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



SOMMAIRE

1) SYNTHÈSE DU PROJET

- 1.1) *Attribution des rôles et responsabilités*
- 1.2) *Rappel des objectifs définis*

2) MISE EN ŒUVRE DU PROJET

- 2.1) *Schéma d'architecture réseau*
- 2.2) *Plan d'adressage*

3) DOCUMENTATION TECHNIQUE

- 3.1) *Guide d'installation*
 - 3.1.1) *Mise en place et paramétrage du pare-feu : pfSense*
 - 3.1.2) *Mise en place d'un VPN site-à-site sécurisé : IPsec*
 - 3.1.3) *Paramétrage des serveurs Windows*
 - 3.1.4) *Déploiement d'Active Directory*
 - 3.1.5) *Installation du cluster Active Directory*
 - 3.1.6) *Installation du service DHCP*
 - 3.1.7) *Installation du service DFS*
 - 3.1.8) *Installation de la solution de sauvegarde*
- 3.2) *Guide d'exploitation*
 - 3.2.1) *Paramétrage de l'environnement Active Directory*
 - 3.2.2) *Mise en place du pool DHCP et de son basculement*
 - 3.2.3) *Configuration du partage DFS et de la réplication DFSR*
 - 3.2.4) *Déploiement des stratégies de groupe (GPO)*
 - 3.2.5) *Configuration de la sauvegarde sur TrueNAS*
 - 3.2.6) *Mise en place des clichés instantanés : Shadow Copy*
 - 3.2.7) *Déploiement du portail captif : AD RADIUS et pfSense*

1) SYNTHÈSE DU PROJET

1.1) Attribution des rôles et responsabilités

Dans le cadre de ce projet, je suis le seul intervenant et assume l'ensemble des rôles techniques et organisationnels.

Mes responsabilités couvrent les domaines suivants :

- *Préparation, installation et configuration des serveurs (Windows et pare-feu pfSense)*
- *Mise en place des GPO et intégration des clients dans l'Active Directory*
- *Création et gestion des utilisateurs et des droits*
- *Configuration du VPN inter-sites (IPSec)*
- *Mise en place du serveur de fichiers avec redondance et sauvegardes (SAN + Shadow Copy)*
- *Gestion du portail captif pour l'accès WAN*
- *Suivi global du projet, gestion des ressources et respect des délais*

1.2) Rappel des objectifs définis

Ce projet a pour objectif de concevoir et mettre en œuvre une infrastructure informatique hautement disponible, sécurisée et interconnectée entre les deux sites d'IFIDE, à Strasbourg et Mulhouse. L'ensemble de la réalisation est pris en charge par une seule personne, de l'élaboration du cahier des charges à la configuration des différents services.

La priorité est donnée à la fiabilité, à la sécurité des échanges, à la continuité des services, ainsi qu'à la centralisation de la gestion du système d'information.

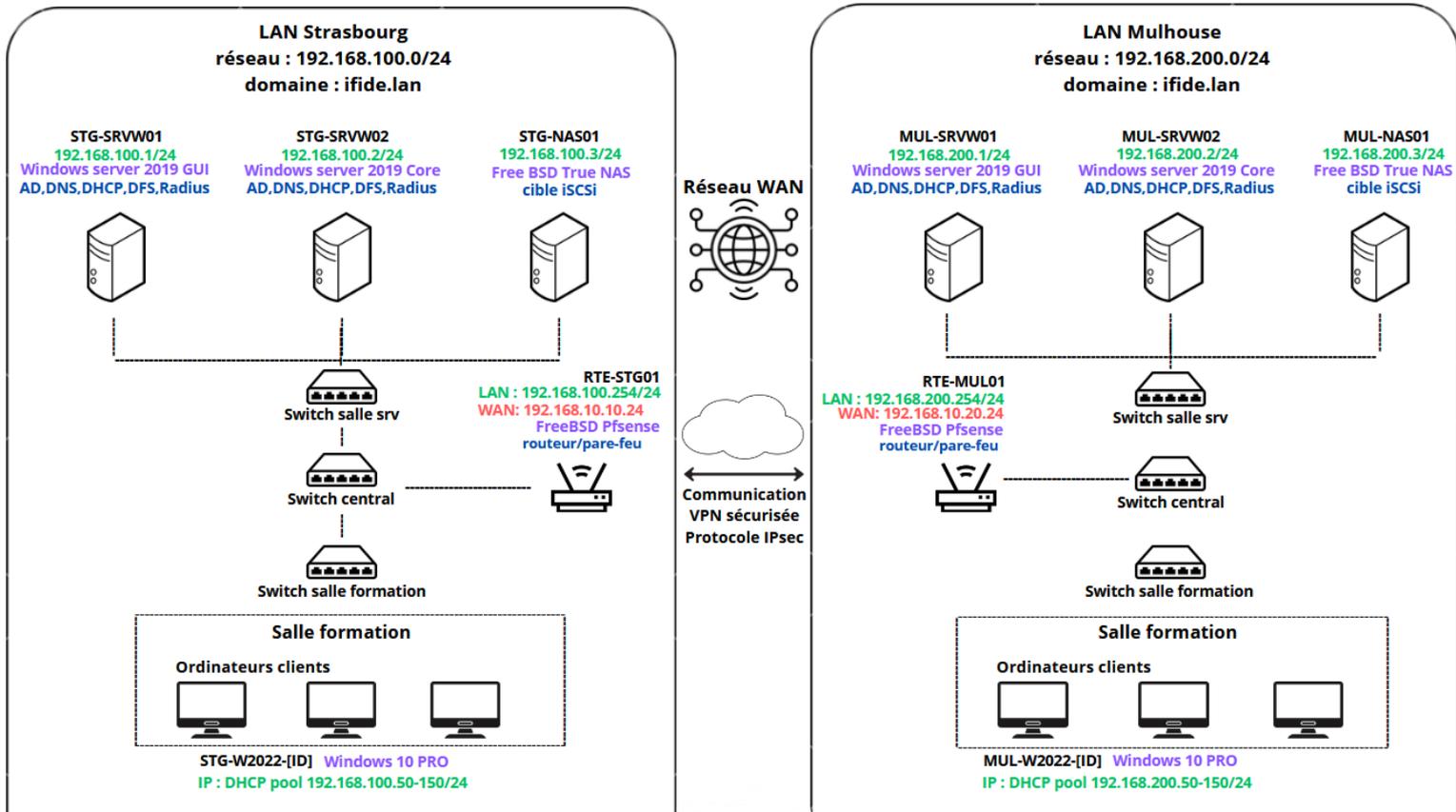
Les objectifs principaux sont les suivants :

- *Création d'un système d'information centralisé et unifié entre les deux sites, facilitant la gestion des utilisateurs, des ressources, et des politiques de sécurité via Active Directory ;*
- *Mise en œuvre d'un VPN chiffré (IPSec) pour interconnecter de façon sécurisée les deux sites et permettre un échange fluide des données ;*
- *Déploiement de serveurs Windows avec services en redondance : contrôleurs de domaine, DHCP, partage de fichiers, avec configuration des GPO pour uniformiser les postes clients ;*
- *Installation d'un portail captif sécurisé, avec authentification unique (SSO) via les identifiants Active Directory, pour contrôler l'accès des utilisateurs au réseau WAN ;*
- *Mise en place d'un plan d'adressage et de nommage homogène, assurant la cohérence de l'infrastructure sur les deux sites ;*
- *Gestion des droits d'accès et de la sécurité des données, en fonction des profils (administratifs, enseignants, élèves), avec une attention portée à la conformité légale et à la confidentialité des données ;*
- *Mise en œuvre de solutions de sauvegarde et de redondance (Shadow Copy, réplication, espace SAN iSCSI), afin d'assurer la continuité des services en cas de panne matérielle ou logicielle ;*
- *Amélioration du service utilisateur grâce à une administration plus simple et à un accès fluide aux ressources, quel que soit le site.*

La planification du projet, incluant le tableau d'adressage, la hiérarchisation des tâches et les délais de mise en œuvre, a été établie de manière réaliste afin d'anticiper les éventuels aléas techniques. L'objectif est d'obtenir une infrastructure fiable, scalable et maintenable dans le temps, tout en optimisant les coûts de possession et d'exploitation.

2. MISE EN ŒUVRE DU PROJET

2.1) Schéma d'architecture réseau



2.2) Plan d'adressage

SITE	NOM	ADRESSE IP	MASQUE	PASSERELLE	DNS
STRASBOURG					
STRASBOURG	RTE-STG01	LAN : 192.168.100.254 WAN : 192.168.10.10	255.255.255.0	WAN : 192.168.10.254	192.168.100.1 192.168.100.2
STRASBOURG	STG-SRVW01	192.168.100.1	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
STRASBOURG	STG-SRVW02	192.168.100.2	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
STRASBOURG	STG-NAS01	192.168.100.3	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
STRASBOURG	STG-W2022xx	DHCP	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
MULHOUSE					
MULHOUSE	RTE-MUL01	LAN : 192.168.200.254 WAN : 192.168.10.20	255.255.255.0	WAN : 192.168.10.254	192.168.200.1 192.168.200.2
MULHOUSE	MUL-SRVW01	192.168.200.1	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
MULHOUSE	MUL-SRVW02	192.168.200.2	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
MULHOUSE	MUL-NAS01	192.168.200.3	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
MULHOUSE	MUL-W2022xx	DHCP	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2

3. DOCUMENTATION TECHNIQUE

Ce document présente la mise en place de l'infrastructure interconnectée entre les sites de Strasbourg et Mulhouse, ainsi que les procédures d'installation, d'exploitation et de maintenance du système et du réseau.

Plan de nommage

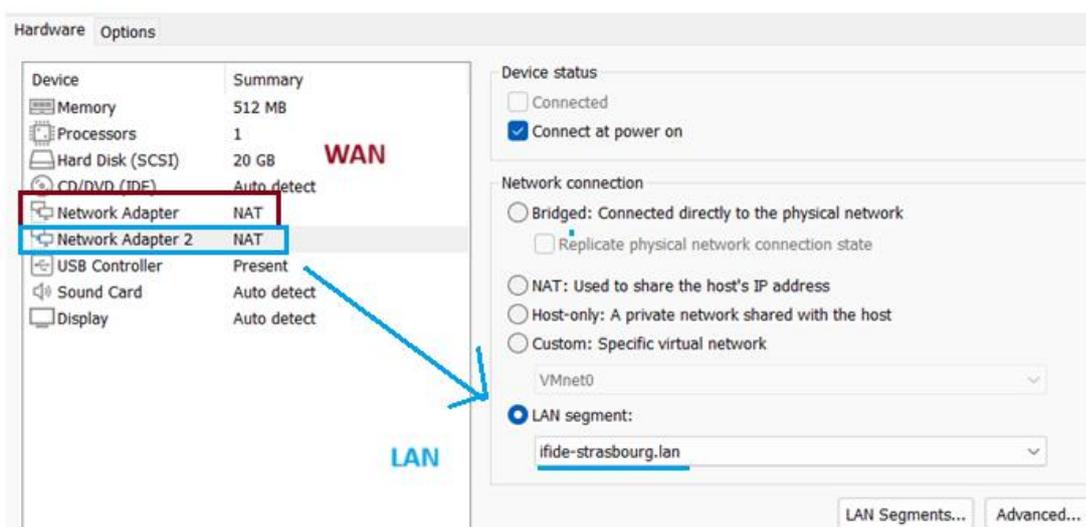
📍 : Strasbourg et Mulhouse Entreprise : IFIDE sup-formation

Ressources	Nom Machine
Serveurs Active Directory	STG-SRVWxx / MUL-SRVWxx
Serveurs de Stockage	STG-NASxx / MUL-NASxx
Routeurs	RTE-STGxx / RTE-MULxx
Ordinateurs Clients	STG-W2022xx / MUL-W2022xx

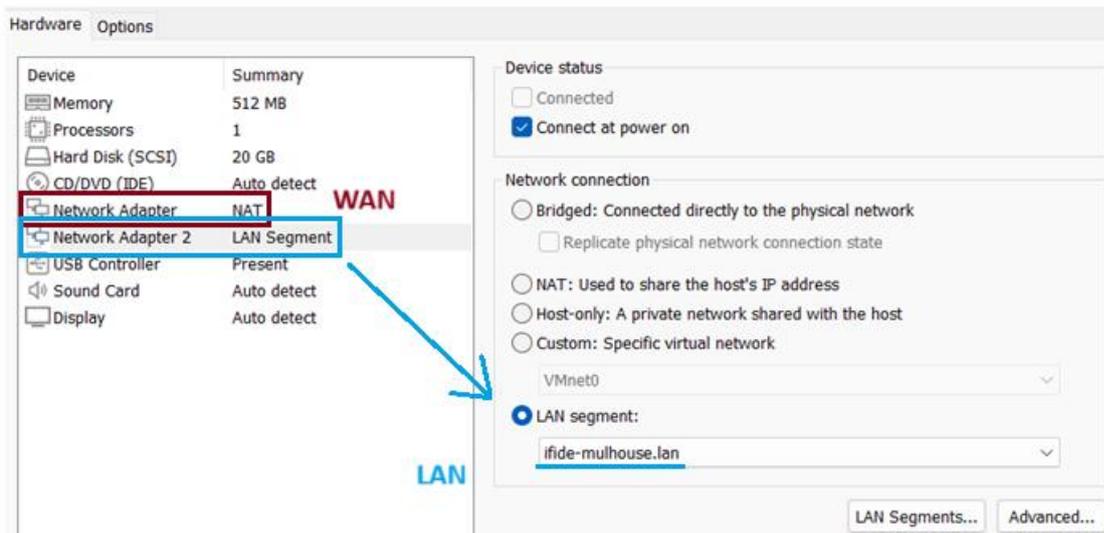
STG désigne les ressources situées à Strasbourg, tandis que MUL identifie celles de Mulhouse.

Prérequis de création des machines virtuelles :

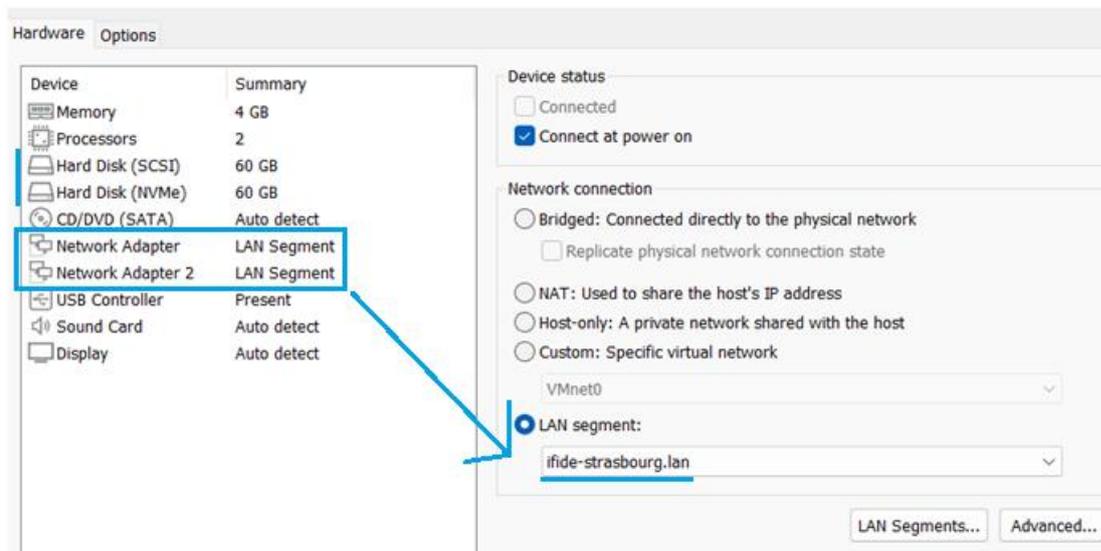
- Routeur/Pare-feu du site de Strasbourg (pfSense FreeBSD)



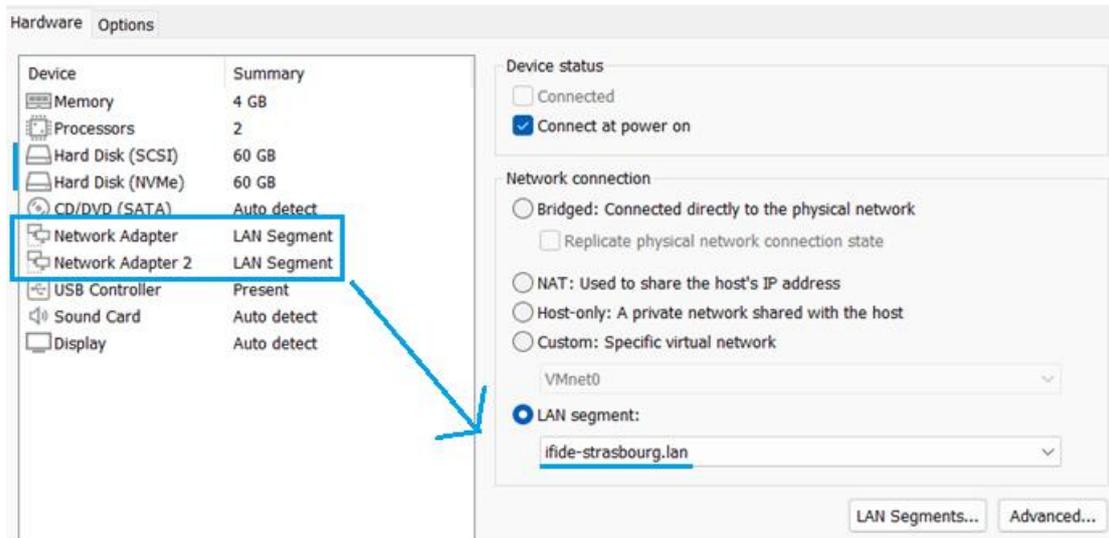
- Routeur/Pare-feu du site de Mulhouse (pfSense FreeBSD)



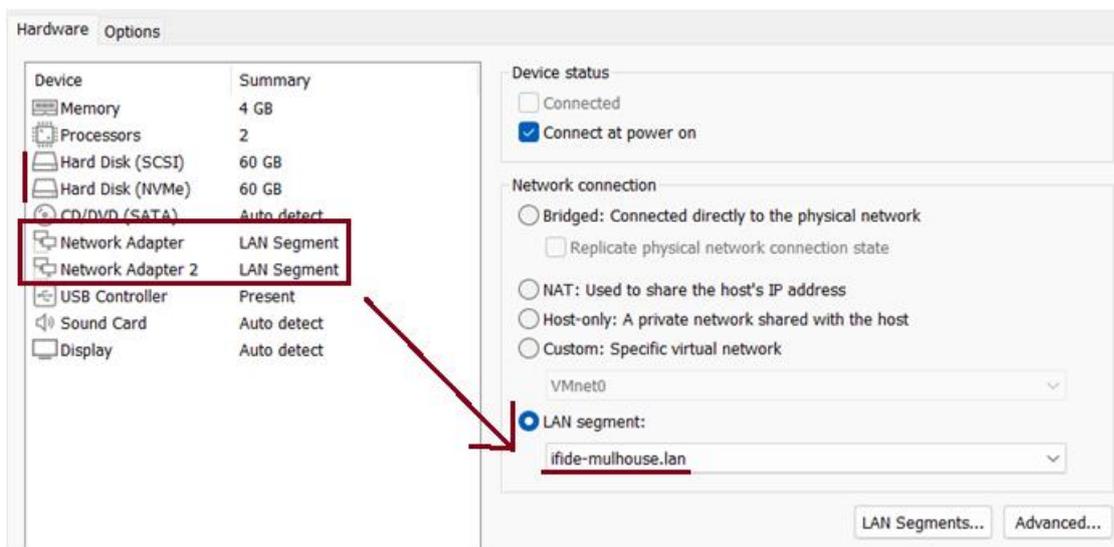
- Serveur principal pour le site de Strasbourg (Windows Server 2019 GUI)



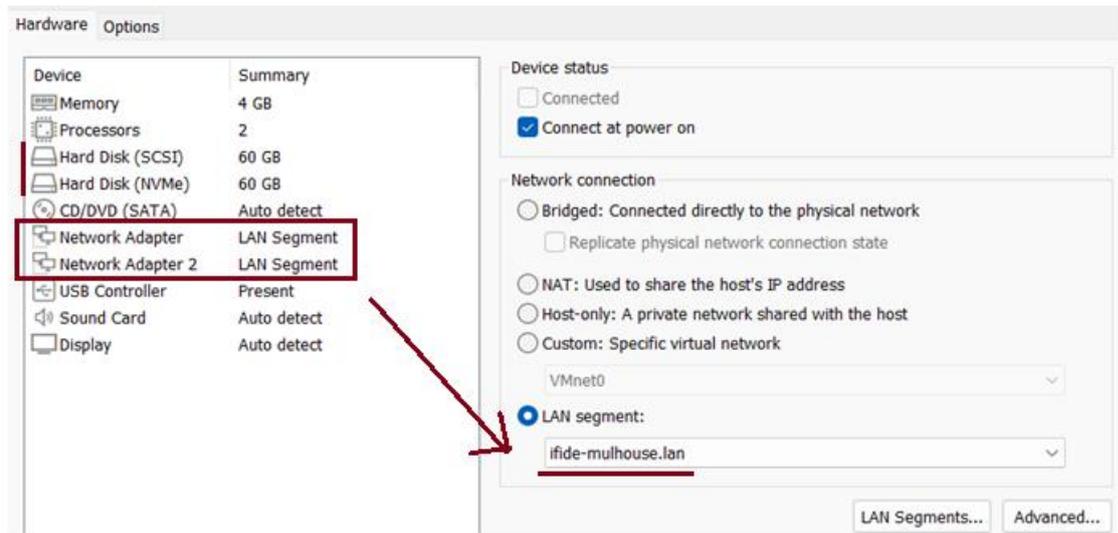
- Serveur secondaire pour le site de Strasbourg (Windows Server 2019 Core)



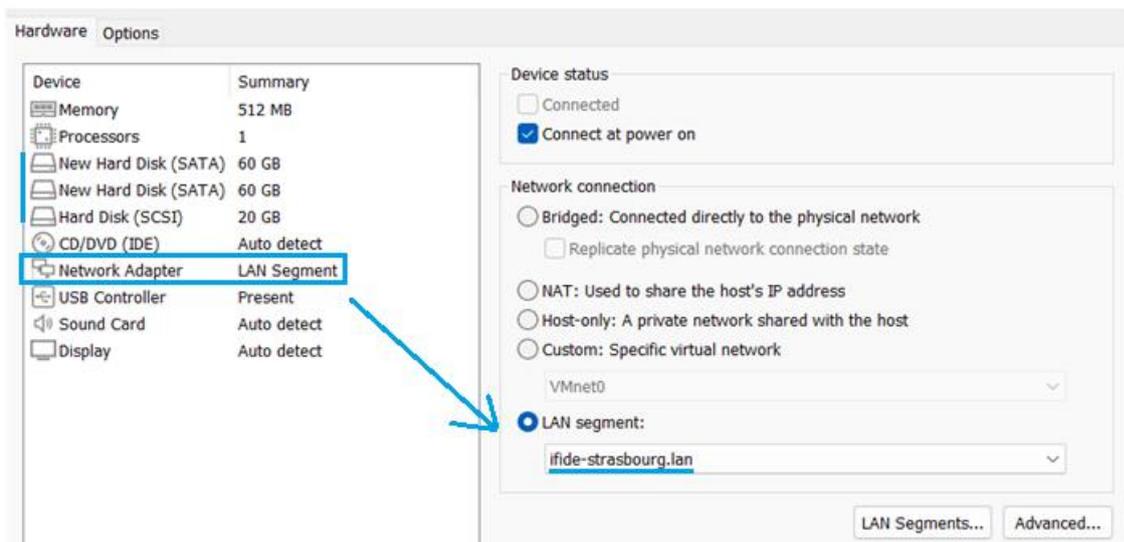
- Serveur principal pour le site de Mulhouse (Windows Server 2019 GUI)



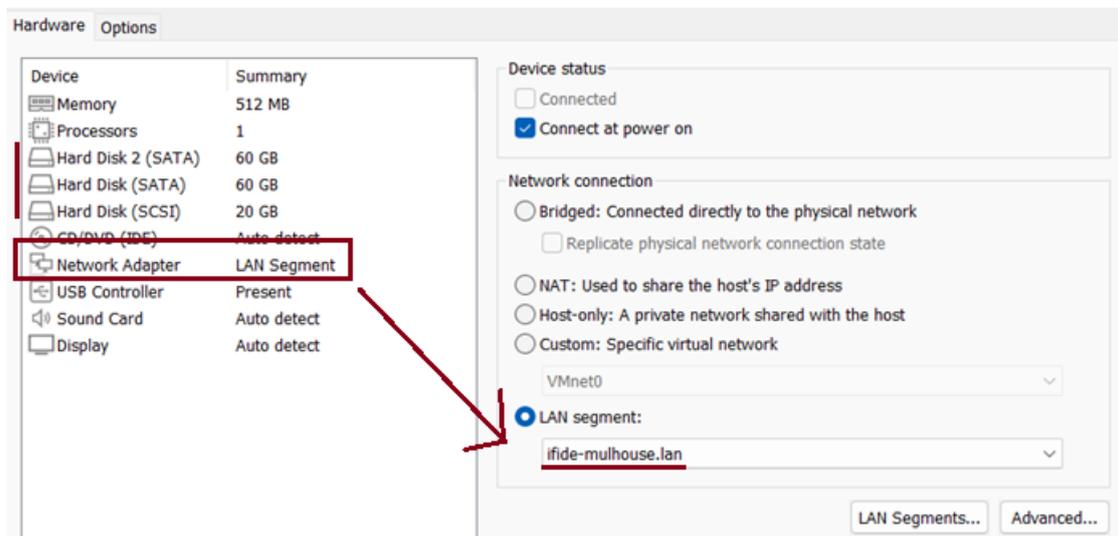
- Serveur secondaire pour le site de Mulhouse (Windows Server 2019 Core)



- Serveur NAS pour le site de Strasbourg (TrueNAS FreeBSD)



- Serveur NAS pour le site de Mulhouse (True NAS FreeBSD)



- ☐ RTE-STG01
- ☐ RTE-MUL01
- ☐ STG-SRVW01
- ☐ STG-SRVW02
- ☐ MUL-SRVW01
- ☐ MUL-SRVW02
- ☐ STG-NAS01
- ☐ MUL-NAS01

Vos machines virtuelles sont désormais prêtes et correctement nommées selon leur rôle (routeurs, serveurs GUI/Core, NAS).



N'oubliez pas d'insérer les bonnes images ISO avant de démarrer vos VM.

3.1) *Guide d'installation*

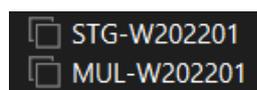
Cette documentation d'installation présente l'ensemble des prérequis nécessaires pour le déploiement de chaque machine virtuelle, ainsi que le détail des étapes à suivre pour l'installation des systèmes et la configuration des services.

3.1.1) *Mise en place et paramétrage du pare-feu : pfSense*

Pour procéder à l'installation de pfSense, la machine virtuelle doit être configurée selon les paramètres définis précédemment. **Une machine cliente, ici configurée sous Windows Server 2022, sera utilisée pour accéder à l'interface web du routeur pfSense.**

Vous pouvez la nommer selon la convention définie précédemment, par exemple :

STG-W2022xx ou MUL-W2022xx, en fonction du site.



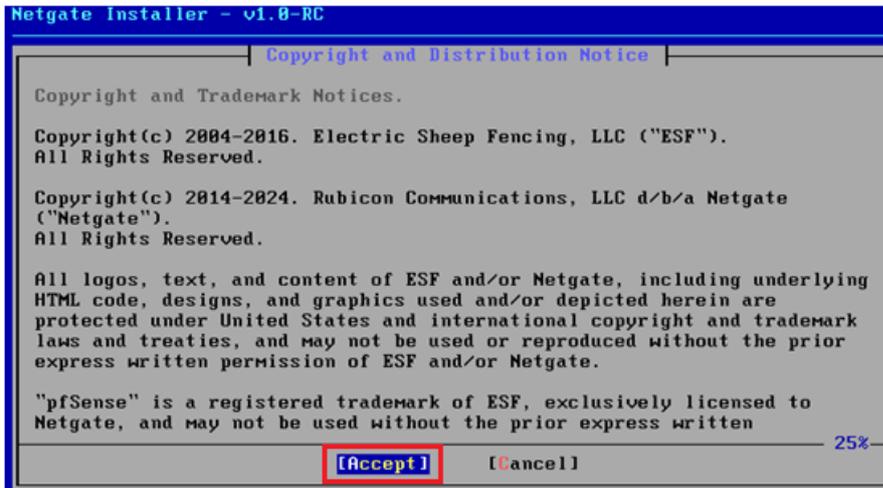
Celle-ci devra être connectée au même réseau LAN que le pare-feu correspondant : 192.168.100.0/24 pour le site de Strasbourg et 192.168.200.0/24 pour le site de Mulhouse.

Installation du système FreeBSD pour pfSense

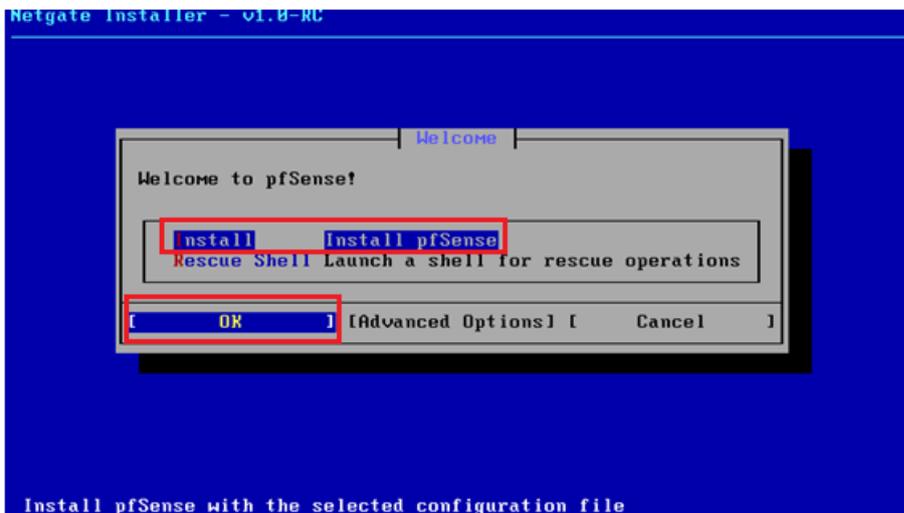
Démarrez la machine virtuelle RTE-STG01 pour lancer l'installation de pfSense sur le site de Strasbourg.



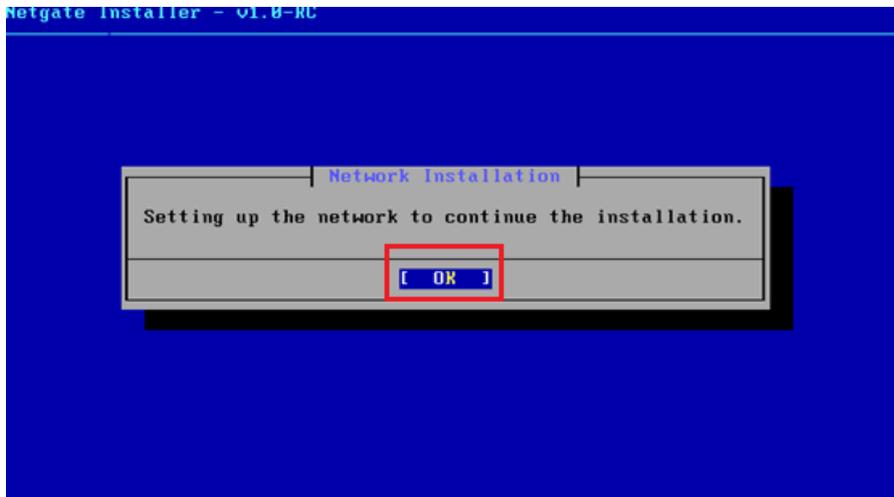
À l'écran des conditions d'utilisation, appuyez sur la touche [ENTRÉE] pour accepter et poursuivre l'installation.



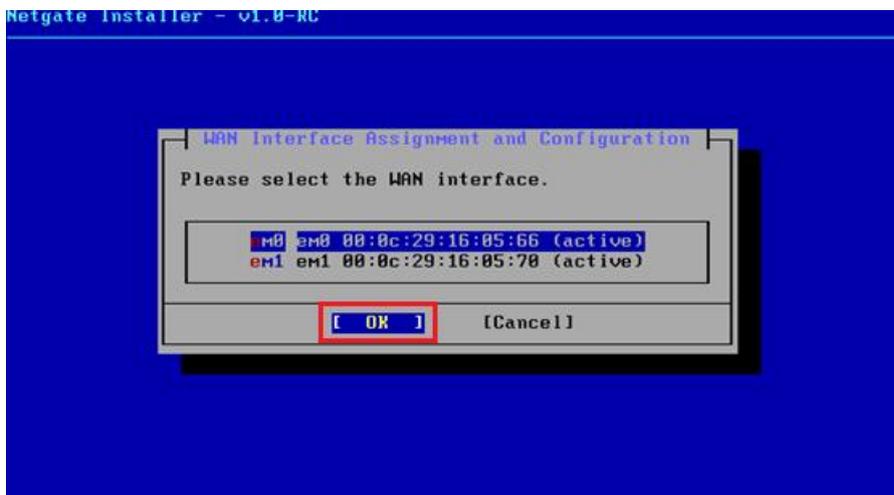
Sélectionnez « Install » à l'aide des flèches directionnelles, puis appuyez sur la touche [ENTRÉE].



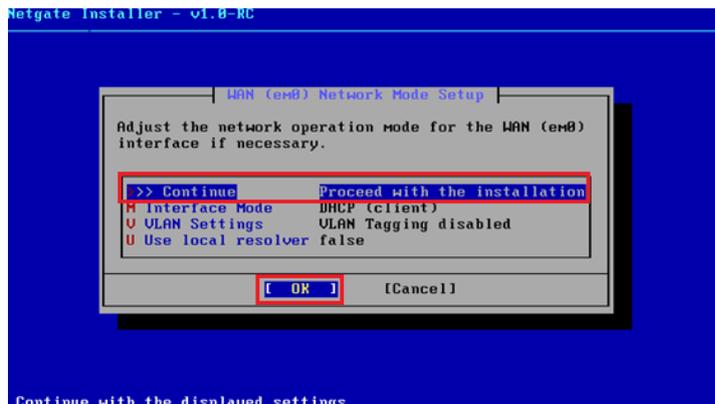
À cette étape, appuyer sur la touche [ENTRÉE] pour permettre à pfSense de configurer automatiquement la connexion réseau et accéder à Internet afin de poursuivre l'installation.



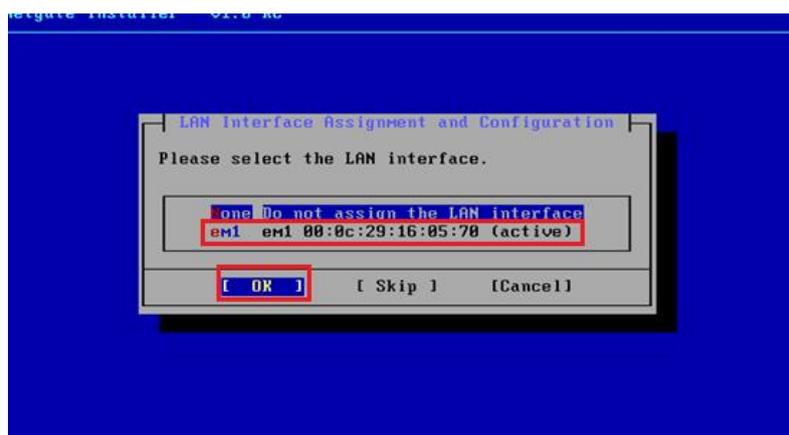
Sélectionnez l'interface em0, pour configurer le WAN puis appuyez sur [ENTRÉE].



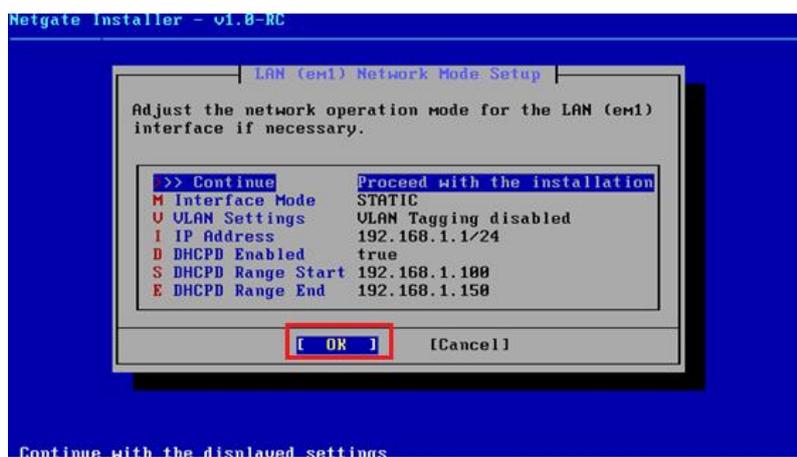
Sélectionnez « Continue » pour poursuivre l'installation et appuyez sur [ENTRÉE].



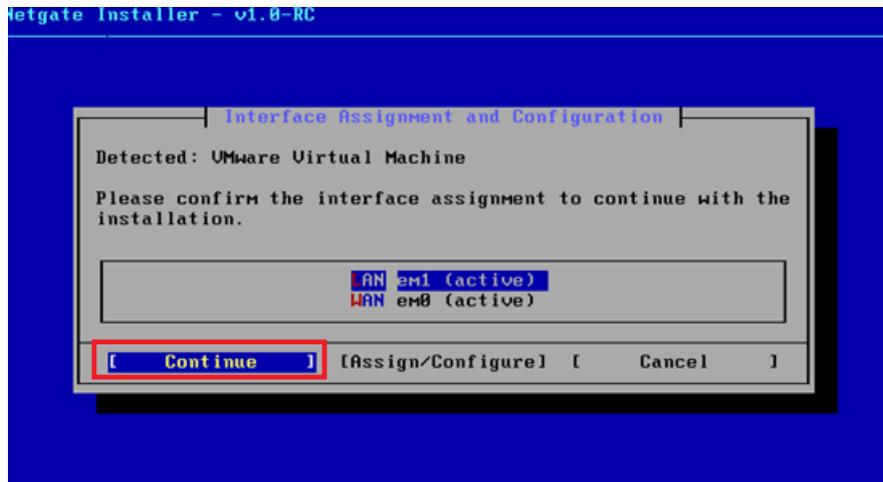
Sélectionnez em1 comme interface LAN, puis validez avec [ENTRÉE].



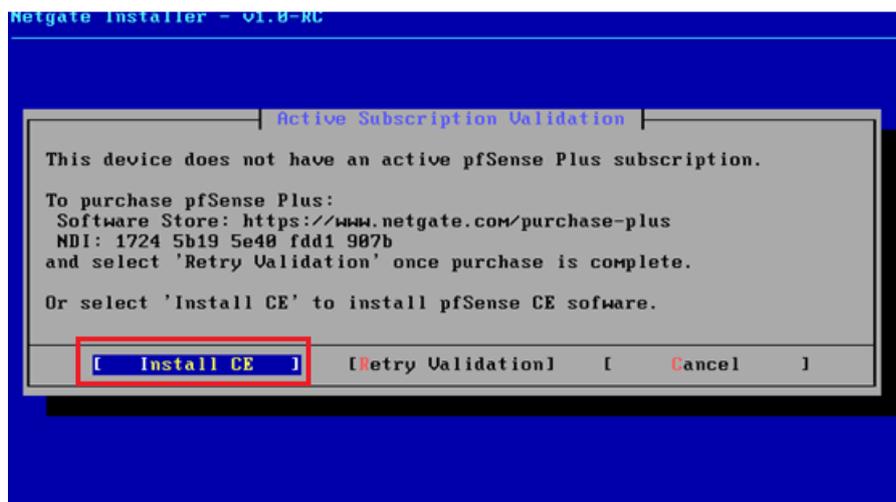
Laissez les paramètres proposés par défaut puis validez avec [ENTRÉE] pour continuer l'installation.



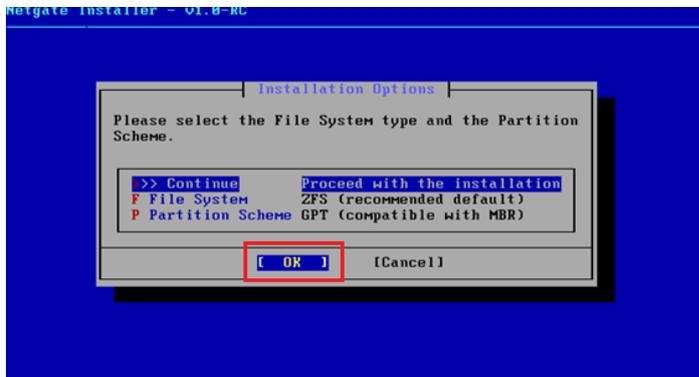
Confirmez l'assignation des interfaces en appuyant sur [ENTRÉE] pour continuer.



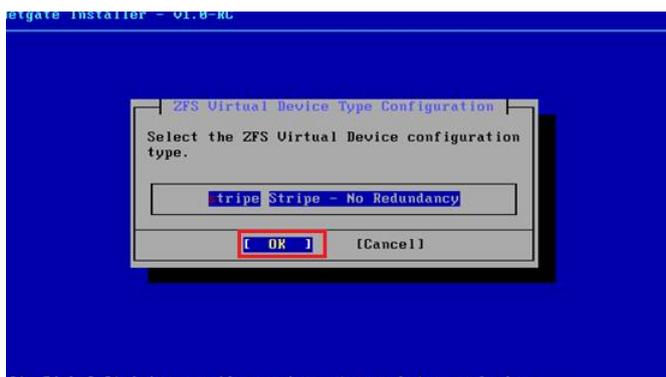
Sélectionnez "Install CE" pour lancer l'installation de la version gratuite de pfSense.



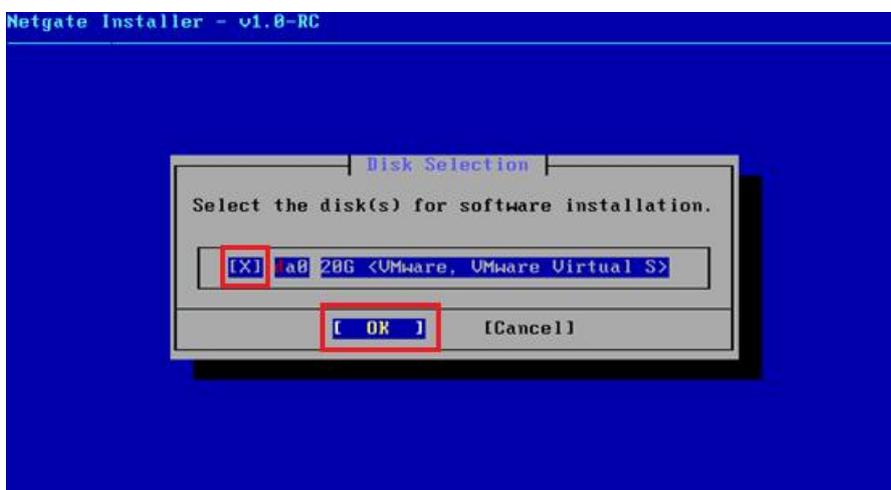
Appuie sur [ENTRÉE] pour continuer l'installation avec ces paramètres recommandés.



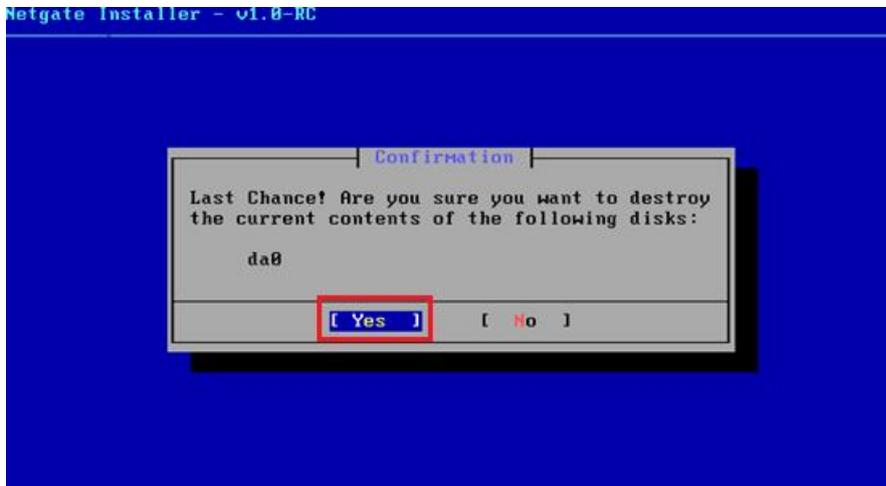
Sélectionnez Stripe – No Redundancy puis validez en appuyant sur [ENTRÉE].



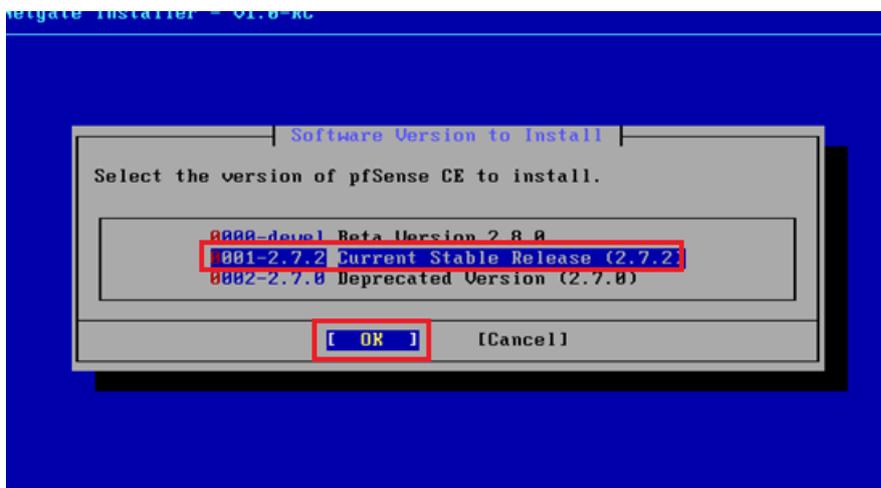
Sélectionnez le disque proposé avec la barre d'espace pour l'installation (ici, le disque de 20 Go), puis appuyez sur [ENTRÉE].



Appuyez simplement sur la touche [ENTRÉE] pour valider l'étape et poursuivre l'installation.

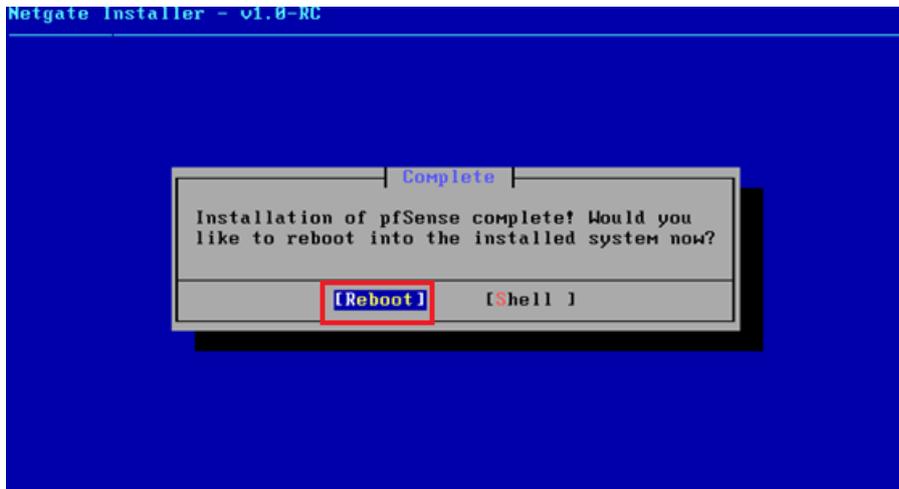


Sélectionnez la version 2.7.2 Current Stable Release, puis appuyez sur [ENTRER] pour continuer l'installation.



Puis patientez...

Après l'apparition du message confirmant la fin de l'installation, cliquez sur **[Reboot]** pour redémarrer le système.



Votre installation est prête.

À présent, nous allons procéder à la configuration réseau de pfSense afin de permettre l'accès à son interface web, indispensable pour les prochaines opérations.

Configuration réseau pfSense

Interface LAN

Commencez par configurer l'interface LAN en appuyant sur la touche **2**, puis validez avec **[ENTRÉE]**.



Sélectionnez ensuite « 2 » pour la carte LAN puis [ENTRÉE].

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
```

Écrivez "n" lorsque l'on vous demande si vous souhaitez configurer l'adresse IPv4 via DHCP, puis renseignez l'adresse IP **192.168.100.254** pour le site de Strasbourg et validez avec [ENTRÉE].

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254
```

Indiquez **24** comme masque de sous-réseau (ce qui correspond à 255.255.255.0), puis appuyez sur [ENTRÉE].

```
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
```

Le configurateur vous demandera ensuite de renseigner une passerelle par défaut pour le réseau WAN. Comme nous configurons ici le réseau LAN, appuyez simplement sur [ENTRÉE] pour laisser vide (none).

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

Comme l'IPv6 ne sera pas utilisé, appuyez sur [ENTRÉE] pour laisser vide (none).

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

Nous n'activerons pas de serveur DHCP sur l'interface LAN, car ce rôle sera assuré par les serveurs Windows Server configurés ultérieurement.

```
Do you want to enable the DHCP server on LAN? (y/n) n
```

Si vous souhaitez conserver le protocole HTTPS pour l'accès à l'interface web, tapez "n" puis appuyez sur [ENTRÉE].

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

Comme l'indique le message de fin de configuration, pour accéder à l'interface web de pfSense, saisissez l'adresse IP LAN suivante dans la barre d'adresse de votre navigateur : <https://192.168.100.254/>.

```
The IPv4 LAN address has been set to 192.168.100.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.100.254/
Press <ENTER> to continue.
```

Interface WAN

La configuration statique de l'interface WAN n'est pas obligatoire, mais elle permet d'assurer une stabilité nécessaire pour la mise en place du VPN par la suite. Pour cela, suivez les étapes suivantes :

Pour commencer la configuration statique de l'interface WAN, tapez sur la touche 2 puis appuyez sur [ENTRÉE].

Ensuite, entrez le numéro de l'interface WAN, ici 1, puis tapez n pour refuser la configuration par DHCP.

Indiquez ensuite l'adresse IP statique souhaitée, ici 192.168.10.10, puis validez avec [ENTRÉE].

L'adresse IP configuré est 192.168.10.10 pour correspondre au tableau d'adressage.

```
LAN (lan)      -> em1      -> v4: 192.168.100.254/24

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

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: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.10.10
```



Attention : Pour l'interface WAN, il est essentiel de définir une passerelle par défaut. Contrairement à l'interface LAN, celle-ci permet à pfSense — et donc à tout le réseau local derrière — d'accéder à Internet. Sans passerelle, aucune connexion extérieure ne sera possible.

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

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.10.254 IMPORTANT
```

Validez la passerelle par défaut avec y, puis refusez l'IPv6 avec n et appuyez sur [ENTRÉE].

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

Configuration réseau finale pour Strasbourg :

```
The IPv4 WAN address has been set to 192.168.10.10/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 17245b195e40fdd1907b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4: 192.168.10.10/24
LAN (lan)      -> em1          -> v4: 192.168.100.254/24

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

Enter an option: █
```

À présent, l'interface WAN va être configurée en statique. Les mêmes étapes devront être réalisées sur le routeur/pare-feu de Mulhouse, en adaptant les paramètres et l'adressage IP en fonction du site.

Configuration réseau finale pour Mulhouse :

```
The IPv4 WAN address has been set to 192.168.10.20/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 926f2889e89c62c06661

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4: 192.168.10.20/24
LAN (lan)      -> em1          -> v4: 192.168.200.254/24

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

Enter an option: █
```

Il est désormais temps d'accéder à l'interface web de pfSense afin d'effectuer les dernières configurations, notamment la mise en place du VPN et la définition des règles de pare-feu.

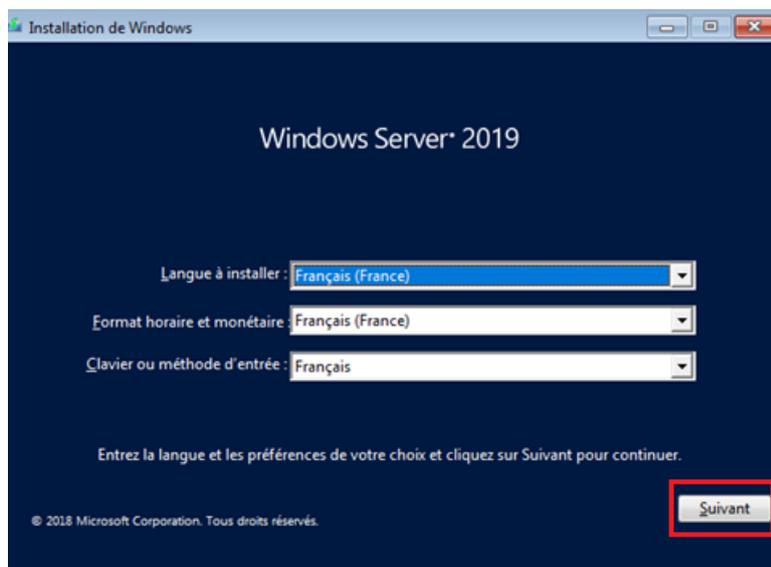
Accès à l'interface web de pfSense

Pour ce faire, nous allons utiliser notre serveur principal de Strasbourg, **STG-SRVW01**, configuré avec une adresse IP dans le même réseau que pfSense.

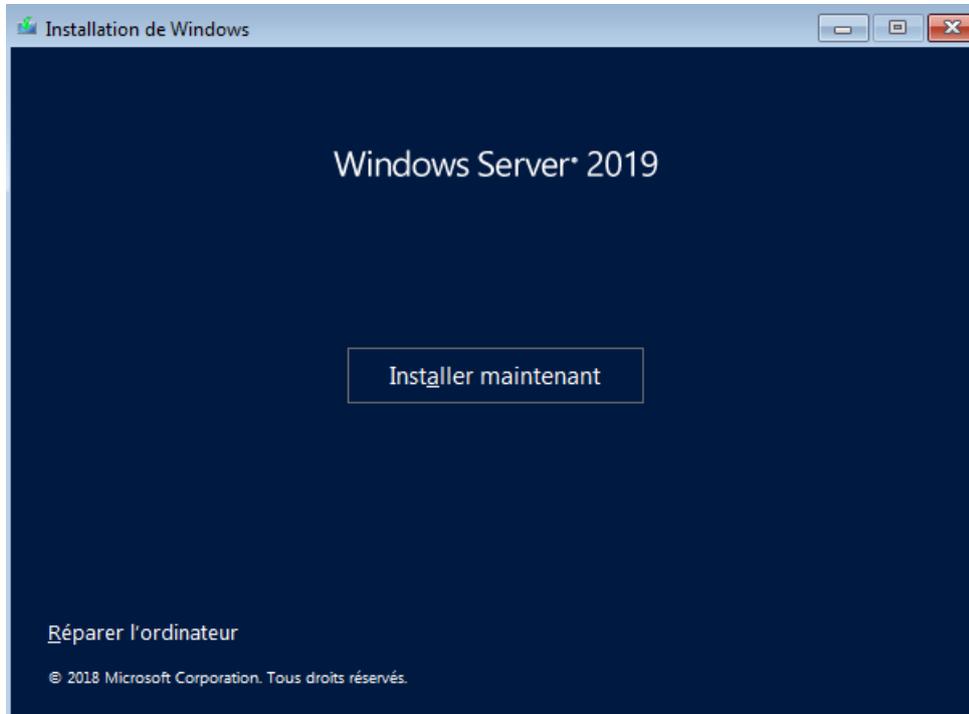
En l'occurrence, et d'après le tableau d'adressage, nous allons lui attribuer l'adresse **192.168.100.1** avec le masque **255.255.255.0** et la passerelle **192.168.100.254**.

Une fois la configuration réseau appliquée, ouvrez un navigateur web et saisissez l'adresse suivante : <https://192.168.100.254> pour accéder à l'interface de gestion pfSense.

Dans un premier temps, choisissez les paramètres de langue, de format horaire et de clavier selon vos préférences, puis cliquez sur **Suivant** pour lancer l'installation de Windows Server 2019.

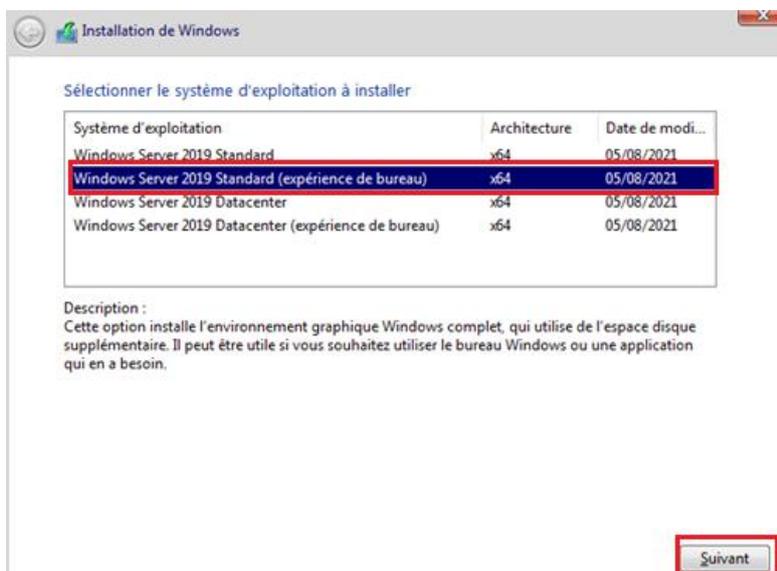


Cliquez sur **Installer maintenant** pour lancer l'installation de Windows Server 2019.



Patiencez...

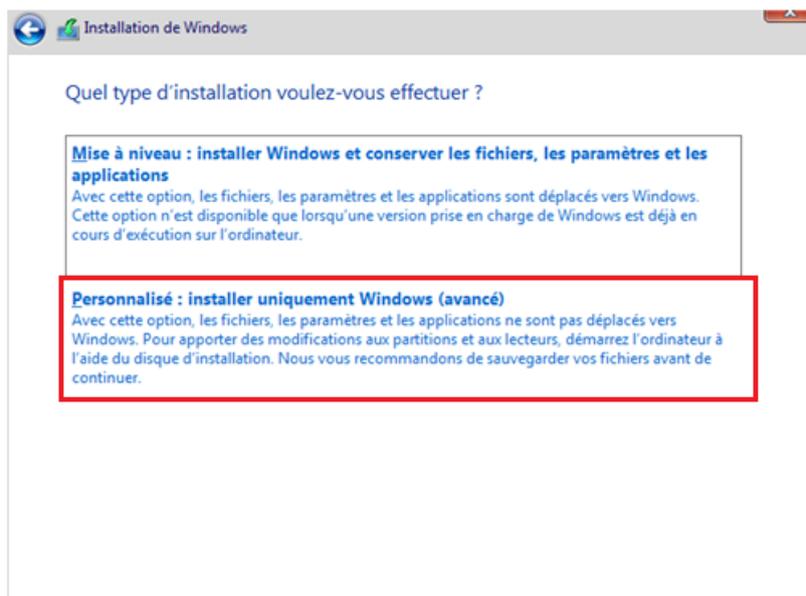
Sélectionnez **Windows Server 2019 Standard (expérience de bureau)**, puis cliquez sur **Suivant** pour bénéficier de l'interface graphique complète.



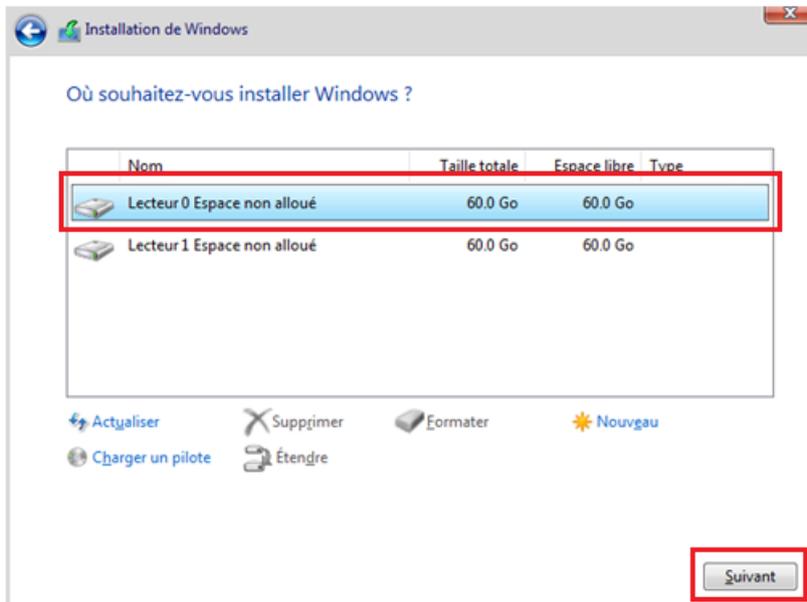
Cochez "J'accepte les termes du contrat de licence", puis cliquez sur **Suivant** pour continuer l'installation.



Sélectionnez "**Personnalisé : installer uniquement Windows (avancé)**", afin de procéder à une installation propre du système d'exploitation.

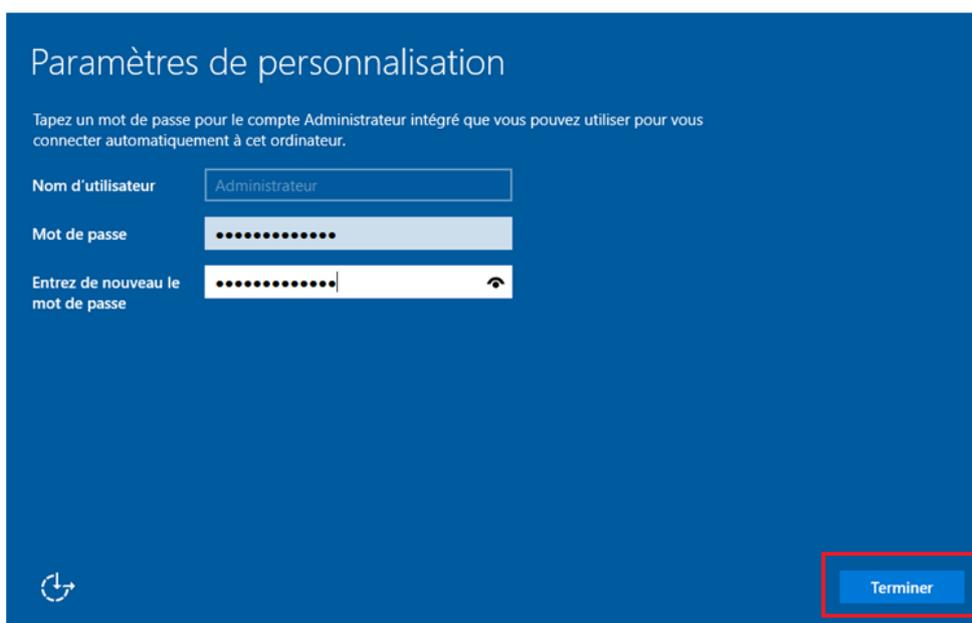


Choisissez un des lecteurs avec l'espace non alloué (par exemple *Lecteur 0*), puis cliquez sur **Suivant** pour lancer l'installation de Windows Server 2019.



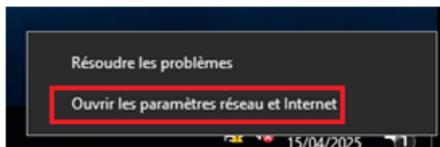
Patientez...

Définissez un mot de passe pour le compte **Administrateur**, confirmez-le dans le champ en dessous, puis cliquez sur **Terminer** pour finaliser la configuration.

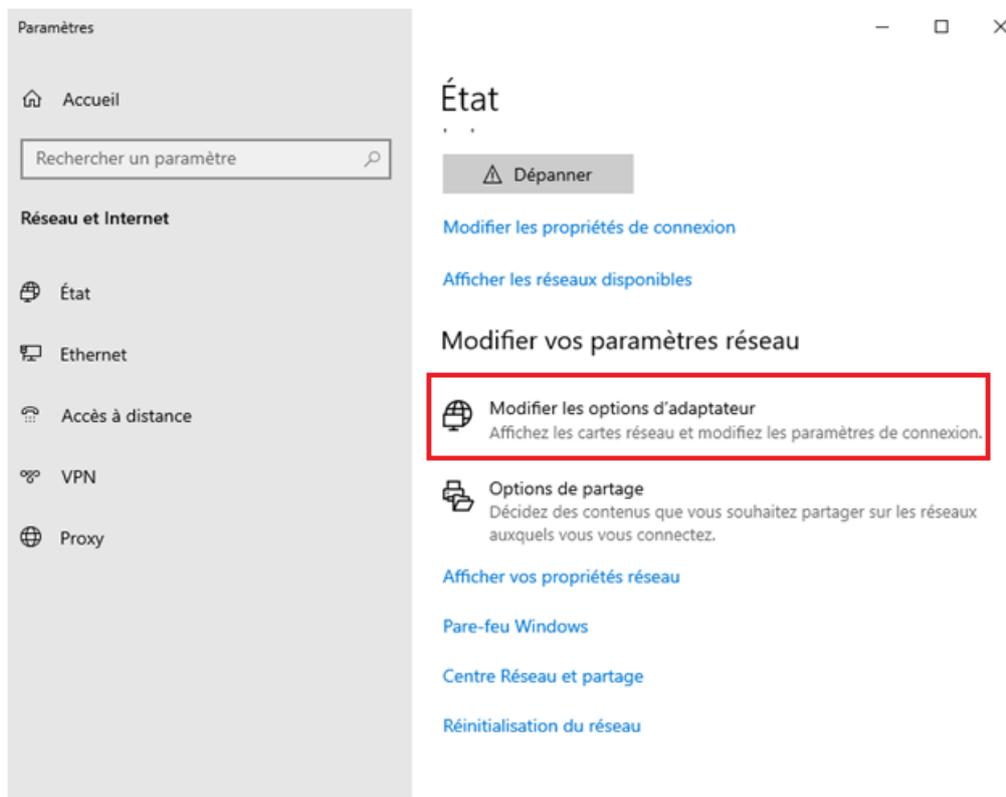


Vous êtes désormais connecté à votre environnement Windows Server. Nous allons maintenant configurer son adresse IP afin qu'il soit correctement intégré au réseau local de Strasbourg, conformément au plan d'adressage.

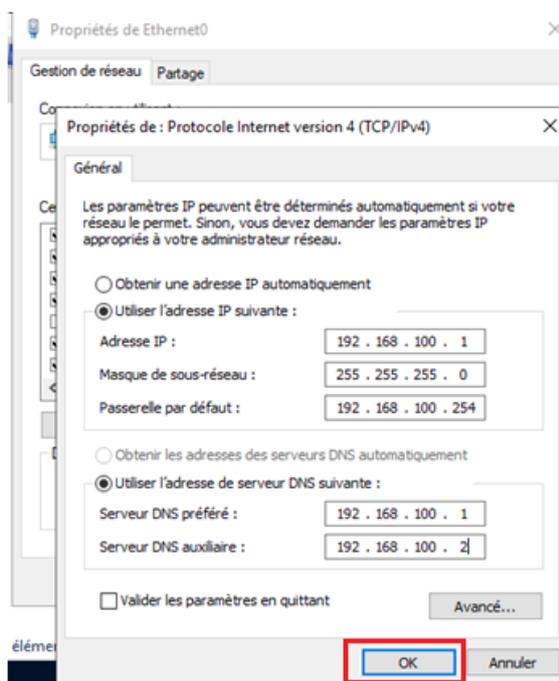
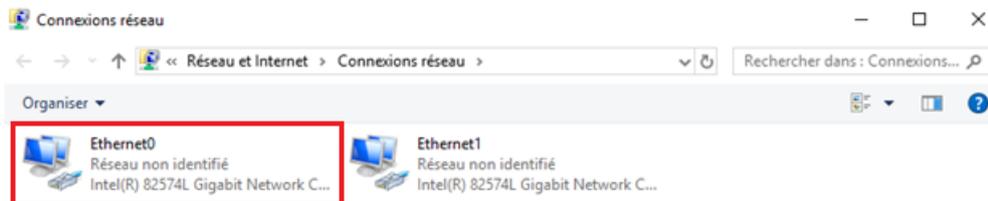
Effectuez un clic droit sur l'icône réseau en bas à droite, puis cliquez sur "**Ouvrir les paramètres réseau et Internet**" afin d'accéder aux options de configuration de l'adresse IP.



Cliquez sur "**Modifier les options d'adaptateur**".

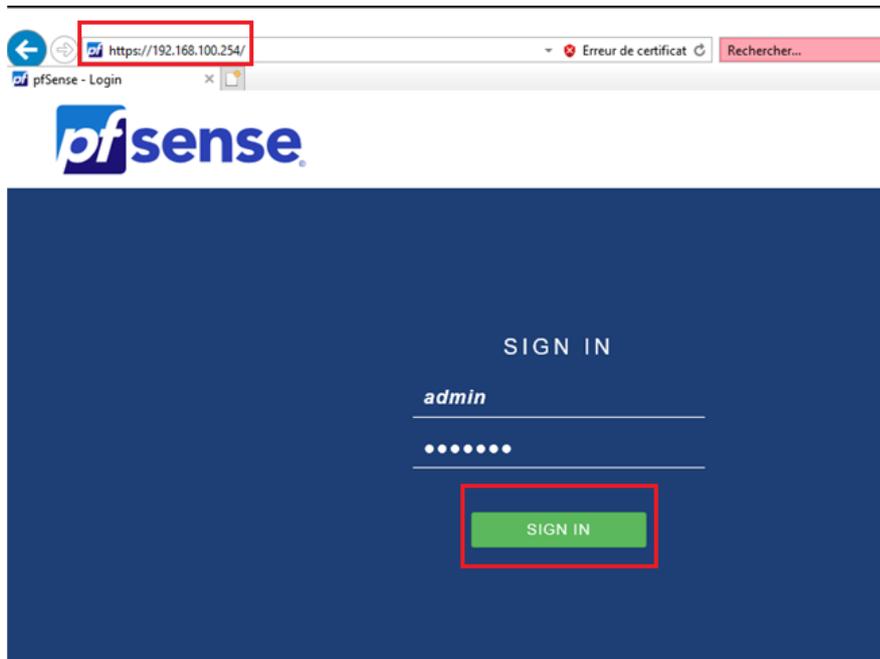


Clic droit sur **Ethernet0** > **Propriétés** > **Protocole IPv4 attribué** > l'IP **192.168.100.1**, masque **255.255.255.0**, passerelle **192.168.100.254**, DNS **192.168.100.1**.

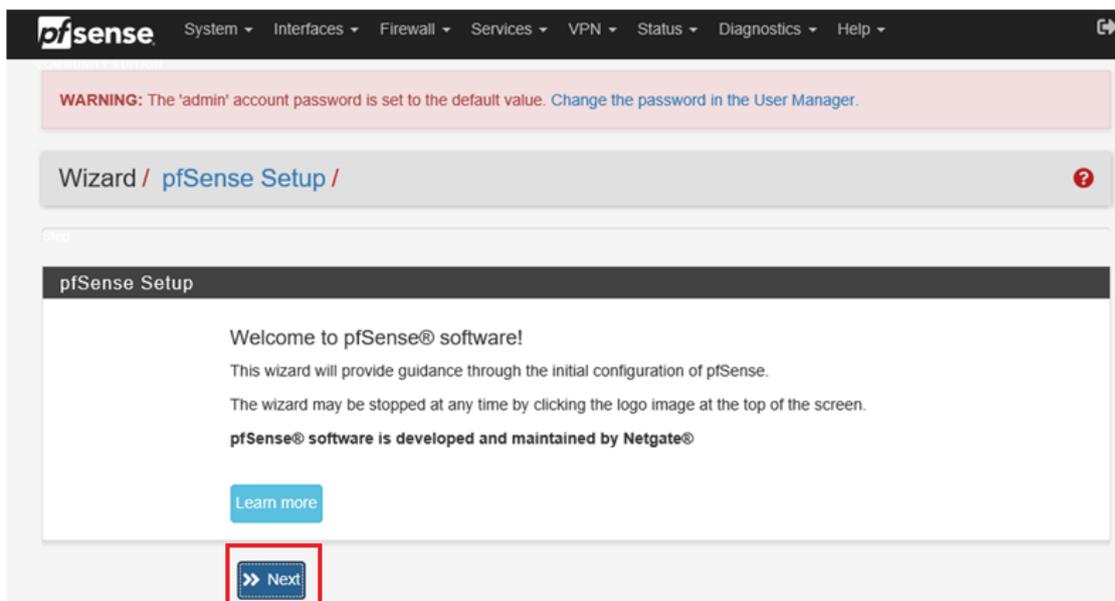


Votre environnement étant désormais sur le même réseau que le pfSense, vous pouvez ouvrir un navigateur et accéder à l'interface web en saisissant : <https://192.168.100.254>.

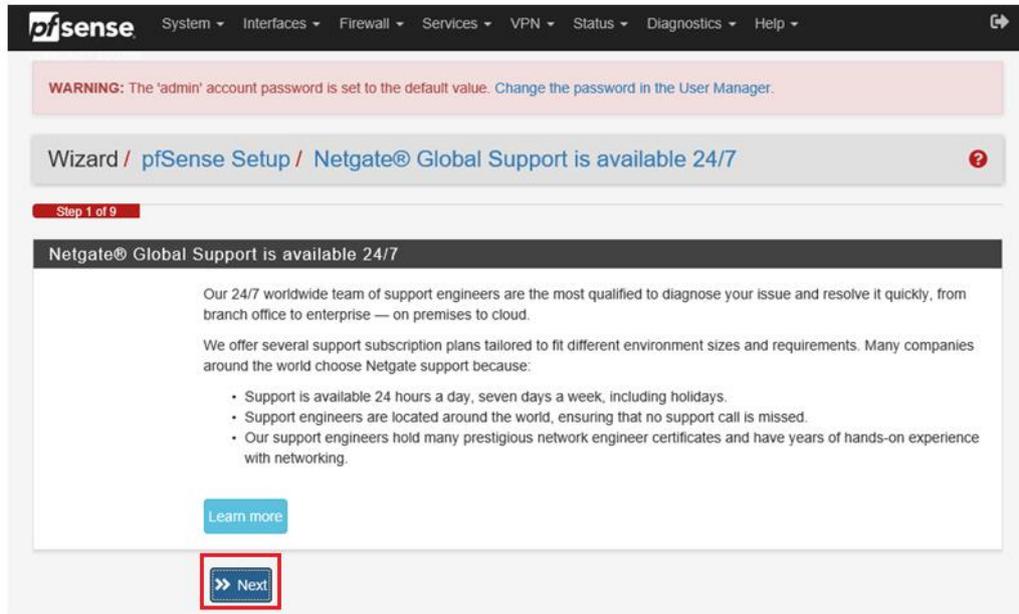
Connectez-vous avec les identifiants par défaut : **admin / pfsense** 



Une fois connecté à l'interface web de pfSense, une configuration initiale du pare-feu vous sera proposée. Cliquez simplement sur "Next" pour poursuivre.

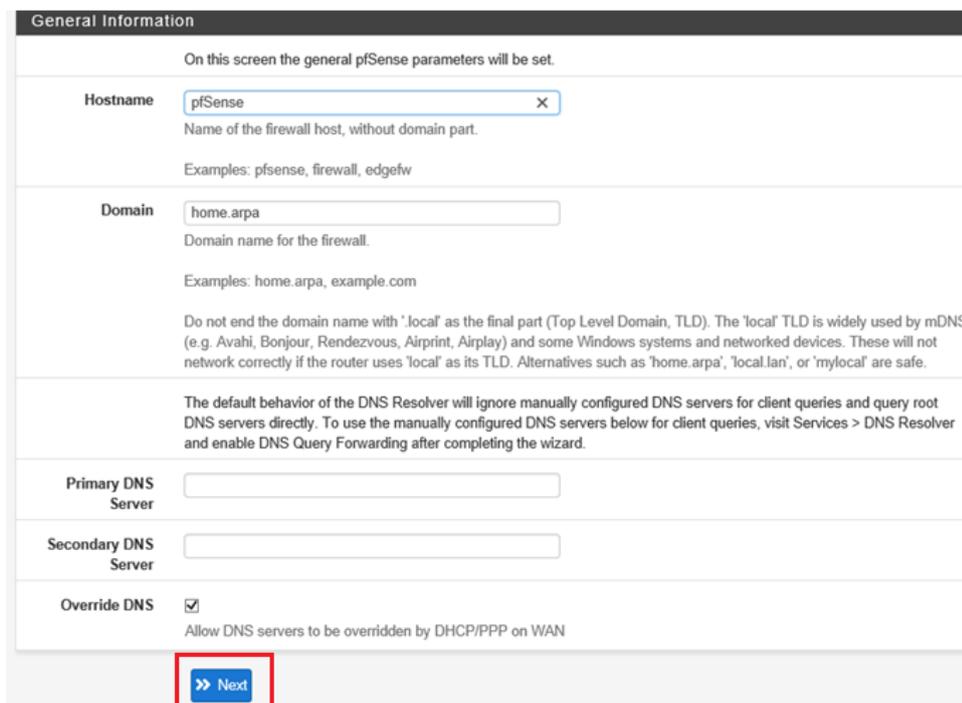


Le message d'information concernant le support 24/7 de Netgate apparaît ensuite. Cliquez sur "Next" pour continuer.



The screenshot shows the pfSense web interface. At the top, there is a navigation menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Wizard / pfSense Setup / Netgate® Global Support is available 24/7". It indicates "Step 1 of 9" and contains text about Netgate's 24/7 support team. A "Learn more" button is visible, and a "Next" button is highlighted with a red box.

Vous pouvez modifier ici le nom d'hôte du routeur si nécessaire, puis cliquez sur "Next" pour poursuivre.

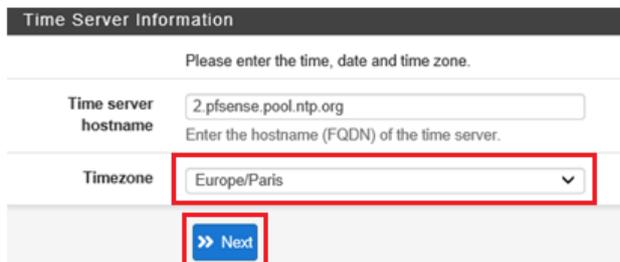


The screenshot shows the "General Information" configuration page in pfSense. It contains the following fields and options:

- Hostname:** A text input field containing "pfSense". Below it, a description: "Name of the firewall host, without domain part." and examples: "Examples: pfsense, firewall, edgefw".
- Domain:** A text input field containing "home.arpa". Below it, a description: "Domain name for the firewall." and examples: "Examples: home.arpa, example.com".
- Primary DNS Server:** An empty text input field.
- Secondary DNS Server:** An empty text input field.
- Override DNS:** A checkbox that is checked. Below it, a description: "Allow DNS servers to be overridden by DHCP/PPP on WAN".

A "Next" button is highlighted with a red box at the bottom of the page.

Choisissez le fuseau horaire approprié, ici **Europe/Paris**, afin d'éviter toute désynchronisation du pare-feu avec les machines du réseau LAN. Un mauvais paramètre horaire pourrait entraîner des dysfonctionnements au niveau du routage et des services réseau.



Time Server Information

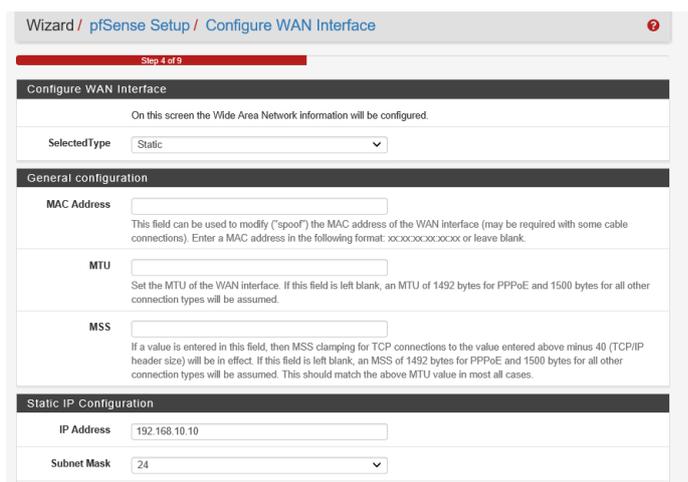
Please enter the time, date and time zone.

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

Timezone: Europe/Paris

Next

Cliquez sur **Next** pour poursuivre la configuration.



Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

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

SelectedType: Static

General configuration

MAC Address: [Empty]
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

MTU: [Empty]
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

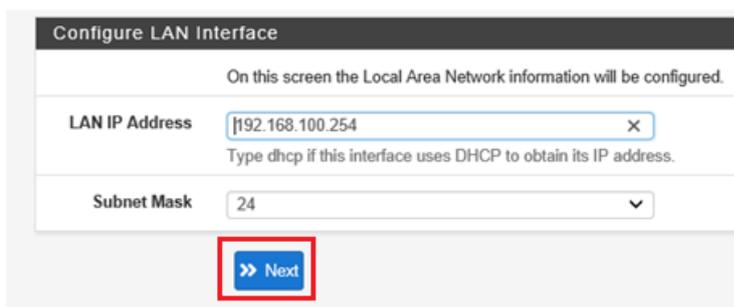
MSS: [Empty]
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address: 192.168.10.10

Subnet Mask: 24

Laissez l'adresse IP LAN telle qu'elle a été définie précédemment (192.168.100.254) ainsi que le masque 24, puis cliquez sur **Next** pour continuer la configuration.



Configure LAN Interface

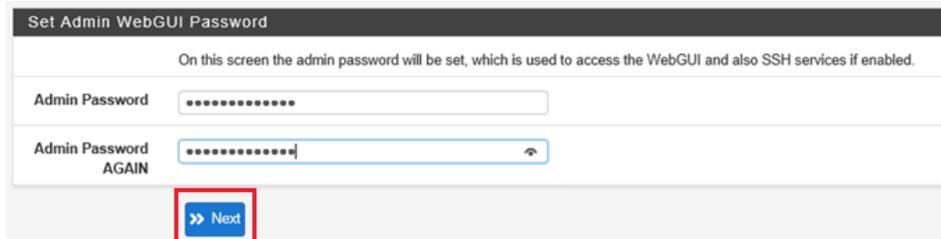
On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.100.254
Type dhcp if this interface uses DHCP to obtain its IP address.

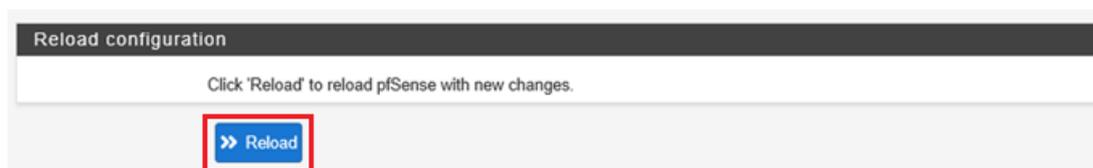
Subnet Mask: 24

Next

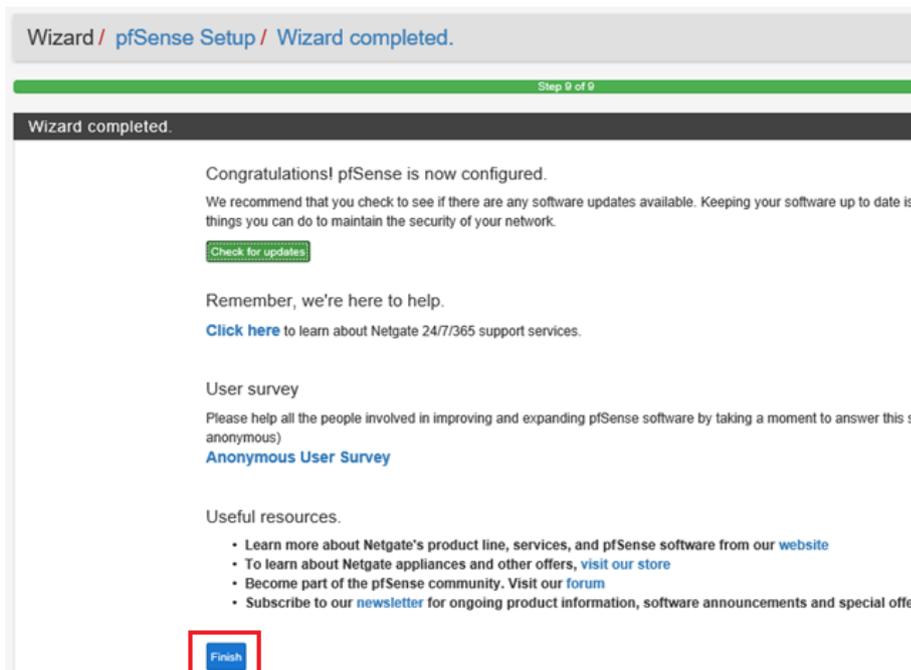
Modifiez impérativement le mot de passe administrateur pour sécuriser le routeur, puis cliquez sur **Next**. Pensez à enregistrer ce mot de passe dans un gestionnaire comme KeePass si plusieurs personnes doivent y accéder.



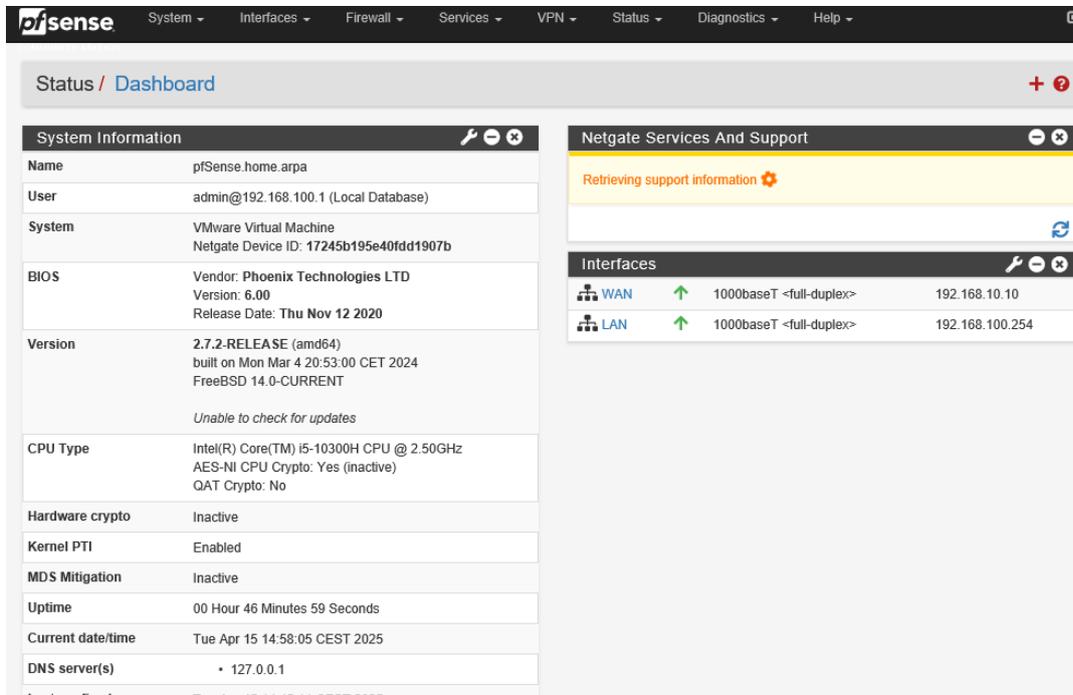
Cliquez sur **Reload** et patientez le temps que les configurations s'appliquent.



Patiencez, puis **Finish** pour confirmer et quittez la configuration globale du routeur.



Ainsi, vous accédez désormais au tableau de bord de l'interface web de pfSense.



3.1.2) Mise en place d'un VPN site-à-site sécurisé : IPsec

Pour la mise en place du VPN site-à-site, nous utiliserons le protocole IPsec, largement adopté dans ce contexte. Pour débiter la configuration, cliquez sur VPN → IPsec dans le menu supérieur.



Pour initialiser le tunnel IPSec, cliquez sur **Add P1** afin de créer la première phase de la connexion VPN.

IPsec Tunnels								
ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
								+ Add P1

Configuration de la phase 1 IPSec

Ajoutez une description au tunnel afin de faciliter son identification pour l'administration, puis renseignez l'adresse WAN du routeur distant correspondant au site de destination.

General Information	
Description	STG -> MUL <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1
IKE Endpoint Configuration	
Key Exchange version	IKEv2 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	192.168.10.20 <small>Enter the public IP address or host name of the remote gateway.</small>

Pour la configuration des paramètres IKE :

- **Key Exchange Version** : L'option *Auto* est conseillée si la version du protocole d'échange de clés entre les deux sites est inconnue. Toutefois, il est préférable d'utiliser *IKEv2*, reconnu comme la norme actuelle, dès lors que cela est possible sur chaque site.
- **Internet Protocol** : Sélectionnez *IPv4*, car la configuration réseau repose uniquement sur cette version du protocole.
- **Interface** : Choisissez *WAN*, afin que le tunnel VPN utilise cette interface comme point de communication vers le site distant.

Cliquez sur **Generate Pre-Shared Key** pour générer une clé pré-partagée. Cette clé devra impérativement être conservée, car elle sera utilisée pour la configuration du routeur distant.

Phase 1 Proposal (Authentication)

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

My identifier My IP address

Peer identifier Peer IP address

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

[Generate new Pre-Shared Key](#)

Ensuite, sélectionnez l’algorithme de chiffrement pour le tunnel VPN IPSec. Ce choix dépend des exigences de sécurité de l’entreprise. Il est important de noter que ce paramètre influence directement les performances du VPN :

- Une **valeur élevée** offre une **meilleure sécurité**, mais peut **réduire les performances**.
- À l’inverse, une **valeur plus légère** améliore la **rapidité**, mais au détriment de la **protection**.

Le bon compromis doit donc être adapté au contexte d’usage et aux priorités de l’organisation.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm	Key length	Hash	DH Group	
AES	256 bits	SHA256	16 (4096 bit)	Delete

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

Add Algorithm [+ Add Algorithm](#)

À cette étape, vous pouvez spécifier le port utilisé par le protocole **IKEv2**, qui utilise par défaut les ports **UDP 500 et 4500**. En laissant ce champ vide, pfSense appliquera automatiquement ces ports standards.

Cliquez ensuite sur **Save** pour enregistrer la configuration.

Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	<div style="display: flex; justify-content: space-between;"> <div> <input type="text" value="Remote IKE Port"/> UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500). </div> <div> <input type="text" value="Remote NAT-T Port"/> UDP port for NAT-T on the remote gateway. ⓘ </div> </div>
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	<input type="text" value="10"/> Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Max failures	<input type="text" value="5"/> Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.
<input type="button" value="Save"/>	



Rappel important :

Sur les deux pfSense Strasbourg et Mulhouse, pensez à désactiver les options **"Block private networks"** et **"Block bogon networks"** dans l'interface **WAN**.

Cela est nécessaire pour permettre le bon fonctionnement du VPN, car les adresses utilisées entre les sites font partie des plages privées (192.168.x.x) et seraient bloquées par défaut.

Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
<input type="button" value="Save"/>	

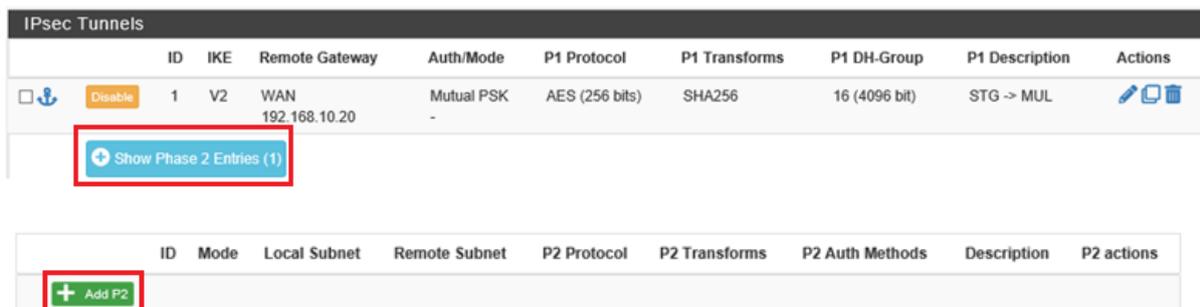
Pour plus d'informations concernant les options avancées, vous pouvez consulter la documentation officielle proposée par Netgate : <https://docs.netgate.com>

Nous passons maintenant à la configuration de la **Phase 2**, qui permet d'établir la liaison entre le réseau LAN de Strasbourg et celui de Mulhouse.

Configuration de la phase 2 du Tunnel

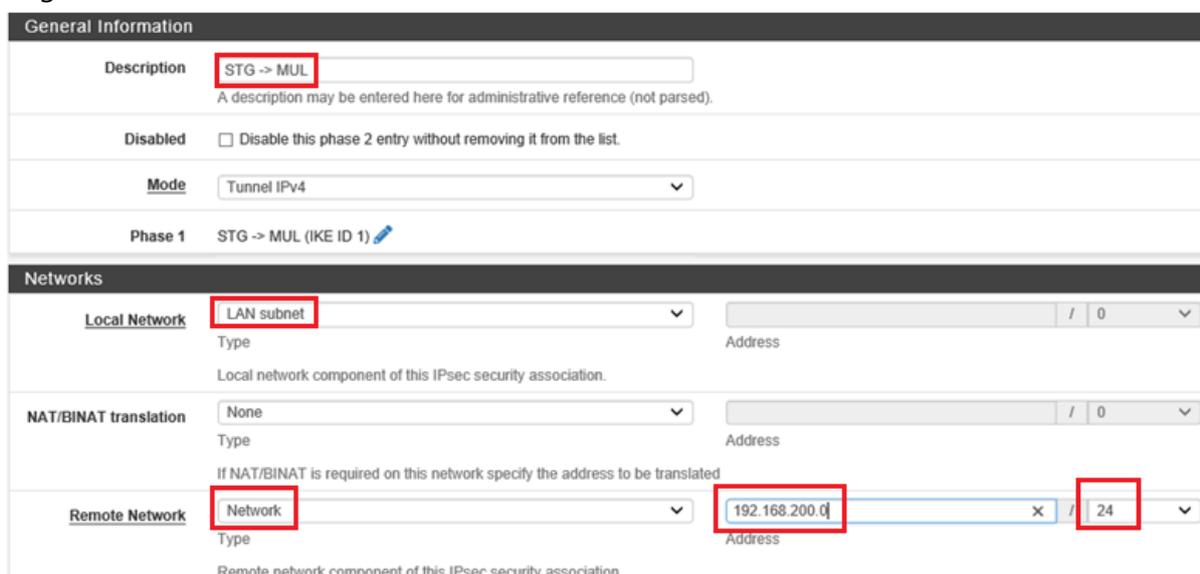
Pour commencer la configuration de la phase 2 du tunnel, cliquez sur Show Phase 2 **Entries**.

Cliquez sur **Add P2**.



The screenshot shows the 'IPsec Tunnels' configuration page. At the top, there is a table with columns: ID, IKE, Remote Gateway, Auth/Mode, P1 Protocol, P1 Transforms, P1 DH-Group, P1 Description, and Actions. A single entry is visible with ID 1, IKE V2, Remote Gateway WAN (192.168.10.20), Auth/Mode Mutual PSK, P1 Protocol AES (256 bits), P1 Transforms SHA256, P1 DH-Group 16 (4096 bit), and P1 Description STG -> MUL. Below the table, a button labeled '+ Show Phase 2 Entries (1)' is highlighted with a red box. Further down, a button labeled '+ Add P2' is also highlighted with a red box.

Ajoutez une description pour faciliter l'administration, puis renseignez l'adresse du réseau LAN distant à atteindre via le VPN. Pour une connexion de **Strasbourg vers Mulhouse**, le réseau distant sera **192.168.200.0/24** ; inversement, depuis **Mulhouse vers Strasbourg**, il s'agira de **192.168.100.0/24**.



The screenshot shows the 'General Information' and 'Networks' configuration page. In the 'General Information' section, the 'Description' field is set to 'STG -> MUL'. The 'Mode' is set to 'Tunnel IPv4'. In the 'Networks' section, the 'Local Network' is set to 'LAN subnet'. The 'Remote Network' is set to 'Network' with the address '192.168.200.0/24'.

Ensuite, sélectionnez le protocole de chiffrement pour le tunnel. Par défaut, pfSense utilise ESP, qui convient parfaitement pour une liaison VPN sécurisée.

Phase 2 Proposal (SA/Key Exchange)

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

Encryption Algorithms

<input checked="" type="checkbox"/> AES	256 bits	<input type="text" value="v"/>
<input checked="" type="checkbox"/> AES128-GCM	128 bits	<input type="text" value="v"/>
<input type="checkbox"/> AES192-GCM	Auto	<input type="text" value="v"/>
<input type="checkbox"/> AES256-GCM	Auto	<input type="text" value="v"/>
<input type="checkbox"/> CHACHA20-POLY1305		

Hash Algorithms SHA1 SHA256 SHA384 SHA512 AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group 14 (2048 bit)

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

- **Protocol** : Sélectionnez **ESP**, qui permet à la fois le chiffrement et l'authentification des paquets échangés sur le tunnel VPN. Contrairement à **AH**, ESP ajoute une couche de sécurité supplémentaire en chiffrant les données.
- **Encryption Algorithms** : Choisissez **AES** ou **AES128-GCM**. Pour cette démonstration, nous conserverons les valeurs par défaut, mais notez que **AES256** est recommandé en environnement de production.
- **Hash Algorithms** : Sélectionnez **SHA512** pour garantir un niveau de sécurité élevé lors du hachage des données.

Cochez ensuite **Keep Alive** afin de maintenir le tunnel actif en permanence et d'initier automatiquement la liaison VPN site-à-site au démarrage du routeur.

Cliquez enfin sur **Save** pour enregistrer la configuration.

Keep Alive

Automatically ping host

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 check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This check ignores the P1 option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this only needs to be enabled on one P2.

Le tunnel a été créé correctement.

IPsec Tunnels																													
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions																				
<input type="checkbox"/>	1	V2	WAN 192.168.1.225	Mutual PSK -	AES (256 bits)	SHA256	16 (4096 bit)	STG -> MUL	  																				
<table border="1"> <thead> <tr> <th></th> <th>ID</th> <th>Mode</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> <th>Description</th> <th>P2 actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>1</td> <td>tunnel</td> <td>LAN</td> <td>192.168.200.0/24</td> <td>ESP</td> <td>AES (256 bits), AES128-GCM (128 bits)</td> <td>SHA512</td> <td>STG -> MUL</td> <td>  </td> </tr> </tbody> </table>											ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions	<input type="checkbox"/>	1	tunnel	LAN	192.168.200.0/24	ESP	AES (256 bits), AES128-GCM (128 bits)	SHA512	STG -> MUL	  
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions																				
<input type="checkbox"/>	1	tunnel	LAN	192.168.200.0/24	ESP	AES (256 bits), AES128-GCM (128 bits)	SHA512	STG -> MUL	  																				
<input type="button" value="+ Add P2"/>																													
							<input type="button" value="+ Add P1"/>	<input type="button" value="Delete P1s"/>																					

À présent, il est nécessaire d'ajouter une règle de pare-feu sur l'interface IPsec et sur l'interface LAN afin d'autoriser la communication entre les deux réseaux locaux : **192.168.100.0/24 (Strasbourg)** et **192.168.200.0/24 (Mulhouse)**.

Mise en place des règles de pare-feu

Pour renforcer la sécurité du système d'information, nous allons définir des règles de pare-feu strictes.

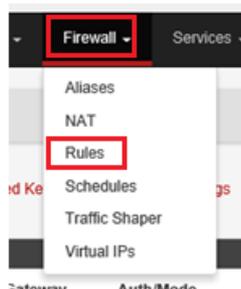
Par défaut, tout le trafic est autorisé sur l'interface LAN. Nous allons donc restreindre cela et ne conserver que les règles essentielles au bon fonctionnement de la communication intersite et du trafic interne.

Ensuite, afin d'autoriser les échanges via le tunnel VPN, il est nécessaire d'ajouter une règle sur l'interface IPsec, apparue après la configuration du tunnel.

Enfin, sur l'interface WAN, nous bloquerons l'intégralité du trafic entrant, en n'autorisant uniquement que les communications entre les deux adresses IP WAN des routeurs de chaque site.

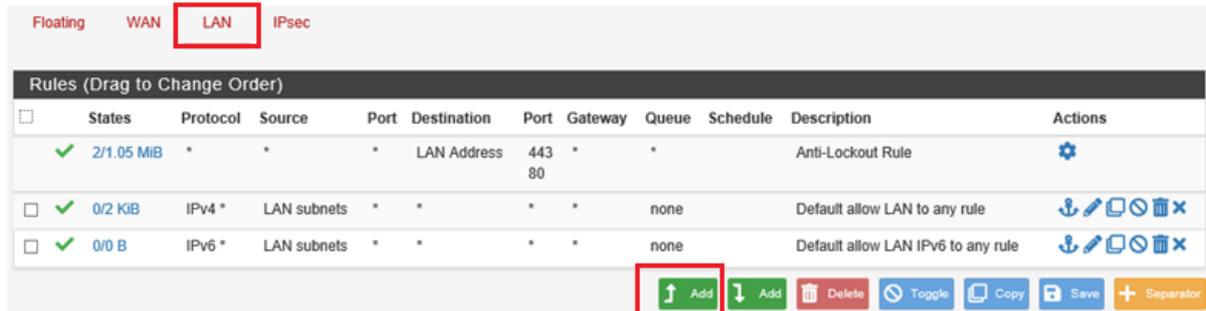
Règles sur l'interface LAN

Pour rajouter des règles de pare-feu, cliquez sur **Firewall → Rules**



Cliquez ensuite sur **LAN**, puis sur **Add** pour ajouter une règle.

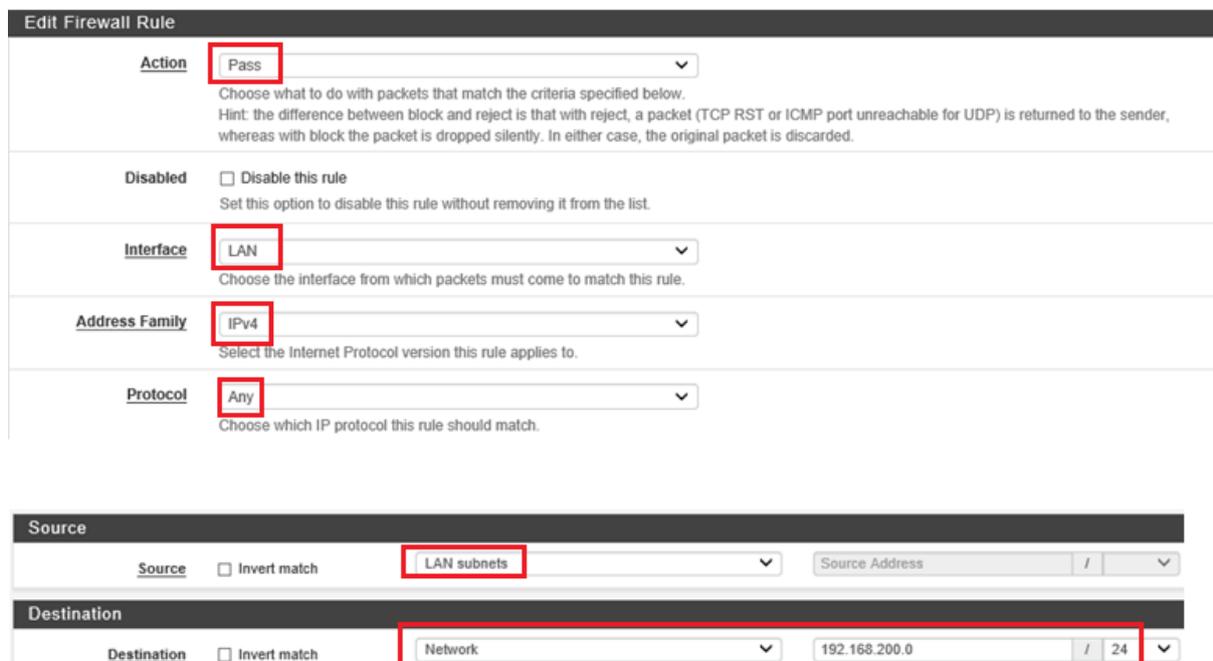
À noter : pfSense lit les règles de pare-feu de haut en bas et s'arrête dès qu'une règle correspond au trafic. L'ordre des règles est donc crucial pour le bon fonctionnement du filtrage.



States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/1.05 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	⚙️
✓ 0/2 KIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	📌 🗑️ 🔄 🚫
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 🗑️ 🔄 🚫

Commencez par créer une règle de pare-feu autorisant le trafic en provenance du réseau LAN distant vers le réseau LAN local.

⚠️ Cette règle devra être adaptée en fonction du routeur/pare-feu sur lequel vous effectuez la configuration.



Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface LAN

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

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol Any

Choose which IP protocol this rule should match.

Source

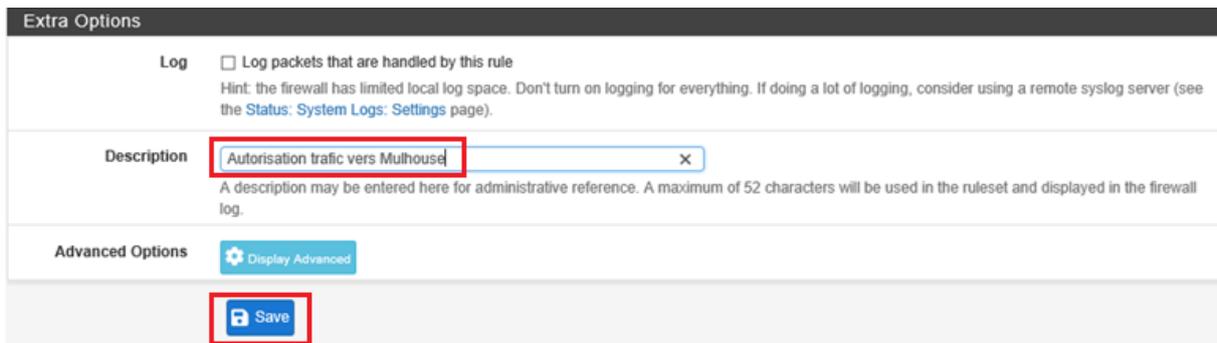
Source Invert match LAN subnets Source Address /

Destination

Destination Invert match Network 192.168.200.0 / 24

Création de la règle de pare-feu (LAN → réseau distant)

- **Action** : Pass pour autoriser le trafic défini dans la règle
- **Interface** : LAN
- **Address Family** : IPv4 (ajoutez IPv6 si nécessaire)
- **Protocol** : Any pour autoriser tous les protocoles
- **Source** : LAN Subnets (soit 192.168.100.0/24 pour Strasbourg, 192.168.200.0/24 pour Mulhouse)
- **Destination** : sous-réseau distant — ex : 192.168.200.0/24 si vous êtes à Strasbourg



Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description ✕
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

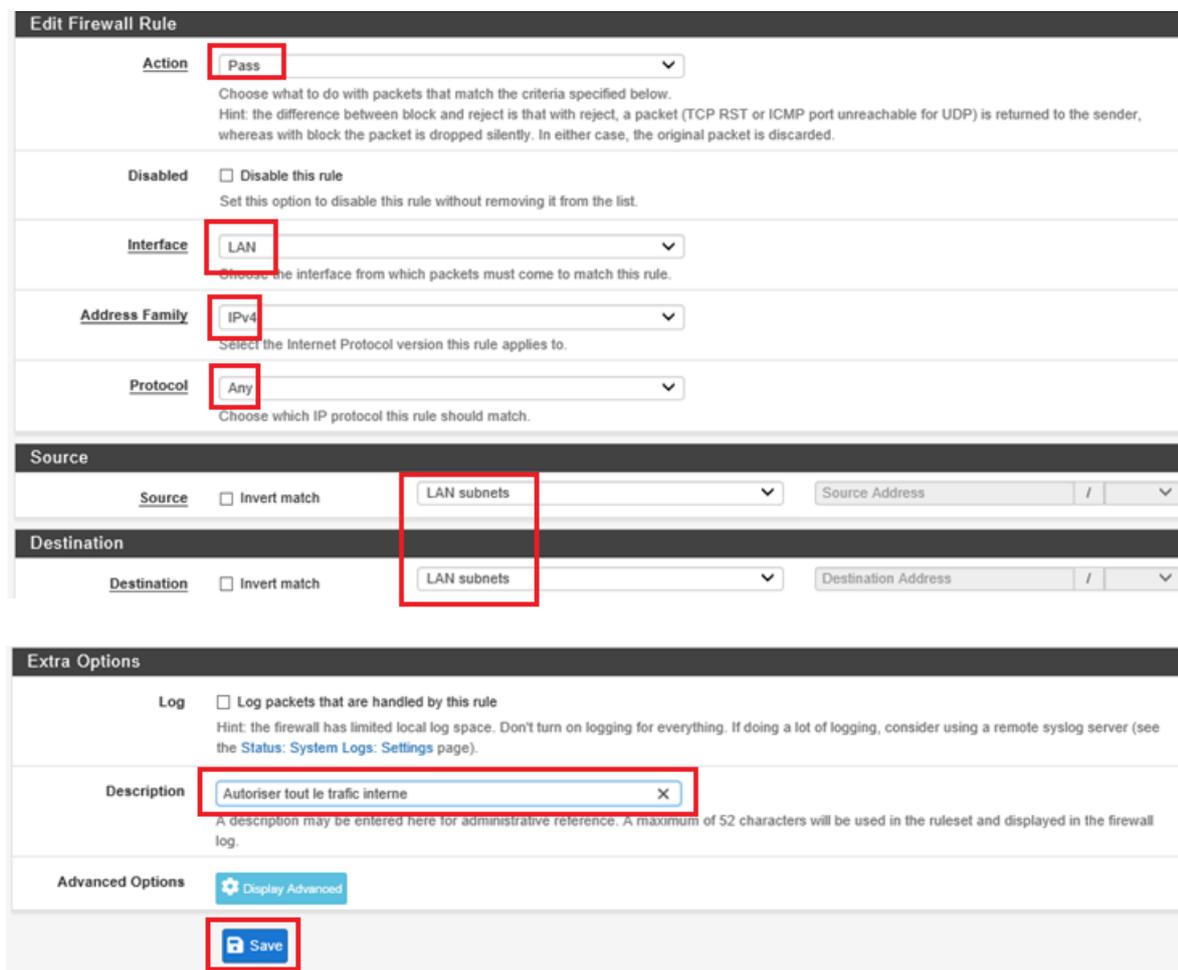
- **Description** : Ajoutez un libellé clair pour l'administration, comme *"Autorisation trafic vers site distant"*

Puis, appuyez sur **Save** et cliquez sur **Apply Changes** pour valider les changements sur les règles.

À présent, nous allons également mettre en place les règles de pare-feu sur l'interface LAN, n'autorisant uniquement que le trafic sur tous les ports au sein du réseau LAN, ainsi que l'accès à Internet en ouvrant les ports 80, 443 et 53

Règles pour autoriser tout le trafic intranet

Indiquez **LAN Address** en source et en destination, ce qui correspond au sous-réseau local, avec **IPv4**, tous les protocoles et tous les ports, puis cliquez sur **Save** pour enregistrer la règle.



Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface

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

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

Source Invert match /

Destination

Destination Invert match /

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

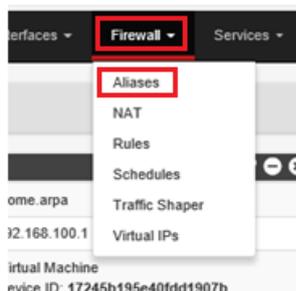
Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

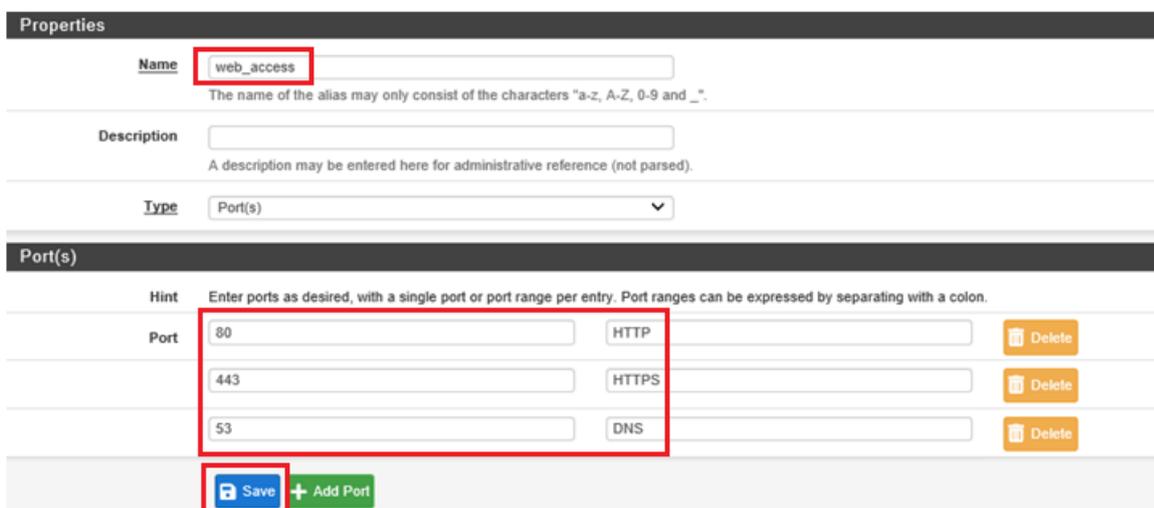
Advanced Options

Règles pour autoriser l'accès Internet sur l'interface LAN

Tout d'abord, rajoutez un alias de ports pour inclure les ports 80 (HTTP), 443 (HTTPS) et 53 (DNS), nécessaires pour accéder à une page web. Pour cela, cliquez sur **Firewall** → **Aliases**.



Ensuite, cliquez sur **Add** et ajoutez les ports. L'intérêt des alias est de regrouper plusieurs ports non successifs afin d'éviter de créer une règle par port, ce qui rend les règles de pare-feu plus lisibles.

A screenshot of the 'Properties' form for a Firewall Alias. The 'Name' field contains 'web_access' and is highlighted with a red box. Below it, the 'Description' field is empty. The 'Type' dropdown is set to 'Port(s)'. Below the 'Port(s)' section, there is a table with three rows, each representing a port and its protocol. The first row is '80 HTTP', the second is '443 HTTPS', and the third is '53 DNS'. These three rows are highlighted with a red box. At the bottom, there is a blue 'Save' button and a green '+ Add Port' button. The 'Save' button is also highlighted with a red box.

Port	Protocol	Action
80	HTTP	Delete
443	HTTPS	Delete
53	DNS	Delete

Enfin, ajoutez une règle autorisant le trafic depuis le LAN vers toutes les destinations (Internet), en utilisant l'alias web_access pour les ports. Cochez les protocoles TCP et UDP, car HTTP et HTTPS utilisent TCP, tandis que le DNS fonctionne en UDP.

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface LAN

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

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP

Choose which IP protocol this rule should match.

Source

Source Invert match LAN subnets Source Address /

⚙️ Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match Any Destination Address /

Destination Port Range (other)

From web_access Custom To (other) Custom web_access Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everyt the Status: System Logs: Settings page).

Description Autoriser web access

A description may be entered here for administrative reference. A maximum log.

Advanced Options ⚙️ Display Advanced

💾 Save

Ainsi, pour résumer, voici un aperçu final des règles de pare-feu appliquées sur l'interface LAN.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1.66 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	LAN subnets	*	*	none		Autoriser tout le trafic interne	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN subnets	*	*	web_access	*	none		Autoriser web access	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	192.168.200.0/24	*	*	none		Autorisation trafic vers Mulhouse	
<input type="checkbox"/>	0/234 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

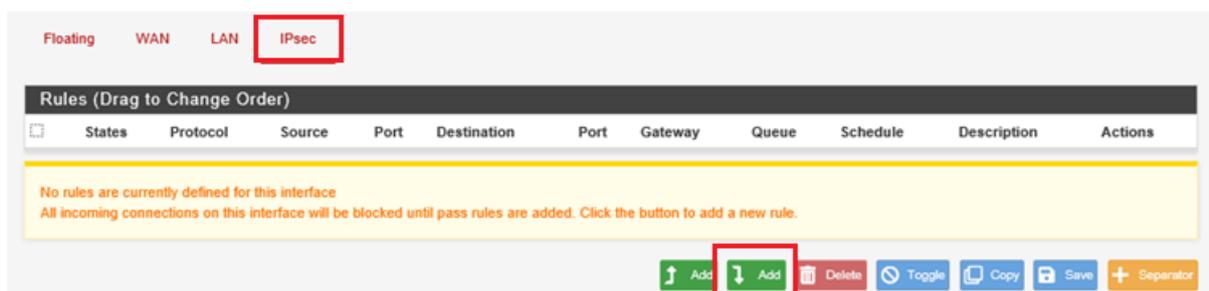
Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Règles pour IPSec

Maintenant que les règles de pare-feu sur l'interface LAN sont en place, il convient d'ajouter une règle sur l'interface IPSec afin de permettre le passage du trafic provenant du sous-réseau distant à travers le tunnel VPN.

Pour cela, accédez à l'onglet **IPSec**, puis cliquez sur **Add** pour créer une nouvelle règle.

Cette règle devra avoir pour source le sous-réseau distant. Par exemple, sur le pare-feu de Strasbourg, le sous-réseau distant est **192.168.200.0/24**.



Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

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

Protocol
 Choose which IP protocol this rule should match.

Source

Source Invert match /

Destination

Destination Invert match

Extra Options

Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Ainsi, sur l'interface IPsec, la règle présente est comme ci-dessous :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.200.0/24	*	LAN subnets	*	*	none	Autorisation trafic Mulhouse to LAN	<input type="button" value="Save"/> <input type="button" value="Copy"/> <input type="button" value="Toggle"/> <input type="button" value="Delete"/> <input type="button" value="Add"/> <input type="button" value="Add"/>

Règles sur l'interface WAN

Sur l'interface **WAN**, deux règles de pare-feu doivent être ajoutées.

La première consistera en une règle **implicite de blocage**, visant à refuser tout le trafic entrant sur cette interface.

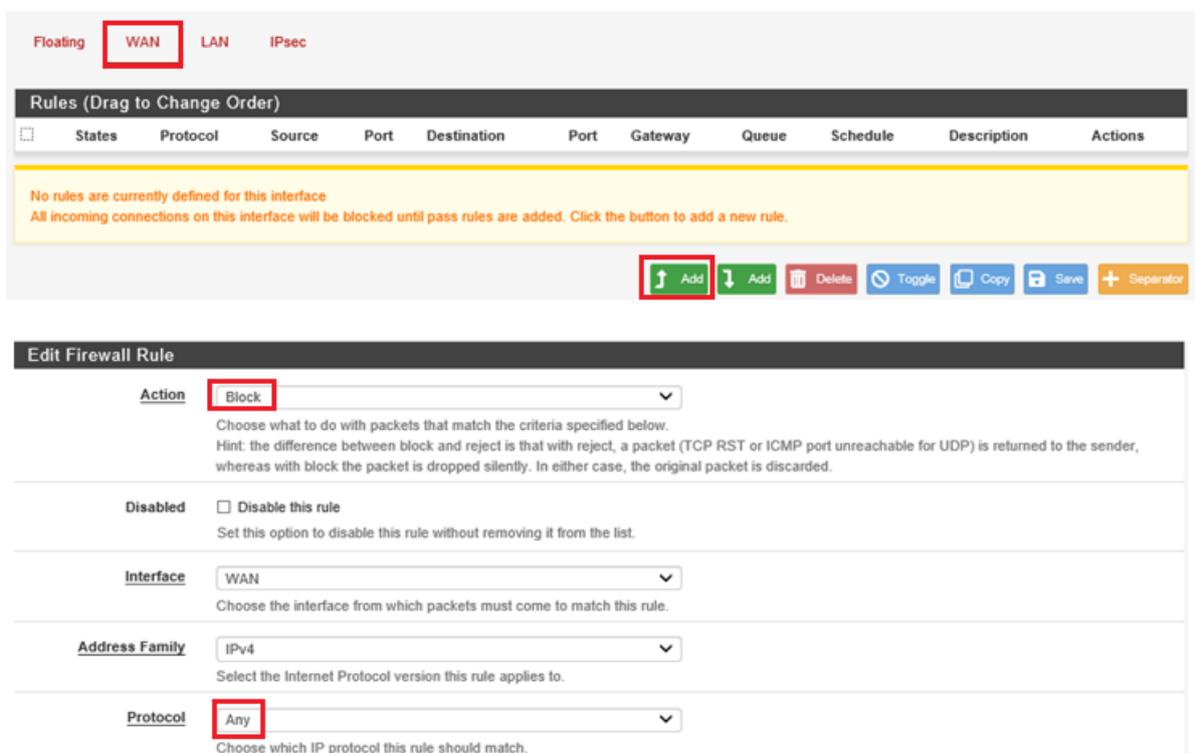
La seconde autorisera **uniquement le trafic en provenance de l'adresse IP WAN du site distant**, afin de permettre et maintenir la liaison VPN site-à-site.

Règles bloquant tout le trafic

Comme pour l'interface LAN, nous allons mettre en place une règle de pare-feu sur l'interface **WAN** afin de **bloquer l'ensemble du trafic**. Cette mesure renforce la sécurité en protégeant le système contre d'éventuelles cyberattaques externes.

Pour cela, créez une règle de **blocage (Block)** sur l'interface **WAN**, en appliquant cette restriction à **tous les protocoles, toutes les sources et toutes les destinations**.

Cette règle doit être appliquée uniquement en **IPv4**, car l'interface **IPv6 n'a pas été configurée** ; le trafic IPv6 sera donc ignoré par défaut.



The screenshot shows the Mikrotik WinBox Firewall configuration interface. At the top, there are tabs for 'Floating', 'WAN', 'LAN', and 'IPsec', with 'WAN' selected. Below this is a table for 'Rules (Drag to Change Order)' with columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A yellow message box states: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.' Below the message box are buttons for 'Add', 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'. The 'Add' button is highlighted with a red box. Below this is the 'Edit Firewall Rule' form. The 'Action' dropdown is set to 'Block' (highlighted with a red box). The 'Interface' dropdown is set to 'WAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'Any' (highlighted with a red box).

Source	
Source	<input type="checkbox"/> Invert match Any
Source Address /	
Destination	
Destination	<input type="checkbox"/> Invert match Any
Destination Address /	
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Tout bloquer A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>
<input type="button" value="Save"/>	

Règle autorisant que le trafic provenant du site distant

Edit Firewall Rule	
Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	

Source	
Source	<input type="checkbox"/> Invert match Address or Alias 192.168.10.20
Source Address /	
Destination	
Destination	<input type="checkbox"/> Invert match WAN address
Destination Address /	
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Autorisation WAN traffic MUL -> STG A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>
<input type="button" value="Save"/>	

Pour finaliser l'ensemble des règles de pare-feu, il reste à autoriser uniquement le trafic provenant de l'adresse IP WAN du site distant : **192.168.10.20** si vous êtes sur **Strasbourg**, ou **192.168.10.10** si vous êtes à **Mulhouse**.

Ainsi les règles sur l'interface **WAN** sont :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.10.20	*	WAN address	*	*	none	Autorisation WAN trafic MUL -> STG	
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	*	*	*	none	Tout bloquer	

Configuration sur le routeur/pare-feu de Mulhouse

Les manipulations effectuées précédemment sur le routeur/pare-feu de Strasbourg doivent désormais être reproduites sur celui de Mulhouse, en adaptant les adresses IP et paramètres selon la configuration de ce site.

⚠ Point de vigilance : La clé pré-partagée (Pre-Shared Key) doit être strictement identique à celle générée sur le pare-feu de Strasbourg pour garantir le bon établissement du tunnel VP

Configuration des paramètres réseau de la machine principale de Mulhouse pour son intégration au réseau local via une IP statique

Propriétés de : Protocole Internet version 4 (TCP/IPv4) ✕

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement
 Utiliser l'adresse IP suivante :

Adresse IP :
 Masque de sous-réseau :
 Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement
 Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :
 Serveur DNS auxiliaire :

Valider les paramètres en quittant

Sur le routeur/pare-feu du site de Mulhouse, voici les configurations et règles de pare-feu mises en place :

Configuration du Tunnel Phase 1

Tunnel créée correctement.

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.10.10	Mutual PSK	AES (256 bits)	SHA256	16 (4096 bit)	MUL -> STG	  
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/>	1	tunnel	LAN	192.168.100.0/24	ESP	AES (256 bits), AES128-GCM (128 bits)	SHA512	MUL -> STG	  

+ Add P1 - Delete P1s

Règles de pare-feu

Interface WAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.10.10	*	WAN address	*	*	none	Autorisation WAN trafic STG -> MUL	  
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	*	*	none		Tout bloquer	  

↑ Add ↓ Add - Delete ⏸ Toggle 📄 Copy 💾 Save + Separator

Interface LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/1.03 MiB	*	*	LAN Address	443-80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	LAN subnets	*	*	none		Autoriser tout le trafic interne	  
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	*	*	web_access	*	none		Autoriser web access	  
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	192.168.100.0/24	*	*	none		Autorisation trafic vers Strasbourg	  
<input type="checkbox"/>	✓	0/1 KiB	IPv4 *	*	*	*	*	none		Default allow LAN to any rule	  
<input type="checkbox"/>	✓	0/0 B	IPv6 *	*	*	*	*	none		Default allow LAN IPv6 to any rule	  

↑ Add ↓ Add - Delete ⏸ Toggle 📄 Copy 💾 Save + Separator

Interface IPsec

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.100.0/24 *	LAN subnets	*	*	none		Autorisation trafic Strasbourg to LAN	

↑ Add
↓ Add
🗑 Delete
🔄 Toggle
📄 Copy
💾 Save
+ Separator

Test de l'interconnexion VPN site à site

🔍 Avant de diagnostiquer la connexion VPN site-à-site, assurez-vous que :

- Le service IPsec est bien démarré et opérationnel sur le routeur/pare-feu.
- L'état de la connexion IPsec est actif.
- Le ping depuis une machine du site de Strasbourg vers Mulhouse fonctionne correctement (en veillant à autoriser le protocole ICMP sur les pare-feux des postes concernés).

État du service IPsec

Pour vérifier l'état du service IPsec, cliquez sur **Status** → **Services**



Le service IPsec est bel et bien activé, donc tout est bon.

Services			
Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	    
ipsec	IPsec VPN	✓	    
ntpd	NTP clock sync	✓	    
syslogd	System Logger Daemon	✓	   
unbound	DNS Resolver	✓	    

État de la connectivité VPN

Pour vérifier l'état de la connexion VPN, cliquez sur **Status** → **IPSec**

La connexion VPN a bel et bien été établie !

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #5	MUL -> STG 	ID: 192.168.10.20 Host: 192.168.10.20:500 SPI: 37910526512b274f	ID: 192.168.10.10 Host: 192.168.10.10:500 SPI: 1f913b8bd097b933	IKEv2 Initiator	Rekey: 23399s (06:29:59) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_4096	Established 860 seconds (00:14:20) ago 
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #2	MUL -> STG 	192.168.200.0/24	Local: cce54e92 Remote: c7793c8c	192.168.100.0/24	Rekey: 2192s (00:36:32) Life: 2740s (00:45:40) Install: 860s (00:14:20)	AES_GCM_16 (128) IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0 Installed 

Test de connectivité intersite par ping

Enfin, pour vérifier davantage la connectivité entre les deux sites, nous allons effectuer un test de ping entre les machines de chaque site.

Avant de diagnostiquer l'état de la connexion VPN site-à-site, assurez-vous que :

- Le service IPSec est bien démarré et fonctionnel sur les deux routeurs/pare-feux
- L'état du tunnel IPSec indique qu'il est actif
- Le ping entre les machines des deux sites est possible — en veillant à **activer les règles ICMP "Demande d'écho - Trafic entrant (ICMPv4)"** dans le pare-feu Windows de chaque serveur.

Ping du serveur STG-SRVW01 vers MUL-SRVW01

```
C:\Users\Administrateur>hostname
STG-SRVW01

C:\Users\Administrateur>ping 192.168.200.1

Envoi d'une requête 'Ping' 192.168.200.1 avec 32 octets de données :
Réponse de 192.168.200.1 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.200.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Ping du serveur MUL-SRVW01 vers STG-SRVW01

```
C:\Users\Administrateur>hostname
MUL-SRVW01

C:\Users\Administrateur>ping 192.168.100.1

Envoi d'une requête 'Ping' 192.168.100.1 avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps=4 ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=126

Statistiques Ping pour 192.168.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 4ms, Moyenne = 2ms
```

 **Les connexions entre les sites ont bien été établies avec succès !**

Les pings entre les machines des deux sites sont fonctionnels

Maintenant que le VPN site à site est en place, nous allons mettre commencer l'harmonisation et l'installation de l'environnement Active Directory.

3.1.3) Paramétrage des serveurs Windows

Avant d'installer les rôles sur le serveur, il est nécessaire de réaliser certaines configurations de base : renommage de la machine, association des cartes réseau (NIC Teaming) et configuration IP statique. Ces étapes peuvent être effectuées via l'interface graphique, PowerShell ou l'outil interactif sconfig, présenté dans la suite de la documentation.

Configuration minimale recommandée du serveur

Système d'exploitation : Windows Server 2019 Standard (version GUI ou Core)

Processeur : 64 bits

Mémoire vive (RAM) : 4 Go minimum (8 Go recommandé)

Stockage :

- 60 Go pour le système
- 60 Go pour les données

Réseau :

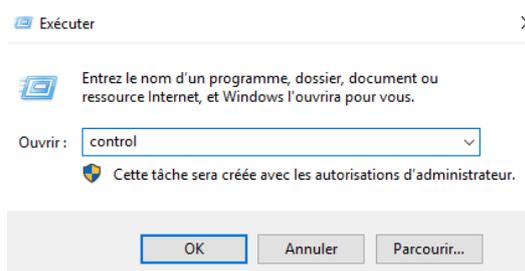
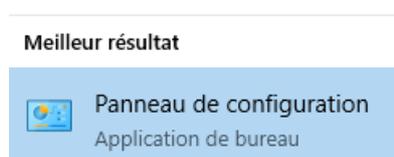
- 2 cartes réseau pour la mise en place du NIC Teaming
- Connexion au LAN de chaque site

Changement du nom de l'ordinateur

Pour renommer une machine sous Windows, deux méthodes sont possibles : via l'interface graphique (Panneau de configuration) ou en ligne de commande avec PowerShell.

Mode graphique

Ouvrez le Panneau de configuration en le recherchant dans la barre Windows ou en saisissant control dans le menu Exécuter (Windows + R).



Cliquez ensuite sur **Paramètres système avancés**, puis suivez les étapes ci-dessous.

Ajuster les paramètres de l'ordinateur Afficher par : Catégorie ▾

Système et sécurité
 Consulter l'état de votre ordinateur
 Afficher les journaux d'événements

Réseau et Internet
 Connexion à Internet
 Afficher l'état et la gestion du réseau

Matériel
 Afficher les périphériques et imprimantes
 Ajouter un périphérique

Programmes
 Désinstaller un programme
 Activer ou désactiver des fonctionnalités Windows

Comptes d'utilisateurs
 Modifier le type de compte

Apparence et personnalisation

Horloge et région
 Définir l'heure et la date
 Modifier les formats de date, d'heure ou de nombre

Options d'ergonomie
 Laisser Windows suggérer les paramètres
 Optimiser l'affichage

Sécurité et maintenance
 Vérifier l'état de votre ordinateur et résoudre les problèmes |
 Modifier les paramètres de contrôle de compte d'utilisateur |
 Résoudre des problèmes informatiques courants

Pare-feu Windows Defender
 Vérifier l'état du pare-feu | Autoriser une application via le Pare-feu Windows

Système
 Afficher la quantité de mémoire RAM et la vitesse du processeur |
 Autoriser l'accès à distance | Lancer l'assistance à distance |
 Afficher le nom de cet ordinateur

Options d'alimentation
 Modifier le comportement des boutons d'alimentation |
 Modifier les conditions de mise en veille de l'ordinateur

Outils d'administration
 Défragmenter et optimiser vos lecteurs | Créer et formater des partitions de disque dur |
 Afficher les journaux d'événements | Tâches planifiées |
 Générer un rapport sur l'intégrité du système

Informations système générales

Édition Windows

Windows Server 2019 Standard

© 2018 Microsoft Corporation. Tous droits réservés.

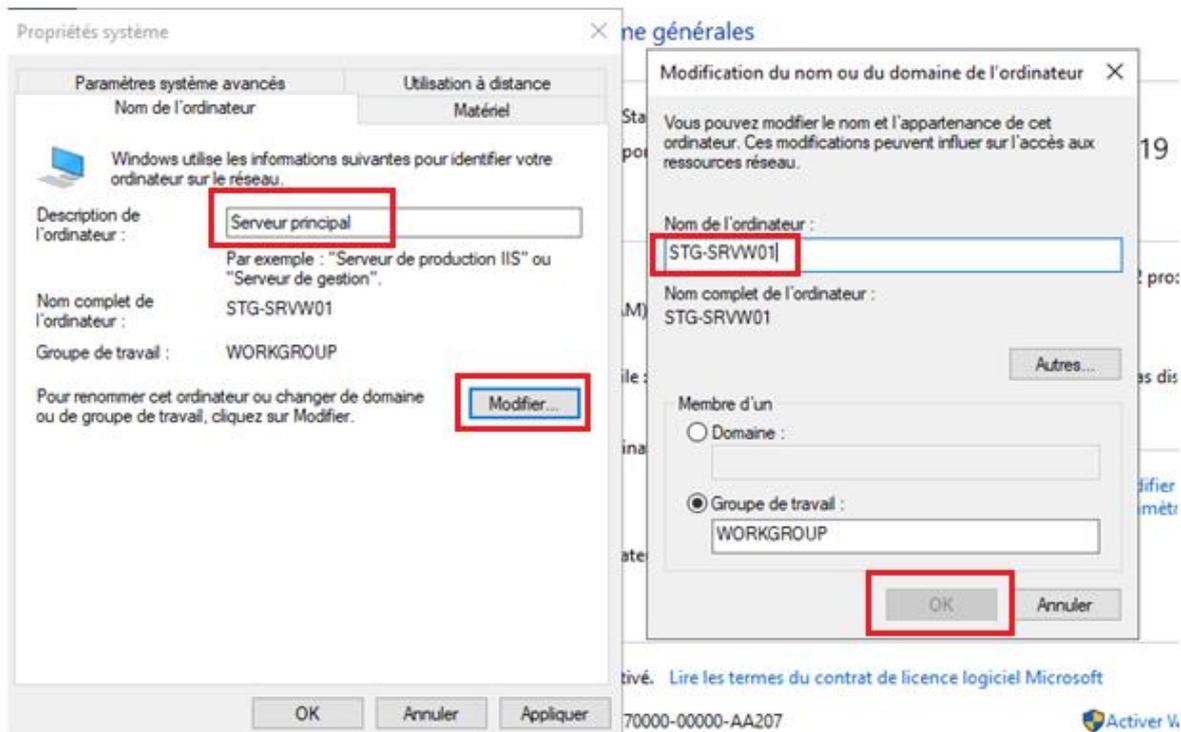
Windows Server* 2019

Système

Processeur : Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz 2.50 GHz (2 processeurs)
 Mémoire installée (RAM) : 4,00 Go
 Type du système : Système d'exploitation 64 bits, processeur x64
 Stylet et fonction tactile : La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur :	STG-SRVW01	
Nom complet :	STG-SRVW01	
Description de l'ordinateur :		
Groupe de travail :	WORKGROUP	



Redémarrez le serveur pour appliquer les modifications.

Sous PowerShell

Il est également possible de renommer le serveur via PowerShell, ce qui est plus rapide et particulièrement utile sur les versions Core de Windows Server. La commande à utiliser est la suivante :

```
Rename-Computer "STG-SRVW01"
```

Ensuite, redémarrez le serveur pour appliquer les modifications. Sous PowerShell, utilisez la commande suivante :

```
Restart-Computer
```

La façon la plus simple de vérifier le nom du serveur est d'utiliser la commande hostname, que ce soit en CMD ou dans PowerShell :

```
C:\Users\Administrateur>hostname
STG-SRVW01
C:\Users\Administrateur>
```

Configuration de l'association des cartes réseaux : NIC Teaming

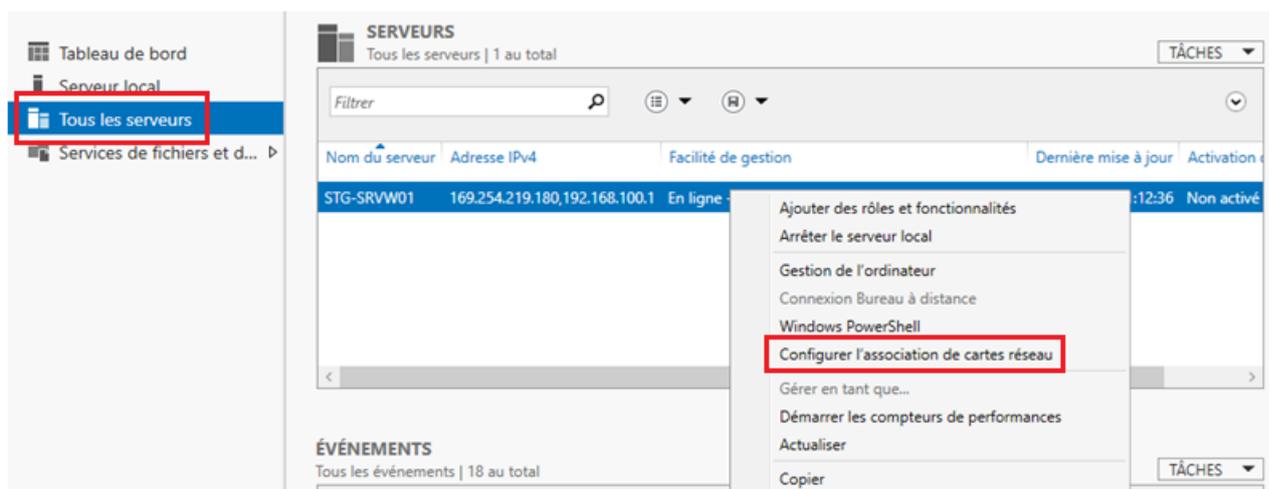
Pour assurer la **tolérance aux pannes** et optimiser la **répartition de charge réseau**, nous allons configurer le **NIC Teaming**, une fonctionnalité native de Windows Server. Cette configuration permet également d'améliorer la **bande passante** globale, répondant ainsi aux besoins de haute disponibilité du client.

Deux méthodes seront présentées :

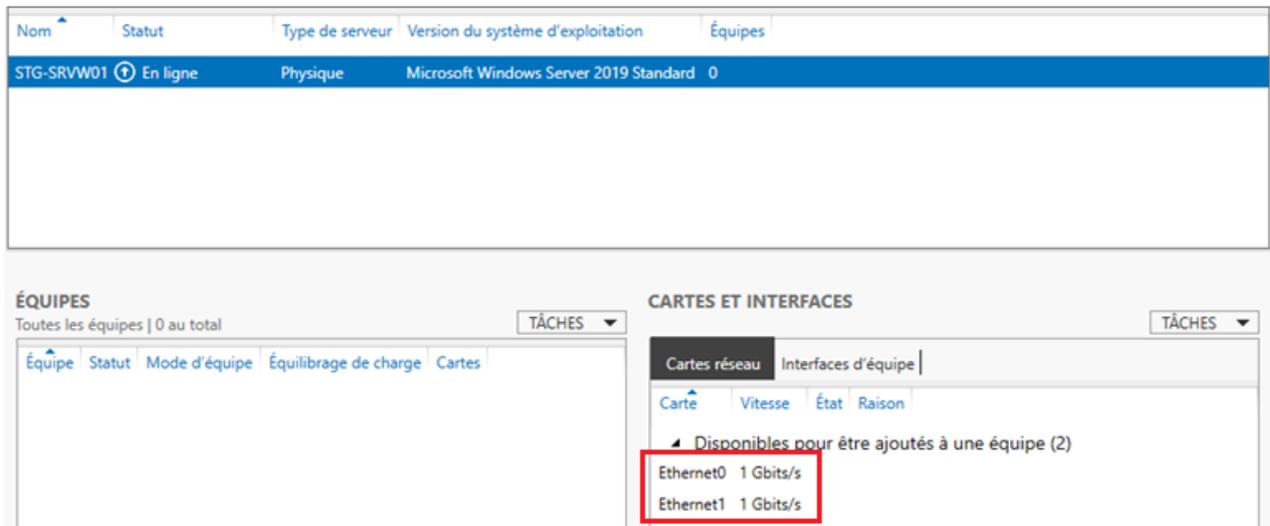
- **En mode graphique** via le Gestionnaire de serveur
 - **En ligne de commande via PowerShell**, notamment utile pour les serveurs Windows en version Core.
- ♦ **Remarque** : il est indispensable de disposer de **plus d'une carte réseau** pour pouvoir créer une équipe d'agrégation (NIC Teaming).

Mode graphique

Dans le Gestionnaire de serveur, accédez à l'onglet **Tous les serveurs**, faites un clic droit sur le serveur concerné, puis cliquez sur **Configurer l'association de cartes réseau**.



Dans la fenêtre d'association des cartes, les deux interfaces réseau apparaissent avec une vitesse par défaut de 1 Gbit/s.



Pour créer une nouvelle équipe, cliquez sur **Tâches**, puis sélectionnez **Nouvelle équipe**.



Donnez un nom à l'équipe, puis sélectionnez les cartes réseau à inclure dans celle-ci en les cochant.

Association de cartes réseau X

Nouvelle équipe

Nom de l'équipe :

Cartes membres :

Dans l'équipe	Carte	Vitesse	État	Raison
<input checked="" type="checkbox"/>	Ethernet0	1 Gbits/s		
<input checked="" type="checkbox"/>	Ethernet1	1 Gbits/s		

Propriétés supplémentaires

Mode d'équipe :

Mode d'équilibrage de charge :

Carte réseau en attente :

Interface d'équipe principale : [LAN : VLAN par défaut](#)

- **Mode d'équipe** : *Indépendant du commutateur* — permet d'utiliser des cartes reliées à des commutateurs différents, augmentant ainsi la tolérance aux pannes et la haute disponibilité.
- **Équilibrage de charge** : *Hachage d'adresse* — répartit intelligemment le trafic entre les interfaces réseau.
- **Carte réseau en veille** : *Aucune* — les deux interfaces restent actives pour optimiser les performances.

Cliquez ensuite sur **OK** pour finaliser la création de l'équipe.

ÉQUIPES

Toutes les équipes | 1 au total

Équipe	Statut	Mode d'équipe	Équilibrage de charge	Ca
LAN	OK	Indépendant du commutateur	Hachage d'adresse	2

CARTES ET INTERFACES

Cartes réseau | Interfaces d'équipe

Carte	Vitesse	État	Raison
LAN (2)			
Ethernet0	1 Gbits/s	Actif	
Ethernet1	1 Gbits/s	Actif	

Le NIC Teaming a été correctement créé et configuré.

Sous Powershell

Pour créer l'association des cartes réseau via PowerShell, commencez par identifier le nom des interfaces disponibles à l'aide de la commande suivante :

Get-NetAdapter

Ensuite, créez l'équipe d'agrégation des interfaces réseau à l'aide de la commande suivante :

```
New-NetLbfoTeam -Name LAN -TeamMembers Ethernet0,Ethernet1 -TeamingMode SwitchIndependent -LoadBalancingAlgorithm TransportPorts
```

Name : nom de l'équipe d'agrégation

TeamMembers : interfaces réseau à inclure dans l'équipe

TeamingMode : mode d'association des cartes (identique à celui vu en interface graphique)

LoadBalancingAlgorithm : TransportPorts (équivalent au hachage d'adresse, utilisé par défaut si aucun autre algorithme n'est précisé)

```
PS C:\Users\Administrateur> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet1	Intel(R) 82574L Gigabit Network Co...#2	8	Up	00-0C-29-8A-10-62	1 Gbps
Ethernet0	Intel(R) 82574L Gigabit Network Conn...	5	Up	00-0C-29-8A-10-58	1 Gbps

```
PS C:\Users\Administrateur> New-NetLbfoTeam -Name LAN -TeamMembers Ethernet0,Ethernet1 -TeamingMode SwitchIndependent -LoadBalancingAlgorithm TransportPorts
```

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

```
Name : LAN
Members : {Ethernet0, Ethernet1}
TeamName : LAN
TeamingMode : SwitchIndependent
LoadBalancingAlgorithm : TransportPorts
Status : Degraded
```

Pour vérifier que l'association des cartes réseau a bien été effectuée, exécutez la commande suivante :

Get-NetLbfoTeam

```
PS C:\Users\Administrateur> Get-NetLbfoTeam

Name           : LAN
Members        : {Ethernet1, Ethernet0}
TeamNics       : LAN
TeamingMode    : SwitchIndependent
LoadBalancingAlgorithm : TransportPorts
Status         : Up

PS C:\Users\Administrateur> ipconfig

Configuration IP de Windows

Carte Ethernet LAN :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::ddb0:dedc:2711:8c55%10
    Adresse d'autoconfiguration IPv4 . . . . : 169.254.140.85
    Masque de sous-réseau. . . . .          : 255.255.0.0
    Passerelle par défaut. . . . .         :
PS C:\Users\Administrateur>
```

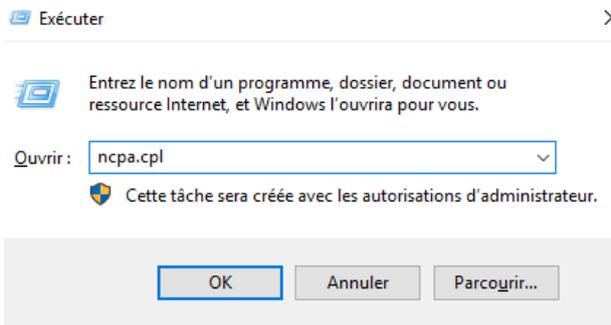
Une fois l'association des cartes réseau configurée, il convient désormais de renseigner l'adressage IP du serveur : une étape essentielle avant l'installation des rôles et fonctionnalités.

Configuration réseau du serveur

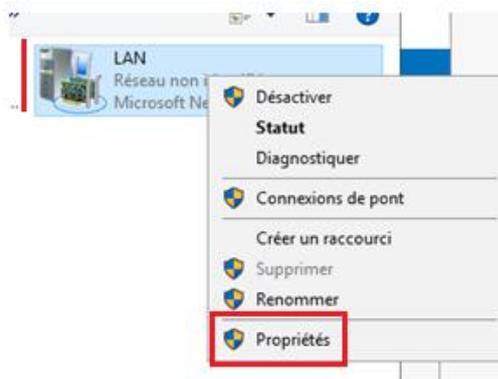
Pour la configuration réseau, nous allons attribuer une adresse IP statique à l'interface issue de l'association des cartes réseau. Nous commencerons par effectuer cette configuration via le Panneau de configuration.

Mode graphique

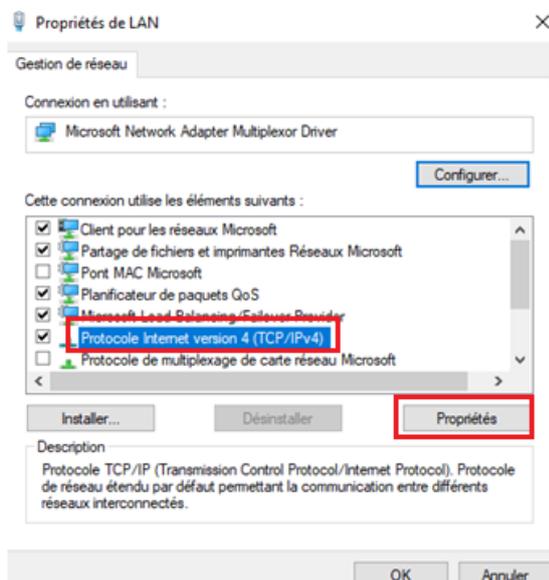
Il existe plusieurs façons d'accéder à la configuration des interfaces réseau via le Panneau de configuration. Pour simplifier l'opération, nous utiliserons le menu Exécuter (**Windows + R**) en saisissant la commande **ncpa.cpl**, qui ouvre directement la fenêtre des connexions réseau.



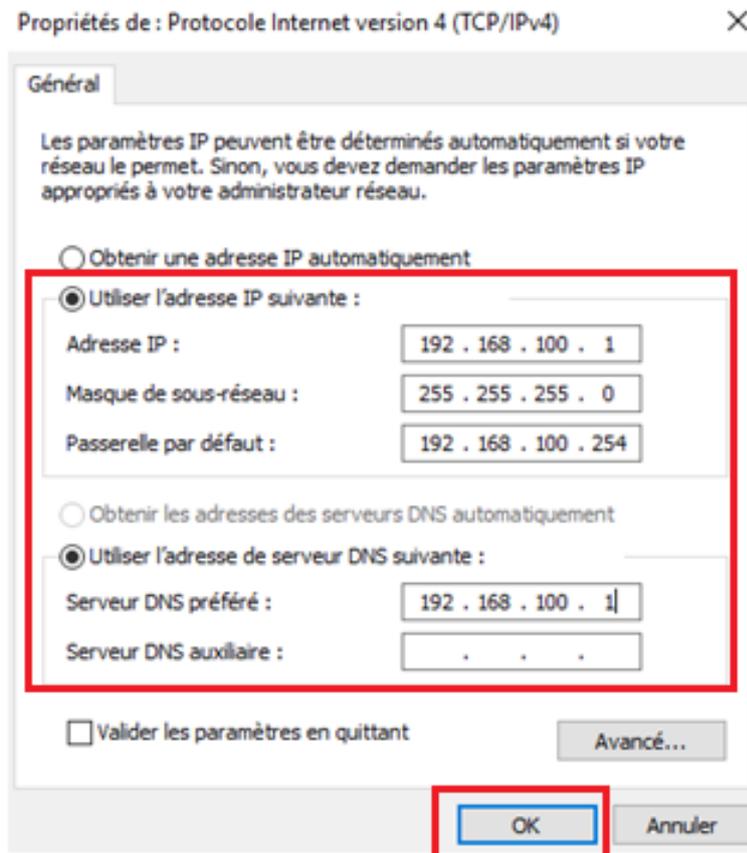
Sélectionnez ensuite l'interface correspondant à l'équipe d'association, faites un clic droit dessus, puis cliquez sur **Propriétés**.



Cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur le bouton **Propriétés**.



Configurez ensuite l'adresse IP en vous référant au plan d'adressage défini pour le projet (par exemple, 192.168.100.1/24 pour le serveur principal de Strasbourg). Cliquez sur **OK** pour valider la configuration.



Vérifiez la configuration IP en exécutant la commande `ipconfig` depuis l'invite de commande ou PowerShell.

```
PS C:\Users\Administrateur> ipconfig

Configuration IP de Windows

Carte Ethernet LAN :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::a535:90ec:c69a:a21%19
    Adresse IPv4. . . . . : 192.168.100.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.100.254
```

Sous PowerShell

Comme pour la configuration du NIC Teaming, il est nécessaire de récupérer des informations sur l'interface à configurer, en l'occurrence l'interface LAN du serveur Windows. Pour cela, la commande à utiliser sous PowerShell est : **Get-NetAdapter**.

Cette méthode sera notamment utilisée pour la configuration réseau des serveurs Windows Core.

Les captures d'écran en ligne de commande présentées ci-dessous correspondent à la configuration du serveur **STG-SRVW02** (serveur Core de Strasbourg).

```
PS C:\Users\Administrateur> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet0	Intel(R) 82574L Gigabit Network Co...#2	7	Up	00-0C-29-84-6F-A5	1 Gbps
LAN	Microsoft Network Adapter Multiplexo..	10	Up	00-0C-29-84-6E-AF	2 Gbps
Ethernet1	Intel(R) 82574L Gigabit Network Conn...	5	Up	00-0C-29-84-6E-AF	1 Gbps

Récupérez ensuite l'index de l'interface à configurer, puis saisissez la commande suivante :

```
PS C:\Users\Administrateur> New-NetIPAddress -InterfaceIndex 10 -IPAddress 192.168.100.2 -PrefixLength 24 -DefaultGateway 192.168.100.254
```

```
New-NetIPAddress -InterfaceIndex 11 -IPAddress 192.168.100.2 -PrefixLength 24 -DefaultGateway 192.168.100.254
```

InterfaceIndex : numéro d'index de l'interface à configurer

IPAddress : adresse IP que l'on souhaite attribuer

PrefixLength : longueur du préfixe du masque de sous-réseau (notation CIDR)

DefaultGateway : adresse de la passerelle par défaut du réseau

Les étapes de configuration du NIC Teaming et de l'adressage IP ont également été appliquées sur les serveurs du site de Mulhouse, de manière identique à celles décrites précédemment pour Strasbourg, en adaptant uniquement les adresses IP et la passerelle réseau.

Utilisation de sconfig pour la configuration des serveurs

Sconfig est un outil intégré à Windows Server permettant d'effectuer diverses configurations de manière interactive sur les serveurs en version Core.

Il permet notamment de renommer l'ordinateur, configurer le réseau, activer le Bureau à distance, rejoindre un domaine, et bien plus.

Pour l'exécuter, il suffit de taper sconfig dans l'invite de commande ou dans PowerShell.

```
=====
Configuration du serveur
=====
1) Domaine ou groupe de travail :      Groupe de travail:  WORKGROUP
2) Nom d'ordinateur :                  STG-SRVW02
3) Ajouter l'administrateur local
4) Configurer l'administration à distance  Activé
5) Paramètres de Windows Update :      DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                 Désactivé

8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie           Inconnu
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

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

Il suffit ensuite de sélectionner le numéro correspondant à l'action souhaitée.

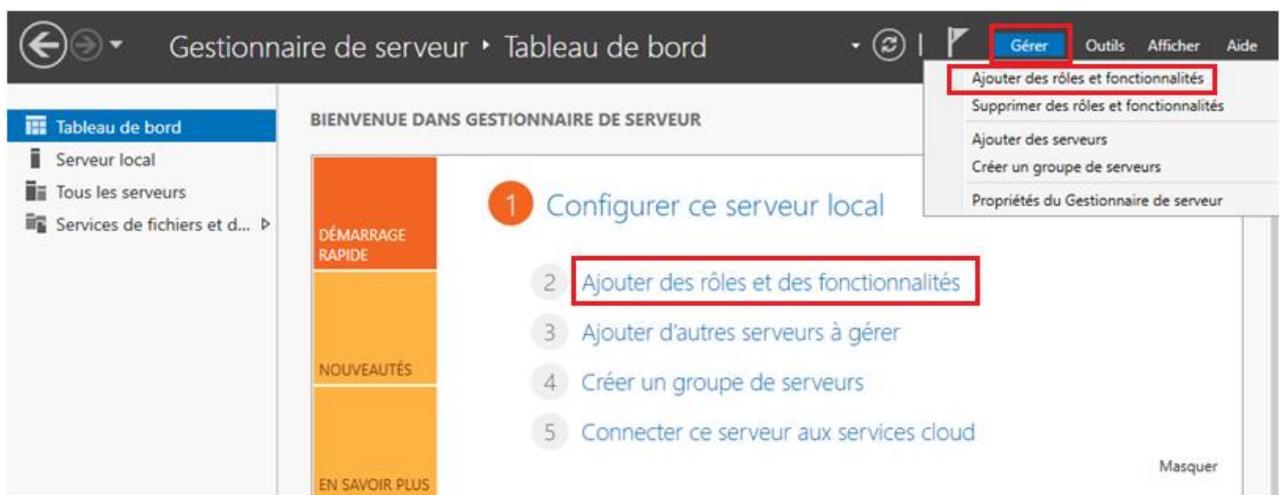
L'utilisation de cet outil est fortement recommandée pour réaliser rapidement les principales configurations système.

Une fois les paramètres de base appliqués, nous pouvons désormais passer à l'installation des rôles et services, en commençant par **Active Directory**, afin d'assurer la **redondance** et la **haute disponibilité** du domaine.

3.1.4) Déploiement d'Active Directory

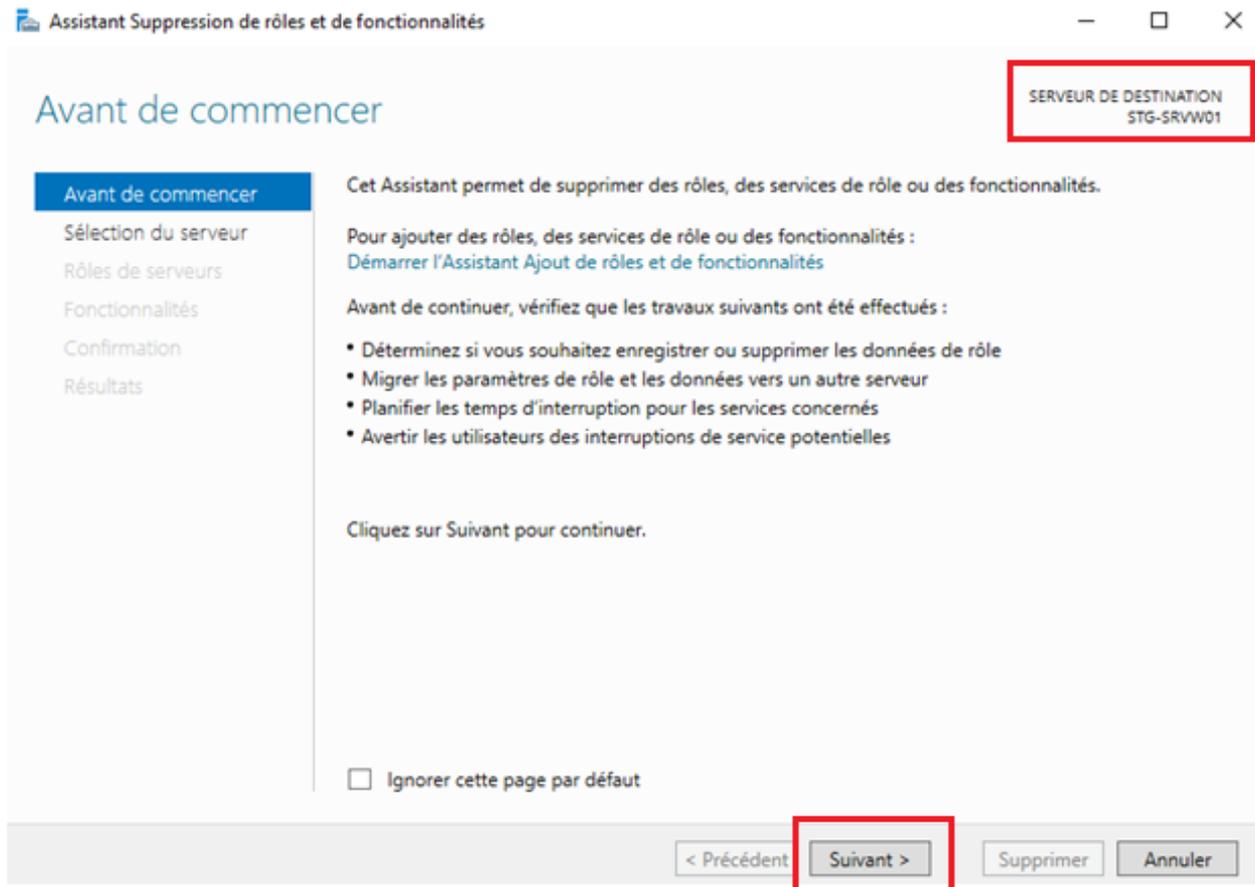
Installation en mode graphique

Pour installer le service d'annuaire Active Directory, il nous faut aller sur le **Gestionnaire de Serveur**, cliquer sur **Gérer**, et puis **Ajouter des rôles et des fonctionnalités**. Vous pouvez également cliquer directement sur **Ajouter des rôles et des fonctionnalités** présents sur le Tableau de bord.

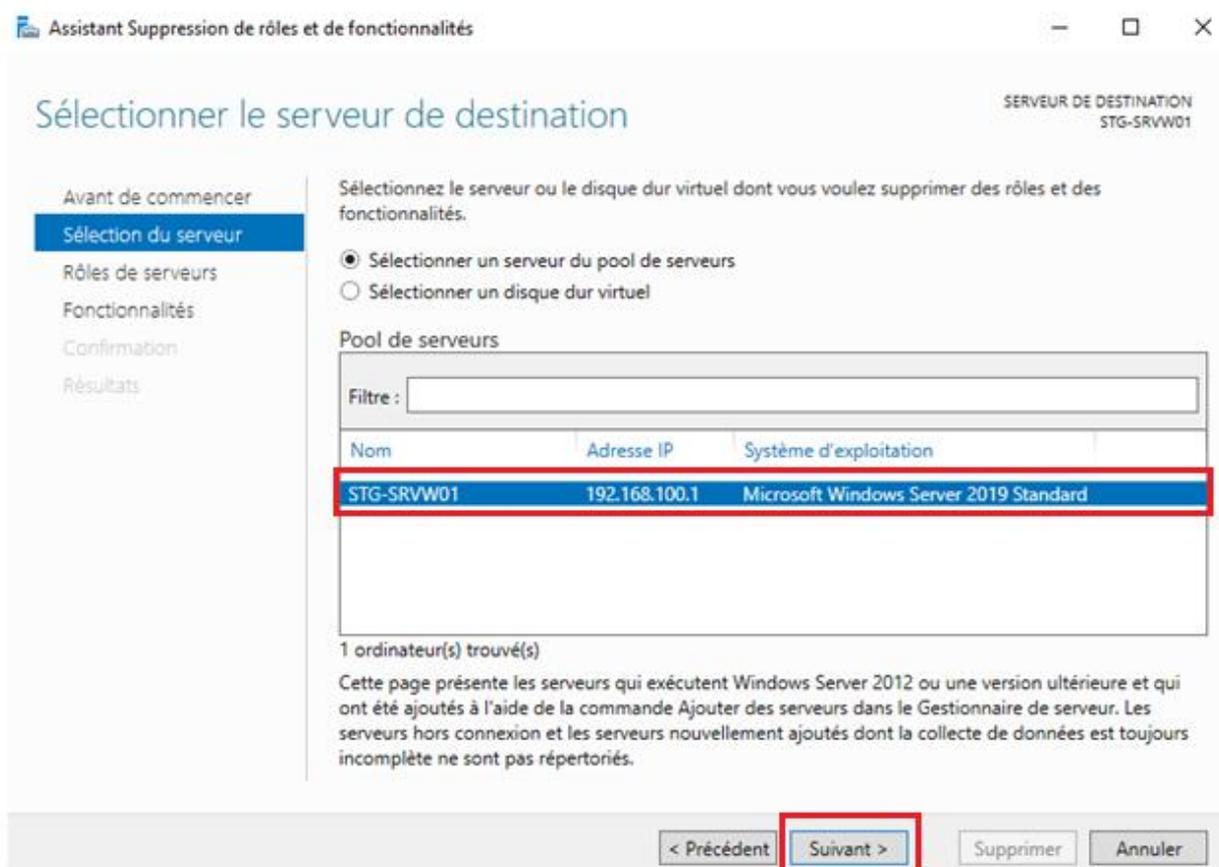


Une fenêtre s'affiche pour sélectionner le **serveur de destination** de l'installation (dans notre cas, STG-SRVW01).

Cliquez ensuite sur **Suivant** jusqu'à atteindre l'étape de sélection du rôle à installer.



À mesure que d'autres serveurs seront intégrés au domaine, il est essentiel de bien sélectionner le serveur concerné lors de l'installation des rôles. Une convention de nommage claire et cohérente en amont facilite cette identification. Dans notre cas, pour cette première installation, seul le **serveur principal de Strasbourg (STG-SRVW01)** est disponible.



Assistant Suppression de rôles et de fonctionnalités

SÉLECTIONNER LE SERVEUR DE DESTINATION
STG-SRVW01

Avant de commencer
Sélection du serveur
 Rôles de serveurs
 Fonctionnalités
 Confirmation
 Résultats

Sélectionnez le serveur ou le disque dur virtuel dont vous voulez supprimer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

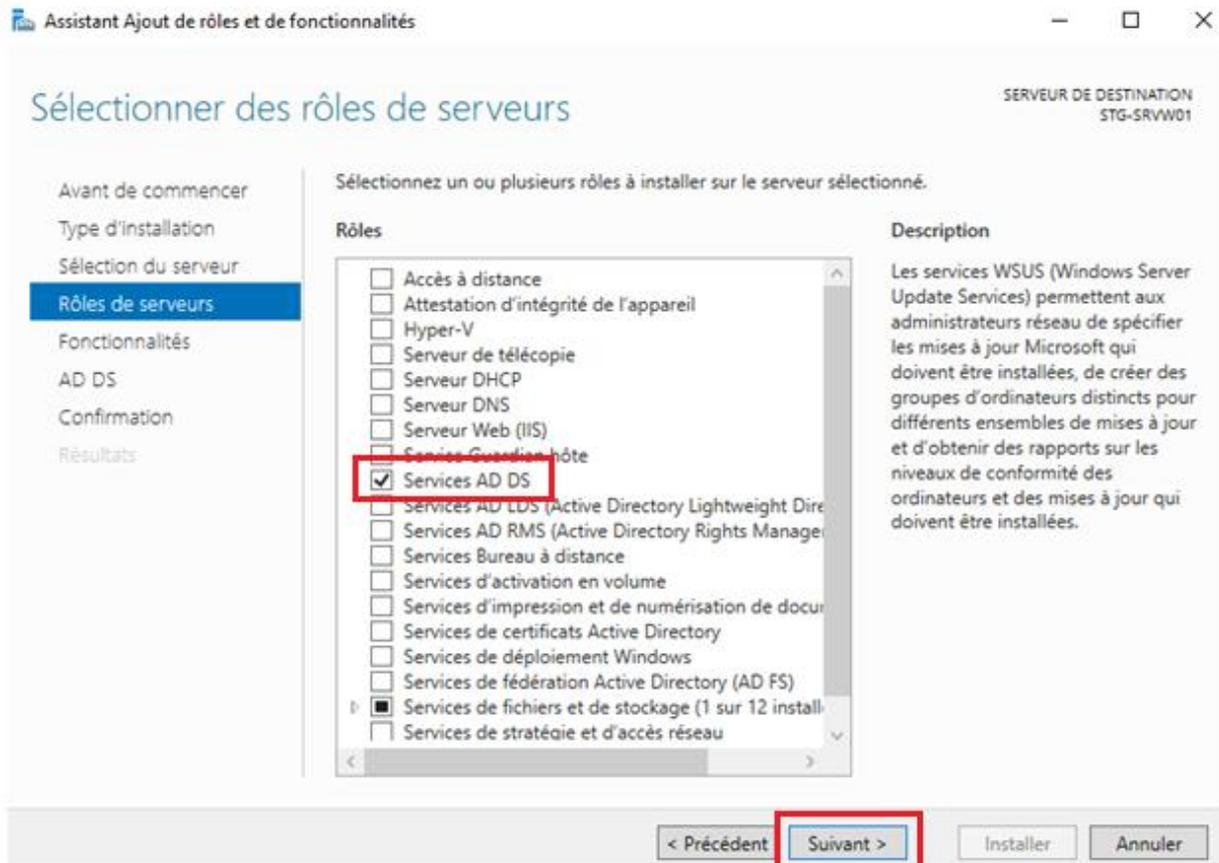
Nom	Adresse IP	Système d'exploitation
STG-SRVW01	192.168.100.1	Microsoft Windows Server 2019 Standard

1 ordinateur(s) trouvé(s)

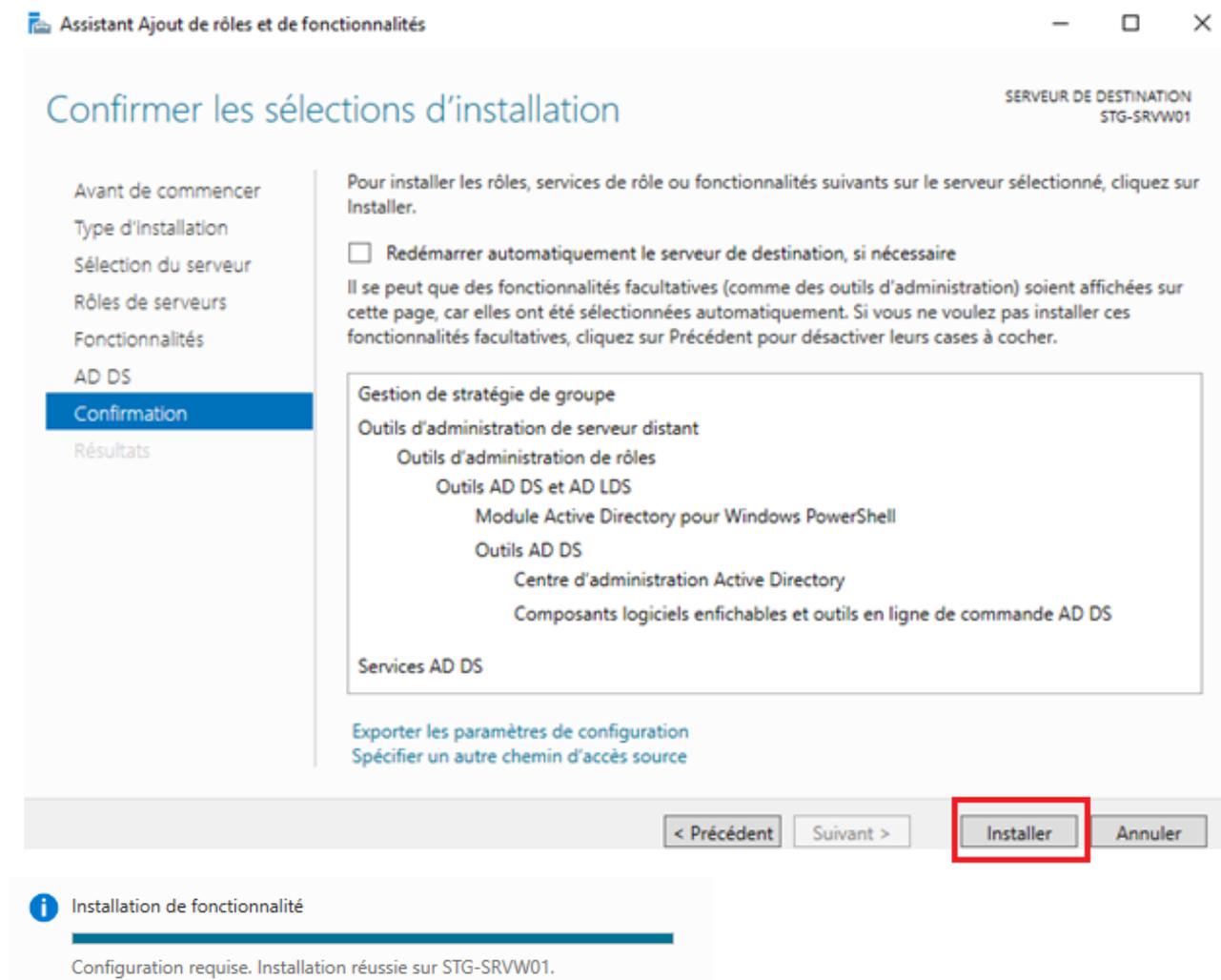
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Supprimer Annuler

Sélectionnez ensuite **Services AD DS** afin d'installer les **Services de domaine Active Directory**.



Cliquez sur **Suivant** jusqu'à l'étape finale, puis sur **Installer** pour lancer l'installation du rôle **Active Directory Domain Services**.



Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
STG-SRVW01

Confirmer les sélections d'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

- Gestion de stratégie de groupe
- Outils d'administration de serveur distant
 - Outils d'administration de rôles
 - Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - Outils AD DS
 - Centre d'administration Active Directory
 - Composants logiciels enfichables et outils en ligne de commande AD DS
- Services AD DS

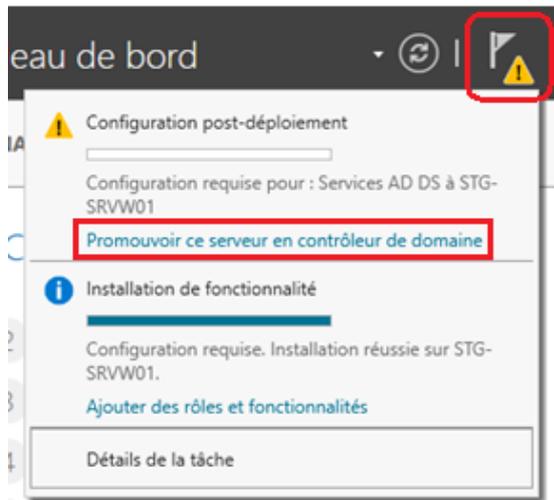
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > **Installer** Annuler

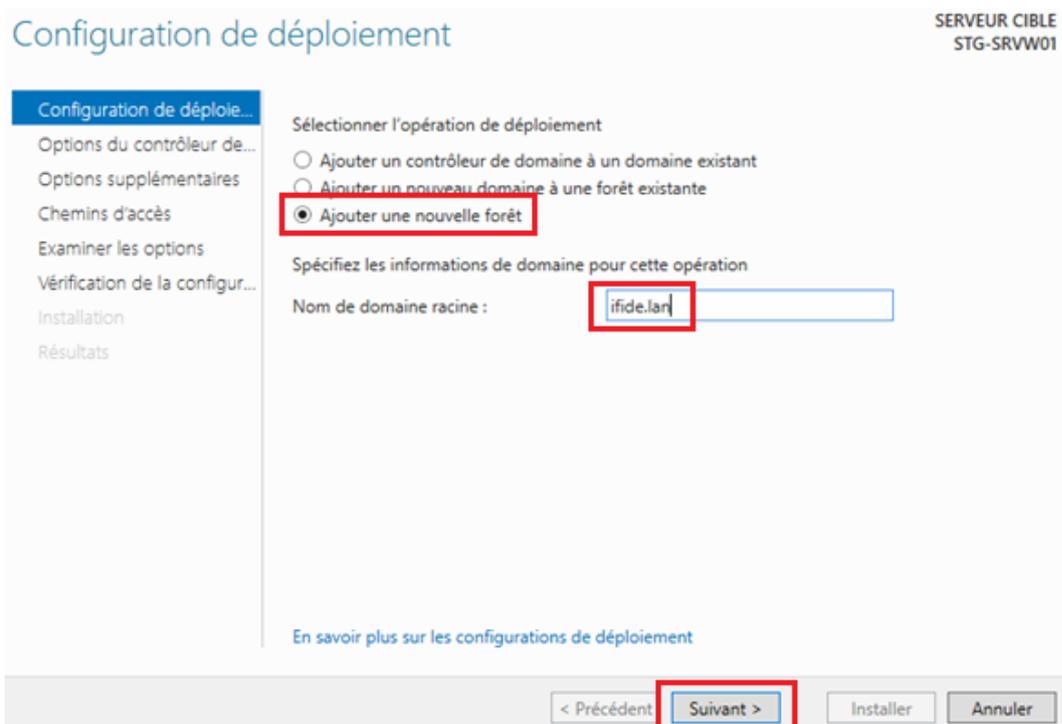
i Installation de fonctionnalité
Configuration requise. Installation réussie sur STG-SRVW01.

Promotion du serveur en contrôleur de domaine

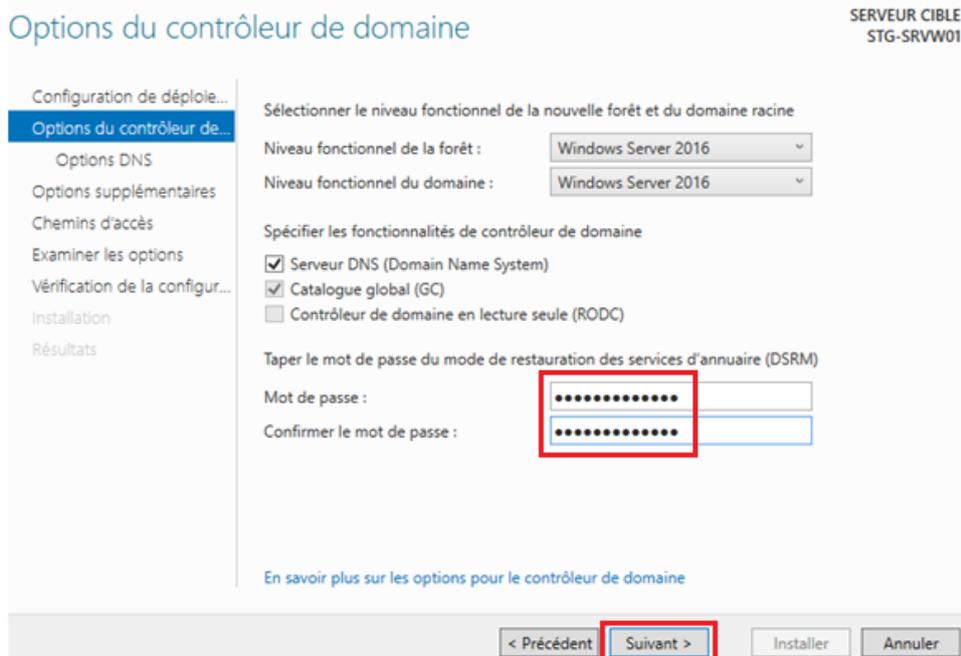
Pour promouvoir un serveur en tant que contrôleur de domaine, ouvrez le **Gestionnaire de serveur**, cliquez sur l'**icône d'avertissement** en haut à droite (panneau jaune avec un drapeau), puis sélectionnez **"Promouvoir ce serveur en contrôleur de domaine"**.



Sélectionnez **"Ajouter une nouvelle forêt"**, puis renseignez le nom de domaine défini pour ce projet, ici : **ifide.lan**.



À cette étape, laissez les niveaux fonctionnels par défaut (Windows Server 2016), conservez les options **Serveur DNS** et **Catalogue global** cochées, puis définissez un **mot de passe pour le mode de restauration des services d'annuaire (DSRM)**. Cliquez ensuite sur **Suivant**.



Options du contrôleur de domaine

SERVEUR CIBLE
STG-SRVW01

Configuration de déploiement...
Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la configuration...
 Installation
 Résultats

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

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)

Catalogue global (GC)

Contrôleur de domaine en lecture seule (RODC)

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

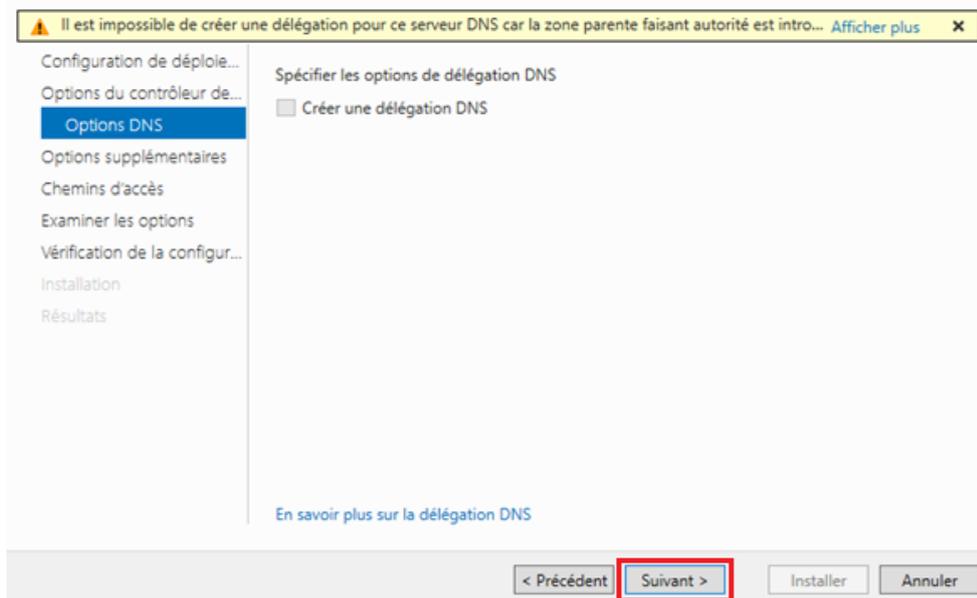
Mot de passe : [masked]

Confirmer le mot de passe : [masked]

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

< Précédent **Suivant >** Installer Annuler

Cette étape affiche un message informatif indiquant qu'aucune délégation DNS ne peut être créée, ce qui est normal dans le cadre d'une nouvelle forêt locale.



Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#) X

Configuration de déploiement...
 Options du contrôleur de...
Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la configuration...
 Installation
 Résultats

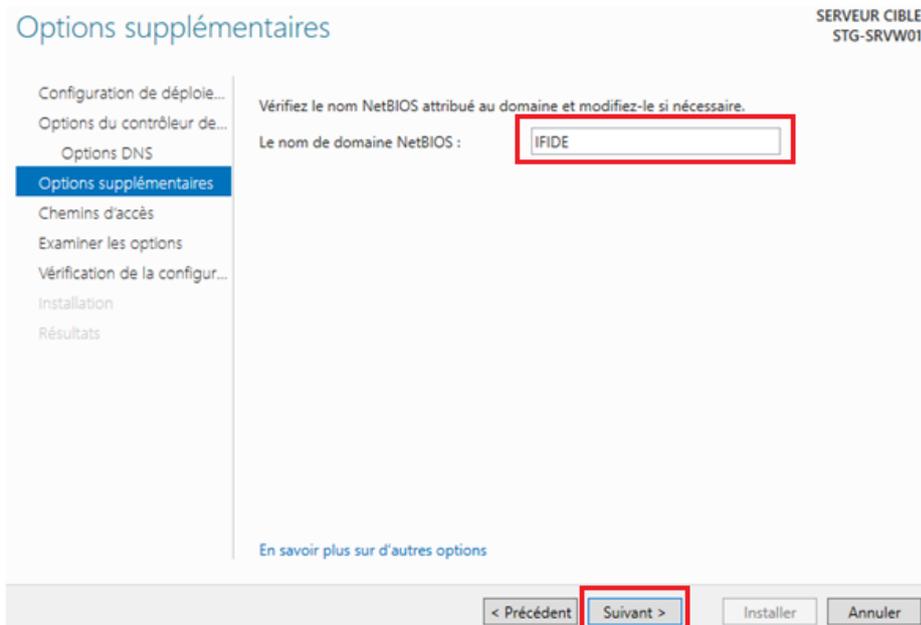
Spécifier les options de délégation DNS

Créer une délégation DNS

[En savoir plus sur la délégation DNS](#)

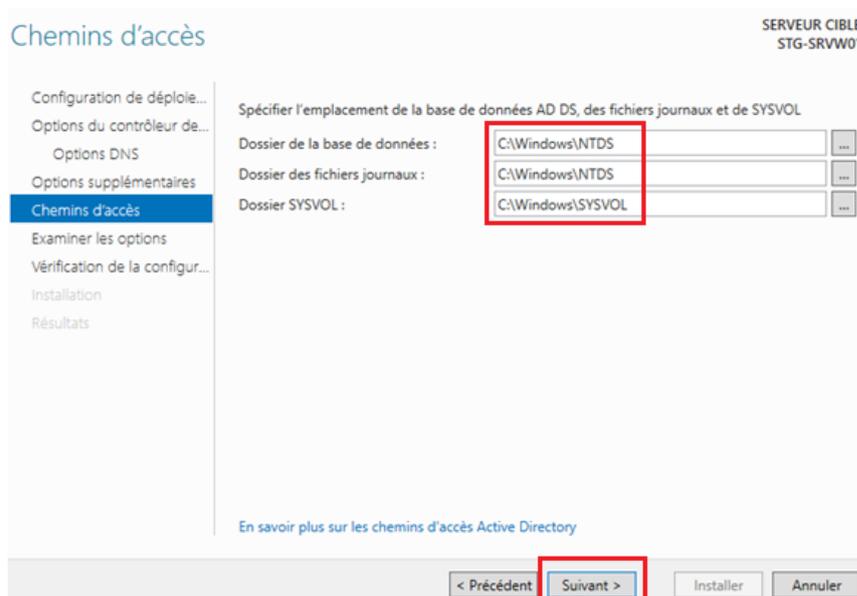
< Précédent **Suivant >** Installer Annuler

À cette étape, vous pouvez vérifier et éventuellement modifier le **nom NetBIOS** attribué au domaine.

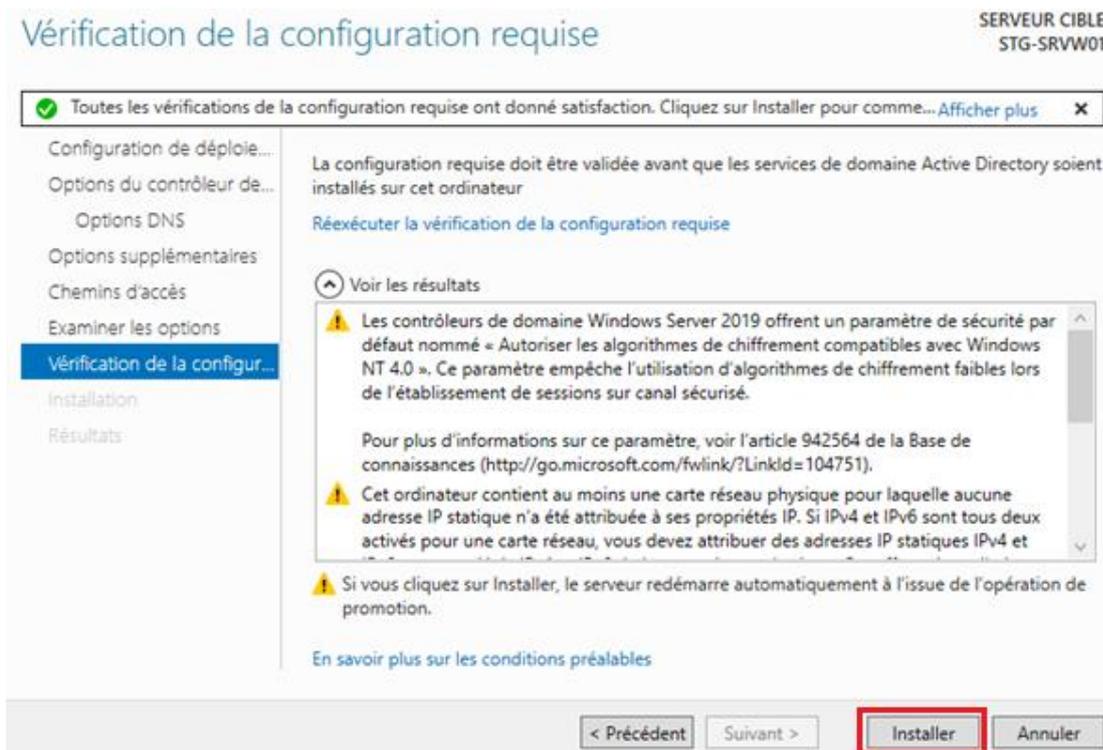


Les chemins d'accès par défaut, indiqués sur la fenêtre suivante, représentent les emplacements des dossiers suivants :

- **Base de données Active Directory**
- **Fichiers journaux**
- **Dossier SYSVOL** (répertoire système spécial des contrôleurs de domaine)



Enfin, cliquez sur **Installer** et attendez la fin de la promotion. À la fin de l'installation, il est impératif de **redémarrer le serveur** pour appliquer les modifications et se connecter au domaine **IFIDE.LAN**.



Après le redémarrage du serveur, l'écran de connexion affichera le **nom NetBIOS du domaine** et le compte **Administrateur**. Par défaut, le mot de passe de l'administrateur du domaine est identique à celui de l'administrateur local du serveur.



Le rôle Active Directory étant désormais installé, nous allons passer à la mise en place du cluster du domaine Active Directory entre les sites de Strasbourg et Mulhouse, en assurant la redondance et la réplication entre les deux contrôleurs de domaine.

3.1.5) Installation du cluster Active Directory

Avant d'installer le cluster, les prérequis suivants doivent être réalisés sur les serveurs de Mulhouse :

- Renommer chaque serveur
- Mettre en place le NIC Teaming (association des cartes réseau)
- Configurer les paramètres réseau, en définissant une IP statique et en renseignant comme serveur DNS l'adresse IP du contrôleur de domaine de Strasbourg (192.168.100.1) pour permettre la jonction au domaine.

Configuration du DNS sur les serveurs Windows

Avant de rejoindre le domaine, il est nécessaire de s'assurer que le nom de l'ordinateur, l'association des cartes réseau (NIC Teaming) ainsi que l'adressage IP statique ont bien été configurés.

Afin de permettre la jonction au domaine, le **serveur DNS** utilisé par les serveurs de Mulhouse doit pointer vers le **contrôleur de domaine principal situé à Strasbourg** (192.168.100.1).

Cette configuration peut être réalisée :

Via l'**interface graphique** (Panneau de configuration > Connexions réseau) pour les serveurs avec GUI,

En **PowerShell** après avoir identifié l'interface réseau avec Get-NetAdapter,

Ou plus simplement via l'outil **sconfig**, en choisissant l'option 8 (Paramètres réseau), puis 2 (Configurer le DNS).

MUL-SRVW01

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

Valider les paramètres en quittant

Avancé...

OK Annuler

MUL-SRVW02

```

=====
Configuration du serveur
=====
1) Domaine ou groupe de travail :           Groupe de travail: WORKGROUP
2) Nom d'ordinateur :                       MUL-SRVW02
3) Ajouter l'administrateur local
4) Configurer l'administration à distance   Activé
5) Paramètres de Windows Update :           DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                       Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie                 Inconnu
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option 8
  
```

Cela affichera ensuite la ou les cartes réseau disponibles sur le serveur. Il suffira alors de saisir le numéro correspondant à l'interface à configurer.

```

Cartes réseau disponibles

Index#  Adresse IP      Description
3       192.168.200.2      Microsoft Network Adapter Multiplexor Driver
Sélectionner Index# de la carte réseau (Vide=Annuler) :
  
```

Ensuite, appuyez sur 2 pour configurer les **serveurs DNS** associés à cette interface.

```

-----
Paramètres de carte réseau
-----

Index NIC          3
Description        Microsoft Network Adapter Multiplexor Driver
Adresse IP         192.168.200.2   fe80::40c9:5c56:cb14:c4a2
Masque de sous-réseau 255.255.255.0
DHCP activé        Faux
Passerelle par défaut 192.168.200.254
Serveur DNS préféré
Serveur DNS auxiliaire

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

Sélectionner une option : 2
  
```

Indiquez ensuite l'adresse IP du **serveur principal de Strasbourg** (192.168.100.1) comme **serveur DNS** afin de permettre la jonction au domaine.

```

Serveur DNS auxiliaire

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

Sélectionner une option : 2
Serveurs DNS

Entrer un nouveau serveur DNS préféré (Vide = Annuler) : 192.168.100.1
  
```

Adresse IP Serveur principal Strasbourg

Le DNS a bien été configuré.

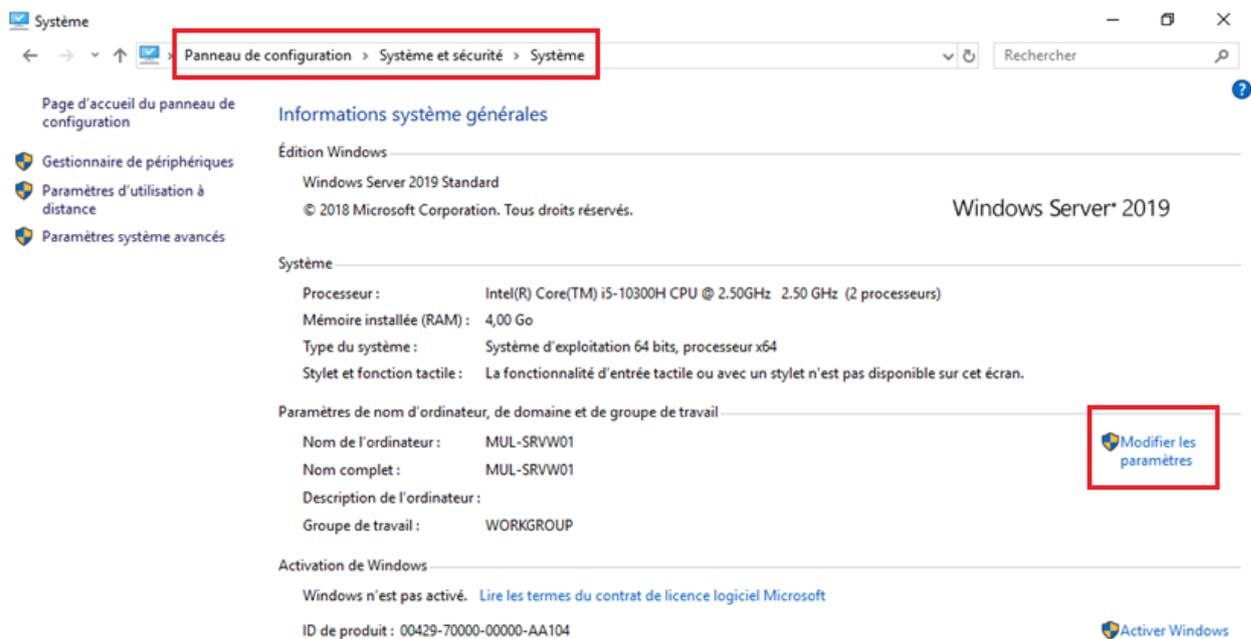
Joindre les serveurs dans le domaine

Les serveurs DNS étant désormais configurés sur chaque machine, nous pouvons procéder à la jonction au domaine Active Directory.

Nous allons détailler ici la méthode graphique pour les serveurs avec interface GUI, ainsi que la méthode en ligne de commande via sconfig pour les serveurs en Core.

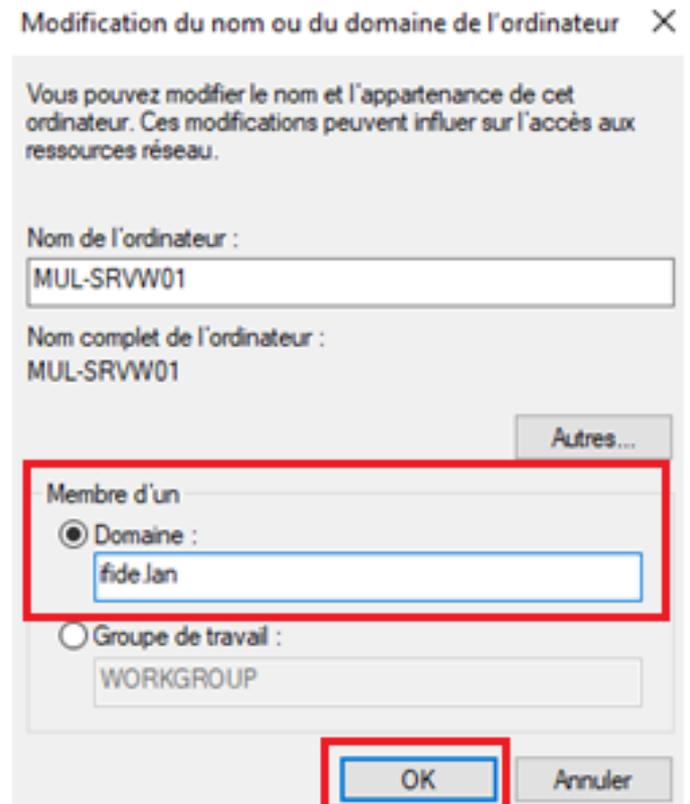
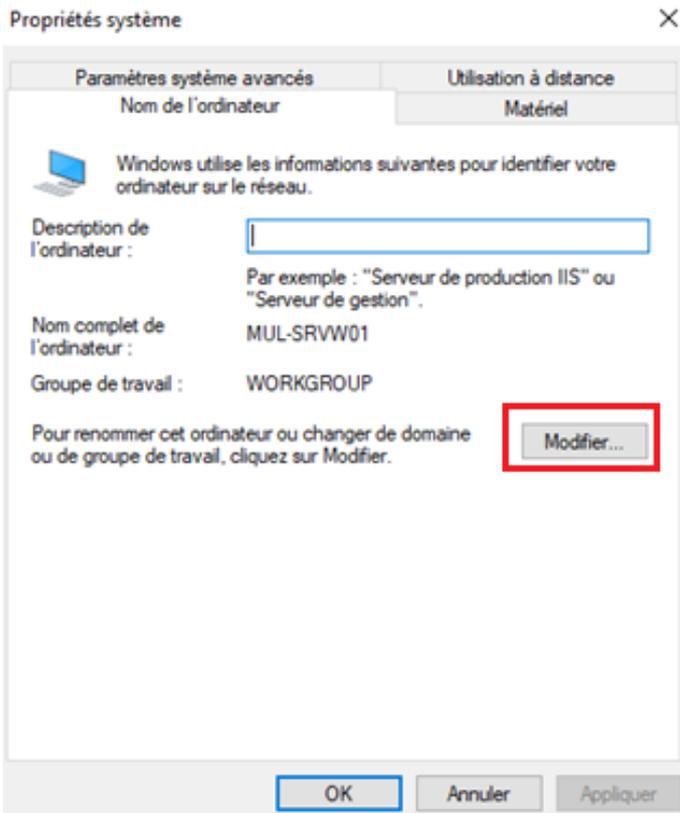
Joindre le domaine en GUI

En mode graphique, ouvrez le **Panneau de configuration**, puis **Système et sécurité > Système**, et cliquez sur **Modifier les paramètres**.

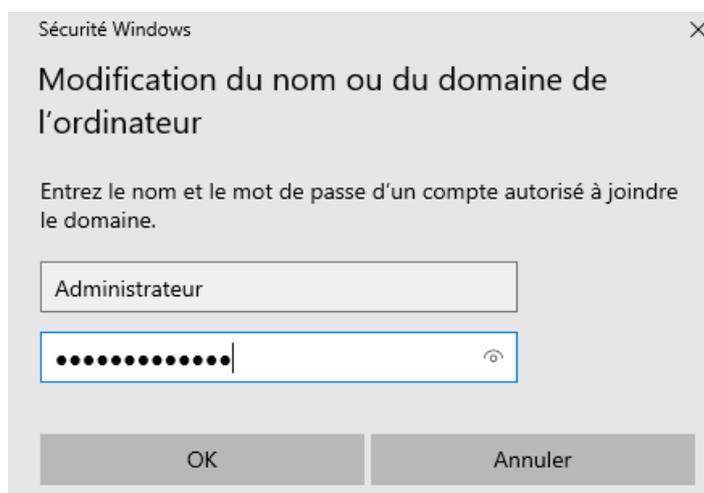


Une fenêtre s'ouvrira : cliquez sur **Modifier...** pour changer le nom de l'ordinateur et le joindre à un domaine.

Saisissez le nom de domaine **ifide.lan** puis cliquez sur **OK**.



Une fenêtre d'authentification apparaîtra : saisissez les identifiants du compte Administrateur du domaine **ifide.lan**.



Une fois la jonction confirmée, un redémarrage du serveur est nécessaire.

Modification du nom ou du domaine de l'ordinateur ✕

 Bienvenue dans le domaine ifide.lan.

OK

Nous allons maintenant voir la **jonction au domaine via PowerShell** pour les **serveurs Core**, puis la **gestion centralisée des serveurs** depuis la console graphique du serveur principal, notamment pour l'installation des rôles et la mise en place de la **redondance Active Directory**.

Joindre le domaine par PowerShell

Sous PowerShell, la jonction à un domaine peut se faire en une seule commande, ce qui en fait une méthode rapide et efficace.

L'outil **sconfig** permet également cette opération.

Pour rappel, voici la commande à exécuter sur la machine à joindre au domaine :

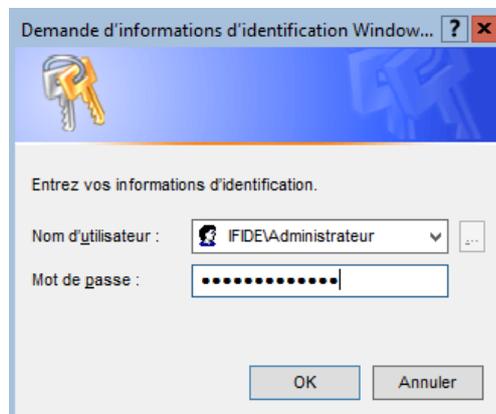
```
Add-Computer -DomainName "ifide.lan" -Credential(Get-Credential "IFIDE\Administrateur")
```

Add-Computer -DomainName «ifide.lan» -Credential(Get-Credential «IFIDE\Administrateur»)

Credential : correspond aux identifiants d'un utilisateur du domaine.

L'utilisation de Get-Credential permet de saisir les informations de connexion du compte **IFIDE\Administrateur**.

Une fenêtre d'authentification apparaîtra (même sur un serveur Core) pour entrer le mot de passe associé.



Il suffit ensuite de **redémarrer les serveurs**, puis de **gérer l'ensemble des serveurs depuis le serveur principal** situé à Strasbourg.

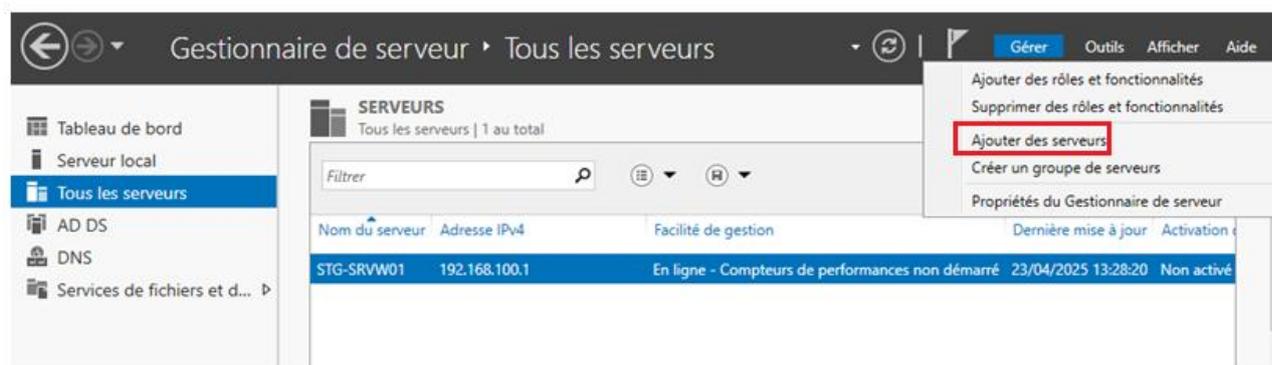
Installation des redondances du domaine Active Directory

Maintenant que les serveurs ont rejoint le domaine, ils peuvent être administrés directement depuis la console du Gestionnaire de serveurs.

Nous allons donc procéder à l'installation des rôles et services Active Directory sur les serveurs de Mulhouse (**MUL-SRVW01 et MUL-SRVW02**), afin d'assurer la haute disponibilité du domaine et de répondre aux exigences du client.

Ajout des serveurs dans le Gestionnaire de serveur

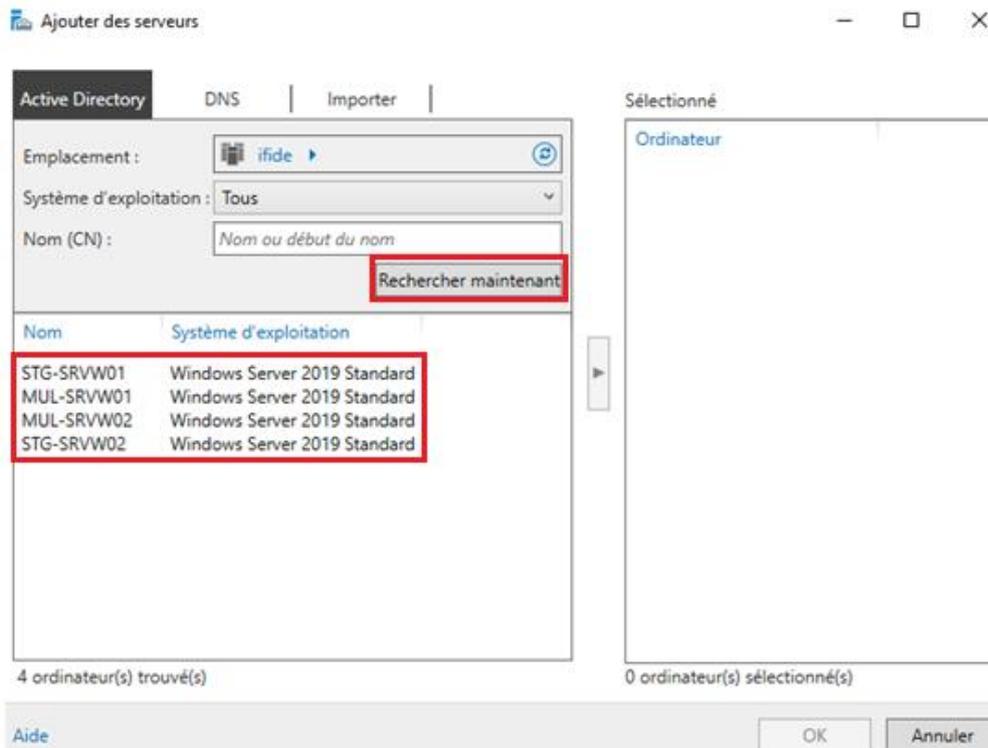
Sur **STG-SRVW01**, le serveur principal de Strasbourg et du domaine, ouvrez le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des serveurs**.



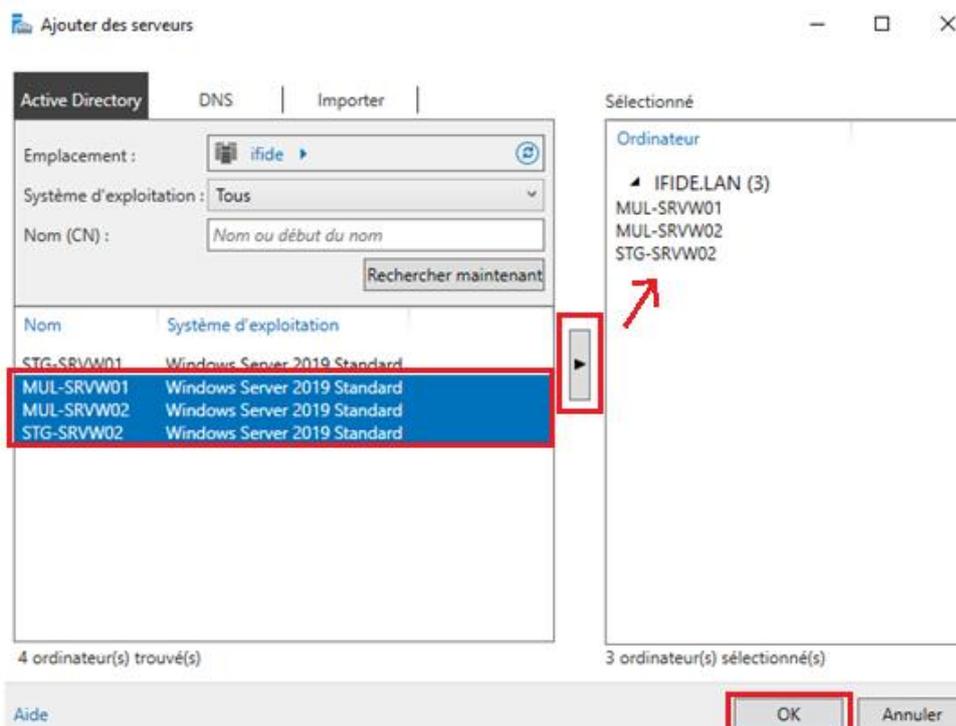
Une fenêtre apparaîtra : vous pouvez saisir le nom de chaque serveur, puis cliquer sur **Rechercher**, ou simplement cliquer sur **Rechercher maintenant** pour afficher tous les serveurs disponibles.

⚠ Attention : il est recommandé de saisir quelques caractères du nom de la machine afin de filtrer les résultats, sinon la recherche affichera **tous les ordinateurs du domaine**.

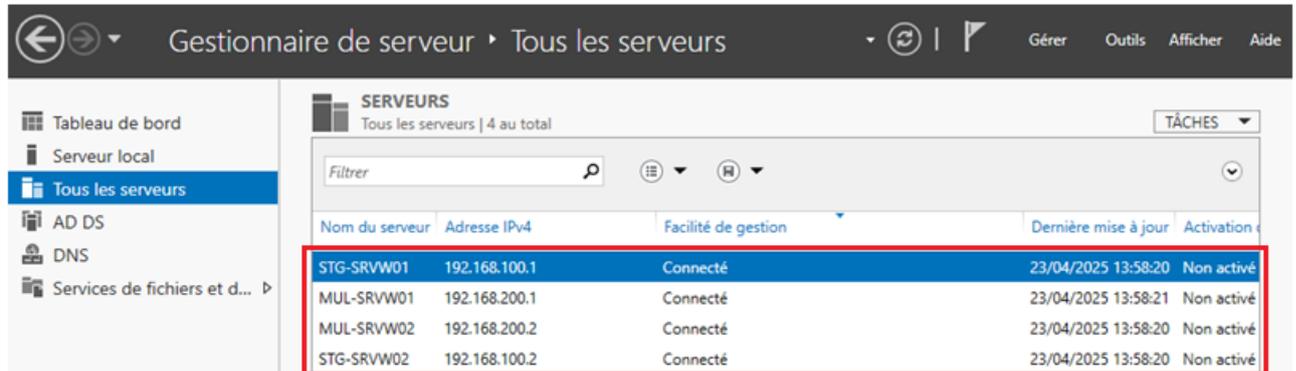
Dans notre cas, cela ne pose pas de problème puisque seuls les **quatre serveurs** sont présents dans l'environnement.



Sélectionnez ensuite les serveurs à ajouter (STG-SRVW02, MUL-SRVW01 et MUL-SRVW02), cliquez sur la flèche vers la droite, puis validez l'ajout.



Lors de l'actualisation, nous pouvons ainsi voir que les serveurs ont été ajoutés, et procéder à l'installation de l'Active Directory et des contrôleurs de domaine dans la même forêt, pour mettre en place le cluster de l'Active Directory.



Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation
STG-SRVW01	192.168.100.1	Connecté	23/04/2025 13:58:20	Non activé
MUL-SRVW01	192.168.200.1	Connecté	23/04/2025 13:58:21	Non activé
MUL-SRVW02	192.168.200.2	Connecté	23/04/2025 13:58:20	Non activé
STG-SRVW02	192.168.100.2	Connecté	23/04/2025 13:58:20	Non activé

À présent, nous allons passer à l'installation de l'Active Directory sur les serveurs à partir du **Gestionnaire de serveur**.

Ajout du rôle Active Directory et promotion en tant que contrôleur de domaine

Pour installer les contrôleurs de domaine sur le site de Mulhouse, nous allons ajouter le rôle **Active Directory** en cliquant sur **Gérer → Ajouter des rôles et fonctionnalités**, comme cela a été fait pour le serveur principal.

Cependant, à l'étape de sélection du serveur, il est nécessaire de choisir sur **quel serveur** le ou les rôles seront installés.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
MUL-SRVW01.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
MUL-SRVW01.ifide.lan	192.168.200.1	Microsoft Windows Server 2019 Standard
STG-SRVW02.ifide.lan	192.168.100.2	Microsoft Windows Server 2019 Standard
STG-SRVW01.ifide.lan	192.168.100.1	Microsoft Windows Server 2019 Standard
MUL-SRVW02.ifide.lan	192.168.200.2	Microsoft Windows Server 2019 Standard

4 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

Ensuite, la suite de l'installation du service reste identique à celle réalisée précédemment. La différence se situe au niveau de la **promotion du serveur en contrôleur de domaine**, où il faudra cette fois **joindre la forêt existante : ifide.lan**.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
MUL-SRVW01.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Hyper-V
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS**
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (1 sur 12 installés)
- Services de stratégie et d'accès réseau

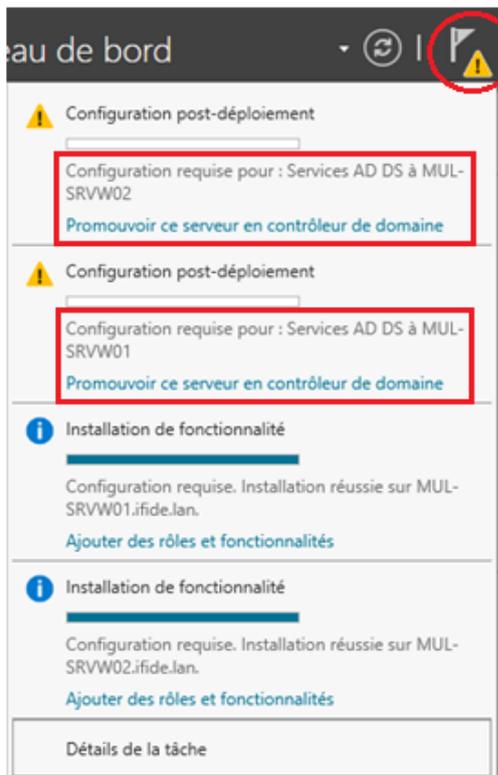
Description

Les services WSUS (Windows Server Update Services) permettent aux administrateurs réseau de spécifier les mises à jour Microsoft qui doivent être installées, de créer des groupes d'ordinateurs distincts pour différents ensembles de mises à jour et d'obtenir des rapports sur les niveaux de conformité des ordinateurs et des mises à jour qui doivent être installées.

< Précédent **Suivant >** Installer Annuler

Promotion des serveurs en tant que contrôleurs de domaine

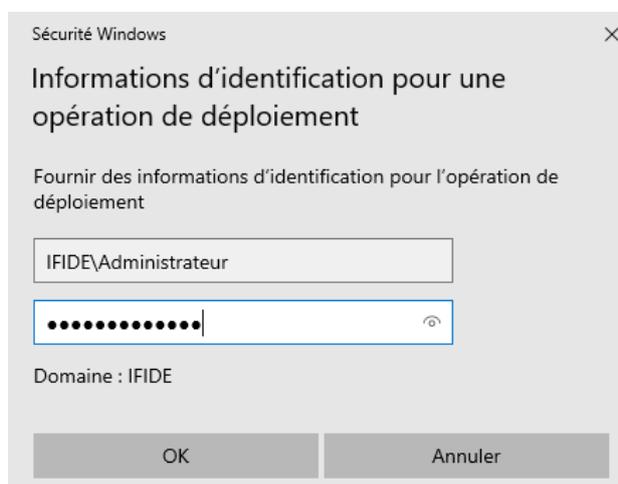
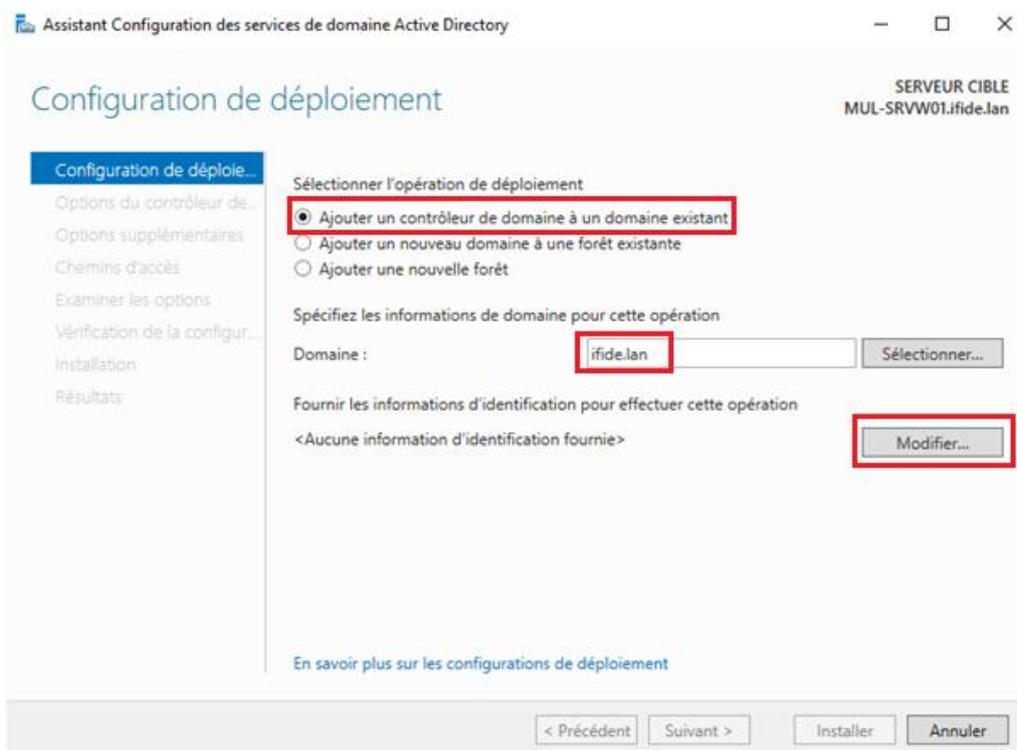
Maintenant que le rôle est installé, un message s'affiche dans le **Gestionnaire de serveur**, nous invitant à promouvoir le serveur en tant que contrôleur de domaine.



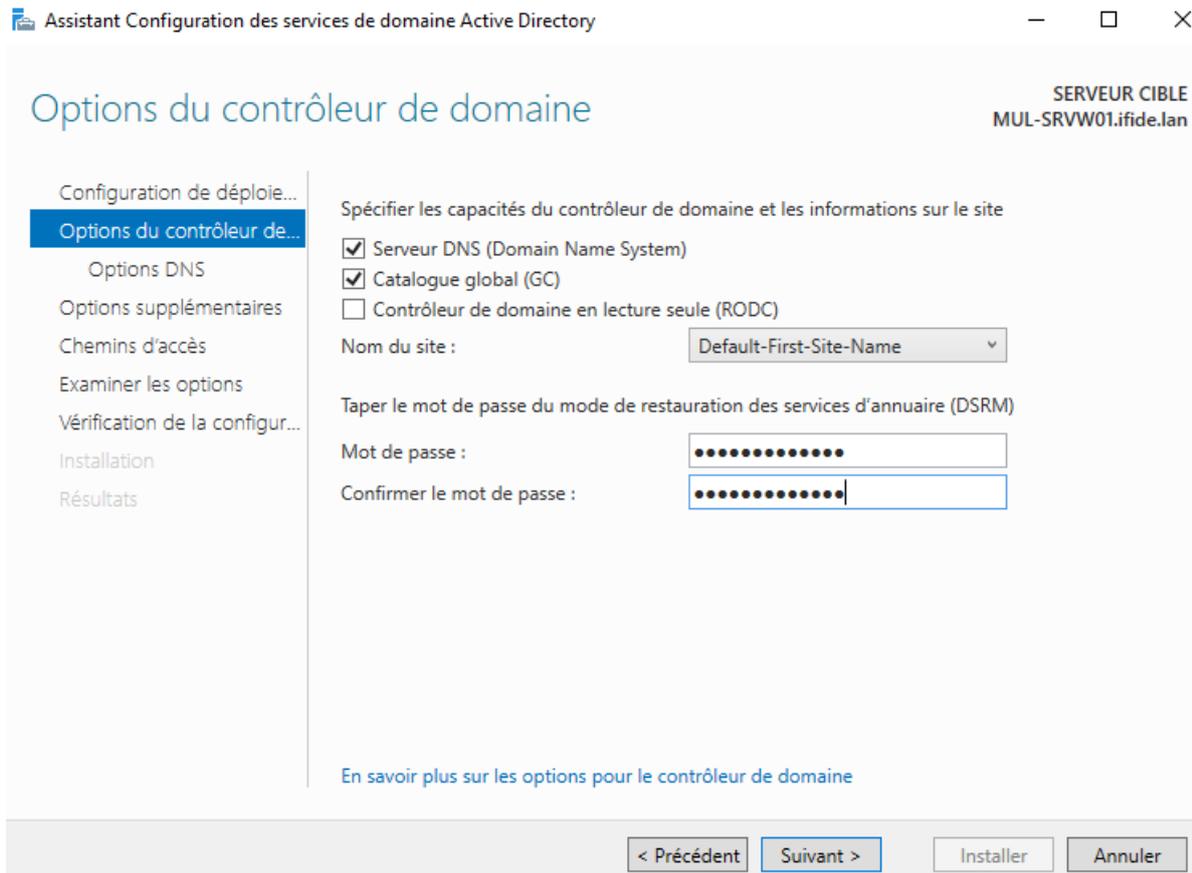
Cependant, il est préférable de procéder à la **promotion des contrôleurs de domaine un par un**, afin d'éviter d'éventuels conflits de configuration au sein du domaine.

Ensuite, dans la fenêtre **Configuration du déploiement**, cochez "**Ajouter un contrôleur de domaine à un domaine existant**", afin d'ajouter les serveurs en tant que secondaires. Cela permettra la **synchronisation**, la **redondance** et la **haute disponibilité** du domaine entre les sites de **Strasbourg** et **Mulhouse**.

Cliquez sur **Modifier**, puis saisissez les identifiants de l'administrateur du domaine en précisant le domaine dans l'identifiant : **IFIDE\Administrateur**.



Saisissez ensuite le **mot de passe de récupération** du domaine, utilisé en cas de **démarrage en mode sans échec**.



Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
MUL-SRVW01.ifide.lan

Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

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

Nom du site : Default-First-Site-Name

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

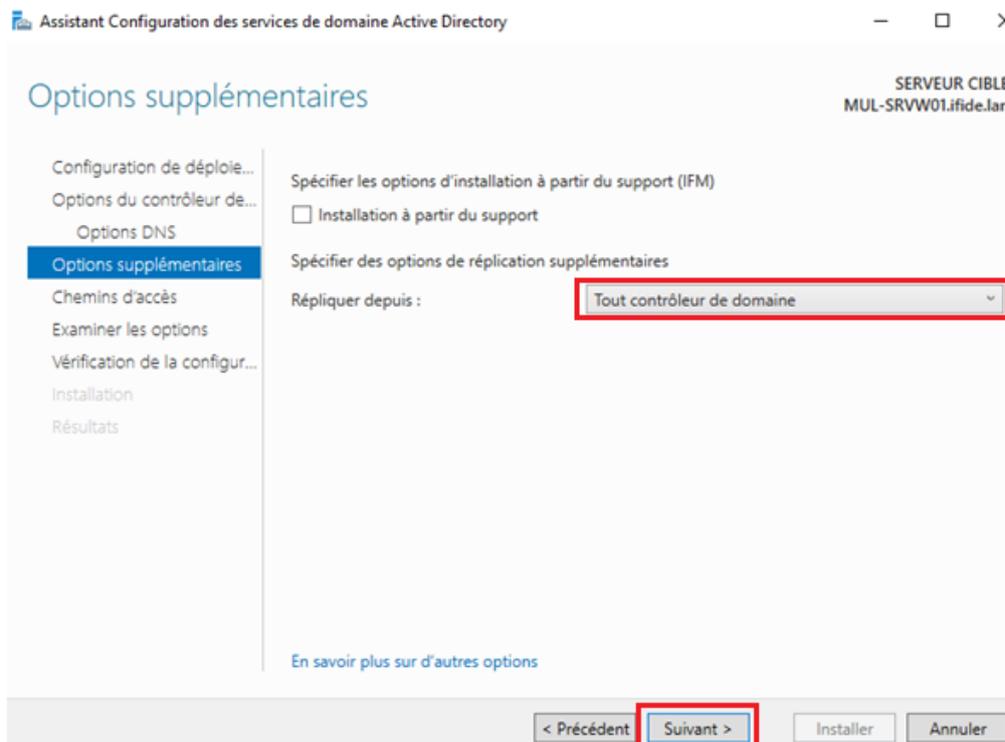
Mot de passe : [masqué]

Confirmer le mot de passe : [masqué]

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

< Précédent Suivant > Installer Annuler

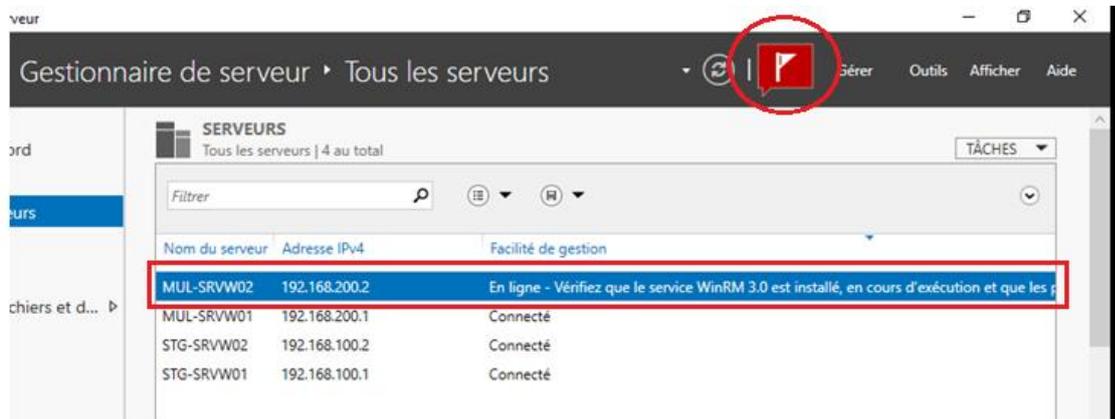
Ensuite, dans les **Options supplémentaires**, sélectionnez **"Tous les contrôleurs de domaine"** pour la **réplication**, afin que la base de données du domaine soit correctement synchronisée et répliquée.



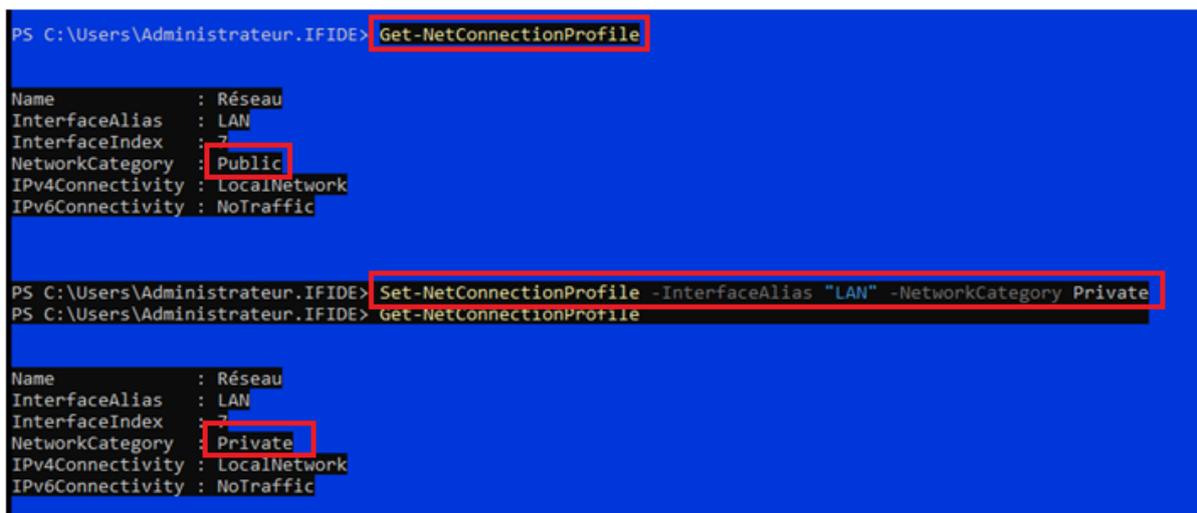
Enfin, lancez l'installation : le **serveur distant redémarrera automatiquement** après la promotion en tant que contrôleur de domaine.

N'oubliez pas de **promouvoir également les autres serveurs** prévus en tant que contrôleurs de domaine.

Un message d'avertissement s'affiche encore brièvement dans la colonne "Facilité de gestion" pour MUL-SRVW02, indiquant de vérifier que le service WinRM 3.0 est actif et que les ports de pare-feu sont ouverts.



Après avoir défini le profil réseau en "Privé" et activé manuellement les règles pare-feu liées à WinRM, WMI et DCOM, le serveur MUL-SRVW02 a pu être reconnu comme connecté par le Gestionnaire de serveur.



Le test **Test-WSMan MUL-SRVW02** a été exécuté depuis **STG-SRVW01**, confirmant que la communication **WinRM** fonctionne correctement entre les deux serveurs.

La réponse affichée valide que **le service est actif**, que **les ports sont ouverts**, et que le serveur distant est **accessible à distance** pour la gestion depuis le Gestionnaire de serveur.

```
PS C:\Users\Administrateur> Test-WSMan MUL-SRVW02

wsmid      : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor   : Microsoft Corporation
ProductVersion  : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

MUL-SRVW02	192.168.200.2	Connecté
MUL-SRVW01	192.168.200.1	Connecté
STG-SRVW02	192.168.100.2	Connecté
STG-SRVW01	192.168.100.1	Connecté

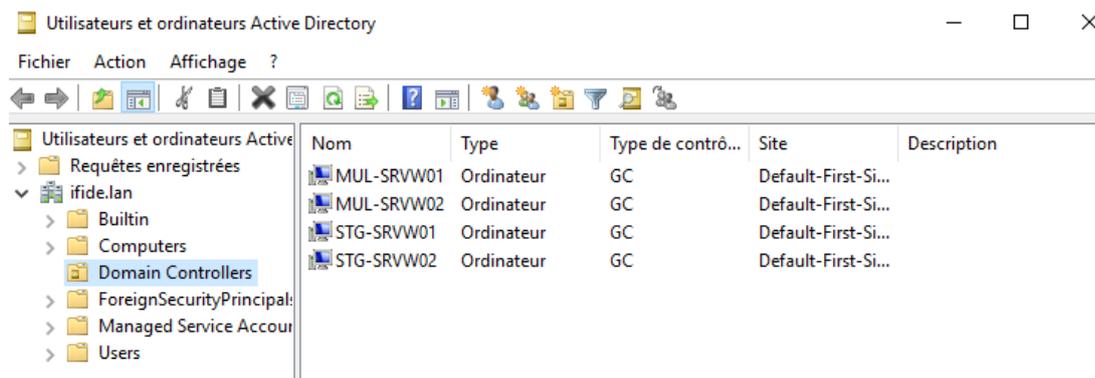
Il suffit de **réaliser exactement les mêmes étapes** pour **STG-SRVW02** que pour **MUL-SRVW02**, afin de lever le message d'avertissement et permettre la gestion complète du serveur depuis le Gestionnaire de serveur.

Vérification de l'ajout des contrôleurs de domaine

Pour vérifier que tous les serveurs Active Directory sont bien contrôleurs de domaine, nous ouvrons l'outil **Utilisateurs et ordinateurs Active Directory**, accessible depuis le menu Démarrer, la console MMC, ou le Gestionnaire de serveur.

Une fois dans l'outil, cliquez sur **ifide.lan > Domain Controllers**.

Si les promotions ont été correctement effectuées, les serveurs **STG-SRVW01**, **MUL-SRVW01**, **MUL-SRVW02** et **STG-SRVW02** apparaîtront dans cette unité d'organisation.



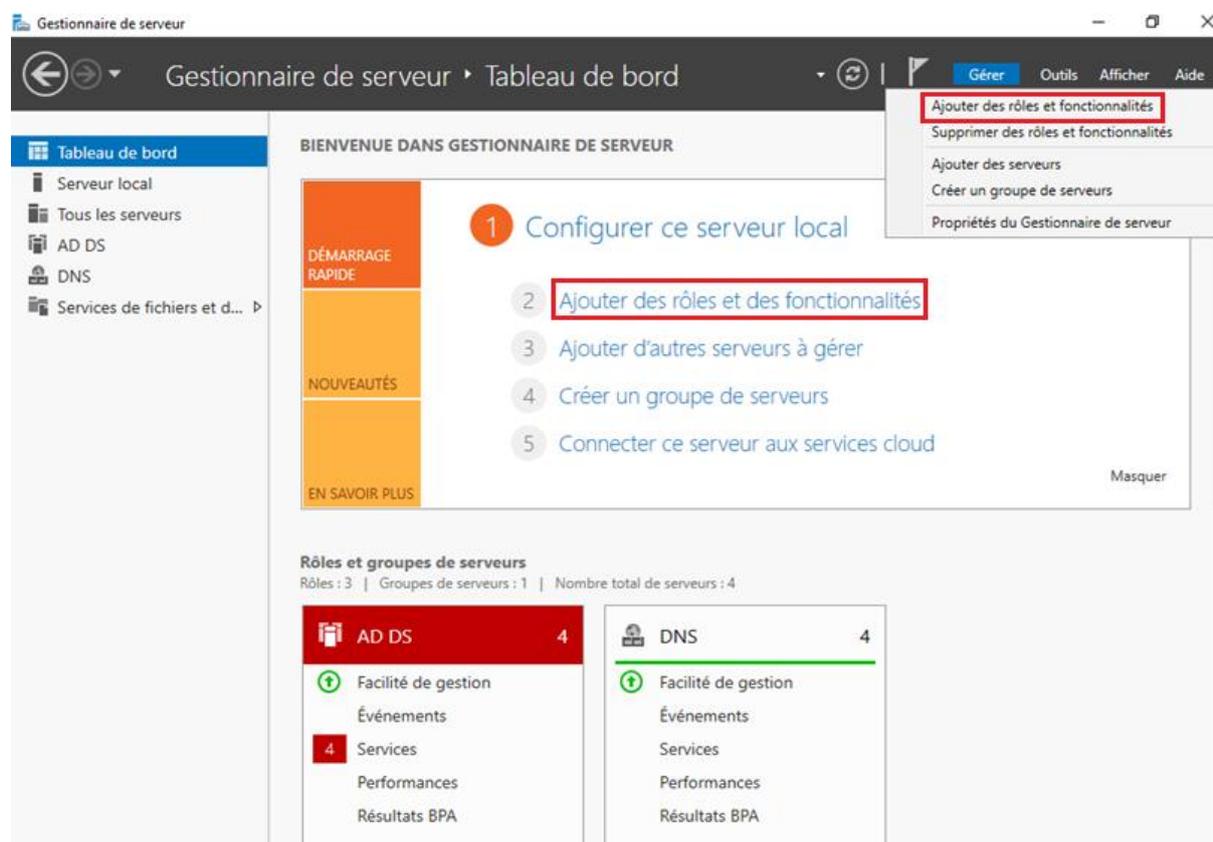
3.1.6) Installation du service DHCP

Dans le cadre de l'infrastructure à mettre en place, il est prévu d'installer un **serveur DHCP** afin d'assurer la **distribution dynamique des adresses IP** pour les machines clientes du réseau. Sans entrer dans les détails techniques du fonctionnement du service, les étapes ci-dessous décrivent l'installation du **rôle DHCP sous Windows Server**.

Ces opérations seront à réaliser sur **les quatre serveurs** du projet, afin de permettre la **configuration du basculement DHCP** de part et d'autre des sites LAN.

Installation graphique

Pour installer le rôle en mode graphique, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Gérer → Ajouter des rôles et des fonctionnalités**.



Ensuite, sélectionnez le **serveur de destination** sur lequel le rôle DHCP sera installé.
 Cette opération devra être **répétée pour chacun des quatre serveurs**, en sélectionnant à chaque fois le serveur concerné dans la liste.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
STG-SRVW01.ifide.lan

Avant de commencer
 Type d'installation
Sélection du serveur
 Rôles de serveurs
 Fonctionnalités
 Confirmation
 Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

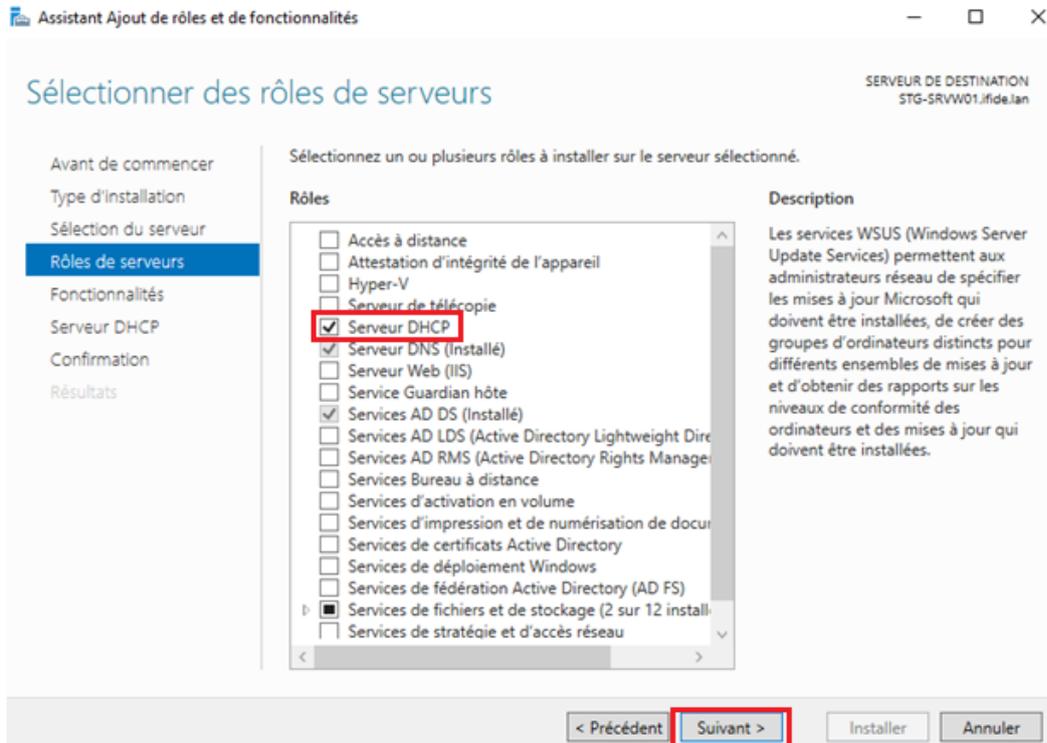
Nom	Adresse IP	Système d'exploitation
MUL-SRVW01.ifide.lan	192.168.200.1	Microsoft Windows Server 2019 Standard
STG-SRVW02.ifide.lan	192.168.100.2	Microsoft Windows Server 2010 Standard
STG-SRVW01.ifide.lan	192.168.100.1	Microsoft Windows Server 2019 Standard
MUL-SRVW02.ifide.lan	192.168.200.2	Microsoft Windows Server 2019 Standard

4 ordinateur(s) trouvé(s)

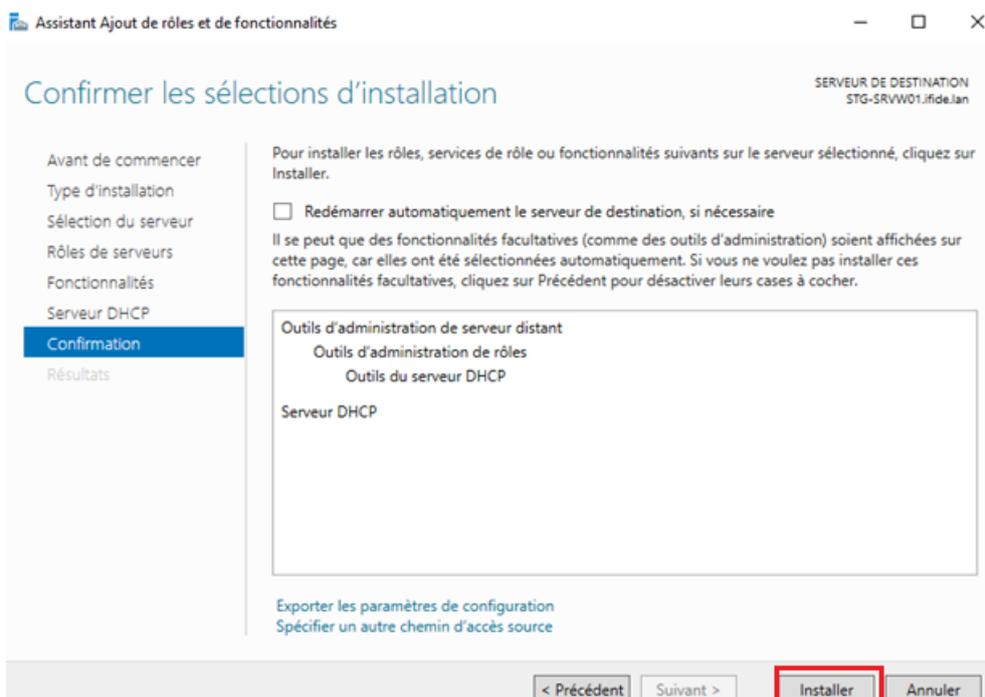
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

Sélectionnez ensuite le rôle DHCP, puis cliquez sur **Suivant**.



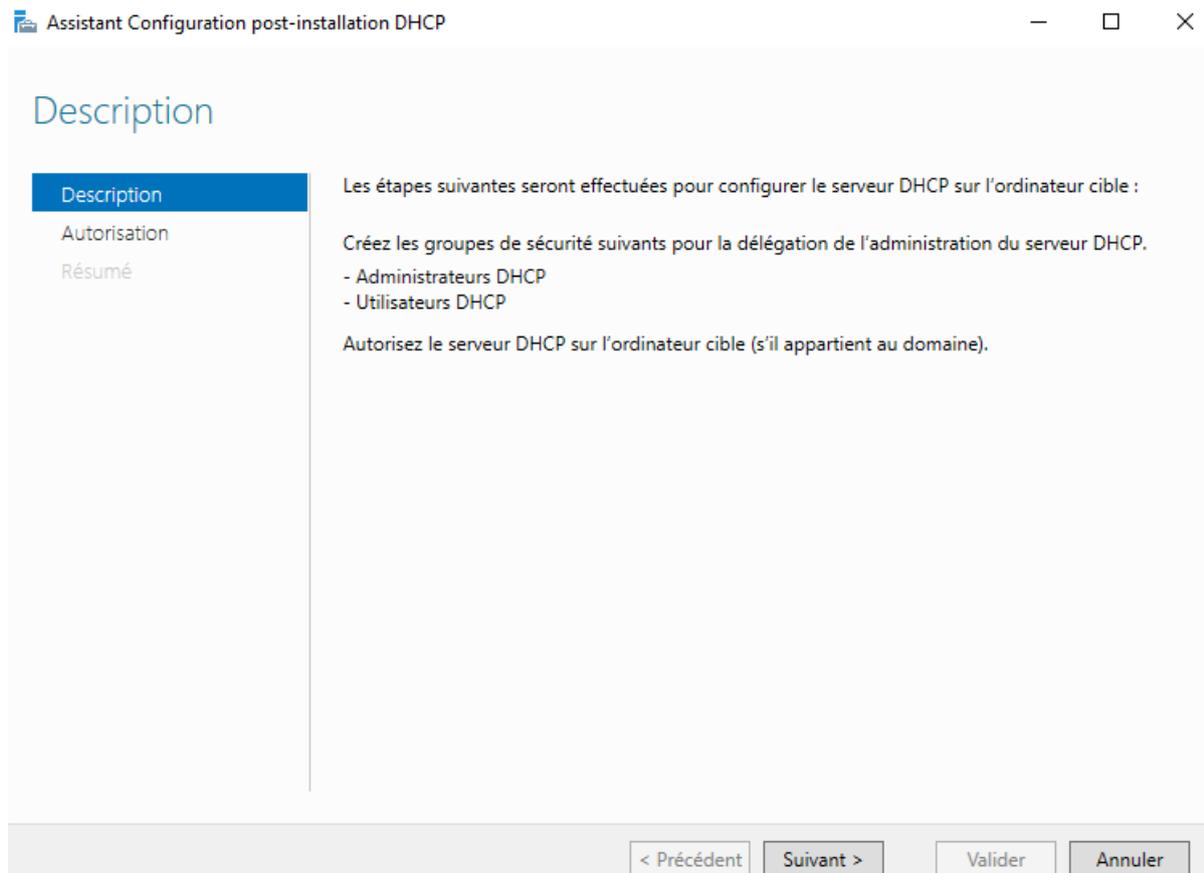
Cliquez ensuite sur **Suivant** jusqu'à l'étape finale, puis cliquez sur **Installer** pour lancer l'installation du rôle.



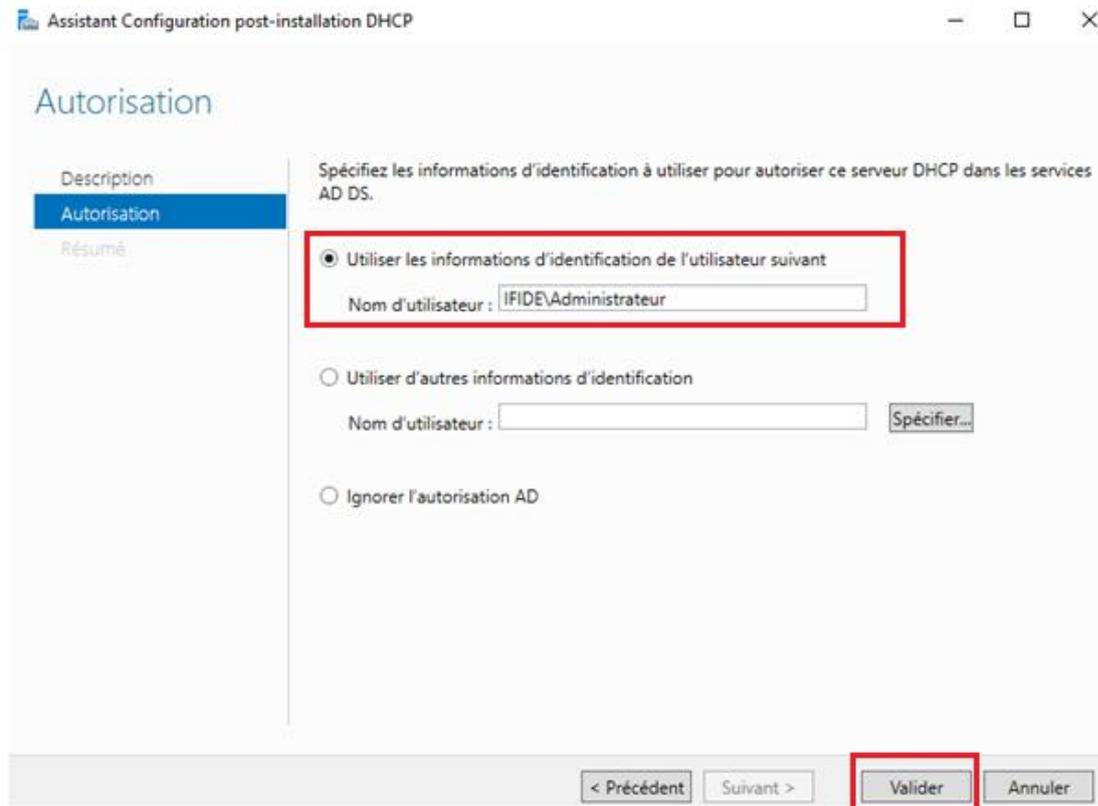
Enfin, cliquez sur l'**étendard jaune** dans le Gestionnaire de serveur, puis sélectionnez "**Terminer la configuration DHCP**".



Cette étape permet de donner au **contrôleur de domaine** les autorisations nécessaires pour administrer le serveur DHCP, ce qui est **essentiel à son bon fonctionnement**. Cliquez ensuite sur **Suivant**.

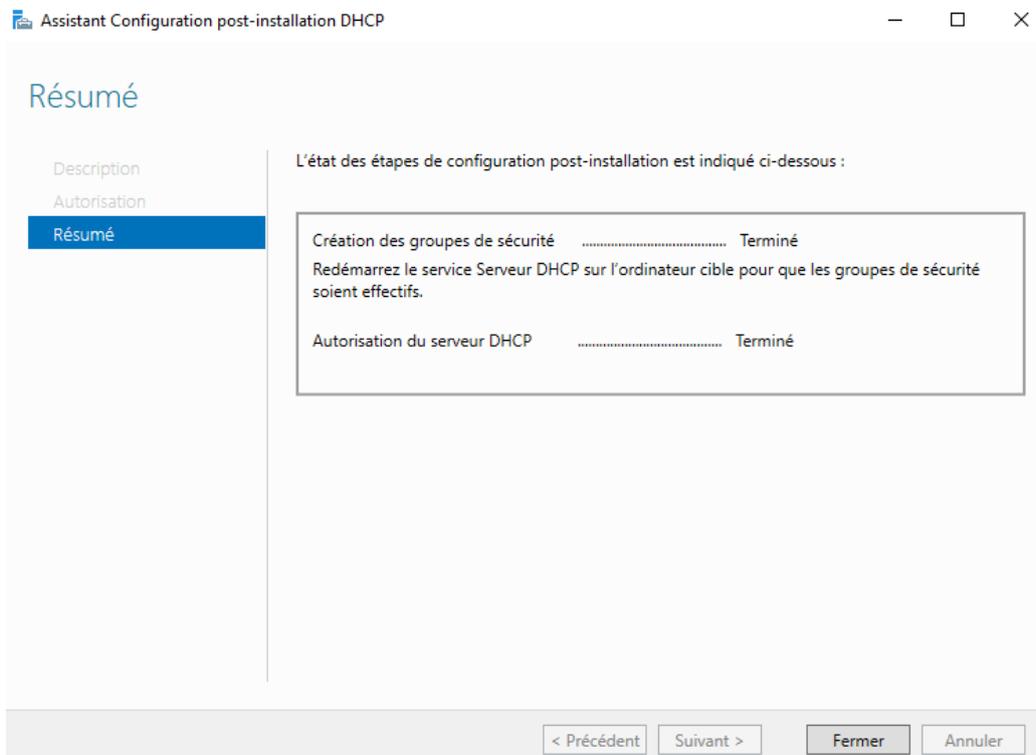


Laissez cochée l'option "Utiliser les informations d'identification de l'utilisateur suivant", puis cliquez sur **Valider**.

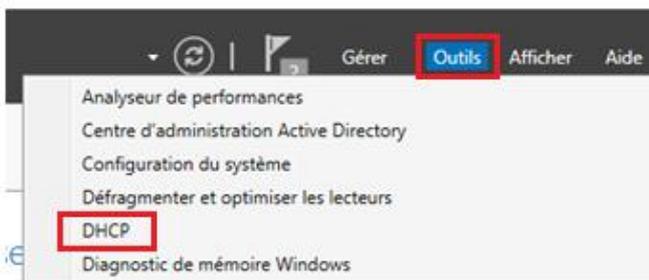


The screenshot shows the 'Assistant Configuration post-installation DHCP' window. The 'Autorisation' step is active, with a sidebar containing 'Description', 'Autorisation', and 'Résumé'. The main area contains the instruction: 'Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.' There are three radio button options: 'Utiliser les informations d'identification de l'utilisateur suivant' (selected), 'Utiliser d'autres informations d'identification', and 'Ignorer l'autorisation AD'. The selected option has a text box for 'Nom d'utilisateur' containing 'IFIDE\Administrateur'. The 'Utiliser d'autres informations d'identification' option has a text box and a 'Spécifier...' button. At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Valider', and 'Annuler'. The 'Valider' button is highlighted with a red box.

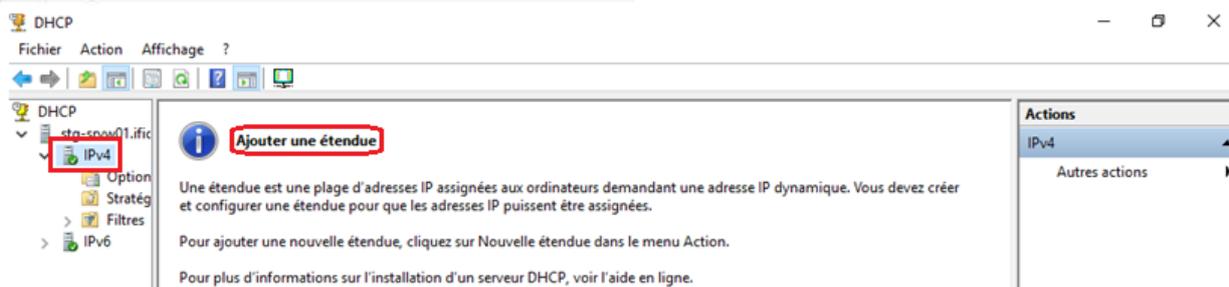
Le service DHCP est désormais installé correctement. Vous pouvez accéder à la **console de gestion DHCP** via **Outils → DHCP**, ou à partir d'une **console MMC personnalisée** si celle-ci a été configurée.



Accès console DHCP



Le service DHCP a été installé et initialisé correctement.



Installation sous PowerShell

Sous PowerShell, l'installation du service DHCP peut se faire en deux commandes simples, ce qui facilite et accélère le déploiement du rôle.

Voici les commandes à saisir :

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

Une fois l'installation du service terminée, saisissez la commande suivante, qui permet d'autoriser le serveur DHCP dans le domaine Active Directory, comme lors de la configuration graphique.

```
Add-DhcpServerInDC -DnsName ifide.lan -Verbose
```

Pour la suite, concernant la **configuration des étendues** et la mise en place du **basculement DHCP**, veuillez-vous référer à la partie

3.2.2 – Mise en place du pool DHCP et de son basculement.

3.1.7) Installation du service DFS

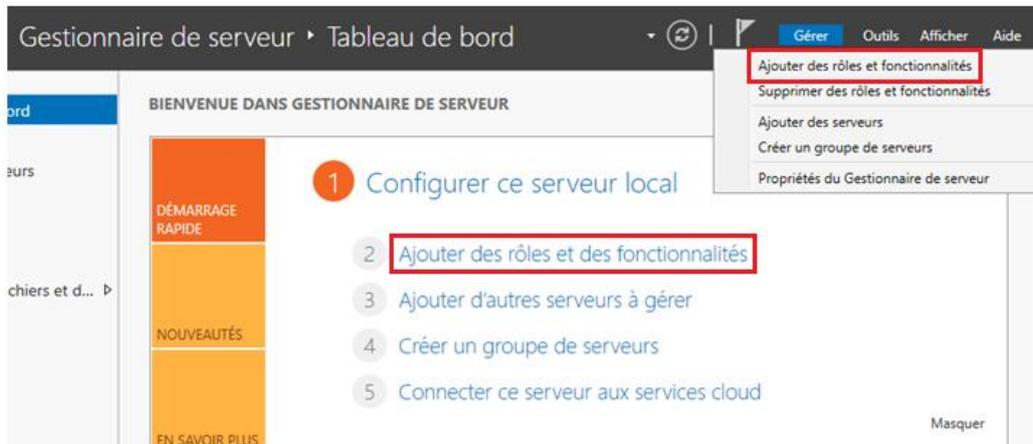
À présent, nous passons à l'installation du rôle **DFS** sur les serveurs.

Dans l'architecture prévue, l'espace de noms DFS sera installé sur les **serveurs en interface graphique** de chaque site, afin de garantir la **haute disponibilité** des fichiers et dossiers distribués.

Ensuite, nous installerons la **réplication DFS** sur l'ensemble des serveurs Windows de l'infrastructure, afin d'assurer la **réplication et la synchronisation des dossiers partagés** entre les différents serveurs.

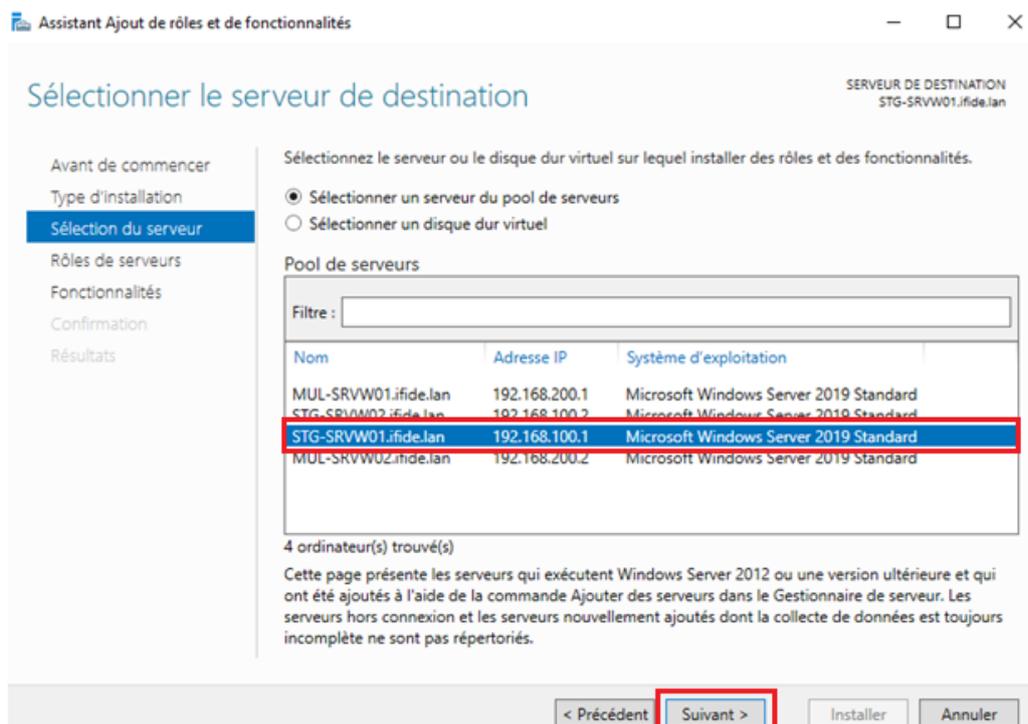
Installation des serveurs Espace de noms DFS

Pour installer l'espace de noms DFS, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Gérer** → **Ajouter des rôles et fonctionnalités**.



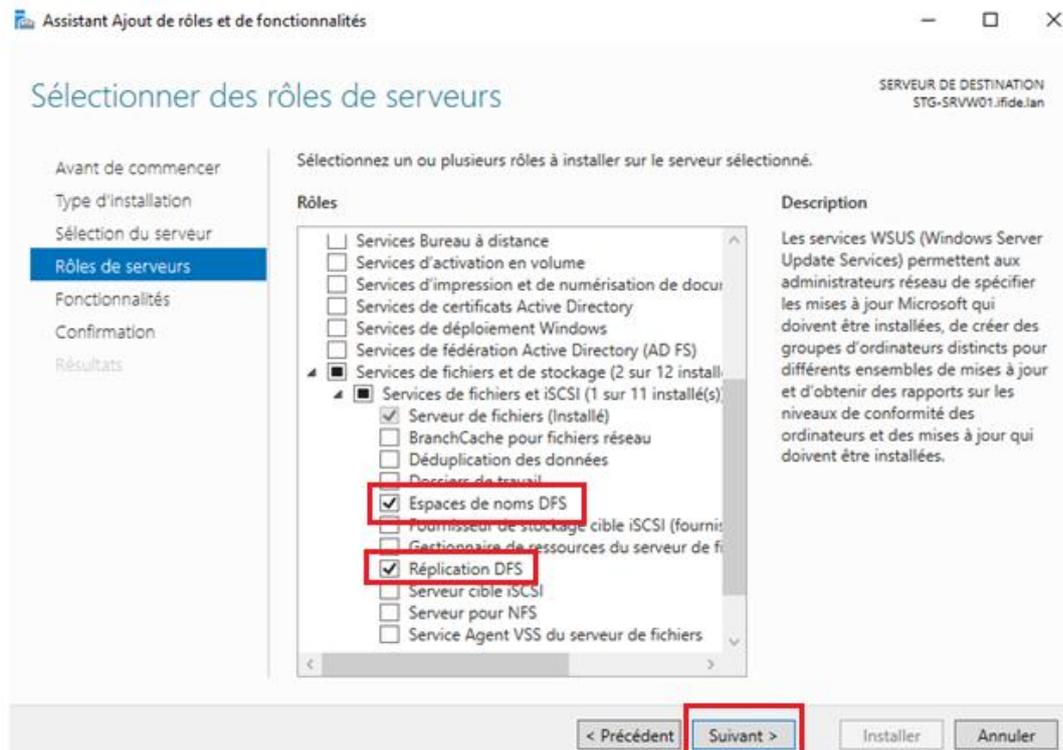
Ensuite, à l'étape de sélection du serveur, installez l'espace de noms DFS sur **STG-SRVW01**, puis sur **MUL-SRVW01**.

Choisissez d'abord l'un des deux serveurs pour effectuer l'installation, puis répétez exactement la même procédure sur le second.



Ensuite, à l'étape de sélection des rôles, cochez **Espace de noms DFS** ainsi que **Réplication DFS**, en prévision de la configuration de la réplication que nous verrons par la suite.

Une fois les rôles sélectionnés, cliquez sur **Suivant** jusqu'à atteindre l'étape d'installation, puis cliquez sur **Installer**.



Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

SERVEUR DE DESTINATION
STG-SRVW01.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

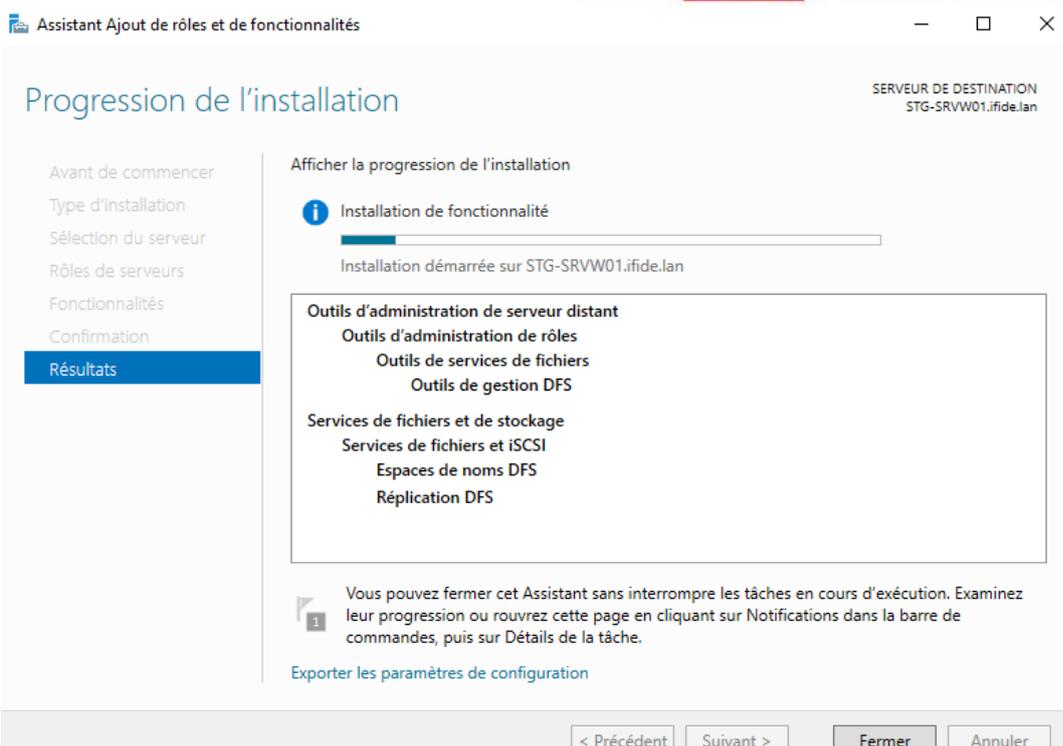
Rôles

- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de docu...
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (2 sur 12 install...
- Services de fichiers et iSCSI (1 sur 11 installé(s))
 - Serveur de fichiers (Installé)
 - BranchCache pour fichiers réseau
 - Déduplication des données
 - Dossier de travail
 - Espaces de noms DFS
 - Fournisseur de stockage cible iSCSI (fourni...
 - Gestionnaire de ressources du serveur de fi...
 - Serveur cible iSCSI
 - Serveur pour NFS
 - Service Agent VSS du serveur de fichiers

Description

Les services WSUS (Windows Server Update Services) permettent aux administrateurs réseau de spécifier les mises à jour Microsoft qui doivent être installées, de créer des groupes d'ordinateurs distincts pour différents ensembles de mises à jour et d'obtenir des rapports sur les niveaux de conformité des ordinateurs et des mises à jour qui doivent être installées.

< Précédent **Suivant >** Installer Annuler



Assistant Ajout de rôles et de fonctionnalités

PROGRESSION DE L'INSTALLATION

SERVEUR DE DESTINATION
STG-SRVW01.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation démarrée sur STG-SRVW01.ifide.lan

Outils d'administration de serveur distant

- Outils d'administration de rôles
- Outils de services de fichiers
- Outils de gestion DFS

Services de fichiers et de stockage

- Services de fichiers et iSCSI
- Espaces de noms DFS
- Réplication DFS

i Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler



Pour renforcer davantage la **haute disponibilité** des données, il est également possible d'installer le **rôle d'espace de noms DFS** sur les **serveurs Core**, afin d'éviter qu'un seul serveur ne constitue un **point de défaillance unique** pour l'accès au partage réseau.

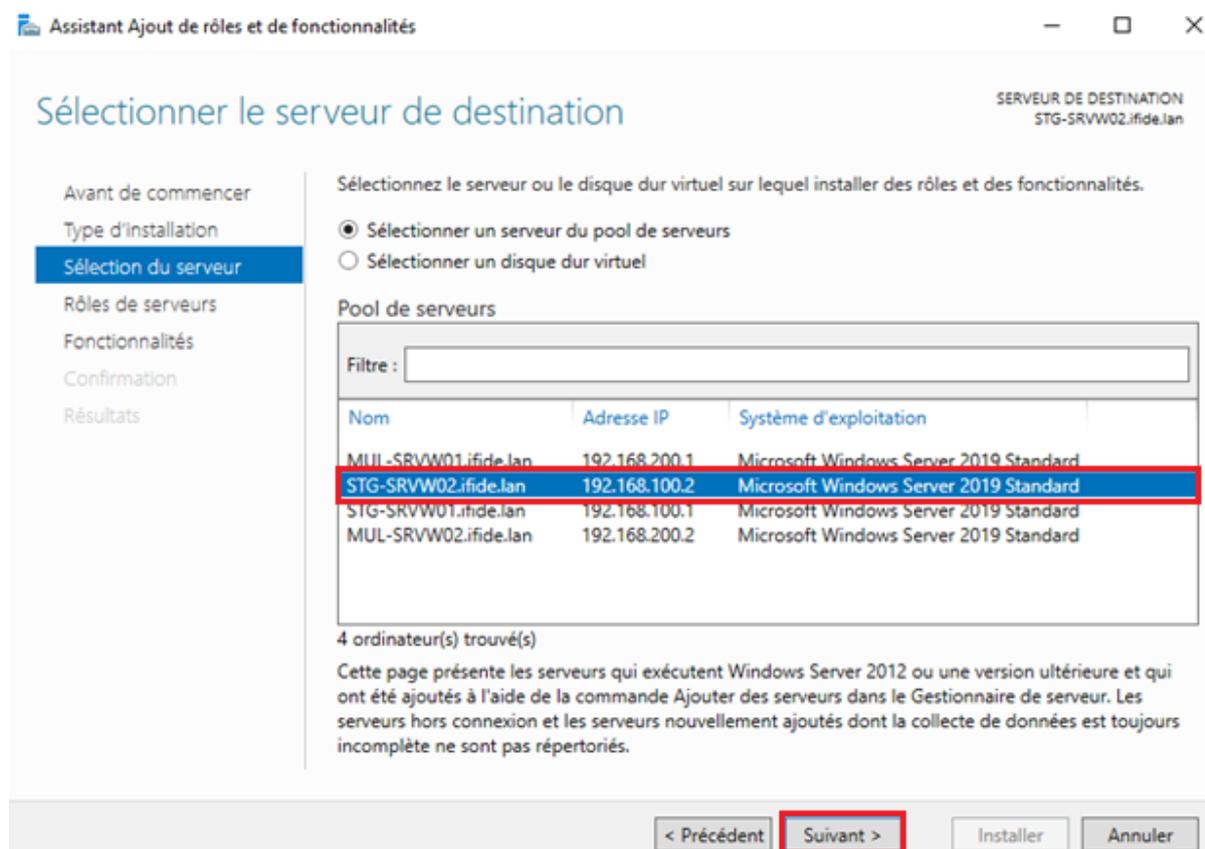
Installation du rôle Réplication DFS

La réplication DFS sera installée sur l'ensemble des quatre serveurs Windows. Le rôle a déjà été installé précédemment sur les serveurs en interface graphique.

Pour la suite, nous procéderons **uniquement à l'installation du rôle Réplication DFS** sur les deux serveurs Core restants de l'infrastructure.

Pour cela, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Ajouter des rôles et fonctionnalités**.

Lors de la sélection du serveur, veillez à bien choisir les **serveurs Core** concernés.



Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
STG-SRVW02.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

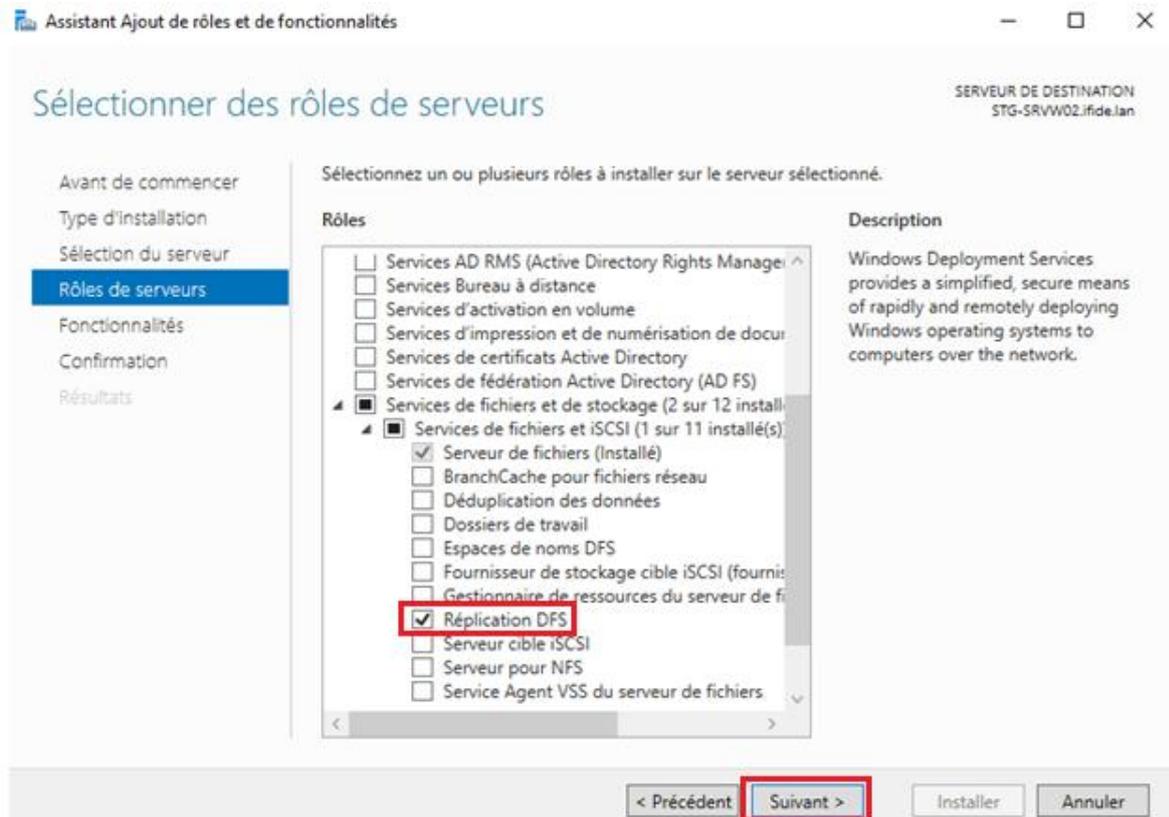
Nom	Adresse IP	Système d'exploitation
MUL-SRVW01.ifide.lan	192.168.200.1	Microsoft Windows Server 2019 Standard
STG-SRVW02.ifide.lan	192.168.100.2	Microsoft Windows Server 2019 Standard
STG-SRVW01.ifide.lan	192.168.100.1	Microsoft Windows Server 2019 Standard
MUL-SRVW02.ifide.lan	192.168.200.2	Microsoft Windows Server 2019 Standard

4 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

Ensuite, à l'étape de sélection des rôles, cochez uniquement **Réplication DFS**.



Enfin, cliquez sur **Suivant** jusqu'à l'étape finale, puis cliquez sur **Installer** pour lancer l'installation du rôle **Réplication DFS**.

Sans le rôle **Espace de noms DFS** installé, ces serveurs permettront uniquement la **réplication des contenus** des dossiers répliqués.

La **haute disponibilité** de l'espace de noms étant déjà assurée par les serveurs principaux de chaque site.

Pour l'exploitation du service, cela sera abordé **dans une section ultérieure** dédiée à la **configuration du partage DFS et de la réplication DFS-R**.

3.1.8) Installation de la solution de sauvegarde

À présent, maintenant que les services nécessaires à la **réplication des données** entre les sites de **Strasbourg** et **Mulhouse** sont en place, nous allons mettre en œuvre une **solution de sauvegarde** afin de garantir la **disponibilité des données** et **minimiser les risques**.

Pour cela, nous utiliserons **Windows Server Backup** avec une cible **iSCSI** pointant vers un serveur **TrueNAS**.

Pour une meilleure compréhension de la procédure de sauvegarde, vous pouvez vous référer au **schéma ci-dessous**.

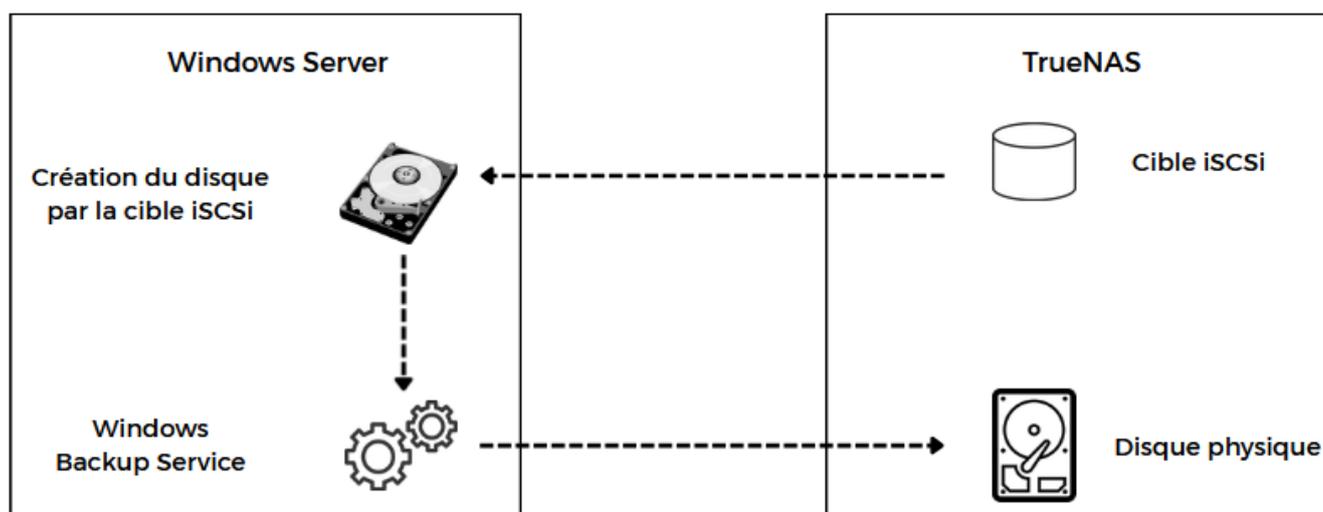


Figure 1 : Processus de sauvegarde des données vers TrueNAS

Ainsi, pour commencer, nous allons procéder à la **mise en place** et à l'**installation du serveur TrueNAS**.

Installation et configuration de TrueNAS

Installation de TrueNAS

TrueNAS étant basé sur **FreeBSD**, son installation nécessite normalement de respecter une configuration matérielle minimale, ainsi que de se procurer l'image d'installation officielle depuis truenas.com.

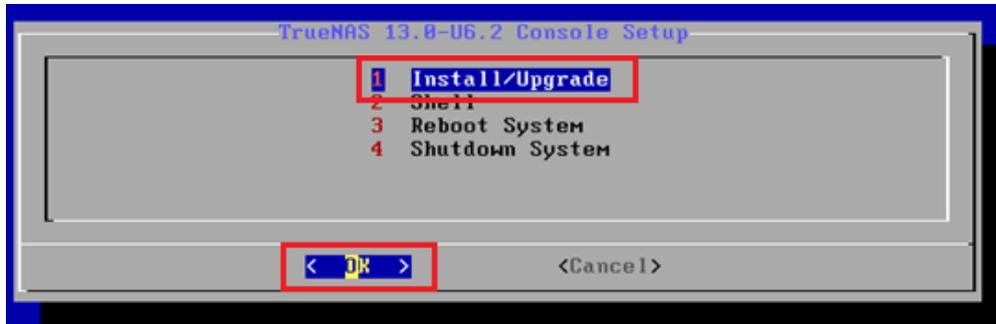
Dans le cadre de cette documentation, nous utiliserons cependant **deux machines virtuelles déjà préparées**, nommées **STG-NAS01** et **MUL-NAS01**, qui avaient été **préparées en amont** au début du projet.

Ces machines disposent de la configuration suivante :

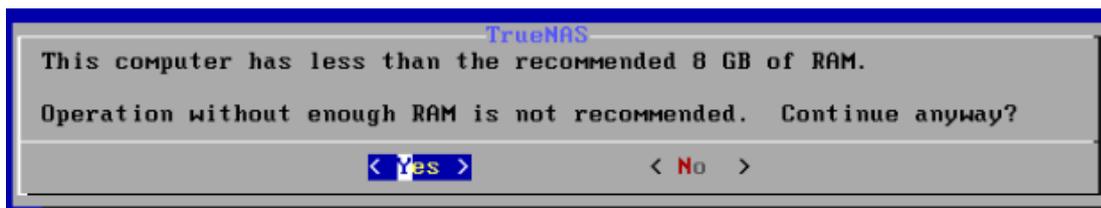
Device	Summary
 Memory	512 MB
 Processors	1
 Hard Disk 2 (SATA)	60 GB
 Hard Disk (SATA)	60 GB
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Auto detect
 Network Adapter	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

Une fois la machine démarrée, il suffira de suivre les étapes de l'installation présentées ci-dessous :

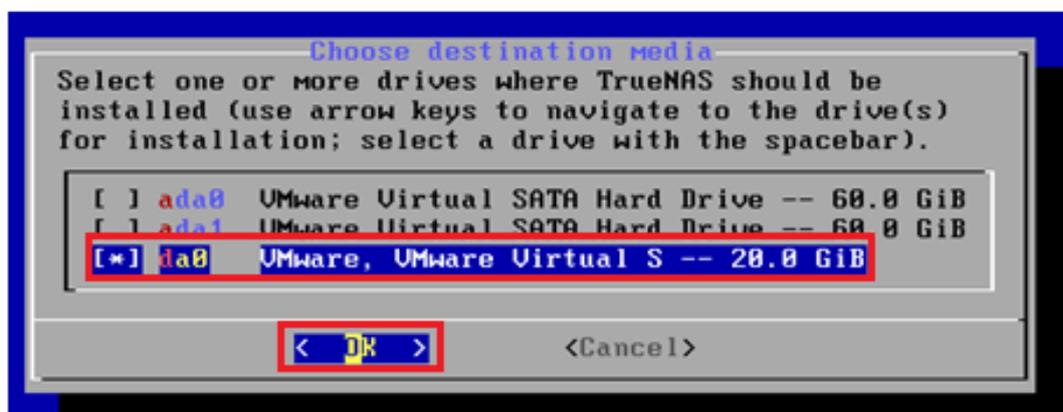
Appuyez sur **Entrée** pour valider, puis sélectionnez l'option **Install/Upgrade**.



Une alerte apparaîtra concernant la **quantité de RAM insuffisante** allouée à la machine. En environnement de production, il est fortement recommandé de respecter les **configurations minimales et recommandées** disponibles sur le **site officiel de TrueNAS**.



Appuyez sur la touche **Espace** pour sélectionner le disque sur lequel installer le système d'exploitation TrueNAS, puis sur **Entrée** pour confirmer.



Le programme d'installation demande ensuite si vous souhaitez **formater le disque** sélectionné pour l'installation.

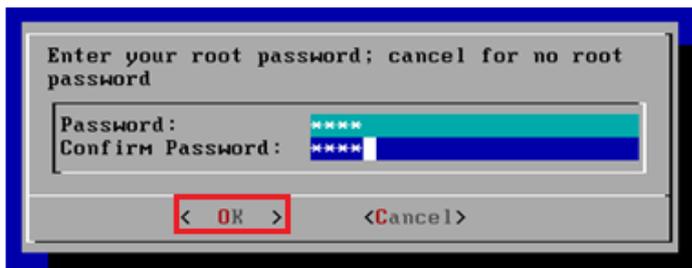
Confirmez en appuyant sur **Entrée**.



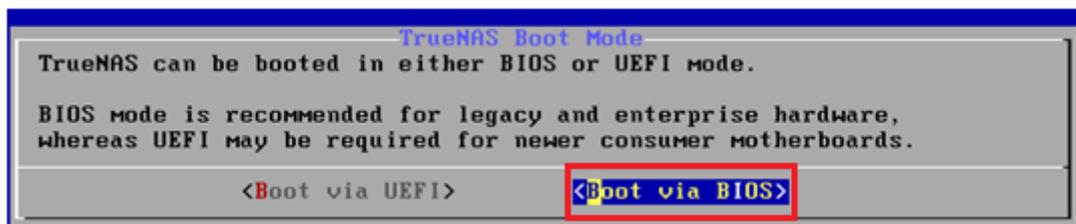
Configurez ensuite le **mot de passe root** de TrueNAS.



La disposition du clavier utilisée par défaut lors de l'installation est en **QWERTY**.



Ensuite, sélectionnez le **mode de démarrage BIOS** pour le système.



Patientez le temps de l'installation, puis procédez au **redémarrage du serveur**.

```
The TrueNAS installation on da0 succeeded!  
Please reboot and remove the installation media.
```

```
< OK >
```



N'oubliez pas de **reproduire les mêmes étapes** pour l'installation du serveur **TrueNAS de Mulhouse**.

Configuration réseau de TrueNAS

Avant de pouvoir exploiter TrueNAS pour la mise en place de la solution de sauvegarde, certaines configurations sont encore nécessaires sur le serveur.

Les prochaines étapes d'administration se feront via l'interface web, ce qui nécessite que le serveur dispose d'une adresse IP accessible sur le réseau.

Selon le **tableau d'adressage** défini dans le dossier de réponse au cahier des charges, les **adresses IP attribuées aux serveurs TrueNAS** sont les suivantes :

- 192.168.100.3/24 pour STG-NAS01
- 192.168.200.3/24 pour MUL-NAS01

Pour cela, au démarrage du serveur, un **menu interactif** s'affiche (similaire à sconfig sous Windows), et reste accessible à tout moment en exécutant la commande **/etc/netcli** depuis le shell.



Le démarrage initial de la machine virtuelle TrueNAS échouait systématiquement à cause d'une mémoire insuffisante. Afin de résoudre ce problème, la mémoire RAM de la VM a été augmentée à 1,2 Go, ce qui a permis au système de démarrer correctement et d'accéder aux menus de configuration réseau.

Ensuite, dans le menu, tapez **1** pour configurer les **interfaces réseau**, puis suivez les étapes indiquées.

```

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: em0
Several input formats are supported
Example 1 CIDR Notation:
192.168.1.1/24
Example 2 IP and Netmask separate:
IP: 192.168.1.1
Netmask: 255.255.255.0 /24 or 24
IPv4 Address: 192.168.100.3/24
Saving interface configuration: Ok
Configure IPv6? (y/n) n
  
```

La configuration réseau étant terminée, nous pouvons désormais accéder à l'**interface web de TrueNAS** pour procéder à la **configuration des disques** et à la **mise en place de la solution de sauvegarde**.

```

Console setup
-----

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

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

Enter an option from 1-11: █
  
```

STG-NAS01

MUL-NAS01

```
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Restarting network: ok

Console setup
-----

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

The web user interface is at:

http://192.168.200.3
https://192.168.200.3

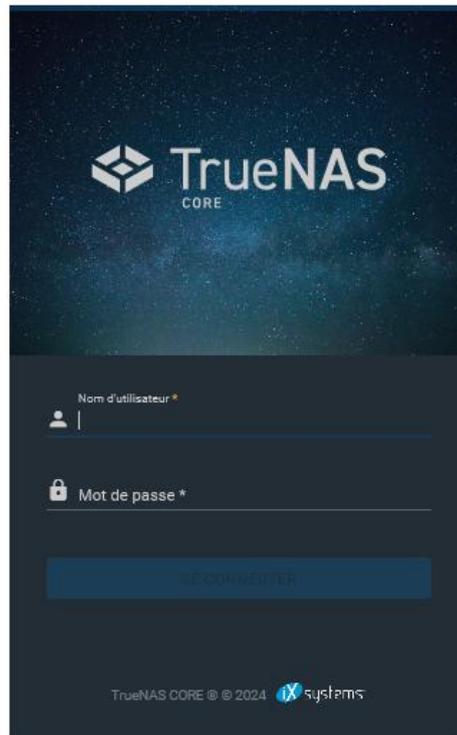
Enter an option from 1-11: █
```

Accès à l'interface web de TrueNAS

Depuis l'un des serveurs disposant d'une interface graphique, saisissez dans un navigateur l'adresse IP du serveur TrueNAS, par exemple : <http://192.168.100.3>.

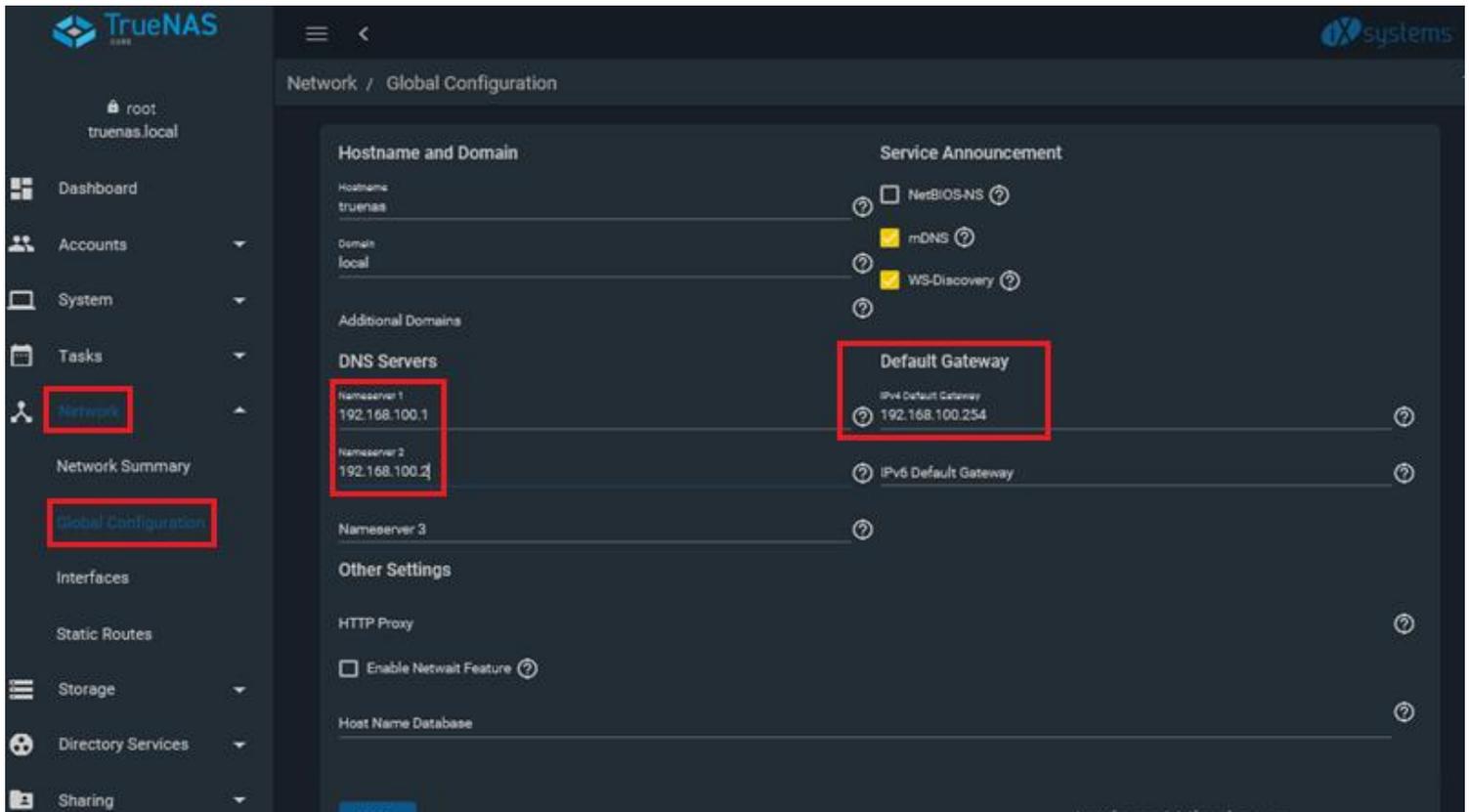
Pour un accès plus intuitif, il est également possible d'ajouter une entrée DNS correspondant à l'adresse IP du serveur TrueNAS, afin d'y accéder via un nom de domaine (FQDN) comme mul-nas01.ifide.lan.

Interface web accessible, installation de TrueNAS terminée avec succès.



Enfin, connectez-vous à l'interface web, puis finalisez la **configuration réseau** de TrueNAS en accédant à **Network → Global Configuration** dans le menu de gauche.

Renseignez ensuite la **passerelle par défaut** du serveur ainsi que les **serveurs DNS**.

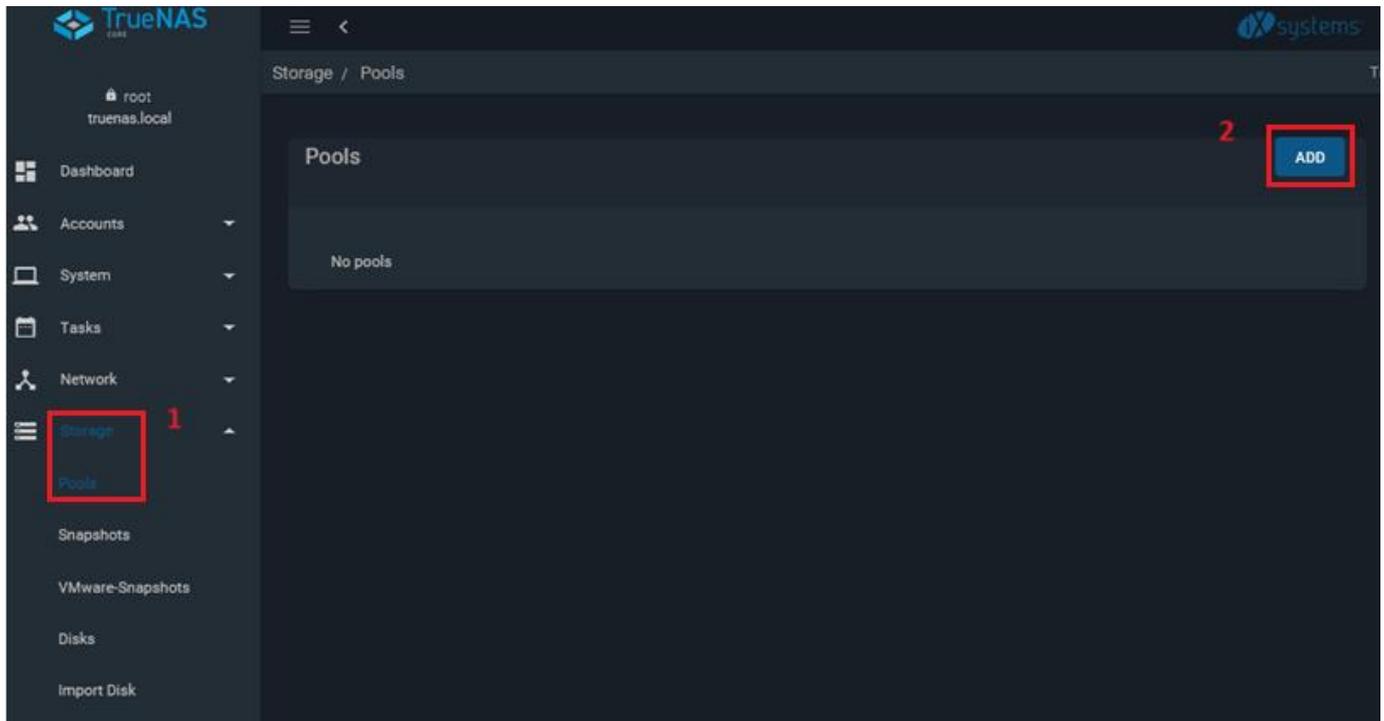


Configuration du RAID des disques dans TrueNAS

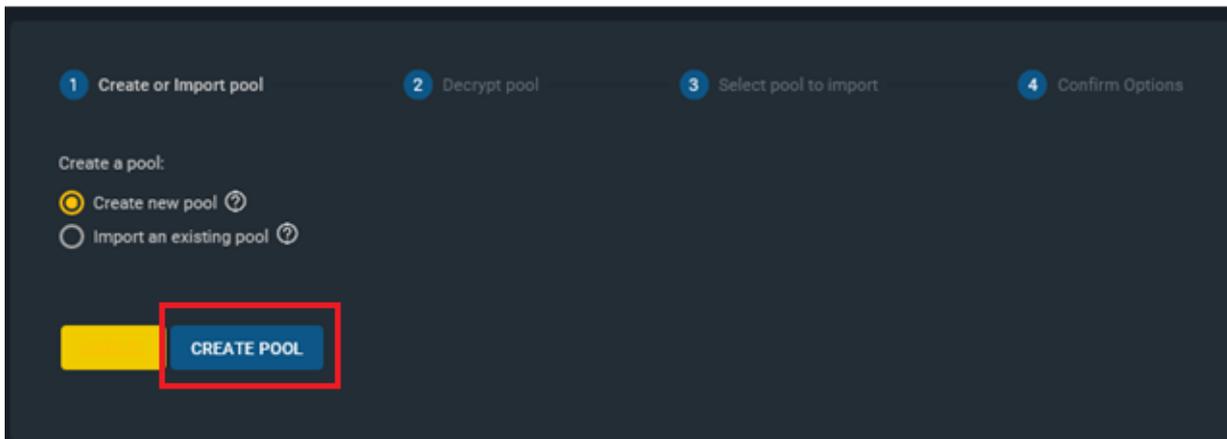
Dans notre configuration, nous souhaitons mettre en place un RAID 1 afin d'assurer une tolérance aux pannes physiques des disques.

Pour cela, dans l'interface web de TrueNAS, cliquez sur **Storage → Pools** depuis le menu de gauche.

Cliquez sur **Add** pour créer un nouveau pool de disques, équivalent à une configuration RAID.

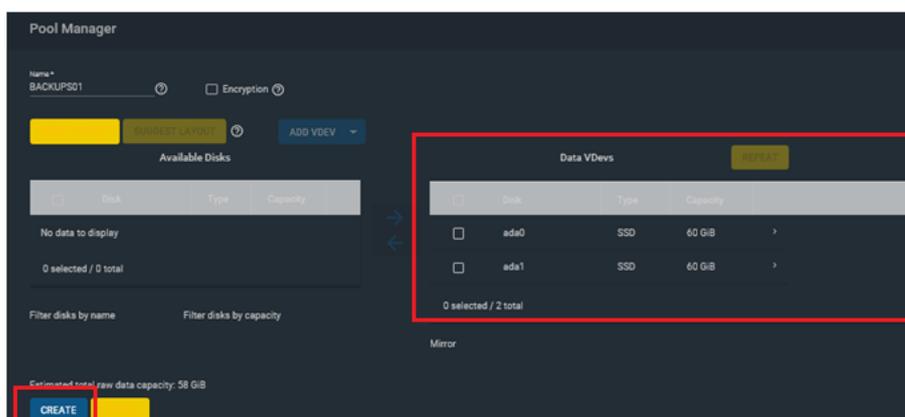
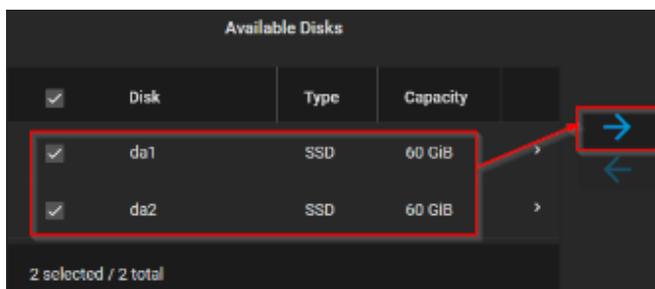
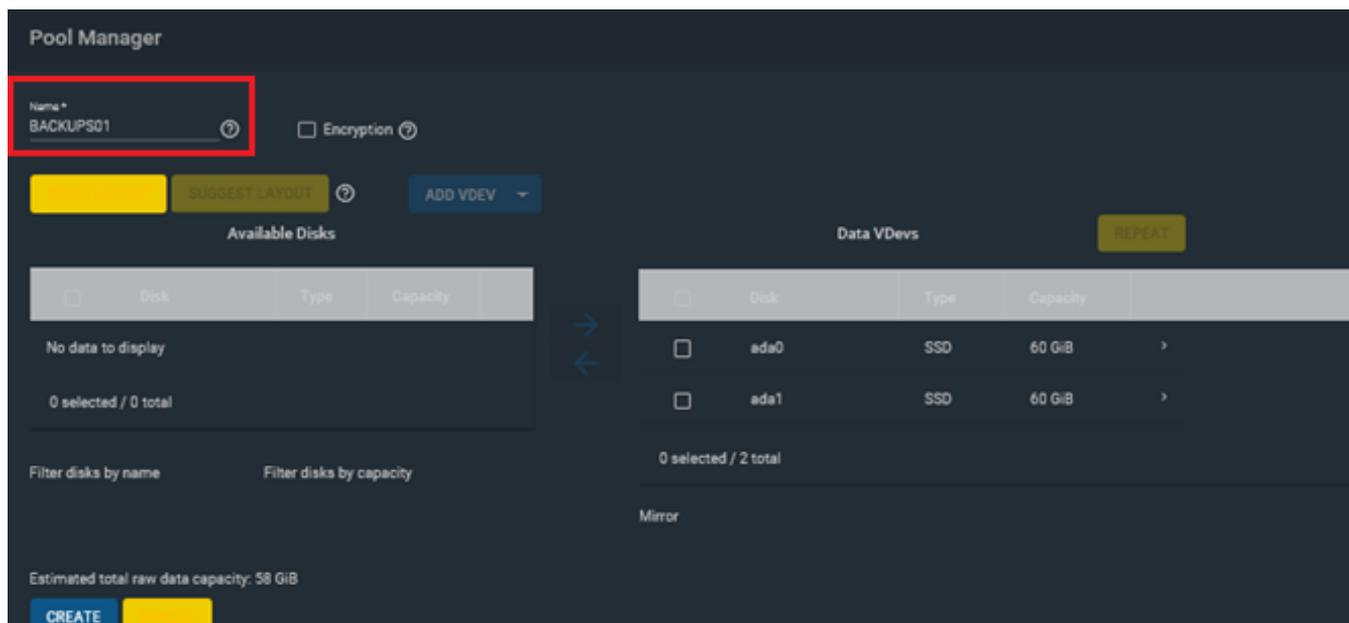


Laissez cochée l'option **Create a new pool**, puis cliquez sur **CREATE POOL**.



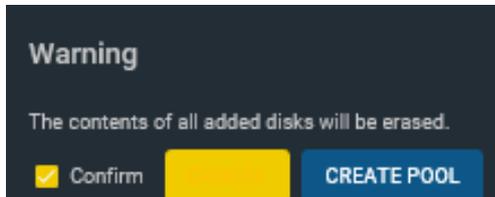
Ensuite, attribuez un nom à votre **pool de disques** : **BACKUPS01** pour le serveur TrueNAS de **Strasbourg**, et **BACKUPS02** pour celui de **Mulhouse**.

Sélectionnez les disques à inclure dans le pool, puis cliquez sur **CREATE** pour confirmer la création du pool et configurer le **RAID** en même temps.

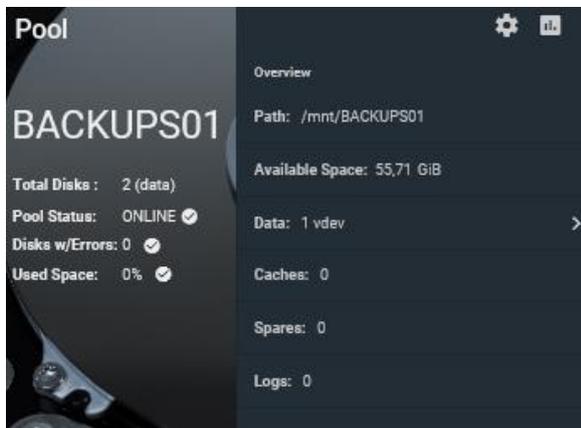


Sauf si les **performances** ou la **capacité de stockage** sont une priorité pour le client, il est fortement recommandé de laisser le type de RAID sur **Mirror**, afin d'assurer une **haute disponibilité** des données.

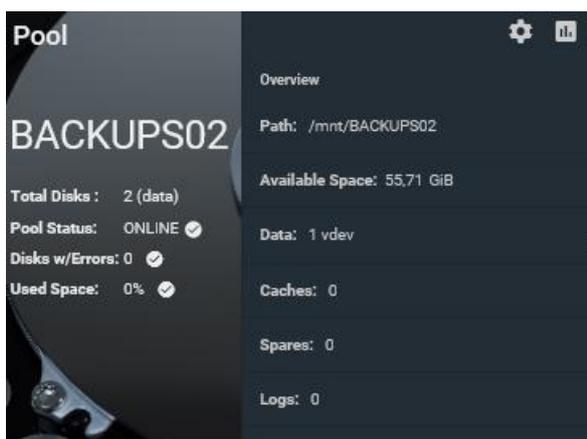
Un message d'alerte s'affichera pour indiquer que tout le contenu des disques sera formaté. Cochez **Confirm**, puis cliquez sur **CREATE POOL** pour valider l'opération.



STG-NAS01 Le pool BACKUPS01 a été créé sur le serveur TrueNAS de Strasbourg.

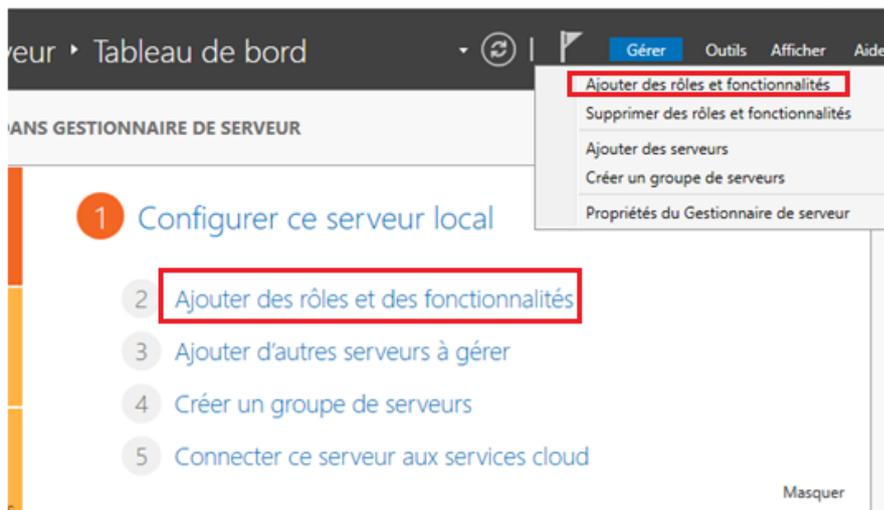


MUL-NAS01 Le pool BACKUPS02 a été créé sur le serveur TrueNAS de Mulhouse.

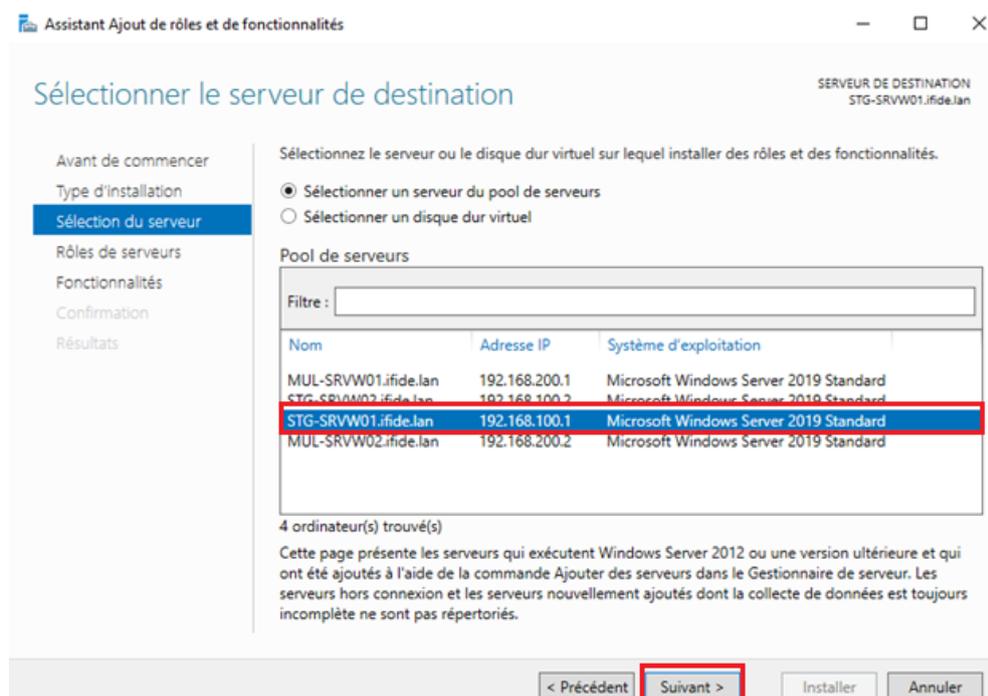


Installation de la fonctionnalité Windows Server Backup

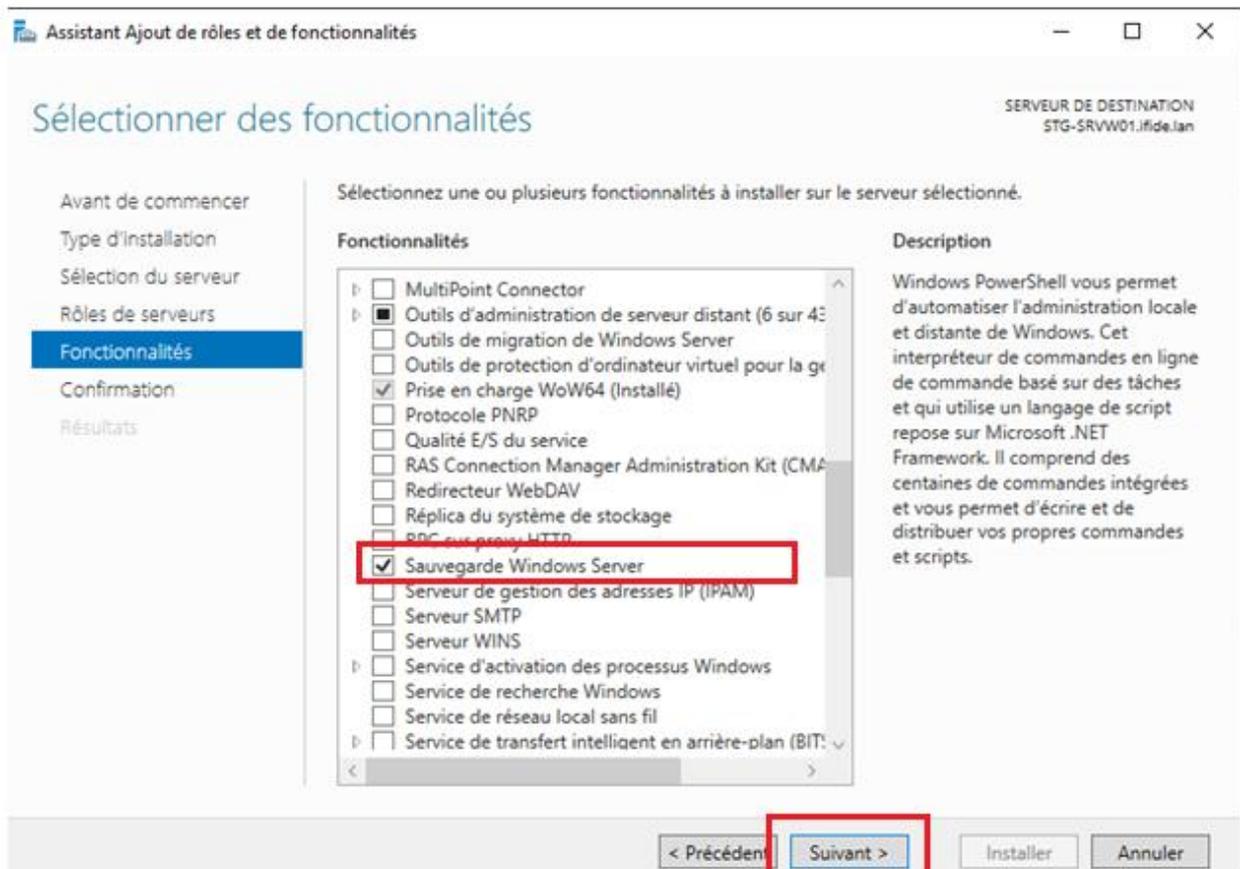
Depuis le Gestionnaire de serveur, cliquer sur **Gérer** puis sur **Ajouter des rôles et des fonctionnalités**



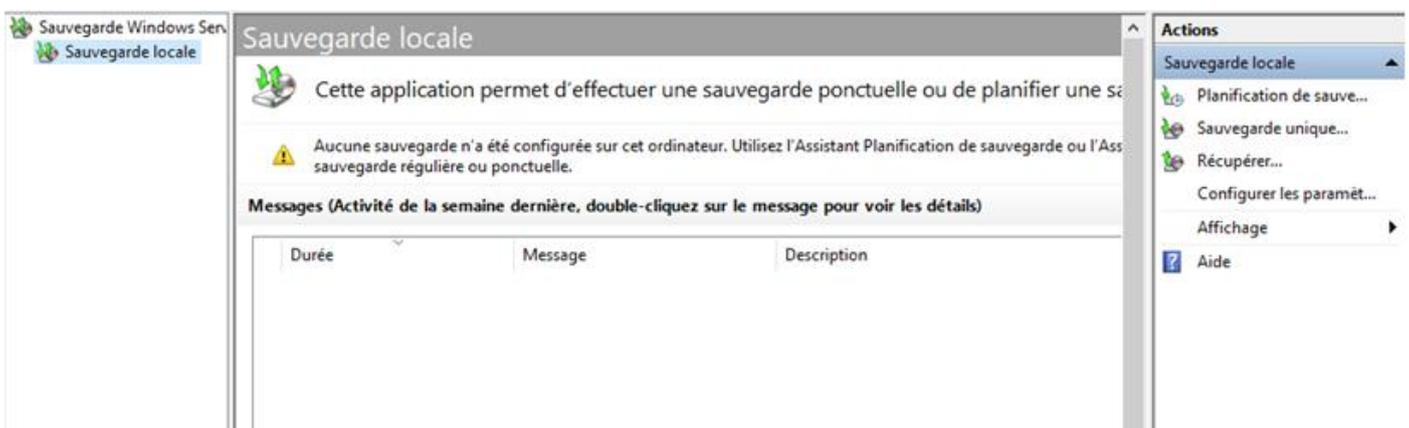
Sélectionnez le serveur sur lequel vous souhaitez installer la fonctionnalité. D'après le cahier des charges, ce sont les serveurs **STG-SRVW01** et **MUL-SRVW01** (en interface graphique) qui doivent recevoir l'installation de Windows Server Backup, car ce sont eux qui hébergent les données à sauvegarder (**DATAS01** et **DATAS03**).



Ensuite, ne sélectionnez **aucun rôle** et cliquez sur **Suivant**. Dans l'onglet **Fonctionnalités**, cochez **Sauvegarde Windows Server**, puis cliquez à nouveau sur **Suivant** pour poursuivre l'installation.



Une fois l'installation finalisée, la fonctionnalité **Sauvegarde Windows Server** est désormais disponible. Pour la suite et la configuration de la sauvegarde vers TrueNAS, référez-vous à la section dédiée à la **configuration de la sauvegarde**.



3.2) Guide d'exploitation

Cette documentation d'exploitation regroupe l'ensemble des actions que j'ai réalisées moi-même en tant qu'administrateur dans le cadre de la mise en place de l'infrastructure pour IFIDE.

Elle détaille les opérations effectuées sur l'environnement Active Directory, la configuration et le basculement des pools DHCP, la mise en place du DFS et de sa réplication, l'application des stratégies de groupe (GPO), l'implémentation de la solution de sauvegarde avec clichés instantanés vers TrueNAS via iSCSI, ainsi que la configuration du portail captif conforme RGPD via le service RADIUS.

3.2.1) Paramétrage de l'environnement Active Directory

Tout d'abord, nous allons commencer la configuration de l'environnement **Active Directory** en créant les **unités d'organisation (UO)**, les **utilisateurs** et les **groupes**, conformément au cahier des charges.

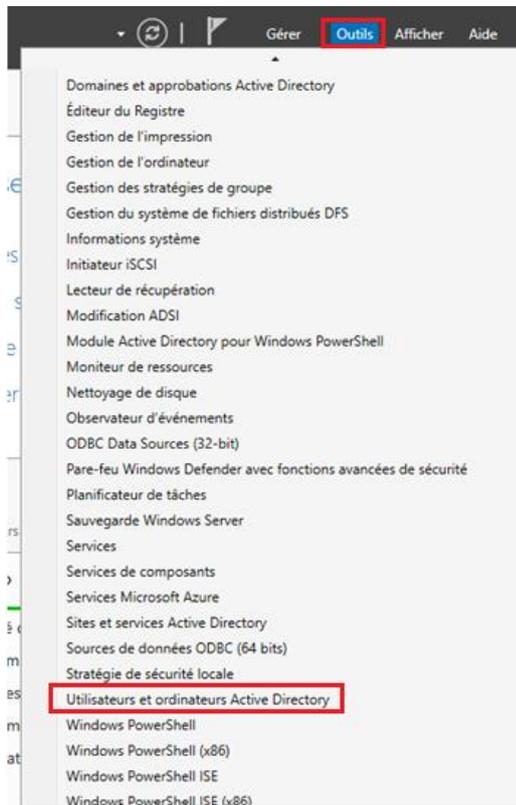
Création des Unités d'Organisation (UO)

Les **Unités d'Organisation (UO)** permettent d'organiser et de hiérarchiser la **forêt Active Directory** de manière structurée.

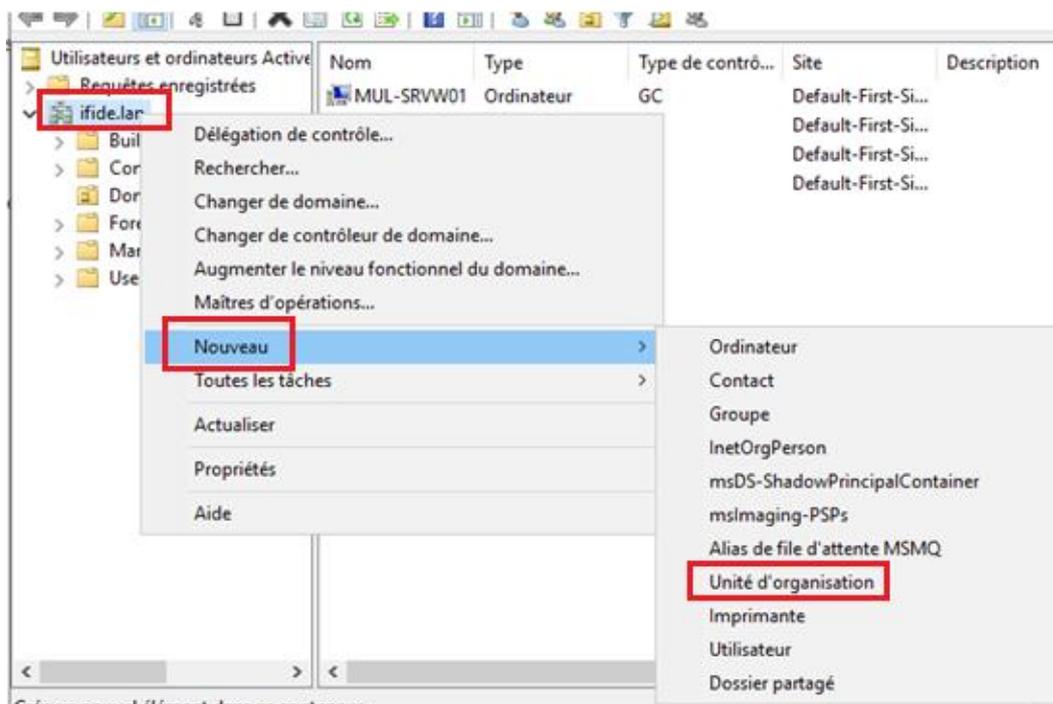
Pour créer une UO, il est possible d'utiliser soit la console **Utilisateurs et ordinateurs Active Directory**, soit **PowerShell**.

Cependant, pour faciliter l'administration, nous utiliserons ici la **console graphique**.

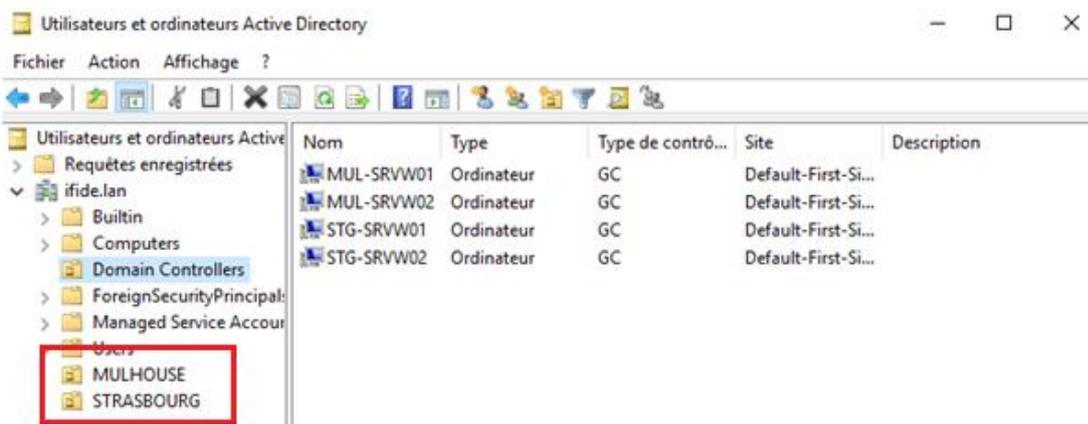
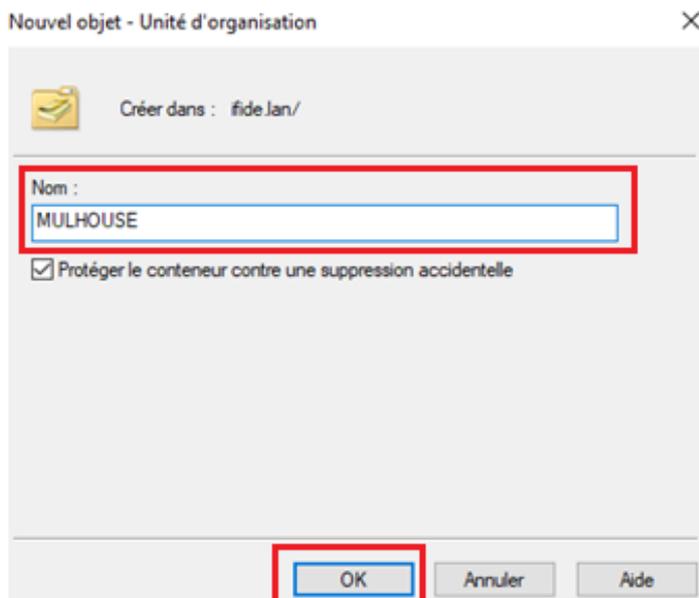
Pour l'ouvrir, accédez au **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.



Ensuite, pour créer une unité d'organisation, effectuez un clic droit sur le nom de votre domaine Active Directory, puis sélectionnez **Nouveau** → **Unité d'organisation** :



Ensuite, saisissez le **nom de l'unité d'organisation**, puis laissez cochée l'option "**Protéger contre les suppressions accidentelles**" afin de prévenir toute mauvaise manipulation dans la console Active Directory.



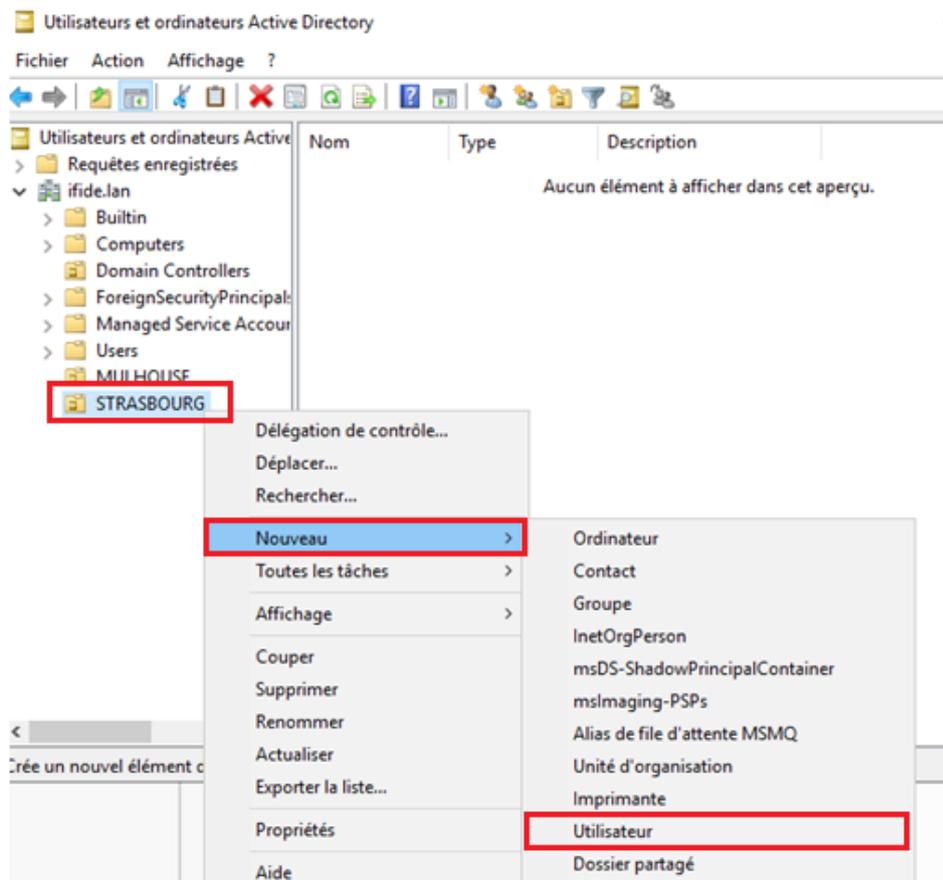
Les unités d'organisation ont été créées correctement.

Création des utilisateurs

Pour créer un utilisateur, positionnez-vous dans l'UO concernée, effectuez un clic droit, puis sélectionnez **Nouveau → Utilisateur**.

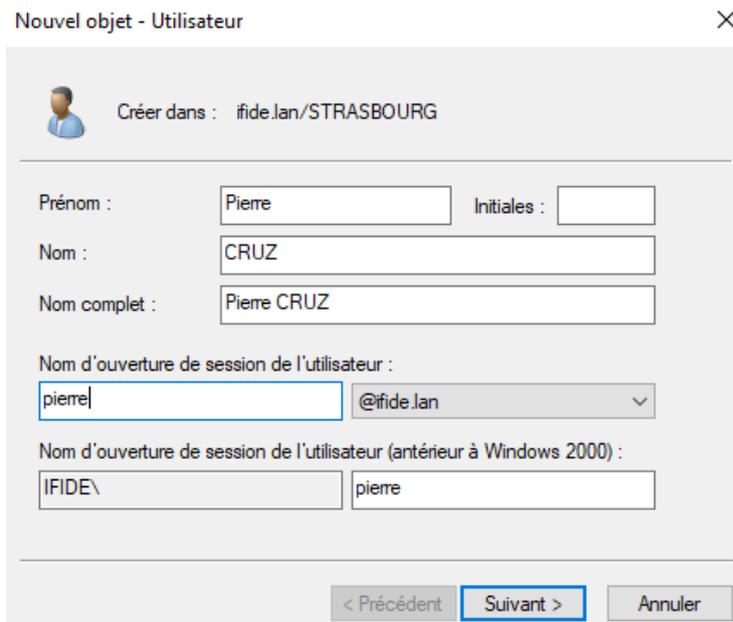
Les utilisateurs à créer sont les suivants :

- Paul et Pierre dans l'UO STRASBOURG
- Isabelle et Nathalie dans l'UO MULHOUSE
- ADMIN à la racine Users du domaine, en tant que compte administrateur de secours.



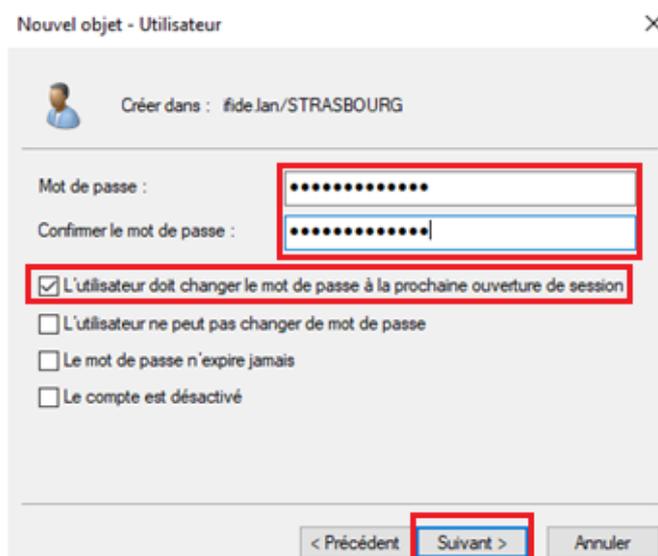
Remplissez ensuite la **fiche de l'utilisateur** pour finaliser sa création (comme dans l'exemple de Pierre).

À noter que les étapes sont identiques pour la création de **n'importe quel utilisateur** dans l'Active Directory.

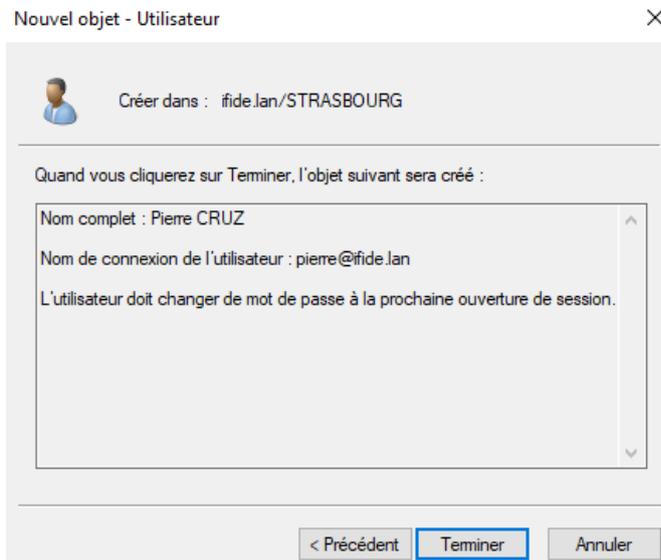


Saisissez ensuite un **mot de passe provisoire** à communiquer à l'utilisateur, puis laissez cochée l'option "**L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**".

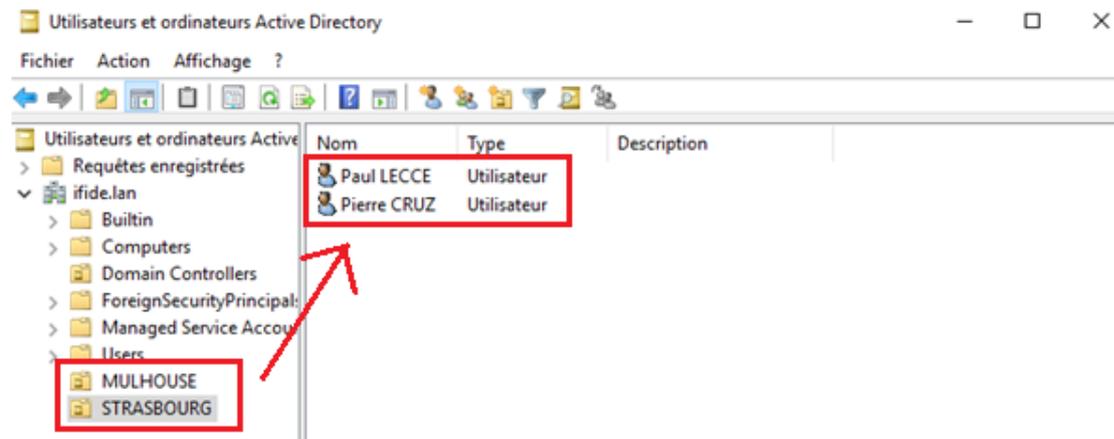
Cela permet à chaque utilisateur de définir un mot de passe personnel, garantissant la **confidentialité de ses données**.



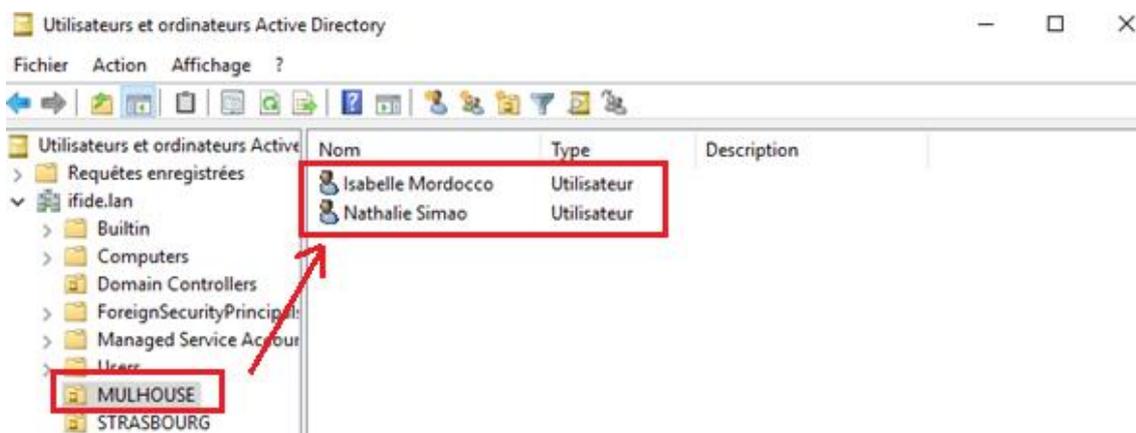
Enfin, cliquez sur **Terminer** pour finaliser la création de l'utilisateur.



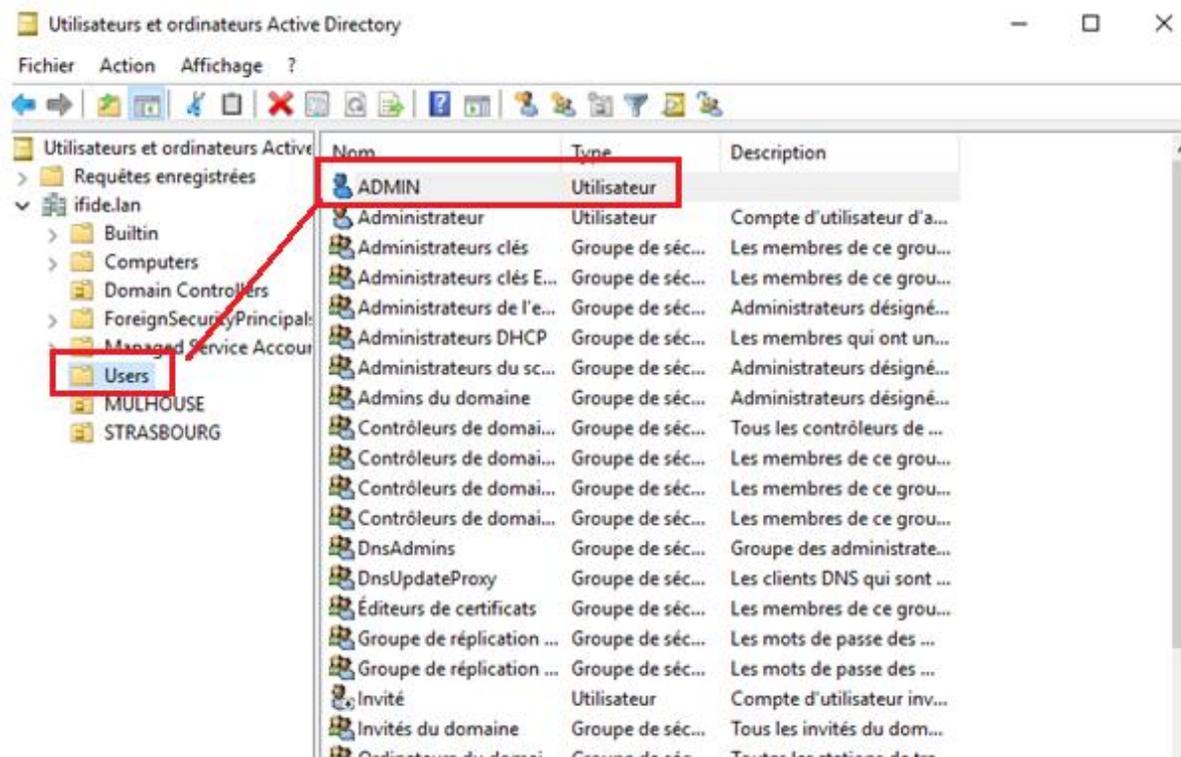
Utilisateurs créés dans l'UO STRASBOURG



Utilisateurs créés dans l'UO MULHOUSE



L'utilisateur ADMIN créé dans la racine



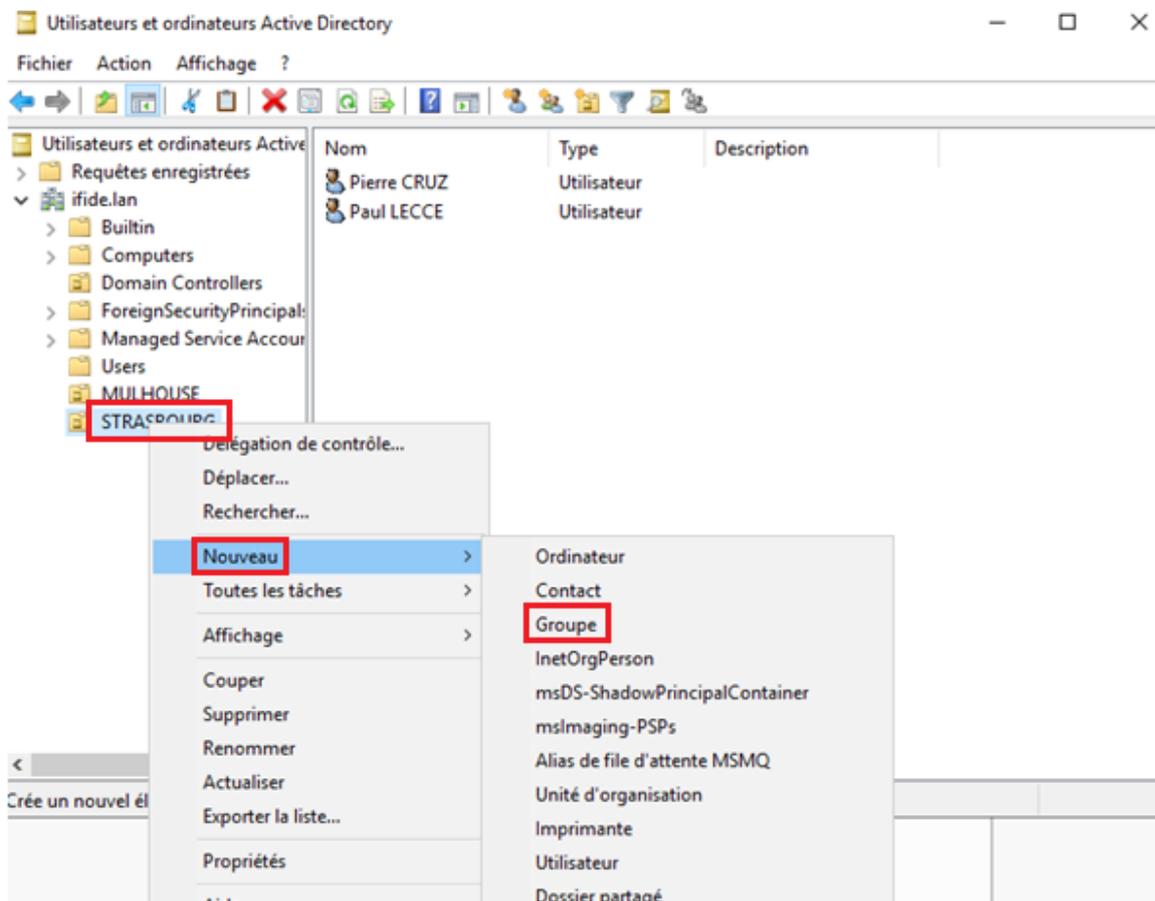
Maintenant que les utilisateurs ont été créés, nous pouvons passer à la **création des groupes**.

Création des groupes

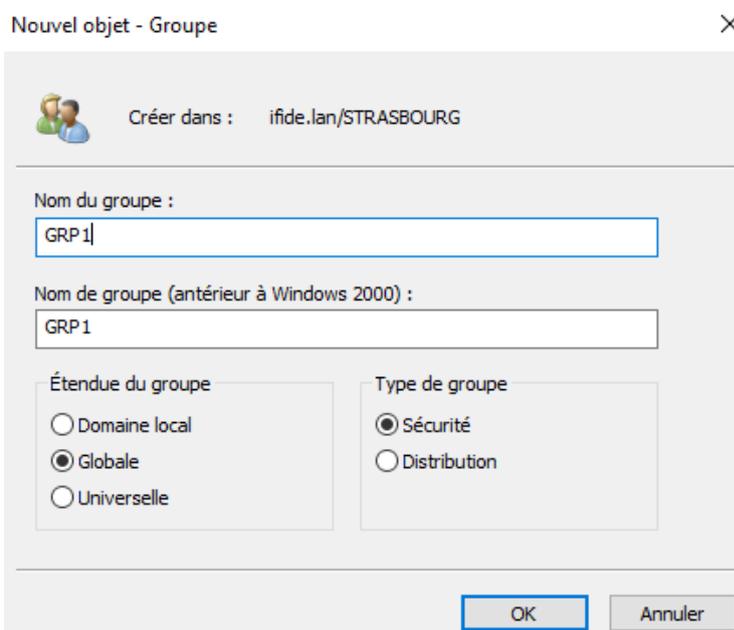
Pour créer un groupe, sélectionnez l'UO souhaitée, effectuez un clic droit, puis cliquez sur **Nouveau → Groupe**.

Les groupes à créer sont les suivants :

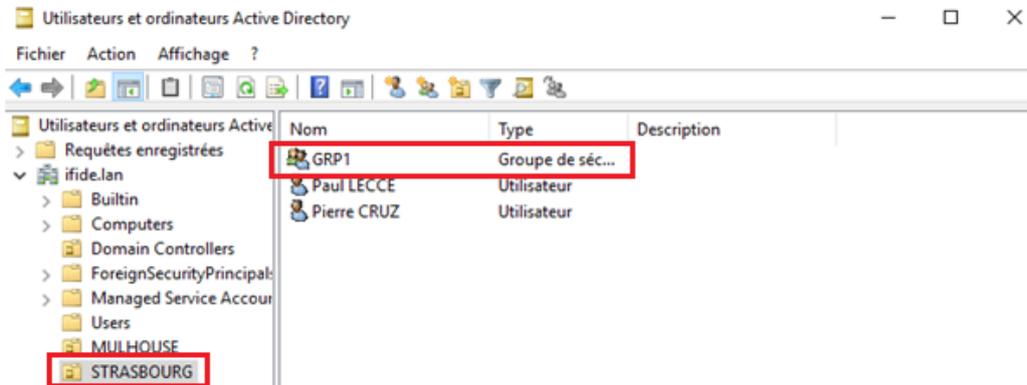
- GRP1 dans l'UO STRASBOURG
- GRP2 dans l'UO MULHOUSE
- RADIUS_Allow à la racine du domaine, pour les utilisateurs autorisés à se connecter au portail captif.



Ensuite, saisissez le **nom du groupe**, cliquez sur **OK**, et la **création du groupe** sera effectuée.

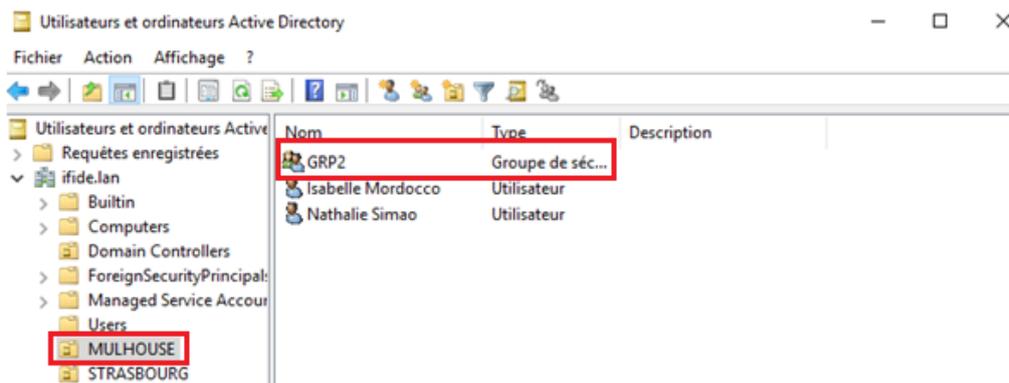


STRASBOURG



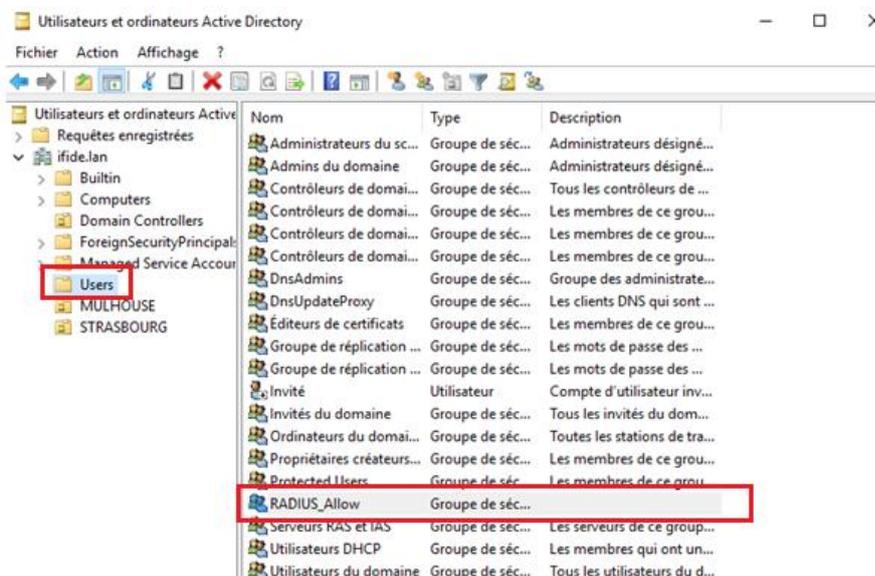
Nom	Type	Description
GRP1	Groupe de séc...	
Paul LECCE	Utilisateur	
Pierre CRUZ	Utilisateur	

MULHOUSE



Nom	Type	Description
GRP2	Groupe de séc...	
Isabelle Mordocco	Utilisateur	
Nathalie Simao	Utilisateur	

LA RACINE



Nom	Type	Description
Administrateurs du sc...	Groupe de séc...	Administrateurs désigné...
Admins du domaine	Groupe de séc...	Administrateurs désigné...
Contrôleurs de domai...	Groupe de séc...	Tous les contrôleurs de ...
Contrôleurs de domai...	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domai...	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domai...	Groupe de séc...	Les membres de ce grou...
DnsAdmins	Groupe de séc...	Groupe des administrate...
DnsUpdateProxy	Groupe de séc...	Les clients DNS qui sont ...
Éditeurs de certificats	Groupe de séc...	Les membres de ce grou...
Groupe de réplication ...	Groupe de séc...	Les mots de passe des ...
Groupe de réplication ...	Groupe de séc...	Les mots de passe des ...
Invité	Utilisateur	Compte d'utilisateur inv...
Invités du domaine	Groupe de séc...	Tous les invités du dom...
Ordinateurs du domai...	Groupe de séc...	Toutes les stations de tra...
Propriétaires créateurs...	Groupe de séc...	Les membres de ce grou...
Protected Users	Groupe de séc...	Les membres de ce grou...
RADIUS_Allow	Groupe de séc...	
Serveurs RAS et IAS	Groupe de séc...	Les serveurs de ce group...
Utilisateurs DHCP	Groupe de séc...	Les membres qui ont un...
Utilisateurs du domaine	Groupe de séc...	Tous les utilisateurs du d...

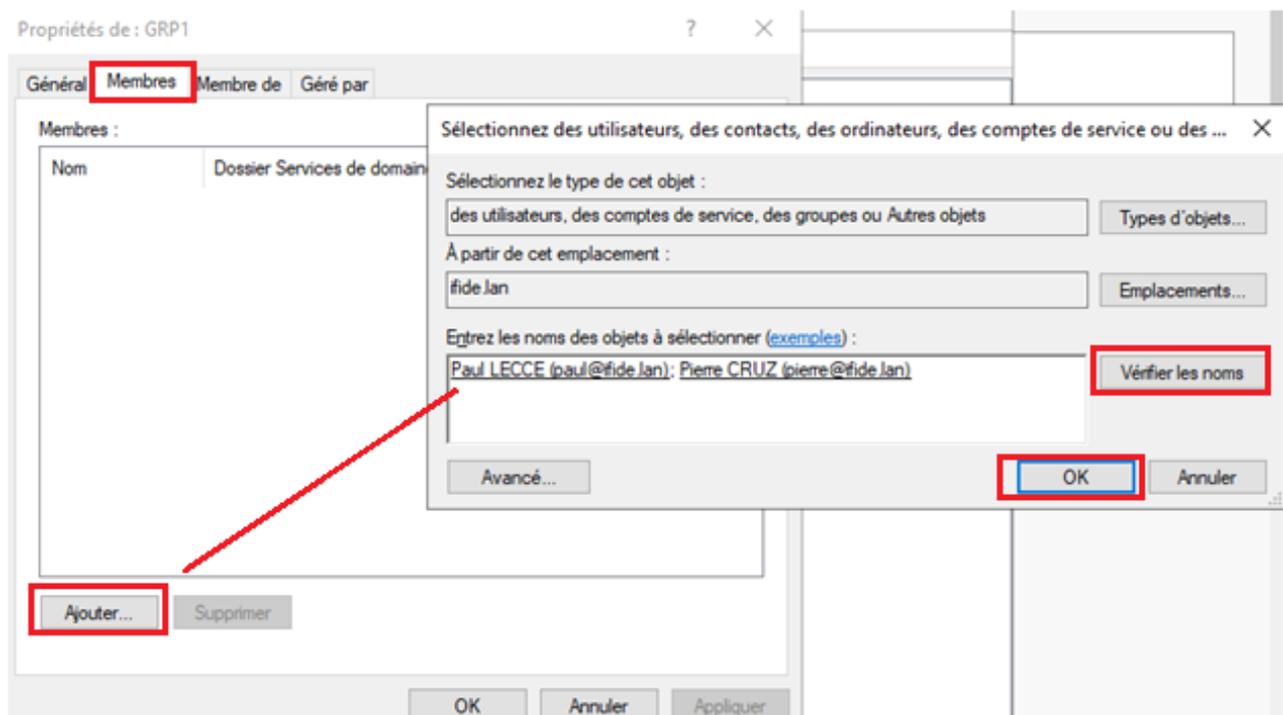
Ajout des utilisateurs dans leurs groupes

Enfin, les dernières opérations à réaliser dans la console Active Directory consistent à ajouter les utilisateurs dans leurs groupes respectifs. Les actions à effectuer sont les suivantes :

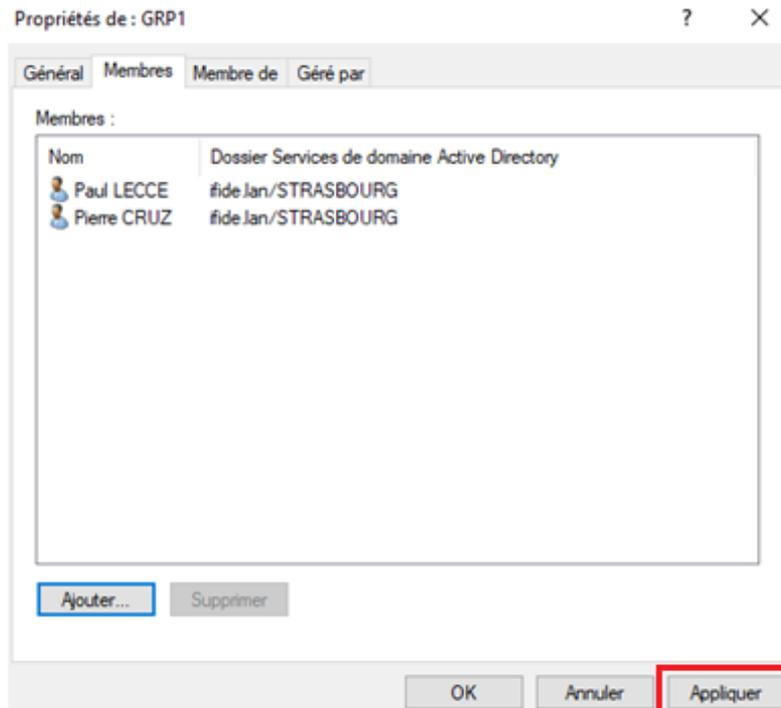
- Ajouter Paul et Pierre dans le groupe GRP1
- Ajouter Nathalie et Isabelle dans le groupe GRP2
- Ajouter l'utilisateur ADMIN dans le groupe Administrateurs

Pour cela, il est possible de passer soit par les fiches utilisateurs, soit directement par les groupes.

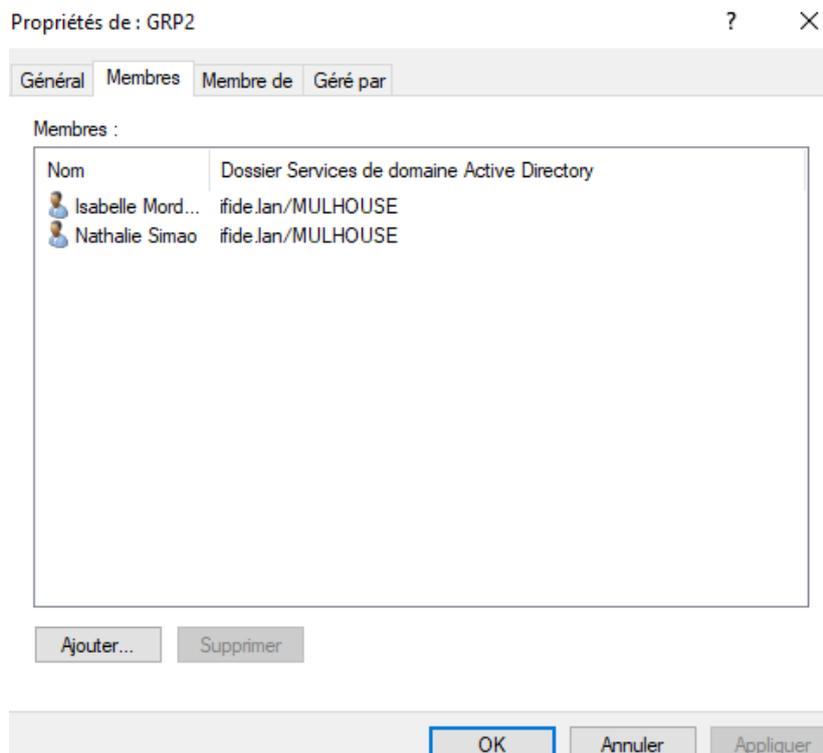
Dans notre cas, nous passerons par les groupes : double-cliquez sur le groupe concerné, cliquez sur l'onglet **Membres**, puis sur **Ajouter**. Sélectionnez les utilisateurs à inclure et validez avec OK.



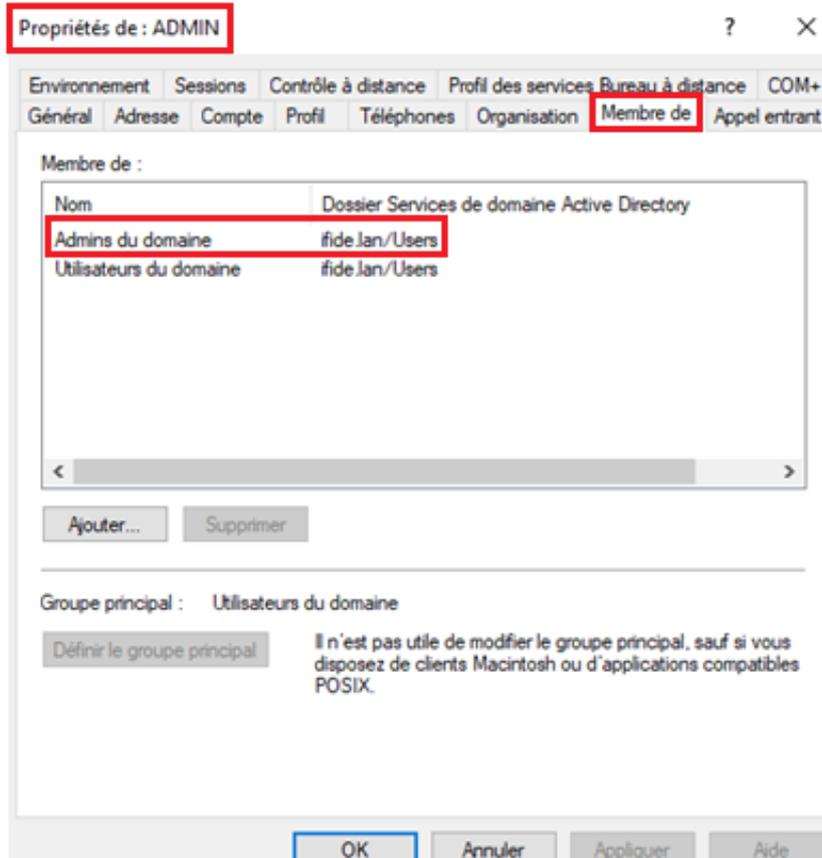
Enfin, cliquez sur **Appliquer** puis **OK** pour finaliser l'ajout des membres au groupe.



Membres du groupe GRP2 :



Groupe de l'utilisateur ADMIN



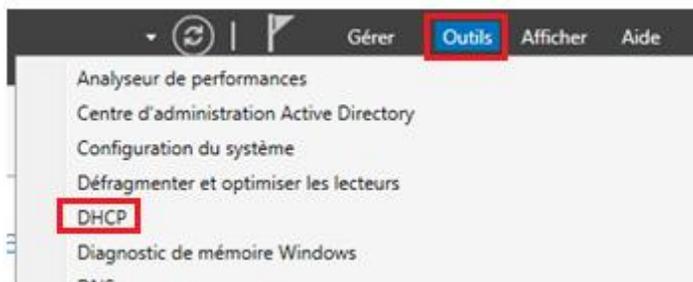
L'ajout des utilisateurs dans leurs groupes respectifs a été effectué avec succès.

3.2.2) Mise en place du pool DHCP et de son basculement

Dans cette partie, nous allons créer les pools DHCP correspondant aux plages d'adresses IP destinées aux machines clientes du réseau. Ensuite, nous mettrons en place le basculement DHCP afin d'assurer une haute disponibilité du service en cas de défaillance d'un des serveurs.

Configuration des étendues DHCP

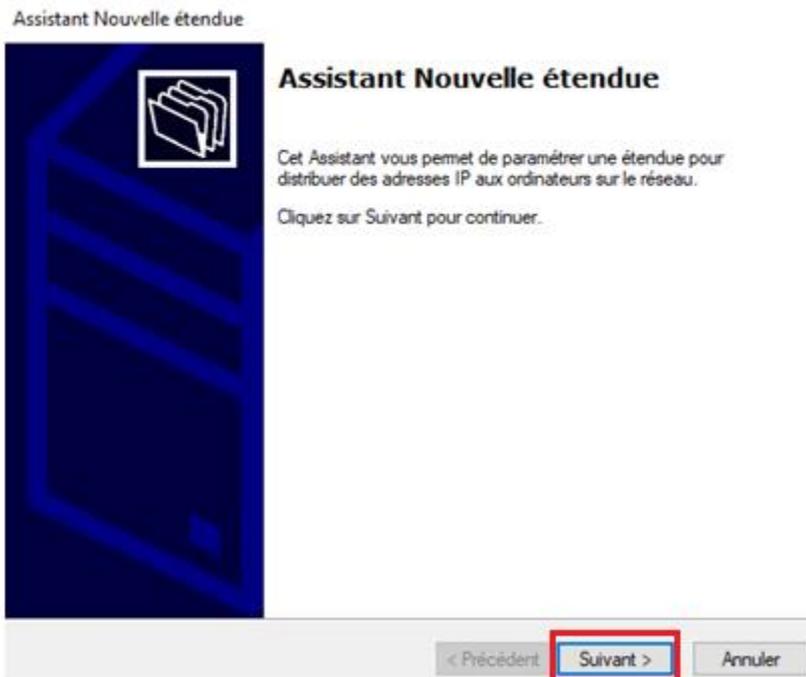
Pour configurer une étendue DHCP sur le serveur, nous utiliserons la console d'administration dédiée plutôt que PowerShell. Pour cela, rendez-vous dans le **Gestionnaire de serveurs**, puis cliquez sur **Outils** → **DHCP** afin d'ouvrir la console de gestion du service DHCP.



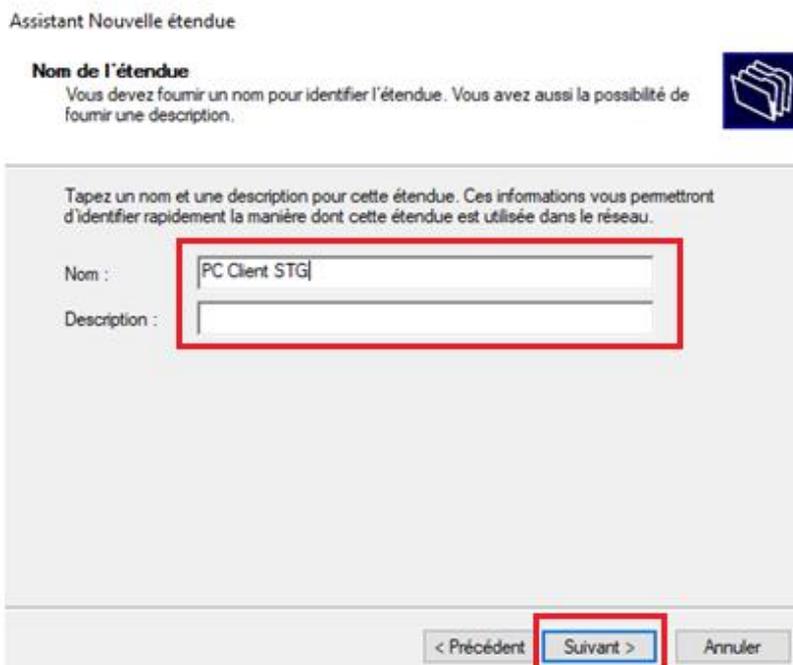
Pour créer une nouvelle étendue, effectuez un **clic droit sur "IPv4"**, puis sélectionnez **"Nouvelle étendue"**.



Une fenêtre d'assistant de configuration s'ouvre, cliquez sur **Suivant** et poursuivez les étapes décrites ci-dessous pour configurer l'étendue DHCP.



Nommez ensuite le pool DHCP. Dans notre cas, pour Strasbourg, nous l'appellerons **PC Client STG**.



Définissez ensuite l'étendue du pool DHCP conformément au **tableau d'adressage** et au **schéma réseau** :

- Pour **Strasbourg** → 192.168.100.50 - 192.168.100.150 (masque /24)
- Pour **Mulhouse** → 192.168.200.50 - 192.168.200.150 (masque /24)

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 :

Comme l'étendue définie ne chevauche pas les adresses IP réservées aux serveurs, vous pouvez passer l'étape d'**exclusion d'adresse**. Cliquez alors sur **Suivant**.

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

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



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

Adresse IP de début : . . . Adresse IP de fin : . . .

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

Ensuite, définissez la **durée du bail DHCP**. Par défaut, elle est fixée à **8 jours**. Dans notre cas, nous allons l'étendre à **14 jours** afin de garantir une attribution stable des adresses IP pendant deux semaines.

Assistant Nouvelle étendue

Durée du bail

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



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

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

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

Limitée à :

Jours : Heures : Minutes :

< Précédent **Suivant >** Annuler

L'assistant vous demandera ensuite si vous souhaitez configurer les **options DHCP** de l'étendue (passerelle par défaut, serveur DNS et serveur WINS pour les clients). Cochez "**Oui, je souhaite configurer ces options maintenant**", puis cliquez sur **Suivant**.

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

- Oui, je veux configurer ces options maintenant

 Non, je configurerai ces options ultérieurement

< Précédent **Suivant >** Annuler

Pour la **passerelle par défaut**, saisissez l'adresse IP du routeur correspondant :

- Pour le réseau **Strasbourg (STG)** : 192.168.100.254 (RTE-STG01)
- Pour le réseau **Mulhouse (MUL)** : 192.168.200.254 (RTE-MUL01)

Cliquez ensuite sur **Ajouter**, puis sur **Suivant**.

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

À cette étape, seule l'adresse IP du contrôleur de domaine principal (192.168.100.1) est renseignée. Les autres adresses DNS seront ajoutées manuellement. Nom de domaine : ifide.lan

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text" value="192.168.100.1"/>	<input type="button" value="Ajouter"/>
<input type="button" value="Résoudre"/>		<input type="button" value="Supprimer"/>
		<input type="button" value="Monter"/>
		<input type="button" value="Descendre"/>

< Précédent

Nous pouvons nous passer de l'utilisation des serveurs WINS, cliquez simplement sur **Suivant**.

Assistant Nouvelle étendue

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.



Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text"/>	<input type="button" value="Ajouter"/>
<input type="button" value="Résoudre"/>		<input type="button" value="Supprimer"/>
		<input type="button" value="Monter"/>
		<input type="button" value="Descendre"/>

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent

PROJET 1

Enfin, laissez cochée l'option **Oui** pour activer l'étendue immédiatement, cliquez sur **Suivant**, puis sur **Terminer**.

Assistant Nouvelle étendue

Activer l'étendue

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



Voulez-vous activer cette étendue maintenant ?

Oui, je veux activer cette étendue maintenant.

Non, j'activerai cette étendue ultérieurement

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue



Fin de l'Assistant Nouvelle étendue

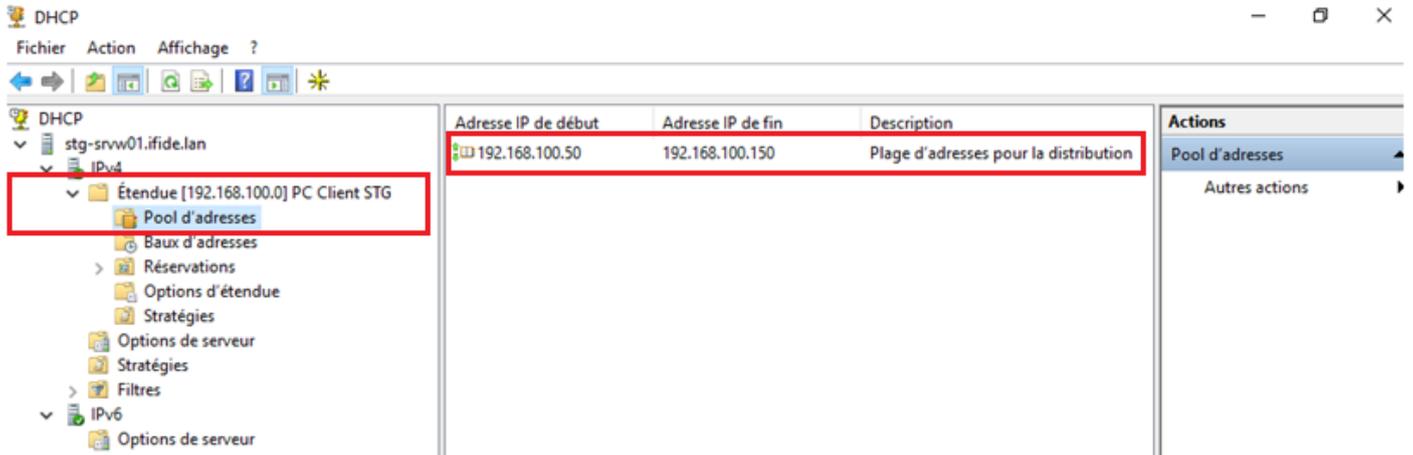
L'Assistant Nouvelle étendue s'est terminé correctement.

Pour offrir une haute disponibilité pour cette étendue, configurez le basculement pour l'étendue nouvellement ajoutée en cliquant avec le bouton droit sur l'étendue, puis en cliquant sur Configurer un basculement.

Pour fermer cet Assistant, cliquez sur Terminer.

< Précédent **Terminer** Annuler

L'étendue a été créée correctement et est désormais active sur le serveur DHCP.



Comme mentionné précédemment, il est maintenant temps de procéder à la **configuration du basculement DHCP** sur les serveurs Core.

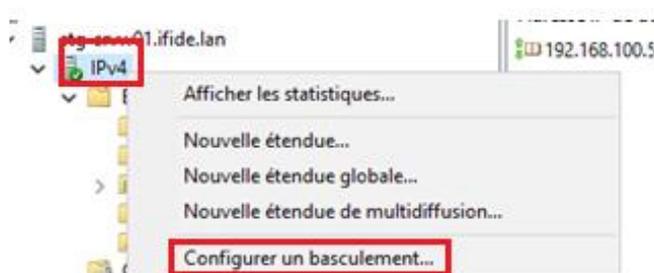
Conformément au cahier des charges et à la section dédiée à l'installation du rôle DHCP, ce rôle doit être présent sur **l'ensemble des serveurs** afin d'assurer la haute disponibilité du service

Configuration du basculement DHCP

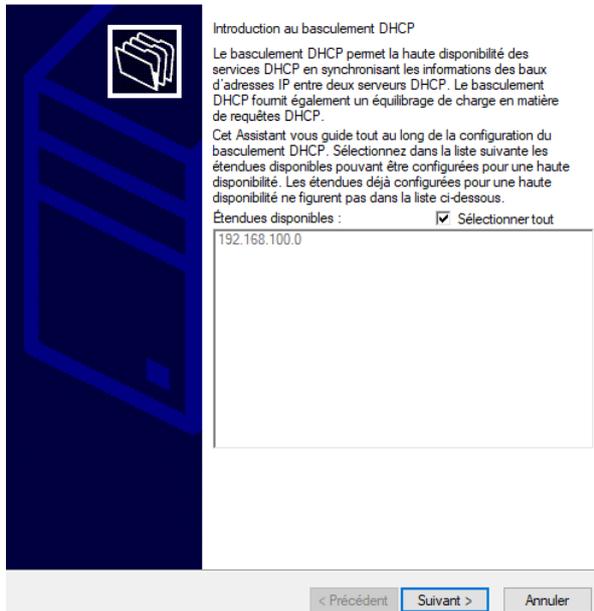
Pour configurer le basculement DHCP, ouvrez la console DHCP depuis le serveur principal.

Faites un clic droit sur "IPv4", puis sélectionnez "**Configurer un basculement**".

Une fenêtre de configuration s'ouvrira, cliquez sur **Suivant** pour continuer.



Configurer un basculement



Introduction au basculement DHCP

Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.

Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.

Étendues disponibles : Sélectionner tout

192.168.100.0

< Précédent Suivant > Annuler

Ensuite, sélectionnez le **serveur DHCP partenaire** pour le basculement. Dans le cas du serveur **STG-SRVW01**, le partenaire sera **STG-SRVW02**, c'est-à-dire le **deuxième serveur** du site de Strasbourg.

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



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

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

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

Serveur partenaire : Ajouter un serveur

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

< Précédent Suivant > Annuler

Configurez ensuite le mode de basculement DHCP.

Dans notre cas, nous sélectionnons le mode **Équilibrage de charge**, afin que **les deux serveurs DHCP restent actifs en permanence**. Cela garantit une haute disponibilité du service : si le serveur principal devient indisponible, le serveur secondaire prendra automatiquement le relais avec **100 % de la charge**.

À noter : le mode *Serveur de secours* peut être utilisé dans d'autres contextes, mais il n'active le second serveur qu'en cas de panne du principal.

Enfin, pour renforcer la sécurité de la synchronisation entre les deux serveurs, **renseignez un secret partagé** (mot de passe commun) à cette étape.

Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire stg-srvw02

Nom de la relation :

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

Mode :

Pourcentage d'équilibrage de charge

Serveur local : %

Serveur partenaire : %

Intervalle de basculement d'état : minutes

Activer l'authentification du message

Secret partagé :

< Précédent **Suivant >** Annuler

Configurer un basculement

Un basculement va être configuré entre stg-srvw01.fide.lan et stg-srvw02 avec les paramètres suivants.

Étendus :

Nom de la relation : stg-srvw01.fide.lan-stg-srvw02

Délai de transition maximal du client (MCLT) : 1 h 0 min

Mode : Équilibrage de charge

Intervalle de basculement d'état : Désactivé

Pourcentage d'équilibrage de charge

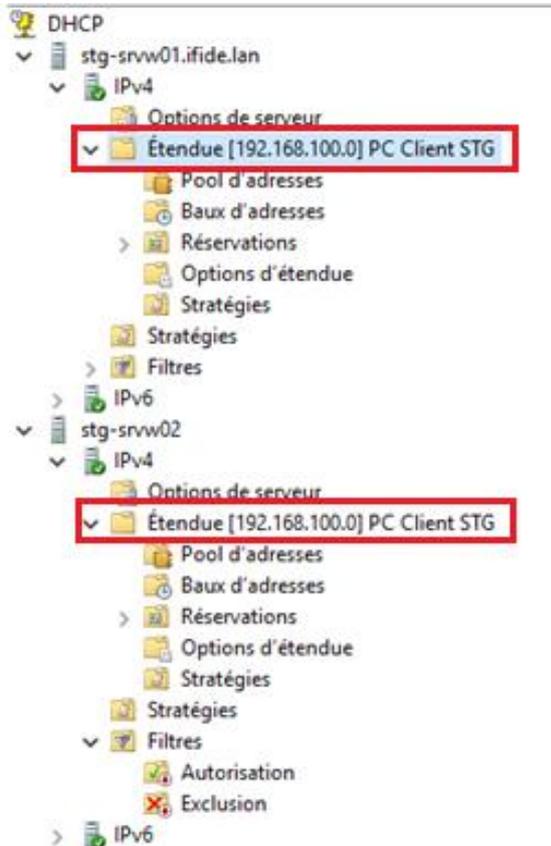
Serveur local : 50 %

Serveur partenaire : 50 %

< Précédent **Terminer** Annuler

Cliquez enfin sur **Terminer** pour finaliser la configuration du basculement DHCP.

Une fois cette opération effectuée, en ajoutant le second serveur DHCP à la console, on peut constater que le **basculement DHCP a bien été pris en compte et est actif** sur les deux serveurs concernés.



Le serveur secondaire STG-SRVW02 a bien récupéré l'étendue DHCP configurée sur STG-SRVW01, validant ainsi la mise en place du basculement DHCP pour le site de Strasbourg.

À présent, nous allons passer à la phase de vérification du bon fonctionnement du service DHCP, ainsi que du basculement DHCP entre les serveurs configurés.

Test du fonctionnement DHCP

Test service DHCP

Pour vérifier le bon fonctionnement du service DHCP, connectez une machine cliente au réseau LAN de Strasbourg ou de Mulhouse.

Pour réaliser les différents tests liés au fonctionnement du service DHCP et au basculement, nous allons utiliser les **machines clientes STG-W202201 et MUL-W202201**, qui avaient été **préparées en amont** au début du projet.

Ces postes clients, positionnés respectivement sur les **réseaux LAN de Strasbourg et de Mulhouse**, serviront à **vérifier l'attribution dynamique d'adresses IP**, ainsi que le **comportement des serveurs en cas de basculement**.

Depuis cette machine, ouvrez l'invite de commande et exécutez les commandes suivantes :

```
Ipconfig /release
```

Cette commande permet de **libérer l'adresse IP** actuellement attribuée à la machine cliente par le serveur DHCP (**DHCP Release**).

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

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . .: fe80::20e9:29bf:b3b1:4bd9%4
    Passerelle par défaut. . . . . :
```

Ensuite, exécutez la commande suivante pour **initier une nouvelle demande d'adresse IP** auprès du serveur DHCP présent sur le réseau.

Cette commande déclenchera la séquence classique : **DHCP Discover → DHCP Offer → DHCP Request → DHCP Ack**.

```
Ipconfig /renew
```

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

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : ifide.lan
    Adresse IPv6 de liaison locale. . . . : fe80::20e9:29bf:b3b1:4bd9%4
    Adresse IPv4. . . . . : 192.168.100.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

Enfin, en exécutant la commande **ipconfig /all**, on obtient des informations détaillées telles que l'adresse du serveur DHCP émetteur, la durée de bail attribuée, la passerelle par défaut, ainsi que le suffixe DNS du domaine.

```
Configuration IP de Windows

Nom de l'hôte . . . . . : STG-W202201
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: ifide.lan

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : ifide.lan
    Description. . . . . : Intel(R) 82574L Gigabit Network Connection
    Adresse physique . . . . . : 00-0C-29-CC-43-20
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale . . . . : fe80::20e9:29bf:b3b1:4bd9%4 (préféré)
    Adresse IPv4. . . . . : 192.168.100.100 (préféré)
    Masque de sous-réseau . . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 24 avr11 2025 12:30:42
    Bail expirant. . . . . : jeudi 8 mai 2025 12:30:41
    Passerelle par défaut. . . . . :
    Serveur DHCP . . . . . : 192.168.100.2
    IAID DHCPv6 . . . . . : 100666409
    DUID de client DHCPv6. . . . . : 00-01-00-01-2F-9B-C8-27-00-0C-29-CC-43-20
    Serveurs DNS. . . . . : 192.168.100.1
    NetBIOS sur Tcpi. . . . . : Activé
```

Adresse IP reçu par le serveur

Durée et détails du bail DHCP

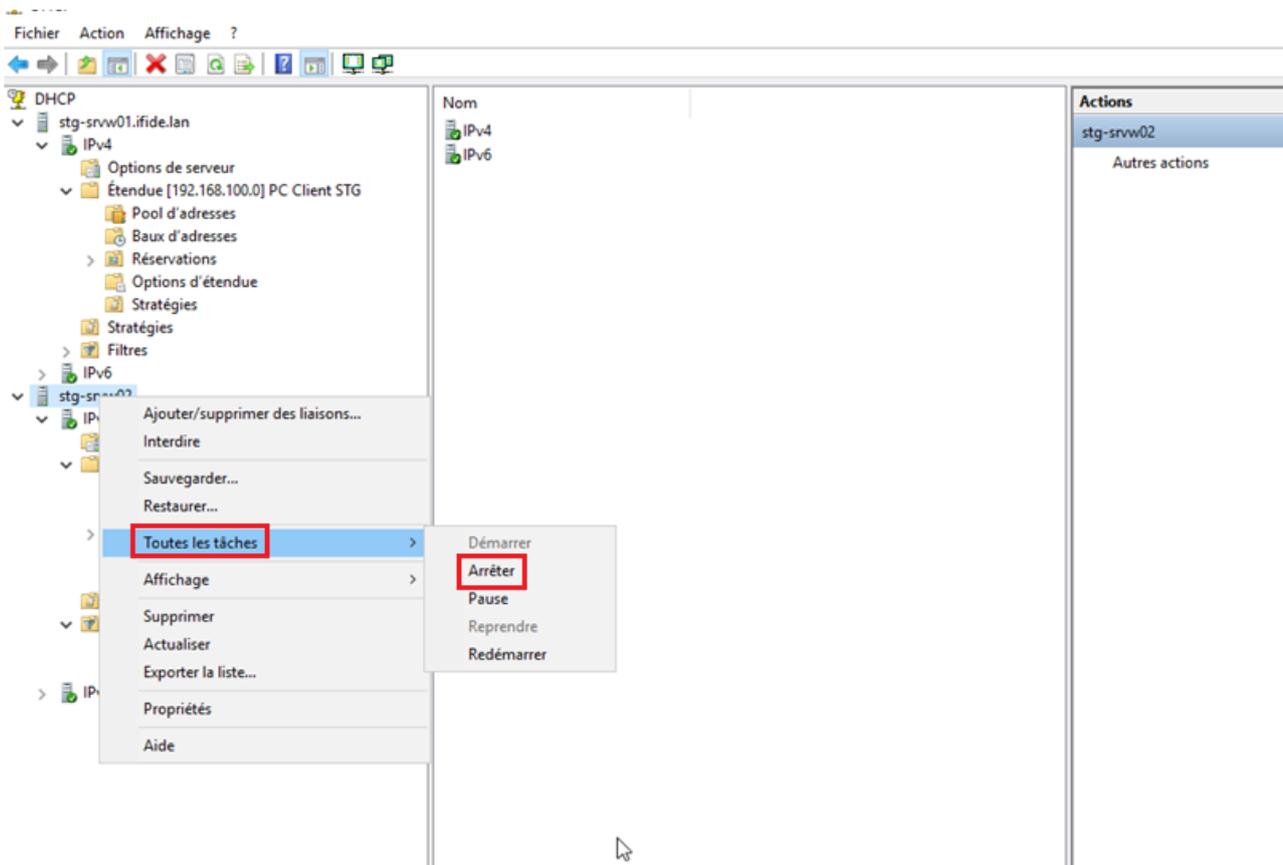
Le serveur DHCP (ici STG-SRVW02)

Le serveur DHCP est pleinement fonctionnel et distribue correctement les adresses IP aux machines clientes.

Test basculement DHCP

Afin de vérifier que le basculement DHCP fonctionne correctement, il suffit de simuler l'arrêt du service DHCP sur le serveur principal. Pour cela, faites un clic droit sur ce serveur dans la console DHCP, cliquez sur "**Toutes les tâches**", puis sélectionnez "**Arrêter**". Ensuite, relancez une demande d'adresse IP depuis une machine cliente et observez si le serveur secondaire prend le relais.

Dans mon cas, j'arrête le serveur DHCP **STG-SRVW02**, étant donné que c'est lui qui a attribué l'adresse IP à la machine cliente, afin de vérifier si **STG-SRVW01** prend bien le relais.



Le serveur DHCP STG-SRVW01 est à présent hors service afin de simuler une panne.

À présent, sur une machine cliente, effectuez à nouveau une demande d'adresse IP via DHCP en utilisant les commandes mentionnées précédemment.

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

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::20e9:29bf:b3b1:4bd9%4
    Passerelle par défaut. . . . . :

C:\Users\Administrateur>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . : ifide.lan
    Adresse IPv6 de liaison locale. . . . . : fe80::20e9:29bf:b3b1:4bd9%4
    Adresse IPv4. . . . . : 192.168.100.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

Les machines clientes parviennent à obtenir une adresse IP, confirmant ainsi le bon fonctionnement du service DHCP.

Et en visualisant les informations par `ipconfig /all` :

```
Configuration IP de Windows

Nom de l'hôte . . . . . : STG-W202201
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: ifide.lan

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . : ifide.lan
    Description. . . . . : Intel(R) 82574L Gigabit Network Connection
    Adresse physique . . . . . : 00-0C-29-CC-43-20
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::20e9-29bf-b3b1-4bd9%4(préféré)
    Adresse IPv4. . . . . : 192.168.100.100(préféré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 24 avril 2025 12:44:04
    Bail expirant. . . . . : jeudi 8 mai 2025 12:44:03
    Passerelle par défaut. . . . . :
    Serveur DHCP . . . . . : 192.168.100.1
    ID DHCPv6 . . . . . : 10000469
    DUID de client DHCPv6. . . . . : 00-01-00-01-2F-9B-C8-27-00-0C-29-CC-43-20
    Serveurs DNS. . . . . : 192.168.100.1
    NetBIOS sur Tcpip. . . . . : Activé
```

Adresse obtenue via le serveur DHCP et détails du bail DHCP.

Serveur DHCP émetteur : (STG-SRVW01)

Le basculement DHCP a été réalisé correctement.

Bien évidemment, cette procédure doit être reproduite à l'identique sur le site de Mulhouse, en configurant l'étendue DHCP sur MUL-SRVW01 et en mettant en place le basculement vers MUL-SRVW02.

MULHOUSE

DHCP

Fichier Action Affichage ?

	Adresse IP de début	Adresse IP de fin	Description	Actions
<ul style="list-style-type: none"> ▼ DHCP ▼ mul-srvw01.ifide.lan <ul style="list-style-type: none"> ▼ IPv4 <ul style="list-style-type: none"> ▼ Étendue [192.168.200.0] PC Client MUL <ul style="list-style-type: none"> Pool d'adresses Baux d'adresses > Réservations Options d'étendue Stratégies Options de serveur Stratégies > Filtres > IPv6 	192.168.200.50	192.168.200.150	Plage d'adresses pour la distribution	<ul style="list-style-type: none"> Pool d'adresses Autres actions

DHCP

- ▼ mul-srvw01.ifide.lan
 - ▼ IPv4
 - ▼ Étendue [192.168.200.0] PC Client MUL
 - Pool d'adresses
 - Baux d'adresses
 - > Réservations
 - Options d'étendue
 - Stratégies
 - Options de serveur
 - Stratégies
 - > Filtres
- ▼ mul-srvw02
 - ▼ IPv4
 - ▼ Étendue [192.168.200.0] PC Client MUL
 - Pool d'adresses
 - Baux d'adresses
 - > Réservations
 - Options d'étendue
 - Stratégies
 - Options de serveur
 - Stratégies
 - > Filtres
 - > IPv6

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

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::146d:70d4:eb68:8e05%4
    Passerelle par défaut. . . . . :
```

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

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . : ifide.lan
    Adresse IPv6 de liaison locale. . . . . : fe80::146d:70d4:eb68:8e05%4
    Adresse IPv4. . . . . : 192.168.200.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.200.254
```

```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : MUL-W202201
    Suffixe DNS principal . . . . . :
    Type de noeud. . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: ifide.lan

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . : ifide.lan
    Description. . . . . : Intel(R) 82574L Gigabit Network Connection
    Adresse physique . . . . . : 00-0C-29-00-3F-9C
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::146d:70d4:eb68:8e05%4(préfééré)
    Adresse IPv4. . . . . : 192.168.200.100(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 24 avril 2025 13:10:52
    Bail expirant. . . . . : jeudi 24 avril 2025 14:10:52
    Passerelle par défaut. . . . . : 192.168.200.254
    Serveur DHCP . . . . . : 192.168.200.2
    IAID DHCPv6 . . . . . : 100666409
    DUID de client DHCPv6. . . . . : 00-01-00-01-2F-9B-D3-46-00-0C-29-00-3F-9C
    Serveurs DNS. . . . . : 192.168.100.1
    NetBIOS sur Tcpip . . . . . : Activé
```

Le serveur DHCP pour MULHOUSE est pleinement fonctionnel et distribue correctement les adresses IP aux machines clientes.

3.2.3) Configuration du partage DFS et de la réplication DFSR

Maintenant que les utilisateurs ont été créés et que le service DHCP est configuré, nous allons passer à l'étape suivante : la mise en place des partages via DFS, ainsi que la configuration de la réplication des données à l'aide de DFSR (Distributed File System Replication).

Maintenant que nous avons créé les utilisateurs et configuré le service DHCP, nous allons entamer la **configuration des partages sous DFS**, ainsi que la mise en place de la **réplication des données via DFSR**.

Tout d'abord, dans une logique de **bonne pratique**, il est recommandé de **séparer la partition système** (le disque local C:\) des **données exploitées par l'entreprise** (documents partagés, travaux à rendre, cours, etc.).

C'est pourquoi un **second disque** a été prévu dans la configuration matérielle.

Ainsi, avant de procéder à la création des partages, nous commencerons par **initialiser et partitionner ce second disque**, qui sera utilisé comme **lecteur D:\ dédié aux données**.

Gestion des disques

Pour la gestion des disques, plusieurs options sont possibles :

- Utiliser le Gestionnaire de disques Windows via la commande diskmgmt.msc
- Utiliser l'utilitaire Diskpart, efficace mais nécessitant une certaine aisance en ligne de commande
- Utiliser PowerShell, particulièrement adapté aux administrateurs familiers de cet environnement
- Ou encore utiliser le Gestionnaire des disques/volumes intégré au Gestionnaire de serveur

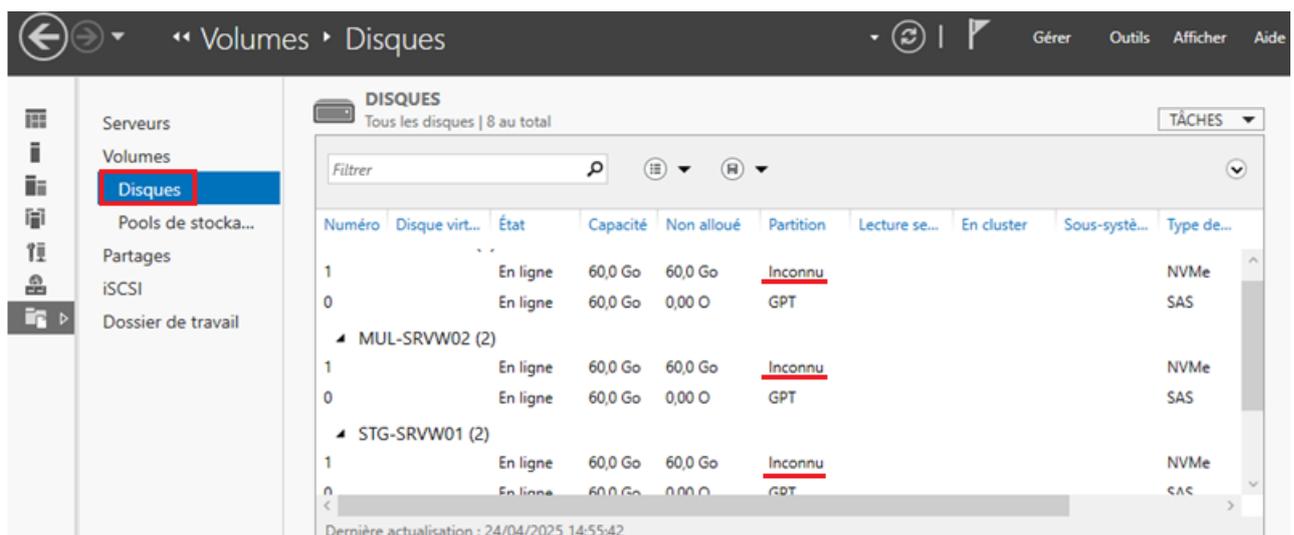
Dans cette documentation, et afin de faciliter l'administration, nous opterons pour l'interface du Gestionnaire de serveur, qui permet de visualiser rapidement l'état des disques présents et disponibles sur chaque serveur géré.

Initialisation des disques

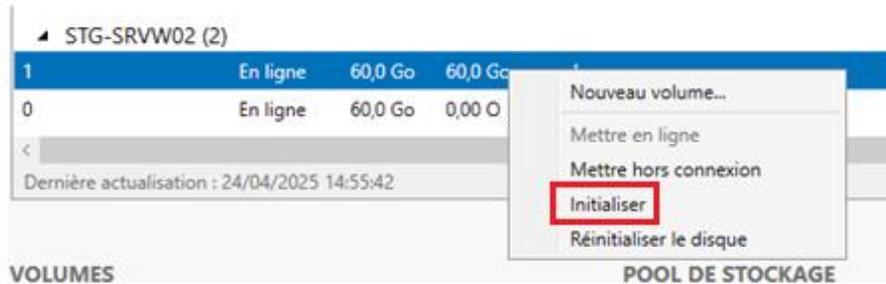
Pour commencer, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Services de fichiers et de stockage**.



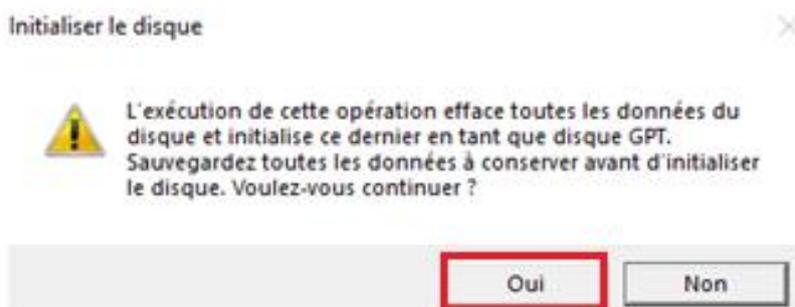
Ensuite, cliquez sur **Disques**. Les disques non partitionnés apparaîtront alors avec le statut **Inconnu**.



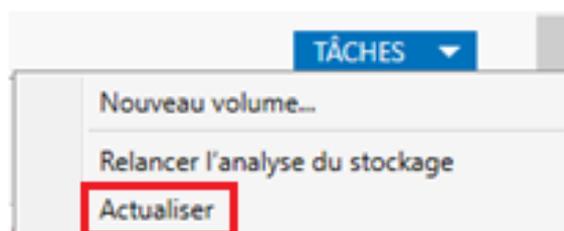
Puis, sélectionnez l'un des disques non partitionnés, effectuez un **clic droit**, puis cliquez sur **Initialiser le disque**.



Une fenêtre s'affichera pour vous proposer l'initialisation du disque. Sélectionnez le format **GPT**, recommandé par défaut dans le Gestionnaire de serveur, car le format **MBR est désormais obsolète**. Cliquez ensuite sur **OK** pour valider.



Enfin, actualiser la Gestion des disques en cliquant sur **Tâches** puis **Actualiser**, afin de visualiser si les disques sont bel et bien initialisés au format GPT.



DISQUES
Tous les disques | 8 au total

Filtrer

Numéro	Disque virt...	État	Capacité	Non alloué	Partition	Lecture se...	En cluster	Sous-systè...	Type de...
1		en ligne	60,0 Go	0,00 O	GPT				NVMe
0		En ligne	60,0 Go	0,00 O	GPT				SAS
▲ STG-SRVW01 (2)									
1		En ligne	60,0 Go	60,0 Go	GPT				NVMe
0		En ligne	60,0 Go	0,00 O	GPT				SAS
▲ STG-SRVW02 (2)									
1		En ligne	60,0 Go	60,0 Go	GPT				NVMe
0		En ligne	60,0 Go	0,00 O	GPT				SAS

Dernière actualisation : 24/04/2025 15:09:49

Les disques ont été initialisés correctement.

Création des volumes des disques

Maintenant que les disques ont été initialisés, il est nécessaire de créer des volumes afin de les rendre accessibles en écriture par le système.

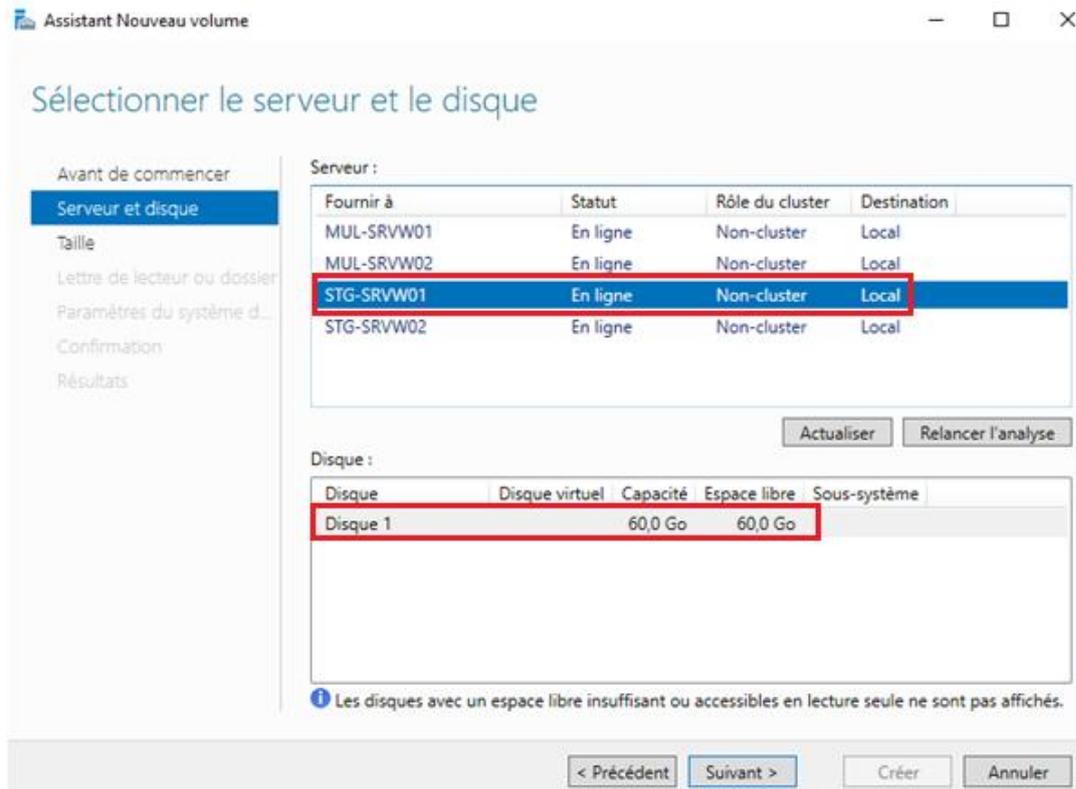
Pour cela, effectuez un clic droit sur le disque initialisé, puis sélectionnez **Nouveau volume**.

▲ STG-SRVW01 (2)									
1		En ligne	60,0 Go	60,0 Go	GPT				NVMe
0		En ligne	60,0 Go	0,00 O	GPT				SAS
▲ STG-SRVW02 (2)									
1		En ligne	60,0 Go	60,0 Go	GPT				NVMe
0		En ligne	60,0 Go	0,00 O	GPT				SAS

Context menu options:

- Nouveau volume...
- Mettre en ligne
- Mettre hors connexion
- Réinitialiser le disque

Sélectionnez ensuite le **serveur concerné**, et vous constaterez que le **disque 1 de 60 Go**, initialisé précédemment, apparaît comme **disponible** pour la création d'un nouveau volume.

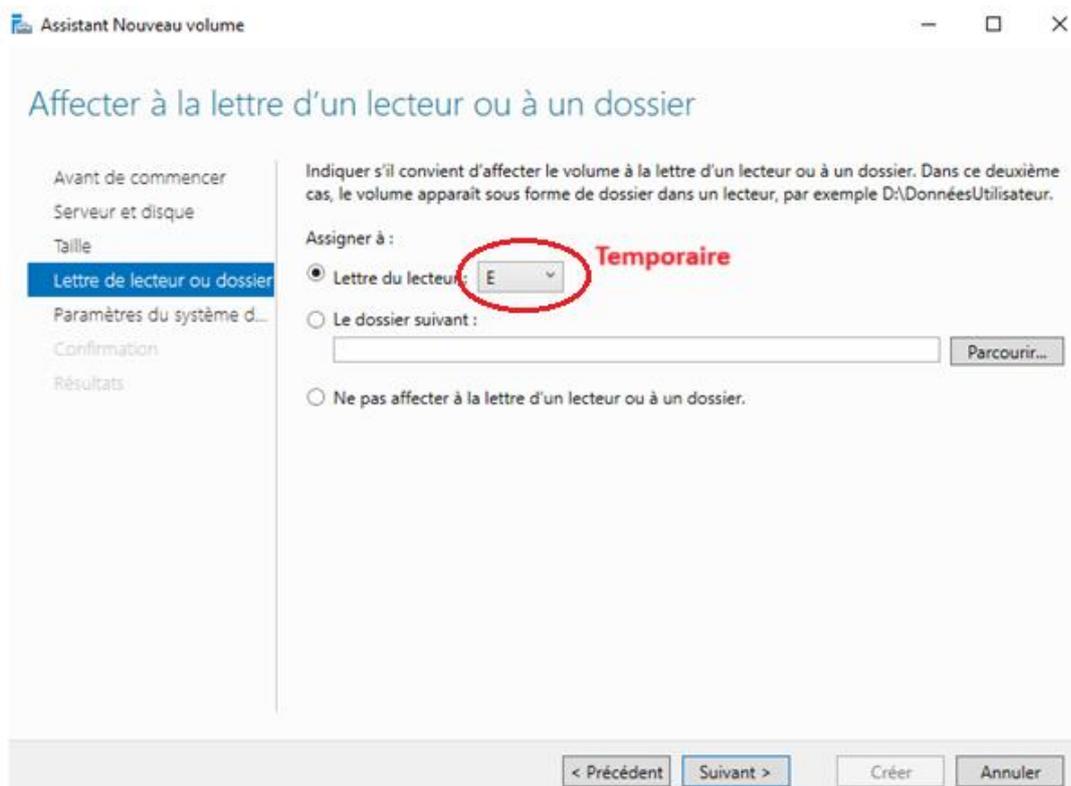


À l'étape **Taille du volume**, l'assistant propose par défaut la **taille maximale disponible**. Laissez cette valeur telle quelle, puis cliquez sur **Suivant**.



Ensuite, à l'étape d'attribution de la lettre du lecteur, et conformément au cahier des charges, la lettre **D** : aurait dû être attribuée au disque contenant les données.

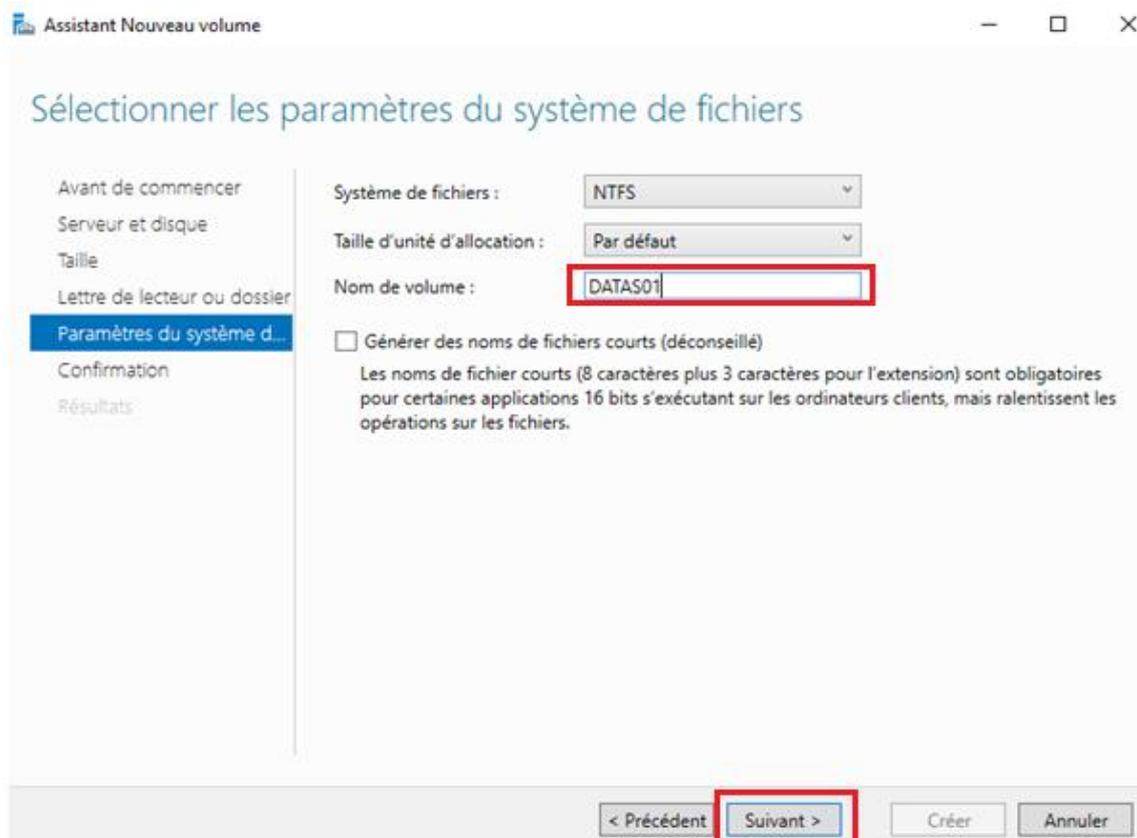
Toutefois, celle-ci n'étant pas disponible au moment de la configuration, nous avons temporairement attribué la lettre **E** : qui pourra être ajustée par la suite via la gestion des disques.



Ensuite, nommez le volume selon la convention définie lors de la présentation du projet :

- DATAS01 pour STG-SRVW01
- DATAS02 pour STG-SRVW02
- DATAS03 pour MUL-SRVW01
- DATAS04 pour MUL-SRVW02

Laissez la **taille d'unité d'allocation par défaut** (4096 octets), qui correspond à la **taille minimale d'un bloc de données** sur le disque.



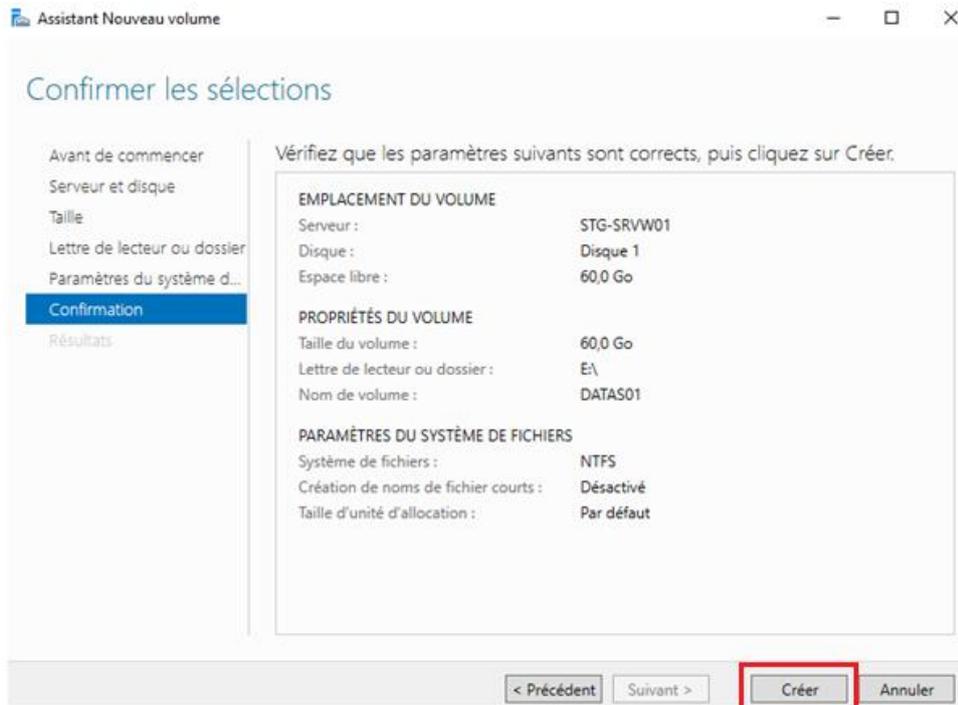
The screenshot shows the 'Assistant Nouveau volume' window with the title 'Sélectionner les paramètres du système de fichiers'. On the left, a navigation pane lists steps: 'Avant de commencer', 'Serveur et disque', 'Taille', 'Lettre de lecteur ou dossier', 'Paramètres du système d...' (highlighted), 'Confirmation', and 'Résultats'. The main area contains the following settings:

- Système de fichiers : NTFS
- Taille d'unité d'allocation : Par défaut
- Nom de volume : DATAS01
- Générer des noms de fichiers courts (déconseillé)

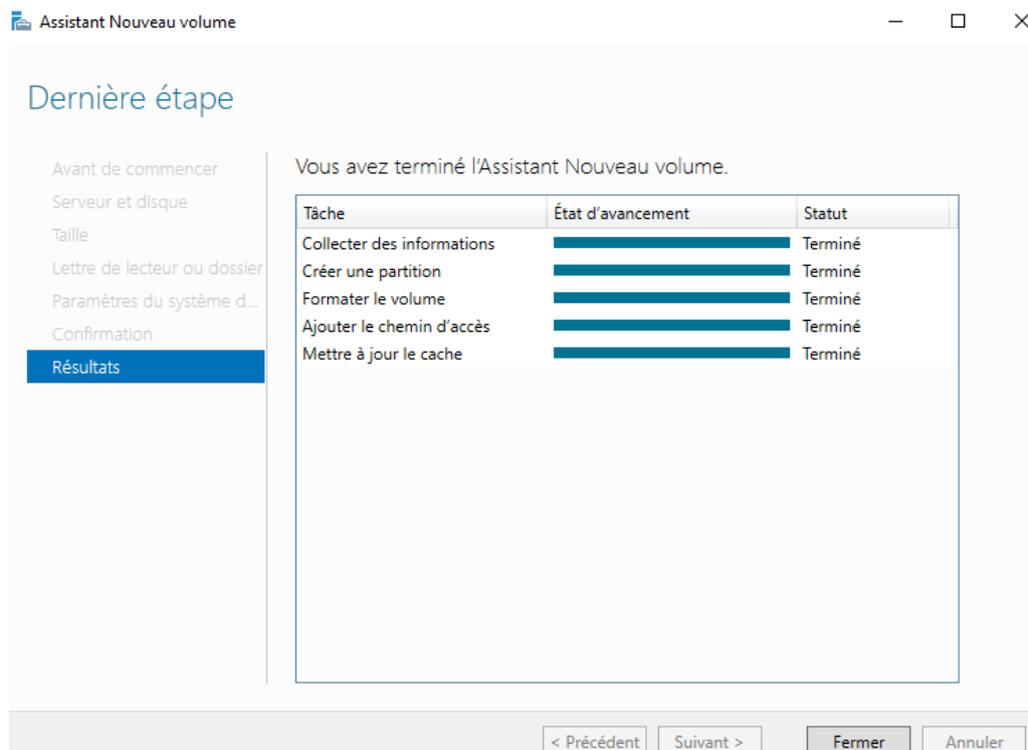
Below the checkbox, a note states: 'Les noms de fichier courts (8 caractères plus 3 caractères pour l'extension) sont obligatoires pour certaines applications 16 bits s'exécutant sur les ordinateurs clients, mais ralentissent les opérations sur les fichiers.'

At the bottom, there are four buttons: '< Précédent', 'Suivant >' (highlighted), 'Créer', and 'Annuler'.

Enfin, vérifiez les **paramètres de configuration** définis, puis cliquez sur **Créer** pour finaliser l'opération.



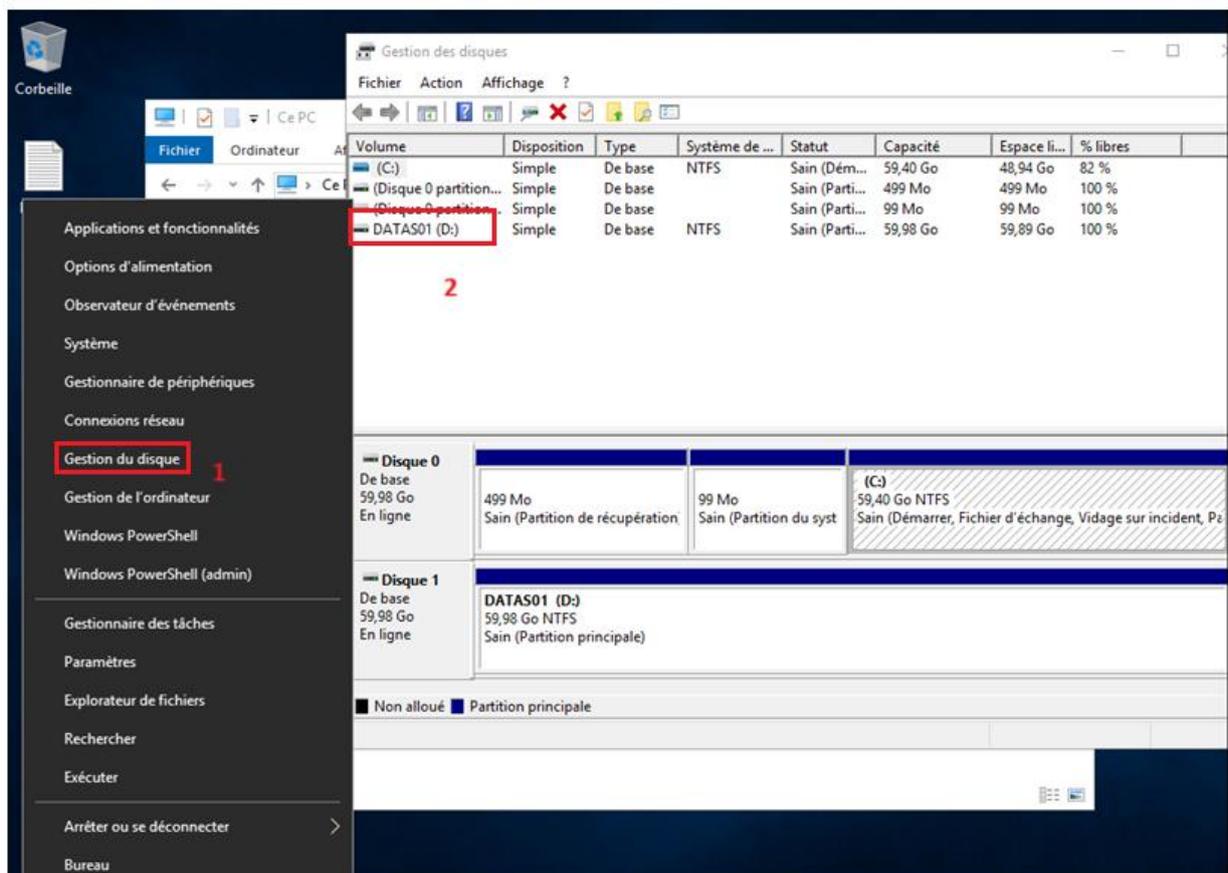
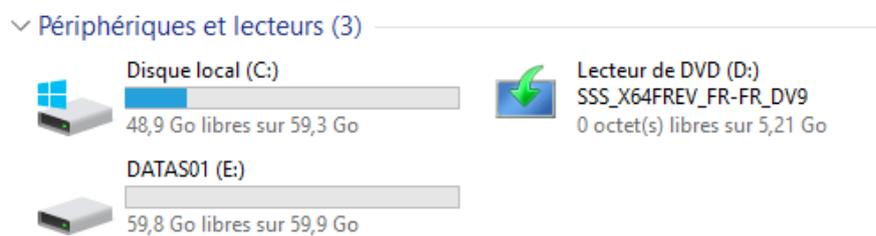
Le volume a été créé correctement, sans erreur.



Vérification du nouveau volume :

Pour vérifier que le nouveau volume a bien été créé, ouvrez l'Explorateur de fichiers, puis cliquez sur **Ce PC**.

Les ISO étaient montés automatiquement en tant que lecteur DVD (D:), je les ai donc retirés des VM maintenant que l'installation est terminée, afin de libérer la lettre **D** : pour l'attribution des disques de données.



Les lettres des lecteurs ont bien été inversées : le volume **DATAS01** est désormais monté sur **D** : comme prévu, et le lecteur DVD a été déplacé en **E** : Je retirerai l'ISO entièrement un peu plus tard afin de ne plus afficher de lecteur optique dans l'explorateur.

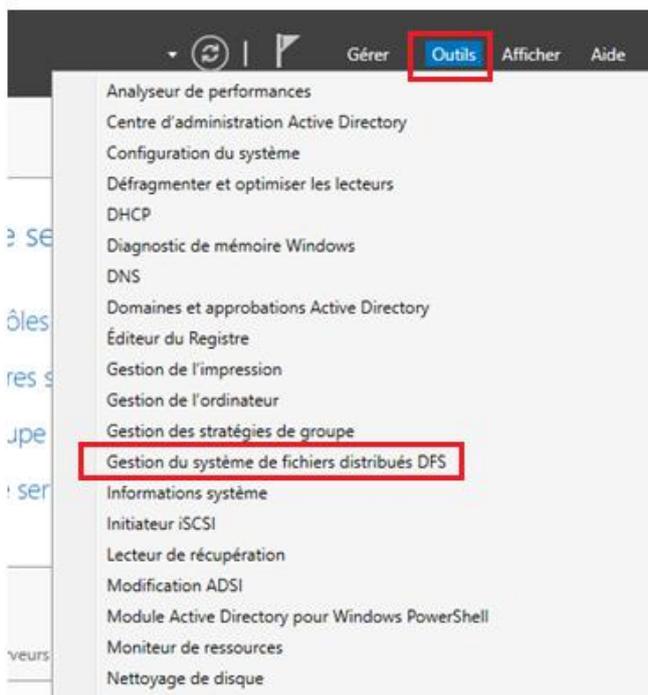


Le lecteur D:\DATAS01 a bien été créé et est pleinement opérationnel.

Les autres volumes de données ont bien été créés sur les serveurs respectifs : DATAS02 sur STG-SRVW02, DATAS03 sur MUL-SRVW01 et DATAS04 sur MUL-SRVW02.

Création de l'espace de nom DFS

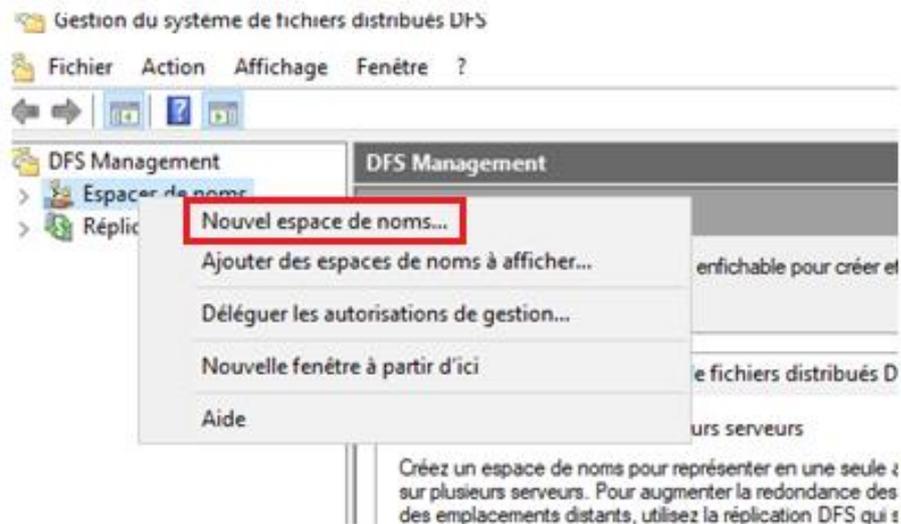
Pour commencer la configuration du DFS, ouvrez la console de gestion du DFS, accessible depuis le Gestionnaire de serveur.



Pour cela, cliquez sur **Outils**, puis sur **Gestion du système de fichiers distribués (DFS)**.

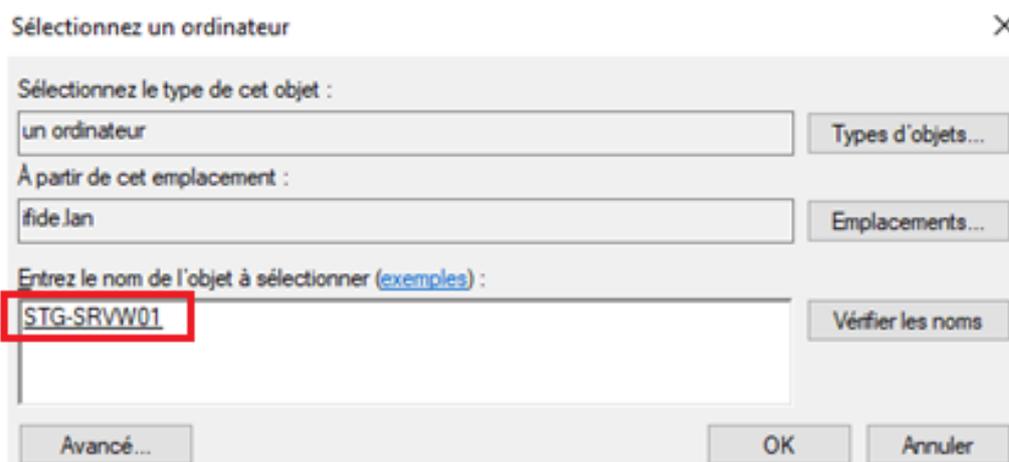
Il est également possible d'y accéder via une console MMC personnalisée si nécessaire.

Dans la console DFS, effectuez un clic droit sur "Espaces de noms", puis sélectionnez "Nouvel espace de noms".

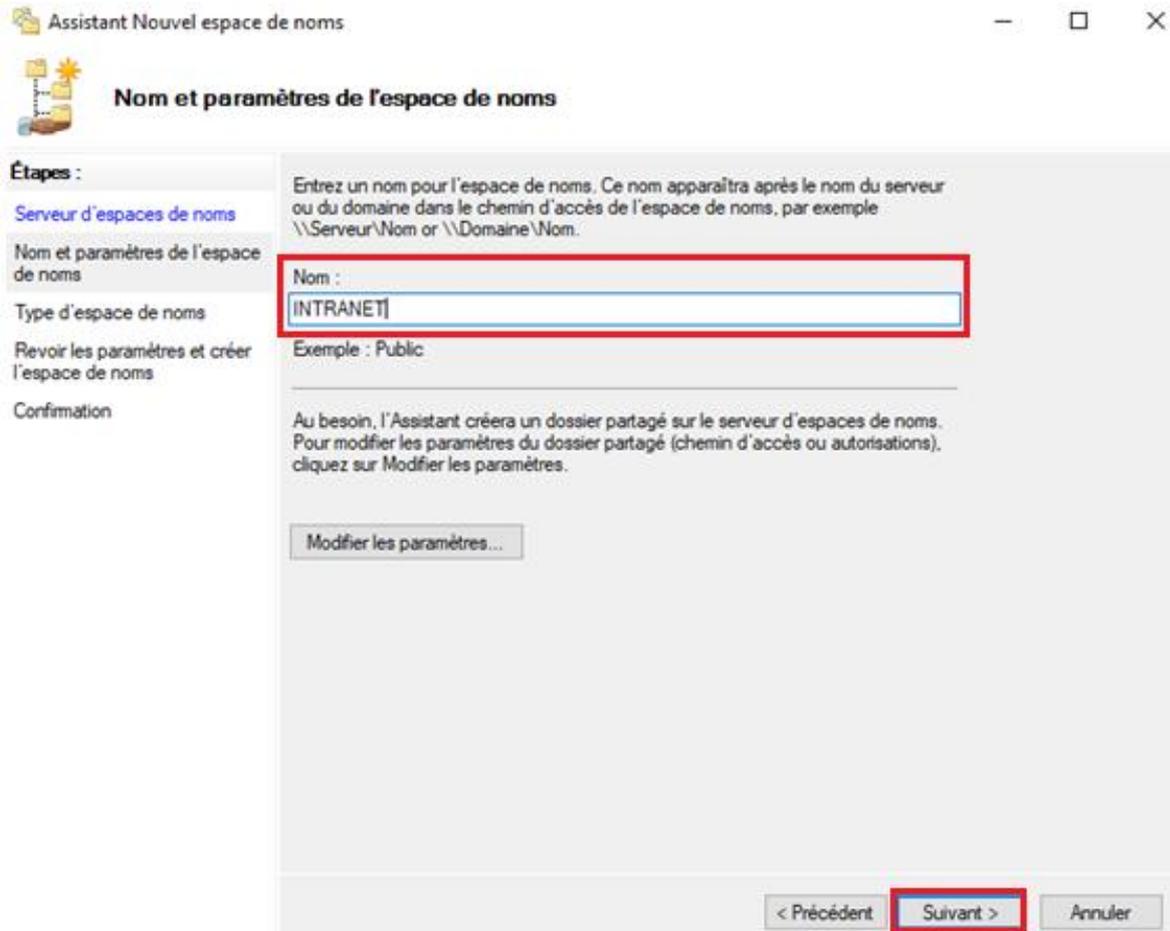


Ensuite, cliquez sur **Parcourir** pour sélectionner le **serveur d'espace de noms** (ici STG-SRVW01).

Saisissez le **nom du serveur d'espace de noms**, puis **vérifiez les noms**.



Puis, saisissez le **nom de l'espace de noms**, qui dans notre cas est **INTRANET**, conformément au cahier des charges.



Assistant Nouvel espace de noms

Nom et paramètres de l'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms**
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.

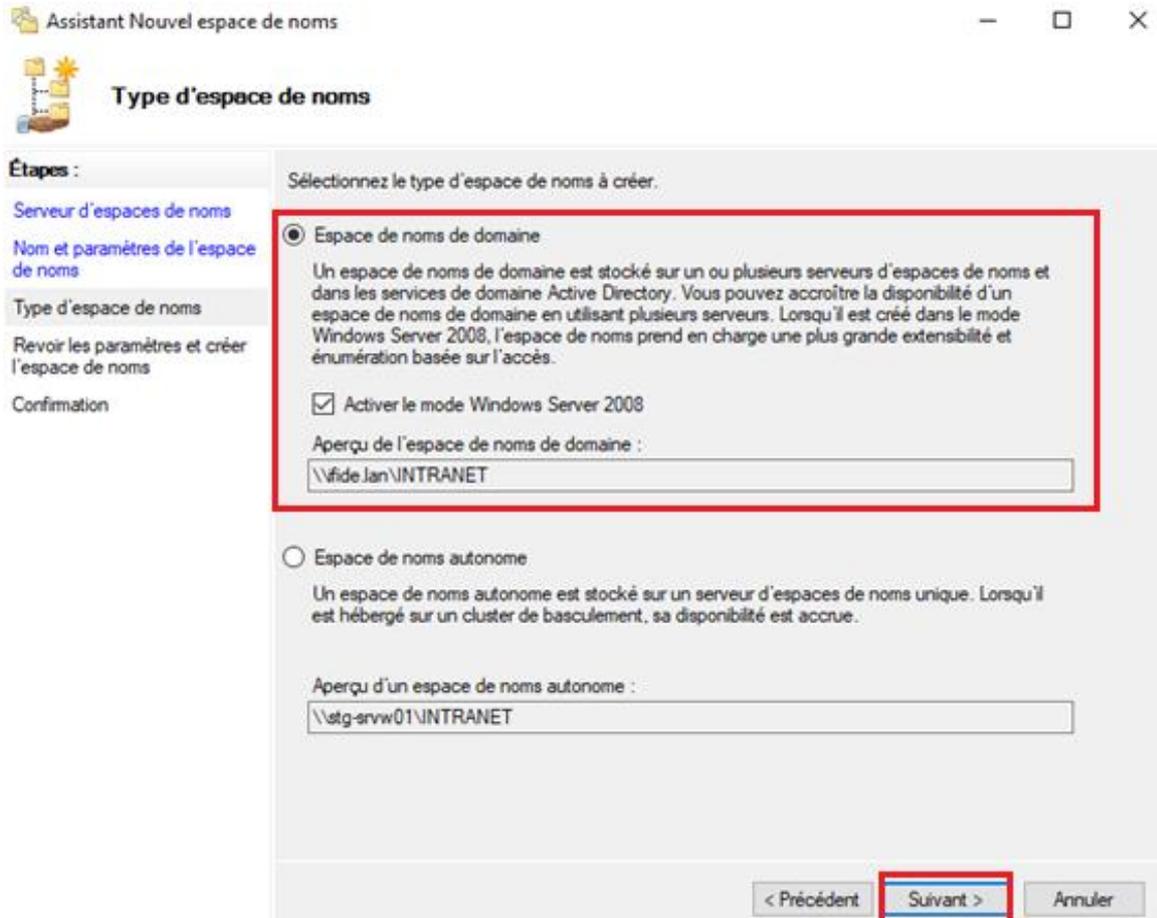
Nom :

Exemple : Public

Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.

< Précédent **Suivant >** Annuler

Cochez ensuite **Espace de noms de domaine** pour rendre cet espace de noms DFS accessible via l'adresse : <\\nomdedomaine\espacedenom>.



Assistant Nouvel espace de noms

Type d'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Sélectionnez le type d'espace de noms à créer.

Espace de noms de domaine

Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande extensibilité et énumération basée sur l'accès.

Activer le mode Windows Server 2008

Aperçu de l'espace de noms de domaine :

\\fide.lan\INTRANET

Espace de noms autonome

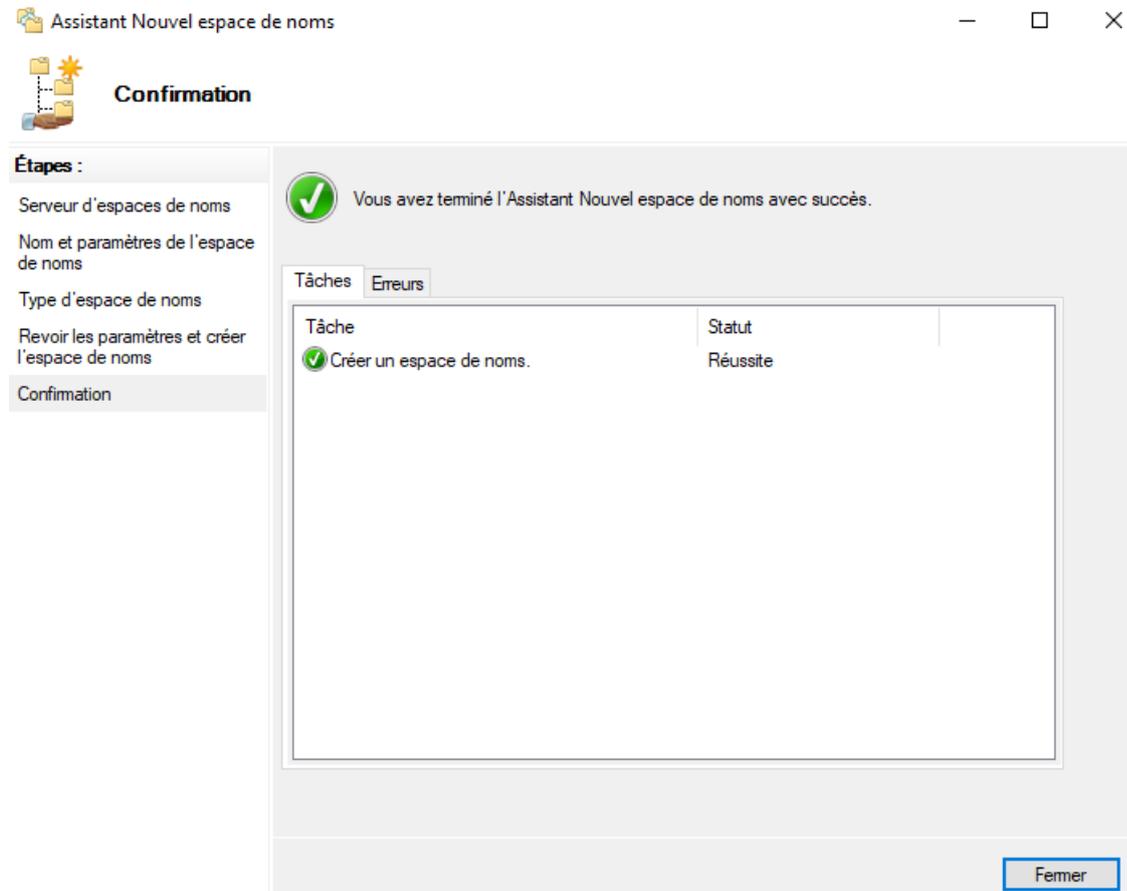
Un espace de noms autonome est stocké sur un serveur d'espaces de noms unique. Lorsqu'il est hébergé sur un cluster de basculement, sa disponibilité est accrue.

Aperçu d'un espace de noms autonome :

\\stg-srvw01\INTRANET

< Précédent **Suivant >** Annuler

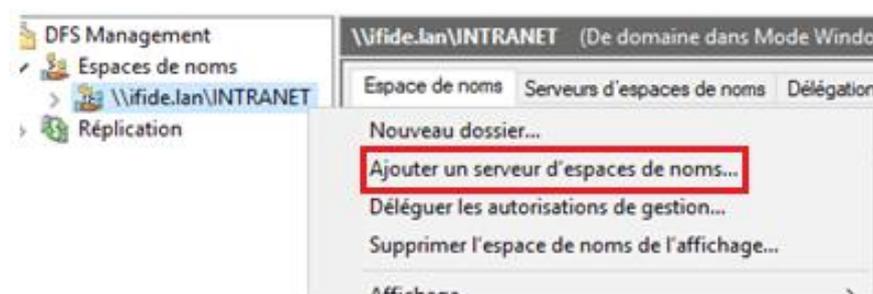
L'espace de noms a été créé correctement.



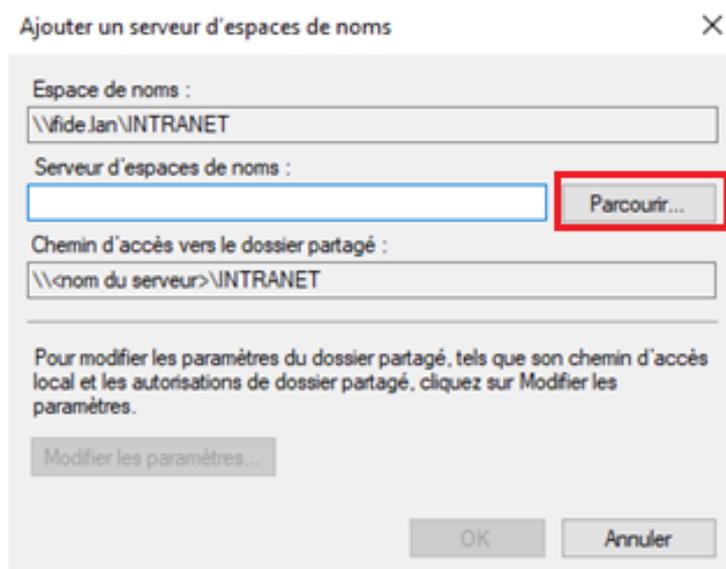
Ajout d'un serveur d'espace de noms supplémentaire

L'ajout d'un autre serveur d'espace de noms permet d'assurer la redondance de l'espace de noms, garantissant ainsi la haute disponibilité des données de l'IFIDE.

Pour ce faire, toujours dans la console de gestion DFS, faites un clic-droit sur l'espace de noms, puis sélectionnez **Ajouter un nouveau serveur d'espace de noms**.



Ensuite, cliquez sur **Parcourir**, puis saisissez le nom du **nouveau serveur d'espace de noms** : **MUL-SRVW01**.



Ajouter un serveur d'espaces de noms

Espace de noms :
\\fide.lan\INTRANET

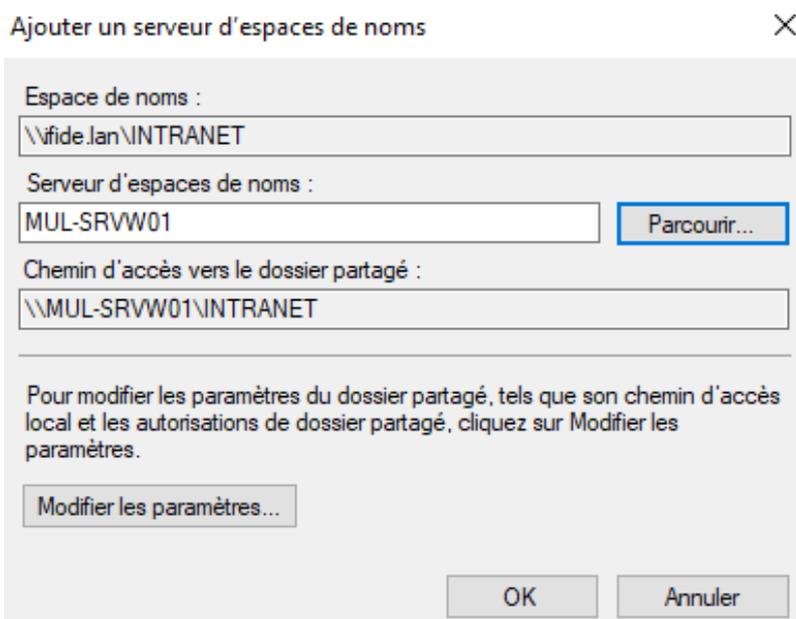
Serveur d'espaces de noms :
 Parcourir...

Chemin d'accès vers le dossier partagé :
\\<nom du serveur>\INTRANET

Pour modifier les paramètres du dossier partagé, tels que son chemin d'accès local et les autorisations de dossier partagé, cliquez sur Modifier les paramètres.

Modifier les paramètres...

OK Annuler



Ajouter un serveur d'espaces de noms

Espace de noms :
\\fide.lan\INTRANET

Serveur d'espaces de noms :
MUL-SRVW01 Parcourir...

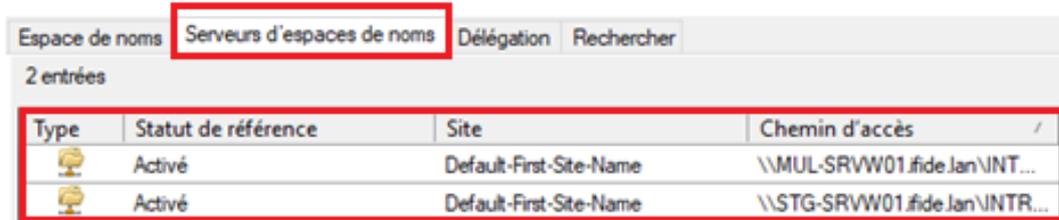
Chemin d'accès vers le dossier partagé :
\\MUL-SRVW01\INTRANET

Pour modifier les paramètres du dossier partagé, tels que son chemin d'accès local et les autorisations de dossier partagé, cliquez sur Modifier les paramètres.

Modifier les paramètres...

OK Annuler

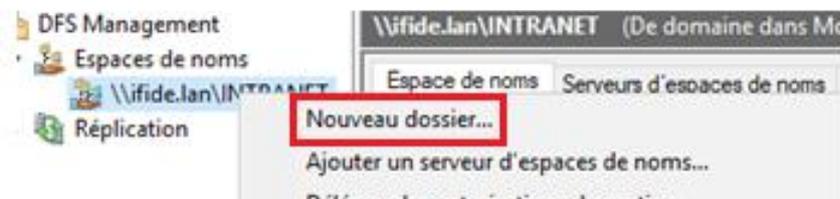
Pour vérifier que le nouveau serveur a bien été ajouté, cliquez sur **Serveurs d'espace de noms**. Si l'ajout a été effectué correctement, deux entrées devraient apparaître dans la console.



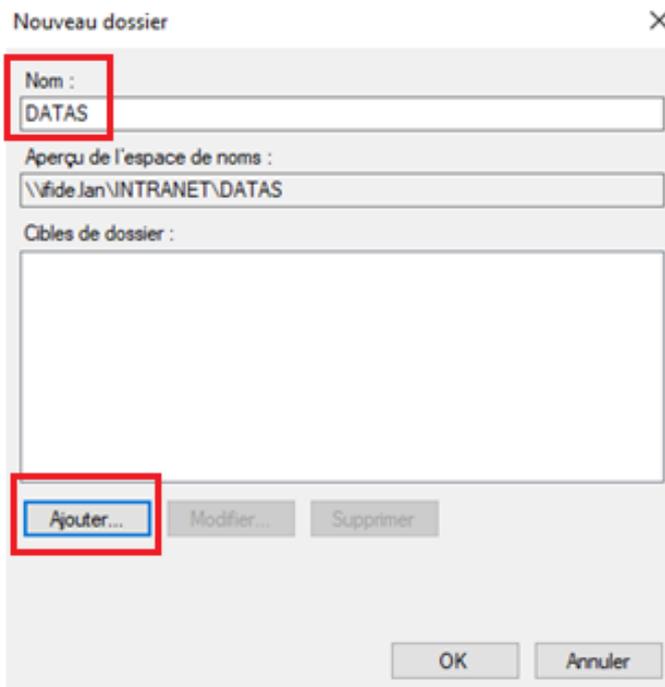
Type	Statut de référence	Site	Chemin d'accès
	Activé	Default-First-Site-Name	\\MUL-SRVW01.fide.lan\INT...
	Activé	Default-First-Site-Name	\\STG-SRVW01.fide.lan\INTR...

Création d'un dossier partagé dans l'espace de noms

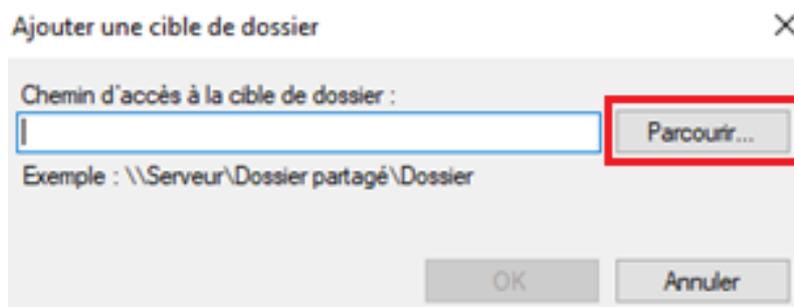
Tout d'abord, nous allons créer un dossier partagé dans l'espace de nom INTRANET, qui pointera vers le disque **D:** et contiendra les dossiers **USERS**, **GROUPES**, et **TRANSFERT** de l'IFIDE. Pour ce faire, sur la console DFS, faites un clic-droit sur l'espace de noms DFS, puis cliquez sur **Nouveau dossier**.



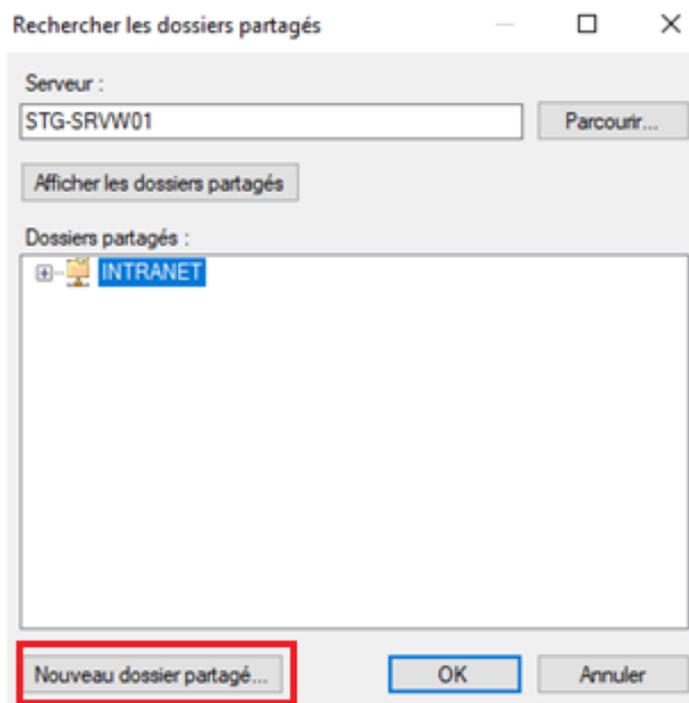
Ensuite, une fenêtre apparaîtra, vous demandant de nommer l'accès du nouveau dossier sous l'espace de noms et d'ajouter la cible DFS. Dans cette opération, nous allons créer un accès DFS avec le nom **DATAS**, qui ciblera le partage du lecteur D:\ du serveur **STG-SRVW01**.



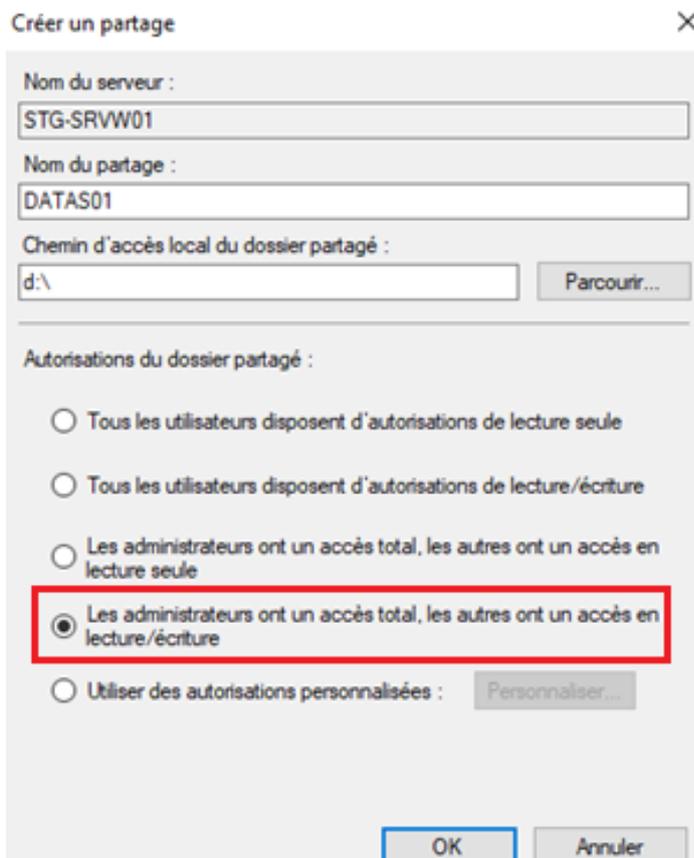
Cliquez ensuite sur **Ajouter** pour ajouter une cible au dossier partagé. Puis une fenêtre apparaîtra, cliquez sur **Parcourir**.



Si vous avez déjà partagé les dossiers (ou lecteurs) souhaités, vous pourrez voir les différents dossiers partagés présents sur le serveur désigné. Sinon, vous pouvez cliquer sur **Nouveau dossier partagé**.



Puis, saisissez le nom du partage (nous avons choisi **DATAS01**) pour identifier les différents dossiers partagés lors de l'opération de réplication. Spécifiez le chemin d'accès local du dossier, qui sera le lecteur ****D:****, et définissez les droits de partage : **Administrateurs en accès complet** et **lecture/écriture** pour tout le monde.



Créer un partage

Nom du serveur :
STG-SRVW01

Nom du partage :
DATAS01

Chemin d'accès local du dossier partagé :
d:\ Parcourir...

Autorisations du dossier partagé :

Tous les utilisateurs disposent d'autorisations de lecture seule

Tous les utilisateurs disposent d'autorisations de lecture/écriture

Les administrateurs ont un accès total, les autres ont un accès en lecture seule

Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture

Utiliser des autorisations personnalisées : Personnaliser...

OK Annuler

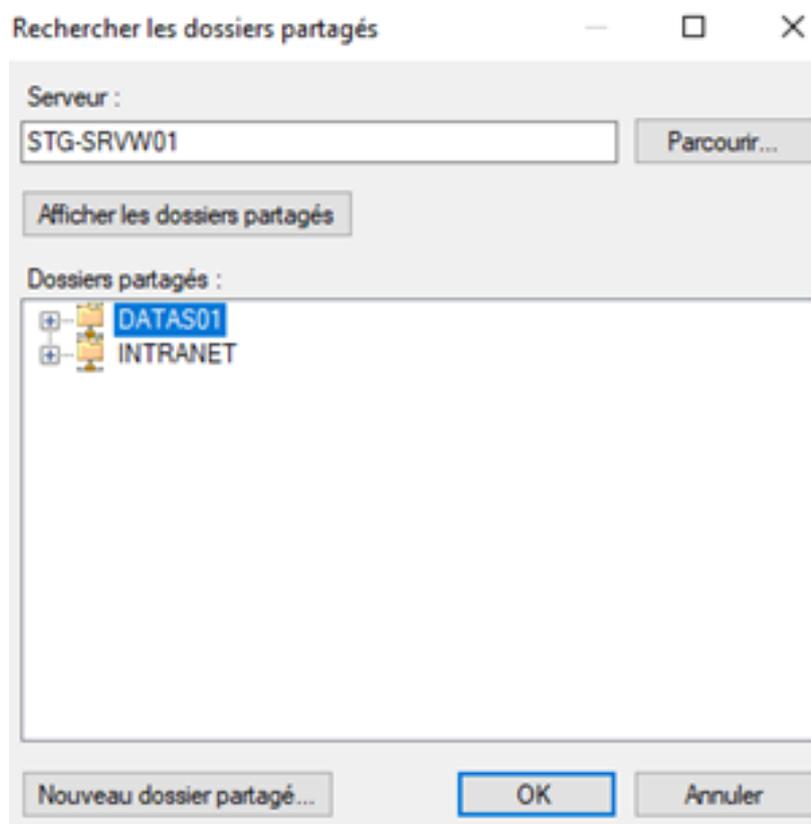
Nom du serveur : Le serveur cible qui partage le dossier

Nom du partage : Le nom du dossier partagé

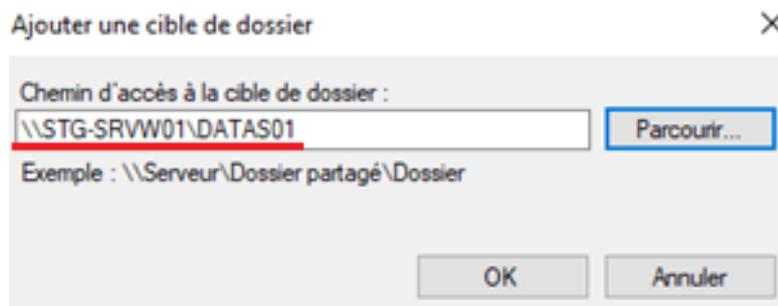
Chemin d'accès local : Le chemin local sur le serveur cible du dossier à partager

Autorisations : **Administrateur** avec **contrôle total** et **lecture/écriture** pour tout le monde, conformément aux exigences du cahier des charges.

Sélectionnez ensuite le nouveau partage **DATAS01**, puis cliquez sur **OK**.

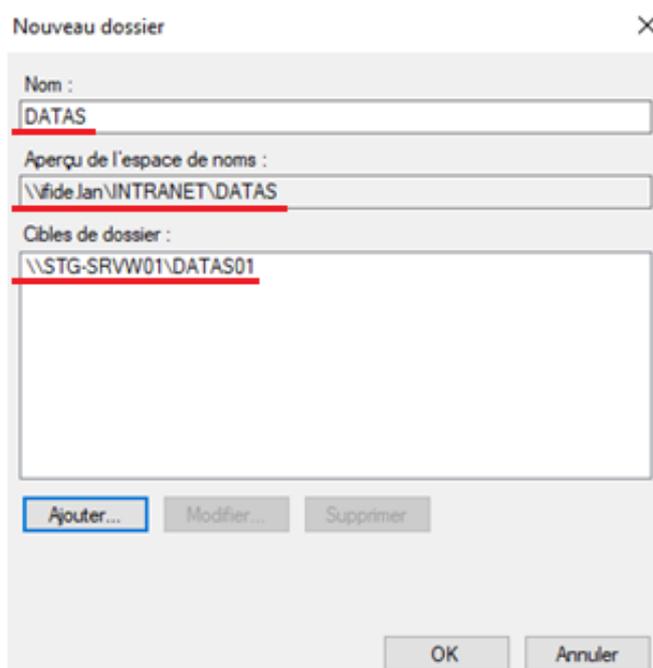


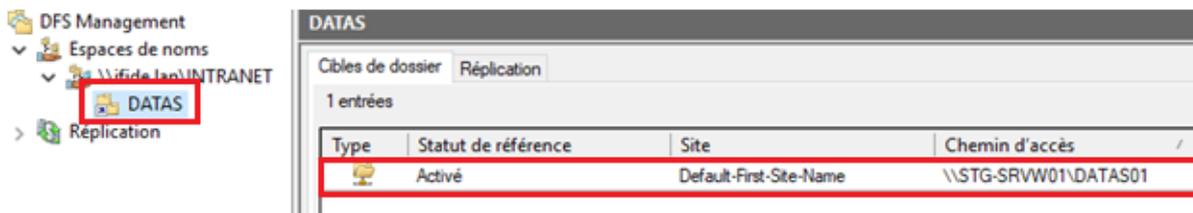
Le chemin de la cible du dossier sera ensuite proposé automatiquement. Cette cible correspond au **chemin d'accès réseau direct** au dossier, en dehors de la structure DFS. Il est important de considérer le DFS comme une **organisation hiérarchique** de tous les dossiers partagés entre les serveurs, permettant une meilleure gestion du **partage** et de la **synchronisation** des données.



➔ Vous pouvez également **partager tous les dossiers en amont** avant de les intégrer dans la hiérarchie de l'espace de noms DFS.

Enfin, un **récapitulatif** du nouveau dossier DFS s'affichera. Cliquez sur **OK** pour confirmer la création du dossier partagé dans l'espace de noms DFS.





Le dossier a été créé correctement.

À présent, nous allons répliquer le dossier DATAS vers trois autres cibles DFS :

- DATAS02 sur le serveur STG-SRVW02
- DATAS03 sur le serveur MUL-SRVW01
- DATAS04 sur le serveur MUL-SRVW02

Mise en place de la réplication DFSR

Pour la réplication DFSR, deux grandes méthodes s'offrent à vous :

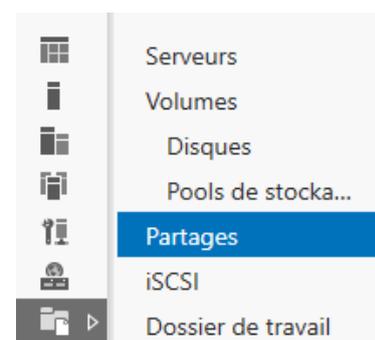
1. Ajouter manuellement les cibles de dossier au dossier **DATAS** (partages DATAS02, DATAS03, DATAS04) ; la console proposera ensuite automatiquement de configurer la réplication.
2. Créer au préalable un groupe de réplication DFSR, qui ajoutera ensuite automatiquement les cibles DFS au dossier à répliquer.

Dans cette documentation, nous allons commencer par créer le groupe de réplication DFS, puis configurer les dossiers à répliquer.

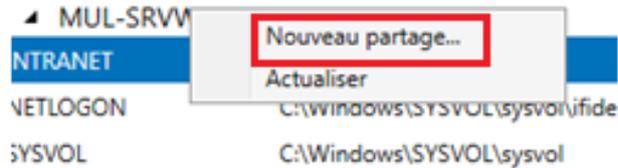
Partage des dossiers DATAS

À l'aide du Gestionnaire de serveur, vous pouvez facilement partager le dossier DATAS sur chaque serveur, y compris sur les serveurs Core.

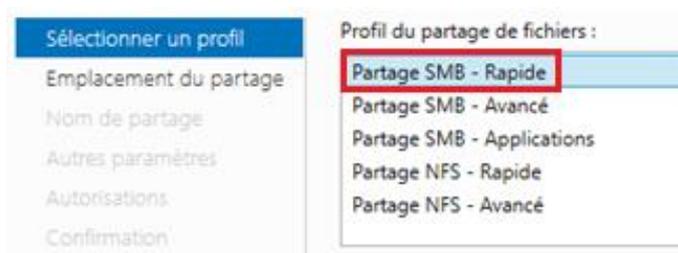
Pour cela, cliquez sur **Services de fichiers et de stockage** → **Partages**.



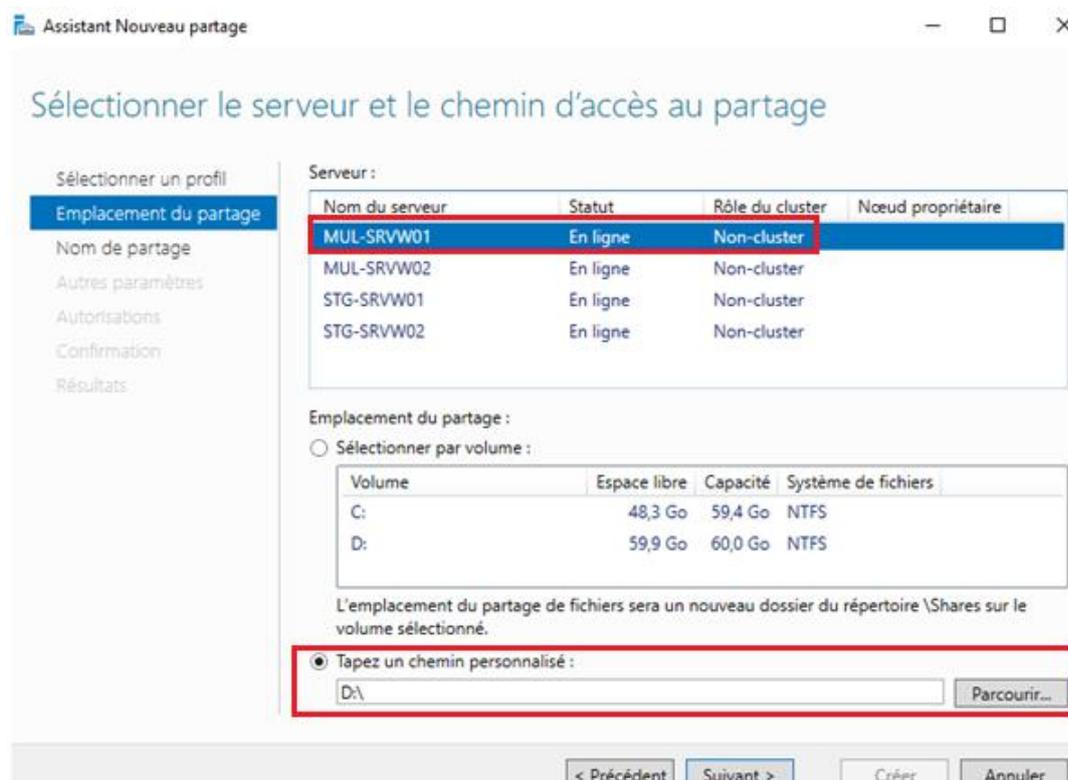
Ensuite, effectuez un clic droit sur l'un des serveurs, puis sélectionnez **Nouveau partage**.



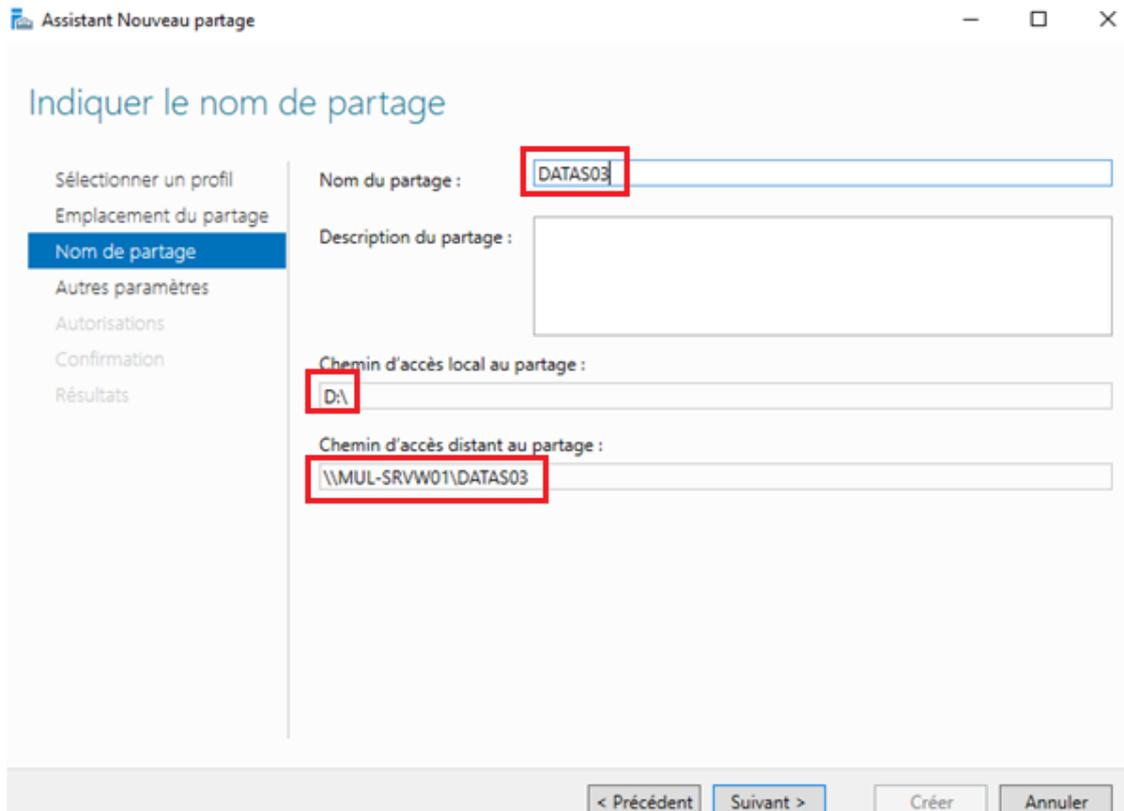
Puis, sélectionnez **Partage SMB – Rapide**.



Sélectionnez le serveur hébergeant le dossier à partager, indiquez le chemin personnalisé vers le dossier (par exemple D:\), puis cliquez sur **Suivant** pour poursuivre la configuration du partage.



Ensuite, nommez le partage **DATAS03**, correspondant à la cible de partage sur le serveur **MUL-SRVW01**.



Assistant Nouveau partage

Indiquer le nom de partage

- Sélectionner un profil
- Emplacement du partage
- Nom de partage**
- Autres paramètres
- Autorisations
- Confirmation
- Résultats

Nom du partage :

Description du partage :

Chemin d'accès local au partage :

Chemin d'accès distant au partage :

< Précédent Suivant > Créer Annuler

Pensez à personnaliser les autorisations du partage : Administrateurs en contrôle total, et Tout le monde en lecture/écriture. Enfin, cliquez sur Créer pour finaliser le partage du dossier.

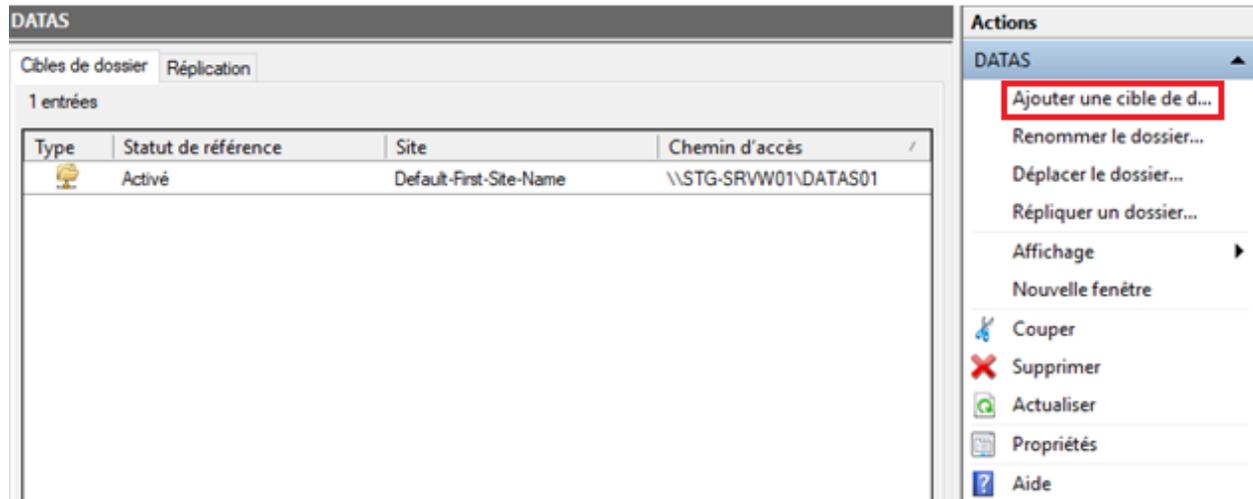
▲ MUL-SRVW01 (4)			
INTRANET	C:\DFSRoots\INTRANET	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\ifide.l...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
DATAS03	D:\	SMB	Non-cluster
▲ MUL-SRVW02 (3)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ifide.l...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
DATAS04	E:\	SMB	Non-cluster
▲ STG-SRVW01 (4)			
DATAS01	d:\	SMB	Non-cluster
INTRANET	C:\DFSRoots\INTRANET	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\ifide.l...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ STG-SRVW02 (3)			
NETLOGON	C:\Windows\SYSVOL\sysvol\ifide.l...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
DATAS02	E:\	SMB	Non-cluster

Les dossiers DATAS ont bien été partagés avec succès.

Création d'un groupe de réplication DFS

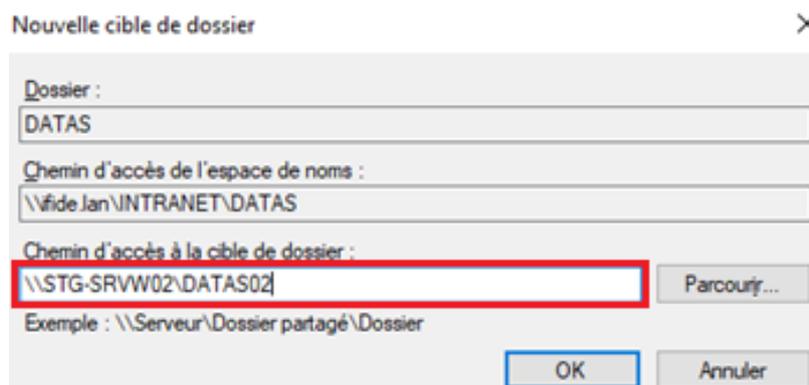
Pour créer un groupe de réplication DFS, il suffit d'ajouter les autres cibles de dossier au dossier DATAS dans l'espace de noms DFS.

Pour cela, dans la console DFS, effectuez un clic droit sur le dossier DATAS, puis sélectionnez **Ajouter une cible de dossier**.

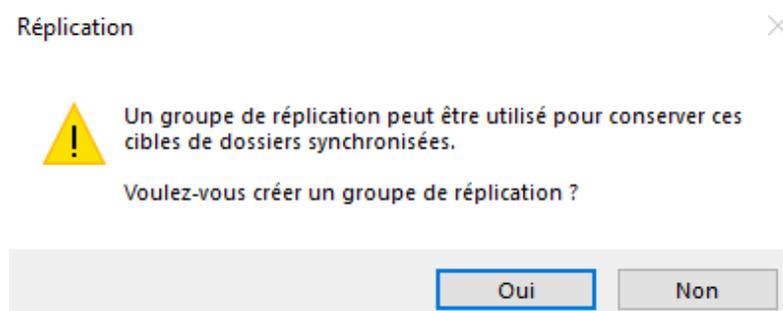


Ensuite, saisissez le **chemin réseau** des différentes cibles de dossier à ajouter :

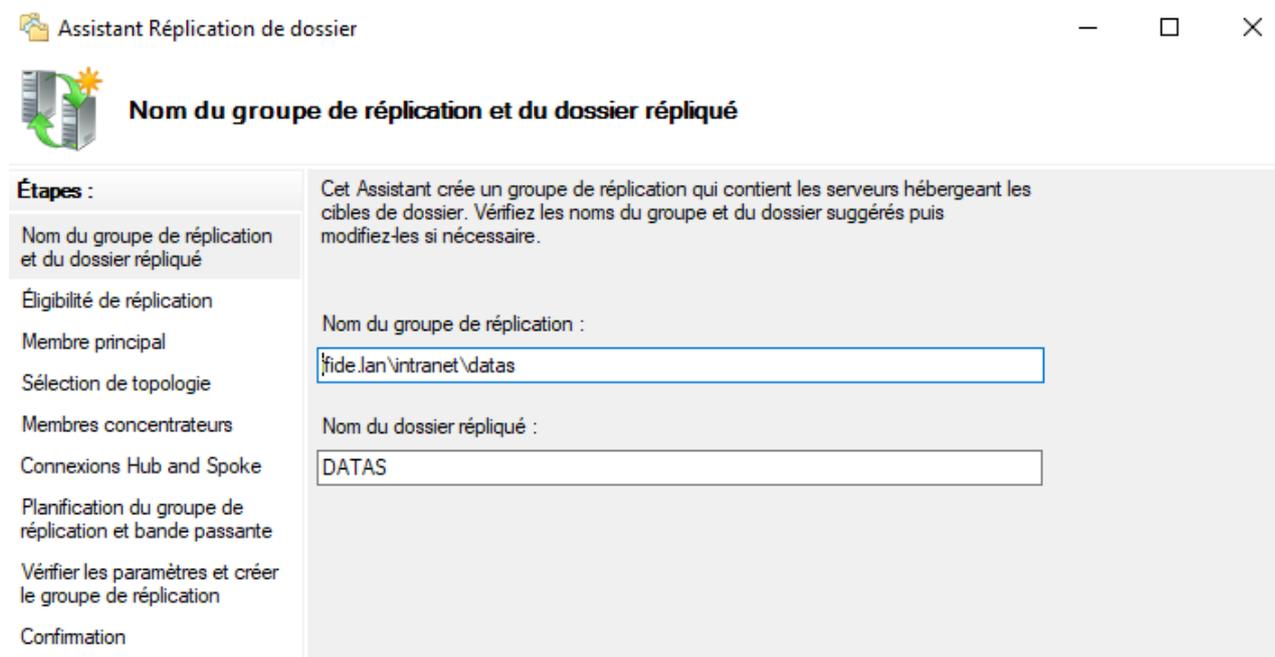
- \\STG-SRVW02\DATAS02
- \\MUL-SRVW01\DATAS03
- \\MUL-SRVW02\DATAS04

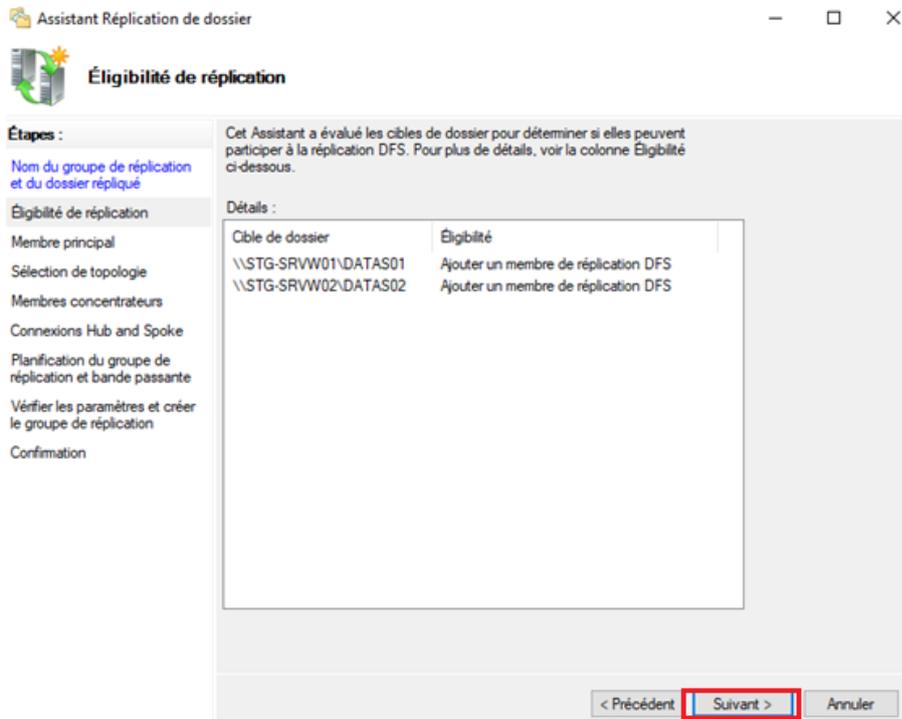


Lors de l'ajout d'une cible de dossier, une fenêtre vous proposera de **créer un groupe de réplication**. Cliquez sur **Oui** pour lancer l'assistant.

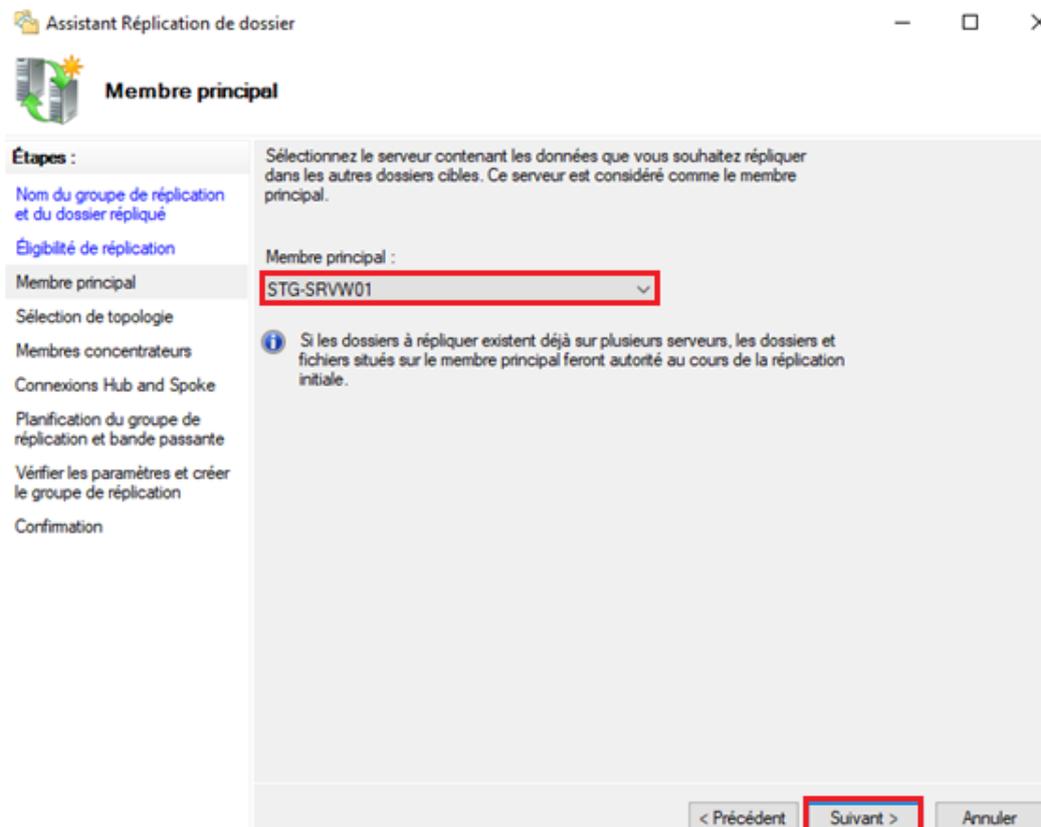


L'assistant complétera automatiquement les informations nécessaires. Cliquez simplement sur **Suivant** pour poursuivre.





En tant que **membre principal de la réplication**, sélectionnez le serveur principal : **STG-SRVW01**.



Ensuite, sélectionnez l'option **Maille pleine**, afin que la réplication s'effectue **entre tous les serveurs**.

Assistant Réplication de dossier

Sélection de topologie

Étapes :

- Nom du groupe de réplication et du dossier répliqué
- Éligibilité de réplication
- Membre principal
- Sélection de topologie**
- Planification du groupe de réplication et bande passante
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez une topologie de connexions parmi les membres du groupe de réplication.

Hub et Spoke

Cette topologie requiert au moins 3 membres dans le groupe de réplication. Les membres spoke sont connectés à un ou deux hubs. Cette topologie est adaptée aux scénarios de publication où les données proviennent du membre hub et se répliquent sur les membres spoke.



Maille pleine

Dans cette topologie, chaque membre est répliqué avec tous les autres membres du groupe de réplication. Cette topologie est surtout adaptée lorsqu'il existe au plus dix membres dans le groupe de réplication.



Aucune topologie

Sélectionnez cette option si vous souhaitez créer une topologie personnalisée une fois l'Assistant terminé. Aucune réplication ne peut s'effectuer tant que vous n'avez pas créé la topologie personnalisée.

< Précédent **Suivant >** Annuler

Afin de répondre aux besoins du client, laissez l'option **Réplication en continu** activée, ce qui permettra une **synchronisation permanente** des cibles de dossier DFS.

Assistant Réplication de dossier

Planification du groupe de réplication et bande passante

Étapes :

- Nom du groupe de réplication et du dossier répliqué
- Éligibilité de réplication
- Membre principal
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez la planification de réplication et la bande passante à utiliser par défaut pour toutes les nouvelles connexions dans le groupe de réplication.

Réplicier en continu à l'aide de la bande passante spécifiée
 Utilisez cette option pour activer la réplication 24 heures sur 24 et sept jours sur sept, avec la bande passante suivante :

Bande passante :
 Complète

Réplicier aux jours et heures spécifiés
 Utilisez cette option pour spécifier les jours et heures de réplication par défaut. La planification de réplication initiale n'a pas d'intervalles de réplication. Vous devez en créer au moins un pour que la réplication puisse avoir lieu.

Modifier la planification...

< Précédent **Suivant >** Annuler

Confirmation

Étapes :

- Nom du groupe de réplication et du dossier répliqué
- Éligibilité de réplication
- Membre principal
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

 Vous avez terminé l'Assistant Réplication de dossier avec succès.

Tâches	Erreurs
Créer le groupe de réplication.	Réussite
Créer les membres.	Réussite
Mettre à jour la sécurité du dossier.	Réussite
Créer un dossier répliqué.	Réussite
Créer des objets d'appartenance.	Réussite
Mettre à jour les propriétés du dossier.	Réussite
Créer les connexions.	Réussite

 Pour définir une taille suffisante pour le quota de dossier intermédiaire pour empêcher la réplication de ralentir ou de s'arrêter, vous devez prendre en compte la taille des fichiers à répliquer. Pour plus d'informations, reportez-vous au [guide d'optimisation des dossiers intermédiaires](#).

Fermer

DATAS			
Cibles de dossier		Réplication	
2 entrées			
Type	Statut de référence	Site	Chemin d'accès
	Activé	Default-First-Site-Name	\\STG-SRVW01\DATAS01
	Activé	Default-First-Site-Name	\\STG-SRVW02\DATAS02

La nouvelle cible de dossier a été ajoutée avec succès, et le groupe de réplication a été créé correctement.

Répétez l'opération pour les deux autres serveurs en ajoutant les partages restants comme cibles, et veillez à cocher l'option **Maille pleine pour tous les membres**.

Nouvelle cible de dossier

Dossier : DATAS

Chemin d'accès de l'espace de noms : \\file.lan\INTRANET\DATAS

Chemin d'accès à la cible de dossier : \\MUL-SRVW01\DATAS03 Parcourir...

Exemple : \\Serveur\Dossier partagé\Dossier

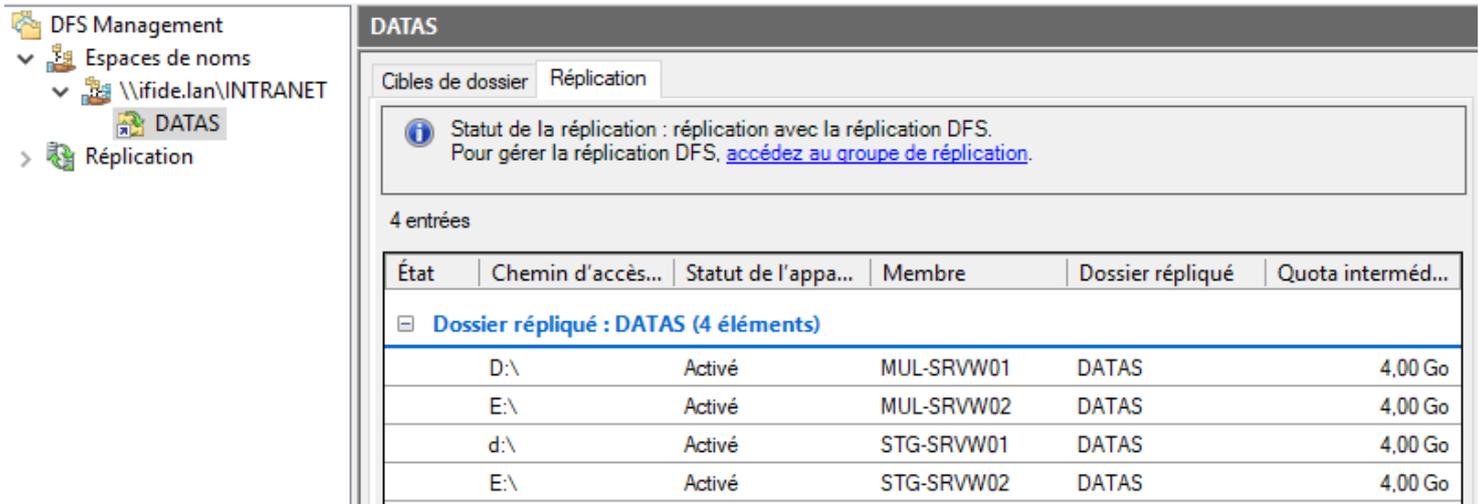
Ajouter cette cible de dossier au groupe de réplication à l'aide de la topologie suivante :

Connexion bidirectionnelle simple sur : ▼

Maille pleine sur tous les membres

Connexions personnalisées : Personnaliser...

OK Annuler



The screenshot shows the DFS Management console with the following structure:

- DFS Management
 - Espaces de noms
 - \\ifide.lan\INTRANET
 - DATAS**
 - Réplication

The main pane displays the 'DATAS' folder details under the 'Réplication' tab:

Statut de la réplication : réplication avec la réplication DFS.
 Pour gérer la réplication DFS, [accédez au groupe de réplication.](#)

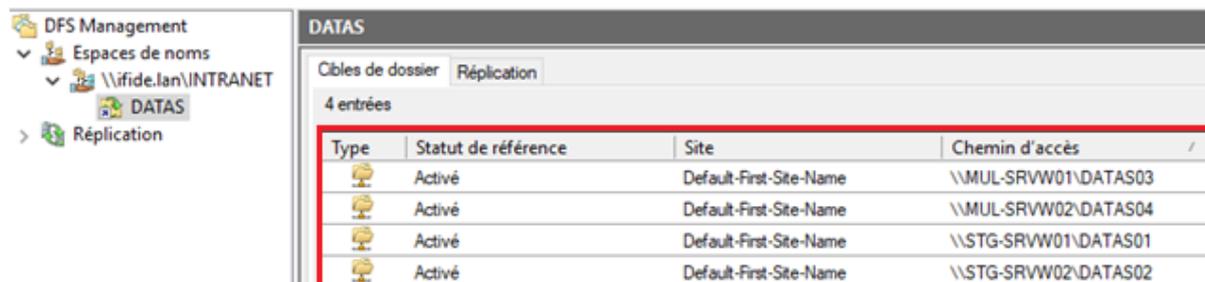
4 entrées

État	Chemin d'accès...	Statut de l'appa...	Membre	Dossier répliqué	Quota interméd...
Dossier répliqué : DATAS (4 éléments)					
	D:\	Activé	MUL-SRVW01	DATAS	4,00 Go
	E:\	Activé	MUL-SRVW02	DATAS	4,00 Go
	d:\	Activé	STG-SRVW01	DATAS	4,00 Go
	E:\	Activé	STG-SRVW02	DATAS	4,00 Go

La réplication du dossier DATAS est bien appliquée et opérationnelle sur l'ensemble des serveurs concernés.

Test de réplication DFSR

Avant de procéder au test de réplication DFSR, vérifions que toutes les cibles de dossiers sont bien présentes dans le dossier DATAS situé sous l'espace de noms DFS.

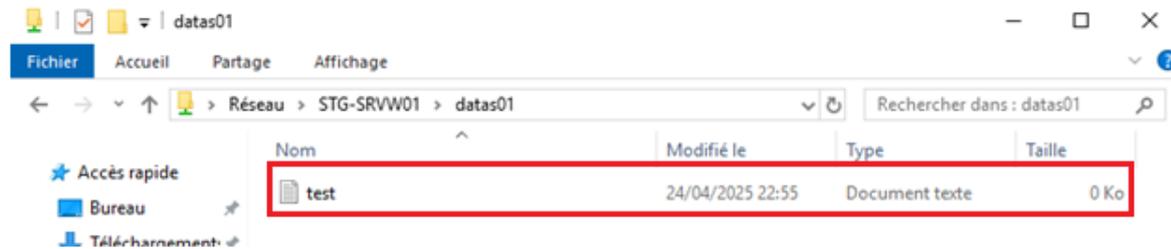


The screenshot shows the 'Cibles de dossier' tab for the DATAS folder:

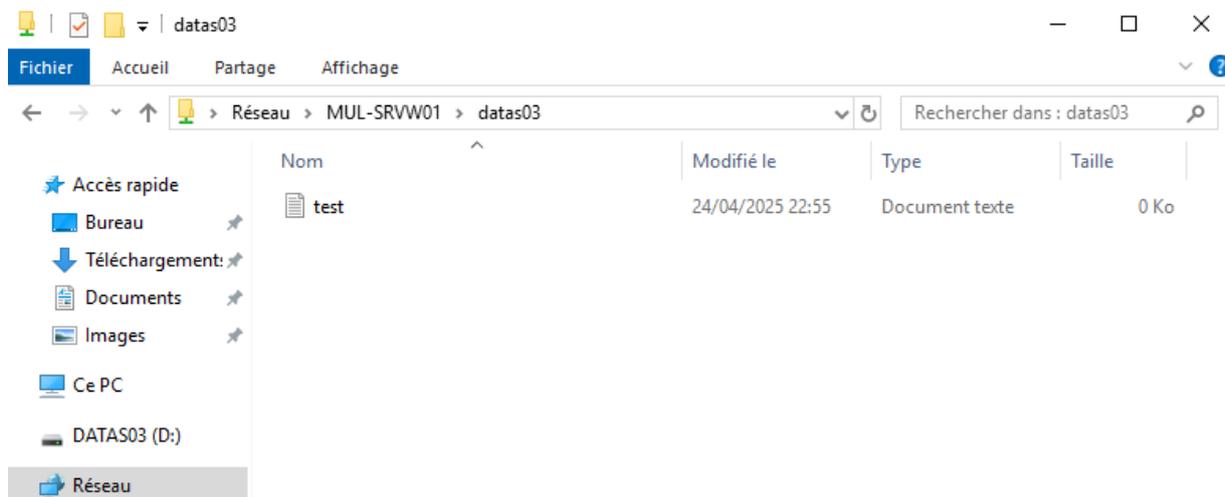
4 entrées

Type	Statut de référence	Site	Chemin d'accès
	Activé	Default-First-Site-Name	\\MUL-SRVW01\DATAS03
	Activé	Default-First-Site-Name	\\MUL-SRVW02\DATAS04
	Activé	Default-First-Site-Name	\\STG-SRVW01\DATAS01
	Activé	Default-First-Site-Name	\\STG-SRVW02\DATAS02

À présent, sur le serveur principal de Strasbourg, crée un fichier de test dans le partage \\STG-SRVW01\DATAS01.

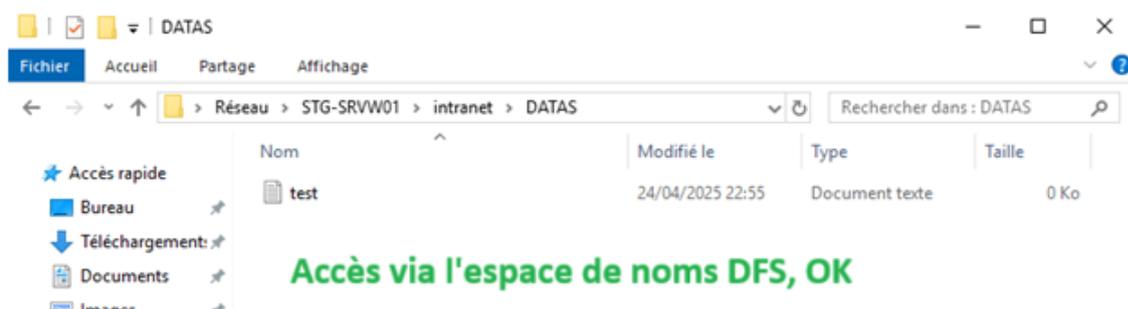


Vérifions ensuite si le fichier a bien été répliqué sur le partage réseau de MUL-SRVW01\DATAS03.



Réplication du partage réseau effectuée avec succès

Vérifions maintenant si le fichier est accessible via l'espace de noms : \\IFIDE.LAN\INTRANET\DATAS\



Vérifions si le fichier est bien présent sur le disque physique D:\ d'un des serveurs, autre que STG-SRVW01 et MUL-SRVW01.

Au début, le fichier ne semblait pas présent sur D:\, car certains serveurs (comme STG-SRVW02) ont le volume de données monté sur E:\ au lieu de D:\. Ce n'est pas problématique, seule la lettre change – la réplication fonctionne parfaitement. ✓

```

C:\Users\Administrateur.IFIDE>hostname
STG-SRVW02

C:\Users\Administrateur.IFIDE>dir D:\
Le périphérique n'est pas prêt.

C:\Users\Administrateur.IFIDE>dir E:\
Le volume dans le lecteur E s'appelle DATAS02
Le numéro de série du volume est 944F-B9C7

Répertoire de E:\

24/04/2025  22:55                0 test.txt
             1 fichier(s)                0 octets
             0 Rép(s) 63 732 125 696 octets libres

C:\Users\Administrateur.IFIDE>

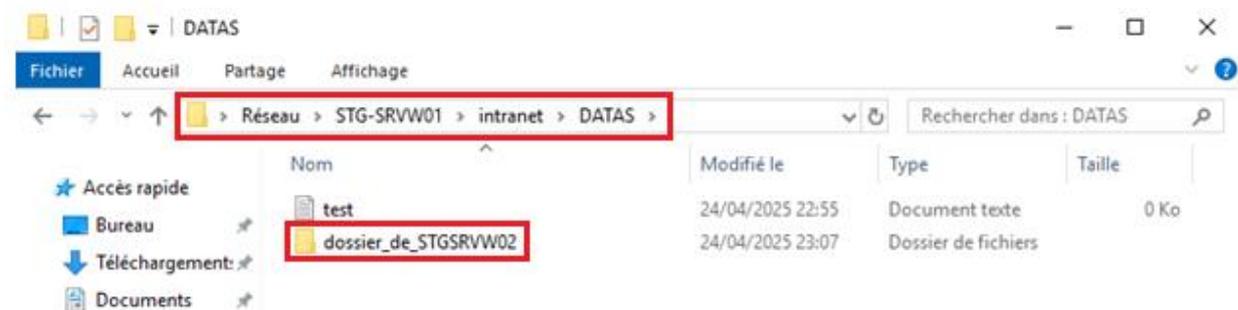
```

Le fichier est bel et bien présent sur tous les disques physiques des serveurs.

Enfin, vérifions si l'inverse est également répliqué, en créant un dossier dans le disque DATAS02 du serveur STG-SRVW02.

```
C:\Users\Administrateur.IFIDE>mkdir E:\dossier_de_STGSRVW02
```

Sur **STG-SRVW01**, et en accédant au partage via l'**espace de noms DFS**, vérifiez si le dossier nouvellement créé apparaît bien.



Le dossier est bien répliqué, aussi bien sur le partage via l'espace de noms que physiquement sur les disques des serveurs.

Ainsi, à travers ces tests d'intégration, la configuration et la mise en place de la réplication DFSR se sont déroulées correctement, sans erreur, avec des cibles de dossiers conformes au cahier des charges :

- \\STG-SRVW01\DATAS01
- \\STG-SRVW02\DATAS02
- \\MUL-SRVW01\DATAS03
- \\MUL-SRVW02\DATAS04

3.2.4) Déploiement des stratégies de groupe (GPO)

Les **GPO** (stratégies de groupe) sont un ensemble d'outils intégrés aux serveurs Windows permettant de **centraliser la gestion de l'environnement des utilisateurs** ainsi que la **configuration des machines** du domaine.

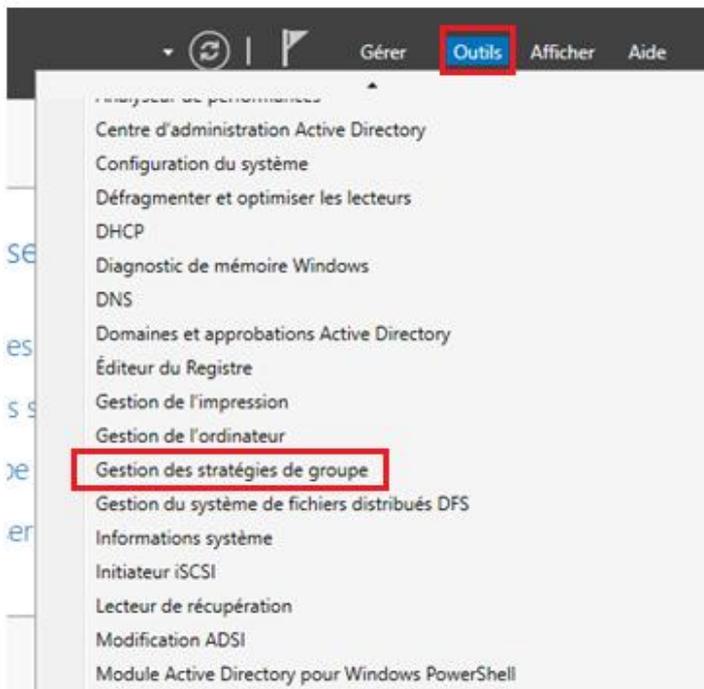
Chaque stratégie possède ses propres paramètres, définis par l'administrateur, et qui seront ensuite appliqués sur les **postes de travail** et les **comptes utilisateurs** concernés.

Dans notre cas, les GPO mettront en œuvre les actions suivantes :

- Interdiction d'accès au Panneau de configuration
- Blocage des ports USB
- Masquage et blocage de l'accès aux disques locaux
- Blocage des consoles PowerShell et Invite de commandes
- Déploiement d'un fond d'écran personnalisé
- Mappage des lecteurs réseau (personnel et transfert)
- Redirection des dossiers utilisateurs
- Mise en place d'une politique de mot de passe sécurisé

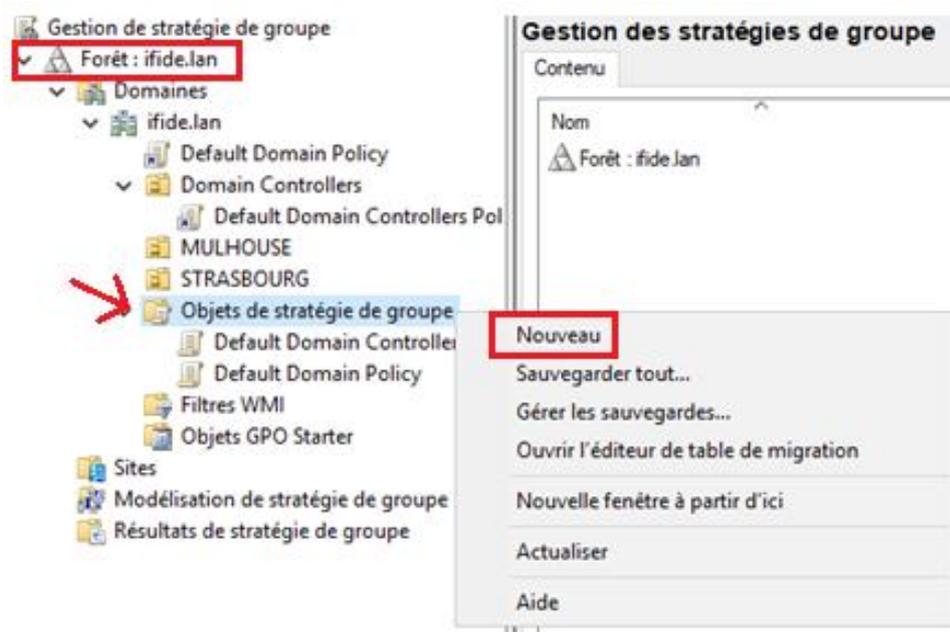
Création et configuration des stratégies de groupe (GPO)

Pour accéder à la configuration des GPO, ouvrez l'outil d'administration nommé **Gestion des stratégies de groupe**, accessible soit depuis le menu Démarrer, soit directement via le **Gestionnaire de serveur**.

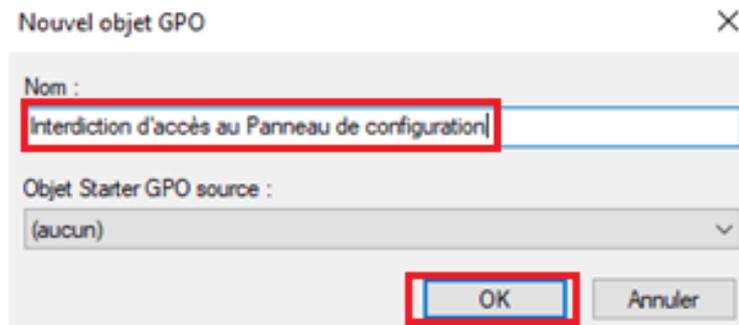


Une fois dans la **Gestion des stratégies de groupe**, sélectionnez la **forêt principale**, puis naviguez jusqu'à **Objets de stratégie de groupe**.

Faites un **clic droit** dessus, puis cliquez sur **Nouveau** pour créer une nouvelle stratégie.



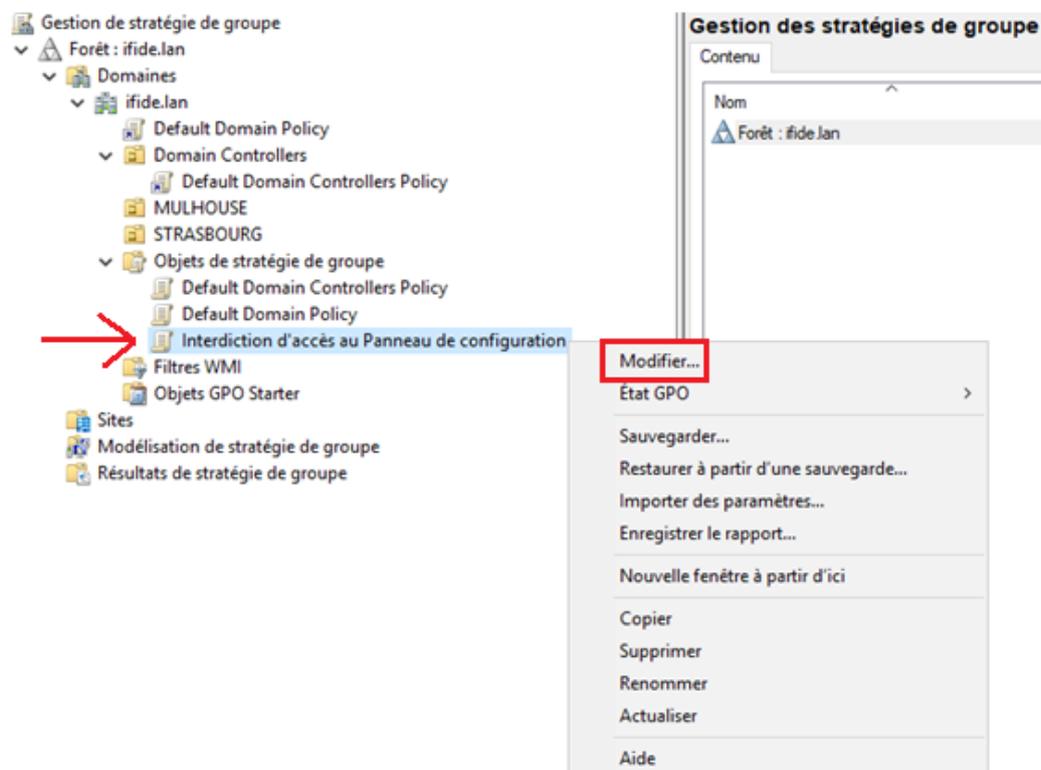
Attribuez un nom à la stratégie afin de pouvoir l'identifier facilement par la suite.



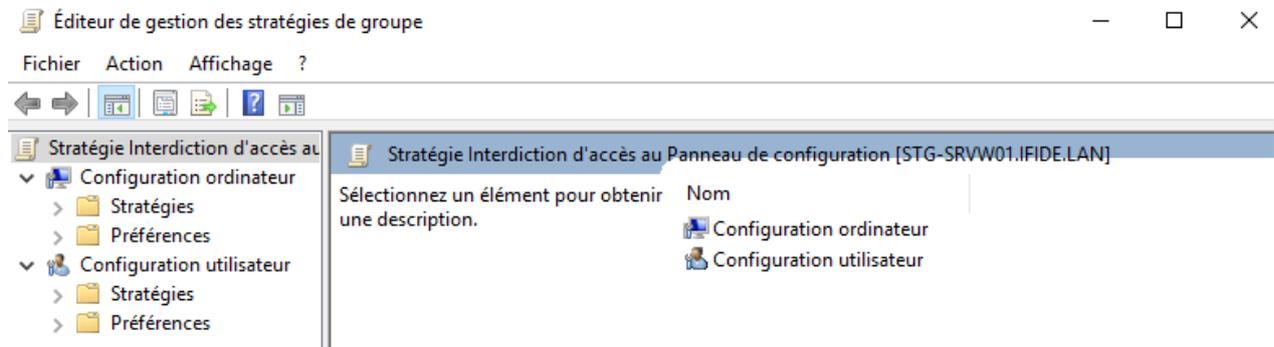
Une fois créée, la stratégie apparaîtra dans la **liste des stratégies** de votre forêt.

Interdiction d'accès au panneau de configuration

Ensuite, sélectionnez la GPO souhaitée, effectuez un clic droit dessus, puis choisissez Modifier.



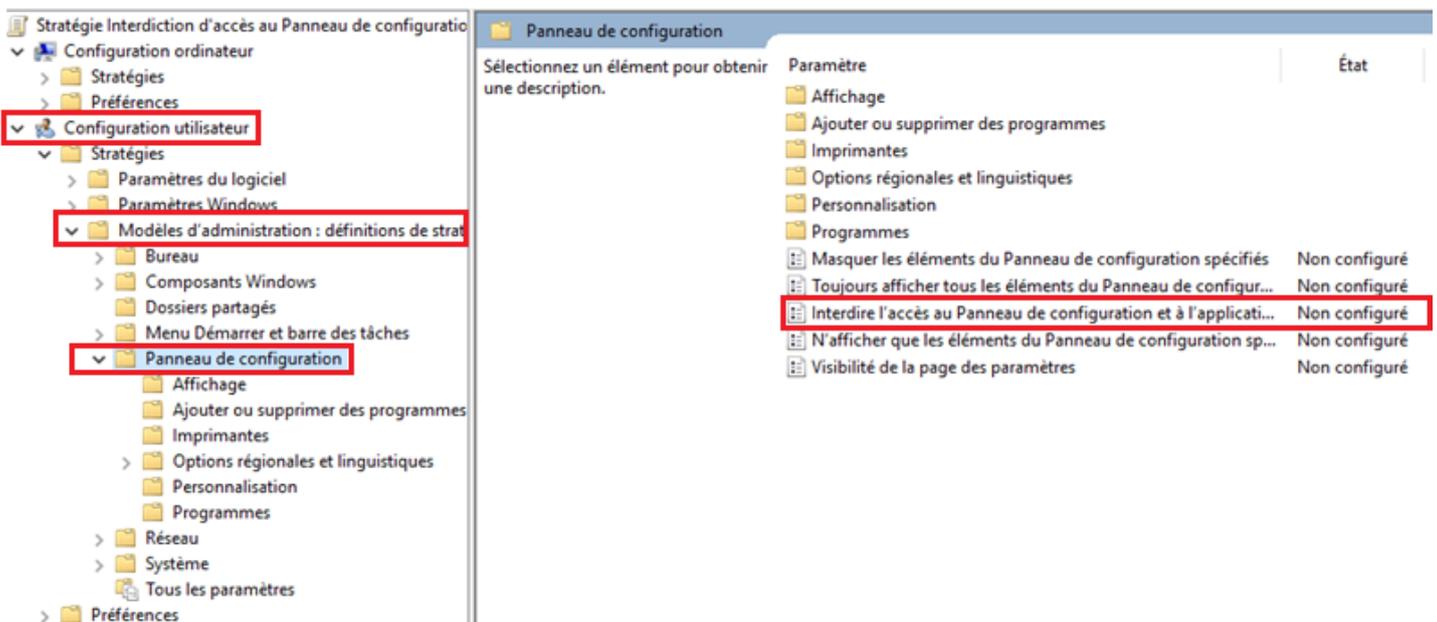
Nous voici désormais dans l'Éditeur de stratégie de groupe.



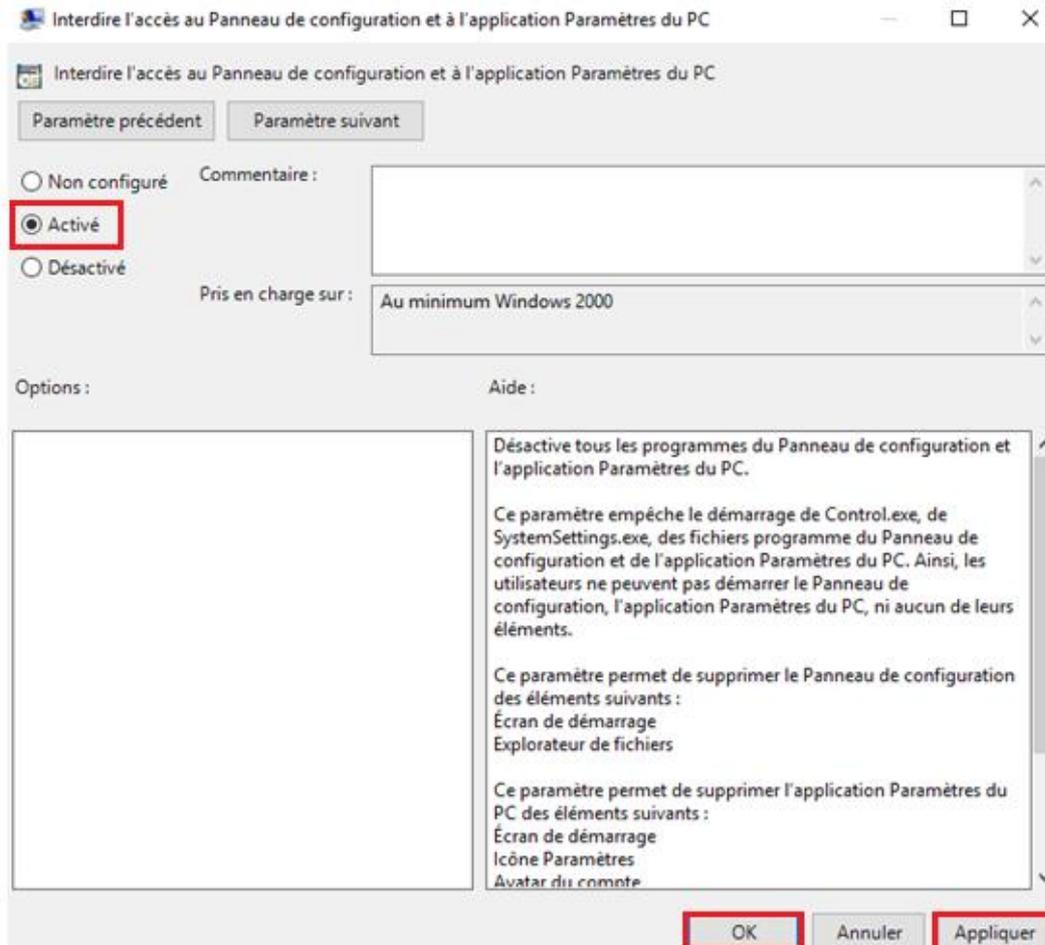
Ensuite, configurez la stratégie de groupe. Dans ce contexte, les paramètres s'appliqueront principalement aux **utilisateurs**, il s'agit donc d'une **stratégie utilisateur**, appliquée à la **connexion de session**.

À l'inverse, une stratégie de type **ordinateur** s'applique au **démarrage de la machine**.

Déroulez le menu **Configuration utilisateur** → **Modèles d'administration** → cliquez sur **Panneau de configuration** → puis double-cliquez sur **Interdire l'accès au Panneau de configuration et à l'application Paramètres PC**.



Cochez l'option **"Activé"**, puis cliquez sur **"Appliquer"**, et enfin sur **"OK"** pour valider les modifications.



Notre première GPO est ainsi **configurée**. ✓

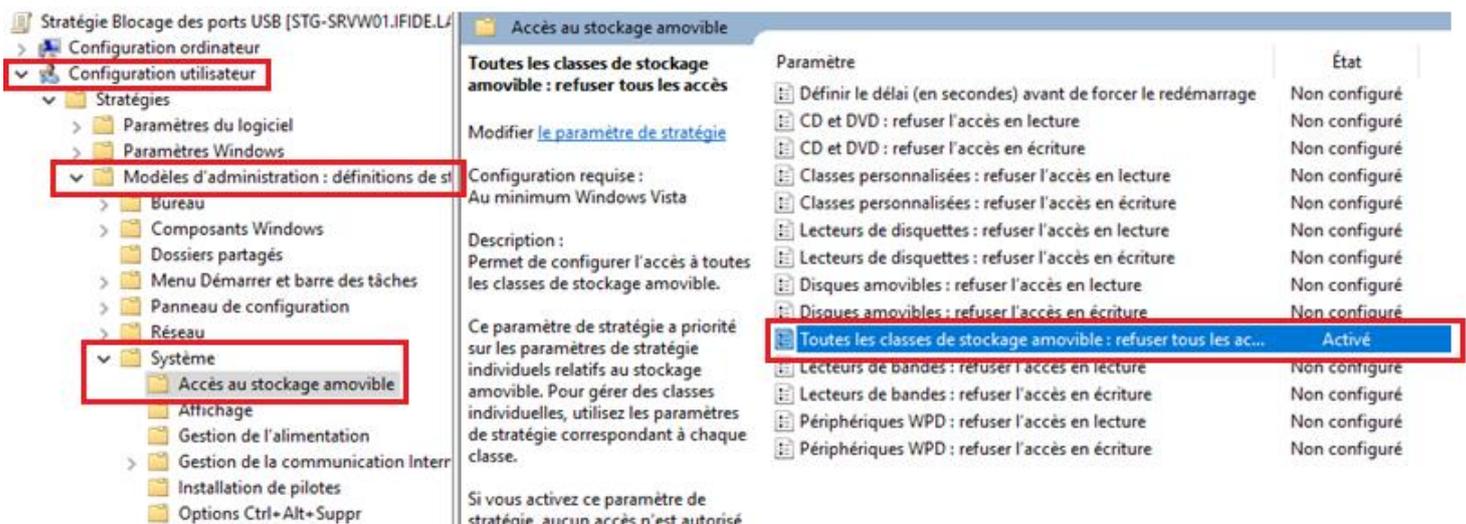
Blocage des ports USB

Comme pour la première stratégie, nous allons **créer une nouvelle règle** afin de mieux nous y retrouver.

Une fois créée, effectuez un clic droit dessus, puis cliquez sur **Modifier**.

Nous restons dans la section "**Configuration utilisateur**", car cette stratégie s'applique principalement aux utilisateurs.

Ensuite, accédez à "**Modèles d'administration**" → "**Système**" → "**Accès au stockage amovible**", puis double-cliquez sur "**Toutes les classes de stockage amovible : refuser tous les accès**".



The screenshot shows the Windows Group Policy Editor interface. The left-hand navigation pane is expanded to show the path: Configuration utilisateur > Modèles d'administration : définitions de stratégie > Système > Accès au stockage amovible. The main pane displays the details for the strategy 'Toutes les classes de stockage amovible : refuser tous les accès'. The 'État' (State) column shows that this strategy is 'Activé' (Enabled), which is highlighted with a red box. Other strategies listed include 'Définir le délai...', 'CD et DVD : refuser l'accès...', 'Classes personnalisées...', 'Lecteurs de disquettes...', 'Disques amovibles...', 'Lecteurs de bandes...', and 'Périphériques WPD...'. The 'État' for these other strategies is 'Non configuré'.

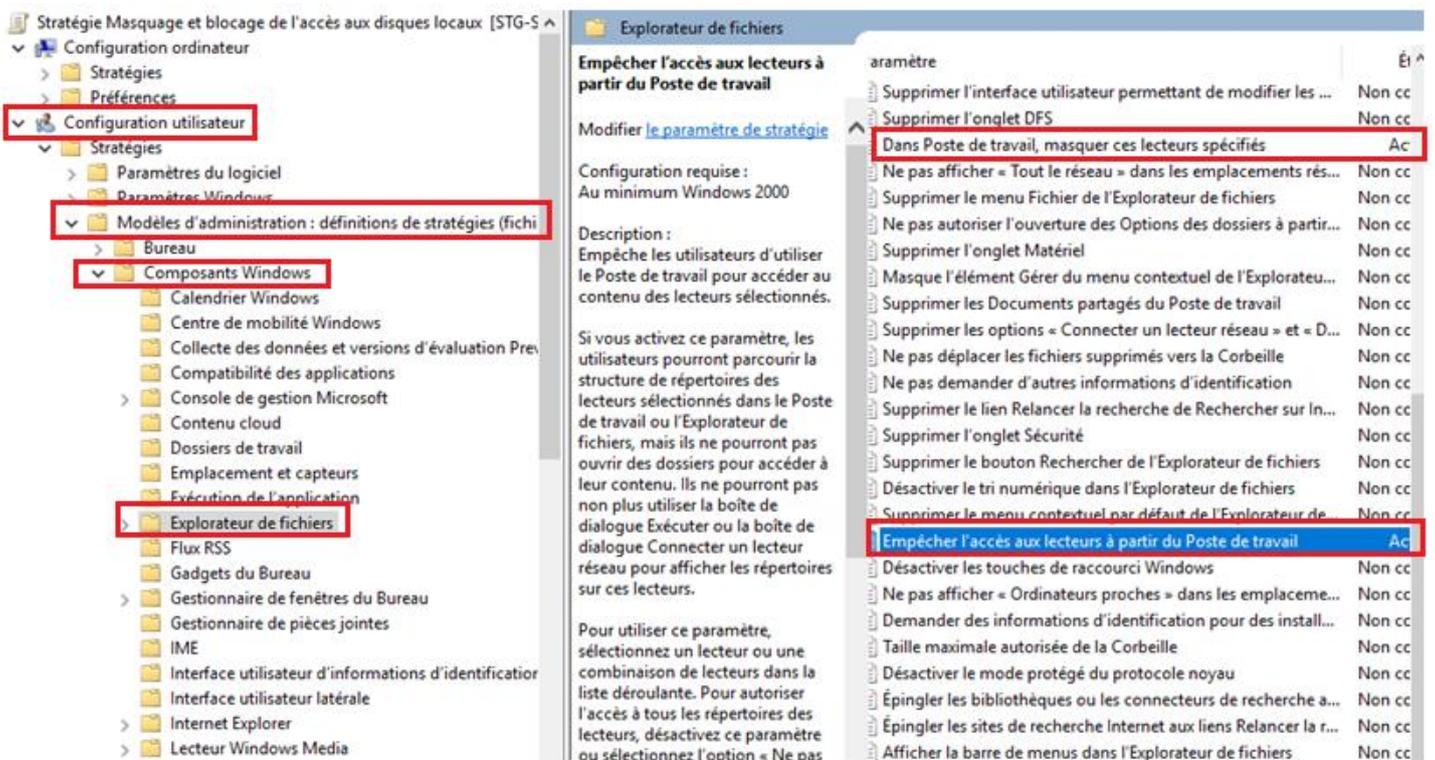
Paramètre	État
Définir le délai (en secondes) avant de forcer le redémarrage	Non configuré
CD et DVD : refuser l'accès en lecture	Non configuré
CD et DVD : refuser l'accès en écriture	Non configuré
Classes personnalisées : refuser l'accès en lecture	Non configuré
Classes personnalisées : refuser l'accès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

Cochez l'option "**Activé**", puis cliquez sur "**Appliquer**", et enfin sur "**OK**" pour valider les modifications.

Masquage et blocage de l'accès aux disques locaux

Déroulez le menu "Configuration utilisateur" → "Modèles d'administration" → "Composants Windows" → "Explorateur de fichiers".

Double-cliquez ensuite sur "Dans Poste de travail, masquer ces lecteurs spécifiés", puis sur "Empêcher l'accès aux lecteurs à partir du Poste de travail".



The screenshot shows the Group Policy Editor window titled "Stratégie Masquage et blocage de l'accès aux disques locaux [STG-5]". The left-hand navigation pane is expanded to show the following path: Configuration ordinateur > Configuration utilisateur > Modèles d'administration : définitions de stratégies (fichiers) > Bureau > Composants Windows > Explorateur de fichiers. The right-hand pane displays the policy "Empêcher l'accès aux lecteurs à partir du Poste de travail". The policy is currently set to "Non configuré". A list of related policies is shown on the right, with "Dans Poste de travail, masquer ces lecteurs spécifiés" and "Empêcher l'accès aux lecteurs à partir du Poste de travail" highlighted in red and blue respectively.

Paramètre	État
Supprimer l'interface utilisateur permettant de modifier les ...	Non cc
Supprimer l'onglet DFS	Non cc
Dans Poste de travail, masquer ces lecteurs spécifiés	Ac
Ne pas afficher « Tout le réseau » dans les emplacements rés...	Non cc
Supprimer le menu Fichier de l'Explorateur de fichiers	Non cc
Ne pas autoriser l'ouverture des Options des dossiers à partir...	Non cc
Supprimer l'onglet Matériel	Non cc
Masque l'élément Gérer du menu contextuel de l'Explorateur...	Non cc
Supprimer les Documents partagés du Poste de travail	Non cc
Supprimer les options « Connecter un lecteur réseau » et « D...	Non cc
Ne pas déplacer les fichiers supprimés vers la Corbeille	Non cc
Ne pas demander d'autres informations d'identification	Non cc
Supprimer le lien Relancer la recherche de Rechercher sur In...	Non cc
Supprimer l'onglet Sécurité	Non cc
Supprimer le bouton Rechercher de l'Explorateur de fichiers	Non cc
Désactiver le tri numérique dans l'Explorateur de fichiers	Non cc
Supprimer le menu contextuel par défaut de l'Explorateur de...	Non cc
Empêcher l'accès aux lecteurs à partir du Poste de travail	Ac
Désactiver les touches de raccourci Windows	Non cc
Ne pas afficher « Ordinateurs proches » dans les emplace...	Non cc
Demander des informations d'identification pour des install...	Non cc
Taille maximale autorisée de la Corbeille	Non cc
Désactiver le mode protégé du protocole noyau	Non cc
Épingler les bibliothèques ou les connecteurs de recherche a...	Non cc
Épingler les sites de recherche Internet aux liens Relancer la r...	Non cc
Afficher la barre de menus dans l'Explorateur de fichiers	Non cc

Cochez l'option "**Activé**", puis dans les **options situées en dessous**, sélectionnez "**Restreindre au lecteur C uniquement**".

Cliquez sur **Appliquer**, puis sur **OK**. (Répétez cette configuration pour la seconde règle également.)



The screenshot shows the Windows Group Policy Editor interface for the policy "Dans Poste de travail, masquer ces lecteurs spécifiés". The policy is set to "Activé" (Active), which is highlighted with a red box. Below this, the "Options" section shows a dropdown menu with "Restreindre au lecteur C uniquement" selected, also highlighted with a red box. The "Aide" (Help) section provides detailed information about the policy, including its purpose and usage instructions.

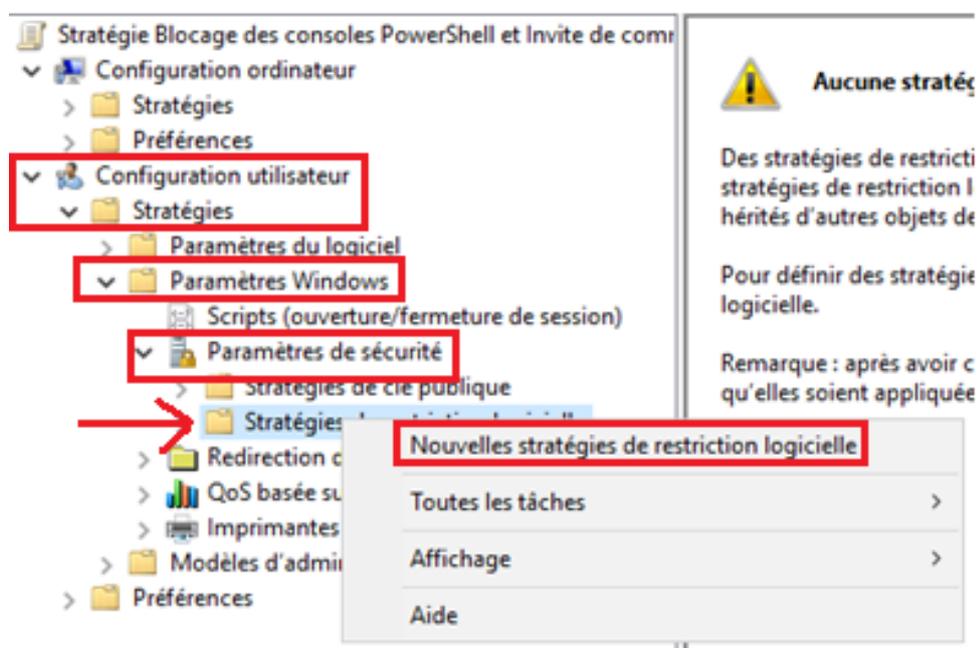
Nous allons à présent créer notre **dernière règle**, qui aura pour objectif de **bloquer l'accès aux commandes PowerShell** ainsi qu'à l'**Invite de commandes (cmd)**.

Blocage des consoles PowerShell et Invite de commandes

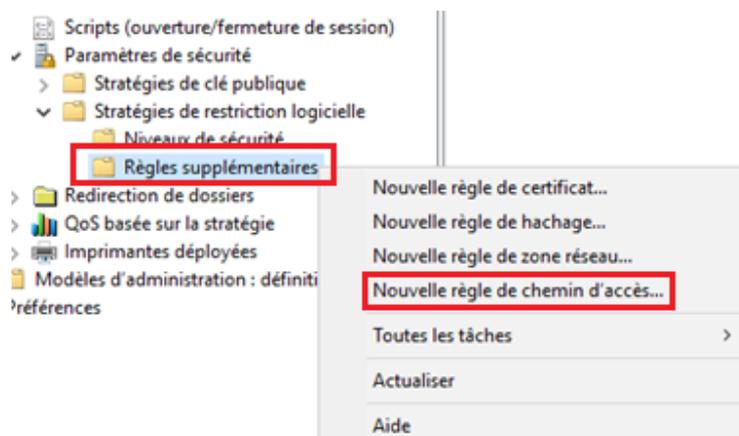
Le blocage de PowerShell nécessite une méthode un peu plus avancée.

Déroulez le menu "Configuration utilisateur" → "Stratégies" → "Paramètres Windows" → "Paramètres de sécurité".

Effectuez un clic droit sur "Stratégies de restriction logicielle", puis sélectionnez "Créer une nouvelle stratégie".



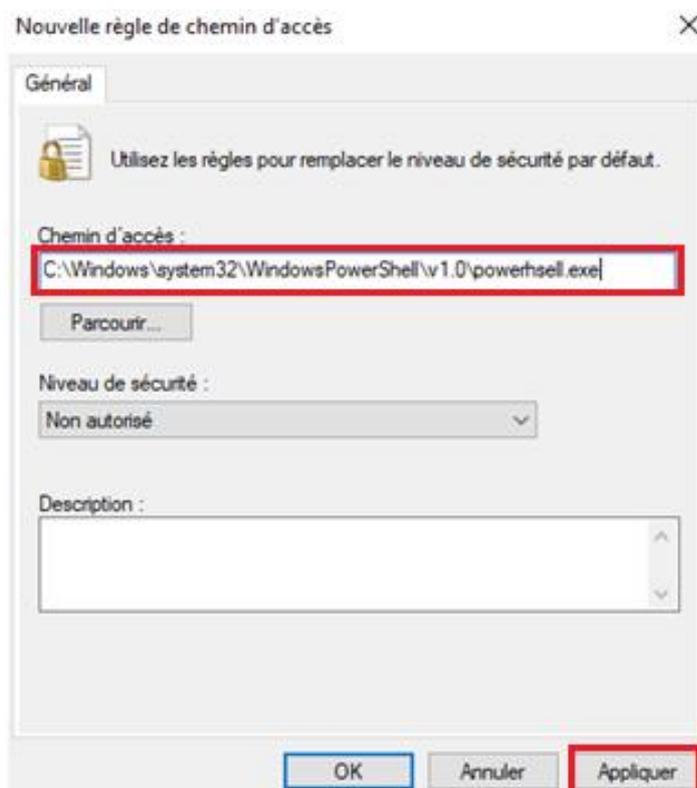
Par la suite, deux nouveaux menus apparaissent. Effectuez un clic droit sur "Règles supplémentaires", puis cliquez sur "Créer une nouvelle règle de chemin d'accès".



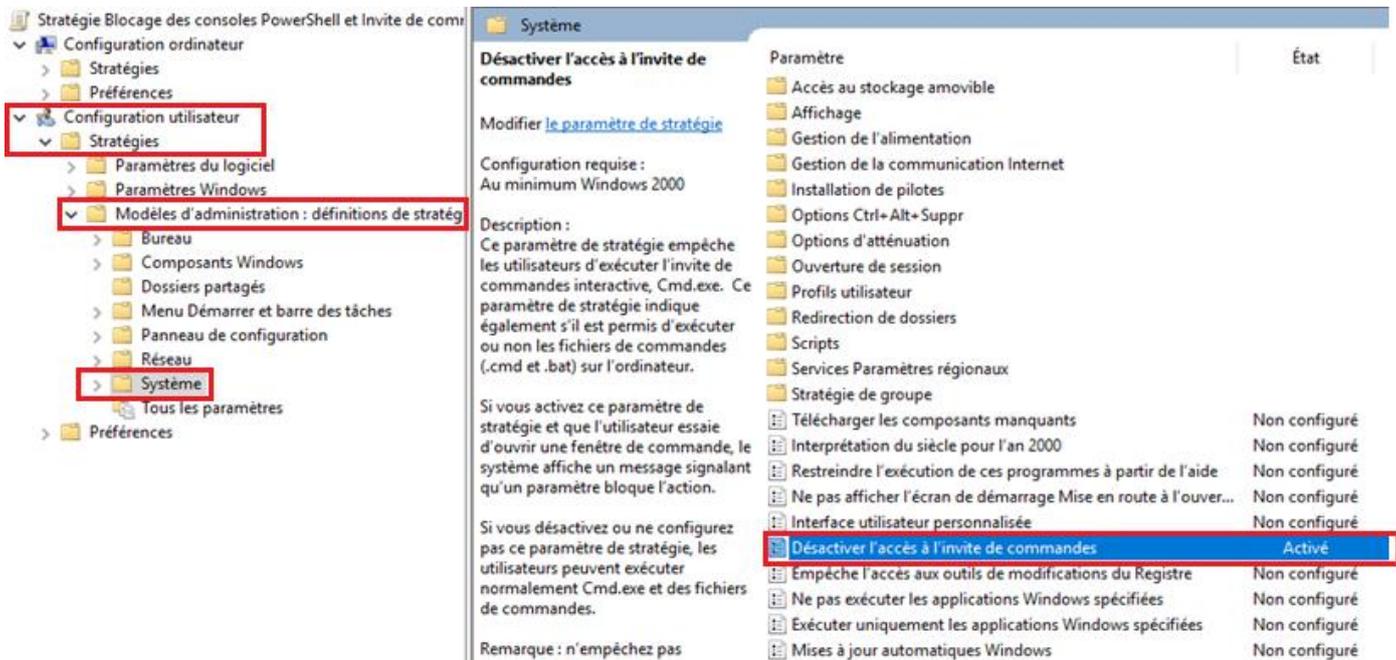
Par défaut, PowerShell est installé à l'emplacement suivant sur Windows :

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

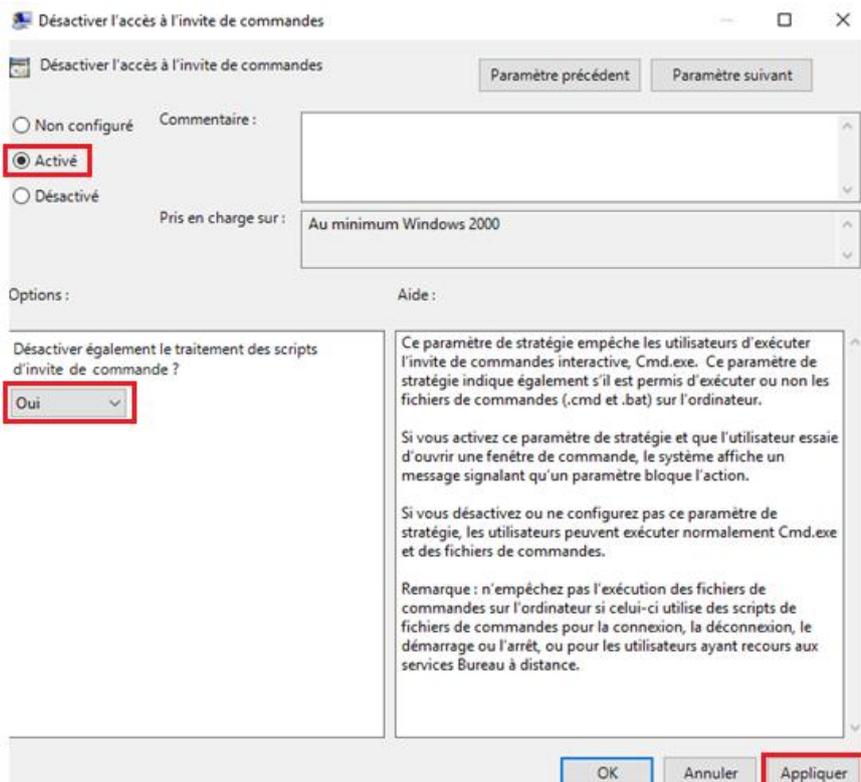
Spécifiez le chemin, définissez le niveau de sécurité souhaité (par exemple "Non autorisé"), puis cliquez sur **Appliquer**.



À présent, pour bloquer l'accès à l'invite de commandes, procédez comme suit :
 Déroulez le menu "Configuration utilisateur" → "Modèles d'administration" →
 "Système", puis double-cliquez sur "Désactiver l'accès à l'invite de commandes".



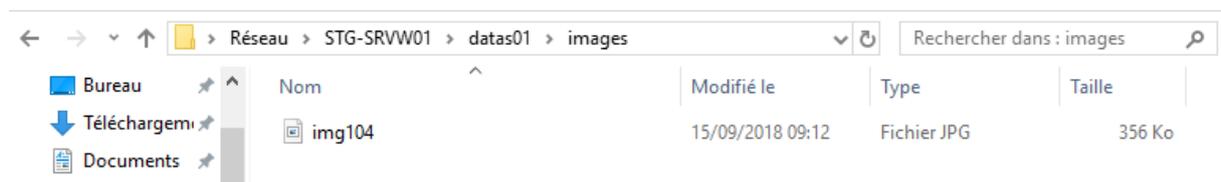
Cochez la case "Activé".
 Vous pouvez choisir de
 laisser les scripts de
 l'invite de commandes
 actifs si nécessaire, mais
 les bloquer peut
 également apporter une
 couche de sécurité
 supplémentaire.
 Cliquez ensuite sur
 Appliquer, puis sur OK.



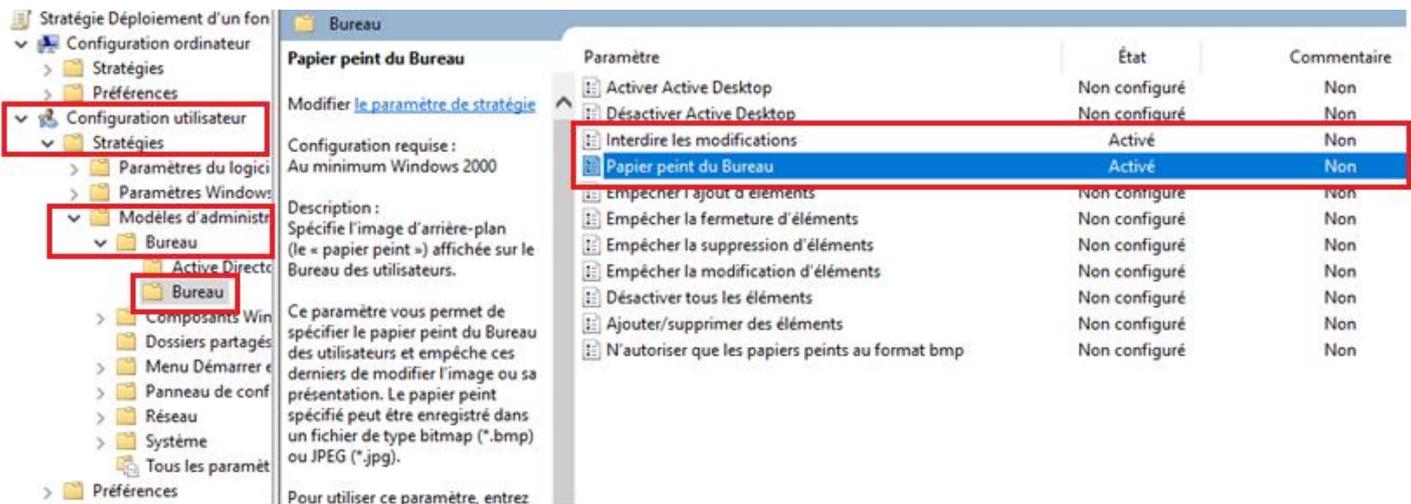
Déploiement d'un fond d'écran personnalisé

Tout d'abord, placez l'image dans un dossier partagé, de préférence situé dans un dossier accessible via l'espace de noms DFS.

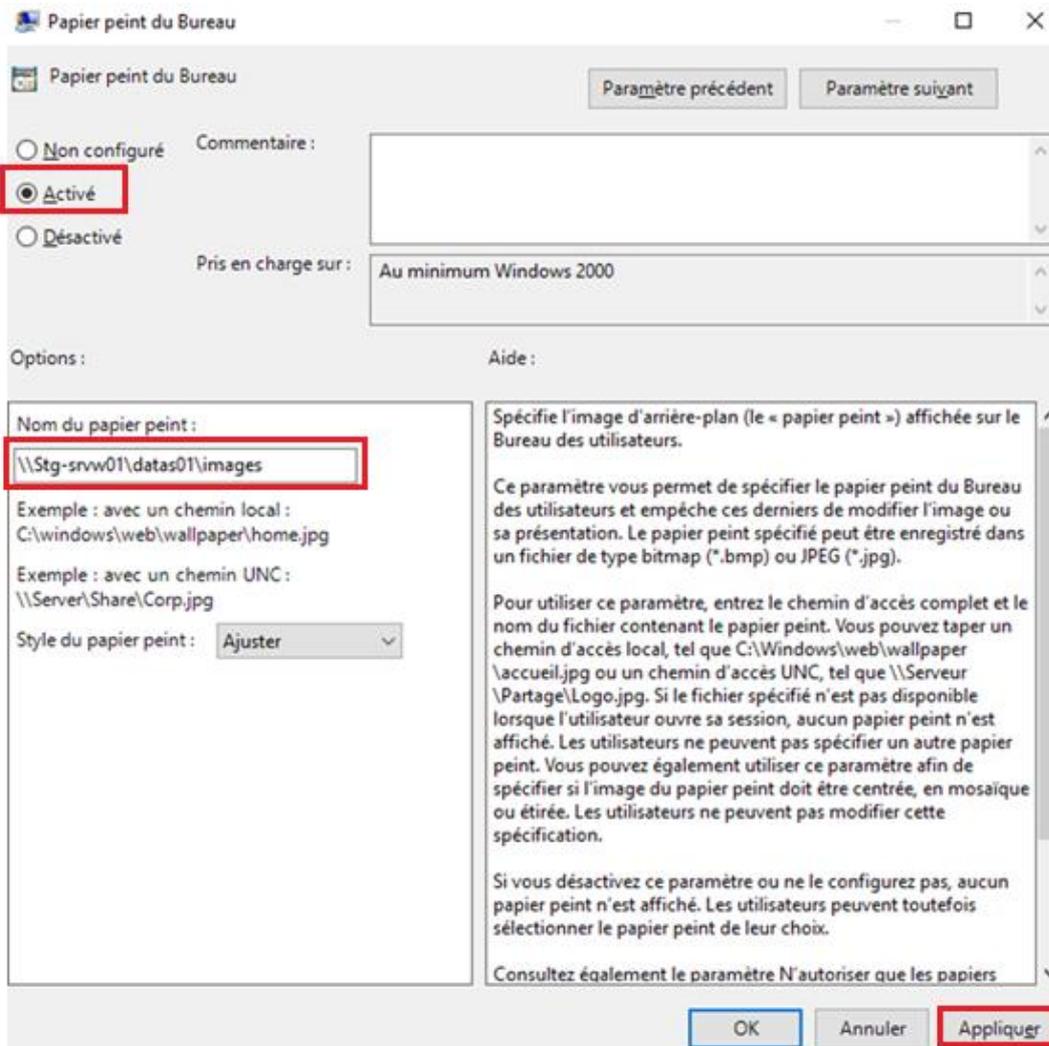
Ce dossier doit être accessible en lecture pour les utilisateurs, mais il est recommandé de restreindre la consultation du contenu afin d'éviter toute suppression accidentelle par un utilisateur.



Ensuite, dans la configuration de la GPO, accédez à : **Configuration utilisateur** → **Stratégies** → **Modèles d'administration** → **Bureau** → **Bureau**, puis double-cliquez ici :



Cochez la case « **Activé** », puis dans le champ « **Nom du papier peint** », indiquez le chemin réseau vers l'image (par exemple \\STG-SRVW01\datas01\images
Cliquez ensuite sur **Appliquer**, puis **OK**.



Papier peint du Bureau

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

Désactivé

Pris en charge sur : Au minimum Windows 2000

Options : Aide :

Nom du papier peint : \\Stg-srvw01\datas01\images

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

Exemple : avec un chemin UNC : \\Server\Share\Corp.jpg

Style du papier peint : Ajuster

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

Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l'image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (*.bmp) ou JPEG (*.jpg).

Pour utiliser ce paramètre, entrez le chemin d'accès complet et le nom du fichier contenant le papier peint. Vous pouvez taper un chemin d'accès local, tel que C:\Windows\web\wallpaper\accueil.jpg ou un chemin d'accès UNC, tel que \\Serveur\Partage\Logo.jpg. Si le fichier spécifié n'est pas disponible lorsque l'utilisateur ouvre sa session, aucun papier peint n'est affiché. Les utilisateurs ne peuvent pas spécifier un autre papier peint. Vous pouvez également utiliser ce paramètre afin de spécifier si l'image du papier peint doit être centrée, en mosaïque ou étirée. Les utilisateurs ne peuvent pas modifier cette spécification.

Si vous désactivez ce paramètre ou ne le configurez pas, aucun papier peint n'est affiché. Les utilisateurs peuvent toutefois sélectionner le papier peint de leur choix.

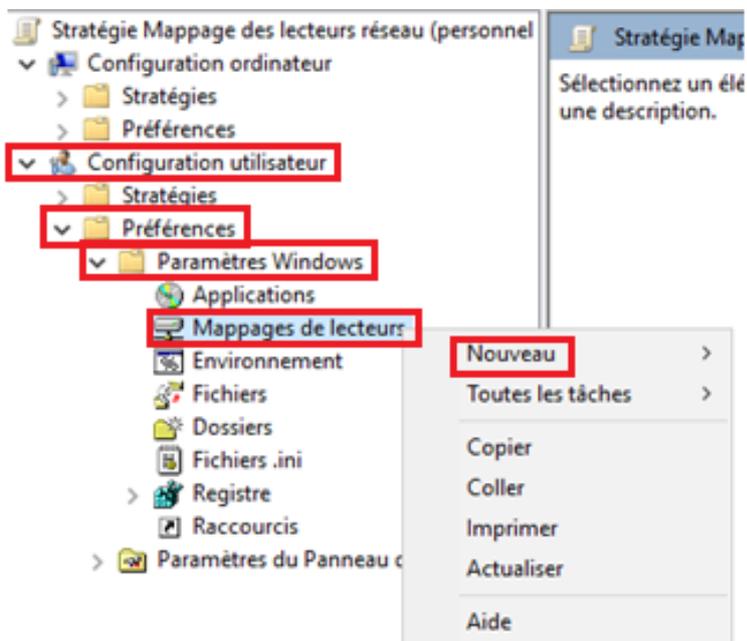
Consultez également le paramètre N'autoriser que les papiers

OK Annuler **Appliquer**

Mappage des lecteurs réseau (personnel et transfert)

Mappage lecteur T

Rendez-vous dans **Configuration utilisateur** → **Préférences** → **Paramètres Windows**, puis effectuez un clic droit sur **Mappage de lecteur** et sélectionnez **Nouveau** → **Lecteur**.



Sélectionnez l'action **Mettre à jour** (le lecteur sera créé s'il n'existe pas encore, et mis à jour s'il est déjà présent), indiquez le **chemin réseau** du partage, choisissez la **lettre de lecteur** à attribuer, puis cliquez sur **Appliquer**.

Nouvelles propriétés de Lecteur ×

Général Commun

 Action : Mettre à jour ▼

Emplacement : \\fide.lan\intranet\DATAS\TRANSFERT ...

Reconnecter : Libeller en tant que : TRANSFERT

Lettre de lecteur

Utiliser le premier disponible, en commençant à :

Utiliser : T ▼

Se connecter en tant que (facultatif)

Nom d'utilisateur :

Mot de passe : Confirmer le mot de passe

Masquer/Afficher ce lecteur

Aucune modification

Masquer ce lecteur

Afficher ce lecteur

Masquer/Afficher tous les lecteurs

Aucune modification

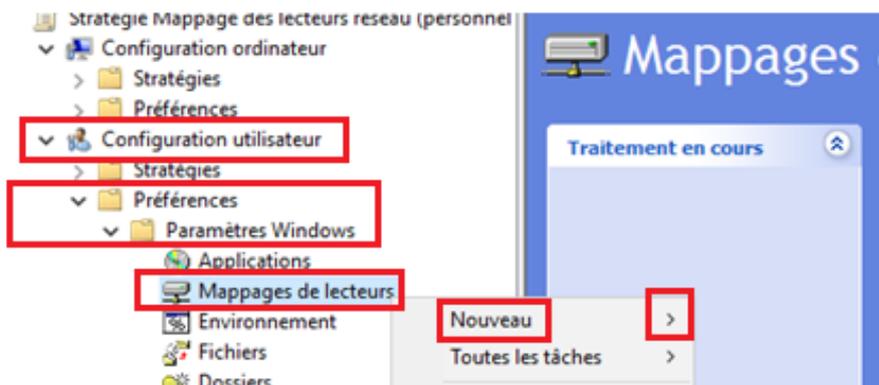
Masquer tous les lecteurs

Afficher tous les lecteurs

OK
Annuler
Appliquer
Aide

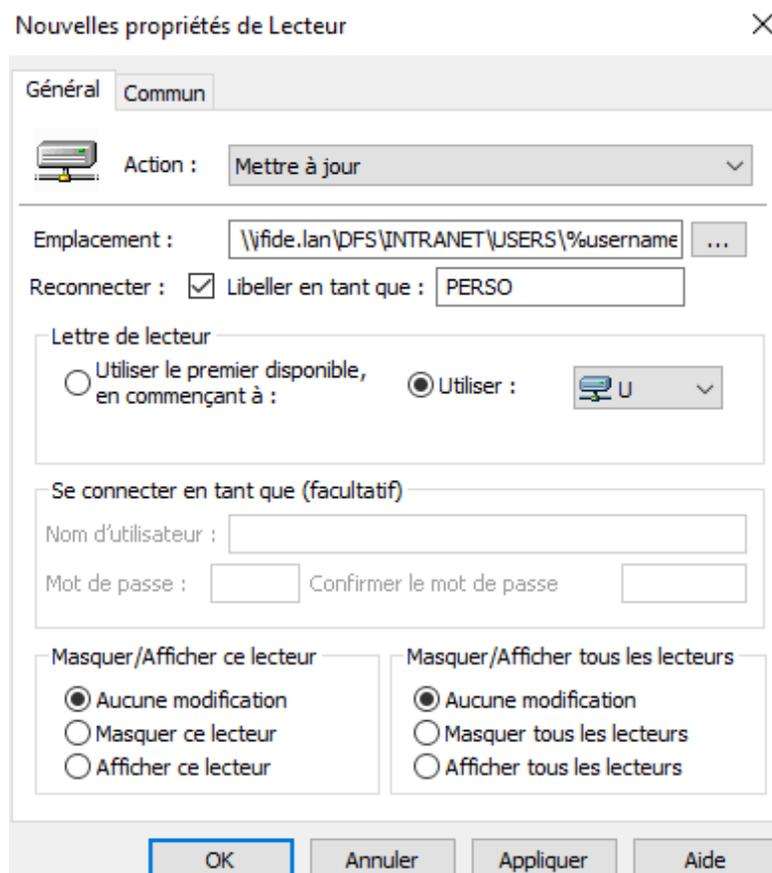
Mappage lecteur U

Pour le mappage du **lecteur personnel**, accédez à **Configuration utilisateur** → **Préférences** → **Paramètres Windows**, puis ajoutez un **nouveau lecteur mappé**.



Choisissez l'action **Mettre à jour**.

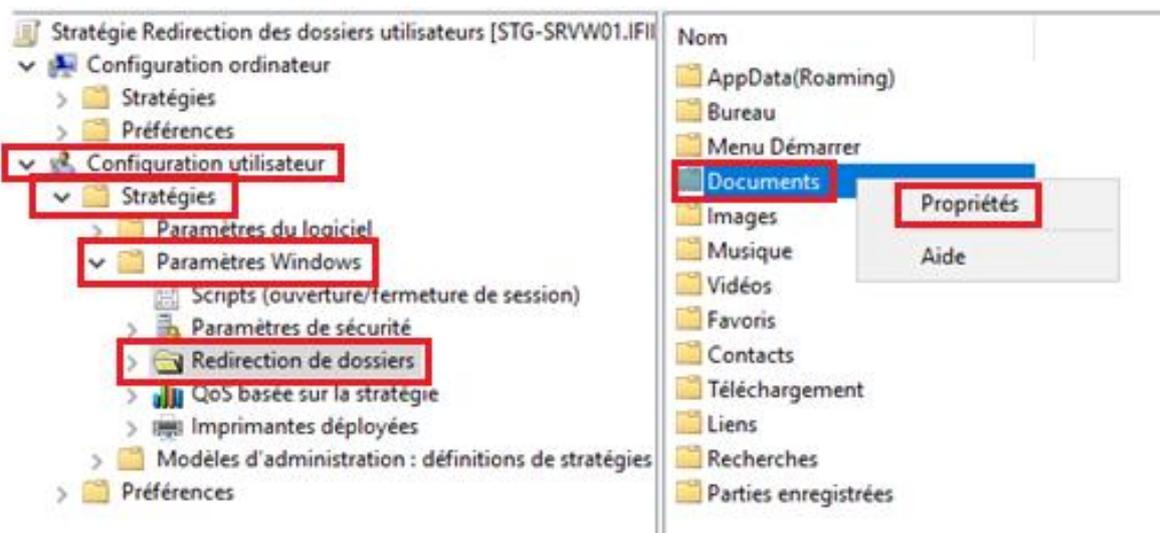
Dans le champ **Emplacement**, indiquez le chemin du dossier cible, en y ajoutant la variable **%username%** pour faire référence automatiquement à l'utilisateur connecté. Enfin, affectez la lettre de lecteur réseau **U**:



Redirection des dossiers utilisateurs

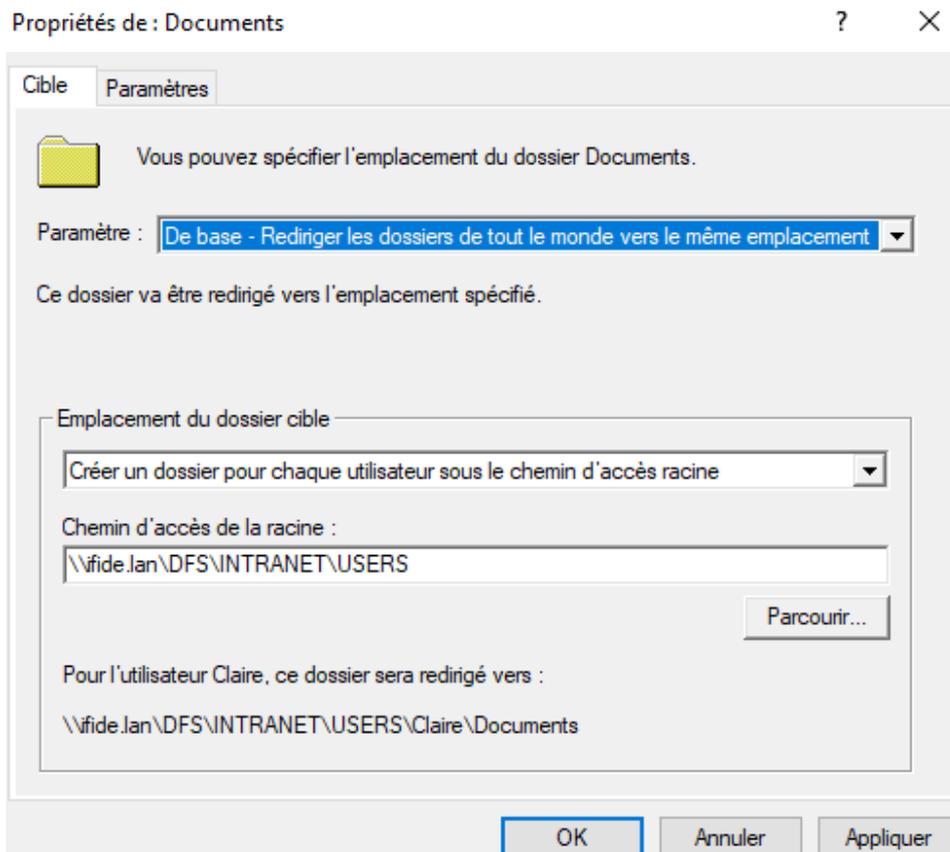
Dans la configuration de la GPO, accédez à **Configuration utilisateur** → **Stratégies** → **Paramètres Windows** → **Redirection de dossier**.

Dans un premier temps, nous allons procéder à la redirection du dossier "Documents".



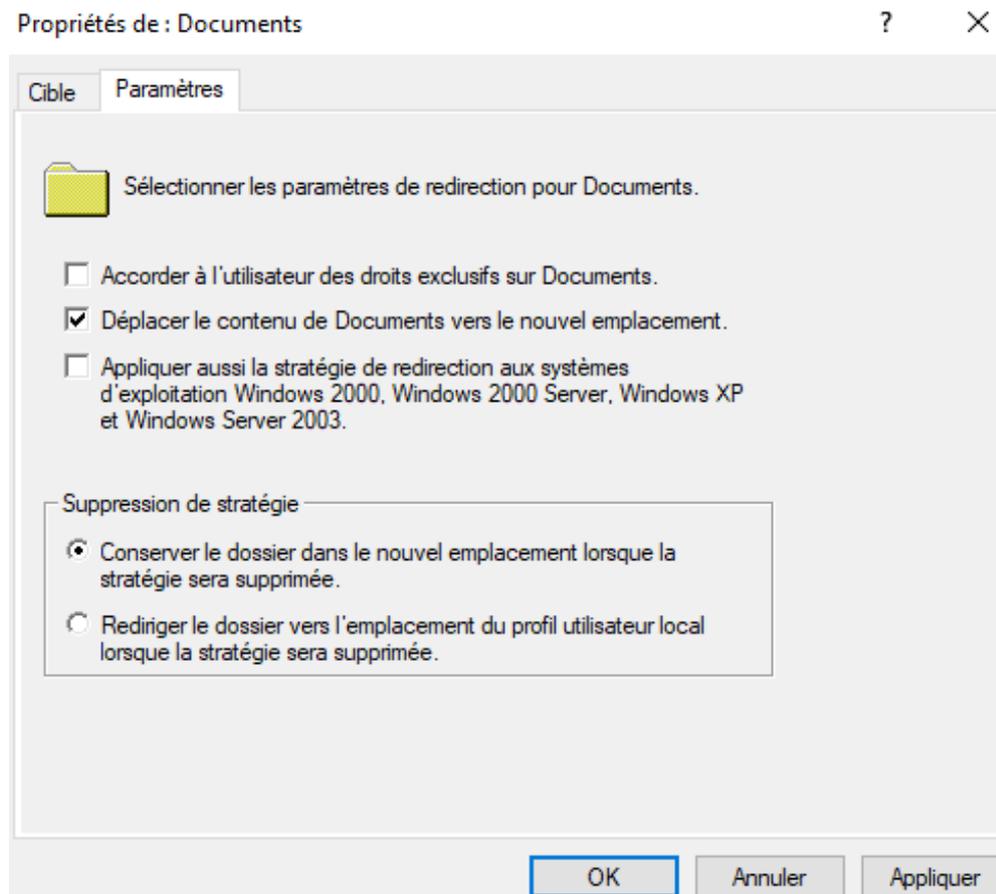
Sélectionnez le paramètre « De base », puis dans l'emplacement du dossier cible, choisissez l'option « Créer un dossier pour chaque utilisateur sous le chemin d'accès racine ».

Indiquez ensuite le chemin du dossier racine dans lequel seront créés les dossiers personnels des utilisateurs.



Dans l'onglet **Paramètres**, ne cochez pas l'option « **Accorder à l'utilisateur des droits exclusifs sur Documents** », afin de permettre aux administrateurs d'avoir accès aux dossiers des utilisateurs.

Cliquez ensuite sur **Appliquer**, puis sur **OK**.

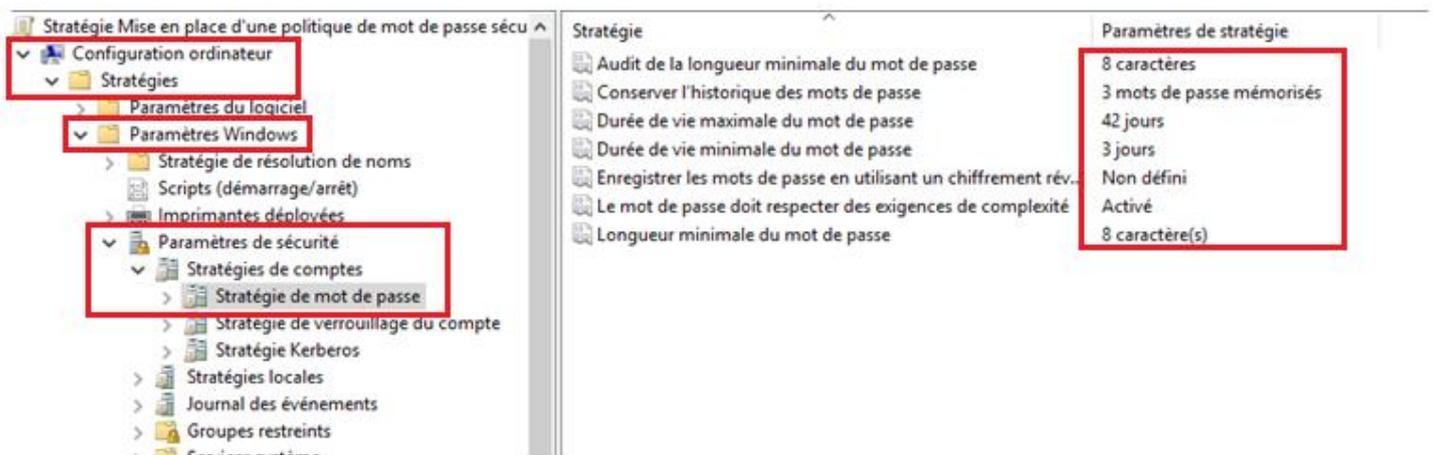


Répétez les mêmes étapes pour configurer la **redirection du dossier Bureau**, en suivant la même logique que pour le dossier Documents.

Mise en place d'une politique de mot de passe sécurisé

Etant une stratégie de groupe qui est effective avant la connexion à la session utilisateur, cette stratégie s'effectuera donc sur la configuration ordinateur. Il est à noter que les valeurs suivantes sont pour le contexte de l'utilisateur, pour les administrateurs, la longueur de mot de passe recommandée est de 12 caractères avec obligation de mettre en place les complexités (caractères spéciaux, majuscules, minuscules).

Pour configurer la stratégie de groupe, allez dans **Configuration ordinateur** → **Stratégies** → **Paramètres Windows** → **Paramètres de sécurité** → **Stratégies de comptes** → **Stratégie de mot de passe**.



- Longueur minimale et Audit de la longueur minimale : définissent la longueur minimale du mot de passe, ici fixée à 8 caractères.
- Historique des mots de passe (par exemple 3) : empêche l'utilisateur ou l'administrateur de réutiliser les 3 derniers mots de passe saisis.
- Durée de vie maximale : détermine le nombre de jours avant que le mot de passe expire et doive être changé.
- Durée de vie minimale : oblige l'utilisateur à attendre un certain nombre de jours (ici 3) avant de pouvoir modifier son mot de passe à nouveau.

Ces stratégies contribuent à une meilleure sécurisation des mots de passe des utilisateurs. Toutefois, une autre stratégie complémentaire est recommandée : la stratégie de verrouillage de compte, permettant de se protéger contre les attaques par force brute ou tentatives malveillantes de mot de passe.

Stratégie	Paramètres de stratégie
Durée de verrouillage des comptes	0
Réinitialiser le compteur de verrouillages du compte après	30 minutes
Seuil de verrouillage du compte	5 tentatives d'ouvertures de sess...

Durée de verrouillage des comptes : correspond au temps pendant lequel un compte reste verrouillé après avoir atteint le seuil de tentatives échouées.

Si la valeur est définie sur 0, le compte restera verrouillé jusqu'à l'intervention d'un administrateur.

Seuil de verrouillage des comptes : détermine le nombre de tentatives de connexion échouées autorisées. Une fois ce seuil atteint, le compte est verrouillé automatiquement.

Les différentes stratégies de groupe ont bien été créées et nommées de manière explicite afin de faciliter leur gestion et leur application sur les utilisateurs et postes du domaine.

-  Objets de stratégie de groupe
 -  Blocage des consoles PowerShell et Invite de commandes
 -  Blocage des ports USB
 -  Default Domain Controllers Policy
 -  Default Domain Policy
 -  Déploiement d'un fond d'écran personnalisé
 -  Interdiction d'accès au Panneau de configuration
 -  Mappage des lecteurs réseau (personnel et transfert)
 -  Masquage et blocage de l'accès aux disques locaux
 -  Mise en place d'une politique de mot de passe sécurisé
 -  Redirection des dossiers utilisateurs

3.2.5) Configuration de la sauvegarde sur TrueNAS

Pour la configuration de la sauvegarde vers TrueNAS, nous allons suivre les étapes suivantes :

1. Configurer la cible iSCSI sur le serveur TrueNAS.
2. Depuis le serveur Windows, monter un disque avec la cible iSCSI (lecteur I:\) pour créer un SAN (Storage Area Network).
3. Planifier la sauvegarde sur ce disque monté.
4. Tester la sauvegarde et la restauration en supprimant une donnée sur le serveur.

Configuration de la cible iSCSI

Pour permettre à nos serveurs Windows d'utiliser les disques TrueNAS pour une sauvegarde externalisée, nous allons mettre en place des cibles iSCSI, un protocole IP de stockage réseau permettant de monter l'équivalent d'un disque local sur les serveurs.

Cependant, avant de procéder à la configuration des cibles iSCSI, il est nécessaire de créer un volume sur le serveur TrueNAS.

L'option recommandée pour cela est la création d'un Zvol.

Création d'un dataset Zvol

Depuis le menu **Storage** → **Pools** de l'interface TrueNAS, nous pouvons ajouter un volume Zvol comme illustré ci-dessous :

Volumes AJOUTER

BACKUPS01 (System Dataset Pool) ONLINE ✔ | 8.66 MiB (0%) Utilisé | 55.71 GiB Libre ⚙️ ^

Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
BACKUPS01	FILESYSTEM	8.66 MiB	55.71 GiB	lz4	15.90	false	OFF	

⋮

Actions dataset
 Ajouter un dataset
Ajouter un zvol
 Modifier les options
 Modifier les autorisations
 Quotas utilisateur
 Quotas de groupes
 Créer un instantané

Ensuite, donnez un nom au volume Zvol, spécifiez la taille du volume, **n'oubliez pas** de cocher **Force size**, pour forcer la taille du volume et éviter de rencontrer l'erreur que seule l'utilisation de 80% de la capacité du disque est recommandée.

Aussi, vous allez activer la fonctionnalité de **déduplication de données** sur le volume, qui permet de réduire les coûts de consommation de données en réduisant la quantité d'espace disque utilisée par les données **dupliquées et redondantes** sur le disque.

Lorsque vous avez terminé, cliquez sur **SUBMIT**.

Nom du zvol *

iSCSI-STG01

Commentaires

Taille pour ce zvol *

40 GiB

Taille de la force

Synchroniser

Niveau de compression *

lz4 (recommended)

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

On

Sparse

Lecture seule

Hériter (off)

Options de chiffrement

Héritage (non chiffré)

ENVOYER **ANNULER** **OPTIONS AVANCÉES**

Volumes **AJOUTER**

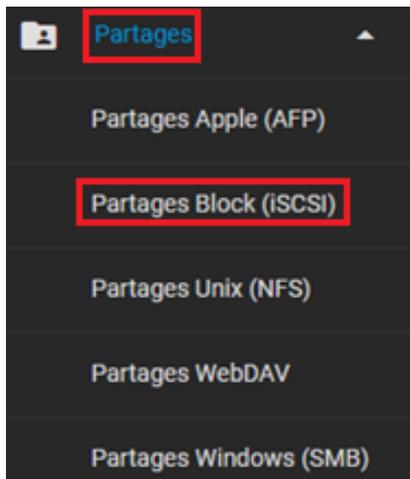
BACKUPS01 (System Dataset Pool) ONLINE ✔ | 40.64 GiB (73%) Utilisé | 15.08 GiB Libre

Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
BACKUPS01	FILESYSTEM	40.64 GiB	15.08 GiB	lz4	15.55	false	OFF	
iSCSI-STG01	VOLUME	40.63 GiB	55.71 GiB	lz4	1.00	false	ON	

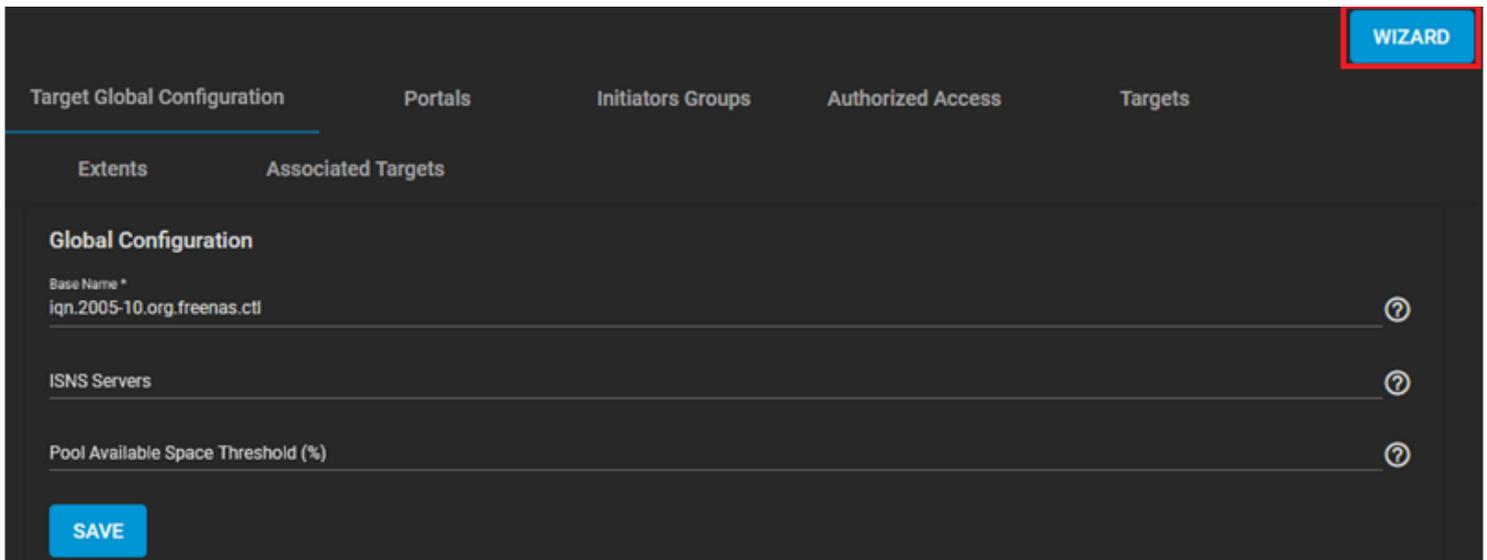
Le volume Zvol iSCSI-STG01 a été créé

Configuration de la cible et portail iSCSI

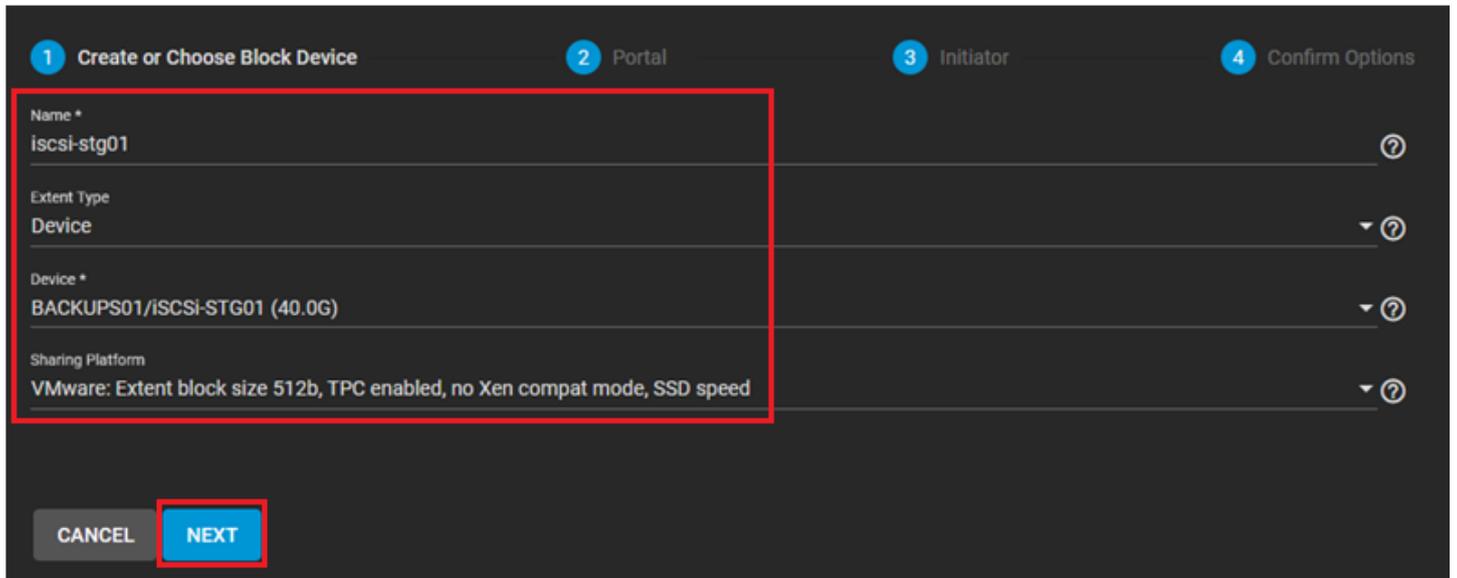
Sur l'interface web de TrueNAS, cliquez sur **Sharing** → **Block Shares (iSCSI)**



Ensuite, vous avez le choix entre configurer les options manuellement ou utiliser l'assistant de configuration (**Wizard**) qui vous guidera étape par étape.



Puis, remplissez les informations, et sélectionnez le pool de disque que nous avons créé précédemment.



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

Name *
iscsi-stg01

Extent Type
Device

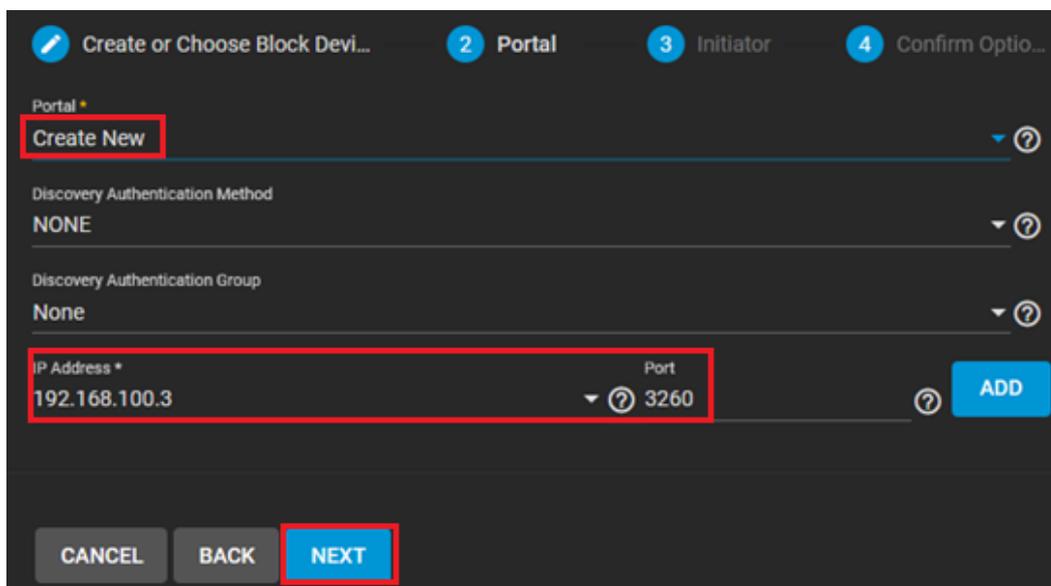
Device *
BACKUPS01/ISCSI-STG01 (40.0G)

Sharing Platform
VMware: Extent block size 512b, TPC enabled, no Xen compat mode, SSD speed

CANCEL NEXT

Ensuite, il est demandé de configurer le **portail iSCSI**. Ce sont ces informations qui **seront utilisées** lorsque vous **voudrez** vous connecter au serveur TrueNAS **depuis** le serveur Windows afin d'ajouter les disques (les Zvols) comme s'ils étaient des disques locaux.

Pour plus d'informations sur la sécurité, il est possible de sécuriser davantage la découverte en **ajoutant** une méthode d'authentification supplémentaire (par exemple, via CHAP). Cependant, dans le cadre de cette documentation technique, nous laisserons la méthode de découverte **sur NONE** (aucune authentification requise pour la découverte initiale).



1 Create or Choose Block Devi... 2 Portal 3 Initiator 4 Confirm Optio...

Portal *
Create New

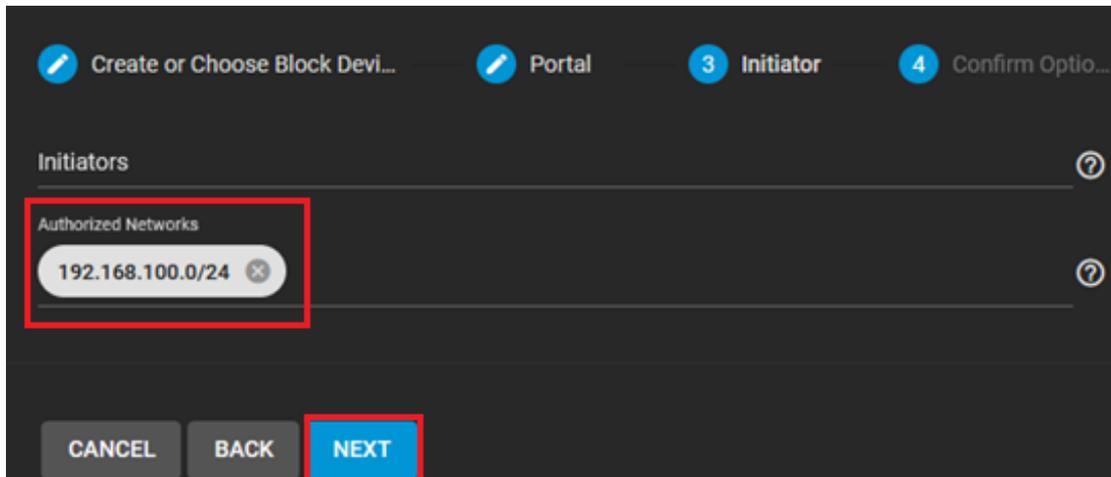
Discovery Authentication Method
NONE

Discovery Authentication Group
None

IP Address * Port
192.168.100.3 3260

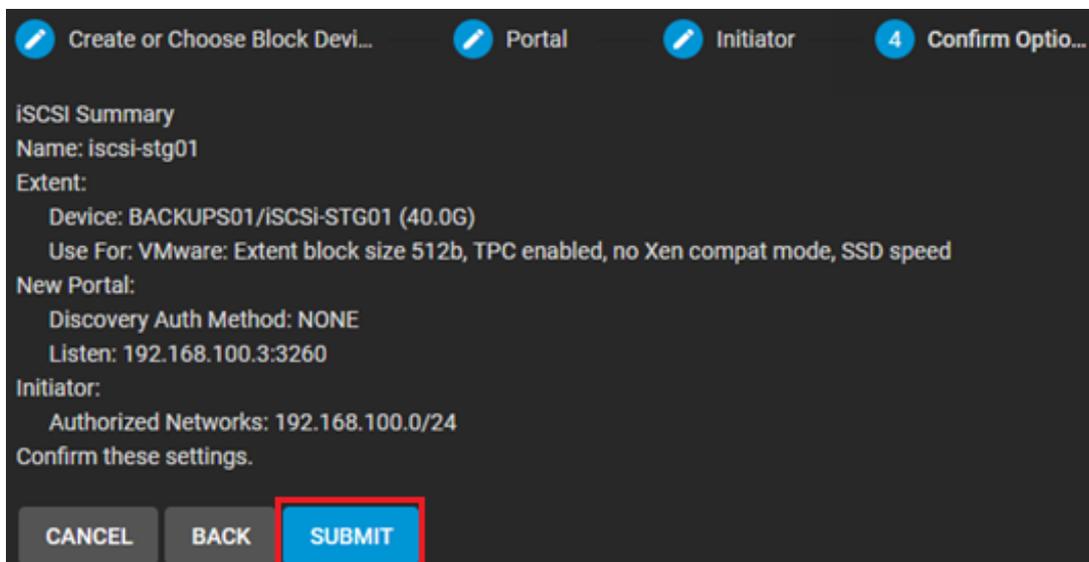
CANCEL BACK NEXT ADD

Puis, vous pouvez ajouter une couche de sécurité sur la découverte de votre stockage sur TrueNAS en restreignant l'accès aux machines provenant du sous-réseau **192.168.100.0/24**. Correspondant au sous-réseau de Strasbourg.



The screenshot shows the 'Initiator' configuration step in the TrueNAS web interface. The progress bar at the top indicates the current step is '3 Initiator'. The 'Authorized Networks' field is highlighted with a red box and contains the value '192.168.100.0/24'. The 'NEXT' button is also highlighted with a red box.

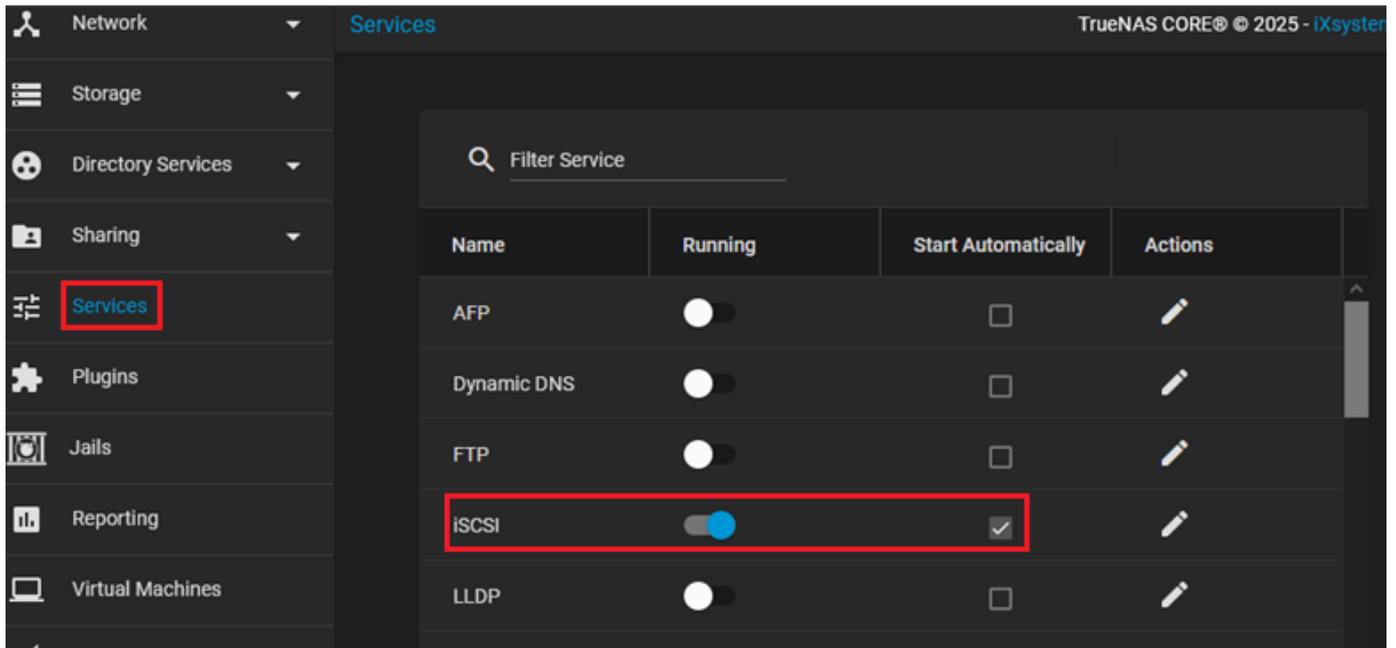
Un résumé des configurations saisies sera affiché. Vérifiez si des modifications sont nécessaires, puis cliquez sur **SUBMIT** pour finaliser.



The screenshot shows the 'iSCSI Summary' configuration step in the TrueNAS web interface. The progress bar at the top indicates the current step is '4 Confirm Optio...'. The 'SUBMIT' button is highlighted with a red box.

iSCSI Summary
Name: iscsi-stg01
Extent:
Device: BACKUPS01/iSCSI-STG01 (40.0G)
Use For: VMware: Extent block size 512b, TPC enabled, no Xen compat mode, SSD speed
New Portal:
Discovery Auth Method: NONE
Listen: 192.168.100.3:3260
Initiator:
Authorized Networks: 192.168.100.0/24
Confirm these settings.

Enfin, n'oubliez pas d'activer le service **iSCSI** sur TrueNAS. Pour ce faire, allez dans **Services**, activez le service **iSCSI** et cochez l'option "**Start automatically**" afin qu'il démarre à chaque redémarrage du serveur.

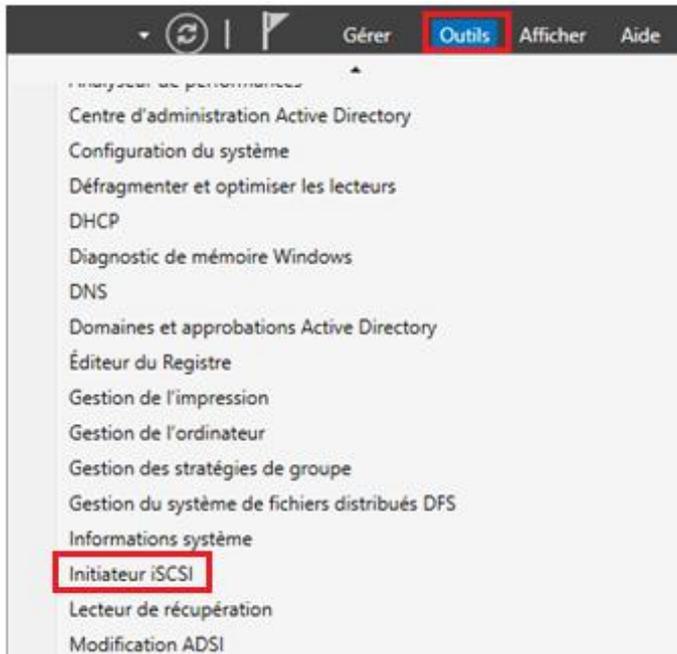


Maintenant, il vous faut monter le disque iSCSI sur le serveur Windows pour y effectuer les sauvegardes du serveur.

Affectation du nouveau disque iSCSI sur Windows Server

Découverte du portail iSCSI

Allez sur le **Gestionnaire de Serveurs**, puis cliquez sur **Outils** → **Initiateur iSCSI**.



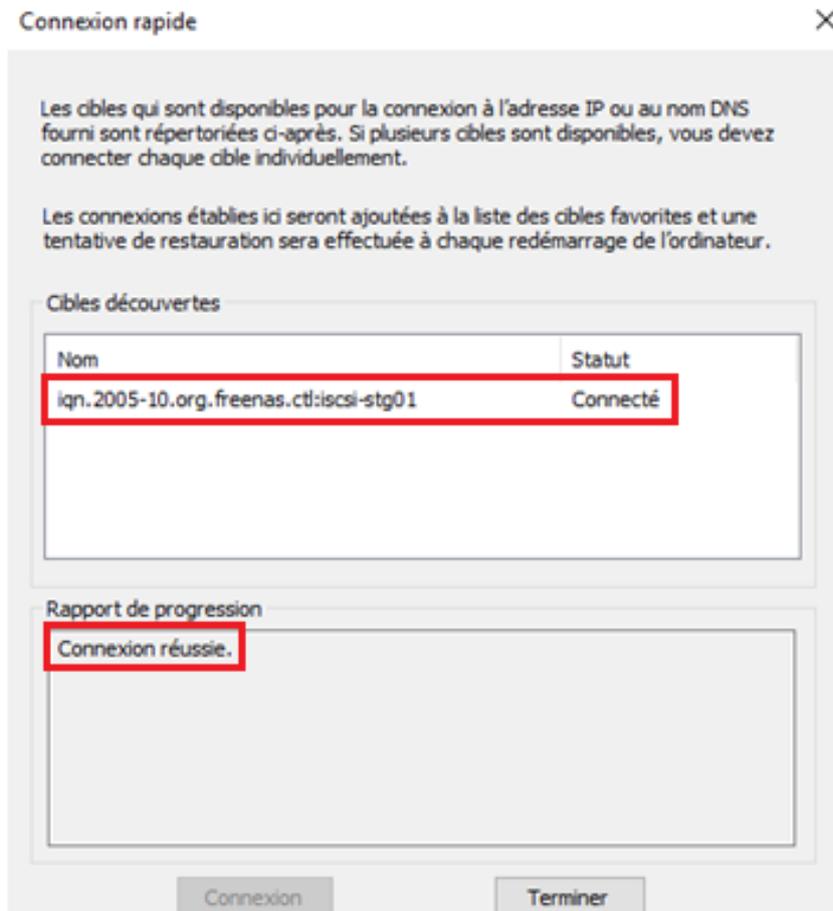
Une fenêtre vous avertira que le service Initiateur iSCSI n'est pas démarré, alors qu'il est nécessaire pour cette opération. Cliquez sur **Oui** pour l'activer.



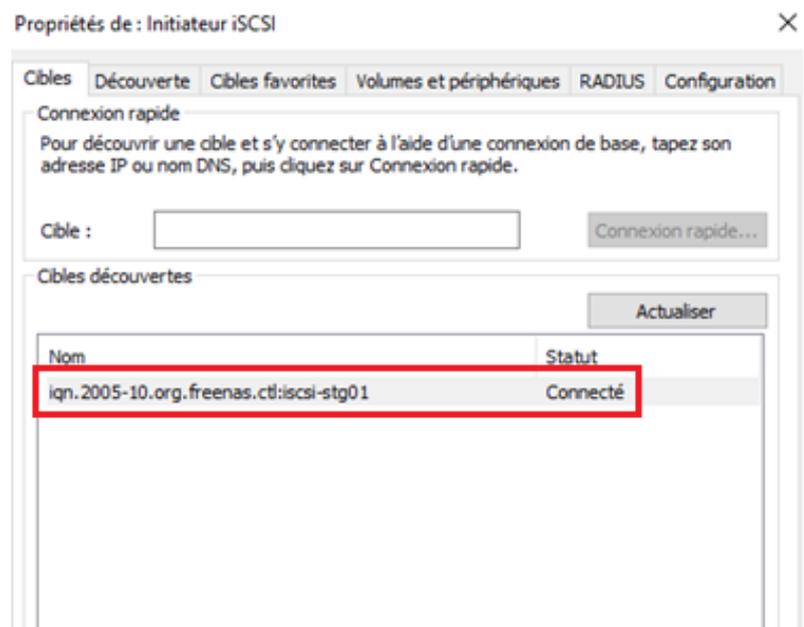
Ensuite, sur la fenêtre d'initiateur iSCSI, sous l'onglet Cibles, renseignez l'adresse IP du serveur TrueNAS et cliquez sur **connexion rapide**.



Puis, une fenêtre vous **confirmera** que la connexion est réussie et que la cible iSCSI a été ajoutée.



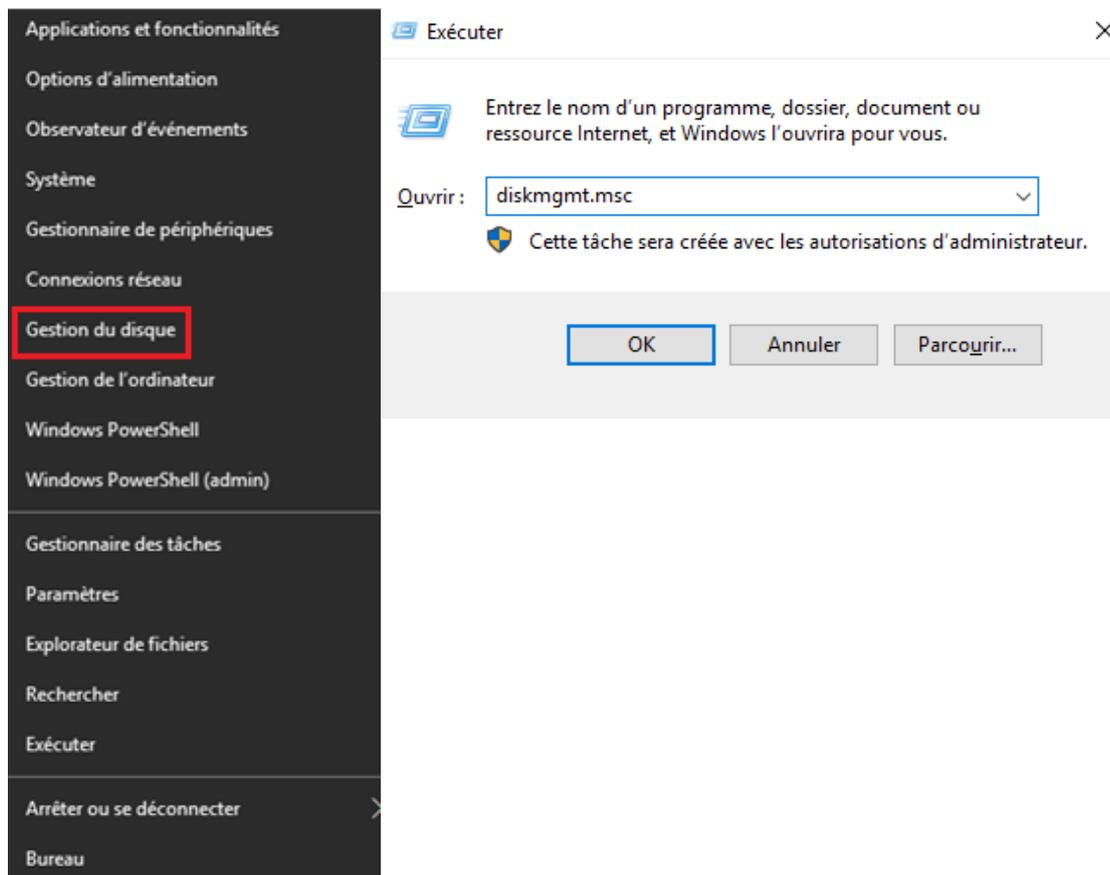
À présent, le disque iSCSI est détecté par Windows et vous pouvez le **rendre utilisable** (l'initialiser, le partitionner et le formater) pour qu'il apparaisse comme un nouveau volume.



Montage du disque iSCSI

Sur le **Gestionnaire de serveurs**, nous pouvons remarquer qu'un nouveau disque est disponible, le disque iSCSI de TrueNAS. Pour le monter, vous pouvez répéter la procédure effectuée auparavant, ou utiliser la gestion du disque de l'ordinateur.

Pour ouvrir la gestion des disques, vous pouvez soit faire un clic-droit sur le menu **Démarrer** et cliquer sur **Gestion des disques**, ou bien taper **diskmgmt.msc** sur le menu Exécuter.



Gestion des disques

Fichier Action Affichage ?

Volume	Disposition	Type	Système de ...	Statut	Capacité	Espace li...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	59,40 Go	47,94 Go	81 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	499 Mo	499 Mo	100 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	99 Mo	99 Mo	100 %
DATAS01 (D:)	Simple	De base	NTFS	Sain (Parti...	59,98 Go	59,35 Go	99 %

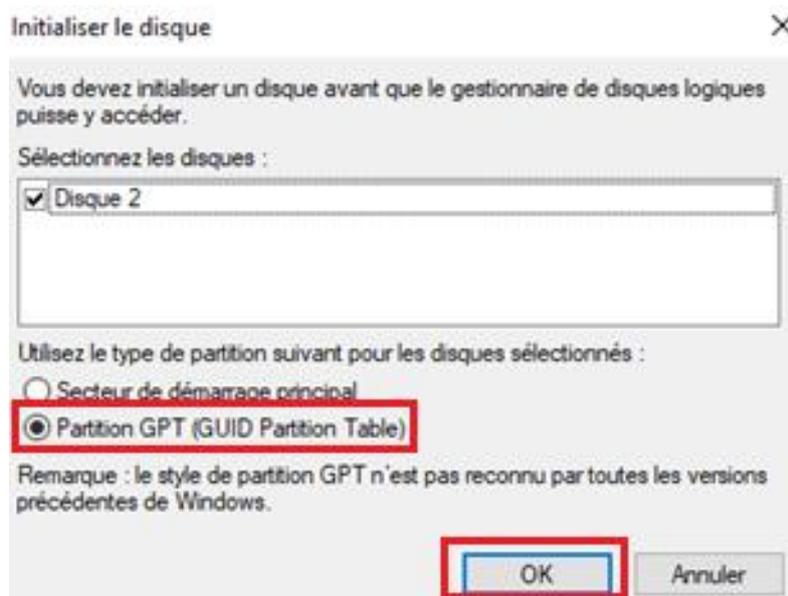
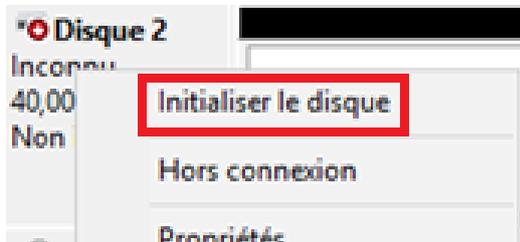
Disque 0 De base 59,98 Go En ligne	499 Mo Sain (Partition de récupération)	99 Mo Sain (Partition du système EFI)	(C:) 59,40 Go NTFS Sain (Démarrer, Fichier d'échange, Vidage sur incident, Partition principale)
Disque 1 De base 59,98 Go En ligne	DATAS01 (D:) 59,98 Go NTFS Sain (Partition principale)		
*Disque 2 Inconnu 40,00 Go Hors conn...	40,00 Go Non alloué		
CD-ROM 0 DVD (E:)			

■ Non alloué ■ Partition principale

Ensuite, faites un clic-droit sur le disque hors ligne (le disque iSCSI) puis cliquez sur **En ligne** pour l'activer.



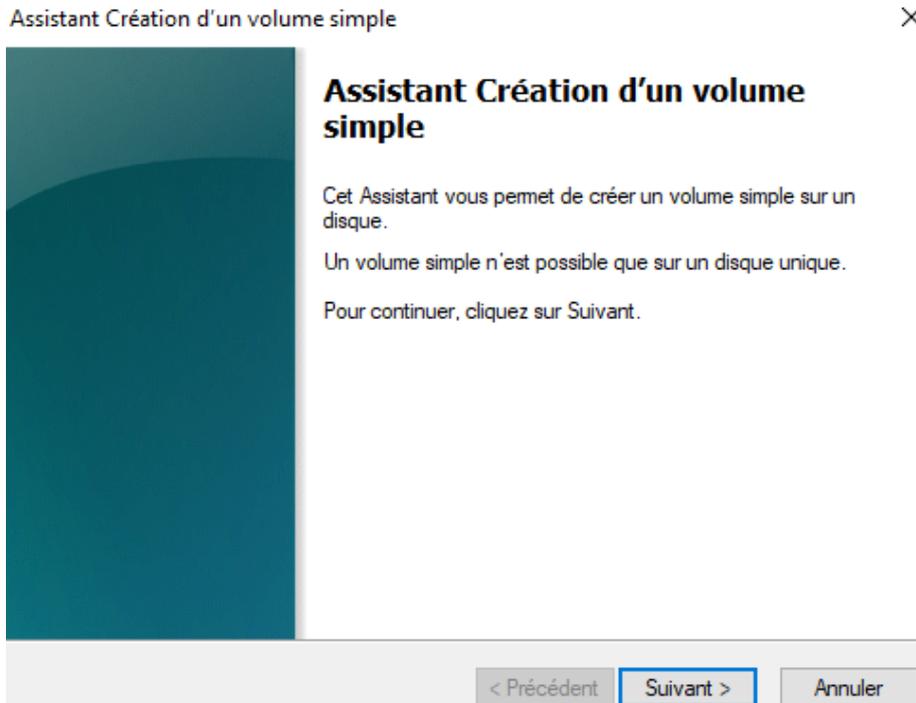
Puis, faites à nouveau un clic droit sur le disque. Dans le menu qui apparaît, sélectionnez **Initialiser le disque** et choisissez le format **GPT**.



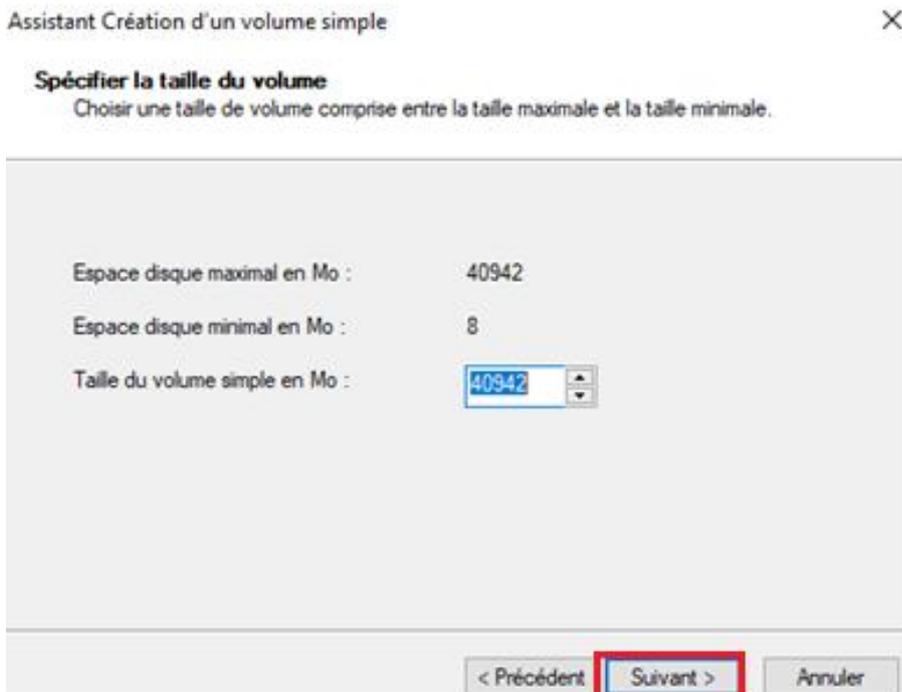
Maintenant que le disque est initialisé, il faut créer un volume sur le disque iSCSI pour qu'on puisse l'utiliser pour la sauvegarde Windows Backup. Pour ce faire, faites un clic droit sur le disque marqué Non alloué, et cliquez sur **Nouveau volume simple**.



L'Assistant Création d'un volume simple **apparaîtra**. Cliquez sur **Suivant** pour continuer.



Laissez la taille maximale du disque, et cliquez sur **Suivant**.



Attribuez la lettre I au lecteur, et cliquez sur **Suivant**.

Assistant Création d'un volume simple ×

Attribuer une lettre de lecteur ou de chemin d'accès
Pour un accès plus facile, vous pouvez assigner une lettre de lecteur ou un chemin d'accès au lecteur sur votre partition.

Attribuer la lettre de lecteur suivante : I ▼

Monter dans le dossier NTFS vide suivant :

Ne pas attribuer de lettre de lecteur ni de chemin d'accès de lecteur

Suivant >

Nommez le volume, **BACKUP01** pour celui de Strasbourg et **BACKUP02** pour Mulhouse, puis cliquez sur **Suivant**.

Assistant Création d'un volume simple ×

Formater une partition
Pour stocker des données sur cette partition, vous devez d'abord la formater.

Indiquez si vous voulez formater cette partition, et le cas échéant, les paramètres que vous voulez utiliser.

Ne pas formater ce volume

Formater ce volume avec les paramètres suivants :

Système de fichiers :

Taille d'unité d'allocation :

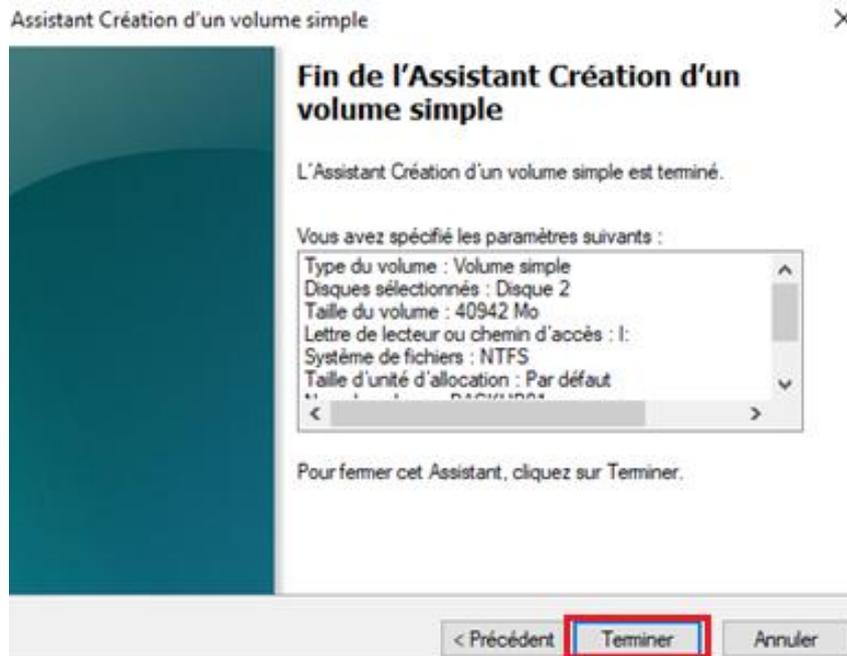
Nom de volume :

Effectuer un formatage rapide

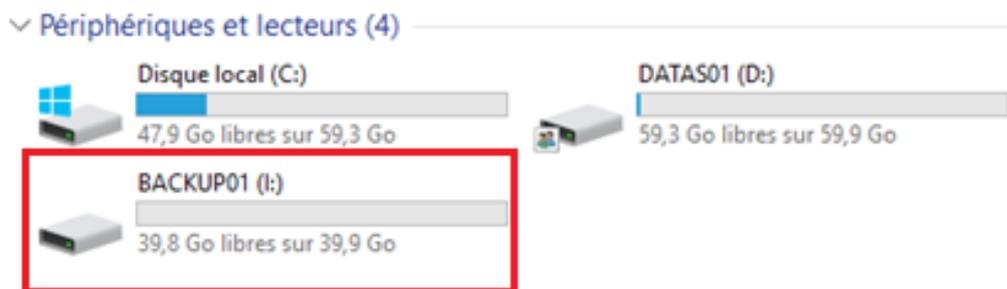
Activer la compression des fichiers et dossiers

Suivant >

Le volume a été créé. Cliquez sur **Terminer** pour fermer l'assistant de création de volume.



À présent, en vous rendant dans l'Explorateur de fichiers, vous remarquerez que le disque iSCSI est bien **monté** sur le serveur.

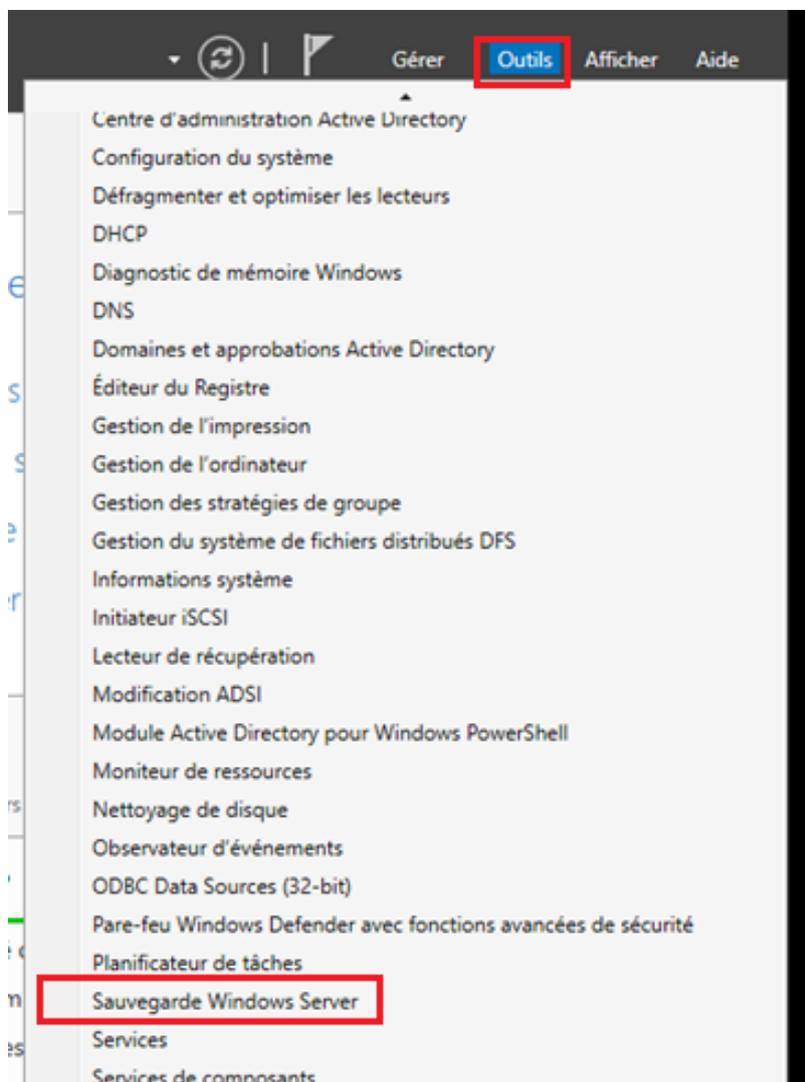


Disque iSCSI monté correctement sur Windows Server

Enfin, il nous reste à configurer la planification de la sauvegarde vers ce disque iSCSI (situé sur TrueNAS) en utilisant la fonctionnalité Sauvegarde Windows Server.

Configuration de Windows Backup Server

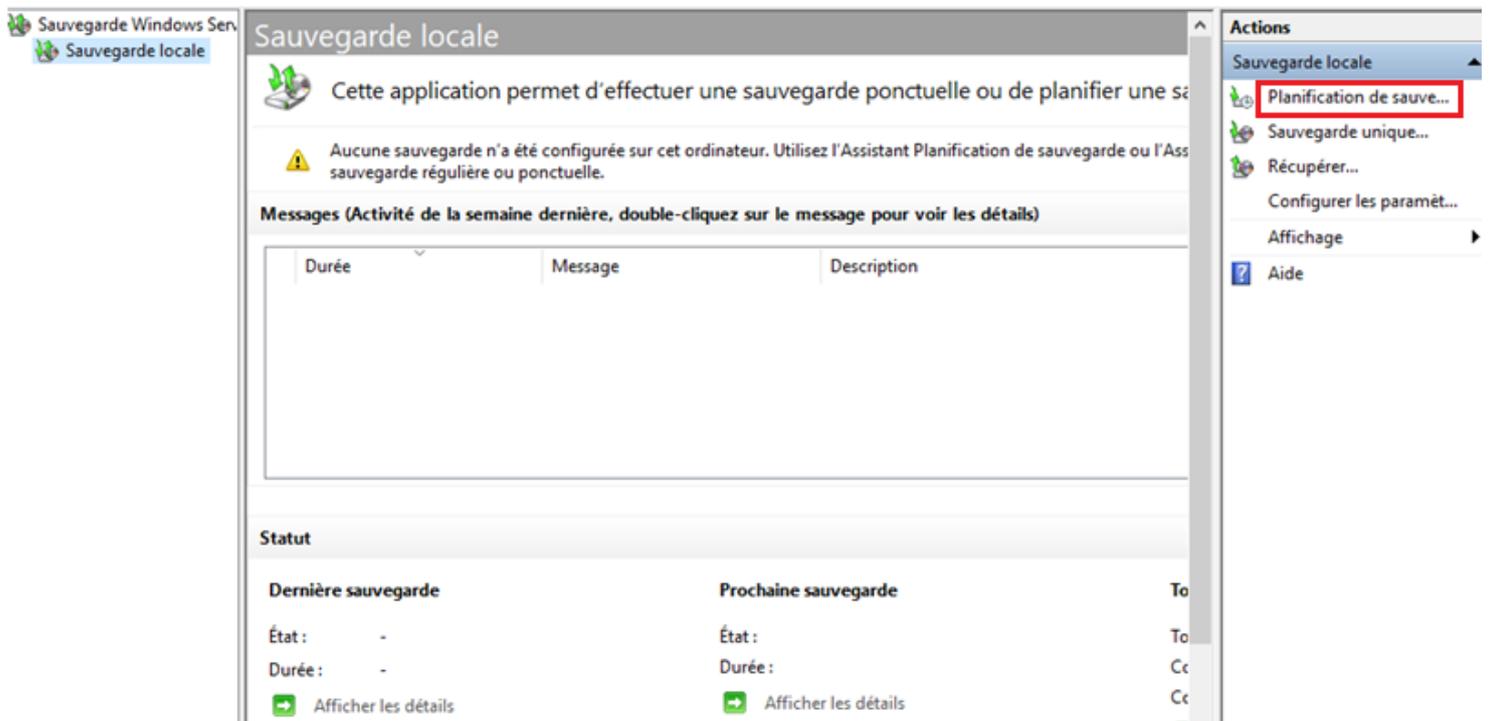
Pour planifier une sauvegarde du serveur en utilisant Windows Backup Server, allez sur le **Gestionnaire de serveur**, cliquez sur **Outils** → **Sauvegarde Windows Server**.



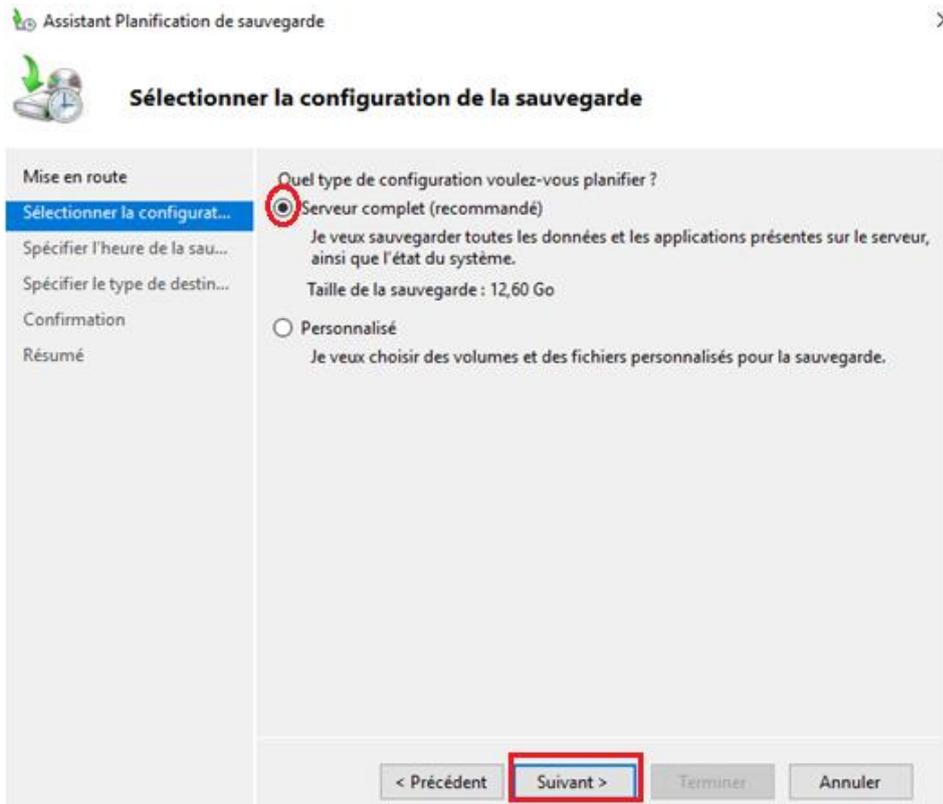
Une console de **Sauvegarde Windows Server** s'ouvrira. Voici une explication des principales options disponibles :

- **Planification de sauvegarde** : C'est l'option principale qui nous intéresse. Elle permet de configurer des sauvegardes automatiques et régulières.
- **Sauvegarde unique** : Permet de lancer une sauvegarde immédiatement, sans planification. Utile pour des tests ou des besoins ponctuels.
- **Récupérer** : Permet de lancer le processus de restauration de données à partir de sauvegardes existantes.
- **Configurer les paramètres de performances** : Permet d'ajuster la manière dont la sauvegarde utilise les ressources du serveur (CPU, bande passante) ou de définir le type de sauvegarde (complète, incrémentielle).

Dans le cadre de cette documentation technique, cliquez sur **Planification de sauvegarde** pour configurer votre première sauvegarde planifiée.



Ensuite, sur la **première étape** (ou "l'écran d'accueil") de l'assistant, cliquez sur **Suivant**, et laissez cocher **Serveur complet**, et appuyez sur **Suivant**.



Paramétrez ensuite l'heure de lancement de la sauvegarde. Notre choix se porte sur **tous les jours à 20h** afin de minimiser l'impact sur la bande passante du serveur pendant les heures d'activité. Nous partons du principe qu'à cette heure, le corps éducatif de l'IFIDE a cessé ses activités.

Assistant Planification de sauvegarde



Spécifier l'heure de la sauvegarde

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

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

Tous les jours
Sélectionnez une heure : 20:00

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

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

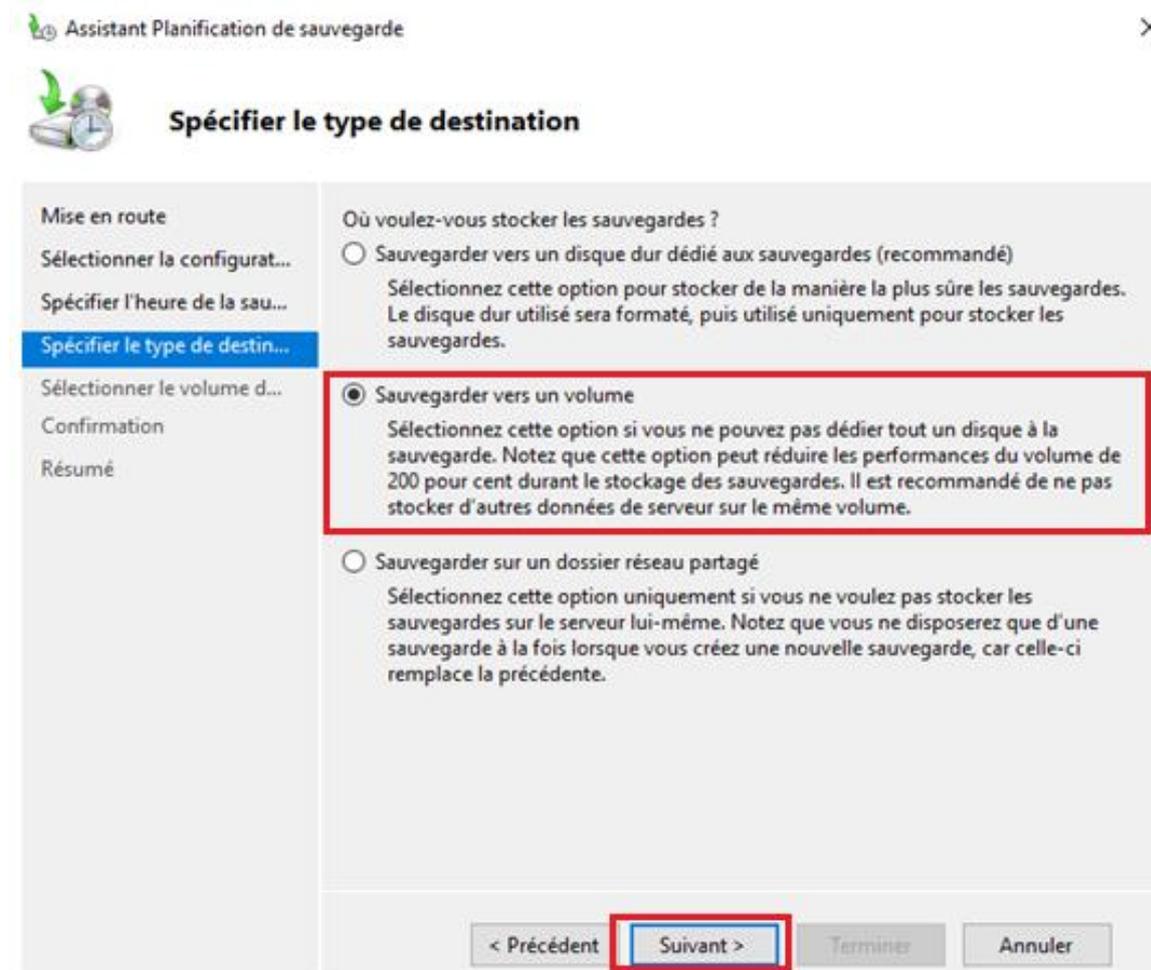
Ajouter >

< Supprimer

Heure planifiée :
21:00

< Précédent **Suivant >** Terminer Annuler

Puis, **sélectionnez** l'option **Sauvegarde vers un volume** pour stocker les sauvegardes sur le volume iSCSI que nous avons créé. Ce choix est fait car nous utiliserons également ce volume pour stocker les clichés instantanés des disques. Contrairement à l'option "Sauvegarde vers un disque dur dédié", qui formate le disque et le réserve exclusivement à la sauvegarde, l'option "Sauvegarde vers un volume" nous permet de partager l'espace de ce volume iSCSI pour d'autres usages comme les instantanés.



Assistant Planification de sauvegarde

Spécifier le type de destination

Mise en route
Sélectionner la configurat...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Sélectionner le volume d...
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

Ensuite, sur l'écran de **sélection du volume**, cliquez sur **Ajouter**.

Assistant Planification de sauvegarde

Sélectionner le volume de destination

Sélectionnez un ou plusieurs volumes pour stocker vos sauvegardes. Utilisez plusieurs volumes sur plusieurs disques pour stocker les sauvegardes hors site.

Volume	Disque	Capacité	Espace libre

Ajouter Supprimer

< Précédent Suivant > Terminer Annuler

Sélectionnez le disque iSCSI monté **BACKUP01**.

Ajouter des volumes

Volume	Disque	Capacité	Espace libre
DATAS01 (D:)	VMware Virtual NVMe Disk	59,98 Go	59,35 Go
BACKUP01 (I:)	TrueNAS iSCSI Disk SCSI...	39,98 Go	39,90 Go

OK Annuler

Un message d'avertissement **apparaîtra**. Cliquez sur **OK** pour confirmer l'exclusion du volume BACKUP01 de la liste des éléments à sauvegarder (puisque'il s'agit de la destination).

Sauvegarde de Windows Server ×



Le volume sélectionné est inclus dans la liste des éléments à sauvegarder. L'ajout de ce volume en tant que destination de stockage de sauvegarde va le supprimer de la liste des éléments à sauvegarder. Voulez-vous exclure ce volume de la sauvegarde ?

OK

Annuler

Enfin, cliquez sur **Terminer** pour finaliser la planification de la sauvegarde.

Assistant Planification de sauvegarde ×



Confirmation

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Sélectionner le volume d...

Confirmation

Résumé

Vous allez créer la planification de sauvegarde suivante.

Heures de la sauvegarde : 20:00

Fichiers exclus : Aucun

Option avancée : Sauvegarde complète VSS

Destinations de sauvegarde

Nom	Taille	Espace utilisé
BACKUP01 (I:)	39,98 Go	87,73 Mo

Éléments de sauvegarde

Nom
DATAS01 (D:)
Disque local (C:)
État du système
Partition du système EFI
Récupération
Récupération complète

< Précédent

Suivant >

Terminer

Annuler

Statut : La planification de sauvegarde a bien été créée.

Votre première sauvegarde planifiée aura lieu à 29/04/2025 20:00.

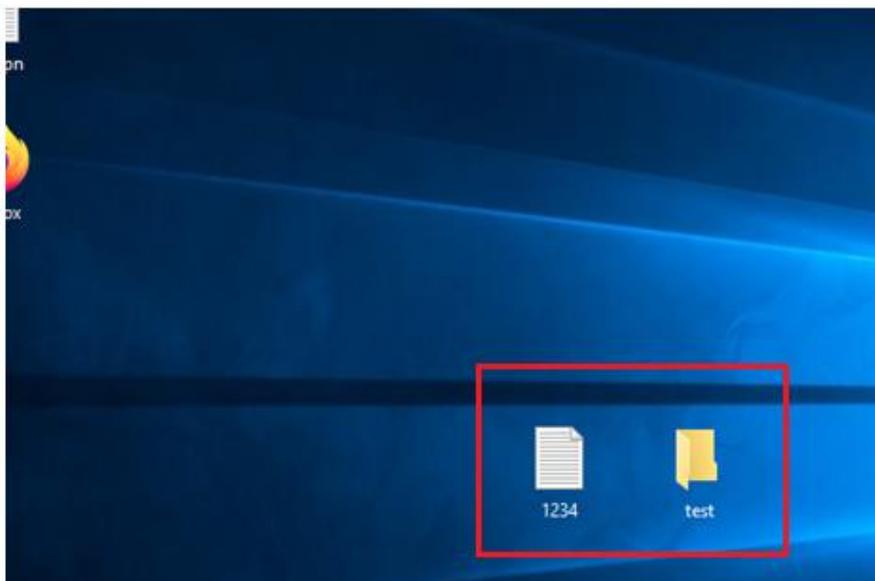
Test de sauvegarde et récupération

Afin de tester la solution de sauvegarde, nous allons effectuer une sauvegarde unique, puis procéder à une récupération des données.

Le scénario de test sera le suivant :

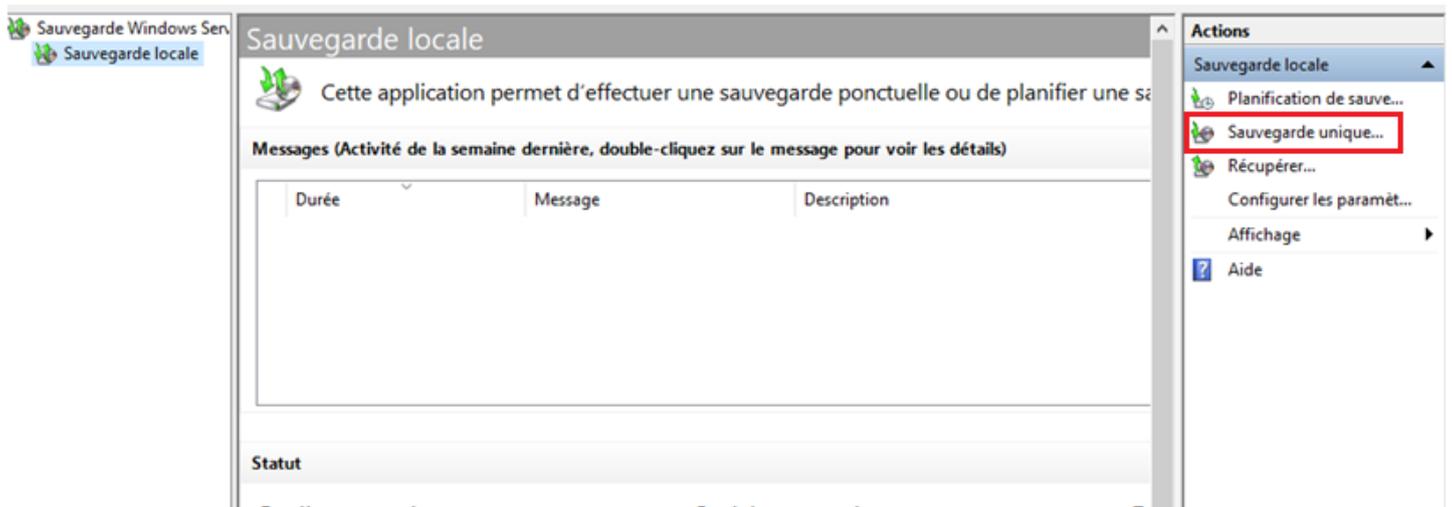
1. Créer un fichier "1234" et un dossier "test" sur le Bureau du serveur.
2. Lancer la sauvegarde unique.
3. Supprimer le fichier et le dossier créés, puis vider la Corbeille.
4. Restaurer la sauvegarde et interpréter les résultats obtenus.

Pour commencer, créez le fichier et le dossier nécessaires au test.

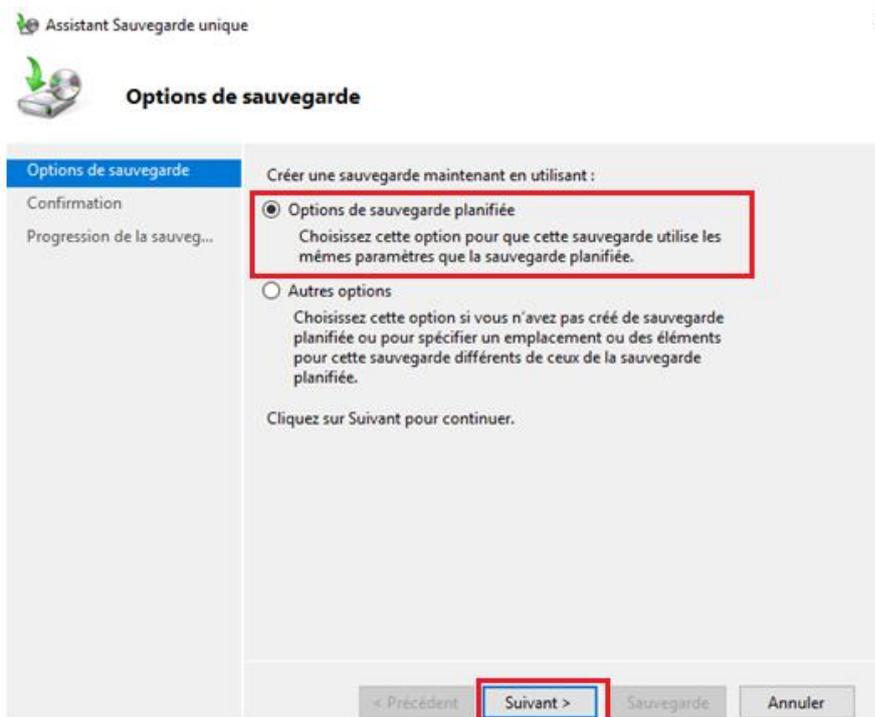


Sauvegarde unique

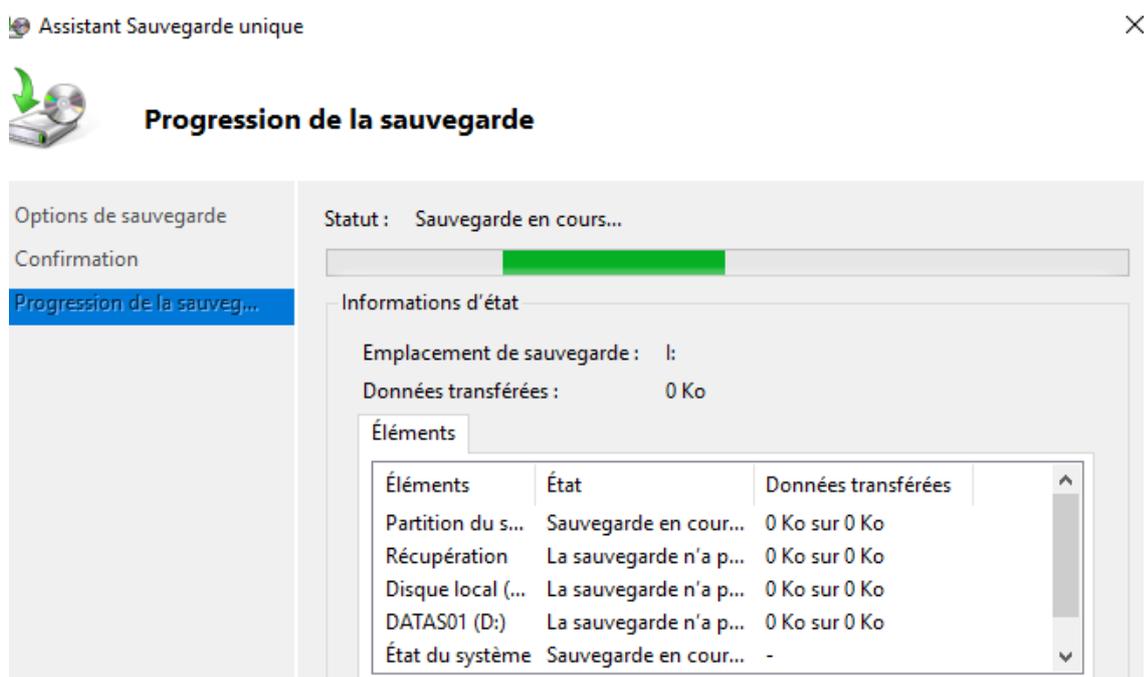
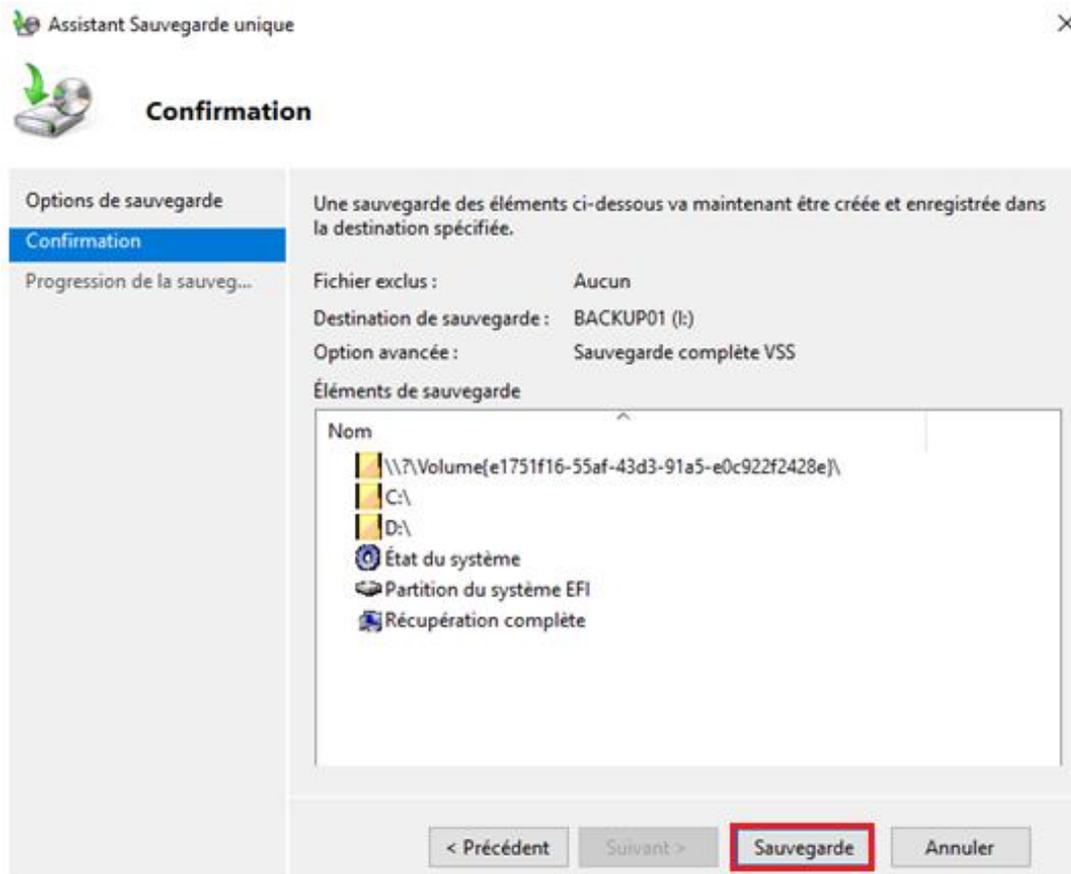
Lancez une sauvegarde en cliquant sur **Sauvegarde unique**.



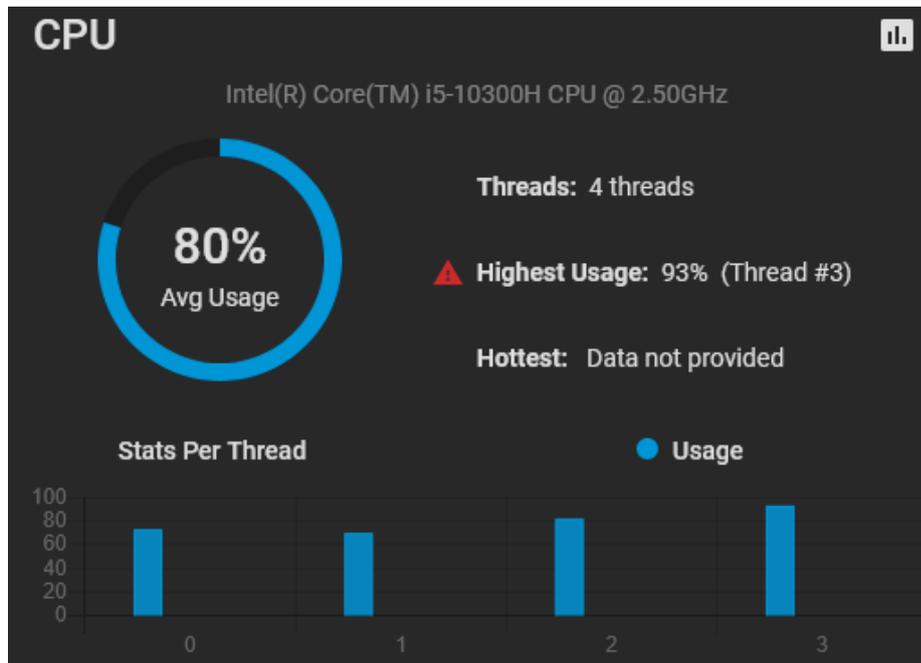
Laissez cocher l'option **Options de sauvegarde planifiée** pour que la sauvegarde unique utilise les mêmes options que la sauvegarde planifiée **configurée** précédemment.



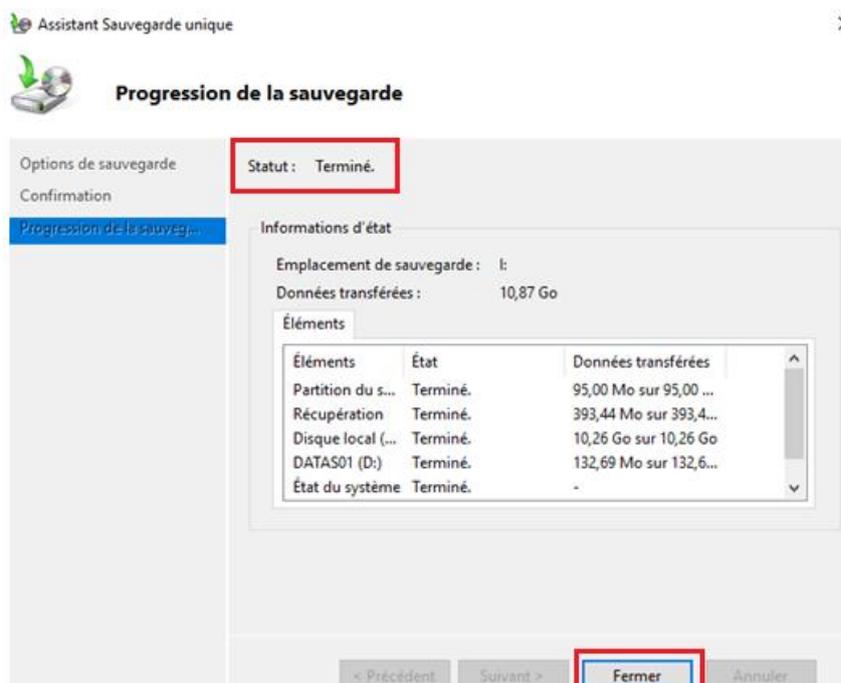
Puis, cliquez sur **Sauvegarde** et patientez pendant la sauvegarde.



Parallèlement, si vous surveillez l'activité sur l'interface de TrueNAS, vous pourrez remarquer que le serveur utilise des ressources **pendant la sauvegarde** (CPU, RAM, activité disque). Cela **confirme** que la sauvegarde est bien en cours d'écriture sur le stockage hébergé par TrueNAS.



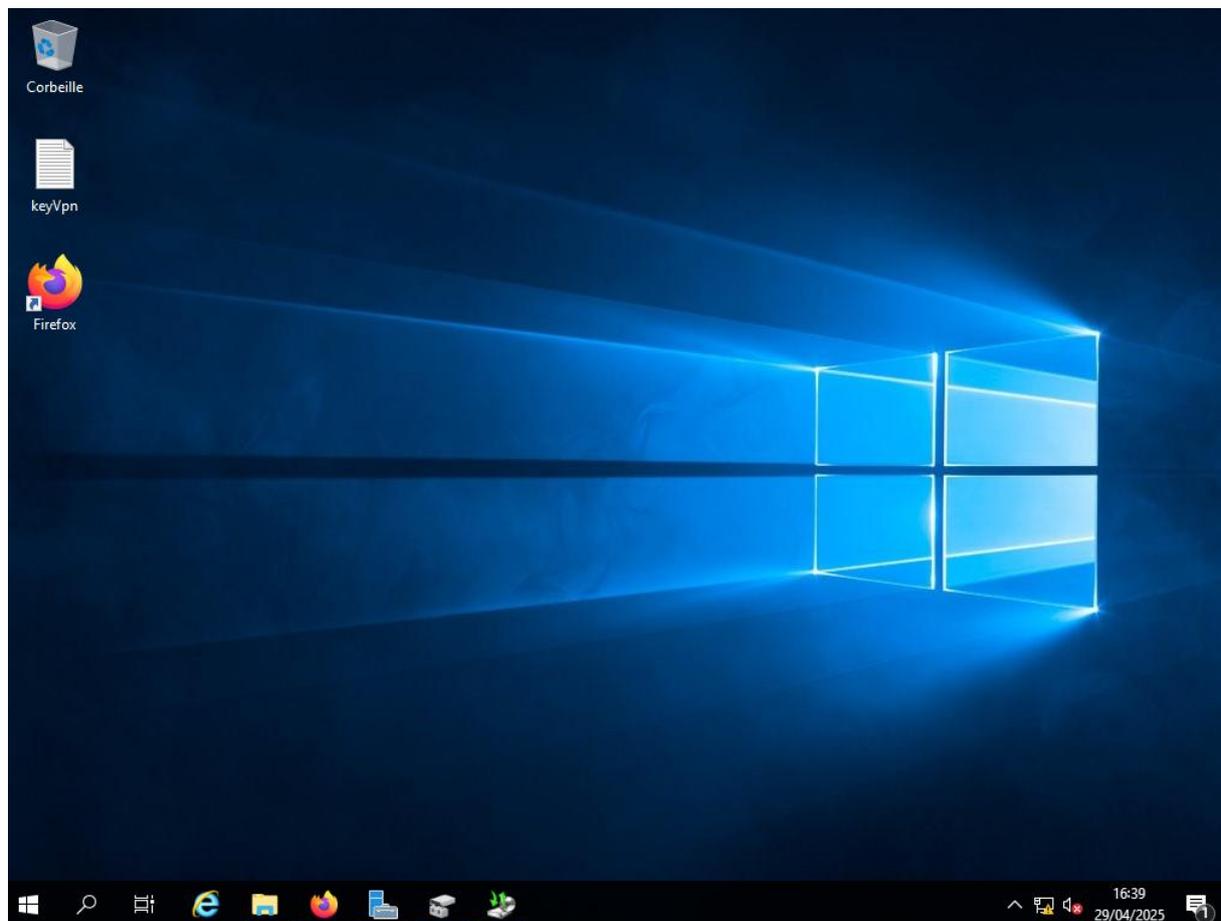
La sauvegarde terminée, passez à présent au test de restauration des données.



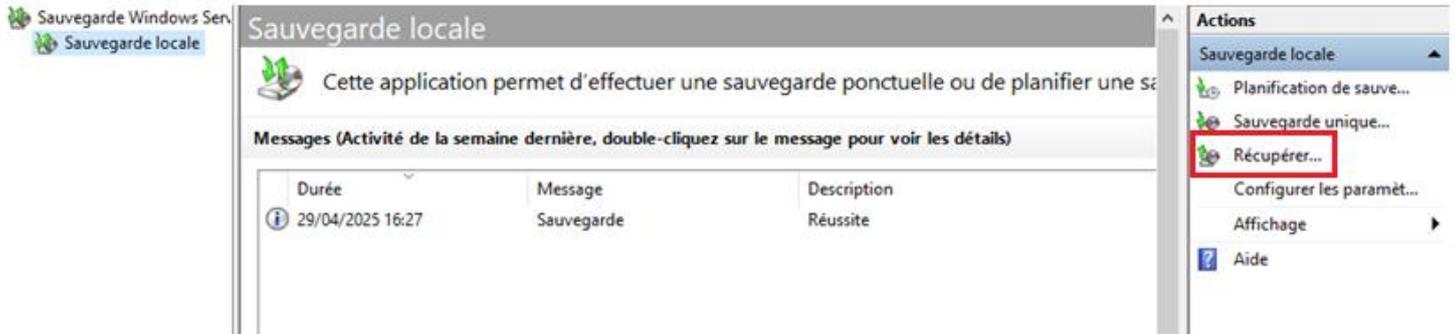
Test de restauration

Afin de tester la restauration, nous allons supprimer le dossier "test" et le fichier "1234" que nous avons créés sur le Bureau (ou même supprimer tous les éléments non nécessaires du Bureau).

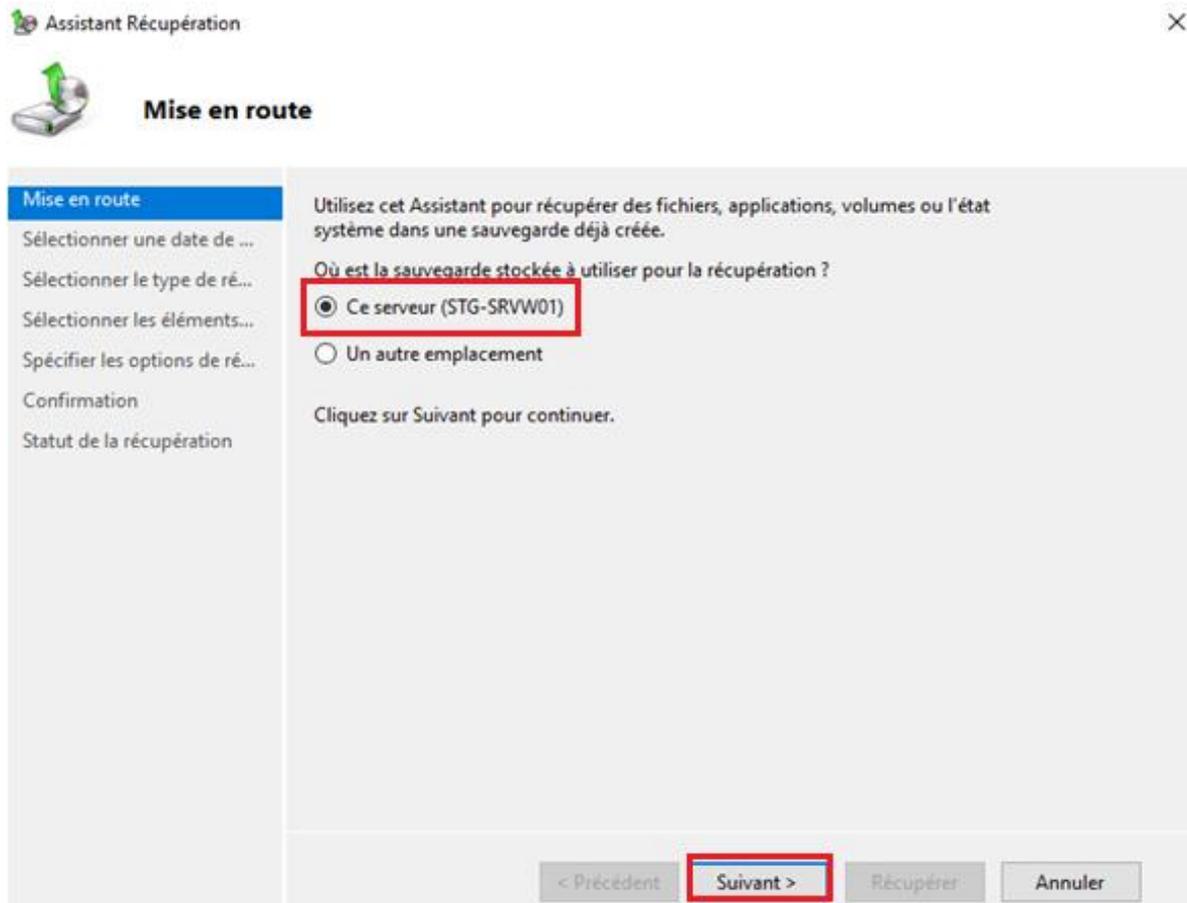
Assurez-vous que le Bureau et la Corbeille sont vides pour simuler une perte de données.



Ensuite, ouvrez la console de Windows Backup, cliquez sur **Récupérer**.



Sélectionnez ensuite **Ce serveur** comme source pour la récupération.



Puis, sélectionnez la sauvegarde à utiliser pour la récupération. Étant donné que nous n'avons effectué qu'une seule sauvegarde, **conservez la sélection par défaut**, puis cliquez sur **Suivant**.

Assistant Récupération ×

 **Sélectionner une date de sauvegarde**

Mise en route

Sélectionner une date de ...

Sélectionner le type de ré...

Sélectionner les éléments...

Spécifier les options de ré...

Confirmation

Statut de la récupération

Sauvegarde la plus ancienne : 29/04/2025 16:27

Sauvegarde la plus récente : 29/04/2025 16:27

Sauvegardes disponibles

Sélectionnez la date d'une sauvegarde à utiliser pour la récupération. Des sauvegardes sont disponibles pour les dates affichées en gras.

avril 2025						
lun.	mar.	mer.	jeu.	ven.	sam.	dim.
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Date de sauvegarde : 29/04/2025

Durée : 16:27 v

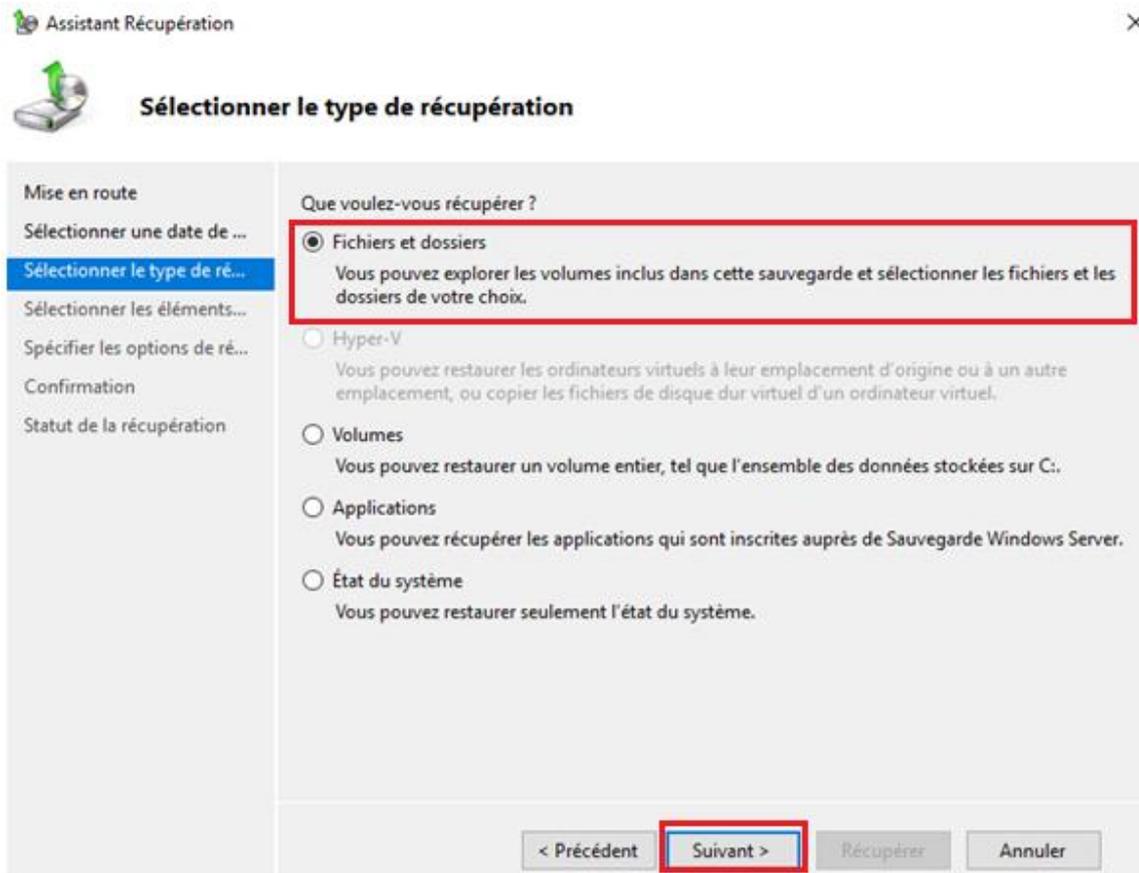
Emplacement : BACKUP01 (I:)

État : Disponible en ligne

Éléments récupérables : [Récupération complète:](#)
[État du système: Partit...](#)

< Précédent
Suivant >
Récupérer
Annuler

À l'étape du type de récupération, conservez la sélection sur **Fichiers et dossiers**, puis cliquez sur **Suivant**.



À l'étape de sélection des éléments à récupérer, choisissez le disque **C:**. Pour notre test, comme les fichiers se trouvaient sur le Bureau, le disque C:\ est le bon emplacement source.

Assistant Récupération



Sélectionner les éléments à récupérer

Mise en route

Sélectionner une date de ...

Sélectionner le type de ré...

Sélectionner les éléments...

Spécifier les options de ré...

Confirmation

Statut de la récupération

Parcourez l'arborescence des éléments disponibles pour trouver les fichiers ou dossiers à récupérer. Cliquez sur un élément dans l'arborescence ou sous Nom pour le sélectionner pour la récupération.

Éléments disponibles :

- STG-SRVW01
 - Il s'agit d'une partition systèm
 - Récupération
 - Disque local (C:)**
 - DATAS01 (D:)

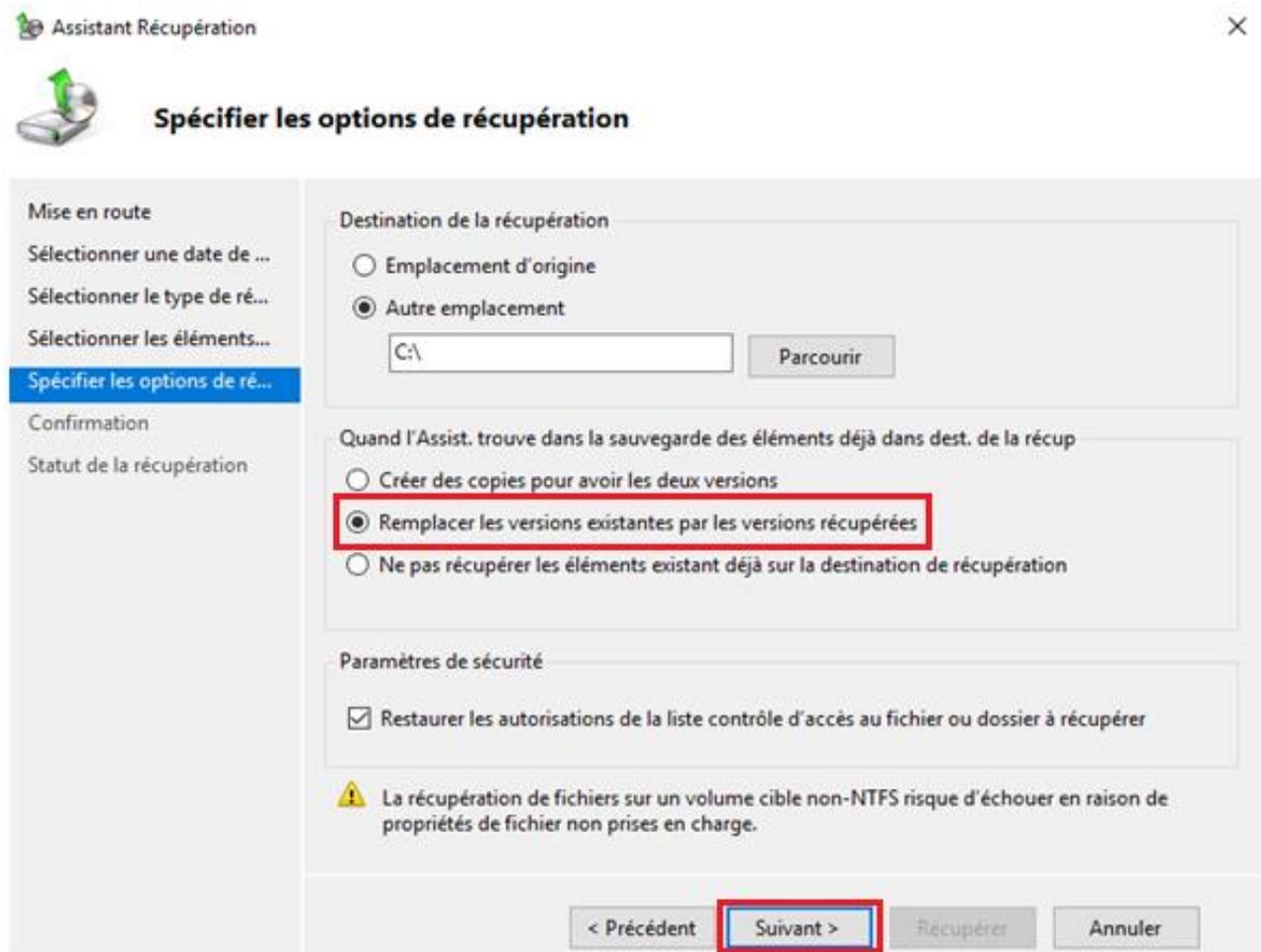
Éléments à récupérer :

Nom	Date de modi...
\$Recycle.Bin	15/09/2018 0...
DFSRoots	24/04/2025 1...
PerfLogs	23/04/2025 1...
Program Files	29/04/2025 1...
Program Files (x86)	29/04/2025 1...
ProgramData	29/04/2025 1...
Recovery	15/04/2025 1...
System Volume Informa...	29/04/2025 1...
Users	15/04/2025 1...
Windows	24/04/2025 1...
Documents and Settings	15/04/2025 1...
pagefile.sys	29/04/2025 1...

< Précédent
Suivant >
Récupérer
Annuler

Ensuite, choisissez la destination de récupération. Étant donné que les données d'origine provenaient du disque C.; écrire C:\ plusieurs options vous sont **proposées**. Vous êtes libre de choisir l'une des trois options de récupération **proposées** selon vos besoins.

Dans le cadre de ce test, nous allons sélectionner l'option qui **remplace les fichiers présents** par ceux de la sauvegarde.



Assistant Récupération

Spécifier les options de récupération

Mise en route

Sélectionner une date de ...

Sélectionner le type de ré...

Sélectionner les éléments...

Spécifier les options de ré...

Confirmation

Statut de la récupération

Destination de la récupération

Emplacement d'origine

Autre emplacement

C:\

Quand l'Assist. trouve dans la sauvegarde des éléments déjà dans dest. de la récup

Créer des copies pour avoir les deux versions

Remplacer les versions existantes par les versions récupérées

Ne pas récupérer les éléments existant déjà sur la destination de récupération

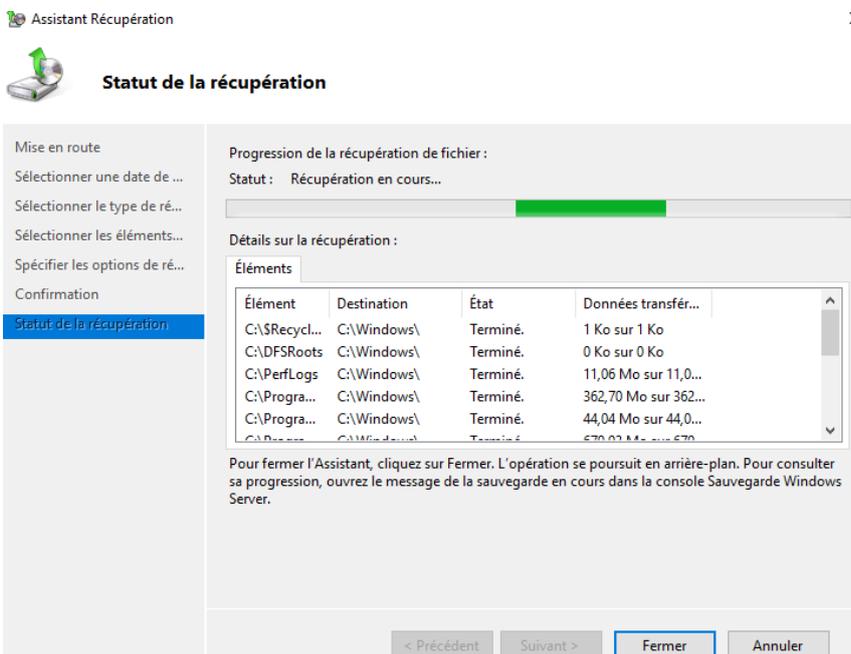
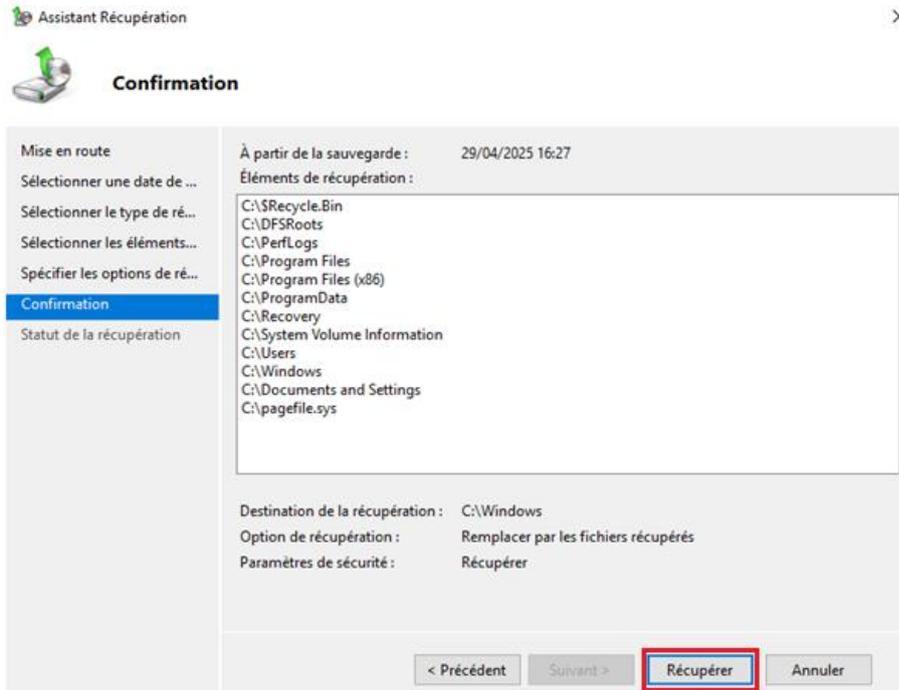
Paramètres de sécurité

Restaurer les autorisations de la liste contrôle d'accès au fichier ou dossier à récupérer

 La récupération de fichiers sur un volume cible non-NTFS risque d'échouer en raison de propriétés de fichier non prises en charge.

< Précédent **Suivant >** Récupérer Annuler

Enfin, pour lancer la récupération, cliquez sur **Récupérer**.



Sauvegarde locale



Cette application permet d'effectuer une sauvegarde ponctuelle ou de planifier une sauvegarde.

Messages (Activité de la semaine dernière, double-cliquez sur le message pour voir les détails)

Durée	Message	Description
29/04/2025 17:12	Récupération de fichiers	Réussite
29/04/2025 16:27	Sauvegarde	Réussite

Récupération de fichiers

Description : Récupération de fichiers

Emplacement de sauvegarde : I:

À partir de la sauvegarde : 29/04/2025 16:27

État : Réussite

Informations d'état

Heure de début : 29/04/2025 16:49

Heure de fin : 29/04/2025 17:12

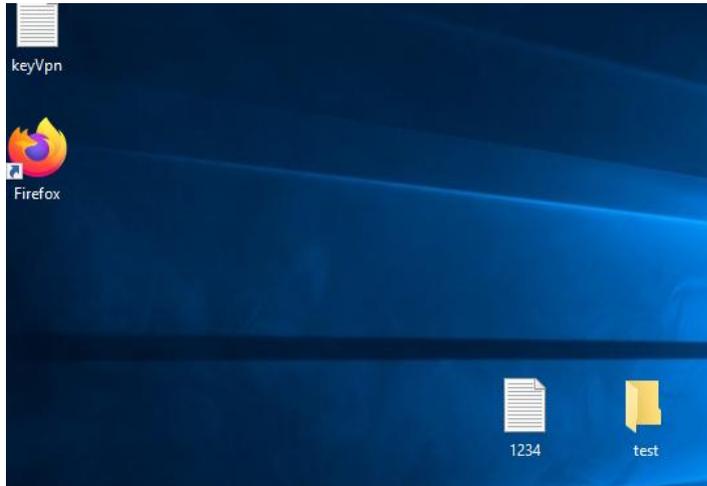
Données transférées : 9,59 Go

Éléments

Nom	Destinat...	État	Données tr...
C:\\$Recycle...	C:\Wind...	Terminé.	1 Ko
C:\DFSRoots	C:\Wind...	Terminé.	0 Ko
C:\PerfLogs	C:\Wind...	Terminé.	11,06 Mo
C:\Program ...	C:\Wind...	Terminé.	362,70 Mo
C:\Program ...	C:\Wind...	Terminé.	44,04 Mo
C:\Program...	C:\Wind...	Terminé.	679,93 Mo
C:\Recovery	C:\Wind...	Terminé.	1 Ko
C:\System V...	C:\Wind...	Terminé.	11,62 Mo
C:\Users	C:\Wind...	Terminé.	168,91 Mo

[Afficher la liste de tous les fichiers récupérés](#)

OK



Restauration OK → Solution de sauvegarde opérationnelle

La procédure de mise en place de la solution de sauvegarde (incluant ZVOL, iSCSI et la configuration Windows Server Backup) a été répliquée pour le site de Mulhouse (MUL), avec les adaptations requises.

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
BACKUPS02	FILESYSTEM	40.64 GiB	15.08 GiB	lz4	15.39	false	OFF	
iSCSI-MUL01	VOLUME	40.63 GiB	55.71 GiB	lz4	1.00	false	ON	

Portal Group ID	Listen	Description	Discovery Auth Method	Discovery Auth Group
1	192.168.200.3:3260	iscsi-mul01	NONE	



Résumé

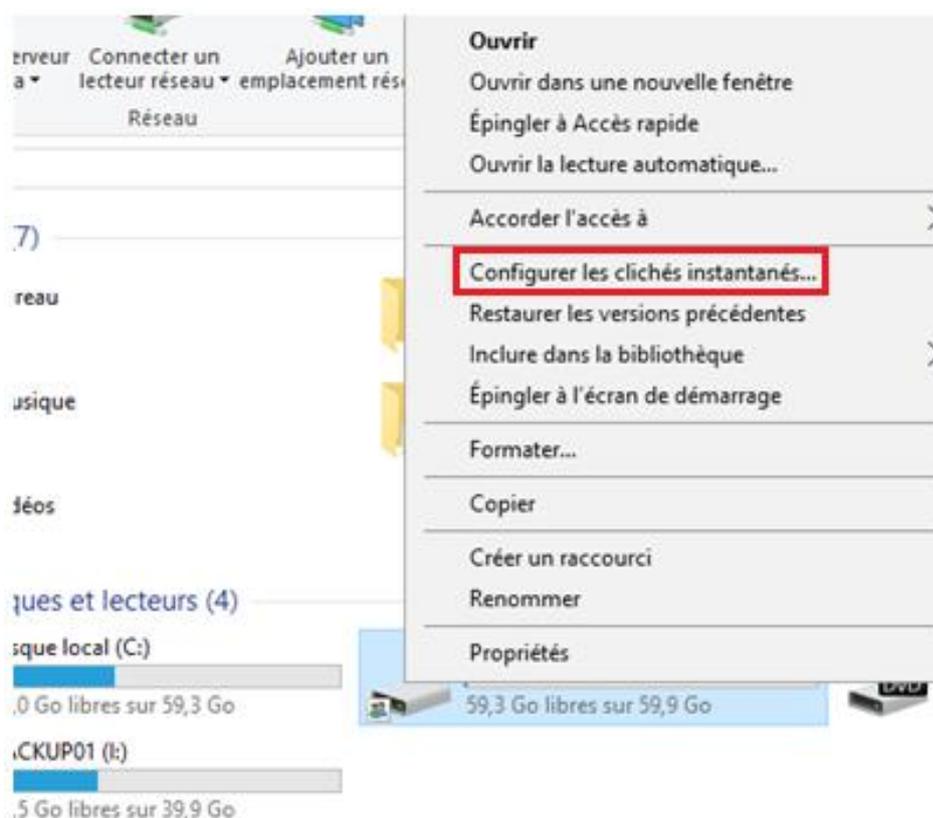
Mise en route	Statut : La planification de sauvegarde a bien été créée.
Sélectionner la configurat...	Votre première sauvegarde planifiée aura lieu à 30/04/2025 20:00.
Spécifier l'heure de la sau...	

3.2.6) Mise en place des clichés instantanés : Shadow Copy

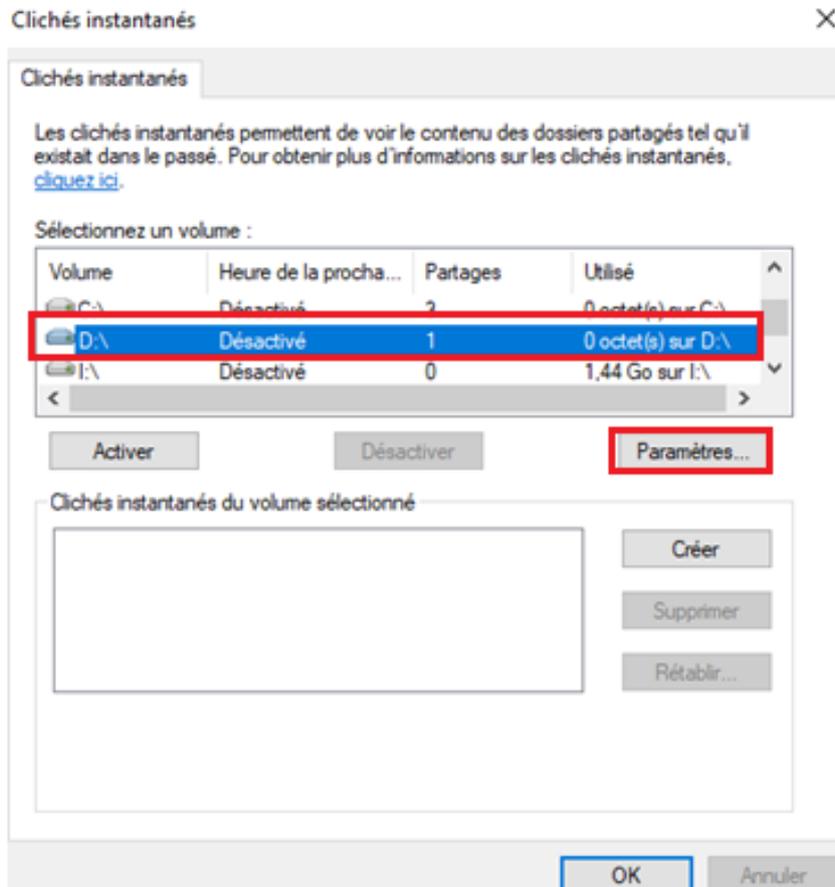
Configuration des clichés instantanés

Vu le temps imparti pour la récupération rapide des données via la sauvegarde, il est pertinent de mettre en place les clichés instantanés (ou Shadow Copy en anglais). Pour répondre à la demande du client spécifiée dans le cahier des charges, ces clichés instantanés seront stockés sur le disque iSCSI dédié afin qu'ils soient centralisés et facilement gérables, ou potentiellement externalisés par la suite.

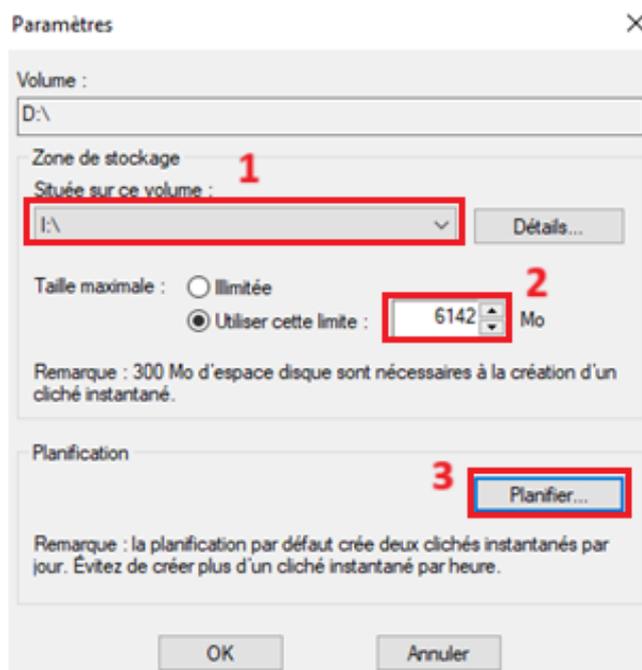
Pour procéder à leur configuration, faites un clic-droit sur le disque sur lequel vous souhaitez activer les clichés instantanés (par exemple, le disque D:), puis cliquez sur "**Configurer les clichés instantanés**".



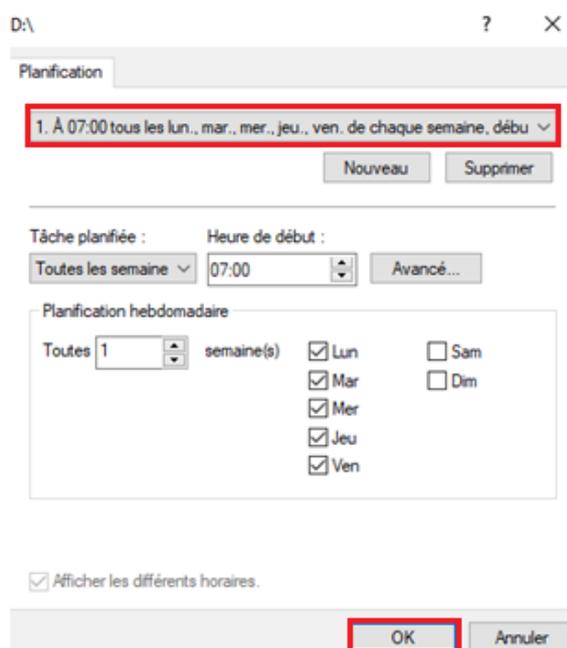
Ensuite, **sélectionnez** le disque, puis cliquez sur **Paramètres** pour **configurer** les clichés instantanés.



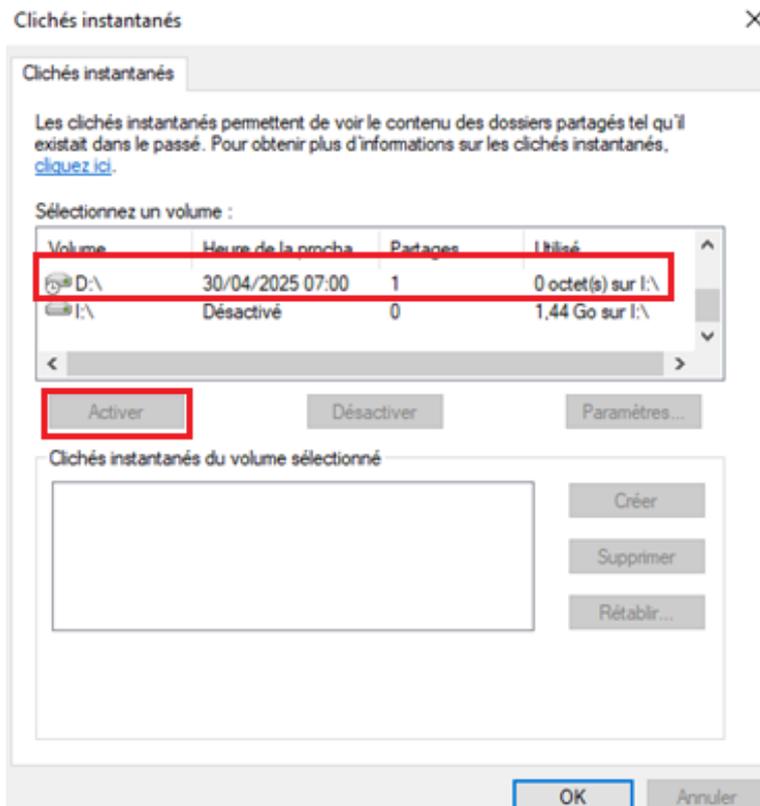
Puis, dans les paramètres, sélectionnez le lecteur *I:* (qui correspond au disque iSCSI) comme emplacement de stockage pour les clichés instantanés. Ensuite, définissez la limite de taille que les clichés instantanés peuvent utiliser sur ce disque distant (par défaut, la limite est fixée à 10 % de la capacité totale du disque).



Cliquez sur **Planifier** si vous souhaitez modifier la **planification** des clichés **instantanés**. Dans notre cas, **nous conserverons** la planification par défaut ; ainsi, les clichés instantanés seront lancés tous les jours à 7h00.



Enfin, cliquez sur **Activer** pour finaliser la configuration des clichés instantanés. Un premier cliché instantané sera alors effectué. Vous pouvez également cliquer sur **Créer** pour prendre un cliché instantané manuellement (ce qui est utile pour les tests ultérieurs).



Test de restauration par les clichés instantanés

Pour effectuer le test de restauration par les clichés instantanés, nous allons suivre les étapes suivantes :

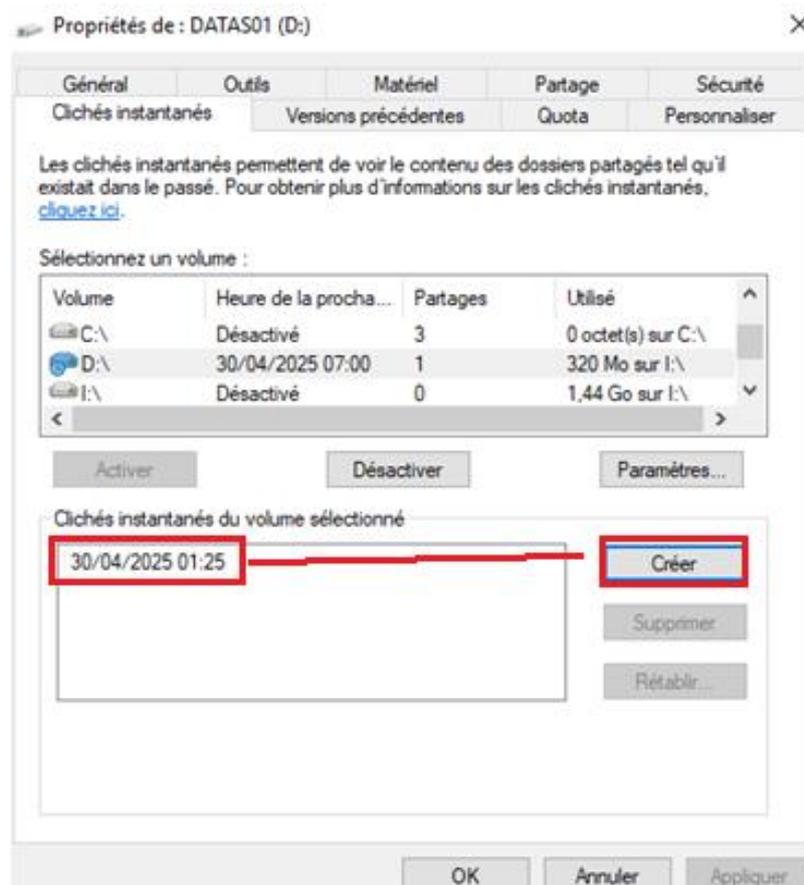
1. Créer des fichiers dans le lecteur D:\
2. Créer un cliché instantané
3. Supprimer les fichiers
4. Restaurer les fichiers à partir des clichés instantanés et interpréter le résultat.

Ainsi, pour commencer, créez les fichiers dans le lecteur D:

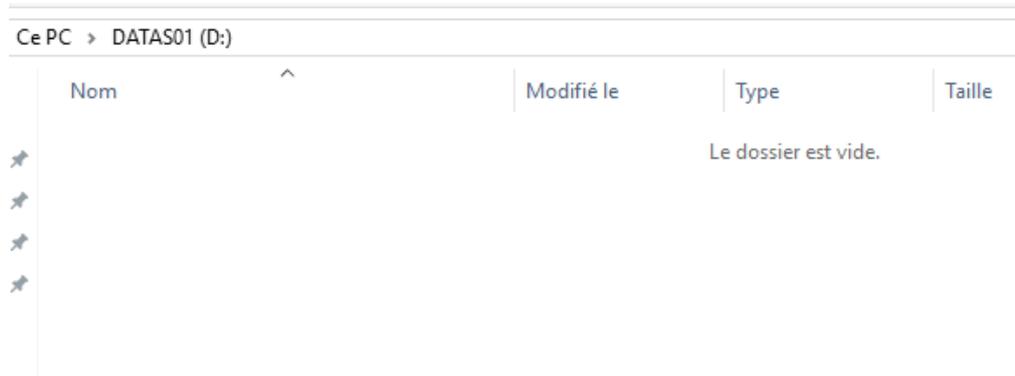
» Ce PC > DATAS01 (D:) >

Nom	Modifié le	Type	Taille
dossier_de_STGSRVW02	24/04/2025 23:07	Dossier de fichiers	
images	25/04/2025 00:32	Dossier de fichiers	
Firefox Installer.exe	29/04/2025 15:17	Application	374 Ko
test.txt	24/04/2025 22:55	Document texte	0 Ko
TESTESTEST	30/04/2025 01:23	Dossier de fichiers	
TESTESTEST.txt	30/04/2025 01:23	Document texte	0 Ko

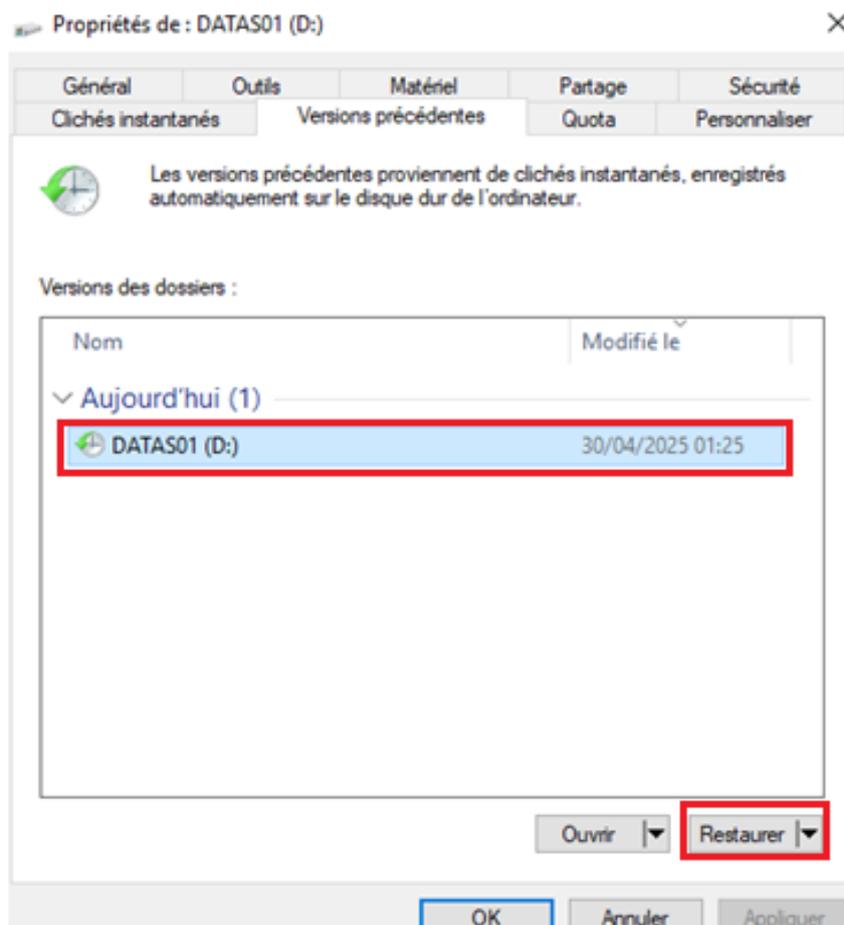
Ensuite, créez le cliché instantané.



Puis, supprimez le contenu du disque D:\.



Enfin, utilisez les clichés instantanés pour **restaurer** les fichiers et **visualisez** les résultats. Pour ce faire, faites un clic-droit sur le lecteur **concerné**, puis sélectionnez **Versions précédentes**.



Versions précédentes



La version précédente du dossier a été correctement restaurée.

OK

Presse-papiers		Organiser	Nouveau	
Ce PC > DATAS01 (D:) >				
	Nom	Modifié le	Type	Taille
je	dossier_de_STGSRVW02	24/04/2025 23:07	Dossier de fichiers	
	images	30/04/2025 01:27	Dossier de fichiers	
ement:	TESTESTEST	30/04/2025 01:23	Dossier de fichiers	
ts	Firefox Installer.exe	29/04/2025 15:17	Application	374 Ko
	test.txt	24/04/2025 22:55	Document texte	0 Ko
	TESTESTEST.txt	30/04/2025 01:23	Document texte	0 Ko

Les fichiers et dossiers ont été restaurés, la solution de clichés instantanés est fonctionnelle.

La configuration des clichés instantanés doit également être réalisée pour le site de Mulhouse (MUL).

3.2.7) Déploiement du portail captif : AD RADIUS et pfSense

Installation du rôle NPS

NPS (Network Policy Server) est le service utilisé pour fournir les services RADIUS nécessaires à la mise en place du portail captif. Il opère notamment sur les ports UDP **1812**, **1813**, **1645** et **1646**. Pour installer ce rôle, ouvrez le **Gestionnaire de serveur**, puis cliquez sur « **Ajouter des rôles et fonctionnalités** ».



Sélectionnez ensuite le serveur sur lequel installer le rôle.

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER LE SERVEUR DE DESTINATION

SERVEUR DE DESTINATION
STG-SRVW01.ifide.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

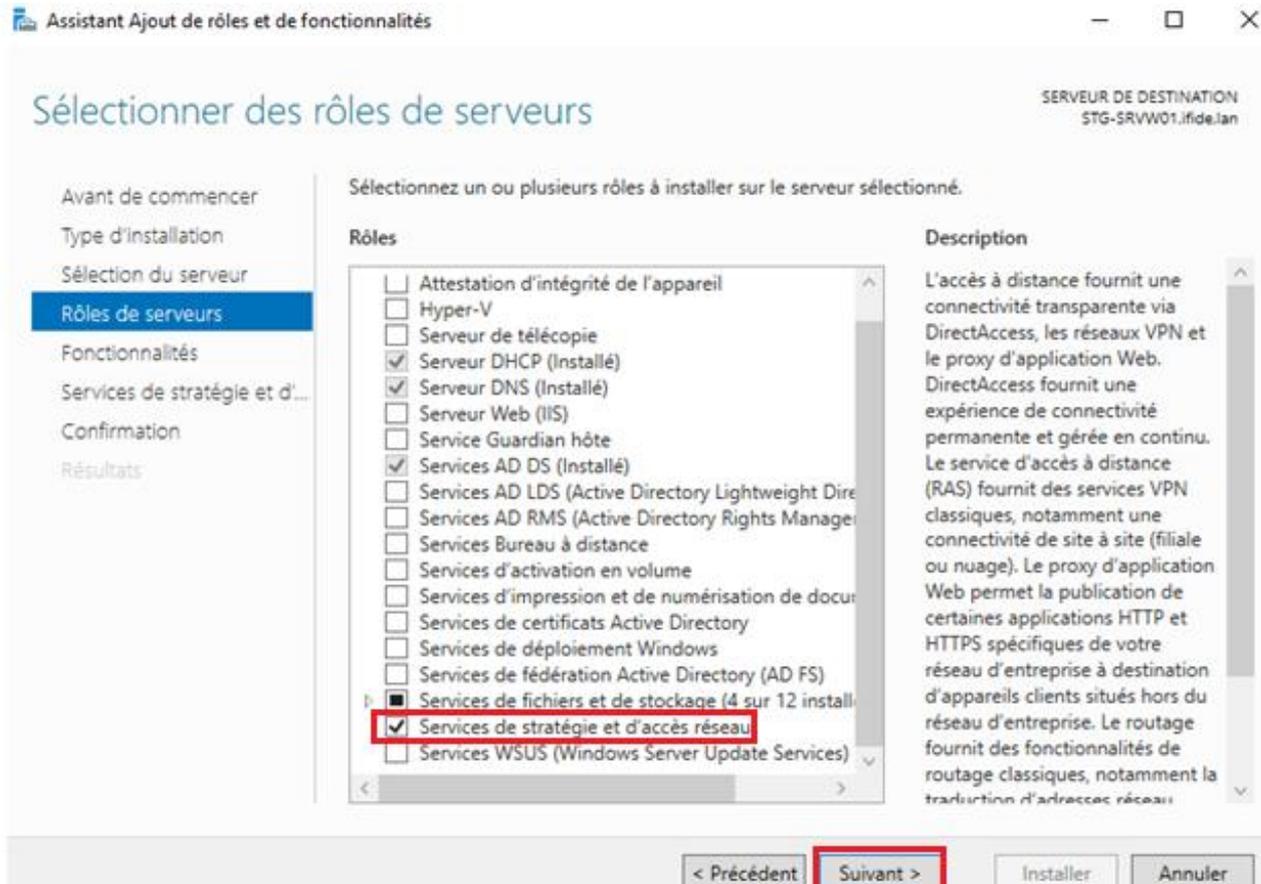
Nom	Adresse IP	Système d'exploitation
MUL-SRVW01.ifide.lan	192.168.200.1	Microsoft Windows Server 2019 Standard
STG-SRVW01.ifide.lan	192.168.100.1	Microsoft Windows Server 2019 Standard

2 ordinateur(s) trouvé(s)

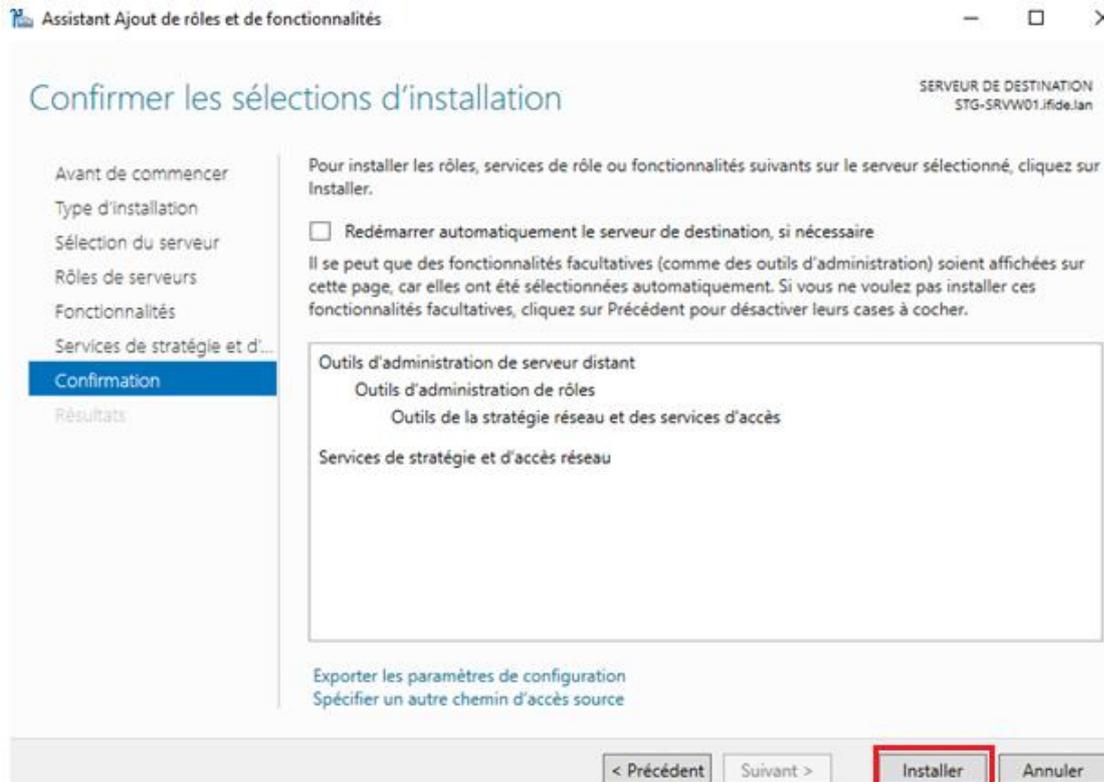
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

Ensuite, cochez les « Services de stratégie et d'accès réseau ». Cliquez sur « Ajouter des fonctionnalités » puis Suivant.

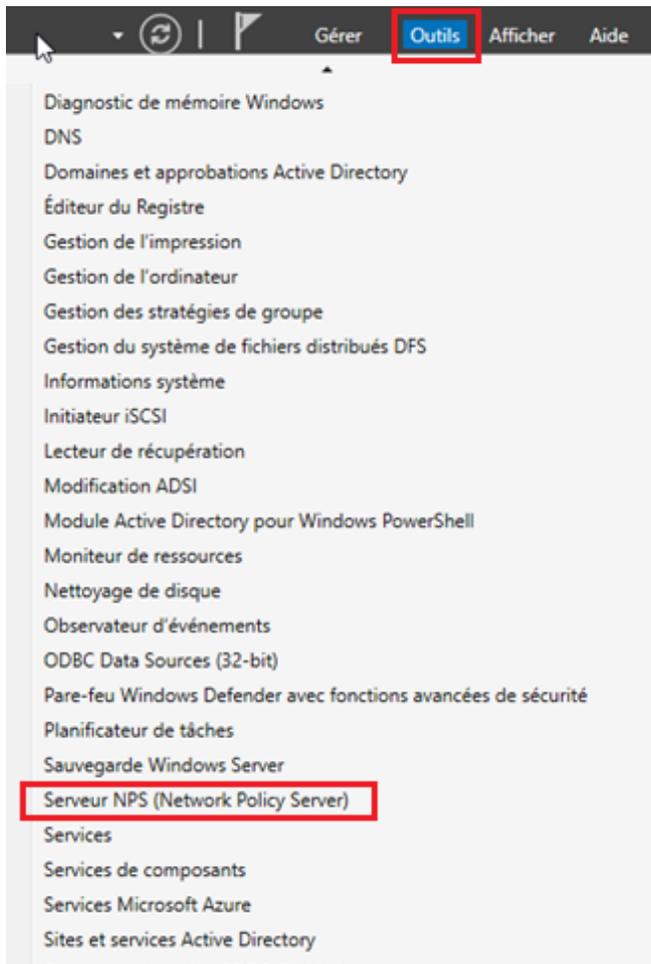


Enfin, procédez jusqu'à l'étape d'installation.



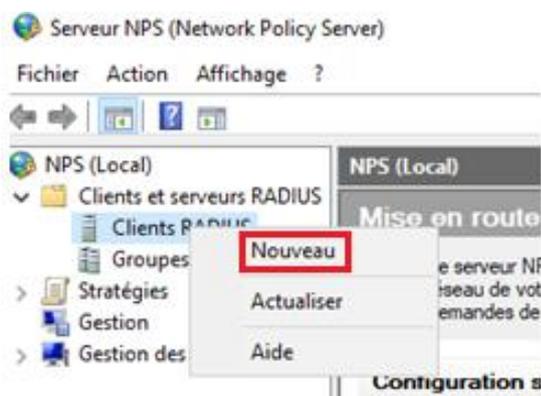
Configuration du service NPS

Afin d'accéder au service NPS, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Outils** → **Serveur NPS (Network Policy Server)**.

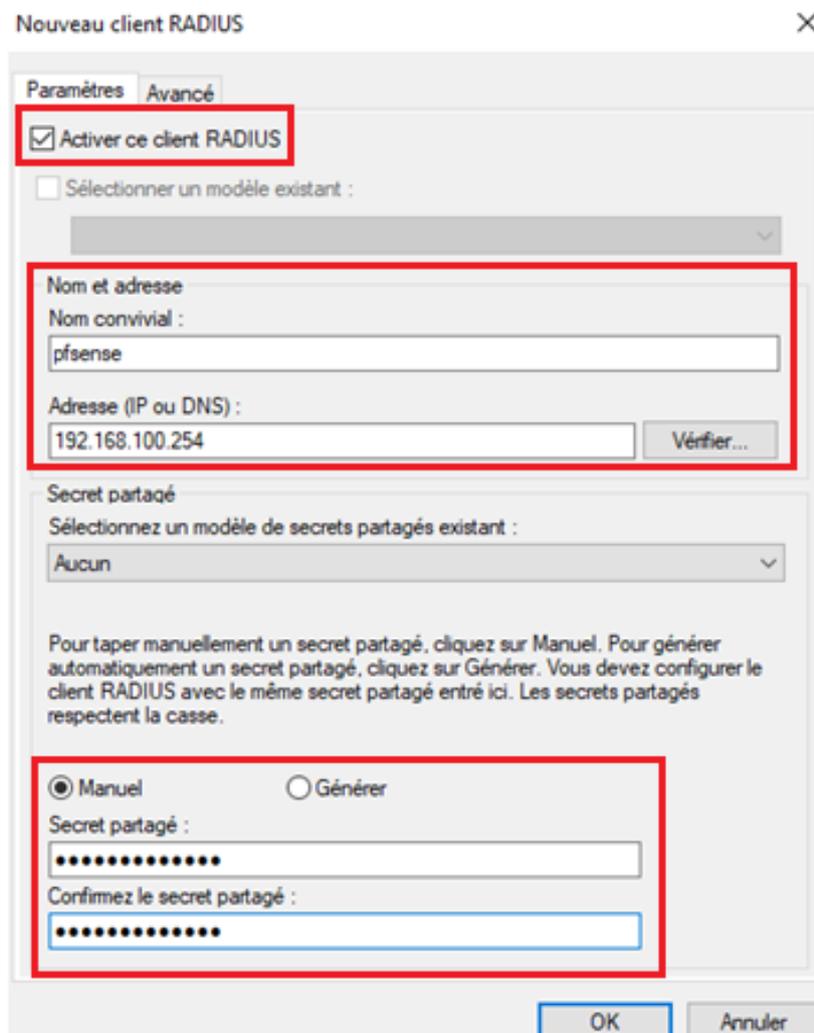


Création d'un nouveau client RADIUS

Pour créer un nouveau client RADIUS, faites un clic-droit sur « **Clients RADIUS** » puis « **Nouveau** ».



Cochez la case d'activation du client RADIUS. Ensuite, **indiquez** le nom convivial pour ce client ainsi que son adresse IP ou son nom DNS. Enfin, **indiquez ou générez** un secret partagé (code) qui devra être configuré de manière identique sur le client et le serveur RADIUS. Dans ce cas précis, le client RADIUS sera le routeur/pare-feu pfSense.

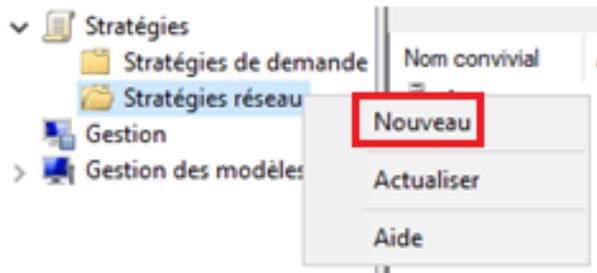


Le client RADIUS est créé, passons à présent à la mise en place de la stratégie réseau, autorisant les utilisateurs à être **authentifiés** sur le portail captif.

NPS (Local)		Clients RADIUS													
<ul style="list-style-type: none"> ✓ Clients et serveurs RADIUS <ul style="list-style-type: none"> Clients RADIUS Groupes de serveurs RA > Stratégies > Gestion > Gestion des modèles 	<p>Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.</p> <table border="1"> <thead> <tr> <th>Nom convivial</th> <th>Adresse IP</th> <th>Fabricant du périphérique</th> <th colspan="2">État</th> </tr> </thead> <tbody> <tr> <td>pfsense</td> <td>192.168.100.254</td> <td>RADIUS Standard</td> <td colspan="2">Activé</td> </tr> </tbody> </table>					Nom convivial	Adresse IP	Fabricant du périphérique	État		pfsense	192.168.100.254	RADIUS Standard	Activé	
Nom convivial	Adresse IP	Fabricant du périphérique	État												
pfsense	192.168.100.254	RADIUS Standard	Activé												

Création d'une nouvelle stratégie réseau

Pour créer une nouvelle stratégie réseau, effectuez un clic-droit sur **Stratégies réseau** puis cliquez sur **Nouveau**.



Nommez la stratégie puis cliquez sur Suivant.

Nouvelle stratégie réseau ×

 **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 :

Ensuite, nous allons ajouter les Groupes d'utilisateurs **ciblés**. Pour ce faire, cliquez sur Ajouter.

Nouvelle stratégie réseau ×

 **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 :

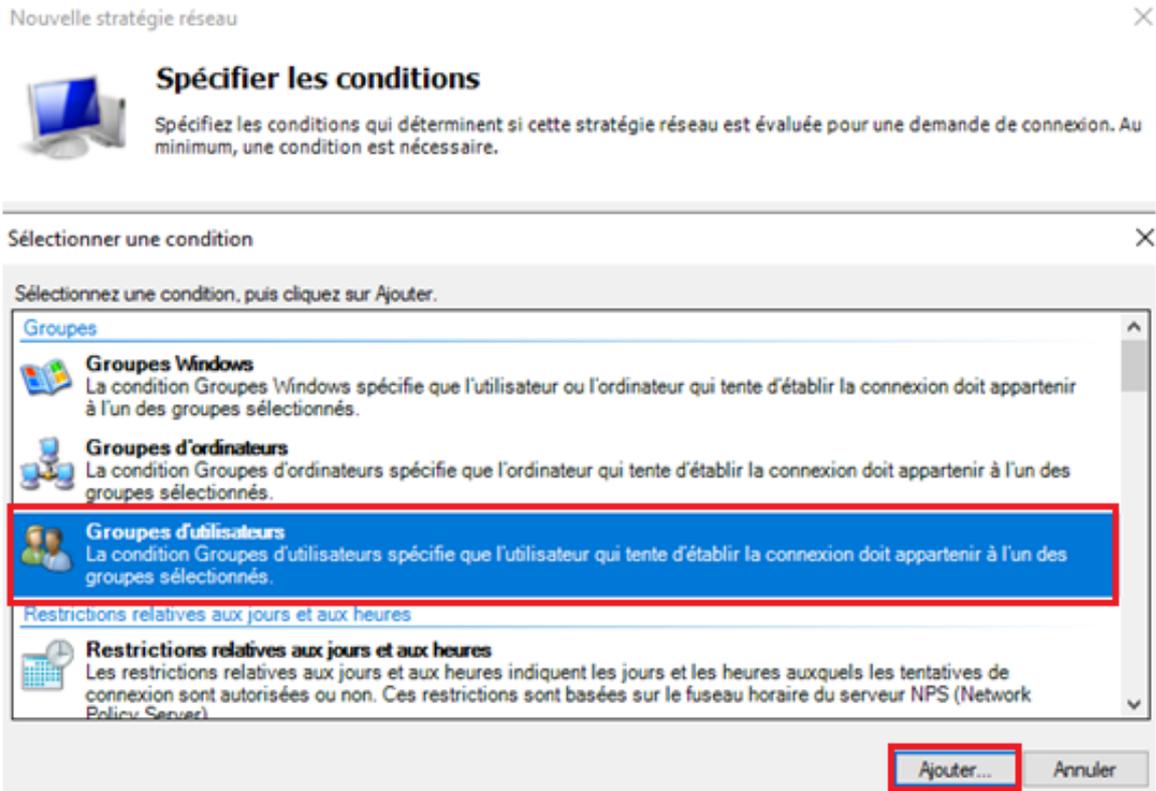
Condition	Valeur
-----------	--------

Description de la condition :

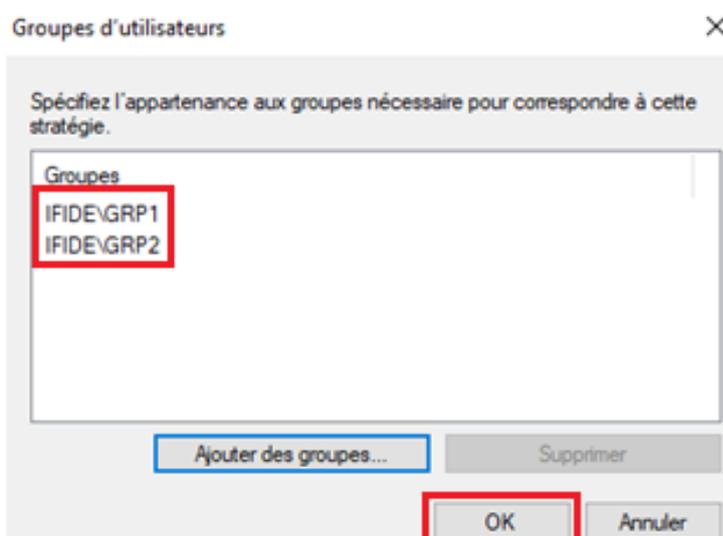
Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Sélectionnez les Groupes d'utilisateurs **souhaités**, puis cliquez sur **Ajouter**.



Ajoutez les groupes en cliquant sur le bouton « **Ajouter des groupes** ». Après avoir sélectionné les groupes souhaités, cliquez sur **OK** pour valider.



Ensuite, **cochez** l'option « **Accès accordé** » afin d'autoriser l'accès aux groupes d'utilisateurs, puis cliquez sur **Suivant**.

Nouvelle stratégie réseau ×

 **Spécifier l'autorisation d'accès**
Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

Accès accordé
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

Accès refusé
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Vous pouvez laisser la configuration des mécanismes d'authentification **par défaut** et cliquer sur **Suivant**. **Toutefois**, vous avez la possibilité de cocher d'autres mécanismes d'authentification, tel que l'authentification chiffrée CHAP, **si nécessaire**.

Nouvelle stratégie réseau

✕



Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter...

Modifier...

Supprimer

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

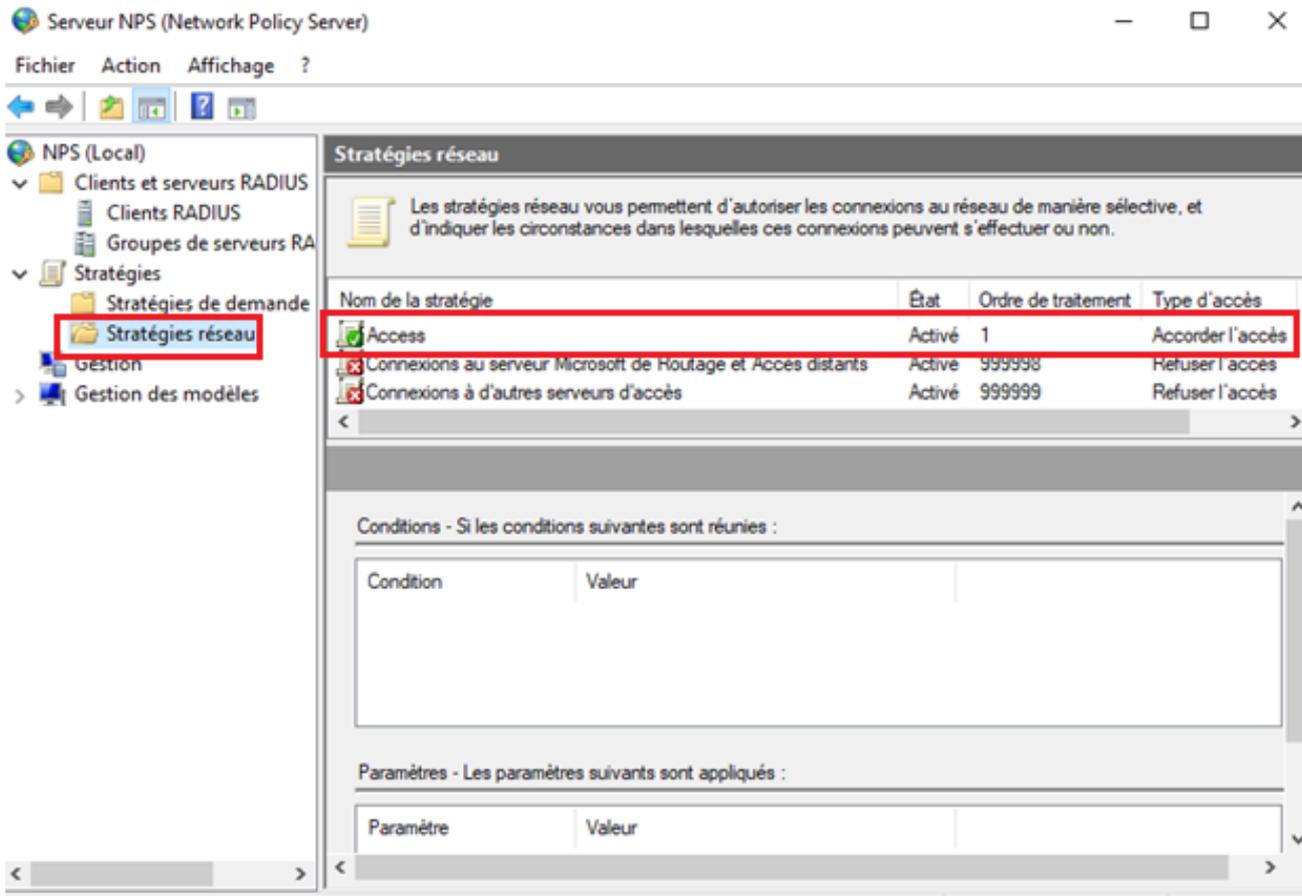
Précédent

Suivant

Terminer

Annuler

Ensuite, **cliquez** sur **Suivant** afin de finaliser la configuration et de vérifier que la nouvelle stratégie réseau a bien été créée.



À présent, il est **temps** de configurer le service du portail captif sous pfSense.

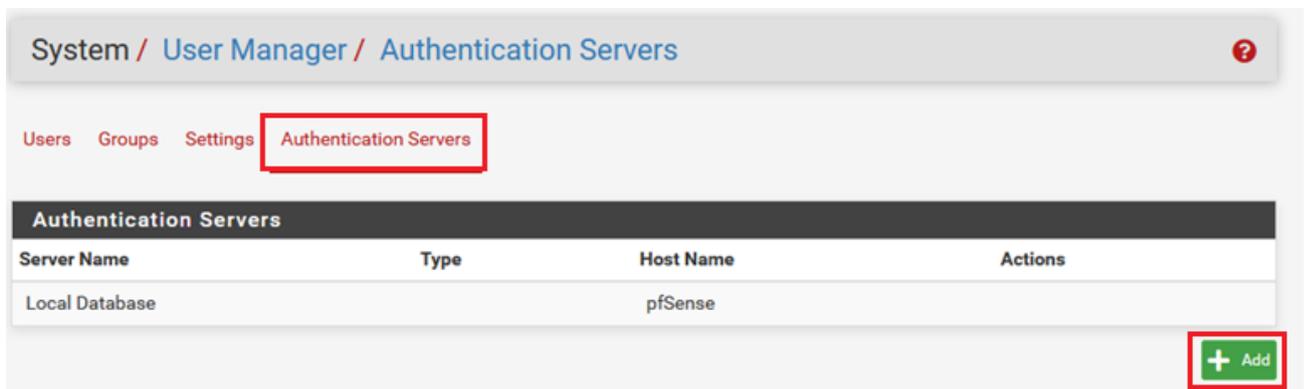
Configuration du portail captif sous pfSense

Pour lier pfSense au service d'authentification RADIUS, il est nécessaire d'indiquer les paramètres du serveur RADIUS dans le routeur/pare-feu pfSense. C'est le portail captif de pfSense qui interceptera les demandes de connexions des utilisateurs et les redirigera initialement vers sa page de connexion. Ensuite, il interrogera le serveur RADIUS spécifié pour l'authentification.

Pour réaliser cela, il faut d'abord créer une entrée de type "Authentication Server" dans l'interface de pfSense. Puis, activez le service **Captive Portal** en le configurant pour utiliser le serveur d'authentification RADIUS créé précédemment.

Création du serveur d'authentification

Naviguez dans le menu **System** → **User Manager** → **Authentication Server**, puis cliquez sur « **Add** ».



System / User Manager / Authentication Servers

Users Groups Settings **Authentication Servers**

Server Name	Type	Host Name	Actions
Local Database	RADIUS	pfSense	

+ Add

Ensuite, **configurez** les informations suivantes pour le nouveau serveur d'authentification (les termes entre parenthèses sont souvent les libellés dans l'interface) :

- **Nom convivial** : Indiquez un nom pour identifier ce serveur.
- **Type** : Sélectionnez **RADIUS**.
- **Adresse du serveur (Hostname or IP address)** : Saisissez l'adresse IP du serveur NPS principal.
- **Secret partagé (Shared Secret)** : Entrez la clé secrète qui **doit être identique** à celle configurée sur le serveur NPS.

Enfin, cliquez sur **Save** pour valider la création du serveur d'authentification.

Server Settings	
Descriptive name	STG RADIUS
Type	RADIUS

RADIUS Server Settings	
Protocol	MS-CHAPv2
Hostname or IP address	192.168.100.1
Shared Secret	*****
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	<input type="text"/>
	This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute	LAN - 192.168.100.254
	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.
	<input type="button" value="Save"/>

System / User Manager / Authentication Servers

Users Groups Settings Authentication Servers

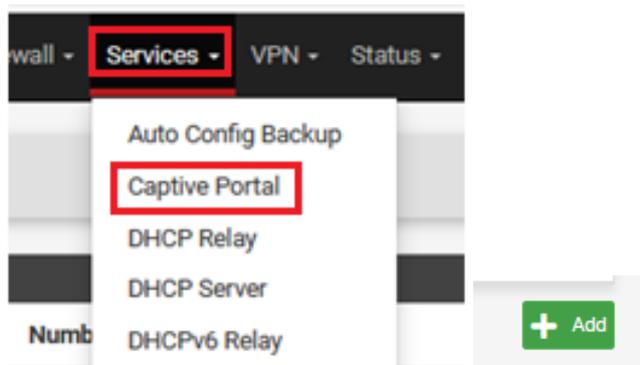
Authentication Servers			
Server Name	Type	Host Name	Actions
STG RADIUS	RADIUS	192.168.100.1	  
Local Database		pfSense	

Le serveur d'authentification est ajouté correctement.

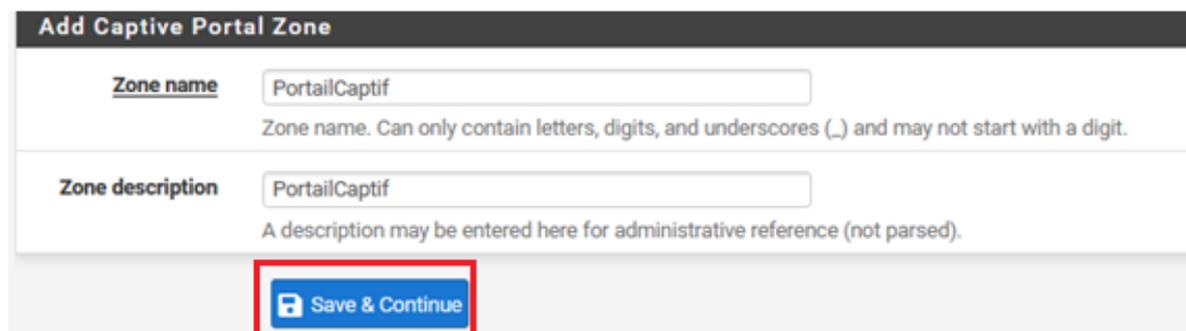
À présent, passons à la configuration du service Portail Captif sous pfSense.

Configuration du service portail captif

Naviguez dans le menu **Services** → **Portail Captif**, puis cliquez sur « **Ajouter** ».



Renseignez les informations demandées puis cliquez sur **Suivant**.

A screenshot of the 'Add Captive Portal Zone' form in pfSense. The form has two input fields: 'Zone name' and 'Zone description'. Both fields contain the text 'PortailCaptif'. Below the 'Zone name' field, there is a note: 'Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.' Below the 'Zone description' field, there is a note: 'A description may be entered here for administrative reference (not parsed)'. At the bottom of the form, there is a blue 'Save & Continue' button with a floppy disk icon, which is highlighted with a red box.

Cochez l'activation du portail captif, puis sélectionnez l'interface LAN.

Captive Portal Configuration

Enable **Enable Captive Portal**

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

Interfaces

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

Ensuite, dans cette section, **vous pouvez configurer** des éléments de personnalisation tels qu'une image **pour le logo**, une image d'arrière-plan, ou encore les **termes et conditions d'utilisation** du portail captif afin d'informer les utilisateurs.

L'affichage de ces termes et conditions est **fortement recommandé** pour le respect des législations en vigueur et l'obtention du consentement des utilisateurs (notamment pour la conformité au **RGPD**), ce qui répond aux exigences spécifiées dans le cahier des charges.

Captive Portal Login Page

Display custom logo image **Enable to use a custom uploaded logo**

Logo Image Aucun fichier sélectionné.
Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, it can be of any image type: .png, .jpg, .svg **This image will not be stored in the config.** The default logo will be used if no custom image is present.

Display custom background image **Enable to use a custom uploaded background image**

Background Image Aucun fichier sélectionné.
Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. **This image will not be stored in the config.** The default background image will be used if no custom background is present.

Terms and Conditions
Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

Choisissez la méthode d'authentification et sélectionnez le Serveur d'authentification créé précédemment

Authentication

Authentication Method Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server STG RADIUS
Local Database

You can add a remote authentication server in the [User Manager](#).

Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Secondary authentication Server STG RADIUS
Local Database

You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs.

This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

- **Cochez** la case « **Send RADIUS accounting packets** » pour activer la gestion des paquets RADIUS et permettre le monitoring de l'état du réseau et des connexions sur le serveur de destination (NPS).
- Pour l'**Accounting Server**, choisissez le serveur **STG RADIUS** configuré précédemment.
- Enfin, pour « **Send accounting updates** », **cochez** l'option « **No Updates** » pour ne permettre aucune mise à jour d'accounting intermédiaire.

Puis **enregistrez** les paramètres configurés en cliquant sur **Save**.

Accounting

RADIUS Send RADIUS accounting packets.
If enabled, accounting request will be made for users identified against any RADIUS server.

Accounting Server You can add a Radius Accounting server in the [User Manager](#).

Send accounting updates No updates Stop/Start Stop/Start (FreeRADIUS) Interim

Services / Captive Portal 📊 📄 ?

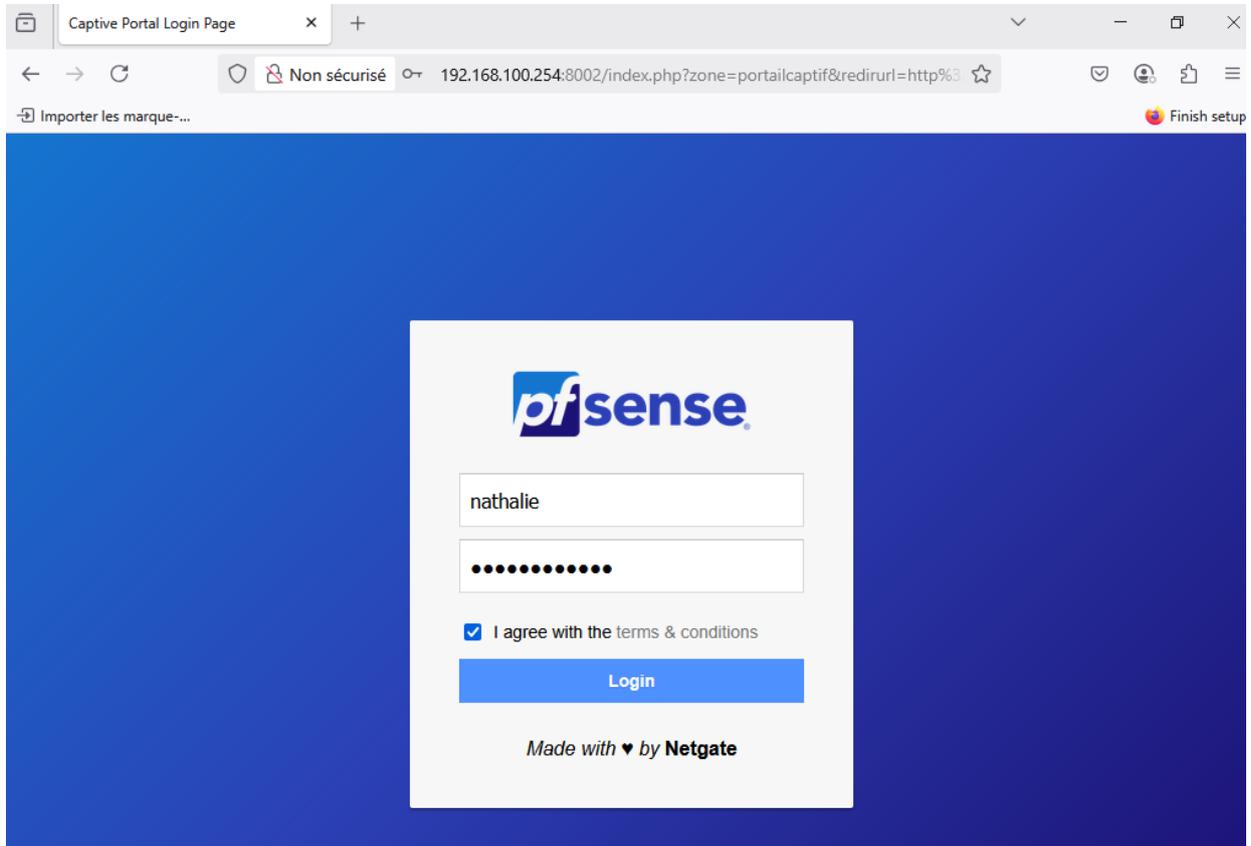
Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
PortailCaptif	LAN	0	PortailCaptif	 

À présent, **passons au** test de fonctionnement du portail captif.

Test d'intégration du portail captif

Pour effectuer les tests d'intégration, connectez-vous avec un compte utilisateur, puis ouvrez un navigateur Internet (Firefox, Microsoft Edge, Chrome, Brave, etc.).



Depuis Windows Server 2019, l'installation du service NPS n'ouvre pas les ports par défaut exploités par RADIUS qui sont les ports 1812,1813,1645, et 1646 en UDP sur les serveurs, bloquant ainsi toute requête d'authentification des utilisateurs.

Afin de résoudre ce problème, deux options sont sollicitées par l'équipe Microsoft :

1. Lancez la commande permettant de modifier l'identificateur de sécurité du compte de service pour détecter et autoriser efficacement le trafic RADIUS à travers le pare-feu Windows. Sans cette exception, le pare-feu supprime le trafic RADIUS.
2. Ajouter une règle personnalisée sur le pare-feu qui autorise les connexions entrantes à travers les ports mentionnés précédemment (1812,1813,1645,1646 UDP)

Modification du SID unique des services IAS

La commande permettant la modification du SID unique est la suivante (à exécuter sur une invite de commande ou PowerShell avec les droits d'administrateur) :

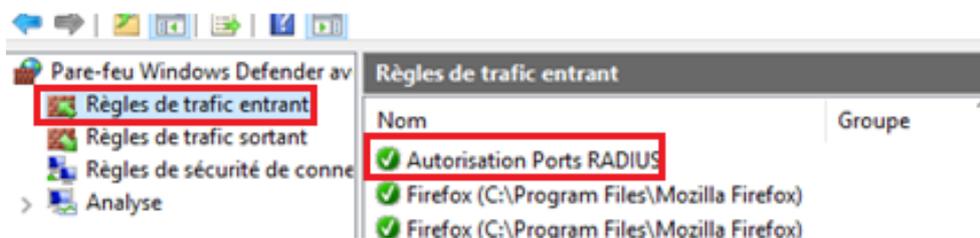
```
PS C:\Users\Administrateur> sc.exe sidtype IAS unrestricted
```

Après l'exécution de la commande, il vous faudra par la suite redémarrer le serveur pour appliquer les modifications apportées.

D'où l'intérêt de la seconde option, qui ne nécessite pas de redémarrer le serveur, mais de rajouter une règle qui autorise le flux sur le pare-feu de Windows.

Ajout règle pare-feu Windows autorisant les ports par défaut RADIUS

Nous nous limiterons sur la méthode graphique, mais rien ne vous empêche d'effectuer les opérations avec PowerShell, ou encore via les commandes de l'invite de commande.



Propriétés de : Autorisation Ports RADIUS

Étendue Avancé Entités de sécurité locales Utilisateurs distants

Général Programmes et services Ordinateurs distants Protocoles et ports

Protocoles et ports

Type de protocole : UDP

Numéro de protocole : 17

Port local : Ports spécifiques
1812, 1813, 1645, 1646
Exemple : 80, 443, 5000-5010

Port distant : Tous les ports
Exemple : 80, 443, 5000-5010

Paramètres ICMP (Internet Control Message Protocol) : Perso...

OK Annuler Appliquer

Propriétés de : Autorisation Ports RADIUS

Général Programmes et services Ordinateurs distants Protocoles et ports

Étendue Avancé Entités de sécurité locales Utilisateurs distants

Profils

Spécifiez les profils auxquels cette règle s'applique.

Domaine

Privé

Public

Types d'interfaces

Spécifier les types d'interfaces auxquels cette règle doit s'appliquer. Personnaliser...

Traversée latérale

La traversée latérale permet à l'ordinateur d'accepter des paquets entrants non sollicités qui sont passés par un périphérique de périmètre, tel qu'un routeur NAT (Network Address Translation) ou un pare-feu.

Bloquer la traversée latérale

Empêcher les applications de recevoir du trafic non sollicité directement d'Internet via un périphérique de périmètre NAT (Network Address Translation).

Action

Autoriser la connexion

Autoriser la connexion seulement si elle est sécurisée

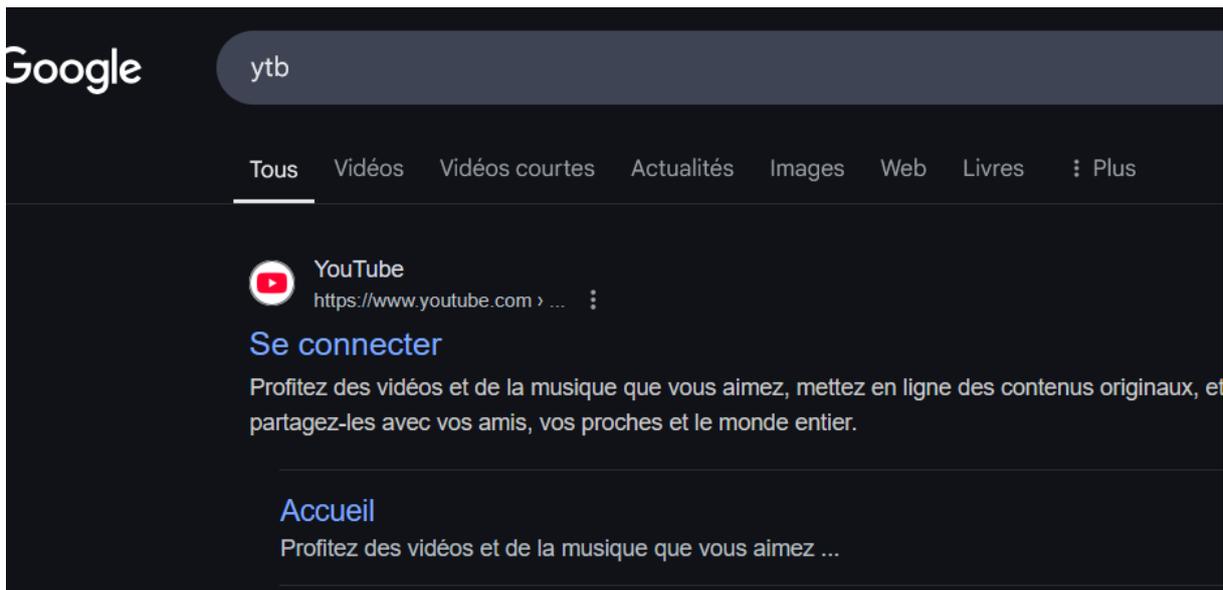
Personnaliser...

Bloquer la connexion

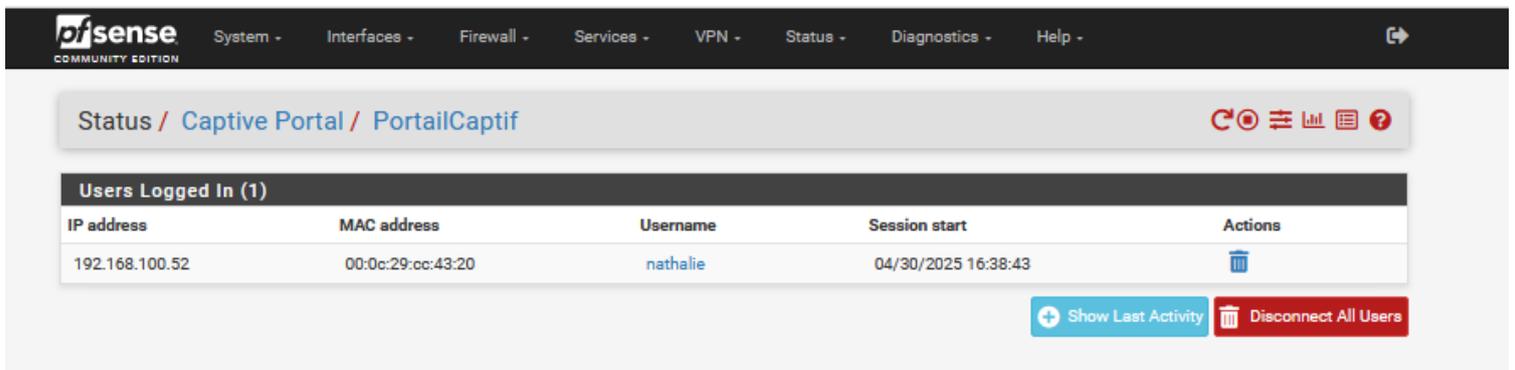
OK Annuler Appliquer

A présent, les requêtes d'authentification sont autorisées sur le réseau, et les utilisateurs pourront ainsi par la suite se connecter au portail captif.

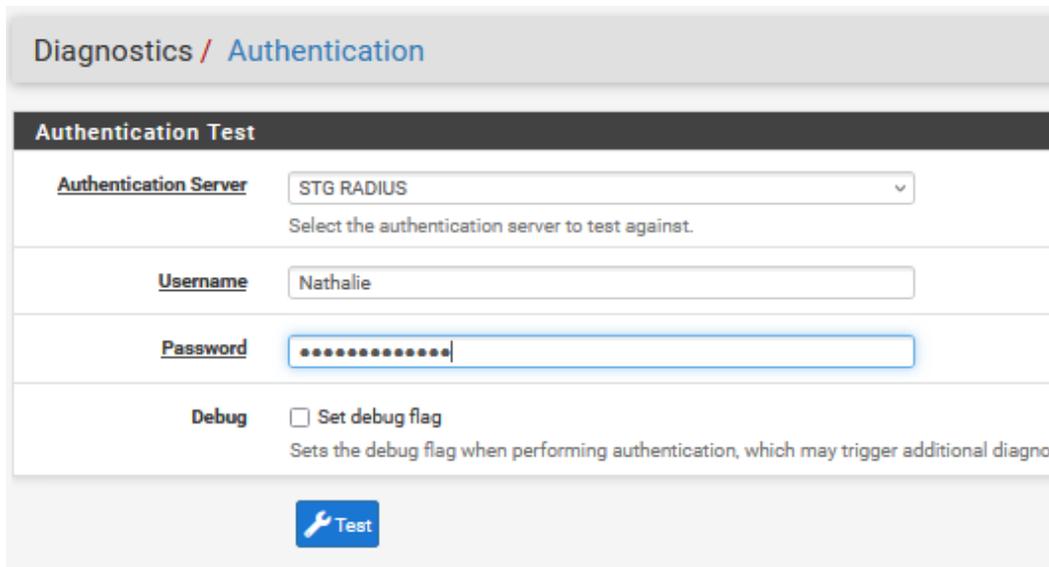
Après authentification, les utilisateurs ont bel et bien accès à Internet.



Nous pouvons également voir dans la liste des utilisateurs connecté sur pfSense en allant sur **Status → Captive Portal** :

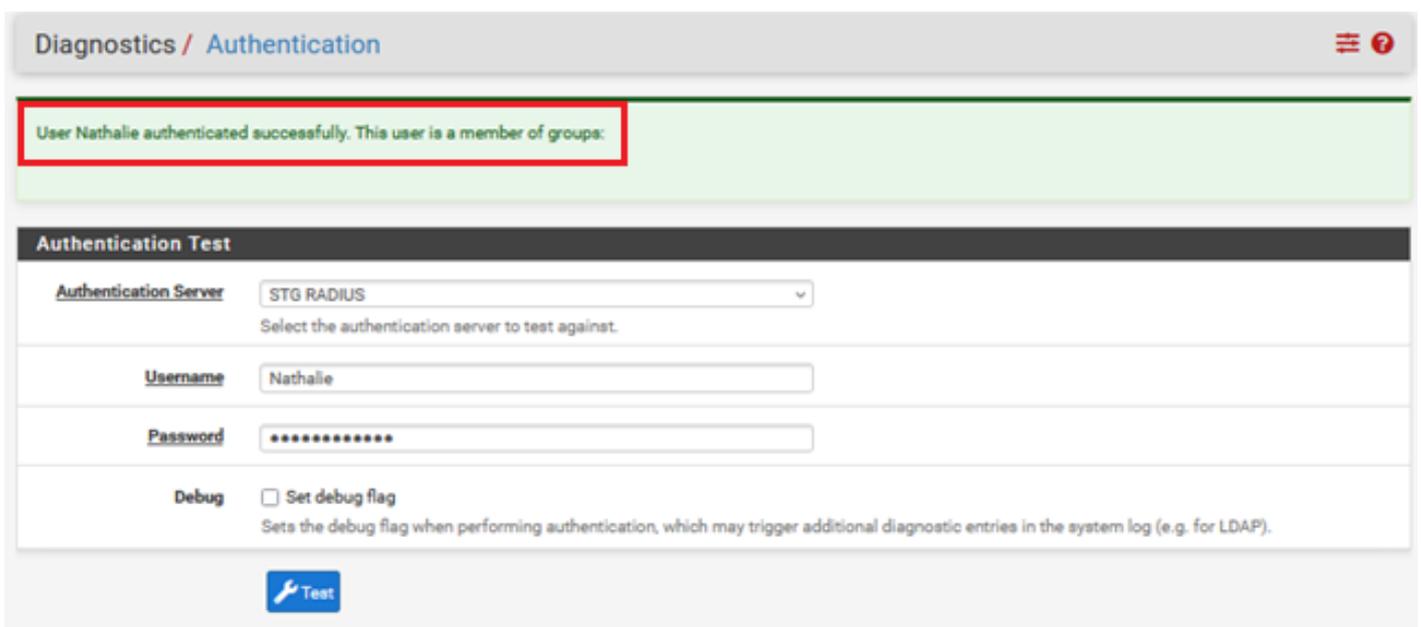


Enfin, nous pouvons également tester le bon fonctionnement de nos serveurs d'authentification sur pfSense en allant dans **Diagnostics** → **Authentication**. Puis renseignez les identifiants AD et cliquez sur **Test** :



The screenshot shows the 'Diagnostics / Authentication' page in pfSense. The 'Authentication Test' section is active. It features a dropdown menu for 'Authentication Server' set to 'STG RADIUS'. Below it is a text input for 'Username' containing 'Nathalie' and a password input field with masked characters. A 'Debug' section has an unchecked checkbox for 'Set debug flag'. At the bottom is a blue 'Test' button with a wrench icon.

De cette manière, vous pouvez déjà savoir en amont si le serveur d'authentification accepte la requête d'authentification.



This screenshot shows the same 'Authentication Test' interface as above, but with a green success message at the top: 'User Nathalie authenticated successfully. This user is a member of groups:'. The message is enclosed in a red rectangular box. The form fields and the 'Test' button remain visible below the message.