Formation BTS SIO – Option SISR

Réalisé par Pareja Tristan et Laurie Trintignac

Projet Gestion Horizons

Session 2023-2025

Sommaire

Introduction du Projet :

Contexte

Le cabinet Gestion Horizons, en pleine croissance, souhaite moderniser son infrastructure informatique afin d'assurer la sécurité, la disponibilité et l'accessibilité de ses données. Face à une utilisation croissante du numérique, les associés ont exprimé plusieurs besoins stratégiques :

- Protéger efficacement leurs données sensibles,
- Mettre en place un système de sauvegarde fiable,
- Permettre un accès sécurisé aux ressources depuis n'importe quel appareil (PC ou mobile, en local comme à distance),
- Et encadrer l'usage de l'informatique au sein du cabinet via des règles claires et des formations ciblées.

Le projet "Gestion Horizons" a été lancé dans ce cadre afin de proposer une architecture réseau sécurisée telles que :

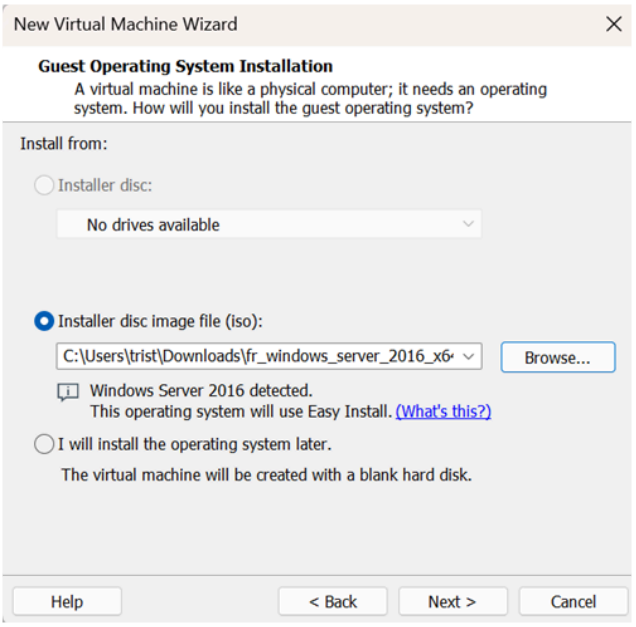
- un pare-feu (Pfsense)
- un serveur Active Directory pour la gestion centralisée des utilisateurs,
- une solution de sauvegarde automatisée,
- un accès distant via OpenVPN,
- et des outils de sécurité comme Mailinblack et CrowdStrike.

L'objectif est de permettre au cabinet de gagner en efficacité, en sécurité et en mobilité, tout en accompagnant les collaborateurs dans cette transition grâce à des sessions de formation et de sensibilisation.

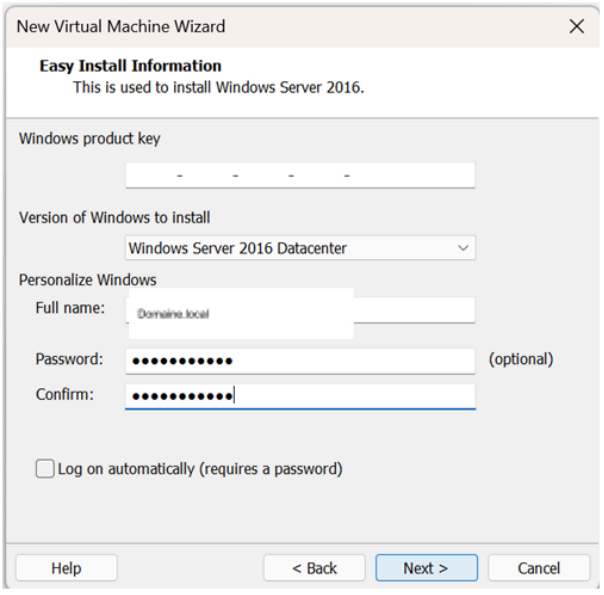
I – Création d'une VM Windows Server et compte administrateur

1. Création de la VM Windows Server

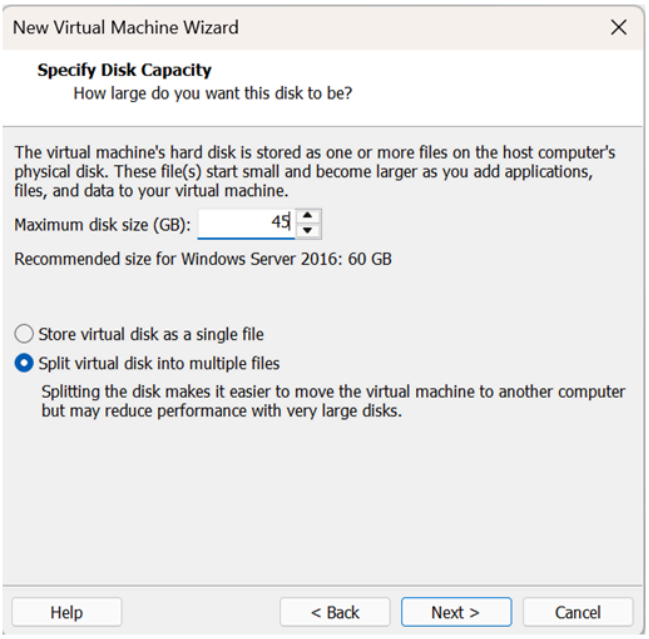
I. Nous allons commencer par créer notre VM Windows Server. Pour cela, vous avez juste à suivre les captures d'écran ci-dessous. Pensez à installer au préalable une image ISO de Windows Server.
Commencez la création d'une VM et pensez à sélectionner l'image ISO de Windows Server que vous avez installée. Nous utiliserons ici une ISO de Windows Server 2016.



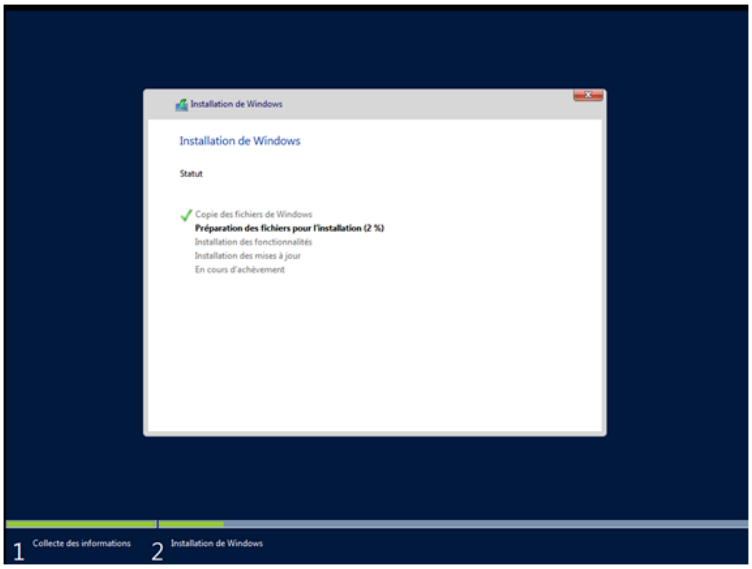
Appuyez sur Next, et une fois arrivé(e) à cette page choisissez un mot de passe et un nom.



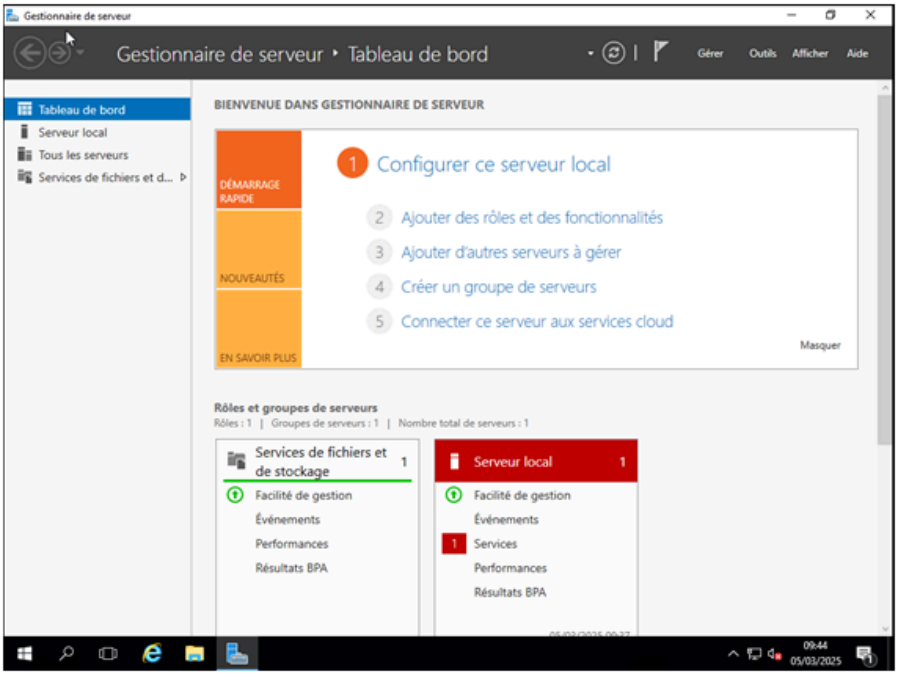
Concernant la taille, 45 GO vous suffiront largement pour ce que nous allons faire dessus.



Une fois fini, la suite de l'installation se fera toute seule. Vous avez juste à attendre que toute l'installation soit terminée.



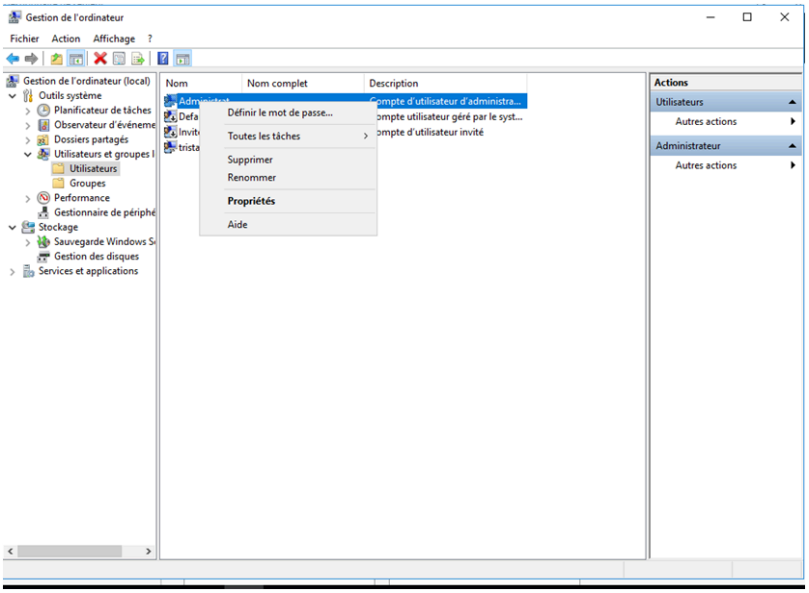
Une fois l’installation finie, votre VM se lance automatiquement et vous voici arrivé(e) sur la page d’accueil d’une VM Windows Server.



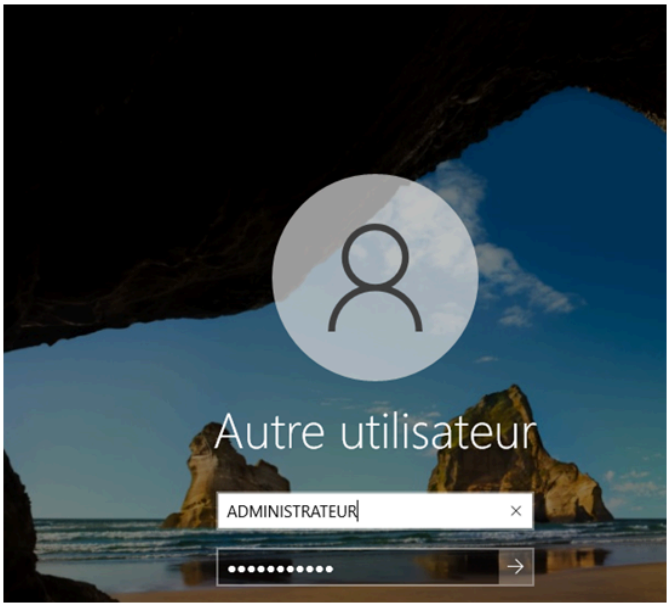
2. Passage sur un compte administrateur

Par la suite, il va falloir que vous soyez sur le compte administrateur sinon vous serez bloqués dans certaines étapes que nous allons réaliser.

Faites alors un clic droit sur votre icône Windows et rendez-vous dans « Gestion de l'ordinateur ». Une fois dedans, cliquez sur « Utilisateurs et groupes », puis « Utilisateurs ». Ouvrez donc le fichier, effectuez un clic droit sur le compte administrateur et sélectionnez « Définir le mot de passe ». Rentrez alors un mot de passe pour ce dernier.



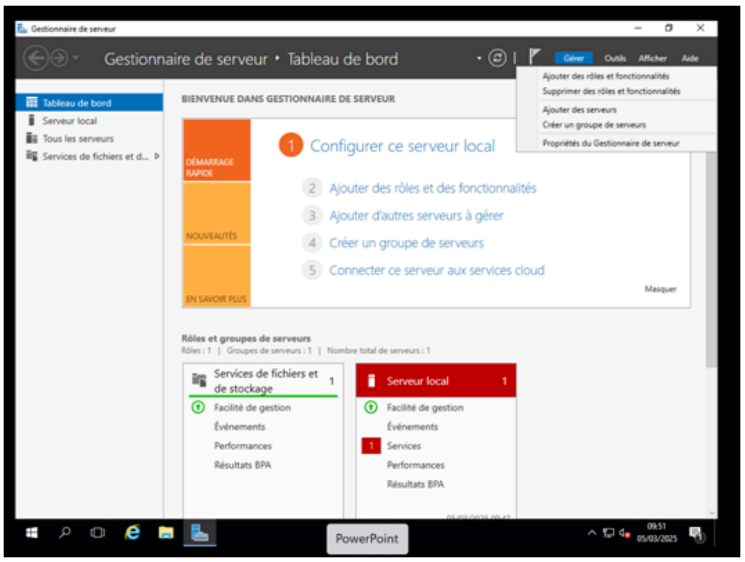
Vous pouvez alors vous déconnecter et changer de session afin de vous connecter à la session administrateur.



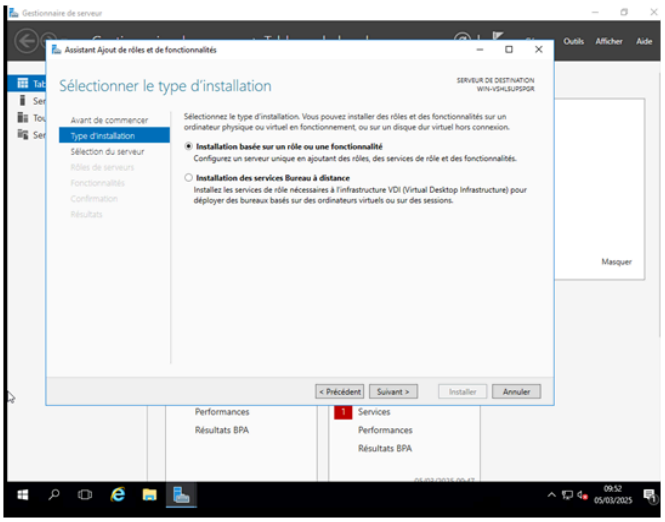
II – Création et configuration des rôles AD DS et DNS

1. Création des rôles AD DS et DNS

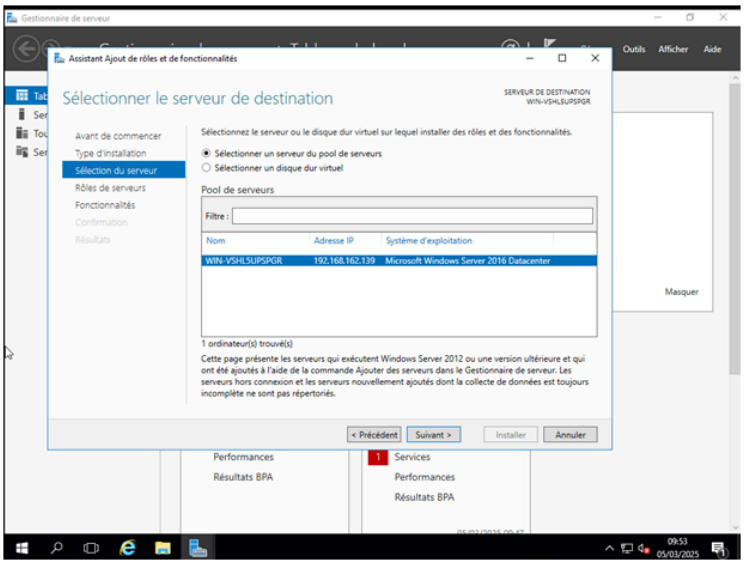
Nous allons commencer par créer chacun de nos rôles. La création se fera en même temps pour tous, mais il faudra en revanche les configurer un par un.
Commencez alors par cliquer sur « Gérer » et sélectionnez « Ajouter des rôles et fonctionnalités »



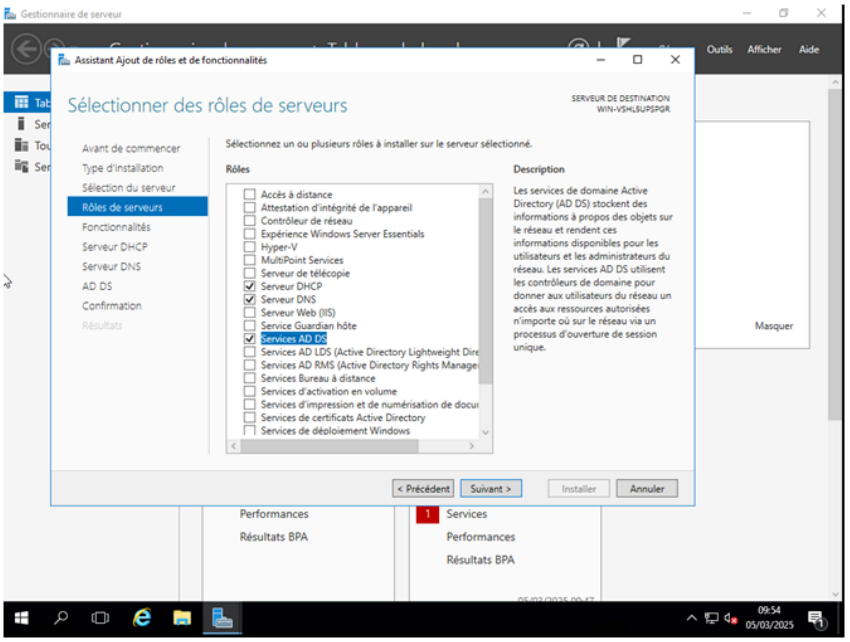
Une page d'installation s'ouvre, cochez la première case puis faites«Suivant»



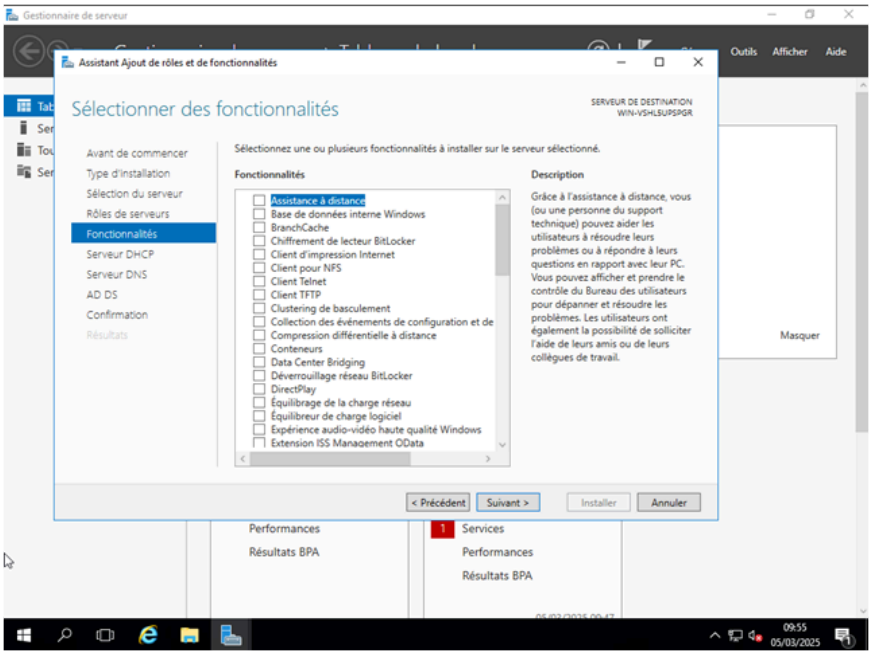
Sélectionnez tout bonnement votre serveur puis passez à l'étape suivante.



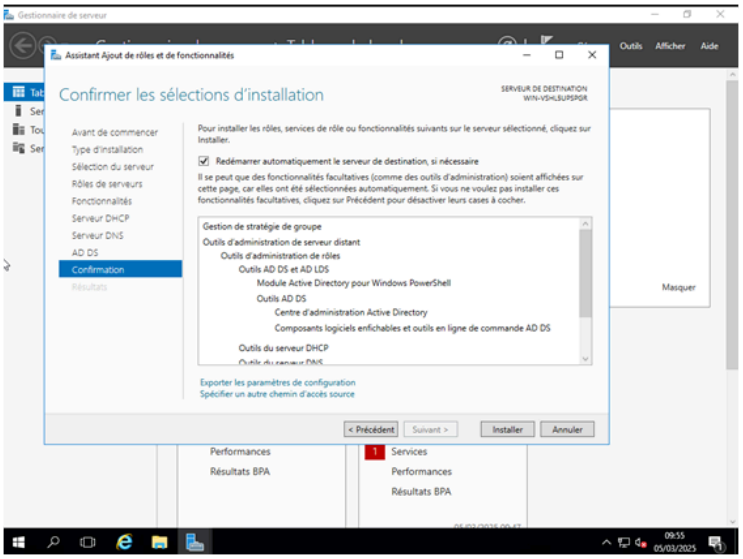
Vous arrivez alors à la sélection des rôles que vous souhaitez installer sur votre serveur. Comme dit précédemment, nous allons installer les rôles DNS et AD DS. Cochez ces rôles et passez à l'étape suivante.



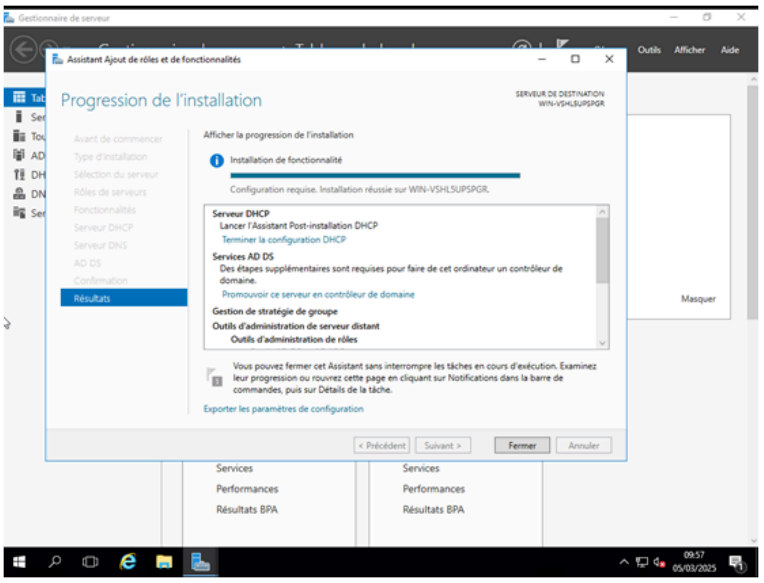
Concernant les fonctionnalités, vous pouvez ne rien faire et directement cliquer sur « Suivant »



Cliquez sur « Suivant » jusqu'à arriver à l'étape Confirmation. Sur cette page, cochez la case « Redémarrer automatiquement », puis cliquez sur le bouton « Installer » situé en bas à droite.

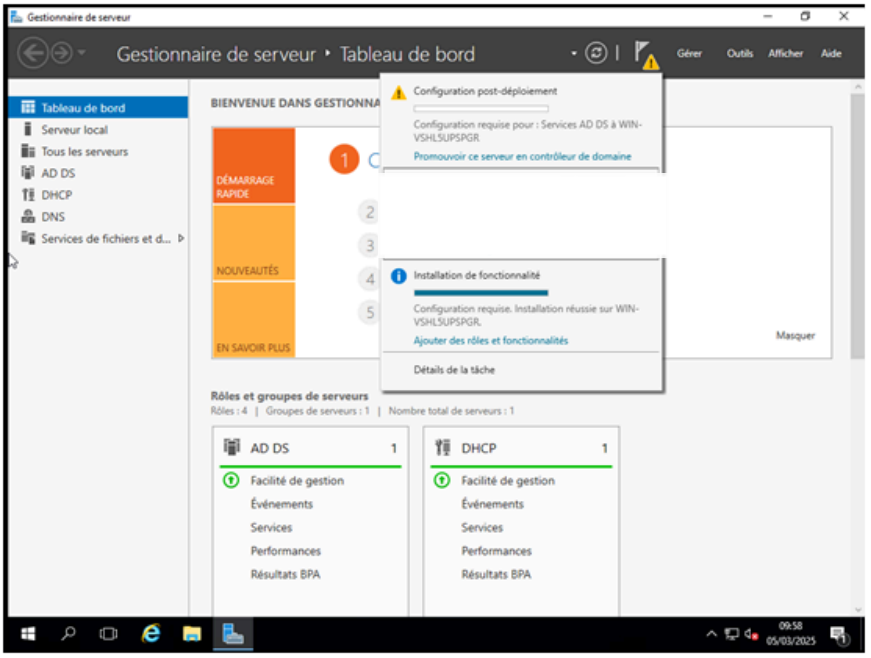


L’installation se fera toute seule, une fois finie vous n’avez qu'à cliquer sur « Fermer »



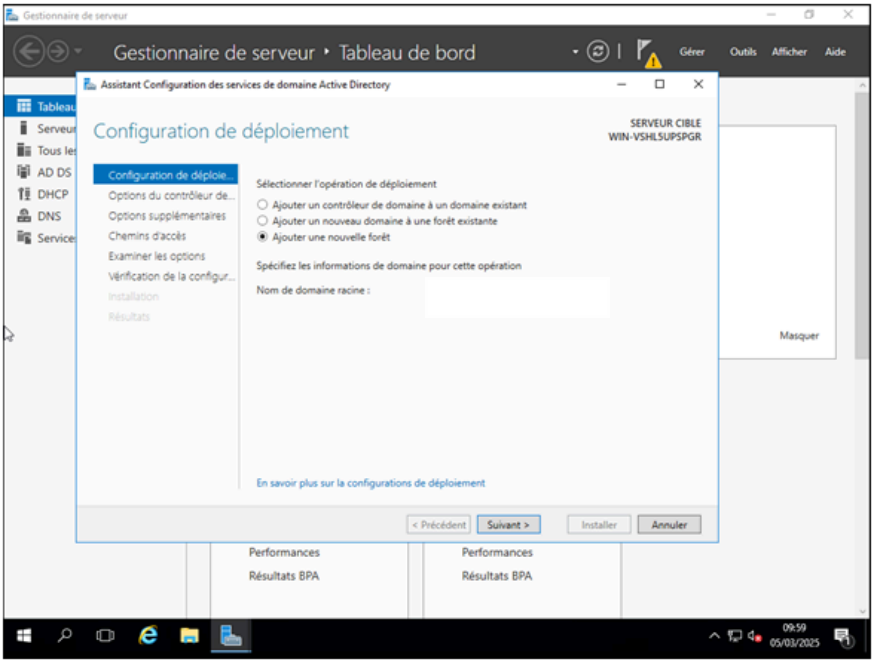
2. Configuration des rôles AD DS et DNS

Vous avez désormais tous les rôles installés, mais ce n’est pas fini, car il faut maintenant tous les configurer !

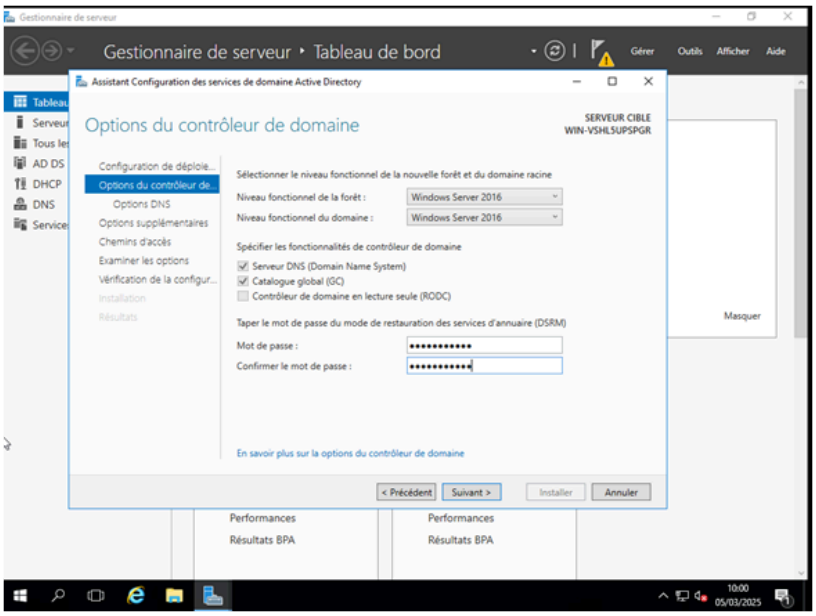


A. Configuration de l'AD DS / Domaine / Forêt

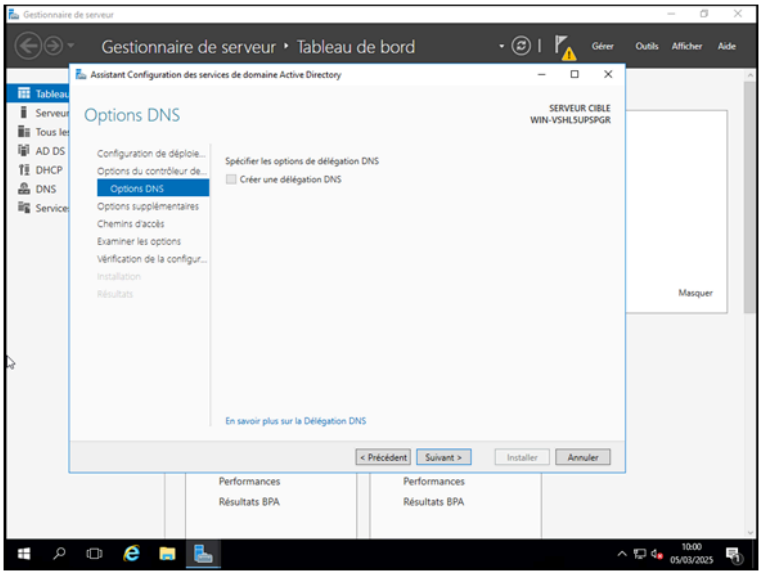
En cliquant sur le drapeau et sur « Promouvoir ce serveur en contrôleur de domaine », la page suivante va s'ouvrir. Choisissez d'ajouter une nouvelle forêt et entrez le nom de "domaine.local" que vous souhaitez créer.



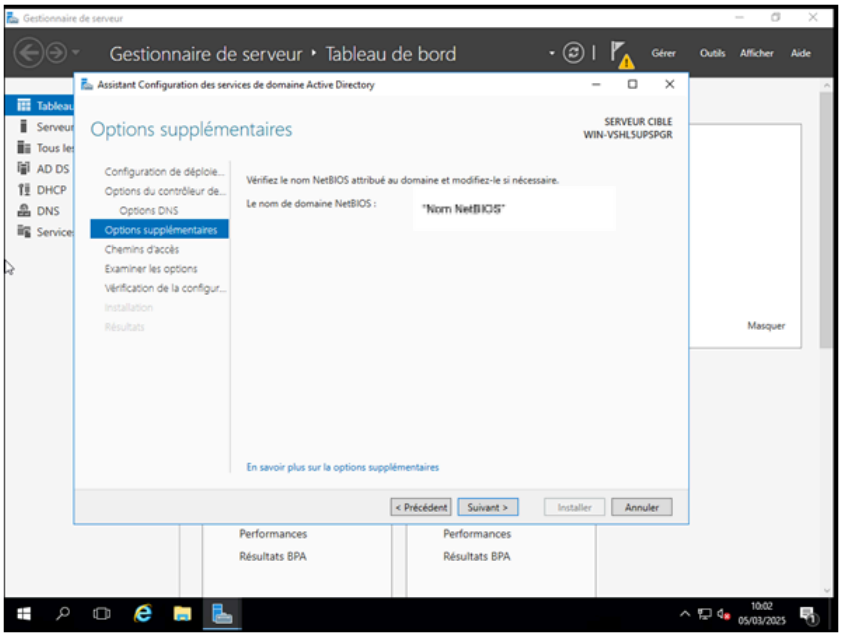
Pour la suite, sélectionnez les mêmes paramètres que sur l'image ci-dessous et choisissez en plus un mot de passe qui vous sera utile pour rejoindre ce domaine.



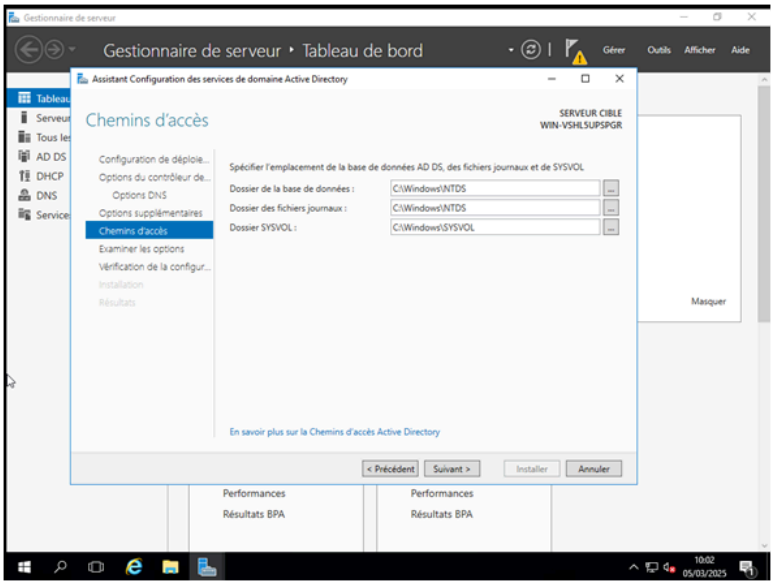
Concernant la délégation DNS, vous n'avez pas besoin d'en faire une ! Vous pouvez directement passer à l'étape suivante.



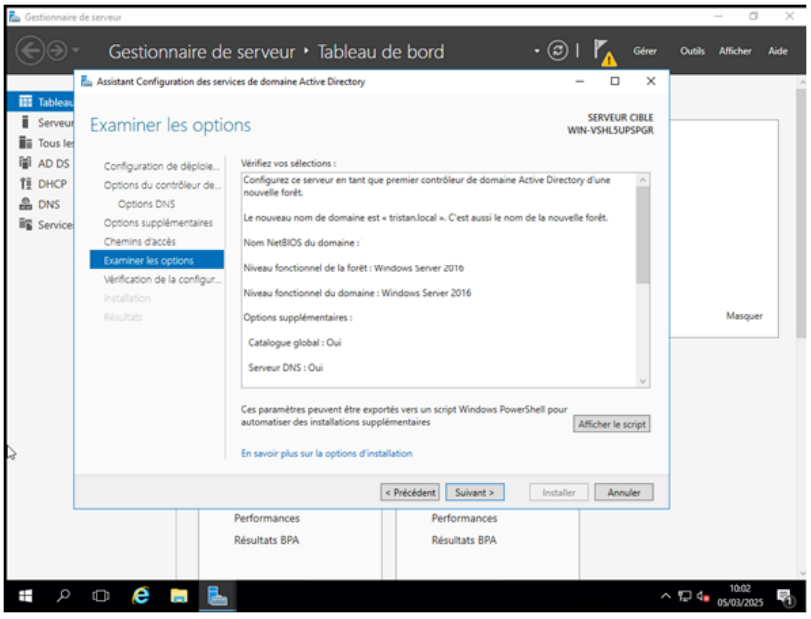
Ensuite, il vous sera demandé un nom de domaine NetBIOS. Choisissez alors ce que vous voulez, mais souvenez-vous-en.



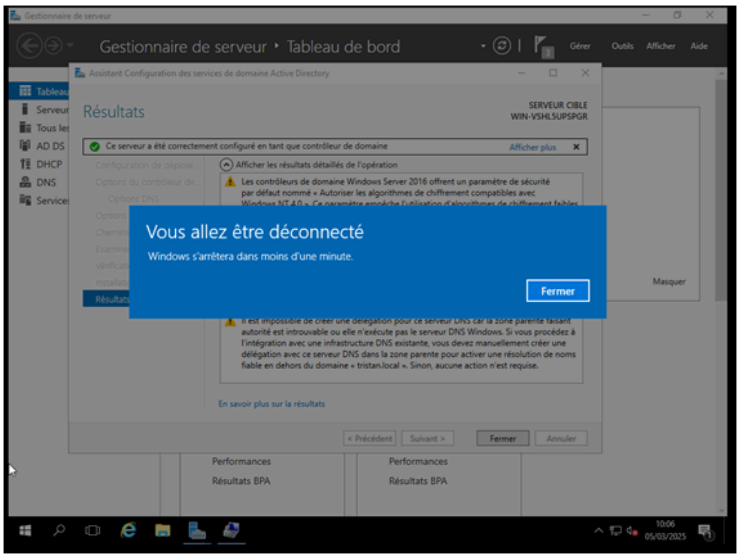
Sur cette étape, ne touchez à rien et laissez les dossiers sélectionnés par défaut.



Vous voici devant un petit récapitulatif de vos choix. Si vous avez tout suivi, vous devriez avoir quelque chose de similaire. Bien sûr, le nom changera ainsi que la version de Windows Server si vous n'avez pas pris la même.



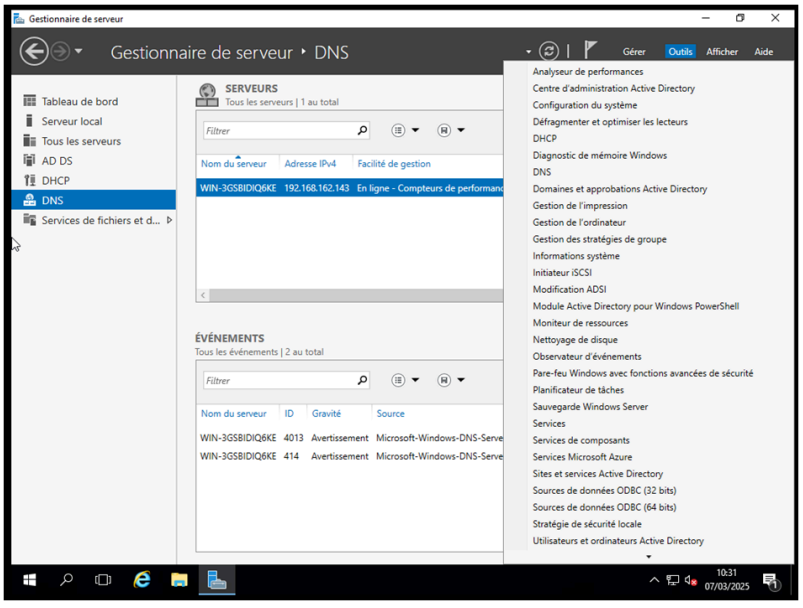
Vous avez alors fini de configurer l'AD DS ! Vous possédez désormais un domaine ainsi qu'une forêt qui pourra être rejointe par d'autres VM. C'est d'ailleurs ce que l'on fera à la fin avec une VM Windows. Cependant, vous n'avez pas encore fini puisqu' il reste encore le DNS à configurer. Cliquez alors sur « Fermer » et votre VM va redémarrer toute seule.



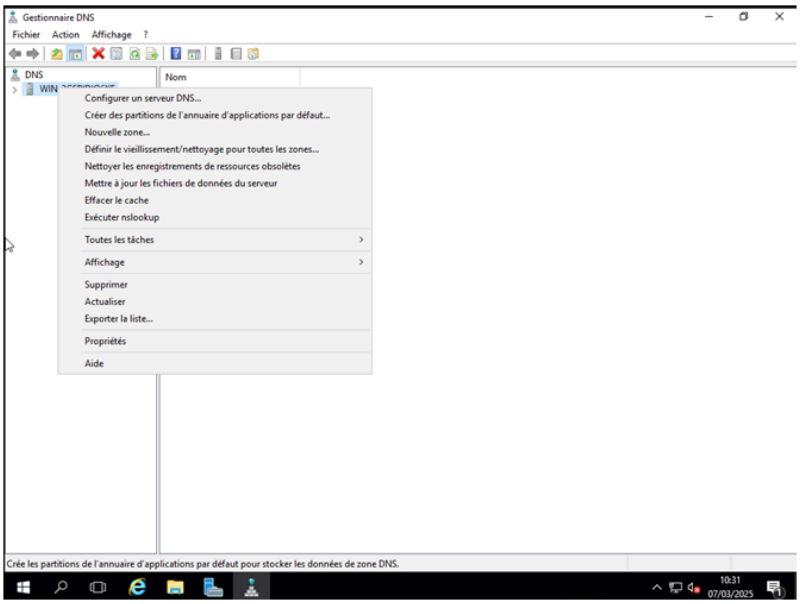
B. Configuration du DNS

Nous allons maintenant pouvoir passer à la configuration du DNS.
Un DNS sert à traduire les noms de domaine (comme google.com) en adresses IP compréhensibles par les ordinateurs. Il permet d'accéder aux sites web sans avoir à retenir leur adresse IP. C'est un peu les pages jaunes d'internet !

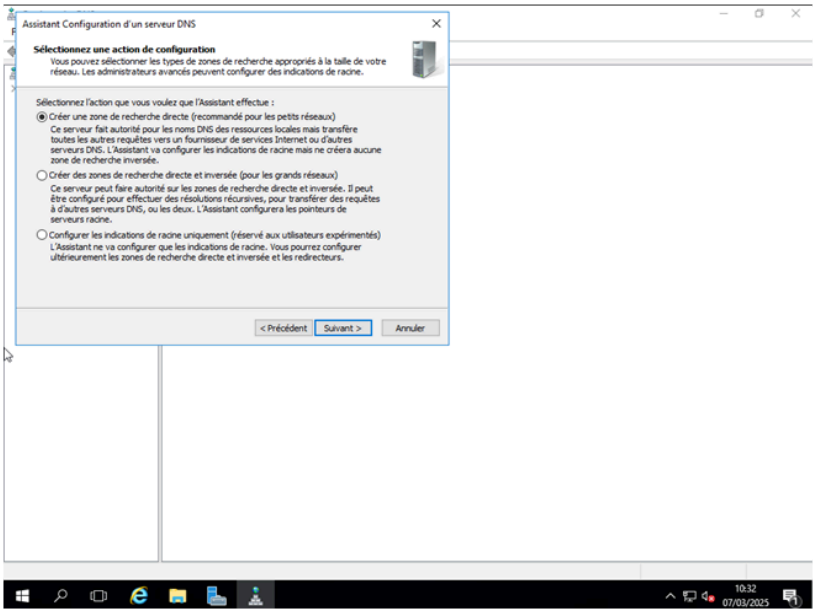
Cliquez sur « Outils » et sélectionnez « DNS » dans le menu déroulant.



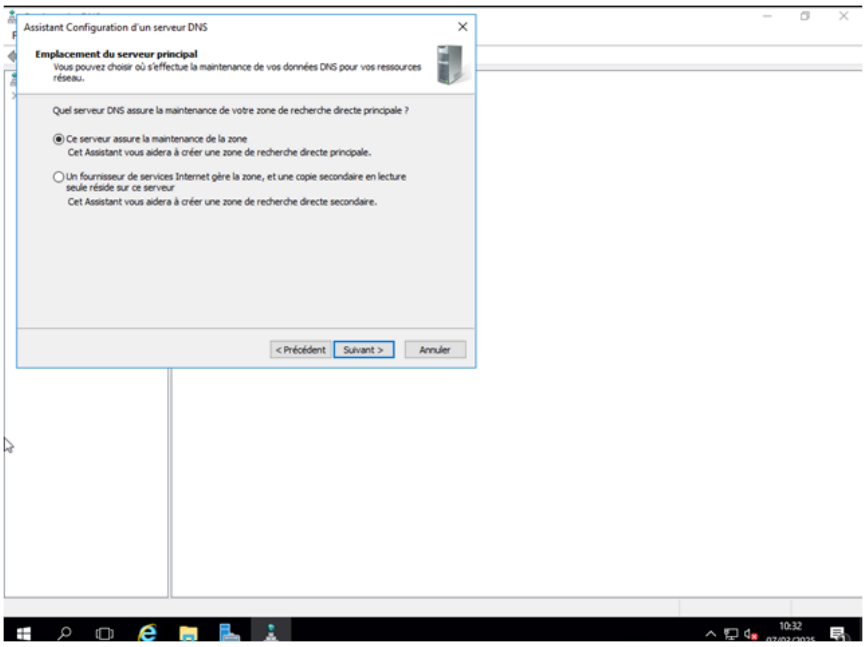
La page ci-dessous va s'ouvrir, cliquez alors sur « Configurer un serveur DNS »



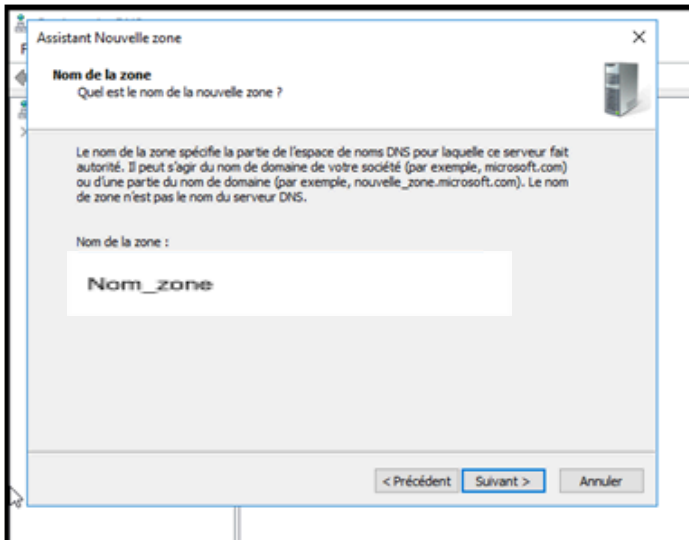
Laissez la première option qui sera déjà automatiquement cochée puis passez à l'étape suivante.



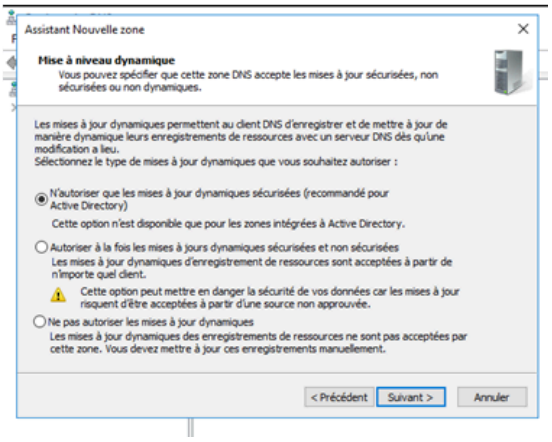
Tout comme l'étape précédente, laissez la première option, qui est elle aussi sélectionnée automatiquement, puis passez à l'étape suivante.



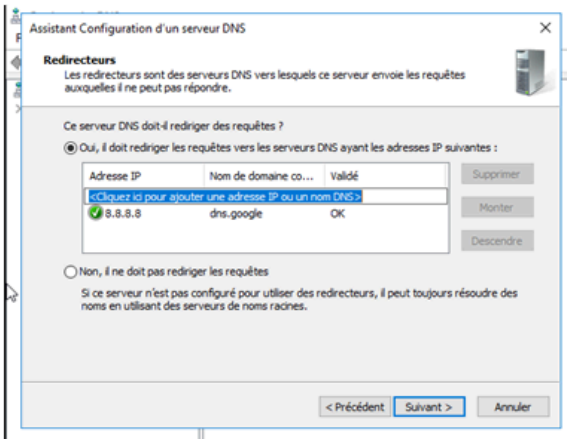
Désormais, choisissez le nom de la zone. Vous pouvez, si vous le voulez, choisir le même nom que vous aviez choisi pour la création de votre domaine.



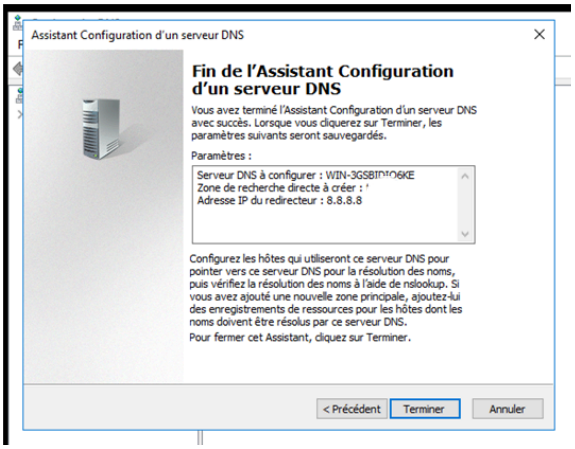
Encore une fois, laissez la première option, qui sera automatiquement cochée lorsque vous arriverez sur la page. Vous pouvez alors passer à l'étape suivante.



Ici, on nous demande de choisir un redirecteur. Notre DNS enverra une requête à ce dernier pour obtenir une réponse à une demande, si jamais il ne l'a pas. Nous allons entrer 8.8.8.8, qui n'est autre que l'IP du DNS de Google.



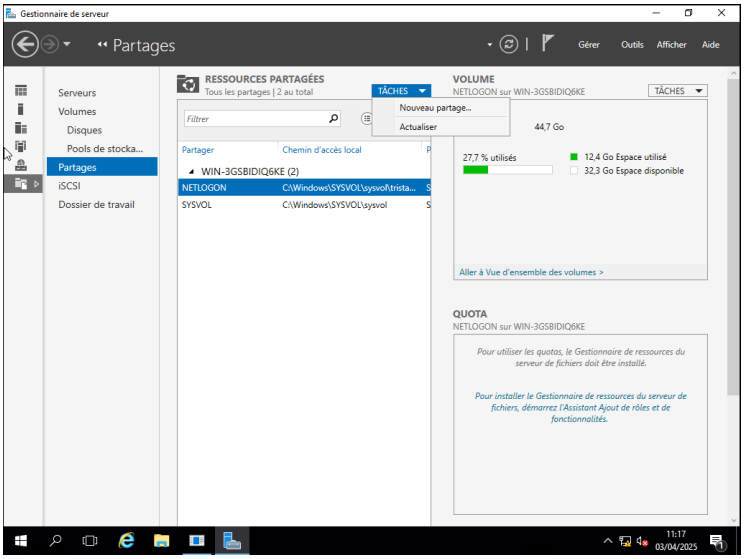
Et voilà, vous avez désormais aussi terminé la configuration de votre DNS. Cliquez sur le bouton « Terminer » et la page se fermera.



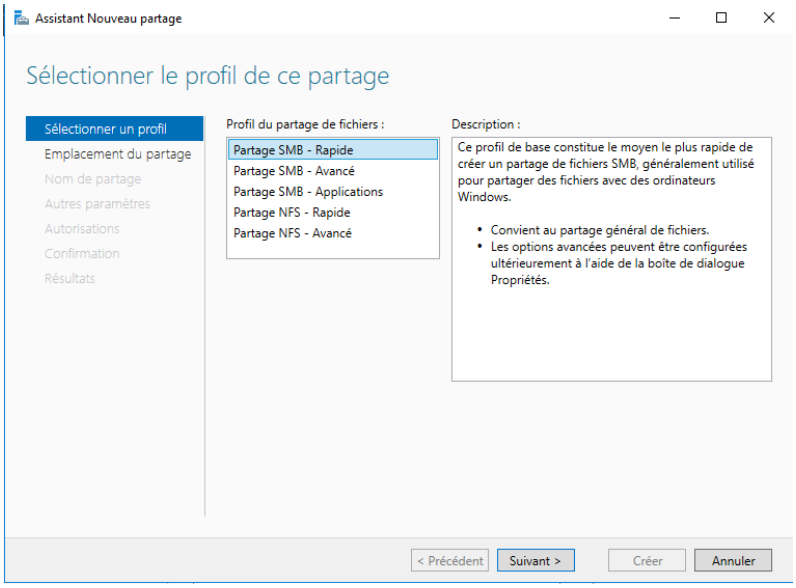
III - Création d’un serveur de sauvegarde et dossier partagé ainsi que mise en place d’un Raid 5

1. Création d’un serveur serveur de sauvegarde et dossier partagé

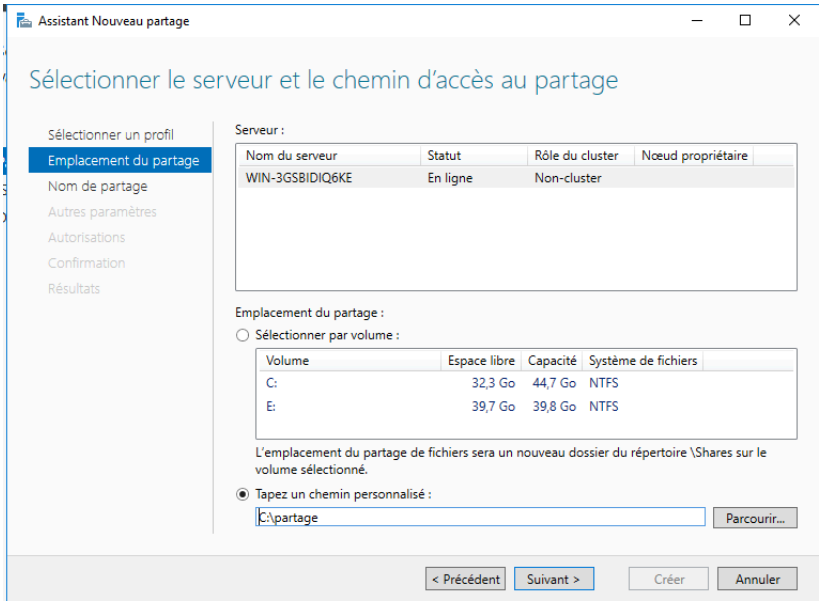
Pour commencer la création de votre serveur de sauvegarde, rendez-vous dans l’onglet “Partages” dans le gestionnaire de serveur, cliquez sur “Tâches” et “Nouveau partage”



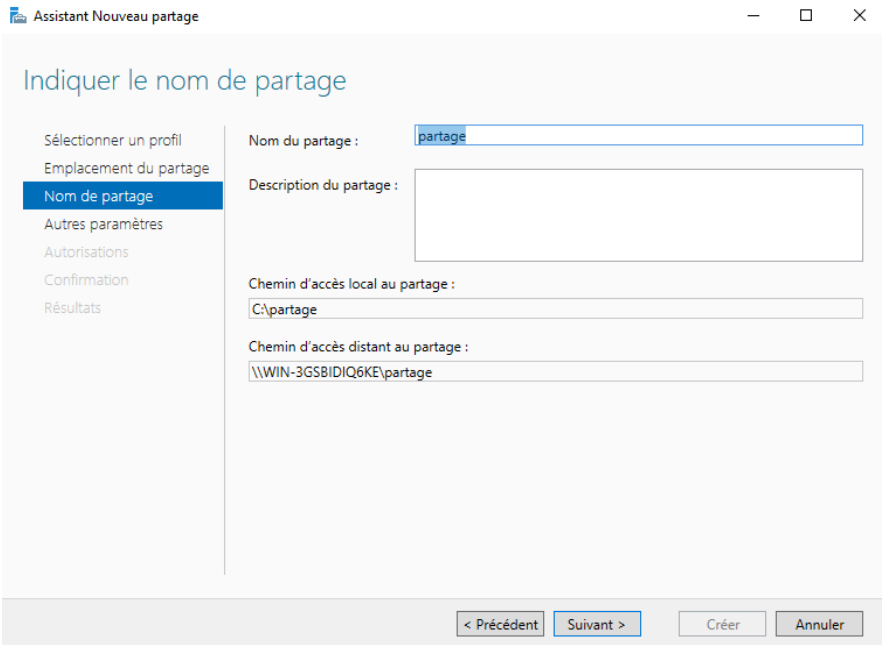
Par la suite, sélectionnez le “Partage SMB - Rapide” et faites “Suivant”



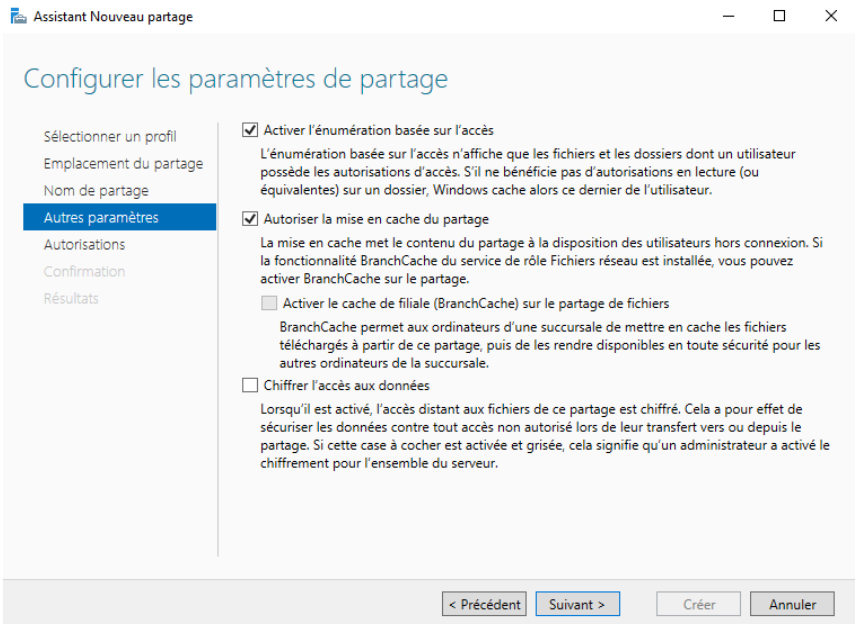
Ici, vous allez devoir choisir votre serveur mais surtout le chemin d'accès au partage. Nous vous conseillons alors de créer un dossier au préalable afin de choisir un chemin personnalisé pour ce dernier.



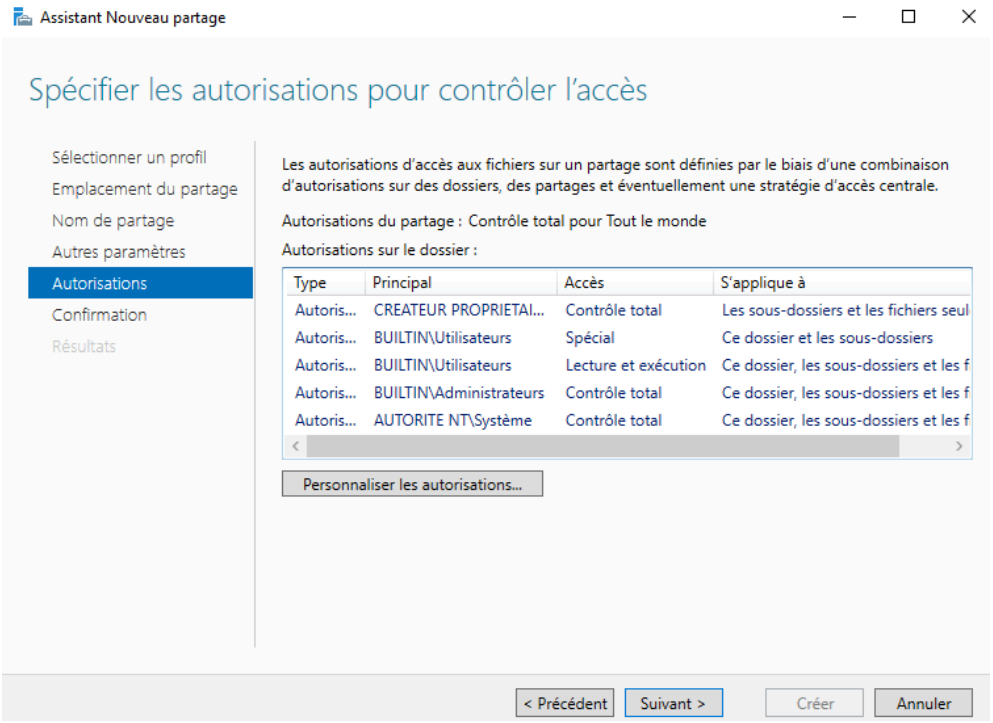
Dans la prochaine étape il suffira tout simplement de donner un nom à ce partage, vous pouvez en plus si vous voulez lui donner une description.



Dans cette étape, nous devons choisir certains paramètres pour le partage. Seulement deux d'entre eux nous intéressent. Activer alors l'énumération basée sur l'accès (la première case) et La mise en cache (la deuxième case)

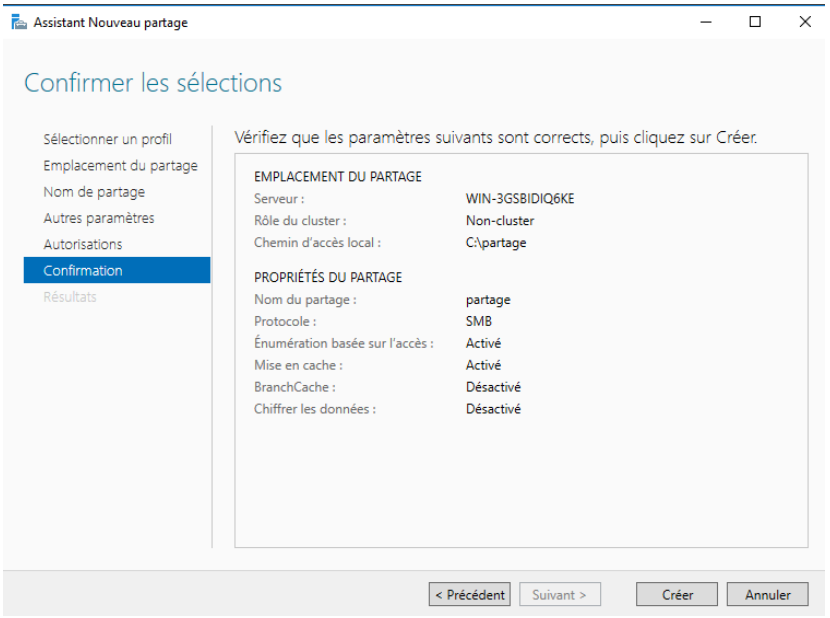


Vous accédez désormais à la page des autorisations, nous n'avons rien à spécifier en particulier alors cliquez directement sur "Suivant"

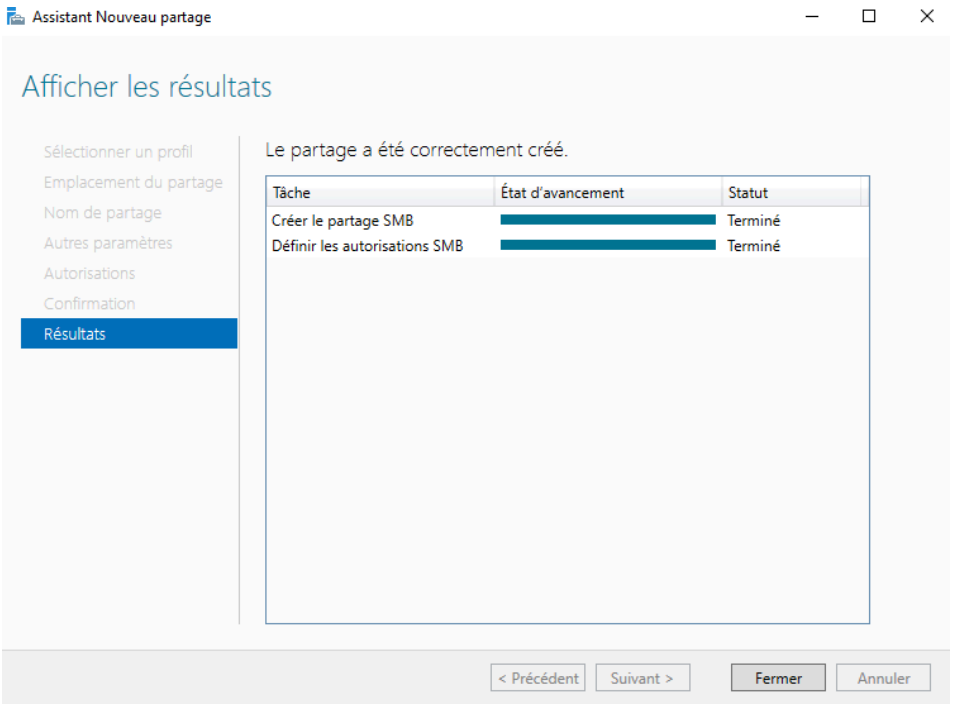


Nous arrivons désormais à la fin de notre paramétrage, Vous avez sur cette page un récapitulatif de ce que vous venez de faire, les fonctionnalités activées ou encore le chemin d'accès du partage.

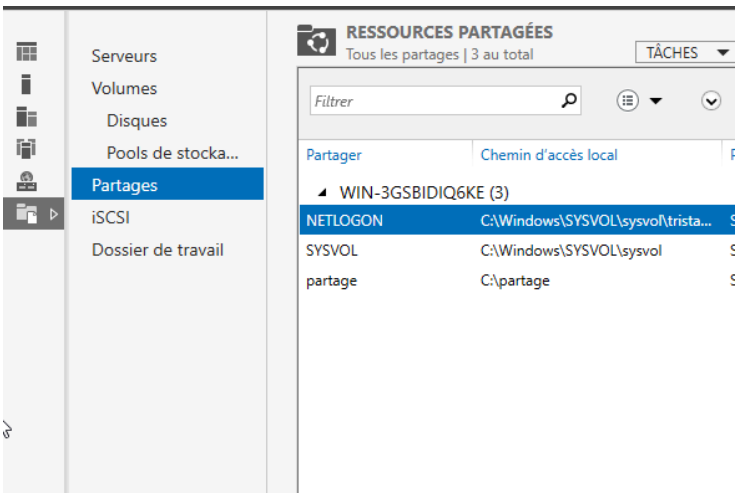
Vous pouvez si tout est bon cliquez sur “Créer”



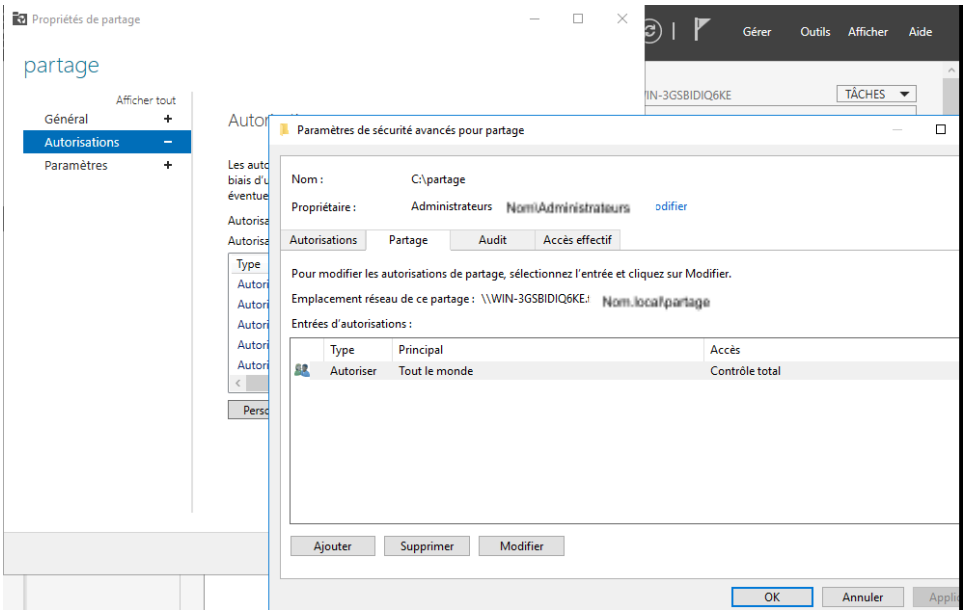
Une fois que vous aurez cliquez sur “Créer” la page “Résultats” s’affiche. Cette dernière indique que le partage est bien fonctionnel ainsi que les autorisations qui y sont liées.



Désormais en revenant dans votre onglet “Partages” du gestionnaire de serveur, vous pouvez constater que votre partage existe bel et bien et c’est rajouter à la liste.

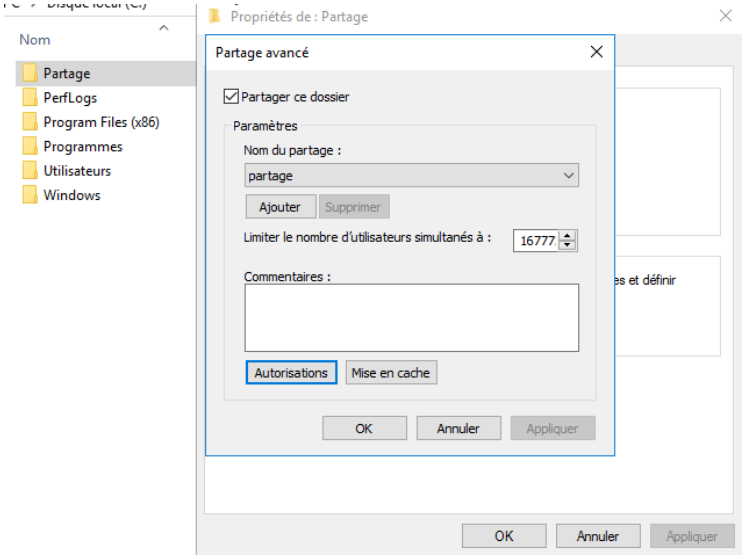


Afin que tout le monde ait accès à ce dernier, cliquez sur votre partage et rendez-vous dans les “Autorisations” Dans ce dernier vérifier que tout le monde y aura accès. Si vous le désirez vous pouvez en plus gérer l’accès à ce dernier (écriture, lecture, contrôle total).



Afin de bien s’assurer que tout le monde aura accès à votre dossier “Partage” rendez-vous sur ce dernier, réaliser un clique droit dessus - “Propriété” et cliquez sur “Partage avancé”

Une fois sur cette page allez dans “Autorisations” et rajoutez tout le monde à l’intérieur, ici nous donnons le “contrôle total” sur ce dernier à tout le monde.



2. Création d’un RAID 5 sur le serveur

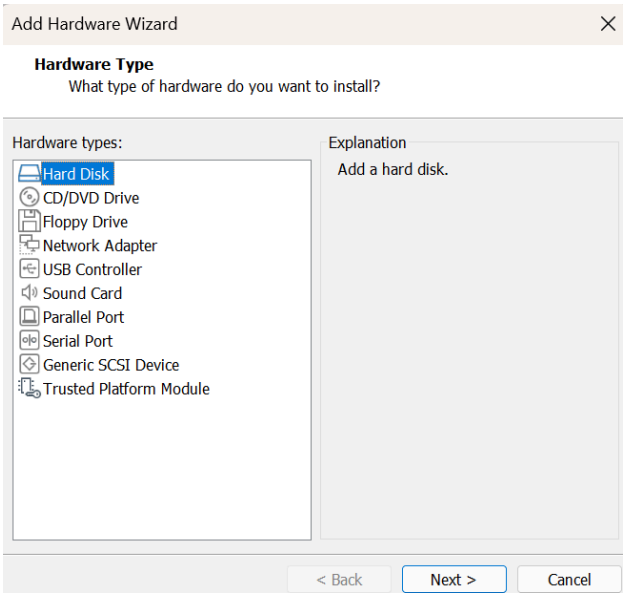
Pour commencer, à quoi sert-il d’avoir un RAID 5 et que permet-il?

Le RAID 5 est une solution de stockage utilisée pour sécuriser les données tout en gardant de bonnes performances. Il fonctionne avec au moins 3 disques, où les données et une parité (une sorte de sauvegarde) sont réparties. En cas de panne d’un disque, les données peuvent être récupérées grâce à celles présentes sur les autres. Ce système permet donc de continuer à fonctionner même si un disque tombe en panne.

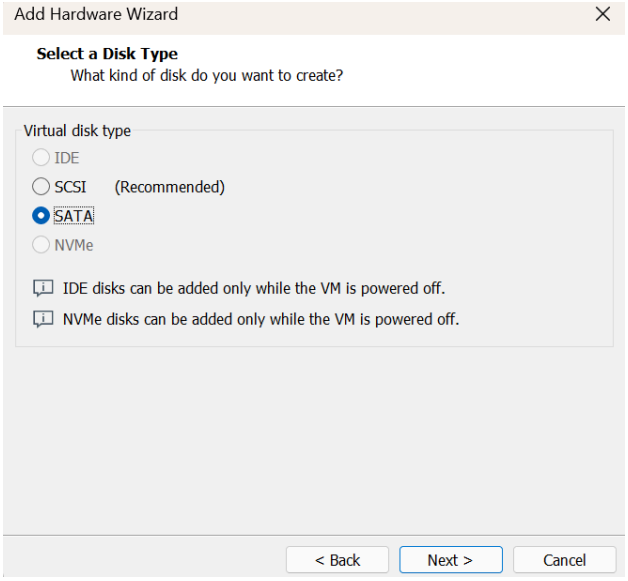
Le RAID 5 peut alors facilement assurer la continuité de l'activité si jamais un disque tombe en panne et il est très pratique pour cela.

Comme expliqué au dessus, le RAID 5 a besoin de 5 disques afin de pouvoir être configuré. De ce fait vous allez devoir répéter les deux prochaines étapes 3 fois afin d’avoir vos 3 disques qui seront réservé à votre RAID 5

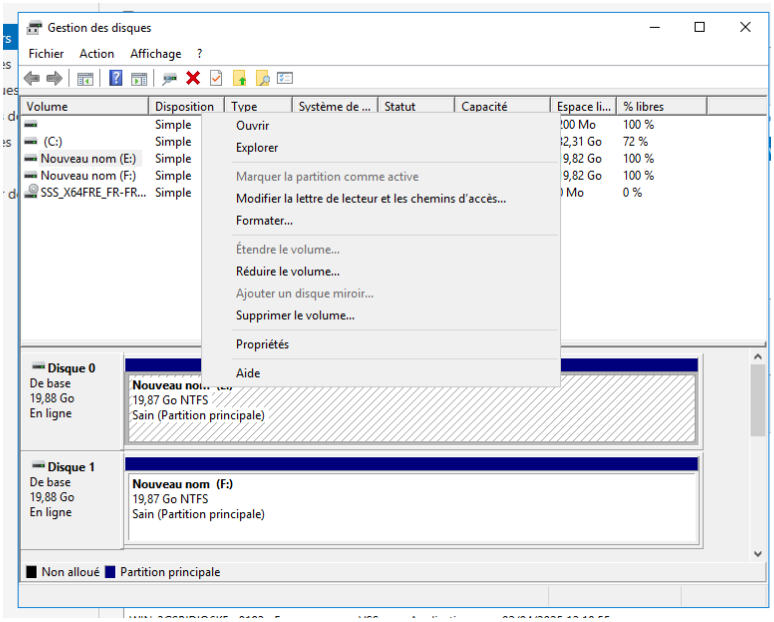
Rendez-vous dans les paramètres de votre VM, et ajoutez un équipement. Une fois dessus sélectionnez “Hard Disk”



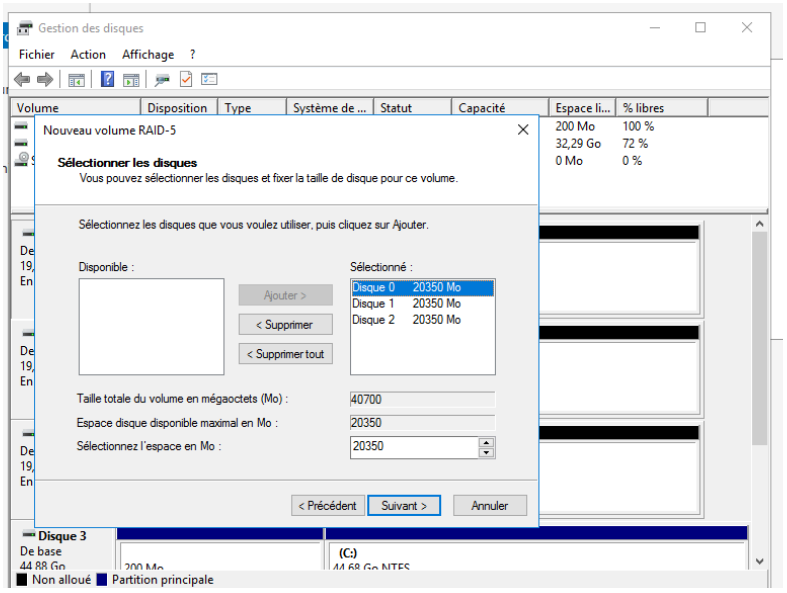
Une fois fait, il vous sera demandé le type de disque, pour du RAID nous allons choisir d’utiliser des disques SATA. Derrière vous seras demandé la taille du disque, de notre côté nous choisirons 20GO pour chaque disque.



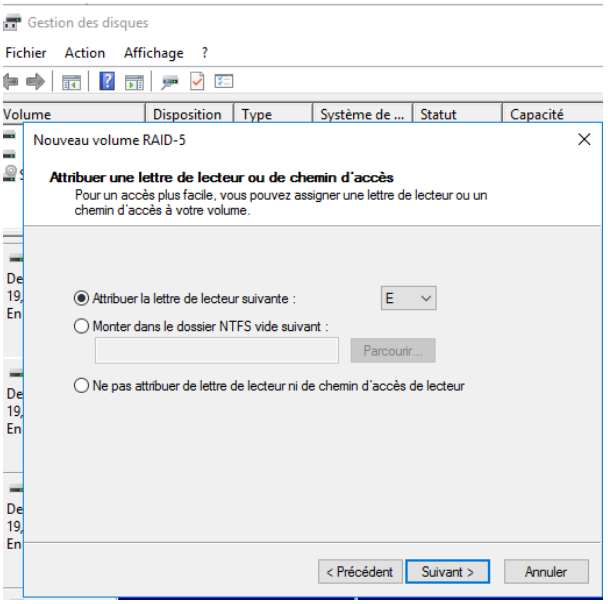
Une fois que vous avez répété l'opération 3 fois, vous pouvez redémarrer votre VM. Dans cette dernière, réaliser un clique droit sur le logo Windows et cliquez sur “ Gestion des disques” Vous pouvez constater que vos disques sont bel et bien présents !



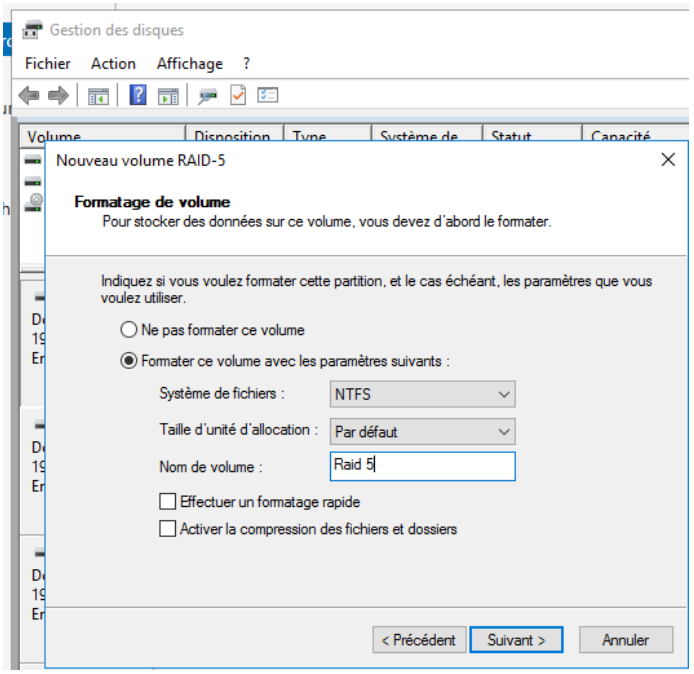
Réalisez un clique droit sur la petite barre bleu de votre disque et cliquez sur “Nouveau volume RAID-5” Une fois dessus sélectionnez les 3 disques créés précédemment pour la création de ce dernier.



Après avoir cliqué sur “Suivant” vous arrivez sur cette petite page. Ne touchez à rien il n’y a rien besoin de faire ici.

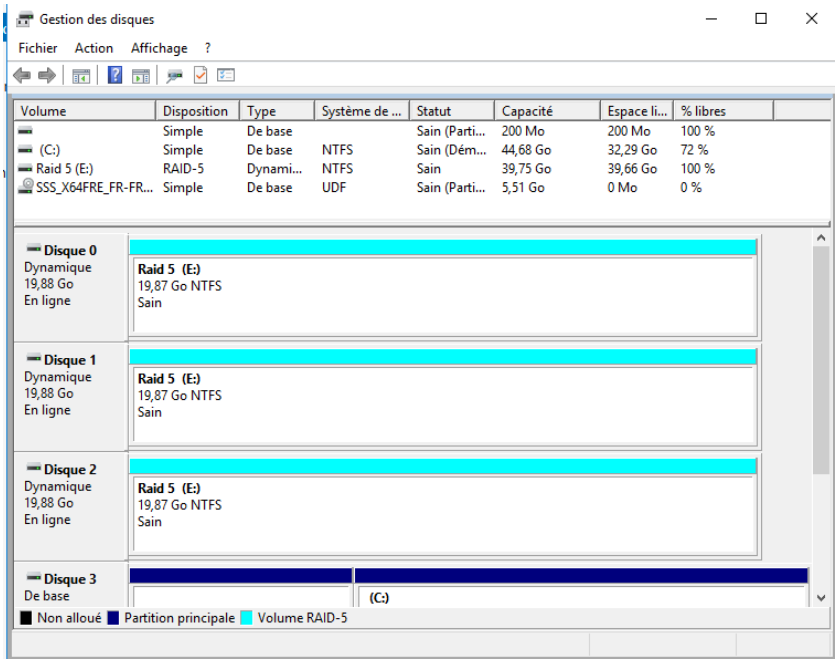


Maintenant vous allez devoir formater le volume afin de pouvoir réaliser un raid 5 avec vos disques.Pour “Système de fichiers” choisissez “NTFS” ensuite donné un juste un nom à votre volume



Par la suite vous aurez une sorte de chargement le temps que le volume se formate. Cette étape est assez rapide et vous devriez vite apercevoir cela dans la gestion des disques.

Vous pouvez alors constater que votre 3 disques font partie du Raid 5 et vous avez désormais terminé la mise en place de ce dernier.

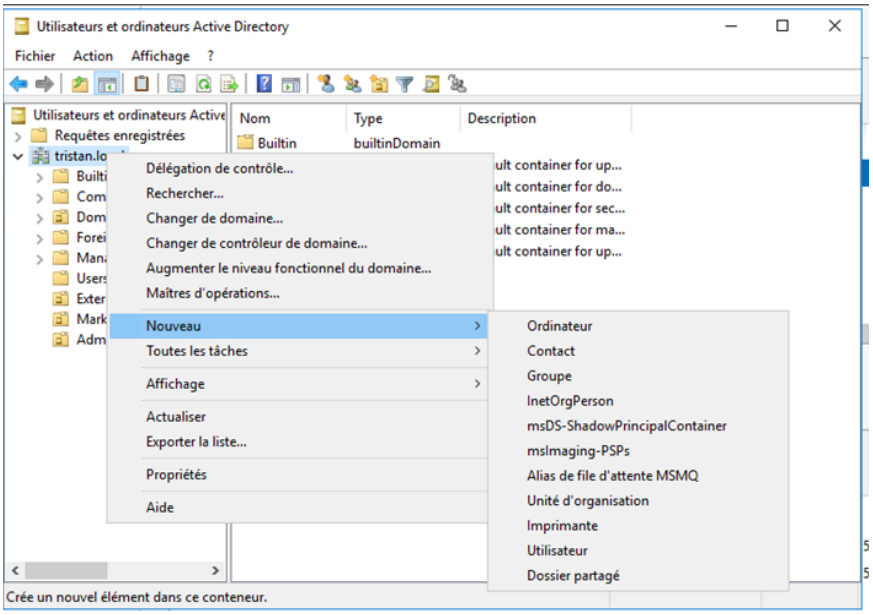


IV - Création d'unités d'organisations et utilisateurs

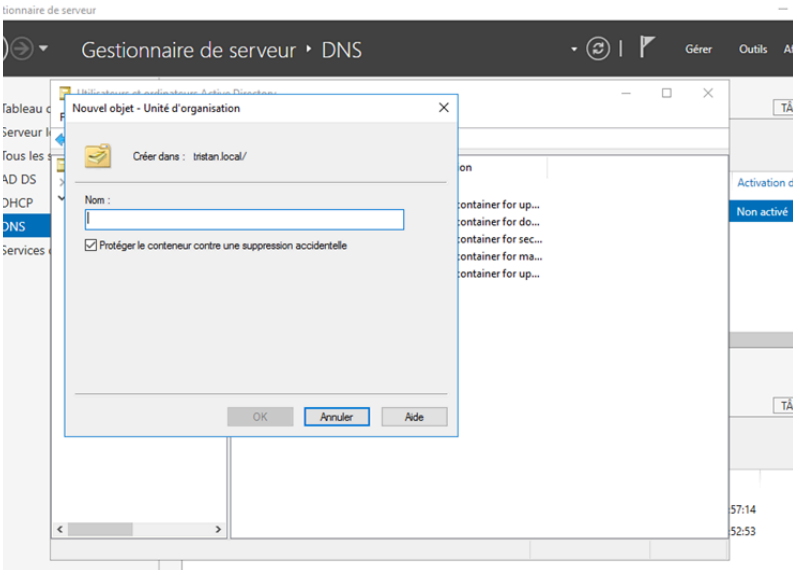
1. Comment créer une unité d'organisation

Nous allons désormais créer des unités d'organisation. Celles-ci vont nous permettre de ranger nos utilisateurs afin d'avoir une meilleure gestion de notre serveur.

Pour cela, rendez-vous dans « Utilisateurs et ordinateurs Active Directory ». Une fois dedans, faites un clic droit sur votre domaine, puis allez dans « Nouveau » et cliquez sur Unité d'organisation.



Une fois que vous avez cliqué, il vous sera alors demandé de choisir un nom pour cette unité. Choisissez un nom qui vous permettra de reconnaître les utilisateurs placés dedans. (Exemple : compta)

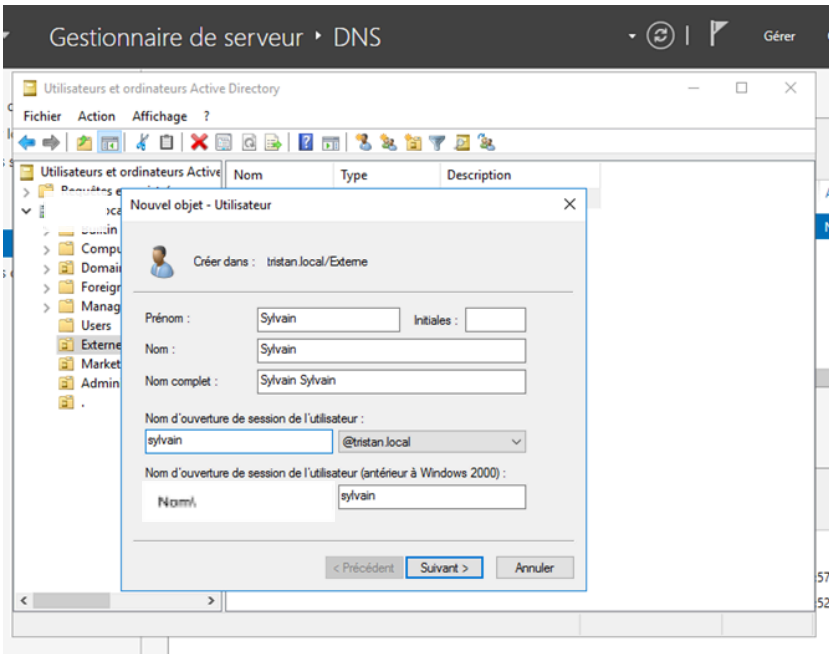


Et voilà, vous avez déjà réussi à créer une unité d'organisation. A chaque fois que vous irez dans “Utilisateurs et ordinateurs Active Directory” vous verrez alors sur le côté la liste de vos unités d’organisations.

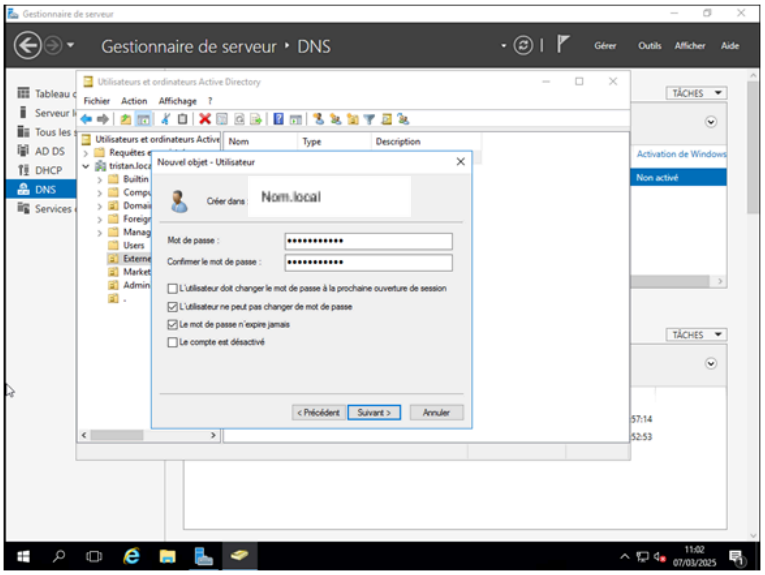
2. Comment créer un utilisateur

N’allons pas chercher bien loin ! Cliquez simplement sur votre unité d’organisation que vous venez de créer, faites un clic droit dessus, puis sélectionnez « Nouveau » > « Utilisateur ».

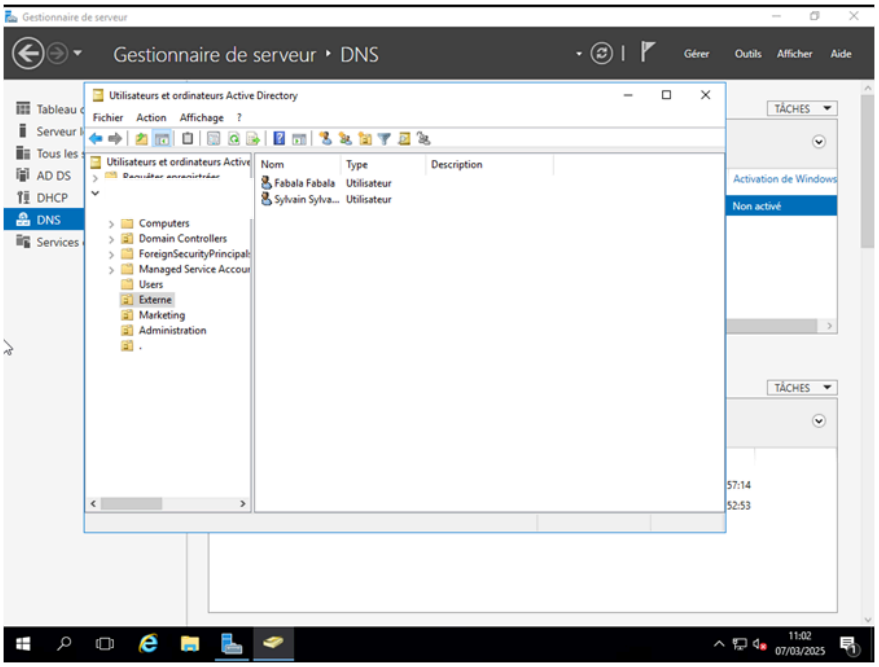
Voilà, la page ci-dessous va s’ouvrir et vous allez alors pouvoir créer un utilisateur. Remplissez les champs et cliquez sur « Suivant ».



Par la suite, il vous sera demandé de lui créer son mot de passe. Vous pouvez aussi, avec les cases ci-dessous, choisir quelques options concernant ce dernier.



Et voilà, vous savez désormais comment créer un utilisateur dans une unité d'organisation ! Vous devriez alors voir les utilisateurs que vous avez créés à l'intérieur de cette dernière.



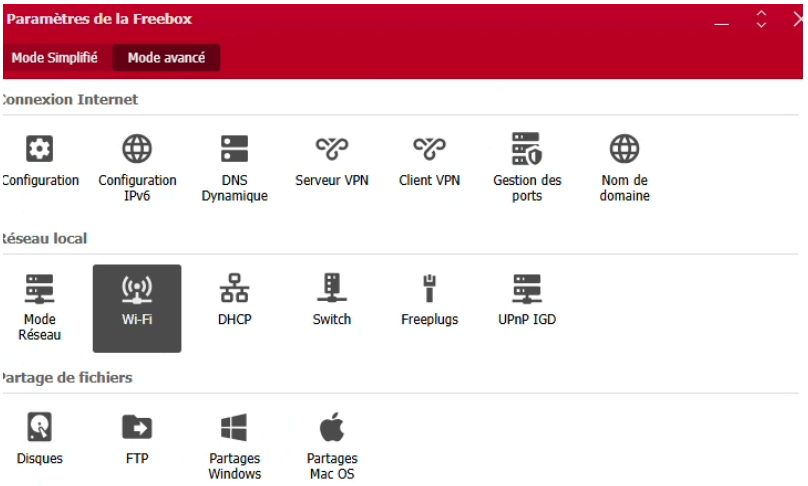
V - Création d’un Wi-Fi Guest

1. Création du Wi-Fi

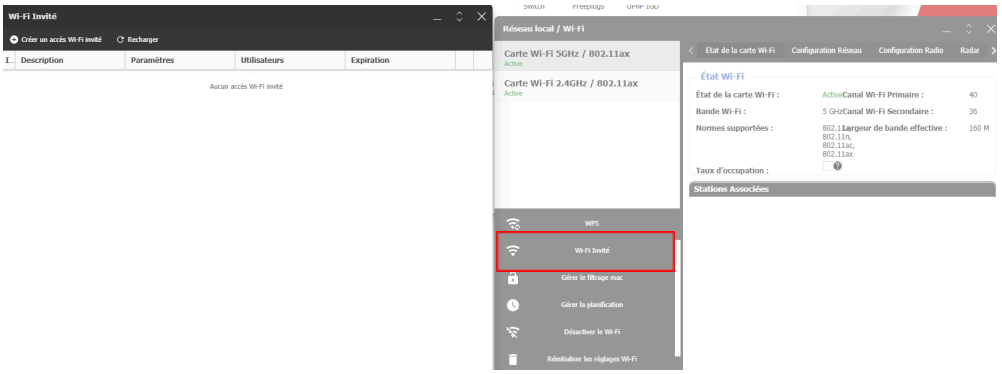
Nous allons désormais créer un Wi-Fi Guest afin que les personnes venant au cabinet puissent avoir un réseau sur lequel se connecter et avoir accès à internet.

Pour cela rendez-vous directement sur le site de votre Freebox et cliquez sur “Paramètres de la Freebox”

Une fois dans “Paramètres de la Freebox” cliquez sur “Wi-Fi”



Vous arrivez alors sur cette page et sur cette dernière que vous allez pouvoir créer votre Wi-Fi GUEST. Cliquez en bas à gauche sur “Wi-Fi invité”



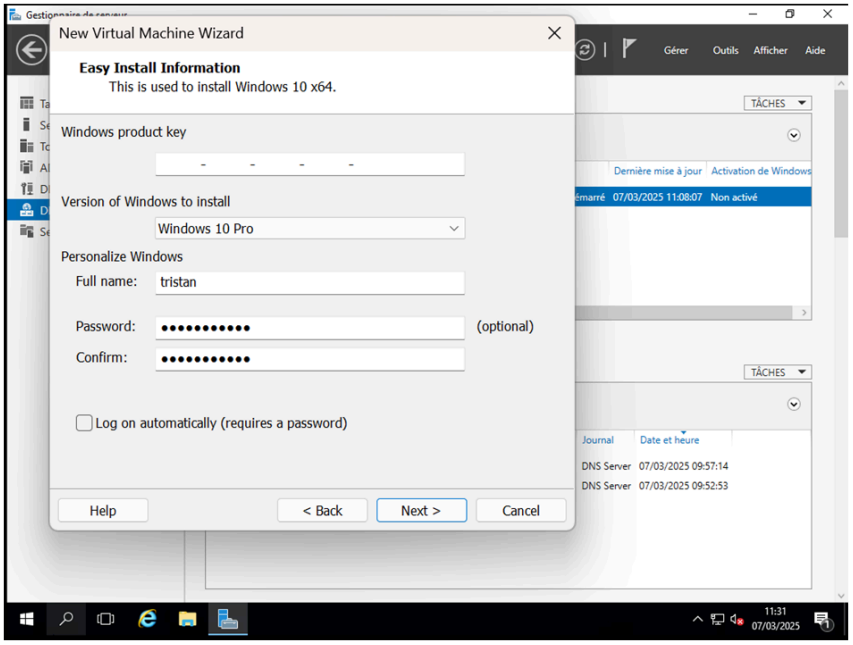
Une fois que vous aurez cliqué dessus, cette petite page va s’ouvrir, cette dernière vous permet tout simplement de créer le Wi-Fi Guest ou de le modifier s’il est déjà existant.

Et voilà, vous avez désormais un Wi-Fi Guest disponible dans votre cabinet. Les personnes de passage dans ce dernier peuvent alors l’utiliser afin d’avoir un accès internet.

VI - Création d’une VM Windows et comment rejoindre un domaine

1. Création de la VM Windows

Nous allons désormais créer une VM Windows afin de rejoindre le domaine précédemment créé sur notre Windows Serveur, nous en profiterons aussi pour tester le fichier de partage du serveur de sauvegarde. La seule particularité dans la création de cette dernière sera de choisir la version Pro de Windows, sinon il sera impossible de le rejoindre.

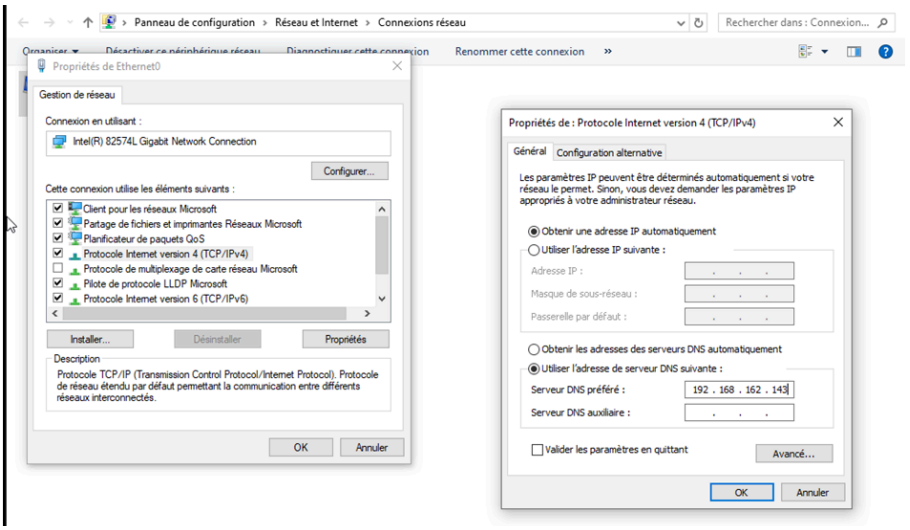


Une fois la VM faite, choisissez l’espace disque que vous voulez lui donner et l’installation se fera toute seule par la suite.

2. Rejoindre un domaine avec une VM Windows

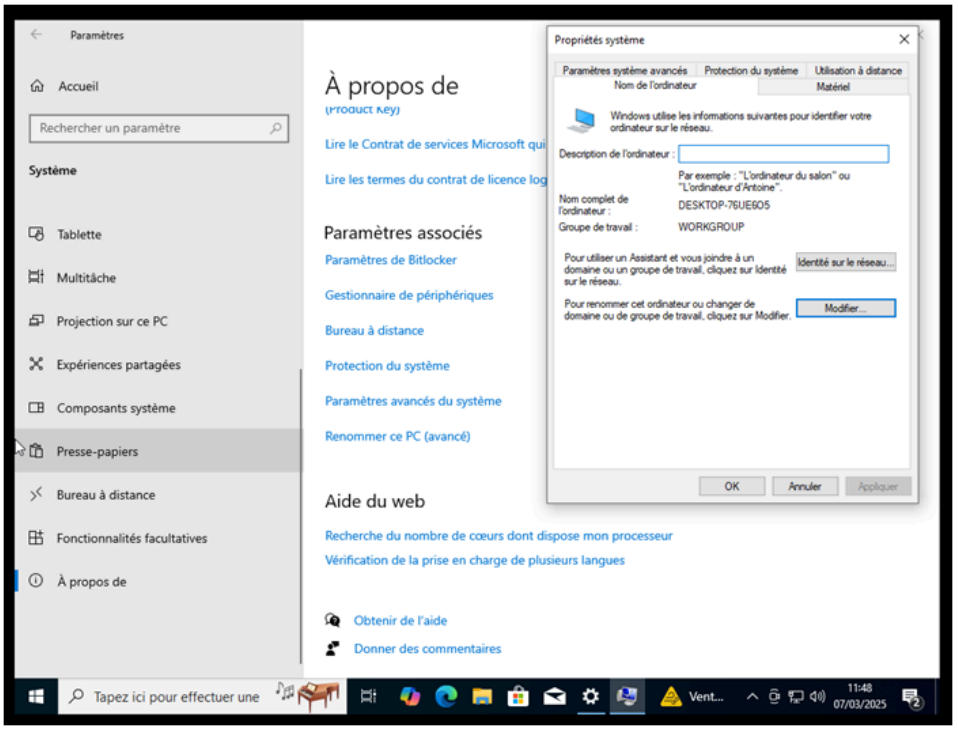
Une fois connectée à votre VM Windows, rendez-vous directement dans le panneau de configuration, puis "Réseau et Internet". Faites un clic droit sur votre connexion réseau et allez dans "Propriétés". Dans cette fenêtre, double-cliquez sur « Protocole Internet version 4 (TCP/IPv4) ».

Une nouvelle page va alors s'ouvrir. Dans cette dernière, cochez la case « Utiliser l'adresse de serveur DNS suivante » et renseignez l'IP de votre VM Windows Serveur.

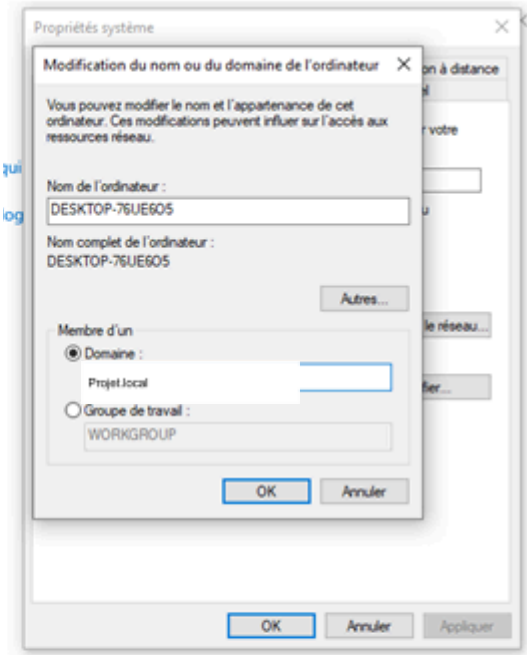


On va maintenant pouvoir passer à la partie rejoindre le domaine ! Allez dans les paramètres, puis "Système", et rendez-vous dans la section « À propos de ». Cliquez sur « Renommer ce PC (avancé) ».

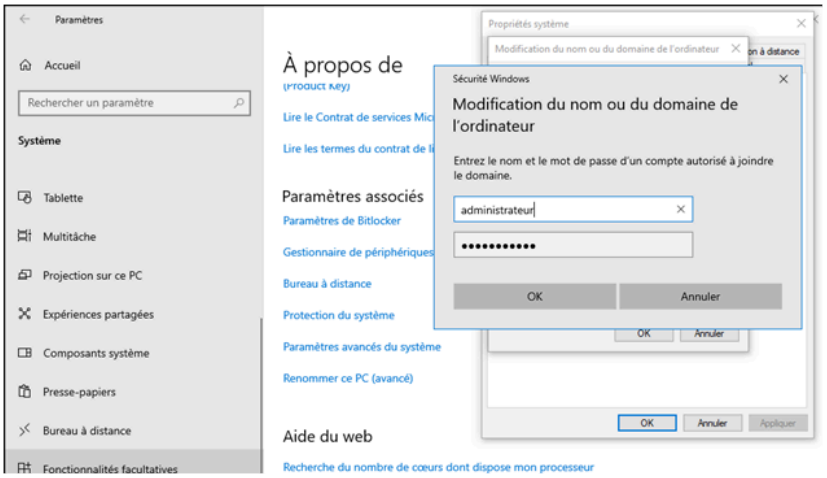
Sur la page qui s'ouvre, sélectionnez le bouton « Modifier ».



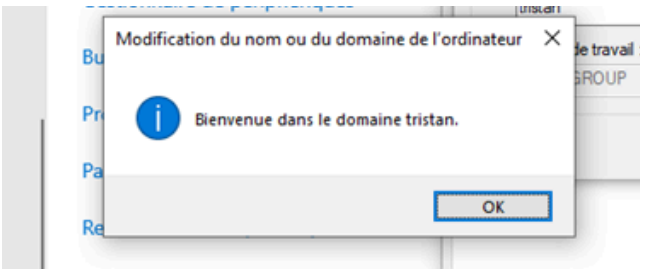
Entrez le nom du domaine que vous aviez créé sur votre VM Windows Serveur. Si ce dernier se nomme Projet.local, écrivez alors Projet



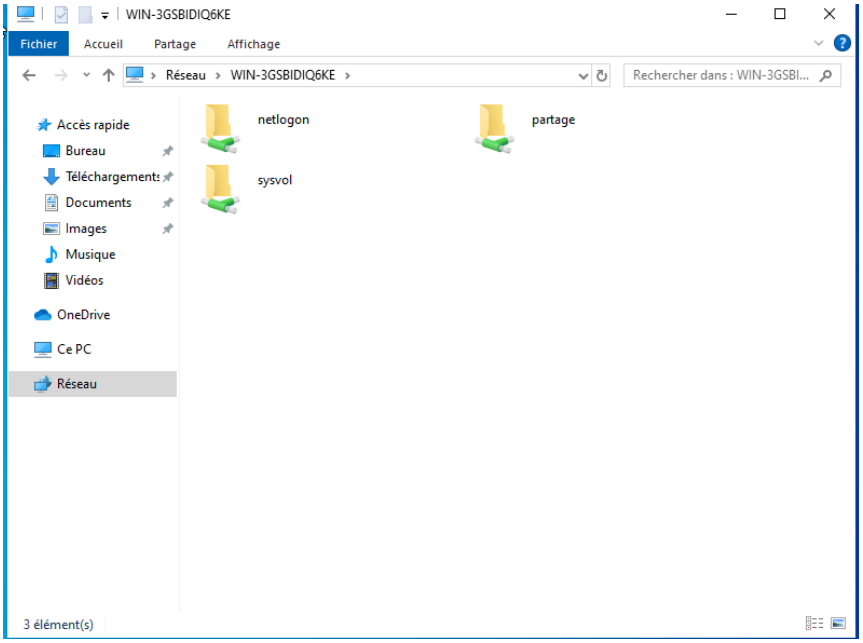
Une fois que vous avez cliqué sur « OK », cette page s'ouvre. Vous devez alors entrer les identifiants de la session administrateur que vous aviez créés afin d'accéder au domaine.



Et voilà,votre VM est désormais dans le domaine créé via votre Windows Serveur.



Nous allons au passage tester le dossier que nous avions partagé via notre Windows Server. Pour cela nous allons ouvrir l'explorateur de fichiers et tout simplement entrer le chemin d'accès que nous avions choisi au moment de sa création.



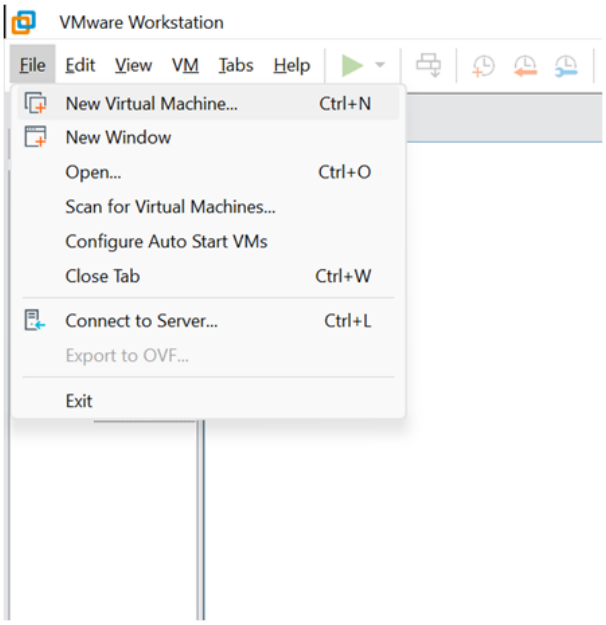
Nous pouvons effectivement voir que le dossier “partage” est présent et que nous pouvons y accéder, cela signifie que nous avions alors bien fait le partage pour notre serveur de sauvegarde.

VII - Création d’une VM Debian et d’un NextCloud

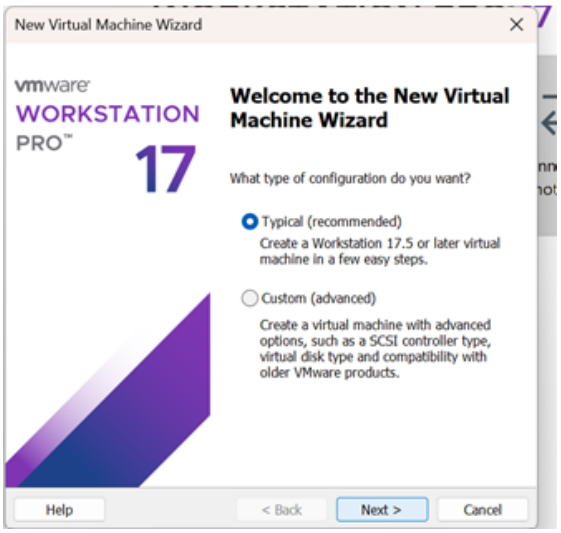
1. Création d’une VM Debian

Afin de créer cette dernière, voici une liste de captures d’écran indiquant les endroits où cliquer ainsi que les options à suivre.

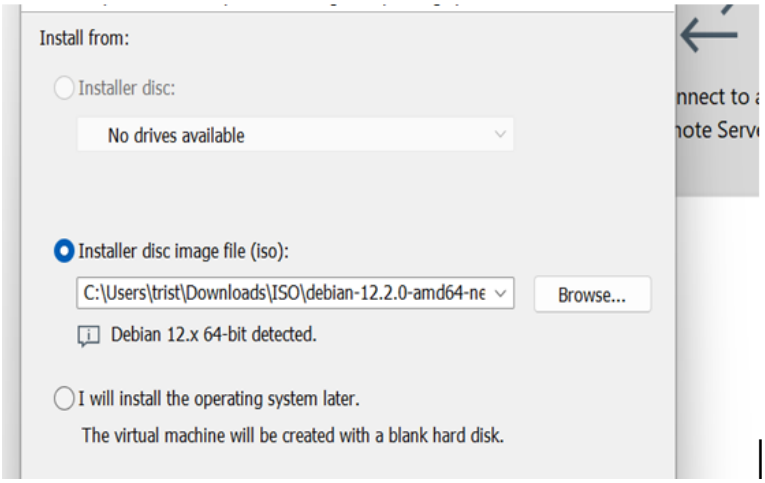
Sélectionnez « New Virtual Machine… »



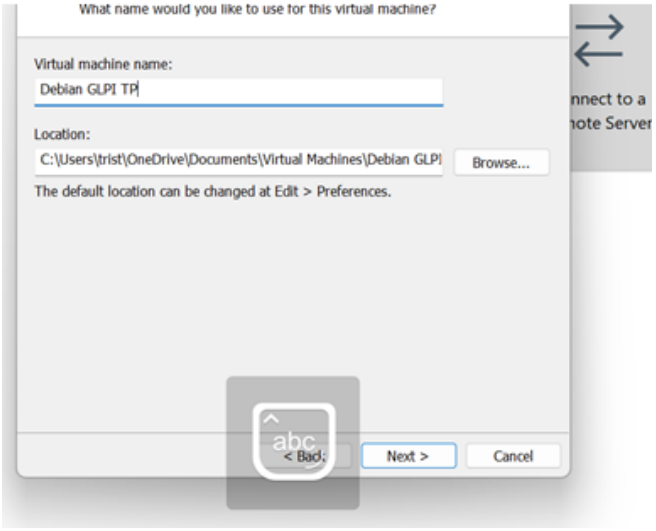
Pour la suite, sélectionnez les mêmes options que sur les captures d’écran.



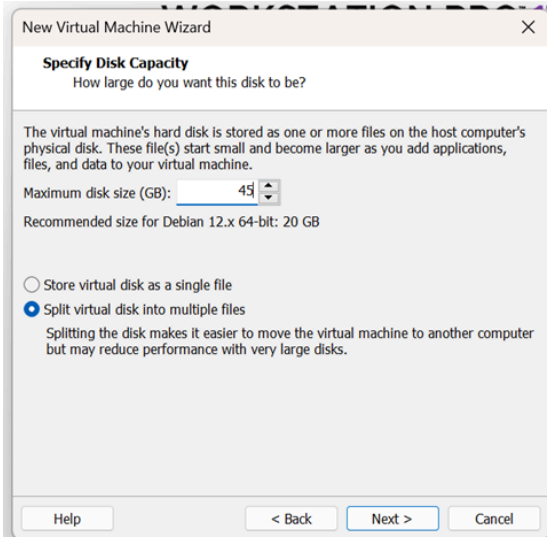
Ici, vous devez sélectionner votre iso Debian 12.



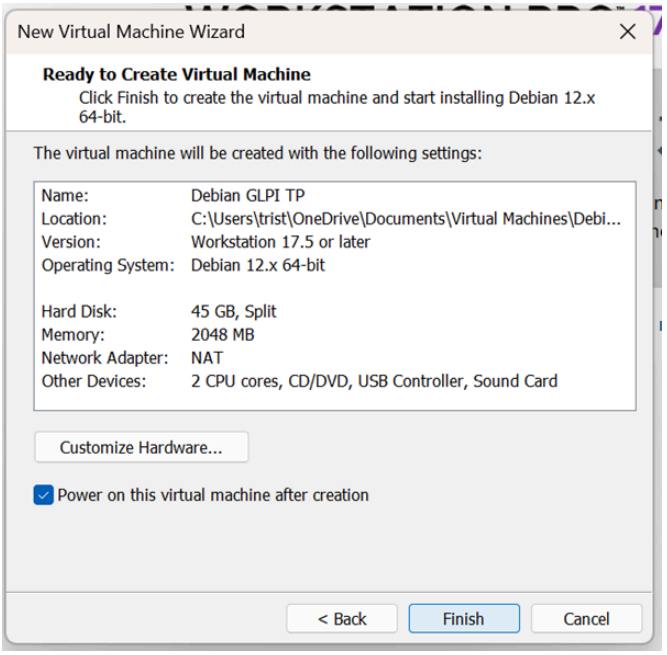
Donnez-lui par la suite le nom que vous voulez.



Choisissez-ici la taille que vous voulez allouer à son disque dur.

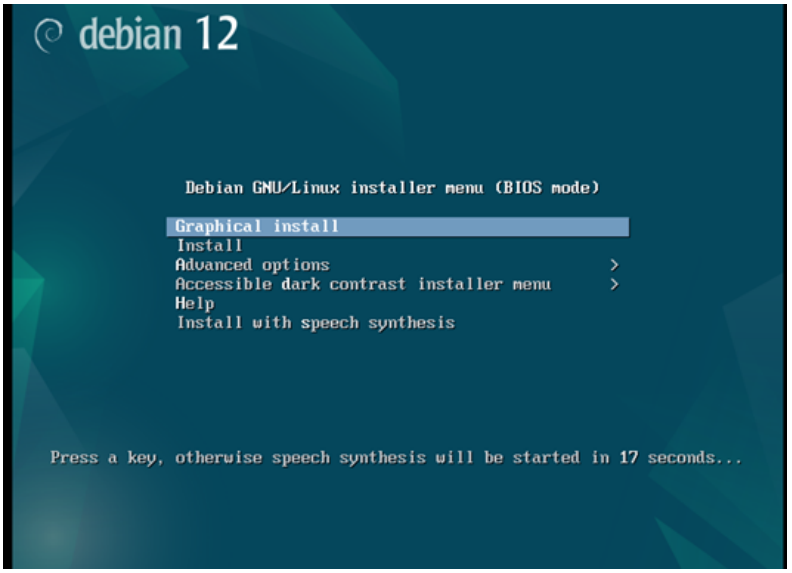


Tout est bon, vous pouvez cliquer sur “finish” et lancer votre VM.



2. Lancement de la VM et configuration

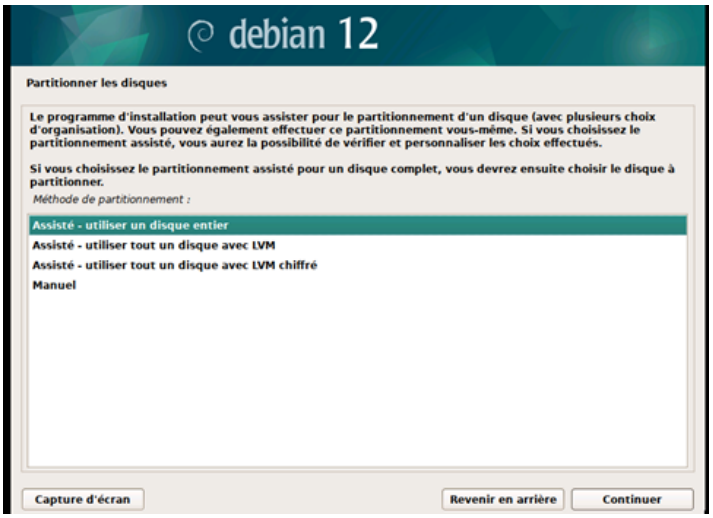
Quand vous lancez cette dernière, cliquer sur Graphical install



Ensuite vous allez devoir choisir la langue sélectionnée tout le temps français.

Par la suite, vous allez devoir donner un nom à votre système. Une fois fait, cliquez sur suivant et donnez-lui aussi un mot de passe. Celui-ci marche pour l’utilisateur root (admin du système), alors faites attention et notez bien le mot de passe.

Par la suite, vous allez devoir partitionner les disques. Ici vous devez choisir Assisté – utiliser un disque entier comme sur l'image ci-dessous.



Cliquez sur continuer et dites que vous voulez tout partitionner dans une seule partition.

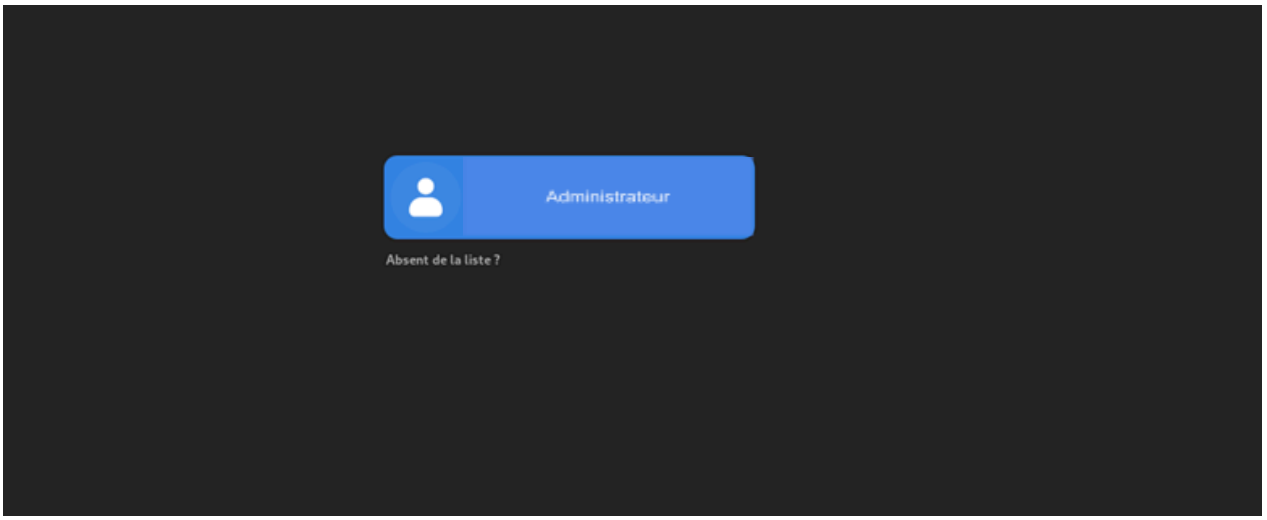
Pour la prochaine étape, faites attention et pensez bien à cocher oui pour appliquer les changements sur le disque. La case non est automatiquement cochée de base, vous devez changer et cocher oui

Ensuite, votre VM vous demandera si vous souhaitez analyser d'autres supports. Etant donné que nous n'avons pas d'autres, vous pouvez laisser cocher non et cliquer sur continuer.

Pour continuer, il vous sera demandé de choisir un miroir de l'archive. Sélectionnez donc deb.debian.org comme sur l'image ci-dessous.

Par la suite, il vous sera demandé un domaine. Passez directement à la prochaine étape et ne rentrez rien.

Et voilà votre VM, et maintenant finie. Vous pouvez vous authentifier avec le mot de passe choisi préalablement.



VIII - Création d’un NextCloud sur une VM Debian

1. Création du NextCloud

A. Installation du serveur web Apache2

Commencez par passer en mode admin.

```
tristan@tristan:~$ su
Mot de passe :
```

Ensuite, mettez à jour l’index des paquets Debian afin de pouvoir télécharger la dernière version d’Apache2.

```
root@tristan:/home/tristan# sudo apt update
```

Installer Apache2

```
root@debian:/home/laurie# sudo apt-get install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-data apache2-utils
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-data apache2-utils
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 593 ko dans les archives.
Après cette opération, 1 905 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 apache2-data al
l 2.4.62-1~deb12u2 [160 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 apache2-utils a
md64 2.4.62-1~deb12u2 [210 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 apache2 amd64 2
.4.62-1~deb12u2 [223 kB]
593 ko réceptionnés en 0s (1 431 ko/s)
Sélection du paquet apache2-data précédemment désélectionné.
```

Avec ces deux commandes, cela permet de savoir si le service Apache2 est bel et bien actif. Si oui il sera retourné que le statut est actif.

```
root@debian:/home/laurie# sudo systemctl is-enabled apache2
enabled
root@debian:/home/laurie# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab>
     Active: active (running) since Wed 2025-04-02 14:19:35 CEST; 1min 10s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 4377 (apache2)
      Tasks: 55 (limit: 2241)
     Memory: 14.8M
        CPU: 156ms
     CGroup: /system.slice/apache2.service
             ├─4377 /usr/sbin/apache2 -k start
             ├─4379 /usr/sbin/apache2 -k start
             └─4380 /usr/sbin/apache2 -k start

avril 02 14:19:35 debian systemd[1]: Starting apache2.service - The Apache HTTP>
avril 02 14:19:35 debian apachectl[4376]: AH00558: apache2: Could not reliably >
avril 02 14:19:35 debian systemd[1]: Started apache2.service - The Apache HTTP >
lines 1-16/16 (END)
```

B. Configuration du pare-feu

Commencez par installer le pare-feu UFW avec la commande suivante.

```
root@debian:/home/laurie# sudo apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  iptables libip6tc2
Paquets suggérés :
  firewalld rsyslog
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 ufw
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 548 ko dans les archives.
Après cette opération, 3 411 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Installez Openssh et mettez le à jour avec UFW.

```
root@debian:/home/laurie# sudo apt install --reinstall openssh-server
sudo ufw app update OpenSSH
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  openssh-sftp-server runit-helper
Paquets suggérés :
  molly-guard monkeysphere ssh-askpass
Les NOUVEAUX paquets suivants seront installés :
  openssh-server openssh-sftp-server runit-helper
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 529 ko dans les archives.
Après cette opération, 2 218 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 openssh-sftp-se
rver amd64 1:9.2p1-2+deb12u5 [65,8 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 runit-helper al
l 2.15.2 [6 520 B]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 openssh-server
```

Par la suite installez et activez openssh ainsi que UFW.

```
root@debian:/home/laurie# sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
root@debian:/home/laurie# sudo ufw enable
Firewall is active and enabled on system startup
```

Ajoutez le port HTTP et le port HTTPS qui doivent être utilisés par le serveur Web. Pour cela, exécutez cette commande.

```
root@debian:/home/laurie# sudo ufw allow "WWW Full"
Rule added
Rule added (v6)
root@debian:/home/laurie#
```

Recharger UFW pour qu'il applique les changements.

```
root@debian:/home/laurie# sudo ufw reload
Firewall reloaded
```

Avec la commande status vous pouvez voir les règles actives. Vous pouvez alors vérifier que votre WWW est actif.

```
root@tristan:/home/tristan# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
OpenSSH                    ALLOW       Anywhere
WWW Full                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
OpenSSH (v6)               ALLOW       Anywhere (v6)
WWW Full (v6)              ALLOW       Anywhere (v6)
```

C. Activer PHP 8.2

Pour les meilleures performances, Nextcloud recommande PHP 8.2, qui est inclus par défaut dans Debian 12, de sorte il suffit alors d'installer les paquets nécessaires.

```
root@debian:/home/laurie# sudo 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
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  autoconf automake autopoint autotools-dev binutils binutils-common
  binutils-x86-64-linux-gnu build-essential bzip2-doc debhelper dh-autoreconf
  dh-strip-nondeterminism dpkg-dev dwz fakeroot g++ g++-12 gcc gcc-12 gettext
  icu-devtools intltool-debian libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libapache2-mod-php8.2
  libarchive-cpio-perl libarchive-zip-perl libasan8 libbinutils libblkid-dev
  libbrotli-dev libbz2-dev libc-dev-bin libc-devtools libc6-dev libcairo2-dev
  libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdebhelper-perl libdeflate-dev
  libdjvulibre-dev libdpkg-perl libexif-dev libexpat1-dev libfakeroot
  libffi-dev libfile-fcntllock-perl libfile-stripnondeterminism-perl
  libfontconfig-dev libfreetype-dev libfreetype6-dev libgcc-12-dev
  libgdk-pixbuf-2.0-dev libglib2.0-dev libglib2.0-dev-bin libgprofng0
```

Vérifiez que vous avez la bonne version de PHP et activez les extensions.

```
root@debian:/home/laurie# php --version
php -m
PHP 8.2.28 (cli) (built: Mar 13 2025 18:21:38) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.2.28, Copyright (c) Zend Technologies
    with Zend OPcache v8.2.28, Copyright (c), by Zend Technologies
[PHP Modules]
apcu
bcmath
bz2
```

Ouvrez le fichier de configuration avec la commande nano, si vous désirez en ajoutant un -l juste après le nano il est possible d'afficher les numéros de ligne dans le fichier de conf

```
root@tristan:/home/tristan# sudo nano /etc/php/8.2/apache2/php.ini
```

Commencez par vous rendre ligne 979 afin de régler le fuseau horaire.

```
979 ;date.timezone = data.timezone = Europe/Amsterdam
```

Ligne 435, modifier la mémoire limite.

```
435 memory_limit = 512M
```

Ligne 855, modifier la taille max des fichiers pouvant être upload.

```
855 upload_max_filesize = 500M
```

Ligne 703, augmenter la taille maximale des posts.

```
703 post_max_size = 600M
```

Ligne 409 vérifier que le max_execution_time soit bien à 300.

```
409 max_execution_time = 300
```

Activez PHP oPCache.

```
966 ;zend_extension=opcache
```

Ajoutez la configuration dans la section oPCache recommandée par NextCloud pour Debian 12.

```
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
```

Une fois tout cela fait, vous pouvez enregistrer et quitter le fichier de configuration.
Par la suite redémarrez le service Apache2 pour que tous les changements soient pris en compte.

```
root@tristan:/home/tristan# sudo systemctl restart apache2
```

D. Mettre en place le serveur MariaDB sa base de donnée et des utilisateurs

Installer MariaDB

```
root@tristan:/home/tristan# sudo apt install mariadb-server
```

Activez MariaDB et avec la commande status vérifiez qu'il soit bien actif.

```
root@tristan:/home/tristan# sudo systemctl is-enabled mariadb
sudo systemctl status mariadb
```

Utilisez la commande suivante pour créer un mot de passe root, supprimer les utilisateurs anonymes et effacer la base de données de test

```
root@tristan:/home/tristan# sudo mariadb-secure-installation
```

Suite à la commande, tapez ci-dessus, une liste de questions vous sera posée. Répondez "Y" à tout sauf à celle ci-dessous ou vous devez répondre "n".

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

Créez ensuite une nouvelle base de données ainsi que l'utilisateur correspondant. Pour vous connecter au serveur MariaDB

```
root@tristan:/home/tristan# sudo mariadb -u root -p
```

Utilisez les commandes ci-dessous afin de créer une nouvelle base de données avec l'utilisateur et le mot de passe qui va avec.

```
CREATE DATABASE nextcloud_db;
CREATE USER 'tristan'@'localhost' IDENTIFIED BY 'VotreMotDePasse';
GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'tristan'@'localhost';
FLUSH PRIVILEGES;
```

Téléchargez les codes sources actuels pour pouvoir utiliser NextCloud de manière optimale sous Debian 12.

```
root@tristan:/home/tristan# sudo apt install curl unzip -y
```

Ensuite, allez dans le répertoire */var/www* et téléchargez le code source le plus récent de NextCloud

```
root@tristan:/home/tristan# cd /var/www/
curl -o nextcloud.zip https://download.nextcloud.com/server/releases/latest.zip
```

Décompressez le fichier et changez ensuite les propriétaires du répertoire

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

E.Configuration d’Apache2

Il va désormais falloir configurer un hôte virtuel Apache2.

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

Une fois dans le fichier, rentrez ceci. Pensez à changer l’ip 192.168.208.219 avec votre IP à vous.

```
<VirtualHost *:80>
  ServerName nextcloud.192.168.208.219
  DocumentRoot /var/www/nextcloud/


  # log files
  ErrorLog /var/log/apache2/files.192.168.208.219-error.log
  CustomLog /var/log/apache2/files.192.168.208.219-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>
```

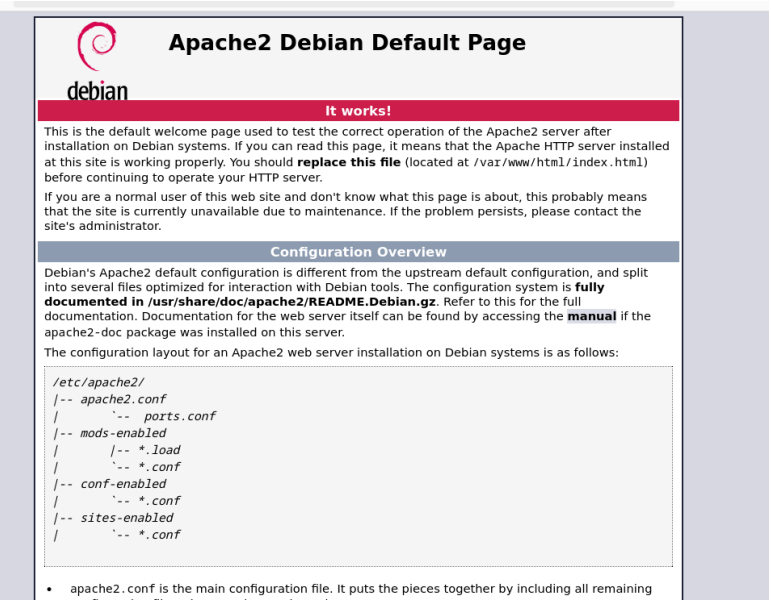
Activez ensuite la configuration avec la commande suivante et vérifiez-la avec un configtest

```
root@tristan:/var/www# sudo a2ensite nextcloud.conf
sudo apachectl configtest
```

Si vous obtenez le résultat « syntaxe OK », redémarrez Apache2.

```
root@tristan:/var/www# sudo systemctl restart apache2
```

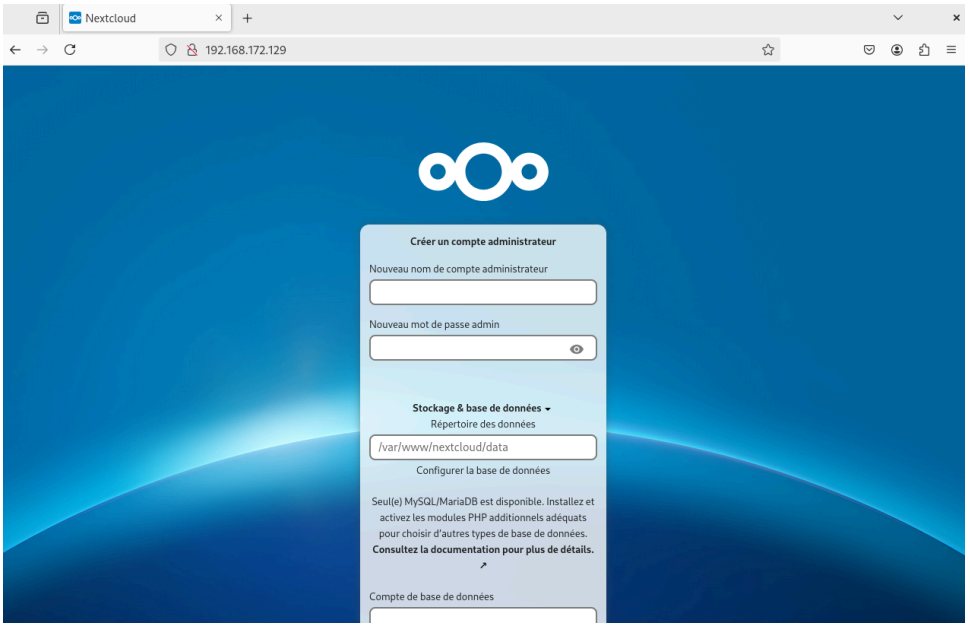
Vous avez terminé, cependant il est possible que vous rencontriez un petit bug. En effet, en voulant accéder à votre NextCloud en ligne **(Tapez votre ip dans la barre de recherche)** vous tombez sur cette page et c'est normal !
Ceci est la page d'affichage de base de Debian.



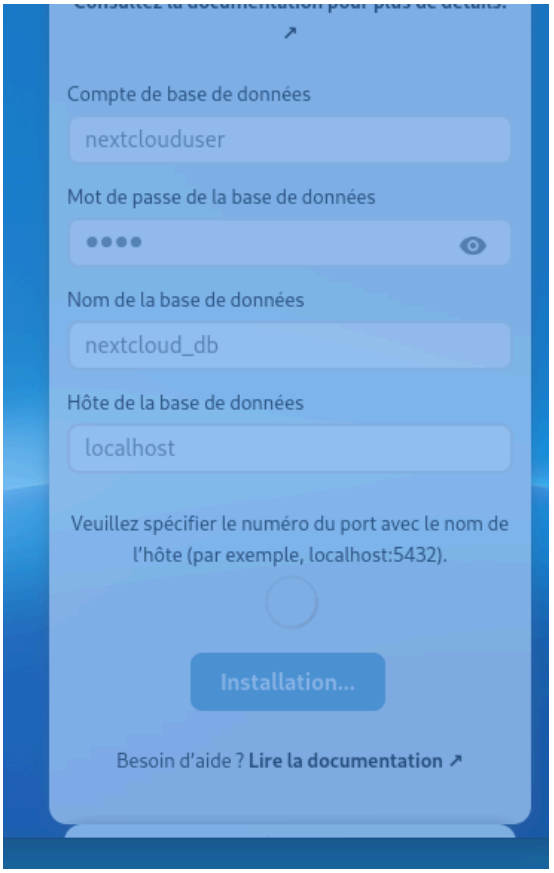
Pour désactiver cette dernière vous avez juste à rentrer cette commande :

```
root@tristan:~# sudo a2dissite 000-default.conf
```

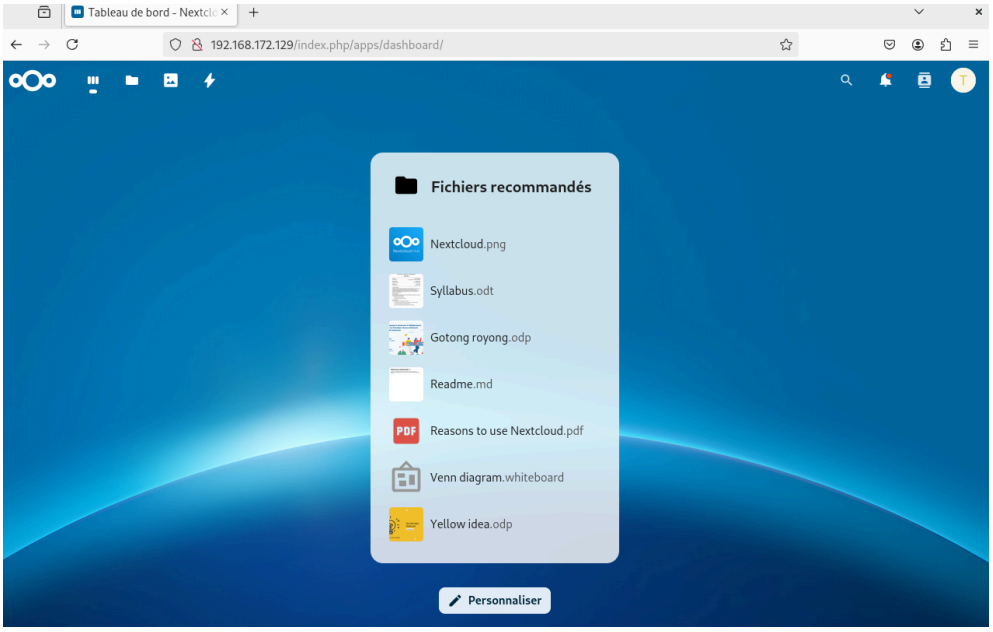
Désormais en rentrant votre IP vous tomberez sur la page de connexion NextCloud ! Identifiez-vous avec les logins que vous aviez créés précédemment et le compte de votre base de données.



Voici avec le login, le mot de passe et le nom de la base renseigné :



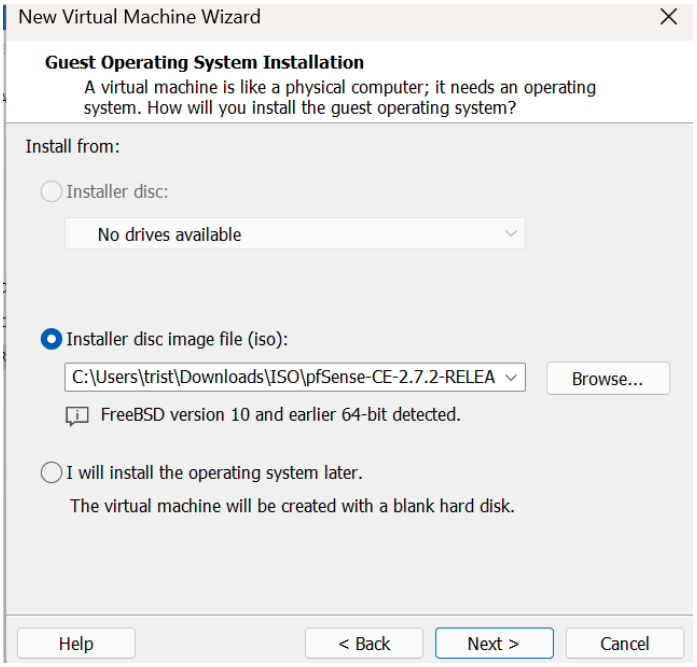
Vous voici désormais avec un NextCloud prêt à l'utilisation.



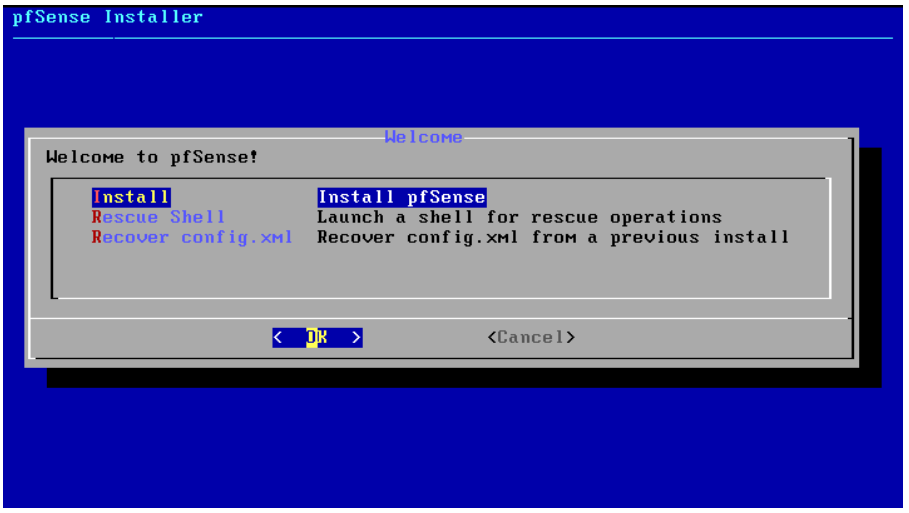
IX - Création d'une VM PfSense

1. Création de la VM et configuration

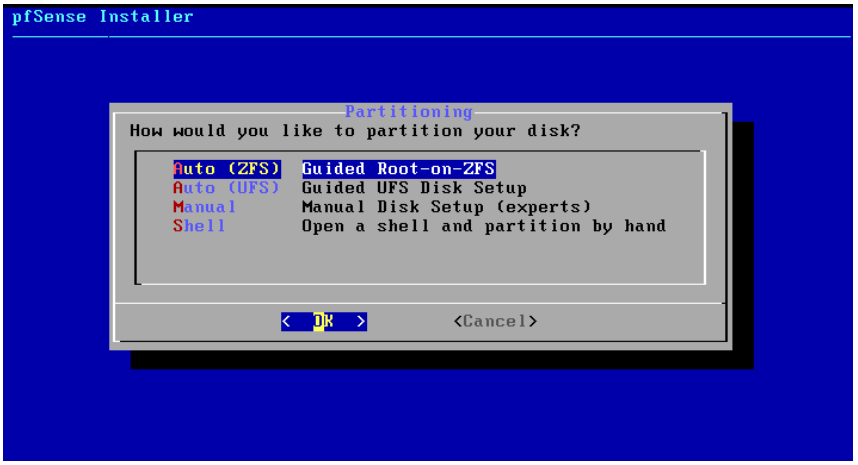
Pour la création de la VM, faites comme avec la VM Windows et Windows Server. Téléchargez un ISO PfSense et sélectionnez-le lors de la création.



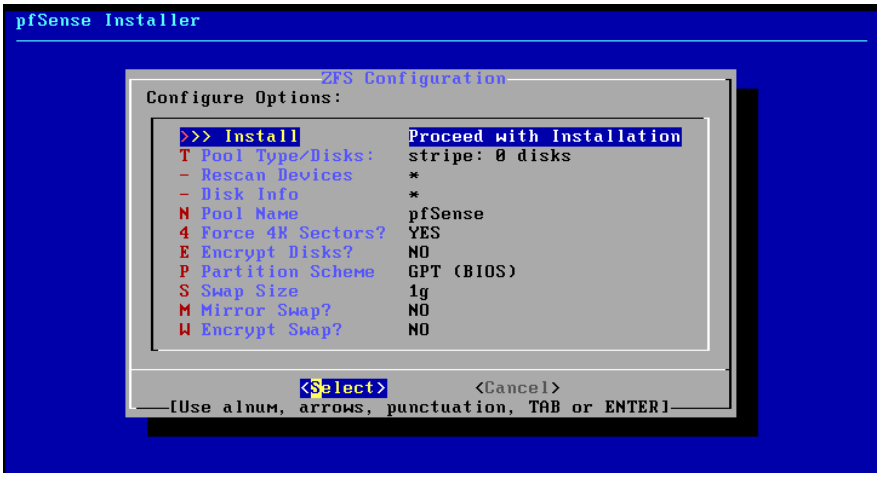
Sélectionnez la première option, “Install”.



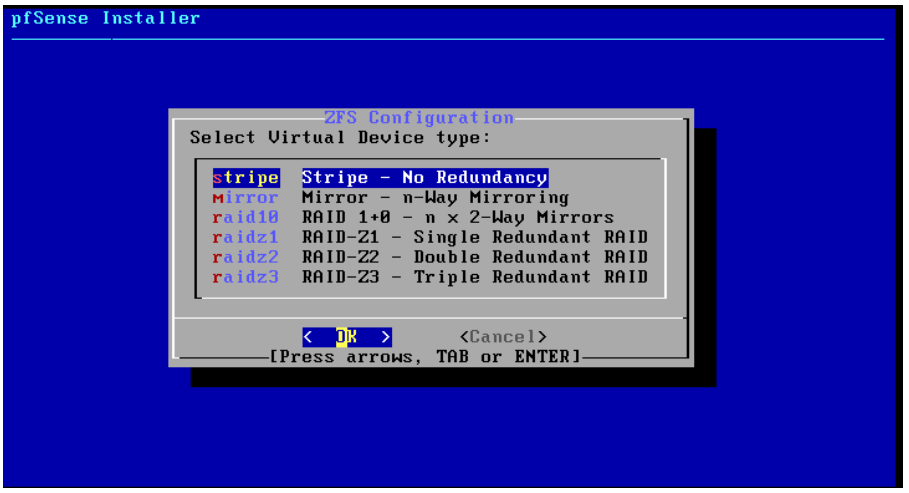
Pour la partition de disque restez sur la première option : “Auto (ZFS)”.



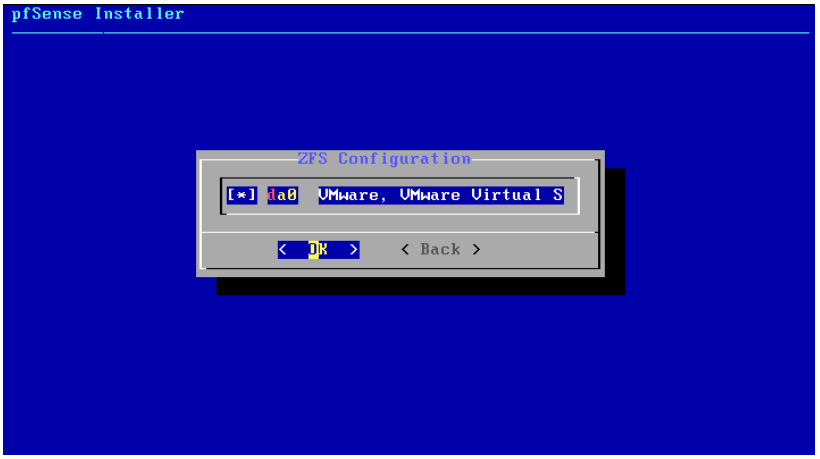
Vous avez ici la possibilité de configurer des options, ne changez rien et faites “Install.



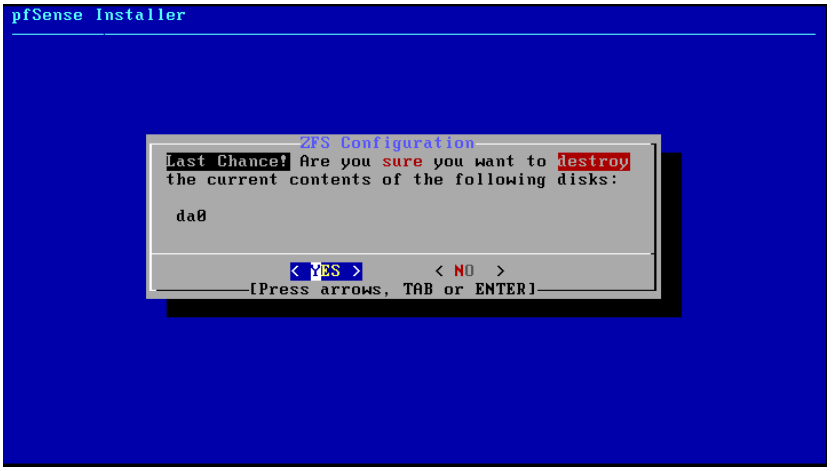
Ici nous ne faisons pas de RAID ou de miroir avec notre PfSense, restez alors sur l'option "Stripe".



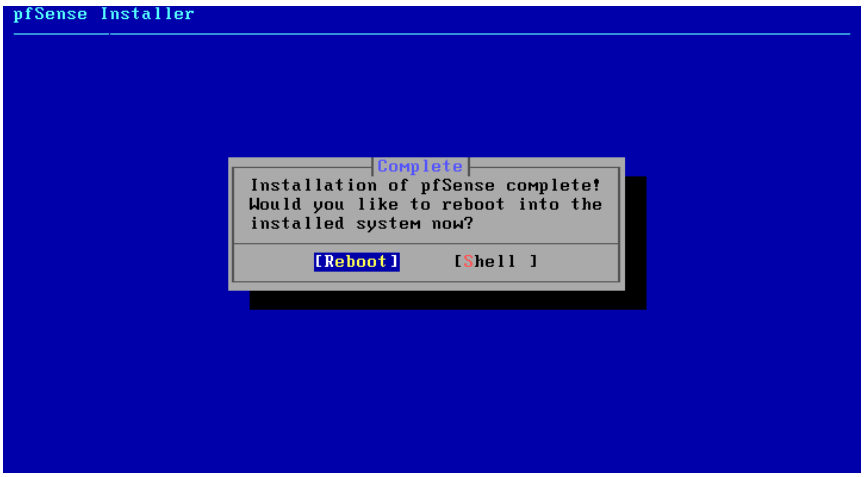
Appuyez sur la touche Espace de votre clavier afin de cocher la case puis faites "Ok".



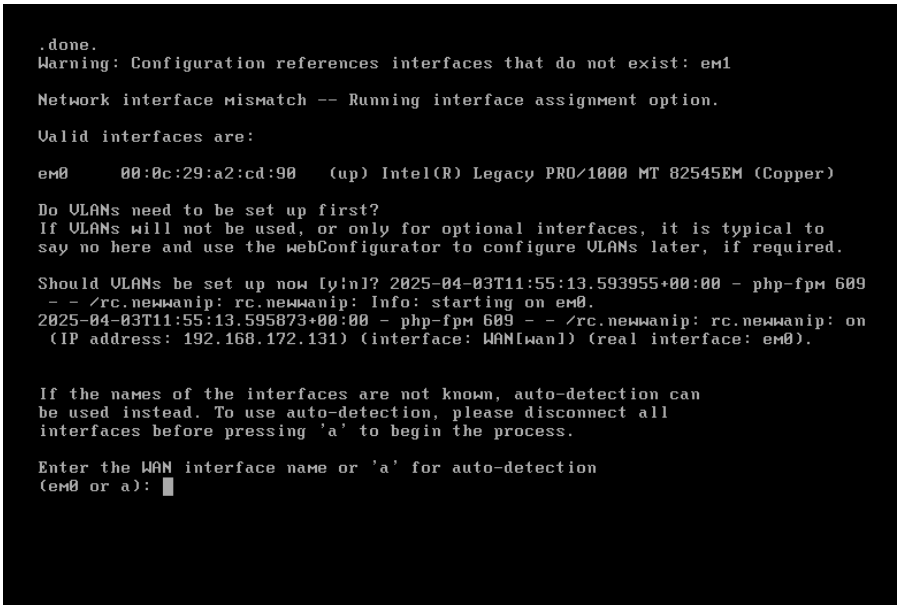
Vous devez ici dire que "Yes" vous êtes sûr de vouloir faire cela.



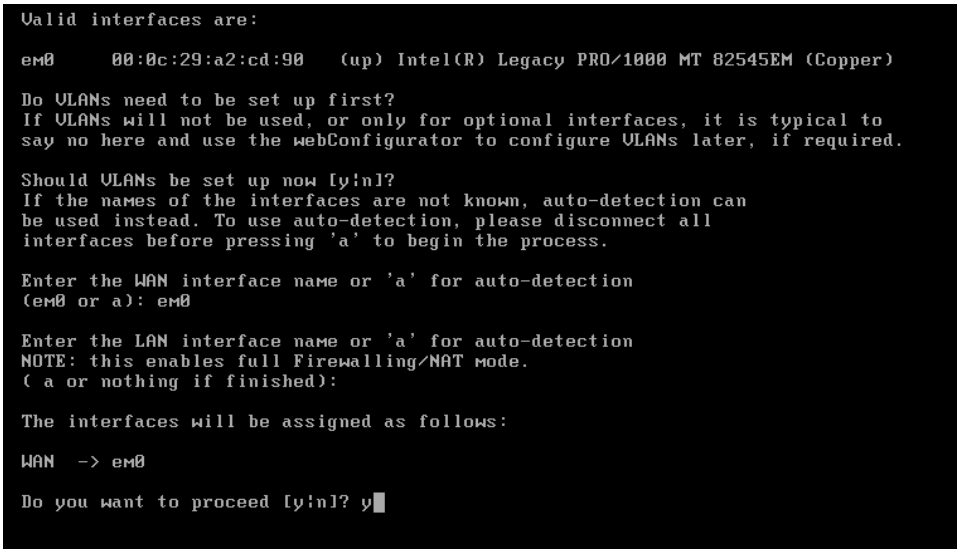
Si ce message apparaît c'est bon signe, cela signifie que l'installation est complète et qu'il propose un reboot afin d'appliquer le système.



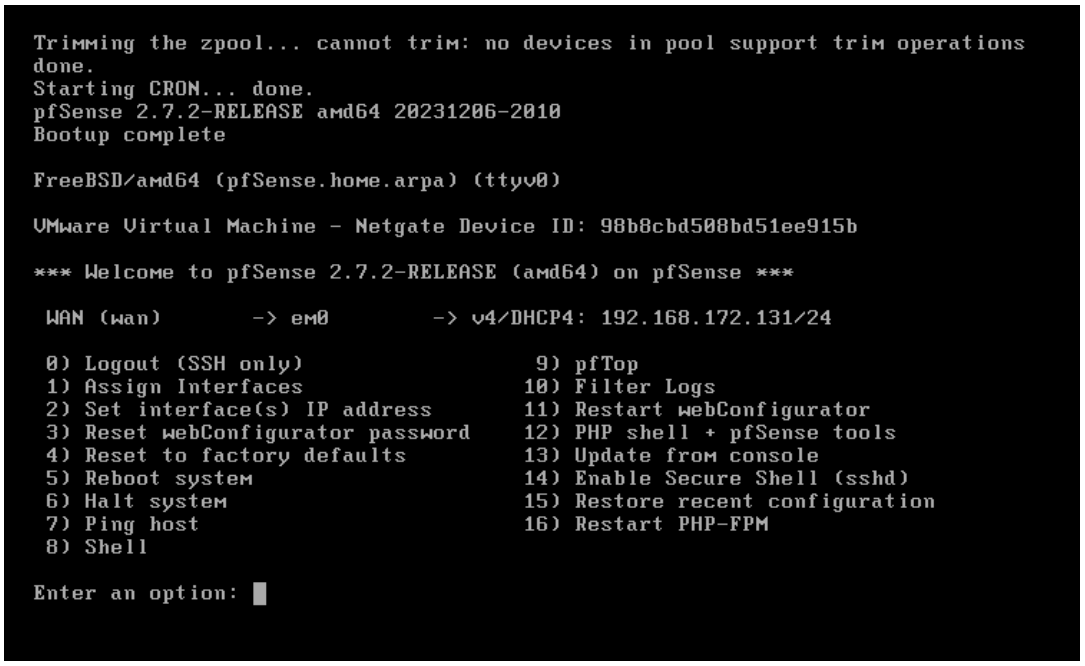
Après avoir Reboot, voici la page que vous aurez, tapez "em0"



Vous allez affecter "em0" à la patte WAN, tapez "y" afin de confirmer votre choix.



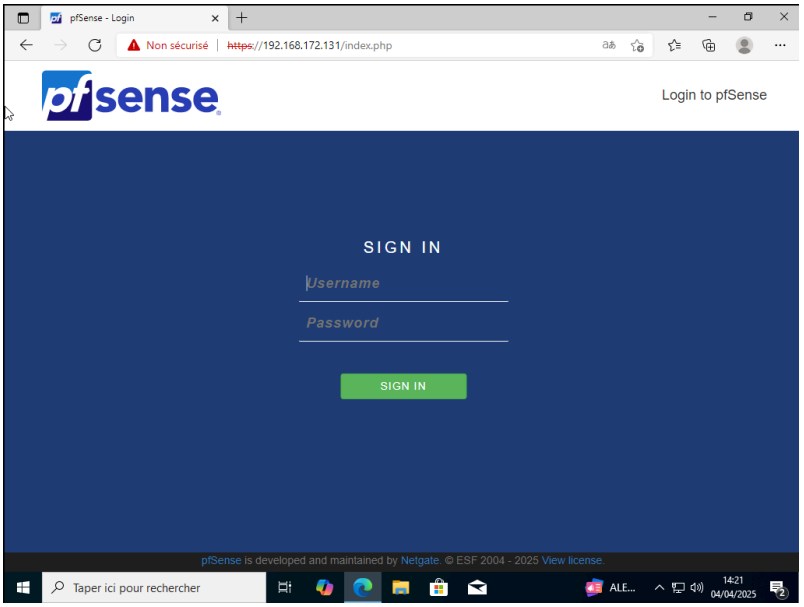
Et voila votre PfSense est désormais fini et prêt à l'utilisation. Vous pouvez de plus en effet voir que la patte "em0" est bel bien affectée au WAN avec votre IP à la fin.



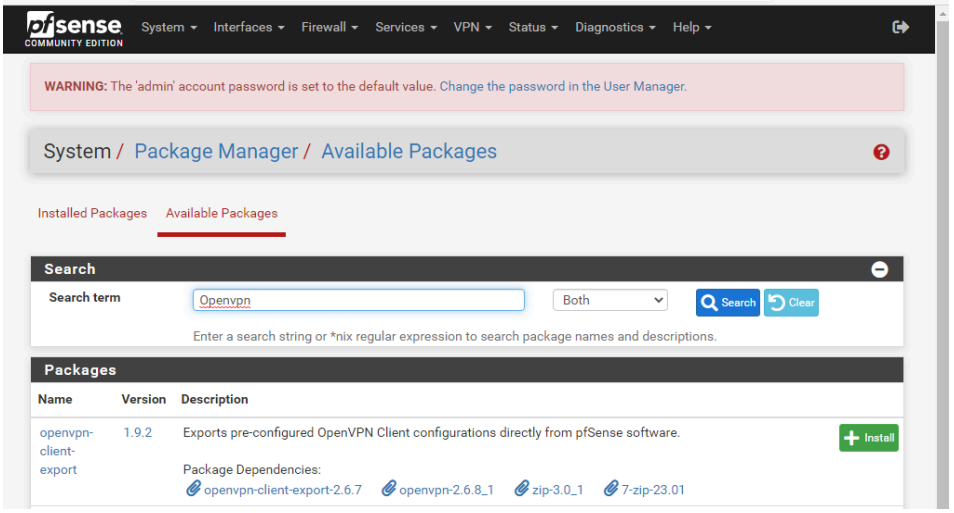
X - Création d’un OpenVPN

1. Installation et configuration d’Openvpn

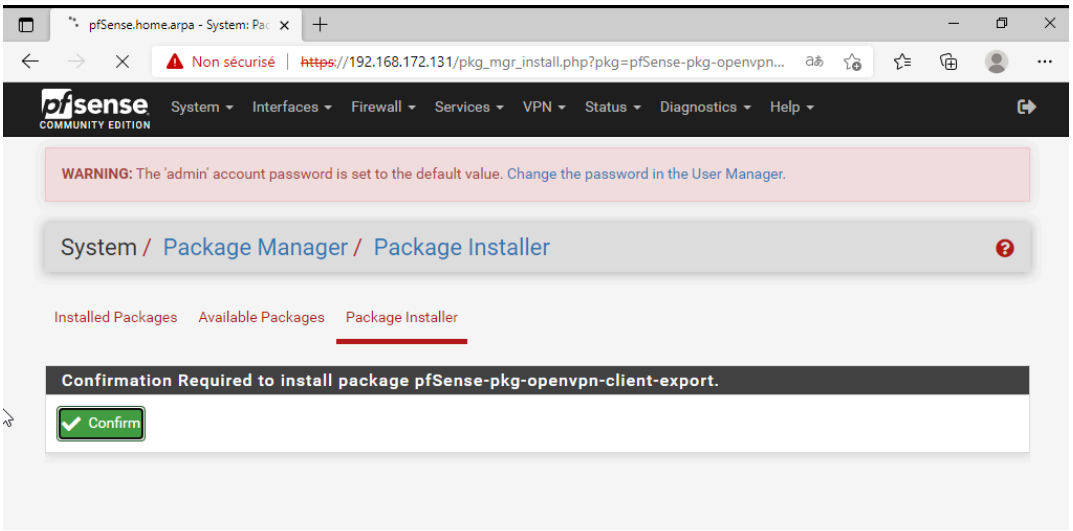
Pour commencer la création de ce dernier, vous devez vous rendre sur votre PFSense via votre VM Windows. Pour y accéder, tapez tout simplement l’ip du PfSense dans la barre de recherche. (Username de base : admin Password de base : pfsense)



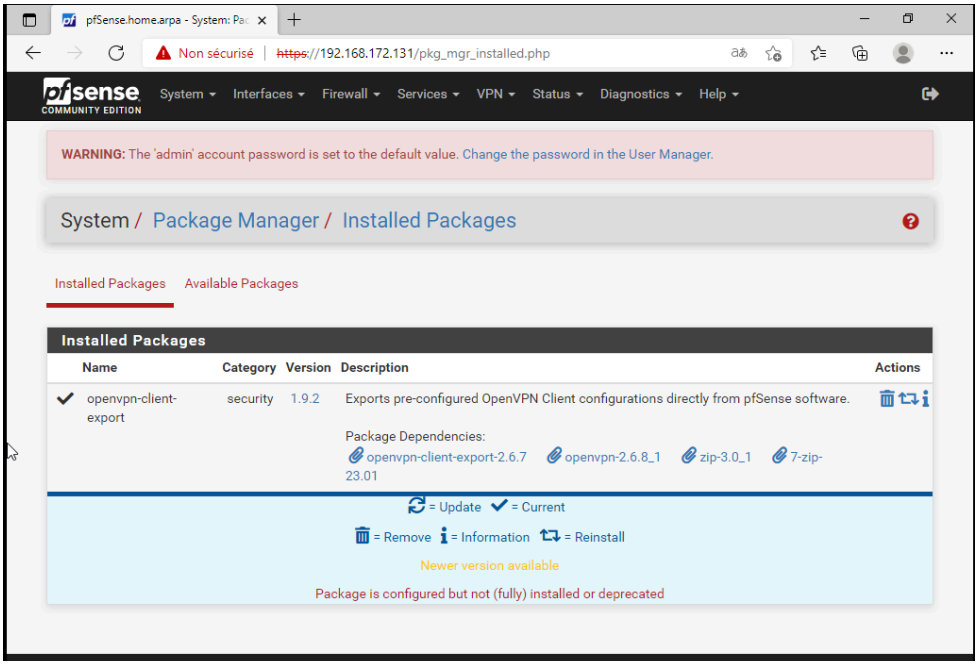
Une fois dessus, rendez-vous directement dans “Package Manager” - “Available Packages” et recherchez celui d’OpenVPN. Une fois trouvé cliquez sur “Install”



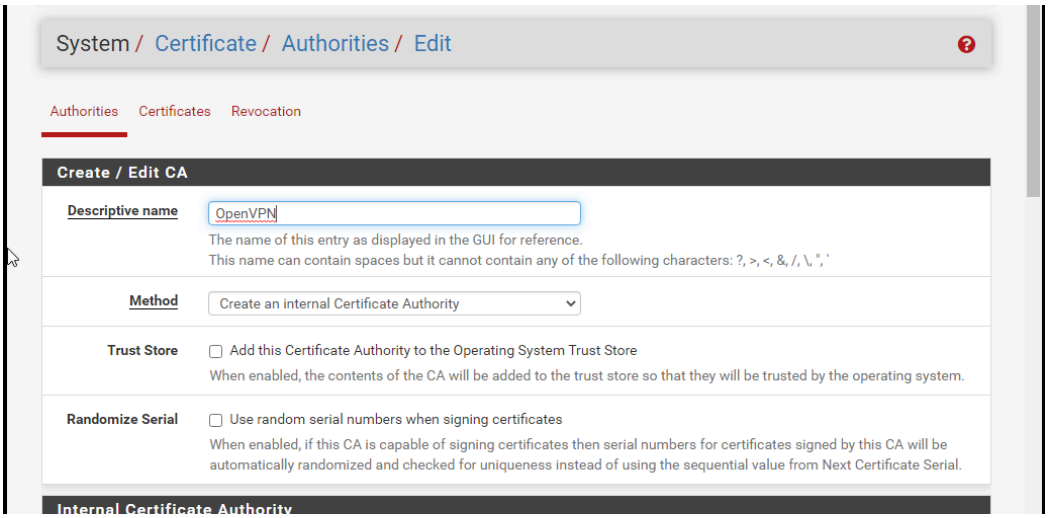
Une confirmation d'installation vous sera demandée, cliquez tout simplement sur "Confirm" puis laissez l'installation se faire.



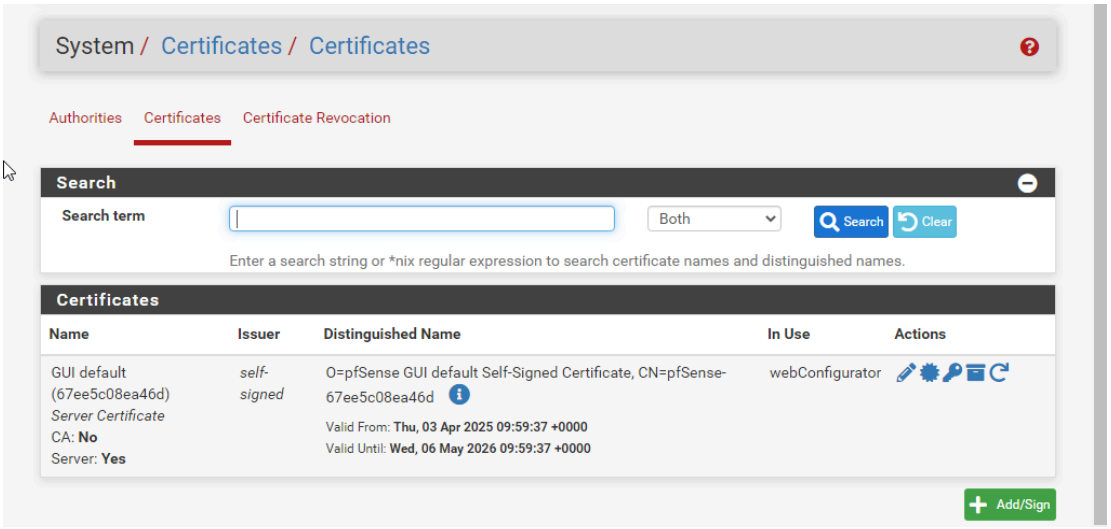
Une fois l'installation finie, vous pouvez constater en allant dans "Installed Packages" que l'installation à bien fonctionné. Comme vous le voyez aussi ce n'est pas la bonne version. Nous reviendrons plus tard sur ce point.



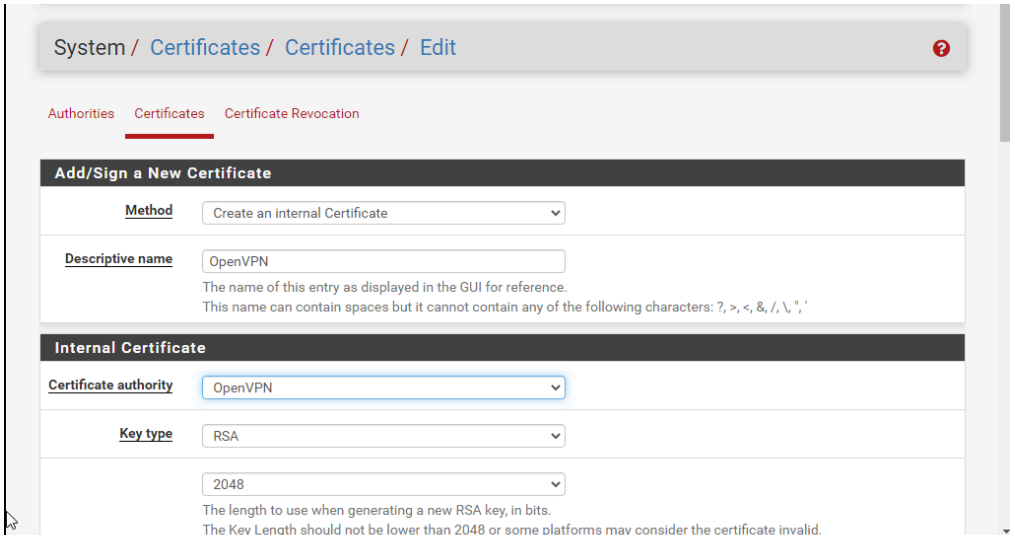
Avant toute chose rendez-vous dans “System”-”Certificate”-”Authorities” et commencez par créer une autorisation. Dans cette dernière donnez le nom que vous voulez.



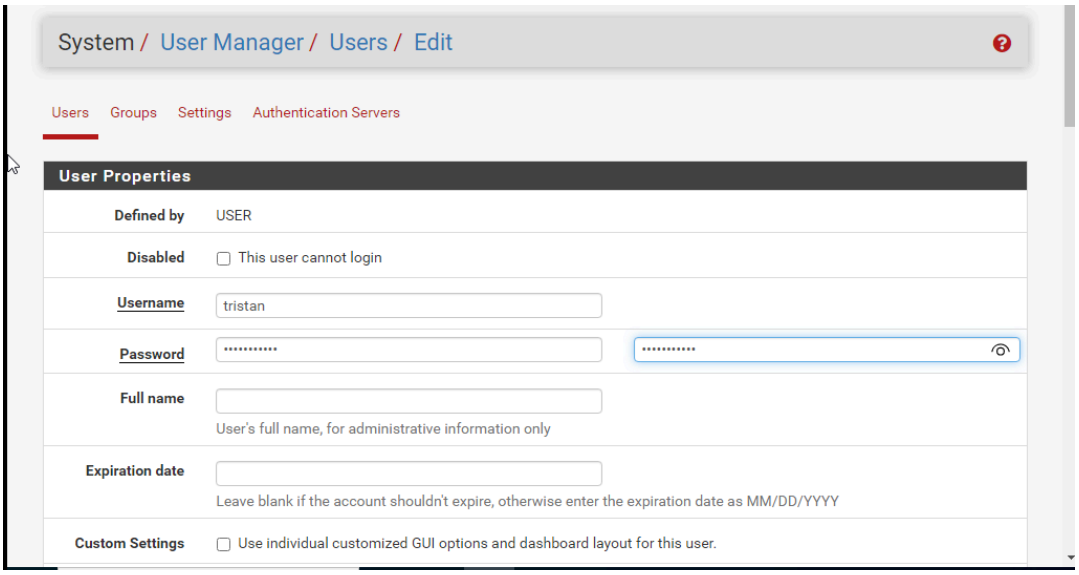
Nous allons donc commencer la création de certificats. Pour cela rendez-vous dans “System”-”Certificates”-”Certificates” puis cliquez sur “Add/Sign”.



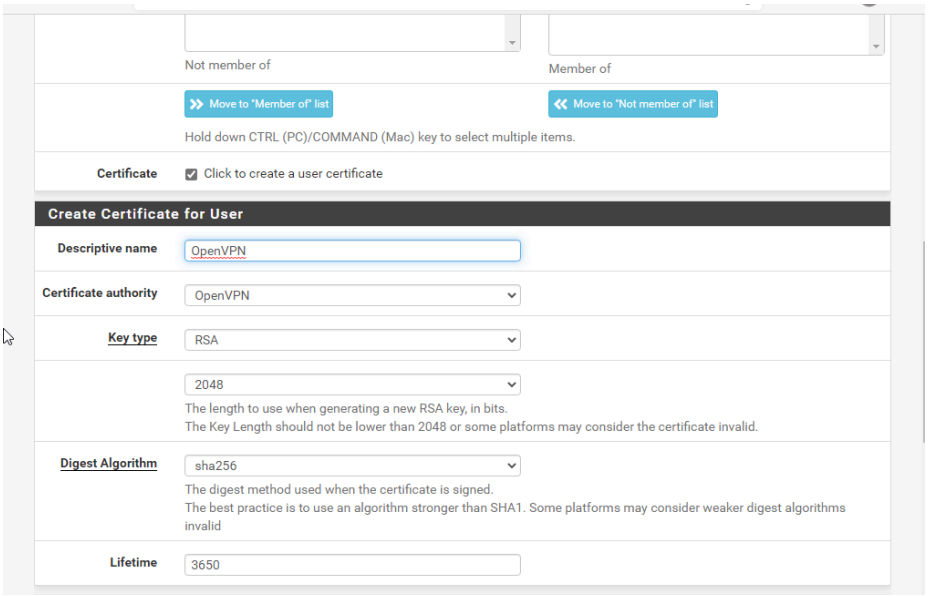
Une fois sur la création du certificat, il n'y aura que trois choses à modifier. Modifier dans un premier temps le nom de ce dernier, dans un deuxièmes temps sélectionnez votre Certificate authority *(celui que vous avez créé juste avant)* et pour finir sélectionnez "Server Certificate" et non pas "User Certificate".



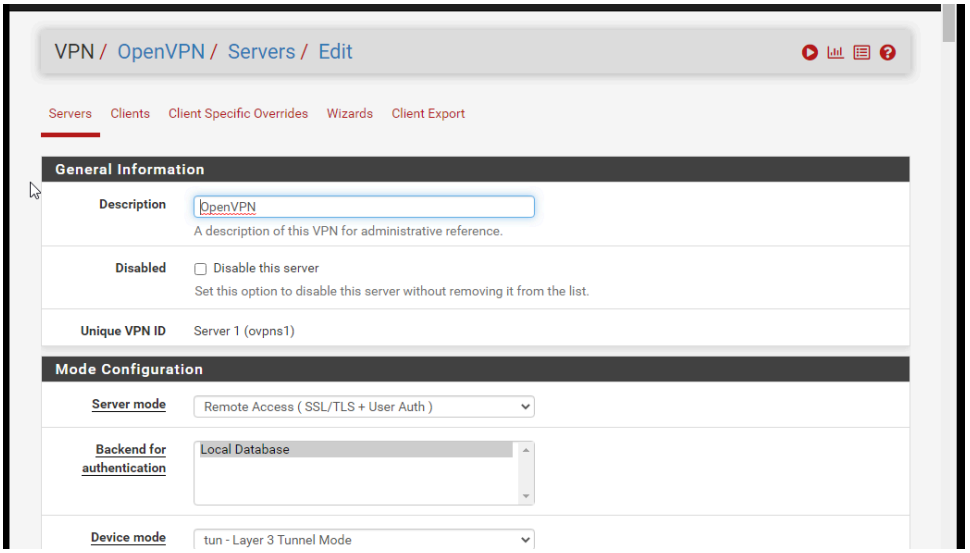
Maintenant il faudra créer un utilisateur, pour cela rendez-vous dans "System"-User Manager" et cliquez sur le bouton "Add". Donnez lui le nom et le mot de passe qui vous conviennent.



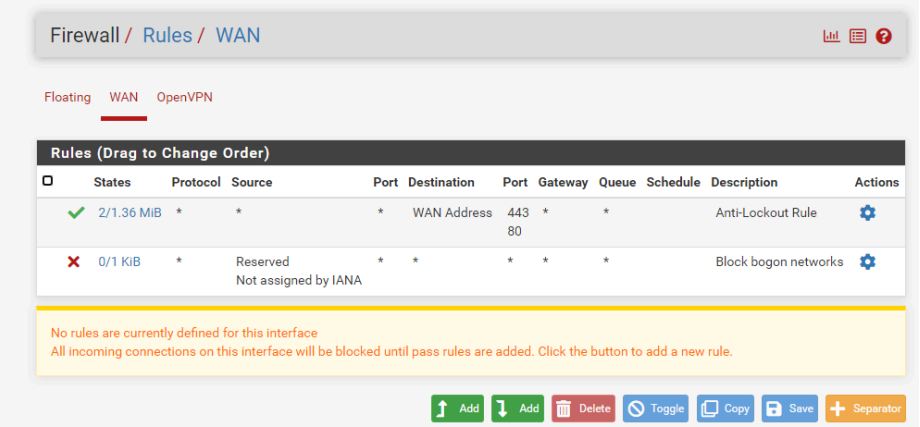
Pendant la création de ce dernier, il sera important de cocher la case “Click to create a user certificate” cette dernière va permettre de créer un certificat user en même temps que la création de notre user. Cochez alors la case et sélectionnez votre “Certificate authority”.



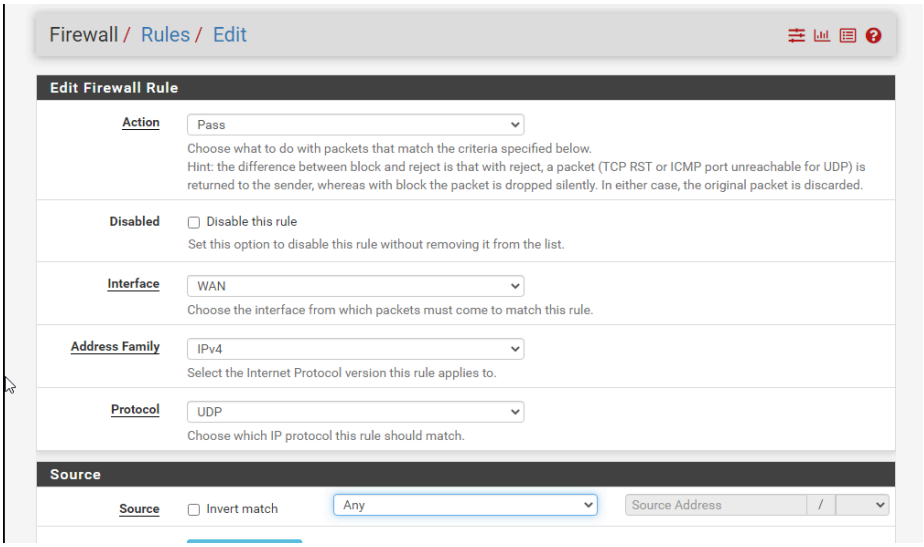
Il va maintenant falloir créer une autorisation pour le Remote Access via OpenVPN, pour cela rendez-vous dans “VPN”-”OpenVPN”-”Servers” et cliquez sur “ADD” Donnez le nom que vous désirez mais surtout pensez à choisir “Remote Access (SSL/TLS + User Auth)” dans la partie “Server mode”.



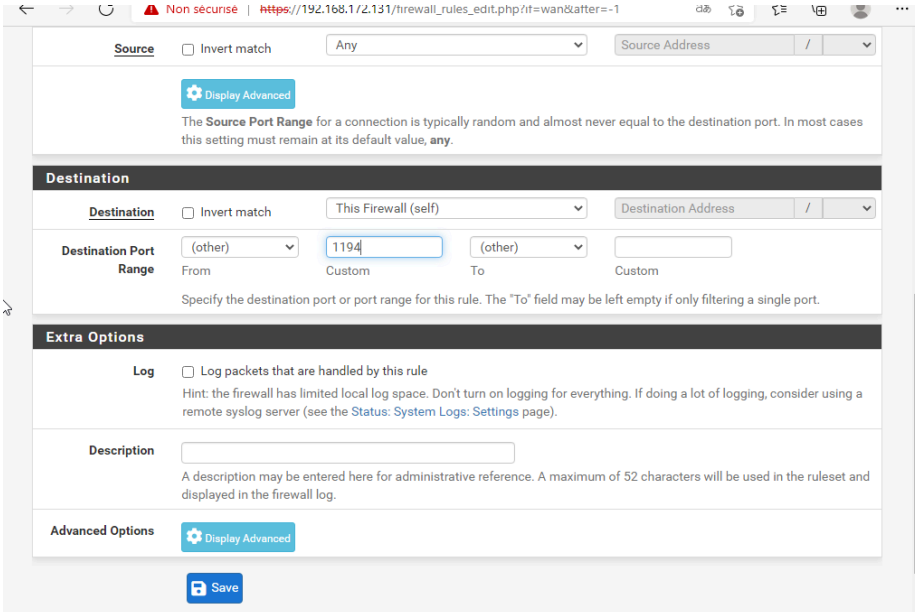
La fin du paramétrage approche, maintenant allez dans “Firewall”-”Rules”-”WAN” et ajoutez une nouvelle règle.



Dans cette dernière, choisissez l’action PASS et le Protocol UDP.



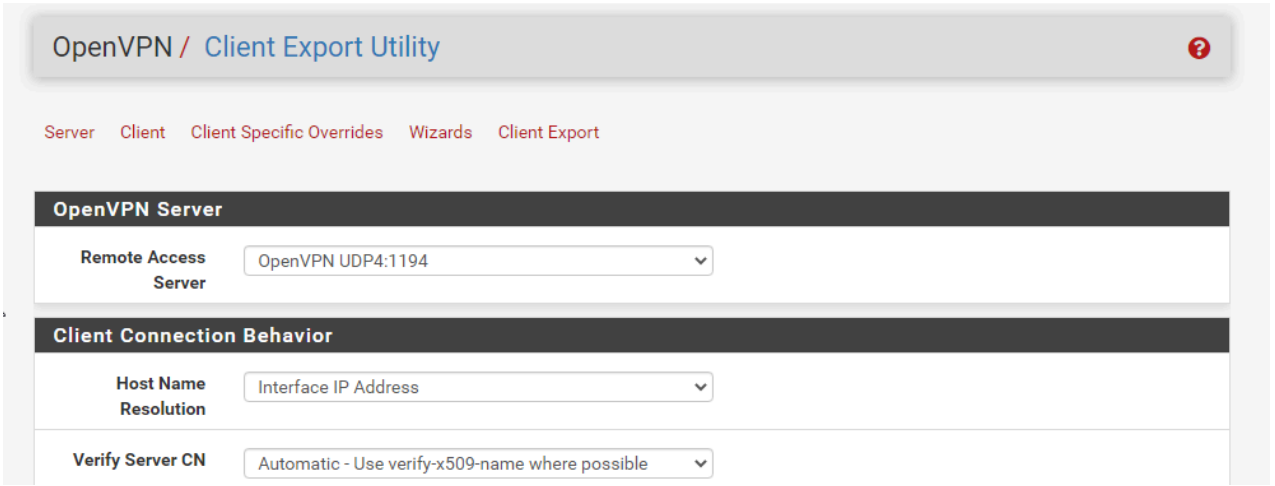
De plus pour la Destination prenez l'option "This Firewall (self) et pour la destination du port tapez le 1194. Une fois fait, vous pouvez cliquez sur "Save".



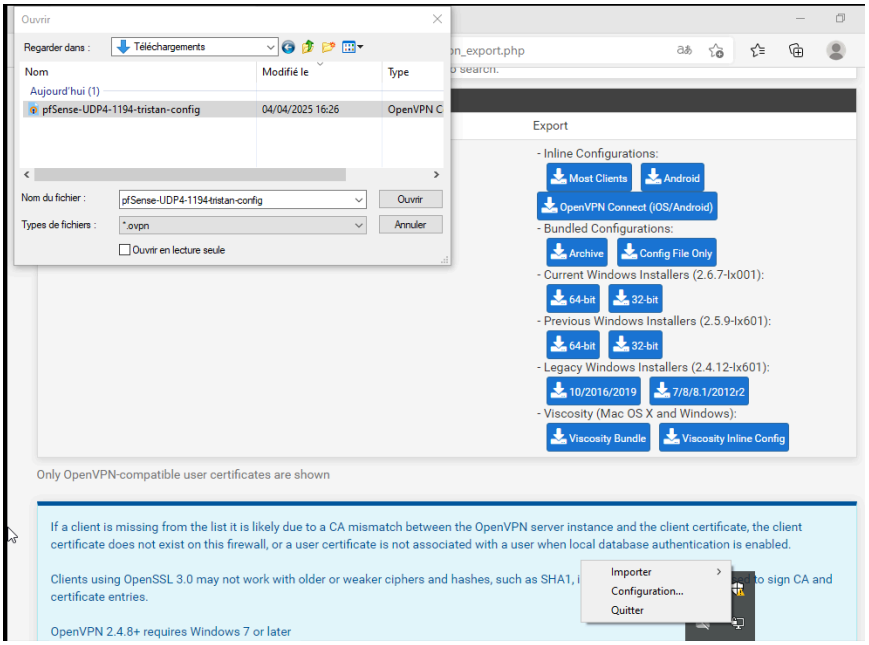
2. Installation du client et du lancement d'OpenVPN

Installez OpenVPN GUI, pour cela allez sur ce site et installez la version qui vous correspond : https://www.01net.com/telecharger/utilitaire/reseau/openvpn.html

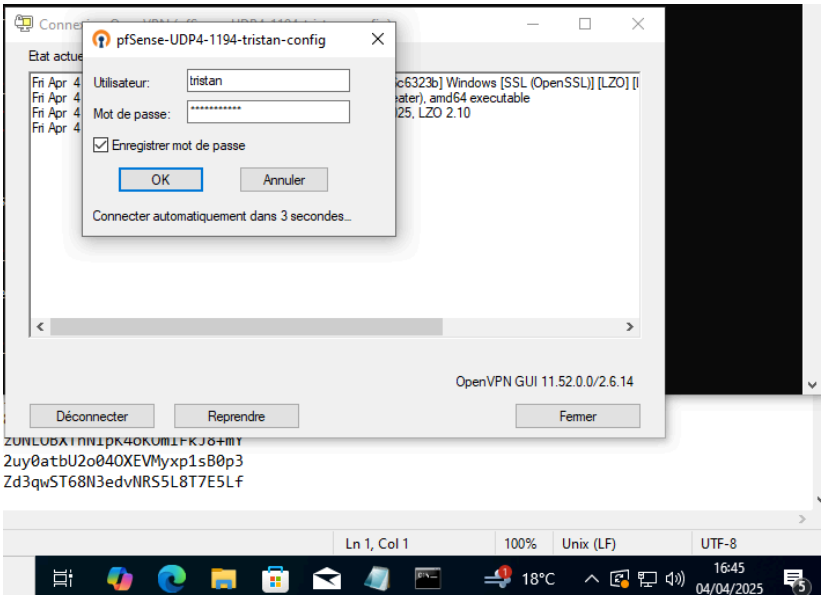
Pour le client souvenez-vous que l'export n'était pas à jour, pour avoir celui à jour, retournez dans "VPN"-OpenVPN"-"Client Export Utility" et descendez tout en bas.



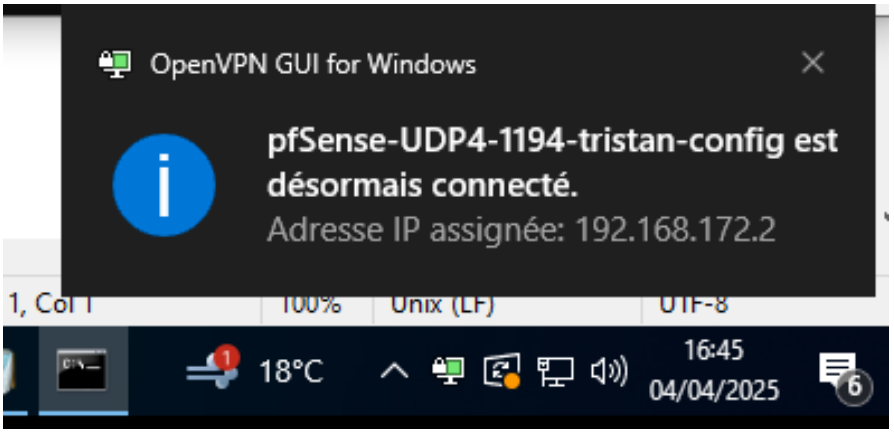
Une fois en-bas si vous avez tout bien fait vous devriez avoir tous les exports de disponible comme sur l'image ci-dessous. Téléchargez alors le "Most Clients". Une fois téléchargé, lancez votre OpenVPN, faites un clique droit dessus et "Importer". Sélectionnez alors tout simplement le fichier "Most Clients" que vous venez de télécharger.



Pour finaliser la connexion il vous sera demandé d'entrer l'utilisateur et le mot de passe de votre OpenVPN. Entrez le puis faites "Ok".



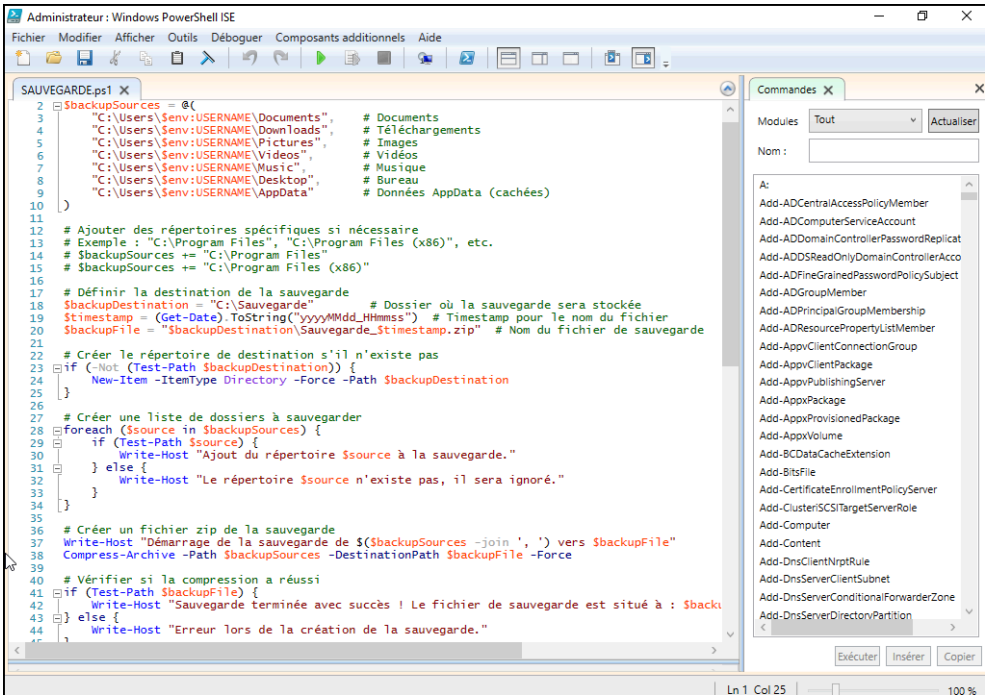
Voilà vous êtes maintenant connecté via votre OpenVPN, il est donc bien fonctionnel et disponible. Temps que vous êtes connecté dessus, vous aurez en bas à droite de votre écran un petit écran vert signifiant que vous êtes dessus.



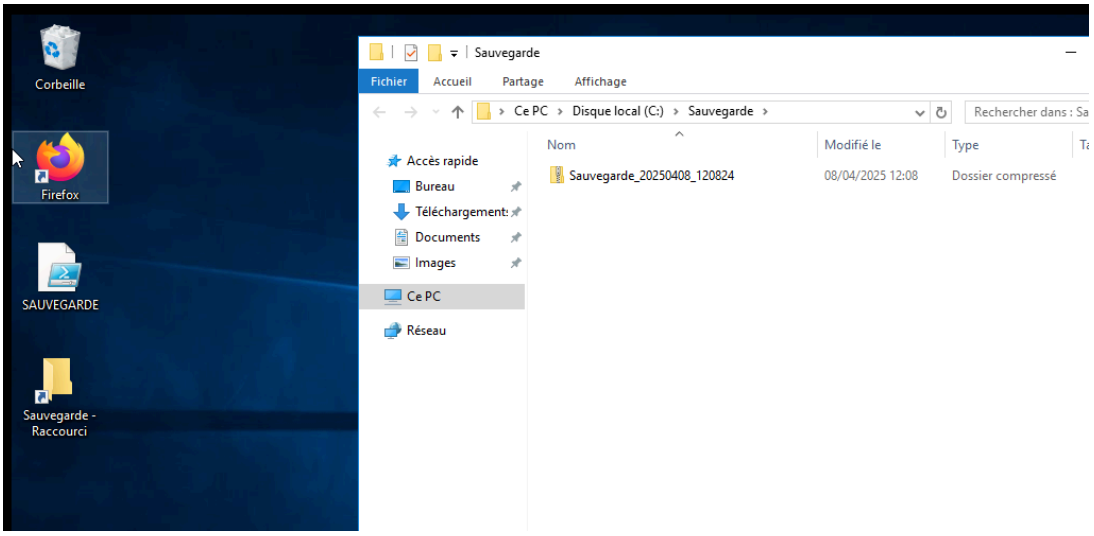
XI - Script de sauvegarde PowerShell ISE

1. Faire la sauvegarde

Pour faire la sauvegarde, nous allons utiliser un script PowerShell trouvé en ligne permettant de faire une sauvegarde du server AD. Pour cela ouvrez donc PowerShell ISE et enregistrez ce script à l'intérieur.

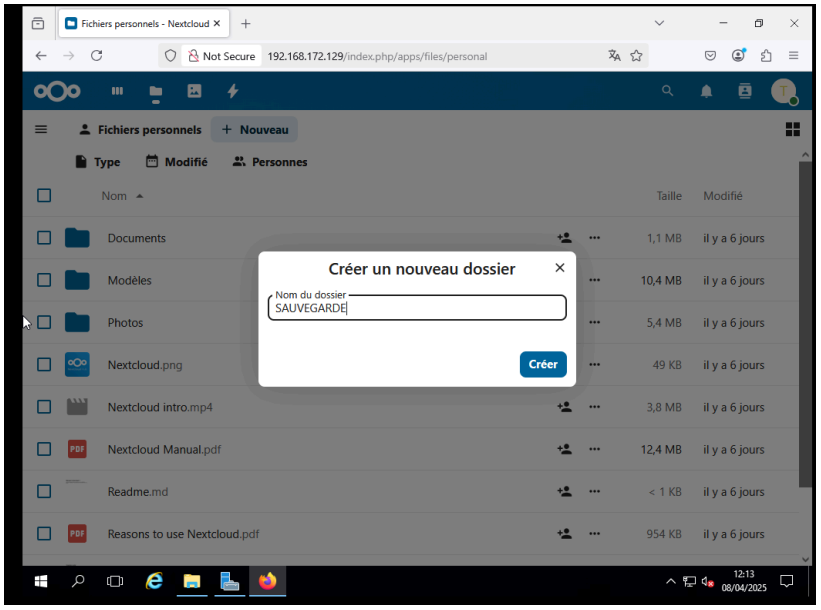


Enregistrez le script sur le bureau pour pouvoir l'exécuter en double cliquant dessus et mettez le raccourci du dossier sauvegarde qui se trouve dans C:\Sauvegarde (endroit ou la sauvegarde sera envoyé). Comme vous pouvez le voir avec l'image ci-dessous, une sauvegarde ZIP se trouve bel et bien dans le dossier sauvegarde. Cette dernière résulte du lancement du script.

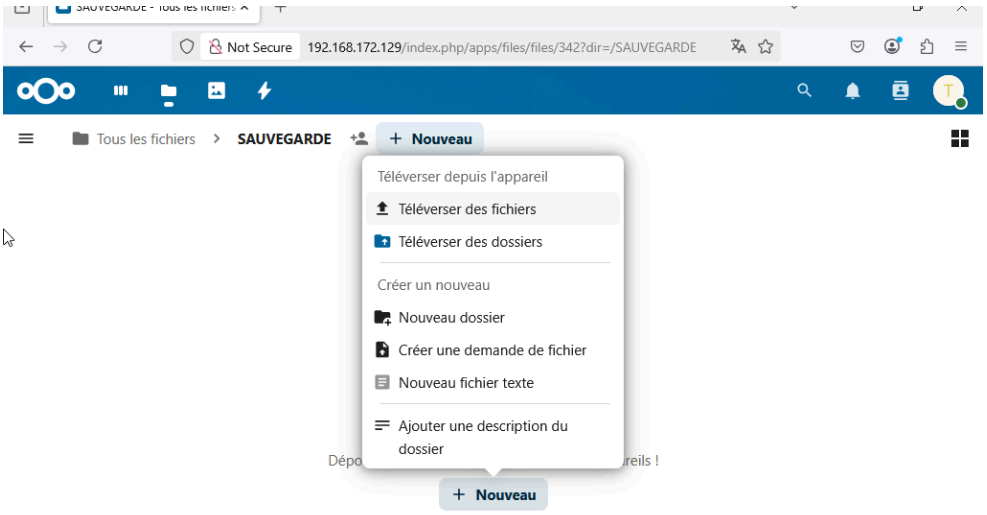


2. Déposer la sauvegarde sur NextCloud

Pour cela, connectez vous à votre NextCloud web. Une fois dessus créer un dossier qui vous permettras d'y déposer vos fichier .Zip contenant vos sauvegardes.



Une fois créé, rendez-vous dans le dossier et téléversez votre fichier.



Une fois le téléversement fini, vous pouvez constater que la sauvegarde est belle et bien présente dans votre dossier. Vous avez donc une sauvegarde de disponible sur votre NextCloud !