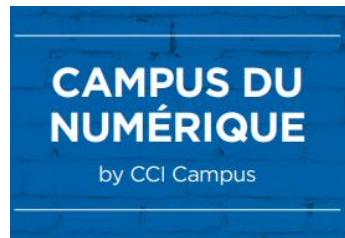


PROJET M2i



AP3

Documentation Technique

Durée du projet : Du 02/09/2022 au 31/12/2022

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l'auteur ou des auteurs et n'engagent aucunement CCI Campus

Table des matières

1 Installation des routeur/pare-feu.....	4
1.1 Routeur/Pare-feu du site A	4
1.1.1 Installation de pfSense	4
1.1.2 Configuration à partir de pfSense	8
1.1.3 Configuration à partir d'une machine cliente	9
1.2 Routeur /pare-feu du site B.....	12
2 Création de la liaison VPN	13
2.1 Configuration de IPsec sur le site A	13
2.1.1 Configuration de la phase 1.....	13
2.1.2 Configuration de la phase 2.....	15
2.2 Configuration de IPsec sur le site B	17
2.3 Test de la liaison VPN	17
2.4 Règles du pare-feu.....	17
2.4.1 Création d'alias.....	17
2.4.2 Interface WAN	18
2.4.3 Interface LAN.....	18
2.4.4 Interface IPsec	18
3 Installation et configuration des serveurs Windows.....	20
3.1 Configuration de l'IP Bonding.....	20
3.2 Installation des rôles et fonctionnalités	22
3.3 Mise en place de l'ADDS.....	24
3.3.1 Installation et ajout des contrôleurs de domaine	26
3.4 Mise en place du DNS.....	39
3.4.1 Ajout de zones inversées.....	41
3.4.2 Ajout d'un pointeur (PTR).....	45
3.5 Mise en place du DHCP.....	47
3.5.1 Autoriser le service DHCP dans l'AD.....	47
3.5.2 Création d'une étendue pour l'attribution d'adresses.....	48
3.5.3 Création d'un basculement	53
3.6 Mise en place du DFS/DFSR.....	56
3.6.1 Configuration dossier du DFS :	56
3.6.2 Création dossier partagé :	66
3.6.3 Configuration espace de nom et réPLICATION :	75
3.7 Mise en place de RADIUS	90

3.7.1 Crédation des utilisateurs.....	91
3.7.2 Crédation du groupe RADIUS	94
3.7.3 Inscription du serveur RADIUS dans l'AD	96
3.7.4 Ajout d'un client RADIUS	98
3.7.5 Ajout d'une nouvelle stratégie	99
4 Crédation du portail Captif.....	105
4.1 Liaison du portail captif à l'AD.....	105
4.2 Crédation du portail Captif	105
4.3 Exclusion de certaines machines.....	106
5 Installation des serveurs de stockage.....	107
5.1 Installation de TrueNAS.....	107
5.2 Configuration système et réseau	110
5.3 Mise en place des Volumes et du RAID	112
5.4 Crédation et configuration Zvol.....	112
5.5 Configuration ISCSI	114
5.5.1 Configuration sur le serveur NAS	114
5.5.2 Configuration sur le serveur Windows.....	115
6 Sauvegarde du Windows serveur :	115
6.1 Sauvegarde Unique :	118
6.2 Planification de sauvegarde :	123
7 Mise en place des GPO	134
7.1 Crédation du lecteur U pour le dossier personnel de l'utilisateur	134
7.2 Crédation du lecteur T sur le répertoire TRANSFERT	138
7.3 Déployer et bloquer un fond d'écran.....	139
7.4 Rediriger les dossiers « mes documents » et « bureau » vers le dossier personnel de l'utilisateur.....	141
7.5 Interdire l'accès au panneau de configuration.....	144
7.6 Bloquer les ports USB	145
7.7 Masquer et bloquer les accès aux disques locaux des postes	146
7.8 Bloquer l'accès aux consoles Powershell et Invité de commande	149

1 Installation des routeur/pare-feu

1.1 Routeur/Pare-feu du site A

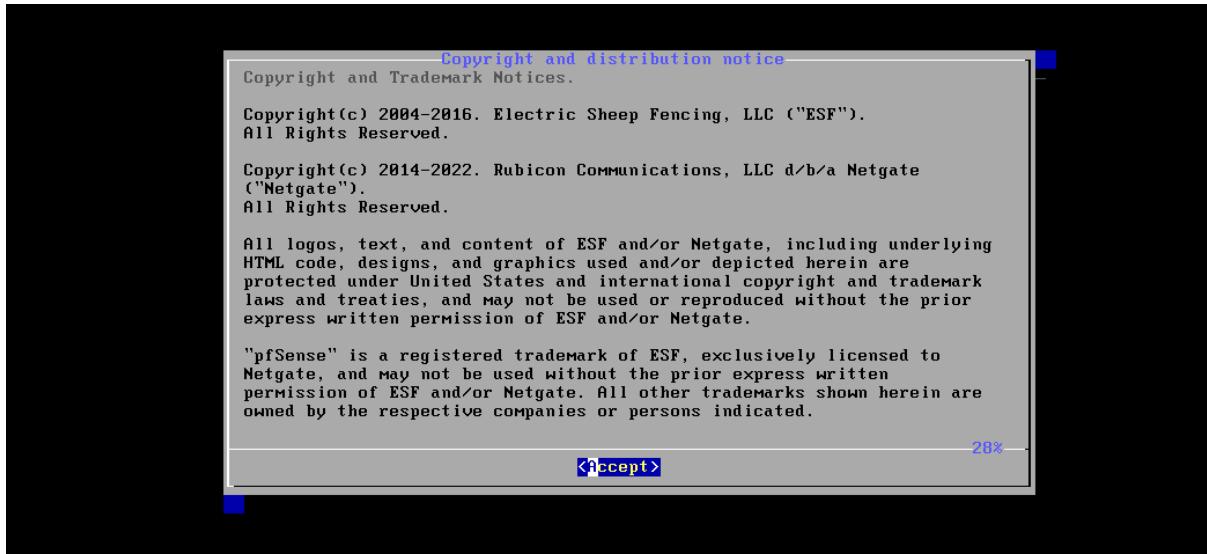
1.1.1 Installation de pfSense

On télécharge l'image ISO depuis le site officiel : <https://www.pfsense.org/download/>

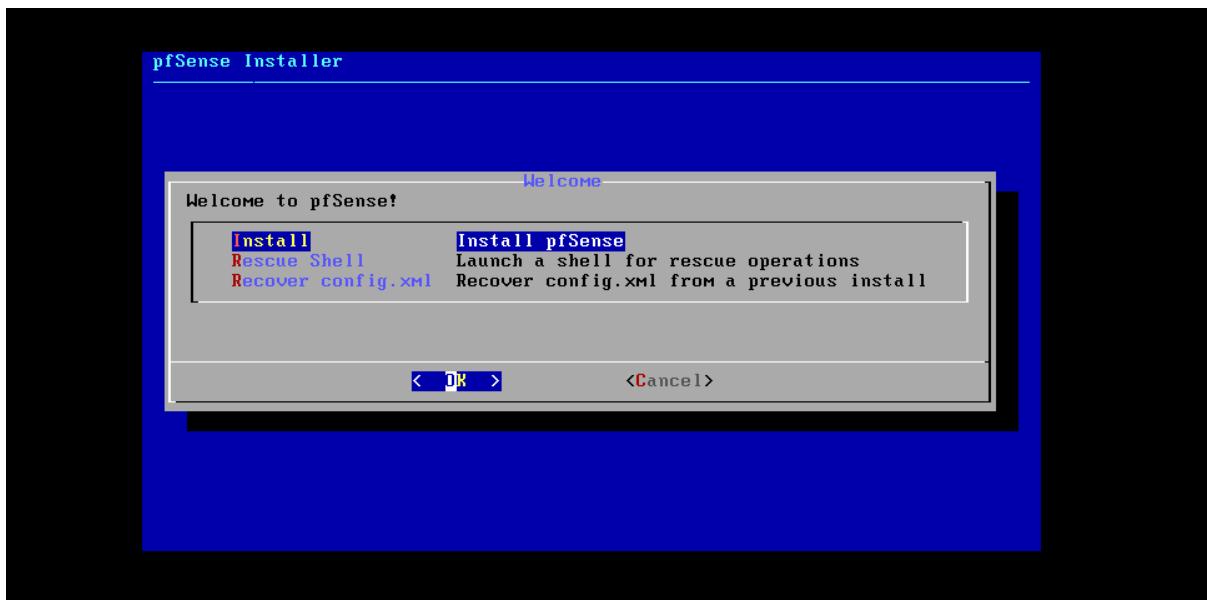
On crée une machine virtuelle à partir de cette ISO.

Nous allons configurer 2 cartes réseaux sur la machine virtuelle : la 1^{ère} sera en NAT (interface WAN) et la 2^e sur un réseau privé nommé VMnet1 (interface LAN).

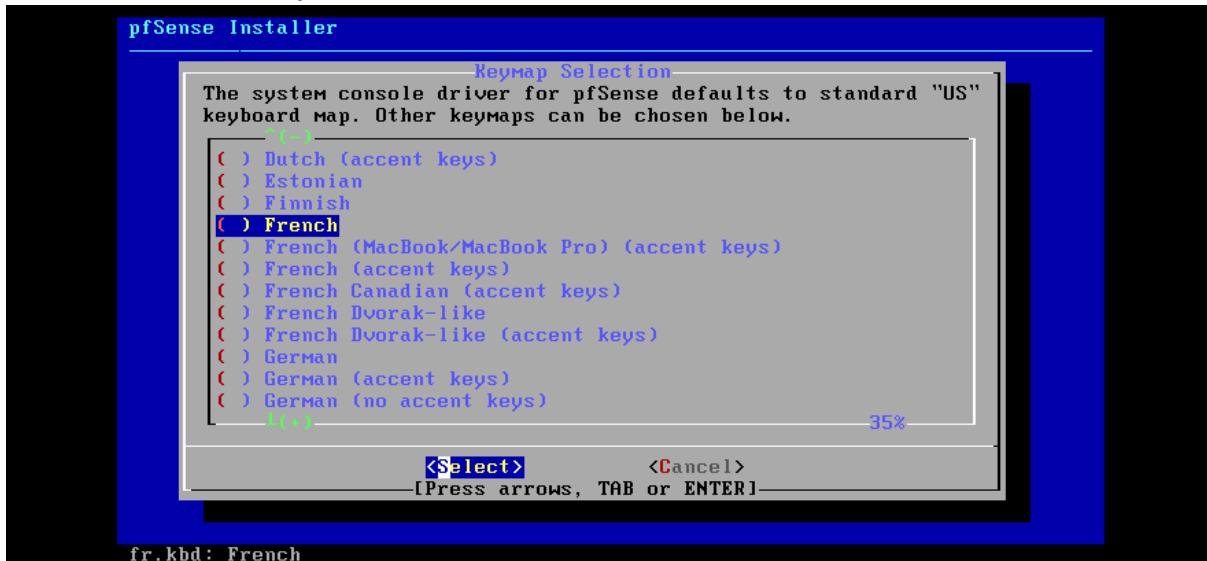
On accepte les copyrights :



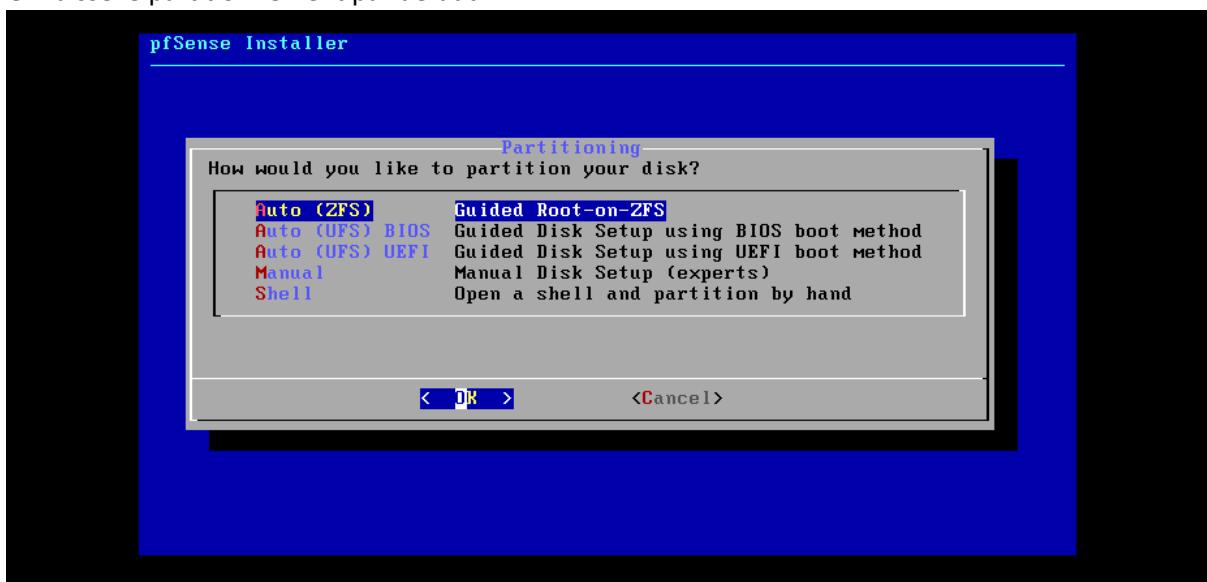
On choisit de faire une installation :



On choisit le clavier français :



On laisse le partitionnement par défaut :



On ne configure pas d'autres options :



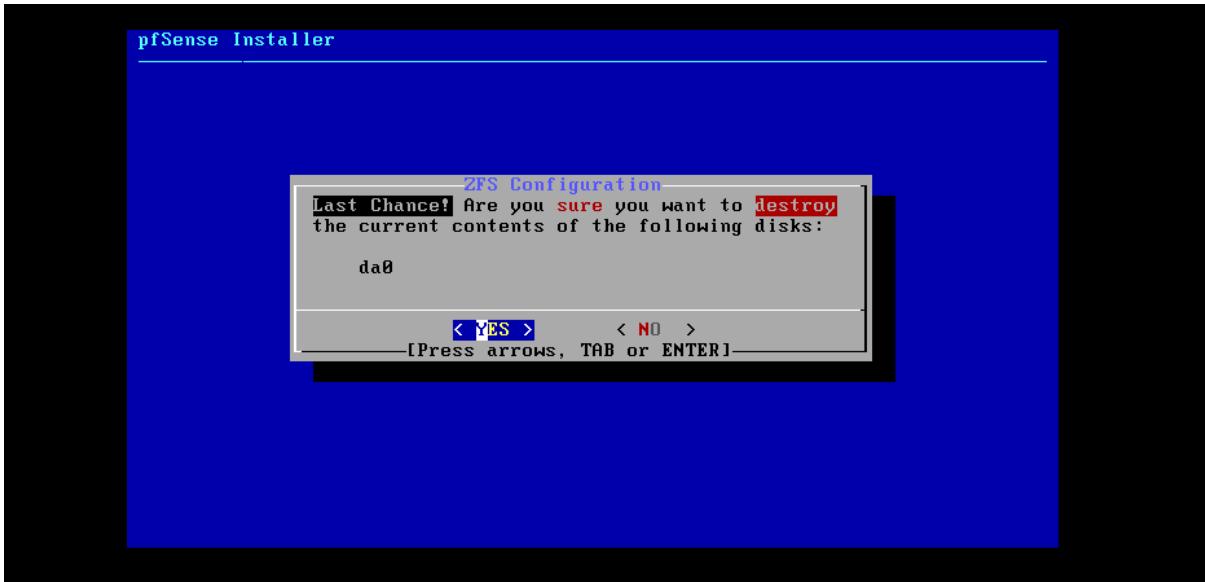
On ne met pas de raid en place :



On sélectionne le disque dur où installer l'OS :



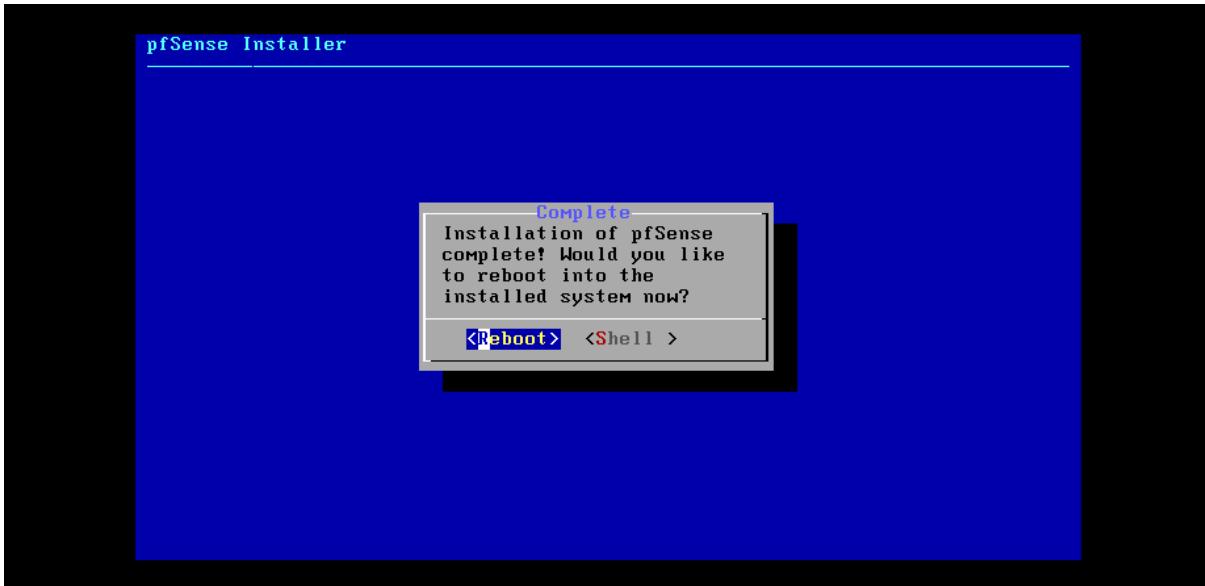
On dit oui pour formater le disque :



On ne fait pas de modifications supplémentaires :



On redémarre :



1.1.2 Configuration à partir de pfSense

Dans le cadre de la maquette, nous allons laisser l'interface WAN en mode DHCP.

Il n'y a donc que la carte réseau LAN à configurer. Voici comment la configurer :

- On tape 2 pour rentrer dans l'option *Set Interface IP address*
- On tape 2 pour sélectionner l'interface numéro 2 (LAN)
- On attribue l'adresse IP : 192.168.100.1
- On donne le masque de sous réseau : 24

```

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
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:
> 192.168.100.1

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

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

```

- On ne donne pas de passerelle, on appuie juste sur entrer
- On ne donne pas d'adresse ipv6, on appuie juste sur entrer
- On tape « n » pour ne pas activer le DHCP
- On dit oui pour utiliser le protocole http
- On appuie sur Entrer pour finir

```

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:
>

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

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 LAN address has been set to 192.168.100.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.100.1/

Press <ENTER> to continue.■

```

On peut voir que l'adresse ip a bien été modifiée :

```

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)          -> em0           -> v4/DHCP4: 192.168.183.136/24
LAN (lan)          -> em1           -> v4: 192.168.100.1/24

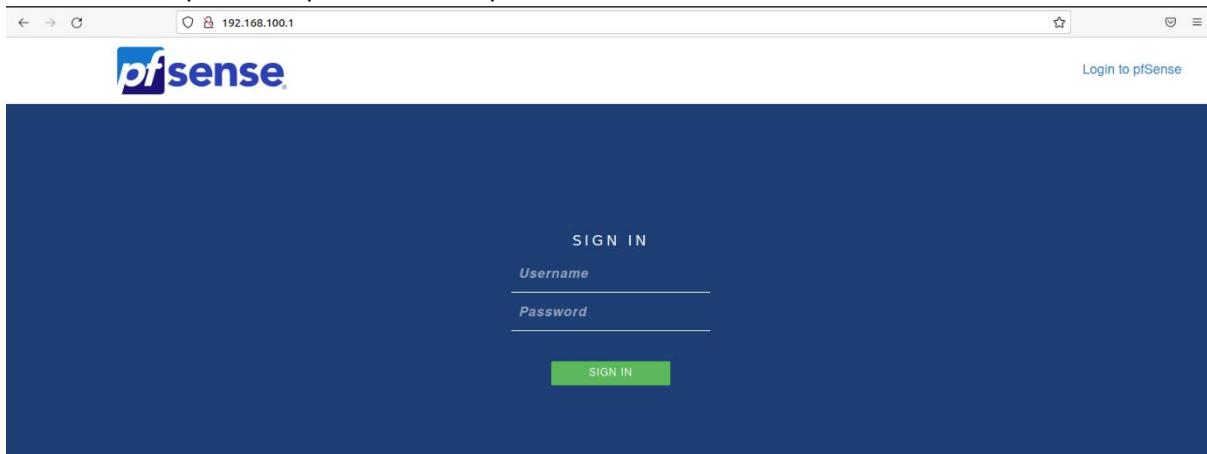
```

1.1.3 Configuration à partir d'une machine cliente

A partir de maintenant, nous utiliserons pfSense à partir de son interface Web.

Pour cela, il faut à partir d'une autre machine qui se trouve dans le même réseau LAN, taper dans un navigateur l'adresse ip de l'interface LAN de pfSense.

Une page d'authentification apparait. On rentre les identifiants, qui sont par défaut « admin » pour le username et « pfSense » pour le mot de passe :



On appuie sur « Next » :

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®

[Learn more](#)

» Next

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

» Next

On définit un nom d'hôte, un nom de domaine et 2 serveur DNS publiques :

General Information

On this screen the general pfSense parameters will be set.

Hostname	RTE-STG01
EXAMPLE: myserver	
Domain	CCI-CAMPUS.LAN
EXAMPLE: mydomain.com	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	1.1.1.1
Secondary DNS Server	1.0.0.1
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

» Next

Dans la partie « Time server hostname », on laisse le serveur par défaut et on sélectionne la timezone de Paris :

Time Server Information

Please enter the time, date and time zone.

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

Timezone: Europe/Paris

>> Next

Dans la configuration de l'interface WAN, on ne change rien. On fait attention que les 2 cases suivantes soient décochées.

La 1^{ère} case bloque sur l'interface WAN les adresses IP entrantes qui sont des adresses réservées pour les réseaux privés (10.x.x.x :8, 172.16.x.x/12 et 192.168.x.x :16). Cette option nous empêcherait de réaliser notre maquette, car notre interface WAN aurait certainement une adresse IP en 192.168.x.x.

La 2^e case bloque à la fois les adresses IP réservés aux réseaux privés, mais aussi les adresses IP bogon, c'est-à-dire les adresses non attribuées par l'IANA ou par les RIR. Ces adresses sont donc des adresses qui ne peuvent pas être routés sur internet, puisqu'elles ne sont pas distribuées par l'IANA.

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

Dans la configuration de l'interface LAN, on ne change rien :

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.100.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

On définit un mot de passe sécurisé :

Set Admin WebGUI Password

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

Admin Password:
Admin Password AGAIN:

>> Next

On appuie ensuite sur « Reload » puis sur « finish ». Le setup wizard est terminé.

On se rend System > Advanced. Ici nous allons passer du protocole HTTP au protocole HTTPS. Cela est important pour que nos données (surtout les données d'authentification qui comprennent le mot de passe) ne soient pas échangées en clair sur le réseau. Pour cela il faut simplement cocher la case « HTTPS (SSL/TLS) », et laisser le certificat SSL se généré tout seul :

The screenshot shows the pfSense web interface under 'System / Advanced / Admin Access'. The 'Admin Access' tab is selected. In the 'Protocol' section, the radio button for 'HTTPS (SSL/TLS)' is selected, while 'HTTP' is unselected. Below this, the 'SSL/TLS Certificate' dropdown is set to 'webConfigurator default (635ae72e6fcae)'. A note at the bottom states: 'Certificates known to be incompatible with use for HTTPS are not included in this list.'

A présent on peut voir qu'on accède bien à pfSense en HTTPS :

The screenshot shows a browser window with two tabs: 'RTE-STG01.CCI-CAMPUS' and 'RTE-MUL01.CCI-CAMPUS'. The active tab is 'RTE-MUL01.CCI-CAMPUS' and its URL is 'https://192.168.100.1/system_advanced_admin.php'. The page title is 'pfSense - COMMUNITY EDITION'. The navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

1.2 Routeur /pare-feu du site B

Il faut suivre exactement les mêmes étapes que pour le routeur du site A, en changeant les paramètres suivants :

- Il faut attribuer l'adresse IP LAN suivante : 192.168.200.1
- Il faut mettre l'interface LAN dans le réseau VMnet2
- Il faut donner le nom d'hôte suivant : RTE-MUL01

2 Création de la liaison VPN

2.1 Configuration de IPsec sur le site A

2.1.1 Configuration de la phase 1

Il faut d'abord créer un nouveau tunnel VPN. Pour cela, on se rend dans VPN > IPsec > Tunnels > Add P1 :

Voici les paramètres importants qu'il faut modifier :

Description : la description est facultative. On peut préciser qu'il s'agit du serveur VPN du site A

Key Exchange Protocol : IKEv2. Ce protocole est plus sûr, plus fiable et plus rapide que IKEv1

Internet Protocol : IPv4

Interface : WAN

Remote Gateway : 192.168.183.129 (il s'agit de l'interface WAN du serveur PfSense du site B). Il faut faire attention car dans le cadre de notre maquette l'adresse IP de l'interface WAN peut être amenée à changer (changement de réseau, durée du bail DHCP expirée, ...). Si l'adresse IP WAN change, il faudra renseigner la nouvelle adresse ici.

Authentification Method : Mutual PSK (l'authentification entre les 2 serveurs VPN se fera à l'aide d'une clé pré-partagée entre ces 2 serveurs)

My identifier : My IP address

Peer identifier : Peer IP Address

Pre-shared key : pour le serveur du site A : on génère une clé.
 pour le serveur du site B : on rentre la clé générée précédemment pour le site A

Encryption Algorithm : AES256, 128 bits, SHA 256, 14 (2048 bits)

Nous ne touchons pas aux paramètres qui suivent, à savoir les parties « Expiration and Replacement » et « Advanced Options ».

Désormais la phase 1 est configurée.

2.1.2 Configuration de la phase 2

Nous allons cliquer sur VPN > IPsec > Tunnels > Add P2 :

Voici les paramètres importants qu'il faut modifier :

Mode : Tunnel IPv4

Local Network : LAN subnet (pour que le site B accède au sous réseau du site A, donc le réseau 192.168.100.0)

NAT/BINAT : None

Remote network : Network et 192.168.200.0/24 (pour que le site A accède au réseau distant, celui du site B)

General Information

- Description**: serveur VPN du site A . phase 2
A description may be entered here for administrative reference (not parsed).
- Disabled**: Disable this phase 2 entry without removing it from the list.
- Mode**: Tunnel IPv4
- Phase 1**: serveur VPN du site A (IKE ID 1)

Networks

- Local Network**: LAN subnet / 0
Type: Local network component of this IPsec security association.
- NAT/BINAT translation**: None / 0
Type: If NAT/BINAT is required on this network specify the address to be translated
- Remote Network**: Network / 24
Type: Address: 192.168.200.0 / 24
Remote network component of this IPsec security association.

Protocol : ESP (car le protocole AH ne chiffre pas les données)

Encryption Algorithm : AES256 et 128 bits

Phase 2 Proposal (SA/Key Exchange)

Protocol	ESP	Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.
Encryption Algorithms	<input type="checkbox"/> AES <input type="checkbox"/> AES128-GCM <input type="checkbox"/> AES192-GCM <input checked="" type="checkbox"/> AES256-GCM <input type="checkbox"/> Blowfish <input type="checkbox"/> 3DES	<input type="button" value="Auto"/> <input type="button" value="Auto"/> <input type="button" value="Auto"/> <input type="button" value="128 bits"/> <input type="button" value="Auto"/> <input type="button" value="Auto"/>

Automatically ping host : 192.168.200.1 (nous mettons l'adresse ip du serveur pfSense distant). Ce paramètre envoie un paquet ICMP à l'adresse IP renseignée. Si le paquet ICMP n'obtient pas de réponse, pfSense va tenter d'initialiser à nouveau la phase 2 du tunnel VPN.

Keep alive : on coche la case seulement pour un des 2 sites. Ce paramètre va vérifier régulièrement si liaison VPN est toujours active ou non, et l'initialiser si elle n'est plus active.

Keep Alive

- Automatically ping host**: 192.168.200.1
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.
- Keep Alive**: Enable periodic keep alive check
Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel mode P2 entries. For IKEv2 without split connections, this only needs enabled on one P2.

Il ne faut pas oublier d'appliquer les changements :

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

2.2 Configuration de IPsec sur le site B

La configuration du serveur VPN du Site B est la même que pour le site A, avec seulement les paramètres suivants qui changent :

Dans la phase 1 :

Remote Gateway : 192.168.183.128 (on met l'adresse du serveur VPN du site A et non du site B)

Pre-Shared Key : on ne génère pas une clé, mais on copie celle qui a déjà été générée.

Dans la phase 2 :

Remote Network : 192.168.100.0 /24

Automatically ping host : 192.168.100.1

Keep alive : attention à ne l'activer que sur un des deux serveurs (l'activer sur les 2 serveurs enverraient sur le réseau des trames inutiles)

2.3 Test de la liaison VPN

Pour vérifier que la connexion VPN est bien active on peut se rendre dans Status > IPsec. On voit que la liaison est bien active :

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #2	serveur VPN du site A	ID: 192.168.183.136 Host: 192.168.183.136:500 SPI: f67b1feac456bee9	ID: 192.168.183.137 Host: 192.168.183.137:500 SPI: db7a795b13f75ac7	IKEV2 Responder	Rekey: 25205s (07:00:05) Reauth: Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	Established 183 seconds (00:03:03) ago
Disconnect P1							
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1 #2	serveur VPN du site A . phase 2	192.168.100.0/24 Local: c3d3c49a Remote: c9983044	192.168.200.0/24	Rekey: 2835s (00:47:15) Life: 3417s (00:56:57) Install: 183s (00:03:03)	AES_GCM_16 (256) IPComp: None	Bytes-In: 252 (252 B) Packets-In: 3 Bytes-Out: 560 (560 B) Packets-Out: 4	Installed Disconnect P2

2.4 Règles du pare-feu

2.4.1 Création d'alias

Nous allons créer 2 alias, qui seront utiliser pour les règles de pare-feu ci-dessous. Pour cela on se rend dans Firewall > Aliases

Le 1^{er} va regrouper les adresses réseau de nos deux réseaux LAN :

Properties							
Name	2_reseaux_lan						
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".							
Description							
Type	Network(s)						
Network(s)							
Hint	Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.						
Network or FQDN	192.168.100.0	/	24	/	LAN Site A	Delete	
	192.168.200.0	/	24	/	LAN Site B	Delete	

Le 2^e alias va regrouper les 3 ports nécessaires pour un accès WEB (http, HTTPS et DNS) :

Properties

Name	acces_web	The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and _'.	
Description	DNS, HTTP et HTTPS	A description may be entered here for administrative reference (not parsed).	
Type	Port(s)		
Port(s)			
Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.		
Port	53	DNS	Delete
	80	HTTP	Delete
	443	HTTPS	Delete

2.4.2 Interface WAN

Ici on bloque tout le trafic (tous les ports et tous les protocoles en IPv4 et IPv6) venant de l'interface WAN. C'est-à-dire que rien venant d'internet n'est autorisé à entrer sur le LAN, à part si la demande a été initiée par une machine du LAN (avec une règle de pare-feu accès web sur l'interface LAN) :

Floating WAN **LAN** IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /29 KIB	IPv4+6 *	*	*	*	*	*	none		Bloque tout sur le WAN	

Add Add Save

2.4.3 Interface LAN

On va créer 4 règles. La 1^{ère} pour autoriser tout le trafic TCP/UDP en IPv4 entre les LAN du site A et du site B. La 2^e pour autoriser l'accès vers les sites internet. La 3^e pour autoriser le protocole ICMPv4 entre les 2 LAN. Et la dernière règle pour bloquer tout le trafic :

Floating **WAN** LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 1 /9.19 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 28 /72.30 MiB	IPv4 *	2_reseaux_lan	*	2_reseaux_lan	*	*	none		Autorise tout entre les 2 LAN	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 2 /1.07 GiB	IPv4 TCP/UDP	LAN net	*	*	acces_web	*	none		Autorise Acces WEB	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 ICMP	2_reseaux_lan	*	2_reseaux_lan	*	*	none		Autorise ICMPv4 entre les 2 LAN	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 0 /225 KIB	IPv4+6 *	*	*	*	*	*	none		Bloque tout le trafic	

Add Add Save

2.4.4 Interface IPsec

On va créer 3 règles. La 1^{ère} pour autoriser tout le trafic TCP/UDP en IPv4 entre les LAN du site A et du site B. La 2^e pour autoriser le protocole ICMPv4 entre les 2 LAN. Et la dernière règle pour bloquer

tout le trafic.

The screenshot shows a network configuration interface with a tab bar at the top: Floating, WAN, LAN, and IPsec. The IPsec tab is selected, indicated by a red underline. Below the tabs is a table titled "Rules (Drag to Change Order)".

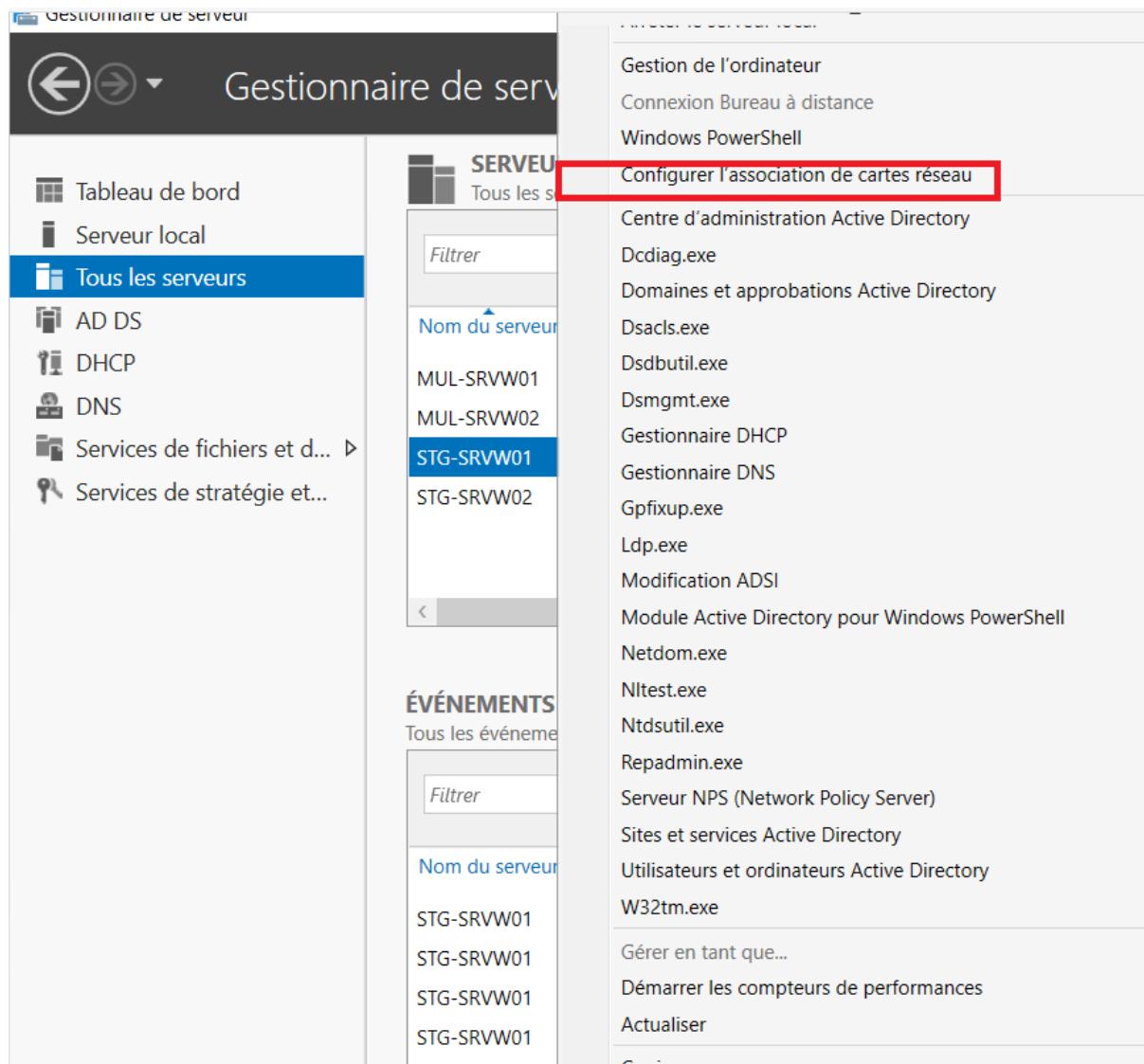
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 6.91 MiB	IPv4 *	2_reseaux_lan	*	2_reseaux_lan	*	*	none		Autorise tout entre les 2 LAN	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any	2_reseaux_lan	*	2_reseaux_lan	*	*	none		Autorise ICMP entre les 2 LAN	
<input type="checkbox"/>	✗ 0 / 155 KiB	IPv4+6 *	*	*	*	*	*	none		Bloque tout le traffic IPv4 + IPv6	

At the bottom right of the table are several buttons: Add, Add, Delete, Save, and Separator.

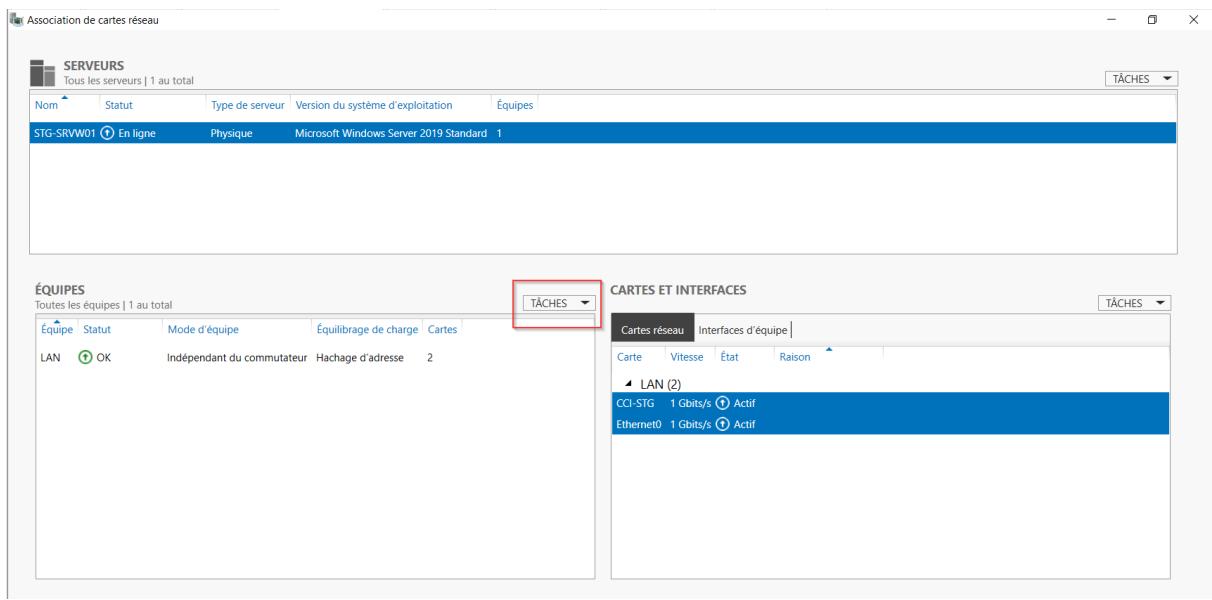
3 Installation et configuration des serveurs Windows

3.1 Configuration de l'IP Bonding

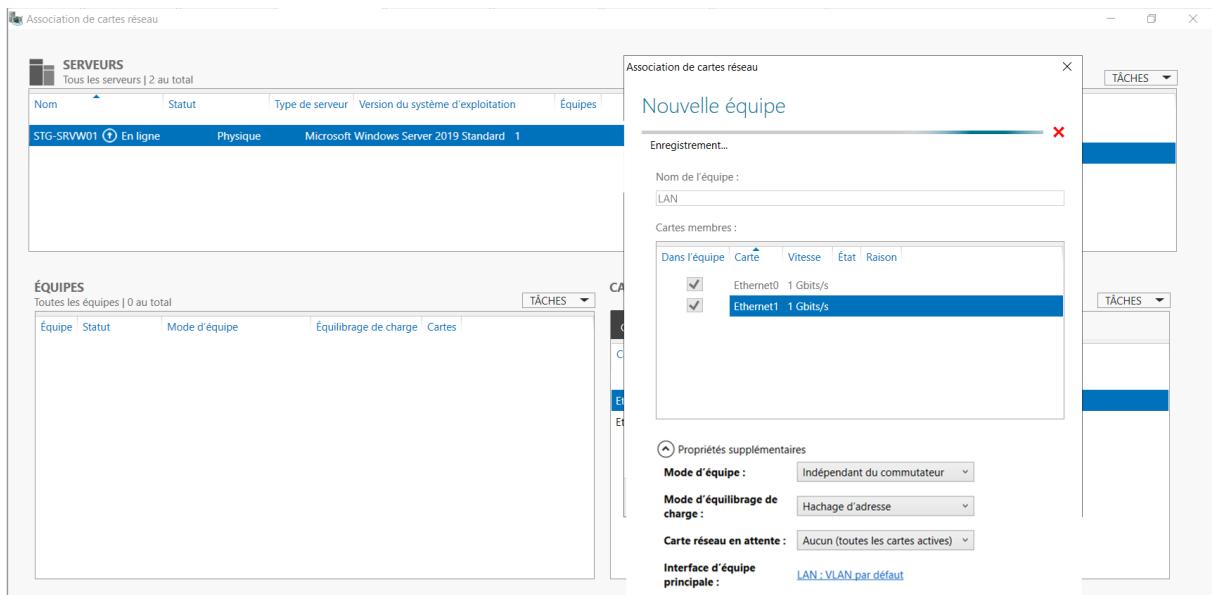
On effectue un clic droit sur le serveur auquel on souhaite configurer l'association de cartes réseaux :



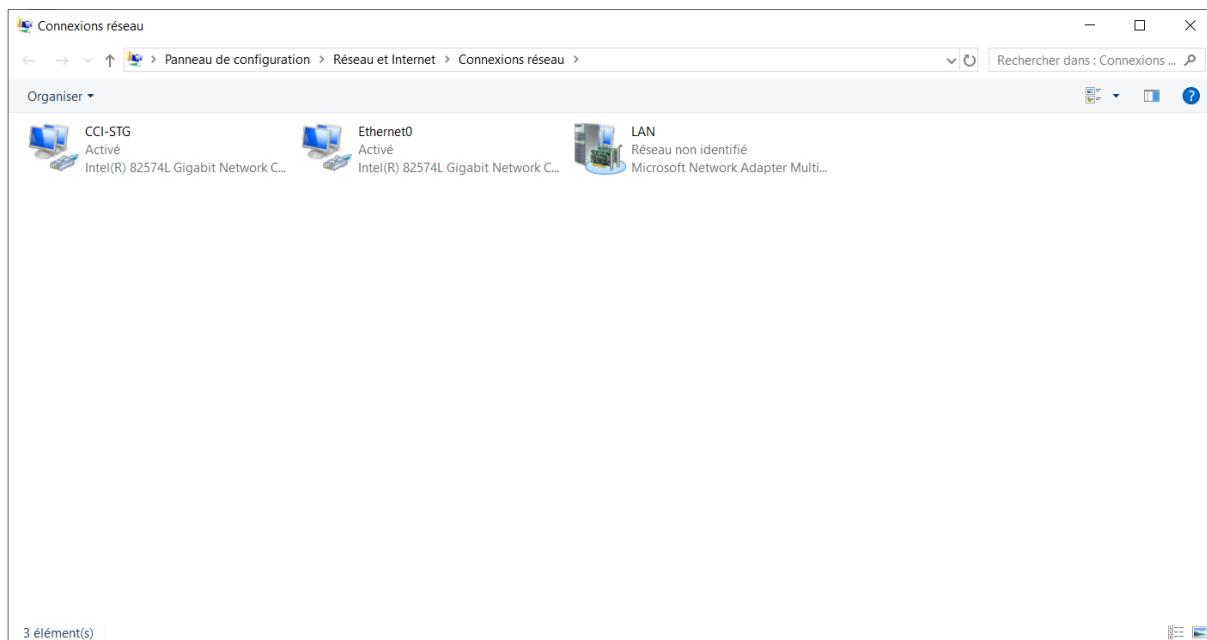
On se dirige vers les « Tâches » et on clique sur « Nouvelle équipe »



On sélectionne les deux cartes et on choisit les propriétés suivantes :



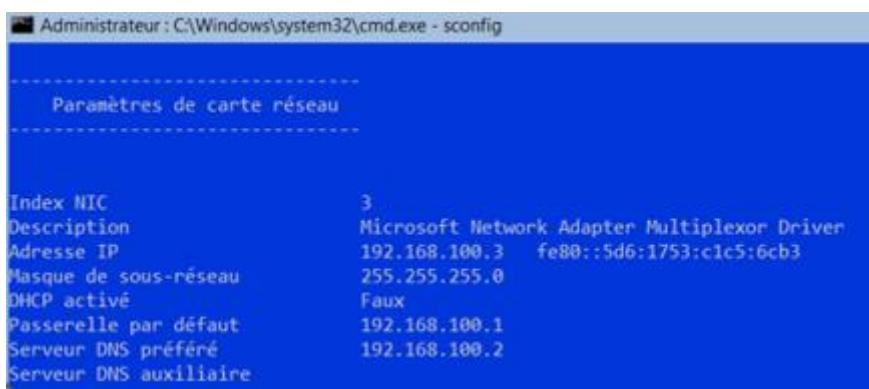
On remarque que l'association de cartes a bien faite.



On la retrouve également sur Strasbourg :

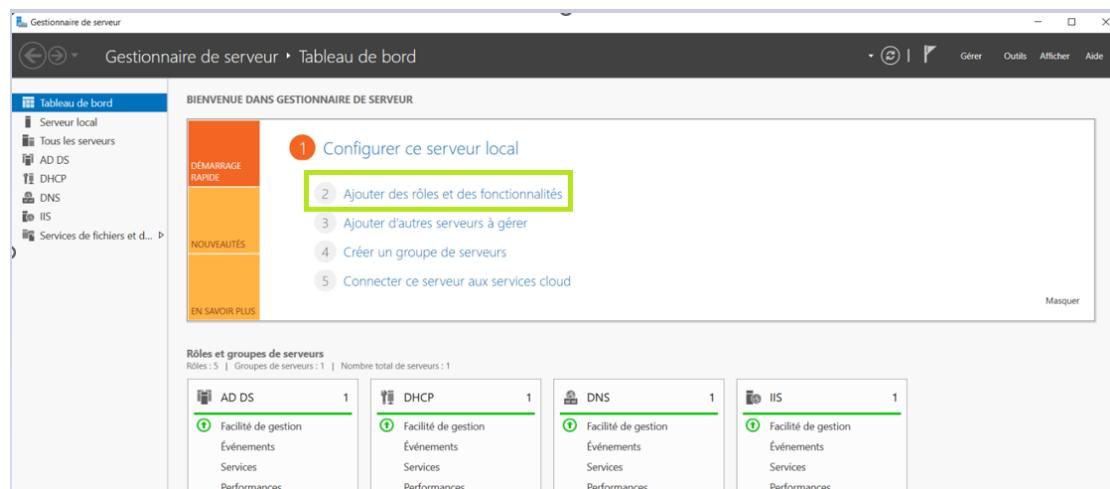
- Index NIC = 3

Cela indique que c'est la troisième carte réseau et par conséquent le LAN



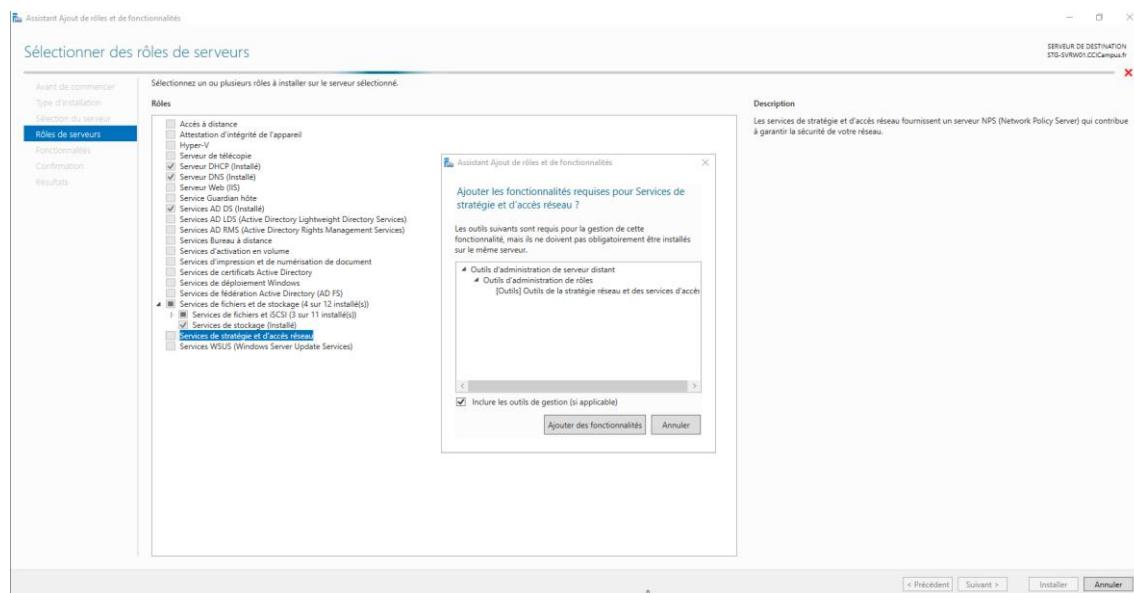
3.2 Installation des rôles et fonctionnalités

Pour éviter de se répéter, nous allons installer tous les rôles en une manipulation. Pour cela, cliquer sur « Ajouter des rôles et des fonctionnalités ». Cela sera fait sur tous les serveurs.

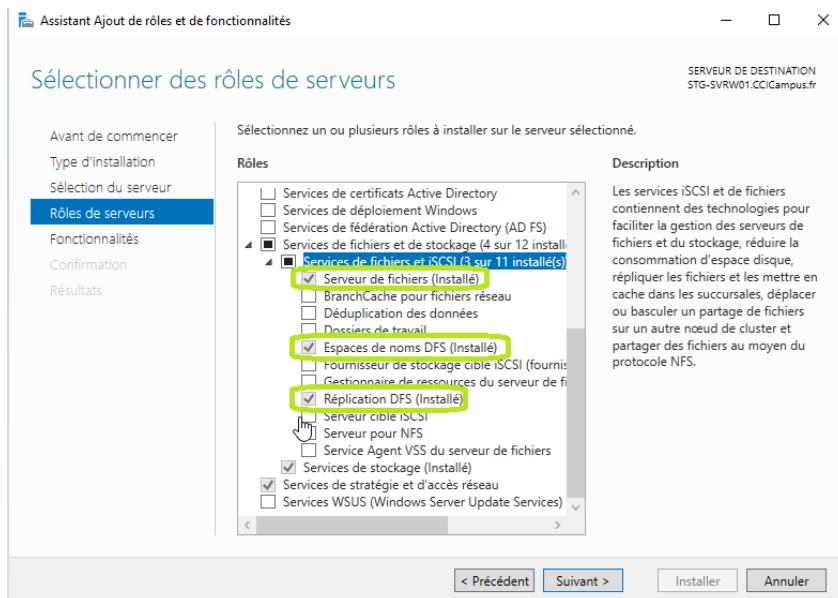


Puis installer les rôles suivants :

- **DHCP**
- **DNS**
- **ADDS**
- **Services de fichiers (DFS + DFSR)**
- **Services de stratégie et d'accès réseau (RADeUS)**



Une fois tous les rôles et services installés, nous pouvons débuter leur configuration.



3.3 Mise en place de l'ADDS

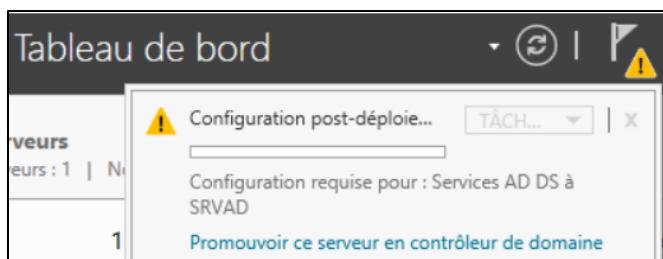
Avant de lister les différentes étapes pour mettre en place l'AD, il est primordial de souligner que dans notre cas nous aurons un seul domaine : CCI-CAMPUS.LAN. De plus, le site de Strasbourg possèdera le contrôleur de domaine principal. A savoir que le deuxième serveur de Strasbourg et les deux serveurs du site de Mulhouse seront également des contrôleurs de domaines. Au total, nous en aurons quatre.

Par ailleurs, il faut tout aussi bien préciser qu'avant de pouvoir ajouter le site de Mulhouse en tant que contrôleur de domaine, il faut mettre en place un VPN site à site qui permettra aux deux sites de communiquer entre-eux.

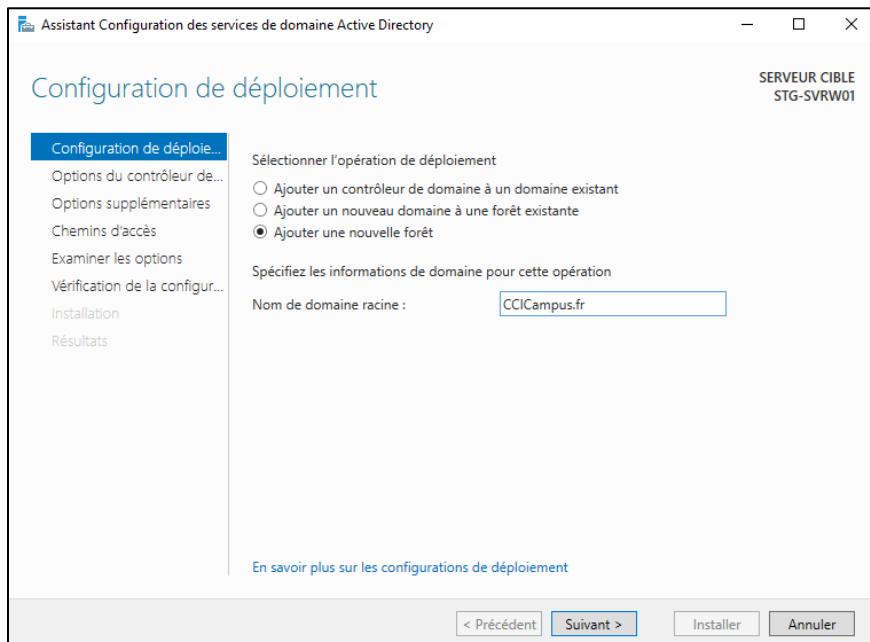
Commençons par configurer l'Active Directory :

Dans les images qui vont suivre le domaine se nommera : CCICAMPUS.FR. Retenez que **cette appellation n'a été utilisé que pour le prototype de ce projet et qu'en réalité le nom de domaine sera bien : CCI-CAMPUS.LAN.**

Une fois les rôles installés, vous aurez une icône « attention » qui vous informera que vous devez effectuer une configuration de l'AD. C'est-à-dire, la créer. Cliquer sur « Promouvoir ce serveur en contrôleur de domaine » :

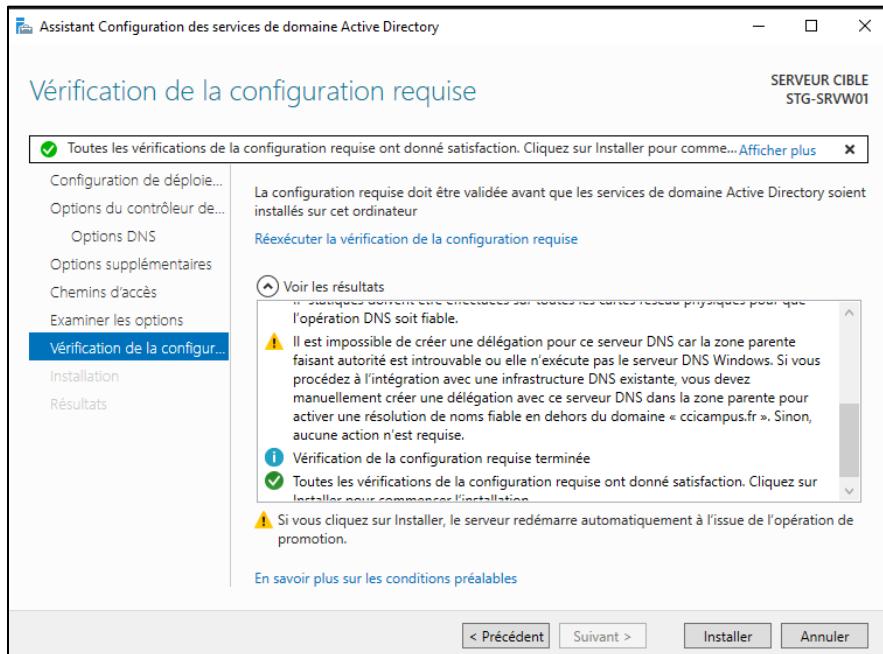


Ensuite, sélectionner « Ajouter une nouvelle forêt » et renseigner le nom de domaine :



Puis on informe le mot de passe du compte (Administrateur) :

Si tout est correcte, l'AD pourra être installer :



3.3.1 Installation et ajout des contrôleurs de domaine

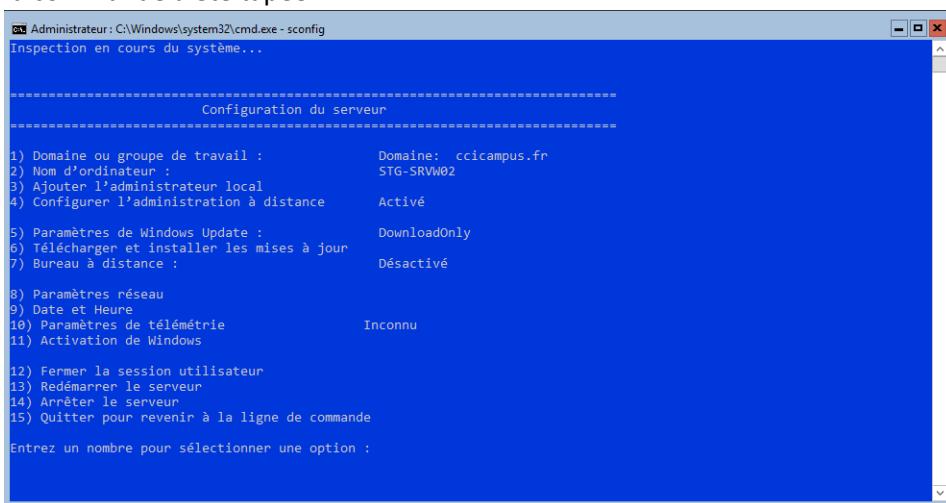
Comme évoqué plus haut, nous avons trois autres contrôleurs à ajouter. Nous allons suivre avec le second serveur windows du site de Strasbourg. Etant un serveur core, l'ajout dans le domaine sera fait en ligne de commandes. Cependant, une fois dans le domaine nous pourrons l'ajouter dans les serveurs du serveur principal de Strasbourg et le gérer à partir de là.

3.3.1.1 STG-SRVW02 :

La commande nous permettant de configurer le serveur :



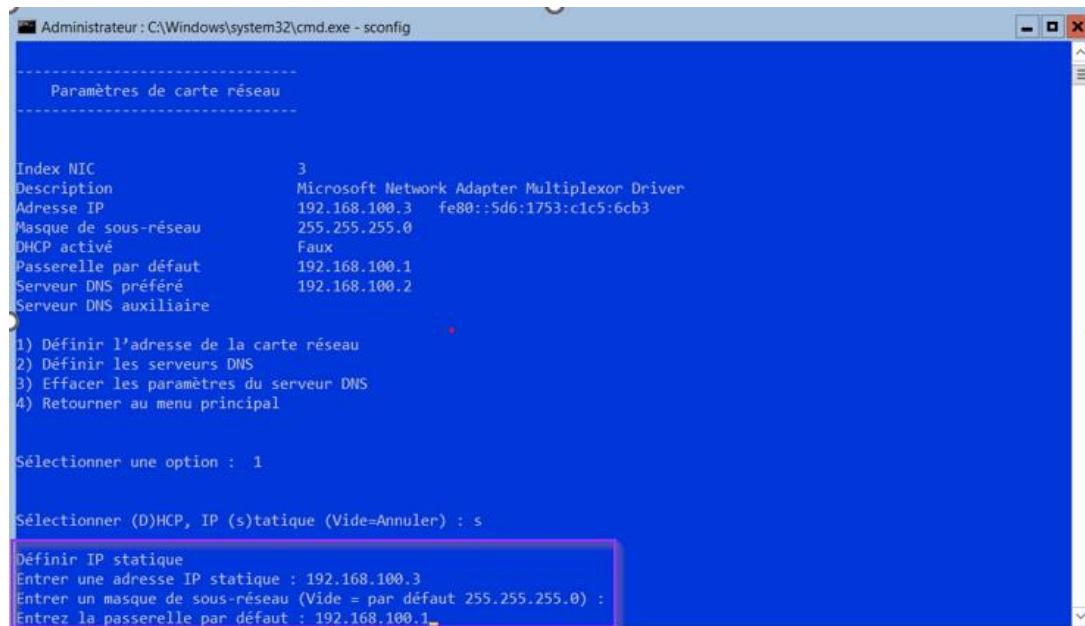
Ici on remarque que le serveur est déjà dans le domaine mais voici l'interface qui s'ouvrira après que la commande a été tapée :



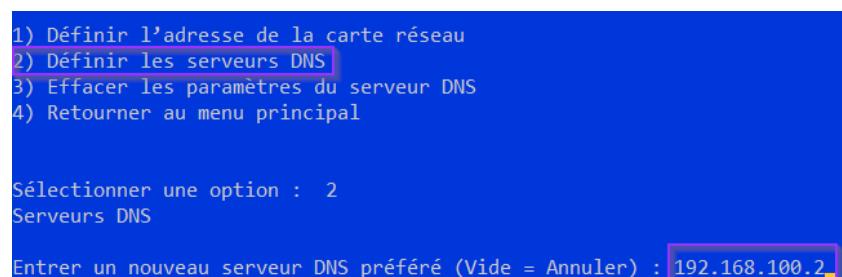
Nous allons modifier les paramètres réseaux (8) et on choisit la carte réseau que nous souhaitons modifier :

Cartes réseau disponibles		
Index#	Adresse IP	Description
1	192.168.100.3	Intel(R) 82574L Gigabit Network Connection
Sélectionner Index# de la carte réseau (Vide=Annuler) :		

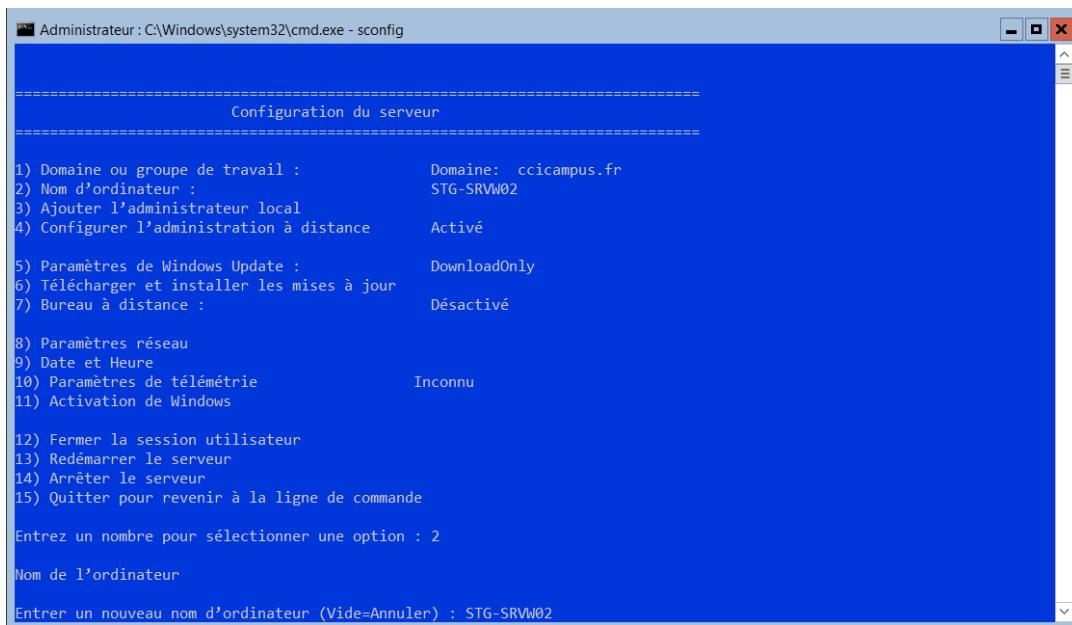
On informe les informations suivantes :



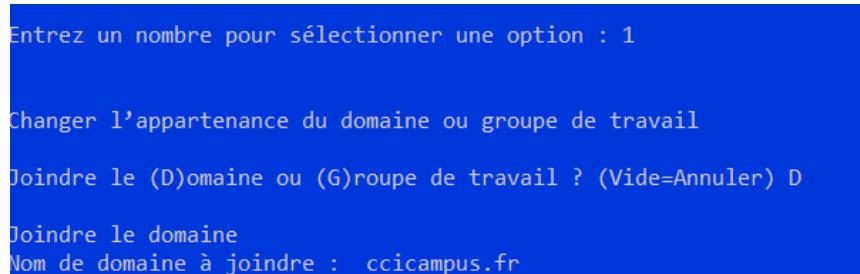
On indique ensuite le DNS qui fera référence au serveur principal :



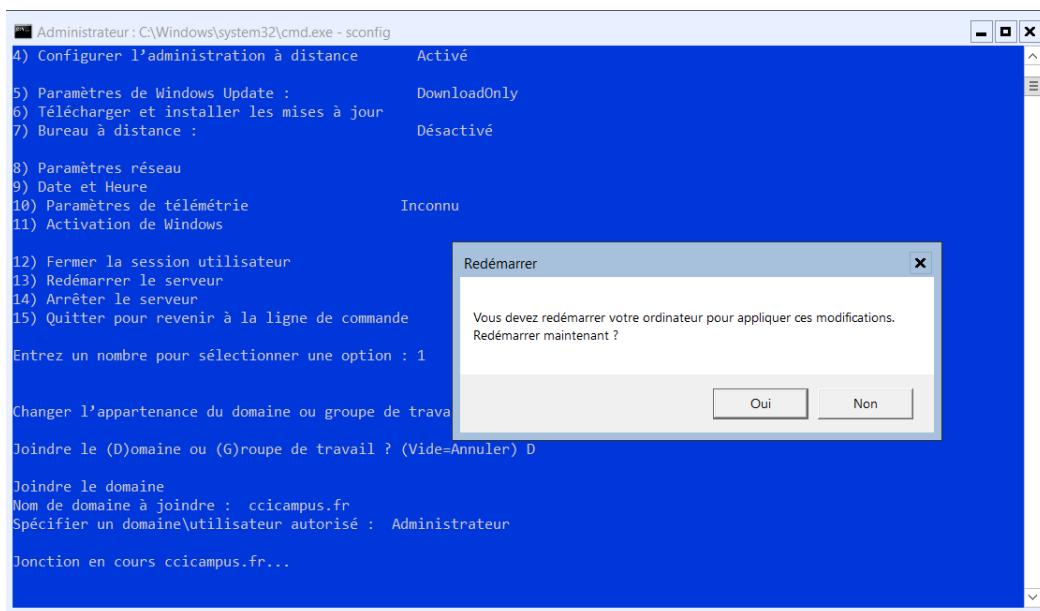
Puis on retourne au menu principal et on change le nom de l'ordinateur (2) :



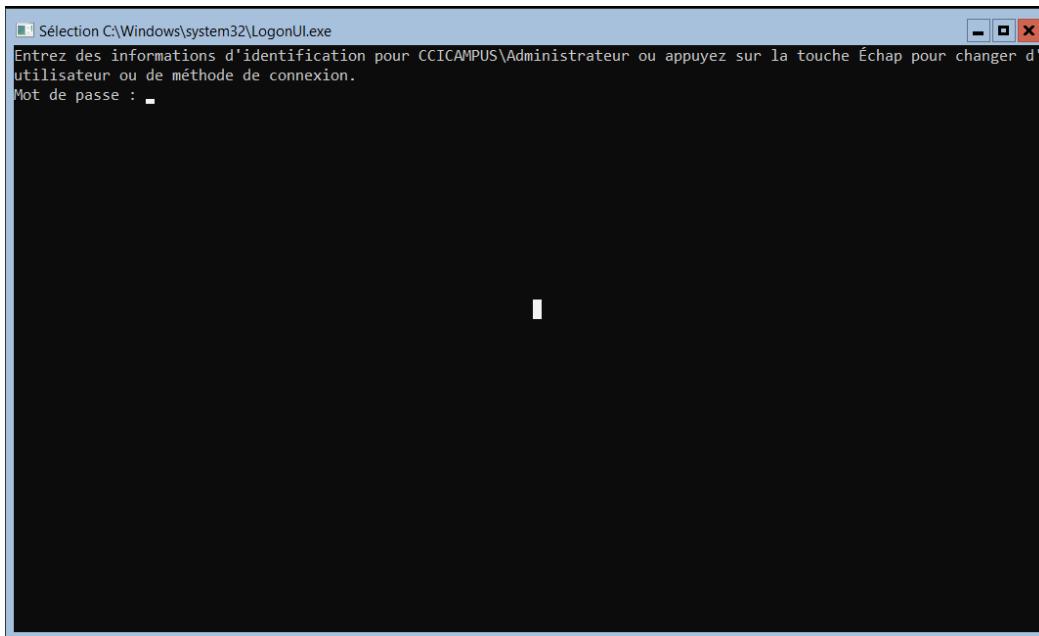
Puis on termine par l'ajout du domaine :



Avec les informations d'un utilisateur, le mieux c'est l'Administrateur :



Une fois qu'il aura redémarrer, il vous demandera les informations d'authentification d'un utilisateur du domaine.



Penser à désactiver le pare-feu :

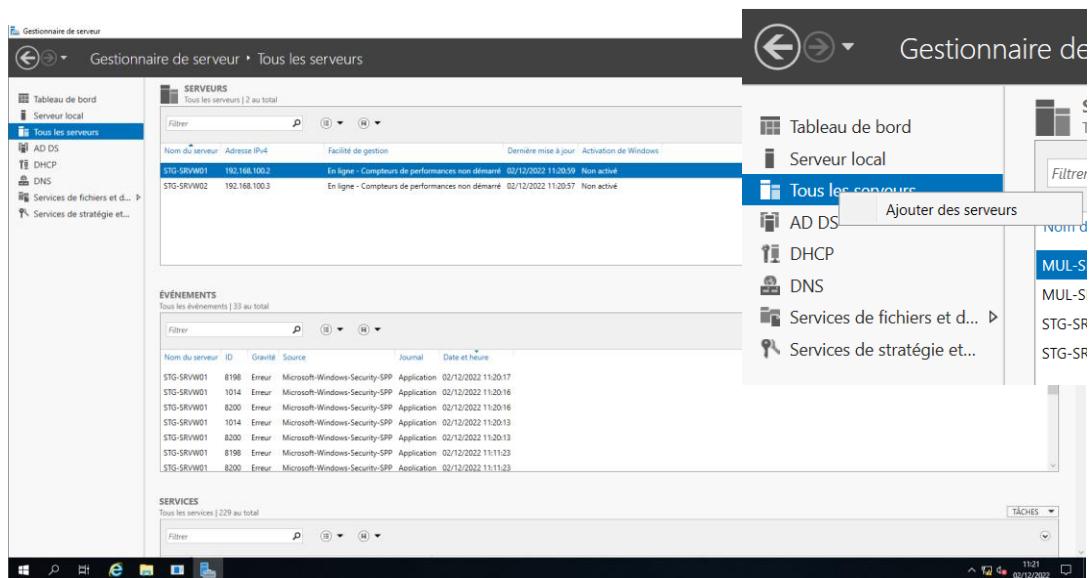
```

Administrator: C:\Windows\system32\cmd.exe - powershell
C:\Users\Admin>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

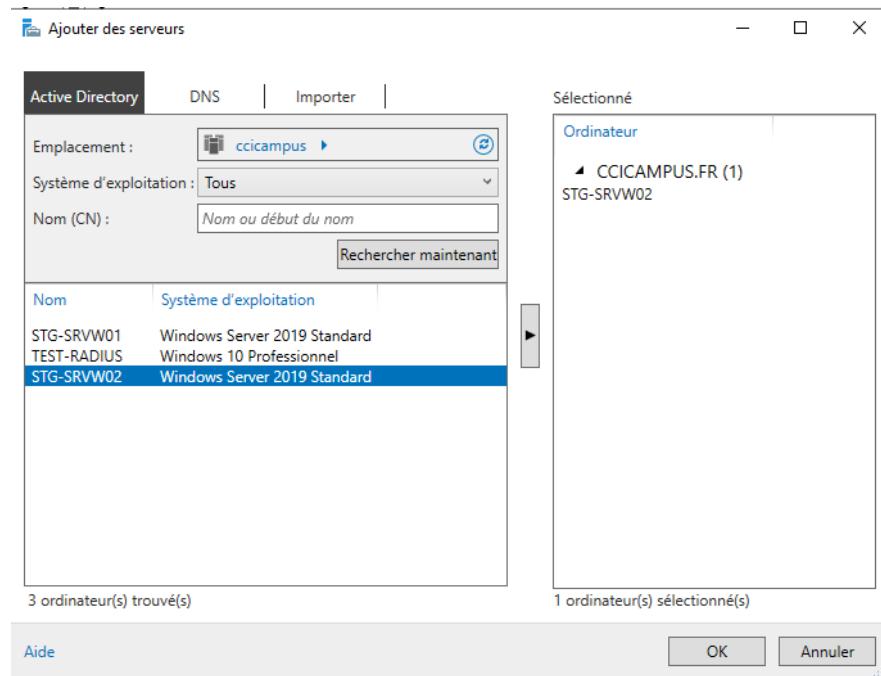
PS C:\Users\Admin> Set-NetFirewallProfile -Profile * -Enabled false
PS C:\Users\Admin>

```

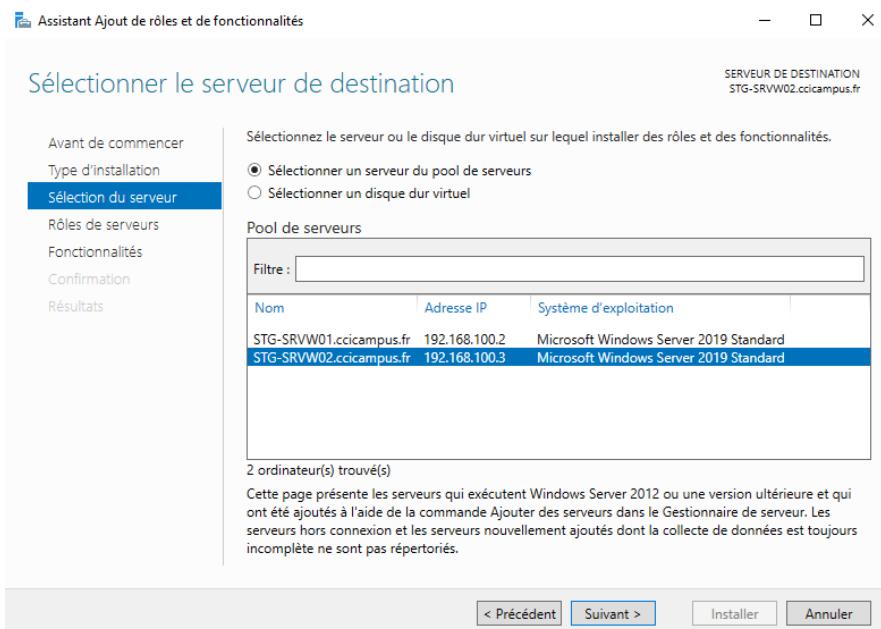
Maintenant nous pouvons l'ajouter à la liste des serveurs du serveur principal :



On recherche le serveur et on clique sur la flèche du milieu pour l'ajouter puis sur « ok »

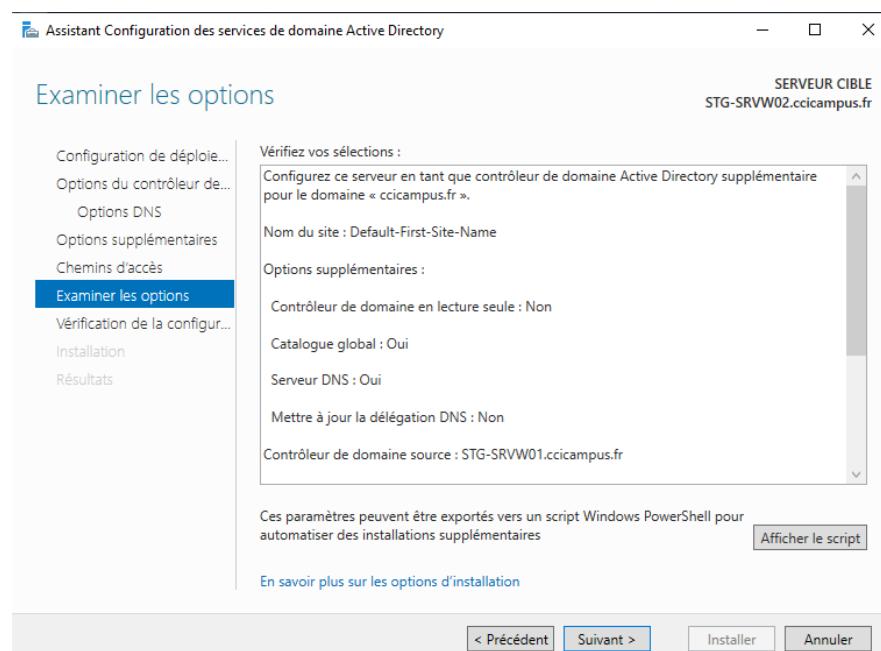
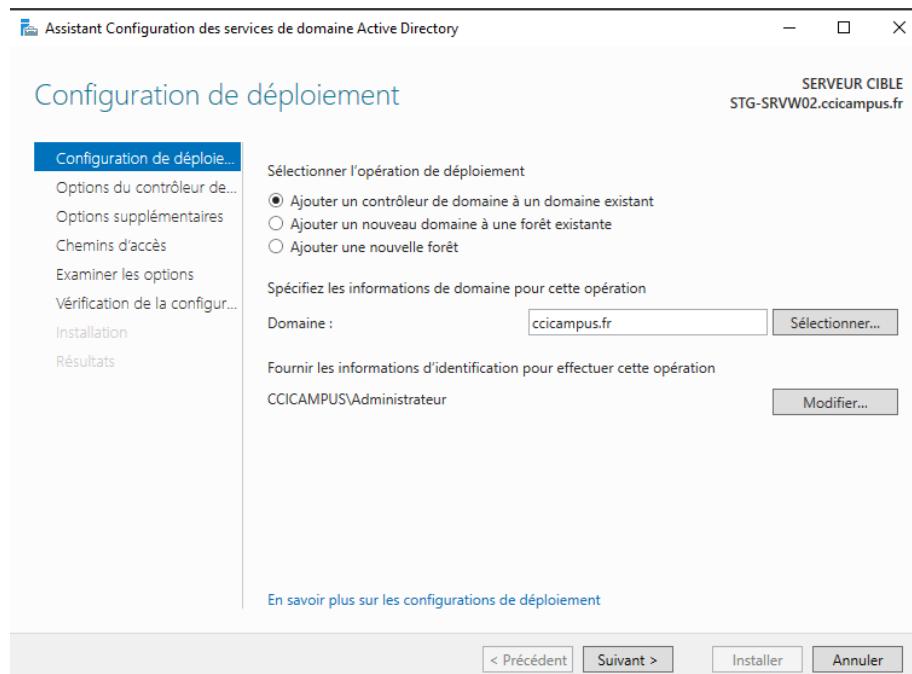


De là, nous pouvons procéder à la même manière qu'au grand 1 de cette partie en ajoutant les mêmes fonctionnalités.

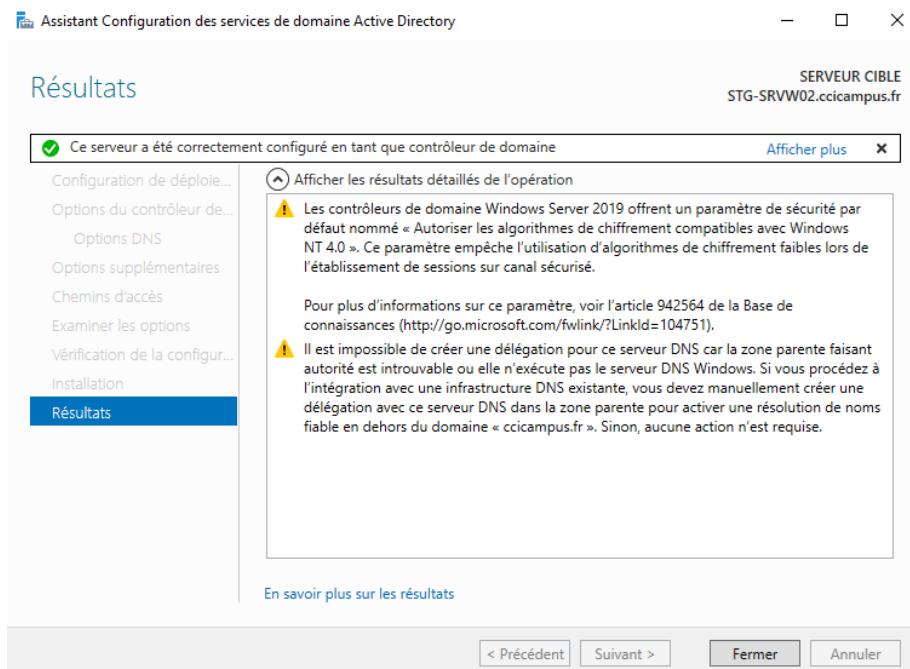


Lorsque les rôles ont été installés, il nous suffit de configurer l'AD du second serveur :

- On choisit « Ajouter un contrôleur de domaine à un domaine existant »
- On informe le domaine
- On indique les identifiants de l'administrateur du domaine pour s'y connecter

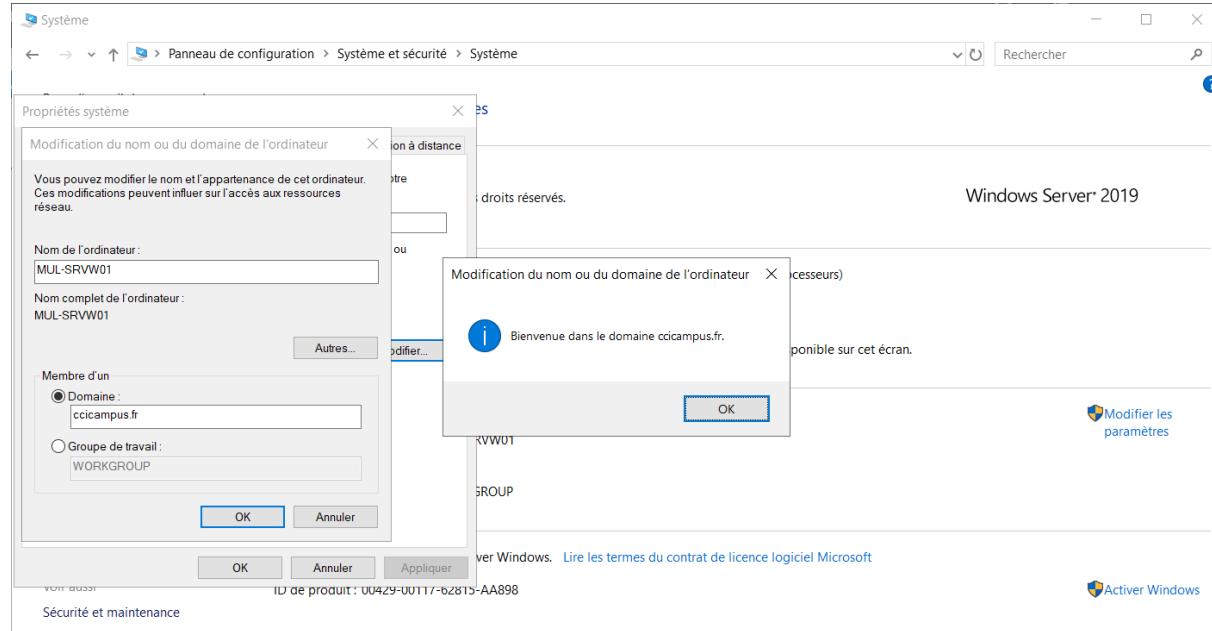


Voilà le deuxième contrôleur de domaine a été ajouté :

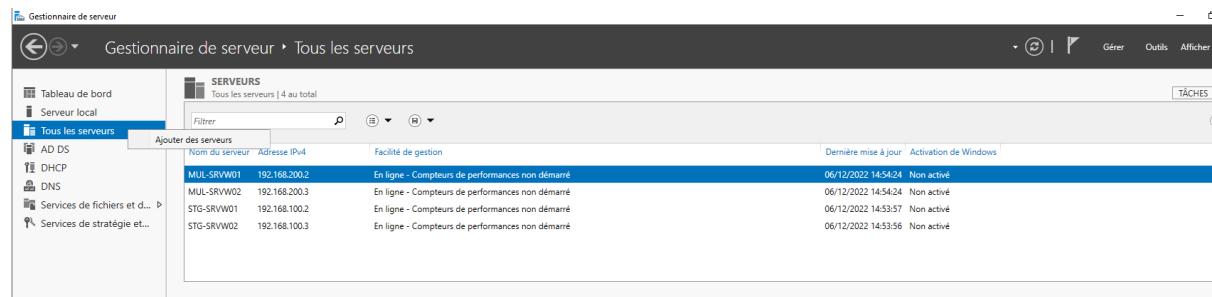


3.3.1.2 MUL-SRVW01 :

Continuons avec les serveurs du site de Mulhouse. Le premier serveur dispose d'une interface graphique et communique déjà avec le site de Strasbourg grâce au VPN. Nous avons juste besoin de l'ajouter dans le domaine :

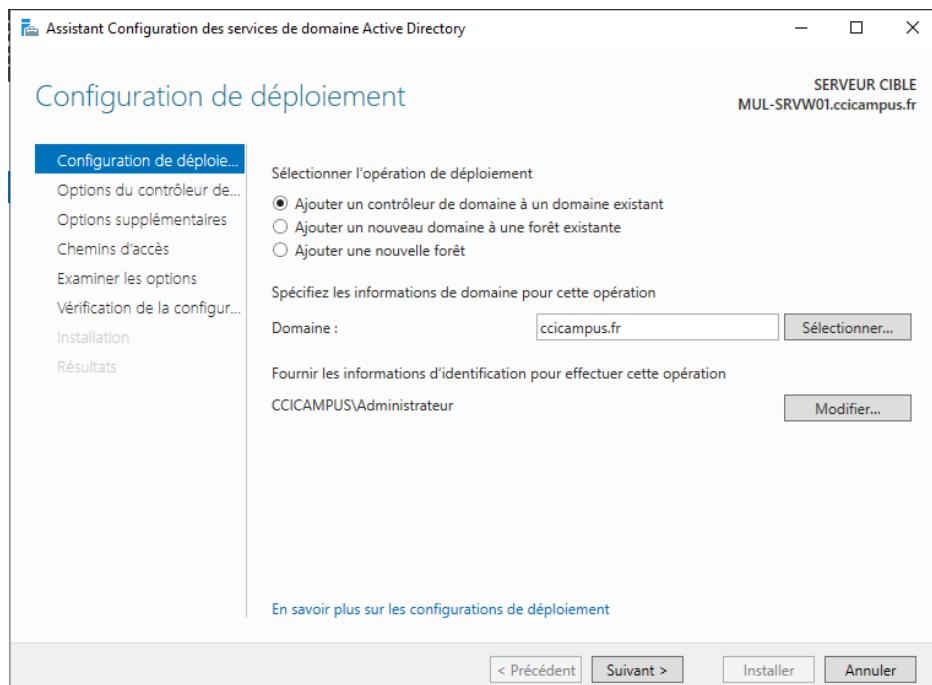


A partir d'ici, on peut l'ajouter dans la liste des serveurs du serveur principal :

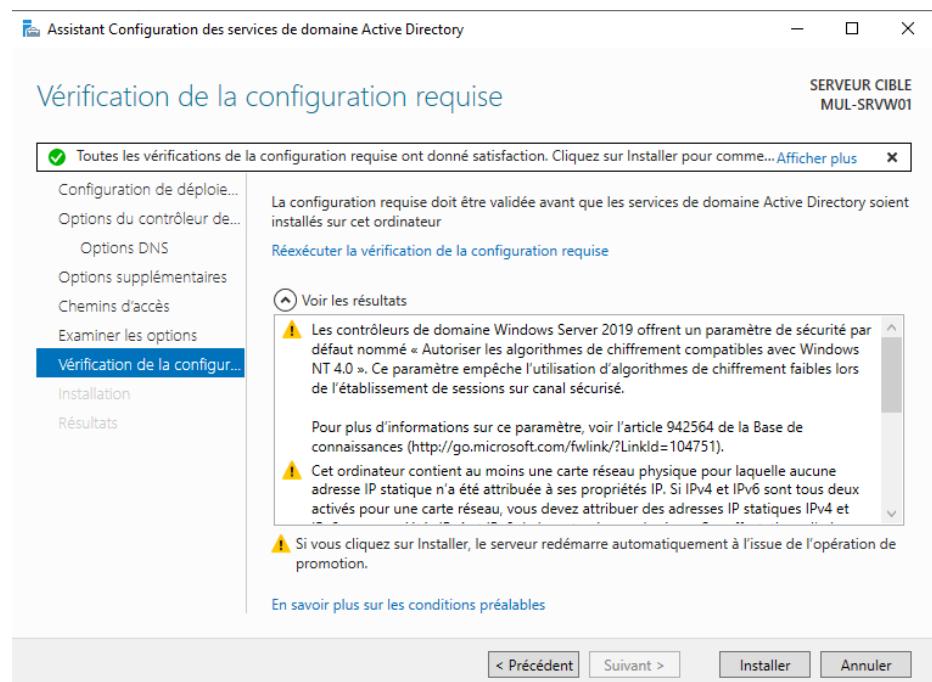


Puis nous pouvons y configurer le serveur : ajout des rôles et l'ajouter en tant que contrôleur de domaine.

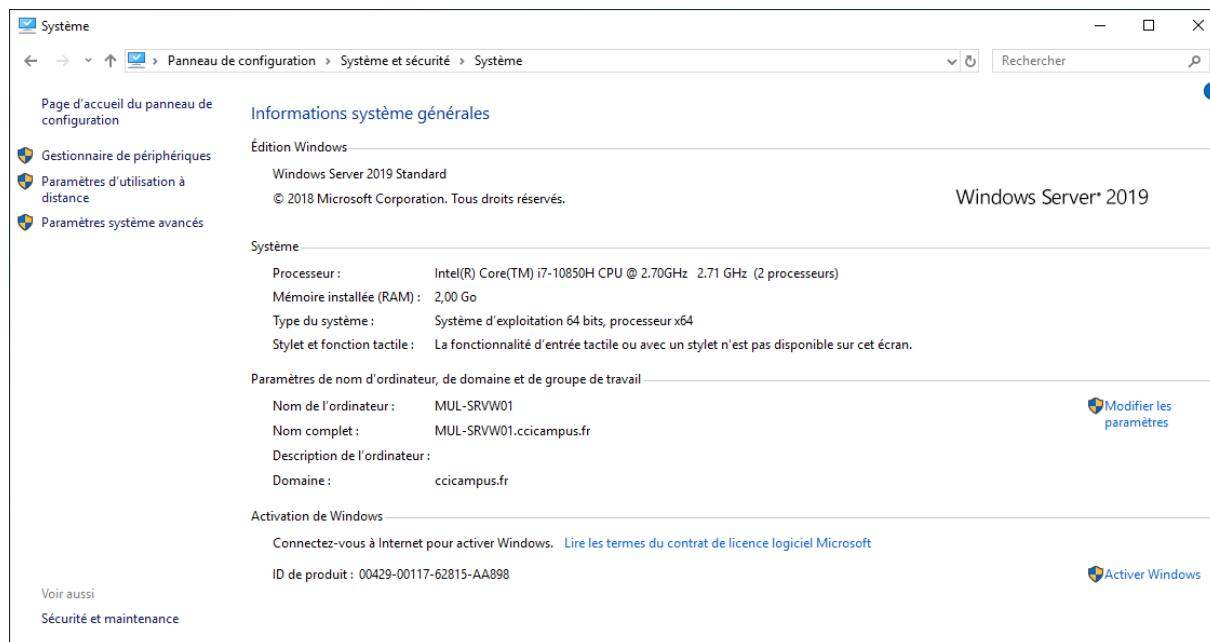
Une fois les rôles installés, on procède comme pour le second serveur :



Le troisième contrôleur de domaine a été ajouté :

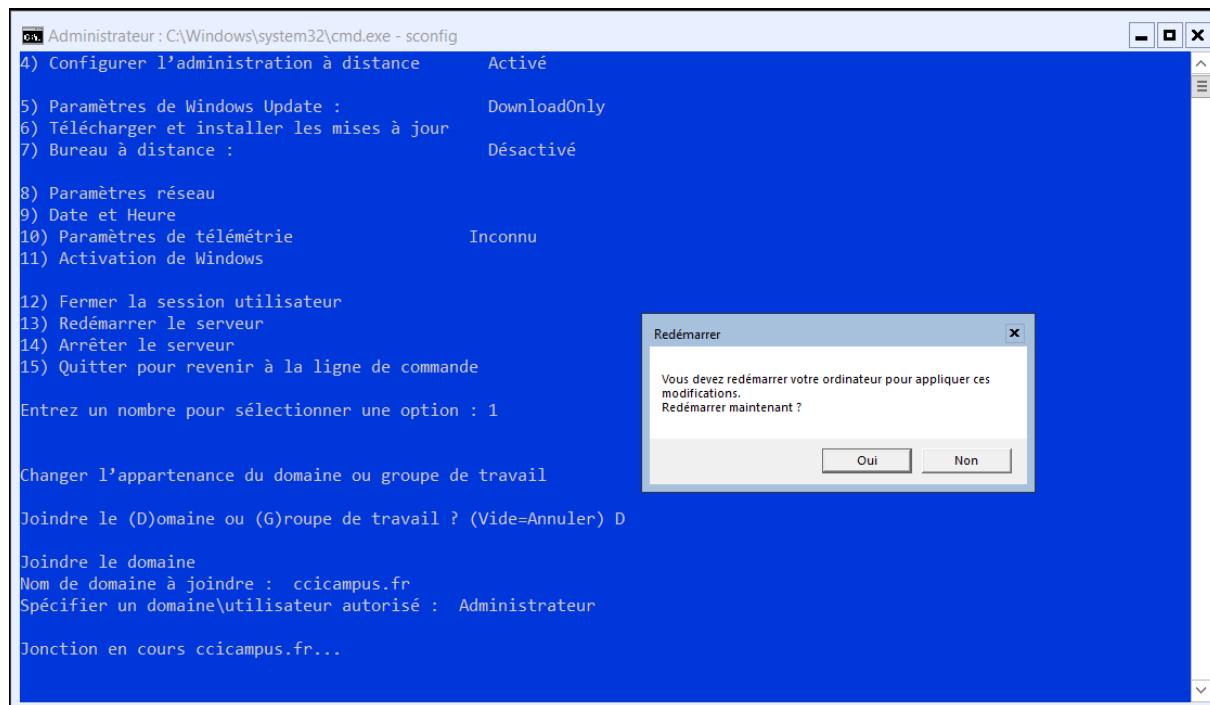


Il est bien dans le domaine :

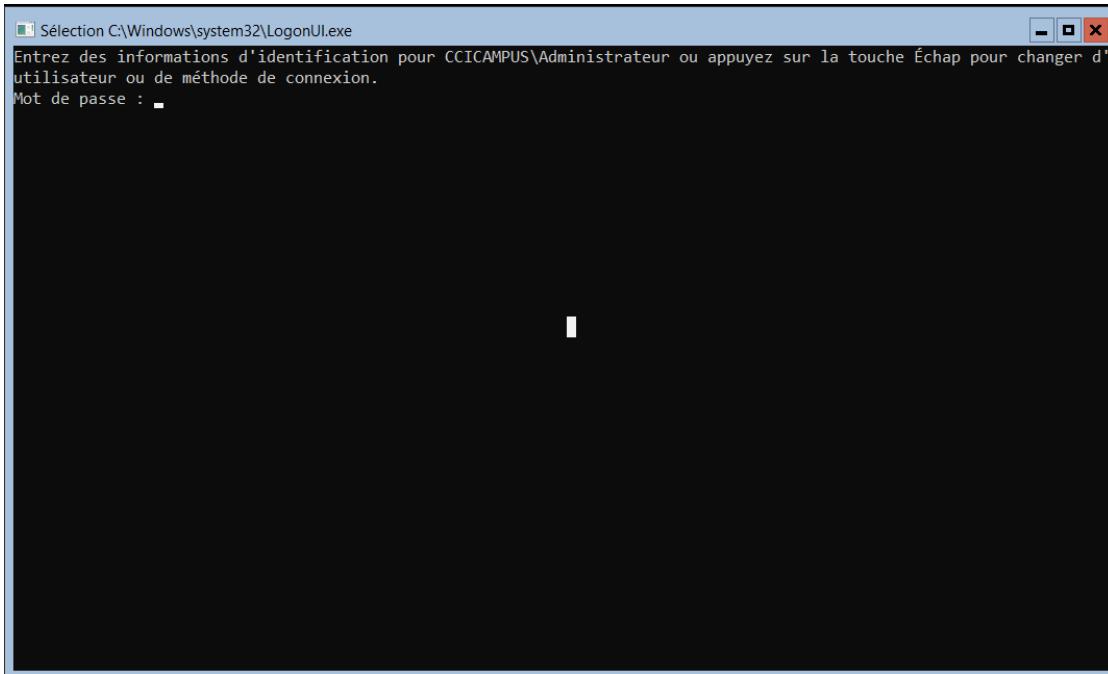


3.3.1.3 MUL-SRVW02 :

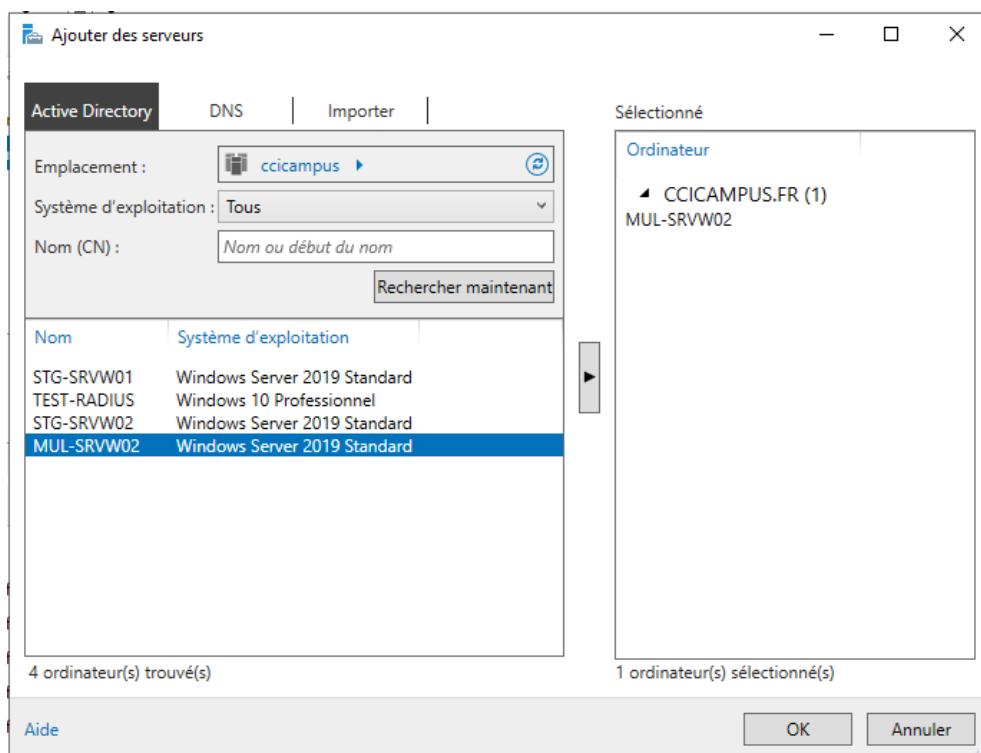
Etant aussi un serveur core, la procédure sera la même que pour le second serveur de Strasbourg sauf pour l'adressage IP et le nom de l'ordinateur bien évidemment.



Comme pour le STG-SRVW02, il vous demandera des identifiants d'un utilisateur du domaine. Cela prouve bien qu'il y est inscrit.



Ajoutons-le à la liste du serveur principal et ajoutons les rôles nécessaires pour ensuite l'ajouter en tant que quatrième contrôleur de domaine.



The screenshot shows the 'All servers' list in the Server Manager. There are four servers listed:

Nom du serveur	Adresse IPv4	Etat	Dernière mise à jour	Activation de Windows
MUL-SRVW01	192.168.200.2	En ligne - Compteurs de performances non démarré	06/12/2022 14:54:24	Non active
MUL-SRVW02	192.168.200.3	En ligne - Compteurs de performances non démarré	06/12/2022 14:54:24	Non active
STG-SRVW01	192.168.100.2	En ligne - Compteurs de performances non démarré	06/12/2022 14:53:57	Non active
STG-SRVW02	192.168.100.3	En ligne - Compteurs de performances non démarré	06/12/2022 14:53:56	Non actif

A nouveau, nous allons procéder, comme pour les autres serveurs, à la configuration du rôle AD :

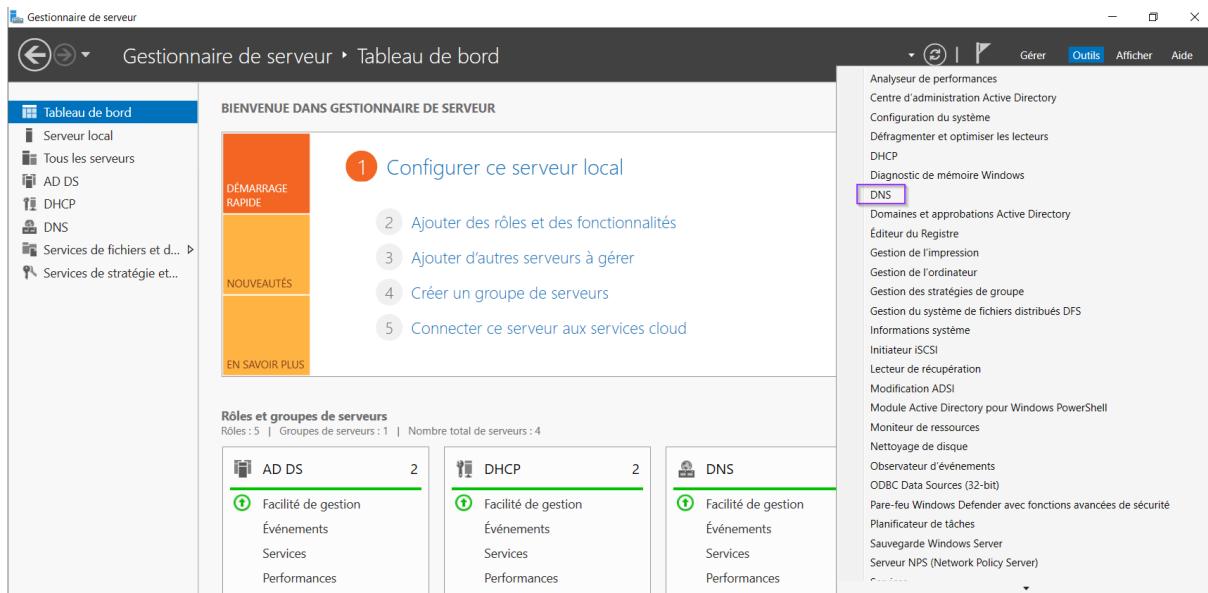
The screenshot shows the 'Deployment Configuration' step of the Active Directory Domain Services configuration wizard. It is configured to add a domain controller to an existing domain ('Ajouter un contrôleur de domaine à un domaine existant'). The target server is MUL-SRVW02.ccicampus.fr. The domain is ccicampus.fr, and the administrator is CCICAMPUS\Administrateur.

Et voilà notre quatrième contrôleur :

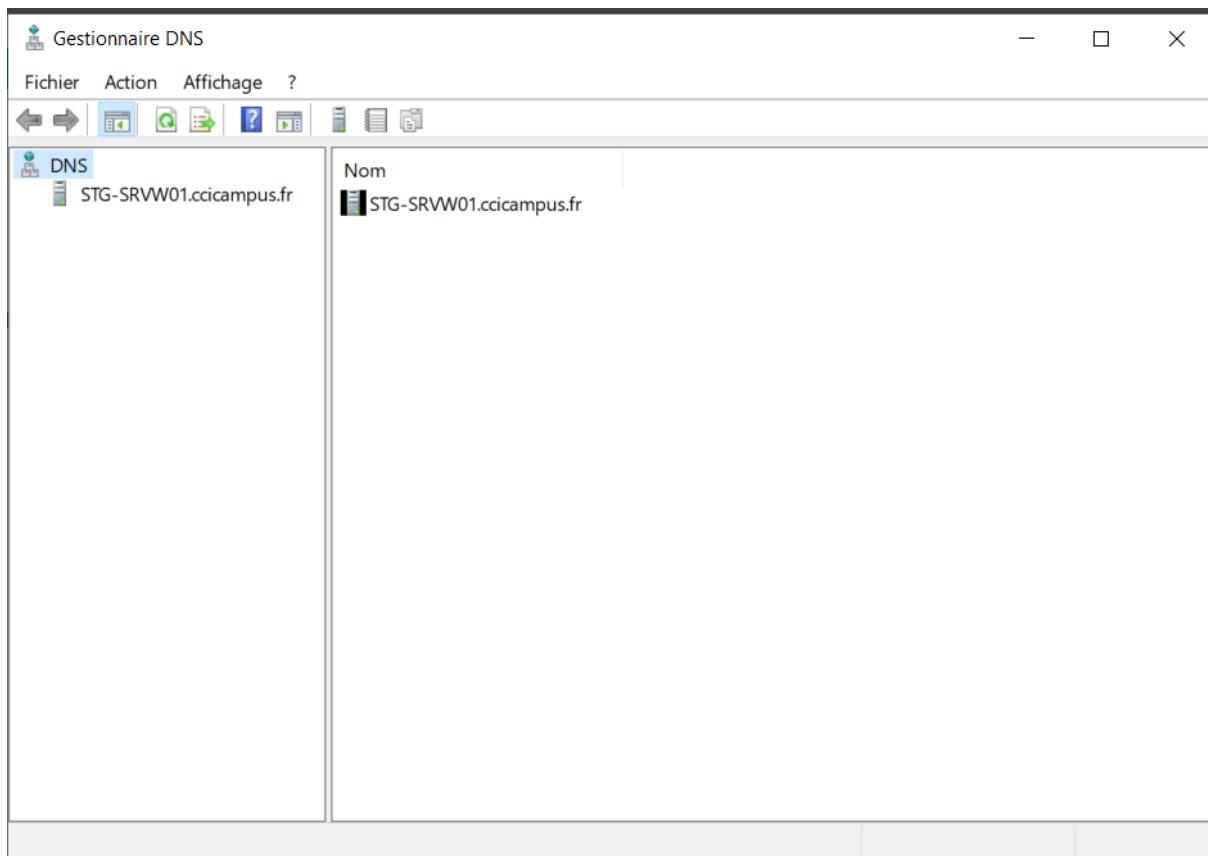
The screenshot shows the 'Results' step of the Active Directory Domain Services configuration wizard. It confirms that the server has been successfully configured as a domain controller. A warning message states that Windows Server 2019 does not support delegation for DNS zones. The target server is MUL-SRVW02.ccicampus.fr.

3.4 Mise en place du DNS

La gestion du DNS s'effectue en parcourant ce chemin :



Voici l'interface :



Par défaut, lors de la création du domaine et de sa configuration, le DNS sera également configuré.
Cela est le cas pour la zone directe :

The screenshot shows the Windows DNS Manager interface. On the left, the tree view shows the root node 'DNS' expanded to show 'STG-SRVW01.ccicampus.fr', which further expands to 'Zones de recherche directes' containing '_msdcs', '_sites', '_tcp', '_udp', 'DomainDnsZones', and 'ForestDnsZones'. Below these are several static A records for hosts like 'MUL-SRVW01', 'MUL-SRVW02', 'stg-srvw01', 'STG-SRVW02', and 'TEST-RADIUS' with IP addresses ranging from 192.168.100.2 to 100.3. There are also dynamic SOA, NS, and A records for the domain itself.

Nom	Type	Données	Horodateur
_msdcs	Source de nom (SOA)	[216], stg-srvw01.ccicampus...	statique
_sites	Serveur de noms (NS)	stg-srvw01.ccicampus.fr.	statique
_tcp	Serveur de noms (NS)	stg-srvw02.ccicampus.fr.	statique
_udp	Serveur de noms (NS)	mul-srvw02.ccicampus.fr.	statique
DomainDnsZones	Serveur de noms (NS)	mul-srvw01.ccicampus.fr.	statique
ForestDnsZones	Hôte (A)	192.168.100.3	30/12/2022 16:00:00
(identique au dossier parent)	Hôte (A)	192.168.100.2	30/12/2022 16:00:00
(identique au dossier parent)	Hôte (A)	192.168.200.2	02/12/2022 15:00:00
(identique au dossier parent)	Hôte (A)	192.168.200.3	05/12/2022 10:00:00
MUL-SRVW01	Hôte (A)	192.168.200.2	statique
MUL-SRVW02	Hôte (A)	192.168.200.3	statique
stg-srvw01	Hôte (A)	192.168.100.2	statique
STG-SRVW02	Hôte (A)	192.168.100.3	statique
TEST-RADIUS	Hôte (A)	192.168.100.30	30/12/2022 17:00:00

On aperçoit bien les quatre serveurs.

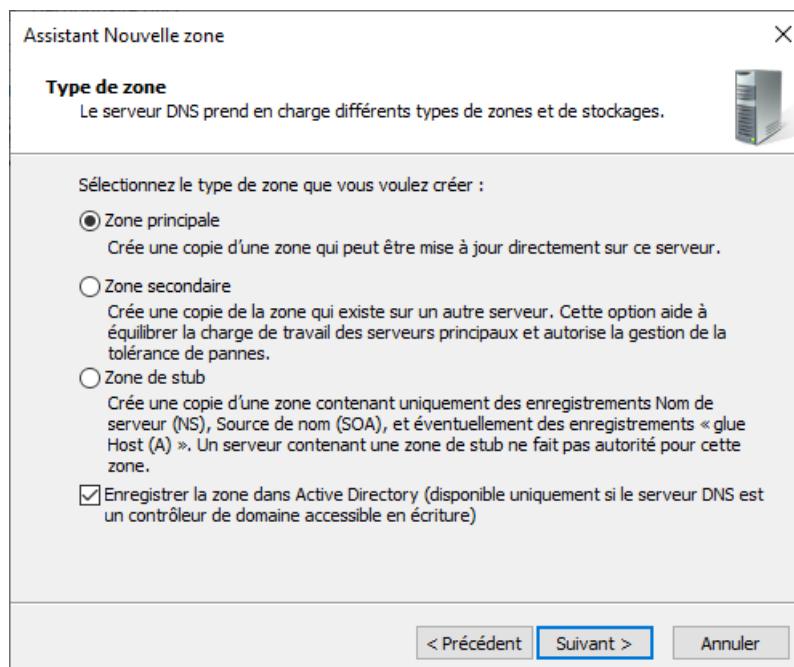
3.4.1 Ajout de zones inversées

Par contre, on peut également renseigner la zone inversée. La procédure suivante est à effectuer sur tous les serveurs :

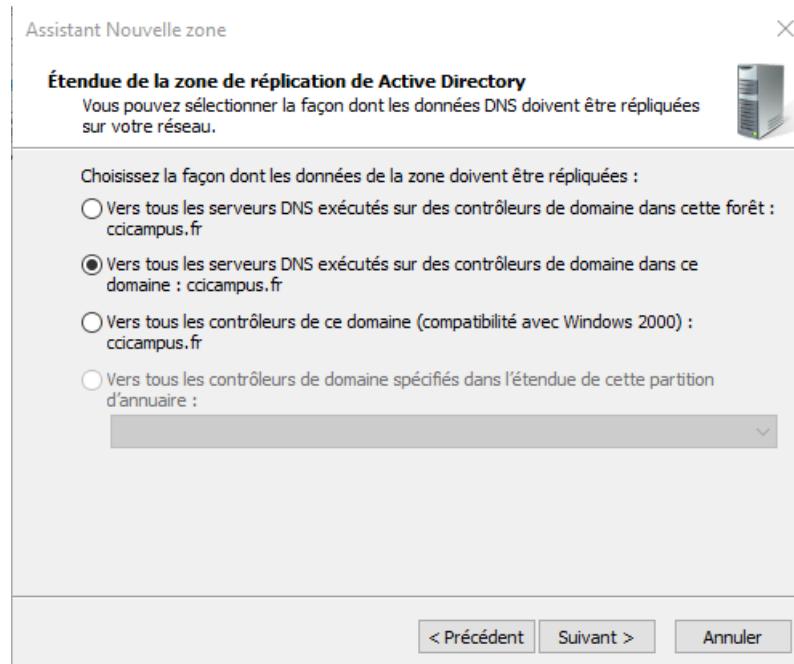
On crée une nouvelle zone :

The screenshot shows the Windows DNS Manager interface. The tree view shows the root node 'DNS' expanded to show 'STG-SRVW01.ccicampus.fr', which further expands to 'Zones de recherche directes' and 'Zones de recherche inversée'. The 'Zones de recherche inversée' node has a context menu open with the option 'Nouvelle zone...' highlighted. The main pane displays two entries under the 'Nom' column: '100.168.192.in-addr.arpa' and '200.168.192.in-addr.arpa'. These entries have 'Type' columns showing 'Serveur principal intégré à Acti...' and 'État' columns showing 'En cours d'ex...'. The 'Maître d' entry is partially visible.

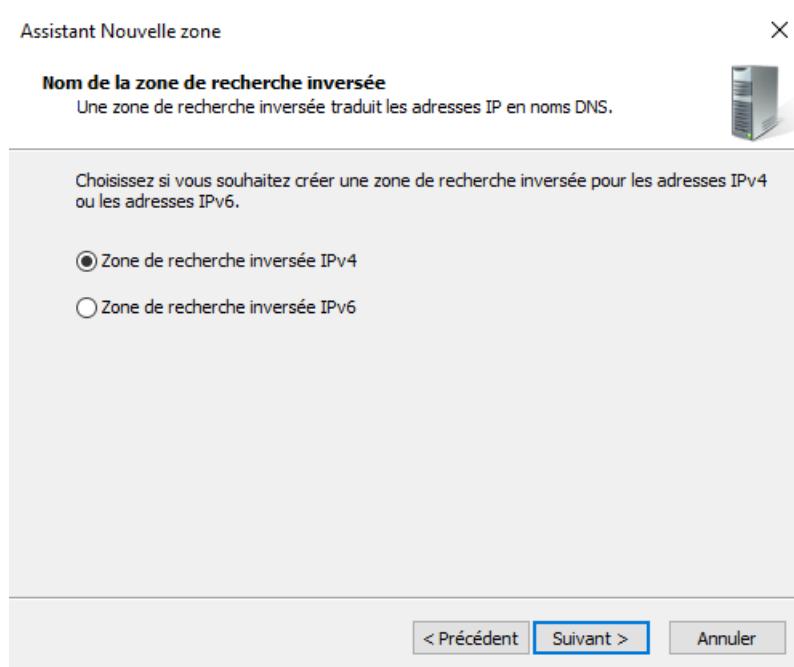
On choisit la « zone principale » :



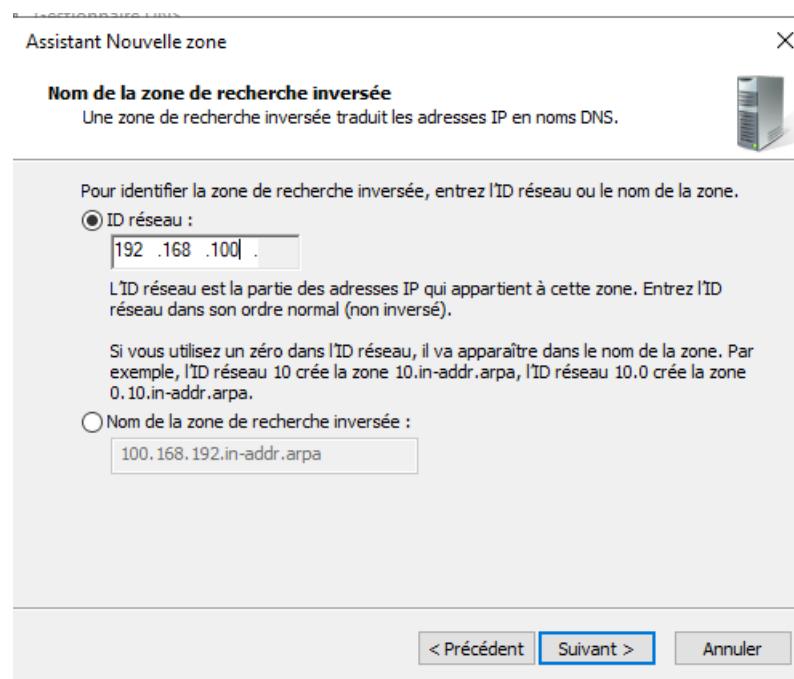
Puis « vers tous les serveurs DNS exécutés sur les contrôleurs de domaine dans ce domaine »

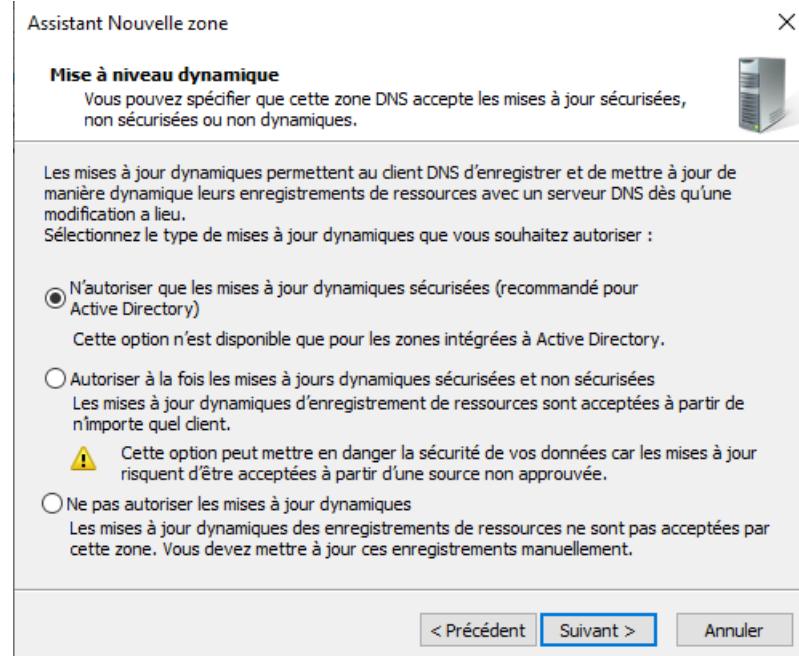


On prend l'IPv4 :

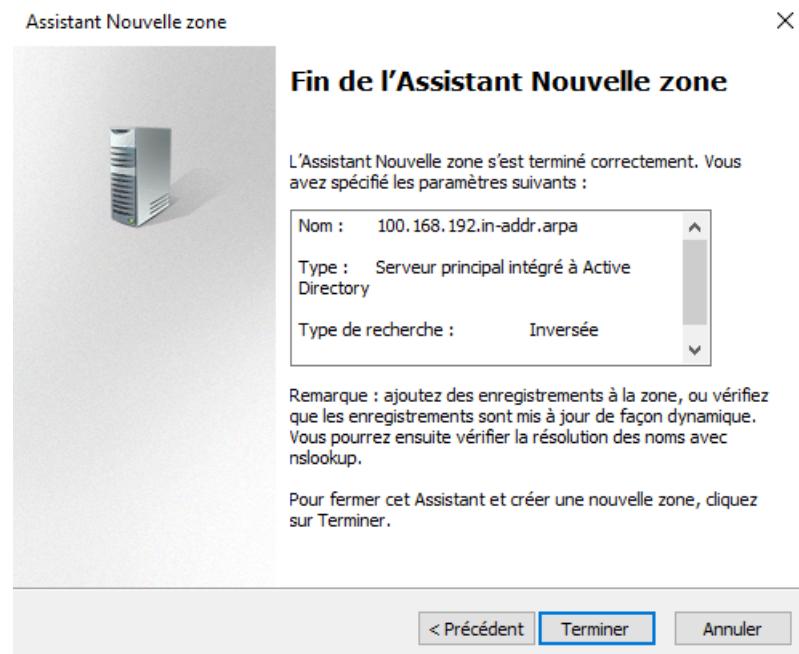


Pour l'ID réseau, personnellement nous avons informés les deux adresses : 192.168.100.0 et 192.168.200.0 en effectuant deux zones inversées (ce qui n'est pas nécessaire). Il suffit de mettre l'ID réseau du réseau de Strasbourg sur les deux serveurs et celui de Mulhouse pareillement.



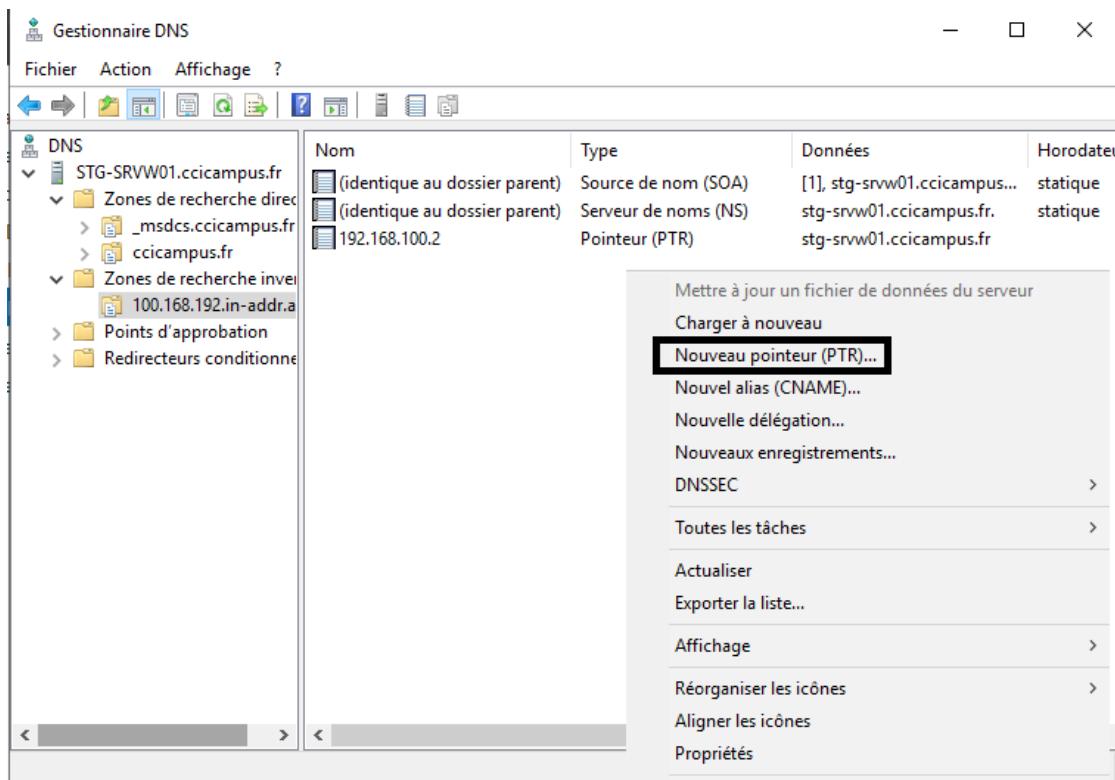


La nouvelle zone sera créée une fois que vous aurez cliqué sur « Terminer »

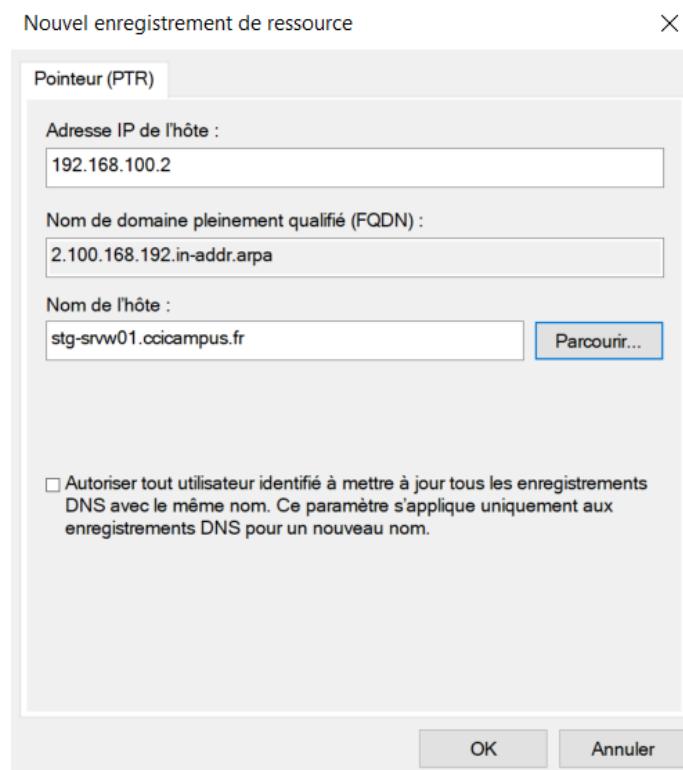


3.4.2 Ajout d'un pointeur (PTR)

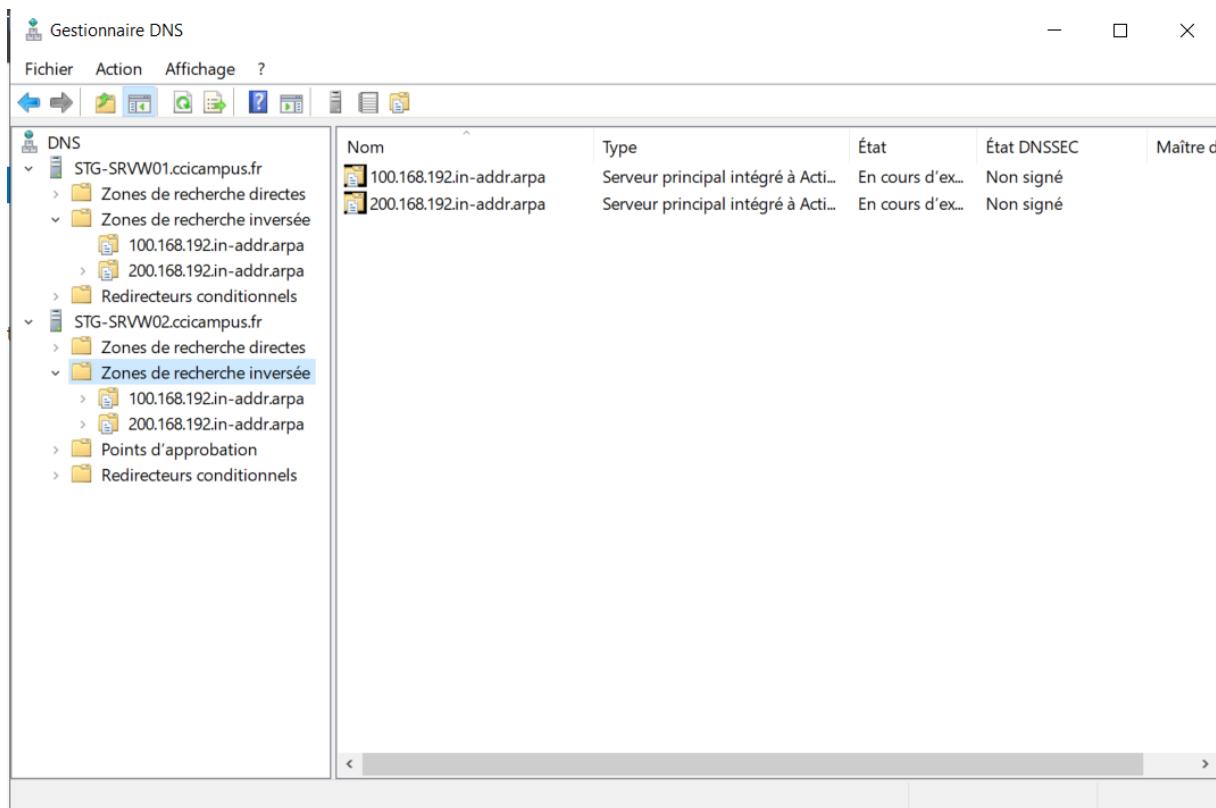
Ensuite pour que la zone inversée fonctionne il faut indiquer un pointeur (PTR) :



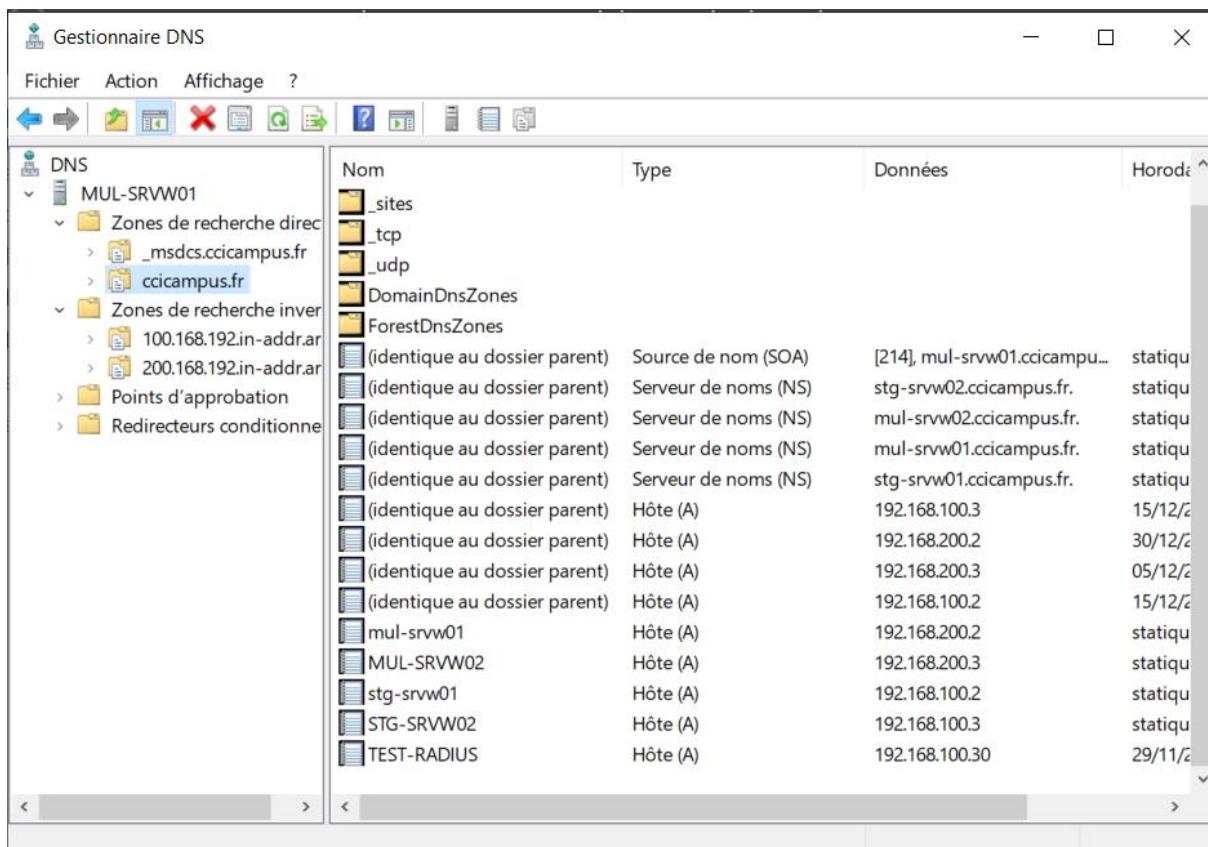
On informe le nom d'hôte :



Voilà ce que cela donne :



A nouveau, cela est à faire sur les autres serveurs. Ici, on aperçoit seulement les serveurs de Strasbourg mais ceux de Mulhouse sont également à faire. Exemple pour celui de Mulhouse :



3.5 Mise en place du DHCP

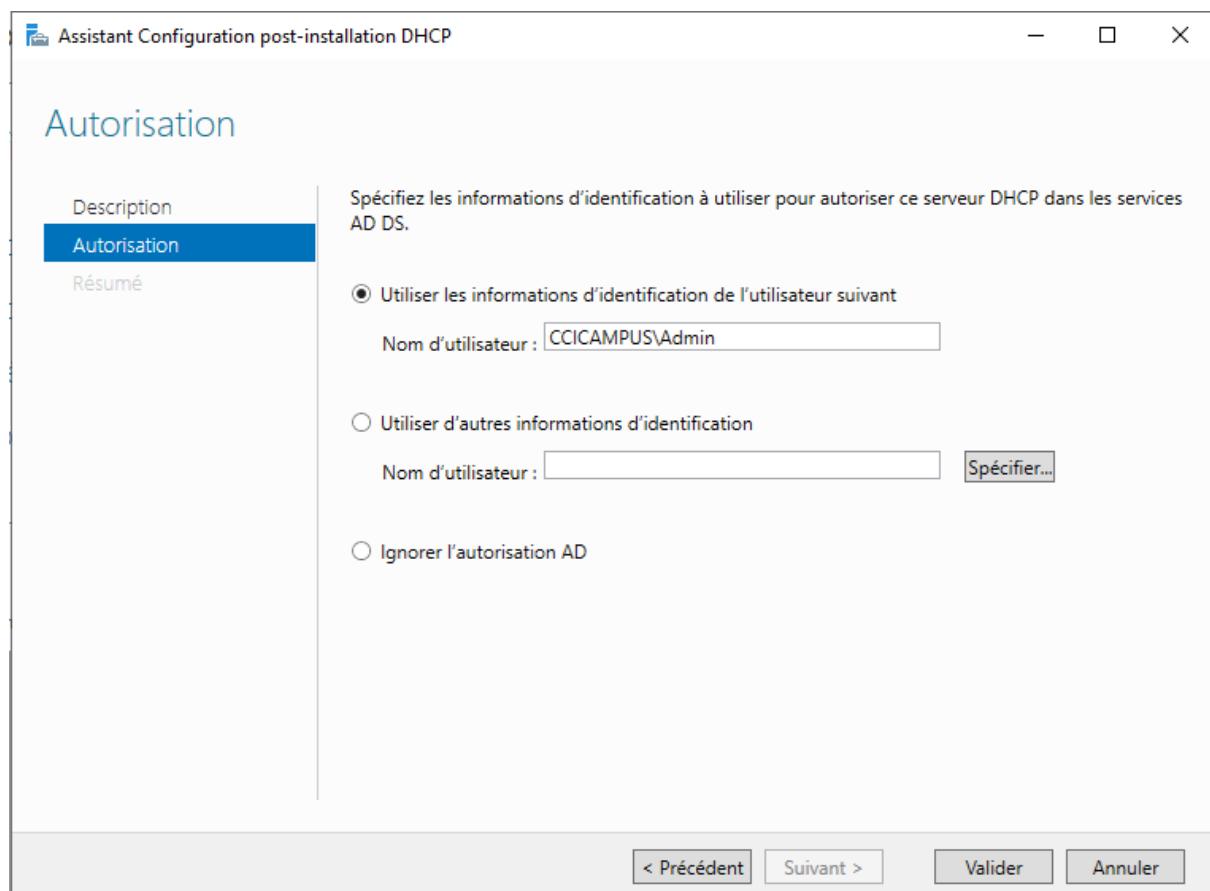
De même que pour le service DNS, le service DHCP est à configurer sur tous les serveurs. Les étapes suivantes sont à reproduire sur le serveur principal de Strasbourg et sur celui de Mulhouse. Afin d'éviter les répétitions, nous prendrons l'exemple du serveur principal (STG-SRVW01).

3.5.1 Autoriser le service DHCP dans l'AD

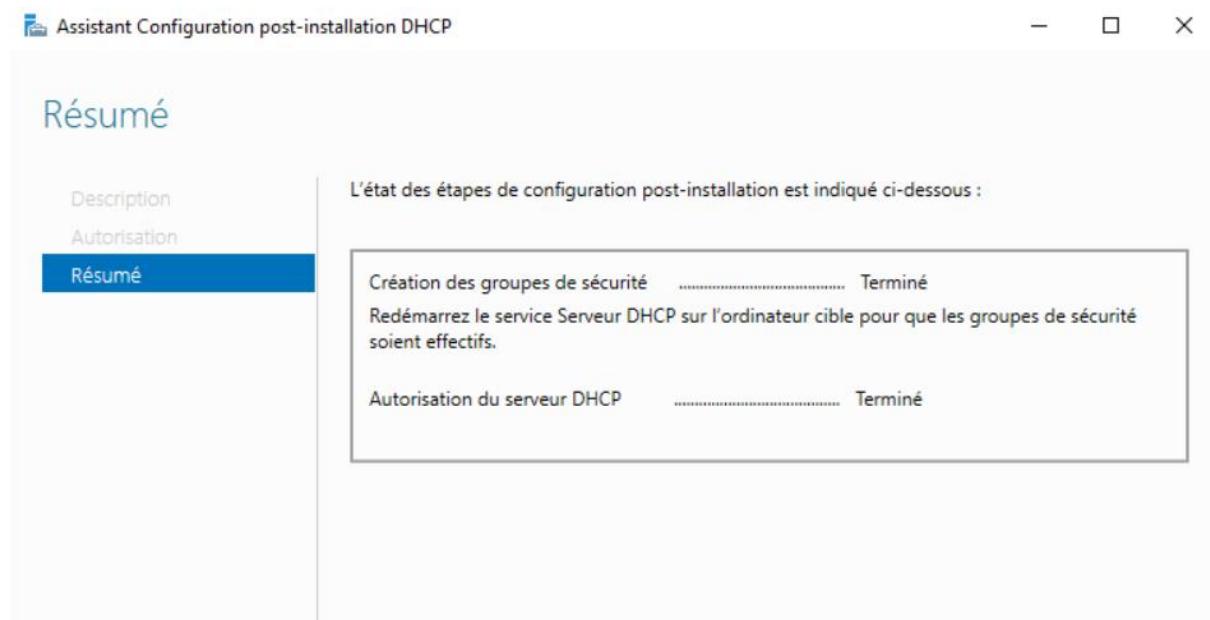
Pour le DHCP, il y a également une configuration à faire avant de pouvoir accéder à son gestionnaire :



On choisit le premier choix, cela permet de l'autoriser dans le domaine :

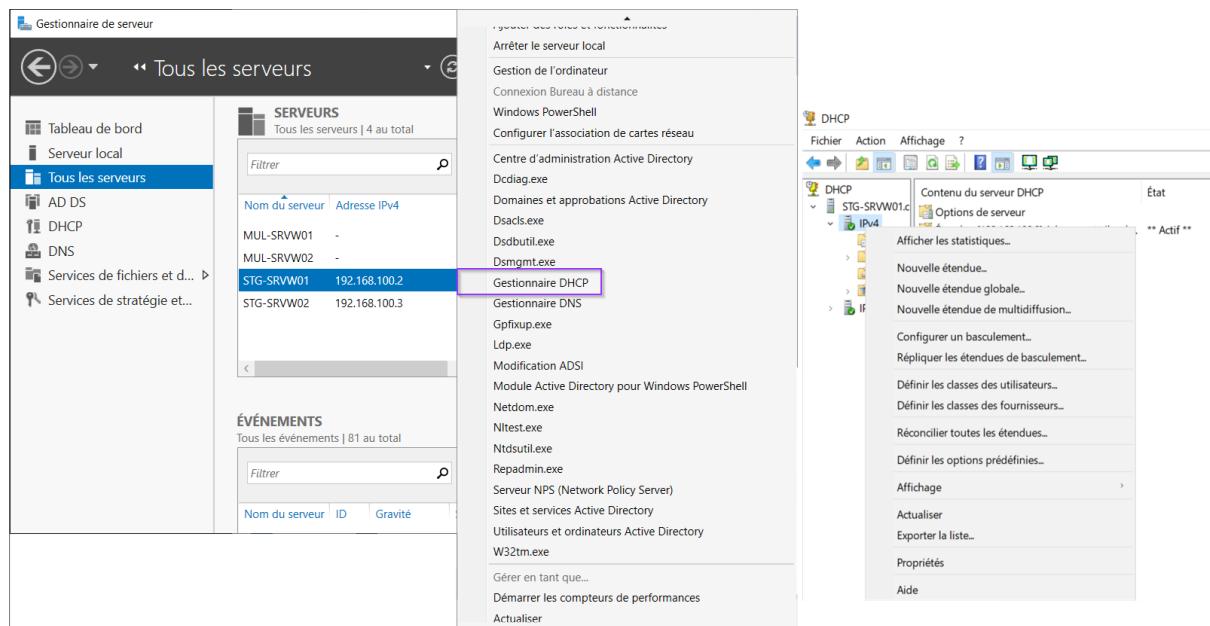


Puis on redémarre le service DHCP :

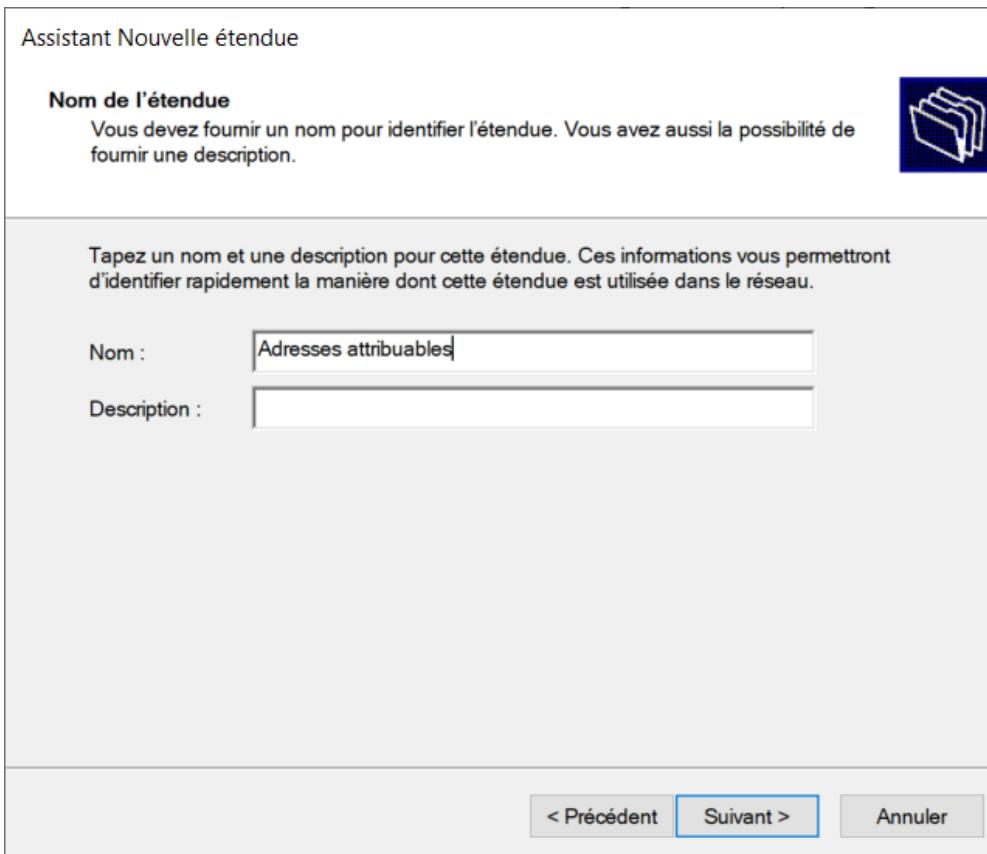
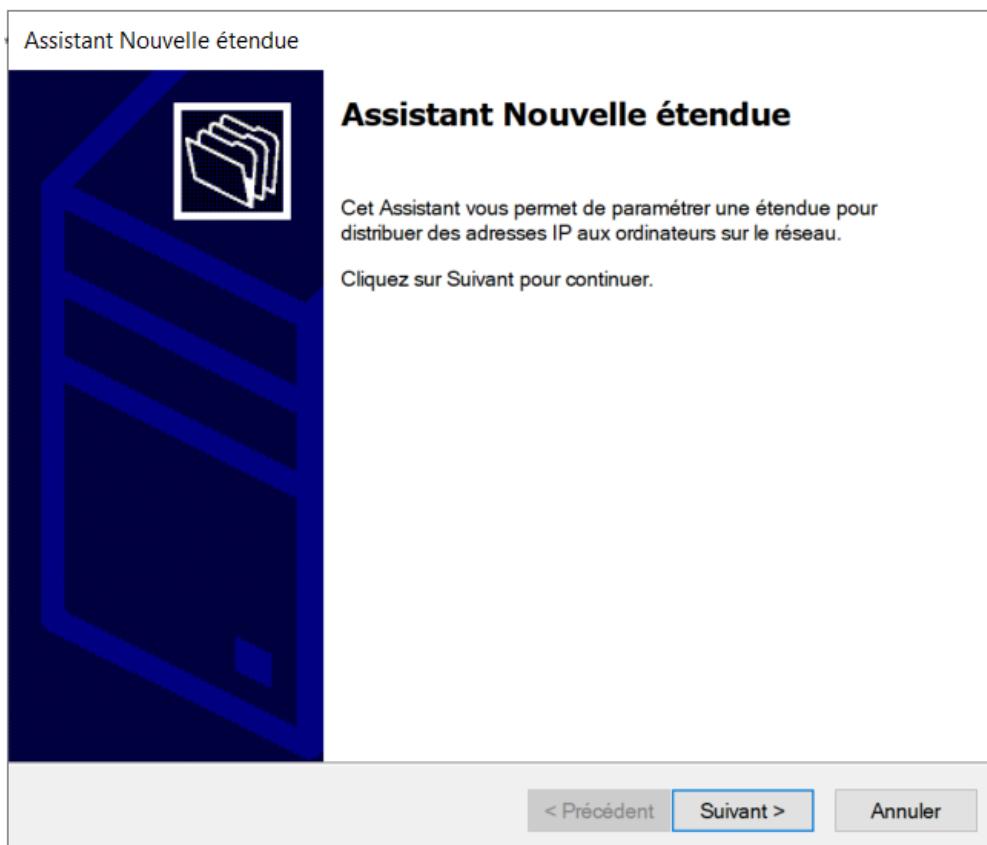


3.5.2 Création d'une étendue pour l'attribution d'adresses

On se rend dans le gestionnaire DHCP et déroule la flèche du serveur. Ensuite, on effectue un clic droit sur « IPv4 » et on clique sur « Nouvelle étendue ».



Ce qui nous amène ici :



On indique ensuite l'adresse de début et de fin attribuable ainsi que le masque de sous-réseau :

Assistant Nouvelle étendue

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

Paramètres de configuration pour serveur DHCP

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

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent Suivant > Annuler

On peut aussi bien choisir une plage à exclure :

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 DHCPOFFER.

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

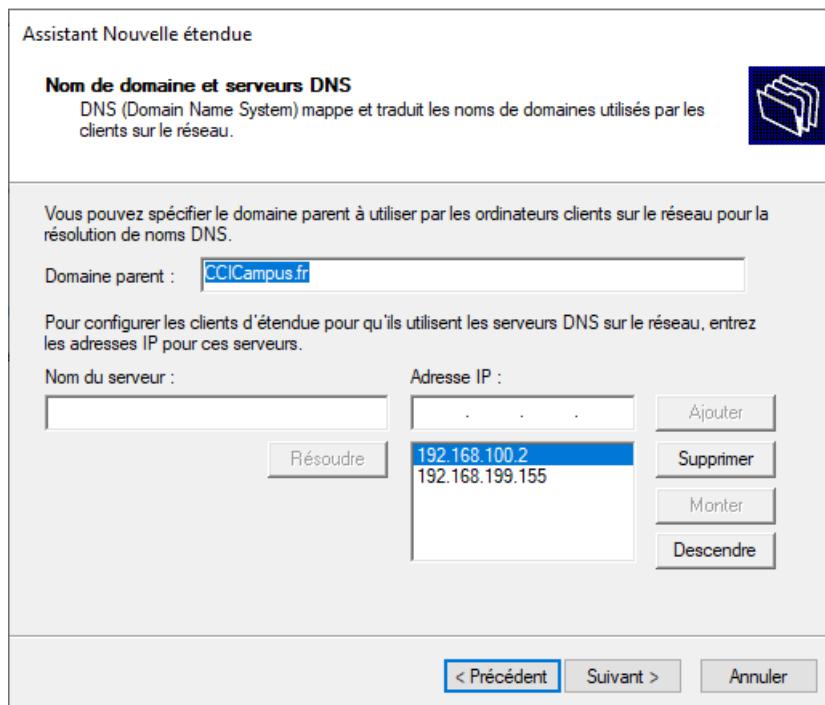
Adresse IP de début : Adresse IP de fin : Ajouter

Plage d'adresses exclue :
192.168.100.1 sur 192.168.100.29 Supprimer

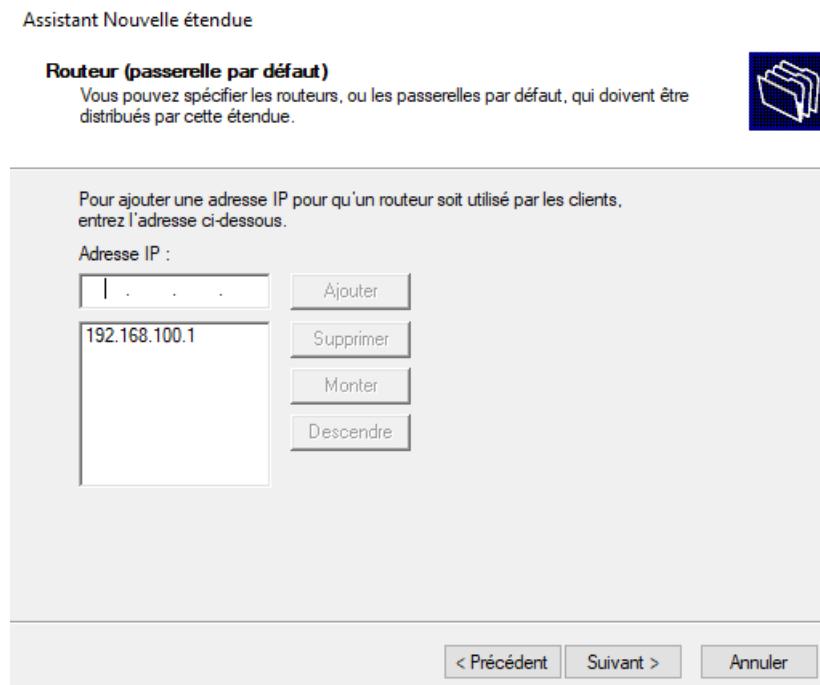
Retard du sous-réseau en millisecondes :

< Précédent Suivant > Annuler

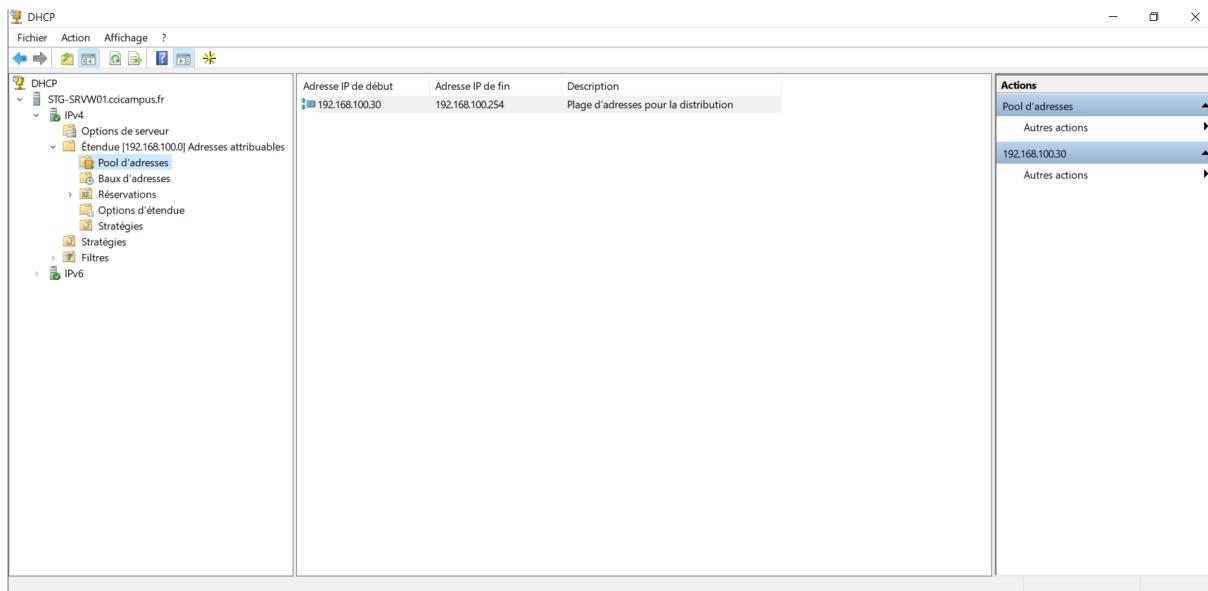
On informe ensuite le domaine et les DNS :



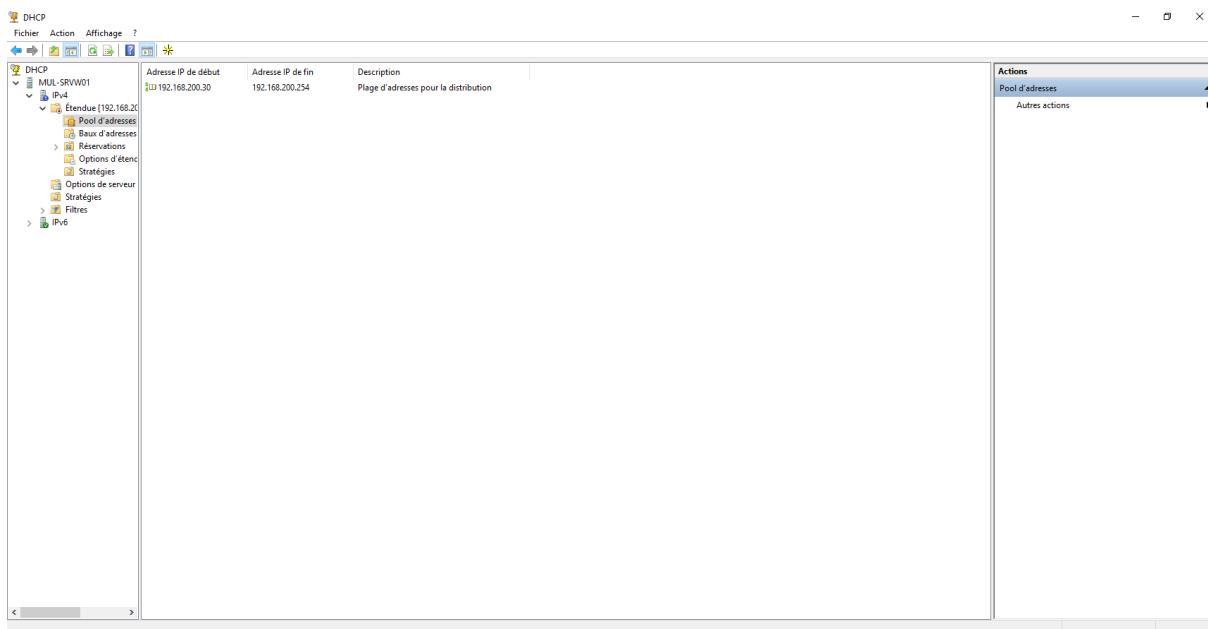
On y renseigne également la passerelle :



L'étendue a été créée :



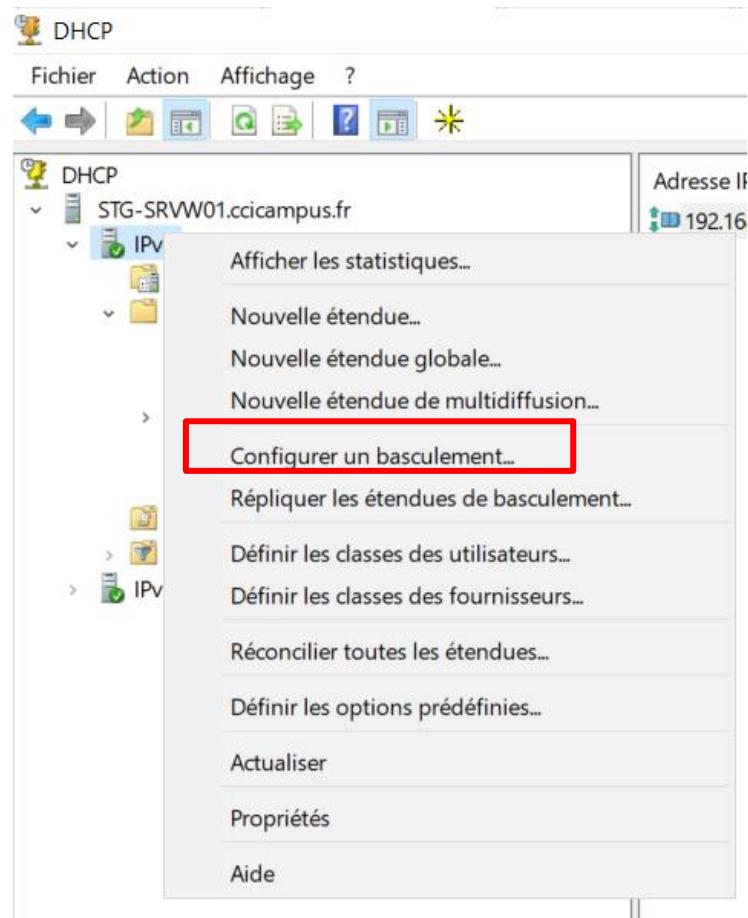
Pour Mulhouse :



3.5.3 Création d'un basculement

La mise en place de la fonctionnalité de basculement pour le DHCP offre une haute disponibilité des serveurs. Ainsi, il peut tout aussi bien fonctionner simultanément ou prendre le relais si un des serveurs tombe en panne.

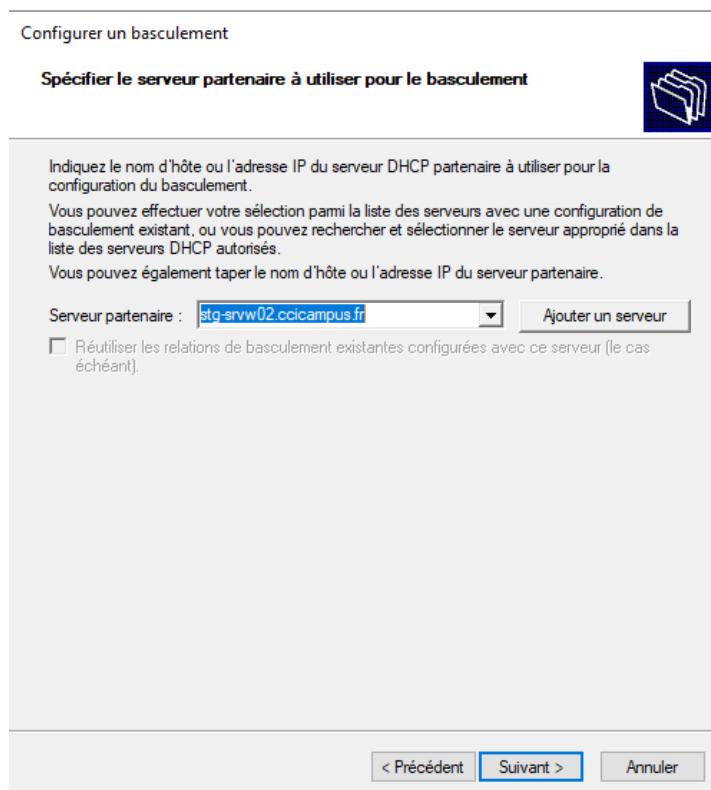
Pour créer un basculement, il faut se rendre dans l'assistant de la configuration du basculement :



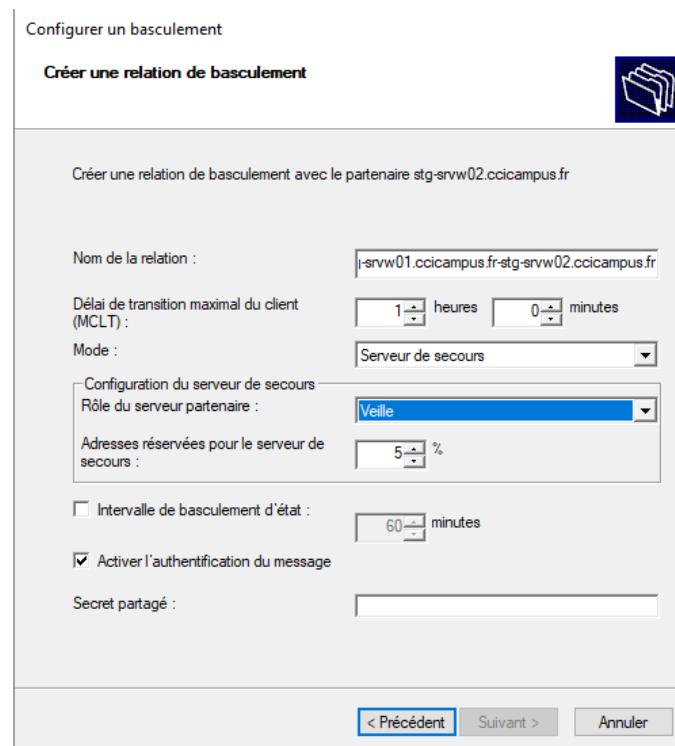
Voici l'assistant :



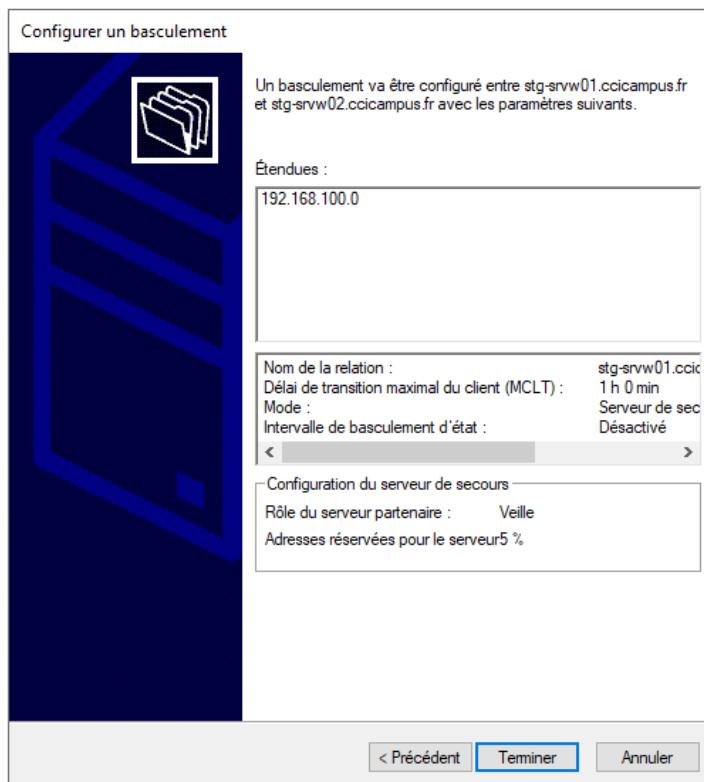
On y informe ensuite le serveur avec qui il fera le basculement. Dans notre cas, le serveur principal de Strasbourg fera un basculement avec le second serveur. Cela vaut aussi pour le site de Mulhouse.



Pour que le second serveur prenne le relais en cas de défaillance, il faut sélectionner le mode « serveur de secours » :



Le basculement a été configuré :



Pour Mulhouse aussi le basculement a été effectué :

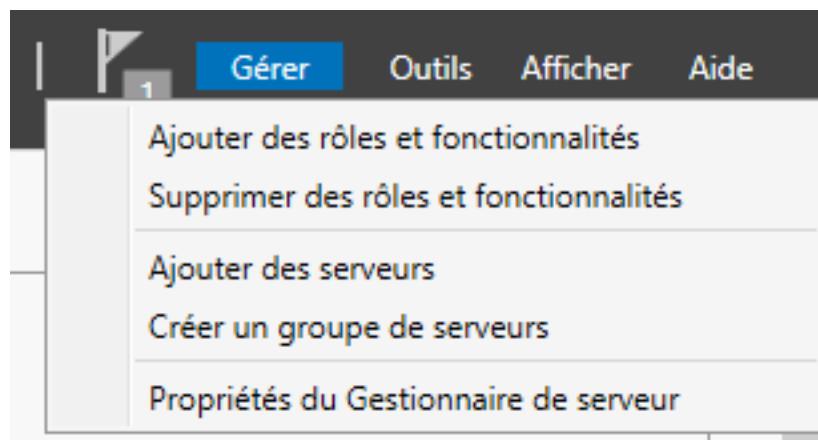


3.6 Mise en place du DFS/DFSR

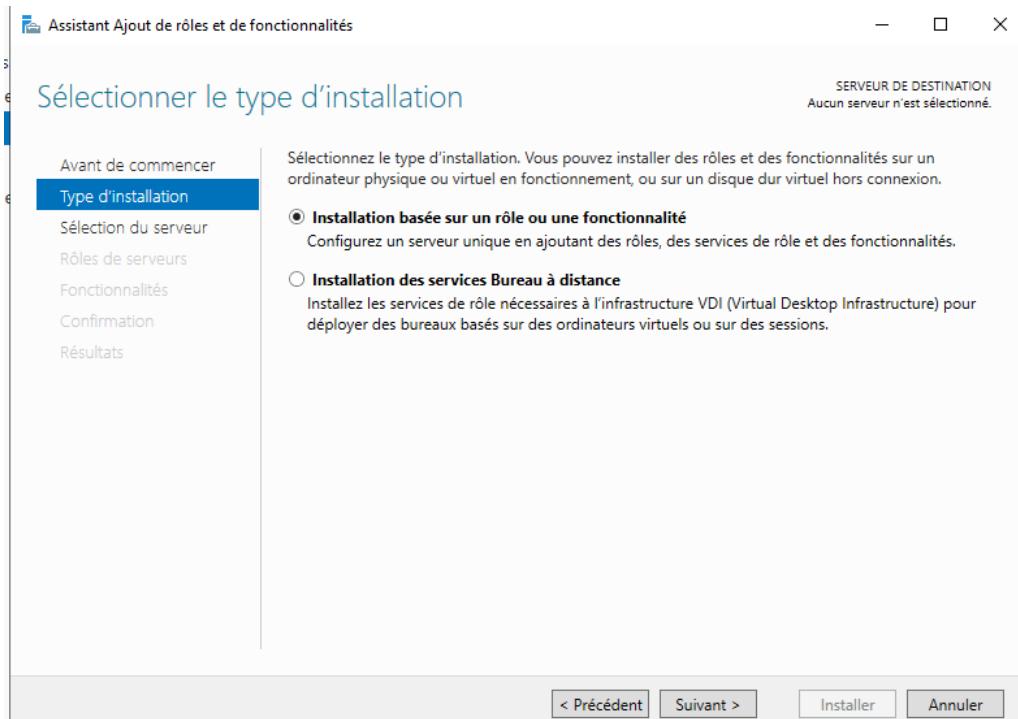
3.6.1 Configuration dossier du DFS :

Le DFS se fait majoritairement sur le serveur principal situé à Strasbourg (STG-SRVW01) les étapes sur les autres serveurs seront précisées.

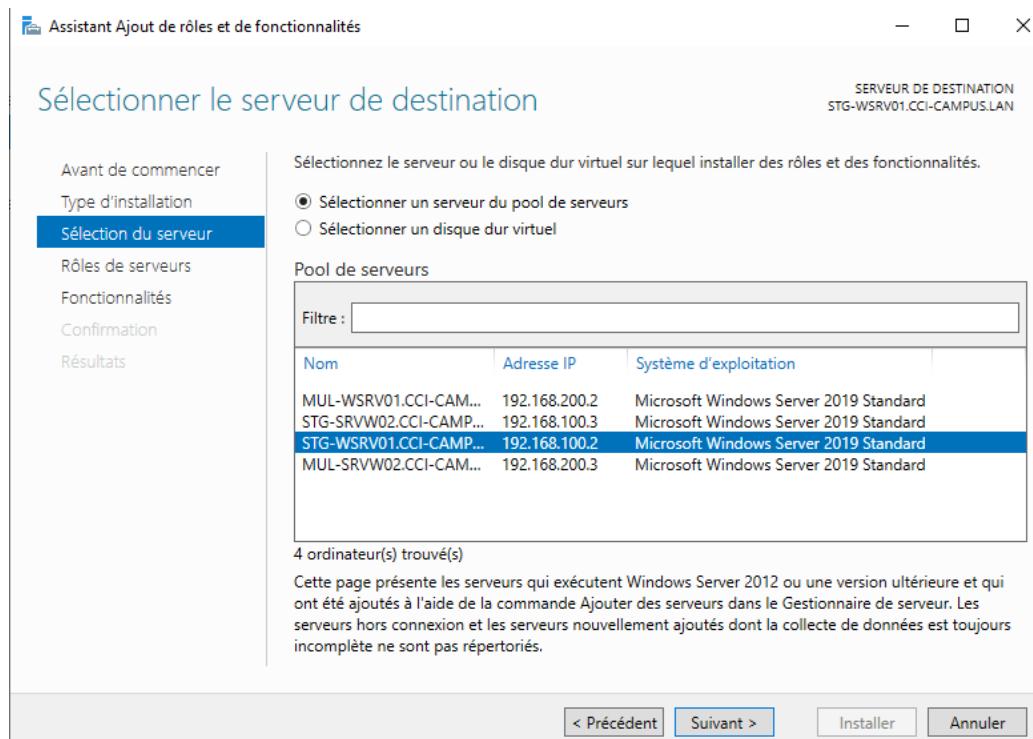
Pour commencer, il faut que nous ajoutions le rôle à notre serveur, donc rendez vous dans le gestionnaire de serveur. En haut à droite cliquez sur « Gérer », puis « ajouter des rôles et fonctionnalités »



Faites « suivant »

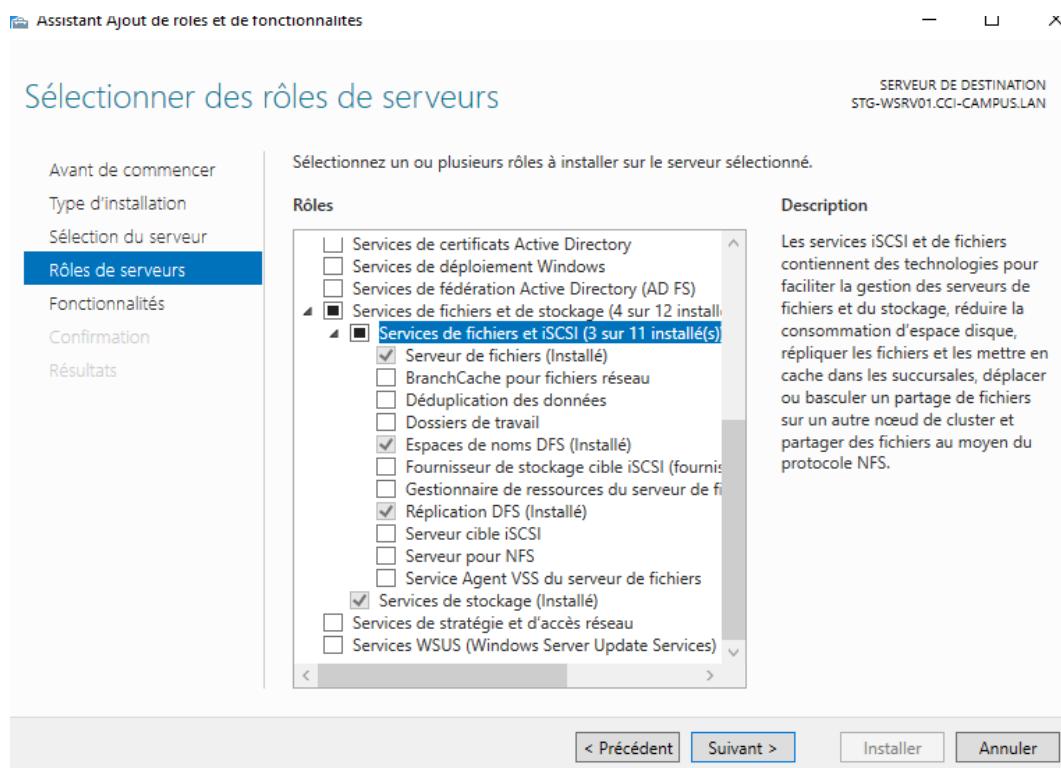


Sélectionnez le serveur principal et faites « suivant »



Ajouter le service Espace de nom DFS et RéPLICATION DFS situé dans le sous dossier Service de fichier et stockages

Faites ensuite suivant et installer

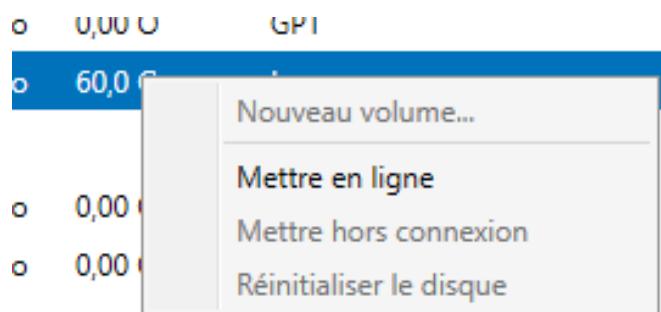


Une fois le rôle installé, rendez-vous dans le gestionnaire de serveur puis dans les disques

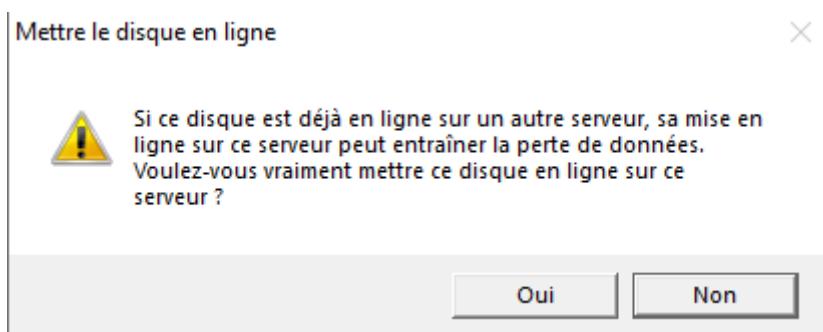
Les disques durs des différents Serveurs seront listés, ceux qui nous intéressent ici sont les disques secondaires de 60 Gb

Numéro	Disque virt...	État	Capacité	Non alloué	Partition	Lecture se...	En cluster	Sous-systè...	Type de...	Nom
▲ MUL-SRVW02 (2)										
1	En ligne	60,0 Go	0,00 0		GPT				NVMe	VMware Virtual NVMe...
0	Hors conn...	60,0 Go	60,0 Go		Inconnu				SAS	VMware, VMware Virt...
▲ MUL-WSRV01 (2)										
1	En ligne	60,0 Go	0,00 0		GPT				NVMe	VMware Virtual NVMe...
0	Hors conn...	60,0 Go	0,00 0		GPT	✓			SAS	VMware, VMware Virt...
▲ STG-SRVW02 (2)										
1	En ligne	60,0 Go	0,00 0		GPT				NVMe	VMware Virtual NVMe...
0	Hors conn...	60,0 Go	0,00 0		GPT	✓			SAS	VMware, VMware Virt...
▲ STG-WSRV01 (2)										
1	En ligne	60,0 Go	0,00 0		GPT				NVMe	VMware Virtual NVMe...
0	Hors conn...	60,0 Go	0,00 0		GPT	✓			SAS	VMware, VMware Virt...

Faites un clic droit sur le disque hors ligne et cliquez sur mise en ligne



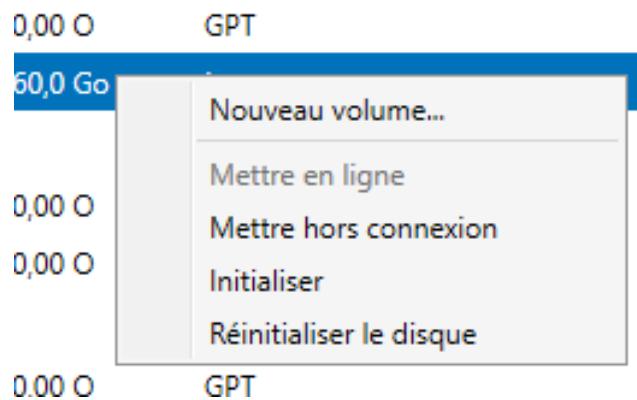
Accepter la mise en ligne



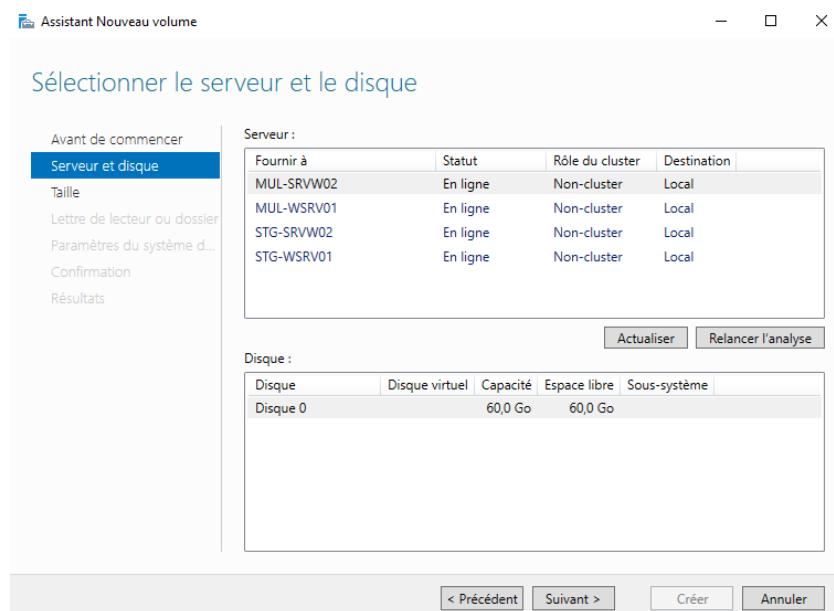
Répétez l'action pour chaque disque hors ligne afin qu'ils soient tous opérationnel

DISQUES										TÂCHES
Numéro	Disque virt...	État	Capacité	Non alloué	Partition	Lecture se...	En cluster	Sous-systè...	Type de...	Nom
▲ MUL-SRVW02 (2)										
1		En ligne	60,0 Go	0,00 O	GPT				NVMe	VMware Virtual NVMe...
0		En ligne	60,0 Go	60,0 Go	Inconnu				SAS	VMware, VMware Virt...
▲ MUL-WSRV01 (2)										
1		En ligne	60,0 Go	0,00 O	GPT				NVMe	VMware Virtual NVMe...
0		En ligne	60,0 Go	0,00 O	GPT				SAS	VMware, VMware Virt...
▲ STG-SRVW02 (2)										
1		En ligne	60,0 Go	0,00 O	GPT				NVMe	VMware Virtual NVMe...
0		En ligne	60,0 Go	0,00 O	GPT				SAS	VMware, VMware Virt...
▲ STG-WSRV01 (2)										
1		En ligne	60,0 Go	0,00 O	GPT				NVMe	VMware Virtual NVMe...
0		En ligne	60,0 Go	0,00 O	GPT				SAS	VMware, VMware Virt...

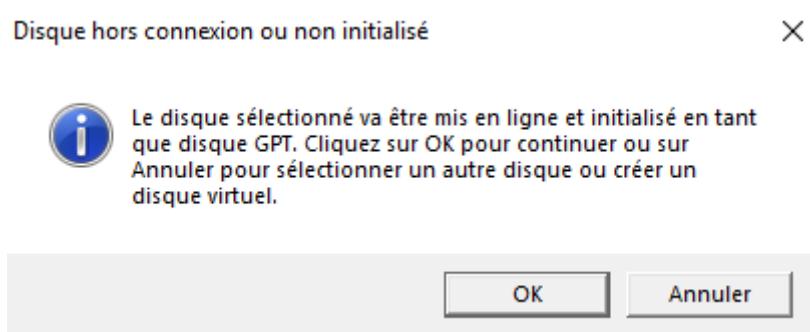
Continuer en créant un nouveau volume en faisant clic droit sur le disque récemment mis en ligne



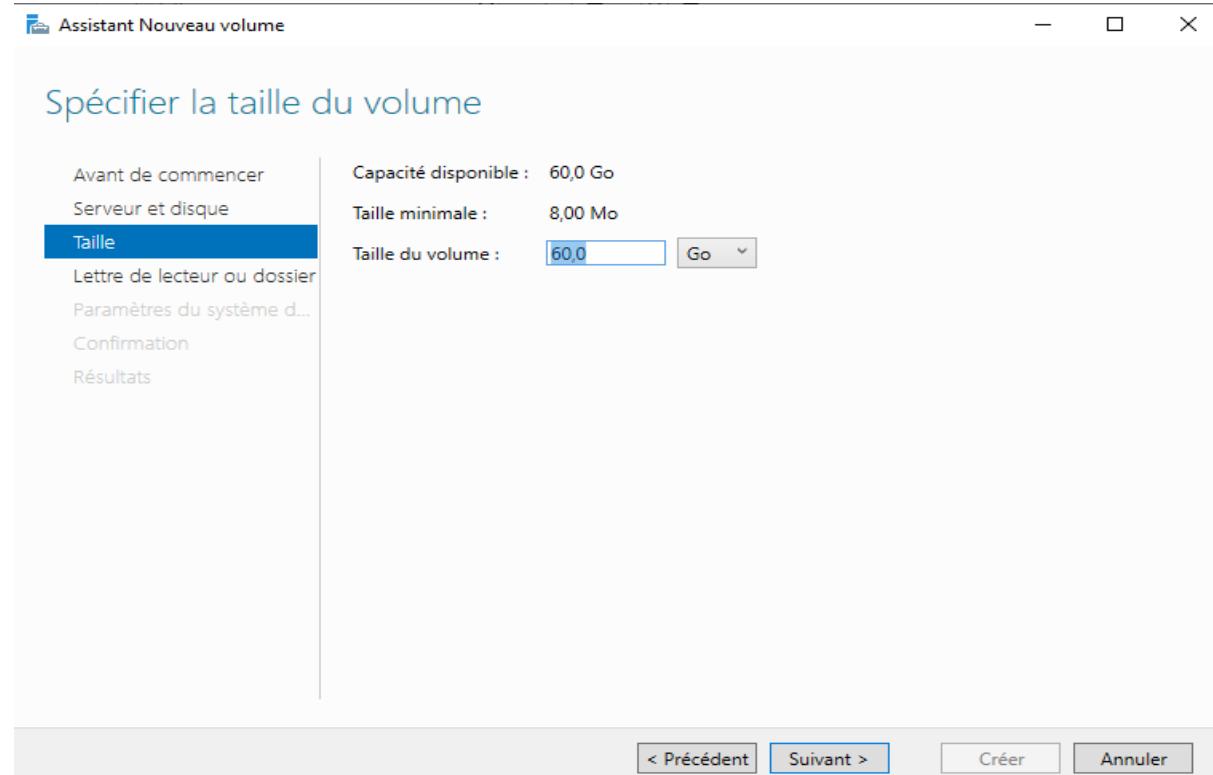
Sélectionner le serveur ainsi que le disque sur lequel vous voulez créer le volume et faites « suivant »



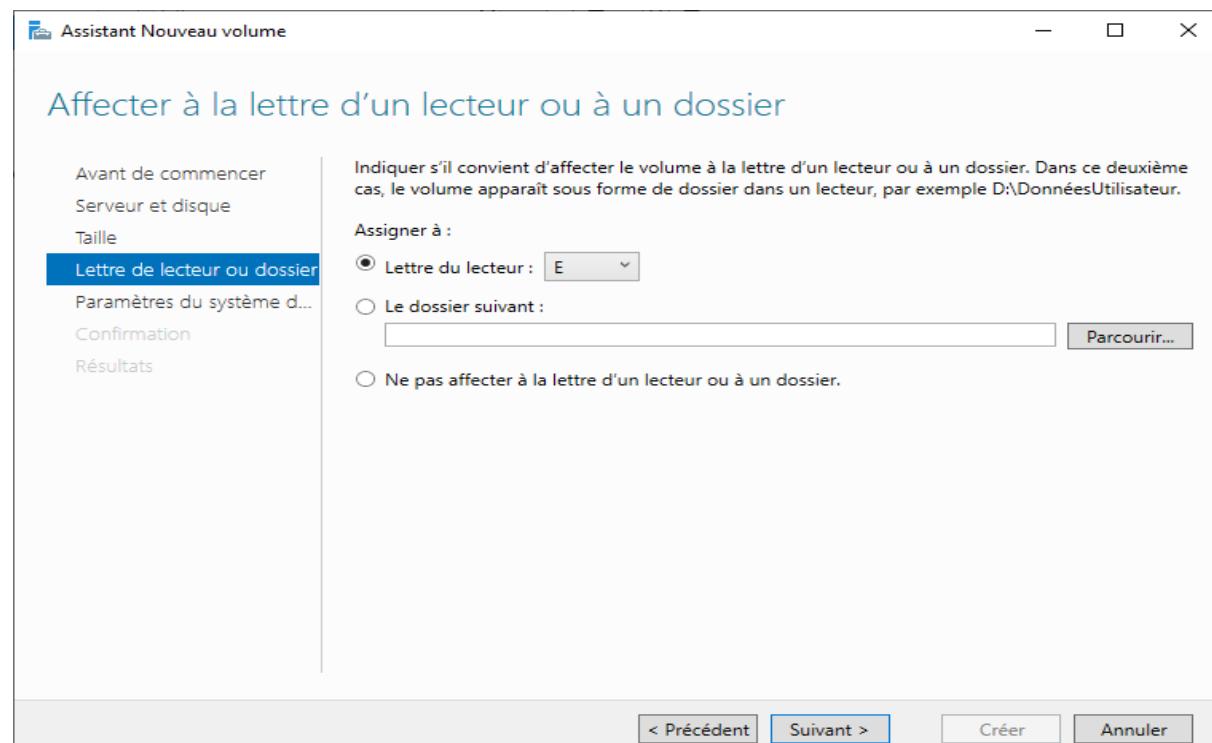
Faites « OK »



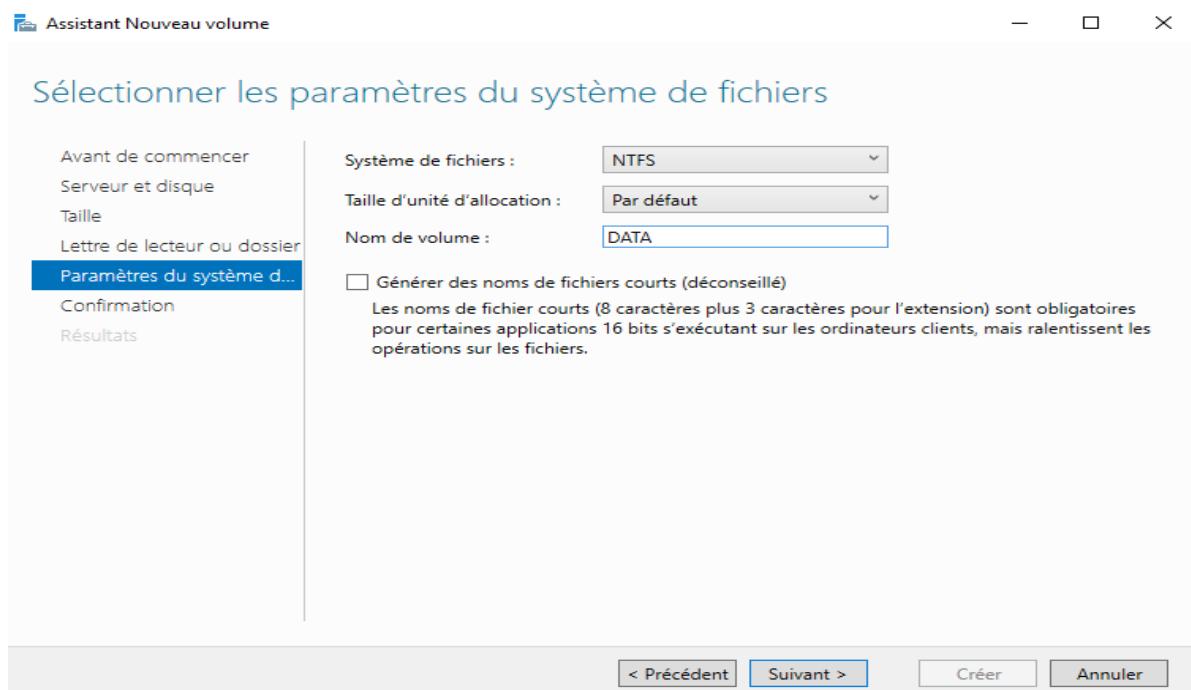
Cliquez sur «suivant»



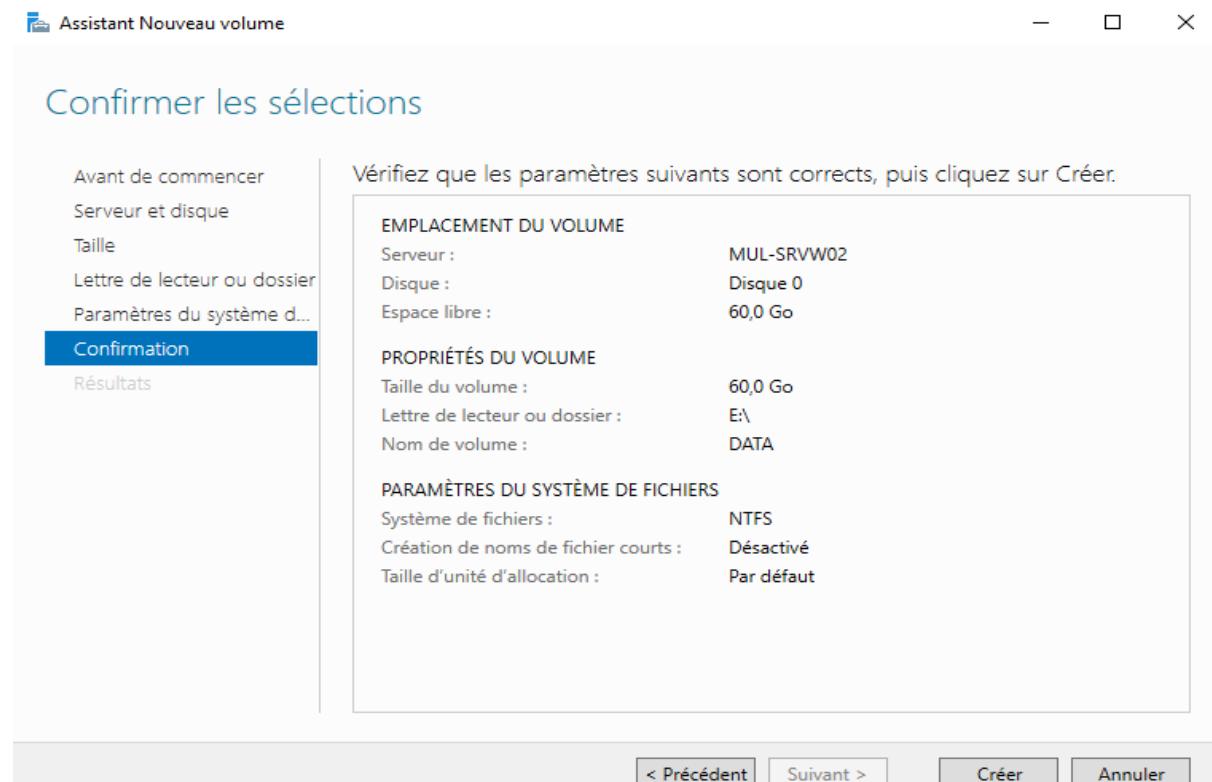
Choisissez la lettre pour votre nouveau lecteur



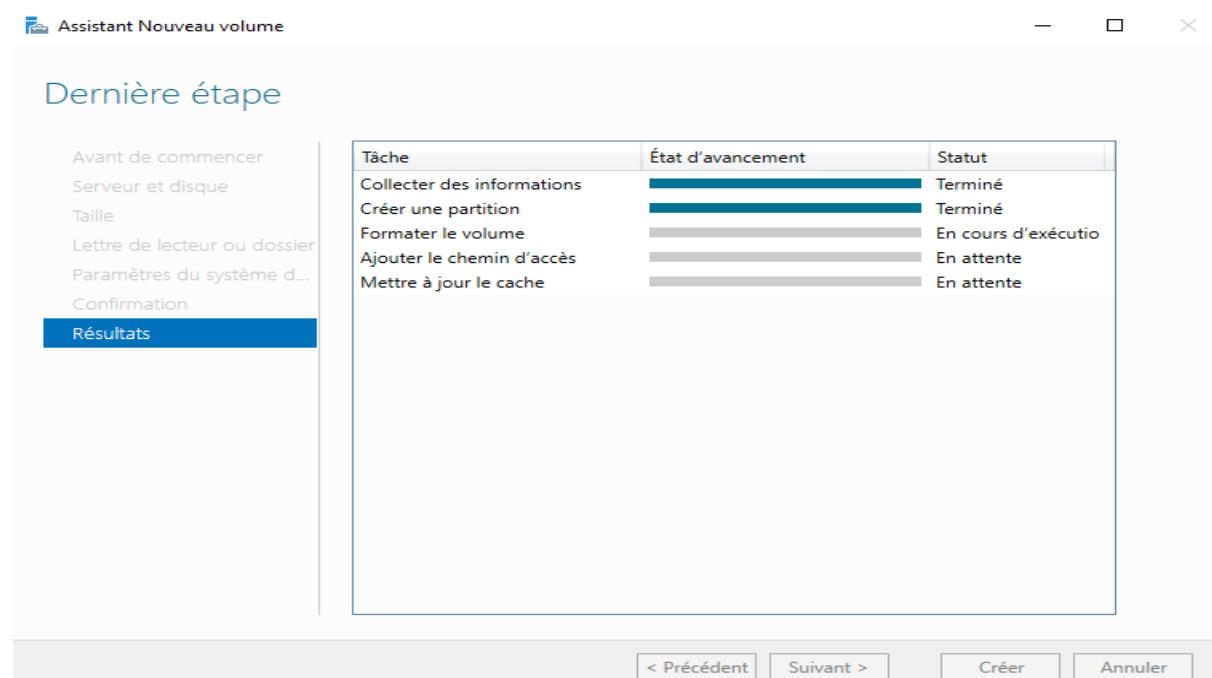
Choisissez le nom du volume (DATA sera le nom choisi dans ce cas pour tous les volumes du DFS)



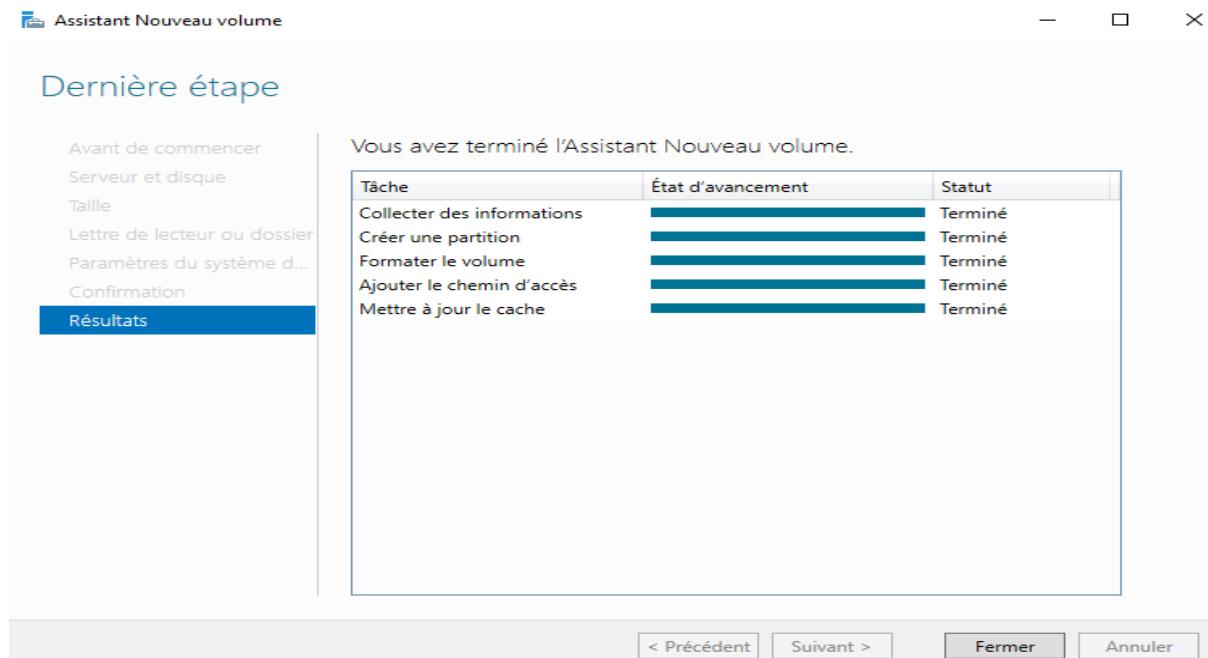
Faites «créer »



Création du volume en cours



Votre volume à bien été créé, faites suivant



Répété l'action pour les disques secondaires des 4 serveurs

L'étapes suivantes est de crée les dossiers suivants pour le serveur attribuer à chaque dossier

Important : les dossiers devront être crée sur les disques durs secondaire initialisé précédemment

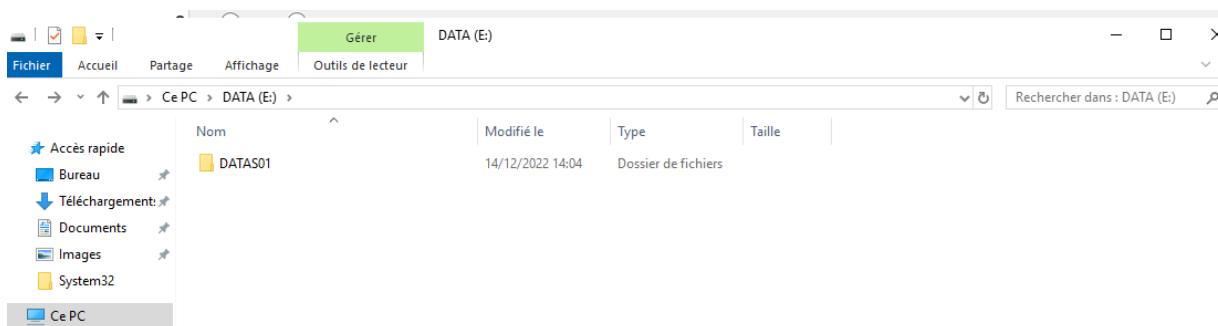
Data01 : STG-SRVW01

Data02: STG-SRVW02

Data03: MUL-SRVW01

Data04 : MUL-SRVW02

Pour les serveurs graphiques, aller dans le nouveau lecteur et faites clic droit, crée un nouveau dossier



Pour le serveur en ligne de commande, faites un mkdir (nom de la lettre du lecteur choisie, ici B) :
\nom du dossier

Ce qui donne dans le cas du serveur MUL-SRVW02

```
Mkdir b:\Datas04
```

```
: \Users\Administrateur.CCI-CAMPUS>mkdir b:\DATAS04
: \Users\Administrateur.CCI-CAMPUS>dir b:\
Le volume dans le lecteur B s'appelle DATA
Le numéro de série du volume est A6E3-6A47
```

Répété l'action sur tous les serveurs.

3.6.2 Création dossier partagé :

Une fois tout le dossier créé, revenez sur le serveur principal et aller dans l'onglet dossier partagé du gestionnaire de serveur

Faites un clic droit et faites nouveau partage

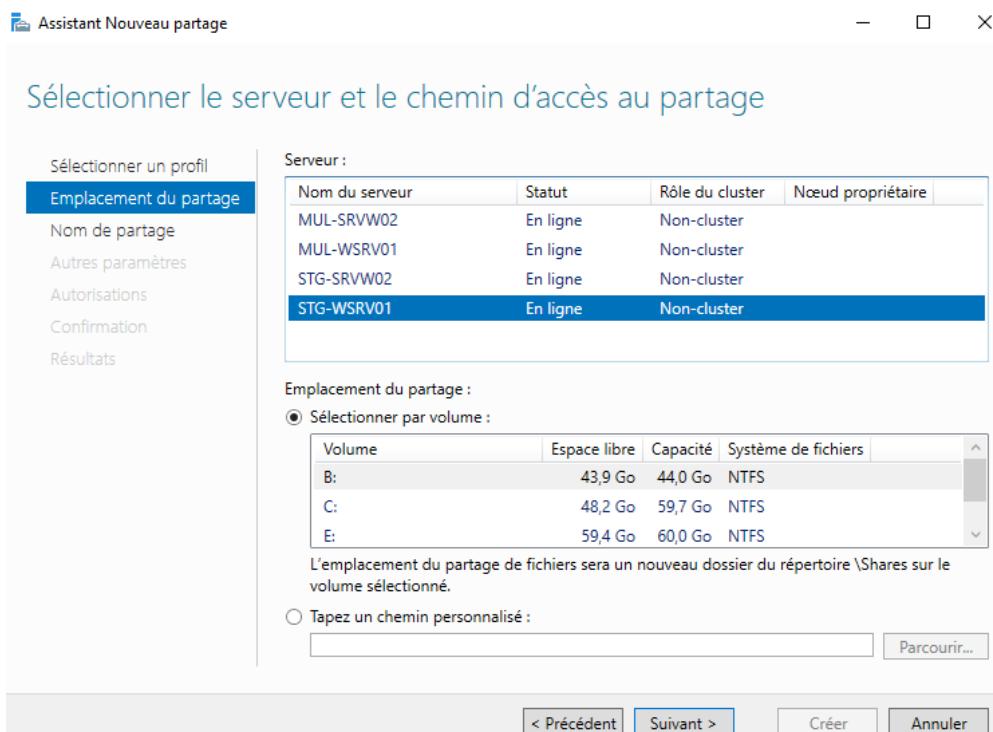
Partager	Chemin d'accès local	Protocole	Type de disponibilité
DFS	C:\DFSRoots\DFS	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ MUL-SRVW02 (3)			
DFS	C:\DFSRoots\DFS	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ MUL-WSRV01 (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ STG-SRVW02 (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ STG-WSRV01 (2)			
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster

Sélectionner Partage SMB rapide et faites «suivant»

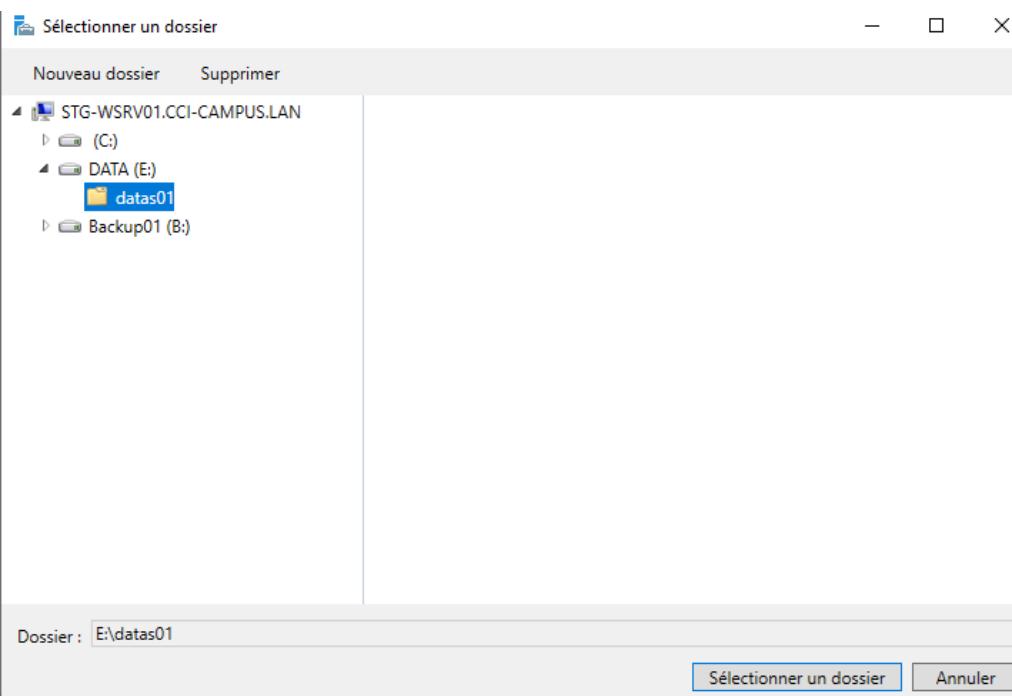
Sélectionner un profil		Profil du partage de fichiers :	Description :
<input checked="" type="radio"/>	Emplacement du partage	Partage SMB - Rapide	Ce profil de base constitue le moyen le plus rapide de créer un partage de fichiers SMB, généralement utilisé pour partager des fichiers avec des ordinateurs Windows.
<input type="radio"/>	Nom de partage	Partage SMB - Avancé	• Convient au partage général de fichiers.
<input type="radio"/>	Autres paramètres	Partage SMB - Applications	• Les options avancées peuvent être configurées ultérieurement à l'aide de la boîte de dialogue Propriétés.
<input type="radio"/>	Autorisations	Partage NFS - Rapide	
<input type="radio"/>	Confirmation	Partage NFS - Avancé	
<input type="radio"/>	Résultats		

< Précédent Crée

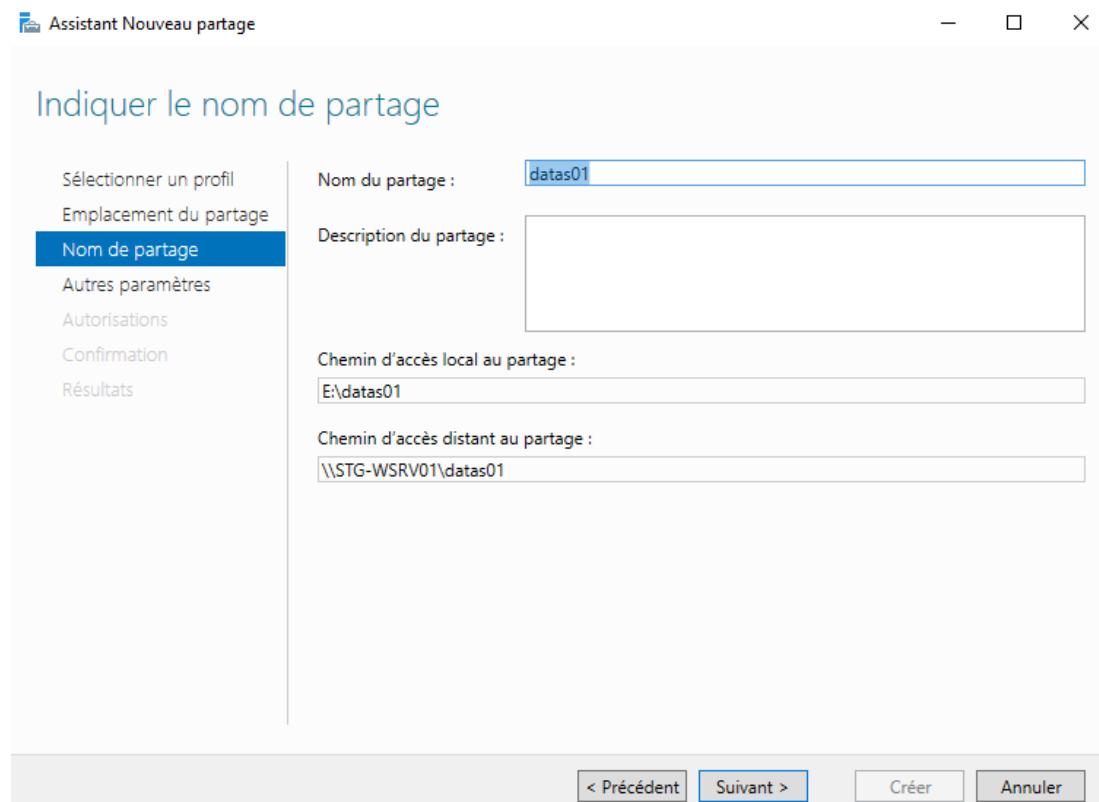
Choisissez le serveur sur lequel vous voulez initialiser le dossier partagé



Sélectionner à chaque fois le dossier créé dans l'étape précédente



Nommé votre partage de la même manière que le plan de nommage de création des dossiers vu précédemment et faites « suivant »



Laissez les paramètres par défaut et faites « suivant »

Assistant Nouveau partage

Configurer les paramètres de partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Activer l'énumération basée sur l'accès
L'énumération basée sur l'accès n'affiche que les fichiers et les dossiers dont un utilisateur possède les autorisations d'accès. S'il ne bénéficie pas d'autorisations en lecture (ou équivalentes) sur un dossier, Windows cache alors ce dernier de l'utilisateur.

Autoriser la mise en cache du partage
La mise en cache met le contenu du partage à la disposition des utilisateurs hors connexion. Si la fonctionnalité BranchCache du service de rôle Fichiers réseau est installée, vous pouvez activer BranchCache sur le partage.

Activer le cache de filiale (BranchCache) sur le partage de fichiers
BranchCache permet aux ordinateurs d'une succursale de mettre en cache les fichiers téléchargés à partir de ce partage, puis de les rendre disponibles en toute sécurité pour les autres ordinateurs de la succursale.

Chiffrer l'accès aux données
Lorsqu'il est activé, l'accès distant aux fichiers de ce partage est chiffré. Cela a pour effet de sécuriser les données contre tout accès non autorisé lors de leur transfert vers ou depuis le partage. Si cette case à cocher est activée et grisée, cela signifie qu'un administrateur a activé le chiffrement pour l'ensemble du serveur.

< Précédent Suivant > Créez Annuler

Pour chaque dossier partagé dans cette étape, nous allons accorder des droits spécifiques

Rendez-vous dans Personnaliser les autorisations

Assistant Nouveau partage

- □ ×

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...](#)

< Précédent

Suivant >

Créer

Annuler

Aller dans l'onglet partage

Paramètres de sécurité avancés pour datas01

- □ ×

Nom : E:\datas01

Propriétaire : Administrateurs (CCI-CAMPUS\Administrateurs) [Modifier](#)

Autorisations

Partage

Audit

Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

Type	Principal	Accès	Hérité de	S'applique à
Auto...	Administrateurs (CCI-CAMPUS\Administrateurs)	Contrôle total	Aucun	Ce dossier seulement
Auto...	Administrateurs (CCI-CAMPUS\Administrateurs)	Contrôle total	E:\	Ce dossier, les sous-dossiers et...
Auto...	Système	Contrôle total	E:\	Ce dossier, les sous-dossiers et...
Auto...	CREATEUR PROPRIETAIRE	Contrôle total	E:\	Les sous-dossiers et les fichiers...
Auto...	Utilisateurs (CCI-CAMPUS\Ut...)	Lecture et exécution	E:\	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (CCI-CAMPUS\Ut...)	Spéciale	E:\	Ce dossier et les sous-dossiers

[Ajouter](#)

[Supprimer](#)

[Afficher](#)

[Désactiver l'héritage](#)

Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet

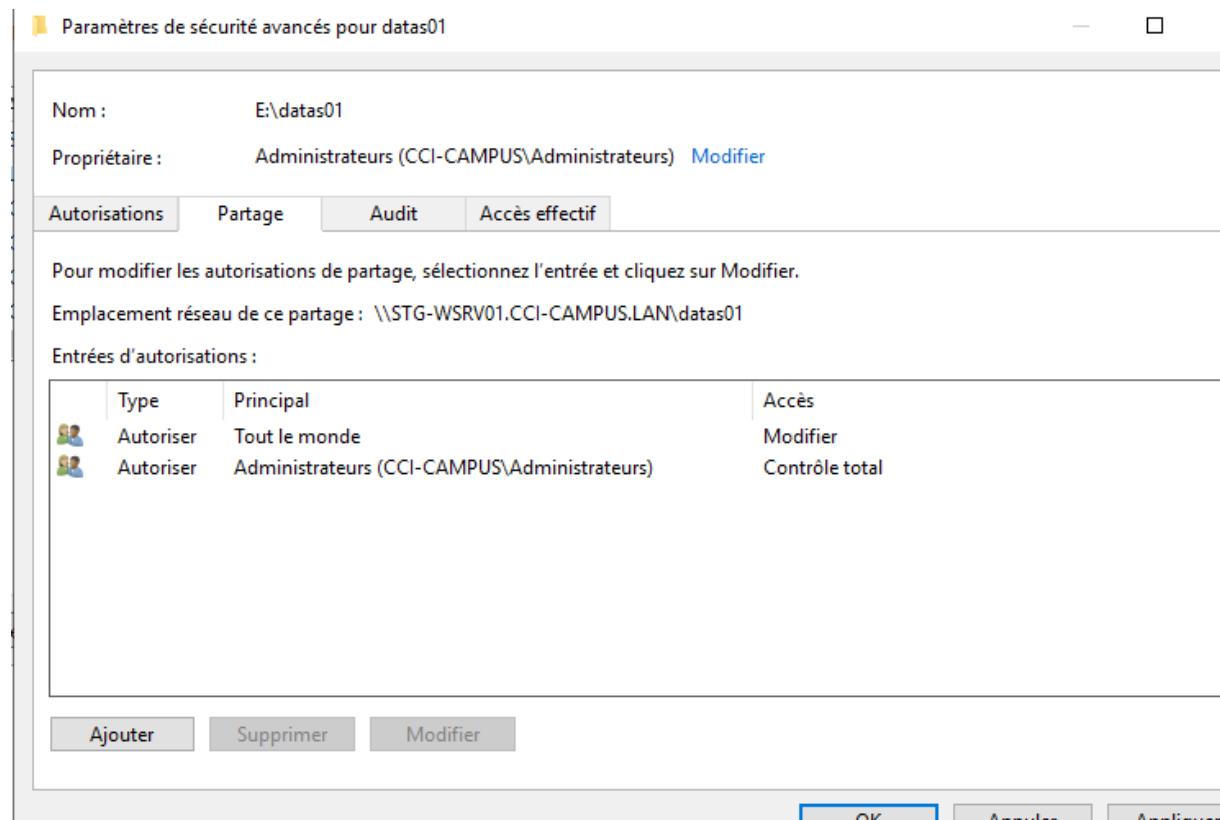
OK

Annuler

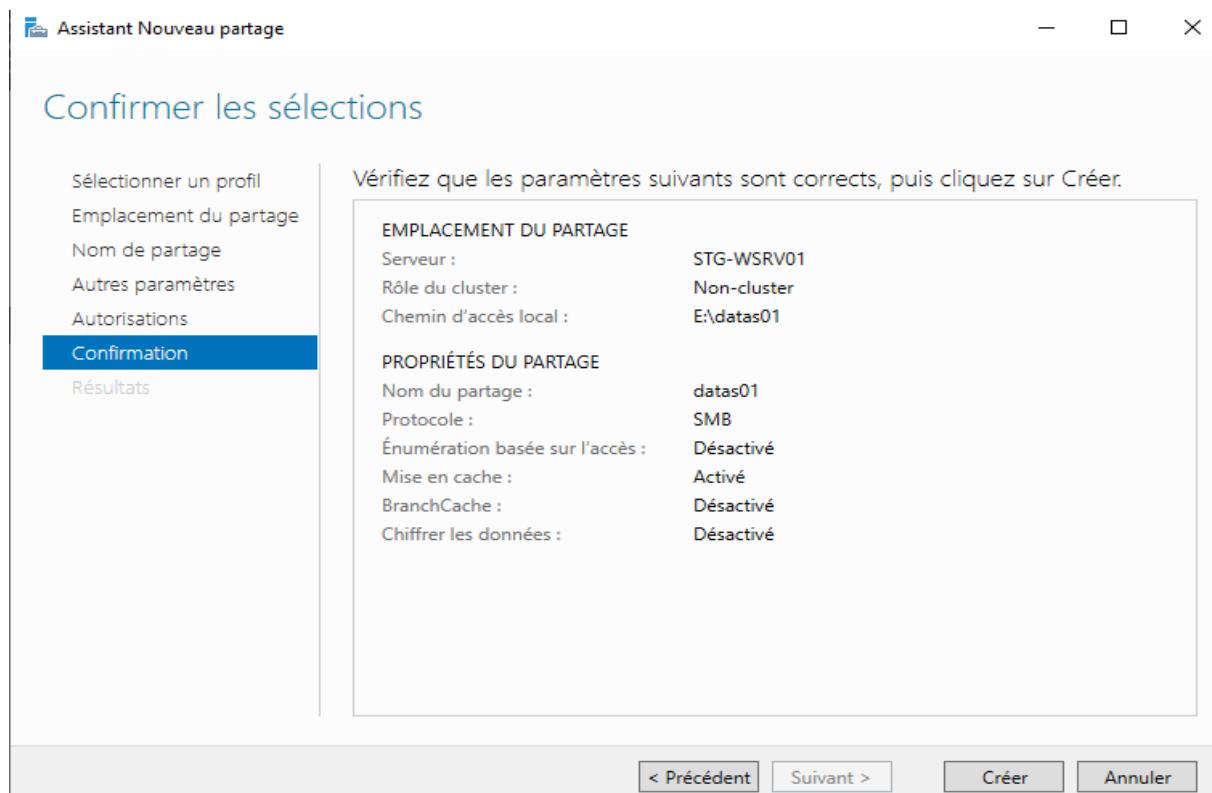
Appliquer

Ajouter le groupe administrateur et accorder lui le contrôle total, de cette manière les admins du domaine pourront le gérer sans soucis.

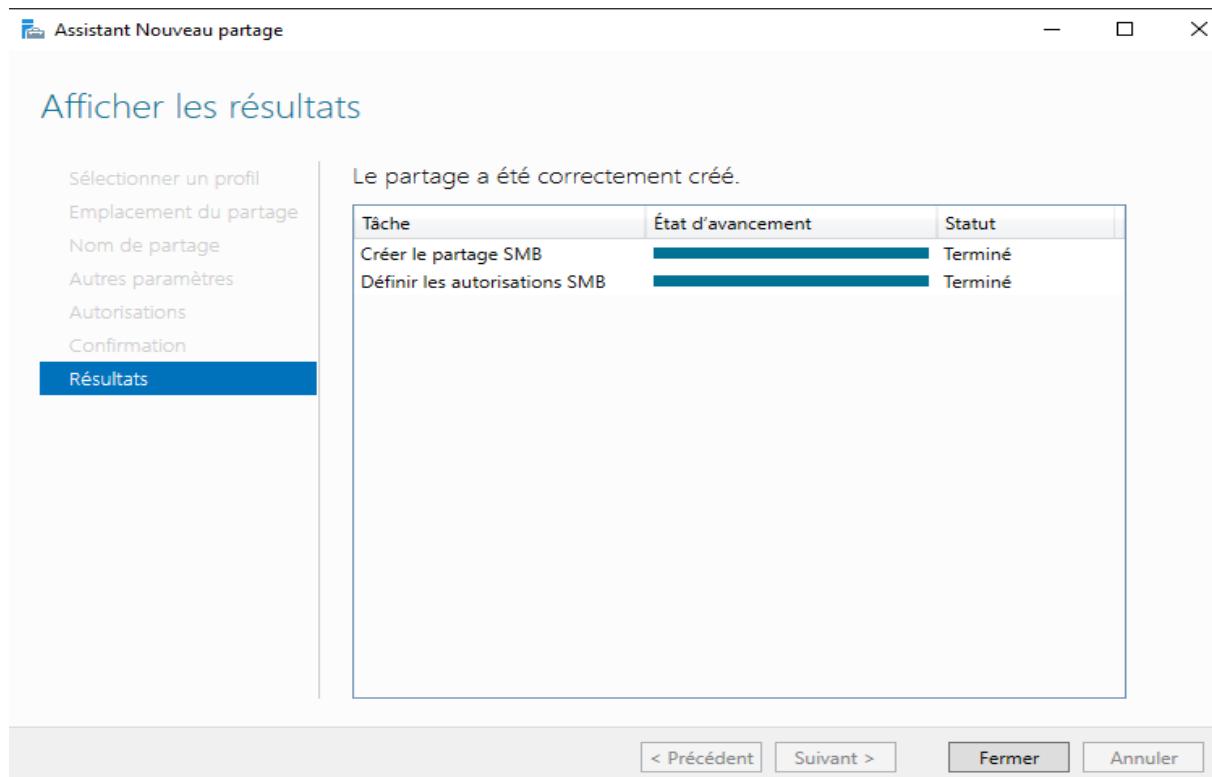
De plus pour le groupe « tout le monde » accorder uniquement les droits en modification, donc lecture et écriture.



Cliquez sur « crée » afin d'initialiser le partage



Votre partage à bien été créée



Réitéré l'opération sur tous les serveurs de manière à avoir les 4 partages sur les 4 dossiers.

Une fois les 4 partage crée, ils devraient s'afficher de la manière ci-contre dans la partie dossier partagé du gestionnaire de serveur

► MUL-SRVW02 (4)

DFS	C:\DFSRoots\DFS	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
datas04	E:\datas04	SMB	Non-cluster

► MUL-WSRV01 (3)

NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
datas03	B:\datas03	SMB	Non-cluster

► STG-SRVW02 (3)

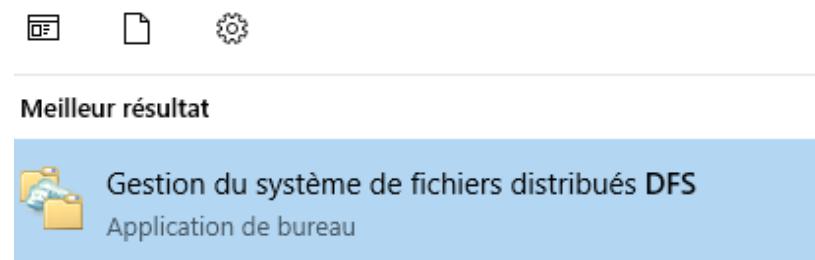
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
datas02	B:\datas02	SMB	Non-cluster

► STG-WSRV01 (3)

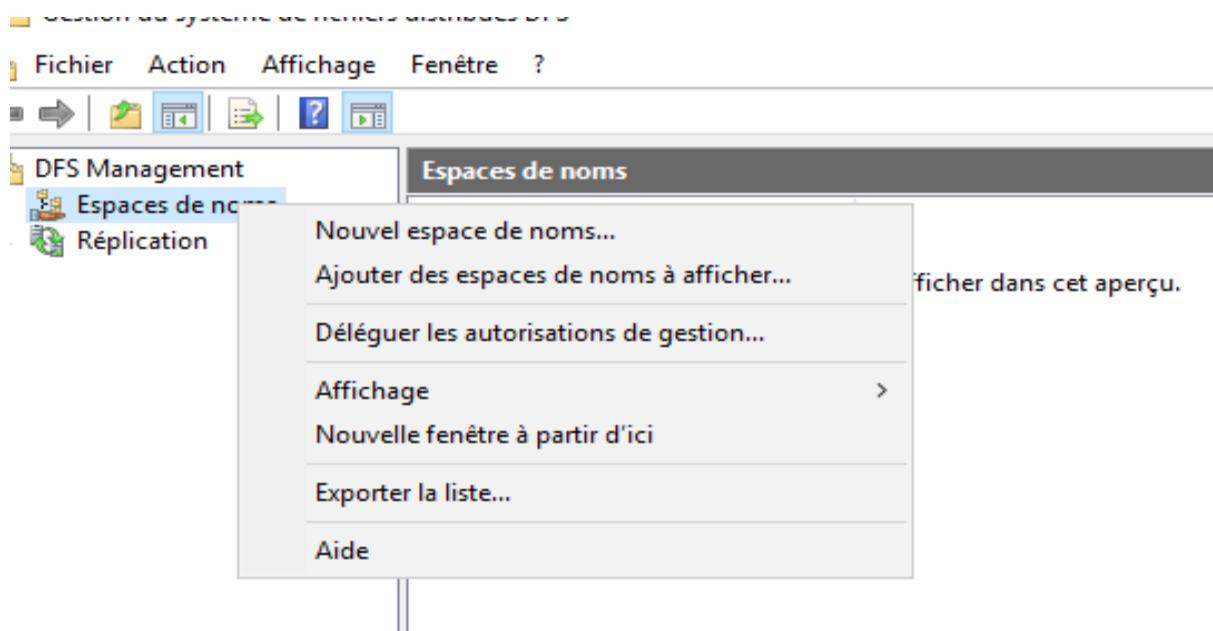
NETLOGON	C:\Windows\SYSVOL\sysvol\CCI-C...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
datas01	E:\datas01	SMB	Non-cluster

3.6.3 Configuration espace de nom et réPLICATION :

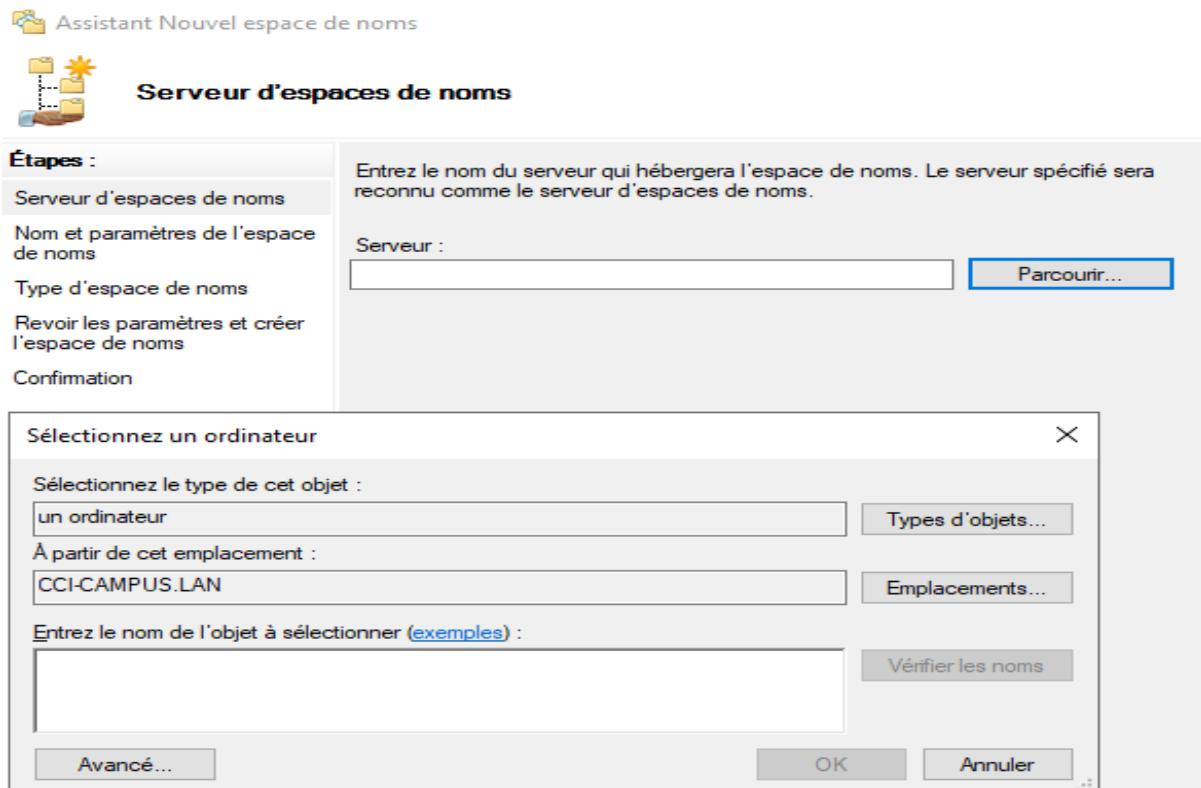
Pour la suite, rendez-vous dans l'applicatif gestion du système de fichier distribués DFS dans l'explorateur Windows



Faites un clic droit sur espaces de nom et faites nouvel espace de nom

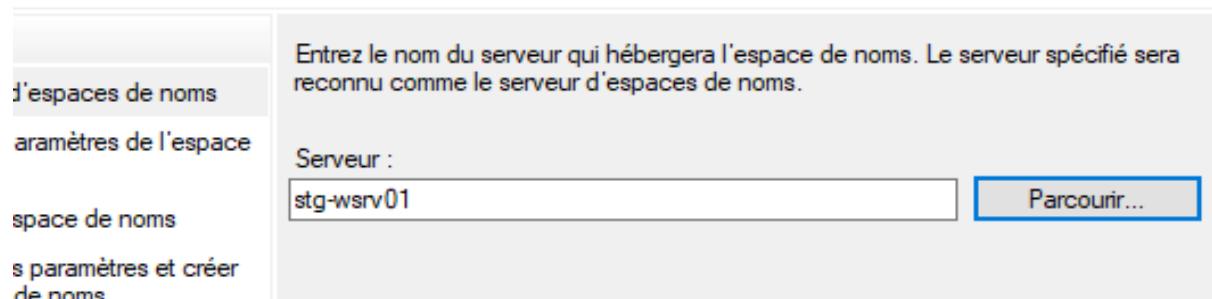


Chercher à l'aide de l'outil de recherche et Sélectionner le serveur qui hébergera l'espace de nom, ici STG-SVRW01



Une fois sélectionné faites suivant

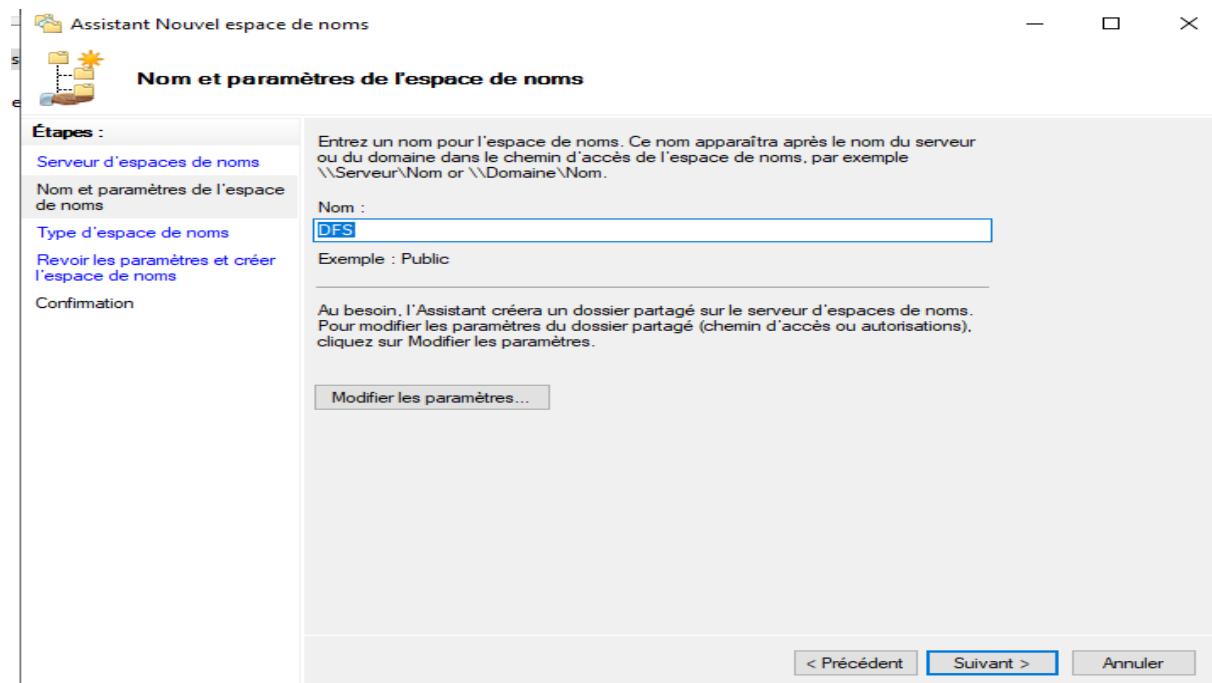
Serveur d'espaces de noms



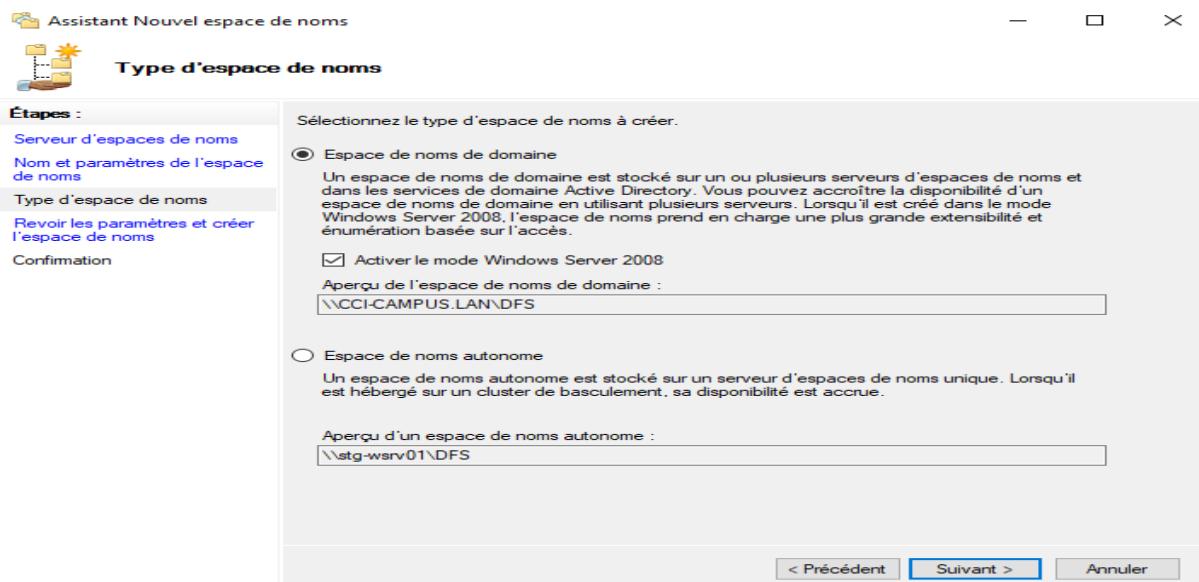
Nommée le fichier qui sera créé dans l'espace de nom et qui apparaîtra juste après lui

Ici nous avons pris DFS comme nom

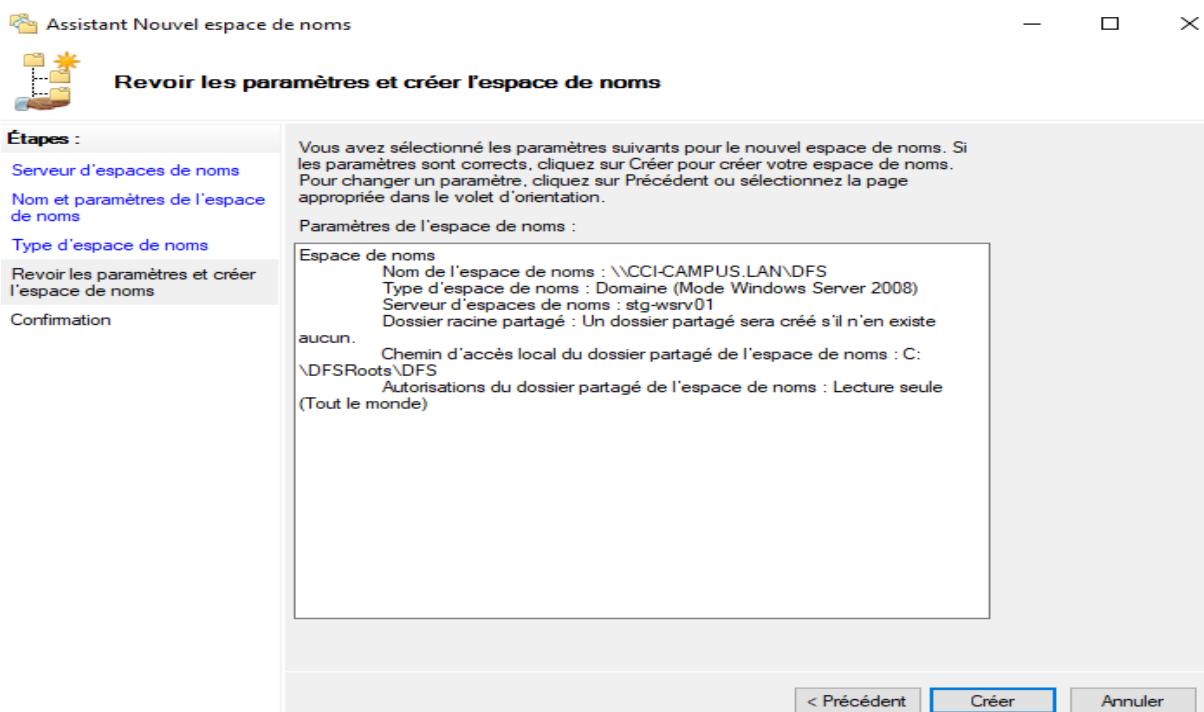
Faites « suivant »



Laisser les paramètres par défaut et faites « suivant »

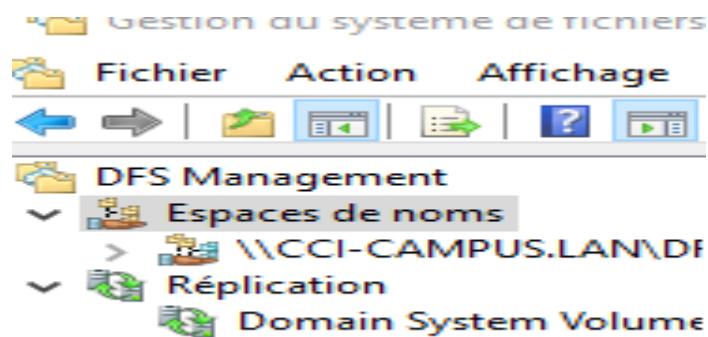


Faites « crée »



Une fois l'espace de nom créé, il apparaitra sur l'onglet Espace de nom.

Cliquez sur l'espace de nom CCI-CAMPUS.LAN



Allez dans l'onglet Serveur d'espace de nom

\CCI-CAMPUS.LAN\DFS (De domaine dans Mode Windows Server 2008)

Espace de noms	Serveurs d'espaces de noms	Délégation	Rechercher
1 entrées			
Type	Statut de référence	Site	Chemin d'accès
Activé		Default-First-Site-Name	\STG-WSRV01\DFS

Puis rendez-vous à droite, et faites « ajouter un serveur d'espace de nom »

Actions

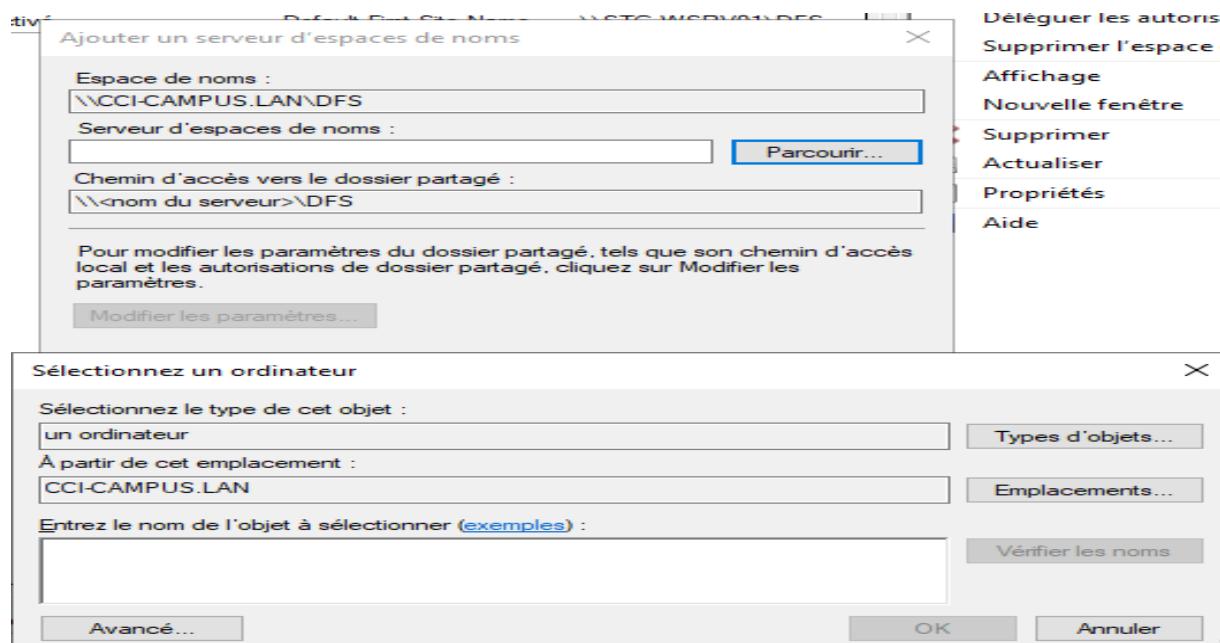
\CCI-CAMPUS.LAN\DFS

- Nouveau dossier...
- Ajouter un serveur d'espaces de noms...
- Déléguer les autorisations de gestion...
- Supprimer l'espace de noms de l'affichage...

Affichage

Faites parcourir et chercher les autres serveurs avec le nom :

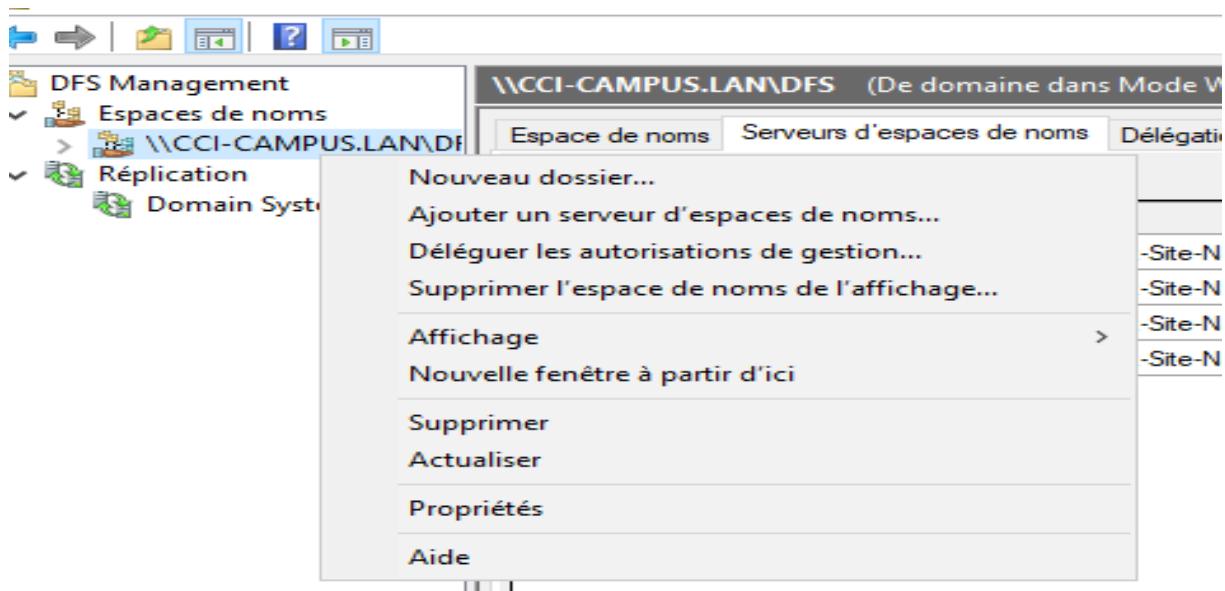
- STG-SVRW01
- STG-SVRW02
- MUL-SVRW01
- MUL-SRVW02



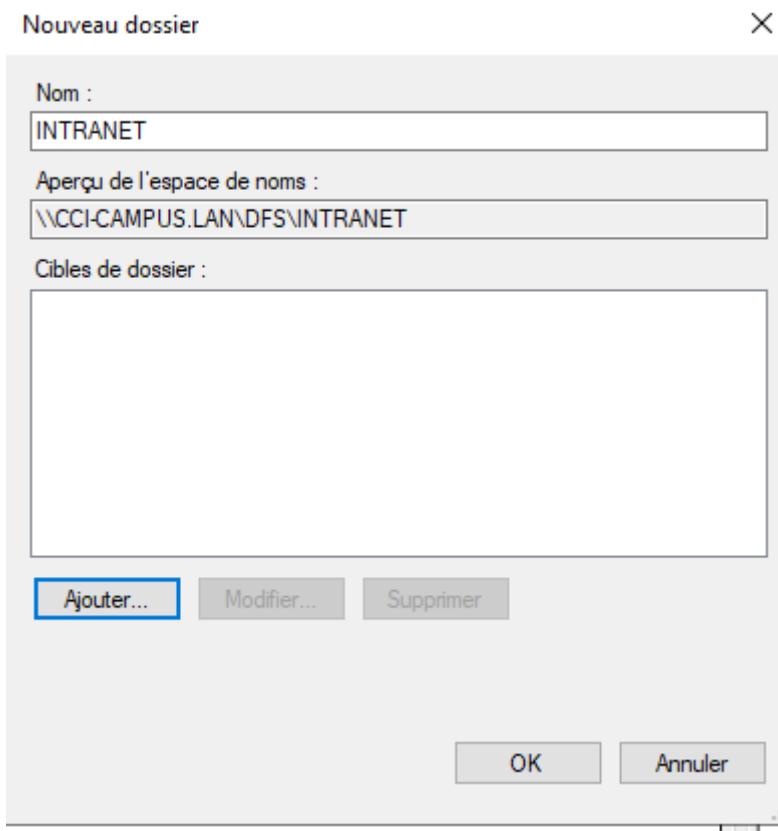
Une fois tout les serveurs ajouté l'onglet devrais ressembler à cela

\CCI-CAMPUS.LAN\INTRANET (De domaine dans Mode Windows Server 2008)			
Espace de noms	Serveurs d'espaces de noms	Délégation	Rechercher
4 entrées			
Type	Statut de référence	Site	Chemin d'accès
dossier	Activé	Default-First-Site-Name	\MUL-SRVW02.CCI-...
dossier	Activé	Default-First-Site-Name	\MUL-WSRV01.CCI-...
dossier	Activé	Default-First-Site-Name	\STG-SRVW02.CCI-...
dossier	Activé	Default-First-Site-Name	\STG-WSRV01.CCI-...

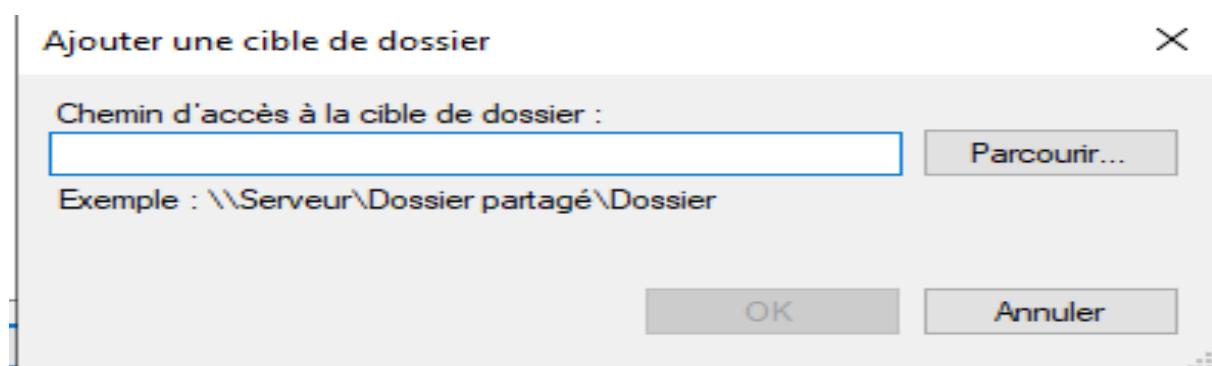
Revenez sur l'onglet de l'espace de nom DFS crée plus tôt et faites un clic droit, puis nouveau dossier



Nommez ce dossier INTRANET et cliquez sur ajouter afin d'ajouter les différents dossiers

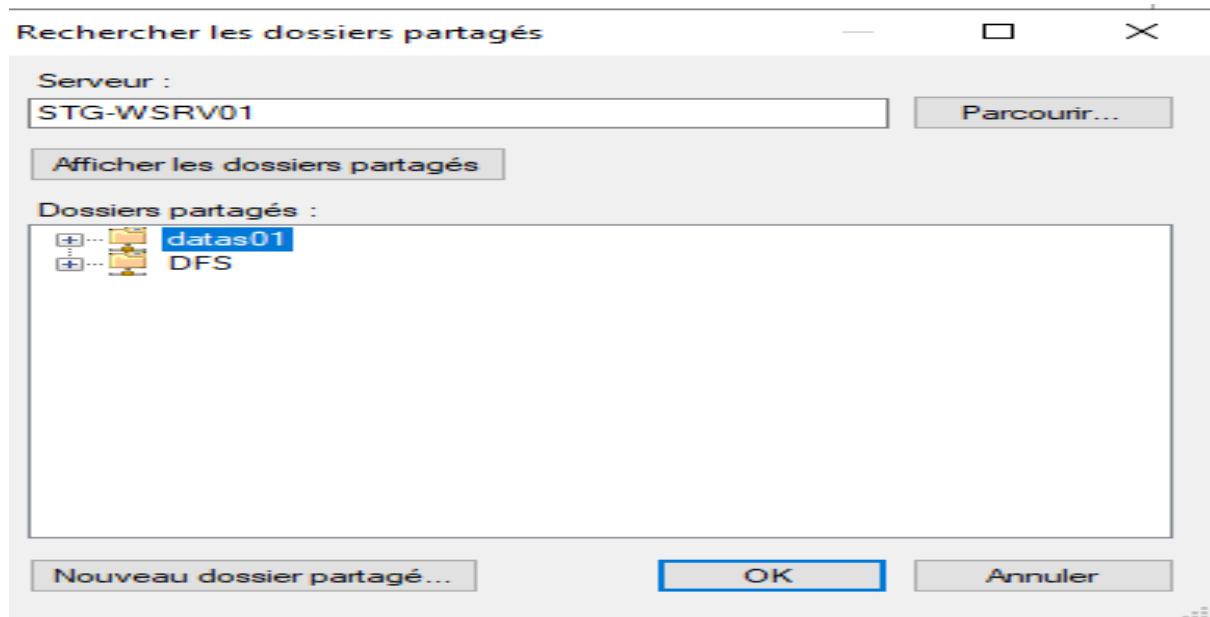


Cliquez sur parcourir pour chercher le dossier à ajouter

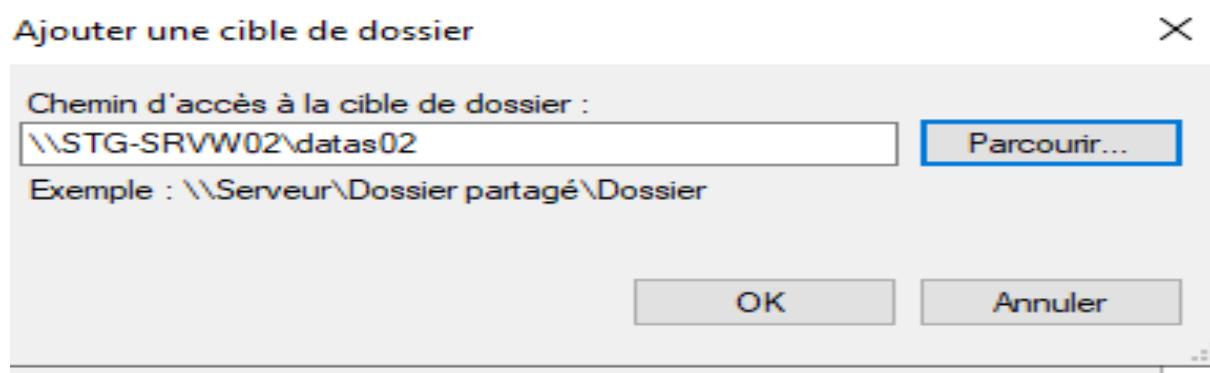


Allez dans parcourir à nouveau pour chercher le serveur voulu

Puis une fois celui-ci sélectionner, cliquez sur le dossier ayant pour plan de nommage datasXX et faites «OK»



Faites ok pour ajouter la cible de dossier partagé

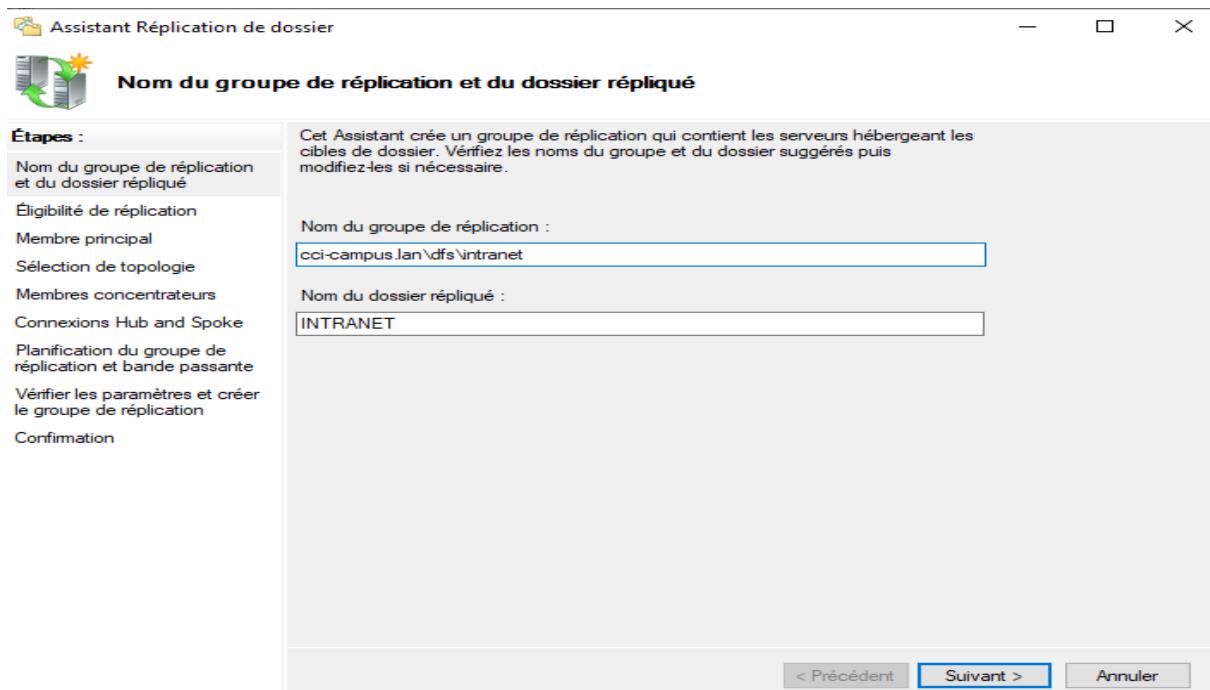


Important : Réitéré l'action pour chacun des 4 dossier répartie sur les 4 serveurs

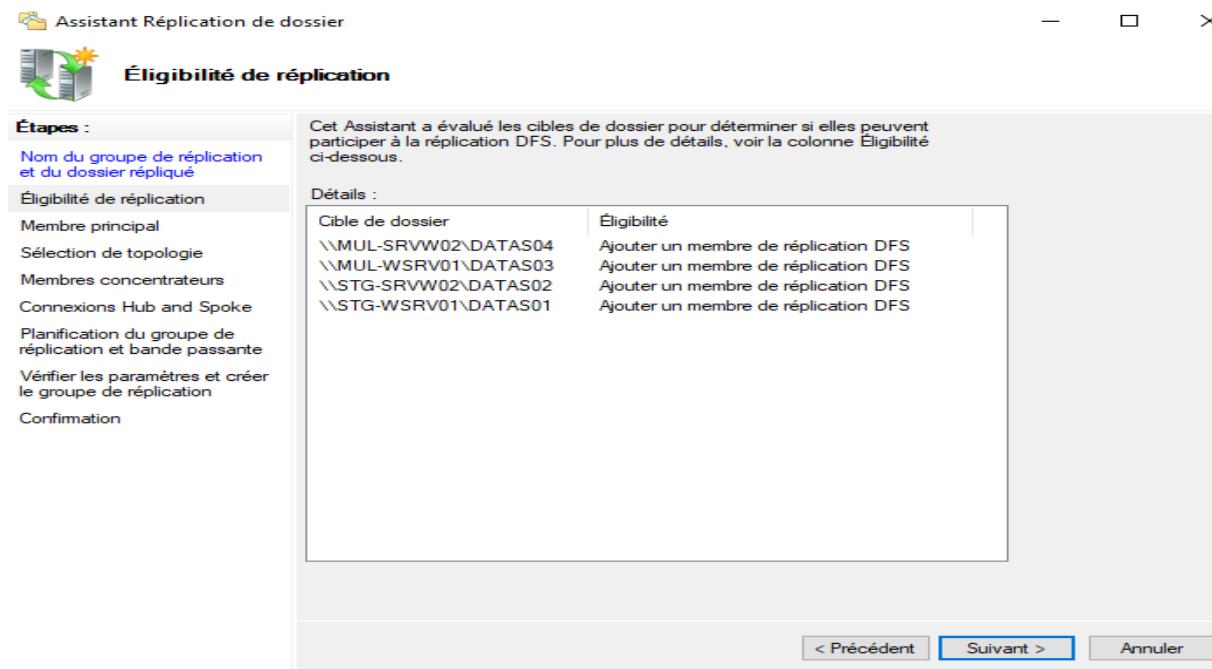
Une fois les 4 ajouté faites «suivant» et il vous sera proposé de crée un groupe de réPLICATION.

Faites «OK» et cette page s'afficheras

Donner le nom du fichier intranet crée précédemment et faites «suivant»

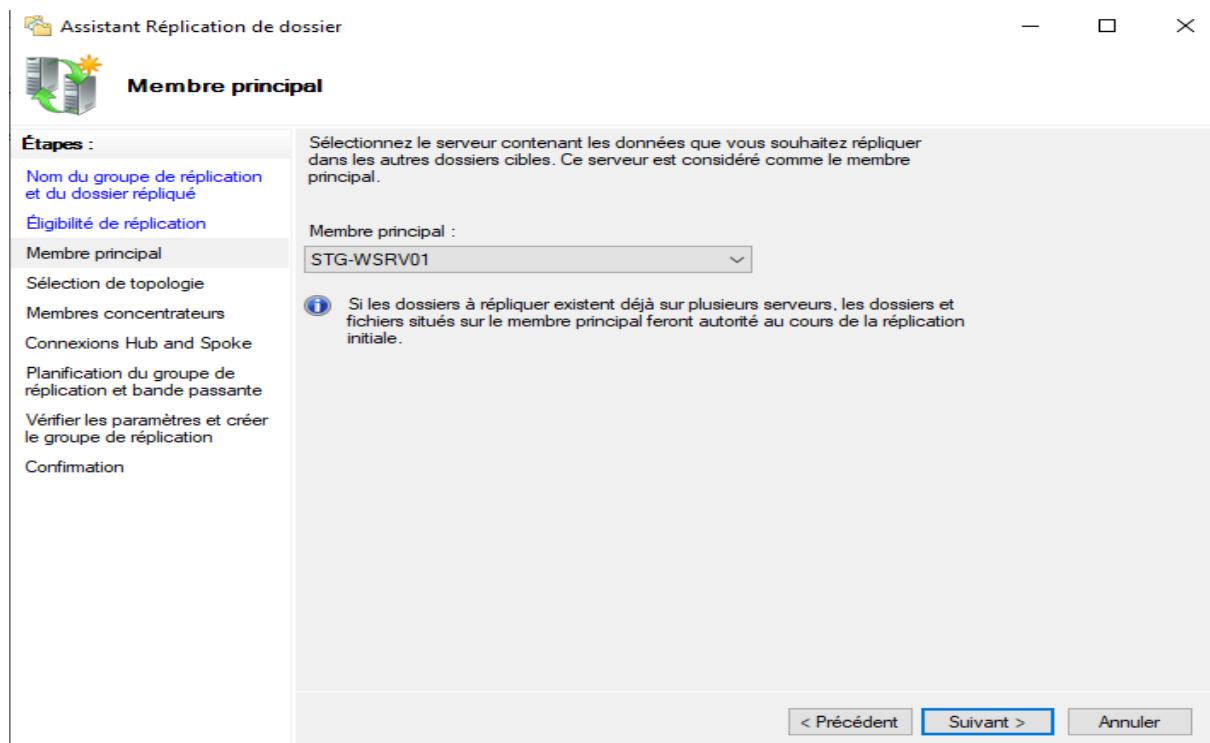


Les cibles de dossier crée précédemment serons listé, faites simplement «suivant»

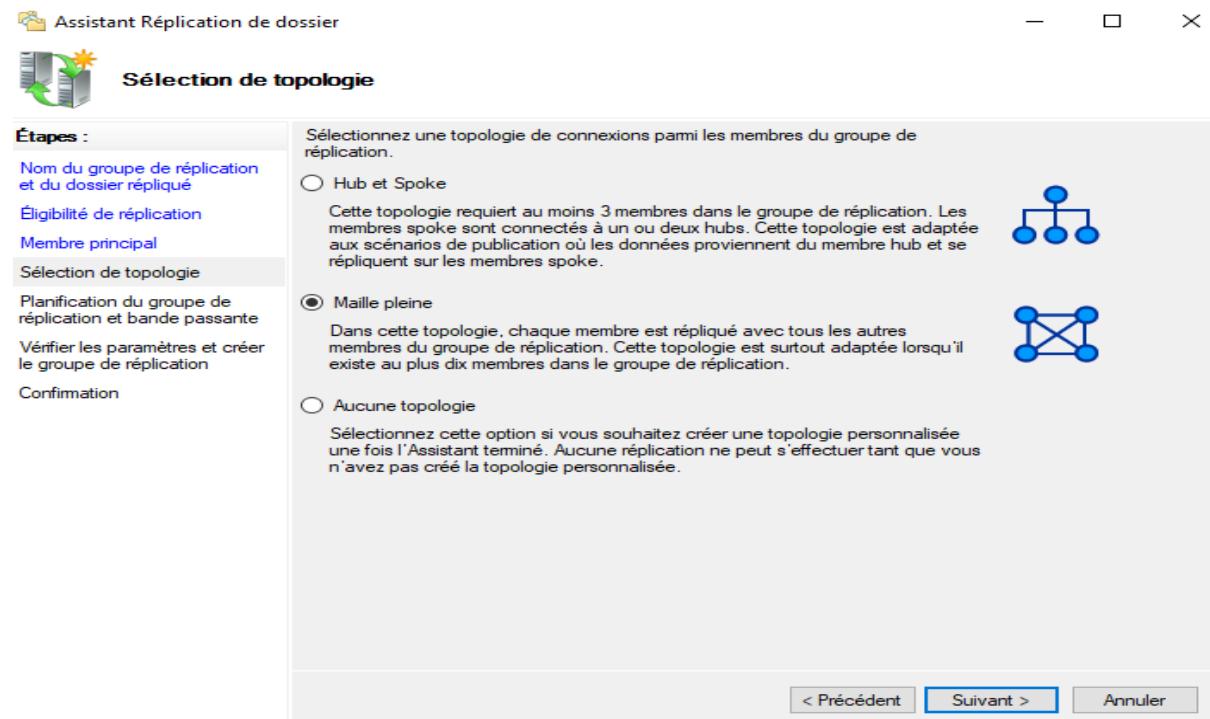


Choisissez le membre principal du dossier de réplication. Nous prendrons le serveur principal de Strasbourg, comme le montre l'image ci-contre

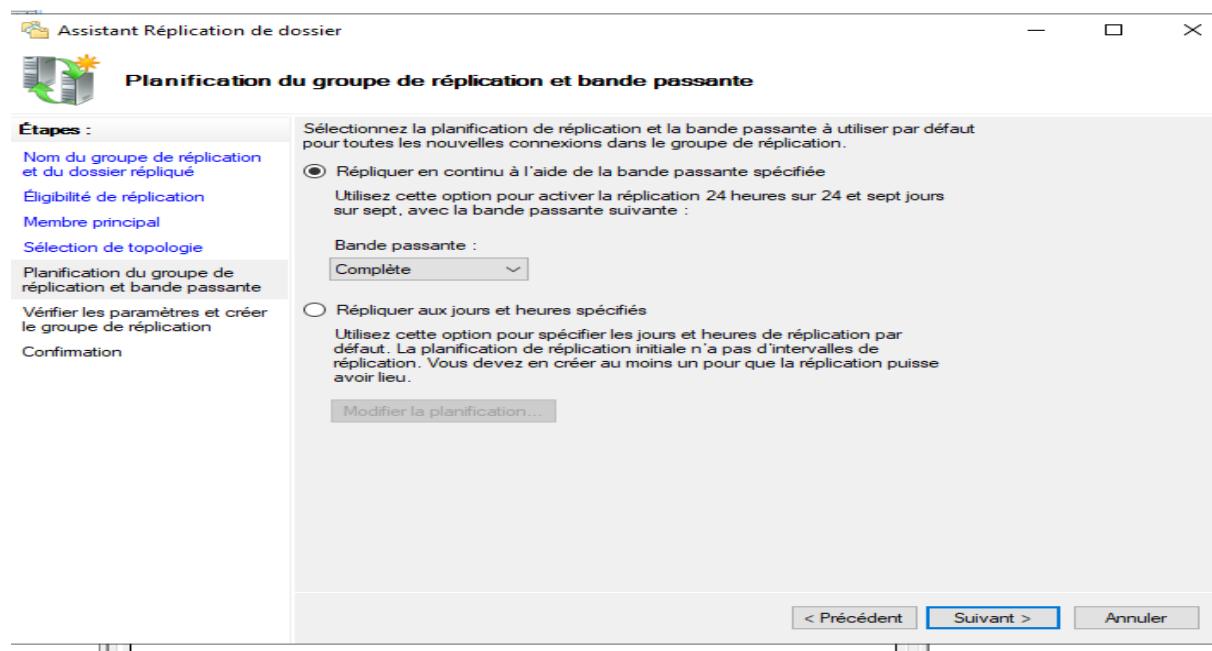
Faites « »suivant» »



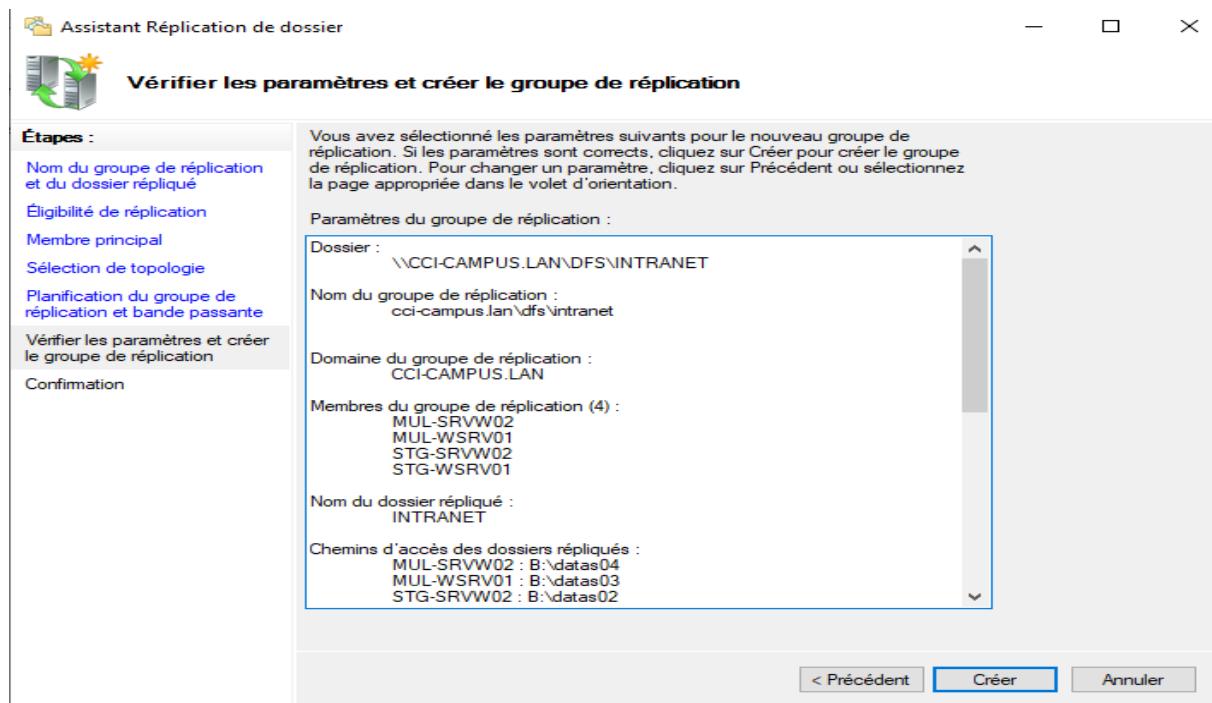
Sélectionner une topologie en maille pleine et faites « suivant »



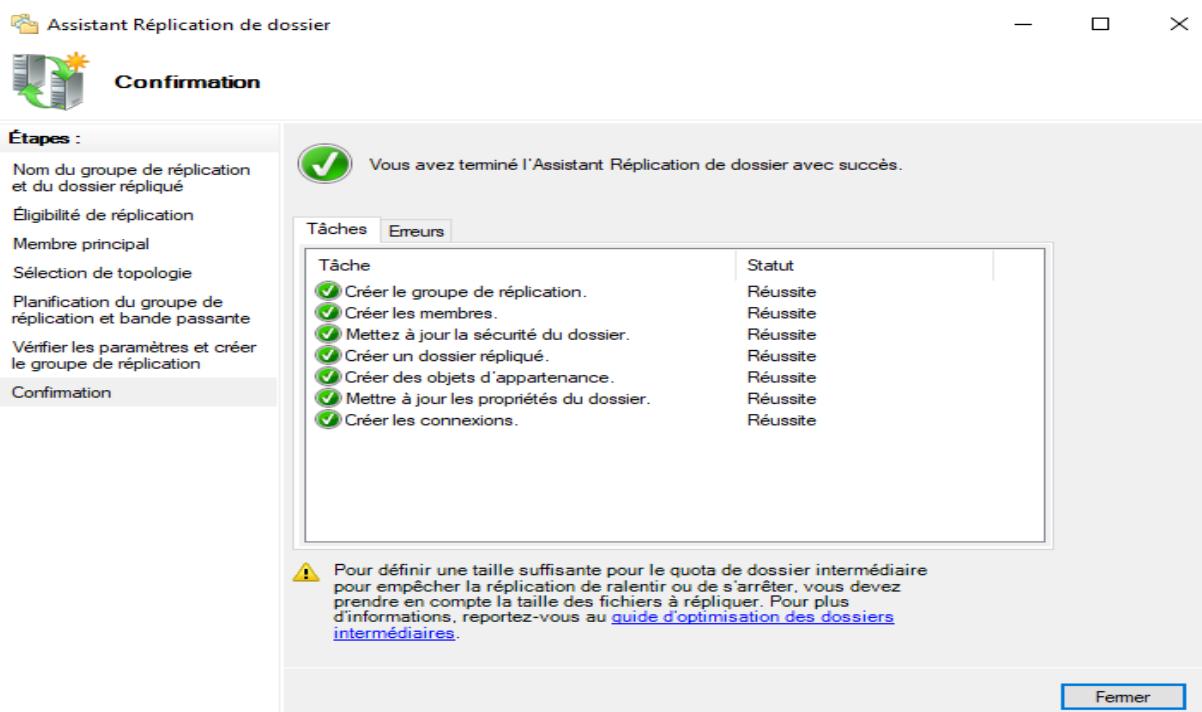
Laissez les paramètres par défaut et faites «suivant»



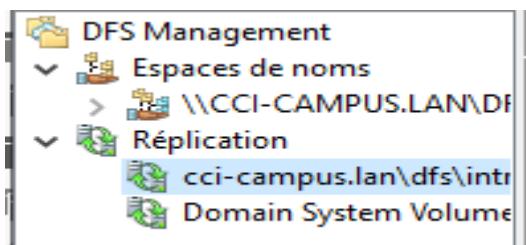
Cliquez sur «crée»



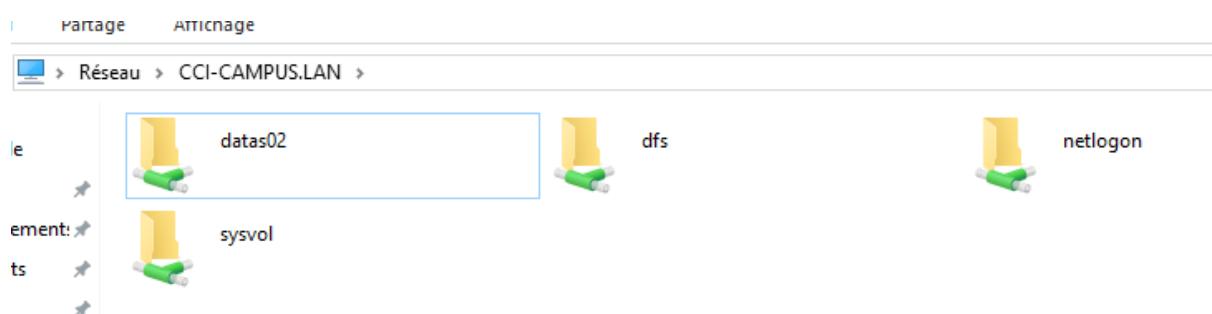
Votre réPLICATION à bien été créée



La réPLICATION apparaîtra elle aussi dans l'onglet de l'applicatif DFS



Nous pouvons voir qu'en chercher notre espace de nom nous avons bien le fichier DFS qui apparaît



Nous pouvons aussi voir que toutes les liaisons entre le dossier ont été correctement effectuer.

Vous pouvez retrouver ce paramètre dans l'applicatif DFS et sur la réPLICATION créée.

Appartenances Connexions Dossiers répliqués Délégation							
12 entrées							
État	Membre d'envoi	/	Statut de la connexion	Site d'envoi	Membre de réception	Type de planification	Site de réception
▀ Membre d'envoi : MUL-SRVW02 (3 éléments)							
	MUL-SRVW02	Activée	Default-First-Site-Name	MUL-WSRV01	Planification du groupe ...	Default-First-Site-Name	
	MUL-SRVW02	Activée	Default-First-Site-Name	STG-SRVW02	Planification du groupe ...	Default-First-Site-Name	
	MUL-SRVW02	Activée	Default-First-Site-Name	STG-WSRV01	Planification du groupe ...	Default-First-Site-Name	
▀ Membre d'envoi : MUL-WSRV01 (3 éléments)							
	MUL-WSRV01	Activée	Default-First-Site-Name	MUL-SRVW02	Planification du groupe ...	Default-First-Site-Name	
	MUL-WSRV01	Activée	Default-First-Site-Name	STG-SRVW02	Planification du groupe ...	Default-First-Site-Name	
	MUL-WSRV01	Activée	Default-First-Site-Name	STG-WSRV01	Planification du groupe ...	Default-First-Site-Name	
▀ Membre d'envoi : STG-SRVW02 (3 éléments)							
	STG-SRVW02	Activée	Default-First-Site-Name	MUL-SRVW02	Planification du groupe ...	Default-First-Site-Name	
	STG-SRVW02	Activée	Default-First-Site-Name	MUL-WSRV01	Planification du groupe ...	Default-First-Site-Name	
	STG-SRVW02	Activée	Default-First-Site-Name	STG-WSRV01	Planification du groupe ...	Default-First-Site-Name	
▀ Membre d'envoi : STG-WSRV01 (3 éléments)							
	STG-WSRV01	Activée	Default-First-Site-Name	MUL-SRVW02	Planification du groupe ...	Default-First-Site-Name	
	STG-WSRV01	Activée	Default-First-Site-Name	MUL-WSRV01	Planification du groupe ...	Default-First-Site-Name	
	STG-WSRV01	Activée	Default-First-Site-Name	STG-SRVW02	Planification du groupe ...	Default-First-Site-Name	

Pour tester, nous allons crée un fichier test sur le dossier partagé Datas01

Nom	Modifié le	Type	Taille
test	29/12/2022 20:01	Document texte	0 Ko

Après plusieurs minutes d'attentes nous pouvons voir que le fichier se trouve bien dans l'espace de nom

Nom	Modifié le	Type	Taille
test	29/12/2022 20:01	Document texte	0 Ko

Et qu'il se trouve dans les autres dossiers partagés, il a donc bien été répliqué

Partage	Affichage
Réseau > 192.168.100.3 > datas02	
Nom	Modifié le
test	29/12/2022 20:01
Type	Taille
Document texte	0 Ko

3.7 Mise en place de RADIUS

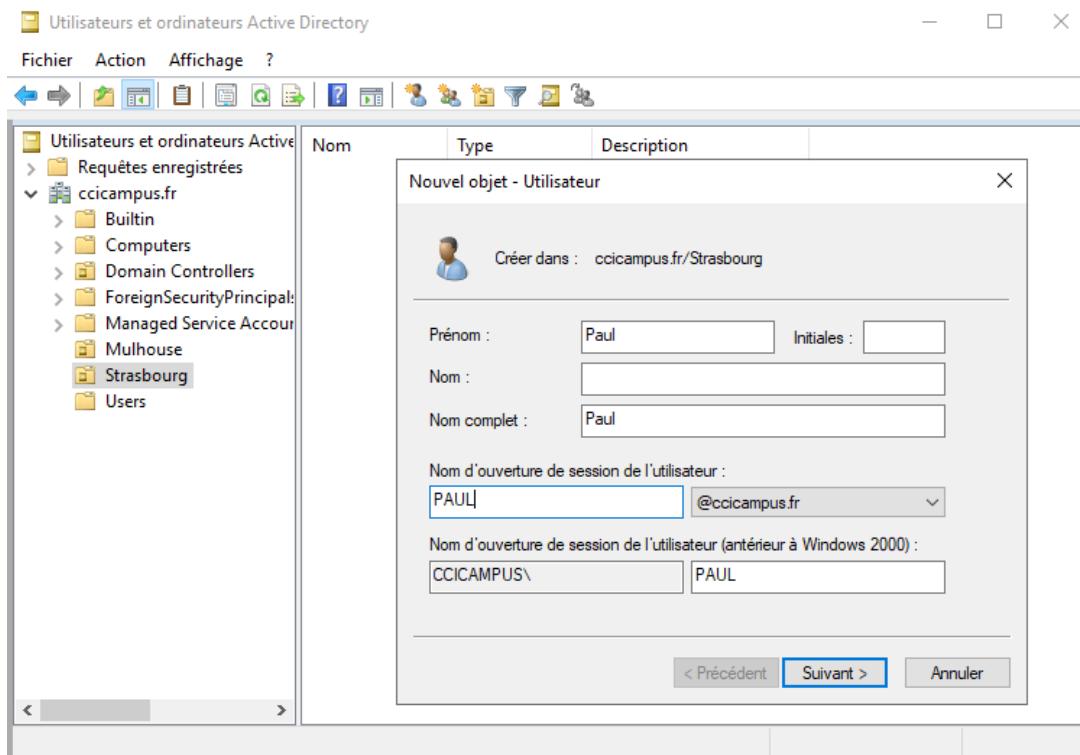
Dans cette partie, seul la mise en place du RADIUS sera démontrée. Cependant, il se complète avec la configuration d'un portail captif. Je vous invite à consulter la partie dédiée au ce sujet-là.

3.7.1 Création des utilisateurs

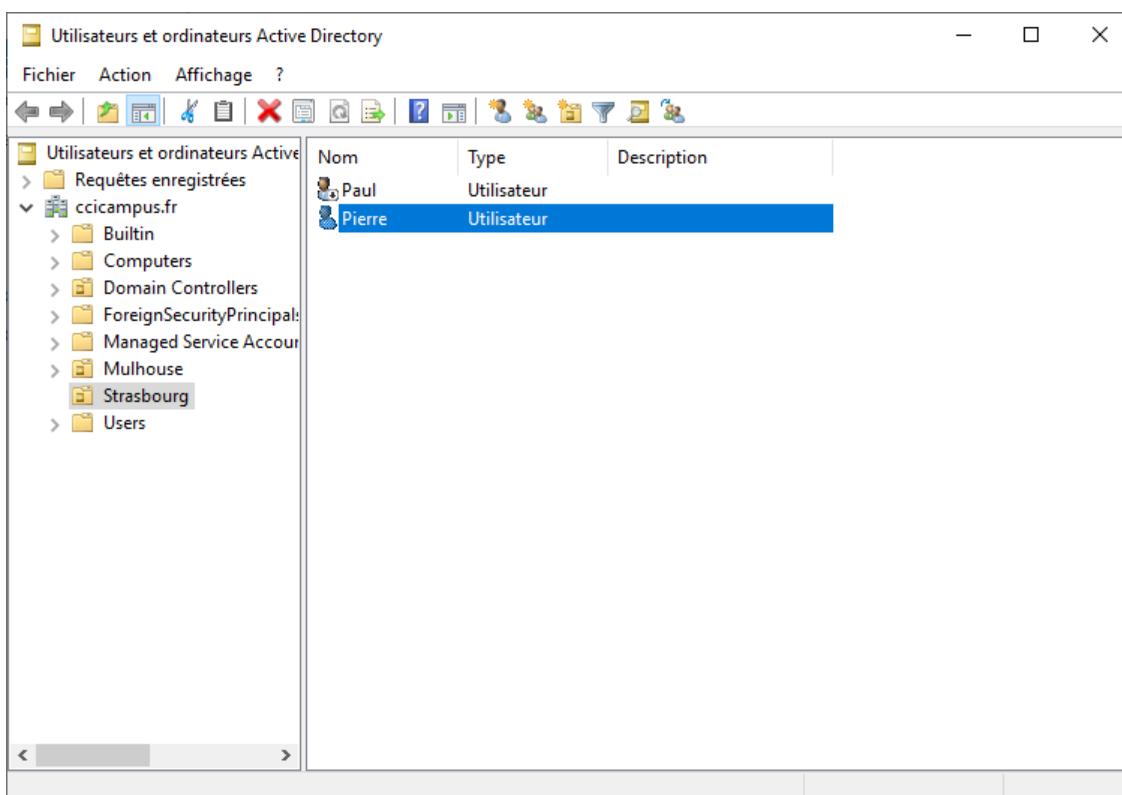
Afin de tester par la suite si un utilisateur peut se connecter avec l'authentification par RADIUS, il faut créer des utilisateurs :

The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane displays the structure of the Active Directory, including the root node 'Utilisateurs et ordinateurs Active' and a specific domain 'ccicampus.fr' which is expanded to show 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', 'Mulhouse', and 'Strasbourg'. A context menu is open over the 'Mulhouse' container, listing options like 'Délégation de contrôle...', 'Déplacer...', and 'Rechercher...'. Below this, a larger secondary context menu is displayed, listing various object types: 'Nouveau' (with 'Ordinateur' as the first option), 'Toutes les tâches', 'Couper', 'Supprimer', 'Renommer', 'Actualiser', 'Propriétés', 'Aide', and 'Utilisateur'. The 'Utilisateur' option is highlighted with a red rectangle.

Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Domain Con...	Unité d'organis...	Default container for do...
ForeignSecur...	Conteneur	Default container for sec...
Managed Se...	Conteneur	Default container for ma...
Mulhouse	Unité d'organis...	
Strasbourg	Unité d'organis...	



Pareil pour Pierre



On fait la même chose pour les utilisateurs de Mulhouse :

Nouvel objet - Utilisateur

Créer dans : ccicampus.fr/Mulhouse

Prénom :	Isabelle	Initiales :	
Nom :			
Nom complet :	Isabelle		
Nom d'ouverture de session de l'utilisateur :			
ISABELLE		@ccicampus.fr	
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
CCICAMPUS\		ISABELLE	

< Précédent Suivant > Annuler

Pareil pour Nathalie :

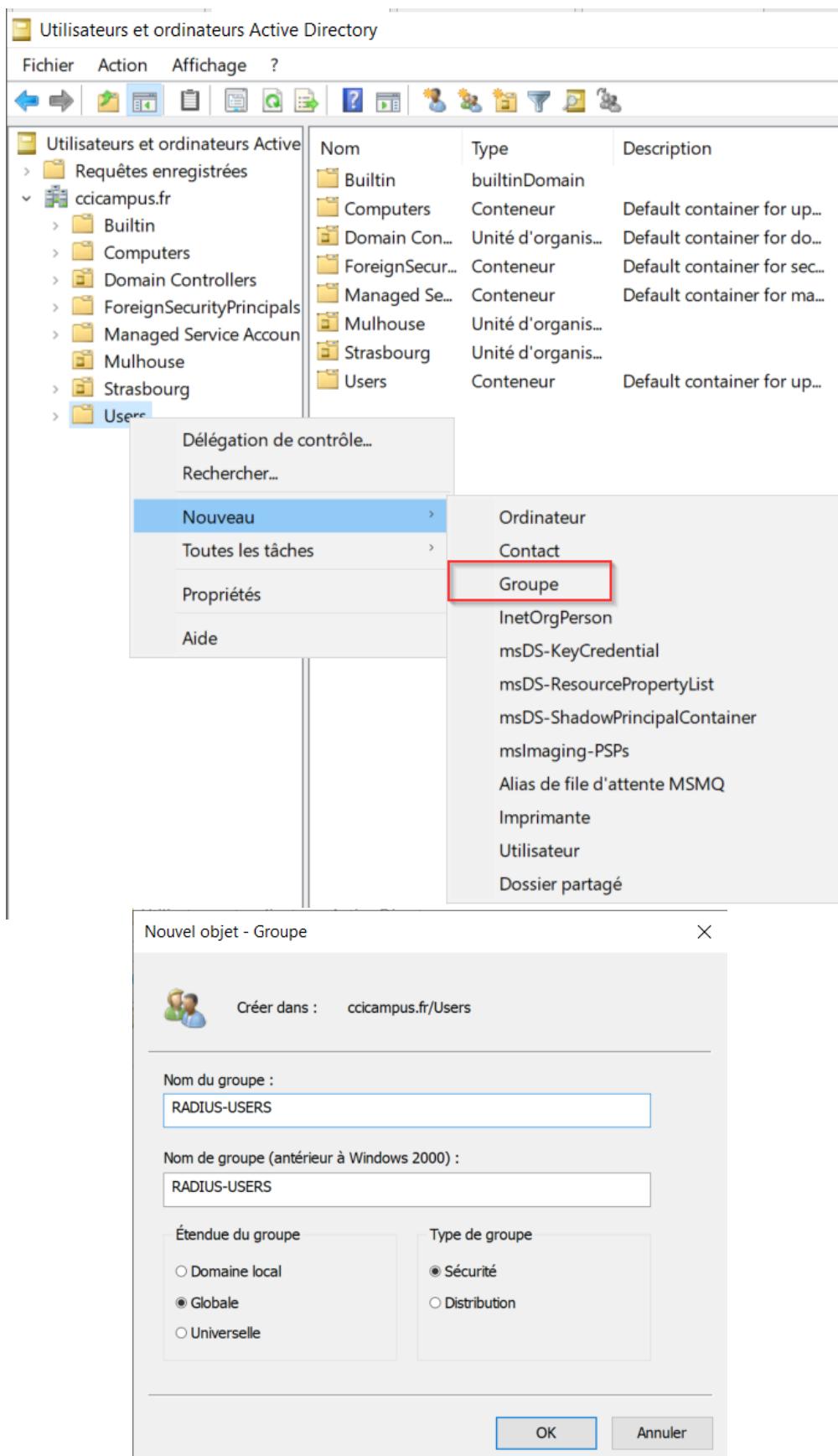
Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom	Type	Description
Isabelle	Utilisateur	
Nathalie	Utilisateur	

3.7.2 Création du groupe RADIUS

Une fois les utilisateurs créés, passons à la création du groupe :



Le groupe créé, on peut y ajouter des membres :

The screenshot shows the 'Propriétés de : RADIUS-USERS' dialog box. On the left, there's a sidebar with 'Ajouter...' and 'Supprimer' buttons. On the right, a search interface is displayed with fields for 'Nom' (Name) and 'Description', and checkboxes for 'Comptes désactivés' (Disabled accounts) and 'Mot de passe sans date d'expiration' (Password never expires). Below the search interface is a table titled 'Résultats de la recherche' (Search results) containing a list of users and their details. The user 'Isabelle' is selected in the list.

Nom	Adresse de mes...	Description	Dossier
Invités du domaine	Tous les invité...		ccicampus.fr/Users
Isabelle			ccicampus.fr/Mul...
Nathalie			ccicampus.fr/Mul...
Ordinateurs du domaine	Toutes les statio...		ccicampus.fr/Users
Paul			ccicampus.fr/Str...
Pierre			ccicampus.fr/Str...
Propriétaires créateurs de l...	Les membres de...		ccicampus.fr/Users
Protected Users	Les membres de...		ccicampus.fr/Users
RADIUS-USERS			ccicampus.fr/Users
Utilisateurs du domaine	Tous les utilisate...		ccicampus.fr/Users

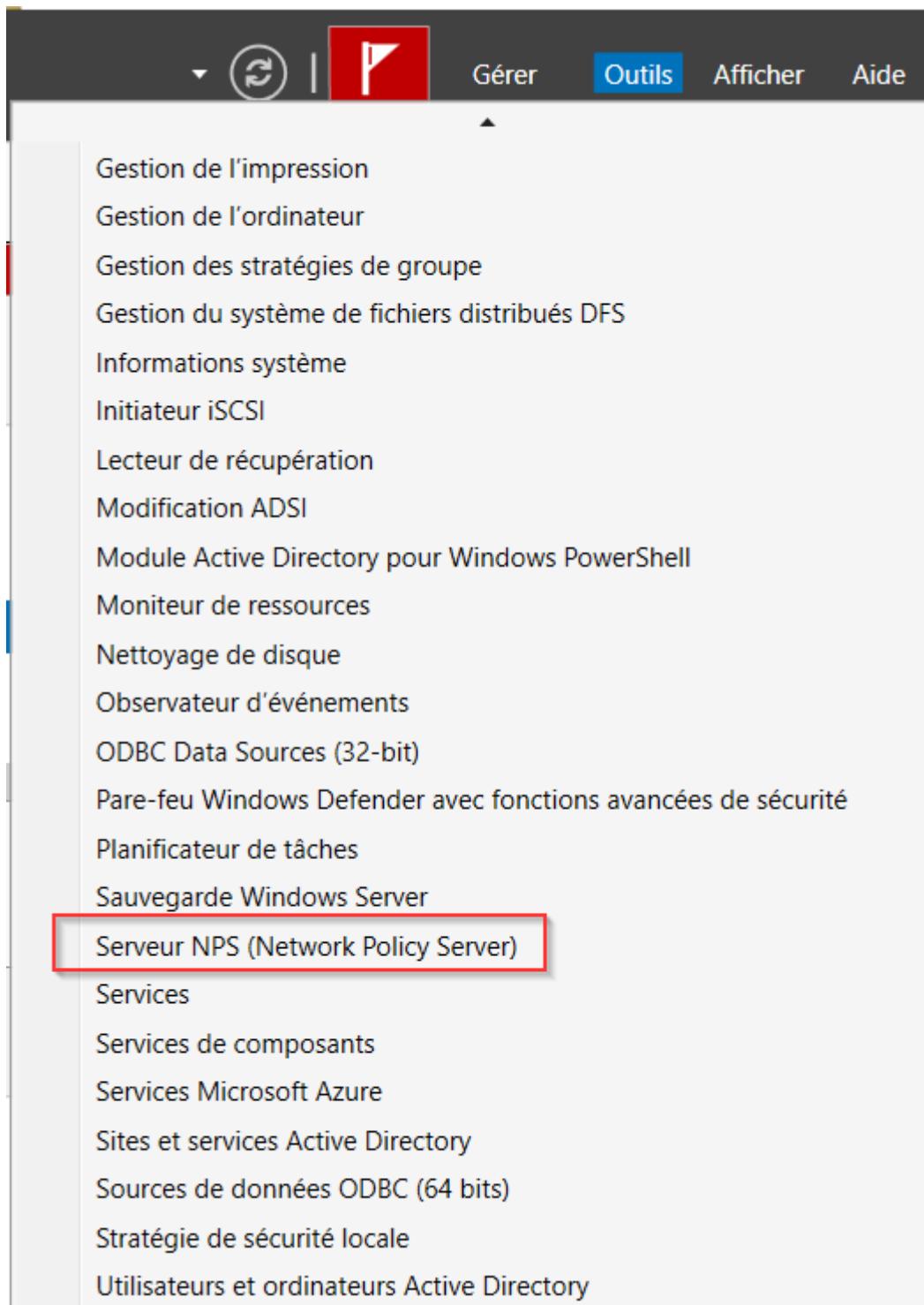
The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' management console. On the left, a tree view shows the domain structure. On the right, a detailed view of the 'RADIUS-USERS' group properties is shown. The 'Membres' tab is selected, displaying a list of members: Isabelle, Nathalie, Paul, and Pierre, each associated with a specific 'Dossier' (Container).

Nom	Dossier
Isabelle	ccicampus.fr/Mulhouse
Nathalie	ccicampus.fr/Mulhouse
Paul	ccicampus.fr/Strasbourg
Pierre	ccicampus.fr/Strasbourg

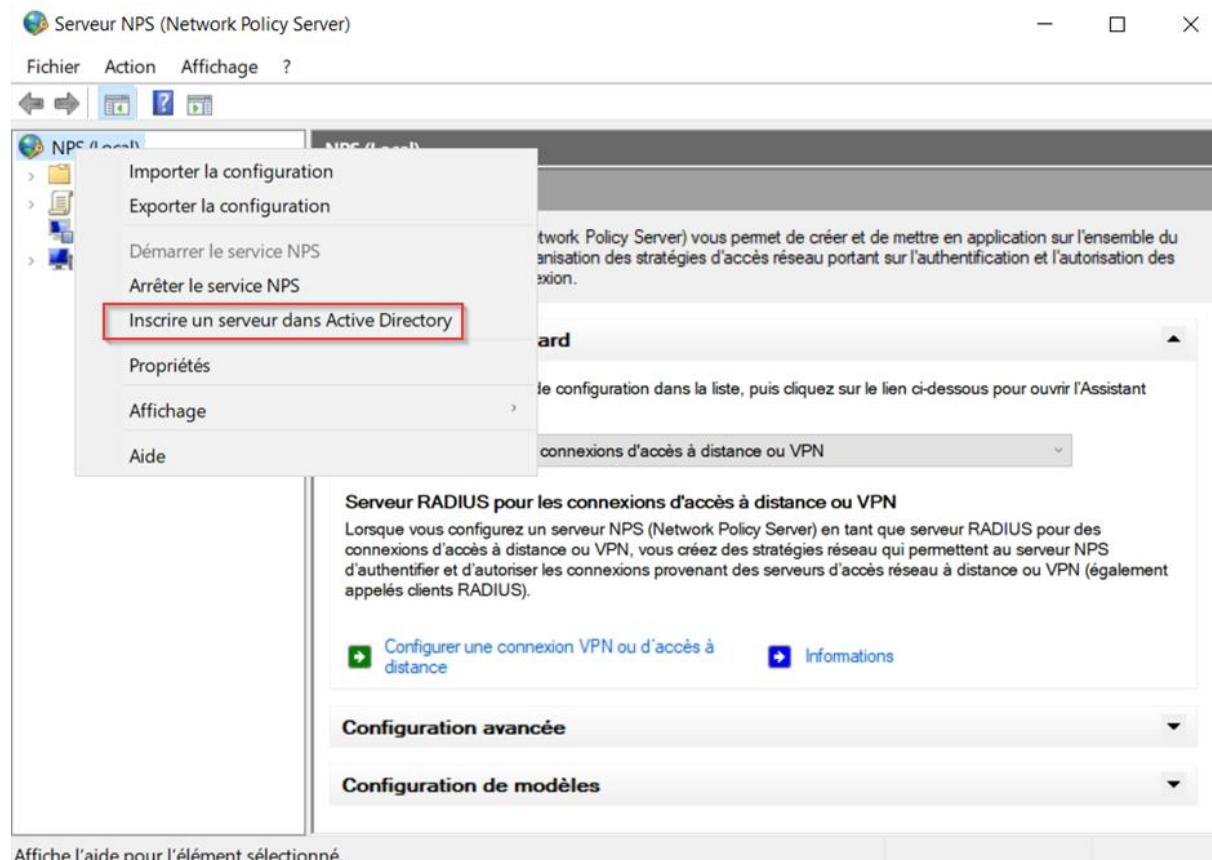
3.7.3 Inscription du serveur RADIUS dans l'AD

Maintenant que les utilisateurs et que le groupe ont été créés, nous allons pourvoir commencer à configurer le RADIUS.

Pour cela, on va se diriger vers le service prévu à cet effet :



Le gestionnaire s'ouvre puis il faut l'inscrire dans l'Active Directory. A faire de même pour les autres serveurs !

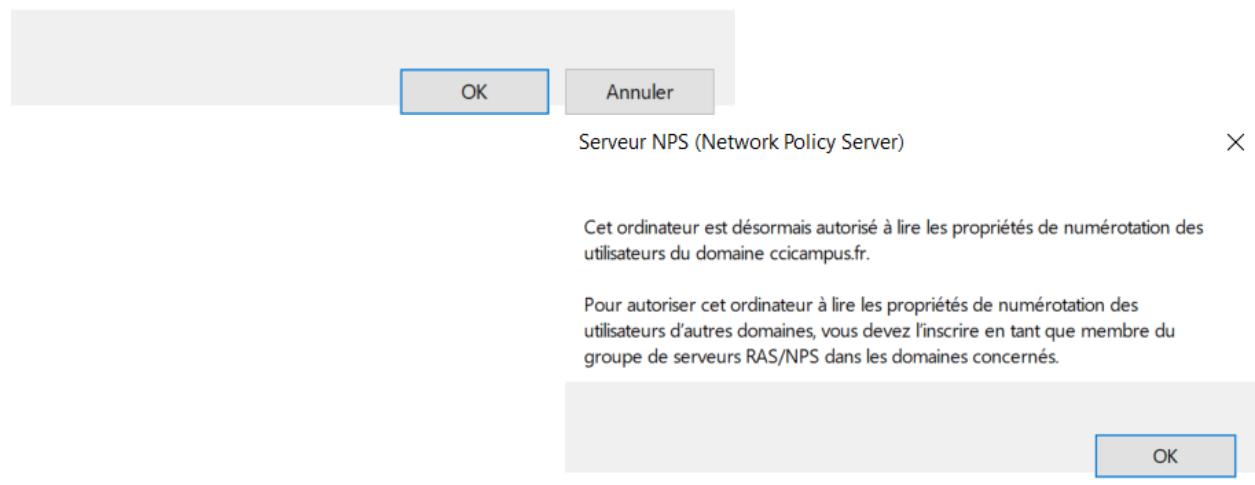


On clique sur OK :

Serveur NPS (Network Policy Server) X

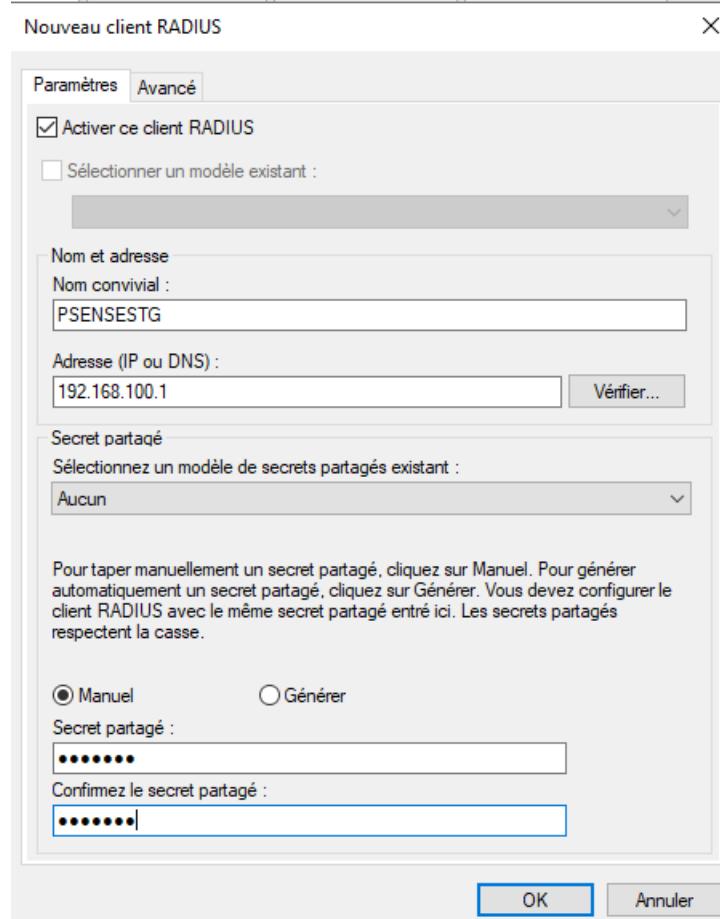
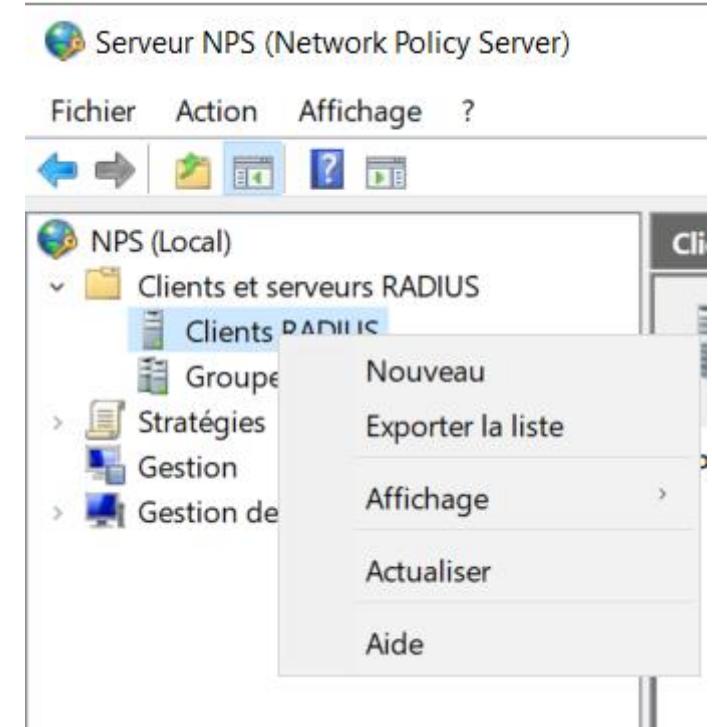
Pour permettre aux serveurs NPS (Network Policy Server) d'authentifier les utilisateurs dans Active Directory, les ordinateurs NPS doivent être autorisés à lire les propriétés de numérotation des utilisateurs du domaine.

Voulez-vous autoriser cet ordinateur à lire les propriétés de numérotation des utilisateurs du domaine ccicampus.fr ?



3.7.4 Ajout d'un client RADIUS

Notre client RADIUS sera le serveur VPN sous PFSENSE :



3.7.5 Ajout d'une nouvelle stratégie

Nouvelle stratégie réseau X

Spécifier le nom de la stratégie réseau et le type de connexion



Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :

Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Type de serveur d'accès réseau :

Spécifique au fournisseur :

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

On choisit le groupe d'utilisateur créé préalablement qui leur permettra de se connecter :

Nouvelle stratégie réseau X

Spécifier les conditions



Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

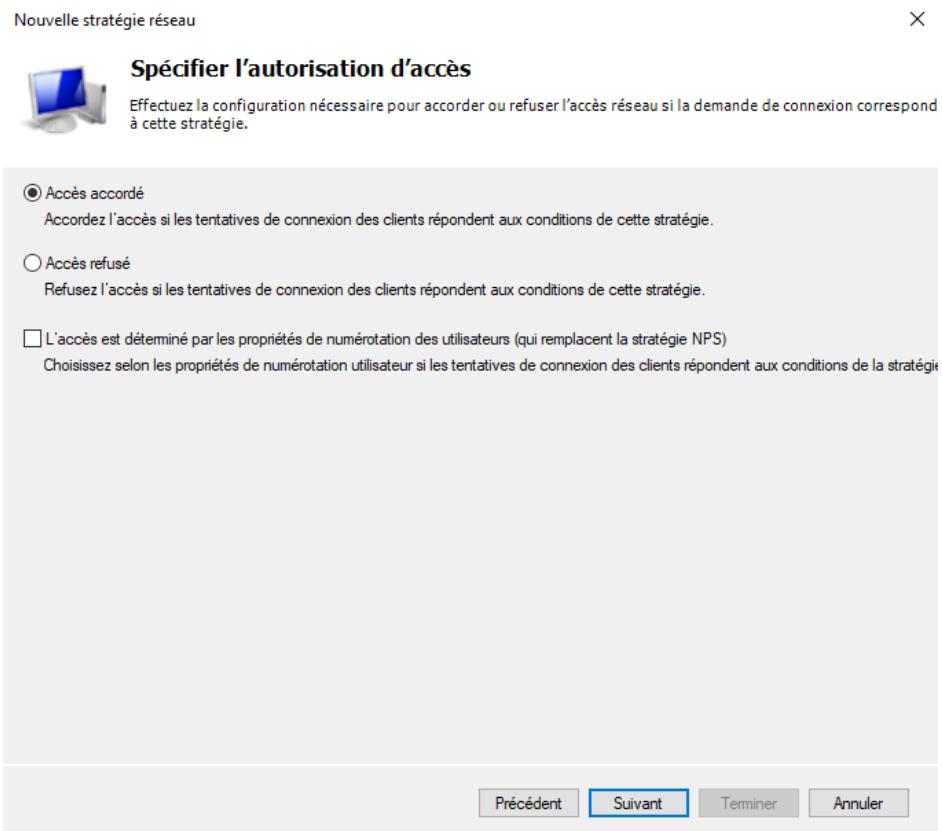
Condition	Valeur
Groupes d'utilisateurs	CCICAMPUS\RADIUS-USERS

Description de la condition :
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

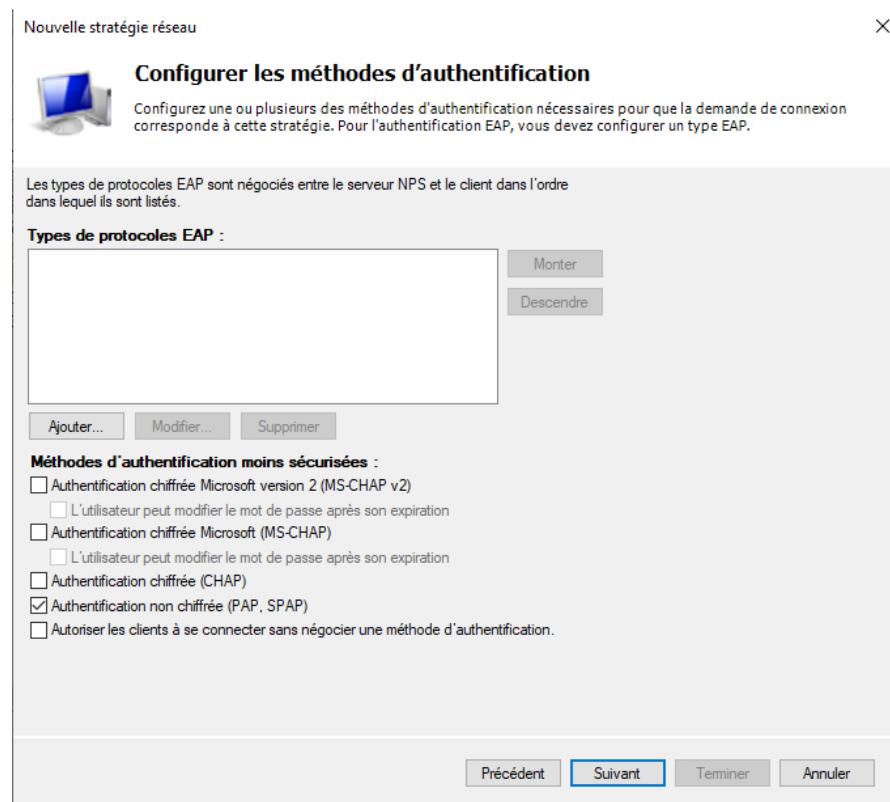
[Ajouter...](#) [Modifier...](#) [Supprimer](#)

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

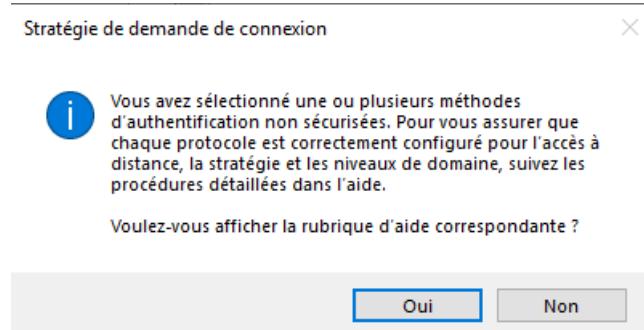
On informe que ce groupe a l'autorisation de se connecter au réseau :



Ensute, on choisit la manière dont les utilisateurs doivent identifier :



Sélectionner « non » :



On peut configurer des contraintes mais dans notre cas on cliquera sur suivant :

Nouvelle stratégie réseau X

Configurer des contraintes



Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

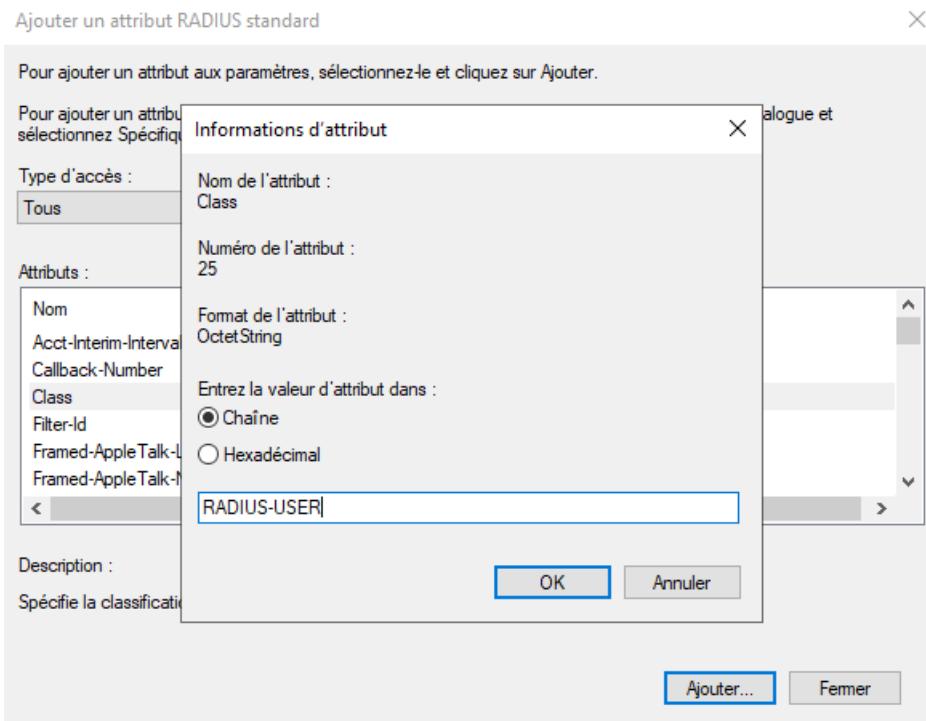
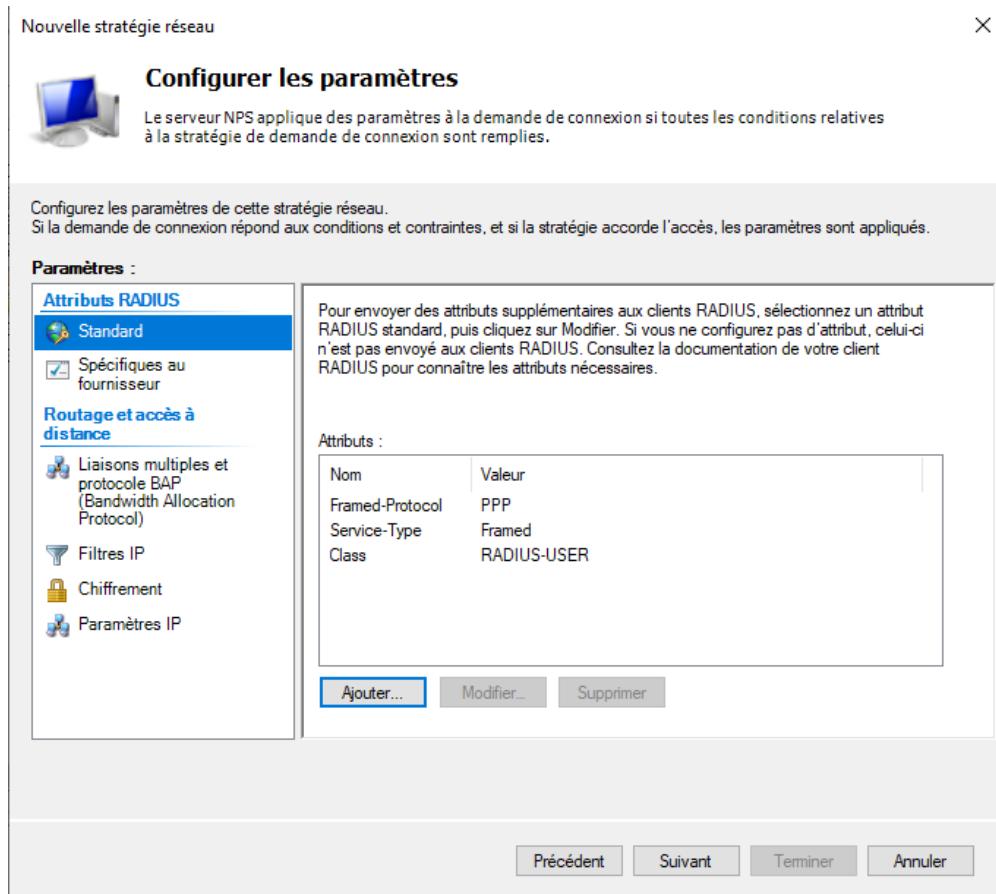
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

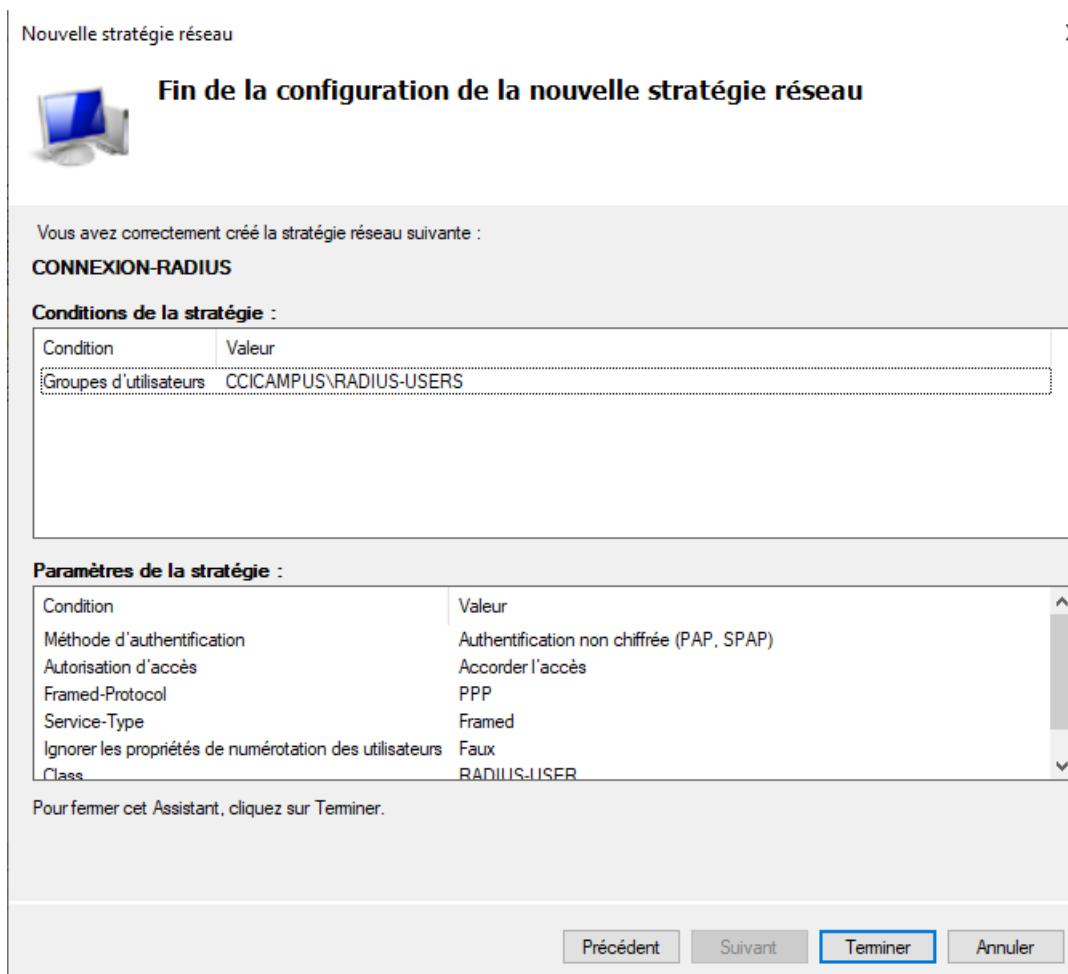
Contraintes <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Délai d'inactivité <input type="checkbox"/> Délai d'expiration de session <input type="checkbox"/> ID de la station appelée <input type="checkbox"/> Restrictions relatives aux jours et aux heures <input type="checkbox"/> Type de port NAS 	<p>Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion</p> <p><input type="checkbox"/> Déconnecter au-delà de la durée d'inactivité maximale</p> <div style="text-align: center; margin-top: 10px;"> <input style="width: 40px; height: 20px;" type="text" value="1"/> ▲ ▼ </div>
--	--

Précédent
Suivant
Terminer
Annuler

On ajoute un attribut Class qui simplifiera l'identification et le suivi d'un utilisateur :



On vérifie que la configuration correspond bien à nos attentes et on clique sur « Terminer » :



La stratégie a bien été créée et doit être en première ligne :

4

The screenshot shows the Windows Server Network Policy Server (NPS) interface. On the left, the navigation pane shows 'NPS (Local)' with 'Clients et serveurs RADIUS' and 'Stratégies'. Under 'Stratégies', there are 'Stratégies de demande' and 'Stratégies réseau'. The right pane displays the 'Stratégies réseau' (Network Policies) screen. It includes a descriptive note about network policies and a table of existing policies:

Nom de la stratégie	État	Ordre de traitement	Type d'accès
CONNEXION-RADIUS	Activé	1	Accorder l'accès
Connexions au serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès
Connexions à d'autres serveurs d'accès	Activé	3	Refuser l'accès

Below the table, the 'CONNEXION-RADIUS' policy is selected, showing its conditions and parameters. The 'Conditions' section lists a user group: 'Groupes d'utilisateurs CCICAMPUS\RADIUS-USERS'. The 'Paramètres' section shows no applied parameters.

Création du portail Captif

4.1 Liaison du portail captif à l'AD

On se rend dans SystemUser > ManagerAuthentication > Servers

On donne les informations suivantes :

The screenshot shows the 'Server Settings' configuration page. The 'Descriptive name' is set to 'AD_RADIUS' and the 'Type' is 'RADIUS'. The 'Protocol' is 'MS-CHAPv2'. The 'Hostname or IP address' is '192.168.100.2'. The 'Shared Secret' is '*****'. The 'Services offered' is 'Authentication and Accounting'. The 'Authentication port' is '1812' and the 'Accounting port' is '1813'. The 'Authentication Timeout' is '5'. The 'RADIUS NAS IP Attribute' is 'LAN - 192.168.100.1'. A note states: 'Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.' At the bottom, there is a 'Save' button and a link to 'Activer Windo Accédez aux paran'.

4.2 Création du portail Captif

On se rend dans Services > Captive Portal > Add

On donne un nom et une description :

On active le portail captif sur l'interface LAN

On modifie les paramètres suivants :

After authentication redirection URL : <https://google.fr>. Quand l'utilisateur seaura connecté au portail captif, il sera redirigé sur le site de google.

MAC filtering : on désactive

Authentification Server : on sélectionne la liaison à RADIUS créé précédemment.

4.3 Exclusion de certaines machines

Nos serveurs et routeurs n'ont pas besoin de se connecter au portail captif. Cela impacterait l'utilisation de certains services.

On va donc les autoriser à discuter sur le réseau sans faire la connexion au portail captif. Pour cela on se rend dans Services > Captive Portal > Notre portail captif > Allowed IP Addresses. Ici on renseigne

les adresses IP des passerelles, des Windows Server et du serveur NAS :

IP Addresses	Description	Actions
⇒ 192.168.100.1		
⇒ 192.168.100.2		
⇒ 192.168.100.3		
⇒ 192.168.100.4		
⇒ 192.168.200.1		
⇒ 192.168.200.2		
⇒ 192.168.200.3		

→ = All connections to the address are allowed, ← = All connections from the address are allowed, ⇌ = All connections to or from the address are allowed

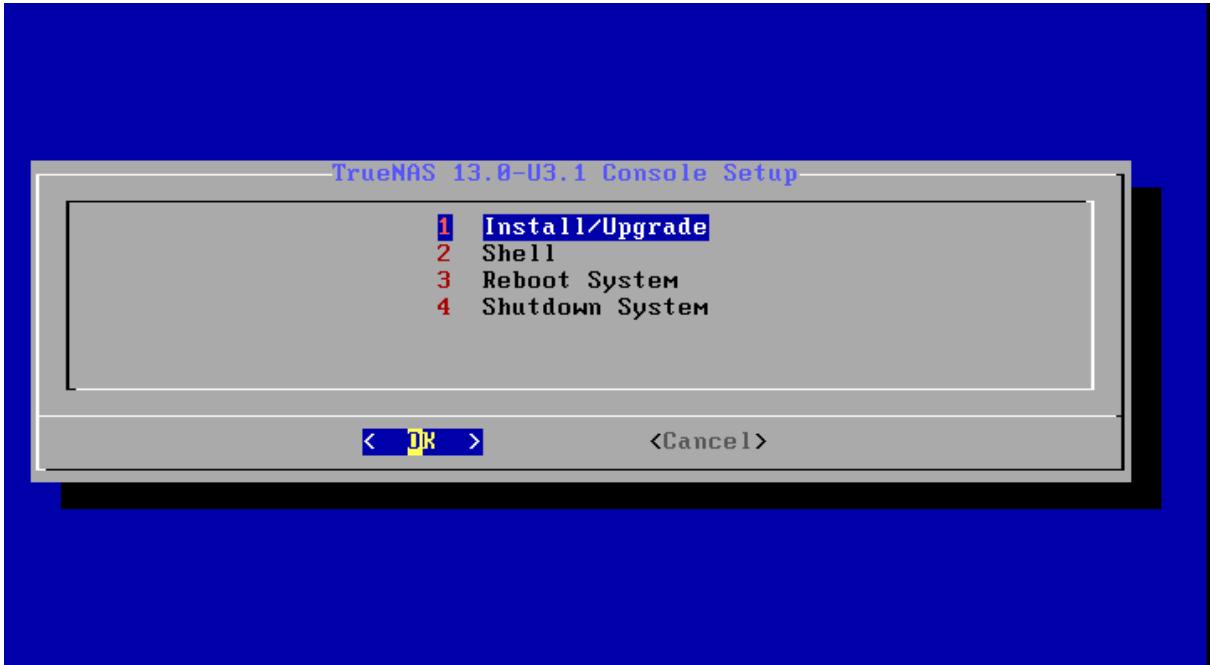
5 Installation des serveurs de stockage

5.1 Installation de TrueNAS

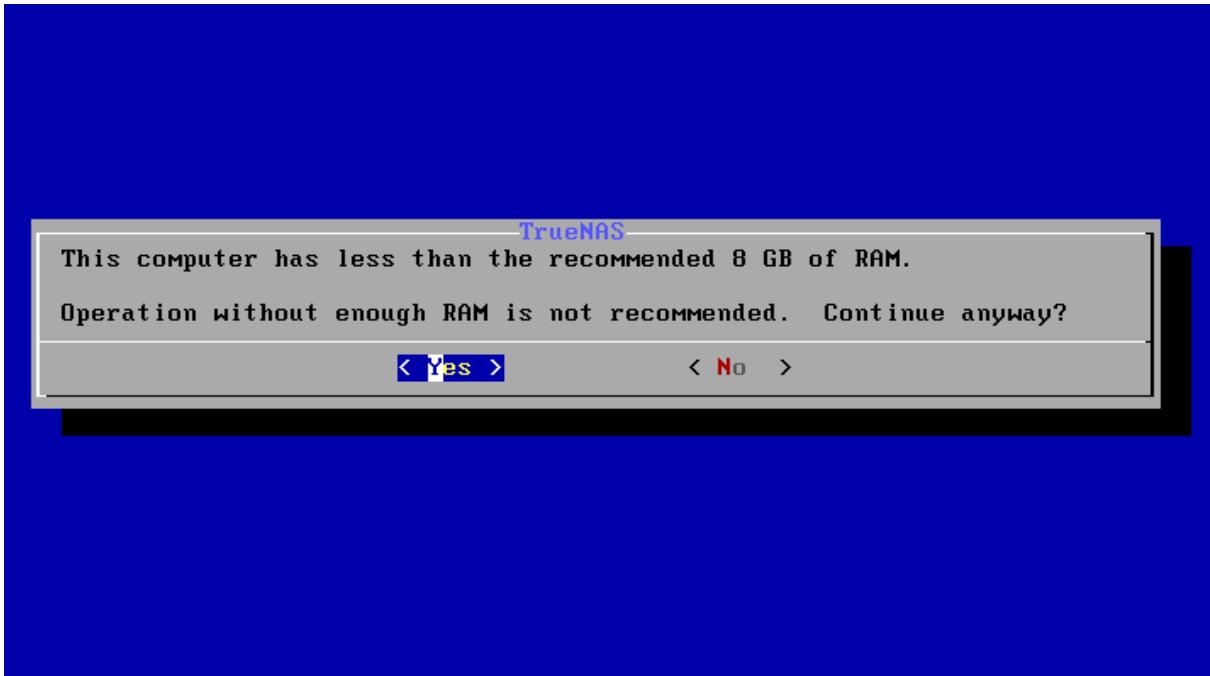
Dans un nous allons lancer l'iso avec 2 GB de RAM et un disque de 20 GB et deux disques de 60 GB. Il faudra également mettre le Vmnet1 pour le site de Strasbourg et Vnet2 pour le site de Mulhouse :

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
Hard Disk 2 (SCSI)	60 GB
Hard Disk 3 (SCSI)	60 GB
CD/DVD (IDE)	Using file C:\Users\jules\Doc...
Network Adapter	Custom (Vmnet1)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Pour l'installation de l'iso, nous allons sélectionner : Install/Upgrade :



Un message indiquant qu'il est recommandé d'utiliser 8 GB de RAM va apparaître, faites YES, 2GB serons suffisant pour ce projet :

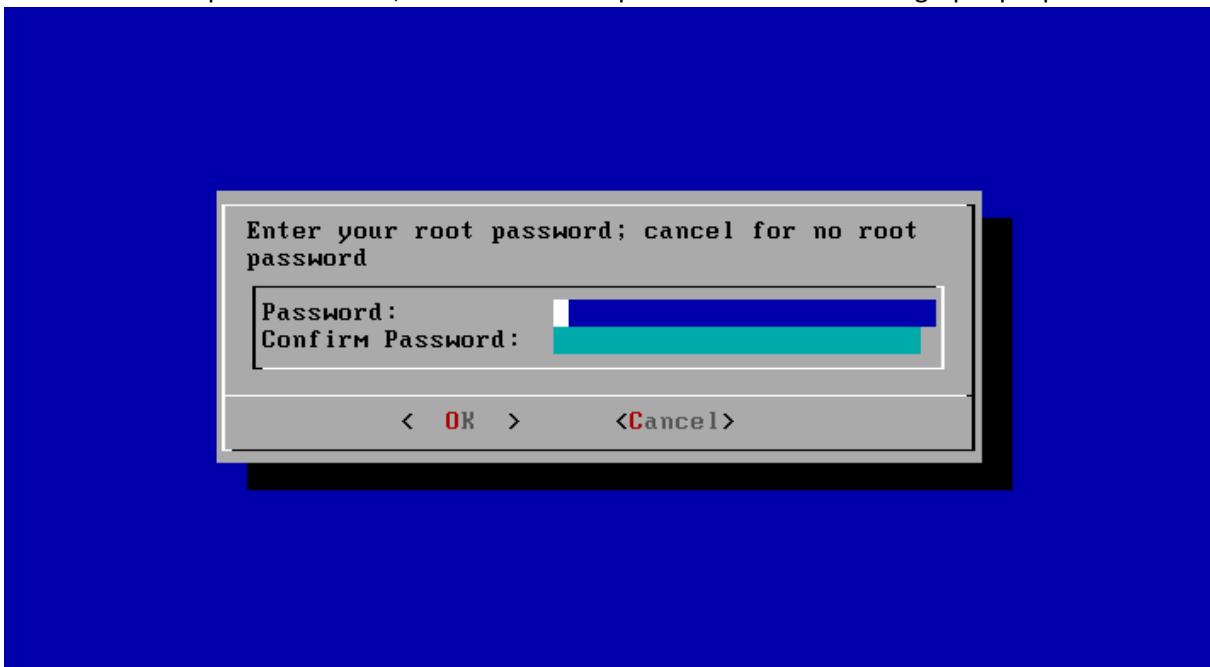


Nous allons maintenant sélectionner le disque sur lequel l'installation de l'Iso se fera.

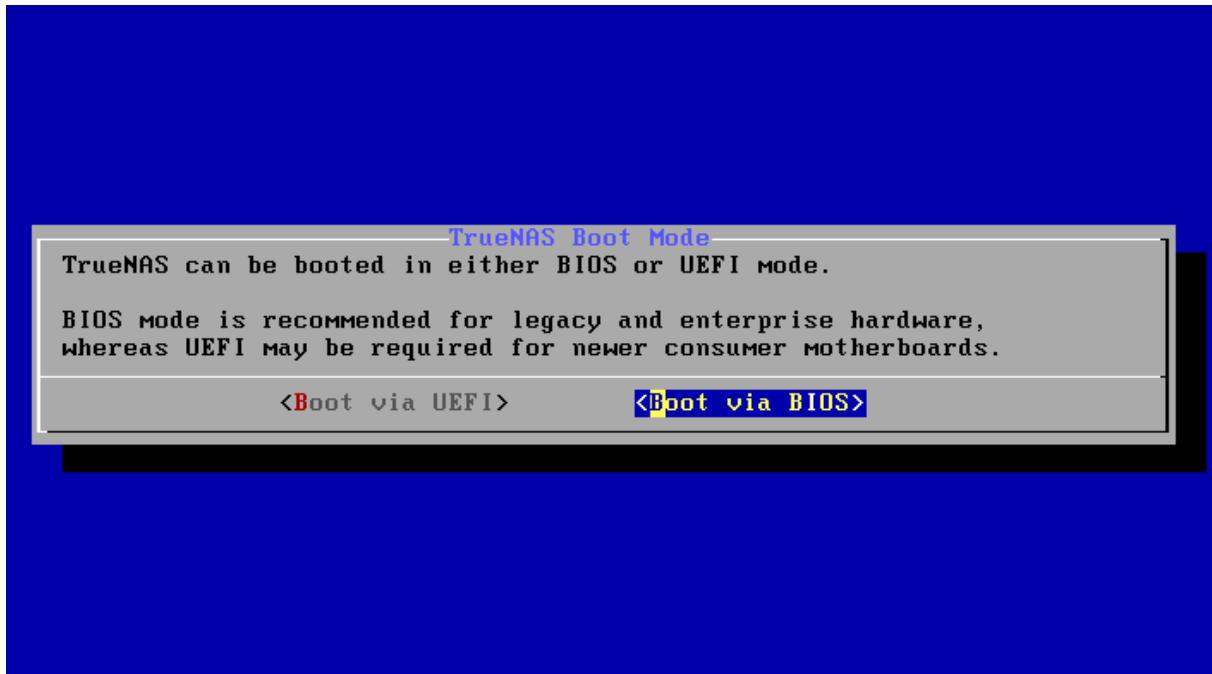
On fait espace sur le disque pour le sélectionner. Puis on fait entrer. Ici nous utiliserons le disque de 20 GB :



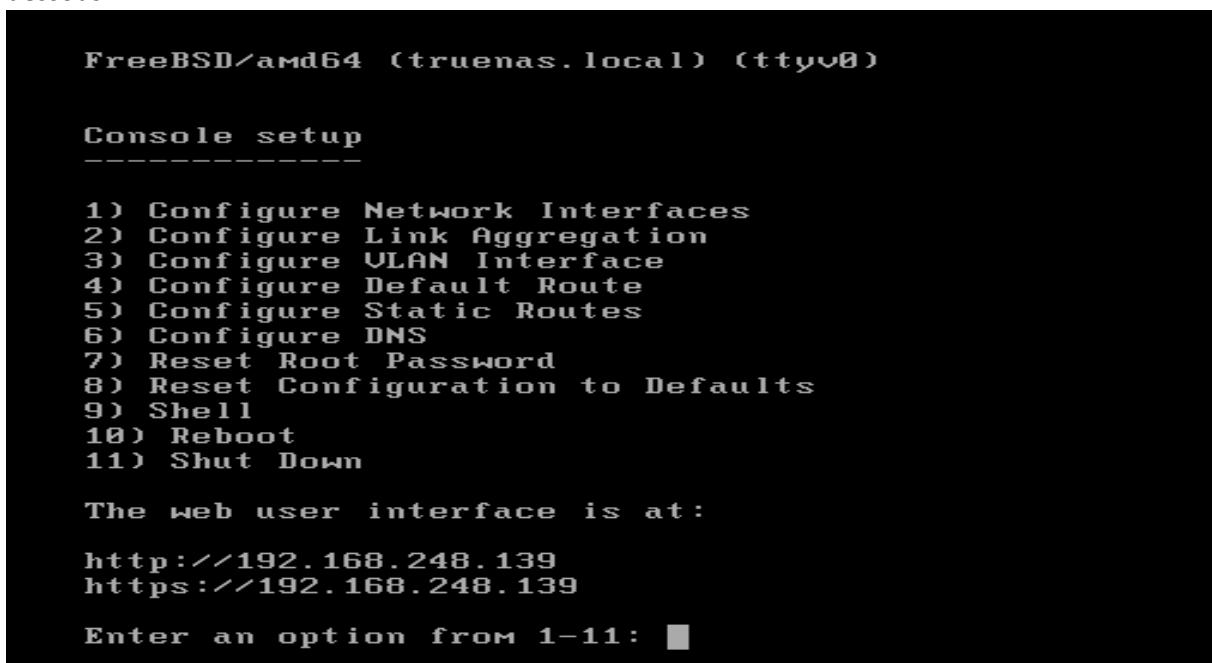
Entrez le mot de passe souhaiter, il sera nécessaire pour l'accès à l'interface graphique plus tard :



Sélectionnez « boot via bios » :



Une fois l'installation terminé, il faudra reboot et nous arriveront finalement sur l'interface ci-dessous :



5.2 Configuration système et réseau

Dans un premier temps, il nous faudra change l'adresse IP du Nas.

Pour cela :

Nous allons faire 1 puis entrer

Nous allons ensuite sélectionner l'interface em0

Puis faire non deux fois pour ne pas réinitialiser les paramètre réseau et activé le DHCP

Faites maintenant oui pour configurer l'IPV4 où nous allons entrer les informations suivantes :

IPV4 : 192.168.100.4 pour le NAS de Strasbourg
 192.169.200.4 pour le NAS de Mulhouse

NETMASK : 255.255.255.0

Faites encore une fois non pour ne pas configurer l'IPV6.

```

9) Shell
10) Reboot
11) Shut Down

The web user interface is at:

http://0.0.0.0
https://0.0.0.0

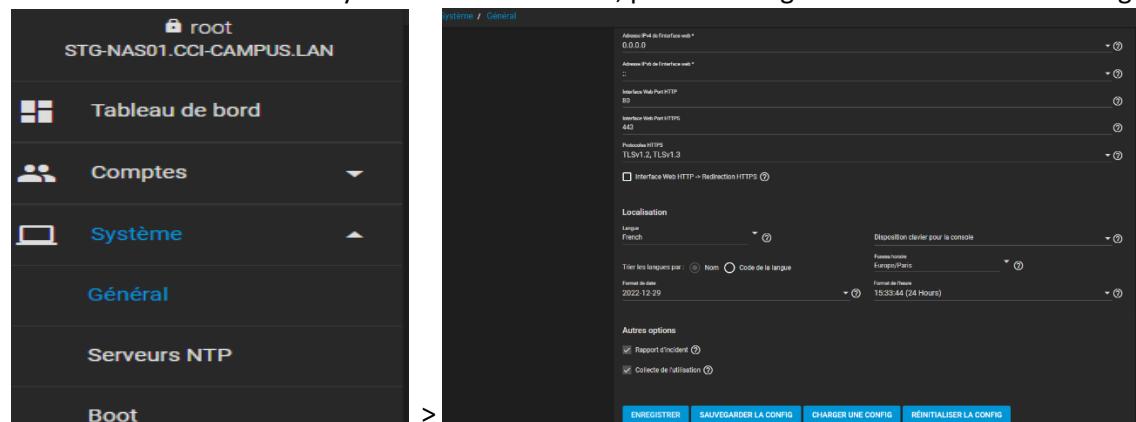
Enter an option from 1-11: 1
1) em0
Select an interface (q to quit): 1
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name:
Several input formats are supported
Example 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:192.168.100.4
IPv4 Netmask:255.255.255.0/24

```

Le reste de la configuration se fera via l'interface graphique. Pour cela taper l'adresse IP du serveur NAS dans le navigateur d'un client qui se trouve dans le même réseau que le NAS.

On tape le nom d'utilisateur « root » et le mot de passe défini lors de l'installation.

On se rend ensuite dans « Système » > « Général », puis on change le fuseau horaire et la langue :



A présent on se rend dans « Réseau » > « Configuration Global ». Ici nous rentrons :

Le nom du serveur NAS : STG-NAS01 ou MUL-NAS01

Le nom du domaine (le serveur ne sera pas ajouté au domaine pour autant)

Les serveurs DNS, à savoir : 192.168.100.2, 192.168.200.3, 192.168.200.2 et 192.168.200.3

La passerelle : 192.169.100.1 pour STG-NAS01 et 192.168.200.1 pour MUL-NAS01.

5.3 Mise en place des Volumes et du RAID

On se rend dans « Stockage » > « Volume ». On clique sur Ajouter un Volume > Créer un volume. On déclare que ce volume est en RAID avec nos 2 disques dur :

Le volume en RAID a bien été créé :

A présent on clique sur ce volume et on active la déduplication.

5.4 Crédation et configuration Zvol

Ici, on clique sur les 3 points sur le volume crée précédemment et on clique sur ajouter un Zvol :

Nous allons le nommée Backup01 pour Strasbourg et Backup02 pour Mulhouse.

On rentre également la taille que votre volume va faire, en sachant que on ne peut mettre plus de 80% de l'espace de stockage du disque d'origine. Les autres paramètres sont laissés par défaut :

Nom du zvol *
Backup01

Commentaires

Taille pour ce zvol *
40 GiB

Taille de la force ?

Synchroniser

Niveau de compression *

ZFS Deduplication is an advanced option meant for experts only. Proceed carefully.

Déduplication ZFS *

Sparse ?

Lecture seule
Hériter (off)

Options de chiffrement

Héritage (non chiffré) ?

ENVOYER ANNULER OPTIONS AVANCÉES

Votre Zvol est maintenant créé sur le volume :

Stockage / Volumes

TrueNAS CORE® © 2022 - iXsystems, Inc.

Volumes

AJOUTER

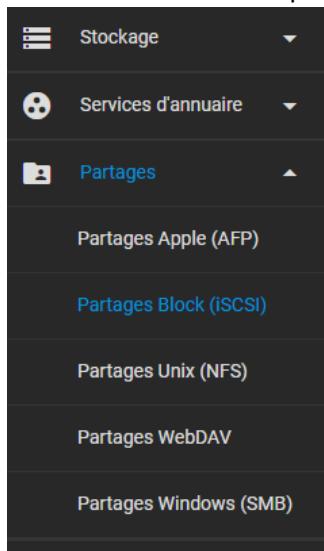
RAID01 (System Dataset Pool)		ONLINE ✓ 40.64 GiB (73%) Utilisé 15.08 GiB Libre						
Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
RAID01	FILESYSTEM	40.64 GiB	15.08 GiB	lz4	16.81	false	OFF	
Backup01	VOLUME	40.63 GiB	55.71 GiB	Hérite (lz4)	1.00	false	OFF	

5.5 Configuration iSCSI

5.5.1 Configuration sur le serveur NAS

Cette partie est identique sur les deux sites, les différences de paramétrage seront citées s'il y en a.

Pour cela nous allons depuis le serveur NAS nous rendre dans Partages > Partage Block (iSCSI) :



On clique sur Wizard :

On nomme ensuite notre partage (backup01 pour Strasbourg et backup02 pour Mulhouse), on sélectionne le device et on utilise le Zvol crée plus tôt. Ensuite, on fait « suivant » :

On fait « créer un nouveau portail ». On laisse les paramètres par défauts, sauf pour l'IP où on renseigne celle de notre NAS :

Créer ou sélectionner un périphérique bloc (Block Device)

2 Portail

3 Initiateur

4 Confirmer les options

Portail *
Create New

Méthode d'authe (Discovery Method): NONE

Groupe d'authe (Discovery Group): Aucun

Adresse IP *
192.168.100.4

Port
3260

AJOUTER

ANNULER RETOUR SUIVANT

Pour ce partage, nous n'avons pas mis en place d'utilisateur ou de réseau particulier ayant accès. On fait simplement « suivant » :

Créer ou sélectionner un périphérique bloc (Block Device)

3 Initiateur

4 Confirmer les options

Initiateurs

Réseaux autorisés

ANNULER RETOUR SUIVANT

Votre liaison ISCSI est initialisée sur votre NAS :

Create or Choose Block Device

Portal

Initiator

4 Confirm Options

ISCSI Summary
Name: backup01
Extent:
Device: RAID01/Backup01zvol (44.0G)
Use For: VMware: Extent block size 512b, TPC enabled, no Xen compat mode, SSD speed
New Portal:
Discovery Auth Method: NONE
Listen: 192.168.100.4:3260
Confirm these settings.

CANCEL BACK SUBMIT

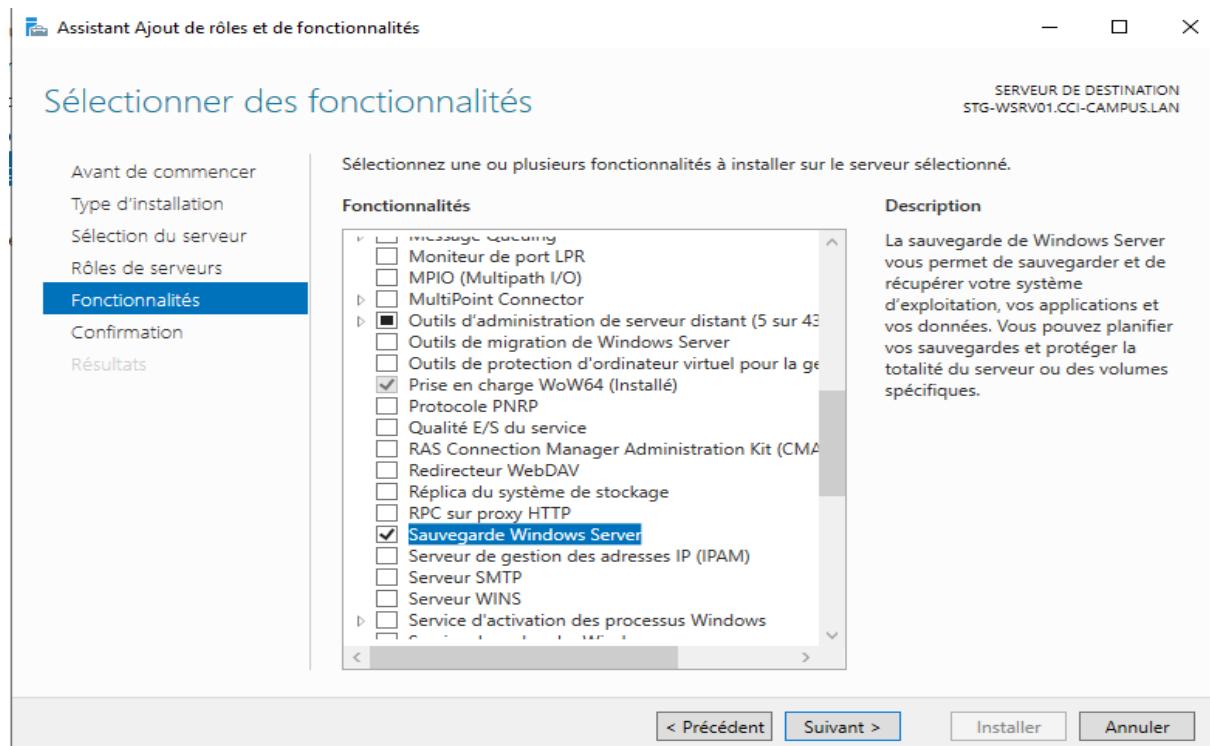
Ne pas oublier d'activer le service ISCSI dans l'onglet « service ».

5.5.2 Configuration sur le serveur Windows

Encore une fois cette manipulation est identique sur les deux sites.

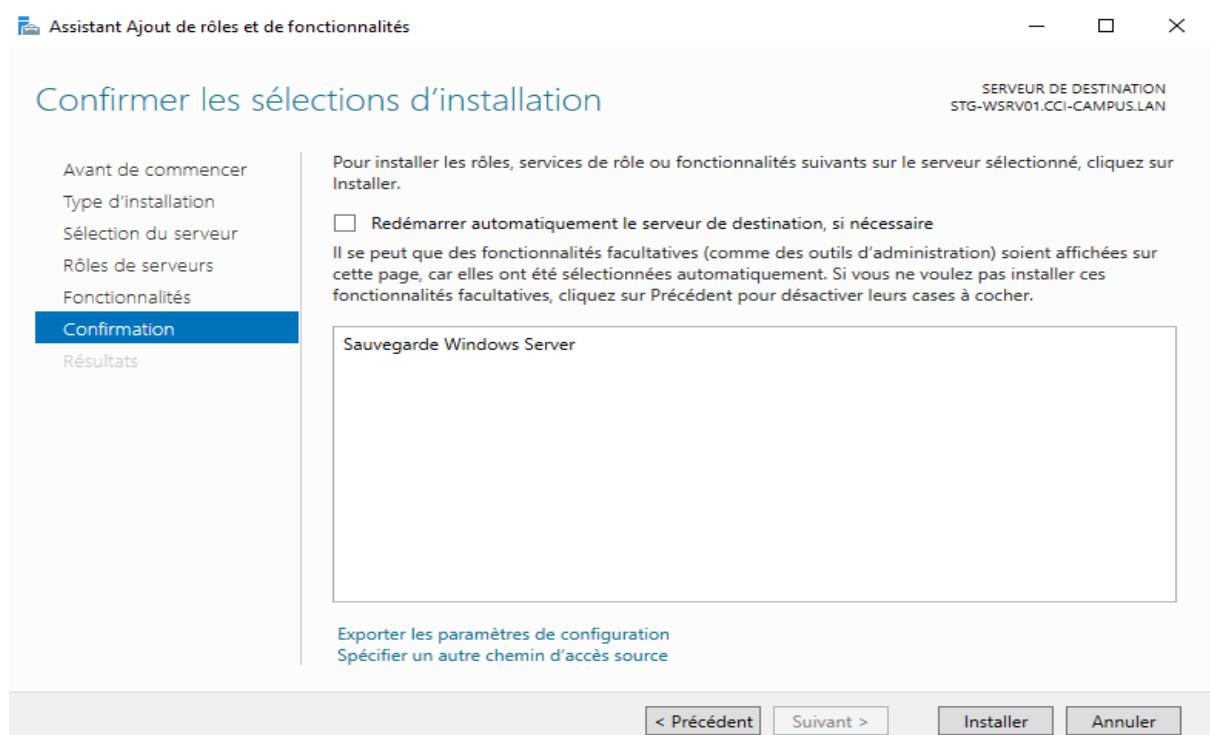
6 Sauvegarde du Windows serveur :

Dans un premier temps, il faut ajouter la fonctionnalité dans le gestionnaire de serveur. Suivez la même méthode que les fonctionnalités ajoutées précédemment et sélectionner sauvegarde

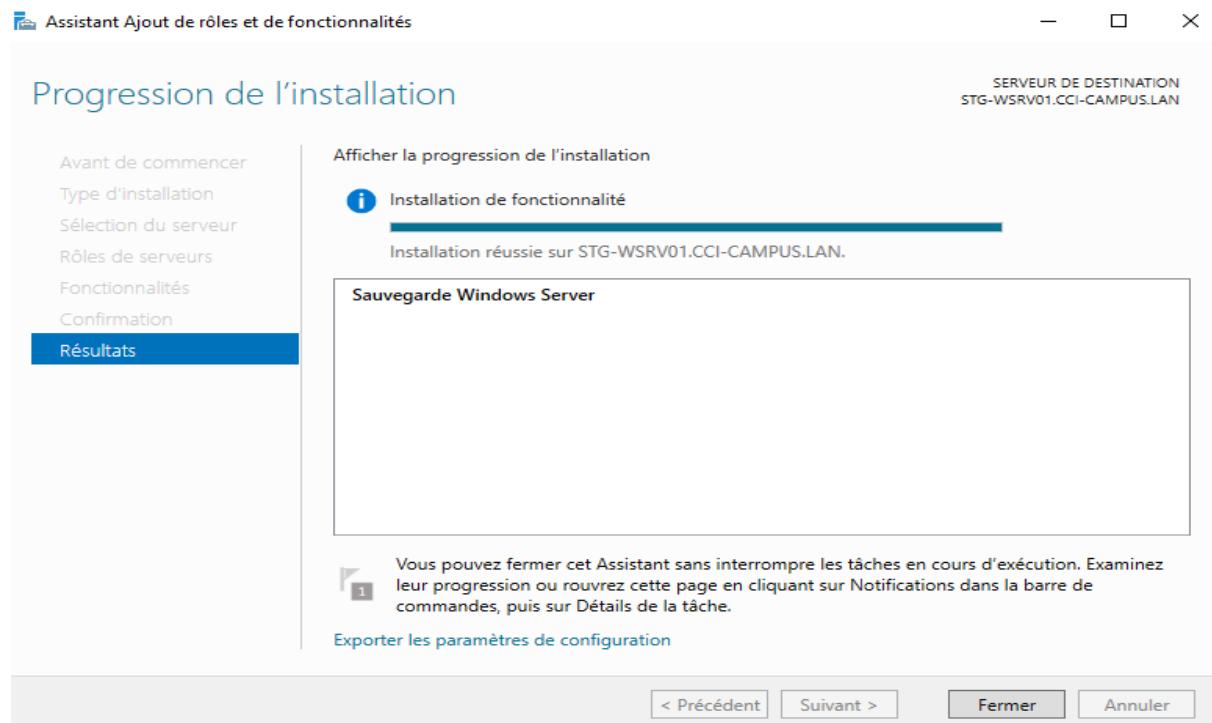


Windows Server dans la partie fonctionnalité.

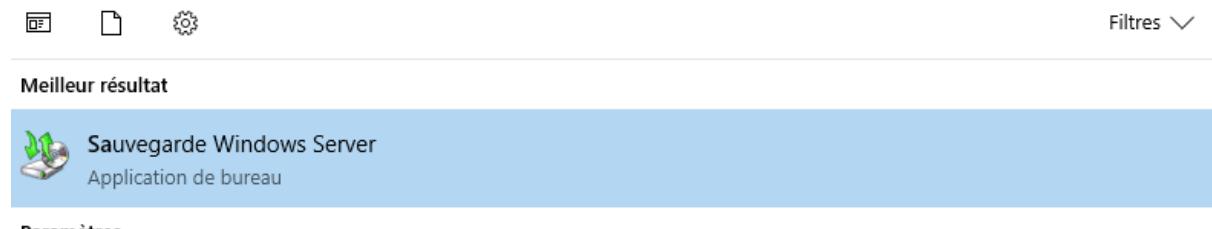
Faites «suivant» jusqu'à l'installation, et cliquez sur installer



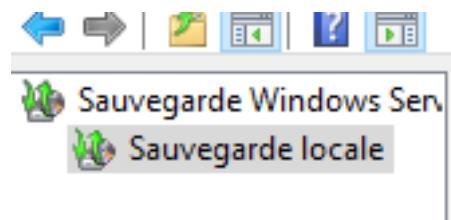
Votre fonctionnalité à bien été installé



Rendez-vous dans l'applicatif sauvegarde Windows serveur, trouvable dans l'explorateur windows.

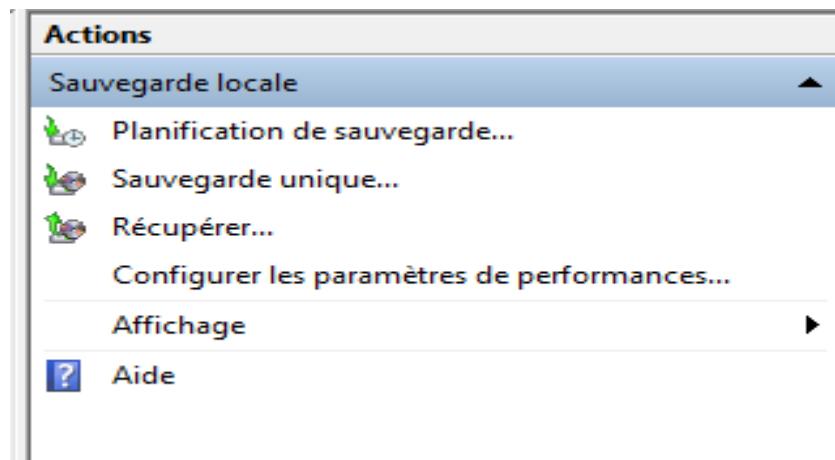


Une fois la page ouverte, rendez vous dans l'onglet sauvegarde locale

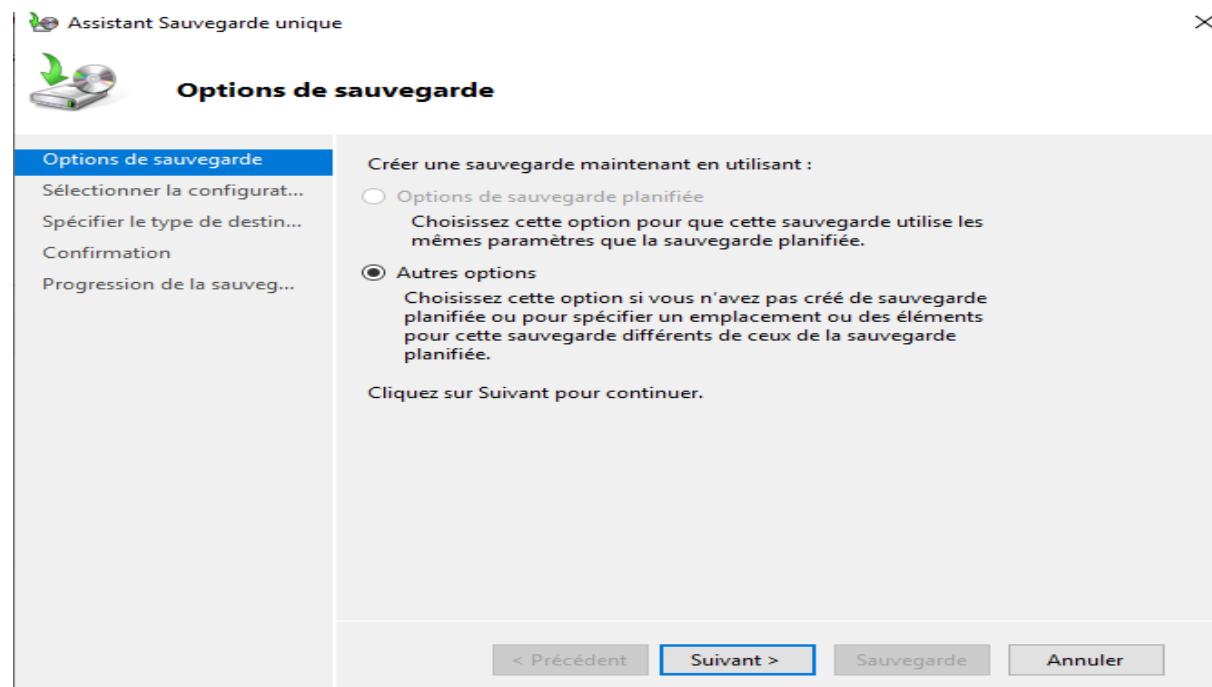


6.1 Sauvegarde Unique :

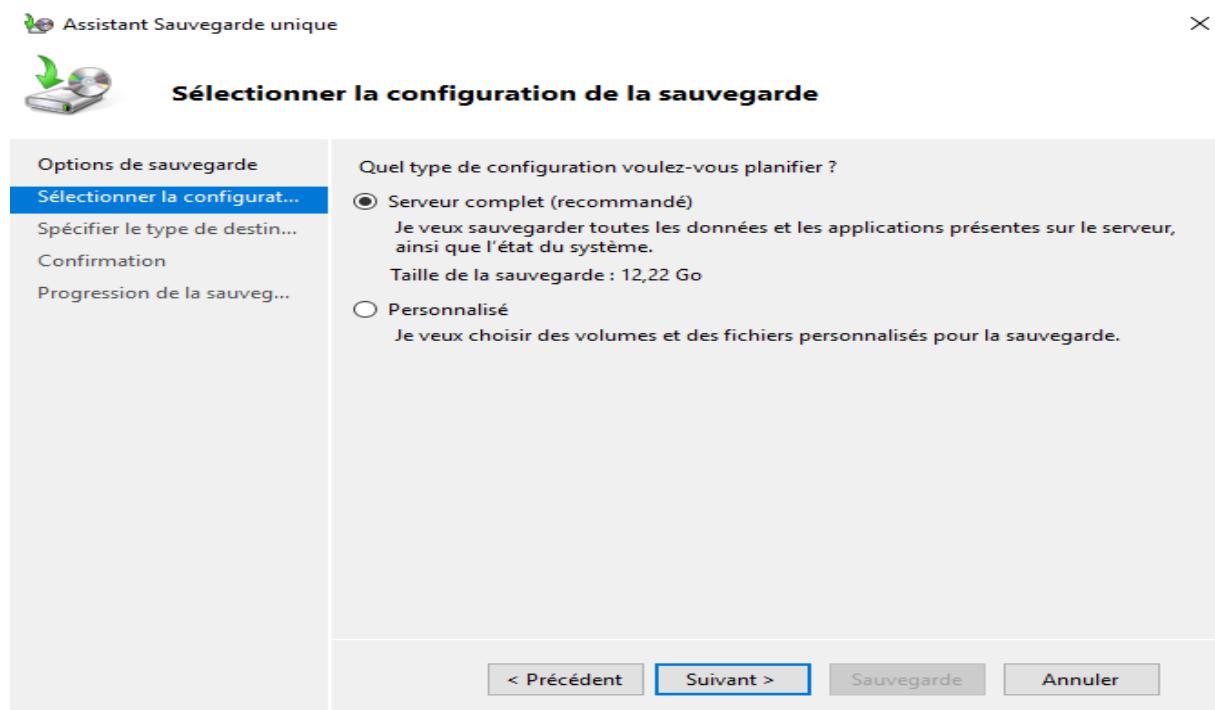
Puis dans la fonctionnalité à droite faites sauvegarde unique



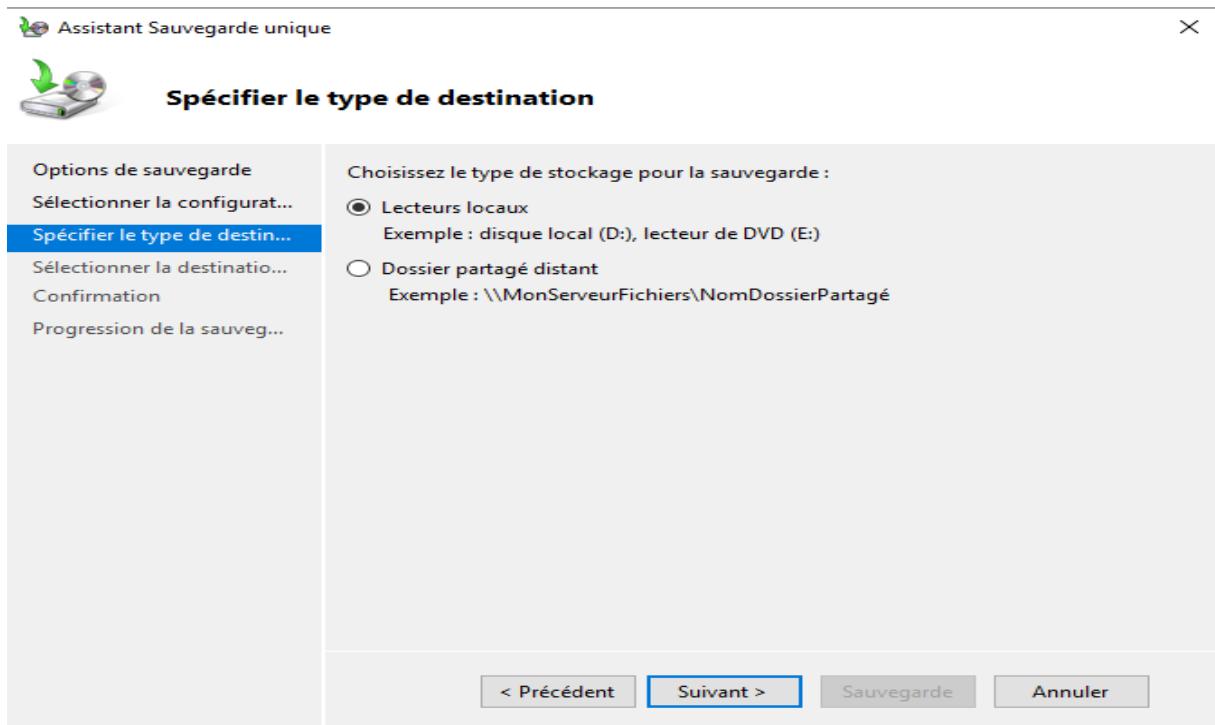
Laissez les paramètres par défaut et faites « suivant » :



Pour cette fois nous voulons faire une sauvegarde complète du serveur, ensuite faites «suivant»



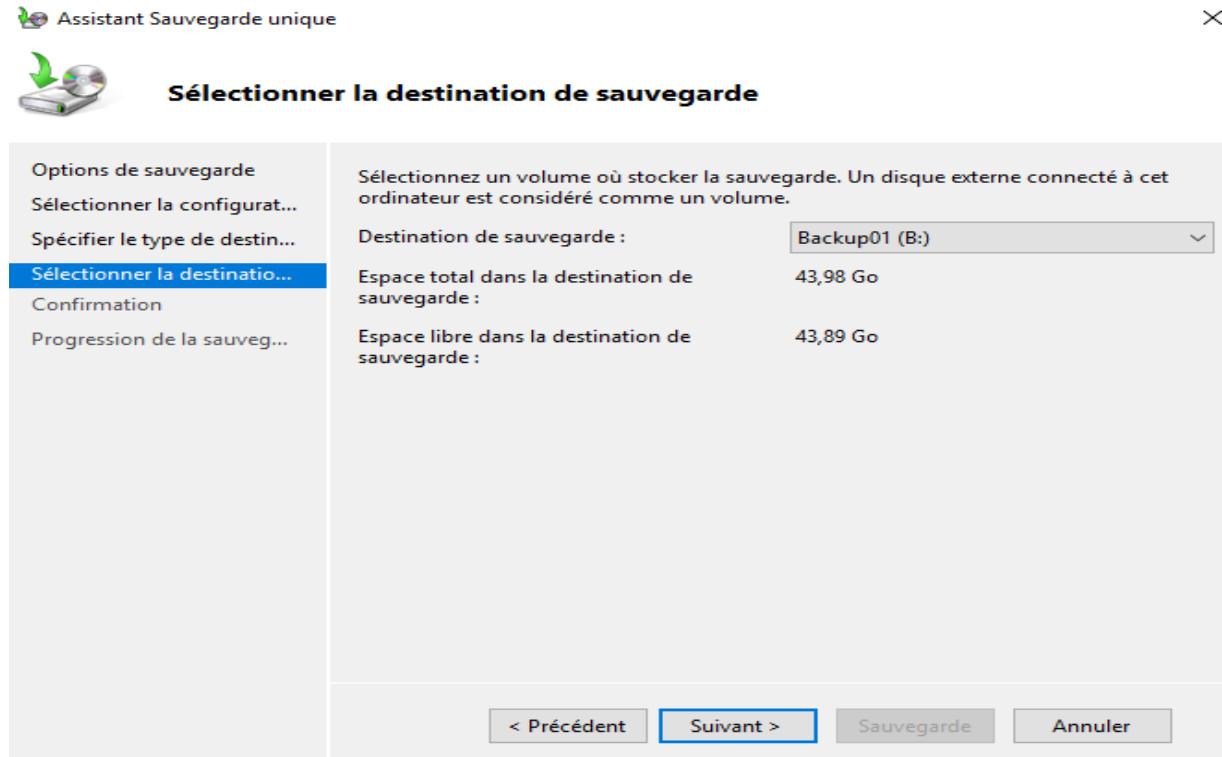
Cocher lecteurs locaux et faites «suivant»



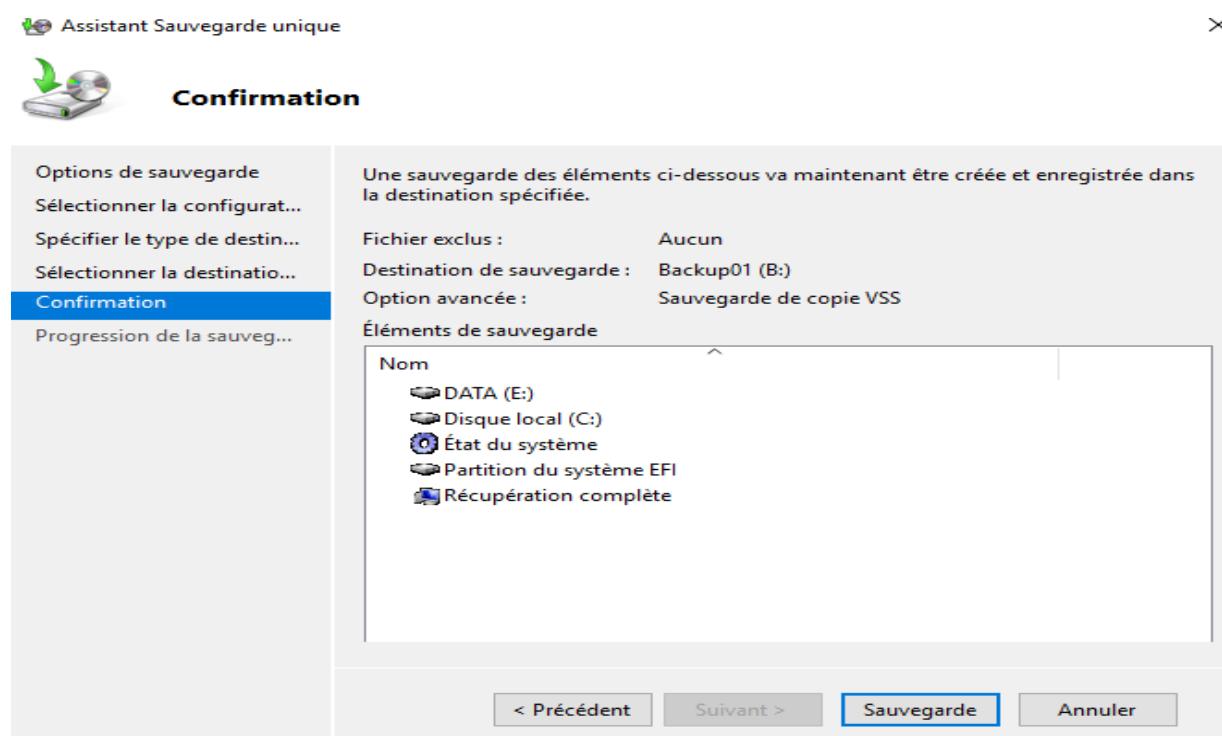
Sélectionner le lecteur Backup01, le lecteur du NAS aura pour rôles de stocker les sauvegardes du Windows serveur

Pour le site de Mulhouse, sélectionner simplement Backup02 à la place

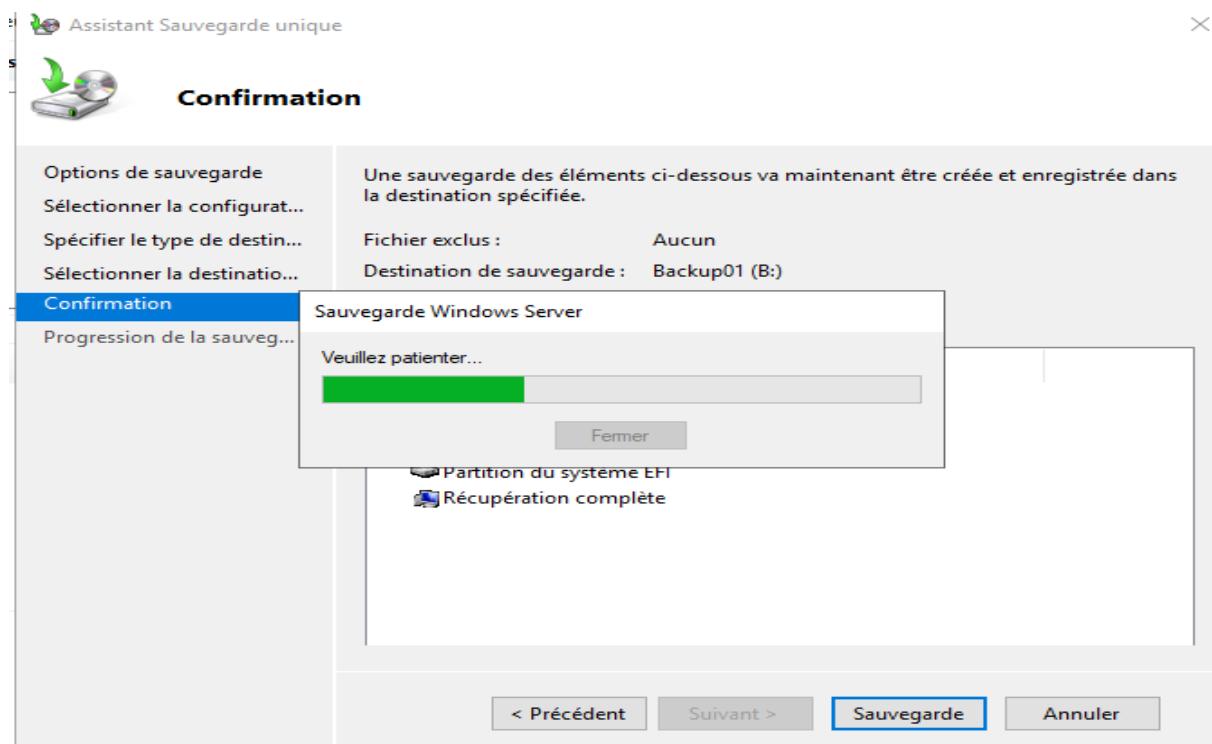
Faites ensuite «suivant»



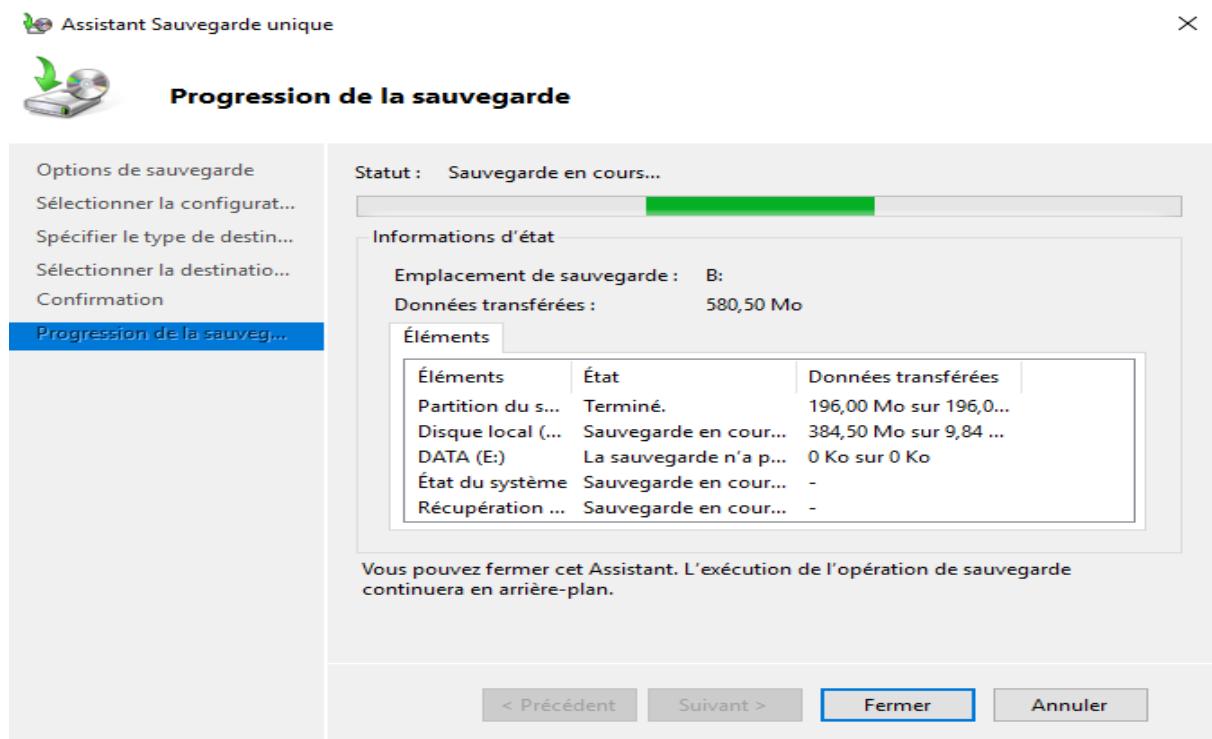
Procéder maintenant à la sauvegarde en cliquant sur sauvegarder



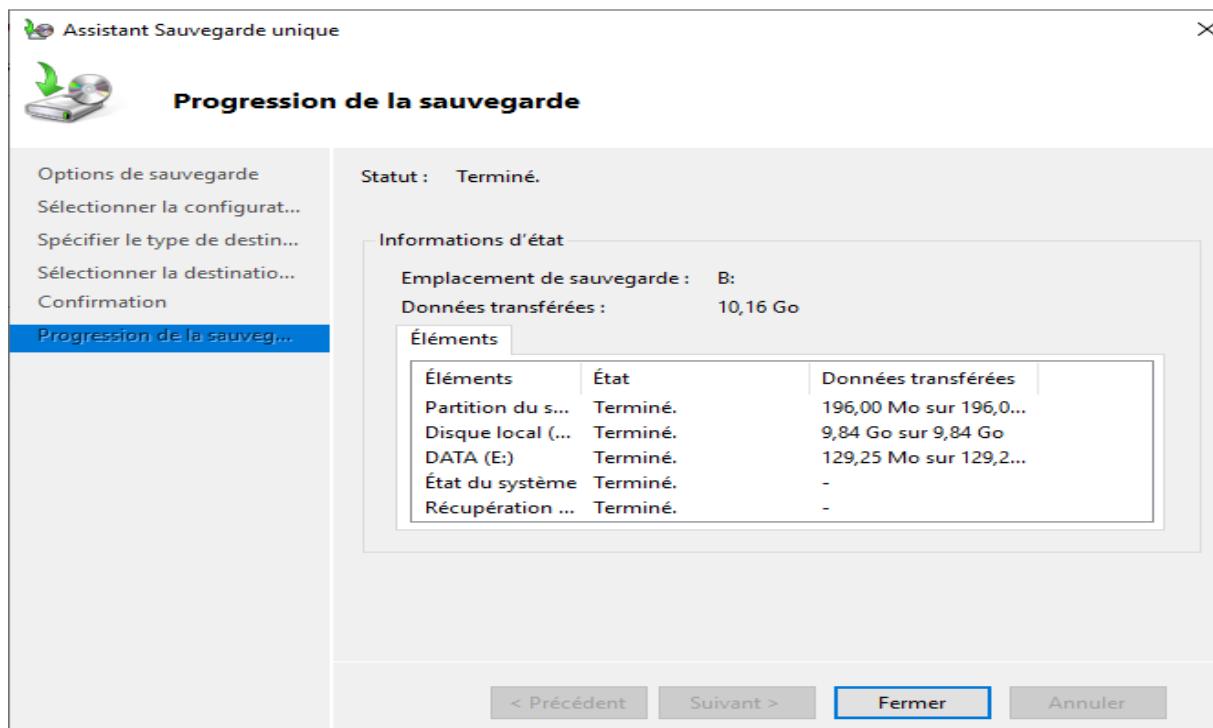
Laisser la sauvegarde se faire, cela prend un peu de temps.



Nous pouvons voir ci-contre que la sauvegarde est en train de s'effectuer volume par volume



Votre sauvegarde est maintenant terminée.



Nous pouvons voir que la sauvegarde à bien été effectuer

Vous aurez les informations de la date et de la statue de la sauvegarde sur l'applicatif

Contre le montre l'image ci-dessous

Durée	Message	Description
29/12/2022 20:32	Sauvegarde	Réussite

Statut

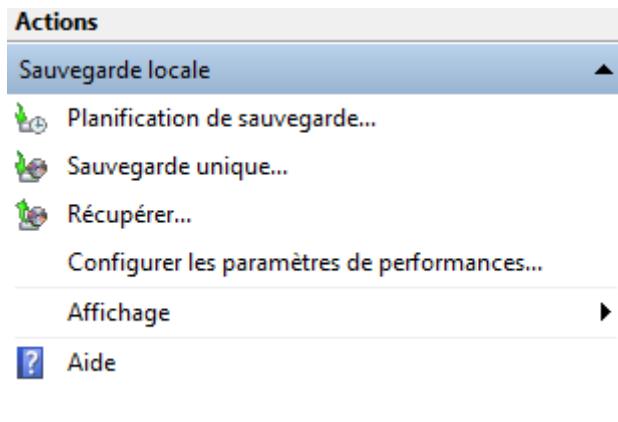
Dernière sauvegarde	Prochaine sauvegarde	Toutes les sauvegardes
État : ✓ Réussite Durée : 29/12/2022 20:32 Afficher les détails	État : Aucune planification Durée : - Afficher les détails	Total des sauvegardes : 1 copies Copie la plus récente : 29/12/2022 20:32 Copie la plus ancienne : 29/12/2022 20:32 Afficher les détails

Nous pouvons d'ailleurs voir dans le disque de backup que notre sauvegarde unique à bien fonctionné

		Accueil	Partage	Affichage
		▼	↑	Ce PC > Backup01 (B:) > WindowsImageBackup > STG-WSRV01 >
cès rapide	Nom		Modifié le	Type
lureau	Backup 2022-12-29 193222		29/12/2022 20:37	Dossier de fichiers
échargement:	Catalog		29/12/2022 20:37	Dossier de fichiers
ocuments	Logs		29/12/2022 20:37	Dossier de fichiers
ages	SPPMetadataCache		29/12/2022 20:37	Dossier de fichiers
	Mediald		29/12/2022 20:32	Fichier

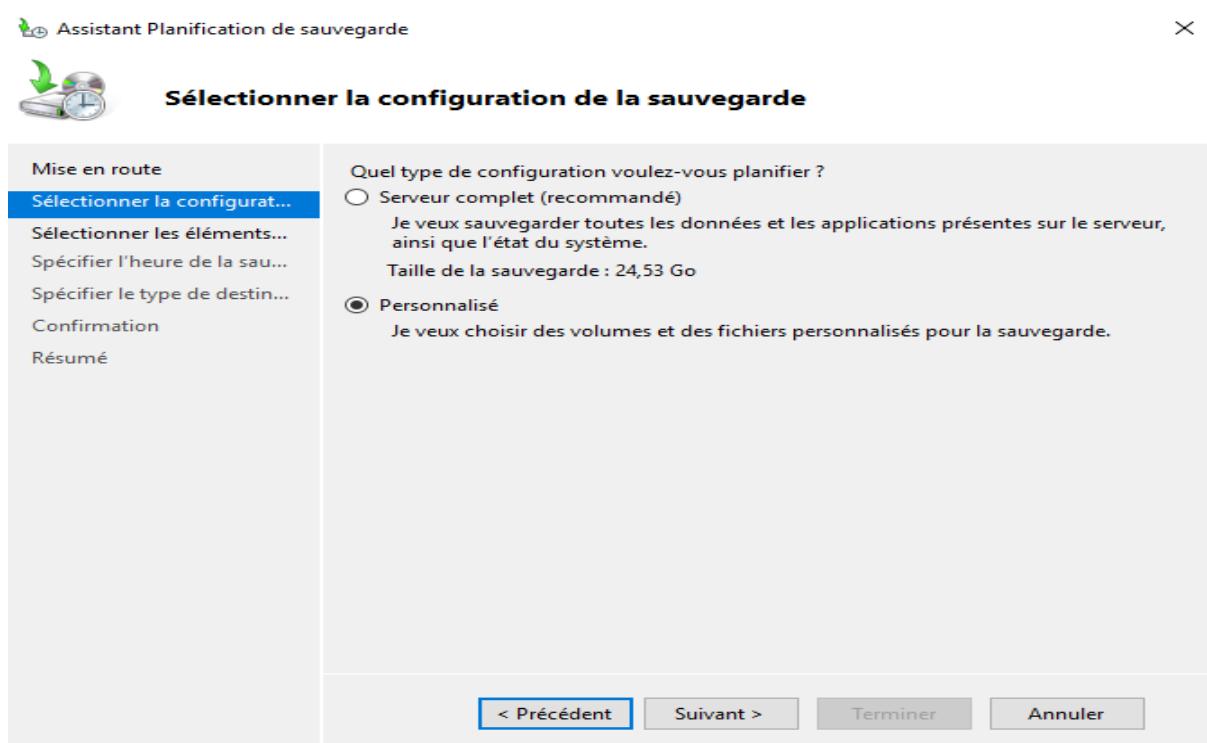
6.2 Planification de sauvegarde :

Dans le cas où une sauvegarde unique n'est pas très pratique question sécurité de donné, il est conseillé de faire une planification de sauvegarde, afin que votre sauvegarde se mette à jour quotidiennement ou de manière hebdomadaire.



Une fois dans planification de sauvegarde, cocher la sauvegarde personnalisée

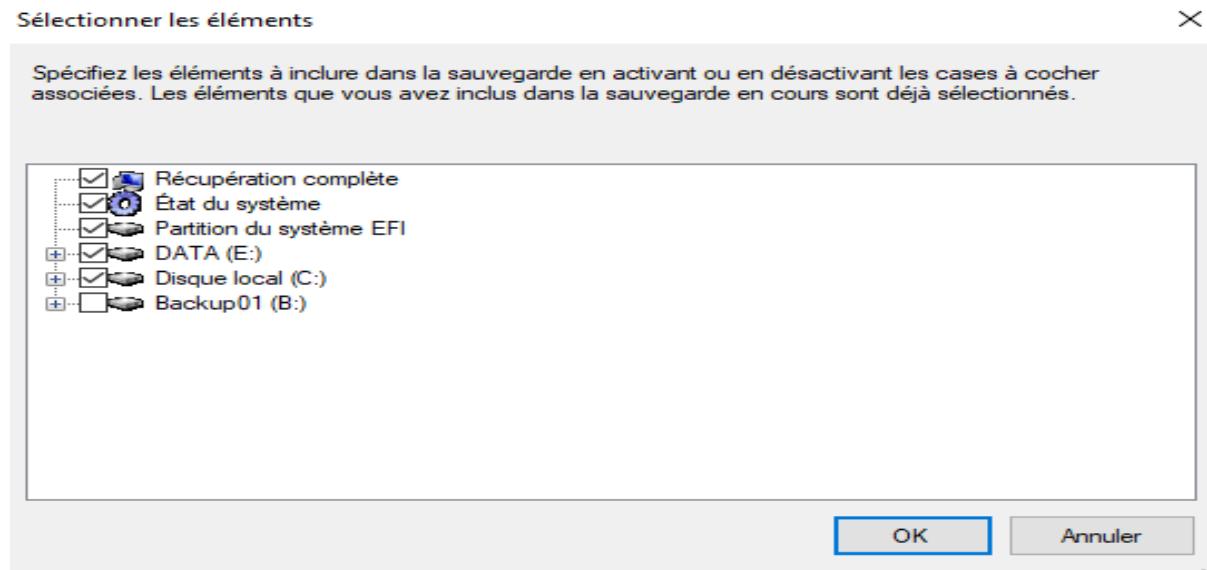
Puis faites « suivant »



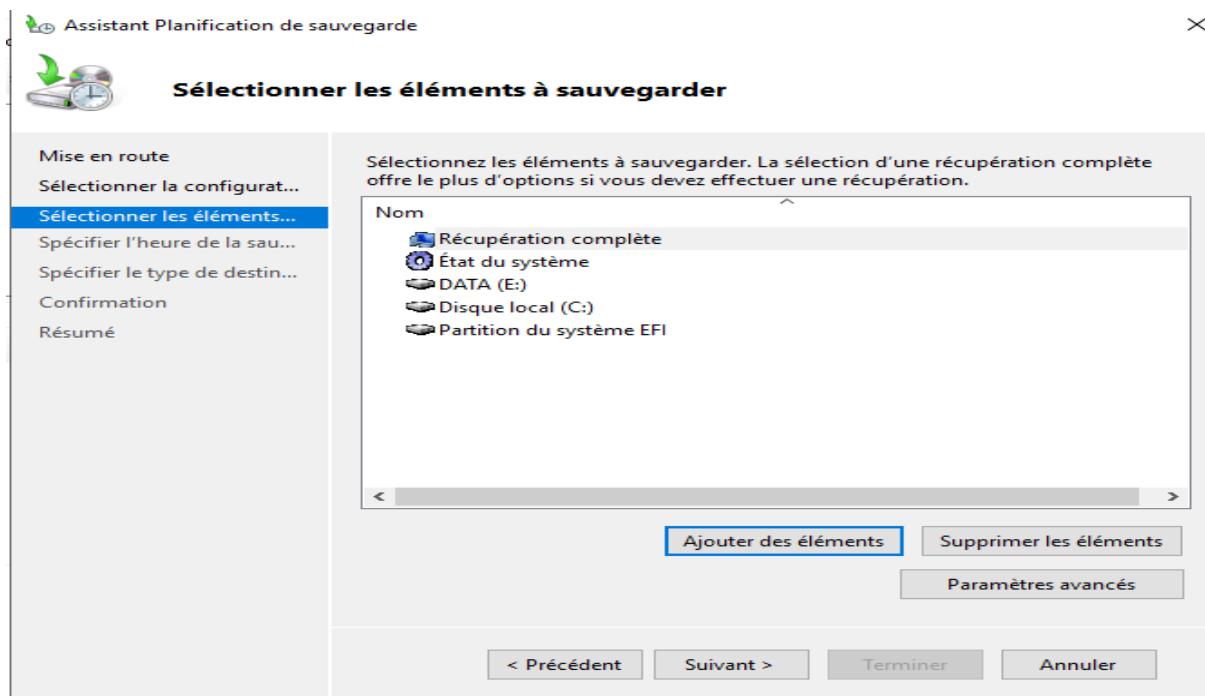
Nous avons sélectionné la sauvegarde personnalisée pour éviter que la sauvegarde ne prenne en compte le volume où est stocker elle-même la sauvegarde.

Selectionnez donc la totalité des volumes à l'exception du Backup01 (Backup02 pour Mulhouse)

Faites ensuite « OK »

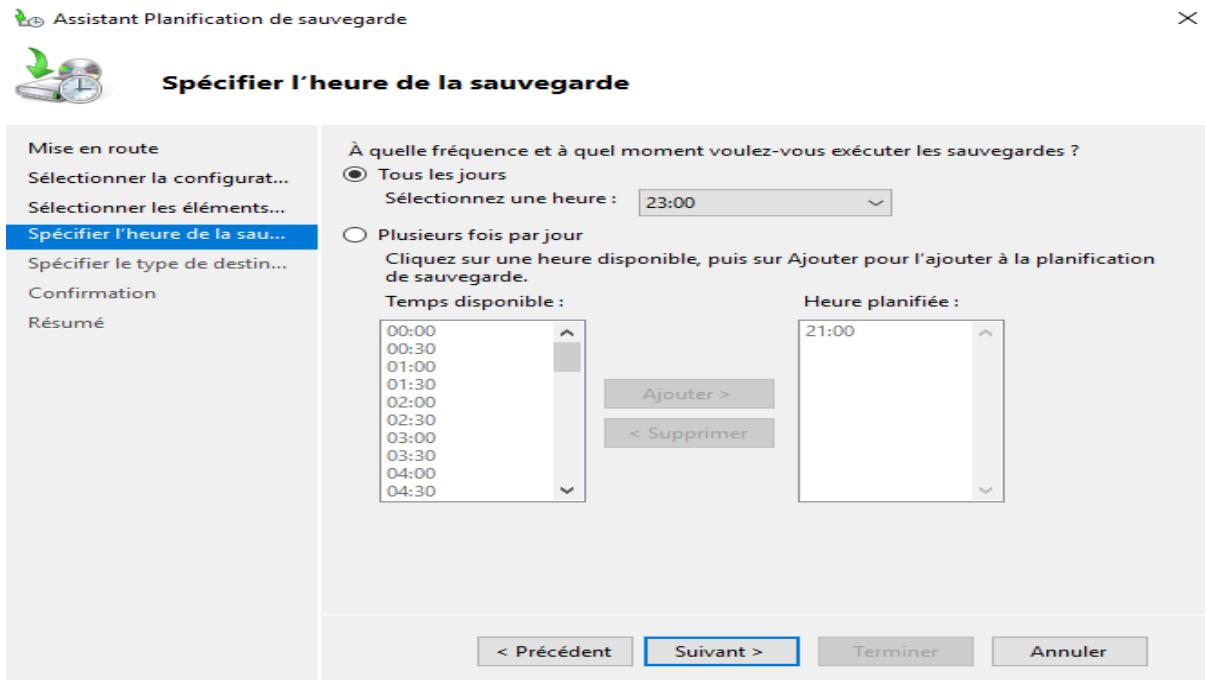


Une fois les éléments sélectionner cliquer sur « suivant »



Selectionner le moment de votre sauvegarde, Ici nous prenons tous les jours à 23h pour éviter que cela n'impacte les utilisateurs la journée.

Cliquer sur « suivant »



Cocher la première case, nous avons un NAS dédié aux sauvegardes

Cliquer sur « suivant »

Spécifier le type de destination

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

Où voulez-vous stocker les sauvegardes ?

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

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

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

< Précédent Suivant > Terminer Annuler

Coché le disque truenas qui serviras de destination à la sauvegarde

Cliquer sur « suivant »

Sélectionner le disque de destination

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

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

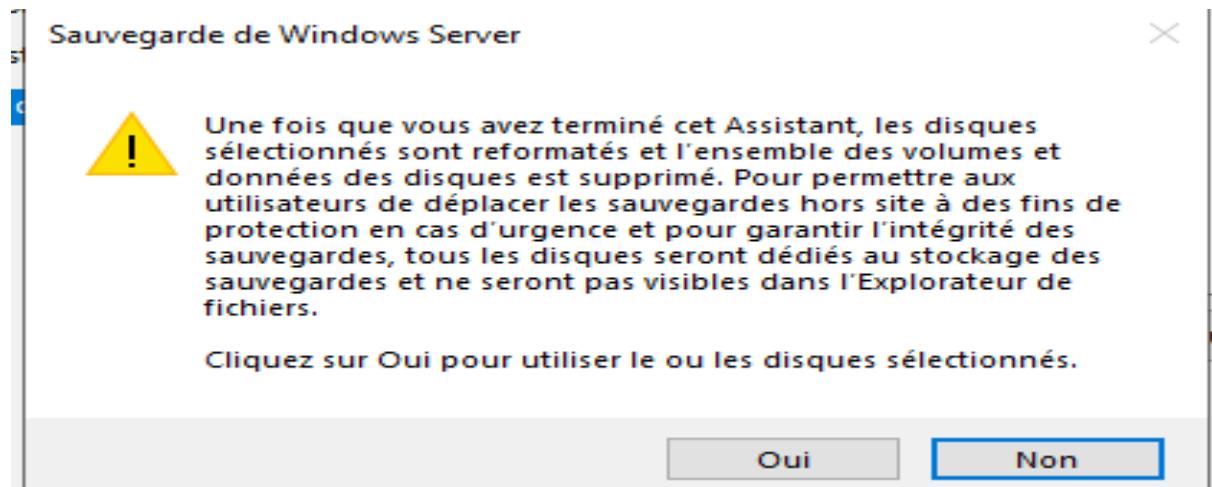
Disques disponibles :

Disque	Nom	Taille	Espace uti...	Volumes prés...
<input checked="" type="checkbox"/> 2	TrueNAS iS...	44,00 Go	12,42 Go	B:\

Afficher tous les disques disponibles...

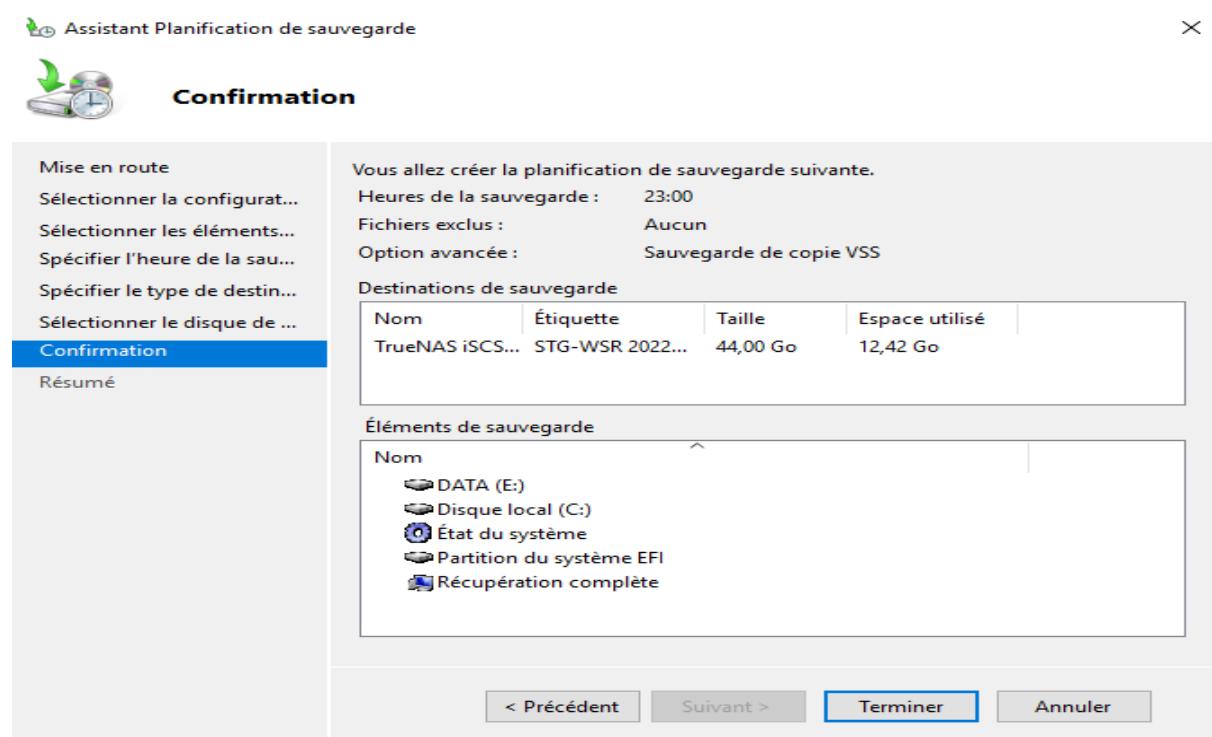
< Précédent Suivant > Terminer Annuler

Un message d'avertissement va s'afficher, faites simplement « OK » nous voulons bel et bien utiliser ce disque

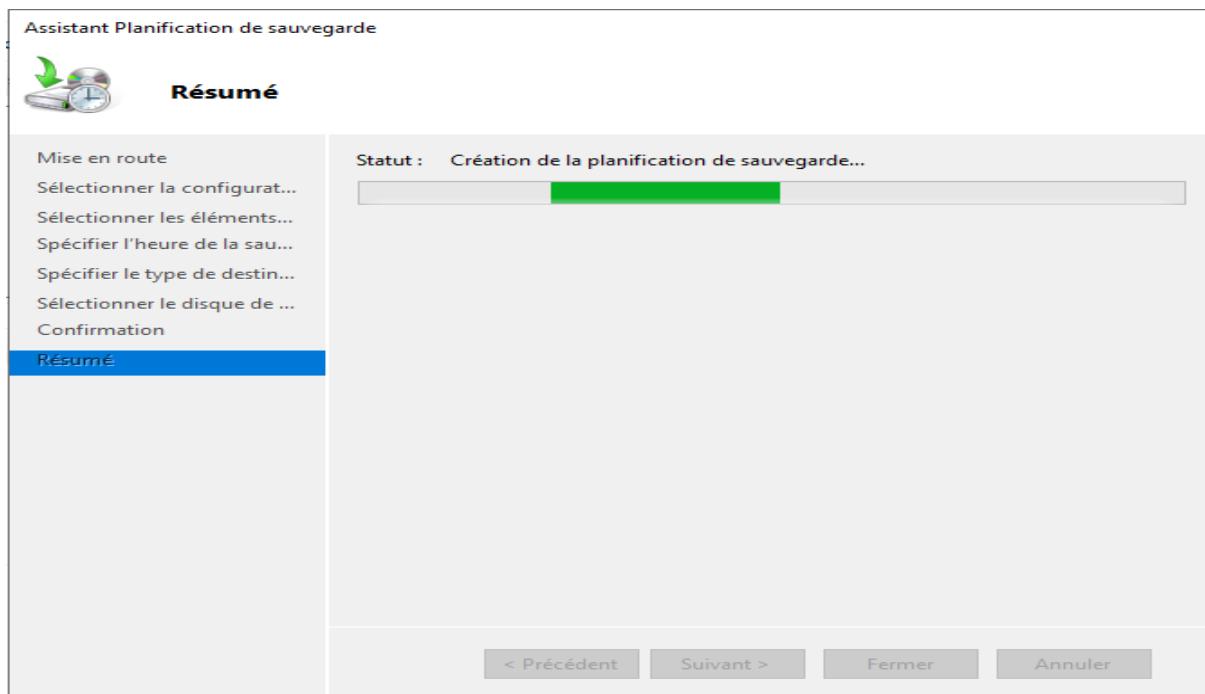


Votre planification de sauvegarde est prête à être effectuer,

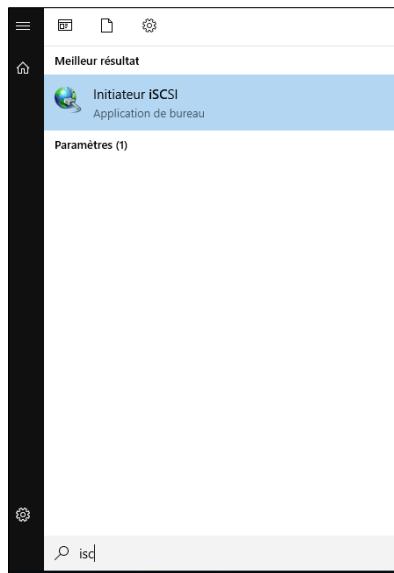
Cliquer sur « Terminer »



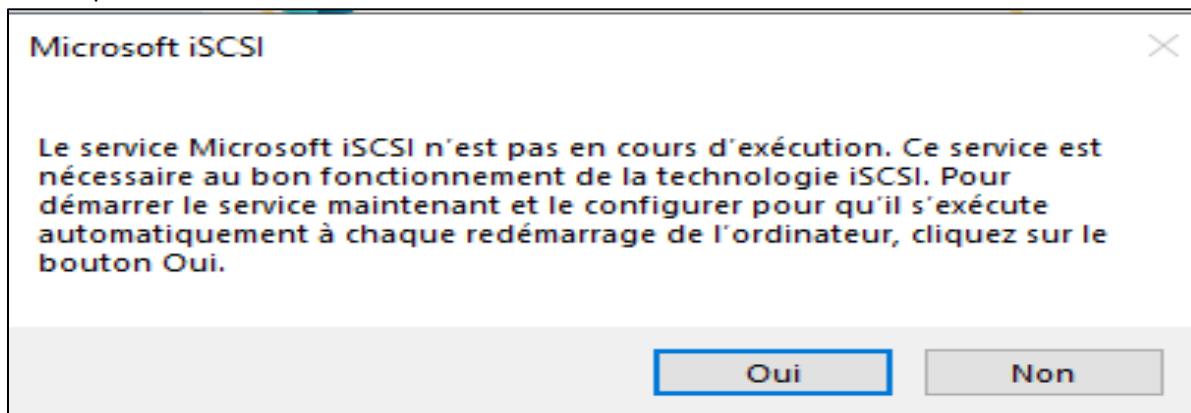
La tâche de planification est en cours de création, patienter que celle-ci se termine



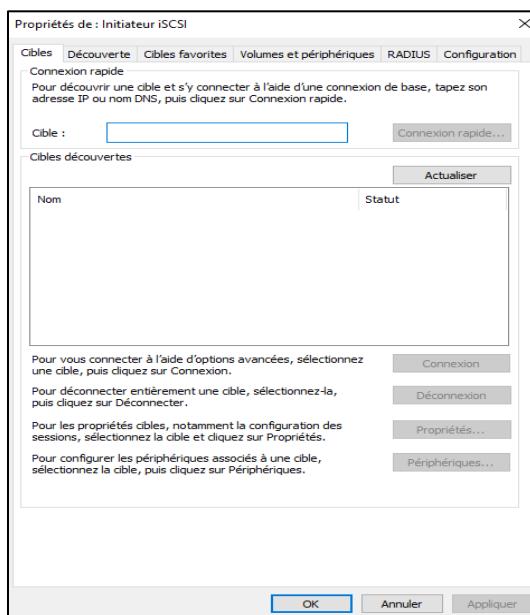
Rendez-vous sur le serveur Windows principal du site de votre NAS. Dans un premier temps, allez dans la barre de recherche de votre Windows serveur et taper « ISCSI » :



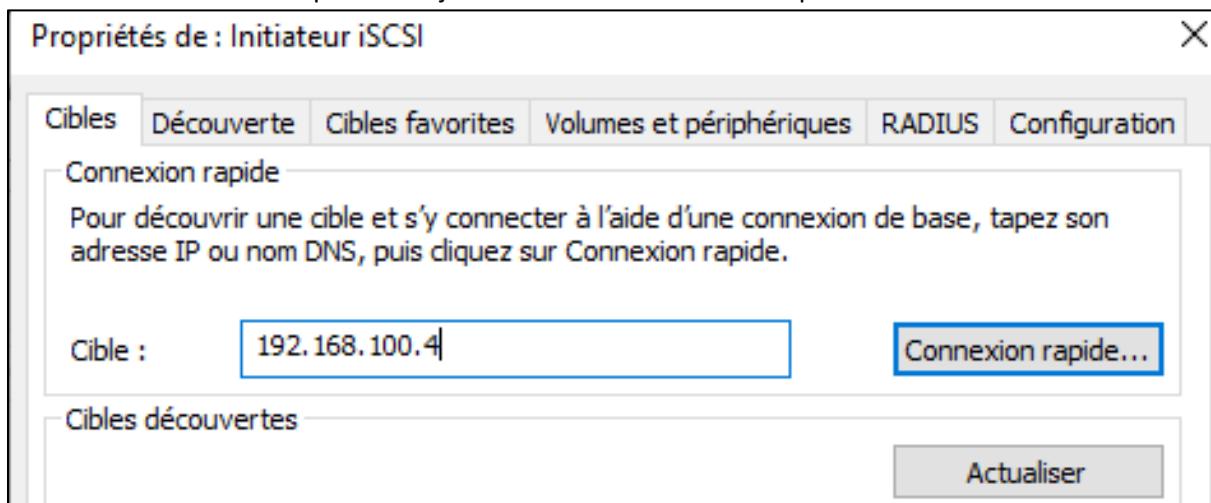
En exécutant l'applicatif il vous sera dit qu'il n'est pas installé sur la machine, faites simplement « oui » pour l'installer :



Une fois le rôle installé cette fenêtre va s'ouvrir :



Entrez l'IP du NAS afin de pouvoir l'ajouter et faites « connexion rapide » :

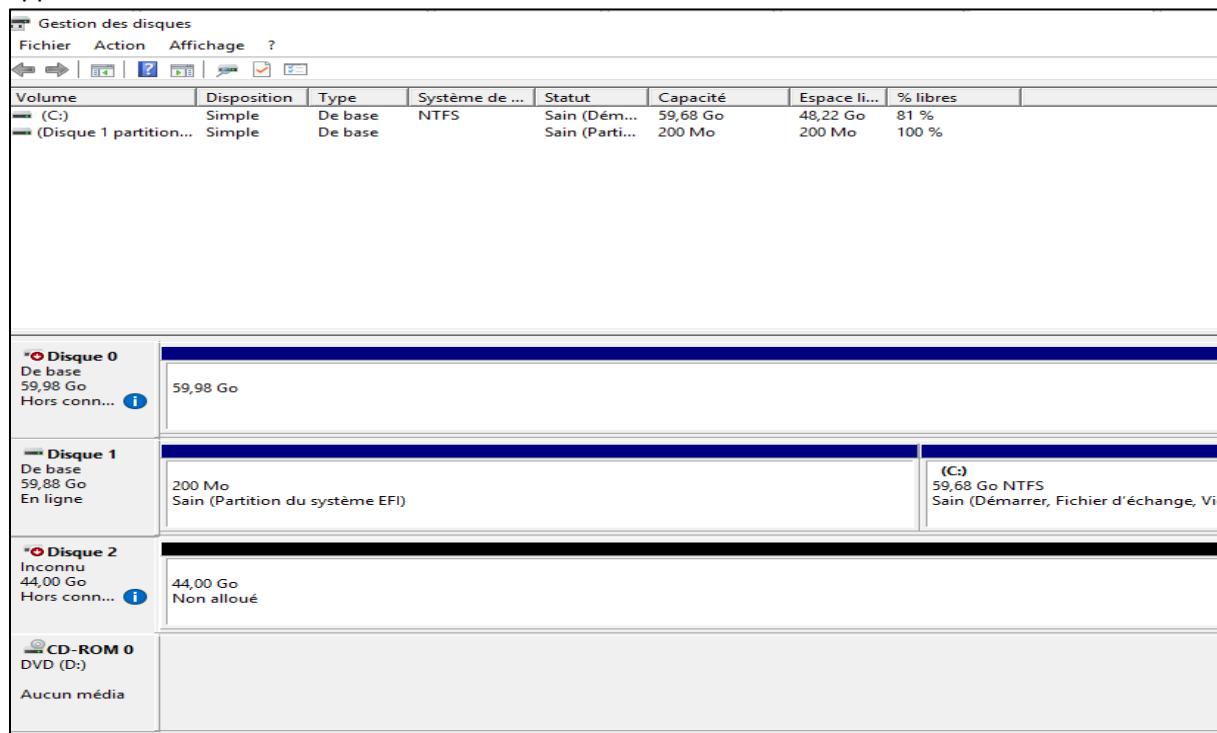


Sélectionnez le NAS et faites « connexion » pour créer la connexion iSCSI :

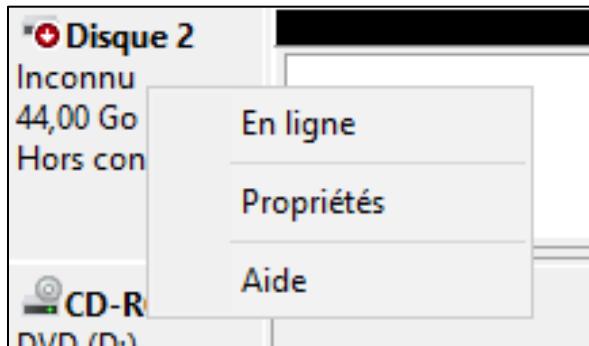
Propriétés de : Initiateur iSCSI

Cibles	Découverte	Cibles favorites	Volumes et périphériques	RADIUS	Configuration
Connexion rapide					
Pour découvrir une cible et s'y connecter à l'aide d'une connexion de base, tapez son adresse IP ou nom DNS, puis cliquez sur Connexion rapide.					
Cible :	192.168.100.4		Connexion rapide...		
Cibles découvertes					
Actualiser					
Nom	Statut				
iqn.2005-10.org.freenas.ctl:backup01	Connecté				
Pour vous connecter à l'aide d'options avancées, sélectionnez une cible, puis cliquez sur Connexion.					
Connexion					
Pour déconnecter entièrement une cible, sélectionnez-la, puis cliquez sur Déconnecter.					
Déconnexion					
Pour les propriétés cibles, notamment la configuration des sessions, sélectionnez la cible et cliquez sur Propriétés...					
Propriétés...					

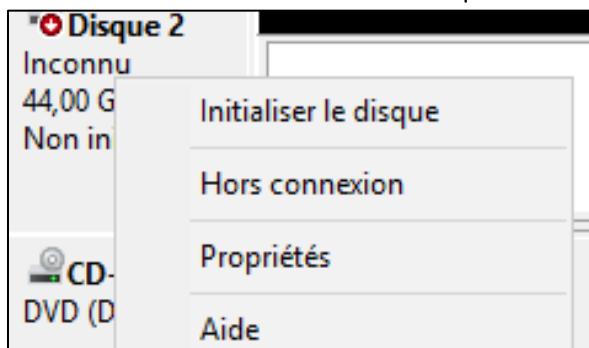
Rendez-vous ensuite dans le gestionnaire de disque. Nous pouvons voir qu'un nouveau disque est apparu :



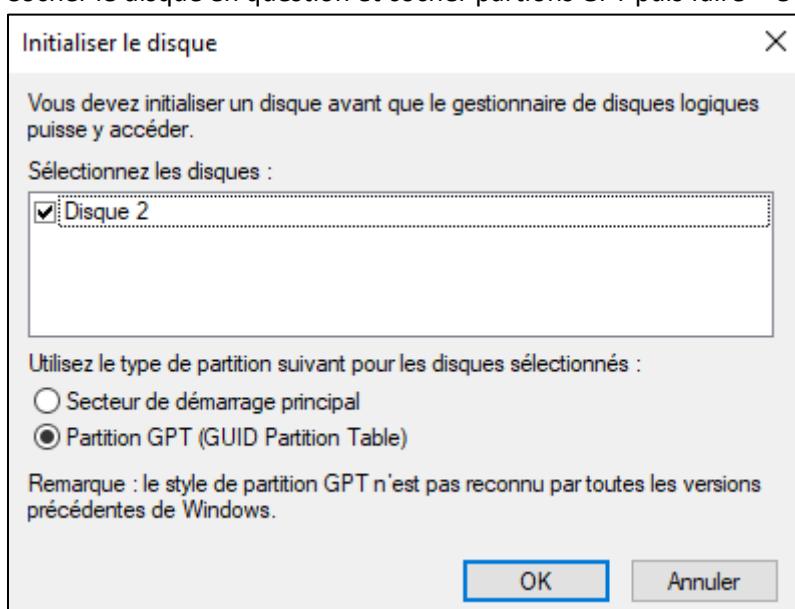
Faire un clic droit sur le disque et faire « En ligne » pour le connecter :



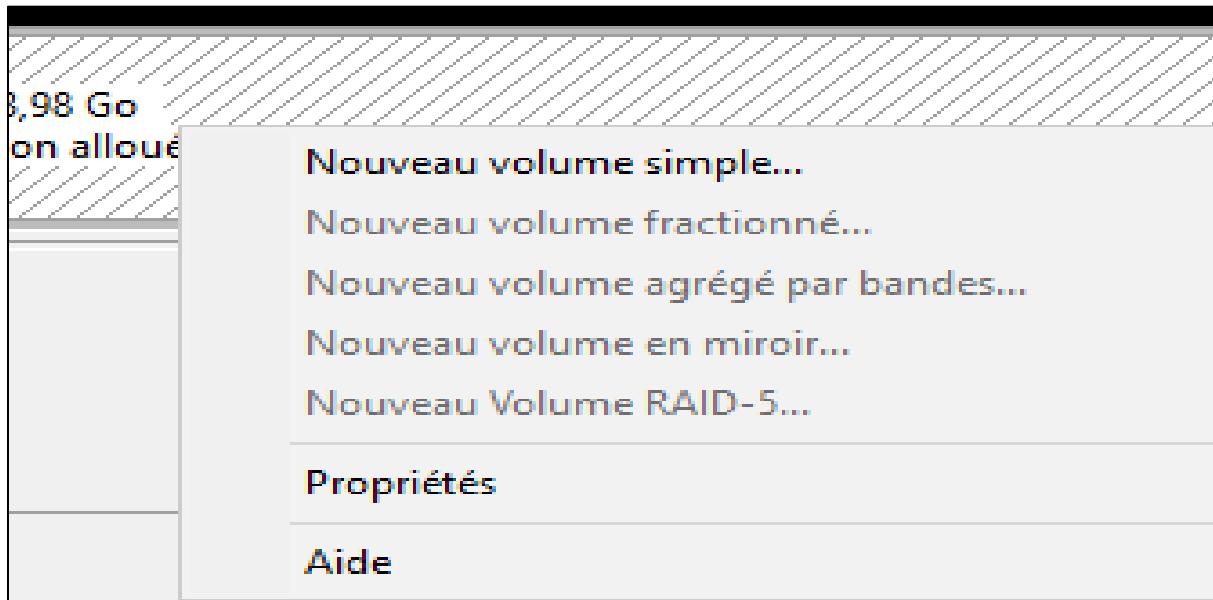
Faire à nouveau un clic droit sur le disque et faites « initialiser le disque » :



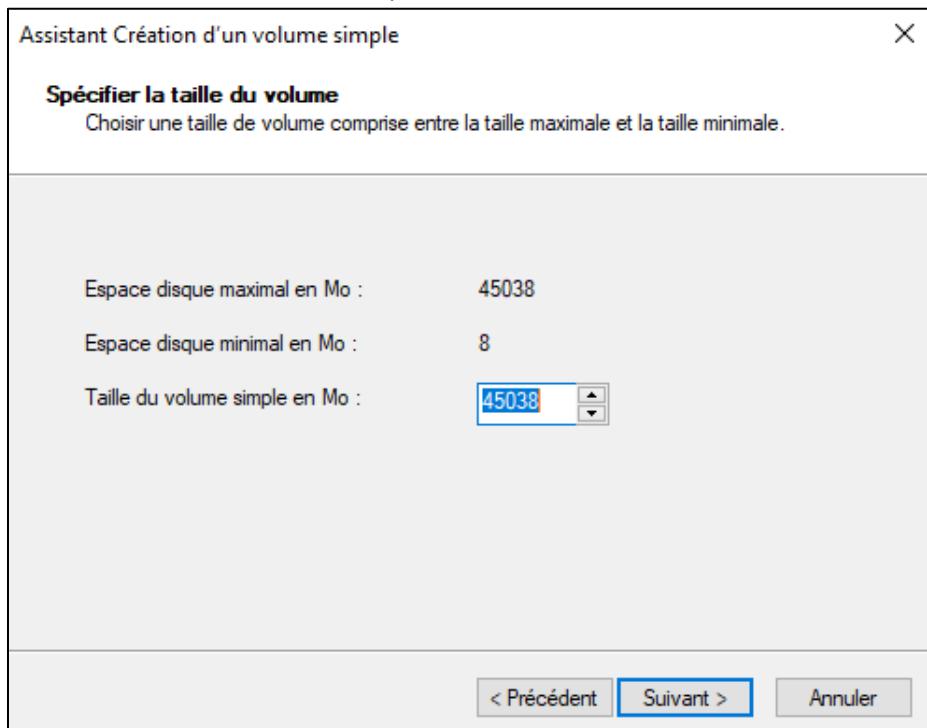
Cocher le disque en question et cocher partitions GPT puis faire « OK »



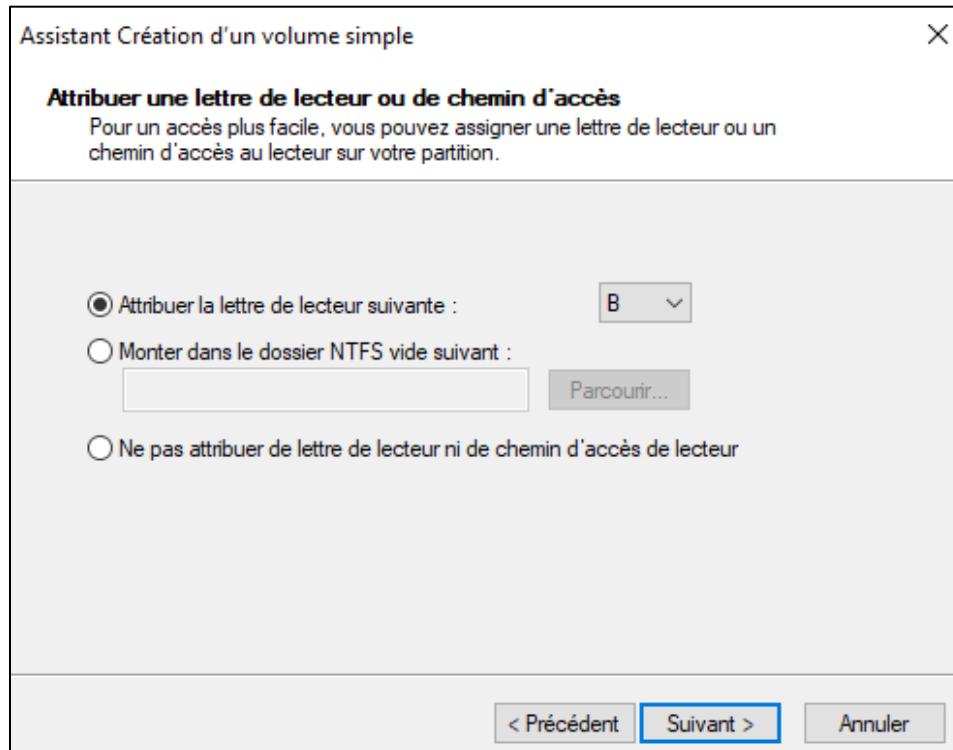
Nous pouvons maintenant faire un clic droit et créer le nouveau volume :



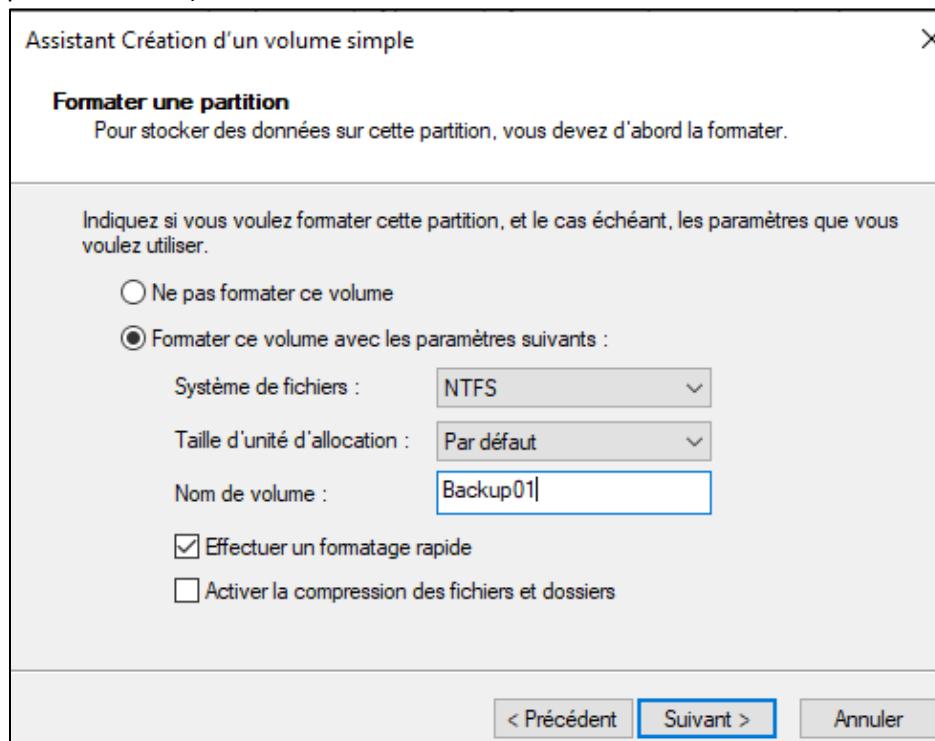
On sélectionne toute la taille disponible :



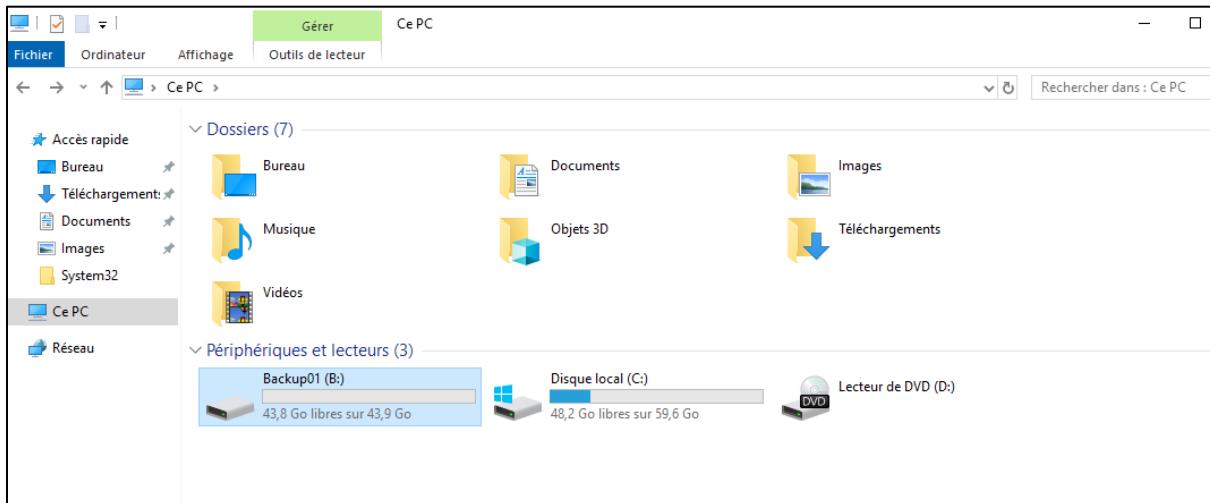
On attribuer la lettre à votre Volume, Ici B :



Faire ensuite un formatage et nommé le nom du volume (Backup01 pour Strasbourg et Backup02 pour Mulhouse) :



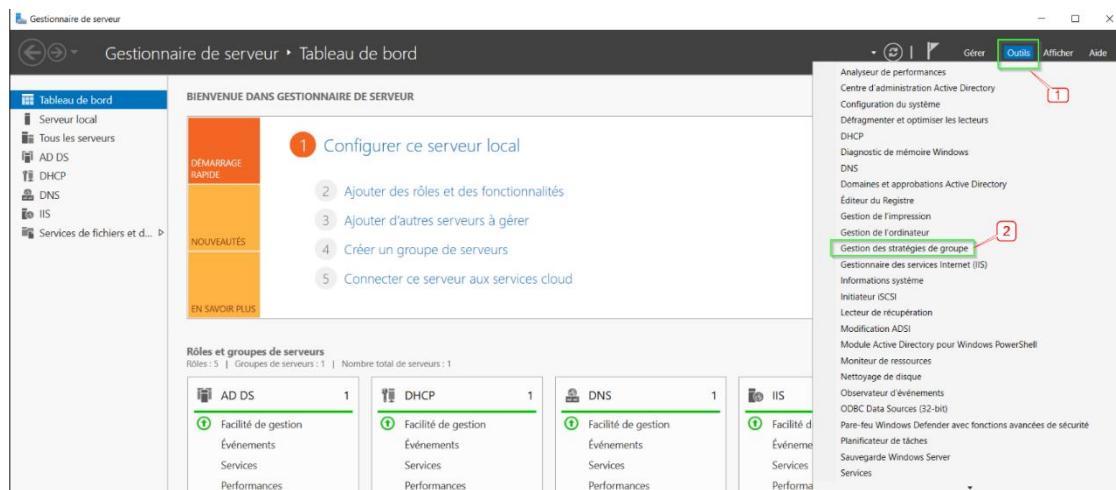
Notre nouveau disque est bien apparu et est bien disponible :



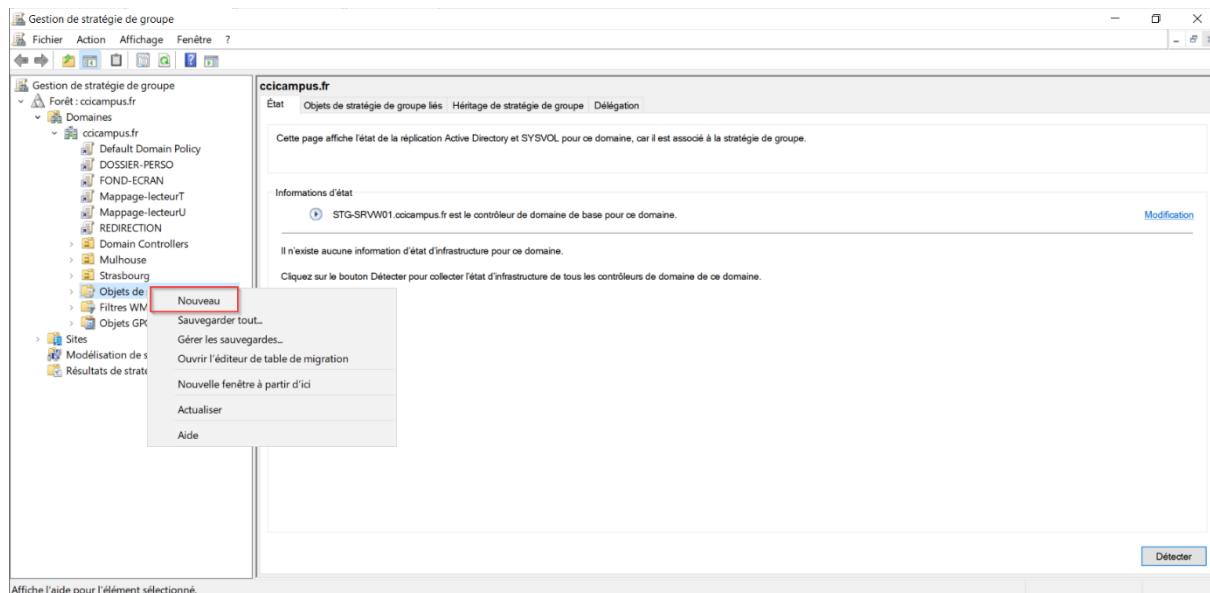
7 Mise en place des GPO

7.1 Crédation du lecteur U pour le dossier personnel de l'utilisateur

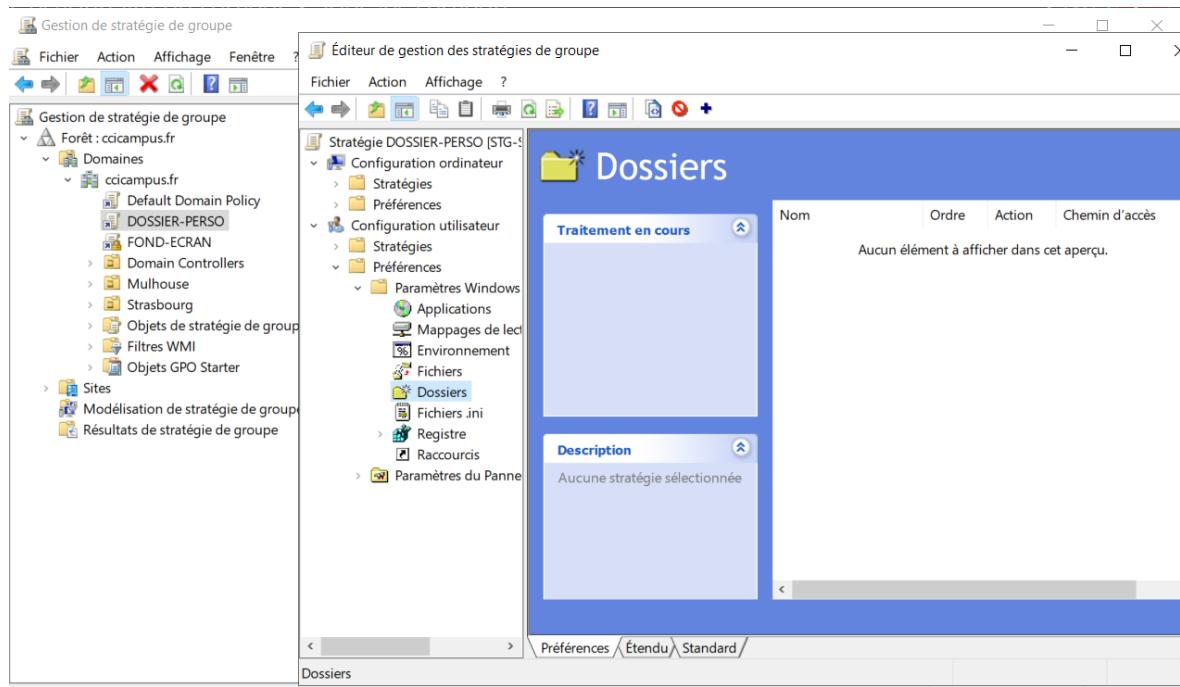
Comme pour toutes les stratégies que l'on va élaborer ci-dessous, il faudra se rendre dans le gestionnaire de stratégie de groupe situé ici :



Et voici l'interface sur laquelle nous devons tomber :



Ensute, on fait un clic droit sur « Objets de stratégie de groupe » et sur « Nouveau ». On renseigne le nom de la stratégie puis on effectue également un clic droit dessus et on clique sur « modifier ». La fenêtre suivante s'ouvrira :

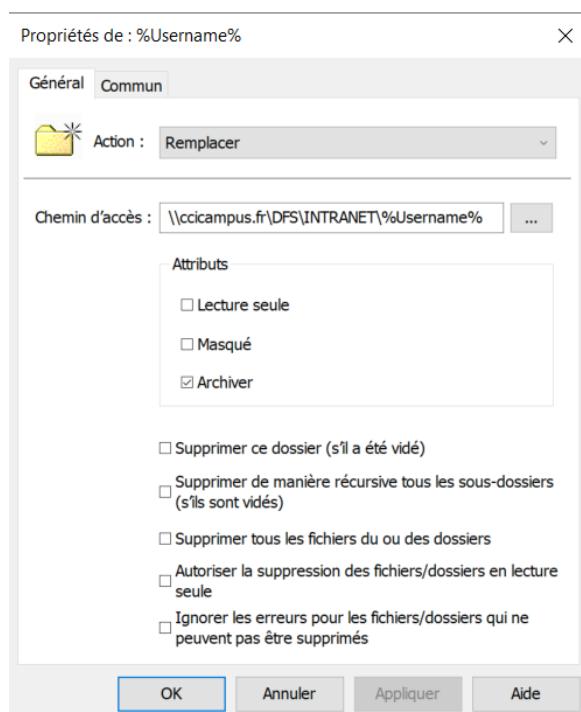


Avant de créer le lecteur, on va lui informer que lors de la première connexion d'un utilisateur de domaine, un dossier sera créé avec le nom de cet utilisateur.

Pour cela, on effectue la manipulation suivante :

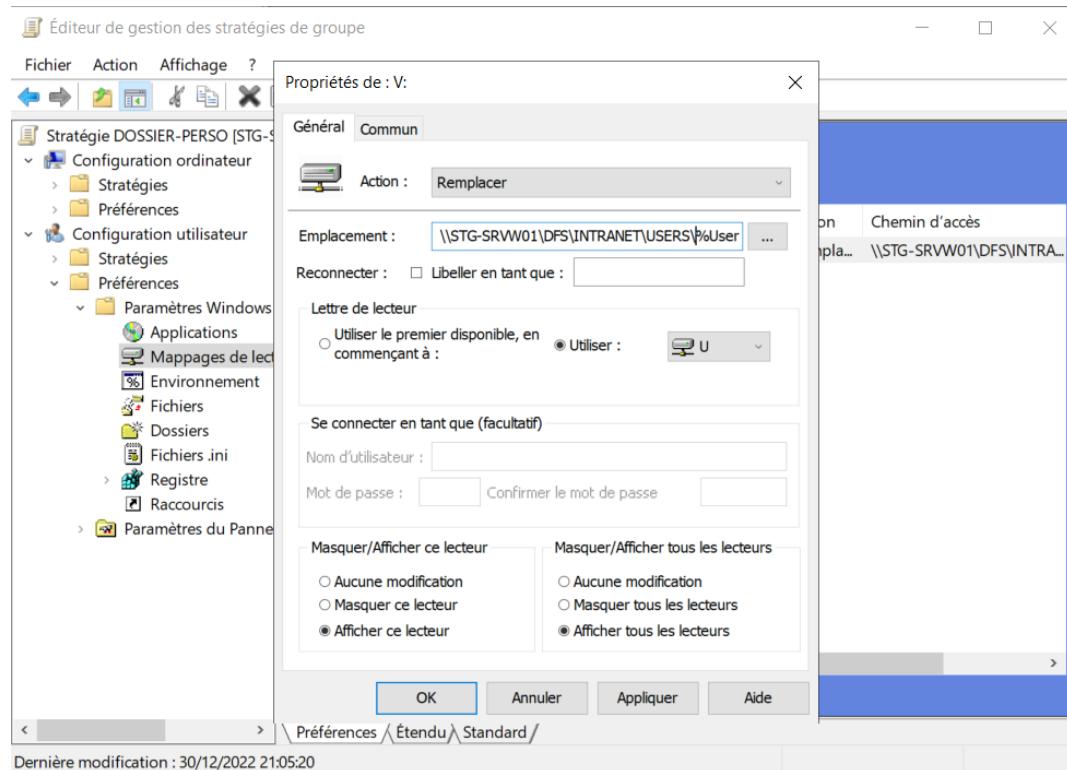
Configuration utilisateur > Préférences > Paramètres Windows > Dossiers > clic droit sur la page

Informer le chemin d'accès du dossier, ici cela sera un chemin réseau : <\\ccicampus.fr\DFS\INTRANET\USERS%\Username%>



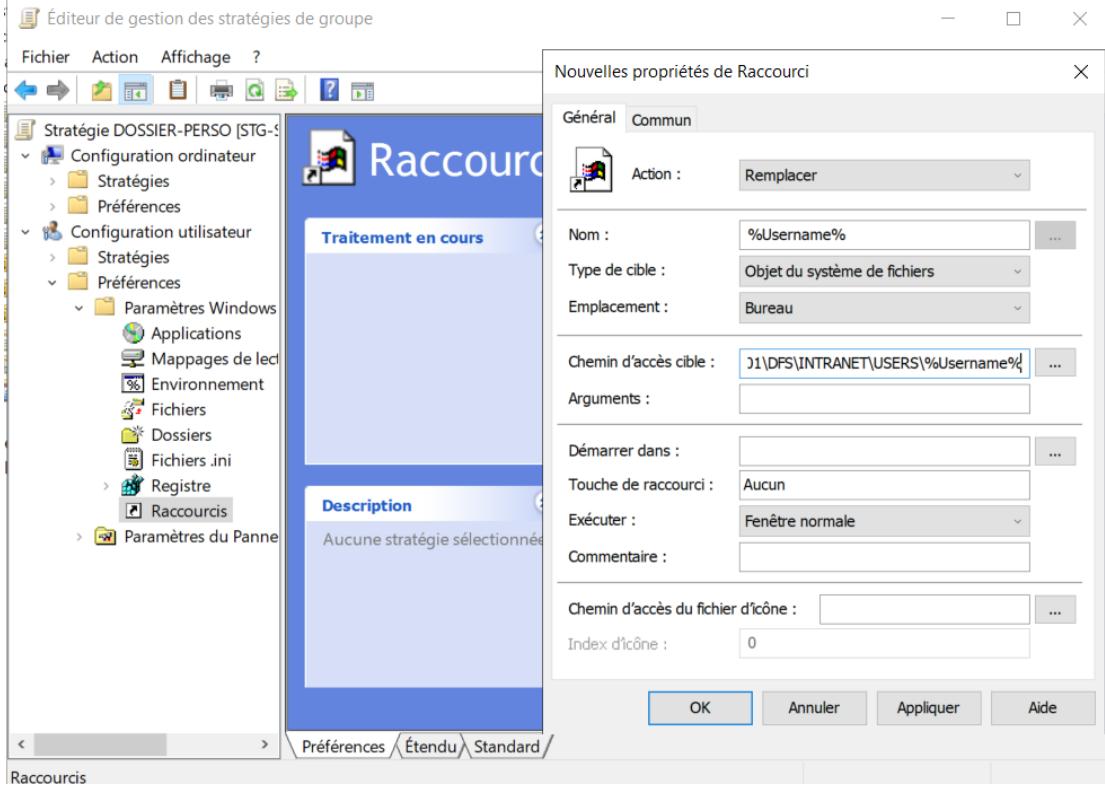
Puis, on crée le mappage du lecteur et on informe son emplacement et sa lettre.

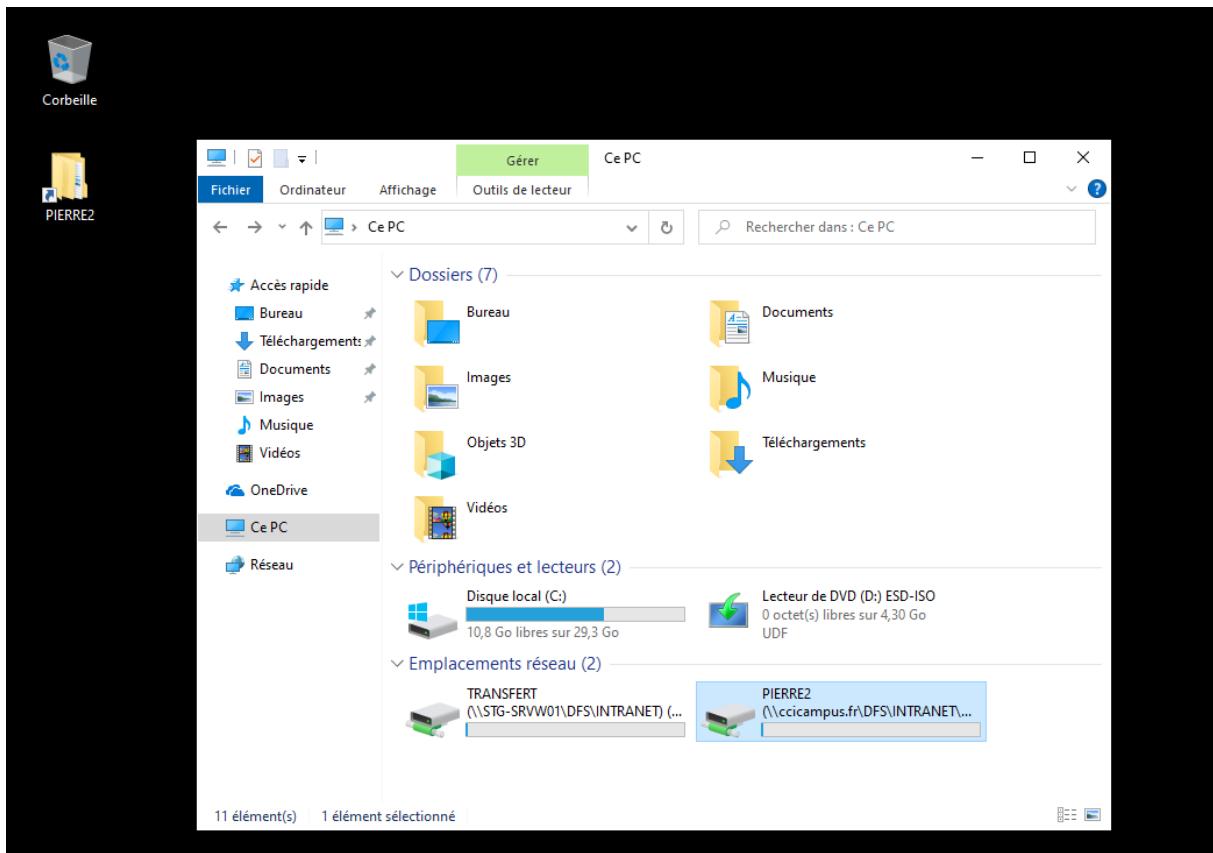
Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteur > clic droit sur l'interface à droite



Dernière modification : 30/12/2022 21:05:20

Puis on va créer un raccourci sur le bureau de ce dossier en y indiquant le chemin d'accès cible :





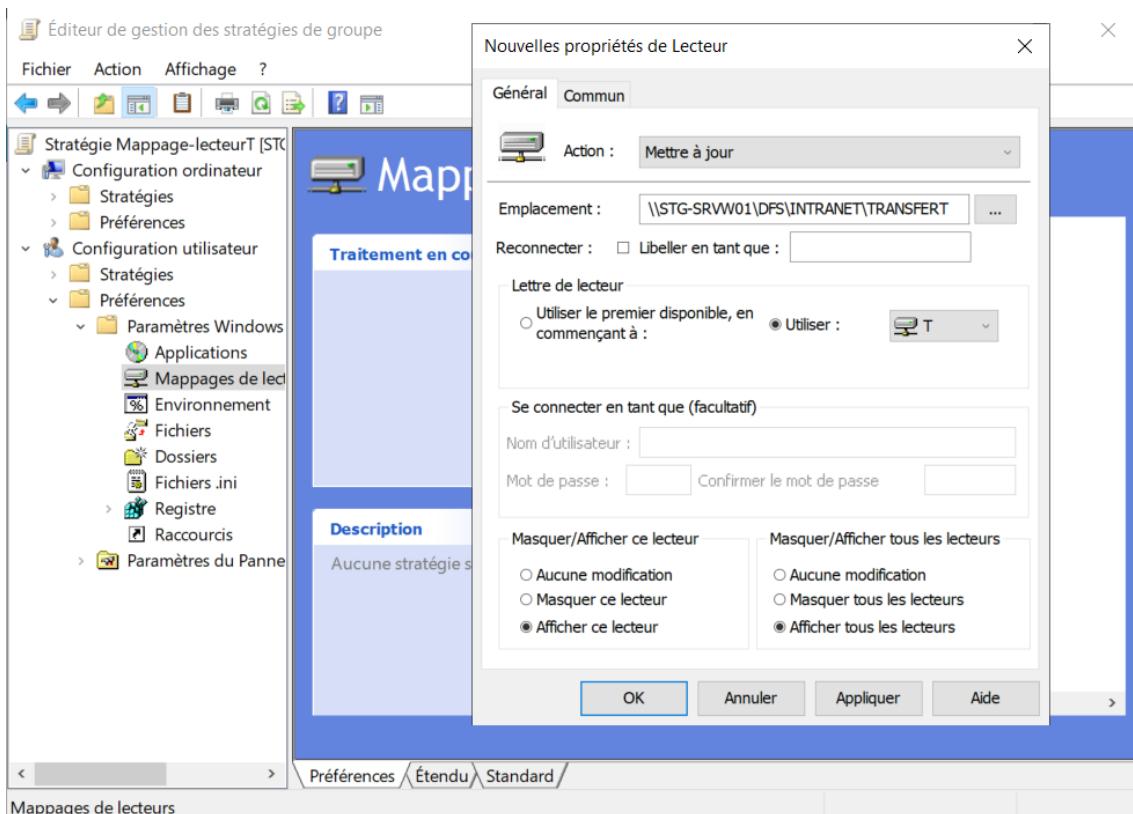
7.2 Crédation du lecteur T sur le répertoire TRANSFERT

Le répertoire TRANSFERT a été créé lors de la configuration du service DFS et DFSR, je vous invite, une nouvelle fois, à consulter la documentation sur le DFS.

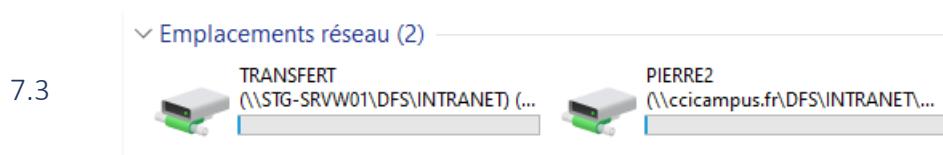
L'élaboration du lecteur T se fait très rapidement, tout d'abord comme pour la première stratégie, on va créer une autre pour ce lecteur-ci (en effectuant les mêmes manipulations vues au-dessus). Par la suite, on se dirige vers :

Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteur > Clic droit sur l'interface et sur nouveau

On y renseigne également l'emplacement du lecteur et sa lettre. Voilà ce qu'il doit apparaître :

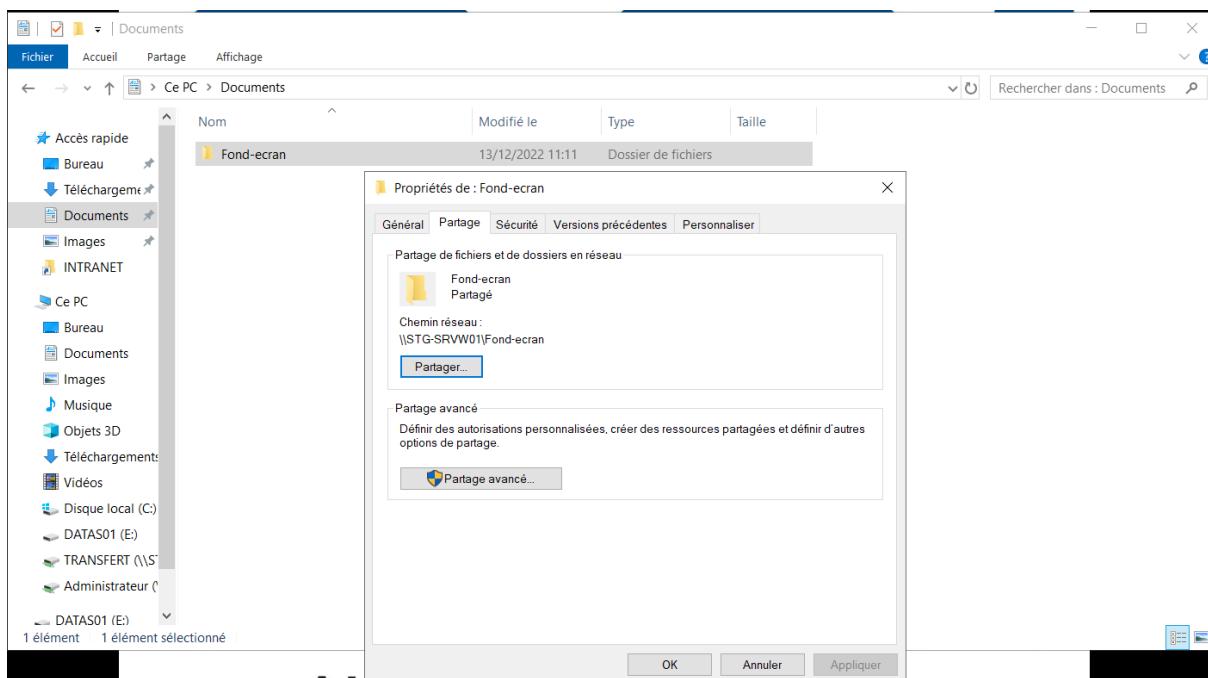


Le lecteur a bien été créé :



Déployer et bloquer un fond d'écran

On va premièrement créer un dossier qui détiendra l'image (jpg) que l'on déployera et que l'on va partager.



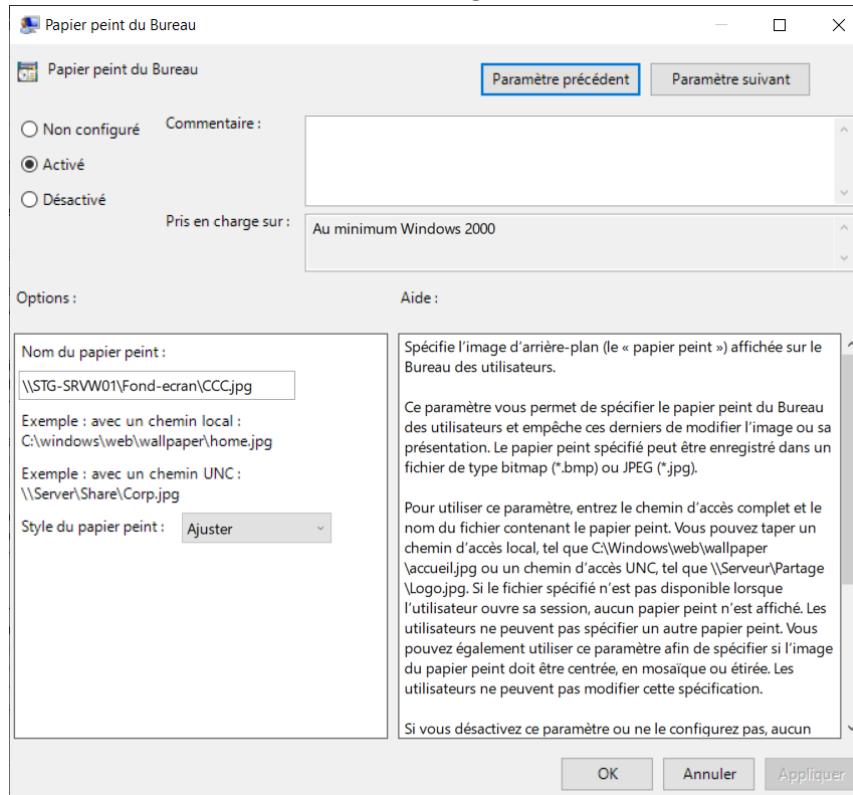
Une fois que cela a été fait, on passe à la création d'une nouvelle stratégie.

Pour affecter un fond d'écran précis :

Configuration utilisateur > Modèles d'administration > Bureau > Bureau > Papier peint du bureau> clic droit et modifier

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	Non configuré	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
Empêcher la modification 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

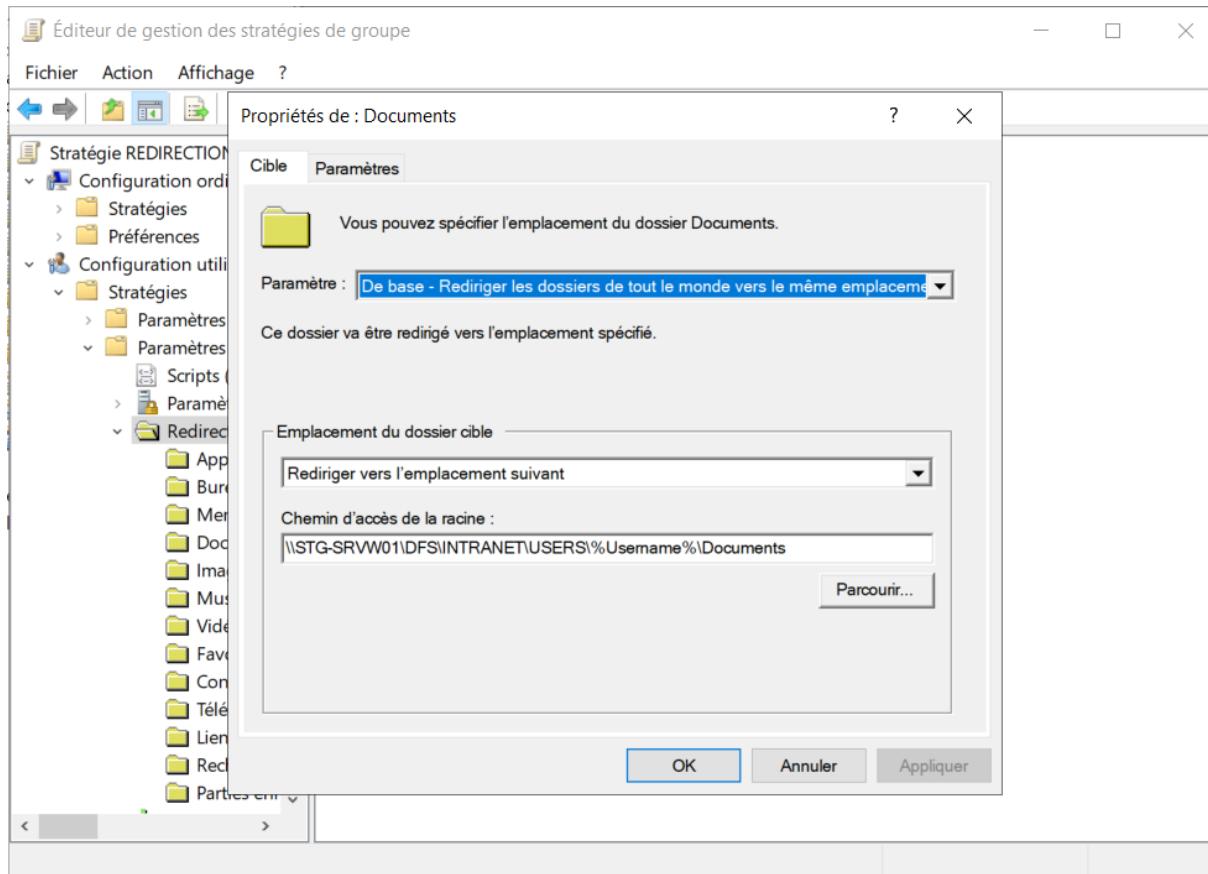
On active et informe où chercher l'image :



7.4 Rediriger les dossiers « mes documents » et « bureau » vers le dossier personnel de l'utilisateur

De même, on crée une nouvelle stratégie puis on se dirige vers :

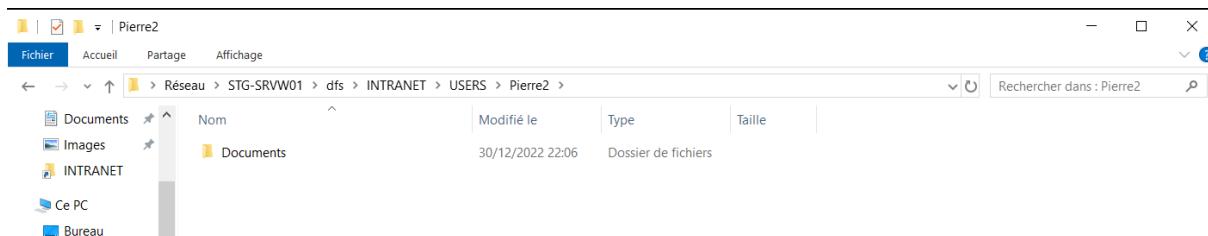
Configuration utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers > Documents > Propriétés



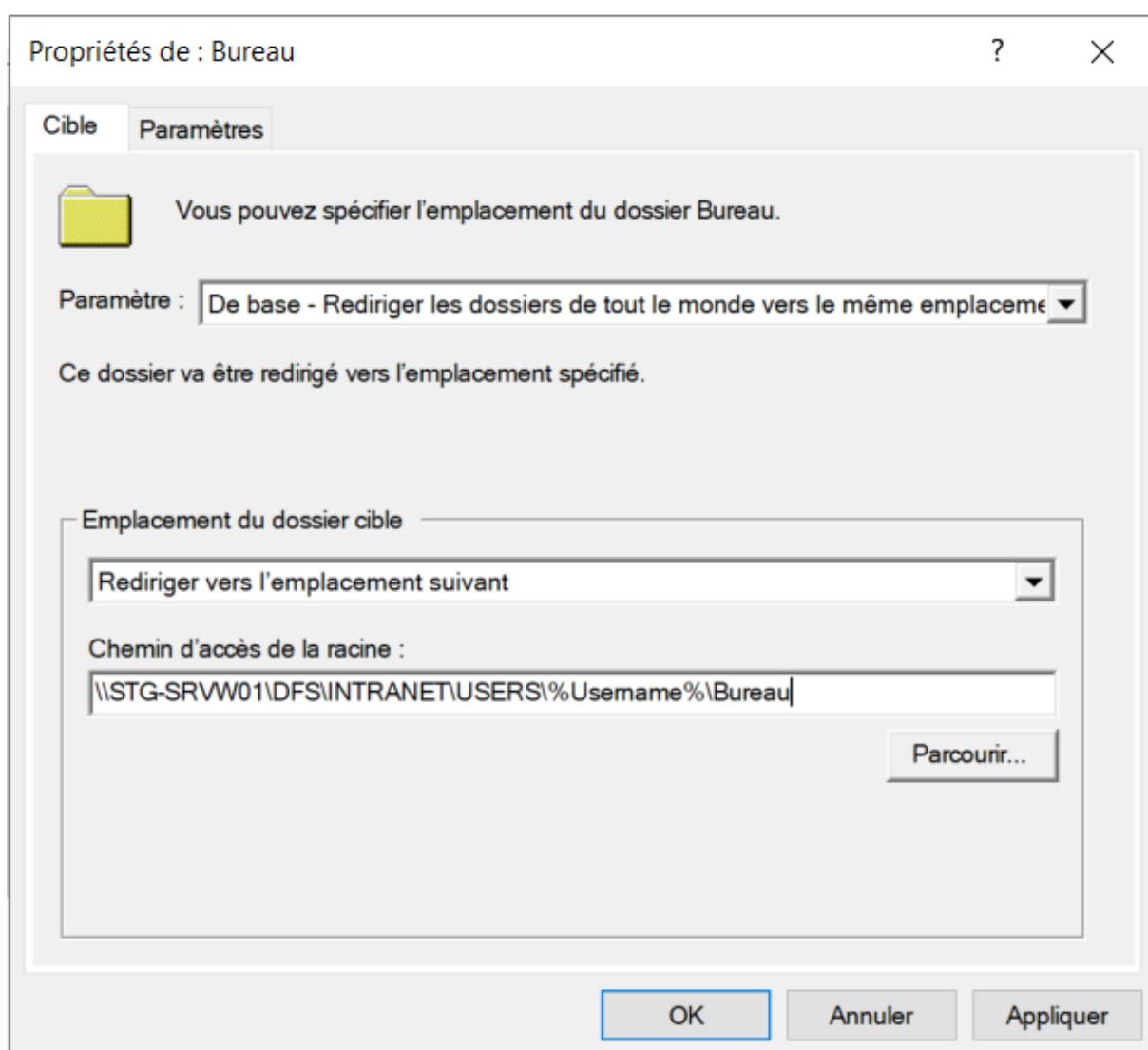
Ici on redirige le dossier Documents et Bureau, pour cela on indique où le dossier sera redirigé, en l'occurrence sur le chemin réseau suivant :

<\\STG-SRVW01\DFS\INTRANET\USERS\%Username%\Documents>

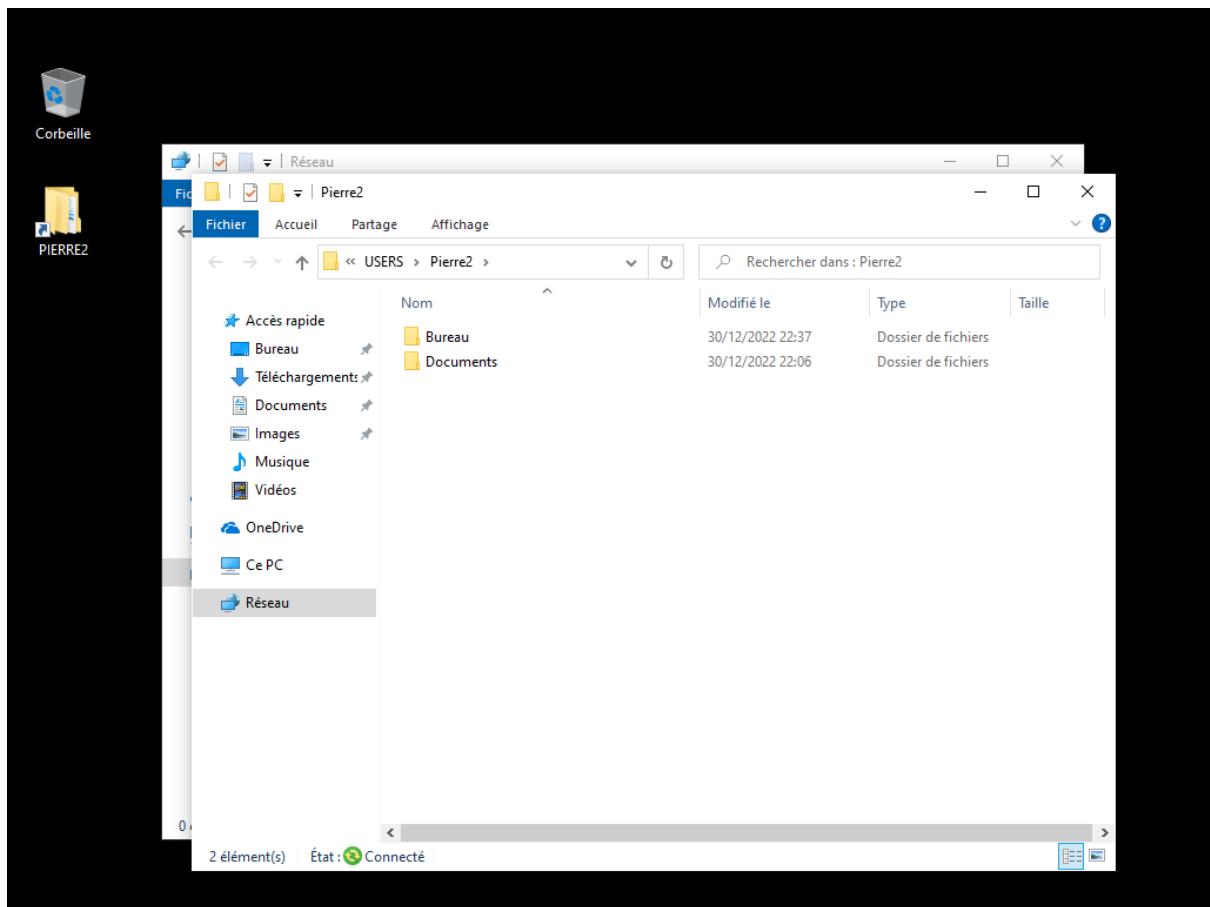
%Username% fait référence au dossier personnel créé préalablement et « Documents » au dossier qui sera redirigé.



Et pour le bureau :

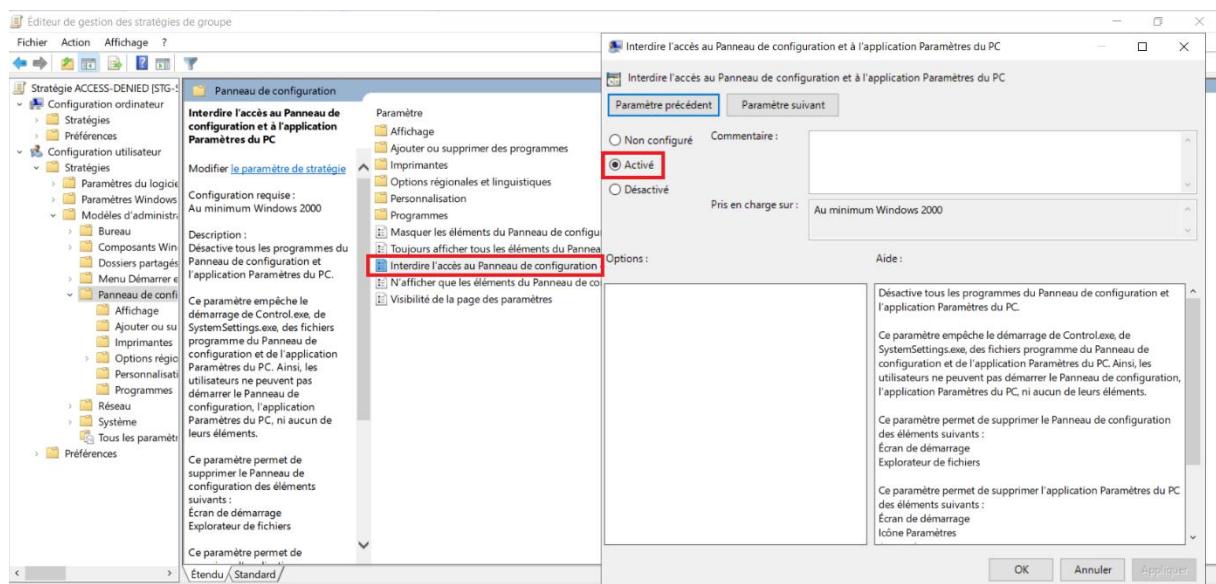


On y a également la redirection :



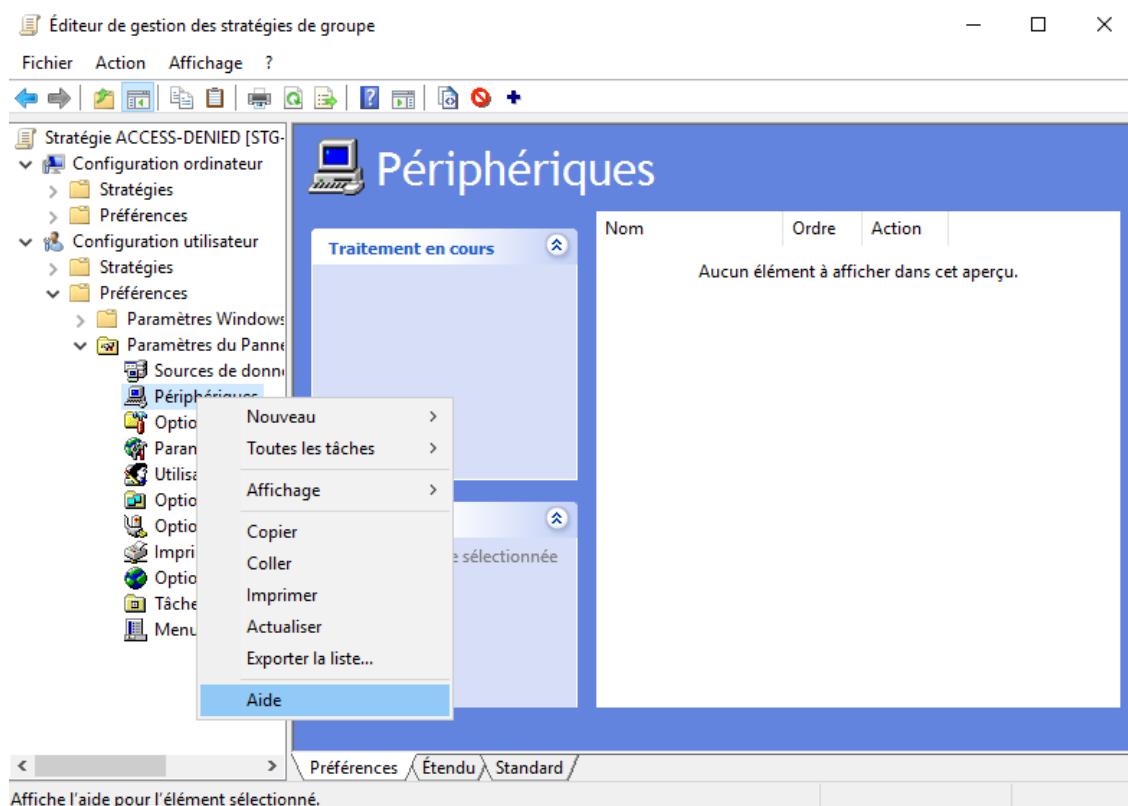
7.5 Interdire l'accès au panneau de configuration

Pour le panneau de configuration rien de plus simple, on suit le chemin suivant :

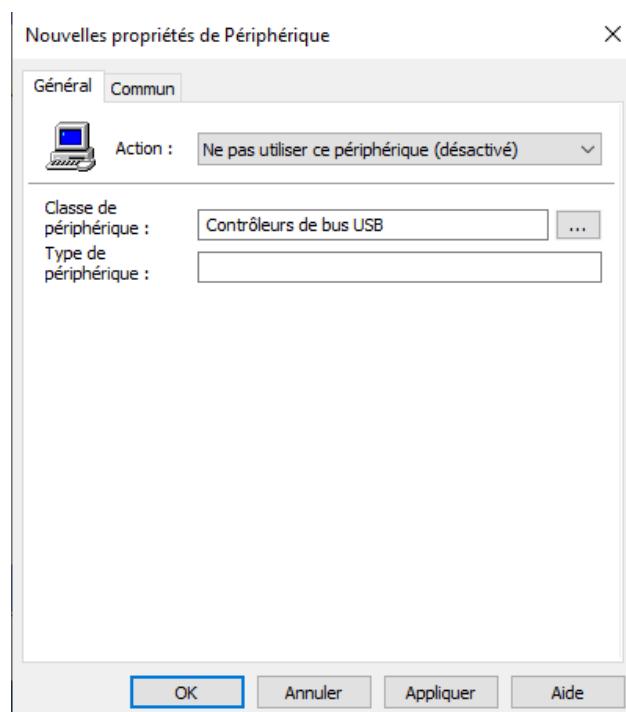


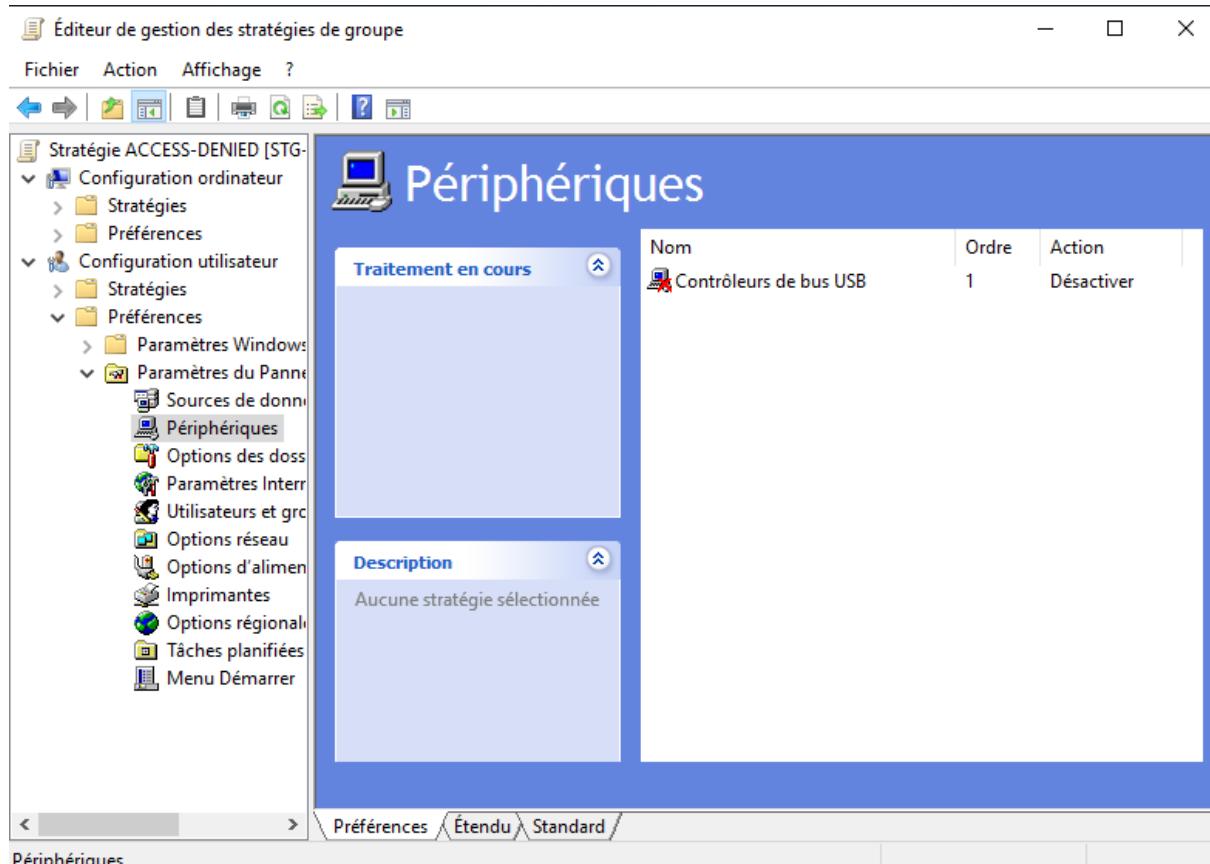
7.6 Bloquer les ports USB

On se dirige vers le chemin suivant et on clique sur nouveau :



On indique la classe de périphérique à bloquer :





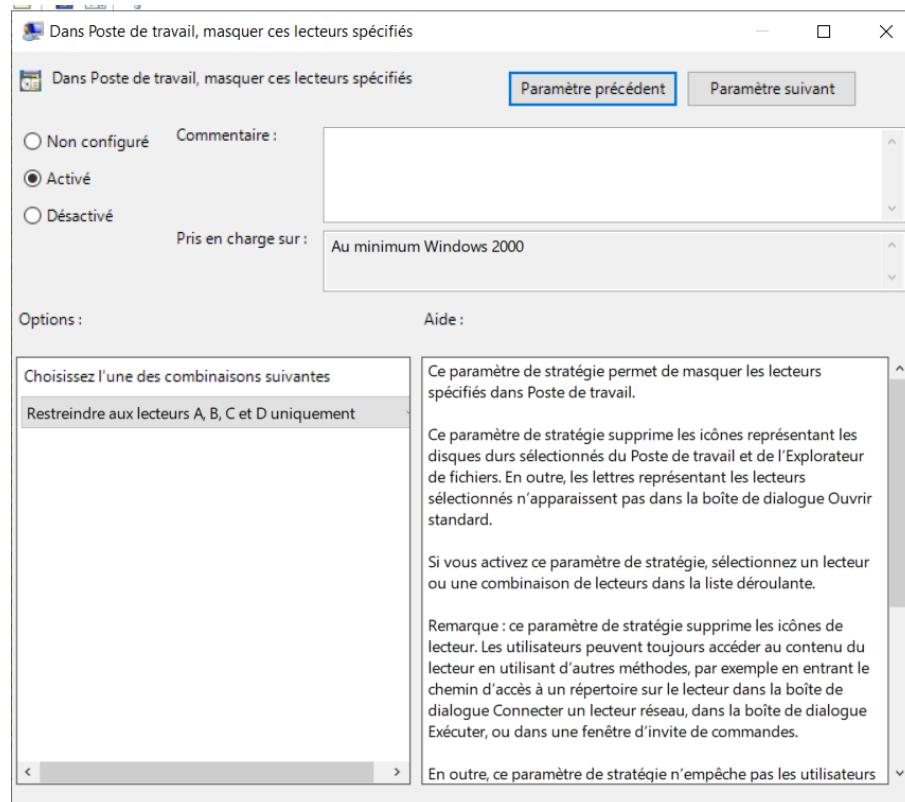
7.7 Masquer et bloquer les accès aux disques locaux des postes

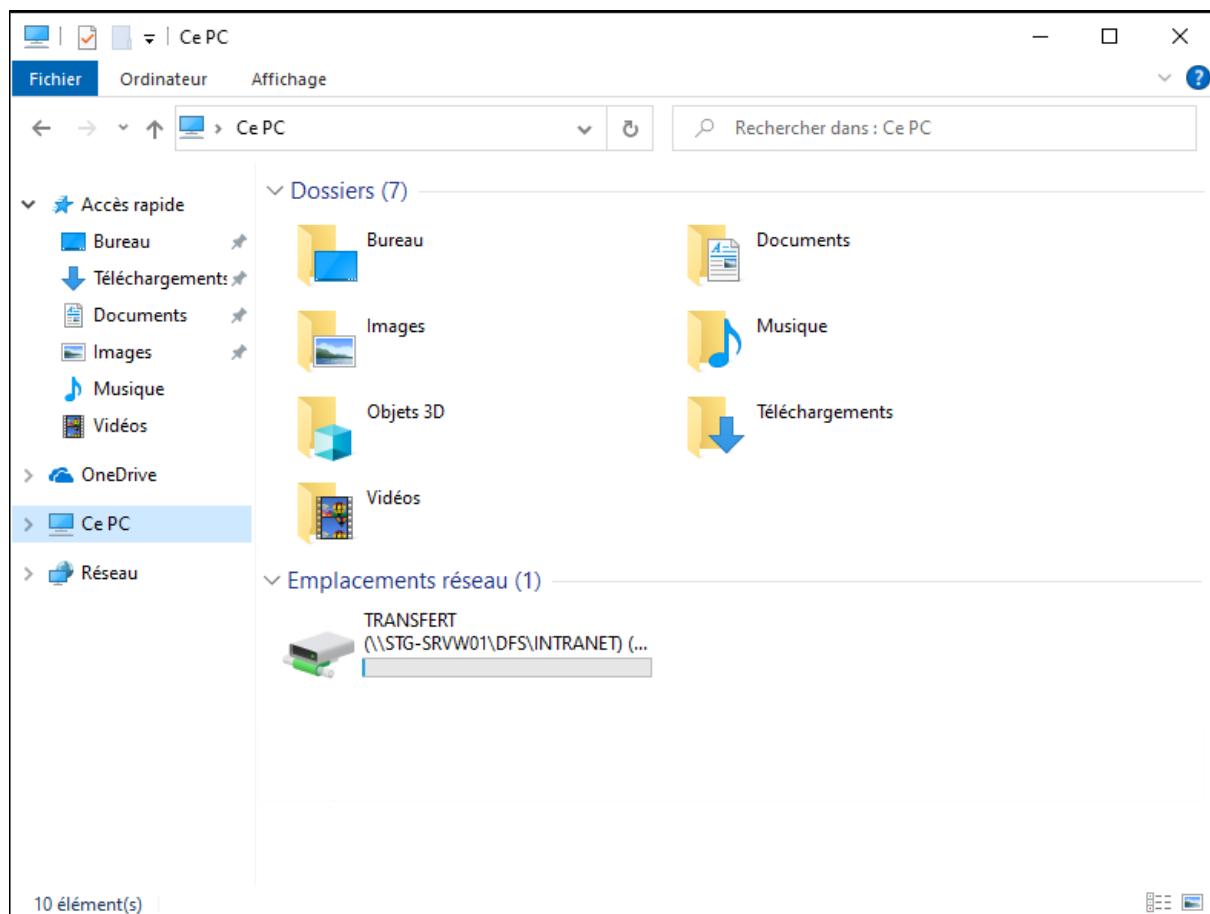
Pour masquer les lecteurs, rendez-vous à cet endroit :

Configuration utilisateur > Stratégies > Modèles d'administrations > Composants windows > Explorateurs de fichiers > Dans Poste de travail, masquer ces lecteurs

Paramètre	État	Commentaire
Boîte de dialogue commune d'ouverture de fichiers	Non configuré	Non
Volet des cadres de l'explorateur	Non configuré	Non
Désactiver l'affichage des miniatures et afficher seulement les icônes sur les dossiers réseau	Non configuré	Non
Désactiver la mise en cache des miniatures dans les fichiers masqués thumbs.db	Non configuré	Non
Activer l'interface classique	Non configuré	Non
Emplacement de tous les fichiers de définition de bibliothèques pour les utilisateurs/ordinateurs.	Non configuré	Non
Désactiver les fonctionnalités de bibliothèque Windows qui utilisent des données de fichier indexé	Non configuré	Non
Désactiver les dossiers communs	Non configuré	Non
Désactiver l'affichage des entrées de recherche récentes de la zone de recherche de l'Explorateur de fichiers	Non configuré	Non
Désactiver l'affichage des fichiers avec le ruban réduit	Non configuré	Non
Ne pas rechercher les raccourcis de l'environnement lors de l'exploration	Non configuré	Non
Nombre maximal de documents récents	Non configuré	Non
Supprimer les fonctionnalités de gravure de CD	Non configuré	Non
Désactiver la mise en cache des miniatures	Non configuré	Non
Supprimer l'interface utilisateur permettant de modifier les paramètres d'animation des menus	Non configuré	Non
Supprimer l'interface utilisateur permettant de modifier les paramètres de l'indicateur de navigation au clavier	Non configuré	Non
Dans Poste de travail, masquer ces lecteurs spécifiés	Non configuré	Non
Ne pas afficher «Tout le réseau» dans les emplacements réseau	Non configuré	Non
Supprimer le menu Fichier de l'Explorateur de fichiers	Non configuré	Non
Ne pas autoriser l'ouverture des Options des dossiers à partir du bouton Options de l'onglet Affichage du ruban	Non configuré	Non
Supprimer l'onglet Matériel	Non configuré	Non
Masquer l'élément Gérer du menu contextuel de l'Explorateur de fichiers.	Non configuré	Non
Supprimer les Documents partagés du Poste de travail	Non configuré	Non
Supprimer les options «Connecter un lecteur réseau» et «Déconnecter un lecteur réseau»	Non configuré	Non
Ne pas déplacer les fichiers supprimés vers la Corbeille	Non configuré	Non
Ne pas demander d'autres informations d'identification	Non configuré	Non
Supprimer le lien Relancer la recherche de Recherche sur Internet	Non configuré	Non
Supprimer l'onglet Sécurité	Non configuré	Non
Supprimer le bouton Rechercher de l'Explorateur de fichiers	Non configuré	Non
Désactiver le tri numérique dans l'Explorateur de fichiers	Non configuré	Non

On choisit les lecteurs qu'on souhaite masquer, en l'occurrence les lecteurs principaux (C:\ et D :\)

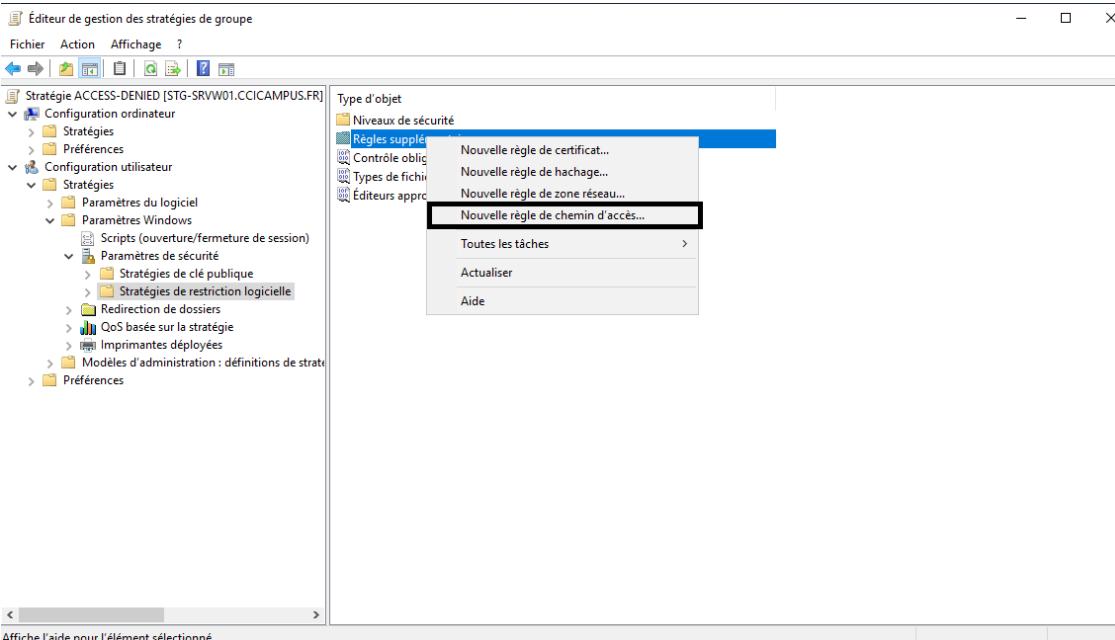
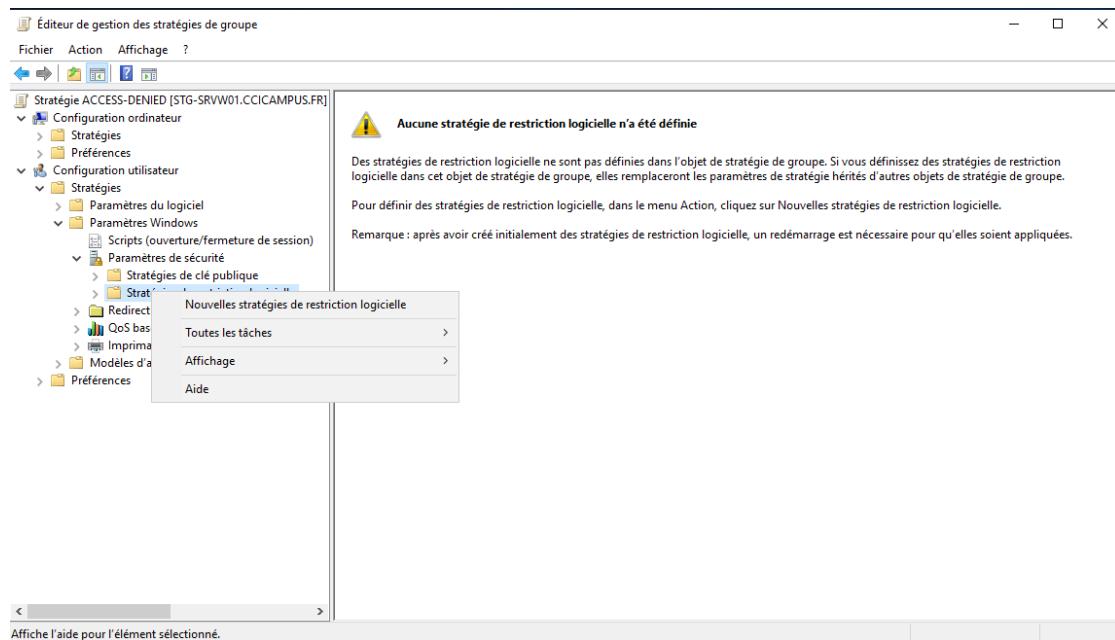


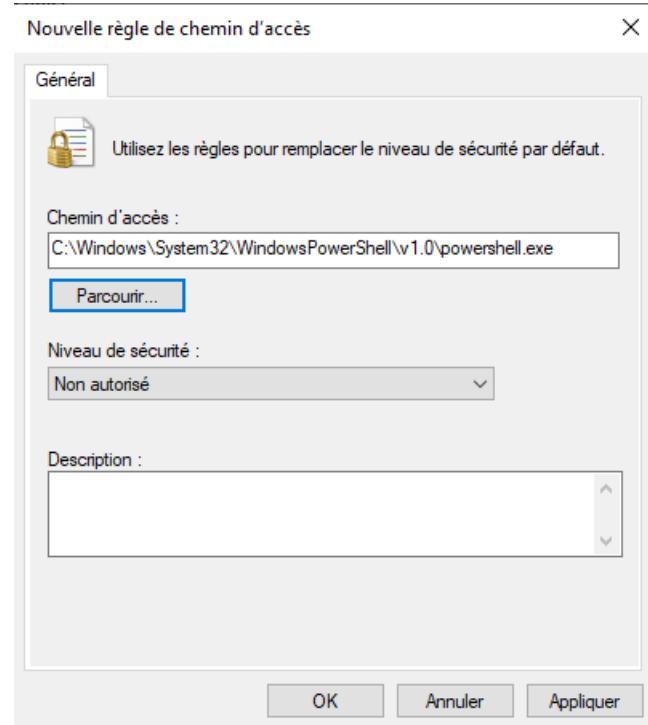


7.8 Bloquer l'accès aux consoles Powershell et Invité de commande

Pour bloquer l'accès à la console Powershell :

Configuration utilisateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de restriction logicielle puis sur « Nouvelles stratégies »





Cette fois, pour bloquer l'accès à l'invite de commandes, il suffit de désactiver l'application :

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

Paramètre	État
Accès au stockage amovible	Non configuré
Affichage	Non configuré
Gestion de l'alimentation	Non configuré
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'ouverture de se...	Non configuré
Interface utilisateur personnalisée	Non configuré
Désactiver l'accès à l'invite de commandes	Non configuré
Empêche l'accès aux outils de modifications du Registre	Non configuré
Ne pas exécuter les applications Windows spécifiées	Non configuré
Exécuter uniquement les applications Windows spécifiées	Non configuré
Mises à jour automatiques Windows	Non configuré

Il ne vous reste plus qu'à l'activer.

