-

BTS SIO 2025 Option SISR

Epreuve E6

-

Situation professionnelle 1 – Documentation Technique

SOMMAIRE

1.1) LOT 1 : Mise en place d'un VPN site à site avec PFSense 3
Documentation de mise en place d'un VPN via IP Sec (PFSense) : 3
Prérequis : 3
Étape 1 : Installation de PFSense 3
Étape 2 : Sur le site A 5
Étape 2 : Sur le site B 9
1.2) LOT 2 : Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement) 13
Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement) 13
Prérequis : 13
Étape 1 : Installation des rôles / fonctionnalités sur le serveur 1 : 13
Installation du rôle sur le serveur 13
Configuration du rôle AD avec mise en place d'une forêt 14
Configuration du rôle DHCP avec création d'une étendue de test 17
Étape 2 : Installation des rôles / fonctionnalités sur le serveur 2 : 20
Installation des rôles AD DS et DHCP sur le second serveur. 22
Configuration du basculement DHCP 24
1.3) LOT 3 : Installation du rôle DFS, DFSR et mise en place de l'espace de nom 25
Installation d'un serveur Windows SERVER 2022 avec les services DFS et DFSR 25
Prérequis : 25
Création du dossier de l'espace de nom DFS : 32
1.4) LOT 4 : Installation de TrueNAS et montage d'une cible iSCSi 40

1) Documentation d'installation

1.1) LOT 1 : Mise en place d'un VPN site à site avec PFSense

Documentation de mise en place d'un VPN via IP Sec (PFSense) :

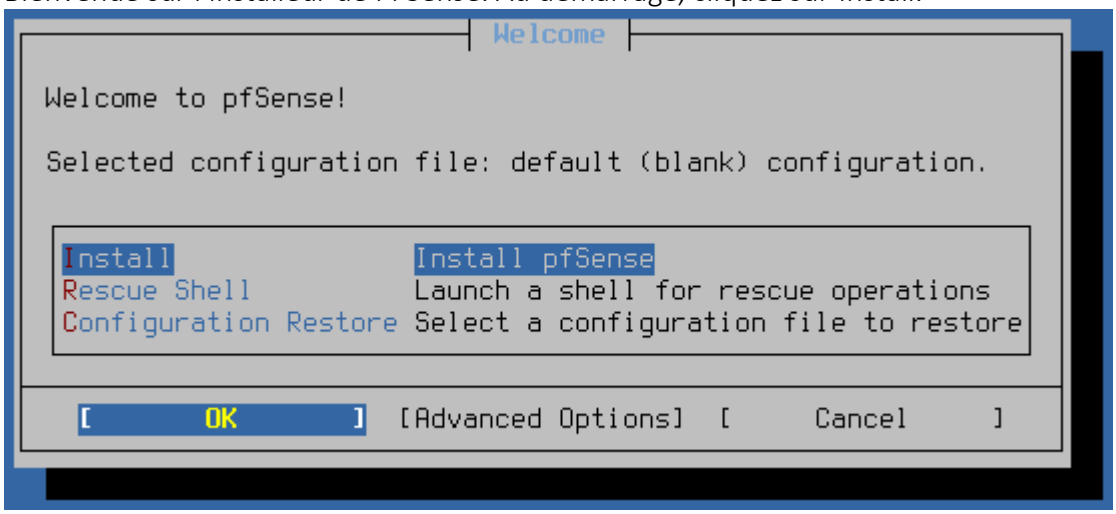
Prérequis :

- 2 routeurs (en l'occurrence PFSense en fera office)
- 2 clients Windows qui serviront à accéder aux pages de configuration
- 2 interfaces réseaux (LAN et WAN)

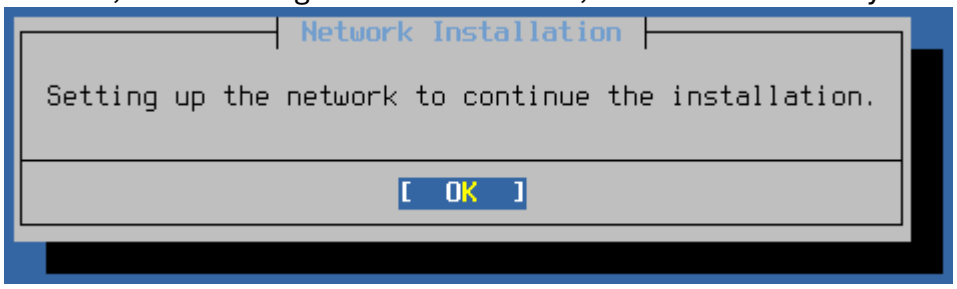
Cet exemple prendra en compte l'interconnexion de 2 routeurs qui seront sur des machines virtuelles, sur des PC différents. Les routeurs auront 2 cartes réseaux, une en Bridge sur la carte Wi-Fi physique, et une en LAN, qui sera la même que celle pour le client Windows. Le client tant qu'à lui aura simplement une carte LAN. C'est grâce à cette interface qu'il pourra accéder a la page de configuration.

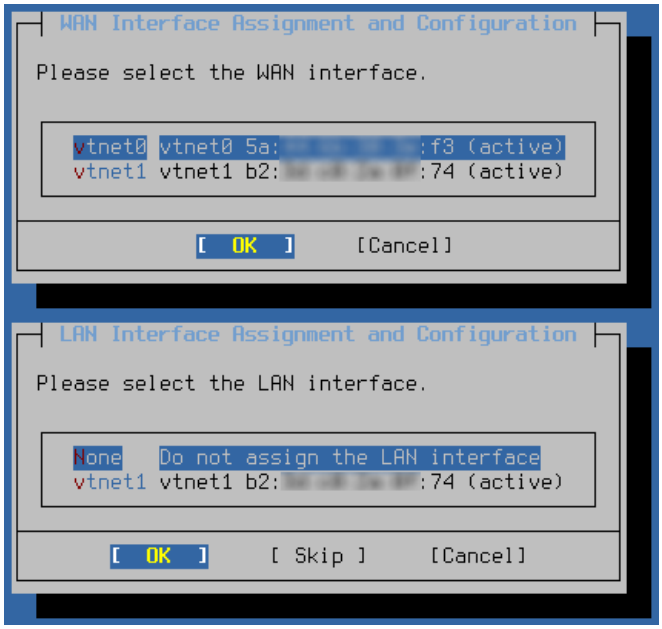
Étape 1 : Installation de PFSense

Bienvenue sur l'installeur de PFSense. Au démarrage, cliquez sur Install.



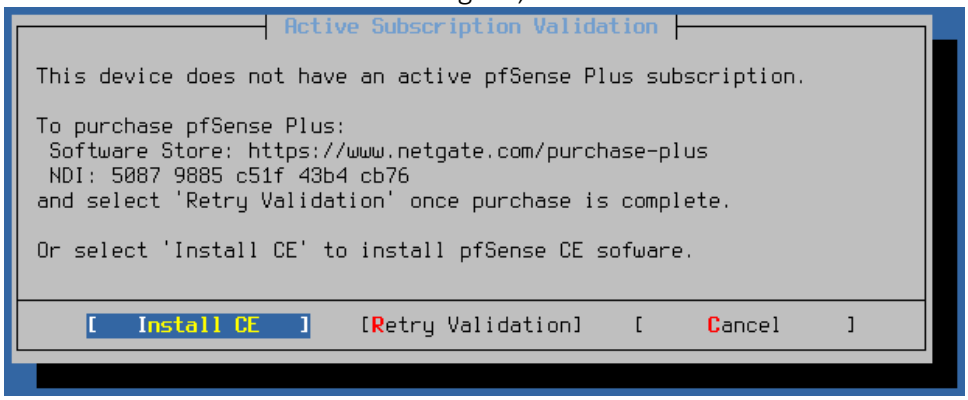
Après avoir démarré l'installation, assigner les interfaces WAN et LAN aux cartes réseaux, la carte Bridge sera la carte WAN, et la carte Host-Only sera la carte LAN.



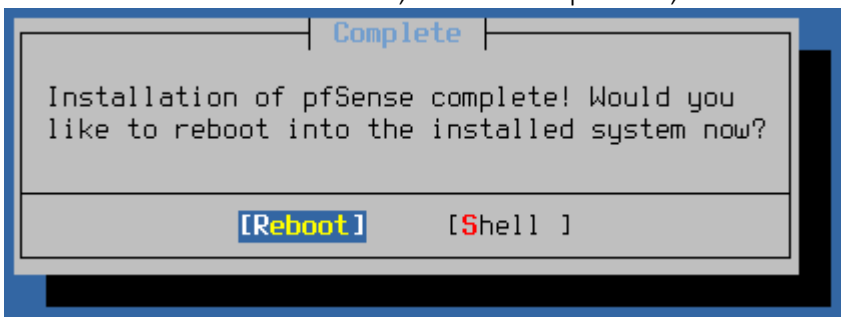


Il est recommandé d'attribuer une adresse IP fixe pour l'adresse LAN, pour éviter les problèmes d'accès à l'interface WEB de PFSense.

Une fois les cartes WAN et LAN assignés, démarrer l'installation des fichiers de pfSense.

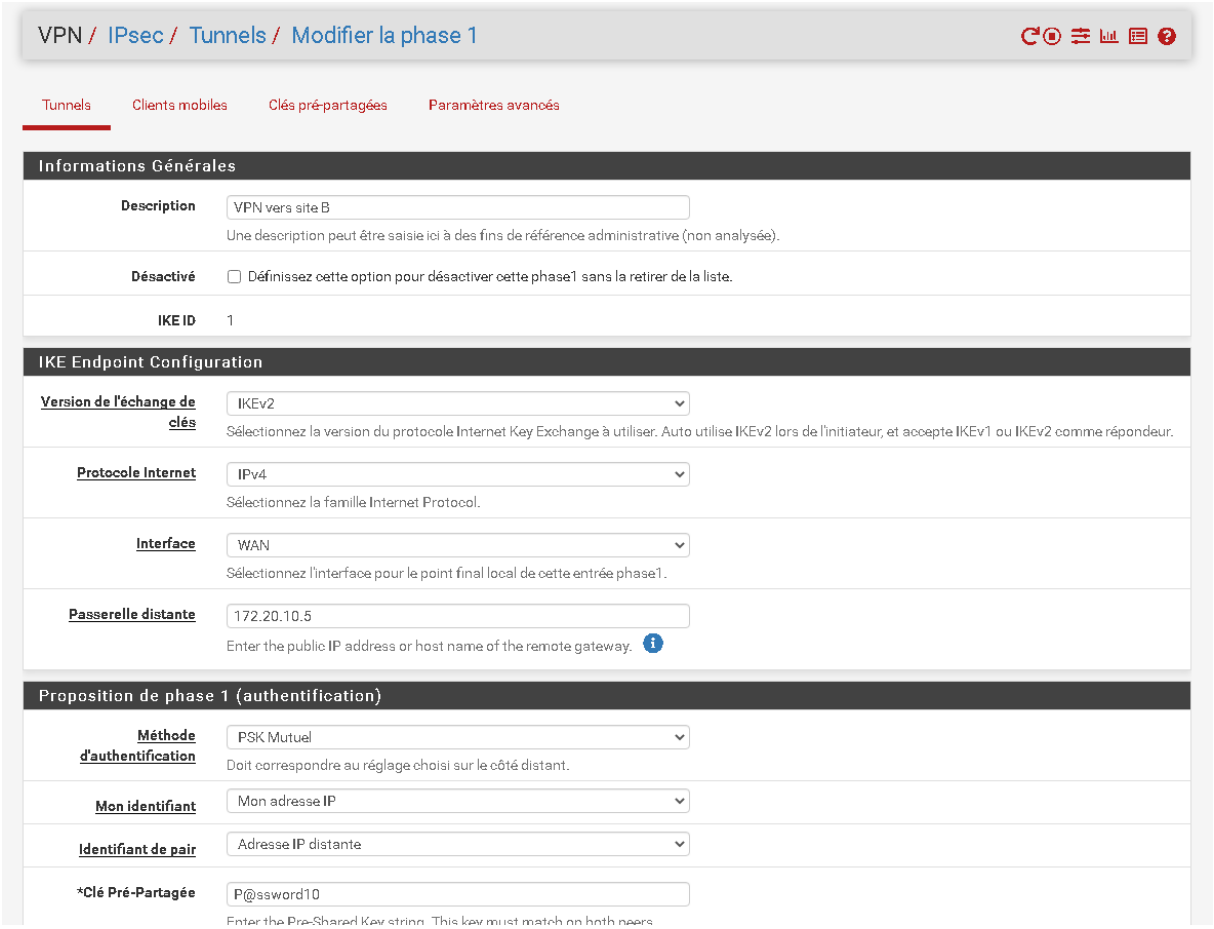


Une fois l'installation terminée, redémarrer pfSense, et l'installations sera alors terminée.

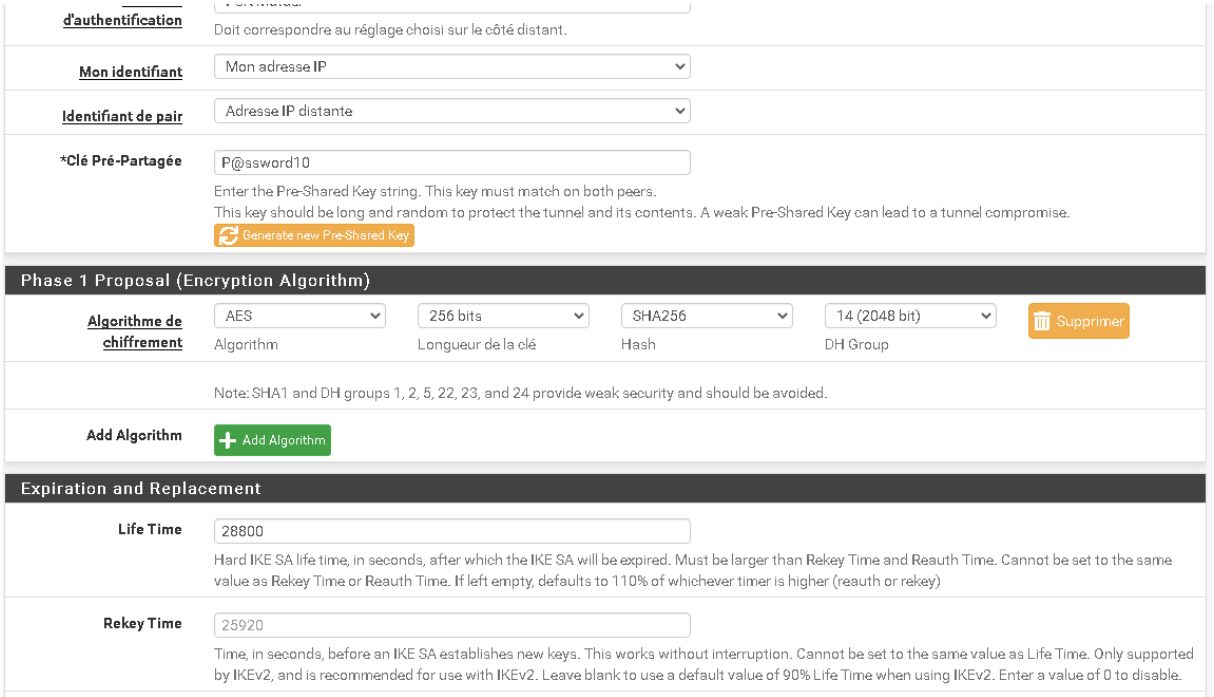


Étape 2 : Sur le site A

Pour accéder à l'interface, rentrer l'adresse LAN de pfSense dans un navigateur.
Dans la section VPN > IP Sec, ajouter une phase P1 :

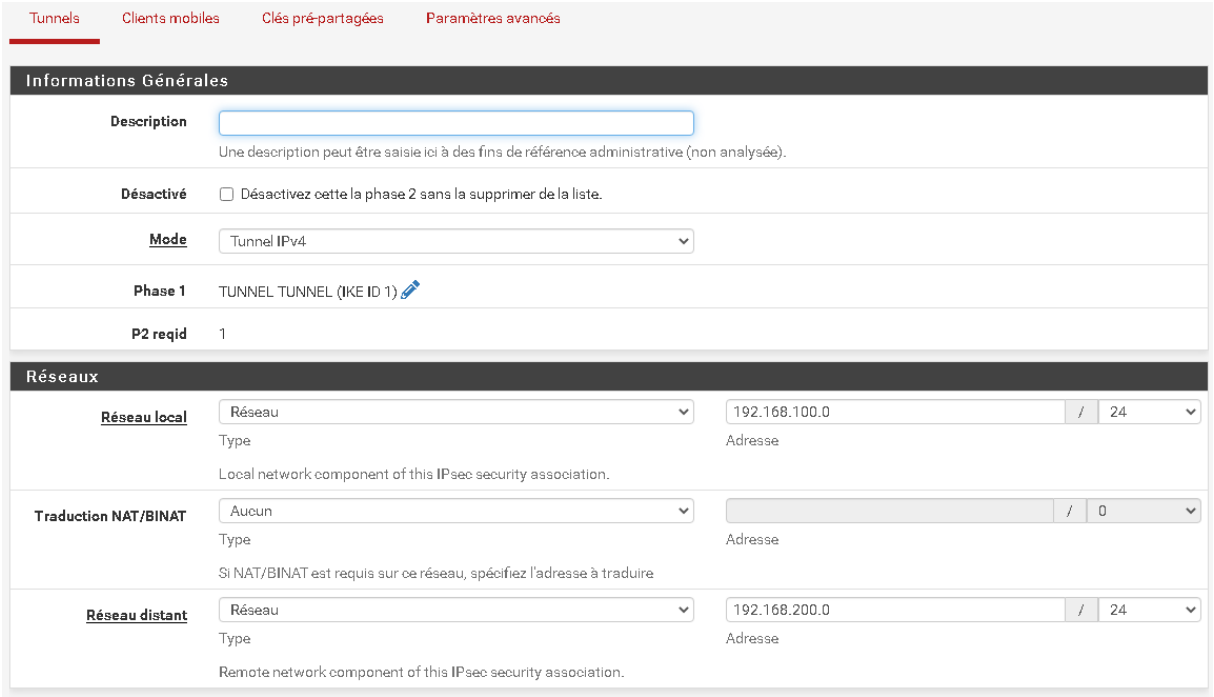


Dans la passerelle distante, renseigner l'adresse WAN du routeur de l'autre site.



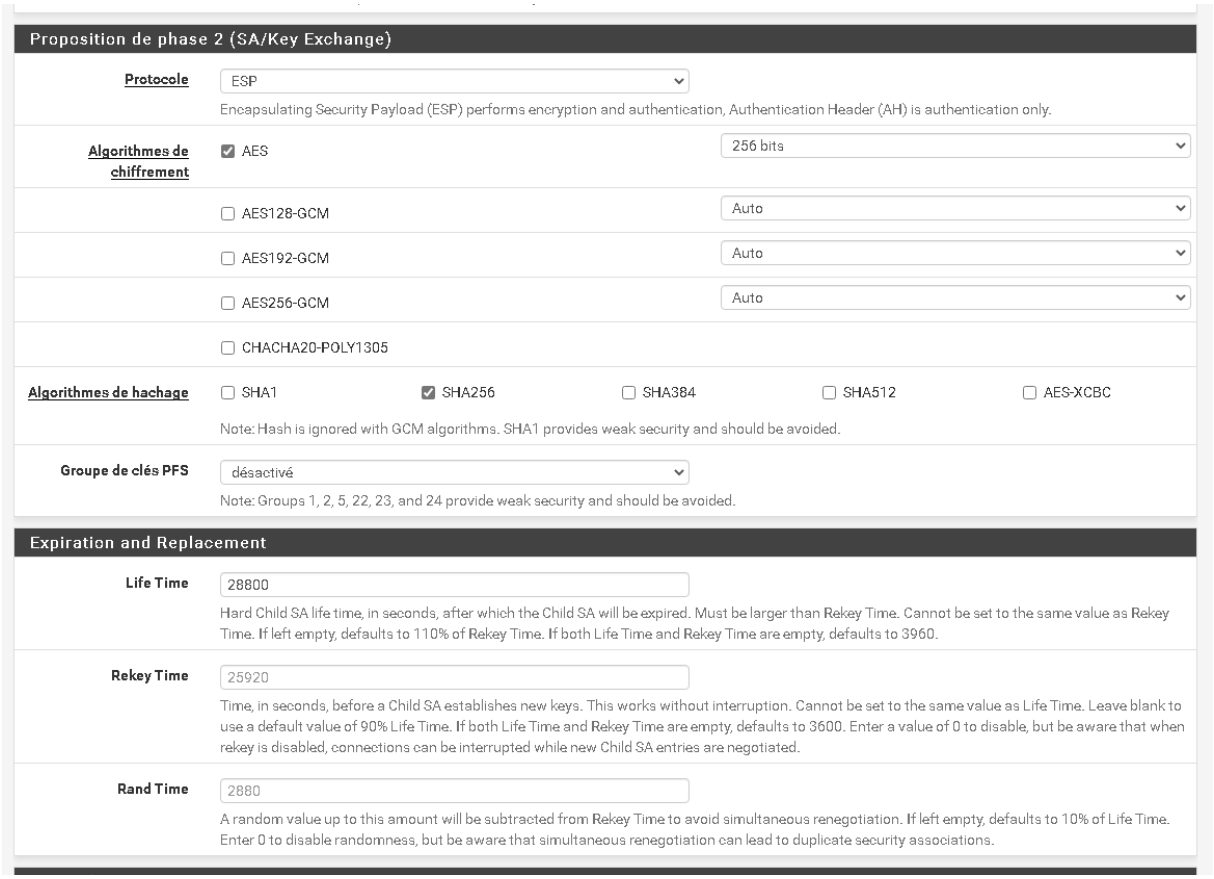
Concernant les paramétrages, renseigner les mêmes que ci-dessus.

Après avoir créé la P1, créer une P2 qui va compléter la configuration de l'élaboration du tunnel.

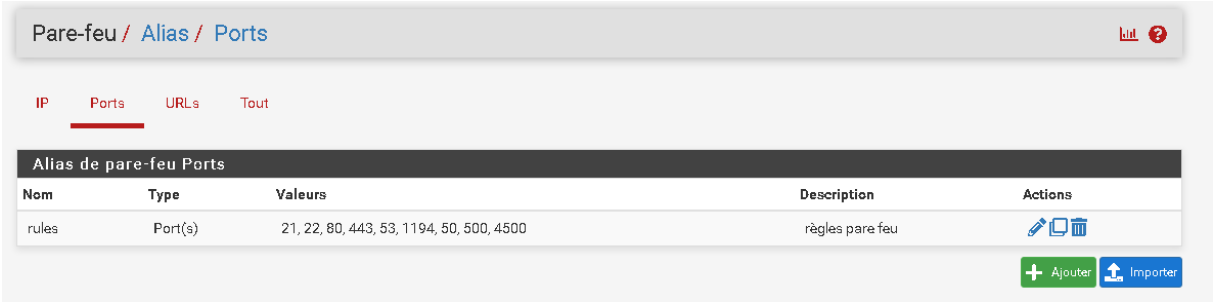


Dans Réseau local, rentrer la plage du réseau LAN du site A, et dans le Réseau distant, rentrer la plage du réseau LAN du site B.

Attention : Il faut bien faire attention à avoir les mêmes réglages sur les P2 des 2 routeurs. Une incohérence pourrait faire crasher le tunnel.

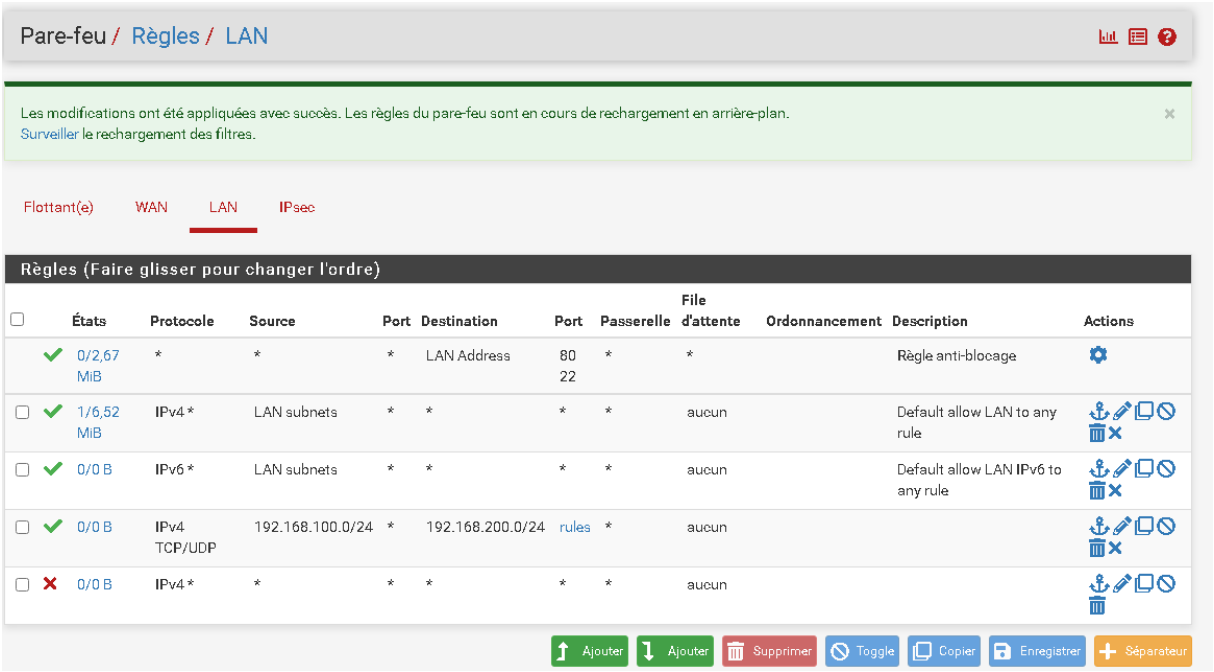


Il faut également qu'il y ait le même algorithme de chiffrement sur les 2 routeurs.
Pour finir, il faut ajouter des règles de pare-feu afin que la communication puisse se faire.
Dans l'onglet Pare-feu > Aliases :



Créer un alias qui va rensenser tous les ports qui doivent être ouverts.

Ensuite, dans Pare-feu > Rules > LAN, ajouter une règle qui va utiliser l'alias pour connaître les ports à ouvrir. A la fin, ajouter une règle qui bloque tous les protocoles de toutes les sources et toutes les destinations. Cela est un principe de sécurité.

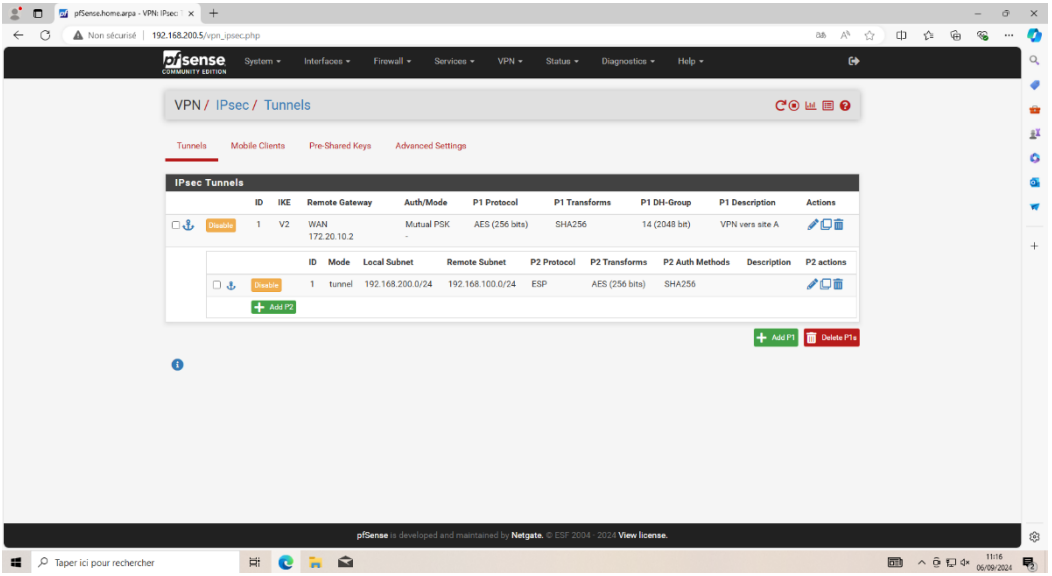

Pare-feu / Règles / LAN
Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan.
Surveiller le rechargement des filtres.
Flottant(e)
WAN
LAN
IPsec
Règles (Faire glisser pour changer l'ordre)
États
Protocole
Source
Port
Destination
Port
Passerelle
File d'attente
Ordonnancement
Description
Actions
0/2,67 MiB * * * LAN Address 80 22 * * Règle anti-blocage
1/6,52 MiB IPv4 * LAN subnets * * * * aucun Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * aucun Default allow LAN IPv6 to any rule
0/0 B IPv4 TCP/UDP 192.168.100.0/24 * 192.168.200.0/24 rules * aucun
0/0 B IPv4 * * * * * * aucun
Ajouter
Ajouter
Supprimer
Toggle
Copier
Enregistrer
Séparateur

Étape 2 : Sur le site B

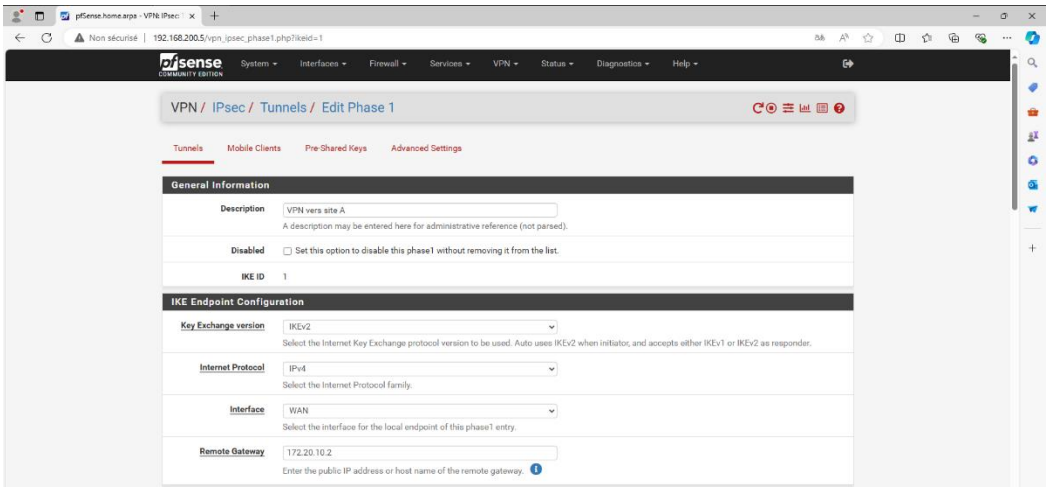
Pour accéder à l'interface, rentrer l'adresse LAN de pfSense dans un navigateur.

1. Configurer le VPN.

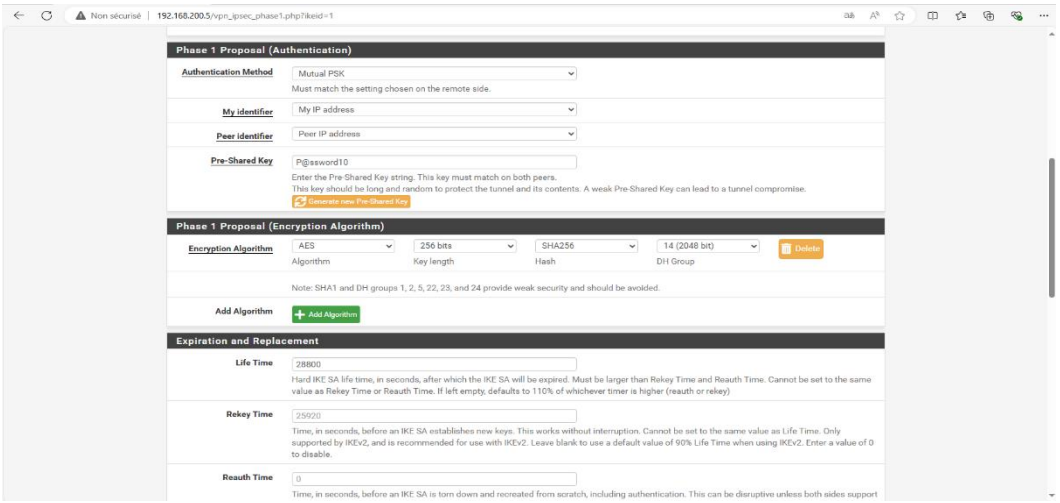
Dans la section VPN > IP Sec, ajouter une phase P1.



P1.

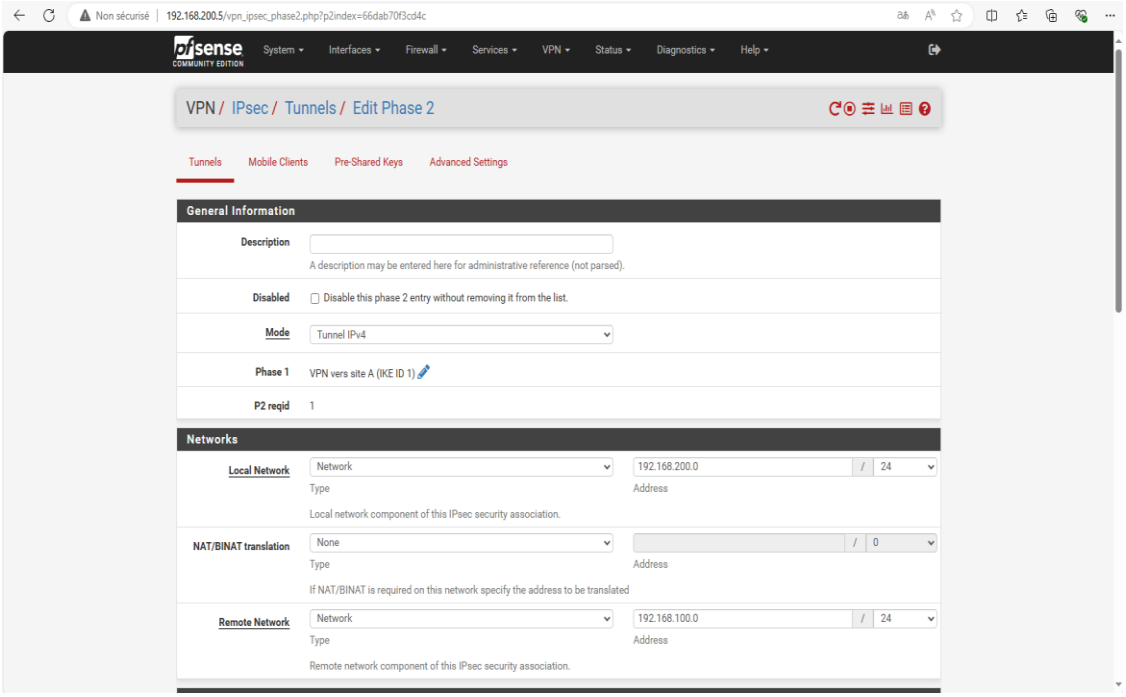


Dans la passerelle distante, renseigner l'adresse WAN du routeur de l'autre site.



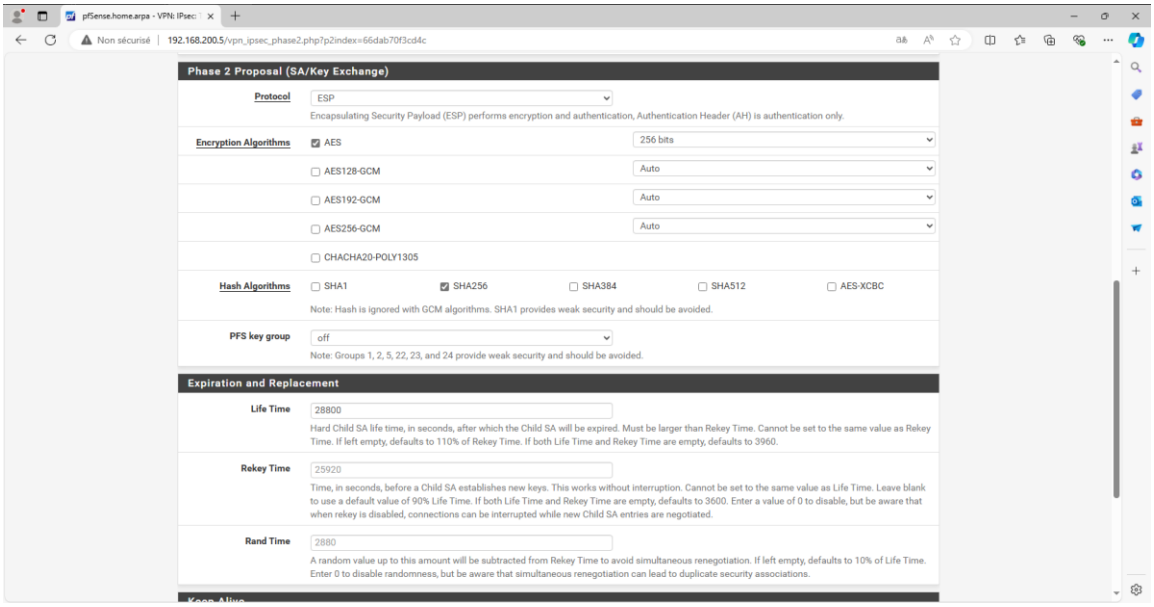
Concernant les paramétrages, renseigner les mêmes que ci-dessus.

P2.
Après avoir créé la P1, créer une P2 qui va compléter la configuration de l'élaboration du tunnel.



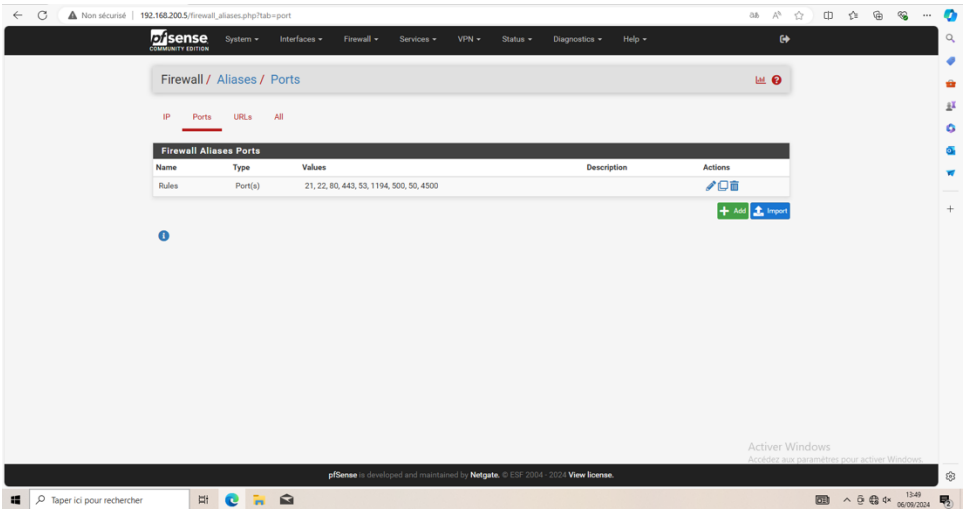
Dans Réseau local, rentrer la plage du réseau LAN du site A, et dans le Réseau distant, rentrer la plage du réseau LAN du site B.

Attention : Il faut bien faire attention à avoir les mêmes réglages sur les P2 des 2 routeurs. Une incohérence pourrait faire crasher le tunnel.

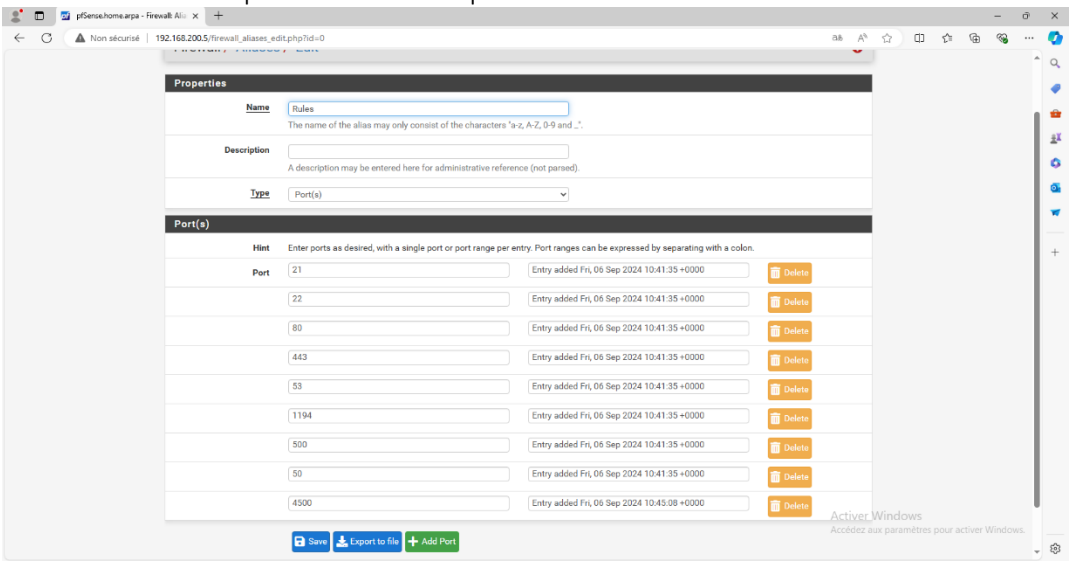


Il faut également qu'il y ait le même algorithme de chiffrement sur les 2 routeurs.

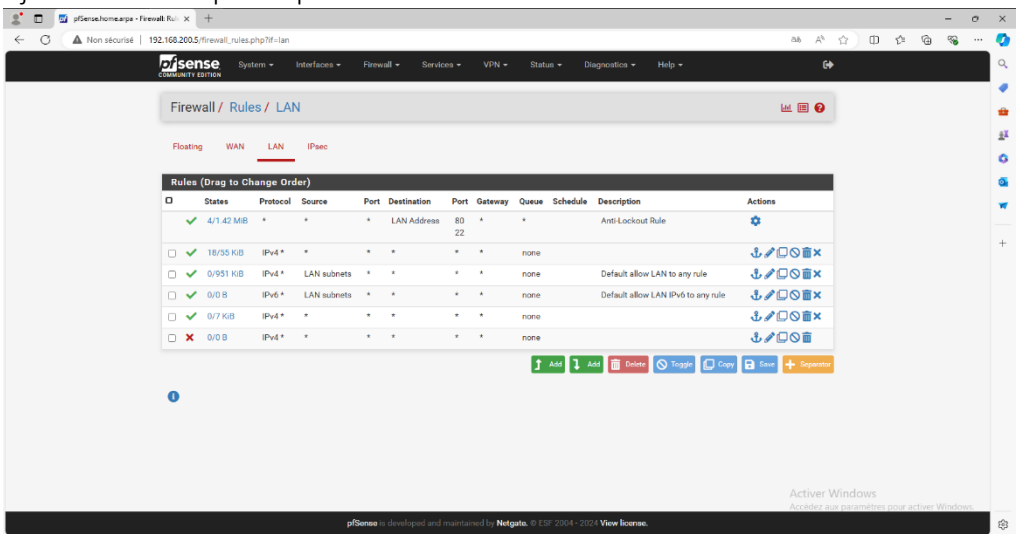
2.Configuration des règles du firewall.



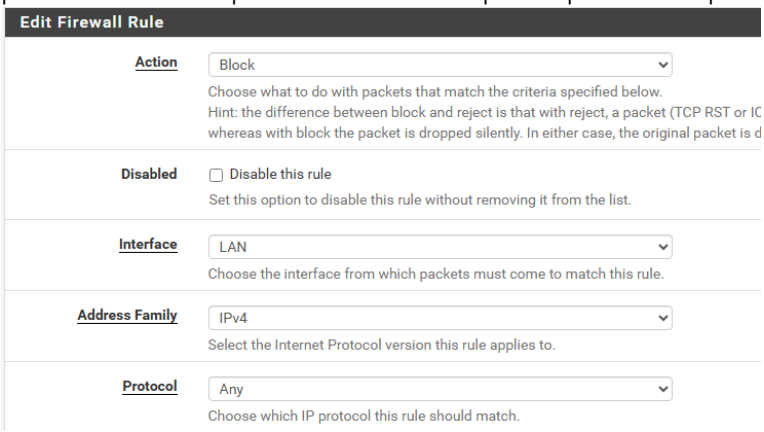
Aller dans Firewall puis Aliases et cliquer dans la section Ports.



Ajouter tous les ports qui vous seront utiles.



Ensuite retourner dans Firewall puis Rules et dans la section Lan et ajouter une règle qui va permettre de bloquer tous les autres ports qui ne sont pas utilisé.



Cela doit être comme ça.

Après toutes ces étapes, vous aurez un tunnel VPN fonctionnel. Vous pourrez vérifier son fonctionnement dans l'onglet Status\IPSec

1.2) LOT 2 : Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement)

Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement)

Prérequis :

- 1 Windows SERVER 2022 avec interface graphique (Carte réseau VMNet1)
- 1 Windows SERVER 2022 Core (Carte réseau VMNet1)
- 1 Routeur (Carte réseau VMNet1, et VMNet2) (optionnel, utilisé dans le cadre du projet M2i)

Description des cartes réseau dans ce cas :

- VMNet 1 : Carte Host-only (réseau LAN)
- VMNet2 : Carte NAT / Bridge (réseau WAN)

Cet exemple utilisera 2 serveurs mentionnés auparavant. Nous passerons par un routeur (PFSense) qui fera office de passerelle entre le réseau local et le réseau WAN. Nous allons voir comment installer les fonctionnalités AD DS, DNS (fonctionnalité obligatoire avec AD DS), ainsi que DHCP. Nous allons également voir comment répliquer tout cela sur le serveur Core pour assurer la disponibilité en cas de panne du serveur 1.
L'installation du rôle DNS ne sera pas mentionnée explicitement car elle est automatiquement installée avec l'Active Directory. Aucune configuration n'est alors requise pour que DNS fonctionne.

Étape 1 : Installation des rôles / fonctionnalités sur le serveur 1 :

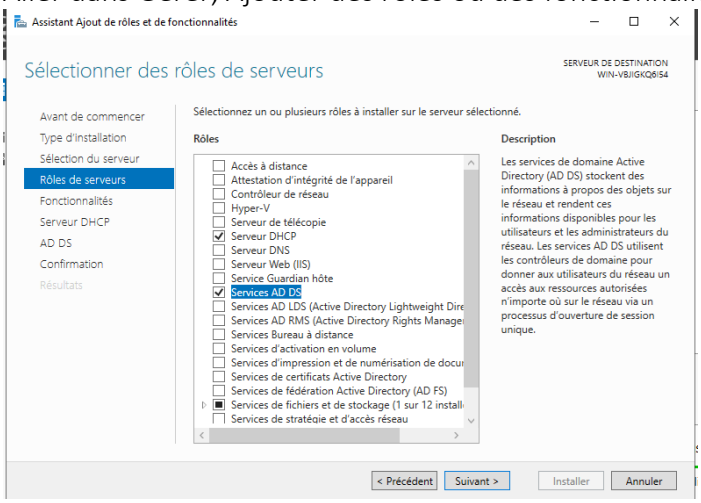
Installation du rôle sur le serveur

Pour commencer, nous allons définir une adresse IP fixe sur le serveur :

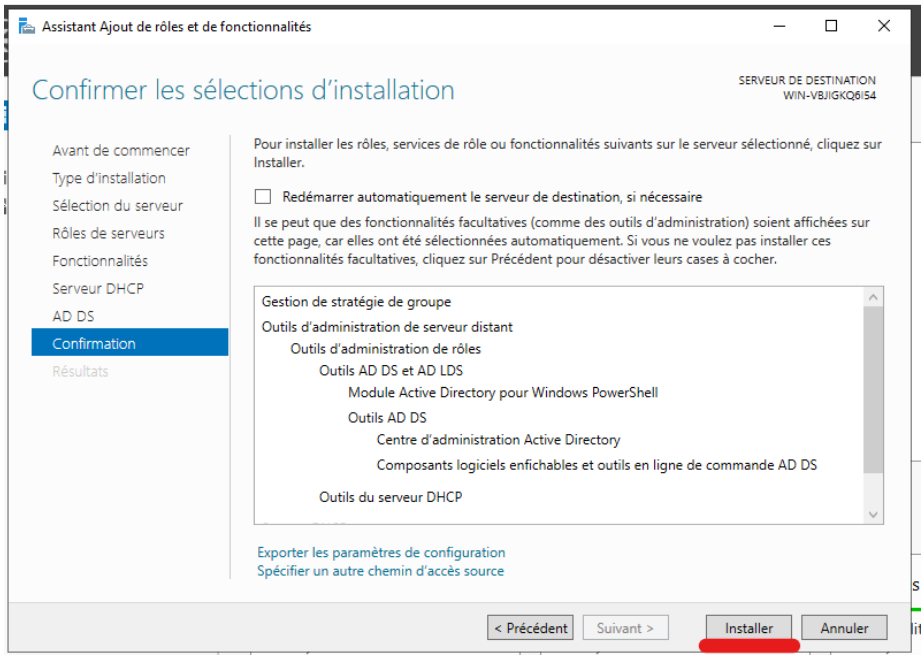
- Aller dans le gestionnaire de serveur sous Serveur Local
- Double cliquer sur Adresse IPv4 attribuée par DHCP
- Cliquer sur sa carte réseau *EthernetX*
- Aller dans les propriétés, puis Protocole Internet version 4
- Dans cette interface il sera alors possible de définir une adresse IP fixe.

Configuration du rôle AD avec mise en place d'une forêt

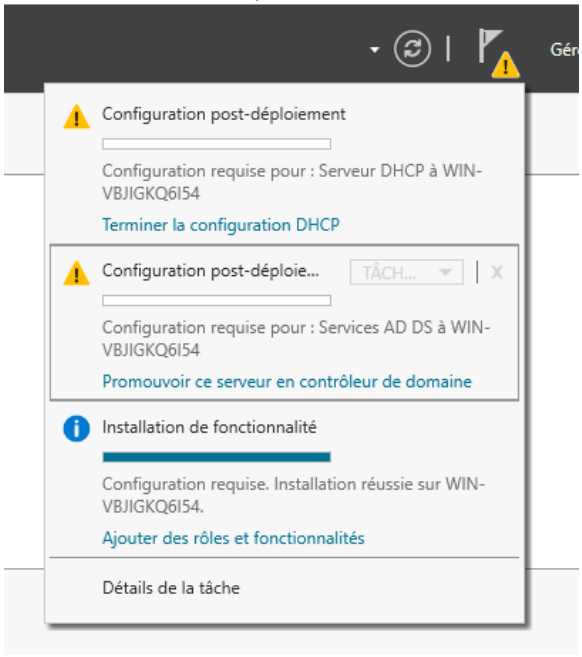
Aller dans Gérer, Ajouter des rôles ou des fonctionnalités, puis sélectionner celles-ci



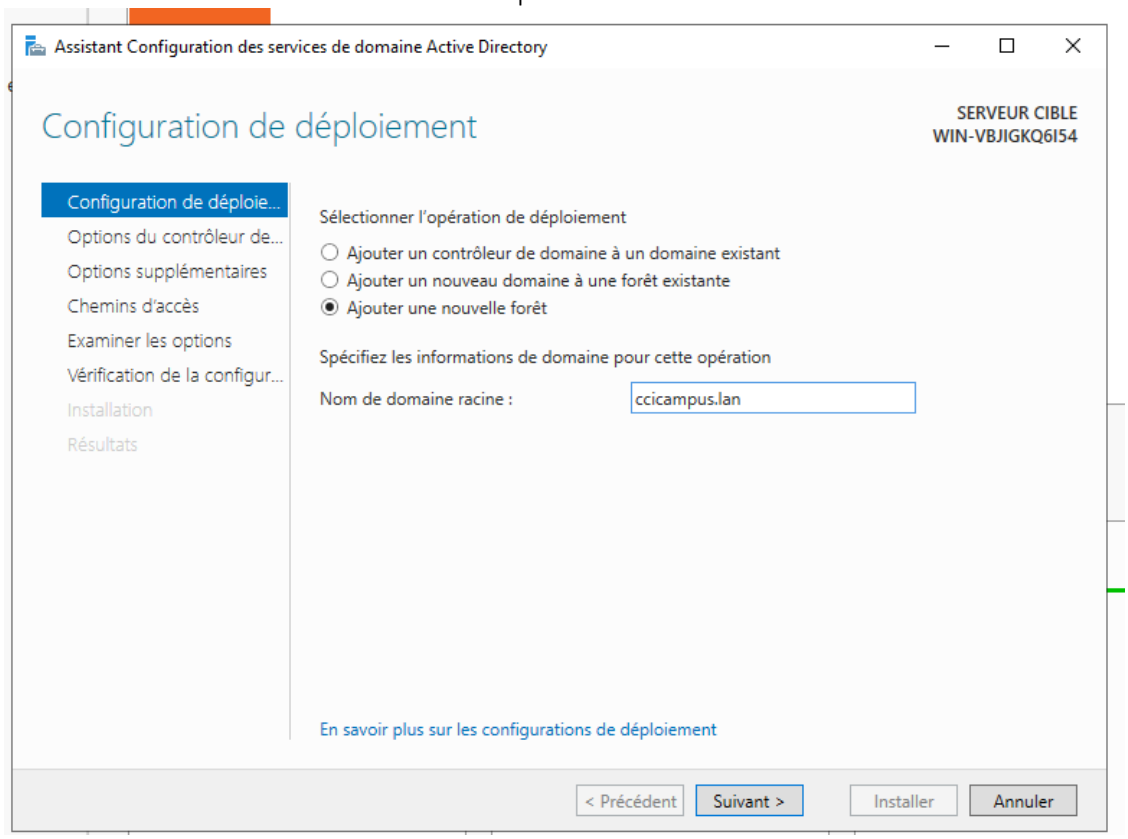
Lancer l'installation des rôles :



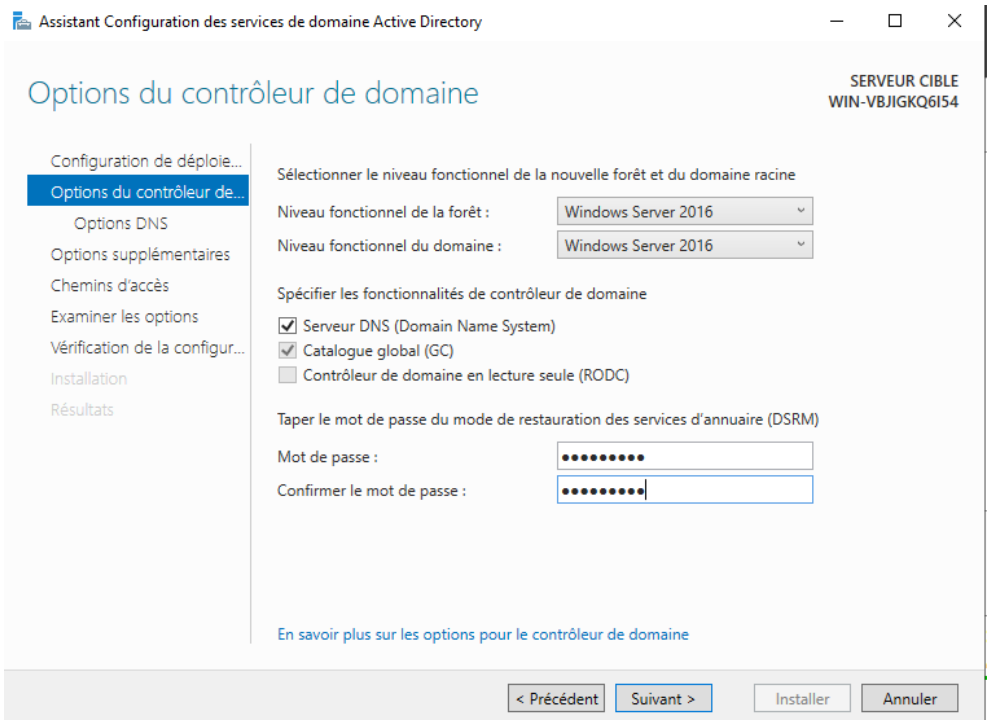
Ensuite, nous allons lancer la création de la forêt Active Directory en cliquant sur Promouvoir ce serveur en tant que contrôleur de domaine :



Nous allons définir le nom du domaine que nous voulons créer.



Nous allons également définir un mot de passe de restauration des services.

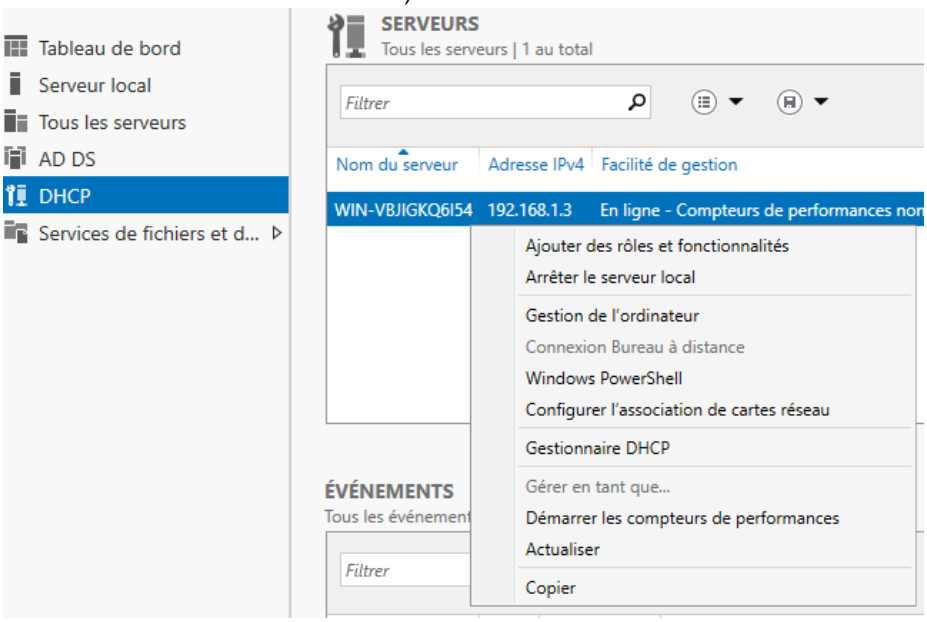


Une fois cela fait, l'AD sera complétement installé, prêt à l'usage.

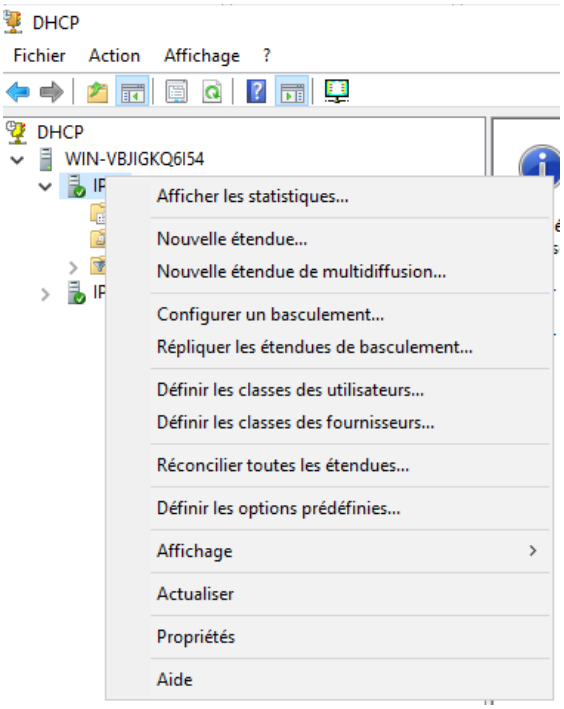
Configuration du rôle DHCP avec création d'une étendue de test

Pour compléter l'installation de DHCP, il suffira de se rendre dans le drapeau en haut à droite, cliquer sur Terminer la configuration DHCP. Il y aura juste à cliquer sur Suivant pour terminer la configuration.

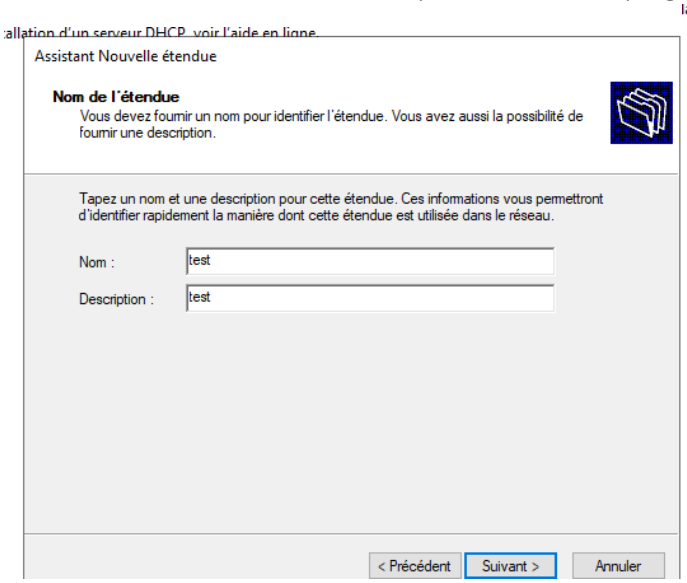
Pour la création d'un bail DHCP, il va falloir se rendre sur le Gestionnaire DHCP :

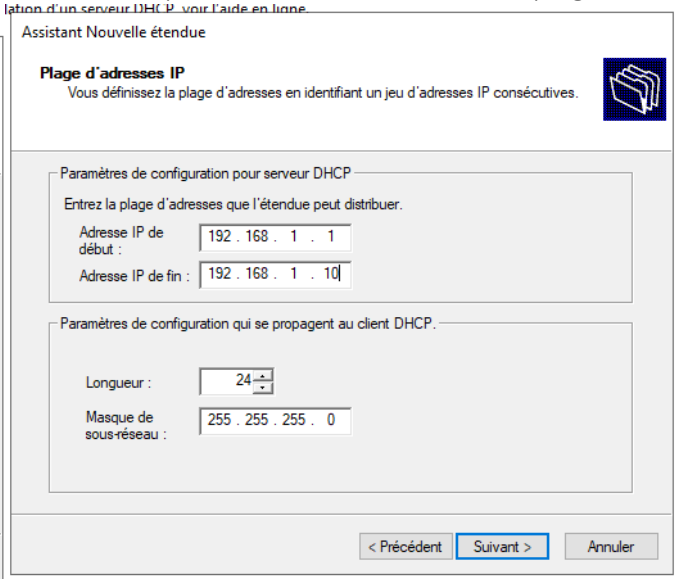


Une fois dessus, il faudra aller dans : *ServerName/IPv4* puis faire clic droit sur IPv4 pour créer une nouvelle étendue.

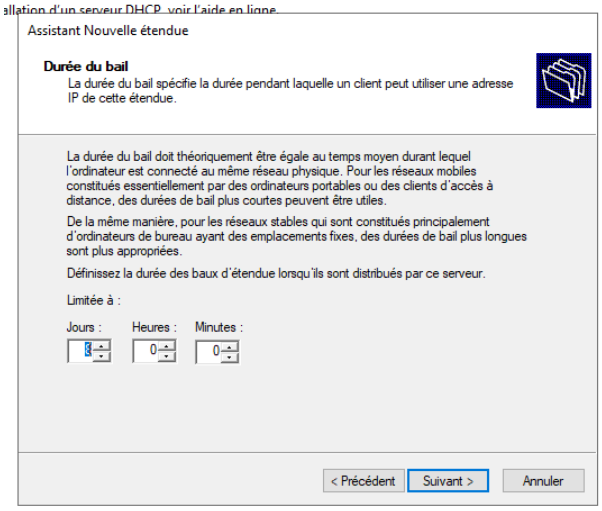


Nous allons ensuite la nommer, puis définir une plage d'adresse que l'on souhaite allouer à la plage.



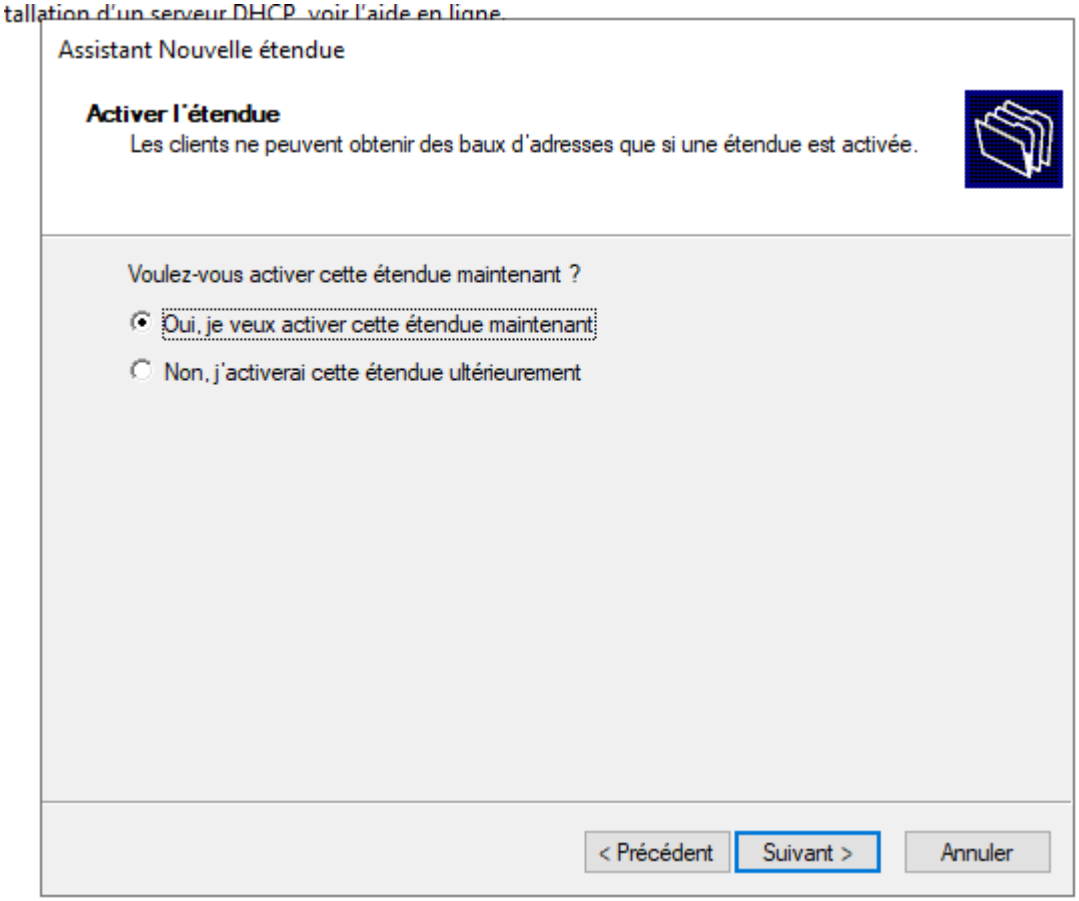


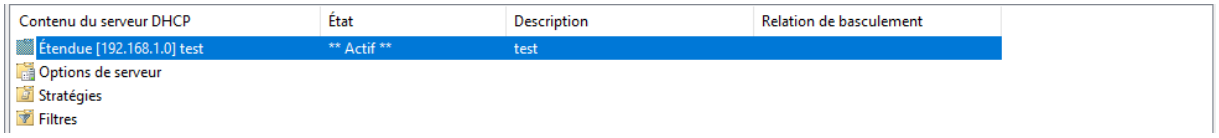
Il est également possible de modifier la durée du bail afin que les adresses utilisées puissent être reprises et ne restent pas bloqués pendant le temps par défaut (8 jours)



A la fin, il faudra alors activer l'étendue, et tout sera prêt à la connexion d'un potentiel client.

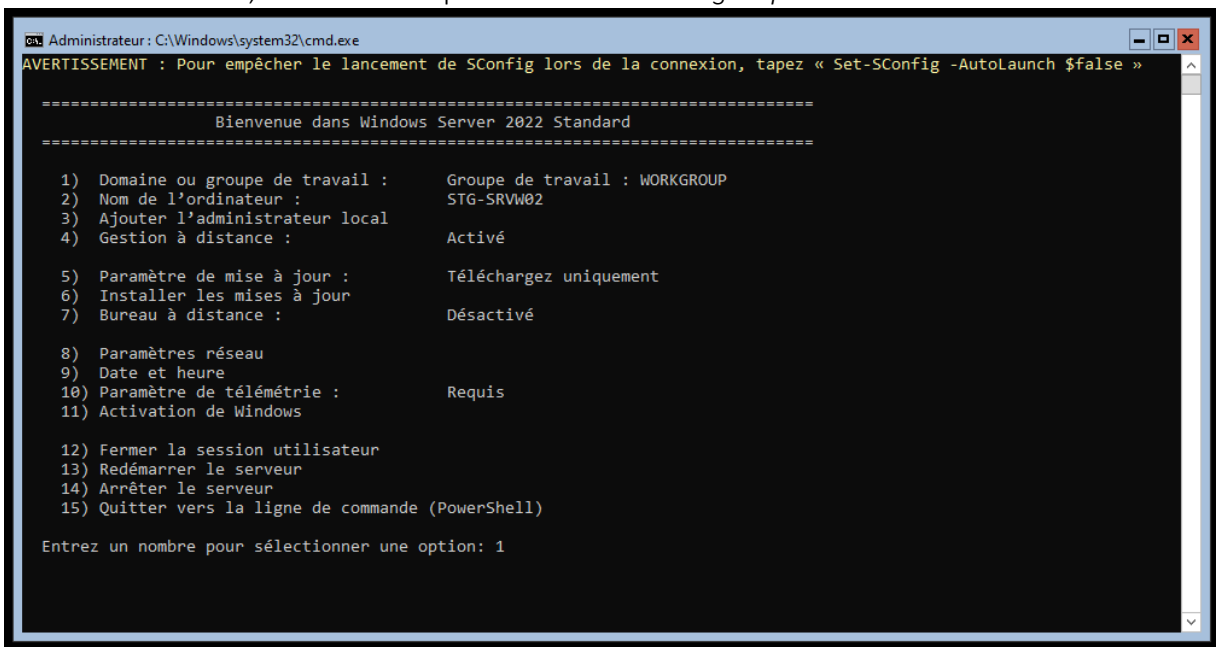
tallation d'un serveur DHCP, voir l'aide en ligne.



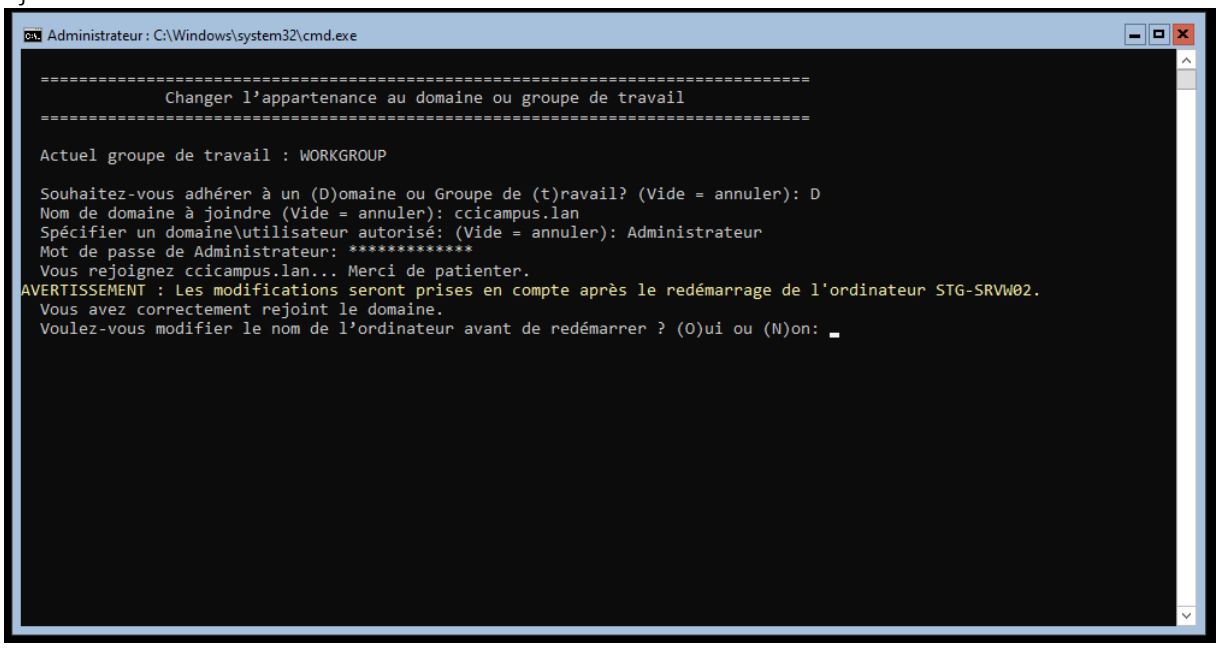


Étape 2 : Installation des rôles / fonctionnalités sur le serveur 2 :

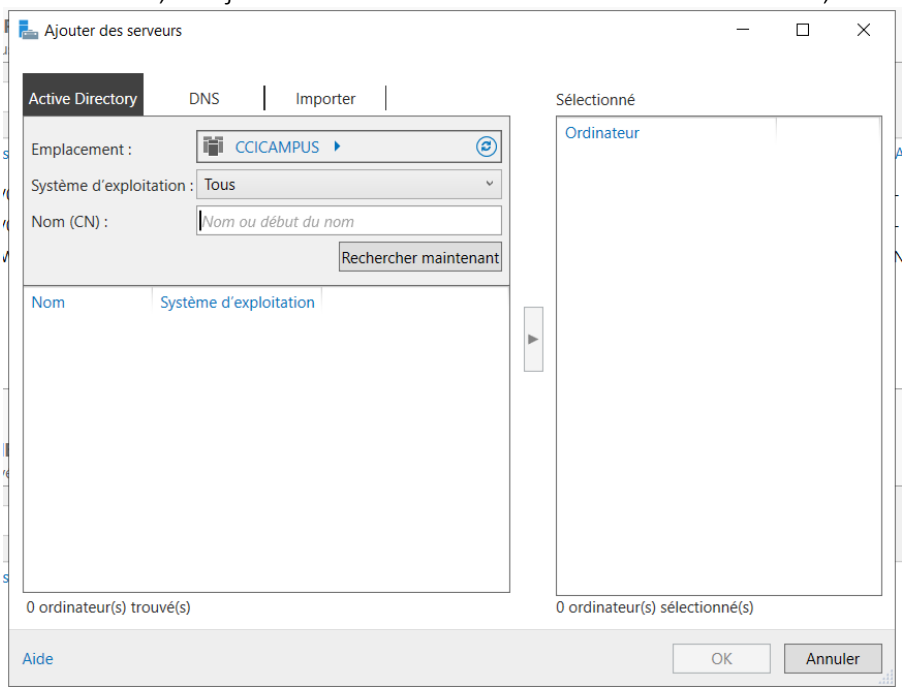
Sur le serveur Core, allons dans la partie 1 *Domaine ou groupe de travail*.



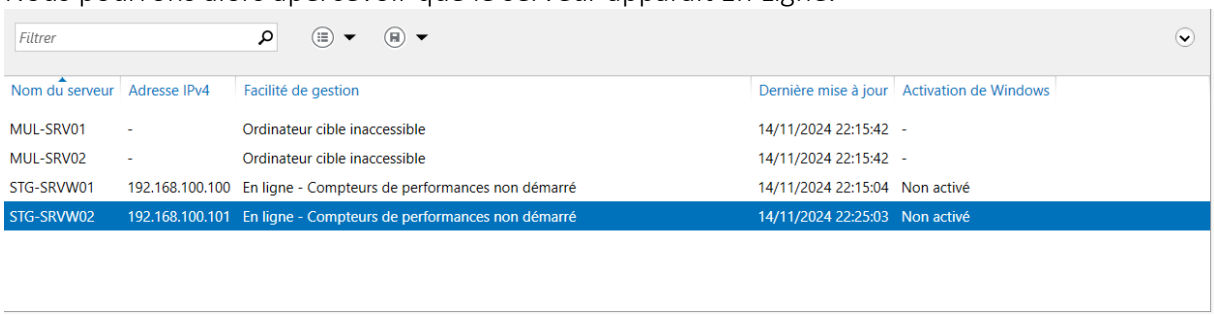
Une fois cela fait, il suffira de sélectionner Domaine, et rentrer le nom du domaine que l'on souhaite ajouter.



Une fois que le serveur sera dans le domaine, il sera possible de l'administrer depuis le serveur 1, pour cela, nous allons nous rendre dans la section Tous les serveurs du gestionnaire de serveur, puis faire Clic droit dessus, et Ajouter un serveur. Il suffira de rentrer son nom, le sélectionner et ce sera bon.

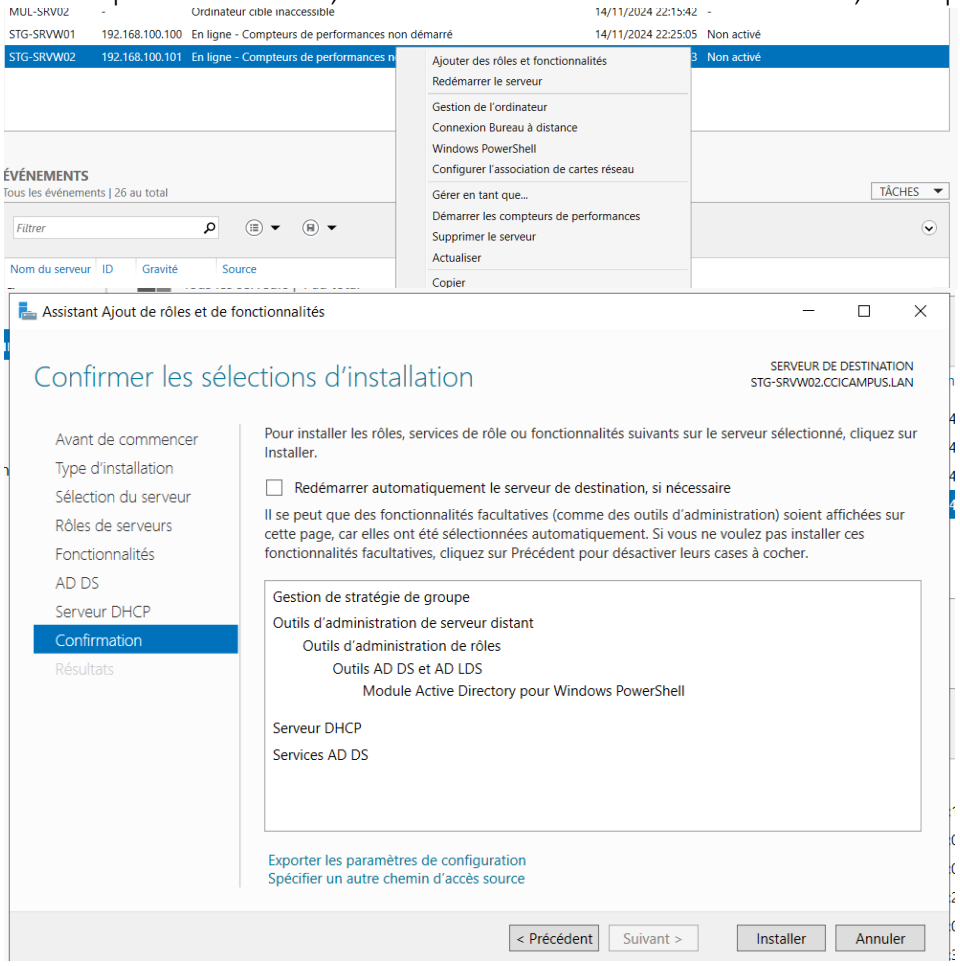


Nous pourrons alors apercevoir que le serveur apparaît En Ligne.



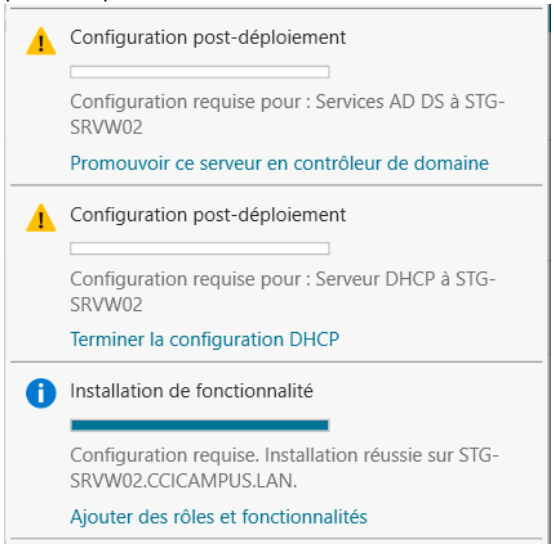
Installation des rôles AD DS et DHCP sur le second serveur.

Pour commencer, nous allons faire clic droit sur le serveur 2, puis ajouter des rôles ou des fonctionnalités. Comme pour le serveur 1, nous allons sélectionner les rôles AD DS, ainsi que DHCP.

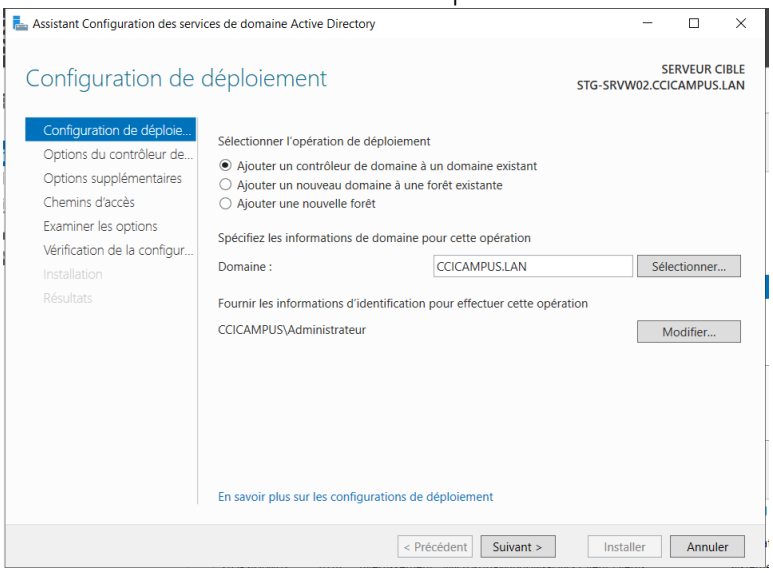


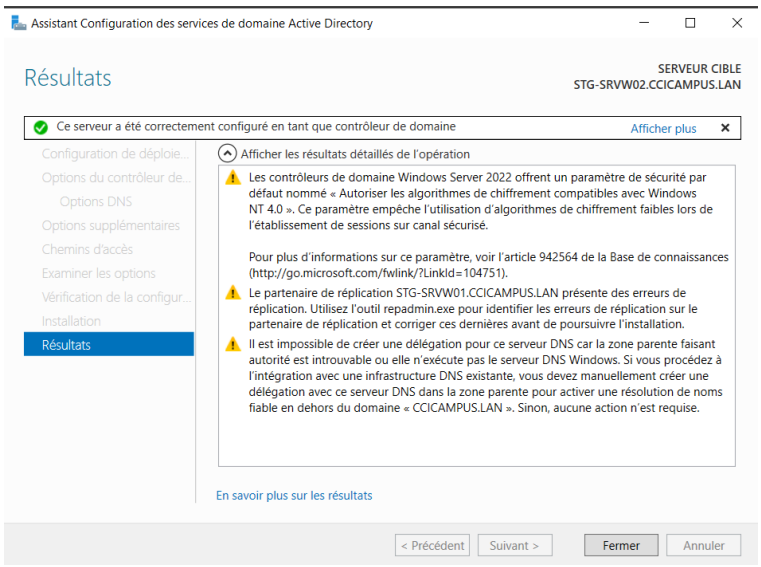
Concernant la configuration du DHCP, elle est identique à celle réalisée auparavant sur le premier serveur.

Pour la configuration de la réplication de l'AD, il faudra se rendre dans le petit drapeau d'information, puis cliquer sur Promouvoir ce serveur en tant que contrôleur de domaine.



Une fois cela fait, nous allons rentrer le domaine déjà existant ici, il faudra également rentrer les informations de connexion du compte Administrateur du domaine.

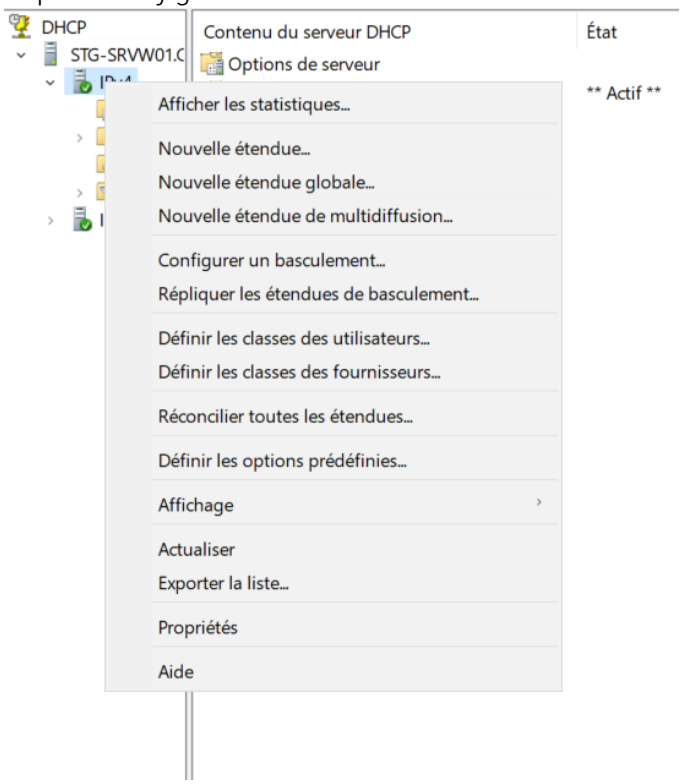




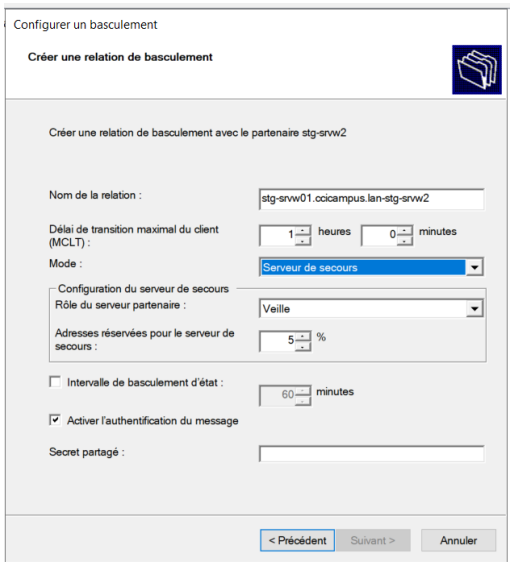
Cette étape nous montre que le serveur est désormais bien contrôleur de domaine secondaire du domaine CCICAMPUS.LAN.

Configuration du basculement DHCP

Nous allons nous rendre sur le gestionnaire DHCP du premier serveur, puis clic droit sur IPv4 pour afficher l'option *Configurer un basculement*.



Une fois dans l'interface, nous allons rentrer les informations du serveur 2 pour définir qui va gérer le basculement, et comment.



1.3) LOT 3 : Installation du rôle DFS, DFSR et mise en place de l'espace de nom

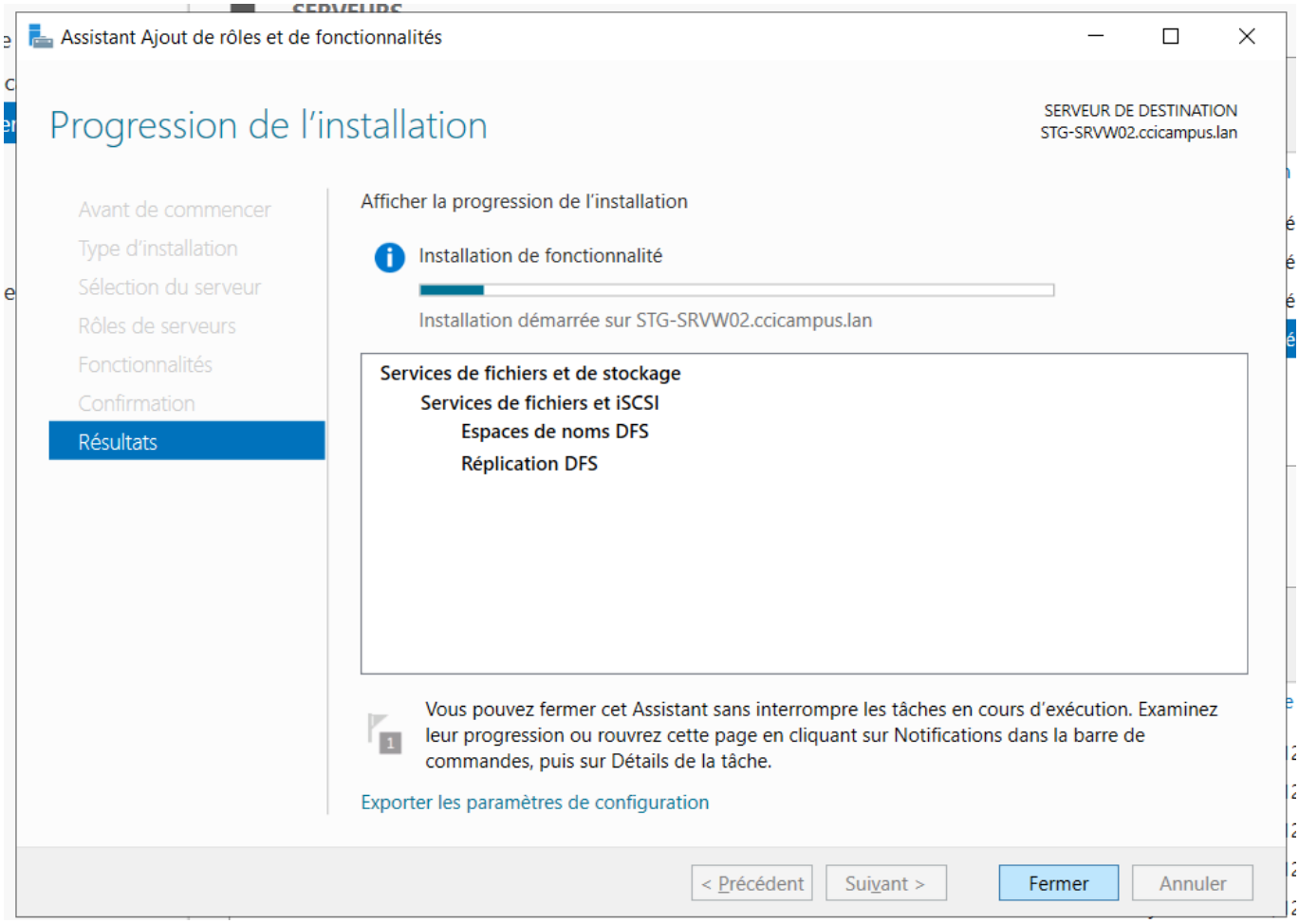
Installation d'un serveur Windows SERVER 2022 avec les services DFS et DFSR

Prérequis :

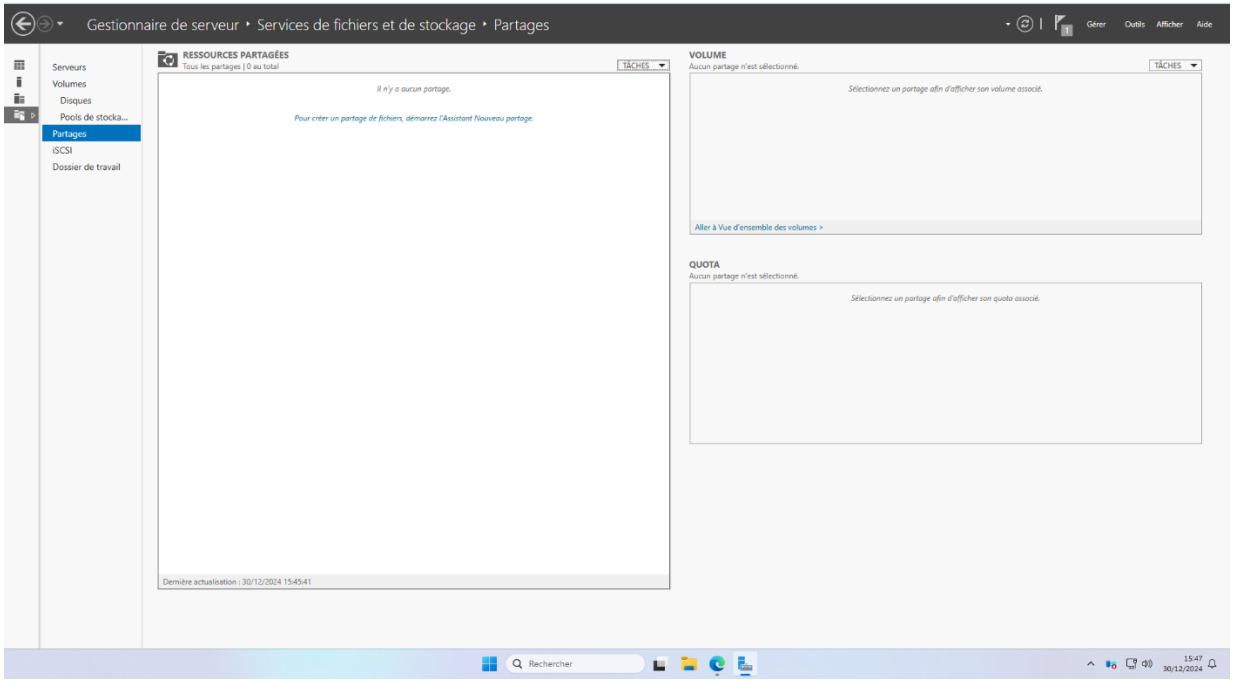
- 1 Windows SERVER 2022 avec interface graphique
- 1 serveur d'annuaire d'authentification (dans ce cas, active directory) avec un domaine (optionnel)

Joignez un domaine ou créez un domaine avec les services Active Directory (il est possible d'utiliser DFS de manière autonome hors domaine, or son utilisation sera alors limitée)

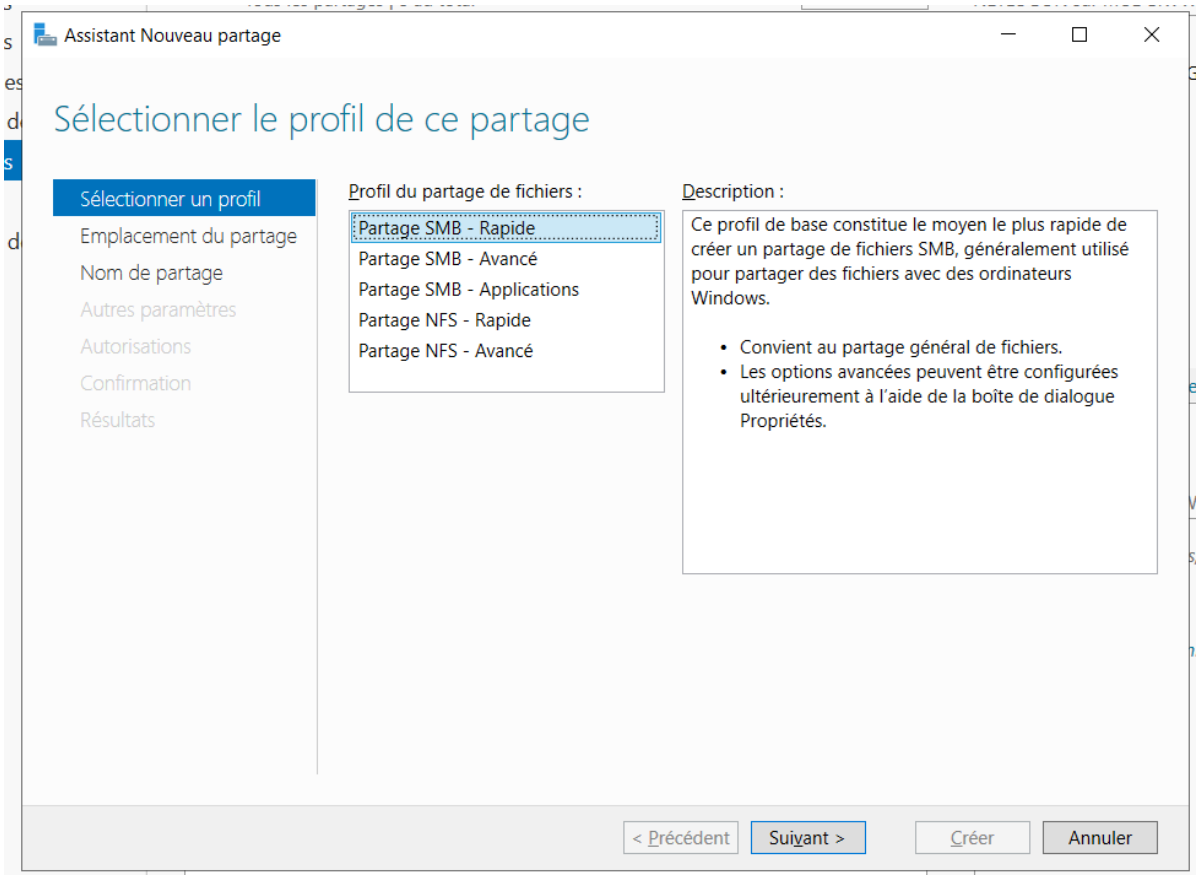
Ajoutez le rôle DFS et Réplication DFS au serveur



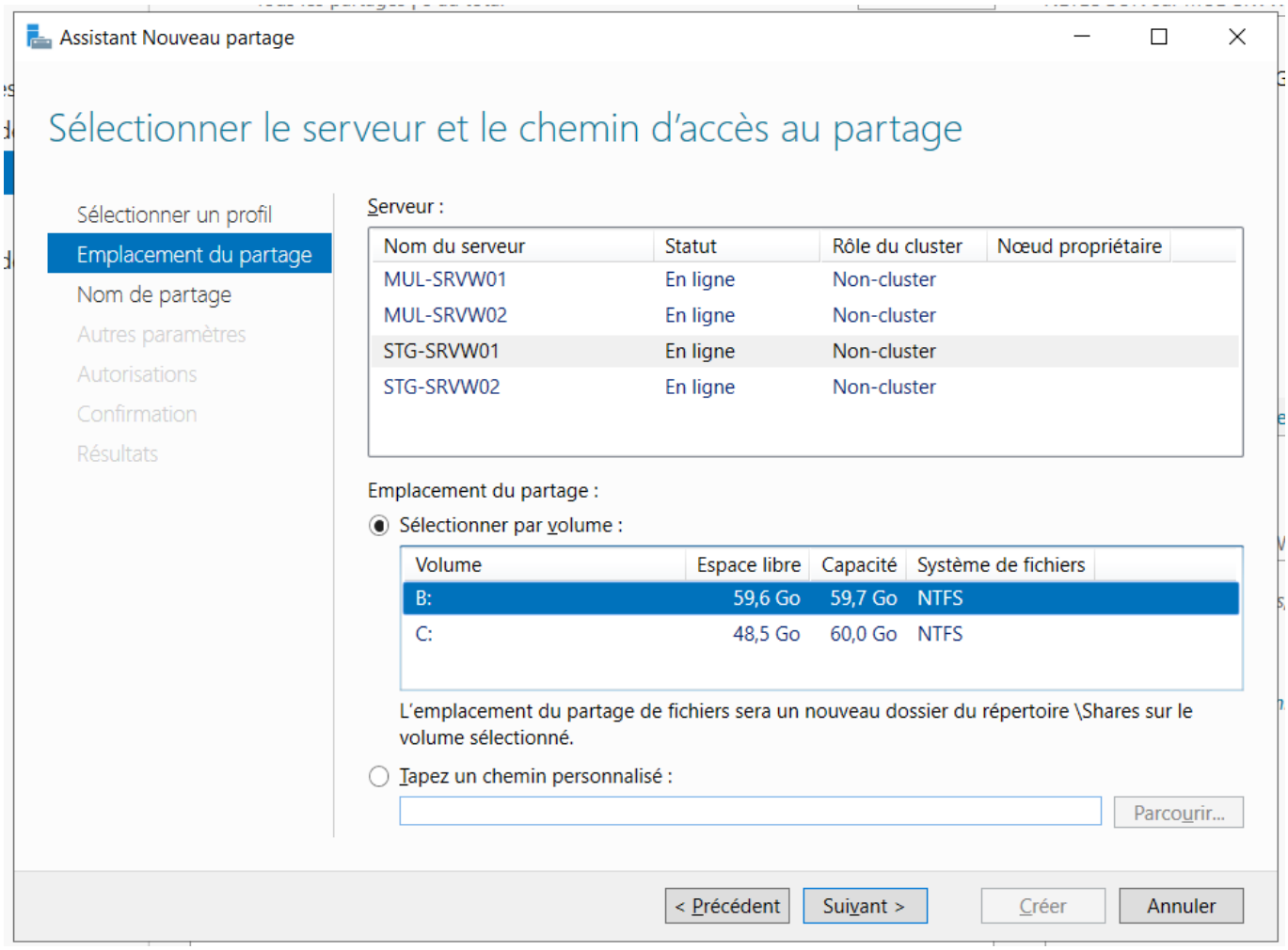
Une fois la fonctionnalité installée, nous allons créer des partages sur les disques des futures cibles DFS. Pour ce faire, nous allons nous rendre dans l'onglet Services de fichier et de stockage, dans le sous onglet « Partages », puis nous allons créer un nouveau partage :



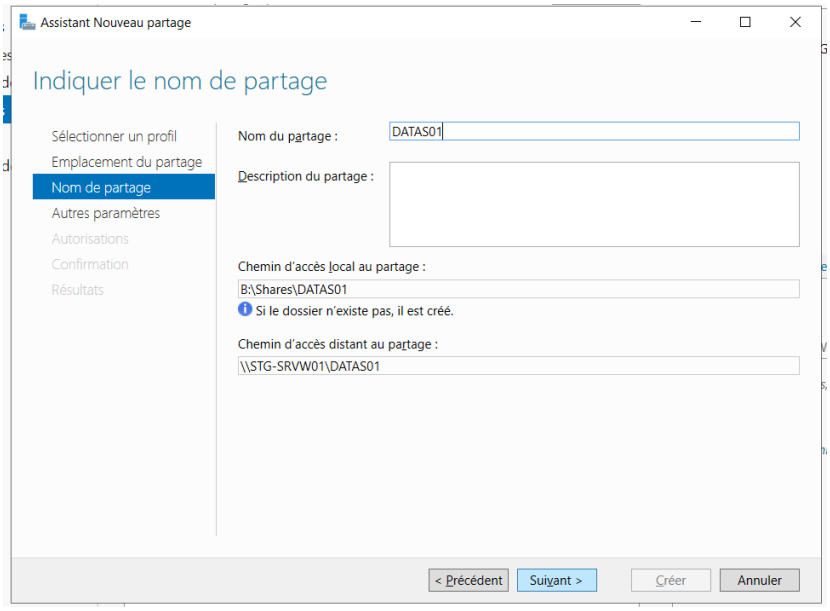
Une fois dedans, nous allons créer un partage SMB Rapide.



Nous allons ensuite choisir le serveur sur lequel nous voulons créer le partage, nous pourrons également choisir son emplacement.

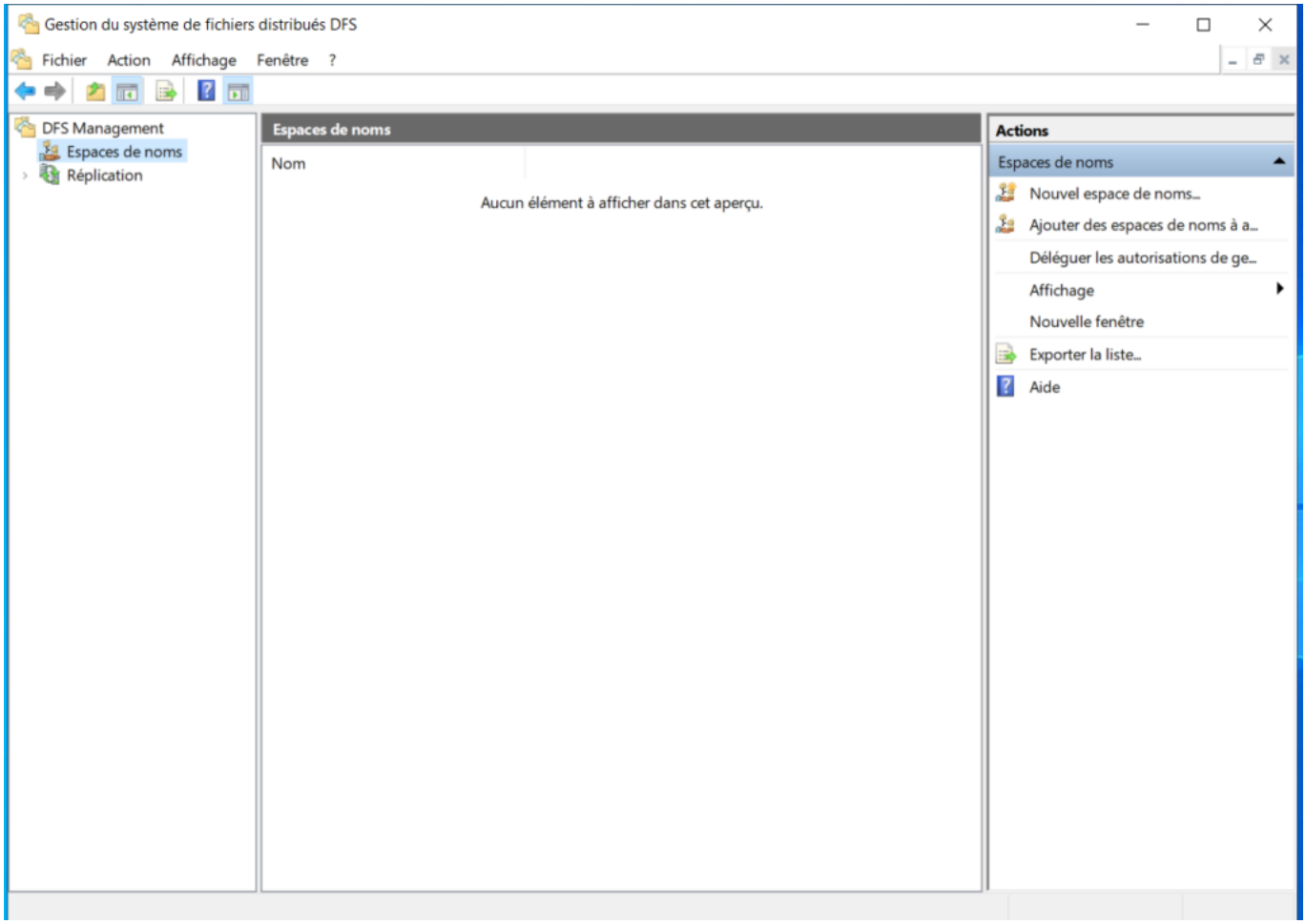


Nous allons également devoir lui donner un nom, afin de pouvoir le retrouver correctement :

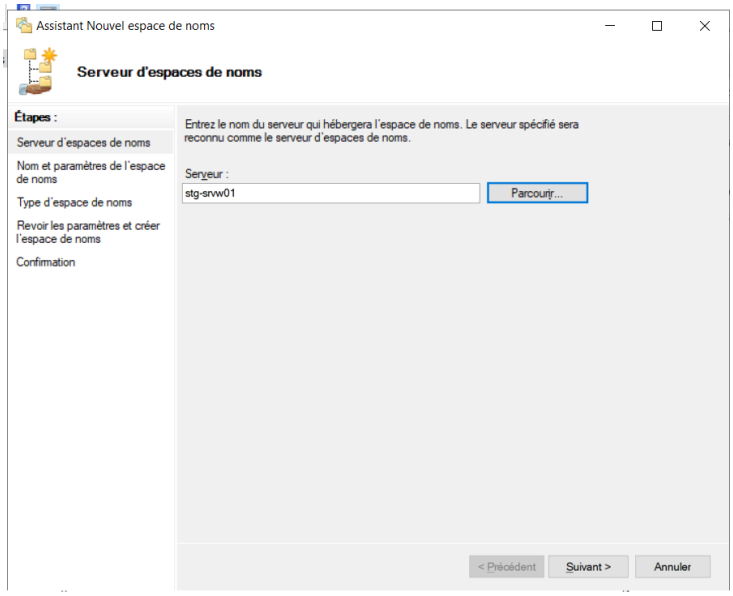


Une fois le partage créé, nous allons mettre en place l'espace de nom.

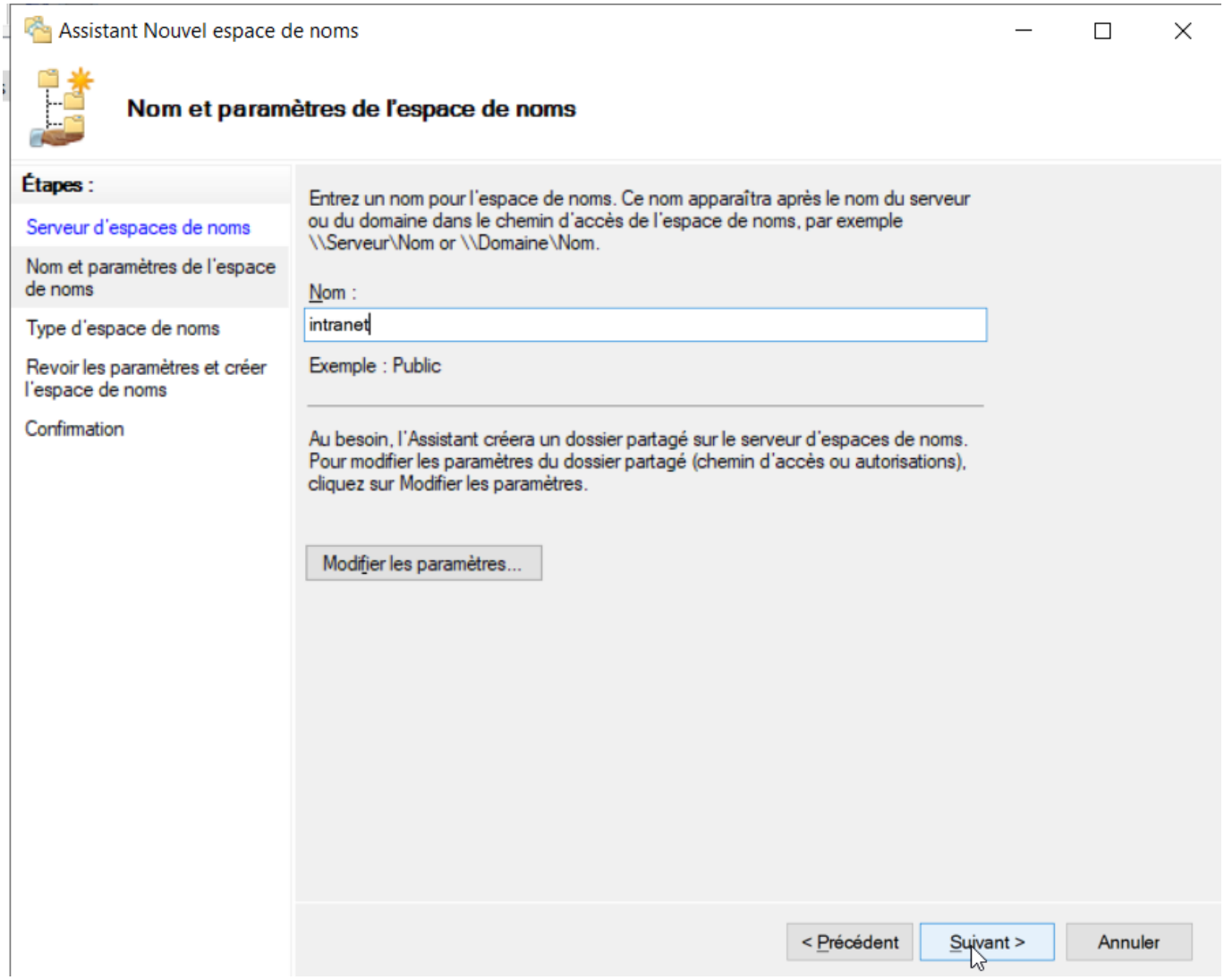
Rentrez dans la console DFS pour créer l'espace de nom



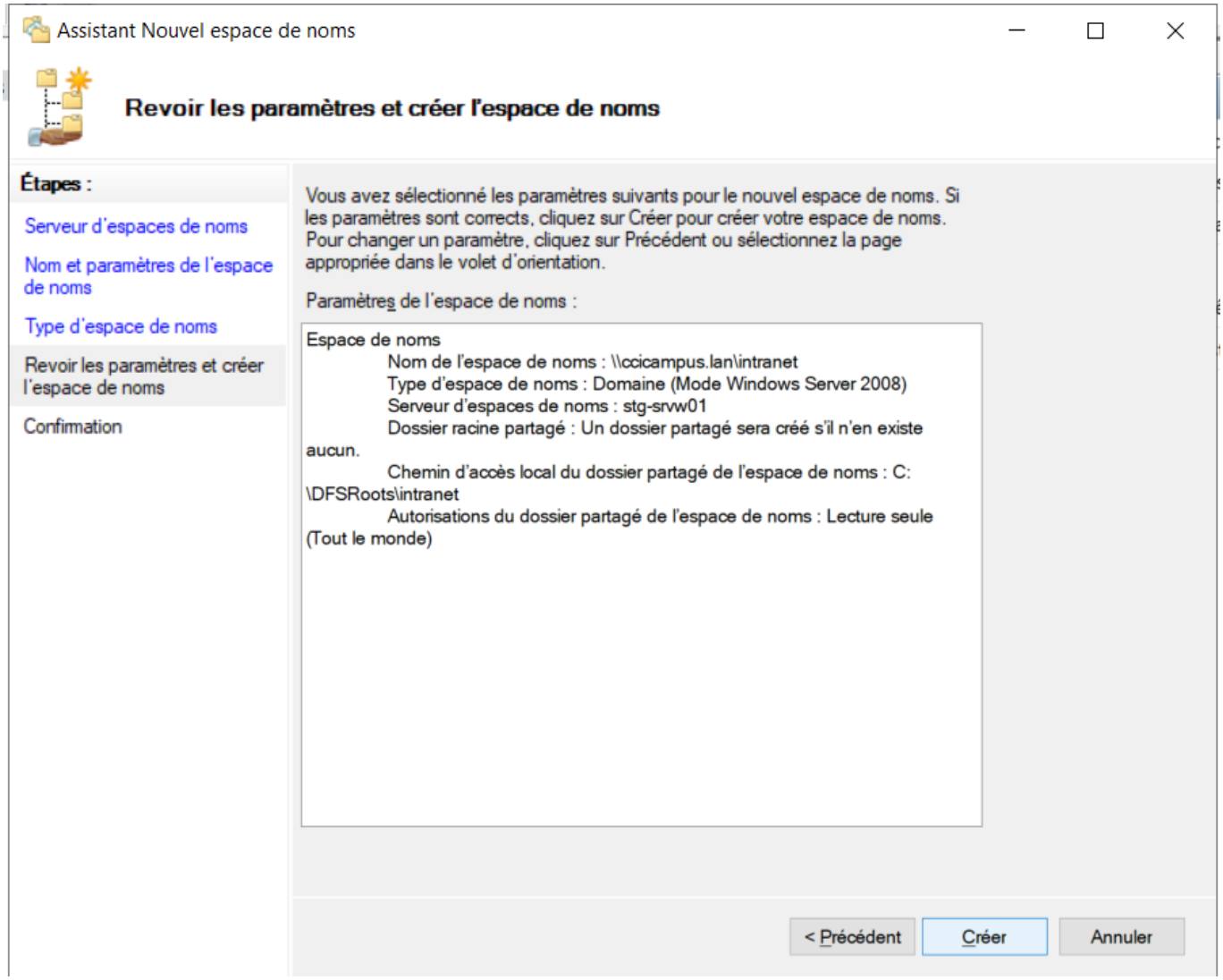
Une fois dedans, créez l'espace de nom avec les paramètres que vous désirez



Nous allons pour commencer choisir le serveur cible principal. Nous allons également lui donner un nom.

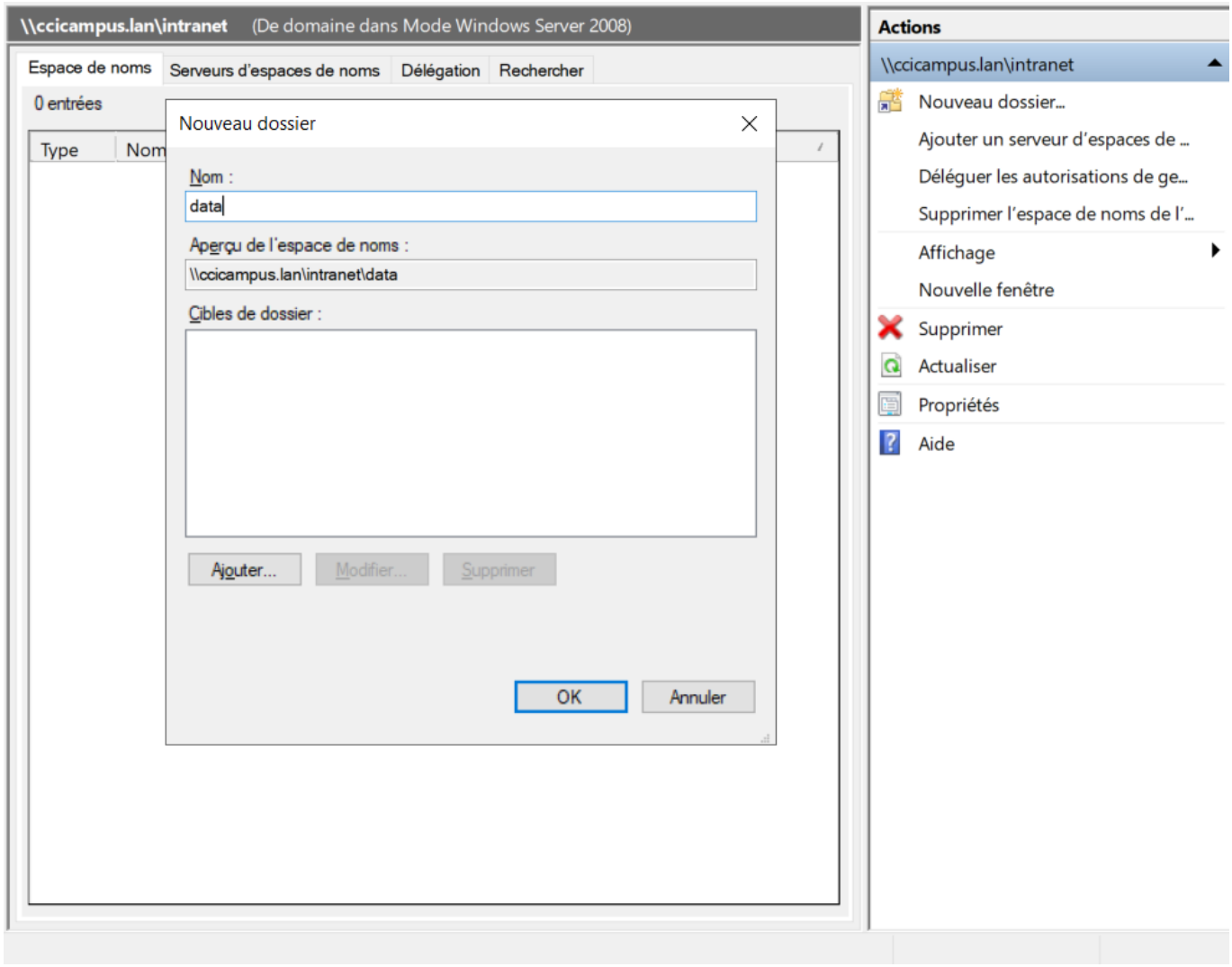


Une fois cela fait, l'espace de nom sera créé

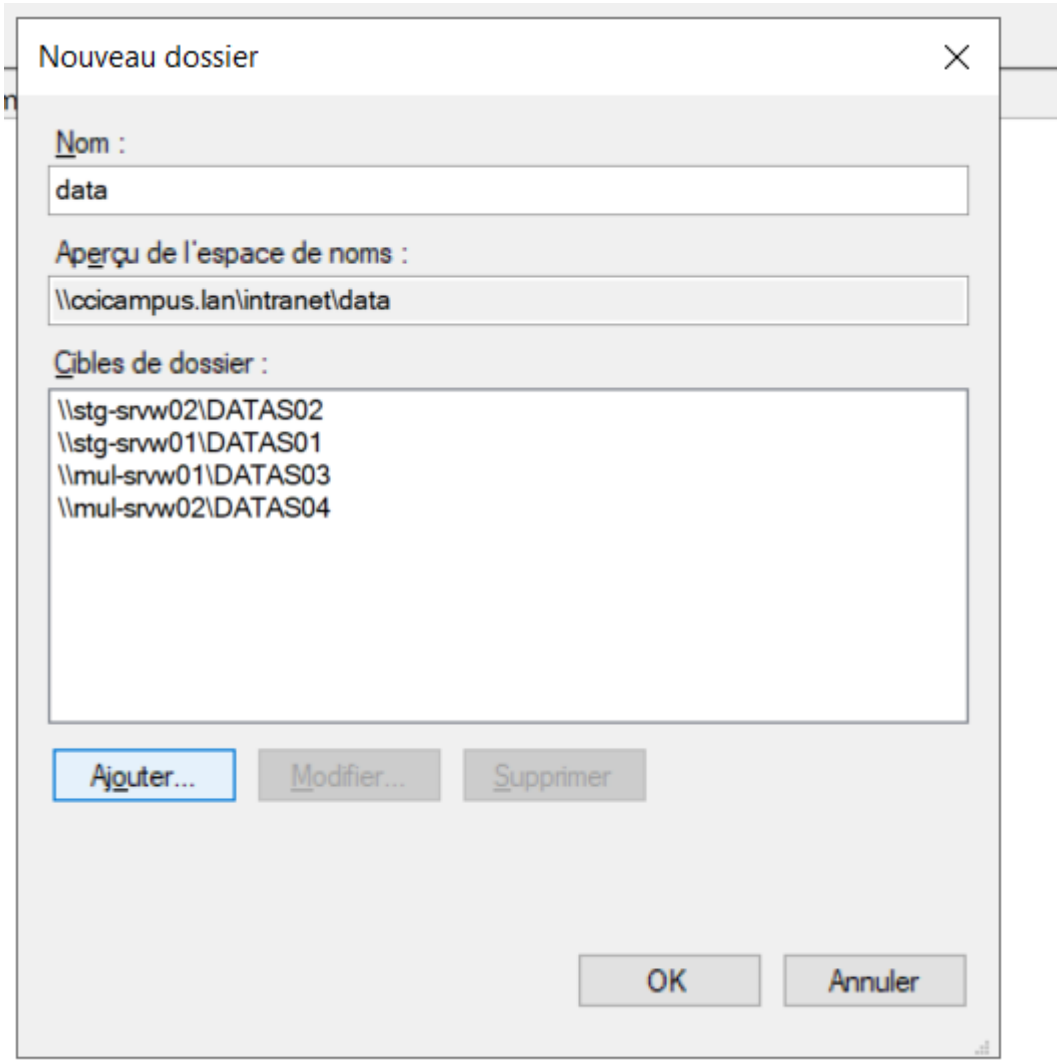


Création du dossier de l'espace de nom DFS :

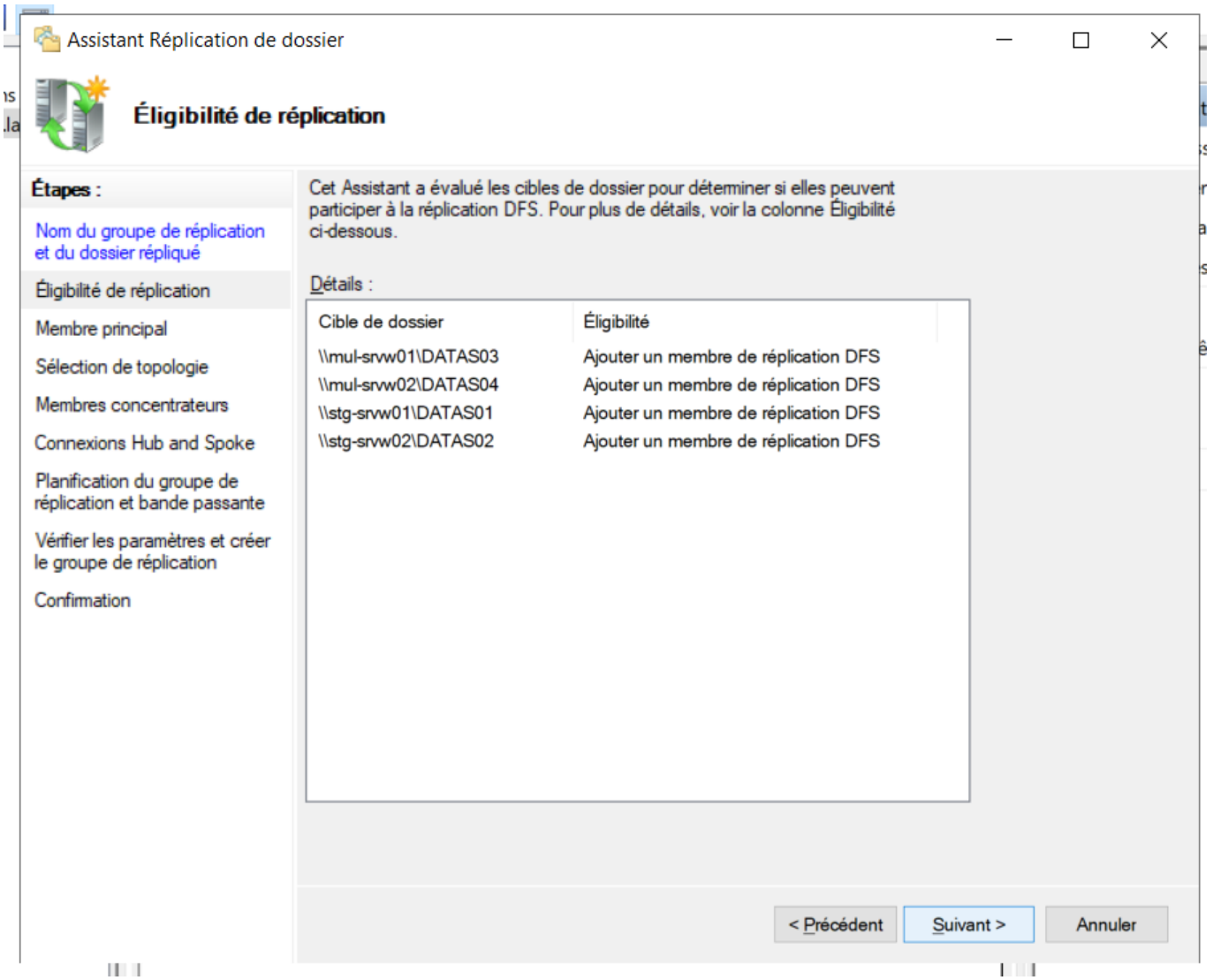
Ensuite nous allons créer un dossier, permettant le stockage de ce que l'on veut dans l'espace de nom.



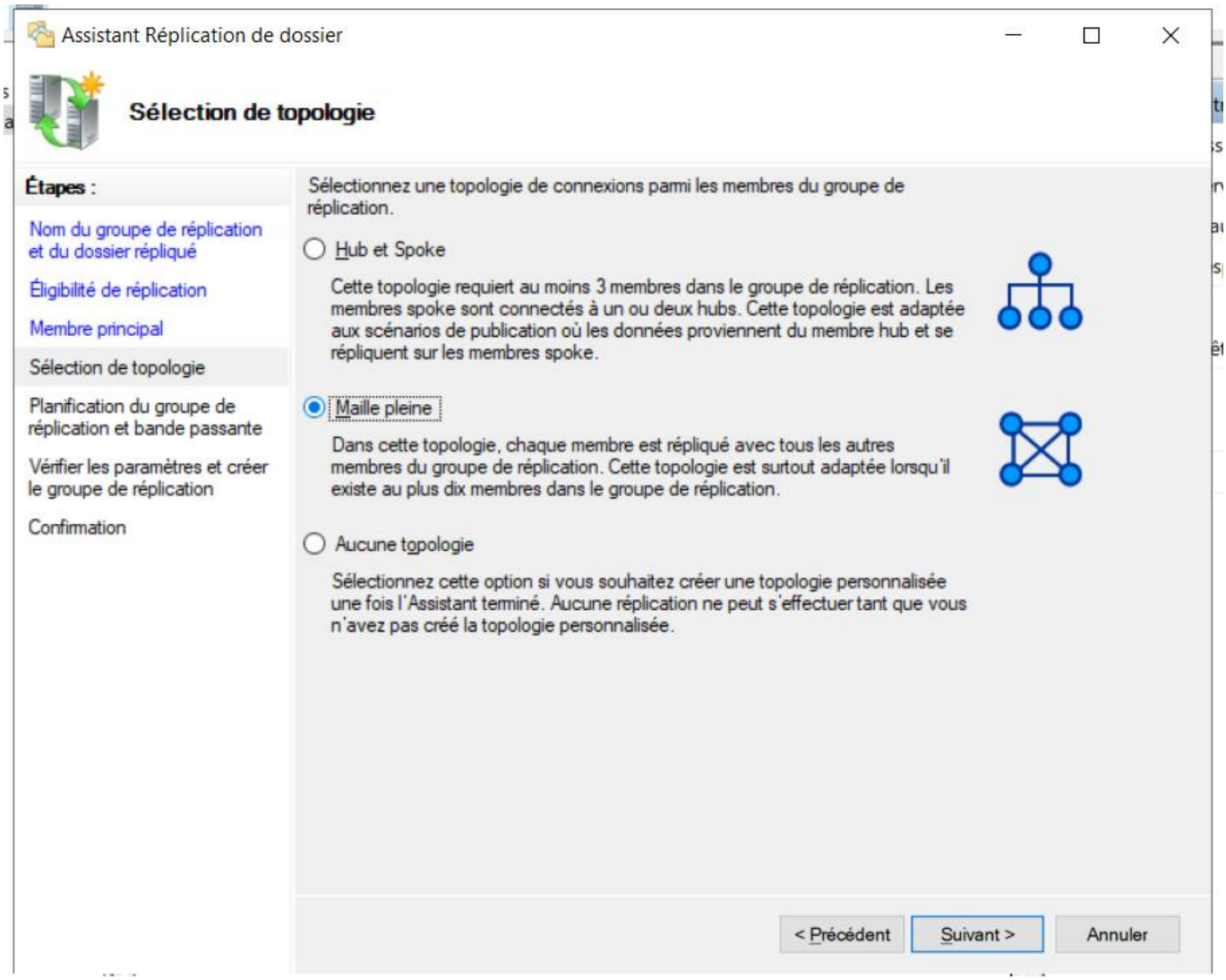
Dans cette prochaine étape, nous allons pouvoir ajouter des cibles (d'autres serveurs) afin d'avoir une haute disponibilité. Dans mon cas j'ajoute alors mes 4 serveurs :



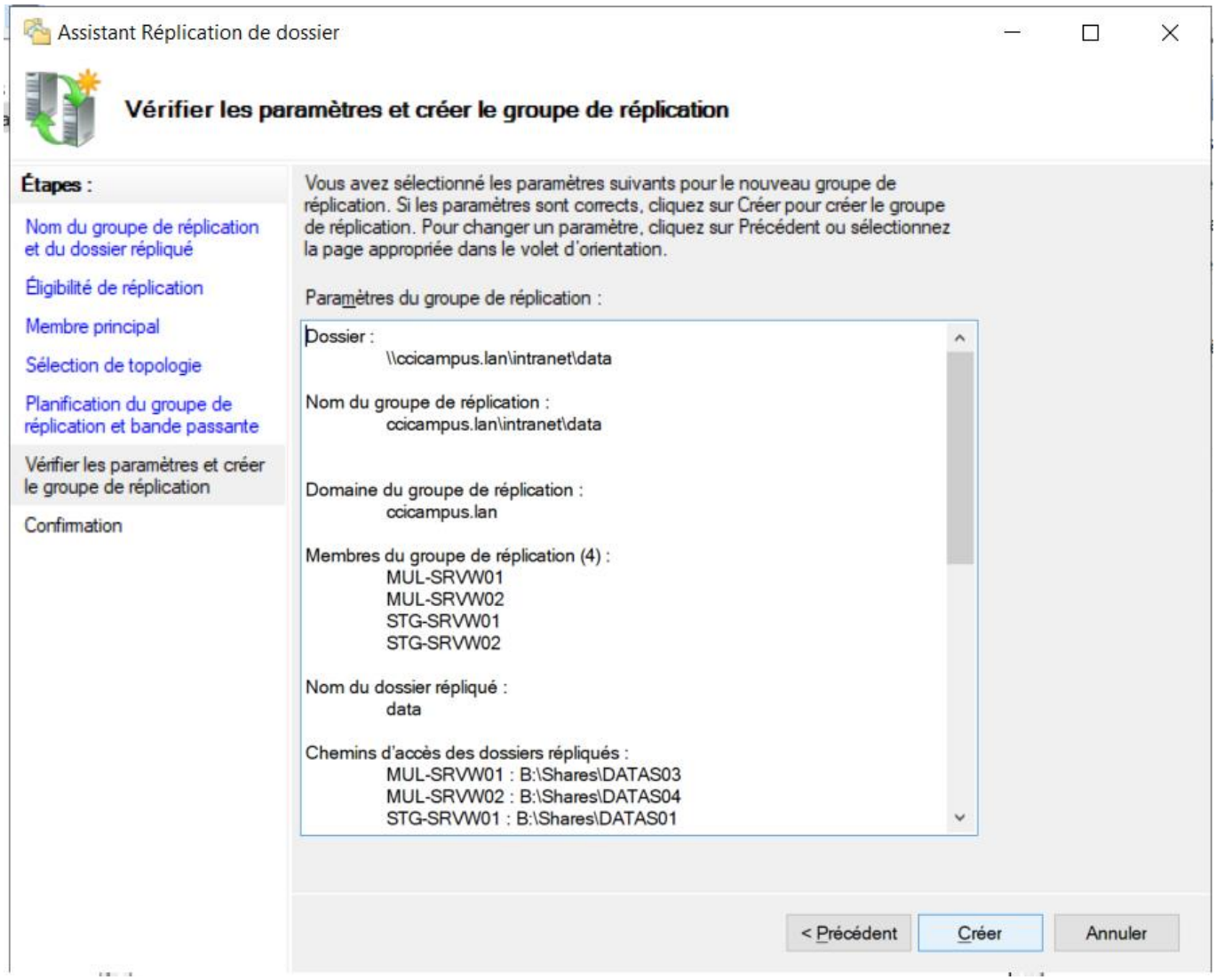
Nous allons alors ajouter les serveurs que l'on veut ajouter comme cible DFS (facultatif)


Assistant Réplication de dossier
Éligibilité de réplication
Étapes :
Nom du groupe de réplication et du dossier répliqué
Éligibilité de réplication
Membre principal
Sélection de topologie
Membres concentrateurs
Connexions Hub and Spoke
Planification du groupe de réplication et bande passante
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Cet Assistant a évalué les cibles de dossier pour déterminer si elles peuvent participer à la réplication DFS. Pour plus de détails, voir la colonne Éligibilité ci-dessous.
Détails :
Cible de dossier
Éligibilité
\\mul-srvw01\DATAS03
Ajouter un membre de réplication DFS
\\mul-srvw02\DATAS04
Ajouter un membre de réplication DFS
\\stg-srvw01\DATAS01
Ajouter un membre de réplication DFS
\\stg-srvw02\DATAS02
Ajouter un membre de réplication DFS
< Précédent
Suivant >
Annuler

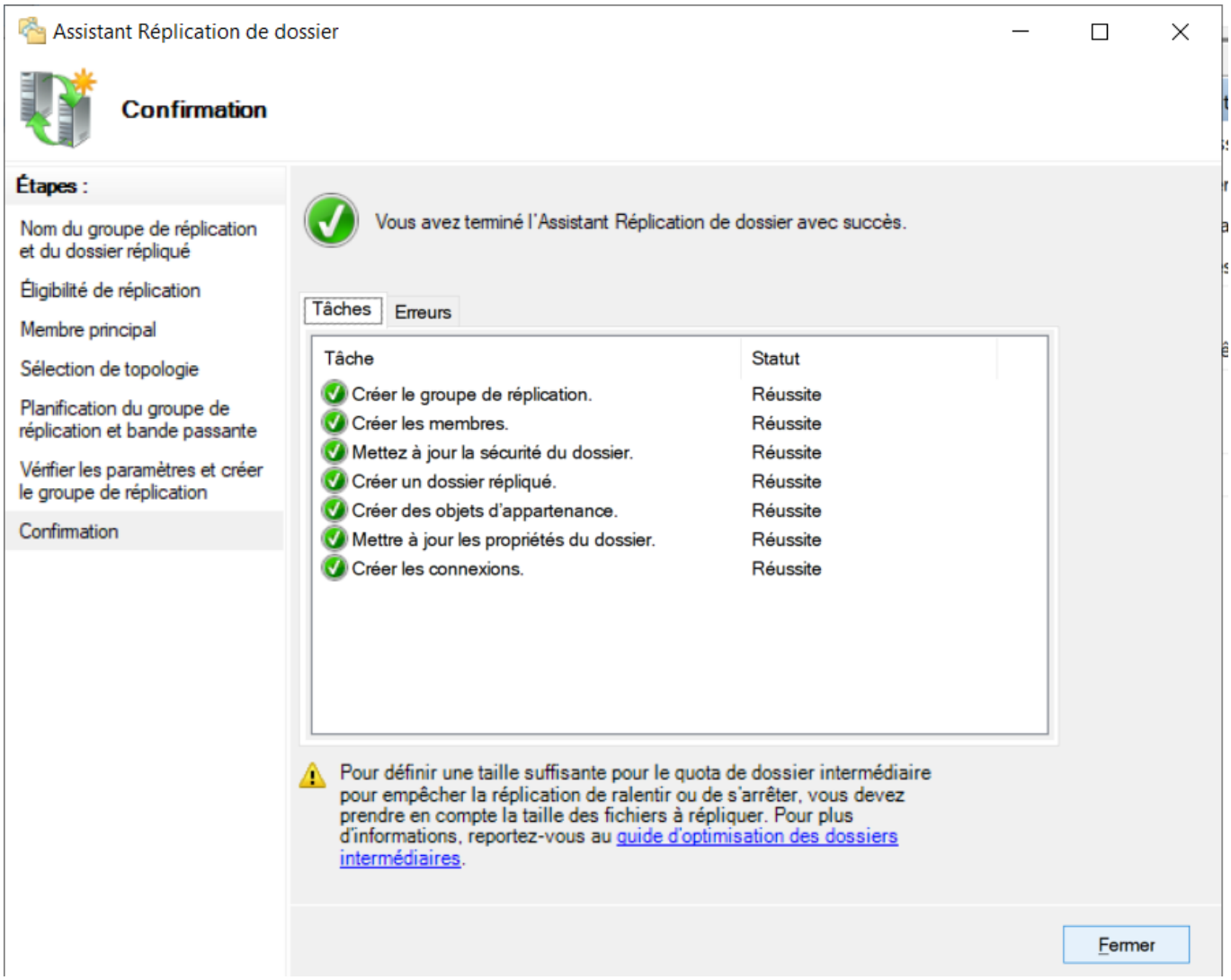
Nous allons choisir la typologie Maille pleine afin de permettre la réplication sur tous les serveurs en temps réel en utilisant la bande passante.



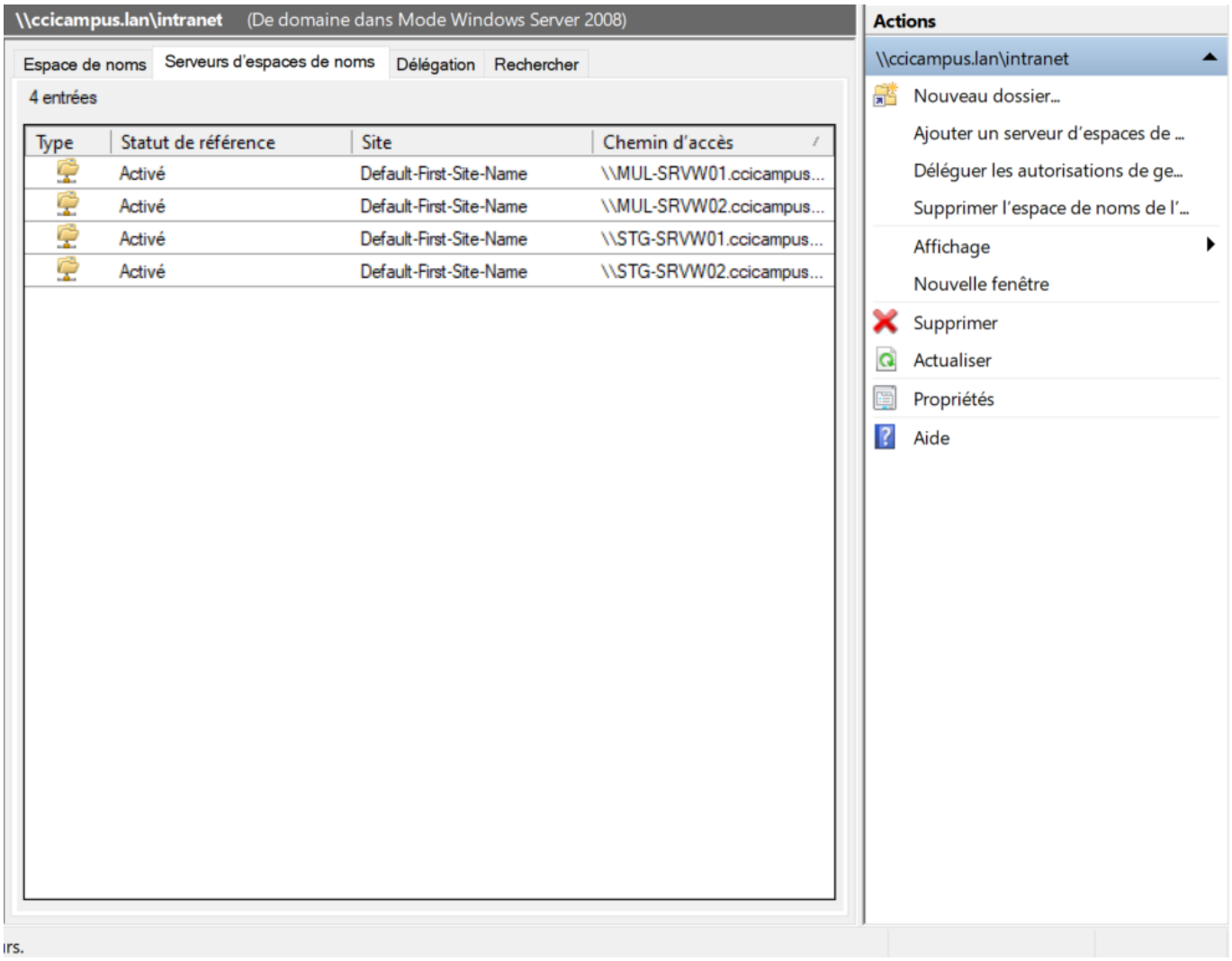
A la fin de cette étape, nous allons pouvoir voir le détail et les chemins sur lesquels seront répliqués l'espace de nom DFS



L'espace de nom est alors prêt à l'emploi, et est répliqué sur tous les serveurs.

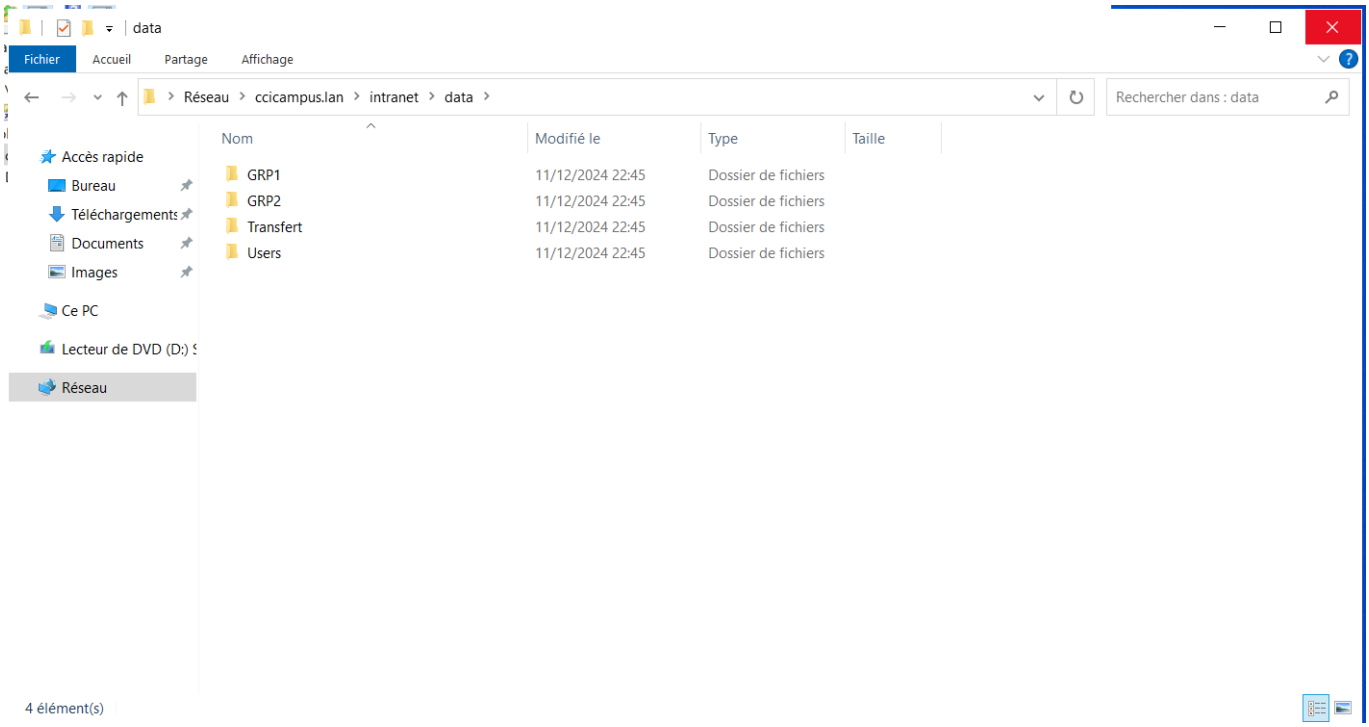

Assistant Réplication de dossier
Confirmation
Étapes :
Nom du groupe de réplication et du dossier répliqué
Éligibilité de réplication
Membre principal
Sélection de topologie
Planification du groupe de réplication et bande passante
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Vous avez terminé l'Assistant Réplication de dossier avec succès.
Tâches
Erreurs
Tâche
Statut
Créer le groupe de réplication.
Réussite
Créer les membres.
Réussite
Mettez à jour la sécurité du dossier.
Réussite
Créer un dossier répliqué.
Réussite
Créer des objets d'appartenance.
Réussite
Mettre à jour les propriétés du dossier.
Réussite
Créer les connexions.
Réussite
Pour définir une taille suffisante pour le quota de dossier intermédiaire pour empêcher la réplication de ralentir ou de s'arrêter, vous devez prendre en compte la taille des fichiers à répliquer. Pour plus d'informations, reportez-vous au guide d'optimisation des dossiers intermédiaires.
Fermer

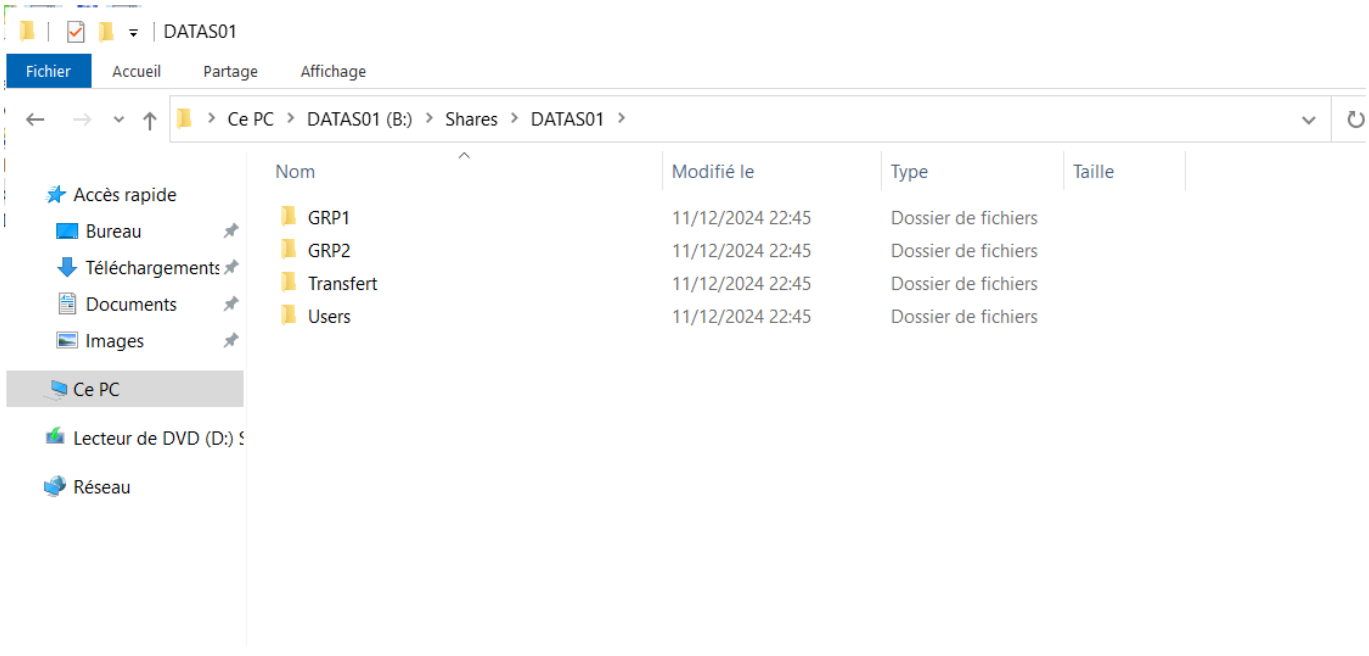
Dans la console DFS, sous espace de nom, nous pouvons vérifier alors les différentes cibles dans la partie Serveurs d'espace de nom



Note : **DFS** utilise plusieurs protocoles pour garantir son bon fonctionnement. SMB (Server Message Block) est utilisé pour accéder aux fichiers partagés, tandis que RPC (Remote Procedure Call) facilite la gestion à distance des configurations. Dans un domaine Active Directory, LDAP permet de localiser les ressources des espaces de noms. Pour la réplication, DFSR utilise RDC (Remote Differential Compression) afin d'optimiser les transferts en synchronisant uniquement les modifications. Enfin, les accès sont sécurisés grâce aux protocoles d'authentification Kerberos ou NTLM. Il faudra alors bien ouvrir les ports en cas de mise en place d'un VPN site à site.

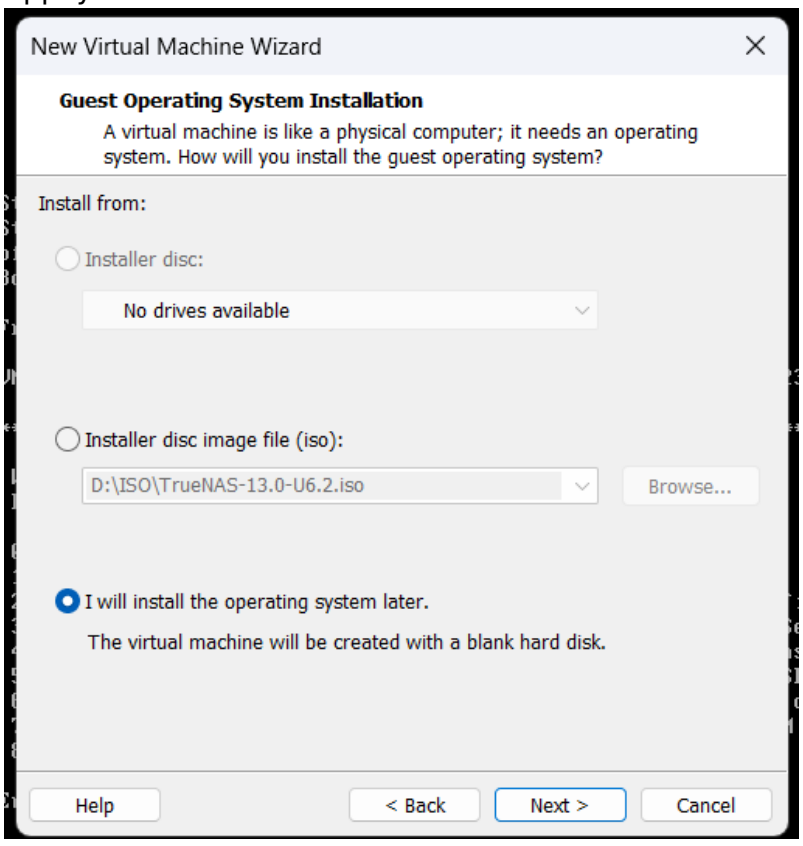
Une fois tout cela fini, nous verrons que l'espace de nom sera accessible, et que si l'on ajoute des dossiers ou des fichiers dedans, tout se répliquera sur les différents partages des cibles que l'on a créés auparavant.



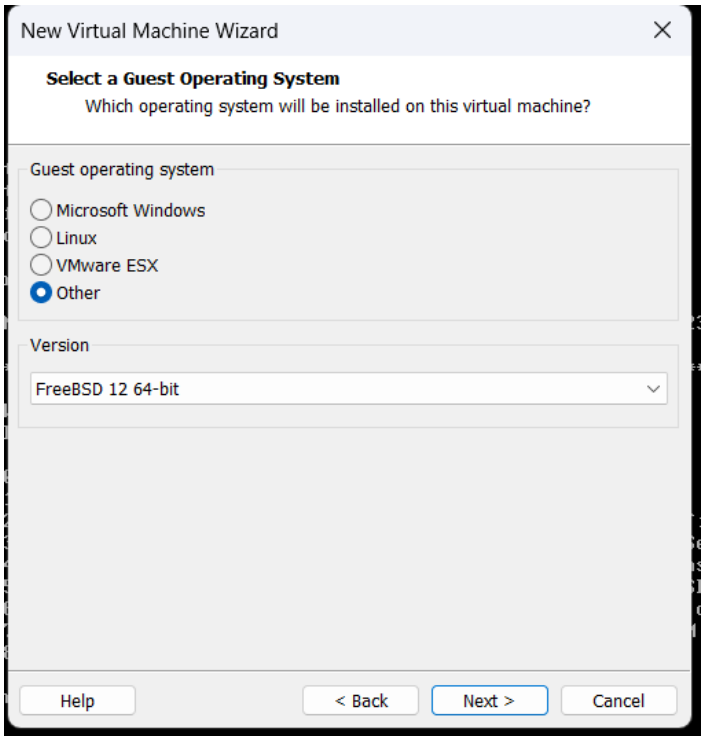


1.4) LOT 4 : Installation de TrueNAS et montage d'une cible iSCSi

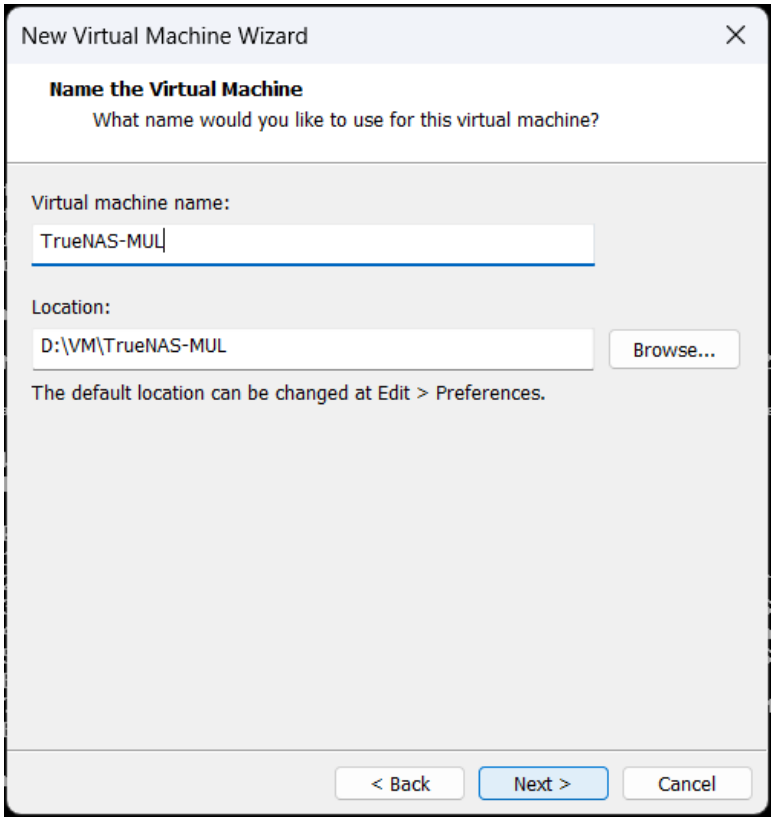
Appuyiez sur next



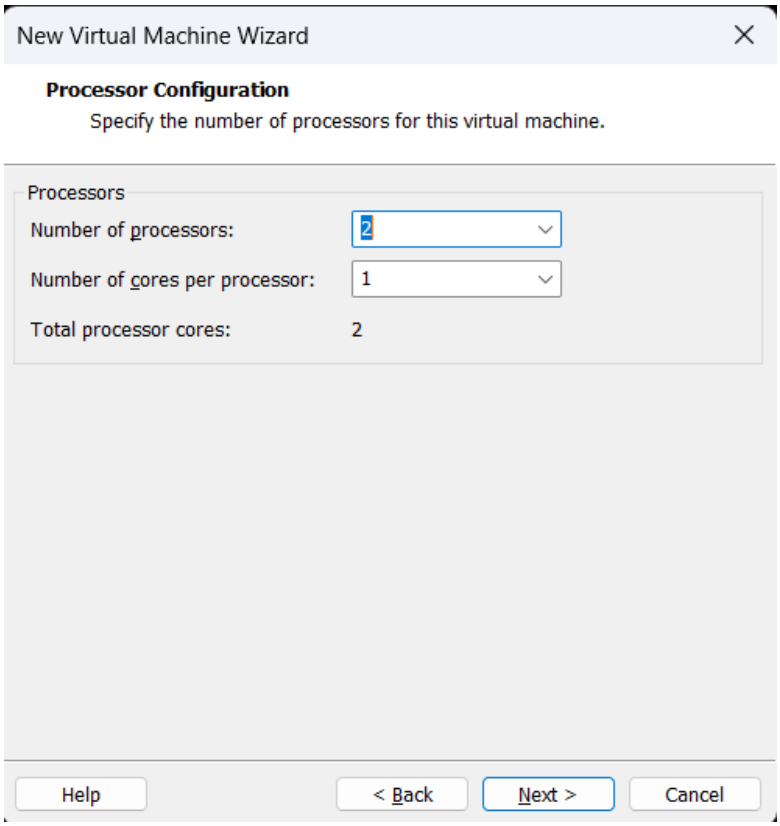
Cochez "I will install the operating system later".



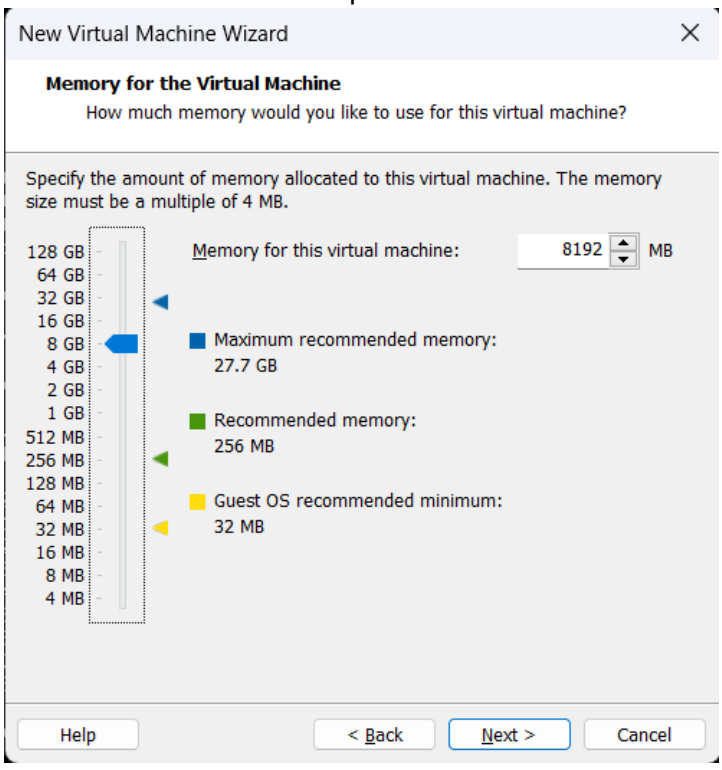
Sélectionnez “Other” et dans le menu déroulant choisissez “FreeBSB 12 64-bit"



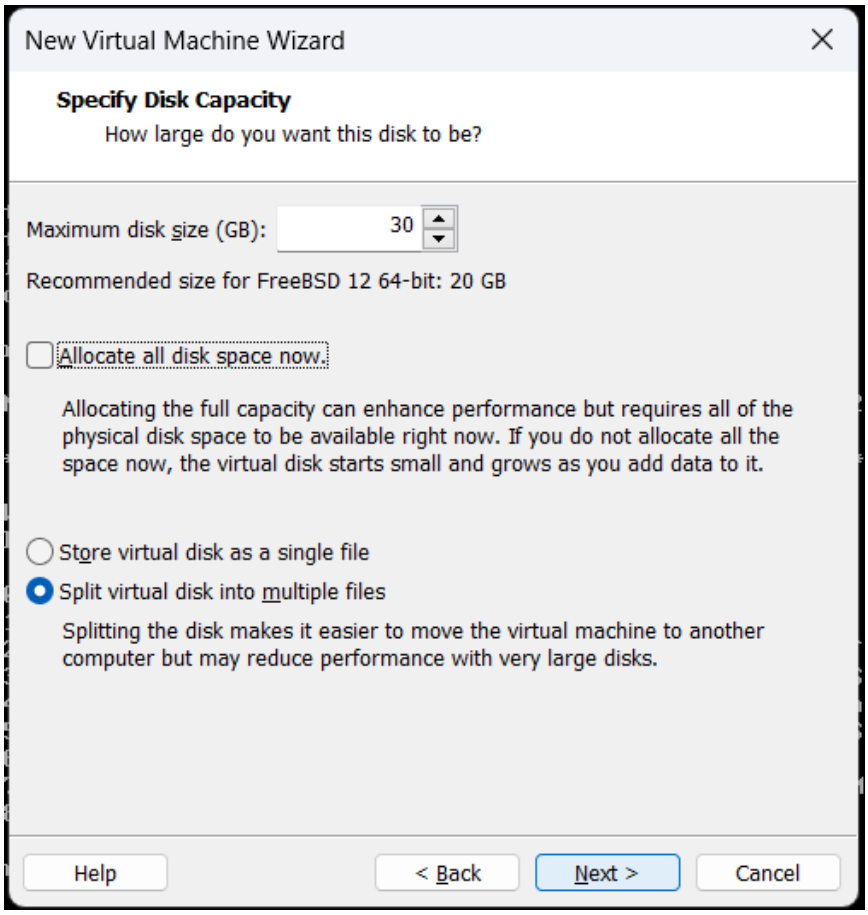
Rentrez le nom de votre machine virtuel dans mon cas “TrueNAS-MUL”



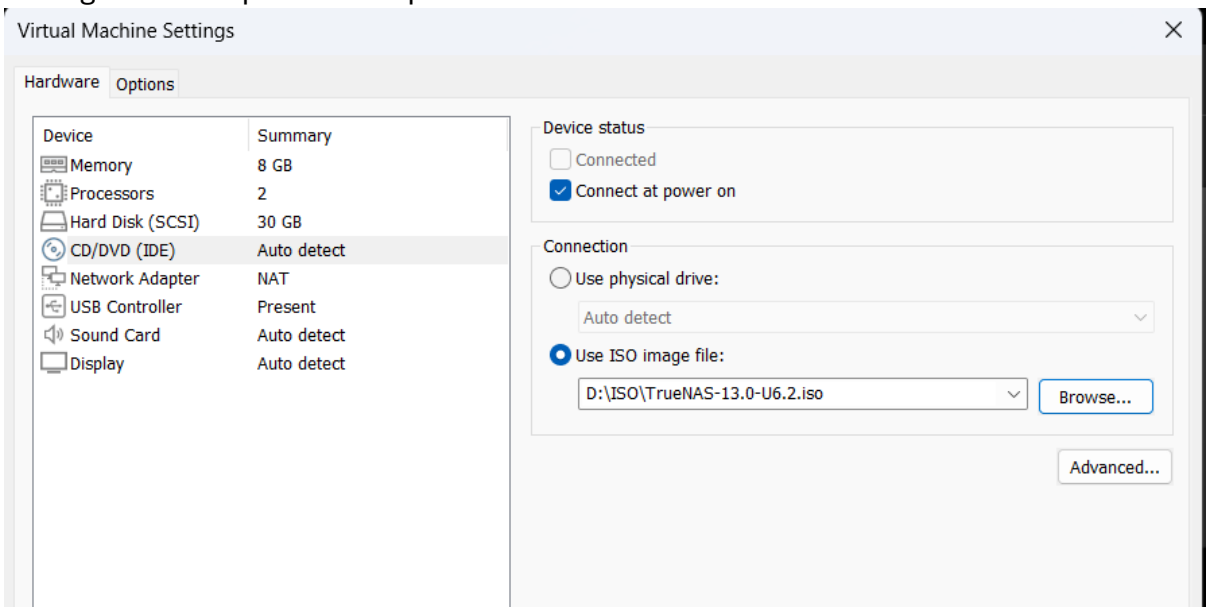
Choisissez le nombre de processeur à mettre dans votre configuration



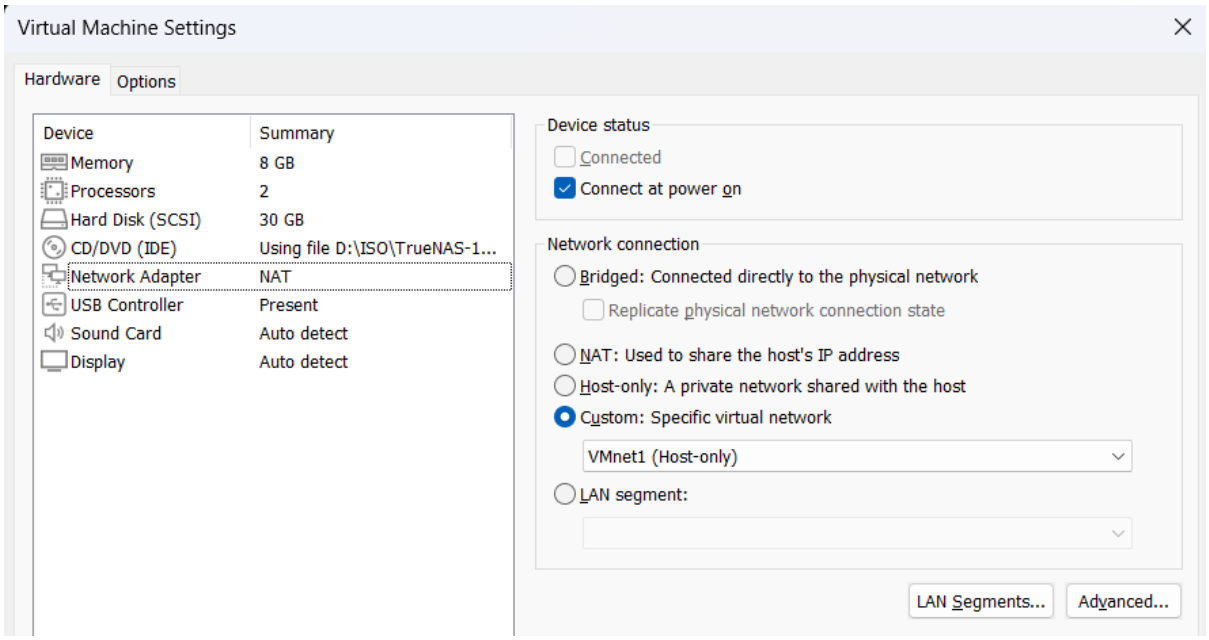
Veuillez bien respecter à mettre 8go de RAM car TrueNAS est assez gourmant.



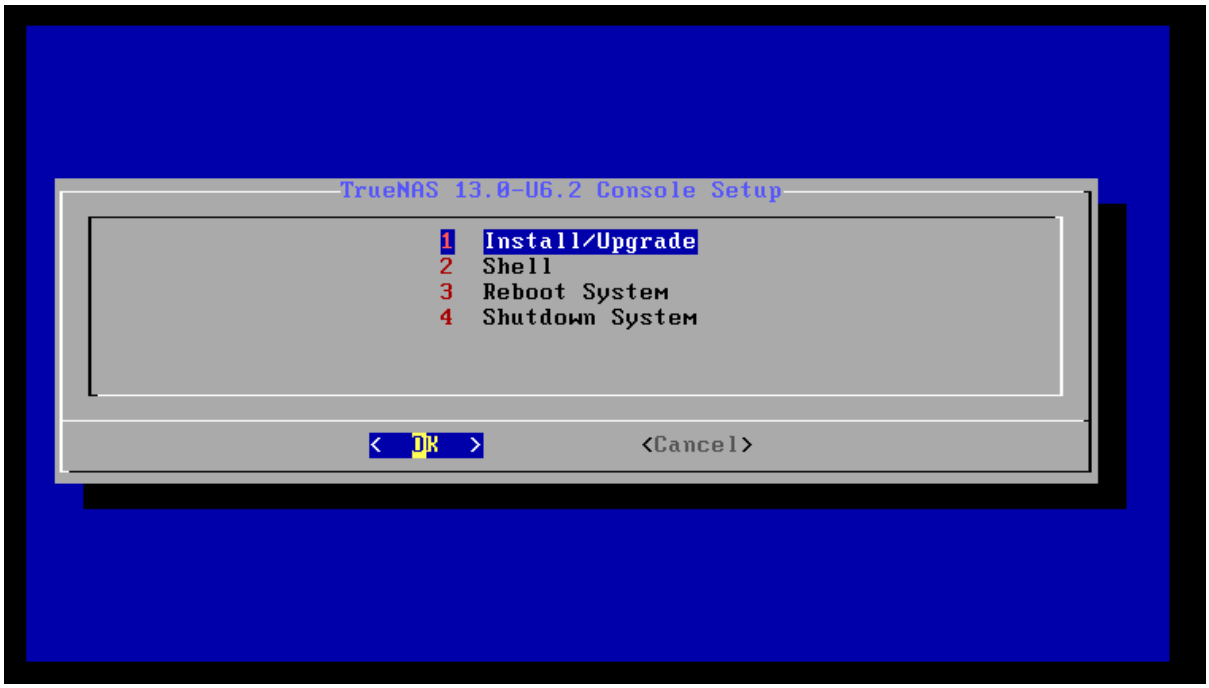
Configurez ici un premier disque et faites Next.



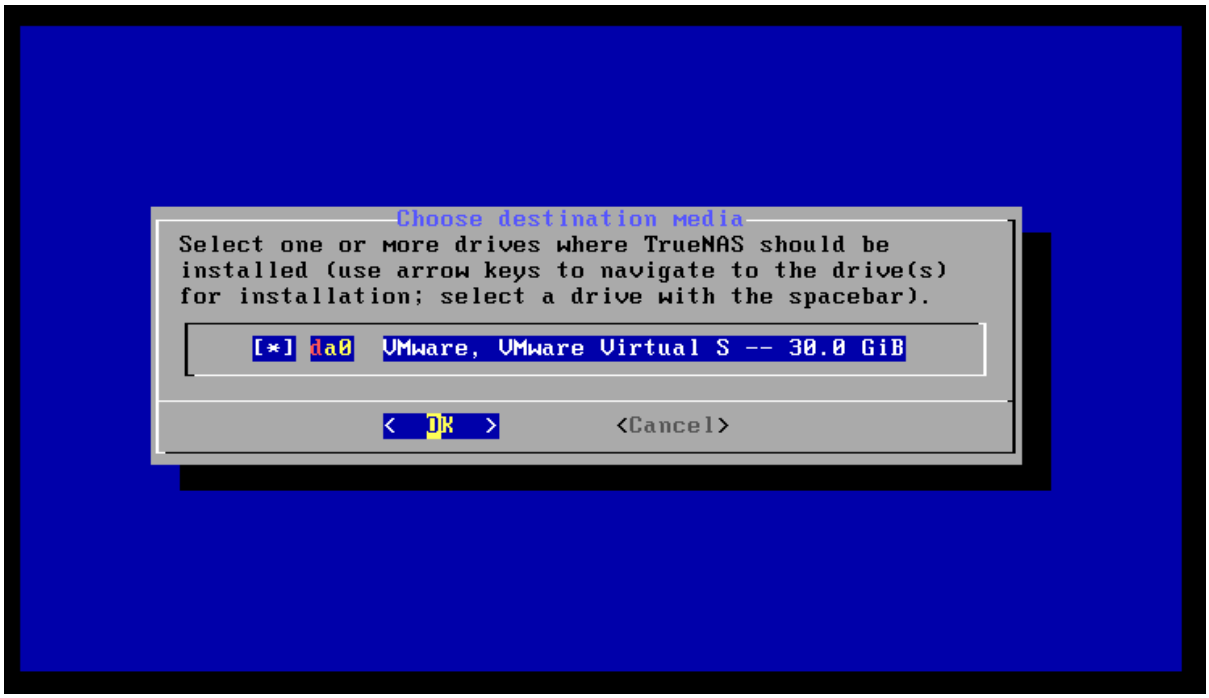
Maintenant allez dans les paramètres de la VM pour ajouter l'ISO de TrueNAS.



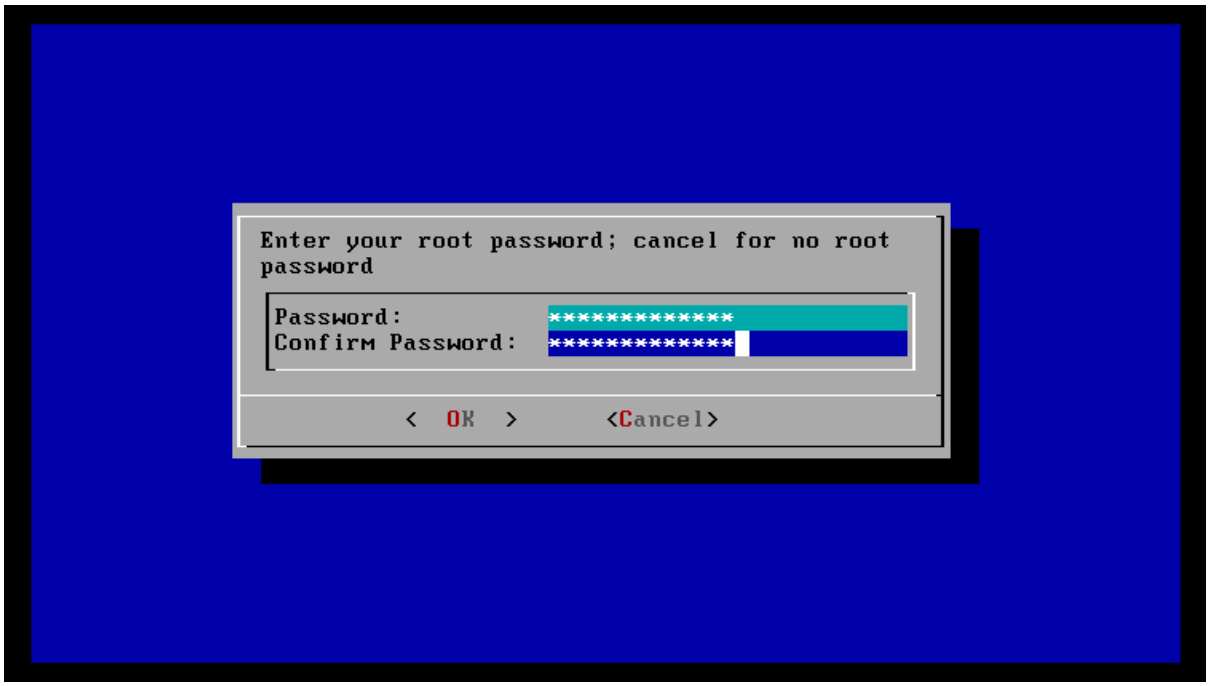
Dans Network Adapter ajoutez votre carte réseaux personnalisé pour qu'elle puisse bien communiquer avec tout le reste de votre infrastructure. On va aussi ajouter un autre disque de 50go.



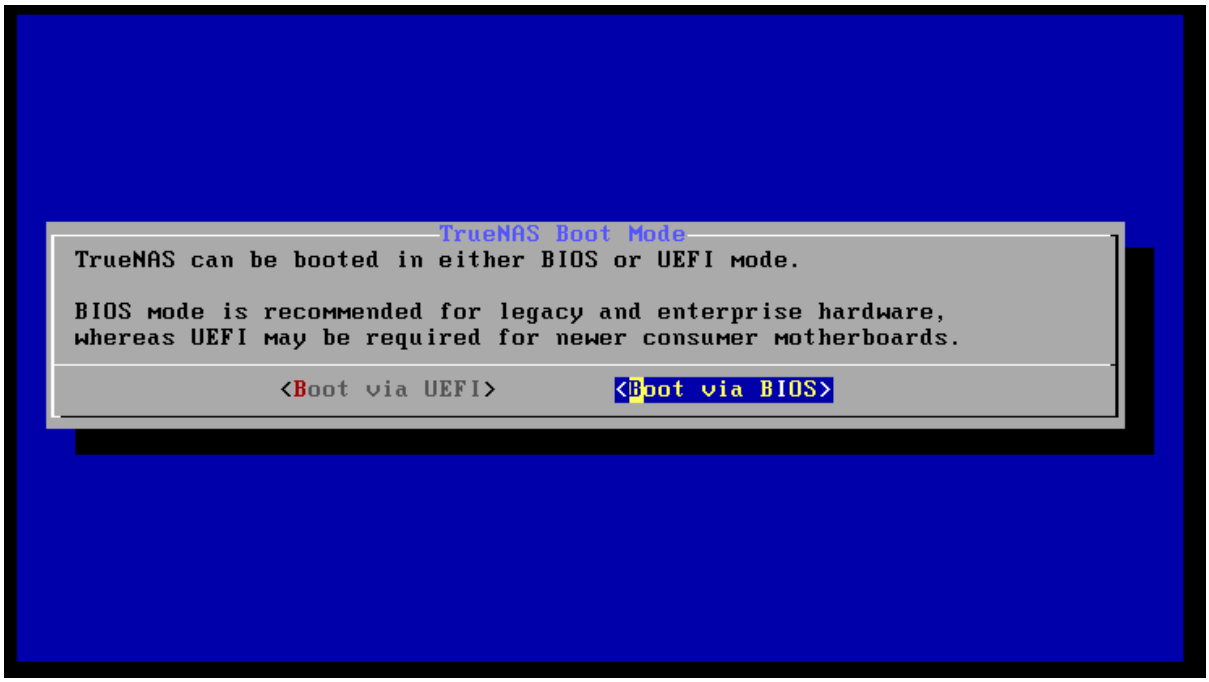
Vous pouvez maintenant lancer TrueNAS. Appuyez sur "Install/Upgrade".



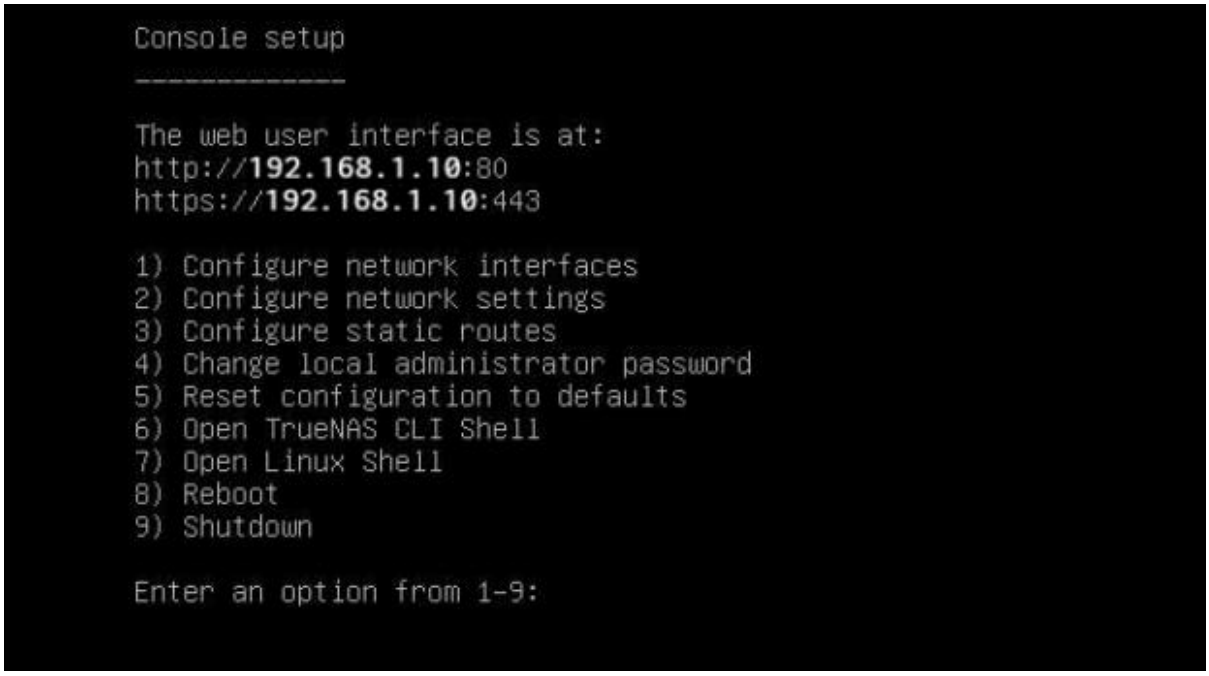
Faites OK.



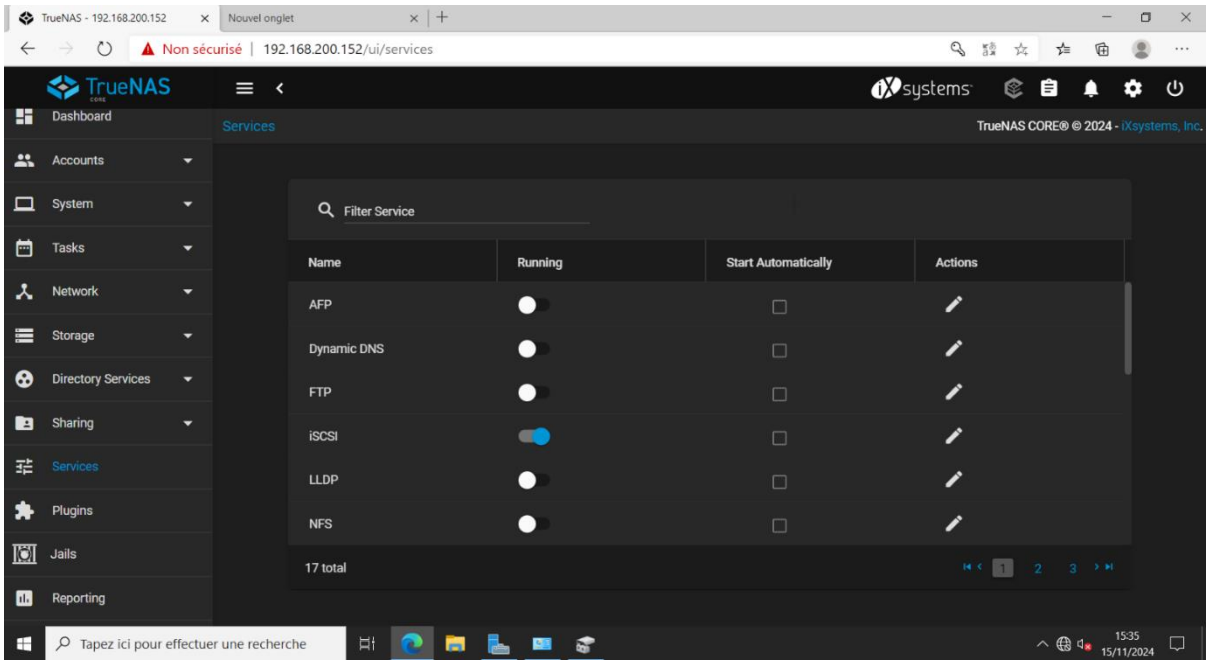
Configurez un mot de passe.



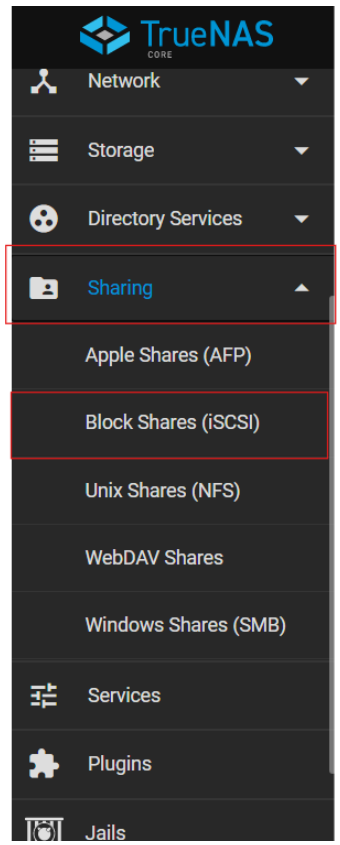
Et choisissez Boot via BIOS.



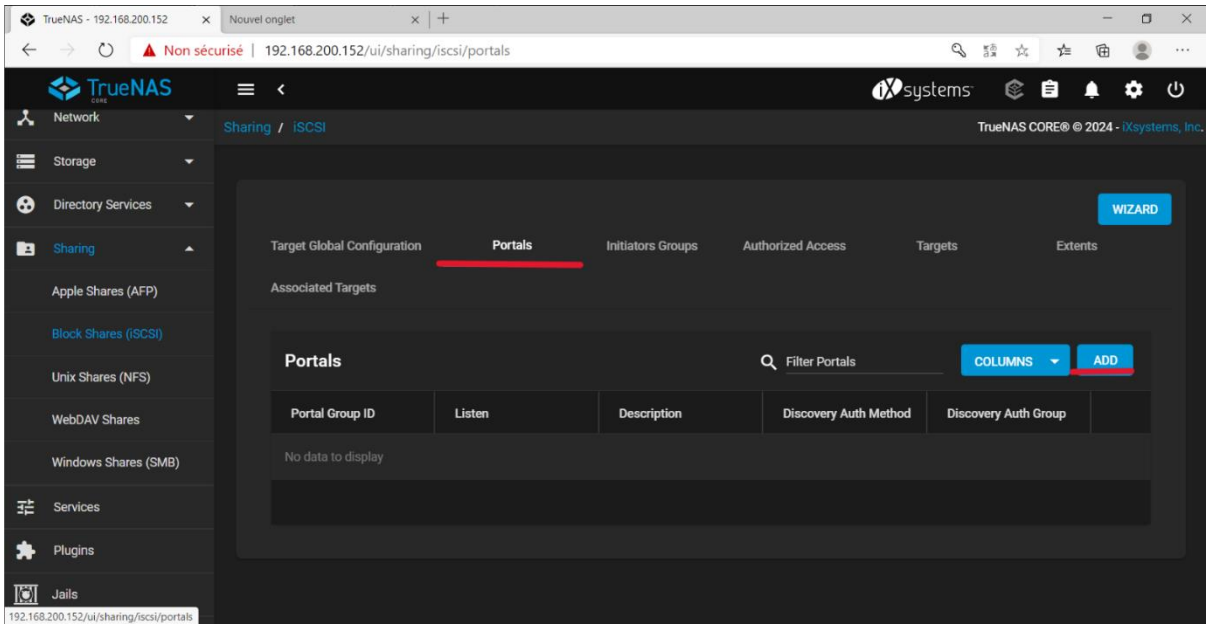
Une fois que TrueNas est bien lancé et configuré vous verrez une page similaire à celle-ci.
Maintenant allez sur votre serveur principal ouvrez une page web et tapez l'adresse ip qu'indique TrueNas.



Allé dans Services et cochez ”ISCSI”.

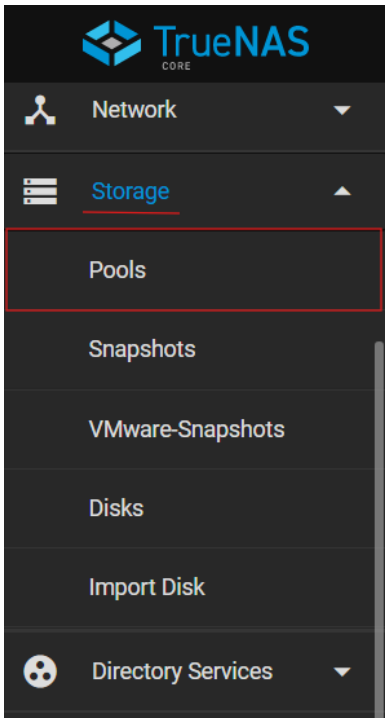


Maintenant allé dans Sharing puis “Block Shares (ISCSI)”

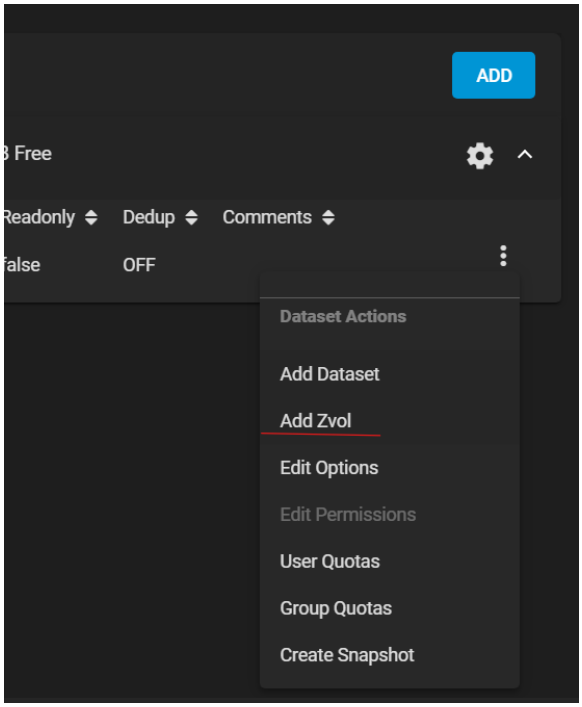


Sélectionner portals et ADD.

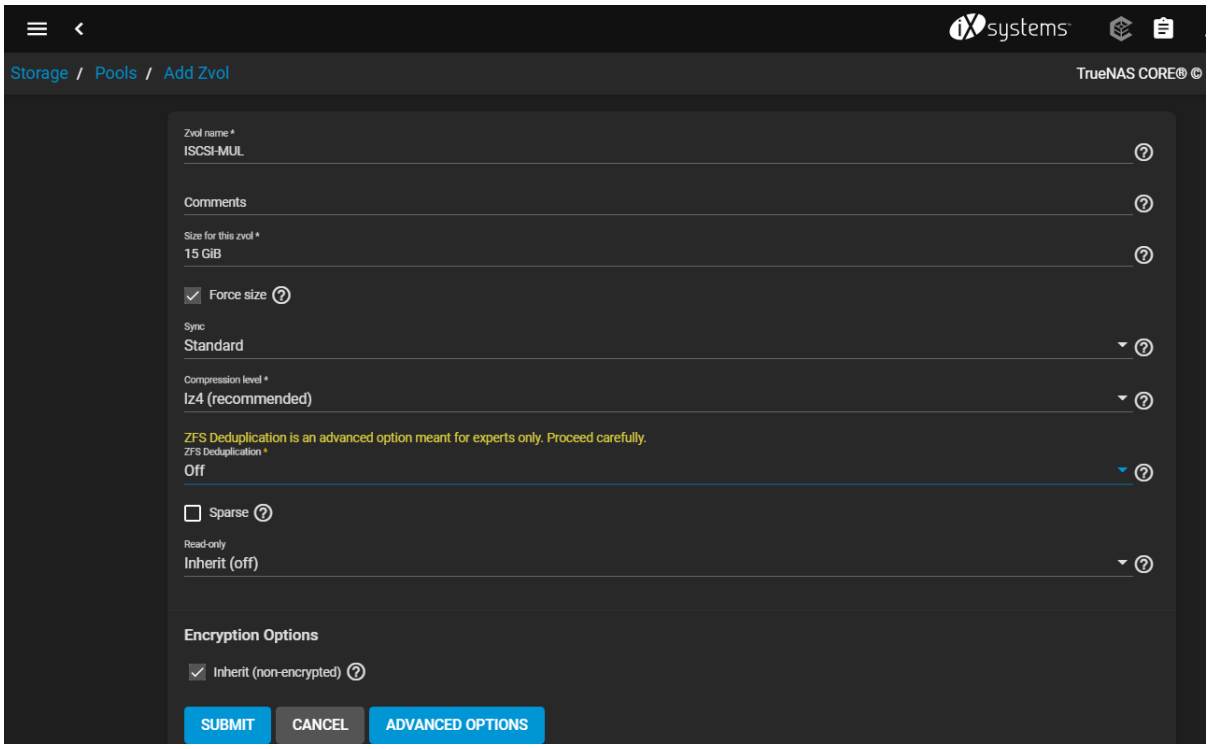
Faites la même chose que sur la capture d'écran. Ajustez bien votre IP par rapport à votre environnement et sauvegardez.



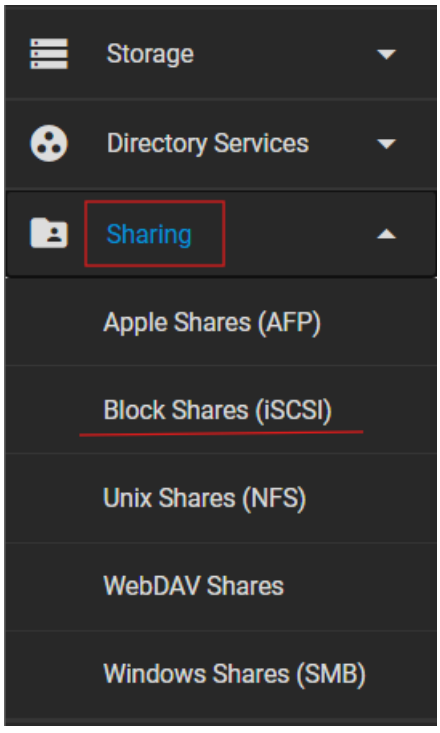
Sur la gauche allez dans Storage puis pools.



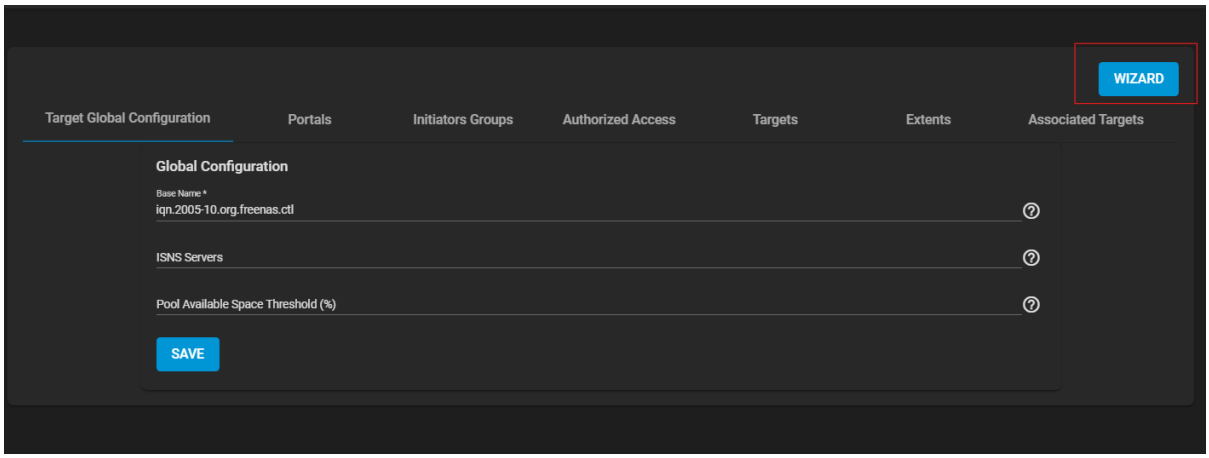
Ici on va créer notre pool de Storage. Appuyez sur add Zvol.



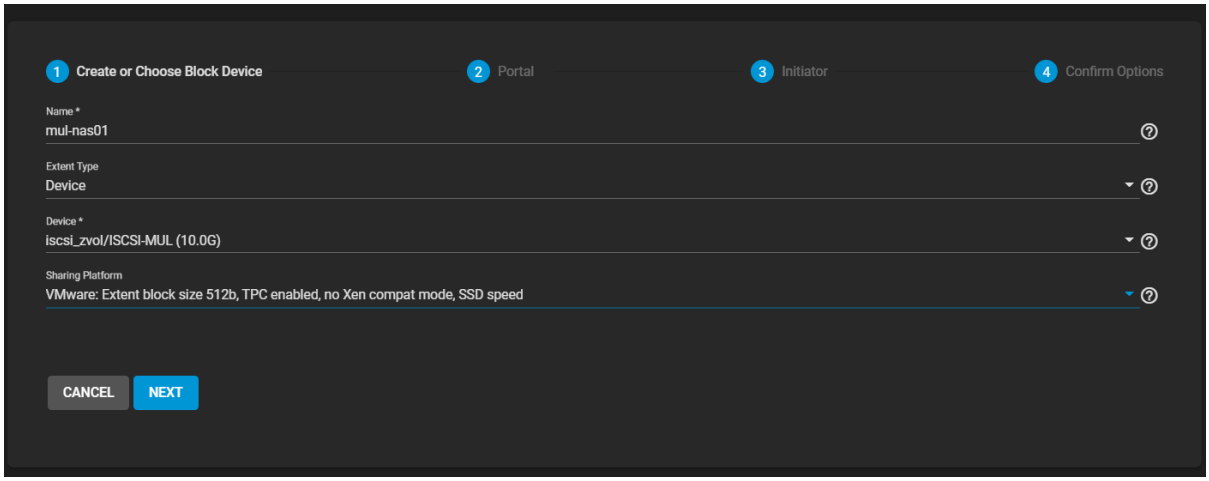
Donnez un nom à votre Pool pour ma part ISCSI MUL. Après donnez lui l'espace qu'il aura c'est à dire 50G et coché bien "force size". Dans Compression level mettez "lz4". Une fois que tout est remplis vous pouvez valider.



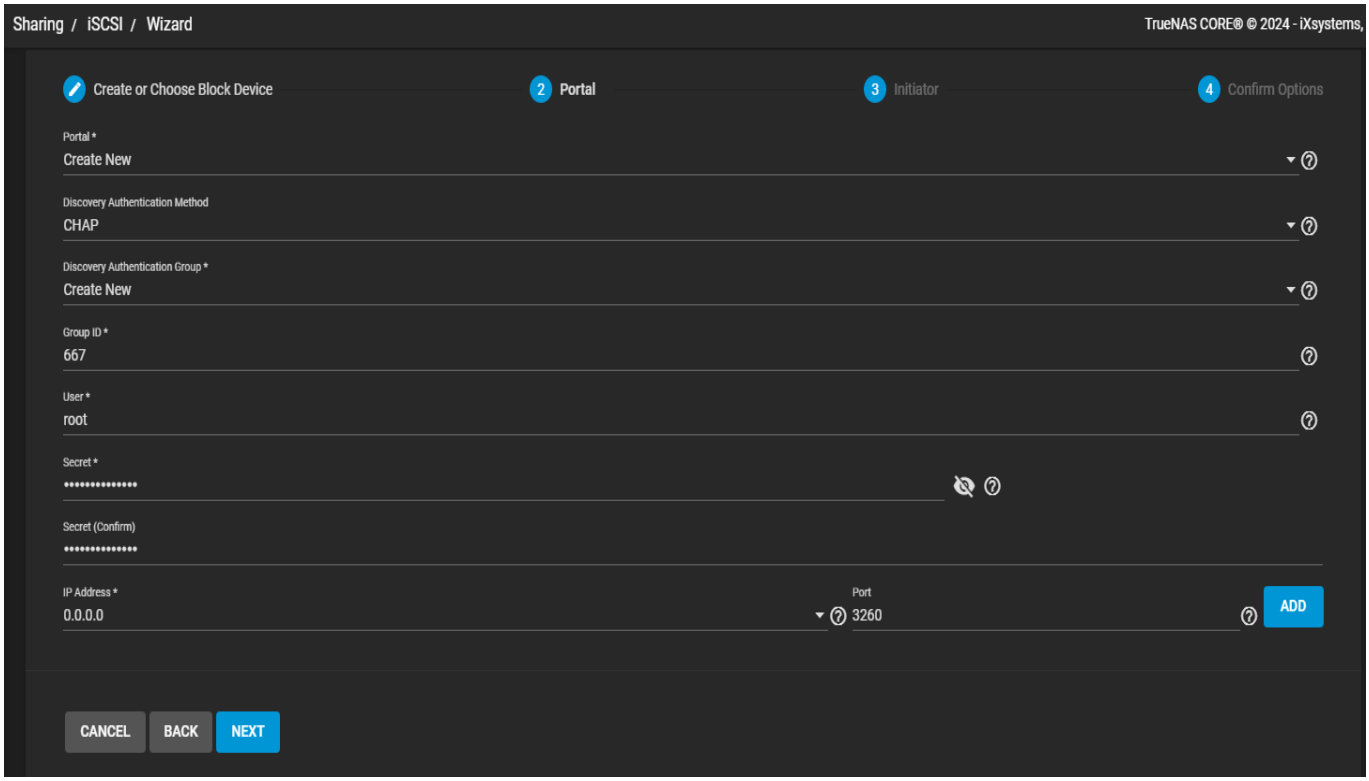
Retourner dans Sharing et "Block Shares (ISCSI)"



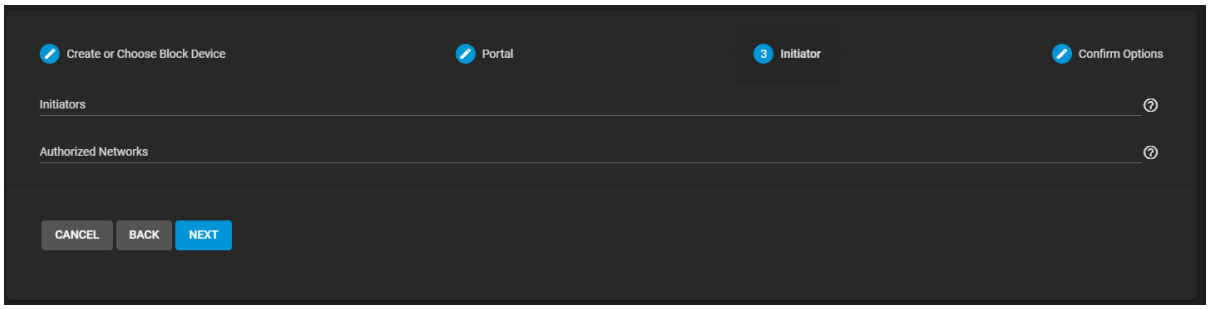
Aller dans WIZARD.



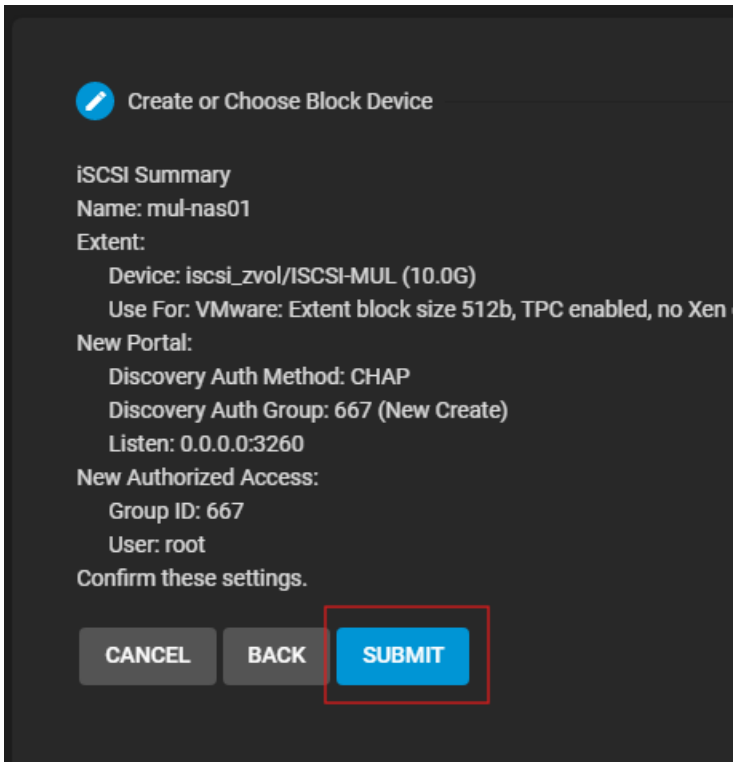
Indiquez un nom, dans Extent type laissez device. Et dans Device il va falloir sélectionner le 2ème disque de 50go (dans ma capture d'écran il y a écrit 10Go mais par la suite j'ai corrigé l'erreur. Dans Sharing Platform mettez VMware.



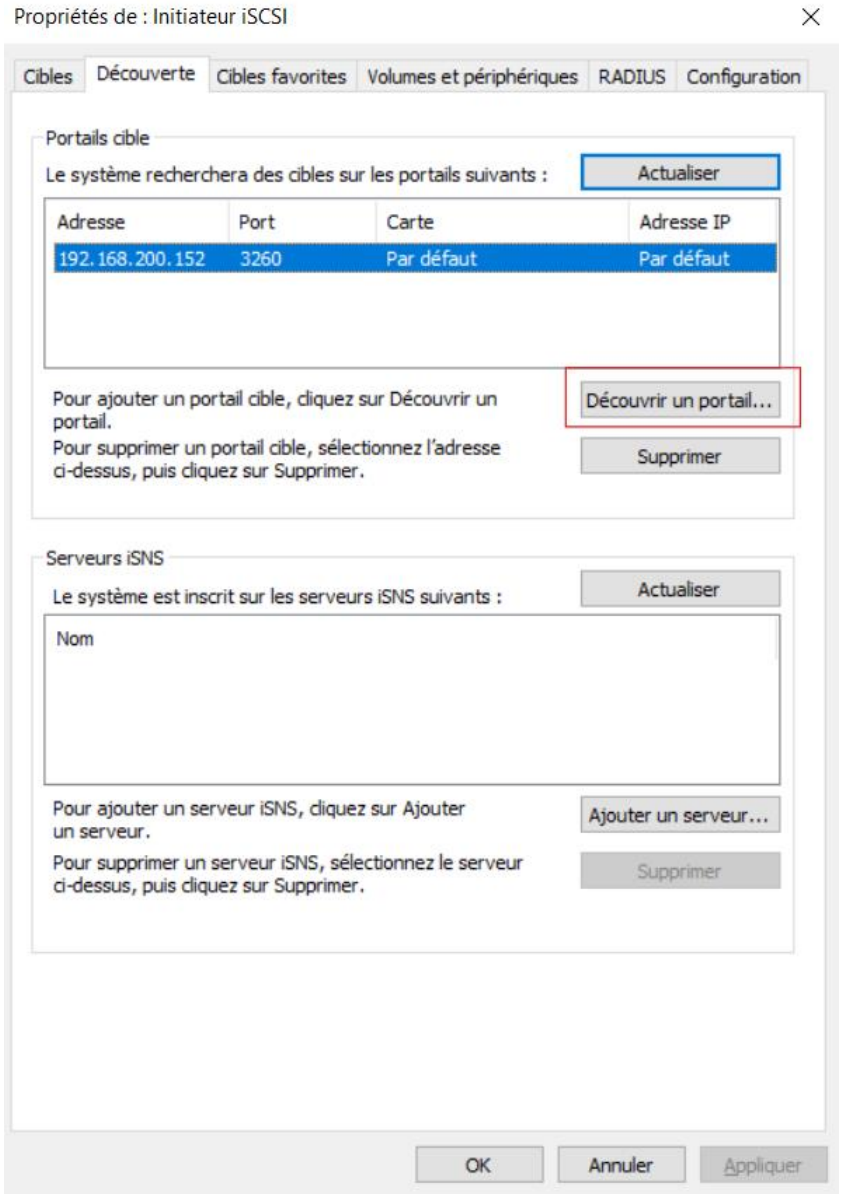
Faites la même chose que sur la capture d'écran ci-dessus. Il va falloir créer un mot de passe pour ensuite établir la connexion avec le partage ISCSI sur Windows server. Dans IP Address laissez 0.0.0.0 et faites Next.



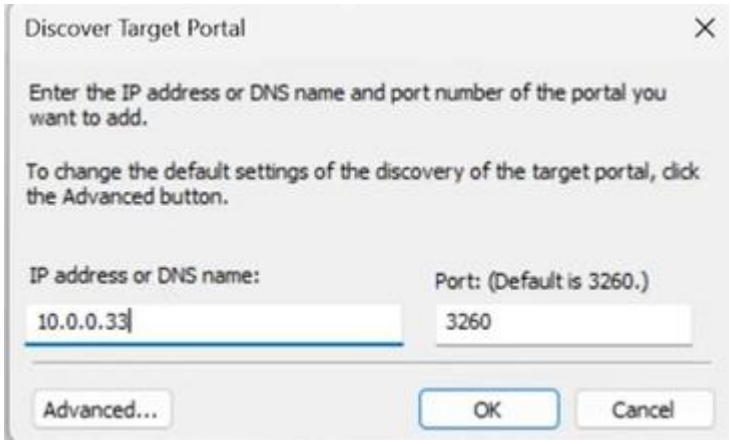
Ici ne changez rien, appuyez sur Next.



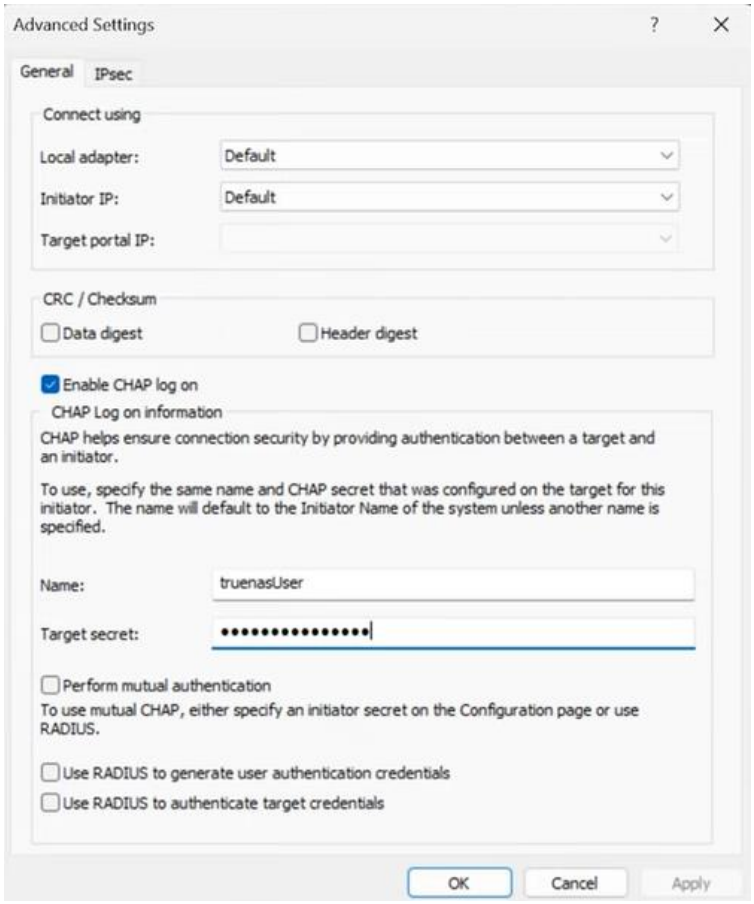
Voici le résumé vous pouvez appuyer sur submit.



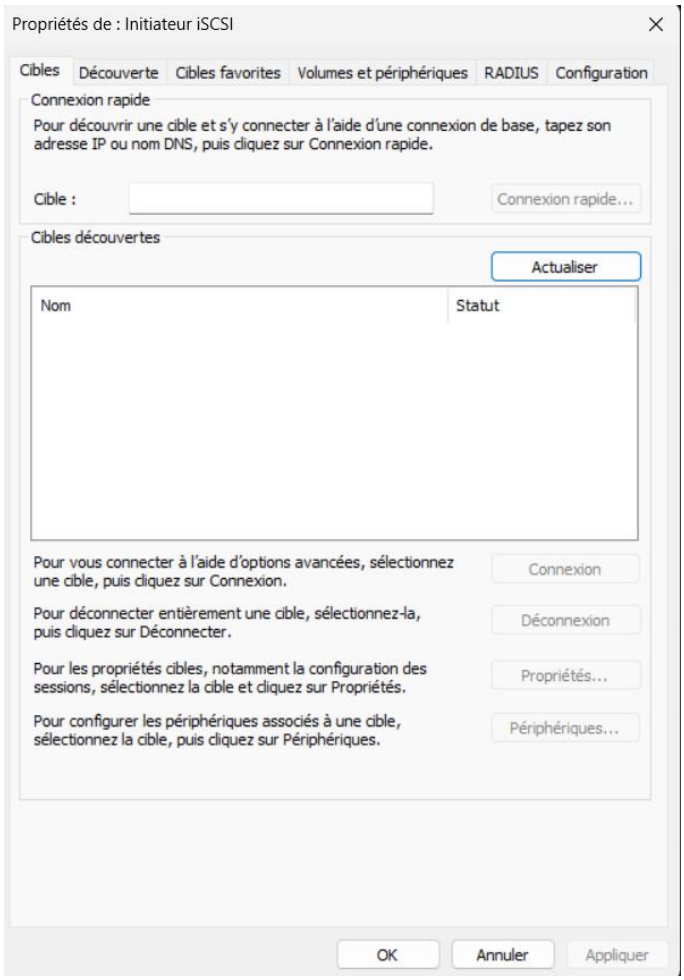
Maintenant Rendez-vous sur votre Windows serveur. Dans la barre de recherche tapez “Initiateur ISCSI” une page comme cela devrais s’ouvrir. Appuyez sur Découvrir un portail.



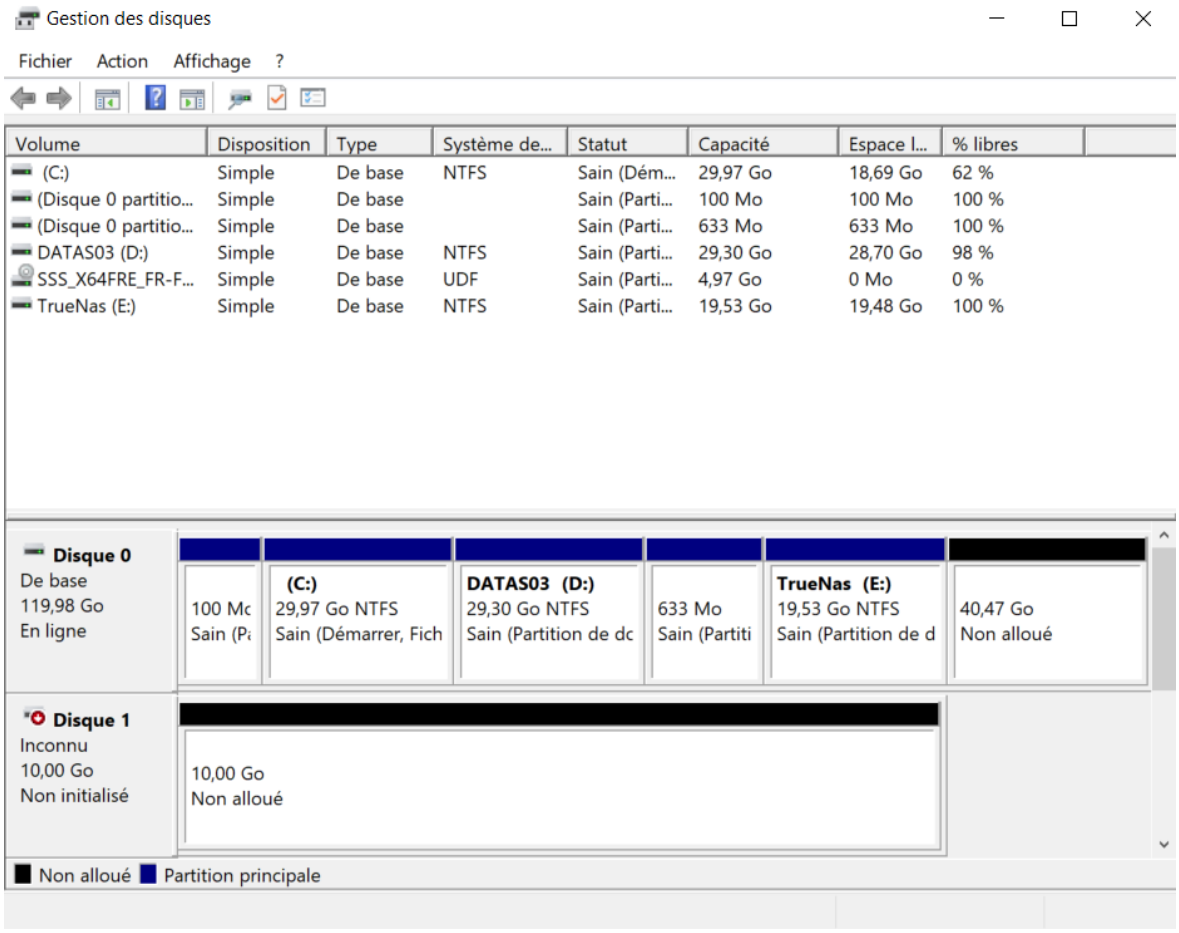
Une page comme ça va s’ouvrir indiquez l’adresse IP de votre TrueNas et appuyez sur Advanced.



Cochez “Enable CHAP log on” et dans name et target secret entré l’utilisateur que vous avez créé juste avant sur l’interface de TrueNas. Validé faite ok.



Une fois connecté, allez dans la section “Cibles”, et faites actualiser : le nom de votre partage devrait apparaitre dans les cibles découvertes. Cliquez sur le partage pour le sélectionner et faites connexion puis ok. Vous pouvez maintenant fermer cette fenêtre et ouvrir le gestionnaire des disques.



Vous pouvez apercevoir que l'on voit bien notre partage il ne reste plus qu'à initialiser le disque et à créer un nouveau volume.