

Documentation serveur DFR et réplication DFS (DFRS)

By – Mathys CANTREL

Sommaire

Contexte :	3
Mise en Place VM :	3
I. Installation de DFS avec l'interface graphique	5
II. Le type de racines DFS choisi	6
III. Créer une racine DFS : espace de noms de domaine	6
IV. Créer l'arborescence de dossiers DFS	9
V. Activation de l'énumération basée sur l'accès avec DFS	11
VI. Ajouter un serveur d'espaces de noms supplémentaire	13
VII. Installation de DFSR avec l'interface graphique	14
VIII. Configuration du groupe de réplication DFSR	15
IX. Gestion des droits sur le dossier DFS :	20
X. Test du DFSR	21
XI. Créer un conteneur VeraCrypt	22

Contexte :

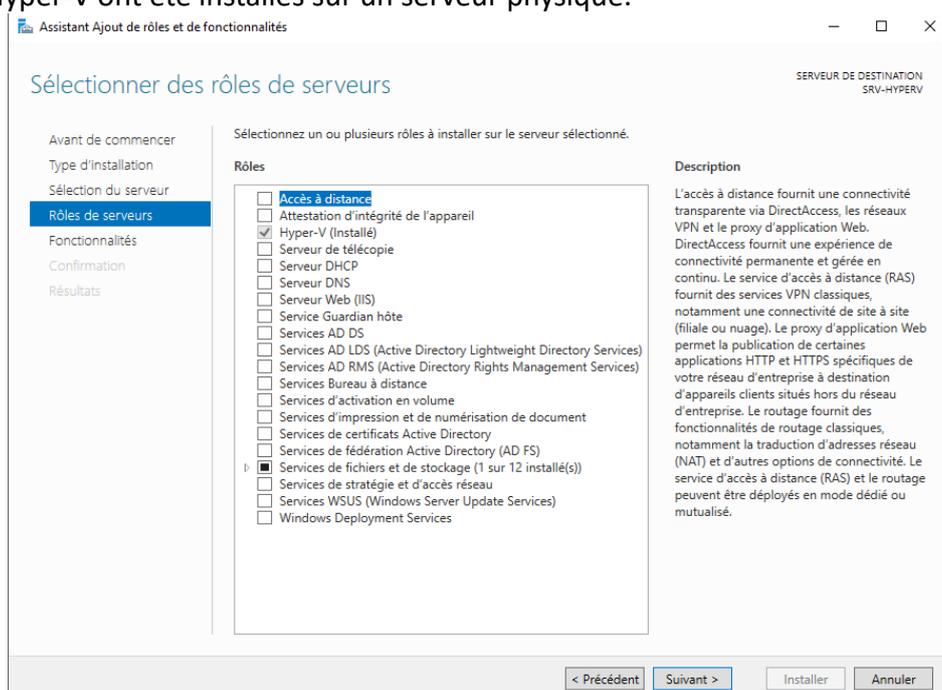
Les entreprises ByteMeUp, Pare-Fouine et Cloud Macronique ont décidé de s'associer pour répondre à un appel à projet d'une agence gouvernementale de cybersécurité. Ce projet simulera une/des cyberattaque(s) sur des infrastructures diverses. Chaque entreprise ayant son domaine de compétences, elles ont décidé de monter chacune une infrastructure spécifique à celles-ci. Ces infrastructures auront un accès sécurisé vers l'extérieur, les 3 infrastructures seront interconnectées entre elles.

L'entreprise Cloud Macronique est spécialisée en réseau. Elle mettra en place une infrastructure avec un wifi sécurisé, un outil de supervision du réseau, un cœur de réseau et une segmentation réseau.

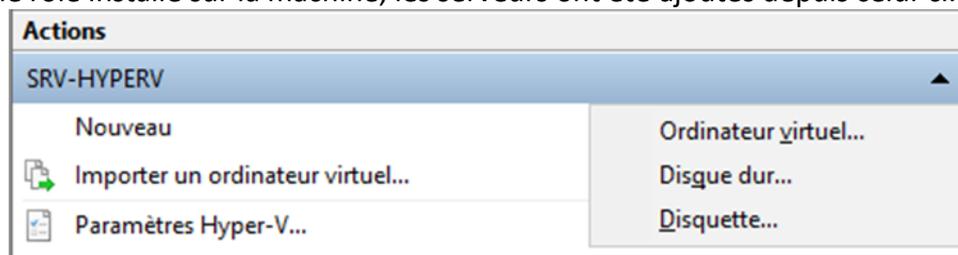
Au sein de cette entreprise, le projet consiste à mettre en place un serveur de fichiers répliqué avec le services DFS (Distributed File System) et DFSR (Distributed File System replication).

Mise en Place VM :

Pour héberger les machines virtuelles de l'infrastructure, Windows Server 2022 et les services Hyper-V ont été installés sur un serveur physique.



Une fois le rôle installé sur la machine, les serveurs ont été ajoutés depuis celui-ci.



Pour les serveurs de fichier, voici leur configuration :

SRV-AD01 :

- Nom : SRV-FICHER1
- RAM : 16GO
- Mémoire : 128GO
- Port réseau : LAN
- ISO : Windows 2022

SRV-AD02 :

- Nom : SRV-FICHER2
- RAM : 16GO
- Mémoire : 128GO
- Port réseau : LAN
- ISO : Windows 2022

Les autres paramètres ont été laissés par défaut.

Ordinateurs virtuels			
Nom	État	Utilisation du processeur	Mémoire affectée
SRV-AD01	Exécution	0 %	16384 Mo
SRV-AD02	Exécution	0 %	16384 Mo
SRV-CONTROLEUR	Désactivé		
SRV-FICHER1	Exécution	0 %	16384 Mo
SRV-FICHER2	Exécution	0 %	16384 Mo
SRV-OMADA	Exécution	0 %	4096 Mo
SRV-SUPERVISION	Exécution	0 %	4096 Mo

Une fois connecté sur les machines, paramétrages des IP en fix :

SRV-FICHER01 :

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 : 172 . 16 . 20 . 14

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

Passerelle par défaut : 172 . 16 . 20 . 254

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 20 . 12

Serveur DNS auxiliaire : 172 . 16 . 20 . 13

SRV-FICHER02 :

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 : 172 . 16 . 20 . 15

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

Passerelle par défaut : 172 . 16 . 20 . 254

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 20 . 12

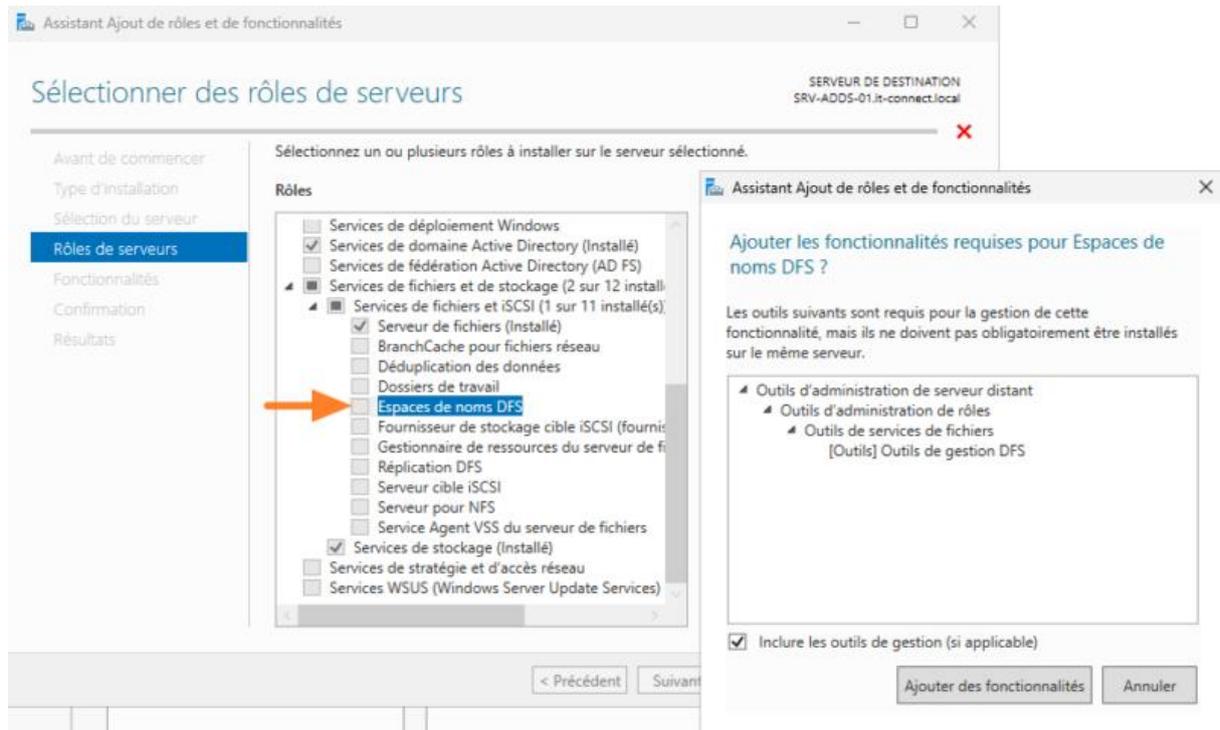
Serveur DNS auxiliaire : 172 . 16 . 20 . 13

Activation de la prise en main à distance depuis les paramètres Windows.

I. Installation de DFS avec l'interface graphique

Dans le « Gestionnaire de serveur », Ajout du rôle et fonctionnalité dans le menu.

Pour l'installation du service DFS, se rendre dans les « Services de fichiers et de stockage » -> « Services de fichiers et iSCSI », installer le rôle « Espaces de nom DFS » et « Ajouter ses fonctionnalités » nécessaires au bon fonctionnement du rôle.



II. Le type de racines DFS choisi

Il existe deux types de racines DFS : "**Racine autonome**" et "**Racine de noms de domaine**". Une racine DFS est également appelée un espace de noms.

- La **Racine autonome (Espace de noms autonome)**, est le choix qui n'a pas été retenu car elle possède trop de contraintes.
- **Racine de noms de domaine (Espace de noms de domaine)**

La racine de noms de domaine qui a été retenue, s'appuie sur le nom de domaine Active Directory et la résolution DNS pour fonctionner. Le nom du serveur DFS n'est donc pas repris dans le chemin UNC puisqu'il est remplacé par le nom de domaine. Ainsi, il est possible d'avoir plusieurs serveurs d'espace de noms (DFSR) pour une même racine de noms de domaine.

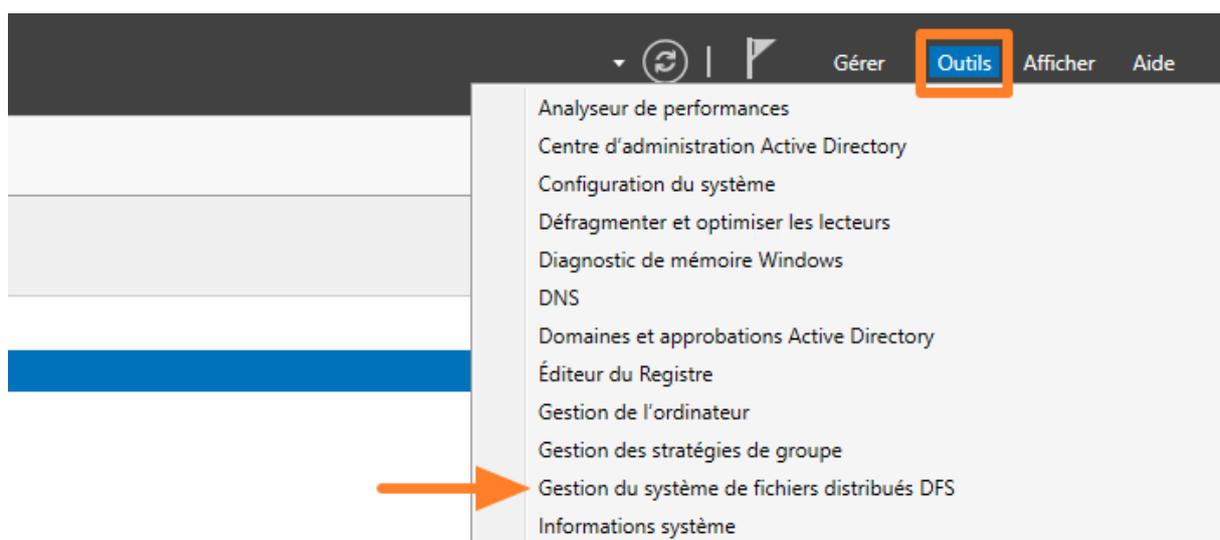
Voici un exemple de chemin d'accès vers une racine de noms de domaine :

<\\cloud-marcronique.local\Partages>

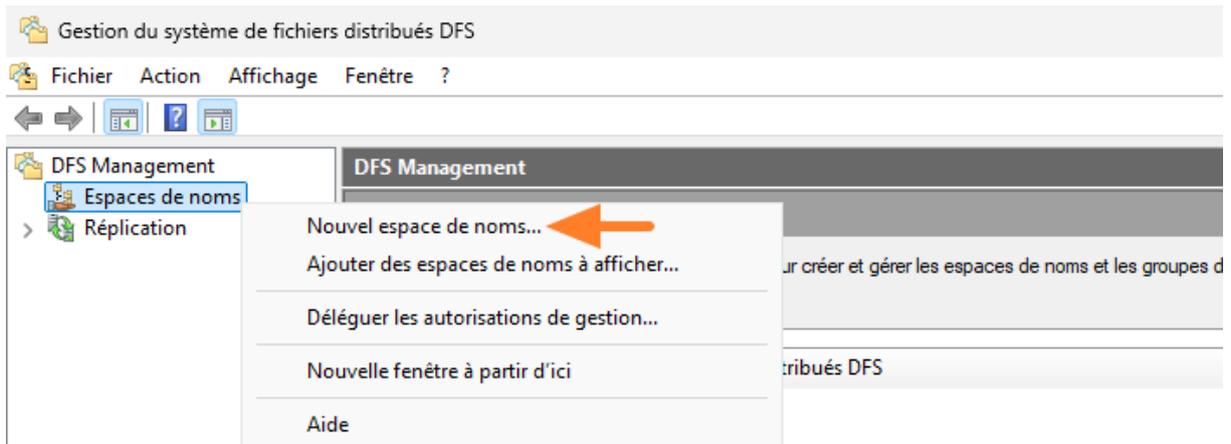
III. Créer une racine DFS : espace de noms de domaine

Création de la racine DFS en prenant le soin de choisir le type "**Espace de noms de domaine**".

Depuis le **Gestionnaire de serveur**, ouverture de la console « **Gestion du système de fichiers distribués DFS** ».



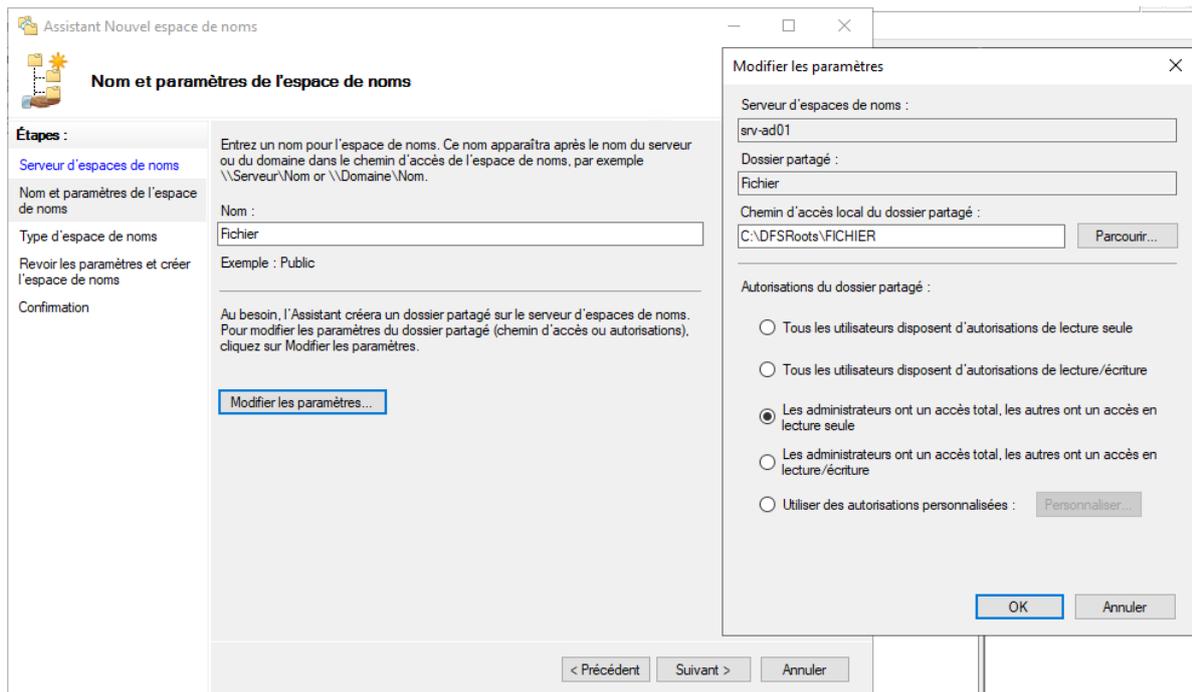
Création d'un « **Nouvel espace de noms...** ».



Lors de l'installation, le serveur d'espace de noms qui hébergera cette nouvelle racine DFS est attendu. Sélection « **SRV-AD01.cloud-macronique.local** » pour gérer l'espace de nom comme choisi précédemment dans la gestion de la Racine de noms de domaine.

Comme nom de racine, il a été choisi « fichier ». Dans les paramètres avancés, modification des autorisations du dossier partagé :

- Les administrateurs ont un accès total, les autres ont un accès en lecture seul.

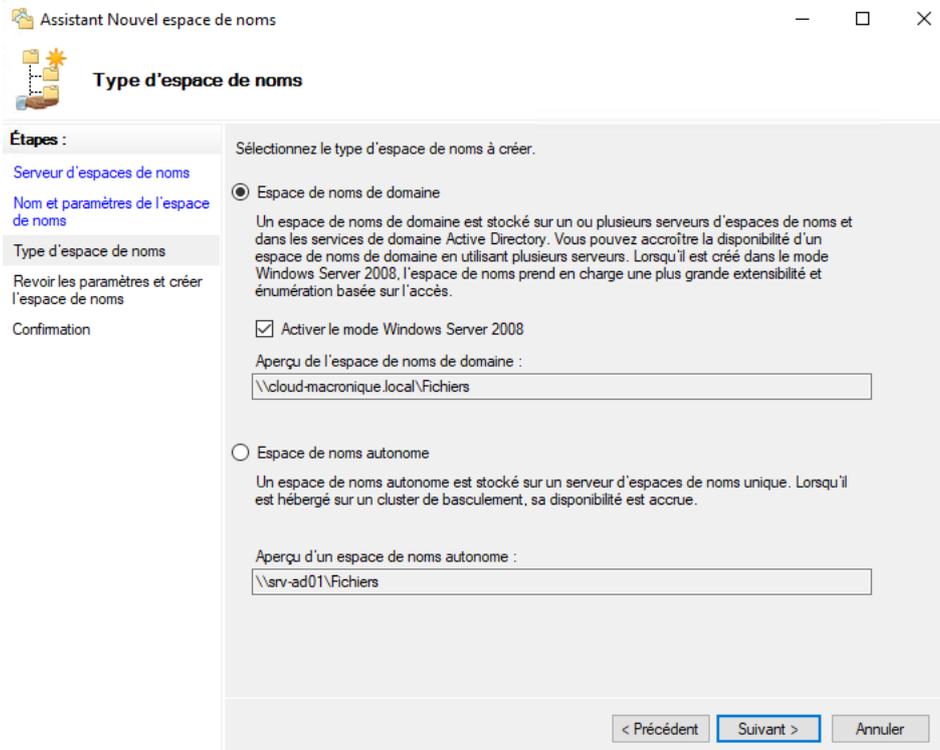


Lors de la sélection du type d'espace de noms, comme choisi précédemment : sélection du paramétrage « **Espace de noms de domaine** ».

Étant donné que notre racine DFS s'appuie sur la résolution DNS pour fonctionner, nous utiliserons le nom de domaine dans le chemin UNC. Ainsi, pour accéder à la racine de l'espace de noms DFS, le chemin réseau sera :

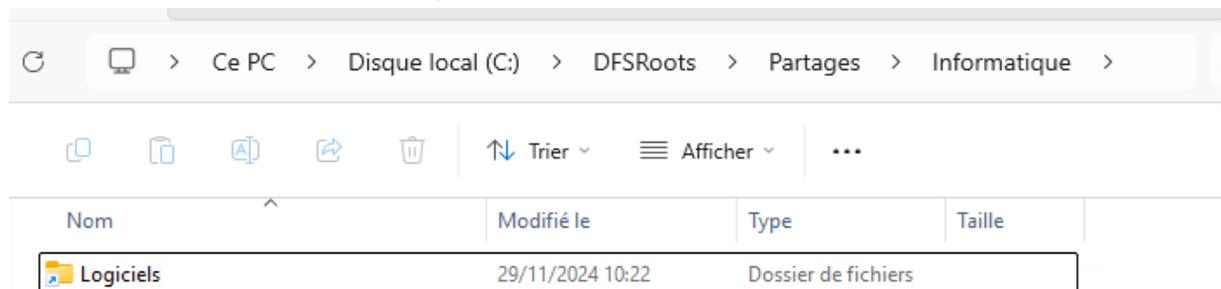
\\cloud-macronique.local\Fichier

"**Activation du mode Windows Server 2008**" pour de meilleures fonctionnalités.



La création de la racine DFS est fini.

Il est à noter que sur un serveur DNS, l'arborescence est créée sur le volume "C" dans un répertoire nommé "**DFSRoots**". Le dossier ne contient aucune donnée, mais il sert à créer l'arborescence de dossiers telle qu'elle est créée dans la console DFS.



IV. Créer l'arborescence de dossiers DFS

Avant la création d'un dossier DFS, Il faut créer les dossiers sur le srv-fichier1 pour la liaison.

Dans le dossier C:\fichier création des dossiers :

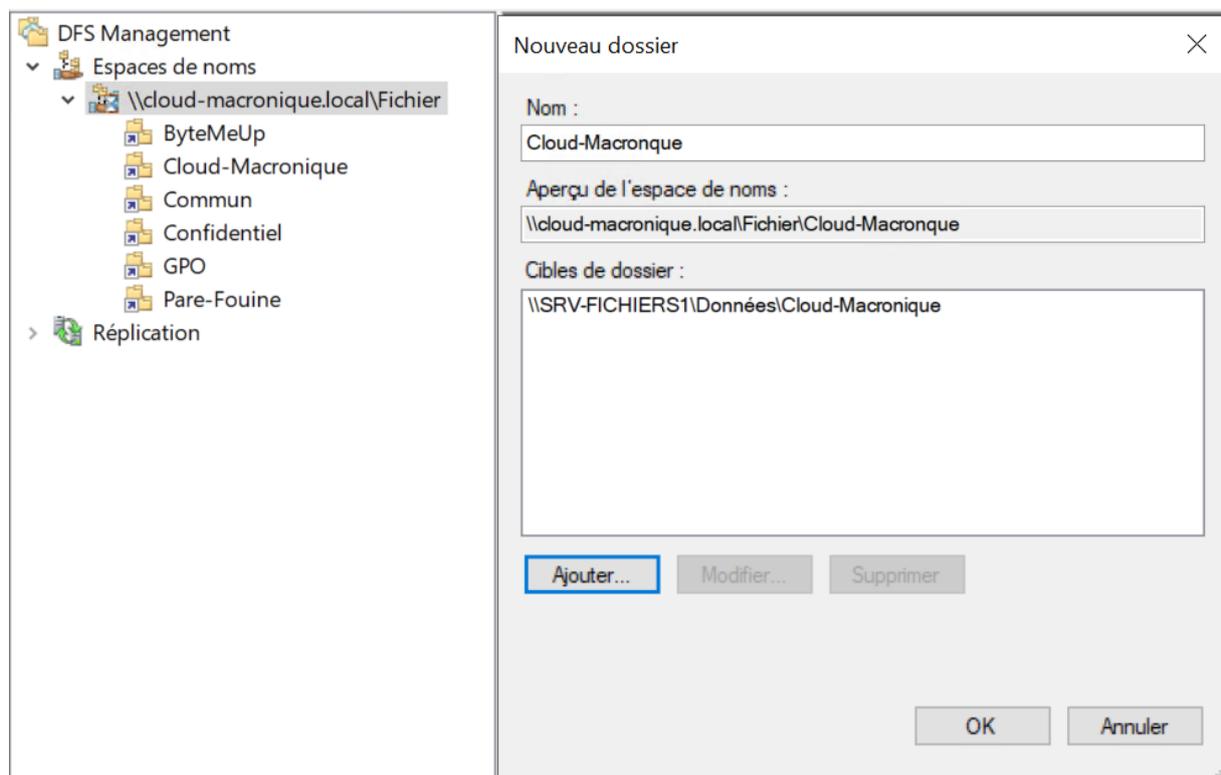
- ByteMeUp
- Commun
- Confidentiel
- GPO
- Pare-Fouine

Afin de créer un dossier, qui aura une « **liaison DFS** » dans la console « **Gestion du système de fichiers distribués DFS** », créer un « **Nouveau dossier** » sur la racine DFS que nous avons créé précédemment.

Le nom de ce dossier sera "**Cloud-Macronique**", le partage sera hébergé sur le serveur "**SRV-FICHIERS01.cloud-macronique.local**" et il se nomme "**Cloud-Macronique**".

Je vais recommencer cette étape pour les dossiers :

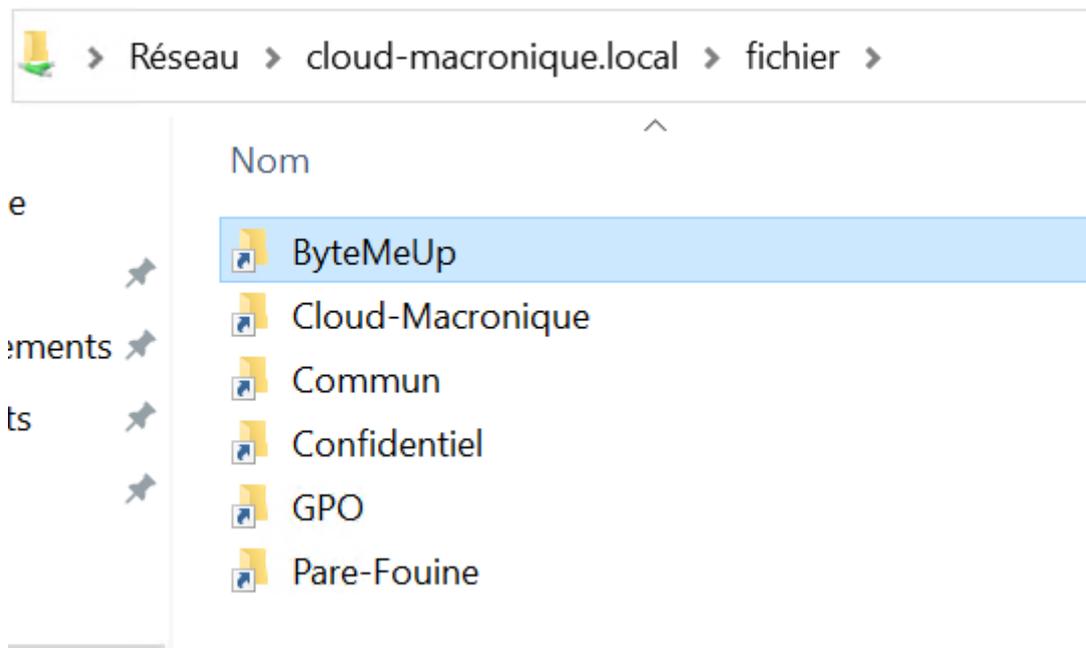
- ByteMeUp
- Commun
- Confidentiel
- GPO
- Pare-Fouine



Test :

Connexion possible sur le dossier DFS via le chemin UNC :

\\cloud-cronique.local\fichier\nom_du_dossier

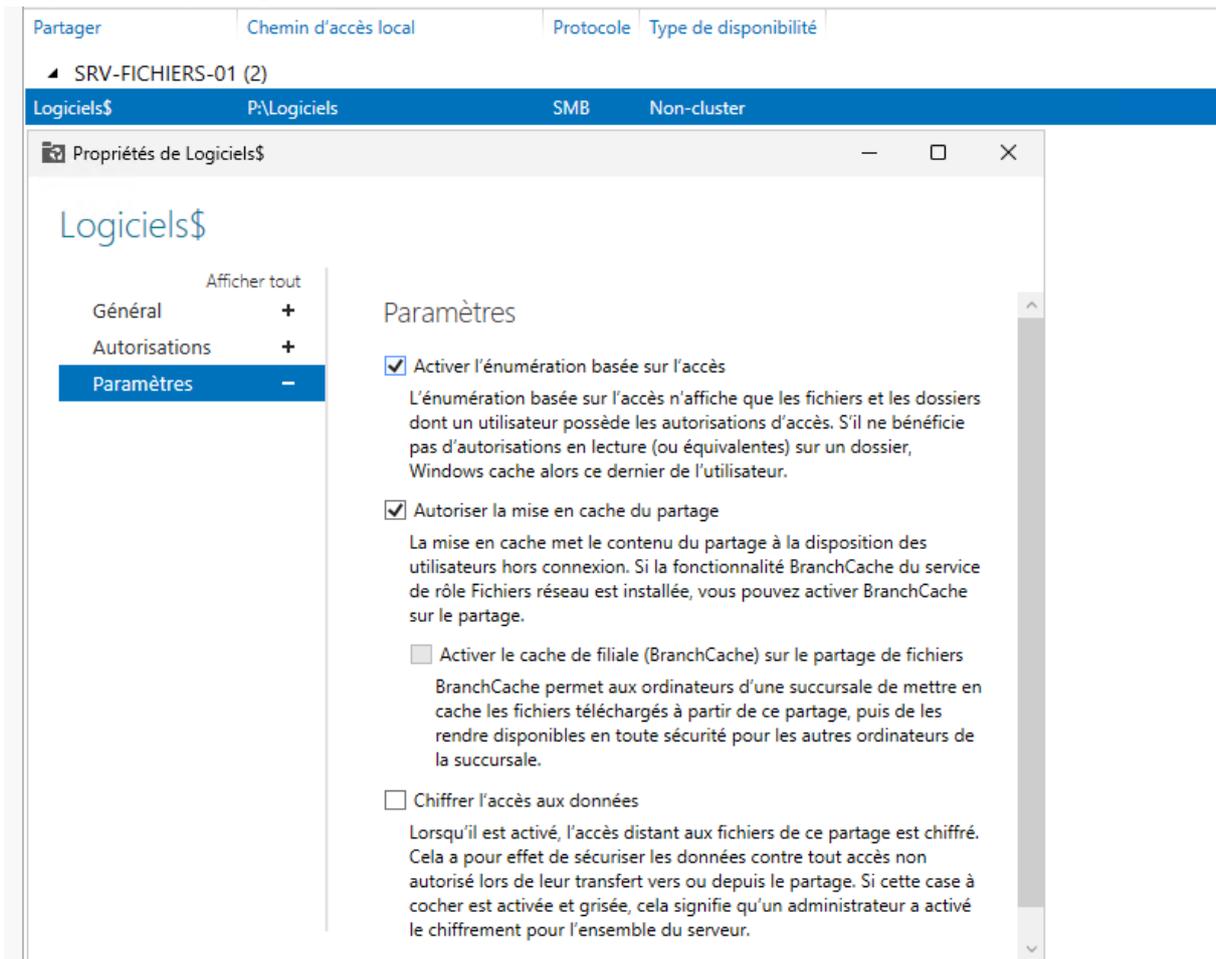


Quant au contenu de ses dossiers, quand ils sont modifiés, déposer ou consulter ils sont en réalité modifiés dans l'espace de stockage "**\\srv-fichier01.cloud-macronique.local\fichier**", de façon dynamique.

V. Activation de l'énumération basée sur l'accès avec DFS

L'énumération basée sur l'accès (ABE) est une fonctionnalité qui permet de **montrer à l'utilisateur uniquement les dossiers auxquels il a le droit d'accéder**, à minima en lecture seule. Autrement dit, si un utilisateur n'a pas les permissions sur un dossier, il ne le verra pas dans son Explorateur de fichiers.

Dans le cadre de l'utilisation de DFS, activation de l'énumération basée sur l'accès dans les propriétés du partage étant référencé comme cible.



De plus, activation de cette option dans les paramètres de l'espace de noms sinon l'espace de noms sera également visible sur les SRV-AD.

Général Références **Avancée**

Les serveurs d'espaces de noms interrogent un contrôleur de domaine pour obtenir les métadonnées d'espace de noms actuelles. Vous pouvez optimiser l'interrogation afin d'améliorer la cohérence ou l'extensibilité de l'espace de noms.

Comment voulez-vous optimiser l'interrogation ?

Optimiser pour la cohérence

Les serveurs d'espaces de noms interrogent l'émulateur du contrôleur de domaine principal (PDC) à chaque modification de l'espace de noms.

Optimiser pour l'extensibilité

Chaque serveur d'espaces de noms interroge son contrôleur de domaine le plus proche à intervalles réguliers. Cette opération est appelée mode d'extensibilité de l'espace de noms.

L'énumération basée sur l'accès masque les dossiers de cet espace de noms que les utilisateurs n'ont pas l'autorisation d'afficher.

Activer l'énumération basée sur l'accès pour cet espace de noms

OK

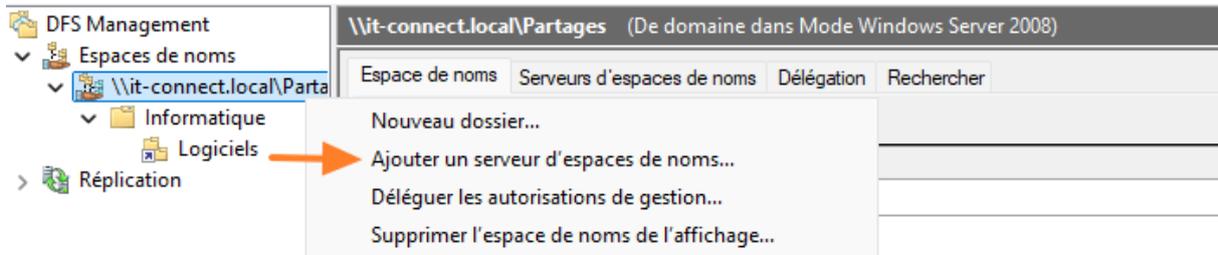
Annuler

Appliquer

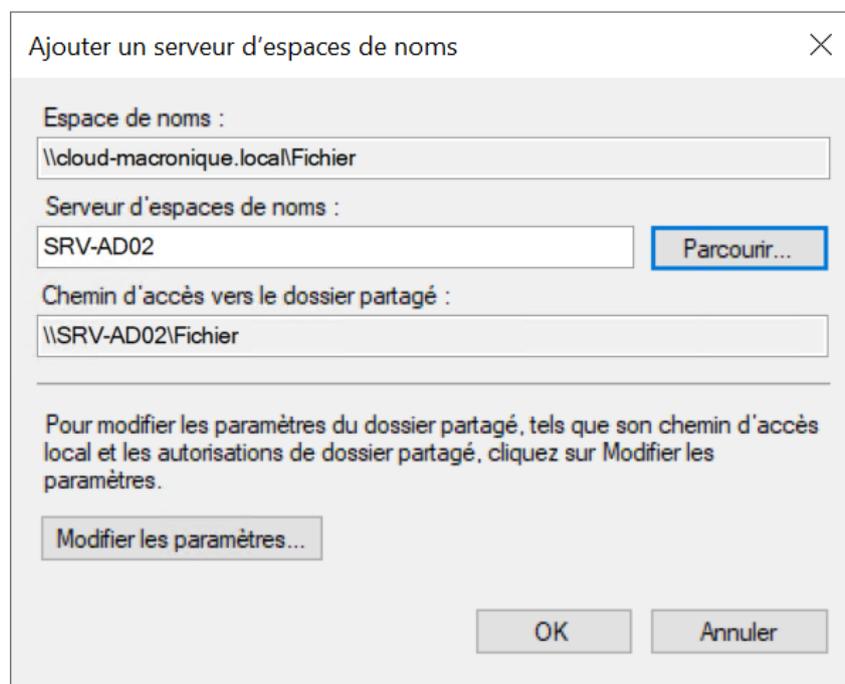
VI. Ajouter un serveur d'espaces de noms supplémentaire

Il est possible d'ajouter plusieurs serveurs DFS pour une racine d'espace de noms. Cela permettra, pour une même racine DFS, d'utiliser plusieurs serveurs et ainsi d'assurer la redondance et la haute disponibilité du service.

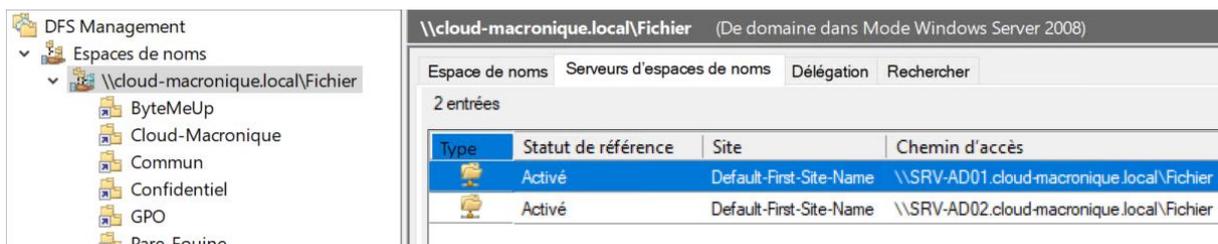
Dans la console DFS « **Ajouter un serveur d'espaces de noms** ».



Sélectionner le second serveur AD qui hébergera le serveur d'espaces de noms.



Pour confirmer la redondance, vérification dans l'onglet « **Serveurs d'espaces de noms** » dans la racine DFS. Désormais, la racine DFS "**Fichiers**" est hébergée par 2 serveurs d'espaces de noms.



Si un serveur est hors service, le second permettra toujours d'accéder à la racine DFS.

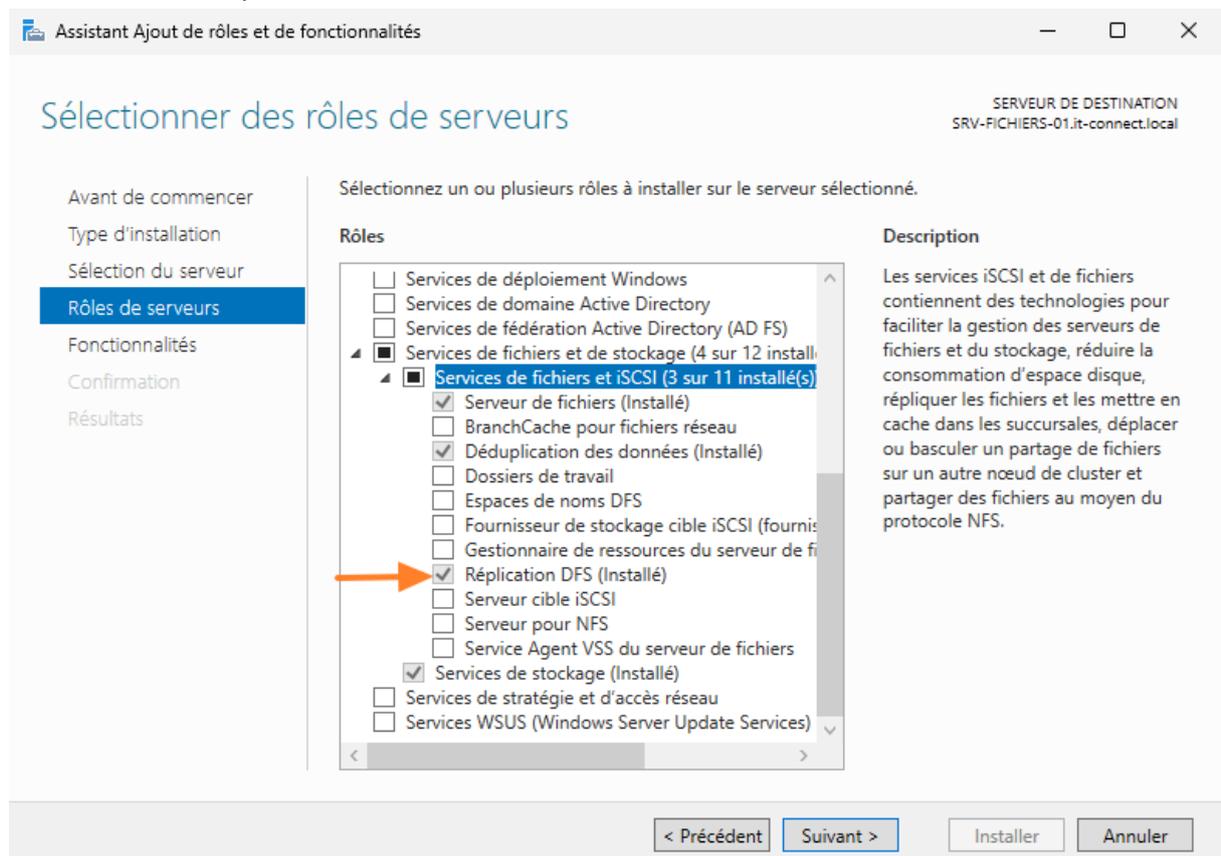
VII. Installation de DFSR avec l'interface graphique

Installation du rôle "DFSR" via l'interface graphique de Windows sur SRV-FICHIERS2.

Dans le « **Gestionnaire de serveur** », installation « **du rôle et ses fonctionnalités** » DFSR.

Dans l'étape "**Rôles de serveurs**" aller dans « **Service de fichiers et de stockage** » ->

« **Services de fichiers et iSCSI** » et sélection du rôle « **Réplication DFS** » et « **Ajout des fonctionnalités** » pour le bon fonctionnement du rôle.



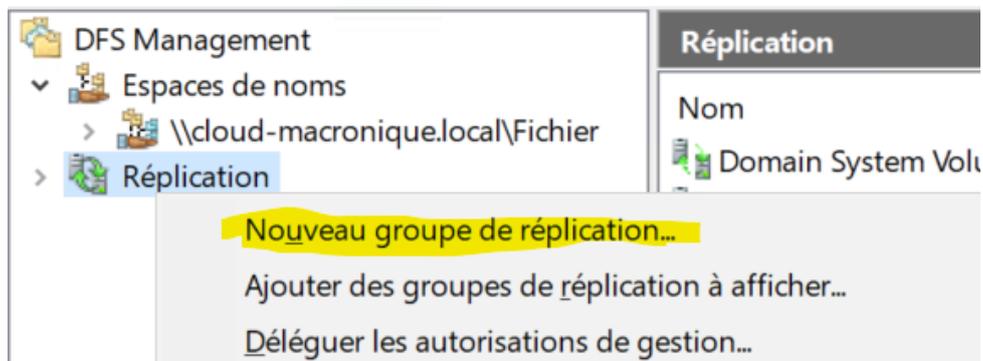
Le rôle DFSR étant sur le serveur de fichier, il faut maintenant le configurer.

VIII. Configuration du groupe de réplication DFSR

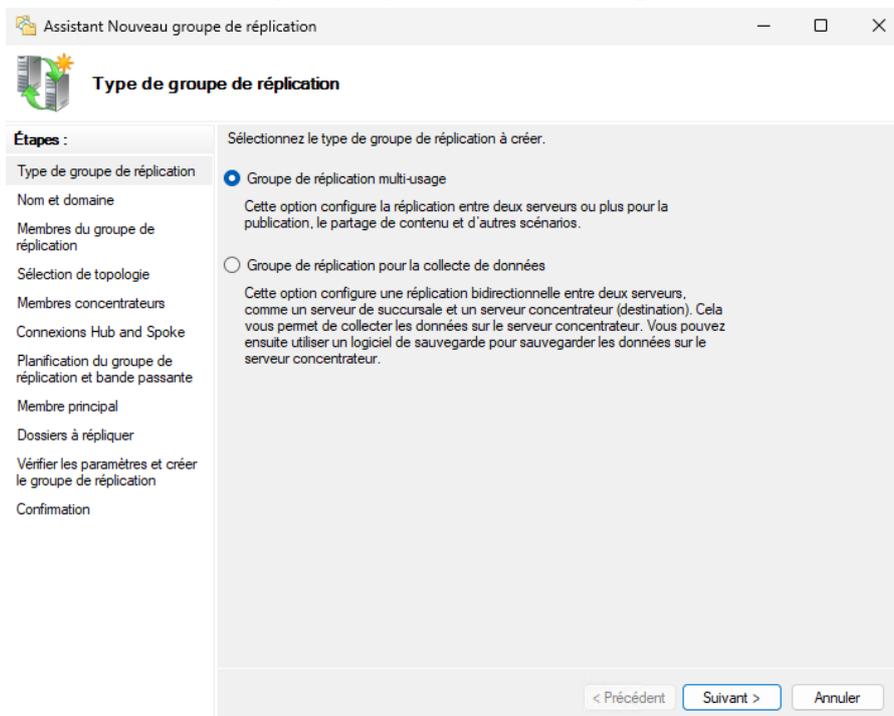
Avant la création d'un DFSR, Il faut créer auparavant les dossiers sur le srv-fichier2 pour la liaison. Dans le dossier C:\fichier création des dossiers :

- ByteMeUp
- Commun
- Cloud-Macronique
- Confidentiel
- GPO
- Pare-Fouine

Dans la console « **Gestion du système de fichiers distribués DFS** », sélectionner « **Réplication** » et ajouter un « **Nouveau groupe de réplication** ».



Lors de la sélection du type de groupe de réplication, pour assurer une haute disponibilité des données, sélection du "**Groupe de réplication multi-usage**".



Pour nommer le groupe de répliations, utilisation des dossiers créés précédemment :
Cloud-Macronique
Le domaine se met automatiquement grâce à la configuration du DFS.

The screenshot shows the 'Assistant Nouveau groupe de répliation' window at the 'Nom et domaine' step. The left sidebar lists the steps: 'Type de groupe de répliation', 'Nom et domaine', 'Membres du groupe de répliation', 'Sélection de topologie', 'Membres concentrateurs', 'Connexions Hub and Spoke', 'Planification du groupe de répliation et bande passante', 'Membre principal', 'Dossiers à répliquer', 'Vérifier les paramètres et créer le groupe de répliation', and 'Confirmation'. The main area contains the following fields and instructions:

- Étapes :** Entrez un nom et un domaine pour le groupe de répliation. Le nom du groupe de répliation doit être unique dans le domaine qui héberge le groupe de répliation.
- Nom du groupe de répliation :** Cloud-Macronique
- Description facultative du groupe de répliation :** (Empty text box)
- Domaine :** cloud-macronique.local (with a 'Parcourir...' button)

Navigation buttons at the bottom: '< Précédent', 'Suivant >', and 'Annuler'.

Lors de la sélection des serveurs, il faut choisir les serveurs sur lesquels les données seront sauvegardées ; dont **les deux serveurs de fichiers** en tant que membres de ce groupe.

The screenshot shows the 'Assistant Nouveau groupe de répliation' window at the 'Membres du groupe de répliation' step. The left sidebar highlights 'Membres du groupe de répliation'. The main area contains the following fields and instructions:

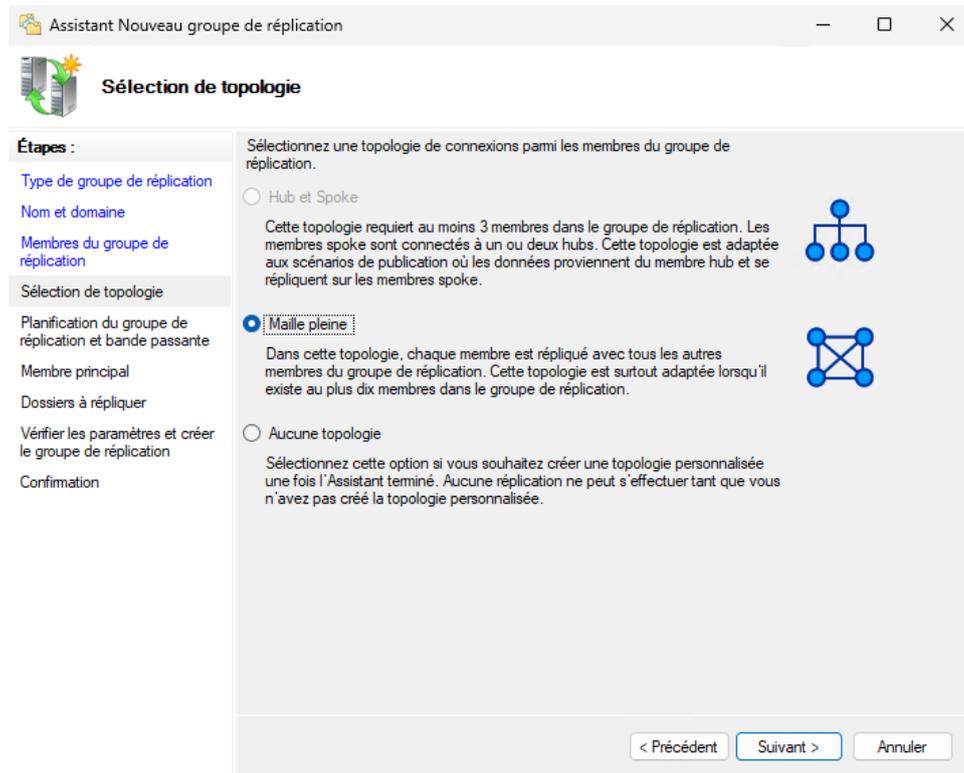
- Étapes :** Cliquez sur Ajouter, puis sélectionnez deux serveurs ou plus qui deviendront membres du groupe de répliation.
- Membres :**

Serveur	Domaine
SRV-FICHIERS1	cloud-macronique.local
SRV-FICHIERS2	cloud-macronique.local

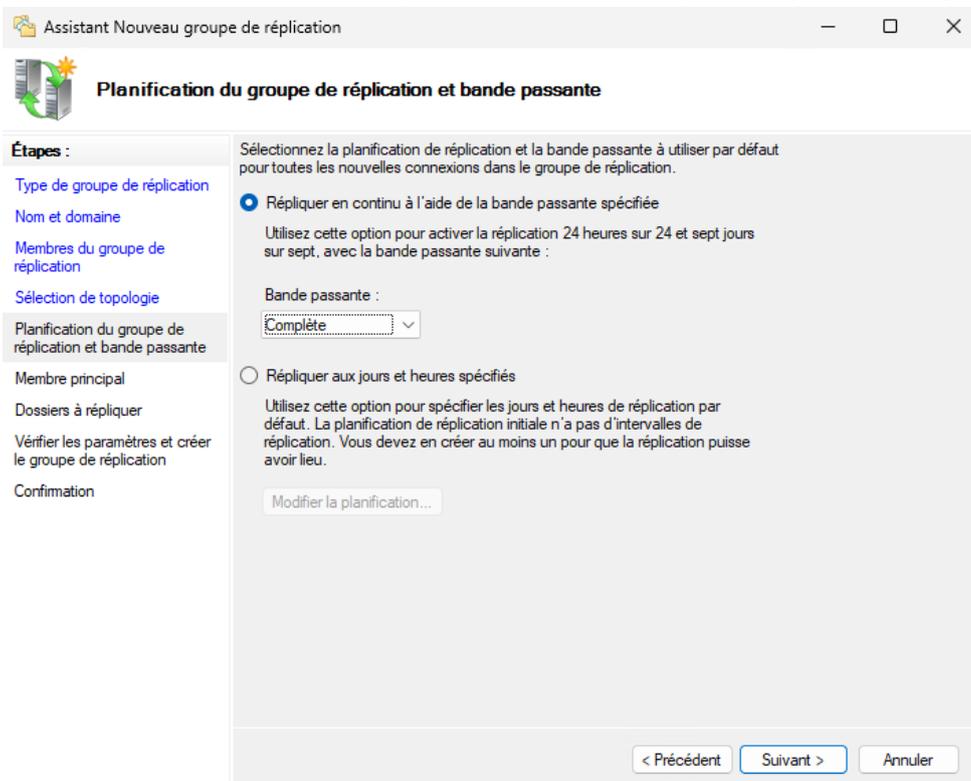
Buttons below the table: 'Ajouter...', 'Supprimer'.

Navigation buttons at the bottom: '< Précédent', 'Suivant >', and 'Annuler'.

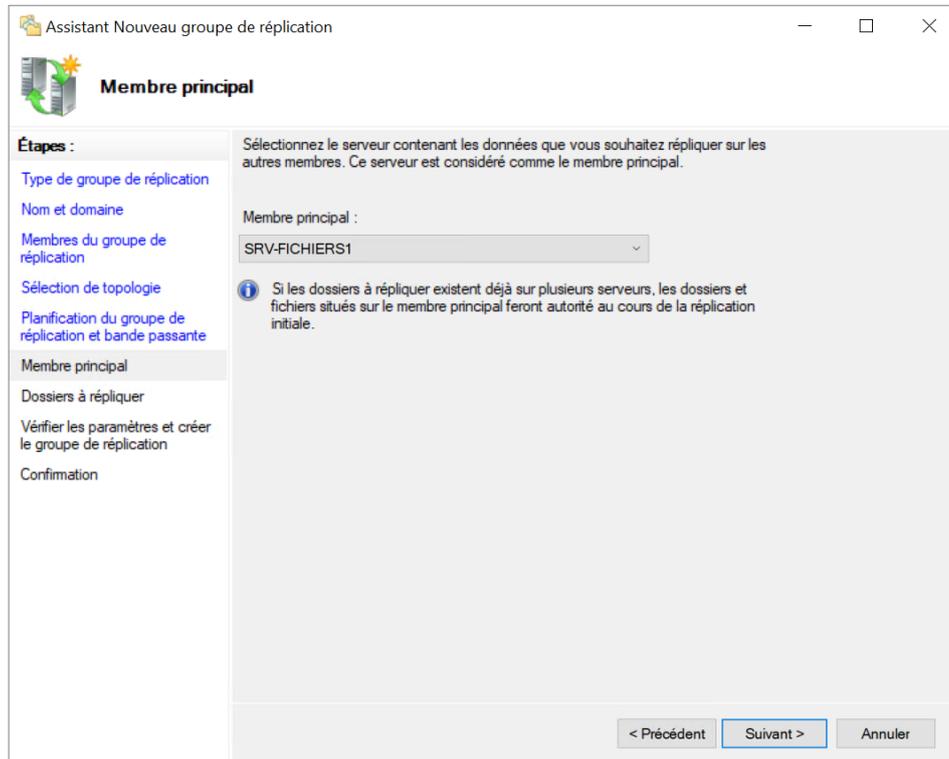
Lors de la sélection du type de topologie. Sélection de la topologie "**Maille pleine**" car avec cette topologie, **la réplication sera bidirectionnelle entre les 2 serveurs.**



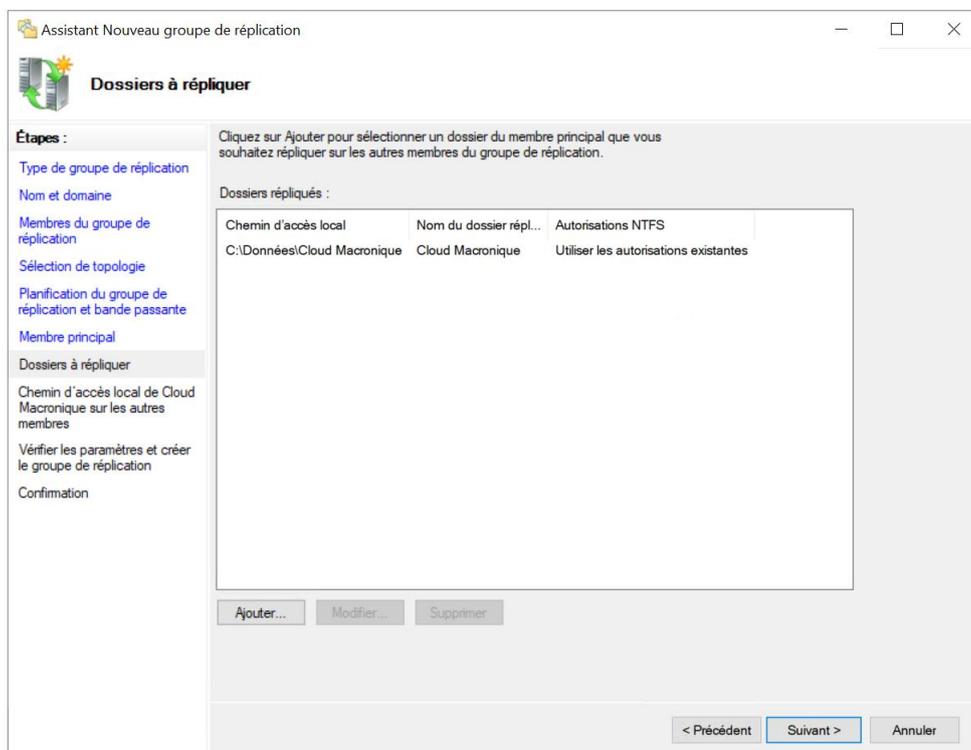
La réplication sera effectuée en continu pour répartir la charge entre les deux serveurs de fichier avec une limitation d'une bande passante de 10 Mo/s pour ne pas surcharger celle-ci.



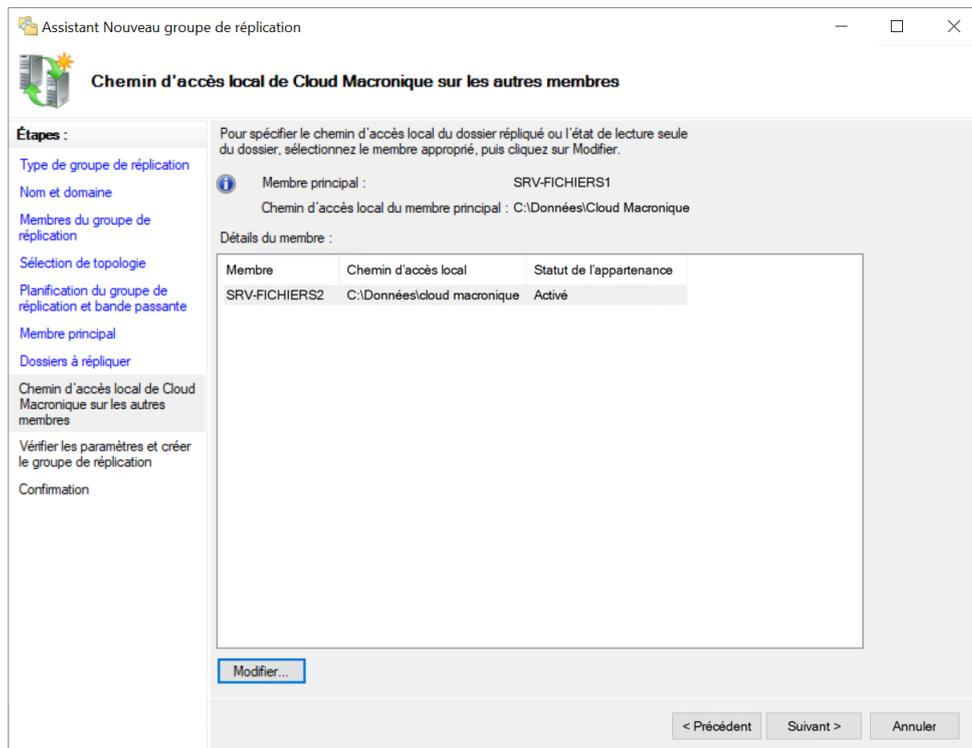
Sélection du SRV-FICHIER1 en tant que membre principal car le serveur contient déjà les données à répliquer.



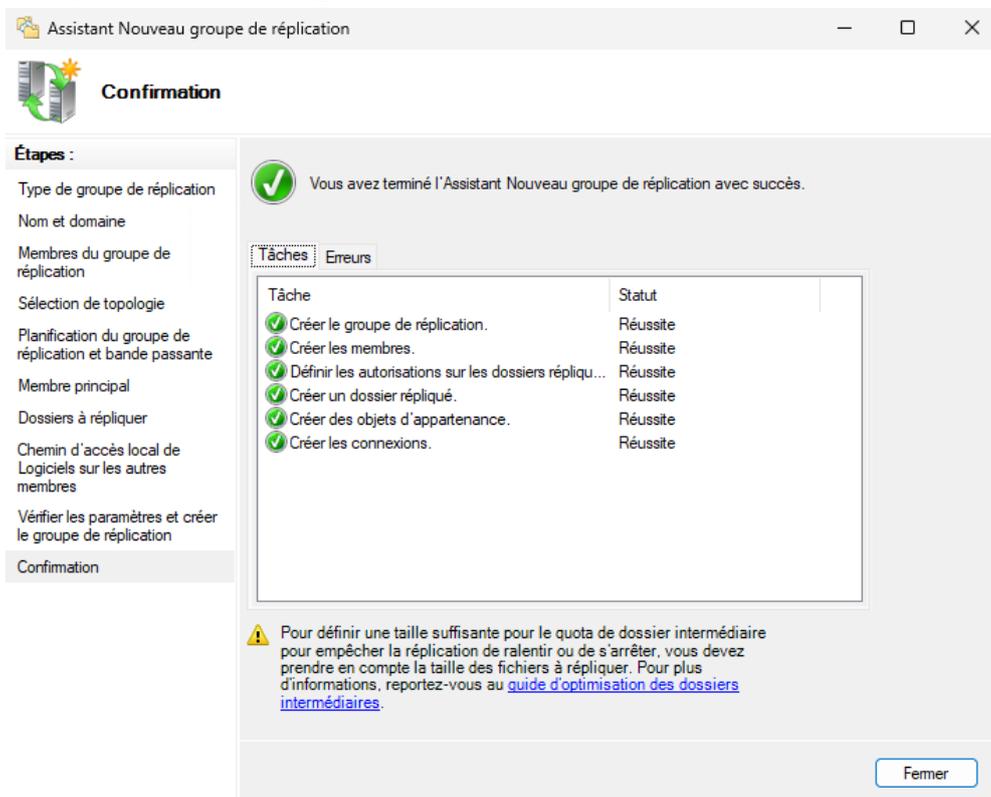
Sélection du répertoire à répliquer sur le SRV-FIHCIER1, qui se trouve dans : « C:\fichier\\Cloud-Macronique ».



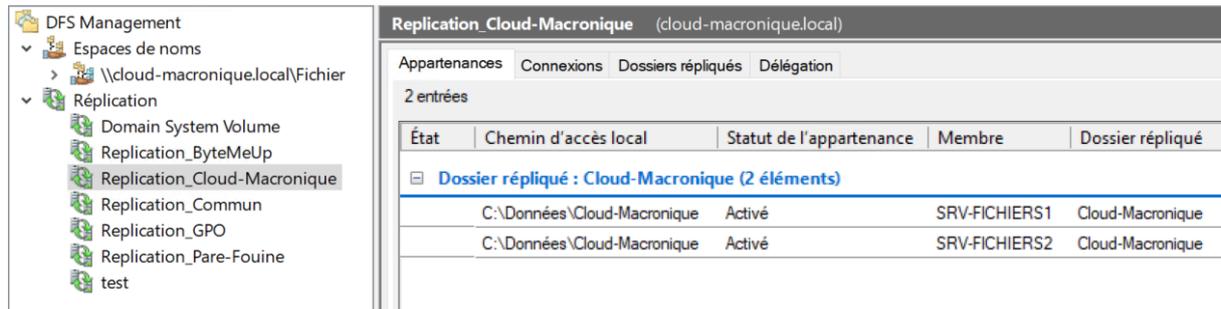
Ajout du répertoire du second serveur membre du groupe. Activation de la synchronisation et sélection du répertoire qui se trouve dans : C:\fichier\cloud-macronique.



La configuration est terminée, lancement de la création du DFSR. Pour bonne confirmation de la création, attente du message de validation suivant.



Une fois fini, les groupes de réplication DFSR étaient correctement visibles dans la console DFS :



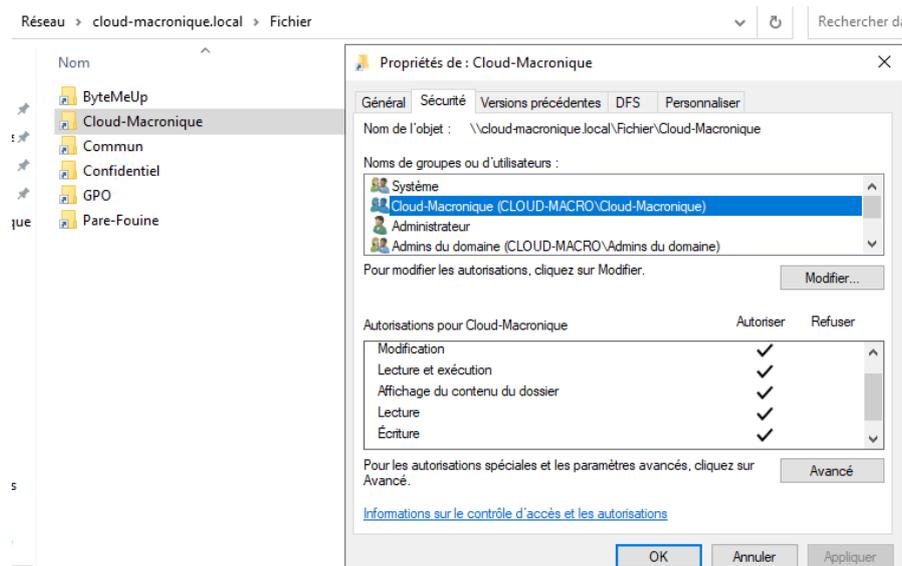
IX. Gestion des droits sur le dossier DFS :

Pour la gestion des droits DFS, il faut dans un premier temps autoriser les utilisateurs spécifiques à accéder au dossier dans l'espace de nom en lecture / écriture.

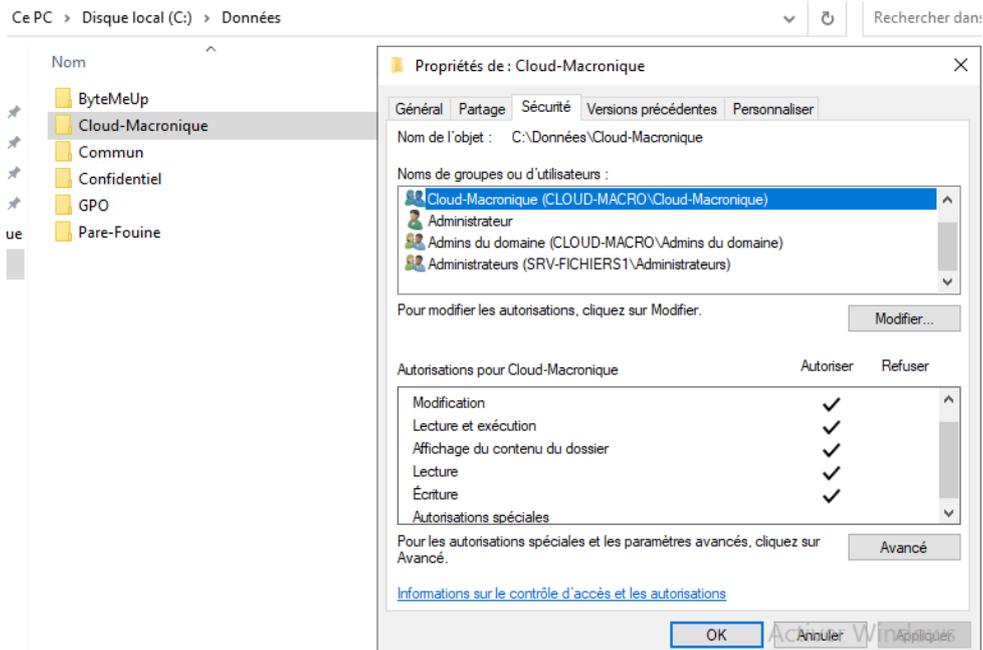
Pour cette configuration, il a été utilisé les groupes de sécurité créés lors de la documentation AD, DHCP, DNS.

Dossier / Groupe :

- ByteMeUp : ByteMeUP
- Cloud-Macronique : Cloud-Macronique
- Commun : Utilisateurs du domaine
- Confidentiel : Louis, Tilio et Mathys
- GPO : Utilisateurs du domaine
- Pare-Fouine : Pare-Fouine



Dans un second temps, il faut faire le même chose sur les dossiers dans les SRV-FICHIERS1 et SRV-FICHIERS2 liés au dossier dans l'espace de nom.



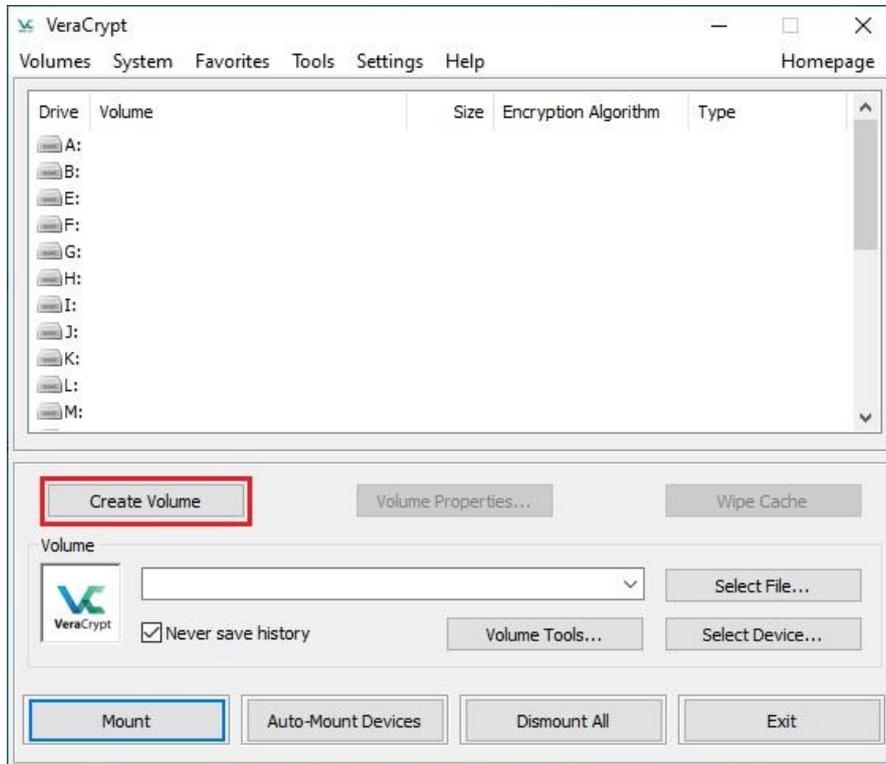
X. Test du DFSR :

- Prise en main d'un poste connecté sur le réseau
- Connexion avec utilisateur : Tilio
- L'utilisateur possède bien les droits pour créer / lire dans commun, Cloud-Macronique et confidentiel sans voir les autres.
- Création d'un fichier dans commun
- Eteindre le SRV-FICHIERS1
- Le dossier \\cloud-macronique.local\fichier\commun est accessible et possède le fichier créé par utilisateur Tilio.

XI. Créer un conteneur VeraCrypt

Installation VeraCrypt sur les 2 serveurs de fichiers.

Une fois VeraCrypt installé, création du nouveau volume sécurisé.



Lors de la création du volume VeraCrypt, sélectionner le paramètre « créer un conteneur VeraCrypt de fichiers cryptés ».



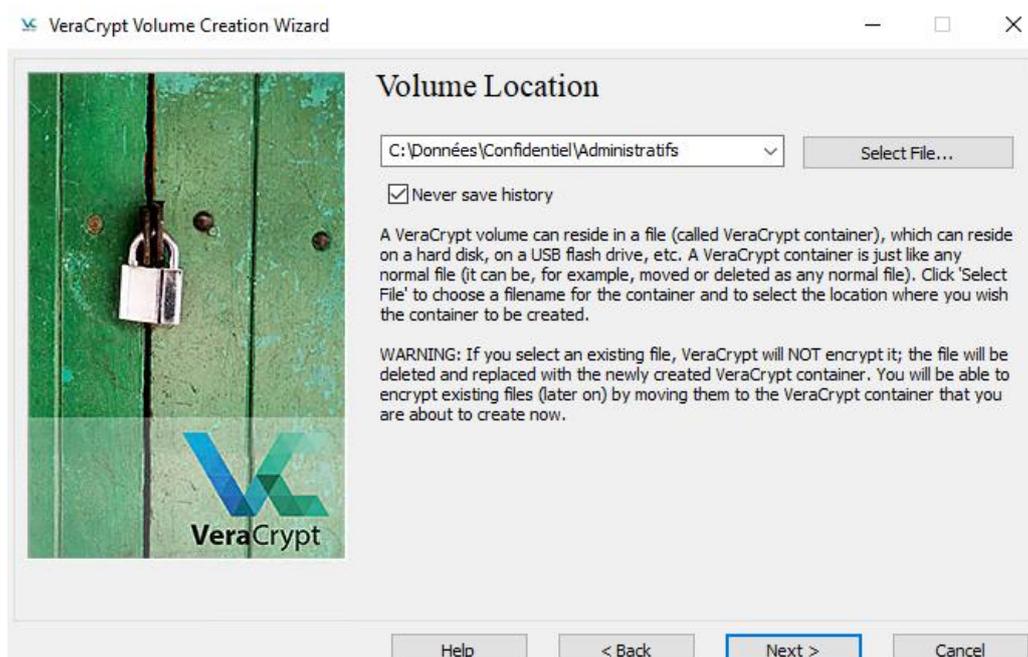
Création d'un volume VeraCrypt standard ou caché. Sélection de la première option « créé un volume VeraCrypt standard » car précédemment a été activé l'ABE (l'énumération basée sur l'accès).



Sélection de l'emplacement de création du volume VeraCrypt.

Saisir le nom du fichier dans le dossier souhaité en .hc.

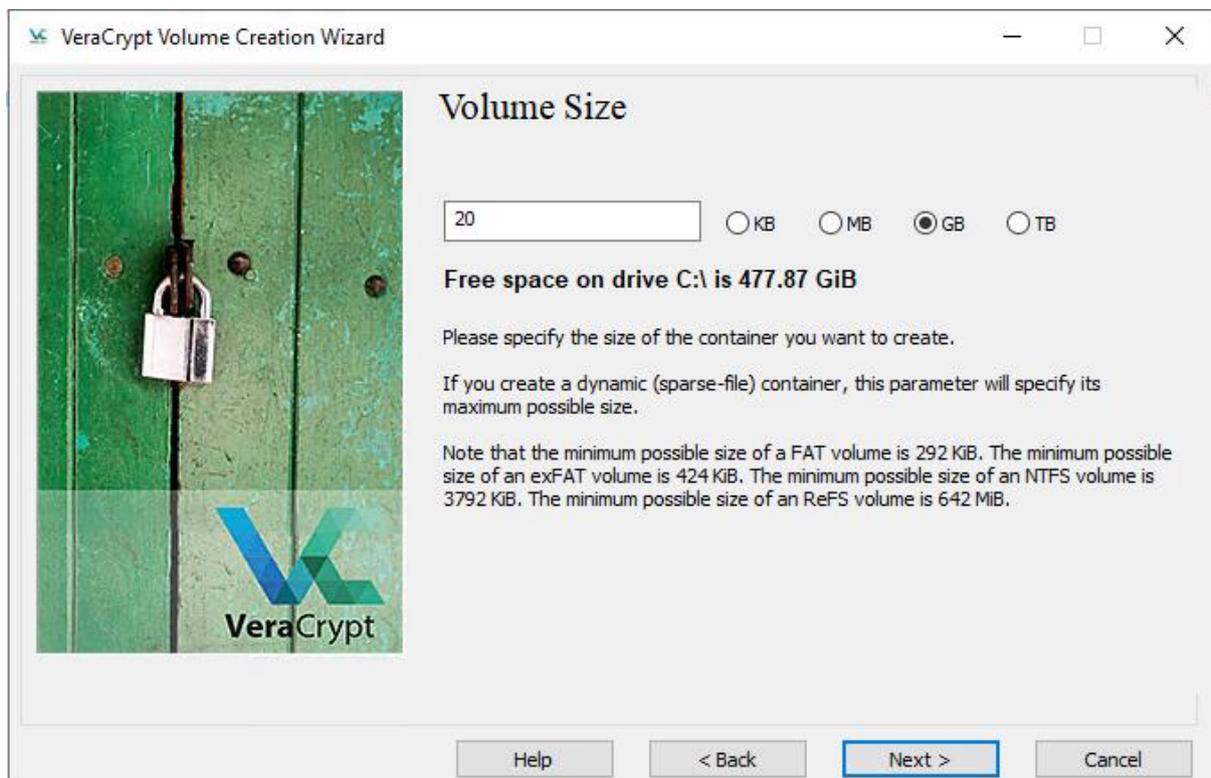
Emplacement du fichier : \\SRV-FICHIERS1\Données\Confidentiel



Lors de la sélection de l'algorithme de chiffrement et de l'algorithme de hachage pour le volume, utilisation des paramètres par défaut.



Indication de la taille du conteneur VeraCrypt à 20GO.



Sélection d'un mot de passe fort pour le volume.

Volume Password

Password:
Confirm:

Use keyfiles Keyfiles...
 Display password
 Use PIM

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

Help < Back **Next >** Cancel

Volume Format

Options
Filesystem: FAT Cluster: Default Quick Format
 Dynamic

Random Pool: **//...+**+,./.*-/+.,-+.,-,...
Header Key:
Master Key:

Done | Speed | Left | Abort

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements
[Green progress bar]

Help < Back **Format** Cancel

Déplacement de la souris jusqu'à ce que l'indicateur de caractère aléatoire devienne vert. Cela permet à VeraCrypt de créer des clés de chiffrement de manière unique pour chacun. Formater pour créer le volume Administratif VeraCrypt.

Précision : Le dossier sera est stocker sur le serveur dans le dossier [\\SRV-FICHIERS1\Données\Confidentiel](#), il sera visible dans le DFS mais ne sera pas répliqué sur le [\\SRV-FICHIERS2](#).