

FEVRE Dan Projet M2i

Epreuve E5

-
Documentation technique situation 1

1) RESUME DU PROJET	3
1.1) Rappel des objectifs fixés	3
2.1) Planning prévisionnel VS Planning réel	3
2.2) Ressources prévues VS Ressources utilisées	6
2.3) Problèmes rencontrés et solutions apportées ou envisagées	8
3) RESULTATS	8
3.1) Résultats attendus VS Résultats obtenus.....	8
4) ANALYSE FINALE	8
4.1) Analyse et état finale du projet.....	8
4.2) Améliorations possibles.....	8
5) CONCLUSION	9
6) DOCUMENTATION TECHNIQUE	9
6.1) Serveur Windows 2019 GUI.....	9
6.2) Serveur Windows 2019 CORE.....	51
6.3) PFSense, VPN, Portail Captif	80
6.4) TRUENAS.....	123
6.5) Sauvegarde et SHADOWCCOPY.....	135

1) RESUME DU PROJET

1.1) Rappel des objectifs fixés

La CCI nous a sollicité pour la mise en place de 2 salles informatiques pour son nouveau cursus M2i à Strasbourg et Mulhouse selon les caractéristiques suivantes :

- Chaque salle doit comporter 1 routeur/pare-feu, 2 serveurs redondés (AD, DHCP, DNS, DFS, DFS-R, RADIUS).
- La mise en place d'un VPN site à site (IPSEC avec protocole ESP) a également été demandé ainsi qu'un serveur de sauvegarde/NAS (iSCSI).
- Etude du projet et réponse au cahier des charges (planning, coûts...)
- La mise en œuvre d'une liaison WAN inter-sites chiffrée
- Harmoniser le plan d'adressage et de nommage sur l'ensemble des sites
- Création de serveurs et rôles/services suivants en haute disponibilité :
- Mise en œuvre d'un portail-captif avec authentification forte (Identification à l'AD via RADIUS)
- Accès aux données stockant les dossiers personnels des enseignants et des élèves à partir des 2 sites.

2) CONDUITE DU PROJET

2.1) Planning prévisionnel VS Planning réel

Pour ce qui est de la partie du livrable 1, les dates sont sensiblement les mêmes sans changements majeur. La partie 2, en revanche a subit quelques changements. Comme vous pouvez le constater sur les diagrammes de GANTT à la suite, J'ai commencé les installations des machines virtuelles avec une semaine d'avance. À la suite de certains problèmes rencontrés qui seront décrit dans la partie adéquate, J'ai également pris un peu de retard pour la fin de la réalisation.

Diagramme Prévisionnel

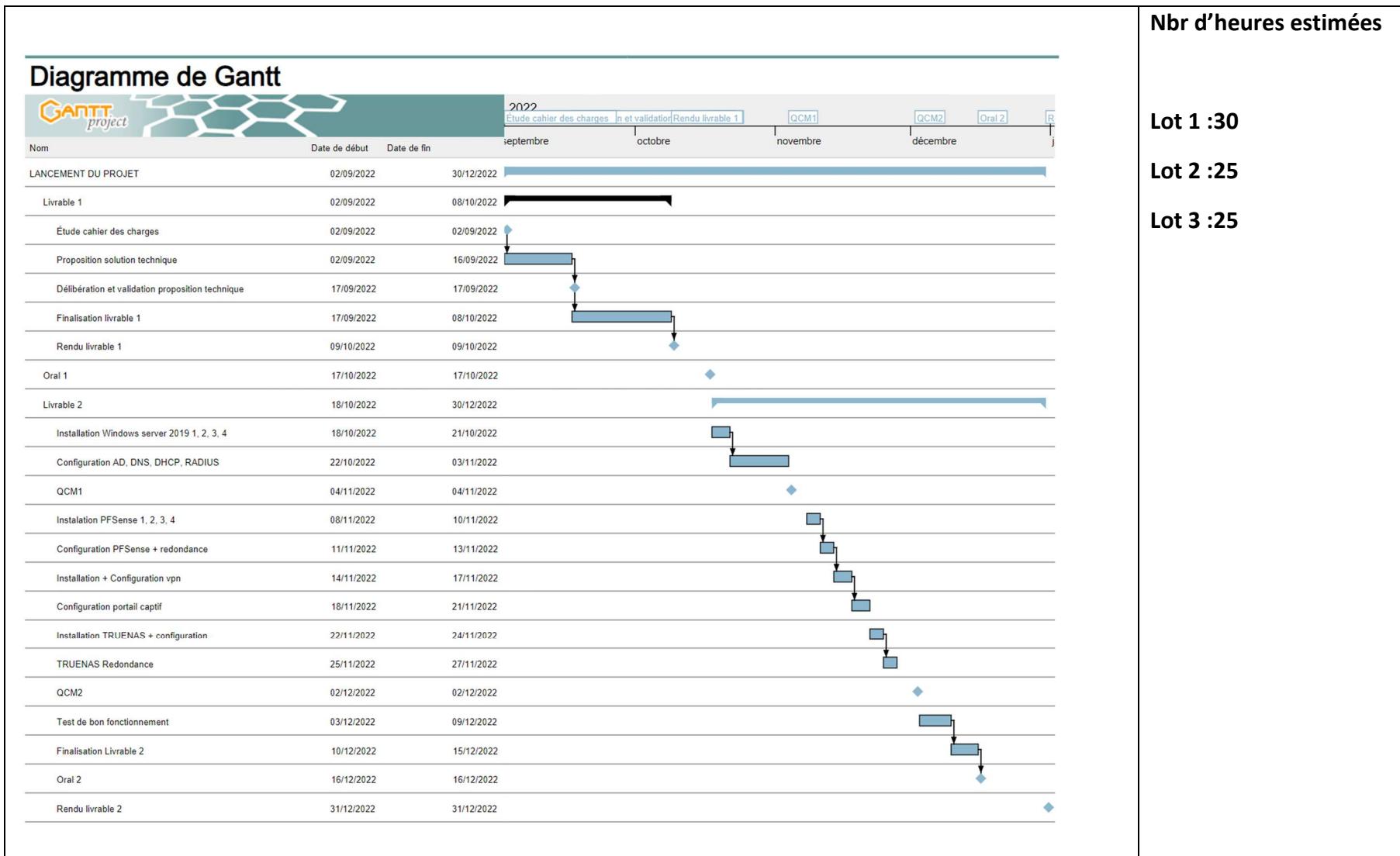
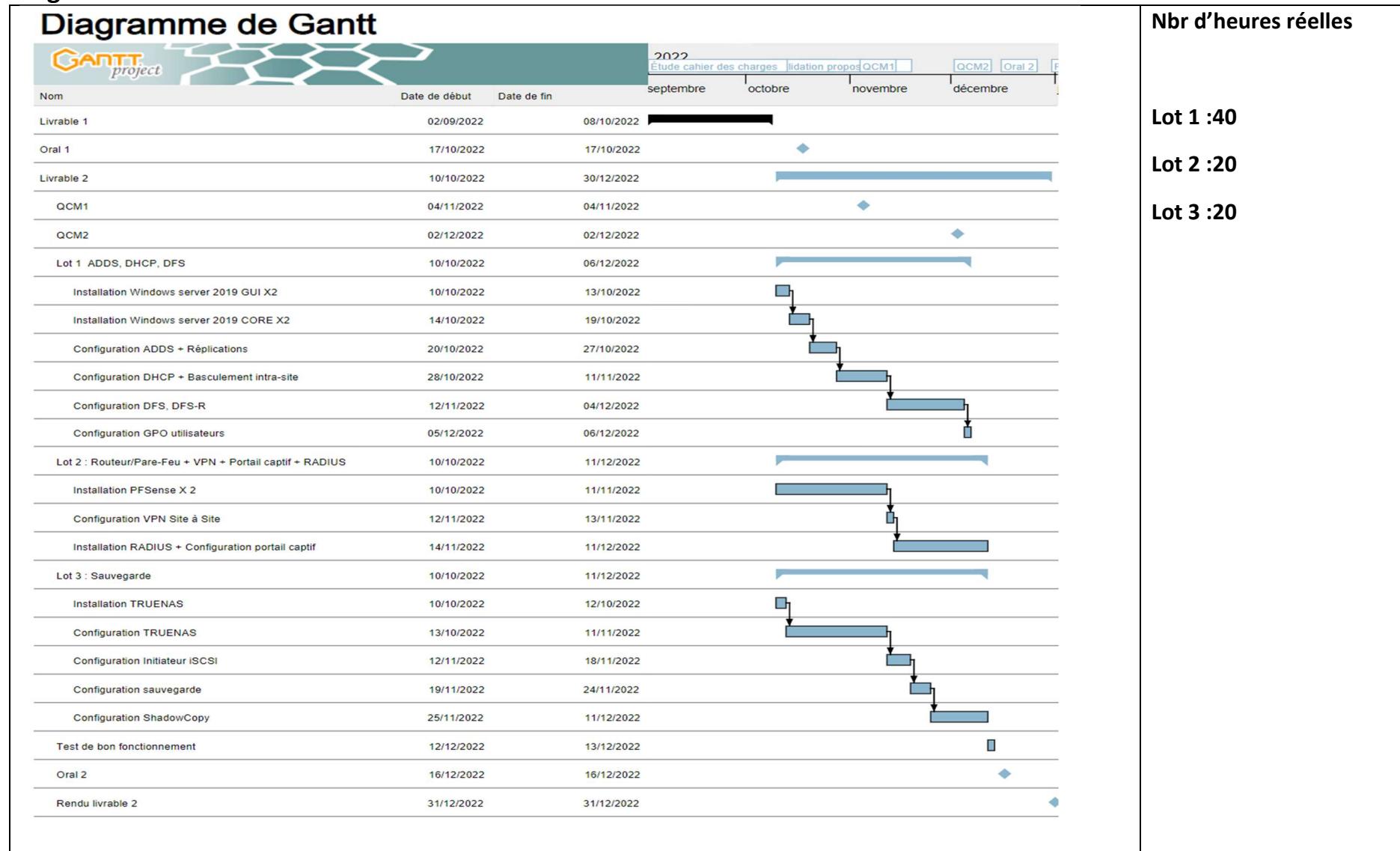


Diagramme Réel



2.2) Ressources prévues VS Ressources utilisées

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
4	Serveur Dell PowerEdge T140 (5JV1T) Intel Xeon E-2224G, 16 Go, 1 To, Graveur DVD - Serveur AD	-	879,95€	3 519,80€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - Serveur PFSense / VPN	-	1 023,95€	2 047,90€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - Serveur Sauvegarde TrueNAS	-	1 023,95€	2 047,90€
2	Onduleur APC Back-UPS Pro 1500VA - 6 Prises - Onduleur STR - Onduleur MLS	-	367,96€	735,92€
2	Switch Cisco CBS110-24T 22 ports 10/100/1000 Mbps + 2 ports combo Ethernet Gigabit/SFP	-	191,15€	382,30€
4	Licence Microsoft Windows Server Standard 2019 (16 Coeurs) 64 Bits	-	799,96€	3199,84€
8	Iiyama ProLite T2252MSC-B1 - Écran LED - 22" 1920 x 1080 Full HD - 60 Hz	-	247,99€	1 983,92€
8	Clavier HP K1500	-	21,58€	172,64€
8	Souris filaire HP X900	-	3,19€	25,52€
1	Contrat de maintenance Durée : 1an (24h24 7J/7)	-		
80	Main d'œuvre pour réalisation	-	119,99€	9 599,20€
TOTAL HT			23 714,94€	
TVA 20%			4 742,99€	
Total TTC			28 457,93€	
Net à payer			28 457,93€	

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
60	HP ProDesk 400 G4 MT - Core i5-7500 3,4 GHz - 8 Go - SSD 256 Go	-	207,99€	12 479,40€
60	Ecran HP 22" LED - VH22 (XON05AA) 1920x1080 px - 5 ms - VGA/DVI-D/DisplayPort	-	111,20€	6 672,00€
90	HP ProBook 450 G8 - Windows 10 Famille 64 bits, 15,6 HD, i3, 8 Go, 256 Go SSD	-	480,00€	43 200,00€
TOTAL HT			62 351,40€	
TVA 20%			12 470,28€	
Total TTC				74 821,68€
Net à payer				74 821,68€

Devis initial

Devis Interne	28 457,93 €	
Devis Externe	74 821,68 €	
Total TTC		103279,61€
Net à payer		103279,61€

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
4	Serveur Dell PowerEdge T140 (5JV1T) Intel Xeon E-2224G, 16 Go, 1 To, Graveur DVD - Serveur AD	-	879,95€	3 519,80€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - Serveur pfSense / VPN	-	1 023,95€	2 047,90€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - Serveur Sauvegarde TrueNas	-	1 023,95€	2 047,90€
2	Onduleur APC Back-UPS Pro 1500VA - 6 Prises - Onduleur STR - Onduleur MLS	-	367,96€	735,92€
2	Switch Cisco CBS110-24T 22 ports 10/100/1000 Mbps + 2 ports combo Ethernet Gigabit/SFP	-	191,15€	382,30€
4	Licence Microsoft Windows Server Standard 2019 (16 Coeurs) 64 Bits	-	799,96€	3199,84€
8	Tivama ProLite T2252MSC-B1 - Écran LED - 22" 1920 x 1080 Full HD - 60 Hz	-	247,99€	1 983,92€
8	Clavier HP K1500	-	21,58€	172,64€
8	Souris filaire HP X900	-	3,19€	25,52€
1	Contrat de maintenance Durée : 1an (24h/24 7j/7)	-		
60	Main d'œuvre pour réalisation	-	119,99€	9 599,20€
TOTAL HT			23 714,94 €	
TVA 20%			4 742,99 €	
Total TTC			28 457,93 €	
Net à payer			28 457,93 €	

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
60	Ecran HP 22" LED - VH22 (X0N05AA) 1920x1080 px - 5 ms - VGA/DVI-D/DisplayPort	-	111,20€	6 672,00€
90	HP ProBook 450 G8 - Windows 10 Famille 64 bits, 15,6 HD, i3, 8 Go, 256 Go SSD	-	480,00€	43 200,00€
90	Licence CAL 1/User	-	40,00€	4500,00€
90	Licence CAL 1/Device	-	32,00€	3600,00€
TOTAL HT			54 357,12 €	
TVA 20%			13 589,28 €	
Total TTC			67 946,40 €	
Net à payer			67 946,40 €	

Devis réajusté

Devis Interne	28 457,93 €	
Devis Externe	67 946,40 €	
Total TTC		96 404,33€
Net à payer		96 404,33€

2.3) Problèmes rencontrés et solutions apportées ou envisagées

Problèmes rencontrés	Solution apporté
Impossibilité d'installer un serveur RADIUS sur un WINDOWS 2019 CORE	Les serveurs RADIUS ont été installé uniquement sur le serveur WINDOWS GUI
Plus de synchronisation AD	Utilisation de la commande : repadmin /syncall /AdeP
Erreur Kerberos	Désactiver service kerberos (menu démarrer, outils d'administration windows, services puis centre de distribution de clés Kerberos puis le désactiver et stopper le démarrage auto) Cmd : netdom resetpwd /s:server2 /ud:mydomain\administrator /pd:* (ex : netdom resetpwd /s:SRV-STG01 /ud:CCI-CAMPUS.LAN\Administrateur /pd:*)
Problème pour rejoindre un domaine AD	Vérifier la config réseau et mettre le serveur AD en dns
Serveur AD plus disponible dans le gestionnaire de serveur	Idem au-dessus

3) RESULTATS

3.1) Résultats attendus VS Résultats obtenus

La difficulté de bien scinder le projet m'a coûté un bon moment d'organisation. De même que les séances en autonomie. Il a été décidé de faire le projet en intégralité par chaque membre du groupe malheureusement il est dur de trouver la même détermination chez chaque personne. Les aléas de la vie peuvent empêcher le bon fonctionnement de ce genre de projet. J'estime que notre projet est viable à 100 %, et totalement conforme au cahier des charges mais également aux demandes facultatives du client.

4) ANALYSE FINALE

4.1) Analyse et état finale du projet

Si vous représentez le client, au vu de la note que j'ai obtenus à la démonstration technique, je peux affirmer que le projet est une réussite. Même si le délai diffère quelque peu du prévisionnel, tout a été fait dans les temps et de manière travaillée et sérieuse.

4.2) Améliorations possibles

Il est effectivement possible d'améliorer légèrement le projet. Je vais vous lister mes propositions :

- La mise en place d'un VPN road warrior
- L'ajout d'un pfSense en plus sur chaque site pour assurer la haute disponibilité.
- La mise en place d'un RAID sur les serveurs Windows
- Une configuration stricte des règles du pare-feu
- La mise en place d'un DMZ + une solution cloud pour la sauvegarde

5) CONCLUSION

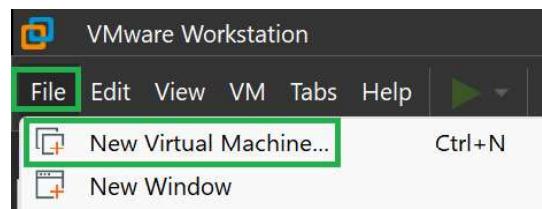
La conduite ainsi que la réalisation d'un projet de ce genre est pleine d'embuches et de pièges. Néanmoins, malgré les difficultés rencontrées, j'ai pu terminer à temps, en respectant la demande du client, le budget imposé ainsi que le délai. Cela aura été une grande expérience pour mon cursus ainsi que pour les projets futurs.

6) DOCUMENTATION TECHNIQUE

6.1) Serveur Windows 2019 GUI

6.1.1) Installation

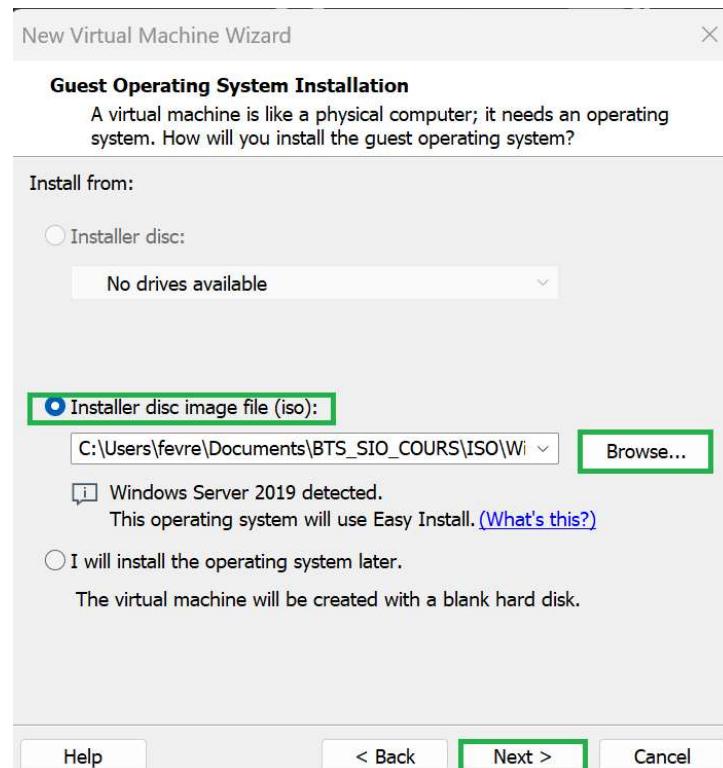
Pour ce projet, nous allons travailler sur Vmware Workstation 16 Pro. Nous allons créer une nouvelle machine virtuelle en cliquant sur File -> New Virtual Machine :



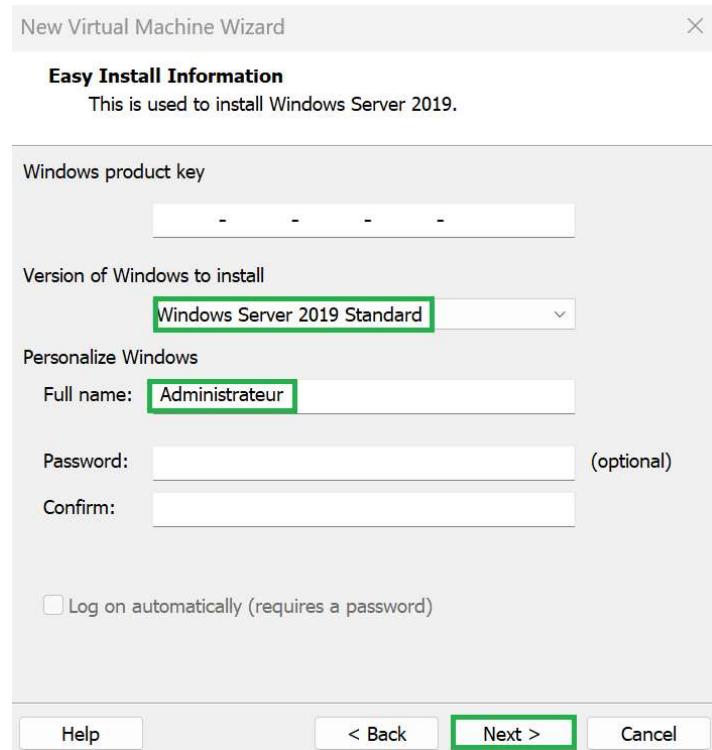
Choisir « Custom » :



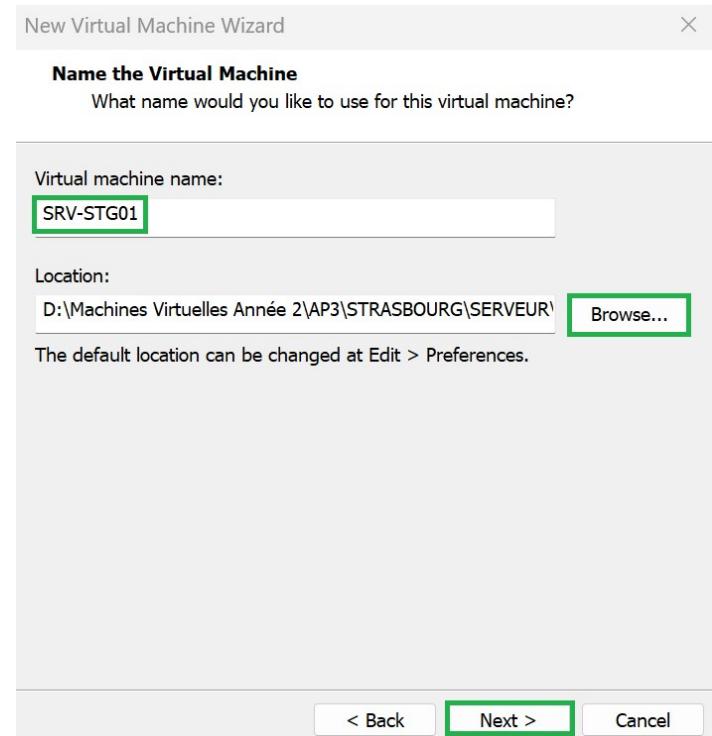
Cliquez ensuite sur **Next**, puis cochez « Installer disc image file (iso) » et cliquez sur **Browse** pour sélectionner le bon fichier iso puis cliquez sur **Next** :



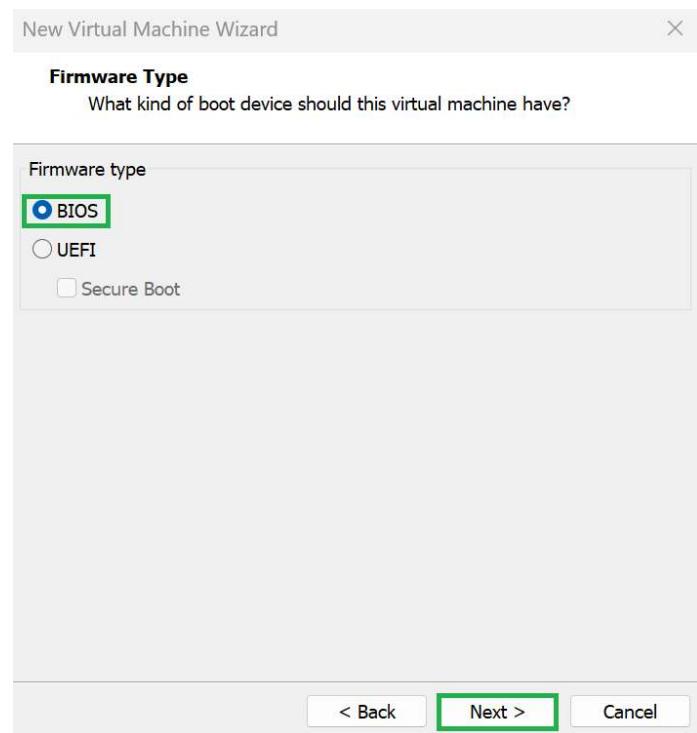
Choisir la version « **Standard** », renseignez un compte pour ouvrir une session au démarrage de la vm (Pour se logger automatiquement, il suffit de cocher « Log on auto » et de renseigner un mot de passe) Nous n'allons pas le faire ici et nous définirons le mot de passe plus tard. Cliquez sur **Next** :



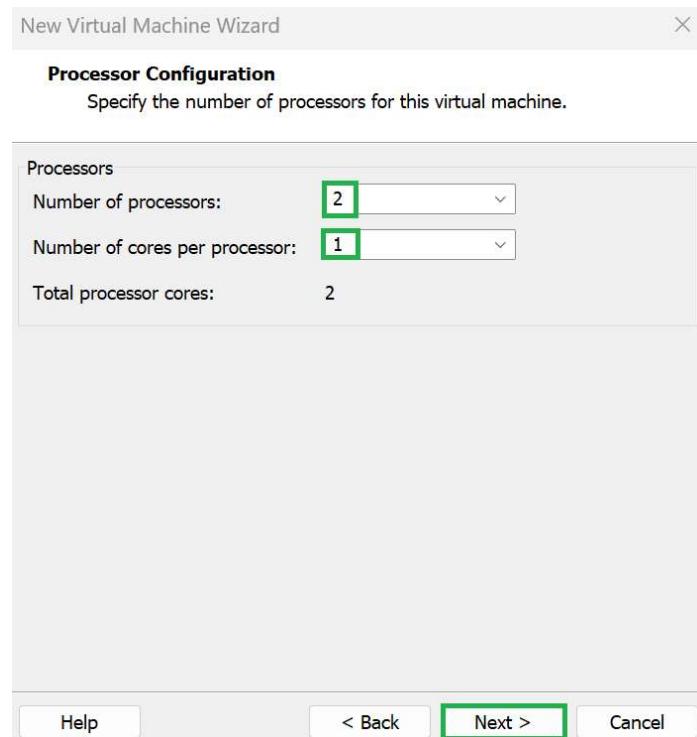
Renseignez le nom de la machine virtuelle puis choisir la localisation avec **Browse** puis cliquez sur **Next** :



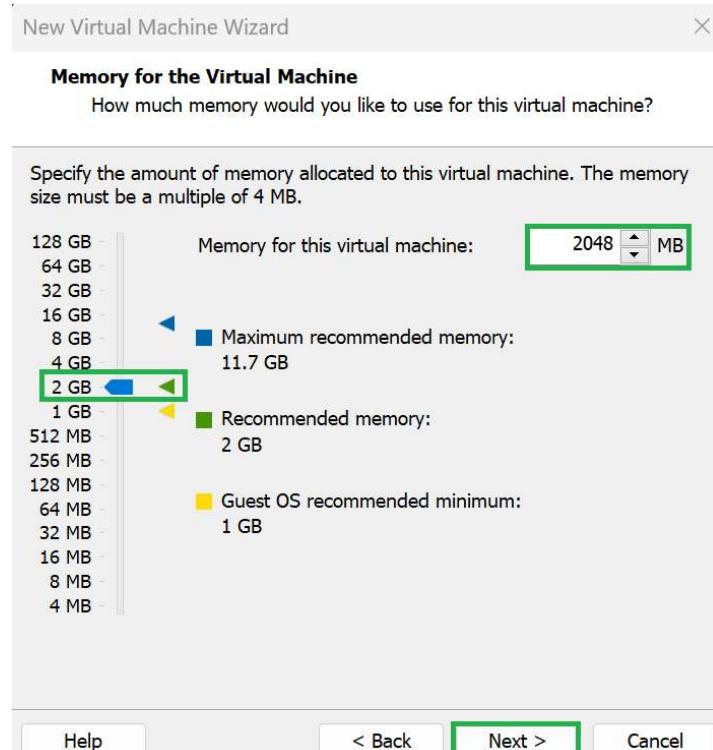
Choisir « Bios » puis cliquez sur **Next** :



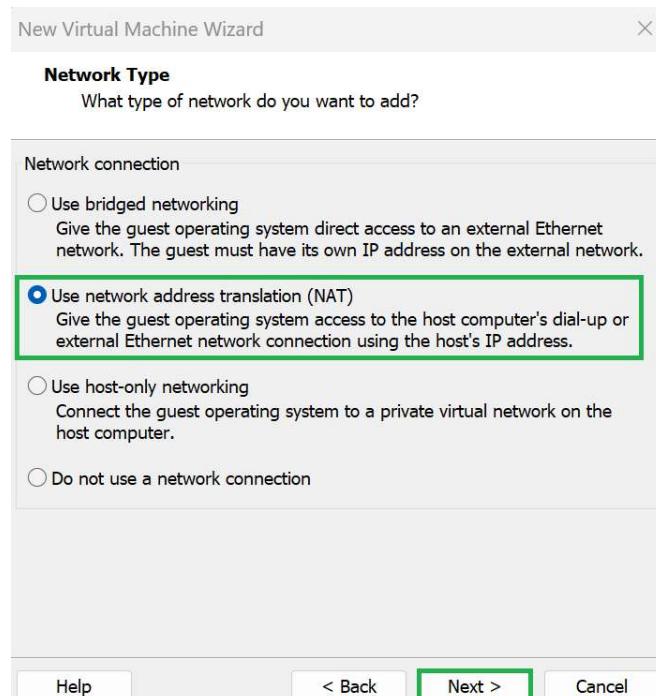
Choisir la configuration suivante :



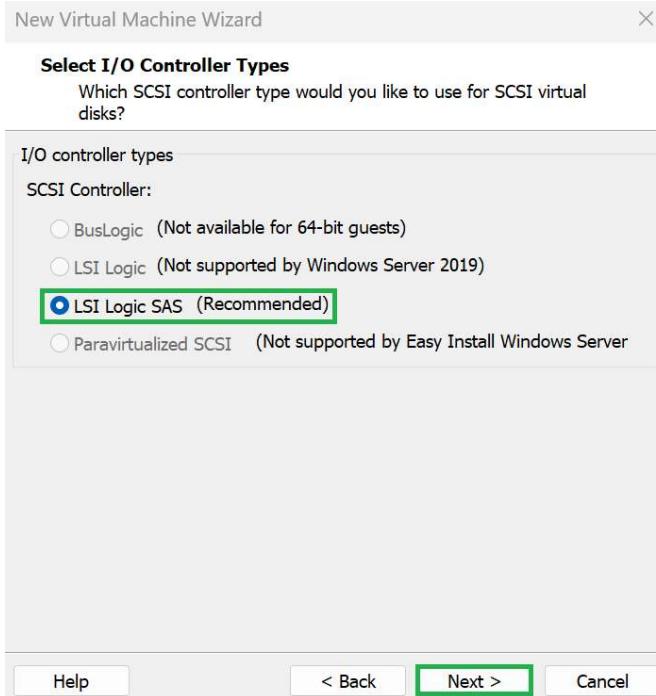
Vu le nombre de machine à faire tourner sur le même ordinateur, nous allons lui attribuer le minimum recommandé, à savoir 2GB :



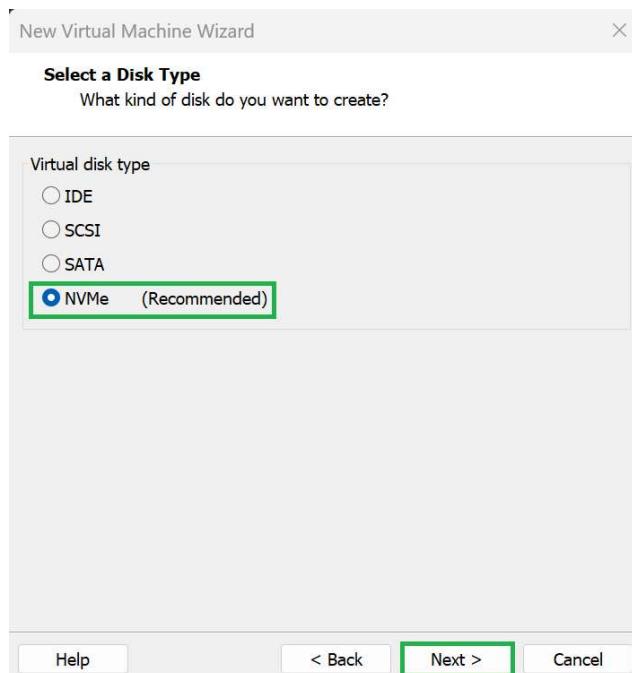
Ensuite :



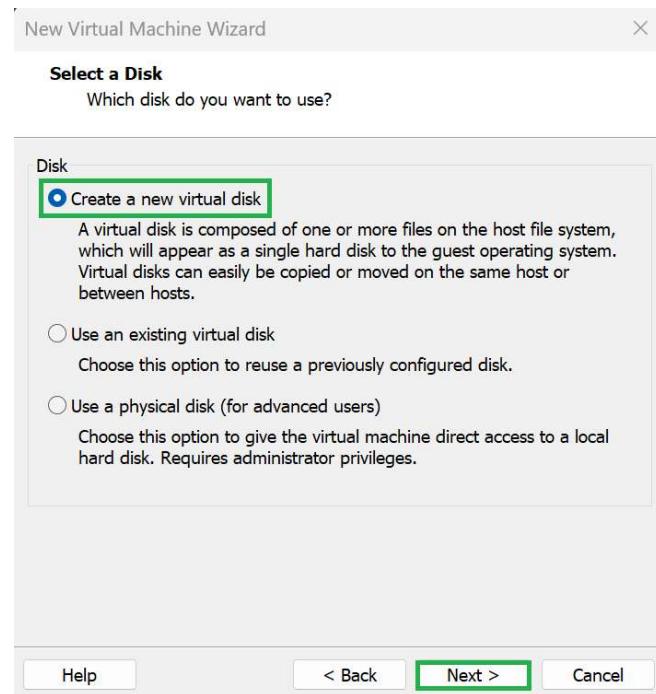
Et :



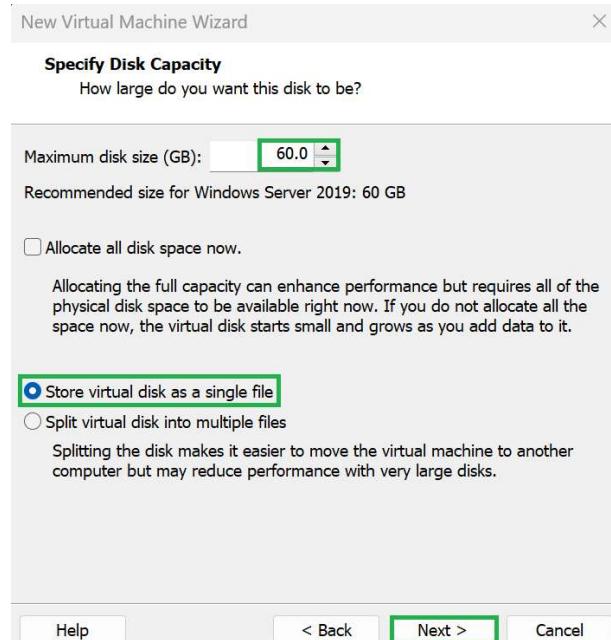
Puis :



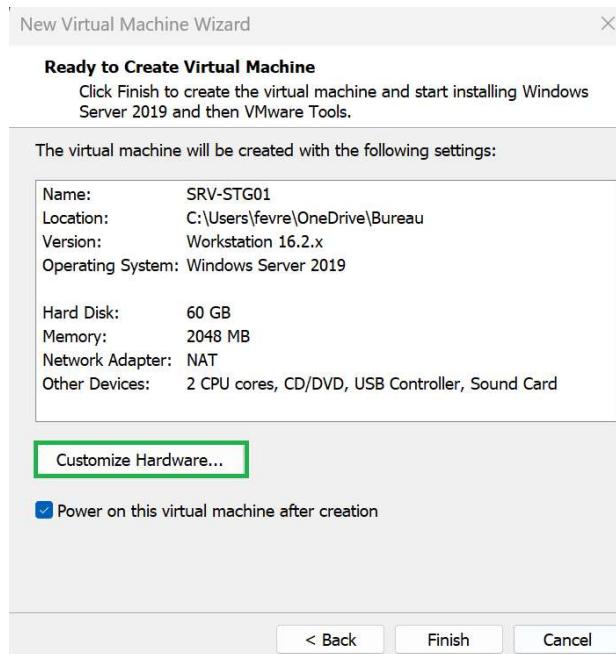
Créer un nouveau disque virtuel et cliquez sur **Next** :



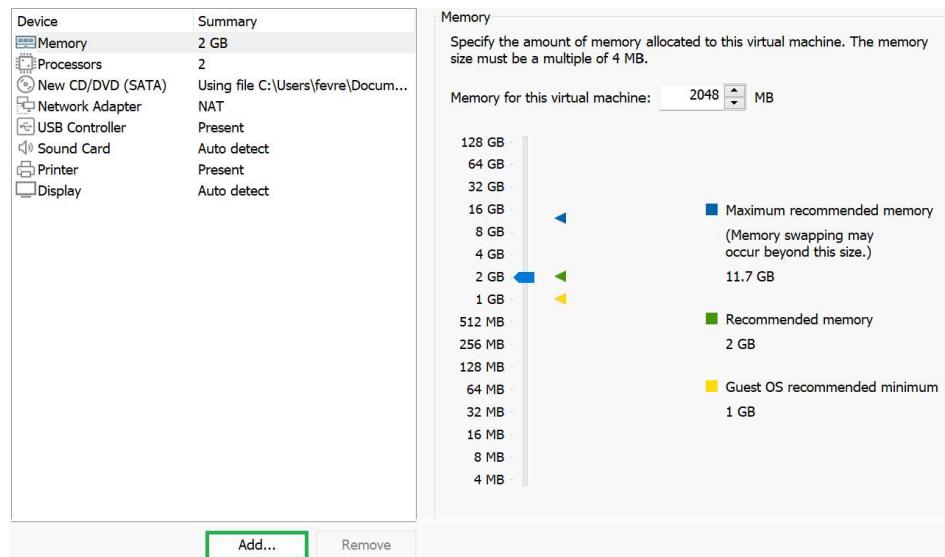
Conformément à la demande du projet, le disque sera de 60 GB et nous allons choisir la première option et surtout de ne pas l'allouer entièrement pour préserver la place sur le disque dur qui contient la VM puis cliquez sur **Next** :



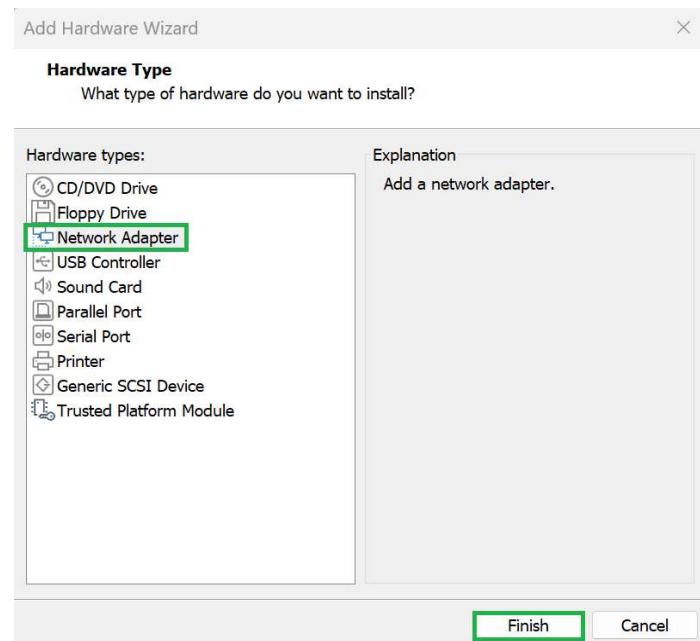
Cliquez sur **Next**, une fenêtre de la sorte se présentera alors à vous. Cliquez sur **Customize Hardware** :



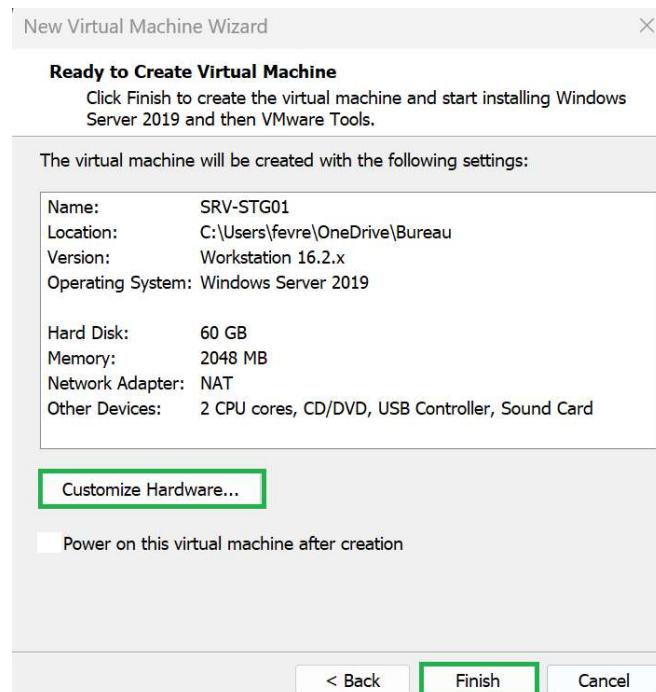
Cliquez sur **Add** :



On va ajouter une deuxième carte réseau, cliquez sur **network Adapter** puis cliquez sur **Next** :

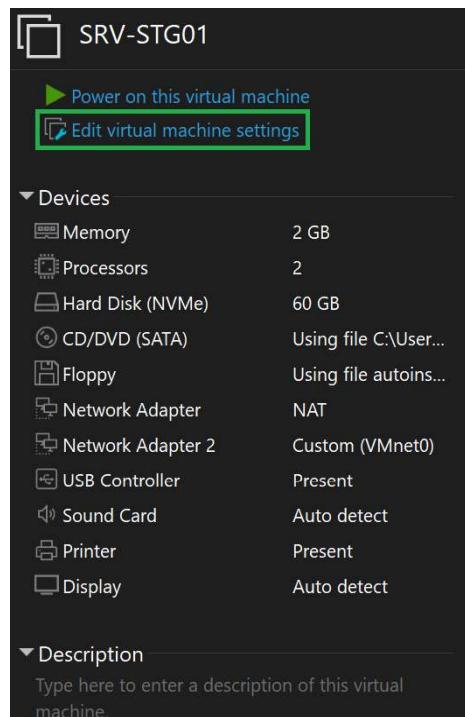


Ensuite cliquez sur **Finish** :

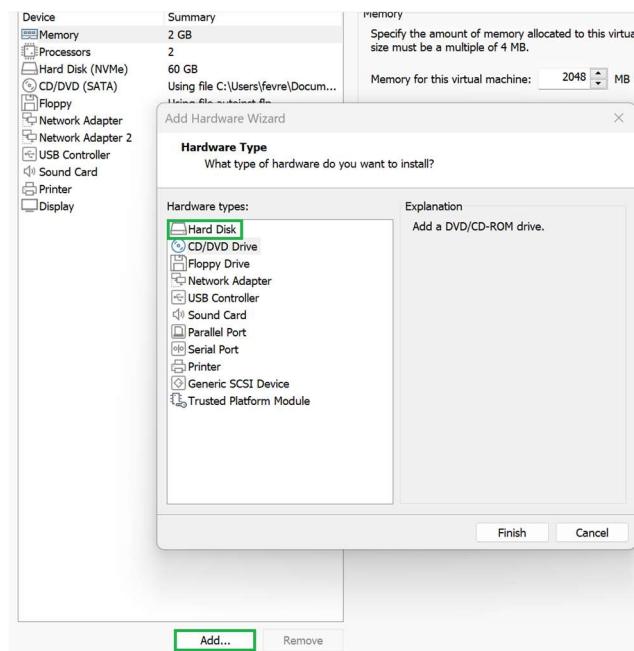


Nous allons maintenant ajouter un deuxième disque comme demander dans les spécifications techniques propre au projet.

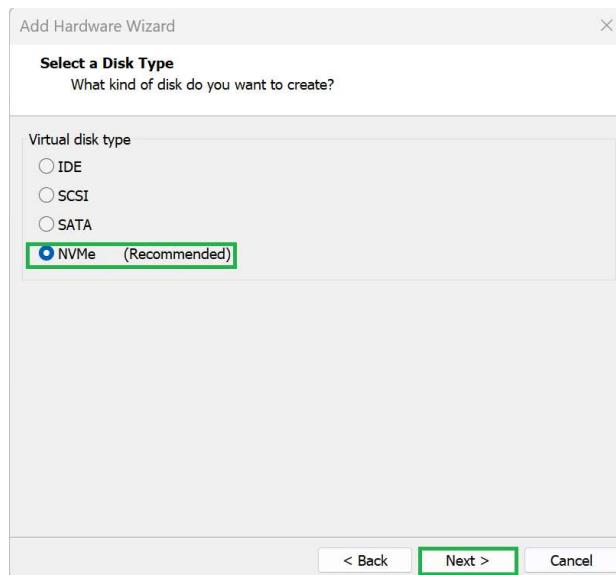
Pour cela, cliquez sur **Edit virtual machine settings** :



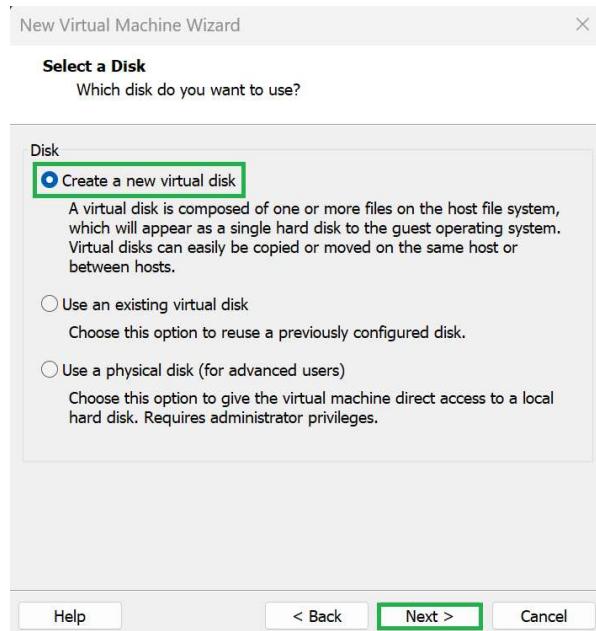
Cliquez sur **Add** puis sur **Hard Disk** :



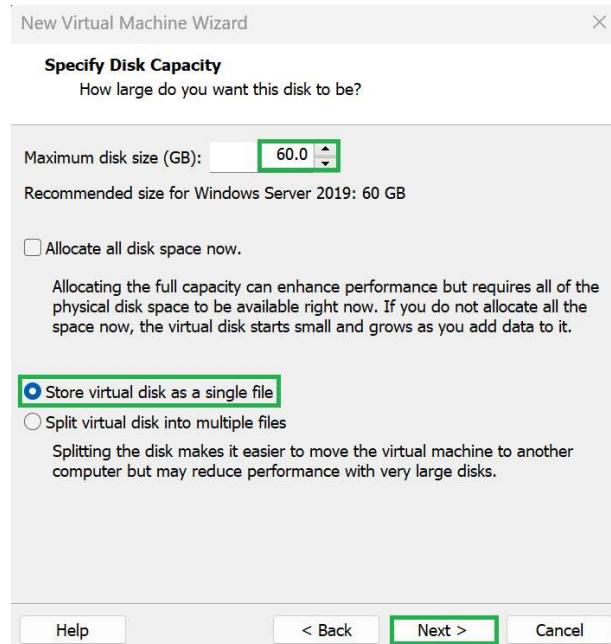
Puis :



Ensuite :



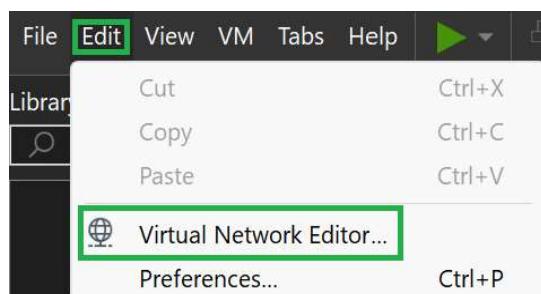
Et comme pour le premier disque :



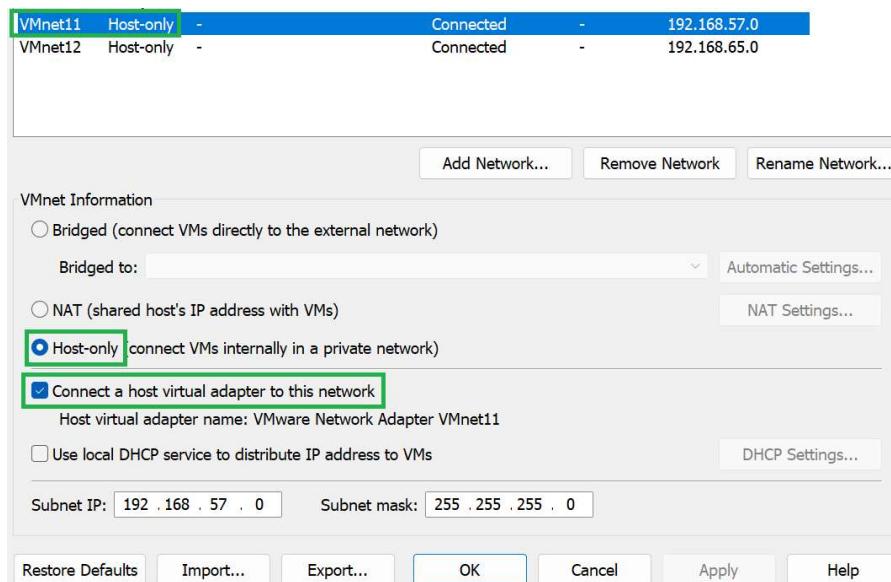
Après validation, nous pouvons voir les deux disques durs ainsi que les deux cartes réseaux qu'on aura mis sur le Vmnet11 en custom :

Hardware Options	
Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	60 GB
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet11)
Network Adapter 2	Custom (VMnet11)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

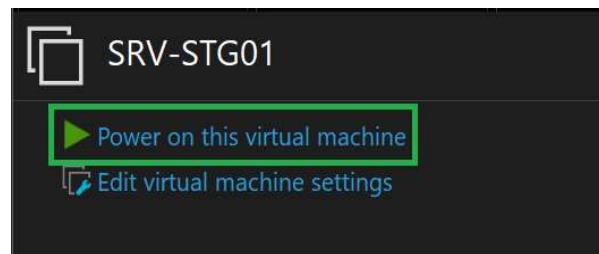
Pour ce qui est du Network Editor :



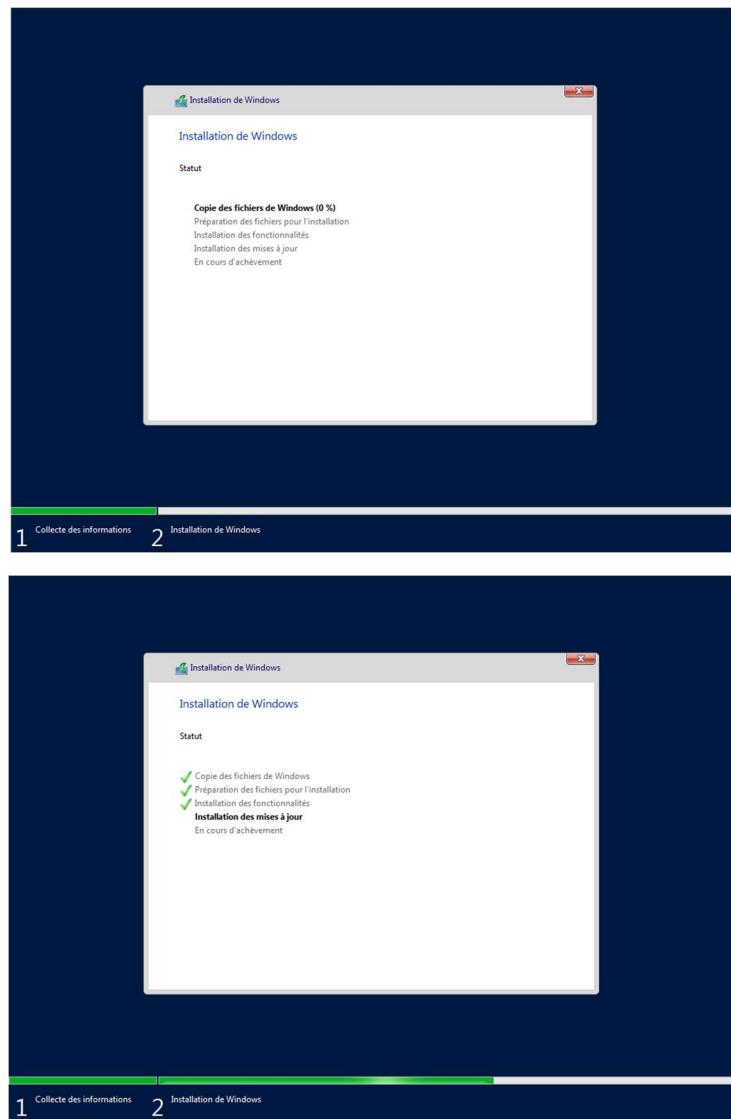
Voici les réglages du vmnet11 :



Nous allons maintenant procéder à l'installation. Cliquez sur **Power on this Virtual machine** :

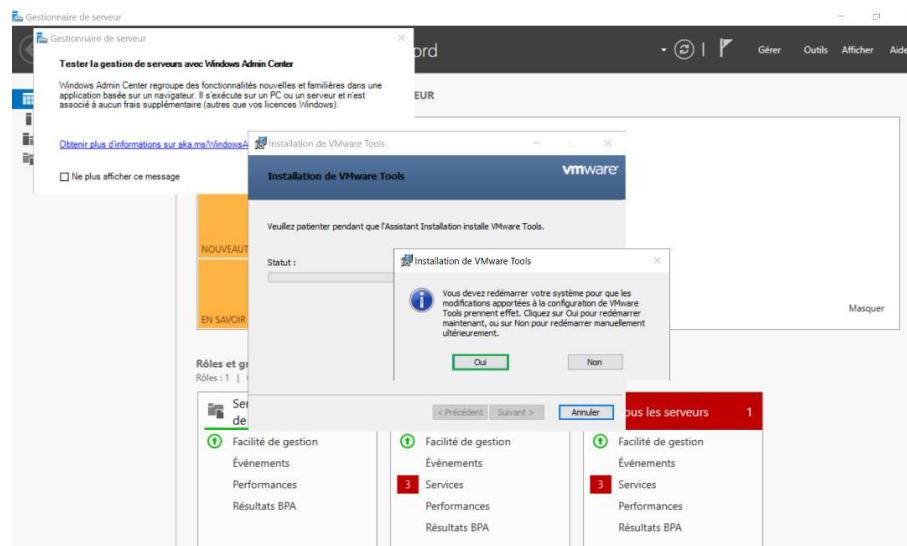


L'installation démarre :



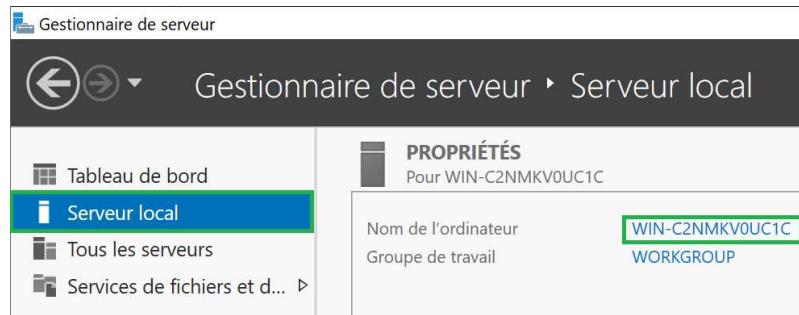
6.1.2) Configuration de base

Une fois tout en vert la vm démarre, on arrive ensuite à l'installation des **Vmware Tools**. Cliquez sur oui pour redémarrer la vm et procéder à l'installation :



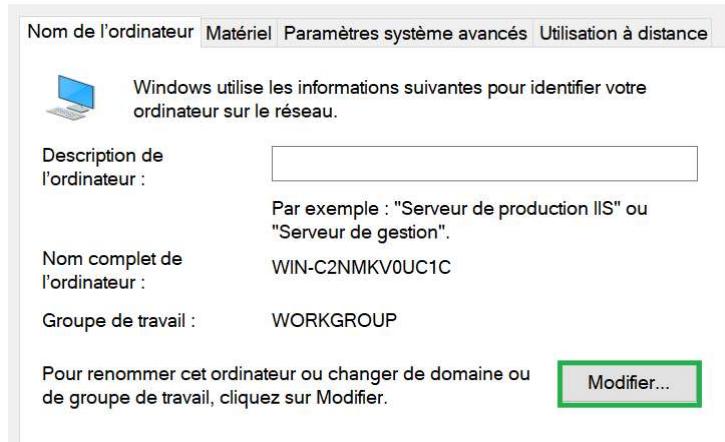
Une fois redémarré, nous allons procéder à la configuration de base de la vm.

Tout d'abord, nous allons aller dans le gestionnaire de serveur à l'onglet **Serveur local** puis cliquez sur le nom de l'ordinateur :

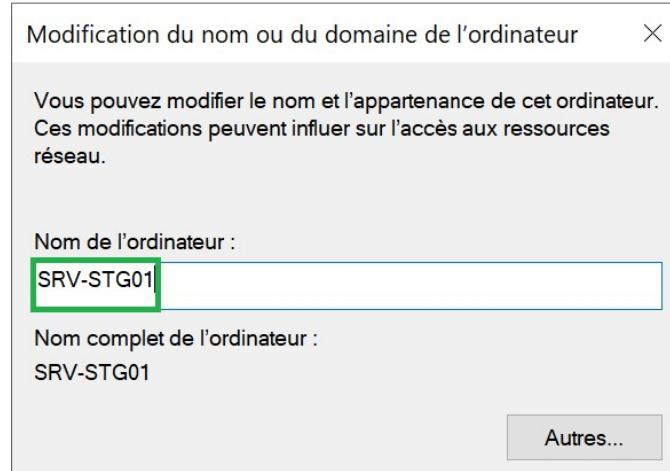


Cliquez sur **modifier** :

Propriétés système



Assignez le nom puis valider :



La VM devra redémarrer pour prendre en compte la modification :

Modification du nom ou du domaine de l'ordinateur

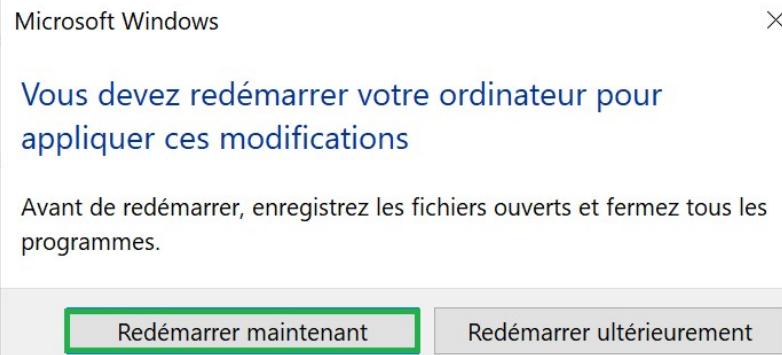


Vous devez redémarrer votre ordinateur pour appliquer ces modifications.

Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.

OK

Cliquez sur **OK** puis validez le redémarrage :



Dans le même onglet qu'avant, on peut voir que le nom à bien été changé. Cette étape doit impérativement se faire avant l'installation de l'AD.



Une fois l'ordinateur redémarré, rendez-vous une fois de plus dans le **Gestionnaire de serveur**, puis dans **Serveur local**, et dans les **Propriétés**. Nous pouvons observer la ligne spécifiant l'état du pare-feu :

Pare-feu Windows Defender Public : Actif

Et un peu plus loin sur cette même ligne :

Antivirus Windows Defender Protection en temps réel : activée

Ainsi que :

Configuration de sécurité renforcée d'Internet Explorer Actif

Commencez par cliquer sur « **Public : Actif** ». Une fenêtre apparaît :

“(P) Pare-feu et protection du réseau

Qui et ce qui peut accéder à vos réseaux.

Réseau avec domaine

Le pare-feu est activé.

Réseau privé

Le pare-feu est activé.

Réseau public (actif)

Le pare-feu est activé.

Cliquez sur chaque ligne bleue puis désactivez les pares-feux.

Pare-feu domaine :

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.



Activé

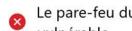
Devient

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.



Le pare-feu du domaine est désactivé. Votre appareil est peut-être vulnérable.



Désactivé

Pare-feu privé :

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau privé.

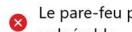


Activé

Devient

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau privé.



Le pare-feu privé est désactivé. Votre appareil est peut-être vulnérable.



Désactivé

Pare-feu public :

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau public.

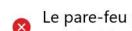


Activé

Devient

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau public.



Le pare-feu public est désactivé. Votre appareil est peut-être vulnérable.



Désactivé

Revenez maintenant dans les propriétés du serveur local, et cliquez sur **Protection en temps réel** :

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.



La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.



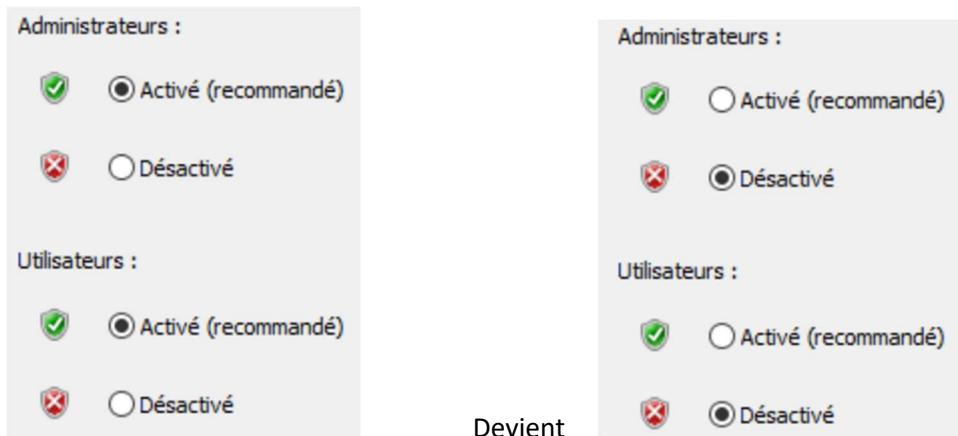
Activé

Devient



Désactivé

Pour finir nous allons désactiver la sécurité renforcée d'internet explorer :



Après actualisation, nous pouvons voir que tout a été pris en compte :



6.1.3) Agrégation de carte réseau (IP Bonding)

Comme indiqué dans les spécificités techniques du projet, nous allons procéder à l'IP Bonding. Cela nous permettra une certaine tolérance de panne ainsi qu'une répartition de charges (pour les interfaces réseaux).

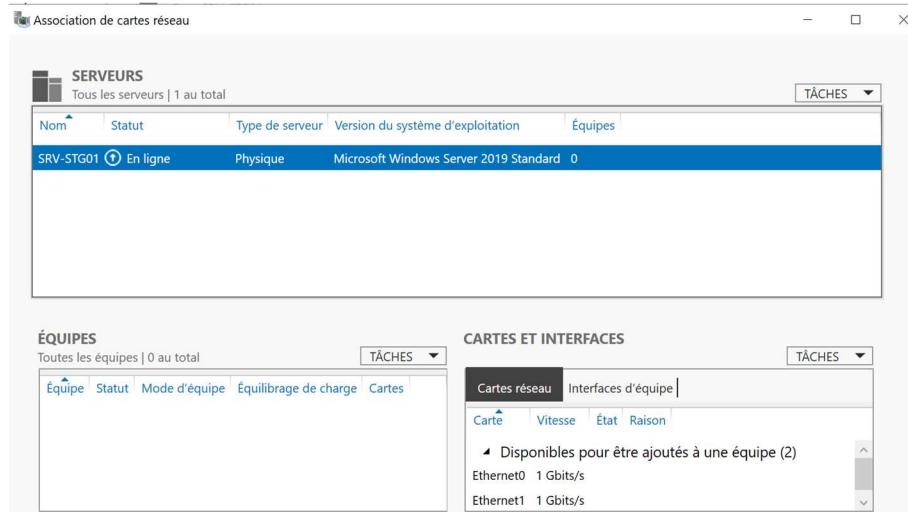
Pour réaliser l'agrégation, rendons-nous dans le gestionnaire de serveur, onglet Serveur local. Nous pouvons voir nos deux cartes réseaux :

Ethernet0	Adresse IPv4 attribuée par DHCP, Compatible IPv6
Ethernet1	Adresse IPv4 attribuée par DHCP, Compatible IPv6

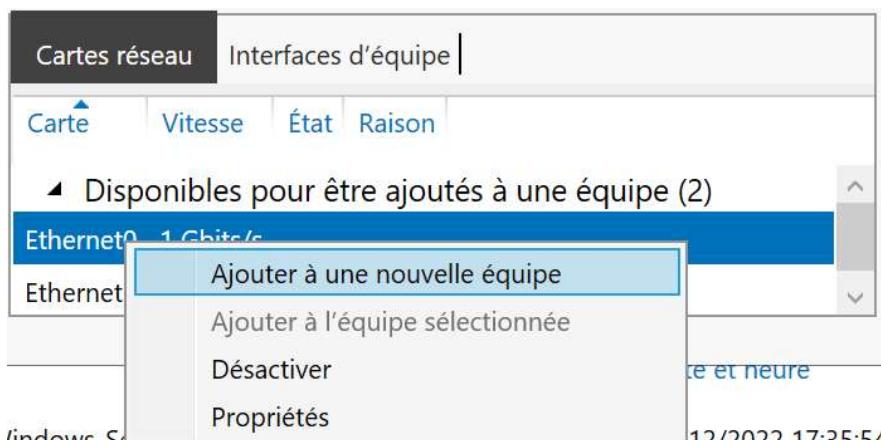
Comme nous l'avons vu plus haut, les deux cartes réseaux sont sur le Vmnet11. Revenez ensuite sur le serveur local dans propriétés et cliquez sur **Désactivé** à droite d'**Association de cartes réseau** :

Association de cartes réseau **Désactivé**

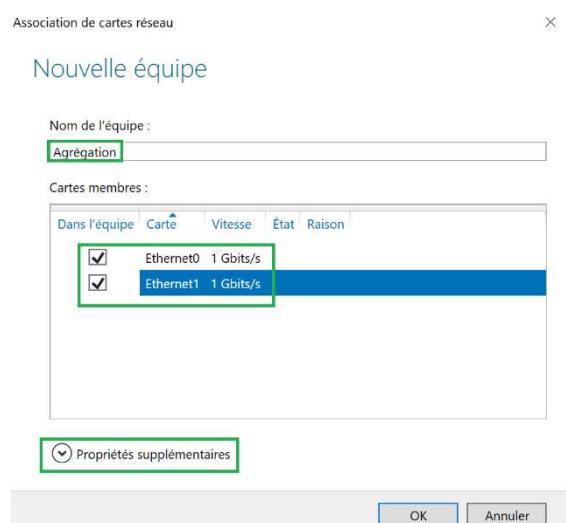
Une fenêtre apparaît :



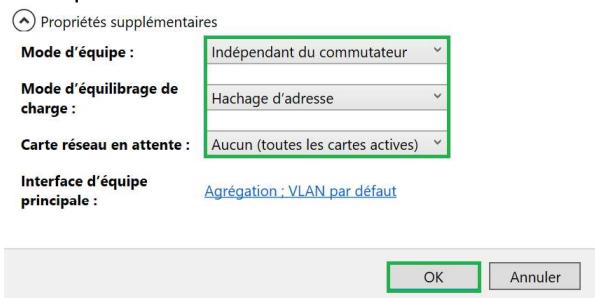
Faites un clic droit sur la première carte puis sélectionnez **Ajoutez à une nouvelle équipe** :



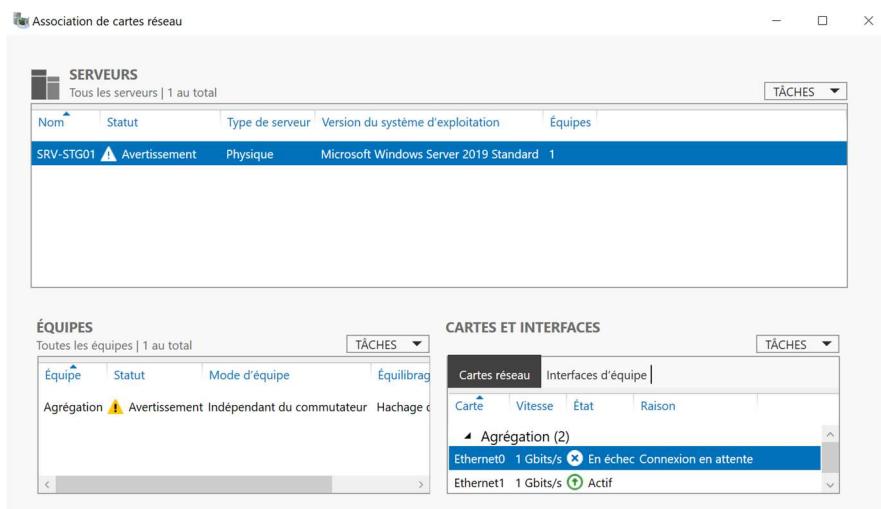
Une fenêtre s'ouvre alors, choisissez le nom puis sélectionnez les deux cartes et cliquez sur **Propriétés supplémentaires** :



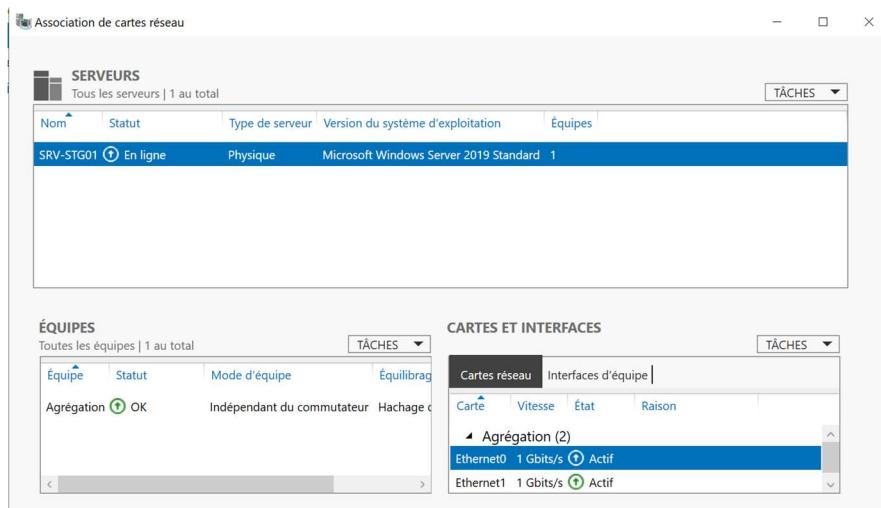
Configurez comme ceci puis cliquez sur **OK** :



Cela peut prendre quelques minutes avant que les deux cartes soient actives donc pas de panique :



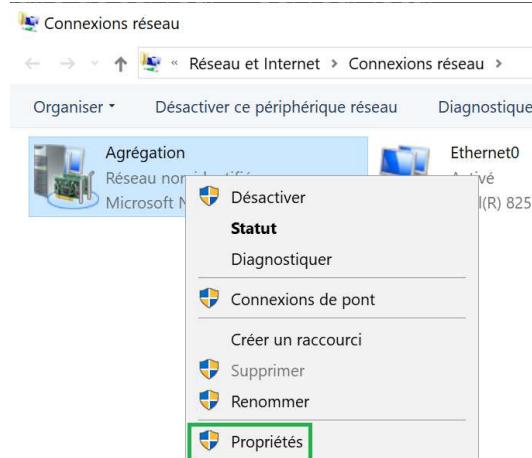
Devient



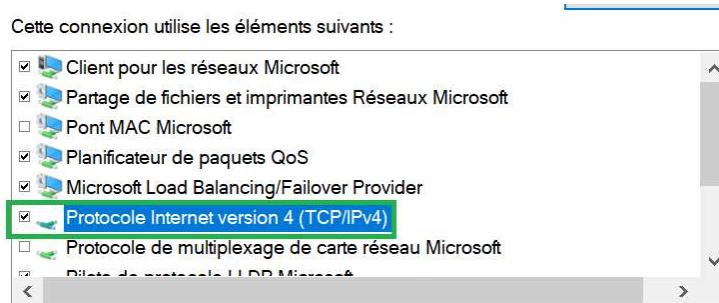
On peut voir que l'agrégation à bien été prise en compte dans le gestionnaire du serveur local :

Association de cartes réseau	Activé
Agrégation	Adresse IPv4 attribuée par DHCP, Compatible IPv6

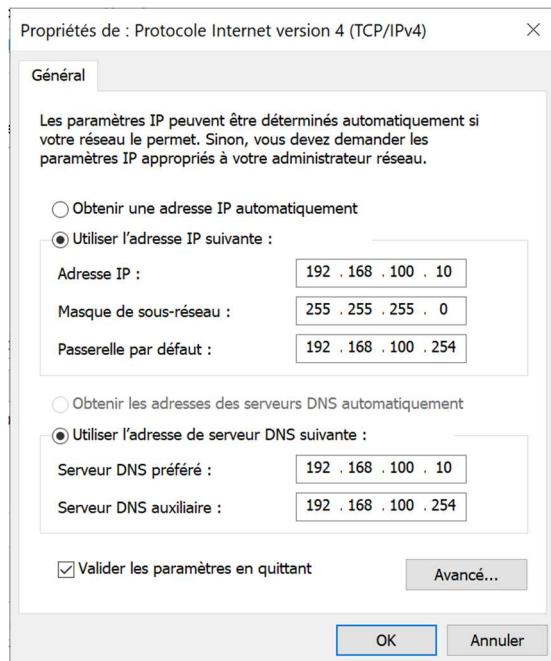
Nous allons maintenant attribuer l'IP statique que nous avons définis dans le tableau d'adressage.
 Pour cela il suffit de cliquer sur **adresse ipv4** à droite d'**Agrégation**, puis faites un clic droit sur **Agrégation** et cliquez sur **Propriétés** :



Faites un double clic sur **Protocole Internet version 4** :



Remplir comme ceci et cliquez sur **OK** :



Ce qui nous donne :

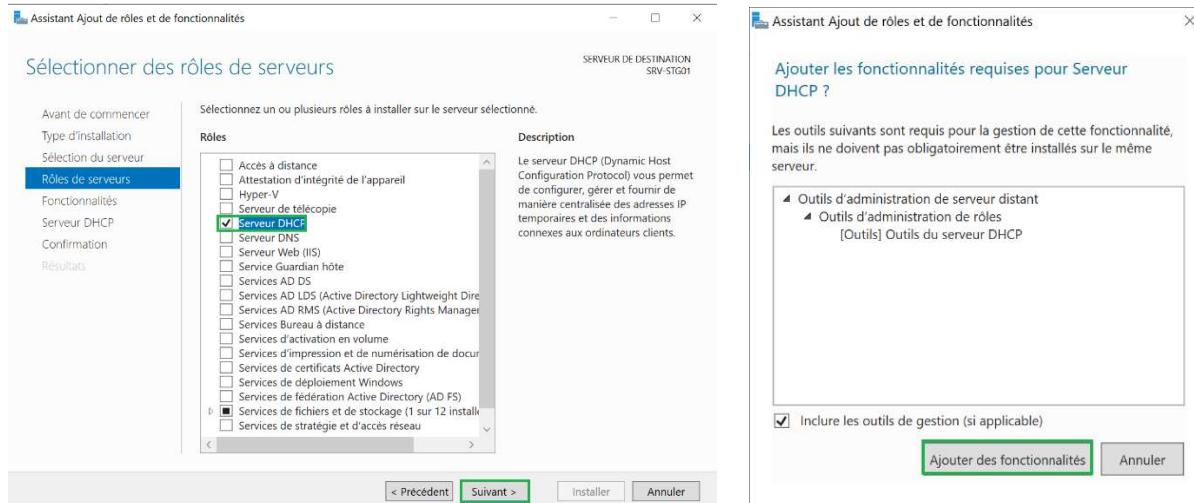
Association de cartes réseau	Activé
Agrégation	192.168.100.10

6.1.4) DHCP

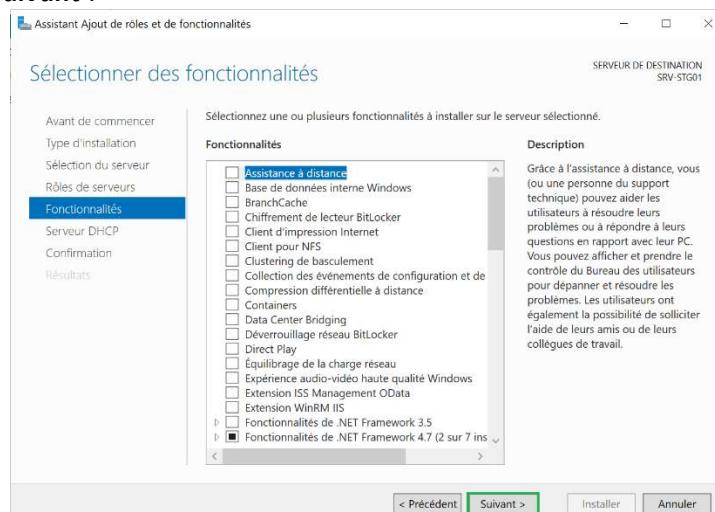
Maintenant que le serveur dispose d'un IP fixe, nous allons pouvoir installer le rôle DHCP. Pour cela, rendez-vous dans le **Tableau de bord** du **Gestionnaire de serveur** et cliquez sur **Ajouter des rôles et des fonctionnalités** :



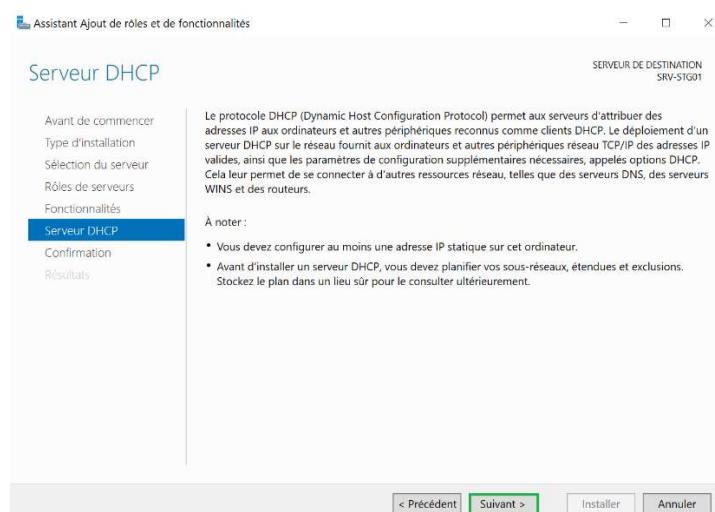
Une fenêtre s'ouvre, cliquez trois fois sur **Suivant** puis sélectionnez le rôle **Serveur DHCP**, une deuxième fenêtre s'ouvre, cliquez sur **Ajouter des fonctionnalités** puis cliquez sur **Suivant** :



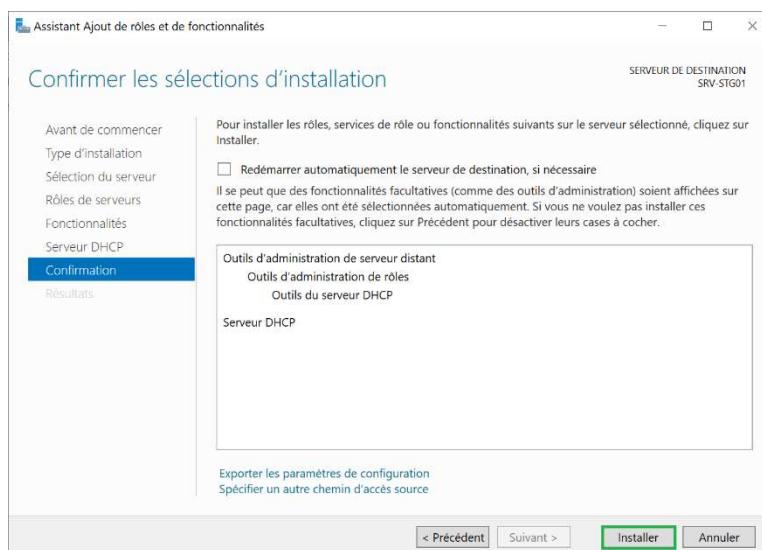
Cliquez encore sur **Suivant :**



Encore une fois **Suivant :**



Ensuite, démarrez l'installation en cliquant sur **Installer** :



L'installation se lance :



Vous pouvez fermer l'assistant.

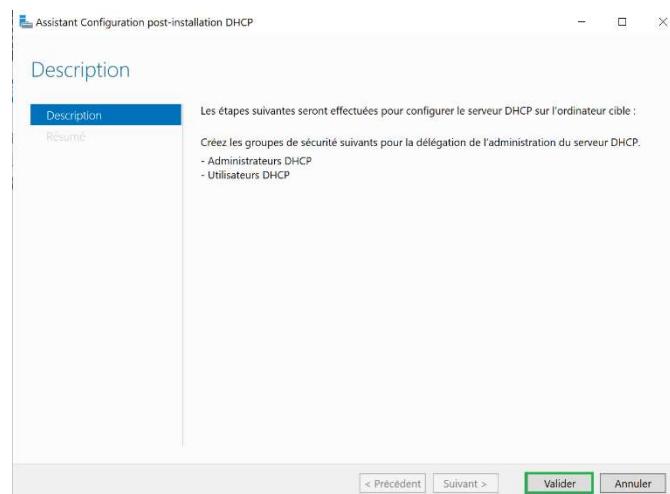
Pour finaliser l'installation du rôle, rendez-vous dans le **Gestionnaire de serveur** et faites un clic gauche sur l'icône comportant un drapeau et un triangle jaune (avec un point d'exclamation)



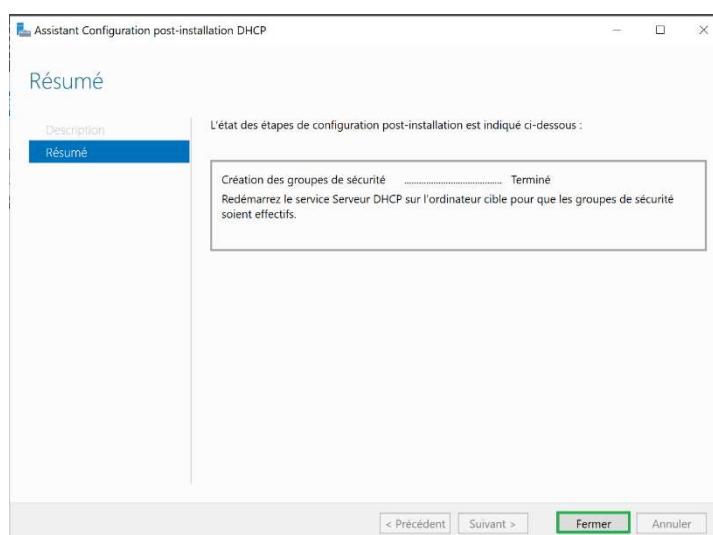
Cliquez ensuite sur **Terminer la configuration DHCP** :



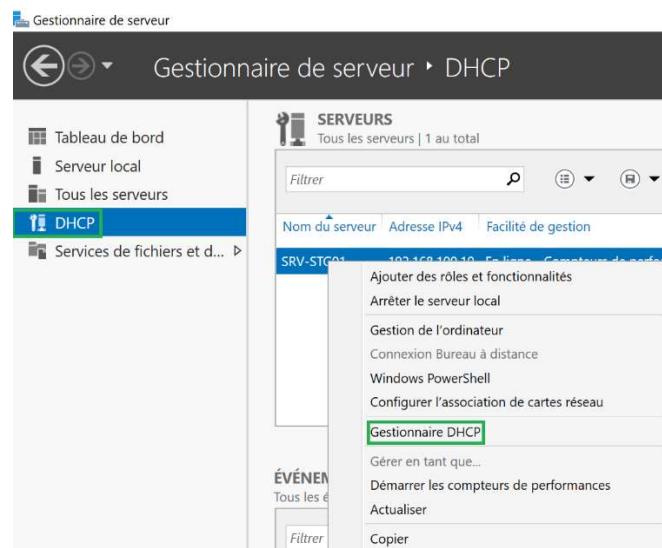
Une fenêtre apparaît. Cliquez sur **Validez** :



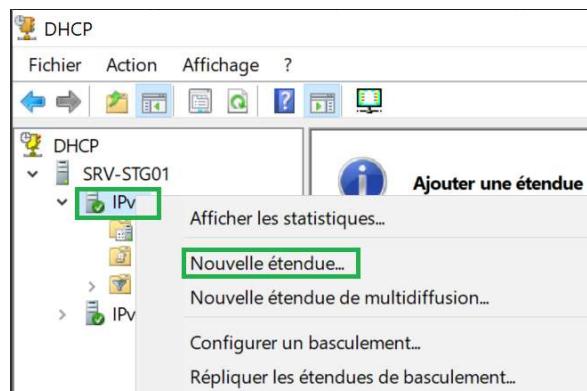
Cliquez sur **Fermer** :



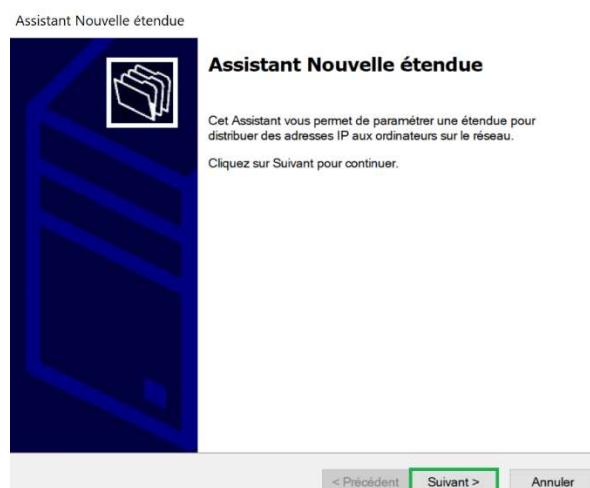
L'installation du rôle DHCP est maintenant terminée. Pour la configuration DHCP, nous allons configurer une étendue pour le site de Strasbourg. Cette étendue sera ensuite répliquée, après l'installation du Serveur CORE de Strasbourg, plus tard dans le livrable. Pour cela, nous allons ouvrir le **Gestionnaire DHCP** :



Nous allons dérouler le nom du serveur, puis faire un clic droit sur **IPv4** et sélectionner **Nouvelle étendue** :



L'assistant s'ouvre alors. Cliquez sur **Suivant** :



Rentrez un nom et une description (optionnel) puis cliquez sur **Suivant** :

Assistant Nouvelle étendue

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

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

Nom : **SITE A - STRASBOURG**

Description :

< Précédent **Suivant >** Annuler

Conformément au plan d'adressage, nous allons faire une étendue du 192.168.100.50 – 192.168.100.254 (Les adresses 192.168.100.2 jusqu'à 192.168.100.50 réservées à la partie serveurs) :

Assistant Nouvelle étendue

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

Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : **192 . 168 . 100 . 50**

Adresse IP de fin : **192 . 168 . 100 . 254**

Paramètres de configuration qui se propagent au client DHCP.

Longueur : **24**

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

< Précédent **Suivant >** Annuler

Nous arrivons ensuite sur une fenêtre où nous allons exclure l'adresse IP 192.168.100.254, que nous attribuerons à notre futur routeur/pare feu PFSense. Renseignez **l'IP de début et de fin** puis cliquez sur **Ajouter**, l'IP apparaîtra dans la partie **Plage d'adresses exclue** puis cliquez sur **Suivant** :

Assistant Nouvelle étendue

Ajout d'exclusions et de retard
Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP-OFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

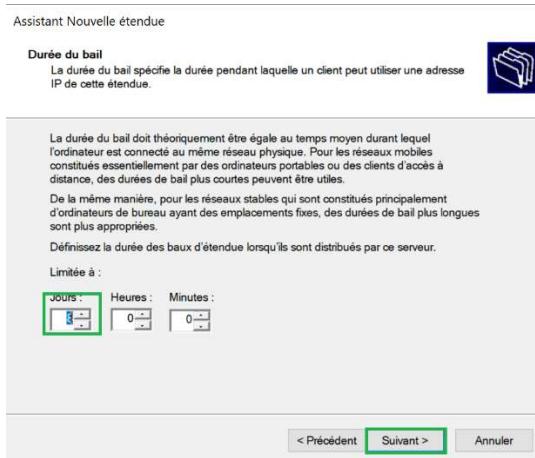
Adresse IP de début : **192 . 168 . 100 . 254** Adresse IP de fin : **192 . 168 . 100 . 254** Ajouter

Plage d'adresses exclue :
Adresse 192.168.100.254 Supprimer

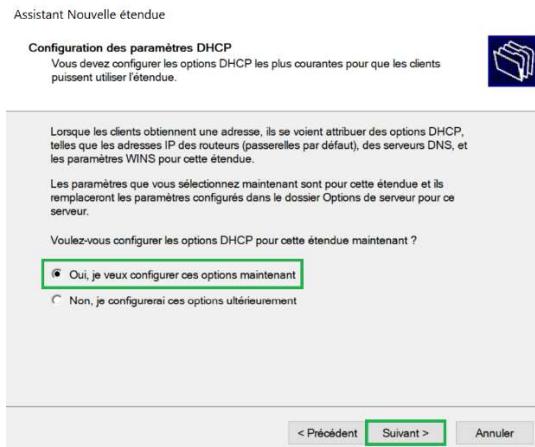
Retard du sous-réseau en millisecondes : **0**

< Précédent **Suivant >** Annuler

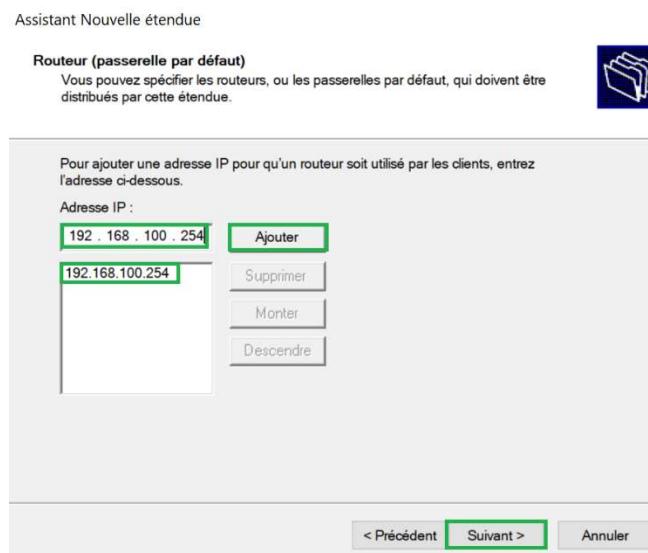
On laisse la durée du bail à 8 jours, cliquez sur **Suivant** :



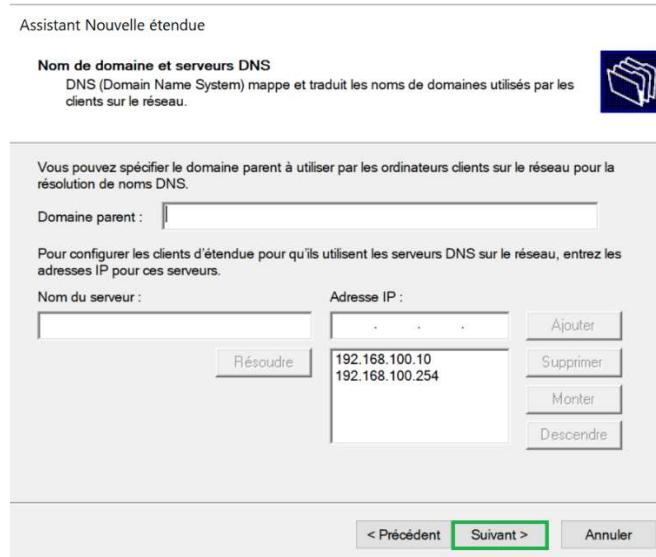
On va configurer les **options DHCP** :



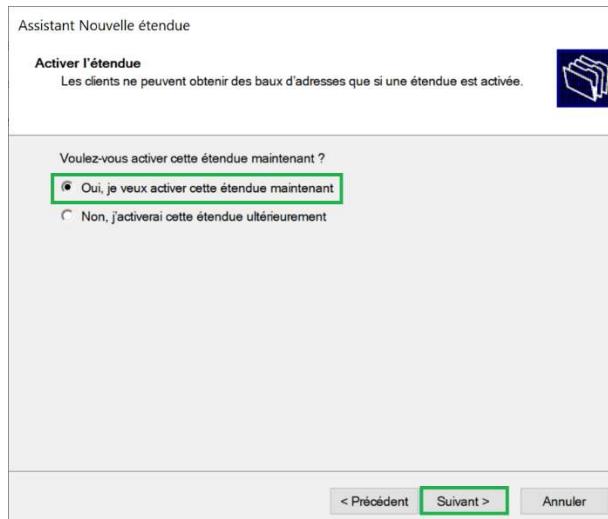
Entrez l'IP de votre futur routeur PFSense, cliquez sur **Ajouter** puis cliquez sur **Suivant** :



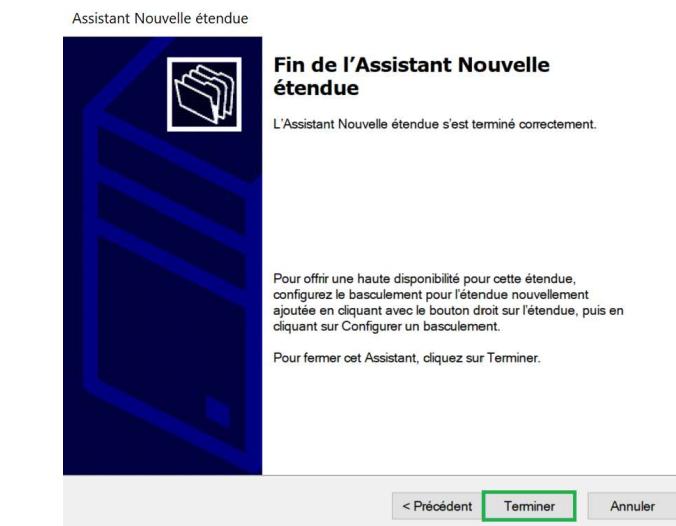
On laisse tel quel puis on clique sur **Suivant** :



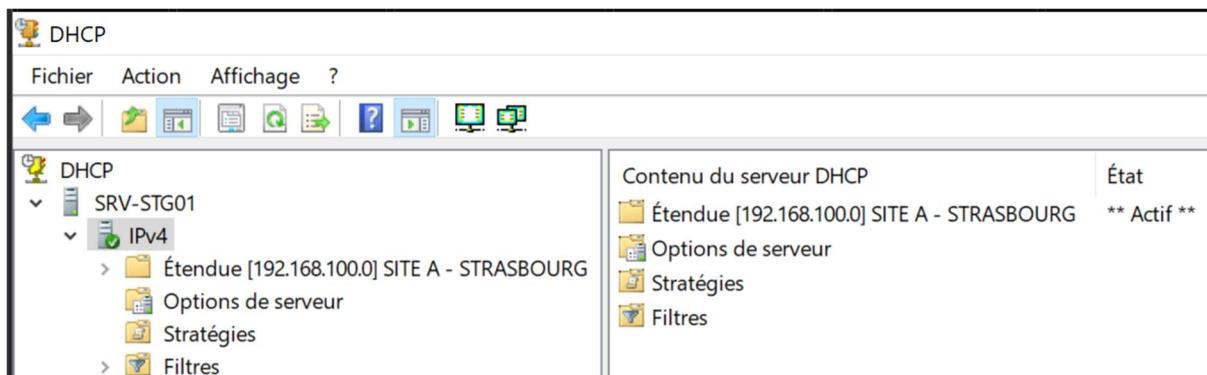
On coche **Oui, je veux activer**, puis on clique sur **Suivant** :



On clique sur **Terminer** :



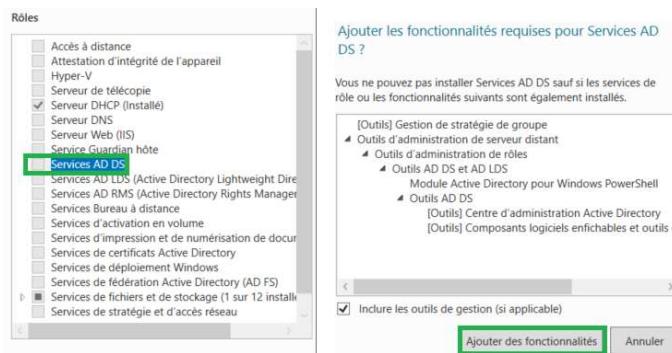
On peut désormais voir que l'étendue est visible dans le **Gestionnaire DHCP** :



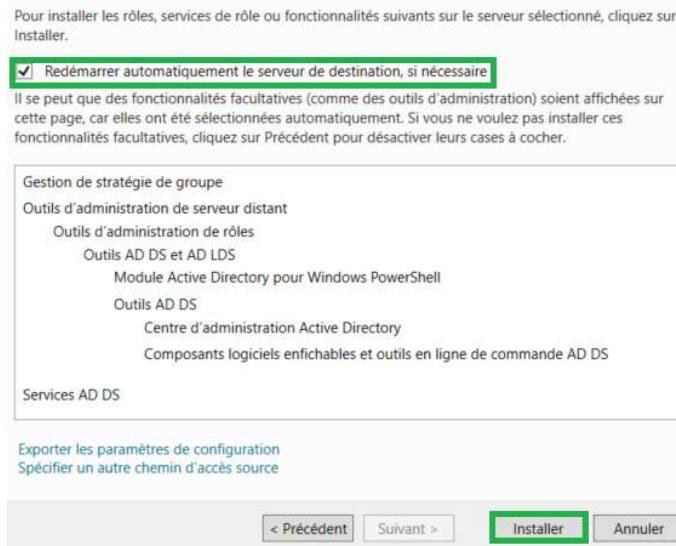
6.1.5) ADDS (Active Directory et DNS)

Nous allons maintenant passer à l'installation du service d'annuaire. Pour cela il existe un rôle qui installe l'Active directory ainsi que le DNS, il s'agit du rôle ADDS.

Cliquez sur **Ajouter des rôles et des fonctionnalités** dans le tableau de bord du **Gestionnaire de serveur**, puis cliquez 3 fois sur **Suivant**. Choisissez ensuite **Services AD DS**, L'assistant s'ouvre, cliquez sur **Ajouter des fonctionnalités** :

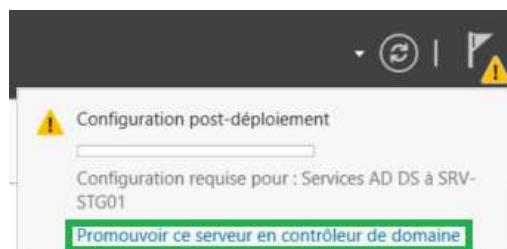


Cochez la case pour que le serveur redémarre automatiquement si nécessaire durant l'installation du rôle, puis cliquez sur **Installer** :



L'installation démarre, cela peut prendre quelques minutes.

Une fois le rôle installé, il nous reste quelques manipulations à effectuer. Pour cela, rendez-vous dans le tableau de bord du serveur et cliquer sur le **drapeau** en haut à droite, puis sur **Promouvoir ce serveur en contrôleur de domaine** :



Cochez la case **Ajouter une nouvelle forêt** et mettez le nom de domaine racine selon les spécifications techniques :

Sélectionner l'opération de déploiement

- Ajouter un contrôleur de domaine à un domaine existant
- Ajouter un nouveau domaine à une forêt existante
- Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : CCI-CAMPUS.LAN

Cliquez sur **Suivant**, puis tapez le mot de passe de restauration que vous avez choisi et cliquez sur **Suivant** :

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016
 Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

- Serveur DNS (Domain Name System)
- Catalogue global (GC)
- Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe : *****
 Confirmer le mot de passe : *****

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent

Suivant >

Installer

Ignorez la délégation DNS et faites une nouvelle fois **Suivant** :

Spécifier les options de délégation DNS

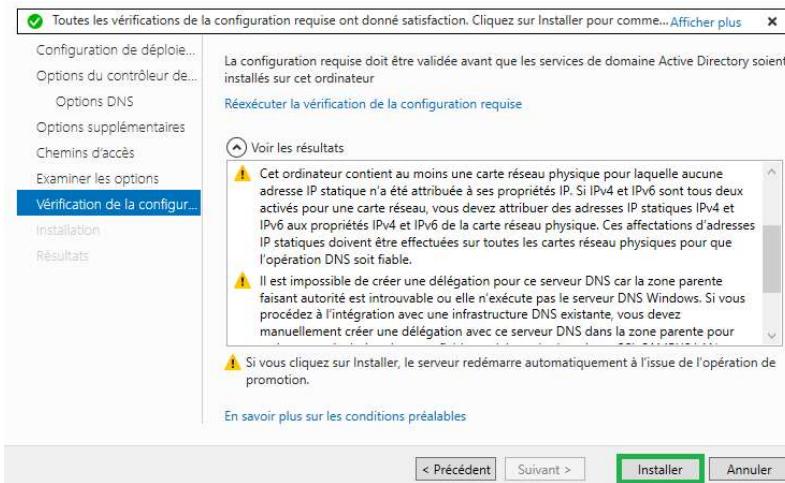
- Créer une délégation DNS

Le nom de domaine NetBIOS devrait être rempli automatiquement :

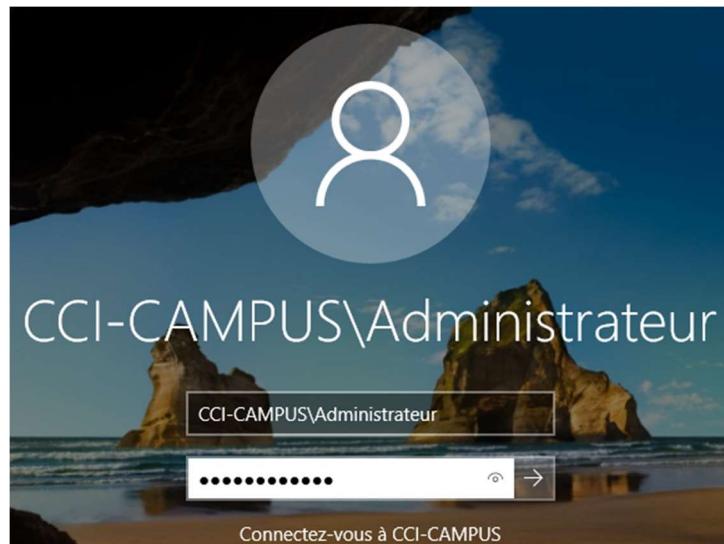
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS : CCI-CAMPUS

Cliquez sur **Suivant**, jusqu'à l'étape de l'installation puis cliquez sur Installer :



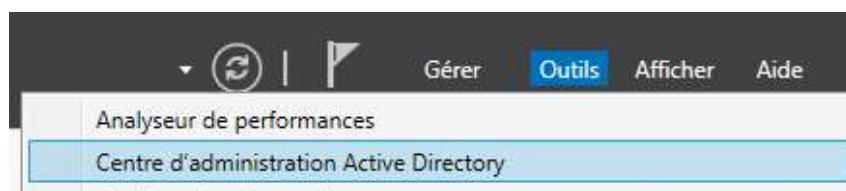
L'installation débute et puis le serveur va redémarrer pour finaliser l'installation, ce qui peut prendre un certain temps. Une fois redémarré, on nous propose de se connecter en **Administrateur du domaine** :



Avant la configuration de l'AD et conformément aux annexes, nous allons tout d'abord définir la stratégie de mot de passe selon les demandes suivantes :

- Longueur de 4 caractères minimum.
- Pas de gestion de l'historique.
- Nom de l'utilisateur en majuscule comme password.

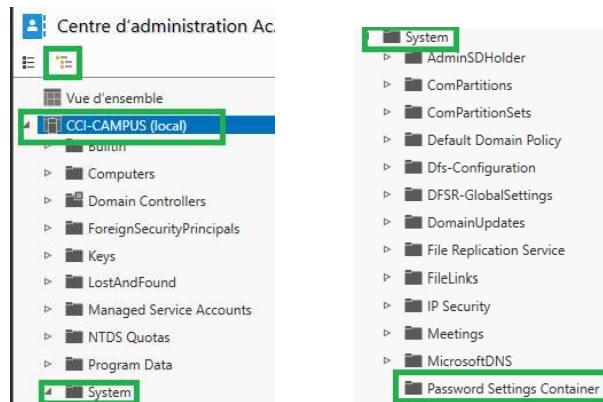
Pour cela, nous allons utiliser la console ADAC. Rendez-vous sur le **tableau de bord** du **Gestionnaire de serveur** et cliquez sur **Outils et Centre d'administration Active Directory** :



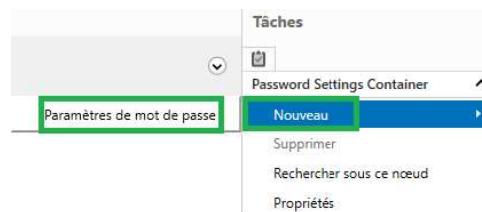
Cela va ouvrir cette fenêtre :



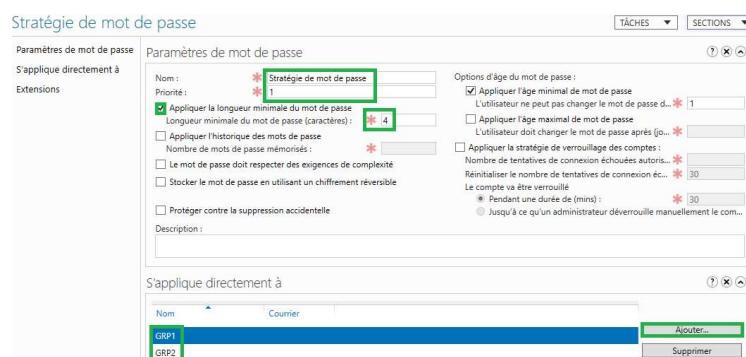
Déroulez le domaine avec le mode **Arborescence**, puis **System** et enfin **Password Settings Container** :



Dans la liste des tâches du volet de droite, cliquez sur **Nouveau** puis sur **Paramètres de mot de passe** :



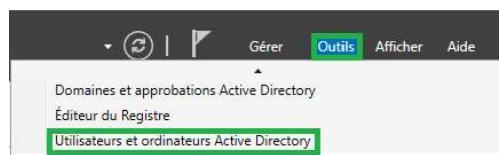
Une nouvelle fenêtre apparaît, Choisissez un nom pour la stratégie et la priorité. Accordez la longueur minimale à 4 et n'oubliez pas de décocher **l'historique, la complexité et l'âge maximal**. Ensuite ajoutez les **GRP1 et GRP2 (nous verrons la création juste après)** pour appliquer cette stratégie. (Nous vérifierons plus tard que cette stratégie ne s'applique pas aux **administrateurs du domaine**) :



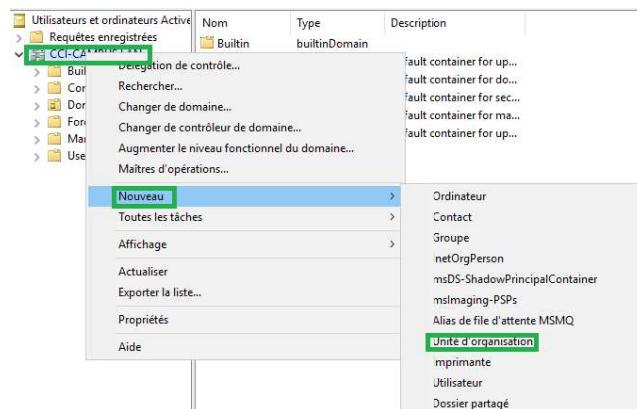
La stratégie est désormais visible :

Password Settings Container (1)			
Nom	Priorité	Type	Description
Stratégie utilisateurs	1	Paramètres...	

Nous allons maintenant passer à la création des groupes et utilisateurs AD. Pour cela rendez-vous dans l'onglet **Outils** du **Gestionnaire de serveur** puis cliquez sur **Utilisateurs et ordinateurs Active Directory** :

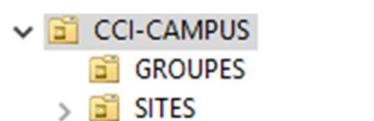


Pour commencer nous allons créer une UO nommé CCI-CAMPUS. Pour cela faites un clic droit sur le domaine puis **Nouveau** et **Unité d'organisation** :



Renseignez **CCI-CAMPUS** et laissez la case **Protéger le contenu coché** et validez :

Dans cette UO, de la même façon, nous allons créer 2 autres UO, **GROUPES** et **SITES** :

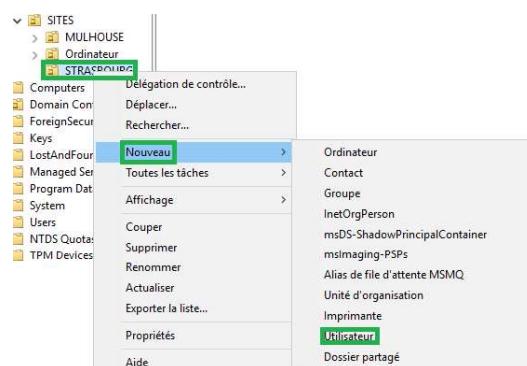


Dans l'UO SITES nous allons créer **3 UO** :

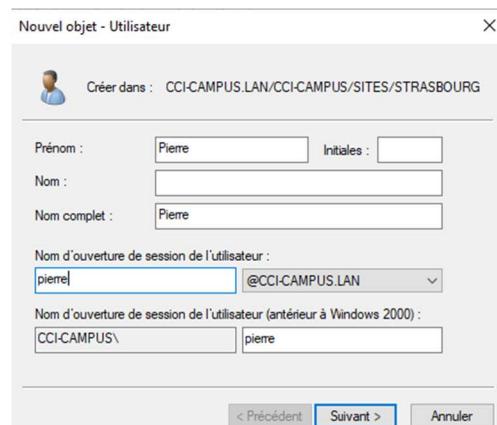
- STRASBOURG
- MULHOUSE
- Ordinateur



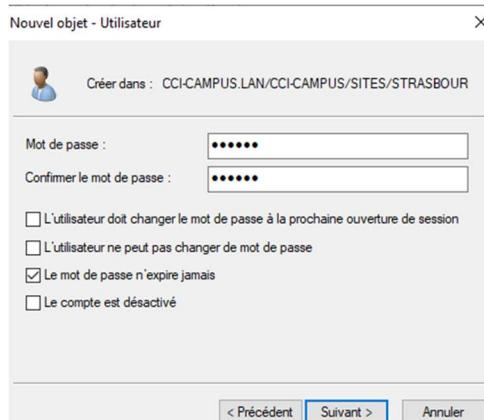
Une fois dans l'UO STRASBOURG, commencez par créer un nouvel utilisateur en faisant un clic droit sur STRASBOURG puis Nouveau et Utilisateur :



Ce nouvel utilisateur s'appelle Pierre. Renseignez comme ceci (Comme cet utilisateur est fictif et que nous n'allons pas ajouter d'autre Pierre, nous n'allons pas prendre la peine d'inventer un nom de famille) et cliquez sur **Suivant** :



Le mot de passe est le nom en majuscule comme demandé dans l'annexe 2. Dans le cadre de l'AP, cochez **Le mot de passe n'expire jamais** et décochez le reste puis cliquez sur **Suivant** :



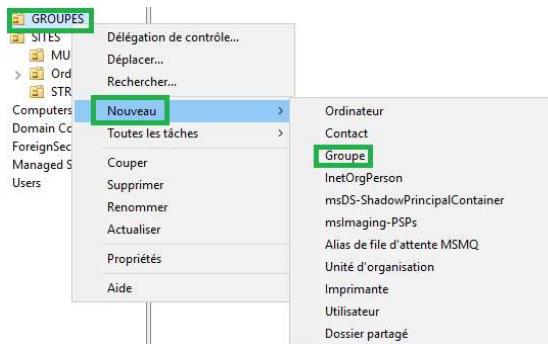
L'utilisateur est désormais créé. Nous allons encore créer un utilisateur nommé Paul dans le même UO puis nous allons créer, dans l'UO MULHOUSE, 2 utilisateurs nommée Nathalie et Isabelle :

Nom	Type	Description
Isabelle	Utilisateur	
Nathalie	Utilisateur	

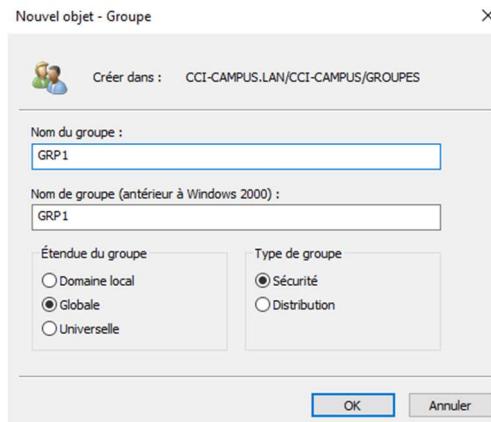
Dans l'UO GROUPES, nous allons créer 3 groupes :

- ADMINS
- GRP1
- GRP2

Pour cela, nous allons faire un clic droit sur l'UO GROUPES puis Nouveau et Groupe :



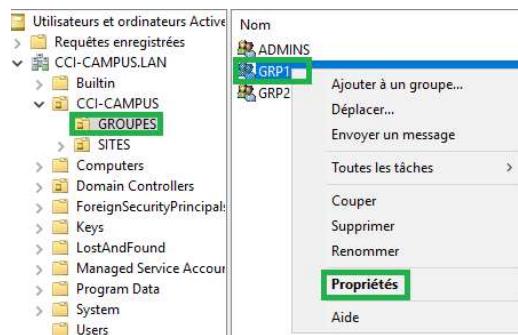
Renseignez le nom du groupe puis laissez-le reste de base puis cliquez sur **OK**.



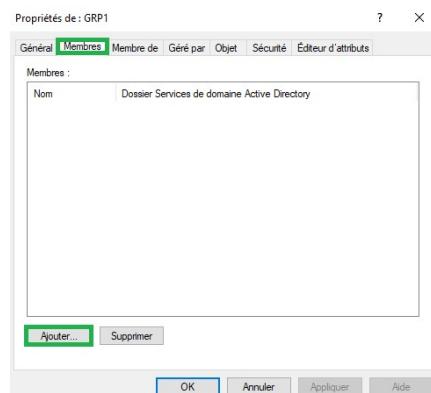
Faites pareil pour le **GRP2** et le groupe **ADMINs**. Après validation, nous pouvons voir que les groupes sont visibles dans l'UO :

Nom	Type
ADMINs	Groupe de sécurité
GRP1	Groupe de sécurité
GRP2	Groupe de sécurité

Une fois les groupes créés, selon *l'annexe 2*, nous allons attribuer des utilisateurs à un groupe précis. Paul et Pierre iront dans le **GRP1** et Nathalie et Isabelle iront dans le **GRP2**. Pour cela, nous allons faire un clic droit sur le **GRP1** puis **Propriétés** :

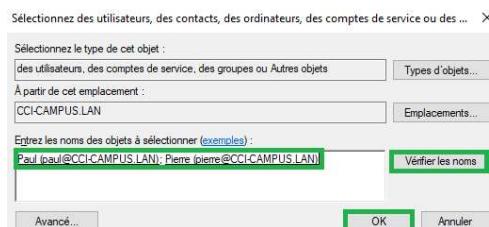


Ensuite on clique sur **Membres** et **Ajouter** :

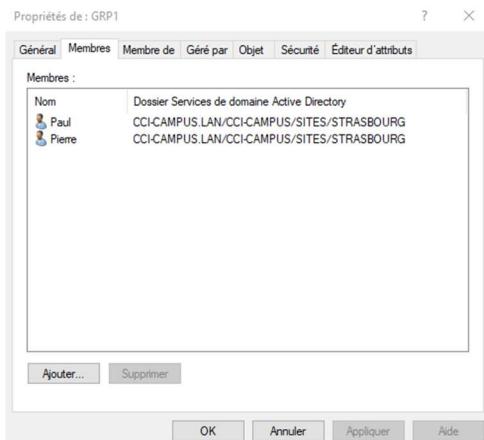


On clique dans l'encadré **Entrez les noms** et on rentre Paul puis on clique sur **Vérifier les noms**, pareil

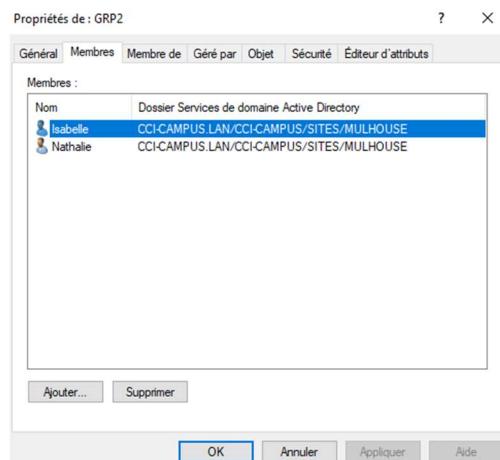
pour Pierre et ensuite on clique sur **OK** :



On peut voir qu'ils sont ajoutés dans le groupe :

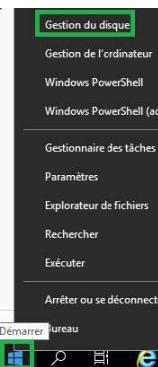


Faites pareil pour le **GRP2** en intégrant Nathalie et Isabelle :

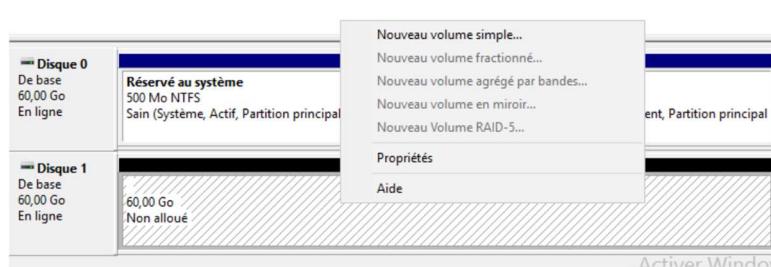


6.1.6) Partage de lecteur réseau

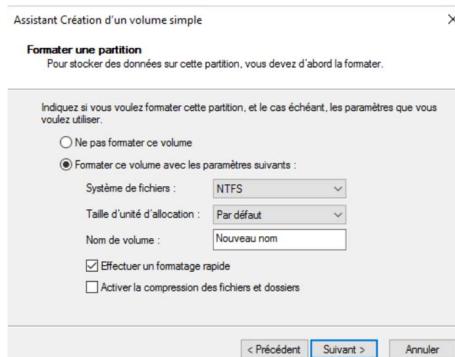
Avant de mettre en place le DFS, nous allons configurer le deuxième disque que nous avons ajouté conformément à la demande du client. Tout d'abord, nous allons vérifier que le second disque est bien initialisé. Pour cela, faites un clic droit sur le logo Windows puis cliquez sur **Gestionnaire de disque** :



Faites un clic droit sur le disque 1 et sélectionnez « En ligne ». Réaliser à nouveau un clic droit sur le disque et cliquez sur Initialiser le disque. Faites ensuite un clic droit dans l'espace non alloué du disque et cliquer sur **Nouveau volume simple** :



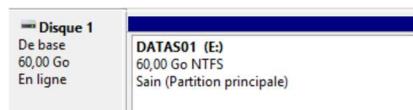
Cliquez sur **Suivant** trois fois de suite (deux fois si vous souhaitez changer la lettre du lecteur), et vous arrivez sur cette fenêtre de l'assistant :



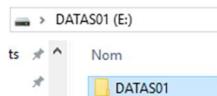
Modifiez le nom du volume en **DATAS01** :

Nom de volume :

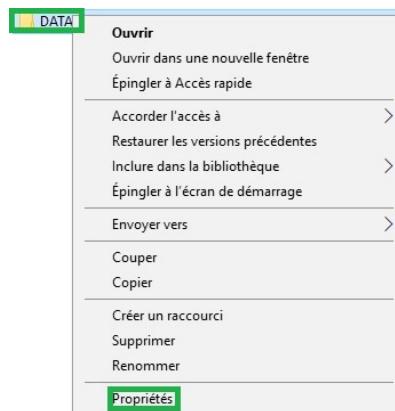
Faites **Suivant** puis **Terminer** :



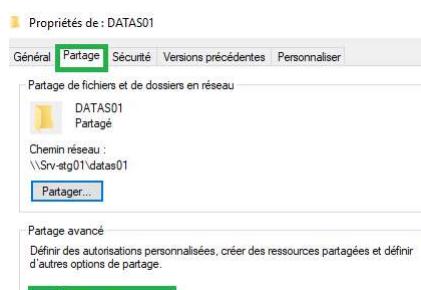
Maintenant que le disque est initialisé, nous allons créer un dossier à l'intérieur nommé **DATAS01** :



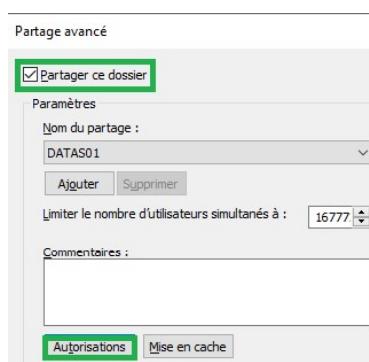
Ensuite, faites un clic droit sur le fichier puis **Propriétés** :



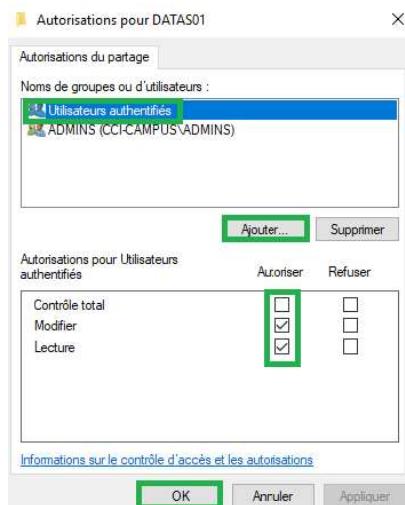
Allez sur l'onglet **Partage** puis cliquez sur l'onglet **Partage avancé** :



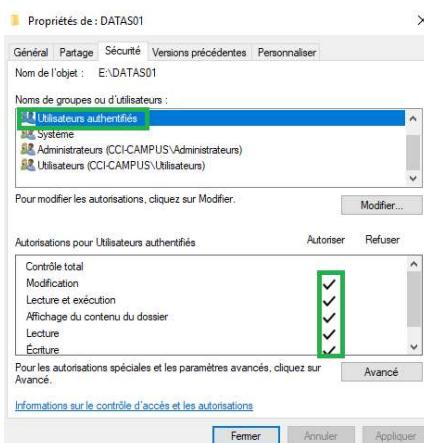
On coche **Partager ce dossier** puis on clique sur **Autorisations** :



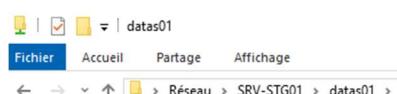
Ajoutez **Utilisateurs authentifiés** avec des autorisations en **lecture et modification** :



Allez dans l'onglet **Sécurité** et ajoutez **Utilisateurs authentifiés** avec tous les droits sauf Contrôle total :



Maintenant que le lecteur est partagé et accessible en réseau par le chemin <\\Srv-stg01\datas01> :

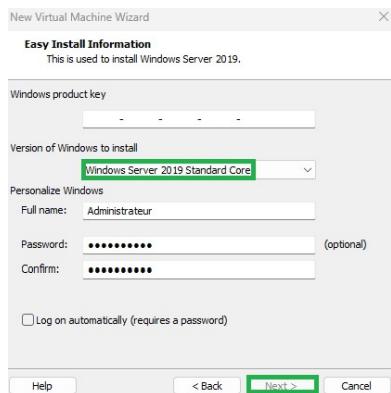


Nous allons mettre le reste de l'installation DFS en pause pour procéder à l'installation du serveur CORE SRV-STG02.

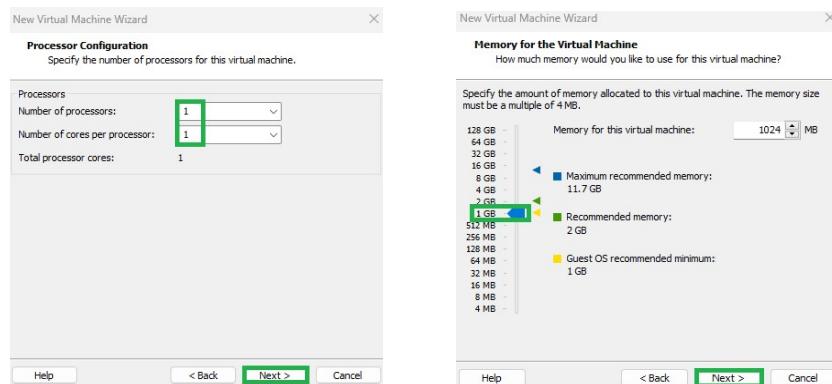
6.2) Serveur Windows 2019 CORE

6.2.1) Installation

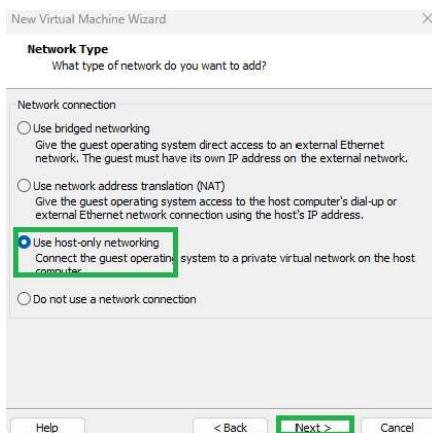
Comme pour le serveur GUI, nous allons créer une nouvelle machine VMware. La base est la même, il faut cliquer sur **File -> New Virtual Machine** puis on choisit Custom et on choisit le fichier ISO. C'est à partir de ce moment qu'il faut bien sélectionner la version **Standard Core** :



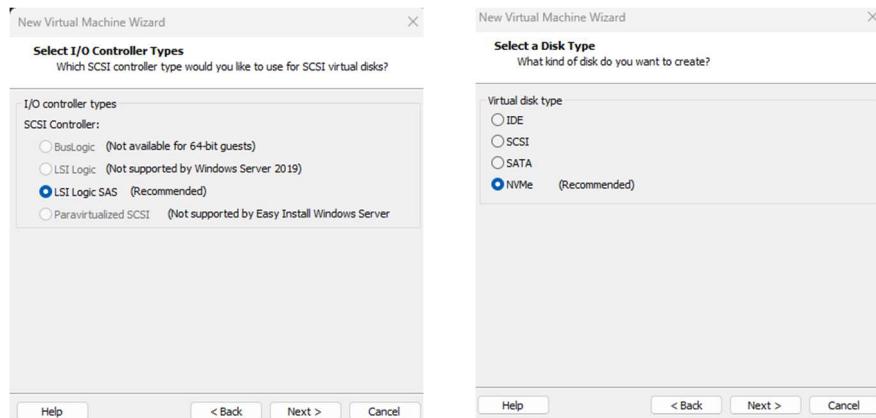
Comme la version Core ne possède pas d'interface graphique, elle n'a pas besoin d'autant de ressources pour fonctionner. Nous allons donc en profiter pour lui mettre uniquement le minimum recommandé 1 GB de RAM et 1 Processeur :



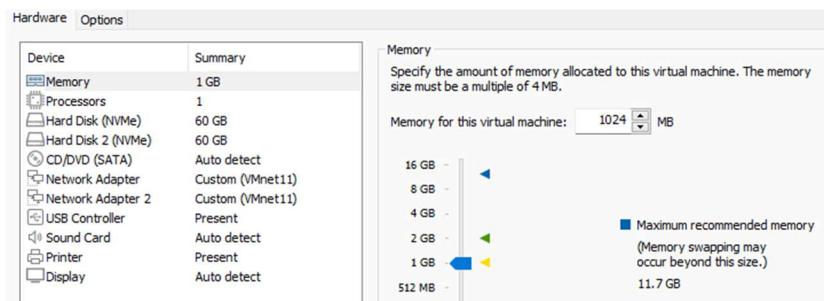
Nous allons la configurer en Host-only (il est possible de la changer plus tard) :



Puis :



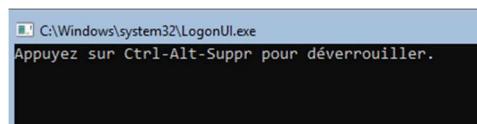
La suite est la même que pour le serveur GUI, On va créer deux disques de 60 GO et ajouter une deuxième carte réseau pour **l'IP BONDING**. L'installation est similaire au serveur GUI (voir installation plus haut dans le document).



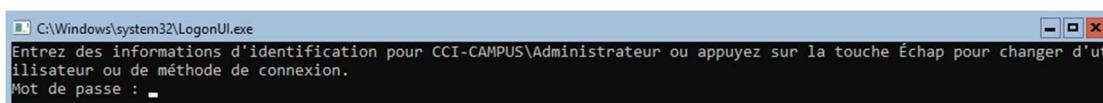
6.2.2) Configuration de base

Nous allons maintenant passer à la configuration du serveur Core. Comme la VM ne dispose pas d'interface graphique, nous allons devoir procéder différent du serveur GUI, néanmoins cela n'est pas beaucoup plus compliquer.

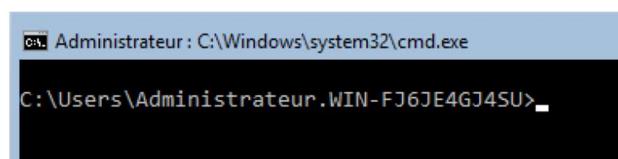
Pour commencer, nous arrivons sur la page de connexion qui est verrouillé :



Déverrouillez-la et on vous demandera un mot de passe, renseignez celui que vous avez choisi lors de la création de la VM :



Nous arrivons ici :



Malgré l'absence d'interface graphique, pour la configuration de base, nous n'allons pas rencontrer de problème insurmontable. Ici, il suffit de taper **sconfig** dans le terminal pour ouvrir l'outil qui va nous intéresser pour cette partie :

```
C:\ Administateur : C:\Windows\system32\cmd.exe - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. Tous droits réservés.

Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail : Domaine:
2) Nom d'ordinateur : WIN-FJ6IE4GI4SU
3) Ajouter l'administrateur local
4) Configurer l'administration à distance Activé
5) Paramètres de Windows Update : DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance : Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie Inconnu
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option :
```

Comme vous pouvez le constater, nous pour configurer la majorité de ce dont nous avons besoin par cet outil. Nous allons donc commencer par changer le nom du serveur par celui choisi dans la convention de nommage. Pour cela il suffit de taper le chiffre **2**, de renseigner le nouveau nom puis d'appuyer sur **Entrer** :

```
Entrez un nombre pour sélectionner une option : 2
Nom de l'ordinateur
Entrer un nouveau nom d'ordinateur (Vide=Annuler) : SRV-STG02
```

Après redémarrage, on peut voir que le serveur dispose maintenant du nom qu'on lui a défini :

```
=====
Configuration du serveur
=====

1) Domaine ou groupe de travail : Domaine:
2) Nom d'ordinateur : SRV-STG02
```

Cela peut être vérifié en retournant dans le terminal classique et en tapant la commande hostname :

```
C:\Users\Administrateur>hostname
SRV-STG02
```

On va ensuite désactiver le pare-feu avec la commande powershell suivante :

```
PS C:\Users\Administrateur> Set-NetFirewallProfile -Profile * -Enabled False
```

6.2.3) Agrégation de carte réseaux (IP BONDING)

Nous allons continuer par l'agrégation de carte réseaux. Pour cela, tapez **powershell** dans le terminal puis la commande **Get-NetIPInterface** pour lister les cartes réseaux :

ifIndex	InterfaceAlias	AddressFamily	NlMtu(Bytes)	InterfaceMetric	Dhcp	ConnectionSt.
6	Ethernet1	IPv6	1500	25	Enabled	Connected
2	isatap.{FD3BF83D-46DB-4BA6-8...	IPv6	1280	75	Disabled	Disconnected
3	isatap.{E15BC840-95DC-46B7-A...	IPv6	1280	75	Disabled	Disconnected
5	Ethernet0	IPv6	1500	25	Enabled	Connected
1	Loopback Pseudo-Interface 1	IPv6	4294967295	75	Disabled	Connected
6	Ethernet1	IPv4	1500	25	Enabled	Connected
5	Ethernet0	IPv4	1500	25	Enabled	Connected
1	Loopback Pseudo-Interface 1	IPv4	4294967295	75	Disabled	Connected

Nous pouvons remarquer nos deux cartes : **Ethernet0** et **Ethernet1**.

Pour créer une association de cartes réseau, nous allons utiliser le cmdlet « **New-NetLbfoTeam** » de la façon suivante :

```
PS C:\Users\Administrateur> New-NetLbfoTeam -Name "Aggregation" -TeamMembers Ethernet0,Ethernet1 -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses
```

On nous invite ensuite à confirmer. Tapez **T** pour dire **Oui** à tout :

```
Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Creates Team:'Aggregation' with TeamMembers:{'Ethernet0', 'Ethernet1'}, TeamNicName:'Aggregation',
TeamingMode:'SwitchIndependent' and LoadBalancingAlgorithm:'IPAddresses'.
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « 0 ») : T
```

L'agrégation est créée :

Name	:	Aggregation
Members	:	{Ethernet0, Ethernet1}
TeamNics	:	Aggregation
TeamingMode	:	SwitchIndependent
LoadBalancingAlgorithm	:	IPAddresses
Status	:	Down

Les deux cartes sont associées :

ifIndex	InterfaceAlias	AddressFamily	NlMtu(Bytes)	InterfaceMetric	Dhcp	ConnectionState	PolicyStore
10	Aggregation	IPv6	1500	20	Enabled	Connected	ActiveStore
2	isatap.{8A3597A0-F6DD-473D-8...	IPv6	1280	75	Disabled	Disconnected	ActiveStore
1	Loopback Pseudo-Interface 1	IPv6	4294967295	75	Disabled	Connected	ActiveStore
10	Aggregation	IPv4	1500	20	Enabled	Connected	ActiveStore
1	Loopback Pseudo-Interface 1	IPv4	4294967295	75	Disabled	Connected	ActiveStore

Il faut maintenant lui attribuer une IP fixe. Pour cela, on retourne sur l'outil sconfig et on fait le choix 8 :

```
Entrez un nombre pour sélectionner une option : 8

-----
Paramètres réseau
-----

Cartes réseau disponibles
Index#  Adresse IP      Description
       3     192.168.100.20 Microsoft Network Adapter Multiplexor Driver
```

Tapez 3 :

Index NIC	3
Description	Microsoft Network Adapter Multiplexor Driver
Adresse IP	192.168.100.20
Masque de sous-réseau	255.255.255.0
DHCP activé	Faux
Passerelle par défaut	192.168.100.254
Serveur DNS préféré	192.168.100.10
Serveur DNS auxiliaire	192.168.100.20

1) Définir l'adresse de la carte réseau
 2) Définir les serveurs DNS
 3) Effacer les paramètres du serveur DNS
 4) Retourner au menu principal

Puis tapez 1 pour définir l'ip comme ceci :

```
Sélectionner une option : 1

Sélectionner (D)HCP, IP (s)tatique (Vide=Annuler) : s
Définir IP statique
Entrer une adresse IP statique : 192.168.100.20
Entrer un masque de sous-réseau (Vide = par défaut 255.255.255.0) :
Entrer la passerelle par défaut : 192.168.100.254
Affectation d'une adresse IP statique à la carte réseau...
```

Tapez 2 pour renseigner le serveur **DNS** :

```
Sélectionner une option : 2
Serveurs DNS

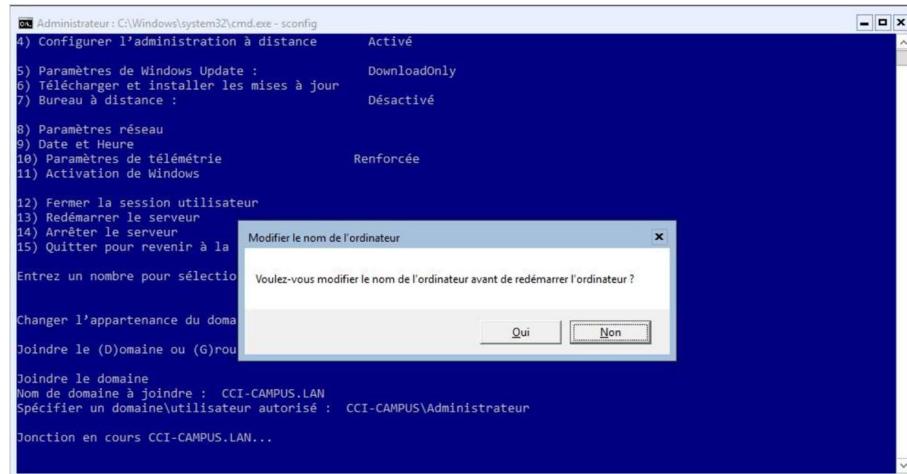
Entrer un nouveau serveur DNS préféré (Vide = Annuler) : 192.168.100.10
Entrer un autre serveur DNS (Vide = aucun) : 192.168.100.20
Serveur DNS alternatif défini.
```

On peut voir que tout est configuré conformément au plan d'adressage :

Index NIC	3
Description	Microsoft Network Adapter Multiplexor Driver
Adresse IP	192.168.100.20 fe80::fid6:ad0a:9706:7458
Masque de sous-réseau	255.255.255.0
DHCP activé	Faux
Passerelle par défaut	192.168.100.254
Serveur DNS préféré	192.168.100.10
Serveur DNS auxiliaire	192.168.100.20

6.2.4) AD DS (Active Directory et DNS)

Nous allons ensuite procéder à l'intégration au domaine. Pour cela retour sur sconfig et faire le choix
 1. On vous demandera quelques informations concernant le domaine à joindre ainsi qu'un compte
 habilité à joindre des machines dans le domaine. Cela fait, une fenêtre apparaît :

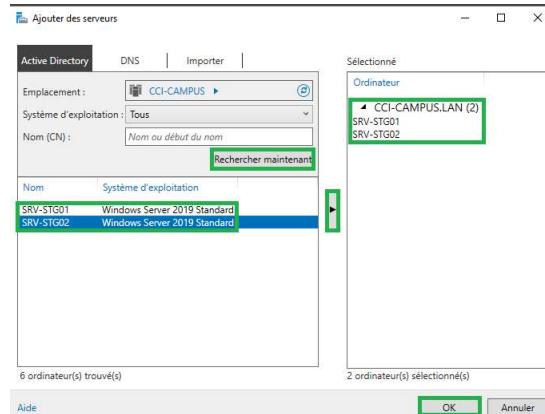


Choisissez **Non** puis on vous demandera de redémarrer le serveur. Cela fait, le serveur est dans le domaine. Nous allons maintenant retourner sur le serveur 1 pour intégrer le serveur Core au gestionnaire de serveurs. Cela simplifiera beaucoup le reste des opérations.

Pour cela, dans le **Gestionnaire de serveur**, rendez-vous dans l'onglet Tous les serveurs et faites un clic droit puis **Ajouter des serveurs** :



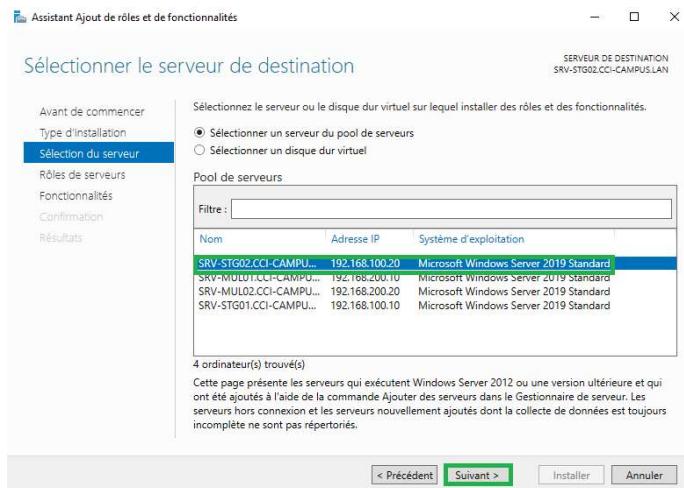
Cliquez sur **Rechercher maintenant**, la liste des serveurs apparaît, il suffit ensuite de cliquer sur le serveur concerné puis de cliquer sur la flèche pour que le nom du serveur se retrouve à droite dans les ordinateurs **Sélectionné**, validez avec **OK** :



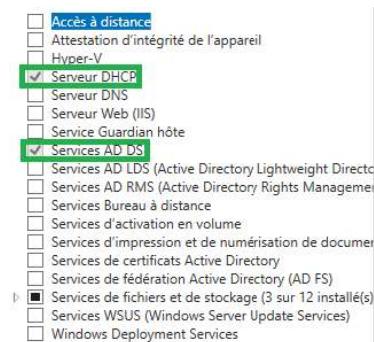
Vous pouvez faire pareil avec les serveurs de l'autre site (MULHOUSE) pour lesquels, l'installation et configuration de base reste la même (une fois les deux PFsense installés et le vpn configuré) :

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
SRV-STG02	192.168.100.20	En ligne - Compteurs de performances non démarré	29/12/2022 10:48:10	00429-70000-00000-AA872 (Activé)
SRV-STG01	192.168.100.10	En ligne - Compteurs de performances non démarré	29/12/2022 10:48:12	00429-70000-00000-AA321 (Activé)
SRV-MUL02	192.168.200.20	En ligne - Compteurs de performances non démarré	29/12/2022 10:48:12	00429-70000-00000-AA144 (Activé)
SRV-MUL01	192.168.200.10	Connecté	29/12/2022 10:48:14	00429-70000-00000-AA874 (Activé)

Ainsi les 4 serveurs sont visibles dans **Tous les serveurs**. Nous allons mettre en place la redondance ADDS sur le serveur Core de Strasbourg. Pour cela, rendez-vous dans le tableau de bord pour ajouter un nouveau rôle. Faite deux fois de suite **Suivant**, Sélectionnez ensuite le serveur que vous souhaitez mettre en contrôleur de domaine secondaire :



Cliquez sur **Suivant** puis cochez la case Services AD DS. On va également cocher la case Serveur DHCP pour configurer le basculement plus tard :

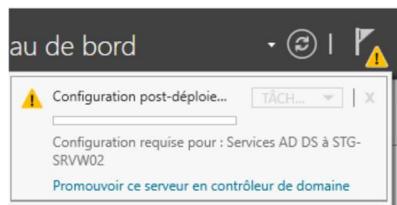


Une nouvelle fenêtre apparaît, cliquez sur **Ajouter des fonctionnalités** puis faites **Suivant** trois fois de suite. Vous pouvez maintenant installer le rôle.

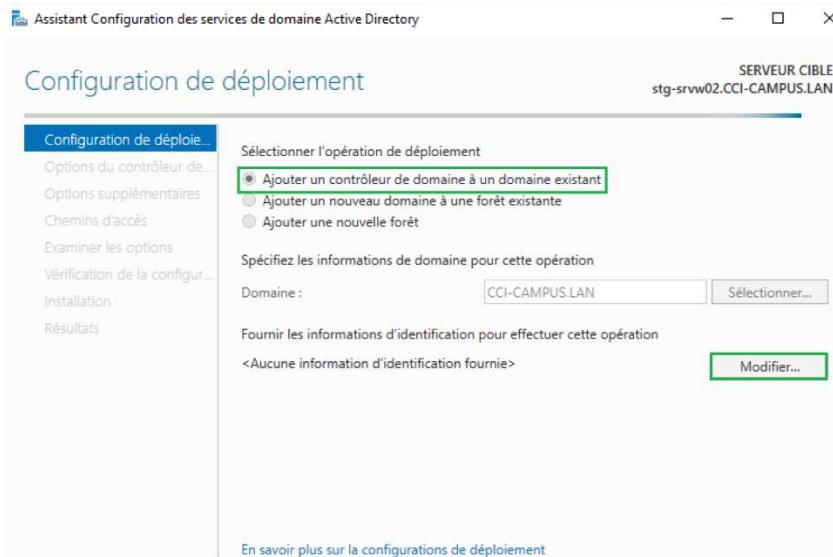
Une fois l'installation terminée, nous pouvons observer :



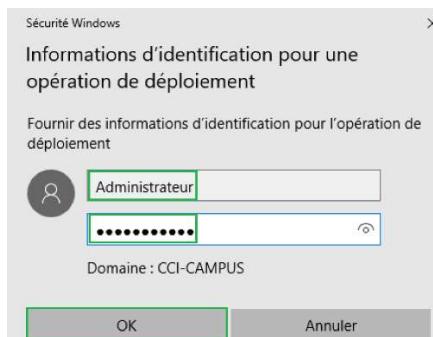
Cliquez ensuite sur l'icône drapeau puis sur **Promouvoir ce serveur en contrôleur de domaine** :



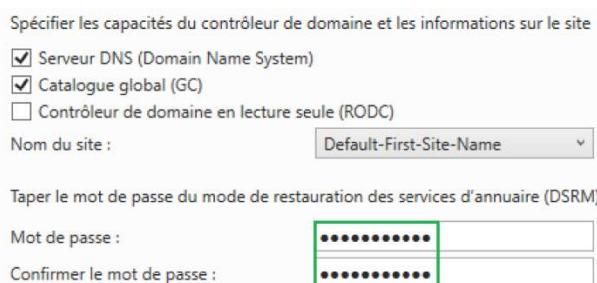
Une nouvelle fenêtre apparaît :



Cliquez sur **Modifier** et compléter avec le compte Administrateur du domaine et mot de passe :



Validez en tapant **OK** Cliquez ensuite sur **Suivant** et compléter en renseignant le mot de passe du **mode de restauration des services d'annuaires** défini sur le premier serveur :



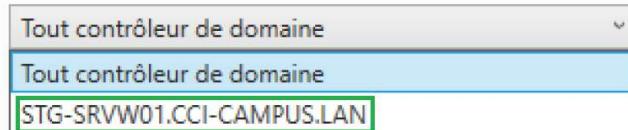
Faites ensuite **Suivant** deux fois de suite et sélectionnez votre serveur principal :

Spécifier les options d'installation à partir du support (IFM)

Installation à partir du support

Spécifier des options de réPLICATION supplémentaires

Répliquer depuis :



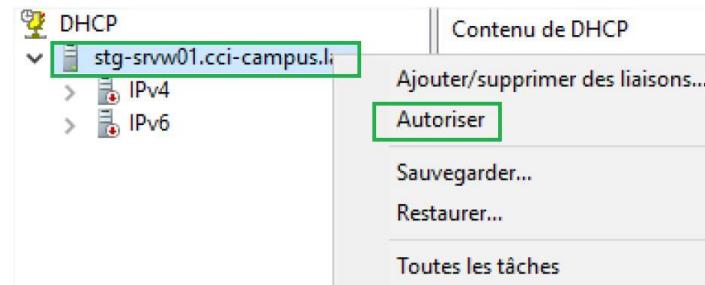
Cliquez sur **Suivant** trois fois de suite puis lancez l'installation. Une fois terminée, vous pouvez observer :



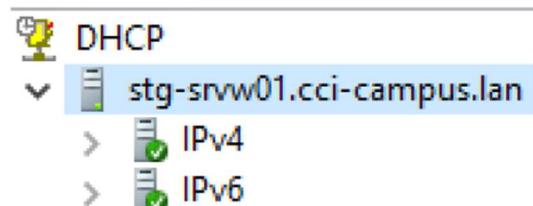
Le serveur est désormais un contrôleur de domaine Active directory.

7.2.5) Basculement DHCP

Passons maintenant à la configuration DHCP. Une fois installé depuis le serveur GUI et la configuration finie (exactement pareil que pour le serveur GUI) puis autoriser le serveur DHCP sur le serveur GUI puis le serveur Core en ouvrant le **Gestionnaire DHCP** puis en faisant un clic droit sur le serveur et en sélectionnant **Autoriser** :



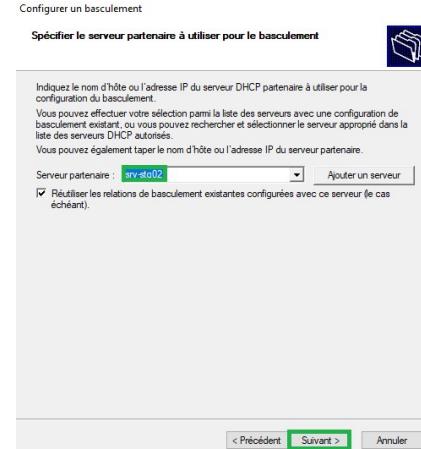
Une fois actualisé, nous pouvons voir :



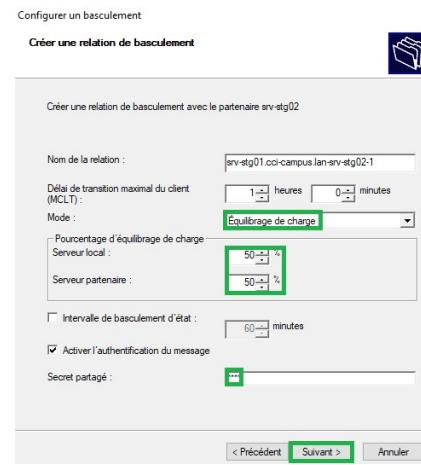
Faites pareil pour le serveur Core puis retournez sur le **Gestionnaire DHCP** du serveur 1 et faites un clic droit sur l'étendue qu'on a précédemment créée et cliquez sur **Configurer un basculement**, une fois l'assistant ouvert, cliquez sur **Suivant** :



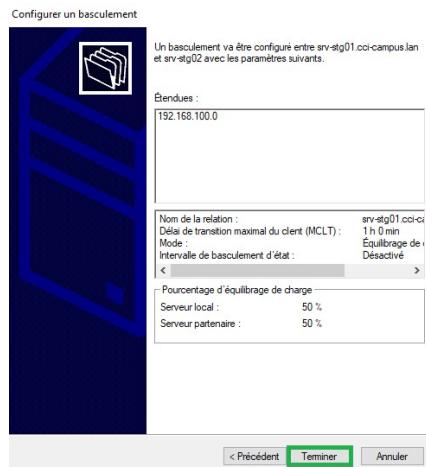
Cliquez sur Ajouter un serveur ou sur la flèche et dérouler pour voir si le second serveur apparaît :



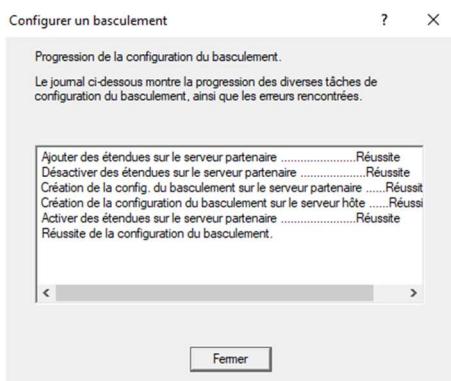
Configurer en **Équilibrage de charge** puis faire **50% 50%** et renseigner un **Secret partagé** puis cliquez sur **Suivant** :



Cliquez sur **Terminer** :



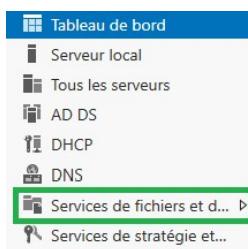
Nous pouvons voir que la configuration est réussie :



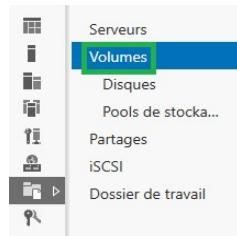
La configuration DHCP est terminée.

6.2.6) Partage de lecteur réseau

Avant de passer à la configuration de DFS, il va falloir initialiser le disque 2 du serveur 2 puis faire un partage réseau avec ce même disque. Pour cela plusieurs façons de faire. Tout d'abord l'outil **Diskpart**, disponible en ligne de commande ainsi que le cmdlet PowerShell **NETSHARE**. De notre côté, nous allons profiter du fait que nous avons ajouté le serveur 2 dans le **Gestionnaire de serveur** 1 et ainsi profiter de l'interface graphique. Commencez par cliquer sur le **Services de fichiers et de stockage** sur le **Gestionnaire de serveur** :



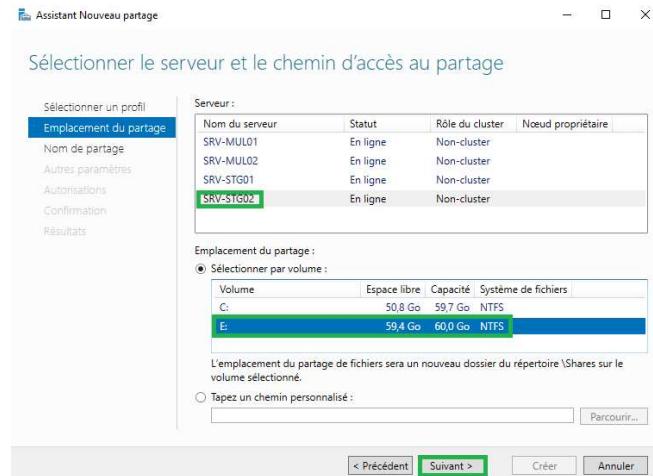
Cliquez ensuite sur **Volumes** :



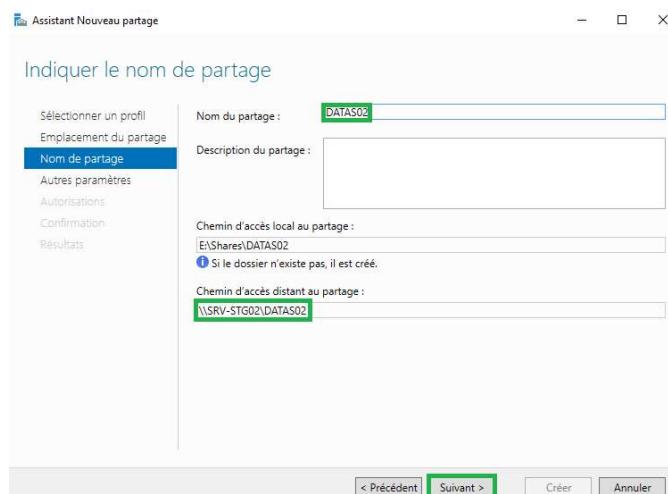
Sélectionnez le serveur 2 dans l'onglet **RESSOURCES PARTAGÉES** puis faites un clic droit sur **TACHES** puis **Nouveau partage** :

Un assistant s'ouvre, cliquez sur **Partage SMB -Rapide** puis sur **Suivant** :

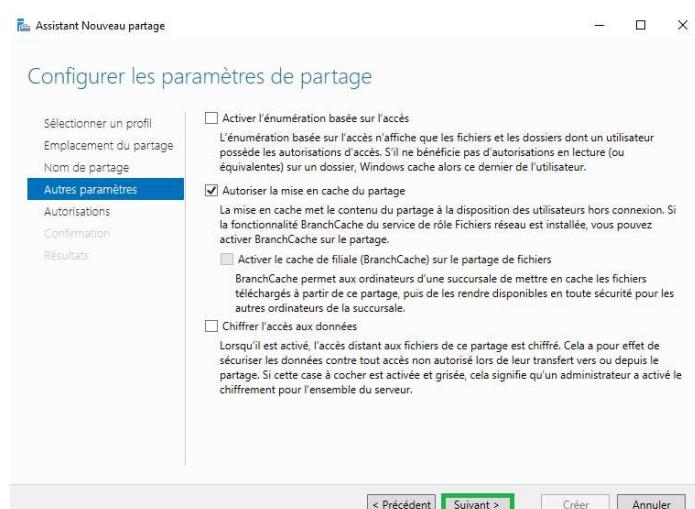
Choisir le bon serveur, puis le bon volume et cliquez sur **Suivant** :



Renseignez le nom du partage, conformément à l'annexe 2 puis vérifier le chemin d'accès distant et cliquez sur **Suivant :**



Laisser comme tel et cliquez sur **suivant :**



Cliquez sur **Personnaliser les autorisations :**

Spécifier les autorisations pour contrôler l'accès

Sélectionner un profil
Emplacement du partage
Nom de partage
Autres paramètres

Autorisations

Confirmation
Résultats

Les autorisations d'accès aux fichiers sur un partage sont définies par le biais d'une combinaison d'autorisations sur des dossiers, des partages et éventuellement une stratégie d'accès centrale.

Autorisations du partage : Contrôle total pour Tout le monde

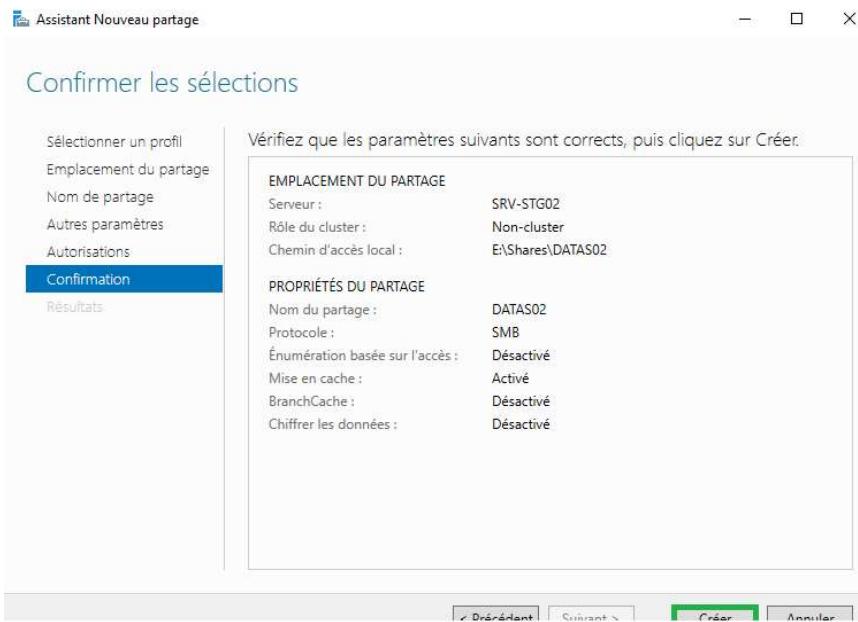
Autorisations sur le dossier :

Type	Principal	Accès	S'applique à
Autoris...	BUILTIN\Utilisateurs	Spécial	Ce dossier et les sous-dossiers
Autoris...	BUILTIN\Utilisateurs	Lecture et exécution	Ce dossier, les sous-dossiers et les f
Autoris...	CREATEUR PROPRIETAIRE	Contrôle total	Les sous-dossiers et les fichiers seul
Autoris...	AUTORITE NT\Système	Contrôle total	Ce dossier, les sous-dossiers et les f
Autoris...	BUILTIN\Administrateurs	Contrôle total	Ce dossier, les sous-dossiers et les f
Autoris...	BUILTIN\Administrateurs	Contrôle total	Ce dossier seulement

< >

Personnaliser les autorisations...

Ajoutez les autorisations nécessaires en partage et en sécurité comme pour le serveur 1 puis validez et cliquez sur Créer :

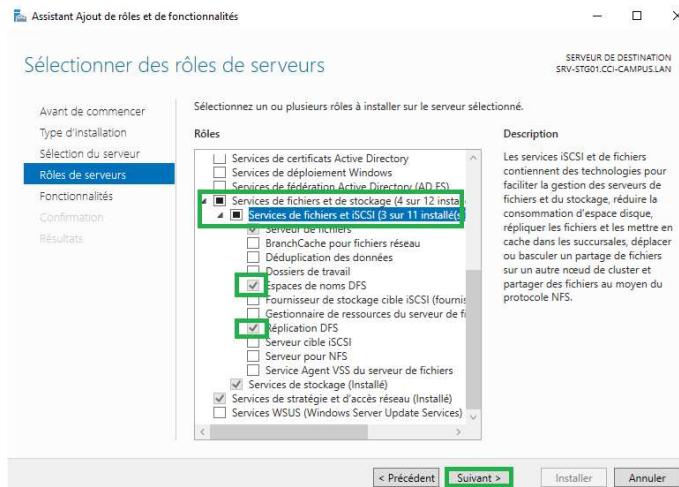


Le partage est désormais accessible sur le réseau :

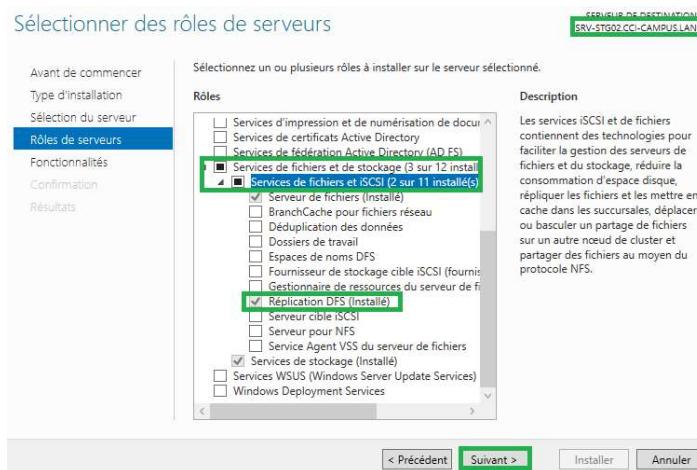


6.2.7) DFS et DFS-R

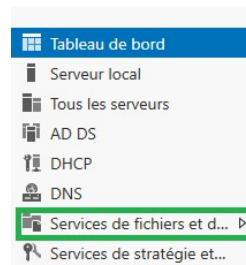
Nous allons maintenant procéder à l'installation DFS sur le serveur 1. Pour cela il faut se diriger vers l'installation des rôle et fonctionnalités puis de faire suivant 3 fois, une fois arrivé sur les rôles à installer, il faut dérouler Services de fichiers et de stockage puis Services de fichiers et iSCSI. Cochez ensuite Espaces de noms DFS puis RéPLICATION DFS :



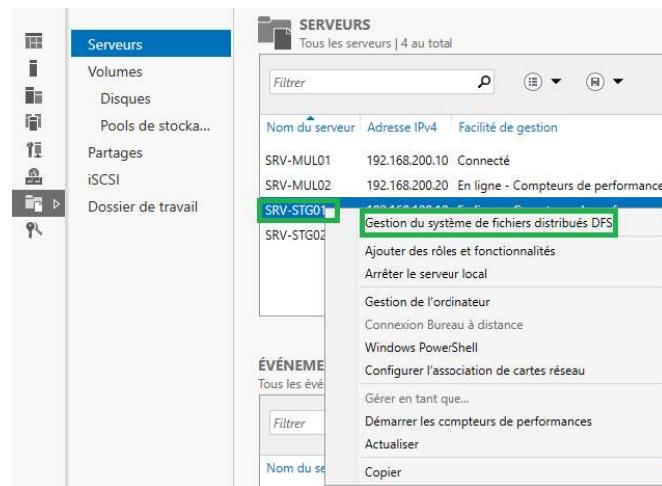
Ensuite faites suivant puis procéder à l'installation. Une fois l'installation terminé faites pareil sur le serveur 2 sans l'espace de noms. Les autres serveurs n'auront besoin que de la réPLICATION DFS :



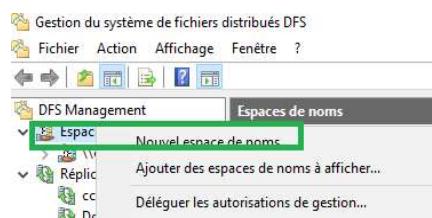
Une fois cela fait sur les 4 serveurs, nous allons créer l'Espace de nom. Pour cela, sur le Gestionnaire de serveur, cliquez sur Services de fichiers et de stockage :



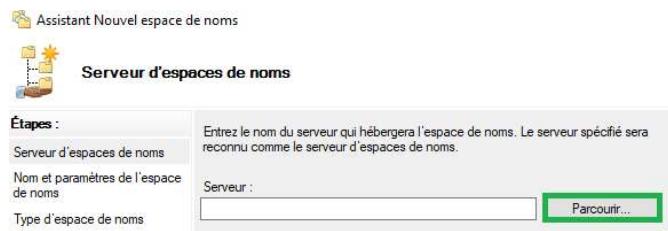
Puis faites un clic droit sur le serveur 1 et **Gestion du système de fichiers distribués DFS** :



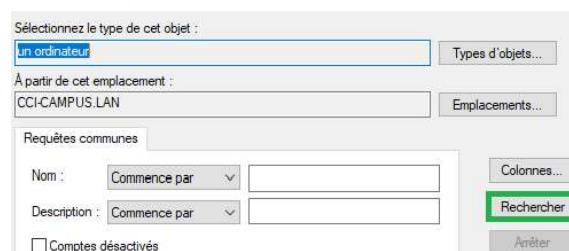
Faites un clic droit sur Espace de noms puis Nouvel espace de noms :



Appuyez sur Parcourir :



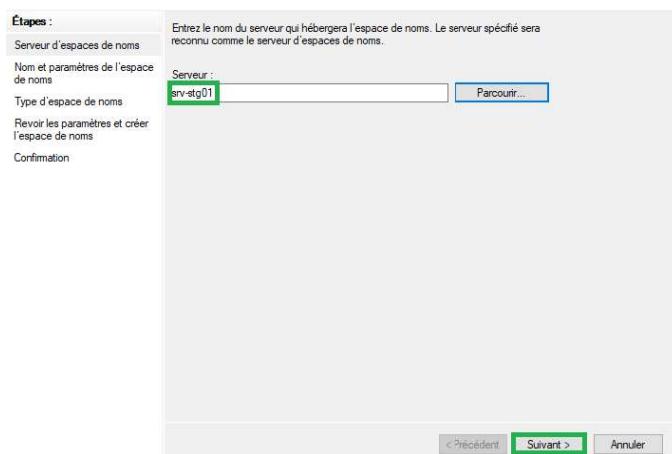
Cliquez sur Avancer puis Rechercher :



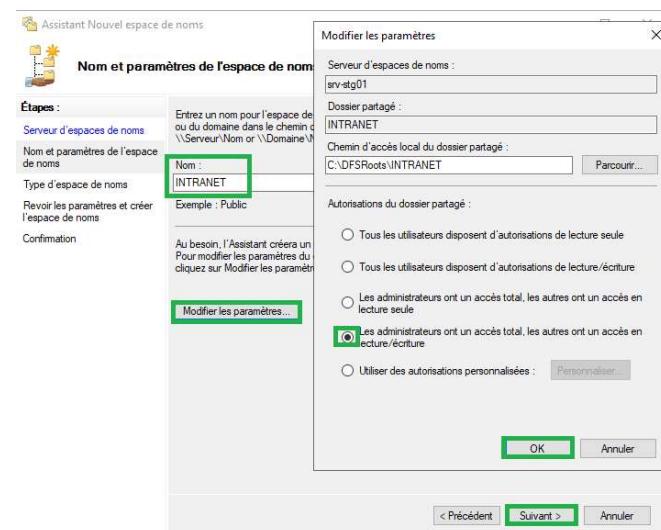
Sélectionnez le bon serveur puis validez :



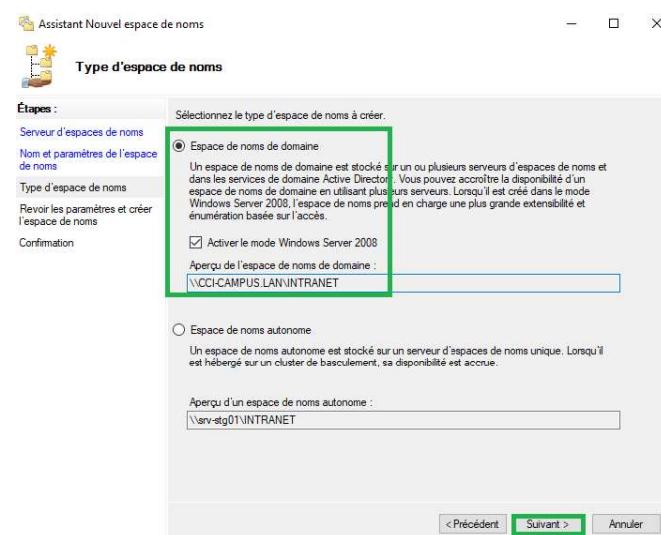
Cliquez sur Suivant :



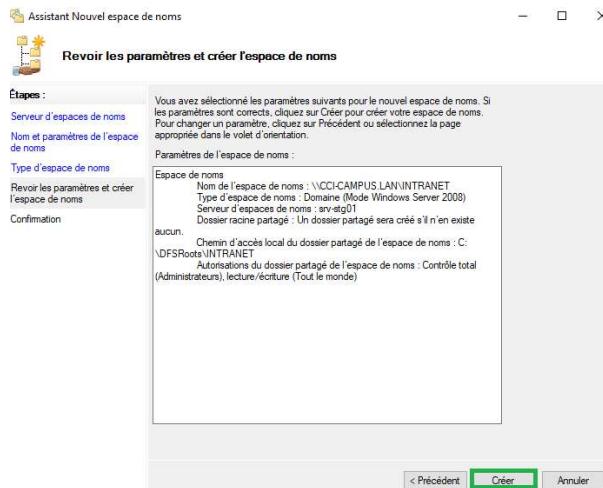
Conformément à l'annexe 2, le nom de l'espace sera INTRANET, ensuite appuyez sur Modifier les paramètres puis cochez la case comme sur la capture et appuyez sur OK. Ensuite cliquez sur Suivant :



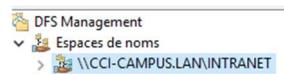
Choisir Espace de noms de domaine puis cliquez sur Suivant :



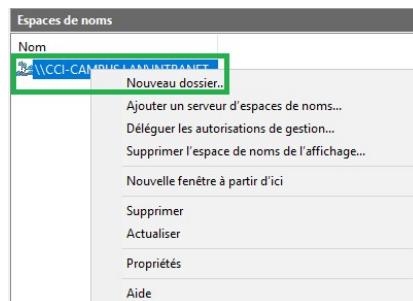
Cliquez ensuite sur créer :



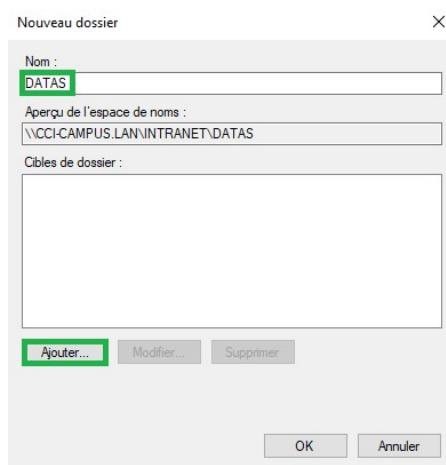
L'espace de nom est désormais visible sur le Gestionnaire DFS :



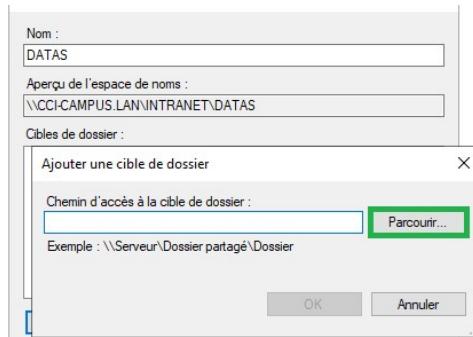
Faites un clic droit sur l'espace de nom puis cliquez sur Nouveau dossier :



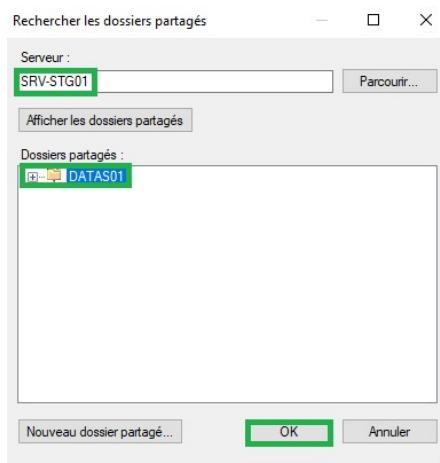
Renseignez un nom pour ce dossier puis cliquez sur Ajouter :



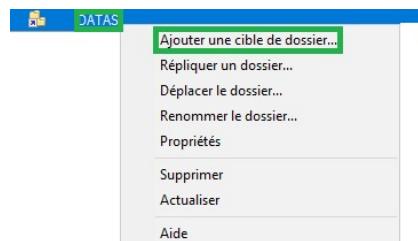
Cliquez sur Parcourir :



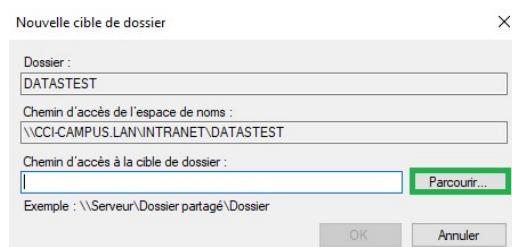
Cliquez sur parcourir puis sur le dossier DATAS du serveur et appuyez sur OK. Validez pour la création du dossier :



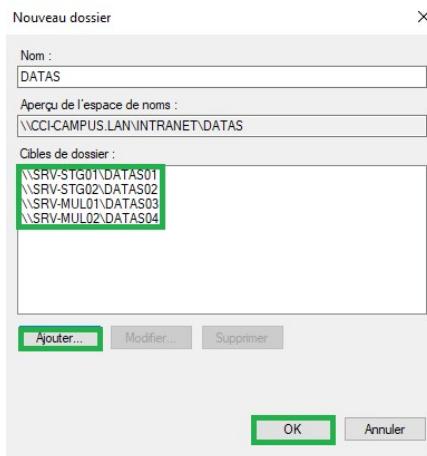
Faites un clic droit sur le nouveau dossier puis cliquez sur Ajouter une cible de dossier :



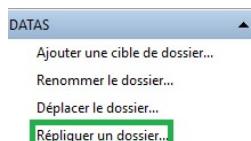
Cliquez sur Parcourir :



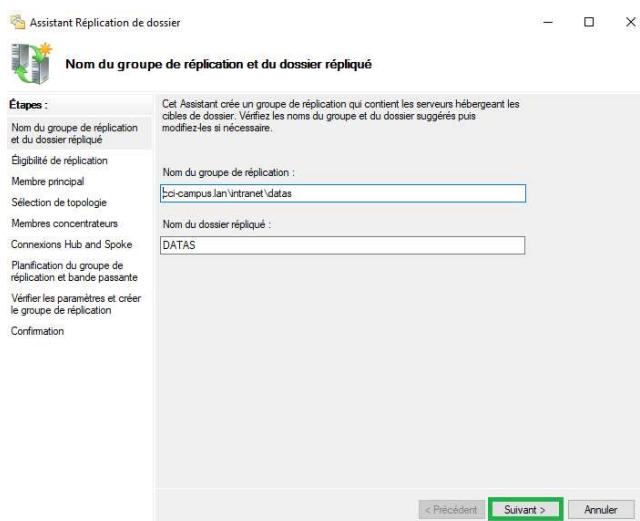
Faites pareil pour tous les serveurs (pointer vers les dossiers DATAS01,02,03,04) :



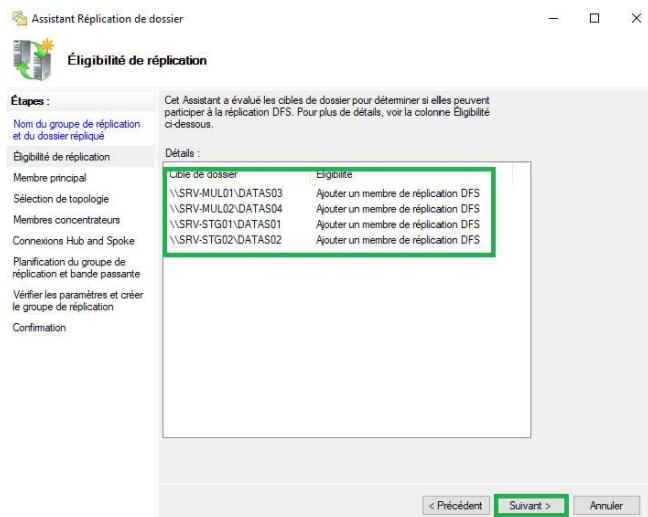
Une fois validé, cliquez sur Répliquer un dossier :



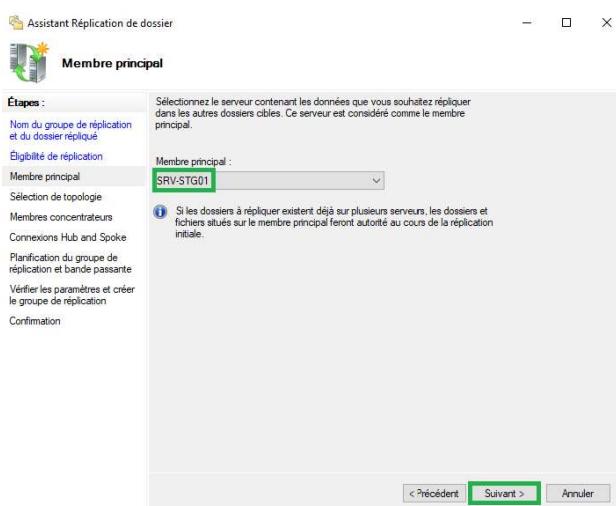
Puis cliquez sur suivant :



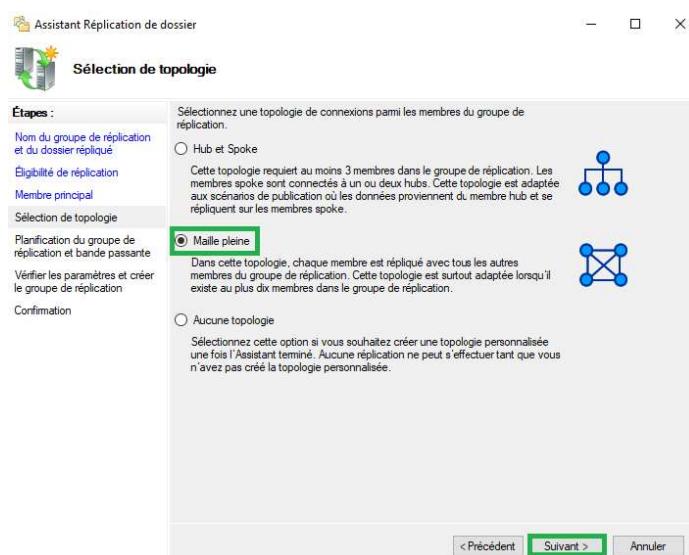
On peut voir les cibles de dossier. Cliquez sur Suivant :



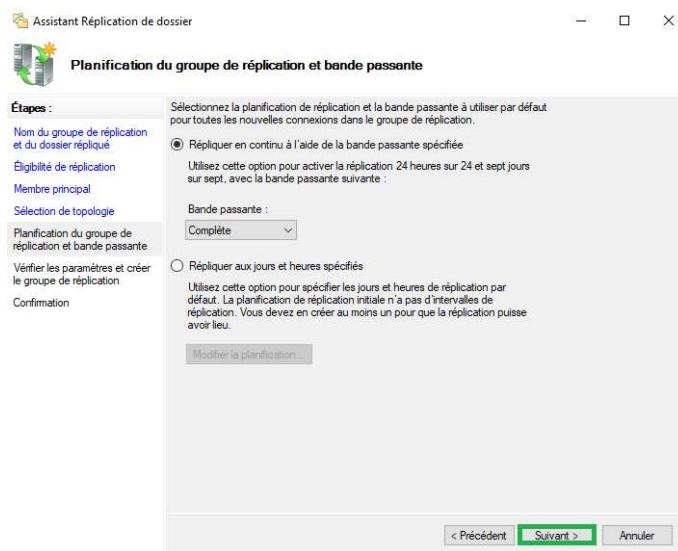
Choisissez le serveur 1 puis cliquez sur Suivant :



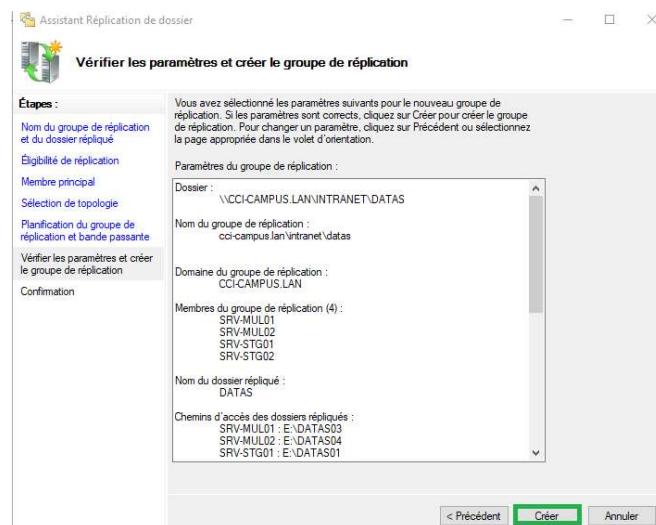
Choisissez la topologie Maille pleine puis cliquez sur Suivant :



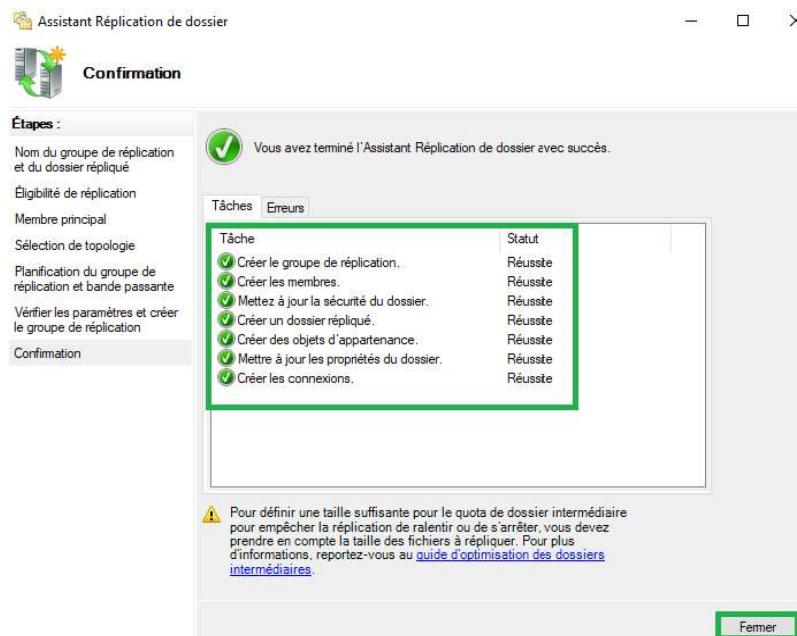
Cliquez sur Suivant :



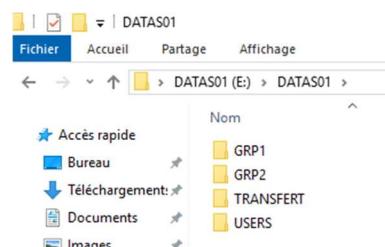
Cliquez sur Créer :



Vous pouvez voir que la réplication est effective. Cliquez sur fermer :



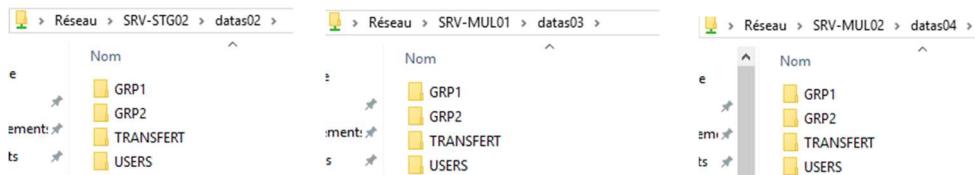
Nous allons maintenant créer des dossiers GRP1, GRP2, TRANSFERT et USERS sur le serveur 1 en local avec les droits nécessaires, indiqués dans l'annexe 2 :



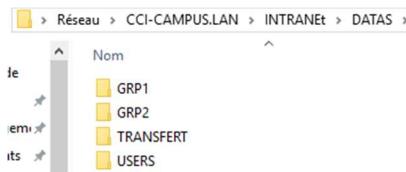
Avec les droits :

Type	Principal	Accès	Type	Principal	Accès
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Autoriser	Utilisateurs authentifiés	Modifier
Auto...	GRP1 (CCI-CAMPUS\GRP1)	Modification	Autoriser	ADMINS (CCI-CAMPUS\ADMINS)	Contrôle total
Auto...	Système	Contrôle total			
Auto...	Administrateurs (CCI-CAMPUS\ADMINS)	Contrôle total			
Type	Principal	Accès	Type	Principal	Accès
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Autoriser	Utilisateurs authentifiés	Modifier
Auto...	GRP2 (CCI-CAMPUS\GRP2)	Modification	Autoriser	ADMINS (CCI-CAMPUS\ADMINS)	Contrôle total
Auto...	Système	Contrôle total			
Auto...	Administrateurs (CCI-CAMPUS\ADMINS)	Contrôle total			
Type	Principal	Accès	Type	Principal	Accès
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Autoriser	Utilisateurs authentifiés	Modifier
Auto...	Système	Contrôle total	Autoriser	ADMINS (CCI-CAMPUS\ADMINS)	Contrôle total
Auto...	Administrateurs (CCI-CAMPUS\ADMINS)	Contrôle total			
Auto...	Utilisateurs authentifiés	Modification			
Type	Principal	Accès	Type	Principal	Accès
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Autoriser	Utilisateurs authentifiés	Modifier
Auto...	Utilisateurs authentifiés	Modification	Autoriser	ADMINS (CCI-CAMPUS\ADMINS)	Contrôle total
Auto...	Système	Contrôle total			
Auto...	Administrateurs (CCI-CAMPUS\ADMINS)	Contrôle total			

Après quelques minutes nous pouvons voir que les dossiers sont répliqués sur tous les serveurs :



Ainsi que sur l'espace de nom :



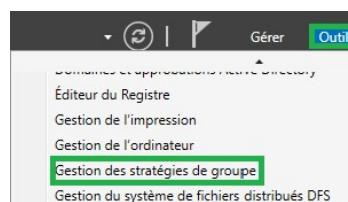
6.2.8) GPO

Pour finir, nous allons configurer les GPO utilisateurs comme indiqué dans l'annexe 2.

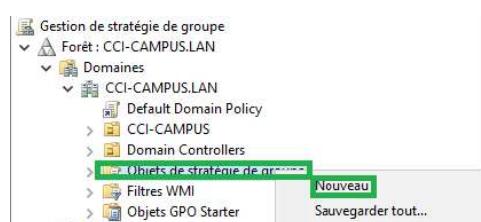
a) Lecteurs réseaux et redirection de dossiers

Pour commencer, nous allons créer une GPO qui créera automatiquement un dossier utilisateur dans le dossier USERS de l'espace de nom et qui va mapper 2 lecteurs (U et T) et faire une redirection du dossier Bureau et Document vers le dossier %USERNAME%.

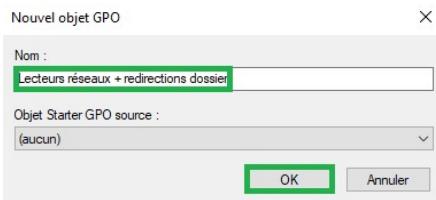
Pour cela, rendez-vous sur le **Gestionnaire de serveur**, cliquez sur **Outils** puis sur **Gestionnaire de stratégie de groupes** :



Déroulez jusqu'à l'UO **Objets de stratégie de groupe**, faites un clic droit puis cliquez sur **Nouveau** :



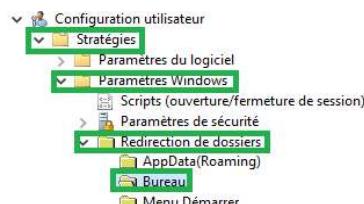
Renseignez le nom de la stratégie puis cliquez sur OK :



Faites clic droit sur la stratégie puis Modifier :

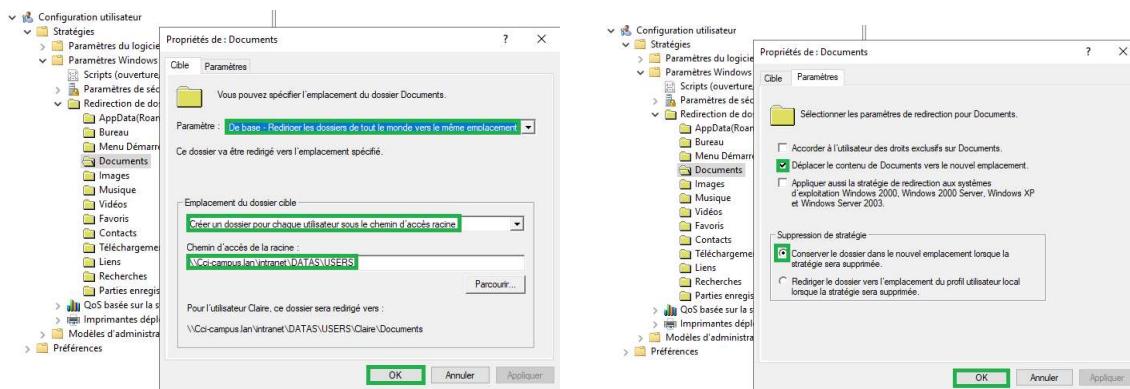
Objets de stratégie de groupe dans CCI-CAMPUS.LAN

Tout d'abord, nous allons configurer la redirection de dossier. Pour cela, on déroule Configuration utilisateur -> Paramètres Windows -> Redirection de dossier puis bureau :

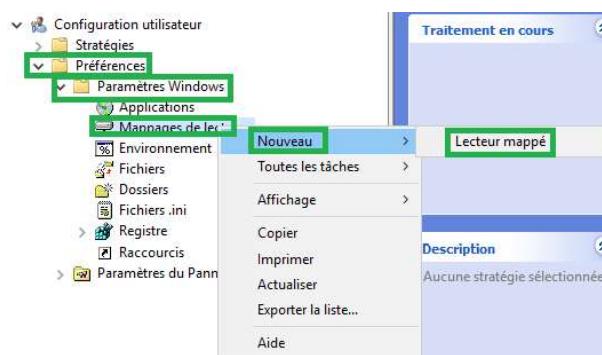


Faites un clic droit puis **Propriétés** et remplissez comme la capture suivante :

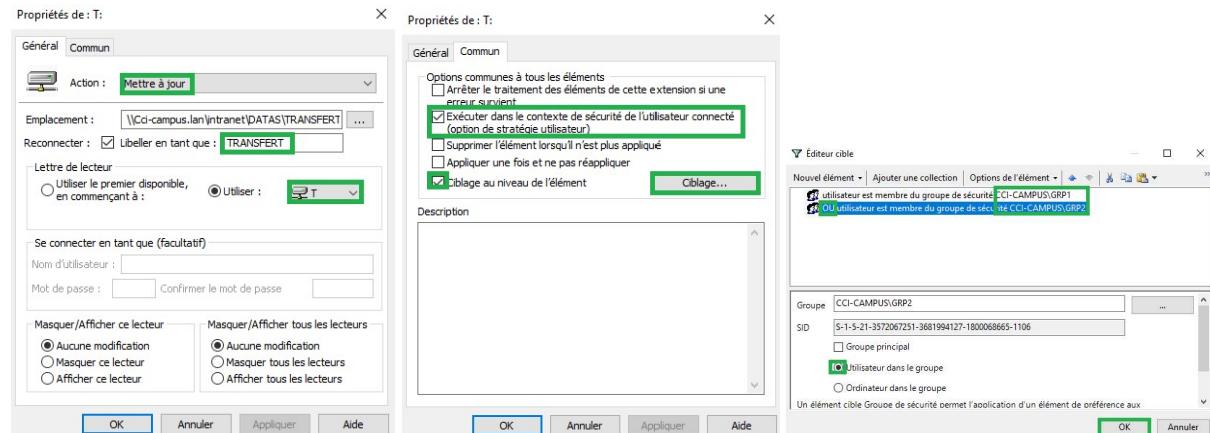
Validez puis faites pareil pour Documents :



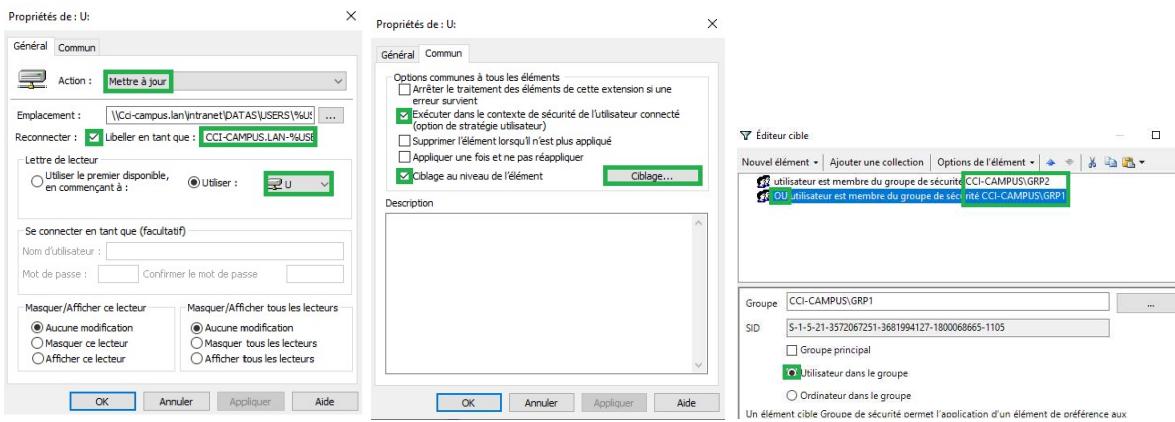
Ensuite nous allons faire le mappage des 2 lecteurs. Toujours sur la Configuration utilisateur -> Préférences -> Paramètres Windows puis faites un clic droit sur Mappage de lecteurs :



On commence par le lecteur T, remplissez comme les captures suivantes :



Puis le lecteur U :



Ce qui nous donne ceci :

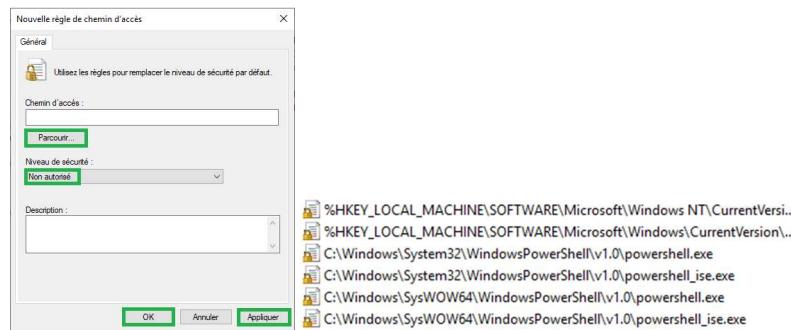
Nom	Ordre	Action	Chemin d'accès	Reconnecter
T:	2	Mettre à jour	\Cci-campus.lan\intranet\DATA\USERS\%u\	Oui
U:	1	Mettre à jour	\Cci-campus.lan\intranet\DATA\USERS\%u\	Oui

Passons maintenant à la GPO des restrictions à tous les utilisateurs. Créez une GPO utilisateurs puis Modifier. Détourez Configuration ordinateur -> Stratégies -> Modèles d'administration -> Système -> Accès au stockage amovible puis faites un double clic sur Toutes les classes de stockage amovible et cochez Activé :

Paramètre	État
Définir le délai (en secondes) avant de forcer le redémarrage	Non configuré
CD et DVD : refuser l'accès en exécution	Non configuré
CD et DVD : refuser l'accès en lecture	Non configuré
CD et DVD : refuser l'accès en écriture	Non configuré
Classes personnalisées : refuser l'accès en lecture	Non configuré
Classes personnalisées : refuser l'accès en écriture	Non configuré
Lecteurs de disquettes : refuser l'accès en exécution	Non configuré
Lecteurs de disquettes : refuser l'accès en lecture	Non configuré
Lecteurs de disquettes : refuser l'accès en écriture	Non configuré
Disques amovibles : refuser l'accès en exécution	Non configuré
Disques amovibles : refuser l'accès en lecture	Non configuré
Disques amovibles : refuser l'accès en écriture	Non configuré
Toutes les classes de stockage amovible : refuser tous les accès...	Activé
Tout stockage amovible : permet l'accès direct pendant des ...	Non configuré

Toujours dans le même GPO, nous allons bloquer l'accès à powershell. Détourez comme sur la capture suivante :

Faites un clic droit sur Règles supplémentaires puis Nouvelle règle de chemin d'accès et renseignez le chemin à restreindre, bien choisir Non Autorisé puis appliquer. Fait de même avec tout les accès powershell comme sur les captures suivantes :



C'est au tour du panneau de configuration. Déroulez comme sur la capture suivante puis faites un double clic sur Interdire l'accès au Panneau de configuration et Activé :

Paramètre	État
Affichage	Non configuré
Ajouter ou supprimer des programmes	Non configuré
Imprimantes	Non configuré
Options régionales et linguistiques	Non configuré
Personnalisation	Non configuré
Programmes	Non configuré
Masquer les éléments du Panneau de configuration spécifiés	Non configuré
Toujours afficher tous les éléments du Panneau de config...	Non configuré
Interdire l'accès au Panneau de configuration et à l'applicati...	Activé
N'afficher que les éléments du Panneau de configuration sp...	Non configuré
Visibilité de la page des paramètres	Non configuré

On continue avec l'invite de commande qui se situe :

Paramètre	État
Gestion de la communication Internet	Non configuré
Installation de pilotes	Non configuré
Options Ctrl+Alt+Suppr	Non configuré
Options d'atténuation	Non configuré
Ouverture de session	Non configuré
Profils utilisateur	Non configuré
Redirection de dossiers	Non configuré
Scripts	Non configuré
Services Paramètres régionaux	Non configuré
Stratégie de groupe	Non configuré
Télécharger les composants manquants	Non configuré
Interprétation du siècle pour l'an 2000	Non configuré
Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré
Ne pas afficher l'écran de démarrage Mise en route à l'ouver...	Non configuré
Interface utilisateur personnalisée	Non configuré
Désactiver l'accès à l'invite de commandes	Activé

Et on finit par masquer les lecteurs locaux des postes :

Paramètre	État
Démarrer l'Explorateur de fichiers avec le ruban réduit	Non configuré
Désactiver l'affichage des extraits en mode d'affichage Cont...	Non configuré
Ne pas rechercher les raccourcis de l'environnement lors de...	Non configuré
Nombre maximal de documents récents	Non configuré
Supprimer les fonctionnalités de gravure de CD	Non configuré
Désactiver la mise en cache des miniatures	Non configuré
Supprimer l'interface utilisateur permettant de modifier les ...	Non configuré
Supprimer l'interface utilisateur permettant de modifier les ...	Non configuré
Supprimer l'onglet DFS	Non configuré
Dans Poste de travail, masquer ces lecteurs spécifiés	Activé
Ne pas afficher « Tout le réseau » dans les emplacements rés...	Non configuré
Supprimer le menu Fichier de l'Explorateur de fichiers	Non configuré
Ne pas autoriser l'ouverture des Options des dossiers à partir...	Non configuré
Supprimer l'onglet Matériel	Non configuré
Masquer l'élément Gérer le menu contextuel de l'Explorateur...	Non configuré
Supprimer les Documents partagés du Poste de travail	Non configuré
Supprimer les options « Connecter un lecteur réseau » et « D...»	Non configuré
Ne pas déplacer les fichiers supprimés vers la Corbeille	Non configuré

La dernière GPO permettra de déployer un fond d'écran identiques à tous les utilisateurs puis de bloquer la modification. Tout d'abord, créer un dossier sur un des partages réseaux puis vous pouvez y copier le papier peint que vous souhaitez. Ensuite, faites comme sur la capture suivante :

Paramètre	État	Commentaire
Activer Active Desktop	Non configuré	Non
Désactiver Active Desktop	Non configuré	Non
Interdire les modifications	Non configuré	Non
Papier peint du Bureau	Activé	Non
Empêcher l'ajout d'éléments	Non configuré	Non
Empêcher la fermeture d'éléments	Non configuré	Non
Empêcher la suppression d'éléments	Non configuré	Non
Désactiver tous les éléments	Non configuré	Non
Ajouter/supprimer des éléments	Non configuré	Non
N'autoriser que les papiers peints au format bmp	Non configuré	Non

Papier peint du Bureau

Pris en charge sur: Au minimum Windows 2000

Options:

Style du papier peint:

Aide:

Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

Exemple : avec un chemin local : C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC : \\SeverShare\Corp.jpg

Pour utiliser ce paramètre, entrez le chemin d'accès complet et le nom du fichier de l'image à paramétrer. Vous pouvez taper un chemin d'accès local, tel que C:\Windows\accueil.jpg ou un chemin d'accès UNC, tel que \\Serveur\Partage\Logo.jpg. Si le fichier spécifié n'est pas disponible lorsque l'utilisateur ouvre sa session, aucun papier peint n'est

Voilà, toutes nos GPO sont créées et prêtes à être liées à l'UO de notre choix. Nous allons les lier à la racine de L'UO SITES :

- Forêt : CCI-CAMPUS.LAN
- Domains
 - CCI-CAMPUS.LAN
 - Default Domain Policy
 - CCI-CAMPUS
 - GROUPE
 - SITES
 - bloquer
 - Copie et déploiement fond d'écran
 - Création Lecteur réseau U (%username%)
 - Utilisateurs
 - MULHOUSE
 - Ordinateur
 - STRASBOURG

Veuillez à bien à refuser l'application des GPO pour les administrateurs dans la délégation de la GPO puis Avancé en bas à droite. Choisir Admins du domaine puis cochez Refusez sur la case Appliquer la stratégie de groupe :

Etendue	Détails	Paramètres	Délégation	État
Ces groupes et utilisateurs ont l'autorisation spécifiée pour cet objet de stratégie de groupe.				
Groupes et utilisateurs :				
Nom	Authorisations acceptées	Hérité		
Administrateurs de l'entre...	Modifier les paramètres, supprimer, modifier la s...	Non		
Admins du domaine (CCI...	Personnalisé	Non		
ENTREPRISE DOMAIN ...	Lecture	Non		
Système	Modifier les paramètres, supprimer, modifier la s...	Non		
Utilisateurs authentifiés	Lecture (à partir du filtre de sécurité)	Non		

Paramètres de sécurité pour Utilisateurs

Sécurité

Noms de groupes ou d'utilisateurs :

- CREATEUR PROPRIÉTAIRE
- Utilisateurs authentifiés
- Système
- Administrateurs du domaine (CCI-CAMPUS\Admins du domaine)**

Ajouter... Supprimer

Autorisations pour Administrateurs du domaine

	Autoriser	Refuser
Écrire	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Créer tous les objets enfants	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Supprimer tous les objets enfants	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Appliquer la stratégie de groupe	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>

Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

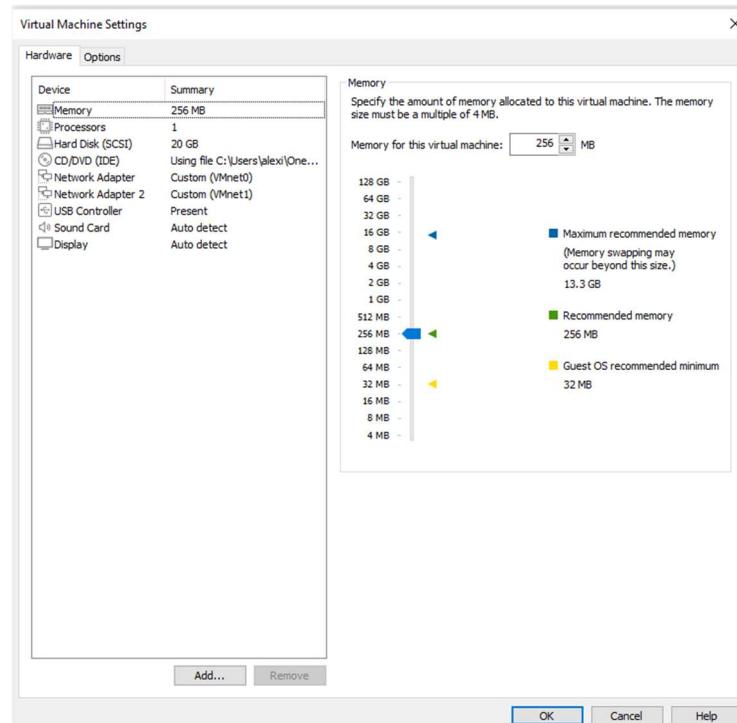
Informations sur le contrôle d'accès et les autorisations

OK Annuler Appliquer

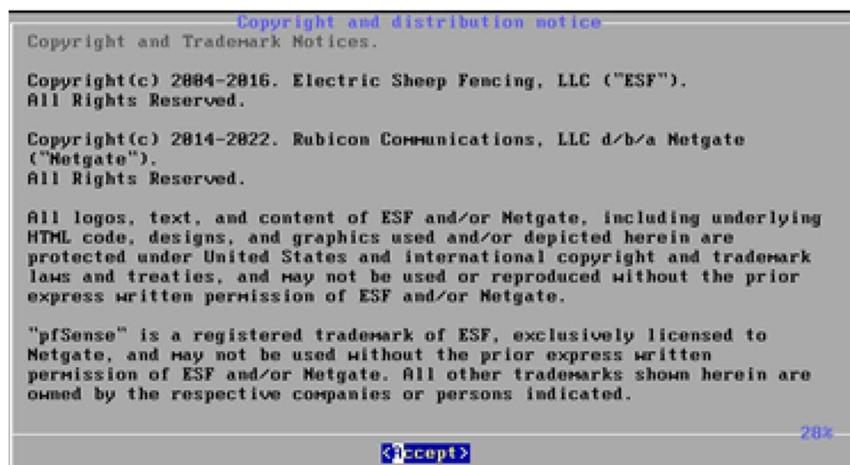
6.3) PFSense, VPN, Portail Captif

6.3.1) Installation pfSense

Dans un premier temps, veuillez configurer vos VM pfSense de cette manière avec **deux cartes réseaux**, l'une en **NAT** ou en **Bridge** que l'on a décidé de laisser en **DHCP** et l'autre en **host-only** pour le LAN.



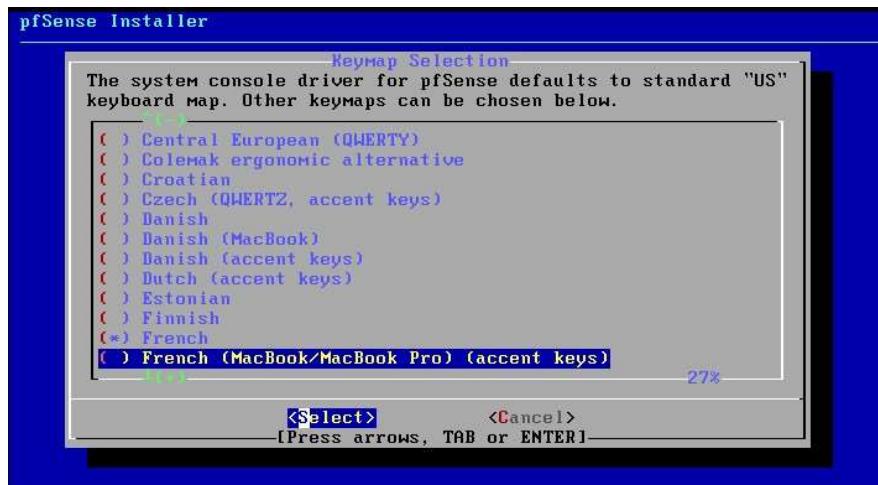
Faire ceci pour les VM Pfsense de **Strasbourg** ainsi que **Mulhouse**.



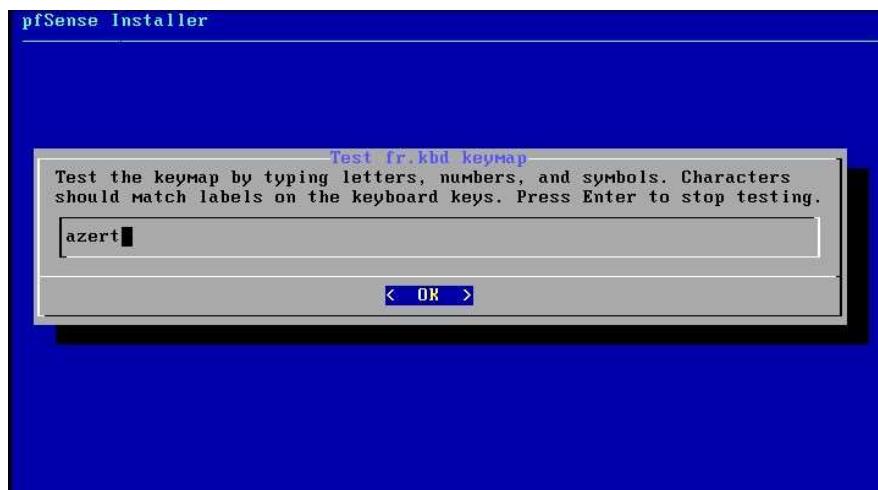
Ici, il faut simplement appuyer sur **accept** et lancer l'installation.



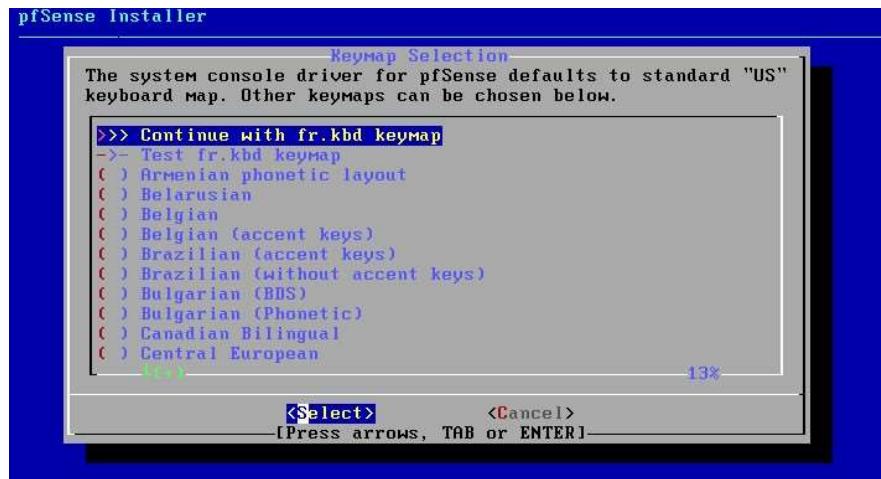
Lancer l'installation qui peut prendre quelques minutes selon votre configuration.



Concernant le clavier, nous allons rechercher le clavier French qui est le clavier français. En remontant tout en haut nous pouvons essayer si le clavier fonctionne correctement en tapant Azerty par exemple.



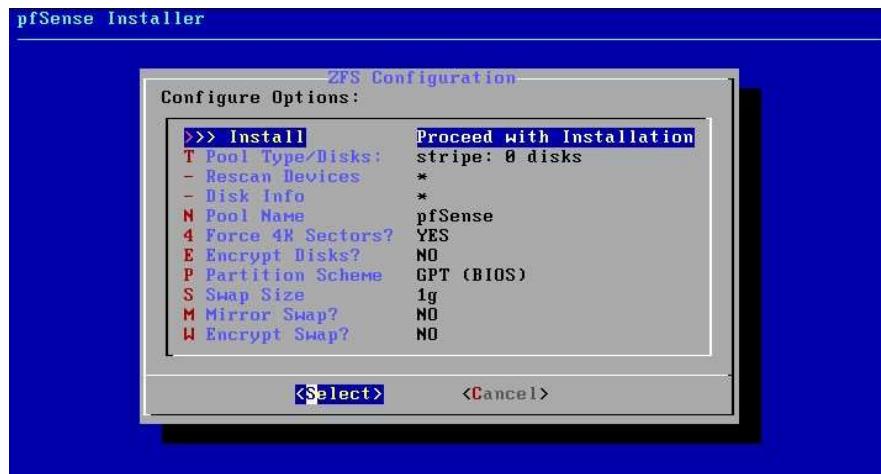
Ici nous voyons que le clavier est bien en français donc en **Azerty** et non en Qwerty.
Nous allons donc pouvoir continuer l'installation.



Une fois le clavier configuré, pfsense va nous demander si nous désirons mettre en place une **partition sur les disques**. Ce n'est pas souhaité dans le cadre de cette AP donc nous laissons **Auto (ZFS)**.



Une fois appuyé sur « **OK** », il suffit de lancer l'installation en vérifiant les informations sur la fenêtre suivante.



Dans cette partie, nous avons la possibilité de mettre en place un **RAID**.

Dans le cadre de ce projet, nous n'en avons pas la nécessité cependant c'est **vivement conseillé** d'en mettre un en place !

La mise en place d'un RAID 1 permet **d'écrire sur les deux disques** en même temps pour assurer la **haute disponibilité des services**. Ceci permet une grande tolérance en cas de disque dur en panne.



Sélectionnons donc le **seul** disque disponible afin de lancer l'installation.



Pfsense nous avertit que l'ensemble des données du disque vont être **détruite** afin de faire l'installation. Il suffit de dire Oui en ayant bien sûr **aucune donnée sur le disque en question**



Le **Shell** n'est pas obligatoire dans ce cas, cela peut permettre de rentrer des **lignes de commandes** avant de reboot le pc.



Ici nous allons redémarrer la machine car l'installation de l'OS est terminée.



6.3.2) Configuration pfsense

Strasbourg :

```
Enter an option: 1

Valid interfaces are:
em0      00:0c:29:dc:9d:75  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:dc:9d:7f (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
```

Sélectionner la **première option** dans le menu afin d'assigner les deux cartes réseaux que nous avons ajouté lors de la configuration de la machine virtuelle.

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y\!n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

Une fois que l'on lance la première option afin d'assigner les cartes réseaux, on nous demande de définir laquelle est sur le réseau WAN et de définir celle qui sera le LAN.

Em0 est notre **WAN**.

EM1 est notre **LAN**.

Afin de configurer les adresses IP, nous devons nous rendre dans la seconde option du menu.

```

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

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1)

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

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to WAN...■

```

Une fois dans celle-ci, nous avons pris la décision de mettre l'adresse WAN en DHCP avec une carte réseaux en Bridged.

```

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 2

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. 255.255.255.8 = 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:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
> ■

```

Revenons dans l'option 2 mais cette fois-ci nous configurons le LAN. Nous avons défini une adresse IP en **192.168.100.254** pour Strasbourg. Le masque de sous réseaux étant un /24 soit **255.255.255.0**. Nous n'avons pas renseigné de Gateway. Lorsque la configuration des adresses est achevée, vous devez arriver sur une fenêtre comme celle-ci avec vos adresses IP configurées à l'étape d'avant.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (UPNStrasbourg.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 3c5fe8f9cec3f502dff9

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UPNStrasbourg ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.236.121/24
LAN (lan)      -> em1      -> v4: 192.168.100.254/24

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

Enter an option: █
```

Configuration Mulhouse :

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:dc:9d:75  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:dc:9d:7f  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
```

Comme sur le site de Strasbourg, il vous faut assigner les cartes réseaux que l'on vient d'ajouter à la machine.

EM0 pour le **WAN**

EM1 pour le **LAN**

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y\!n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

Afin de configurer les adresses IP, nous devons nous rendre dans la seconde option du menu.

```
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

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1)

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

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to WAN...■
```

Une fois dans celle-ci, nous configurons l'adresse WAN sur IPv4 que l'on passe en DHCP.
L'adresse IPv6 ici n'est pas utile.

```

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.200.254

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:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
> █

```

Une fois l'adresse IPv4 du WAN configurée, nous répétons l'opération pour le LAN mais sans mettre de DHCP donc il faut configurer les adresses IP de la manière ci-dessus.

```

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 2475e3194ed2d058b713

**** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ****

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.236.14/24
LAN (lan)      -> em1      -> v4: 192.168.200.254/24

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

Enter an option:

```

Lorsque l'on a fini, nous devrions avoir un menu affichant les adresses IP comme celui-ci.

6.3.3) Configuration Pfsense via l'interface WEB

Strasbourg :

Dans un premier temps, il faudra vous rendre sur un poste client que vous mettez dans **le même sous réseaux que votre pfsense**. Pour l'exemple, mon poste client à l'adresse IP suivante : 192.168.100.3

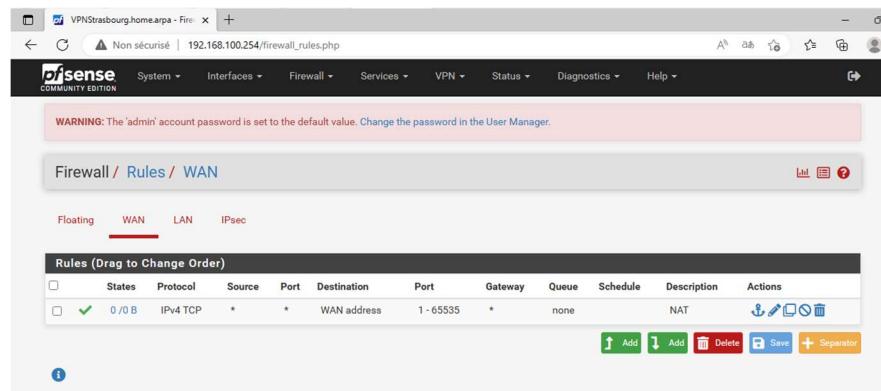
Une fois cette opération effectuée, je me rends sur Internet et je renseigne en **URL l'adresse IP LAN** de mon serveur Pfsense, ici 192.168.100.254

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red arrow points to the 'Rules' link in the Firewall dropdown menu. The main content area displays 'System Information' and 'Netgate Services And Support' sections. The 'System Information' section provides details about the firewall's hardware (Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz), software (Version: 6.00), and network configuration (DNS server(s)). The 'Netgate Services And Support' section offers support resources and a TAC support purchase option.

Une fois que vous êtes arrivé sur cette page, nous allons désormais nous occuper des règles de pare-feu.

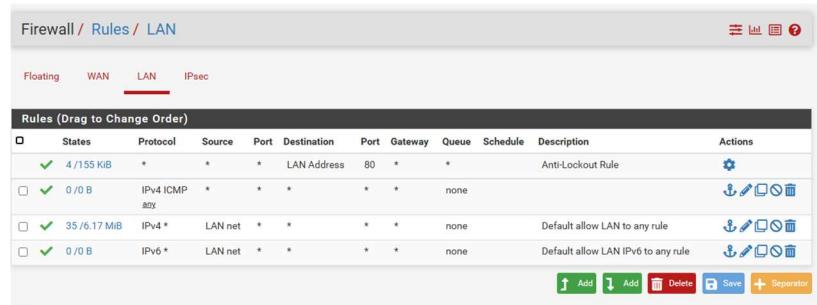
Pour ce faire, rendez-vous dans **Firewall → Rules**

The screenshot shows the pfSense web interface with the 'Firewall' tab selected and 'Rules' highlighted. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red arrow points to the 'Rules' link in the Firewall dropdown menu. The main content area displays 'System Information' and 'Netgate Services And Support' sections. The 'System Information' section provides details about the firewall's hardware (Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz), software (Version: 6.00), and network configuration (DNS server(s)). The 'Netgate Services And Support' section offers support resources and a TAC support purchase option.



Sur le screen ci-dessus, des règles sont déjà mise en place par défaut. Nous n'avons pas la nécessité de les modifier dans le cadre de ce projet.

Nous allons donc ajouter des règles de pare-feu dans l'onglet LAN. Pour créer les règles de pare-feu, rien de plus simple. Rendez-vous dans l'onglet LAN et appuyez sur le bouton vert ADD



The screenshot shows the pfSense Edit Firewall Rule configuration dialog. The Action dropdown is set to "Pass". Other settings include:

- Disabled: Disable this rule
- Interface: IPsec
- Address Family: IPv4
- Protocol: TCP

Under Source and Destination sections, both "Source" and "Destination" dropdowns show "any". Under Destination Port Range, "From" is "(other)" and "To" is "Custom".

Voici le menu de création d'une règle. Comme vu lorsque je me rends sur l'onglet LAN , actuellement des règles sont déjà en place. Prenons la règles ICMP par exemple, pour la créer il suffit de mettre une « **ACTION** » en **pass**, de changer le **protocole TCP en ICMP** et de valider car nous sommes en Source **Any** et en destination **Any**.

Afin d'ajouter une couche de sécurité, il est conseillé d'ajouter des règles de pare-feu bloquant les sources externes de votre entreprise. Actuellement lorsque vous laissez les règles en Any, n'importe qui peut ping vos machines.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP	*	*	*	*	*	none			
0/0 B	IPv4 TCP	*	*	*	*	*	none			

Veuillez après répéter l'opération pour les protocoles sur les captures d'écran ci-dessus.

Comme vous avez pu le voir, dans mes règles de pare-feu, j'ai déjà les règles de pare-feu concernant **IPSEC** ce sont les règles que nous allons devoir créer pour la mise en place du VPN intersite.

Il va falloir revenir à cette étape juste après avoir mis en place le VPN site à site.

6.3.4) Mise en place VPN IPSEC

Strasbourg

Veuillez vous rendre dans cette option pour mettre en place une connexion VPN inter-sites

General Information	
Description	INTERSITE TP A description may be entered here for administrative reference (not parsed).
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1
IKE Endpoint Configuration	
Key Exchange version	IKEv2 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	IPv4 Select the Internet Protocol family.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	192.168.236.14 Enter the public IP address or host name of the remote gateway.
Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK Must match the setting chosen on the remote side.
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	testvpn Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Bien évidemment renseignez une Pre-Shared Key plus sécurisé pour une mise en production

Pour créer la connexion VPN intersite vous devez comprendre que le **Remote Gateway** est l'adresse **WAN** du pfsense de **Mulhouse** si vous êtes sur *l'interface web de Strasbourg* et inversement

Ainsi que la Pré-Shared Key que vous devez renseigner à ***l'identique sur les deux sites.***

La méthode d'authentification est justement le partage de cette pré-shared key entre les deux sites. Vous devez vous rendre dans VPN → IPSEC → Pre-Shared Keys

Identifier	Type	Pre-Shared Key	Actions
vpn	PSK	testvpn	

Notez aussi que le protocole AES 128 bits aujourd'hui est un peu dépassé au niveau sécurité et que l'on est désormais sur du 256 bits en production.

Advanced Options	
Child SA Start Action	Default Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action	Default Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal	Auto Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
MOBIKE	Disable Set this option to control the use of MOBIKE
Gateway duplicates	<input type="checkbox"/> Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	Remote IKE Port UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500). Remote NAT-T Port UDP port for NAT-T on the remote gateway.
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	10 Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Max failures	5 Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.

Les autres paramètres sont laissés par défaut.

Une fois que vous avez ajouté sur le site de Strasbourg le VPN, vous devriez avoir une fenêtre comme celle-ci :

IPsec Tunnels								
	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description Actions
<input type="checkbox"/>	1	V2	WAN 192.168.236.14		AES (128 bits)	SHA256	14 (2048 bit)	INTERSITE TP
Show Phase 2 Entries (1)								

Ainsi une fois que vous avez cette fenêtre, appuyez sur le bouton **Show Phase 2 Entries**

	ID	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/>	1	tunnel LAN	192.168.200.254/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	SITE A SITE	

Lorsque vous allez appuyer dessus, vous n'aurez pas cette ligne donc nous allons la créer.
Pour ce faire allez sur **Add P2**

General Information

Description	SITE A SITE	A description may be entered here for administrative reference (not parsed).
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.	
Mode	Tunnel IPv4	
Phase 1	INTERSITE TP (IKE ID 1)	
P2 reqid	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	/ 24
Type	Address	
Remote network component of this IPsec security association.		

Phase 2 Proposal (SA/Key Exchange)

Protocol	ESP	Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.
Encryption Algorithms	<input checked="" type="checkbox"/> AES <input checked="" type="checkbox"/> AES128-GCM <input type="checkbox"/> AES192-GCM	128 bits 128 bits Auto

Ici, le mode de connexion est bien un mode Tunnel IPv4, la chose la plus importante est de renseigner les Networks en LAN subnet et le Remote Network avec ***l'adresse IP du LAN de Mulhouse pour le site de Strasbourg***

The screenshot shows a configuration page for an IPSEC profile. It includes sections for Hash Algorithms (with SHA256 selected), PFS key group (set to 14 (2048 bit)), and Expiration and Replacement (with Life Time set to 3600, Rekey Time to 3240, and Rand Time to 360). There are also sections for Keep Alive (Automatically ping host) and a Save button at the bottom.

Une fois toutes ces étapes terminées, sauvegardez et retournez dans **Firewall → Rules pour créer les règles IPSEC**

Nous allons désormais nous rendre sur le site de Mulhouse pour configurer l'autre côté du VPN. La configuration étant presque identique, vous allez devoir revenir sur la partie de Strasbourg pour faire celle de Mulhouse.

Mulhouse

La configuration entre les deux sites n'est pas tellement différente.

Dans un premier temps, connectez-vous à l'interface WEB via un poste client dans le même sous-réseau que votre pare-feu de Mulhouse.

Une fois que le client est dans le même sous-réseau, rendez-vous sur Internet et rentrez l'URL 192.168.200.254

The screenshot shows the pfSense home.arpa - Status / Dashboard interface. It displays system information such as Name (pfSense home.arpa), User (admin@192.168.200.30), System (VMware Virtual Machine, Netgate Device ID: 2475e3194ed2d058b713), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020), Version (2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE), CPU Type (Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No), and Hardware crypto (Kernel PTI: Disabled, MDS Mitigation: Inactive). The uptime is listed as 01 Hour 12 Minutes 48 Seconds. On the right, there's a section titled "Netgate Services And Support" with a "Contract type" set to "Community Support". Below it, a "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" section provides links to various support resources.

Nous allons devoir faire les mêmes règles de pare-feu que sur le site de Strasbourg, je vous invite donc à regarder la partie de Strasbourg et de faire exactement la même chose.

Vous allez avoir besoin de créer uniquement les règles LAN et IPSEC.

Mise en place VPN Mulhouse :

The screenshot shows the configuration of a VPN connection. In the "IKE Endpoint Configuration" section, the "Key Exchange version" is set to IKEv2, "Internet Protocol" to IPv4, and the "Interface" is set to WAN. The "Remote Gateway" is specified as 192.168.236.121. In the "Phase 1 Proposal (Authentication)" section, the "Authentication Method" is set to Mutual PSK, "My identifier" is My IP address, "Peer identifier" is Peer IP address, and the "Pre-Shared Key" is testvpn. A note states that the key should be long and random to protect the tunnel and its contents.

Ici, la seule modification par rapport à Strasbourg est la Remote Gateway où nous devons mettre celle de Strasbourg. Dans mon cas 192.168.236.121, le reste de la configuration est par défaut et identique à celle de Strasbourg.

Vous devez renseigner la Pré-Shared key dans cet onglet :

VPN / IPsec / Pre-Shared Keys

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

Pre-Shared Keys			
Identifier	Type	Pre-Shared Key	Actions
vpn	PSK	testvpn	

Add

Une fois que la Phase 1 est configurée, passons à la phase 2 :

General Information	
Description	SITE A SITE A description may be entered here for administrative reference (not parsed).
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	Tunnel IPv4
Phase 1	AP3 VPN (IKE ID 2)
P2 reqid	2
Networks	
Local Network	LAN subnet <input type="text"/> / 0
Type	Address
NAT/BINAT translation	None <input type="text"/> / 0
Type	Address
Remote Network	Network <input type="text"/> 192.168.100.254 <input type="text"/> / 24
Type	Address
Remote network component of this IPsec security association.	
Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.
Encryption Algorithms	<input checked="" type="checkbox"/> AES 128 bits <input checked="" type="checkbox"/> AES128-GCM 128 bits <input type="checkbox"/> AES192-GCM Auto

Vous devez ajouter ici la Remote Gateway de réseau LAN de Strasbourg.

Dans notre cas le LAN de Strasbourg à l'adresse IP suivante : 192.168.100.254

Une fois que cette configuration est terminée, nous allons pouvoir nous rendre dans l'onglet Status → IPsec

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	INTERSITE TP	ID: 192.168.236.121 Host: 192.168.236.121	ID: 192.168.236.14 Host: 192.168.236.14				Disconnected

Cliquez sur **Connect P1 and P2s**

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	INTERSITE TP	ID: 192.168.236.121 Host: 192.168.236.121:500 SPI: e223eff940d85aa0	ID: 192.168.236.14 Host: 192.168.236.14:500 SPI: 72f3b02e5257e7ea	IKEV2 Initiator	Rekey: 25617s (07:06:57) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 37 seconds (00:00:37) ago

Une fois que la connexion est établie, nous allons pouvoir procéder à un test de PING entre les deux pare-feux.

```
C:\Users\Administrateur>ping SRV-MUL01

Envoi d'une requête 'ping' sur SRV-MUL01.CCI-CAMPUS.LAN [192.168.200.10] avec 32 octets de données :
Réponse de 192.168.200.10 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.200.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

```
C:\Users\Administrateur.CCI-CAMPUS>ping SRV-STG01

Envoi d'une requête 'ping' sur SRV-STG01.CCI-CAMPUS.LAN [192.168.100.10] avec 32 octets de données :
Réponse de 192.168.100.10 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.10 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.100.10 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.10 : octets=32 temps=1 ms TTL=126

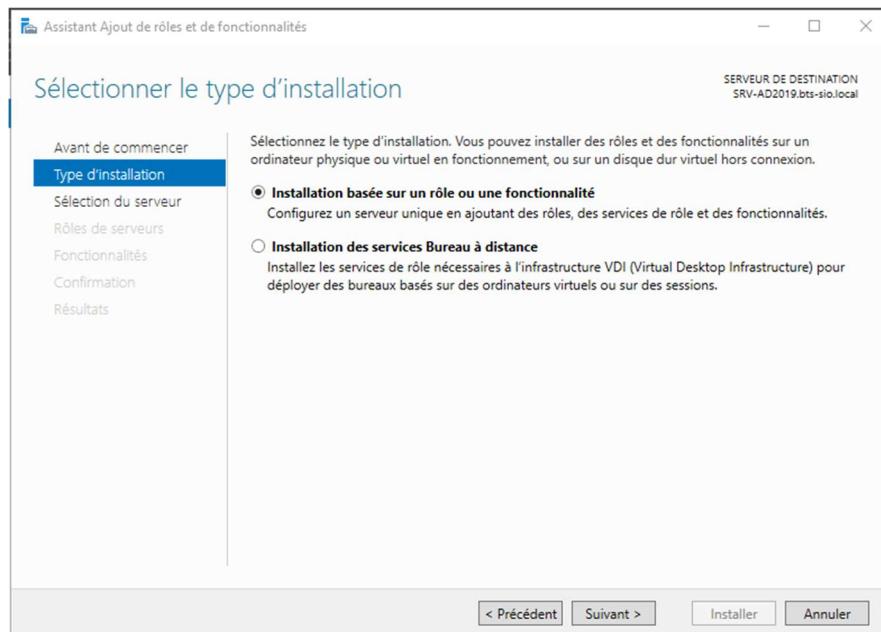
Statistiques Ping pour 192.168.100.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

6.3.5) Installation de radius sur les serveurs Windows

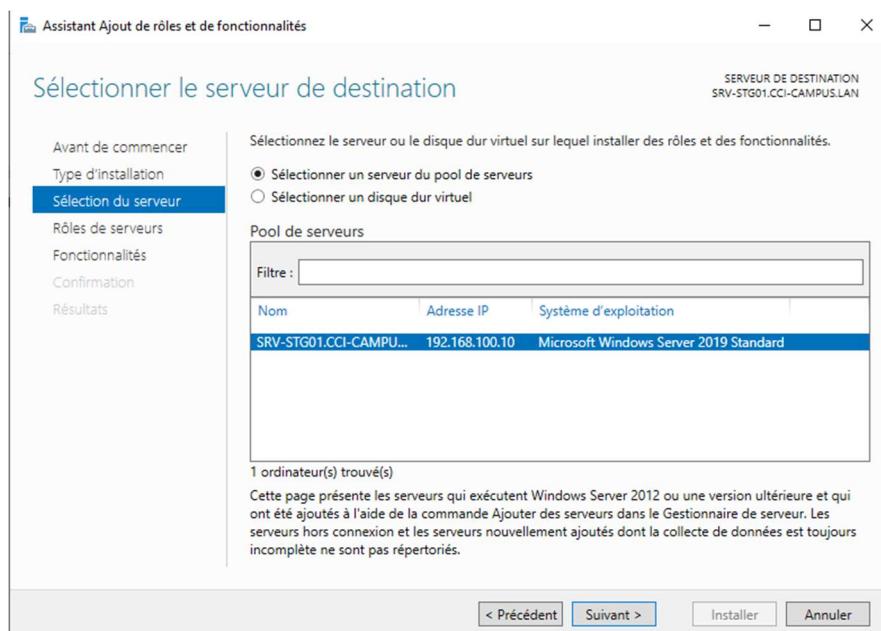
Radius Strasbourg

Une fois que le serveur Windows comprenant l'AD, DNS, DHCP est lancé, ajoutons un nouveau rôle

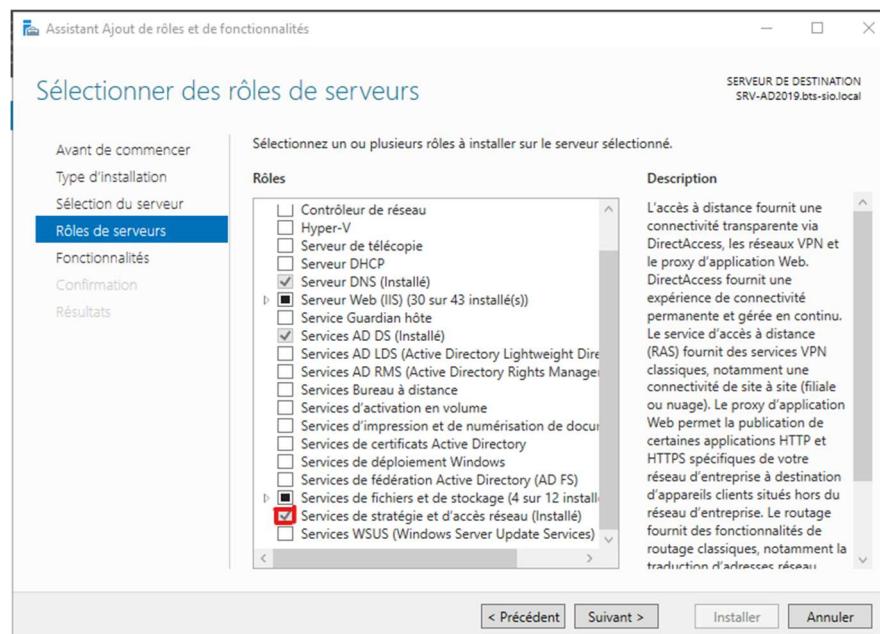




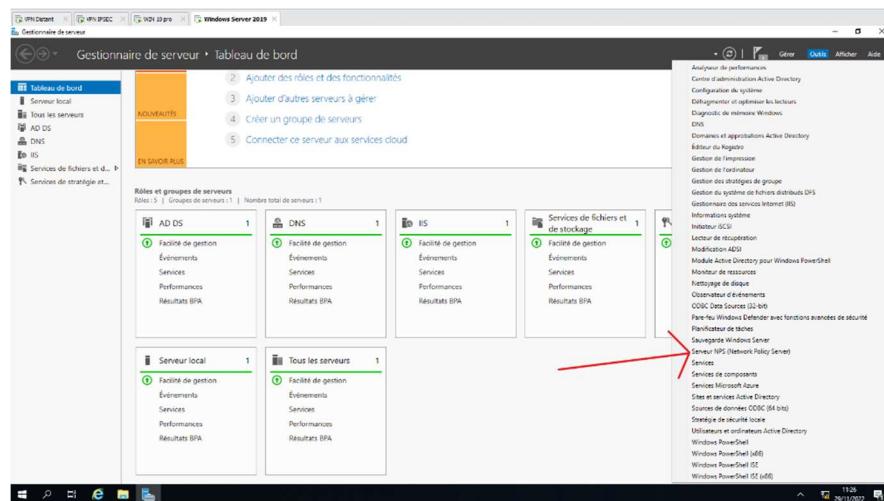
Appuyez sur Suivant.



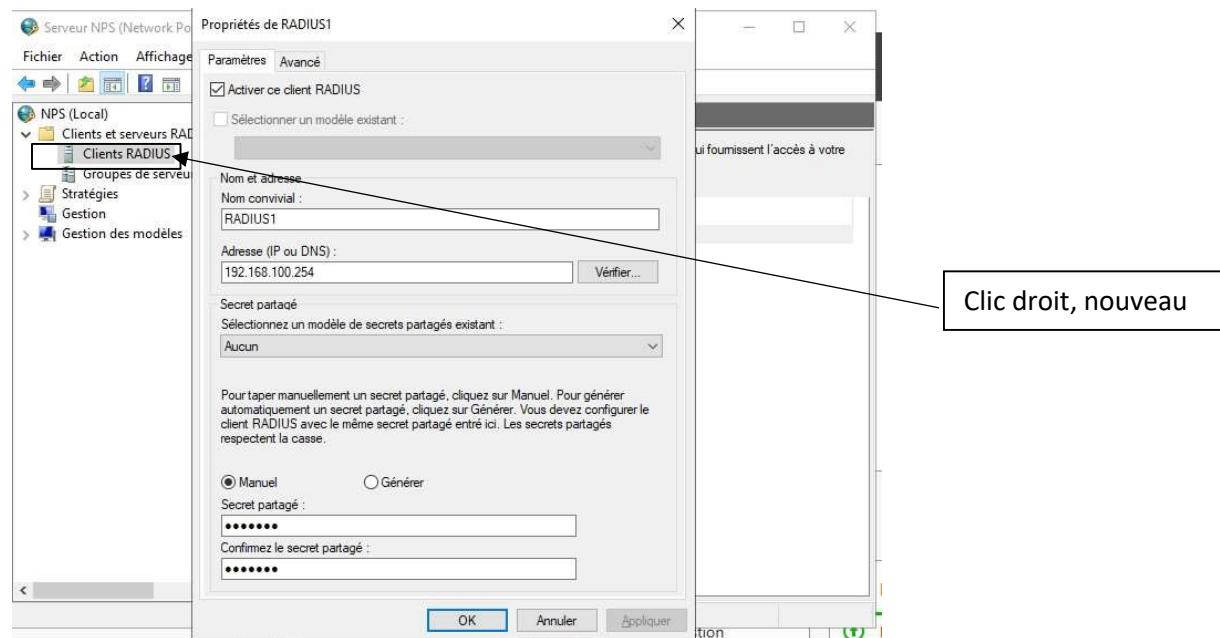
Sélectionnez le serveur en question ici le serveur SRV-STG01.



Cherchez et cochez le Services de stratégie d'accès réseau et faire suivant jusqu'à l'installation



Une fois que le rôle est installé, nous nous rendons dans outils, Serveur NPS.



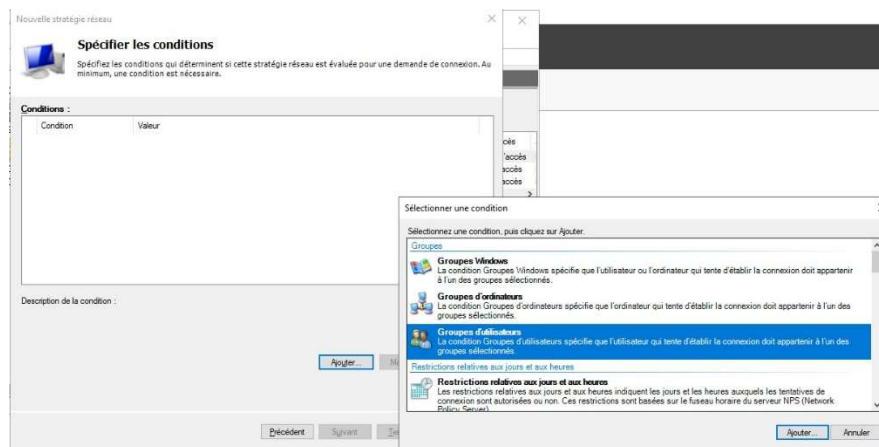
Faire un clic droit sur Clients Radius afin d'ajouter un nouveau client.

Ici nous devons renseigner le nom du client, **ici le client est le Pare-feu de Strasbourg car nous sommes sur le serveur Windows de Strasbourg**

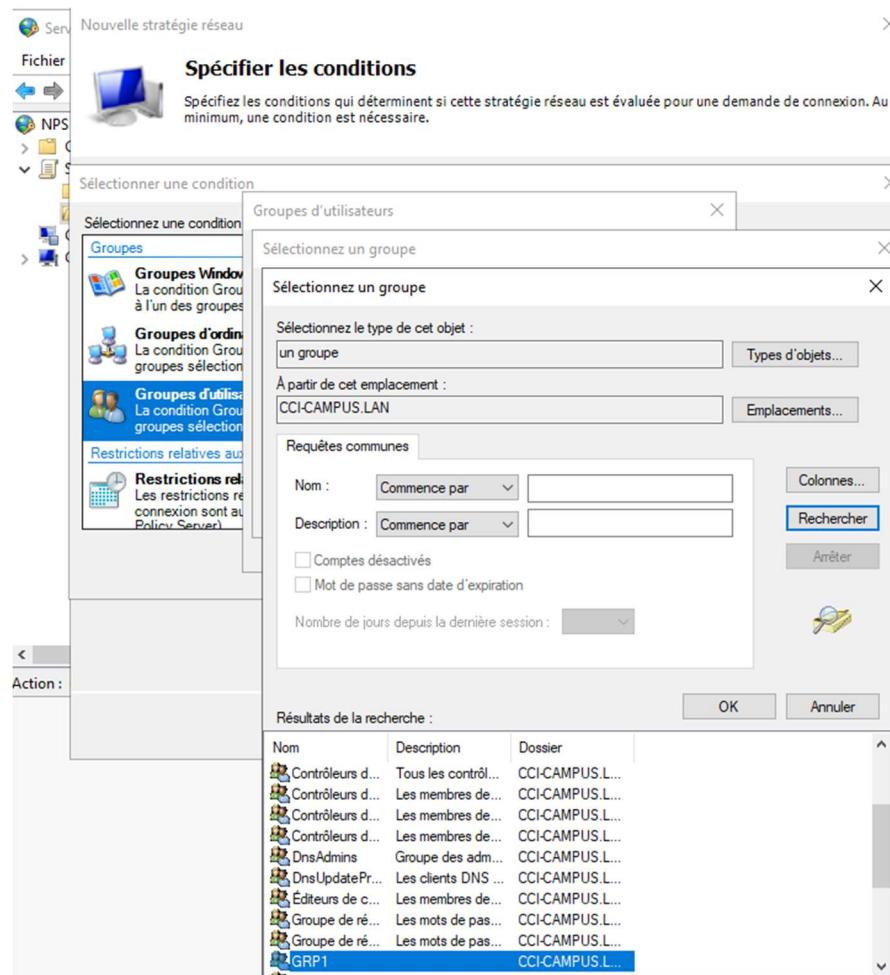
Son adresse IP LAN

Ainsi que créer un secret partagé. Par mesure de sécurité celui-ci doit être plus long que celui que nous avons renseigné lors de ce projet.

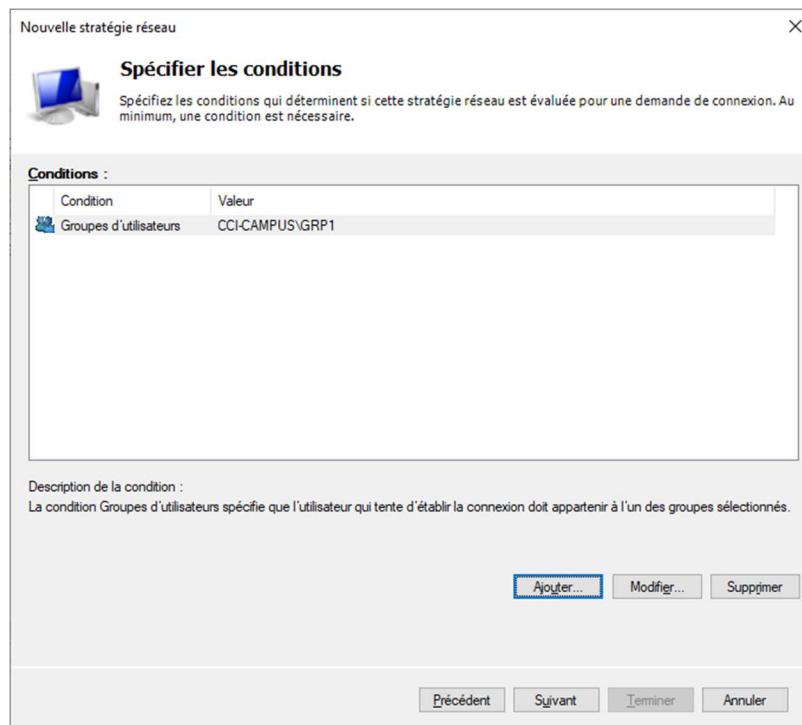
Une fois que le client est créé, nous devons aller dans Stratégie → Stratégie réseau et ajouter une règle comme ci-dessous.



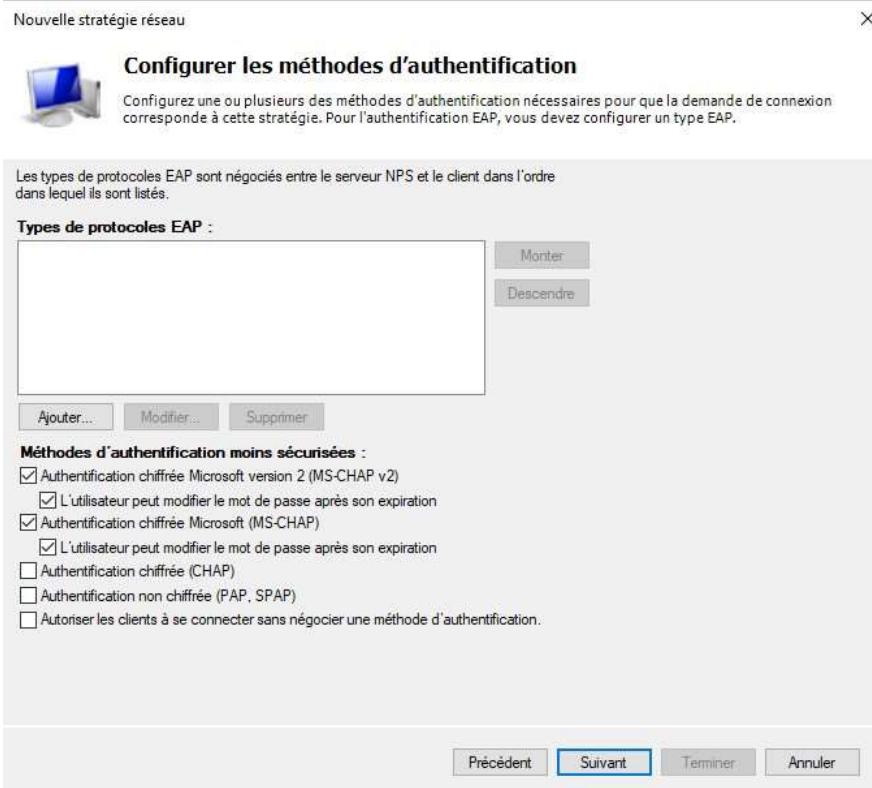
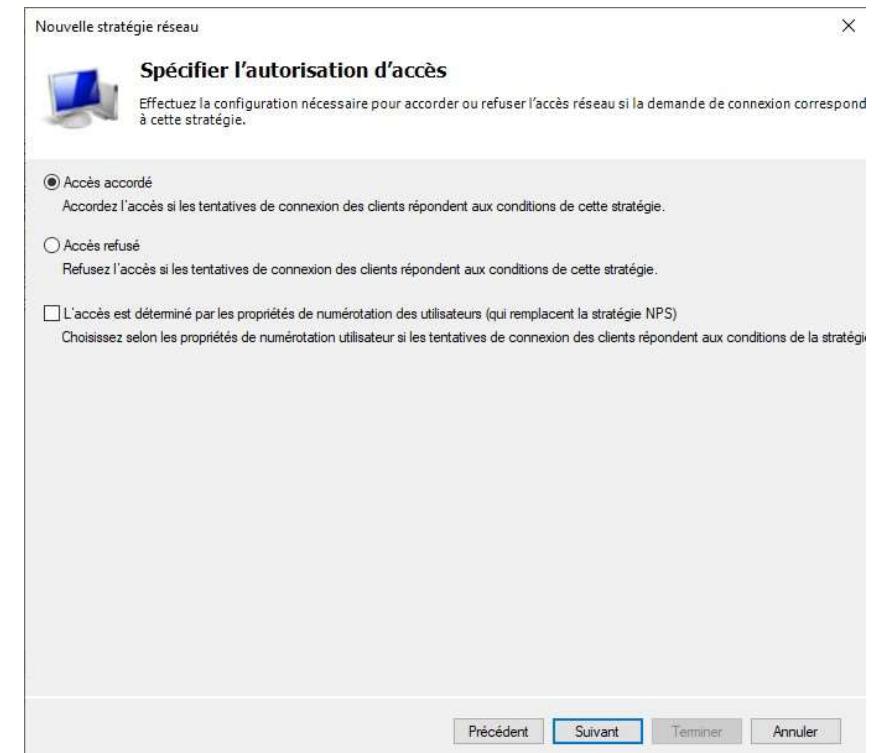
Ici nous choisissons d'ajouter une condition sur un Groupes d'utilisateurs à qui l'on va accorder l'accès au portail captif.



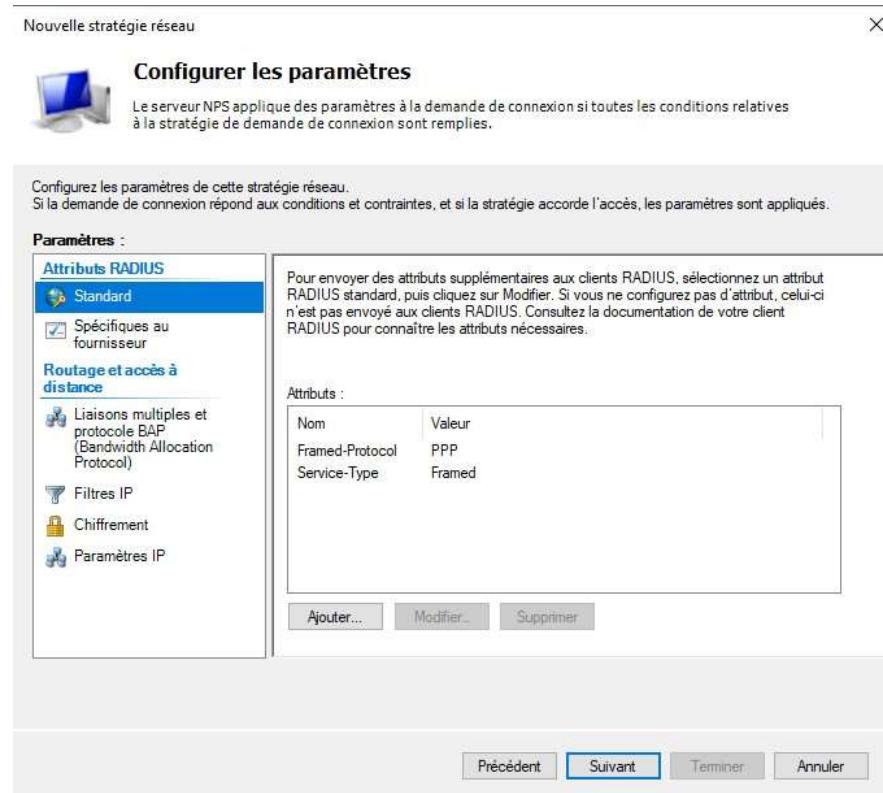
Le GRP1 contient tous les utilisateurs pouvant se connecter au portail captif de Strasbourg.



Une fois le groupe ajouté, faites suivant et cochez la case Accès accordé.



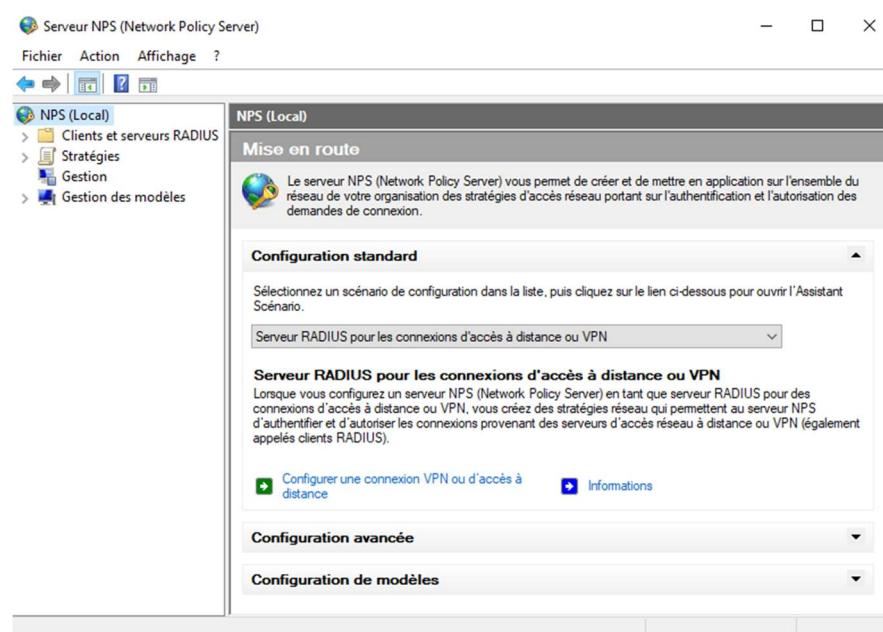
Ici nous laissons les paramètres par défaut, il suffit de faire suivant.

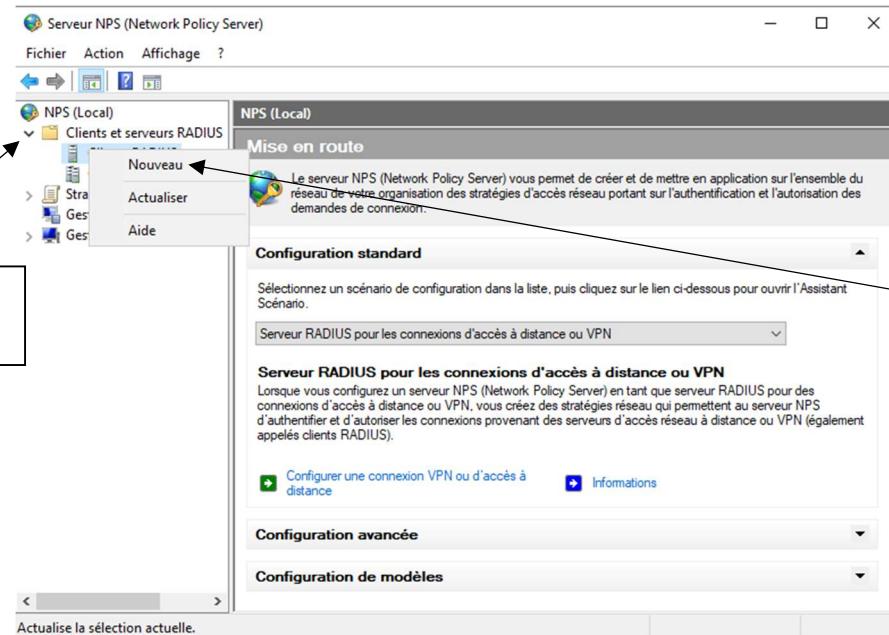


Ici aussi il faut faire suivant.

Radius Mulhouse

Faire l'installation du rôle comme sur le site de Strasbourg.
Une fois le rôle installé se rendre dans Outils → Serveur NPS
Vous devez arriver sur une page comme celle-ci





Propriétés de Mulhouse X

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

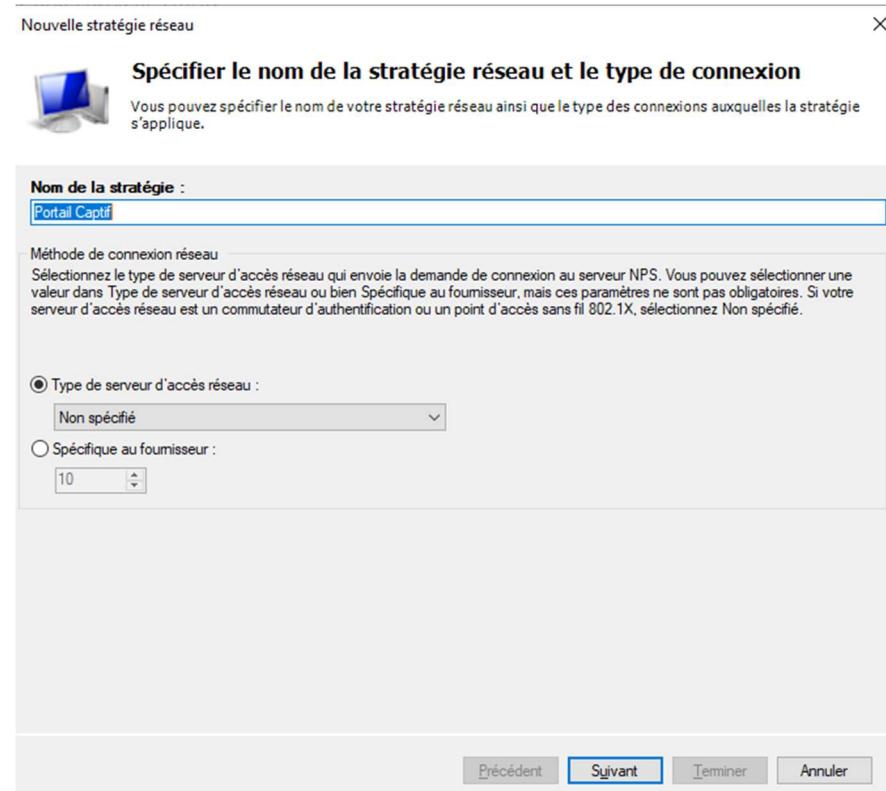
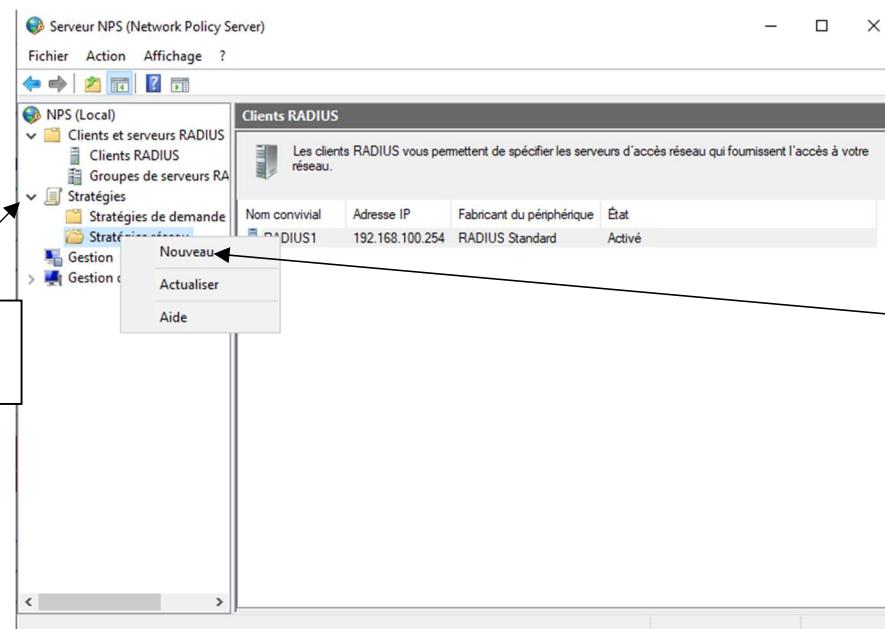
Manuel Générer

Secret partagé :

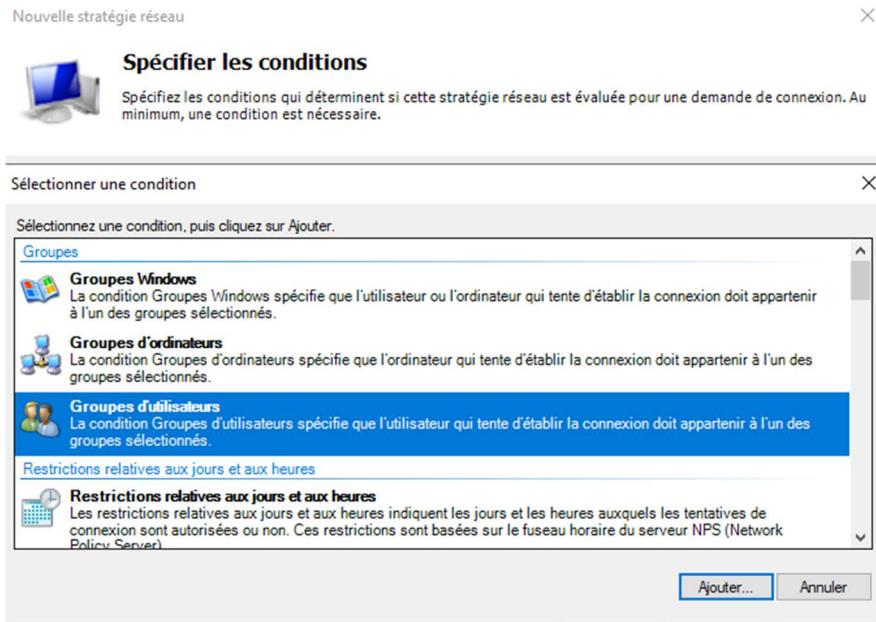
Confirmez le secret partagé :

Renseignez l'adresse IP du LAN de Mulhouse ici 192.168.200.254 ainsi que le Secret partagé.

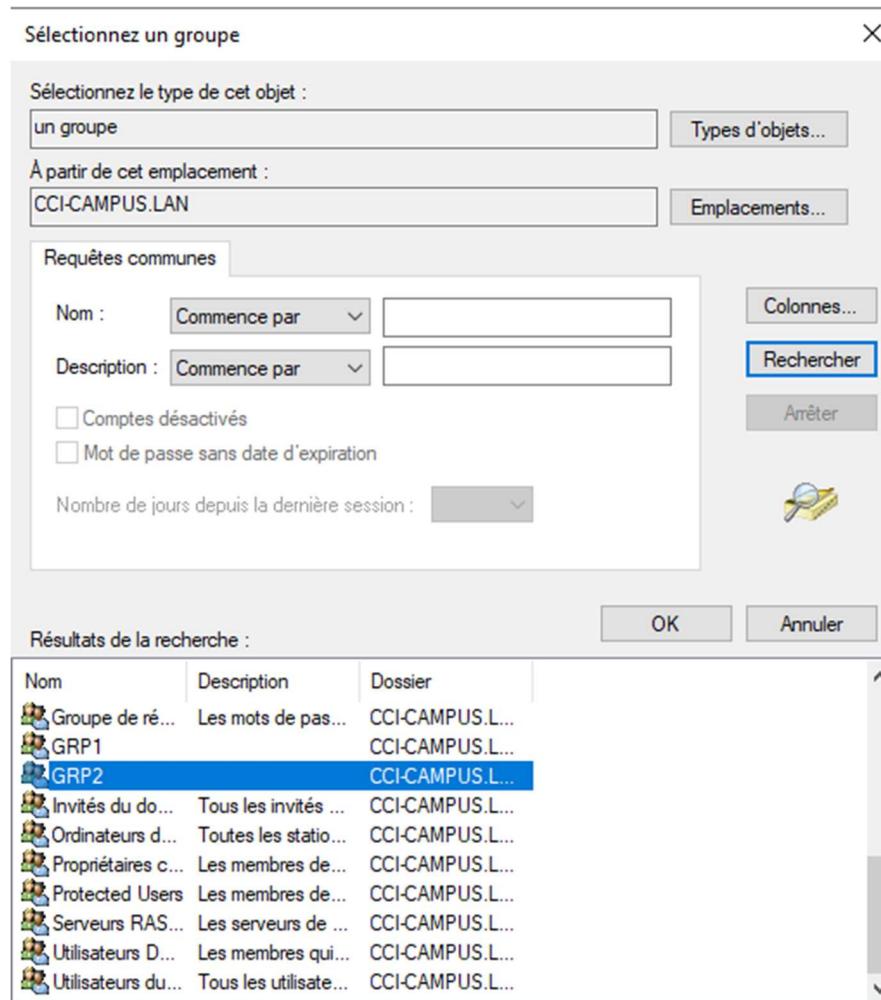
Une fois que le client est ajouté, occupons-nous de la stratégie réseau.

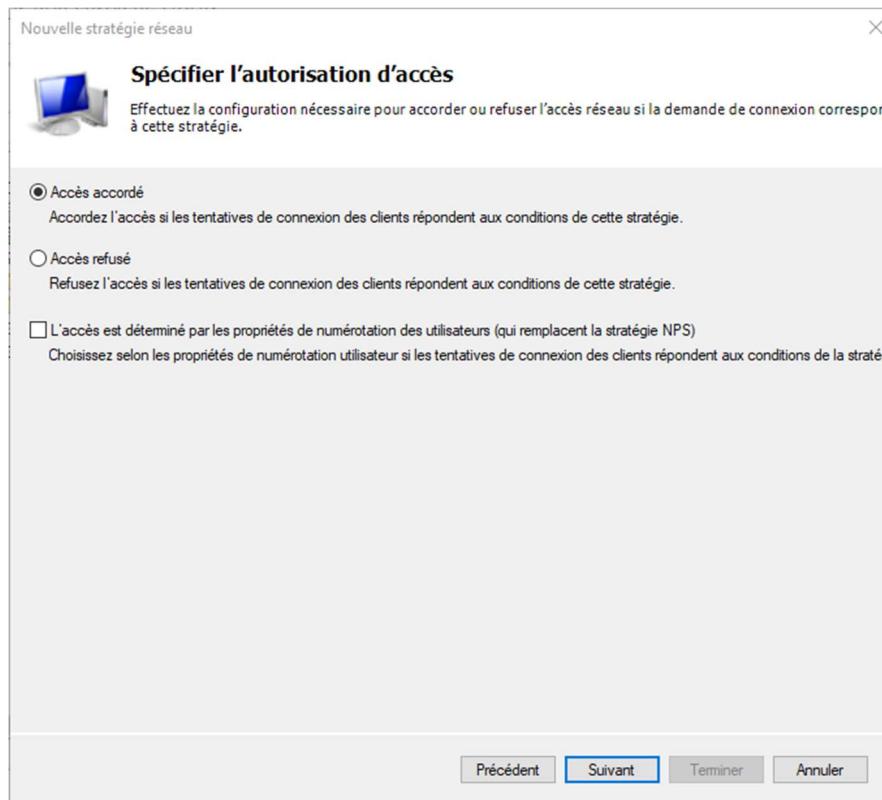


Ici renseignez le nom de la stratégie réseau



Ajoutons comme à Strasbourg un groupe d'utilisateurs avec la permission d'accéder au portail Captif PfSense.





On autorise l'accès uniquement aux groupe GRP2.

Pour le reste de la configuration, il suffit de faire suivant car nous la laissons par défaut.

6.3.6) Configuration portail captif Strasbourg

Retournons sur la page WEB du serveur de Strasbourg. Ensuite, nous allons dans Système et User Manager

Dans un premier temps, nous allons mettre en place dans **User Manager** un serveur

d'authentification.

Pour ce faire vous allez devoir ajouter un nouveau serveur d'authentification avec les données ci-dessus. L'adresse IP 192.168.100.10 est l'adresse IP du serveur Radius de Strasbourg.
Ensuite, nous nous rendons dans Services → Portail Captif et on clique sur **Add**

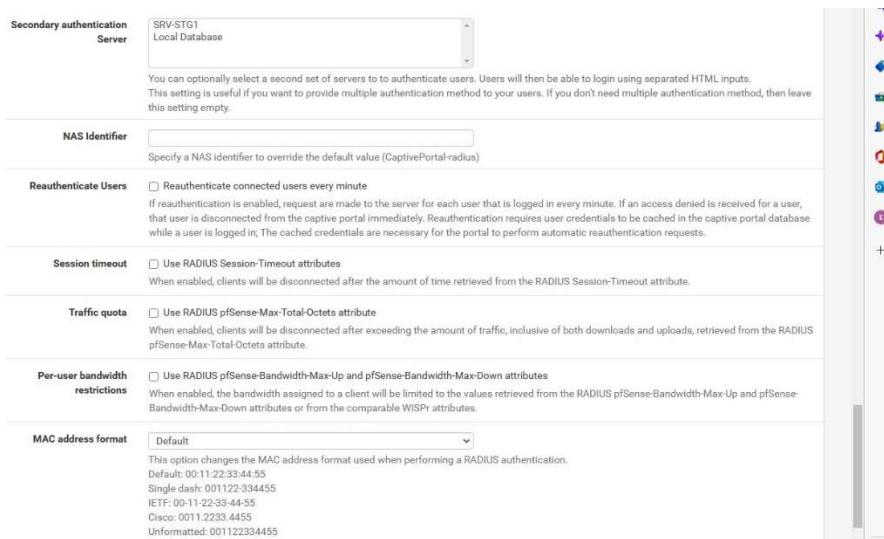
Ici nous sélectionnons l'interface LAN, un peu plus bas nous renseignons le serveur d'authentification précédemment renseigné soit SRV-STG1

The screenshot shows the 'captiveportal.php?zone=radius' configuration page. It includes sections for 'Reset waiting period', 'Logout popup window', 'Pre-authentication redirect URL' (set to https://www.google.fr), 'After authentication Redirection URL', 'Blocked MAC address redirect URL', 'Preserve users database', 'Concurrent user logins' (disabled), 'MAC filtering' (disabled), and 'Pass-through MAC Auto Entry' (disabled). A sidebar on the right contains icons for search, add, and other system functions.

Ici, nous avons choisi l'URL <https://www.google.fr> afin d'en faire la redirection vers notre page de portail captif. Nous avons aussi paramétré le navigateur de recherche pour qu'il accède à cette URL dès que l'on l'ouvre.

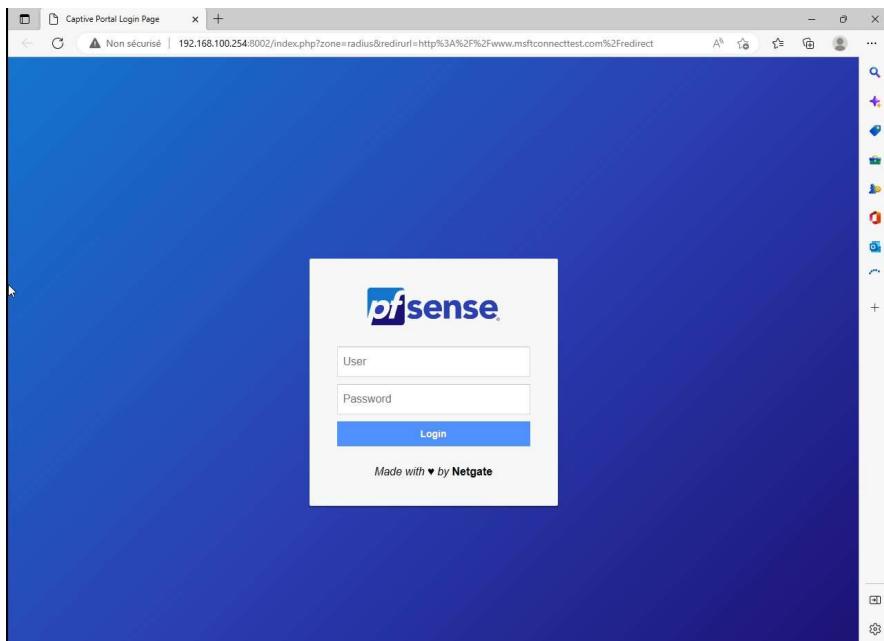
The screenshot shows the 'Captive Portal Login Page' configuration page. It includes sections for 'Display custom logo image' (unchecked), 'Logo Image' (with a 'Choisir un fichier' button and note about file type and storage), 'Display custom background image' (unchecked), 'Background Image' (with a 'Choisir un fichier' button and note about file type and storage), 'Terms and Conditions' (a text area with a note about stripping HTML tags), 'Authentication' (under 'Authentication Method' dropdown set to 'Use an Authentication backend'), and 'Authentication Server' (dropdown set to 'SRV-STG1 Local Database'). A sidebar on the right contains icons for search, add, and other system functions.

Ici nous mettons le serveur SRV-STG1 en tant que Authentication Server afin que ce soit lui qui accède au serveur Radius pour Valider ou non la connexion.



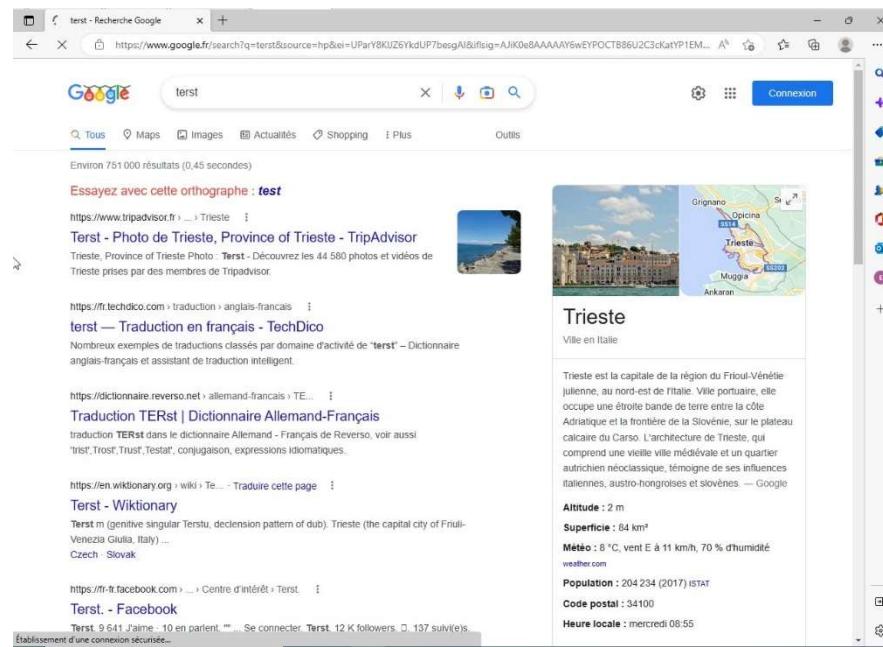
Ici nous n'avons pas renseigné de serveur d'authentification secondaire car nous avons rencontré pas mal de soucis avec nos machines CORE pour l'installation de Radius sur celle-ci.

Dans le cas où vous arrivez à installer RADIUS sur une machine CORE, vous devez alors mettre le second serveur en tant que Serveur d'authentification, le rajouter dans le rôle NPS afin d'assurer la Haute disponibilité du portail captif.



Ici, nous nous connectons avec l'utilisateur du GPO1 que l'on a ajouté précédemment dans le rôle NPS avec la stratégie réseau.

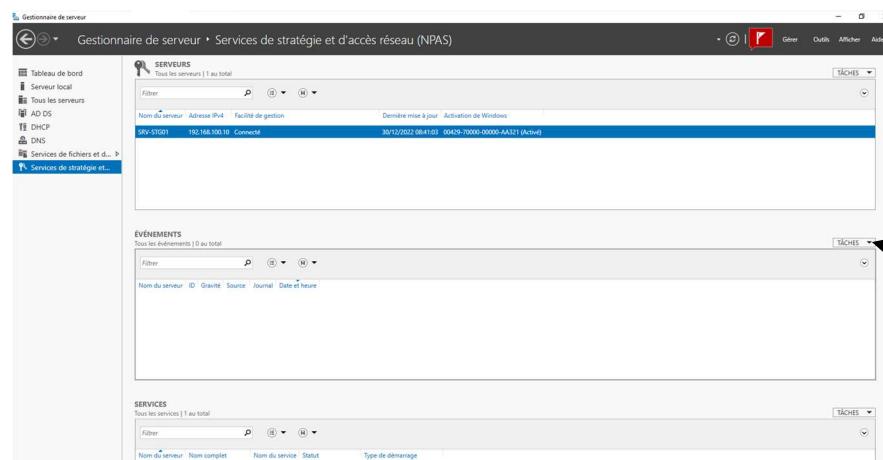
L'utilisateur en question est Paulo



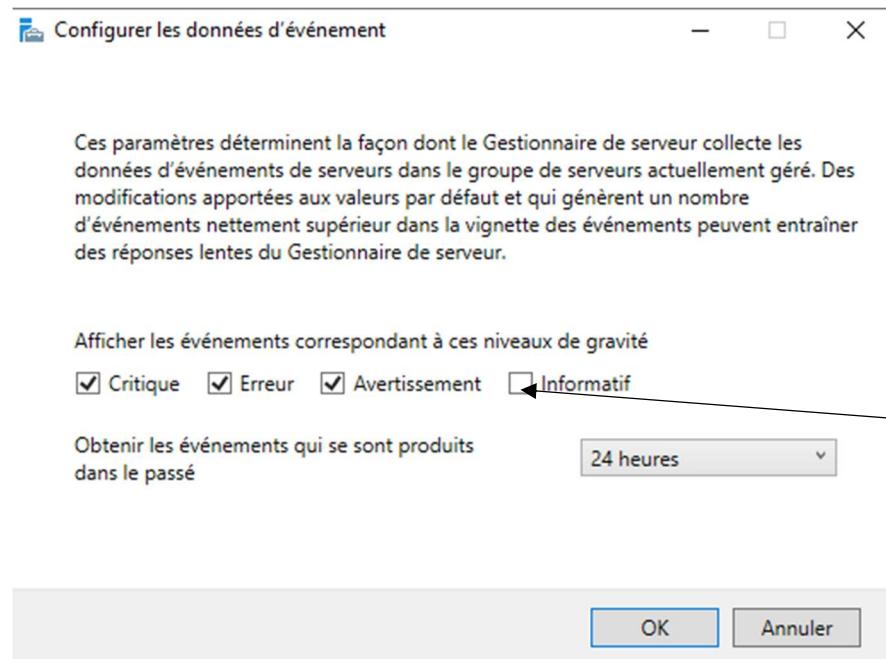
Comme vous pouvez le voir, une fois l'authentification réussie, nous avons accès à Google, nous pouvons effectuer des recherches et accéder aux pages.

Maintenant que nous arrivons à nous connecter, rendons-nous sur le serveur de Mulhouse afin de regarder les Logs.

Pour ce faire, il faut aller dans :



Tâches, configurer les données d'événements



Le serveur NPS a accordé l'accès à un utilisateur.

Utilisateur :

ID de sécurité :	S-1-5-21-3572067251-3681994127-1800068665-14106
Nom de compte :	Paulo
Domaine de compte :	CCI-CAMPUS
Nom de compte complet :	CCI-CAMPUS.LAN/Users/Paulo

Ordinateur client :

ID de sécurité :	S-1-0-0
Nom de compte :	-
Nom de compte complet :	-
Identificateur de la station appelée :	00:0c:29:47:bb:4c\VPNStrasbourg.home.arpa
Identificateur de la station appellante :	-

Serveur NAS :

Adresse IPv4 du serveur NAS :	192.168.100.254
Adresse IPv6 du serveur NAS :	-
Identificateur du serveur NAS :	CaptivePortal-radius
Type de port du serveur NAS :	Ethernet
Port du serveur NAS :	2000

Client RADIUS :

Nom convivial du client :	RADIUS1
Adresse IP du client :	192.168.100.254

Informations détaillées sur l'authentification :

Nom de stratégie de demande de connexion :	Utiliser l'authentification Windows pour tous les utilisateurs
Nom de stratégie réseau :	accès_web
Fournisseur d'authentification :	Windows
Serveur d'authentification :	SRV-STG01.CCI-CAMPUS.LAN
Type d'authentification :	MS-CHAPv2
Type EAP :	-
Identificateur de la session du compte :	-
Résultats de la journalisation :	Les informations de suivi ont été inscrites dans le fichier journal local.

Voici les logs de la connexion de Paulo avec le protocole RADIUS.

6.3.7) Mise en place portail captif Mulhouse

The screenshot shows the pfSense web interface. At the top, there's a navigation bar with tabs: System, Interfaces, Firewall, Services, and others. A red box highlights the "System" tab. Below the navigation, there's a "WARNING: The configuration file" message. The main content area has a "Status / D" button. On the left, there's a sidebar with "System Info" and several sections: Name (Radius Mulhouse), User (Radius), System (Setup Wizard), BIOS (User Manager). The "User Manager" section is also highlighted with a red box. At the bottom, it says "Release Date: Thu Nov 12 2020" and "Version 2.6.0-RELEASE (amd64)".

Dans un premier temps, nous allons mettre en place dans **User Manager** un serveur d'authentification.

The screenshot shows the "User Manager" configuration page. It has two main sections: "Server Settings" and "RADIUS Server Settings". In "Server Settings", the "Descriptive name" is "Radius Mulhouse" and the "Type" is "RADIUS". In "RADIUS Server Settings", the "Protocol" is "MS-CHAPv2", "Hostname or IP address" is "192.168.200.254", "Shared Secret" is ".....", "Services offered" is "Authentication and Accounting", "Authentication port" is "1812", "Accounting port" is "1813", and "Authentication Timeout" is "5". A note below says: "This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token." At the bottom, there's a "Save" button.

Pour ce faire vous allez devoir ajouter un nouveau serveur d'authentification avec les données ci-dessus. L'adresse IP 192.168.200.10 est l'adresse IP du serveur Radius de Strasbourg.
Ensuite, nous nous rendons dans Services → Portail Captif et on clique sur **Add**

Captive Portal Configuration

Enable **Enable Captive Portal**

Description portail captif accès WAN
A description may be entered here for administrative reference (not parsed).

Interfaces WAN LAN
Select the interface(s) to enable for captive portal.

Maximum concurrent connections 1
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes) 30
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout (Minutes)
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Traffic quota (Megabytes)
Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

Pass-through credits per MAC address:
Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Waiting period to restore pass-through credits. (Hours)
Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period Enable waiting period reset on attempted access

Ici nous sélectionnons l'interface LAN, un peu plus bas nous renseignons le serveur d'authentification précédemment renseigné soit SRV-MUL1

above 0 hours if pass-through credits are enabled.

Reset waiting period Enable waiting period reset on attempted access
If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication redirect URL https://www.google.fr
Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \${PORTAL_REDIRECTURL} variable in captiveportal's HTML pages.

After authentication Redirection URL
Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address redirect URL
Blocked MAC addresses will be redirected to this URL when attempting access.

Preserve users database Preserve connected users across reboot
If enabled, connected users won't be disconnected during a pfSense reboot.

Concurrent user logins Disabled
Disabled: Do not allow concurrent logins per username or voucher.
Multiple: No restrictions to the number of logins per username or voucher will be applied.
Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected.
First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.

MAC filtering Disable MAC filtering
If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Pass-through MAC Auto Entry Enable Pass-through MAC automatic addition
When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.

Authentication

Authentication Method	<input checked="" type="checkbox"/> Use an Authentication backend Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the 'submit' button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server	<input type="text"/> Radius Mulhouse Local Database
You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.	
Secondary authentication Server	<input type="text"/> Radius Mulhouse Local Database
You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.	
NAS Identifier	<input type="text"/>
Specify a NAS identifier to override the default value (CaptivePortal-portail_captif)	
Reauthenticate Users	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in. The cached credentials are necessary for the portal to perform automatic reauthentication requests.
Session timeout	<input checked="" type="checkbox"/> Use RADIUS Session-Timeout attributes When enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute.
Traffic quota	<input checked="" type="checkbox"/> Use RADIUS pfSense-Max-Total-Octets attribute When enabled, clients will be disconnected after exceeding the amount of traffic, inclusive of both downloads and uploads, retrieved from the RADIUS pfSense-Max-Total-Octets attribute.

Comme sur Strasbourg, nous n'avons pas renseigné de serveur d'authentification secondaire car nous avons rencontré pas mal de soucis avec nos machines CORE pour l'installation de Radius sur celle-ci.

Dans le cas où vous arrivez à installer RADIUS sur une machine CORE, vous devez alors mettre le second serveur en tant que Serveur d'authentification, le rajouter dans le rôle NPS afin d'assurer la Haute disponibilité du portail captif.

Accounting

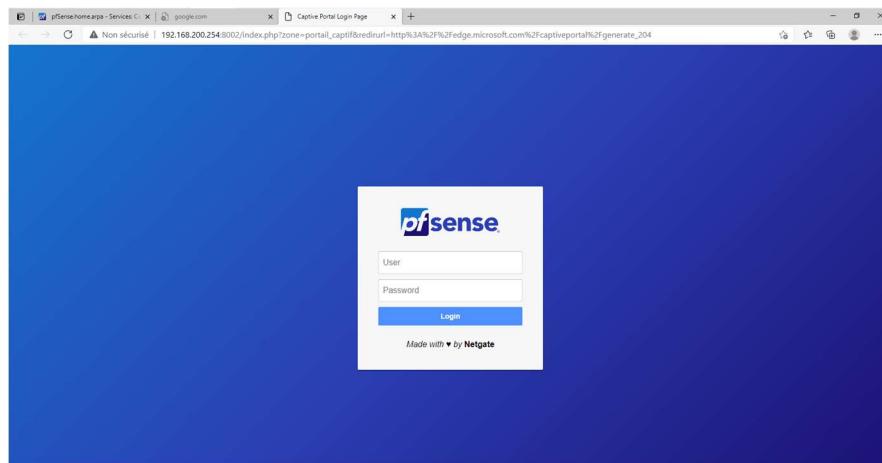
RADIUS	<input checked="" type="checkbox"/> Send RADIUS accounting packets. If enabled, accounting request will be made for users identified against any RADIUS server.
Accounting Server	<input type="text"/> Radius Mulhouse
You can add a Radius Accounting server in the User Manager.	
Send accounting updates	<input checked="" type="radio"/> No updates <input type="radio"/> Stop/Start <input type="radio"/> Stop/Start (FreeRADIUS) <input type="radio"/> Interim
This field set the way Accounting Updates should be done : - If "No updates" is selected, then only one "Accounting Start" and one "Accounting Stop" request will be sent, when any user get connected and disconnected. - If "Interim" is selected, then "Accounting Update" requests will be send regularly (every minute) to the RADIUS server, for each connected user. - In some rare cases, you would like to simulate users to disconnect and reconnect every minute (eg, to send an Accounting Stop then an Accounting Start) instead of sending Accounting updates, this is the purpose of "Stop/Start" option. FreeRADIUS does not support this option very well, you should select "Stop/Start (FreeRADIUS)" instead.	
Accounting style	<input type="checkbox"/> Invert Acct-Input-Octets and Acct-Output-Octets When enabled, data counts for RADIUS accounting packets will be taken from the client perspective, not the NAS. Acct-Input-Octets will represent download, and Acct-Output-Octets will represent upload.
Idle time accounting	<input type="checkbox"/> Include idle time when users get disconnected due to idle timeout This setting change the stop time that will be send in the Accounting Stop request, when a user get disconnected after exceeding the idle timeout. If not checked, the sent stop time will be the last activity time.

HTTPS Options

Login	<input type="checkbox"/> Enable HTTPS login When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.
--------------	---

Une fois que tout cela est fait il reste plus que la partie TEST.

Comme nous avons renseigné la redirection du portail sur l'adresse <https://google.fr>, il ne nous reste plus qu'à accéder à celui-ci et la page du portail captif devrait arriver.



Connectons-nous avec un utilisateur du groupe 2 dans notre cas, Paul
Une fois que nous sommes connectés, nous pouvons désormais naviguer sur Internet avec un recherche « Test » dans notre cas qui fonctionne.

Microsoft Bing

test

TOUT ÉCOLE IMAGES VIDÉOS CARTES ACTUALITÉS SHOPPING À PROPOS DES RÉSULTATS DE RECHERCHE

Environ 2 460 000 000 résultats Date ▾

test – Wiktionnaire
<https://fr.wiktionary.org/wiki/test>
Web test (test) masculin. Coquille externe dure, calcaire ou chitineuse, de certains invertébrés.
Test corné, osseux. Ces parties dures : lorsqu'elles sont recouvertes par les muscles, ...

EXPLORER DAVANTAGE

Test : tous les tests de personnalité et quiz gratuits - aufeminin
aufeminin.com

Test de début : quelle est la vitesse de votre connexion
degroupitest.com

Définitions : test - Dictionnaire de français Larousse
larousse.fr

Test – Wikipedia
fr.wikipedia.org

Tests gratuits, Test en ligne - Psychologies.com
test.psychologies.com

Recommandé pour vous en fonction de ce qui est populaire - Avis

Test – Wikipedia
<https://fr.wikipedia.org/wiki/Test>

< Vue d'ensemble Du latin Testis (témoin) Du latin Testa (récipient rond) >

+ test, sur le Wiktionnaire
Le mot test est polyémique en français et issu de deux étymologies latines distinctes : testis (témoin) et testa (récipient rond).

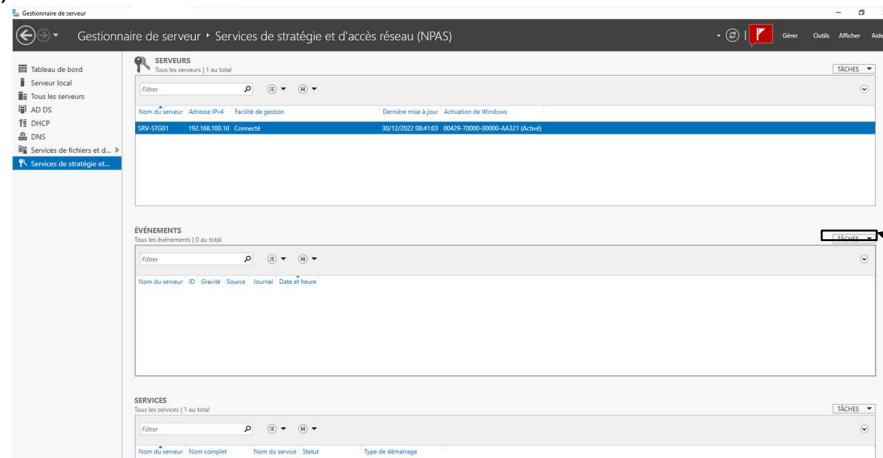
Wikipedia Texte sous licence CC-BY-SA

Temps de Lecture Estimé: 2 min

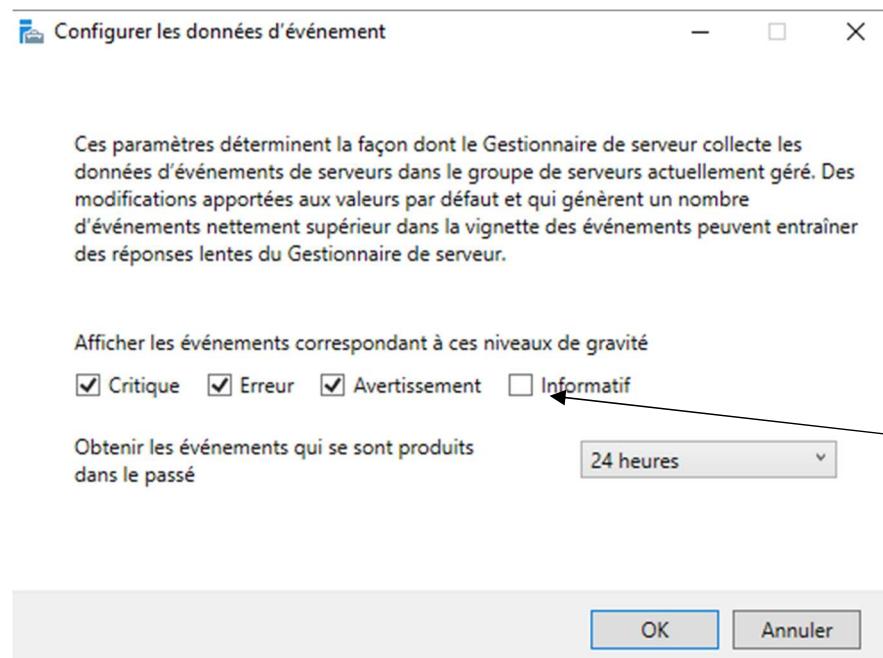
Test : tous les tests de personnalité et quiz gratuits - aufeminin
<https://www.aufeminin.com/tests-quiz/test-tp123989.html>
Web Retrouvez tous nos tests et quiz gratuits : test de personnalité, love test, quiz sur tel ou tel sujet... Quel de plus ludique, instructif et amusant qu'un test ? Pe... Quel de plus ludique ...

Maintenant que nous arrivons à nous connecter, rendons-nous sur le serveur de Mulhouse afin de regarder les Logs.

Pour ce faire, il faut aller dans



Tâches, configurer les données d'événements



Ici, nous devons cocher la case informatif pour avoir les logs de connexion

Dec 16 10:45:40	logportalauth	72613	Zone: portalmul - ACCEPT: Paul, , 192.168.200.253
Dec 16 10:47:25	logportalauth	15236	Zone: portalmul - Reconfiguring captive portal(PortalMul).
Dec 16 10:48:06	logportalauth	74567	Zone: portalmul - DISCONNECT: Paul, , 192.168.200.253
Dec 16 10:49:04	logportalauth	4326	Zone: portalmul - ERROR: Paul, , 192.168.200.253, Error : could not connect to authentication server.
Dec 16 10:49:08	logportalauth	4574	Zone: portalmul - ERROR: Paul, , 192.168.200.253, Error : could not connect to authentication server.
Dec 16 10:49:13	logportalauth	4897	Zone: portalmul - ERROR: Paul, , 192.168.200.253, Error : could not connect to authentication server.
Dec 16 10:50:49	logportalauth	41647	Zone: portalmul - ACCEPT: Paul, , 192.168.200.253
Dec 16 11:01:10	logportalauth	41647	Zone: portalmul - FAILURE: Paul, , 192.168.200.2, Internal Error
Dec 16 11:02:03	logportalauth	89600	Zone: portalmul - Reconfiguring captive portal(PortalMul).
Dec 16 11:02:07	logportalauth	89600	Zone: portalmul - DISCONNECT: Paul, , 192.168.200.253
Dec 16 11:02:15	logportalauth	89600	Zone: portalmul - Reconfiguring captive portal(PortalMul).
Dec 16 11:03:02	logportalauth	16297	Zone: portalmul - ACCEPT: Paul, , 192.168.200.2
Dec 16 11:41:54	logportalauth	49563	Zone: portalmul - DISCONNECT: Paul, , 192.168.200.2
Dec 16 13:54:16	logportalauth	414	Zone: portalmul - RADIUS ACCOUNTING FAILED : No valid RADIUS responses received
Dec 28 12:24:59	logportalauth	414	Zone: portalmul - RADIUS ACCOUNTING FAILED : No valid RADIUS responses received
Dec 29 08:09:19	logportalauth	414	Zone: portalmul - RADIUS ACCOUNTING FAILED : No valid RADIUS responses received
Dec 30 09:26:37	logportalauth	414	Zone: portalmul - RADIUS ACCOUNTING FAILED : No valid RADIUS responses received

6.4) TRUENAS

6.4.1) Configuration minimale

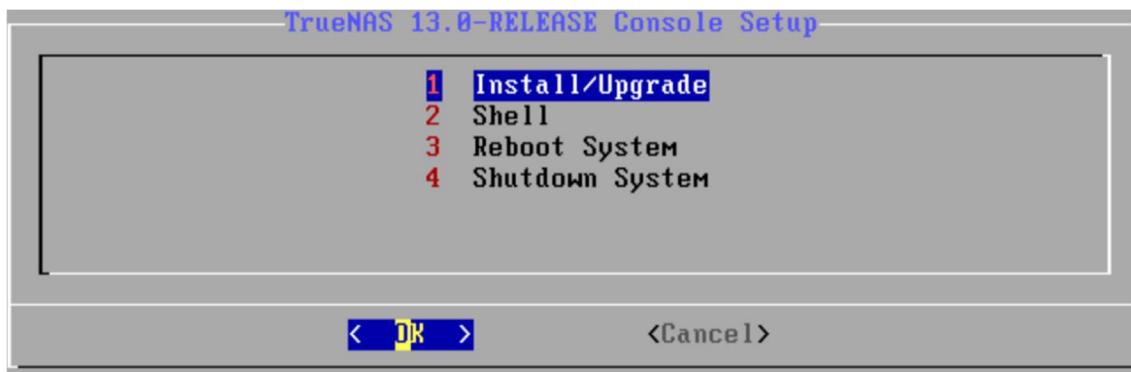
- Processeur 2 cœurs 64 bits
- 8 Go de RAM
- 2 unités de stockage de même taille
- 1 disque d'au moins 16 Go pour que le système fonctionne

Conditions :

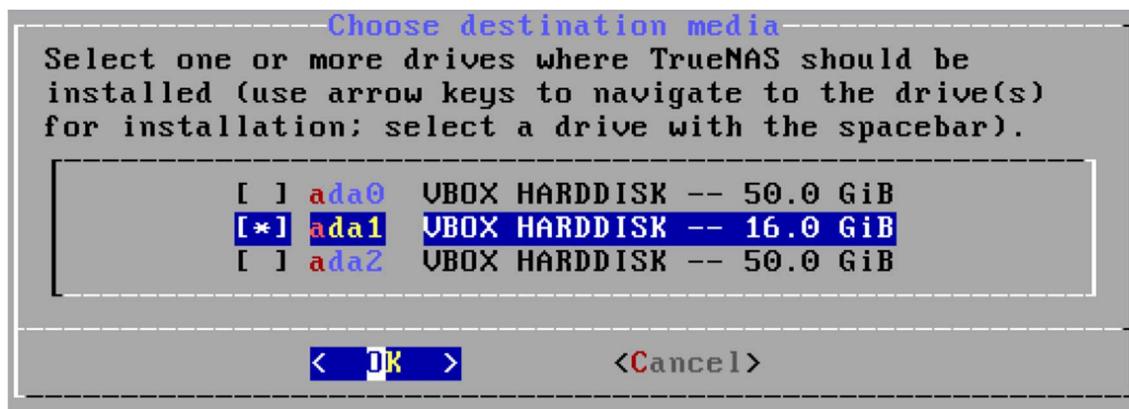
- Fichier ISO TrueNAS.
- Clé USB d'au moins 4 Go.
- Rufus pour graver le fichier ISO sur la clé USB.

Configuration étape par étape de TrueNAS :

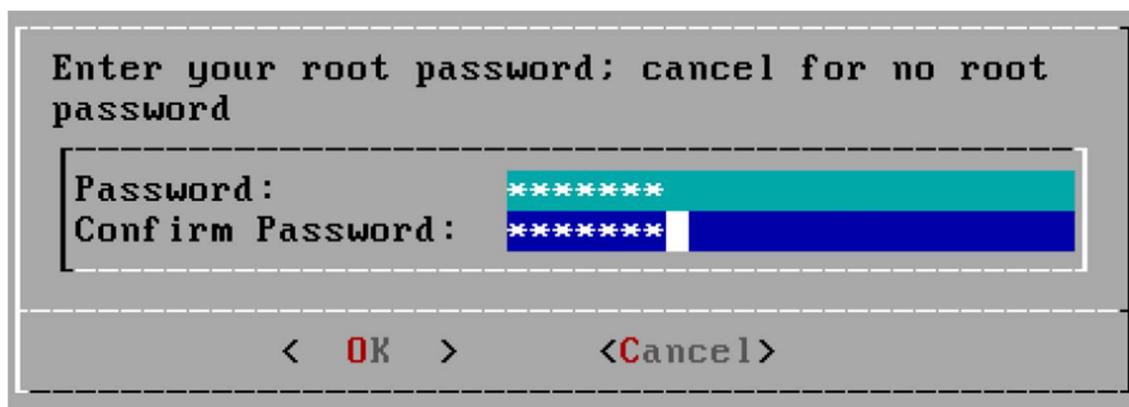
- Gravez le fichier ISO sur la clé USB avec Rufus.
- Branchez la clé USB à votre futur serveur NAS et démarrez la clé USB à partir du BIOS.
- Sur l'interface, sélectionnez l'option Installer/Upgrade à l'aide des touches directionnelles et de la touche Entrée.



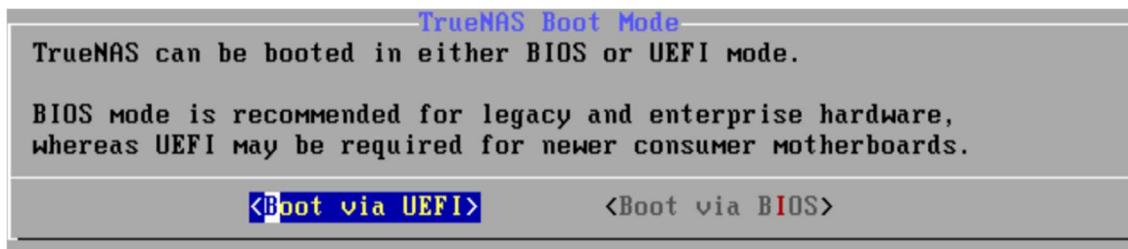
- Sélectionnez le disque pour installer TrueNAS.
- Avec l'aide des touches directionnelles sélectionnez un disque avec la Barre d'espace et appuyez sur Entrée.
 - NB : le disque que vous avez sélectionné pour l'installation ne sera pas utilisé pour le partage de fichiers. Nous allons configurer le partage de fichiers après l'installation.



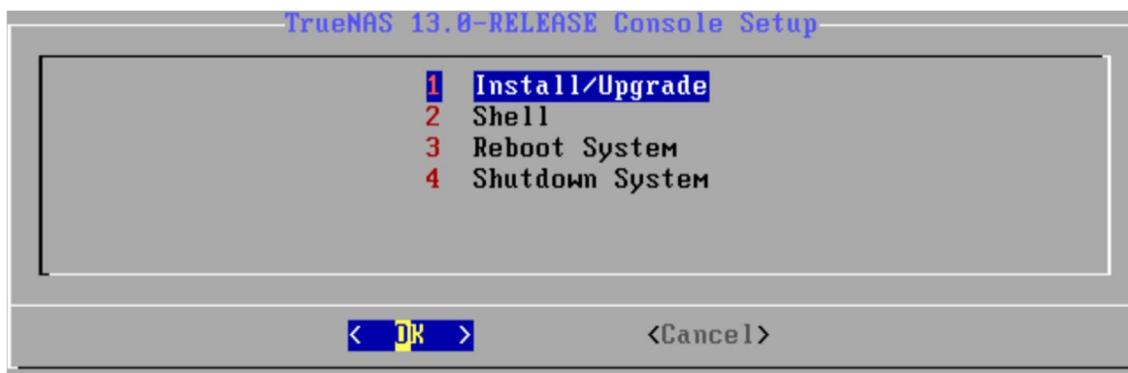
- Définissez le mot de passe du compte root.



- Choisissez le mode de lancement de TrueNAS. Sélectionnez Boot via UEFI



- L'installation commence. Lorsque le processus est terminé, validez Reboot System.



6.4.2) Paramétrage de TrueNAS

- Pour accéder à l'interface TrueNAS, tapez [1] et suivez les configurations suivantes :

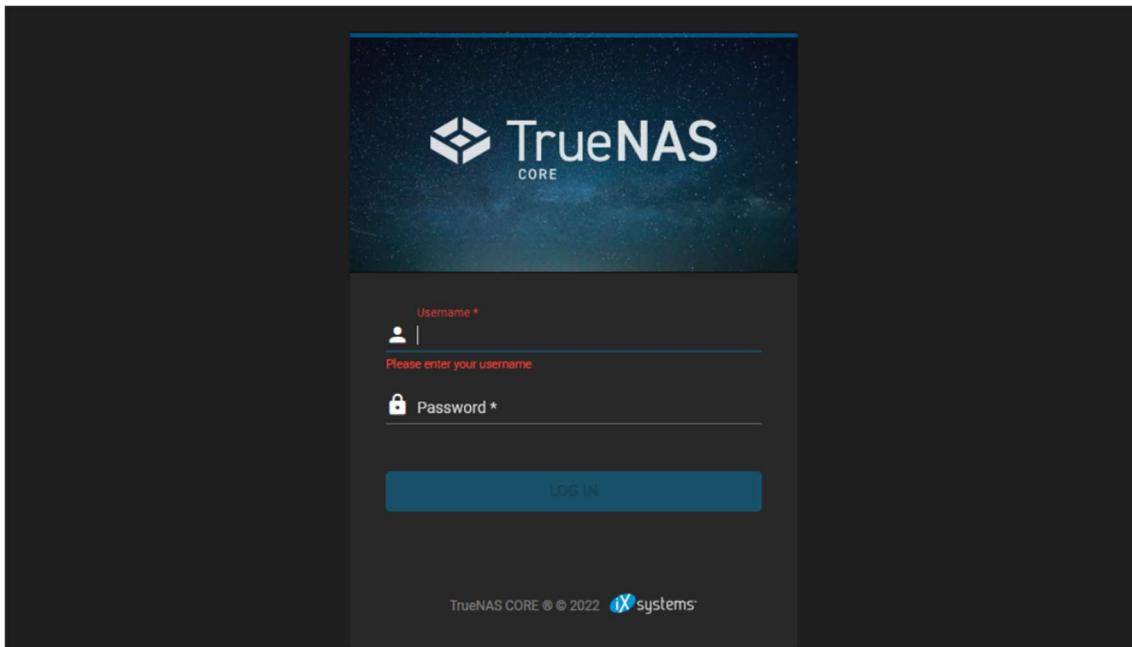
```
The web user interface is at:
http://192.168.100.30
https://192.168.100.30

Enter an option from 1-11: 1
1) em0
Select an interface (q to quit): 1
Delete interface? (y/n) n
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name [NAS]:
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 [192.168.100.30]:
IPv4 Netmask [24]:
Saving interface configuration: Ok
Configure IPv6? (y/n) n
```

Nous devons configurer les disques que nous utiliserons et ajuster les paramètres de partage. Montrons ces étapes étape par étape.

- Lorsque l'adresse IP est configuré. Tapez l'adresse (sur Mozilla Portable) à partir d'un autre appareil au sein du même réseau.

- Nom d' utilisateur : root
- Mot de passe : Pa55w.rd



- Depuis l' onglet Stockage , nous entrons dans la section Pools.
- Sélectionnez l'option Ajouter un pool et créer un nouveau pool avec Créer un nouveau pool .
 - Utilisez la mise en page suggérée.

- Cliquez sur le burger menu puis sur Ajouter un zvol.

- Appliquez les configurations ci-dessus, précisez l'unité de mesure pour la taille du zvol (50 Gib).

- Le volume et le zvol sont créées.

- Depuis l'onglet Service, Activez le service iSCSI.

The screenshot shows the 'Services' page in the TrueNAS web interface. On the left is a sidebar with various system management links. The main area displays a table of services. The 'iSCSI' service is listed with its status as 'On' (blue switch), 'Running' (green circle), and 'Automatically started' (checkmark). There are edit and delete icons for each row.

Nom	En cours	Démarrage automatique	Actions
AFP	●	□	✎
Dynamic DNS	●	□	✎
FTP	●	□	✎
iSCSI	●	✓	✎
LLDP	●	□	✎
NFS	●	□	✎
OpenVPN Client	●	□	✎
OpenVPN Server	●	□	✎
Rsync	●	□	✎

- Depuis l'onglet Partages, Cliquez sur la section Partages Block (iSCSI).
 - Cliquez sur Enregistrer.

The screenshot shows the 'Partages / iSCSI' configuration page. The sidebar lists different share types, with 'Partages Block (iSCSI)' selected. The main panel is titled 'Target Global Configuration' and includes tabs for 'Extents' and 'Associated Targets'. It features fields for 'Nom de base' (iqn.2005-10.org.freenas.ctf), 'Serveurs ISNS', and 'Seuil d'espace disponible dans le volume (%)'. A large blue 'ENREGISTRER' button is at the bottom. A 'WIZARD' button is visible in the top right corner of the main panel.

- Cliquez sur la section Portals et Ajouter.

Partages / iSCSI / Portals / Ajouter

Infos de base

Description

Méthode et groupe d'authentification

Méthode d'authentification de découverte
NONE

Groupe d'authentification de découverte

Adresse IP

Adresse IP * 192.168.100.30 Port 3260

AJOUTER

ENVOYER ANNULER

- Cliquez sur la section Cibles et Ajouter.

Partages / iSCSI / Cibles / Ajouter

Infos de base

Nom de la cible * iscsi

Alias de la cible iscsi

groupe iSCSI

ID de groupe du portail * 1 (iSCSI)

ID de groupe de l'initiateur 1 (ALL Initiators Allowed)

Méthode d'Authentification

Aucun Numéro du groupe d'authentification

AJOUTER

ENVOYER ANNULER

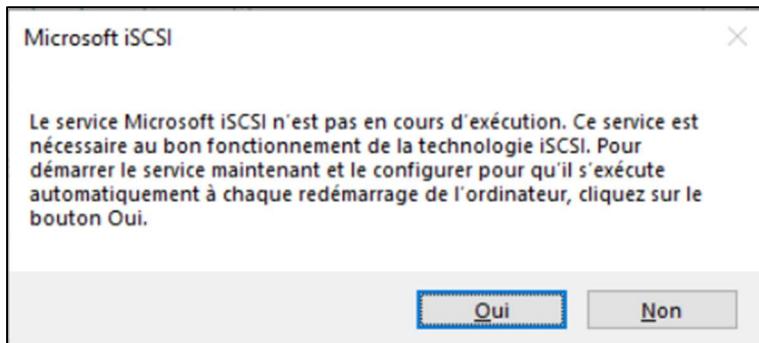
- Cliquez sur la section Extents et Ajouter.

- Cliquez sur la section Associated Targets et Ajouter.

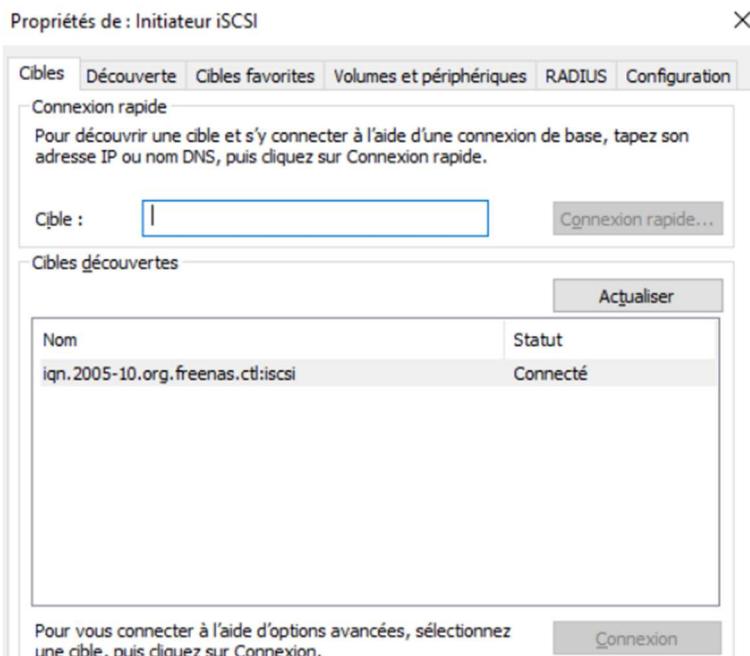
- Sur le Serveur Windows 2019, tapez iSCSI Initiator sur la barre de recherche.



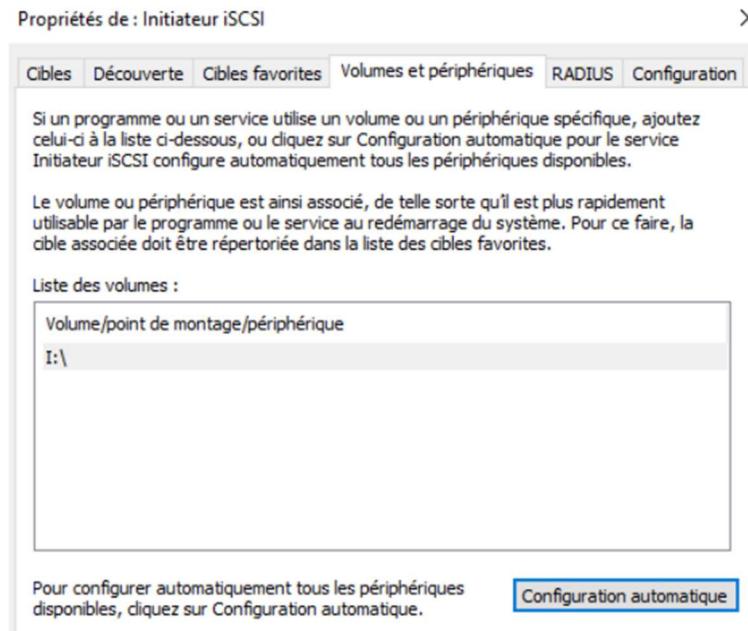
- Autoriser l'installation du rôle.



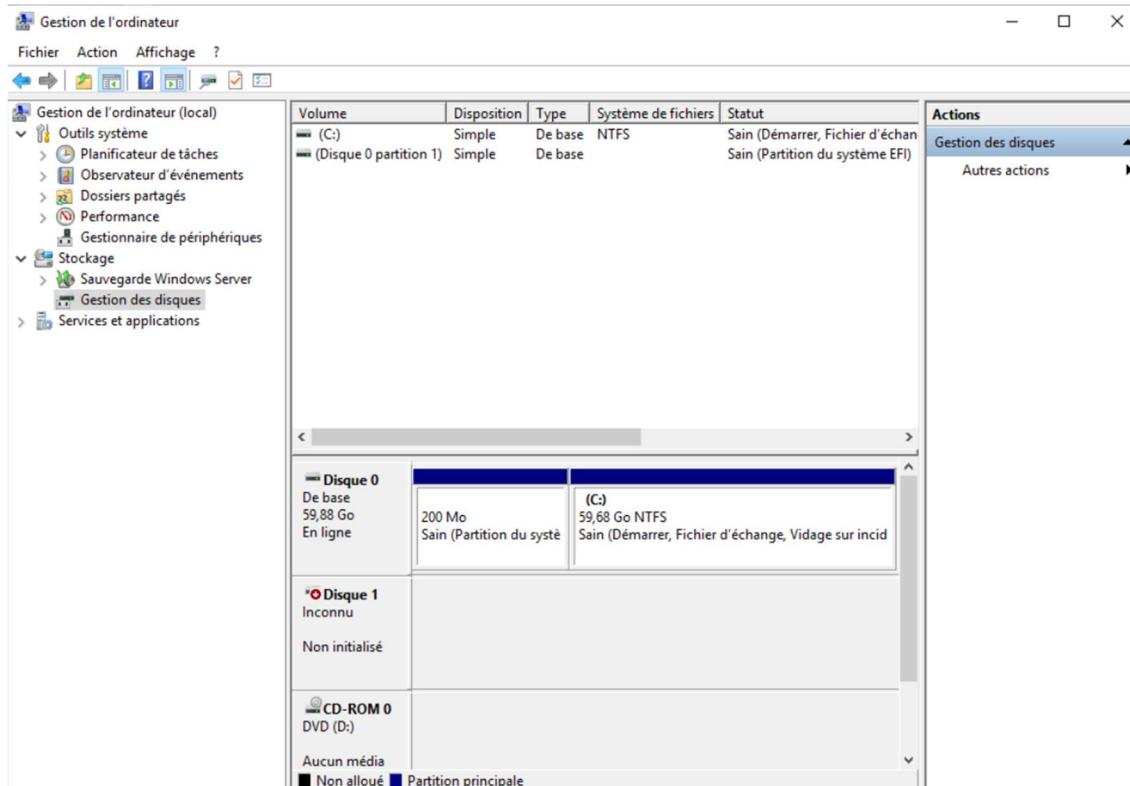
- Dans la section Cible, saisissez l'adresse IP du serveur TrueNAS préalablement configuré. Puis cliquez sur Connexion.



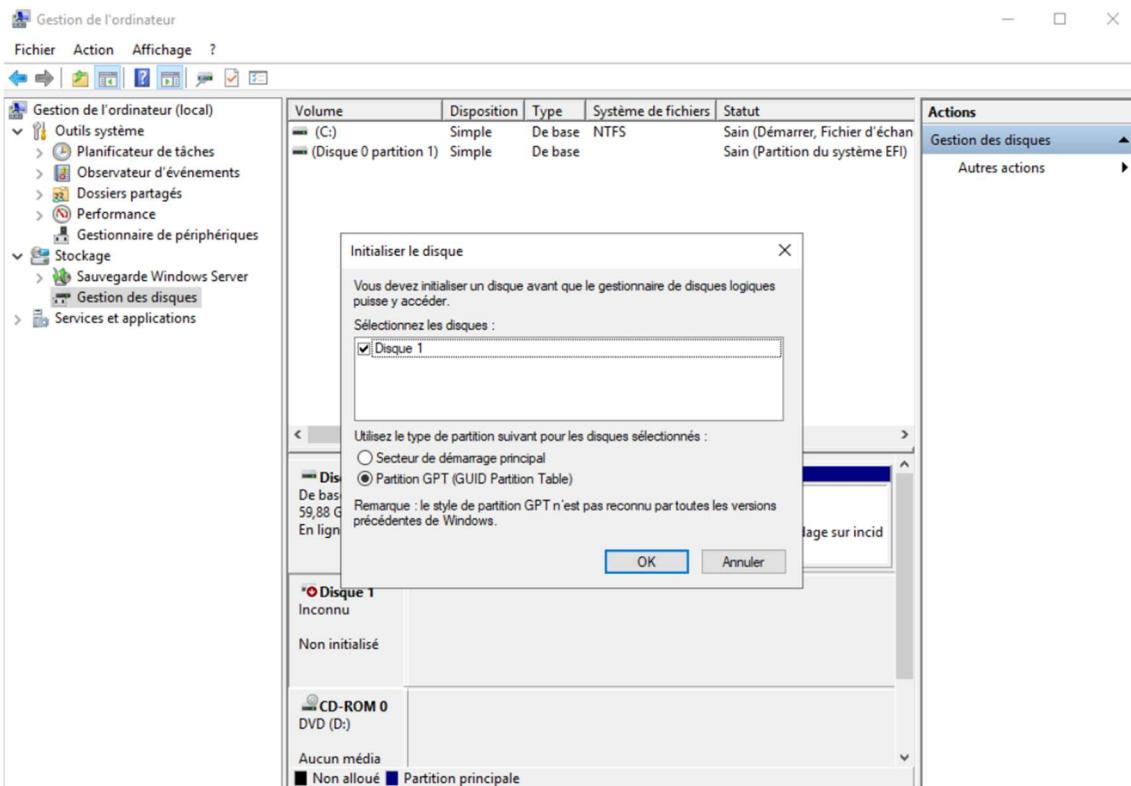
- Dans la section Volumes et périphériques, cliquez sur Configuration automatique.



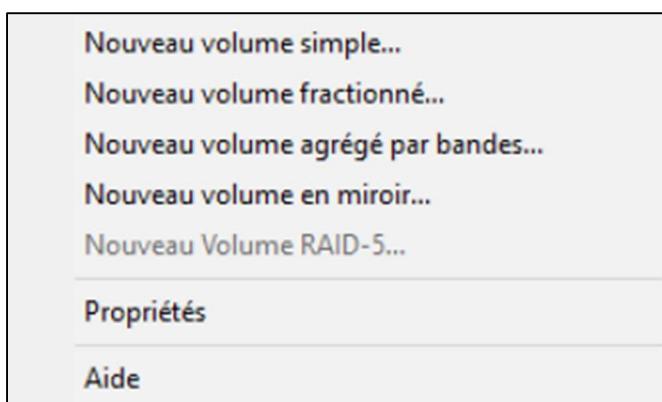
- Cliquez droit sur la barre Windows, puis cliquez sur Gestion de disque.



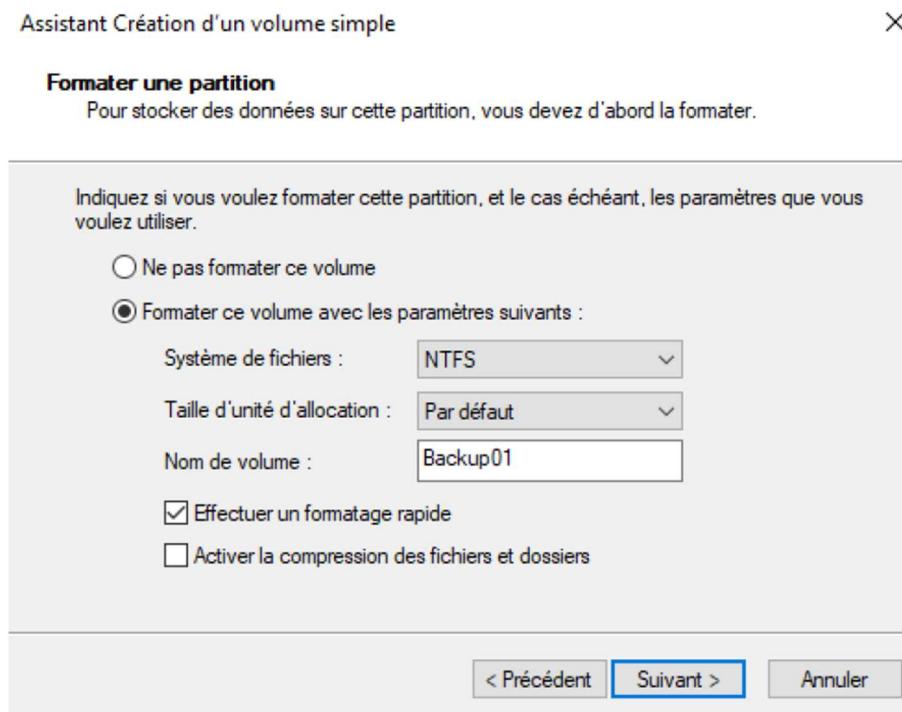
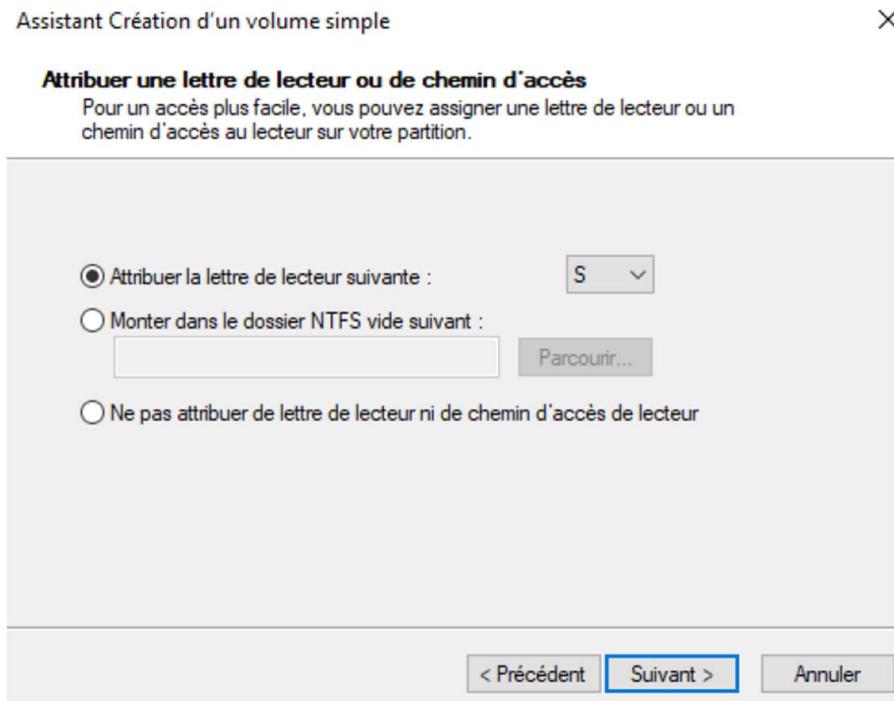
- Cliquez droit sur le disque, puis Initialiser le disque.



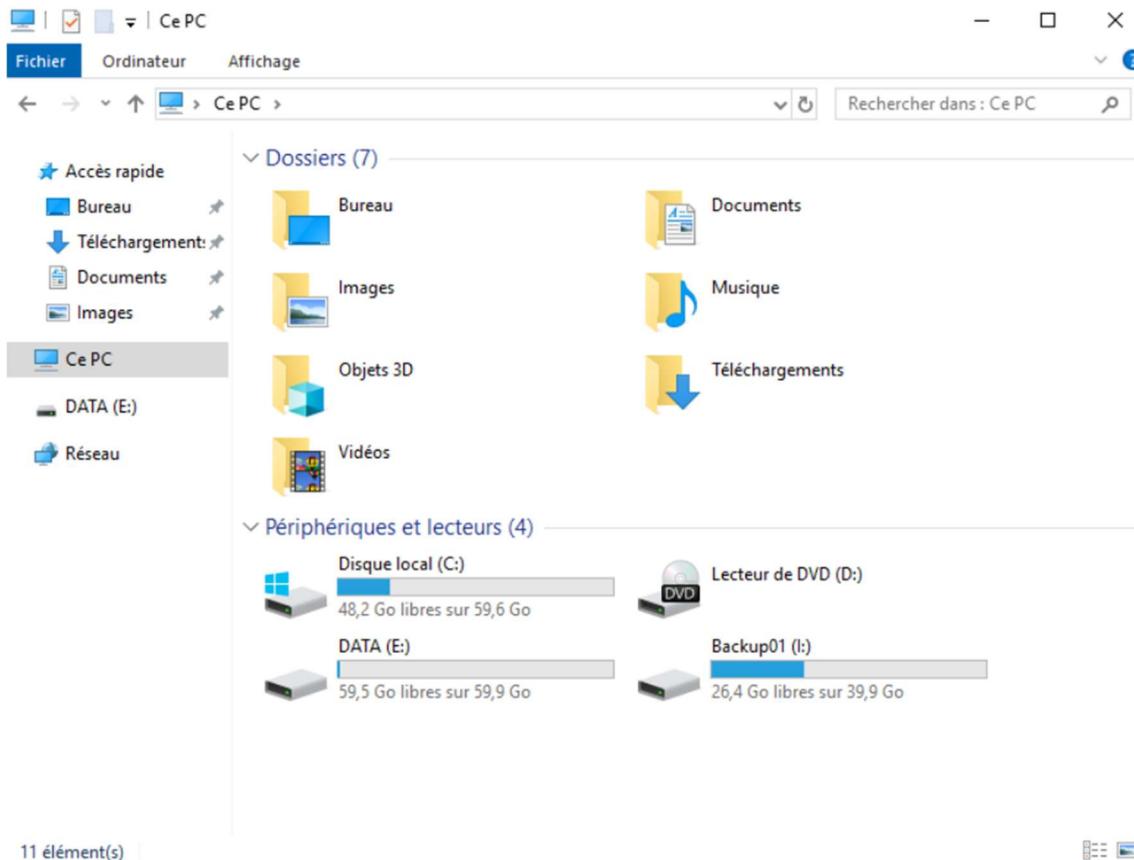
- Cliquez droit sur l'emplacement du disque, puis Nouveau volume simple.



- Procéder à l'installation du nouveau volume, Attribuer une lettre au disque.



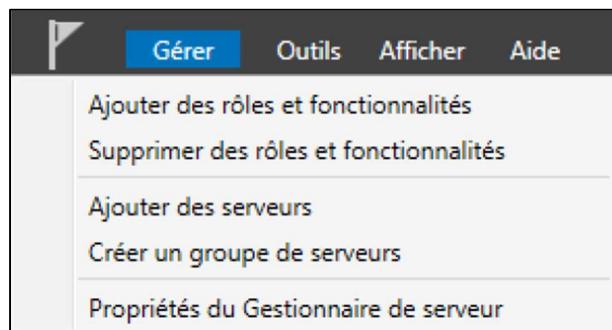
- Le disque est maintenant visible dans l'explorateur de fichiers.



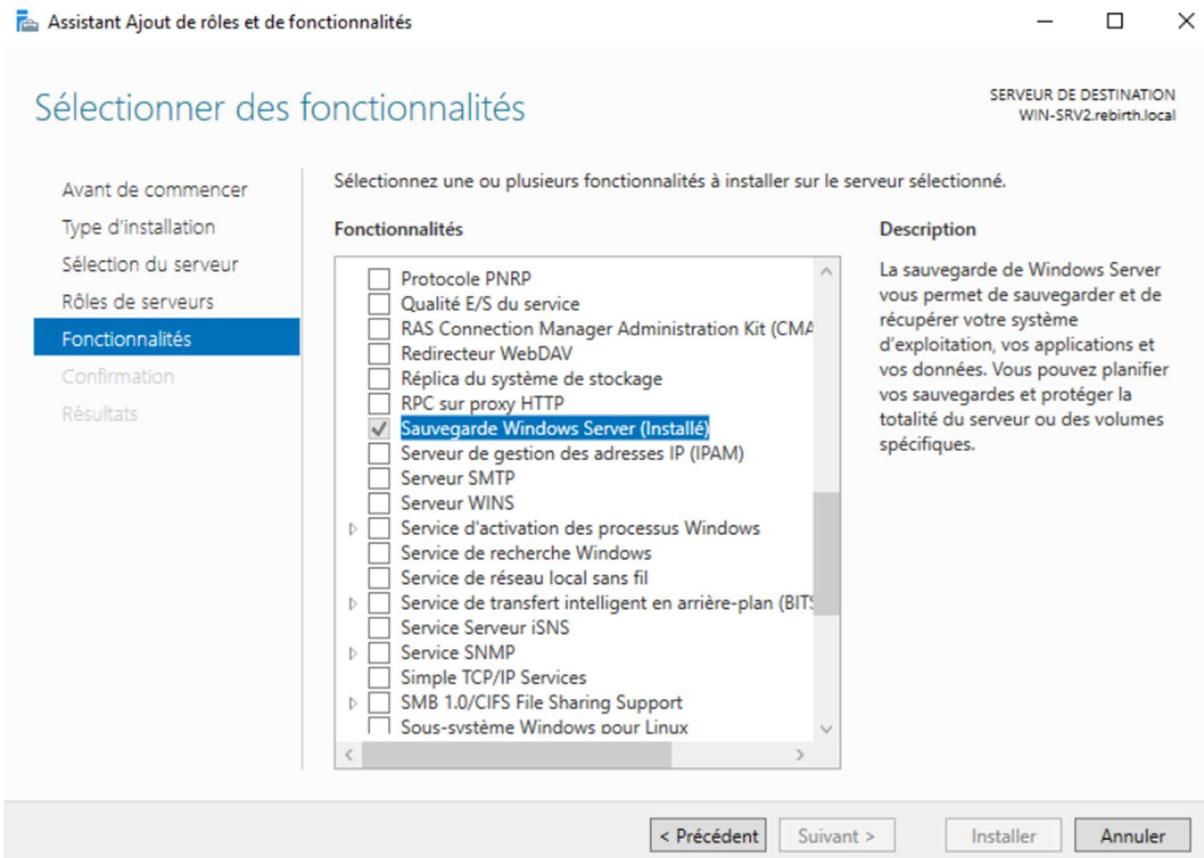
6.5) Sauvegarde et SHADOWCCOPY

6.5.1) Planification de la Sauvegarde Windows Server

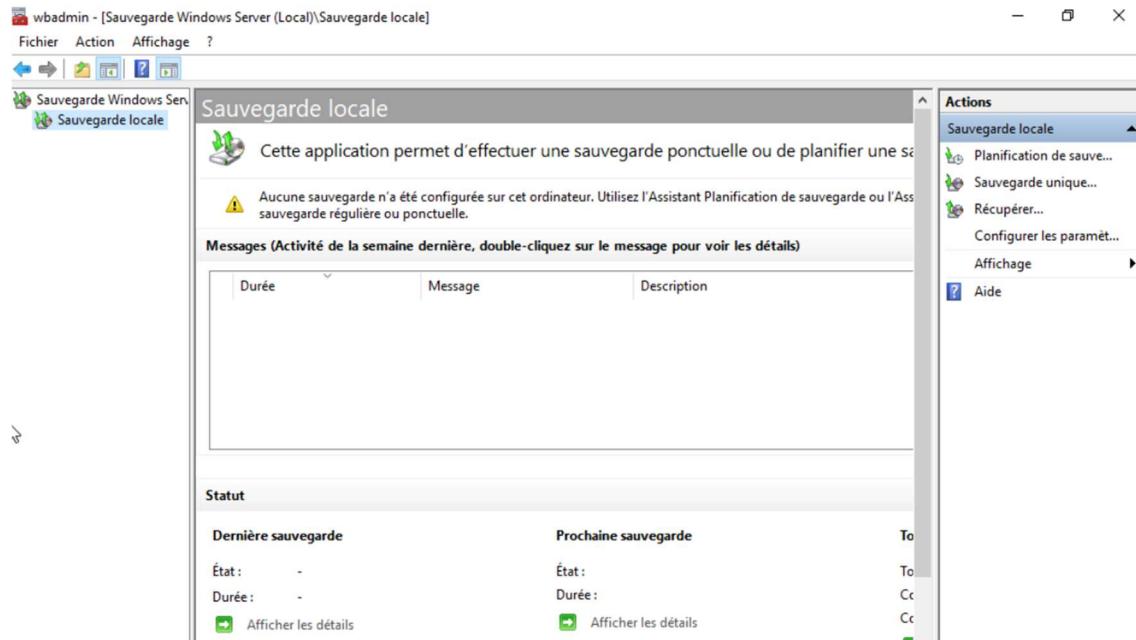
- Cliquez sur Gérer, puis Ajouter des rôles et fonctionnalités.



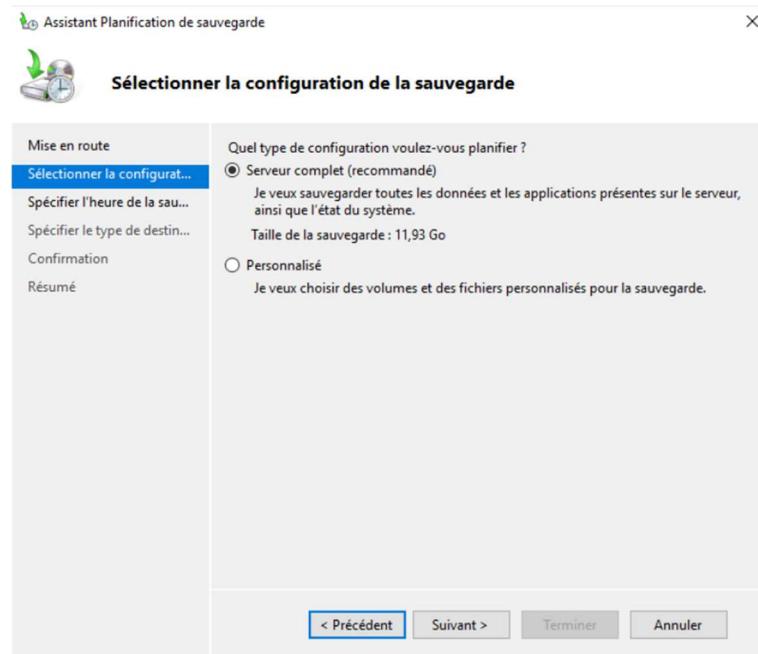
- Procédez à l'installation du rôle : Sauvegarde Windows Server



- Une fois l'installation terminé, lancer l'utilitaire de Sauvegarde Windows Server.

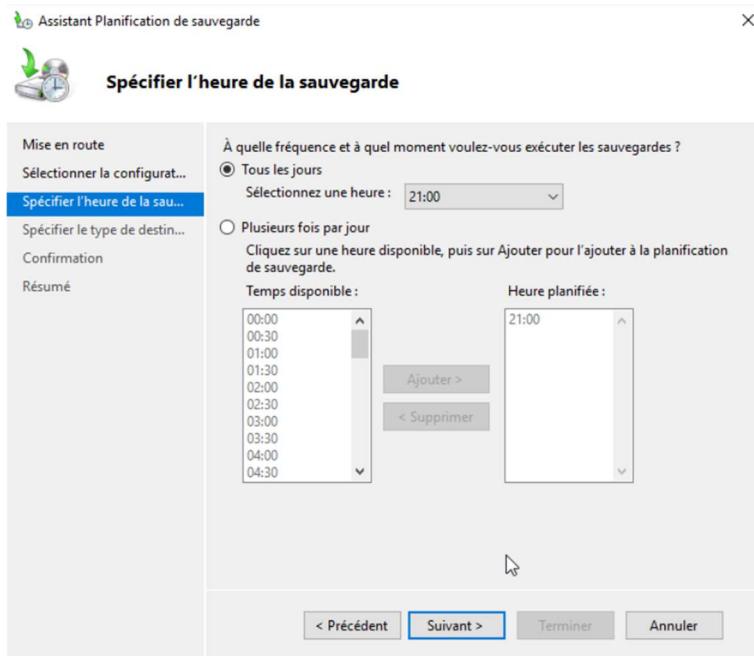


- Sur l'interface à droite de la fenêtre, dérouler le menu Sauvegarde locale, puis cliquez sur Planification de sauvegarde.

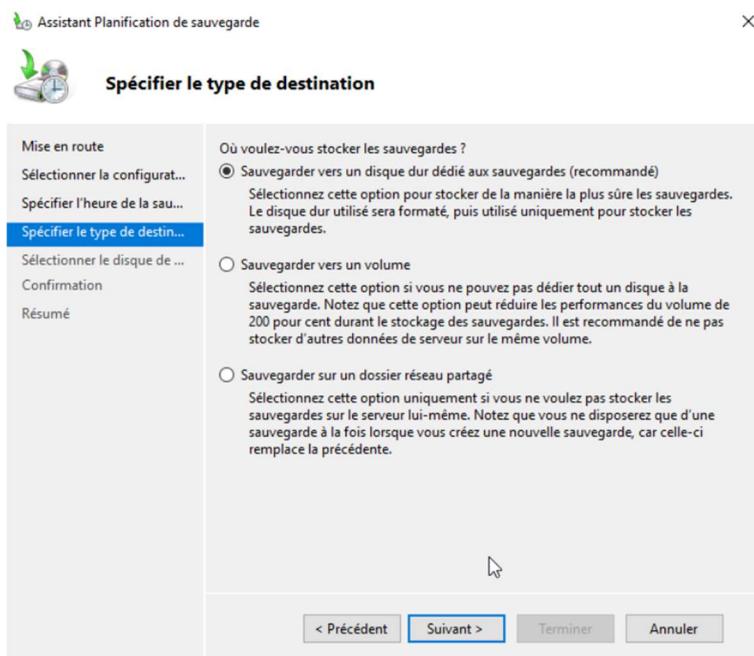


- Sélectionnez Serveur complet, puis Suivant.

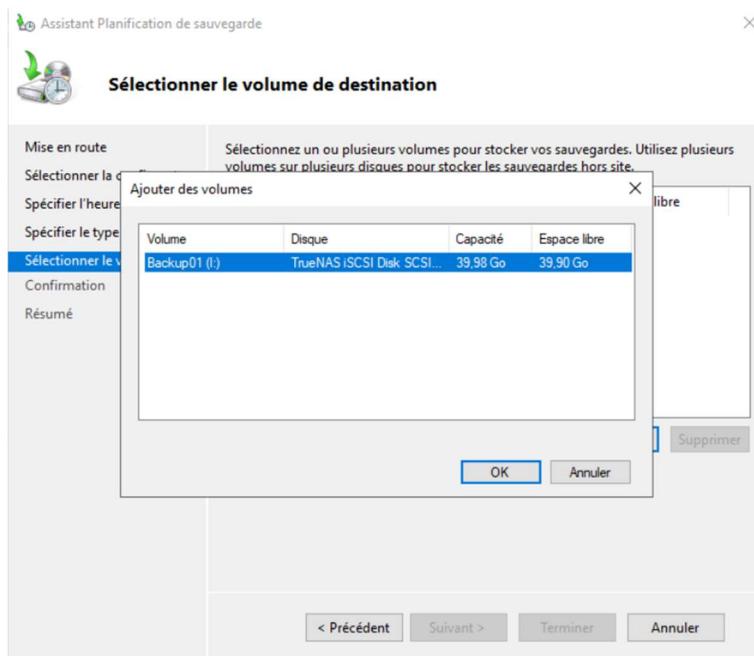
- Configurer la fréquence de l'exécution des sauvegardes, puis Suivant.



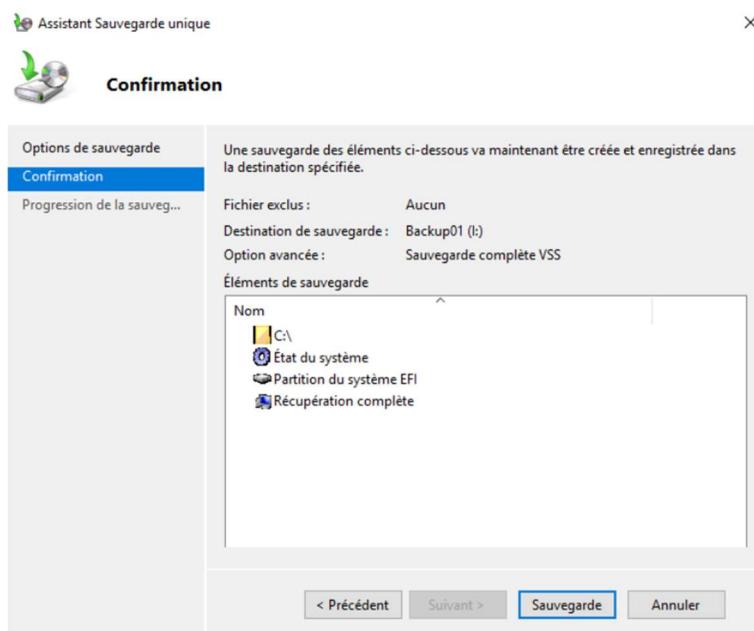
- Selectionnez le premier choix.

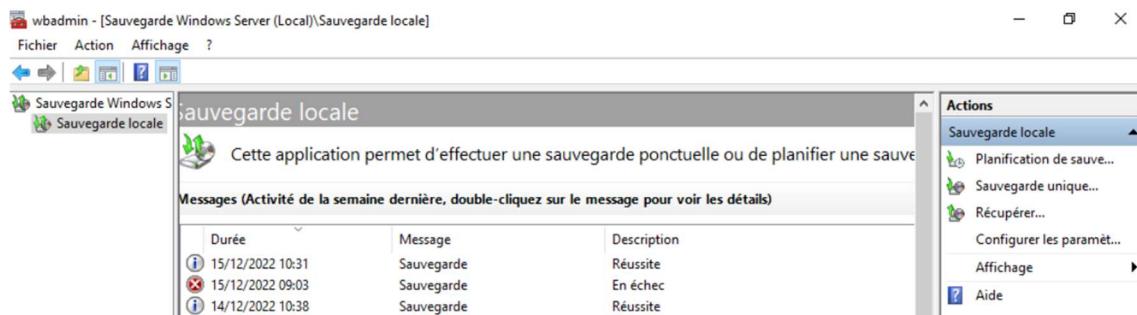
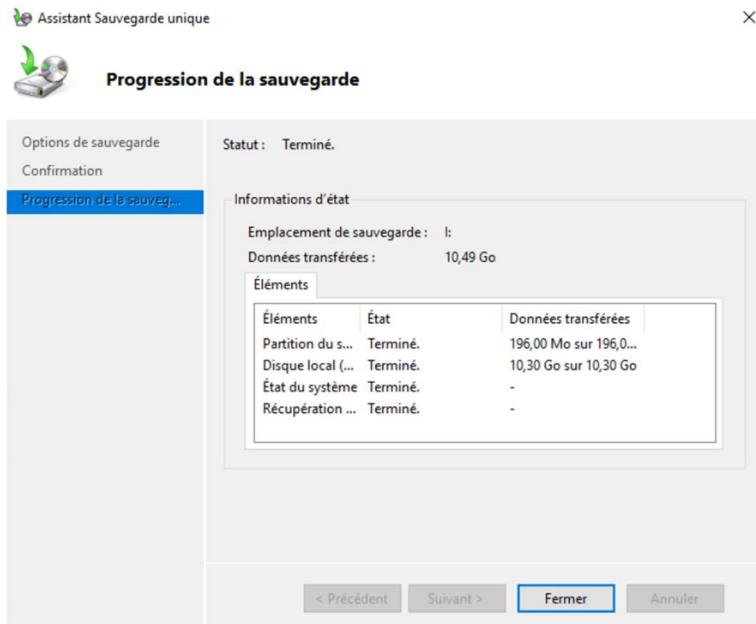


- Sélectionnez le disque TrueNAS, puis cliquez sur OK.



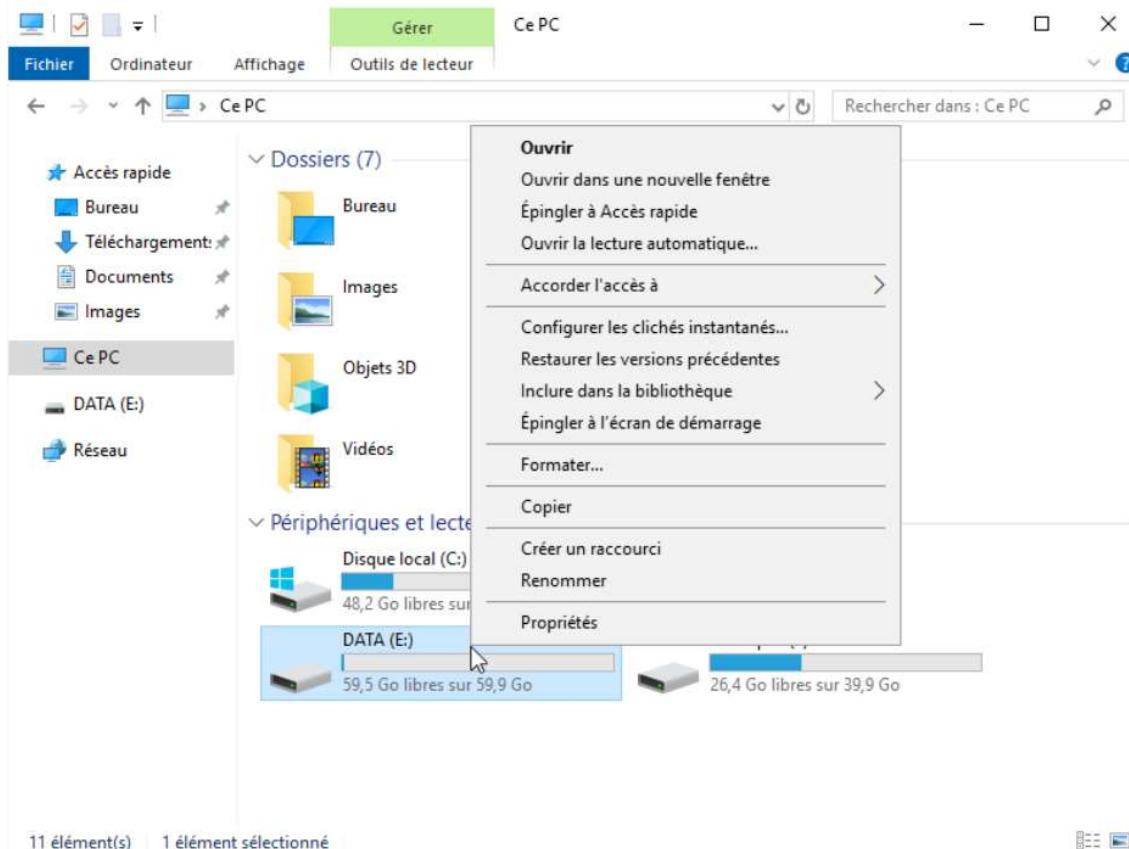
- Vérifiez les éléments saisis puis cliquez sur Sauvegarde.



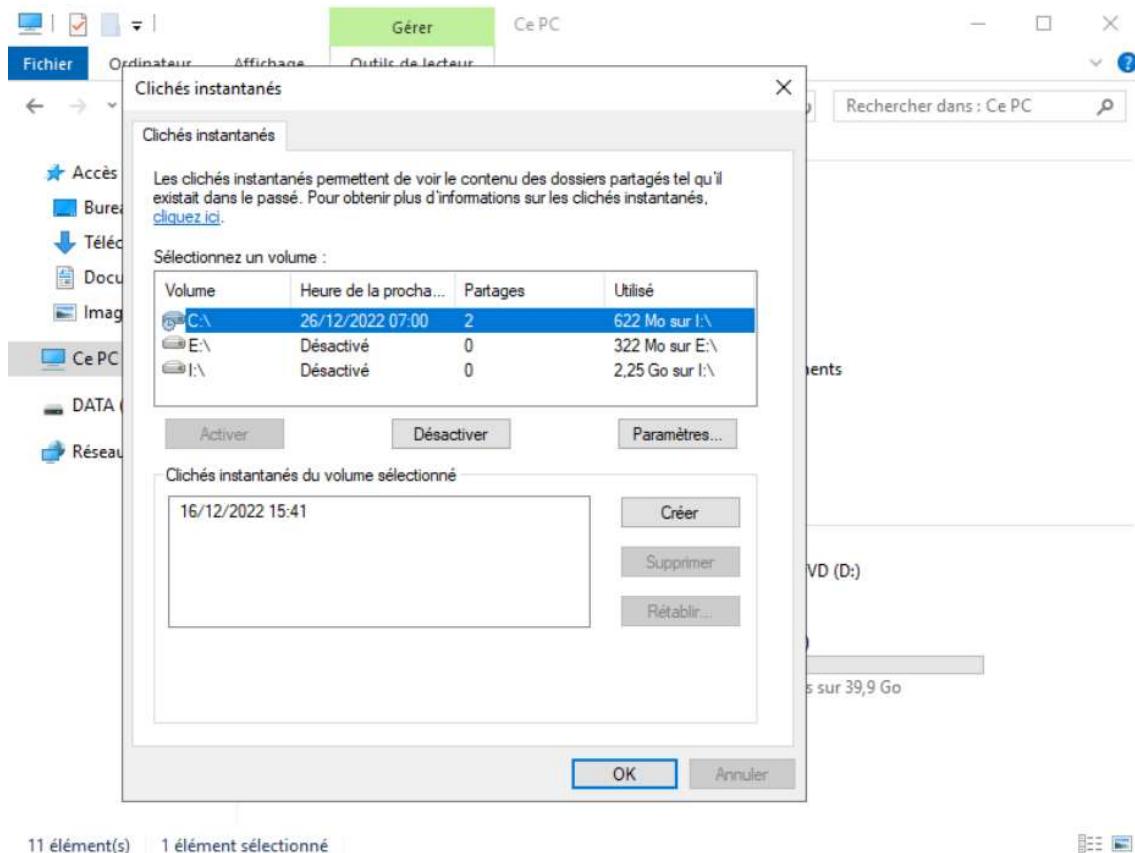


6.4.3) Mise en place de clichés instantanée

- Dans l'explorateur de fichiers, cliquez droit sur le disque source

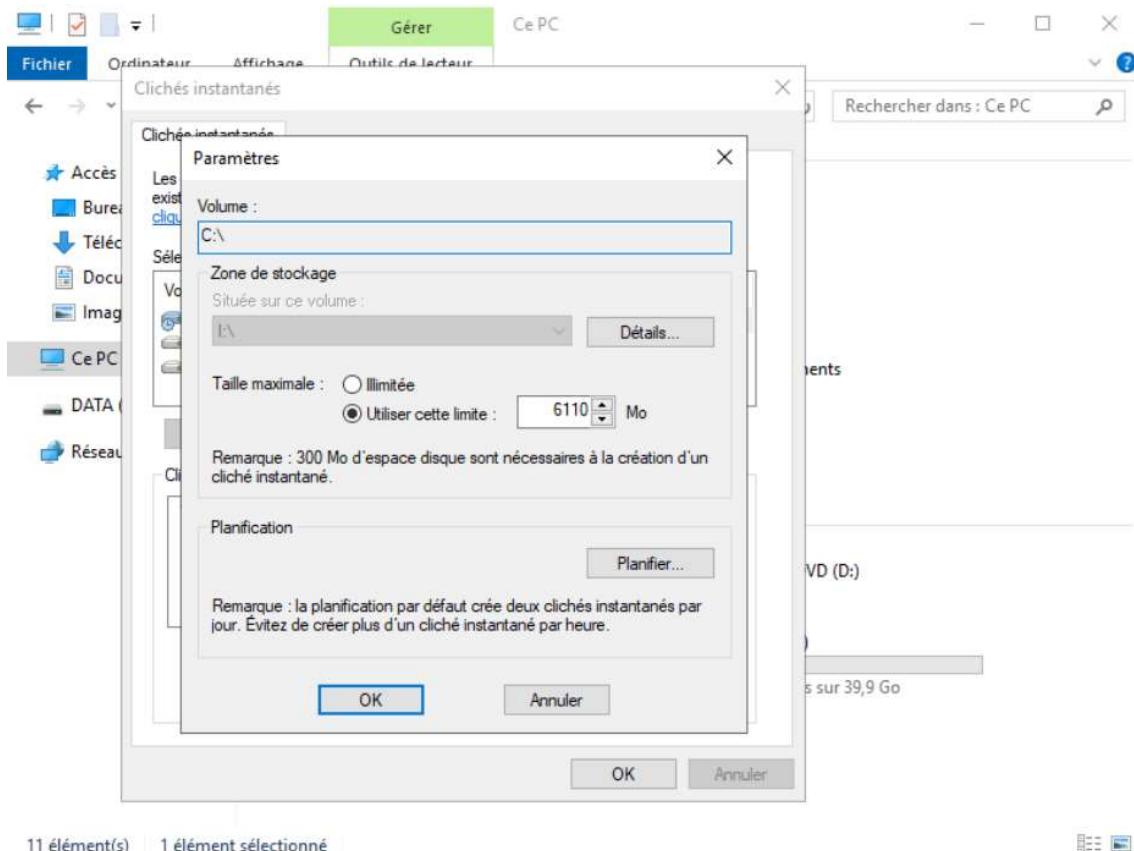


- Sélectionnez le disque source (C:\) : puis cliquez sur Paramètres.



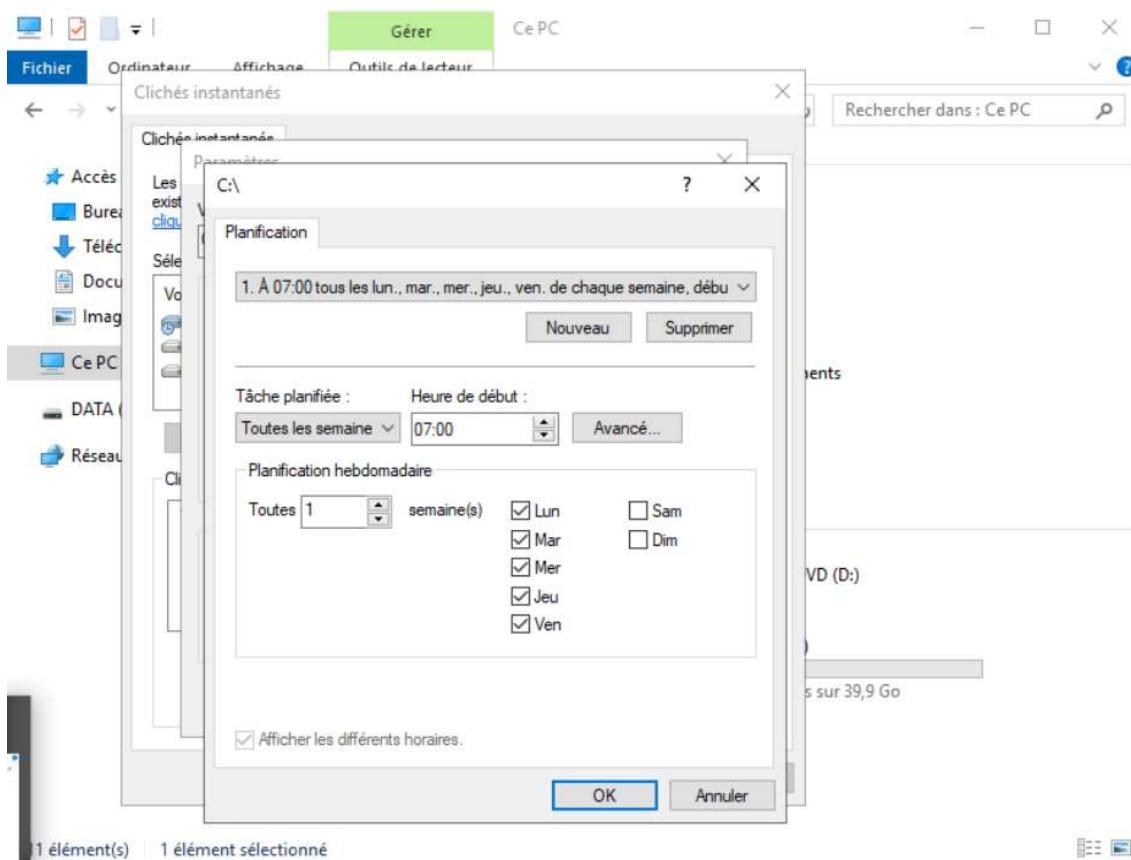
11 élément(s) | 1 élément sélectionné

- Sélectionnez la destination de stockage du clichés instantanés



- Cliquez sur Planifier pour paramétriser la fréquence de clichés de sauvegarde.

- Paramétrer l'heure des clichés instantanée, puis cliquez sur OK.



Pour effectuer un cliché instantané, cliquez sur Créer.

