DOMOTech

CONFIGURATION

Replication AD DNS DHCP

PROCEDURE

Date de création : 04/01/2023
Version : 2.0
Pour validation : DSI
A destination : DSI
Mode de diffusion : SharePoint
Nombre de pages : 25

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document
Dylan Chau	2.0	Mise à jour

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau	04/01/2023	DSI	04/01/2023
Date d'application : 04/01/2023			

Sommaire

Prérequis

- 2 machines virtuelles
- ISO Windows Server 2019
- DAT DOMOTech

Présentation

I. Active Directory

Active Directory (AD) est un annuaire LDAP (Lightweight Directory Access Protocol) développé par Microsoft. Il est spécifique aux systèmes d'exploitation Windows. AD permet de stocker différents types d'objets tels que des utilisateurs, des ordinateurs, des groupes, etc.

Les objectifs essentiels d'Active Directory sont l'identification et l'authentification des utilisateurs et des ressources.

La création d'un domaine dans Active Directory permet d'avoir une base centralisée d'utilisateurs, de groupes et d'ordinateurs, ce qui facilite l'administration et la gestion de la sécurité.

Lorsqu'un domaine est créé, la machine sur laquelle il est créé devient un contrôleur de domaine. Le contrôleur de domaine est au cœur des requêtes du système d'information (SI). Il est recommandé d'avoir au moins deux contrôleurs de domaine pour assurer la disponibilité et la continuité du service. Si l'un des contrôleurs de domaine est corrompu, cela peut entraîner des problèmes.

II. Dynamic Host Configuration Protocol

Le **DHCP** (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer automatiquement les adresses IP et les autres paramètres de configuration réseau aux dispositifs connectés à un réseau. Le processus DORA est utilisé pour décrire l'échange entre le client et le serveur.

III. Domain Name System

le serveur **DNS** (Domain Name System) joue un rôle essentiel en fournissant la résolution des noms de domaine dans une infrastructure réseau. Il permet la résolution des noms en IP et inversement.

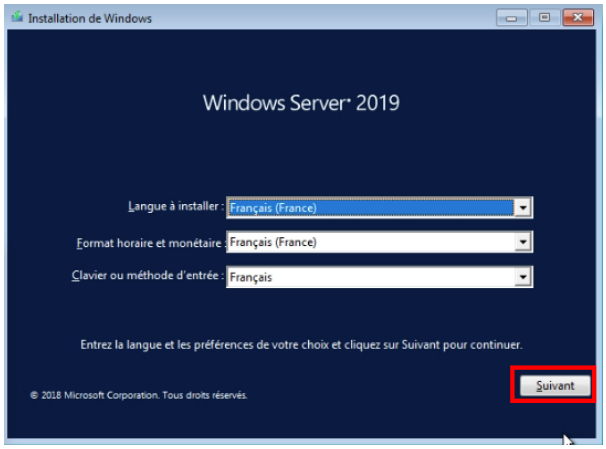
Réplication

L'objectif de la réplication est de permettre :

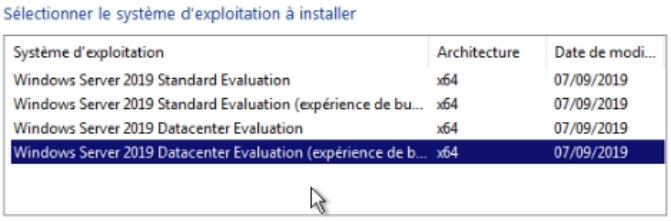
- Haute disponibilité
- Tolérance aux pannes
- Equilibrage des charges
- Redondance des données

I. Installation de Windows Server 2019

- Choisir la langue puis cliquer sur « Suivant ».



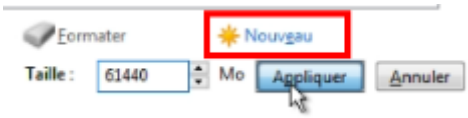
- Choisir l'édition « Datacenter Evaluation expérience de bureau » comme défini dans le DAT.



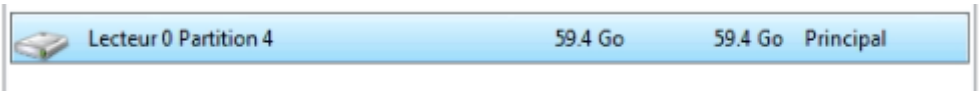
- Accepter les CGU

- Sélectionner « Personnalisé ».

- Créer un nouveau disque.



- Lancer l'installation sur le lecteur principal.

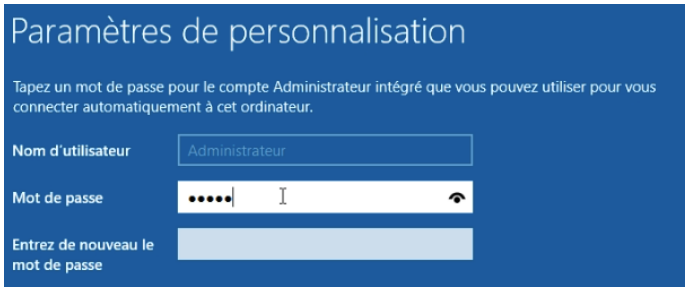


- Finir l'installation.

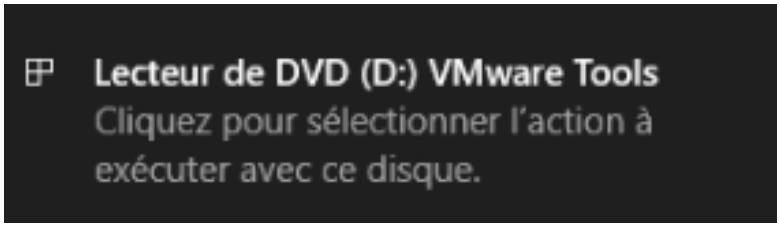
- Réitérer l'opération sur la seconde machine

II. Configuration de base

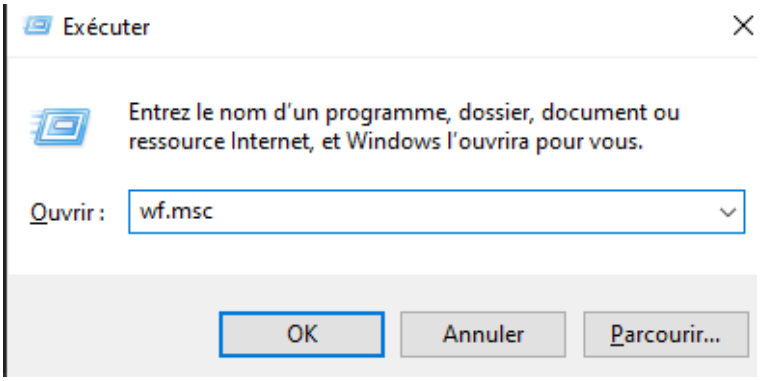
- Définir le mot de passe du compte Administrateur intégré.



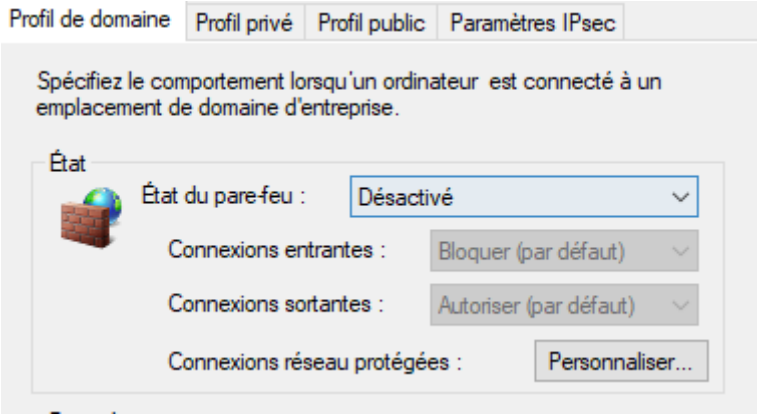
- Installer les drivers VMWare Tools (Pour l'affichage notamment).



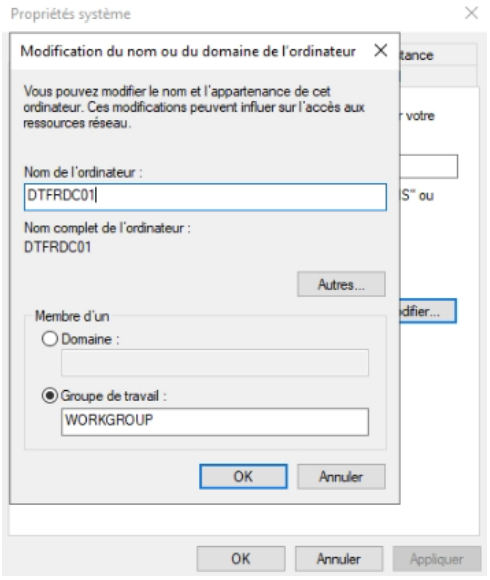
- Faire « Windows + R » puis « wf.msc ».



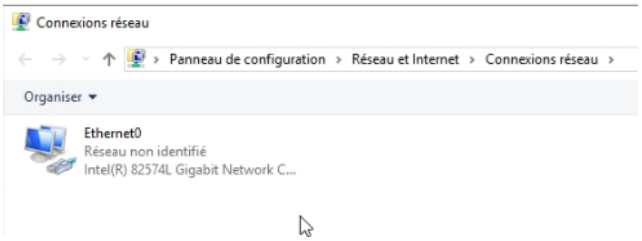
- Désactiver le pare-feu Windows Defender (géré par PFSense). Il faut le désactiver car il pourrait bloquer des flux entrants et sortants.



- Dans les « Propriétés Système », renommer les machines à partir du DAT

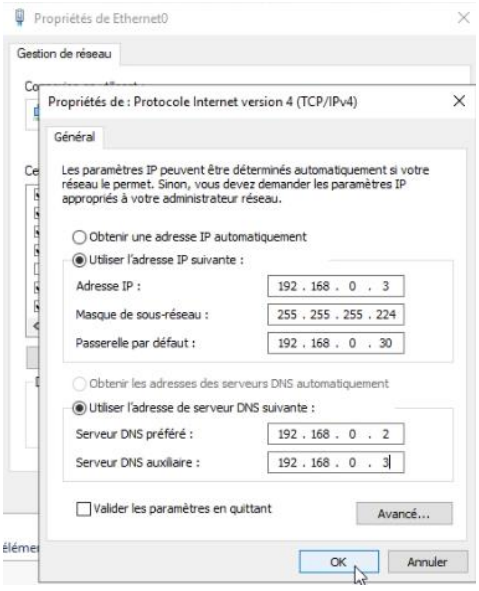


- Faire « Windows + R » puis « ncpa.cpl » pour accéder aux cartes réseaux.



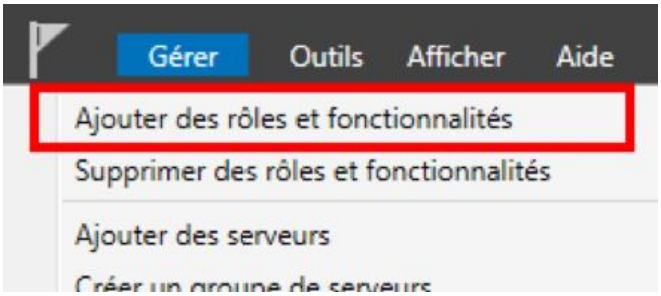
- Faire un clic droit puis « Propriétés ».
- Désactiver TCP/Ipv6

- Ouvrer Protocole Internet version 4 (TCP/IPv4) et configurer la carte réseau de chaque machine en se basant sur le DAT.

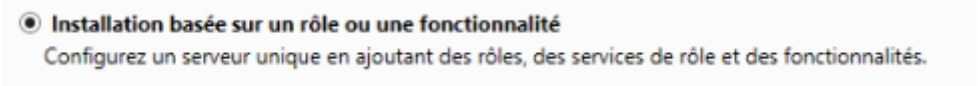


III. Installation des services AD DS, DNS et DHCP

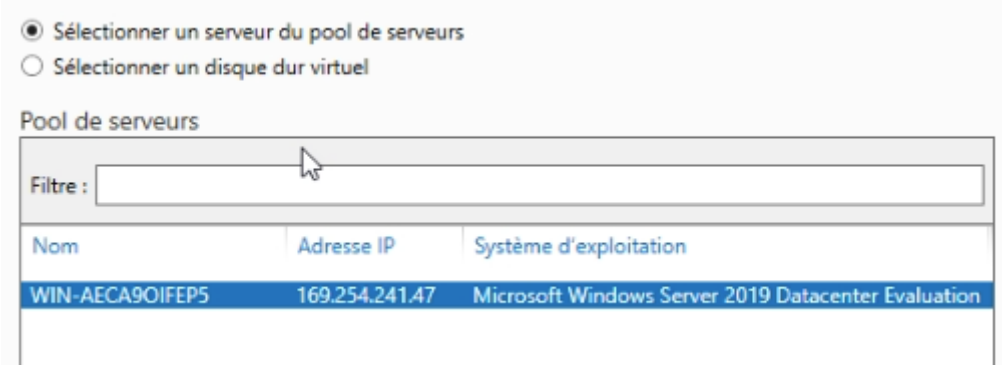
- Cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



- Sur « Avant de commencer », cliquer sur « Suivant ».
- Sur « Type d'installation », laisser par défaut. Cliquer sur « Suivant ».

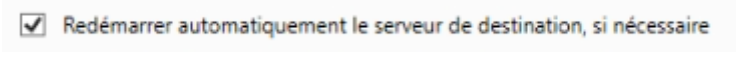


- Sur « Sélection du serveur », choisir « Sélectionner un serveur du pool de serveurs » et choisir notre serveur. Cliquer sur « Suivant ».

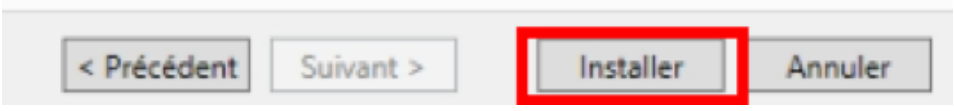


- Sur « Rôles de serveurs », sélectionner AD DS, DNS et DHCP.

- Sur « Fonctionnalités », ne rien sélectionner. A l'heure actuelle nous n'en avons pas besoin.
- Les autres onglets apportent des détails sur les rôles.
- A la page « Confirmation », cocher la ligne pour redémarrer.



- Puis cliquer sur « Installer ».



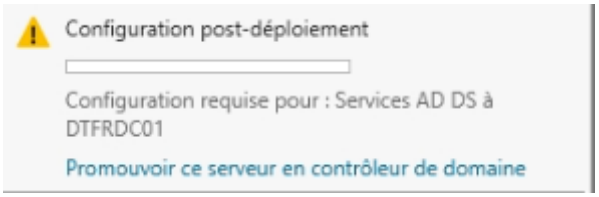
- Le serveur va redémarrer.

IV. Réplication AD

1. Configuration du premier contrôleur de domaine

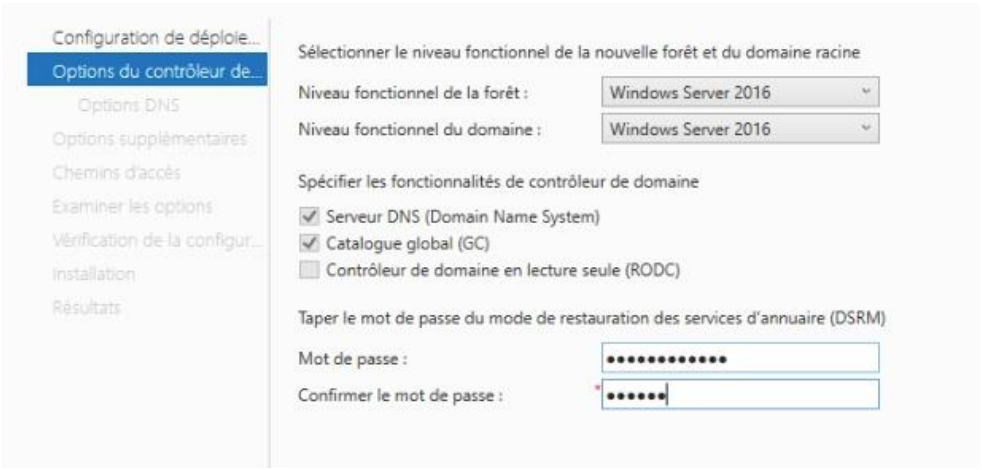
Une fois le serveur redémarré, il va falloir promouvoir le serveur en contrôleur de domaine pour le fonctionnement de l'Active Directory :

- Cliquer sur le drapeau avec le « Warning » puis sur « Promouvoir ce serveur en contrôleur de domaine ».

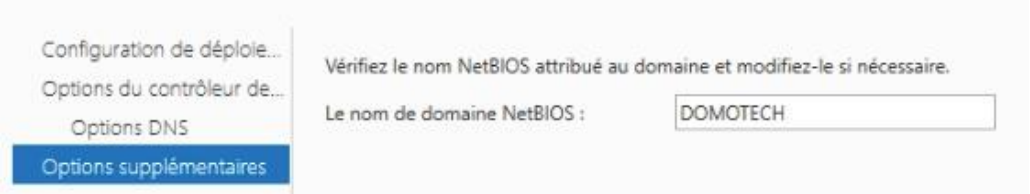


- Nous allons maintenant créer la fôret DOMOTECH. Le nom de domaine racine sera « domotech.priv ».

- Laisser le niveau fonctionnel par défaut et définir un mot de passe DSRM.

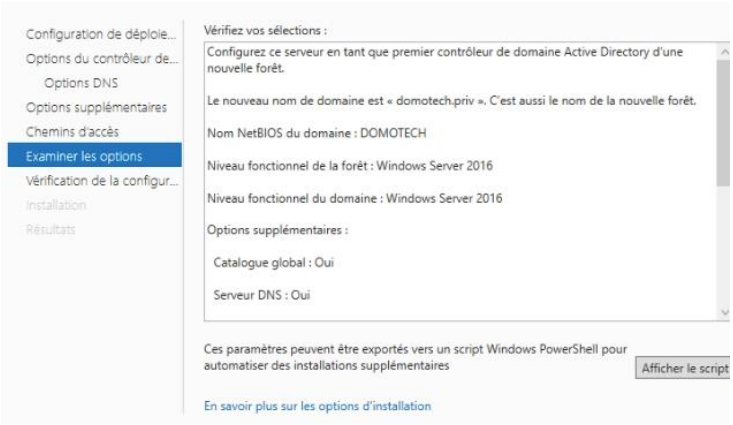


- Sur « Option DNS », cliquer sur « Suivant ».
- Le nom NetBIOS du domaine apparaît.

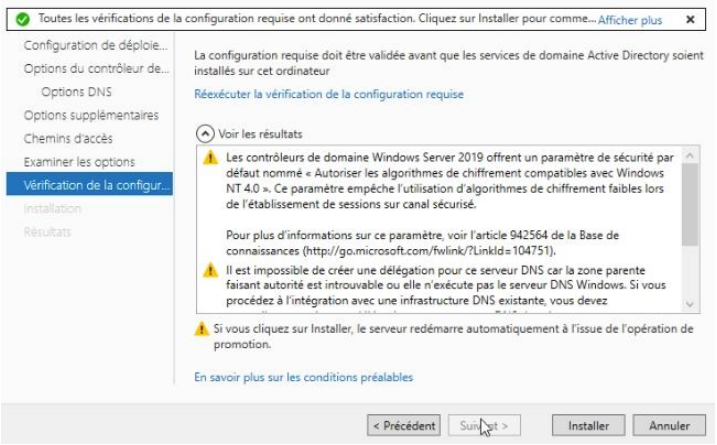


- L’emplacement des fichiers de configuration de l’AD sont affichés.

- Un récapitulatif est affiché.



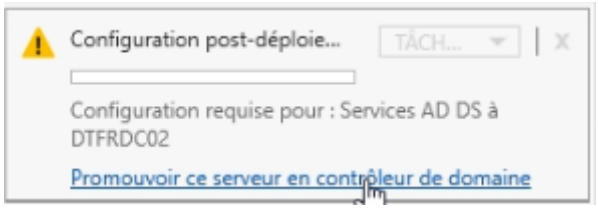
- Démarrer l’installation.



- Une fois terminée, le premier contrôleur de domaine est prêt.

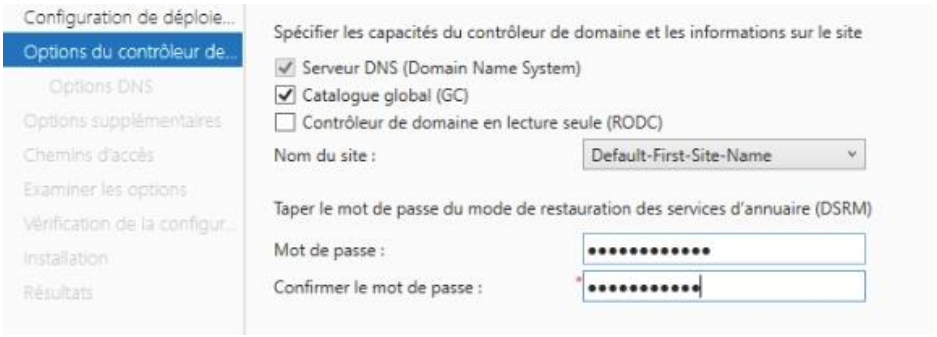
2. Configuration du second contrôleur de domaine

- Cliquer sur le drapeau avec le « Warning » puis sur « Promouvoir ce serveur en contrôleur de domaine ».



- Mettre les paramètres suivants pour ajouter le second contrôleur au domaine. Modifier les credentials avec un compte administrateur du domaine.

- Définir un mot de passe de restauration DSRM.



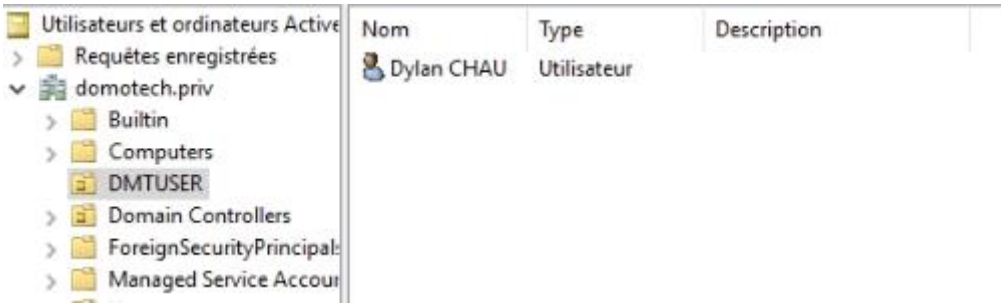
- Sur « Option DNS », cliquer sur « Suivant ».
- Dans « Options supplémentaires », répliquer depuis le premier contrôleur de domaine.

- Finir l'installation comme pour le premier contrôleur de domaine. La réplication est terminée.

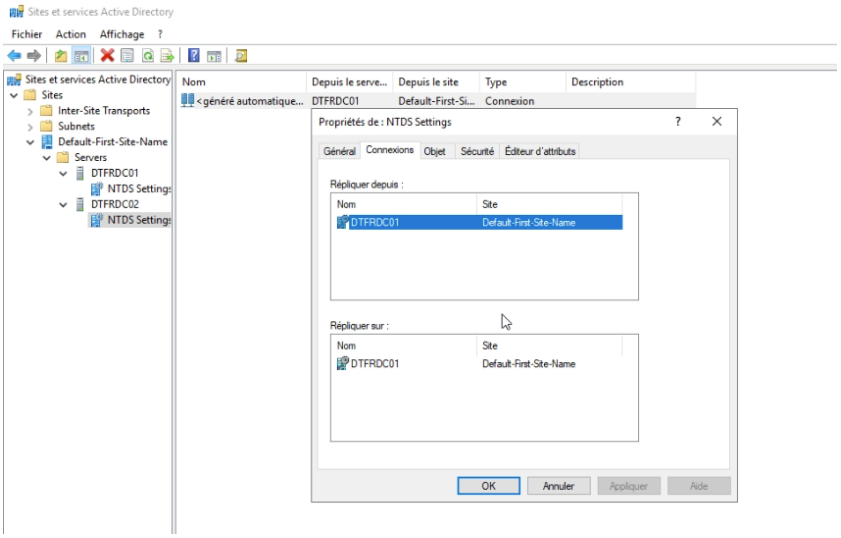
3. Test de réplication AD

Il y a plusieurs méthodes pour vérifier le bon fonctionnement de la réplication AD :

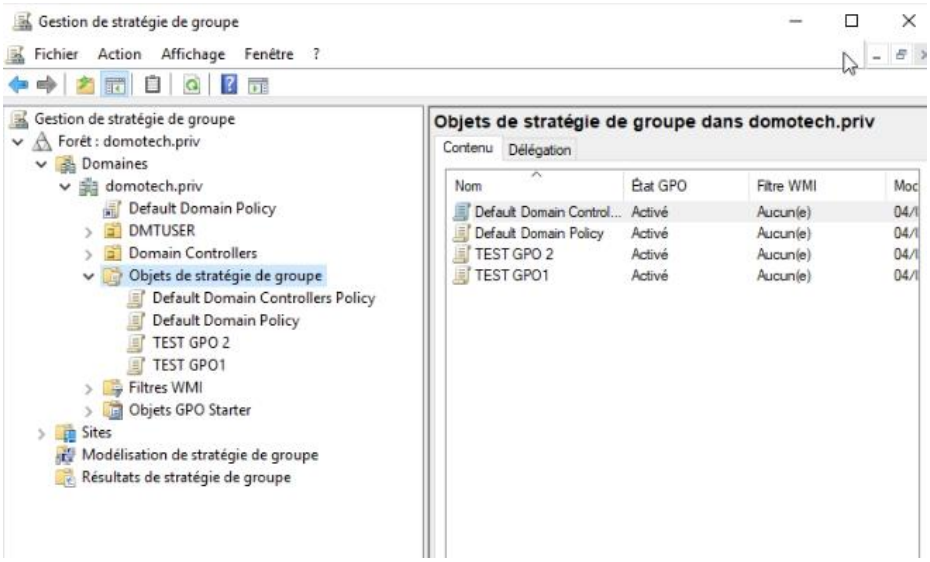
- Créer une unité d'organisation et un utilisateur dedans pour vérifier la réplication.



- Vérifier dans « Sites et services AD », les connexions des 2 contrôleurs.



- Dans « Gestion des stratégies de groupes », créer des GPO et vérifier leur réplication.

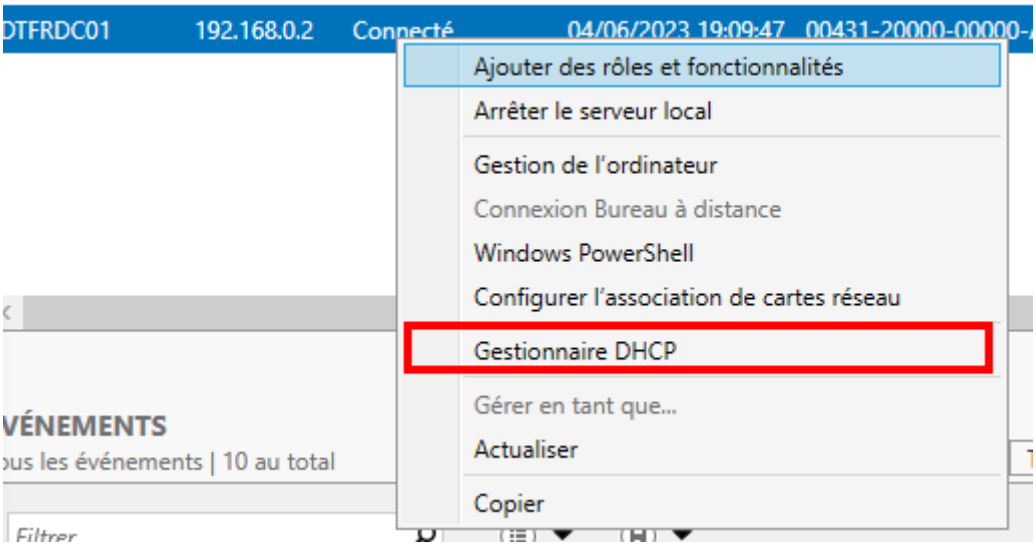


V. Réplication DHCP

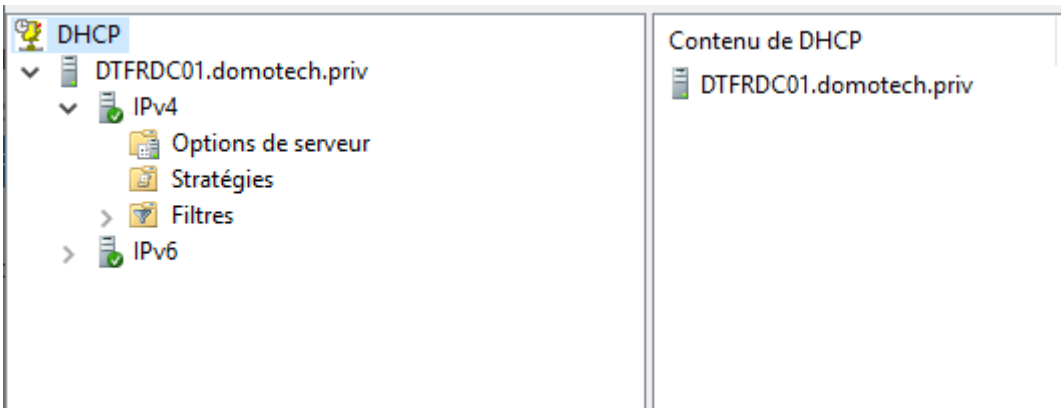
1. Configuration

- Terminer la configuration DHCP après redémarrage du serveur. Cette étape va permettre de créer deux groupes de sécurité dans l'AD pour permettre la délégation quant à la gestion du serveur DHCP et déclarer notre serveur DHCP au sein de l'AD.
- Cliquer ensuite sur « DHCP ».

- Lancer ensuite le gestionnaire DHCP.

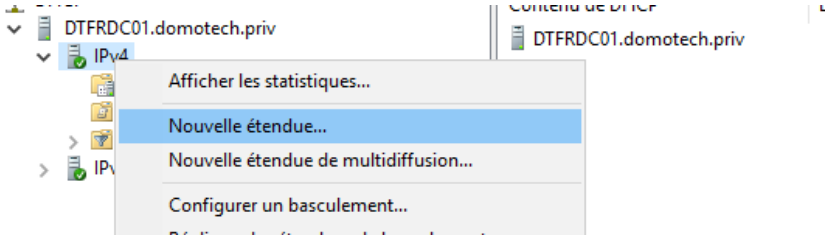


- Le gestionnaire s'affiche ensuite.

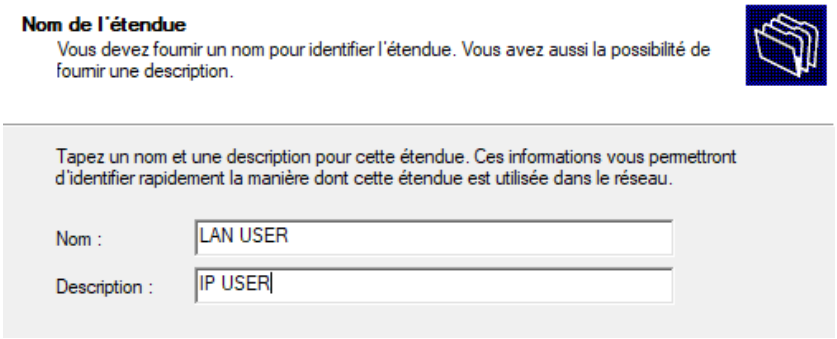


2. Création d'une étendue

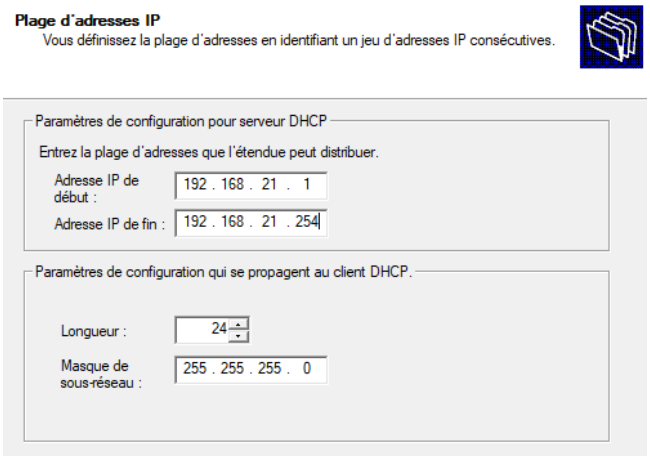
- Faire clic droit sur « IPv4 » puis « Nouvelle étendue »



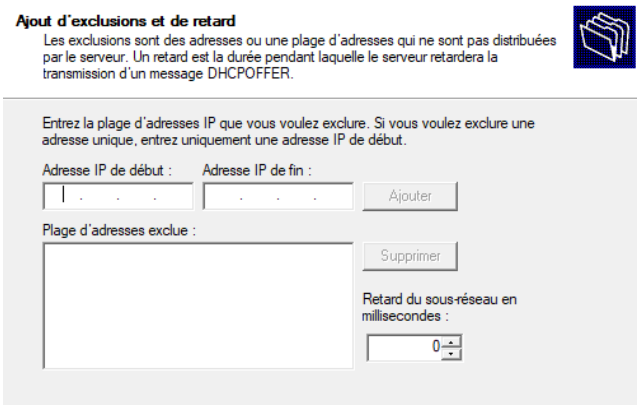
- Donner un nom et une description à l'étendue.



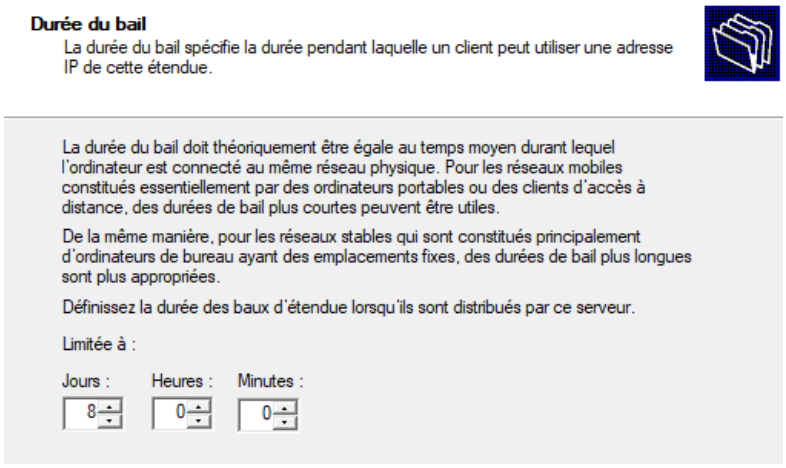
- Paramétrer les IP en fonction du DAT.



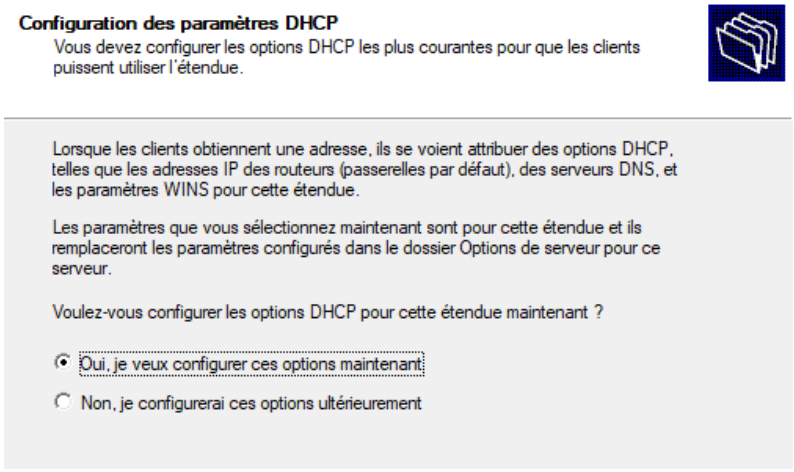
- Il est possible d'exclure des plages adresses. Sur le LAN SERVEUR, il n'y a pas d'exclusions mais des réservations pour les serveurs.



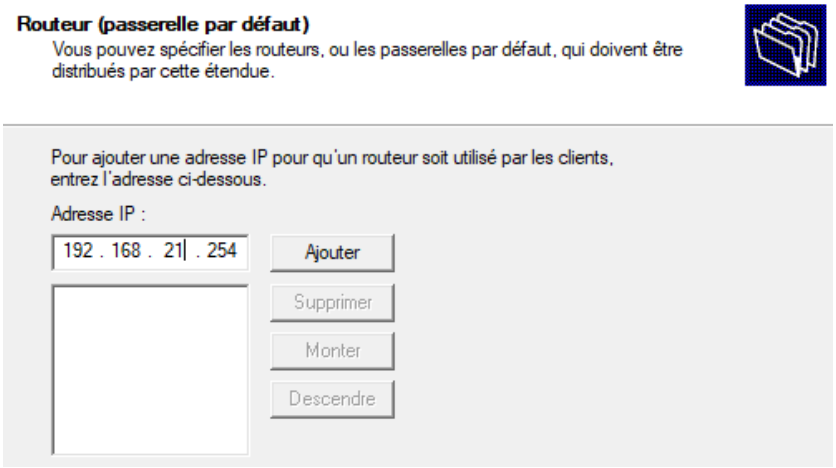
- Laisser la durée du bail par défaut.



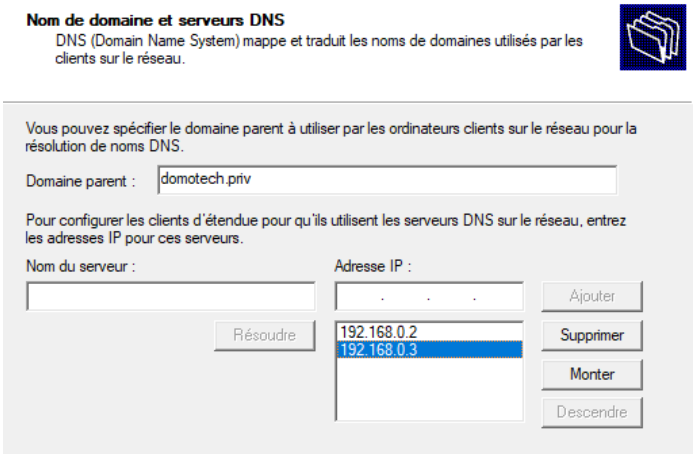
- Configurer les options DHCP.



- Mettre la passerelle par défaut en fonction du DAT. C'est le point de sortie du LAN.



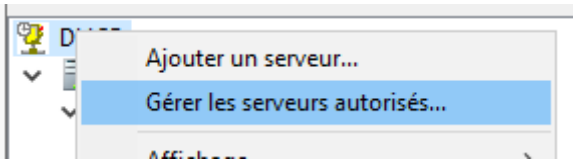
- Les paramètres DNS sont déjà bons par défaut. Il est possible d'en ajouter.



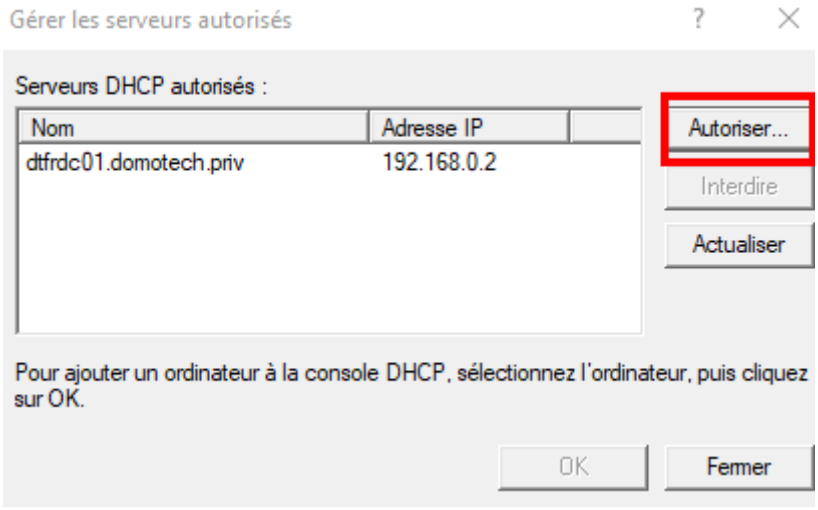
- Ne rien mettre pour les serveurs WINS.
- Activer l'étendue. Il faudra configurer les étendues en fonction du DAT.

3. Configuration du basculement (réplication)

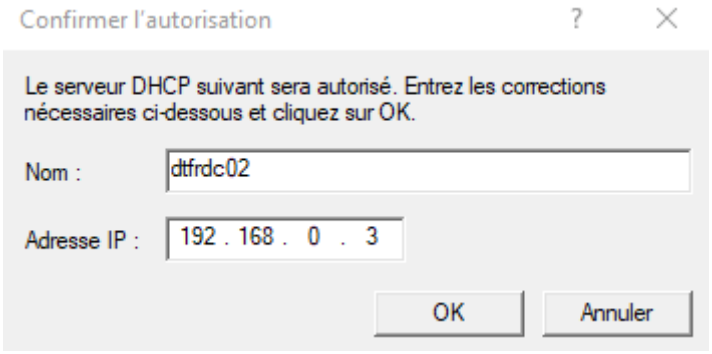
- Sur « DHCP », faire clic droit puis cliquer sur « Gérer les serveurs autorisés ».



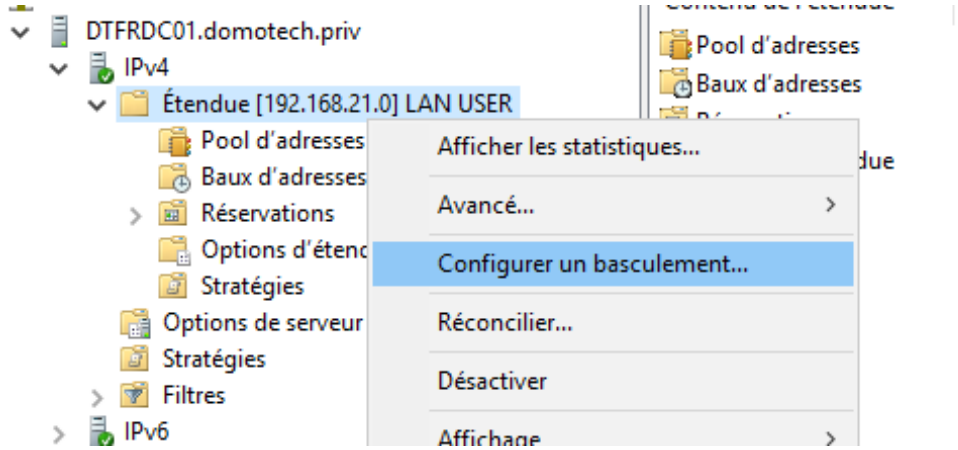
- Cliquer sur « Autoriser ».



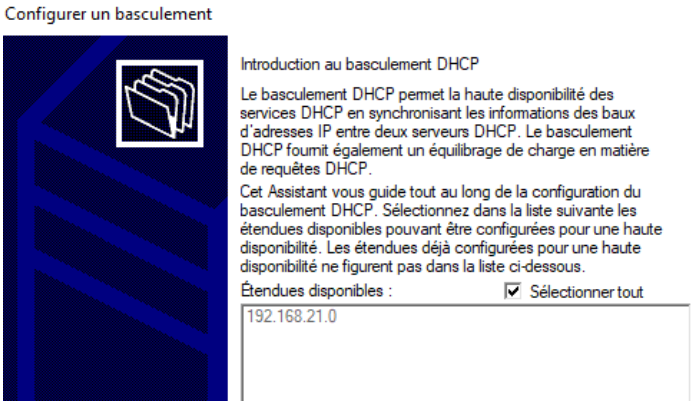
- Ajouter le DC02.



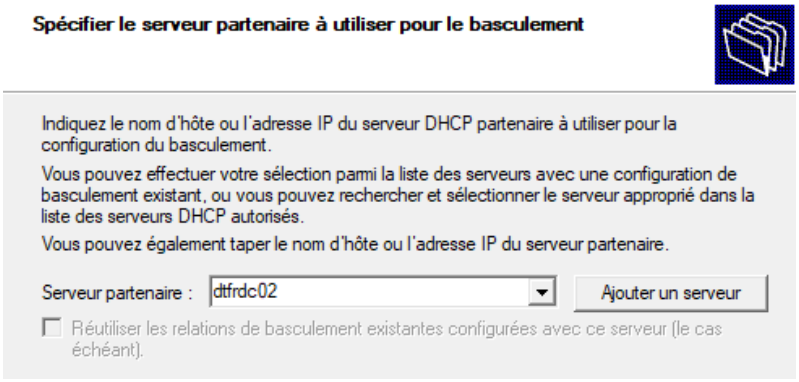
- Sur une étendue, faire clic droit puis « Configurer un basculement ».



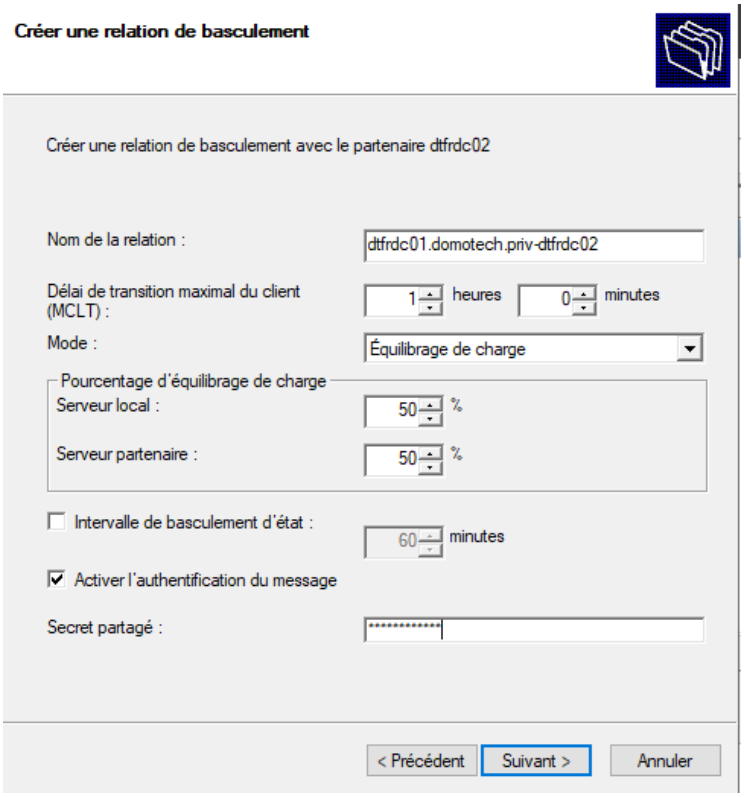
- Par défaut, l'ensemble des étendues sont basculées.



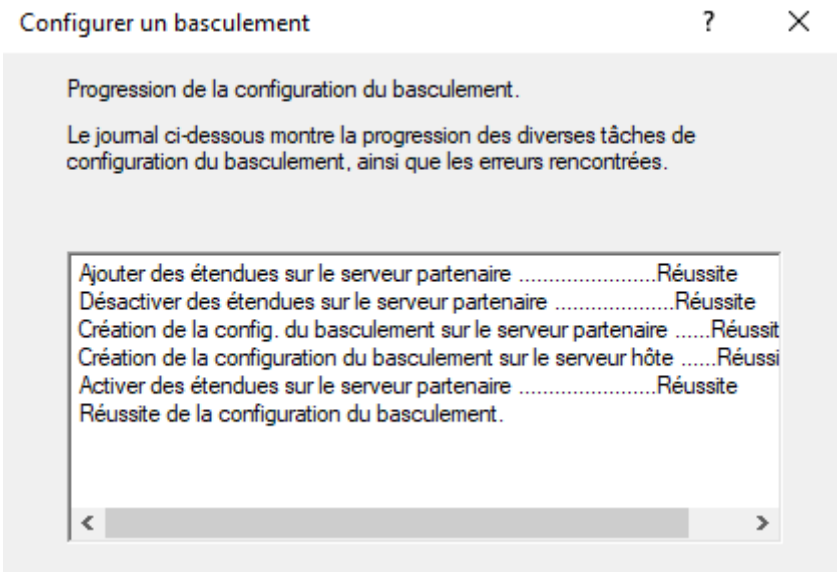
- Ajouter le second serveur en partenaire.



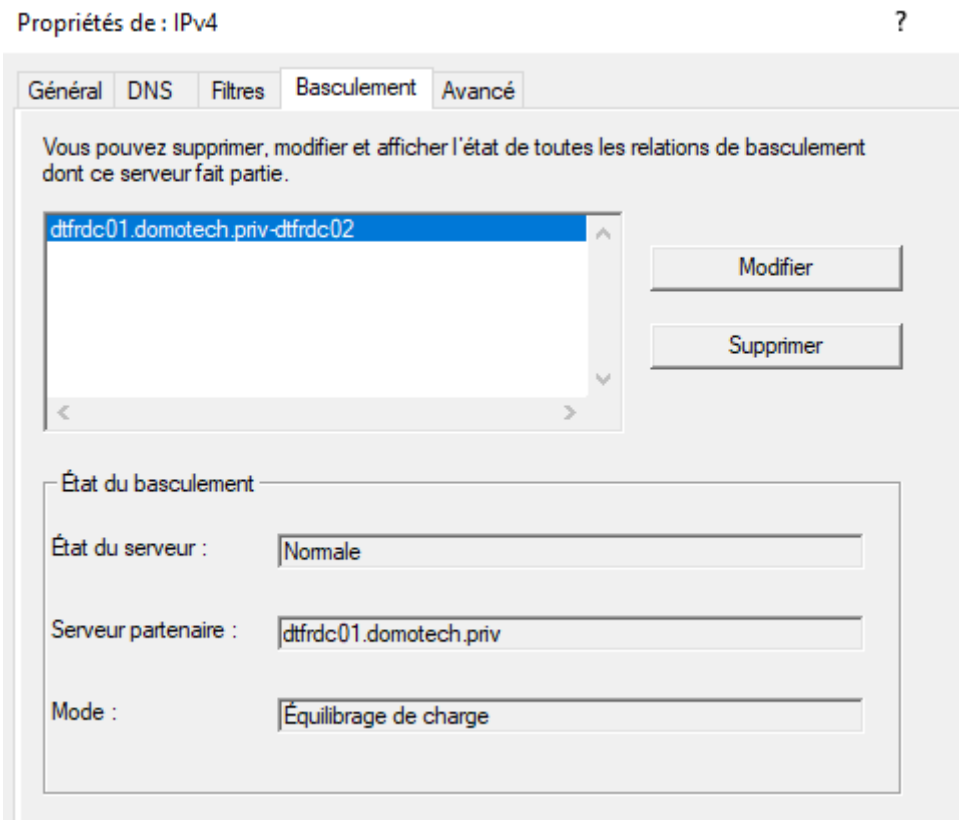
- Choisir les paramètres de basculement. Plusieurs paramètres sont disponibles. Définir un secret partagé.



- Le basculement est terminé.



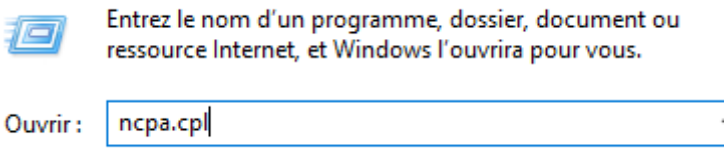
- La relation apparaît bien sur le second contrôleur de domaine.



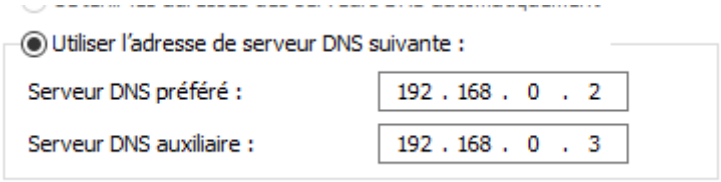
VI. Réplication DNS

Une fois le rôle installé sur les 2 contrôleurs de domaines, il faut réaliser les manipulations suivantes :

- Faire Windows + R et « ncpa.cpl ».



- Vérifier que les serveurs DNS sont bien configurés dans la carte réseau.



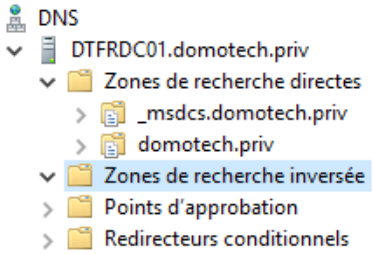
La réplication DNS s'appuie sur le mécanisme de réplication d'Active Directory pour transmettre les modifications entre les contrôleurs de domaine.

Cela signifie que les zones DNS sont intégrées à la réplication d'Active Directory. Lorsqu'une modification est apportée à une zone DNS sur l'un des contrôleurs de domaine, cette modification est automatiquement répliquée aux autres contrôleurs de domaine dans le même domaine. Pour mettre en place la réplication DNS, il faut donc faire la réplication AD.

1. Configuration DNS

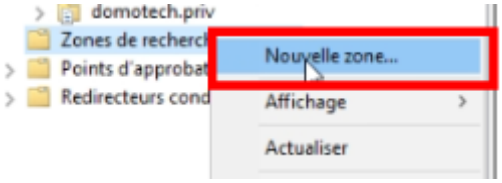
- Se rendre sur le gestionnaire DNS.

- Par défaut, l'arborescence, il y a une zone de recherche directe « domotech.priv ».



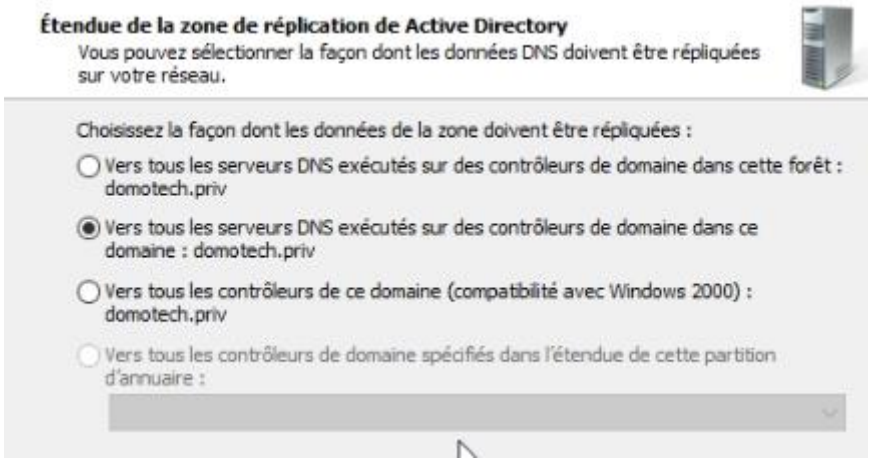
Elle permet de traduire un nom d'hôte en IP. Nous allons mettre en place des zones de recherches inversées pour faire correspondre des IP à des noms d'hôtes.

- Sur « Zones de recherches inversées », faire clic droit et « Nouvelle zone ».

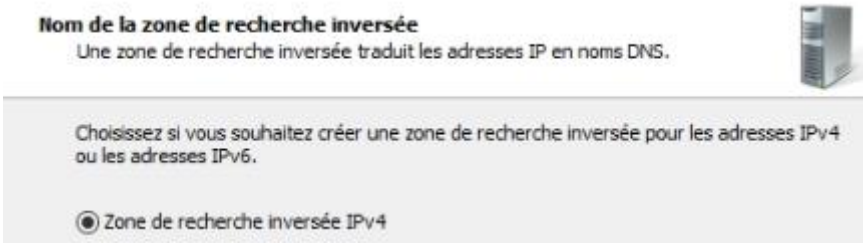


- Choisir « Zone principale » sur le DC01.

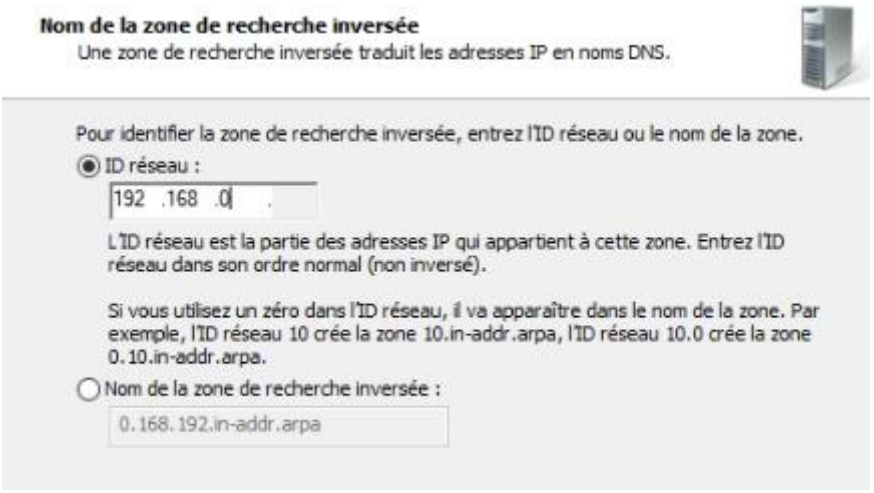
- Laisser le paramètre de réplication par défaut.



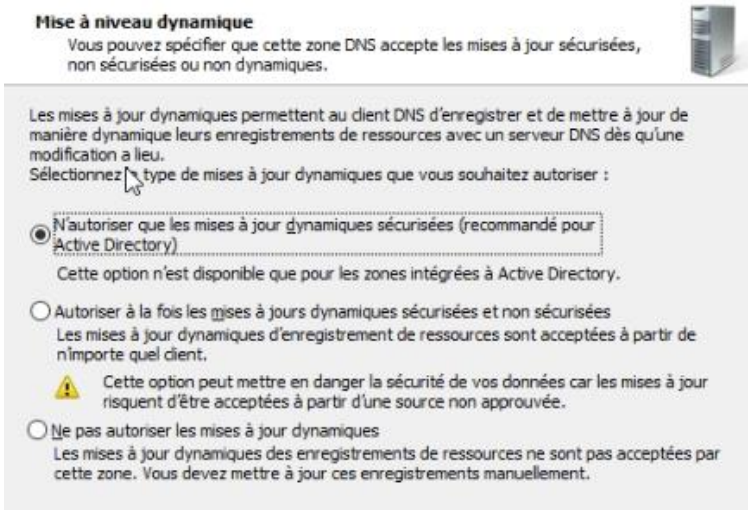
- Choisir « IPv4 ».



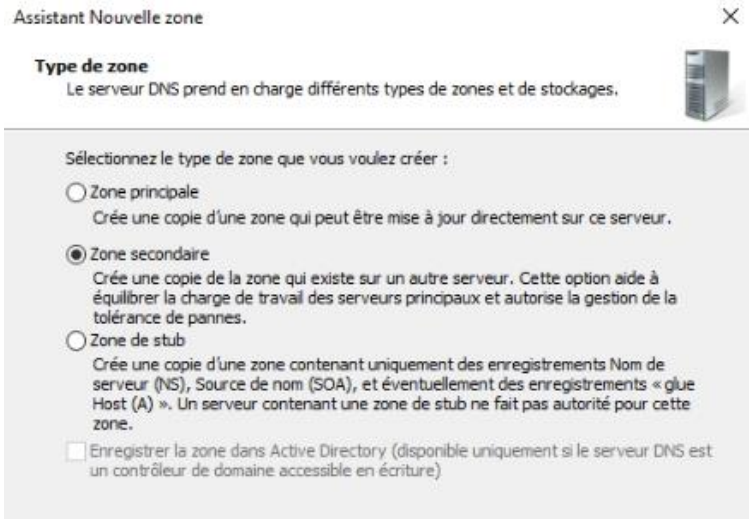
- Renseigner l'ID réseau :



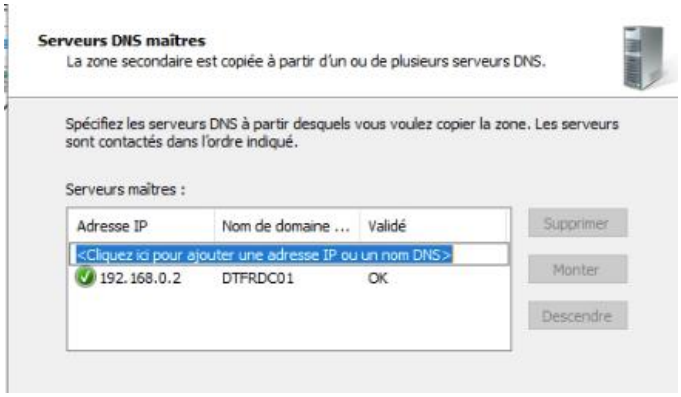
- Pour la mise à niveau dynamique, laisser le paramètre par défaut.



- Sur le DC02, créer la même zone mais en « Zone secondaire ». Cela permettra l'équilibrage des charges et une tolérance des pannes.



- Spécifier l'IP du DC01 en Serveur DNS Maître.



La réplication AD DNS DHCP est terminée.

VII. Cahier de tests

Les tests seront réalisés sur des machines virtuelles VMWare avec les systèmes d'exploitation préalablement définis dans l'invite de commandes.

Liste des commandes :

- Ping IP/Host
- ipconfig /all
- nslookup
- ipconfig /renew
- Connexion Utilisateur
- Présence dans le domaine

Ces tests permettent de vérifier le bon fonctionnement du DHCP, de la résolution des noms.