



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		Valideur	
Nom	Date	Nom	Date
Dylan Chau	04/01/2023	DSI	04/01/2023
Date d'application : 04/01/2023			

Sommaire

Métadonnées.....	2
Prérequis.....	3
Présentation	4
I. Active Directory.....	4
II. Dynamic Host Configuration Protocol.....	4
III. Domain Name System	4
Réplication	4
I. Installation de Windows Server 2019	5
II. Configuration de base	7
III. Installation des services AD DS, DNS et DHCP	9
IV. Réplication AD	10
1. Configuration du premier contrôleur de domaine	10
2. Configuration du second contrôleur de domaine	12
3. Test de réplication AD	13
V. Réplication DHCP	14
1. Configuration	14
2. Création d'une étendue	15
3. Configuration du basculement (réplication)	18
VI. Réplication DNS.....	21
1. Configuration DNS	22
VII. Cahier de tests	25

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 ».

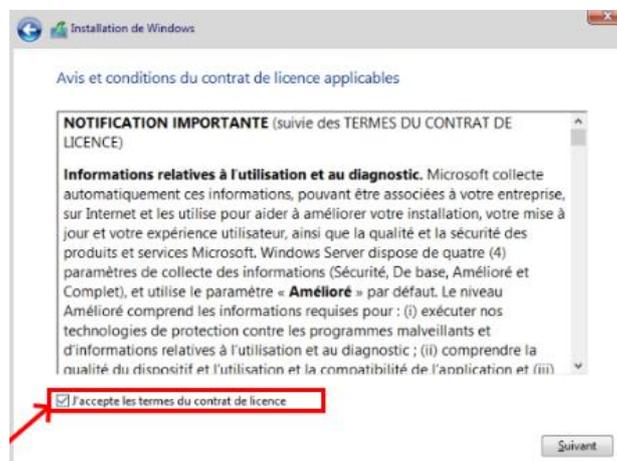


- Choisir l'édition « Datacenter Evaluation expérience de bureau » comme défini dans le DAT.

Sélectionner le système d'exploitation à installer

Système d'exploitation	Architecture	Date de modi...
Windows Server 2019 Standard Evaluation	x64	07/09/2019
Windows Server 2019 Standard Evaluation (expérience de bu...	x64	07/09/2019
Windows Server 2019 Datacenter Evaluation	x64	07/09/2019
Windows Server 2019 Datacenter Evaluation (expérience de b...	x64	07/09/2019

- Accepter les CGU



- Sélectionner « Personnalisé ».



- Créer un nouveau disque.



- Lancer l'installation sur le lecteur principal.



- Finir l'installation.

Installation de Windows

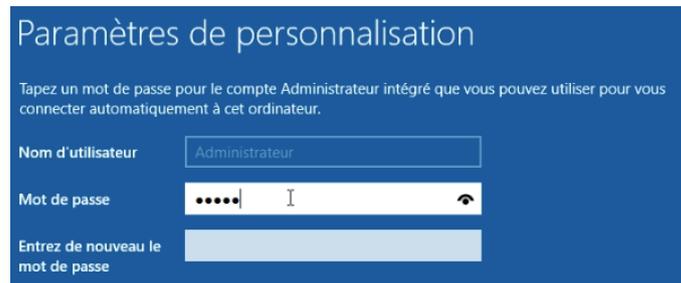
Statut

- ✓ Copie des fichiers de Windows
- Préparation des fichiers pour l'installation (23 %)**
- Installation des fonctionnalités
- Installation des mises à jour
- En cours d'achèvement

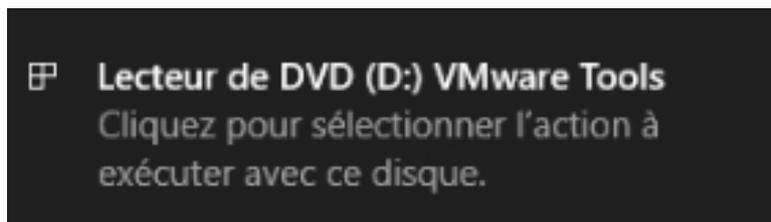
- Répéter l'opération sur la seconde machine

II. Configuration de base

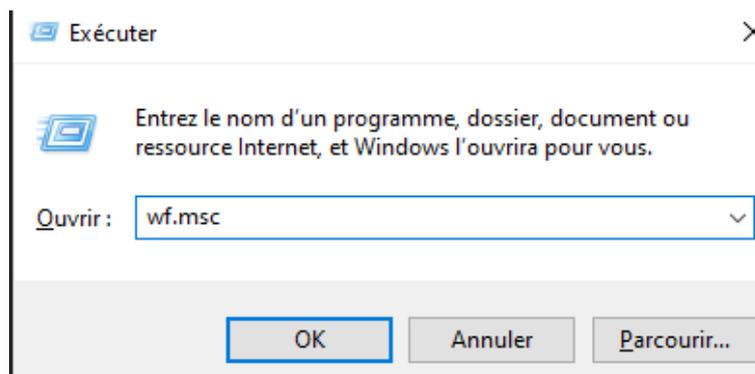
- Définir le mot de passe du compte Administrateur intégré.



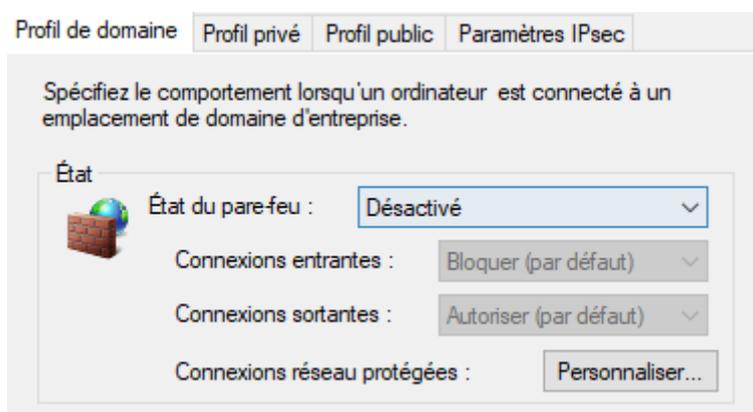
- Installer les drivers VMWare Tools (Pour l'affichage notamment).



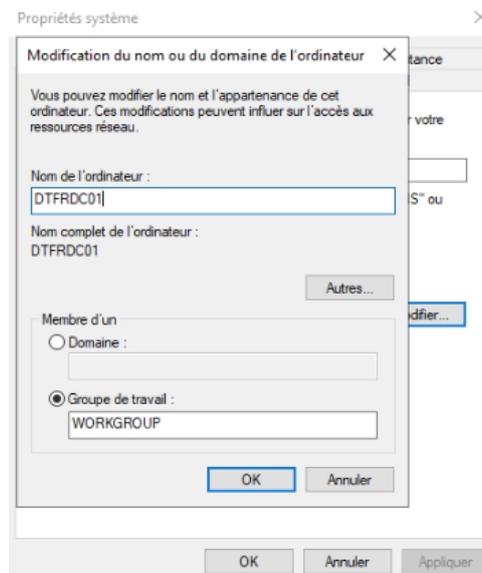
- Faire « Windows + R » puis « wf.msc ».



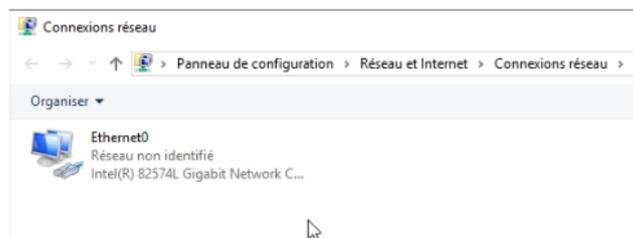
- Désactiver le pare-feu Windows Defender (géré par PFSense). Il faut le désactiver car il pourrait bloquer des flux entrants et sortants.



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



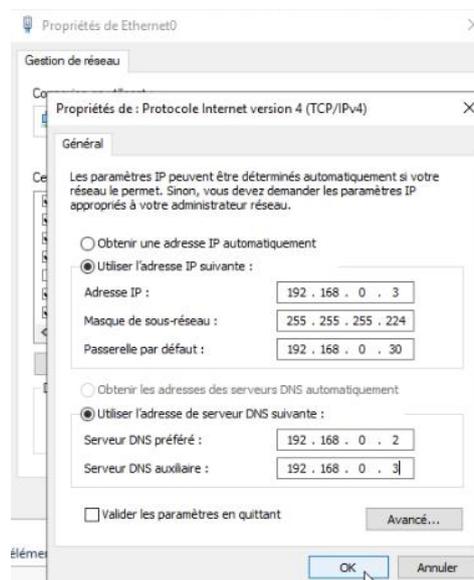
- Faire « Windows + R » puis « ncpa.cpl » pour accéder aux cartes réseaux.



- Faire un clic droit puis « Propriétés ».
- Désactiver TCP/IPv6

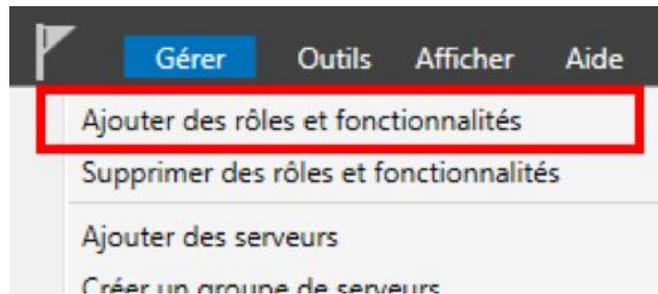


- Ouvrir Protocole Internet version 4 (TCP/IPv4) et configurer la carte réseau de chaque machine en se basant sur le DAT.



III. Installation des services AD DS, DNS et DHCP

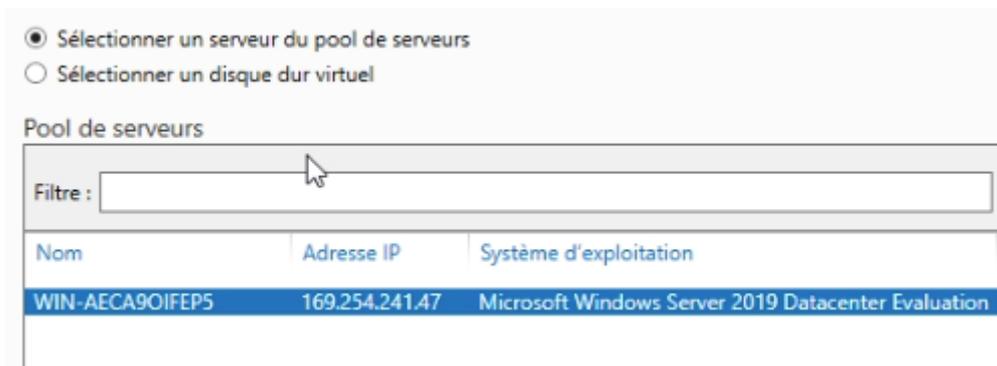
- Cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



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

Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

- 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.

Redémarrer automatiquement le serveur de destination, si nécessaire

- Puis cliquer sur « Installer ».



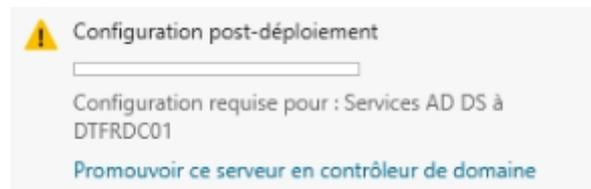
- Le serveur va redémarrer.

IV. Réplication AD

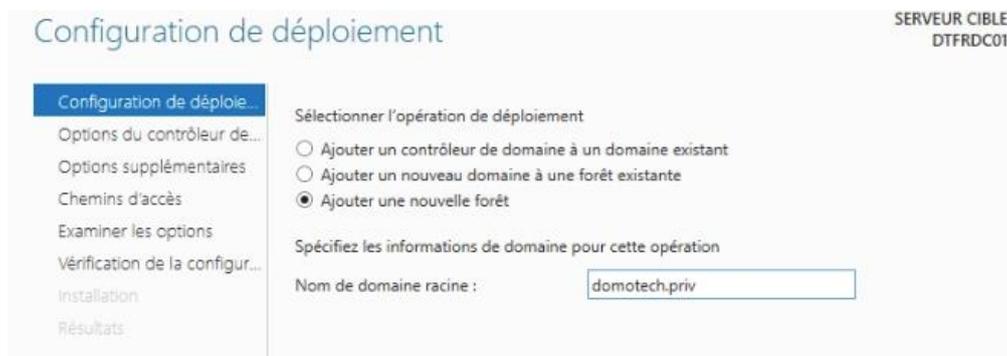
1. Configuration du premier contrôleur de domaine

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

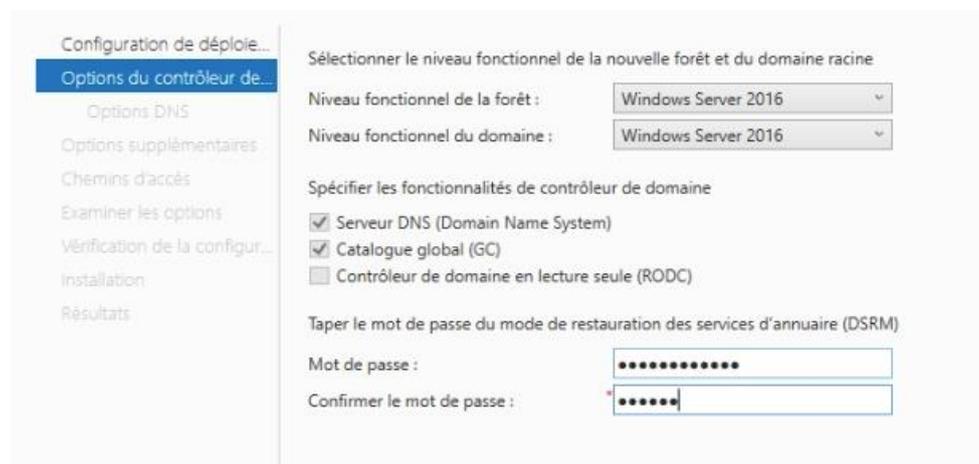
- Cliquer sur le drapeau avec le « Warning » puis sur « Promouvoir ce serveur en contrôleur de domaine ».



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



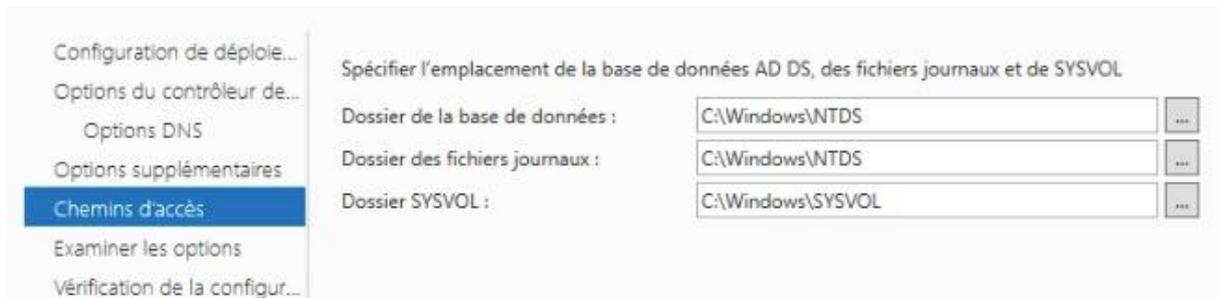
- Laisser le niveau fonctionnel par défaut et définir un mot de passe DSRM.



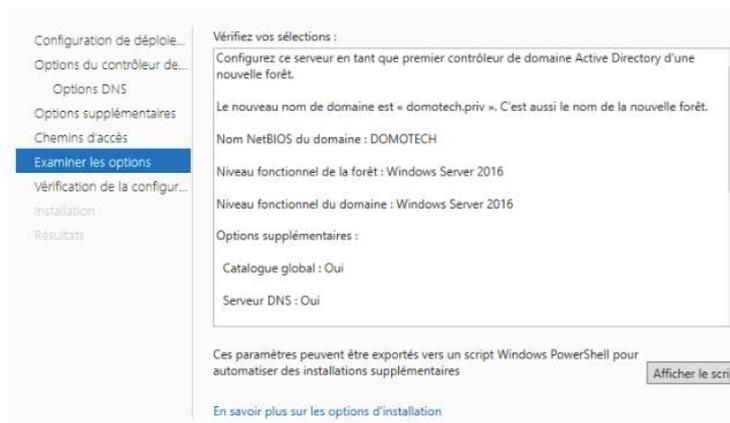
- Sur « Option DNS », cliquer sur « Suivant ».
- Le nom NetBIOS du domaine apparaît.



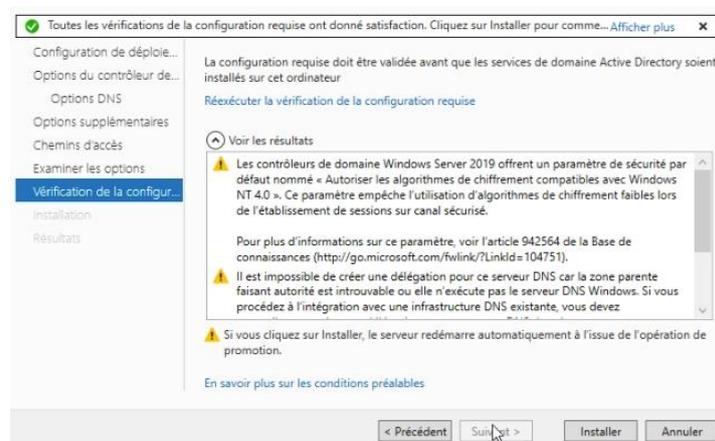
- L'emplacement des fichiers de configuration de l'AD sont affichés.



- Un récapitulatif est affiché.



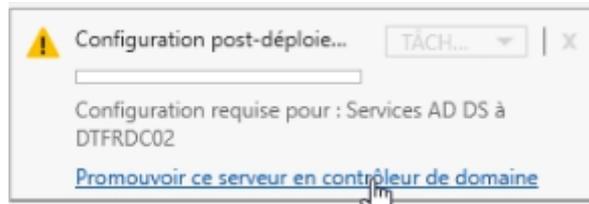
- Démarrer l'installation.



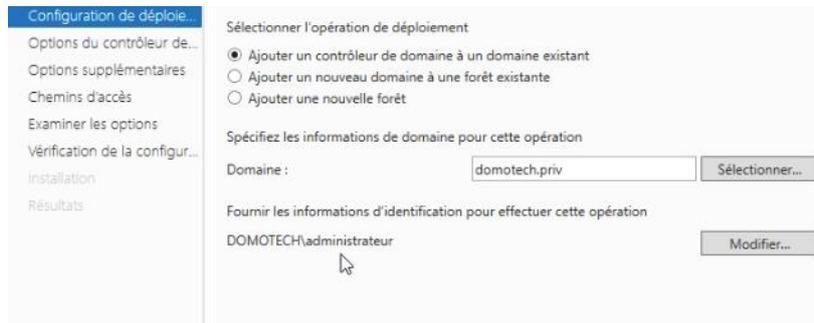
- Une fois terminée, le premier contrôleur de domaine est prêt.

2. Configuration du second contrôleur de domaine

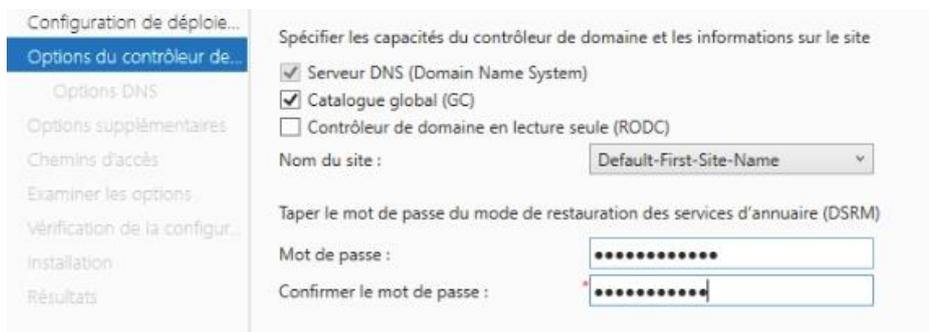
- Cliquer sur le drapeau avec le « Warning » puis sur « Promouvoir ce serveur en contrôleur de domaine ».



- 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.

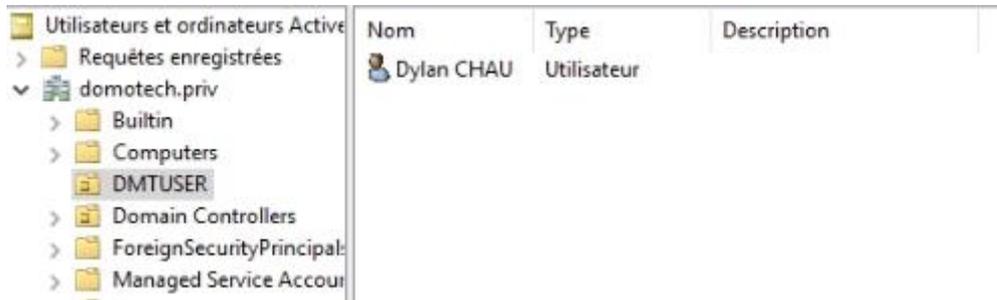


- Finir l'installation comme pour le premier contrôleur de domaine. La réplication est terminée.

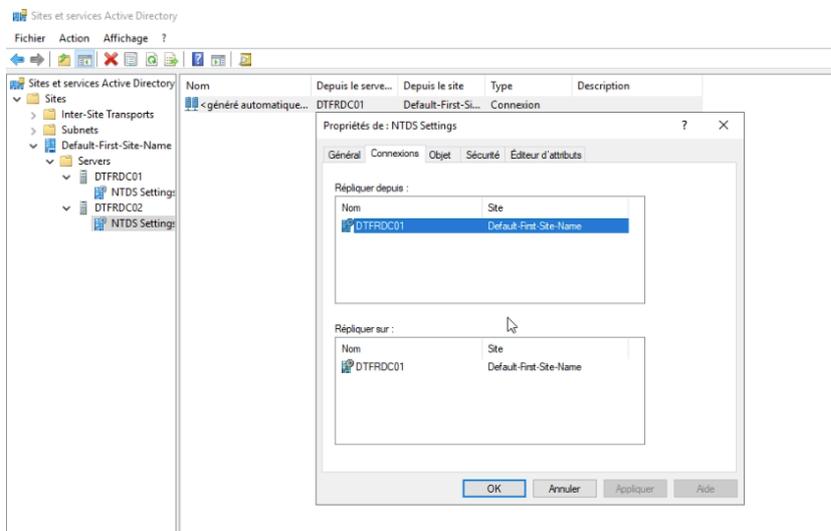
3. Test de réplication AD

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

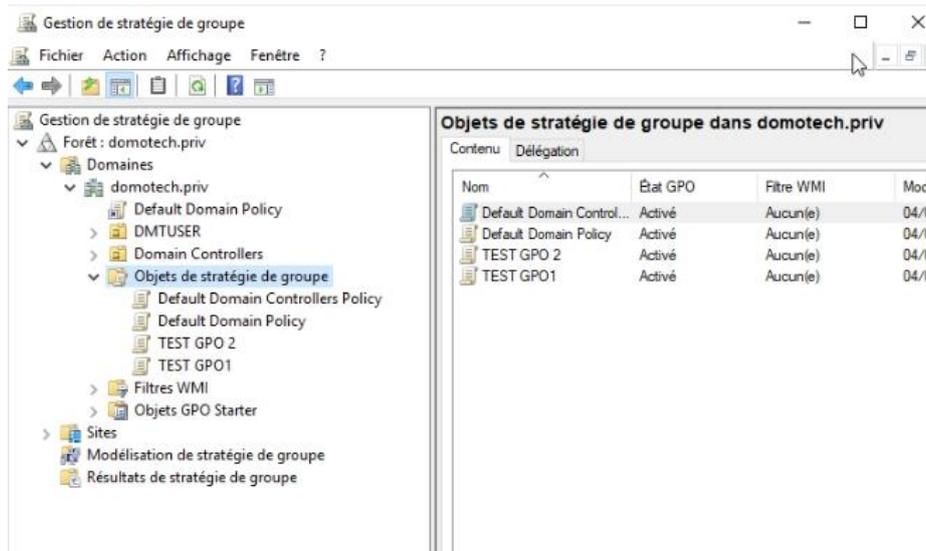
- Créer une unité d'organisation et un utilisateur dedans pour vérifier la réplication.



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



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



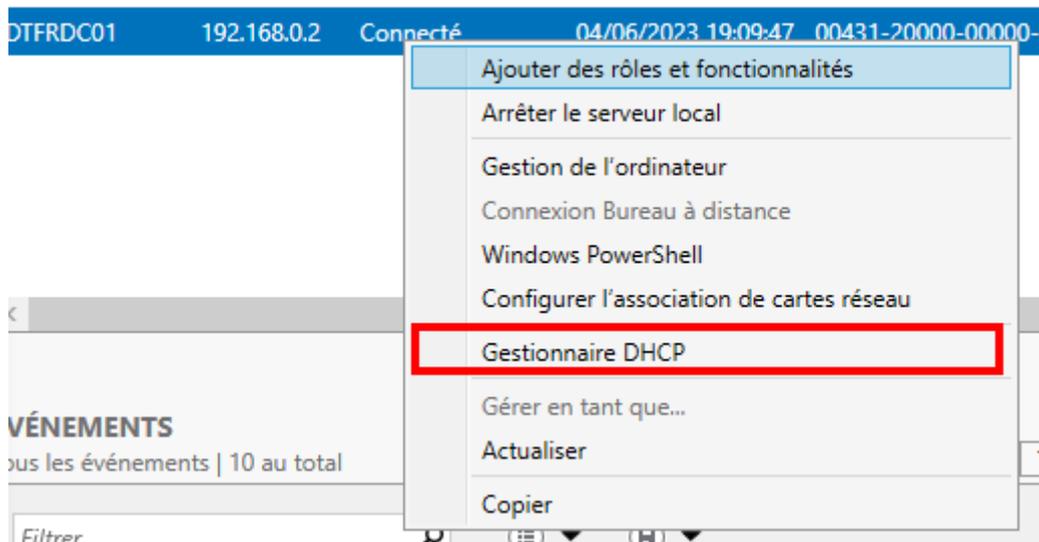
V. Réplication DHCP

1. Configuration

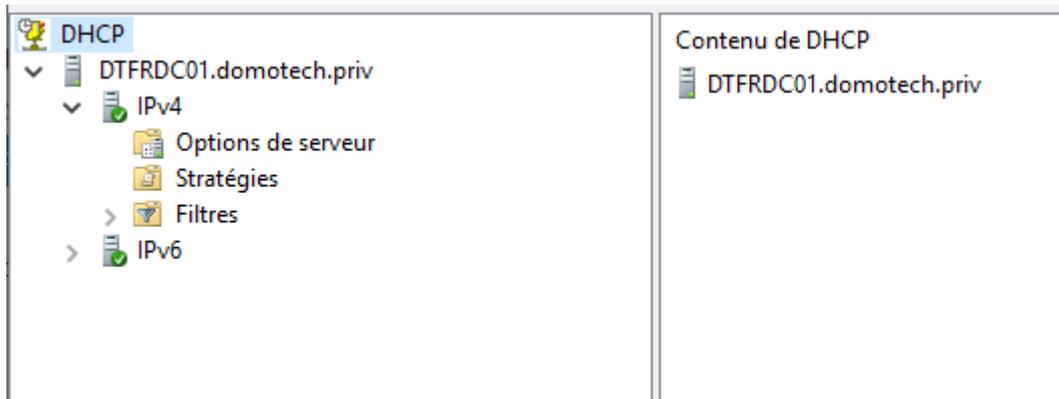
- Terminer la configuration DHCP après redémarrage du serveur. Cette étape va permettre de créer deux groupes de sécurité dans l'AD pour permettre la délégation quant à la gestion du serveur DHCP et déclarer notre serveur DHCP au sein de l'AD.
- Cliquer ensuite sur « DHCP ».



- Lancer ensuite le gestionnaire DHCP.

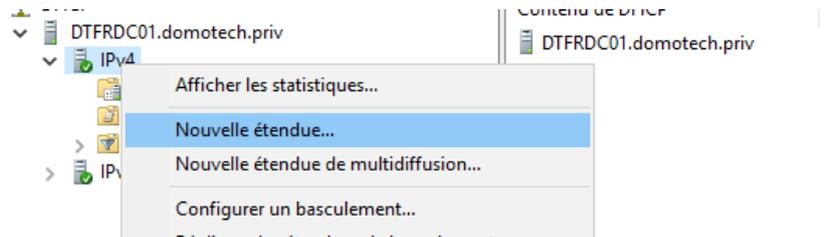


- Le gestionnaire s'affiche ensuite.



2. Création d'une étendue

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



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

Nom de l'étendue

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



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

Nom :

Description :

- Paramétrer les IP en fonction du DAT.

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 :

- 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.

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 :

- Laisser la durée du bail par défaut.

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 :

- Configurer les options DHCP.

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.

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

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 :

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

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 :

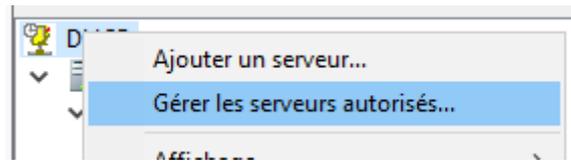
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text" value="."/> . . .	<input type="button" value="Ajouter"/>
<input type="button" value="Résoudre"/>	<input type="text" value="192.168.0.2"/> <input type="text" value="192.168.0.3"/>	<input type="button" value="Supprimer"/>
		<input type="button" value="Monter"/>
		<input type="button" value="Descendre"/>

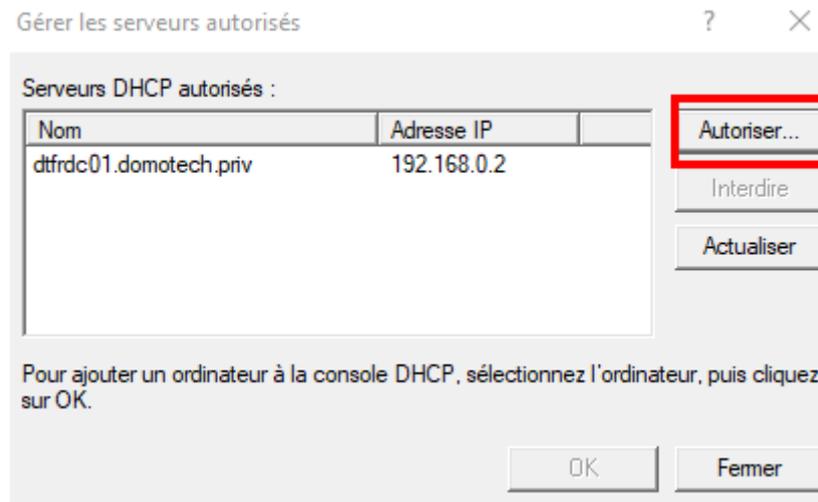
- Ne rien mettre pour les serveurs WINS.
- Activer l'étendue. Il faudra configurer les étendues en fonction du DAT.

3. Configuration du basculement (réplication)

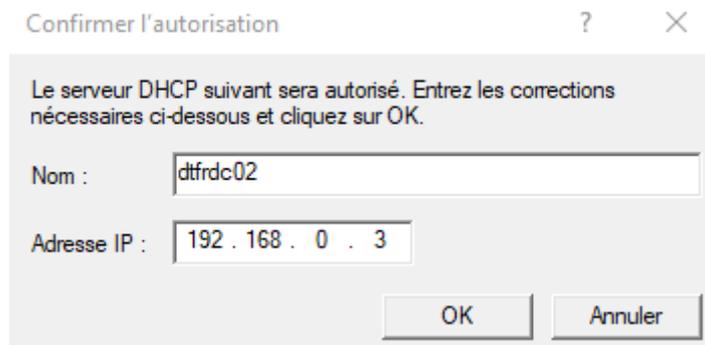
- Sur « DHCP », faire clic droit puis cliquer sur « Gérer les serveurs autorisés ».



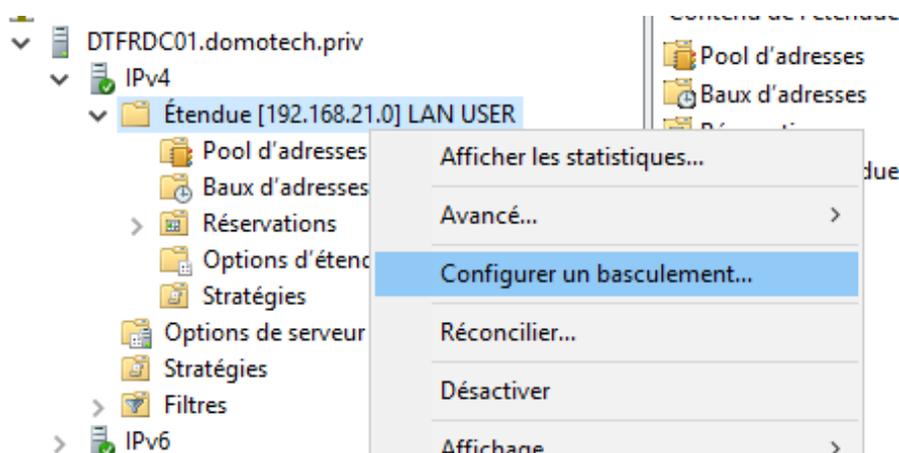
- Cliquer sur « Autoriser ».



- Ajouter le DC02.



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



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

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

192.168.21.0

- Ajouter le second serveur en partenaire.

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 :

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

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

Créer une relation de basculement



Créer une relation de basculement avec le partenaire dtfrdc02

Nom de la relation :

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

Mode :

Pourcentage d'équilibrage de charge

Serveur local : %

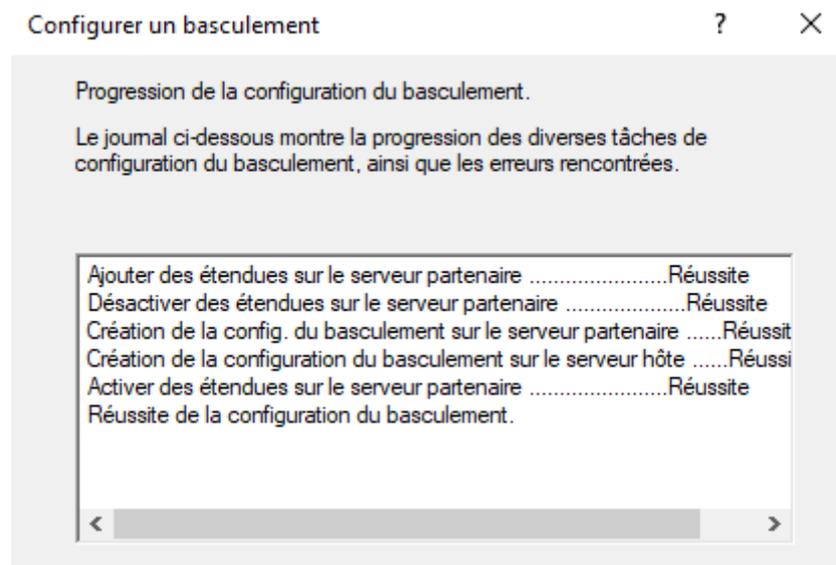
Serveur partenaire : %

Intervalle de basculement d'état : minutes

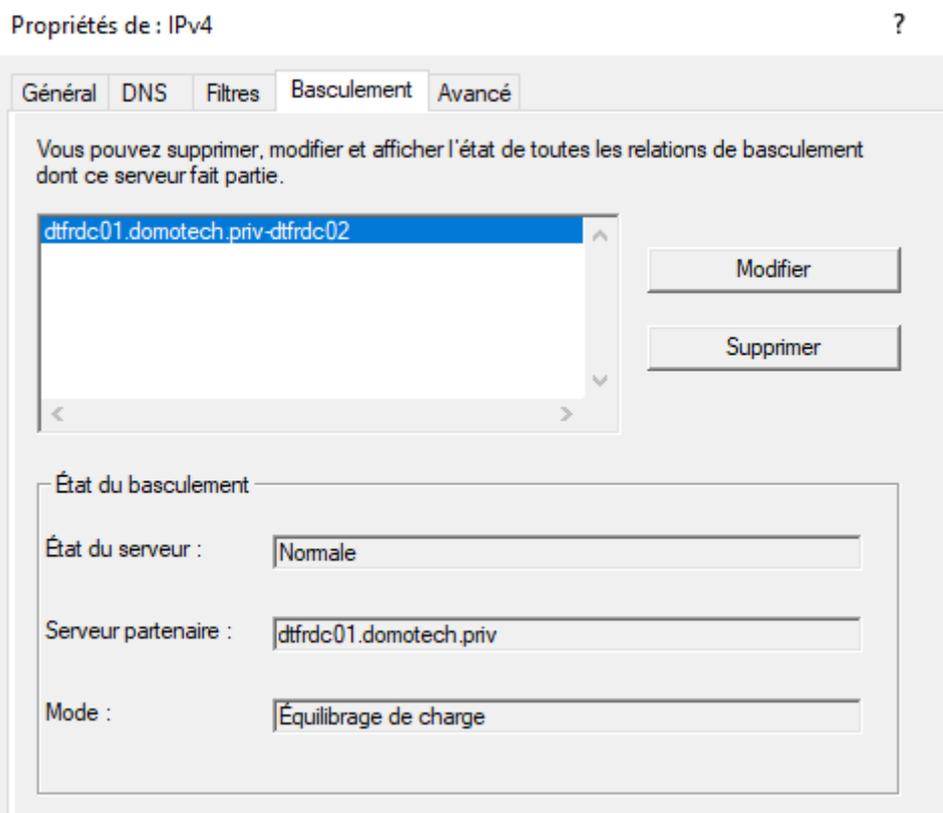
Activer l'authentification du message

Secret partagé :

- Le basculement est terminé.



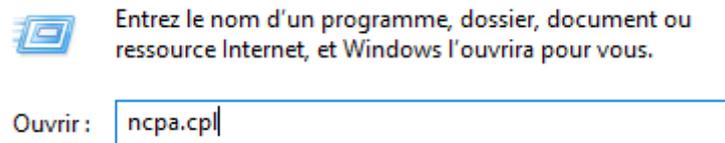
- La relation apparaît bien sur le second contrôleur de domaine.



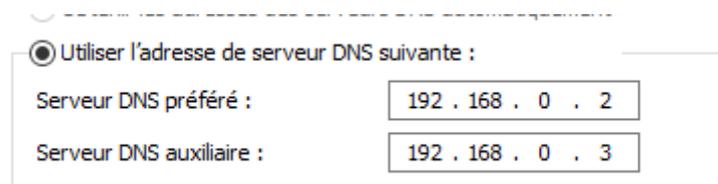
VI. Réplication DNS

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.

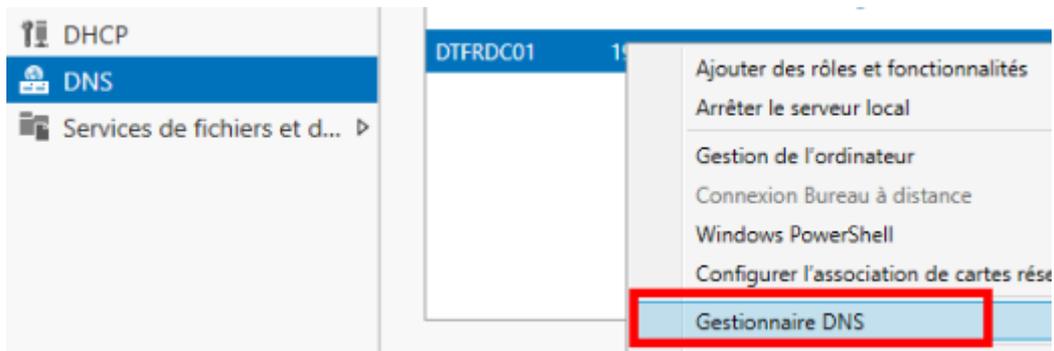


La réplication DNS s'appuie sur le mécanisme de réplication d'Active Directory pour transmettre les modifications entre les contrôleurs de domaine.

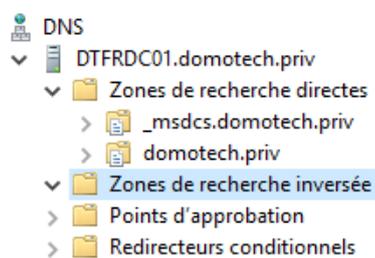
Cela signifie que les zones DNS sont intégrées à la réplication d'Active Directory. Lorsqu'une modification est apportée à une zone DNS sur l'un des contrôleurs de domaine, cette modification est automatiquement répliquée aux autres contrôleurs de domaine dans le même domaine. Pour mettre en place la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

1. Configuration DNS

- Se rendre sur le gestionnaire DNS.

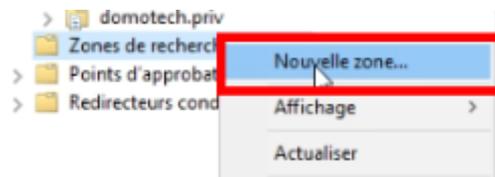


- Par défaut, l'arborescence, il y a une zone de recherche directe « domotech.priv ».

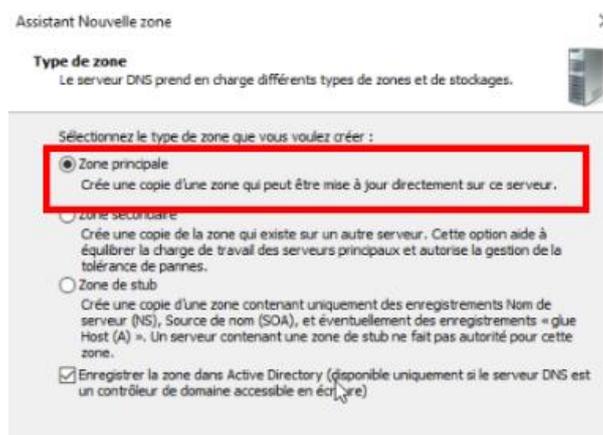


Elle permet de traduire un nom d'hôte en IP. Nous allons mettre en place des zones de recherches inversées pour faire correspondre des IP à des noms d'hôtes.

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



- Choisir « Zone principale » sur le DC01.



- Laisser le paramètre de réplification par défaut.

Étendue de la zone de réplification de Active Directory 

Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : domotech.priv
- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : domotech.priv
- Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : domotech.priv
- Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

- Choisir « IPv4 ».

Nom de la zone de recherche inversée 

Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

- Zone de recherche inversée IPv4

- Renseigner l'ID réseau :

Nom de la zone de recherche inversée 

Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

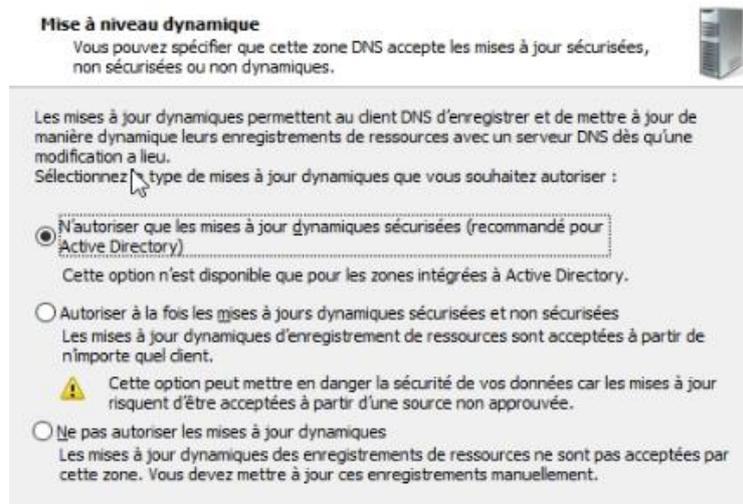
- ID réseau :

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

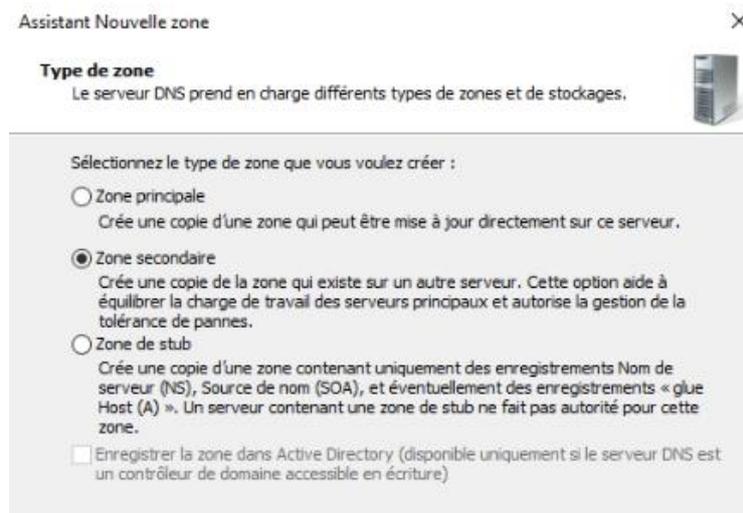
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

- Nom de la zone de recherche inversée :

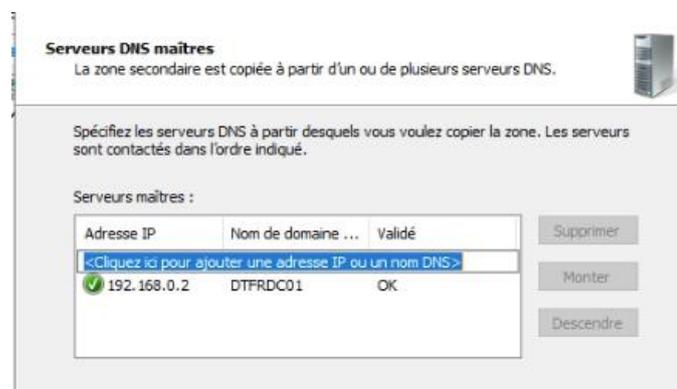
- Pour la mise à niveau dynamique, laisser le paramètre par défaut.



- 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.