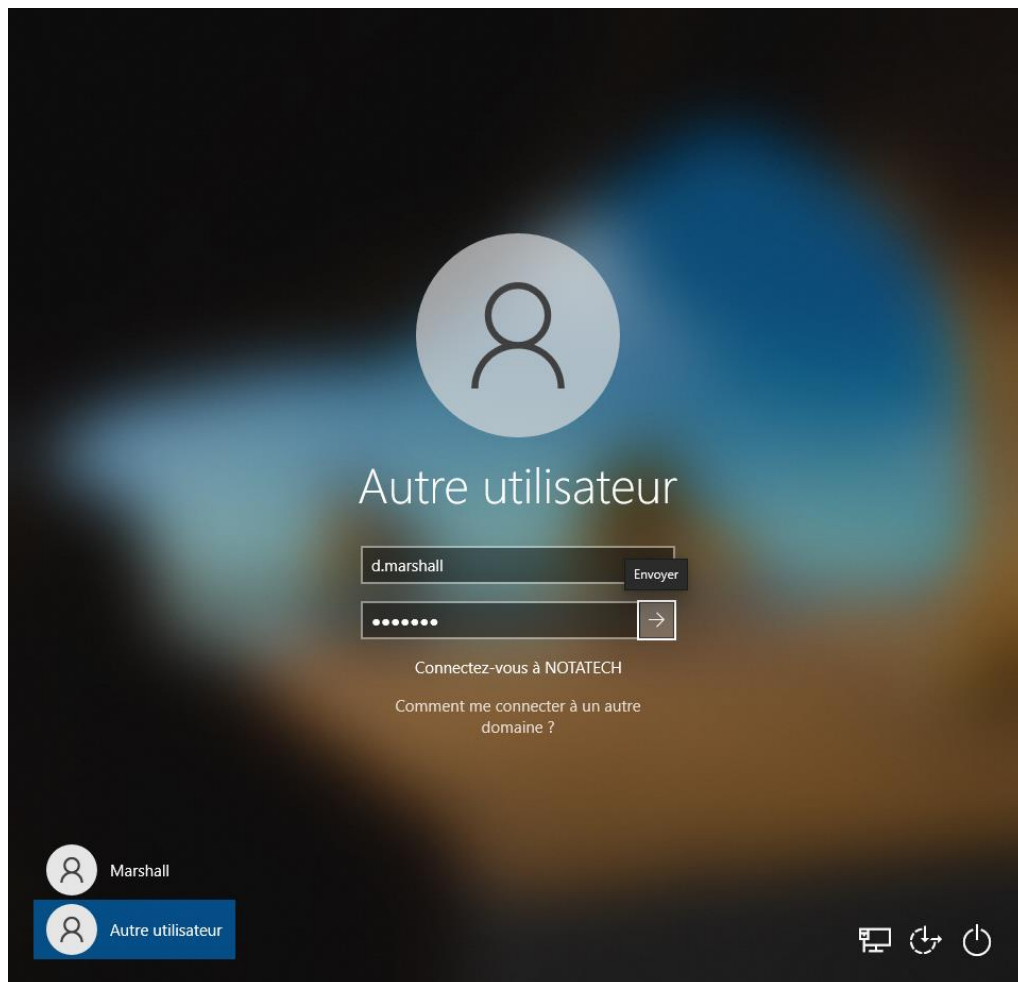
Ensuite sur ma machine cliente, une fois connecté je l'ajoute au domaine que j'ai créer précédemment « notatech.local ».



Ce message apparaîtra 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 vérifie que la connexion à internet fonctionne bien, ping OK tout est bon au niveau de ça

```

C:\> Invite de commandes

Microsoft Windows [version 10.0.19045.3803]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\d.marshall>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=12 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=13 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=42 ms TTL=127

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 11ms, Maximum = 42ms, Moyenne = 19ms

C:\Users\d.marshall>_

```

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 Lemoir	Secrétaire	Administratif	ilemoir	
Marc Beaulieu	Secrétaire	Administratif	mbeaulieu	
Sophie Thibault	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	

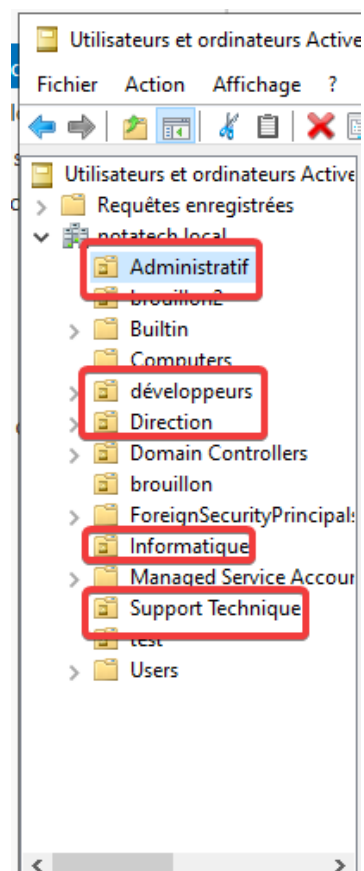
Voici mon script, ce script va me permettre de créer tous les utilisateurs et mes unités d'organisation en respectant le tableau mentionné avant, tout en activant l'option **l'utilisateur devra changer de mot de passe** et désactivant l'option **le mot de passe n'expire jamais**

```

script création utilisateurs AD.ps1* X
1 # Définir le nom du domaine
2 $domain = "notatech.local"
3
4 # Créer les unités d'organisation (OU)
5 $sous = @("Direction", "Informatique", "Administratif", "Support Technique")
6
7 foreach ($sou in $sous) {
8     if (-not (Get-ADOrganizationalUnit -Filter "Name -eq '$sou'" -ErrorAction SilentlyContinue)) {
9         New-ADOrganizationalUnit -Name $sou -Path "DC=notatech,DC=local"
10     }
11 }
12
13 # Tableau des utilisateurs à créer
14 $users = @(
15     @{ Nom = "Pierre Duval"; Poste = "PDG"; Secteur = "Direction"; NomUtilisateur = "pierre.duval" },
16     @{ Nom = "Clara Dupuis"; Poste = "Développeur"; Secteur = "Informatique"; NomUtilisateur = "clara.dupuis" },
17     @{ Nom = "Antoine Lambert"; Poste = "Développeur"; Secteur = "Informatique"; NomUtilisateur = "antoine.lambert" },
18     @{ Nom = "Laura Martine"; Poste = "Développeur"; Secteur = "Informatique"; NomUtilisateur = "laura.martine" },
19     @{ Nom = "Julien Moreau"; Poste = "Développeur"; Secteur = "Informatique"; NomUtilisateur = "julien.moreau" },
20     @{ Nom = "Nadia Girard"; Poste = "Développeur"; Secteur = "Informatique"; NomUtilisateur = "nadia.girard" },
21     @{ Nom = "Isabelle Lemoine"; Poste = "Secrétaire"; Secteur = "Administratif"; NomUtilisateur = "isabelle.lemoine" },
22     @{ Nom = "Marc Beaulieu"; Poste = "Secrétaire"; Secteur = "Administratif"; NomUtilisateur = "marc.beaulieu" },
23     @{ Nom = "Sophie Thibault"; Poste = "Secrétaire"; Secteur = "Administratif"; NomUtilisateur = "sophie.thibault" },
24     @{ Nom = "Camille Perrin"; Poste = "Secrétaire"; Secteur = "Administratif"; NomUtilisateur = "camille.perrin" },
25     @{ Nom = "Eric Roy"; Poste = "Secrétaire"; Secteur = "Administratif"; NomUtilisateur = "eric.roy" },
26     @{ Nom = "Luc Durand"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "luc.durand" },
27     @{ Nom = "Sarah Bernard"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "sarah.bernard" },
28     @{ Nom = "Kevin Fournier"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "kevin.fournier" },
29     @{ Nom = "Helene Petit"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "helene.petit" },
30     @{ Nom = "Jean Fabre"; Poste = "Technicien Support"; Secteur = "Support Technique"; NomUtilisateur = "jean.fabre" }
31 )
32
33 # Créer les utilisateurs
34 foreach ($user in $users) {
35     $souPath = "OU= $($user.Secteur),DC=notatech,DC=local"
36
37     # Vérifier si l'utilisateur existe déjà
38     if (-not (Get-ADUser -Filter "SamAccountName -eq '$($user.NomUtilisateur)'" -ErrorAction SilentlyContinue)) {
39         New-ADUser -Name $user.Nom -GivenName $user.Nom.Split(" ")[0] -Surname $user.Nom.Split(" ")[1] -
40             SamAccountName $user.NomUtilisateur -UserPrincipalName "$($user.NomUtilisateur)@$domain" -
41             Path $souPath -AccountPassword (ConvertTo-SecureString "Root123" -AsPlainText -Force) -
42             Enabled $true -
43             ChangePasswordAtLogon $true -
44             PasswordNeverExpires $false
45     } else {
46         Write-Host "L'utilisateur $($user.Nom) existe déjà."
47     }
48 }
49

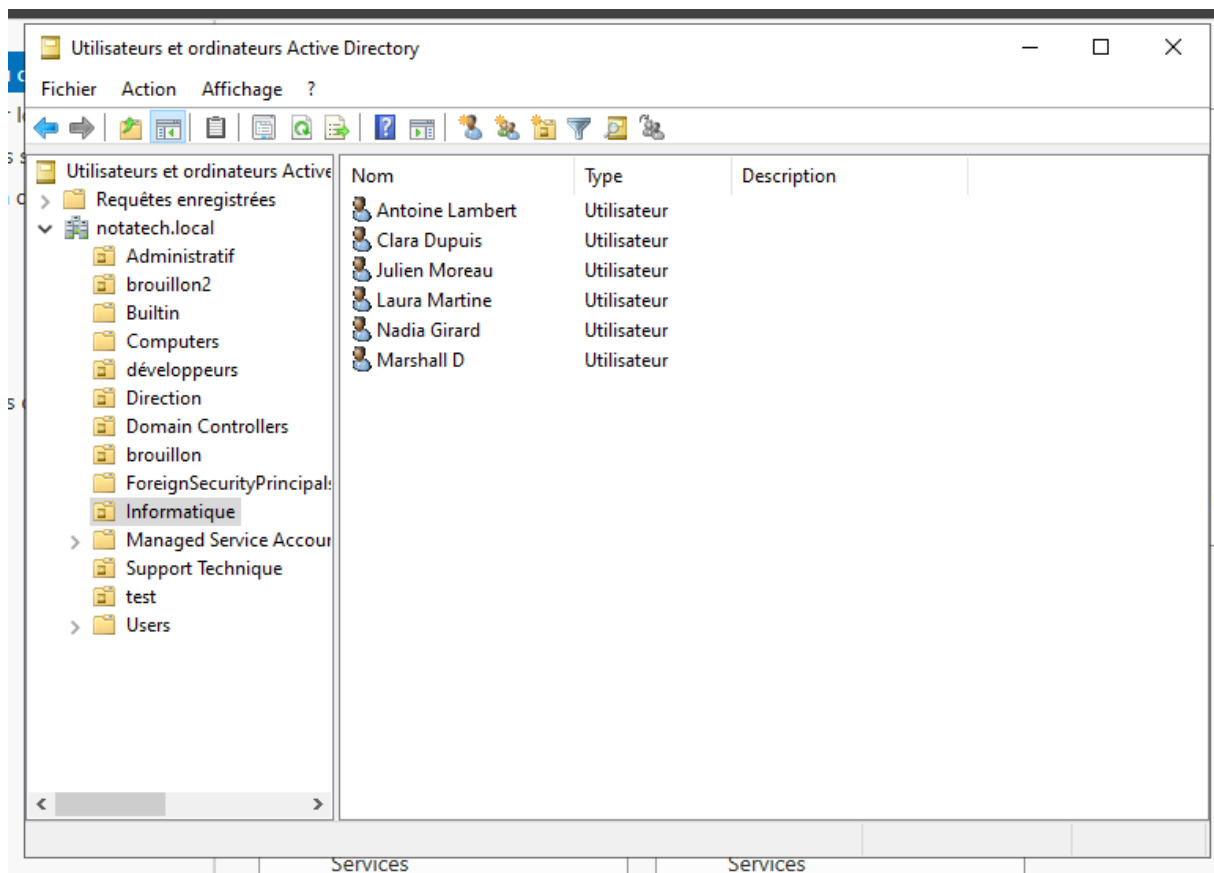
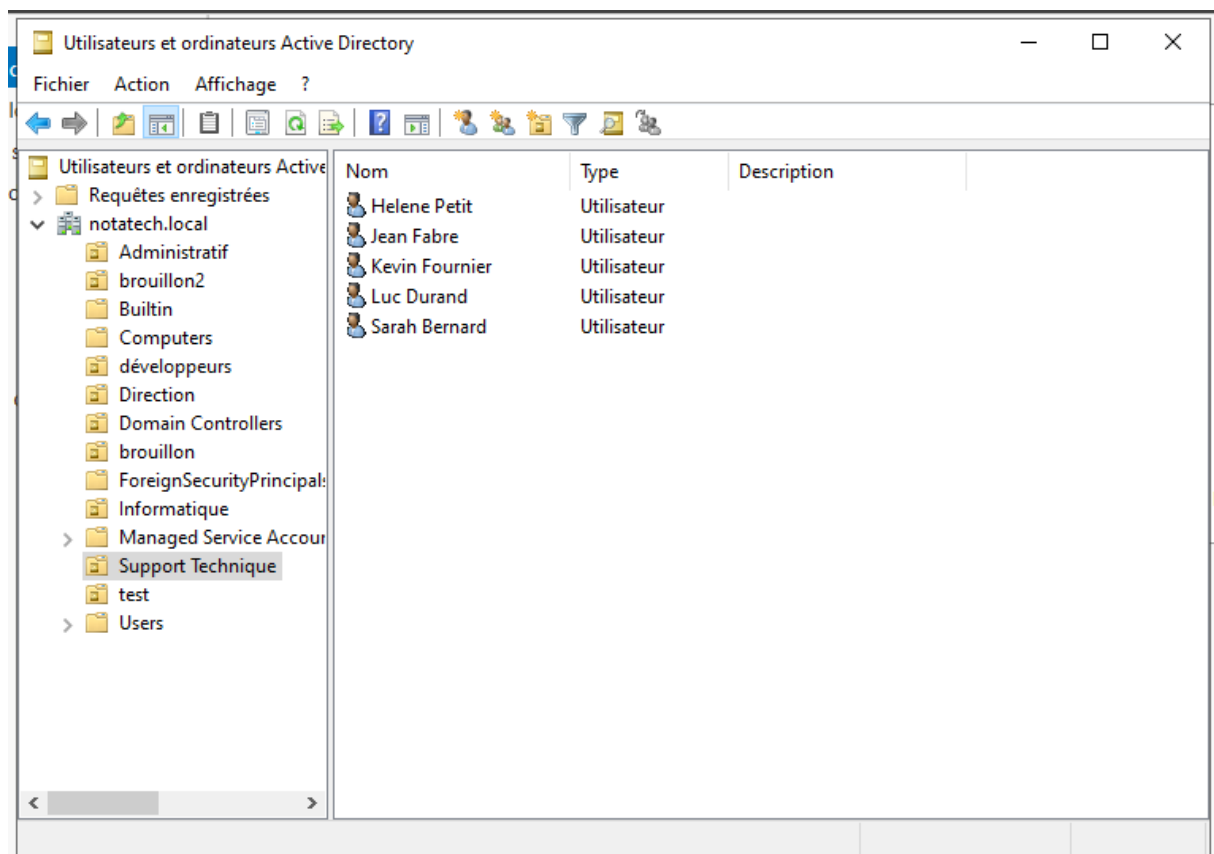
```

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



Et les utilisateurs correspondant aussi

Utilisateurs et ordinateurs Active	Nom	Type
> Requêtes enregistrées		
▼ notatech.local		
Administratif	Camille Perrin	Utilisateur
brouillon2	Eric Roy	Utilisateur
> Builtin	Isabelle Lemoine	Utilisateur
Computers	Marc Beaulieu	Utilisateur
	Sophie Thibault	Utilisateur



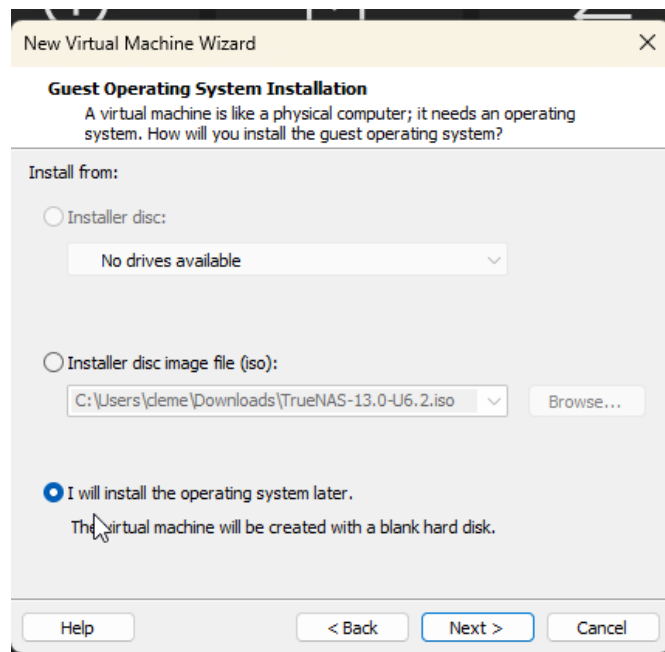
Serveur AD en redondance :

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

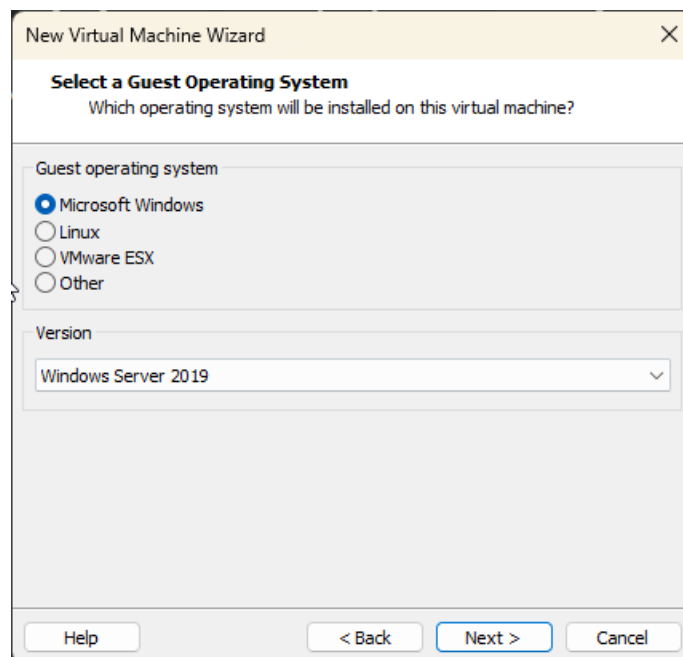
Tout d'abord je commence par créer une nouvelle machine virtuelle Windows server pour la redondance. Ici je sélectionne **custom**



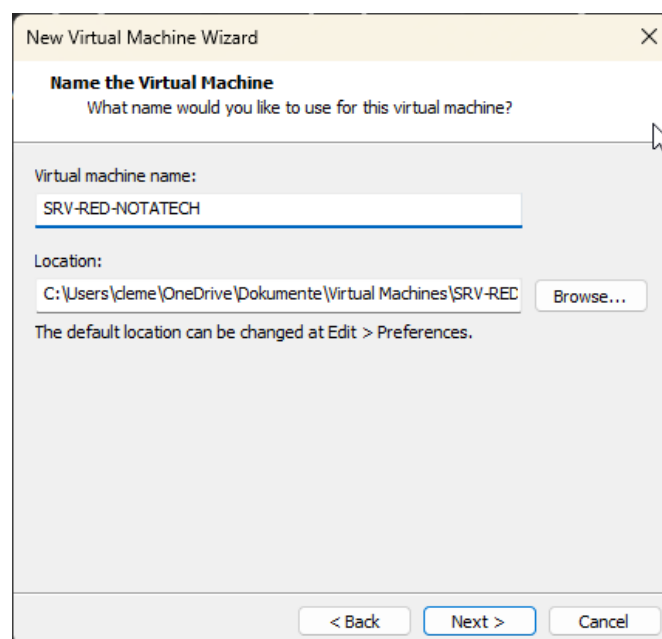
Ensuite comme mon premier serveur j'installerai l'iso plus tard



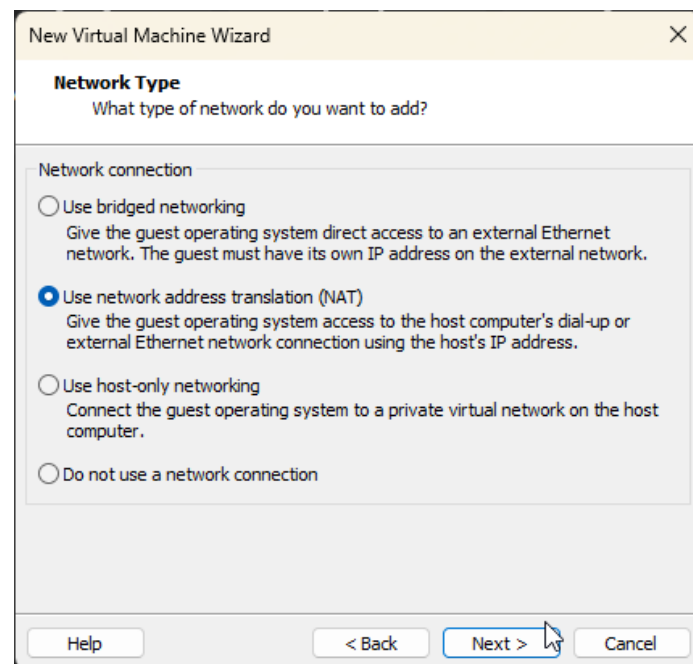
Ici je sélectionne **Windows Server 2019**



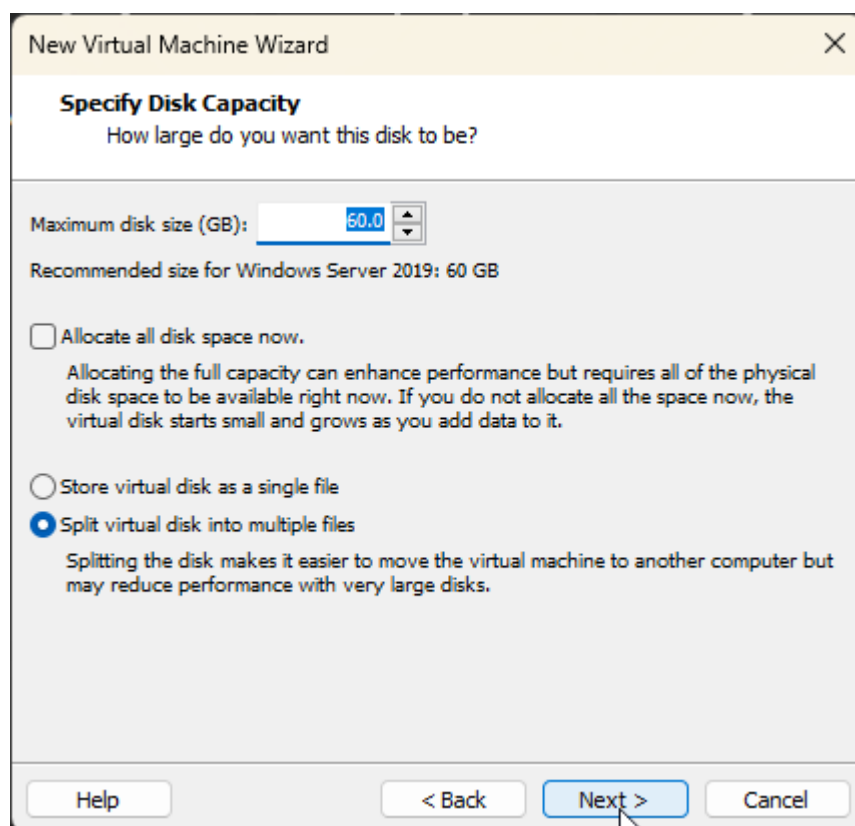
Ensuite ici je nomme mon serveur **SRV-RED-NOTATECH** pour spécifier que c'est mon serveur de redondance



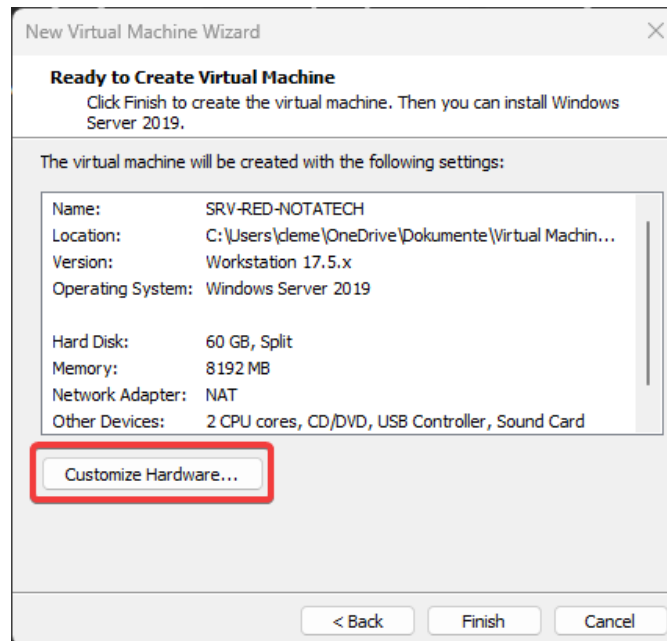
Pour le reste je laisse les options par défaut et ici je sélectionne **NAT**, on en configurera une deuxième plus tard en **LAN segment**



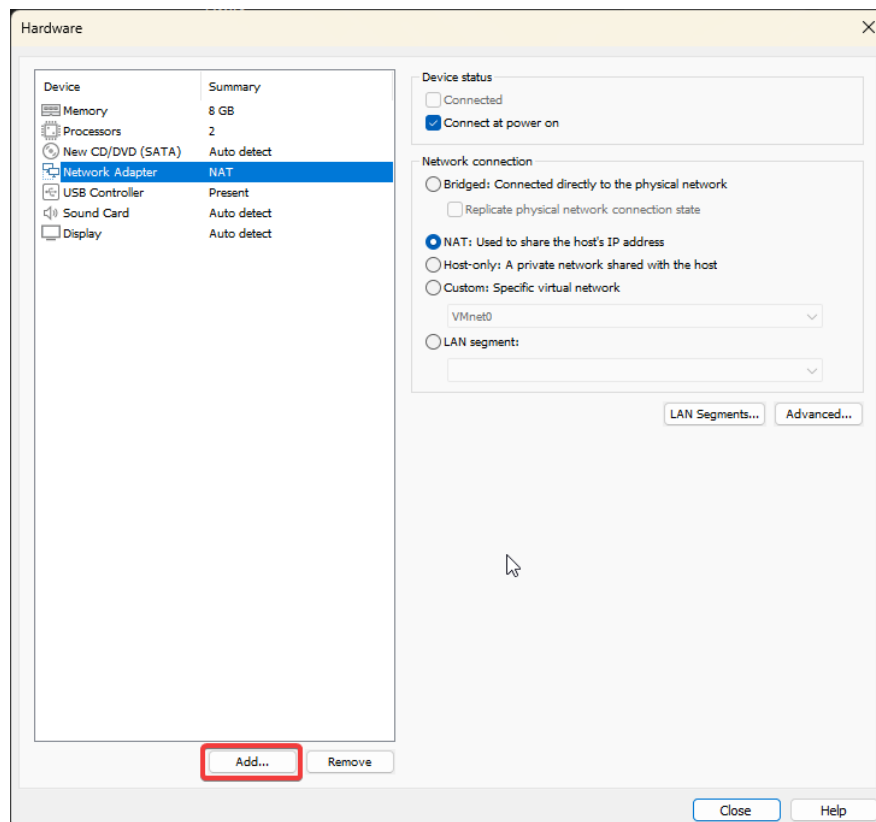
Ici je sélectionne **60GB** pour l'espace disque, ce qui suffira amplement



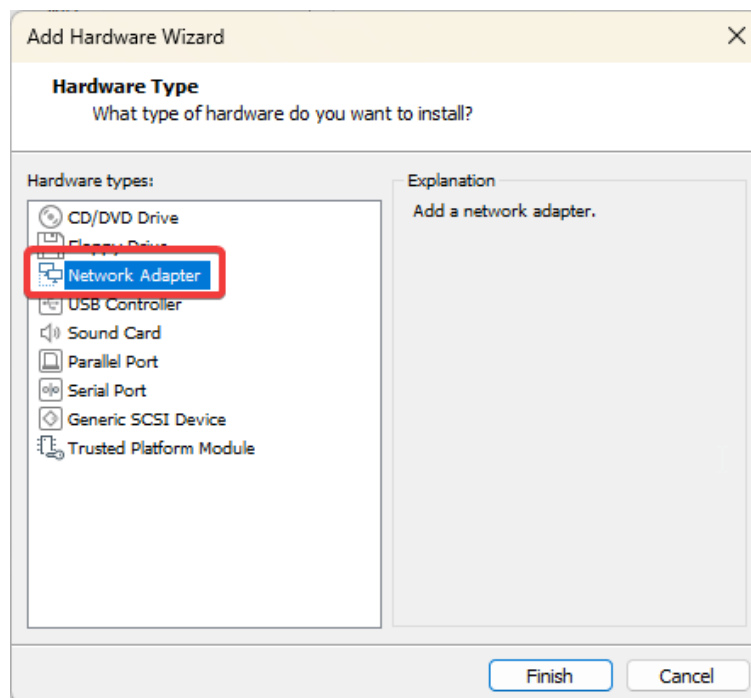
Ensuite étape très importante, ici je sélectionne **Customize Hardware** pour ajouter une autre carte réseau



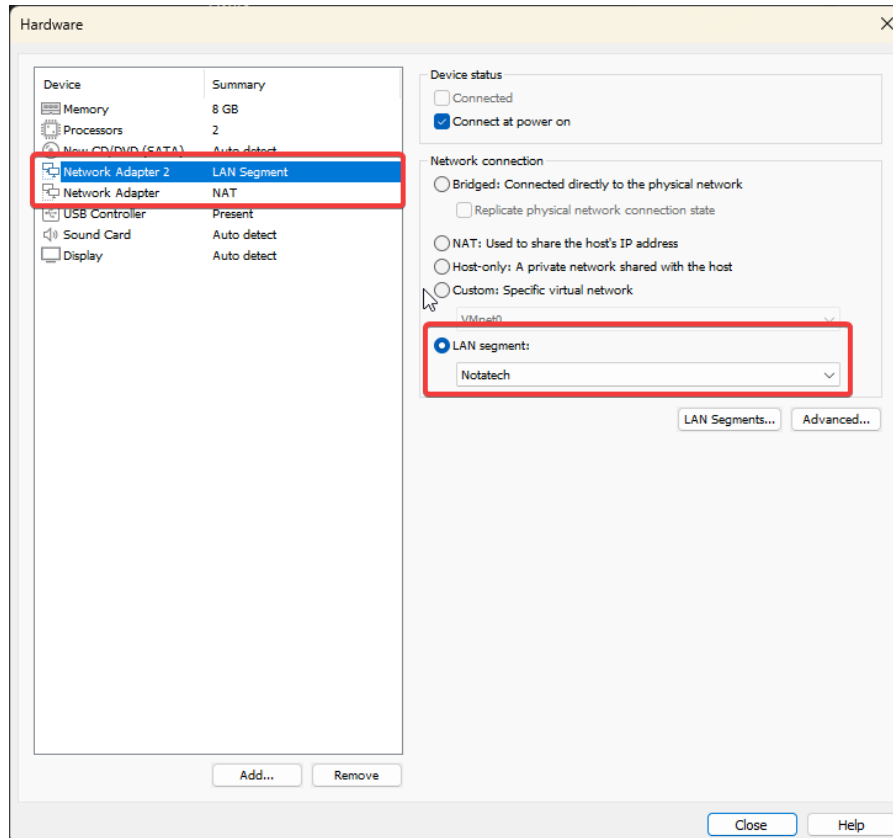
Ensuite ici je clique sur **Add**



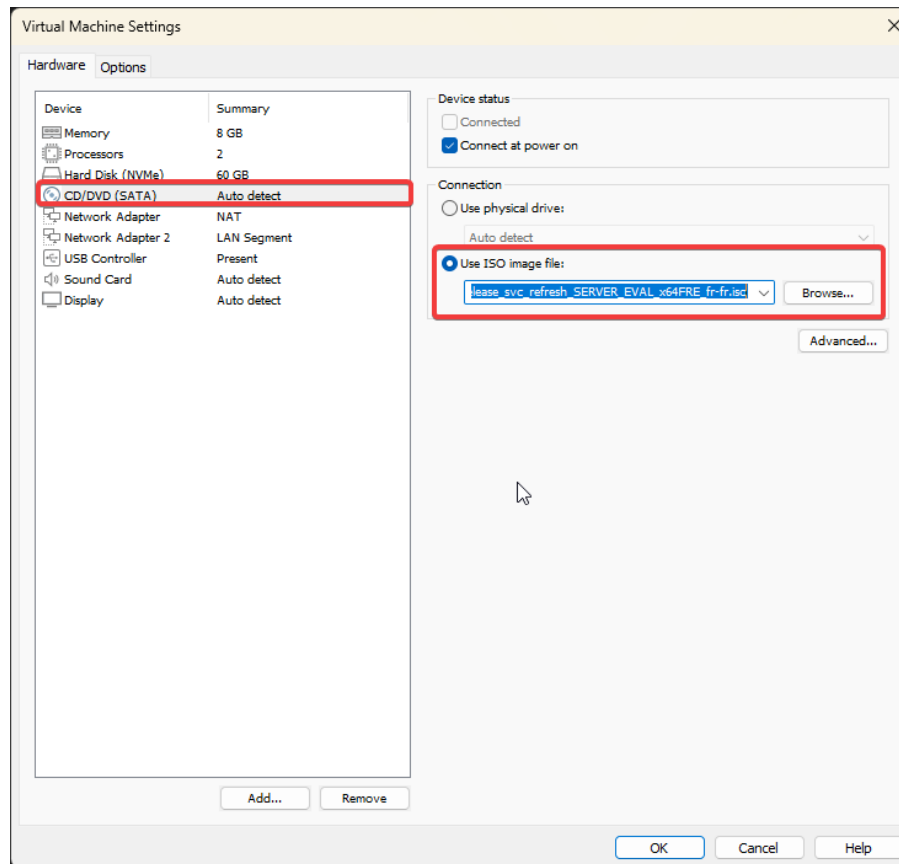
Je sélectionne **Network Adapter** pour ajouter une autre carte réseau a mon serveur



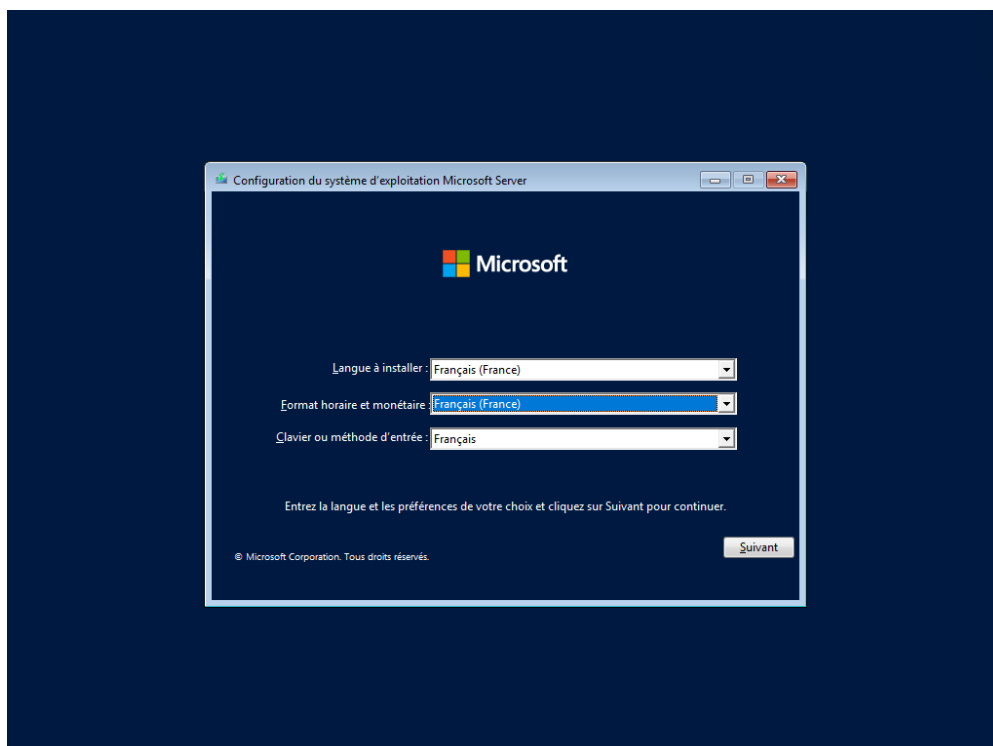
Et je met cette carte en **LAN Segment** et je la met sur le segment **Notatech**, pour que la machine soit directement liée a mon réseau



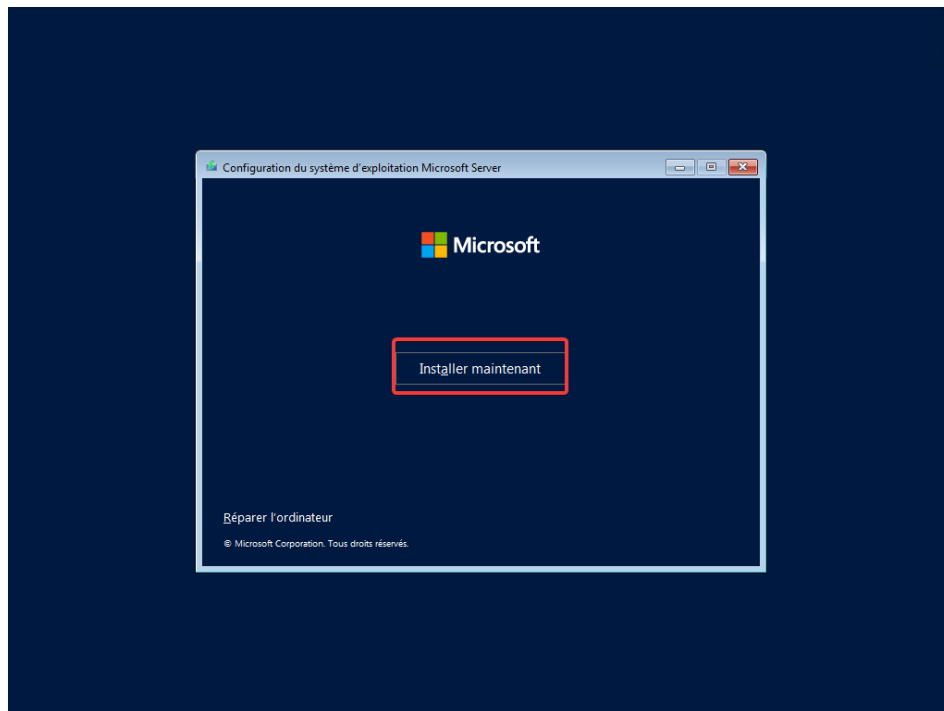
Et finalement je sélectionne l'Iso de mon **Windows server** et démarre ma machine pour débiter l'installation.



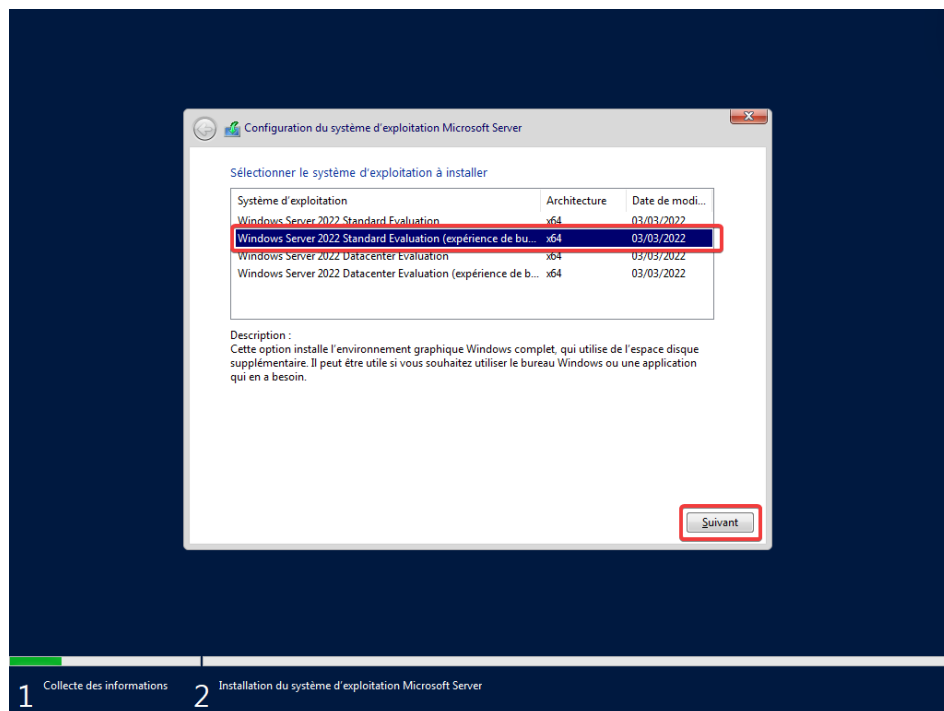
Je démarre donc mon 2^{ème} serveur et suis ces étapes comme nous l'avons fait toute à l'heure



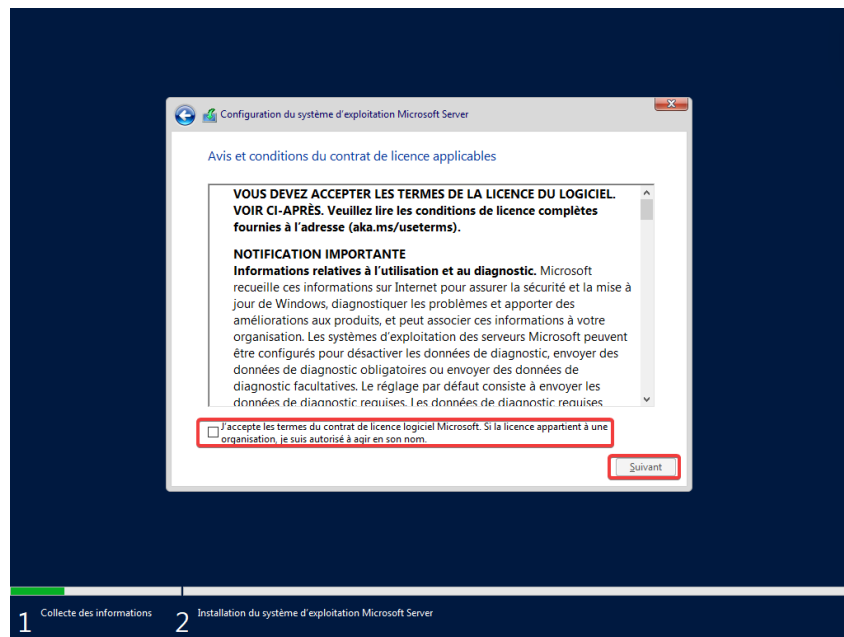
Je clique ici sur « installer maintenant »



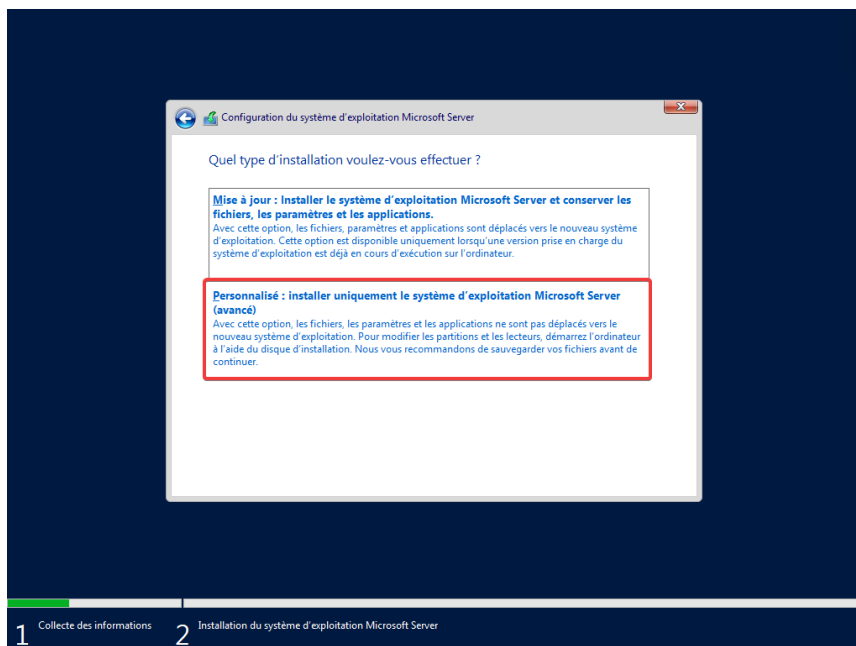
Pour ce qui est du système d'exploitation je sélectionne la 2^{ème} option comme mon premier serveur, Windows server 2022 standard (expérience de bureau)



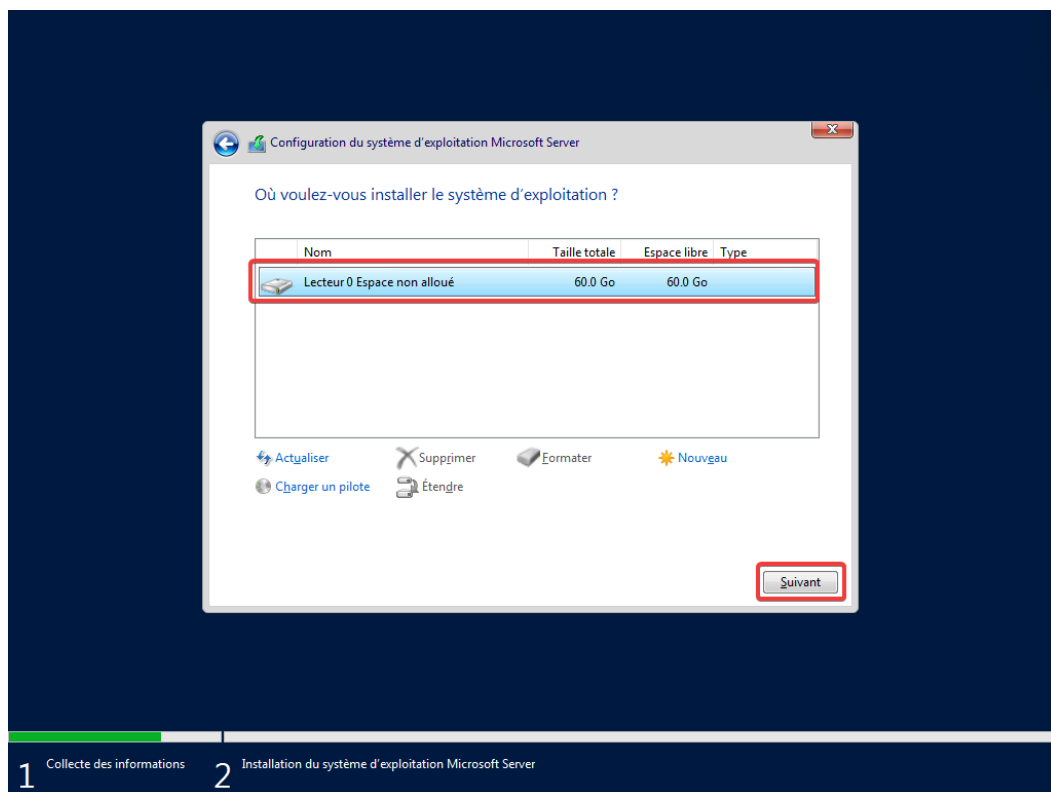
Ensuite j'accepte les conditions d'utilisation de l'appllicable



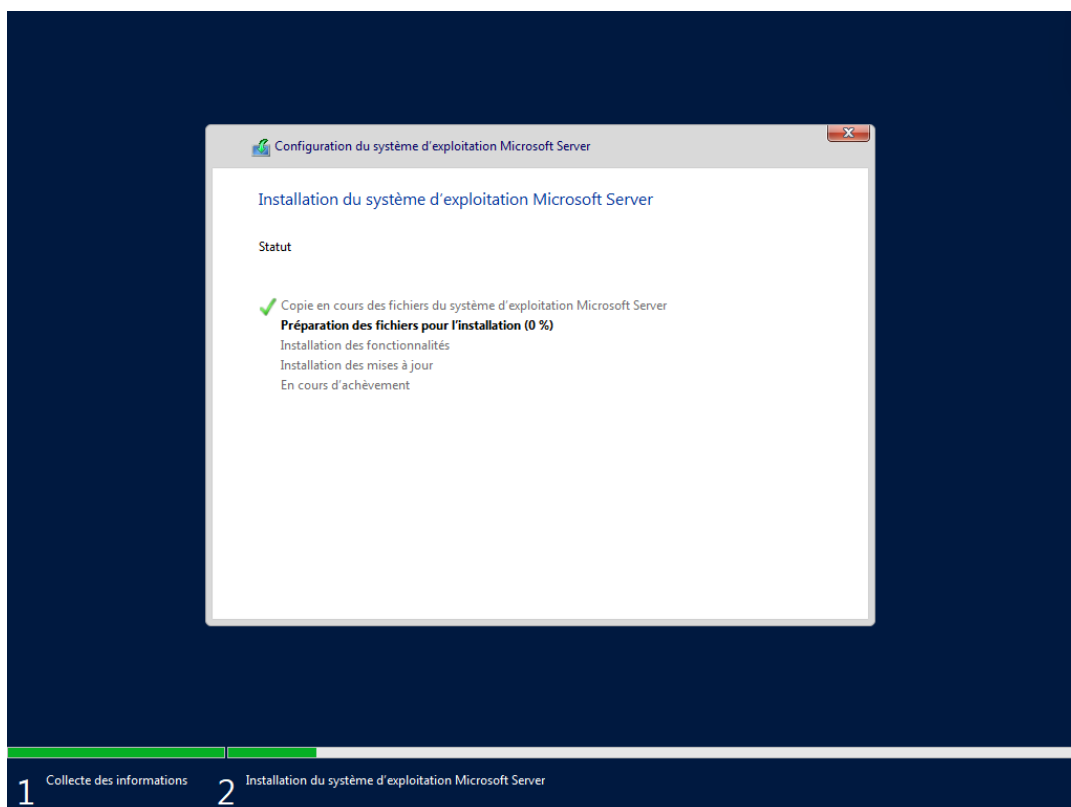
Pour le type d'installation je sélectionne « personnalisé »



Je sélectionne mon disque et clique sur suivant

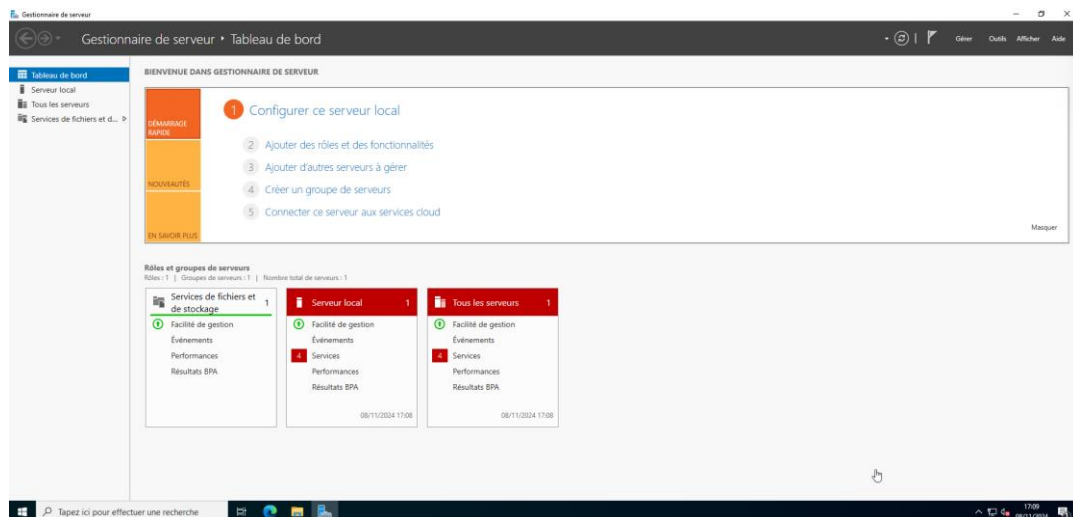


Et l'installation de notre système va finalement se lancer



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

The screenshot shows the 'Paramètres de personnalisation' (Personalization Parameters) window in Windows Server. It has a blue background. At the top, it says 'Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.' (Type a password for the built-in Administrator account that you can use to automatically connect to this computer). Below this are three input fields: 'Nom d'utilisateur' (Username) with 'Administrateur' entered, 'Mot de passe' (Password) with masked characters, and 'Entrez de nouveau le mot de passe' (Re-enter the password) with masked characters. A 'Terminer' (Finish) button is at the bottom right. A circular arrow icon is at the bottom left.

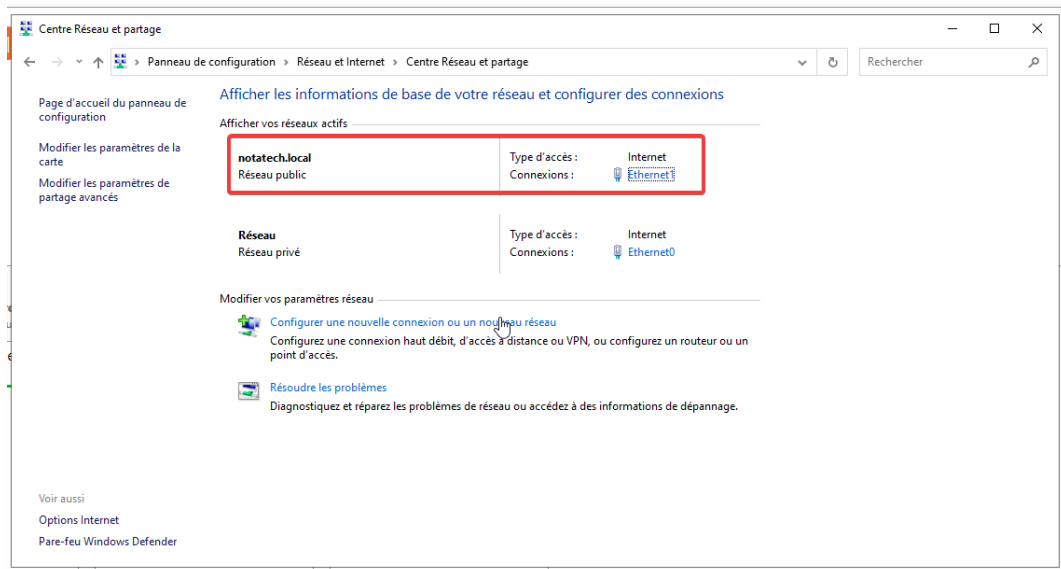


Et voilà nous avons finalement notre 2^{ème} machine de créé et prête à être configurée

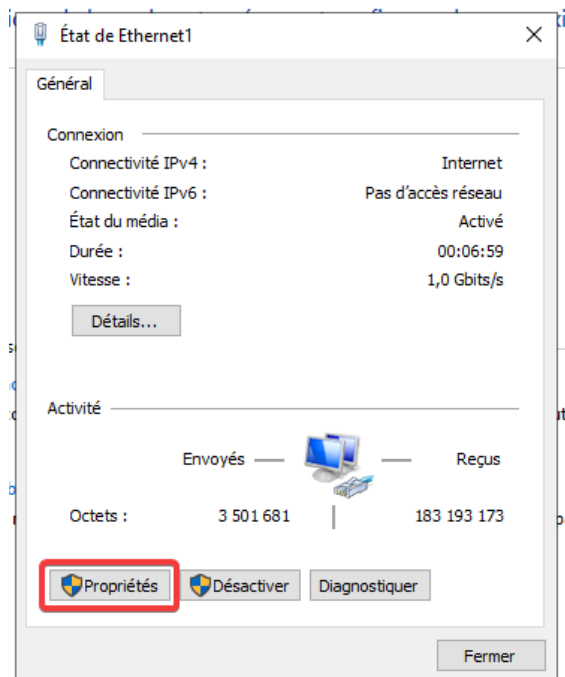
Configuration du 2^{ème} Windows server :

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

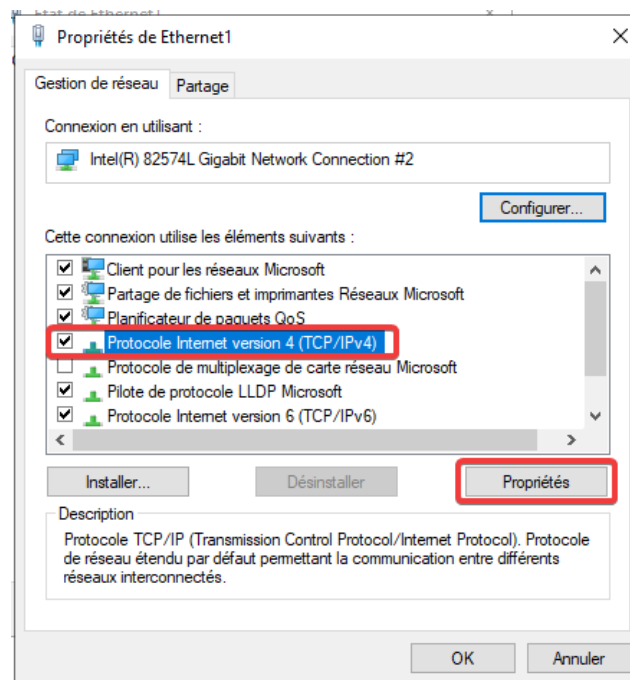
Je commence tout d'abord par configurer mon Windows server en IP fixe, pour cela je me rend dans le panneau de configuration, centre réseau et partage et je clique ici sur ma carte en LAN sur « Ethernet 1 »



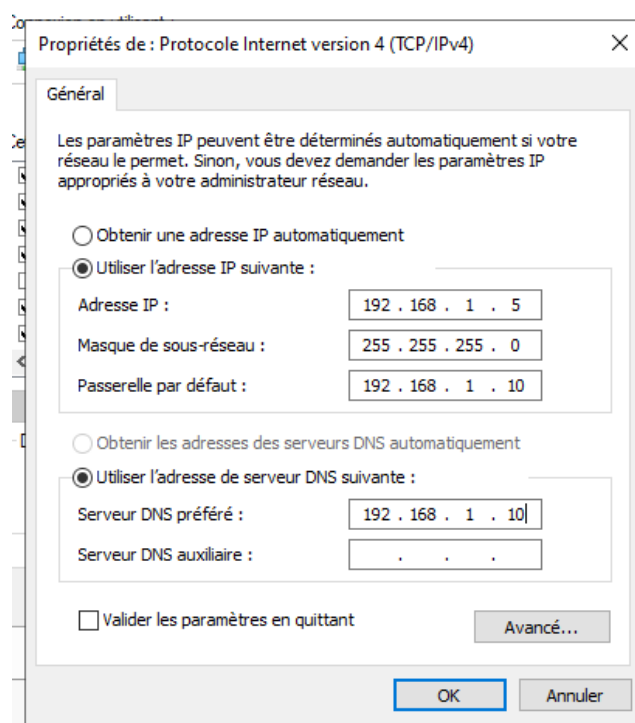
Ensuite je clique sur propriétés pour configurer mon IP fixe



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



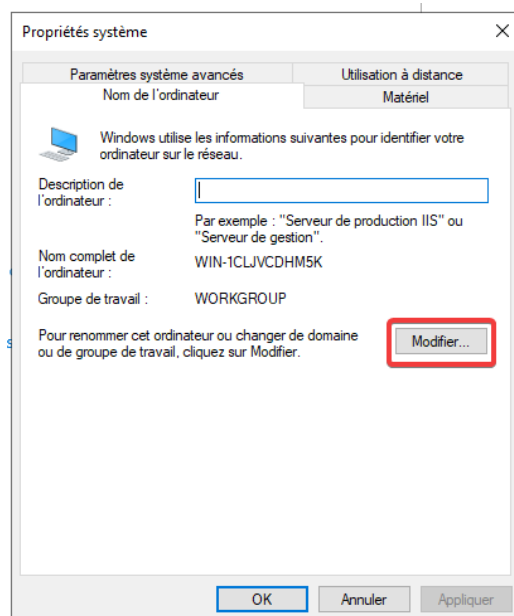
J'arrive finalement sur cette page où je sélectionne « utiliser l'adresse IP suivante » et je configure mon serveur en 192.168.1.5/24 avec la passerelle 192.168.1.10 qui correspond à l'adresse de mon premier serveur



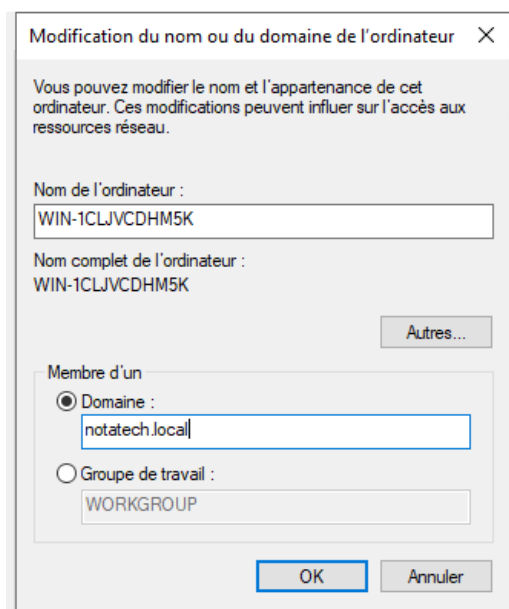
Changement du nom et intégration dans le domaine :

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

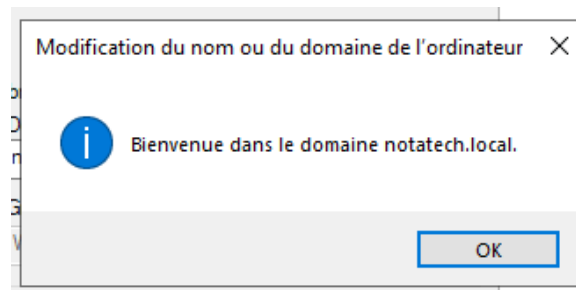
Pour ce faire je me rends dans les propriétés système je clique ici sur « modifier »



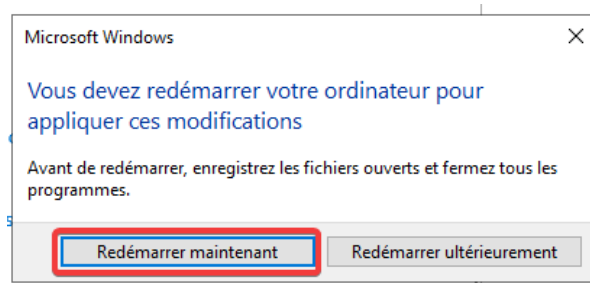
Ici dans domaine je rentre « notatech.local » et je clique ensuite sur OK



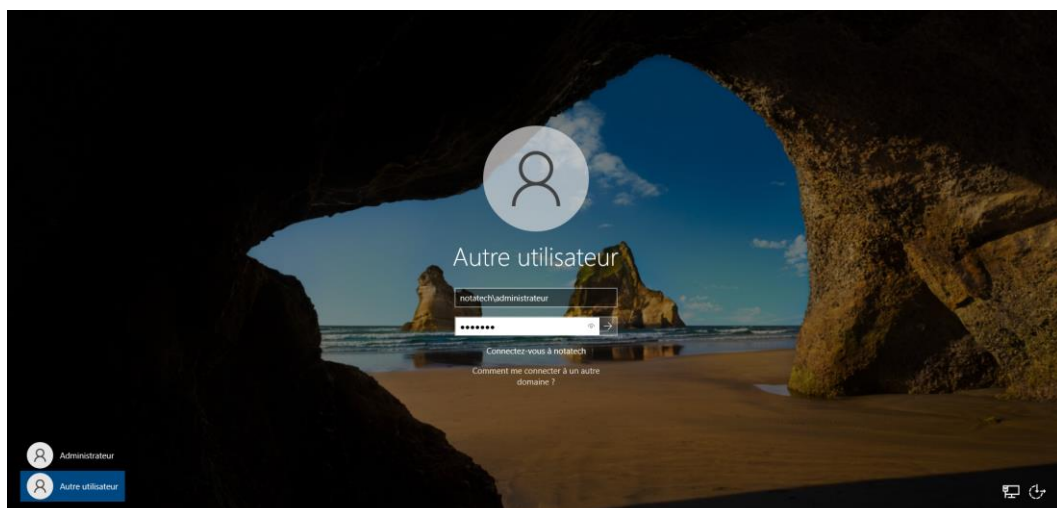
Ce message apparait m'indiquant que ma machine est bien intégrée au domaine donc tout est bon



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

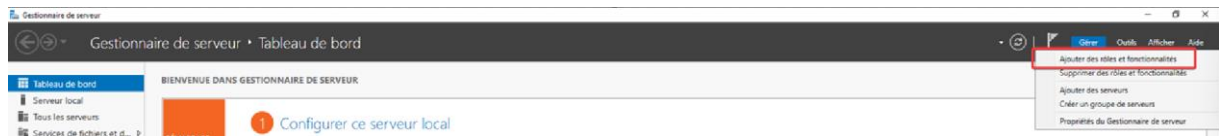


Je peux bien me connecter avec mon domaine, donc tout est bon au niveau de la liaison avec le domaines

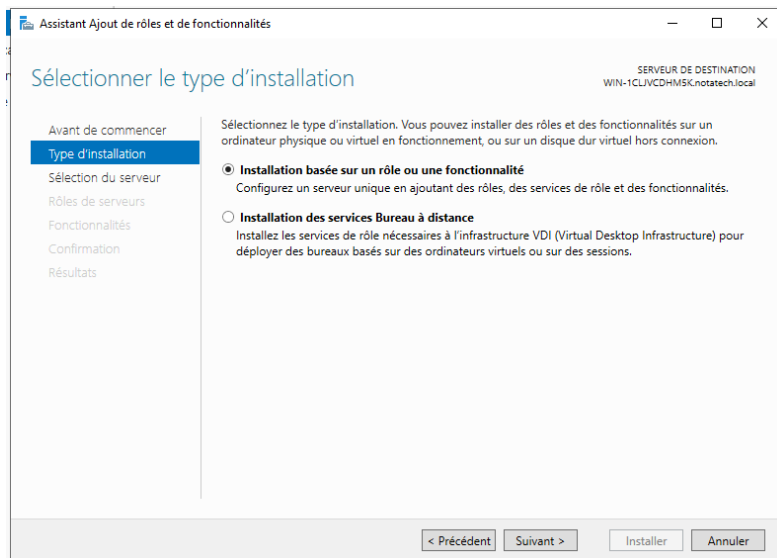


Installation des rôles AD DS sur le 2^{ème} serveur :

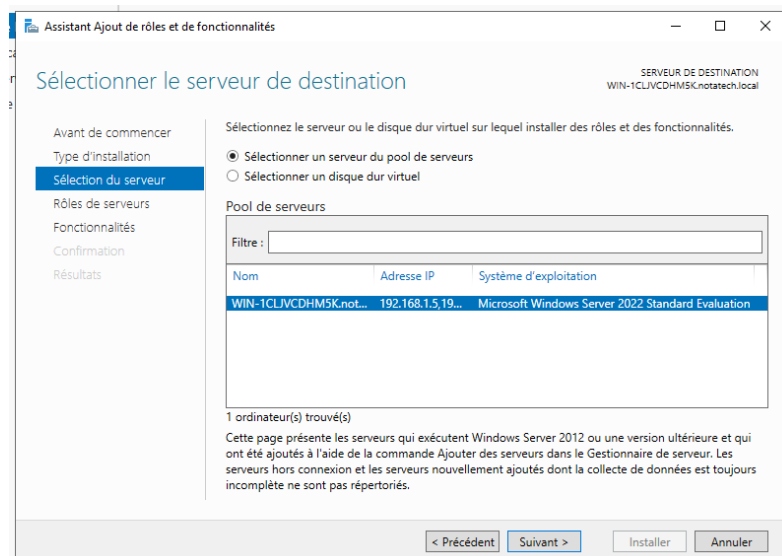
Pour commencer cette installation je me rend d'abord sur le gestionnaire de serveur et vais dans « gérer » et clique sur « ajouter des rôles et fonctionnalités »



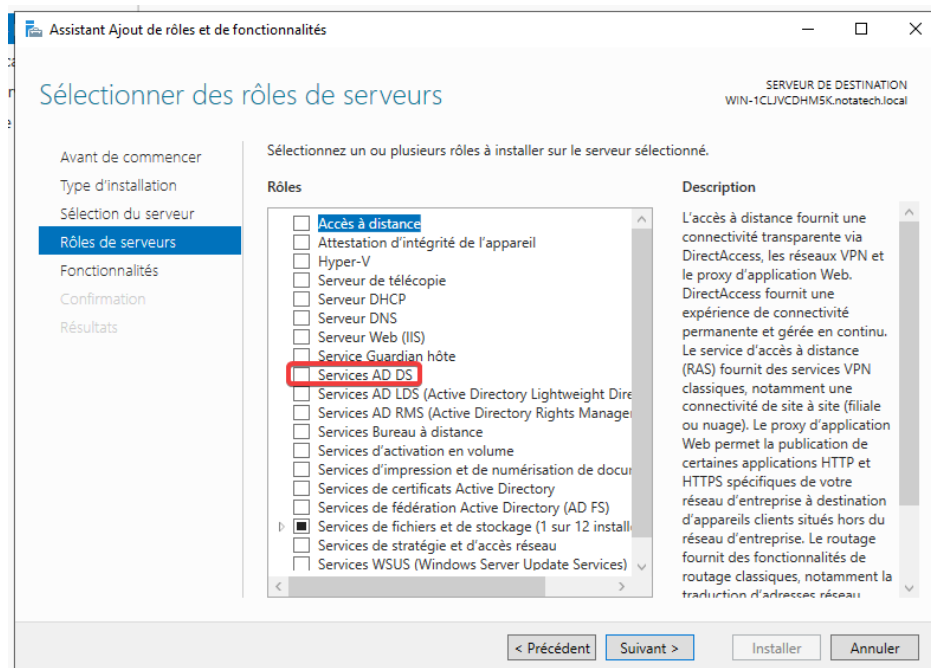
Ici je sélectionne « installation basée sur un rôle ou une fonctionnalité », suivant



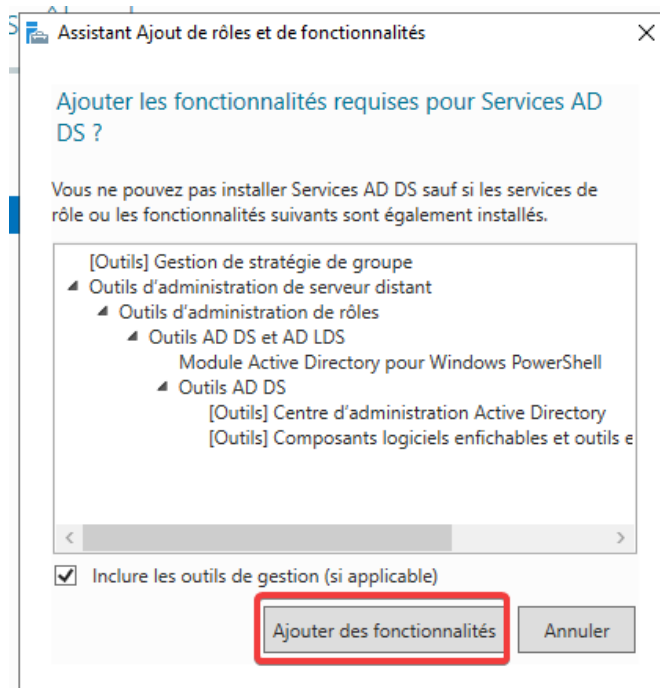
Ici je sélectionne donc mon serveur et fait suivant



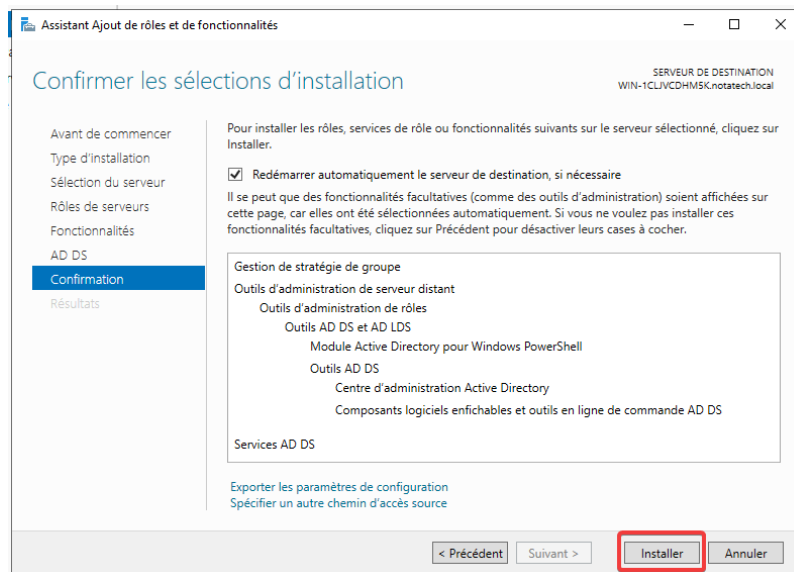
Pour les rôles de serveurs je sélectionne « Services AD DS »



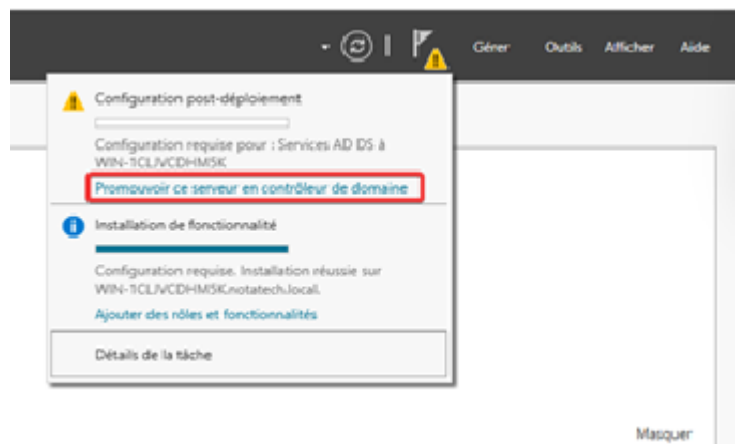
Je clique ici sur « Ajouter des fonctionnalités » et passe a la suite



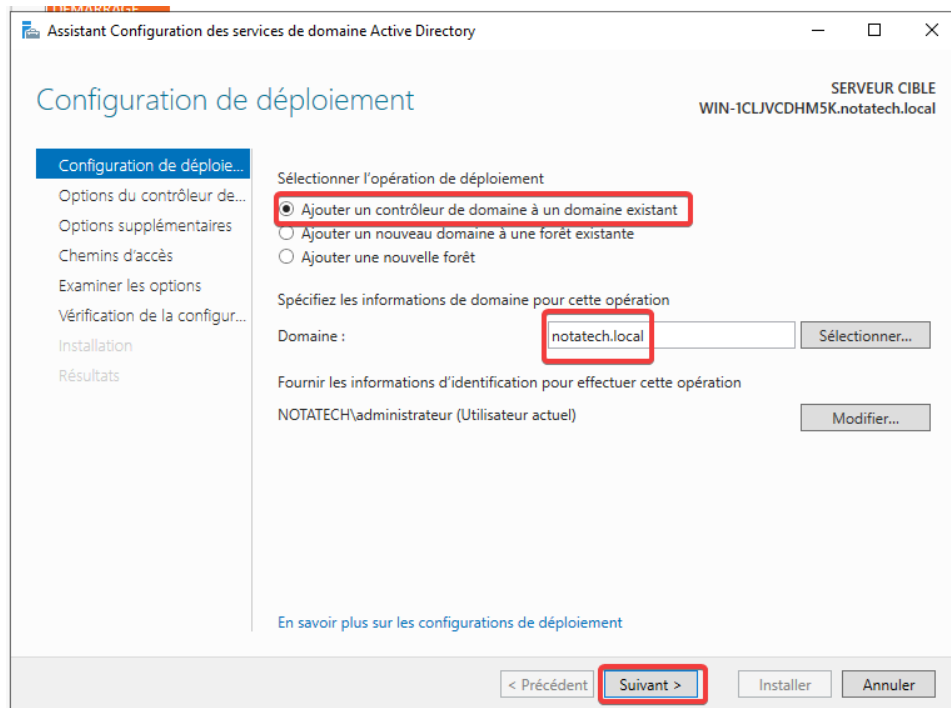
Ensuite je laisse les paramètres par défaut pour la suite et démarre l'installation



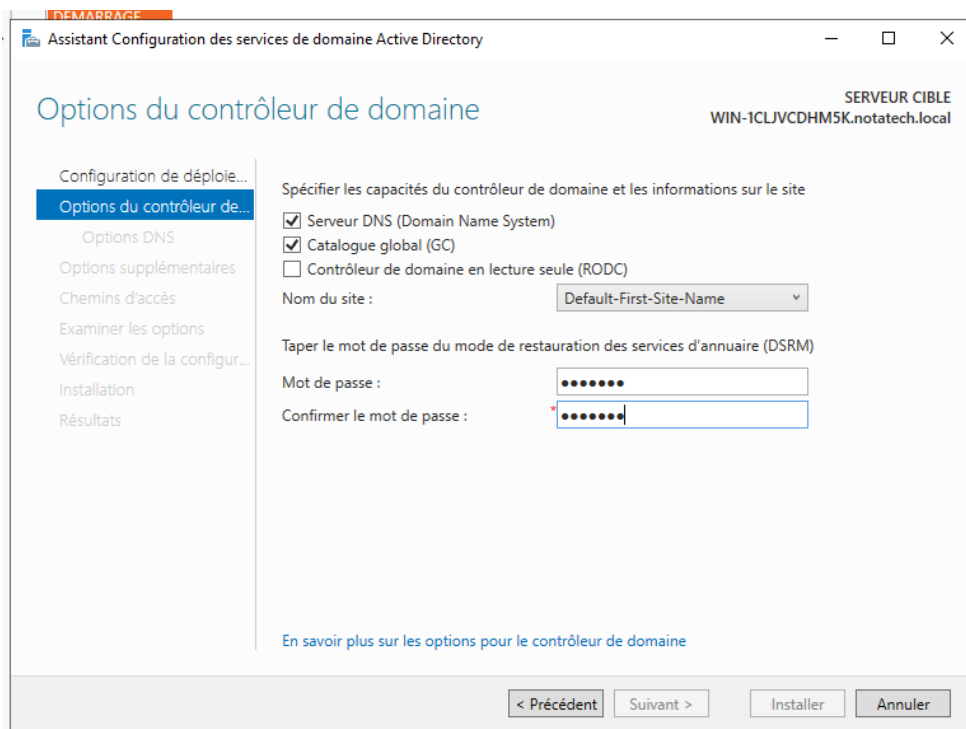
Ensuite une fois ceci installé, je vais **promouvoir ce serveur en contrôleur de domaine**, pour ce faire sur le tableau de bord je clique sur le drapeau, on voit cette notification qui nous propose de promouvoir ce serveur en contrôleur de domaine, je clique donc sur « promouvoir ce serveur en contrôleur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



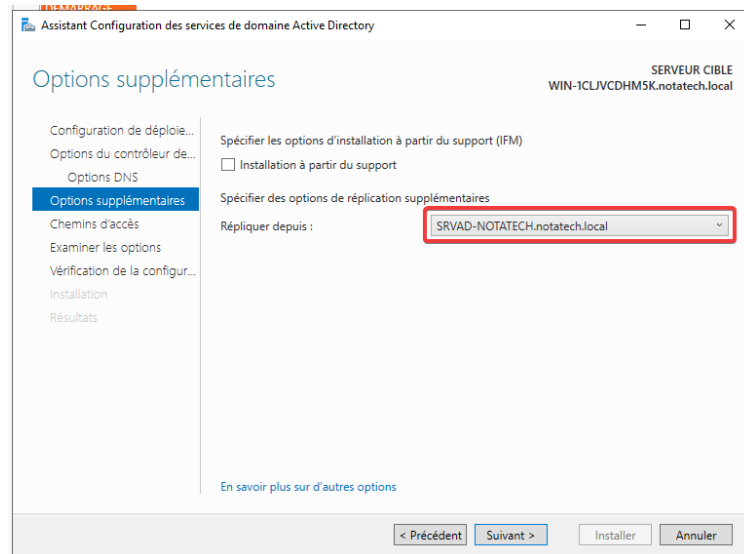
Ensuite ici vu qu'on configure notre 2^{ème} serveur notre forêt est déjà créée, donc nous allons tout simplement ajouter notre contrôleur de domaine au domaine **notatech.local**, je sélectionne donc « ajouter un contrôleur de domaine à un domaine existant et j'écris **notatech.local**.



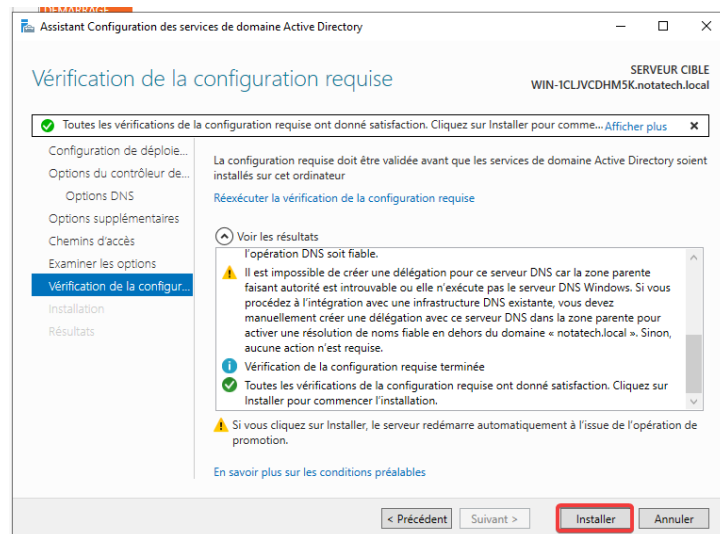
Ici je sélectionne un mot de passe pour le **mode de restauration des services d'annuaire**.



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 réplcation va se faire.



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



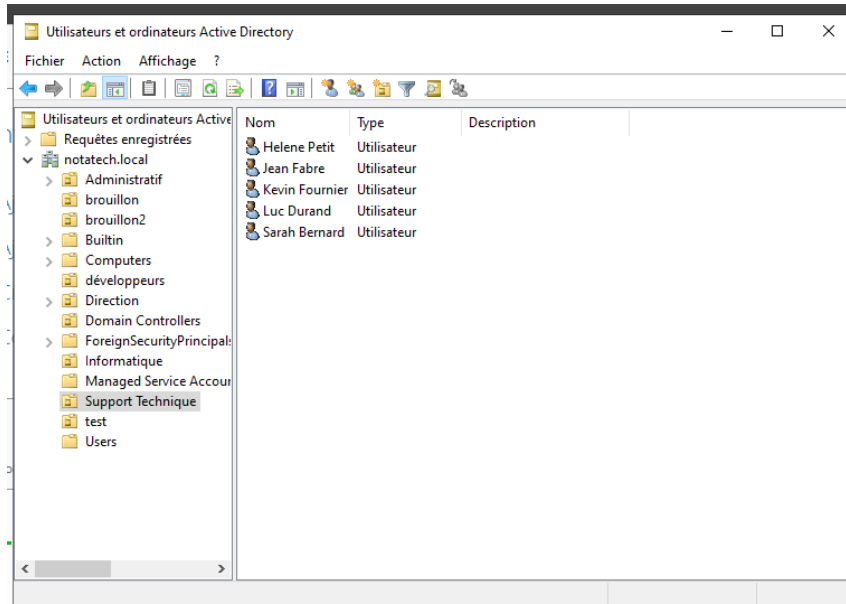
Cette petite banderole va finalement apparaitre et nous confirme que le serveur a été **correctement configuré en tant que contrôleur de domaine**.



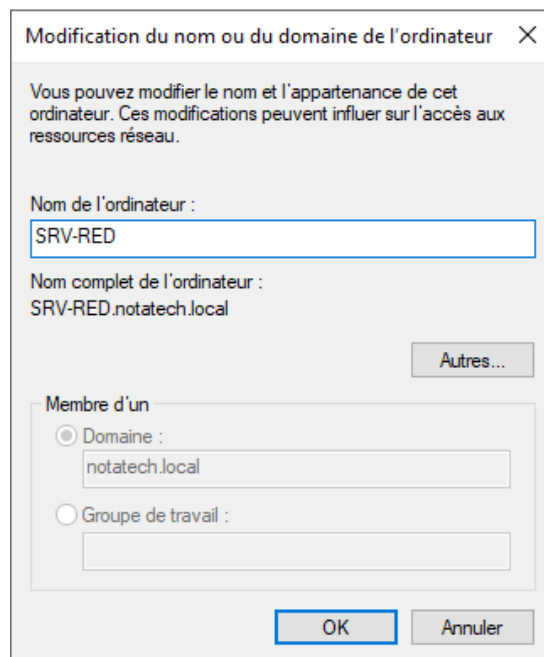
Activation et vérification de la redondance :

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

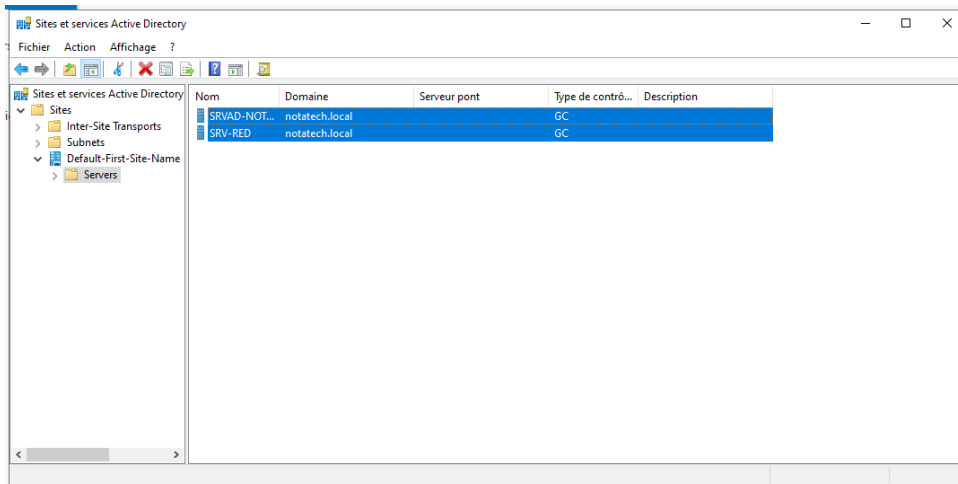
Je commence d'abord par vérifier dans ma console d'utilisateurs et ordinateurs Active Directory que mes utilisateurs et unité d'organisation ont bien été répliqués, c'est bien le cas comme nous pouvons le voir.



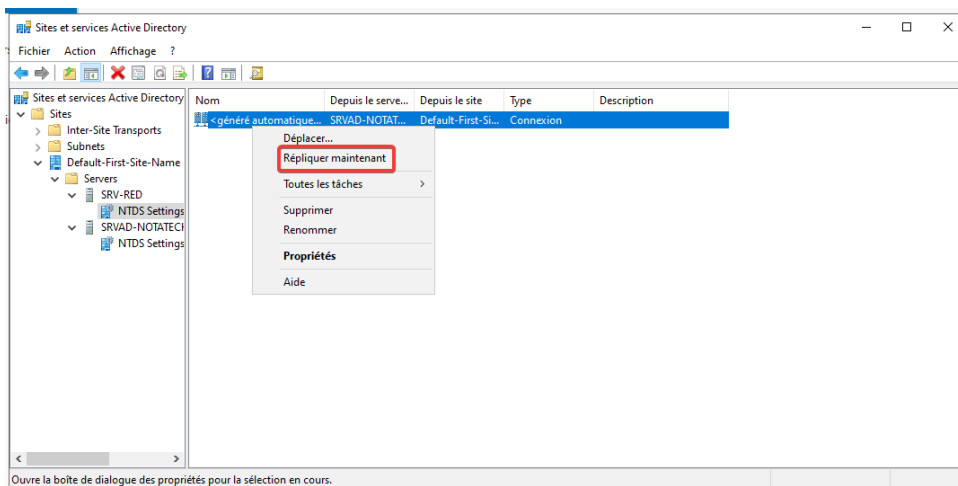
Je commence d'abord par **renommer mon serveur**, je le renomme ici en « **SRV-RED** » pour l'identifier facilement lors de la réplication.



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 clic 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.

```
Administrateur : Invite de commandes

=== INSTANCES VOISINES ENTRANTES ===

DC=notatech,DC=local
  Default-First-Site-Name\SRVAD-NOTATECH via RPC
  GUID de l'objet DSA : 6d6cca80-7b20-4f2b-bb6e-acb962fa982e
  La dernière tentative, le 2024-11-08 18:25:50, a réussi.

CN=Configuration,DC=notatech,DC=local
  Default-First-Site-Name\SRVAD-NOTATECH via RPC
  GUID de l'objet DSA : 6d6cca80-7b20-4f2b-bb6e-acb962fa982e
  La dernière tentative, le 2024-11-08 18:21:34, a réussi.

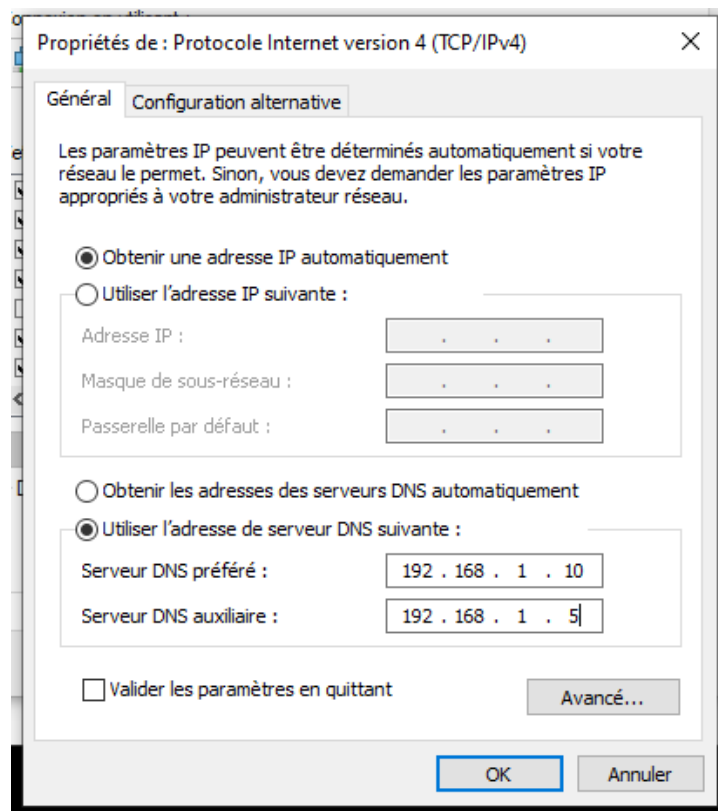
CN=Schema,CN=Configuration,DC=notatech,DC=local
  Default-First-Site-Name\SRVAD-NOTATECH via RPC
  GUID de l'objet DSA : 6d6cca80-7b20-4f2b-bb6e-acb962fa982e
  La dernière tentative, le 2024-11-08 18:21:34, a réussi.

DC=DomainDnsZones,DC=notatech,DC=local
  Default-First-Site-Name\SRVAD-NOTATECH via RPC
  GUID de l'objet DSA : 6d6cca80-7b20-4f2b-bb6e-acb962fa982e
  La dernière tentative, le 2024-11-08 18:24:01, a réussi.

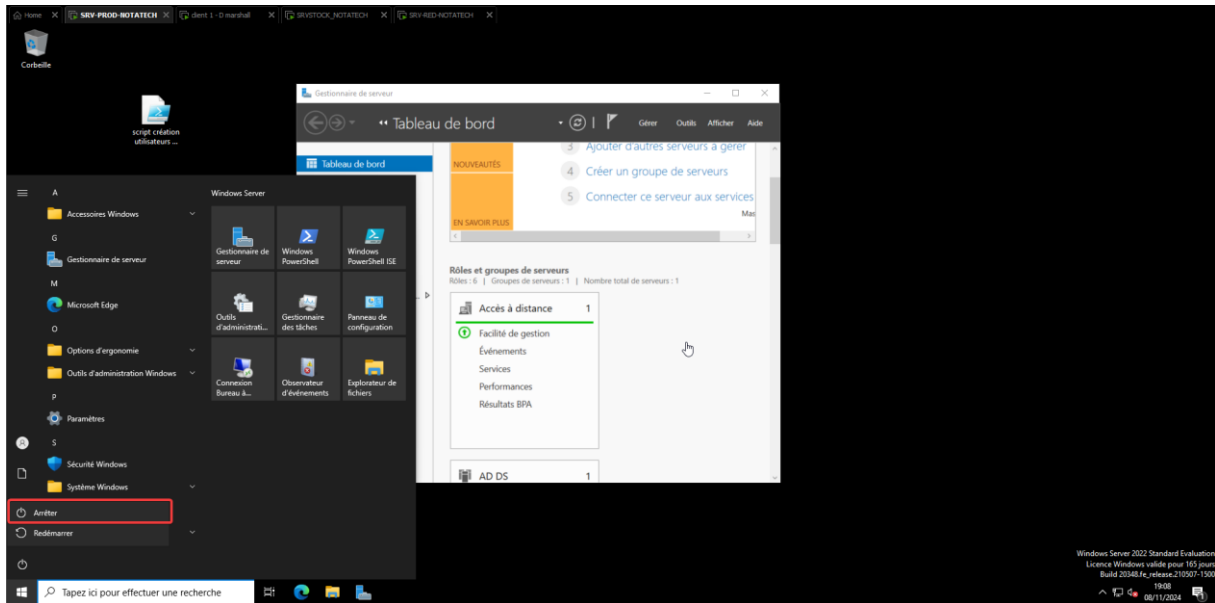
DC=ForestDnsZones,DC=notatech,DC=local
  Default-First-Site-Name\SRVAD-NOTATECH via RPC
  GUID de l'objet DSA : 6d6cca80-7b20-4f2b-bb6e-acb962fa982e
  La dernière tentative, le 2024-11-08 18:21:34, a réussi.

C:\Users\administrateur.NOTATECH>
```

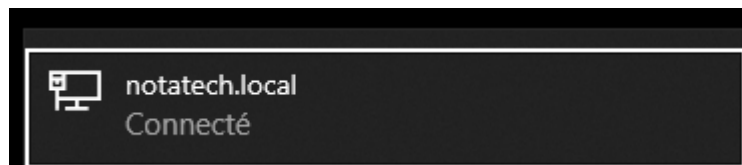
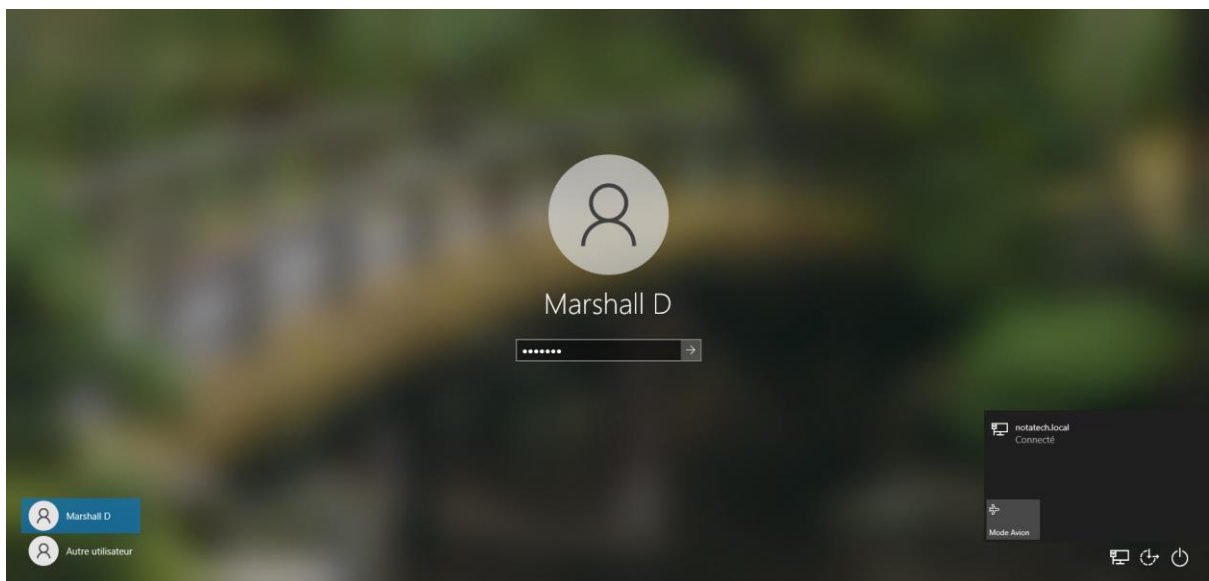
Et finalement nous allons faire le test final pour voir si la réplication fonctionne bien, nous allons éteindre le serveur AD principal **SRV-PROD-NOTATECH** et ensuite je vais essayer de me connecter avec mon ordinateur client à l'utilisateur **D Marshall**, avant ça il faut que je rajoute l'adresse 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 :

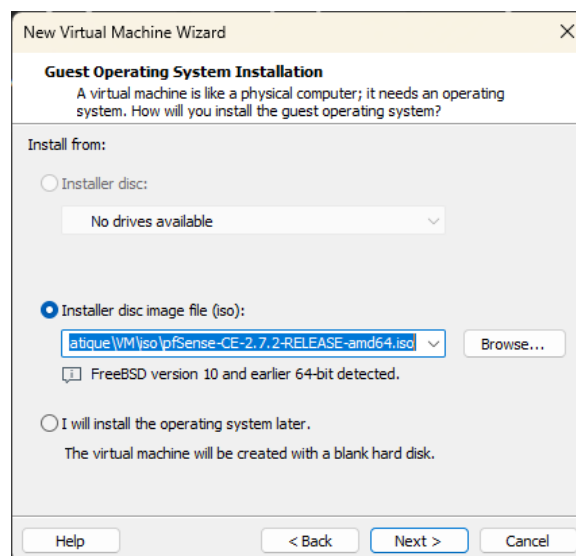
Dans cette partie nous allons voir la création du pare feu PfSense, qui nous permettra de sécuriser notre réseau en mettant en place un IDS et des ACL

1^{ère} étape : création du pfsense :

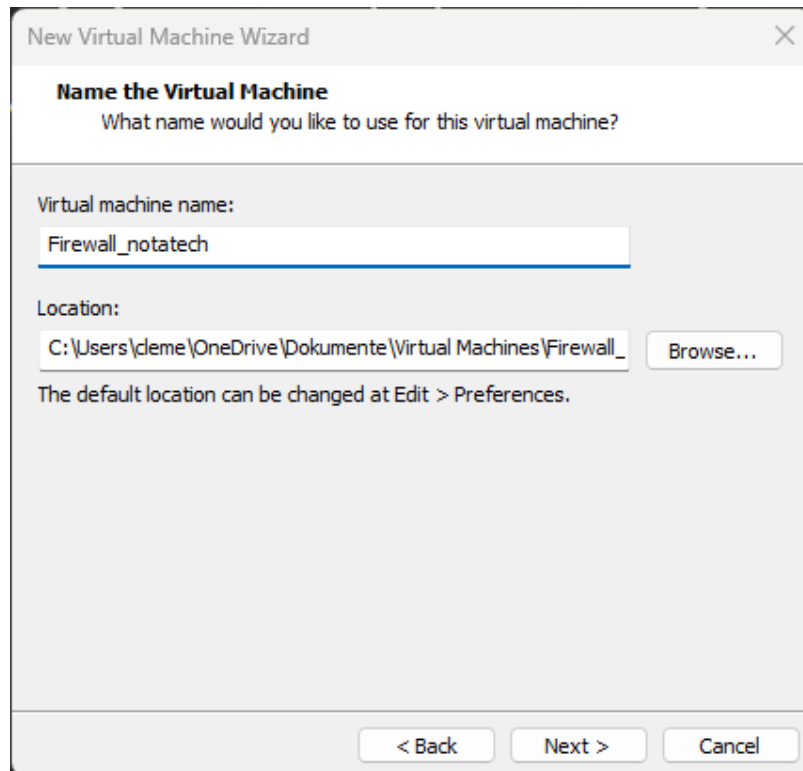
Tout d'abord il va falloir créer la VM Pfsense, comme pour les autres machines je me rend sur vmWare et clique sur créer une nouvelle machine et sélectionne « custom »



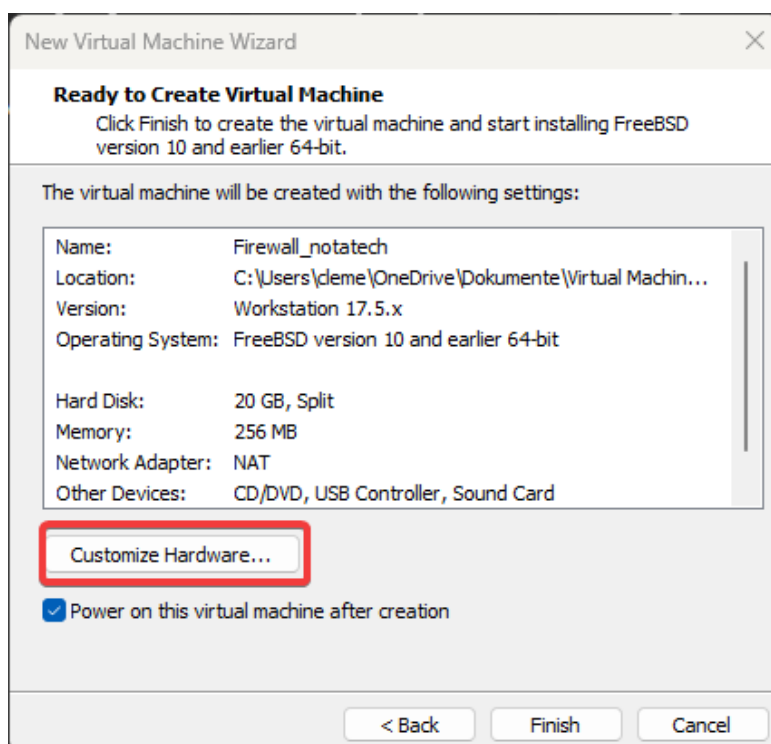
Ensuite ici je sélectionne mon ISO de pfsense et clique sur **suivant**



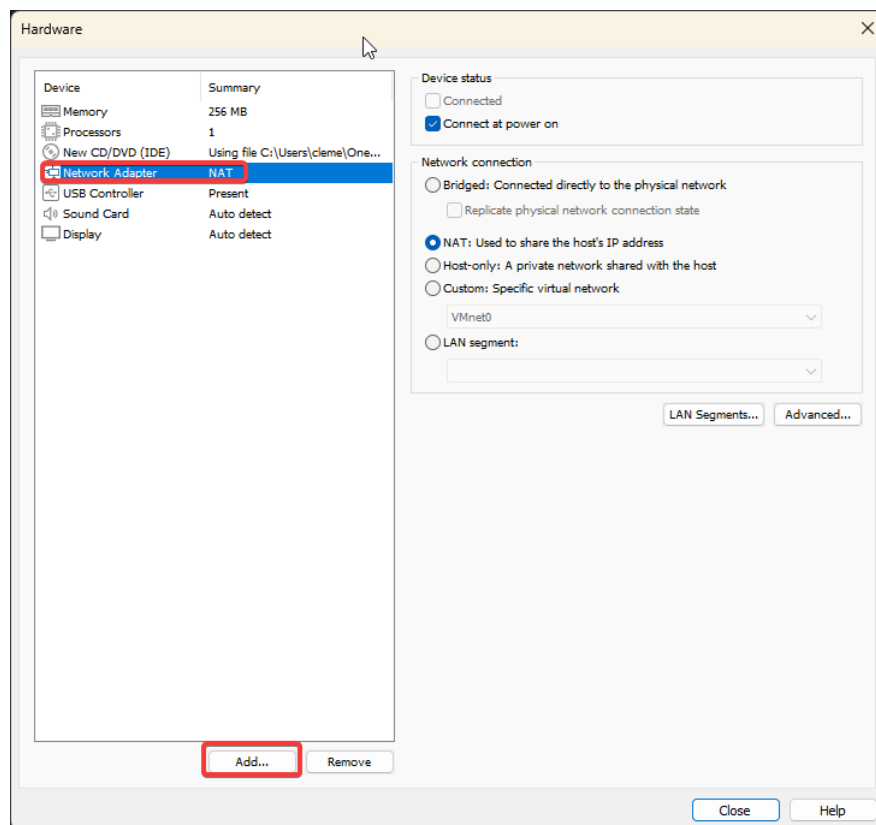
Ensuite, vu que nous sommes en train de faire un pare feu, je nomme ma machine « **Firewall_notatech** »



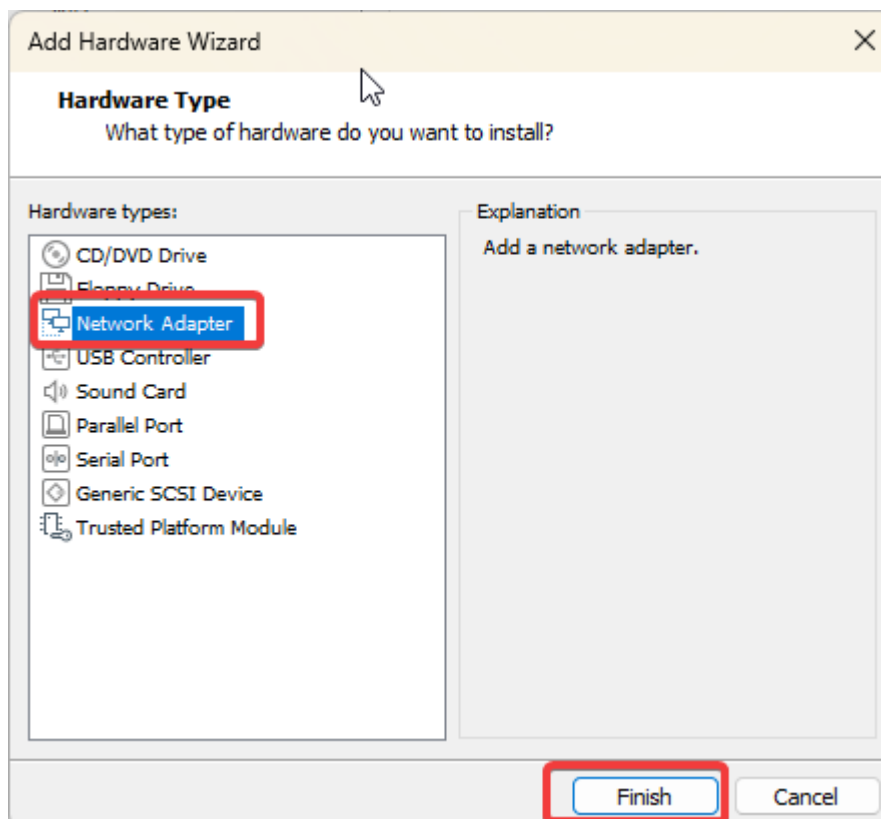
Pour les autres paramètres je les laisse par défaut et arrivé ici je clique sur « **customize hardware** » ici on va ajouter une deuxième carte réseau de manière a en avoir une en NAT et une en LAN segment



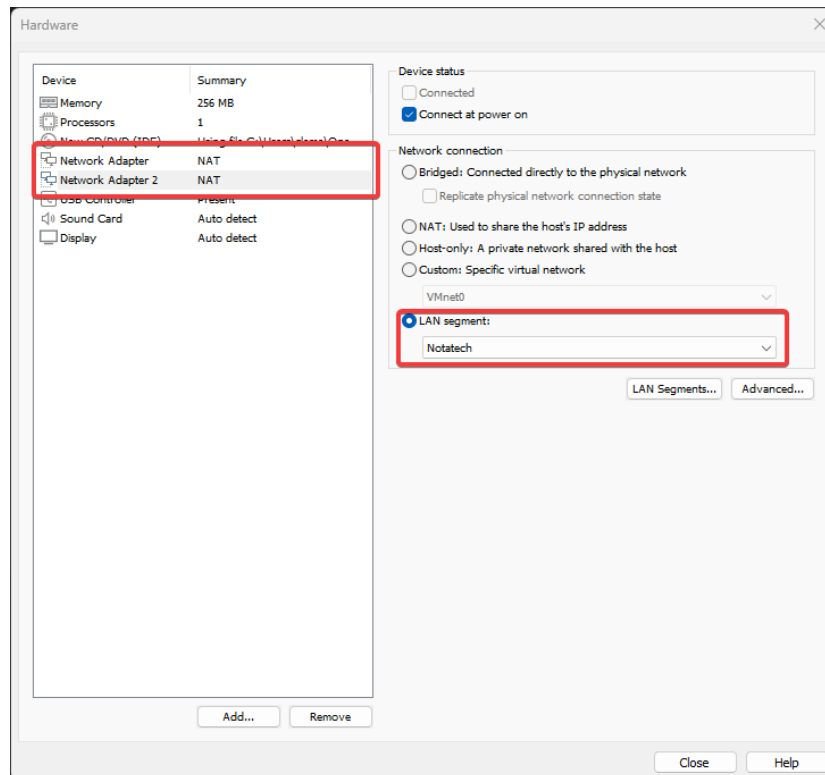
Ici je clique sur « **Add** » pour ajouter un équipement



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

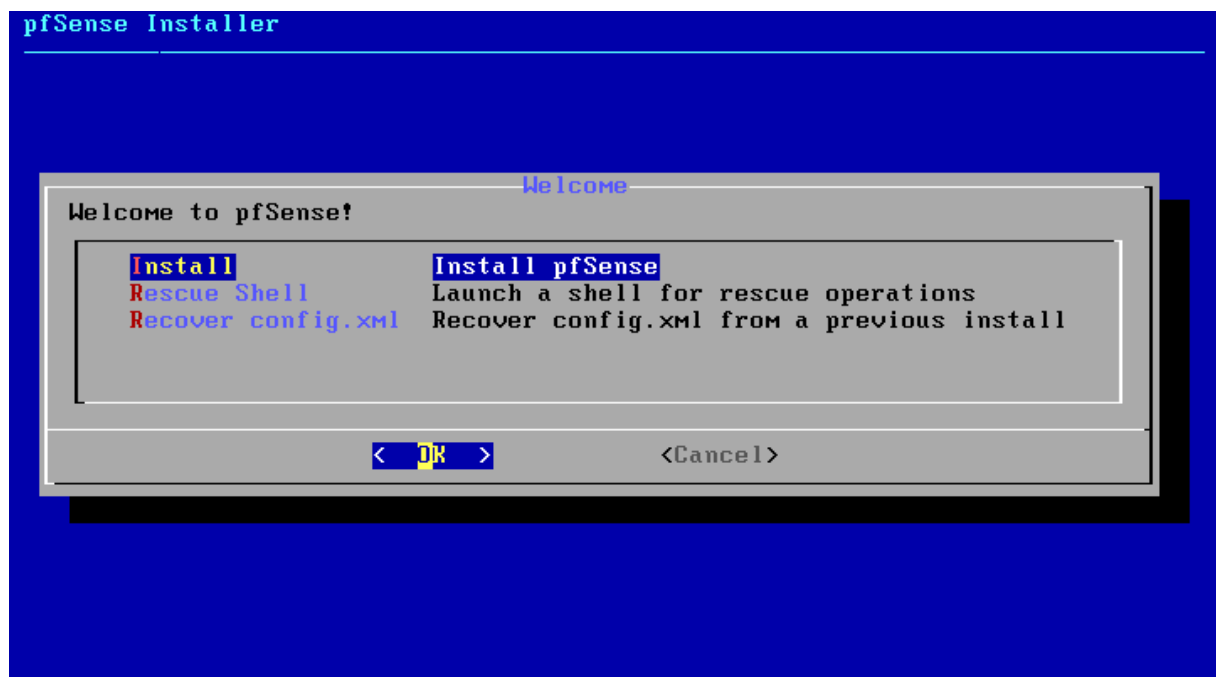


Et finalement je configure cette 2^{ème} carte réseau en LAN segment et la met sur le segment **Notatech**

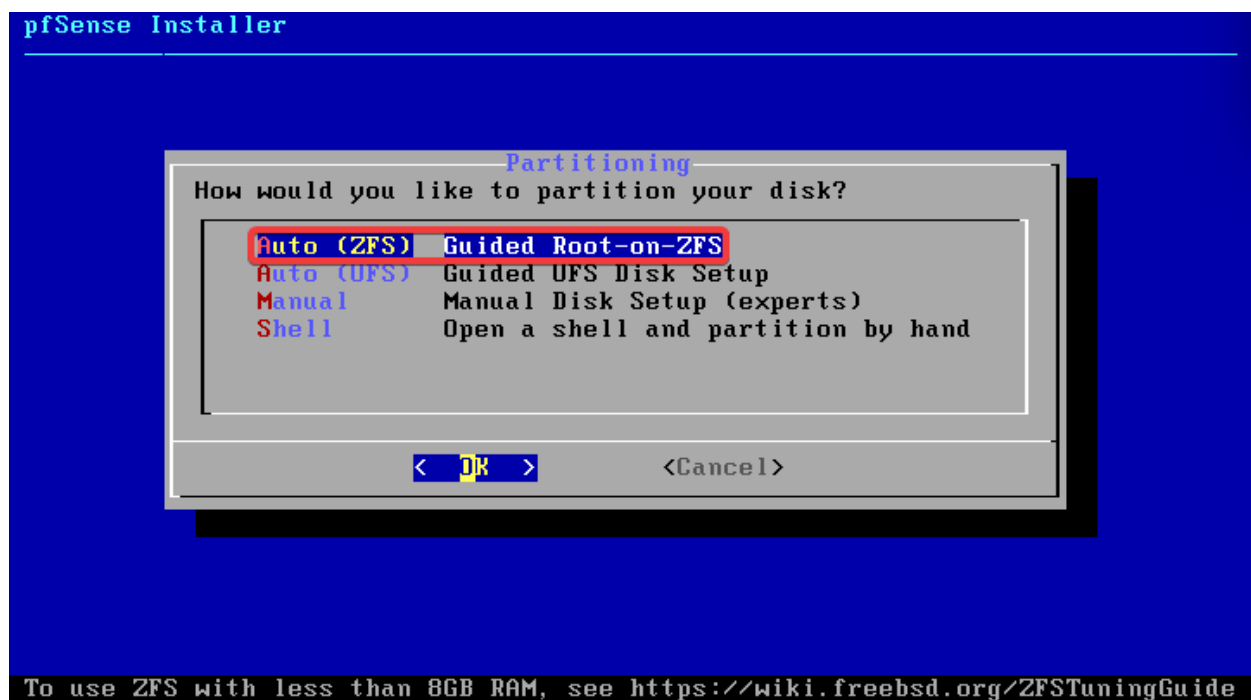


Installation du PfSense :

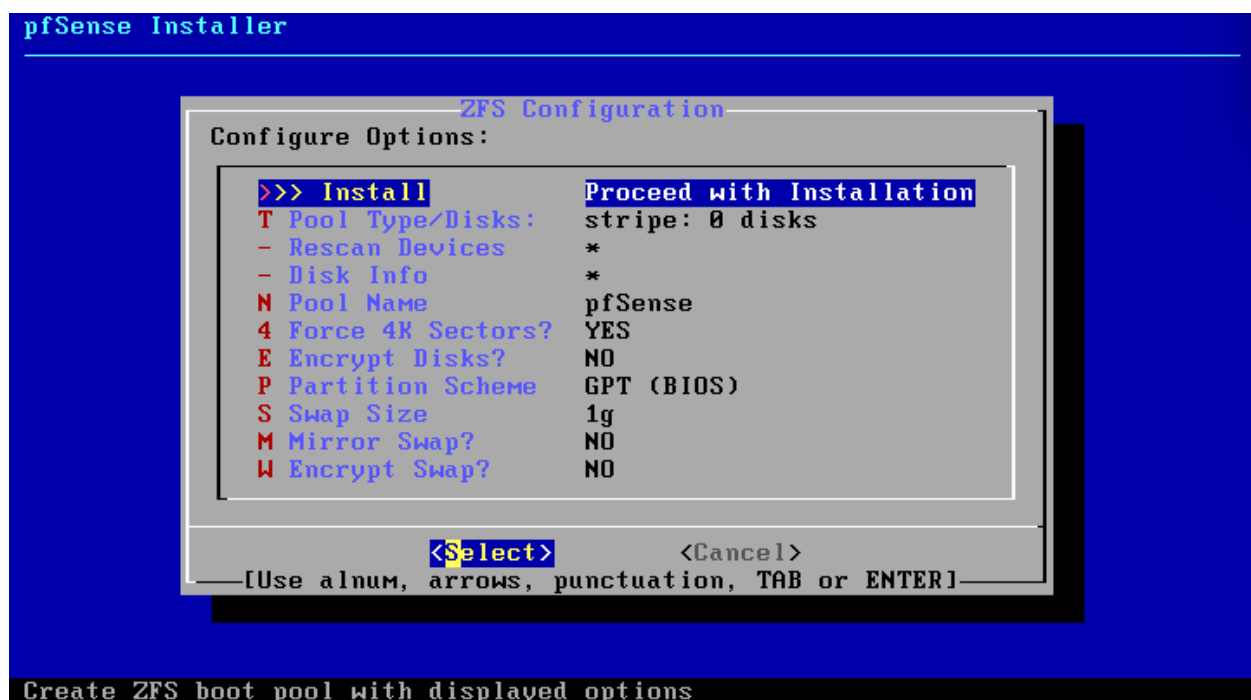
Ici on va passer a la partie installation du système pfsense. Arrivé sur cette première page, je sélectionne « **install PfSense** »



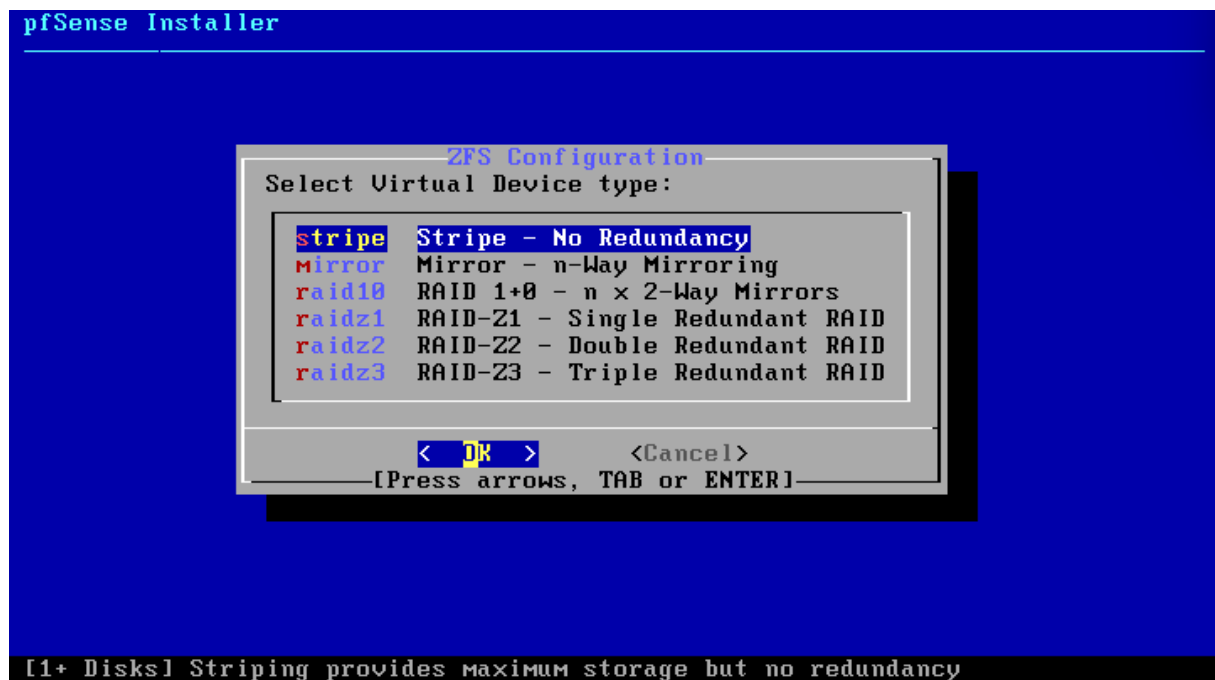
Ici je prend la 1^{ère} option : « **Auto ZFS** »



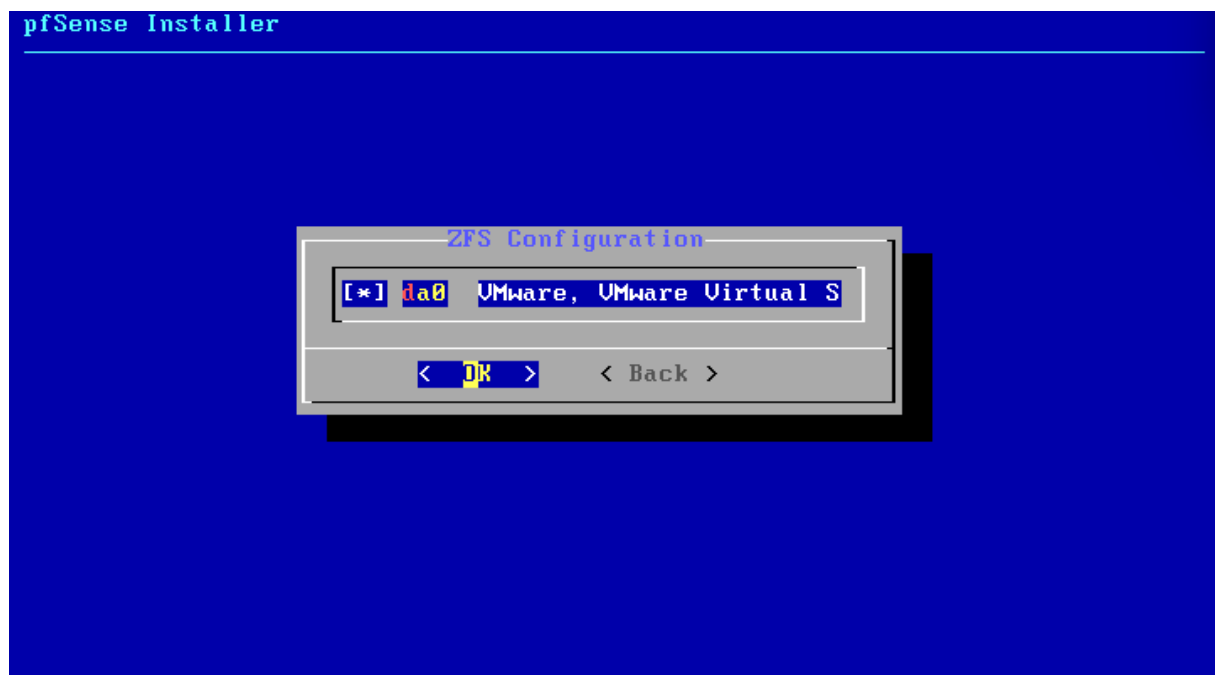
Ici je sélectionne **Install** et fait **Select**



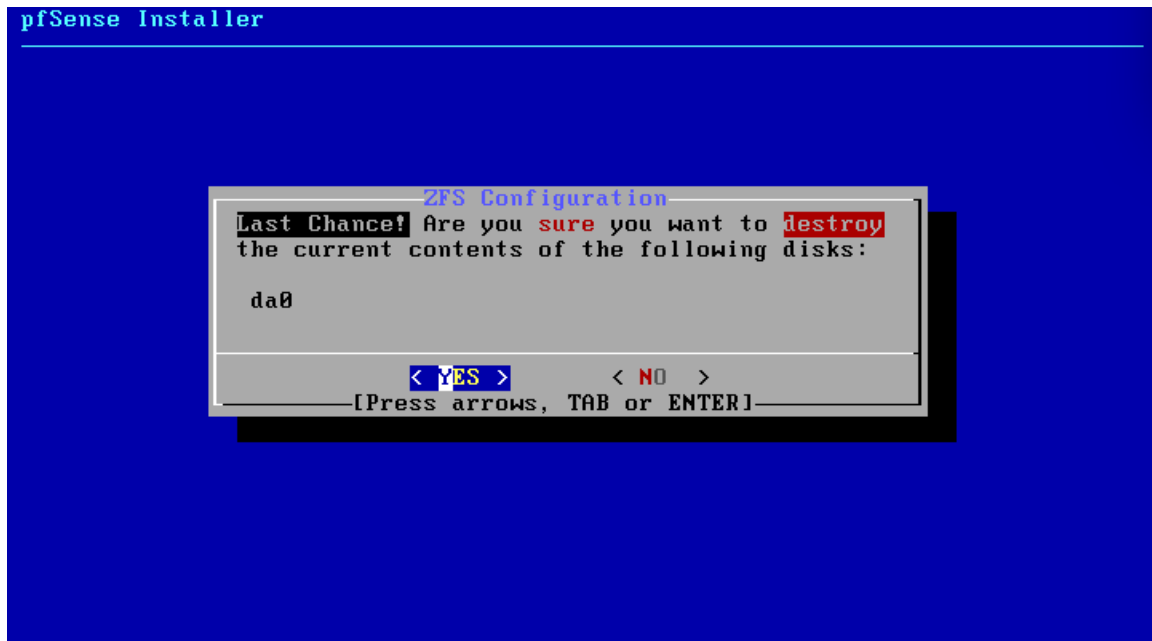
Ici je sélectionne **Stripe** car je ne souhaite pas configurer de redondance pour le moment



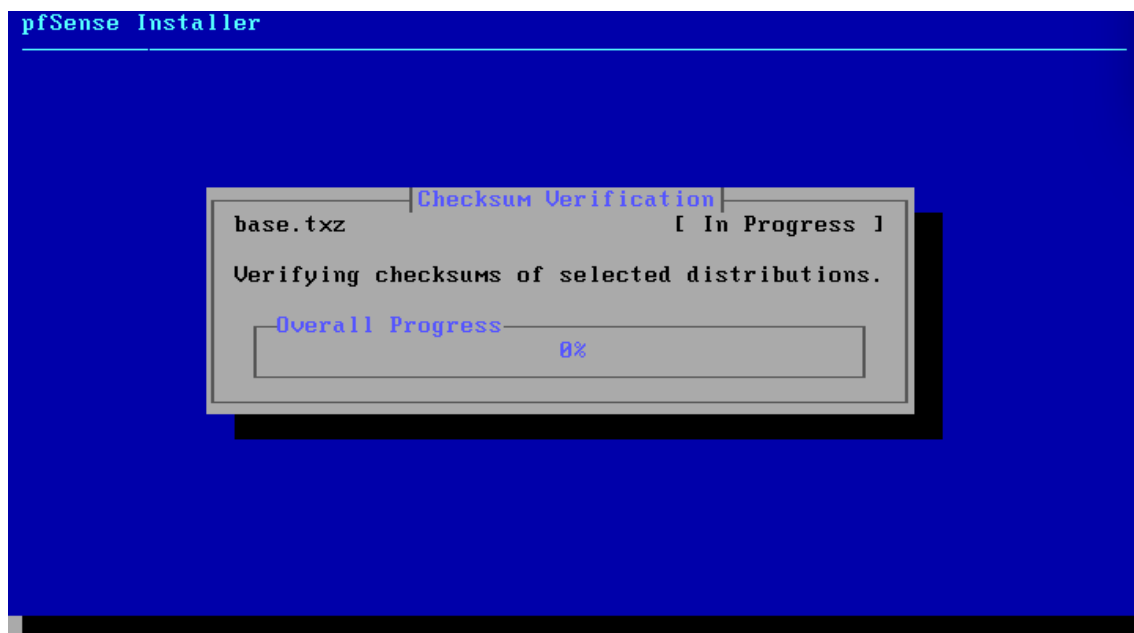
Ensuite je sélectionne mon disque ici et clique sur **OK**



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 redémarré, le PfSense nous affiche une page comme celle-ci, nous indiquant les IP des différentes interfaces et les options de paramètre

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 3f64ecda514e62012b8d

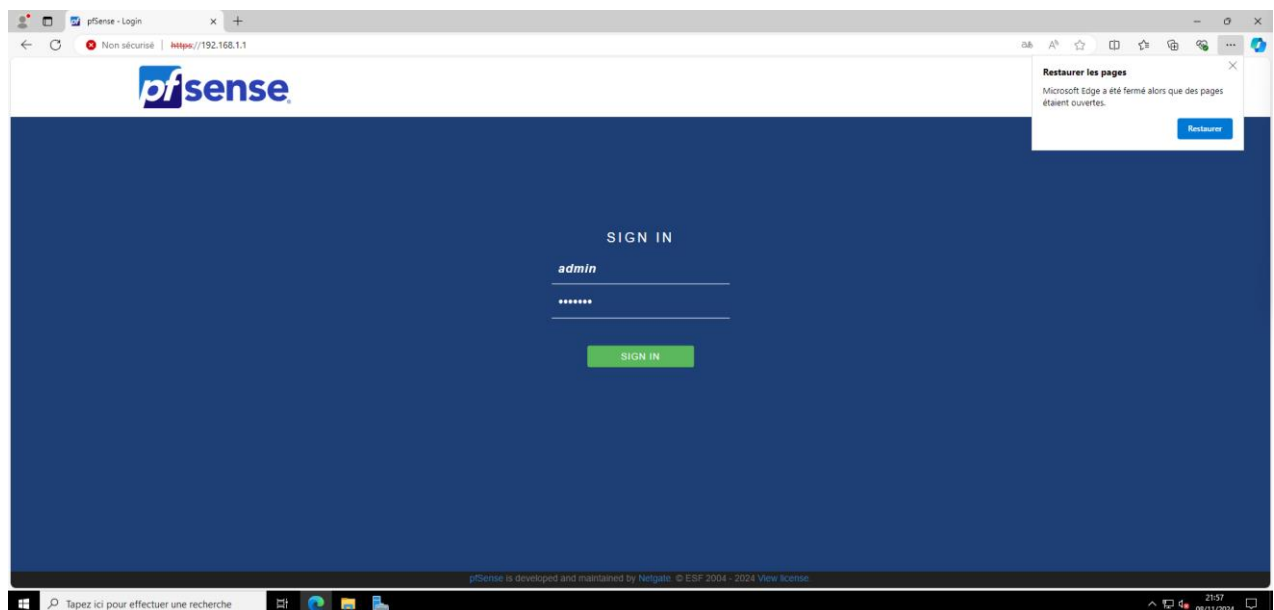
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.73.162/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

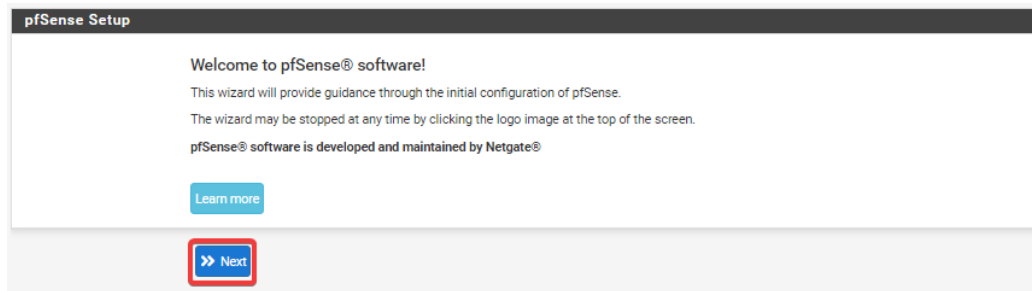
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: 
```

Nous n'allons pas rester plus sur la machine PfSense, nous allons juste la laisser démarrée 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

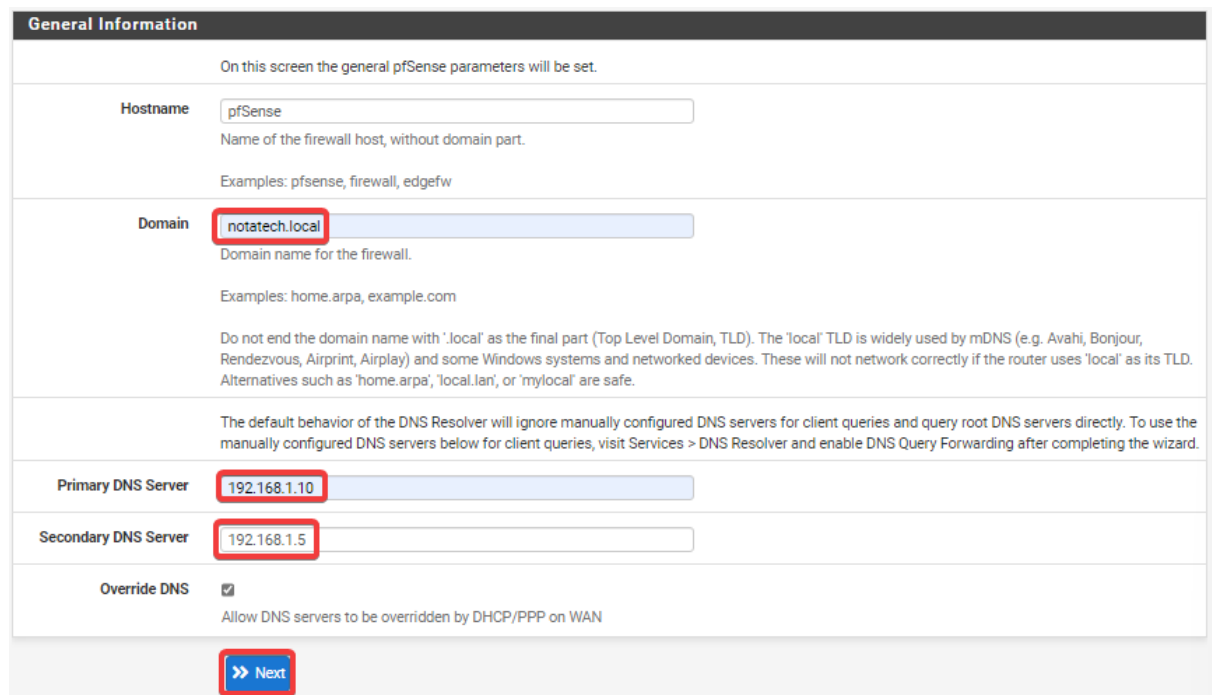


Ensuite nous allons rentrer dans la configuration de notre **PfSense**, je clique donc simplement sur **Next**



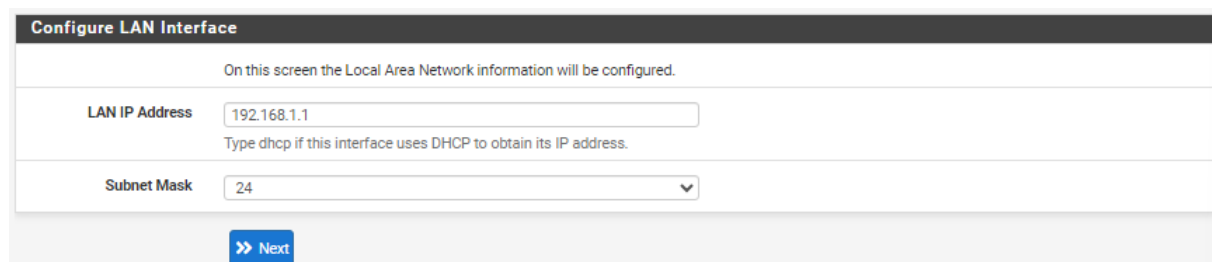
The image shows the 'pfSense Setup' screen. It has a dark header with the text 'pfSense Setup'. Below the header, the text reads: 'Welcome to pfSense® software!', 'This wizard will provide guidance through the initial configuration of pfSense.', 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.', and 'pfSense® software is developed and maintained by Netgate®'. There is a 'Learn more' button and a 'Next' button with a double arrow icon. The 'Next' button is highlighted with a red box.

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**



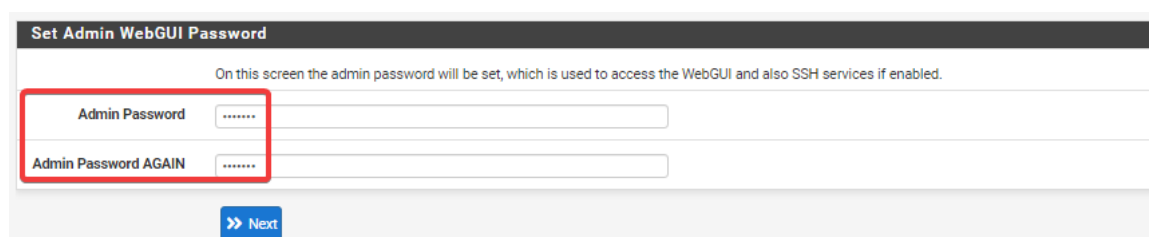
The image shows the 'General Information' screen. It has a dark header with the text 'General Information'. Below the header, the text reads: 'On this screen the general pfSense parameters will be set.' The form contains the following fields: 'Hostname' with the value 'pfSense', 'Domain' with the value 'notatech.local', 'Primary DNS Server' with the value '192.168.1.10', and 'Secondary DNS Server' with the value '192.168.1.5'. There is also a checkbox for 'Override DNS' which is checked. The 'Next' button is highlighted with a red box.

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



The image shows the 'Configure LAN Interface' screen. It has a dark header with the text 'Configure LAN Interface'. Below the header, the text reads: 'On this screen the Local Area Network information will be configured.' The form contains the following fields: 'LAN IP Address' with the value '192.168.1.1' and 'Subnet Mask' with the value '24'. The 'Next' button is highlighted with a red box.

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



Et la configuration principale de notre PfSense est terminée !

Congratulations! pfSense is now configured.

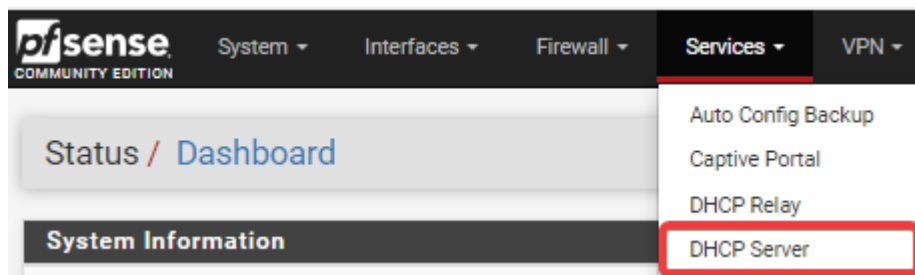
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

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**



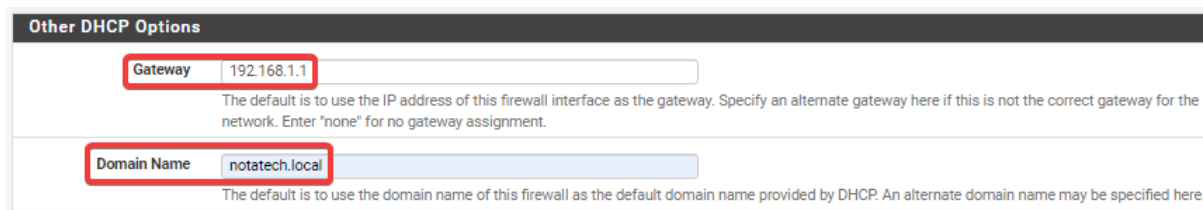
Ici je coche « **Enable DHCP server on LAN interface** », je définis mon **Pool Range** de **192.168.1.100** jusqu'à **192.168.1.200** et finalement je renseigne l'IP de mes 2 serveurs AD dans les **Server Options**

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	☒ Enable DHCP server on LAN interface
BOOTP	☐ Ignore BOOTP queries
Deny Unknown Clients	Allow all clients When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	☐ Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool	
Subnet	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	From 192.168.1.100 To 192.168.1.200 The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options	
WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.1.10
	192.168.1.5

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**



Other DHCP Options

Gateway

The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

Domain Name

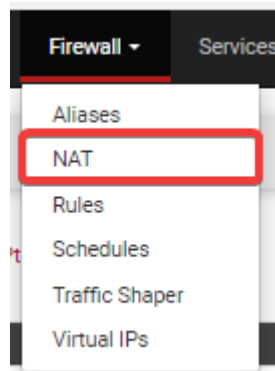
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.

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

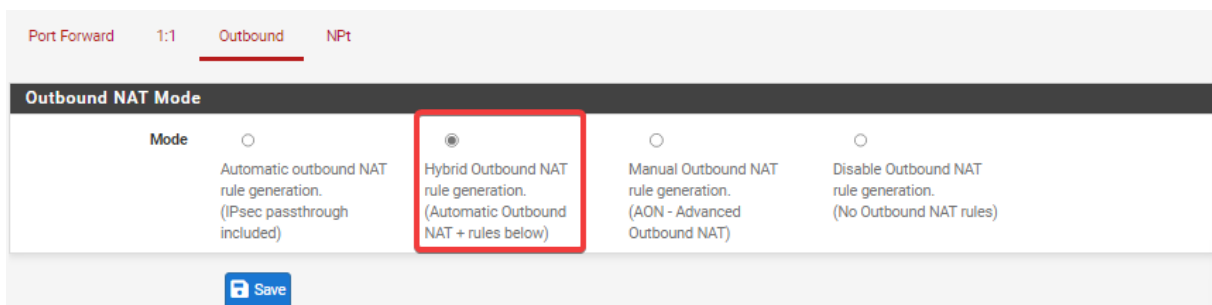
Configuration internet pour les clients :

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

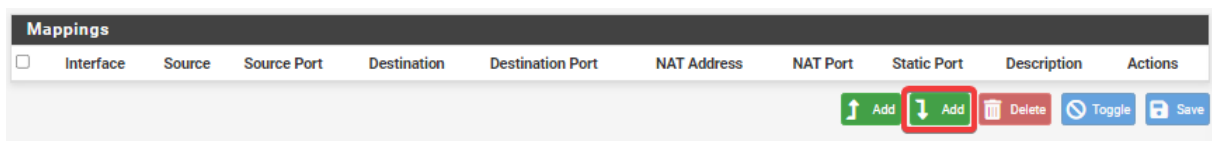
Dans un premier temps, dans l'interface web du PfSense je clique sur **Firewall > NAT**



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

Edit Advanced Outbound NAT Entry

☐ Disabled ☐ Disable this rule

Do not NAT ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface WAN
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which protocol this rule should match. In most cases "any" is specified.

Source Network or Alias 192.168.1.1 / 24
Type Source network for the outbound NAT mapping. Port or Range

Destination Any
Type Destination network for the outbound NAT mapping. Port or Range

☐ Not
Invert the sense of the destination match.

Translation

Address WAN address
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

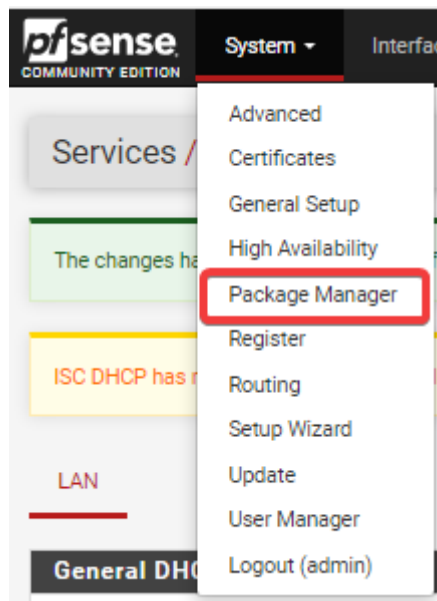
Port or Range ☐ Static Port
Enter the external source Port or Range used for remapping the original source port on connections matching the rule.
Port ranges are a low port and high port number separated by "-".
Leave blank when Static Port is checked.

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

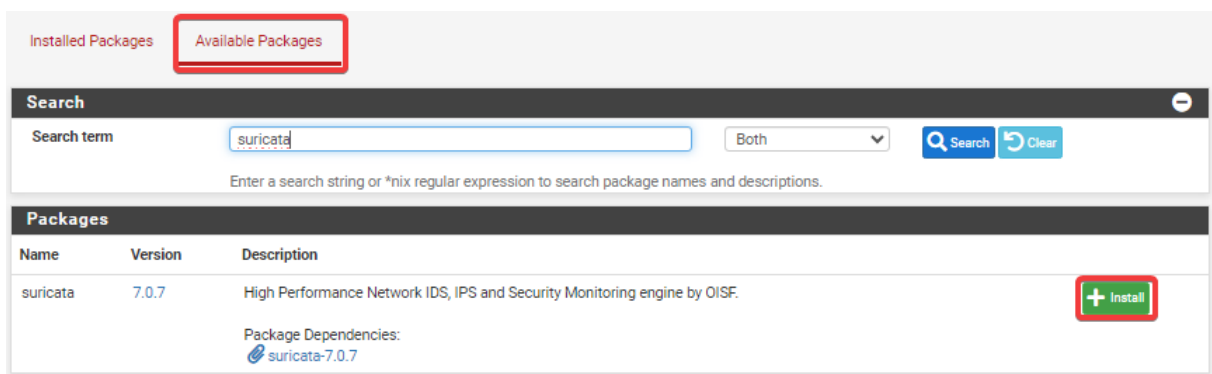
Configuration d'un IPS/IDS :

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

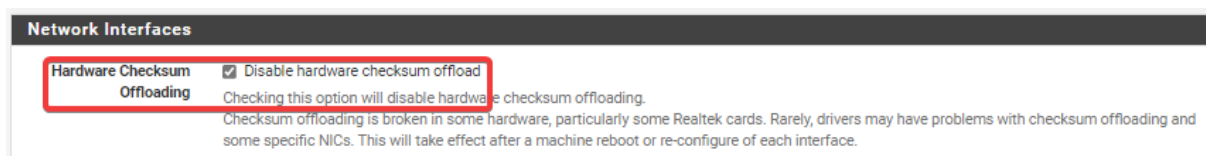
Je commence tout d'abord par me rendre dans **System > Package Manager** sur l'interface web de mon PfSense



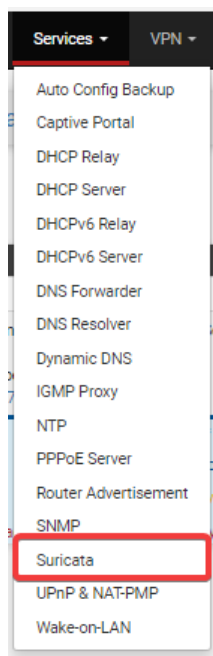
Ensuite je clique sur **Available Packages** et je recherche **Suricata** et je clique sur **Install**



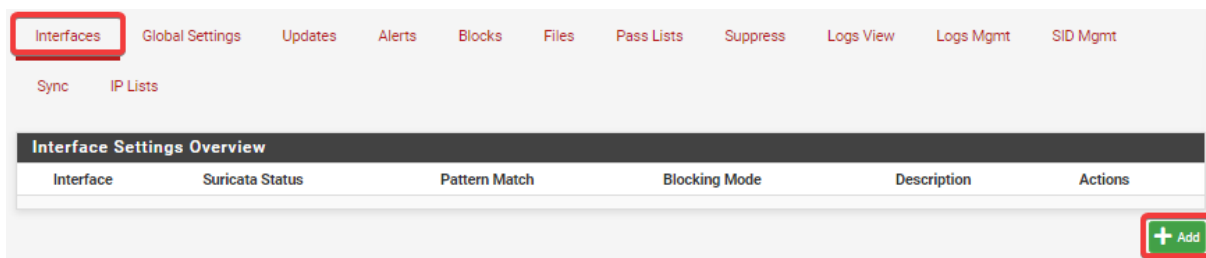
Pour que le Suricata fonctionne bien il faudra tout d'abord désactiver cette option dans **System > Advanced > Networking**



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

WAN Settings

General Settings

Enable ☒ Checking this box enables Suricata inspection on the interface.

Interface WAN (em0)
Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.

Description protection_exterieure
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.

Logging Settings

Send Alerts to System Log ☒ Suricata will send Alerts from this interface to the firewall's system log.
NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.

Log Facility LOCAL1
Select system log Facility to use for reporting. Default is LOCAL1.

Log Priority NOTICE
Select system log Priority (Level) to use for reporting. Default is NOTICE.

Enable Stats Collection ☐ Suricata will periodically gather performance statistics for this interface. Default is Not Checked.

Enable HTTP Log ☒ Suricata will log decoded HTTP traffic for the interface. Default is Checked.

HTTP Log File Type Regular
Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular"

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

Alert and Block Settings

Block Offenders ☒ Checking this option will automatically block hosts that generate a Suricata alert.

IPS Mode Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

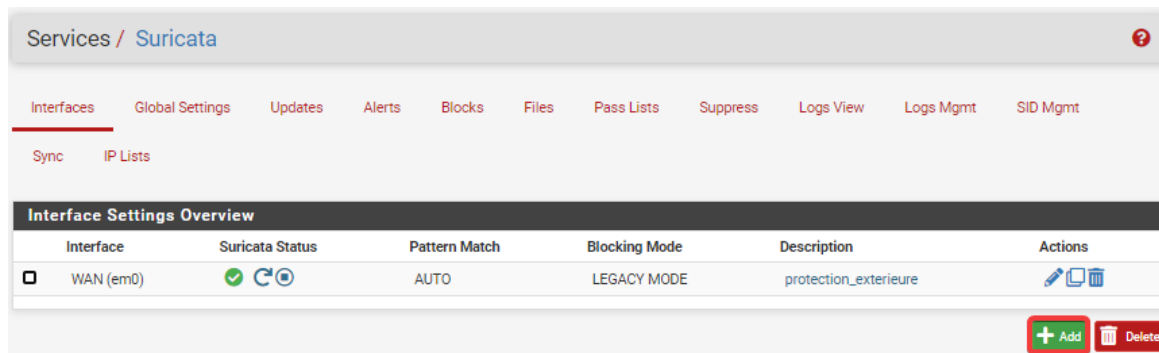
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.

Which IP to Block BOTH
Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

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

LAN Settings

General Settings

Enable ☒ Checking this box enables Suricata inspection on the interface.

Interface LAN (em1) ▼
Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.

Description Surveillance Locale
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.

Logging Settings

Send Alerts to System Log ☒ Suricata will send Alerts from this interface to the firewall's system log.
NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.

Log Facility LOCAL1 ▼
Select system log Facility to use for reporting. Default is LOCAL1.

Log Priority WARNING ▼
Select system log Priority (Level) to use for reporting. Default is NOTICE.

Enable Stats Collection ☐ Suricata will periodically gather performance statistics for this interface. Default is Not Checked.

Enable HTTP Log ☒ Suricata will log decoded HTTP traffic for the interface. Default is Checked.

HTTP Log File Type Regular ▼
Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular"

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