

-
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
<i>Prérequis</i> :	3
<i>Étape 1 : Installation de PFSense</i>	3
<i>Étape 2 : Sur le site A</i>	5
<i>Étape 2 : Sur le site B</i>	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
<i>Prérequis</i> :	13
<i>Étape 1 : Installation des rôles / fonctionnalités sur le serveur 1</i> :	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
<i>Étape 2 : Installation des rôles / fonctionnalités sur le serveur 2</i> :	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
<i>Prérequis</i> :	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) :

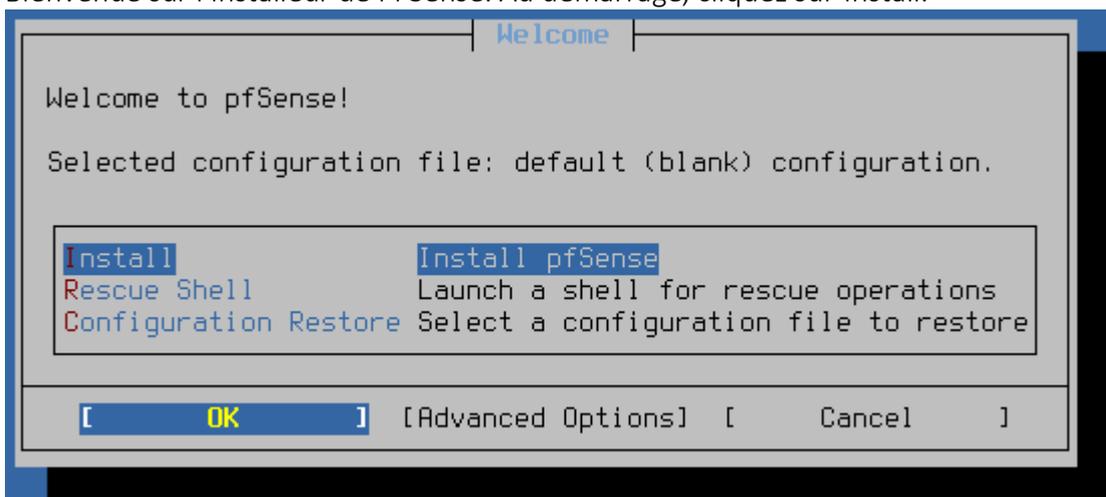
Prérequis :

- 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)

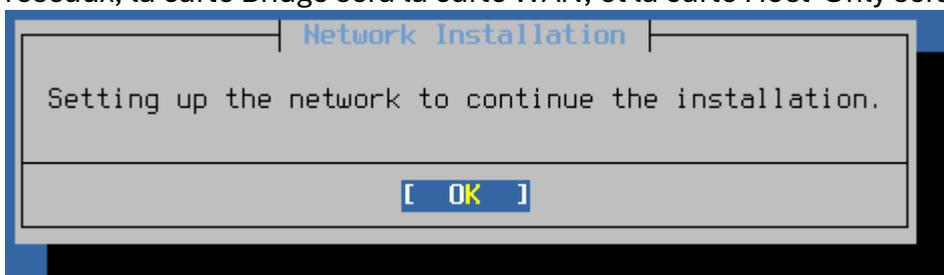
Cet exemple prendra en compte l'interconnexion de 2 routeurs qui seront sur des machines virtuelles, sur des PC différents. Les routeurs auront 2 cartes réseaux, une en Bridge sur la carte Wi-Fi physique, et une en LAN, qui sera la même que celle pour le client Windows. Le client tant qu'à lui aura simplement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

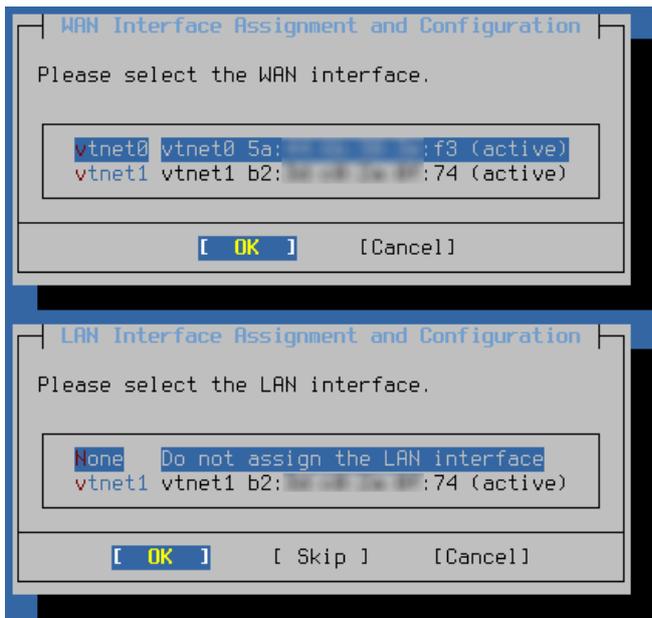
Étape 1 : Installation de PFSense

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

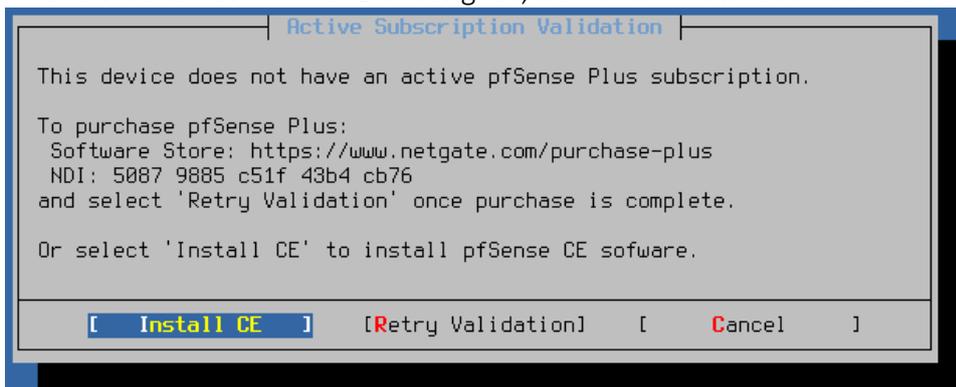


Après avoir démarré l'installation, assigner les interfaces WAN et LAN aux cartes réseaux, la carte Bridge sera la carte WAN, et la carte Host-Only sera la carte LAN.

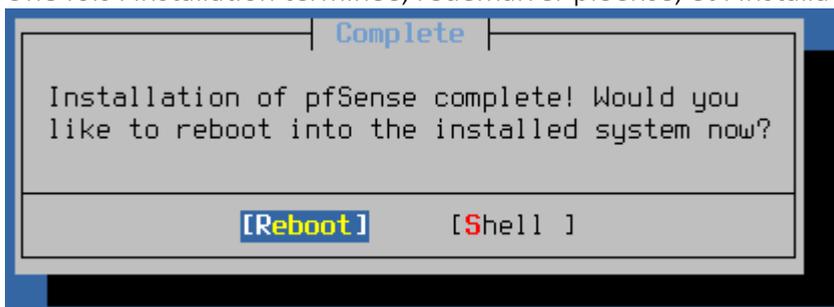




Il est recommandé d'attribuer une adresse IP fixe pour l'adresse LAN, pour éviter les problèmes d'accès à l'interface WEB de pfSense.
 Une fois les cartes WAN et LAN assignés, démarrer l'installation des fichiers de pfSense.



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 :

VPN / IPsec / Tunnels / Modifier la phase 1 🔄 🏠 📄 ?

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

Informations Générales

Description VPN vers site B
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Désactivé Définissez cette option pour désactiver cette phase1 sans la retirer de la liste.

IKE ID 1

IKE Endpoint Configuration

Version de l'échange de clés IKEv2
Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEv2 lors de l'initiateur, et accepte IKEv1 ou IKEv2 comme répondeur.

Protocole Internet IPv4
Sélectionnez la famille Internet Protocol.

Interface WAN
Sélectionnez l'interface pour le point final local de cette entrée phase1.

Passerelle distante 172.20.10.5
Enter the public IP address or host name of the remote gateway. ⓘ

Proposition de phase 1 (authentification)

Méthode d'authentification PSK Mutuel
Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant Mon adresse IP

Identifiant de pair Adresse IP distante

***Clé Pré-Partagée** P@ssword10
Enter the Pre-Shared Key string. This key must match on both peers.

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

d'authentification
Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant Mon adresse IP

Identifiant de pair Adresse IP distante

***Clé Pré-Partagée** P@ssword10
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Algorithme de chiffrement AES 256 bits SHA256 14 (2048 bit) [Supprimer](#)
Algorithm Longueur de la clé Hash DH Group

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm [+ Add Algorithm](#)

Expiration and Replacement

Life Time 28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time 25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

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.

Tunnels		Clients mobiles	Clés pré-partagées	Paramètres avancés
Informations Générales				
Description	<input type="text"/>			
	Une description peut être saisie ici à des fins de référence administrative (non analysée).			
Désactivé	<input type="checkbox"/> Désactivez cette la phase 2 sans la supprimer de la liste.			
Mode	Tunnel IPv4			
Phase 1	TUNNEL TUNNEL (IKE ID 1)			
P2 reqid	1			
Réseaux				
Réseau local	Réseau	192.168.100.0	/	24
	Type	Adresse		
	Local network component of this IPsec security association.			
Traduction NAT/BINAT	Aucun		/	0
	Type	Adresse		
	Si NAT/BINAT est requis sur ce réseau, spécifiez l'adresse à traduire			
Réseau distant	Réseau	192.168.200.0	/	24
	Type	Adresse		
	Remote network component of this IPsec security association.			

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.

Proposition de phase 2 (SA/Key Exchange)

Protocole
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Algorithmes de chiffrement AES
 AES128-GCM
 AES192-GCM
 AES256-GCM
 CHACHA20-POLY1305

Algorithmes de hachage SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

Groupe de clés PFS
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time
Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

Rekey Time
Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

Rand Time
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

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 :

Pare-feu / Alias / Ports [?] [!]

IP **Ports** **URLs** **Tout**

Alias de pare-feu Ports

Nom	Type	Valeurs	Description	Actions
rules	Port(s)	21, 22, 80, 443, 53, 1194, 50, 500, 4500	règles pare feu	

[+ Ajouter](#) [Importer](#)

Créer un alias qui va renseigner 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(a) WAN LAN IPsec

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input checked="" type="checkbox"/>	0/2,67 MiB	*	*	*	LAN Address	80 22	*	*		Règle anti-blocage	⚙️
<input type="checkbox"/>	1/6,52 MiB	IPv4 *	LAN subnets	*	*	*	*	aucun		Default allow LAN to any rule	📌 ✎ 📄 🗑️ ✕
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	aucun		Default allow LAN IPv6 to any rule	📌 ✎ 📄 🗑️ ✕
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	192.168.100.0/24	*	192.168.200.0/24	rules	*	aucun			📌 ✎ 📄 🗑️ ✕
<input type="checkbox"/>	✖ 0/0 B	IPv4 *	*	*	*	*	*	aucun			📌 ✎ 📄 🗑️ ✕

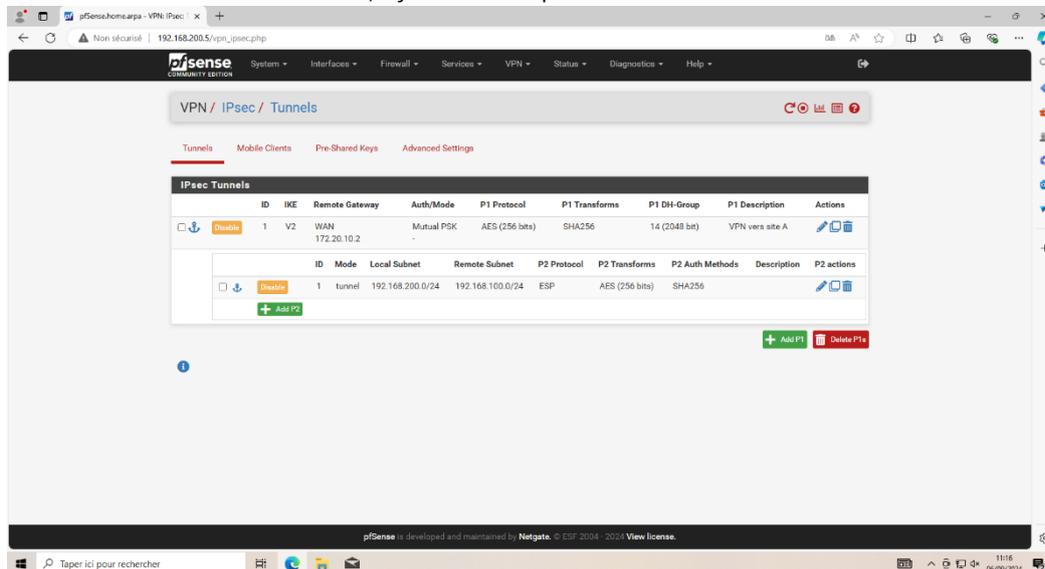
⬆ Ajouter ⬇ Ajouter 🗑 Supprimer 🔄 Toggle 📄 Copier 📁 Enregistrer ⊕ Séparateur

Étape 2 : Sur le site B

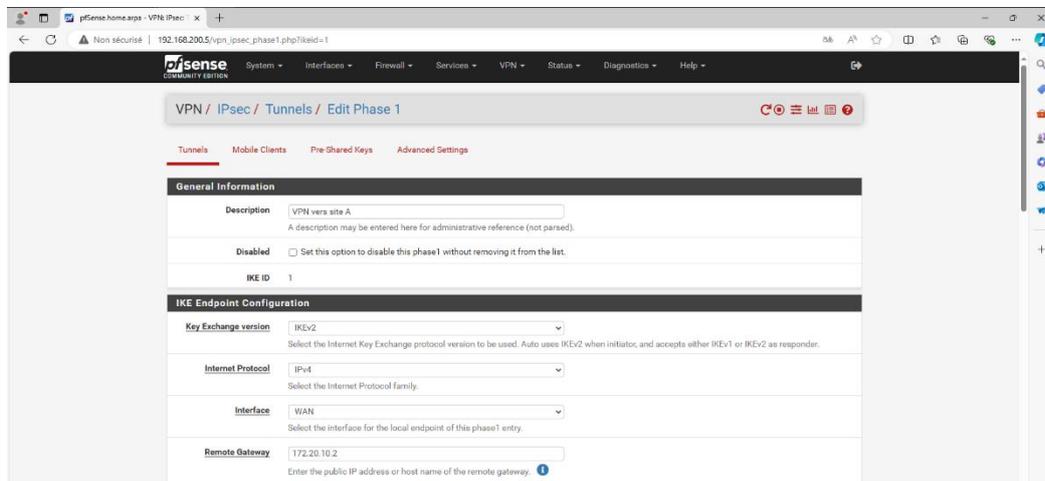
Pour accéder à l'interface, rentrer l'adresse LAN de pfSense dans un navigateur.

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.

Phase 1 Proposal (Authentication)

Authentication Method: Mutual PSK
Must match the setting chosen on the remote side.

My Identifier: My IP address

Peer Identifier: Peer IP address

Pre-Shared Key: P@ssword10
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm: AES, 256 bits, SHA256, 14 (2048 bit)

Expiration and Replacement

Life Time: 28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey).

Rekey Time: 25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time: 0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support

Concernant les paramètres, 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.

VPN / IPsec / Tunnels / Edit Phase 2

General Information

Description: A description may be entered here for administrative reference (not parsed).

Disabled: Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Phase 1: VPN vers site A (IKE ID 1)

P2 reqid: 1

Networks

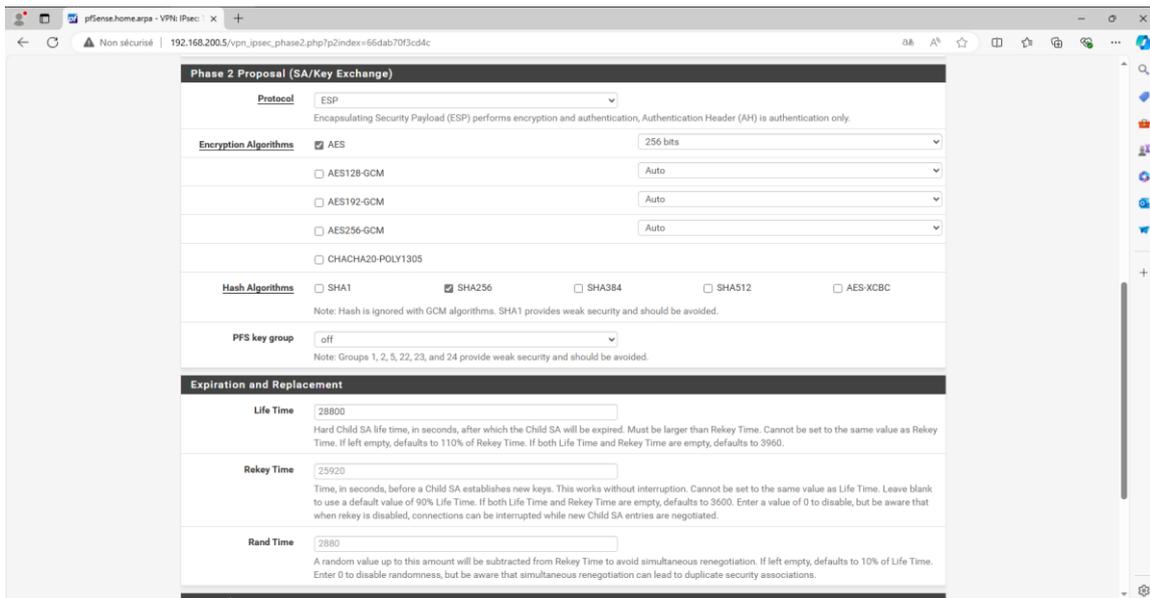
Local Network: Network: 192.168.200.0 / 24
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation: None / 0
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network: 192.168.100.0 / 24
Type: Address
Remote network component of this IPsec security association.

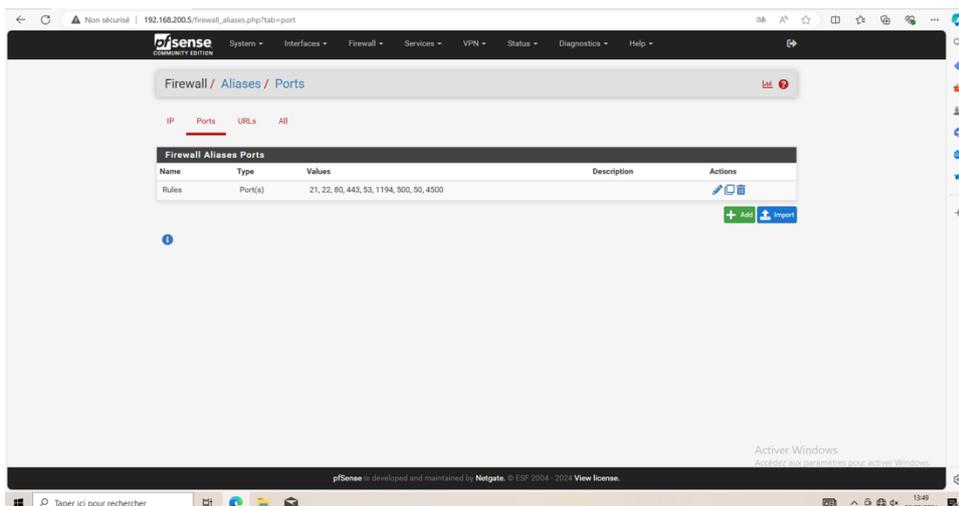
Dans Réseau local, rentrer la plage du réseau LAN du site A, et dans le Réseau distant, rentrer la plage du réseau LAN du site B.

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

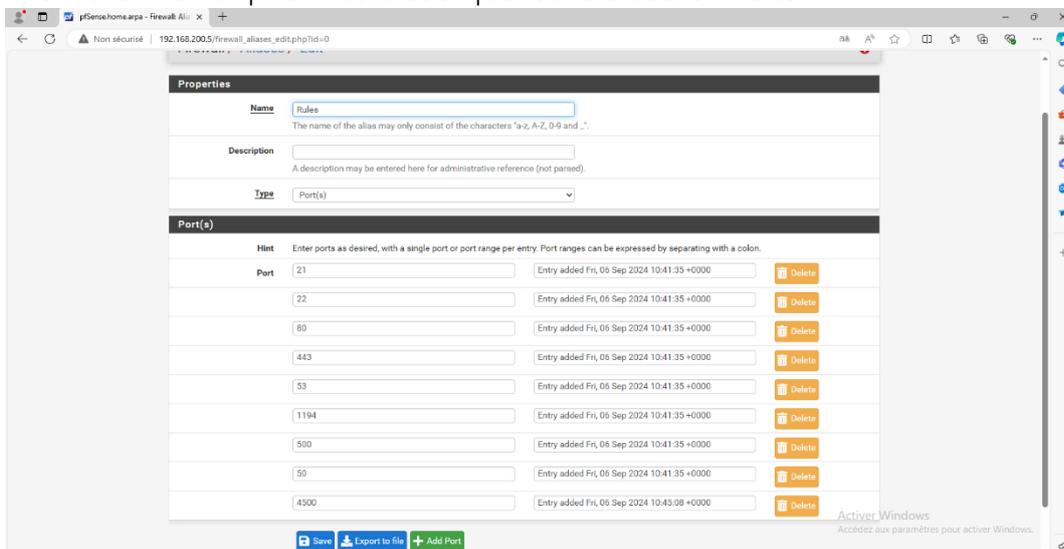


Il faut également qu'il y ait le même algorithme de chiffrement sur les 2 routeurs.

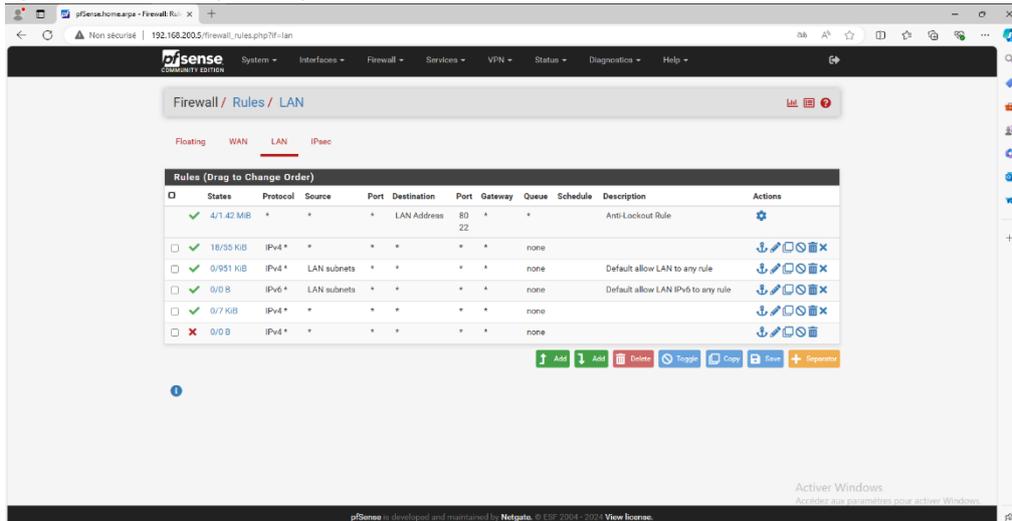
2. Configuration des règles du firewall.



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 utilisés.

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or IC) whereas with block the packet is dropped silently. In either case, the original packet is d

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

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

Protocol Any
Choose which IP protocol this rule should match.

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 :

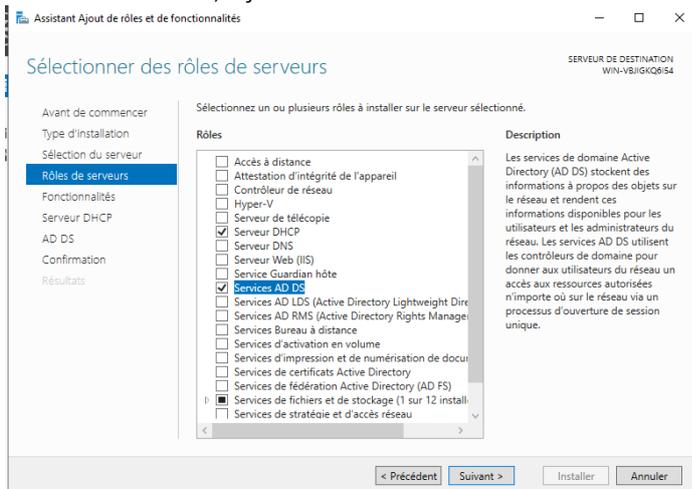
Installation du rôle sur le serveur

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

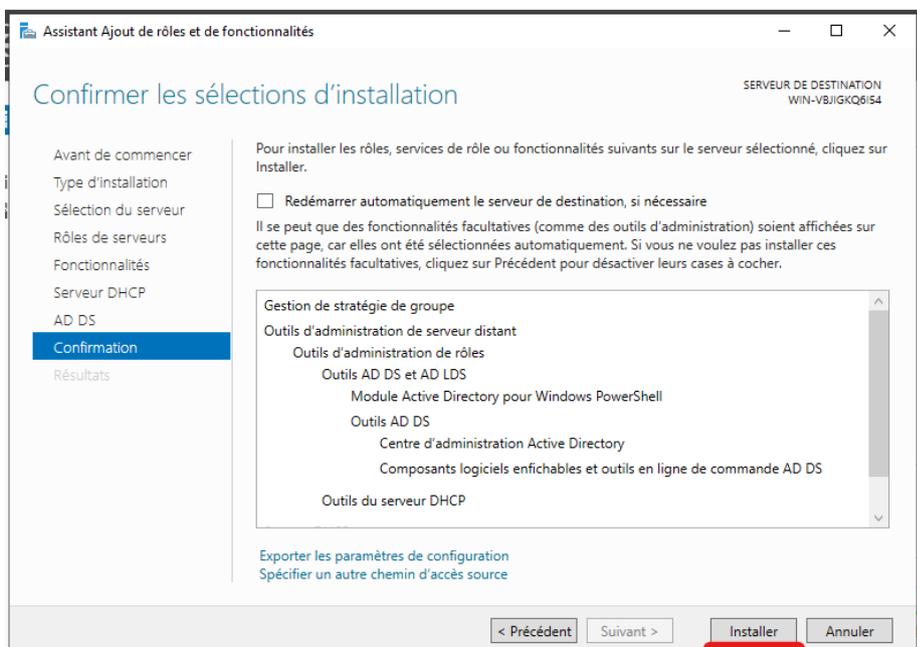
- Aller dans le gestionnaire de serveur sous Serveur Local
- Double cliquer sur Adresse IPv4 attribuée par DHCP
- Cliquer sur sa carte réseau *EthernetX*
- Aller dans les propriétés, puis Protocole Internet version 4
- Dans cette interface il sera alors possible de définir une adresse IP fixe.

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

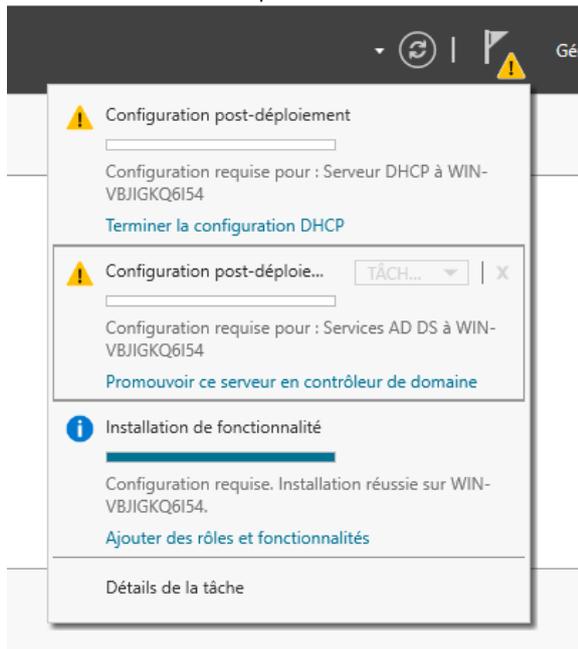
Aller dans Gérer, Ajouter des rôles ou des fonctionnalités, puis sélectionner celles-ci



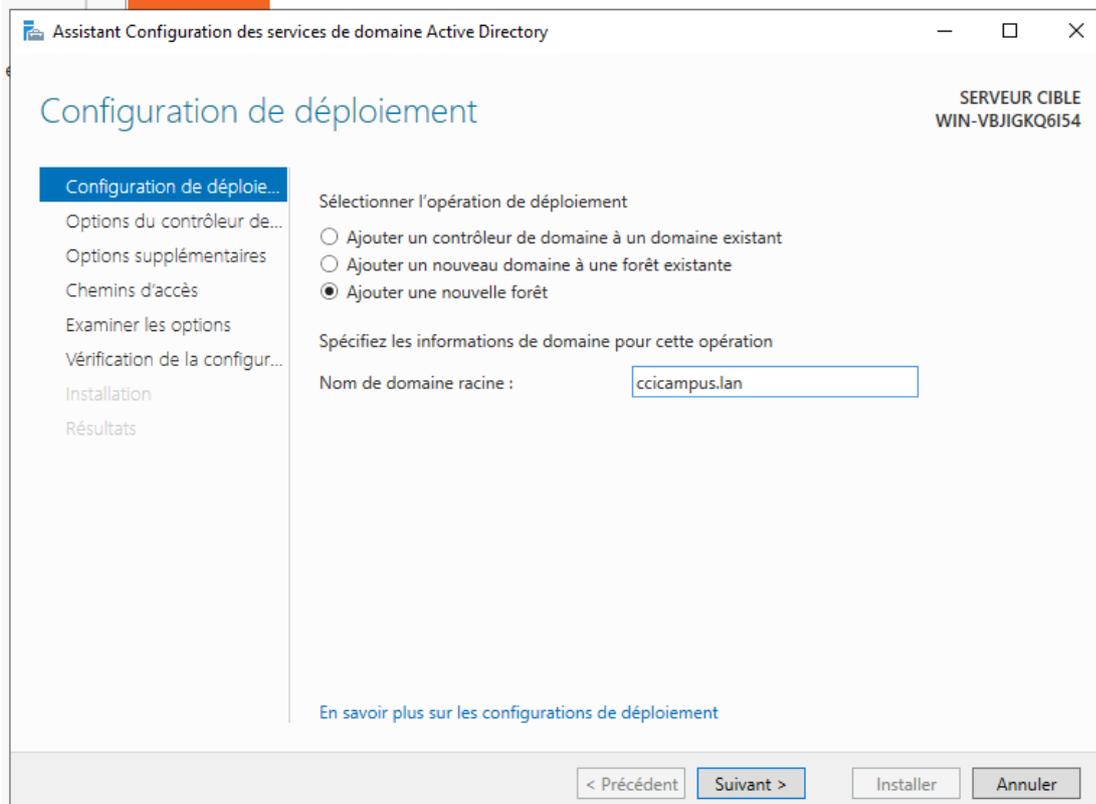
Lancer l'installation des rôles :



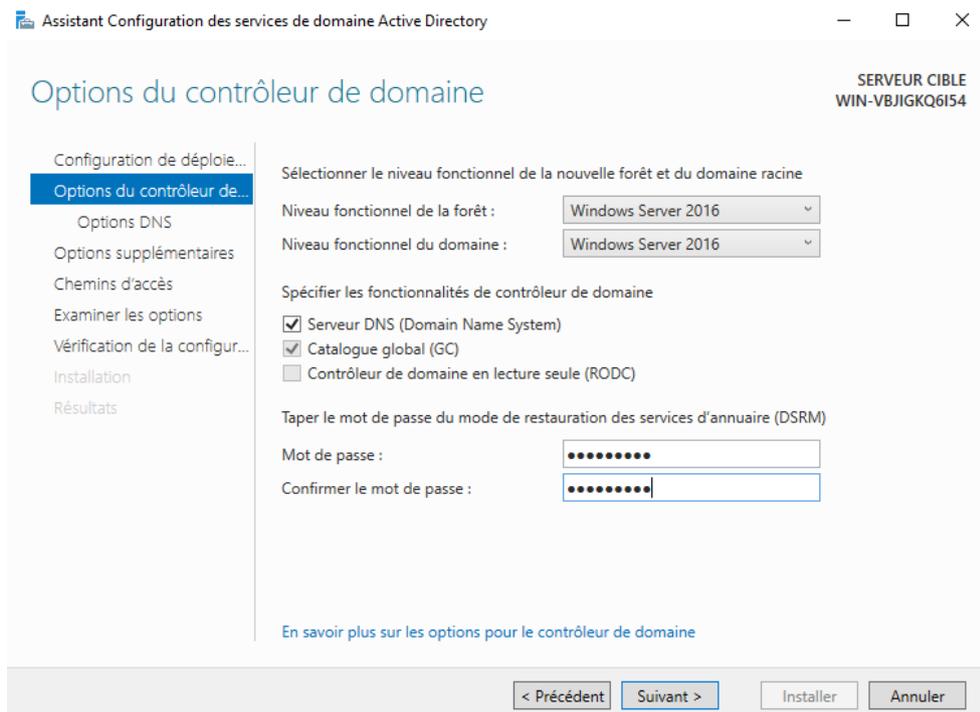
Ensuite, nous allons lancer la création de la forêt Active Directory en cliquant sur Promouvoir ce serveur en tant que contrôleur de domaine :



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



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

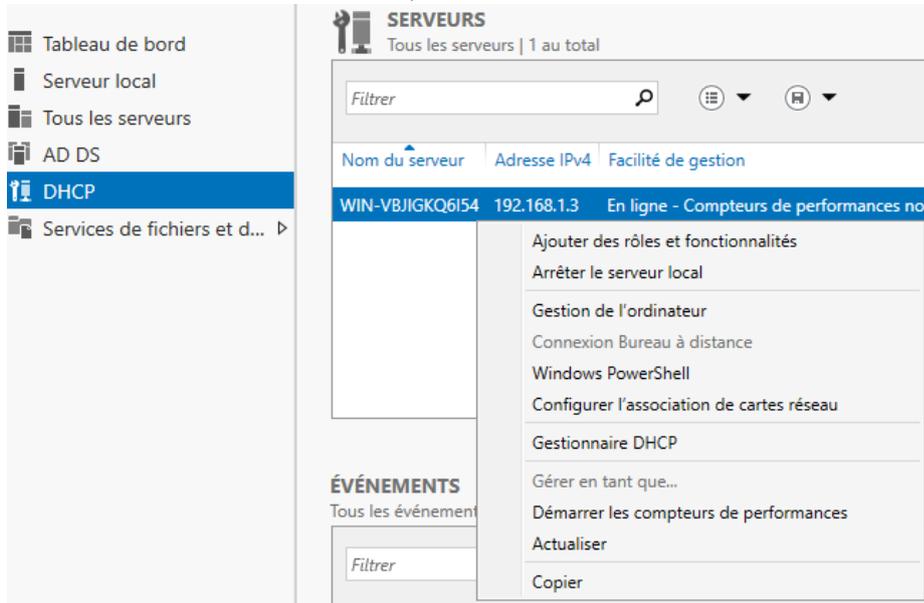


Une fois cela fait, l'AD sera complètement installé, prêt à l'usage.

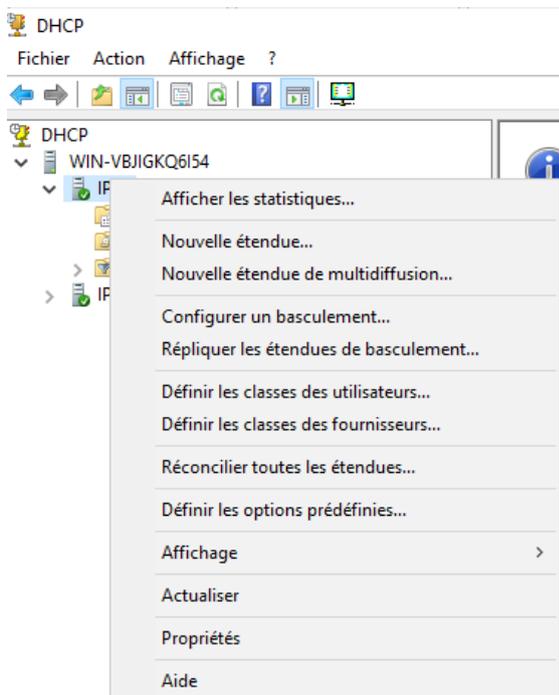
Configuration du rôle DHCP avec création d'une étendue de test

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.

Assistant Nouvelle étendue

Nom de l'étendue
Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

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)

Assistant Nouvelle étendue

Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

< Précédent **Suivant >** Annuler

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

Installation d'un serveur DHCP [voir l'aide en ligne](#)

Assistant Nouvelle étendue

Activer l'étendue
Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.

Voulez-vous activer cette étendue maintenant ?

Oui, je veux activer cette étendue maintenant

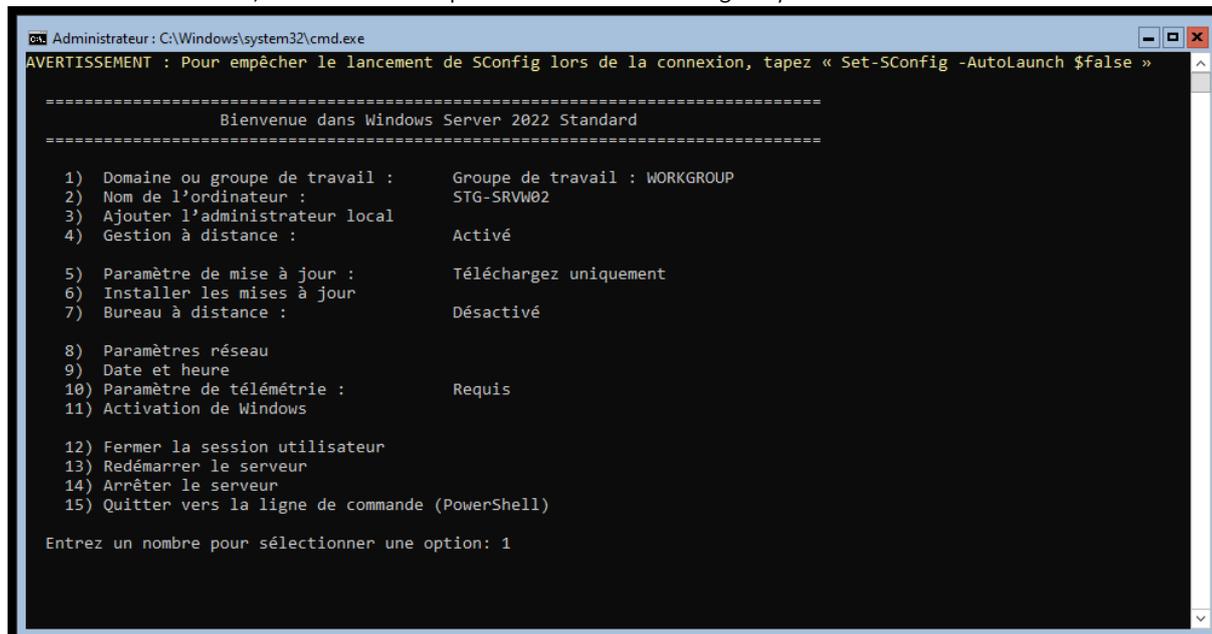
Non, j'activerai cette étendue ultérieurement

< Précédent Suivant > Annuler

Contenu du serveur DHCP	État	Description	Relation de basculement
Étendue [192.168.1.0] test	** Actif **	test	
Options de serveur			
Stratégies			
Filtres			

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

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



```

Administrateur: C:\Windows\system32\cmd.exe
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig -AutoLaunch $false »

=====
                    Bienvenue dans Windows Server 2022 Standard
=====

 1) Domaine ou groupe de travail :   Groupe de travail : WORKGROUP
 2) Nom de l'ordinateur :           STG-SRVW02
 3) Ajouter l'administrateur local
 4) Gestion à distance :           Activé

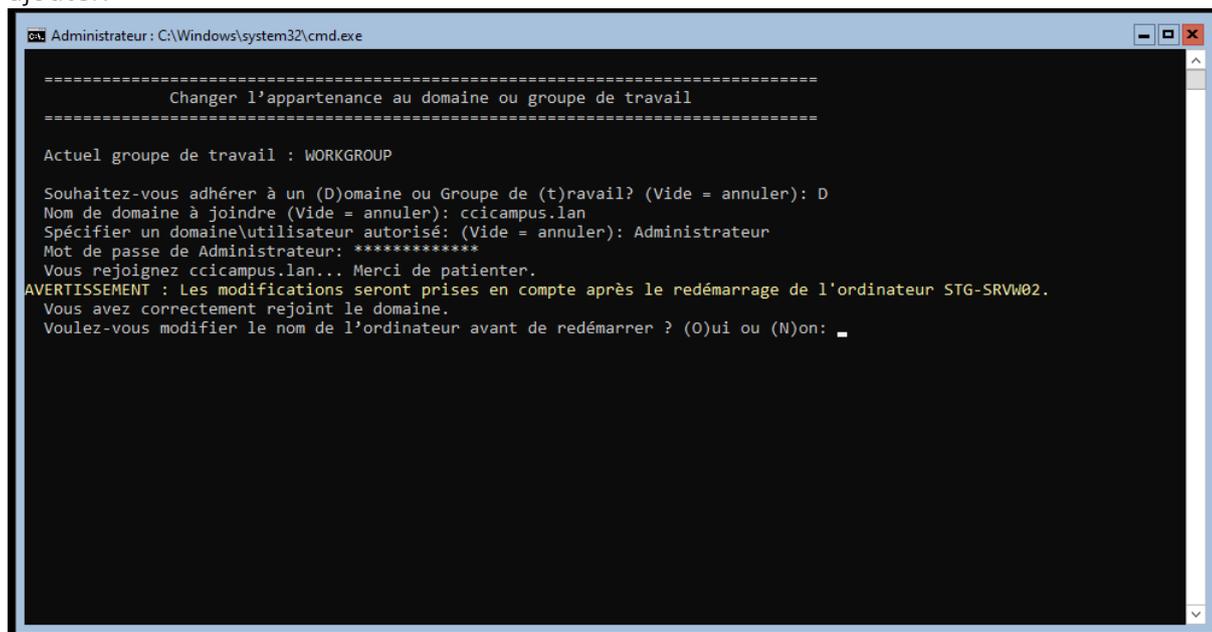
 5) Paramètre de mise à jour :       Téléchargez uniquement
 6) Installer les mises à jour
 7) Bureau à distance :             Désactivé

 8) Paramètres réseau
 9) Date et heure
10) Paramètre de télémétrie :       Requis
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 1
  
```

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



```

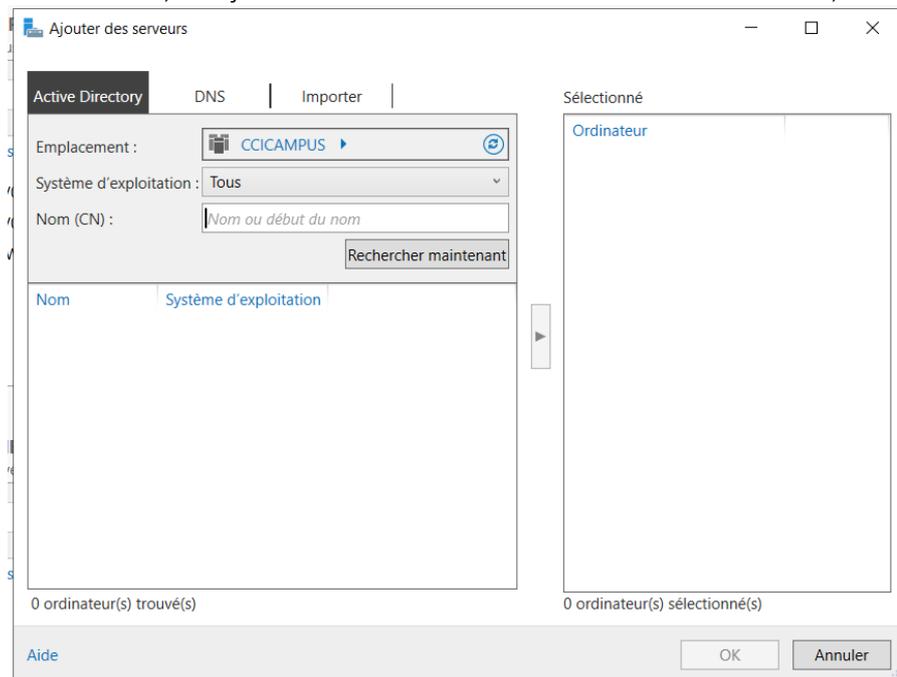
Administrateur: C:\Windows\system32\cmd.exe

=====
                    Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ccicampus.lan
Spécifier un domaine/utilisateur autorisé: (Vide = annuler): Administrateur
Mot de passe de Administrateur: *****
Vous rejoignez ccicampus.lan... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur STG-SRVW02.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on:
  
```

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.

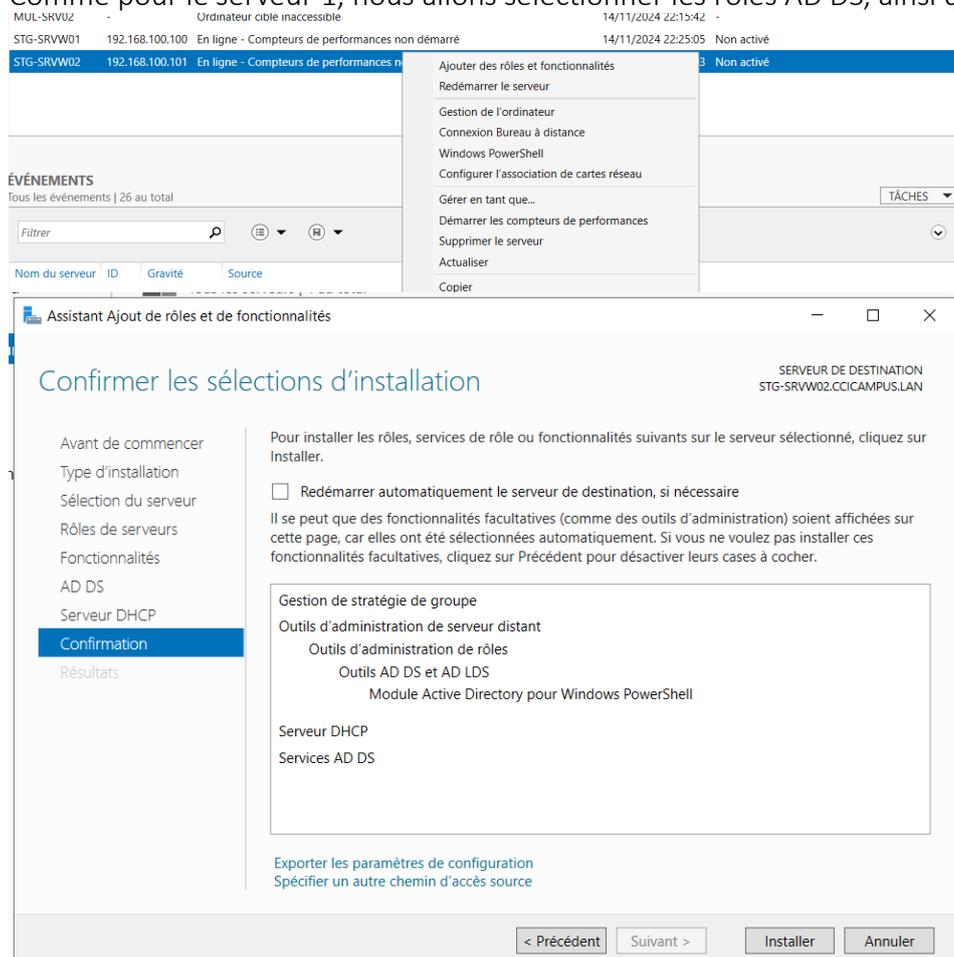


Nous pourrions alors apercevoir que le serveur apparaît En Ligne.

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
MUL-SRV01	-	Ordinateur cible inaccessible	14/11/2024 22:15:42	-
MUL-SRV02	-	Ordinateur cible inaccessible	14/11/2024 22:15:42	-
STG-SRVW01	192.168.100.100	En ligne - Compteurs de performances non démarré	14/11/2024 22:15:04	Non activé
STG-SRVW02	192.168.100.101	En ligne - Compteurs de performances non démarré	14/11/2024 22:25:03	Non activé

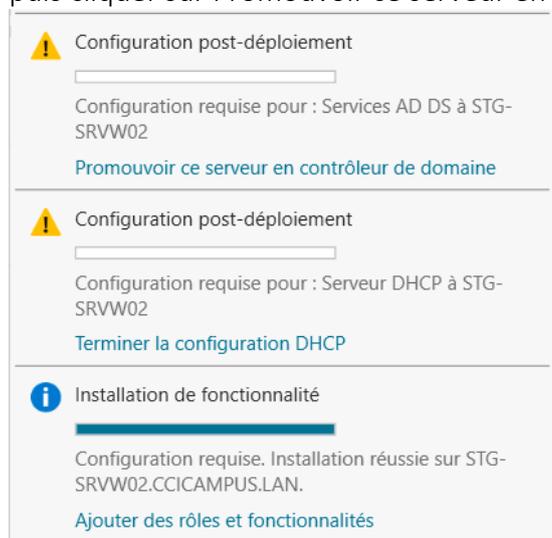
Installation des rôles AD DS et DHCP sur le second serveur.

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.

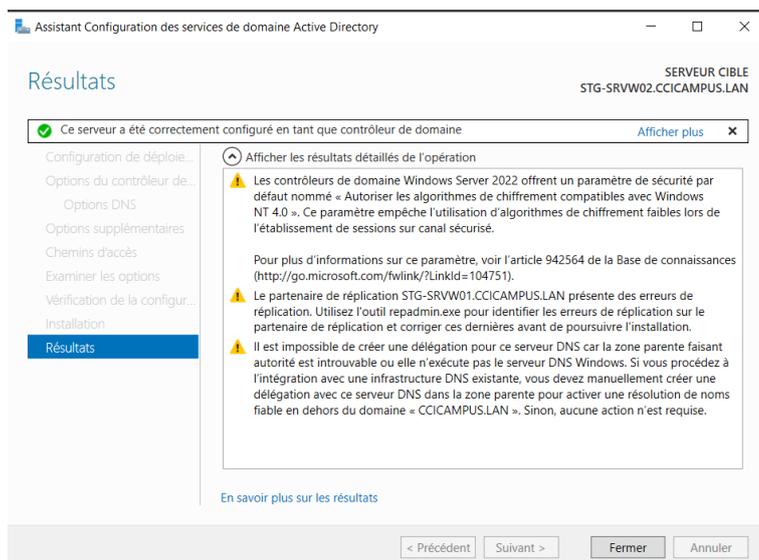
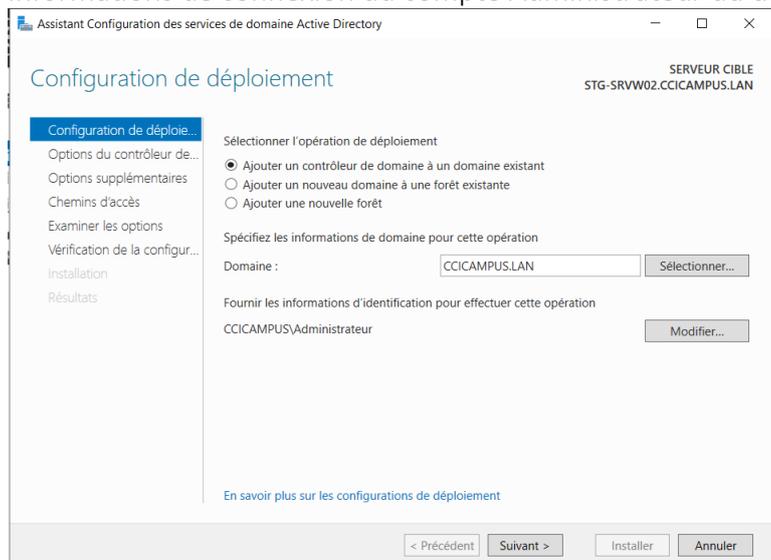


Concernant la configuration du DHCP, elle est identique à celle réalisée auparavant sur le premier serveur.

Pour la configuration de la réplcation 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.



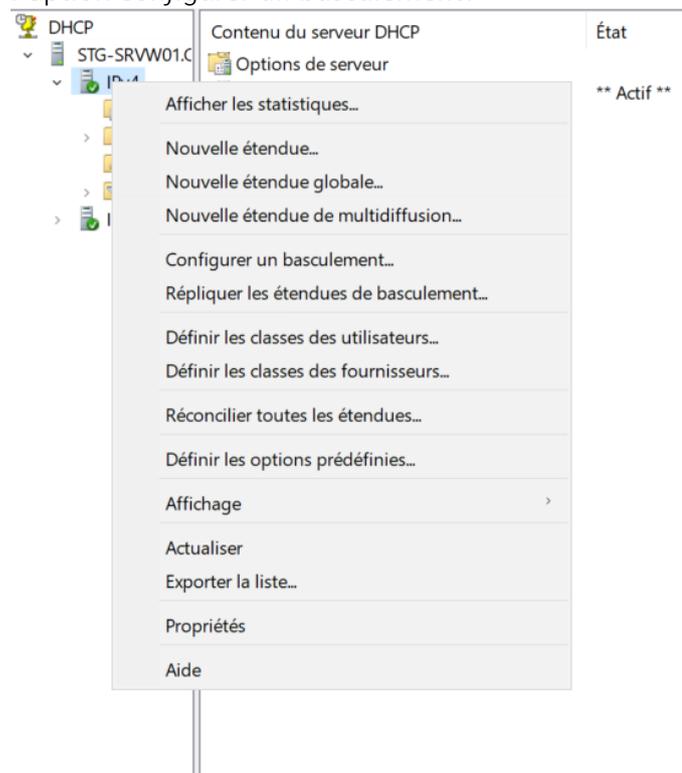
Une fois cela fait, nous allons rentrer le domaine déjà existant ici, il faudra également rentrer les informations de connexion du compte Administrateur du domaine.



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.

The screenshot shows the 'Configurer un basculement' dialog box with the 'Créer une relation de basculement' tab selected. The configuration is for a backup relationship with partner 'stg-srw2'. The fields are as follows:

- Nom de la relation : stg-srvw01.cccampus.lan-stg-srw2
- Délai de transition maximal du client (MCLT) : 1 heures, 0 minutes
- Mode : Serveur de secours
- Rôle du serveur partenaire : Veille
- Adresses réservées pour le serveur de secours : 5 %
- Intervalle de basculement d'état : 60 minutes (checkbox is unchecked)
- Activer l'authentification du message : (checkbox is checked)
- Secret partagé : (empty text box)

Navigation buttons at the bottom: < Précédent, Suivant >, Annuler.

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

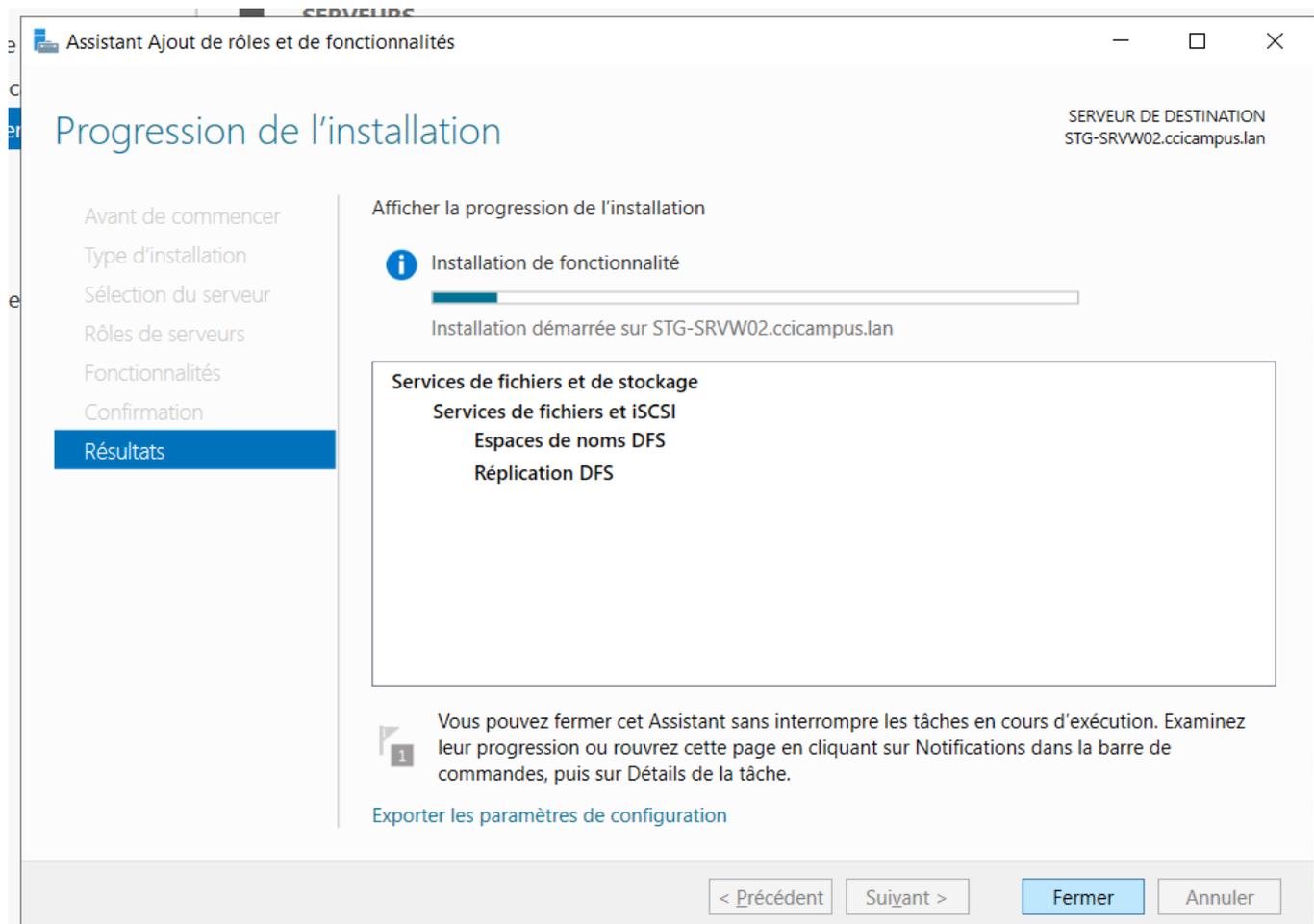
Installation d'un serveur Windows SERVER 2022 avec les services DFS et DFSR

Prérequis :

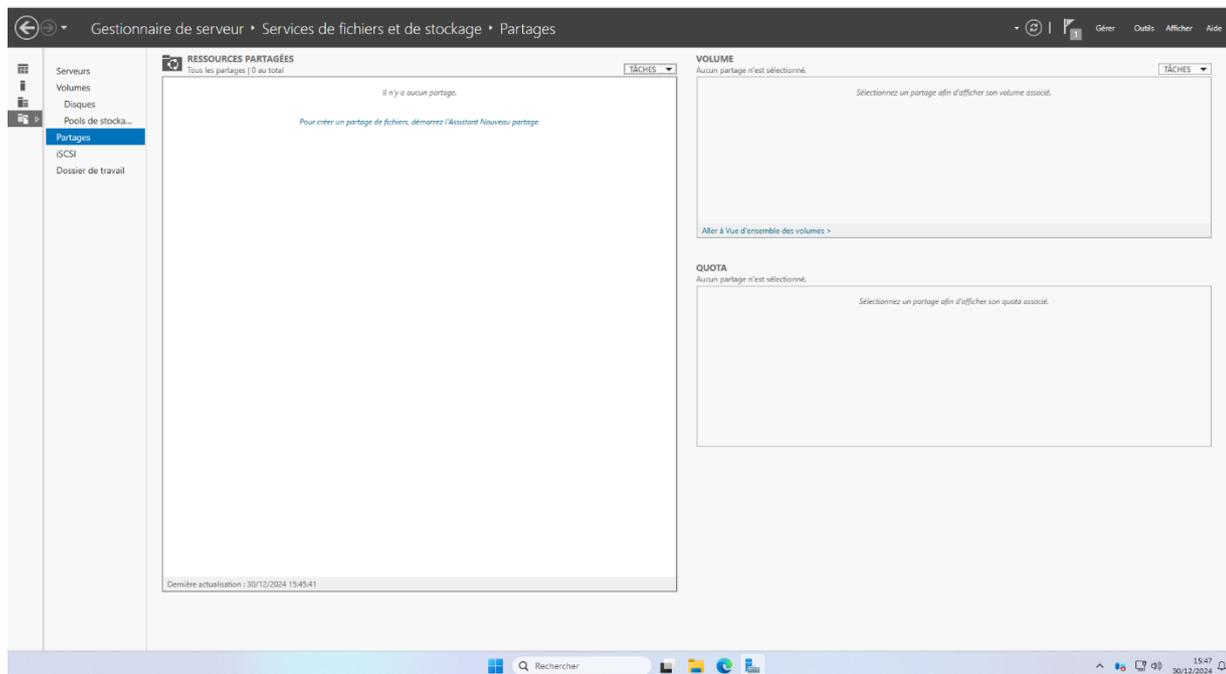
- 1 Windows SERVER 2022 avec interface graphique
- 1 serveur d'annuaire d'authentification (dans ce cas, active directory) avec un domaine (optionnel)

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)

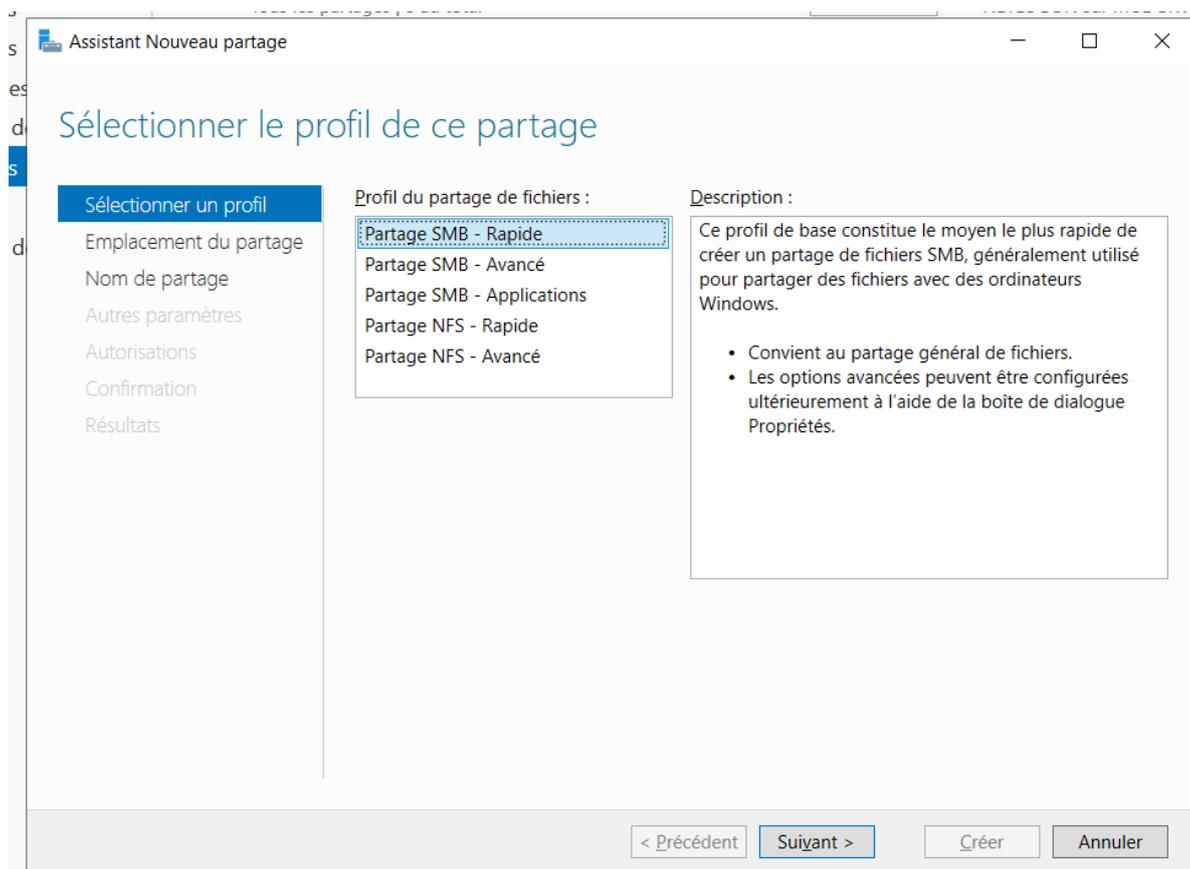
Ajoutez le rôle DFS et Réplication DFS au serveur



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 pourrions également choisir son emplacement.

Assistant Nouveau partage

Sélectionner le serveur et le chemin d'accès au partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Nœud propriétaire
MUL-SRVW01	En ligne	Non-cluster	
MUL-SRVW02	En ligne	Non-cluster	
STG-SRVW01	En ligne	Non-cluster	
STG-SRVW02	En ligne	Non-cluster	

Emplacement du partage :

Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
B:	59,6 Go	59,7 Go	NTFS
C:	48,5 Go	60,0 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

Tapez un chemin personnalisé :

< Précédent **Suivant >** Créer Annuler

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

Assistant Nouveau partage

Indiquer le nom de partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Nom du partage :

Description du partage :

Chemin d'accès local au partage :

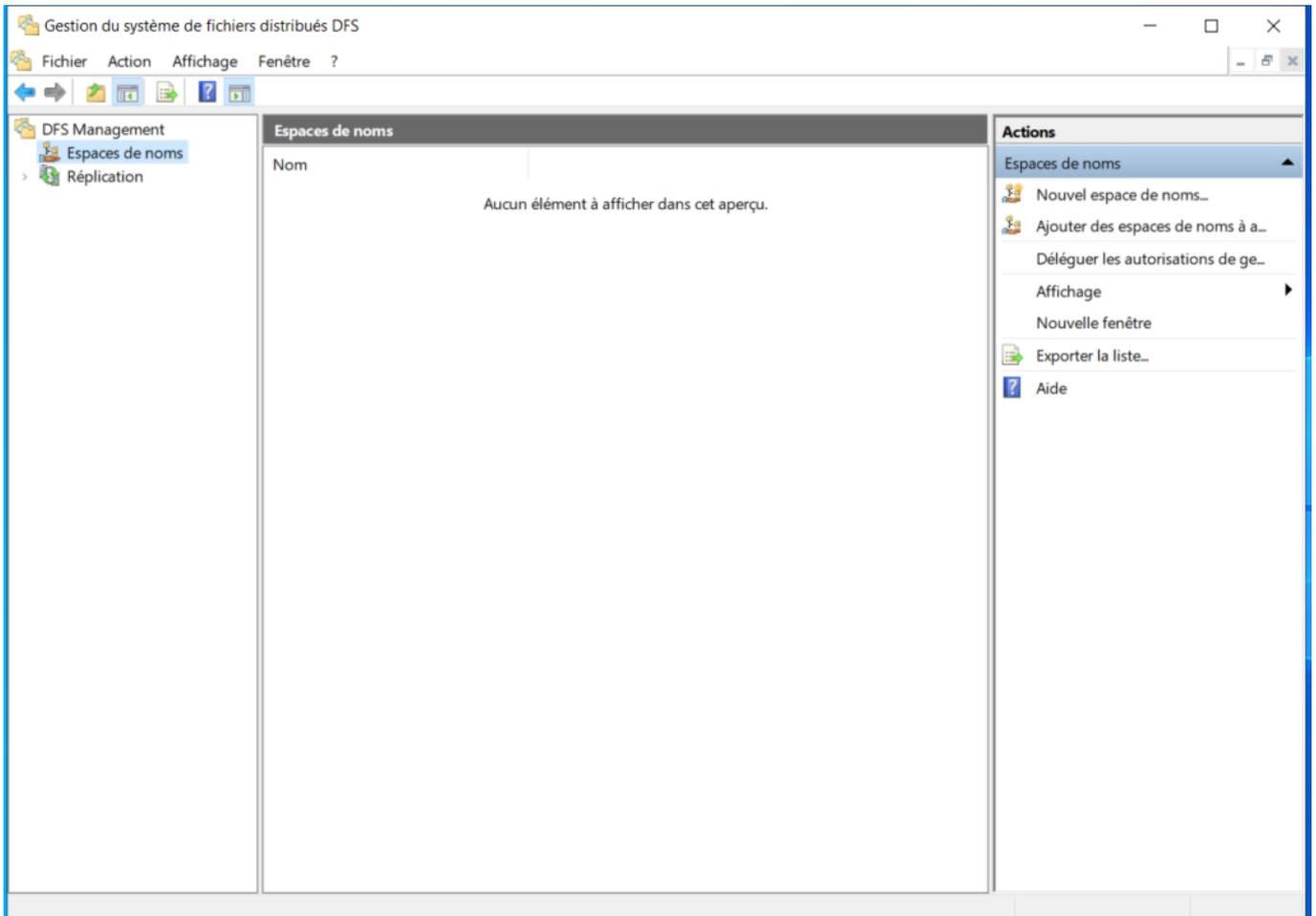
Si le dossier n'existe pas, il est créé.

Chemin d'accès distant au partage :

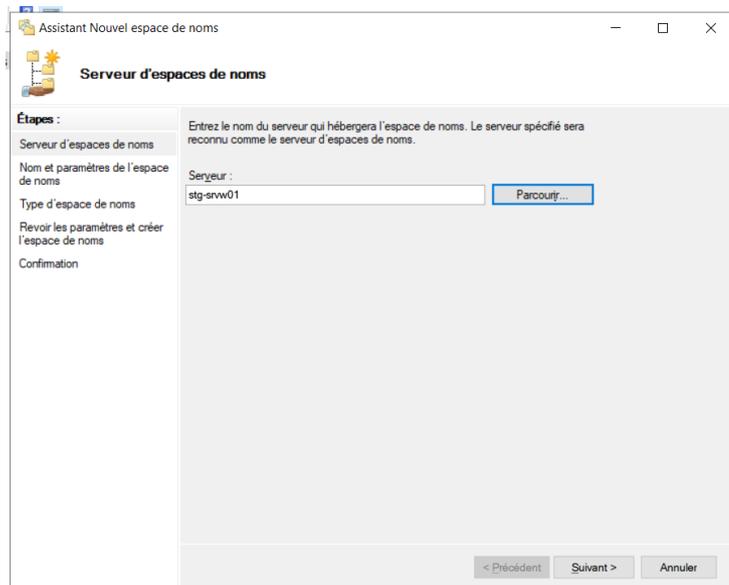
< Précédent **Suivant >** Créer Annuler

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

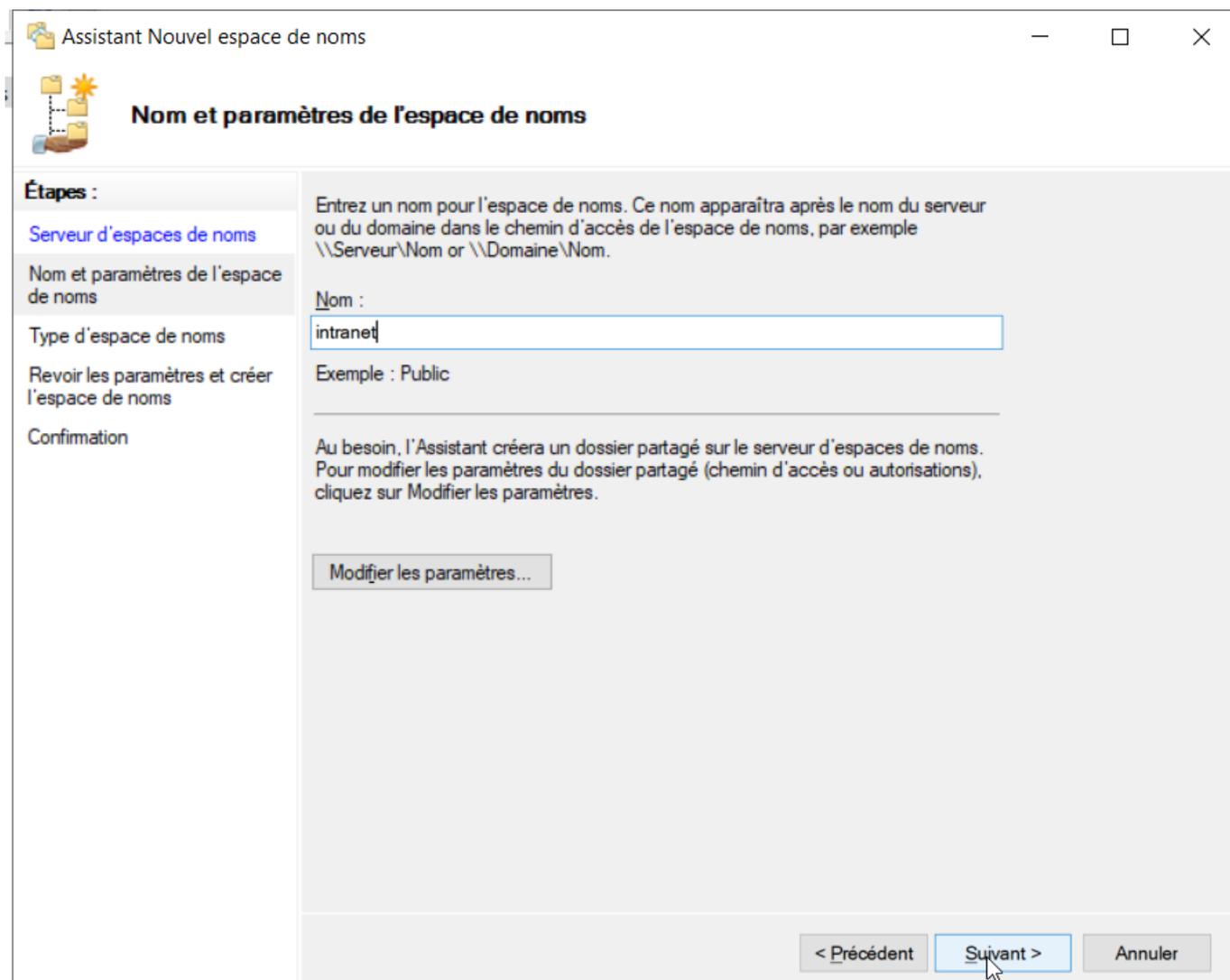
Rentrez dans la console DFS pour créer l'espace de nom



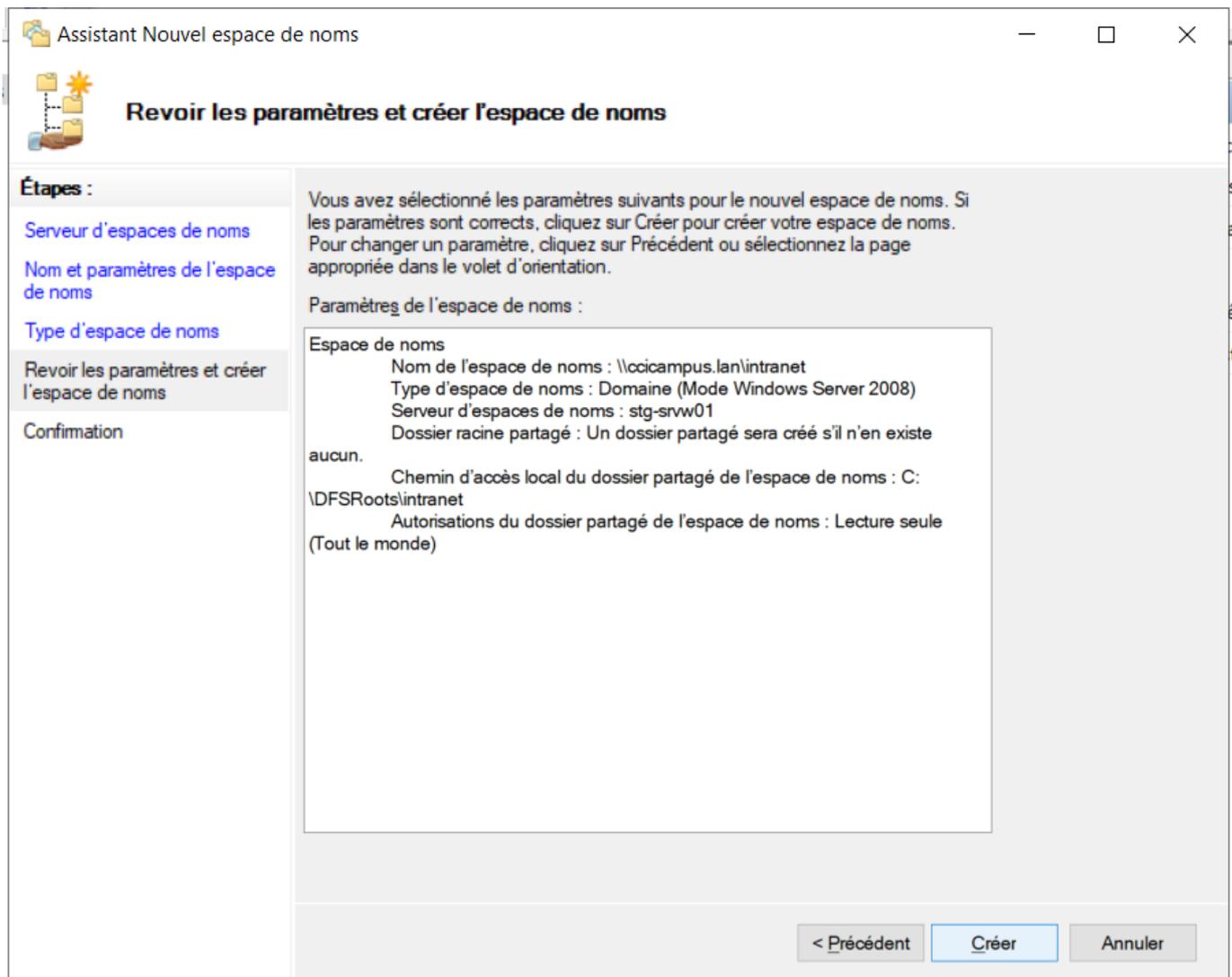
Une fois dedans, créez l'espace de nom avec les paramètres que vous désirez



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

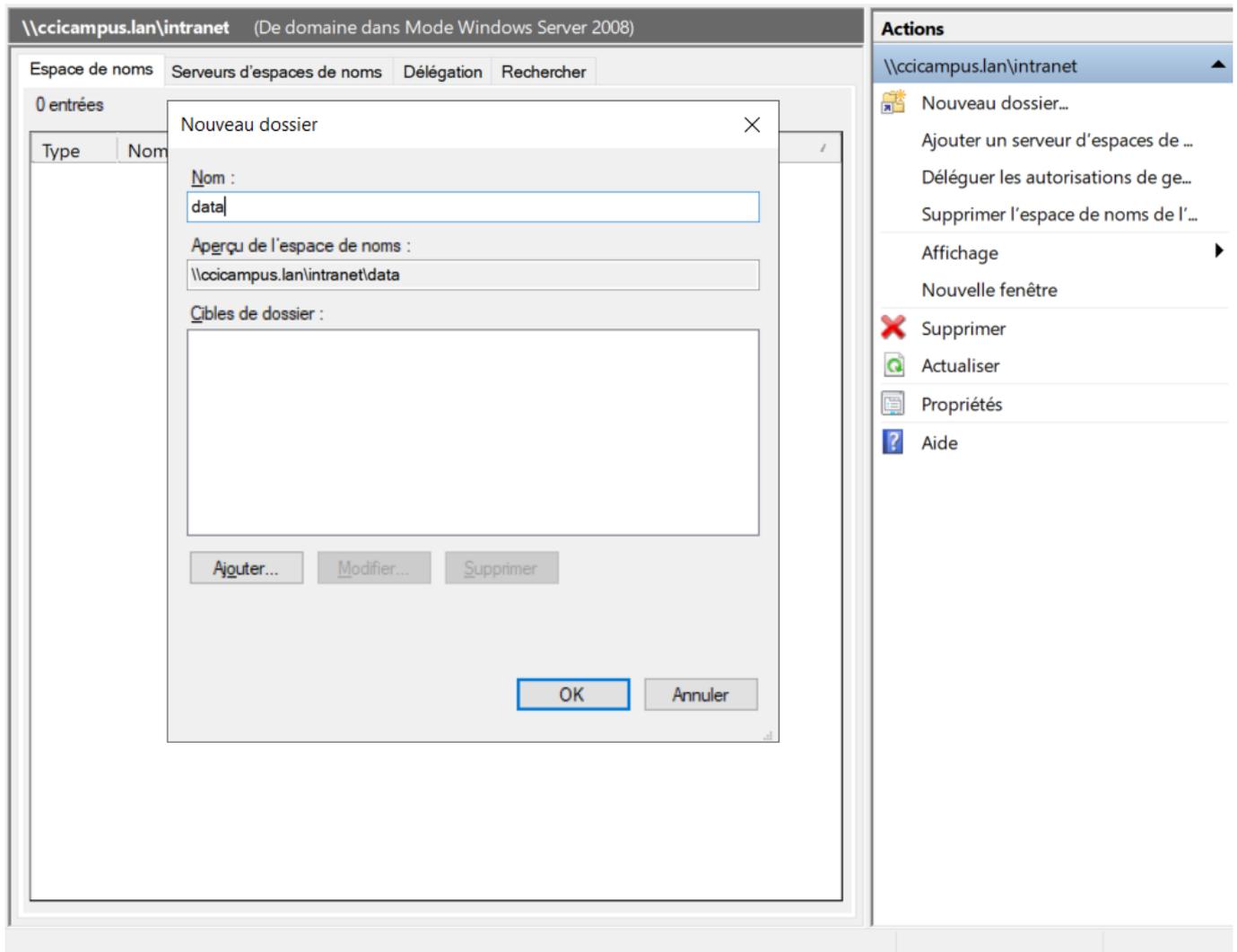


Une fois cela fait, l'espace de nom sera créé

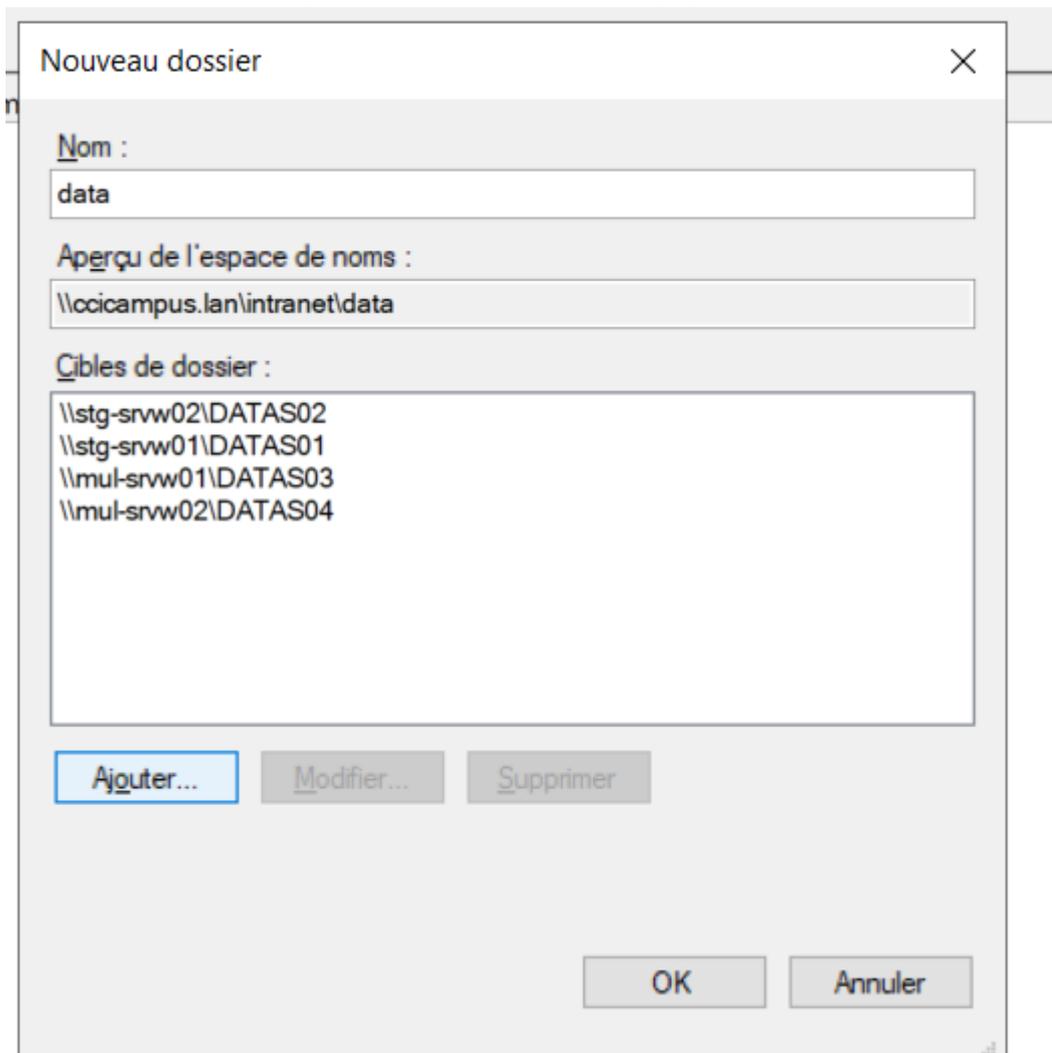


Création du dossier de l'espace de nom DFS :

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

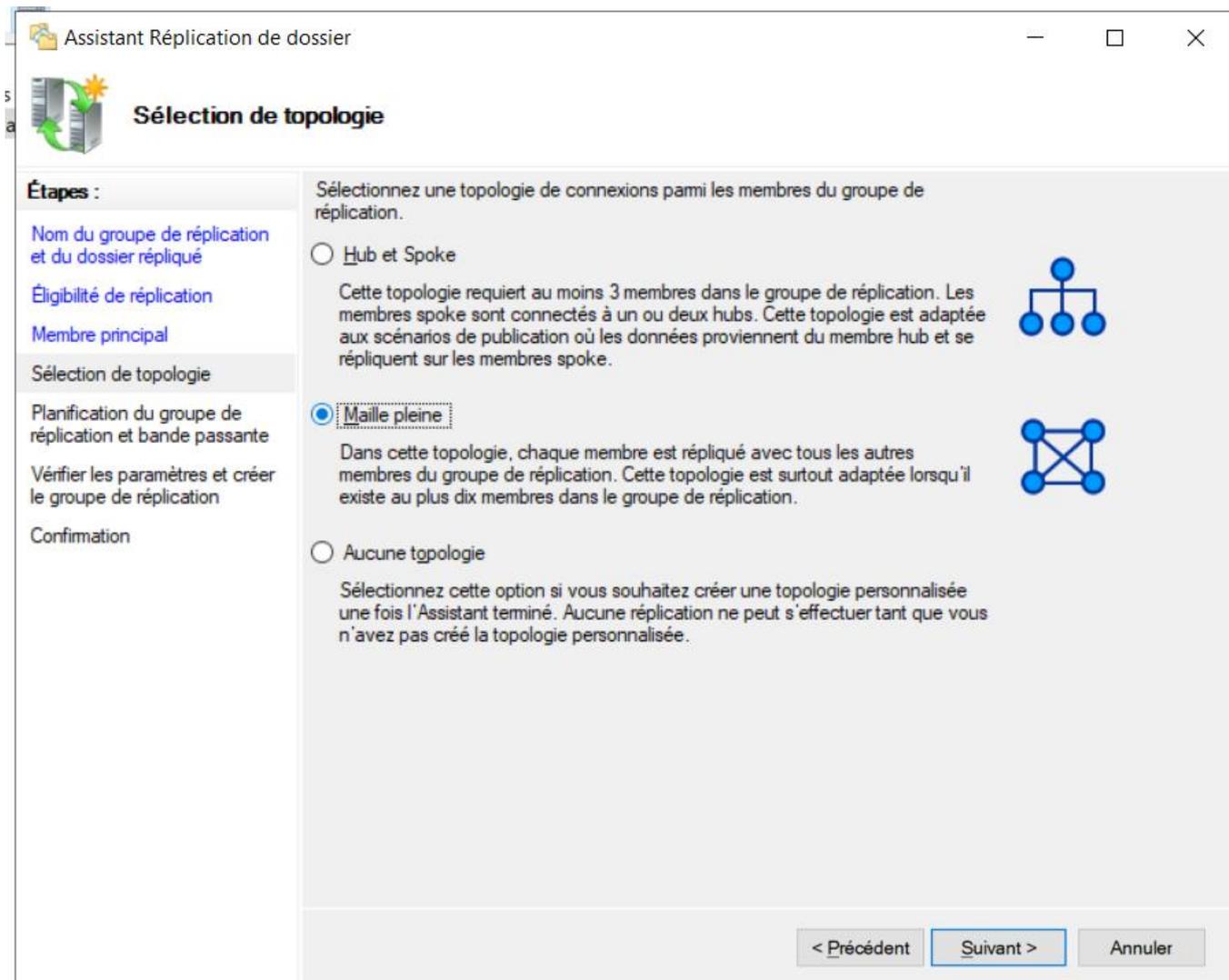
Cet Assistant a évalué les cibles de dossier pour déterminer si elles peuvent participer à la réplication DFS. Pour plus de détails, voir la colonne Éligibilité ci-dessous.

Détails :

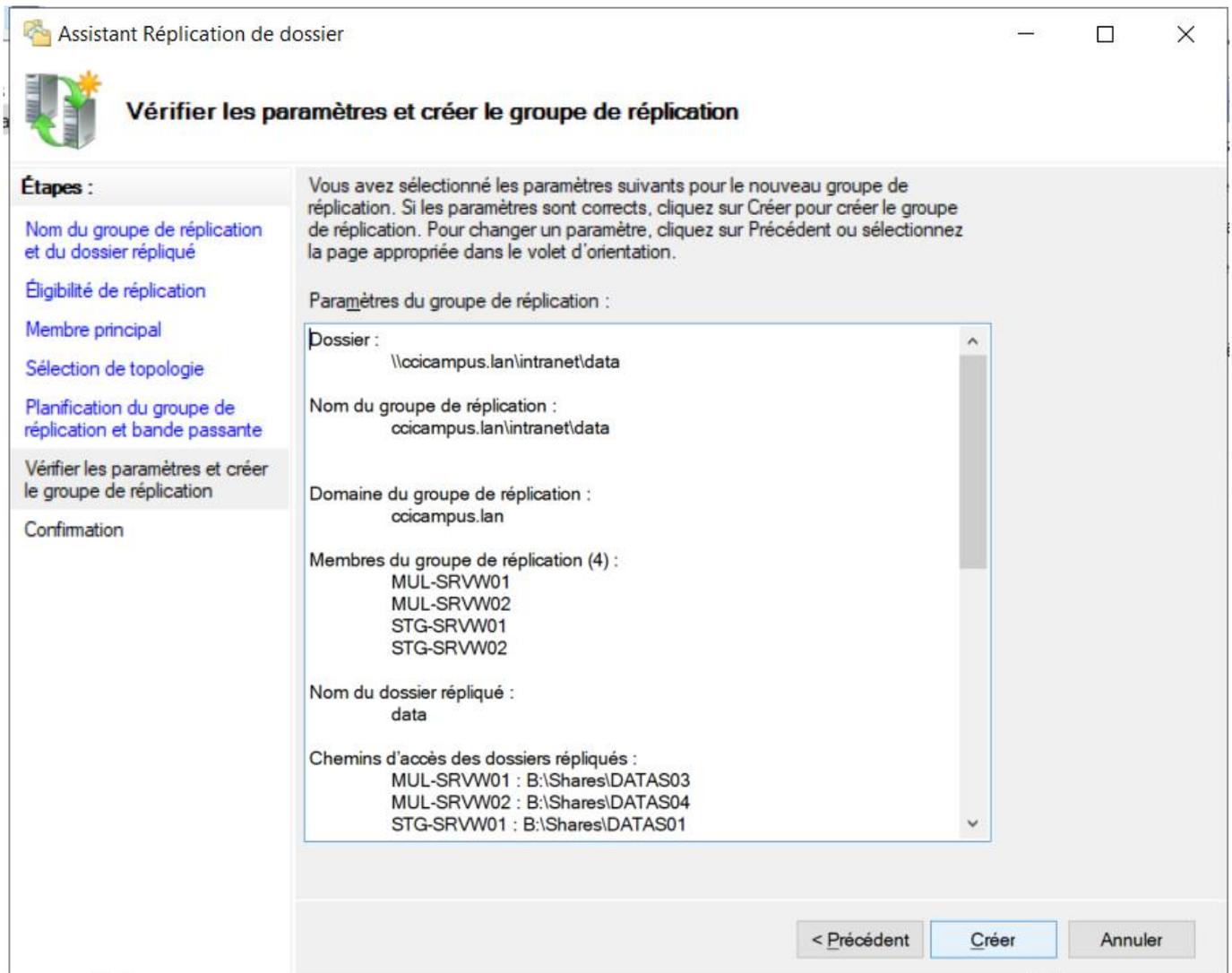
Cible de dossier	Éligibilité
\\mul-srvw01\DATAS03	Ajouter un membre de réplication DFS
\\mul-srvw02\DATAS04	Ajouter un membre de réplication DFS
\\stg-srvw01\DATAS01	Ajouter un membre de réplication DFS
\\stg-srvw02\DATAS02	Ajouter un membre de réplication DFS

< Précédent Suivant > Annuler

Nous allons choisir la topologie 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

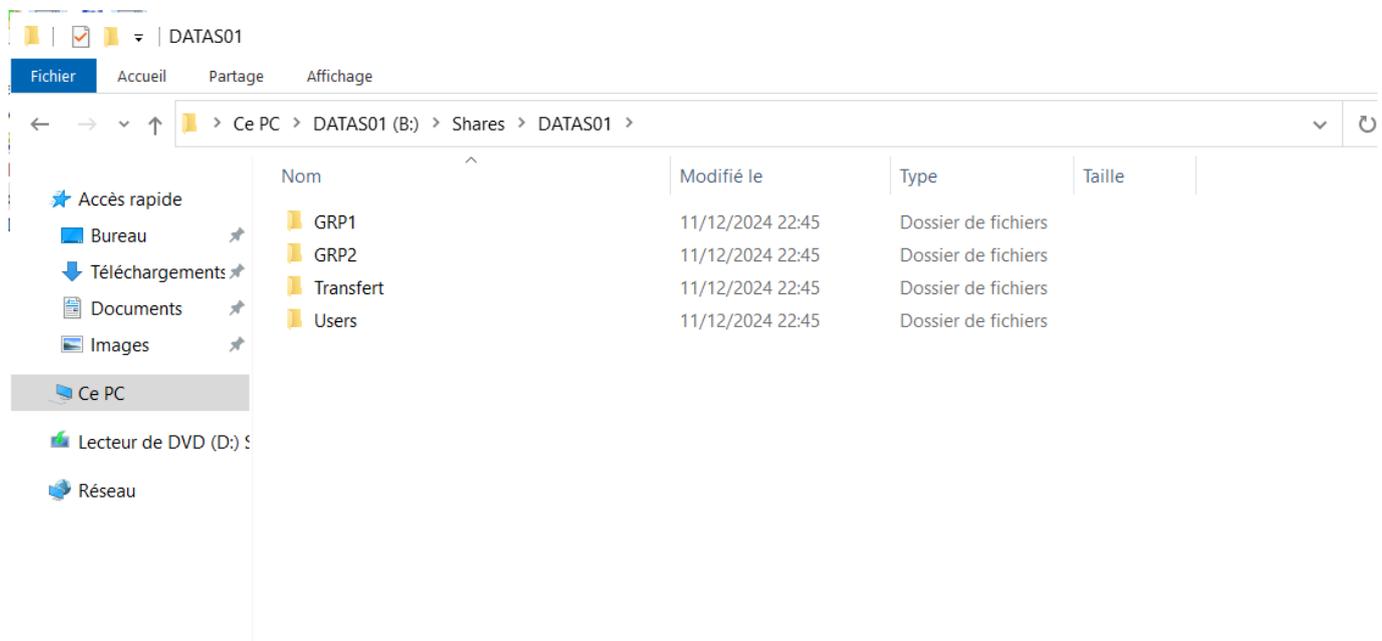
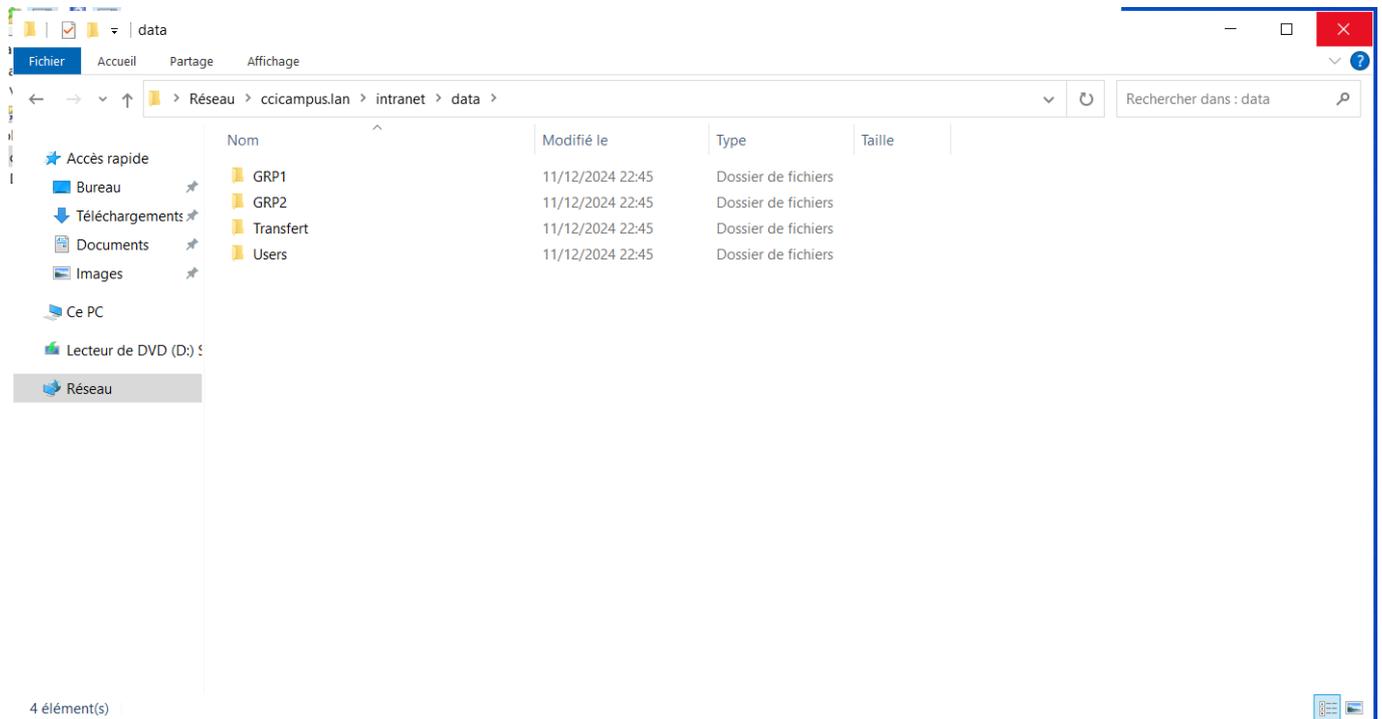
Dans la console DFS, sous espace de nom, nous pouvons vérifier alors les différentes cibles dans la partie Serveurs d'espace de nom

The screenshot shows the DFS console for the domain \\ccicampus.lan\intranet. The left pane displays a table with 4 entries, all of which are active and point to the Default-First-Site-Name. The right pane shows the context menu for the selected name space, including options like 'Nouveau dossier...', 'Ajouter un serveur d'espaces de ...', 'Déléguer les autorisations de ge...', 'Supprimer l'espace de noms de l'...', 'Affichage', 'Nouvelle fenêtre', 'Supprimer', 'Actualiser', 'Propriétés', and 'Aide'.

Type	Statut de référence	Site	Chemin d'accès
	Activé	Default-First-Site-Name	\\MUL-SRVW01.ccicampus...
	Activé	Default-First-Site-Name	\\MUL-SRVW02.ccicampus...
	Activé	Default-First-Site-Name	\\STG-SRVW01.ccicampus...
	Activé	Default-First-Site-Name	\\STG-SRVW02.ccicampus...

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.

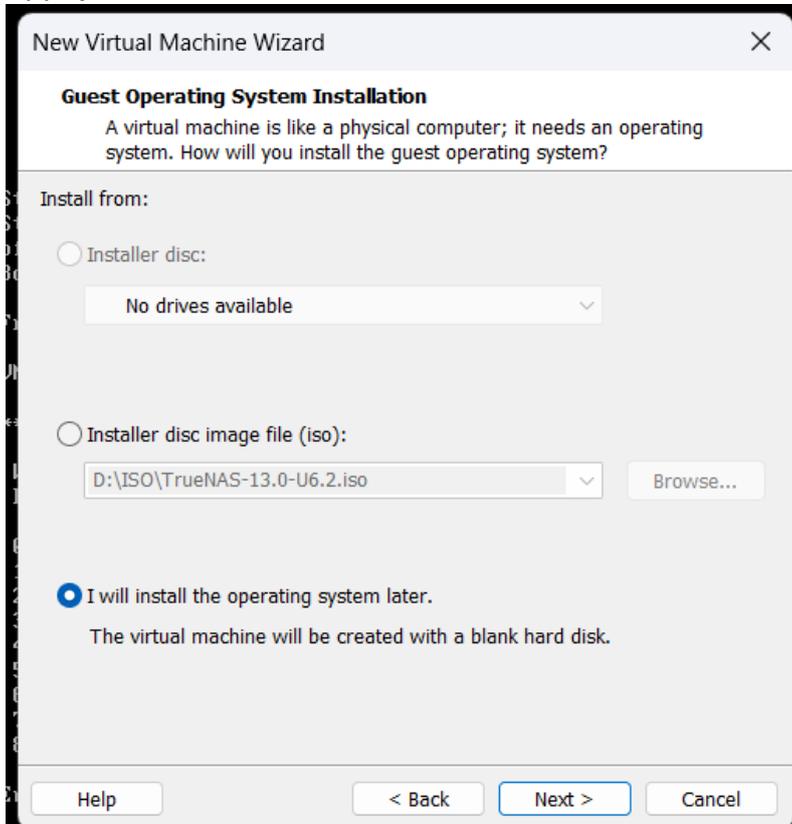
Une fois tout cela fini, nous verrons que l'espace de nom sera accessible, et que si l'on ajoute des dossiers ou des fichiers dedans, tout se répliquera sur les différents partages des cibles que l'on a créés auparavant.



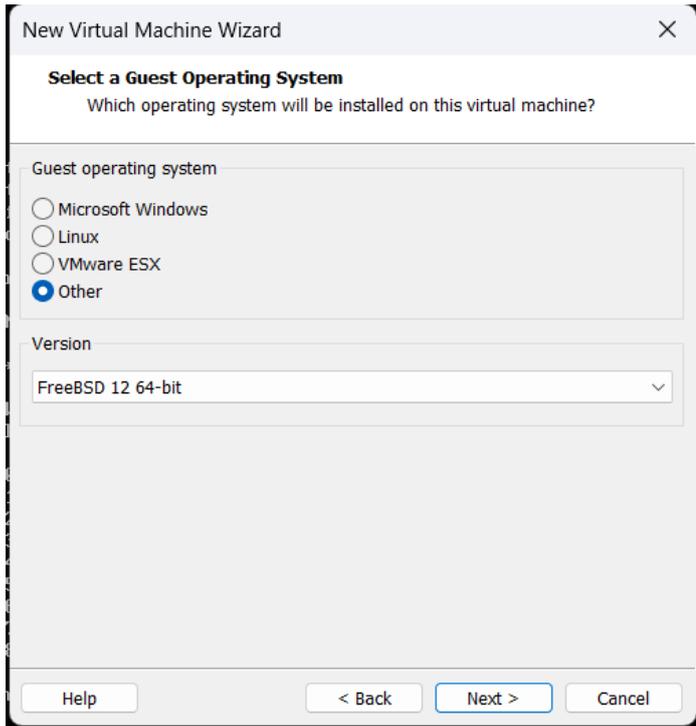
1.4) LOT 4 : Installation de TrueNAS et montage d'une cible iSCSi



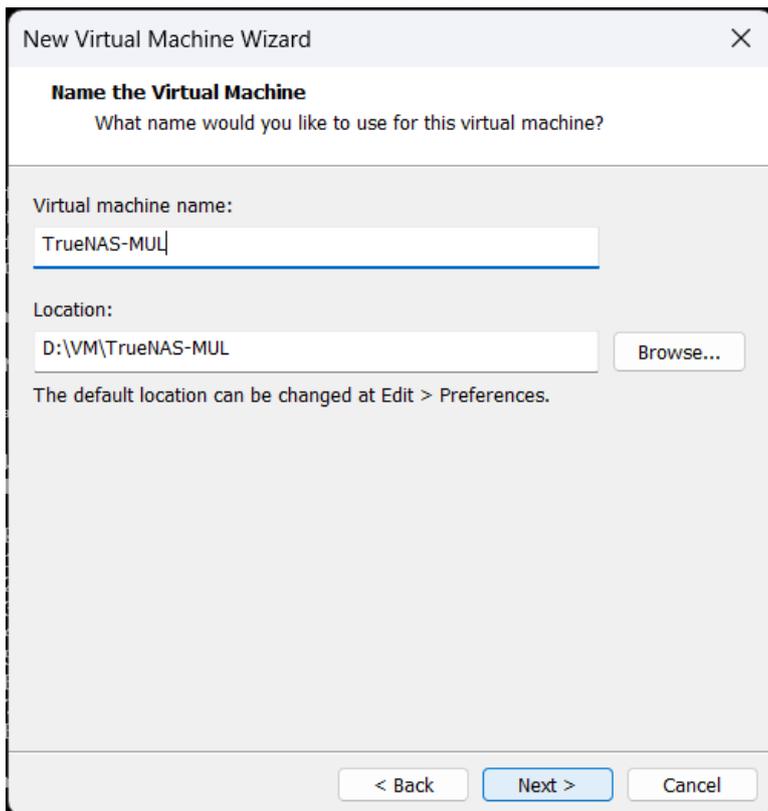
Appuyez sur next



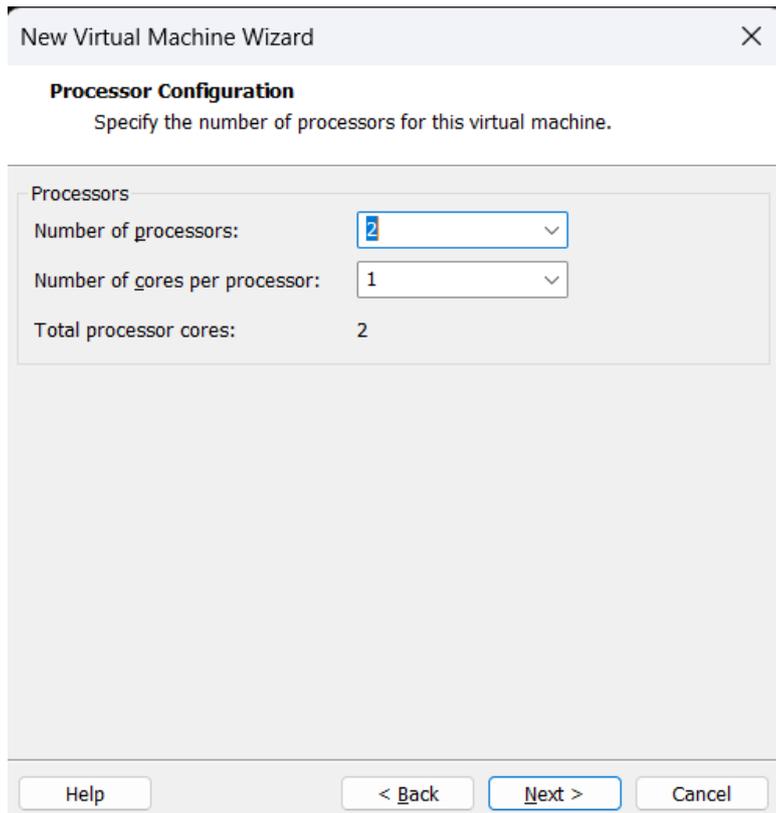
Cochez "I will install the operating system later".



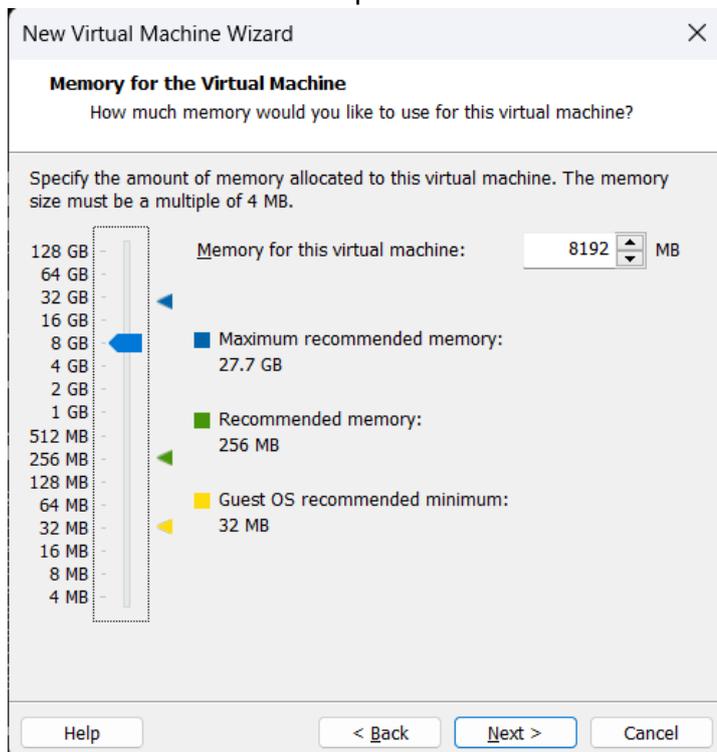
Sélectionnez "Other" et dans le menu déroulant choisissez "FreeBSB 12 64-bit"



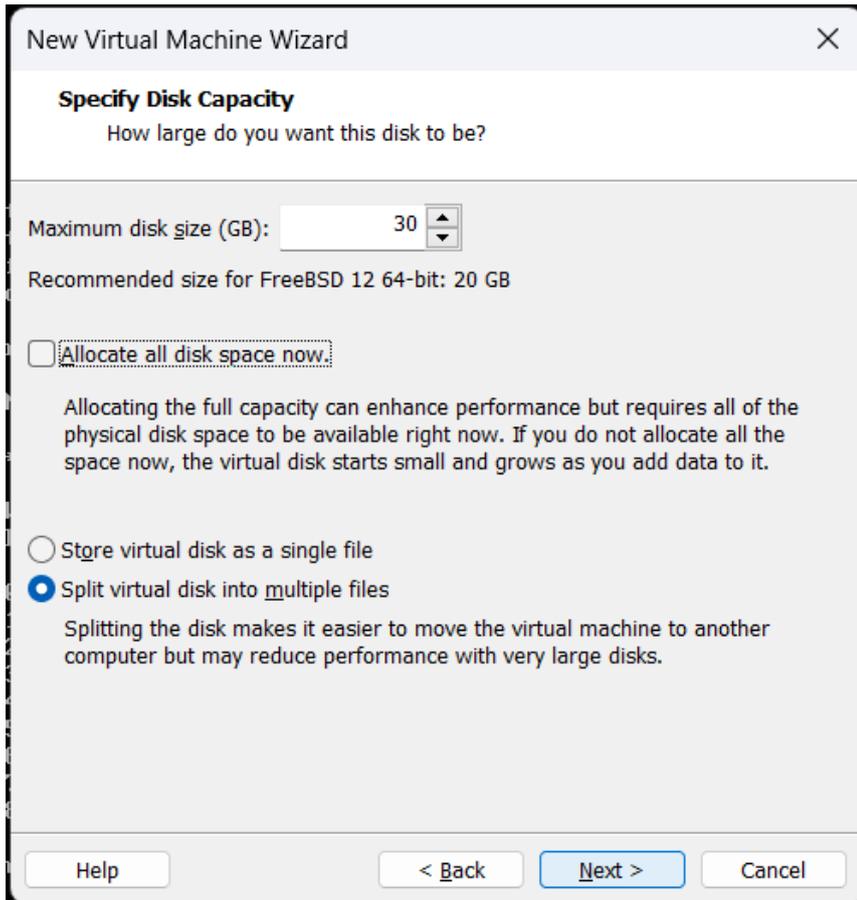
Rentrez le nom de votre machine virtuel dans mon cas "TrueNAS-MUL"



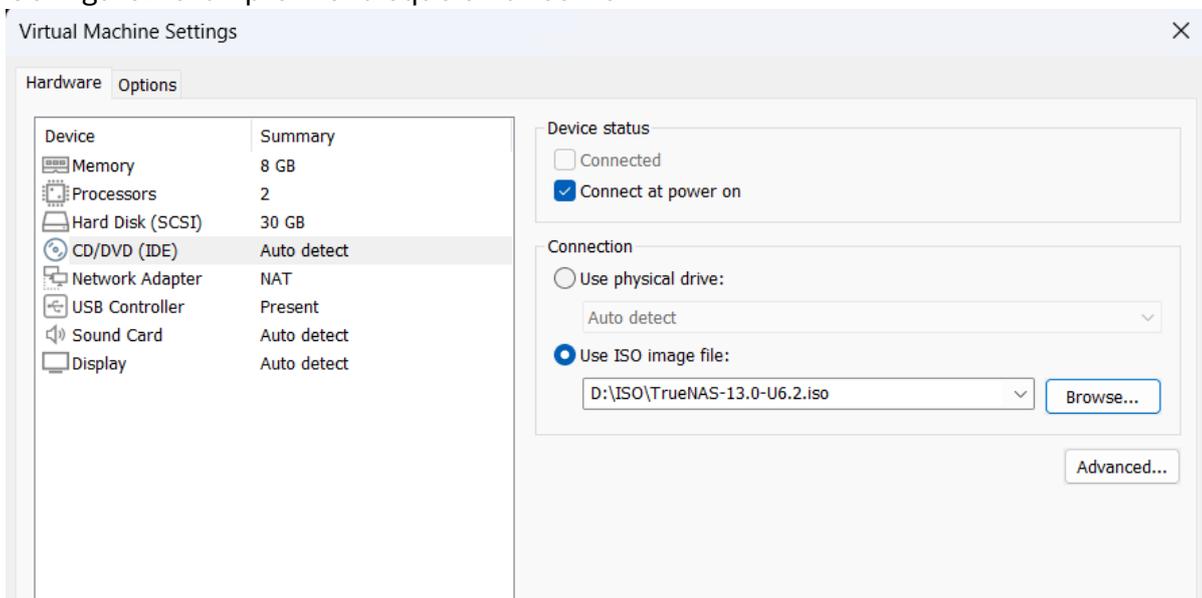
Choisissez le nombre de processeur à mettre dans votre configuration



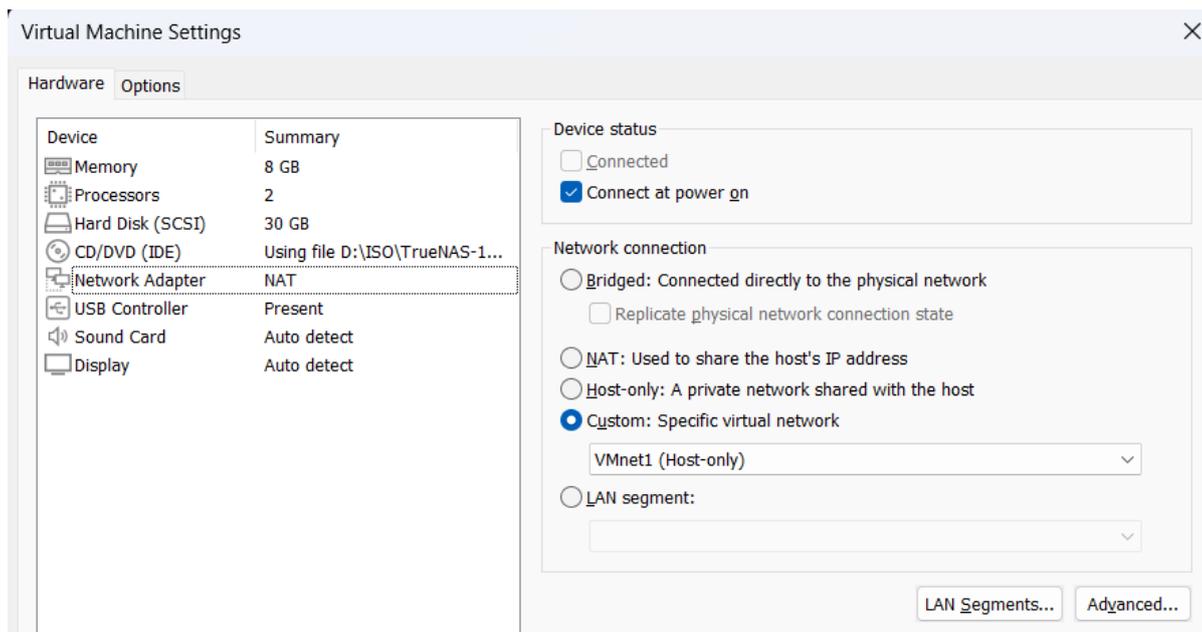
Veuillez bien respecter à mettre 8go de RAM car TrueNAS est assez gourmand.



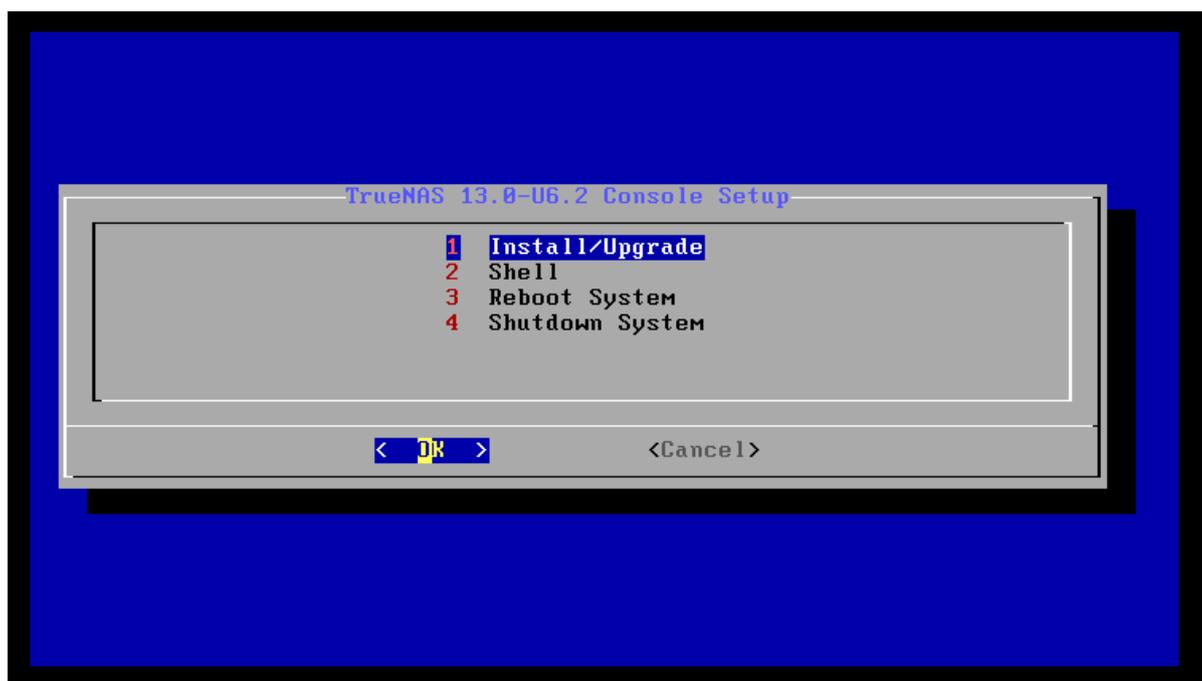
Configurez ici un premier disque et faites Next.



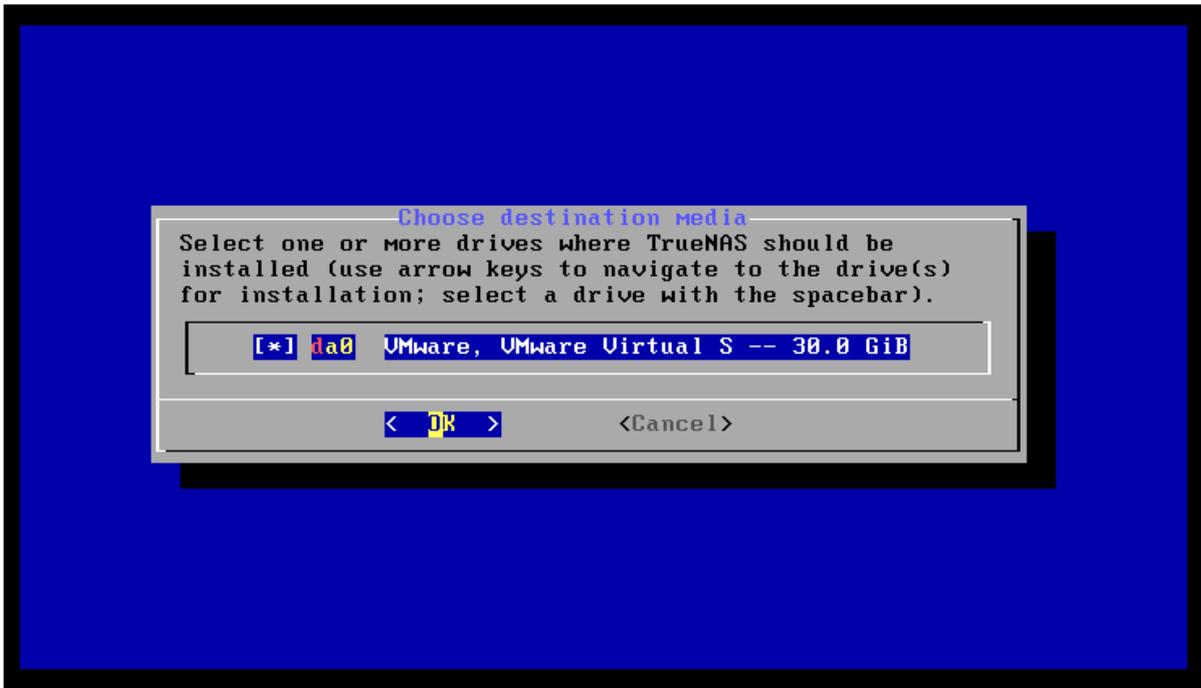
Maintenant allez dans les paramètres de la VM pour ajouter l'ISO de TrueNAS.



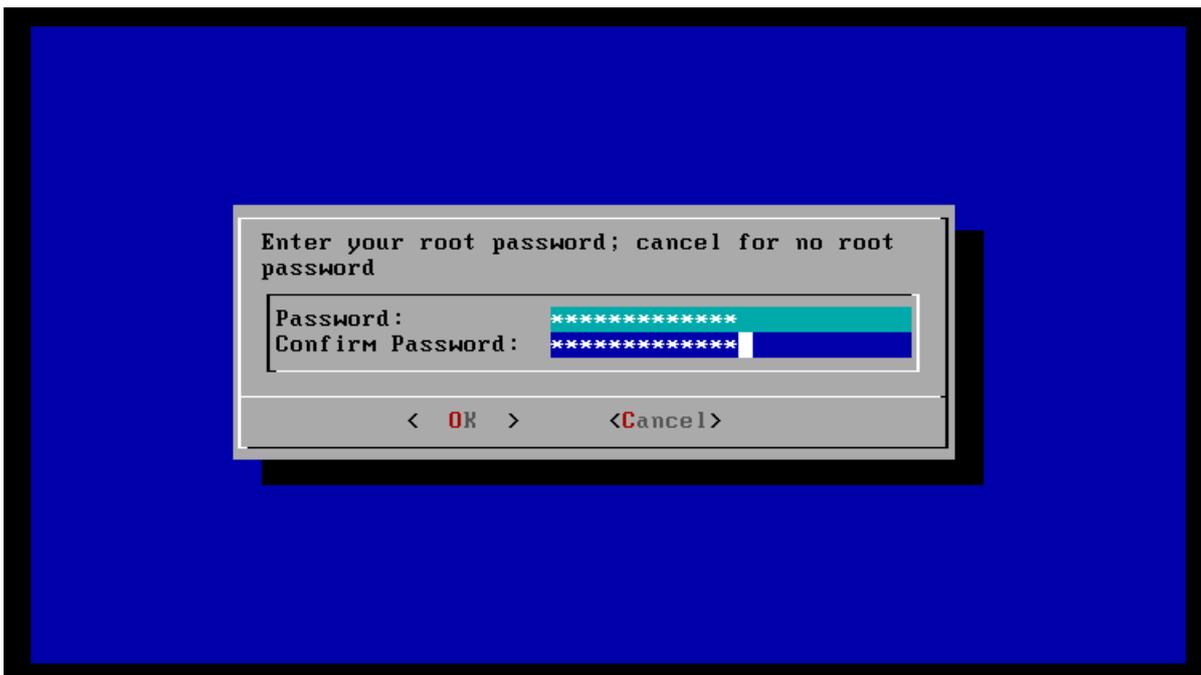
Dans Network Adapter ajoutez votre carte réseaux personnalisé pour qu'elle puisse bien communiquer avec tout le reste de votre infrastructure. On va aussi ajouter un autre disque de 50go.



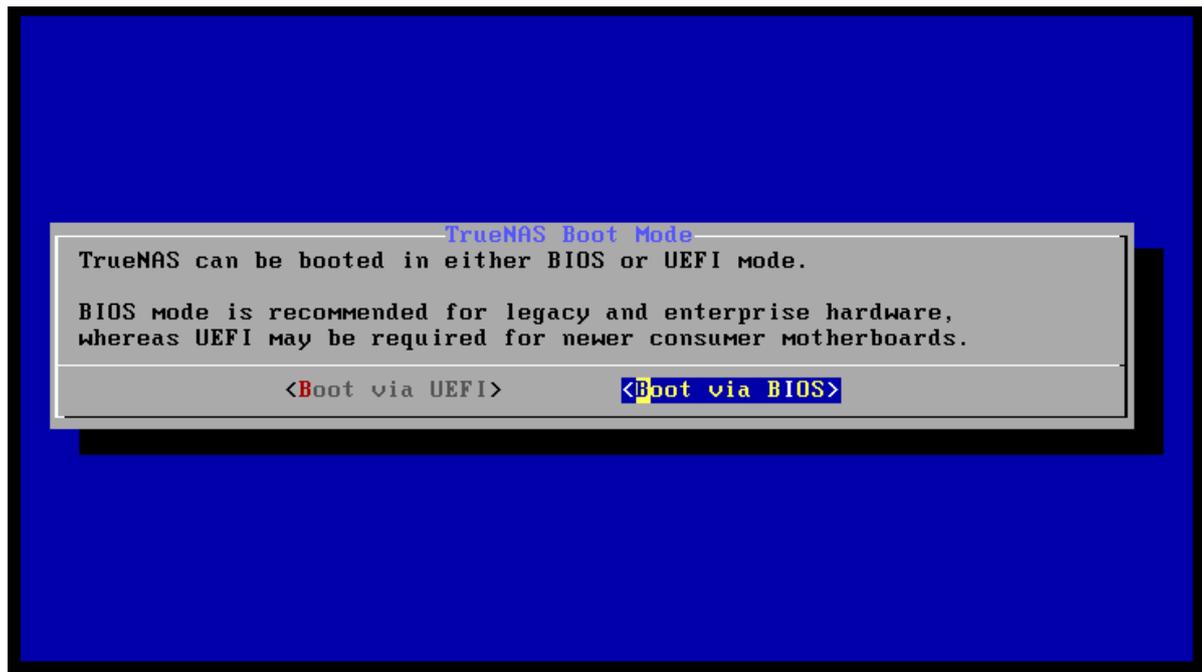
Vous pouvez maintenant lancer TrueNAS. Appuyez sur "Install/Upgrade".



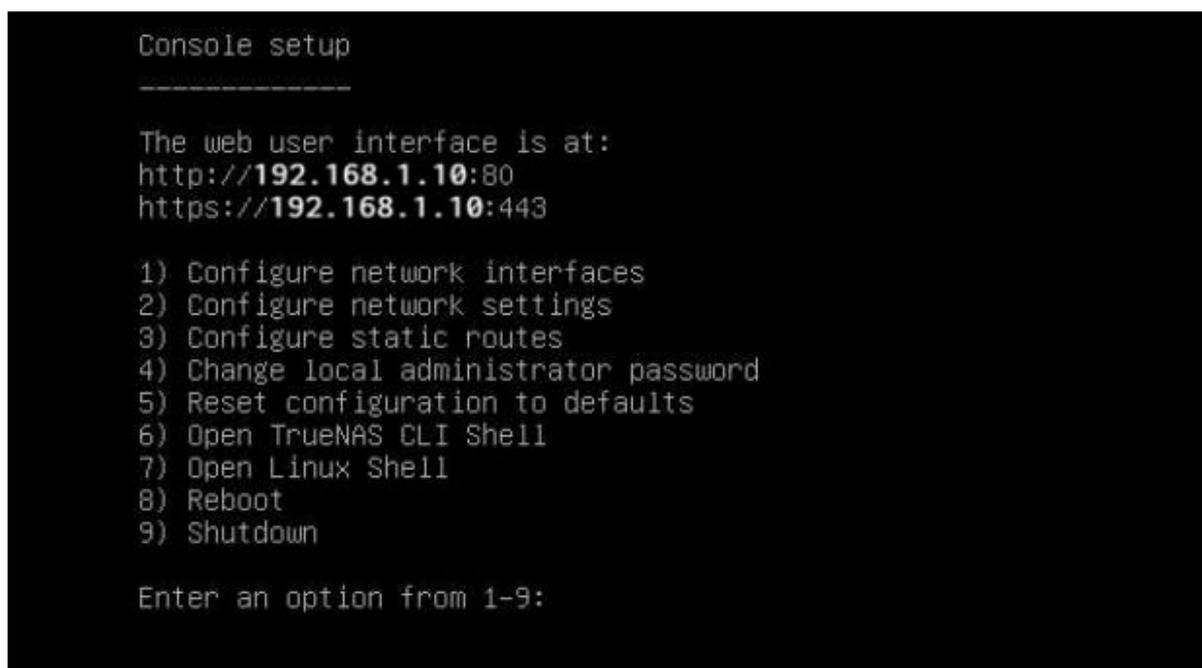
Faites OK.



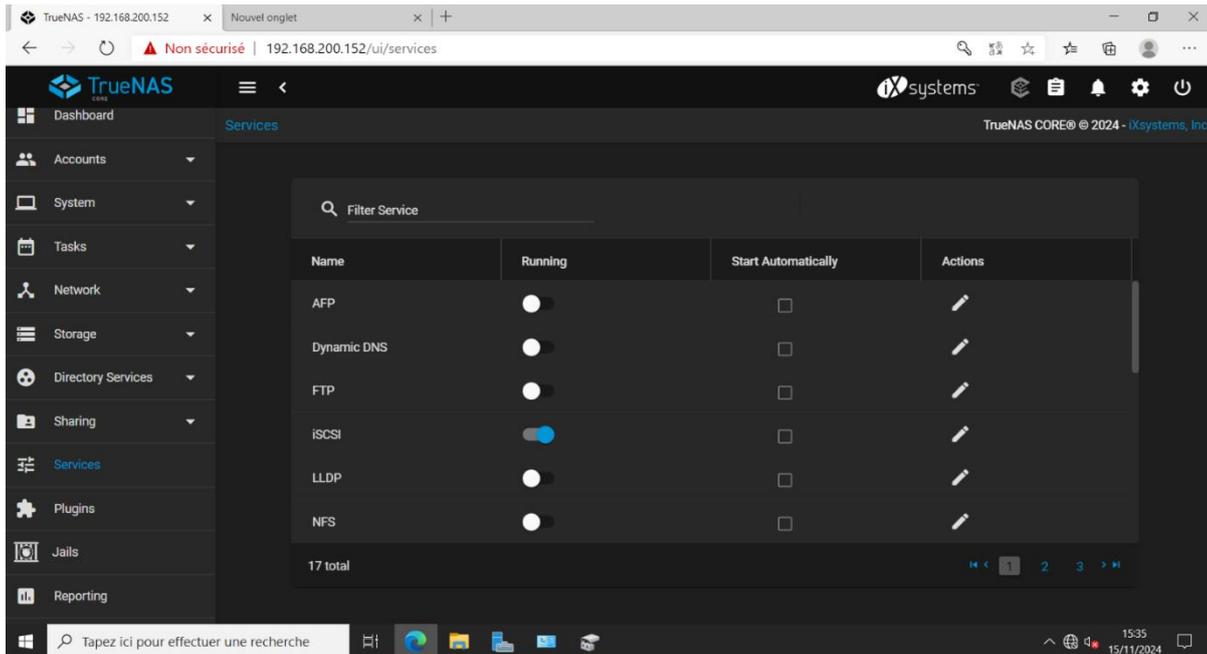
Configurez un mot de passe.



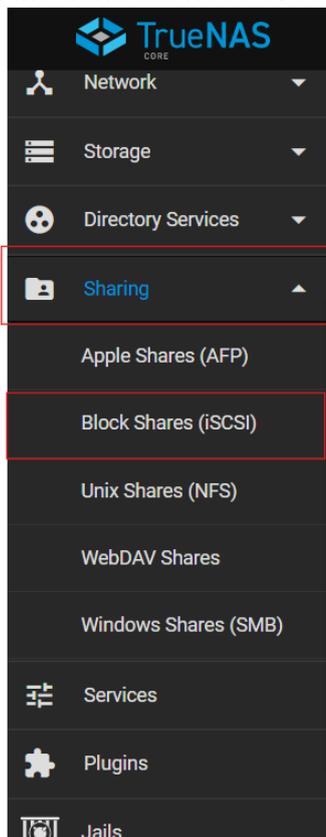
Et choisissez Boot via BIOS.



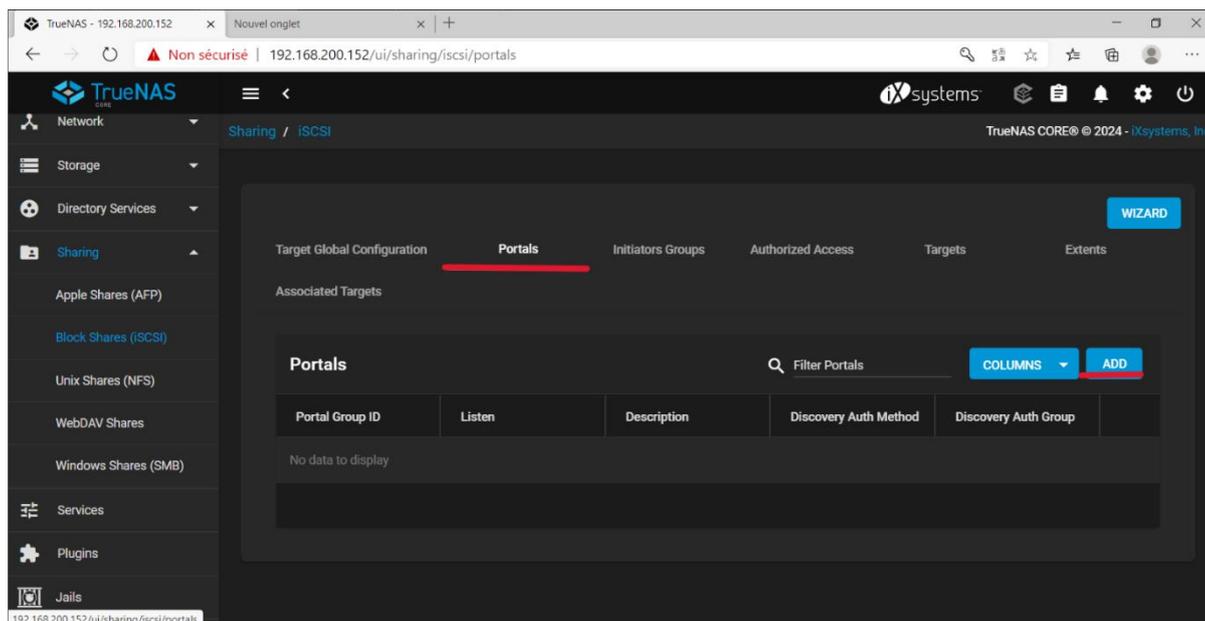
Une fois que TrueNas est bien lancé et configuré vous verrez une page similaire à celle-ci. Maintenant allez sur votre serveur principal ouvrez une page web et tapez l'adresse ip qu'indique TrueNas.



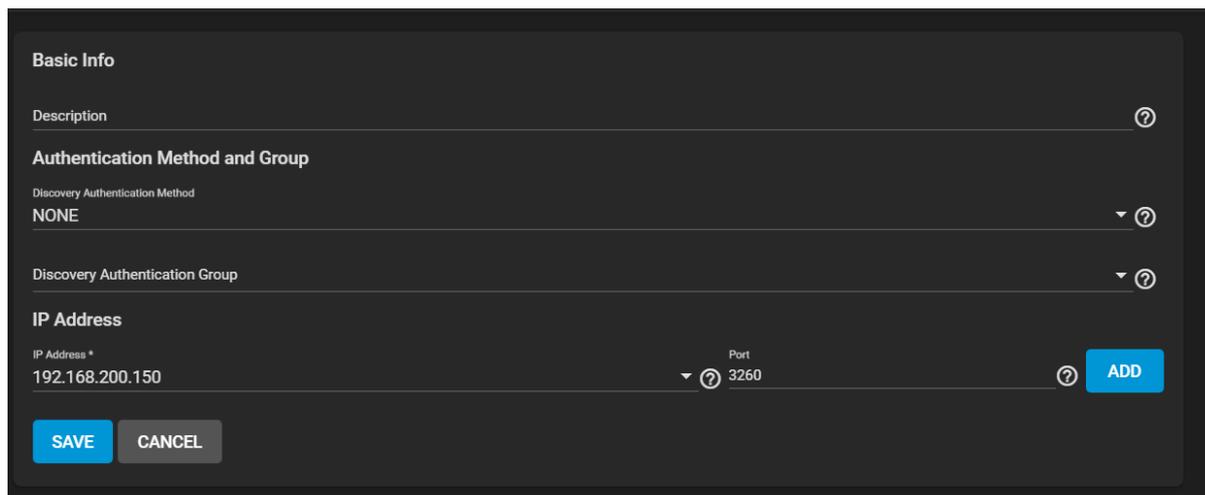
Allé dans Services et cochez "iSCSI".



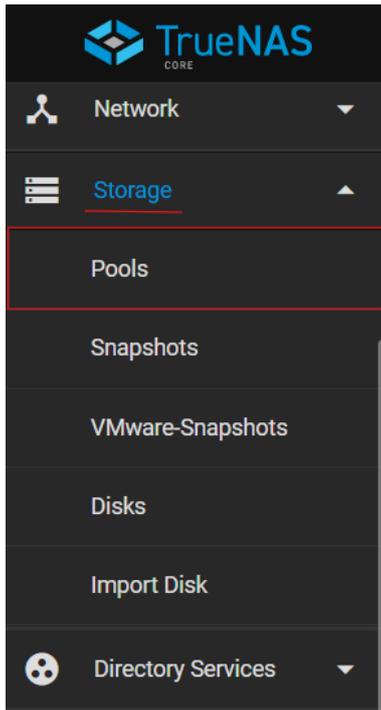
Maintenant allé dans Sharing puis "Block Shares (iSCSI)"



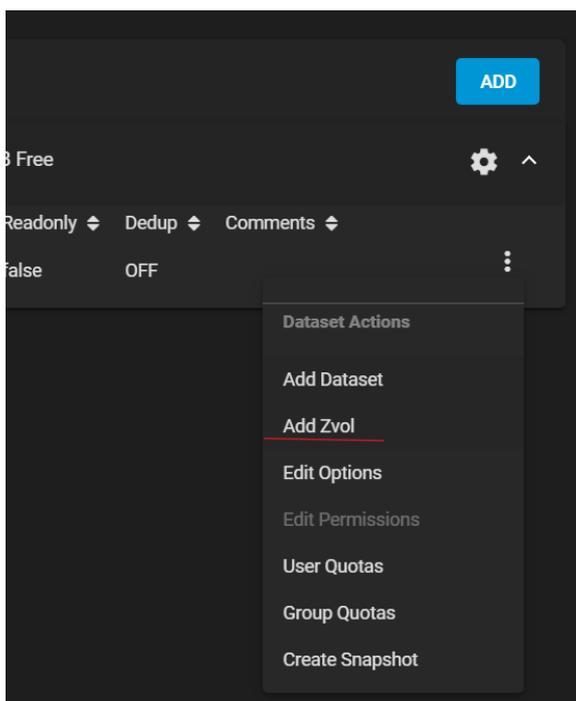
Sélectionner portals et ADD.



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.

Storage / Pools / Add Zvol

Zvol name *
ISCSI-MUL

Comments

Size for this zvol *
15 GiB

Force size

Sync
Standard

Compression level *
lz4 (recommended)

ZFS Deduplication *
Off

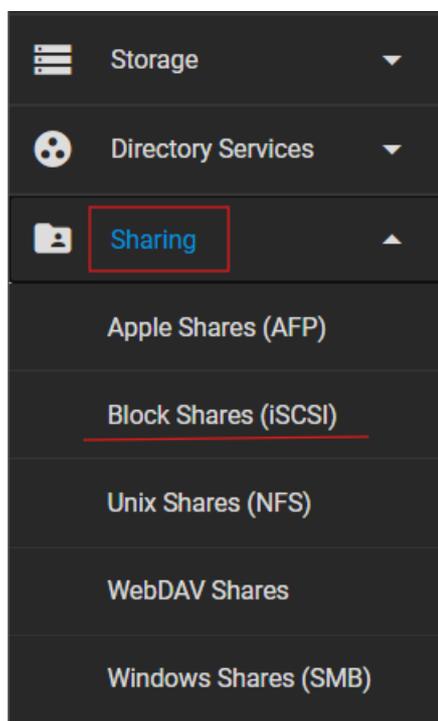
Sparse

Read-only
Inherit (off)

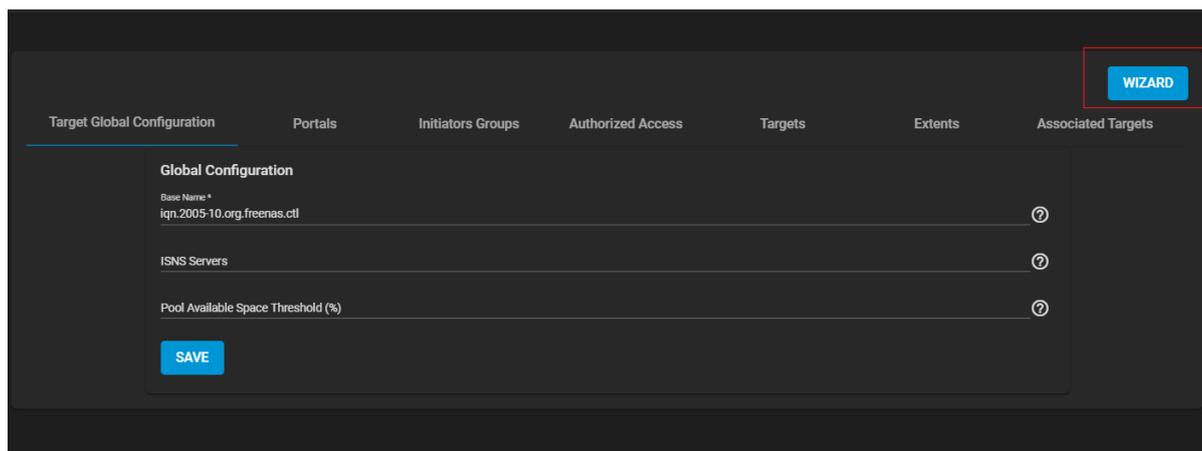
Encryption Options
 Inherit (non-encrypted)

SUBMIT CANCEL ADVANCED OPTIONS

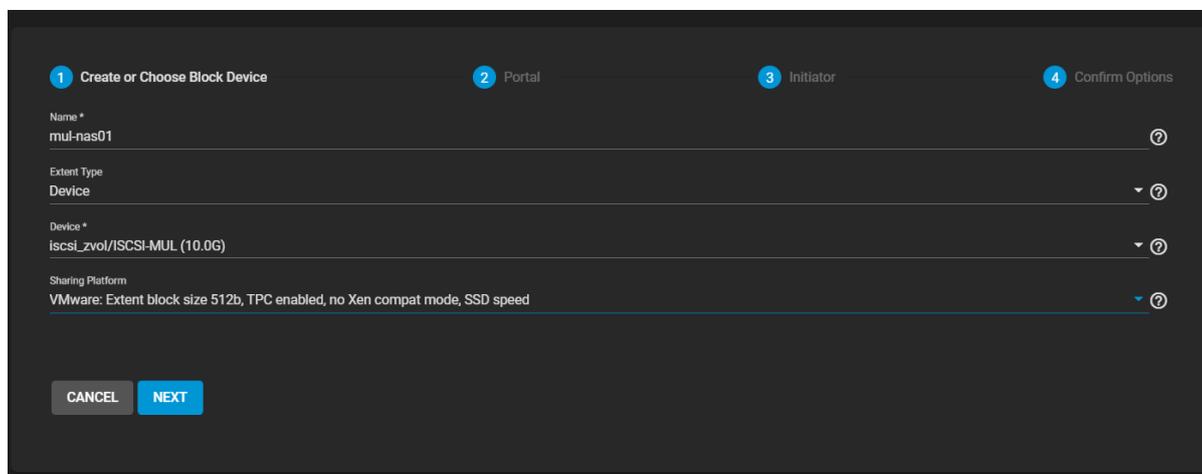
Donnez un nom à votre Pool pour ma part ISCSI MUL. Après donnez lui l'espace qu'il aura c'est à dire 50G et coché bien "force size". Dans Compression level mettez "lz4". Une fois que tout est remplis vous pouvez valider.



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.

Sharing / iSCSI / Wizard TrueNAS CORE © 2024 - iXsystems

1 Create or Choose Block Device 2 Portal 3 Initiator 4 Confirm Options

Portal *
Create New ?

Discovery Authentication Method
CHAP ?

Discovery Authentication Group *
Create New ?

Group ID *
667 ?

User *
root ?

Secret *
..... ?

Secret (Confirm)
.....

IP Address * Port
0.0.0.0 3260 ? ? ADD

CANCEL BACK NEXT

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.

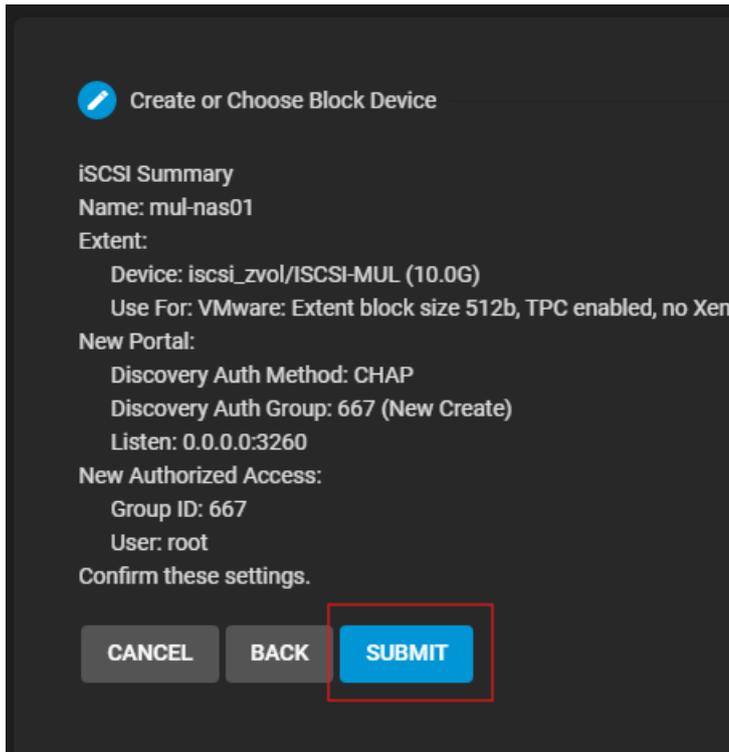
1 Create or Choose Block Device 2 Portal 3 Initiator 4 Confirm Options

Initiators ?

Authorized Networks ?

CANCEL BACK NEXT

Ici ne changez rien, appuyez sur Next.



Voici le résumé vous pouvez appuyer sur submit.

Propriétés de : Initiateur iSCSI

✕

Portails cible

Le système recherchera des cibles sur les portails suivants :

Adresse	Port	Carte	Adresse IP
192.168.200.152	3260	Par défaut	Par défaut

Pour ajouter un portail cible, cliquez sur Découvrir un portail.

Pour supprimer un portail cible, sélectionnez l'adresse ci-dessus, puis cliquez sur Supprimer.

Serveurs iSNS

Le système est inscrit sur les serveurs iSNS suivants :

Nom

Pour ajouter un serveur iSNS, cliquez sur Ajouter un serveur.

Pour supprimer un serveur iSNS, sélectionnez le serveur ci-dessus, puis cliquez sur Supprimer.

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.

Discover Target Portal ✕

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: Port: (Default is 3260.)

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

Advanced Settings

General IPsec

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP:

CRC / Checksum

Data digest Header digest

Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: truenasUser

Target secret:

Perform mutual authentication

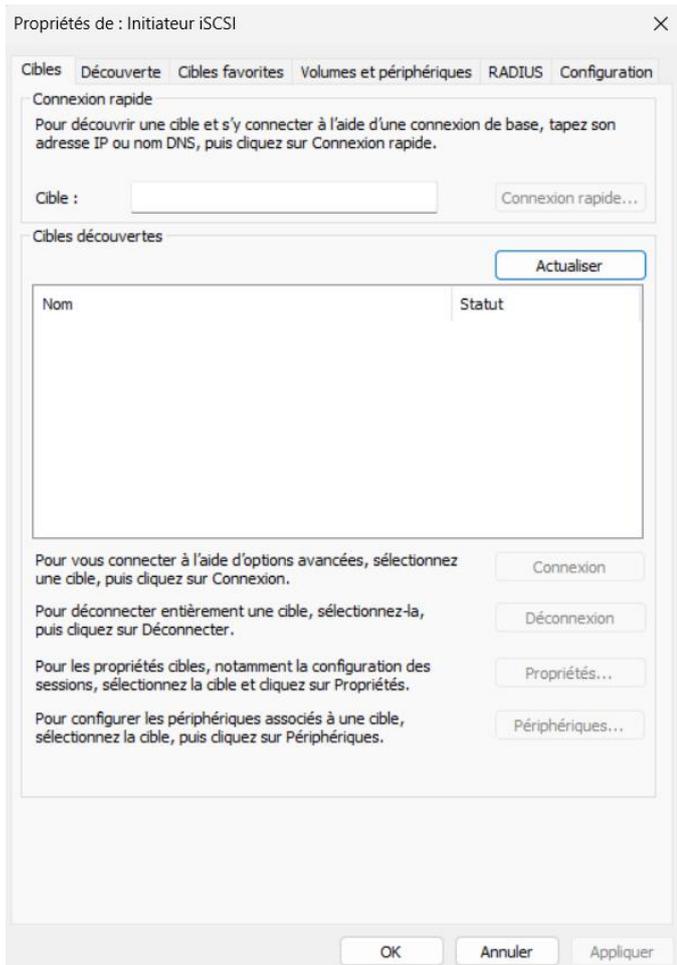
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

Use RADIUS to generate user authentication credentials

Use RADIUS to authenticate target credentials

OK Cancel Apply

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 apparaître 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.

Gestion des disques

Fichier Action Affichage ?

Volume	Disposition	Type	Système de...	Statut	Capacité	Espace l...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	29,97 Go	18,69 Go	62 %
(Disque 0 partitio...	Simple	De base		Sain (Parti...	100 Mo	100 Mo	100 %
(Disque 0 partitio...	Simple	De base		Sain (Parti...	633 Mo	633 Mo	100 %
DATAS03 (D:)	Simple	De base	NTFS	Sain (Parti...	29,30 Go	28,70 Go	98 %
SSS_X64FRE_FR-F...	Simple	De base	UDF	Sain (Parti...	4,97 Go	0 Mo	0 %
TrueNas (E:)	Simple	De base	NTFS	Sain (Parti...	19,53 Go	19,48 Go	100 %

Disque 0
De base
119,98 Go
En ligne

100 Mo Sain (P...	(C:) 29,97 Go NTFS Sain (Démarrer, Fich	DATAS03 (D:) 29,30 Go NTFS Sain (Partition de dc	633 Mo Sain (Partiti	TrueNas (E:) 19,53 Go NTFS Sain (Partition de d	40,47 Go Non alloué
----------------------	--	---	-------------------------	--	------------------------

Disque 1
Inconnu
10,00 Go
Non initialisé

10,00 Go
Non alloué

■ Non alloué ■ Partition principale

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.

