Horizon Management
Documentation Technique
Déploiement Infrastructure Réseau

Projet PPE – BTS SIO – Horizon Management

Auteur : POUPOT Elliot / Étudiant BTS SIO
Date : Avril 2025

Sommaire

1. Introduction

Dans le cadre du projet pour la Maison des Ligues de Lorraine, cette documentation détaille le déploiement d'une infrastructure réseau complète virtualisée. L'objectif est de permettre une gestion centralisée des utilisateurs, machines, et ressources réseau via Windows Server 2022, en intégrant les services Active Directory, DHCP, DNS, et une GPO de partage.

2. Objectifs du Projet

- Installation et configuration de Windows Server 2022

- Déploiement des services AD DS, DHCP, DNS

- Création et application de GPO pour le partage de fichiers

- Intégration de postes clients Windows au domaine

- Configuration d'un routeur PfSense

3. Matériel et Logiciels Utilisés

Matériel :
- Serveur physique ou virtuel
- Routeur PfSense
- Switch manageable Cisco
- Postes clients Windows 11
- Câblage RJ45

Logiciels :
- Windows Server 2022
- VMWare ou VirtualBox
- PfSense
- Outils d'administration Windows

4. Déploiement PfSense

Détails du système :

Un **routeur PfSense** est un dispositif réseau open-source basé sur **FreeBSD** qui sert de **pare-feu, routeur, VPN, et gestionnaire de trafic**. Il offre des fonctionnalités de **NAT, QoS, DHCP, DNS, monitoring, et reporting** avec une interface web intuitive, garantissant une sécurité renforcée et une administration simplifiée.

Il nous servira dans ce cas précis à la bonne configuration de notre **Windows Serveur 2022** ;

Nous déterminons l'ip suivante pour notre réseau privé accueillant ce serveur afin de nous en servir de passerelle pour le réseau NAT.

FreeBSD est un système d'exploitation open source basé sur le système open-source, **UNIX**.

L'image disque de ce système est disponible sur le site officiel (ISO PfSense) et pèse environ 1 Go.

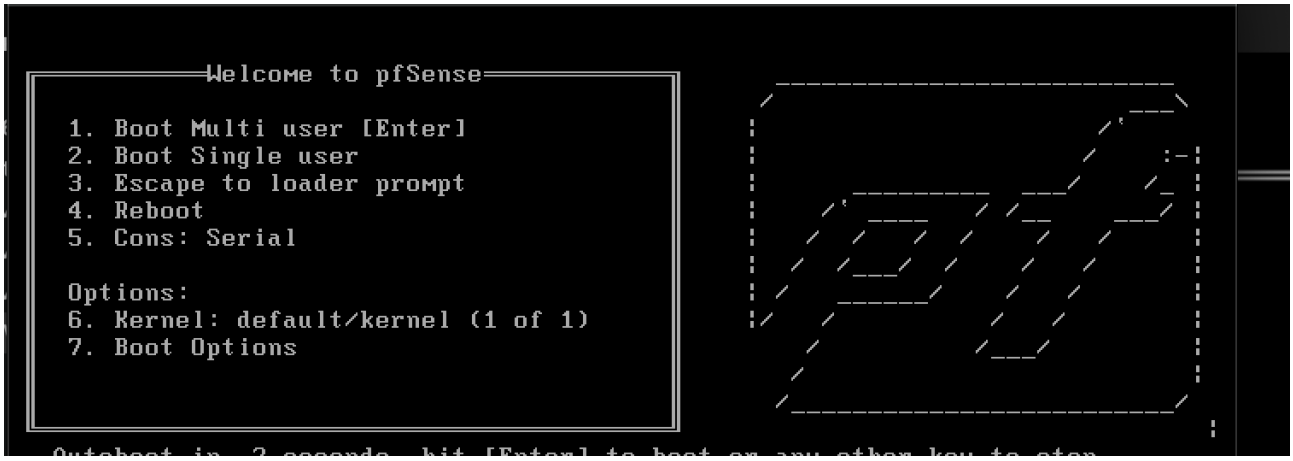
Pré-requis logiciel et matériel :

Les pré-requis pour l'installation de ce système sont les suivants ;

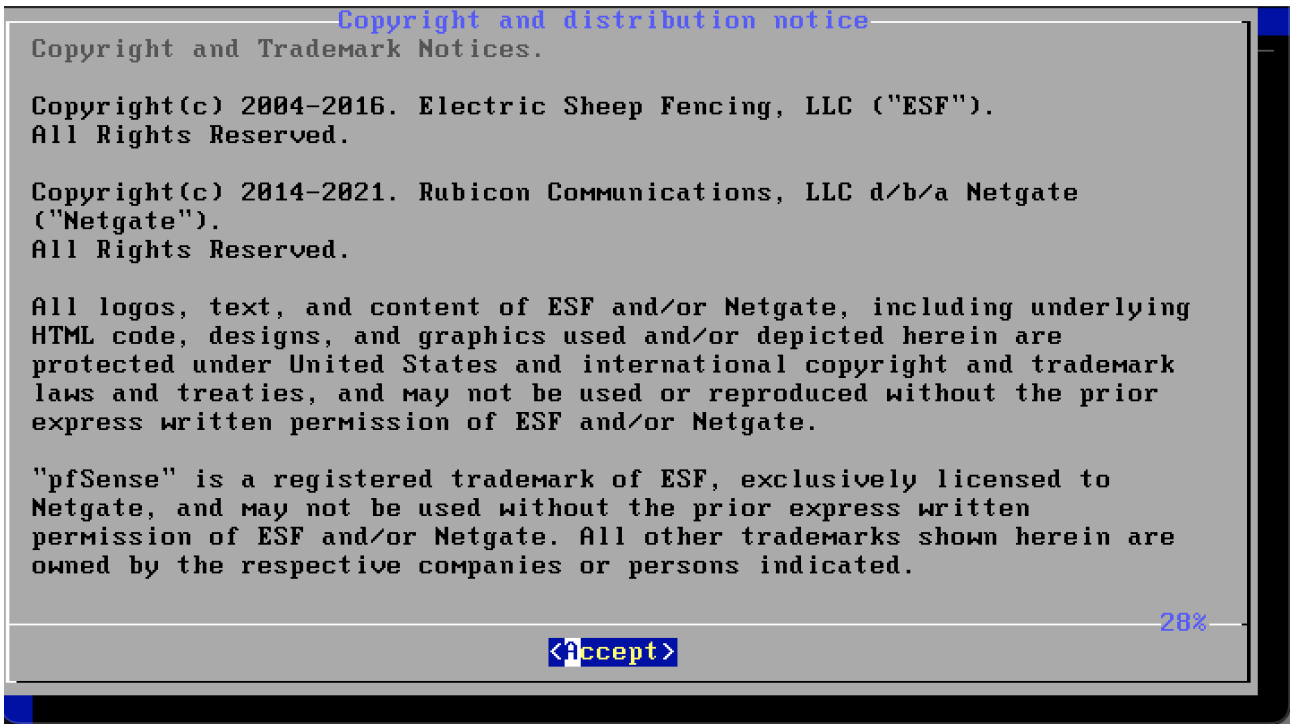
- CPU : 1. GHz x64.
- RAM : 2 Go à 4 Go.
- Stockage : 4 Go pour l'installation de base, recommandé ; 10 Go.
- Interfaces réseau : 2 interfaces ; une patte WAN ainsi qu'une patte LAN.
- Boot : ISO sur support amovible bootable d'au moins 2 Go.

Installation du système :

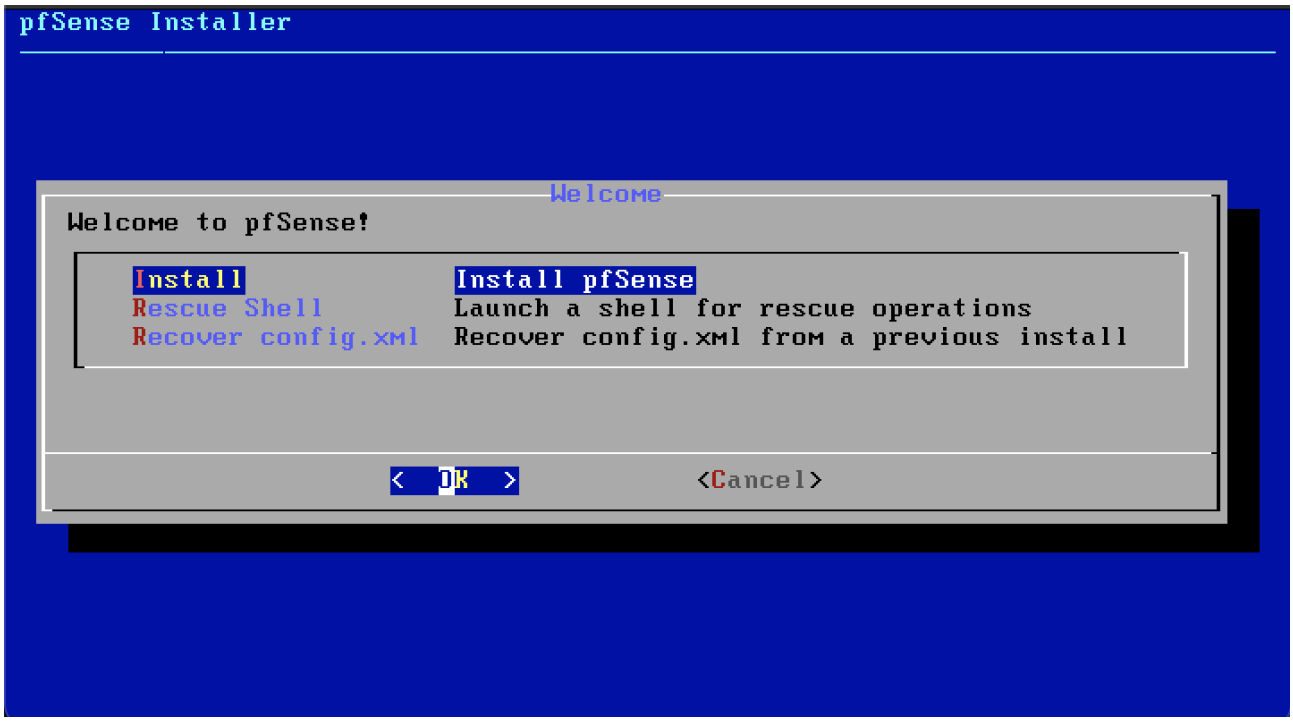
Voici l'écran lors du lancement de l'installation, automatiquement le choix se fera sur 1. si vous ne touchez à rien, et c'est ce que nous souhaitons pour notre procédure.



Acceptez :



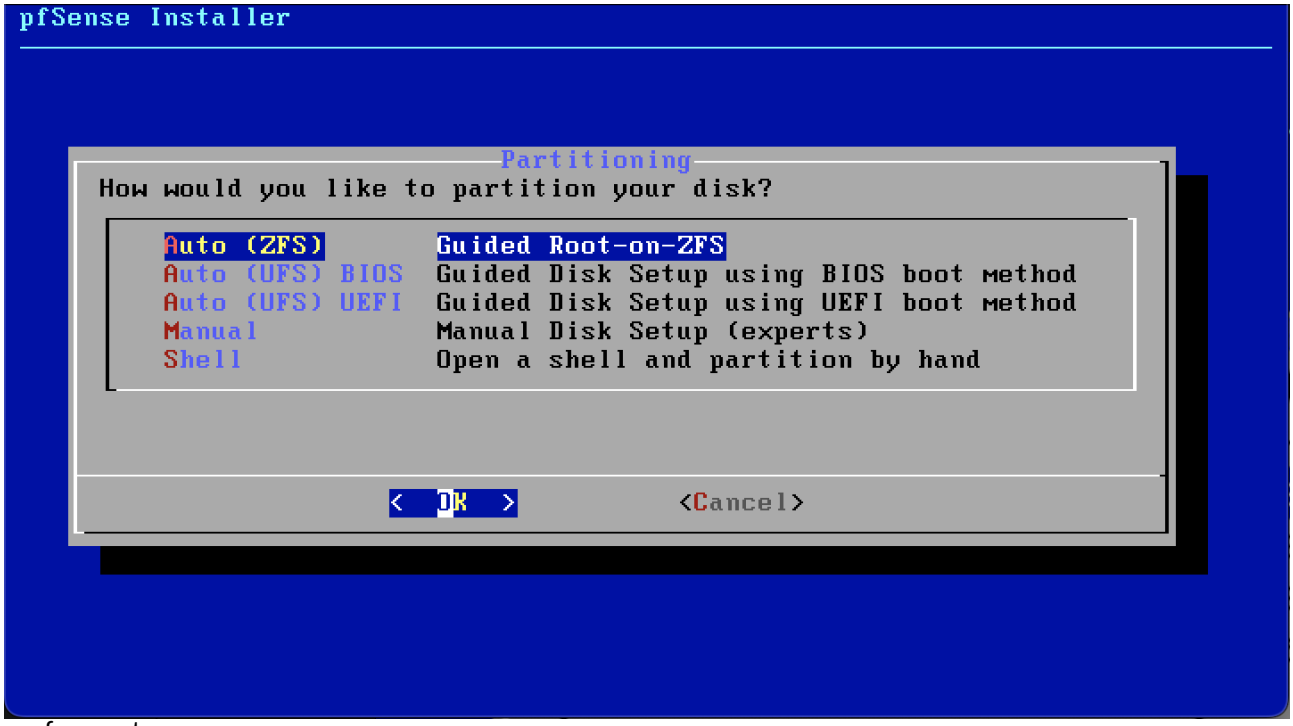
L’installation se fera à l’aide du clavier uniquement, appuyez sur entrée.



Nous choisissons maintenant la disposition du clavier afin qu’elle corresponde aux caractères :

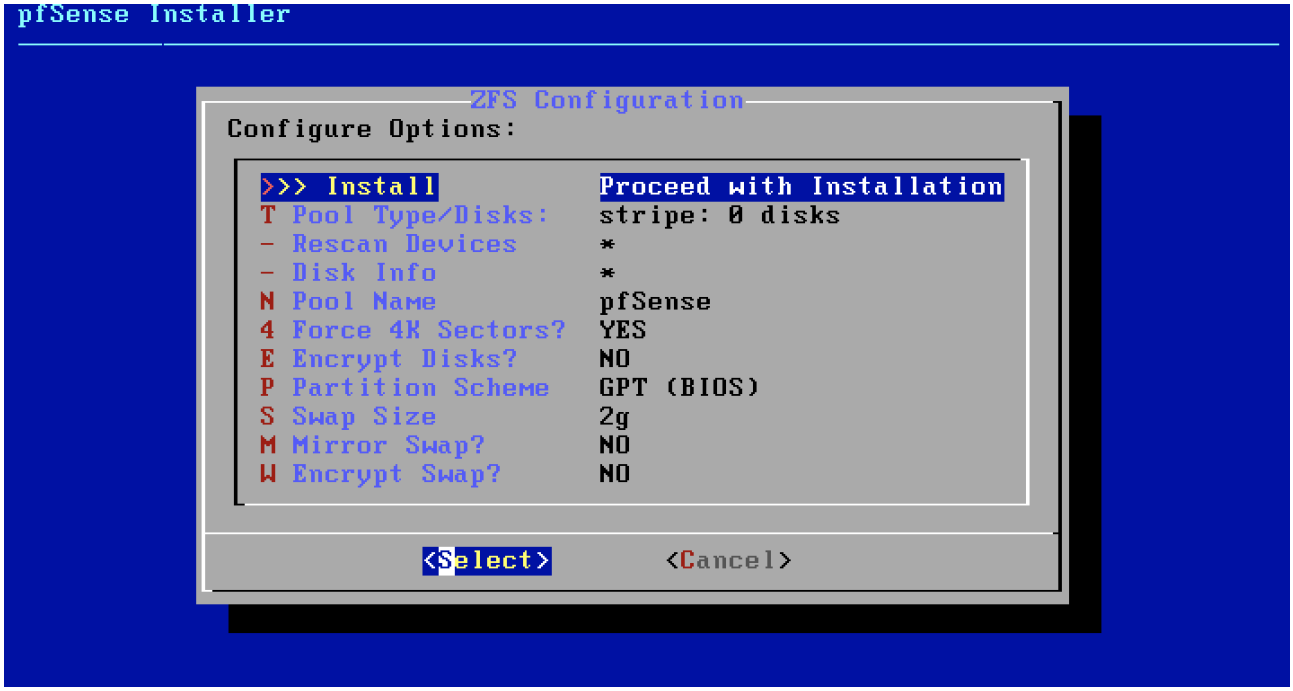

pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with fr.macbook.kbd keymap
->- Test fr.macbook.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
13%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

Nous choisissons le premier paramètre pour procéder à l'installaion ; **Guided Root-On-ZFS** facilite l'installation de pfSense en utilisant ZFS pour un système plus fiable, sécurisé, et

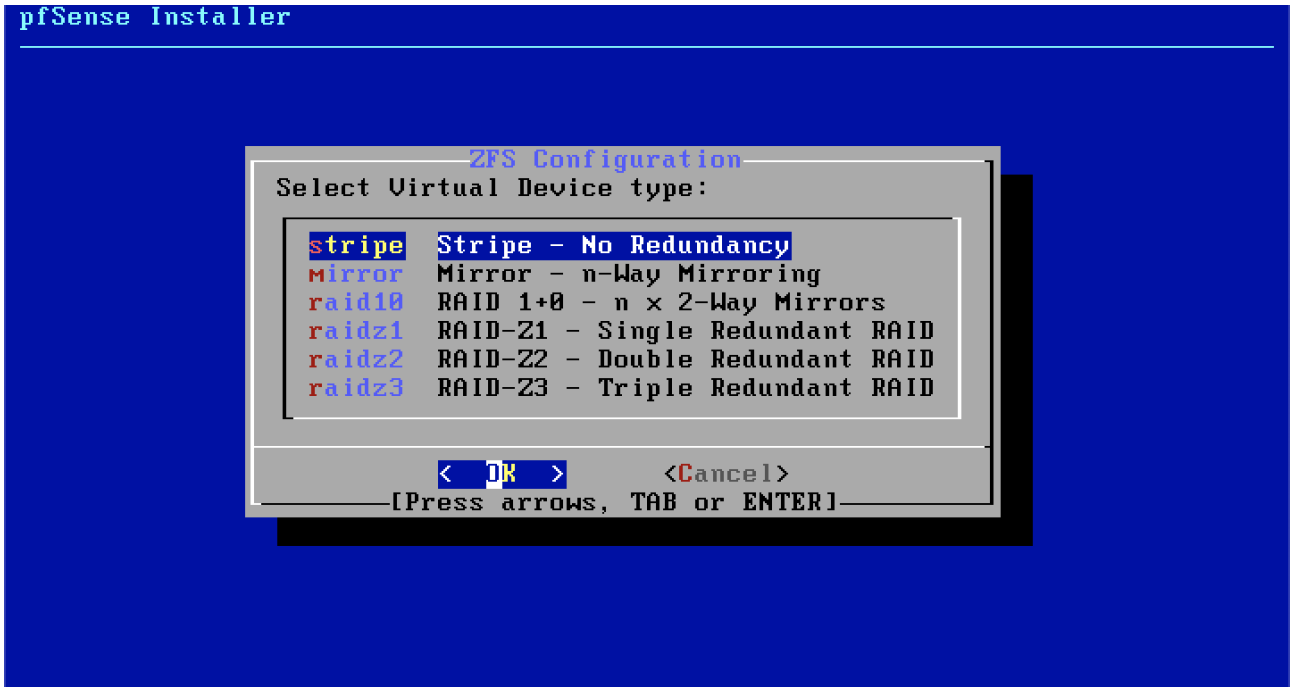


performant.

Nous laisserons les paramètres de base pour le système de gestion de fichiers.

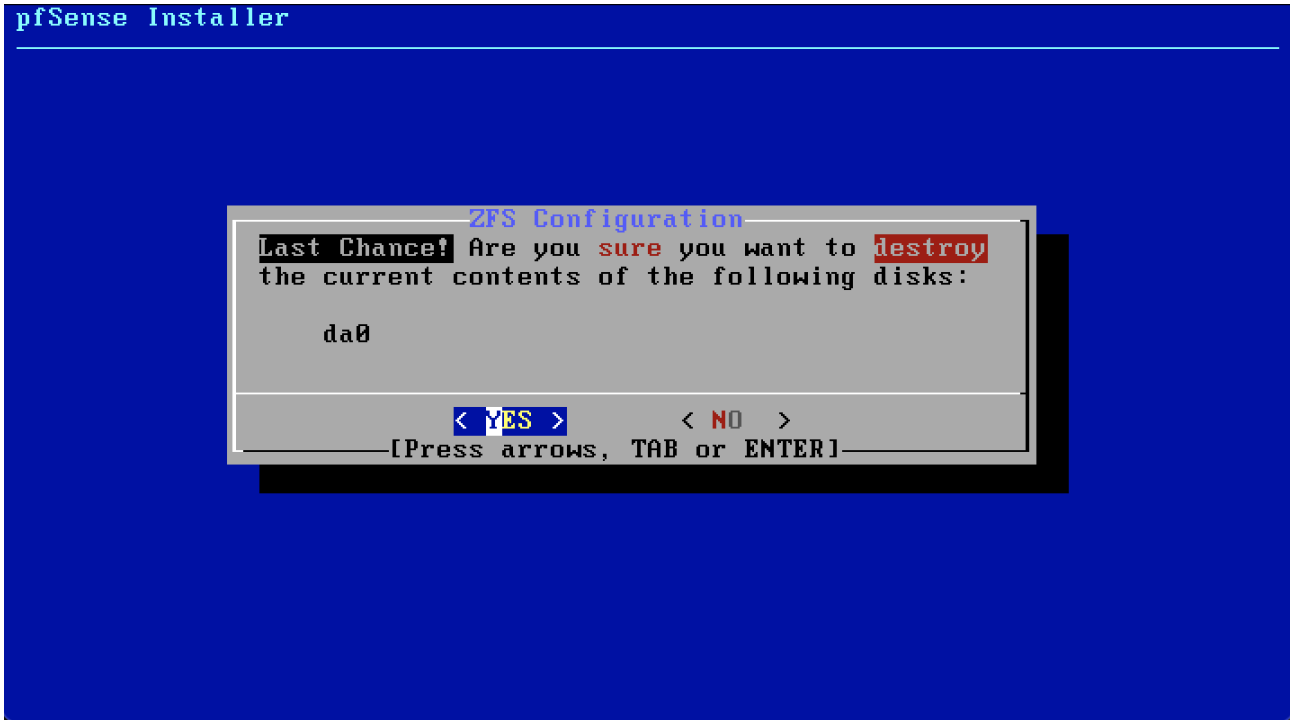


Aucun RAID ne sera configuré sur ce système, aucune redondance n'est nécessaire ; sélectionner le premier paramètre.

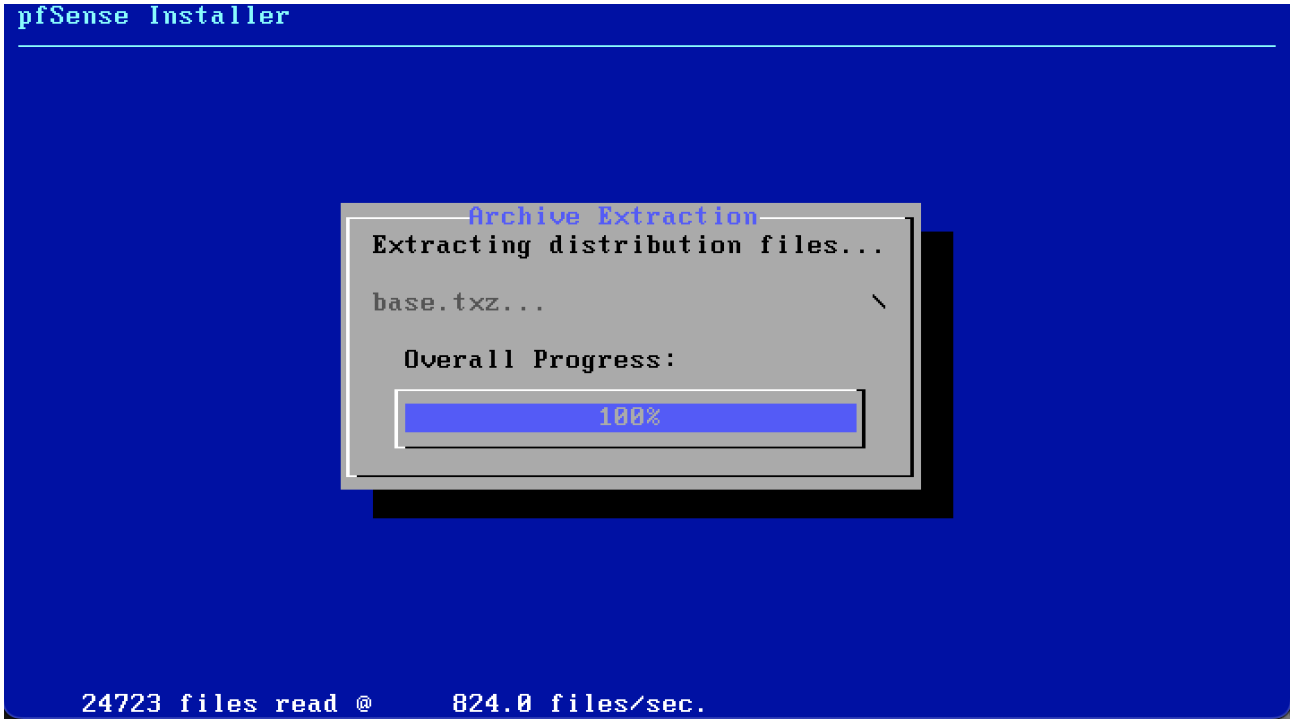


Avec la touche espace, sélectionnez le disque d'installation puis appuyez sur entrée pour valider.

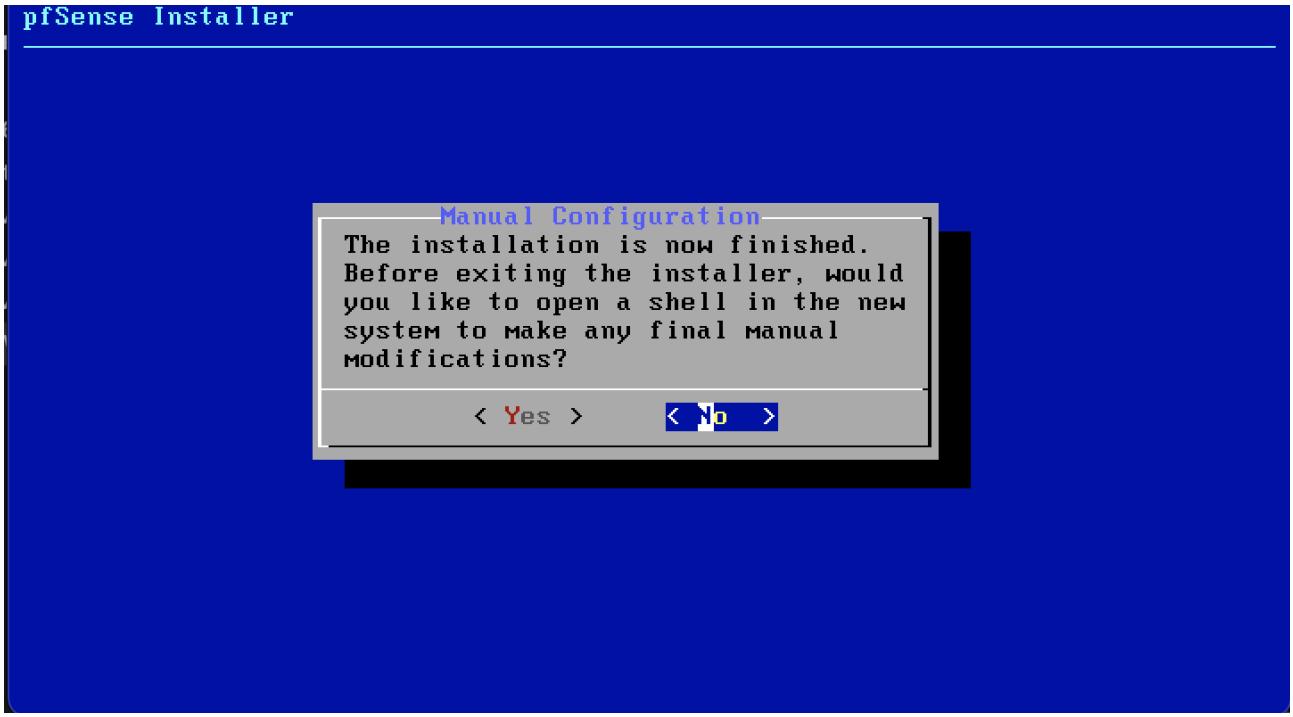
Nous procédons à une installation avec un disque vierge, nous sommes donc sur de vouloir écraser les données sur le disque.



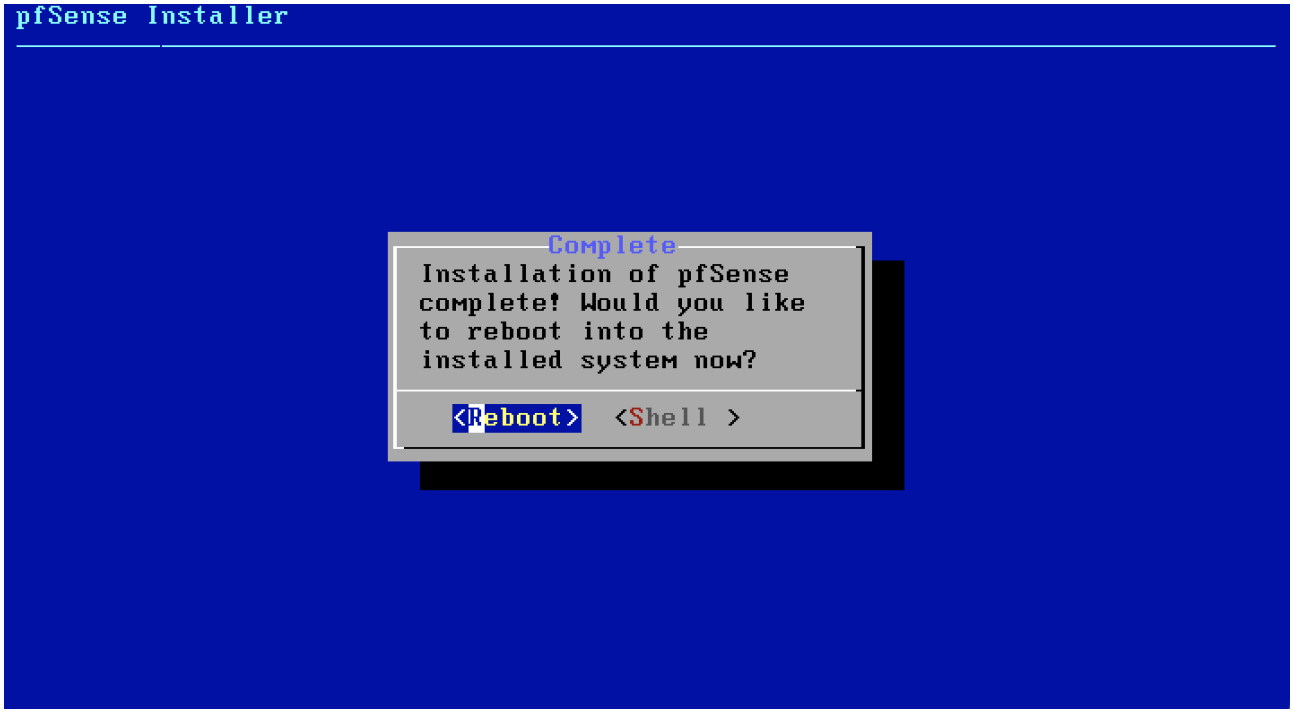
Laissons l'installation se finaliser…



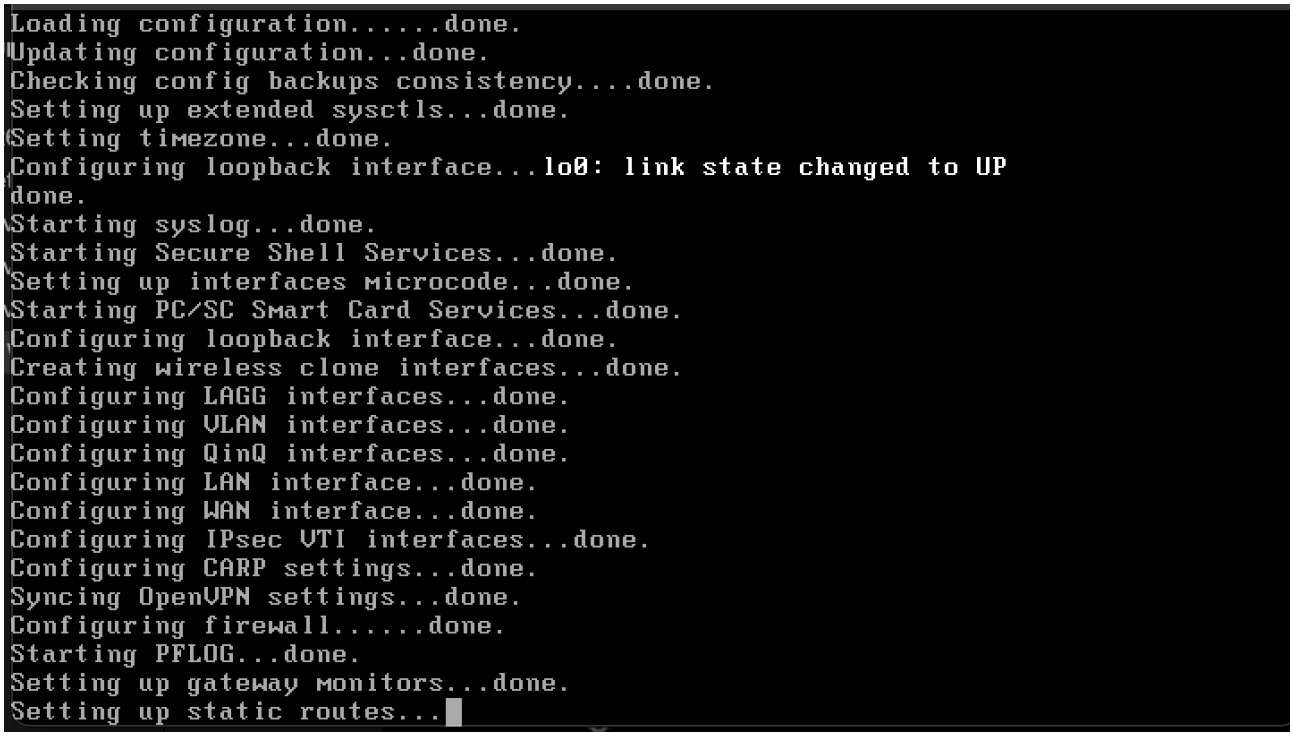
Nous ne souhaitons pas ajouter de paramètres supplémentaires donc choisissons « No ».



Procédons au redémarrage le machine.



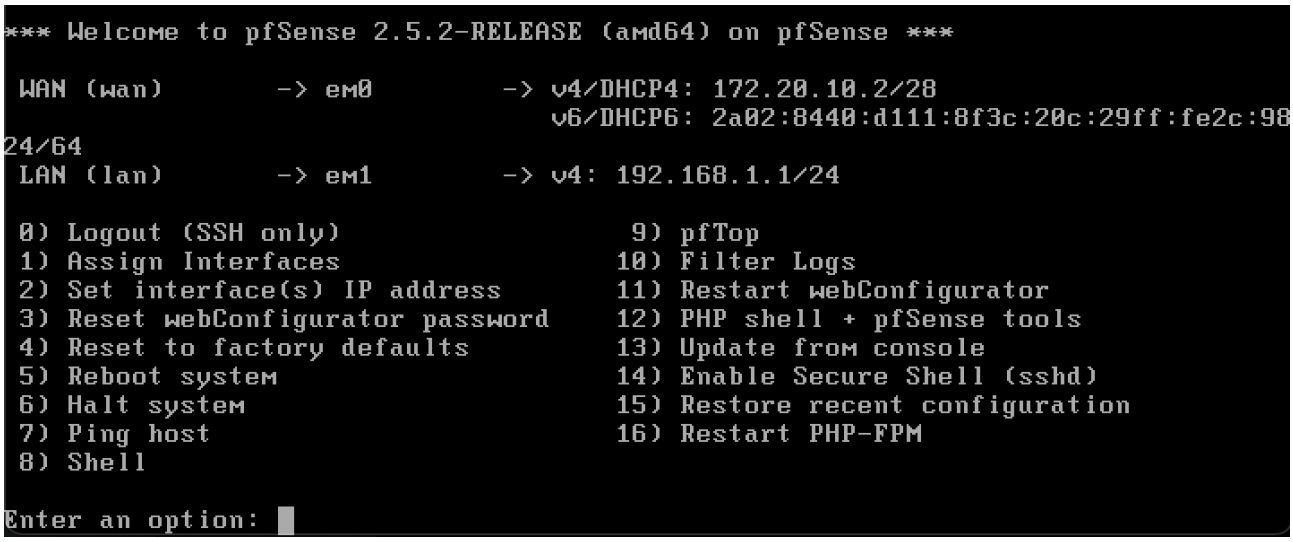
Nous voyons que les étapes de configurations sont bien effectuées sans erreurs au redémarrage :



Et voici finalement la configuration de nos réseaux ;

- @LAN : 192.168.1.0/24
- @WAN : 172.20.10.2/28

Et notre PfSense, avec pour adresse IP : 192.168.1.1



5. Installation de Windows Server 2022

Détails du système :

La plateforme Windows Server permet de créer une infrastructure d'applications, réseaux et services web connectés, du groupe de travail au centre de données. Elle fait le lien entre les environnements locaux et Azure, ajoute des couches de sécurité et vous aide à moderniser vos applications et votre infrastructure.

Windows Server 2022, lancé en **août 2021**, est un système d'exploitation serveur de Microsoft qui succède à Windows Server 2019. Il apporte des améliorations en **sécurité** (Secure Core Server, HTTPS SMB), **virtualisation** (meilleure intégration avec Azure, Hyper-V amélioré), **stockage** (Storage Migration Service amélioré, support SMB Direct), et **réseau** (SDN, DNS amélioré). Disponible en éditions **Standard**, **Datacenter**, et **Datacenter: Azure Edition**, il prend en charge une interface graphique ou une installation en mode **Core** pour des performances optimisées.

Pour notre cas de figure, nous choisirons une installation de type **Standard**, installé **graphiquement**.

L'image disque de ce système est disponible au téléchargement gratuit grâce au centre d'évaluation, en version d'essai d'une durée de 180 jours. (ISO WIN SRV 22)

Les licences pour une pleine utilisation sont, elles, disponible à l'achat sur le site officiel de Microsoft, par lots. (Licence WIN SRV 22)

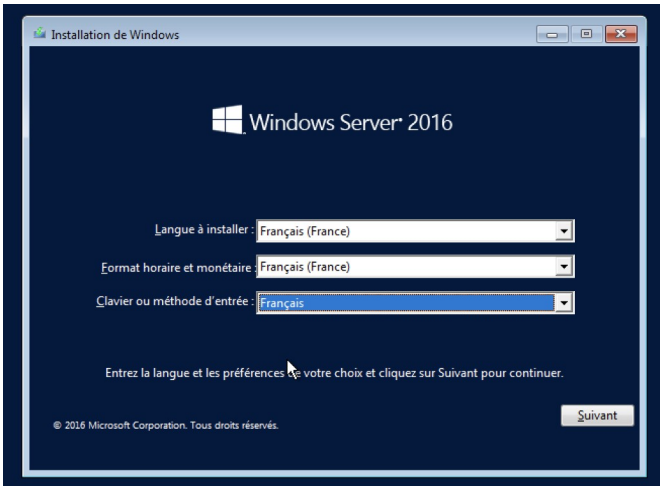
Pré-requis logiciel et matériel :

Les pré-requis pour l'installation de ce système sont les suivants ;

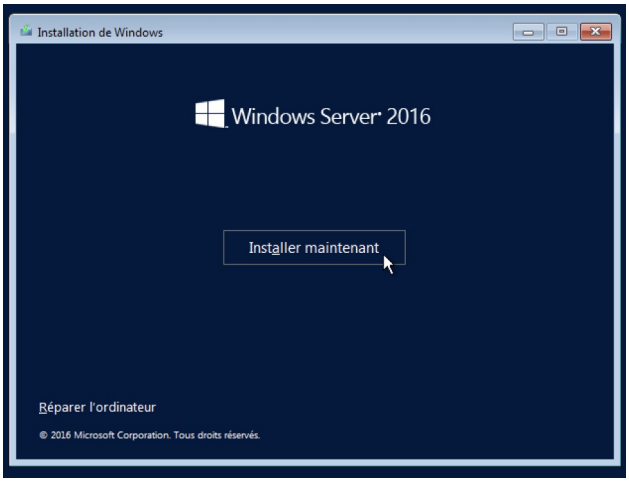
- CPU : 1.4 GHz x64.
- RAM : 2 Go à 4 Go.
- Stockage : 32 Go.
- Boot : ISO sur support amovible bootable d'au moins 8 Go.

Installation du système :

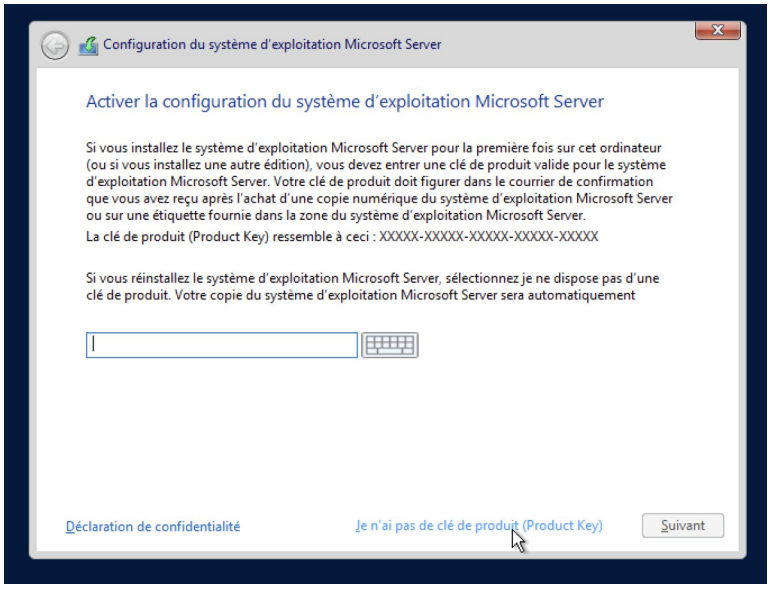
Sélectionnons la langue d'installation, ici, **Français**.



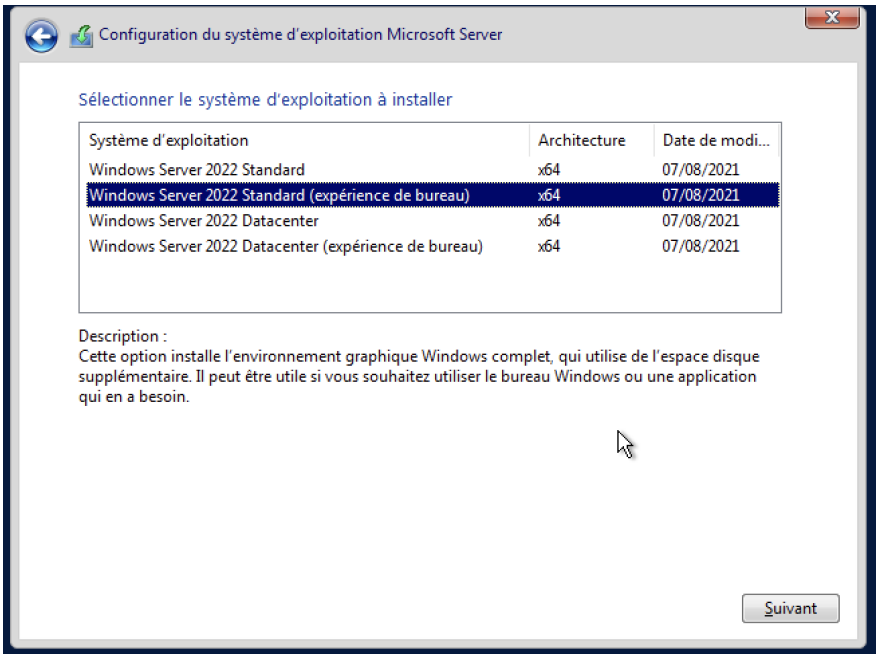
Sélectionner **« Installer maintenant »**.



Il nous est désormais demandé de saisir une clé de licence Windows qui activera la version que vous avez acheté. Dans notre cas nous allons sélectionner **« Je n'ai pas de clé de produit (Product Key)**, nous permettant d'utiliser la version d'essai pour une période de 180 jours.

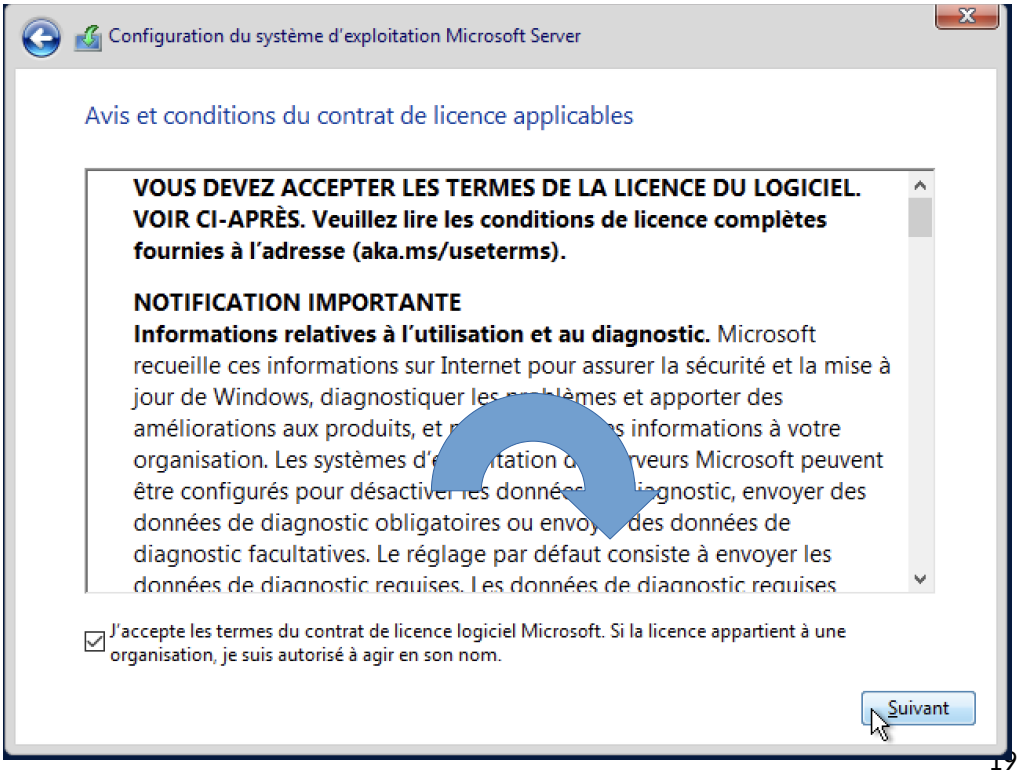


Nous pouvons continuer le processus d'installation, et comme indiqué précédemment dans la documentation, nous choisirons ici le système d'exploitation : **Windows Server 2022 Standard (expérience de bureau)**.

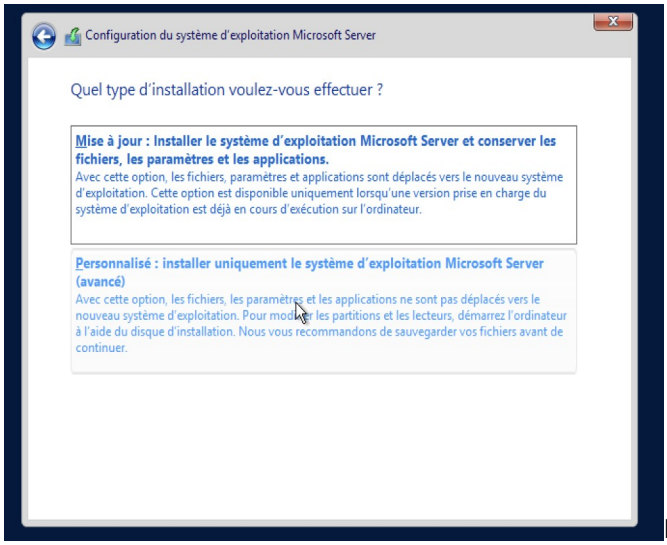


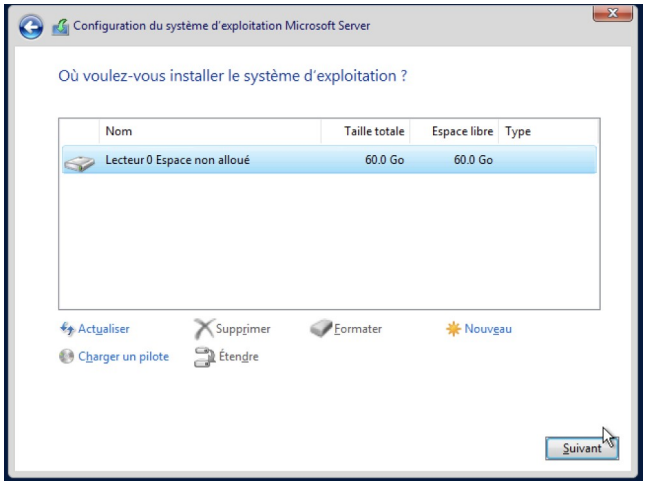
Nous acceptons évidemment les termes du contrat de licence logiciel Microsoft.

Nous pouvons désormais choisir la méthode

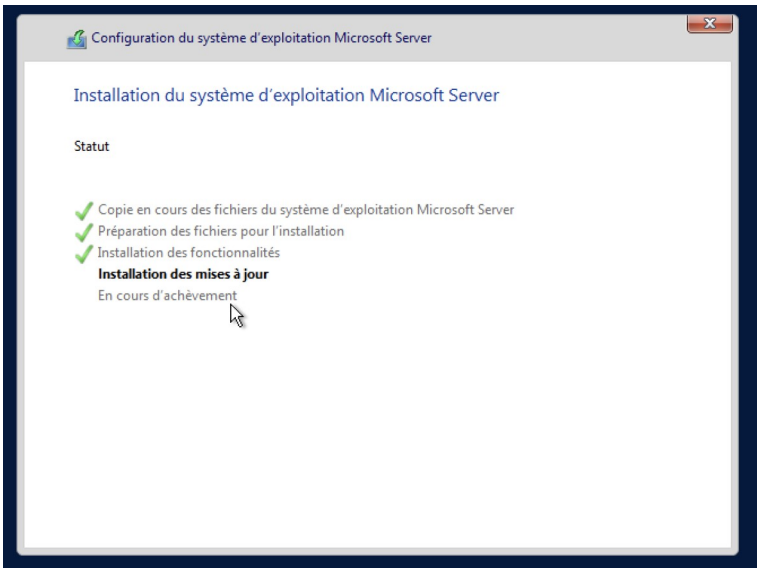


d’installation, je choisi ici la méthode avancée afin de pouvoir visualiser mes disques et sélectionner le correspondant.





L’installation procède alors ;



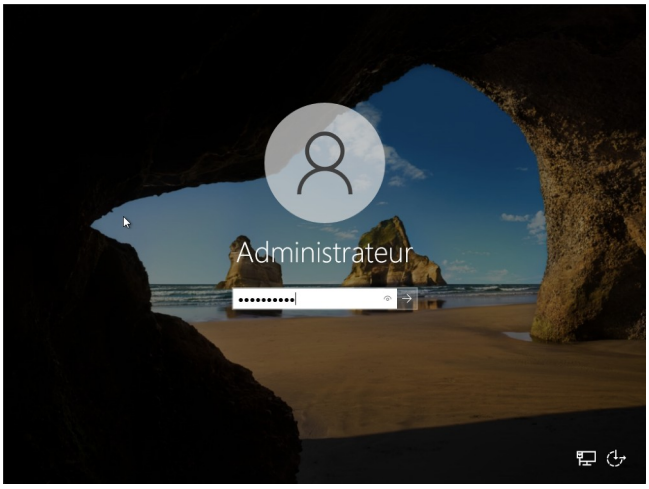
à la fin de laquelle, il vous est demandé de saisir un mot de passe pour votre compte Administrateur.

Afin de mener à bien la sécurité de votre serveur, il vous est conseillé de mettre en place un mot de passe correspondant à certaines caractéristiques, tel que ;

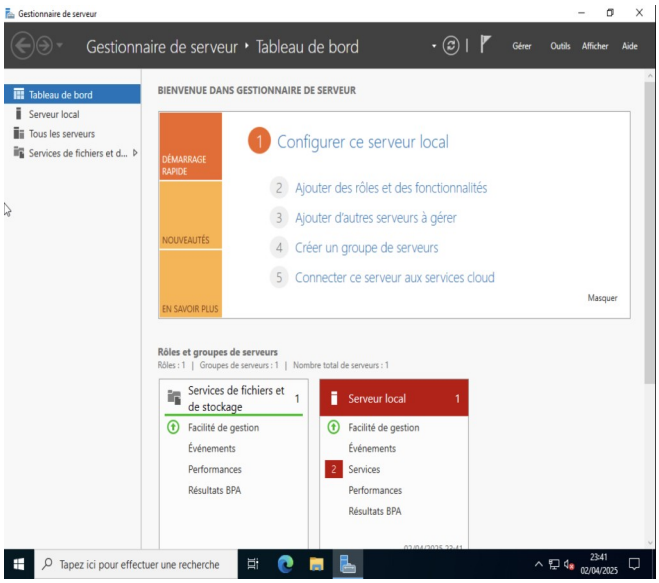
- longueur du mot de passe entre 12 et 16 caractères

- utiliser une combinaison majuscules, minuscules et caractères spéciaux (ex : !, @, $, %,)
- éviter les suites de chiffres ou mot courants
- essayez d'utiliser des mots de passe uniques

Nous voici désormais sur l'écran d'authentification, connectez vous.



Voilà, l'installation du système d'exploitation est terminée.

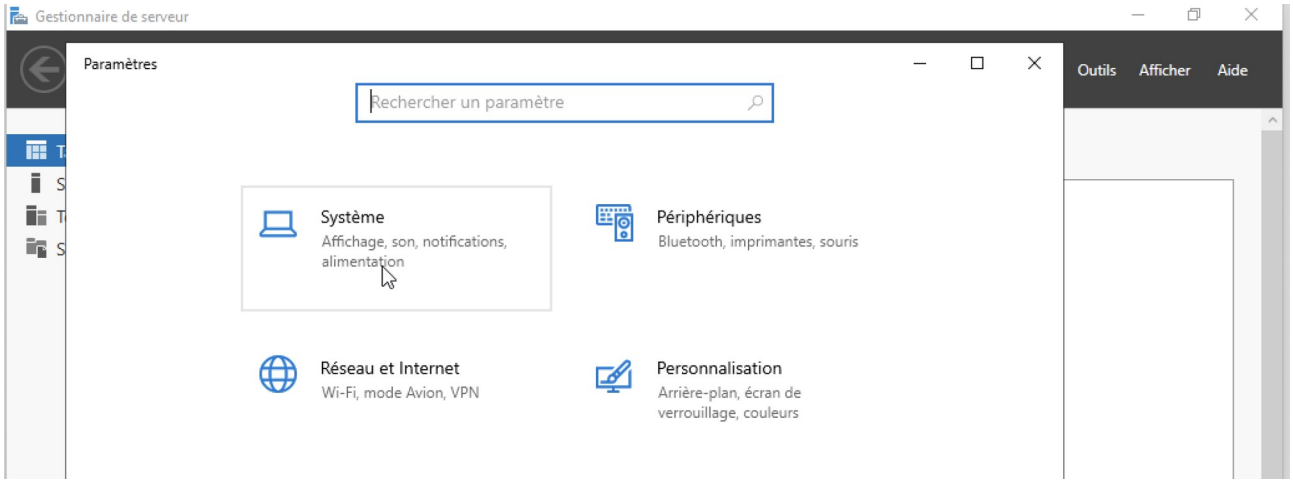


L'utilité d'un serveur Windows réside dans ses fonctionnalités et services qui permettent de gérer efficacement un réseau. Cela inclut la gestion des utilisateurs **(Active Directory)**, le partage de fichiers **(File Services)**, la virtualisation **(Hyper-V)** par exemple.

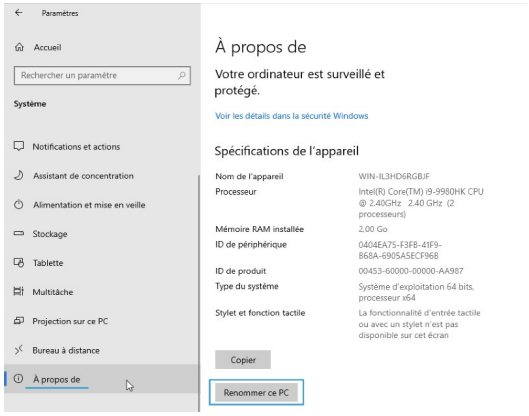
Configuration du système :

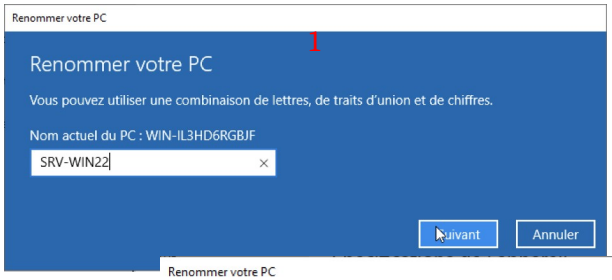
Il est cependant important de bien configurer plusieurs paramètres afin de s'assurer du bon fonctionnement de celui-ci et d'avoir une organisation propre ainsi qu'une dénomination cohérente.

Nous allons alors premièrement renommer notre serveur en **SRV-WIN22** ; pour ceux faire, il faut se rendre dans le menu des paramètres, dans la section **Système**:

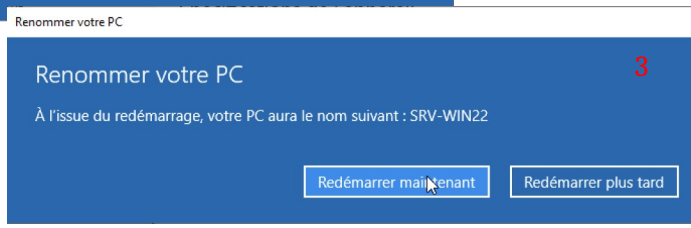


Puis dans l'arborescence à gauche, sélectionner **A propos** puis dans cette section, cliquer sur **Renommer ce pc**.





2



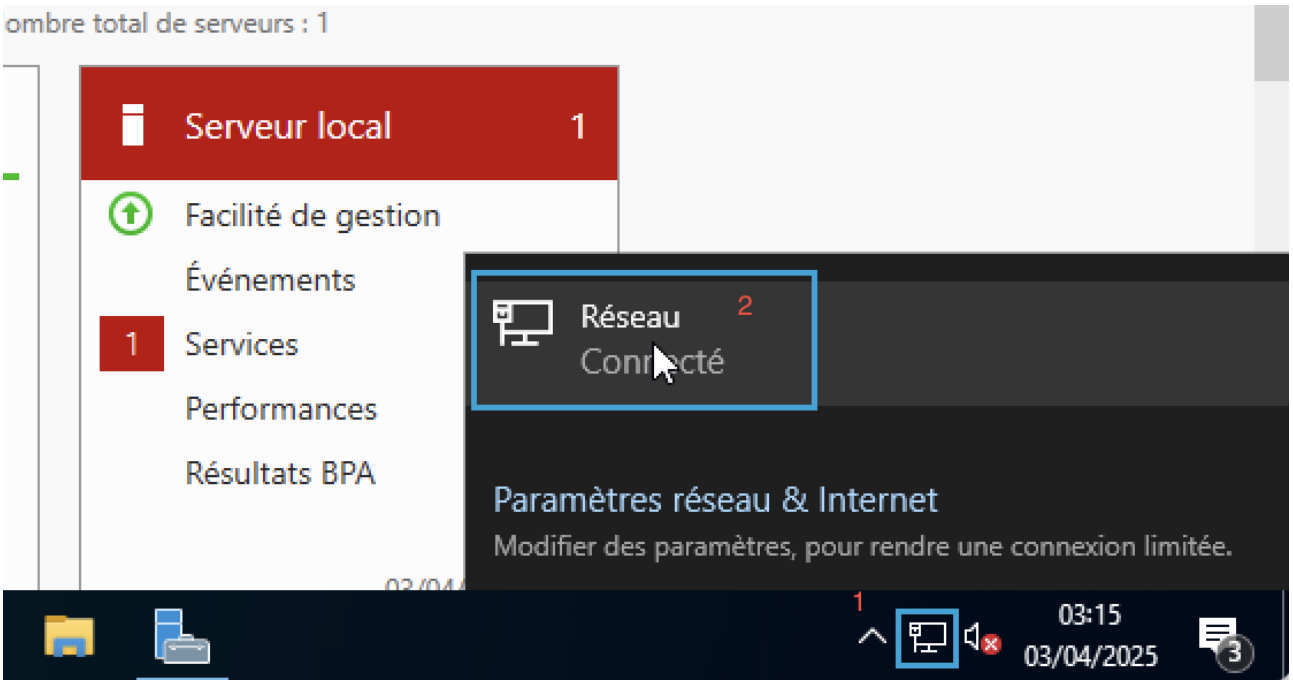
Pour plus de praticité et d'efficacité, il est vivement recommandé de fixer l'IP de son serveur. En effet certains services comme Active Directory, DNS, ou DHCP nécessitent par exemple d'avoir une IP statique et non dynamique.

Nous allons donc définir l'IP de notre machine.

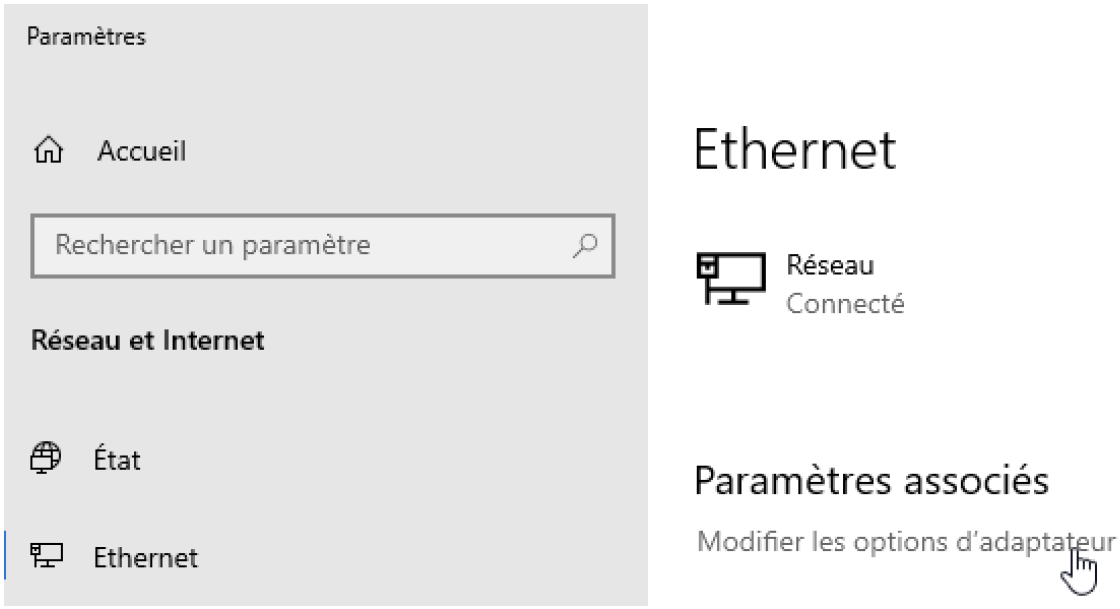
Elle prendra alors l'adresse suivante : **192.168.1.10/24**

Voici comment procéder ;

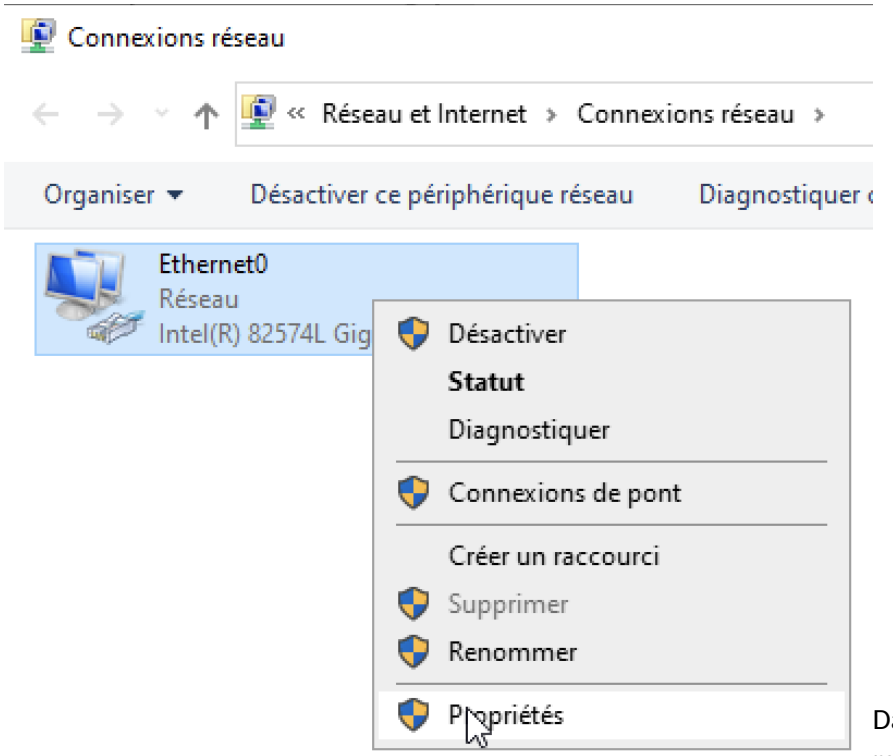
Cliquez sur l'icône réseau à droite de votre barre des tâches, puis cliquez sur le réseau auquel vous êtes connectés :



Le menu des paramètres réseaux s'ouvre, dans l'onglet **Ethernet** nous allons sélectionner **« Modifier les options d'adaptateur »** sous le titre Paramètres associés :

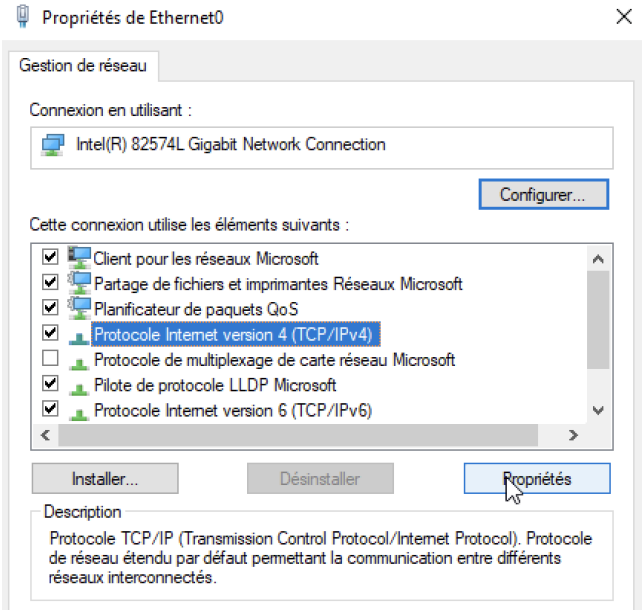


Une nouvelle fenêtre s'ouvre alors présentant vos adaptateurs réseaux, sur lequel nous allons faire un clic droit afin d'ouvrir les propriétés.



Dans les propriétés de mon interface, je

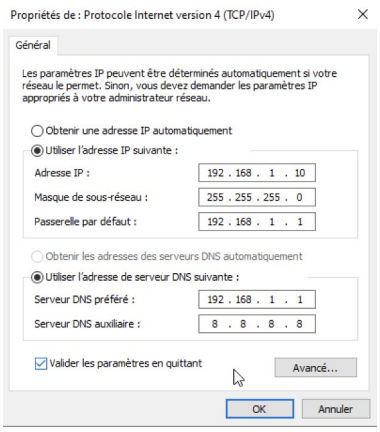
cherche l'élément **Protocole Internet version 4**, plus communément appelé **IPv4**. Nous sélectionnons l'élément puis cliquons sur **« Propriétés ».**



La fenêtre de paramétrage d'adresse ip s'ouvre alors, dans laquelle nous allons renseigner les champs correspondants avec les informations précédemment détaillées.

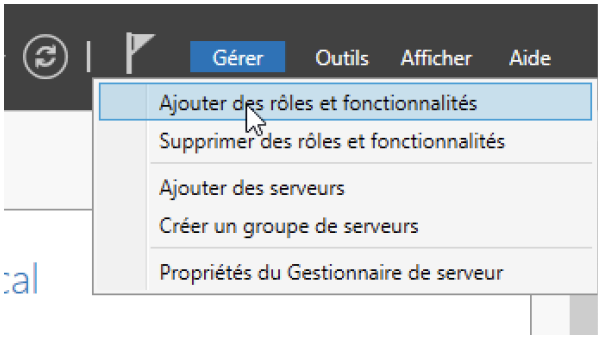
La passerelle sera l'adresse de mon PfSense qui, dans mon cas actuel, fais office de routeur (ainsi que de DNS le temps d'installer ce service sur notre serveur Windows) et donc de passerelle vers le réseau NAT. La documentation de celui-ci est disponible dans la liste de PPE.

Voici donc les paramètres que j'enregistre avant de quitter la fenêtre de configuration ;

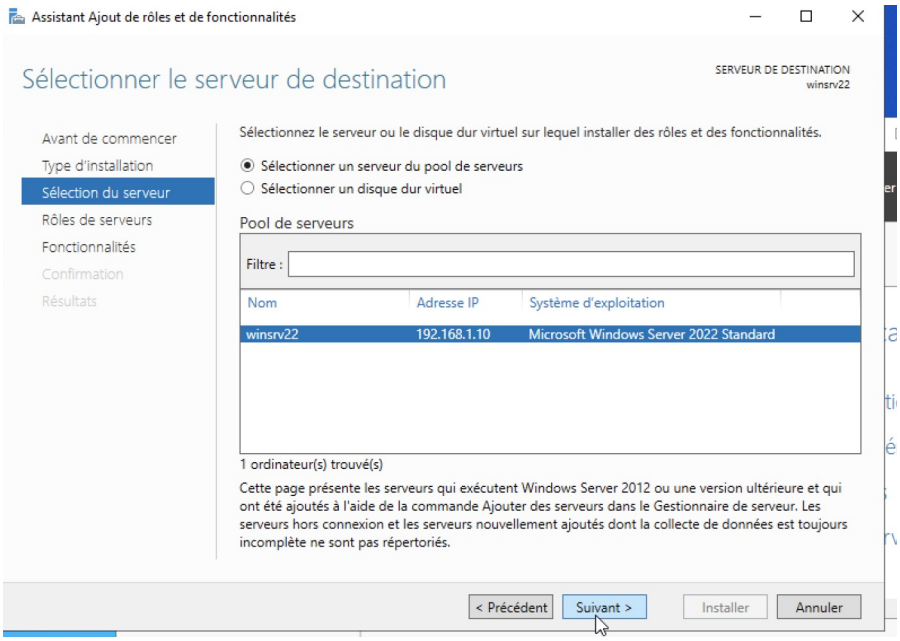


6. Configuration des Services Réseau (AD DS, DNS)

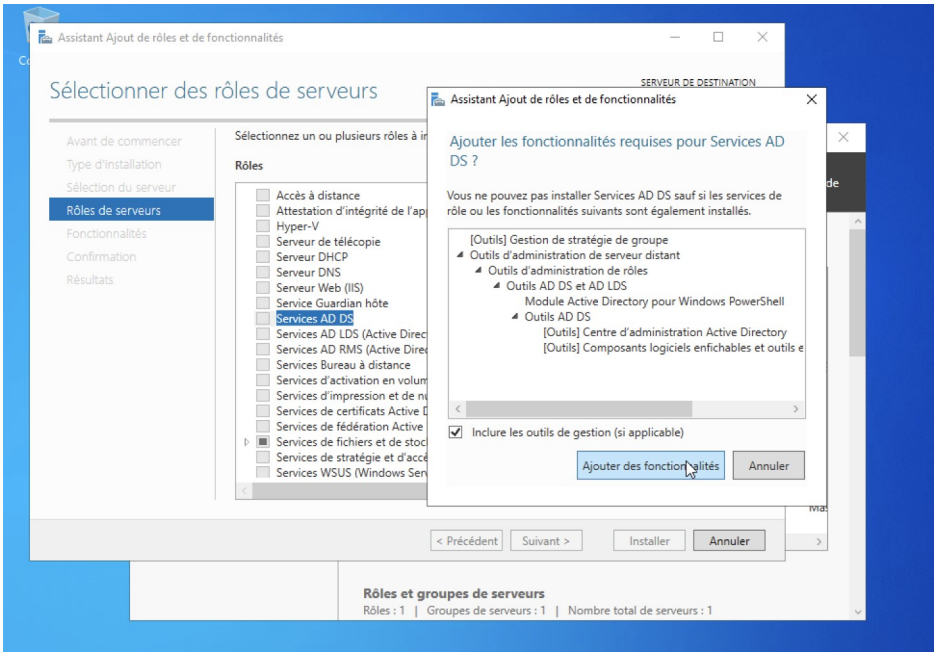
Sur votre machine Windows SRV, cliquez sur l'onglet « Gérer » puis cherchez le paramètre « Ajouter des rôles et fonctionnalités ».



Cliquer sur suivant jusqu'au choix de serveur, choisissez le votre puis appuyez une troisième fois sur le bouton suivant.



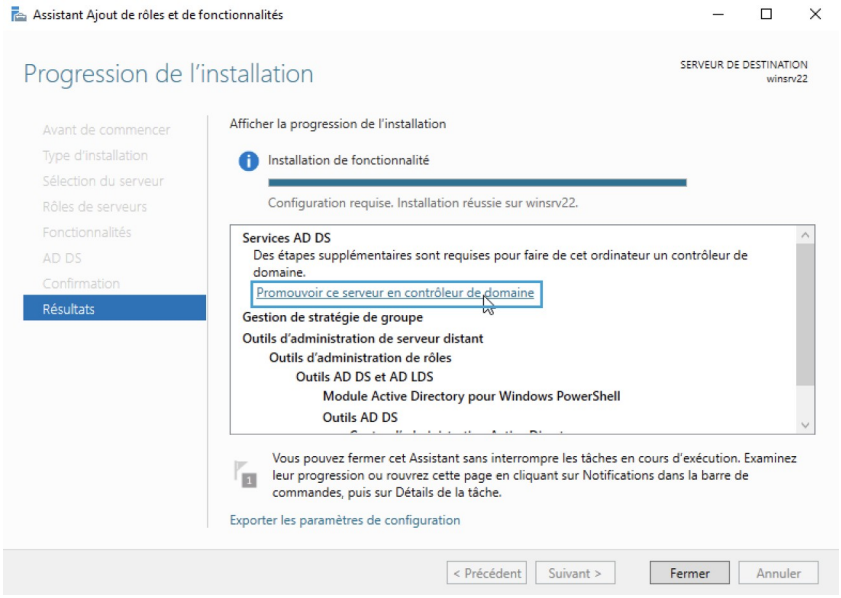
Vous voyez désormais une liste de services et fonctionnalités, dans laquelle nous choisirons celui qui nous intéresse, puis sélectionner **« Ajouter des fonctionnalités »**.



Vous pouvez désormais cliquer le bouton suivant, jusqu'au bouton **« Installer »**.

A l'issu de cette installation, un paramètre nous est propose, surligné et souligné en bleu ;

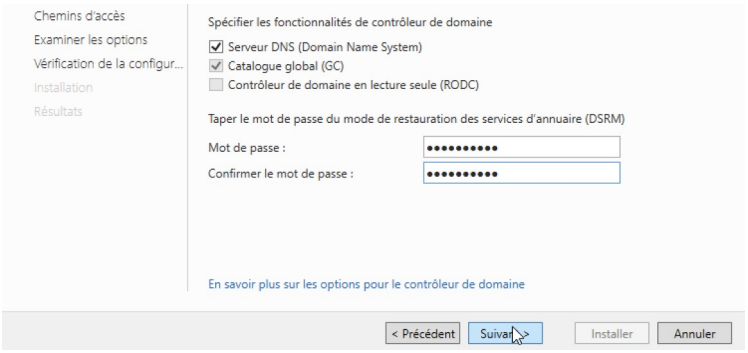
Promouvoir ce serveur en contrôleur de domaine, nous cliquerons sur celui-ci.



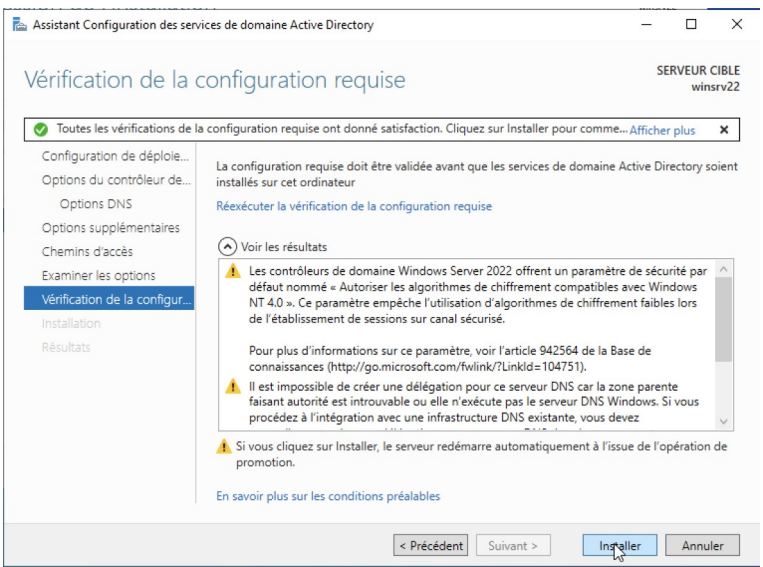
Le contrôleur de domaine permet donc **d'organiser et de sécuriser toutes les données**. Le contrôleur de domaine est le coffret qui contient les clefs du royaume : l'Active Directory.

Nous devons désormais créer le domaine racine, et donc la forêt. Ceci constituera la base de notre **Active Directory**. Nous appellerons notre domaine racine : **HORIZON.lan**.

Vous pouvez désormais cliquer sur suivant puis il vous sera demandé de renseigner un mot de passe robuste (1maj, 1min, 1chiffre, 8carac)



Une dernière vérification est alors effectuée pour vérifier qu'aucun problème n'est remonté lors de l'installation

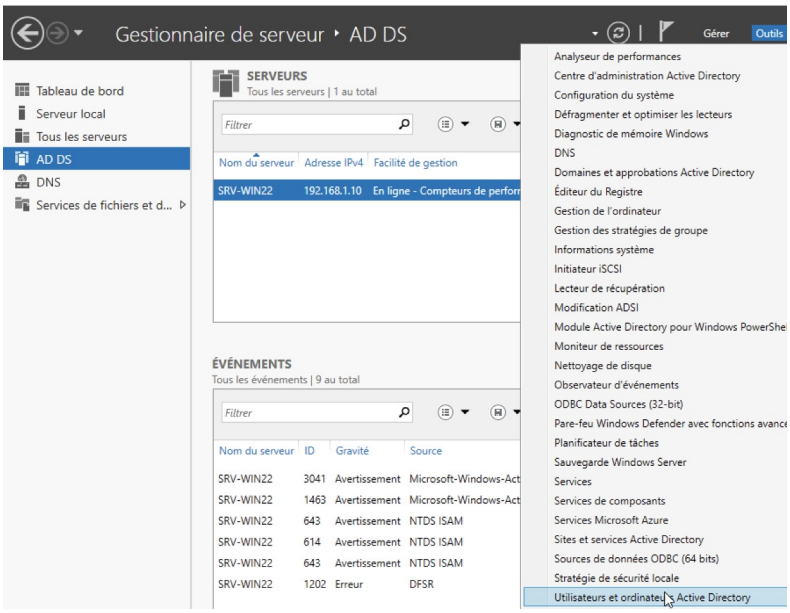


Voici notre écran de connexion lors du redémarrage, nous constatons que le domaine s'est bien lié à notre serveur.

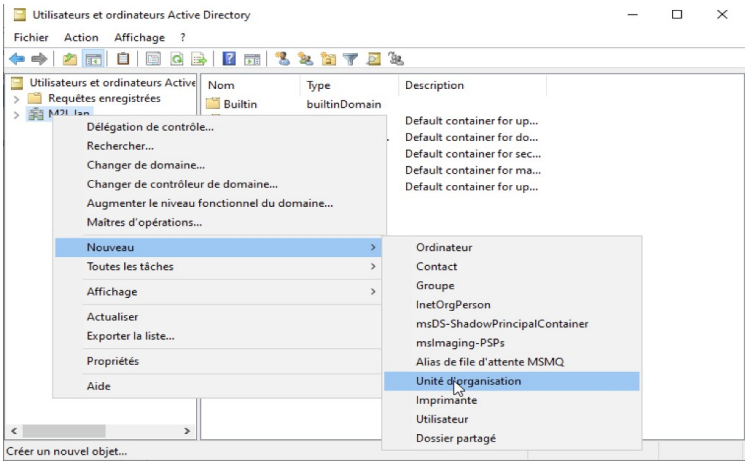
En effet, nous procéderons à la connexion du compte administrateur du domaine : **HORIZON.lan**

7. Création d'Utilisateurs et GPO

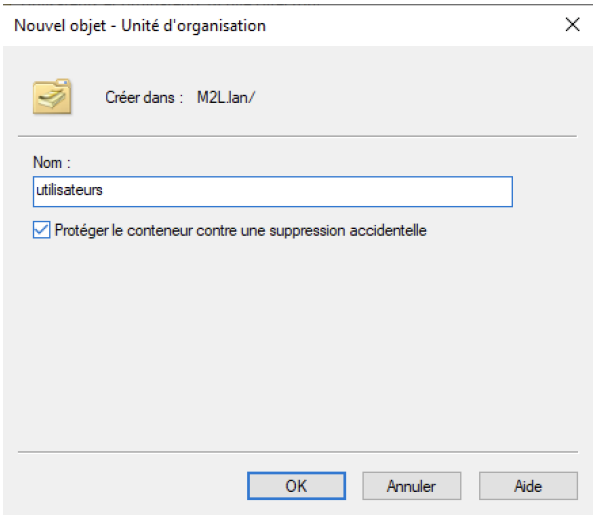
Dans le menu déroulant ; sélectionner le service de gestion d'utilisateurs de l'AD



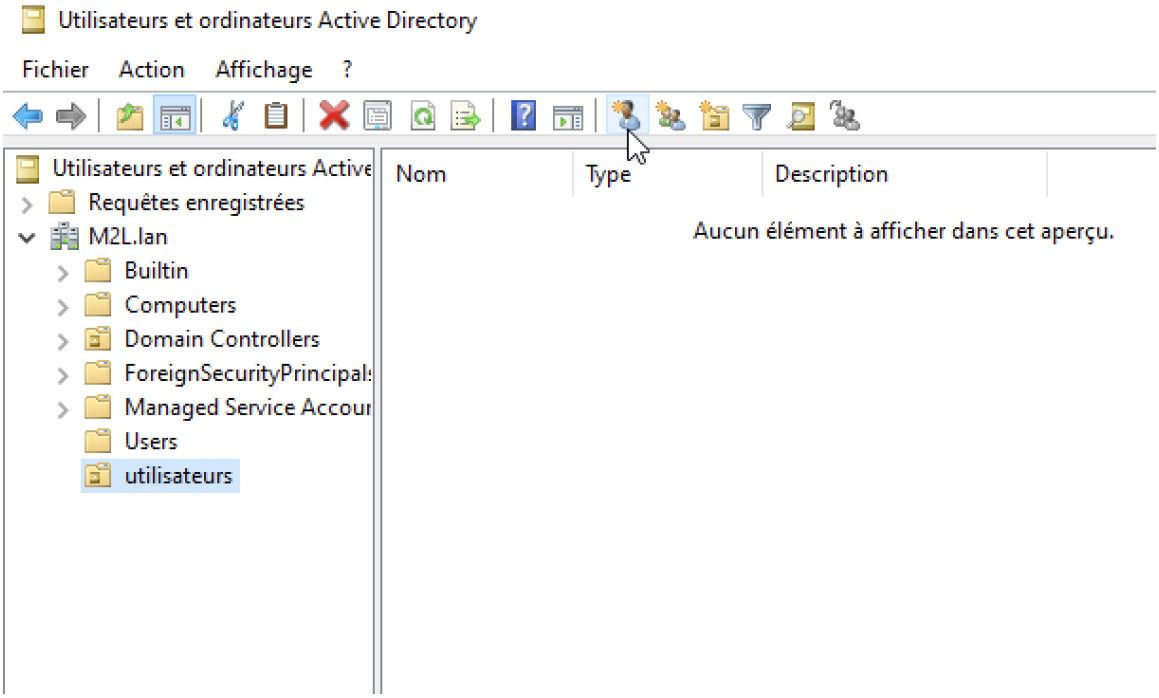
Effectuez un clic droit sur le contrôleur de domaine, survolez **Nouveau** puis cliquez sur **Unité d'organisation.**



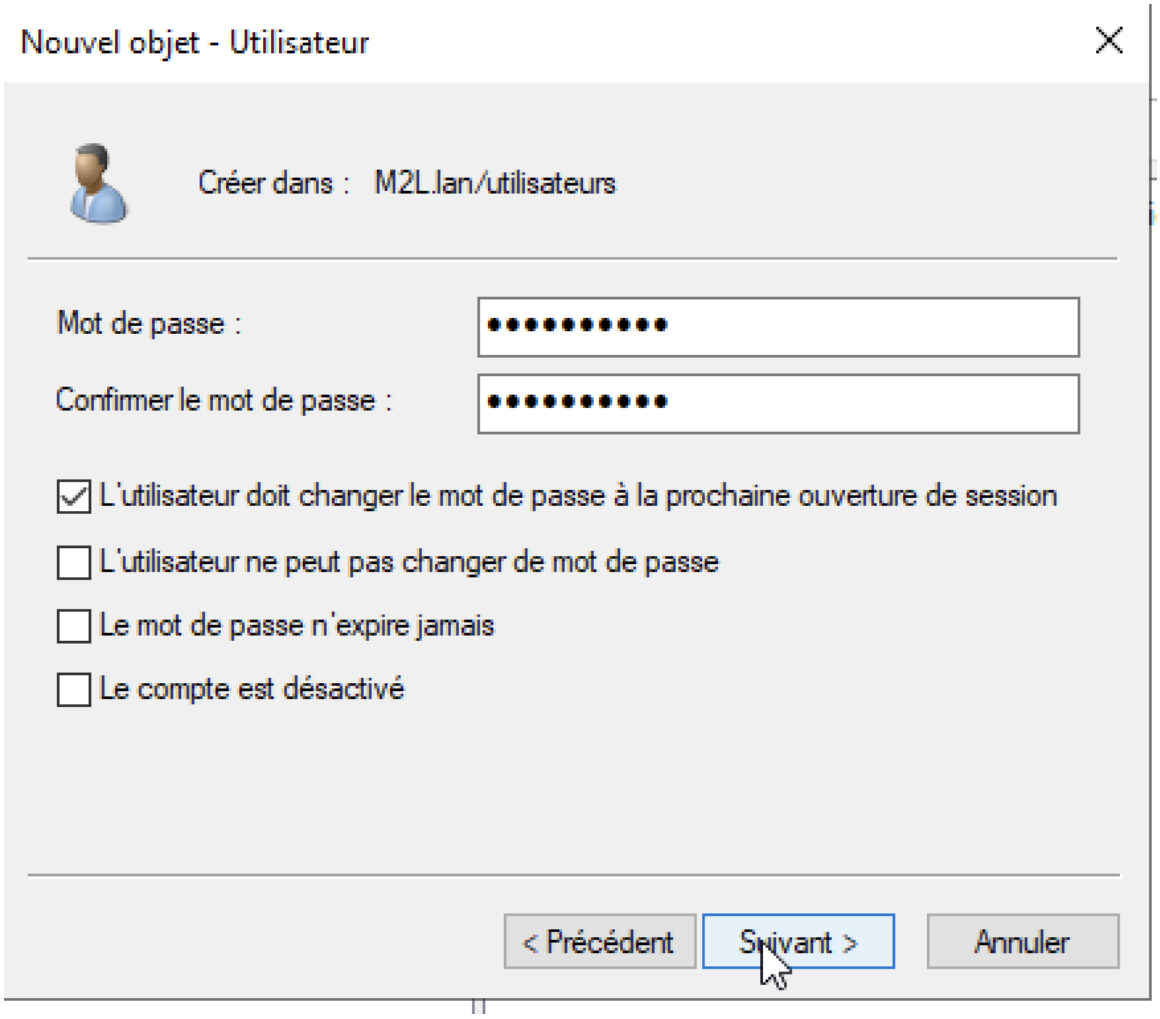
Je l'appelle Utilisateurs et c'est dans cette UO que nous allons créer notre constellation d'UO ce qui nous permettra une organisation optimale de nos utilisateurs.



Cliquez ici pour créer un utilisateur dans l'unité d'organisation que vous avez sélectionné.

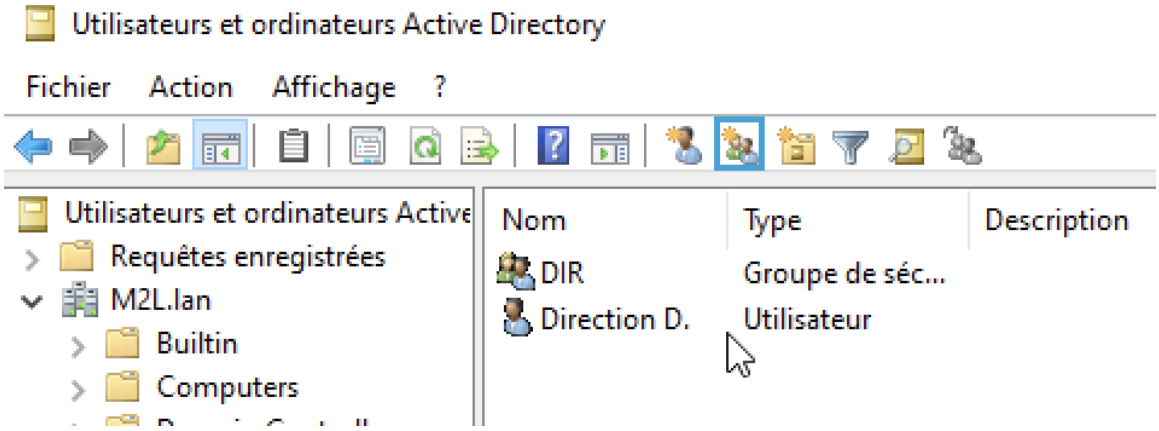


Voici le paramètre important de la création des utilisateurs ; nous favoriserons ici un mot de passe générique, tel que par exemple : m2l.today où « today » correspondrait au jour de la création puis sélectionner l'obligation pour l'utilisateur de changer son mot de passe afin qu'il reste confidentiel et qu'il en soit l'unique détenteur.



Nous allons désormais créer des unités d'organisation correspondantes aux utilisateurs et ainsi, finalement, nous créerons des groupes de sécurité afin de parfaire notre gestion de permissions sur le partage de fichiers.

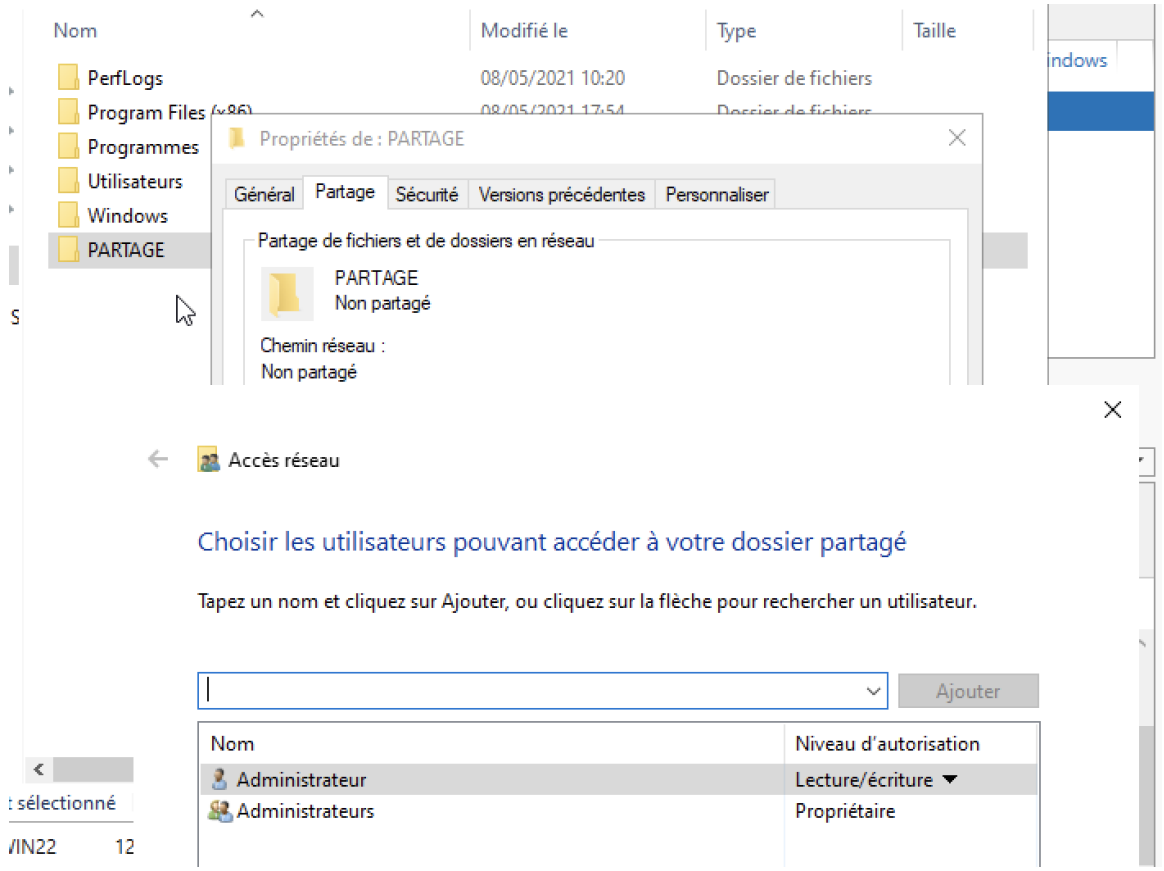
Les partages seront cloisonnés mais la racine restera accessible à tous les utilisateurs, aucun dossier ne sera caché, seulement, chacun de nos utilisateurs auront accès en écriture exclusivement qu'à leurs dossiers et fichiers correspondants. Pour ceux faire, voici comment procéder ;



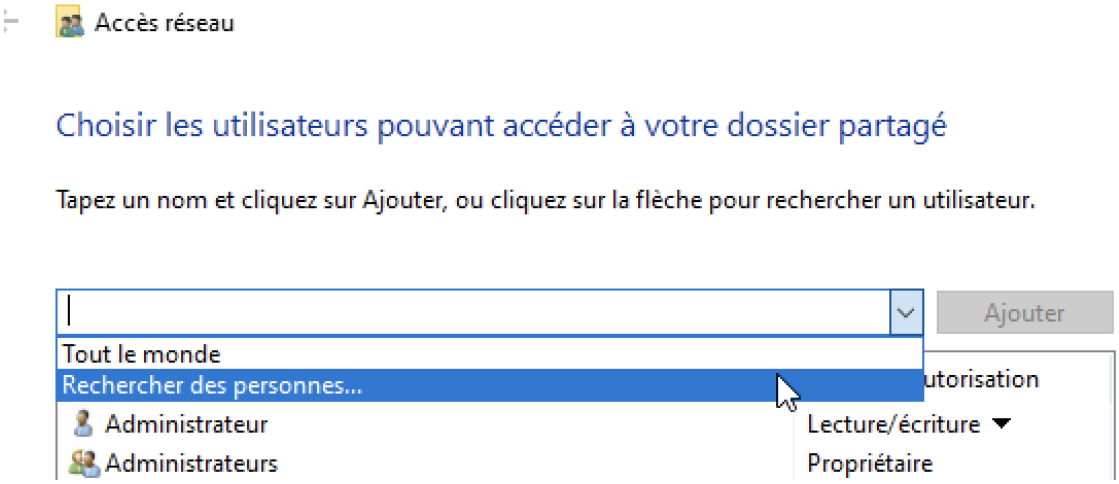
Sélectionnez cette icône encadrée en bleue afin de créer un groupe de sécurité que vous dénommez par le nom du service correspondant.

Je vais aller à la racine de mon ordinateur afin de créer un nouveau dossier et l'appeler « PARTAGE », ce dossier sera accessible en lecture à tous mes utilisateurs. Il sera composé de plusieurs autre fichiers qui auront des droits indépendants à celui ci. Les dossiers seront créés en fonction des différents services et seront administré par les groupes de sécurité précédemment créés.

procédons au partage de fichiers ;

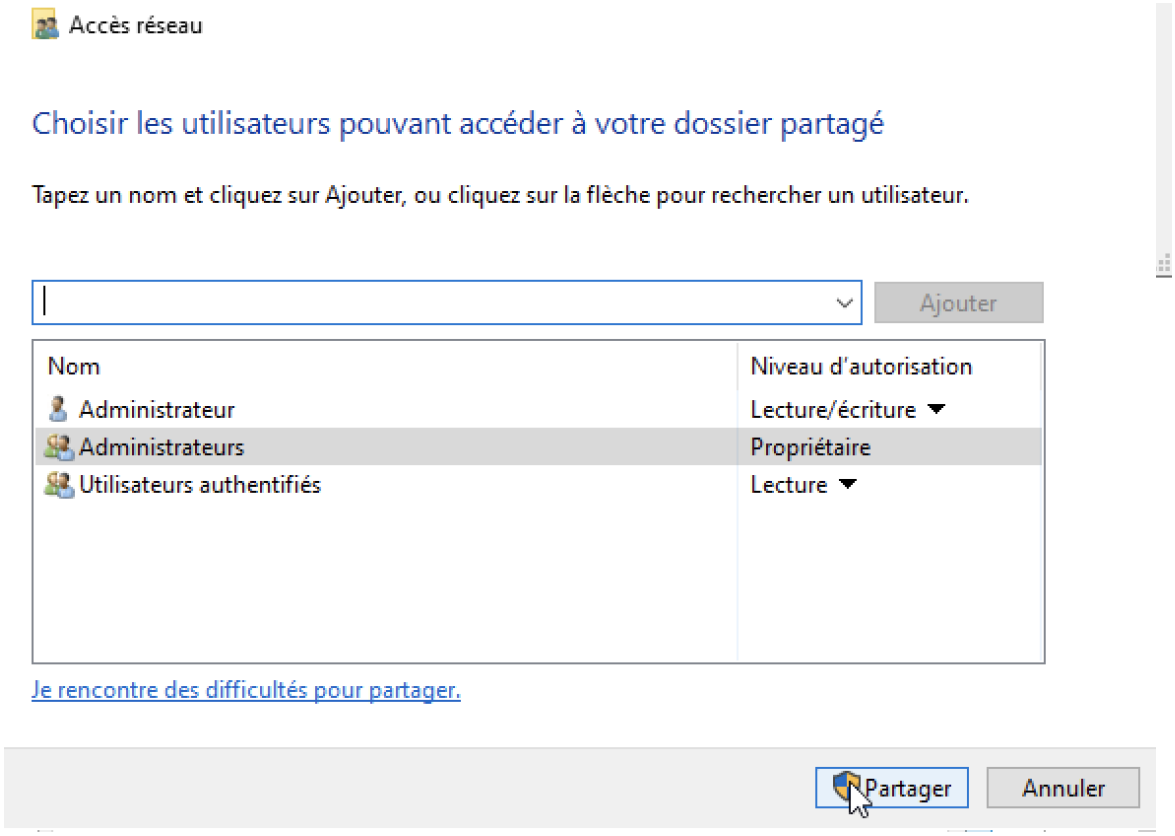


Je clique sur le menu déroulant puis je clique sur rechercher des personnes ;



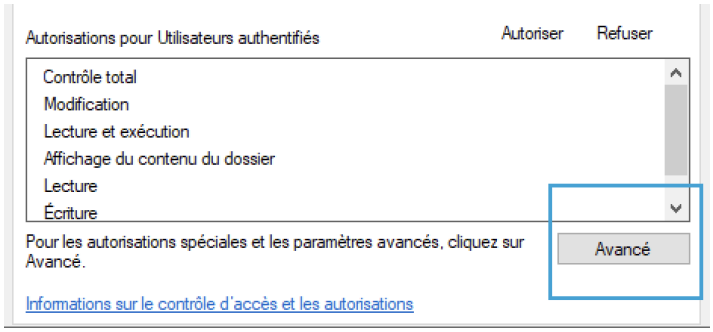
J’ajoute les groupes Utilisateurs authentifiés ainsi que les Administrateurs.

Je n’affecte cependant pas les même droits aux groupes d’utilisateurs ;

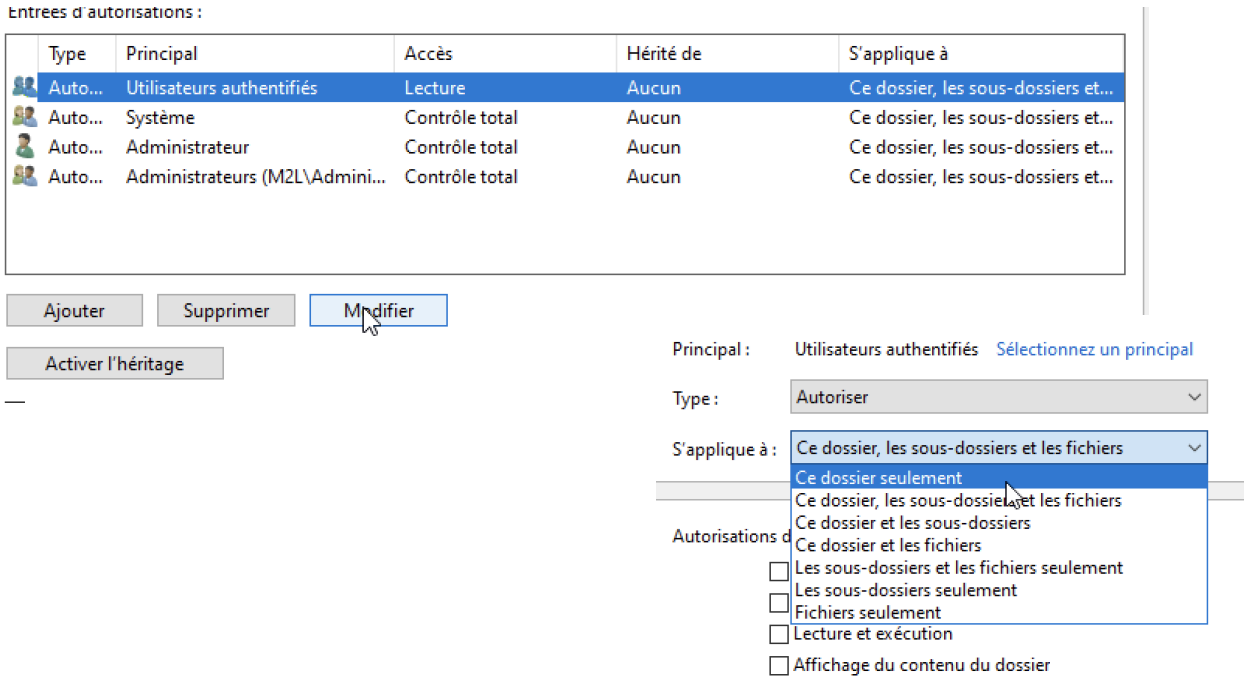


Puis je partage le dossier parent.

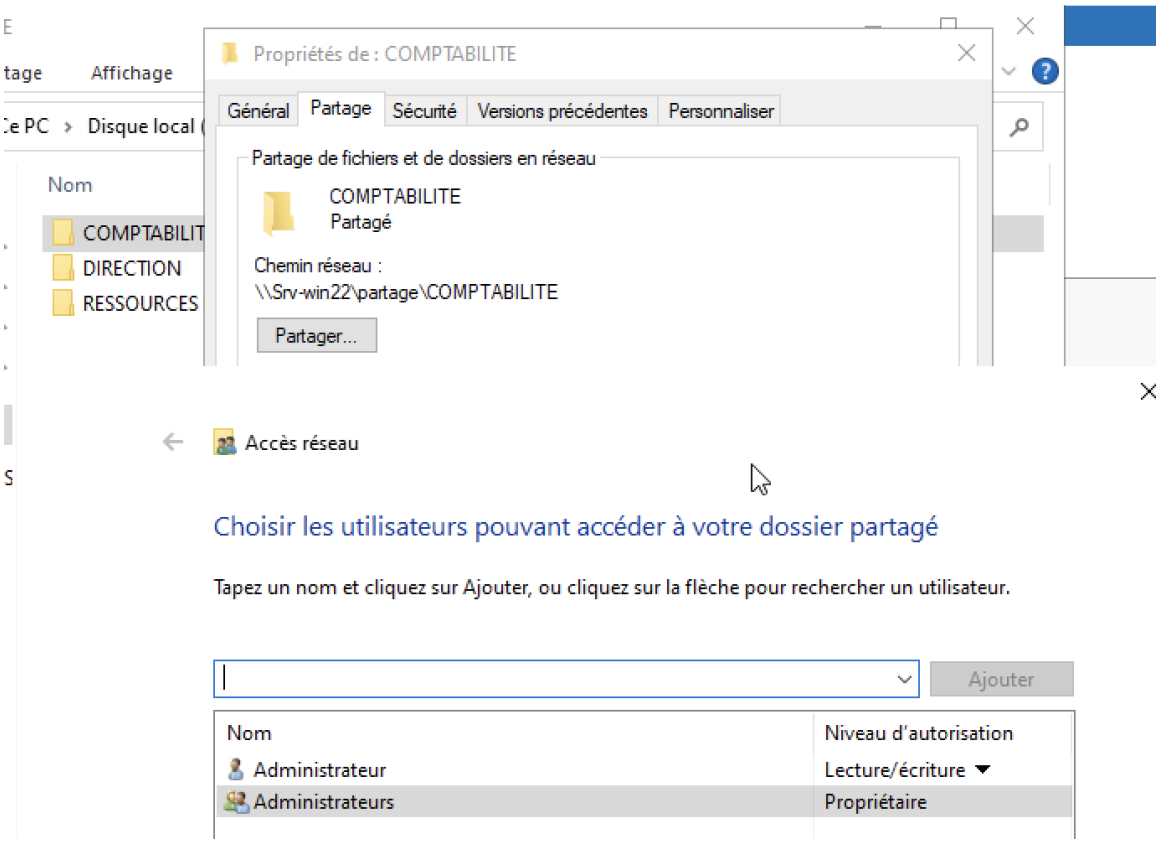
Il faut cependant pousser la configuration un peu plus loin pour que les droits appliqués à notre groupe d’utilisateur général ne descende pas dans notre arborescence. Nous allons alors nous déplacer dans les paramètres avancé de sécurité de notre dossier racine ; « PARTAGE »



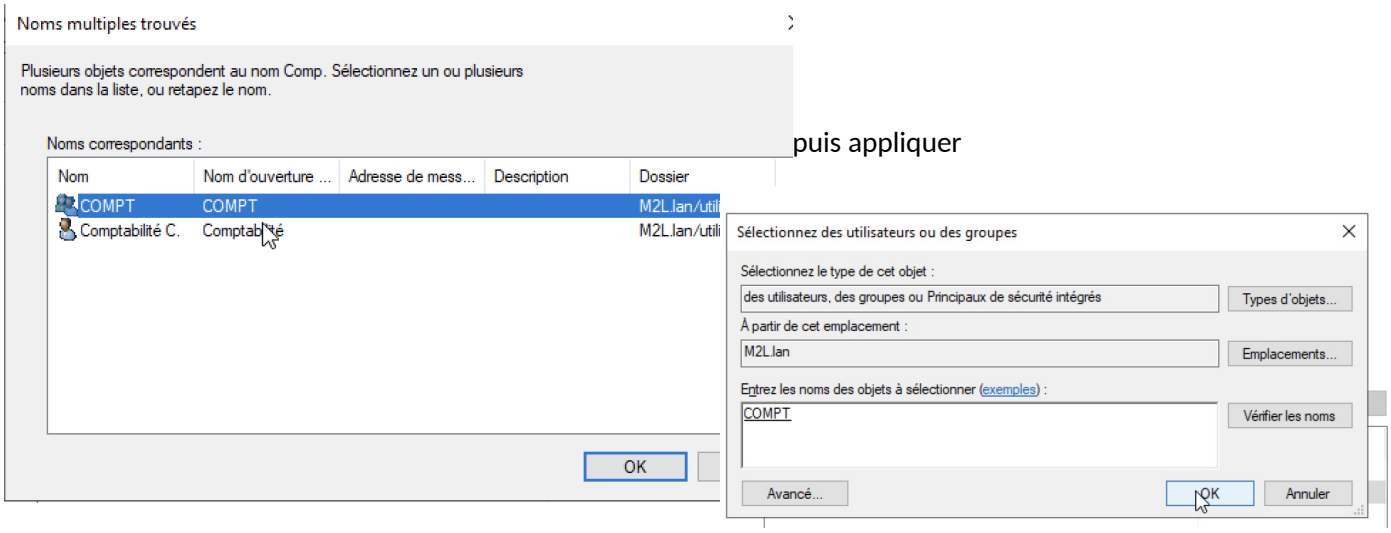
Puis nous allons modifier l'autorisation pour qu'elle ne s'applique uniquement qu'à ce dossier, ce qui nous permettra de configurer des droits différents pour les mêmes utilisateurs sans ressentir d'impact de ce dossier, **les droits ne seront pas hérités entres ces deux dossiers.**



Partageons désormais les dossiers correspondants aux groupes d'utilisateurs correspondants ;

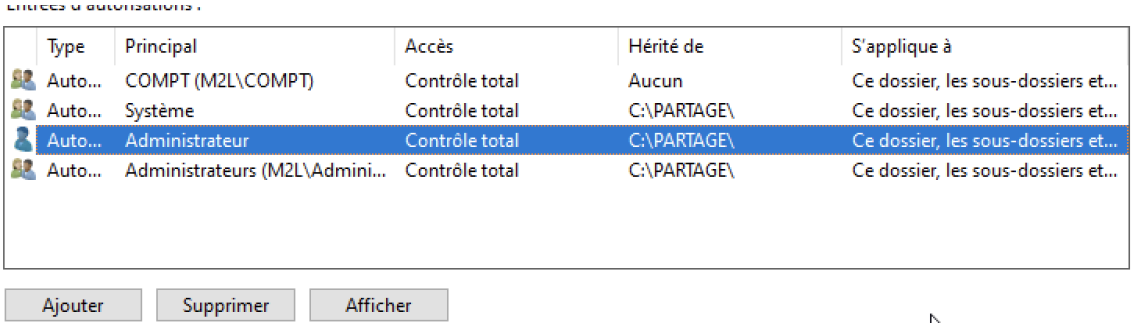


Je me situe dans le dossier futur du service de comptabilité, je cherche alors le groupe ;



puis appliquer

Nous retournons finalement dans les paramètres avancés afin de paramétrer les accès de ce groupe au dossier ; nous définirons lecture / écriture et nous nous assurons que personne ne puisse lire, écrire, modifier, supprimer, hors mis le RSI.



8. Mise en place d’un RAID 5

Détails du service :

Le RAID 5 est **idéal pour les serveurs d'applications et de fichiers disposant d'un nombre limité de disques, mais souhaitant des performances de stockage et une fiabilité accrues** .

Le mécanisme RAID 5 est adapté au stockage de données critique il protège les données grâce à une **parité** répartie.

- Il **supporte la perte d’un disque** sans perte d'information.
- Il offre un **bon compromis** entre **sécurité**, **capacité** et **coût**.

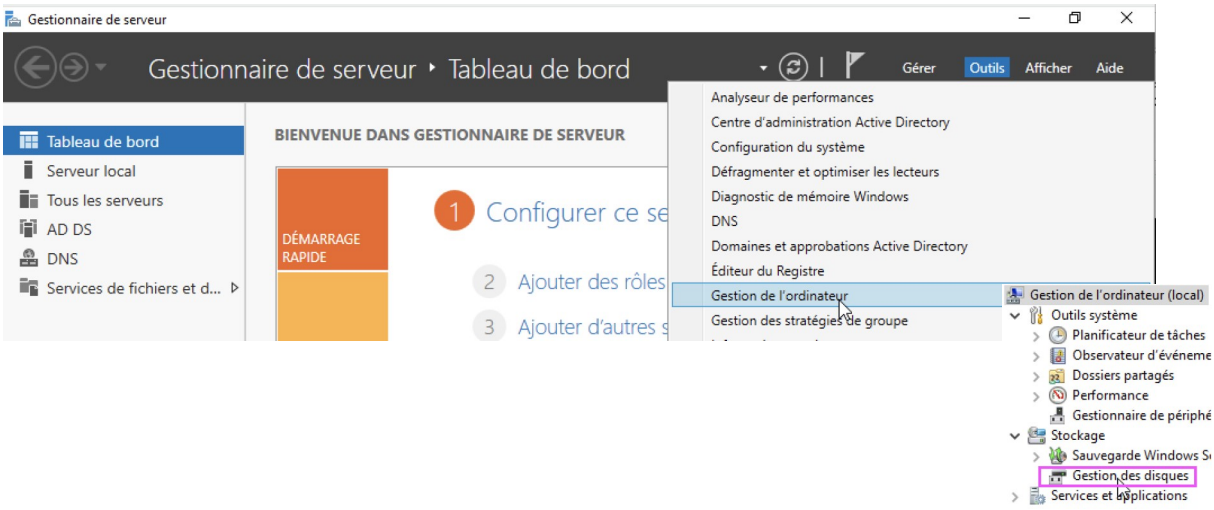
Installation du service :

Procédons maintenant à la création d’un RAID 5 indépendant de notre **PARTAGE** créé ultérieurement.

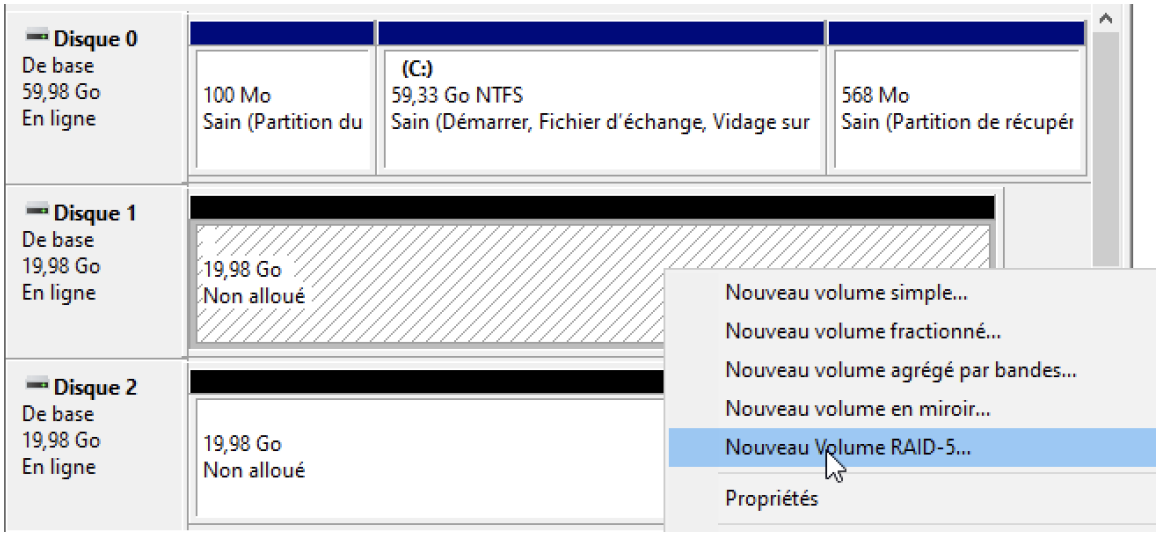
Il faut au préalable vous fournir de 3 disques pour la création du RAID.

Vous pouvez consulter l’état vos disques dans le **Gestionnaire de disques**.

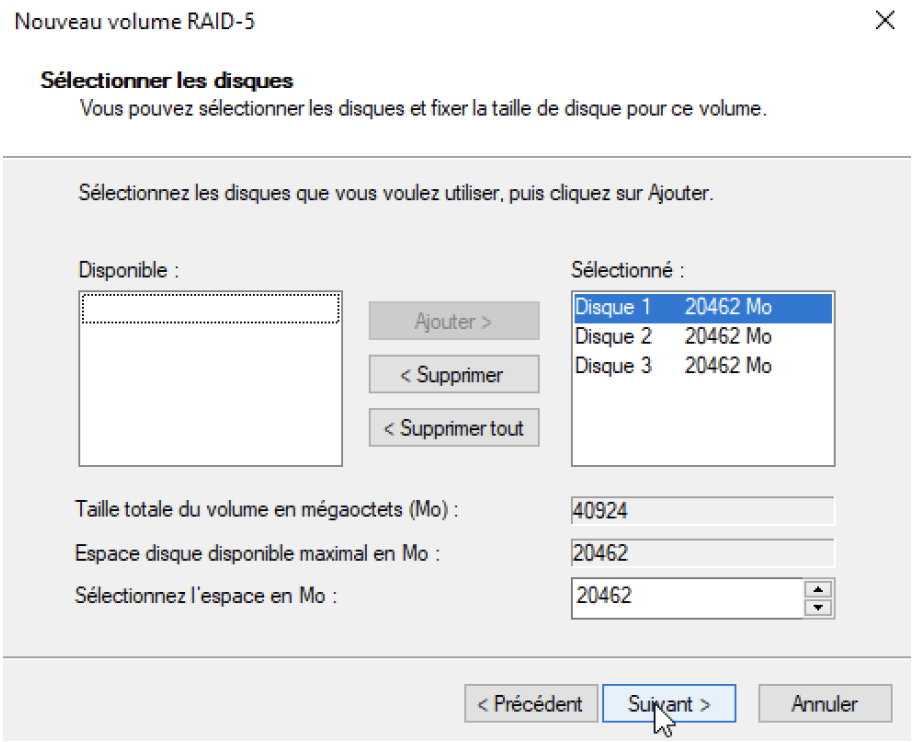
Allez dans « Gestion de l’ordinateur », puis « Gestion des disques »



Vous pouvez alors grâce à la barre déreoulante, vérifier que le système reconnaît bien vos disques, ainsi, cliquez sur l'un des espaces non alloués afin de créer une **volume RAID 5**.



Veillez à ce que vos 3 disques soient bien sélectionnés.



Vous pouvez cliquer sur **suivant** sur les prochaine fenêtres d'installation, formatant les volumes avec le format NTFS.

Le RAID fonctionnera indépendamment de notre **PARTAGE**, un lien direct sera établi par la suite.

9. Installation du système d'exploitation de Debian 12.

Détails des services :

Debian

Debian GNU/Linux est **une distribution spécifique du système d'exploitation Linux disposant de nombreux paquets**. Debian GNU/Linux est : complète : actuellement, Debian inclut plus de 64961 logiciels. Les utilisateurs peuvent choisir quels paquets installer ; Debian fournit un outil à cette fin.

Debian est **l'un des plus anciens systèmes d'exploitation basés sur le noyau Linux** et constitue la base de nombreuses autres distributions Linux. En septembre 2023, Debian est la deuxième plus ancienne distribution Linux encore en développement actif, seule Slackware étant plus ancienne.

Pré-requis logiciel et matériel :

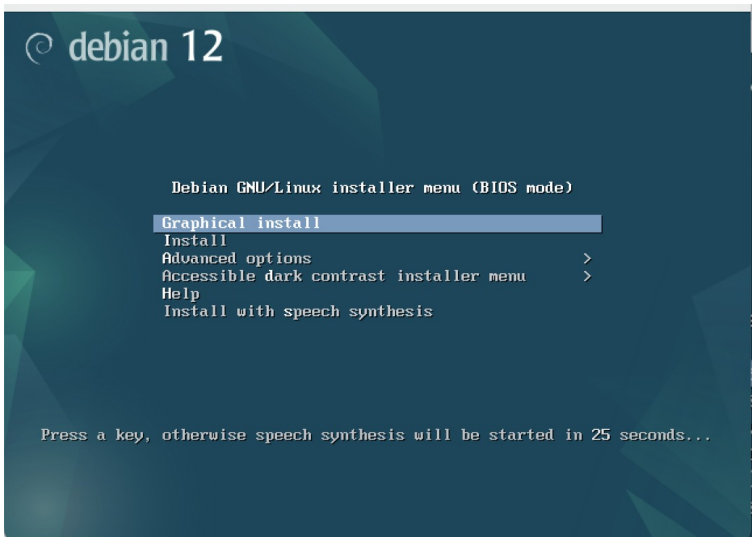
Pour faire tourner notre écosystème nous auront besoin d'au moins ;

- CPU : 1.4 GHz 32x ou x64
- RAM : 2 Go à 4 Go
- Stockage : 20 Go

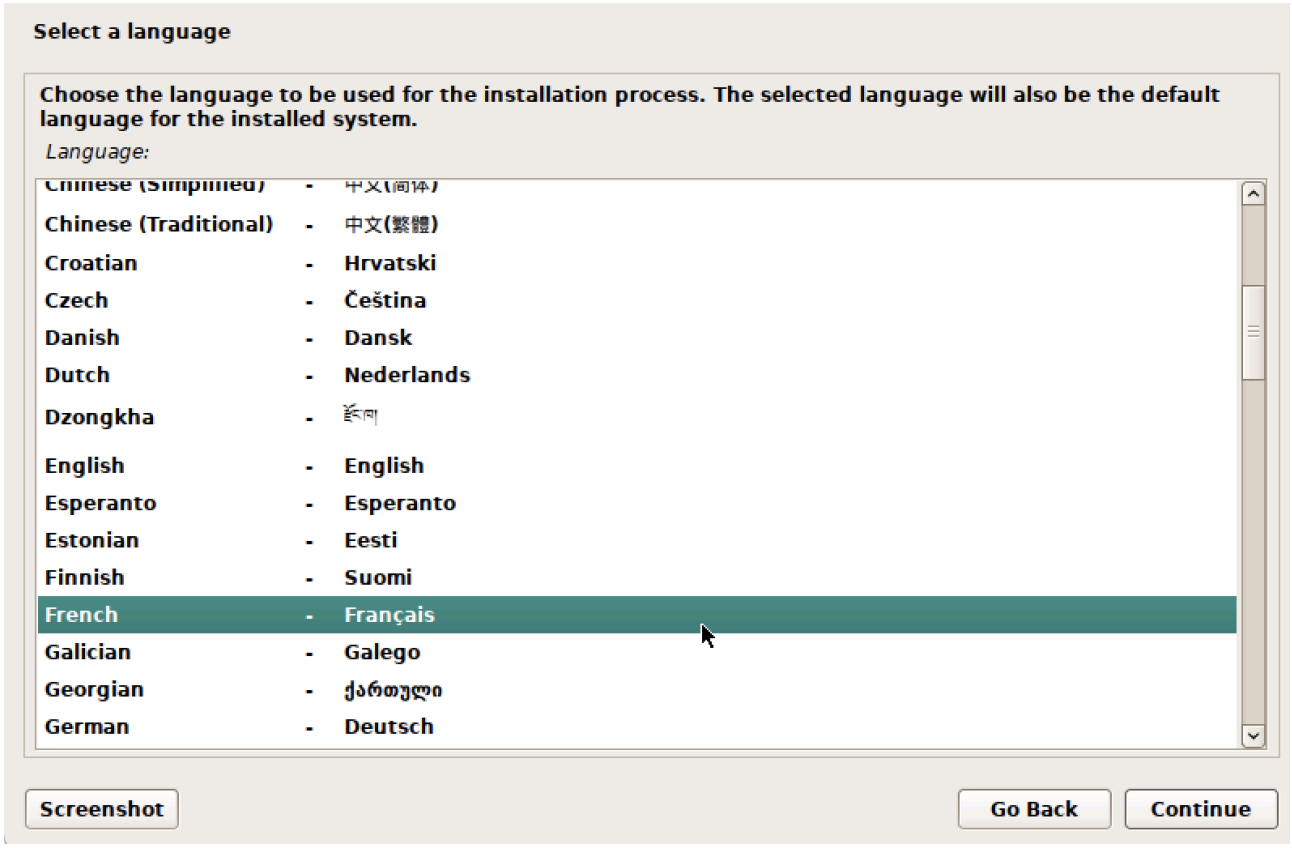
Afin de mener à bien notre installation voici les pré-requis logiciel ;

- ISO d'installation Debian 12 (ISO Deb12)
- Usage d'une clé bootable (Rufus)

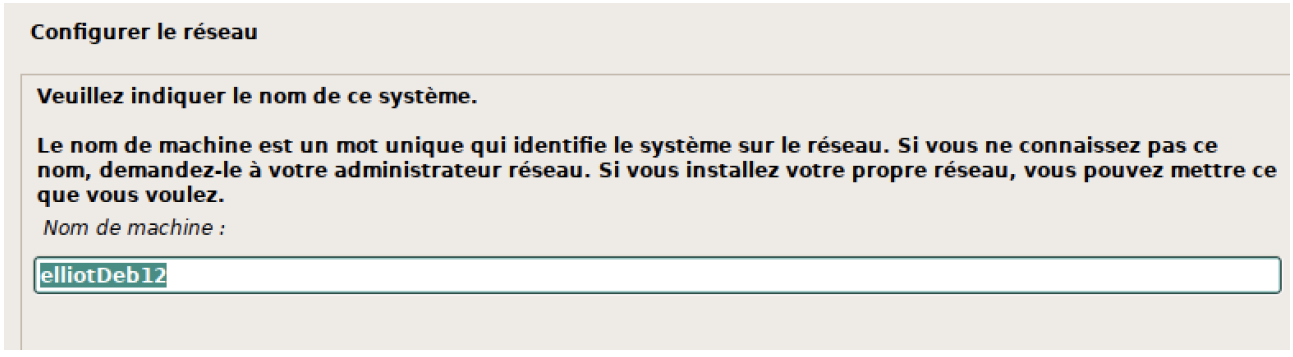
Nous allons effectuer notre installation en mode graphique ;



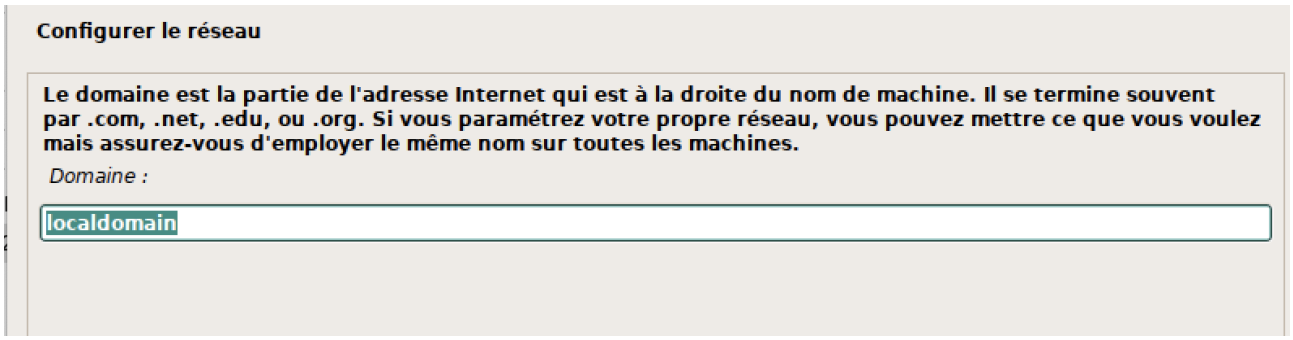
Sur ces trois prochaines pages, sélectionnez votre région



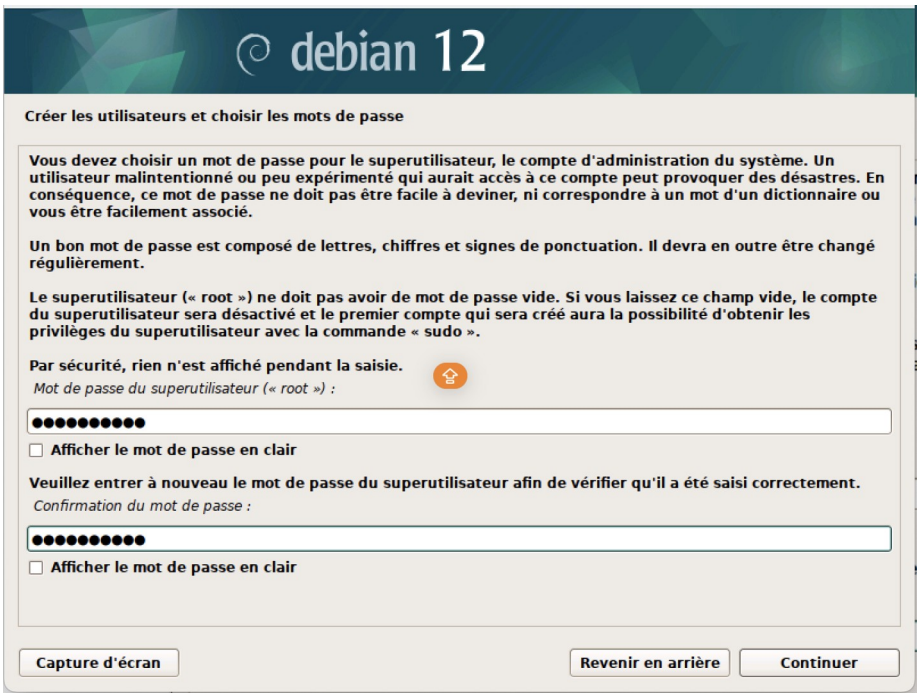
Nous allons désormais définir le nom de notre machine ;



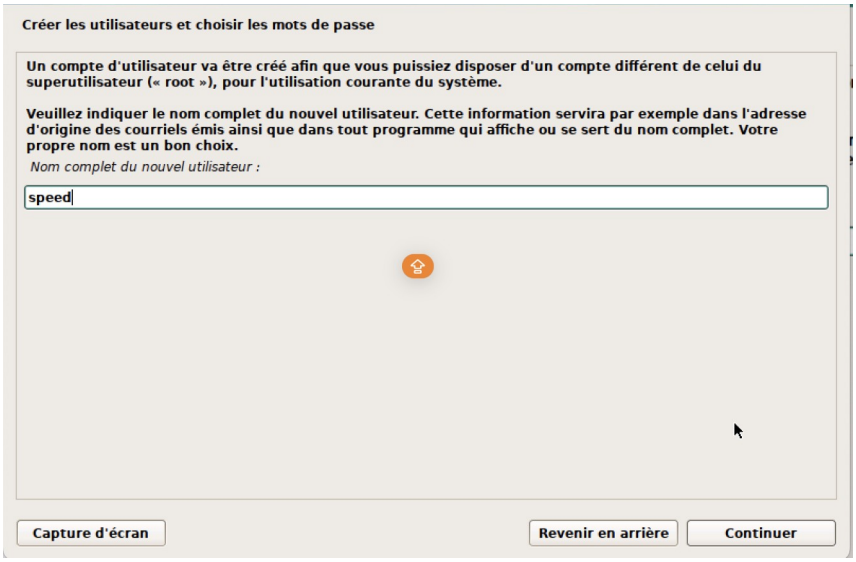
Le domaine reste local, nous ne configurerons pas d'entrée dans un domaine ici.



Nous définissons ici le mot de passe pour l'utilisateur « root »

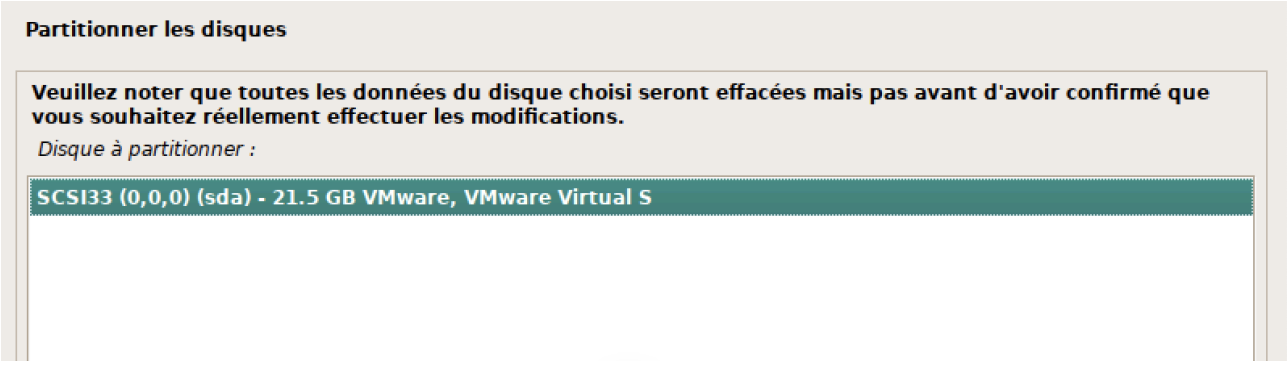


Voici venu la création de notre premier utilisateur ;

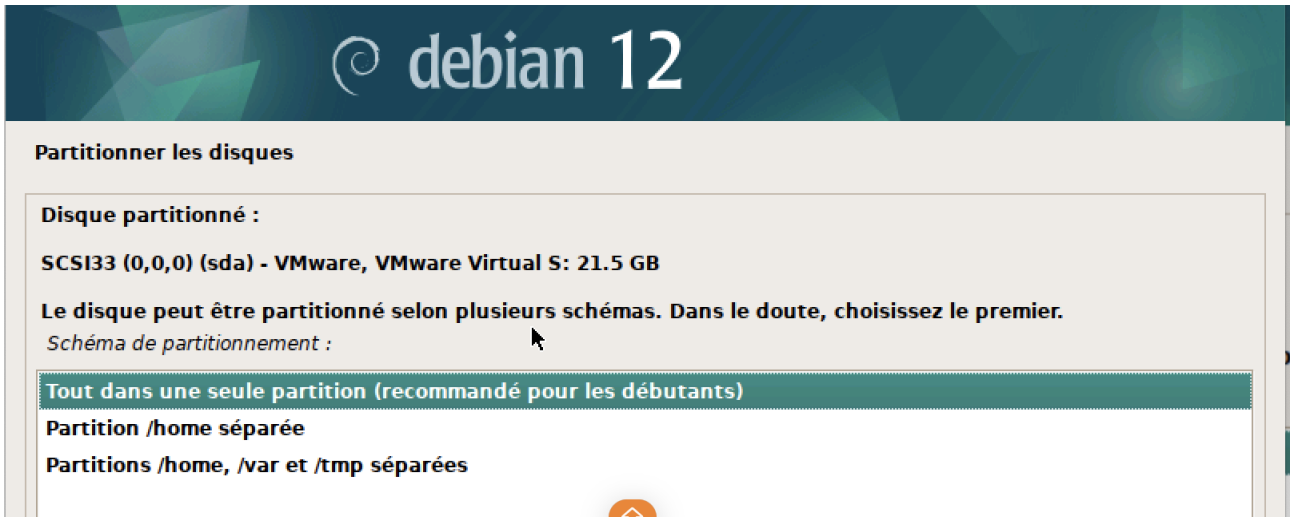


Définissez un mot de passe fort (8 caractères minimum, une minuscule et une majuscule ainsi qu'un caractère spécial).

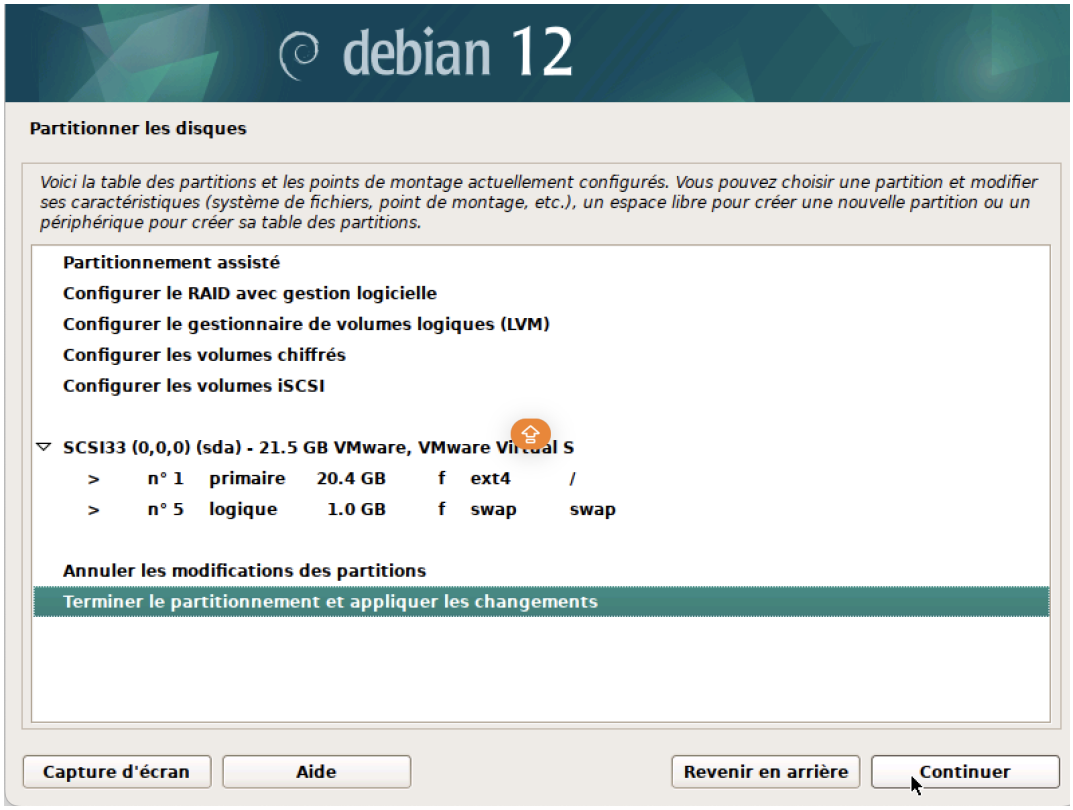
Nous allons désormais choisir le disque d'installation de notre Debian



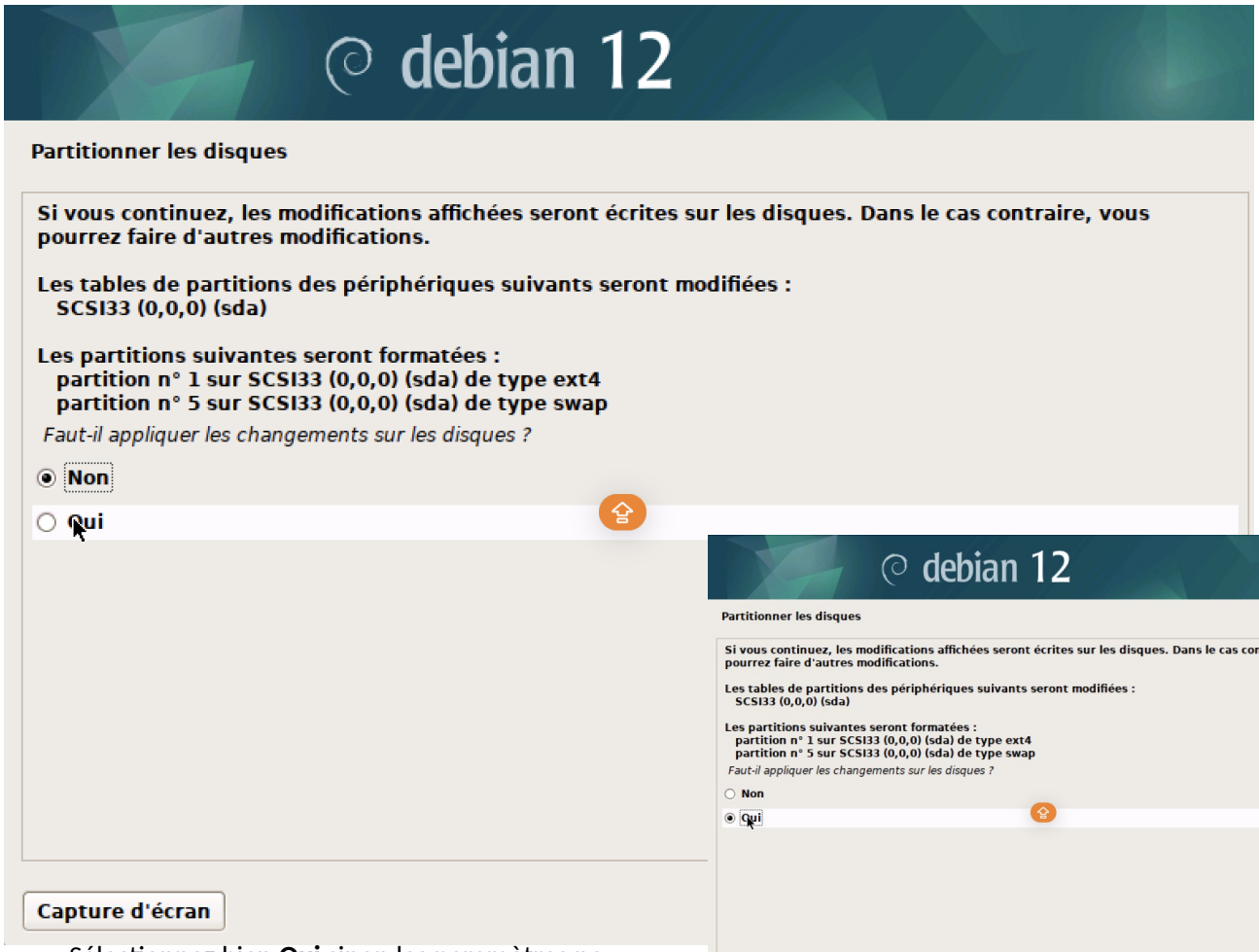
Nous choisirons un partitionnement simple car il n'est pas nécessaire de plus dans notre cas.



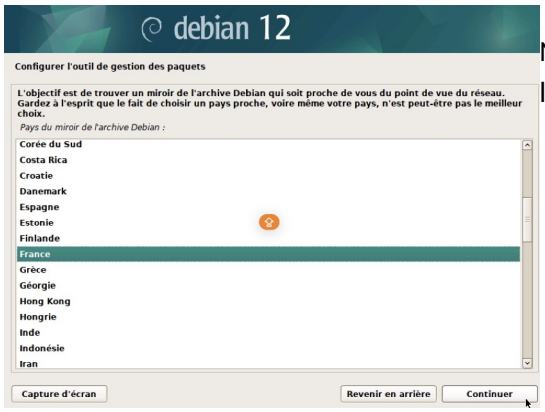
Vérifiez l'application des paramètres du partitionnement sélectionné ;



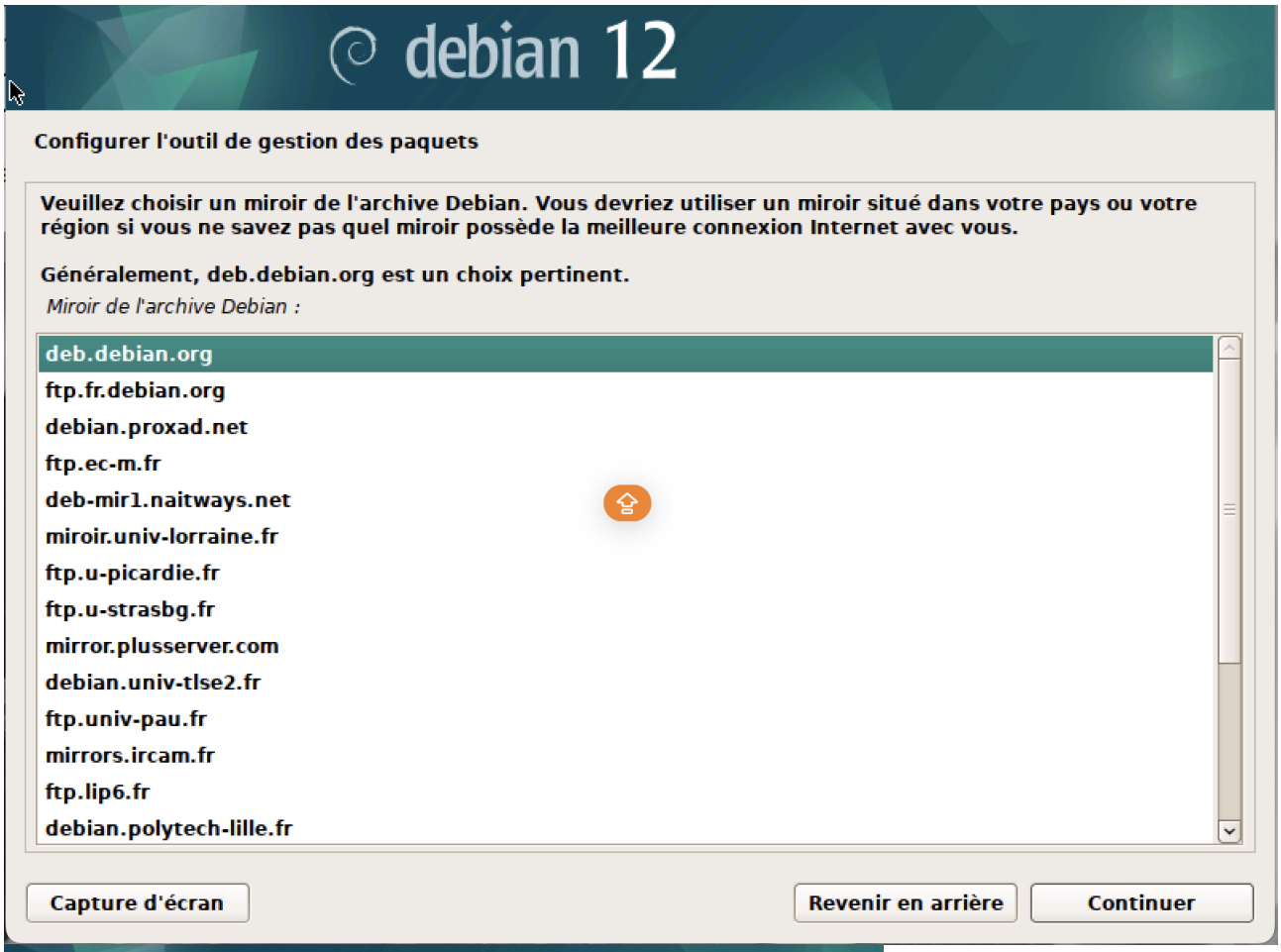
Sélectionnez **Terminer le partitionnement et appliquer les changements,** appuyez sur **continuer.**



Sélectionnez bien **Oui** sinon les paramètres ne s'appliqueront pas.



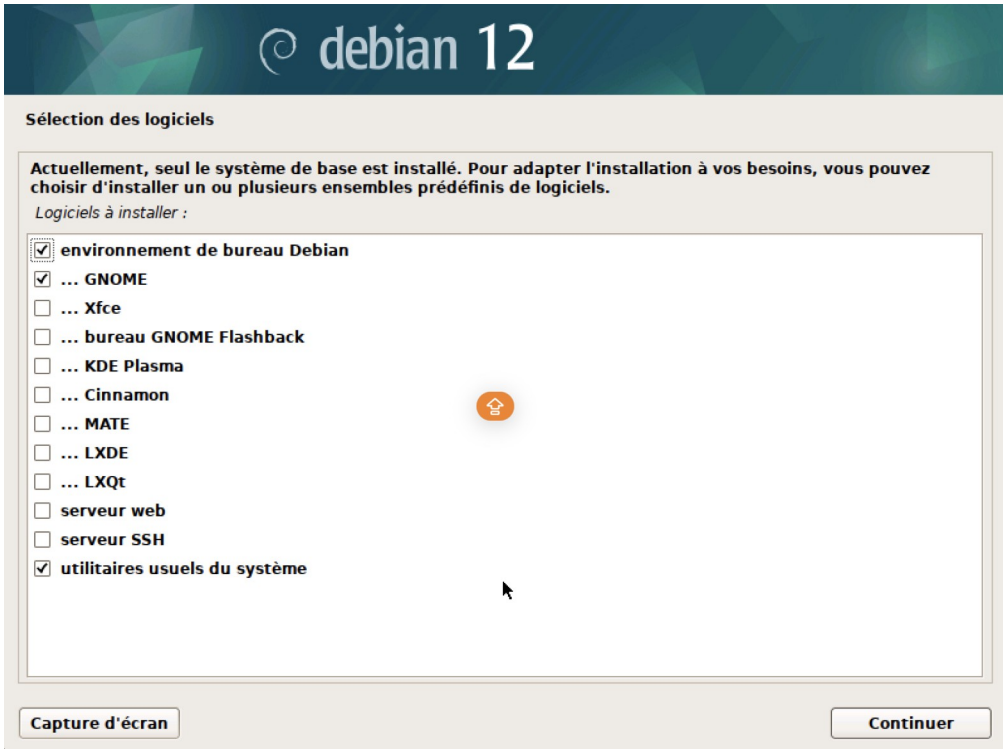
Nous nous situons en France donc nous choisirons les dépôt correspondants à notre région ;



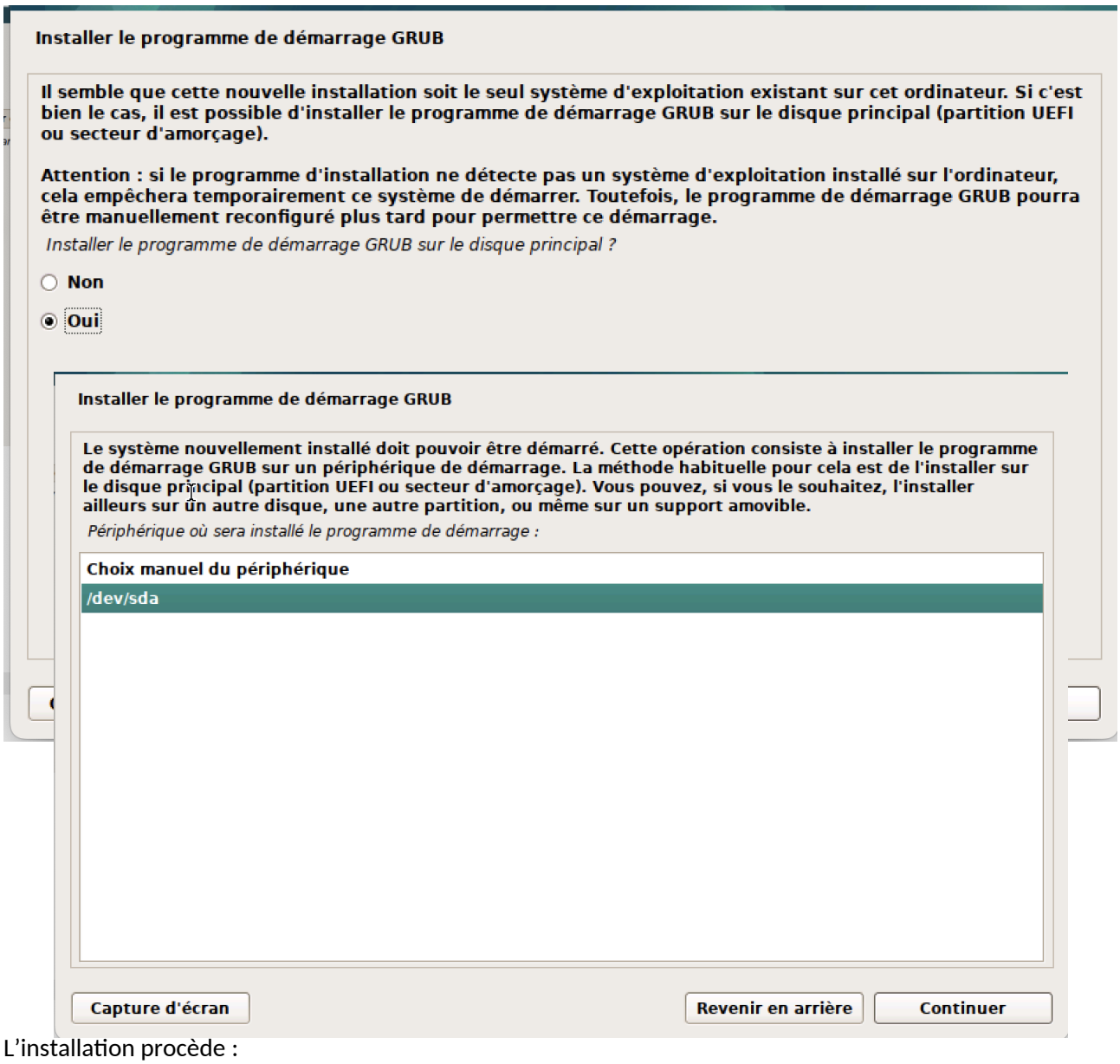
Vous pouvez laisser le choix par défaut.

Suite à quoi, l'installation procède…

Nous sélectionnons **GNOME** comme interface graphique mais le choix vous est libre.

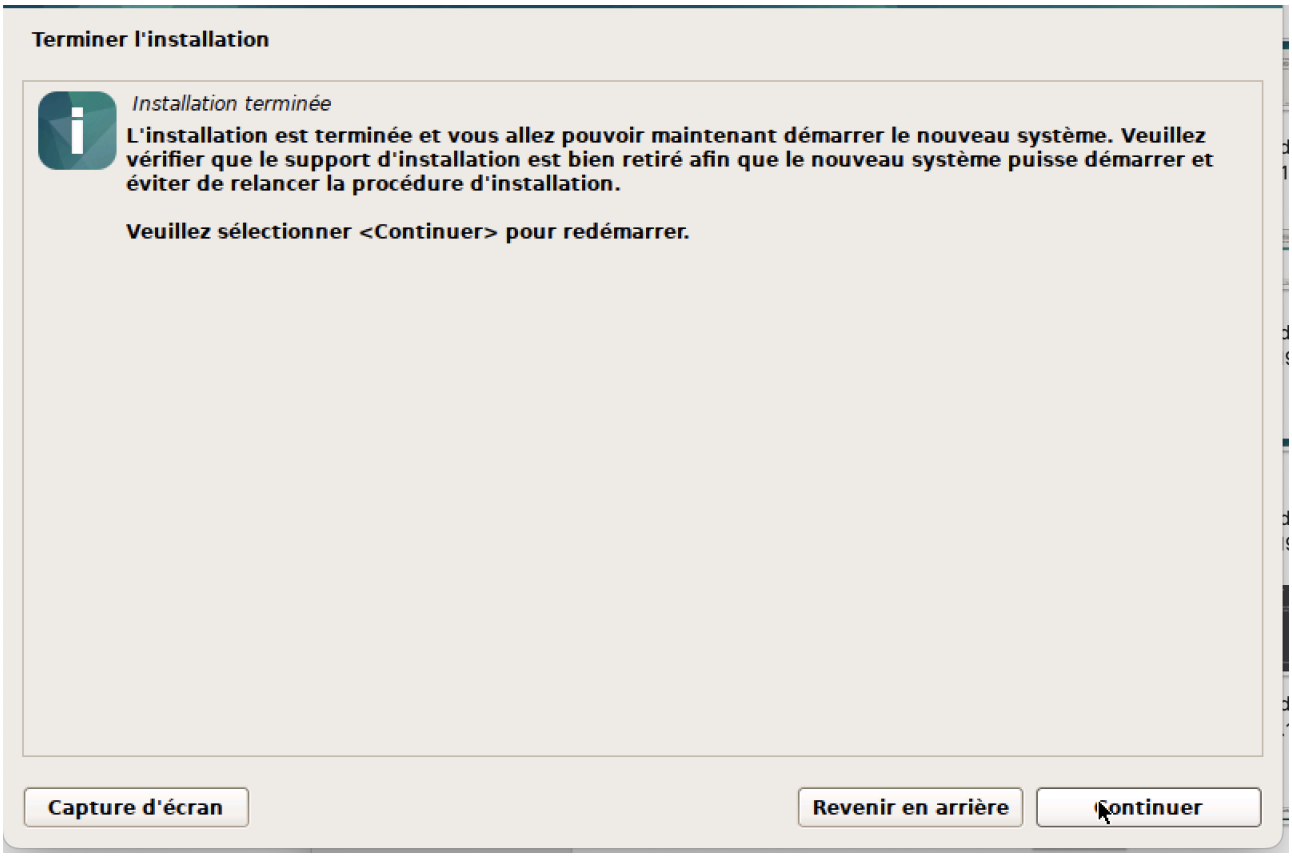


Sélectionnez **Oui** pour installer le programme de démarrage GRUB, par la suite nous allons sélectionner notre disque principal ;



L'installation procède :

Procédez désormais au redémarrage le machine



Vous pouvez maintenant vous connecter avec l'utilisateur fraichement créé et personnaliser votre compte ainsi que les paramètrages.

10. Installation de la solution NextCloud

Installation de la solution NextCloud :

Pour des raisons de praticité, j'élève mes privilèges en **root**.

Je mets ensuite à jour les sources des dépôts et lance les mises à jour si nécessaire avec les commandes suivantes ;

su -

apt update

apt upgrade

```
elliot@deb12speed:~$ su -
Mot de passe :
root@deb12speed:~# apt update
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Atteint :2 http://security.debian.org/debian-security bookworm-security InReleas
e
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
root@deb12speed:~# apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@deb12speed:~#
```

Apache

Premièrement, nous allons procéder à l'installation de notre serveur apache avec la commande suivante ;

apt-get install apache2

```
root@deb12speed:~# apt-get install apache2
```

Puis grâce à la commande ;

systemctl status apache2

Vérifiez si le service est bien en cour d'exécution. Voici ce que la commande devrait vous retourner ;

```
root@deb12speed:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab>
     Active: active (running) since Sun 2025-04-13 16:31:42 CEST; 32s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 3969 (apache2)
      Tasks: 55 (limit: 2241)
     Memory: 11.1M
        CPU: 64ms
     CGroup: /system.slice/apache2.service
             ├─3969 /usr/sbin/apache2 -k start
             ├─3970 /usr/sbin/apache2 -k start
             └─3971 /usr/sbin/apache2 -k start
```

Notre serveur apache est correctement installé, passons à l'installation d'un pare-feu **UFW**

UFW

Installez le paquet ufw ;

apt install ufw

```
root@deb12speed:~# apt install ufw
```

une fois effectué, vous devrez installer OpenSSH ;

apt install –-reinstall openssh-server

```
root@deb12speed:~# apt install --reinstall openssh-server
```

Puis autoriser **OpenSSH** sur le pare-feu **UFW** :

```
root@deb12speed:~# ufw allow OpenSSH
Rules updated
Rules updated (v6)
```

Vous pouvez maintenant activer le pare-feu avec la commande ci-dessous, celle ci devrait vous retourner le même message que sur la capture d'écran ;

```
root@deb12speed:~# ufw enable
Firewall is active and enabled on system startup
```

Nous allons aussi autoriser WWW Full afin d'ajouter le port HTTP et HTTPs pour notre serveur web ;

```
root@deb12speed:~# ufw allow "WWW Full"
Rule added
Rule added (v6)
root@deb12speed:~#
```

La configuration UFW est désormais achevée, nous passons maintenant à l'installation de PHP ainsi que de ses dépendances nécessaires.

PHP

PHP est installé nativement sur notre système d'exploitation **Debian.** Nous aurons alors uniquement besoin d'installer les dépendances nécessaires avec la commande suivante ;

```
apt install -y php php-curl php-cli php-mysql php-gd php-common php-xml php-json php-intl php-pear php-imagick php-dev php-common php-mbstring php-zip php-soap php-bz2 php-bcmath php-gmp php-apcu libmagickcore-dev
```

```
root@12deb:~# sudo apt install -y php php-curl php-cli php-mysql php-gd php-comm
on php-xml php-json php-intl php-pear php-imagick php-dev php-common php-mbstrin
g php-zip php-soap php-bz2 php-bcmath php-gmp php-apcu libmagickcore-dev
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
```

Désormais nous devons ouvrir le fichier de configuration de php afin d'apporter des modifications sur quelques lignes. Le fichier en question se trouve dans ;
/etc/php/8.2/apache2/php.ini

Dans notre cas nous l'éditerons avec **nano** et modifierons les lignes suivantes avec les correspondances suivantes ;

979

```
; https://php.net/date.timezone
date.timezone = Europe/amsterdam
```

435

```
memory_limit = 512M
```

855

```
upload_max_filesize = 500M
```

703

```
max_execution_time = 300
```

409

```
post_max_size = 600M
```

966

```
zend_extension=opcache
```

Ajoutez les paramètres recommandés par **NextCloud pour Debian ;**

```
zend_extension=opcache

;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;

opcache.enable = 1
opcache.interned_strings_buffer = 8
opcache.max_accelerated_files = 10000
opcache.memory_consumption = 128
opcache.save_comments = 1
opcache.revalidate_freq = 1
```

Vous pouvez désormais relancer le service apache pour qu'il prenne les modifications en compte ;

```
root@12deb:~# systemctl restart apache2
root@12deb:~#
```

Nous allons, pour suivre, procéder à l'installation de MariaDB afin de créer notre base de données

MariaDB

Saisissez simplement la commande suivante :

apt install mariadb-server

Suite à quoi vous pourrez contrôler la mise en service de mariadb avec la commande suivante ;

systemctl status mariadb

Elle devrait vous retourner ceci ;

```
root@12deb:~# systemctl is-enabled mariadb
enabled
root@12deb:~# systemctl status mariadb
● mariadb.service - MariaDB 10.11.11 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enal
     Active: active (running) since Sat 2025-04-12 18:51:36 CEST; 25min ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
   Main PID: 37678 (mariadbd)
     Status: "Taking your SQL requests now..."
```

Nous allons alors créer un mot de passe root pour maria db ainsi qu'effacer la base test et les utilisateurs anonymes existants ;

```
root@12deb:~# mariadb-secure-installation
```

nous répondrons non à cette question uniquement,

```
Switch to unix_socket authentication [Y/n] N
```

vous pourrez répondre **Y** aux suivantes ;

```
Change the root password? [Y/n] Y

Remove anonymous users? [Y/n] Y

Disallow root login remotely? [Y/n] Y

Remove test database and access to it? [Y/n] Y

Reload privilege tables now? [Y/n] Y
```

L'installation est terminée, **MariaDB** nous retourne ceci ;

```
All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
root@12deb:~#
```

Nous pouvons maintenant créer notre base de données avec la suite de commande suivante ;

```
Thanks for using MariaDB!
root@deb12speed:~# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE elliot_db;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'speed'@'localhost' IDENTIFIED BY votre mot de passe ;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON elliot_db.* TO 'speed'@'localhost';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]>
```

Avant de passer à l'étape suivante, nous allons télécharger une version récente du code source de **NextCloud** afin d'assurer la compatibilité de l'OS.

```
root@deb12speed:~# apt install curl unzip -y
root@deb12speed:/var/www# curl -o nextcloud.zip https://download.nextcloud.com/server/releases/latest.zip
```

Une fois téléchargé, vous pouvez extraire le code source et ainsi donner les droits correspondants ;

```
root@deb12speed:/var/www# unzip nextcloud.zip
root@deb12speed:/var/www# chown -R www-data:www-data nextcloud
```

Configuration Apache

Nous allons maintenant créer un fichier de configuration pour NextCloud.
J'utilise toujours la commande nano pour ouvrir mon éditeur de texte ;

```
root@12deb:/var/www# nano /etc/apache2/sites-available/nextcloud.conf
```

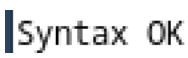
```
 GNU nano 7.2       /etc/apache2/sites-available/nextcloud.conf
<VirtualHost *:80>
 ServerName nextcloud.192.168.5.140
 DocumentRoot/var/www/nextcloud/


# log files
 ErrorLog /var/log/apache2/files.192.168.5.140-error.log
 CustomLog /var/log/apache2/files.192.168.5.140-access.log
combined


 <Directory /var/www/nextcloud/>
  Options +FollowSymlinks
  AllowOverride All


  <IfModule mod_dav.c>
   Dav off
  </IfModule>


  SetEnv HOME /var/www/nextcloud
  SetEnv HTTP_HOME /var/www/nextcloud
 </Directory>
</VirtualHost>


                [ Lecture de 25 lignes ]
```

et voici la configuration que je rentre ;
(attention à bien remplacer mon ip par la votre !)

Vous pouvez alors activer la configuration et essayer la configuration test avec les commandes suivantes ;

a2ensite nextcloud.conf

apachectl configtest



Ce qui vous retourne alors ;

Vous êtes désormais parés à vous lancer dans la configuration de celui-ci par l'interface web de votre navigateur en saisissant l'ip associé.

11. OpenVPN.

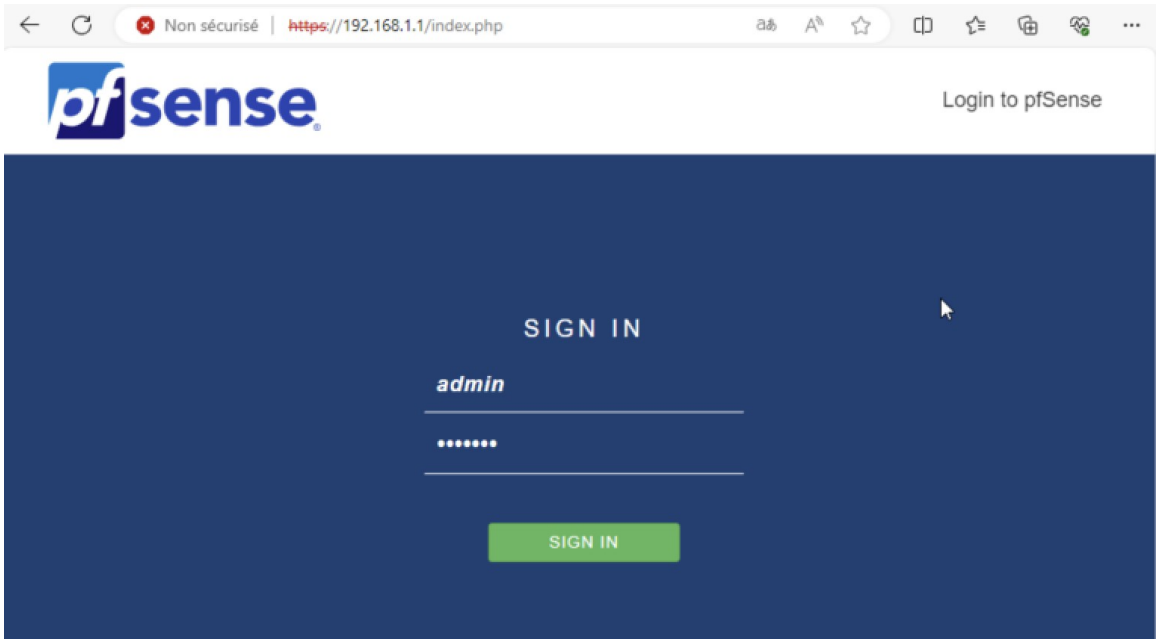
Détails de la solution OpenVPN

Un réseau privé virtuel (VPN) fournit une connexion sécurisée entre deux points d'un réseau (par exemple, un appareil IoT et un serveur). Il crée effectivement un « tunnel » de communication privé, permettant aux utilisateurs d'envoyer et de recevoir des données via Internet public comme s'ils étaient directement connectés à un réseau privé.

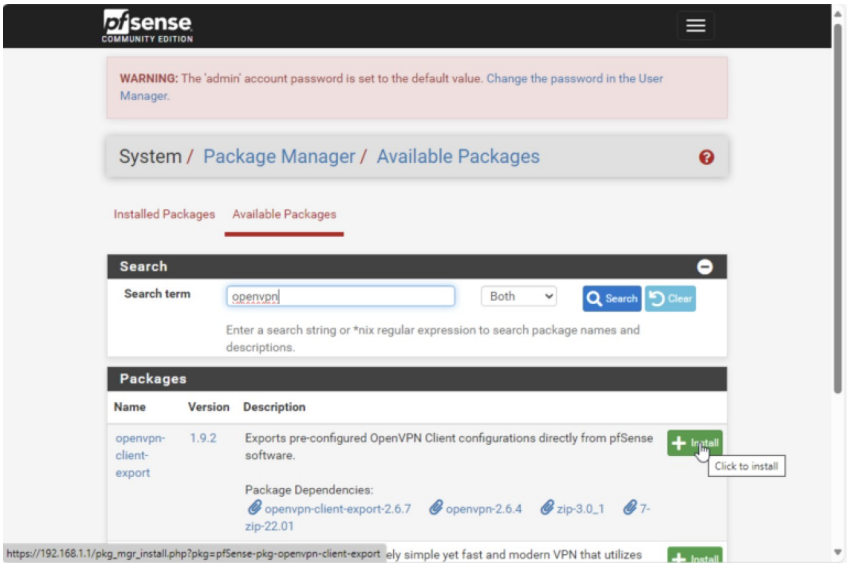
Installation du service

Nous nous connectons premièrement à notre routeur PfSense afin d'installer les paquets nécessaires, les certifications et les autorisations pour sécuriser notre connexion. Mais aussi créer notre utilisateur.

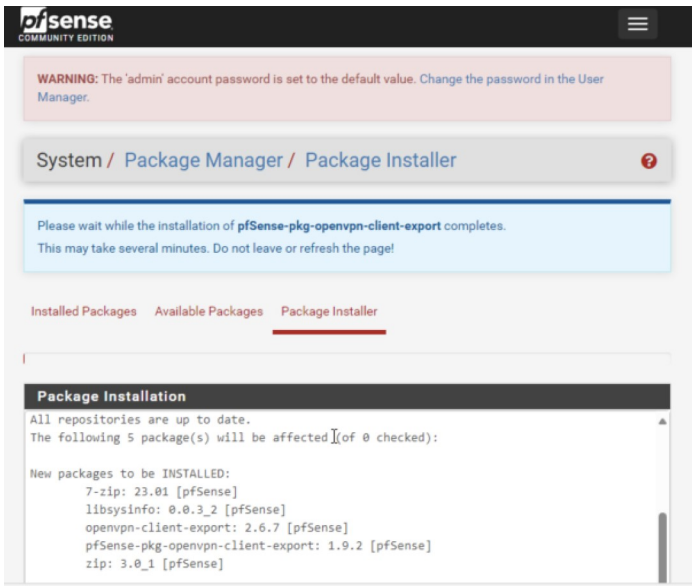
Rentrons alors l'adresse de notre PfSense dans le navigateur d'une machine connectée à mon réseau ; ici 192.168.1.1



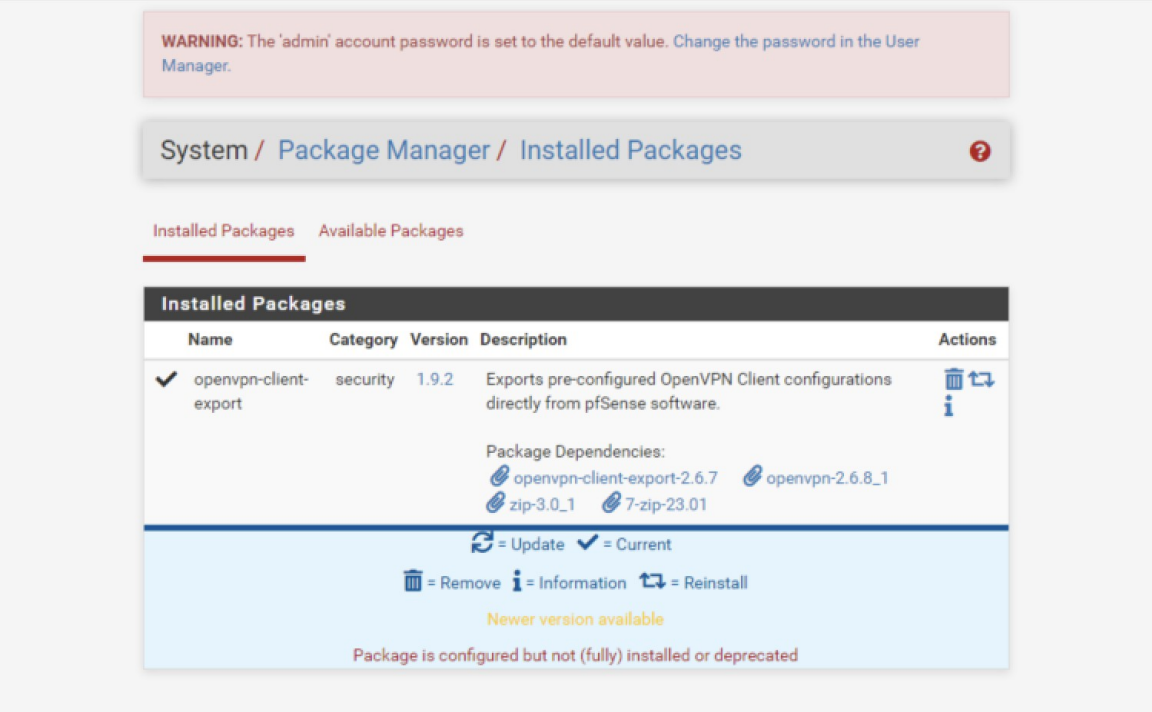
Puis premièrement, nous nous rendons sur le packet manager afin d'installer le paquet d'OpenVPN dans la liste des paquets disponibles.



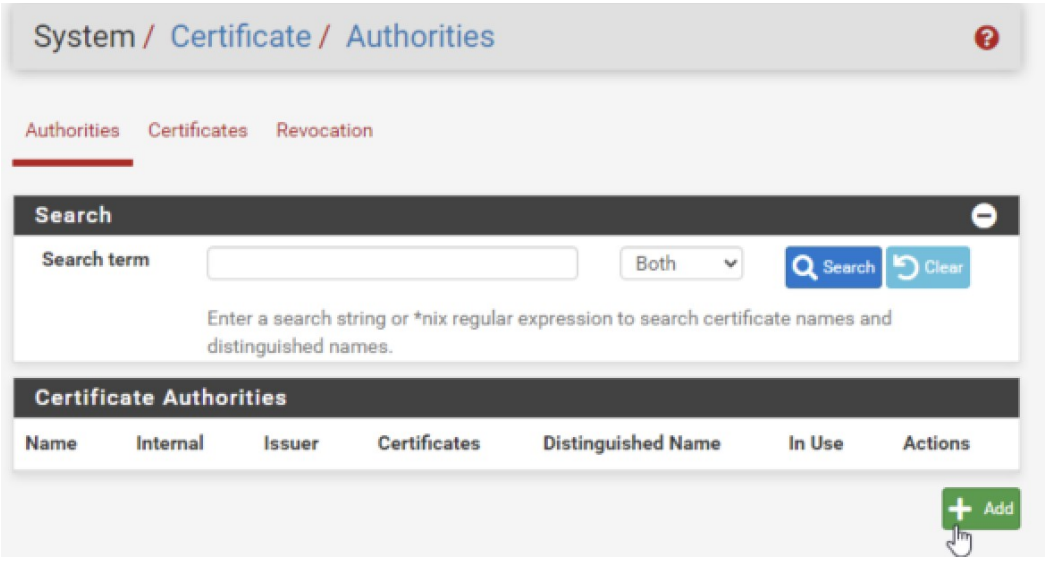
Nous cliquerons donc sur installer et laisserons l'installation procéder…

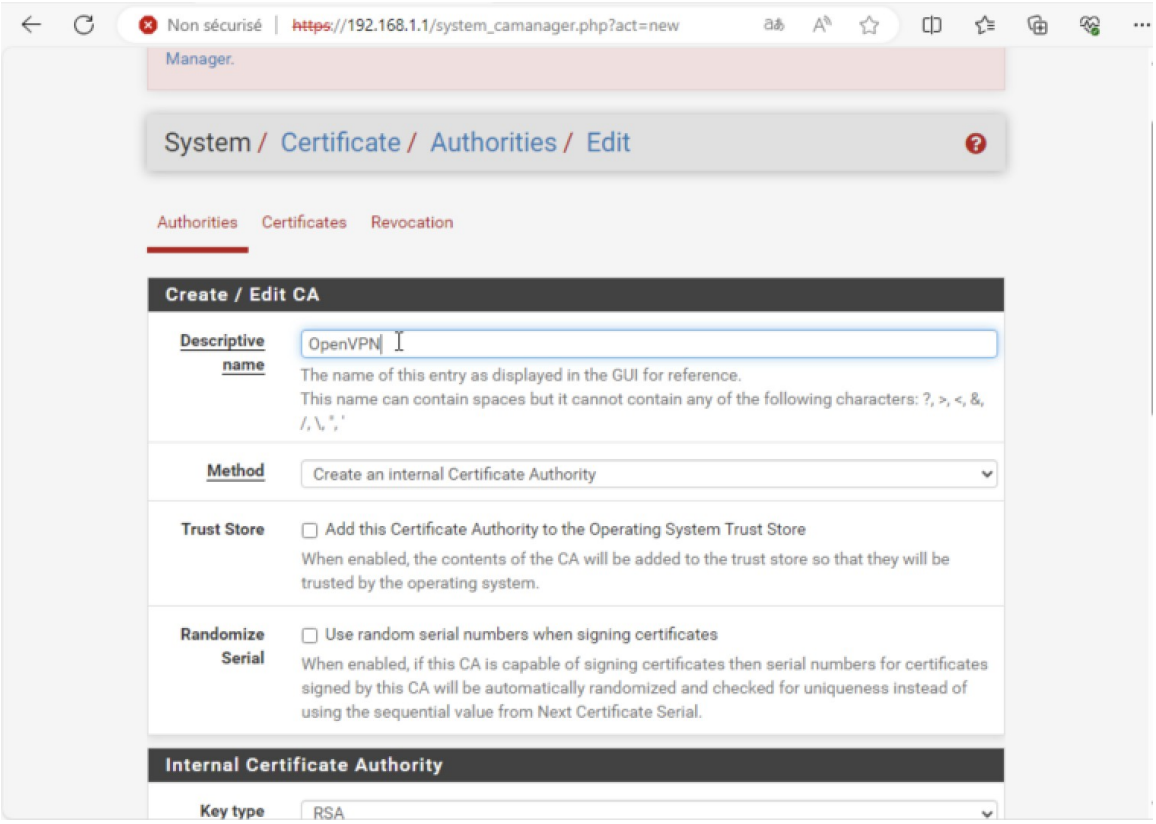


Nous pouvons consulter les paquets installés ;

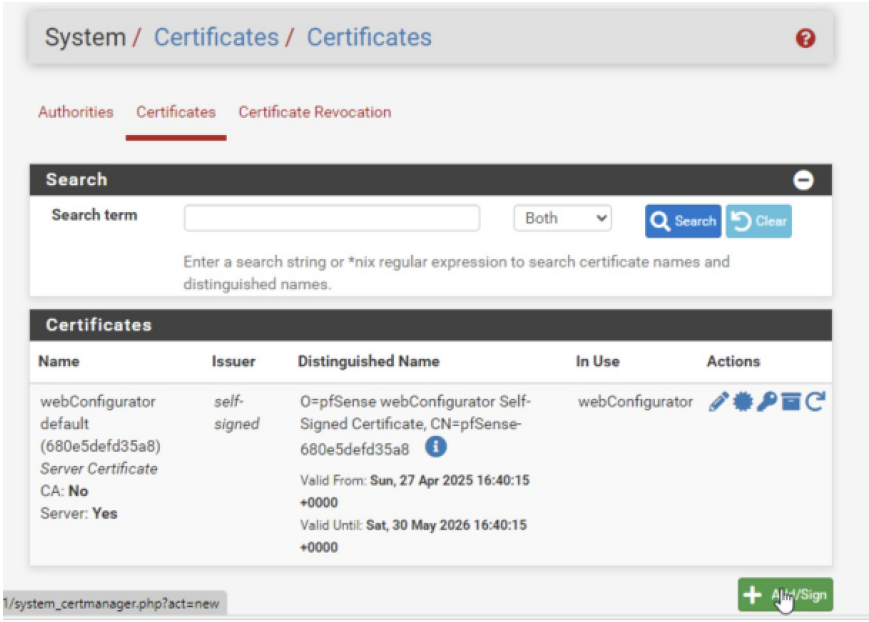


Nous allons désormais définir un certificat d'autorisation pour OpenVPN sur notre PfSense ; toujours dans « Système » mais cette fois dans « Certificate » puis « Authorities » ou nous ajouterons cette dernière.



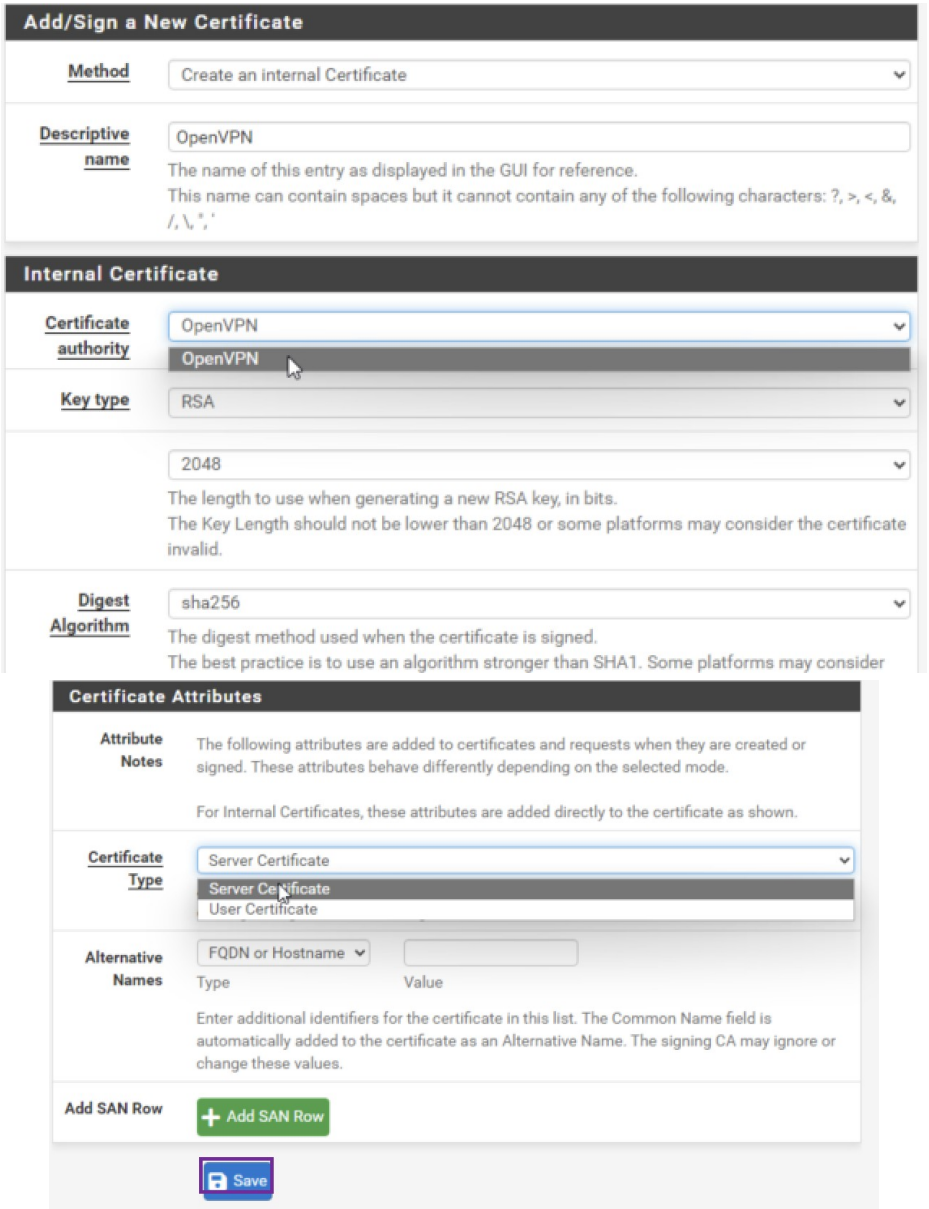


L'autorisation est bien créée, nous créons maintenant le certificat correspondant.



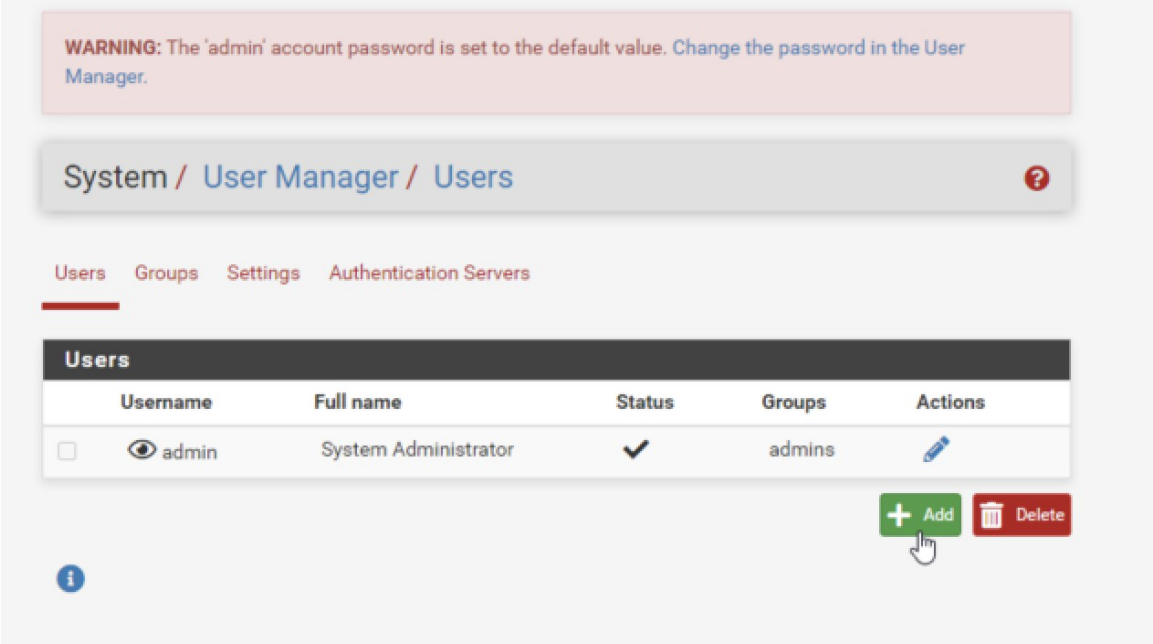
Cliquez sur « ajouter ».

Nous allons ici créer un certificat d'autorisation serveur, nous modifierons alors 3 champs ;
-le champ de description de nom que vous adapterez à votre situation (ici OpenVPN).
-le champ d'autorisation de certificat ; ici nous sélectionnons celui créé ultérieurement.
-le type de certificat ; qui sera ici pour un serveur.

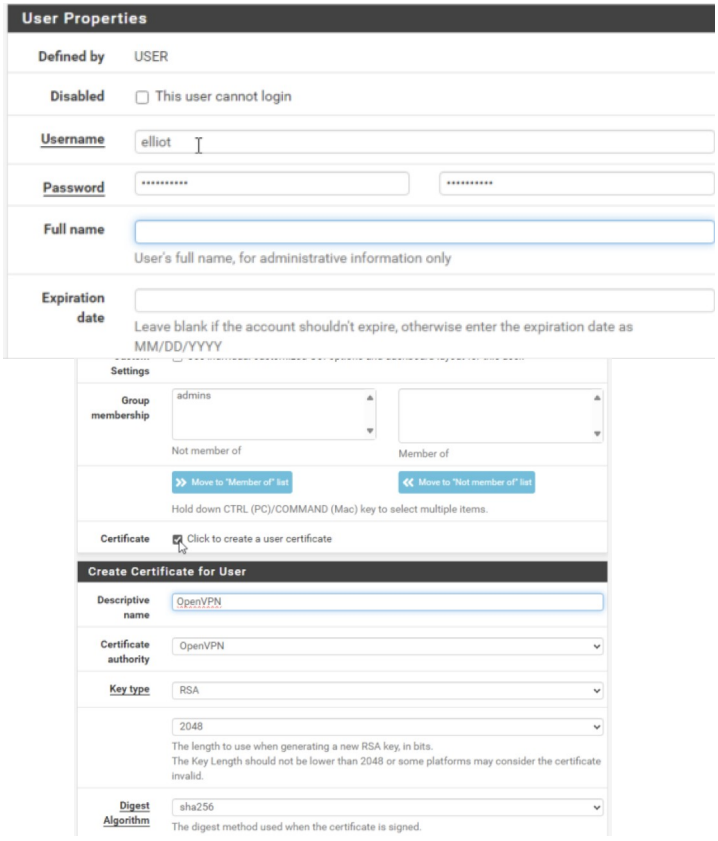


Et, bien sûr, on n'oublie pas de sauvegarder nos paramètres.

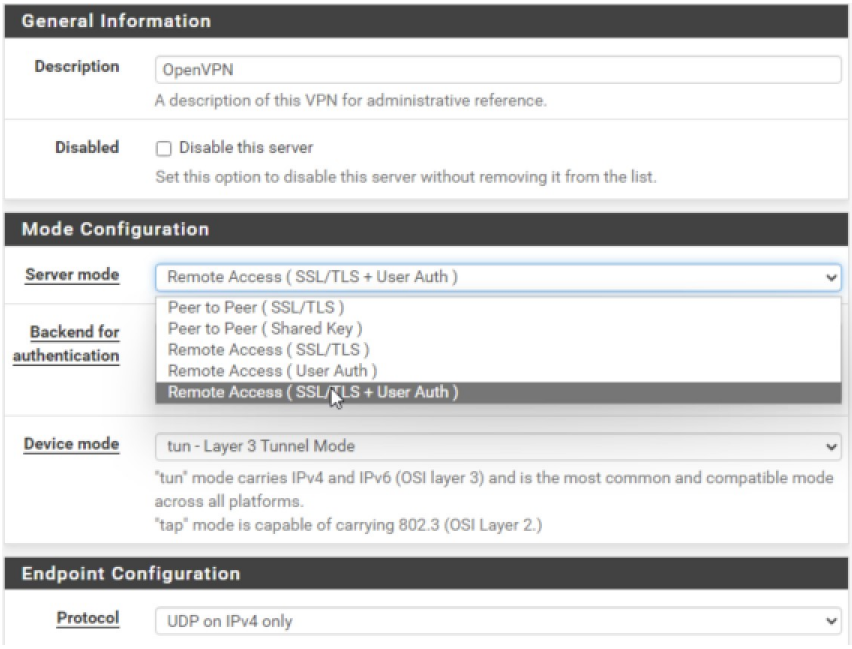
Nous créons maintenant notre utilisateur, toujours dans l'arborescence de « System » mais cette fois-ci dans « User Manager » nous cliquerons sur ajouter.



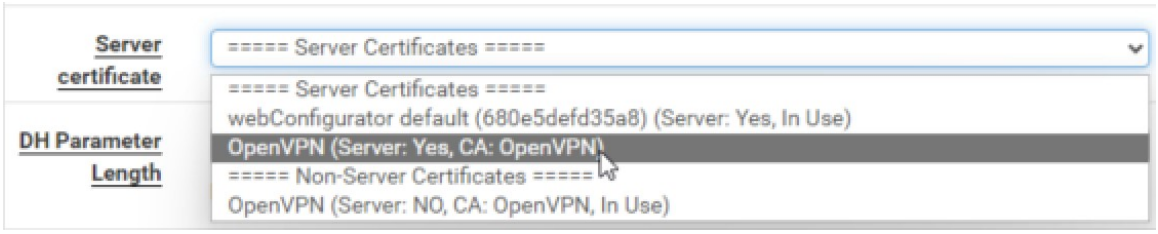
Sur la suite de la création, cochez la case afin de créer un certificat utilisateur correspondant



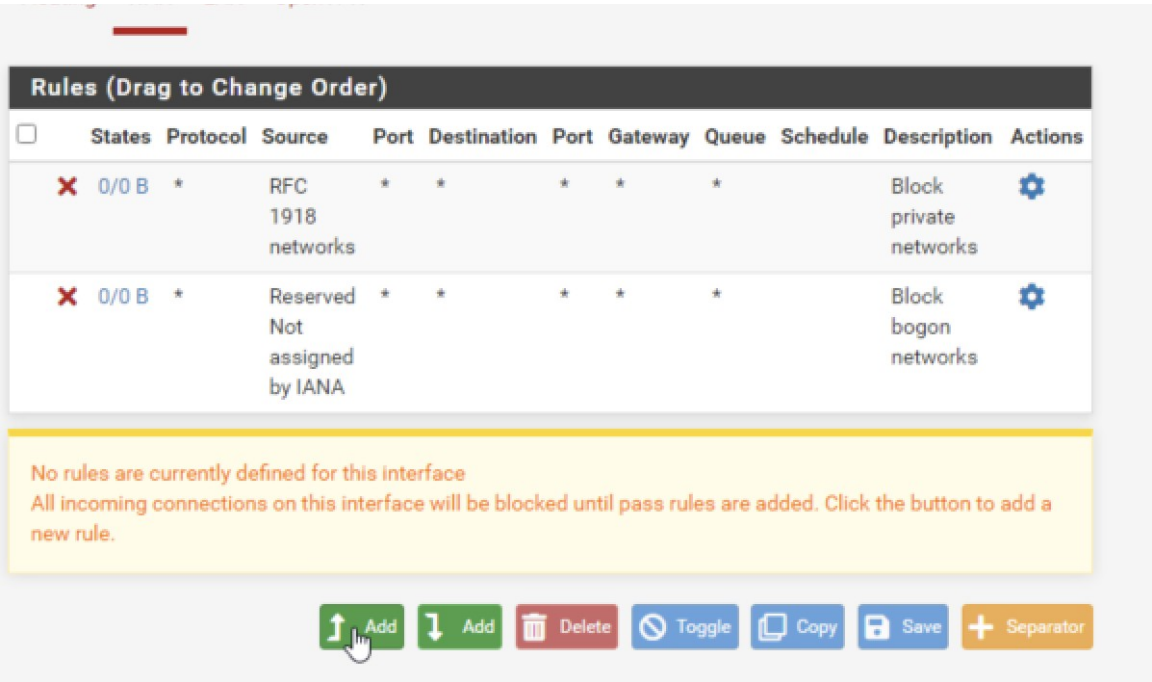
Il nous faut désormais créer une autorisation afin d'autoriser la connexion à distance à OpenVPN
Rendons nous donc dans « VPN », « OpenVPN », « Servers » ou nous cliquerons sur ajouter.
Le nom peut être différent, cependant il est impératif de choisir « Remonte Access (SSL/TLS + UserAUTH) » dans « Server mode »



Il faut aussi choisir le certificat précédemment créé ;

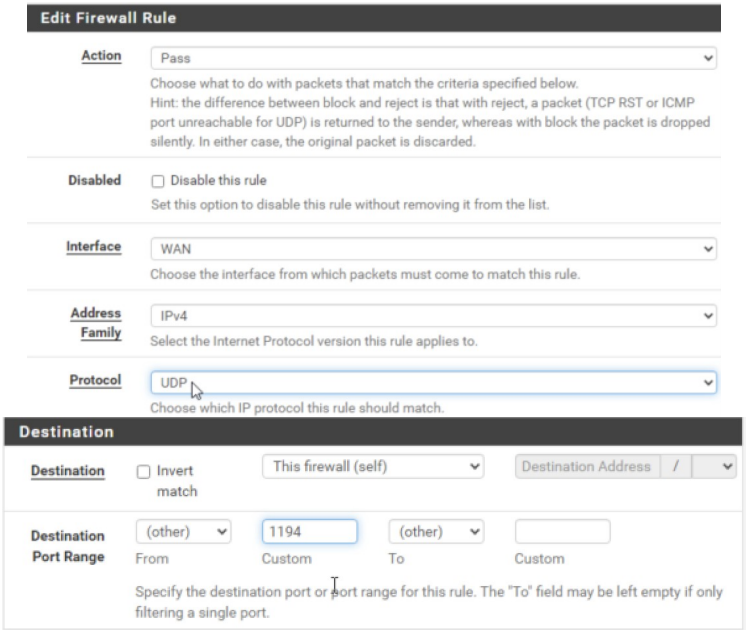


Allons maintenant dans le paramétrage du Firewall, afin de définir une règle sur la patte WAN de notre PfSense…

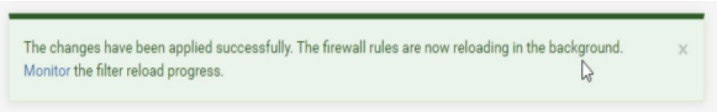


Nous ajoutons une nouvelle règle

Dans cette dernière, nous autoriserons le protocole UDP à transiter avec l'action PASS, la destination elle sera le pare-feu, lui même, à travers le port 1194.



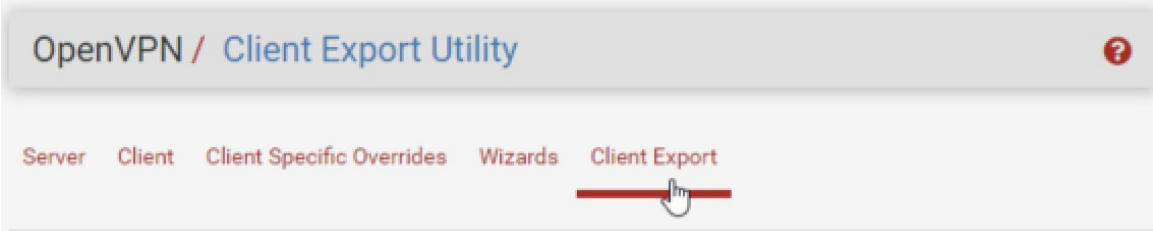
Encore une fois, on n’oublie pas de sauvegarder notre configuration.



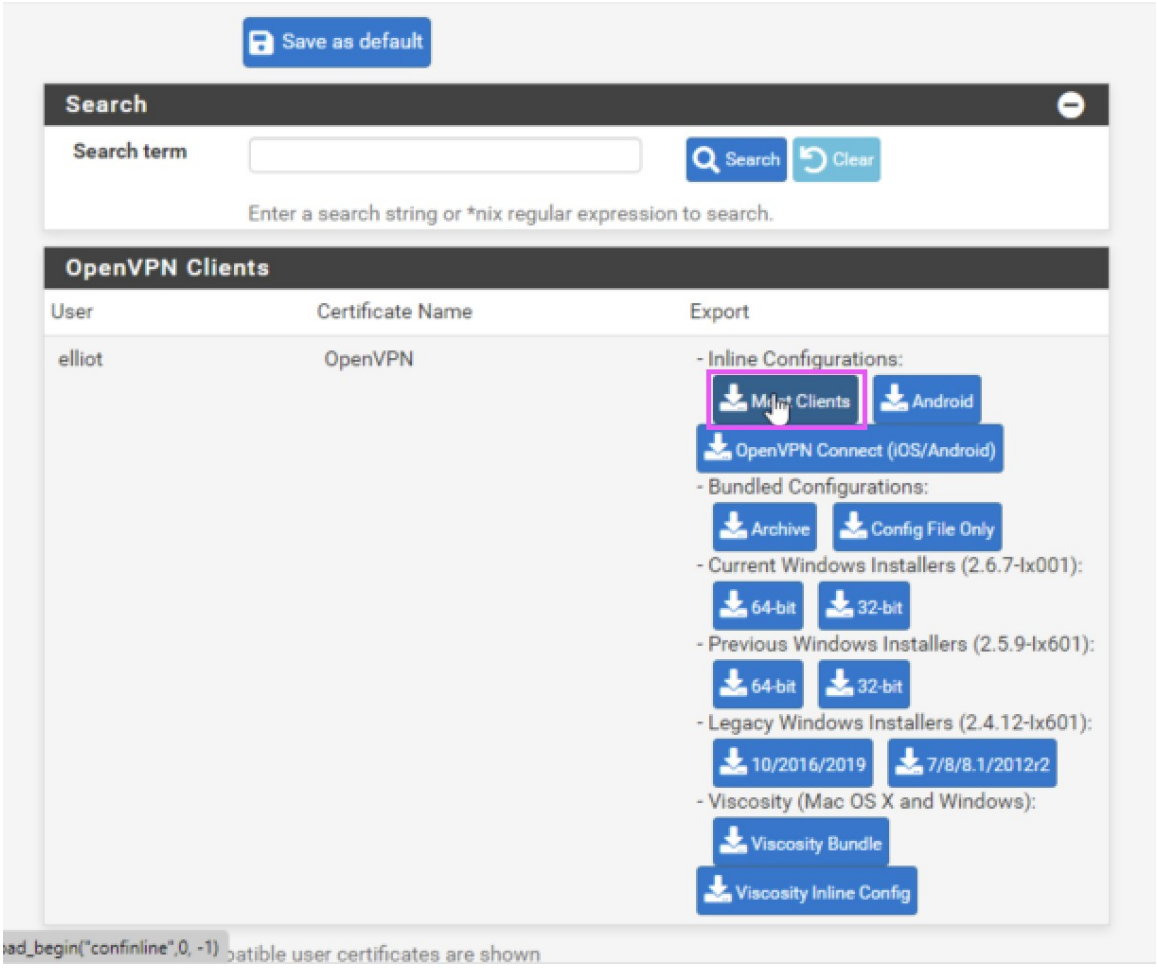
Installation du client

Afin d’installer le client OpenVPN, vous pouvez vous rendre sur ce lien ; [OpenVPN Client]

Nous devons au préalable faire un export de notre OpenVPN depuis l’interface de configuration PfSense, voici comment procéder ;

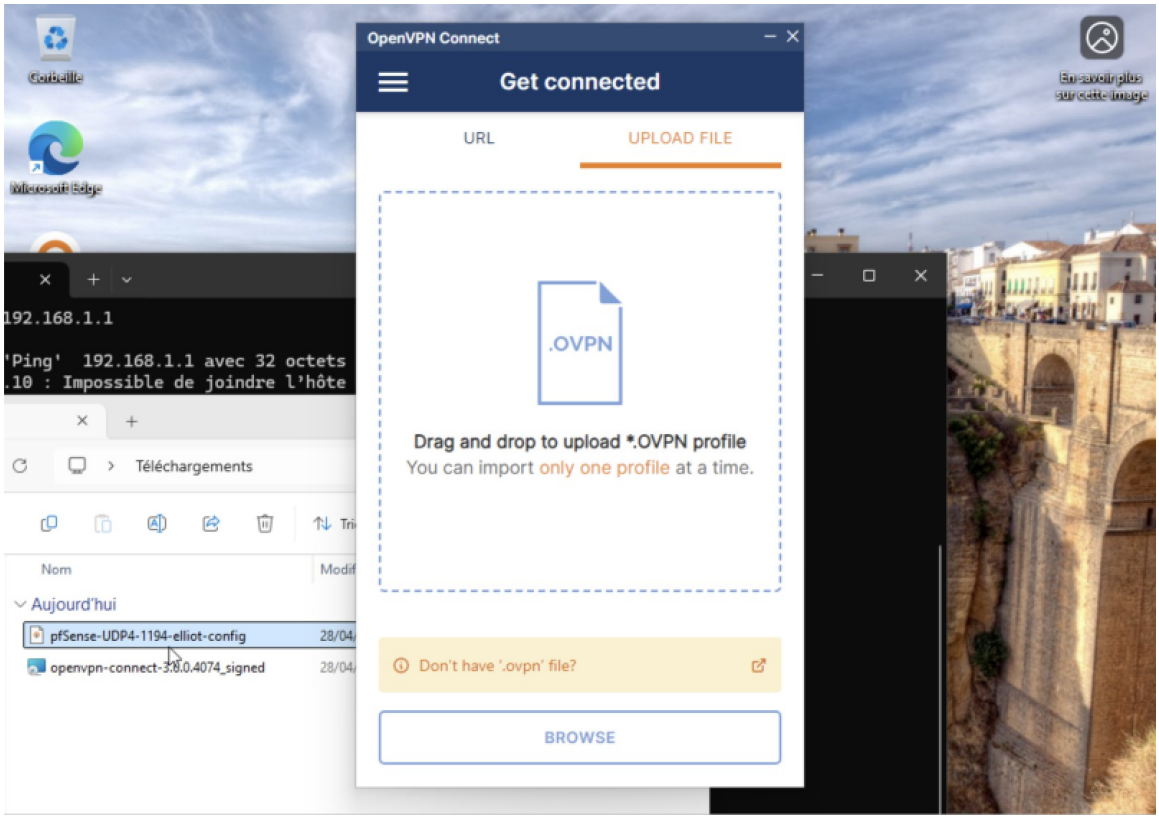


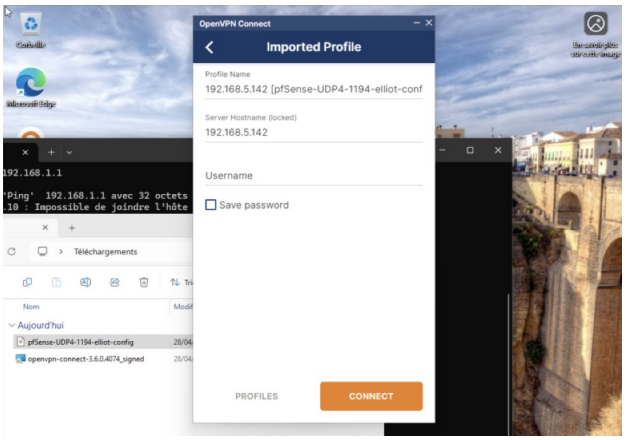
Sélectionner « Most Clients »



Il suffit désormais d'importer le fichier dans notre client OpenVPN puis de nous connecter avec l'utilisateur créé ultérieurement.

Je glisse ce fichier ici pour l'importer :





Vous pouvez établir la connexion avec l'utilisateur précédemment créé.