PROJET E5 BTS SIO SISR :

INFRASTRUCTURE RÉSEAU NOTATECH

Documentation technique

REDOULES CLÉMENT

Contexte :

Dans le cadre de mon **deuxième projet de BTS SIO SISR**, j'ai conçu une **infrastructure réseau robuste et complète** pour l'entreprise fictive **Notatech**, intégrant plusieurs solutions avancées afin de garantir la **sécurité, la gestion centralisée des ressources et la continuité des services**.

L'infrastructure repose sur un **serveur Windows** assurant la gestion des utilisateurs via **Active Directory, DNS et DHCP**, associé à un **pare-feu pfSense** configuré avec **Suricata** pour la détection et prévention des intrusions (**IDS/IPS**).
Parmi les améliorations majeures apportées :

- Un **serveur NAS sous TrueNAS**, garantissant le stockage sécurisé et la redondance des données.
- Un **serveur de sauvegarde Veeam Backup**, permettant une protection optimale et une restauration rapide des données critiques.
- Une plateforme de **gestion de parc informatique via GLPI**.
- La mise en place d'un **serveur VPN OpenVPN**, assurant un accès distant sécur isé.
- L'installation d'un **serveur web IIS**, hébergeant un site internet destiné à l'entreprise.

Cette infrastructure répond aux besoins d'une PME moderne, combinant **sécurité**, **résilience** et **performance**, tout en facilitant la gestion des utilisateurs, des équipements et des services web.

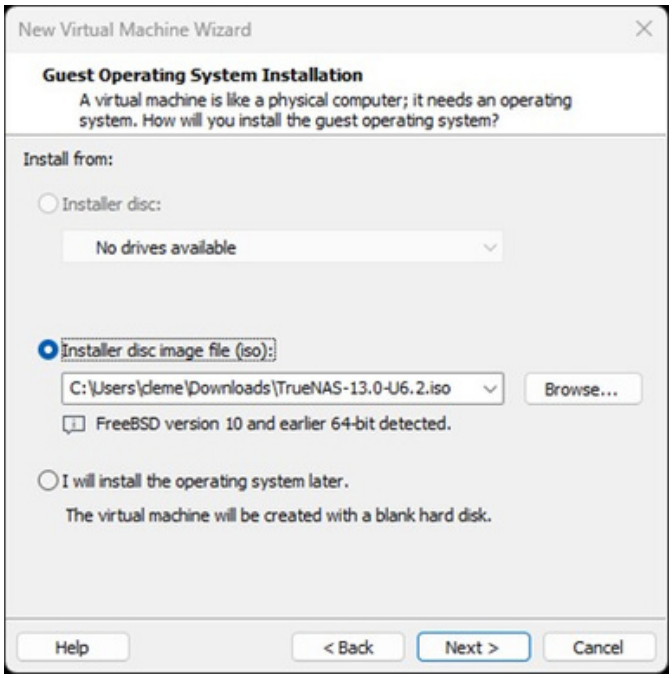
Sommaire :

Dans cette section, je vais expliquer comment j'ai mis en place un serveur NAS sous TrueNAS. Ce serveur permet le stockage sécurisé et la gestion des partages de fichiers, tout en assurant la redondance des données grâce à ZFS.

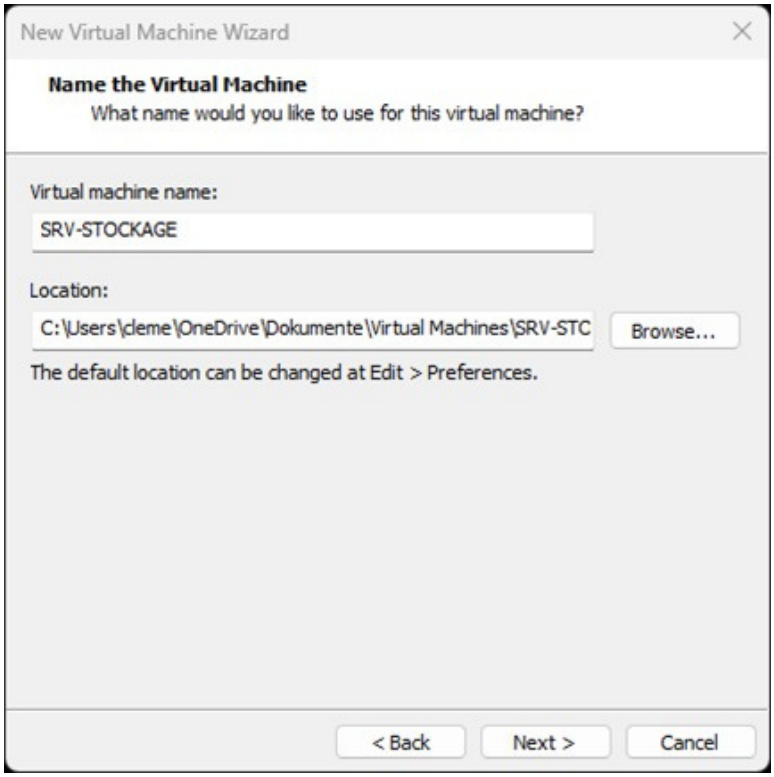
Création du serveur NAS :

Pour ce faire, je commence par me rendre sur vmware et je créer une nouvelle machine virtuelle, au niveau de la configu²ration de la VM je sélectionne **« typical »** car cela suffit a la configuration de notre serveur NAS

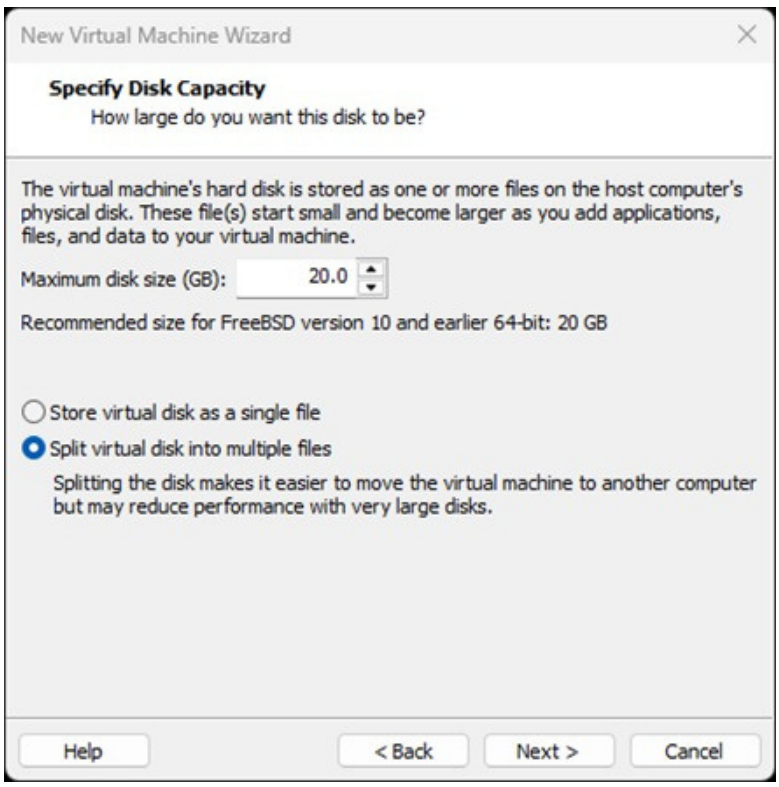
Ensuite ici je sélectionne l'ISO de Truenas afin d'installer l'image de celui-ci sur la machine



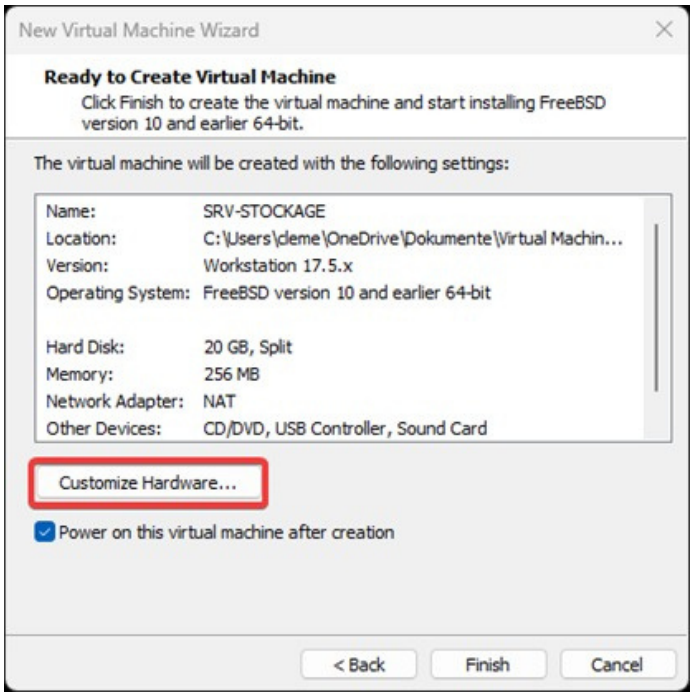
Ensuite ici on me demande de saisir le nom de ma machine, j'écris donc **« SRV- STOCKAGE »** pour bien l'identifier par rapport aux autres serveurs

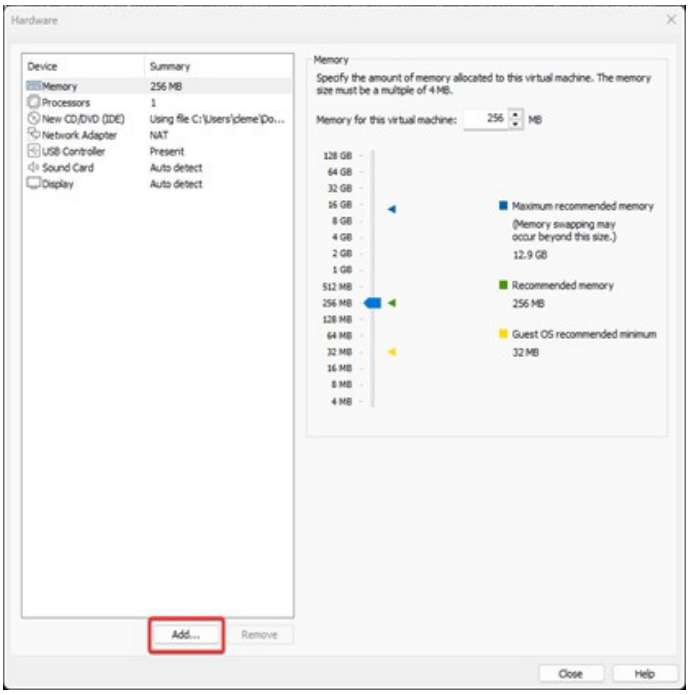


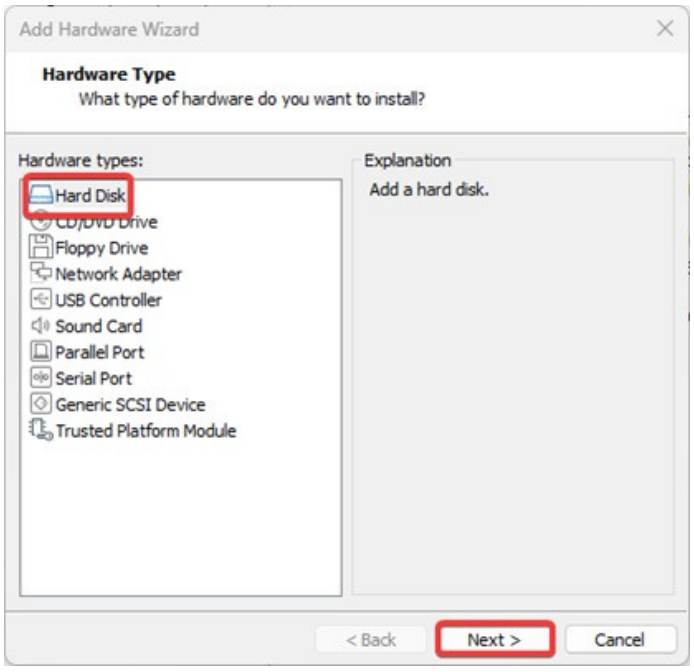
Ensuite ici on me demande de choisir la taille du disque de notre serveur, en sachant que ce disque est le disque système et non celui qui nous permettra de stocker les données, je laisse donc a 20gb

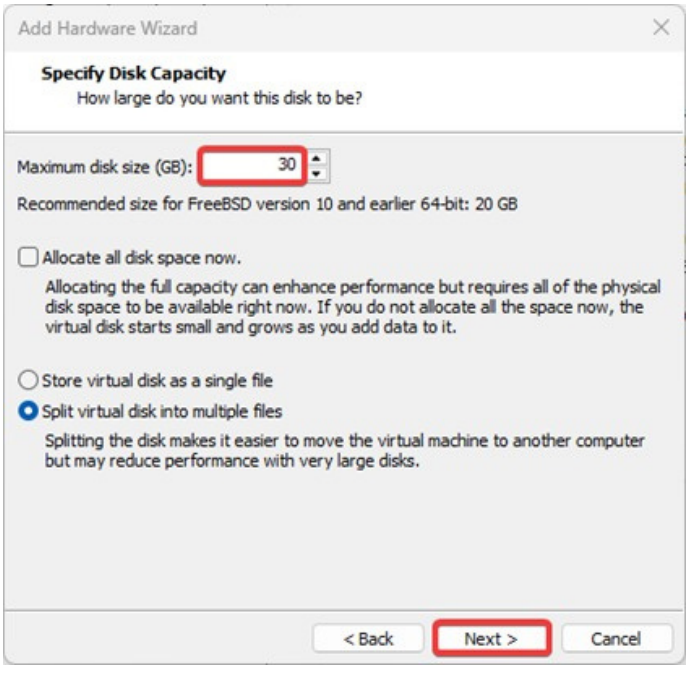


Ensuite ici je vais ajouter un disque, afin d'y stocker les éléments qui seront accessible par le serveur, je sélectionne donc **« customize hardware »**, je clique sur **« Add »**, sélectionne **« Hard Disk »**, et finalement je saisis 30go, ce qui sera amplement suffisant pour stocker des données tels que des fichiers texte, zip etc... que les employés pourraient stocker.

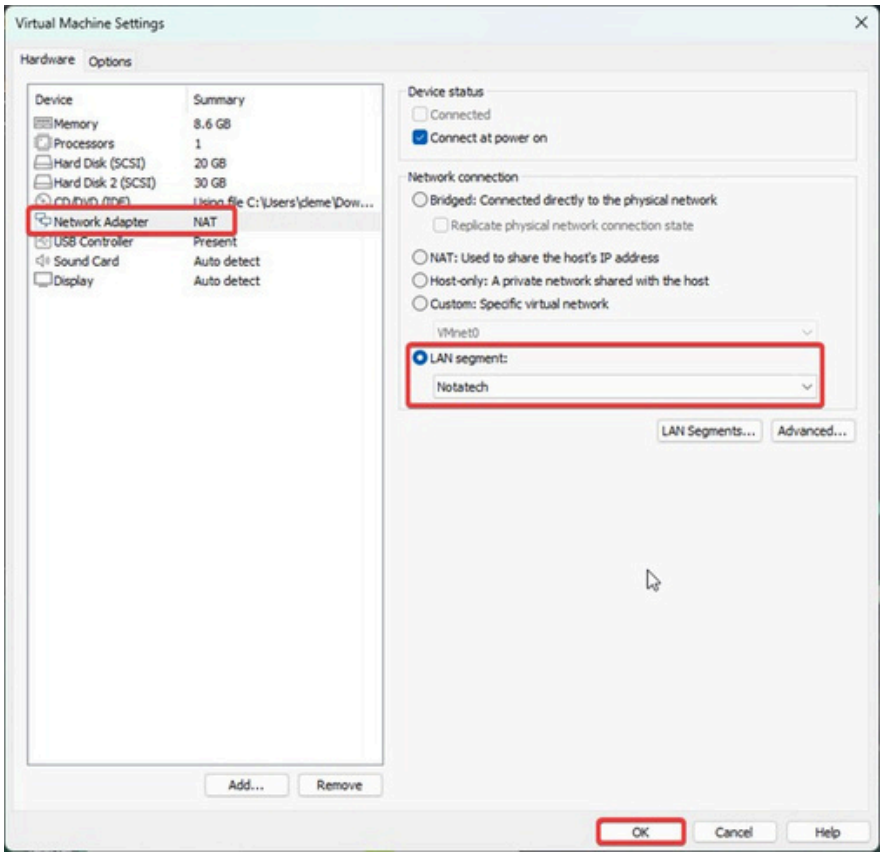








Et par la même occasion avant de continuer je me dois de mettre la machine dans le réseau **Notatech** je me rend donc dans **« network adapter »** et sélectionne dans **« LAN segment »** mon segment **Notatech.**

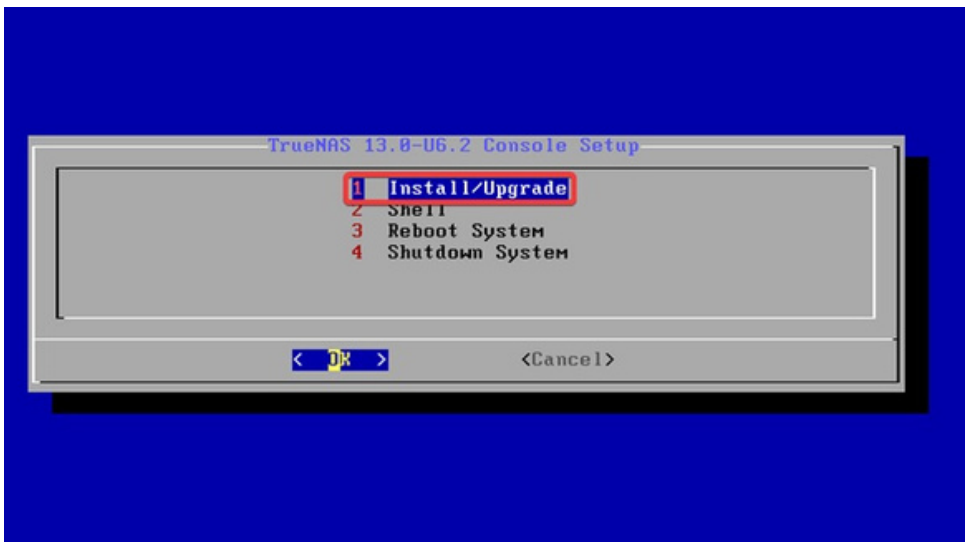


On peut donc finalement démarrer la machine et commencer la configuration de celle-ci

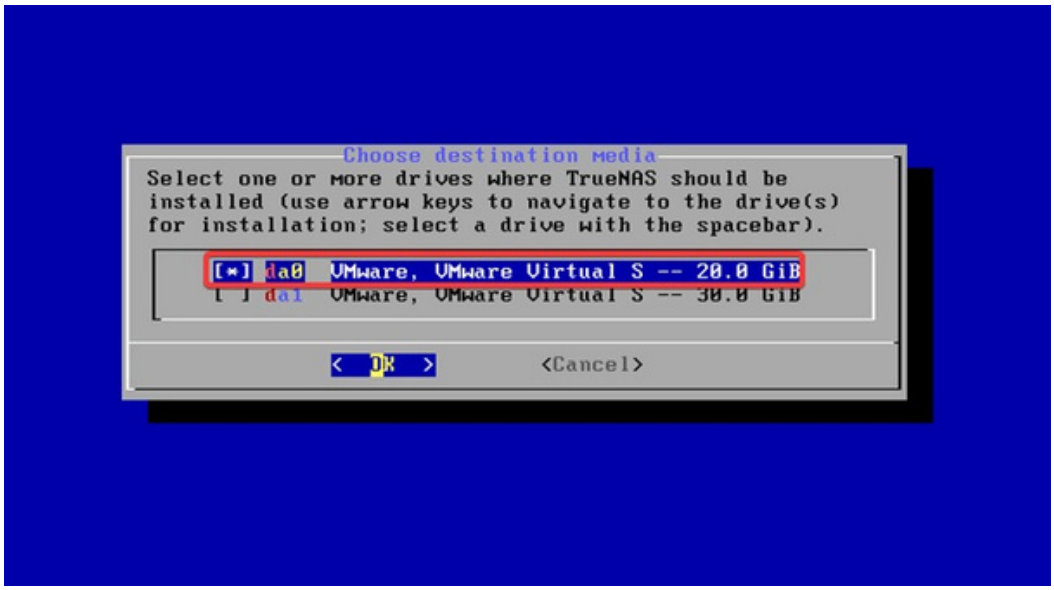
Première configuration du serveur NAS :

Maintenant que le serveur est créé la première configuration doit maintenant être faite.

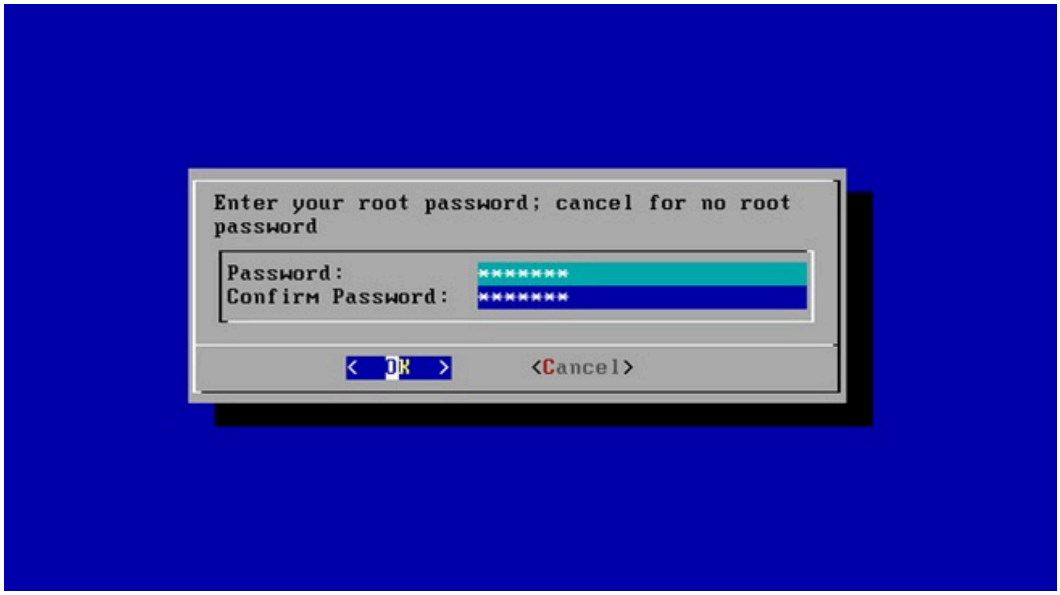
Premièrement en démarrant la machine cet écran apparait, sur cet écran je sélectionne **Install/Upgrade**



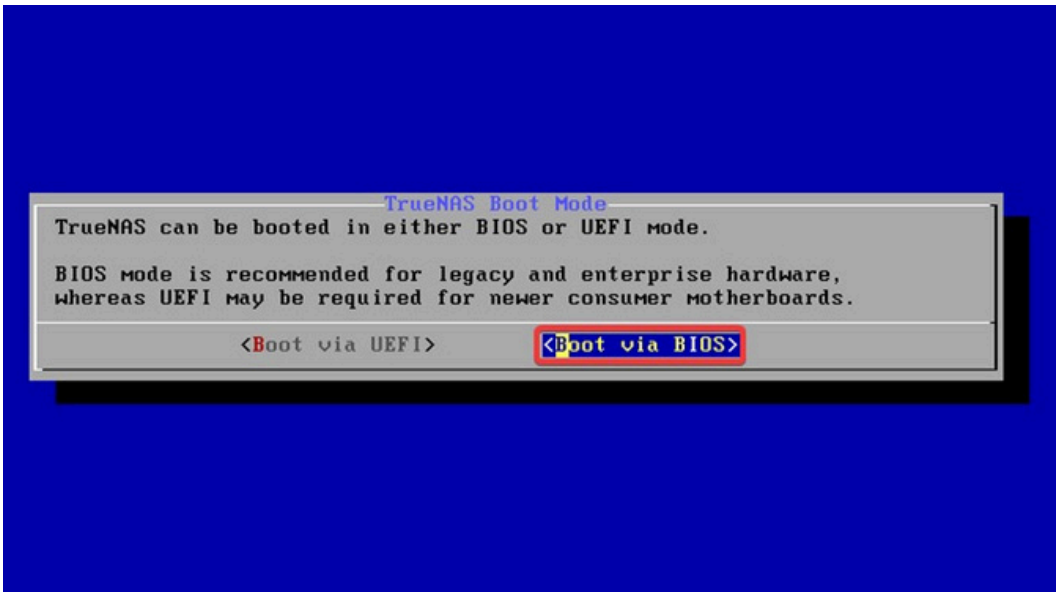
Ensuite ici Truenas me demande de sélectionner le disque ou installer les fichiers nécessaires au fonctionnement de la machine, je sélectionne donc le premier car le 2ème correspond au disque qui servira à stocker les fichiers



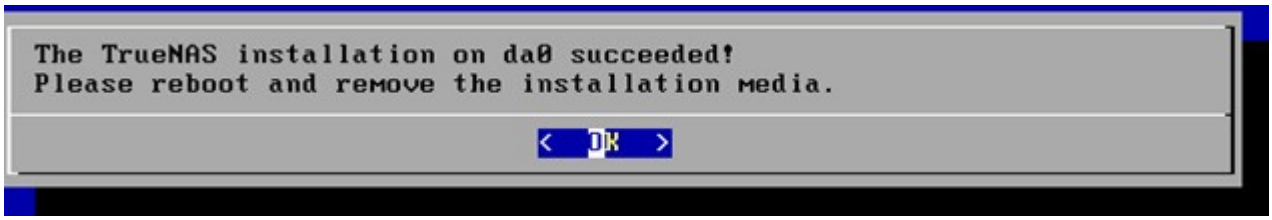
Ensuite ici on me demande de rentrer le mot de passe pour Truenas, je saisis donc le mot de passe et appuie sur **OK.**



Ensuite ici je dois sélectionner le mode de démarrage, vu que nous sommes sur une machine virtuelle je sélectionne donc **« Boot via BIOS »**



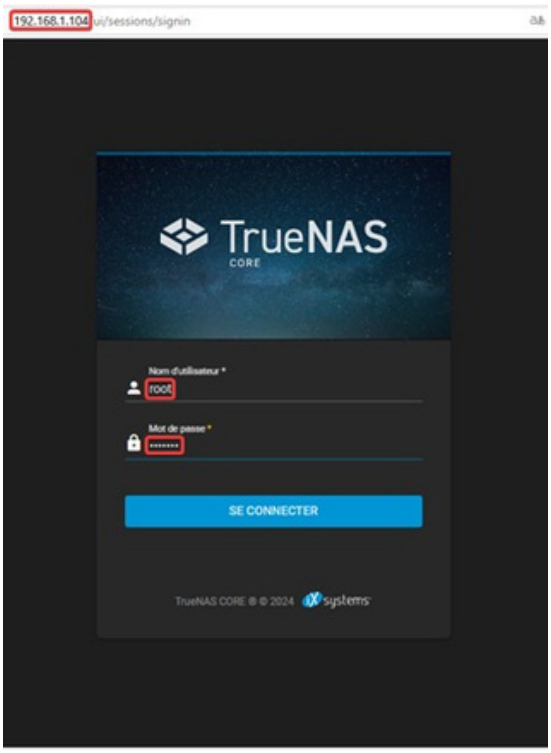
Ensuite le serveur NAS va donc se configurer et cet écran apparait nous confirmant que l'installation sur le disque s'est bien effectuée, je n'ai plus qu'à redémarrer la machine sans le disque d'image et le serveur NAS est prêt



Configuration sur l'interface web du serveur de stockage :

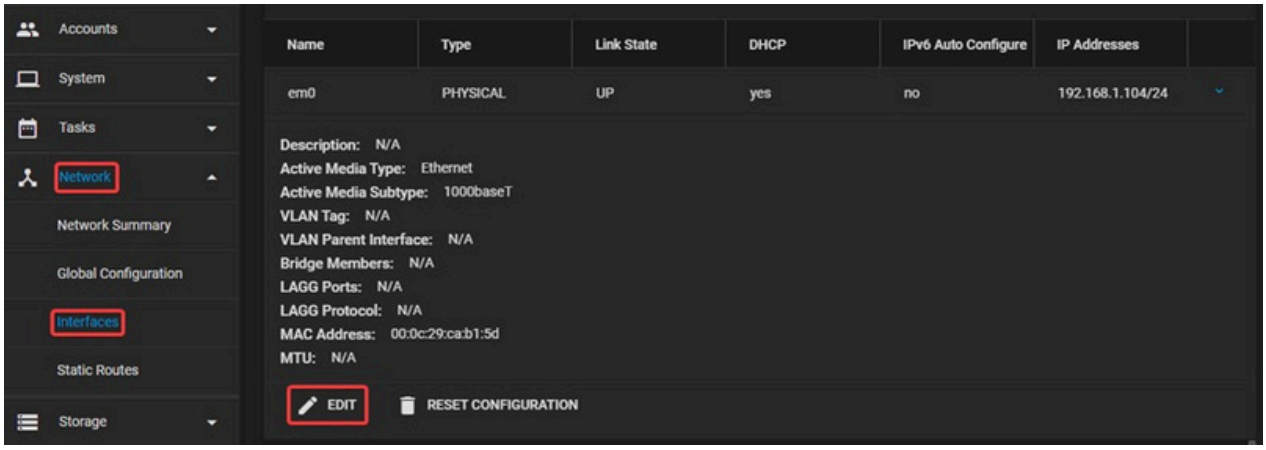
Maintenant que notre serveur NAS est prêt, je vais devoir me rendre sur l'interface web de celui-ci afin de configurer mon disque de stockage et faire en sorte qu'il soit accessible par les utilisateurs

Pour commencer je me rends donc sur mon serveur de production et rentre dans la barre de recherche l'adresse IP de mon serveur NAS, en l'occurrence **« 192.168.1.104 »** et rentre les identifiants pour me connecter à mon serveur

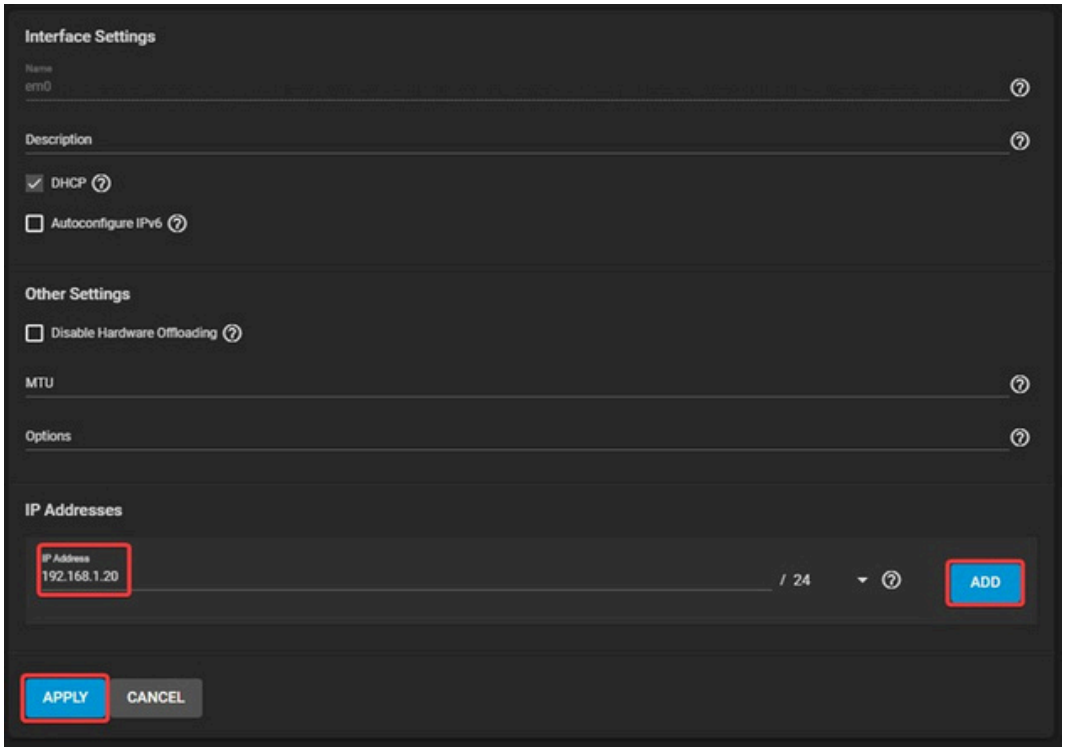


Ensuite une fois connecté je vais tout d'abord commencer par attribuer une autre adresse statique à **mon serveur NAS** car mon adresse est actuellement **192.168.1.104** et j'aimerai la changer **en 192.168.1.20**, car mon **DHCP** attribue des adresses allant de **192.168.1.100** à **192.168.1.200**

Pour ce faire sur l'interface web je clique donc sur **Network, Interfaces** et ensuite **EDIT**

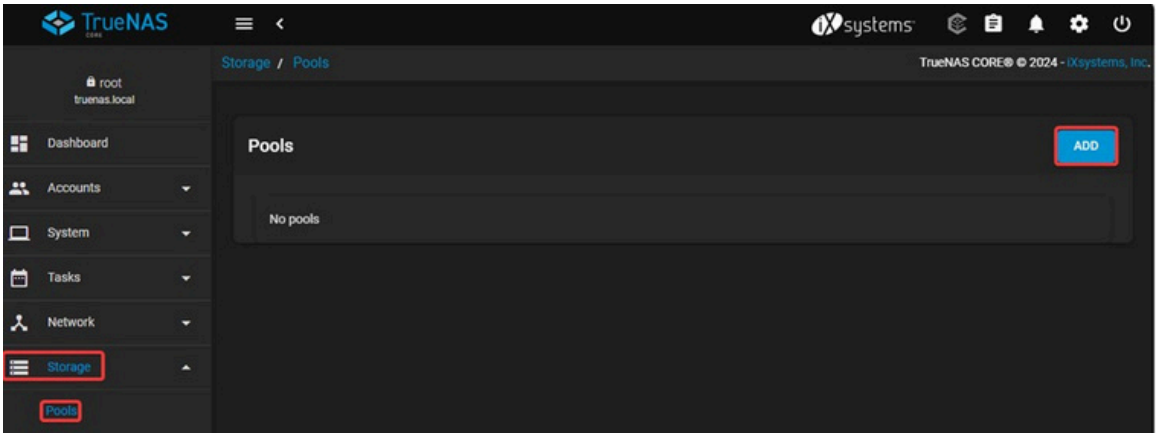


Ensuite je saisi simplement l'adresse IP que je souhaite avoir dans le champ, clique sur **« ADD »** puis **« APPLY »**

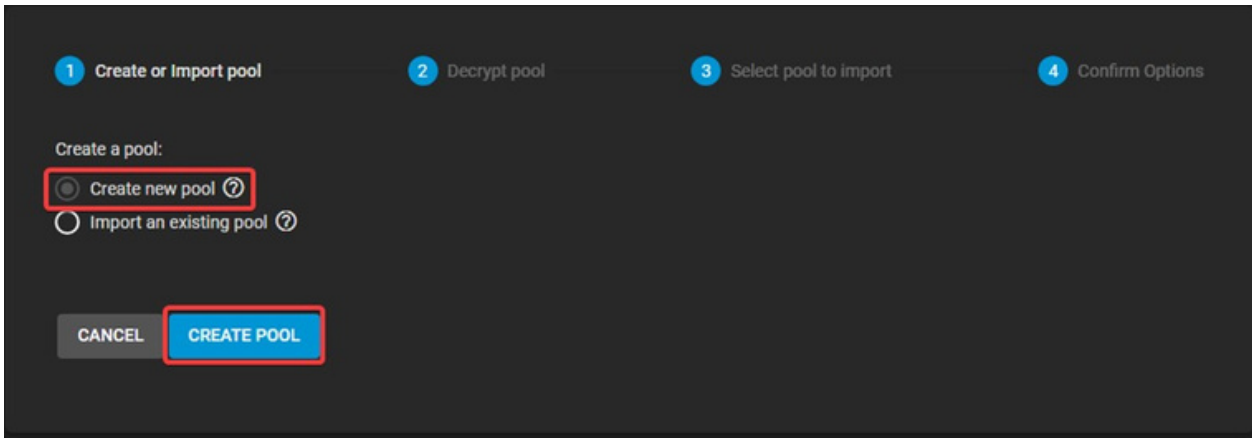


L'adresse de mon Truenas est donc bien en 192.168.1.20, je redémarre simplement mon serveur après ça

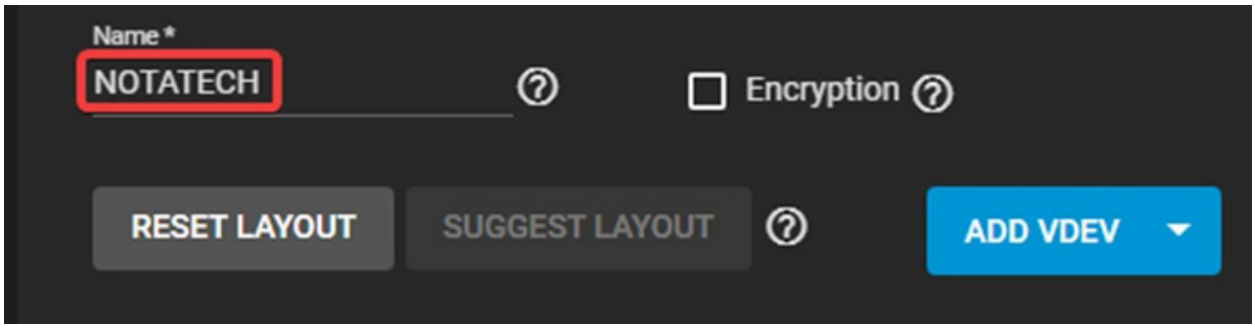
Une fois ceci fait, je vais créer mon **Pool de stockage** pour ce faire je me rend dans **Storage** puis dans **Pools**



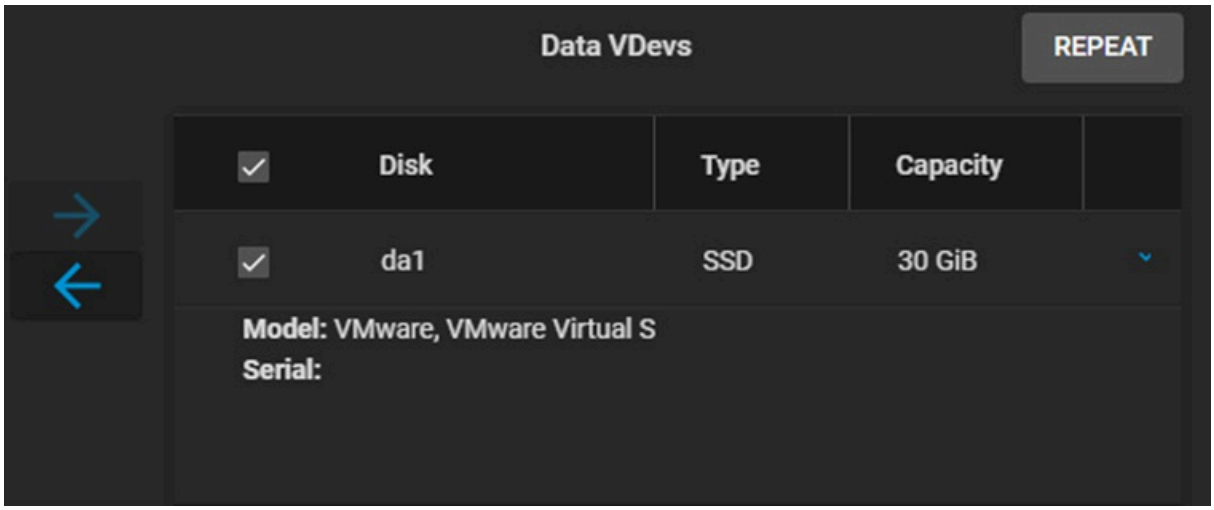
Ensuite ici je sélectionne **« Create new pool »** puis je clique sur **« CREATE POOL »**



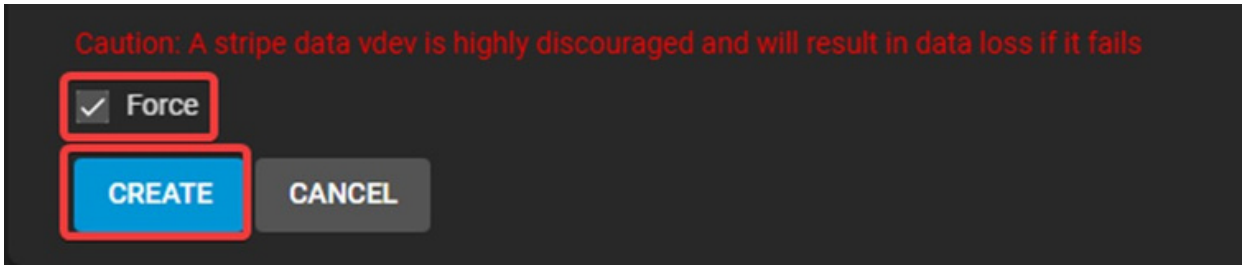
Ensuite pour le nom de mon pool je saisis **NOTATECH**



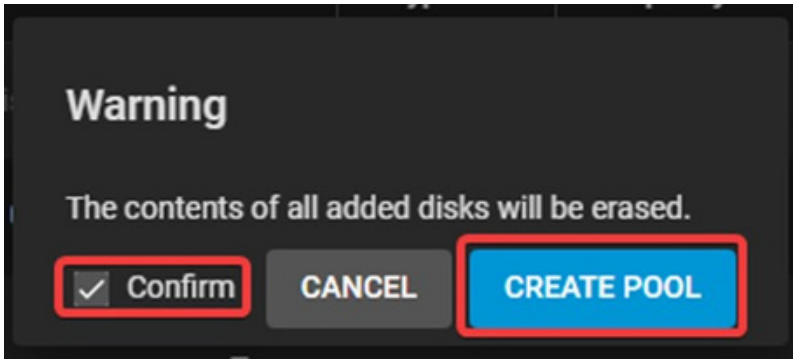
Ensuite ici je sélectionne mon disque dur précédemment ajouté a mon serveur NAS auparavant



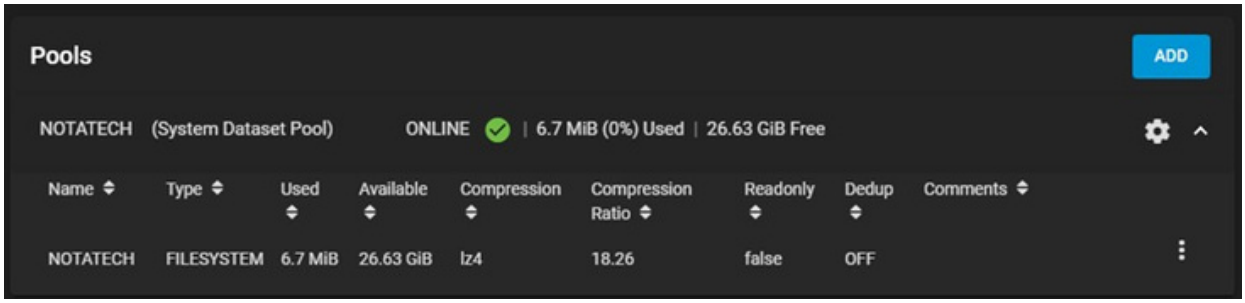
Puis finalement ici un message d'avertissement nous indique que la configuration peut présenter des risques car je n'ai pas configurer de RAID pour le moment mais la configuration fera l'affaire pour le moment, je clique donc sur **« Force »** puis **CREATE**



Je valide finalement cette dernière fenêtre et finit par cliquer sur **« CREATE POOL »**

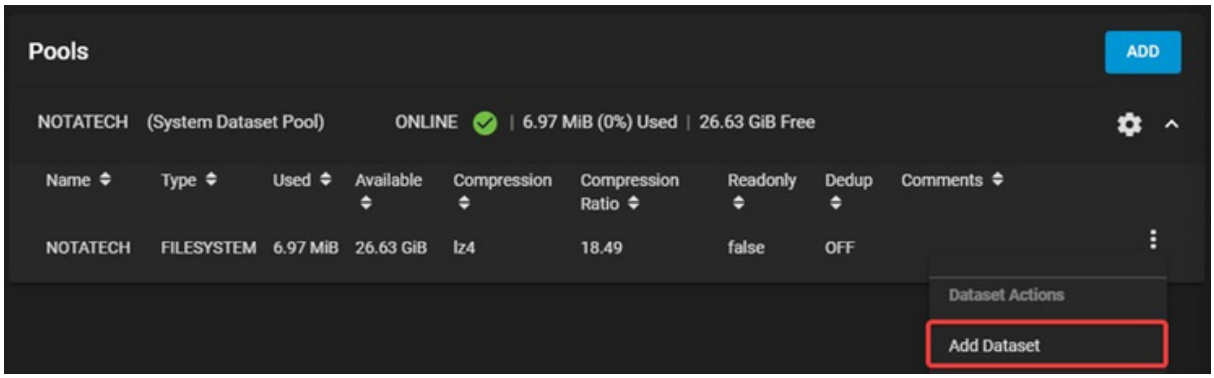


On peut donc finalement voir notre pool de stockage créé et qu'il est bien en ligne !

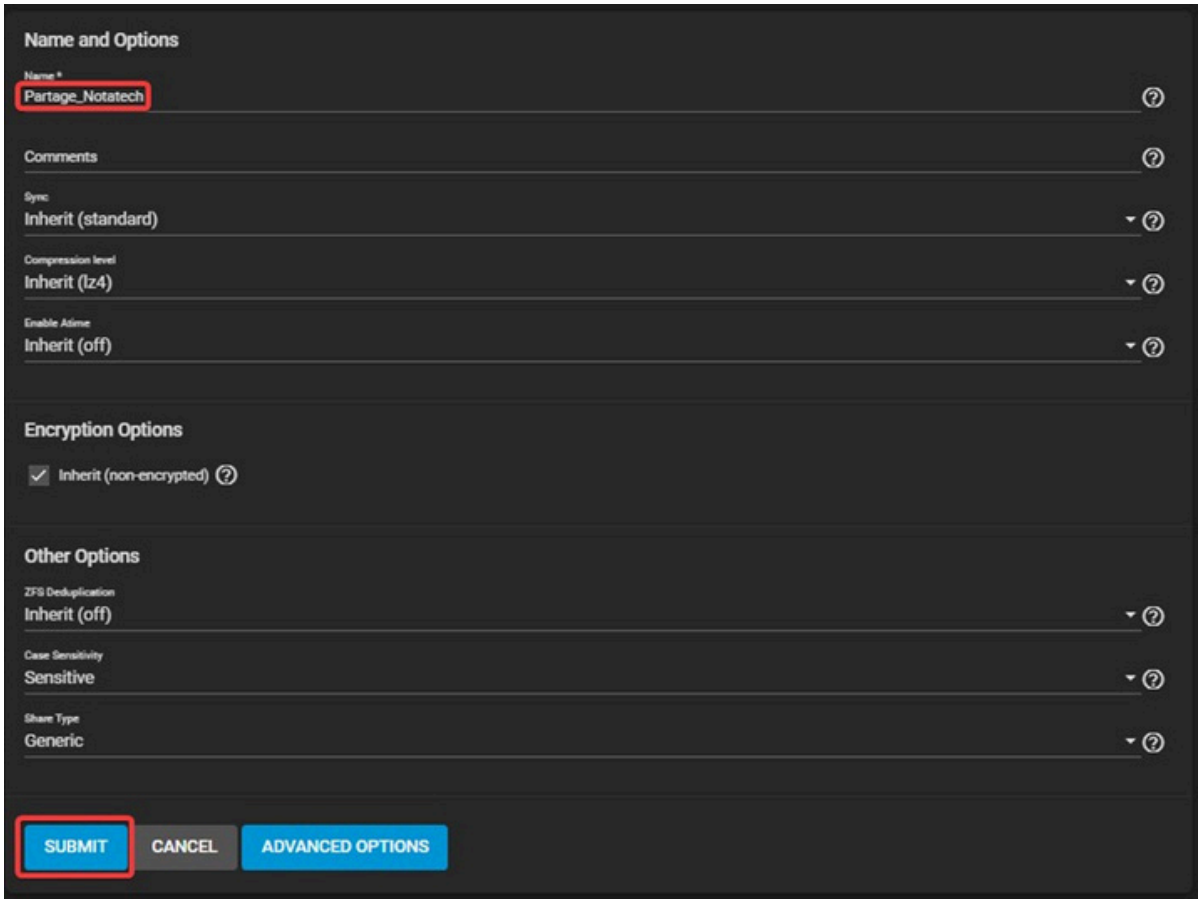


Ensuite pour continuer je dois créer un **dataset**, ce qui me permettra d'éditer les permissions de celui-ci et de partager le disque a tous les employés.

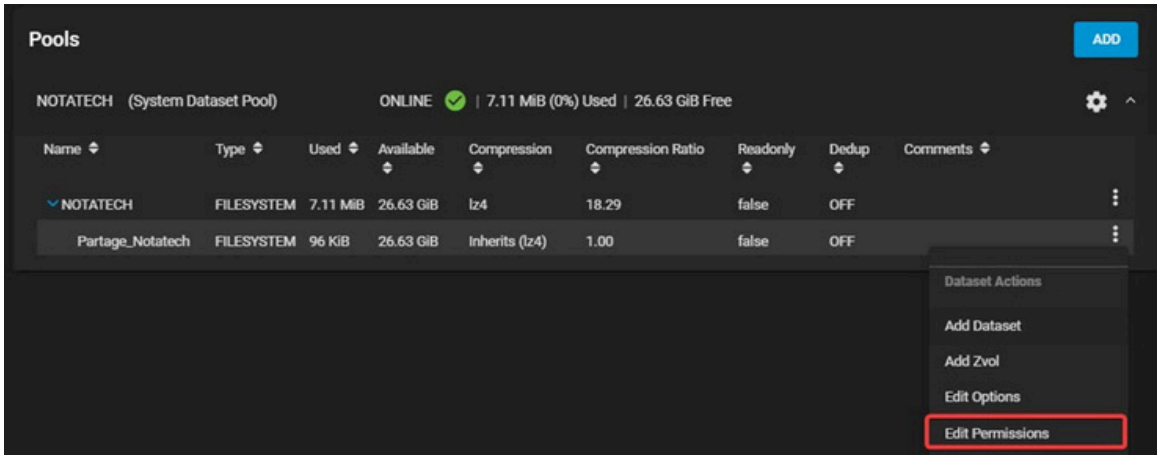
Pour ce faire je clique donc tout d'abord sur **« Add Dataset »** sur mon pool de stockage



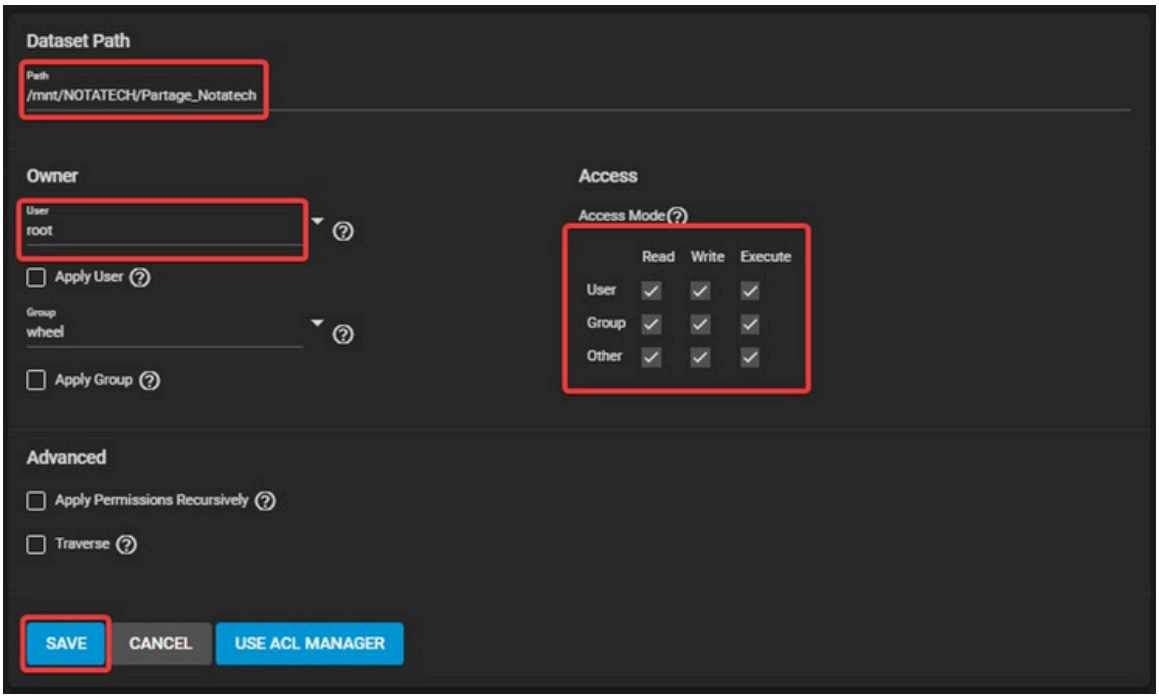
Ensuite cette page apparait, je saisis **« Partage_Notatech »** pour le nom du dataset (cela correspond au nom que les utilisateurs verront apparaitre) je laisse les autres options par défaut et clique sur **« Submit »**



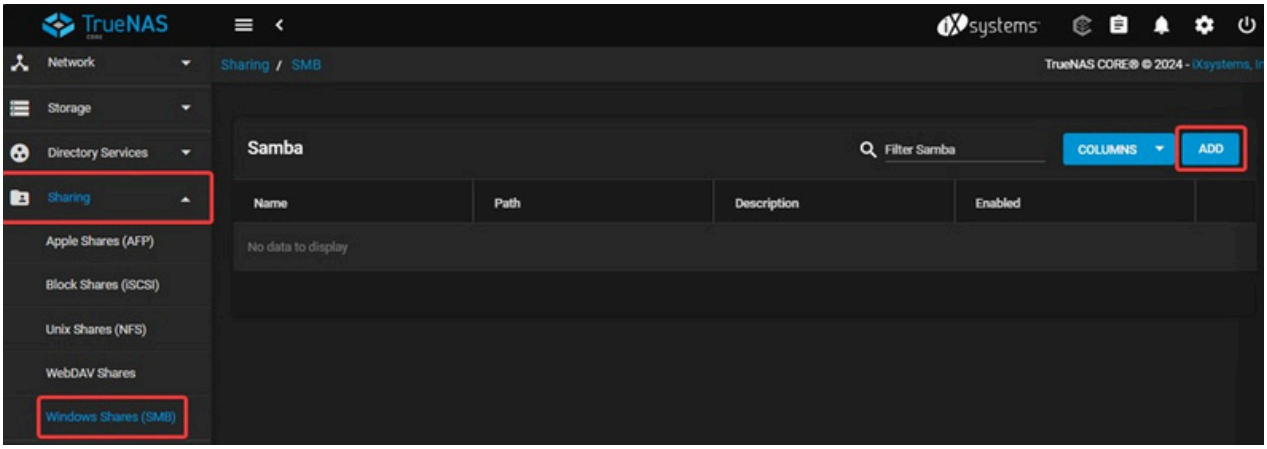
Ensuite sur ce nouveau dataset que je viens de créer je sélectionne **« Edit permissions »**



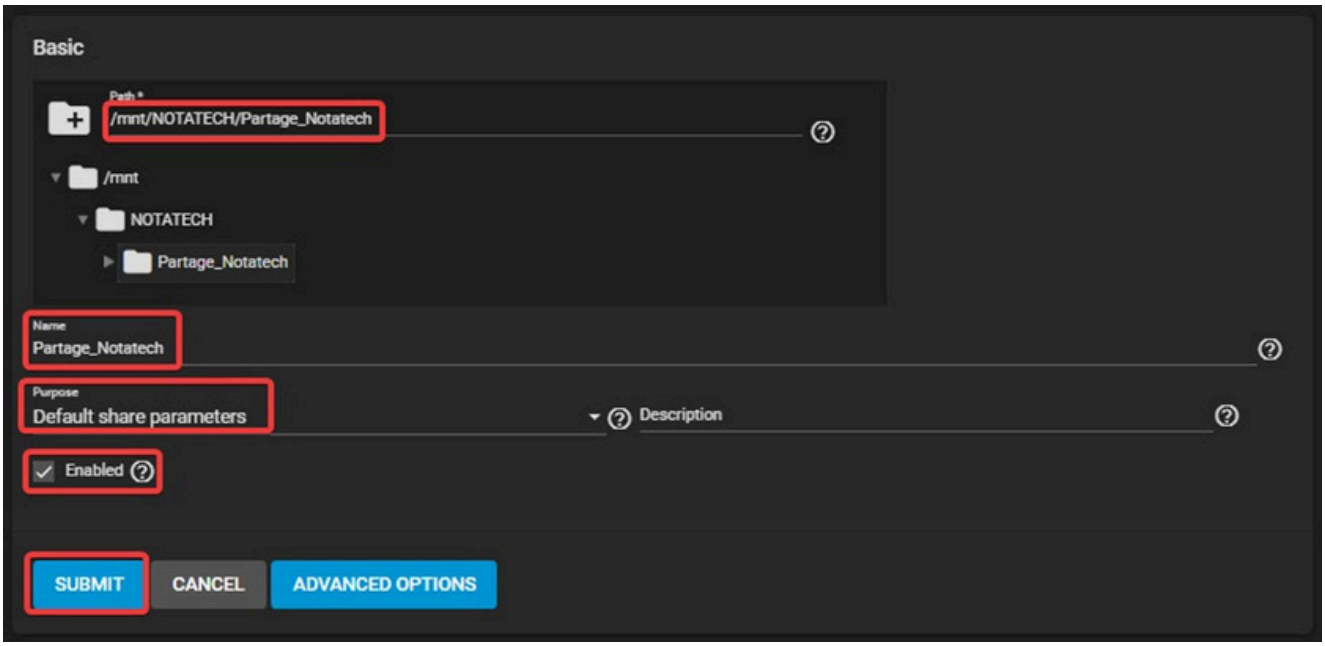
Dans la fenêtre qui s'ouvre on peut voir apparaitre le chemin de notre Dataset, et les permissions, on changera tout ça plus tard quand on aura lié notre serveur NAS a notre Active Diretory



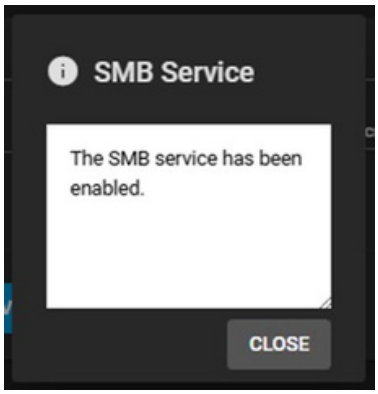
Ensuite je vais devoir activer le SMB afin que le partage de fichiers windows se fasse bien, je me rends donc dans la section **Sharing puis** dans **Windows Shares SMB** et clique sur **Add**



Ensuite ici je sélectionne donc le chemin jusqu'à mon dataset, ce sera le chemin à utiliser pour accéder au dataset depuis un poste, Saisis le nom, coche **Enabled** et valide.

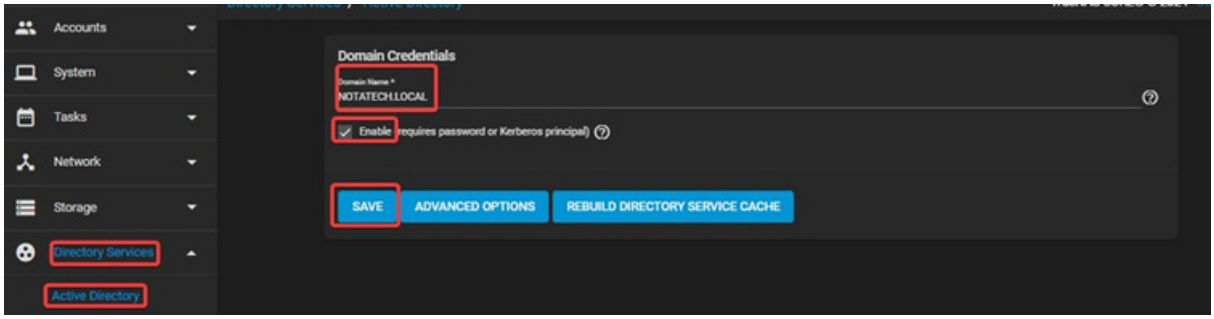


On aura ensuite ce message qui nous valide que le service SMB a bien été activé

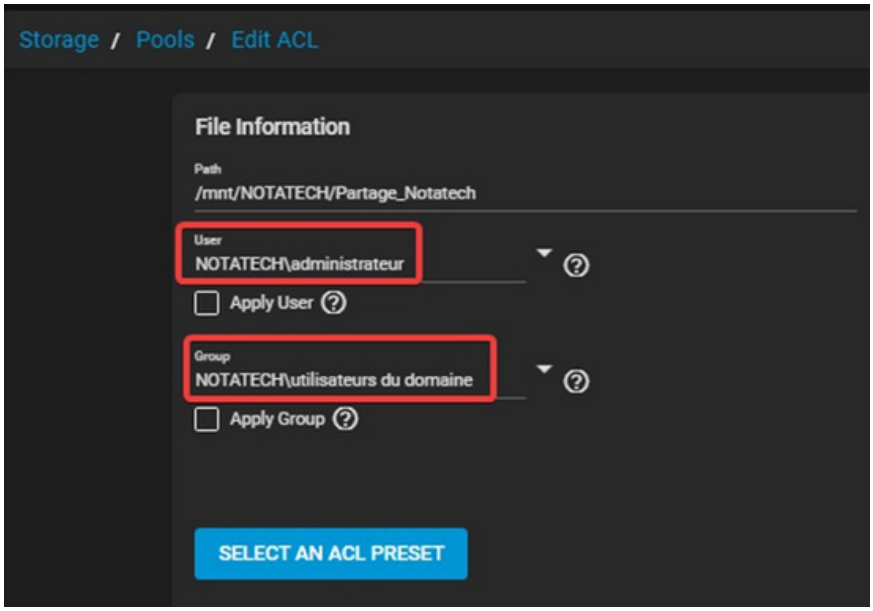


Ensuite je vais devoir lier mon serveur NAS a mon Active directory, pour personnaliser les autorisations selon les utilisateurs du domaines, etc…

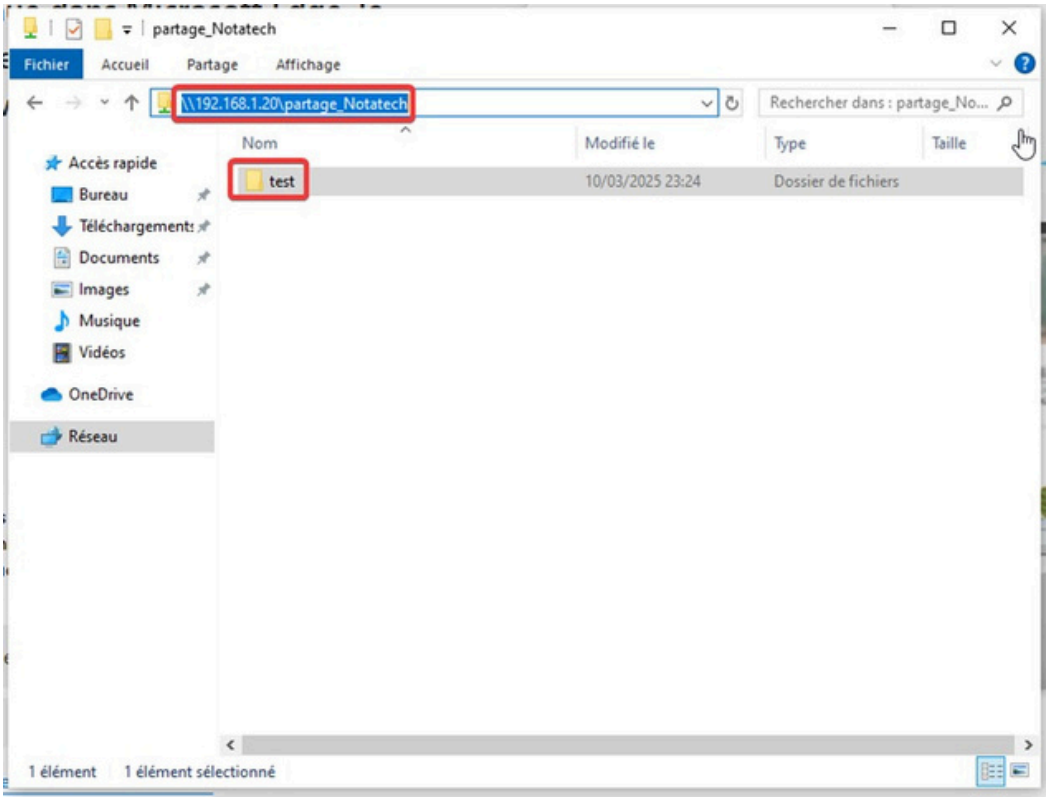
Je me rends donc dans la section **Directory Services/Active Directory**, saisi le nom de mon domaine, saisi mes identifiants administrateur du domaine, coche **Enable** et sauvegarde les changements



Finalement je retourne dans l'éditeur de permission de mon pool de stockage, change l'administrateur par l'administrateur de mon domaine et rend mon pool accessible par tous les utilisateurs étant comme **Utilisateurs du domaine** par mon Active Directory



Pour terminer je fais donc un test sur une machine cliente, l'utilisateur D Marshall, on peut voir que notre Partage_Notatech est donc maintenant bien accessible et qu'on peut lire et écrire dessus avec le dossier test que je viens de créer

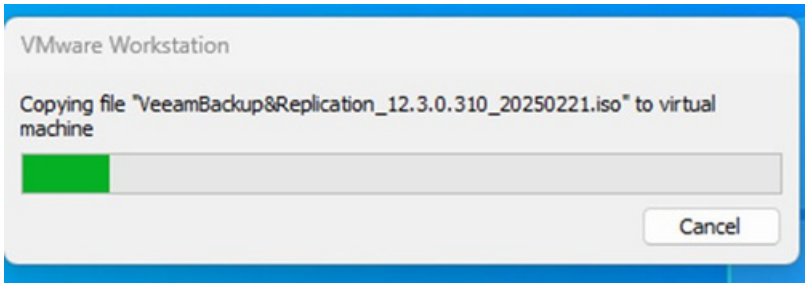


Notre Dataset est donc bien accessible par les employés et notre serveur de partage de fichiers et donc bien fonctionnel !

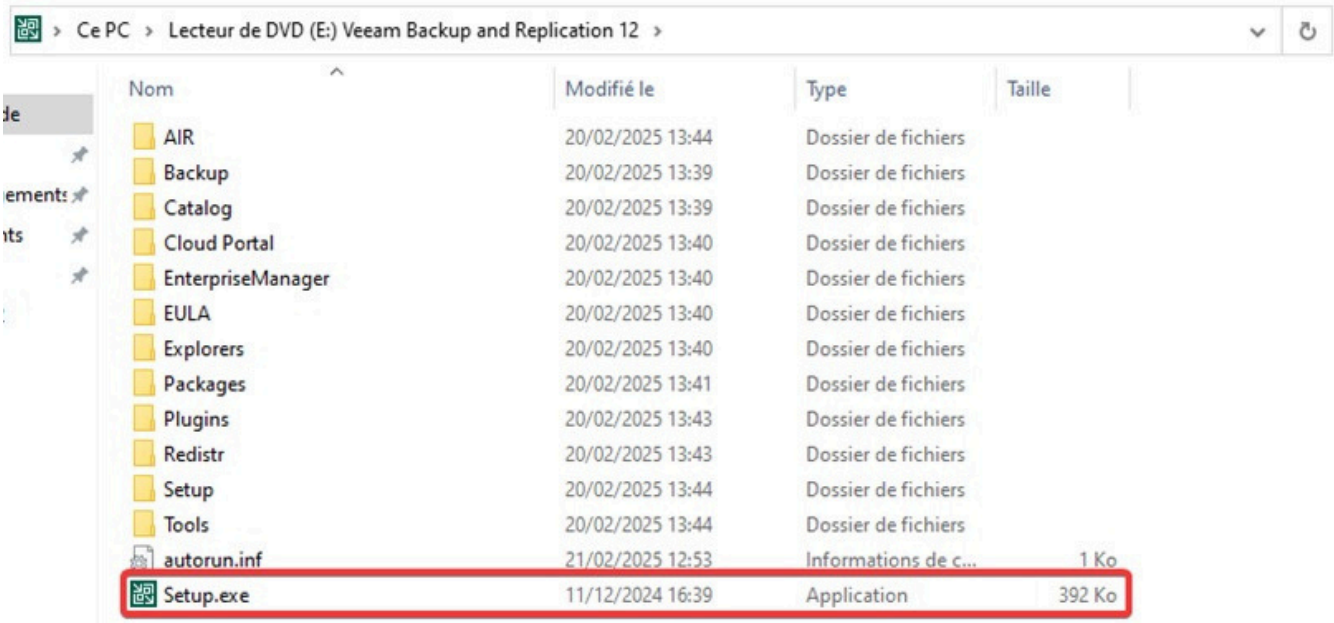
Création de la machine virtuelle VEAM BACKUP pour la récupération de données :

Ici, je vais vous montrer comment j'ai configuré le serveur Veeam Backup & Replication, utilisé pour réaliser des sauvegardes régulières des données critiques de l'infrastructure et garantir une restauration rapide en cas de panne ou sinistre.

Pour ce faire je commence par transférer l'iso de VEEAM sur mon serveur de production

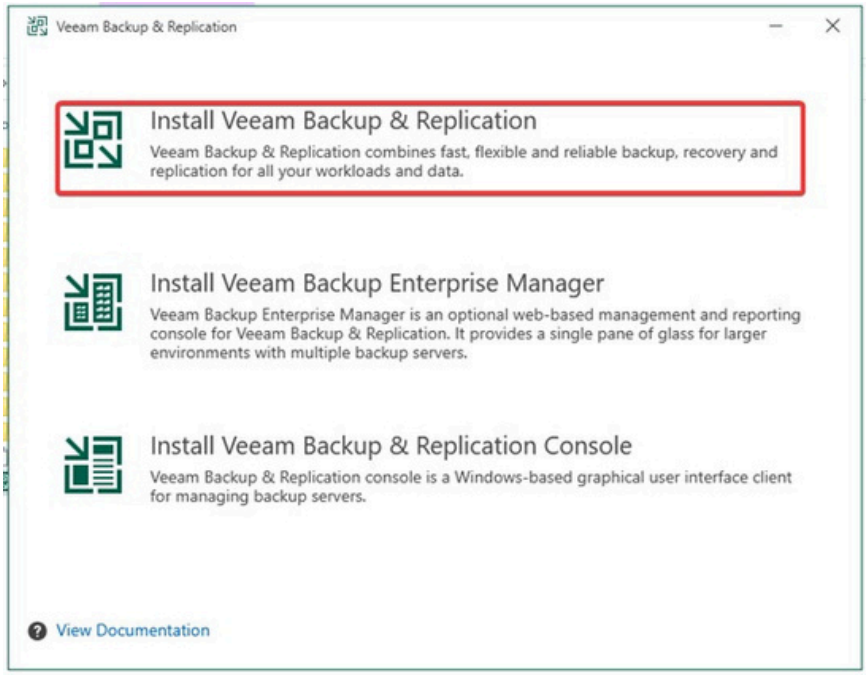


Ensuite dans l'iso de veam une fois celui-ci monté sur le serveur, je clique sur le **Setup.exe** pour démarrer l'installation

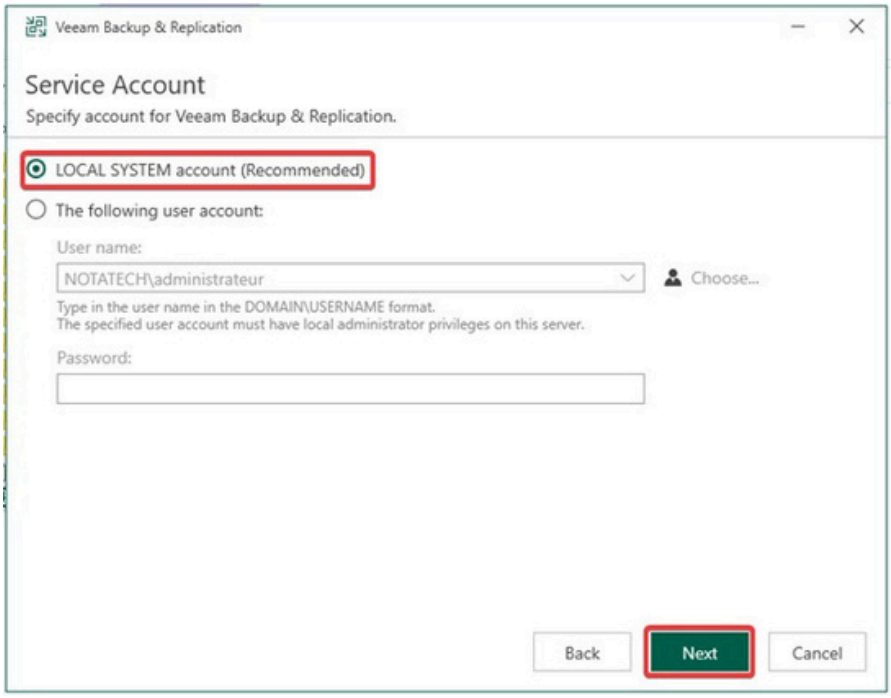


Ensuite cette fenêtre apparait je clique sur **Install**

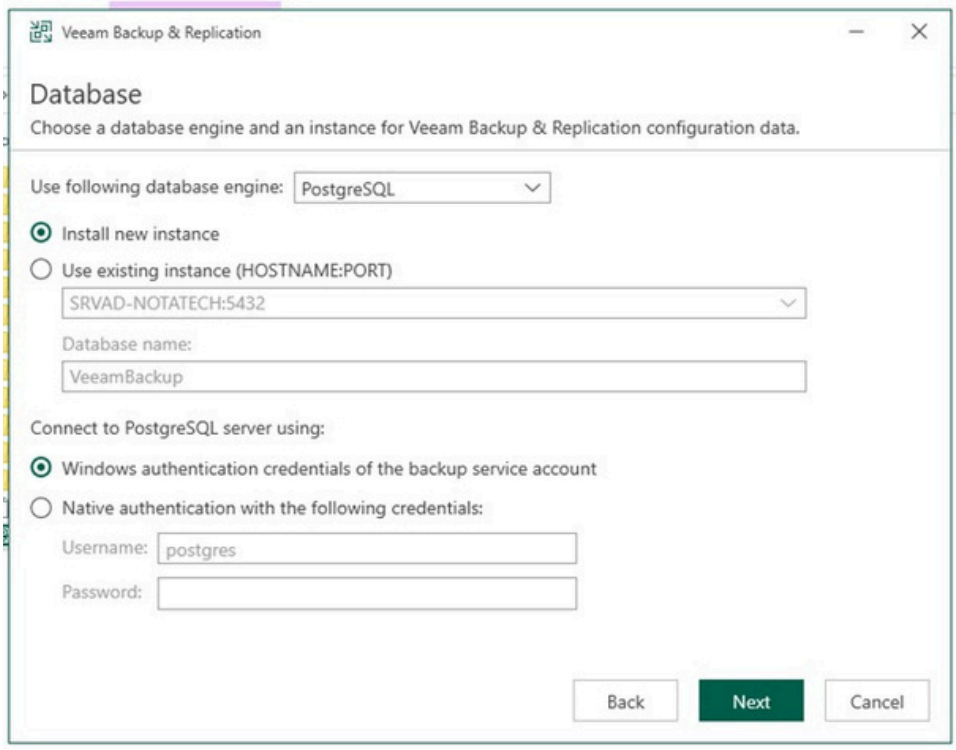
Ici je sélectionne la première option d'installation



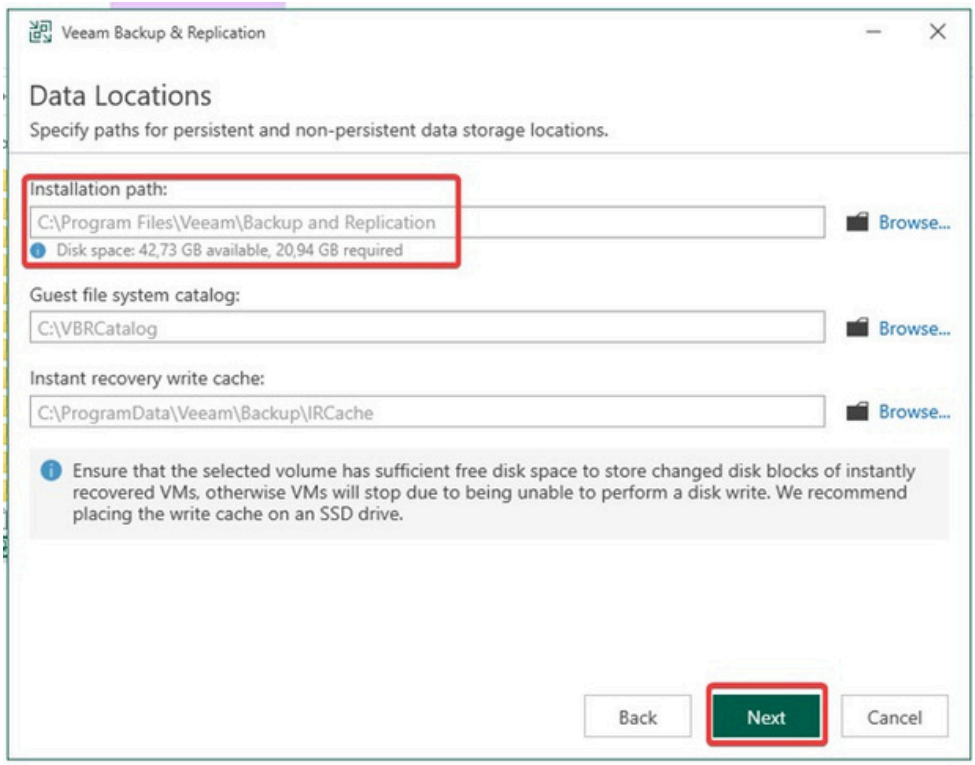
Ici je laisse les paramètres par défaut



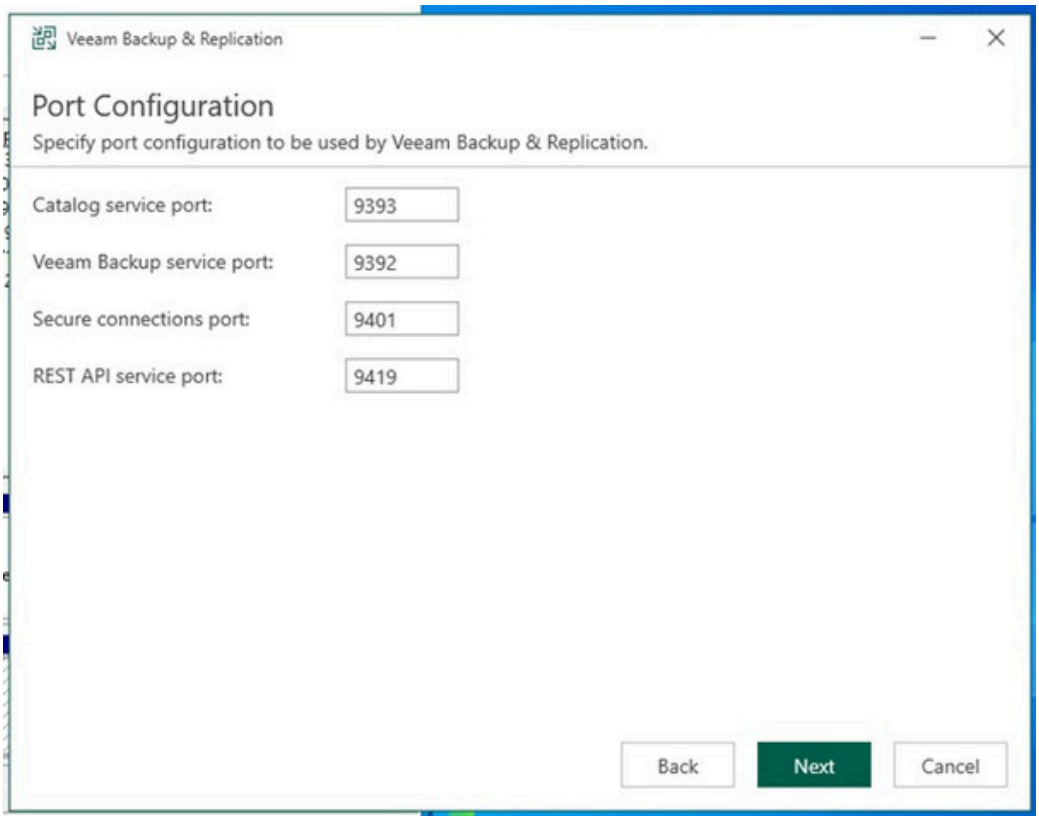
Ici aussi les paramètres par défaut sont ce qui conviennent le mieux a ma configuration



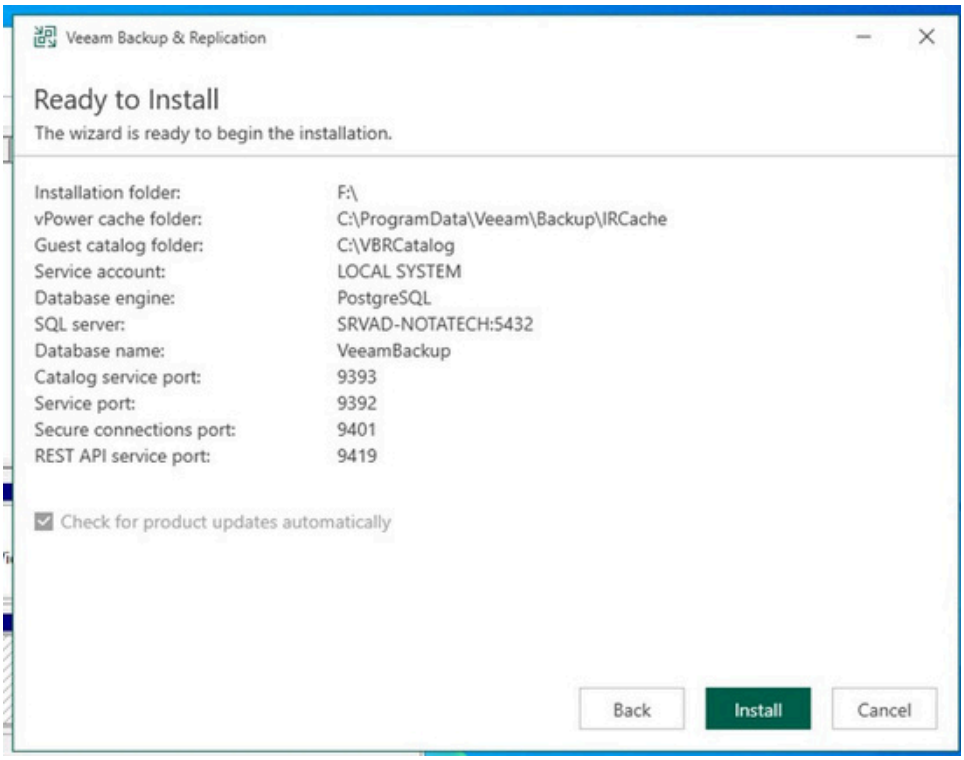
Ici je sélectionne le chemin d'installation pour VEEAM et clique sur **Next**



Ici VEEAM nous propose de changer la configuration des ports, je n'ai pas besoin de les changer je laisse donc par défaut et clique sur **Next**



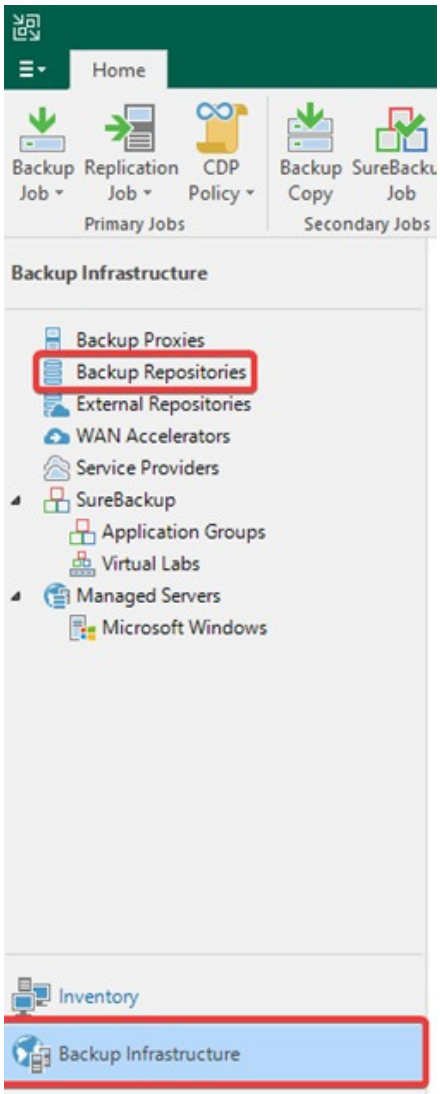
Et finalement je lance l’installation en cliquant sur **Install**



Configuration du backup repositories :

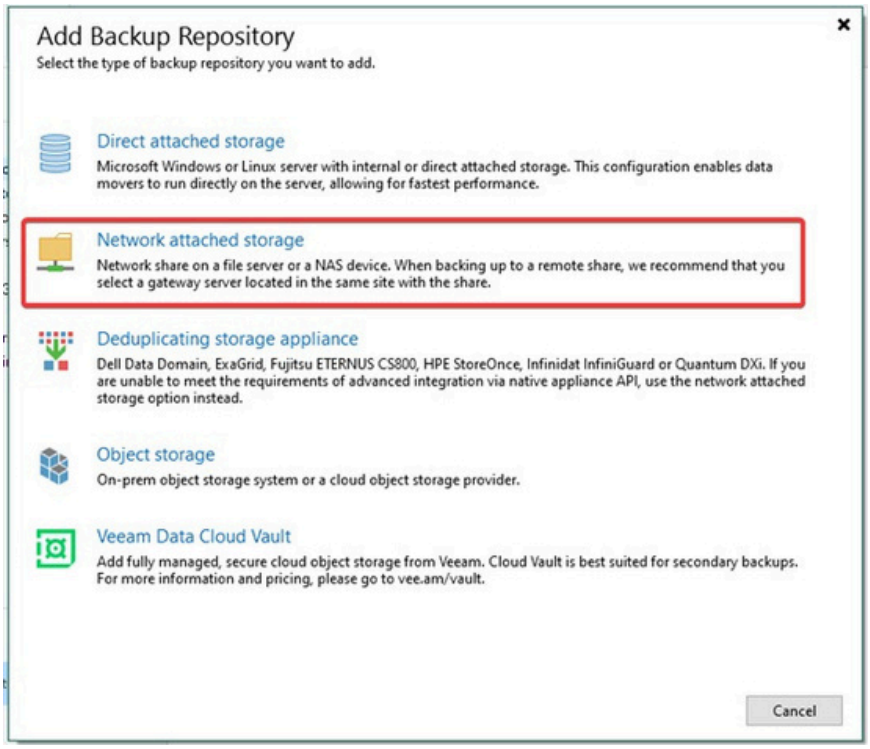
Maintenant que VEEAM est prêt à être utilisé, la première chose a faire est de créer un backup repository, cela permettra de renseigner a VEEAM le chemin vers le dossier partagé « Partage_Notatech » et de pouvoir ensuite en faire une backup

Pour ce faire je commence par me rendre dans la section **Backup repositories** sur l'accueil de VEEAM BACKUP

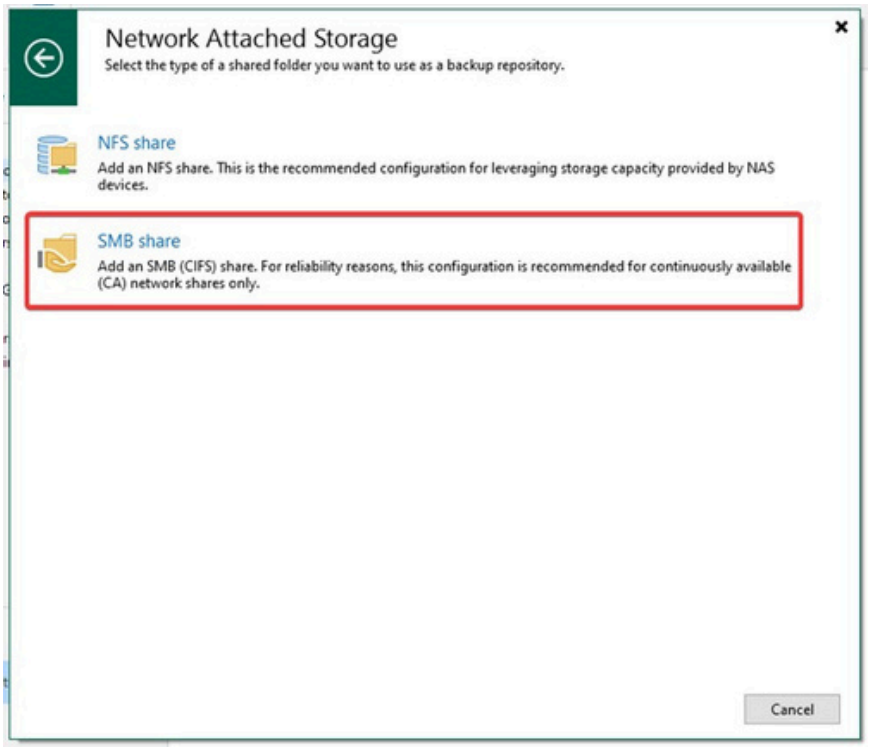


Et je fais ensuite un clique droit et clique sur **« Add backup repository »**

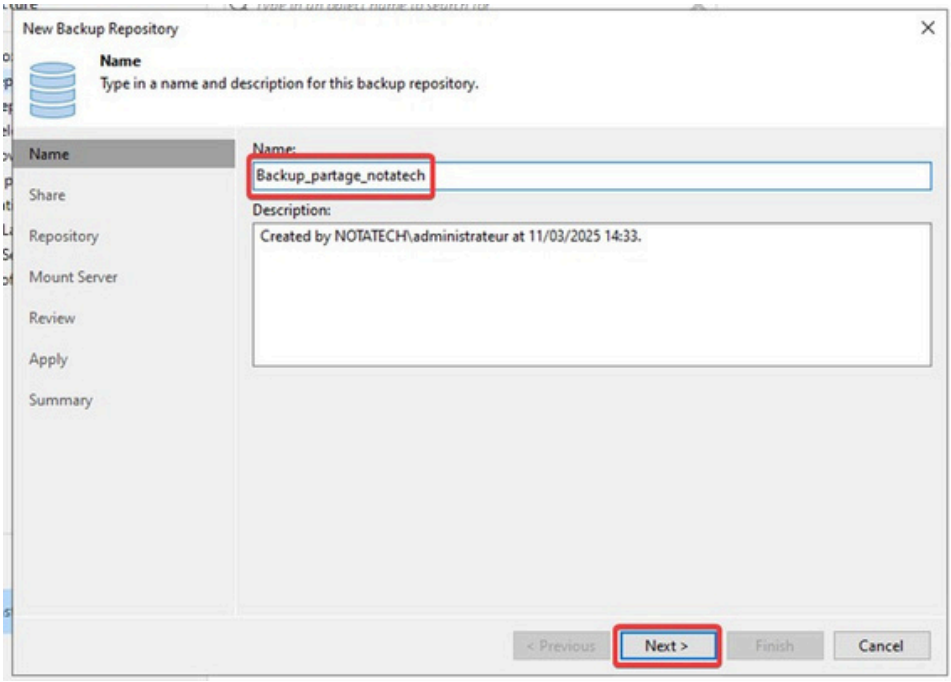
Ensuite cette page apparait, dans celle-ci je sélectionne **« Network attached storage »**



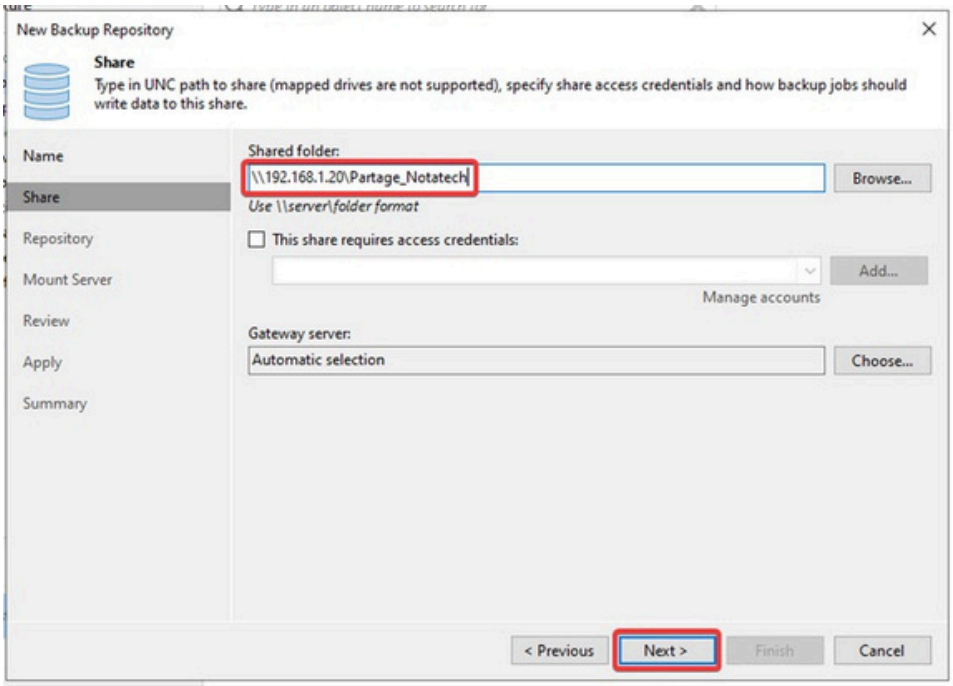
Ensuite pour le mode de partage je sélectionne **« SMB share »** car nous l'avons configuré précédemment sur notre serveur truenas



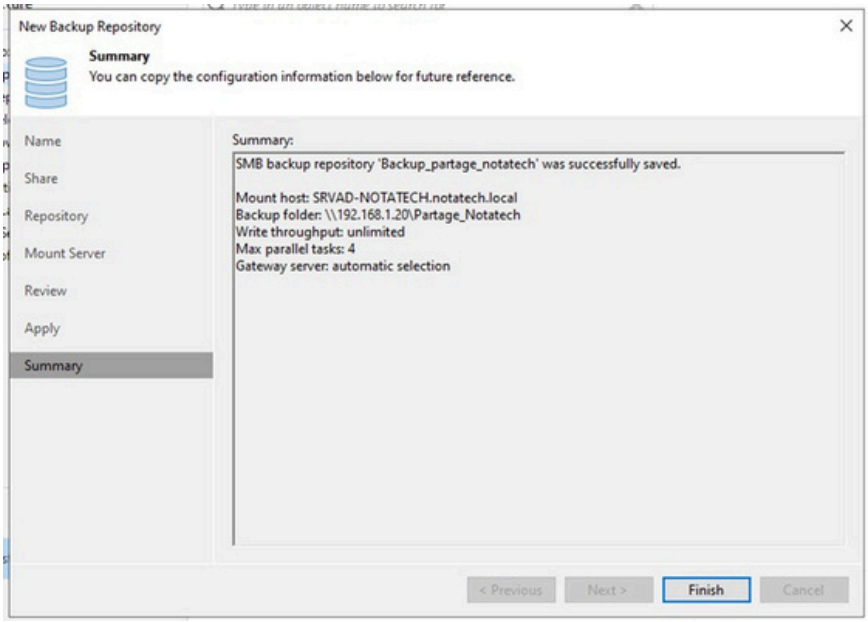
Ensuite pour le nom de mon Backup Repository je saisi
« Backup_partage_notatech » et clique sur **Next**



Ensuite a la section **Share** je saisi le chemin de mon fichier partagé que je veux pouvoir restaurer en l'occurrence **Partage_Notatech**



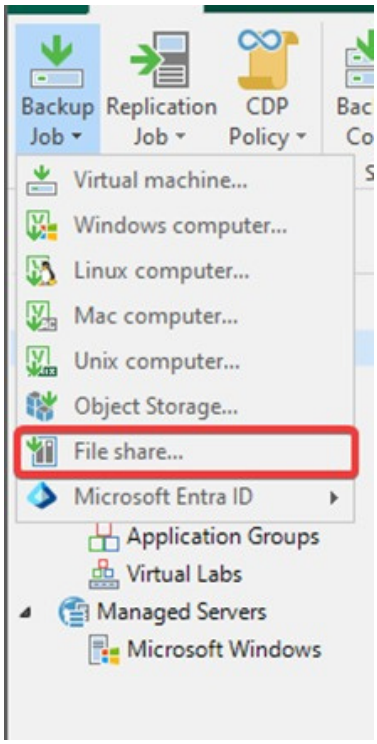
Pour le reste des sections je laisse les paramètres par défaut, cette page apparait nous faisant le récapitulatif de toute la configuration. Je valide en cliquant sur **Finish**



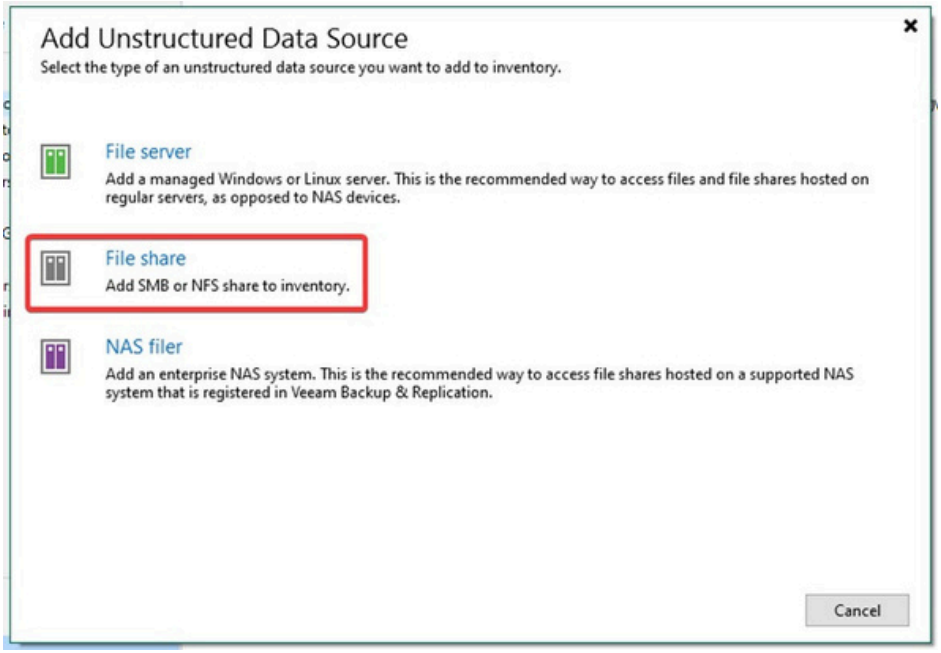
Configuration du backup jobs :

Maintenant que mon backup repository est configuré, je dois créer un backup job. Cette tâche s'exécutera automatiquement aux intervalles définis et assurera la sauvegarde régulière des données. Elle permettra, en cas de besoin, de restaurer les fichiers stockés dans Partage_Notatech, garantissant ainsi la sécurité et l'intégrité des données.

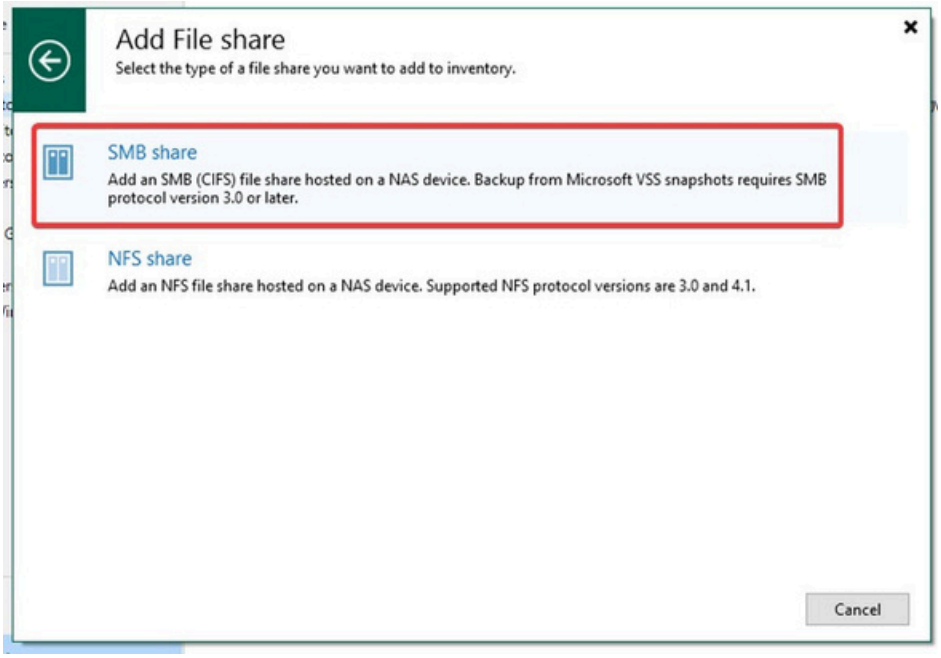
Pour ce faire je me rends donc dans **Backup job** et clique sur **File share**



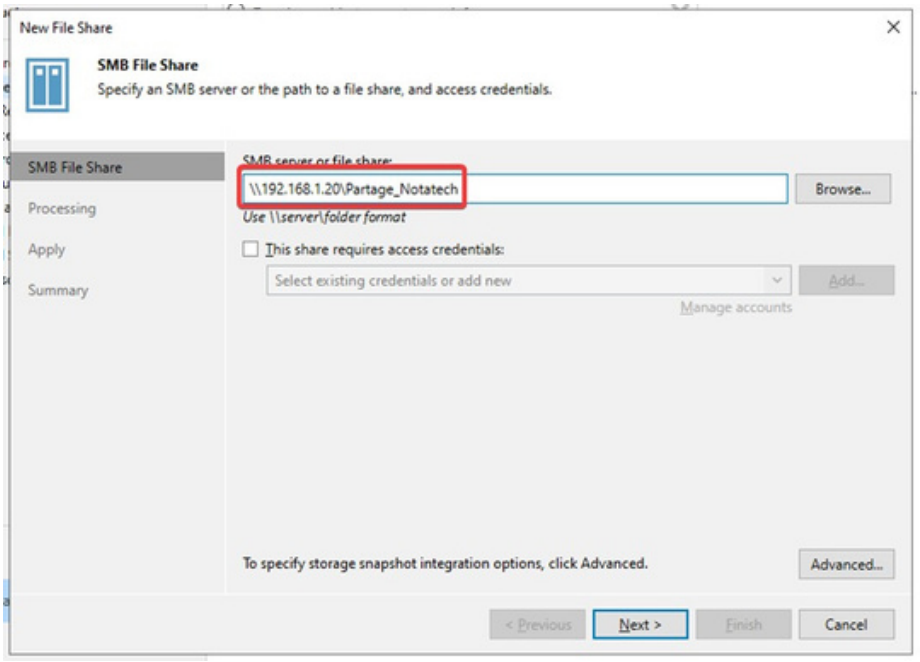
Ensuite ici je sélectionne **File share**



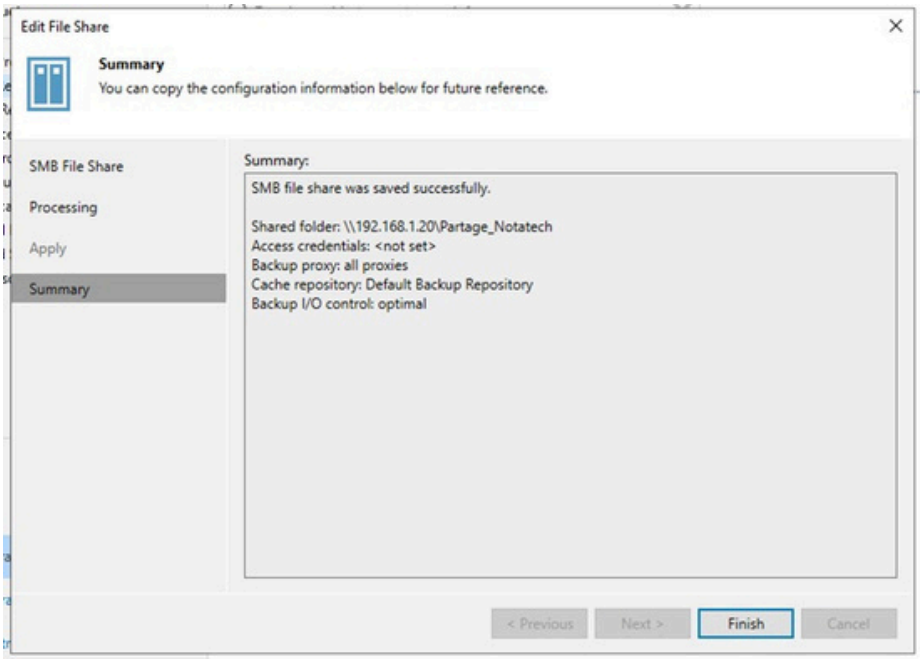
Ensuite ici je sélectionne **SMB share** car ceci correspond au partage qu'on a configuré précedemment



Ensuite ici je saisi le chemin jusqu'à mon dossier **Partage_Notatech** et clique sur **Next**

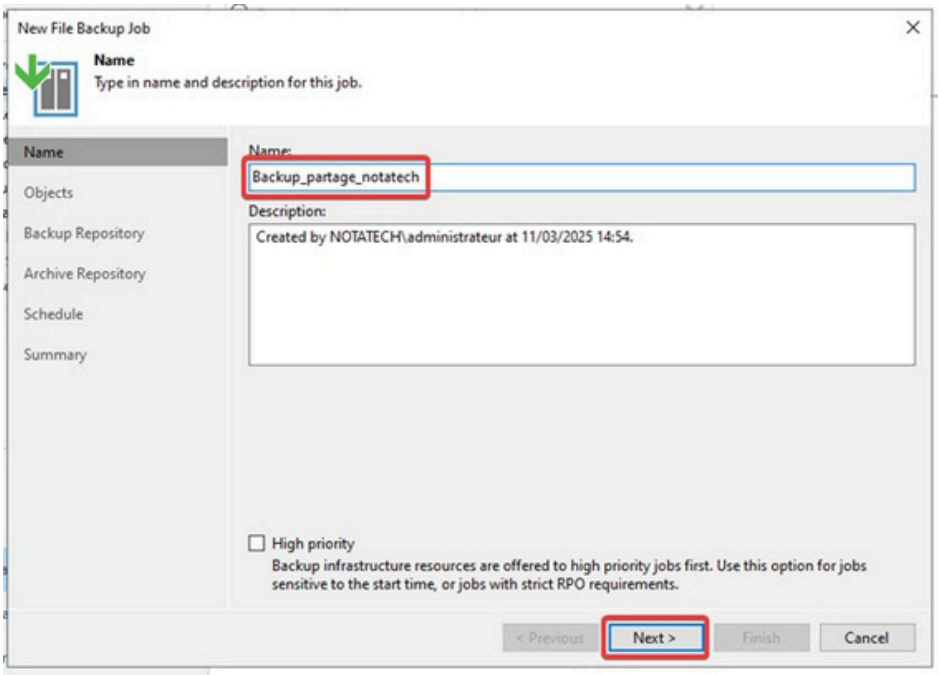


Ensuite pour le reste des paramètres je laisse par défaut et valide en cliquant sur **Finish**

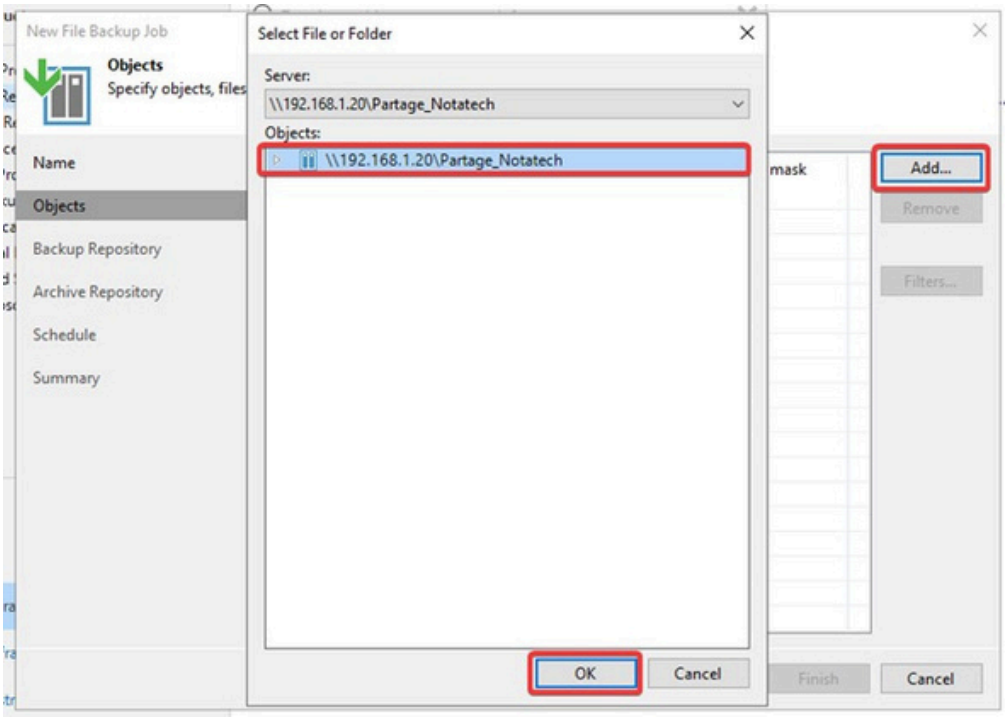


Pour poursuivre la configuration de cette tâche, je me rends dans Backup Jobs, puis dans File Share, comme précédemment. Cela permettra de sélectionner le backup repository précédemment configuré et de définir les intervalles de temps pour l'exécution automatique de la tâche de sauvegarde.

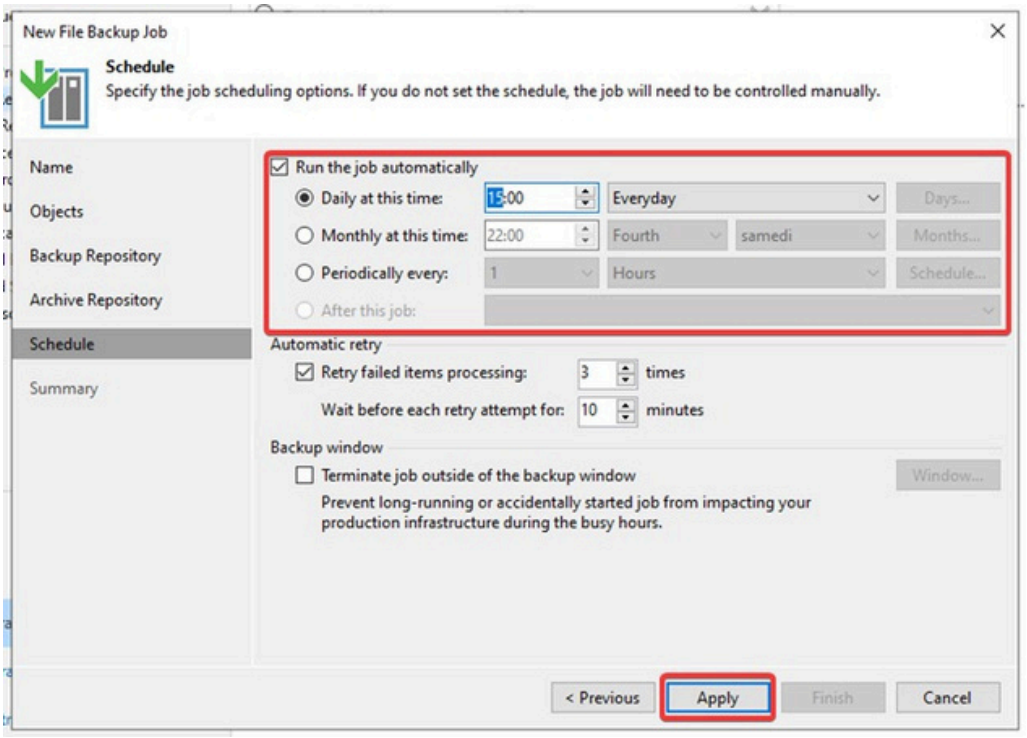
Dans cette section, je saisis le nom **"Backup_Partage_Notatech",** puis je clique sur Next pour passer à l'étape suivante.



Ensuite ici je sélectionne le chemin comme dans les étapes précédentes le chemin jusqu'à mon **Partage_Notatech**



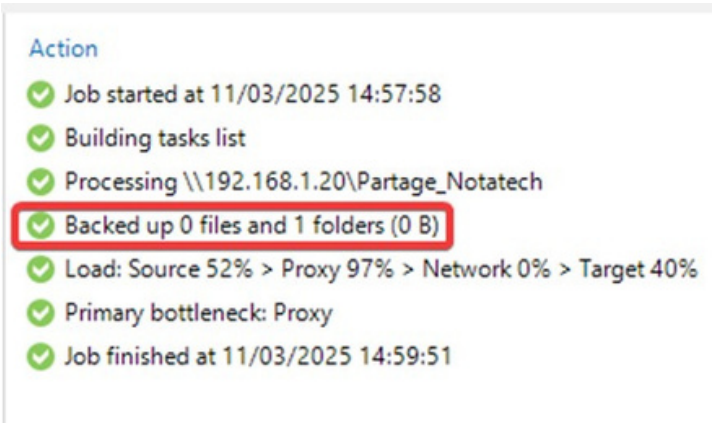
Je passe et laisse les paramètres par défaut jusqu'à la section **« Schedule »** ici cette section permet de définir les intervalles ou exécuter la tâche, je sélectionne **Run the job automatically** et change les paramètres pour que la tâche s'exécute tous les jours a 15 heures



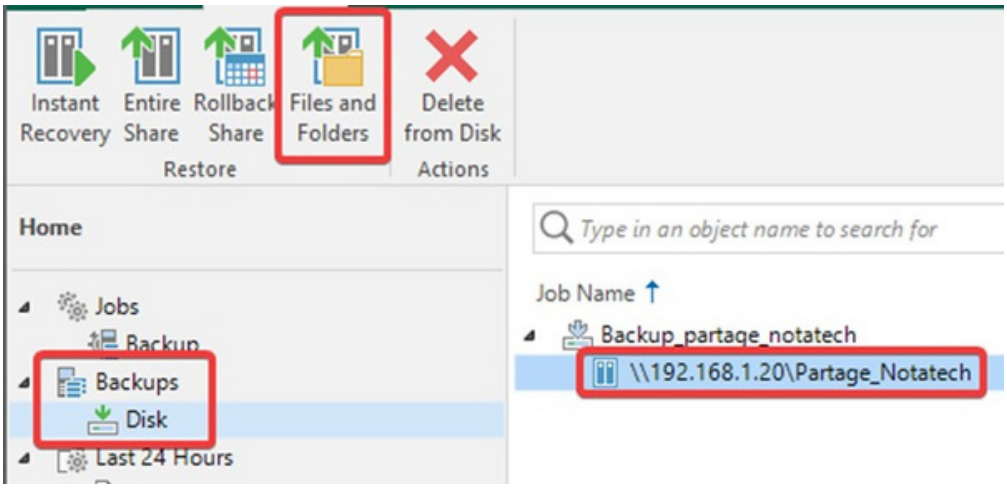
Test de restauration :

Maintenant notre restauration est au point, je fais donc un test pour vérifier son bon fonctionnement.

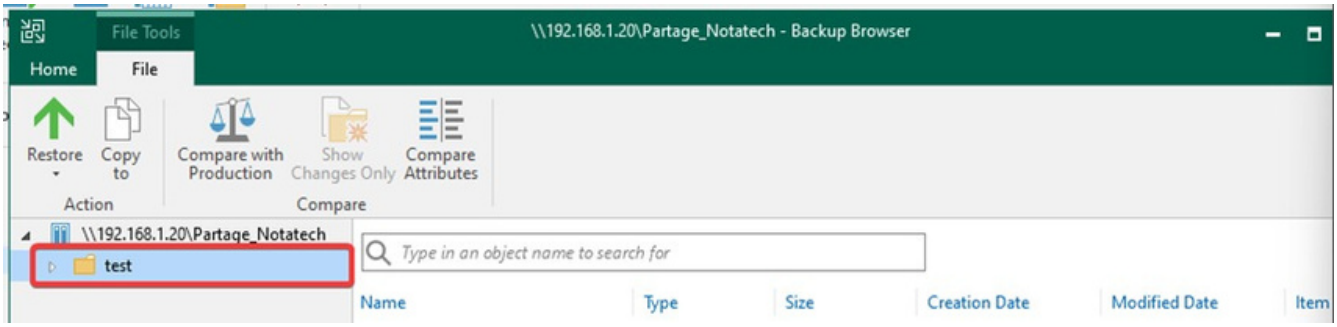
Pour ce faire déjà dans les taches exécutées je vois que la tâche s'est bien exécutée et a bien backup un dossier, le dossier partagé ne contient qu'un fichier « test » comme je l'ai montré précédemment



Ensuite pour récupérer le backup du dossier je me rends dans **Backups** clique sur mon dossier partagé configuré, et clique finalement sur **Files and Folders**



Et je vois bien mon fichier et peux le restaurer ce qui signifie que la restauration de fichiers est bien fonctionnelle !

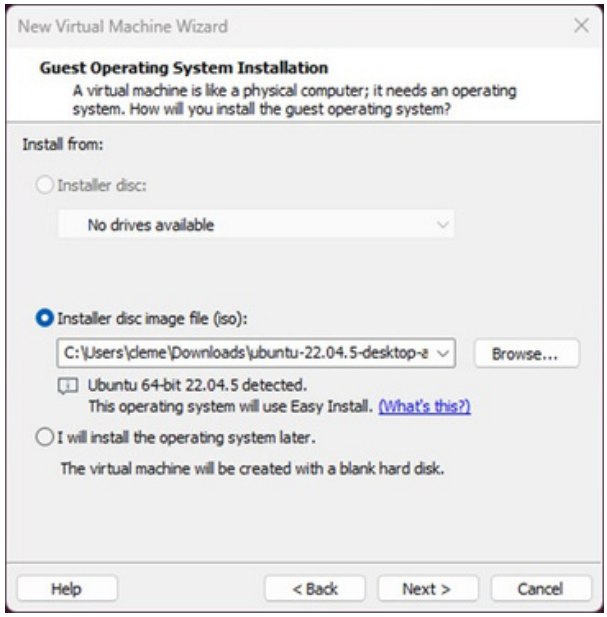


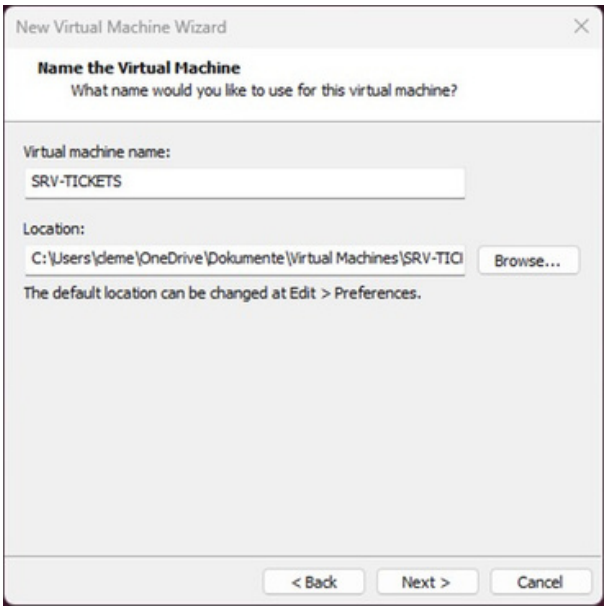
Création et configuration d'un serveur GLPI :

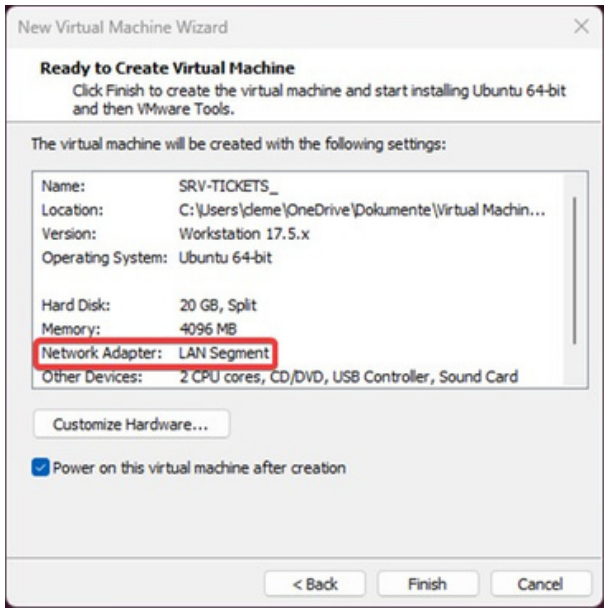
Dans cette partie, je vais expliquer comment j'ai installé et configuré un serveur GLPI. Ce serveur permettra aux employés de soumettre des tickets à l'administrateur réseau lorsqu'ils rencontrent un problème informatique, facilitant ainsi la gestion et le suivi des demandes de support.

Installation du serveur GLPI : Dans cette étape nous allons créer une nouvelle machine virtuelle sous Ubuntu pour y installer le serveur GLPI

Pour ce faire, je réalise ces étapes : je créer une nouvelle machine en sélectionnant **Typical**, je sélectionne l'**ISO** de mon **OS** Ubuntu, je nomme mon serveur **SRV-TICKETS** et très important je mets ma machine dans le LAN segment **Notatech**







Une fois la machine lancée et le système bien installé je commence par ouvrir un terminal et je fais cette commande. Cette commande permet d'installer tous les composants d'un serveur LAMP nécessaire a GLPI.

je fais donc cette première commande :

```
sudo apt install apache2 php php-cli php-mysql php-xml php-mbstring php-curl php-zip

php-bz2 php-soap php-intl
```

Ensuite je fais ces commandes qui me permettent d'installer les paquets de Mysql :

```
sudo apt install mysql-server
sudo apt-get install mysql-server
```

Ensuite je rentre cette commande dans le terminal. Cette commande va nous installer toutes les extensions nécessaires a GLPI des paquets qu'on vient juste d'installer, j'execute cette commande dans le répertoire /var/www :

```
sudo wget https://github.com/glpi-project/glpi/releases/download/10.0.16/glpi
```

Une fois ceci fait je fais cette commande pour extraire le fichier de glpi que nous venons d'installer :

```
sudo tar -xvzf glpi-10.0.16.tgz
```

Après cela je fais ces commandes pour attribuer les permissions nécessaires a Apache2 :

```
sudo chown -R www-data:www-data /var/www/glpi
sudo chmod -R 755 /var/www/glpi
```

Ensuite je fais cette commande pour me mettre en mode root mysql :

```
sudo mysql -u root -p
```

Maintenant que je suis en mode root je fais ces requêtes dans MySql pour créer ma base de données et un utilisateur pour glpi :

```
CREATE DATABASE glpi CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode-ci
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'Root123';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Ensuite je fais cette commande. Cette commande va installer l'extension **LDAP** de php, ce qui nous permettra par la suite de relier notre GLPI a notre annuaire **Active Directory**

```
sudo apt-get install php-ldap
```

Suite a ça je vais devoir créer un fichier de configuration pour apache2, je fais donc cette première commande pour créer le fichier :

```
sudo nano /etc/apache2/sites-available/glpi.conf
```

Dans ce fichier de configuration je met ces lignes :

```
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/glpi
ServerName notatech.local
  <Directory /var/www/glpi>
  Options FollowSymLinks
  AllowOverride All Require
  all granted
  </Directory>
   ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog${APACHE_LOG_DIR}/access.log combined
 </Vir tualHost>
```

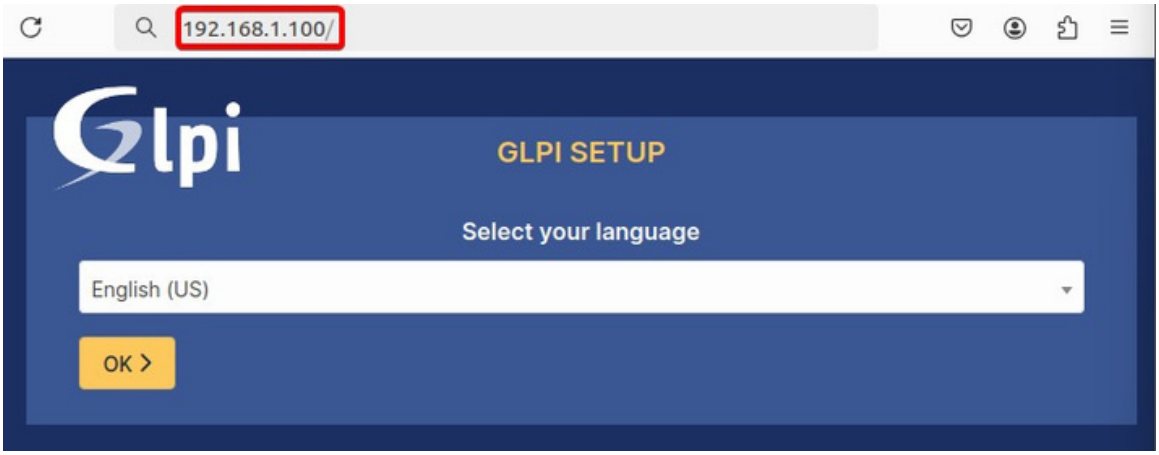
Ensuite je fais ces commandes, ces commandes me permettent d’activer le glpi et d’activer le module rewrite et finalement de redémarrer mon service apache2 :

```
sudo a2ensite glpi.conf
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Pour terminer je fais cette commande pour désactiver le site de base de Apache2 car il ne nous sert pas :

```
sudo a2dissite 000-default.conf
```

Maintenant que tout est terminé je rentre l'adresse IP de mon GLPI dans la barre de recherche :



La page de GLPI s'affiche bien donc la configuration est bonne ! nous pouvons passer a la suite !

Installation de GLPI :

Maintenant que mon serveur est fonctionnel et accessible nous allons le configurer depuis cette page web

Je commence donc par sélectionner ma langue donc **Français** et clique sur **OK**

Ici arrivé à la page du **Setup** je clique sur **Installer** car c'est la première fois que je l'installe sur cette machine

Ensuite cette page apparait, cette page vérifie si nous avons bien tous les prérequis nécessaires a GLPI et en suggère, dans mon cas nous pouvons voir que tous les prérequis sont respectés je peux donc continuer

Ensuite ici les identifiants pour se connecter a MySql sont demandés, ce sont les identifiants que nous avons configurés tout à l'heure avec l'utilisateur **glpi_adm**. Je rentre donc les identifiants et clique sur **Continuer**

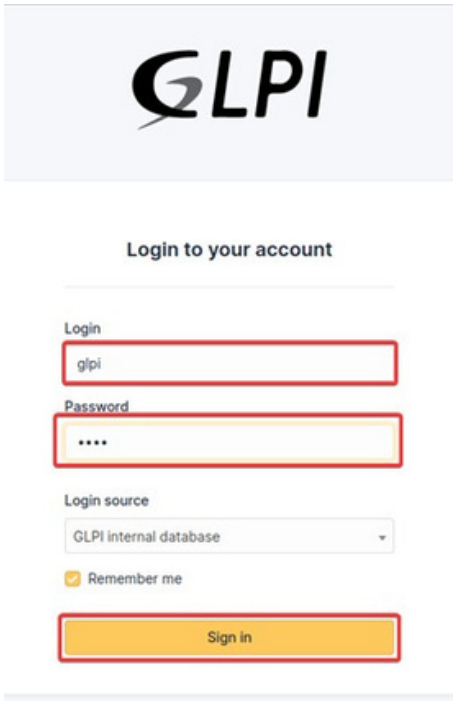
Ensuite ici je sélectionne la base de données créées toute a l'heure **db23_glpi** et clique sur **Continuer**

Ensuite l'initialisation se lance et on voit qu'elle s'est bien passée je peux donc **Continuer**

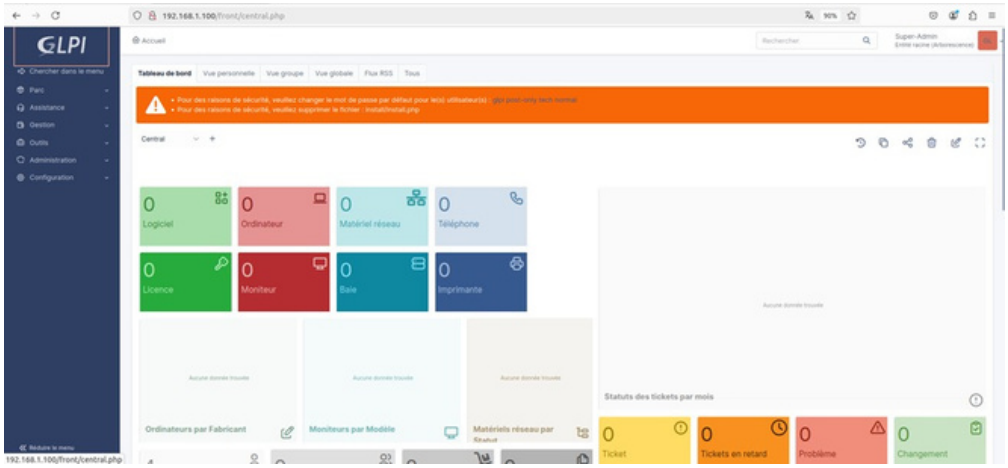
Les autres étapes concernent des acceptations de contrat de licence, etc... je passe donc ces étapes et arrivé à l'étape 6 GLPI nous indique que l'installation est terminée.

Nous pouvons donc normalement commencer à utiliser GLPI !

Je rentre donc les premiers identifiants de GLPI qui sont **glpi/glpi**



Le serveur est bien accessible et fonctionnel ! Nous pouvons maintenant passer à la suite !



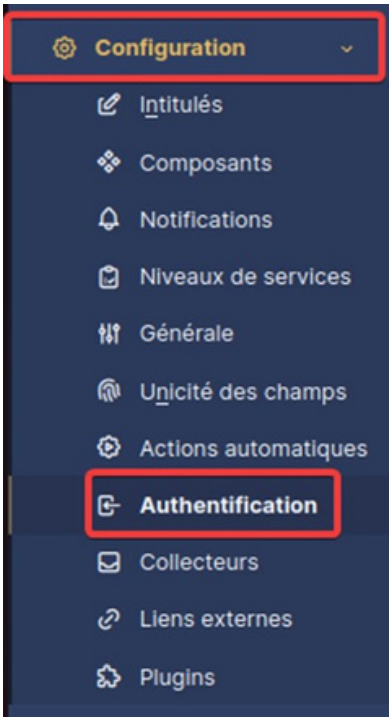
Liaison a lA'ctive Directory :

Maintenant pour plus de facilité nous allons lier notre GLPI a lA'ctive Directory de Notatech, ce qui permettra aux utilisateurs de lA'D de se connecter facilement et de pouvoir créer des tickets.

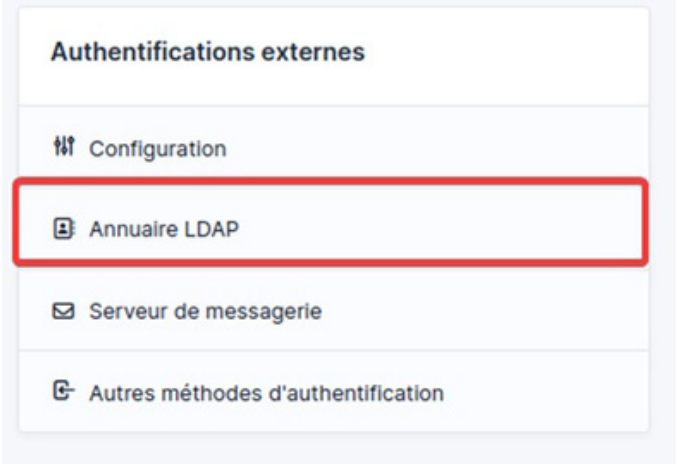
Je commence par faire un ping sur mon serveur GLPI jusqu'à mon serveur AD pour être sûr que la liaison soit bonne, on peut voir que le ping est OK je peux donc continuer

```
--- 192.168.1.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.324/4.845/13.195/4.546 ms
```

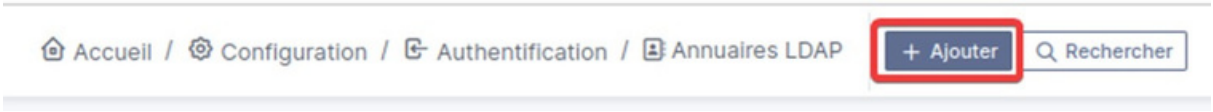
Ensuite sur mon GLPI je me rends dans la section **Configuration** puis je clique sur **Authentification**



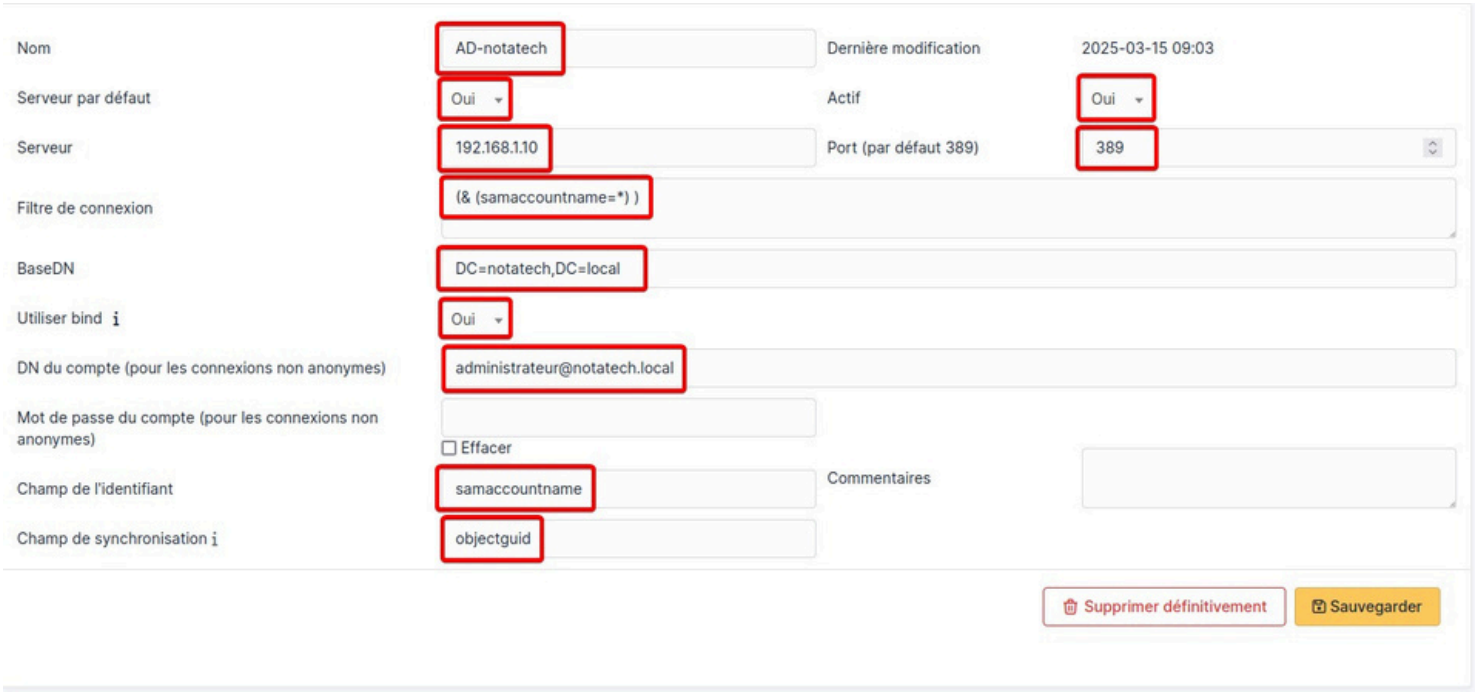
Ce qui m'amène sur cette page ou je sélectionne **Annuaire LDAP**



Ensuite je clique sur **Ajouter**



Nous allons étudier les différentes informations que j'ai rentrées ici…



Informations générales :

Nom : Nom donné à l'annuaire LDAP dans GLPI. Ici, **AD-Notatech** permet de l'identifier facilement.

Actif : Permet d'activer ou désactiver la connexion à l'annuaire. Doit être activé (Oui) pour fonctionner.

Paramètres du serveur LDAP :

Serveur : Adresse IP du serveur Active Directory, ici 192.168.1.10.

Port : 389 pour une connexion non sécurisée LDAP ou 636 pour une connexion chiffrée LDAPS.

Paramètres de recherche des utilisateurs :

Filtre de connexion : (& (samaccountname=*)), permet de rechercher les utilisateurs par leur nom d'utilisateur Windows.

BaseDN : DC=notatech,DC=local, indique à GLPI où chercher les utilisateurs dans l'Active Directory.

Informations d'authentification :

Utiliser bind : Oui, permet à GLPI de se connecter à l'A'D avec un compte spécifique.

DN du compte : CN=Administrateur@notatech.local, identifiant l'administrateur qui a le droit d'accéder à l'annuaire.

Mot de passe du compte : Mot de passe du compte Administrateur ou d'un compte de service dédié.

Champs d'identification et synchronisation :

Champ de l'identifiant : smaccountName, correspond au nom d'utilisateur Windows utilisé pour la connexion.

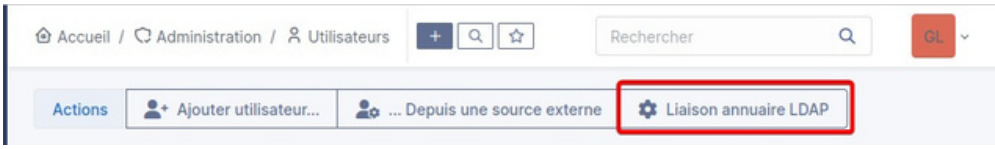
Champ de synchronisation : objectGUID, un identifiant unique propre à chaque utilisateur dans Active Directory.

Importation des utilisateurs Active Directory dans GLPI

Maintenant que notre annuaire LDAP a bien été synchronisé avec notre GLPI il faut importer les utilisateurs

Pour ce faire je commence par me rendre dans l'onglet administration puis utilisateurs

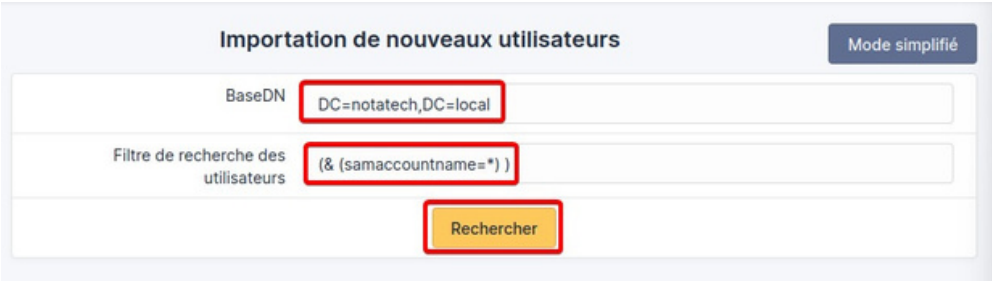
Ensuite sur cette page je clique sur **Liaison annuaire LDAP**



Je sélectionne ensuite **Importation de nouveaux utilisateurs**

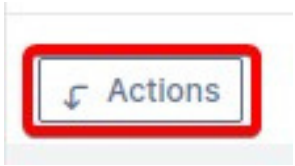
Ici je sélectionne **Mode expert** pour rechercher mes utilisateurs

Sur cette page pour la **BaseDN** ma base DN s'est prérentrée et mon filtre de recherche aussi je clique donc simplement sur **Rechercher**



On voit que les utilisateurs de mon Active Directory s'affichent bien ! je sélectionne donc mes utilisateurs

Après ça je clique sur **Actions**, je sélectionne **importer**, puis **Envoyer**



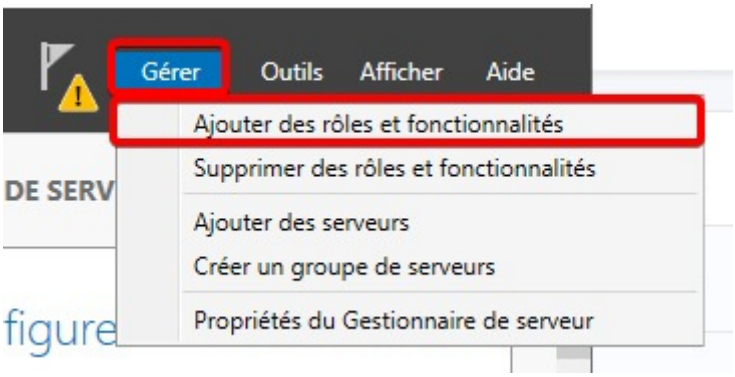
Notre GLPI est donc bien relié a notre annuaire ! Les utilisateurs peuvent maintenant se connecter avec leurs identifiants.

Déploiement d'un site WEB d'entreprise avec IIS :

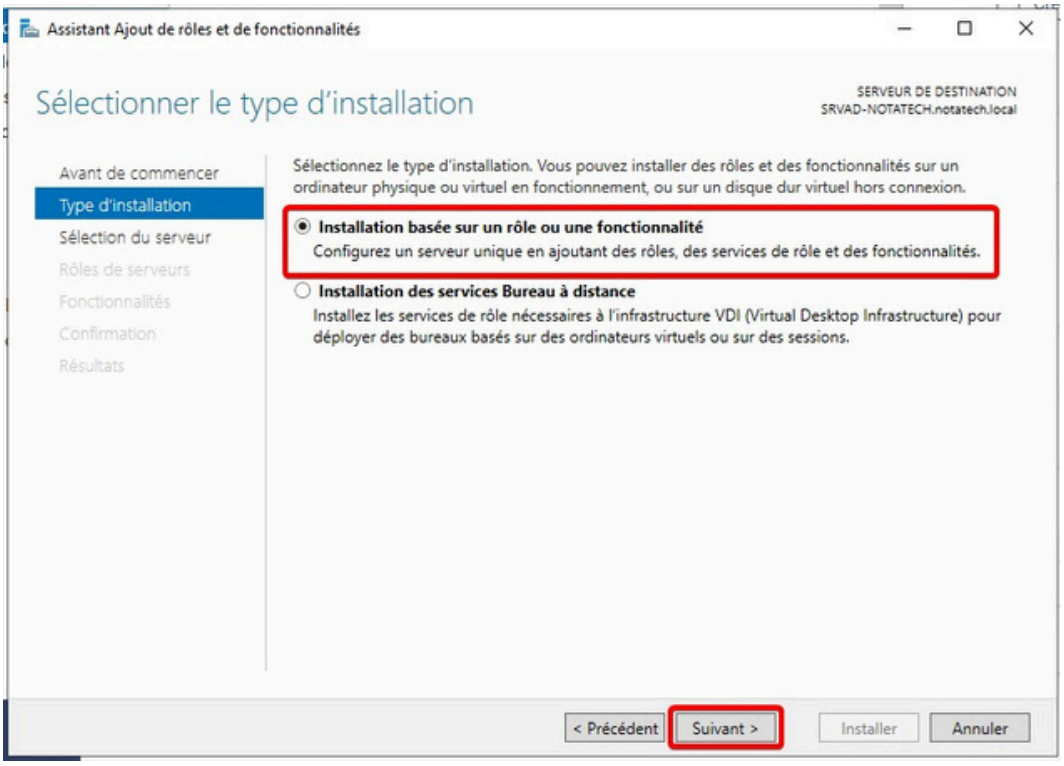
Dans cette partie nous allons voir comment j'ai héberger un site web accessible par les utilisateurs du domaine Notatech.

Installation de IIS sur le Windows Server :

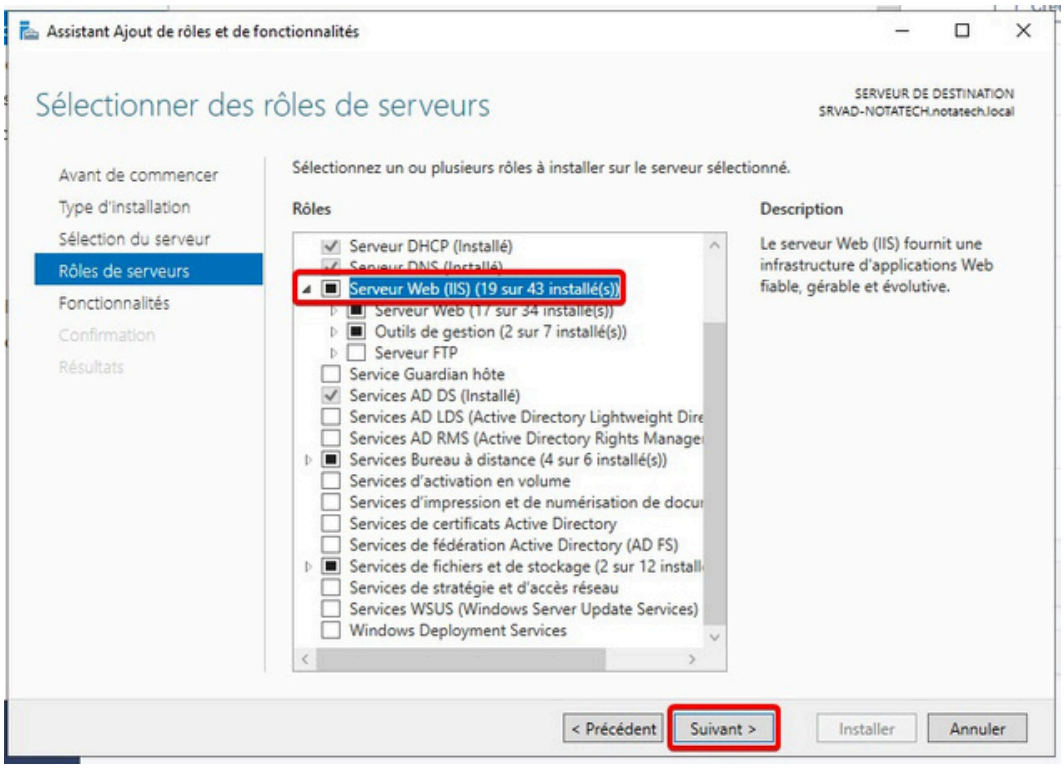
Pour ce faire je commence par me rendre sur le tableau de bord de mon Windows Server sur **Gérer** puis **Ajouter des rôles et fonctionnalités**



Ensuite ici je sélectionne **Installation basée sur un rôle ou une fonctionnalité**

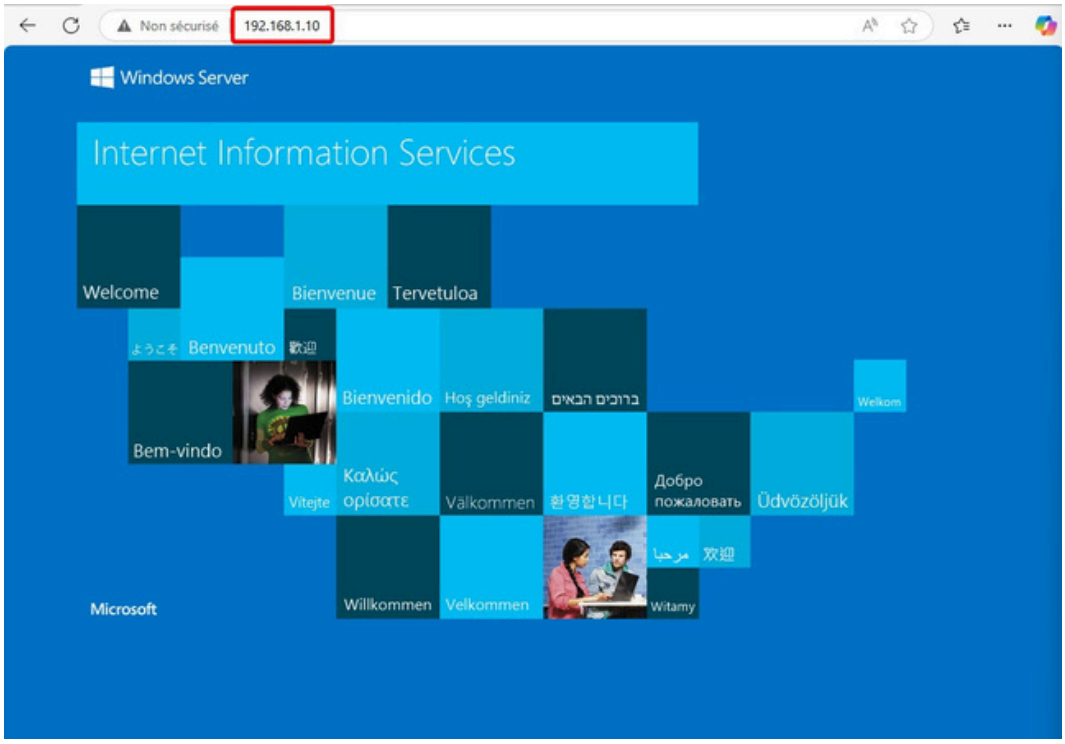


Ici je sélectionne **Serveur Web IIS** et clique sur **Suivant**



Je passe toute la suite de l'installation et valide !

Une fois l'installation terminée pour vérifier que mon serveur IIS est bien fonctionnel, je rentre l'adresse IP de ma machine dans la barre de recherche

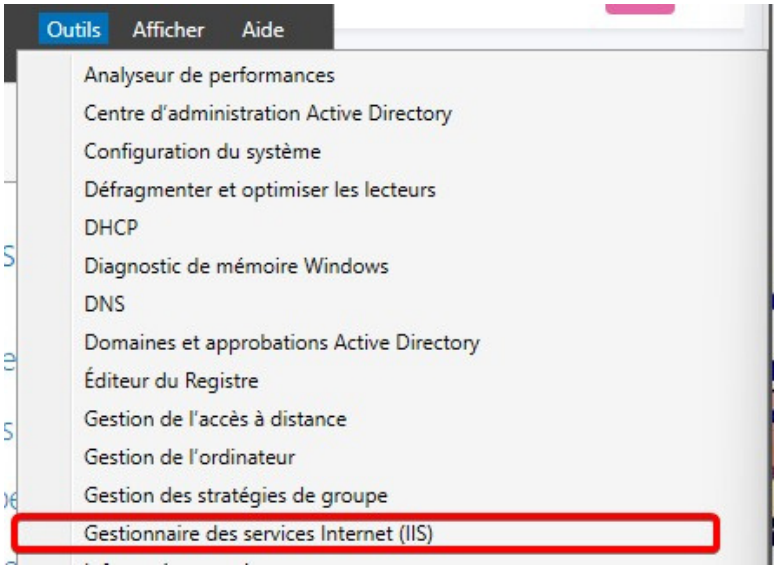


La page s’affiche bien mon serveur IIS est donc bien opérationnel !

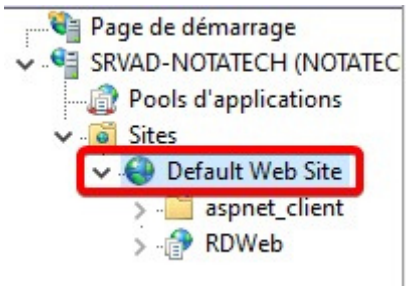
Changement du site web hebergé :

Une fois ceci fait, je vais changer le site web affiché pour mettre le site que je veux mettre a disposition des employés

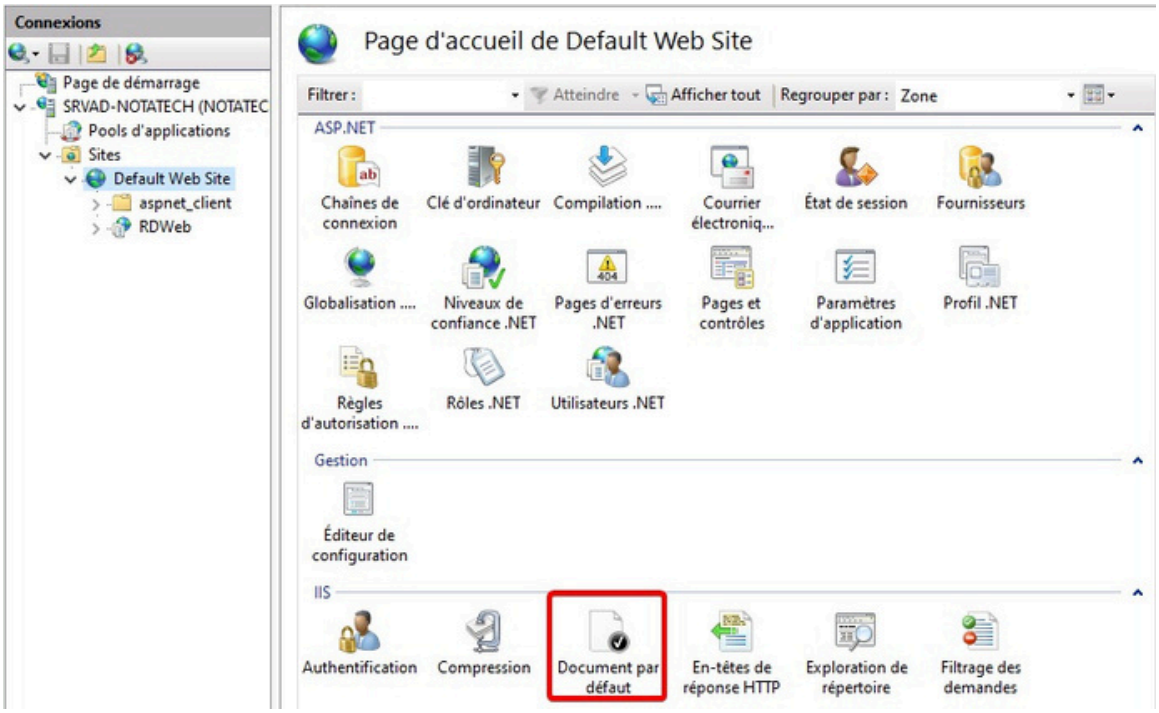
je me rend donc dans la section **Outils** et clique sur **gestionnaire de services Internet IIS**



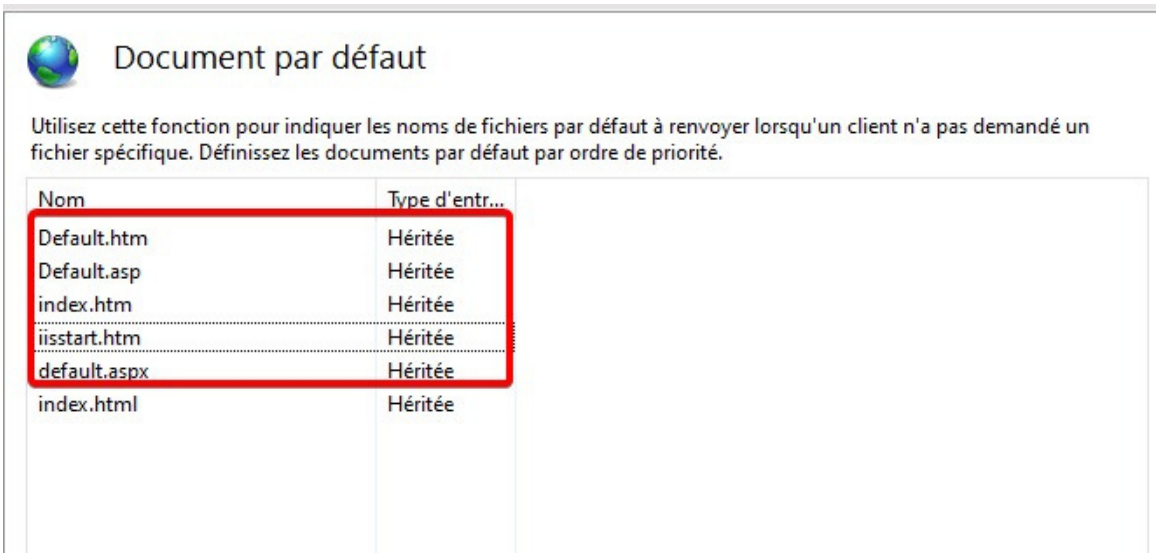
Ensuite ici on peut voir le site par défaut hebergé par IIS, **Default Web Site**



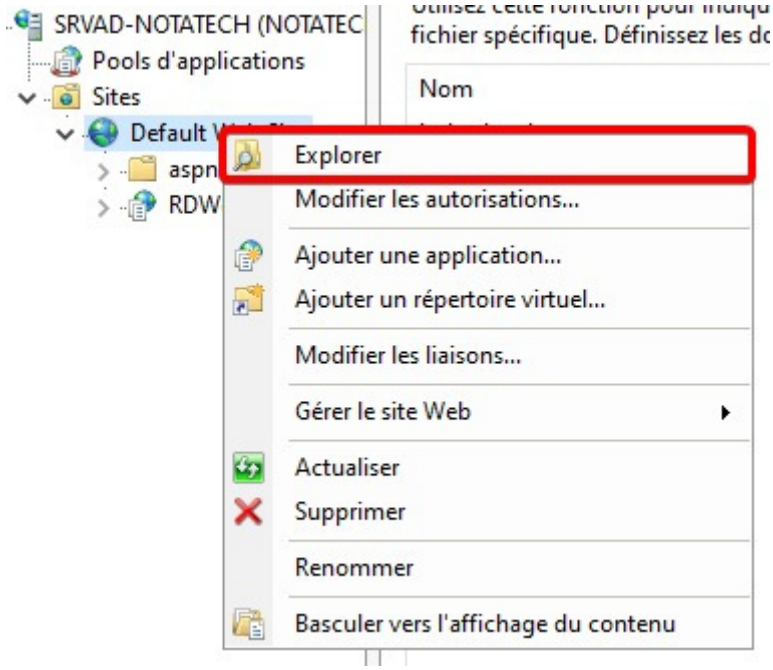
Je clique donc sur le site et sélectionne dans les propositions a droite **Document par défaut**



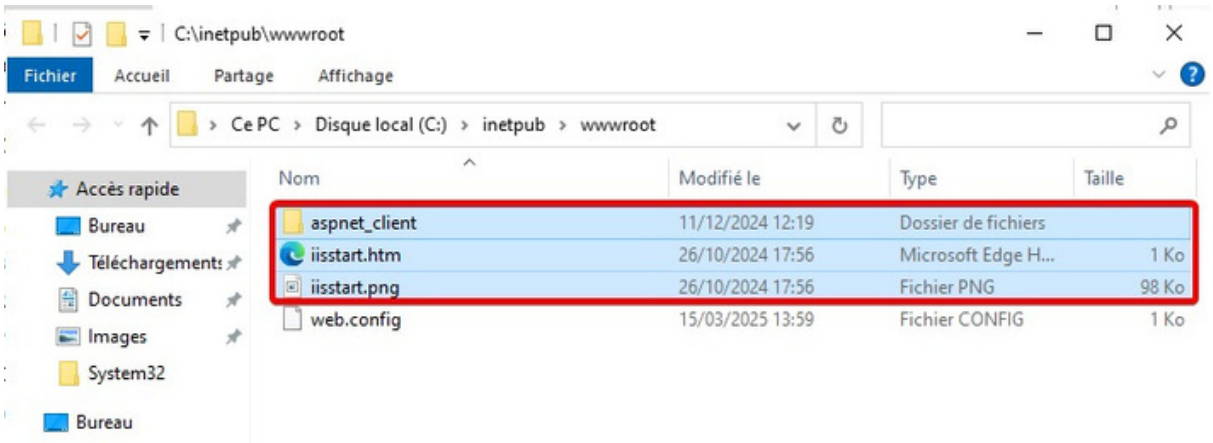
Une fois ceci fait je souhaite garder que mon **index.html** je sélectionne donc tous les autres éléments présents et les supprime



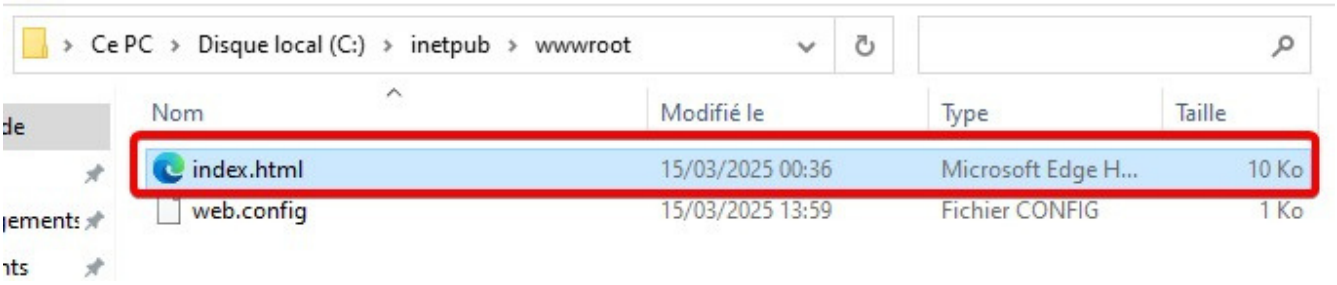
Ensuite ici je fais un clique droit et clique sur **Explorer**



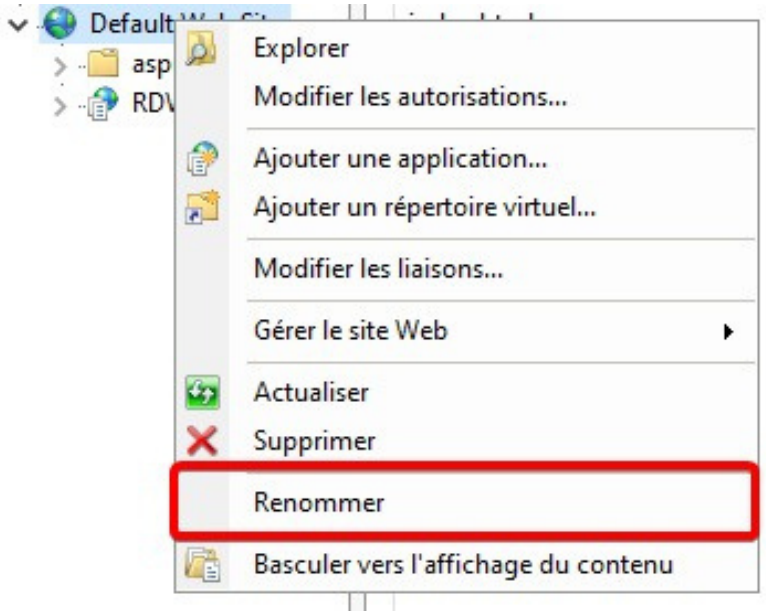
Ensuite dans ce dossier je supprime les fichiers du site web de base a l'exception du fichier **web.config**



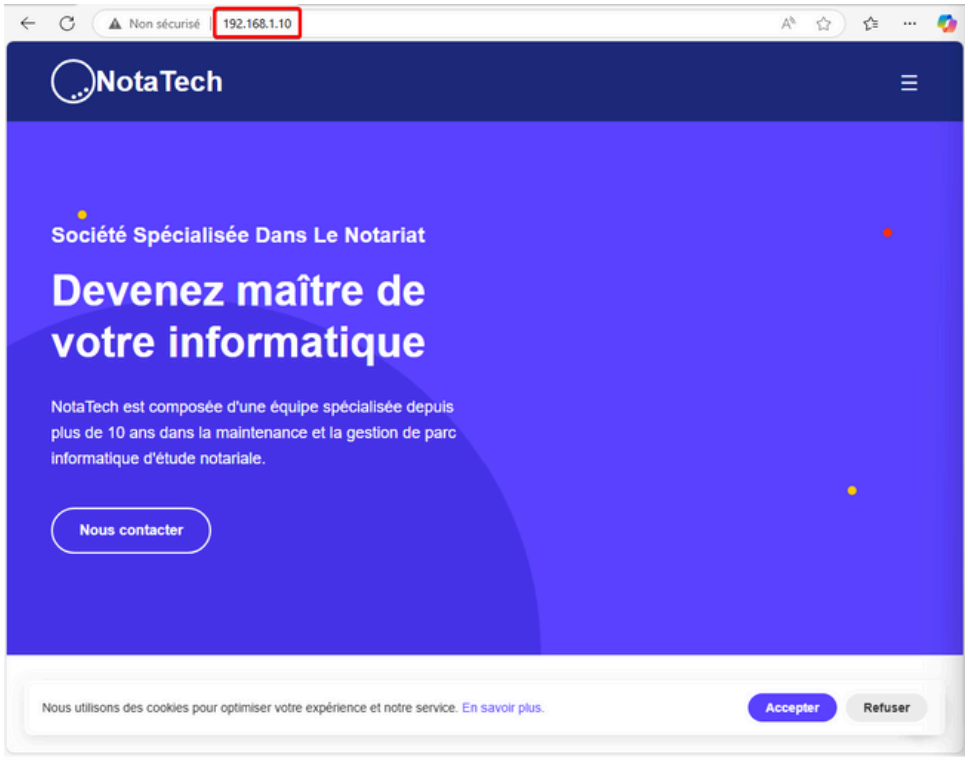
Et j’y ajoute le fichier HTML de mon site web

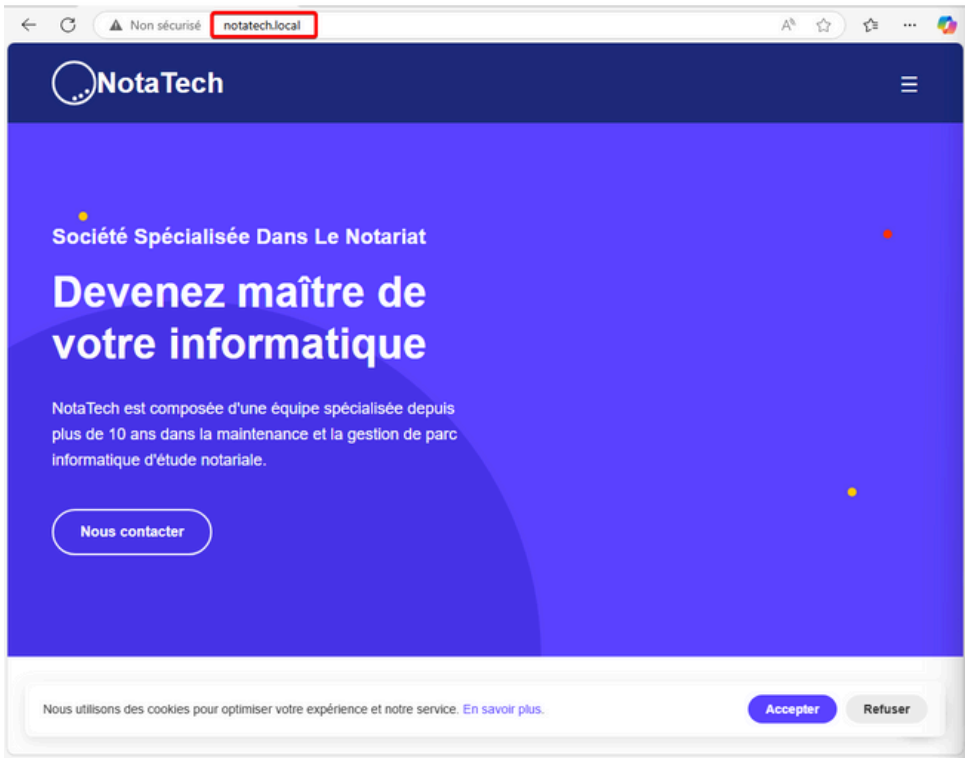


Pour finir je renomme le fichier **Default Web Site** en faisant simplement un clique droit, Renommer



Maintenant quand je rentre l’adresse IP de mon serveur ou mon nom de domaine dans un moteur de recherche j’ai bien mon site qui s’affiche





La configuration est donc bonne notre serveur IIS est terminé !

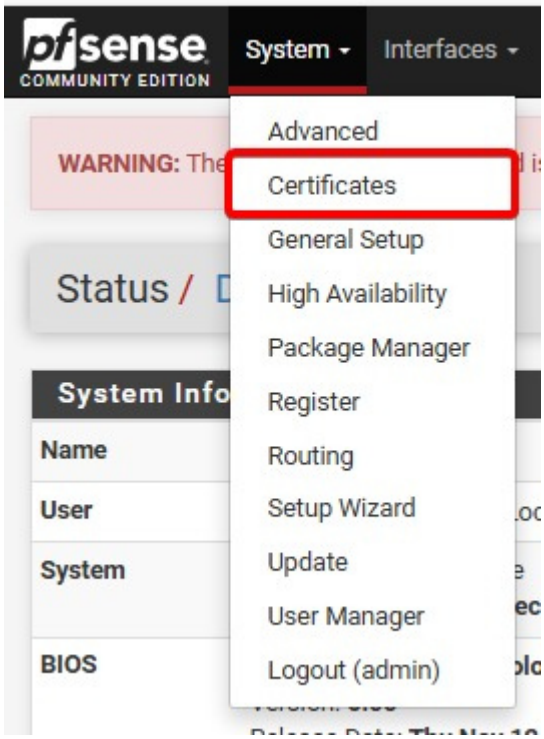
Mise en place de la connexion a distance sécurisée avec OpenVPN :

Je vais maintenant détailler la configuration du serveur OpenVPN sur pfSense. Ce serveur VPN permet aux employés de se connecter à distance en toute sécurité au réseau interne de Notatech, tout en garantissant l'authentification des utilisateurs via Active Directory.

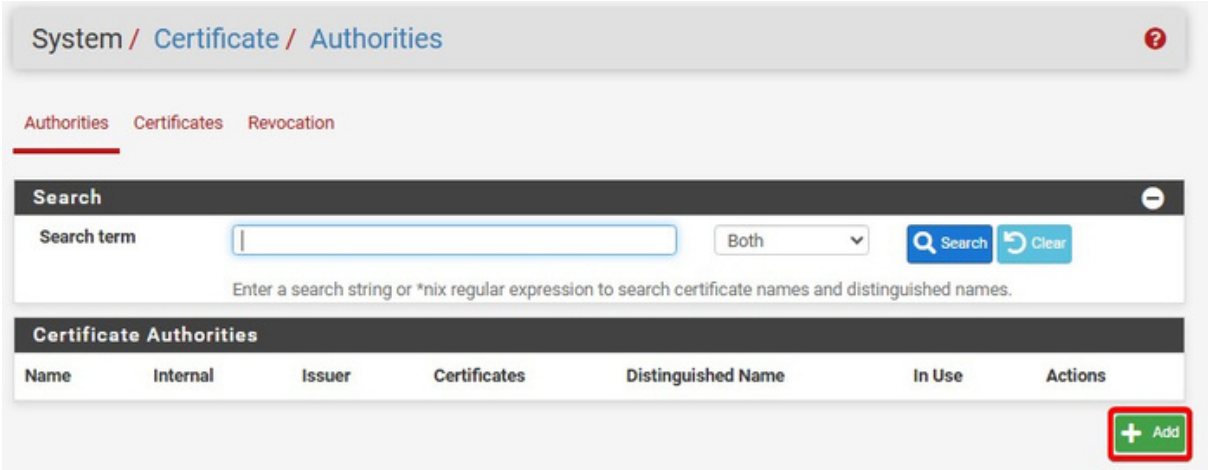
Création de l'autorité de certification :

Premièrement je dois creer une autorité de certification sur mon PfSense

Pour ce faire je commence par me rendre sur l'interface web de configuration de mon PfSense et me rend dans **System > Certificates**



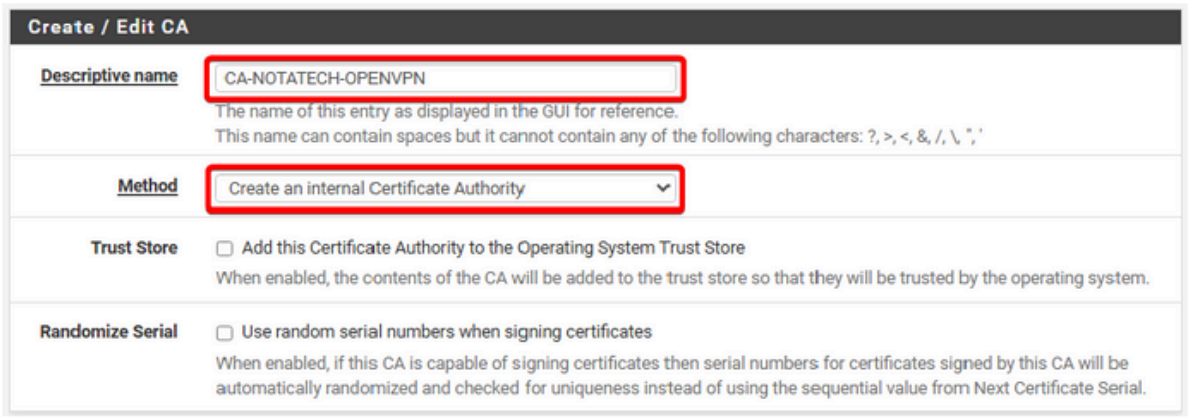
Ensuite sur cette page je clique sur **Add** pour ajouter mon autorité de cer tific ation

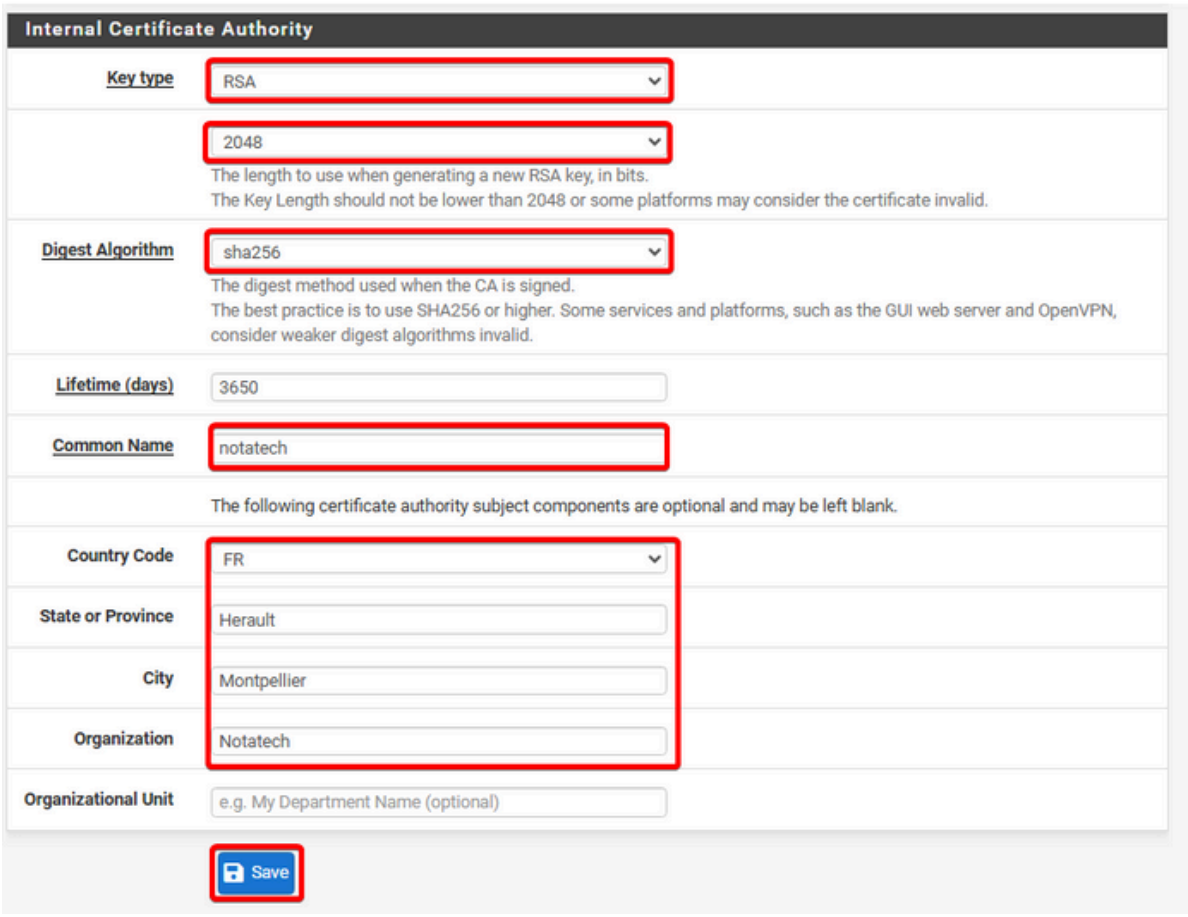


Ici je rentre ces informations

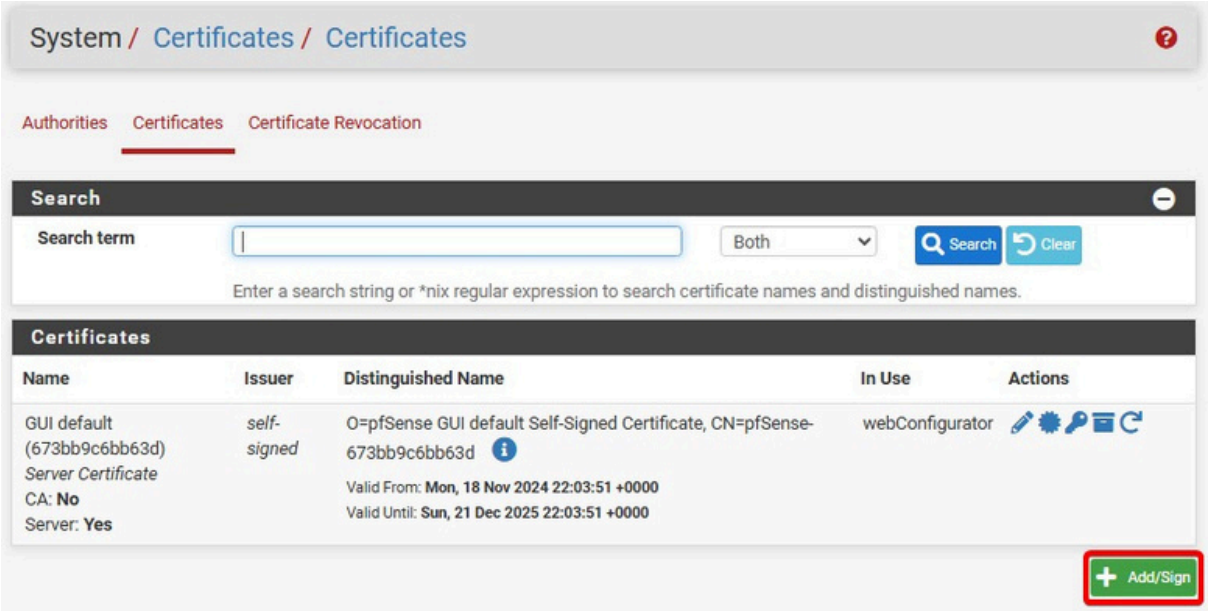
- **Nom descriptif** : CA-NOTATECH-OPENVPN
- **Méthode** : Création d'une autorité de certification interne
- **Type de clé** : RSA
- **Longueur de clé** : 2048 bits (sécurité renforcée)
- **Algorithme de hachage** : SHA-256 (standard sécurisé recommandé)
- **Durée de validité** : 3650 jours (environ 10 ans)
- **Nom commun /Common Name)** : notatech
- **Informations complémentaires** :
  - Pays : FR France
  - État : Hérault
  - Ville : Montpellier
  - Organisation : Notatech

Et je clique ensuite sur **Save**





Ensuite je me rend dans **Certificates** et je clique sur **Add/Sign** pour ajouter un nouveau certificat serveur



Ensuite je rentre ces informations :

- **Méthode** : Création d'un certificat interne
- **Nom descriptif** : VPN-REMOTE
- **Autorité de certification** : CA-NOTATECH-OPENVPN
- **Common Name :** vpn.notatech.local
- **Type de clé** : RSA
- **Longueur de clé** : 2048 bits
- **Algorithme de hachage** : SHA-256
- **Durée de validité** : 3650 jours
- **Type de certificat** : Server Certificate
- **Alternative Names** : FQDN ou Hostname → notatech.local

Add/Sign a New Certificate

Method: Create an internal Certificate

Descriptive name: VPN-REMOTE

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Internal Certificate

Certificate authority: CA-NOTATECH-OPENVPN

Key type: RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256

The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days): 3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name: vpn.notatech.local

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type: Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type	Value
FQDN or Hostname	notatech.local

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

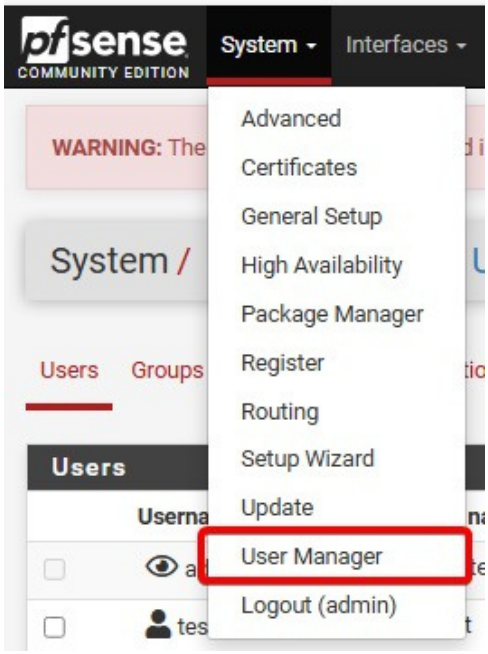
Add SAN Row: + Add SAN Row

Save

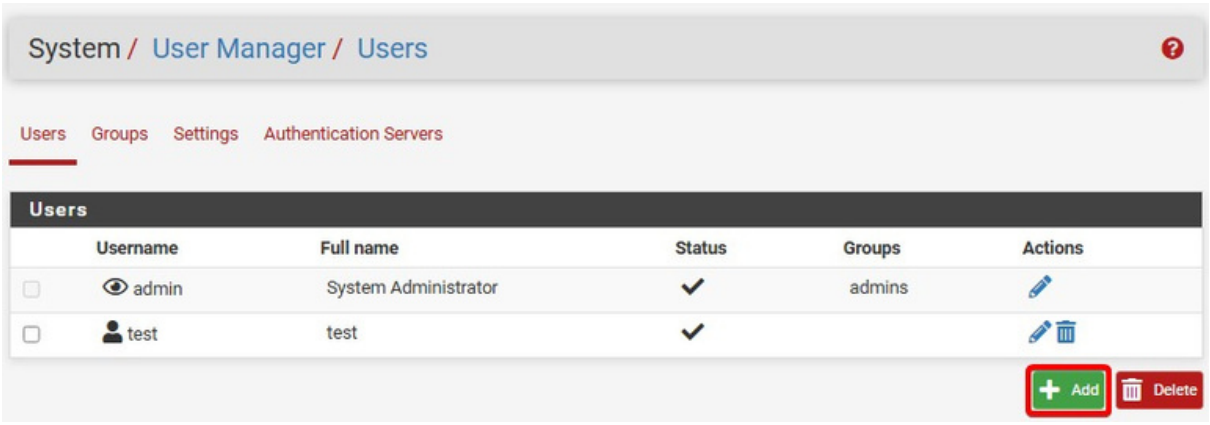
Created internal certificate VPN-REMOTE

Maintenant je vais devoir créer un utilisateur pour la connexion au serveur

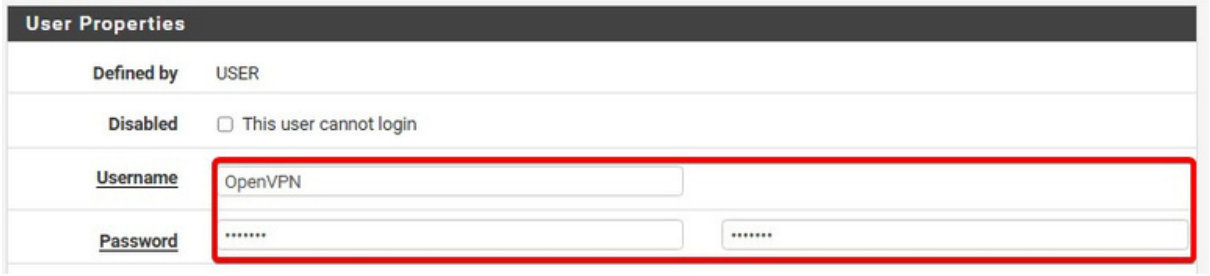
Pour ce faire je me rend donc dans **System > User manager**

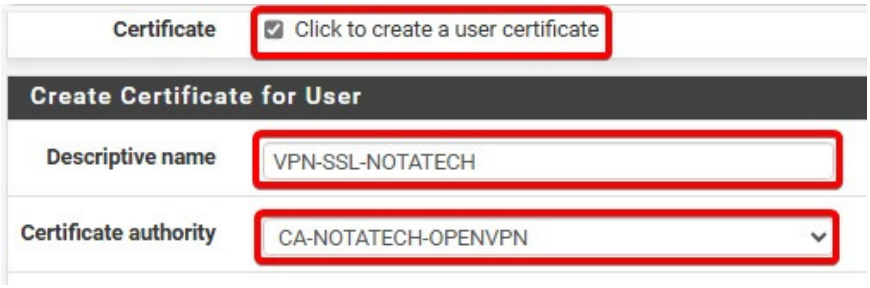


Sur cette page je clique sur **Add**

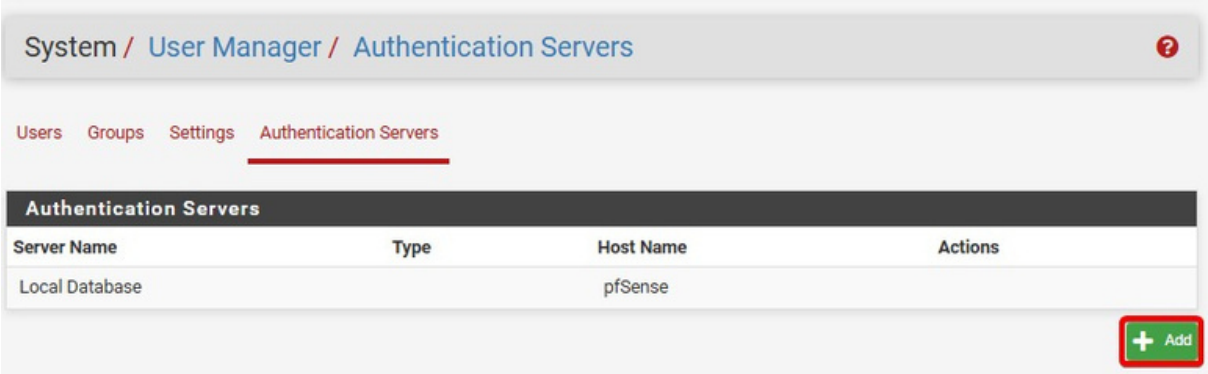


Ensuite je rentre les informations basiques d'un utilisateur **Utilisateur/mot de passe** et très important je coche **Click to create a user certificate,** je sélectionne mon certificat créé précédemment et sauvegarde ces paramètres





Ensuite pour continuer je dois ajouter mon AD aux serveurs d'authentification de PfSense, je me rend donc dans Authentification Servers et clique sur **Add**



Ici je rentre donc ces informations :

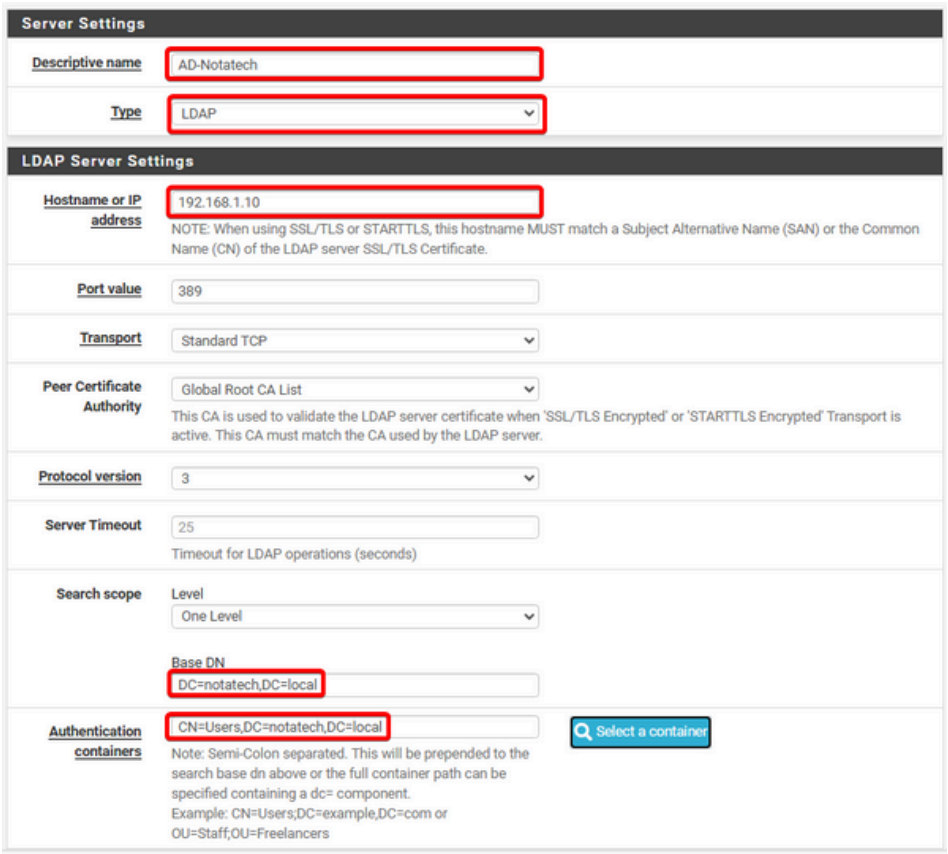
- **Nom descriptif** : AD-Notatech
- **Type** : LDAP
- **Adresse du serveur (Hostname or IP address)** : 192.168.1.10 (IP du serveur Active Directory)
- **Port** : 389 (LDAP non sécurisé, si LDAPS est utilisé, mettre 636)
- **Transport** : Standard TCP
- **Autorité de certification** : Global Root CA List *(si le serveur AD utilise un certificat, il faut le spécifier ici)*
- **Version du protocole** : 3
- **Délai d'attente serveur** : 25 secondes
- **Scope de recherche** : One Level

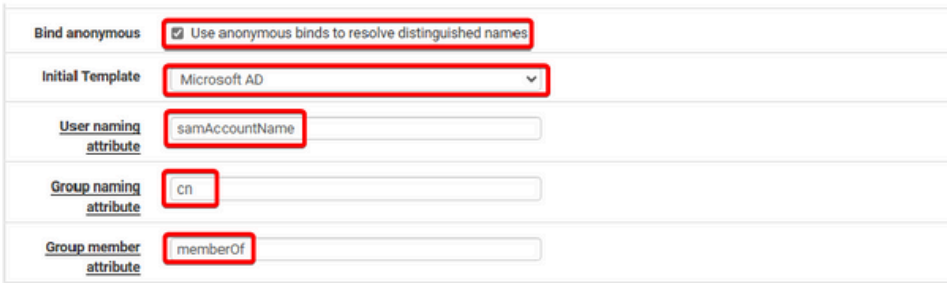
- **Base DN** : `DC=notatech,DC=local` *(domaine de l'AD pour la recherche des utilisateurs et groupes)*
- **Conteneur d'authentification** : `CN=Users,DC=notatech,DC=local`

  (chemin du conteneur où se trouvent les utilisateurs)

Paramètres avancés :

- **Bind anonymous** : Activé *(permet la récupération des noms d'utilisateurs sans authentification, mais pas recommandé en production)*
- **Modèle d'initialisation (Initial Template)** : `Microsoft AD` *(permet d'appliquer les réglages adaptés pour Active Directory)*
- **Attribut d'identification utilisateur** : `sAMAccountName` *(utilisé pour l'authentification des utilisateurs AD, correspond au login Windows)*
- **Attribut de nom de groupe** : `cn` *(nom du groupe dans l'AD)*
- **Attribut des membres de groupe** : `memberOf` *(permet d'identifier les groupes auxquels appartient un utilisateur pour l'authentification et les autorisations)*

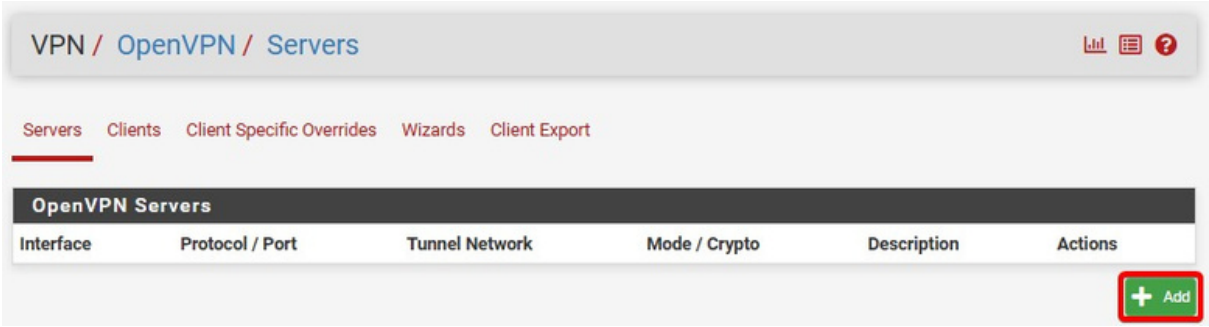




Configuration du serveur OpenVPN :

Maintenant on doit configurer le serveur OpenVPN
Pour ce faire je commence par me rendre dans **VPN > OpenVPN**

Sur cette page je clique sur **Add**



Ensuite dans cette page je rentre ces informations de configuration :

Configuration générale

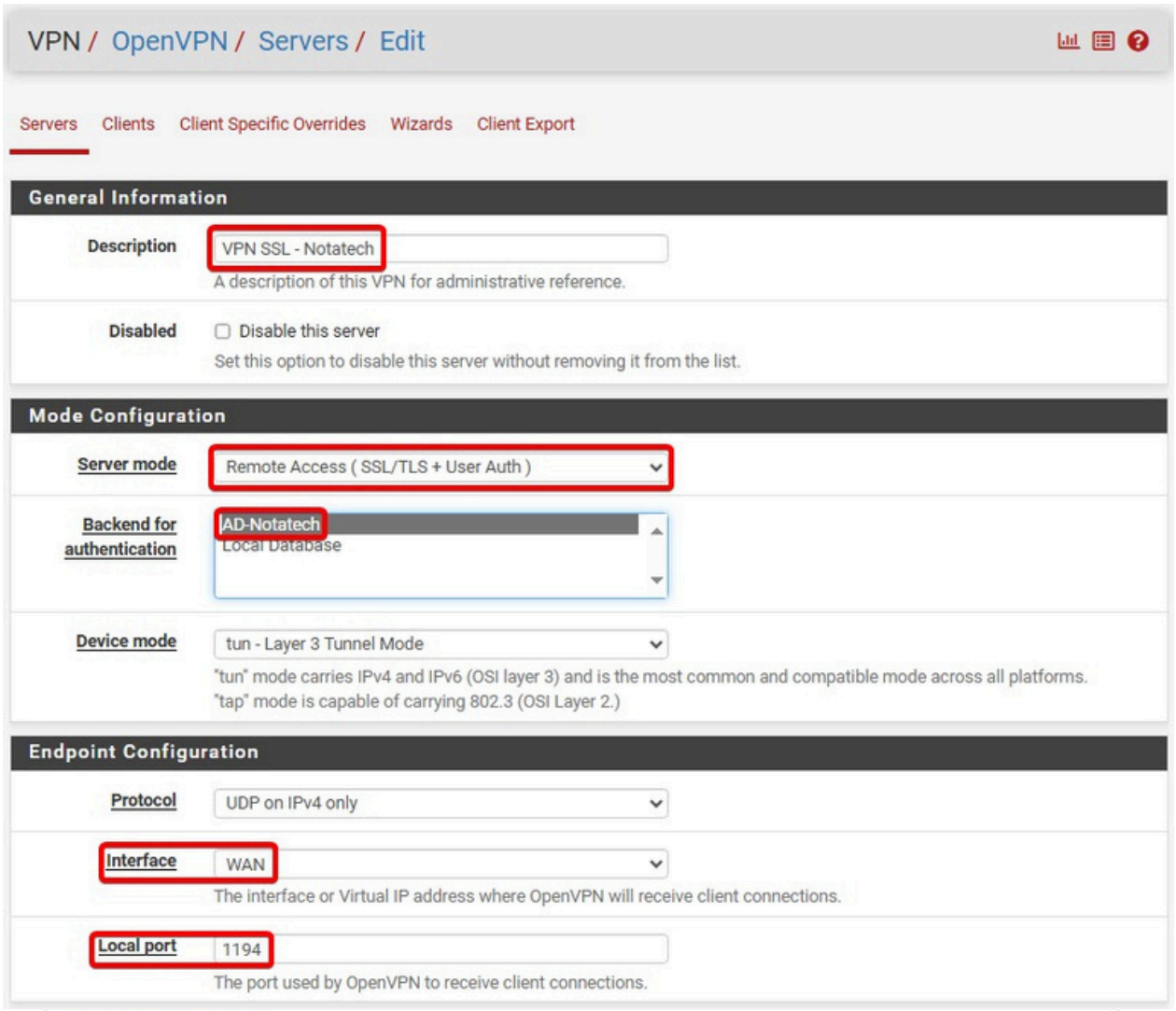
- **Description** : VPN SSL - Notatech *(nom d'identification du serveur VPN dans pfSense)*
- **Mode serveur** : Remote Access (SSL/TLS + User Auth) *(nécessite à la fois un certificat et une authentification utilisateur)*
- **Backend for authentication** : AD-Notatech *(utilise Active Directory pour la'uthentification des utilisateurs VPN)*

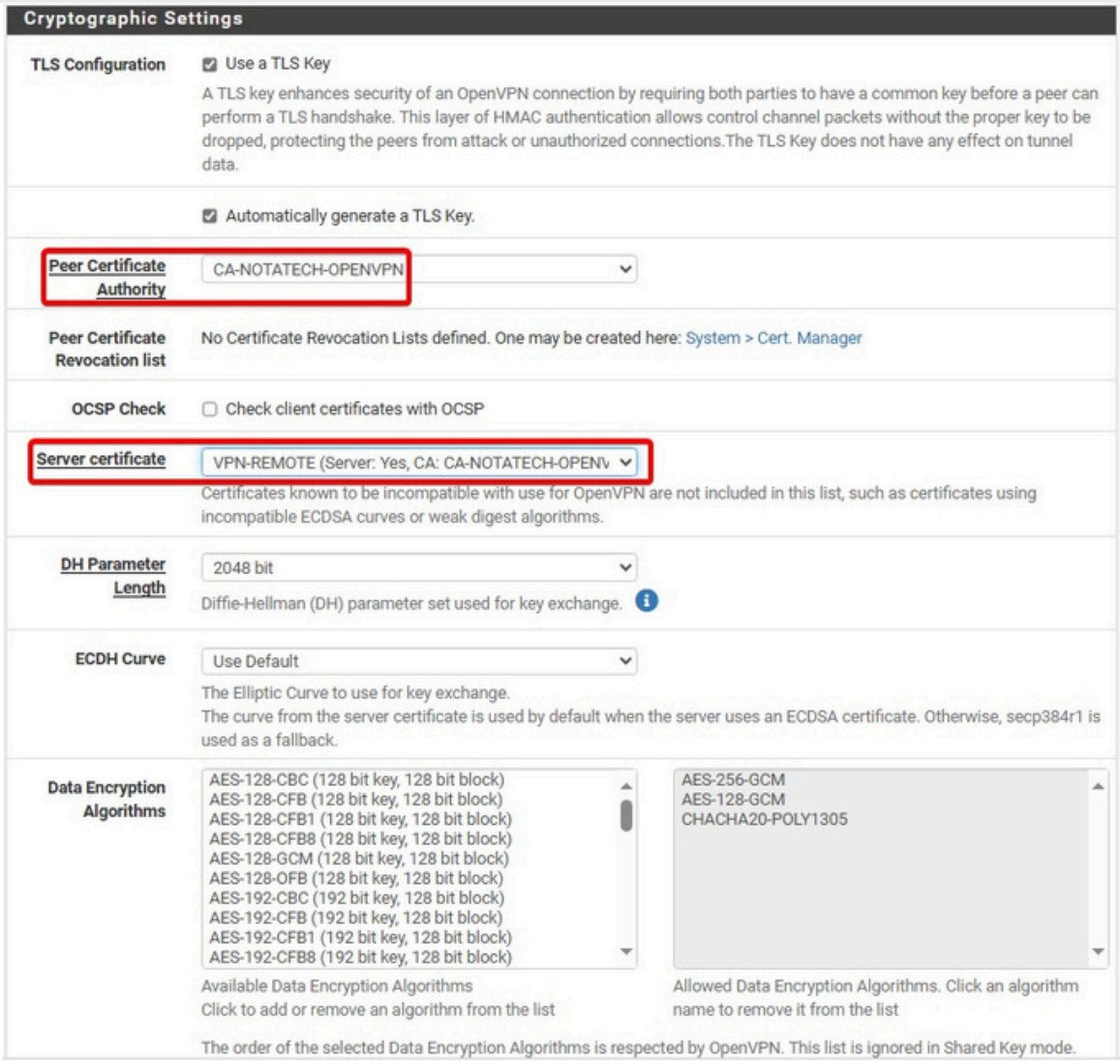
Configuration réseau

- **Protocole** : UDP on IPv4 only *(réduction de la latence par rapport à TCP, utilisation exclusive d'IPv4)*
- **Interface** : WAN *(écoute les connexions entrantes sur l'interface externe du pare-feu)*
- **Port local** : 1194 *(port standard pour OpenVPN, peut être modifié en cas de besoin)*

Configuration cryptographique

- **TLS Configuration** : Utilisation d'une clé TLS pour renforcer la sécurité des connexions VPN.
- **Autorité de certification (Peer Certificate Authority)** : CA-NOTATECH-OPENVPN *(utilisée pour signer les certificats du serveur et des clients)*
- **Certificat serveur** : VPN-REMOTE *(certificat spécifique pour l'authentification du serveur OpenVPN, signé par la CA Notatech)*
- **Longueur du paramètre DH (Diffie-Hellman)** : 2048 bits *(niveau de sécurité recommandé pour lé'change de clés)*
- **Courbe ECDH** : Use Default *(utilise la courbe par défaut définie par le certificat serveur)*
- **Algorithmes de chiffrement des données** :
  - AES-256-GCM *(chiffrement fort et rapide recommandé pour OpenVPN)*
  - AES-128-GCM
  - CHACHA20-POLY1305 *(performant sur les architectures modernes, notamment mobiles)*


VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
Client Export
General Information
Description
VPN SSL - Notatech
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Mode Configuration
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
AD-Notatech
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
1194
The port used by OpenVPN to receive client connections.


Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
Automatically generate a TLS Key.
Peer Certificate Authority
CA-NOTATECH-OPENVPN
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
VPN-REMOTE (Server: Yes, CA: CA-NOTATECH-OPENV
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Et pour la fin de la configuration je rentre ces informations :

- **IPv4 Tunnel Network** : `192.168.1.0/24`
  - C'est le réseau virtuel utilisé pour la communication entre le serveur VPN et les clients connectés.
  - L'adresse `192.168.1.1` sera attribuée au serveur VPN et les autres adresses aux clients VPN.
    Ce réseau ne doit pas entrer en conflit avec ton réseau local.
  -
- **IPv6 Tunnel Network** : *(laissé vide, car non utilisé pour ce VPN)*
- **Redirect IPv4 Gateway** : *(non coché)*
  - Si activé, tout le trafic Internet des clients passera par le tunnel VPN.
  - À activer si tu veux forcer tout le trafic via ton infrastructure locale.

Redirect IPv6 Gateway : *(non coché, pas d'IPv6 configuré pour ce VPN)*

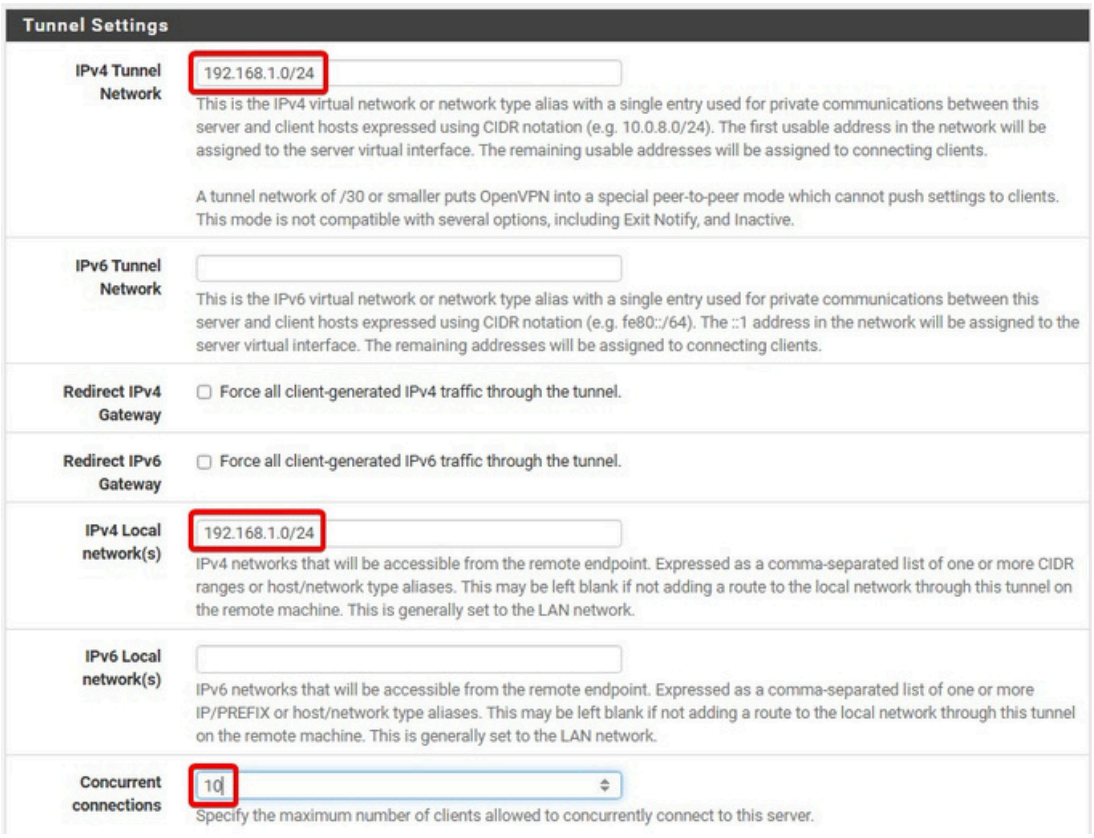
IPv4 Local Network(s) : `192.168.1.0/24`

- Définit les réseaux internes accessibles par les clients VPN.
- Permet aux utilisateurs connectés en VPN d'accéder aux ressources de l'infrastructure locale.

IPv6 Local Network(s) : *(laissé vide, car non utilisé pour ce VPN)*

Concurrent Connections : `10`

- Nombre maximum d'utilisateurs pouvant se connecter simultanément au VPN.
- Peut être augmenté selon les besoins et les performances du serveur.



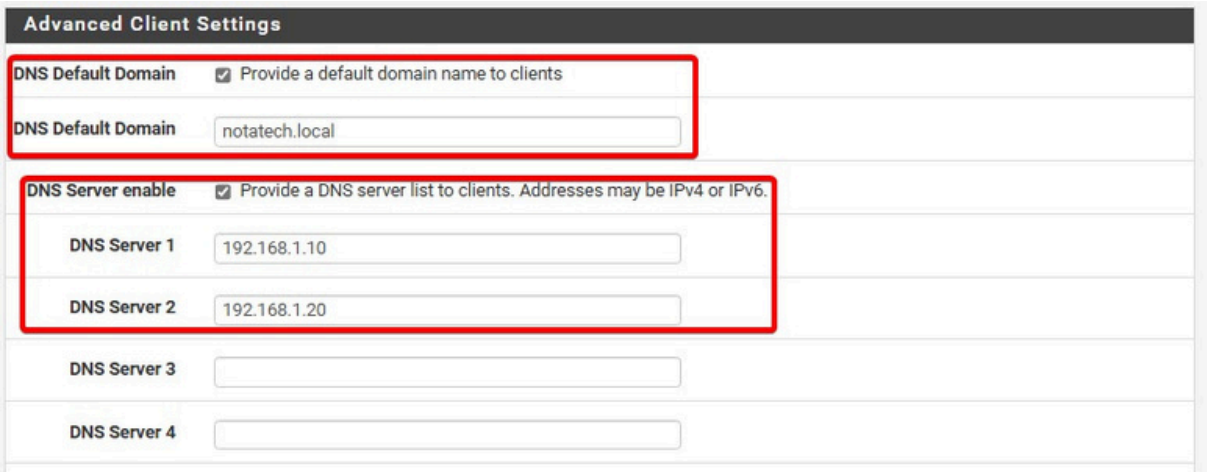
Paramètres des clients (Client Settings)

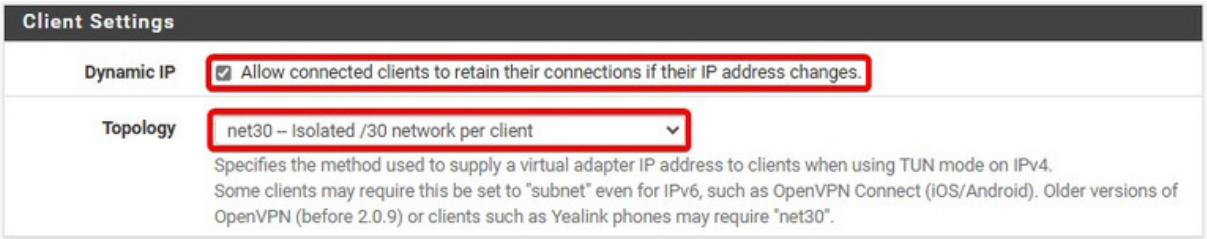
- **Dynamic IP** : ✅ Activé
  - Permet aux clients de conserver leur connexion VPN même si leur adresse IP change (ex. en cas de changement de réseau).
- **Topology** : `net30 -- Isolated /30 network per client`
  - Attribue une plage réseau `/30` à chaque client VPN.
  - Compatible avec les versions plus anciennes d'OpenVPN et certains équipements spécifiques.
  - Si tu veux une configuration plus moderne et simplifiée, **"subnet"** peut être une meilleure option.

Paramètres avancés des clients (Advanced Client Settings)

- **DNS Default Domain** : ✅ `notatech.local`

  Fournit aux clients VPN le domaine par défaut de l'entreprise pour la résolution DNS interne.
- **DNS Server enable** : ✅ Activé
  - **DNS Server 1** : `192.168.1.10` Serveur DNS principal, souvent ton Active Directory)
  - **DNS Server 2** : `192.168.1.20` Second serveur DNS, peut être un AD secondaire ou un autre serveur de résolution DNS interne)

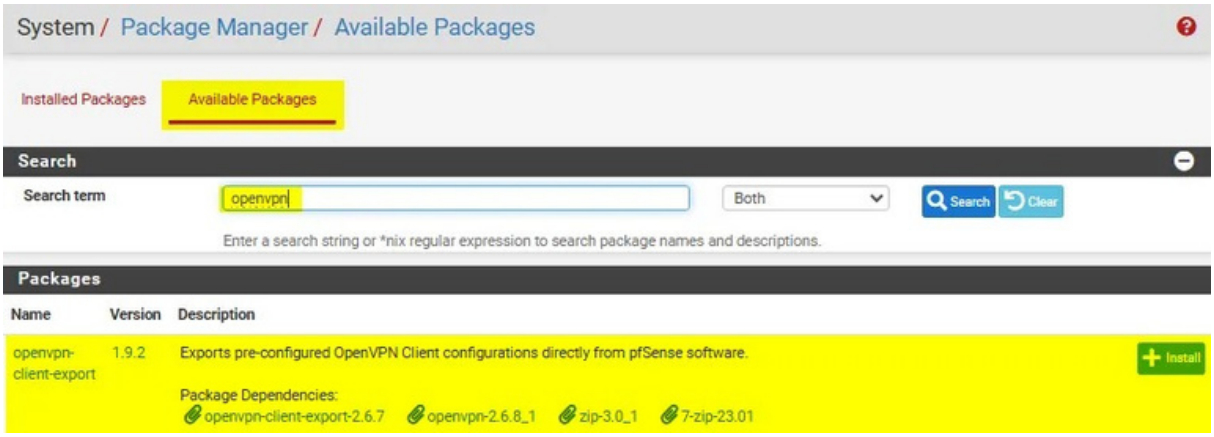




Installation d'openVPN :

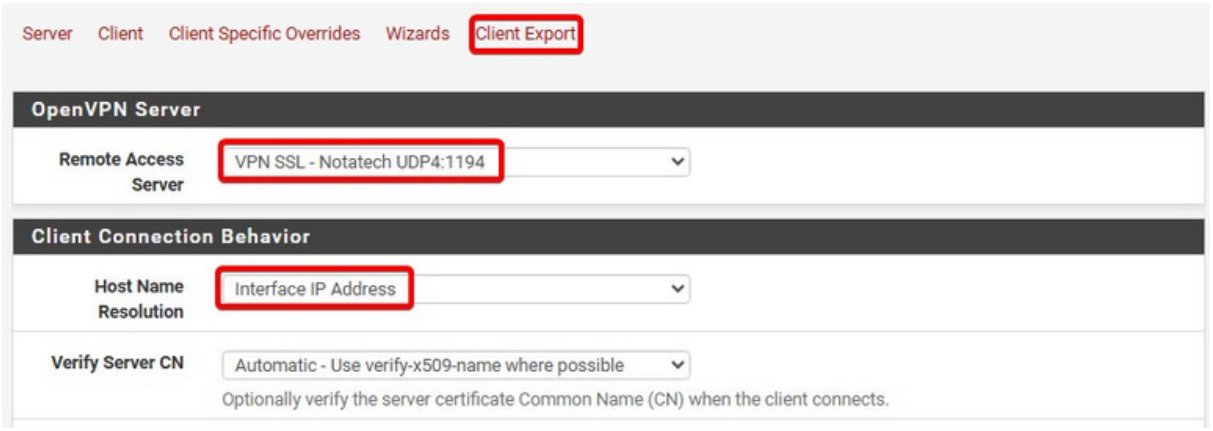
Je passe maintenant a l'installation d'OpenVPN sur mon PfSense.

Pour ce faire je me rend premièrement dans **Package manager > Available Packages** je recherche **OpenVPN** et installe le package OpenVPN

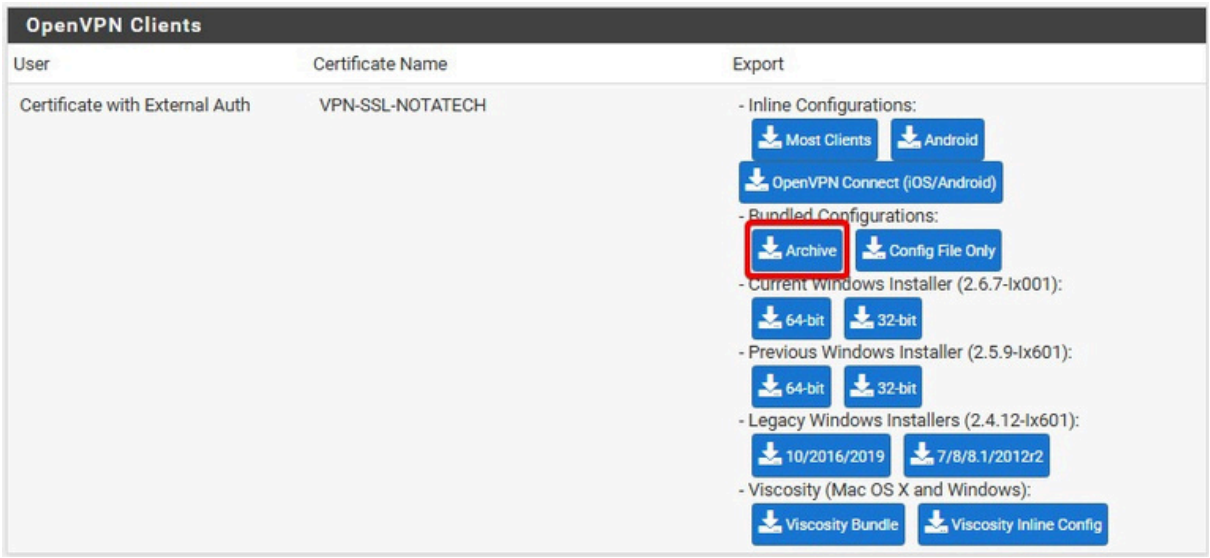


Une fois installé je me rend dans **VPN > OpenVPN** dans l'interface PfSense **:**

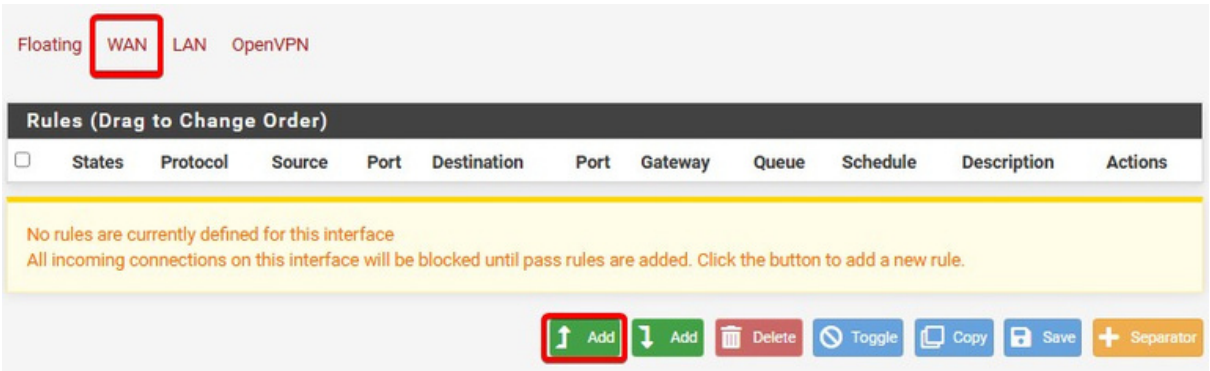
Dans cette étape, je vais dans **VPN > OpenVPN > Client Export** sur pfSense. Je sélectionne le serveur
OpenVPN configuré (**VPN SSL - Notatech UDP1194**), puis je clique sur l'onglet **Client Export**.



Je choisis le format d'exportation souhaité pour récupérer le fichier de configuration **.ovpn** que j'utiliserai sur le client.



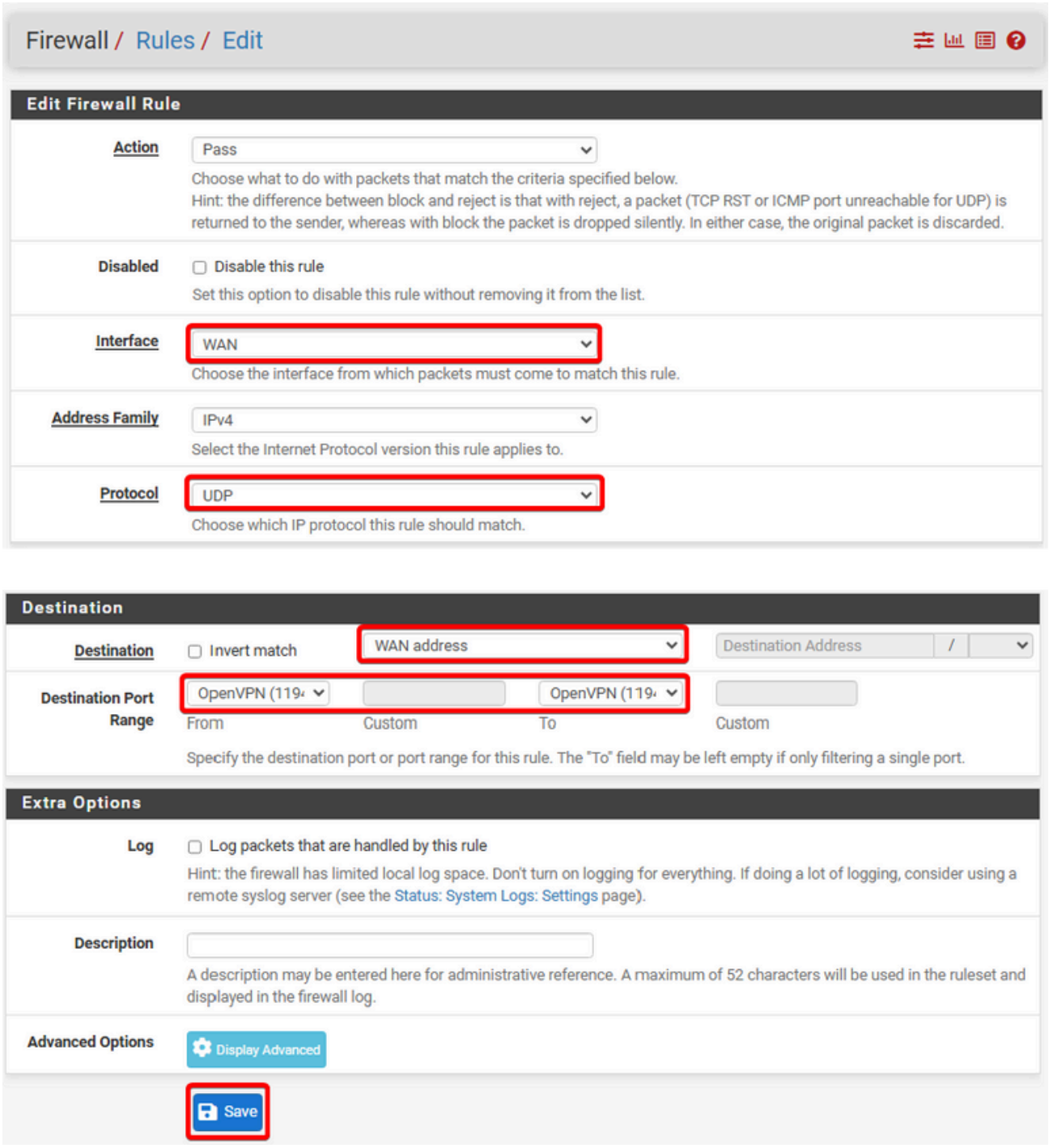
Ici, je me rends dans **Firewall ≣ Rules ≣ WAN** afin de créer une règle permettant d'autoriser le trafic entrant sur le port UDP 1194 utilisé par OpenVPN. Je clique sur **Add** pour ajouter une règle.



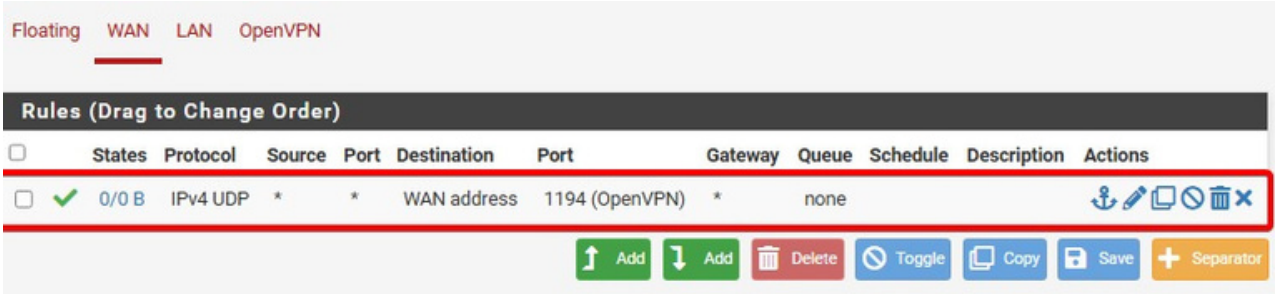
Je configure comme suit :

- **Action** : Pass
- **Interface** : WAN
- **Protocol** : UDP
- **Destination** : WAN address
- **Destination Port Range** : 1194 OpenVPN

Puis je sauvegarde et applique les changements.



Ici on peut voir le résultat final après avoir ajouté la règle WAN. La règle permet explicitement les connexions UDP sur le port 1194 vers l'adresse WAN du pfSense.

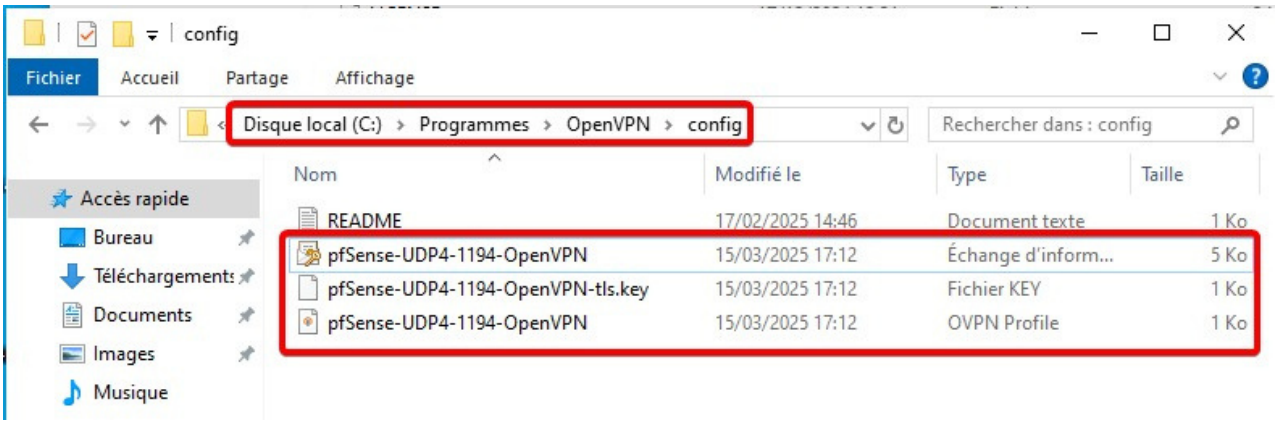


Configuration sur poste client :

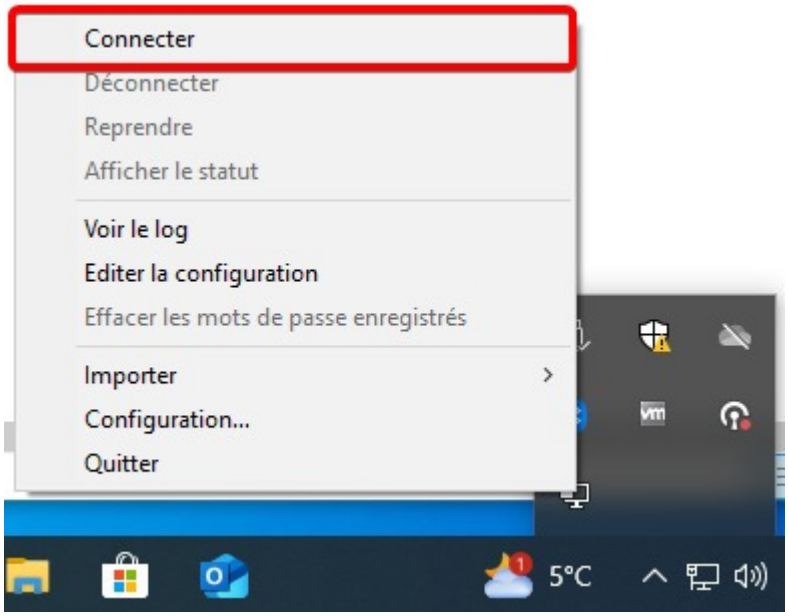
Maintenant nous allons faire la configuration sur le poste client pour que le client puisse se connecter en VPN

Ici sur la machine cliente, je copie le fichier de configuration OpenVPN exporté depuis pfSense dans le dossier **C:\Program Files\OpenVPN\config** sur mon poste client.

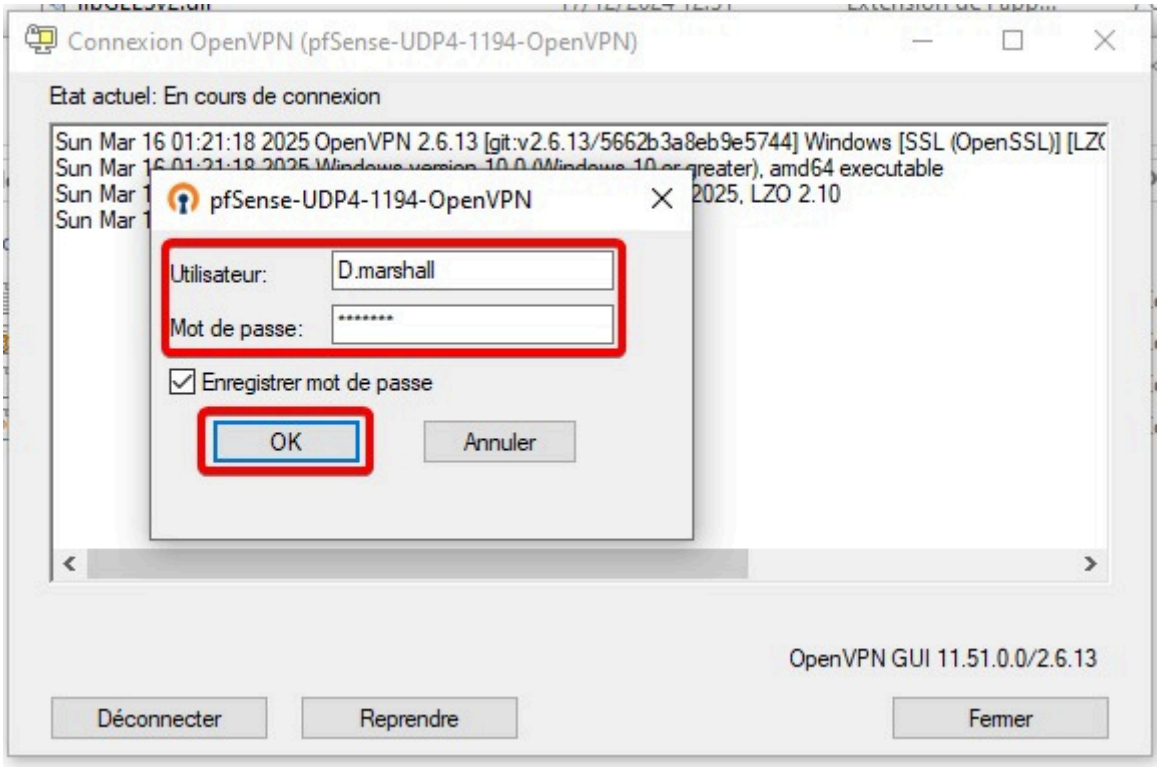
Ce fichier contient tous les paramètres nécessaires pour établir la connexion VPN, y compris les certificats.



Ensuite, je clique-droit sur l'icône OpenVPN dans la barre des tâches, et je clique sur **Connecter**.



Une fenêtre apparaît me demandant le **nom d'utilisateur** et le **mot de passe**. je rentre donc le nom d'utilisateur et mot de passe de mon utilisateur **D Marshall** présent sur mon **Active Directory**



Une fois connecté, une notification s'affiche confirmant la connexion VPN établie avec succès.

La configuration fonctionne donc bien !