Documentation technique

****

Installation d’un serveur AD DS et différents rôles

Table des matières

Nicolas DURAND

Introduction :

Objectif :

L'objectif de cette documentation est de voir comment installer les services AD, DNS et DHCP sur un domaine. Nous verrons aussi la mise en place de redondance afin d'assurer la continuité de ces services.

Matériel :

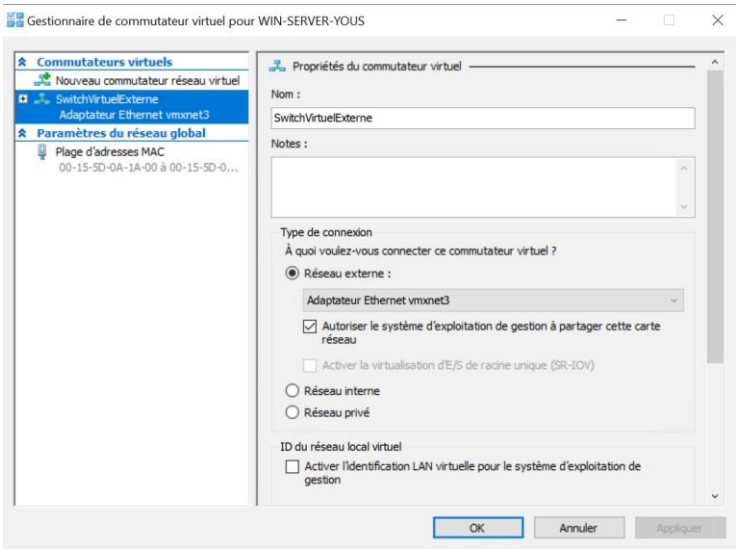
Nous disposons de 2 machines virtuelles Windows Server 2022, une qui jouera le rôle de serveur AD principal et une qui jouera le rôle de serveur AD secondaire, ainsi que d'une machine virtuelle Windows 10 pour les tests. Toutes les VM sont hébergées sur un Windows Server possédant le rôle Hyper-V.

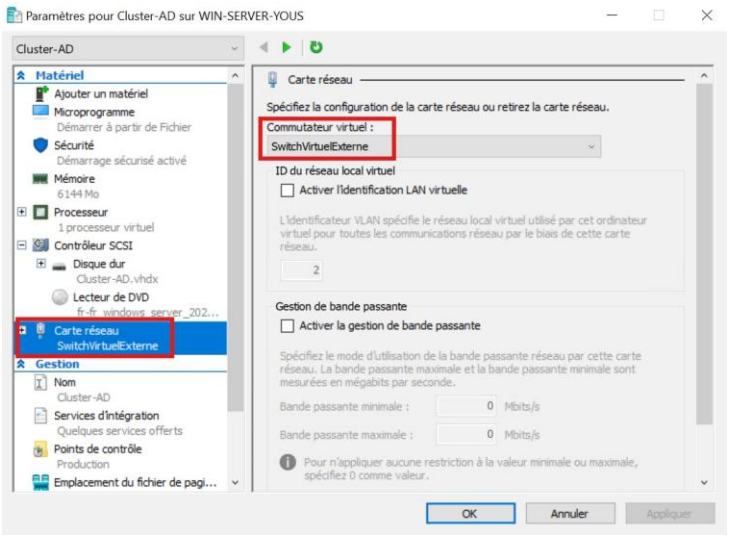
Adressage IP :

Equipement	**Nom**	**Adresse IP (/24)**
VM Windows server 2022	Win-serv-AD	172.16.10.10
VM Windows server 2022	Win-serv-AD-2	172.16.10.11
VM Windows 10	Win-client	DHCP
Passerelle par défaut		172.16.10.254

1. Connectivité

Pour assurer le bon fonctionnement des services, il faut assurer une connectivité entre les machines. Dans notre cas, les 3 VM sont hébergés sur un serveur Hyper-V. On va donc créer, depuis le service Hyper-V, un switch virtuel que l'on va ensuite sélectionner comme connexion pour chacune des VM :





C'est exactement comme si l'on avait 3 machines physiques que l'on branchait sur un commutateur physique.
Ce switch virtuel se présente sur le serveur Hyper-V comme une carte réseau sur laquelle nous allons appliquer une adresse IP afin que les 3 VM aient accès au réseau local et à Internet :

Enfin, on teste la connectivité entre les machines.
Ping de *Win-serv-AD* vers *Win-serv-AD-2* :

```
C:\Users\Administrateur>ping 172.16.10.11

Envoi d'une requête 'Ping'  172.16.10.11 avec 32 octets de données :
Réponse de 172.16.10.11 : octets=32 temps=2 ms TTL=128
Réponse de 172.16.10.11 : octets=32 temps=1 ms TTL=128
```

Ping de *Win-serv-AD-2* vers *Win-client* :

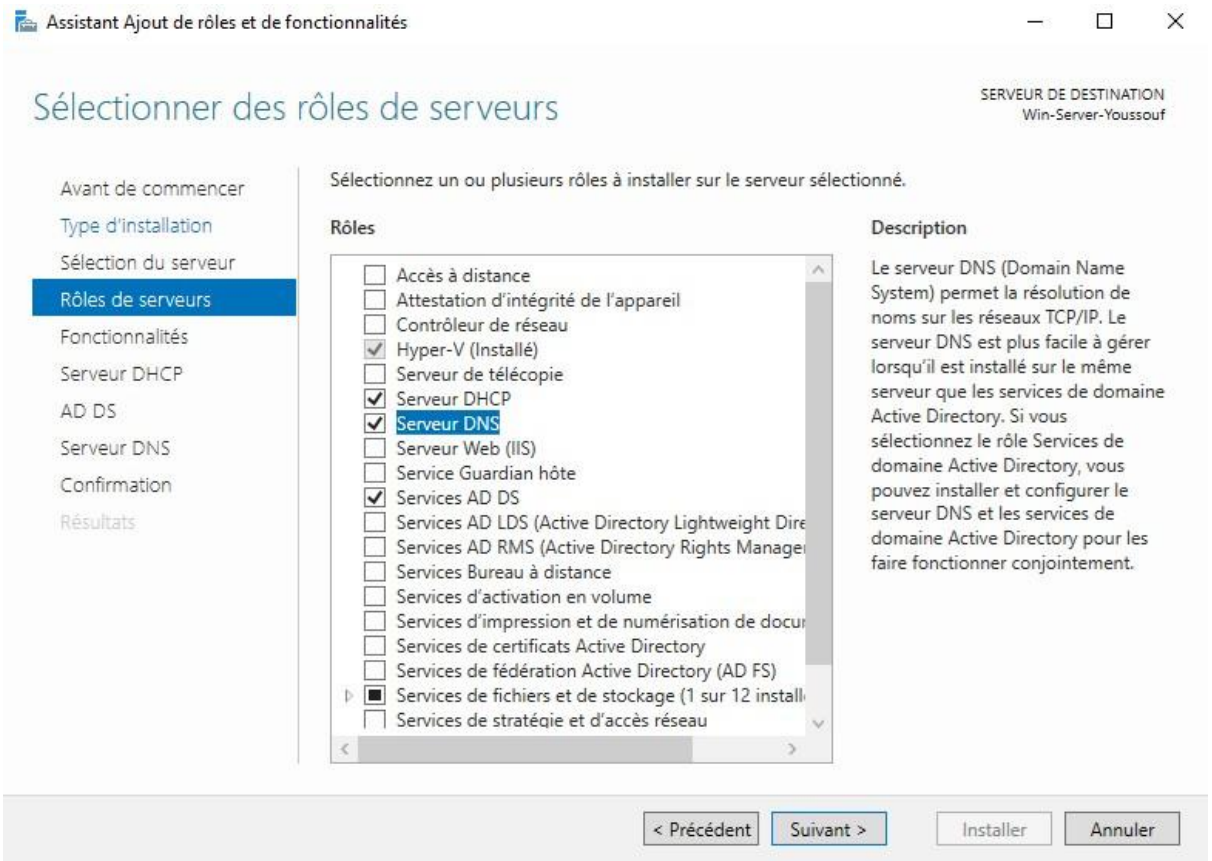
```
C:\Users\administrateur.FYM>ping 172.16.10.57

Envoi d'une requête 'Ping'  172.16.10.57 avec 32 octets de données :
Réponse de 172.16.10.57 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.10.57 : octets=32 temps=1 ms TTL=128
```

2. Service AD / DNS

2.1. Installation des rôles

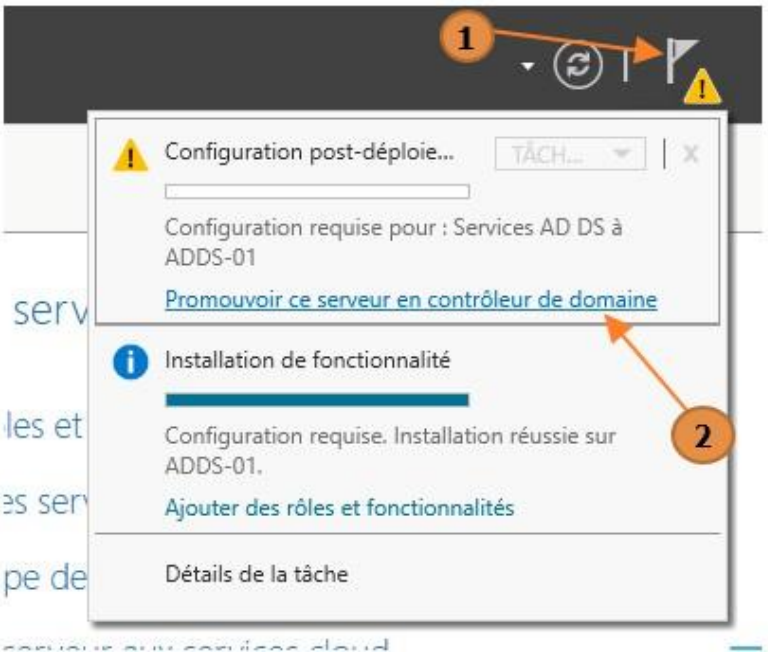
Pour mettre en place des services sur un serveur Windows, il faut se rendre dans le gestionnaire de serveurs et ajouter les rôles que l'on veut. Nous allons dans un premier temps installer tous les rôles dont on a besoin et nous les configurerons un par un par la suite.
Dans notre cas, on installe les rôles AD DS, DNS et DHCP :



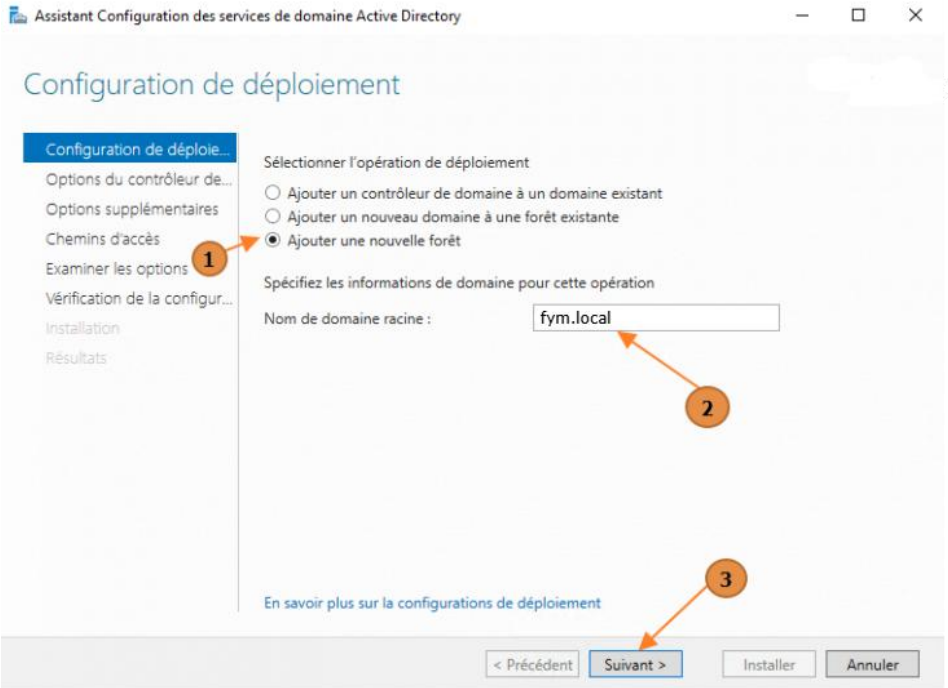
On suit les étapes et on laisse les rôles s'installer.

2.2. Configuration du rôle AD DS

Une fois le rôle installé, on remarque un avertissement en haut à droite de l'écran, représenté par un triangle jaune :

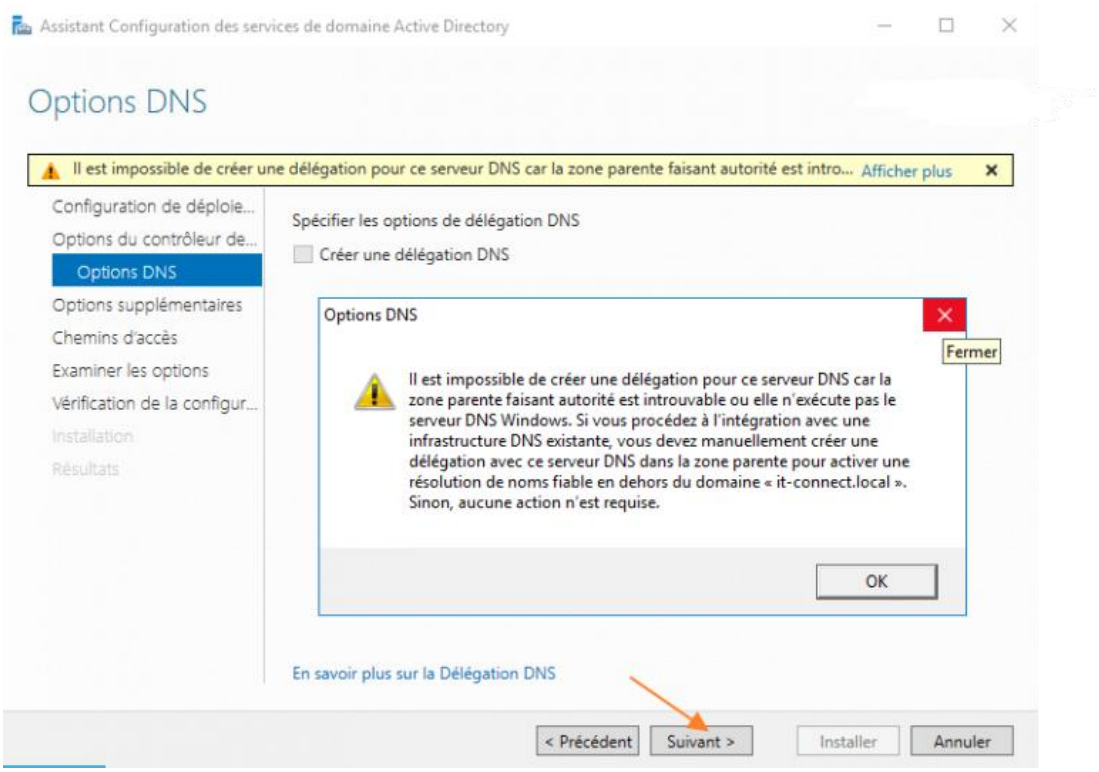


On clique dessus puis sur "Promouvoir ce serveur en contrôleur de domaine". Ensuite, comme il s'agit d'un nouveau domaine dans une nouvelle forêt, on sélectionne "Ajouter une nouvelle forêt" et on indique le nom de domaine :



Puis on ajoute les options DNS et Catalogue global, et on définit le mot de passe DSRM, qui est un mot de passe unique utilisé pour accéder au mode de restauration des services d'annuaire.

Si un message suivant apparaît, on l'ignore et on continue l'installation. Ce message indique simplement qu'aucune zone DNS intégrée à notre domaine n'existe encore, ce qui est normal, puisque l'on vient juste de la créer :

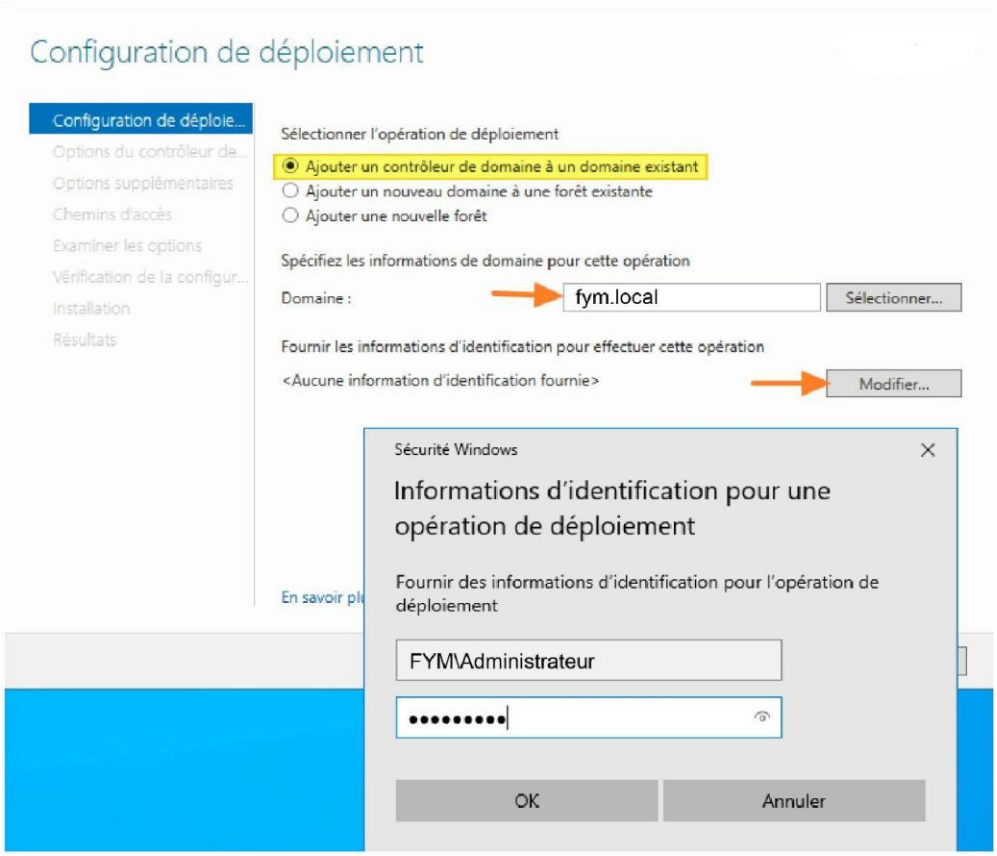


Ensuite, on continue l'installation jusqu'à la fin en cliquant sur "Suivant" aux différentes étapes. Une fois l'installation terminée, le serveur va redémarrer et après ce redémarrage, on pourra enfin utiliser notre serveur en tant que contrôleur de domaine Active Directory.

2.3. Redondance

La redondance est un aspect important dans la mise en place de services au sein d'un réseau d'entreprise. En effet, elle permet d'assurer une continuité de service en cas de panne de l'un équipement. Ici, nous allons voir comment mettre en place la redondance du contrôleur de domaine AD. Il nous faudra donc un deuxième serveur identique au premier. Dans notre cas, on prendra une VM Windows Server 2022. Ainsi, si l'une deux 2 machines tombe en panne ou subit un dysfonctionnement, le service sera toujours fonctionnel et les utilisateurs ne seront pas impactés.

Dans un premier temps, on installe le rôle AD DS sur le second serveur et on suit les mêmes étapes que pour le serveur principal. Une fois le rôle installé, on promeut le serveur en contrôleur de domaine.
C'est à partir de cette étape que l'on va définir ce serveur en tant que serveur secondaire :

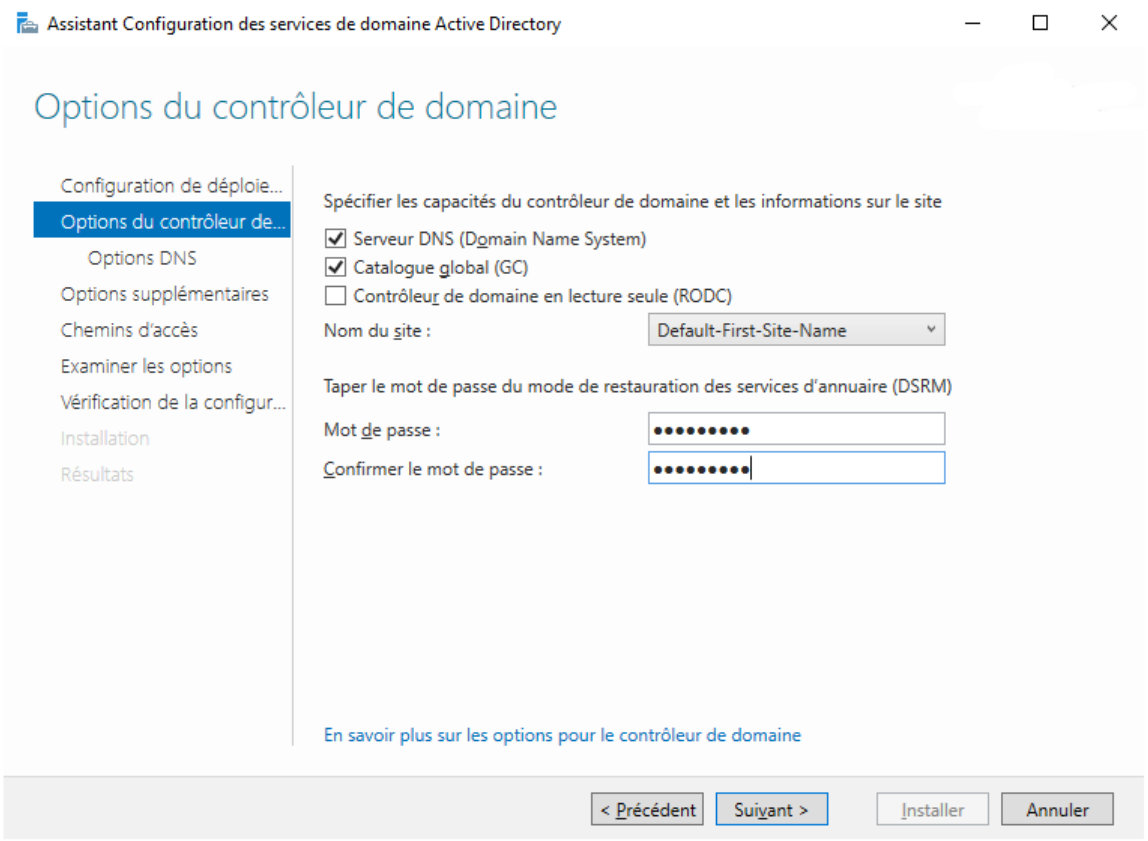


On coche la case “Ajouter un contrôleur de domaine à un domaine existant” et on renseigne le nom du domaine. Ensuite, on se connecte au compte administrateur du domaine.

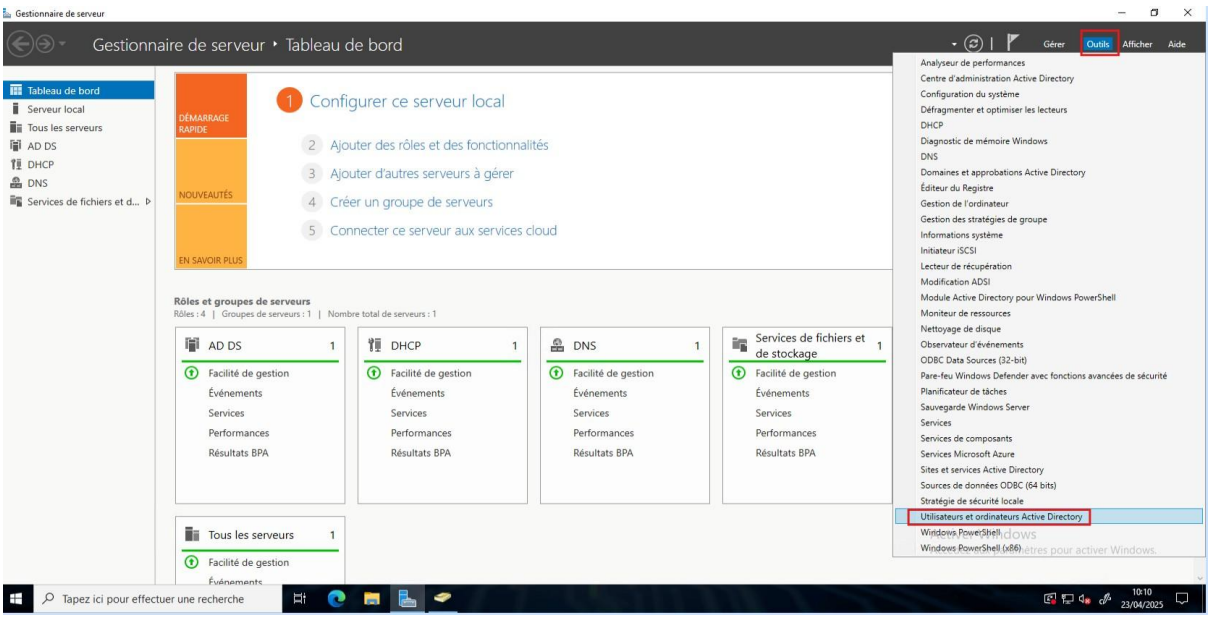
A l'étape suivante, on sélectionne les options suivantes :

- "Serveur DNS" afin qu'il soit aussi serveur DNS, ce qui permettra de redonder ce service au niveau de l'infrastructure
- "Catalogue global (GC)" afin d'avoir deux catalogues globaux

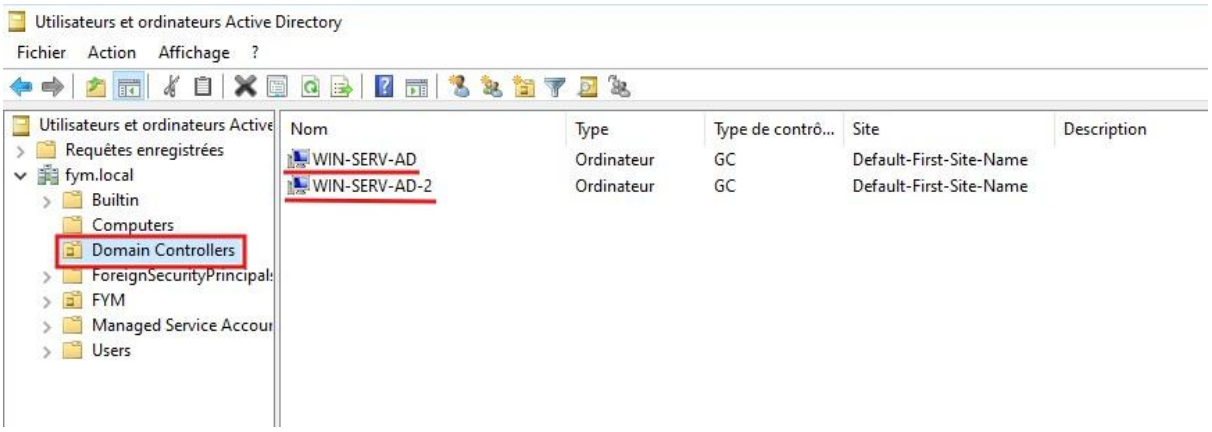
On ne coche pas "Contrôleur de domaine en lecture seule", car nous avons besoin d'un contrôleur de domaine en lecture et écriture



Ensuite, dans “Options supplémentaires”, on choisit le serveur principal dans “Répliquer depuis”. Puis on clique sur Suivant jusqu’à la fin de l’installation en laissant les paramètres prédéfinis.
Après redémarrage de la machine, on peut utiliser ce serveur en tant que contrôleur de domaine secondaire.
Il ne manque plus qu’à vérifier la bonne mise en place de la redondance. Pour ce faire, on se rend sur l’un des deux serveurs (l’un ou l’autre, peu importe). Depuis le gestionnaire de serveur, on se rend dans le menu “Outils” en haut à droite et on clique sur “Utilisateurs et ordinateurs Active Directory” :



On peut observer qu'il y a bien 2 contrôleurs de domaine sur notre domaine "fym.local" :



Désormais, chaque modification (ajout ou suppression d'OU, d'utilisateurs, modifications de droits etc) sera répliquée sur l'autre serveur, que cette modification ait été effectuée sur le serveur principal ou secondaire.

2.4. Mise en place d'une GPO

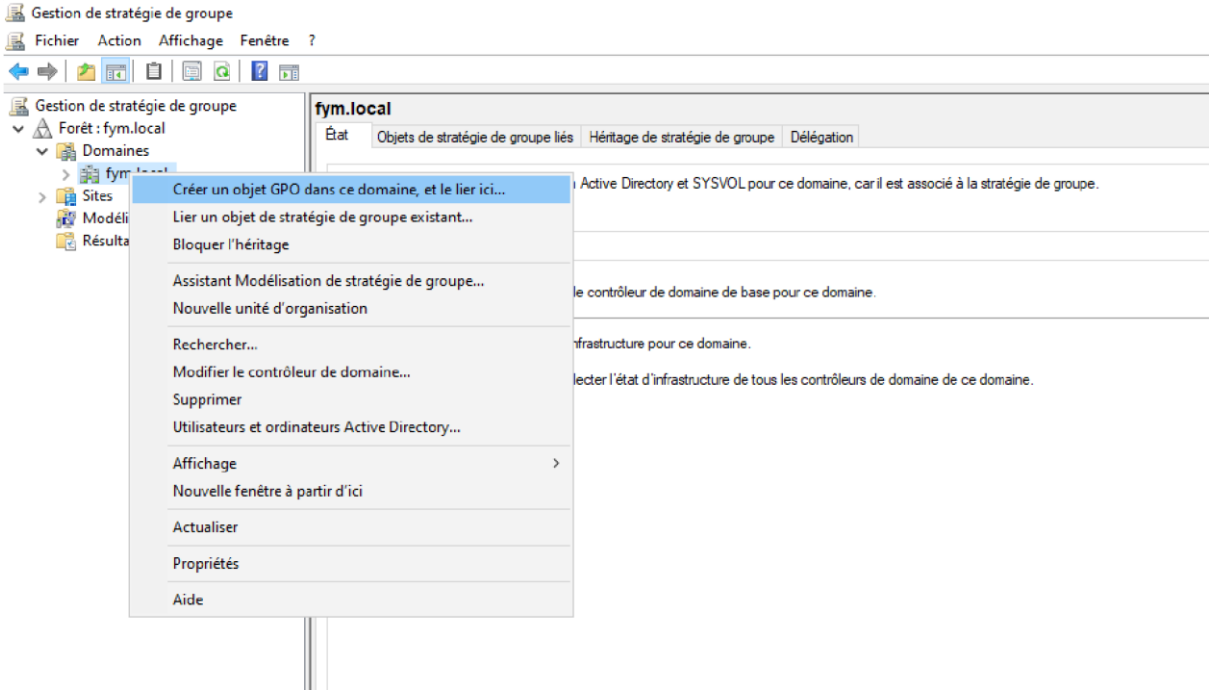
Maintenant, on peut voir comment mettre en place une stratégie de groupe, ou GPO (Group Policy Objects). Une GPO a pour objectif de centraliser et automatiser la gestion de la configuration des ordinateurs et des utilisateurs. Par exemple, si l'on veut déployer le même fond d'écran sur toutes les sessions des utilisateurs du domaine, on peut le faire grâce à une GPO. Cela nous garantit donc un gain de temps et un contrôle sur les utilisateurs du domaine.
C'est ce que nous allons voir dans cette partie.

Pour déployer un fond d'écran, il faut tout d'abord choisir une image que l'on va enregistrer sur le serveur. Ensuite, il faut que les utilisateurs aient accès à cette image afin de pouvoir la définir comme fond d'écran.

Pour ce faire, on va créer un dossier au niveau de la racine du serveur que l'on va appeler "Deploiement$". On peut se permettre de créer ce dossier à la racine car son contenu ne sera pas trop lourd et n'aura pas d'impact sur la capacité de stockage du "C:\". Le signe $ dans le nom du dossier n'est pas obligatoire, mais il permet de cacher le nom du fichier aux utilisateurs. Ainsi, un utilisateur qui veut voir les dossiers et fichiers partagés présents sur le serveur à distance ne verra pas ce dossier.

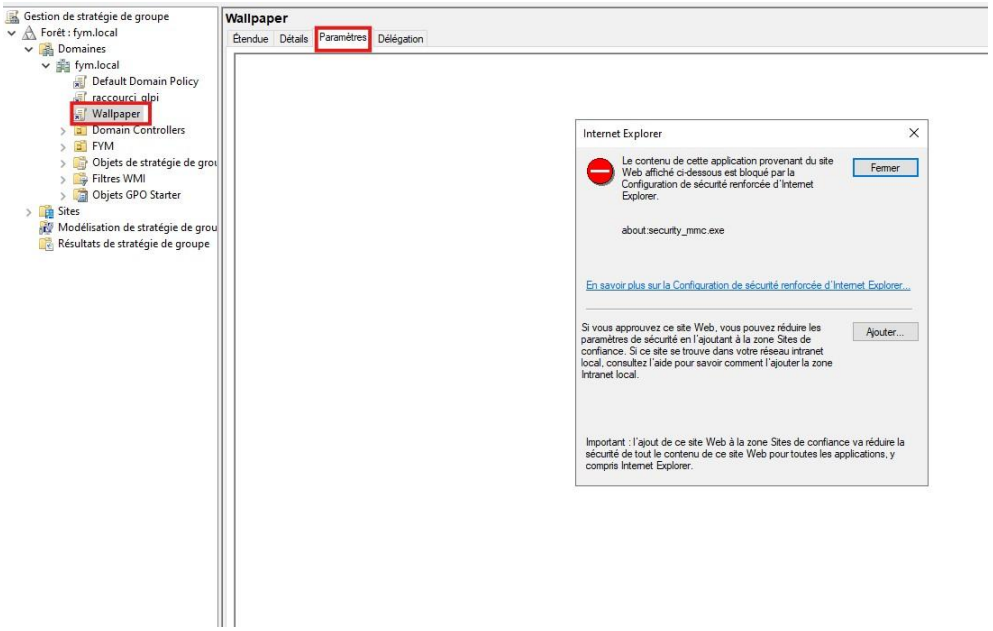
Ensuite, on dépose notre image de fond d'écran dans notre dossier. Vient le moment de partager le dossier afin que l'image se trouvant dedans soit accessible par les utilisateurs du domaine. Pour cela, on fait un clic droit sur le dossier et on clique sur "Propriétés", puis on se rend dans l'onglet

Maintenant, on peut commencer la configuration de la GPO. Pour cela, on recherche dans le menu démarrer du serveur "stratégie" et on clique sur "Gestion des stratégies de groupe". On effectue un clic droit sur le nom de notre domaine et on clique sur la première ligne :

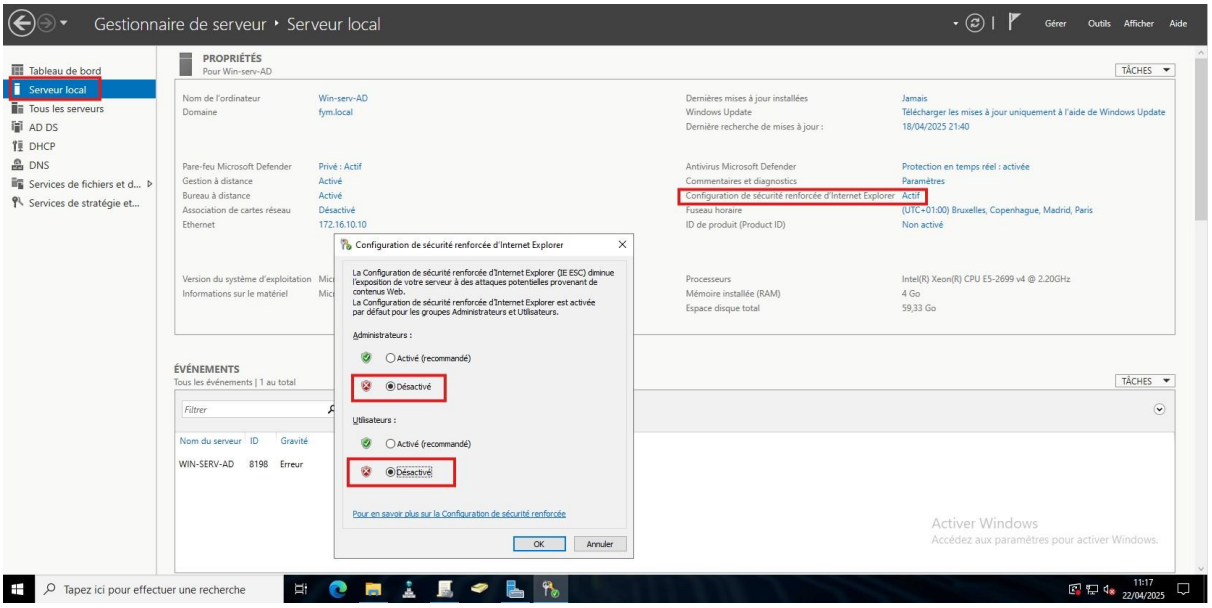


Ensuite, on nomme notre objet GPO et on valide. Appelons-le “Wallpaper”. On le retrouve par la suite dans la liste lorsque l’on clique sur la flèche à gauche du nom de notre domaine.

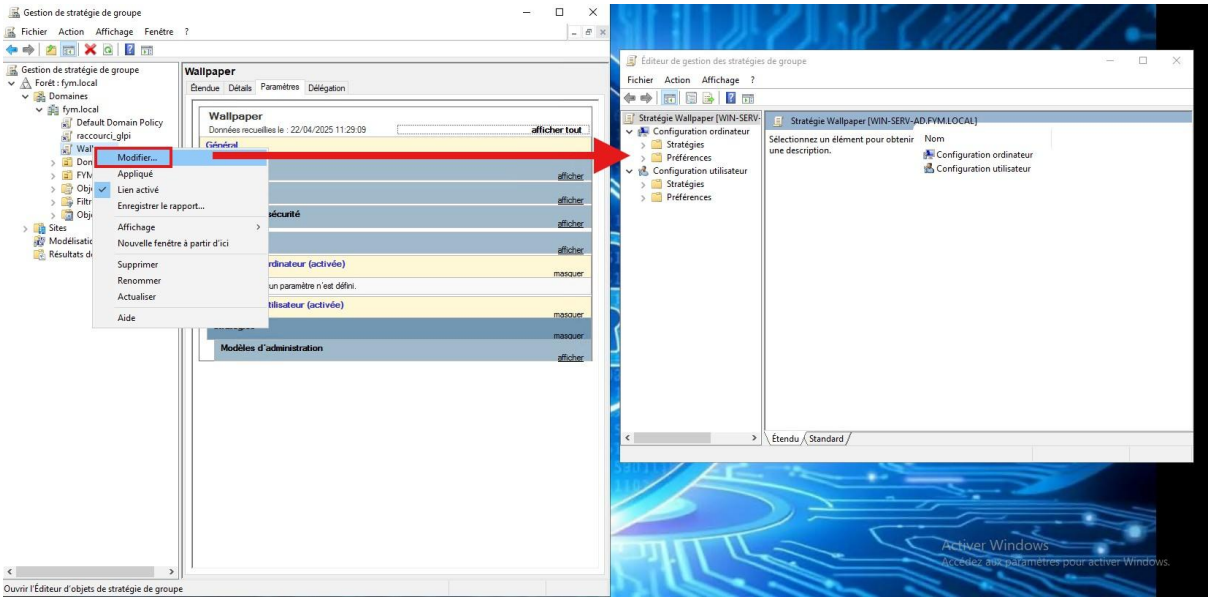
Avant de continuer la configuration de notre objet, prenons le temps de réaliser une courte étape qui sera utile pour toutes les GPO suivantes. En effet, lorsque l’on clique sur notre objet GPO puis que l’on clique sur l’onglet “Paramètres” dans le menu de droite, on obtient systématiquement ce message d’erreur avant de pouvoir accéder aux paramètres de la GPO en question :



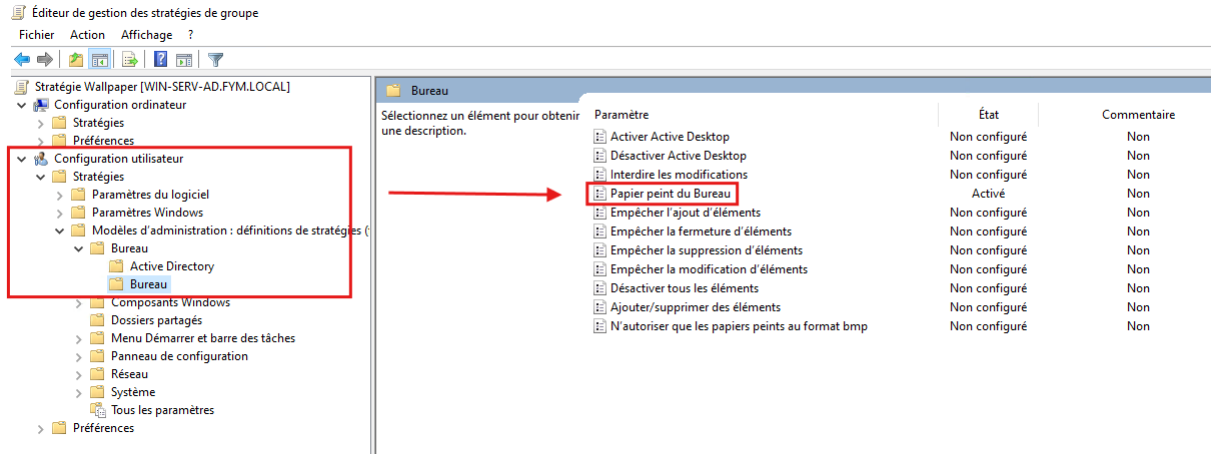
Pour ne plus avoir ce message dérangeant, il faut se rendre dans le gestionnaire de serveur, puis cliquer sur “Serveur local” dans le menu de gauche. Ensuite on cherche la ligne “Configuration de sécurité renforcée d’Internet Explorer” et on clique sur “Actif” juste à droite. Une boîte de dialogue va s’ouvrir (comme sur la capture ci-dessous), et désactive les deux cases :



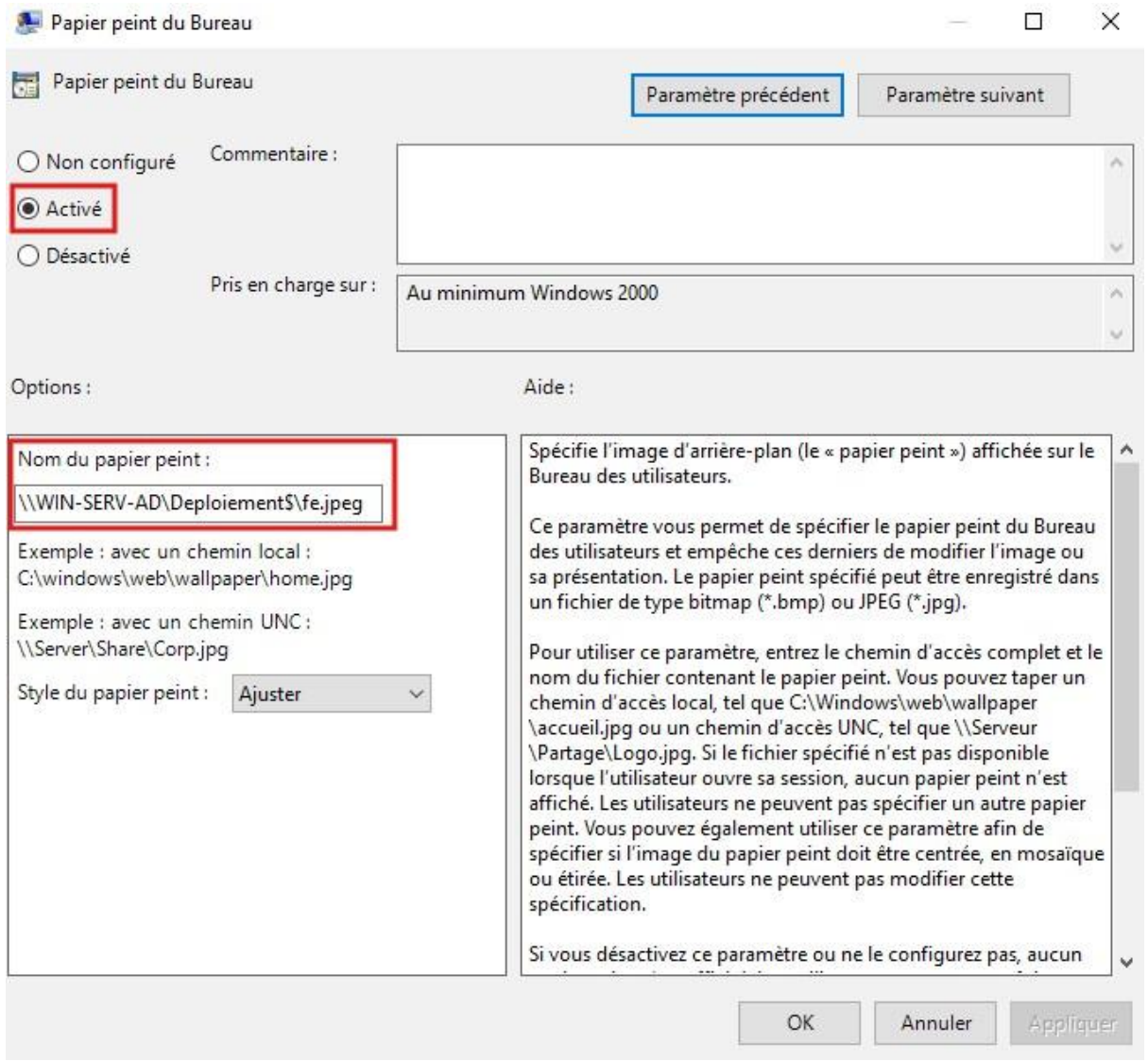
Pour que les modifications soient actives, il faut fermer la fenêtre des GPO et la rouvrir. Maintenant, revenons à la configuration de notre GPO. On fait un clic droit sur notre objet GPO puis on clique sur “Modifier”. Suite à cela, une autre fenêtre va s’ouvrir (à droite sur la capture d’écran ci-dessous) :



C’est à partir de là que l’on va définir la nature de notre stratégie de groupe. Pour une GPO fond d’écran, on va dérouler à partir du menu “configuration utilisateur” jusqu’à arriver sur “Bureau” sur lequel on va cliquer, comme ci dessous :



Après avoir cliqué sur “Bureau”, dans le menu à droite, on double-clique sur “Papier peint du Bureau” :



On vérifie que la case “Activé” est bien cochée, puis on renseigne le chemin vers l’image. Le chemin doit être accessible par les utilisateurs, on renseigne donc un

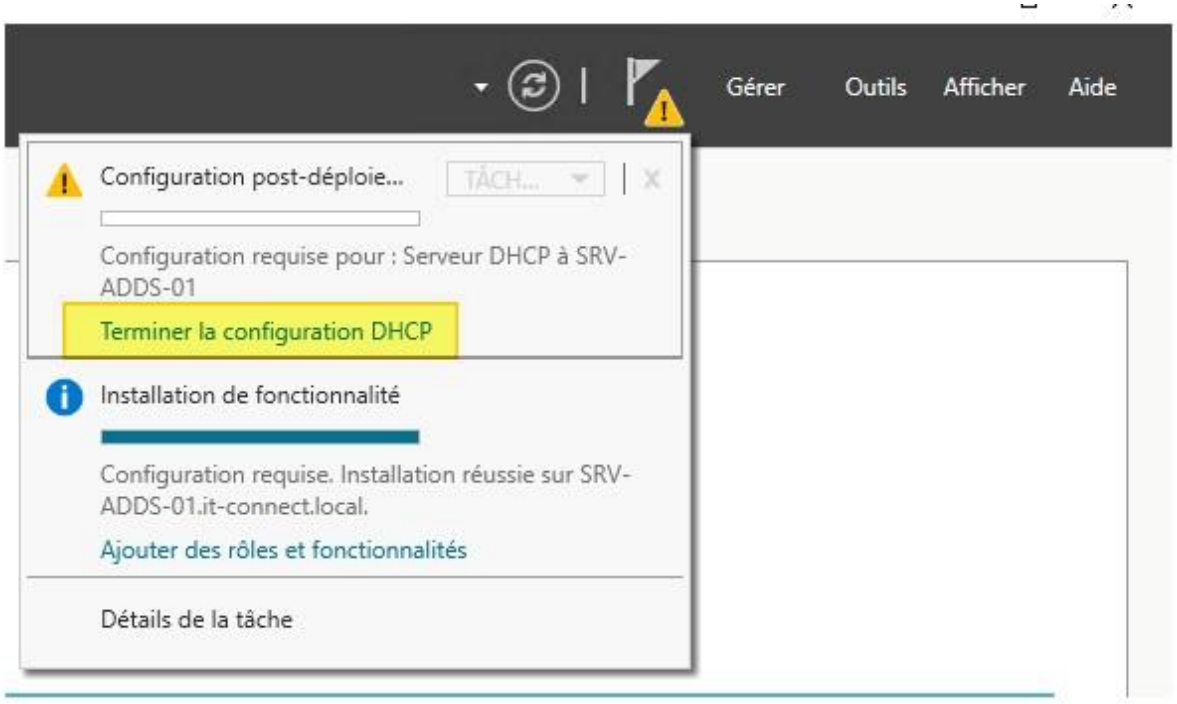
chemin UNC (Universal Naming Convention), autrement dit un chemin réseau vers le dossier partagé, et non pas le chemin local. Pour ce faire, on met en premier “\\” avec le nom du serveur puis le chemin vers l’image sans oublier l’extension. Puis on clique sur “Appliquer”.

Enfin, pour que les modifications soient appliquées sur les utilisateurs, il faut se déconnecter de la session et se reconnecter (attention à bien se déconnecter et à ne pas simplement verrouiller la session).

3. Service DHCP

3.1. Configuration du rôle DHCP

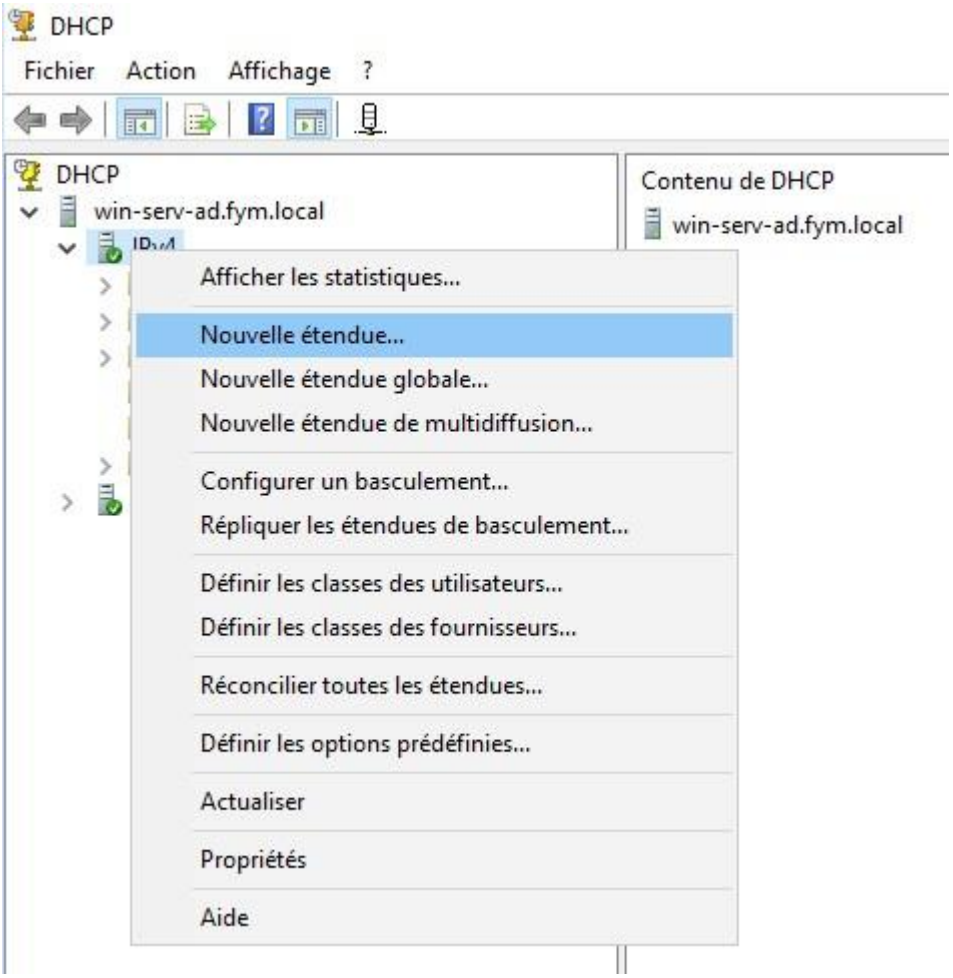
Le rôle DHCP étant déjà installé, nous allons le configurer en commençant par cliquer sur le triangle jaune en haut à droite, puis sur “Terminer la configuration DHCP” :



Ensuite, on sur suivant jusqu’à la fin en laissant les paramètres par défaut, notamment “Utiliser les informations d’identification de l’utilisateur suivant” avec le compte Administrateur du domaine.

Ensuite, on se rend dans le menu de gestion du serveur DHCP. Pour ce faire, on passe par le Gestionnaire de serveur → Outils → DHCP

Pour ajouter une nouvelle étendue DHCP, on clique droit sur IPv4 puis “Nouvelle étendue” :



Ensuite, on nomme notre étendue, puis on suit les étapes, en configurant les options que l'on souhaite. Dans notre cas, on configure :

- l'adresse de début et de fin de la plage distribuée et le masque de sous-réseau
- la durée du bail
- la passerelle par défaut
- le nom de domaine et le serveur DNS

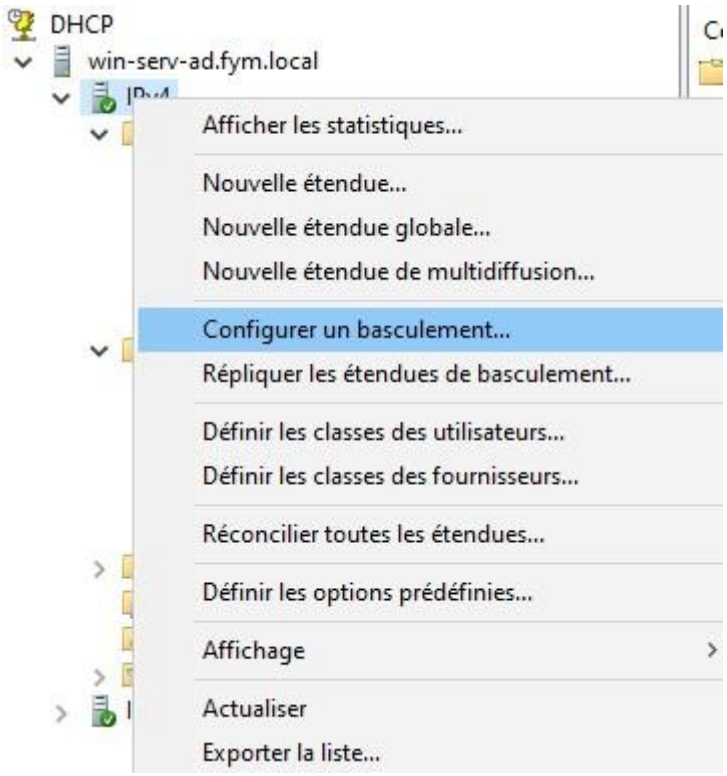
Si l'on veut faire une réservation DHCP, il suffit, une fois que l'étendue est créée et configurée de faire un clic droit sur "Réservations" en dessous du nom de l'étendue et de cliquer sur "Nouvelle réservation" et de suivre les étapes.

3.2. Redondance

Ici, nous allons voir comment mettre en place la redondance du service DHCP. Il nous faudra donc un deuxième serveur identique au premier. Dans notre cas, on prendra la 2ème VM sur laquelle on a déjà installé la redondance AD.

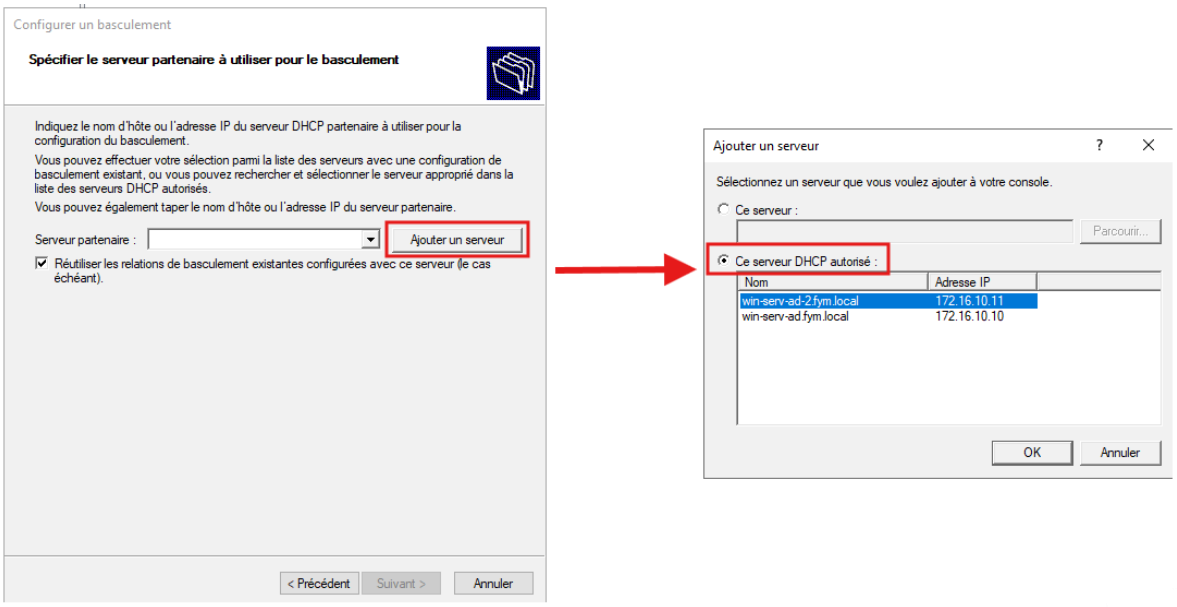
Ainsi, si l'une deux 2 machines tombe en panne ou subit un dysfonctionnement, le service sera toujours fonctionnel et les utilisateurs ne seront pas impactés.

Pour configurer la redondance, il faut faire un clic droit sur ce que l'on veut répliquer. Si l'on souhaite répliquer une seule étendue, on clique sur cette étendue. Si l'on souhaite répliquer toutes les étendues (comme dans notre cas), on clique sur "IPv4". Ensuite, on clique sur "Configurer un basculement" :



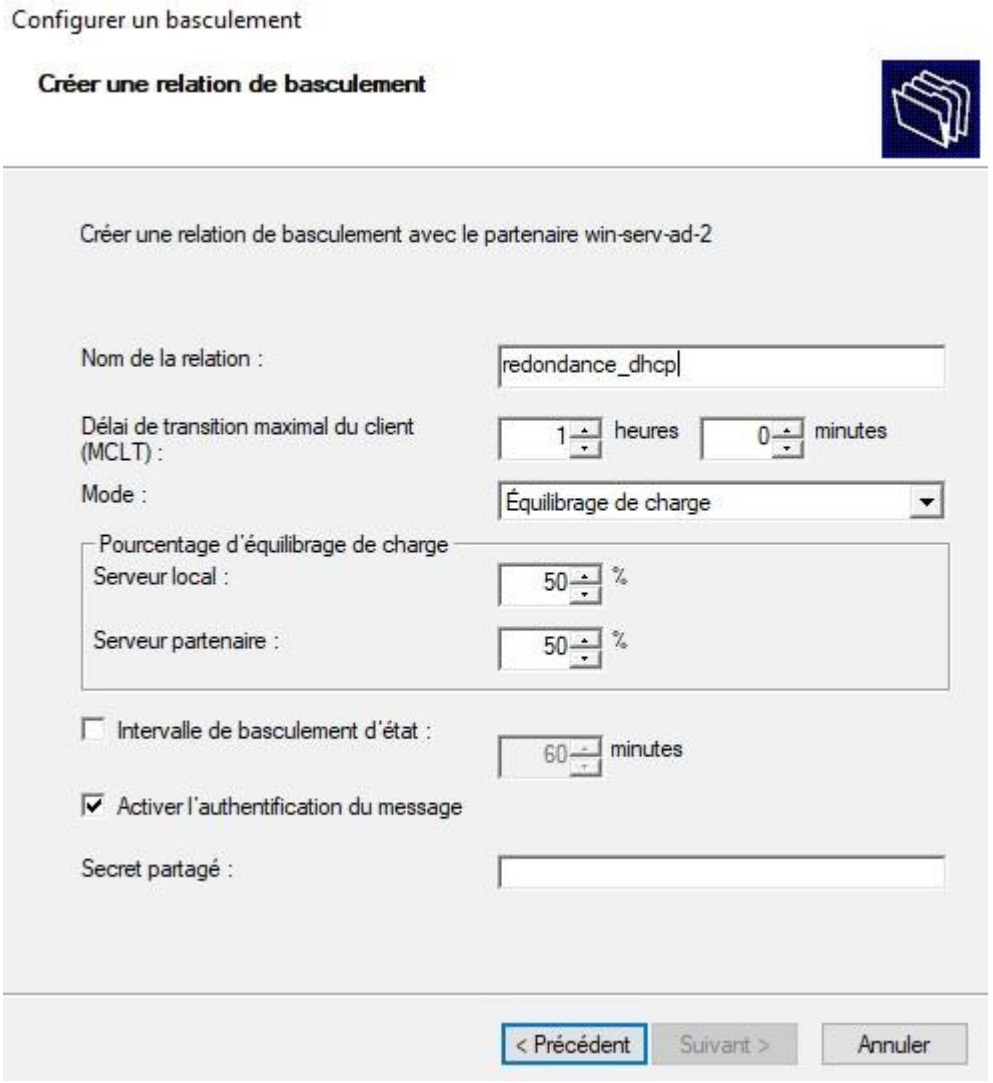
Ensuite, par défaut, toutes les étendues sont sélectionnées, donc on clique sur Suivant :

Puis on sélectionne le serveur secondaire sur lequel on souhaite répliquer les étendues :

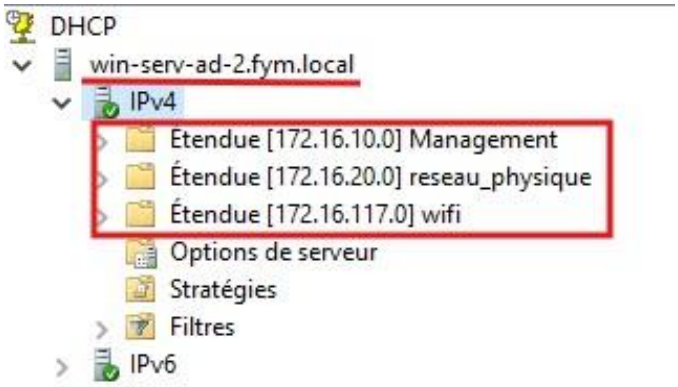


Enfin, avant de valider, on configure les dernières options, à savoir le nom de la relation de basculement, le délai MCLT (temps d'attente du serveur secondaire avant de prendre le contrôle des allocations IP), le mode de basculement (soit Équilibrage de charge, soit Serveur de secours) et enfin l'authentification entre les 2 serveurs

DHCP (facultatif). Concernant le mode, on a préféré le load balance (équilibrage de charge). Ce mode est surtout utile dans le cas d'une grande infrastructure et permet de répartir la charge sur deux serveurs et donc de ne pas surcharger un des deux serveurs pendant que l'autre n'est pas utilisé jusqu'à ce que le premier tombe en panne.



Après avoir validé, la redondance est effective. Pour vérifier cela, on se rend sur le serveur secondaire et on vérifie que les étendues que l'on répliquées apparaissent bien :



Désormais, chaque modification sur ces étendues (ajout ou suppression de réservation, nouveau bail etc) sera répliquée sur l'autre serveur, que cette modification ait été effectuée sur le serveur principal ou secondaire.
Cependant, si l'on ajoute une étendue autre que celles qui ont été répliquées, elle n'apparaîtra pas automatiquement sur l'autre serveur. Il faudra, juste après sa création, configurer le basculement pour celle-ci de la même manière que l'on vient de voir.

3.3. Méthode DORA

Afin de comprendre le fonctionnement du protocole DHCP, voici dans l'ordre les différentes étapes qui se produisent lorsqu'un client effectue une requête DHCP. On parle de méthode DORA (Discover, Offer, Request, Acknowledge) :

DHCP Discover : Le client (de source 0.0.0.0 car il n'a pas encore d'adresse IP) diffuse en broadcast (à toutes les machines du réseaux) qu'il recherche une configuration IP. Il fournit entre autres son adresse MAC.

DHCP Offer : Le serveur (182.160.10.1) répond avec une offre. Autrement dit, il propose au client une configuration IP disponible. Le client peut recevoir plusieurs offres s'il y a plusieurs serveurs DHCP sur le réseau.

DHCP Request : Le client répond au serveur (qu'il préfère) qu'il souhaite prendre cette configuration IP qui lui a été proposée

DHCP ACK : Le serveur confirme au client que la configuration IP lui a été attribuée avec succès. Après avoir reçu cet accusé de réception, le client configure son interface réseau et peut commencer à utiliser le réseau.