AP3

LIVRABLE 3

GROUPE 6

Victor WARTH / Jonas LE COSSEC

Création d'un système d'information hautement disponible et interconnecté

DOCUMENTATION TECHNIQUE

Sommaire

1) INSTALLATION D'UN WINDOWS SERVER 2022 AVEC AD, DHCP ET DNS

1.1) Prérequis

Prérequis pour la Configuration du Serveur Windows avec Active Directory, Serveur DHCP et Serveur DNS

1.1.1) Serveur Windows Server 2022 (VM)

- **Configuration minimale recommandée :**
  - Processeur : 2 cœurs ou plus
  - Mémoire : 2 Go de RAM
  - Espace de stockage : 20 Go d'espace disque disponible

1.1.2) Client Windows 10/11 (VM)

- **Configuration minimale recommandée :**
  - Processeur : 2 cœurs ou plus
  - Mémoire : 2 Go de RAM
  - Espace de stockage : 20 Go d'espace disque disponible

1.1.3) Carte Réseau VMware

- Assurez-vous que la carte réseau de chaque machine virtuelle est correctement configurée dans VMware.
- Désactivez toute configuration de serveur DHCP sur la carte réseau VMware.

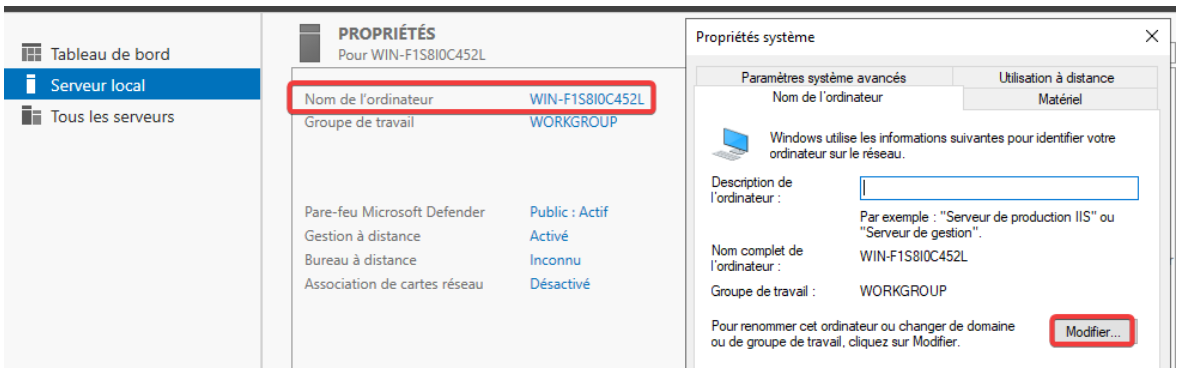
1.2) Pré configuration

<u>Remarque :</u> Il est important de vérifier et changer si besoin le nom du serveur ainsi que d'attribuer une adresse IP statique au serveur avant toute installation. En effet, cela peut créer des conflits si ces paramètres sont changés plus tard après installation de l'AD par exemple.

1.2.1) Changer le nom de l'ordinateur

Pour changer le nom de l'ordinateur il faut cliquer sur le nom de l'ordinateur inscrit dans la section Serveur local du gestionnaire de serveur, puis dans l'onglet « Nom de l'ordinateur » cliquer sur modifier et inscrire le nouveau nom de l'ordinateur.

NB: Il faut redémarrer le serveur pour que le changement de nom soit pris en compte. Dans notre cas nous le redémarreront par la suite.

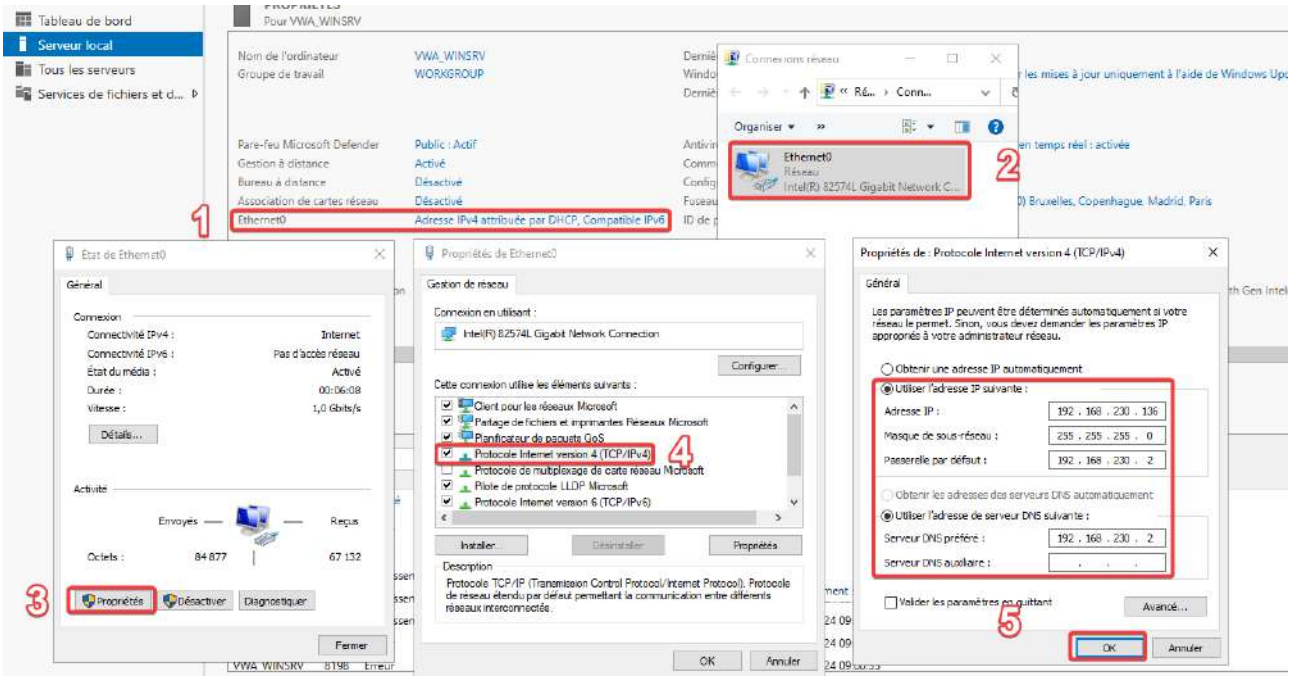


Gestionnaire de serveur > Serveur local > %Nom de l'ordinateur% > Nom de l'ordinateur > Modifier

1.2.2) Configurer une adresse IP statique

L'utilisation d'une adresse IP statique sur un serveur assure une stabilité d'accès et simplifie la gestion, évitant les changements d'adresse dynamique et facilitant la configuration réseau.

Pour attribuer manuellement une adresse IPv4 au serveur il faut cliquer sur la carte réseau **(1)** dans la section Serveur local du gestionnaire de serveur. Ensuite, sélectionné la carte réseau concernée, ici « Ethernet0 » **(2)** puis cliquer sur « Propriétés » **(3)**, « Protocole Internet version 4 » **(4)** enfin, sélectionner « Utiliser l'adresse IP suivante » et renseigner l'adresse IP désirée **(5)**.

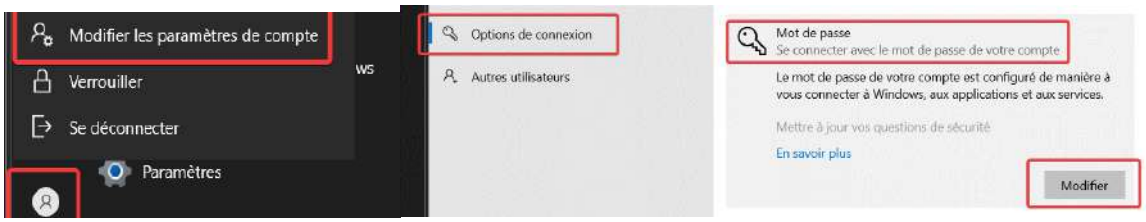


%Ethernet0% > %Ethernet0% > Propriétés > Protocole IPv4

1.2.3) Modification du mot de passe administrateur

Il faut modifier le mot de passe du compte Administrateur et utilisateur, si ce n'est pas fait cela peut créer des erreurs plus tard. (Mot de passe robuste nécessaire → L'utilisation d'un générateur de mot de passe s'avère être une bonne idée.)

Pour modifier le mot de passe d'un compte, il faut aller dans le menu Windows, puis cliquer sur l'icône de l'utilisateur en bas à gauche, puis sur « Modifier les paramètres de compte » puis dans la nouvelle page qui s'est ouverte cliquer sur l'onglet « Options de connexion », enfin, il faut développer la partie « Mot de passe » puis cliquer sur « Modifier »



Menu Windows > Utilisateur > Modifier les paramètres de compte > Options de connexion > Mot de passe

NB: Il ne faut pas oublier de modifier aussi le mot de passe sur le compte Administrateur (Se déconnecter puis se reconnecter sur la session administrateur)

Redémarrer le serveur.

1.3) Installation de l'Active Directory et du DHCP

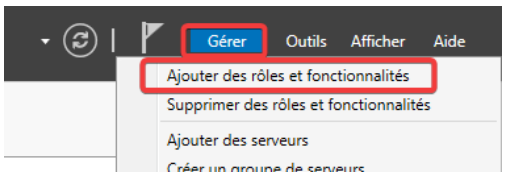
L'Active Directory (AD) est un service de répertoire développé par Microsoft, utilisé pour stocker des informations sur les ressources réseau, tels que les utilisateurs, les groupes, les ordinateurs, et les imprimantes, dans un environnement Windows. Il facilite l'organisation et la gestion des objets réseau, tout en permettant l'authentification et l'autorisation des utilisateurs et des services.

Le serveur DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP et d'autres paramètres de configuration réseau aux dispositifs connectés à un réseau. Il simplifie la gestion des adresses IP en évitant les conflits et en permettant une configuration automatique, ce qui est particulièrement utile dans les réseaux où les dispositifs se connectent et se déconnectent fréquemment.

1.3.1) Ajout des rôles et fonctionnalités

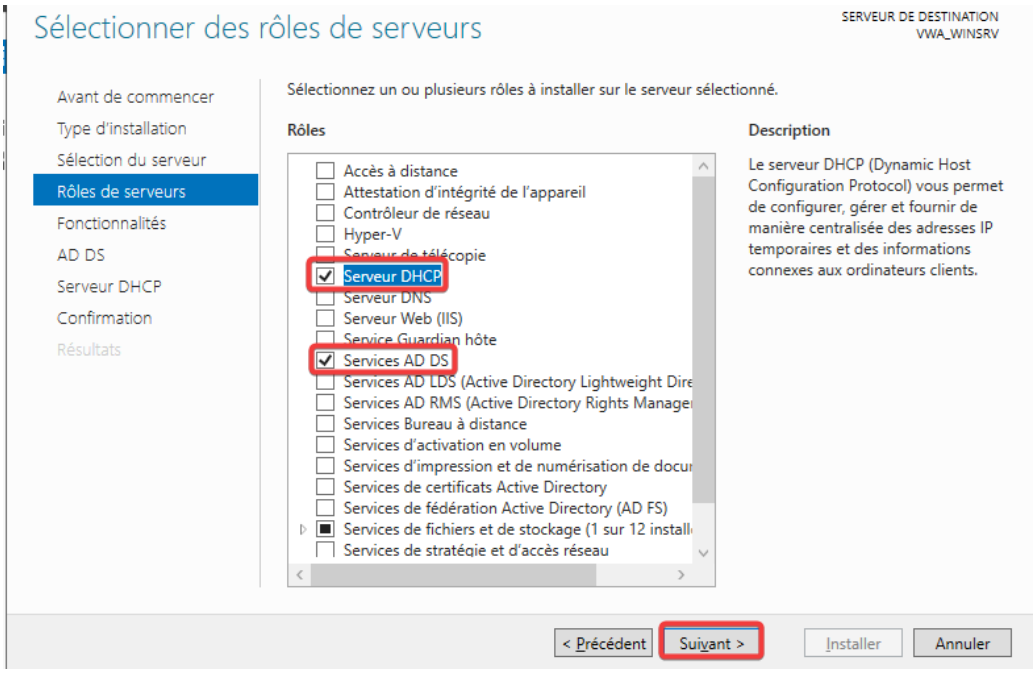
NB: L'Active Directory Domain Services (AD DS) regroupe un annuaire LDAP, un service DNS pour la gestion des domaines, et utilise le protocole Kerberos pour l'authentification des utilisateurs. Il n'est donc **pas nécessaire d'installer le rôle Serveur DNS** (cela peut même créer des conflits).

Pour ajouter les services AD DS et de serveur DHCP il faut cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités » dans le gestionnaire de serveur.



Pour le « Type d'installation » on peut laisser par défaut, puis dans « Sélection du serveur » il faut sélectionner notre serveur.

Ensuite dans l'onglet « Rôles de serveurs » il faut sélectionner « Serveur DHCP » et « Services AD DS ». Ensuite cliquer sur suivant.



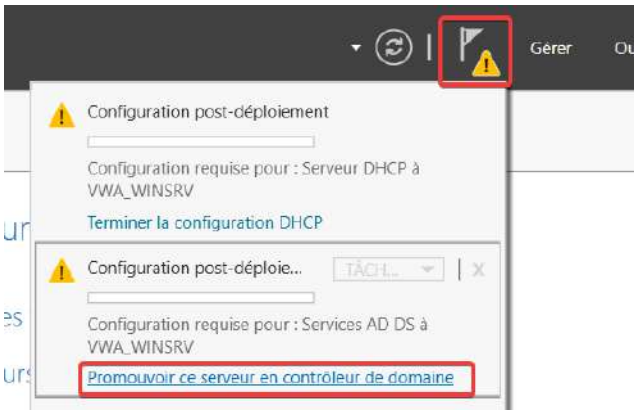
Pour le reste des onglets on peut laisser les paramètres par défaut et cliquer sur suivant et pour finir confirmer l'installation.

Redémarrer le serveur.

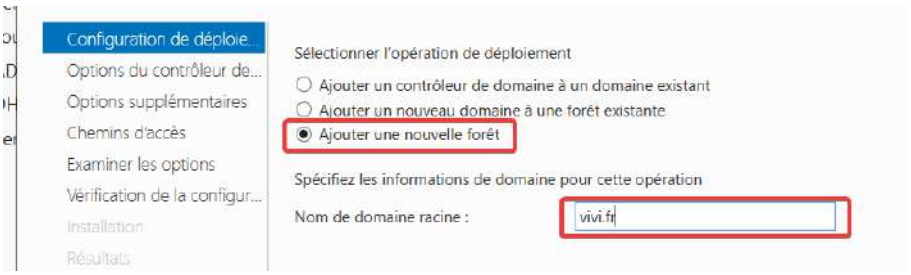
1.3.2) Configuration de l'AD DS

Afin d'utiliser l'AD DS il faudra encore réaliser quelques configurations. On peut notamment voir l'évolution de la configuration en cliquant sur le drapeau en haut a droite du gestionnaire de serveur.

Pour commencer il faut cliquer sur le drapeau puis « Promouvoir ce serveur en contrôleur de domaine »



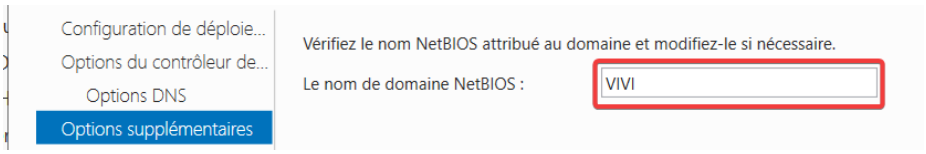
Dans la nouvelle fenêtre qui s'ouvre Il faut ensuite cliquer sur ajouter une nouvelle forêt (ne pas oublier l'extension dans notre cas « .fr »)



Puis on peut laisser les paramètres par défaut et mettre un mot de passe (Dans notre cas ce sera le même que celui de l'administrateur question de simplicité)

Ensuite, on ne souhaite pas ici créer de délégation DNS, on laisse donc la case décochée.

Dans l'onglet suivant, il faut mettre en nom de domaine NetBIOS le même nom que la nouvelle forêt (sans l'extension)



Pour les autres onglets on peut laisser les paramètres par défaut et confirmer l'installation.

Redémarrer le serveur.

1.3.3) Configuration du DHCP

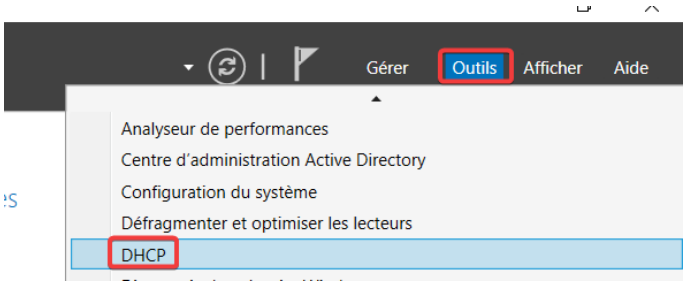
Pour mettre en place le serveur DHCP il faut finir la configuration.

Pour se faire, cliquer sur le drapeau puis sur « Terminer la configuration DHCP » depuis le gestionnaire de serveur.

Dans notre cas on peut laisser tous les paramètres de configuration par défaut.

Redémarrer le serveur.

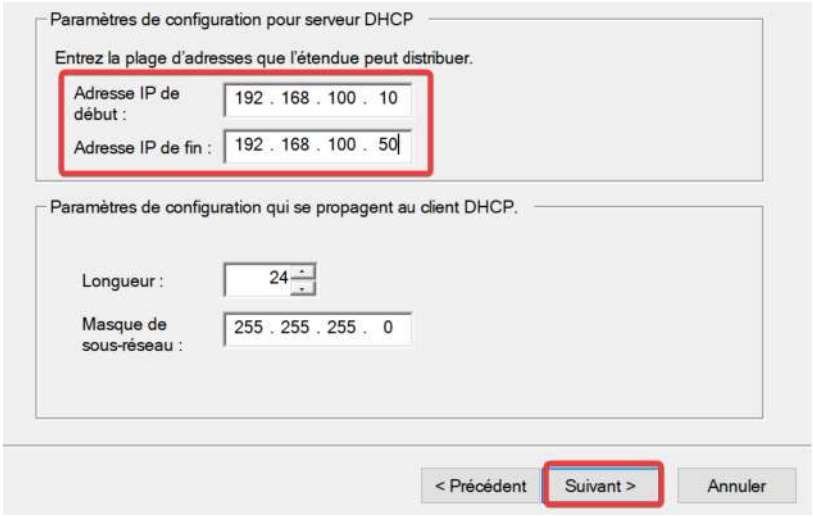
Après avoir redémarrer le serveur il faut maintenant donner dire au DHCP la configuration que l'on souhaite lui donner, pour faire cela il faut aller dans « Outils » puis « DHCP ».



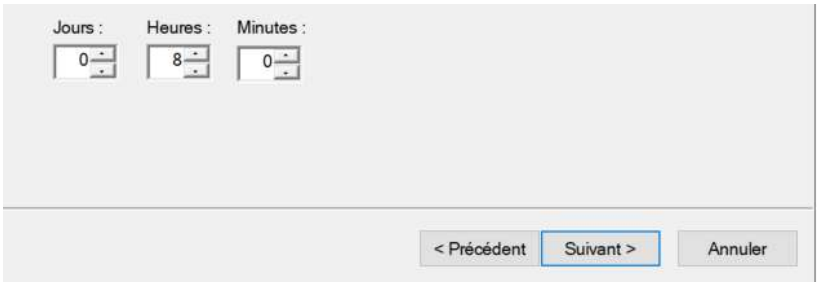
Dans la nouvelle fenêtre qui vient de s'ouvrir on peut développer notre serveur (composé de son nom suivi de notre nom de forêt avec l'extension). Puis il faut faire un clic droit sur « IPv4 » et sélectionner « Nouvelle étendue »

Ensuite, on peut donner un nom (sans importance) à cette étendue, puis, il faut définir la plage d'adresses que le DHCP va attribuer.

NB: Il faut que la plage d'adresse IP soit dans le même réseau que notre serveur.



Ensuite, il faut définir la durée du bail. Par principe on donne un bail de 8 heures.



Dans notre cas on peut laisser les autres paramètres par défaut, puis activer l'étendu.

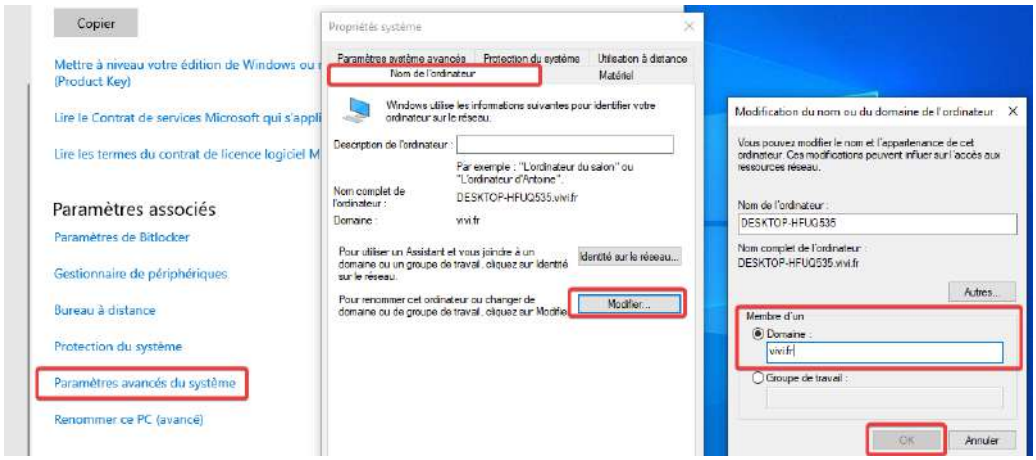
1.4) Exploiter le domaine

Après avoir créé notre domaine on peut maintenant l'utiliser, dans notre exemple pour des clients Windows.

1.4.1) Joindre le domaine

Pour joindre le domaine il faut avoir un client (ici un Windows 10) connecté sur la même interface réseau VMware et au même réseau que le Windows server.

Pour joindre le domaine il faut aller dans les paramètres, puis dans « système », « à propos », ensuite il faut cliquer sur « paramètres avancés du système ». Dans la nouvelle fenêtre qui s'ouvre il faut aller dans la catégorie « nom de l'ordinateur » puis sur « Modifier ». Enfin, « membre d'un » il faut sélectionner « Domaine » et renseigner le domaine avec son extension créé à l'étape 4.2.



Paramètre > Système > A Propos > Paramètres avancés du système > Nom de l'ordinateur > Modifier

On sera ensuite invité à renseigner les informations d'un compte administrateur de l'AD.

Redémarrer le PC

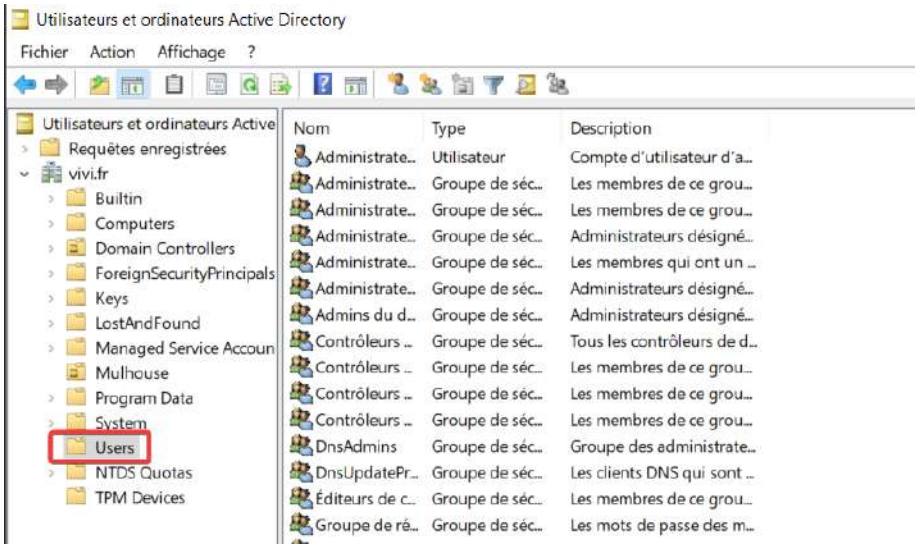
1.4.2) Créer un utilisateur/groupe

La mise en place d'utilisateurs et de groupes au sein de l'Active Directory est essentiel et renforce la gestion efficace des accès et des autorisations au sein de votre environnement informatique.

Pour créer un utilisateur ou un groupe il faut suivre la même procédure de départ.

Pour commencer rendez-vous dans « Outils » puis « Utilisateurs et ordinateurs Active Directory » sur le gestionnaire de serveur.

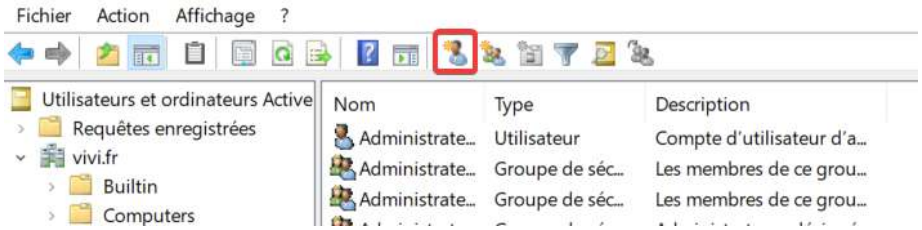
Dans la nouvelle fenêtre qui s'ouvre, vous pouvez développer votre domaine, dans notre cas « vivi.fr », puis on se positionner dans le dossier « Users ».



On peut voir que le dossier contient déjà des utilisateurs génériques générés au moment de la création de l'AD.

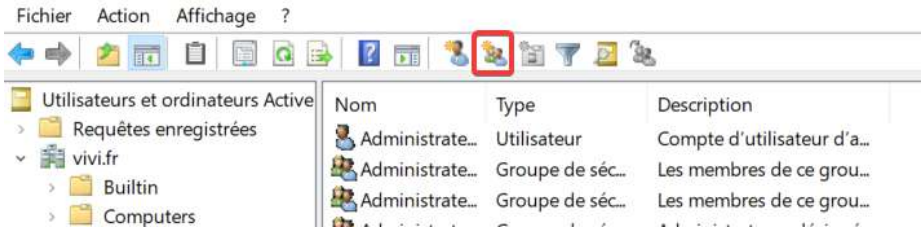
1.4.2 bis) Créer un utilisateur

Pour ajouter un utilisateur il suffit de cliquer sur bouton « Créer un nouvel utilisateur dans le conteneur actuel » puis il suffit de renseigner les informations que vous souhaitez.



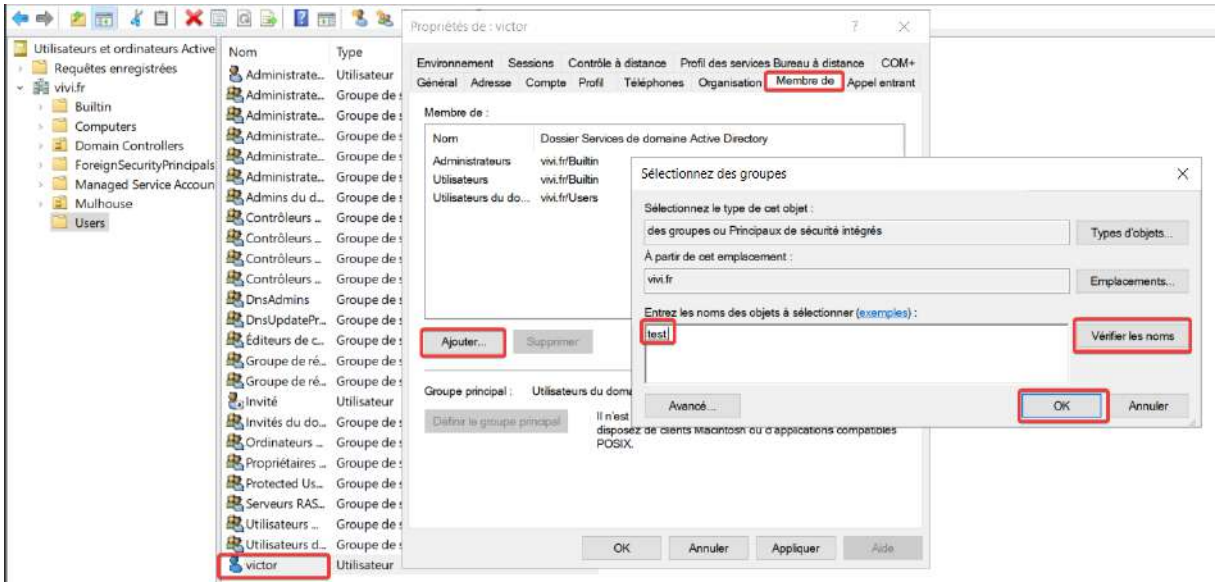
1.4.2 bis) Créer un groupe

Pour créer un groupe il faut cliquer sur le bouton « Créer un nouveau groupe dans le conteneur actuel » puis renseigner les informations que l'on souhaite.



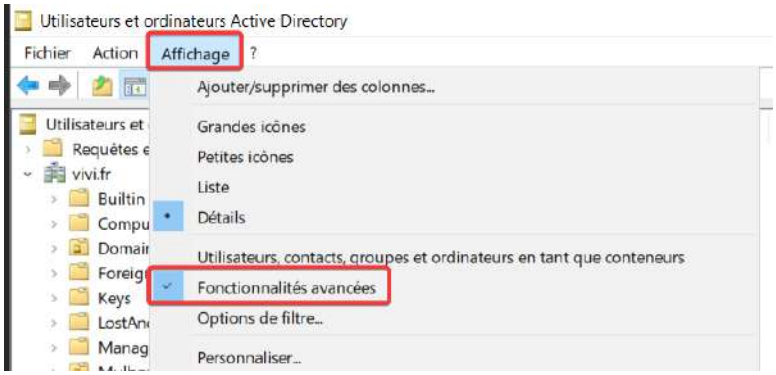
1.4.2 bis) Attribuer un groupe

Pour attribuer un groupe à un utilisateur, il faut double cliquer sur un utilsiateur, ensuite aller dans l'onglet « Membre de » puis cliquer sur « Ajouter ». Il suffit de donner le nom des groupes que l'on souhaite attribuer (il est possible d'en attribuer plusieurs en même temps), pour être certain d'attribuer le bon groupe on peut cliquer sur « vérifier les noms », si le nom du groupe se souligne alors le groupe a été trouvé, dans le cas ou le nom du groupe n'est pas trouvé ou incomplet, une nouvelle fenêtre de sélection s'ouvre.

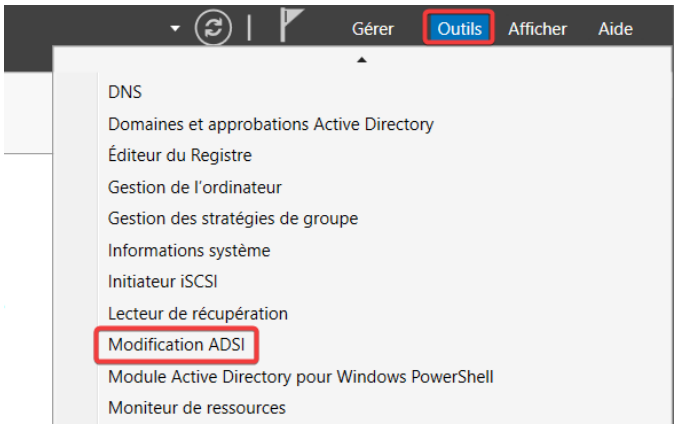


1.4.2 bis) Créer un conteneur

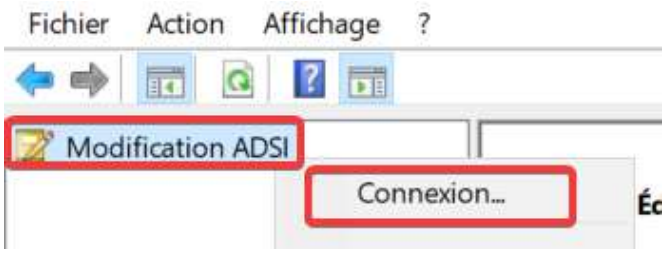
NB: Les conteneurs que nous nous apprêtons à créer sont seulement visible si l'option d'affichage des fonctionnalités avancées est activée.



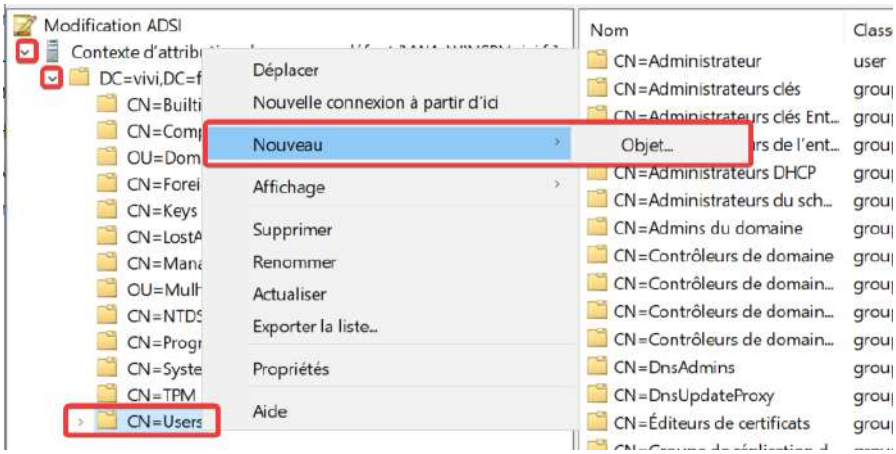
Pour créer un conteneur, il faut se rendre dans « Outils » puis « Modification ADSI »



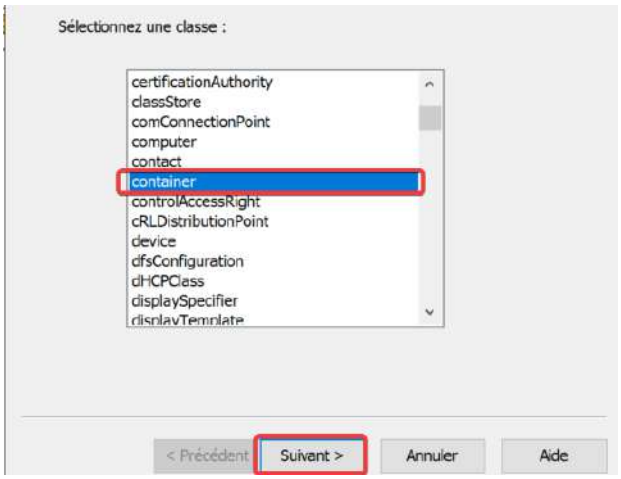
Dans la nouvelle fenêtre qui s'ouvre il faut faire clic droit sur « Modification ADSI » puis « Connexion », ensuite on laisse les paramètres par défaut et on clique sur « Ok »



Par la suite, il faut développer votre nouvelle connexion puis le domaine, puis faire clic droit sur le dossier de votre choix, dans notre cas « Users », puis « Nouveau », « Objet ».



Il faut ensuite cherche l'objet « Container », puis il ne vous reste plus qu'a appuyer sur suivant et le créer.



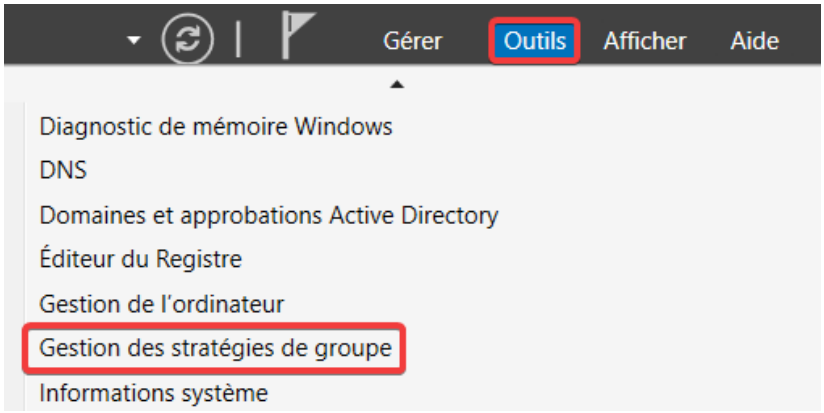
1.4.3) Modifier une GPO

Une GPO (Group Policy Object) est un ensemble de règles de configuration dans un domaine Windows, permettant aux administrateurs de définir des paramètres pour les ordinateurs et utilisateurs, assurant ainsi une gestion centralisée et cohérente des configurations.

Dans notre cas nous allons changer la politique de mot de passe afin de simplifier les accès au serveur.

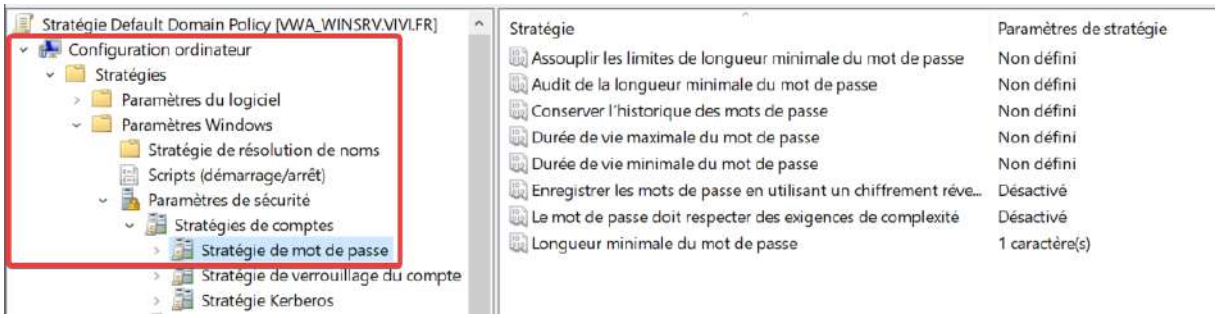
NB: Pour des raisons de sécurité évidentes, il n'est pas recommandé de baisser les exigences au minimum de la politique de mot de passe comme nous allons le faire.

Pour accéder aux GPO, il faut cliquer sur « Outils » puis dans « Gestion des stratégies de groupe » depuis le gestionnaire de serveur.

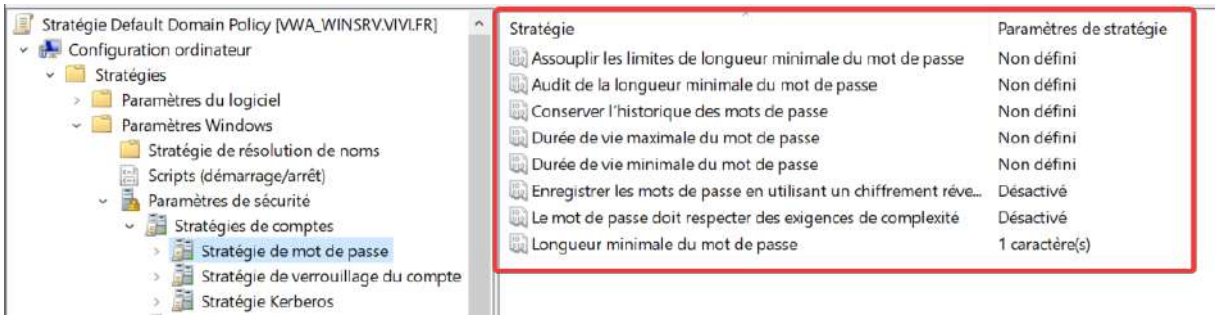


Puis dans la nouvelle fenêtre qui s'ouvre il faut développer la forêt puis « Domaines » puis votre domaine, dans notre cas « vivi.fr ». Ensuite, vous pouvez faire un clic droit sur « Default Domain Policy » enfin cliquer sur « Modifier ».

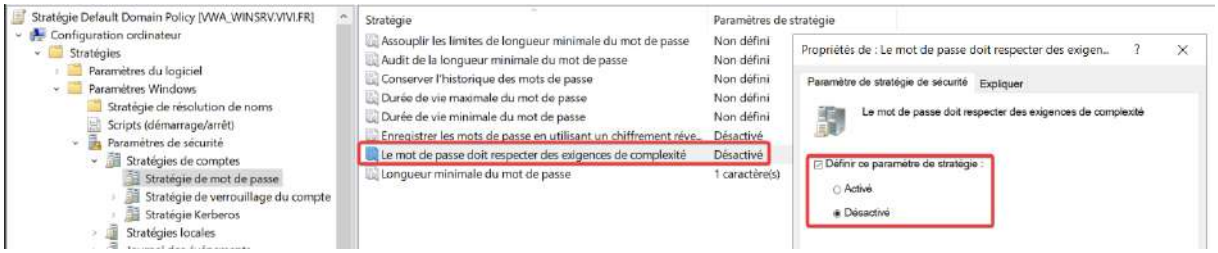
Dans la nouvelle fenêtre il faut développer « Configuration ordinateur », ensuite « Stratégies », puis « Paramètres Windows » et enfin « Paramètres de sécurité ». La stratégie qui nous intéresse dans notre cas est « Stratégie de mot de passe ».



Après avoir cliqué sur « Stratégie de mot de passe » on peut voir dans la partie droite de la fenêtre l'ensemble des stratégies de mot de passe.



A l'aide d'un double clic sur une stratégie il est possible de modifier sa valeur. Dans notre cas, j'ai désactivé la stratégie qui impose une certaine complexité des mots de passe. N'oubliez pas de cliquer sur « Appliquer ».



Si la stratégie n'a pas été prise en compte directement il est possible de forcer son renouvellement en exécutant la commande « gpupdate /force » dans une invite de commande exécuté en administrateur sur le serveur.

```
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

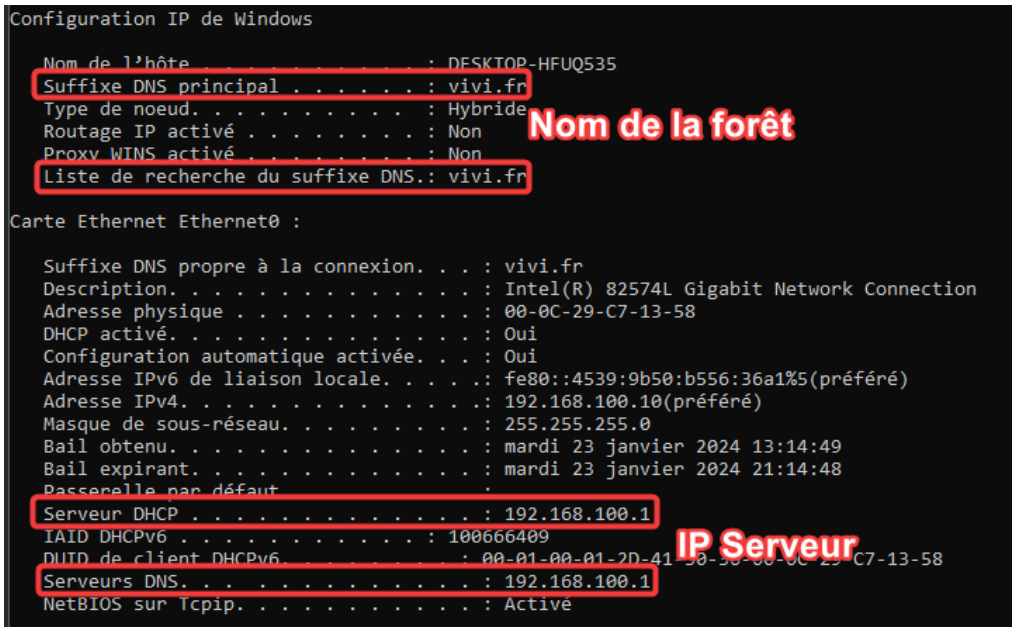
1.4.4) Vérification du domaine sur le PC

1.4.4 bis) Par ligne de commande

Avec la commande « ipconfig /all » il est possible de vérifier le suffixe DNS ainsi que l'adresse du serveur DHCP et du serveur DNS.

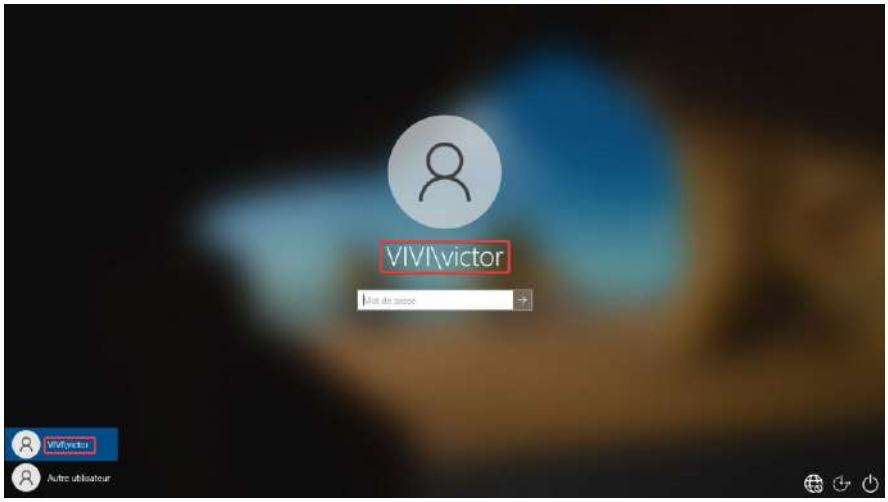
Le suffixe DNS doit correspondre au nom de la forêt donnée dans le contrôleur de domaine.

Les serveurs DHCP et DNS doivent bien être ceux configurer dans le DHCP du serveur (dans notre cas l'IP de ce même serveur).



1.4.4 bis) Par interface graphique

Au moment de la connexion a un utilisateur il est possible de se connecter à un compte de l'Active Directory si vous avez bien joint le domaine. Cela se traduit par le nom NetBios du domaine dans notre cas « VIVI »



1.4.5) Vérification du DHCP sur le PC

Il est possible de vérifier le bon fonctionnement du serveur DHCP sur un poste client. Tout d'abord on peut regarder la configuration de l'IPv4 actuelle avec la commande « ipconfig /all »

```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : vivi.fr
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-C7-13-58
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::4539:9b50:b556:36a1%5(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.100.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 25 janvier 2024 11:53:43
   Bail expirant. . . . . . . . . . . . . : jeudi 25 janvier 2024 19:53:43
   Passerelle par défaut. . . . . . . . . :
```

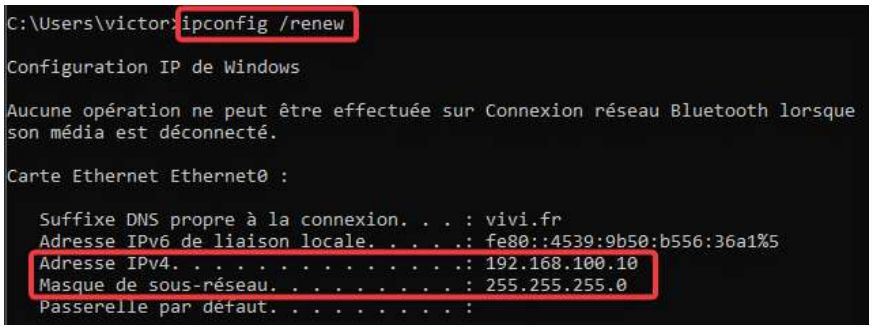
On retrouve bien dans notre cas une adresse contenu dans la plage que l'on a paramétrer dans notre serveur DHCP.

On peut ensuite utiliser les commandes « ipconfig /release » et « ipconfig /renew » qui permettent de résilier et renouveler le bail DHCP. On commence par faire « ipconfig /release » afin de résilier le bail dans un premier temps. On note bien qu'il n'y a plus d'adresse IPv4 ni de masque de sous-réseau attribués à notre machine.

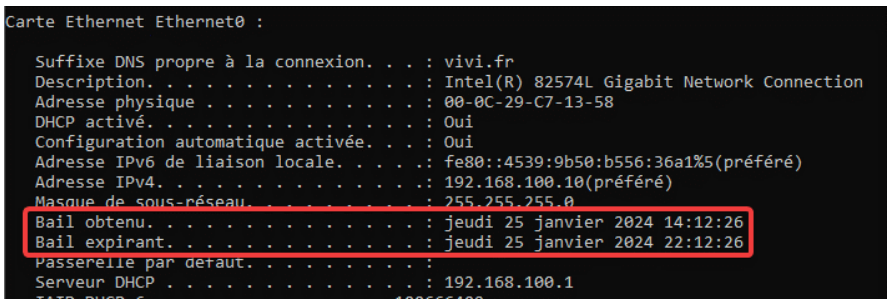
```
C:\Users\victor>ipconfig /release

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion réseau Bluetooth lorsque
son média est déconnecté.

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4539:9b50:b556:36a1%5
   Passerelle par défaut. . . . . . . . . :
```

Ensuite on renouvelle le bail avec « ipconfig /renew ». On peut observer qu'une nouvelle adresse IPv4 nous a été attribuée (dans notre cas la même

que précédemment) qui est toujours contenu dans la plage de notre serveur DHCP.



On peut voir que le bail a bien été renouvelé avec à la commande « ipconfig /all ».



1.5) Redondance

Afin d'assurer la continuité des services et renforcer la fiabilité de notre infrastructure informatique il est possible de mettre en place des solutions de redondance pour nos serveurs Windows.

1.5.1) Pré configuration

Sur un nouveau Windows serveur ayant la même version que l'autre (ce n'est pas une obligation, tout dépend du niveau fonctionnel du domaine et de la forêt), il faut suivre les étapes du chapitre 3. Pré configuration.

Lors de l'étape 3.2 Configurer une adresse IP statique il est nécessaire de modifier les DNS de la façon suivante :

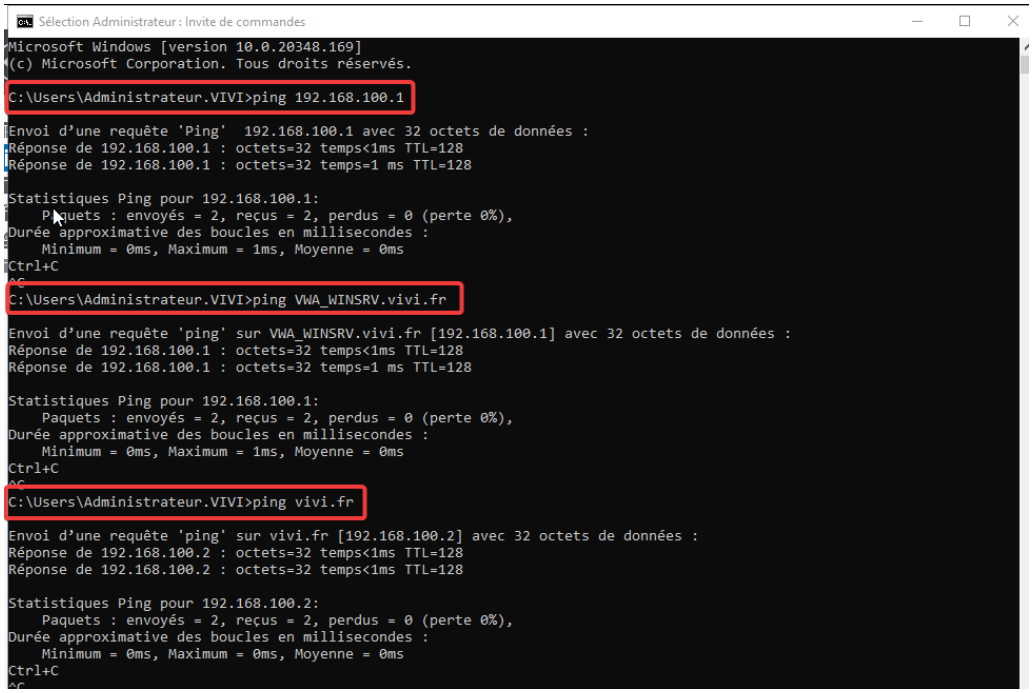
Il faut mettre en Serveur DNS préféré l'adresse IP du premier serveur que l'on a configuré. Et dans DNS auxiliaire il est nécessaire de mettre l'adresse de boucle (127.0.0.1) donc lui-même.

1.5.2) Connection au domaine

1.5.2 bis) Vérification des flux réseau

Il faut vérifier que notre nouveau serveur puisse joindre le premier.

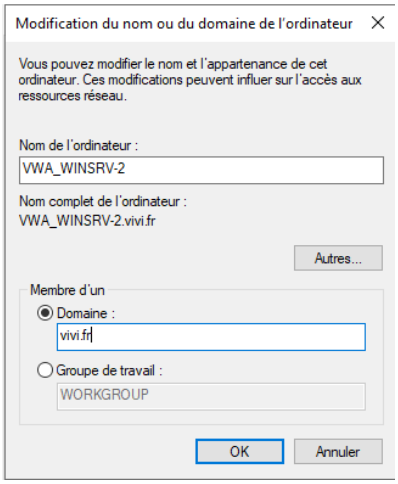
Dans un terminal sur le nouveau windows serveur, tenter de ping l'IP du premier serveur (ici 192.168.100.1) puis son nom complet FQDN (ici VWA_WINSRV.vivi.fr) et enfin le domaine (ici vivi.fr)



Si vous arrivez à ping toutes ces instances alors vous pouvez passer à la suite. Sinon, il faudra vérifier les différentes configurations réalisées précédemment.

1.5.2 bis) Joindre le serveur au domaine

On va ensuite joindre le serveur au domaine comme à l'étape 5.1 Joindre le domaine. La configuration donnera cela dans notre cas :



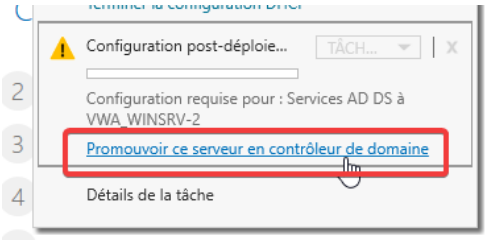
Puis redémarrer le serveur.

Au redémarrage, il est nécessaire de se connecter avec un compte d'administrateur du domaine pour la suite de la configuration.

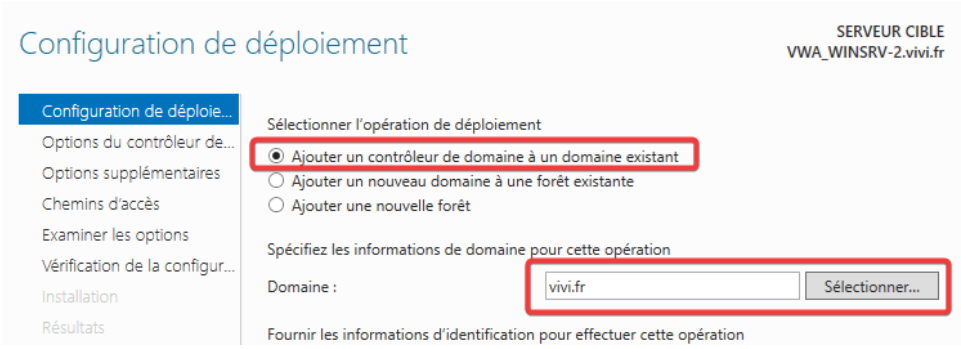
Enfin, il faut ajouter le rôle AD DS et DHCP sur le nouveau serveur.

1.5.3) Configuration des rôles

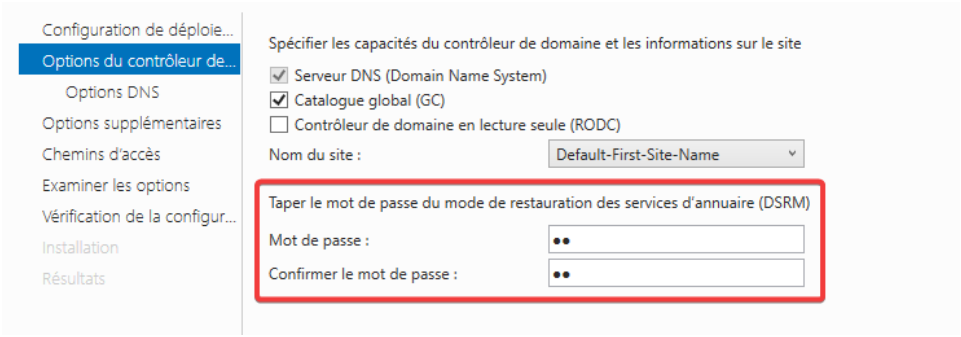
Tout d'abord depuis le gestionnaire de serveur, il faut cliquer sur le petit drapeau, puis sur promouvoir ce serveur en contrôleur de domaine.



Ensuite, on va ajouter le contrôleur de domaine à un domaine existant, il est nécessaire de renseigner le domaine, comme ci-dessous :



Puis il va falloir rentrer le mot de passe DSRM



Puis on peut cliquer sur suivant pour le reste des paramètres et installer.

Enfin, le serveur va redémarrer.

L'actualisation de l'AD peut prendre plusieurs minutes à se faire.

Pour le serveur DHCP, il suffit de cliquer sur le petit drapeau depuis le gestionnaire de serveur et de suivre les étapes pour terminer la configuration (tout laisser par défaut).

Redémarrer le serveur.

1.5.4) Vérification de la redondance

Afin d'être sûr que la redondance fonctionne correctement, il est possible de faire la vérification suivante :

Tout d'abord, depuis un client Windows 10 du domaine, il faut ping le domaine, dans notre cas « vivi.fr ».

```
C:\Users\vivi>ping vivi.fr

Envoi d'une requête 'ping' sur vivi.fr [192.168.100.1] avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=128
```

La commande nous retourne l'adresse IP du premier serveur Windows.

Ensuite, il faut éteindre ce serveur Windows (192.168.100.1 dans notre cas) et recommencer la commande ping sur notre domaine.

```
C:\Users\vivi>ping vivi.fr

Envoi d'une requête 'ping' sur vivi.fr [192.168.100.2] avec 32 octets de données :
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps=1 ms TTL=128
```

Cette fois-ci la commande retourne l'adresse IP du deuxième serveur Windows.

On constate donc que le deuxième serveur a bien le relais, la redondance est donc fonctionnelle.

2) Installation et configuration d'un homelab Proxmox

2.1) Prérequis

Pour monter un hyperviseur Proxmox, il est nécessaire d'avoir une machine suffisamment puissante. Dans notre cas, voici les spécifications techniques de la machine utilisée :

- CPU : Intel Core i7-10700F (8c/16t)
- RAM : 32 Go RAM DDR4 3600 MHz
- STOCKAGE : 1 To M.2 PCIe 3.0 NVMe

> ⓘ INFO
>
> Si vous souhaitez joindre l'hyperviseur depuis Internet, il sera nécessaire d'avoir une connexion Internet.

2.2) Installation de l'OS

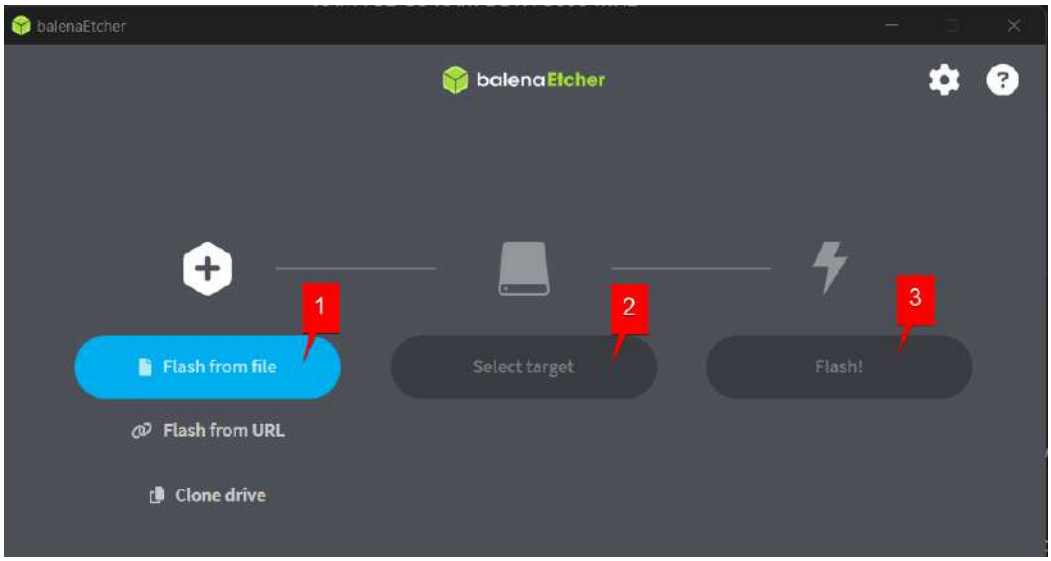
2.2.1) Préparation du support d'installation

Pour commencer, il sera nécessaire de télécharger la dernière version de Proxmox VE (8.2 dans notre cas) : https://www.proxmox.com/en/downloads

Ensuite, il va falloir préparer le support d'installation, dans notre cas, une clé USB bootable.

Pour rendre la clé USB bootable, il est possible d'utiliser un logiciel gratuit comme BalenaEtcher par exemple : https://etcher.balena.io/ :

1. On choisit notre ISO Proxmox VE
2. On sélectionne notre clé USB à rendre bootable
3. On Flash !

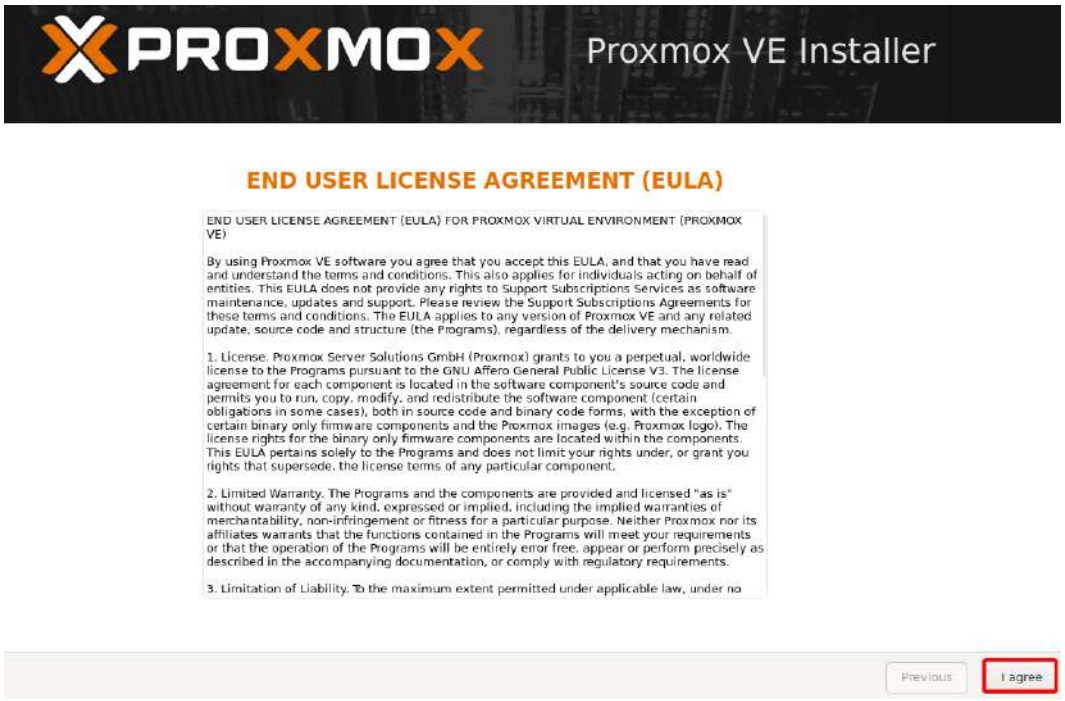


Puis, il ne reste plus qu'à vérifier que la virtualisation est activée dans le BIOS de notre machine et lancer la machine sur l'UEFI de la clé USB bootable.

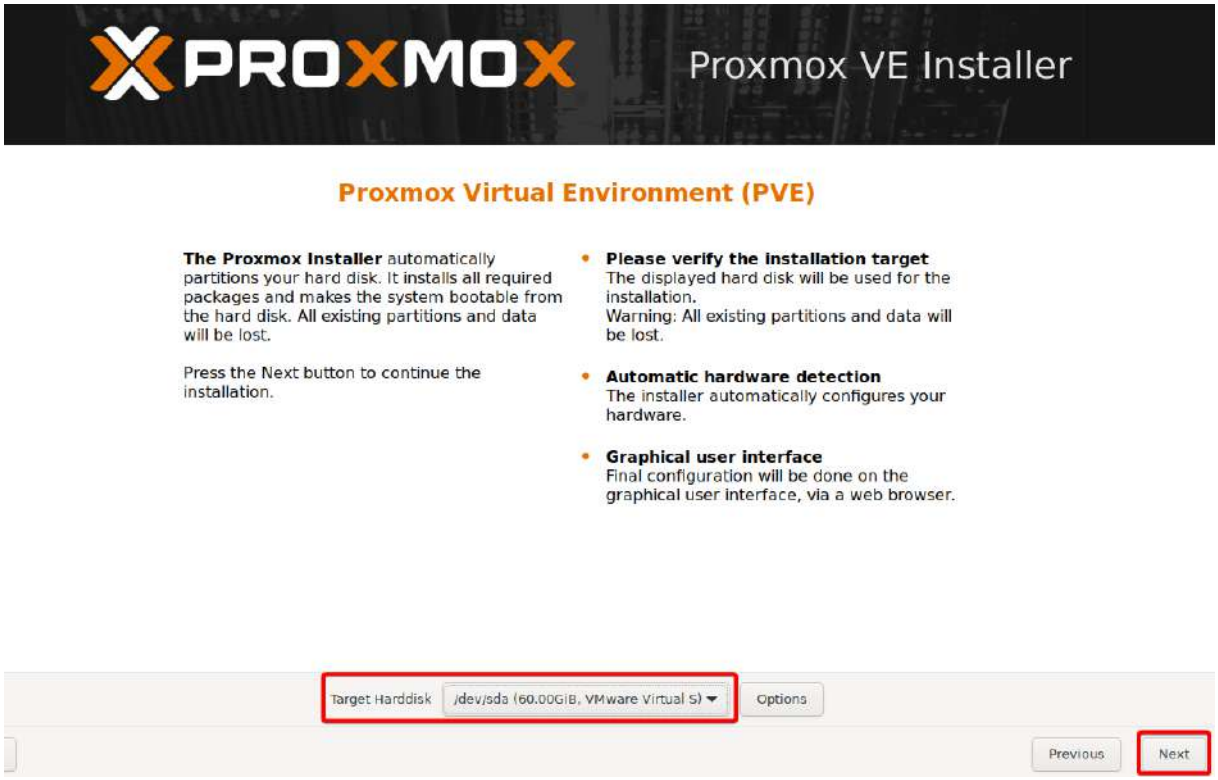
2.2.2) Installation

Dans notre cas, nous allons faire une installation classique :

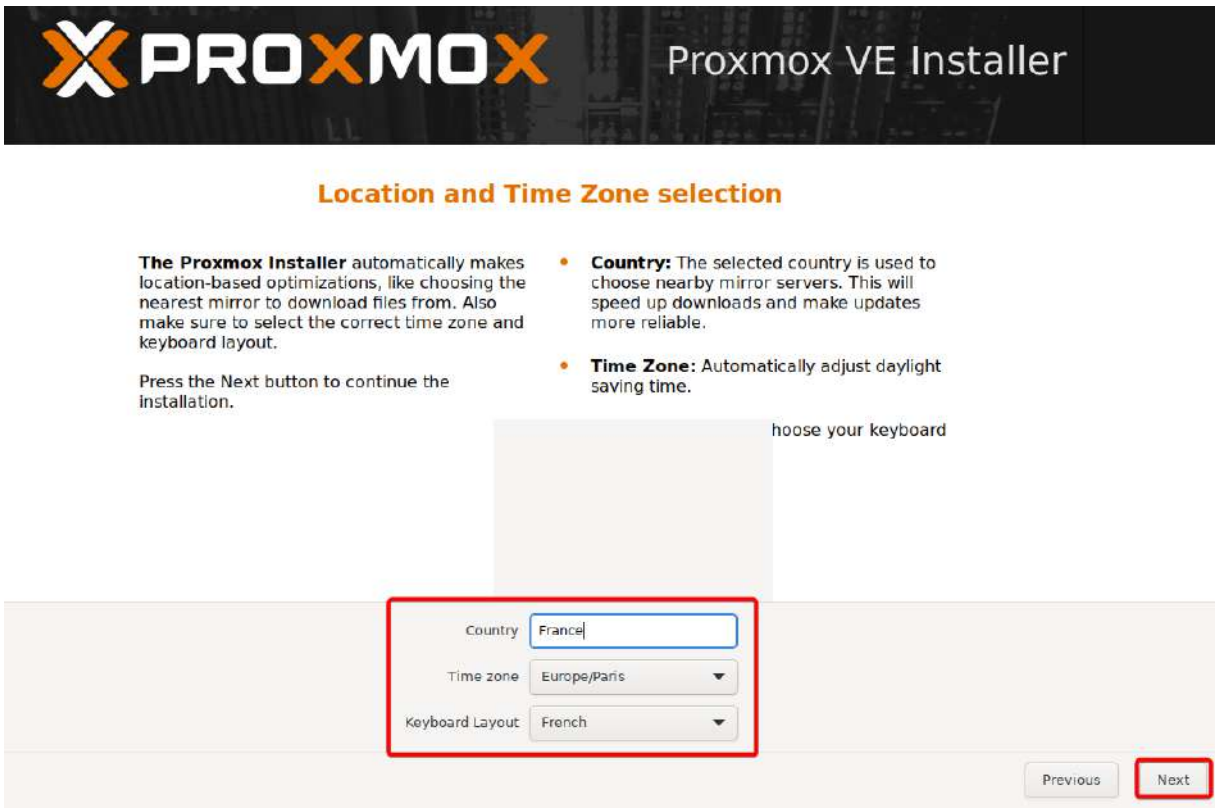
On accepte ensuite l'EULA :



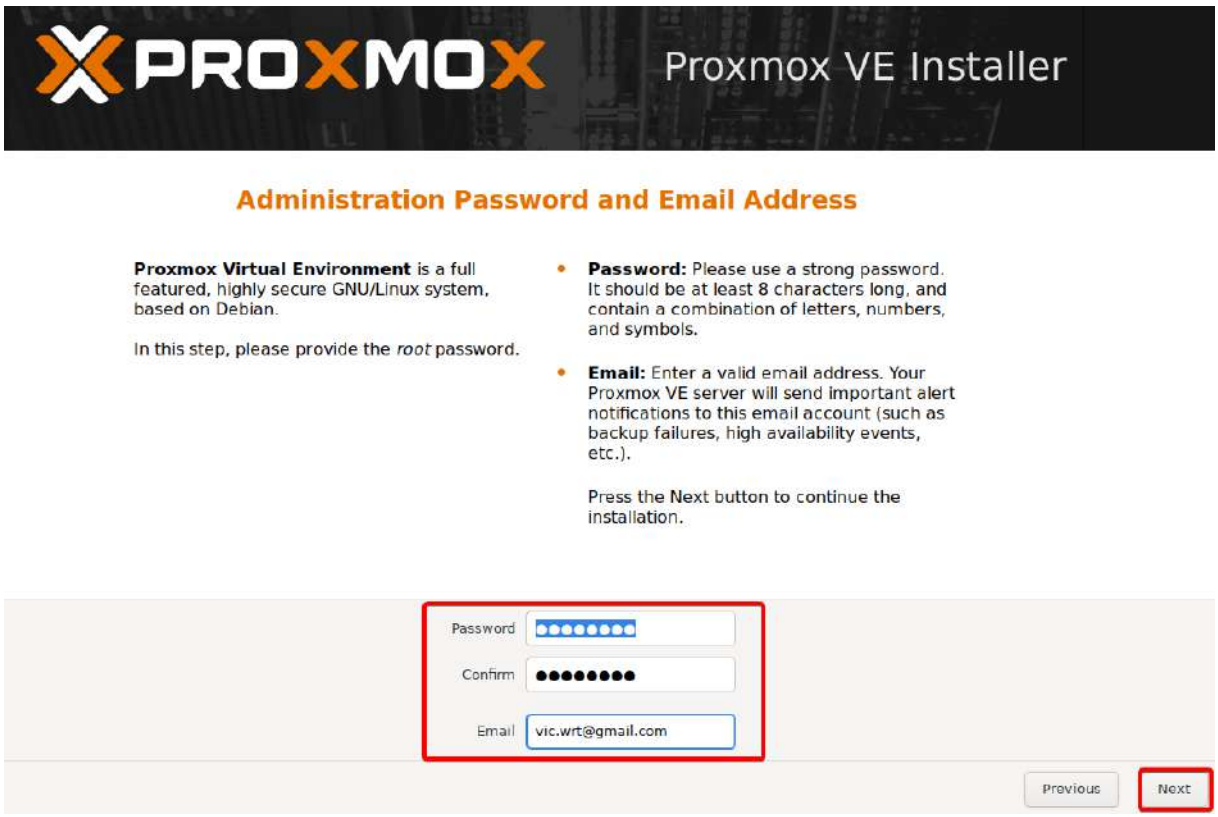
On choisit le disque d'installation :



Puis, la région ainsi que la disposition du clavier :



Ensuite, il faut renseigner le mot de passe root et un email au cas où :



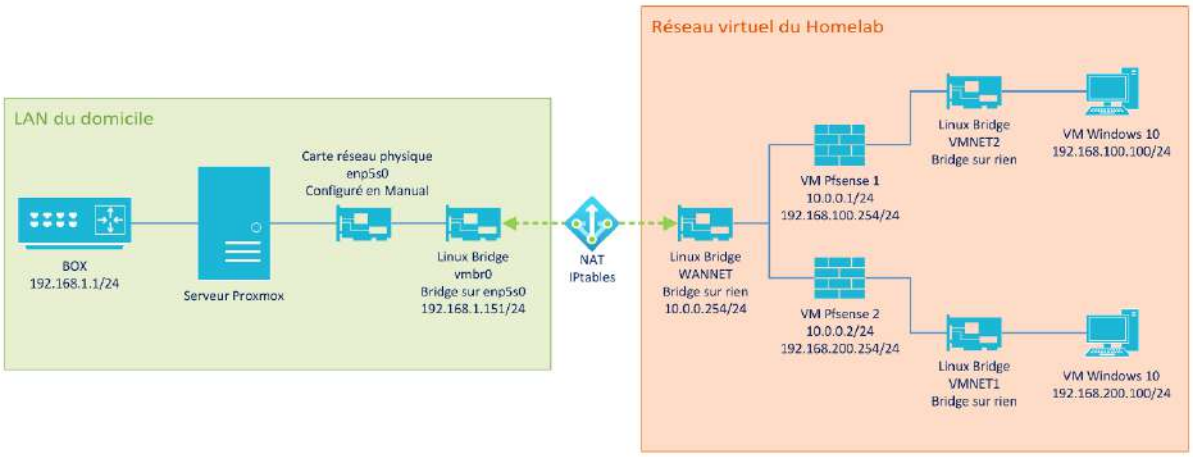
Enfin, on peut renseigner le nom FQDN et les différentes IP (Passerelle, DNS, etc...) :

Il est temps de cliquer sur installer :

2.3) Configuration réseau

2.3.1) Théorie

Dans le cadre d'un home lab, il peut être judicieux de ne pas bridge les VM directement sur notre réseau. Nous allons donc mettre en place une interface réseau virtuelle (Linux bridge) qui ne sera bridge sur aucune interface réseau physique, et pour que le trafic vers Internet passe, nous allons faire du forward (NAT) avec IPtables. Voici un schéma reprenant le fonctionnement :



Cela permet d'isoler notre réseau virtuel et de simuler un "WAN" entre le Linux Bridge WANNET et les VMNET1 et VMNET2 sans pour autant provoquer des conflits sur notre LAN.

2.3.2) Configuration interfaces réseau

Pour commencer, nous allons nous connecter en SSH sur notre serveur proxmox :

```
# Dans un cmd.exe se connecter en root en ssh
ssh root@IP_PROXMOX
```

Supprimer les source.list enterprise et ajouter le dépôt community :

```
# Modifier le premier dépôt enterprise
nano /etc/apt/sources.list.d/pve-enterprise.list

# Commenter la ligne suivante
deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise

# Modifier le second dépôt
nano /etc/apt/sources.list.d/ceph.list

# Commenter la ligne suivante
deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise

# Modifier les dépôts
nano /etc/apt/sources.list

# Ajouter la ligne suivante dans le sources.list
deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription

# Mettre à jour les dépôts
apt update
```

Puis modifier nos interfaces réseau :

```
# modifier les interfaces réseau
nano /etc/network/interfaces
```

Notre fichier de configuration devrait ressembler à cela :

```
auto lo
iface lo inet loopback
iface enp5s0 inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.1.151/24
        gateway 192.168.1.1
        bridge-ports enp5s0
        bridge-stp off
        bridge-fd 0
```

```
source /etc/network/interfaces.d/*
```

Nous allons donc rajouter les interfaces virtuelles souhaitées :

```
auto WANNET
iface WANNET inet static
      address 10.0.0.254/24
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET1
iface VMNET1 inet static
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET2
iface VMNET2 inet static
      bridge-ports none
      bridge-stp off
      bridge-fd 0
```

Ce qui devrait nous donner :

```
auto lo
iface lo inet loopback

iface enp5s0 inet manual

auto vmbr0
iface vmbr0 inet static
      address 192.168.1.151/24
      gateway 192.168.1.1
      bridge-ports enp5s0
      bridge-stp off
      bridge-fd 0

auto WANNET
iface WANNET inet static
      address 10.0.0.254/24 #cette IP sera utilisé comme "passerelle" pour le NAT
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET1
iface VMNET1 inet static
```

```
        bridge-ports none
        bridge-stp off
        bridge-fd 0

auto VMNET2
iface VMNET2 inet static
        bridge-ports none
        bridge-stp off
        bridge-fd 0

source /etc/network/interfaces.d/*
```

Ensuite, nous pouvons redémarrer le service networking et désactiver/réactiver chaque interface virtuelle créée :

```
# redémarrer le service networking
 systemctl restart networking

# redémarrer chaque interface
ifdown WANNET && ifup WANNET
ifdown VMNET1 && ifup VMNET1
ifdown VMNET2 && ifup VMNET2
```

2.3.3) Configuration du NAT IPtables

Il faut ensuite configurer le NAT entre les interfaces vmbr0 et WANNET.

Tout d'abord, il faut autoriser le forwarding IPv4 :

```
# editer le fichier sysctl.conf
nano /etc/sysctl.conf

# Puis décommenter la ligne suivante :
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Après avoir enregistré le fichier, il est nécessaire d'appliquer les changements avec la commande suivante :

```
sysctl -p
```

Maintenant, nous allons appliquer les règles IPtables :

```
# Appliquer du nat (masquerade) pour le réseau source 10.0.0.0/24 qui sortira par l'interface vmbr0
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o vmbr0 -j MASQUERADE
```

```
# Autoriser le flux à transiter entre l'interface WANNET et vmbr0 pour les connections déjà établies et existantes
iptables -A FORWARD -i WANNET -o vmbr0 -j ACCEPT
iptables -A FORWARD -i vmbr0 -o WANNET -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Une fois cela fait, il se nous reste plus qu'à rendre persistante ces règles même après un reboot :

```
# Mettre à jour les paquets
apt update

# Installation de iptables-persistent
apt install iptables-persistent
```

Lors de l'installation, sauvegarder les règles IPv4. Il est aussi possible de les sauvegarder avec la commande suivante :

```
# sauvegarder les reègles en place
netfilter-persistent save

# reload le service pour prise en compte
netfilter-persistent reload
```

Après avoir installé le service, nous allons le restart puis tout sera en place !

```
systemctl restart netfilter-persistent
```

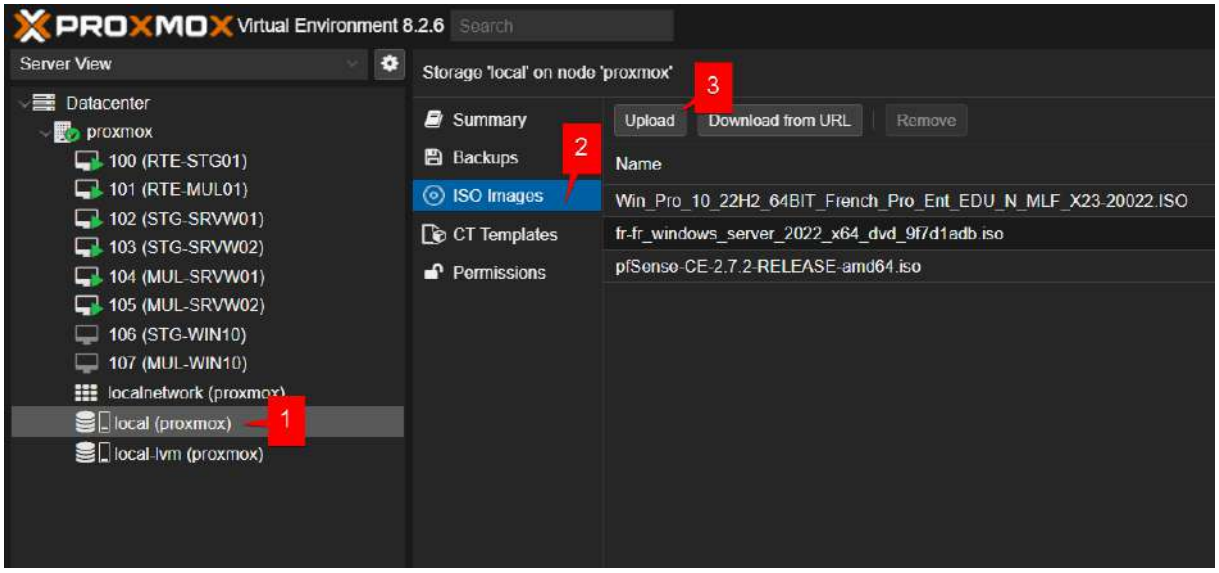
Nos VM connectées à l'interface virtuelle WANNET ont accès à Internet en passant par la passerelle 10.0.0.254/24 et possèdent une plage d'adresse pour elles (10.0.0.0/24), cela pourrait permettre de simuler un "WAN" par exemple.

2.4) Ajouter des ISO et créer sa première VM

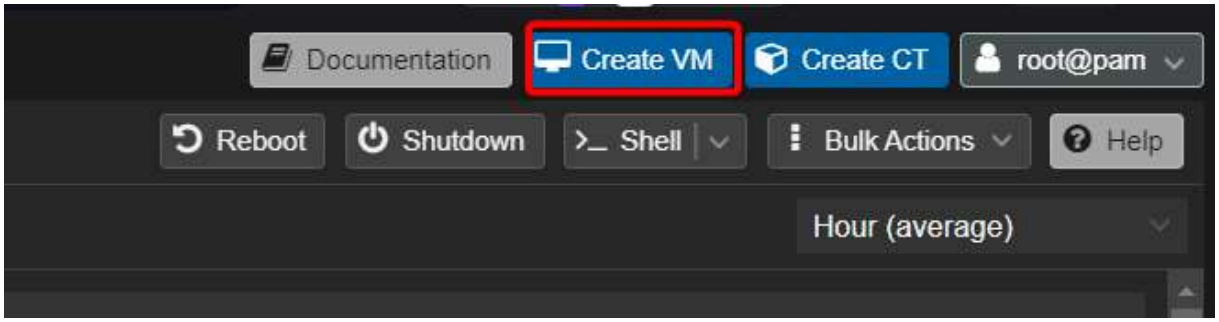
Proxmox prévoit un emplacement spécifique pour les ISO (dans le /var/lib/vz/template/iso) afin de les centraliser.

Pour en ajouter une, il faut se connecter à l'interface promox (https://IP_PROXMOX:8006). Les identifiants sont "root" et le mot de passe mis lors de l'installation.

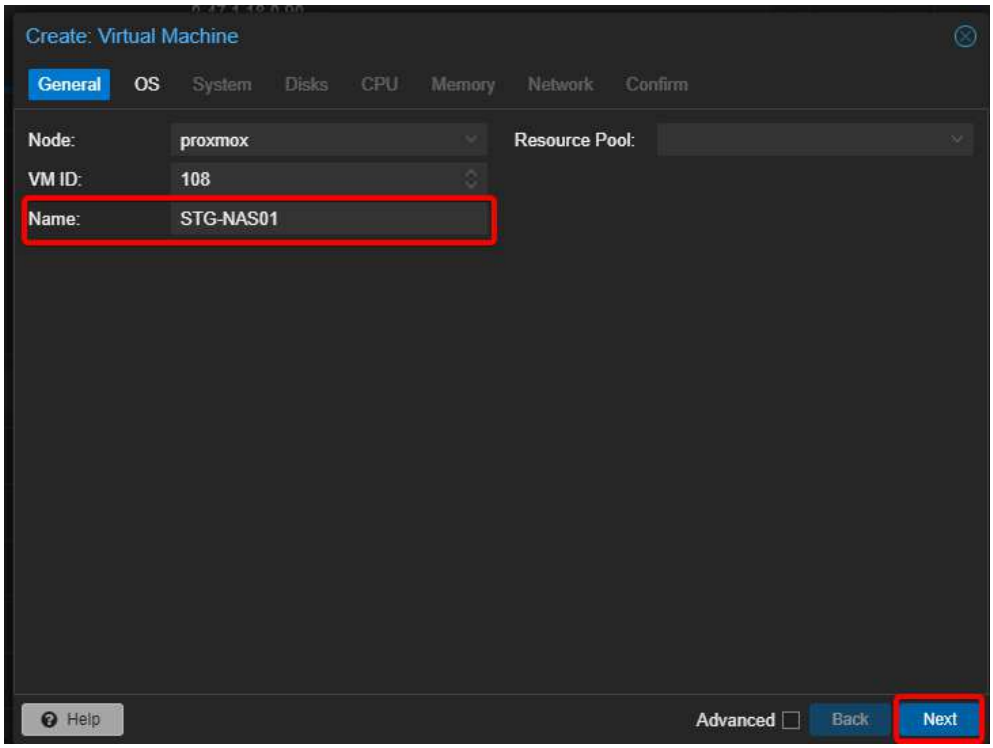
Puis développer le Datacenter et le noeud proxmox, cliquer sur votre stockage local (1), puis ISO Images (2) et enfin Upload (3) :



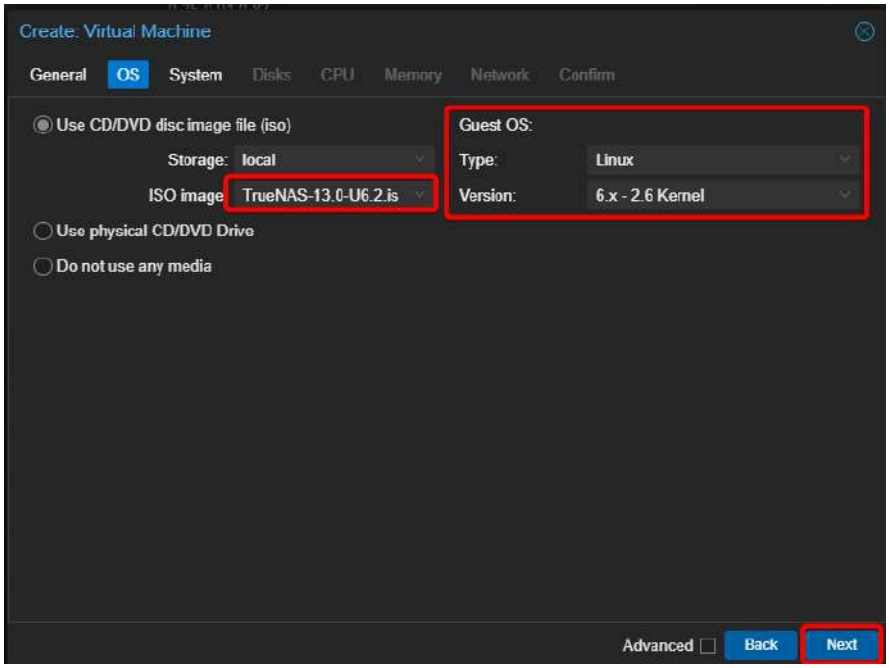
Pour créer votre première VM, nous allons cliquer sur "Create VM" en haut à droite :



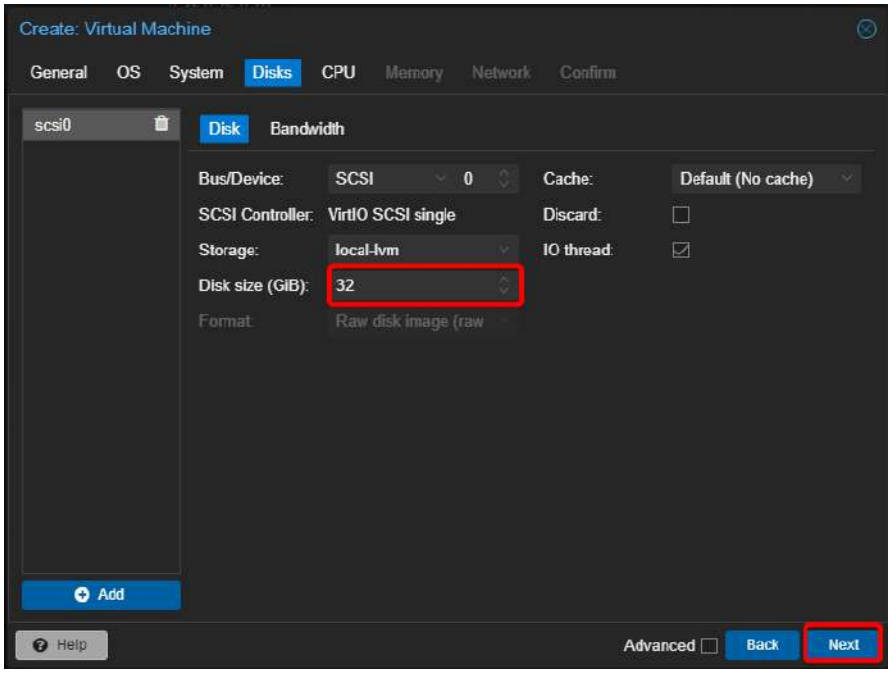
Ensuite, nous allons lui donner un nom, je laisse l'ID par défaut et vérifie qu'elle soit bien dans le nœud proxmox :



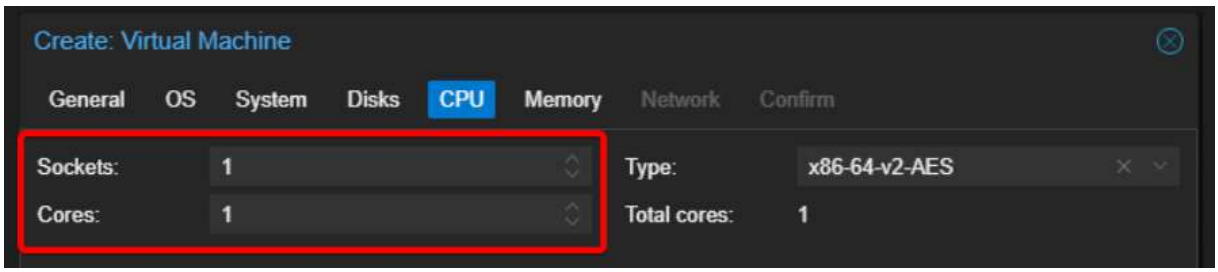
Après je sélectionne l'ISO et l'OS souhaitée :



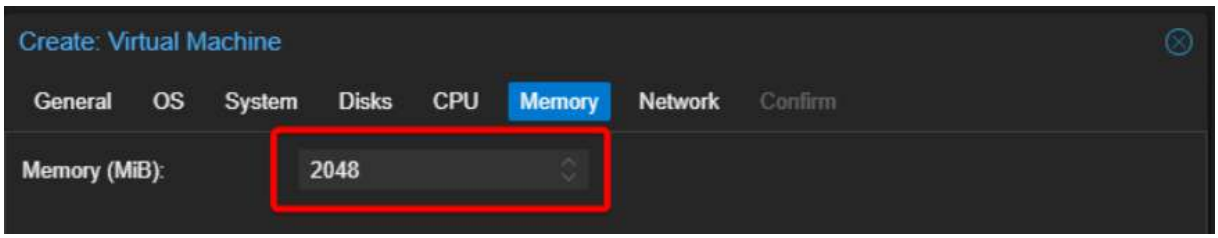
Ensuite, on peut laisser par défaut la partie System, puis on créé un disque virtuel :



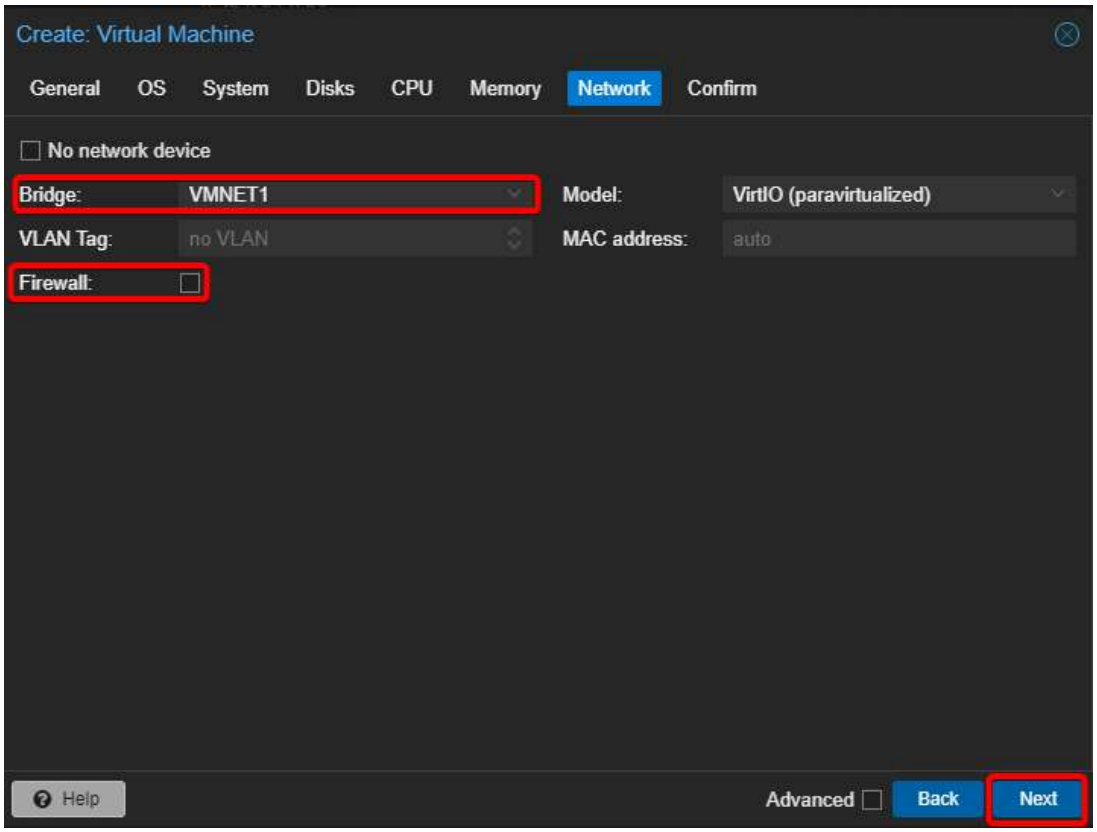
J'attribue le nombre de CPU :



La RAM :



Et enfin, l'interface réseau sur laquelle ma VM sera et je n'oublie pas de décocher le firewall :



On peut ensuite cliquer sur Finish, et voilà, la VM est maintenant créé.

2.5) Joindre l'hyperviseur depuis Internet

Il peut être pratique de joindre son hyperviseur depuis l'extérieur. Certains opérateurs ne permettent plus une ouverture de port correcte en IPv4. Ainsi, nous allons utiliser Tailscale pour rendre notre hyperviseur accessible depuis Internet.

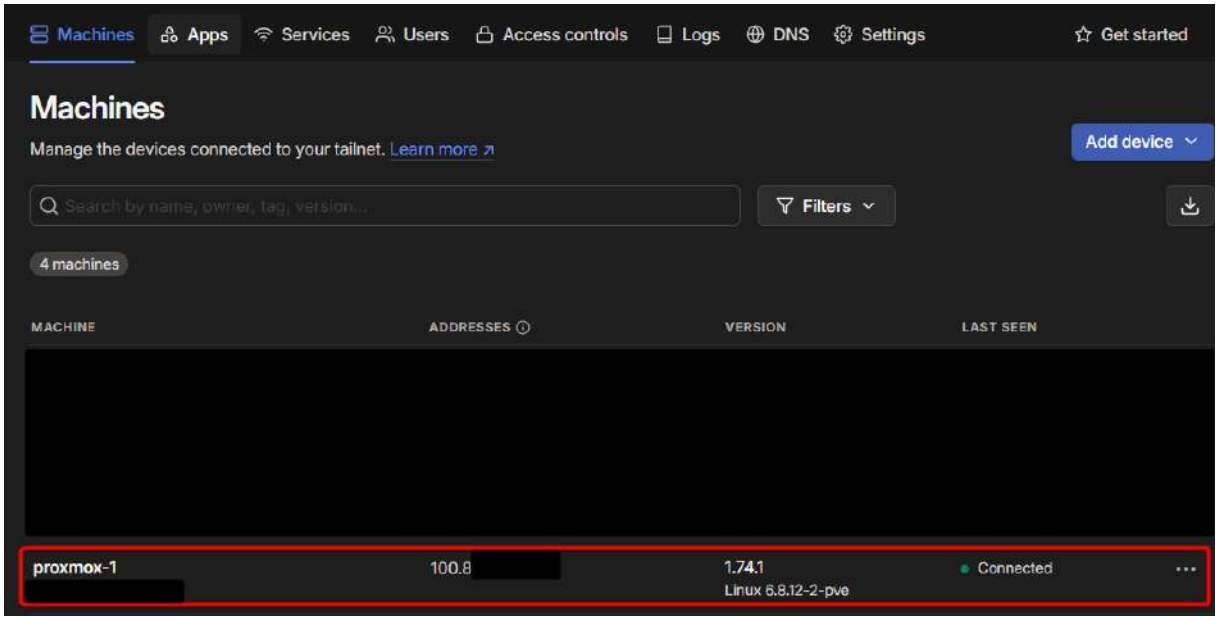
Pour cela, il suffit d'installer tailscale sur notre proxmox :

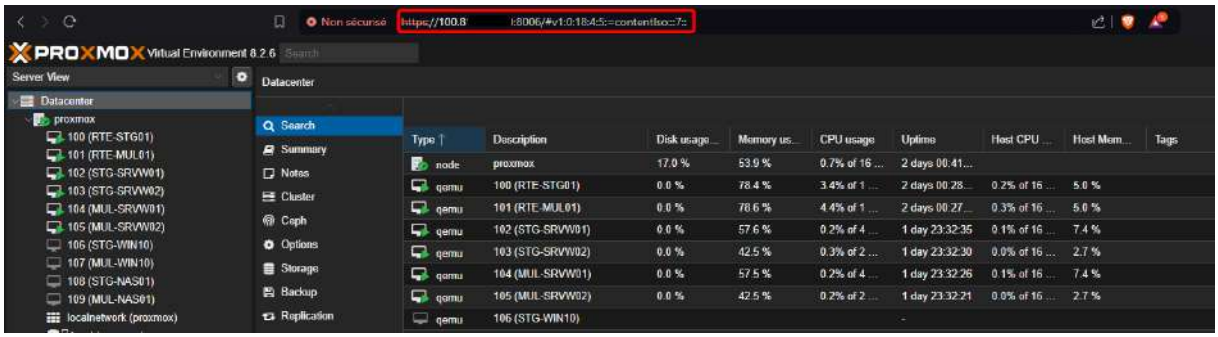
```
# se connecter en SSH
ssh root@IP_PROXMOX

# installer tailscale (nécessite une connexion Internet)
curl -fsSL https://tailscale.com/install.sh | sh
```

```
# lancer le login
tailscale up
```

Ensuite il faudra juste vous connecter sur un autre appareil à votre compte Tailscale avec le lien qui sera renvoyé à la suite du tailscale up.

Pour se connecter dessus avec un autre appareil, il faudra que vous ayez installé et configuré Tailscale sur l'appareil souhaité (https://tailscale.com/download/windows) puis sur l'Admin console, vous pourrez retrouver l'IP Tailnet de votre Hyperviseur et vous y connecter :

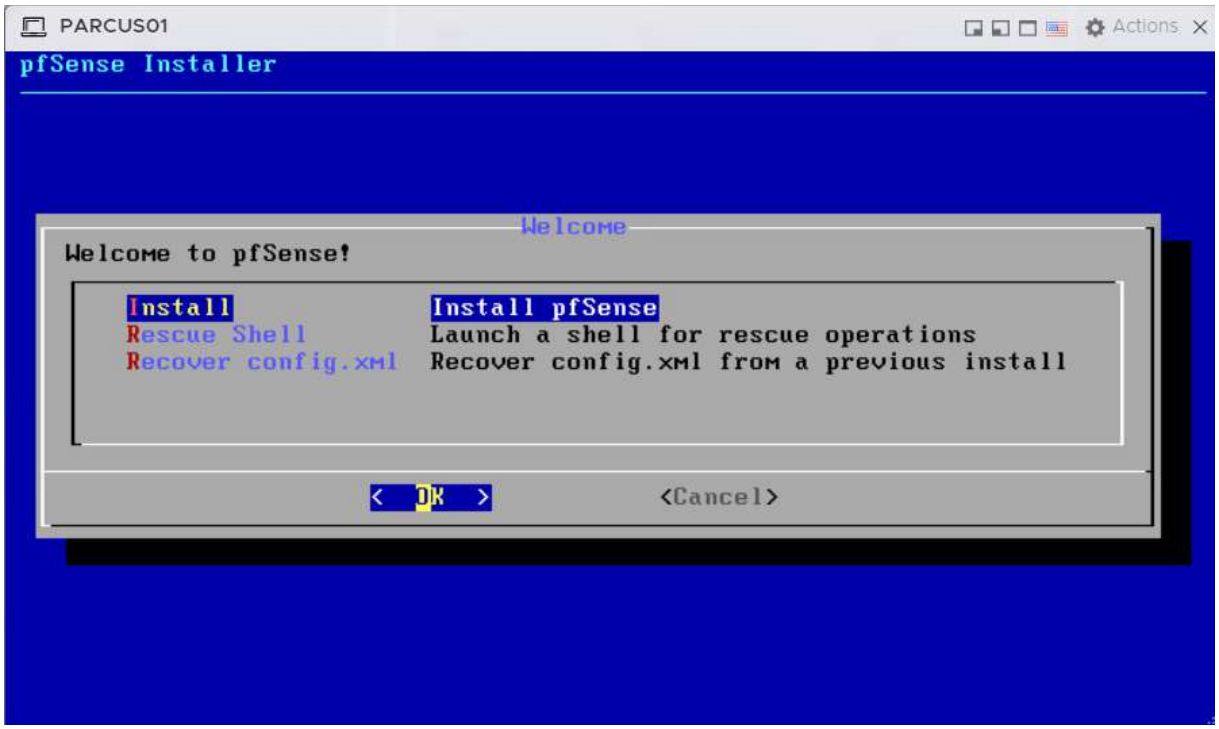


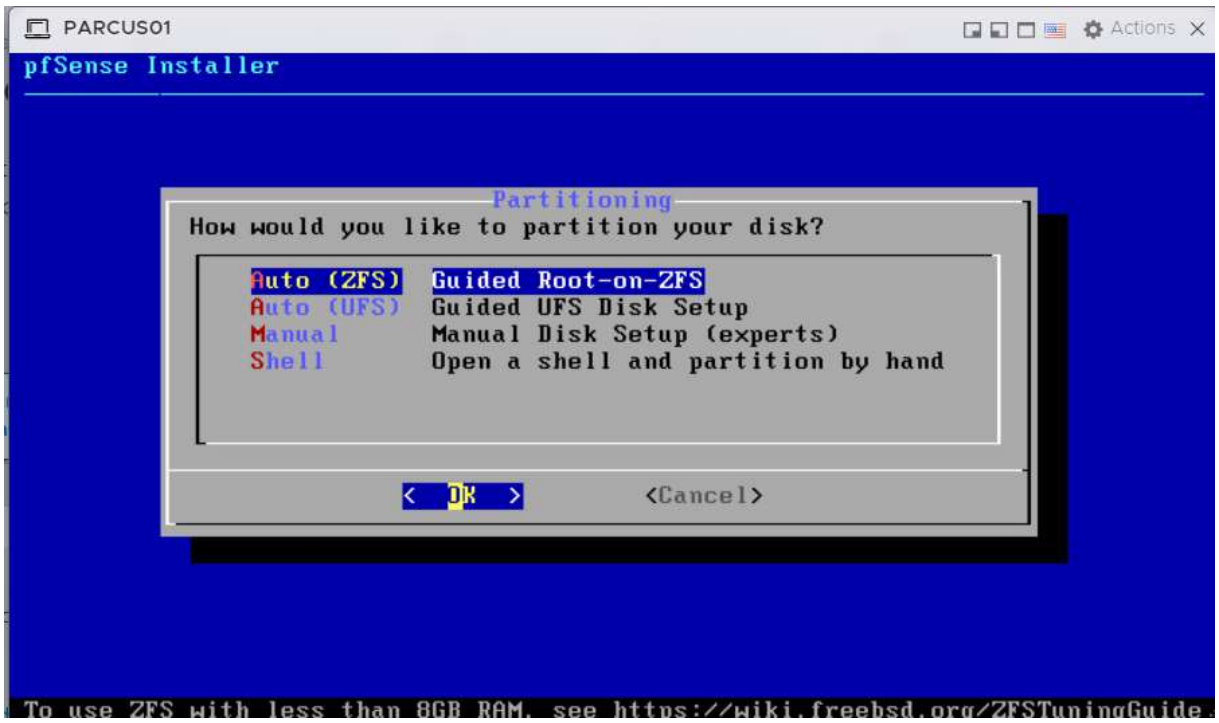


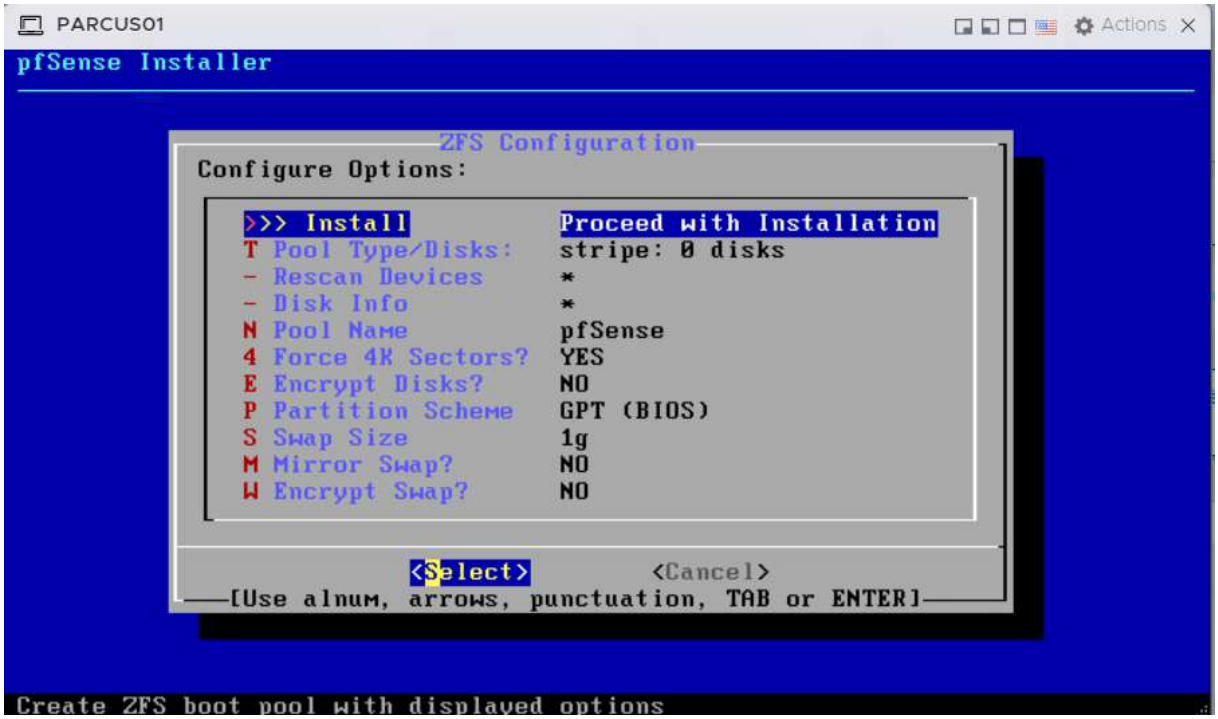
3) Installation et configuration de Pfsense

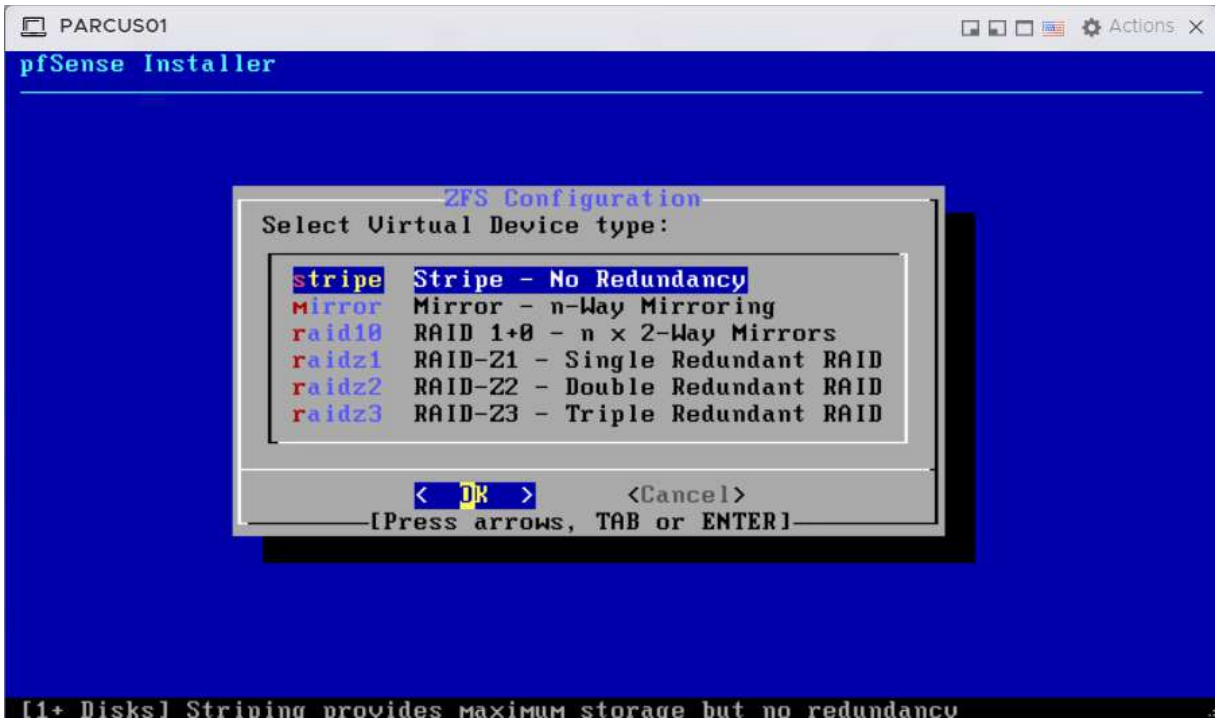
3.1) Installation de Pfsense

Mettre sous tension la machine, puis au lancement, lancer l'installation de pfsense :

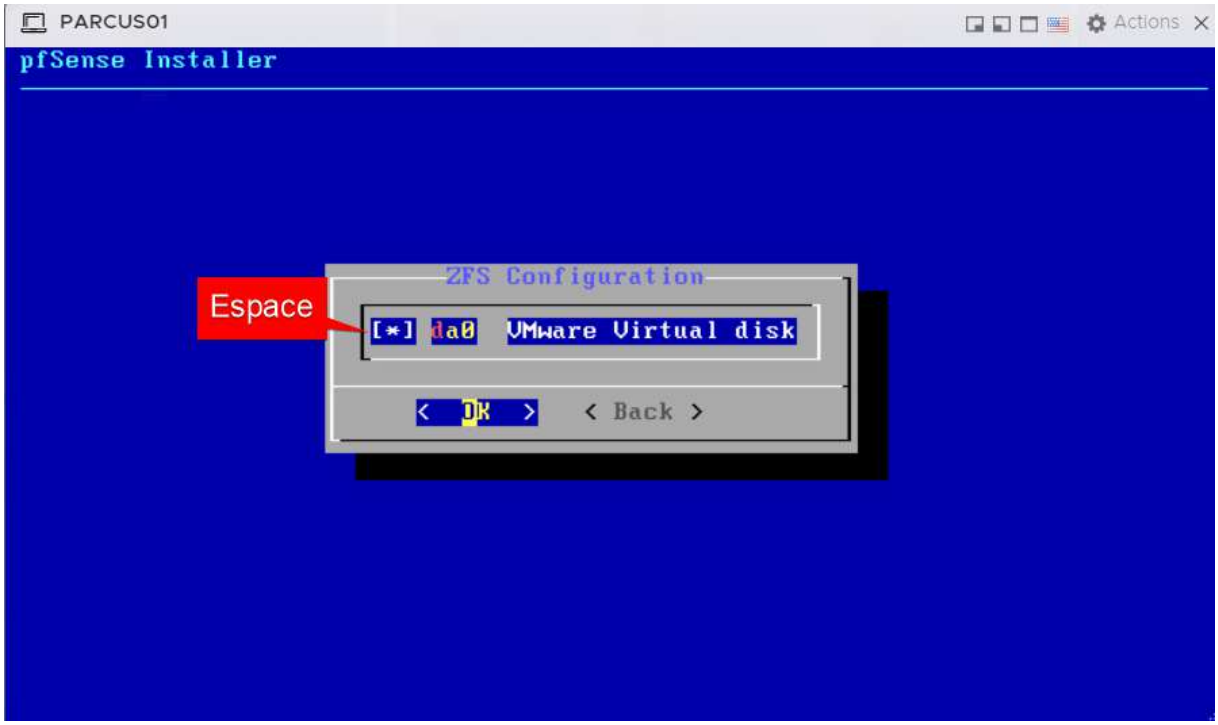


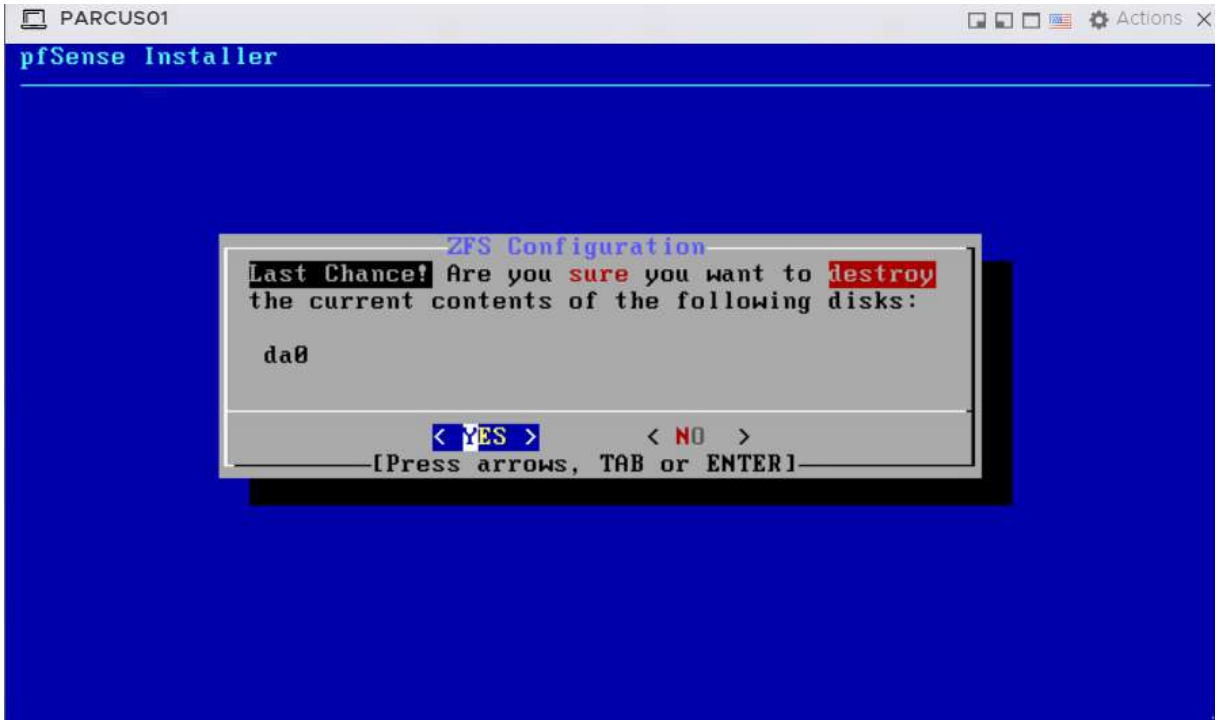



PARCUS01
Actions
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options


PARCUS01
Actions
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy

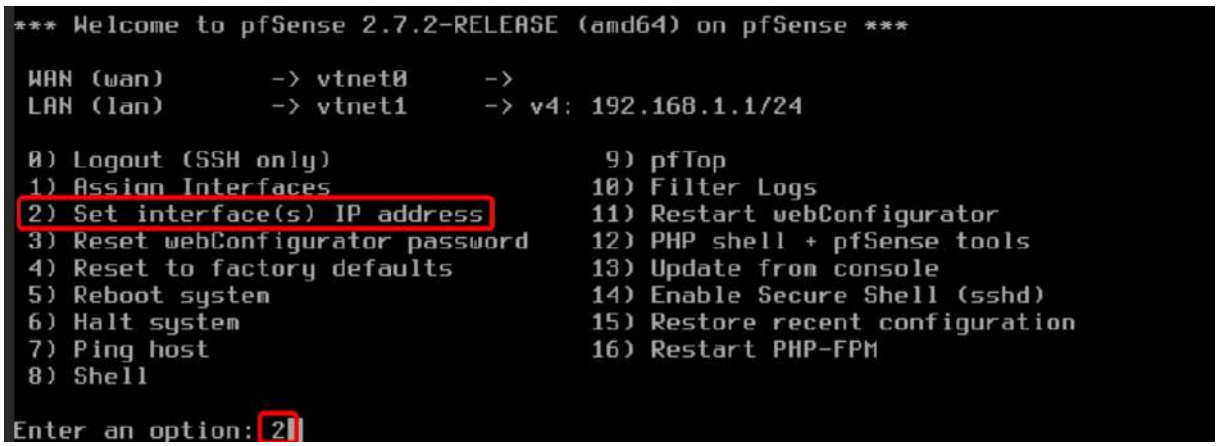
Sélectionner le disque avec la touche espace puis continuer :



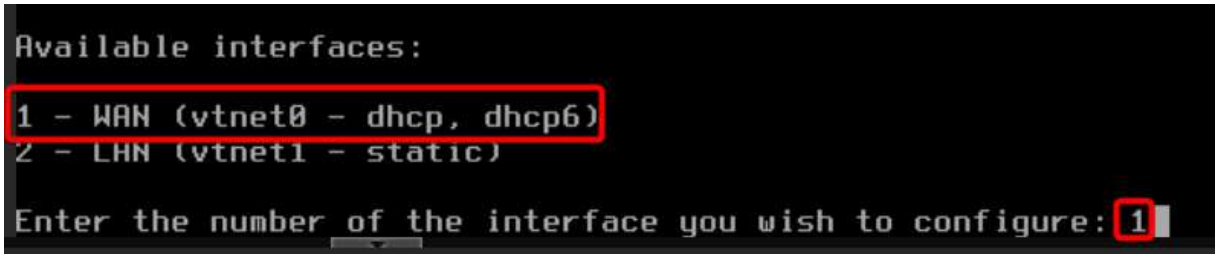


Ensuite, on va nous proposer de reboot la machine, on accepte donc de reboot la machine.

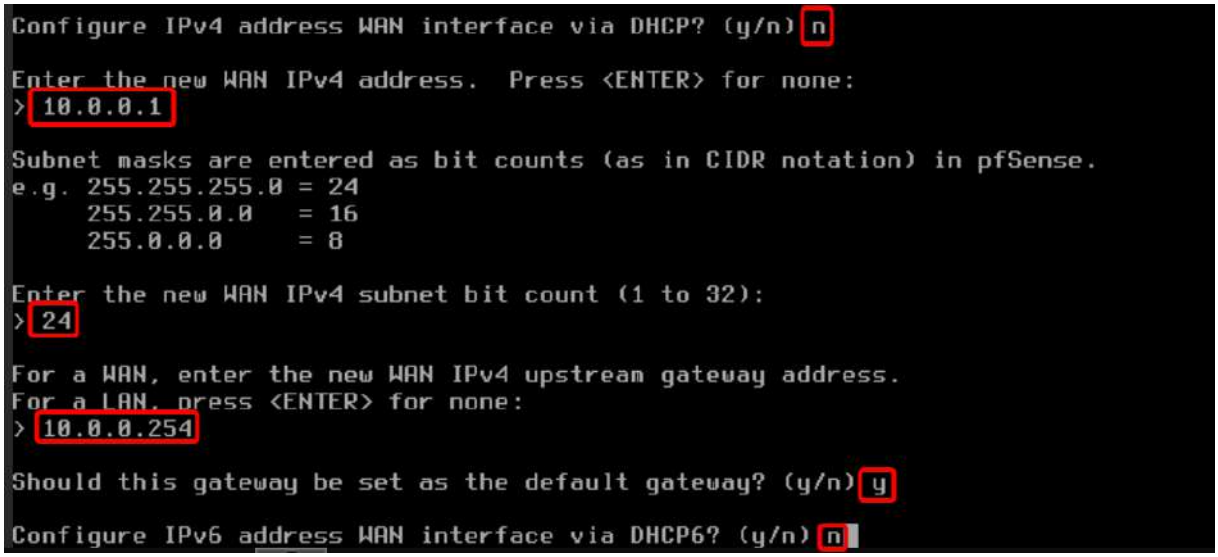
On sélectionne l'option 2 afin de set les adresses IP des interafces réseaux :



Puis, on sélectionne l'interface WAN :



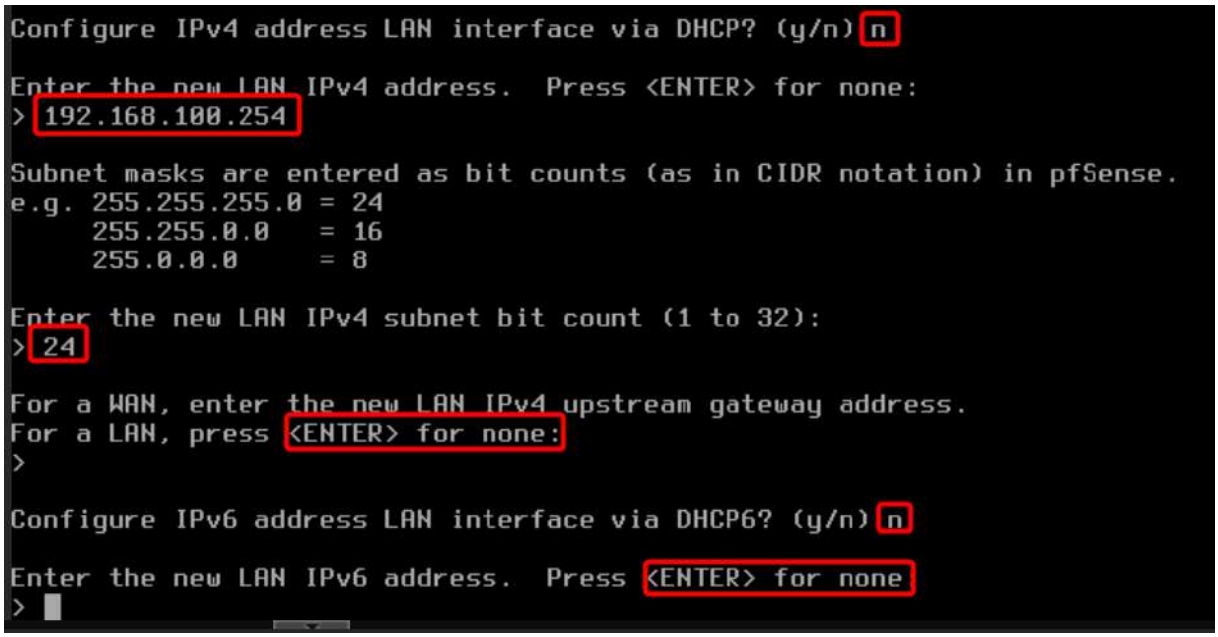
Ensuite, on configure l'adresse IPv4 WAN et la passerelle WAN :



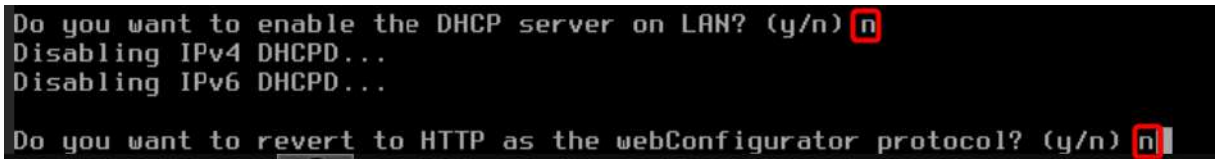
On ne configurera pas d'IPv6 dans notre cas et on laisse le protocole HTTPS :

On configure ensuite l'interface LAN :

On rentre notre IPv4, nous ne configureront pas d'IPv6 :



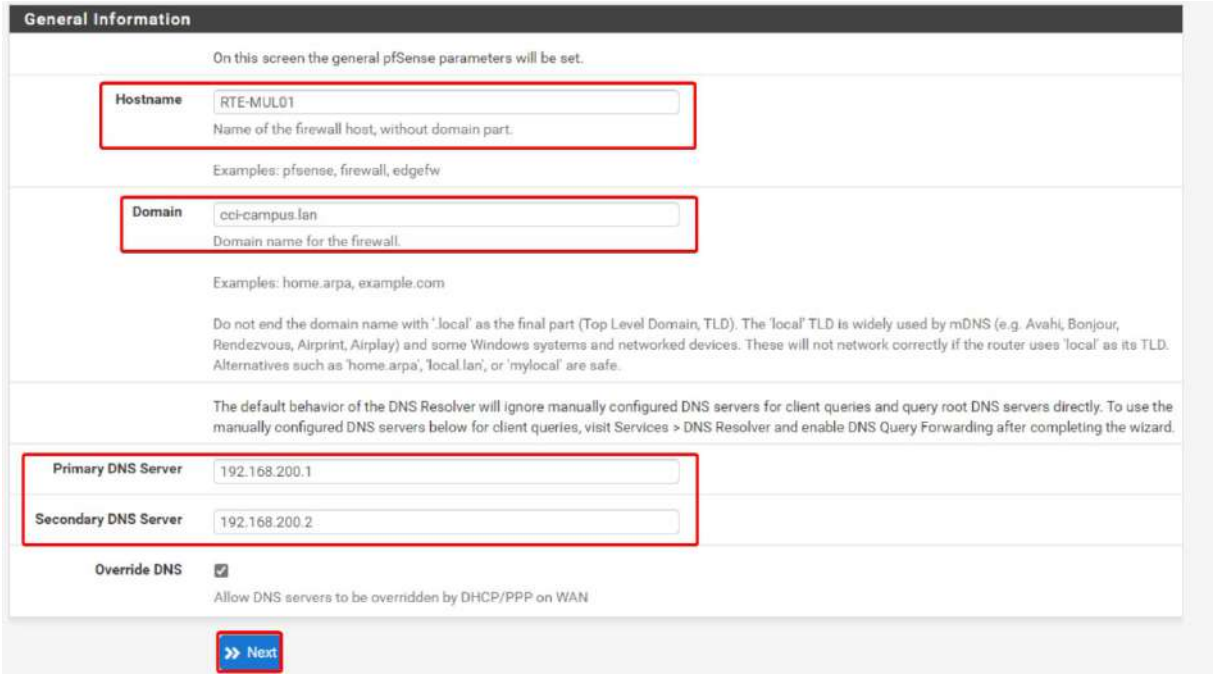
On n'activera pas le serveur DHCP sur le LAN et on laisse le protocole HTTPS :



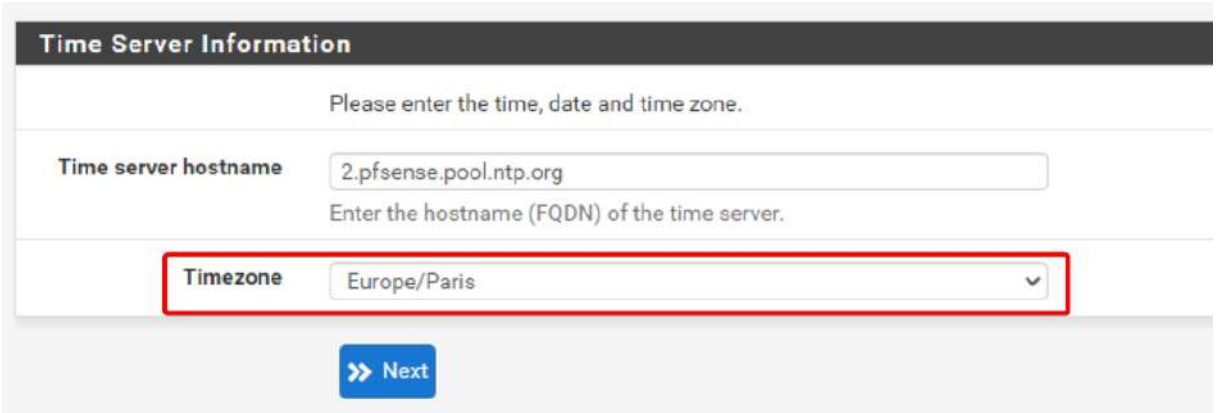
3.2) Configuration de Pfsense

Pour cette partie, il faudra accéder à l'interface web de notre pfsense : https://IP_PFSENSE

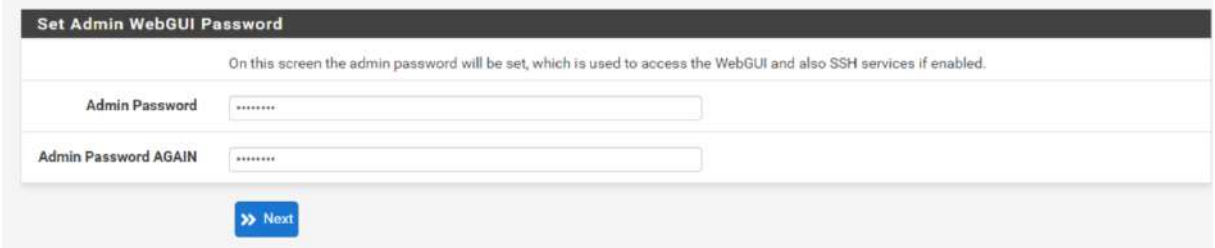
Le wizard va se lancer, il faut donc configurer le hostname, le domaine et les DNS :



On sélectionne notre timezone, puis Next :

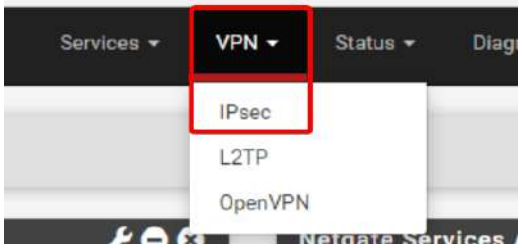


On peut cliquer 2 fois sur suivant, et ensuite saisir notre mot de passe Admin :



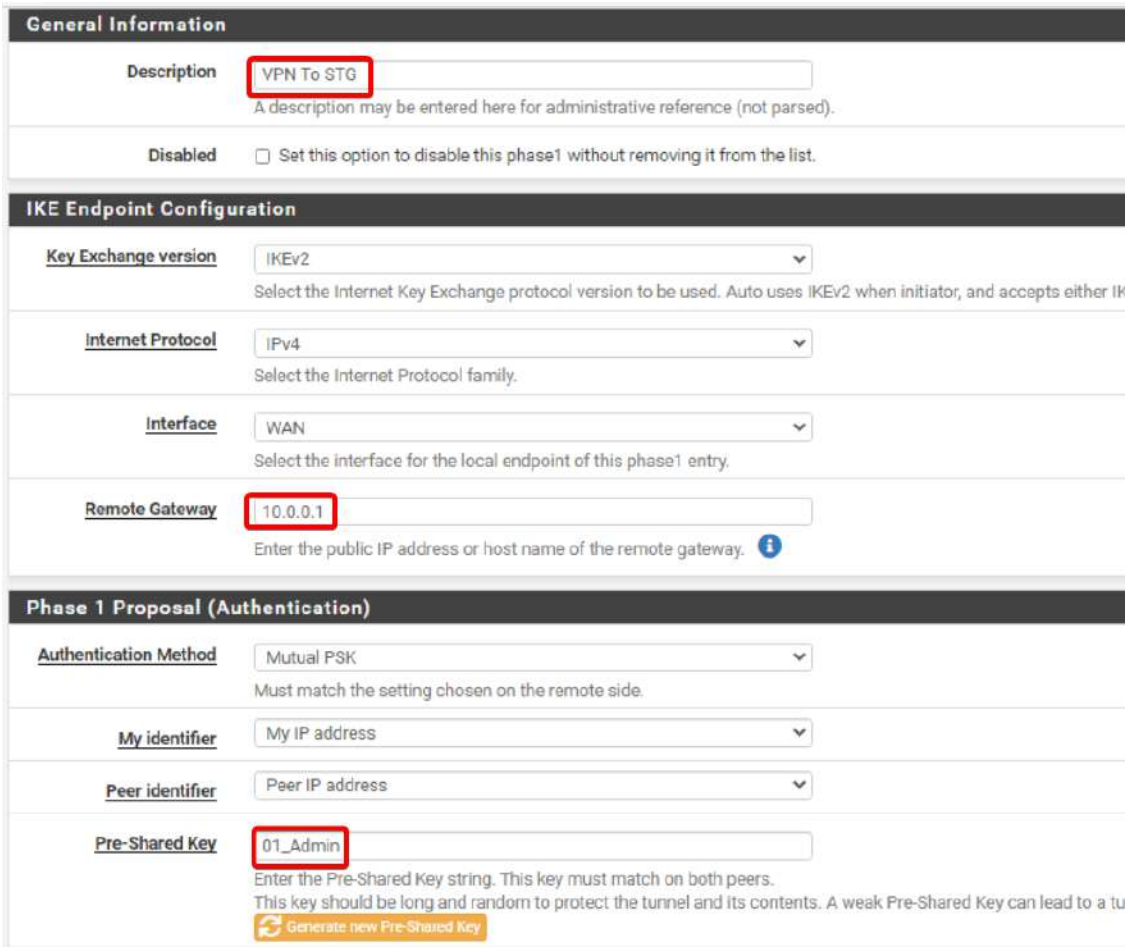
3.3) Mise en place du VPN IPsec site à site

Pour mettre en place le VPN IPsec site à site, on va dans l'onglet "VPN", puis "IPsec" :

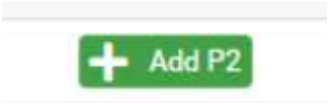


On clique ensuite sur "Add P1" :

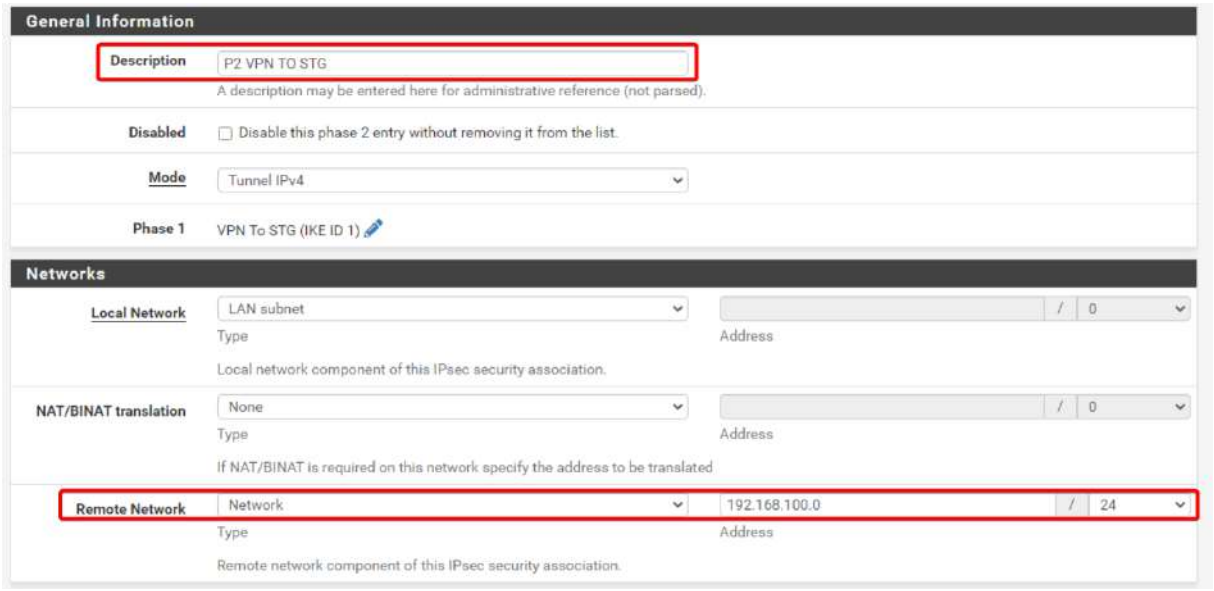
On donne une description à notre P1, l'adresse IP publique de notre pfsense de destination et une clé partagée :



Après avoir sauvegarder la P1, on clique sur Add P2

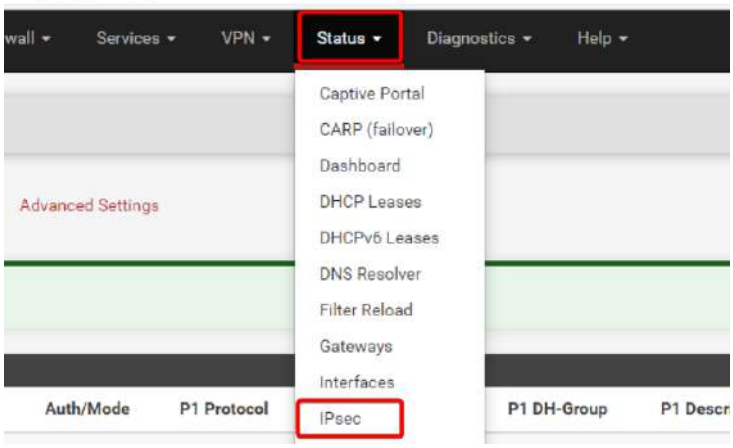


Pour notre P2, il suffira de rentrer la description et le réseau cible (dans notre cas 192.168.100.0/24) et enregistrer / appliquer les modifications :



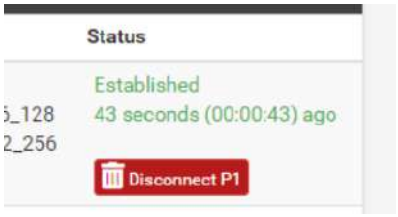
Aller ensuite sur l'interface web de votre deuxième Pfsense, répéter les mêmes opérations en adaptant les adresses IP.

Une fois cela effectué, aller dans l'onglet "Status", puis "IPsec" :

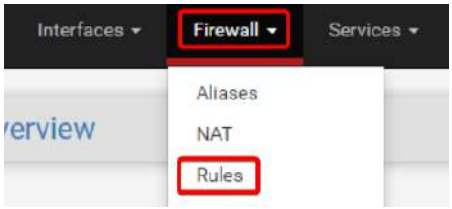


On clique ensuite sur "Connect P1 and P2s" :

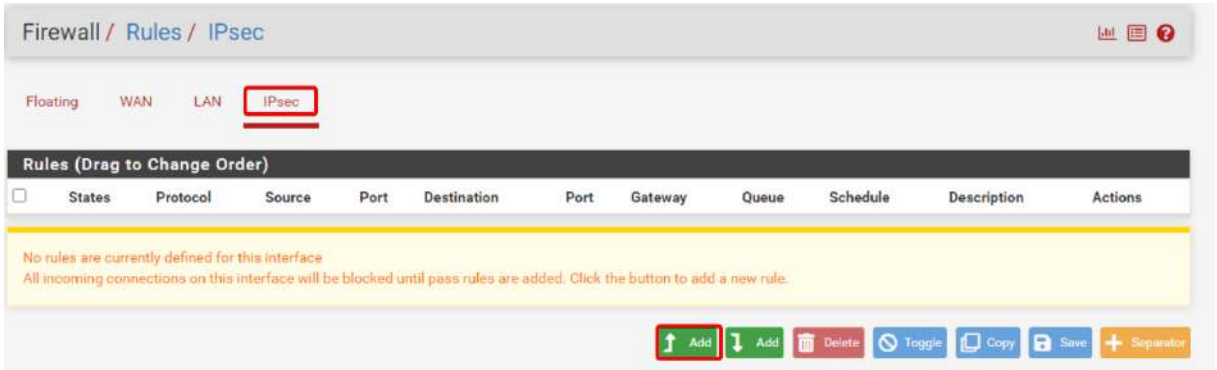
Si la configuration est correcte, la connexion sera considérée comme "Established" :



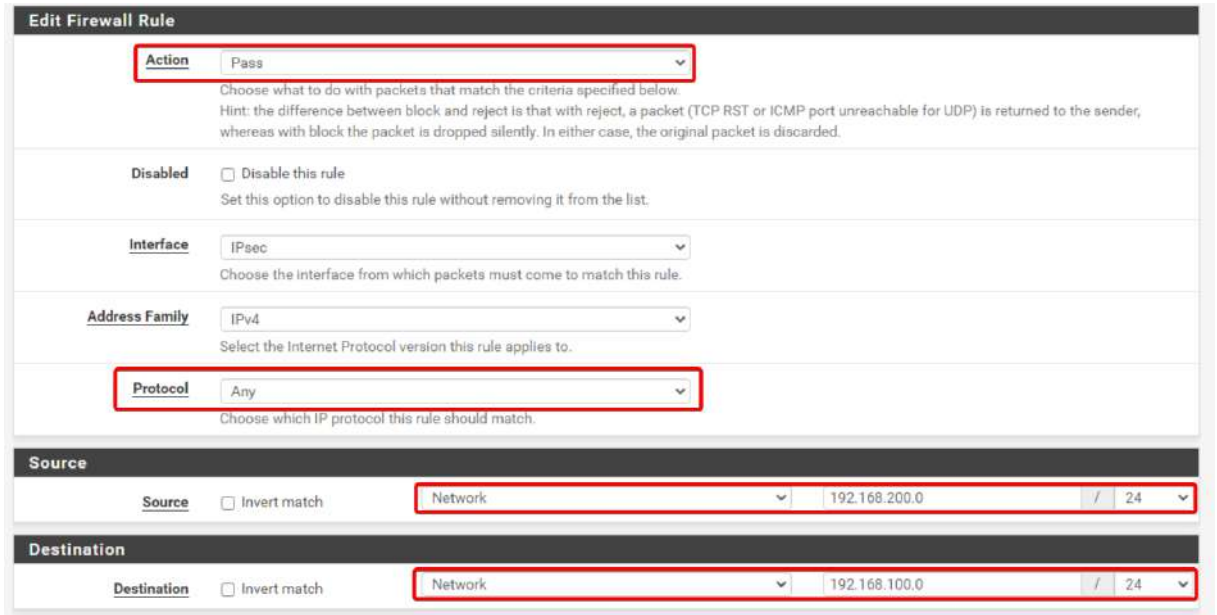
Il ne reste plus qu'à configurer les règles de Firewall, pour se faire, aller dans l'onglet "Firewall", "Rules" :



Puis sous IPsec, cliquer sur Add :



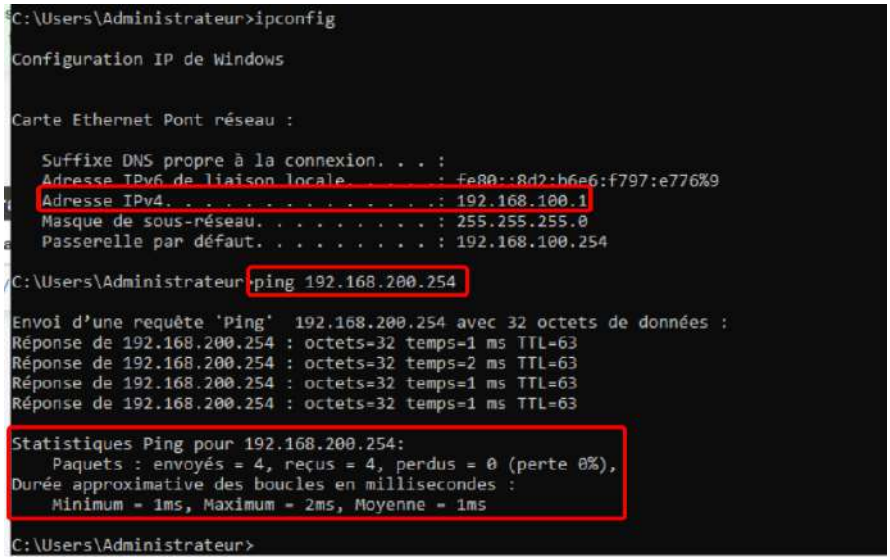
Etant donné que nous sommes sur le pfsense connecté au sous réseau 192.168.100.0/24, nous allons devoir accepter les connexions provenant du sous réseau 192.168.200.0/24 et qui ont pour destination le 192.168.100.0/24 :



On peut ensuite appliquer les changements.

Il est nécessaire de réaliser les mêmes opérations en inversant les réseaux de la règle sur le deuxième pfsense.

Nos machines virtuelles peuvent désormais utiliser le tunnel VPN IPsec :



La configuration Pfsense est maintenant terminée.

4) Configuration supplémentaires Windows Serveur 2022

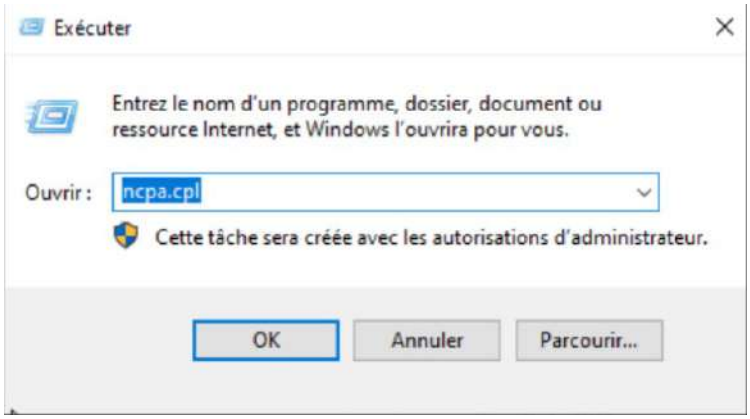
4.1) Redondance réseau (IP Bouding)

4.1.1) Bridge de cartes réseau avec STP actif

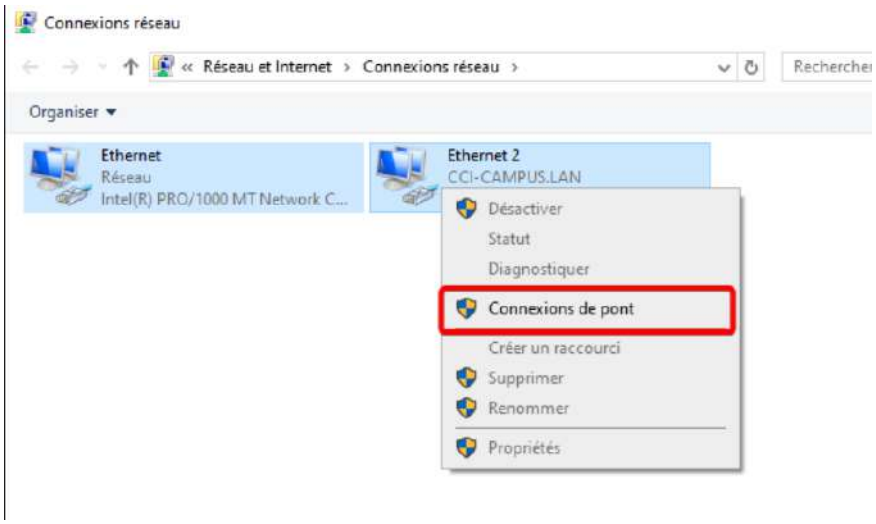
Afin d'assurer la redondance en cas de défaillance d'une carte réseau, il est possible d'utiliser la fonction de pont sur Windows Serveur. Le pont sur Windows sert à relier plusieurs segments réseaux entre eux sans avoir besoin de faire du NAT ou du routage.

> ⚠ Attention
>
> Cette fonction n'est cependant pas prévu pour la redondance, elle peut permettre de la redondance mais peut aussi créer des boucles réseau si le STP n'est pas actif ! De plus, elle ne redirige pas aussi efficacement le flux que le NIC Teaming abordé plus bas !

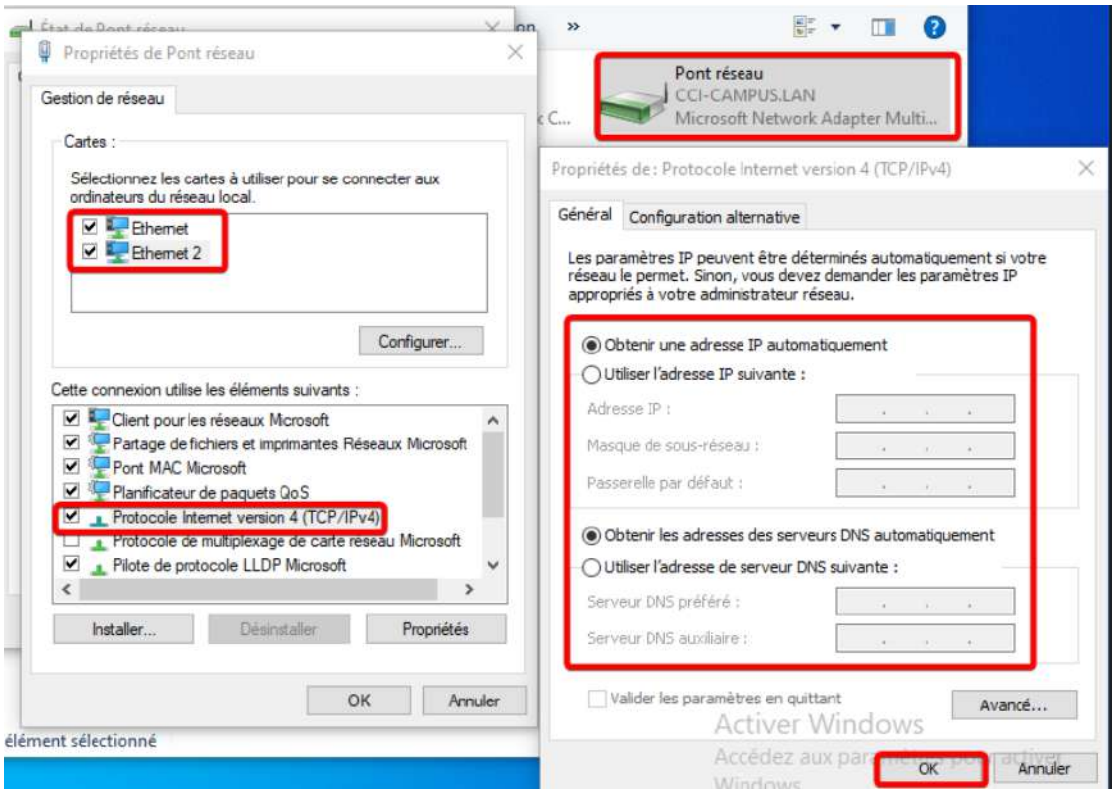
Pour cela, il suffit d'aller dans les connexions réseau du panneau de configuration, dans une fenêtre windows Exécuter (Windows + R) écrire ncpa.cpl :



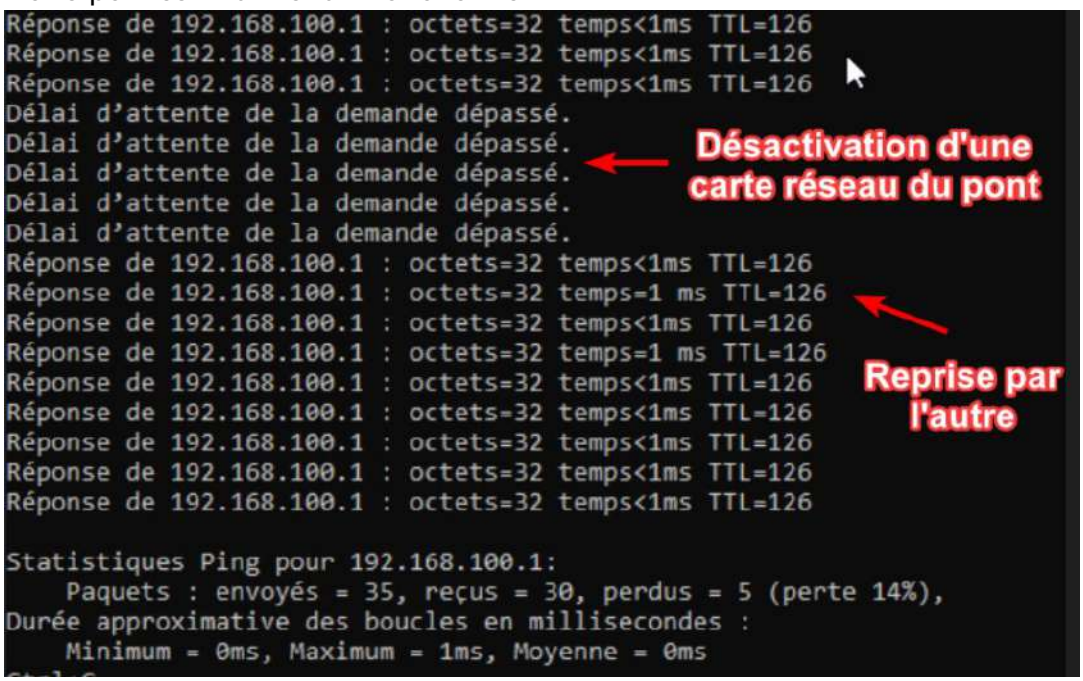
Puis sélectionner les deux cartes réseau et cliquer sur "Connexions de pont" :



Il faudra ensuite faire clic droit sur le pont créé, puis sur propriétés, ensuite on vérifie que nos 2 interfaces réseau sont bien sélectionnées et on double clique sur "Protocole Internet version 4 (TCP/IPv4)" pour venir configurer l'adresse IP statique du pont réseau (si nécessaire) :



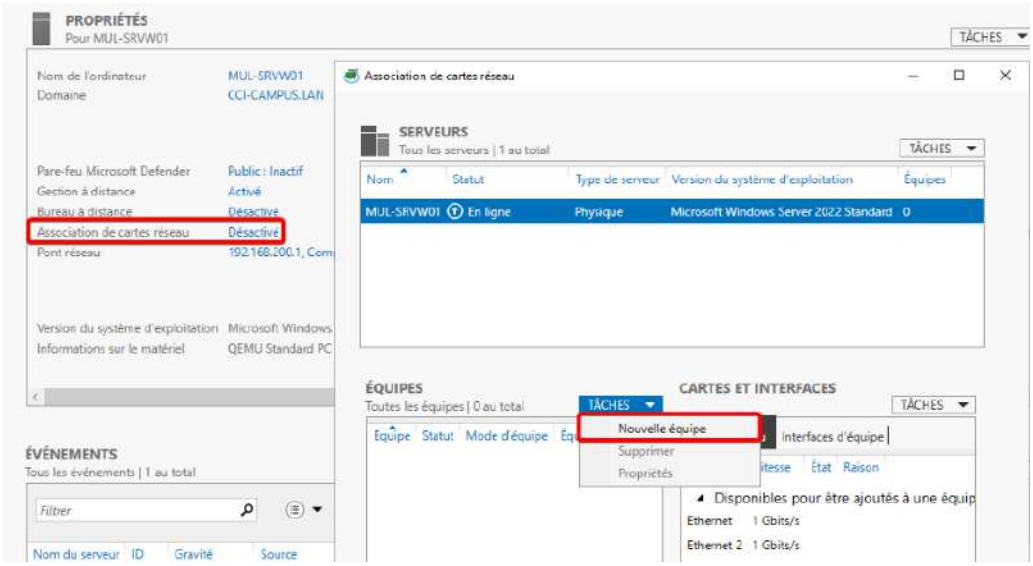
Notre pont est maintenant fonctionnel :



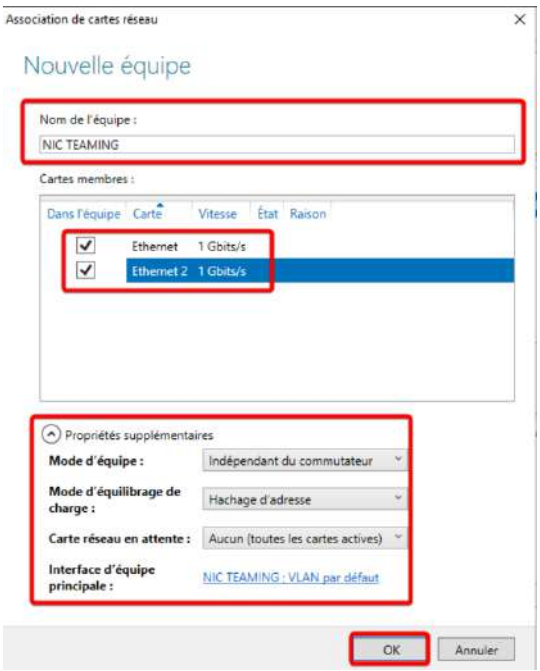
4.1.2) NIC Teaming

Une autre façon (plus capricieuse sur des VM) de créer de la redondance sur les cartes réseau est d'utilise la fonction NIC Teaming de Windows Serveur.

Pour se faire, il faut cliquer sur "Association de cartes réseau" depuis les gestionnaire de serveur, puis dans la rubrique "équipes", on clique sur "Tâches" puis "Nouvelle équipe" :



Puis on donne un nom à notre équipe, on sélectionne nos interfaces réseau et enfin, on règles nos propriétés supplémentaires :

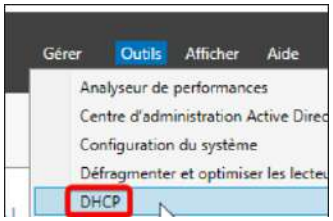


⚠ ATTENTION

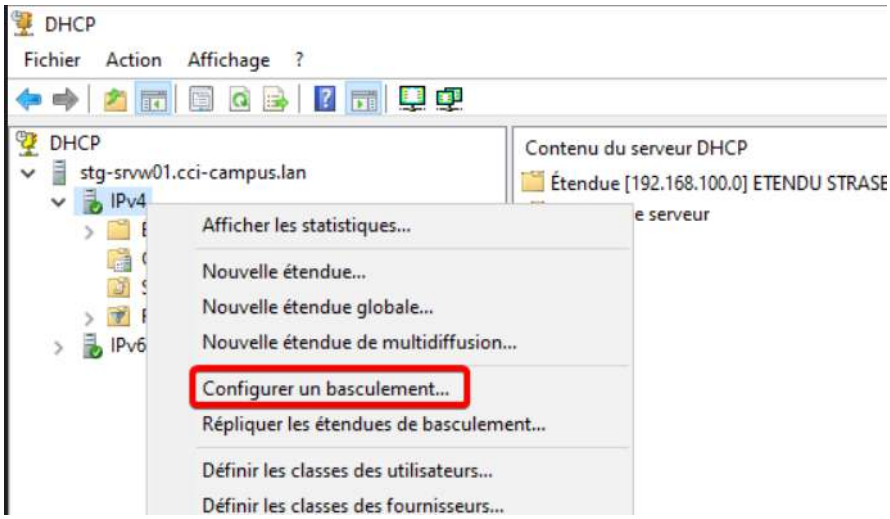
Le NIC Teaming peut ne pas fonctionner dans le cadre de serveurs virtualisés. De plus, la virtualisation n'est pas compatible avec le mode d'équilibrage de charge "Dynamique"

4.2) DHCP de basculement

Pour réaliser la redondance du serveur DHCP, il est nécessaire de créer un basculement DHCP entre les serveurs concernés. Pour se faire, aller dans Outils > DHCP sur le gestionnaire de serveur :

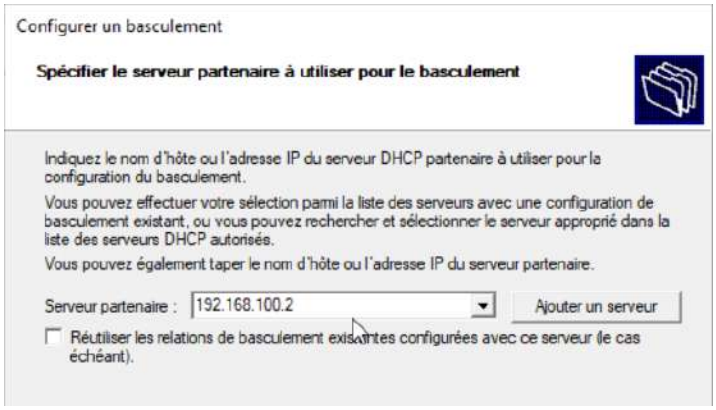


Puis développer le noeud qui correspond à votre serveur, et faite clique droit sur IPv4, puis "Configurer un basculement..." :

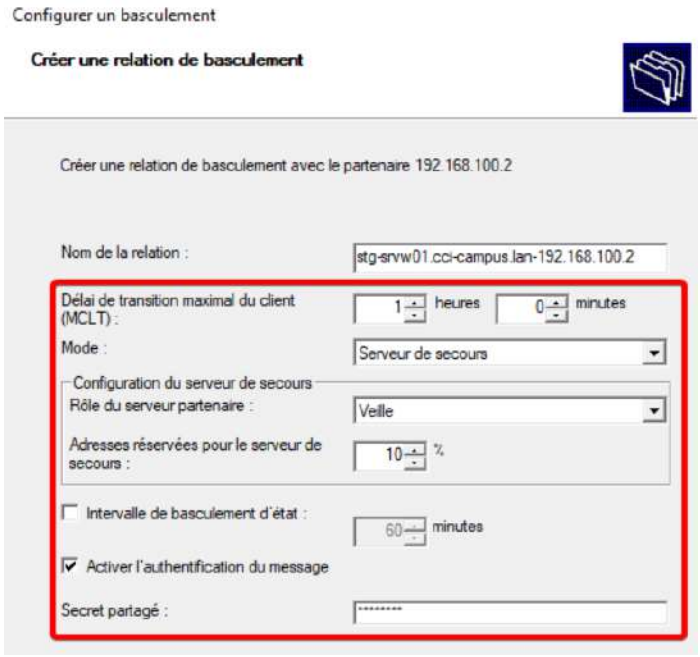


On sélectionne nos étendues :

Puis on choisit le serveur partenaire :



Enfin, on choisit le mode "Serveur de secours" pour de la redondance efficace, on attribue 10% d'adresses de secours et on rentre un secret partagé :



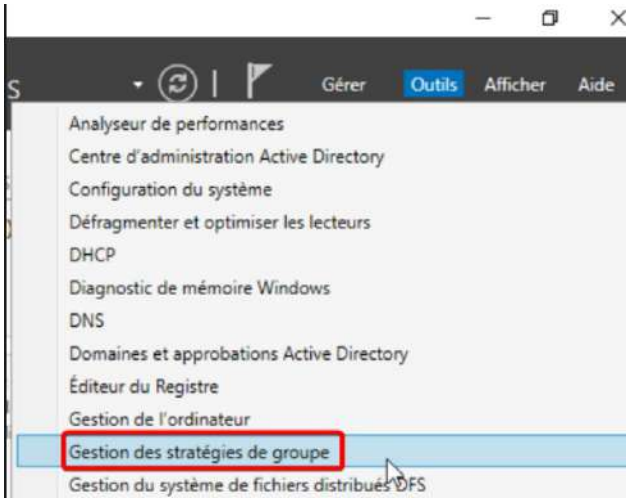
Pour finir, on peut cliquer sur Terminer.

Le basculement est maintenant opérationnel.

4.3) GPO

Les GPO sont pratiquement tout le temps utilisées pour personnaliser les expériences utilisateurs, mais aussi, contrôler et bloquer certains droits pour le bon fonctionnement et la sécurité d'un domaine.

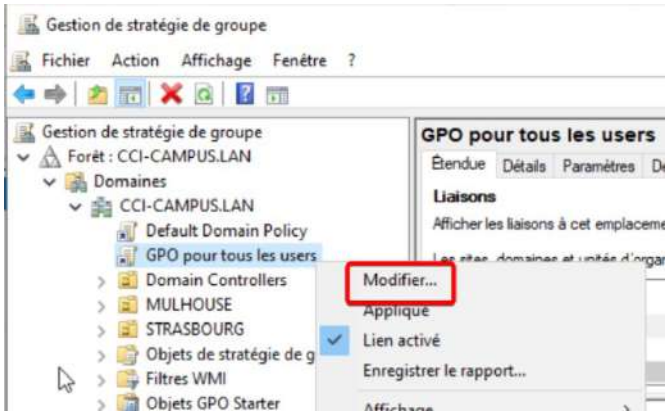
L'entièreté des configurations de ce chapitre se feront dans la console de "Gestion de stratégie de groupe", accessible depuis le gestionnaire de serveur :



Pour éviter de détailler la modification d'une GPO dans tous les chapitres ci-dessous, voici la démarche à suivre :

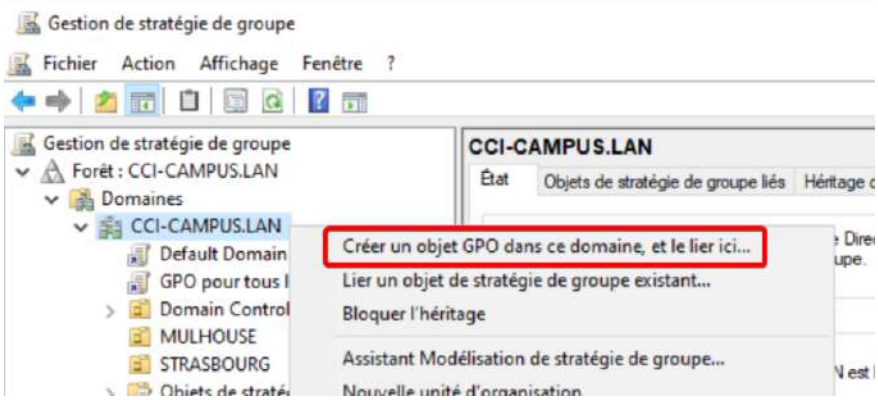
Pour éditer une GPO

Depuis la console de "Gestion des stratégies de groupe", il suffit de faire clic droit sur la GPO à éditer et cliquer sur modifier :



Pour créer une GPO

Toujours depuis la même console, il suffit de faire un clique droit sur le domaine ou l'UO et cliquer sur "Créer un objet GPO dans ce domaine, et le lier ici..." :



Appliquer les changements après modification

Après avoir édité une GPO, il faut lancer la commande suivante pour les mettre à jour sur le poste client :

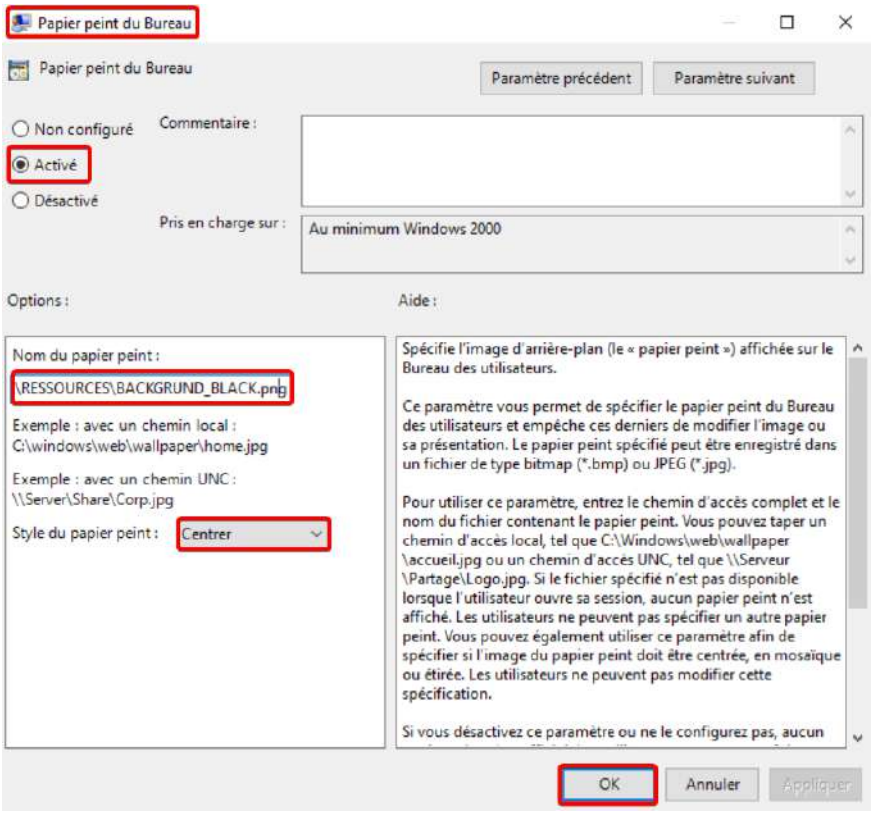
```
# gpupdate /force
```

4.3.1) Déployer un fond d'écran et bloquer son changement

Pour déployer un fond d'écran par GPO, il faut activer le paramètre suivant :

Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > Bureau > Papier peint du Bureau

Puis, il faut renseigner le chemin (UNC de préférence) vers l'image qui servira de fond d'écran :

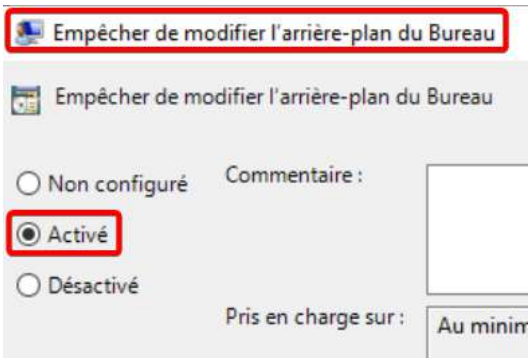


⚠ Attention

Chaque utilisateur qui sera affecté par cette GPO devra avoir au minimum des droits de lecture sur le fichier image. Autrement, le fond d'écran ne s'affichera pas.

Ensuite, pour bloquer le changement de ce fond d'écran, il faut activer le paramètre suivant :

Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Personnalisation > Empêcher de modifier l'arrière-plan du Bureau

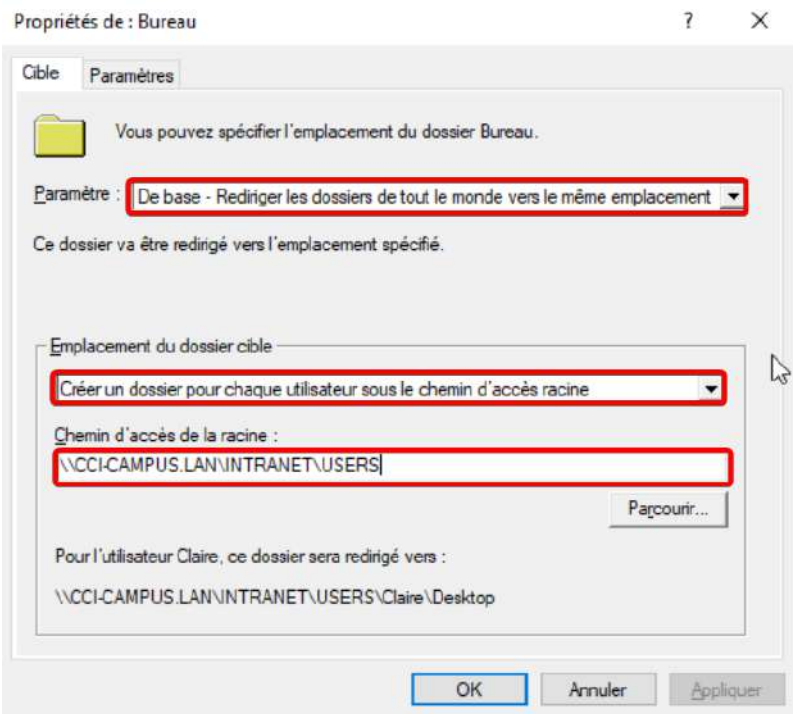


4.3.2) Redirection de dossiers

Pour rediriger des dossiers utilisateurs (par exemple Bureau, Documents) vers un dossier partagé, il faut faire clique droit puis propriétés sur le dossier à rediriger :

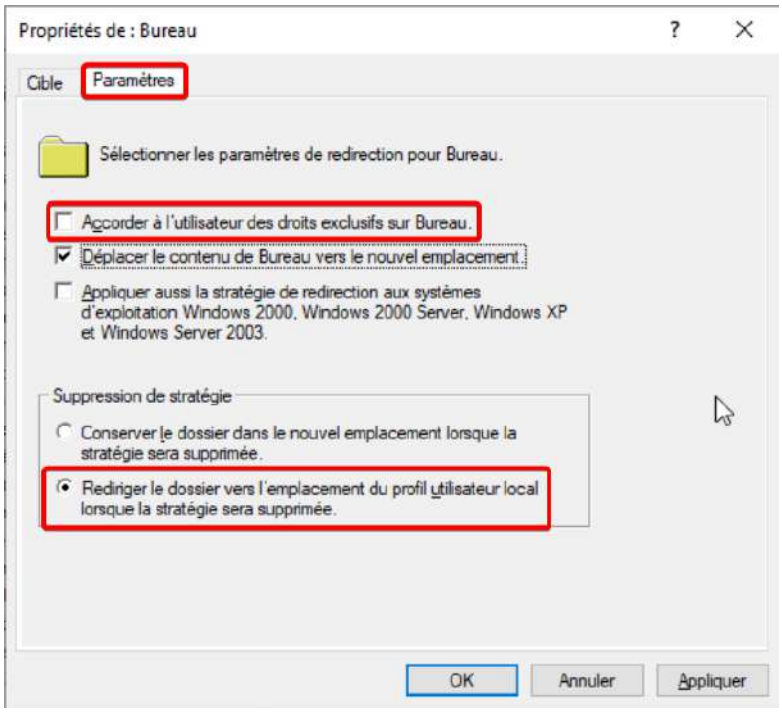
Configuration utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers > Dossier_à_rediriger

Puis on active la redirection de base, si on souhaite créer un dossier par utilisateur il faut sélectionner l'option adéquate, et enfin, le chemin d'accès réseau ou sera redirigé le dossier :



> ⚠ **Attention**
>
> Les utilisateurs affectés par la GPO doivent avoir la permission de créer un dossier dans le répertoire cible, sinon cette partie de la GPO ne s'appliquera pas

Puis dans l'onglet paramètre, on décoche "Accorder à l'utilisateur des droits exclusifs" et on peut cliquer sur appliquer :

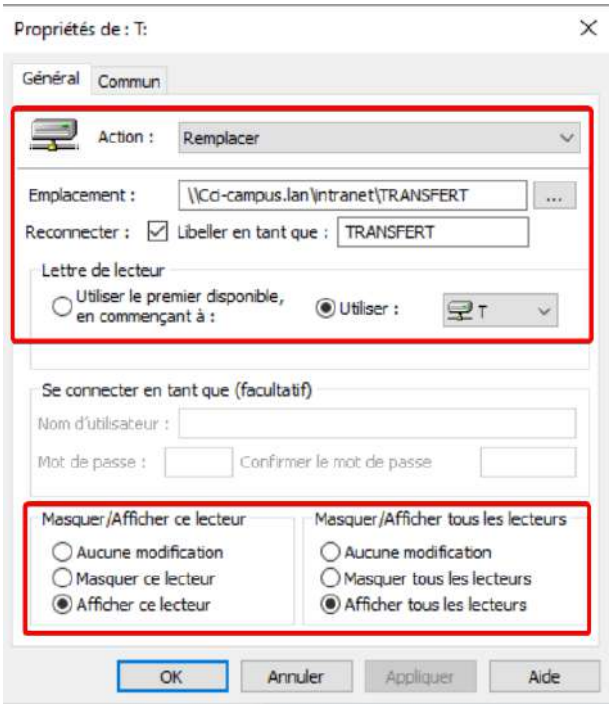


4.3.3) Mappage de lecteurs réseau

Pour mapper un lecteur réseau, il faut faire clique droit, nouveau, lecteur mappé dans l'onglet de droite du paramètre suivant :

Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs

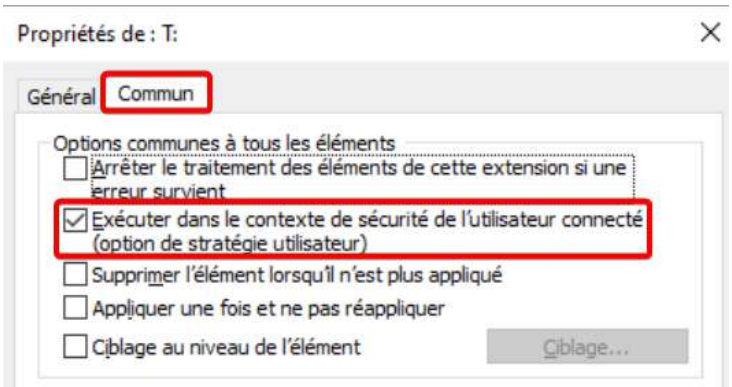
On configure ensuite le lecteur en "Action : Remplacer", puis on coche "Reconnecter" et on spécifie l'emplacement cible, un libeller et une lettre de lecteur. Enfin, on coche "Afficher ce lecteur" et "Afficher tous les lecteurs" :



Info

Pour spécifier un chemin unique à chaque utilisateur on peut utiliser la variable %LogonUser% dans le champs de l'emplacement cible

Dans l'onglet "Commun", il est nécessaire de cocher la case "Exécuter dans le contexte de sécurité de l'utilisateur connecté" :

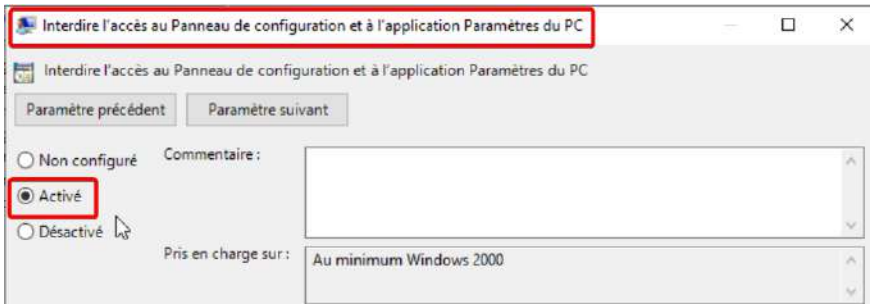


On applique et le lecteur est maintenant mappé.

4.3.4) Interdire l'accès au panneau de configuration

Pour interdire l'accès au panneau de configuration, il faut activer le paramètre suivant :

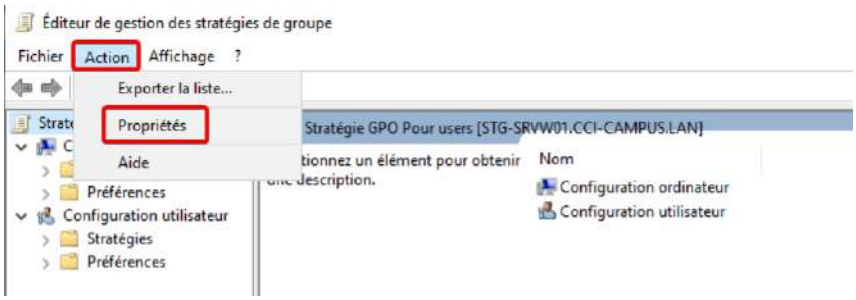
Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC



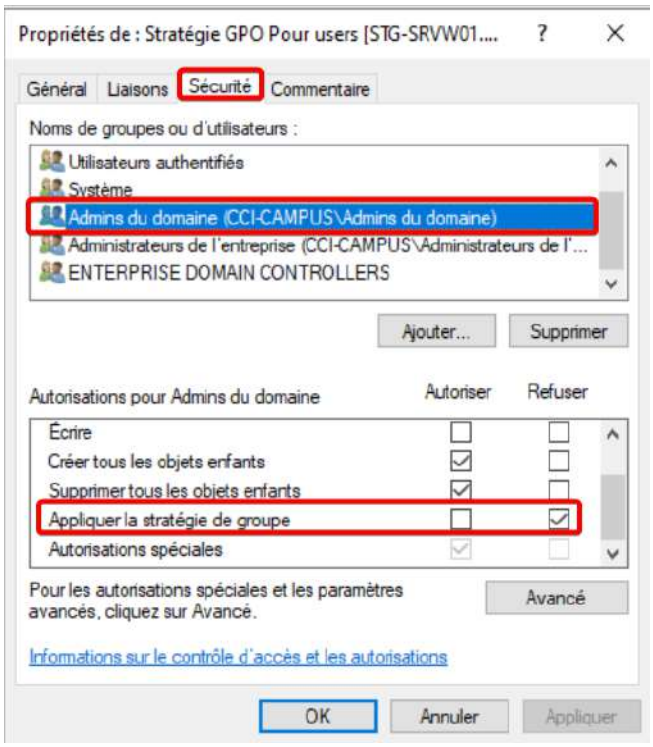
4.3.5) Empêcher l'exécution d'une GPO pour un groupe

Il peut être utile d'empêcher un groupe d'utilisateur compris dans le filtrage de sécurité d'exécuter une GPO, cela peut être pratique pour par exemple exécuter une GPO pour tous les utilisateurs du domaine sauf les admins du domaine.

Pour se faire, il faut aller dans "Action", puis "Propriétés" :



Ensuite, il faut aller dans l'onglet "Sécurité", sélectionner le groupe à exclure et cocher la case "Refuser" en face du champs "Appliquer la stratégie de groupe" :



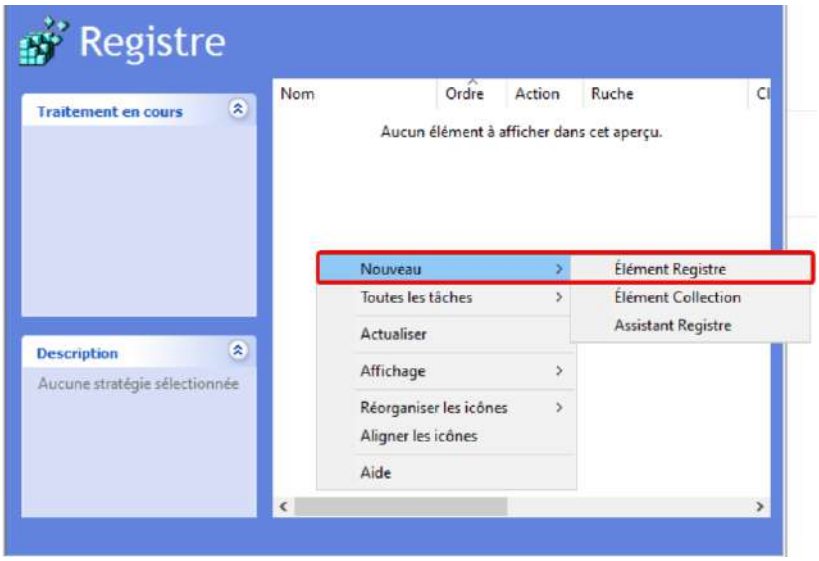
Puis cliquer sur OK.

4.3.6) Bloquer les ports USB par clé de registre

On peut bloquer les ports USB avec une clé de registre. Pour ajouter/modifier une clé de registre, il faut aller au paramètre suivant :

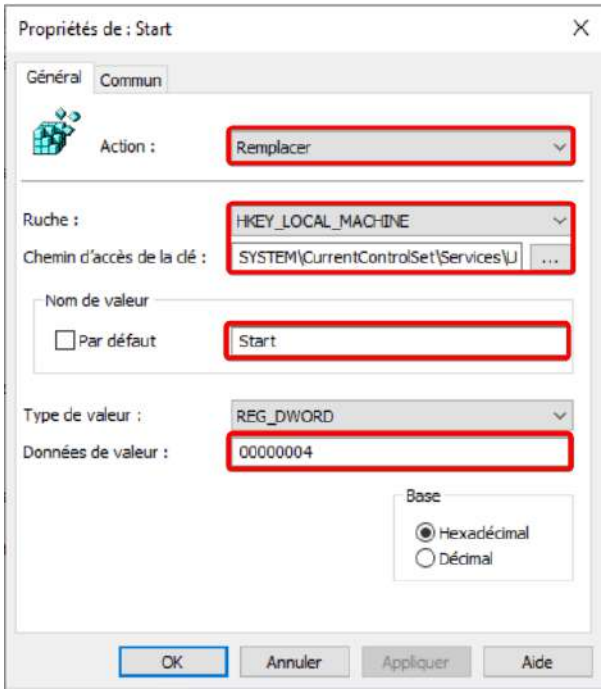
Configuration ordinateur > Préférences > Paramètres Windows > Registre

Puis faire un clic droit dans le panneau de droite, Nouveau, Elément Registre :



Puis mettre en Action "Remplacer", chercher la clé de registre ci-dessous et passer la valeur à 4 :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR\Start



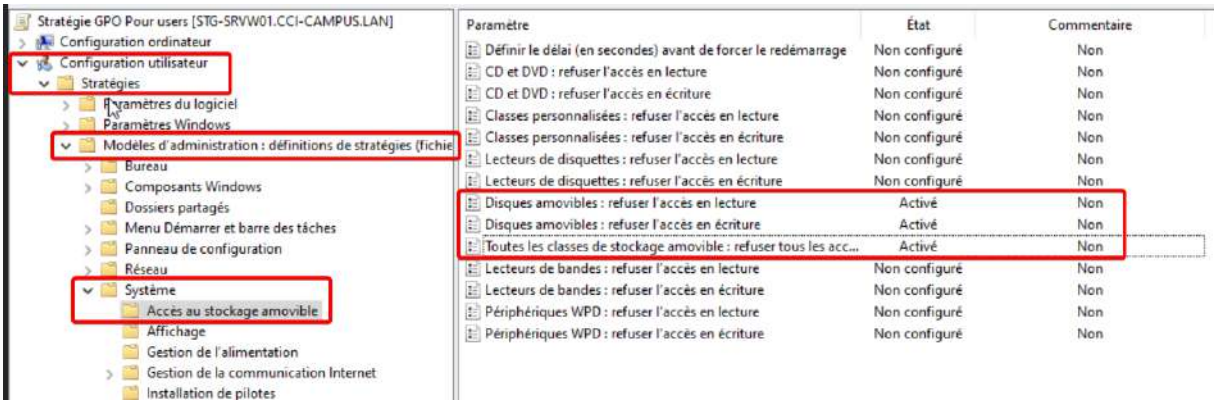
Vous pouvez ensuite cliquer sur OK

4.3.7) Bloquer les ports USB

Pour bloquer les ports USB sans utiliser de clé de registre au niveau de la configuration utilisateur, il faut activer les paramètres suivants :

Configuration utilisateur > Stratégies > Modèles d'administration > Système > Accès au stockage amovible

- Disques amovibles : refuser l'accès en lecture
- Disques amovibles : refuser l'accès en écriture
- Toutes les classes de stockage amovible : refuser tous les accès

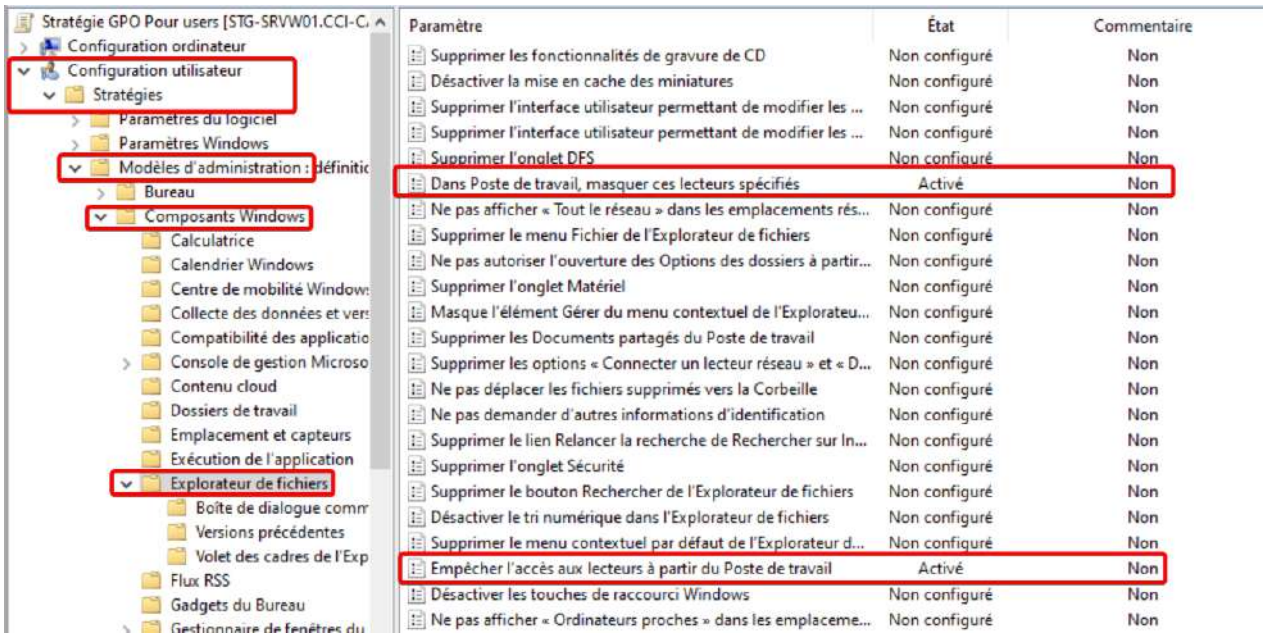


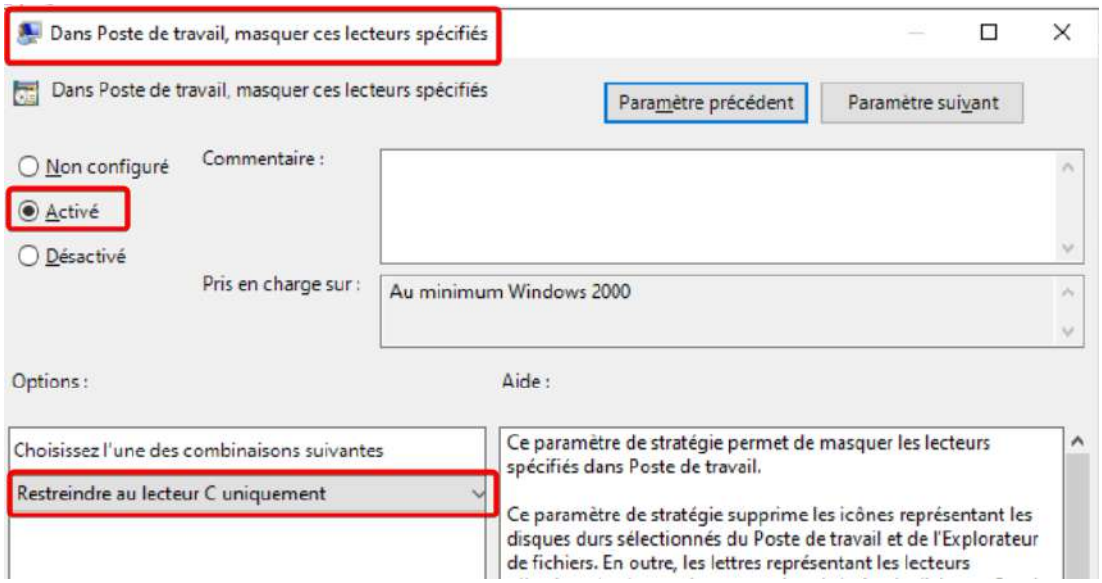
4.3.8) Masquer et empêcher l'accès au lecteur C

Pour masquer et empêcher l'accès à un lecteur, comme le lecteur C, il faut activer les deux paramètres suivants :

Configuration utilisateur > Stratégies > Modèles d'administration > Composants Windows > Explorateur de fichiers

- Dans Poste de travail, masquer ces lecteurs spécifiés
  - Restreindre au lecteur C uniquement
- Empêcher l'acccès aux lecteurs à partir du Poste de travail
  - Restreindre au lecteur C uniquement





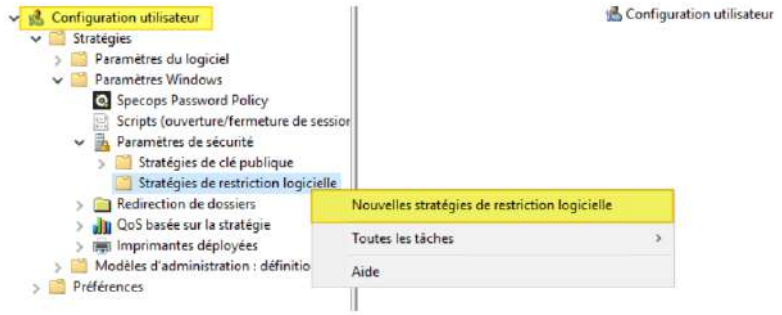
Maintenant, les utilisateurs n'auront plus accès au lecteur C.

4.3.9) Bloquer l'accès aux consoles Powershell et Invite de commande

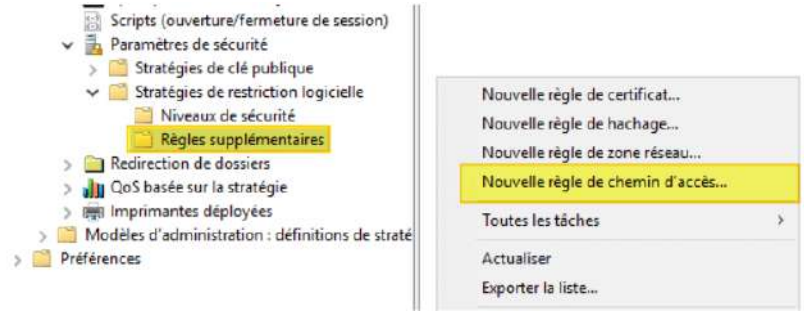
Pour bloquer l'accès aux consoles Powershell, il faut tout d'abord faire un clique droit sur le paramètre suivant :

> Configuration utilisateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de restriction logiciel

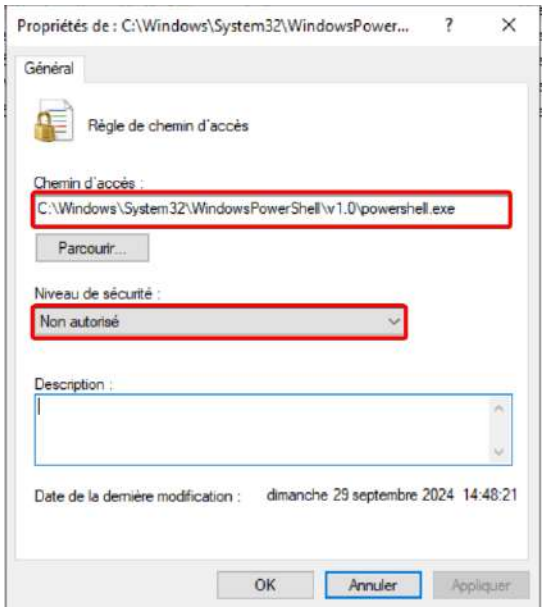
Puis cliquer sur "Nouvelles stratégies de restriction logicielle" :



Nous allons ensuite créer des règles de chemin d'accès, faites donc un clique droit sur "Règles supplémentaires", puis sélectionner "Nouvelle règle de chemin d'accès..." :



Il faut maintenant renseigner le chemin d'accès à PowerShell et mettre le "Niveau de sécurité" en "Non autorisé" :



Enfin, il faudra répéter l'opération pour les différentes versions de Powershell :

```
# PowerShell 7 - 64 bits
C:\Program Files\PowerShell\7\pwsh.exe
# Windows PowerShell - 64 bits
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
# Windows PowerShell - 32 bits
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
# Windows PowerShell ISE - 64 bits
C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
# Windows PowerShell ISE - 32 bits
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe
```

Pour la partie PowerShell, la configuration est terminé.

Pour bloquer l'accès à l'invite de commande, il faut simplement activer le paramètre suivant :

Configuration utilisateur > Stratégies > Modèles d'administration > Système > Désactiver l'accès à l'invite de commandes

La configuration est maintenant opérationnelle.

5) Mise en place DFSR & Déduplication des données

5.1) Prérequis

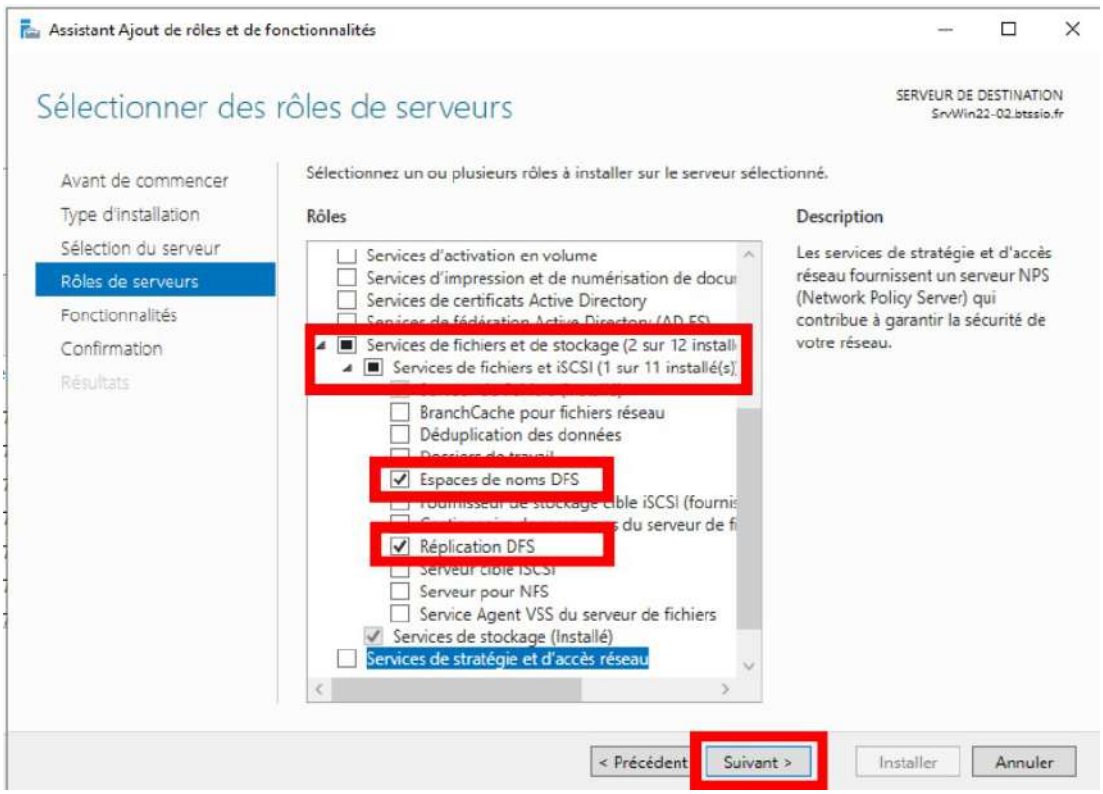
- Il sera nécessaire d'avoir mis en place l'AD DS et si besoin le DHCP.
- Il sera aussi nécessaire d'avoir un deuxième disque qui contiendra les données, par soucis de sécurité et pour éviter que le disque OS ne soit mêlé au disque de données

5.2) DFS

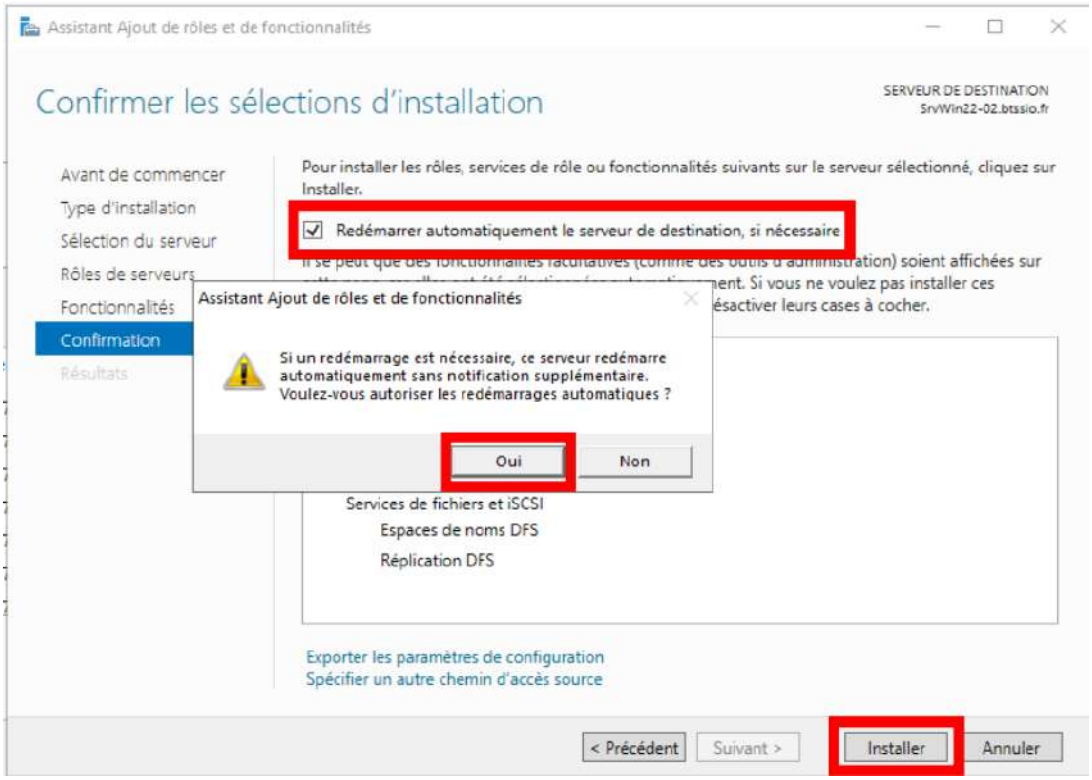
5.2.1) Création et configuration de l'espace de noms

On commence par ajouter le rôle DFS et DFSR depuis le gestionnaire de serveur :

On choisit son serveur cible, puis on sélectionne les rôles "Espaces de noms DFS" et "Réplication DFS" :

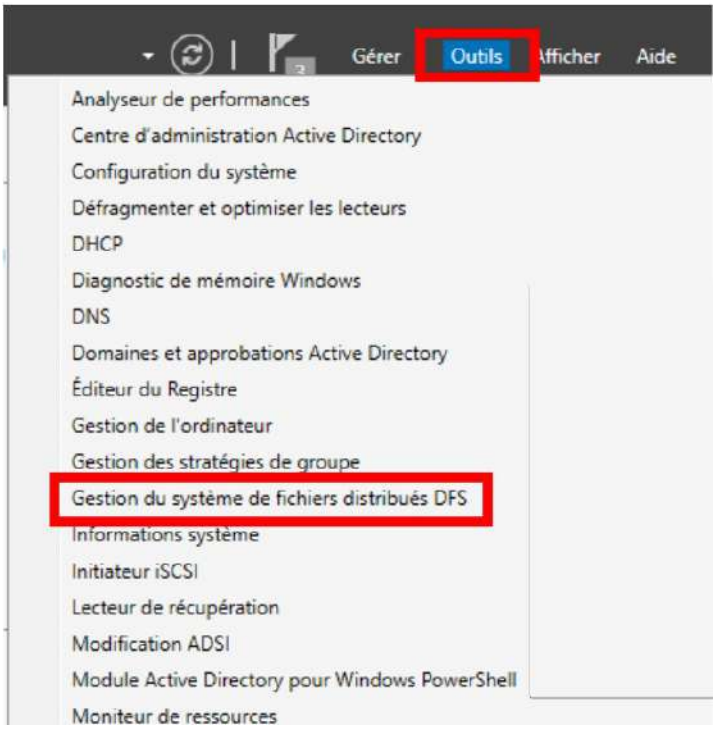


Puis on peut aller jusqu'à la page de Confirmation, on coche « Redémarrer automatiquement le serveur de destination, si nécessaire » et on répond « Oui » à la fenêtre pop-up puis Installer :

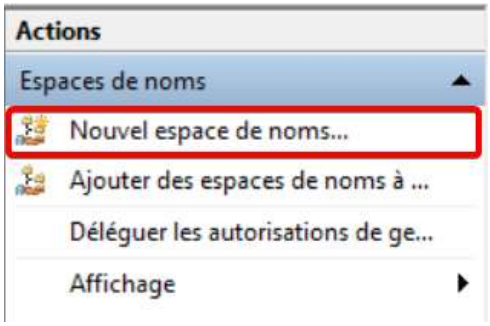


Il faut faire les mêmes opérations sur les autres serveurs que l'on souhaite utilisé pour le DFS

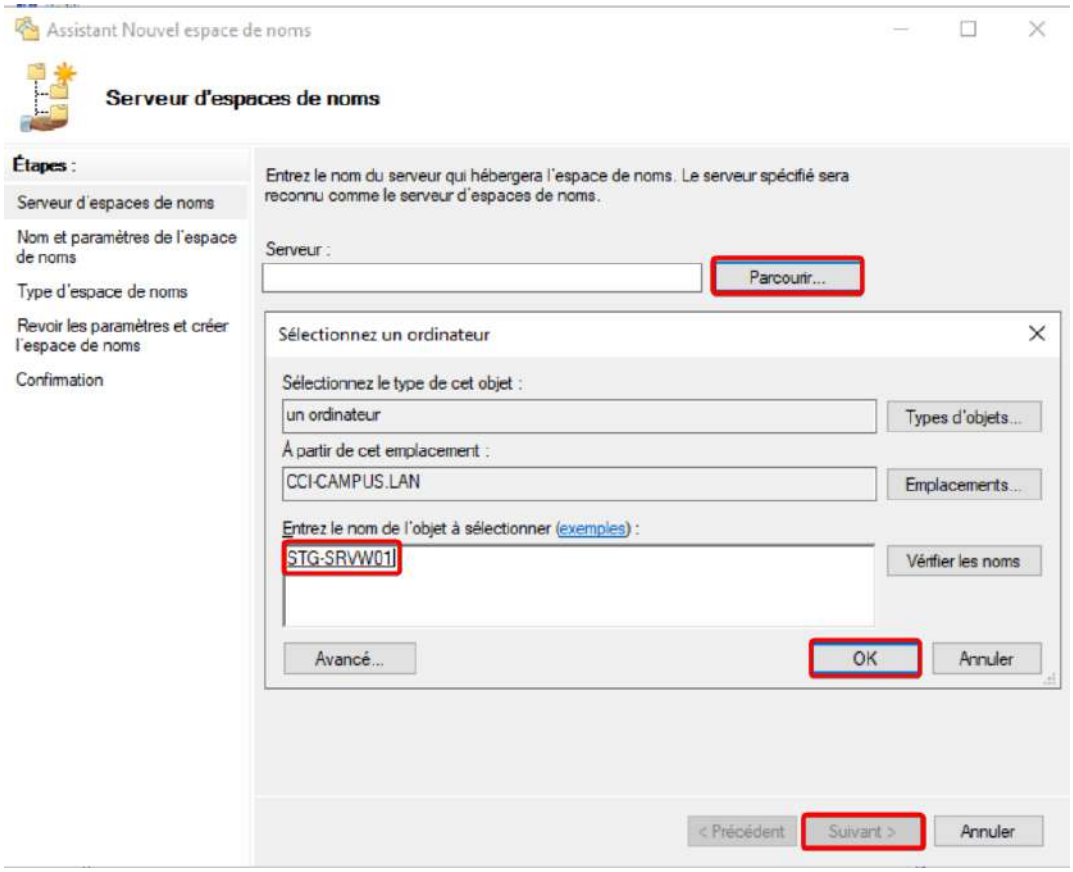
Ensuite, on peut aller dans "Outils" puis "Gestion du système de fichiers distribués DFS":



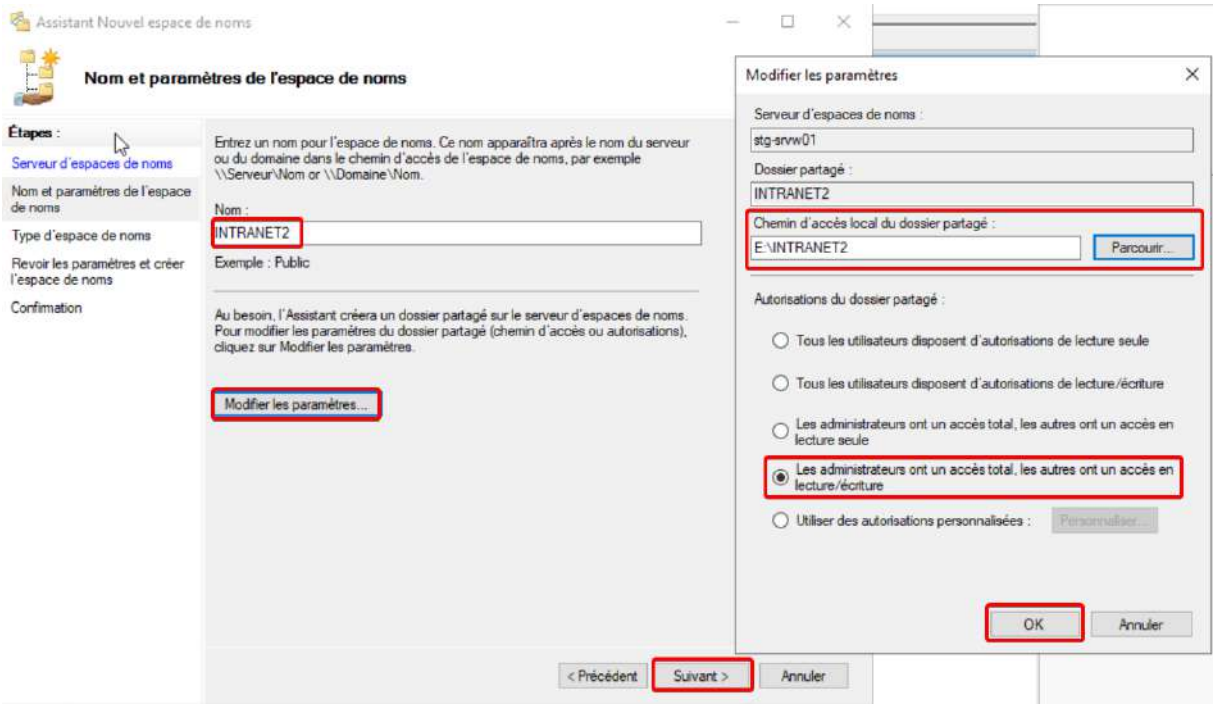
Puis dans le panneau de droite on clique sur "Nouvel espace de noms..."



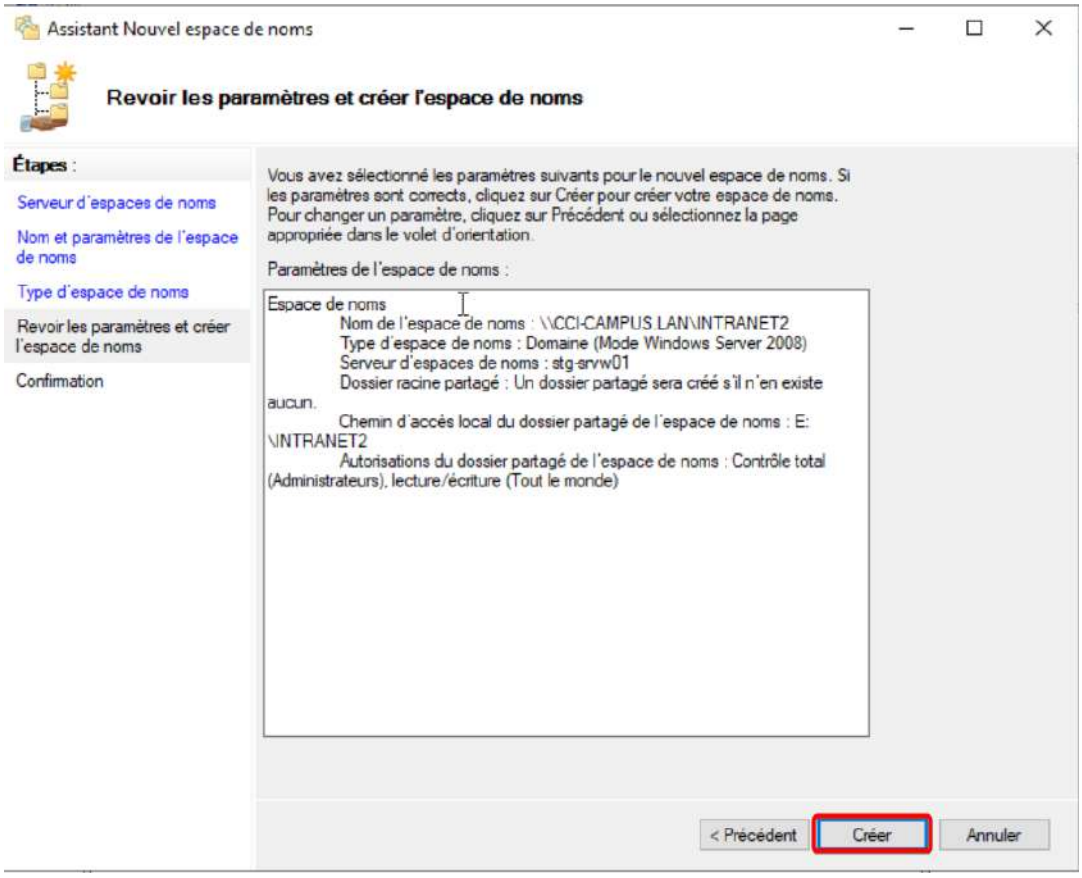
Puis on sélectionne notre serveur principal et on fait suivant :



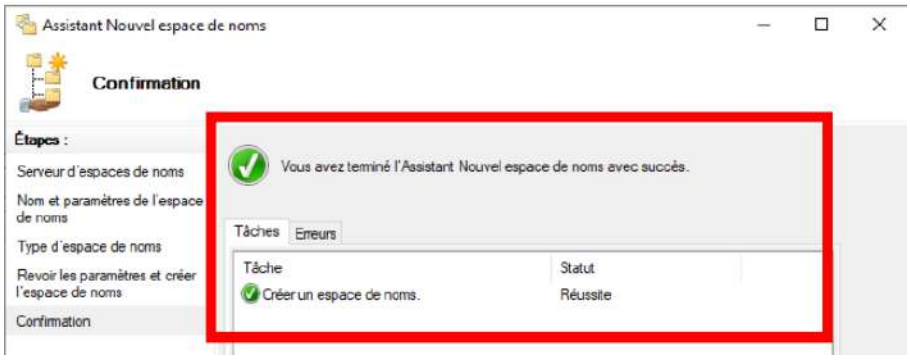
On entre ensuite le nom de l'espace de noms, puis "Modifier les paramètres", on choisit un dossier local pour le partage (créer un dossier sur le deuxième disque) et on change les permissions :



On peut ensuite cliquer sur Suivant et Créer :

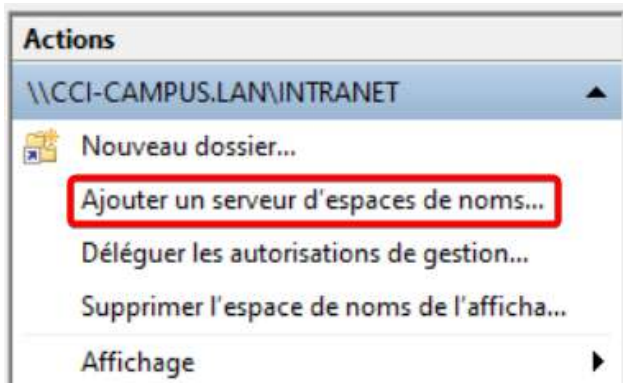


Si tout c'est bien passé vous aurez un message de validation :

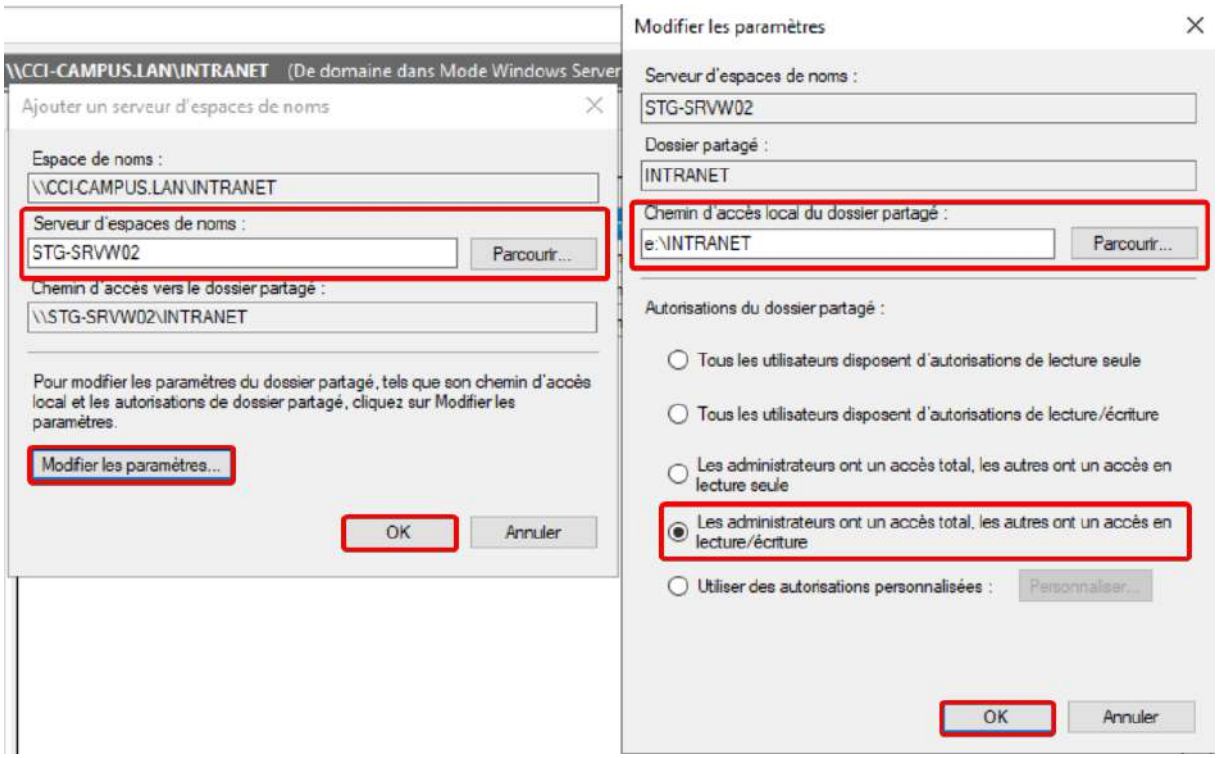


Nous allons maintenant ajouter un deuxième serveur d'espace de noms, cliquer sur votre Espace de noms que vous venez de créer, puis sur "Serveurs d'espaces de noms" :

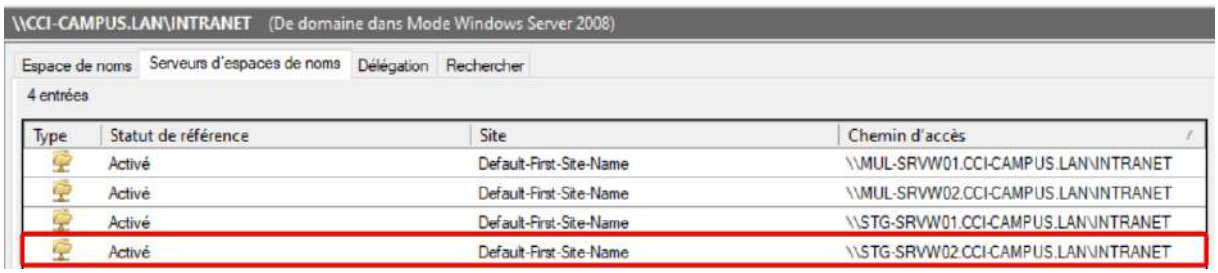
Dans le panneau de droite, il faut cliquer sur "Ajouter un serveur d'espaces de noms..." :



On sélectionne ensuite notre serveur, puis on clique sur "Modifier les paramètres", on sélectionne un chemin d'accès local (créer un dossier sur le deuxième disque) et on modifie les autorisations :

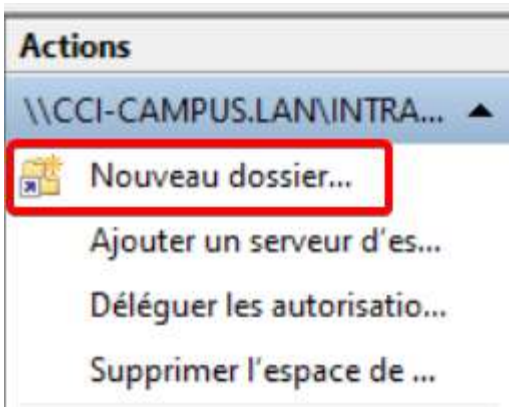


Après avoir cliquer sur OK, on peut voir que notre serveur à été ajouté :

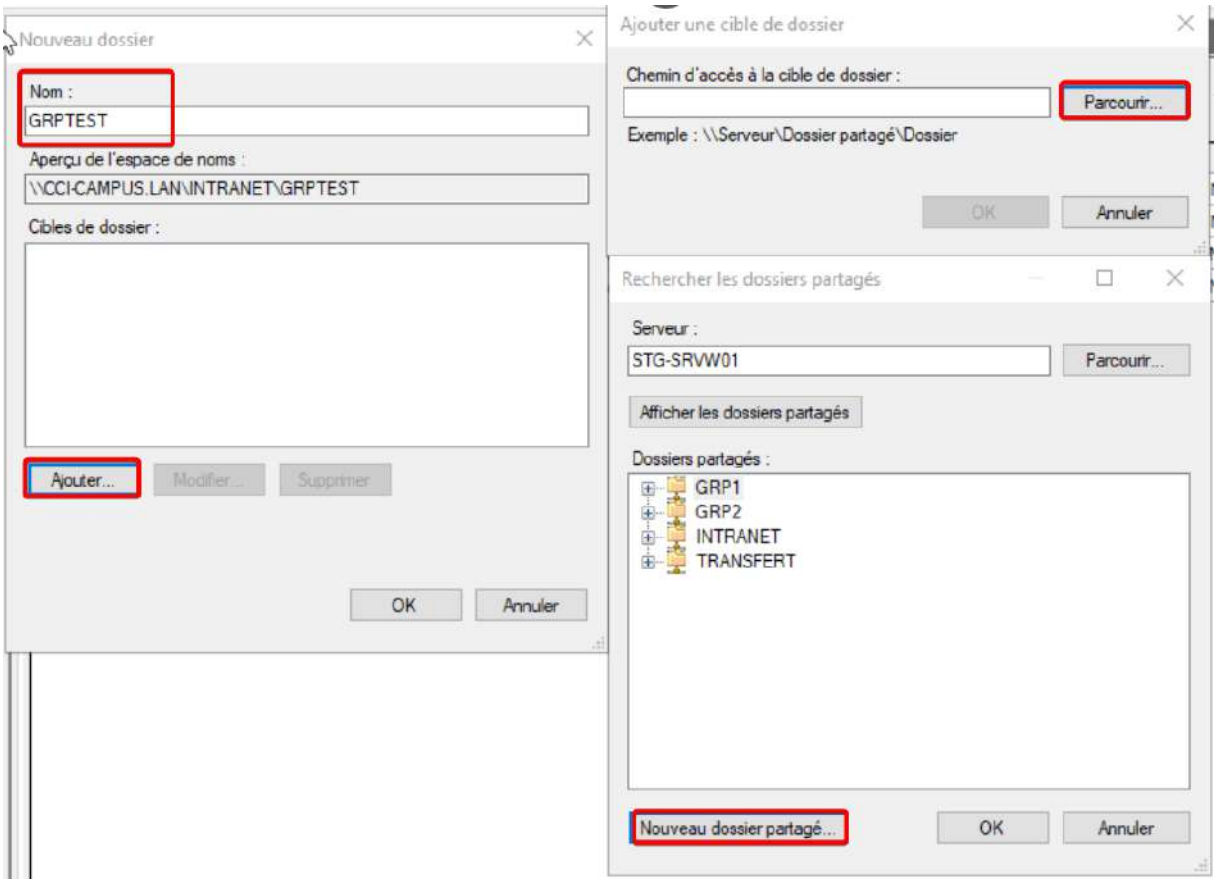


5.2.2) Création d'un dossier cible

Dans le panneau de droite, cliquer sur "Nouveau dossier..." :



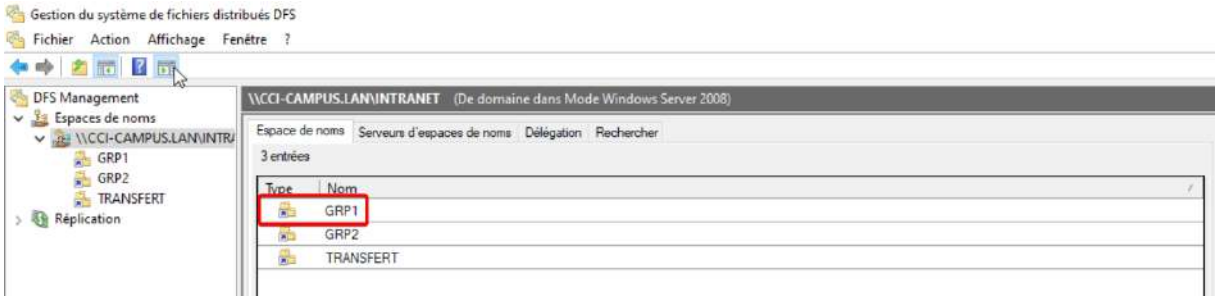
On rentre ensuite un Nom, on clique sur "Ajouter", puis "Parcourir" et enfin "Nouveau dossier partagé..." :



Ensuite on sélectionne un chemin local vers un nouveau dossier sur le deuxième disque, on met nos autorisations (ici personnalisées) et on clique sur OK :

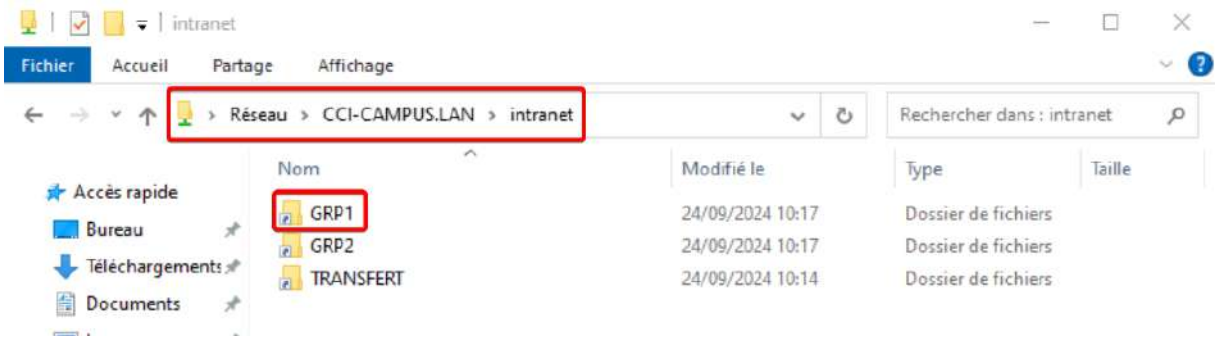
Enfin, on peut sélectionner le dossier partagé que l'on vient de créer et cliquer sur OK.

Si tout est bon, le dossier devrait apparaître dans l'espace de noms :

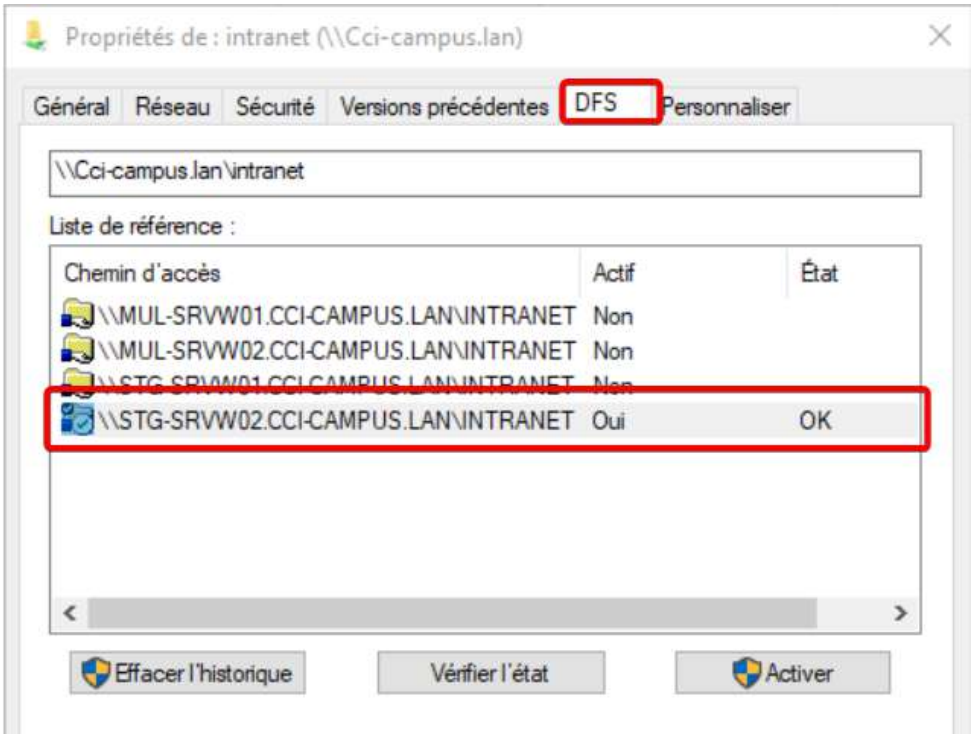


5.2.3) Vérification DFS

On peut aussi vérifier avec un explorateur de fichier depuis un autre appareil dans le domaine : \\CCI-CAMPUS.LAN\intranet\



On peut aussi vérifier depuis les propriétés du dossier, dans l'onglet DFS :



DFS est maintenant mis en place et fonctionnel.

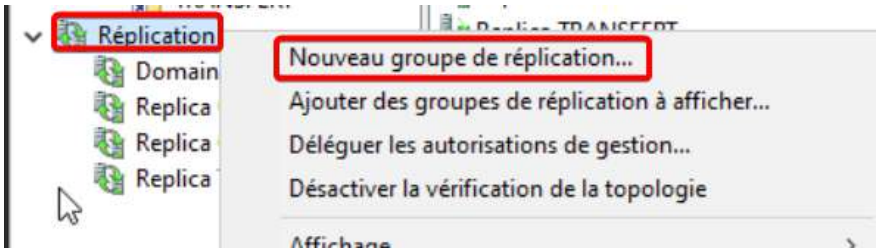
5.3) DFSR

Le problème avec DFS est que le fichier est présent physiquement que sur un seul serveur. C'est donc la que rentre en compte la réplication avec DSFR.

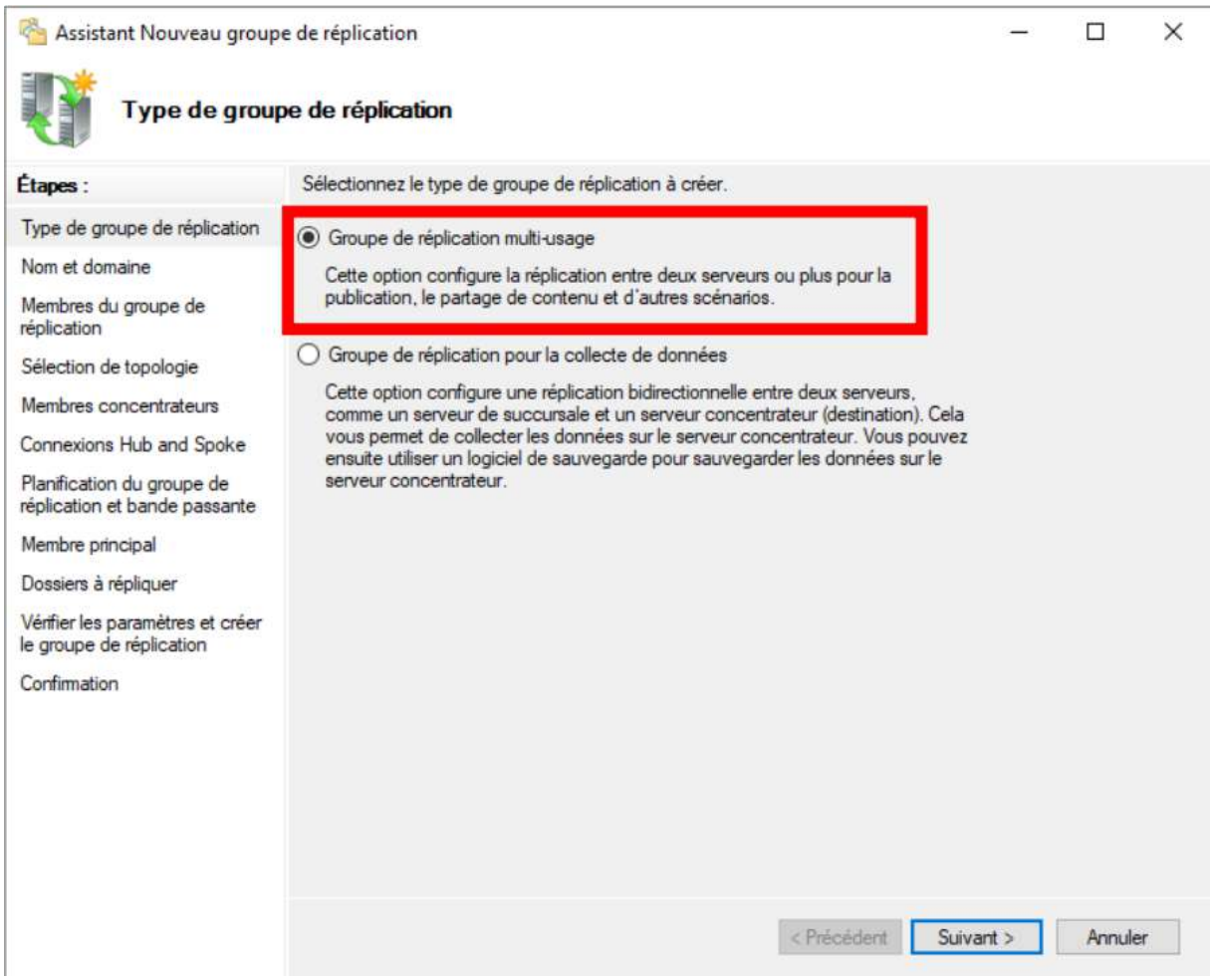
Nous avons déjà installé le rôle de Réplication des données dans le chapitre sur DFS, DFSR est donc déjà installé.

5.3.1) Configuration du DFSR

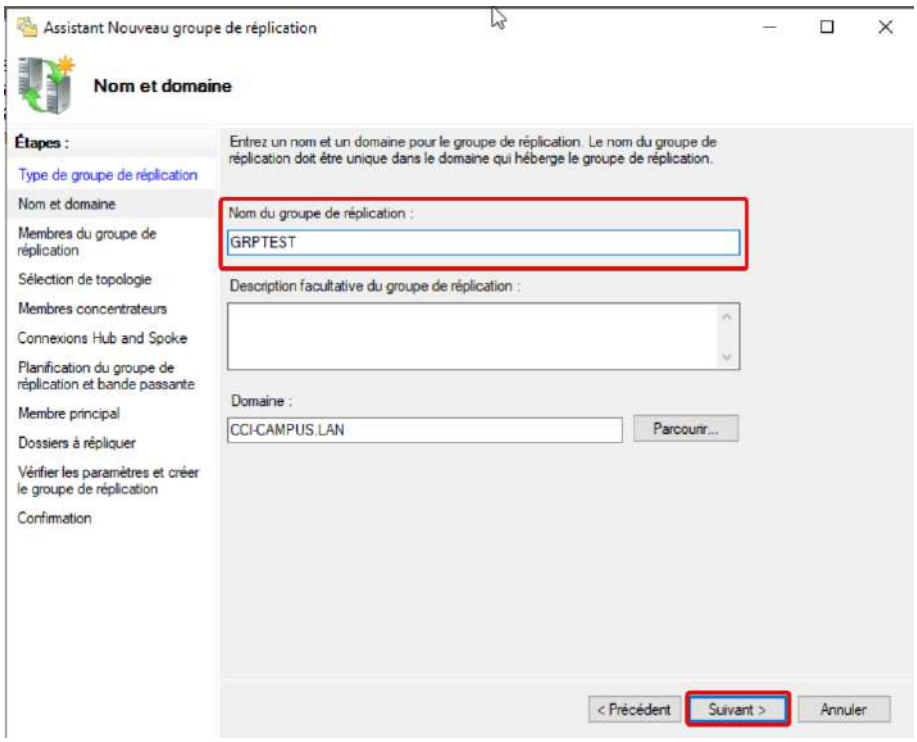
Pour le configurer, il suffit de cliquer sur "Réplication" (dans Gestion du système de fichiers distribués DFS), ensuite faire un clique droit sur "Réplication" et cliquer sur "Nouveau groupe de réplication..." :



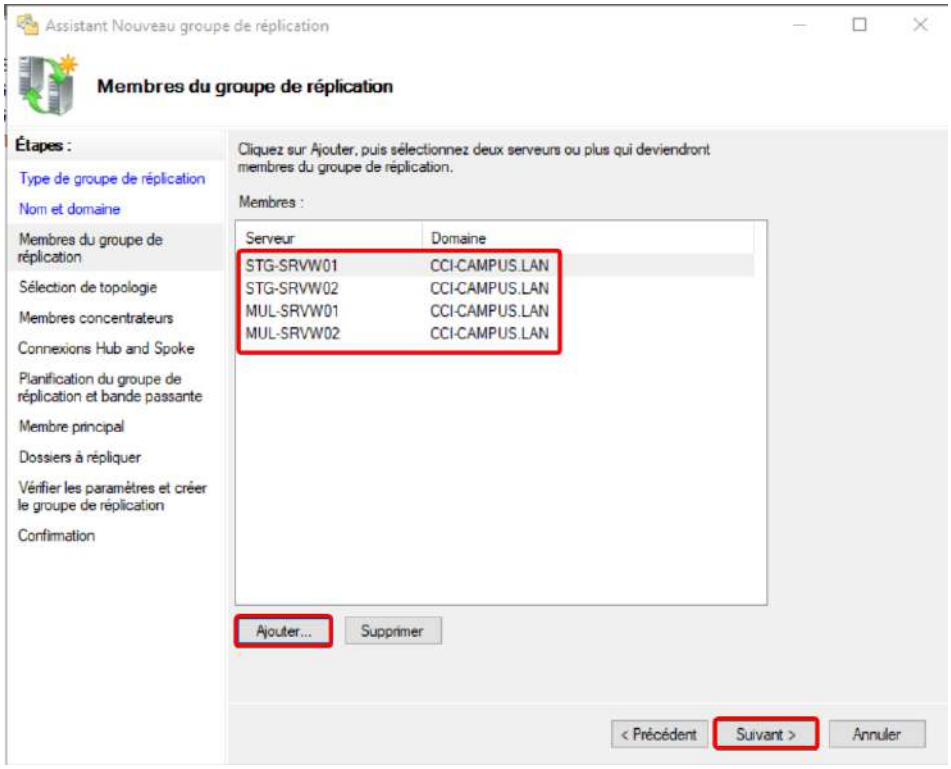
On laisse par défaut :



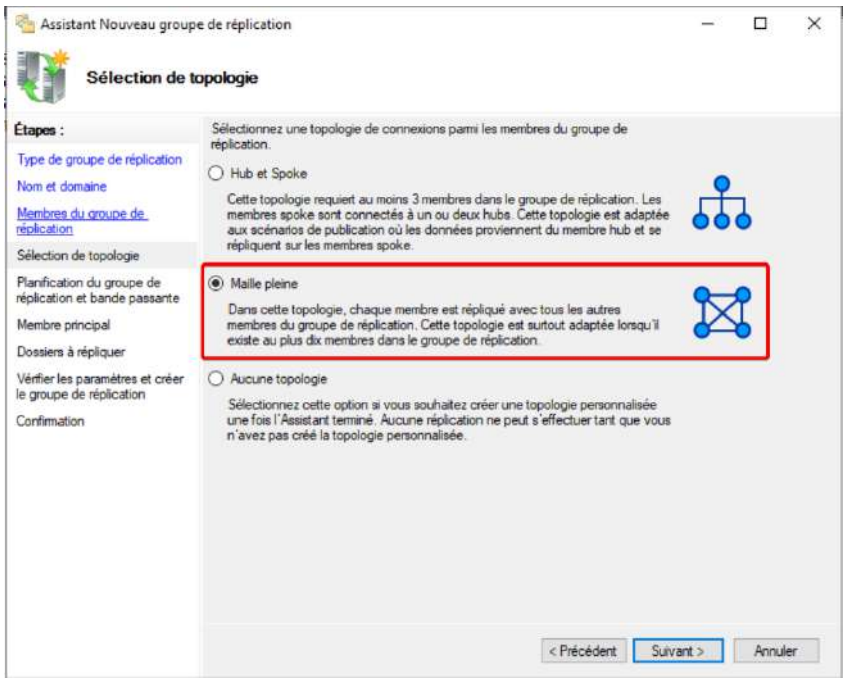
On choisit ensuite un nom :



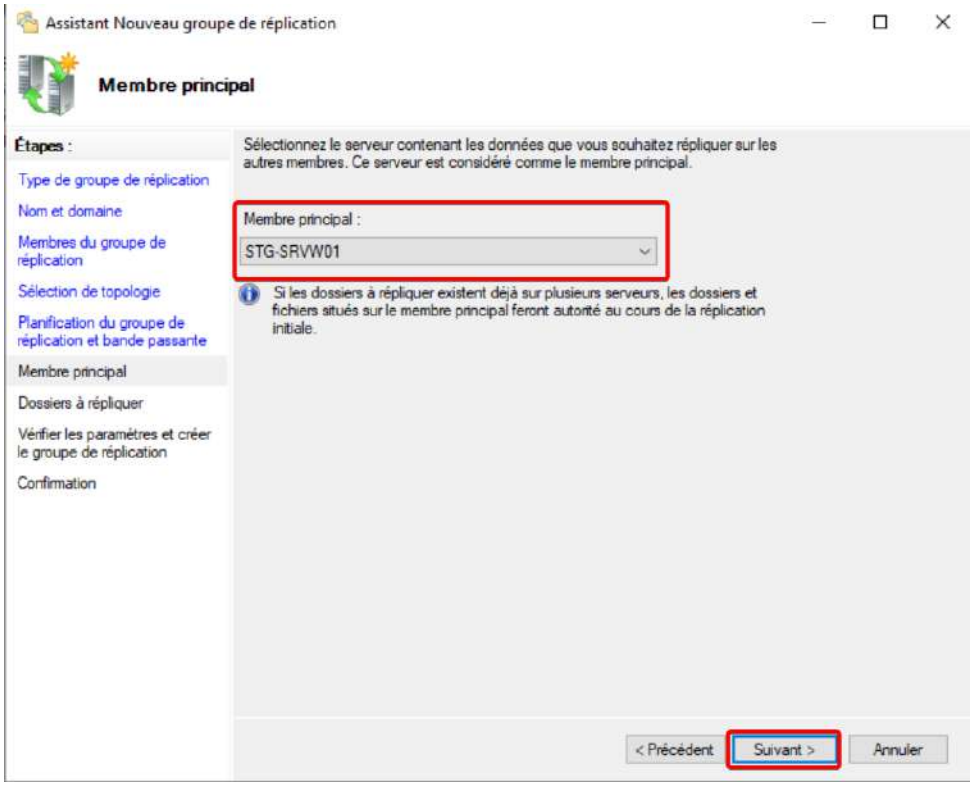
On ajoute ensuite tous nos serveurs qui devront répliquer les données :



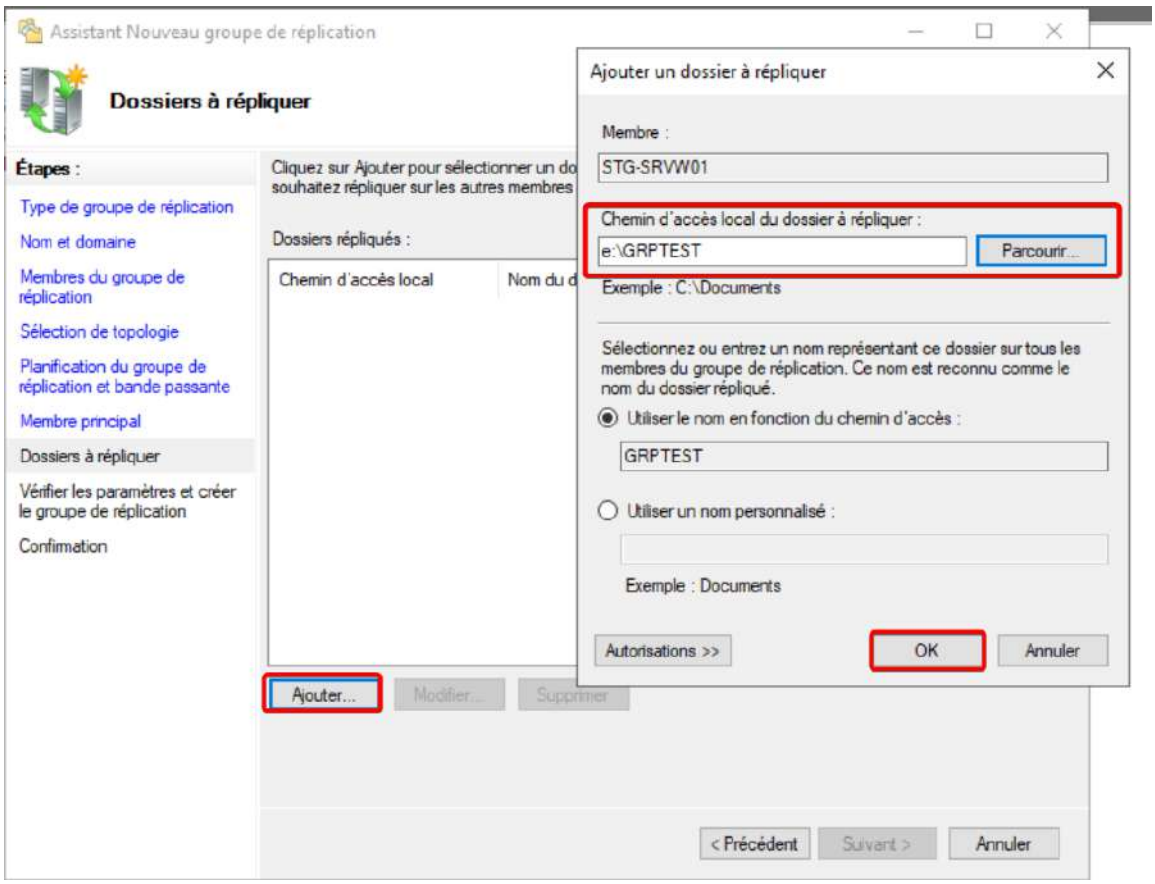
On sélectionne ici "Maille pleine", puis on clique 2 fois sur suivant :



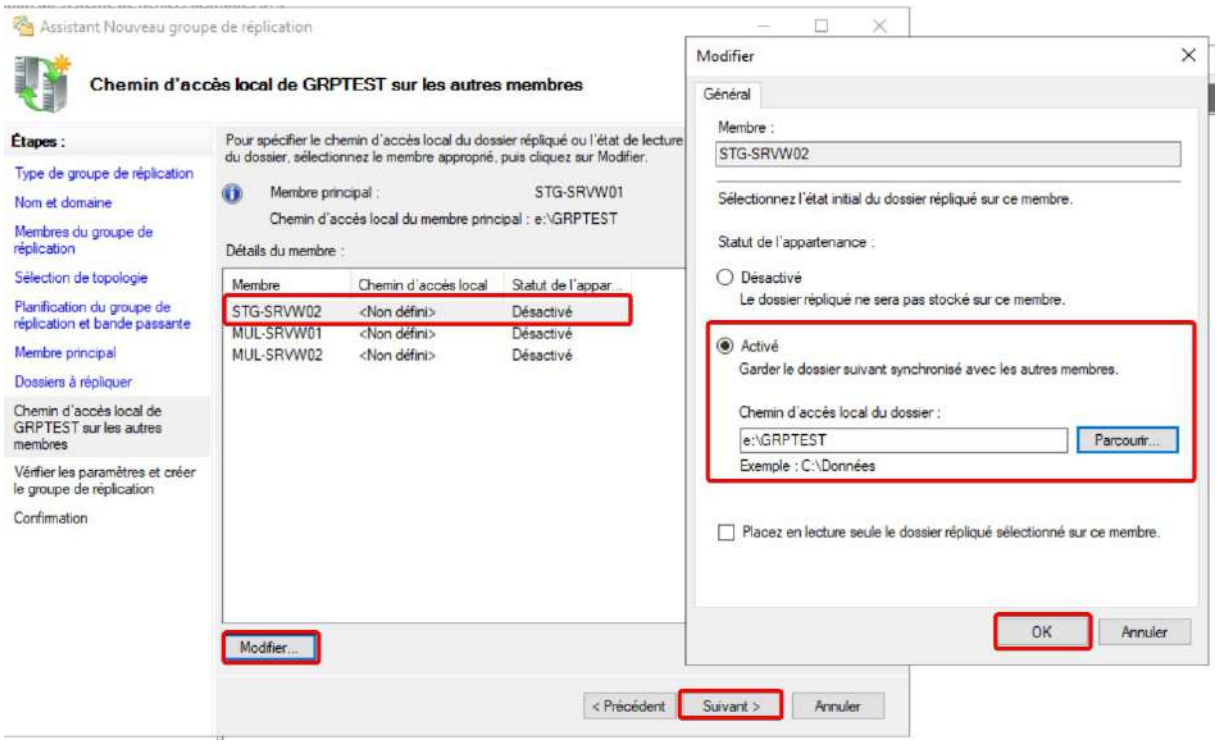
On choisit ensuite le "membre principal" c'est à dire le serveur qui détient localement la donnée à répliquer :



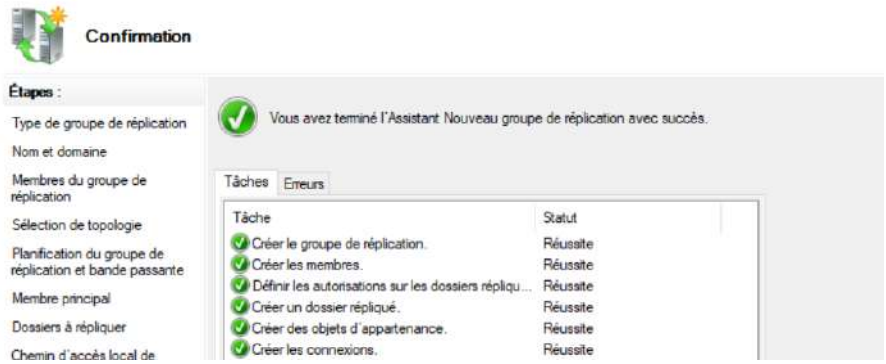
On sélectionne ensuite le chemin vers le dossier local :



On sélectionne ensuite le chaque serveur, on clique sur "Modifier", on Active la réplication on lui attribue un chemin local qui permettra de stocker le contenu du dossier à répliquer :

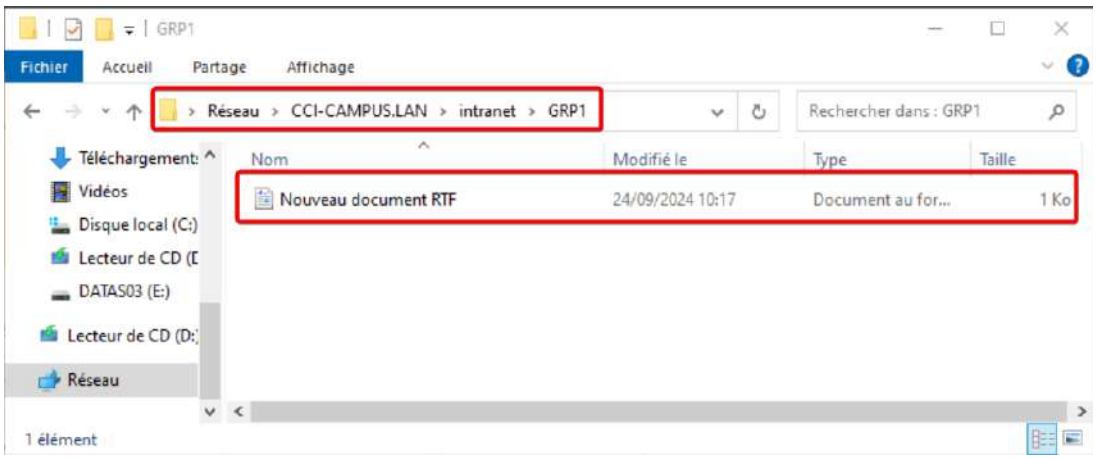


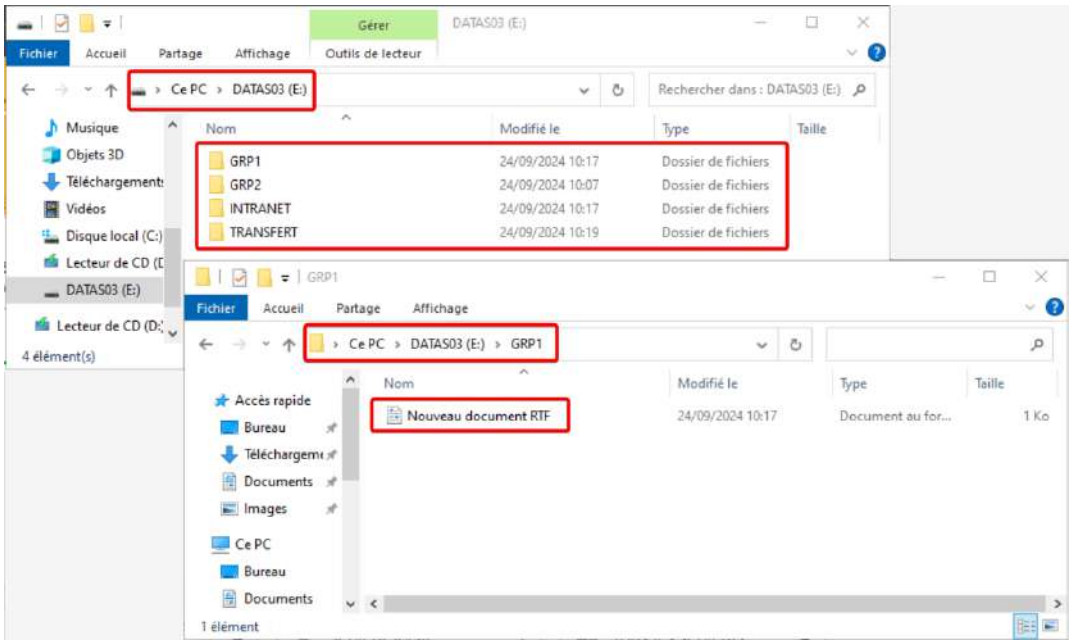
On peut ensuite cliquer sur suivant et créer. Si tout se passe correctement, nous devrions avoir un message de validation :



5.3.2) Vérifications DFSR

On peut vérifier maintenant que la réplication est bien effectuée **LOCALEMENT** sur les différents serveurs :





DFSR est maintenant en place et opérationnel !

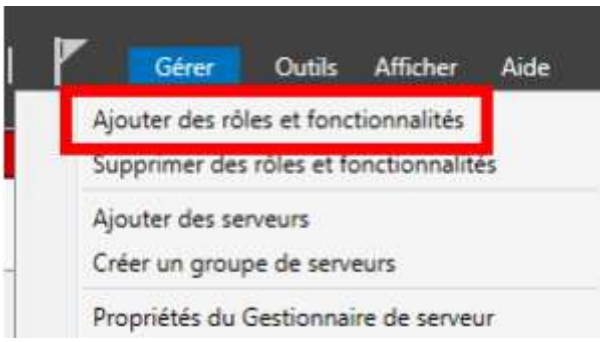
5.4) Déduplication des données

La déduplication peut nous permettre d'économiser un grand espace sur notre infrastructure, elle permet de supprimer les copies inutiles ou redondantes.

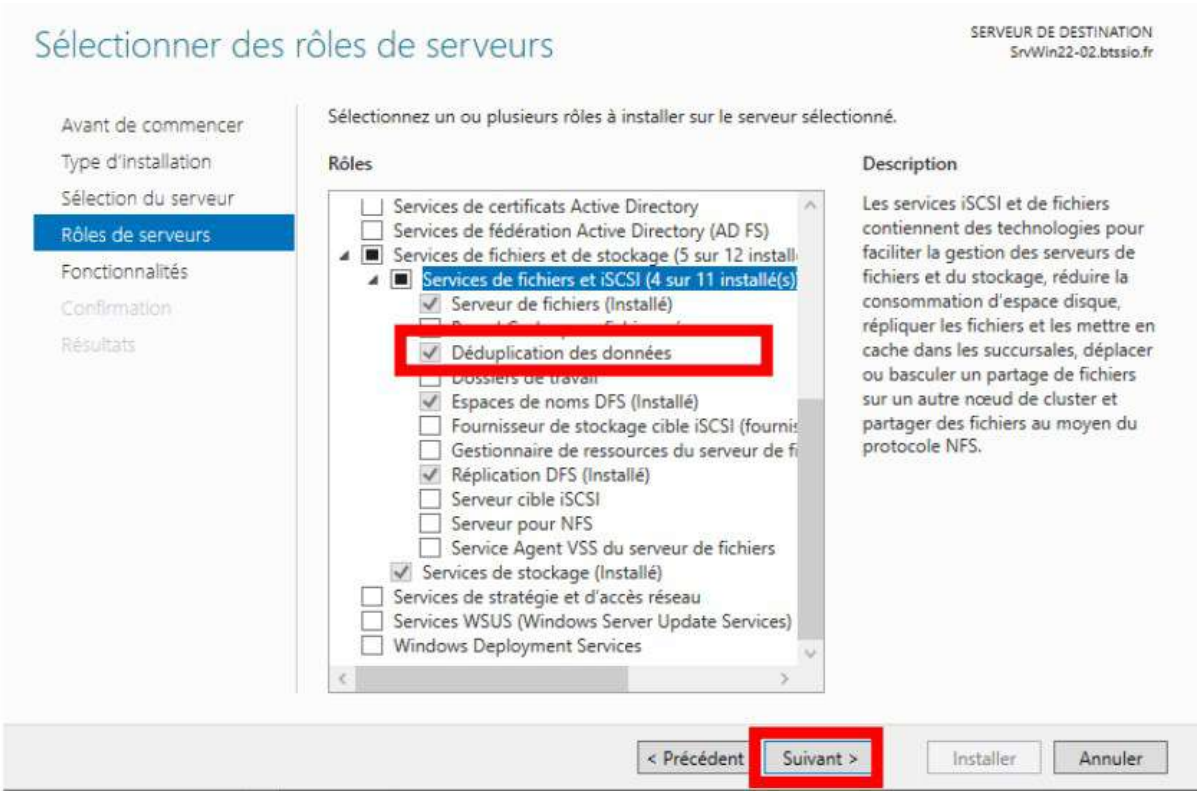
Selon Microsoft, le service de déduplication permettrait d' « obtenir des taux d'optimisation allant jusqu'à 95 % ou une utilisation du stockage divisée par 20 »

5.4.1) Installation et paramétrage du service de déduplication des données

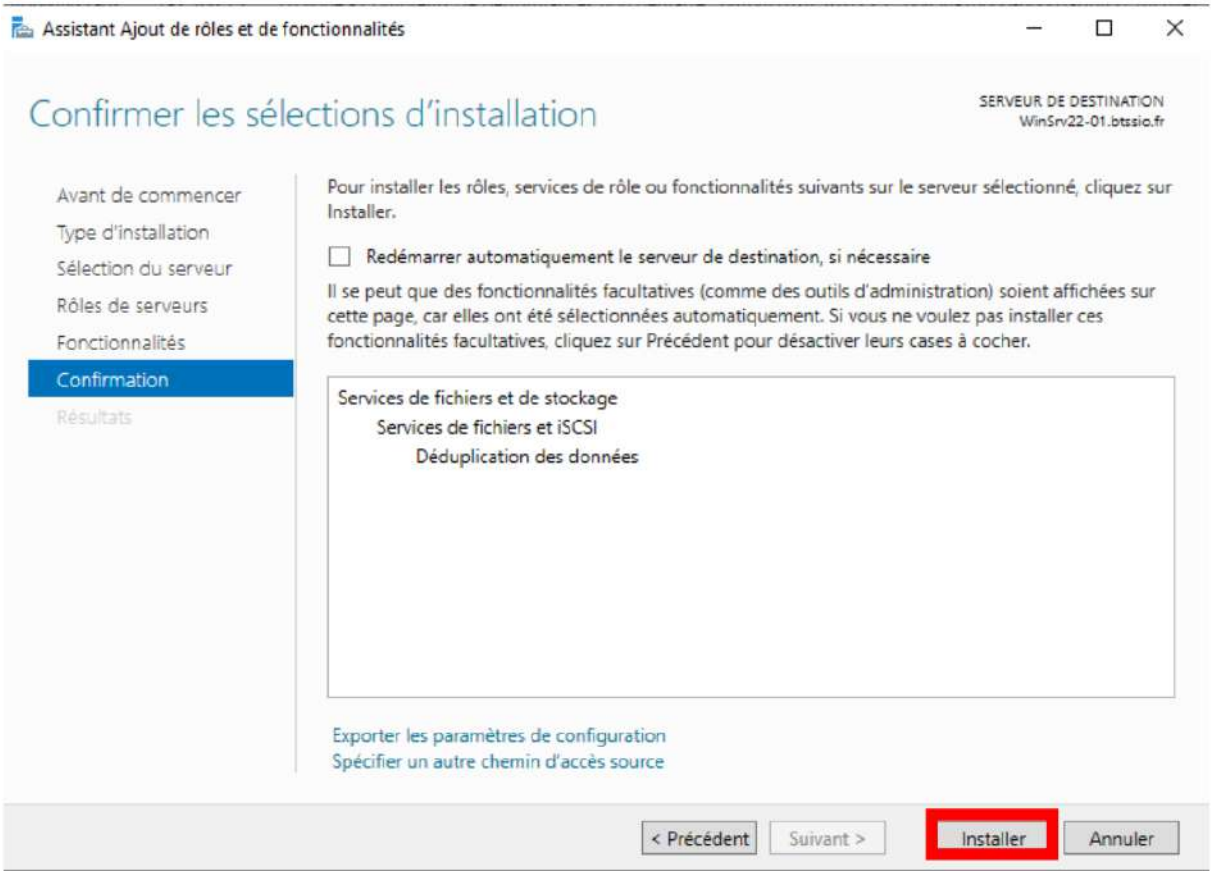
Il faut tout d'abord installer le rôle, dans Gérer sur le gestionnaire de serveur puis "Ajouter des rôles et fonctionnalités" :



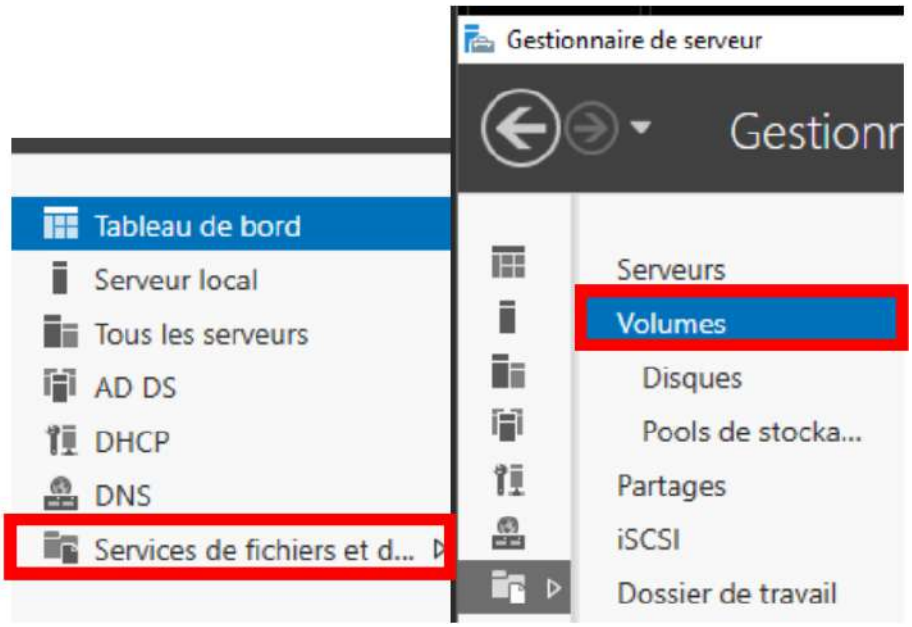
Ensuite, on coche "Déduplication des données" :



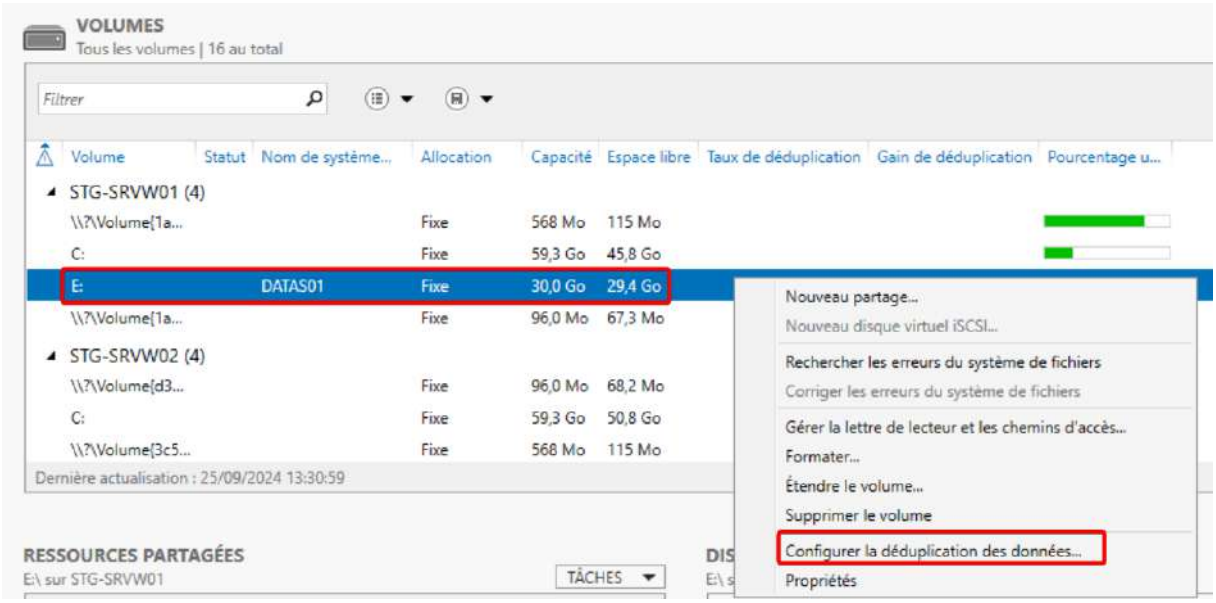
Puis on peut faire Suivant jusqu'à Installer :



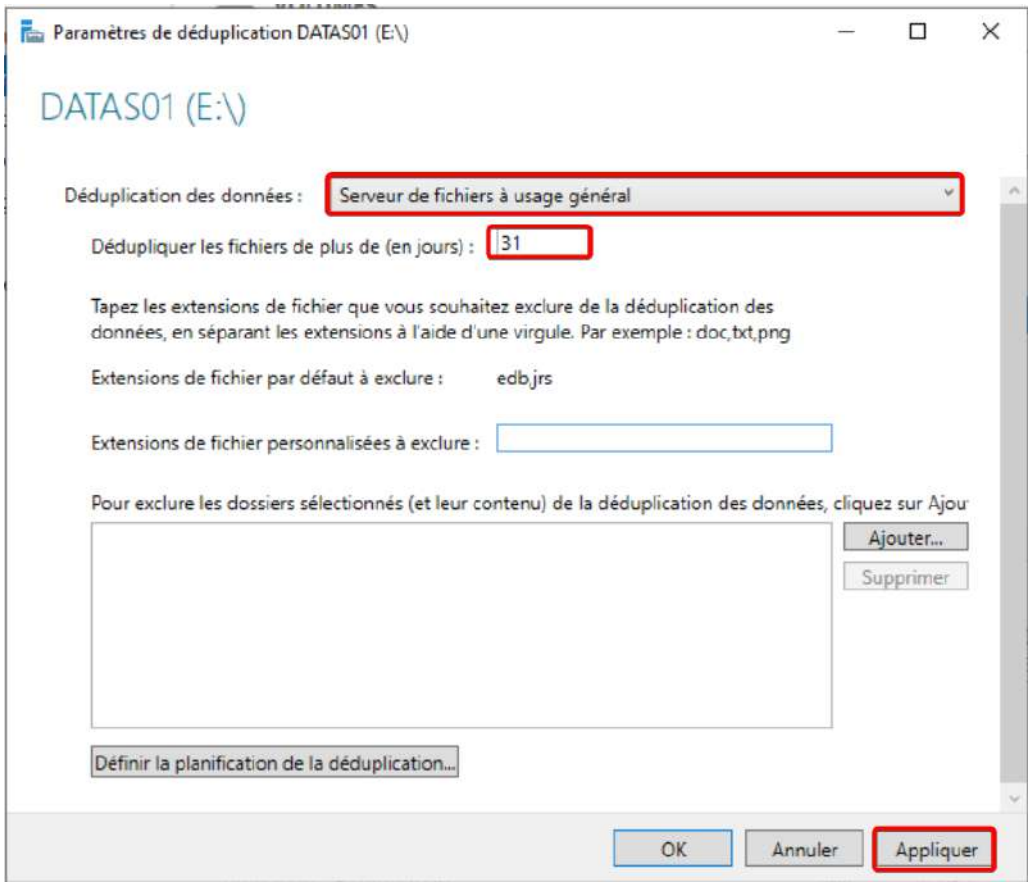
Depuis le gestionnaire de serveur, aller dans "Services de fichiers et de stockages" puis "Volumes"



On cherche notre disque à dédupliquer et on clique sur "Configurer la déduplication des données":



On choisit le type de déduplication, le temps avant déduplication et on clique sur appliquer :



La déduplication est en place.

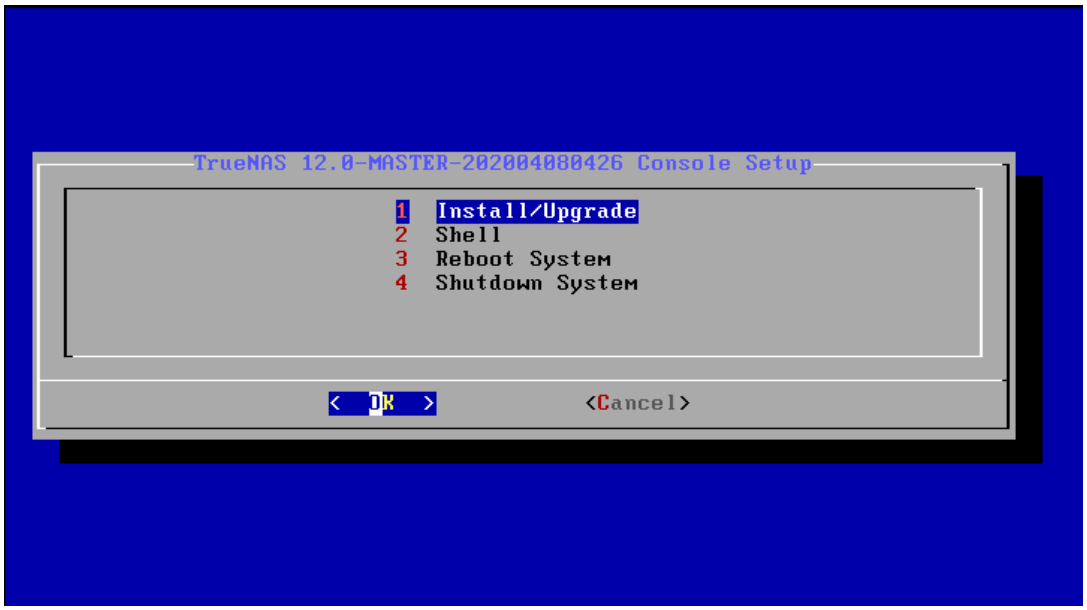
6) Montage d'une cible iSCSI avec TrueNAS Core

TrueNas est une solution de NAS, basé sous FreeBSD 13.0, il existe en plusieurs versions (community/professionnel). Nous allons utiliser cette solution afin de réaliser une cible iSCSI pour faire une sauvegarde complète de nos Windows Serveurs.

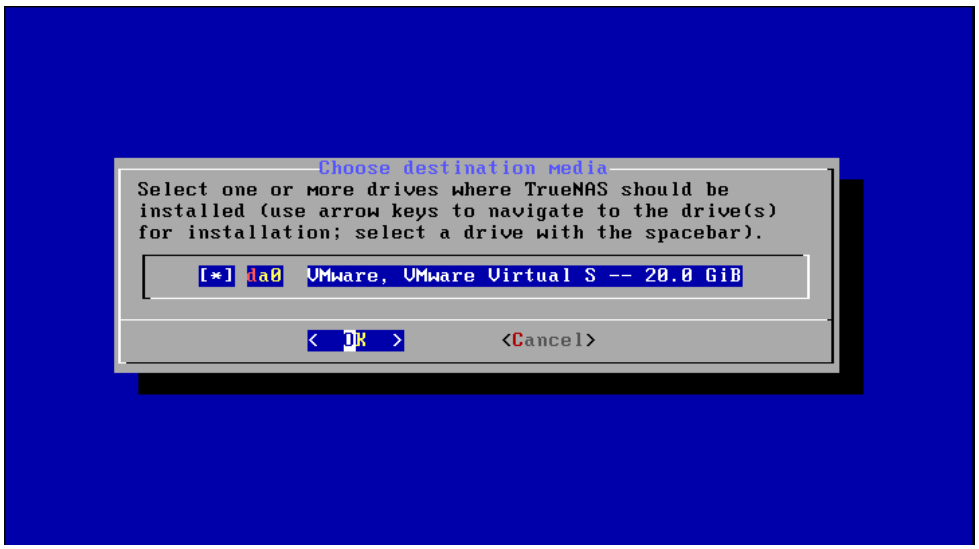
6.1) Installation de TrueNAS

Pour commencer, il faut boot dans le TrueNAS Installer :

Ensuite, on sélectionne "Install/Upgrade" :

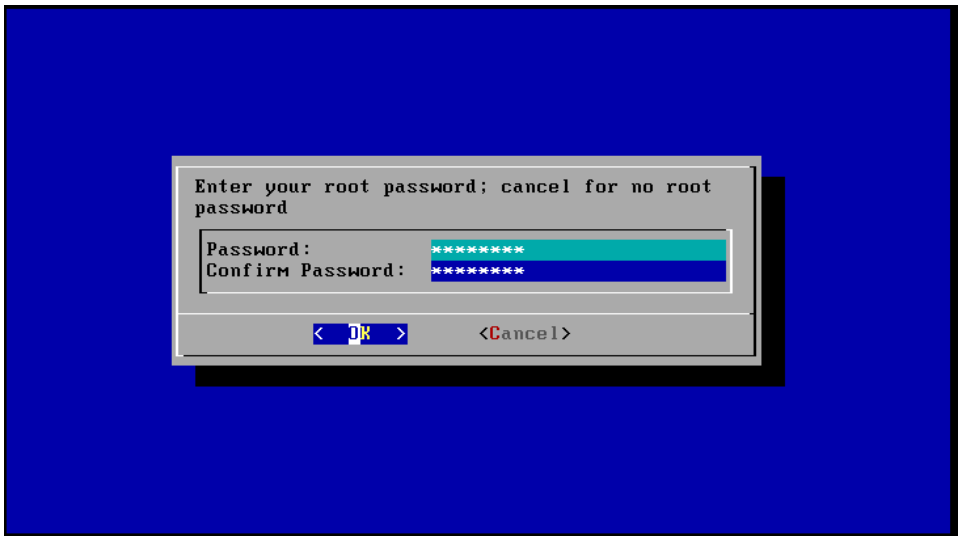


Puis on sélectionne notre disque sur lequel on souhaite installer TrueNAS :

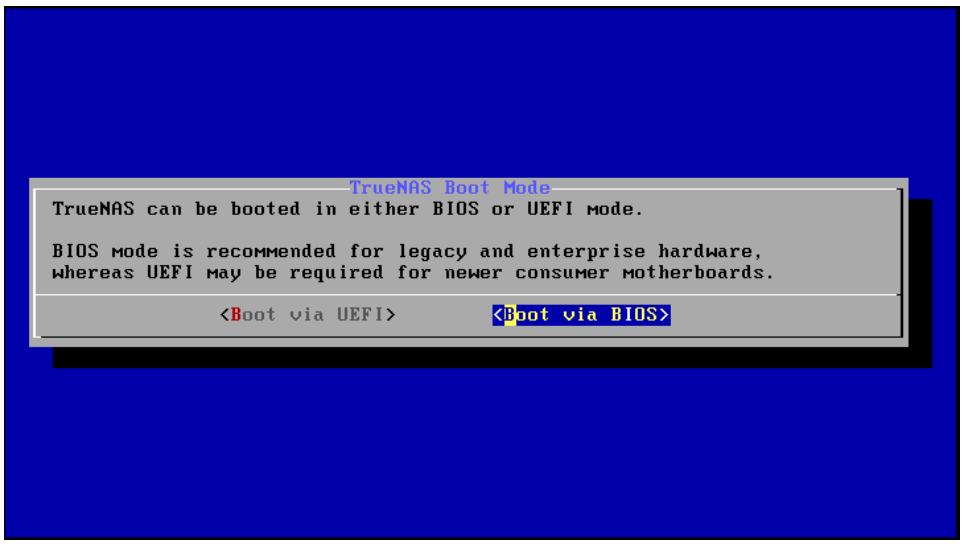


On accepte ensuite les modifications :

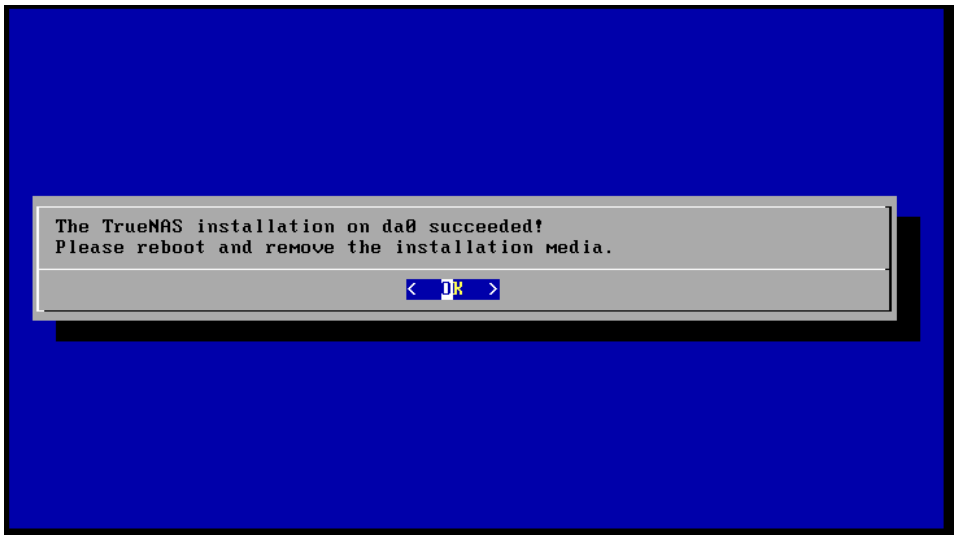
Il faut ensuite choisir le mot de passe root :



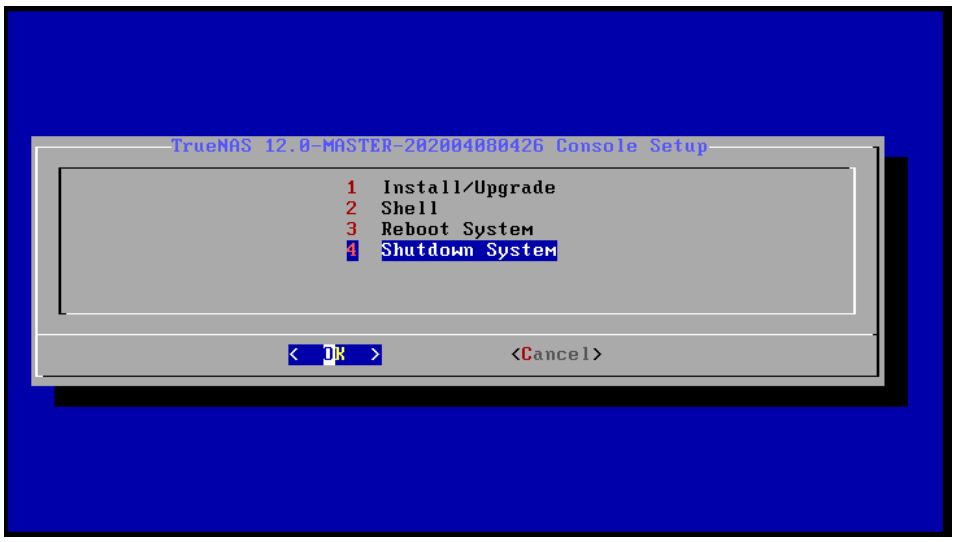
On peut boot via BIOS ou UEFI en fonction de nos besoins :



L'installation est maintenant terminée ! :

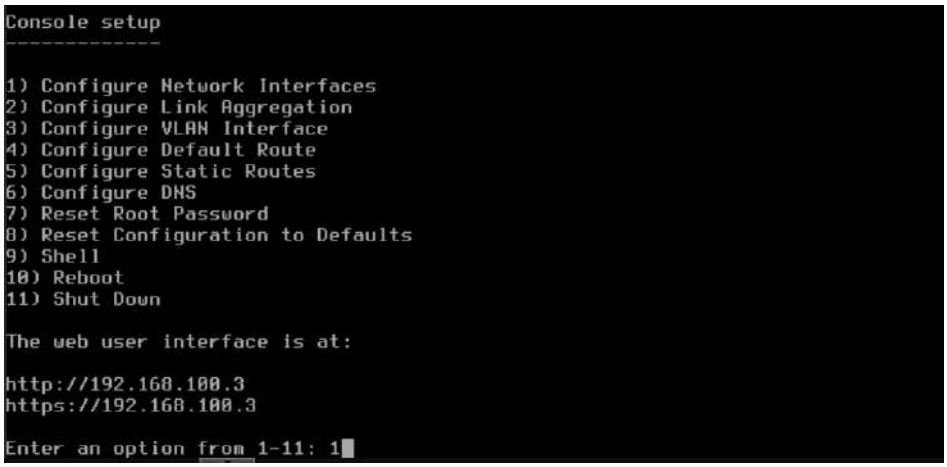


On choisit "Reboot System" ou "Shutdown System”:

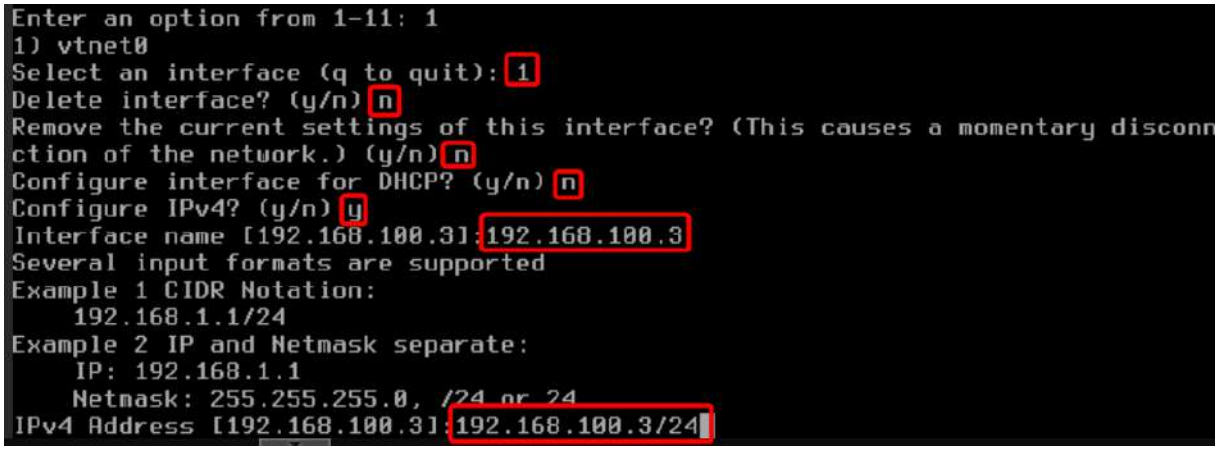


6.2) Configuration de TrueNAS

Nous allons tout d'abord faire la configuration réseau en sélectionnant l'option 1 :

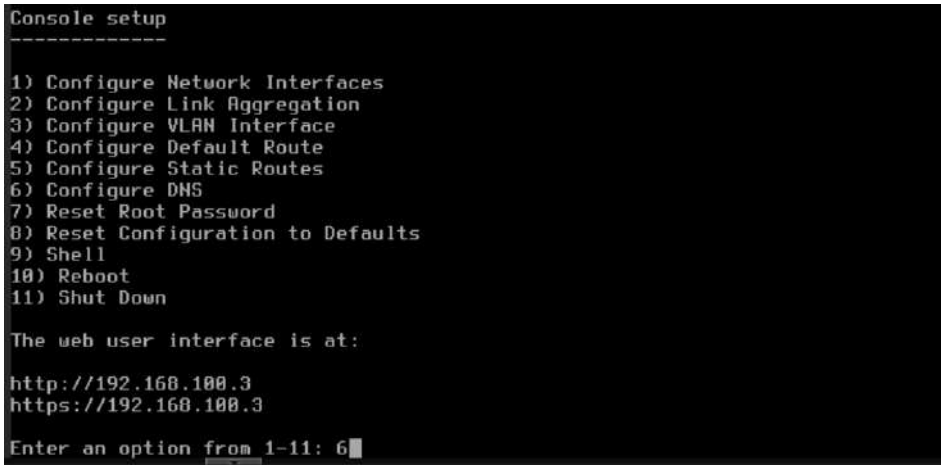


Puis on sélectionne notre carte réseau, ensuite, on fait "n", a nouveau "n", puis si vous souhaitez configurer l'IPv4 via DHCP il faut mettre "y" sinon "n", on rentre ensuite le nom de l'interface et enfin son adresse IP au format CIDR :

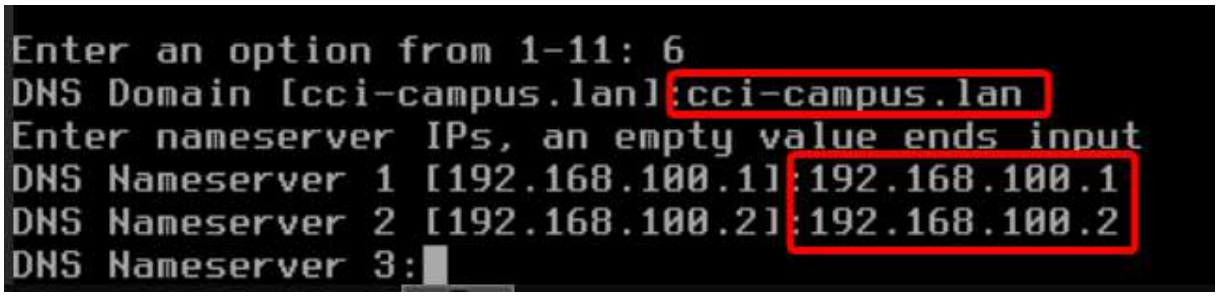


Si l'on souhaite de l'IPv6 on peut mettre "y", dans notre cas nous allons mettre "n".

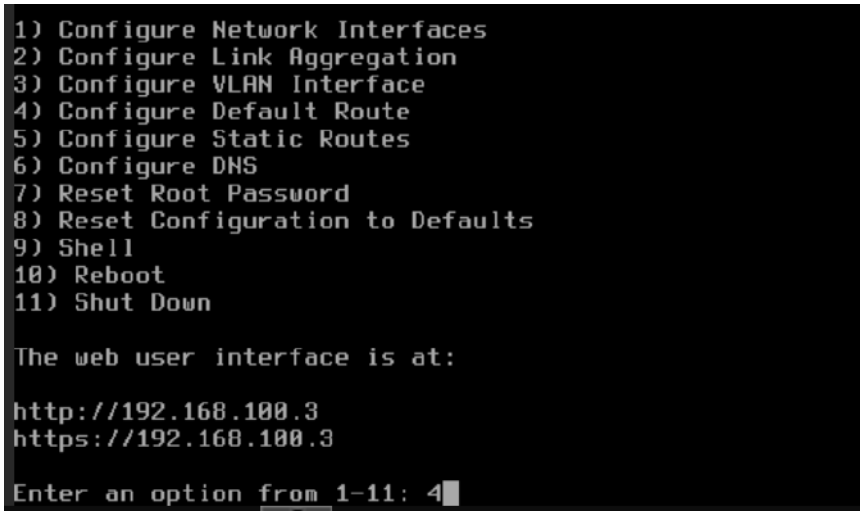
On configure ensuite les DNS avec l'option 6 :



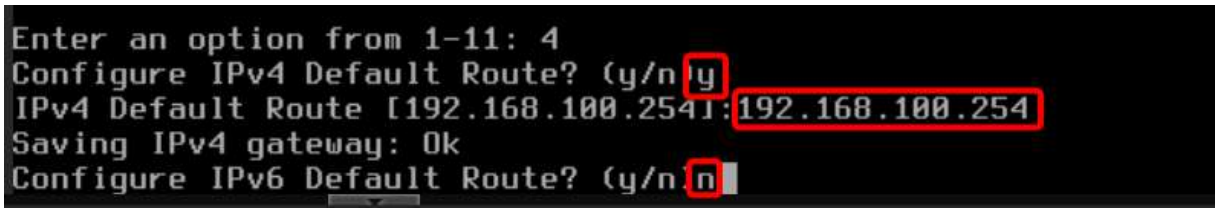
On rentre ensuite le nom du domaine, puis les différents serveurs DNS et enfin on peut appuyer sur entrée :



Pour finir, nous allons configurer la passerelle par défaut avec l'option 4 :



On choisit de configurer une passerelle IPv4 avec y, puis on rentre l'IP de la passerelle en notation CIDR et on ne configure pas de passerelle IPv6 avec n :



La configuration réseau est maintenant terminé.

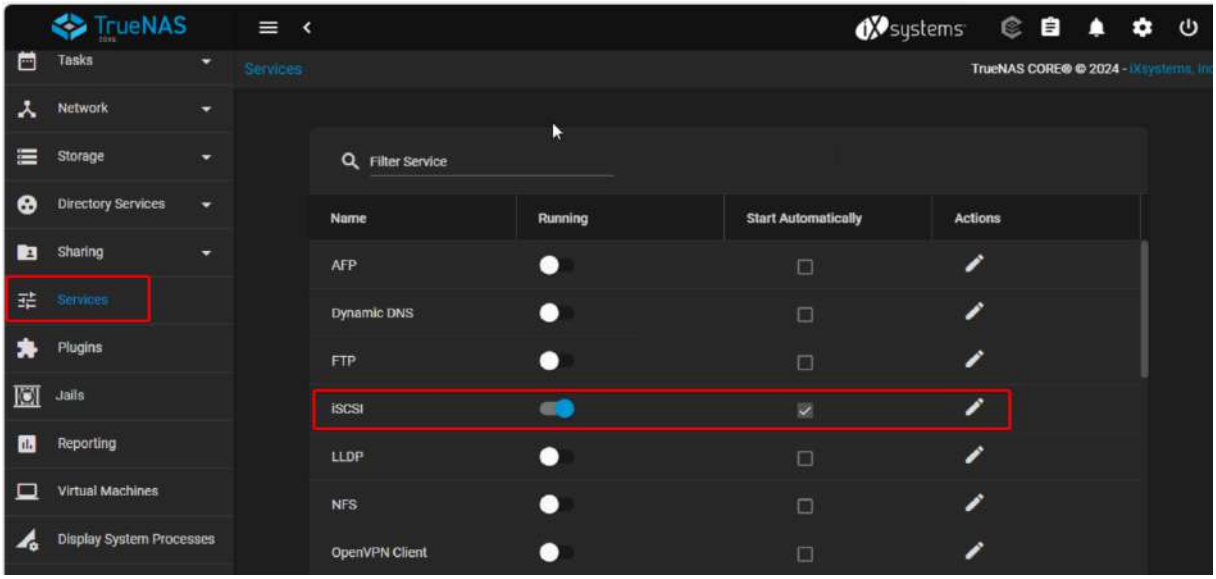
6.3) Configuration d'une cible iSCSI

Tout d'abord, nous allons nous connecter à l'interface web :

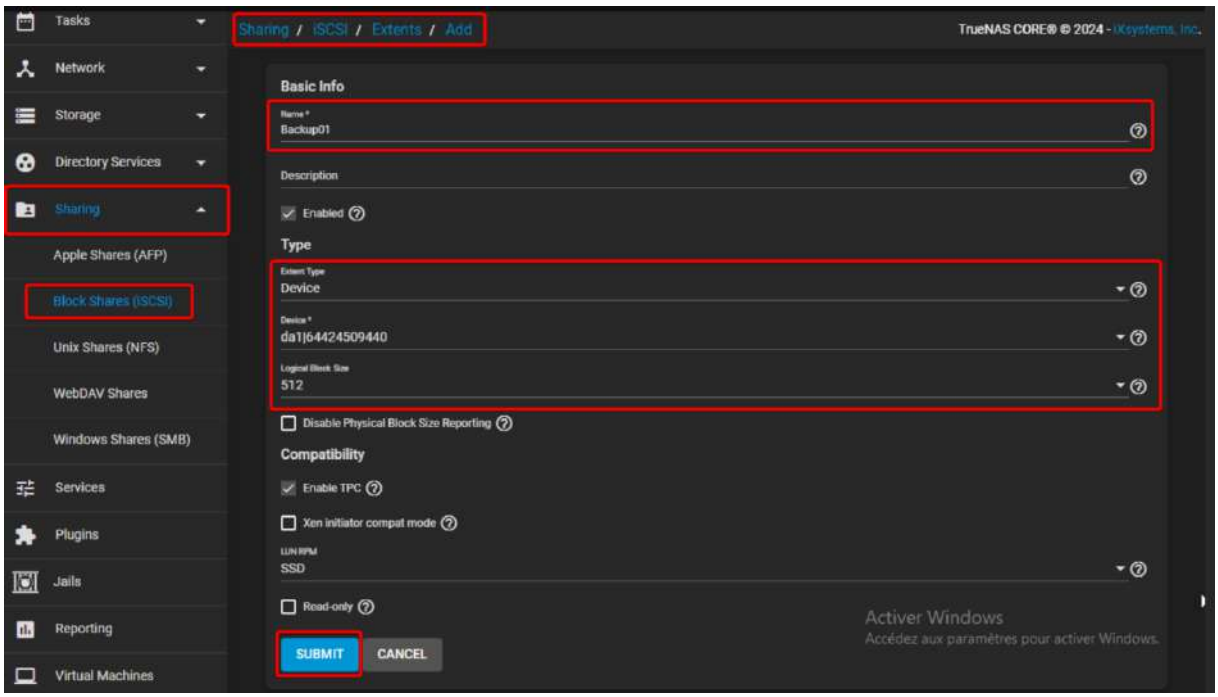
https://IP_NAS

Puis on se connecte avec les identifiants root.

Il faut activer le service iSCSI, dans "Settings" :



Ensuite, il faut ajouter un "Extents" et configurer son nom et le disque à utiliser, puis cliquer sur "Sumbit" :

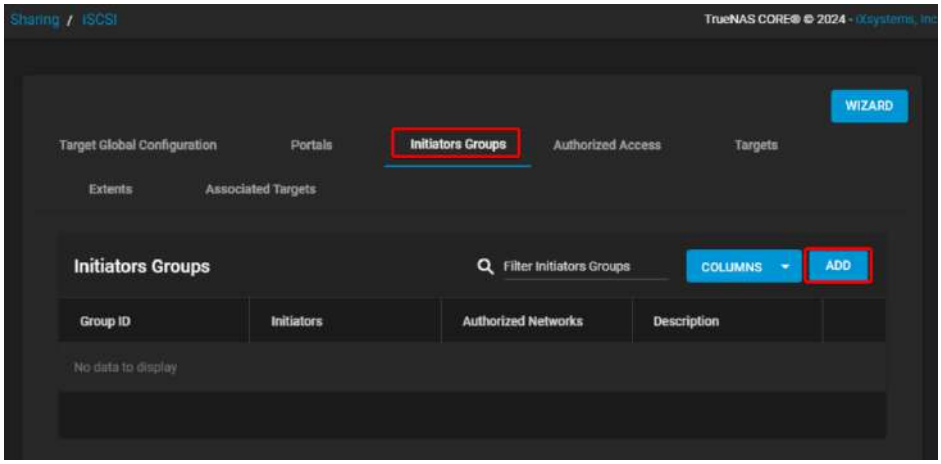


Il faut maintenant créer un "Portal", on vient mettre en adresse IP 0.0.0.0, ce qui signifie qu'il va écouter sur toutes les interfaces réseaux du NAS :

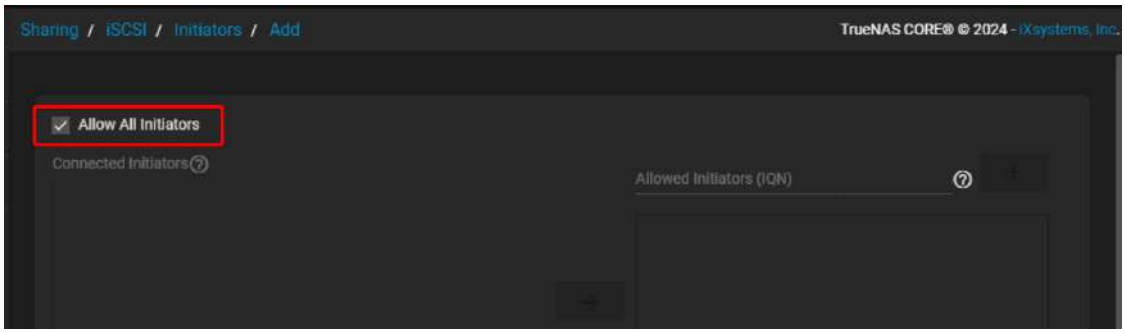
Info

Il est possible d'utiliser le protocole CHAP (protocole basé sur le défi réponse) pour sécuriser la connexion avec le point de montage iSCSI, nécessitant ainsi des informations d'identification.

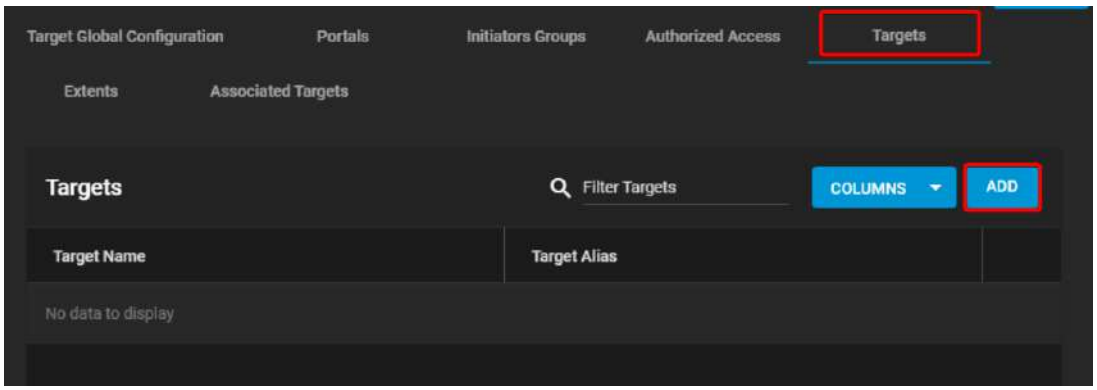
Ensuite, nous allons créer un "Initiators Groups" :



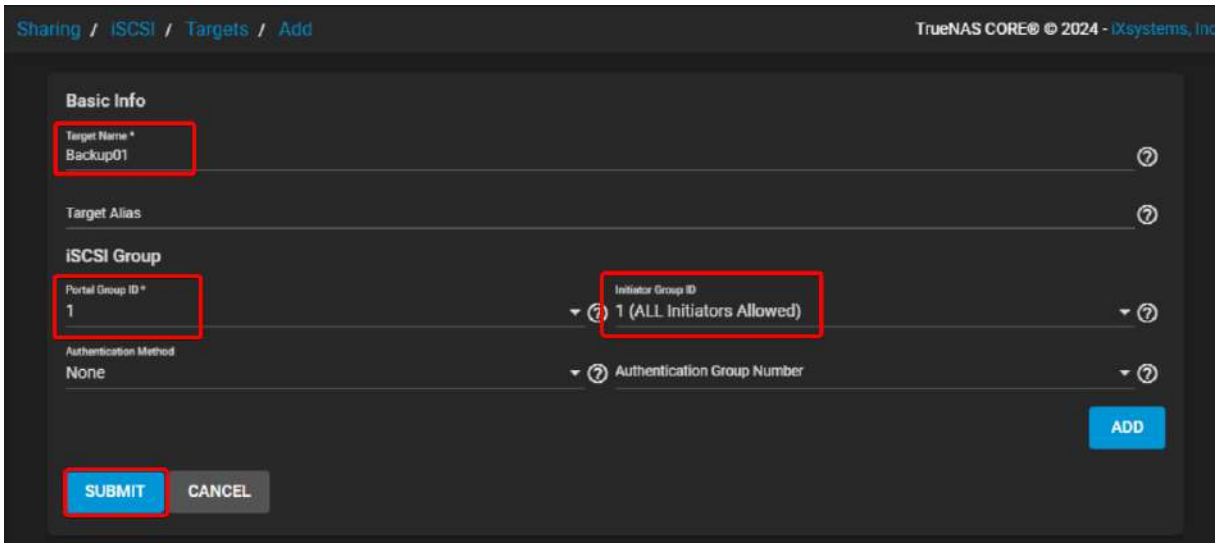
On coche la case "Allow All Initiators" pour autoriser tout le monde, on peut cliquer sur "Save" :



Puis, il faut créer une "Target" :



On va lui donner un Nom, le Portal Group ID qui correspond à celui créé précédemment et le Initiator Group ID créé aussi avant, on peut ensuite valider :



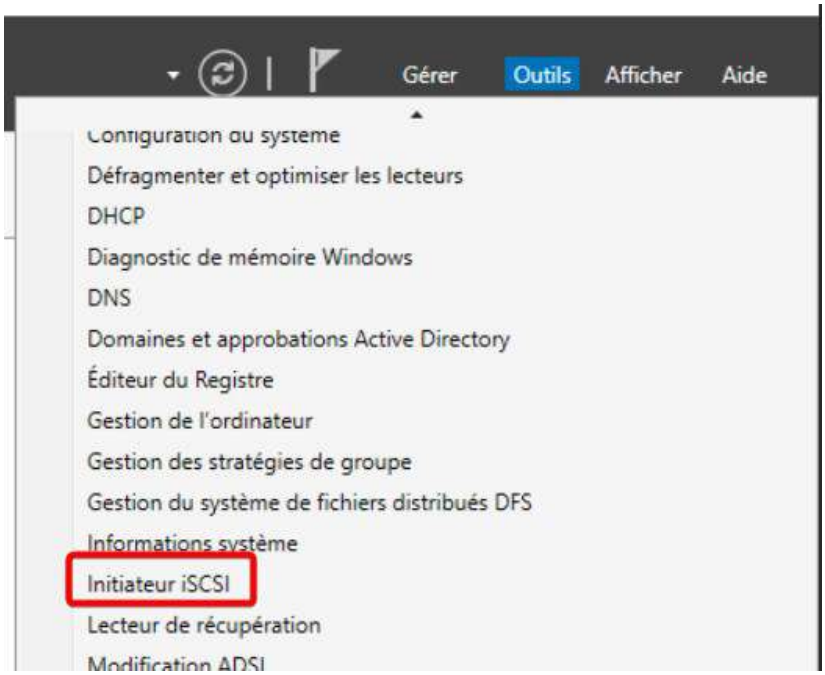
Enfin, nous allons associer notre Target avec notre Extent, pour cela il faut se rendre dans l'onglet "Associated Targets" et créer une nouvelle association.

On sélectionne notre Target et notre Extent, puis on valide :

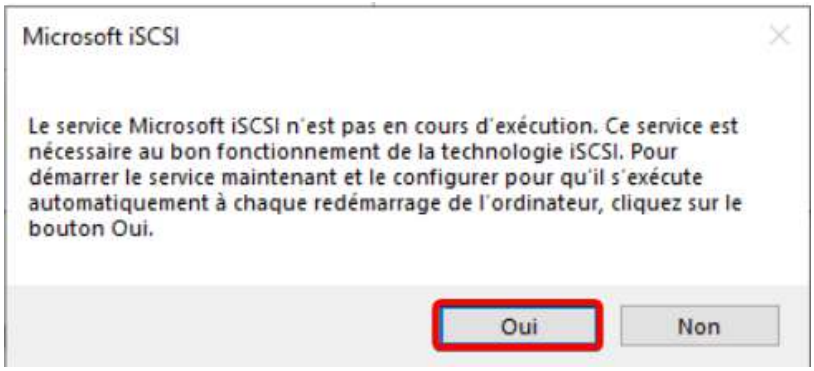
Notre cible iSCSI est maintenant détectable sur le réseau.

6.4) Connexion iSCSI depuis un Windows Serveur

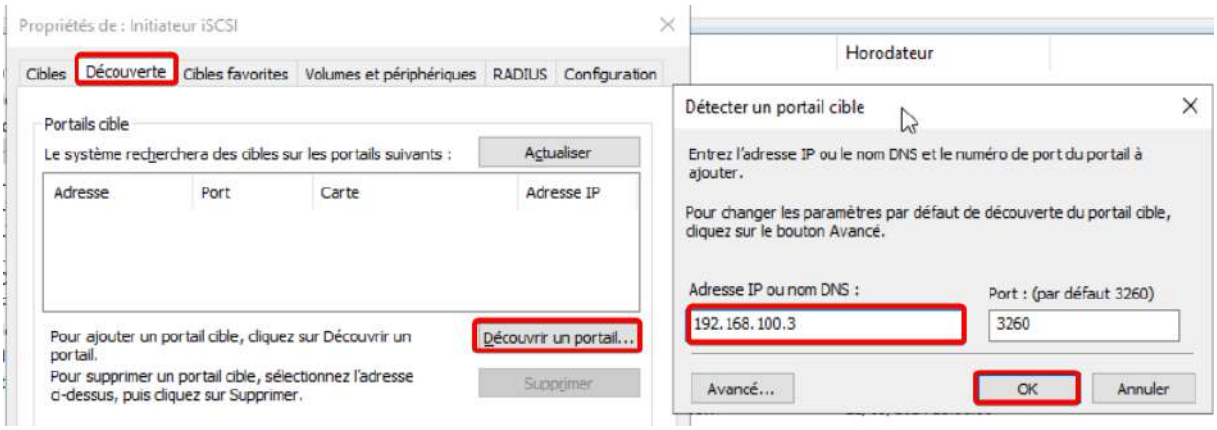
Tout d'abord, il faut ouvrir l'initiateur iSCSI depuis le gestionnaire de serveur :



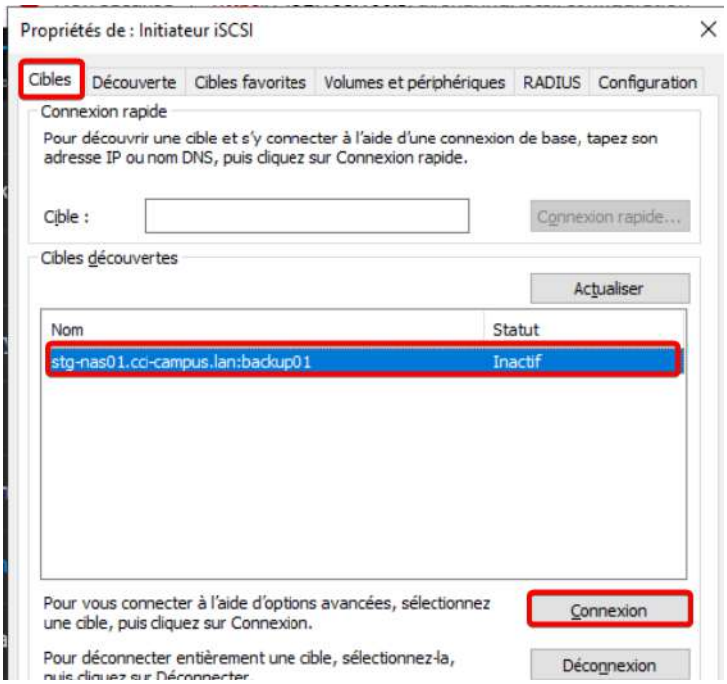
Un message nous demande d'activer le service iSCSI, on accepte :



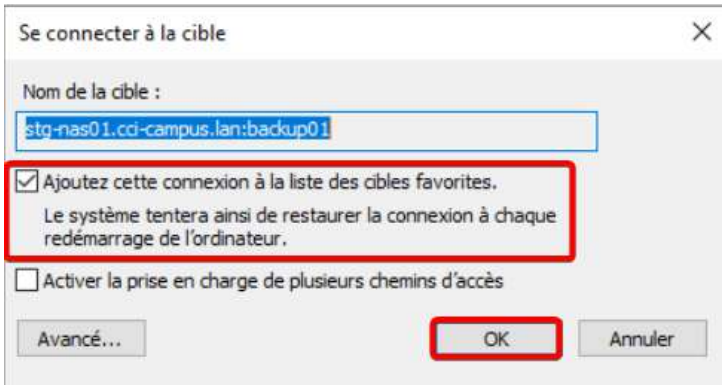
On va dans l'onglet "Découverte", puis on clique sur "Découvrir un portail...", il faut ensuite rentrer l'adresse IP ou le nom DNS de notre NAS et cliquer sur OK :



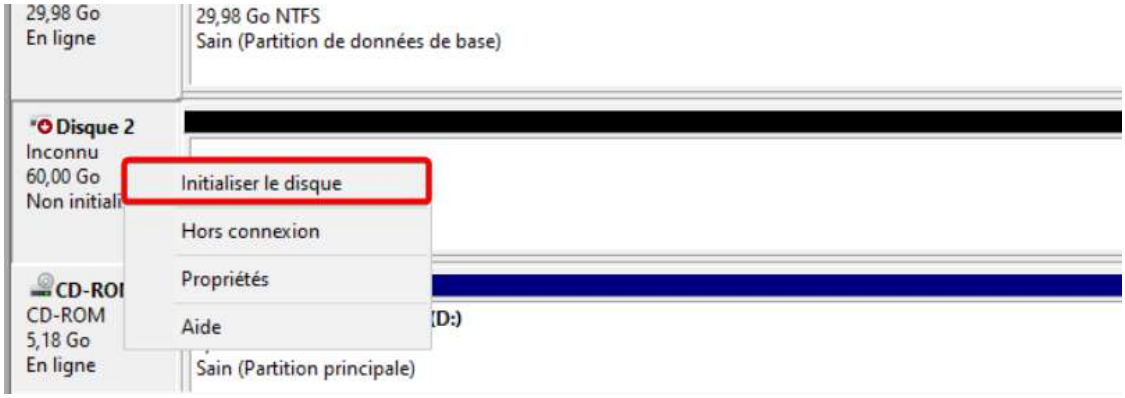
Ensuite, il faut aller dans l'onglet "Cibles" et vérifier que la cible remonte bien, on peut donc cliquer sur "Connexion" :



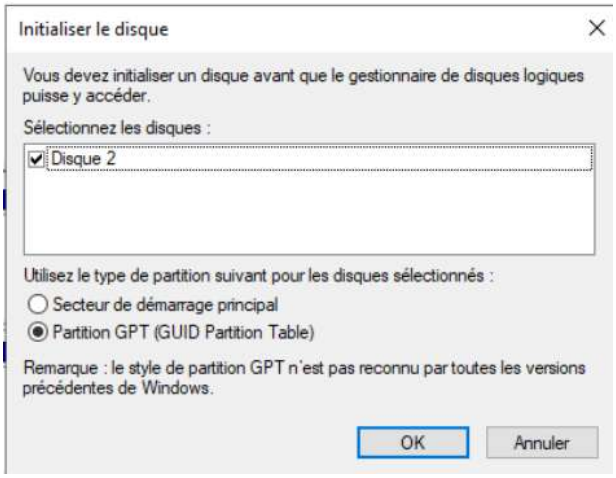
On ajoute la connexion à la liste des cibles favorites afin que la connexion persiste au redémarrage :



Une fois le disque monté il faudra l'initialiser et le formater correctement. Il faut aller dans la console de "Gestion des disques" et faire clique droit sur le nouveau disque, puis "Initialiser le disque" :

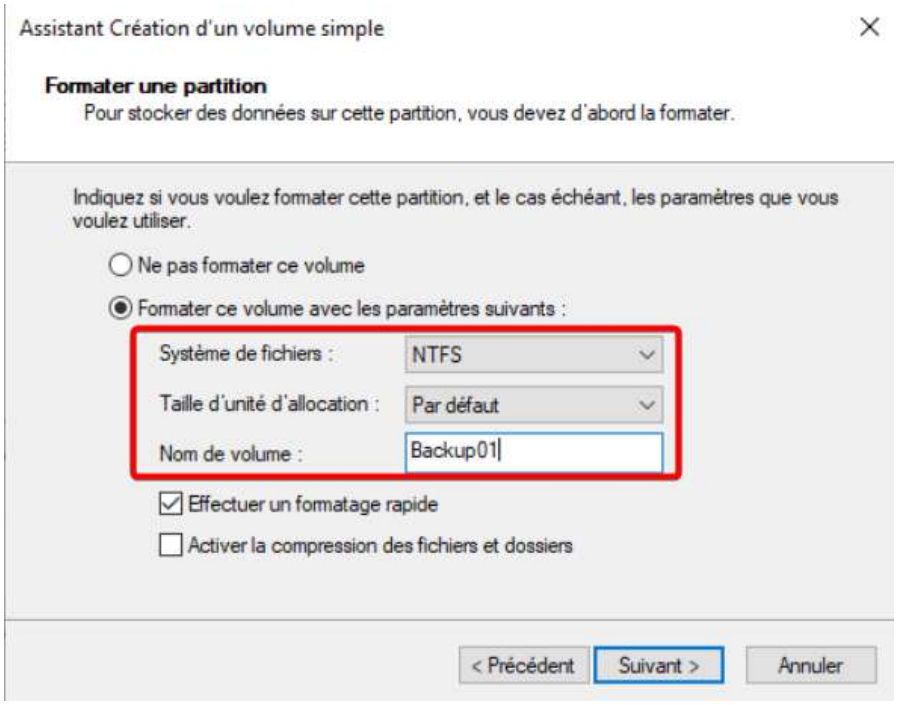


On sélectionne partition GPT (par défaut), puis on valide :



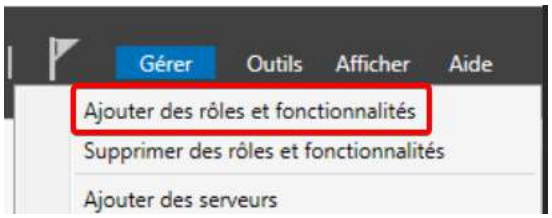
On fait ensuite clique droit sur le disque initialiser et on sélectionne "Nouveau volume simple" :

L'assistant Création d'un volume simple va s'ouvir, on peut cliquer sur suivant et laisser par défaut les options jusqu'au moment de choisir le Système de fichier et le nom du volume. On choisit donc en format NTFS et on donne un nom au volume :

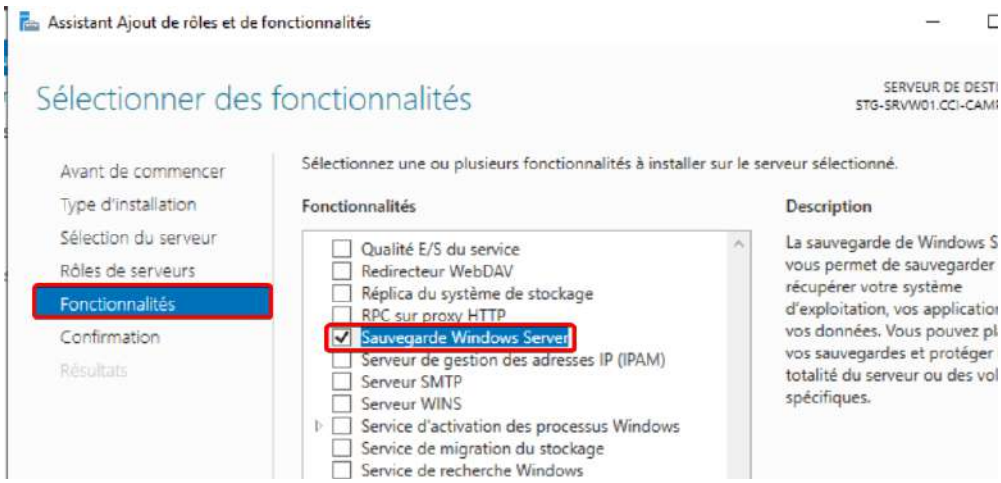


6.5) Configurer les sauvegardes Windows Serveur

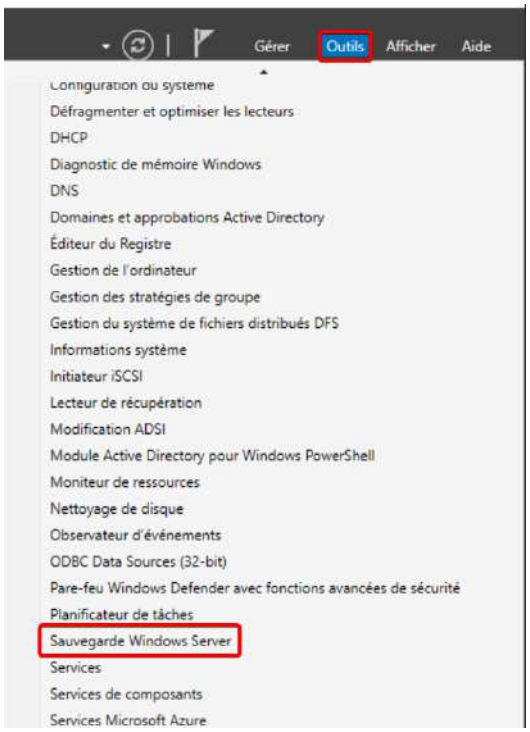
Tout d'abord, il faut ajouter la fonctionnalité "Sauvegarde Windows Server", cliquer sur "Ajouter des rôles et fonctionnalités" depuis votre gestionnaire de serveur :



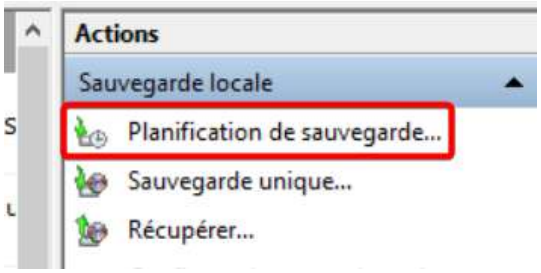
Ensuite, on peut se rendre dans la partie "Fonctionnalités" et cocher "Sauvegarde Windows Server":



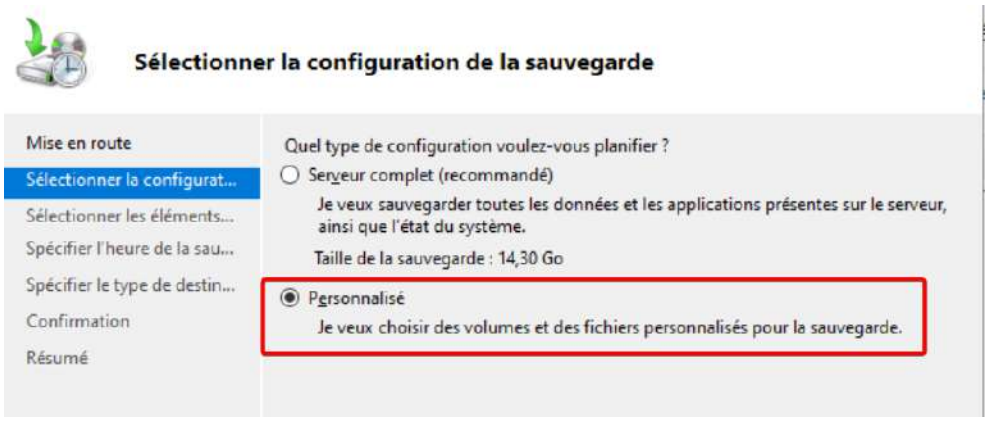
On peut ensuite ouvrir depuis le gestionnaire de serveur, l'outil Sauvegarde Windows Server :



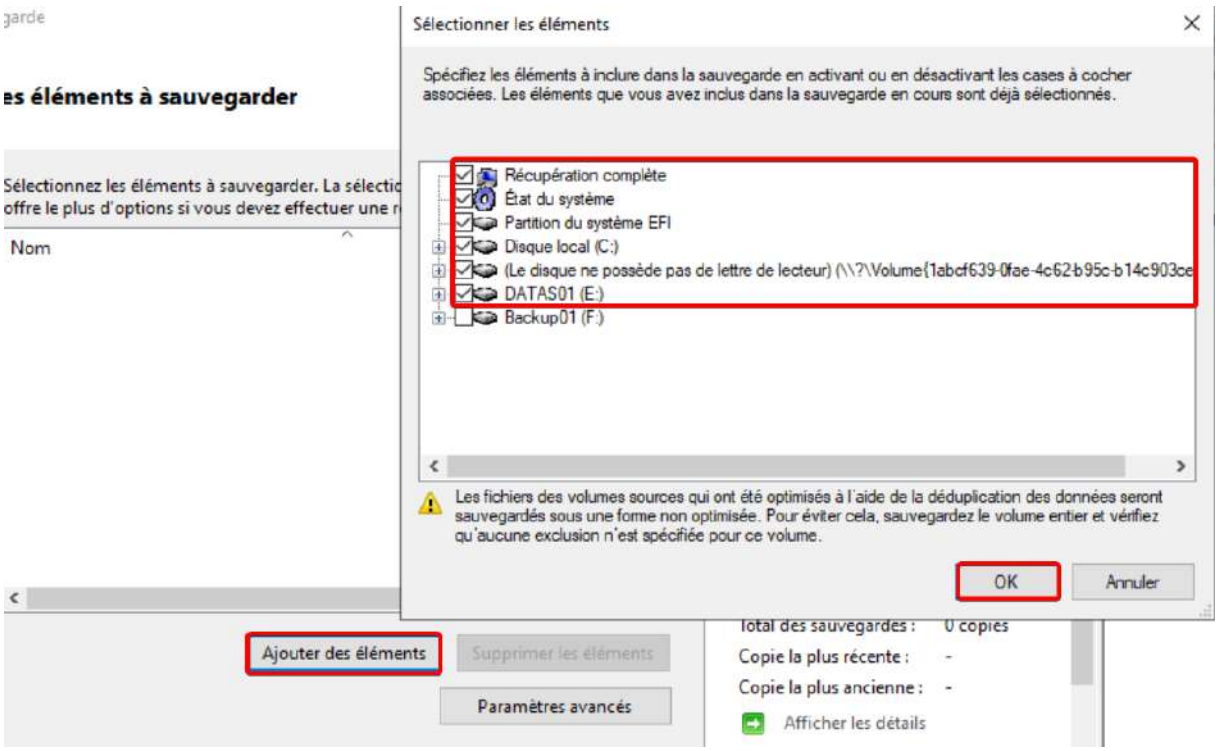
On clique ensuite sur "Planification de sauvegarde..." :



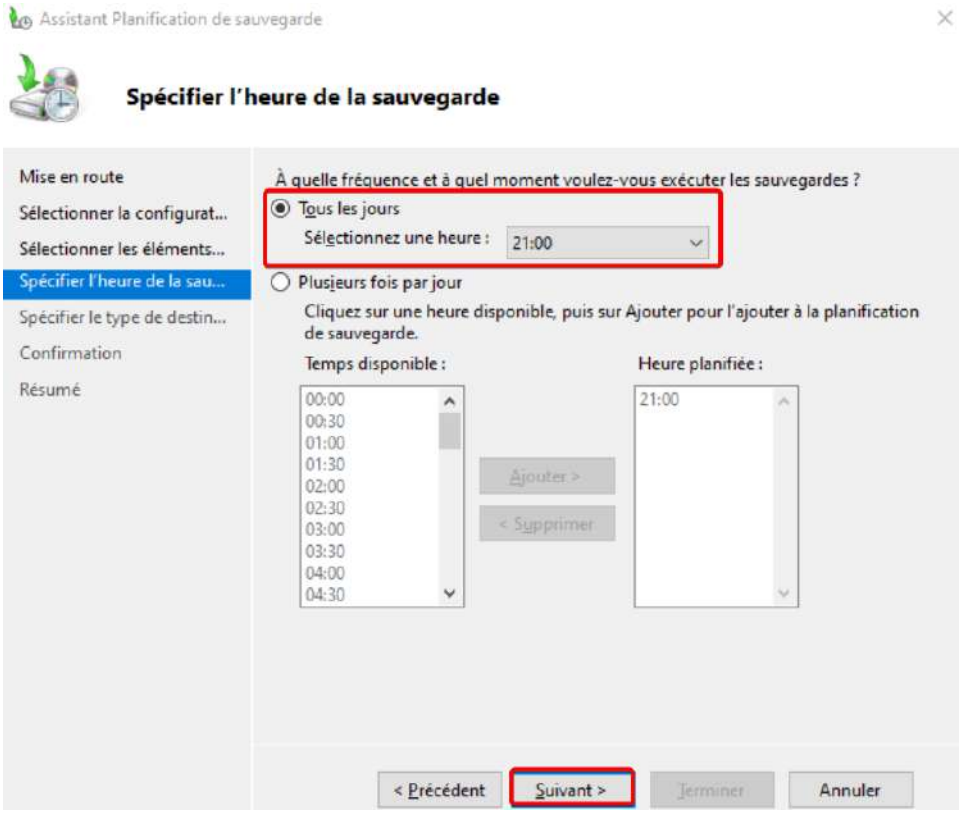
Puis on peut faire suivant, ensuite "Personnalisé" :



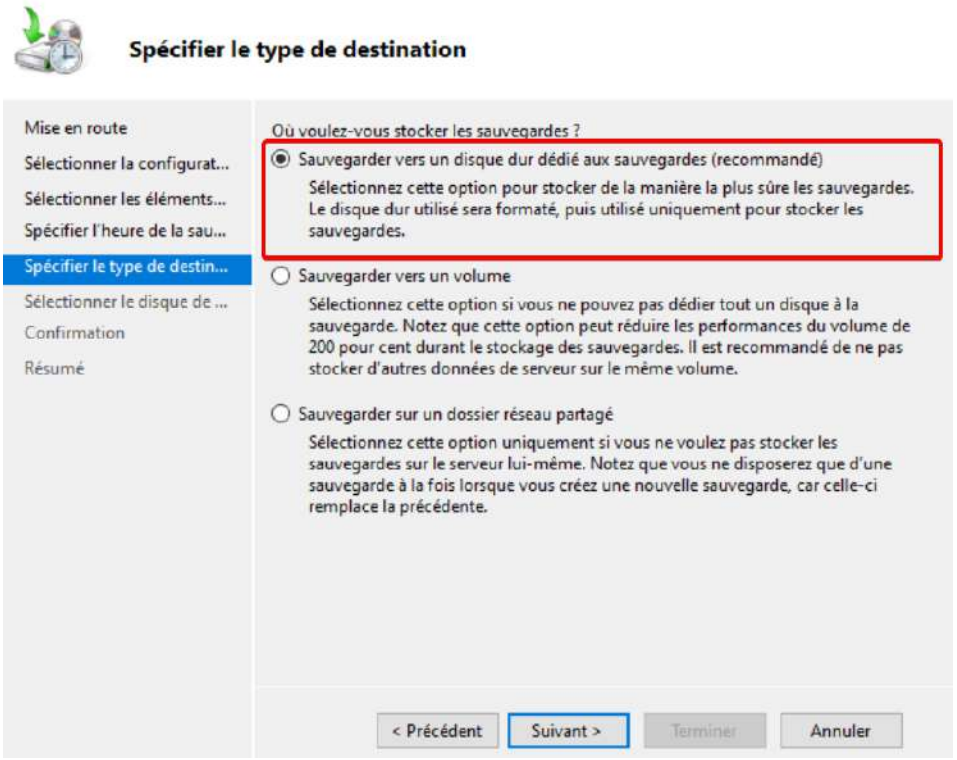
Ensuite, on clique sur "Ajouter des éléments", on sélectionne "Récupération complète" et le disque "DATAS01", puis on peut valider et passer à l'étape suivante :



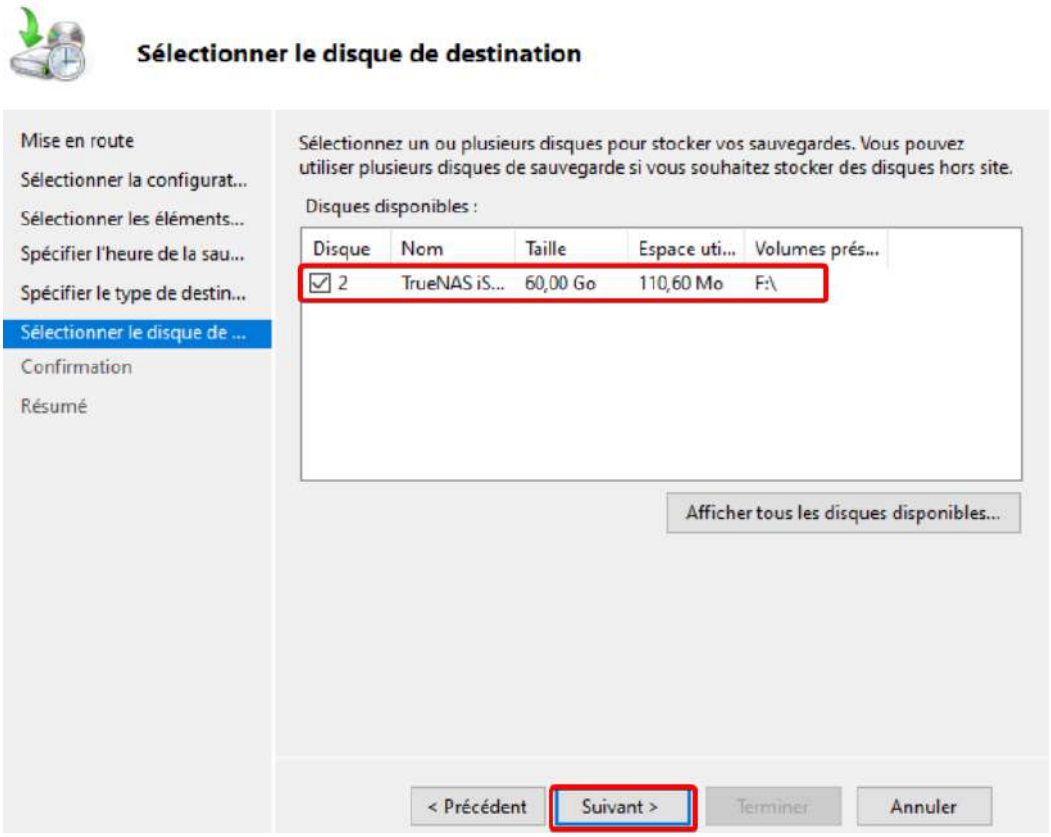
Il faut ensuite sélectionne la fréquence des sauvegardes :



Enfin on sélectionne la première option :



Et on sélectionne enfin notre disque iSCSI :

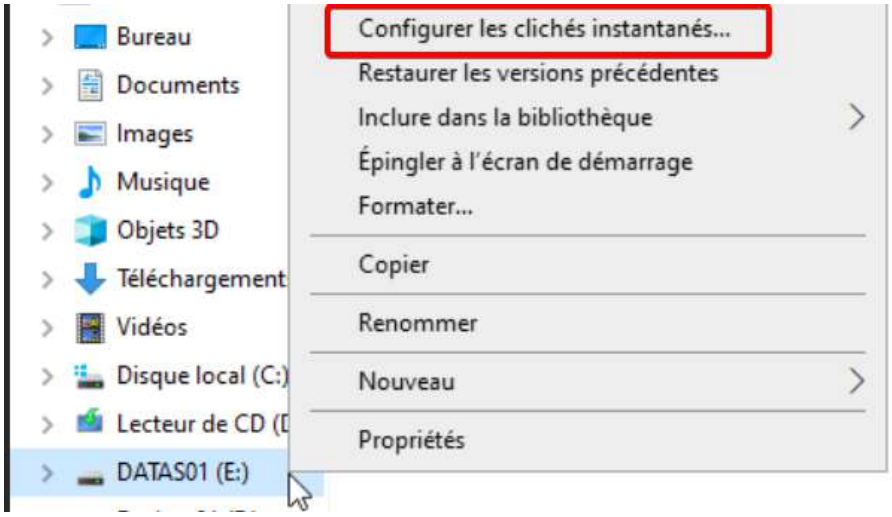


Puis on peut confirmer, notre sauvegarde programmée OS + DATAS est maintenant opérationnelle.

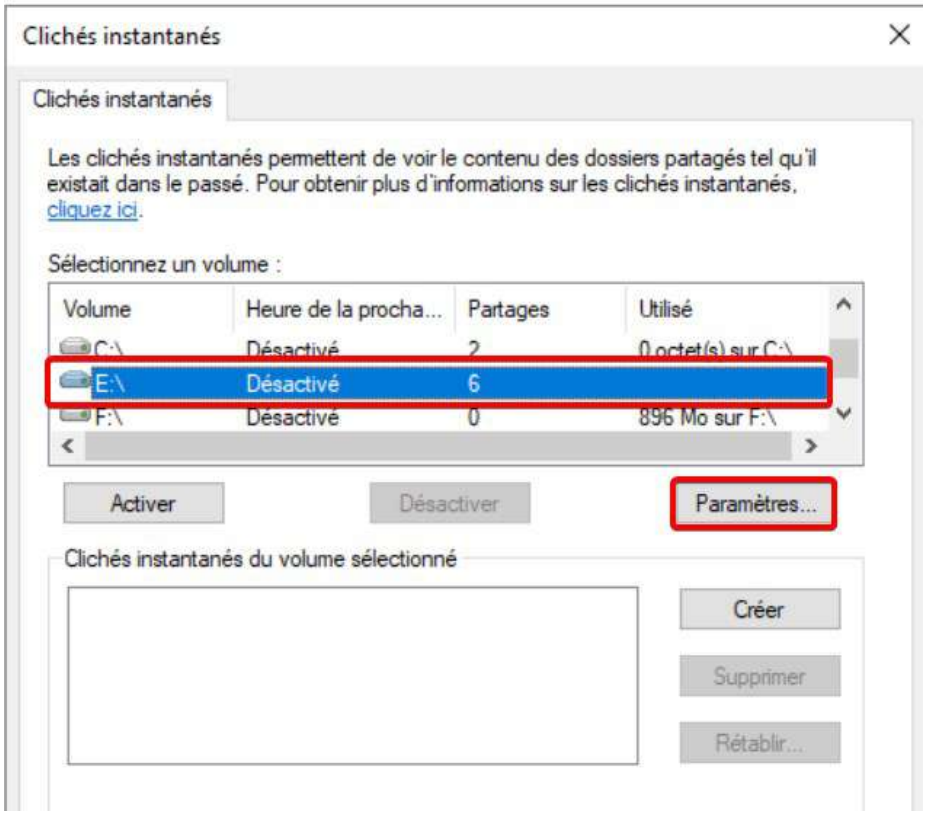
6.6) Configurer les Shadow copies

Les Shadow copies ou clichés instantanés, permettent de faire un snapshot d'un disque. Elles peuvent être pertinente pour des dossiers partagés, et sont très simple à restaurer.

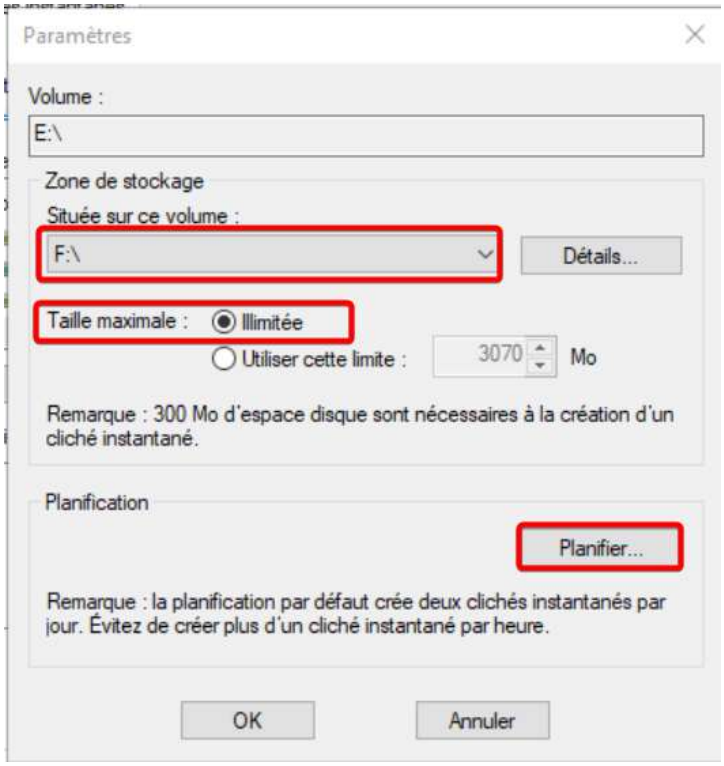
Pour se faire, il faut faire clic droit sur le disque à configurer pour faire des Shadow copies, puis sur "Configurer les clichés instantanés..." :



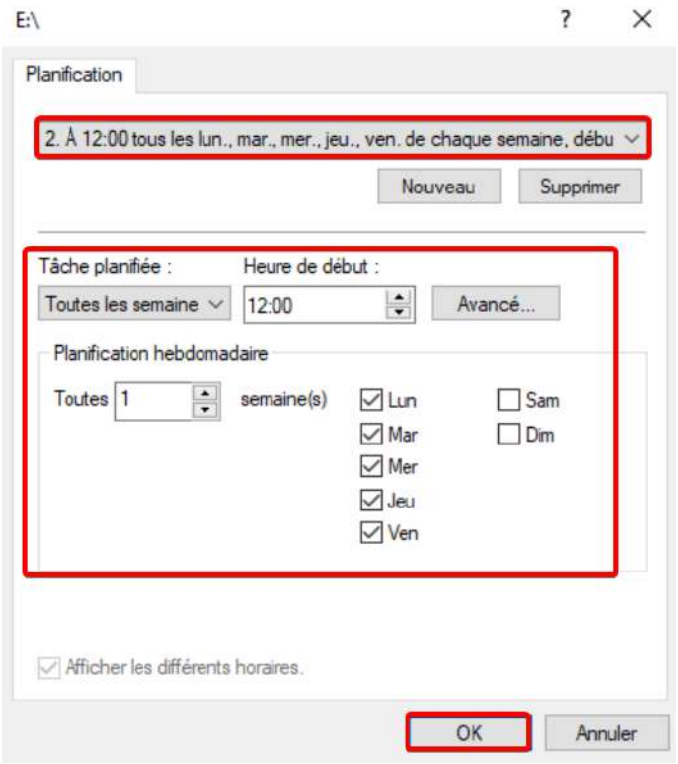
Puis il faut sélectionner le disque et cliquer sur "Paramètres..." :



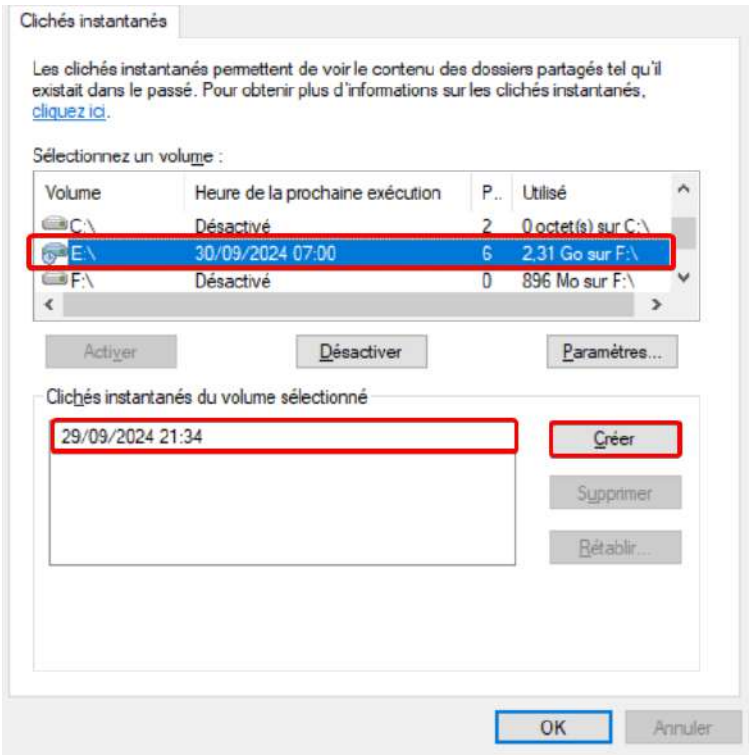
Ensuite, on sélectionne le volume sur lequel on souhaite enregistrer les Shadow copies (dans notre cas F), on mets la taille maximal en illimitée et on peut cliquer sur "Planifier..." :



Puis, on choisis la fréquence à laquelle on souhaite effectuer les Shadow copies et on peut cliquer sur OK :



Enfin, on peut créer notre première snapshot manuellement en cliquant sur le bouton "Créer" et voir l'heure de la prochaine exécution :



Nos Shadow copies sont désormais opérationnelles et enregistrées sur NAS via notre point de montage iSCSI