



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	3
1.1) Prérequis	3
1.1.1) Serveur Windows Server 2022 (VM)	3
1.1.2) Client Windows 10/11 (VM)	3
1.1.3) Carte Réseau VMware	3
1.2) Pré configuration	4
1.2.1) Changer le nom de l'ordinateur	4
1.2.2) Configurer une adresse IP statique	5
1.2.3) Modification du mot de passe administrateur	6
1.3) Installation de l'Active Directory et du DHCP	7
1.3.1) Ajout des rôles et fonctionnalités	8
1.3.2) Configuration de l'AD DS	9
1.3.3) Configuration du DHCP	11
1.4) Exploiter le domaine	13
1.4.1) Joindre le domaine	13
1.4.2) Créer un utilisateur/groupe	14
1.4.2 bis) Créer un utilisateur	15
1.4.2 bis) Créer un groupe	15
1.4.2 bis) Attribuer un groupe	16
1.4.2 bis) Créer un conteneur	17
1.4.3) Modifier une GPO	19
1.4.4) Vérification du domaine sur le PC	21
1.4.4 bis) Par ligne de commande	21
1.4.4 bis) Par interface graphique	21
1.4.5) Vérification du DHCP sur le PC	22
1.5) Redondance	24
1.5.1) Pré configuration	24
1.5.2) Connexion au domaine	25
1.5.2 bis) Vérification des flux réseau	25
1.5.2 bis) Joindre le serveur au domaine	26
1.5.3) Configuration des rôles	27
1.5.4) Vérification de la redondance	28
2) Installation et configuration d'un homelab Proxmox	29
2.1) Prérequis	29
2.2) Installation de l'OS	29
2.2.1) Préparation du support d'installation	29
2.2.2) Installation	30
2.3) Configuration réseau	33
2.3.1) Théorie	33
2.3.2) Configuration interfaces réseau	34
2.3.3) Configuration du NAT IPtables	36

2.4) Ajouter des ISO et créer sa première VM	37
2.5) Joindre l'hyperviseur depuis Internet	40
3) Installation et configuration de Pfsense	42
3.1) Installation de Pfsense	42
3.2) Configuration de Pfsense	47
3.3) Mise en place du VPN IPsec site à site	48
4) Configuration supplémentaires Windows Serveur 2022	52
4.1) Redondance réseau (IP Bouding)	52
4.1.1) Bridge de cartes réseau avec STP actif	52
4.1.2) NIC Teaming	54
4.2) DHCP de basculement	55
4.3) GPO	56
4.3.1) Déployer un fond d'écran et bloquer son changement	58
4.3.2) Redirection de dossiers	59
4.3.3) Mappage de lecteurs réseau	60
4.3.4) Interdire l'accès au panneau de configuration	61
4.3.5) Empêcher l'exécution d'une GPO pour un groupe	62
4.3.6) Bloquer les ports USB par clé de registre	63
4.3.7) Bloquer les ports USB	64
4.3.8) Masquer et empêcher l'accès au lecteur C	65
4.3.9) Bloquer l'accès aux consoles Powershell et Invite de commande	66
5) Mise en place DFSR & Déduplication des données	68
5.1) Prérequis	68
5.2) DFS	68
5.2.1) Création et configuration de l'espace de noms	68
5.2.2) Création d'un dossier cible	73
5.2.3) Vérification DFS	75
5.3) DFSR	76
5.3.1) Configuration du DFSR	76
5.3.2) Vérifications DFSR	80
5.4) Déduplication des données	81
5.4.1) Installation et paramétrage du service de déduplication des données	81
6) Montage d'une cible iSCSI avec TrueNAS Core	84
6.1) Installation de TrueNAS	84
6.2) Configuration de TrueNAS	87
6.3) Configuration d'une cible iSCSI	88
6.4) Connexion iSCSI depuis un Windows Serveur	92
6.5) Configurer les sauvegardes Windows Serveur	95
6.6) Configurer les Shadow copies	98

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.

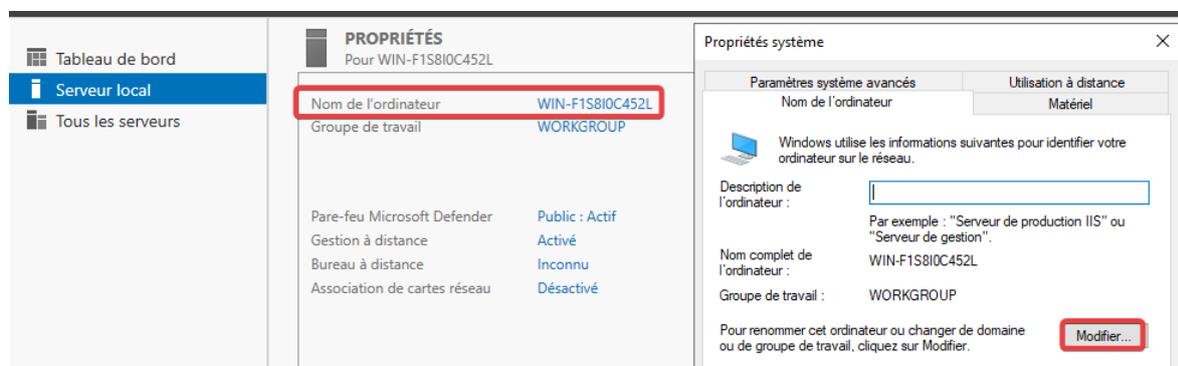
1.2) Pré configuration

Remarque : 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.

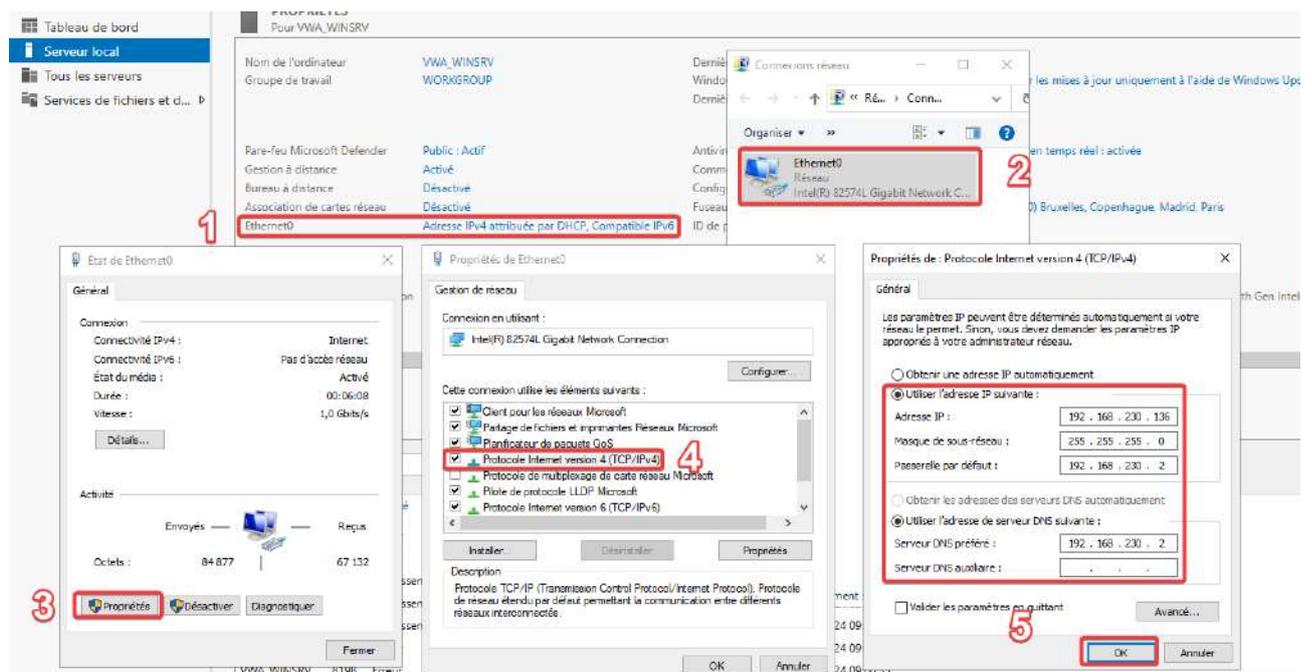


Gestionnaire de serveur > Serveur local > %Nom de l'ordinateur% > Nom de l'ordinateur > Modifier

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).

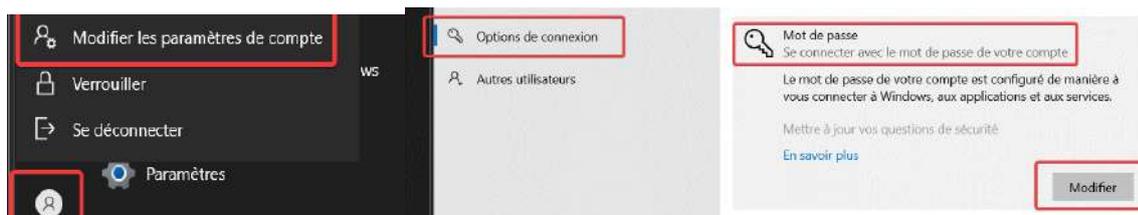


%Ethernet0% > %Ethernet0% > Propriétés > Protocole IPv4

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

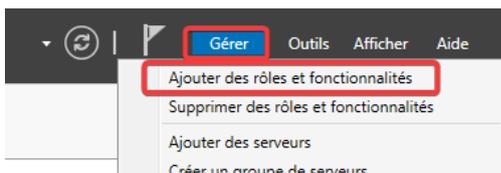
L'Active Directory (AD) est un service de répertoire développé par Microsoft, utilisé pour stocker des informations sur les ressources réseau, tels que les utilisateurs, les groupes, les ordinateurs, et les imprimantes, dans un environnement Windows. Il facilite l'organisation et la gestion des objets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

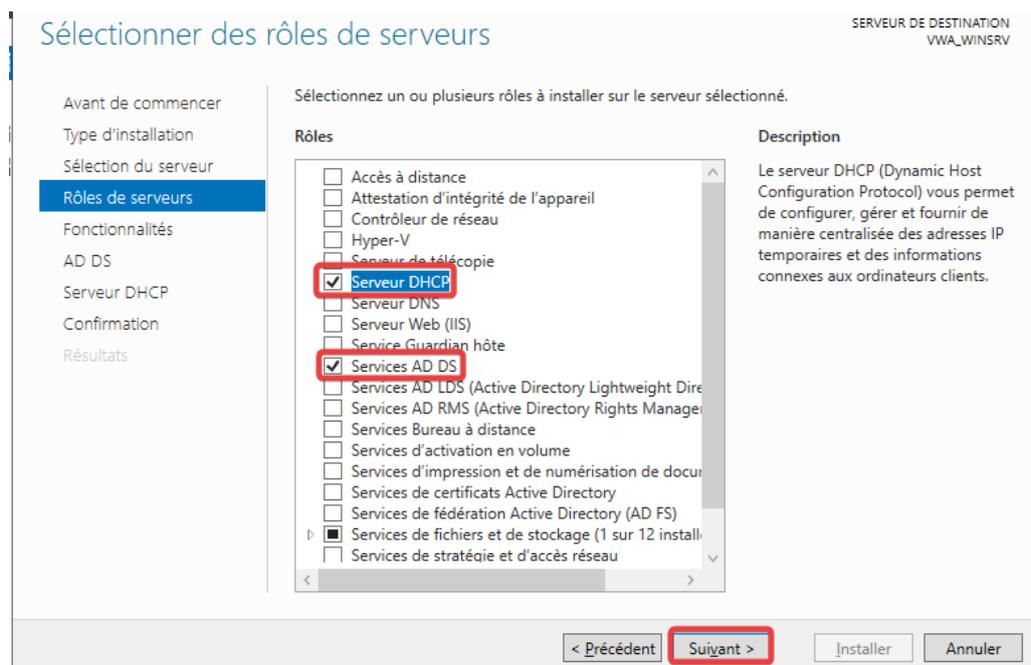
NB: L'Active Directory Domain Services (AD DS) regroupe un annuaire LDAP, un service DNS pour la gestion des domaines, et utilise le protocole Kerberos pour l'authentification des utilisateurs. Il n'est donc **pas nécessaire d'installer le rôle Serveur DNS** (cela peut même créer des conflits).

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.



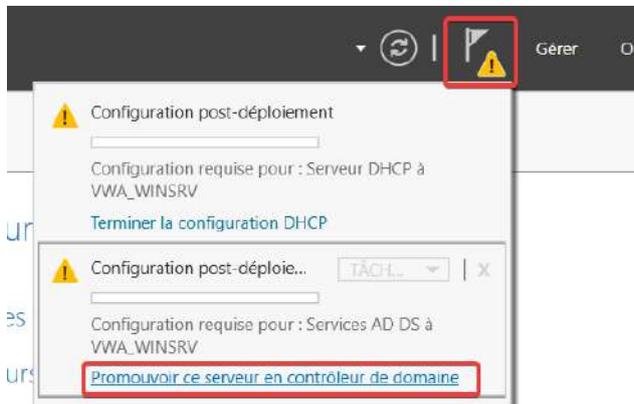
Pour le reste des onglets on peut laisser les paramètres par défaut et cliquer sur suivant et pour finir confirmer l'installation.

Redémarrer le serveur.

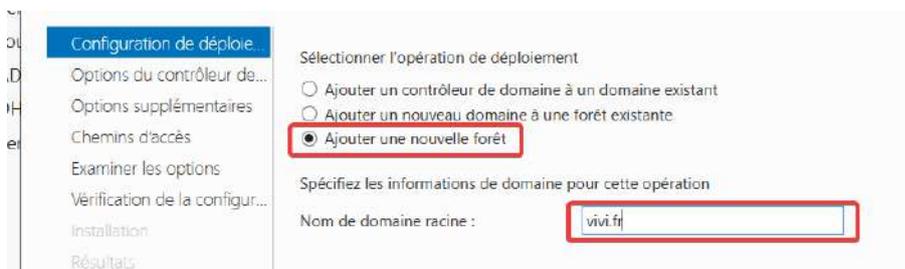
1.3.2) Configuration de l'AD DS

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.

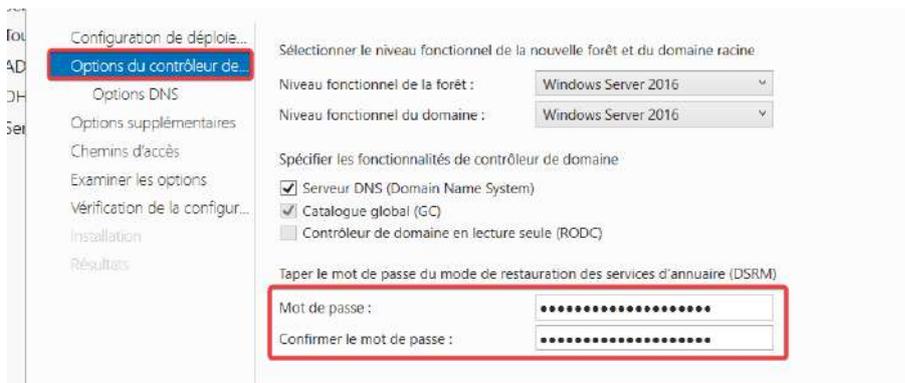
Pour commencer il faut cliquer sur le drapeau puis « Promouvoir ce serveur en contrôleur de domaine »



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 »)

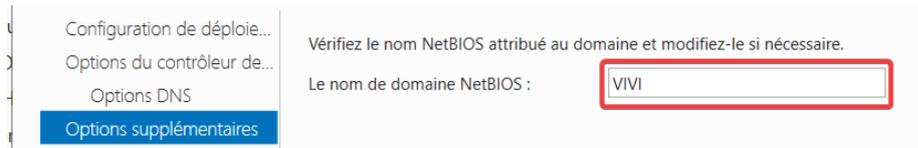


Puis on peut laisser les paramètres par défaut et mettre un mot de passe (Dans notre cas ce sera le même que celui de l'administrateur question de simplicité)



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.

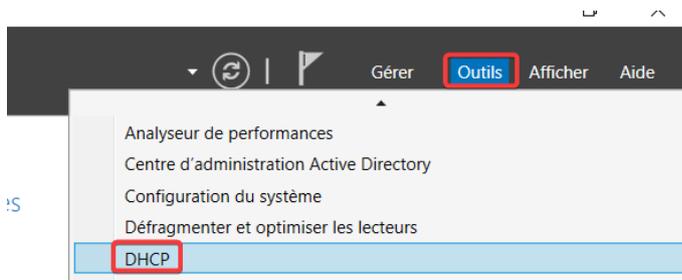
Pour se faire, cliquer sur le drapeau puis sur « Terminer la configuration DHCP » depuis le gestionnaire de serveur.



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.

Paramètres de configuration pour serveur DHCP

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

Adresse IP de début : 192 . 168 . 100 . 10

Adresse IP de fin : 192 . 168 . 100 . 50

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 24

Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

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

Jours : 0

Heures : 8

Minutes : 0

< Précédent Suivant > Annuler

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

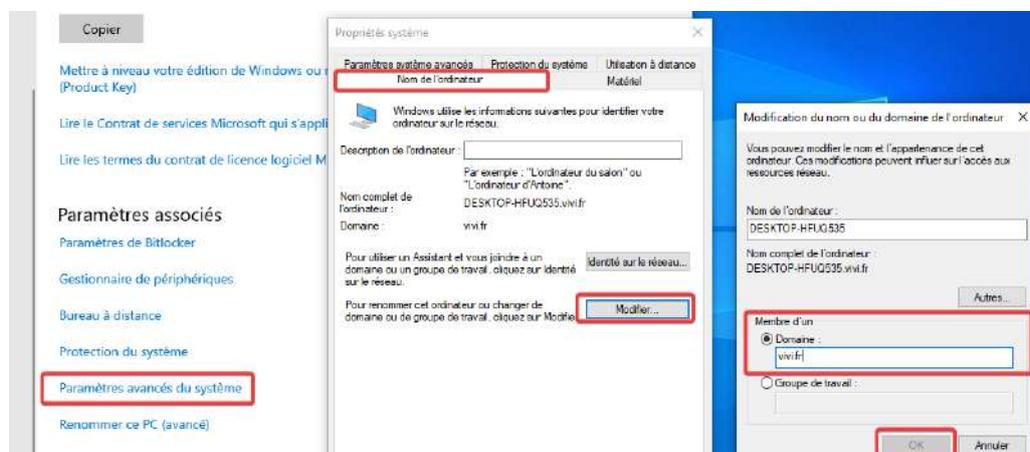
1.4) Exploiter le domaine

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

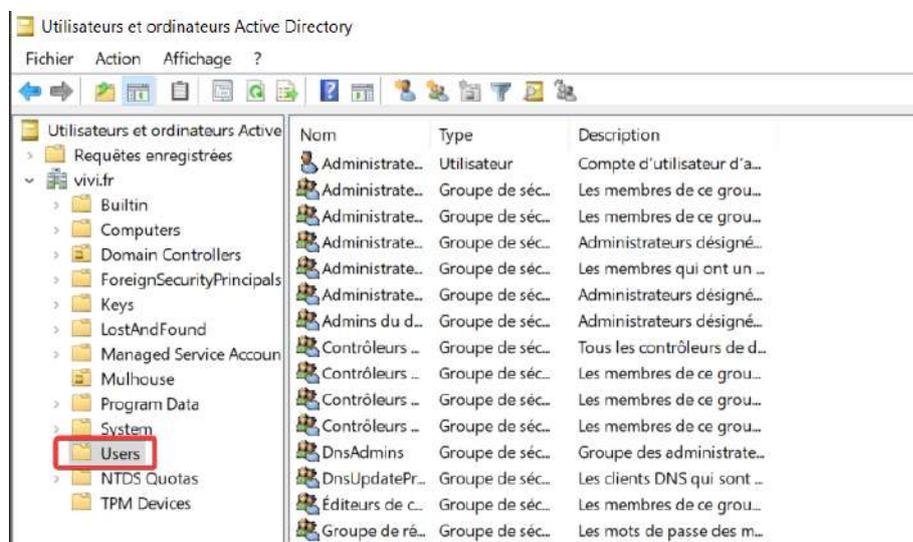
La mise en place d'utilisateurs et de groupes au sein de l'Active Directory est essentiel et renforce la gestion efficace des accès et des autorisations au sein de votre environnement informatique.

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.



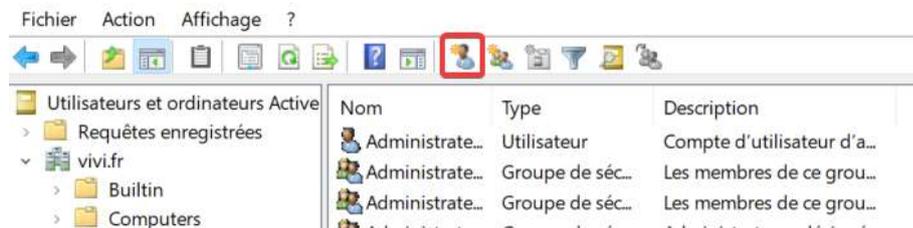
Dans la nouvelle fenêtre qui s'ouvre, vous pouvez développer votre domaine, dans notre cas « vivi.fr », puis on se positionner dans le dossier « Users ».



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

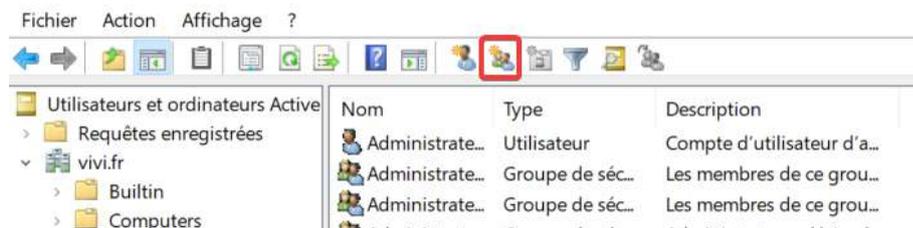
1.4.2 bis) Créer un utilisateur

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.



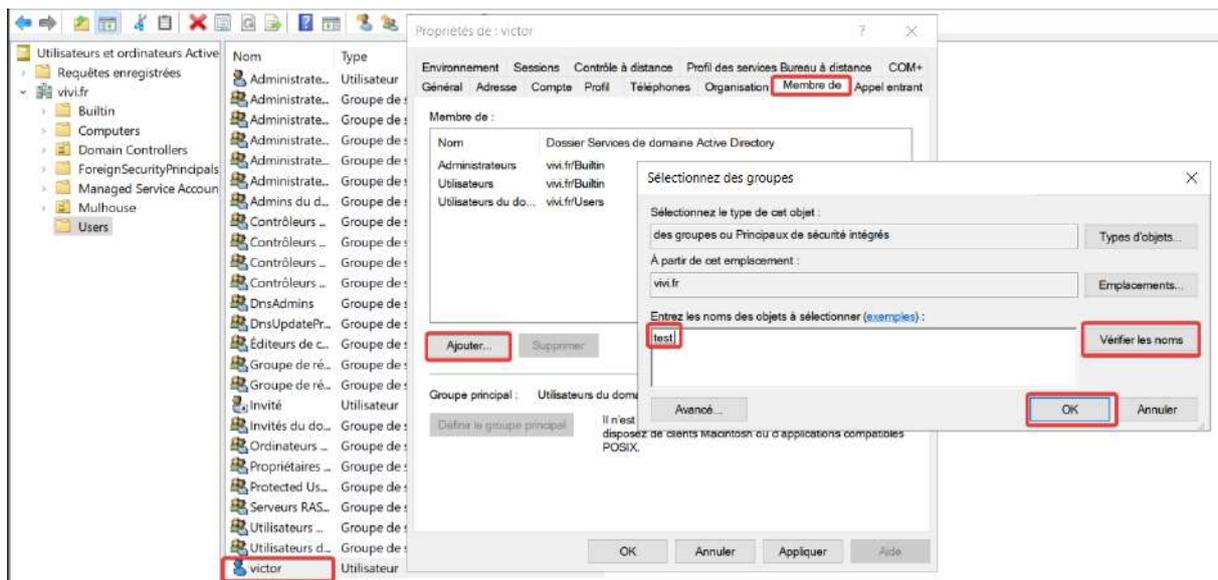
1.4.2 bis) Créer un groupe

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 utilisateur, 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.

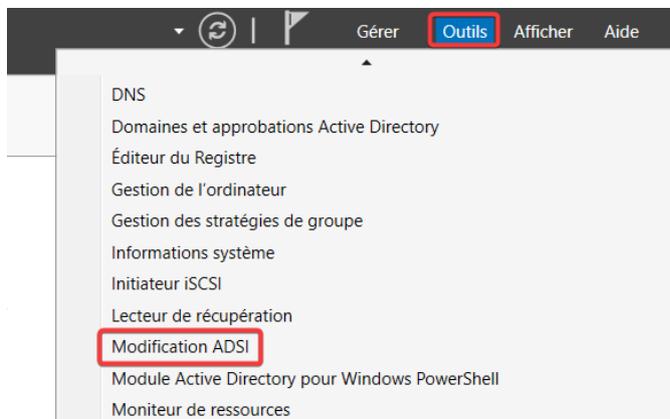


1.4.2 bis) Créer un conteneur

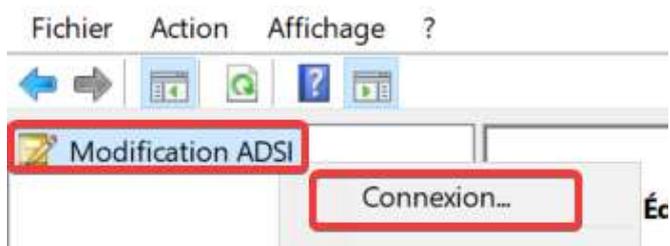
NB: Les conteneurs que nous nous apprêtons à créer sont seulement visible si l'option d'affichage des fonctionnalités avancées est activée.



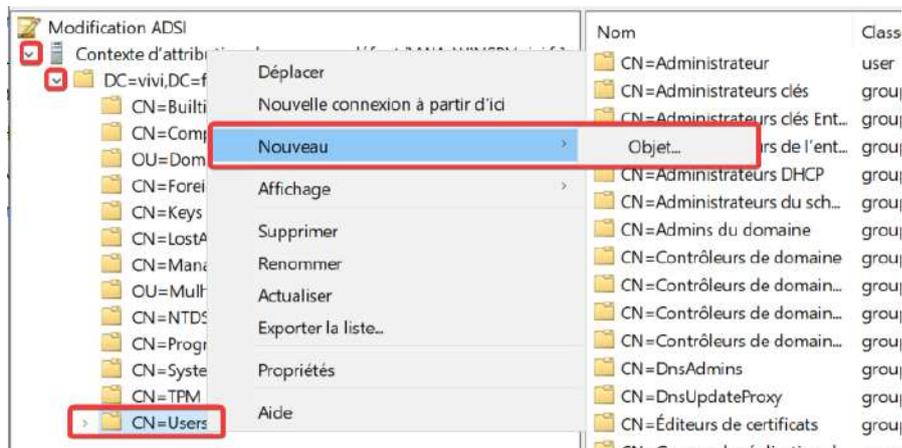
Pour créer un conteneur, il faut se rendre dans « Outils » puis « Modification ADSI »



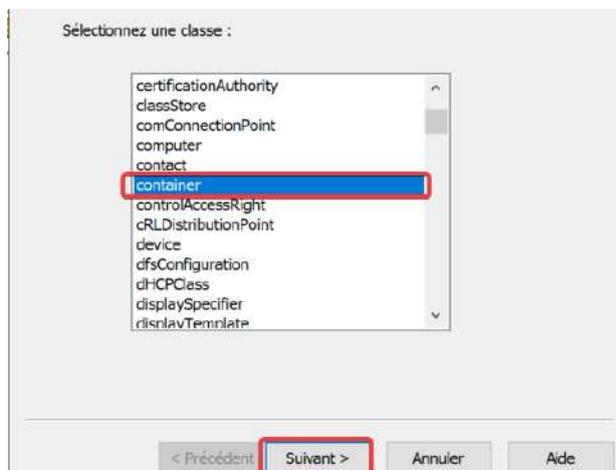
Dans la nouvelle fenêtre qui s'ouvre il faut faire clic droit sur « Modification ADSI » puis « Connexion », ensuite on laisse les paramètres par défaut et on clique sur « Ok »



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 chercher l'objet « Container », puis il ne vous reste plus qu'à appuyer sur suivant et le créer.



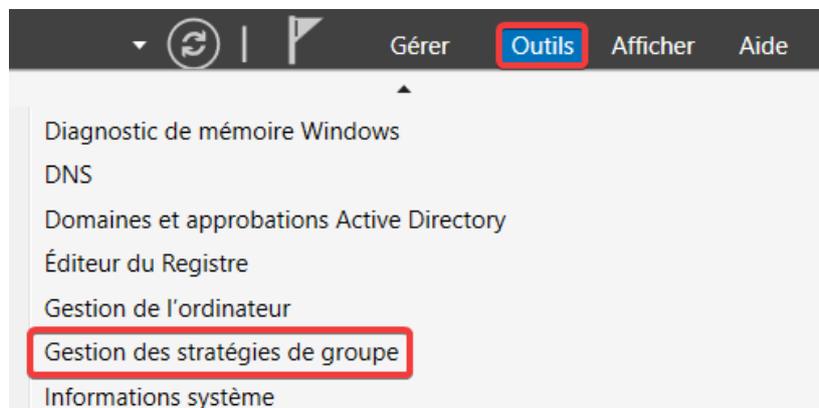
1.4.3) Modifier une GPO

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.

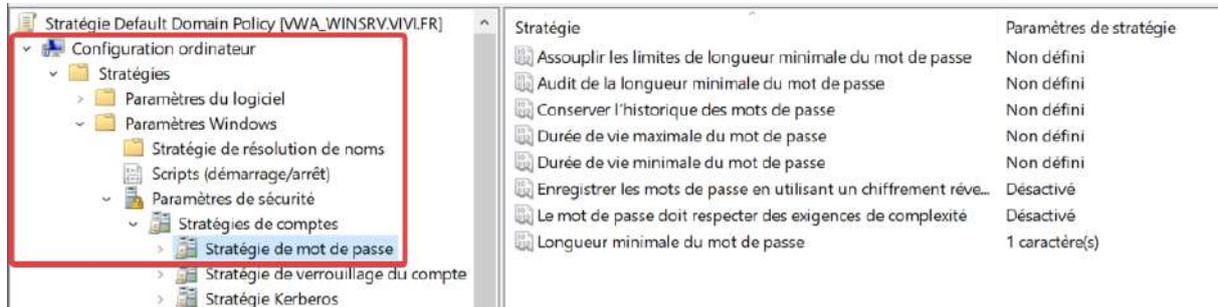
Pour accéder aux GPO, il faut cliquer sur « Outils » puis dans « Gestion des stratégies de groupe » depuis le gestionnaire de serveur.



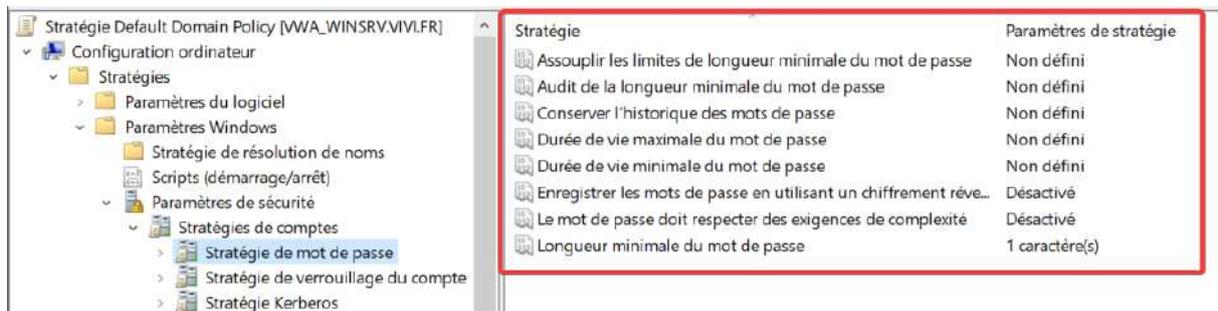
Puis dans la nouvelle fenêtre qui s'ouvre il faut développer la forêt puis « Domaines » puis votre domaine, dans notre cas « vivi.fr ». Ensuite, vous pouvez faire un clic droit sur « Default Domain Policy » enfin cliquer sur « Modifier ».



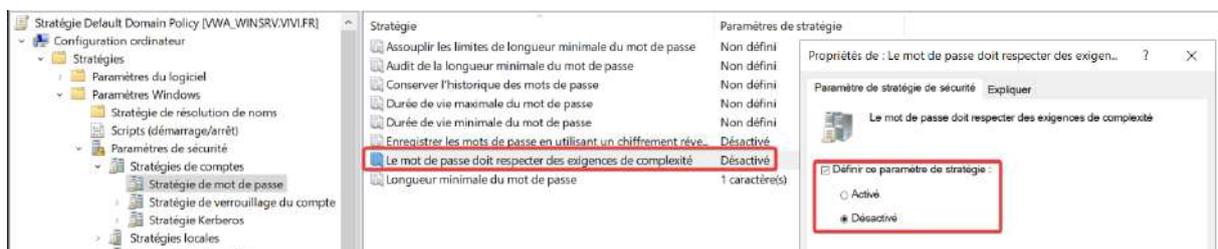
Dans la nouvelle fenêtre il faut développer « Configuration ordinateur », ensuite « Stratégies », puis « Paramètres Windows » et enfin « Paramètres de sécurité ». La stratégie qui nous intéresse dans notre cas est « Stratégie de mot de passe ».



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 configurés dans le DHCP du serveur (dans notre cas l'IP de ce même serveur).

```
Configuration IP de Windows

Nom de l'hôte . . . . . : DESKTOP-HFUQ535
Suffixe DNS principal . . . . . : vivi.fr
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: vivi.fr

Carte Ethernet Ethernet0 :

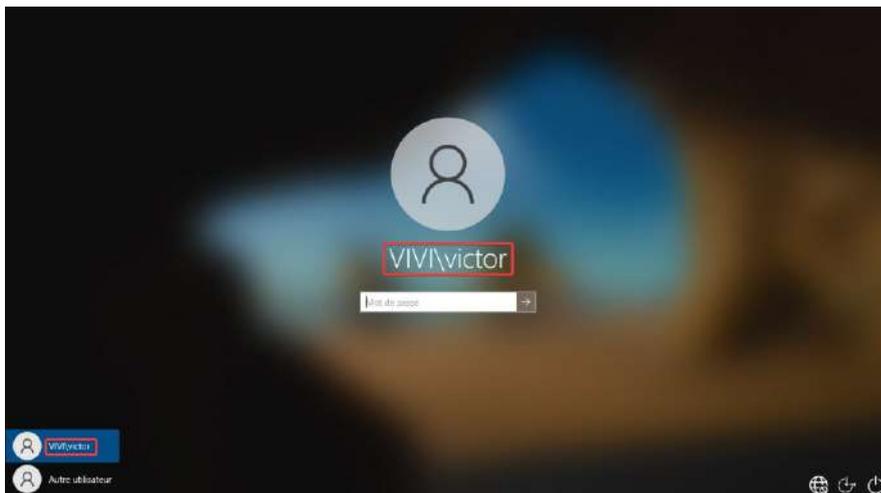
Suffixe DNS propre à la connexion. . . : vivi.fr
Description. . . . . : Intel(R) 82574L Gigabit Network Connection
Adresse physique . . . . . : 00-0C-29-C7-13-58
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::4539:9b50:b556:36a1%5(préféré)
Adresse IPv4. . . . . : 192.168.100.10(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mardi 23 janvier 2024 13:14:49
Bail expirant. . . . . : mardi 23 janvier 2024 21:14:48
Passerelle par défaut :
Serveur DHCP . . . . . : 192.168.100.1
IAID DHCPv6 . . . . . : 100666409
DUID de client DHCPv6 . . . . . : 00-01-00-01-20-41-58-50-00-00-29-C7-13-58
Serveurs DNS. . . . . : 192.168.100.1
NetBIOS sur Tcpip. . . . . : Active
```

Nom de la forêt

IP Serveur

1.4.4 bis) Par interface graphique

Au moment de la connexion à 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.

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

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. . . . : vivi.fr
    Adresse IPv6 de liaison locale. . . . . : fe80::4539:9b50:b556:36a1%5
    Adresse IPv4. . . . . : 192.168.100.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

On peut voir que le bail a bien été renouvelé avec à 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(préfééré)
    Adresse IPv4. . . . . : 192.168.100.10(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 25 janvier 2024 14:12:26
    Bail expirant. . . . . : jeudi 25 janvier 2024 22:12:26
    Passerelle par défaut. . . . . :
    Serveur DHCP . . . . . : 192.168.100.1
```

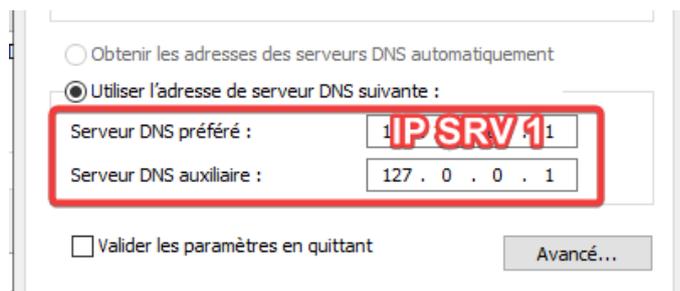
1.5) Redondance

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 :



The screenshot shows the 'Configurer les paramètres de connexion réseau' dialog box in Windows. The 'Obtenir les adresses des serveurs DNS automatiquement' option is unselected, and 'Utiliser l'adresse de serveur DNS suivante' is selected. The 'Serveur DNS préféré' field is highlighted with a red box and contains the text '1IPSRV11'. The 'Serveur DNS auxiliaire' field contains '127.0.0.1'. At the bottom, there is a checkbox for 'Valider les paramètres en quittant' and an 'Avancé...' button.

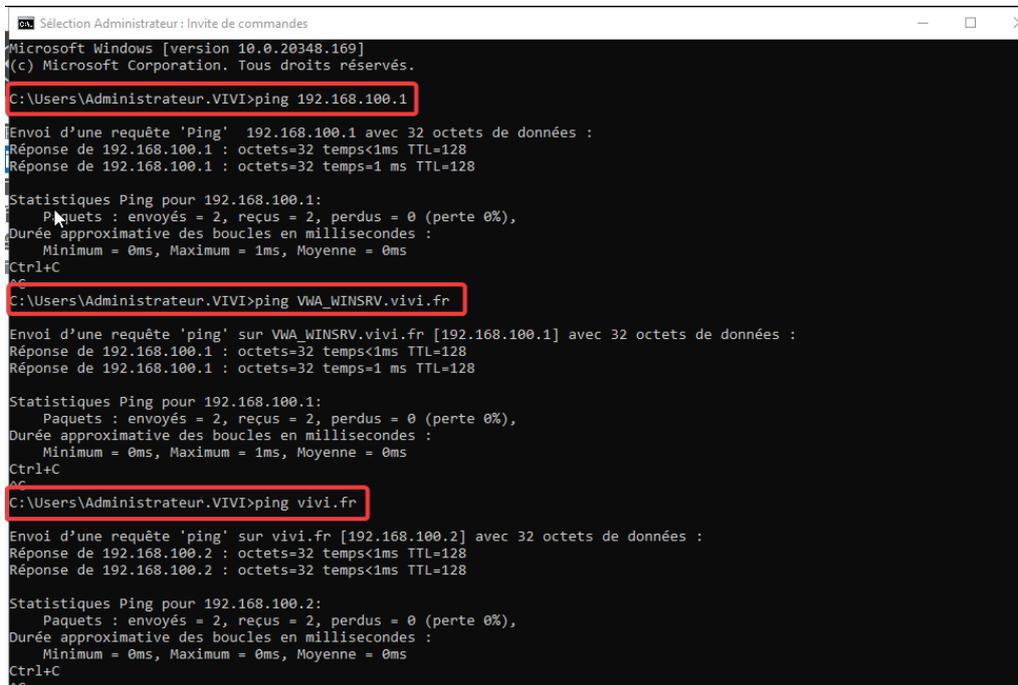
Il faut mettre en Serveur DNS préféré l'adresse IP du premier serveur que l'on a configuré. Et dans DNS auxiliaire il est nécessaire de mettre l'adresse de boucle (127.0.0.1) donc lui-même.

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)



```
Sélection Administrateur: Invite de commandes
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.VIVI>ping 192.168.100.1

Envoi d'une requête 'Ping' 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

Statistiques Ping pour 192.168.100.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
Ctrl+C
^C

C:\Users\Administrateur.VIVI>ping VWA_WINSRV.vivi.fr

Envoi d'une requête 'ping' sur VWA_WINSRV.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

Statistiques Ping pour 192.168.100.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
Ctrl+C
^C

C:\Users\Administrateur.VIVI>ping vivi.fr

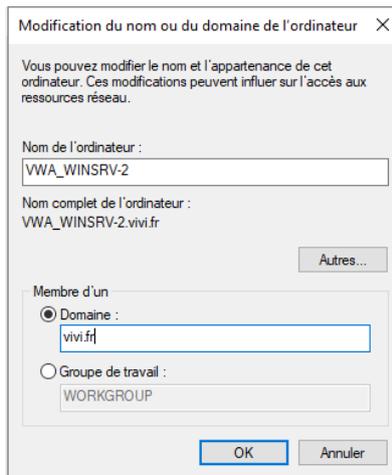
Envoi d'une requête 'ping' sur vivi.fr [192.168.100.2] avec 32 octets de données :
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.100.2:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
```

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 :



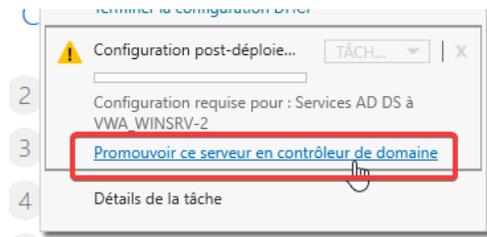
Puis redémarrer le serveur.

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

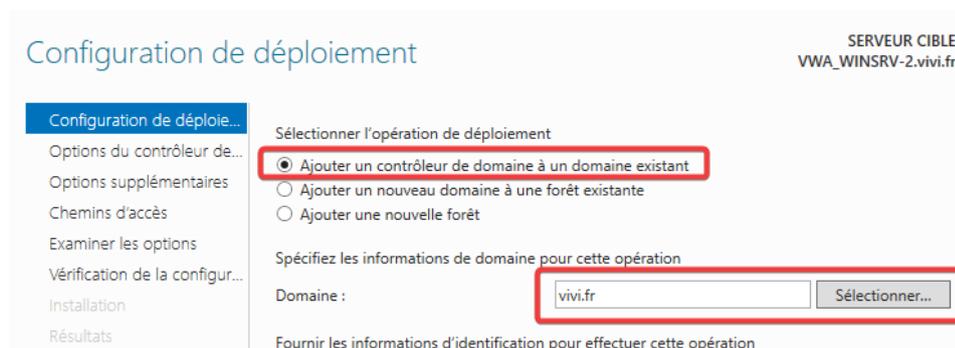
Enfin, il faut ajouter le rôle AD DS et DHCP sur le nouveau serveur.

1.5.3) Configuration des rôles

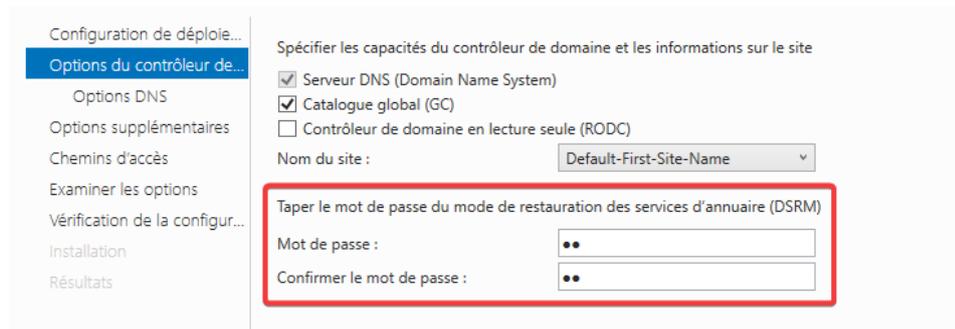
Tout d'abord depuis le gestionnaire de serveur, il faut cliquer sur le petit drapeau, puis sur promouvoir ce serveur en contrôleur de domaine.



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 :



END USER LICENSE AGREEMENT (EULA)

END USER LICENSE AGREEMENT (EULA) FOR PROXMOX VIRTUAL ENVIRONMENT (PROXMOX VE)

By using Proxmox VE software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintenance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox VE and any related update, source code and structure (the Programs), regardless of the delivery mechanism.

1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain obligations in some cases), both in source code and binary code forms, with the exception of certain binary only firmware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only firmware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.
2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.
3. Limitation of Liability. To the maximum extent permitted under applicable law, under no

Previous I agree

On choisit le disque d'installation :

Proxmox Virtual Environment (PVE)

The Proxmox Installer automatically partitions your hard disk. It installs all required packages and makes the system bootable from the hard disk. All existing partitions and data will be lost.

Press the Next button to continue the installation.

- **Please verify the installation target**
The displayed hard disk will be used for the installation.
Warning: All existing partitions and data will be lost.
- **Automatic hardware detection**
The installer automatically configures your hardware.
- **Graphical user interface**
Final configuration will be done on the graphical user interface, via a web browser.

Target Harddisk: /dev/sda (60.00GiB, VMware Virtual S) Options

Previous Next

Puis, la région ainsi que la disposition du clavier :

Location and Time Zone selection

The Proxmox Installer automatically makes location-based optimizations, like choosing the nearest mirror to download files from. Also make sure to select the correct time zone and keyboard layout.

Press the Next button to continue the installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speed up downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.

choose your keyboard

Country: France

Time zone: Europe/Paris

Keyboard Layout: French

Previous Next

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



Administration Password and Email Address

Proxmox Virtual Environment is a full featured, highly secure GNU/Linux system, based on Debian.

In this step, please provide the *root* password.

- **Password:** Please use a strong password. It should be at least 8 characters long, and contain a combination of letters, numbers, and symbols.
- **Email:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the **Next** button to continue the installation.

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



Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installing.

After you have finished, press the **Next** button. You will be shown a list of the options that you chose during the previous steps.

- **IP address (CIDR):** Set the main IP address and netmask for your server in CIDR notation.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Il est temps de cliquer sur installer :



Summary

Please confirm the displayed information. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

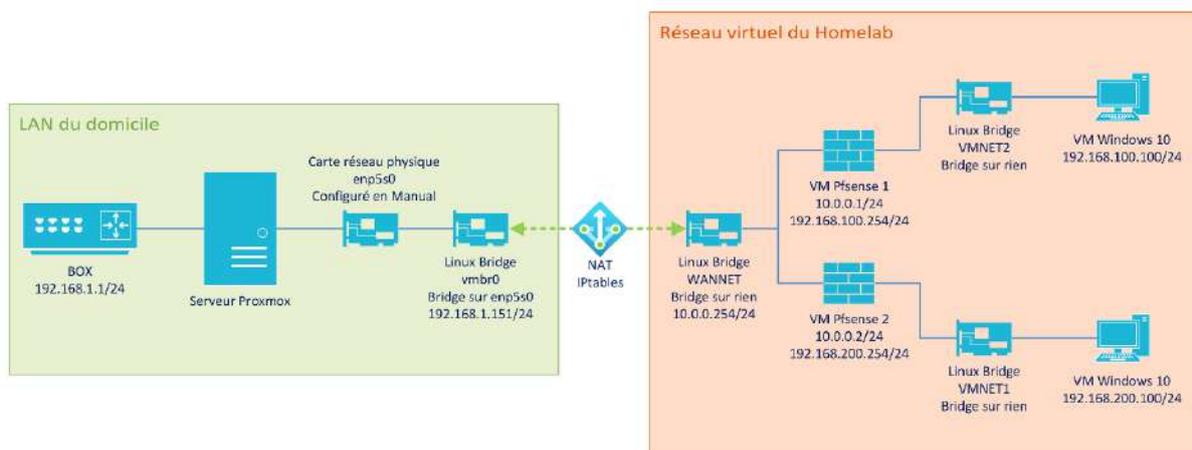
Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	France
Timezone:	Europe/Paris
Keymap:	fr
Email:	vic.wrt@gmail.com
Management interface:	ens33
Hostname:	proxmox
IP CIDR:	192.168.67.143/24
Gateway:	192.168.67.2
DNS:	192.168.67.2



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 vbr0
iface vbr0 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 vubr0
iface vubr0 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 connexions 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 règles 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
```

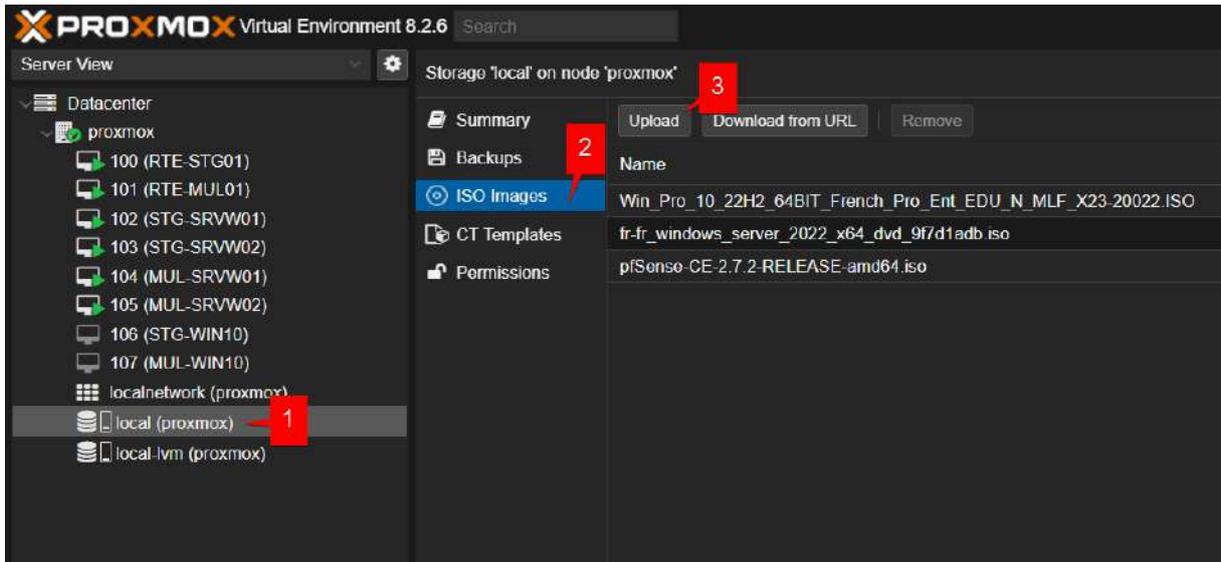
Nos VM connectées à l'interface virtuelle WANNET ont accès à Internet en passant par la passerelle 10.0.0.254/24 et possèdent une plage d'adresse pour elles (10.0.0.0/24), cela pourrait permettre de simuler un "WAN" par exemple.

2.4) Ajouter des ISO et créer sa première VM

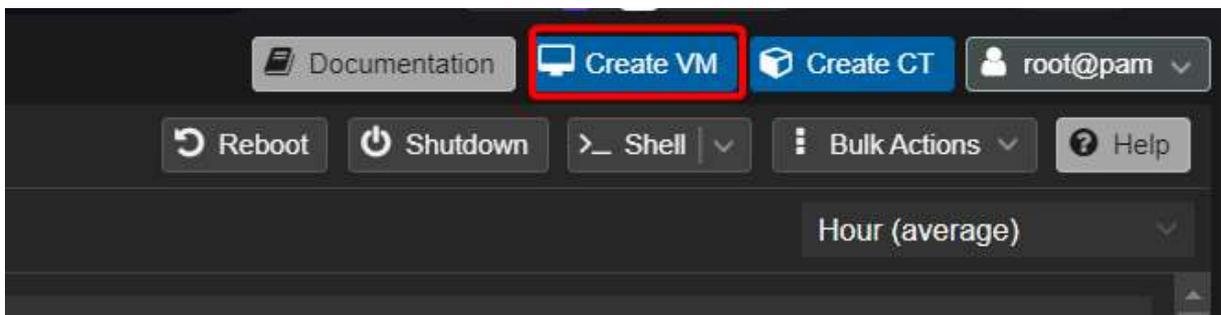
Proxmox prévoit un emplacement spécifique pour les ISO (dans le /var/lib/vz/template/iso) afin de les centraliser.

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

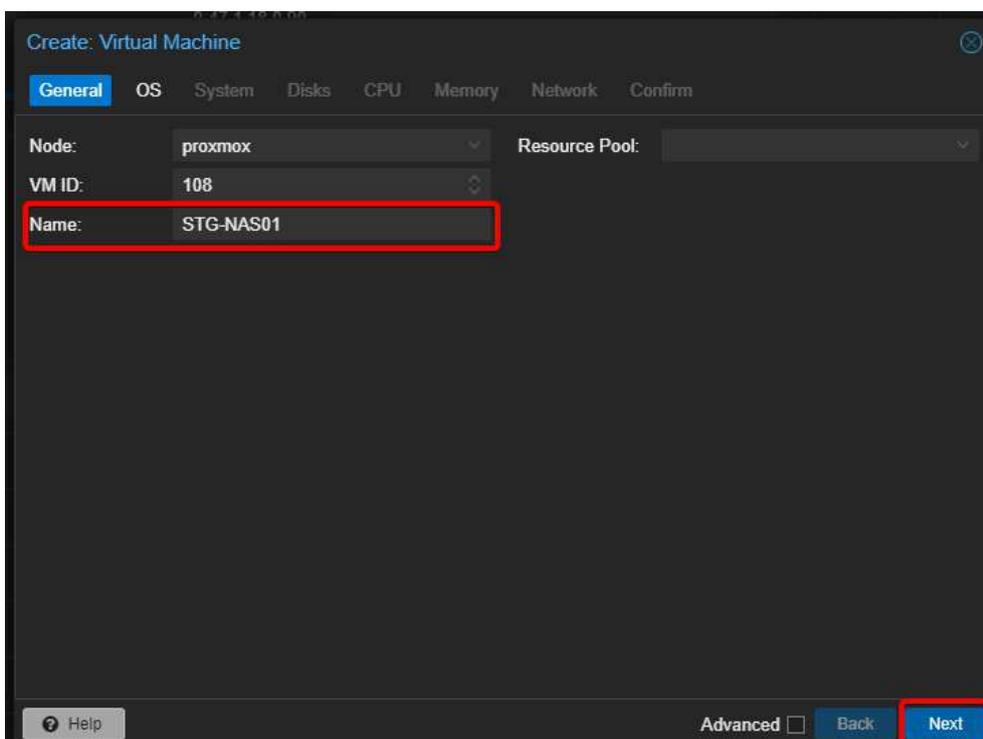
Puis développer le Datacenter et le noeud proxmox, cliquer sur votre stockage local (1), puis ISO Images (2) et enfin Upload (3) :



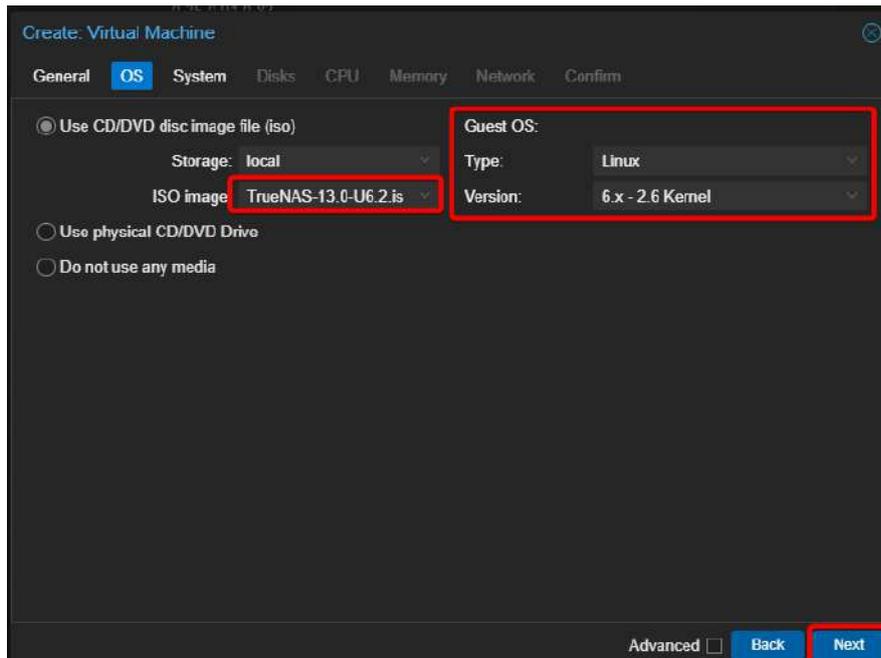
Pour créer votre première VM, nous allons cliquer sur "Create VM" en haut à droite :



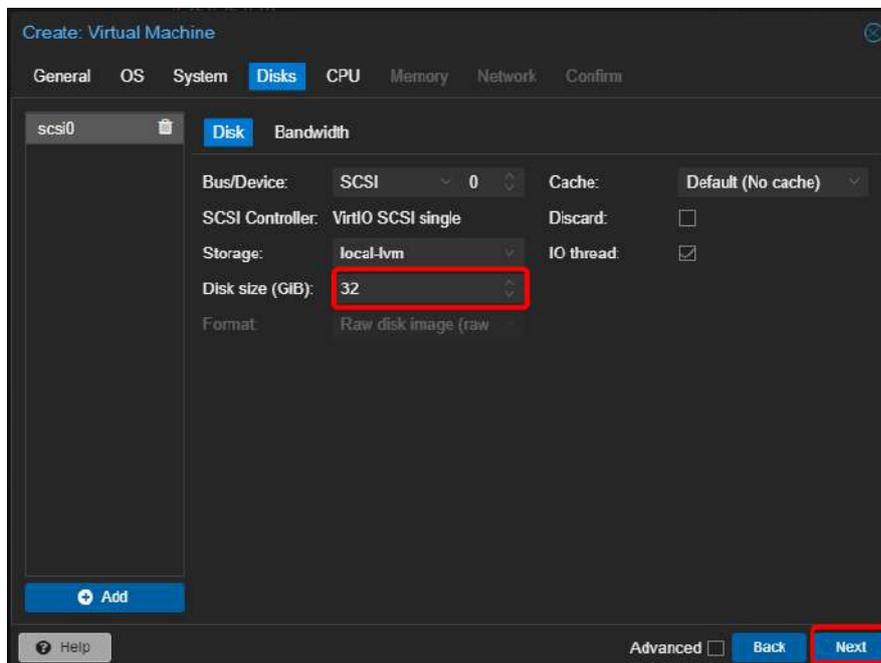
Ensuite, nous allons lui donner un nom, je laisse l'ID par défaut et vérifie qu'elle soit bien dans le nœud proxmox :



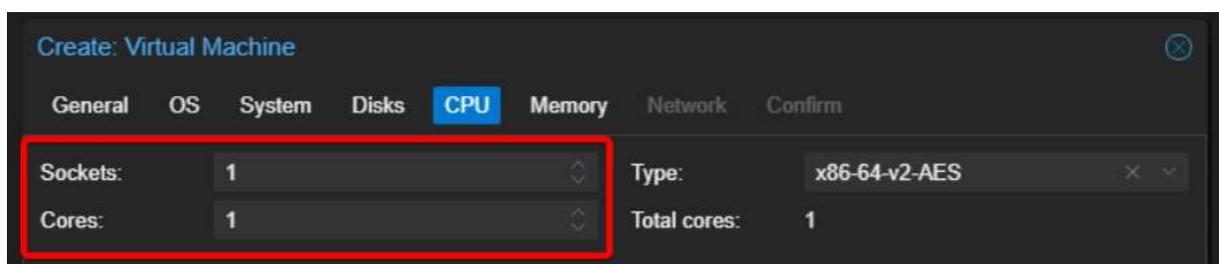
Après je sélectionne l'ISO et l'OS souhaitée :



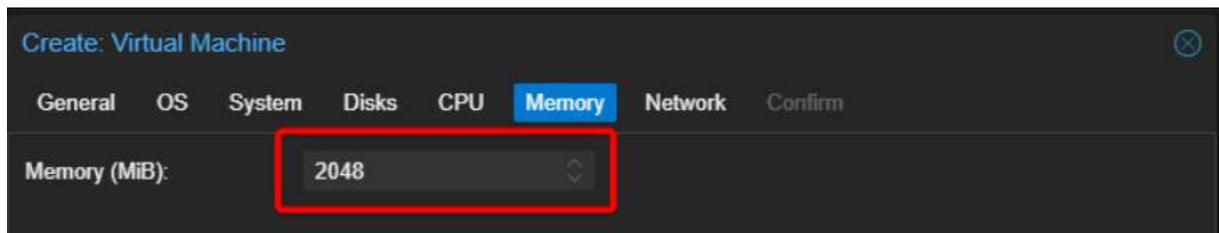
Ensuite, on peut laisser par défaut la partie System, puis on crée un disque virtuel :



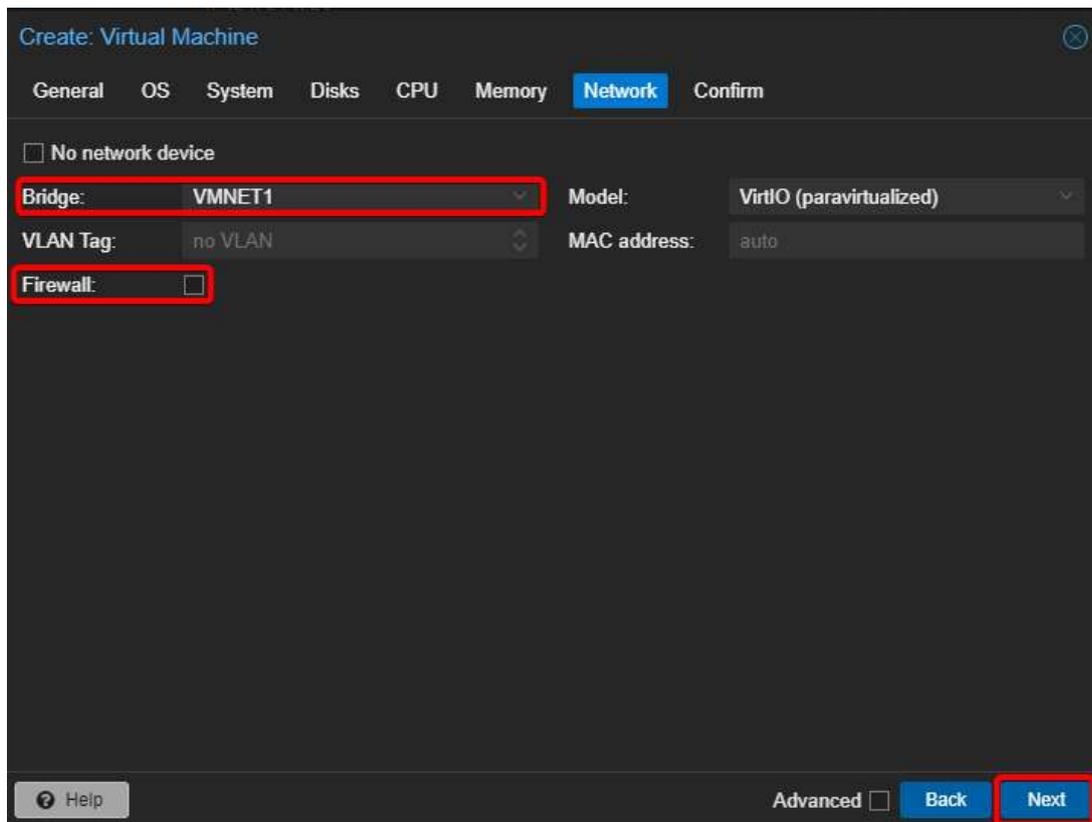
J'attribue le nombre de CPU :



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 :

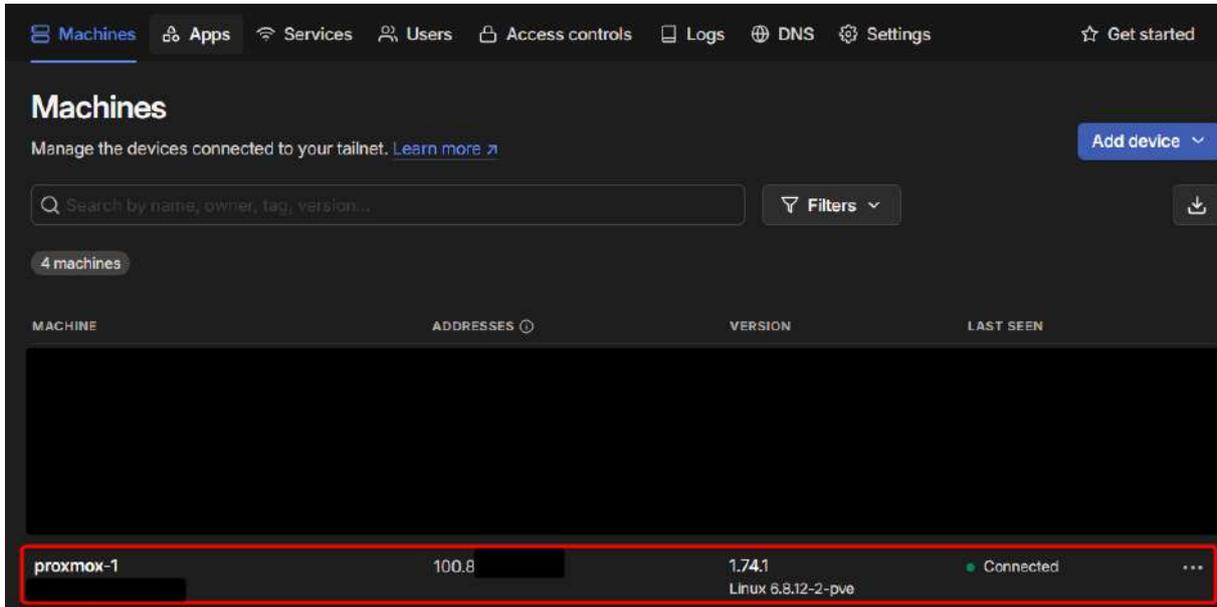
```
# se connecter en SSH
ssh root@IP_PROXMOX

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

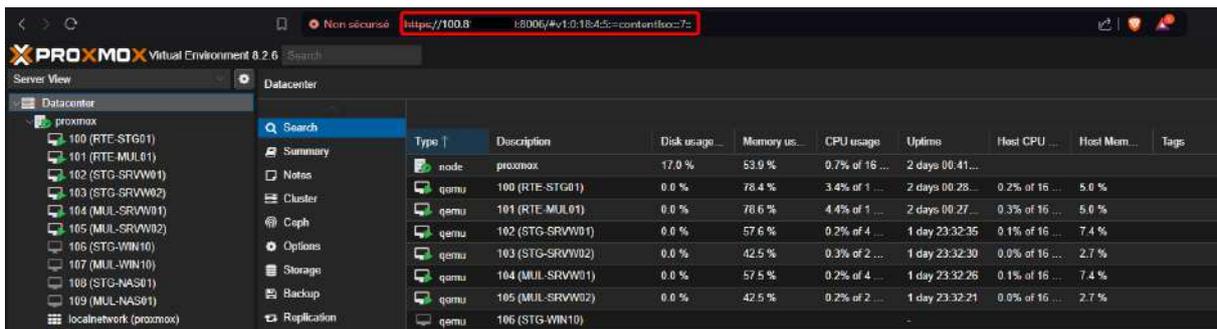
```
# lancer le login  
tailscale up
```

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 :



MACHINE	ADDRESSES	VERSION	LAST SEEN
proxmox-1	100.8	1.74.1 Linux 6.8.12-2-pve	Connected

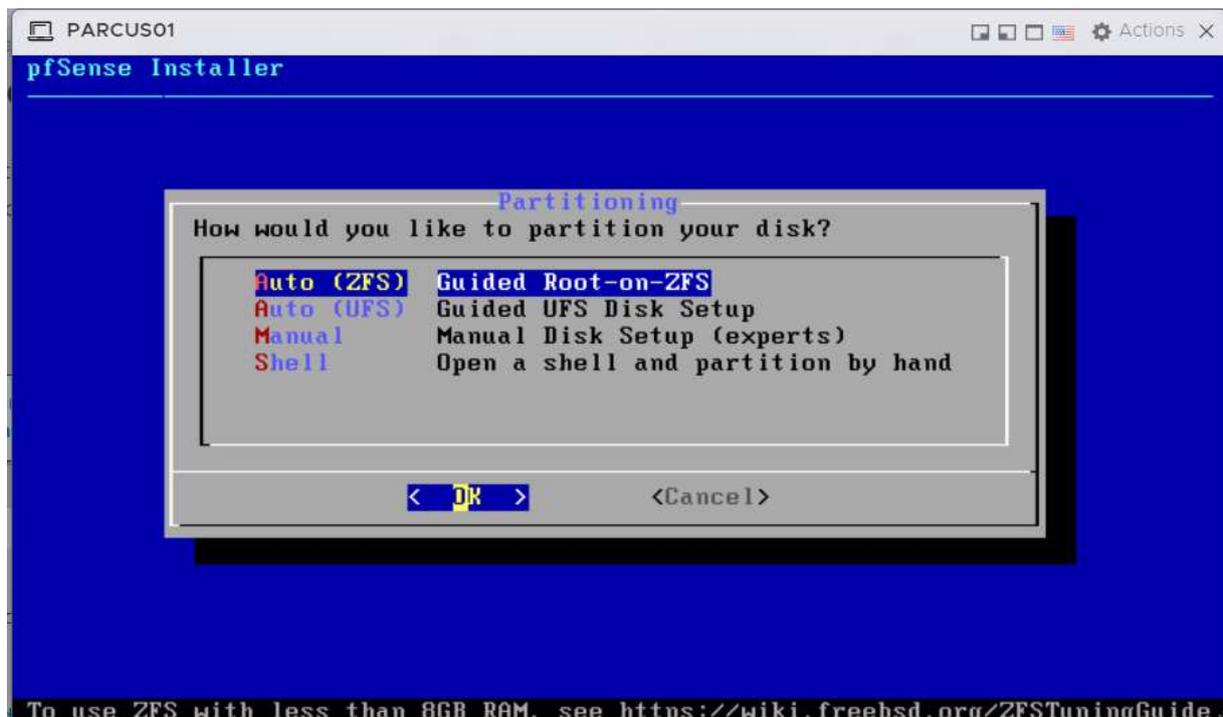
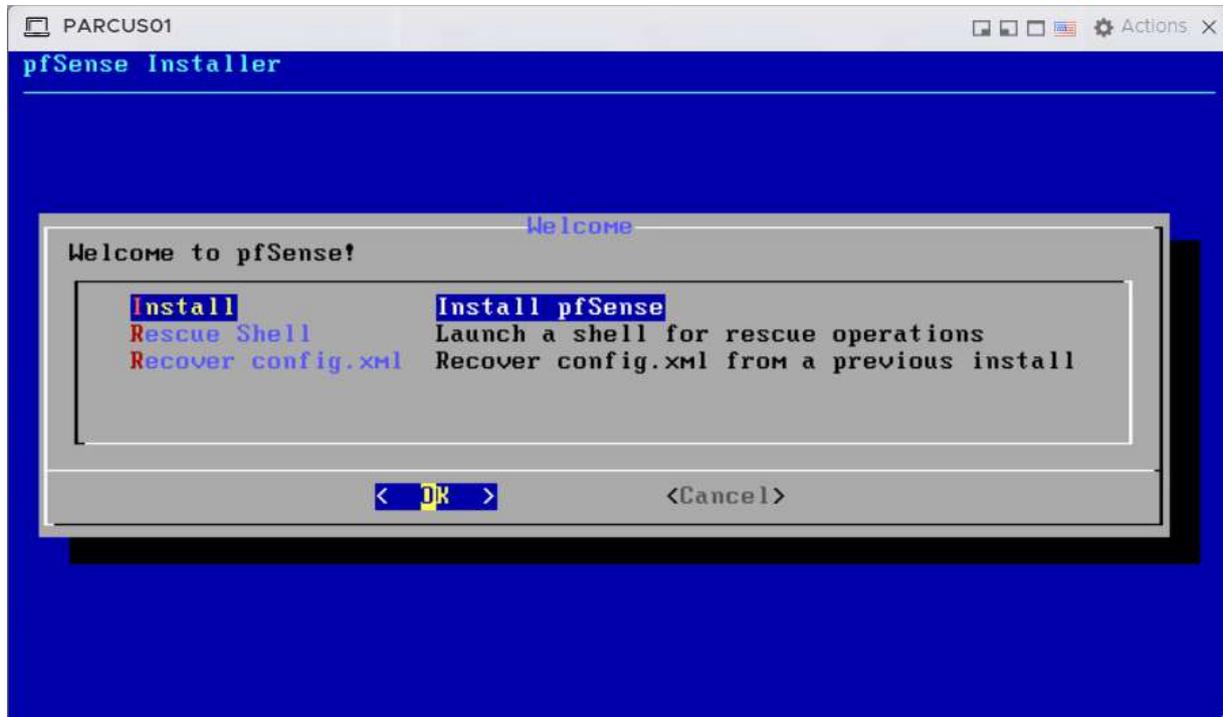


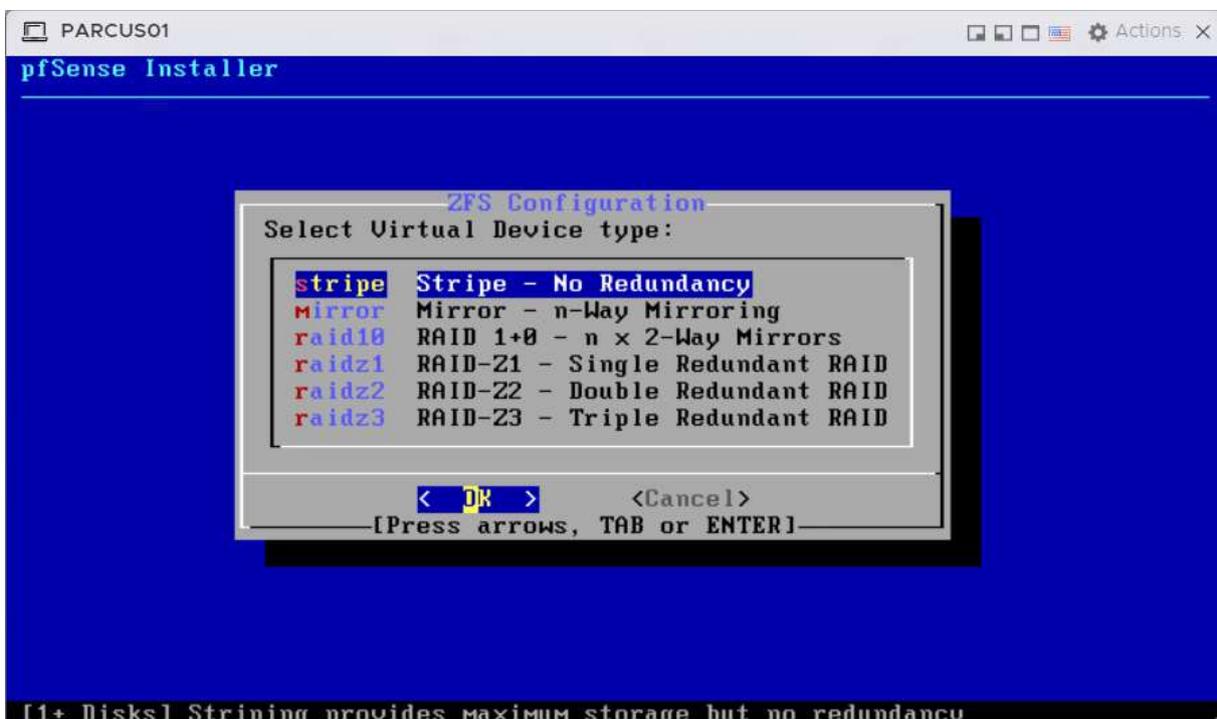
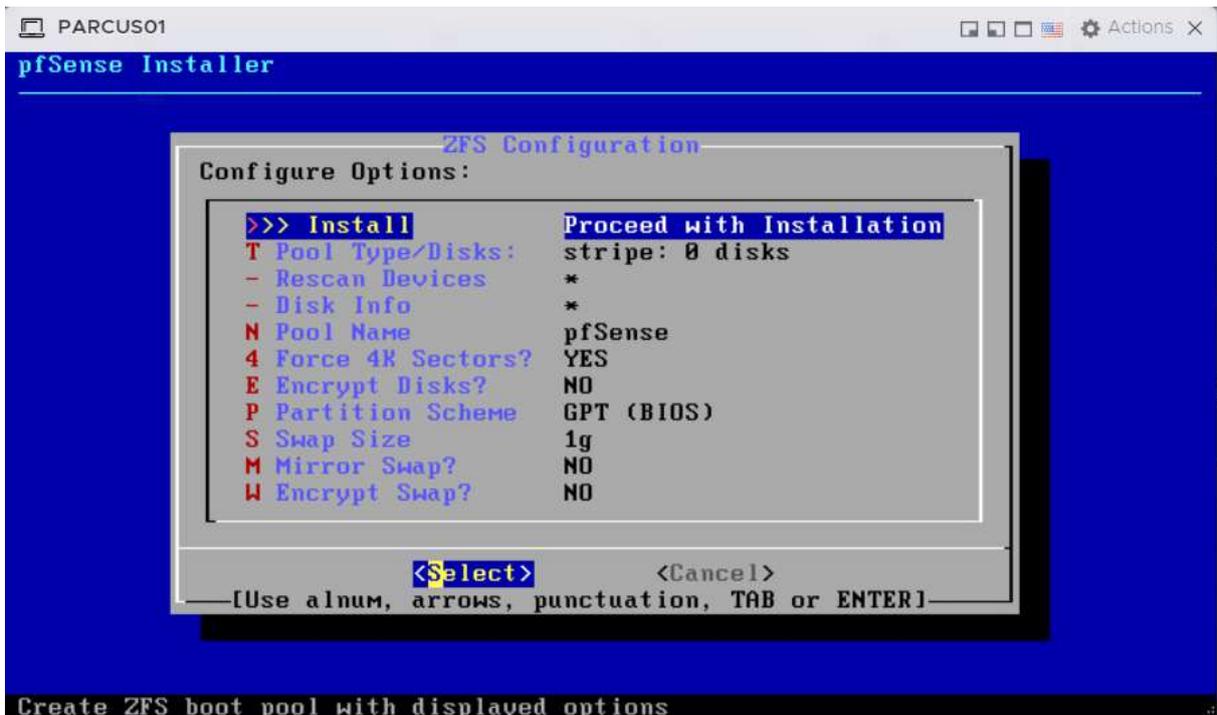
Type	Description	Disk usage	Memory us...	CPU usage	Uptime	Host CPU	Host Mem...	Tags
node	proxmox	17.0 %	53.9 %	0.7% of 16 ...	2 days 00:41...			
qemu	100 (RTE-STG01)	0.0 %	78.4 %	3.4% of 1 ...	2 days 00:28...	0.2% of 16 ...	5.0 %	
qemu	101 (RTE-MUL01)	0.0 %	78.6 %	4.4% of 1 ...	2 days 00:27...	0.3% of 16 ...	5.0 %	
qemu	102 (STG-SRVW01)	0.0 %	57.6 %	0.2% of 4 ...	1 day 23:32:35	0.1% of 16 ...	7.4 %	
qemu	103 (STG-SRVW02)	0.0 %	42.5 %	0.3% of 2 ...	1 day 23:32:30	0.0% of 16 ...	2.7 %	
qemu	104 (MUL-SRVW01)	0.0 %	57.5 %	0.2% of 4 ...	1 day 23:32:26	0.1% of 16 ...	7.4 %	
qemu	105 (MUL-SRVW02)	0.0 %	42.5 %	0.2% of 2 ...	1 day 23:32:21	0.0% of 16 ...	2.7 %	
qemu	106 (STG-WIN10)							

3) Installation et configuration de Pfsense

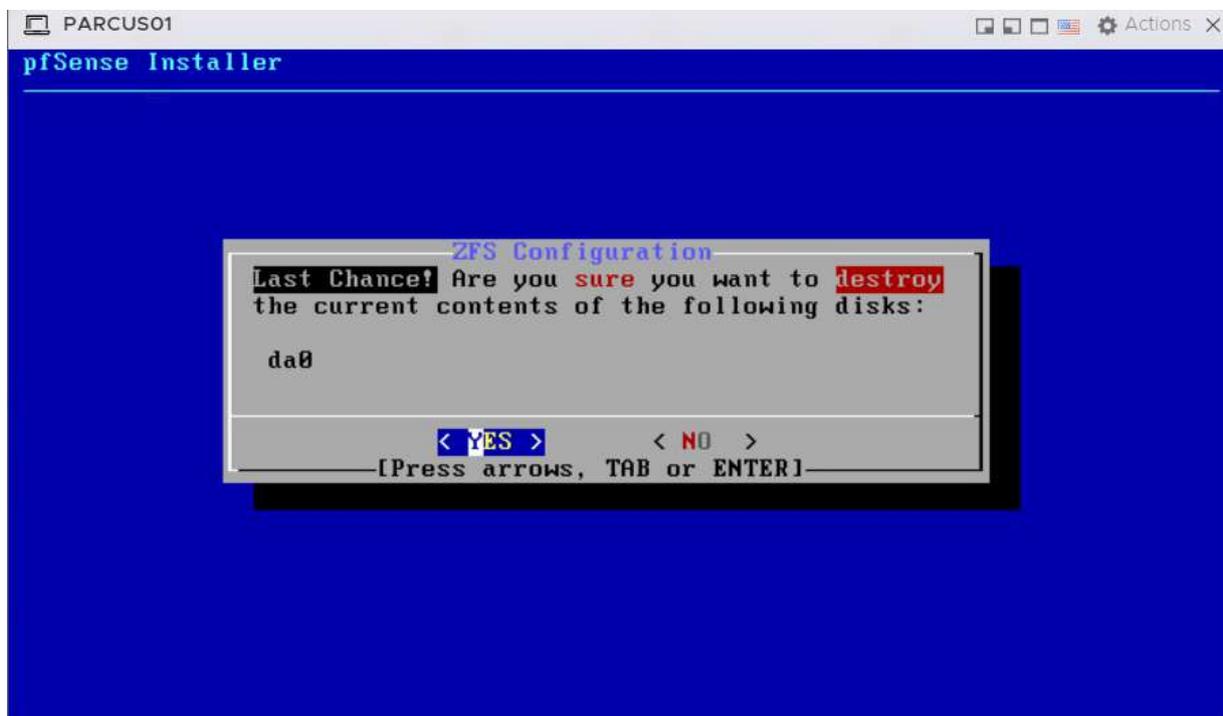
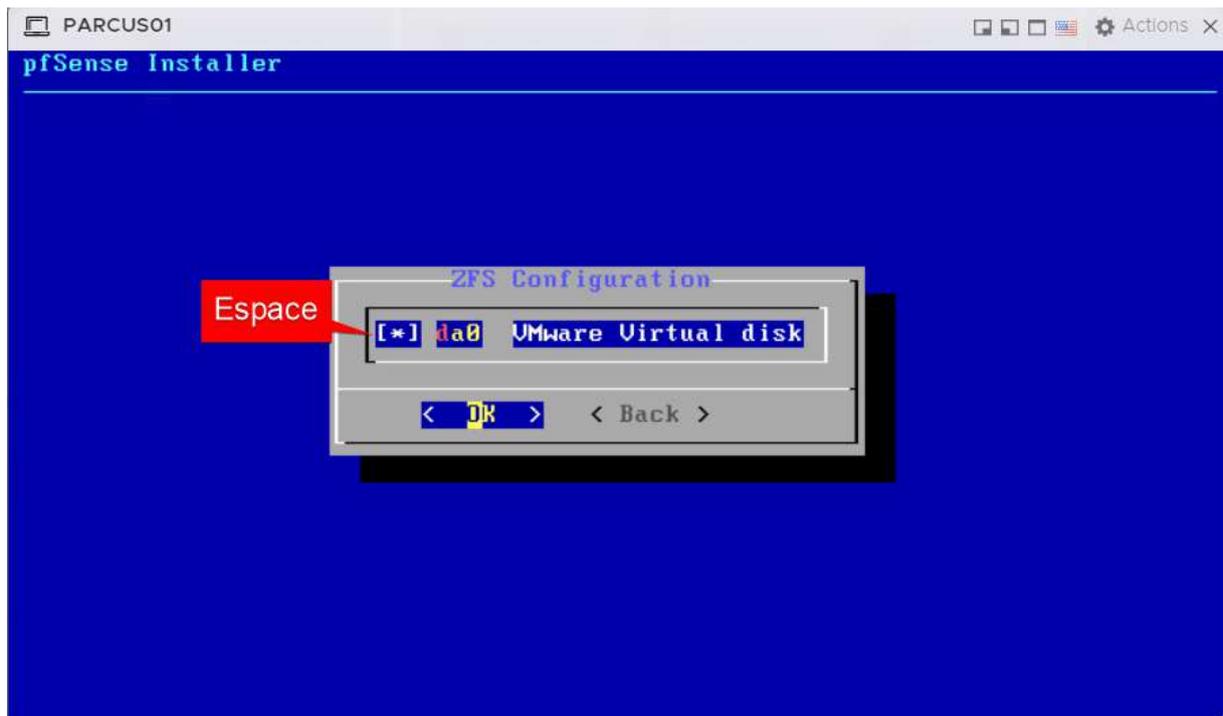
3.1) Installation de Pfsense

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





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 interfaces réseaux :

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> vtnet0      ->
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

Puis, on sélectionne l'interface WAN :

```
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 1
```

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

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.0.254

Should this gateway be set as the default gateway? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n
```

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

```
Enter the new WAN IPv6 address. Press <ENTER> for none
>

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

On configure ensuite l'interface LAN :

```
Available interfaces:
1 - WAN (vtnet0 - static)
2 - LAN (vtnet1 - static)
Enter the number of the interface you wish to configure: 2
```

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

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none
> 
```

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

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

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 :

General Information

On this screen the general pfSense parameters will be set.

Hostname RTE-MUL01
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain cci-campus.lan
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server 192.168.200.1
Secondary DNS Server 192.168.200.2

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

On sélectionne notre timezone, puis Next :

Time Server Information

Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone Europe/Paris

Next

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

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

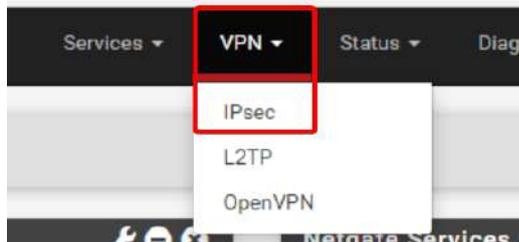
Admin Password

Admin Password AGAIN

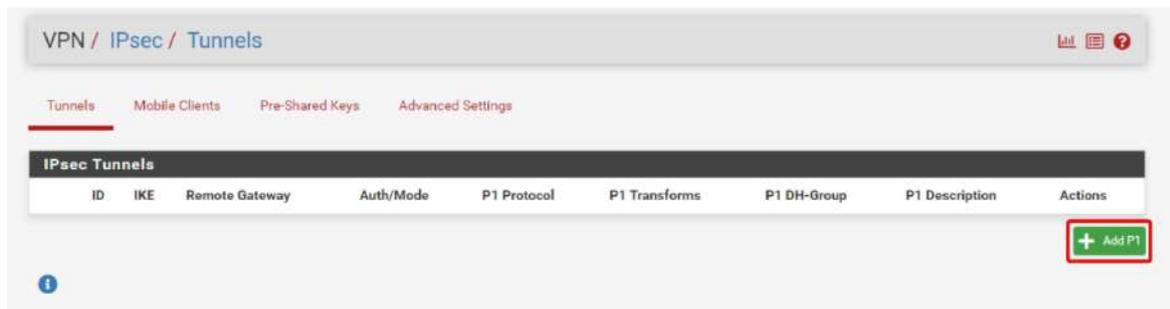
Next

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 :

General Information

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

Disabled: Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version:
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IP

Internet Protocol:
Select the Internet Protocol family.

Interface:
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway:
Enter the public IP address or host name of the remote gateway.

Phase 1 Proposal (Authentication)

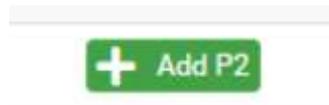
Authentication Method:
Must match the setting chosen on the remote side.

My identifier:

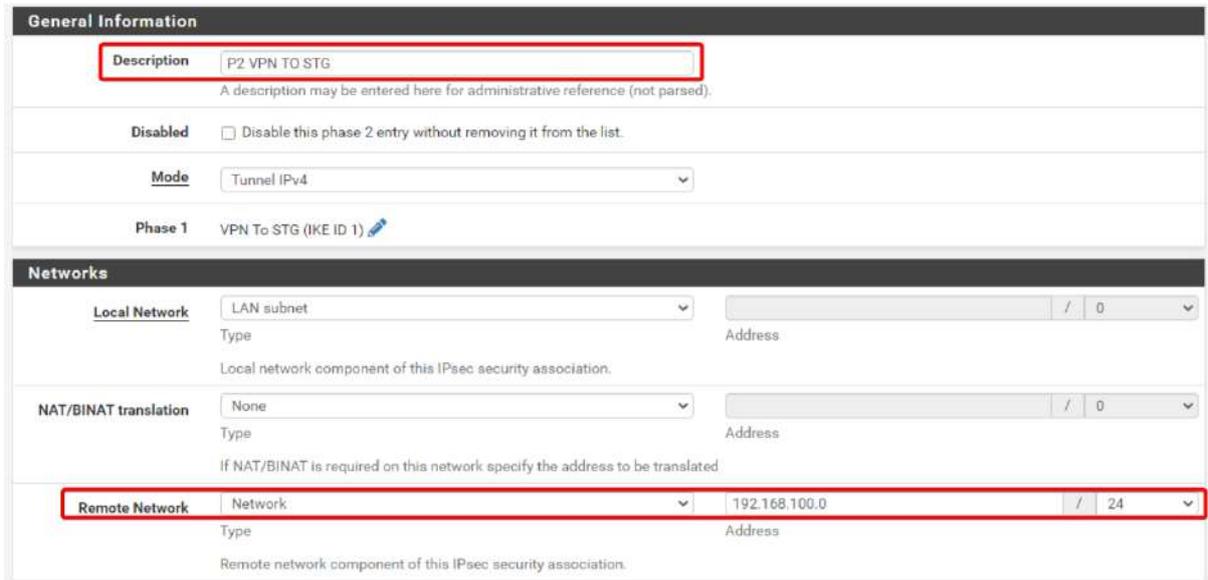
Peer identifier:

Pre-Shared Key:
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tu
[Generate new Pre-Shared Key](#)

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 :



General Information

Description: P2 VPN TO STG
A description may be entered here for administrative reference (not parsed).

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

Mode: Tunnel IPv4

Phase 1: VPN To STG (IKE ID 1)

Networks

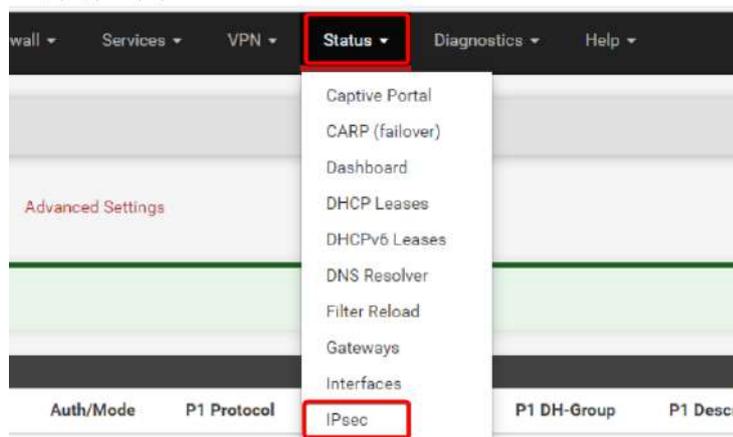
Local Network: LAN subnet / 0
Type: Address
Local network component of this IPsec security association.

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

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

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" :

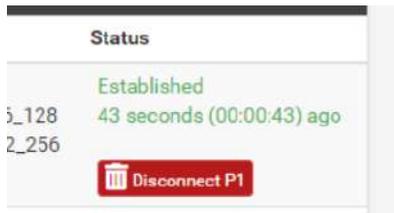


On clique ensuite sur "Connect P1 and P2s" :



ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	VPN TO MUL	ID: 10.0.0.1 Host: 10.0.0.1	ID: 10.0.0.2 Host: 10.0.0.2				Disconnected Connect P1 and P2s Connect P1

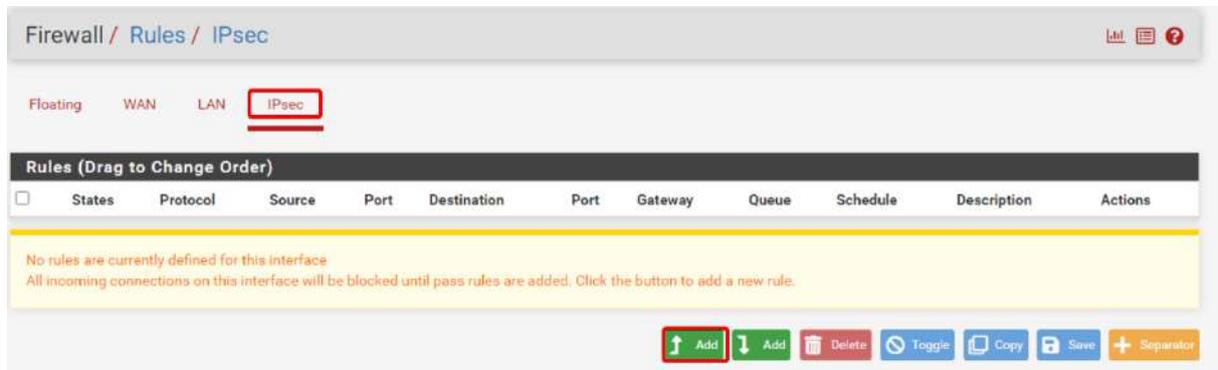
Si la configuration est correcte, la connexion sera considérée comme "Established" :



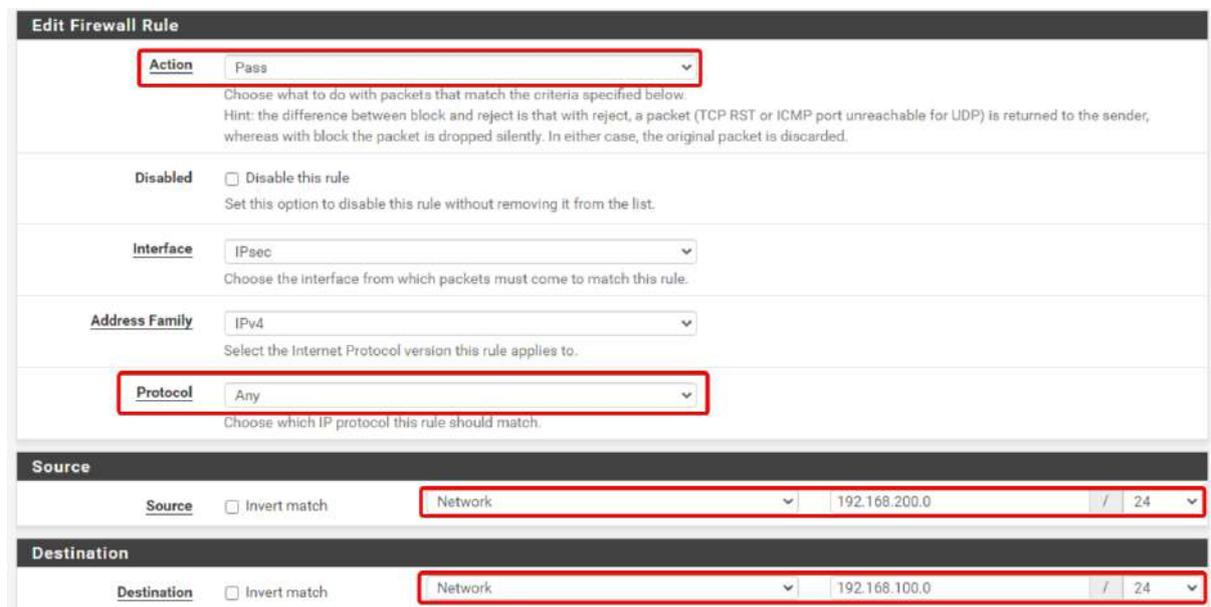
Il ne reste plus qu'à configurer les règles de Firewall, pour se faire, aller dans l'onglet "Firewall", "Rules" :



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 :

```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Pont réseau :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::8d2:b6e6:f797:e776%9
    Adresse IPv4. . . . . : 192.168.100.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.100.254

C:\Users\Administrateur>ping 192.168.200.254

Envoi d'une requête 'Ping' 192.168.200.254 avec 32 octets de données :
Réponse de 192.168.200.254 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.200.254 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.200.254 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.200.254 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 192.168.200.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\Administrateur>
```

La configuration Pfsense est maintenant terminée.

4) Configuration supplémentaires Windows Serveur 2022

4.1) Redondance réseau (IP Bouding)

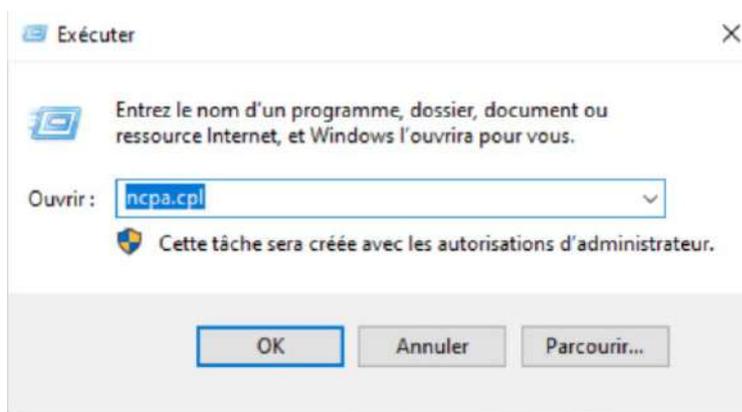
4.1.1) Bridge de cartes réseau avec STP actif

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.

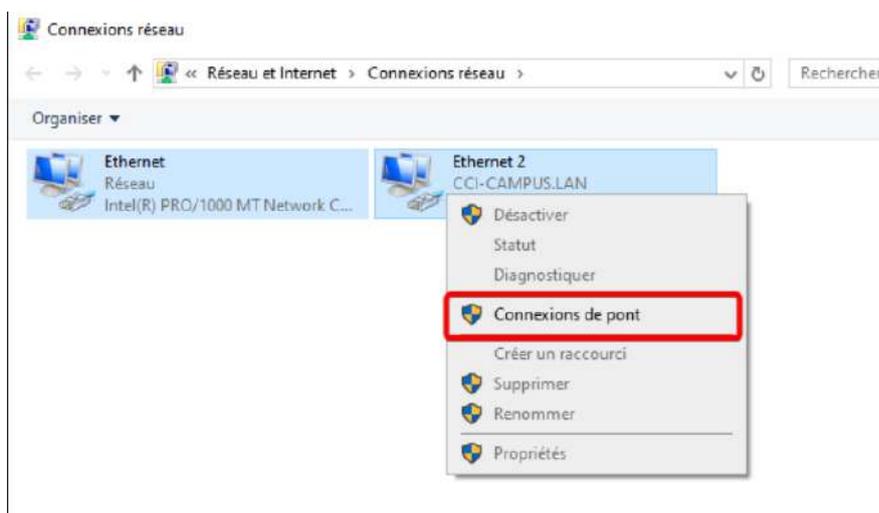
⚠ Attention

Cette fonction n'est cependant pas prévue 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 !

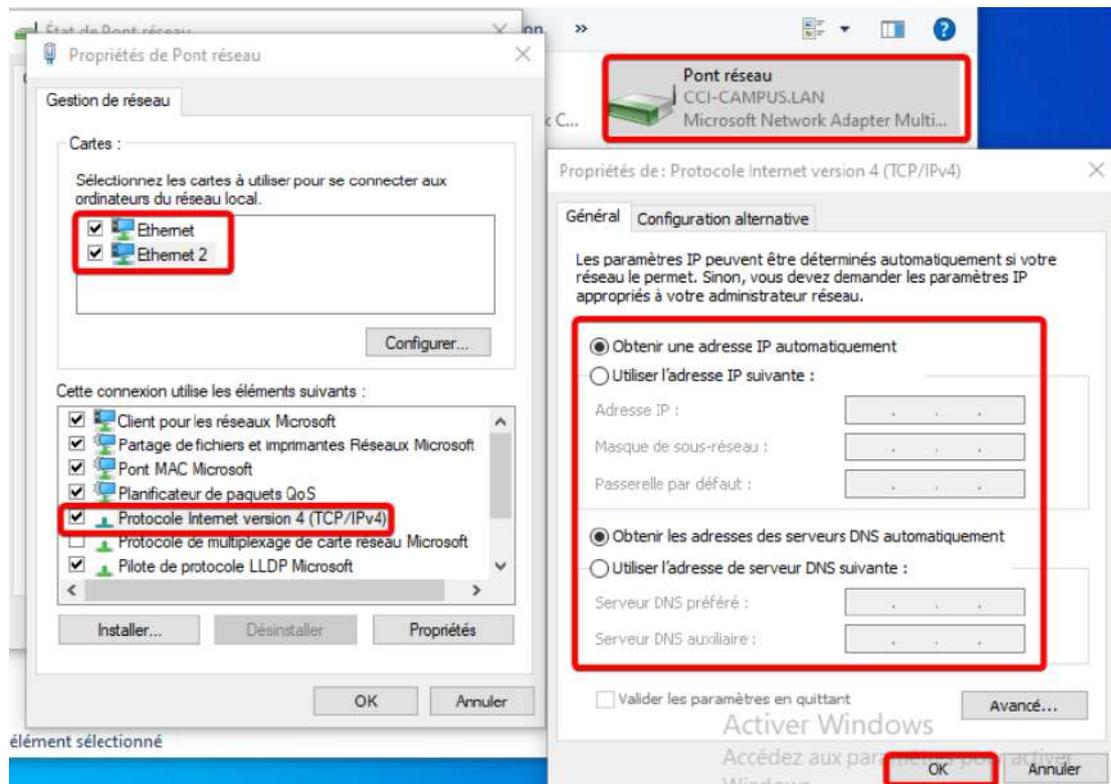
Pour cela, il suffit d'aller dans les connexions réseau du panneau de configuration, dans une fenêtre windows Exécuter (Windows + R) écrire ncpa.cpl :



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 :

```

Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Délai d'attente de la demande dépassé.
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=126
Statistiques Ping pour 192.168.100.1:
  Paquets : envoyés = 35, reçus = 30, perdus = 5 (perte 14%),
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
  
```

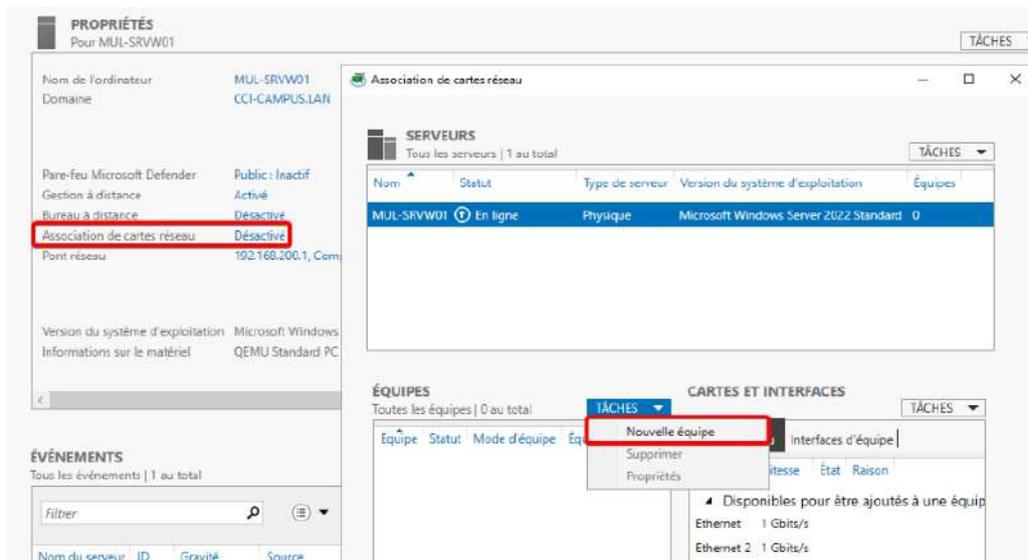
Désactivation d'une carte réseau du pont

Reprise par l'autre

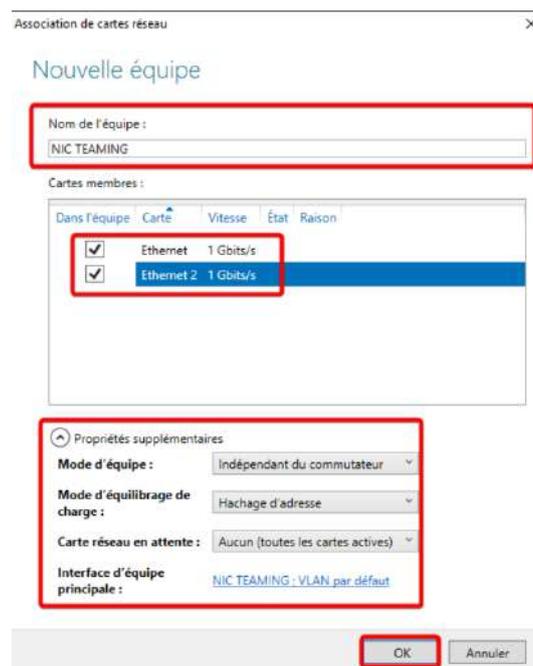
4.1.2) NIC Teaming

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

Pour se faire, il faut cliquer sur "Association de cartes réseau" depuis le 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 règle nos propriétés supplémentaires :

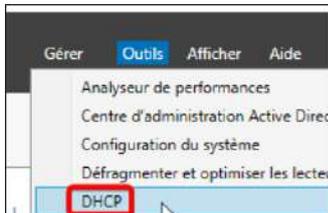


⚠ ATTENTION

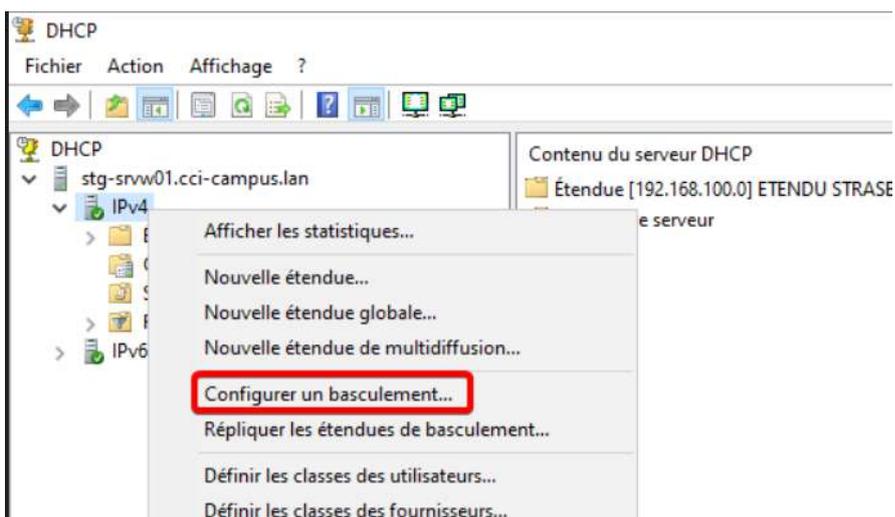
Le NIC Teaming peut ne pas fonctionner dans le cadre de serveurs virtualisés. De plus, la virtualisation n'est pas compatible avec le mode d'équilibrage de charge "Dynamique"

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 :

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire : 192.168.100.2 [Ajouter un serveur]

Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

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 :

Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire 192.168.100.2

Nom de la relation : stg-srvw01.cci-campus.lan-192.168.100.2

Délai de transition maximal du client (MCLT) : 1 heures 0 minutes

Mode : Serveur de secours

Configuration du serveur de secours

Rôle du serveur partenaire : Veille

Adresses réservées pour le serveur de secours : 10 %

Intervalle de basculement d'état : 60 minutes

Activer l'authentification du message

Secret partagé : *****

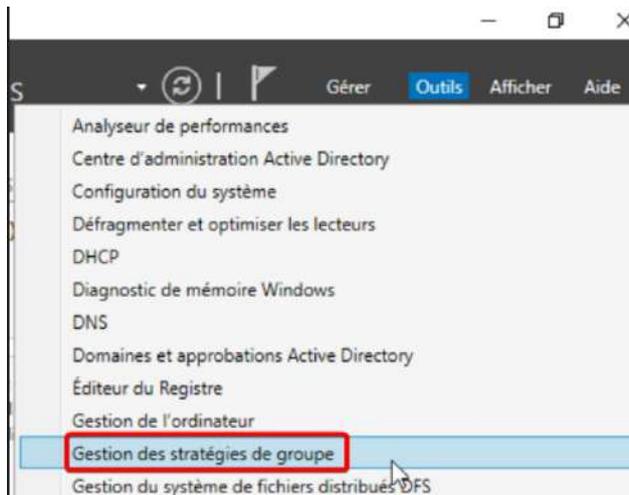
Pour finir, on peut cliquer sur Terminer.

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.

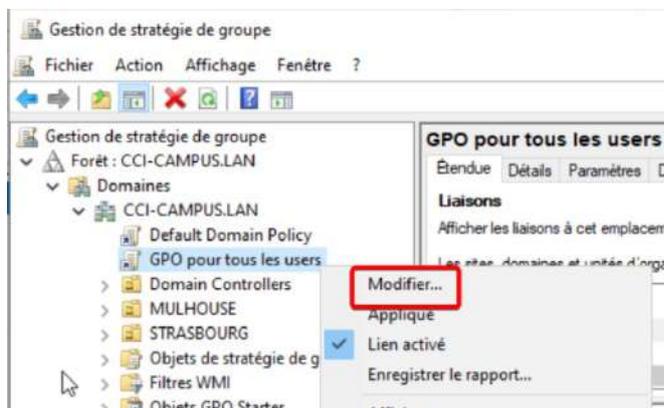
L'entièreté des configurations de ce chapitre se feront dans la console de "Gestion de stratégie de groupe", accessible depuis le gestionnaire de serveur :



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

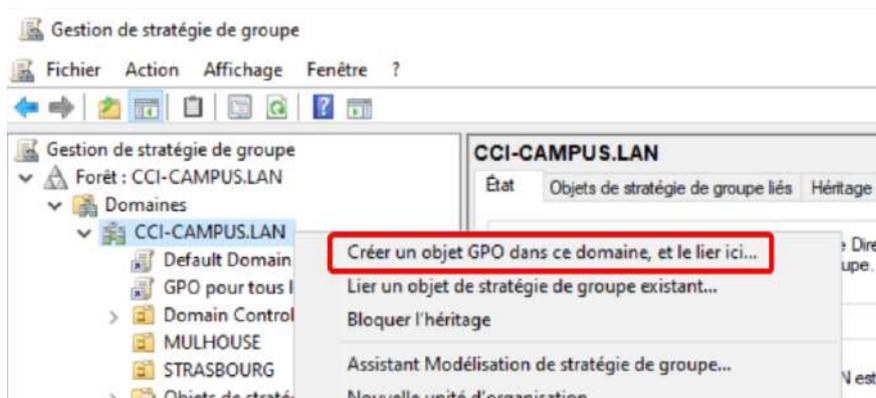
Pour éditer une GPO

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 clic droit sur le domaine ou l'OU 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 :

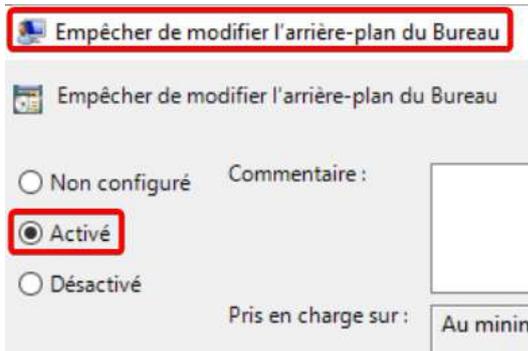
The screenshot shows the 'Papier peint du Bureau' configuration window. The 'Activé' radio button is selected. The 'Nom du papier peint' field contains the UNC path '\\RESSOURCES\BACKGROUND_BLACK.png'. The 'Style du papier peint' dropdown is set to 'Centrer'. The 'OK' button is highlighted.

⚠ 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

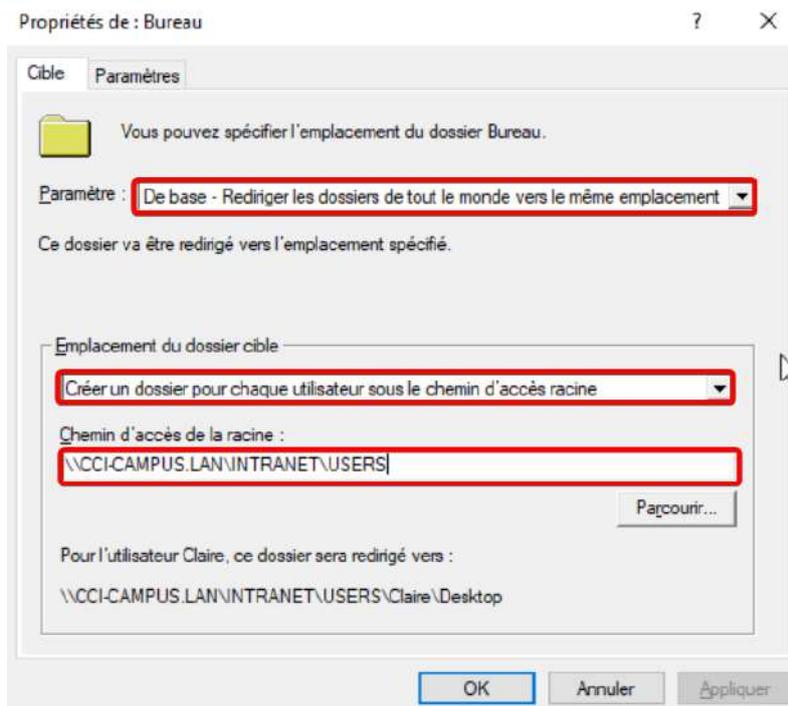


4.3.2) Redirection de dossiers

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

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

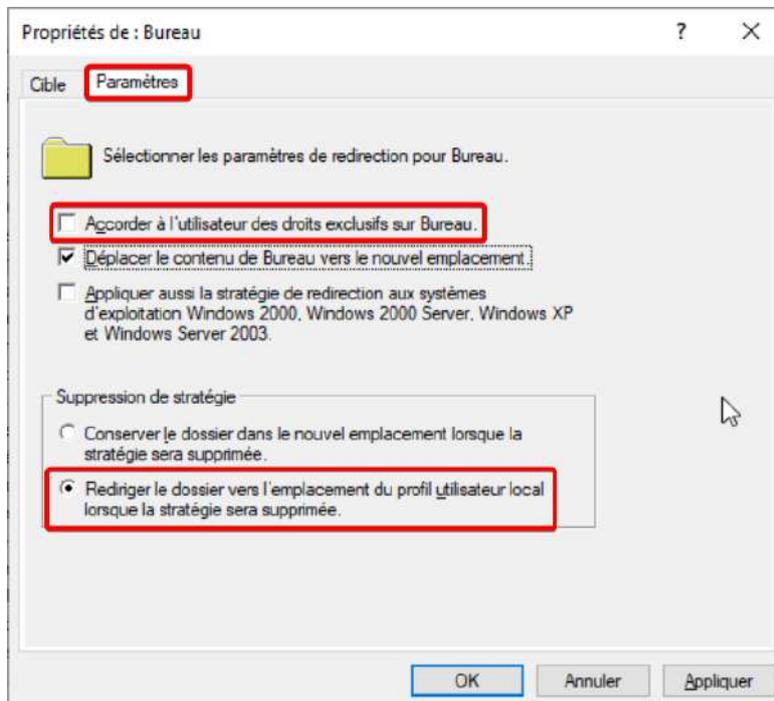
Puis on active la redirection de base, si on souhaite créer un dossier par utilisateur il faut sélectionner l'option adéquate, et enfin, le chemin d'accès réseau ou sera redirigé le dossier :



⚠ 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 :

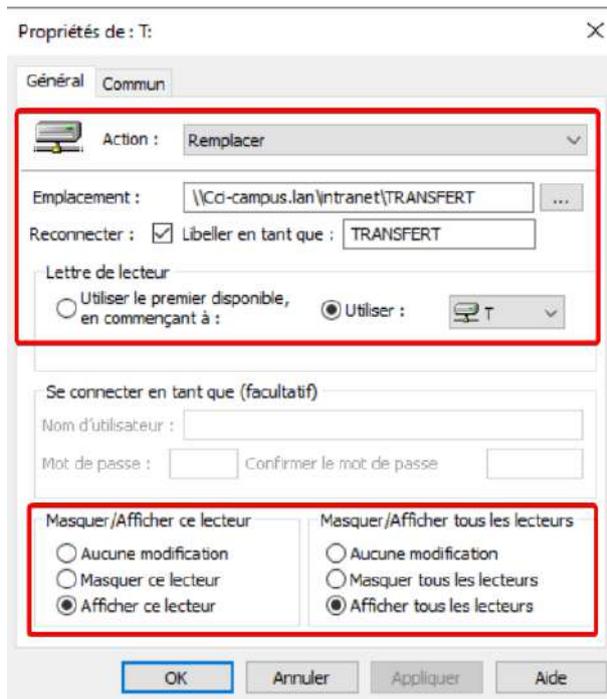


4.3.3) Mappage de lecteurs réseau

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

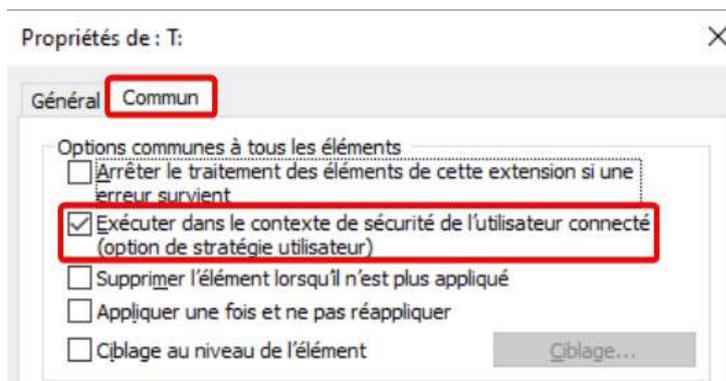
On configure ensuite le lecteur en "Action : Remplacer", puis on coche "Reconnecter" et on spécifie l'emplacement cible, un libeller et une lettre de lecteur. Enfin, on coche "Afficher ce lecteur" et "Afficher tous les lecteurs" :



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



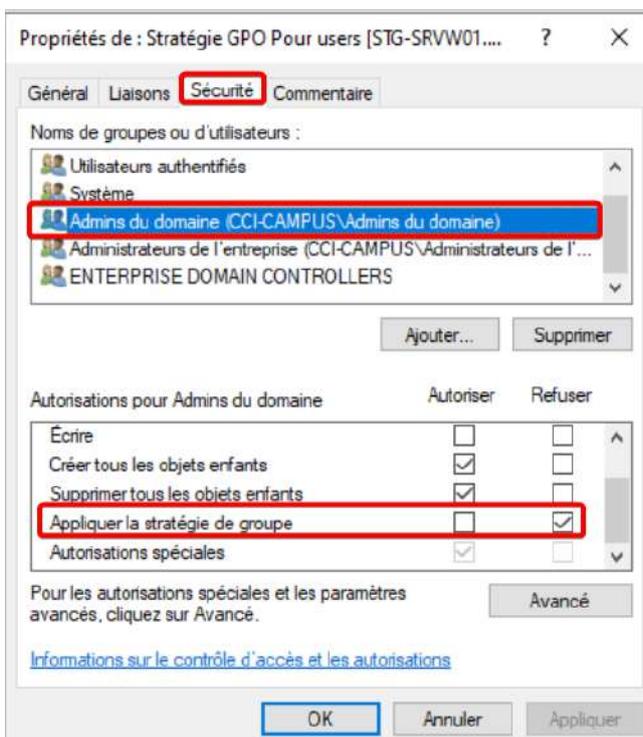
4.3.5) Empêcher l'exécution d'une GPO pour un groupe

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 champ "Appliquer la stratégie de groupe" :



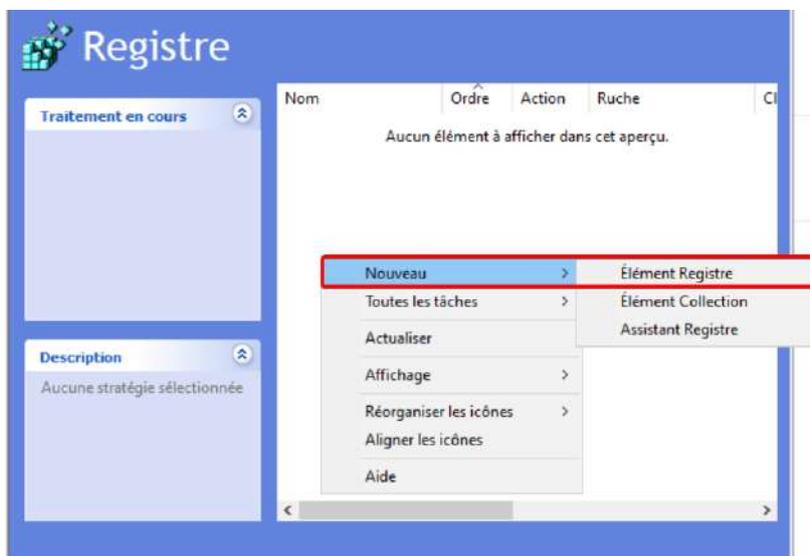
Puis cliquer sur OK.

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 :

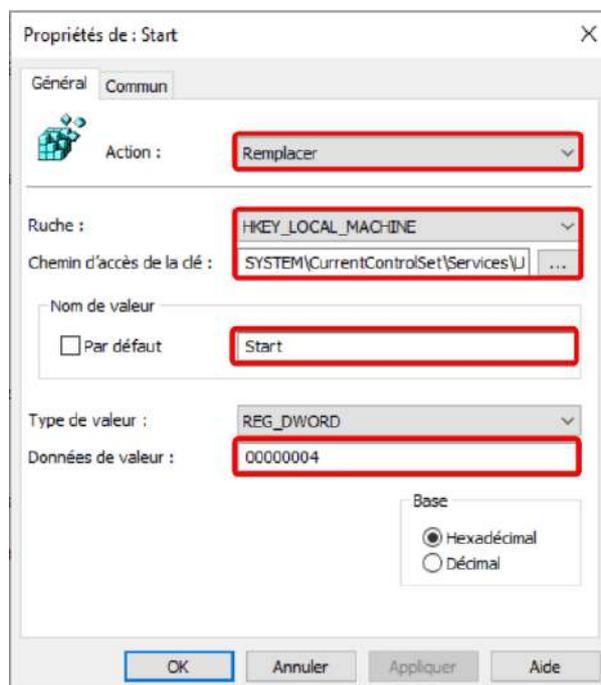
Configuration ordinateur > Préférences > Paramètres Windows > Registre

Puis faire un clic droit dans le panneau de droite, Nouveau, Élément 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

The screenshot shows the Group Policy Editor interface. On the left, the navigation tree is expanded to 'Configuration utilisateur' > 'Stratégies' > 'Modèles d'administration : définitions de stratégies (Fichier)' > 'Système' > 'Accès au stockage amovible'. On the right, a table lists various policies with their status and comments. Three policies are highlighted with red boxes: 'Disques amovibles : refuser l'accès en lecture', 'Disques amovibles : refuser l'accès en écriture', and 'Toutes les classes de stockage amovible : refuser tous les acc...'. All three are set to 'Activé'.

Paramètre	État	Commentaire
Définir le délai (en secondes) avant de forcer le redémarrage	Non configuré	Non
CD et DVD : refuser l'accès en lecture	Non configuré	Non
CD et DVD : refuser l'accès en écriture	Non configuré	Non
Classes personnalisées : refuser l'accès en lecture	Non configuré	Non
Classes personnalisées : refuser l'accès en écriture	Non configuré	Non
Lecteurs de disquettes : refuser l'accès en lecture	Non configuré	Non
Lecteurs de disquettes : refuser l'accès en écriture	Non configuré	Non
Disques amovibles : refuser l'accès en lecture	Activé	Non
Disques amovibles : refuser l'accès en écriture	Activé	Non
Toutes les classes de stockage amovible : refuser tous les acc...	Activé	Non
Lecteurs de bandes : refuser l'accès en lecture	Non configuré	Non
Lecteurs de bandes : refuser l'accès en écriture	Non configuré	Non
Périphériques WPD : refuser l'accès en lecture	Non configuré	Non
Périphériques WPD : refuser l'accès en écriture	Non configuré	Non

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
 - o Restreindre au lecteur C uniquement
- Empêcher l'accès aux lecteurs à partir du Poste de travail
 - o Restreindre au lecteur C uniquement

Paramètre	État	Commentaire
Supprimer les fonctionnalités de gravure de CD	Non configuré	Non
Désactiver la mise en cache des miniatures	Non configuré	Non
Supprimer l'interface utilisateur permettant de modifier les ...	Non configuré	Non
Supprimer l'interface utilisateur permettant de modifier les ...	Non configuré	Non
Supprimer l'onglet DFS	Non configuré	Non
Dans Poste de travail, masquer ces lecteurs spécifiés	Activé	Non
Ne pas afficher « Tout le réseau » dans les emplacements rés...	Non configuré	Non
Supprimer le menu Fichier de l'Explorateur de fichiers	Non configuré	Non
Ne pas autoriser l'ouverture des Options des dossiers à partir...	Non configuré	Non
Supprimer l'onglet Matériel	Non configuré	Non
Masque l'élément Gérer du menu contextuel de l'Explorateur...	Non configuré	Non
Supprimer les Documents partagés du Poste de travail	Non configuré	Non
Supprimer les options « Connecter un lecteur réseau » et « D...	Non configuré	Non
Ne pas déplacer les fichiers supprimés vers la Corbeille	Non configuré	Non
Ne pas demander d'autres informations d'identification	Non configuré	Non
Supprimer le lien Relancer la recherche de Rechercher sur In...	Non configuré	Non
Supprimer l'onglet Sécurité	Non configuré	Non
Supprimer le bouton Rechercher de l'Explorateur de fichiers	Non configuré	Non
Désactiver le tri numérique dans l'Explorateur de fichiers	Non configuré	Non
Supprimer le menu contextuel par défaut de l'Explorateur d...	Non configuré	Non
Empêcher l'accès aux lecteurs à partir du Poste de travail	Activé	Non
Désactiver les touches de raccourci Windows	Non configuré	Non
Ne pas afficher « Ordinateurs proches » dans les emplaceme...	Non configuré	Non

Dans Poste de travail, masquer ces lecteurs spécifiés

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

Désactivé

Pris en charge sur : Au minimum Windows 2000

Options : Aide :

Choisissez l'une des combinaisons suivantes

Restreindre au lecteur C uniquement

Ce paramètre de stratégie permet de masquer les lecteurs spécifiés dans Poste de travail.

Ce paramètre de stratégie supprime les icônes représentant les disques durs sélectionnés du Poste de travail et de l'Explorateur de fichiers. En outre, les lettres représentant les lecteurs

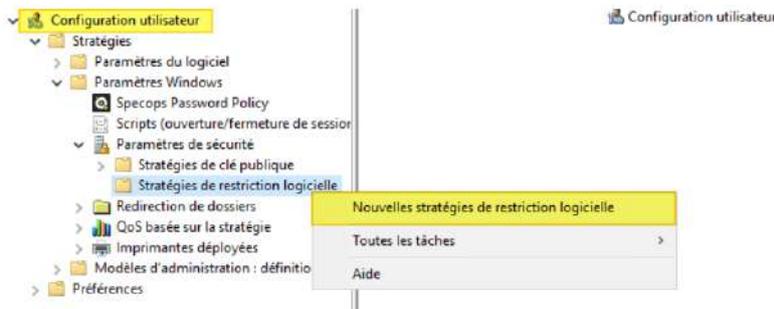
Maintenant, les utilisateurs n'auront plus accès au lecteur C.

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

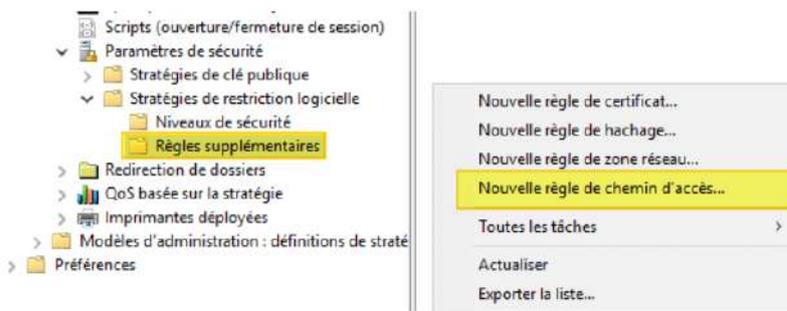
Pour bloquer l'accès aux consoles Powershell, il faut tout d'abord faire un clic droit sur le paramètre suivant :

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

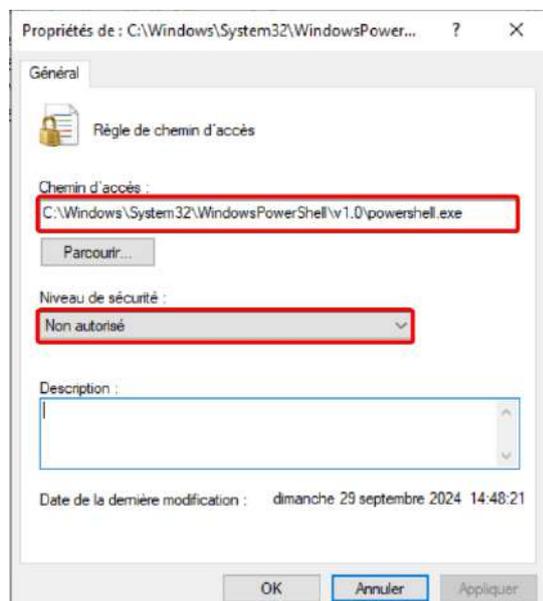
Puis cliquer sur "Nouvelles stratégies de restriction logicielle" :



Nous allons ensuite créer des règles de chemin d'accès, faites donc un clic 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 terminée.

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

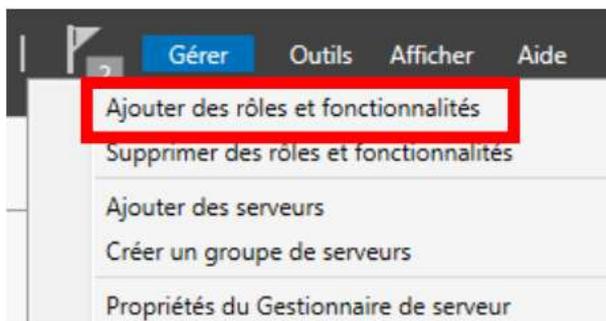
5.1) Prérequis

- 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

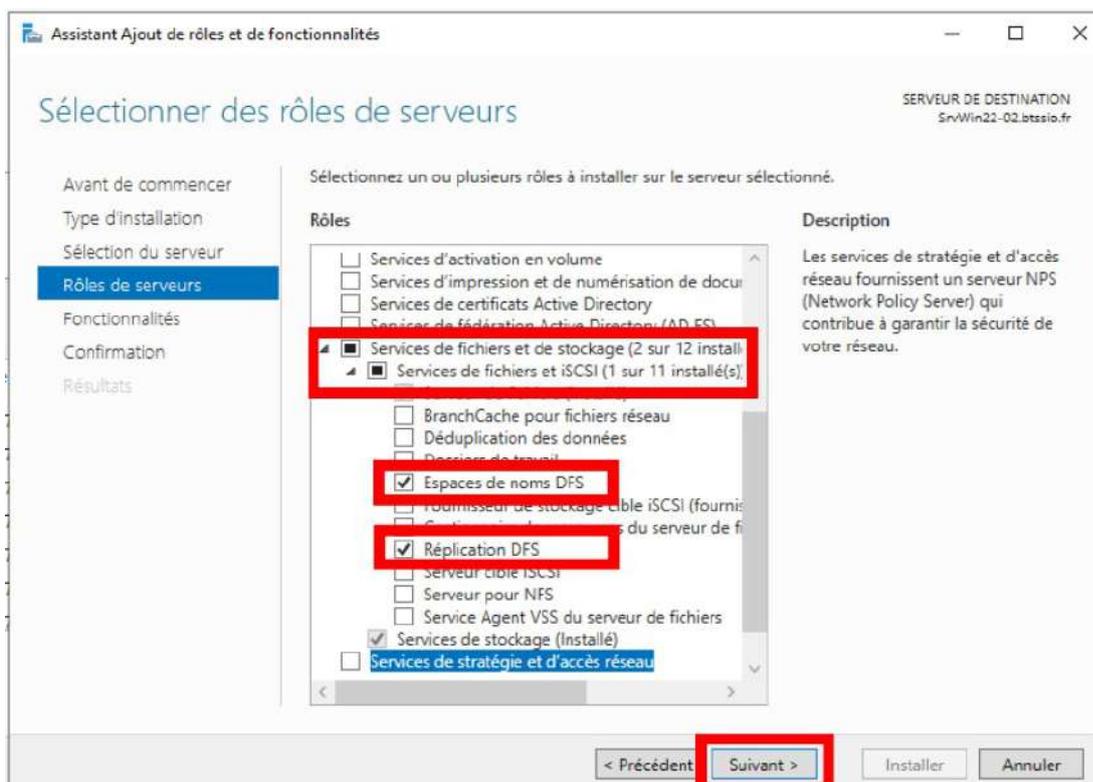
5.2) DFS

5.2.1) Création et configuration de l'espace de noms

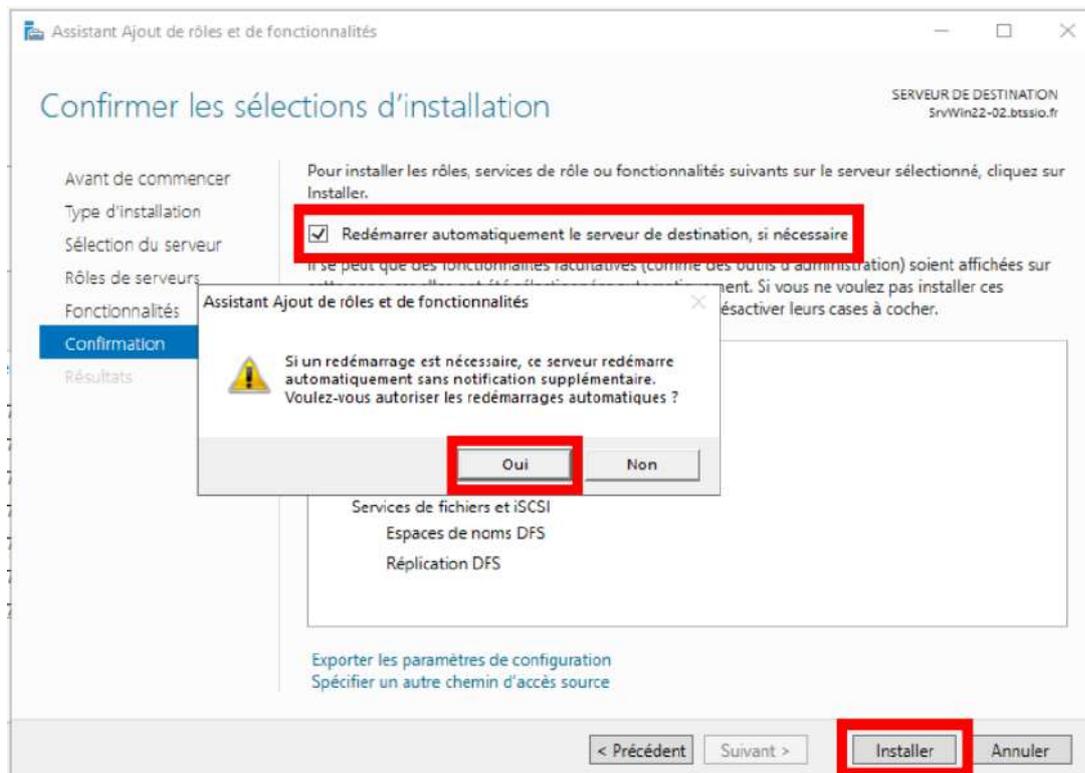
On commence par ajouter le rôle DFS et DFSR depuis le gestionnaire de serveur :



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

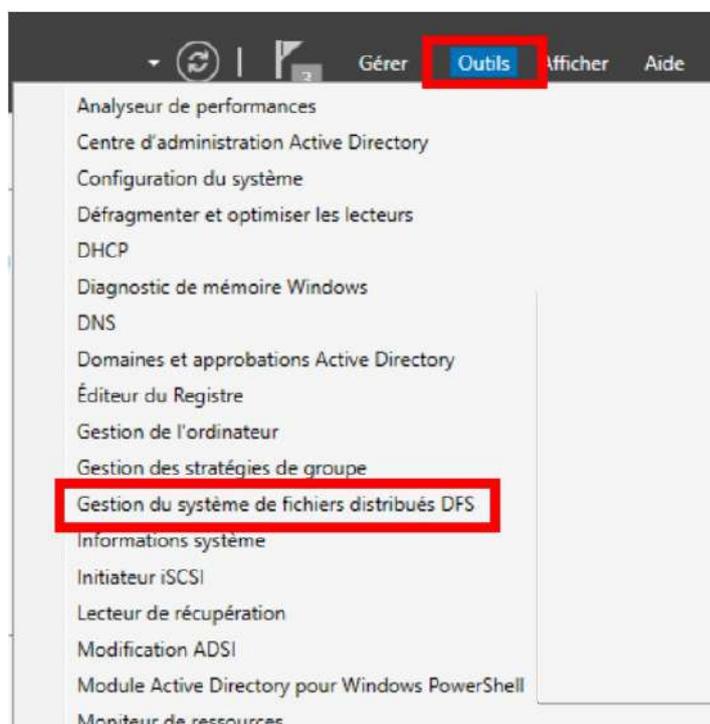


Puis on peut aller jusqu'à la page de Confirmation, on coche « Redémarrer automatiquement le serveur de destination, si nécessaire » et on répond « Oui » à la fenêtre pop-up puis Installer :

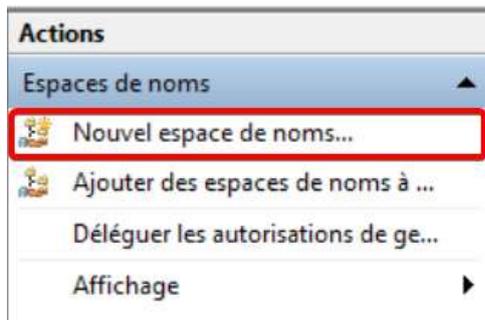


Il faut faire les mêmes opérations sur les autres serveurs que l'on souhaite utilisé pour le DFS

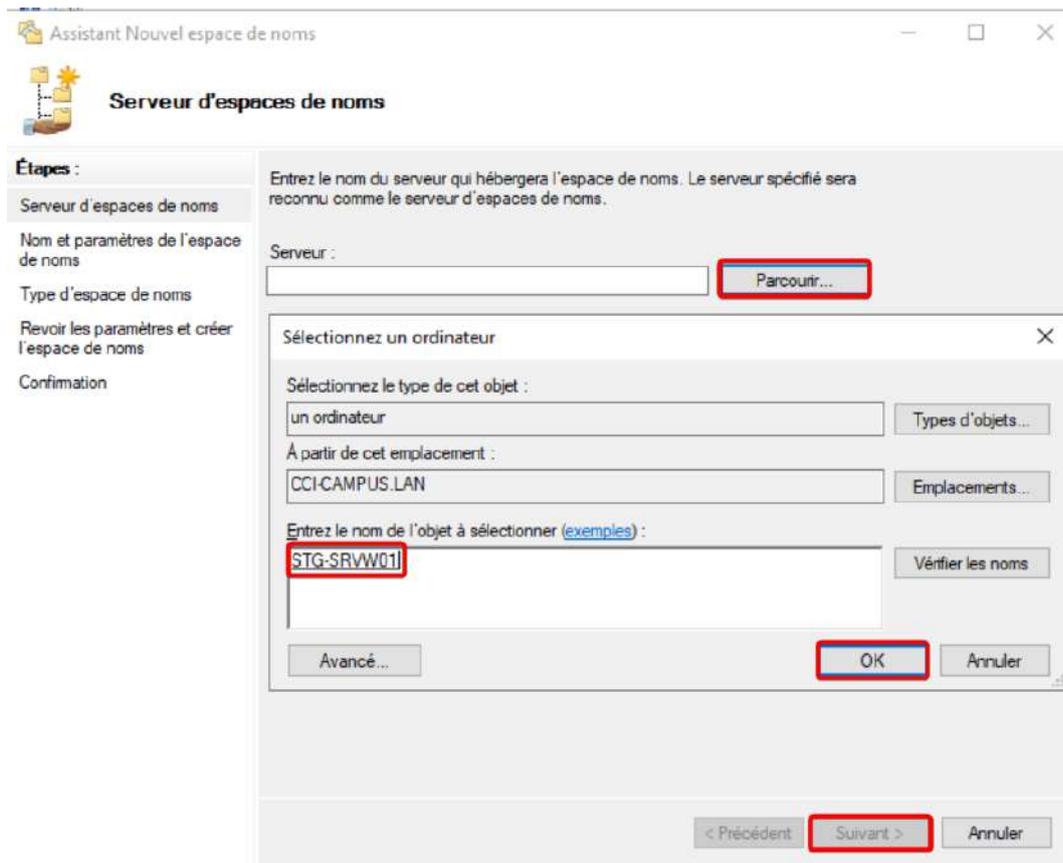
Ensuite, on peut aller dans "Outils" puis "Gestion du système de fichiers distribués DFS":



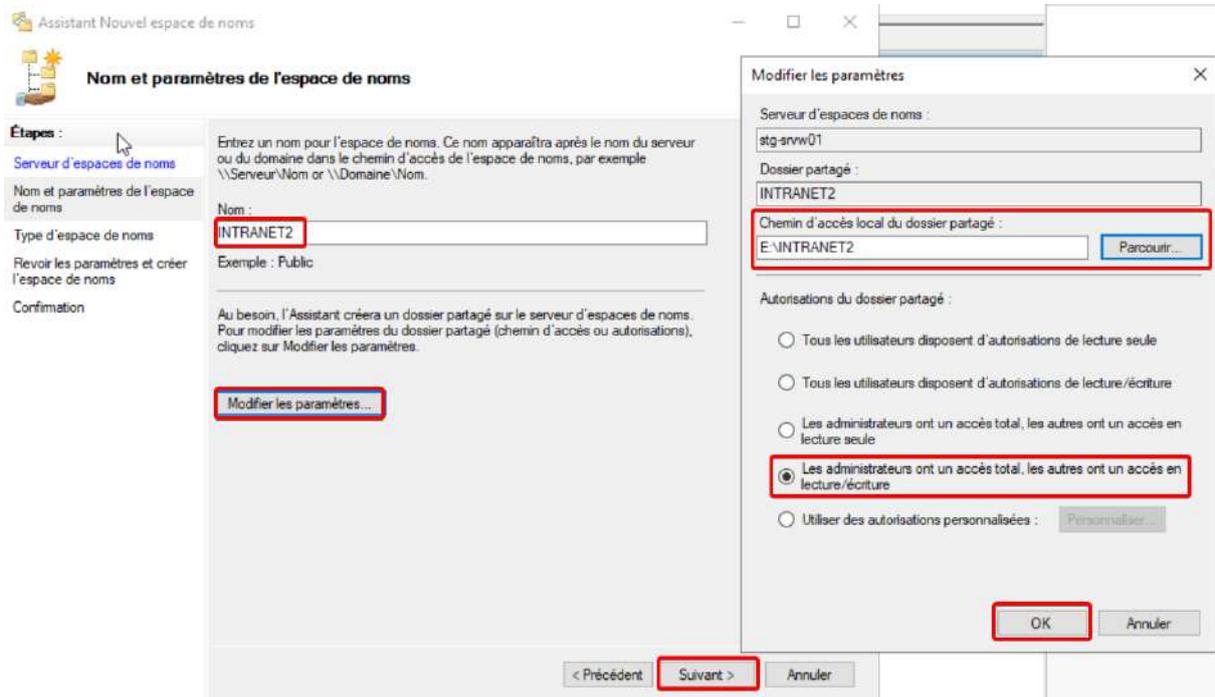
Puis dans le panneau de droite on clique sur "Nouvel espace de noms..."



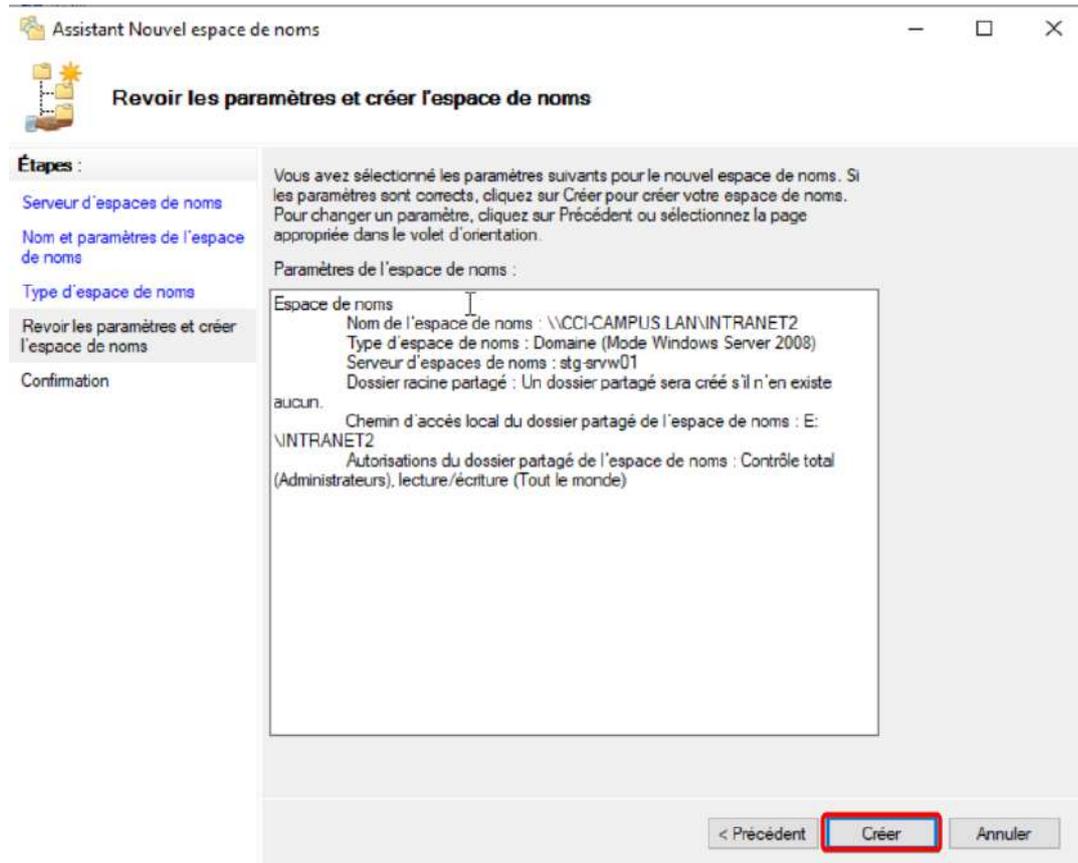
Puis on sélectionne notre serveur principal et on fait suivant :



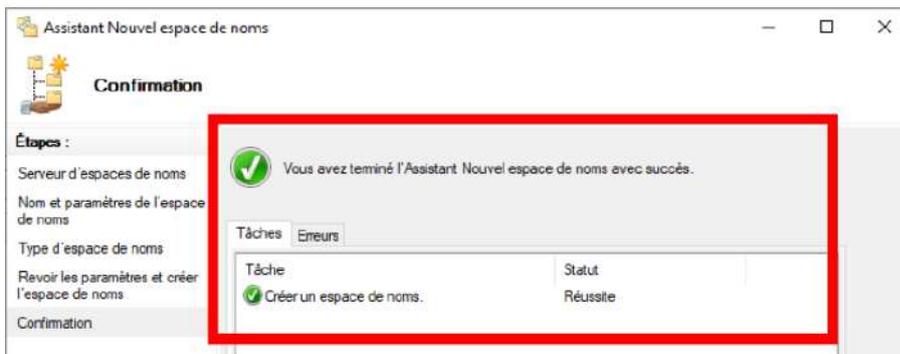
On entre ensuite le nom de l'espace de noms, puis "Modifier les paramètres", on choisit un dossier local pour le partage (créer un dossier sur le deuxième disque) et on change les permissions :



On peut ensuite cliquer sur Suivant et Créer :



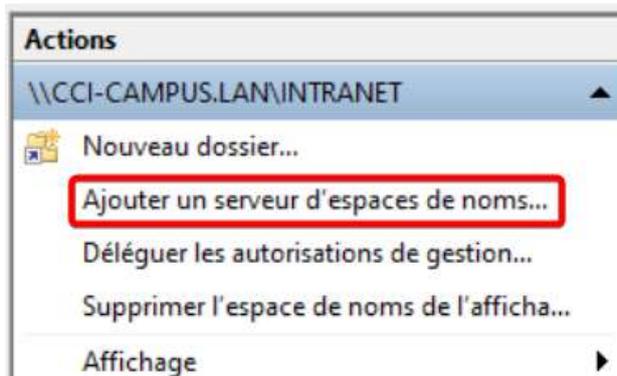
Si tout c'est bien passé vous aurez un message de validation :



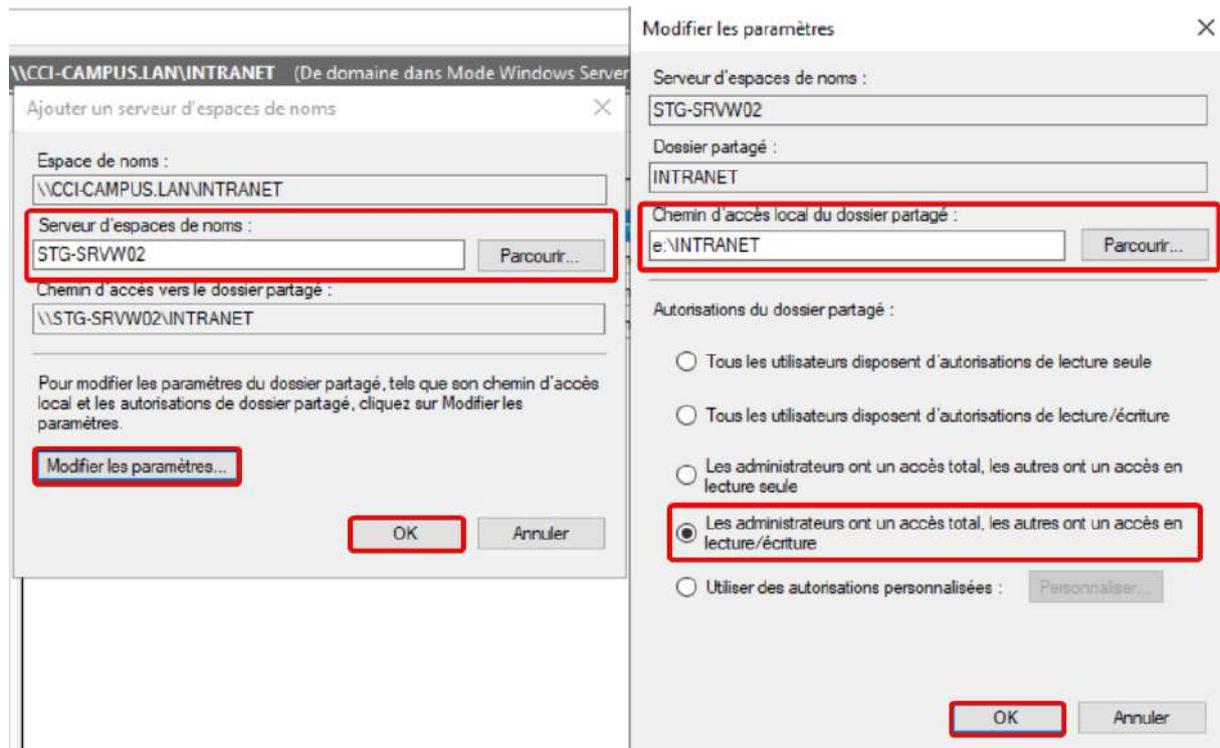
Nous allons maintenant ajouter un deuxième serveur d'espace de noms, cliquer sur votre Espace de noms que vous venez de créer, puis sur "Serveurs d'espaces de noms" :



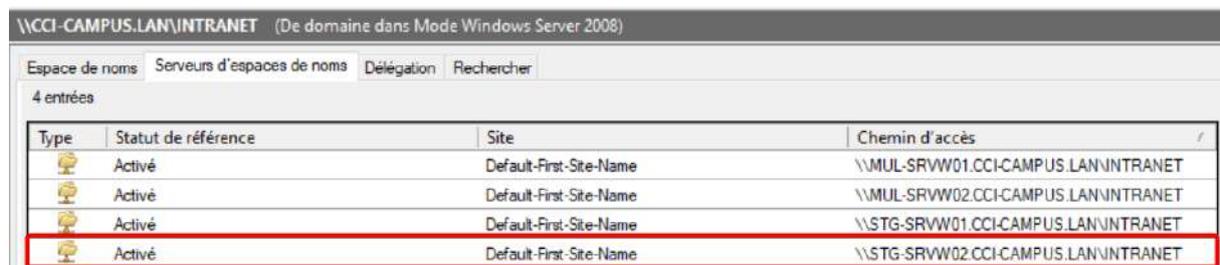
Dans le panneau de droite, il faut cliquer sur "Ajouter un serveur d'espaces de noms..." :



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 :

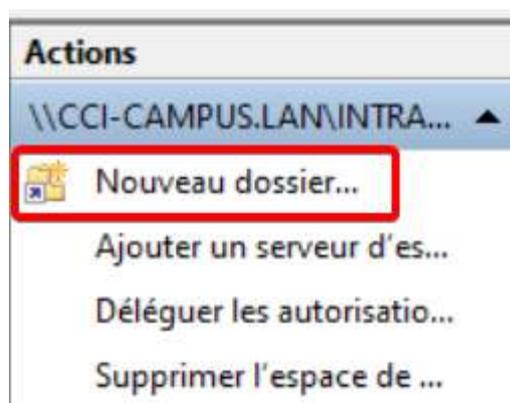


Après avoir cliquer sur OK, on peut voir que notre serveur à été ajouté :

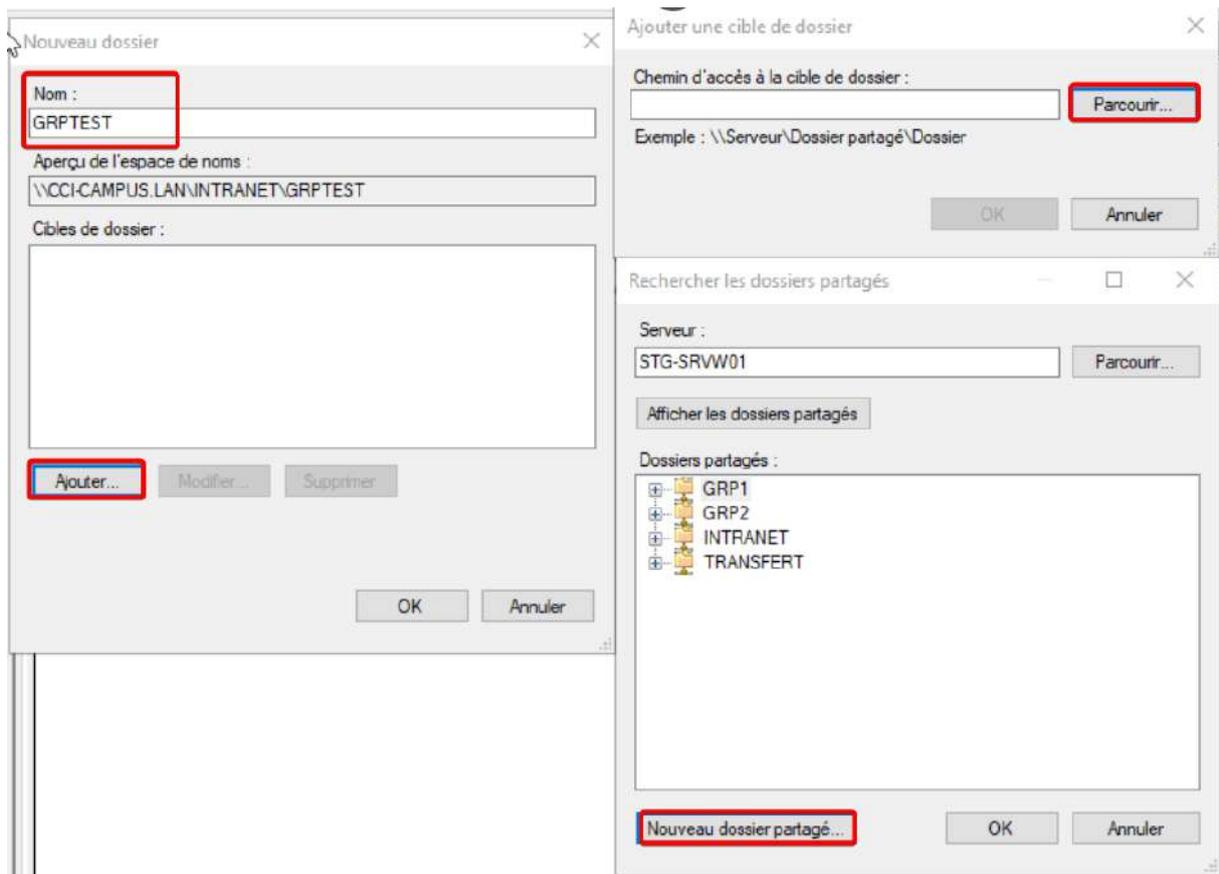


5.2.2) Création d'un dossier cible

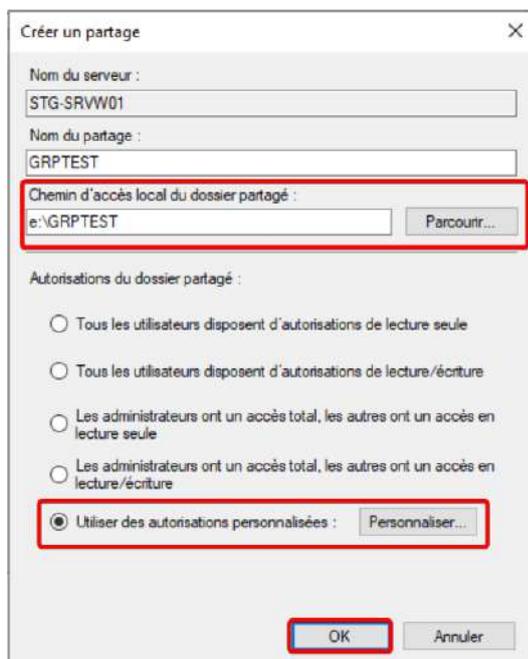
Dans le panneau de droite, cliquer sur "Nouveau dossier..." :



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

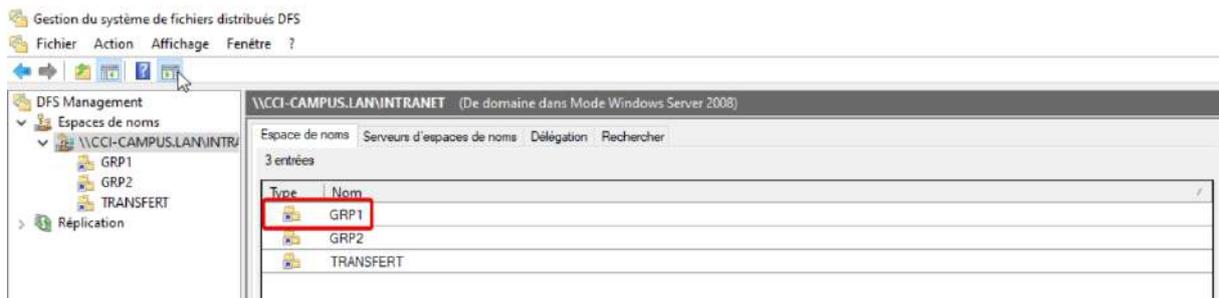


Ensuite on sélectionne un chemin local vers un nouveau dossier sur le deuxième disque, on met nos autorisations (ici personnalisées) et on clique sur OK :



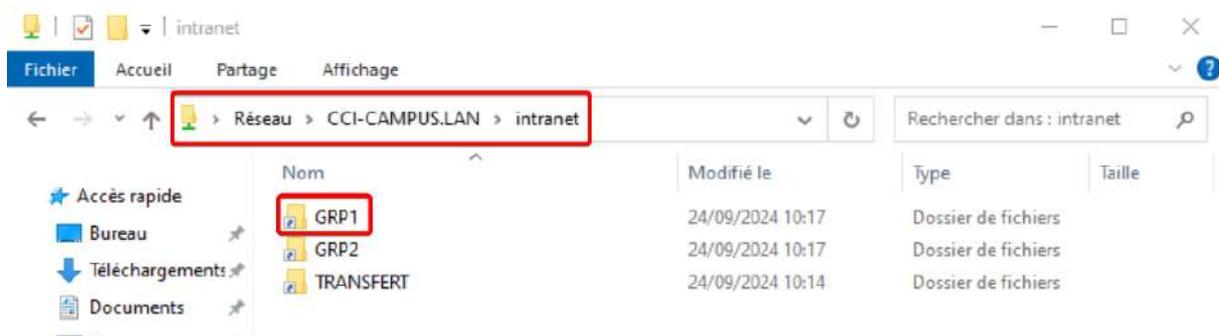
Enfin, on peut sélectionner le dossier partagé que l'on vient de créer et cliquer sur OK.

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

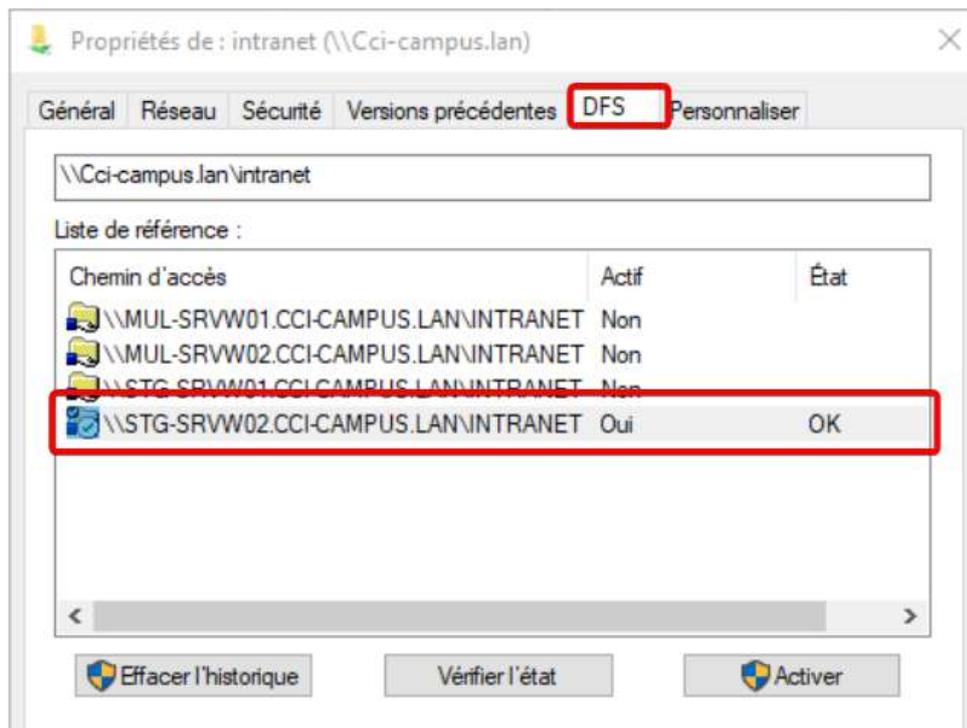


5.2.3) Vérification DFS

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.

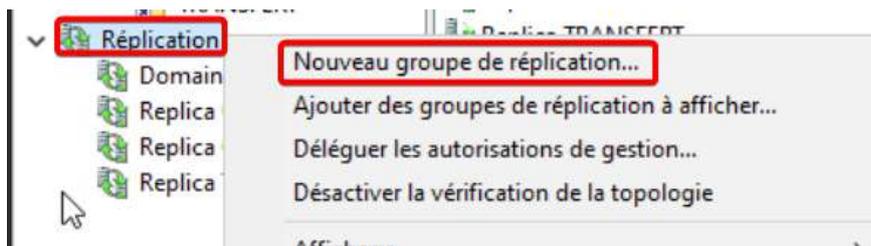
5.3) DFSR

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.

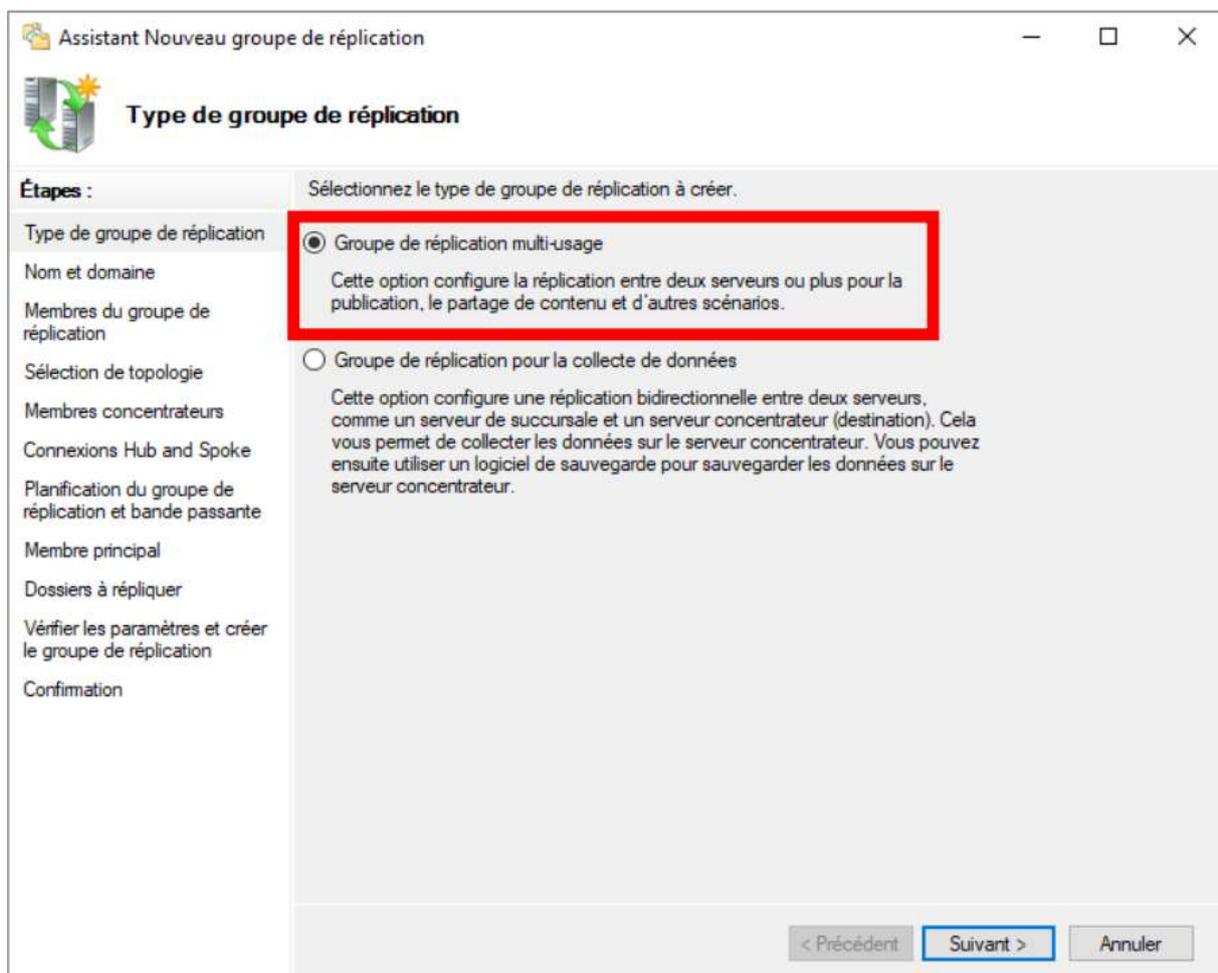
Nous avons déjà installé le rôle de Réplication des données dans le chapitre sur DFS, DFSR est donc déjà installé.

5.3.1) Configuration du DFSR

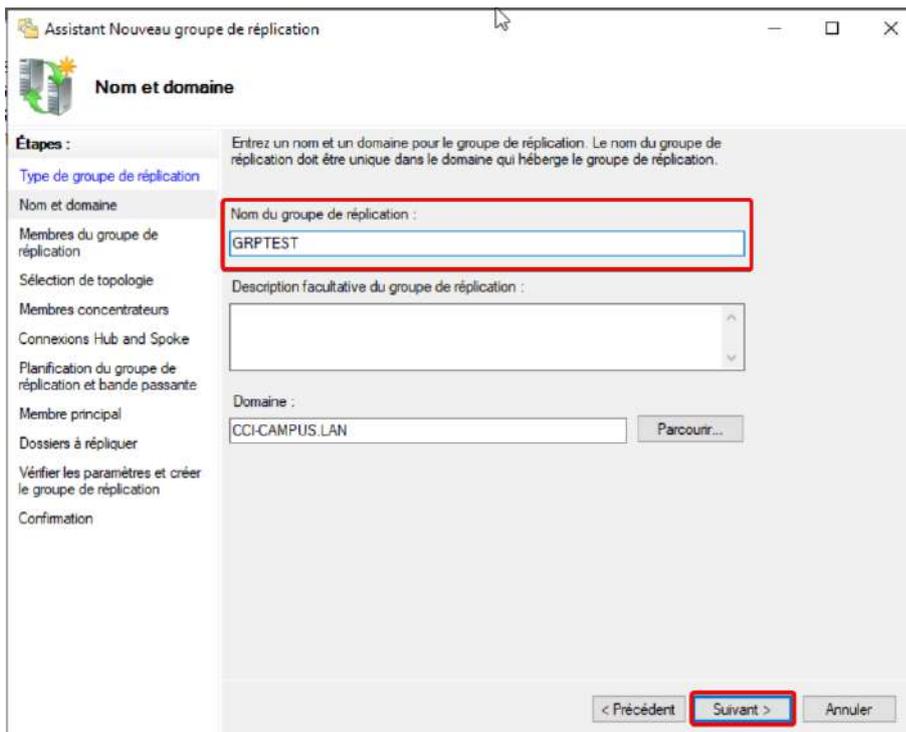
Pour le configurer, il suffit de cliquer sur "Réplication" (dans Gestion du système de fichiers distribués DFS), ensuite faire un clique droit sur "Réplication" et cliquer sur "Nouveau groupe de réplication..." :



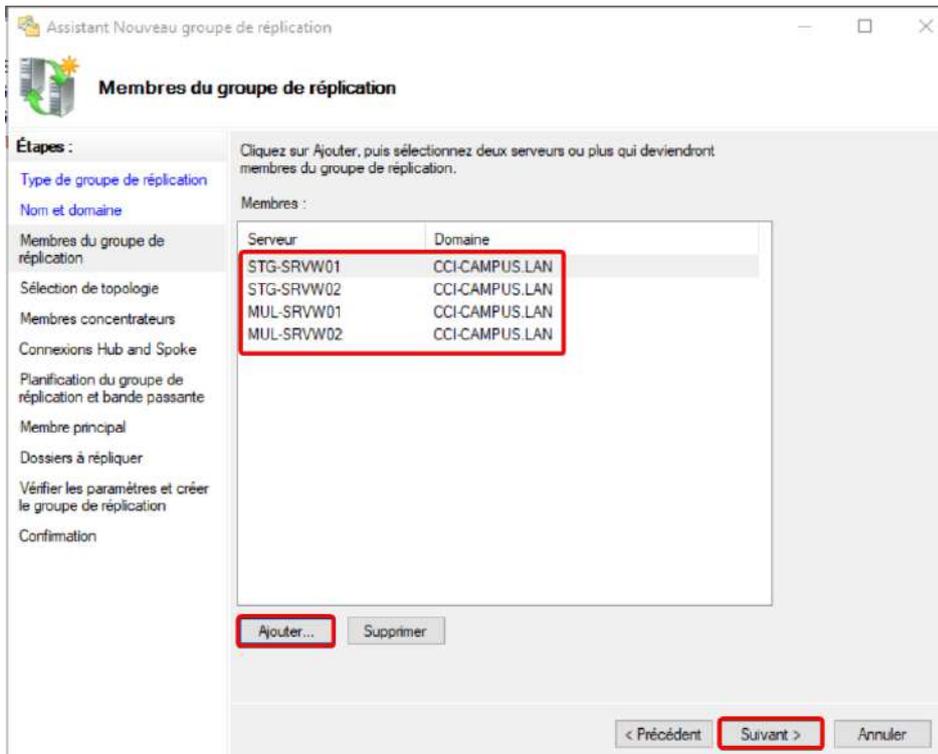
On laisse par défaut :



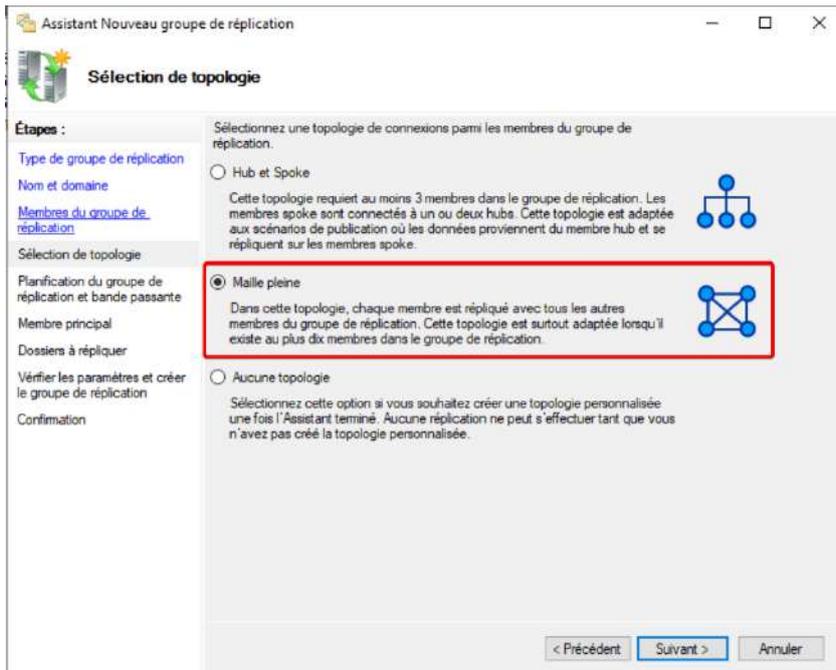
On choisit ensuite un nom :



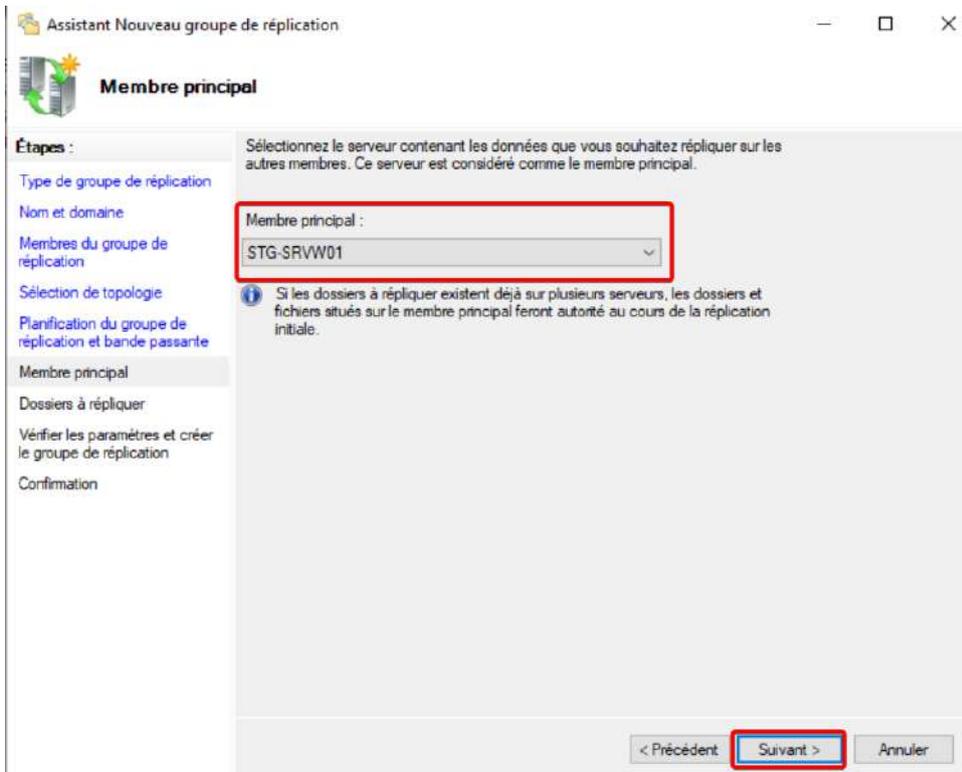
On ajoute ensuite tous nos serveurs qui devront répliquer les données :



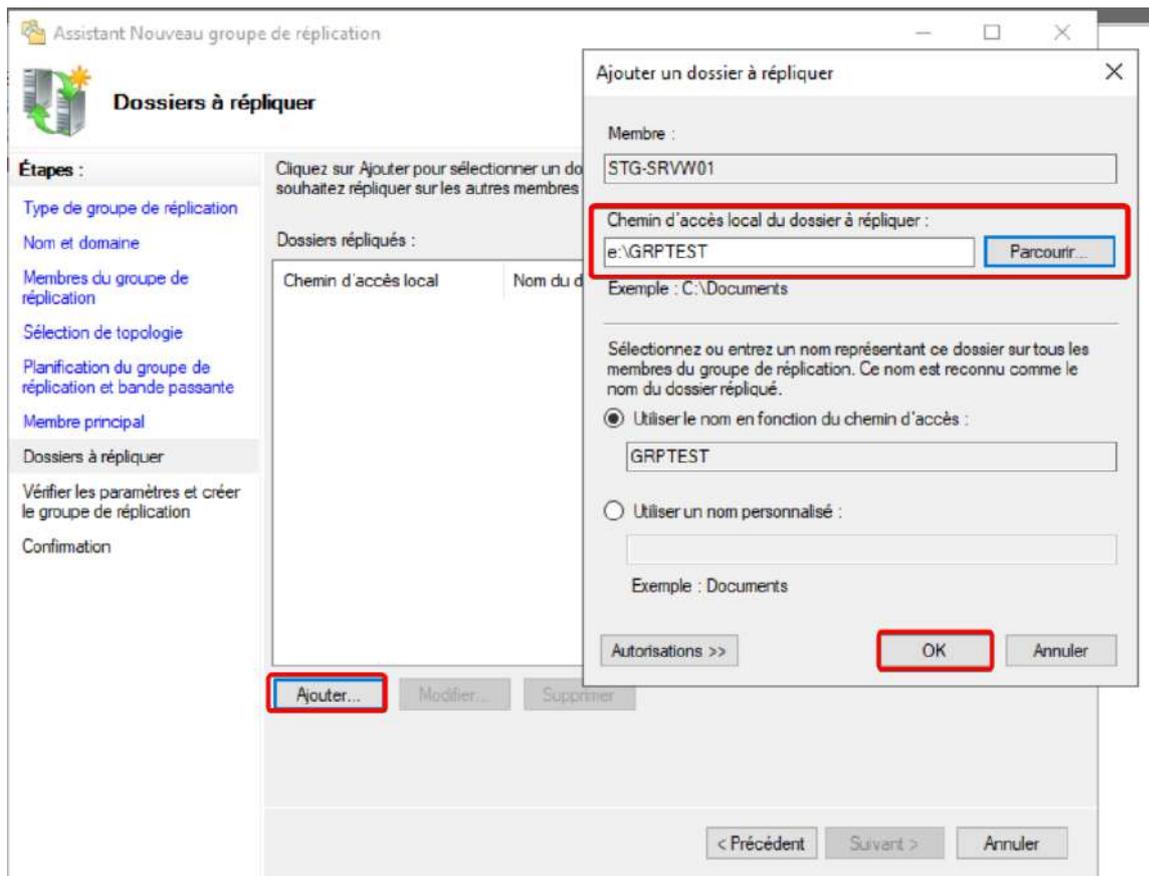
On sélectionne ici "Maille pleine", puis on clique 2 fois sur suivant :



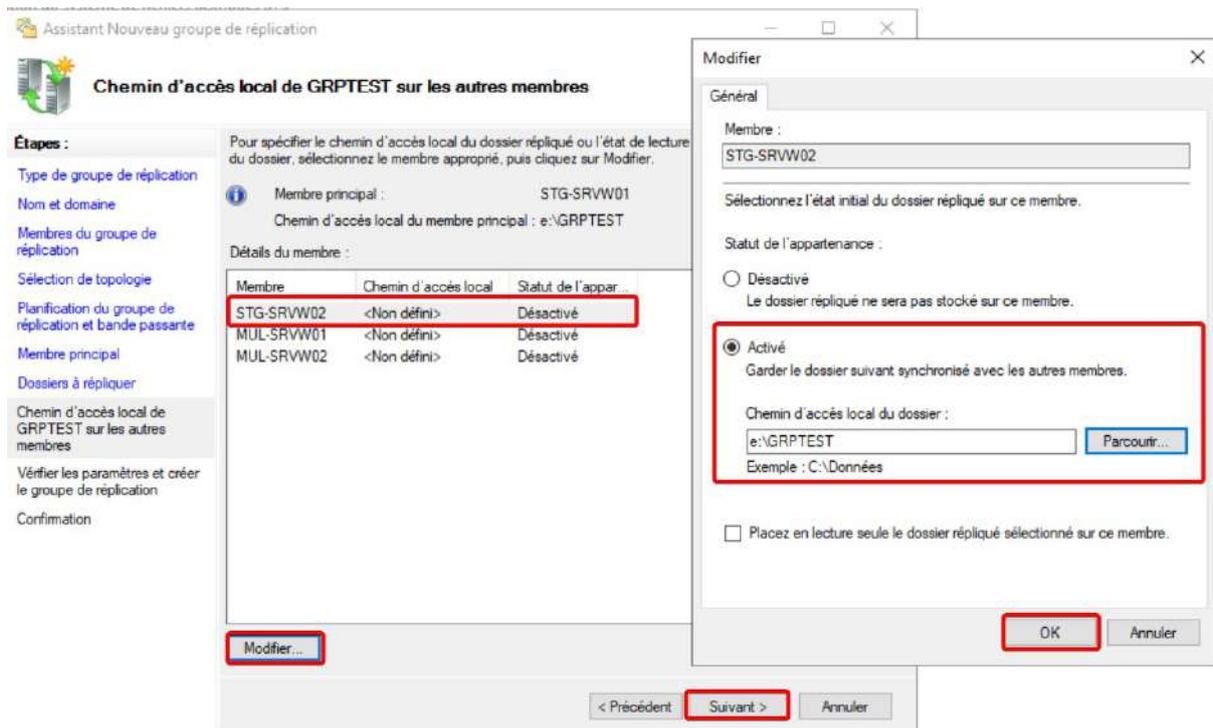
On choisit ensuite le "membre principal" c'est à dire le serveur qui détient localement la donnée à répliquer :



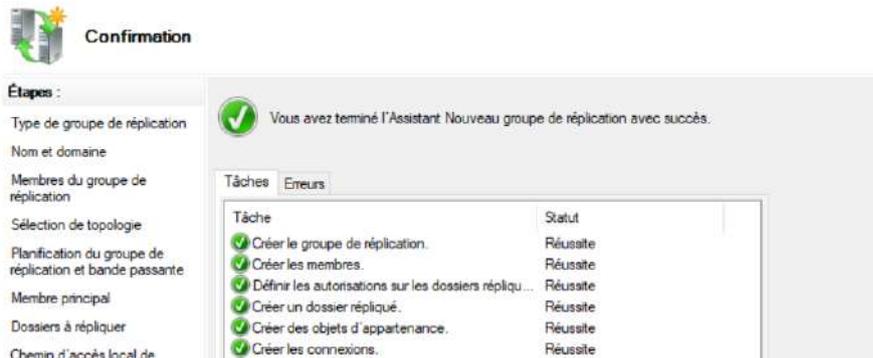
On sélectionne ensuite le chemin vers le dossier local :



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 :

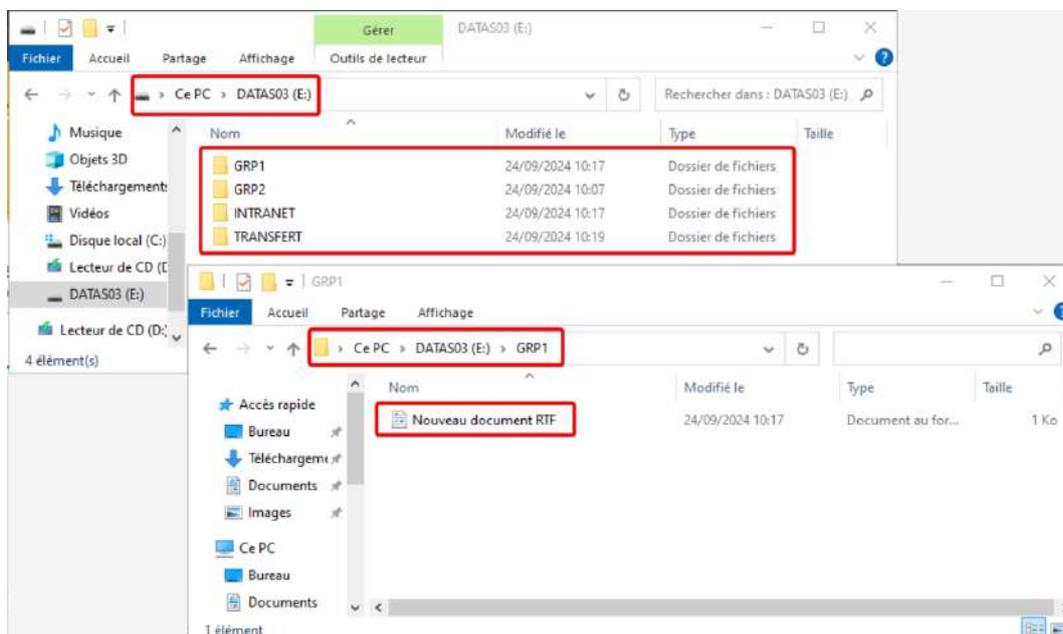
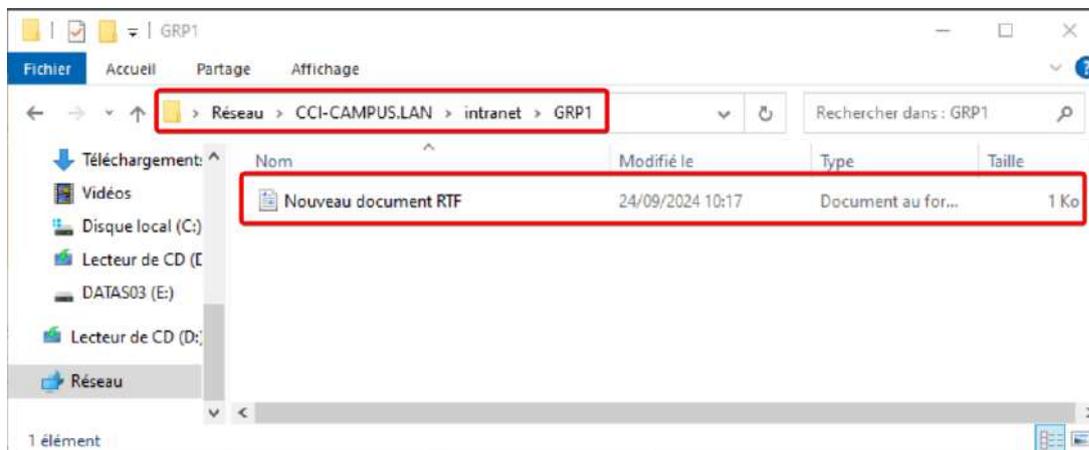


On peut ensuite cliquer sur suivant et créer. Si tout se passe correctement, nous devrions avoir un message de validation :



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 !

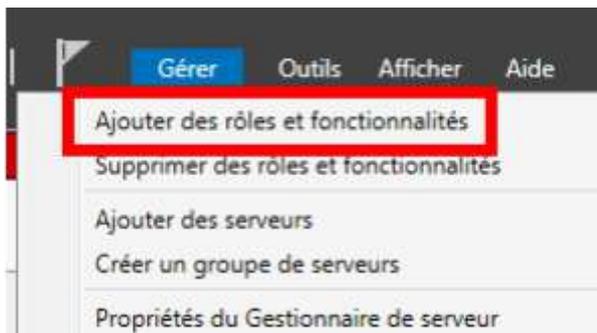
5.4) Déduplication des données

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

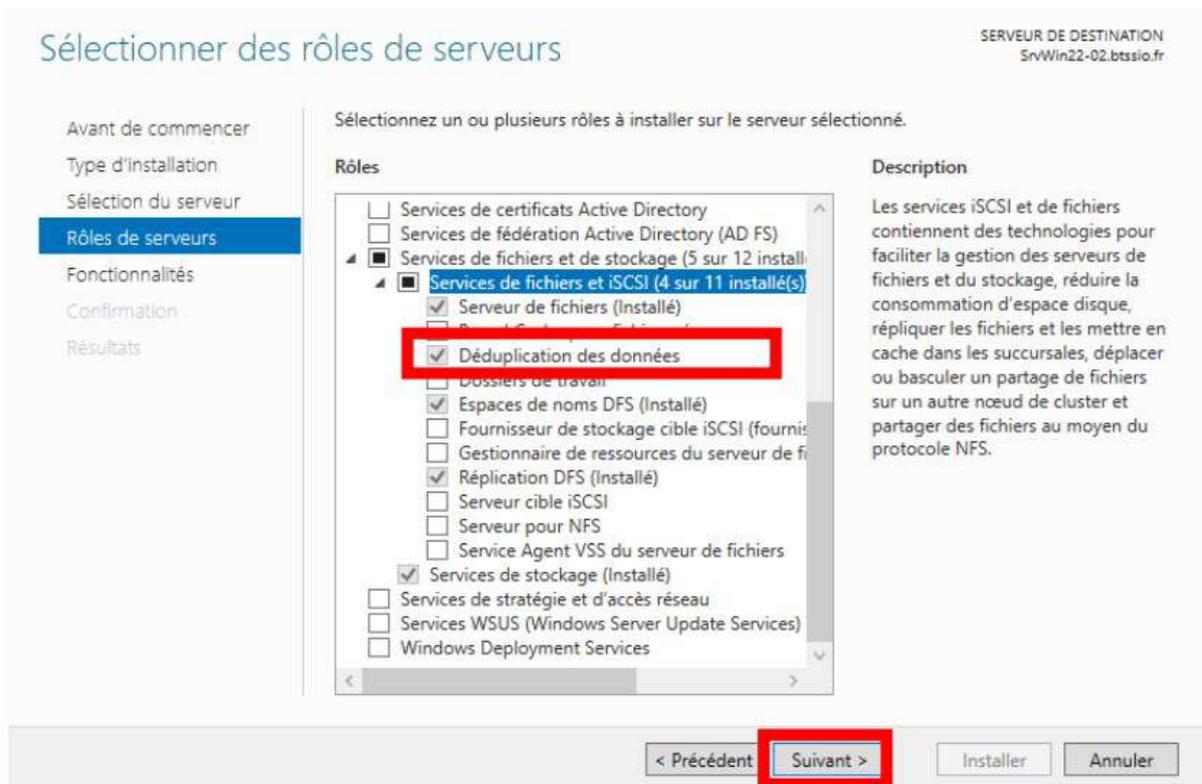
Selon Microsoft, le service de déduplication permettrait d' « obtenir des taux d'optimisation allant jusqu'à 95 % ou une utilisation du stockage divisée par 20 »

5.4.1) Installation et paramétrage du service de déduplication des données

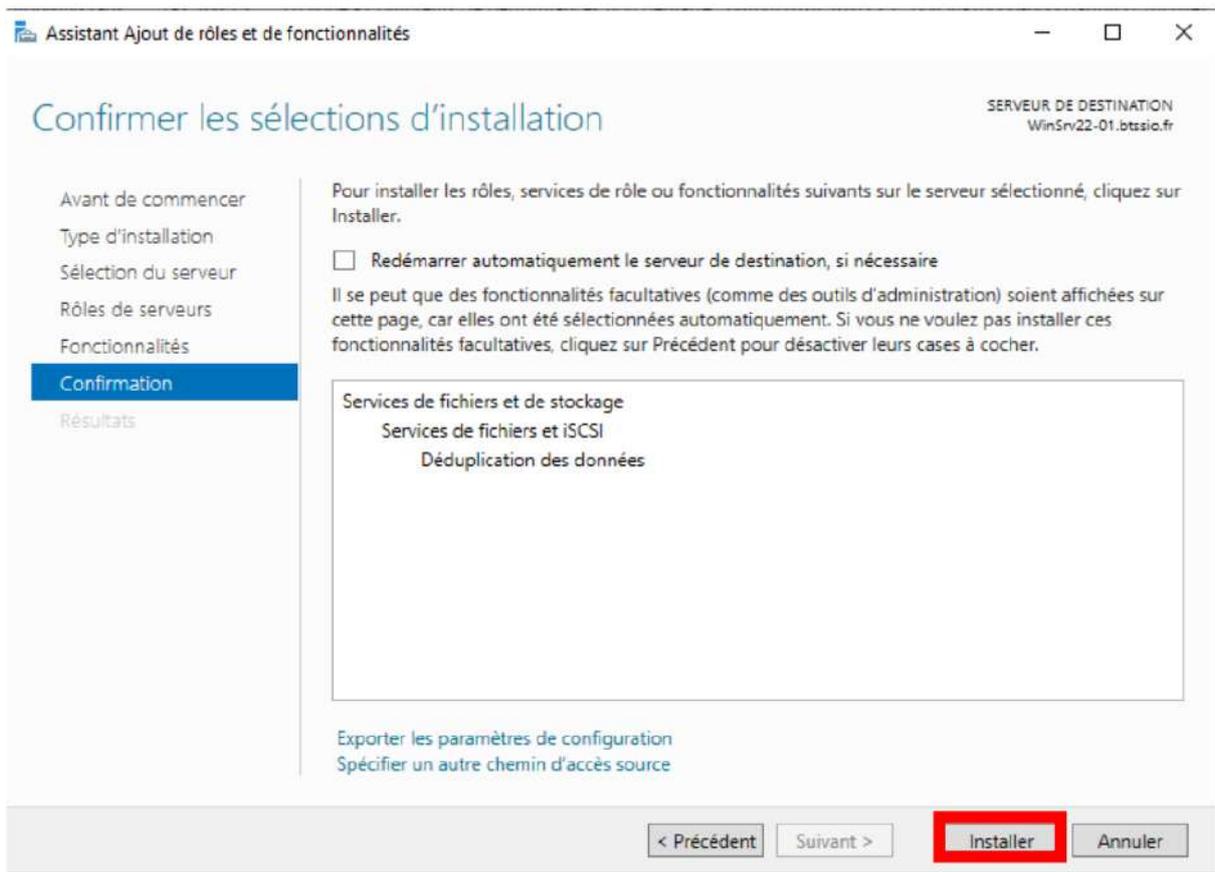
Il faut tout d'abord installer le rôle, dans Gérer sur le gestionnaire de serveur puis "Ajouter des rôles et fonctionnalités" :



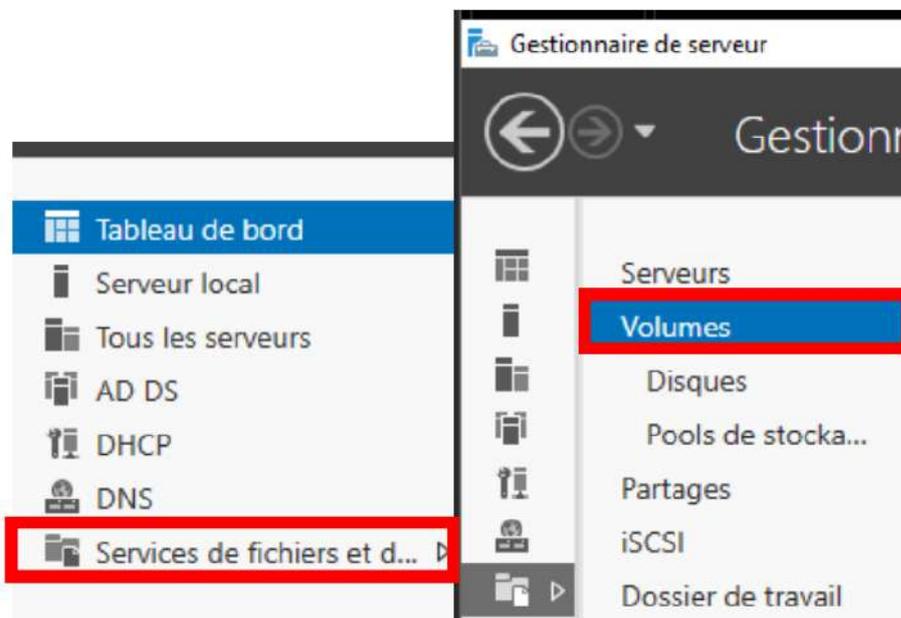
Ensuite, on coche "Déduplication des données" :



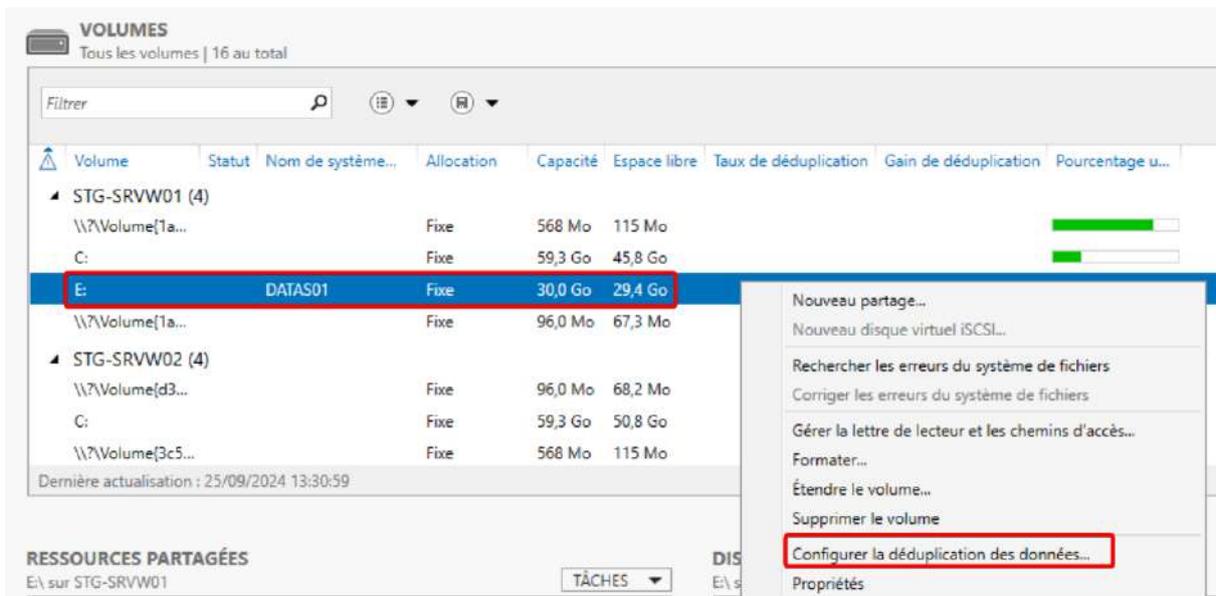
Puis on peut faire Suivant jusqu'à Installer :



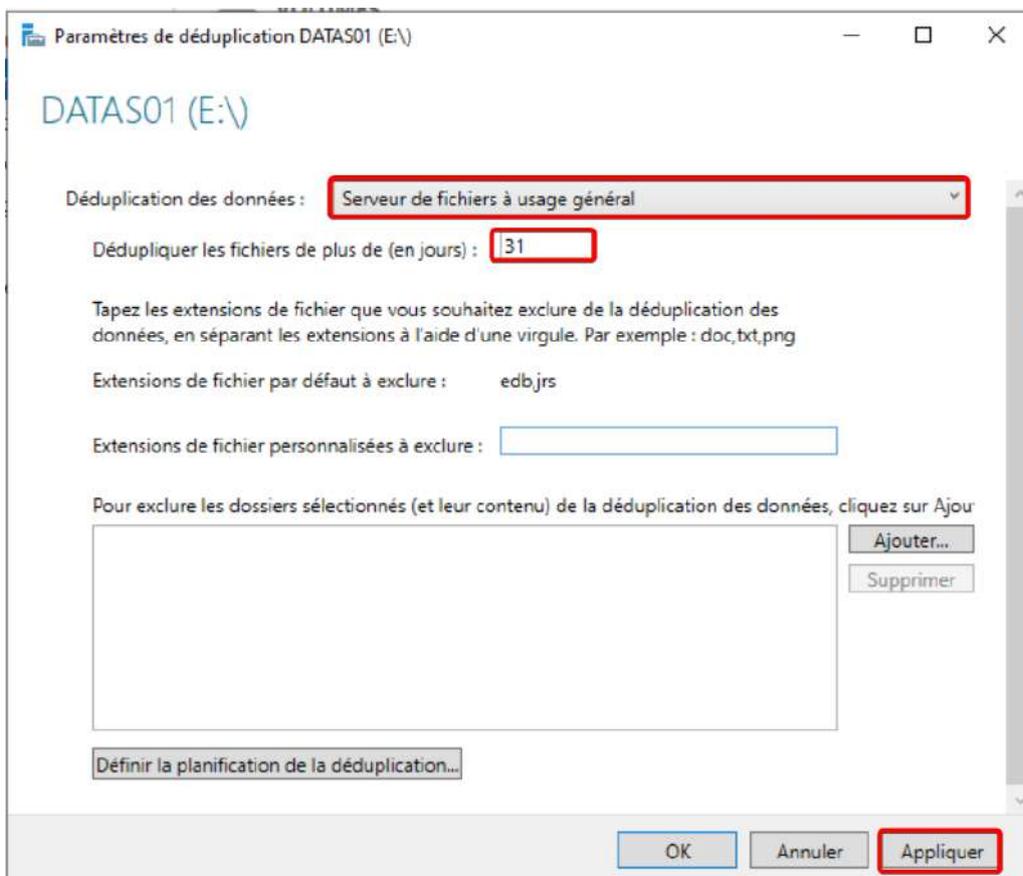
Depuis le gestionnaire de serveur, aller dans "Services de fichiers et de stockages" puis "Volumes"



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 :



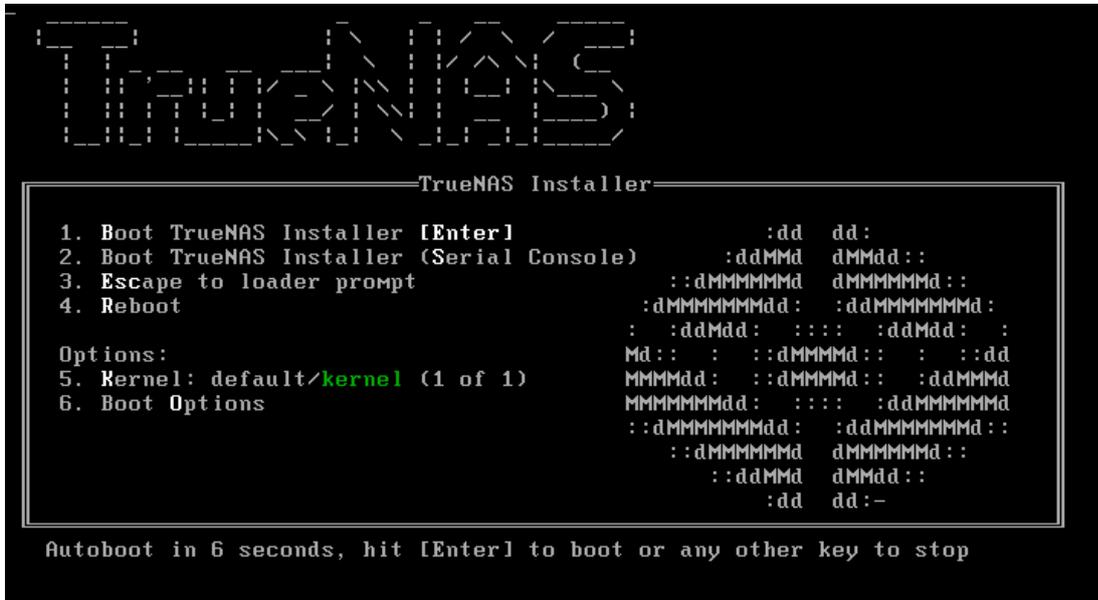
La déduplication est en place.

6) Montage d'une cible iSCSI avec TrueNAS Core

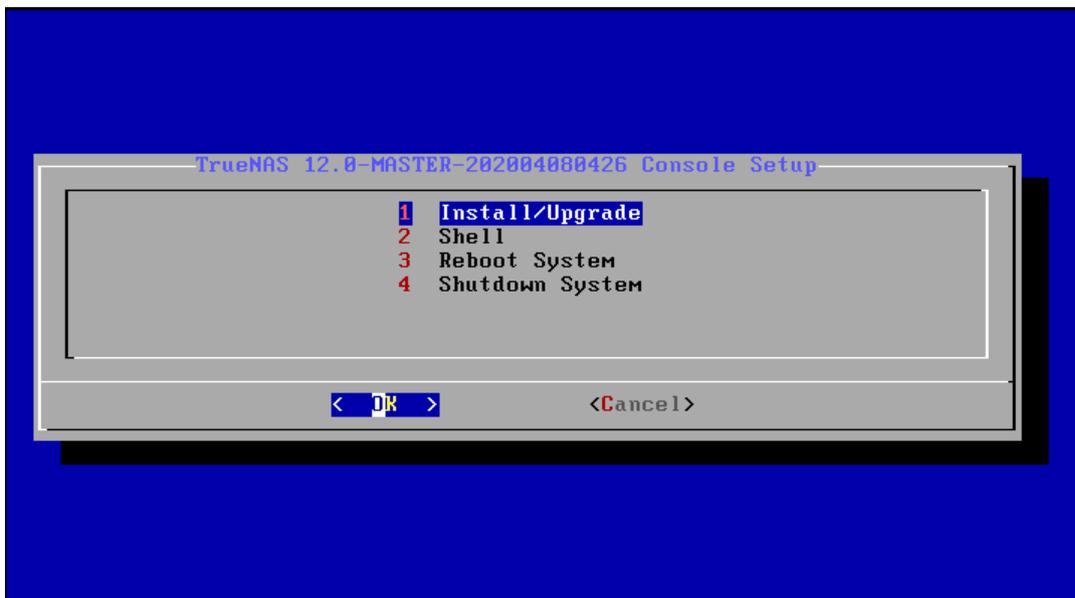
TrueNAS est une solution de NAS, basé sous FreeBSD 13.0, il existe en plusieurs versions (community/professionnel). Nous allons utiliser cette solution afin de réaliser une cible iSCSI pour faire une sauvegarde complète de nos Windows Serveurs.

6.1) Installation de TrueNAS

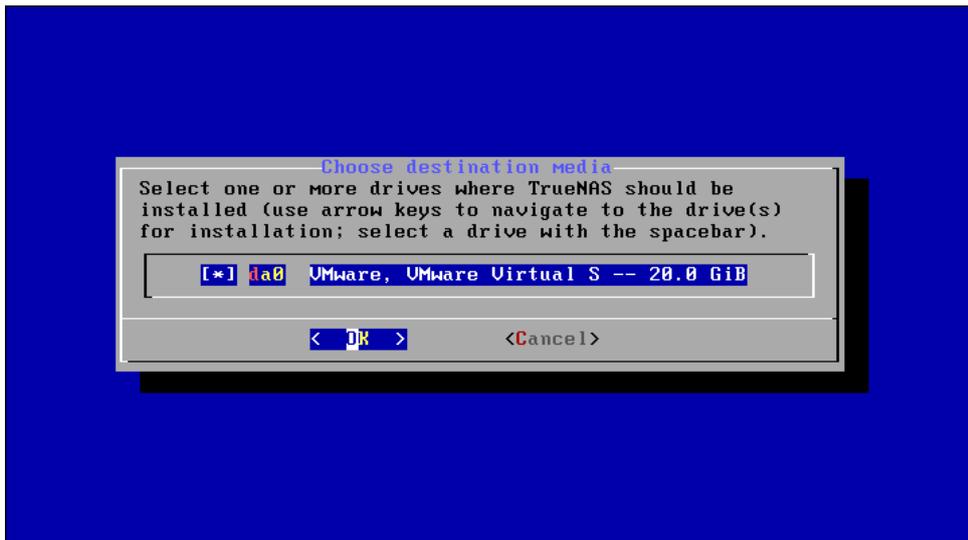
Pour commencer, il faut boot dans le TrueNAS Installer :



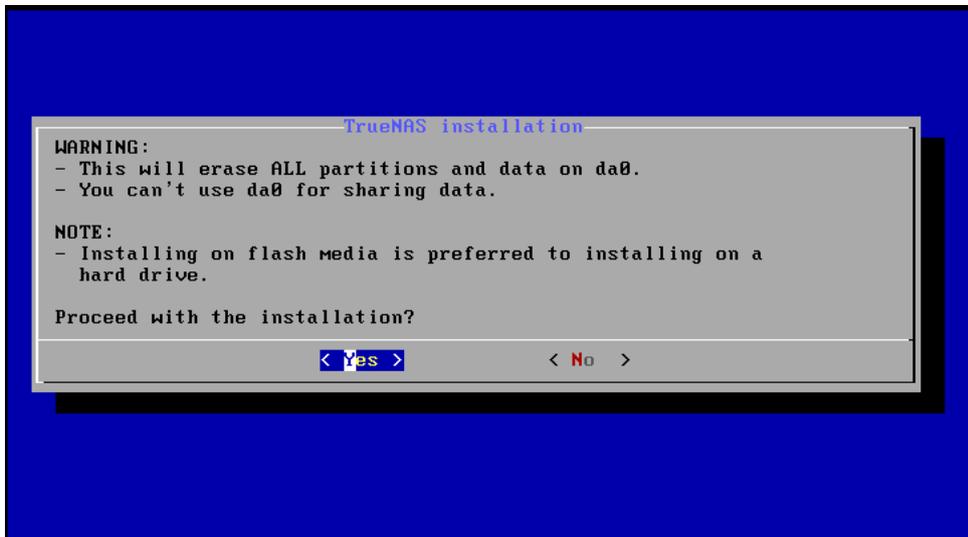
Ensuite, on sélectionne "Install/Upgrade" :



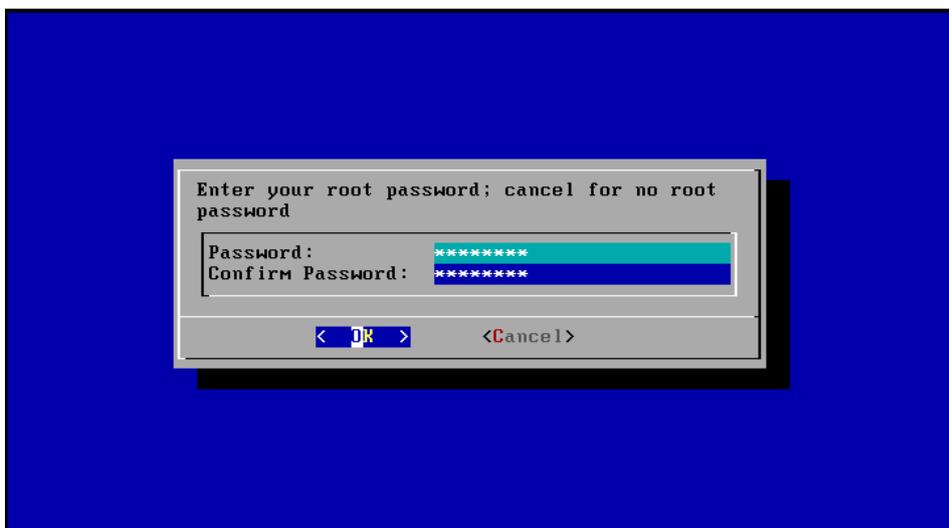
Puis on sélectionne notre disque sur lequel on souhaite installer TrueNAS :



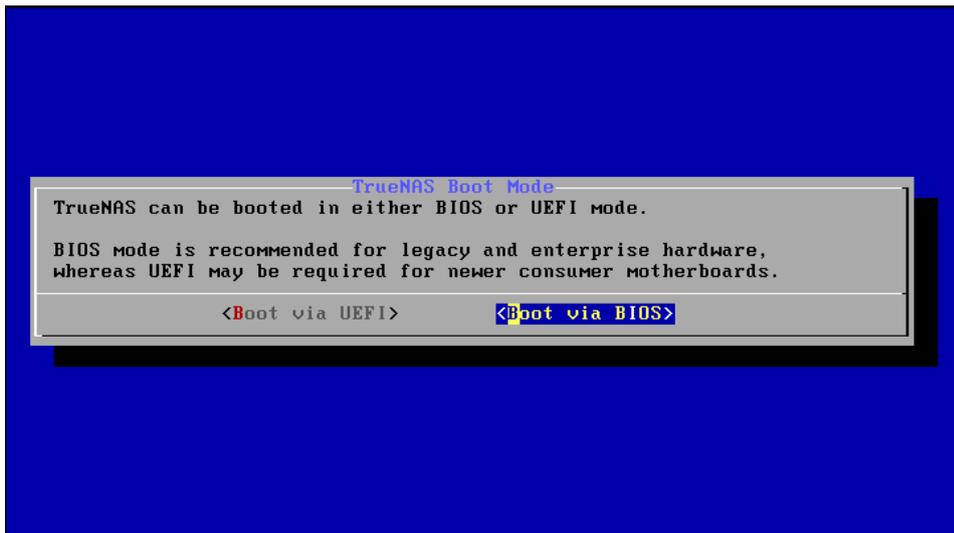
On accepte ensuite les modifications :



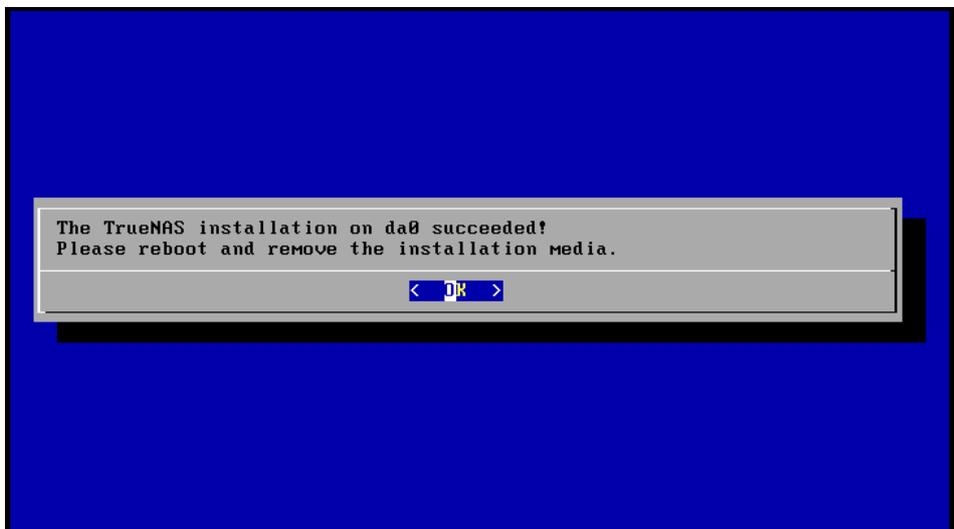
Il faut ensuite choisir le mot de passe root :



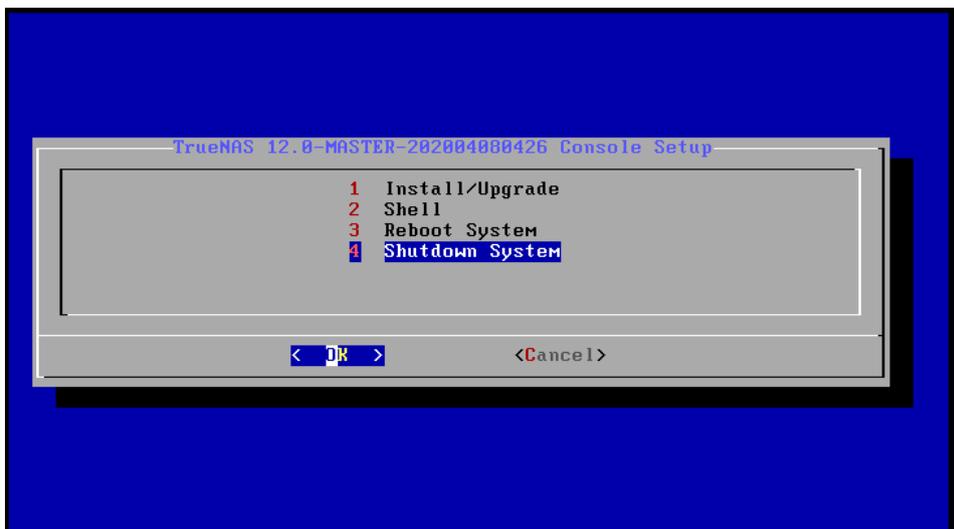
On peut boot via BIOS ou UEFI en fonction de nos besoins :



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 :

```
Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:
http://192.168.100.3
https://192.168.100.3

Enter an option from 1-11: 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 :

```
Enter an option from 1-11: 1
1) vtnet0
Select an interface (q to quit): 1
Delete interface? (y/n) n
Remove the current settings of this interface? (This causes a momentary disconn
ction of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name [192.168.100.3]: 192.168.100.3
Several input formats are supported
Example 1 CIDR Notation:
  192.168.1.1/24
Example 2 IP and Netmask separate:
  IP: 192.168.1.1
  Netmask: 255.255.255.0, /24 or 24
IPv4 Address [192.168.100.3]: 192.168.100.3/24
```

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 :

```
Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:
http://192.168.100.3
https://192.168.100.3

Enter an option from 1-11: 6
```

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

```
Enter an option from 1-11: 6
DNS Domain [cci-campus.lan]: cci-campus.lan
Enter nameserver IPs, an empty value ends input
DNS Nameserver 1 [192.168.100.1]: 192.168.100.1
DNS Nameserver 2 [192.168.100.2]: 192.168.100.2
DNS Nameserver 3: 
```

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

```
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:
http://192.168.100.3
https://192.168.100.3

Enter an option from 1-11: 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 :

```
Enter an option from 1-11: 4
Configure IPv4 Default Route? (y/n) y
IPv4 Default Route [192.168.100.254]: 192.168.100.254
Saving IPv4 gateway: Ok
Configure IPv6 Default Route? (y/n) n
```

La configuration réseau est maintenant terminée.

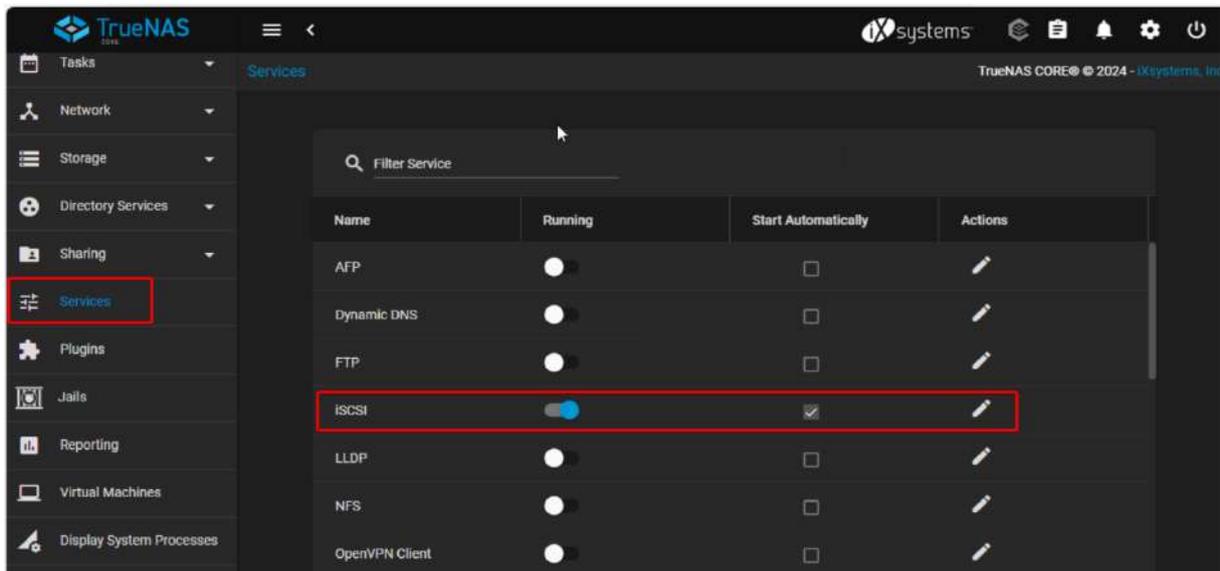
6.3) Configuration d'une cible iSCSI

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

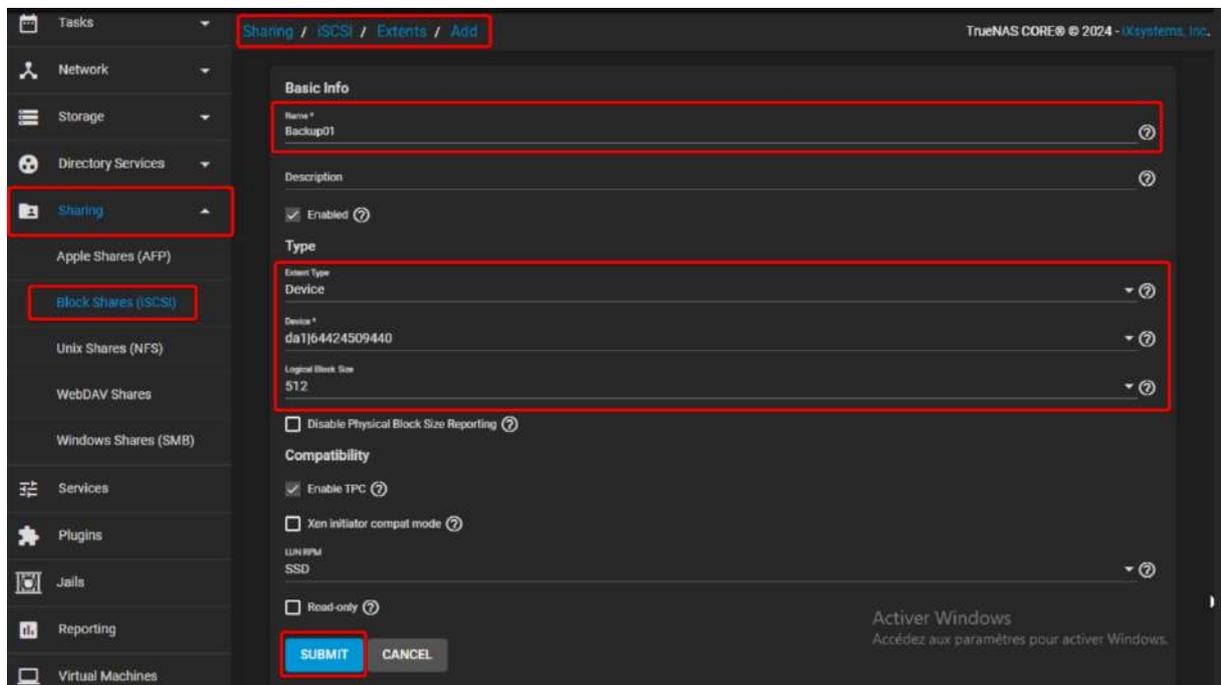
https://IP_NAS

Puis on se connecte avec les identifiants root.

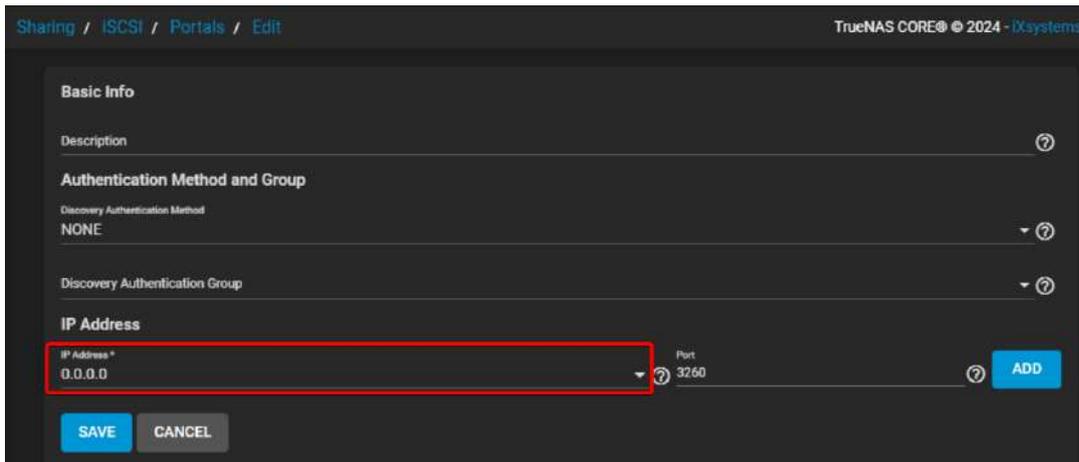
Il faut activer le service iSCSI, dans "Settings" :



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



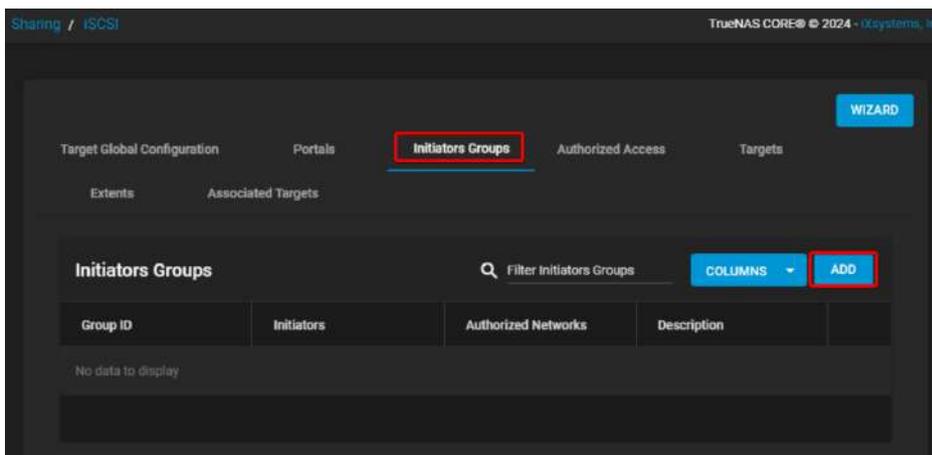
Il faut maintenant créer un "Portal", on vient mettre en adresse IP 0.0.0.0, ce qui signifie qu'il va écouter sur toutes les interfaces réseaux du NAS :



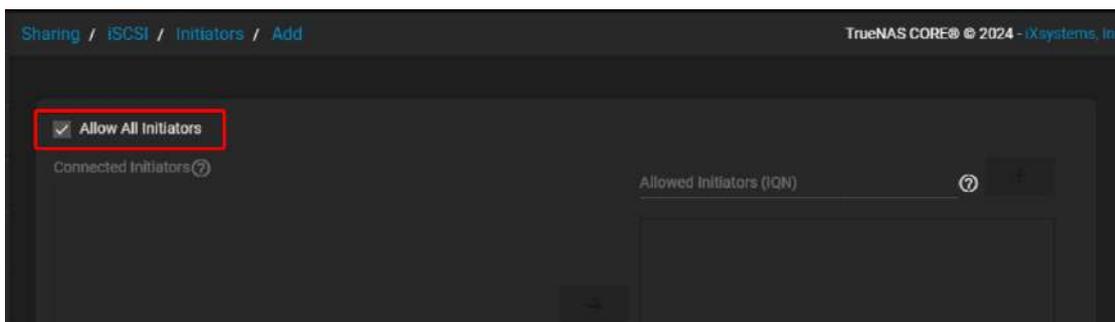
Info

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.

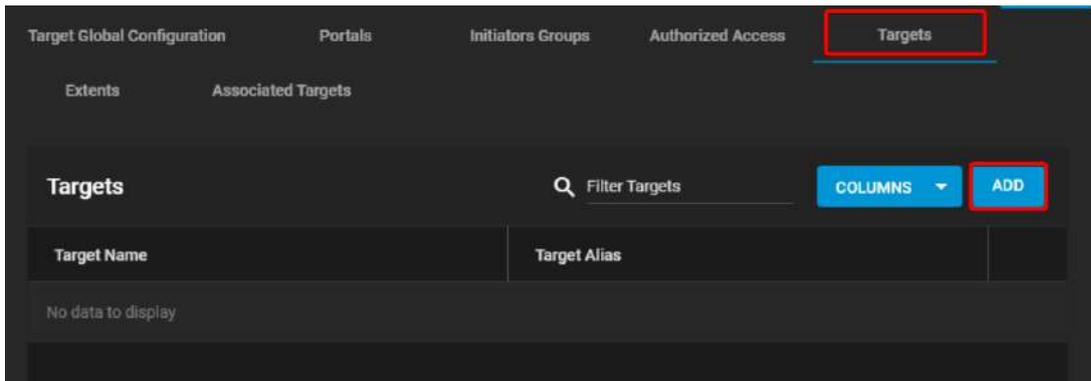
Ensuite, nous allons créer un "Initiators Groups" :



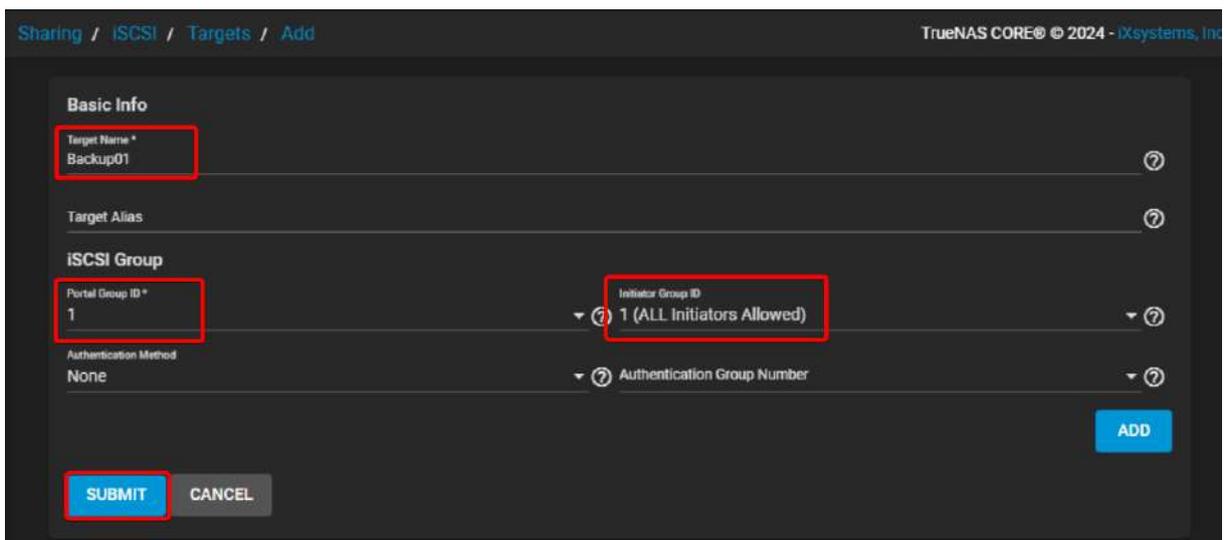
On coche la case "Allow All Initiators" pour autoriser tout le monde, on peut cliquer sur "Save" :



Puis, il faut créer une "Target" :

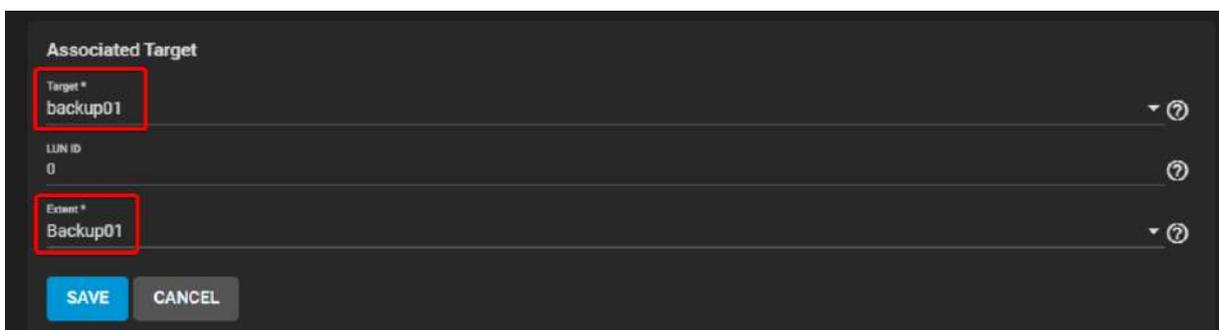


On va lui donner un Nom, le Portal Group ID qui correspond à celui créé précédemment et le Initiator Group ID créé aussi avant, on peut ensuite valider :



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.

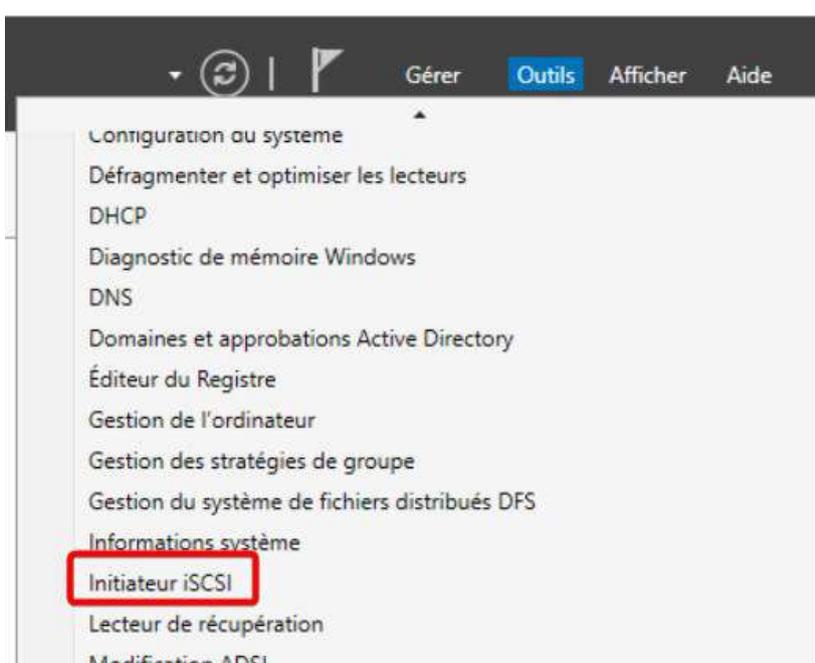
On sélectionne notre Target et notre Extent, puis on valide :



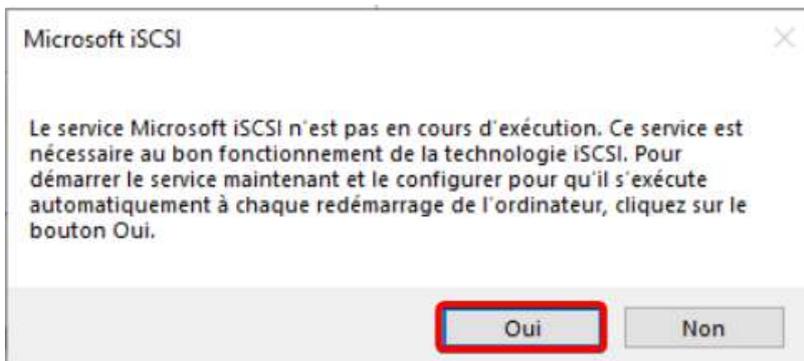
Notre cible iSCSI est maintenant détectable sur le réseau.

6.4) Connexion iSCSI depuis un Windows Serveur

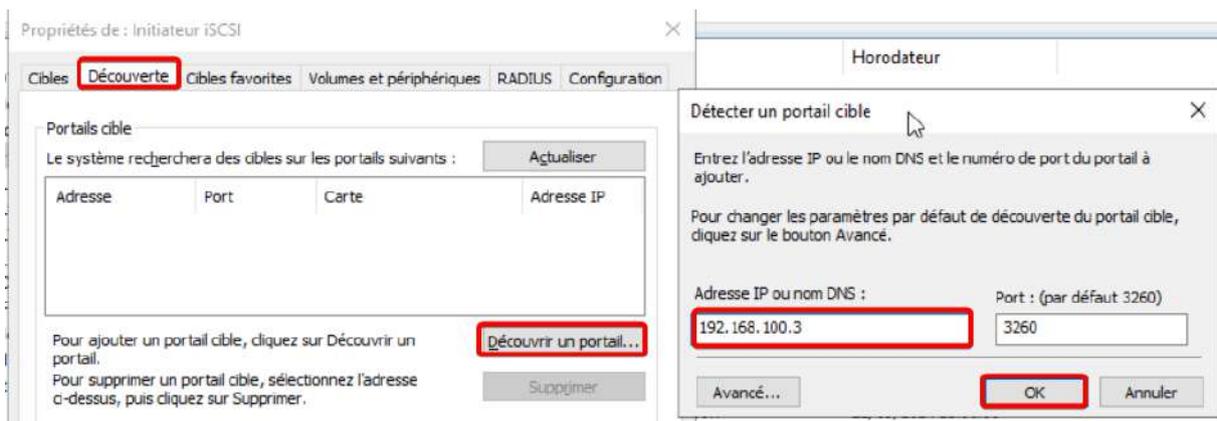
Tout d'abord, il faut ouvrir l'initiateur iSCSI depuis le gestionnaire de serveur :



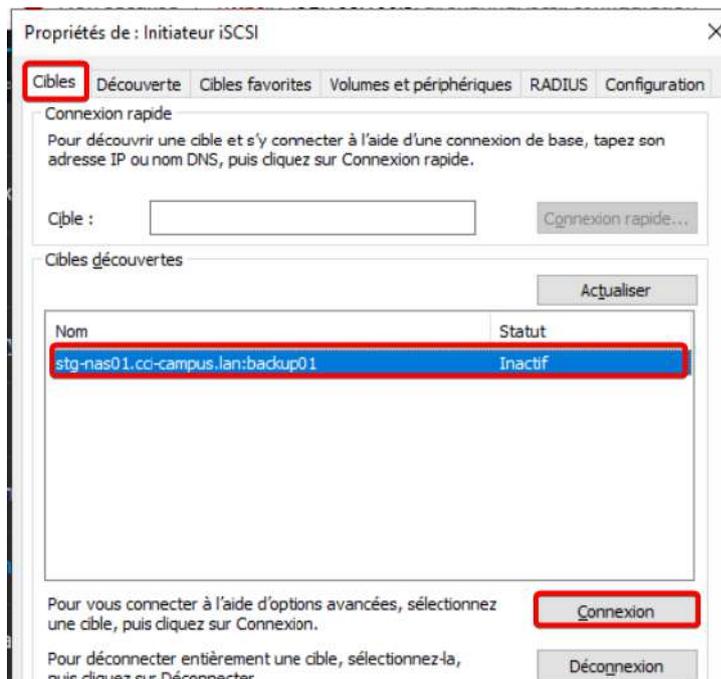
Un message nous demande d'activer le service iSCSI, on accepte :



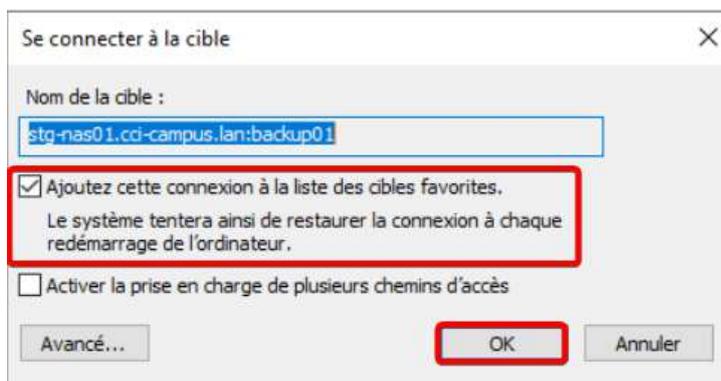
On va dans l'onglet "Découverte", puis on clique sur "Découvrir un portail...", il faut ensuite rentrer l'adresse IP ou le nom DNS de notre NAS et cliquer sur OK :



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



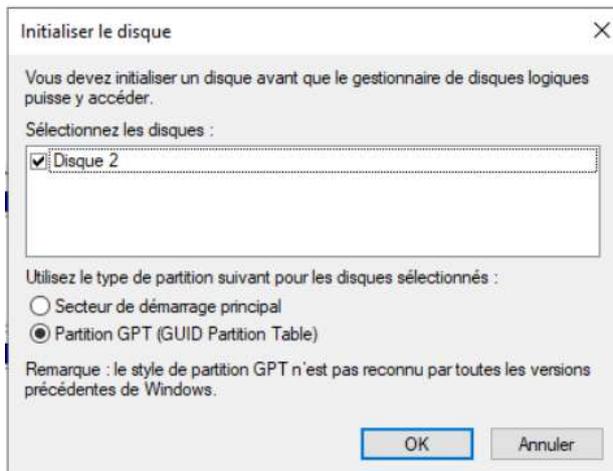
On ajoute la connexion à la liste des cibles favorites afin que la connexion persiste au redémarrage :



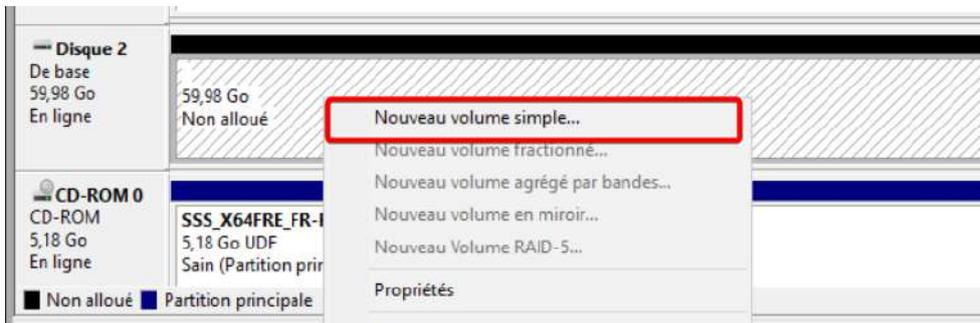
Une fois le disque monté il faudra l'initialiser et le formater correctement. Il faut aller dans la console de "Gestion des disques" et faire clique droit sur le nouveau disque, puis "Initialiser le disque" :



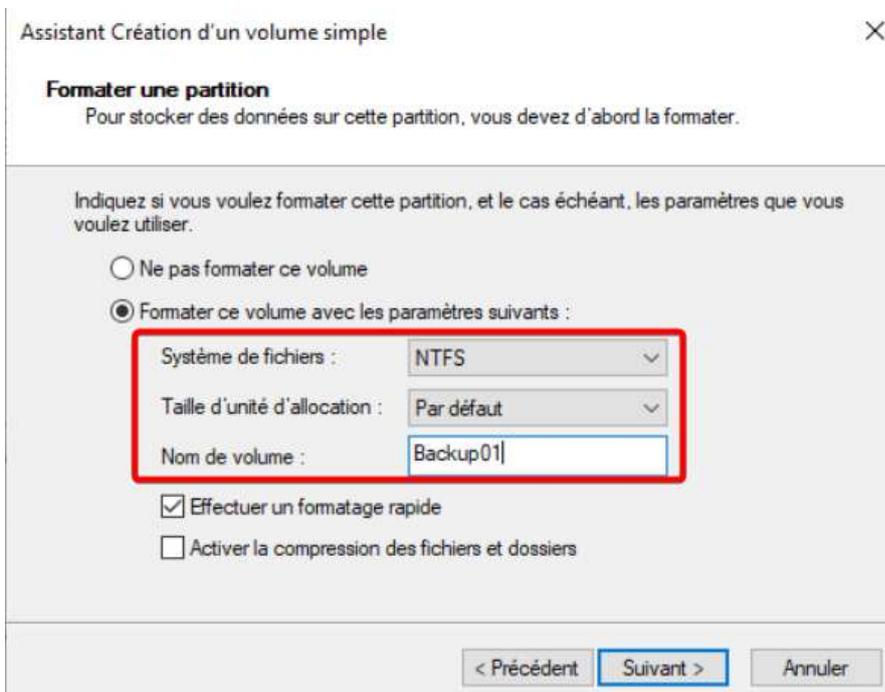
On sélectionne partition GPT (par défaut), puis on valide :



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



L'assistant Création d'un volume simple va s'ouvrir, 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 :

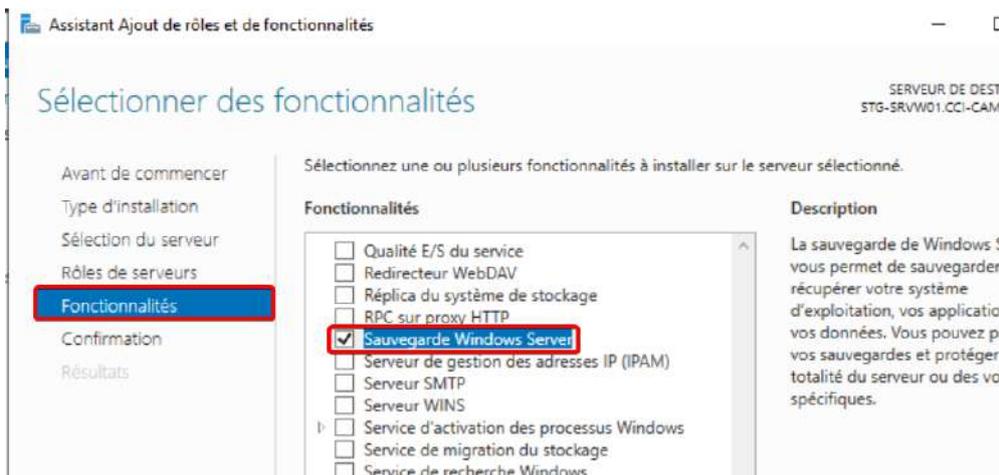


6.5) Configurer les sauvegardes Windows Serveur

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



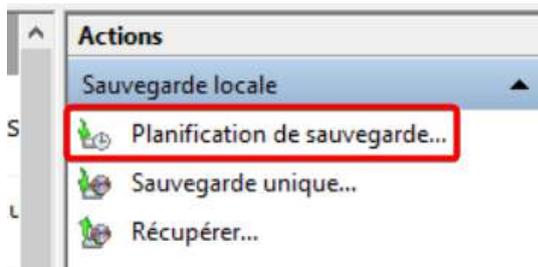
Ensuite, on peut se rendre dans la partie "Fonctionnalités" et cocher "Sauvegarde Windows Server":



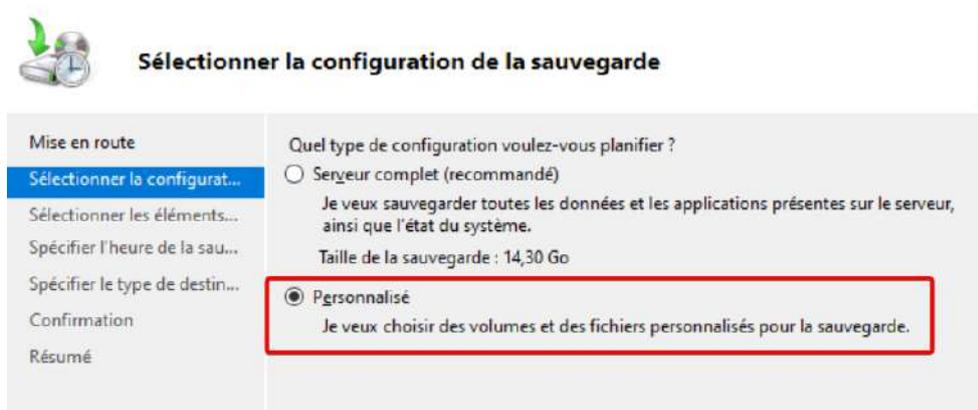
On peut ensuite ouvrir depuis le gestionnaire de serveur, l'outil Sauvegarde Windows Server :



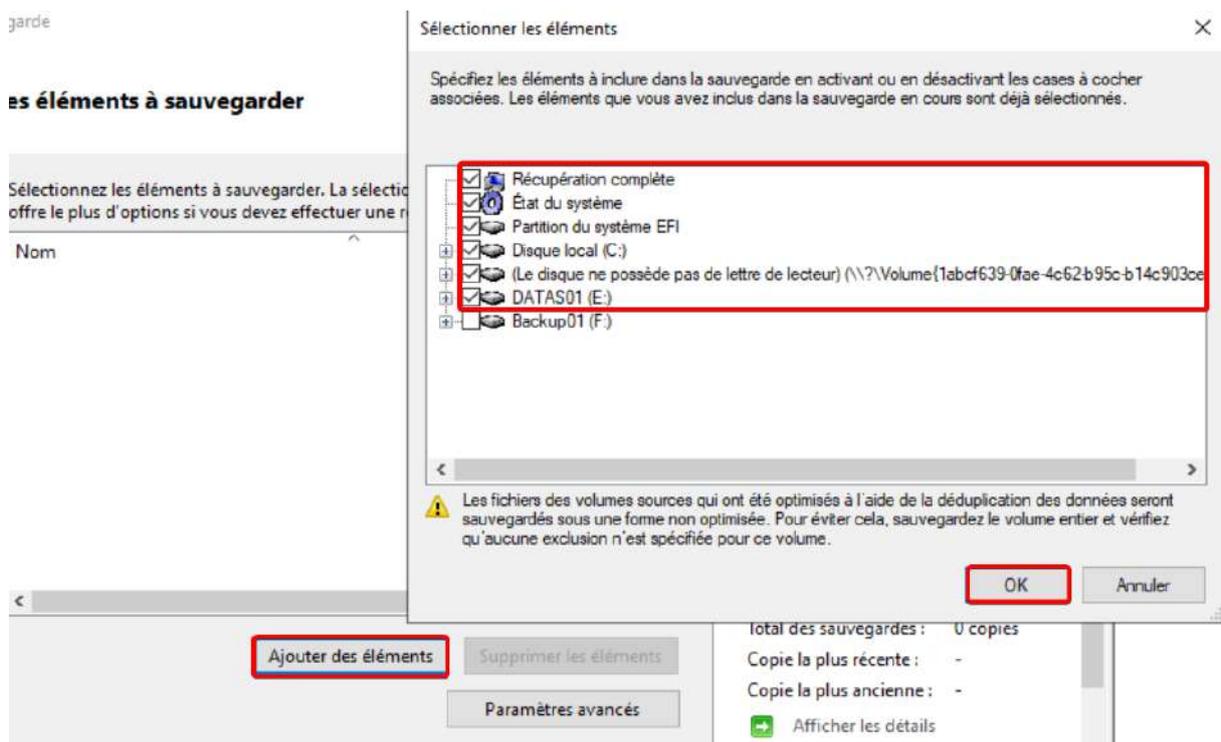
On clique ensuite sur "Planification de sauvegarde..." :



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 sélectionner la fréquence des sauvegardes :

Assistant Planification de sauvegarde

Spécifier l'heure de la sauvegarde

Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Confirmation
Résumé

À quelle fréquence et à quel moment voulez-vous exécuter les sauvegardes ?

Tous les jours
Sélectionnez une heure : 21:00

Plusieurs fois par jour
Cliquez sur une heure disponible, puis sur Ajouter pour l'ajouter à la planification de sauvegarde.

Temps disponible :
00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30

Ajouter >
< Supprimer

Heure planifiée :
21:00

< Précédent Suivant > Terminer Annuler

Enfin on sélectionne la première option :

Assistant Planification de sauvegarde

Spécifier le type de destination

Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Sélectionner le disque de ...
Confirmation
Résumé

Où voulez-vous stocker les sauvegardes ?

Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé)
Sélectionnez cette option pour stocker de la manière la plus sûre les sauvegardes. Le disque dur utilisé sera formaté, puis utilisé uniquement pour stocker les sauvegardes.

Sauvegarder vers un volume
Sélectionnez cette option si vous ne pouvez pas dédier tout un disque à la sauvegarde. Notez que cette option peut réduire les performances du volume de 200 pour cent durant le stockage des sauvegardes. Il est recommandé de ne pas stocker d'autres données de serveur sur le même volume.

Sauvegarder sur un dossier réseau partagé
Sélectionnez cette option uniquement si vous ne voulez pas stocker les sauvegardes sur le serveur lui-même. Notez que vous ne disposerez que d'une sauvegarde à la fois lorsque vous créez une nouvelle sauvegarde, car celle-ci remplace la précédente.

< Précédent Suivant > Terminer Annuler

Et on sélectionne enfin notre disque iSCSI :



Sélectionner le disque de destination

Mise en route
Sélectionner la configurat...
Sélectionner les éléments...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Sélectionner le disque de ...
Confirmation
Résumé

Sélectionnez un ou plusieurs disques pour stocker vos sauvegardes. Vous pouvez utiliser plusieurs disques de sauvegarde si vous souhaitez stocker des disques hors site.

Disques disponibles :

Disque	Nom	Taille	Espace uti...	Volumes prés...
<input checked="" type="checkbox"/>	2	TrueNAS iS...	60,00 Go	110,60 Mo F:\

Afficher tous les disques disponibles...

< Précédent **Suivant >** Terminer Annuler

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

6.6) Configurer les Shadow copies

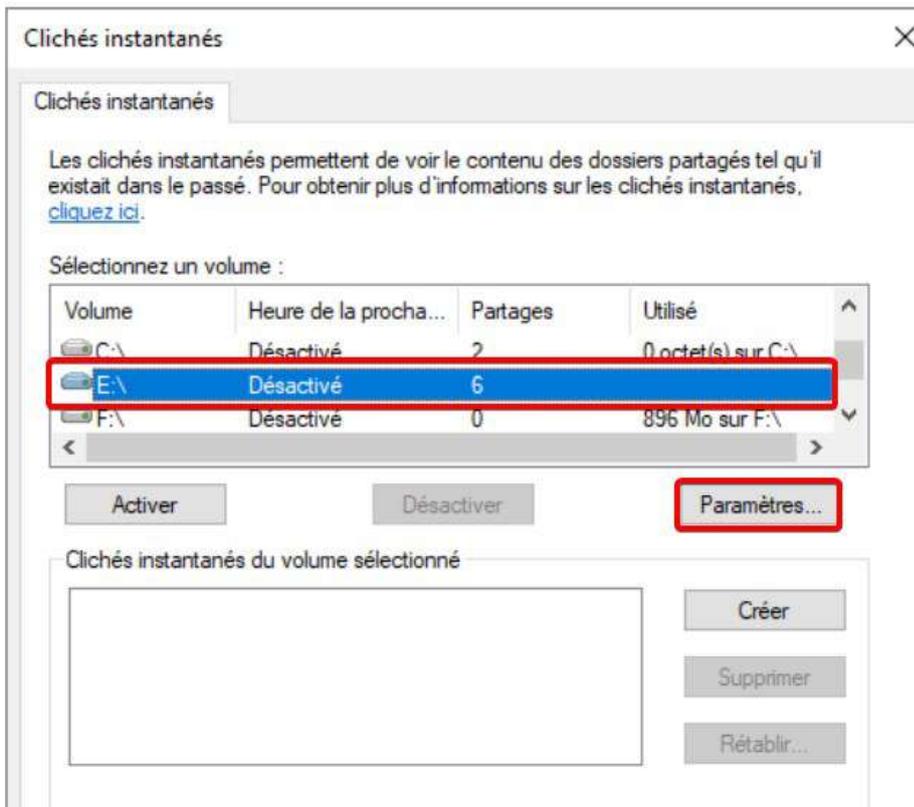
Les Shadow copies ou clichés instantanés, permettent de faire un snapshot d'un disque. Elles peuvent être pertinentes pour des dossiers partagés, et sont très simple à restaurer.

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

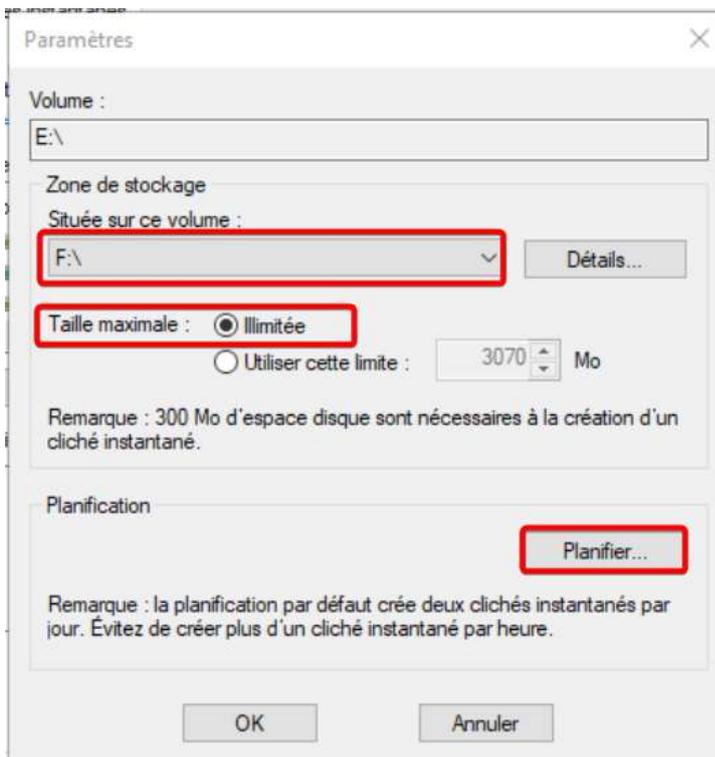
Bureau
Documents
Images
Musique
Objets 3D
Téléchargement
Vidéos
Disque local (C:)
Lecteur de CD (D:)
DATAS01 (E:)

Configurer les clichés instantanés...
Restaurer les versions précédentes
Inclure dans la bibliothèque >
Épingler à l'écran de démarrage
Formater...
Copier
Renommer
Nouveau >
Propriétés

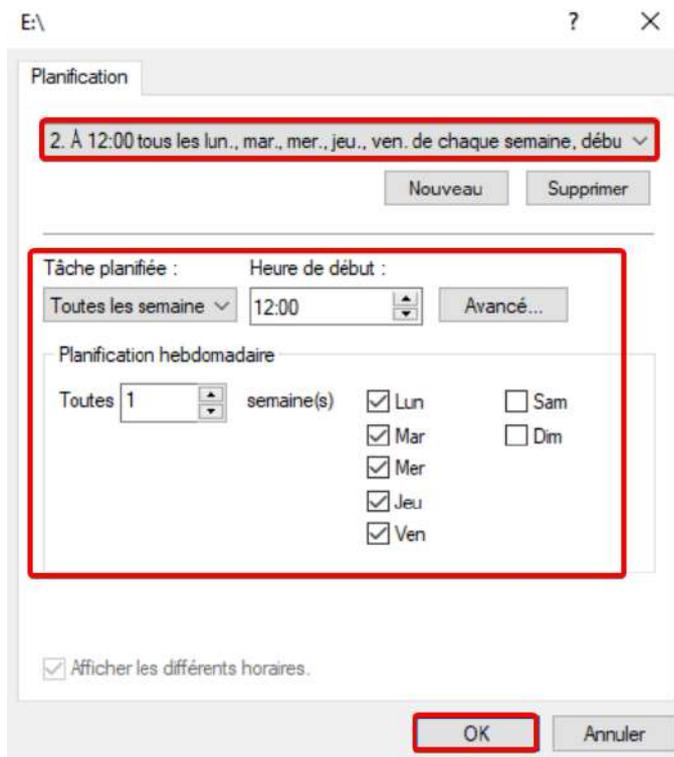
Puis il faut sélectionner le disque et cliquer sur "Paramètres..." :



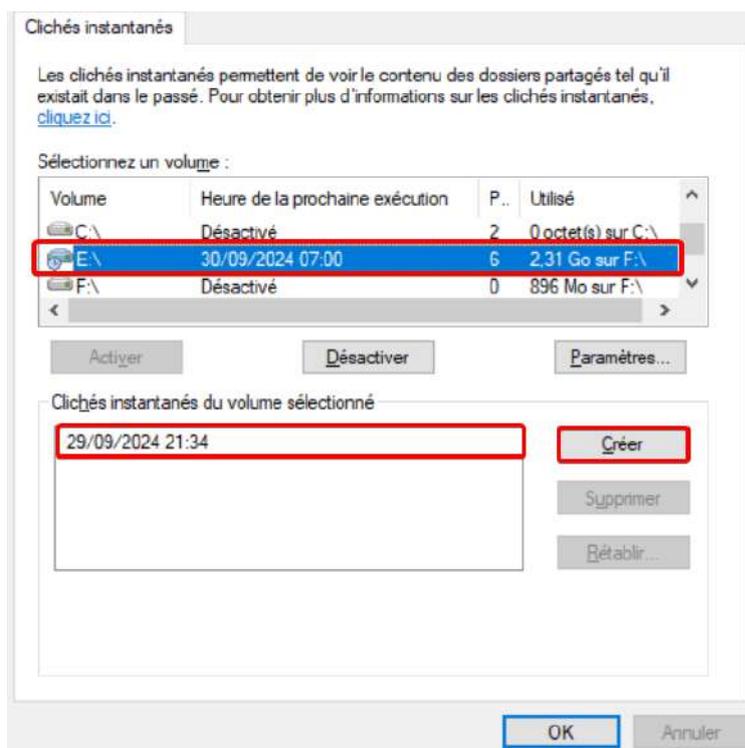
Ensuite, on sélectionne le volume sur lequel on souhaite enregistrer les Shadow copies (dans notre cas F), on met la taille maximal en illimitée et on peut cliquer sur "Planifier..." :



Puis, on choisit 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