HEH.be
Sciences
et technologies

Avenue V. Maistriau 8a
B-7000 Mons
+32 (0)65 33 81 54
scitech-mons@heh.be

WWW.HEH.BE

Année académique **2021 - 2022**

UE : Windows Server

- **AA : Windows Server – Travaux pratiques**

Bachelier en informatique et systèmes
Orientation : Télécommunications et réseaux.

Yoan Pietrzak
yoan.pietrzak@heh.be

WALLONIE-BRUXELLES ENSEIGNEMENT
pôle hainuyer

Table des matières

1 Objectif du cours

1.1 Compétences :

- Collaborer à l'analyse et à la mise en œuvre d'un système informatique.
- Configurer et administrer les serveurs de bases d'un réseau local.

1.2 Contenu :

- Le protocole IPv4 et IPv6 ;
- Les systèmes d'exploitation Windows (clients et serveurs) ;
- Configuration et installation de Windows 2012 Serveur.
- Le serveur DHCP
- Le serveur DNS
- Le serveur de fichiers
- Introduction à l'Active Directory

1.3 Evaluation :

La répartition des points se fait comme suit :

- 60% pour la partie théorique (Monsieur Naizy)
- 40% pour la partie pratique (35% lors de l'examen et 5% de participation aux travaux pratiques)

2 Hyper-V

Hyper-V est un système de virtualisation tel que Virtual Box et VmWare. Il est disponible sur les systèmes d'exploitation serveur depuis Windows Server 2008.

Concernant vos postes, il faut savoir que l'installation d'Hyper-V n'est disponible que sur les versions de Windows 8, Windows 8.1 et Windows 10 (éditions Pro et Enterprise uniquement).

Les prérequis matériels au niveau de la machine sont les suivants :

- Posséder un processeur 64bits ;
- Supporter SLAT[1] ;
- La quantité de mémoire sur la machine hôte doit être supérieure à celle allouée aux machines virtuelles.

Attention de bien activer dans votre BIOS la virtualisation au niveau matériel.

[1] Second Level Address Translation.

2.1 Composants d'une machine virtuelle sous Hyper-V :

Pour accéder au paramètres de votre machine virtuelle, il vous suffit de sélectionner la machine en question et

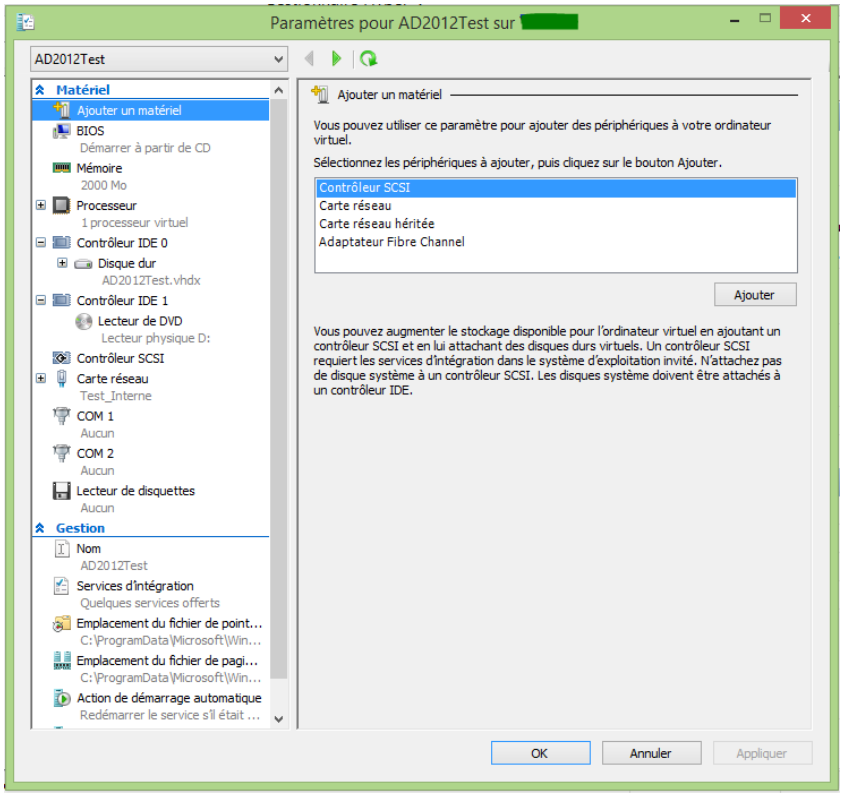

Figure 1 : Composants d'une machine virtuelle.

- **Le BIOS** : permet de configurer l'ordre de boot ;
- **La Mémoire** : Permet d'attribuer une certaine quantité de mémoire vive à la machine. On peut également allouer la mémoire de manière dynamique[2] ;
- **Le processeur** : Il est possible d'allouer un ou plusieurs processeurs à la machine ;
- **Contrôleur IDE** : deux contrôleurs peuvent être configurés pour la VM. Chacun possèdent deux disques au maximum.
- **Contrôleur SCSI** : En ajoutant un contrôleur SCSI, il est possible d'ajouter des disques durs ou des lecteurs DVD.
- **Carte réseau** : par défaut la carte réseau n'est pas héritée, ce qui permet un meilleur débit mais empêche la machine d'effectuer un boot PXE. Pour pallier à ce problème, il faut ajouter une carte réseau héritée.

[2] Ce point sera détaillé au chapitre 2.2 Gestion de la mémoire dynamique avec Hyper-V

2.2 Gestion de la mémoire dynamique avec Hyper-V :

La mémoire dynamique permet d'allouer une quantité de mémoire minimum. Si votre VM à besoin à un moment de plus de ressource, elle sera autorisée à demander une quantité supplémentaire de mémoire. Cette dernière ne pourra pas excéder la quantité maximale accordée.

On peut donc modifier la valeur minimale et maximale de la mémoire dynamique de la machine virtuelle. Cette opération peut également être réalisée lorsque la VM est en fonctionnement.

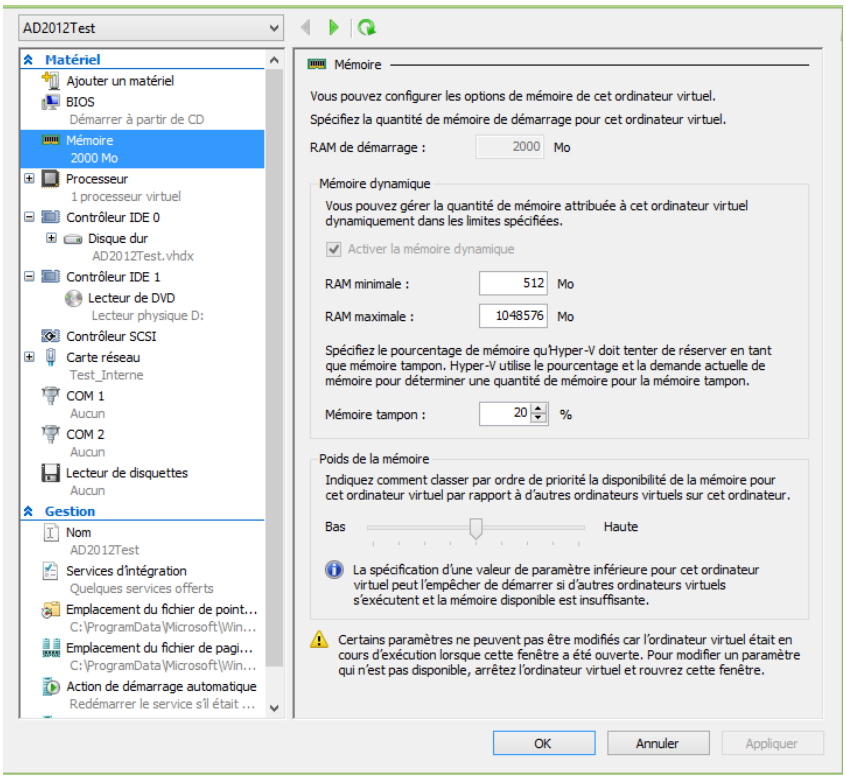

Figure 2 : Mémoire dynamique.

La mémoire tampon permet à la machine virtuelle de se voir attribuer une quantité de RAM supplémentaire en cas de besoin.

2.3 Les disques virtuels et leur gestion :

A partir de la version Windows Server 2012, Hyper-V utilise un nouveau type de fichier, le VHDX. Ce type de fichier est moins sensible à la corruption du fichier suite à une coupure inattendue (tel qu'une coupure de courant par exemple) du serveur. Il est possible de convertir les fichiers VHD[3] existants en VHDX (via ***l'assistant modification de disque dur*** – dans l'onglet « ***Action*** », « ***Modifier le disque*** »).

[3] VHD : Virtual Hard Disk, prédécesseur de VHDX.

Il existe différents types de disques virtuels :

- ***Disque de taille fixe*** : la taille totale est réservée sur le disque. On peut donc limiter la fragmentation sur le disque dur de la machine hôte et améliorer les performances. L'inconvénient est que ce type disque prend de l'espace disque même si le fichier VHD est vide.
- ***Disque de taille dynamique*** : dans ce cas, on définit une taille maximale de fichier. La taille du fichier augmentera en fonction du contenu jusqu'à la taille maximale.
- ***Disque de type pass-through*** : permet à une machine virtuelle d'accéder directement au disque physique de votre machine. Le disque est considéré comme un disque interne pour le système d'exploitation de la machine virtuelle. Je vous déconseille toutefois de travailler de cette manière pour l'élaboration de vos manipulations.

2.4 Les snapshots dans Hyper-V :

Un snapshot correspond à une « photo » de votre machine virtuelle. Ce qui veut dire que vous conservez une copie de votre machine à un instant x.

Celui-ci est contenu dans un fichier portant l'extension AVHD ou AVHDX. Vous pouvez effectuer celui-ci en sélectionnant la machine et en cliquant sur « ***Point de contrôle*** » dans l'onglet « ***Actions*** ».

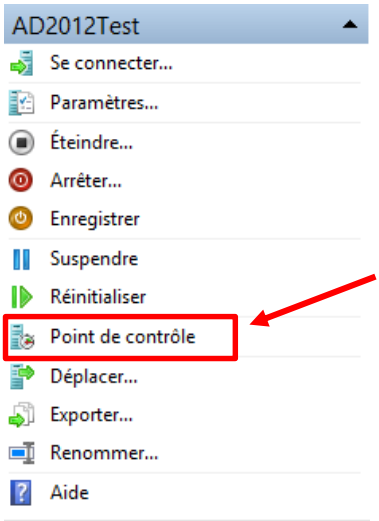

Figure 3 : Snapshot.

Il faut savoir qu'un snapshot ne remplace pas une sauvegarde. Le snapshot vous permet par exemple, en cas de problème, de revenir à un état stable de votre machine.

2.5 Gestion des réseaux virtuels :

Il existe plusieurs types de réseaux qui peuvent permettre aux différentes machines de communiquer entre elles ou avec des équipements externes à votre machine hôte.

Voici les 3 types de réseaux :

- ***Externe*** : Dans ce cas de figure, vous utilisez la carte réseau de la machine hôte dans la machine virtuelle. Ce qui permet à votre machine virtuelle d'accéder aux équipements du réseau physique.
- ***Interne*** : permet de créer un réseau entre la machine physique et les machines virtuelles. Dans ce cas de figure, il est impossible pour les machines du réseau physique de communiquer avec les machines virtuelles.
- ***Privé*** : La communication peut se faire uniquement entre les machines virtuelles.

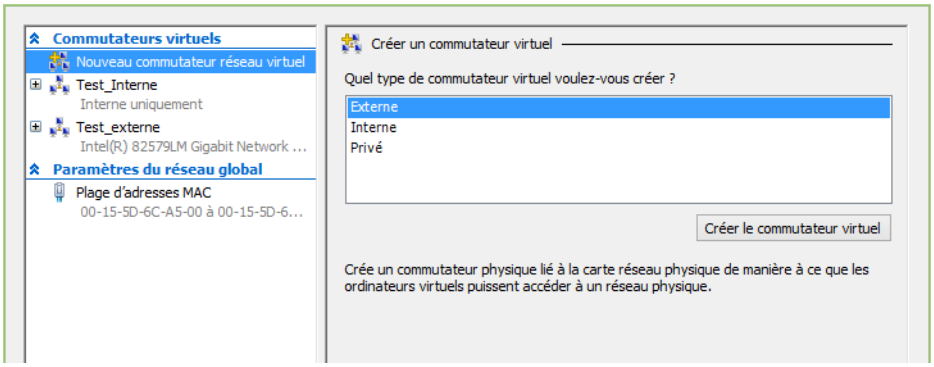

Figure 4 : Gestionnaire de commutateur virtuel.

Afin de créer ou modifier un commutateur virtuel, il suffit de sélectionner dans l'onglet « ***Action*** », l'option « ***Gestionnaire de commutateur virtuel*** ».

2.6 Installation de la fonctionnalité Hyper-V :

Dans le cas ou Hyper-V n'est pas installé sur votre machine, il vous suffit d'aller dans « ***Panneau de configuration*** », sélectionner « ***Programmes et fonctionnalités*** ». Dans ce dernier, sélectionner « ***Activer ou désactiver des fonctionnalités Windows*** ».
Ensuite, il suffit de cocher la fonction « Hyper-V ».

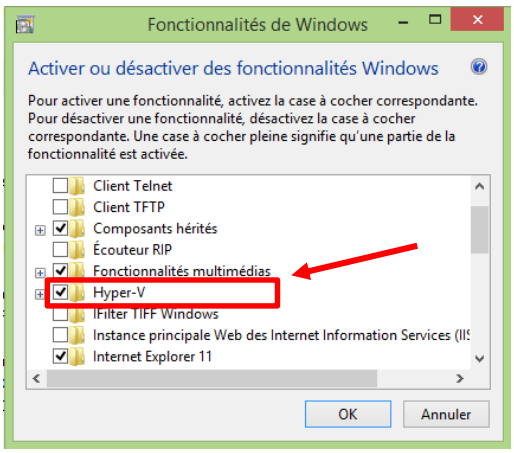

Figure 5 : Ajout de la fonction Hyper-V.

2.7 Configuration de votre VM pour Windows 2012 R2 :

Lors de l'installation de votre machine virtuelle Windows 2012 R2, il faudra respecter les prérequis du système d'exploitation.
Je vous conseille donc d'utiliser la configuration matérielle suivante pour votre VM Windows 2012 R2 :

- ***Processeur :*** une architecture 64 bits avec un minimum de 1,4GHz ;
- ***Mémoire vive*** : le minimum requis est de 512Mo mais 1Go est conseillé.
- ***Espace disque*** : Pour une installation de base sans rôle installé nécessite 15Go. Il faudra donc prévoir un espace suffisant en fonction des rôles du serveur.

3 Windows Server 2012 R2

Avant d'entamer ce point, il vous faudra au préalable télécharger l'ISO de Windows Server 2012 R2 (en anglais de préférence).

Plusieurs versions de Windows sont disponibles :

- ***Edition Standard*** : Pour des environnements physiques, avec peu ou pas de virtualisation.
- ***Edition Datacenter*** : Pour des Datacenter avec forte virtualisation et les Clouds.
- ***Edition Essentials*** : Pour des petites entreprises comptant jusqu'à 25 utilisateurs et 50 appareils.

Il est également possible d'installer Windows Server 2012 R2 en mode Core. Ce mode est dépourvu d'interface graphique et ne peut être gérer qu'à partir de commande DOS et Powershell. Ce type d'installation permet ainsi de réduire les ressources matérielles nécessaires.

3.1 Installation de Windows Server 2012 R2 :

Dans la console Hyper-V, double cliquez sur la machine virtuelle et ensuite cliquez sur le bouton démarrer.

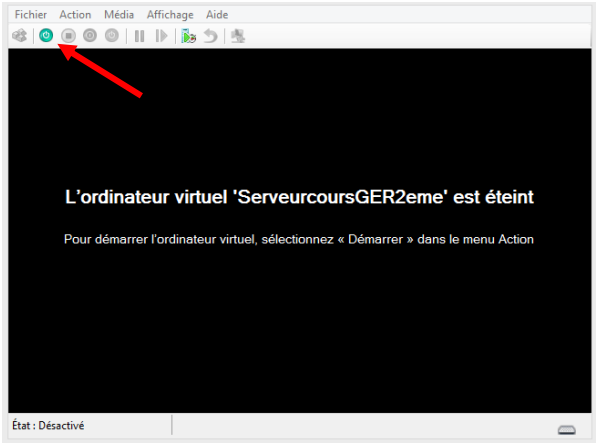

Figure 6 : Console Hyper-V.

Votre machine virtuelle démarre et l'installation de Windows Server 2012 R2 débute.

Première chose, configurer correctement votre clavier. Par défaut, le clavier est en « ***US*** » et l'option « ***Time and currency format*** » est en « ***English (United States)*** ».

Pour ce qui est de la langue, il faut absolument travailler en anglais.

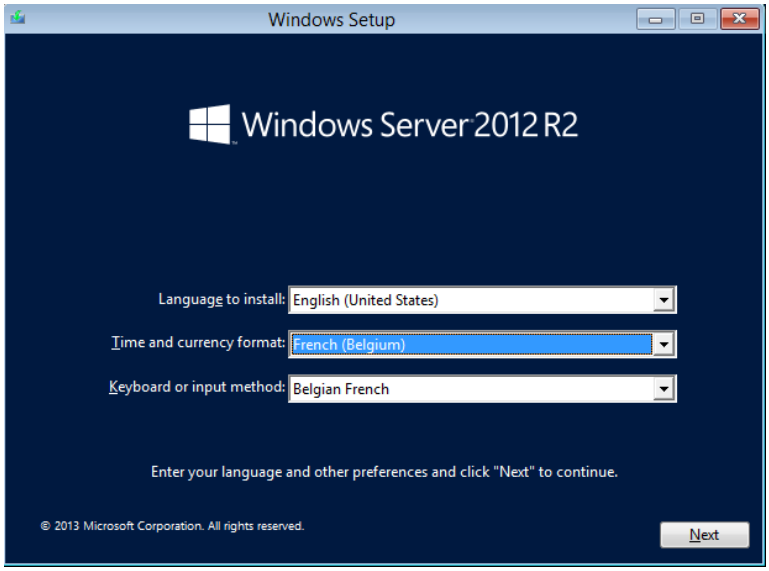

Figure 7 : Configuration clavier.

Une fois ces options configurées, cliquez sur « ***Next*** ». Ensuite cliquez sur « ***Install Now*** ».

Il faut maintenant sélectionner le système d'exploitation correct pour votre machine. Comme cité précédemment, il y a plusieurs versions disponibles. Nous allons choisir dans notre cas la version « ***Standard*** ». ATTENTION de ne pas prendre le mode Server Core Installation.

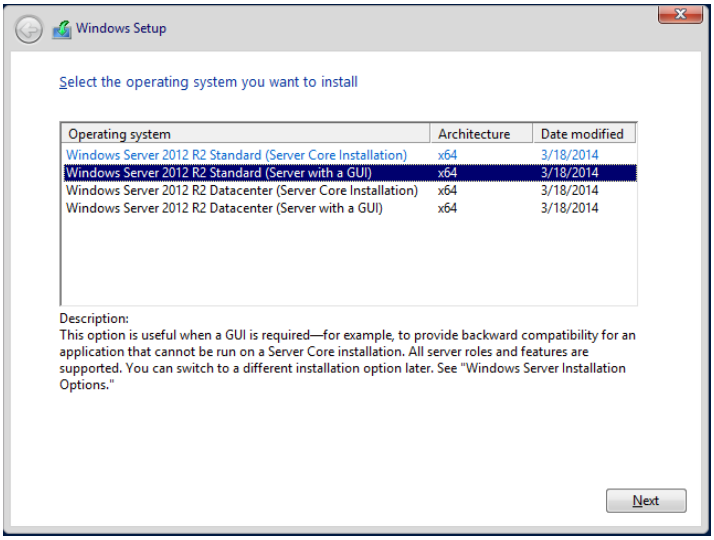

Figure 8 : Choix du système d'exploitation.

Cliquez sur « ***Next*** ». Maintenant sélectionnez le type d'installation que vous voulez réalisée. Je vous conseille de sélectionner l'installation « ***Custom : Install Windows only***

(advanced) ». Ce type d'installation vous permet d'effectuer plusieurs configurations telles que formater, créer ou supprimer une partition, …

Cela vous permettra également de ne plus garder de trace d'une installation ultérieure.

Dans notre cas, vous pouvez aller devoir créer une nouvelle partition et la formater. Ensuite cliquer sur « ***Next*** ».

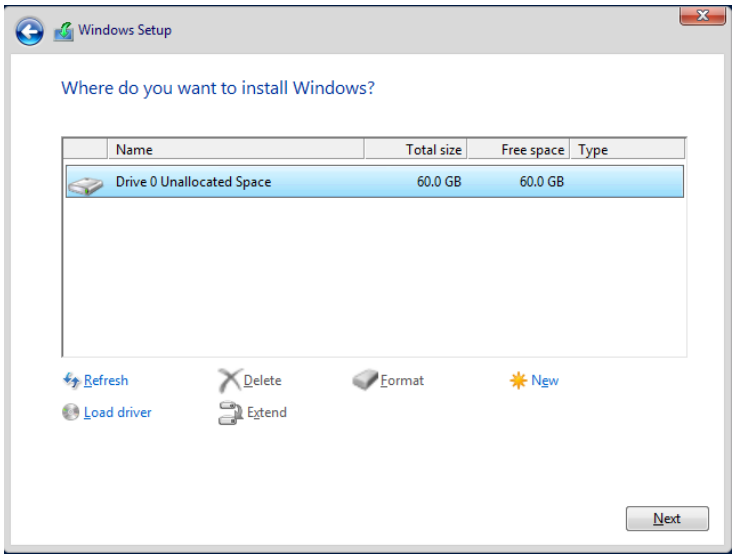

Figure 9 : Windows Setup.

Une fois l'installation terminée, il vous faudra définir un mot de passe pour la session administrateur, changer le nom de la machine et lui attribuer une adresse IP fixe.

3.2 Configuration du nom et de l'IP du serveur :

3.2.1 Changer le nom du serveur :

Dans un premier temps, nous allons changer le nom du serveur. En effet, le nom par défaut peut-être un peu lourd à retenir. Idéalement on va renommer son serveur en fonction de son usage afin de l'identifier facilement.
Pour ce faire, il y a plusieurs possibilités :

- A l'aide de la commande « ***sysdm.cpl*** », cliquer sur le bouton « ***Change*** » et modifier le nom de votre serveur.

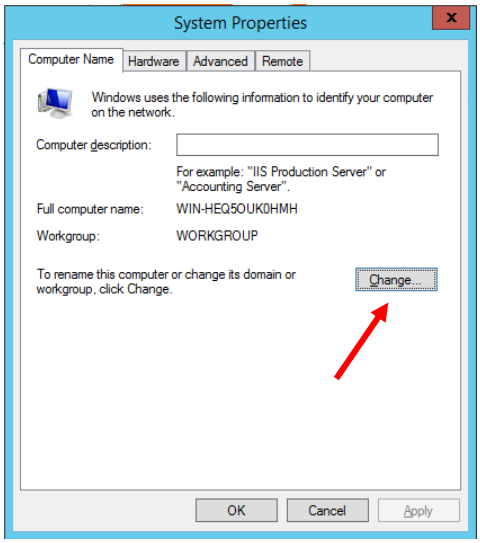

Figure 10 : System Properties.

- A l'aide de la console de gestion du serveur (Console Server Manager – cf. point 3.3).

Dans celui-ci, cliquer sur « ***Configure this local server*** » et ensuite cliquer sur le nom du serveur. Comme dans la méthode précédente, cliquer sur « ***Change*** » et modifier le nom du serveur.

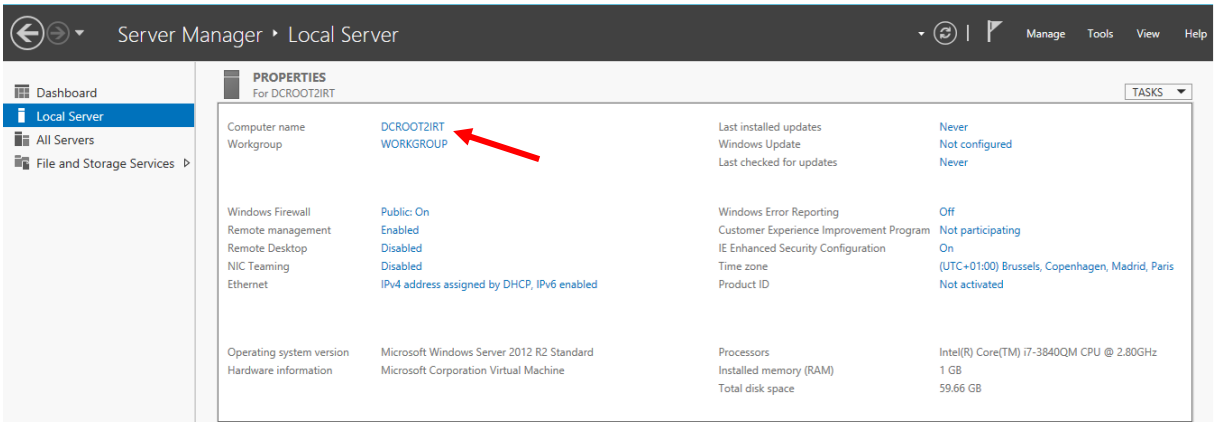

Figure 11 : Local Server – Changement de nom.

3.2.2 Attribuer une adresse IP au serveur :

Encore une fois, il existe plusieurs possibilités pour attribuer une IP à votre serveur.
En voici quelques-unes d'entre elles :

- En mode graphique à l'aide de la commande « ***ncpa.cpl*** », cliquer droit sur la connexion à configurer et sélectionner « ***Properties*** ».

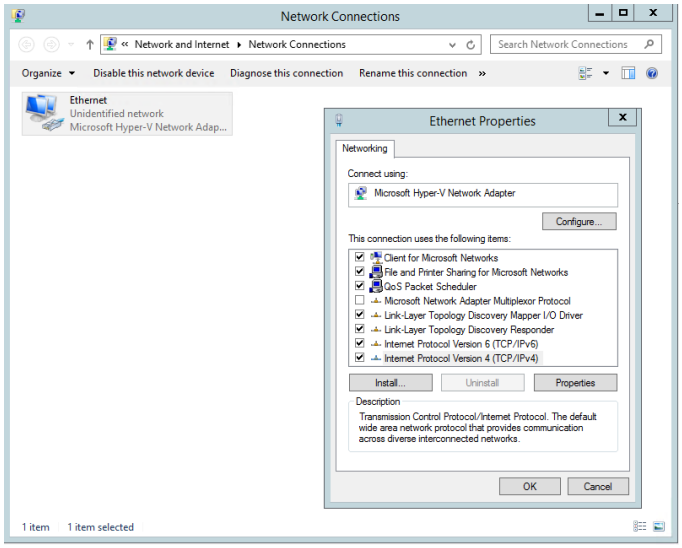

Figure 12 : Network Connections.

Ensuite, sélectionner « ***Internet protocol Version 4 (TCP/IPv4)*** » et cliquer sur « ***Properties*** ». Cocher la case « ***Use the following IP address*** » et attribuer une adresse IP ainsi qu'un masque de sous-réseau à votre carte réseau. Dans un premier temps, il ne sera pas nécessaire de spécifier une adresse pour le DNS.

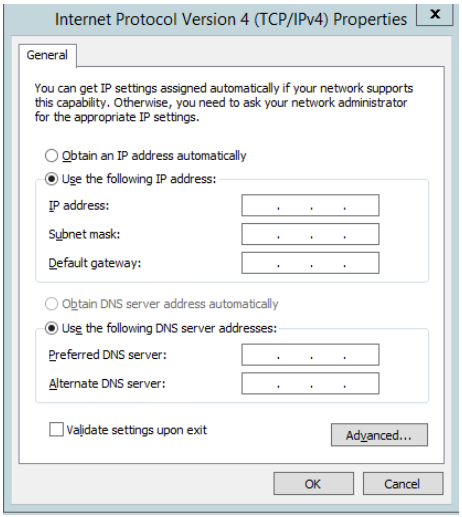

Figure 13 : Configuration de votre carte réseau.

- A l'aide de la commande ***netsh*** dans l'invite de commande.
  Dans un premier temps, on peut afficher les différentes connexions afin d'identifier la connexion à configurer :

  Netsh interface ipv4 show interfaces

  Ensuite afin d'attribuer l'adresse il faudra taper la commande suivante :

  Netsh interface ipv4 set address name="Ethernet" source=static 192.168.1.1 255.255.255.0

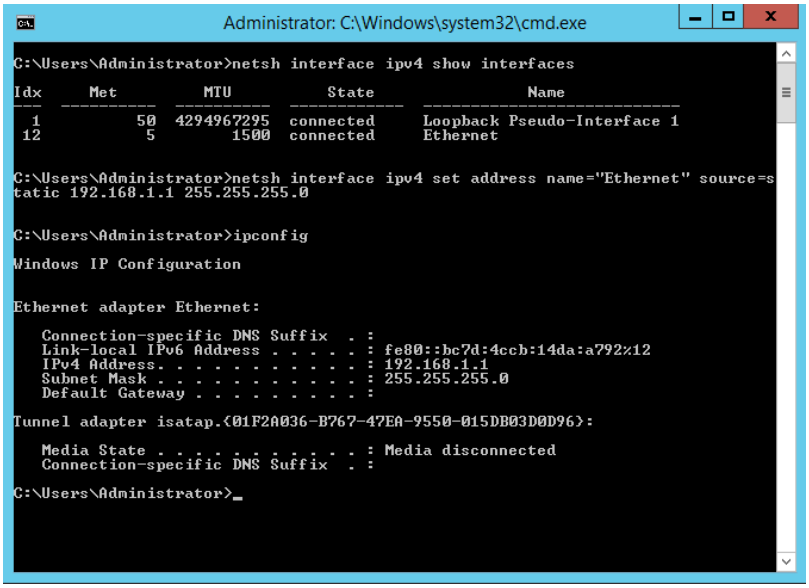

Figure 14 : Ajout d'une IP avec Netsh.

- A l'aide des commandes « ***Powershell*** ». Soit via l'interface powershell, soit en tapant la commande « ***powershell*** » dans l'invite de commande. Entrer la commande suivante afin d'afficher les différentes cartes réseaux :

  Get-NetIPInterface

  Ensuite taper la commande suivante afin d'effectuer la configuration IP de votre serveur :

  New-NetIPAddress -InterfaceIndex <ifIndex> -IPAddress 192.168.1.1 -PrefixLength 24

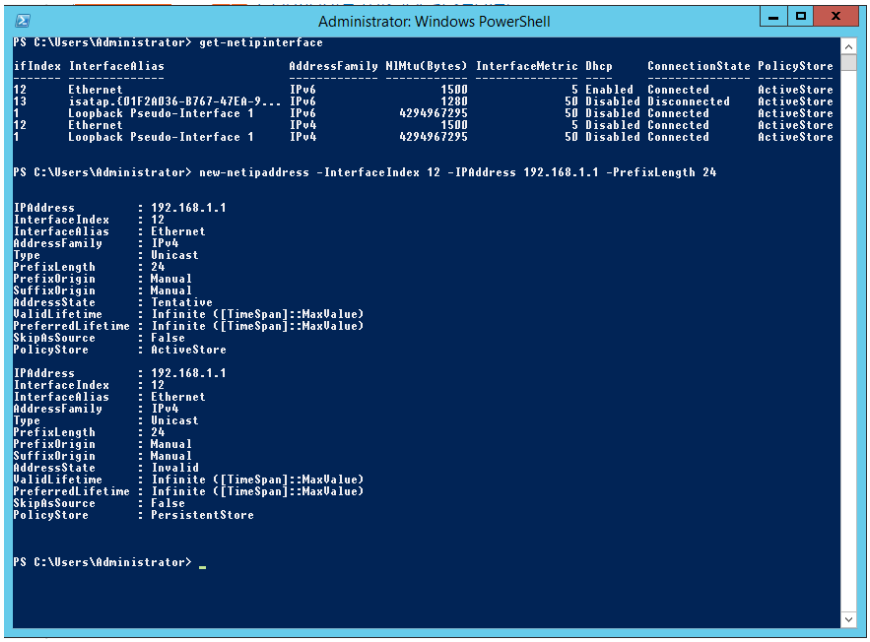

Figure 15 : Ajout d'une IP avec Powershell.

3.3 Console Server Manager :

La console « ***Server Manager*** » permet la gestion de l'ensemble du serveur. Elle permet entre autre l'ajout et la suppression de rôle mais aussi la configuration du serveur même.

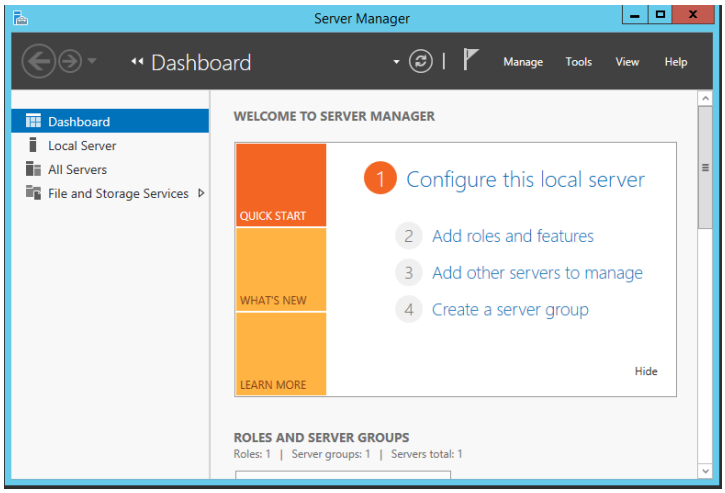

Figure 16 : Server Manager.

La console permet également de s'assurer rapidement qu'aucun problème n'est présent sur le serveur. Comme on peut le voir dans la figure ci-dessous, les rôles ne présentent aucuns problèmes et fonctionnent correctement.

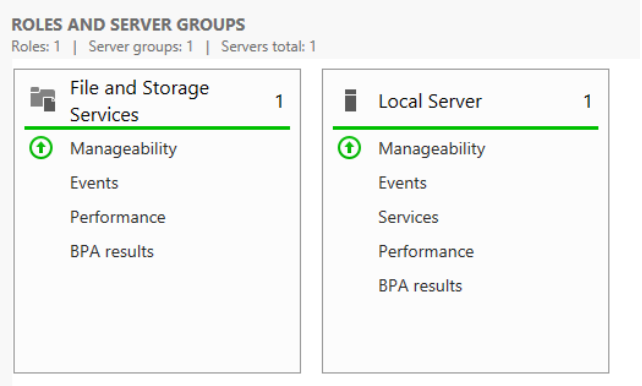

Figure 17 : Tableau de bord.

Les points audités sont les suivants : Evènements, Services, Performances et résultats BPA.

Si par exemple le point « ***Evènement*** » est précédé d'un 1, cela signale à l'administrateur qu'un point est à vérifier. En cliquant sur « ***Evènements*** », une fenêtre présentant le détail de l'évènement apparait.

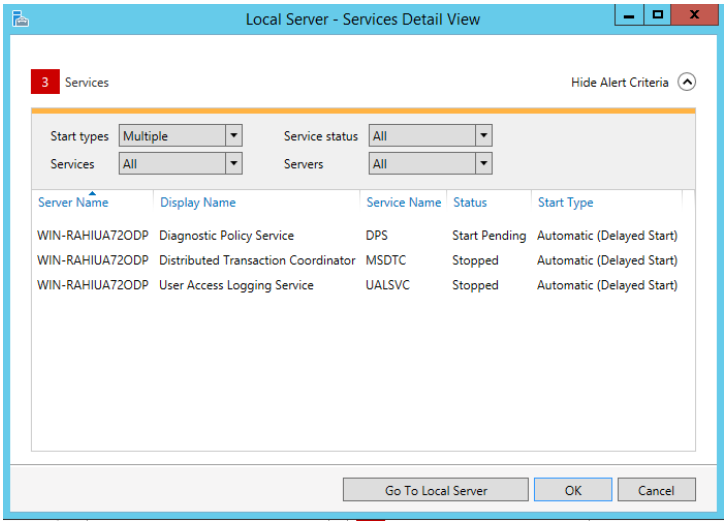

Figure 18 : Détail des services.

On peut donc très rapidement visualiser une erreur et intervenir sur le problème rapidement.

3.3.1 Ajouter un rôle via la console :

Pour ajouter un rôle au serveur c'est assez simple, il suffit de cliquer sur « ***Manage*** » et de sélectionner « ***Add Roles and Features*** ». Pour supprimer un rôle vous procéder de la même manière mais en sélectionnant « ***Remove Roles and Features*** ».

En sélectionnant l'ajout d'un rôle, l'utilitaire d'ajout de rôles démarre, celui-ci vous demandera de sélectionner le server sur lequel vous voulez installer le rôle. Dans notre cas, il ne sera pas difficile de choisir étant donné que nous n'avons qu'un seul serveur.

Ensuite, il faudra simplement sélectionner le rôle à installer et continuer la procédure.

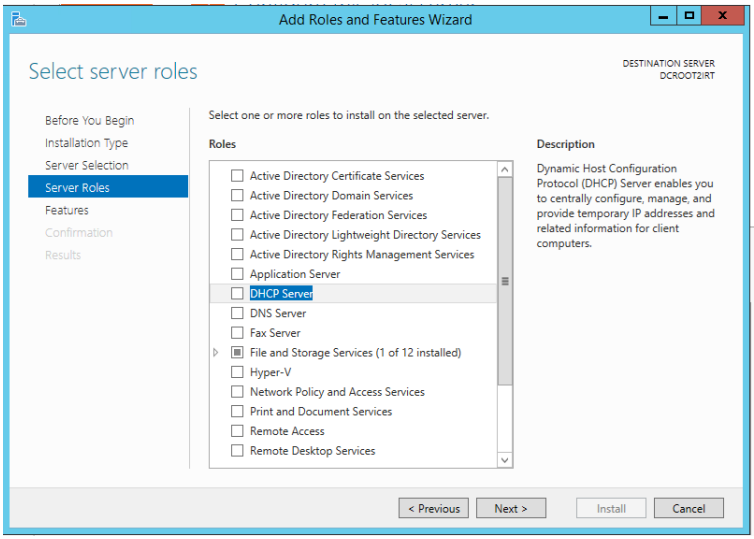

Figure 19 : Ajout d'un rôle.

3.3.1 Paramétrer un rôle à partir de la console :

Lorsque l'installation d'un rôle est réalisée, il est bien entendu intéressant de pouvoir configurer celui-ci. Pour ce faire, il suffit de cliquer sur « ***Tools*** » et de sélectionner le rôle à configurer.

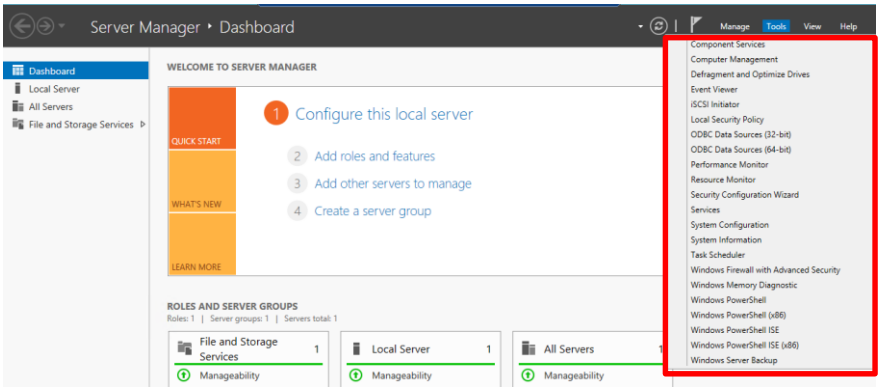

Figure 20 : Configuration d'un rôle.

4 Installation et configuration du rôle DHCP

Le serveur DHCP permet d'attribuer de manière automatique la configuration IP d'une ou plusieurs machines. Cette configuration inclue donc : l'adresse IP, le masque de sous-réseau, la passerelle par défaut ainsi que le DNS.
Un bail est également associé à cette configuration. Celui-ci permet de limité la durée d'utilisation de cette configuration à quelques heures, quelques jours, …

Pour rappel, afin d'obtenir un bail DHCP, le client et le serveur effectuent un échange de trame :

- Le client envoie un broadcast (DHCPDISCOVER) à tous les ordinateurs du réseau.
- Seul le serveur DHCP peut répondre à cette trame. Il renvoi comme réponse une trame DHCPOFFER. Dans cette trame, une configuration IP est donnée au client.
- Le client diffuse alors une trame DHCPREQUEST au serveur DHCP pour l'avertir qu'il accepte la configuration proposée.
- L'adresse IP est stockée dans la base de données du serveur et celui-ci valide la transaction en envoyant un DHCPACK au client.

4.1 Installation du rôle DHCP :

Lors de l'ajout de rôle, il suffit de cocher l'option « ***DHCP Server*** » et de cliquer sur « ***Install*** ».

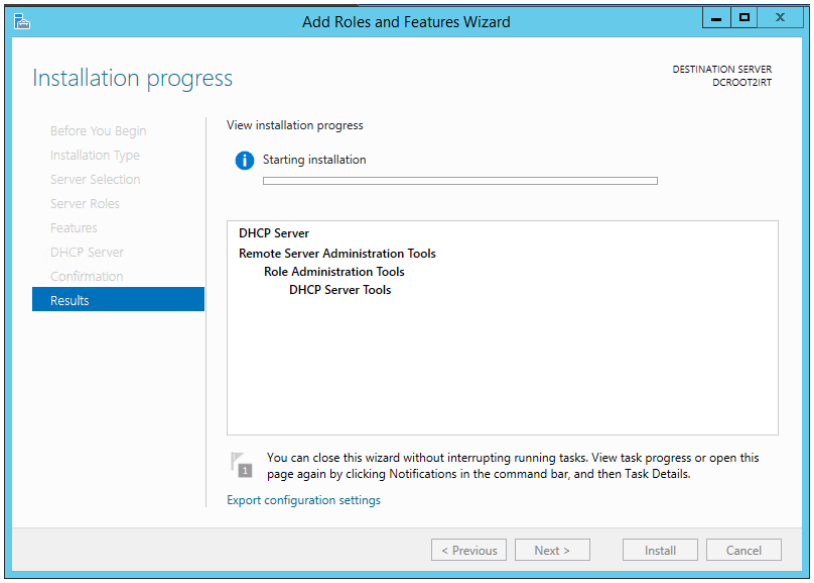

Figure 21 : Installation du rôle DHCP.

Une fois l'installation terminée, il faut bien entendu configurer le serveur DHCP. On peut d'ailleurs le constater dans la console dans la zone de notification. Prenez l'habitude de vérifier les différentes notifications figurants dans cette zone surtout lorsque vous installé une nouvelle fonctionnalité. Cliquer sur « ***Complete DHCP configuration*** » afin de finaliser l'installation du DHCP (voir figure ci-dessous)

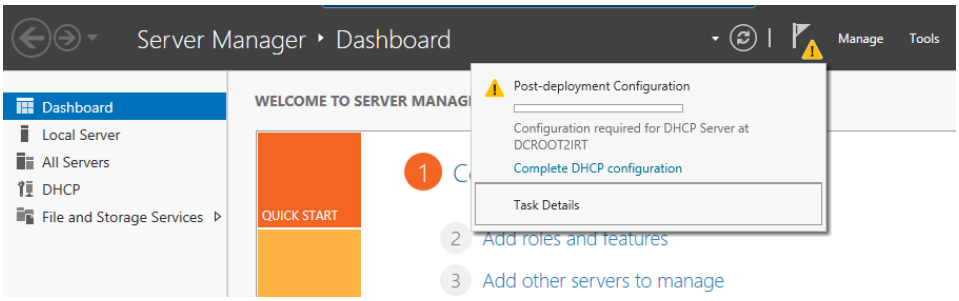

Figure 22 : Zone de notification.

Afin de configurer votre DHCP, vous avez deux possibilités. Soit via la zone de notification en cliquant sur « ***Complete DHCP configuration*** », soit en allant dans le menu « ***Tools*** » et en ouvrant la console DHCP.
Dans un premier temps, nous allons créer une nouvelle étendue. Pour ce faire, cliquer droit sur « ***IPv4*** », « ***New Scope*** ».

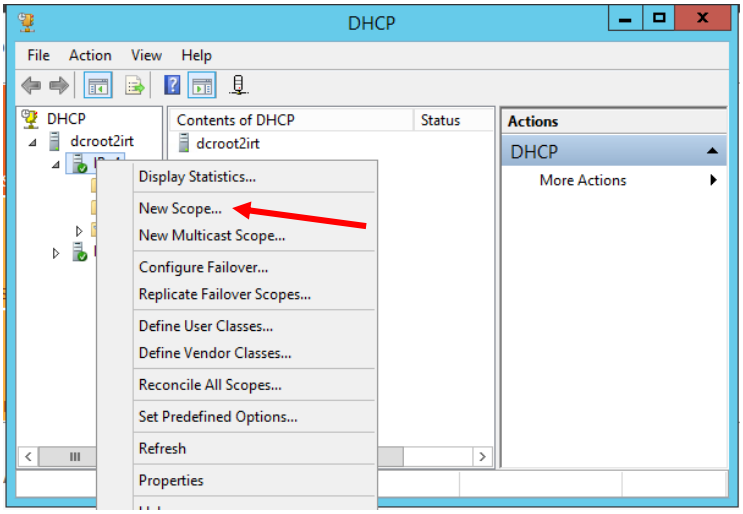

Figure 23 : Nouvelle étendue.

L'étendue va contenir un pool d'adresses IP (ainsi que le masque de sous-réseau) pouvant être distribuées aux machines clientes.
Durant la configuration de l'étendue, il faudra également configurer le bail. Il est également possible de configurer une plage d'exclusion. Cette dernière définit les adresses IP qui doivent être exclus du pool d'adresses attribuables.

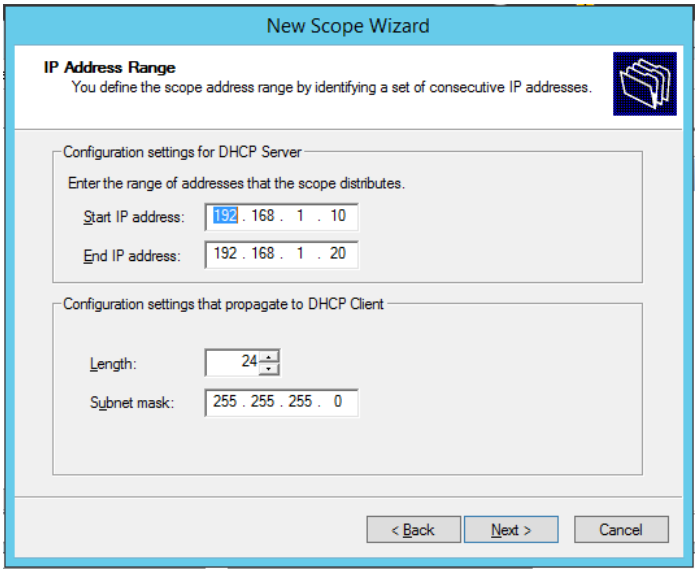

Figure 24 : Configuration du pool d'adresses.

Il reste à configurer les options d'étendues.

4.2 Configuration des options d'étendue :

Les options d'étendue sont les options supplémentaires que vous voulez envoyer en plus de l'adresse IP et du masque de sous-réseau.
Ces options sont par exemples la passerelle par défaut, le serveur DNS, …

Afin de configurer les options d'étendue, cliquer droit sur « ***Scope Options*** » et sélectionner « ***Configure Options*** ». Dans la figure ci-dessous, une option « ***Router*** » est définie. Il s'agit de la passerelle par défaut.

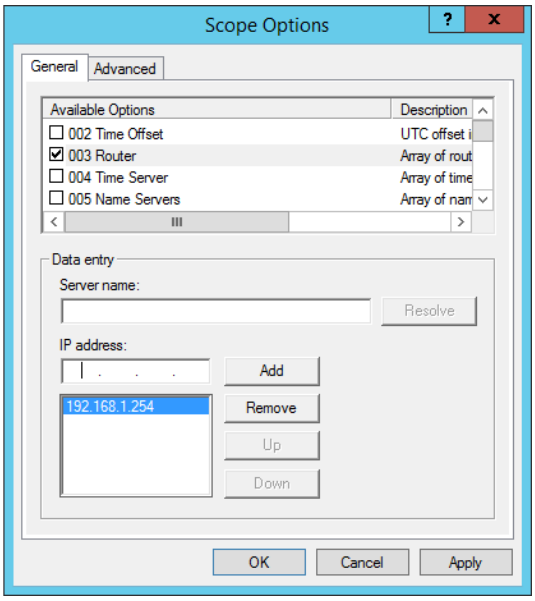

Figure 25 : Configurations des options d'étendue.

4.3 Création d'une classe utilisateur :

Dans un premier temps, cliquer droit sur « ***IPv4*** », « ***Define User Classes*** ». Cliquer sur « ***Add*** » et entrer un nom à la classe utilisateur. Dans la partie « ***ASCII*** », entrer un identifiant.

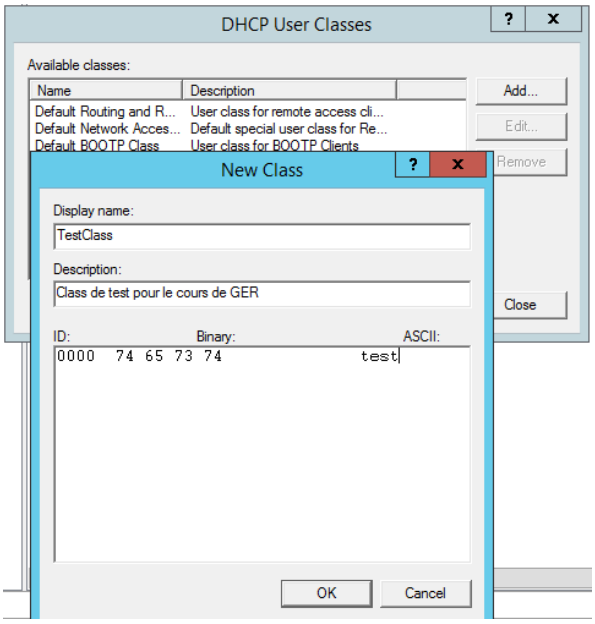

Figure 26 : Création d'une classe utilisateur.

Une fois la classe créée, nous allons créer une nouvelle police. Pour ce faire, cliquez droit sur « ***Policies*** », « ***New Policiy …*** ». Donnez un nom à votre police ainsi qu'une description.

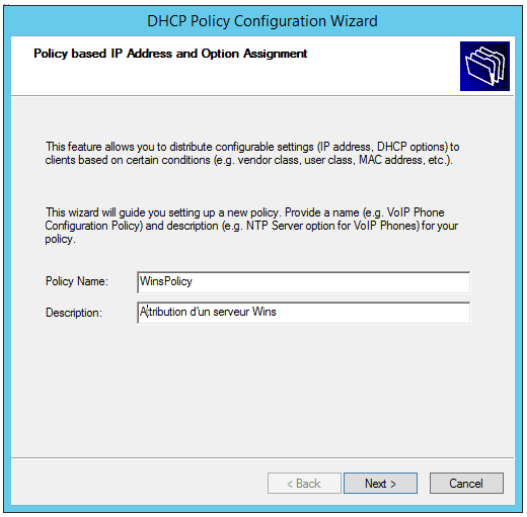

Figure 27 : Policy Name.

Ensuite, ajoutez une condition. Pour ce faire cliquer sur le bouton « ***Add*** ». Dans la fenêtre d'ajout et d'édition des polices, sélectionnez comme critère « ***User Class*** », comme opérateur « ***Equals*** » et comme valeur la classe utilisateur précédemment créée.

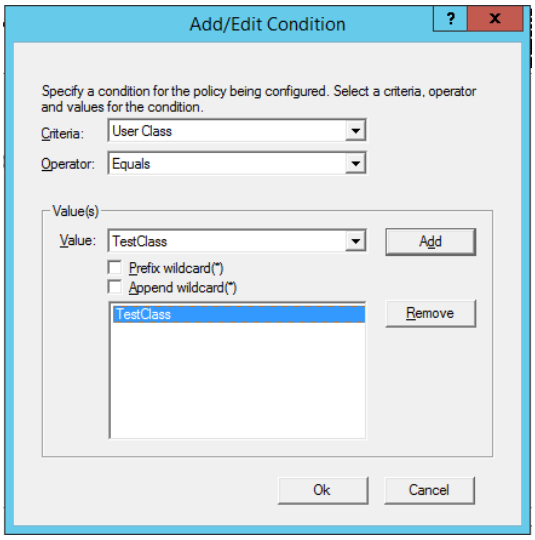

Figure 28 : Ajout et édition de police.

Nous allons maintenant configurer les paramètres associés à la police. Pour ce faire, sélectionnez dans la liste l'option « ***044 WINS/NBNS Servers*** » et entrez une adresse IP associé à celui-ci.

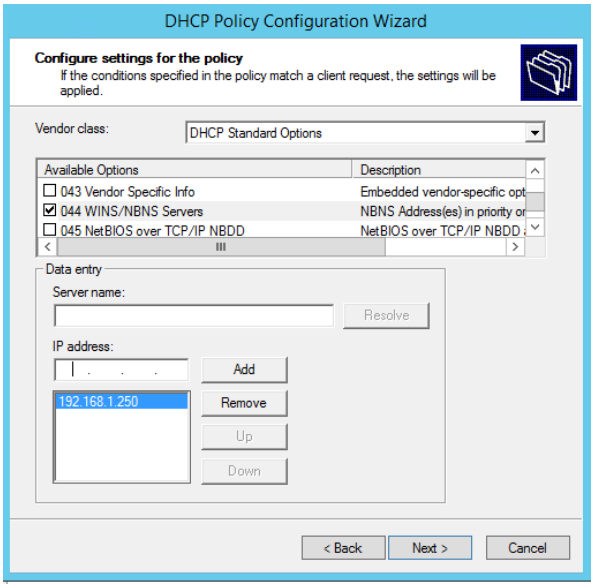

Figure 29 : Configurer les paramètres de la police.

Reste maintenant à configurer le poste client. Pour ce faire, nous allons devoir utiliser la commande « ***ipconfig /setclassid*** » mais au préalable nous avons besoin de connaitre le nom de la carte réseau. Lancer l'invite de commande en mode privilégié et taper les commandes suivantes :

- Afin de connaître le nom de la carte réseau : **netsh interface ipv4 show interfaces**
- Il faut également récupérer le code ASCII de la classe utilisateur (Figure 26 : Création d'une classe utilisateur.)
- Maintenant nous pouvons utiliser la commande : **ipconfig /setclassid "connexion au réseau local" test**

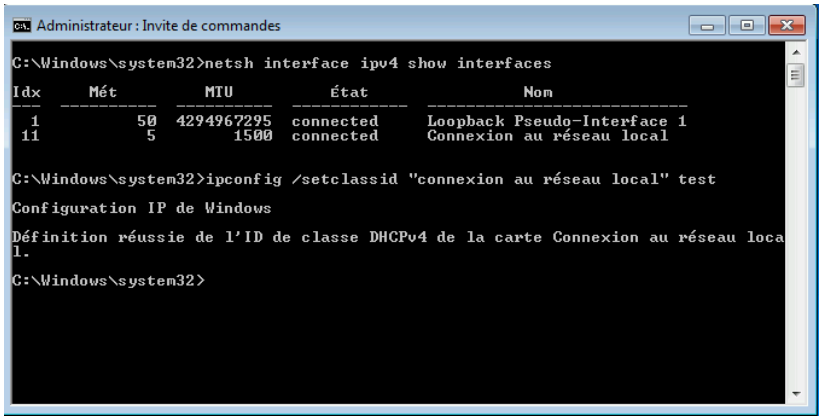

Figure 30 : IPCONFIG /SETCLASSID

Afin de vérifier si la configuration est correcte, il vous suffit de taper la commande « ***ipconfig/all*** »

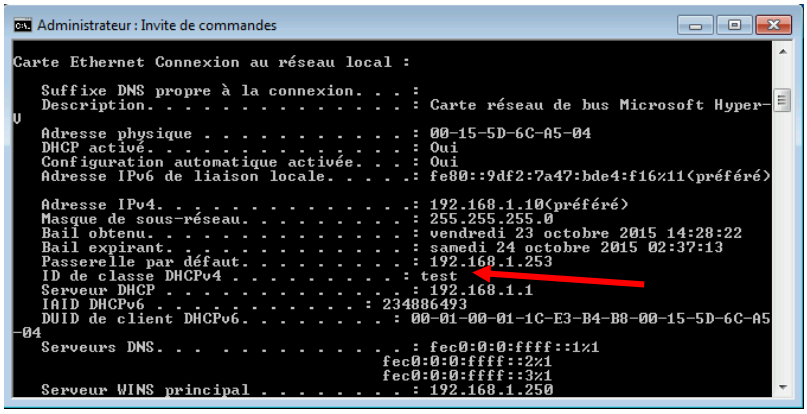

Figure 31 : Vérification de la classe utilisateur sur le poste client.

Pour supprimer un ID de classe, il suffit simplement de taper la commande suivante :

- **ipconfig /setclassid "Connexion au réseau local"**

5 Installation et configuration du rôle DNS

Afin d'accéder à un poste de travail sur le réseau, il est possible d'utiliser son adresse IP ou son nom. Pour ce dernier, un mécanisme de résolution de nom en adresse IP et inversement doit être mis en place.

Un serveur DNS permet la résolution d'un nom d'hôte en adresse IP (et inversement).

DNS est basé sur un système hiérarchique. Les serveurs situés en haut de la hiérarchie sont appelés « ***serveurs racine*** » et sont représentés par un point. Ils permettent la redirection des requêtes vers les serveurs DNS de premier niveau (org, net, com, …).

Au second niveau se trouvent les noms de domaine qui sont réservés par les entreprises ou les particuliers. Ces noms de domaine sont réservés chez un fournisseur d'accès.

5.1 Les différents types de requêtes :

Afin de résoudre un nom, le serveur DNS peut utiliser deux types de requêtes :

- ***Requêtes itératives*** : Le poste client envoie à son serveur DNS une requête afin de résoudre le nom www.youtube.com. Le serveur interroge alors le serveur racine, celui-ci redirige la requête vers le serveur ayant autorité sur la zone « ***.com*** ». Celui-ci peut donc connaître l'adresse IP du serveur faisant autorité sur la zone « ***youtube*** ». L'interrogation de ce dernier permet la résolution de www.youtube.com. Le serveur DNS interne répond alors à la demande du poste client.

- ***Requêtes récursives*** : le client veut toujours résoudre le nom www.youtube.com. Il envoie la demande à son serveur DNS. Celui-ci n'ayant pas autorité sur la zone « ***youtube.com*** », il a besoin d'un serveur externe pour effectuer la résolution. La

demande est donc transmise au redirecteur configuré au préalable par l'administrateur (ce redirecteur peut tout simplement être le serveur DNS du FAI). Si la réponse n'est pas contenue dans la cache du serveur FAI, celui-ci effectuera une requête itérative et transmettra le résultat au serveur qui lui a transmis la demande. Ce dernier pourra donc répondre à son client.

5.2 Les différents types de zones :

Dans un serveur DNS, il est possible de créer 3 types de zones :

- ***La zone primaire*** : possède des droits de lecture et d'écriture sur l'ensemble des enregistrements qu'elle contient. Ce type de zone peut être intégré à Active Directory. Si la zone n'est pas intégrée à Active Directory, il est nécessaire de configurer le transfert de zone.
- ***La zone secondaire*** : est une copie d'une zone primaire. L'écriture est impossible sur ce type de zone, seule la lecture est autorisée. Il est impossible de l'intégrer à Active Directory, un transfert de zone est donc obligatoire.
- ***La zone de stub*** : est une copie d'une zone qui contient uniquement les enregistrements nécessaires à l'identification du serveur DNS faisant autorité pour cette zone.

5.3 Installation du rôle DNS :

Comme pour l'installation du rôle DHCP, il suffit de cocher l'option « ***DNS*** » et de cliquer sur « ***Install*** ».

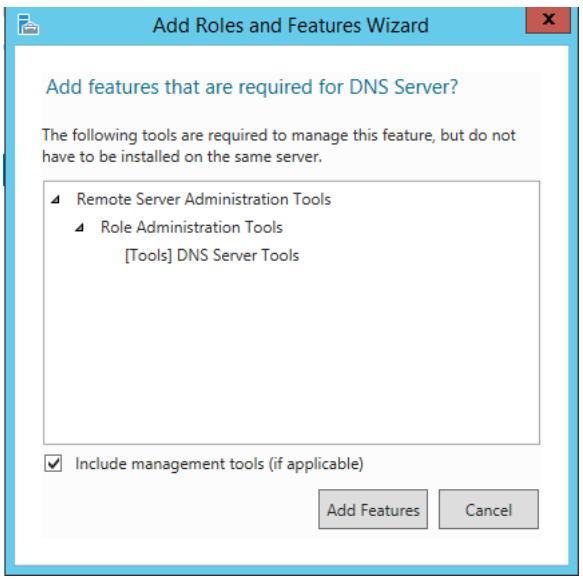

Figure 32 : Ajout du rôle DNS.

5.4 Configuration du rôle DNS :

5.4.1 Configuration d'une zone principale directe :

Une fois l'installation terminée, il faut au préalable ajouter une nouvelle zone de recherche directe (Forward Lookup Zones). Cliquer droit sur « ***Zone de recherche directe*** », « ***Nouvelle Zone …*** ». En ce qui concerne le type de zone, nous allons sélectionner une zone primaire.

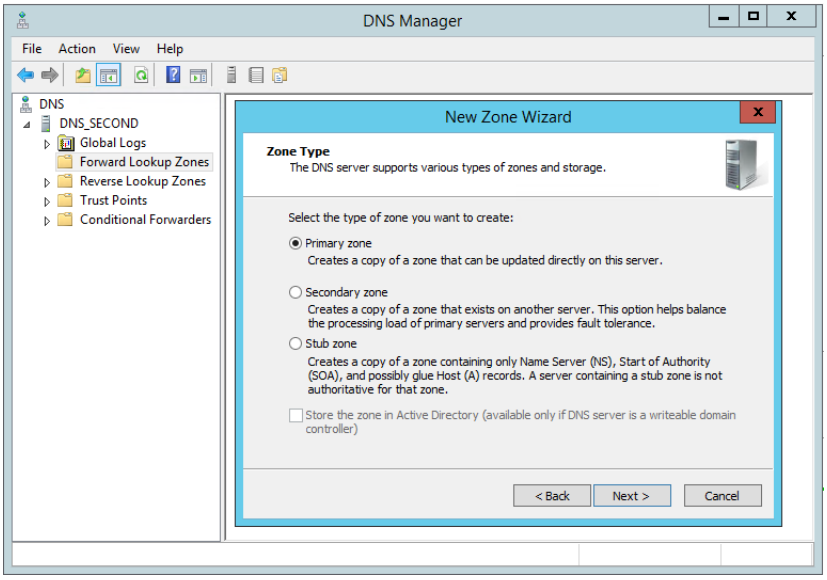

Figure 33 : Ajout d'une nouvelle zone de recherche.

Nous allons bien entendu, donner un nom à notre zone par exemple : votre_société.lan

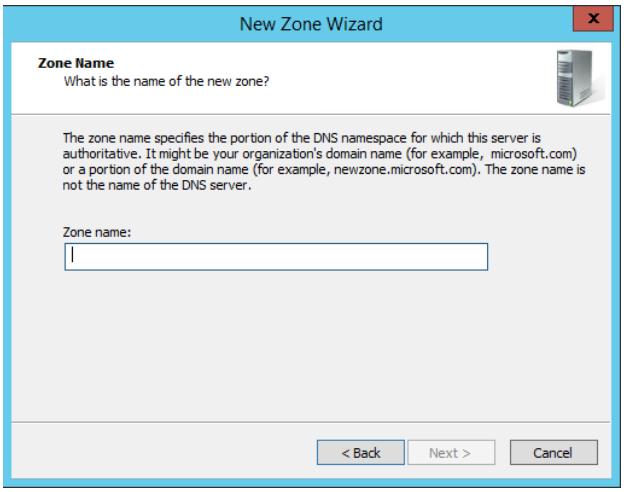

Figure 34 : Attribuer un nom à la zone primaire

5.4.2 Configuration d'une zone principale inverse :

Le principe est le même que pour la création de la zone principal directe, cliquez droit sur « ***Zone de recherche inverse*** », « ***Nouvelle zone …*** », sélectionnez « ***zone primaire*** » ensuite « ***zone de recherche inverse IPv4*** ».

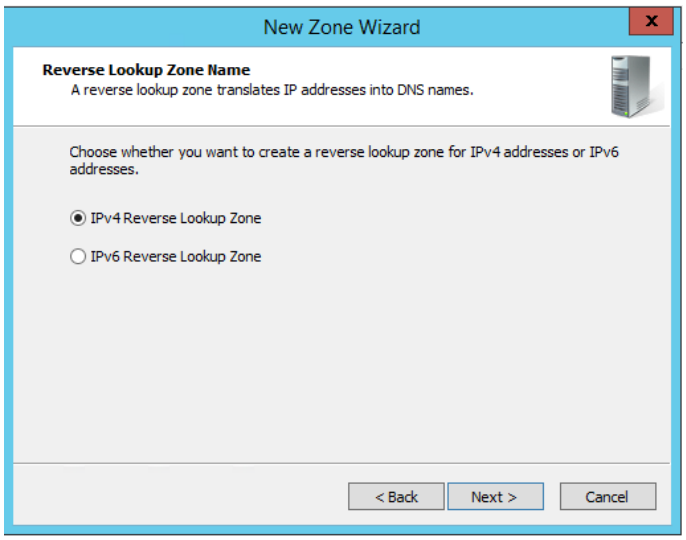

Figure 35 : Zone de recherche inverse IPV4.

Ensuite, vous devez préciser votre identifiant réseau.

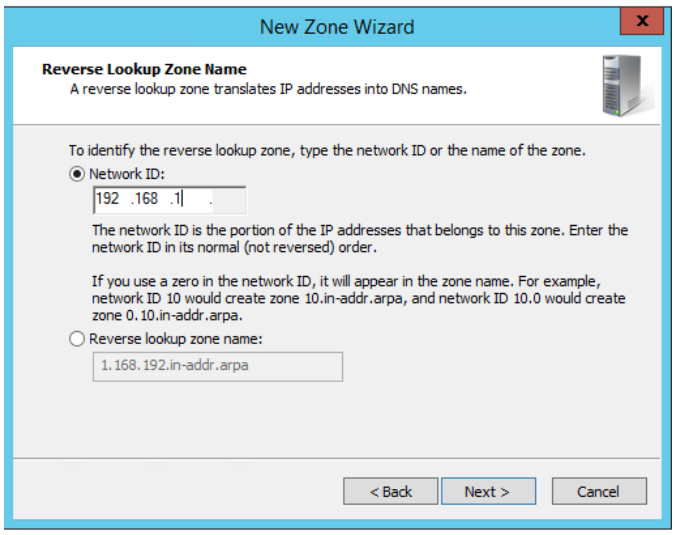

Figure 36 : Network ID.

Suivez ensuite les instructions pour finaliser la configuration.

5.4.3 Configuration d'une zone secondaire directe :

Sur le DNS2 (VM2), créer une zone secondaire. Nommer la zone avec le même nom que vous avez utilisé sur votre DNS principal.

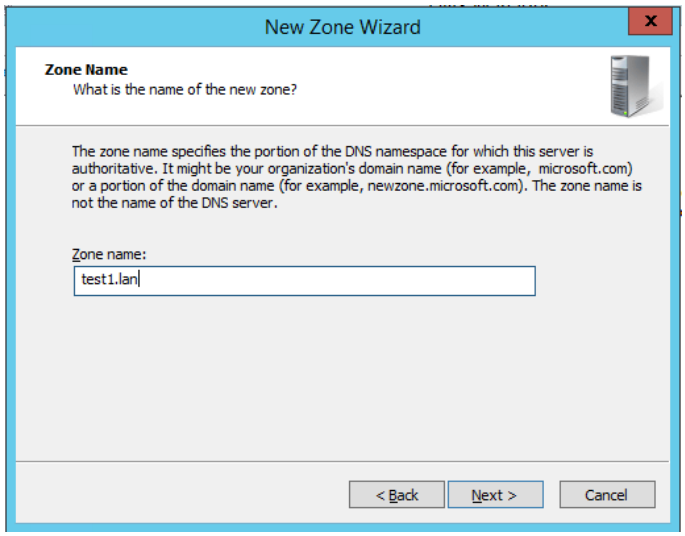

Figure 37 : Nommer la zone secondaire.

Ensuite, il faut bien entendu stipuler l'adresse IP de votre DNS principal.

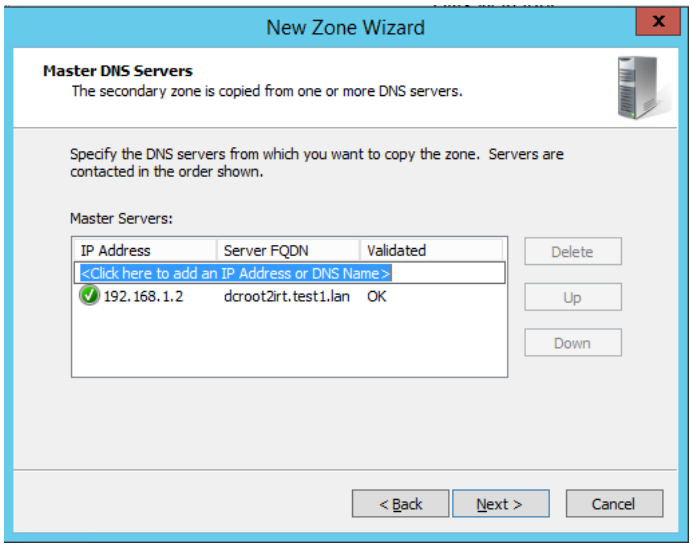

Figure 38 : Adresse IP du DNS Master.

Une fois la zone secondaire créé, on peut constater que le serveur n'a pas récupérer une copie de la zone DNS du serveur principal.

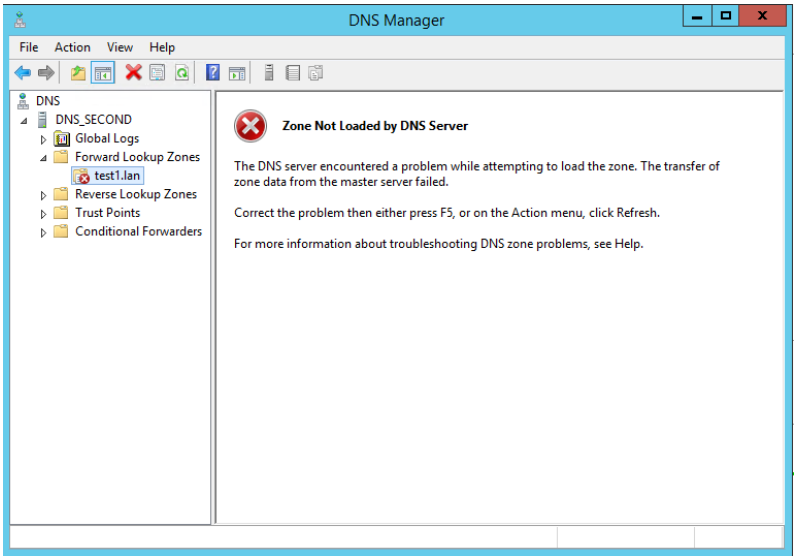

Figure 39 : Copie de la zone non récupérée.

Afin de pallier à ce problème, nous allons simplement autoriser le transfert de zone sur le serveur principal.
Pour ce faire, nous allons sur le serveur principal afin d'y ajouter un nouvel enregistrement de type A pour le serveur secondaire.

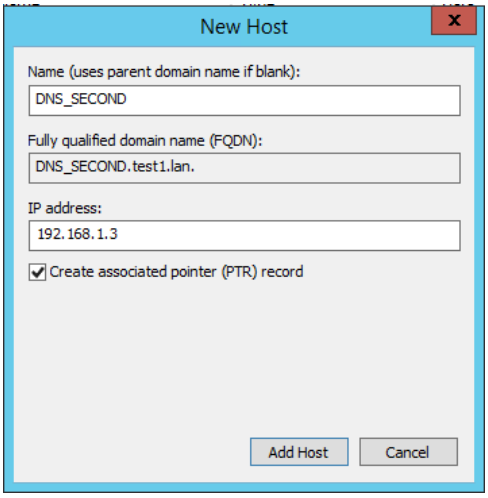

Figure 40 : Nouvel enregistrement de type A – DNS Secondaire.

Nous allons maintenant ajouter le nom d'hôte que nous venons d'ajouter dans les propriétés de la zone.

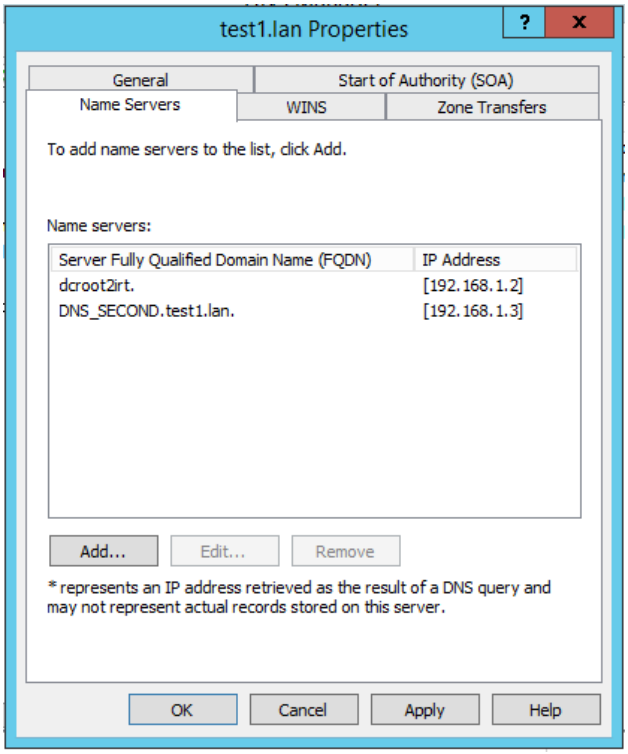

Figure 41 : Ajout du nom d'hôte.

Nous pouvons maintenant retourner sur le serveur secondaire afin de tester le transfert de zone. Pour ce faire, taper la commande suivante dans l'invite de commande :

- **nslookup IP_de_votre_serveur_principal**
- **ls –d votre_nom_de_zone**

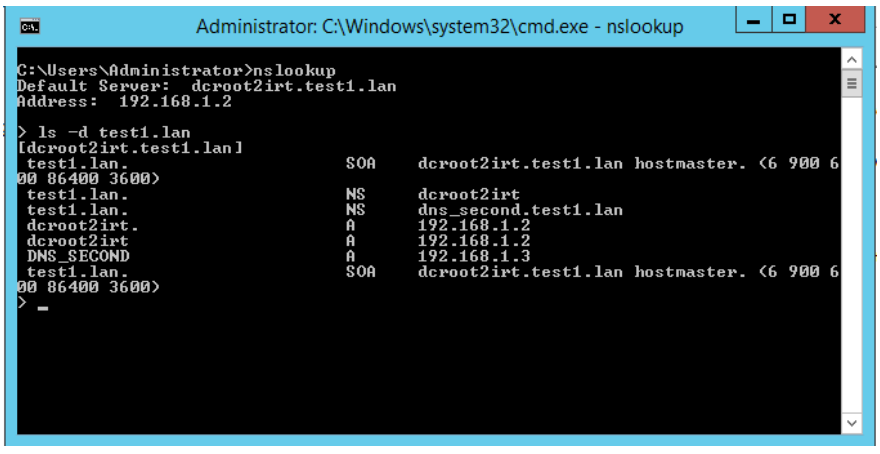

Figure 42 : Vérification du transfert de zone.

La commande « ***ls –d votre_nom_de_zone*** » permet d'effectuer le transfert de zone.
Nous allons maintenant effectuer un transfert de zone à partir de la console DNS.
Pour ce faire, il suffit de faire un clic droit sur la zone, sélectionné « ***All Tasks*** », « ***Transfer from Master*** ».
Vous pouvez bien entendu vérifier votre configuration à l'aide de la commande nslookup.

5.4.4 Délégation de zone :

La délégation de zone permet à un autre serveur DNS de gérer une partie des enregistrements de la zone.

Si nous reprenons notre arborescence actuelle :

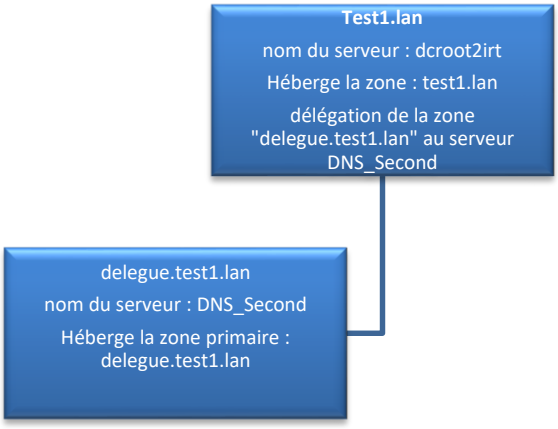

Figure 43 : Arborescence DNS.

Dans ce cas de figure, le domaine ***test1.lan*** comprend un sous-domaine ***delegue.test1.lan.***
Chaque domaine dispose de son propre serveur DNS. Le serveur DNS parent (dcroot2irt) héberge la zone principale ***test1.lan***. On souhaite déléguer l'administration des enregistrements du domaine ***delegue.test1.lan*** au serveur secondaire ***DNS_Second***.
Nous allons donc pour se faire créer une délégation de zone.

Dans un premier temps, nous allons ajouter une zone primaire sur le serveur secondaire ***DNS_Second***. Cette zone sera nommée « ***delegue.test1.lan*** »

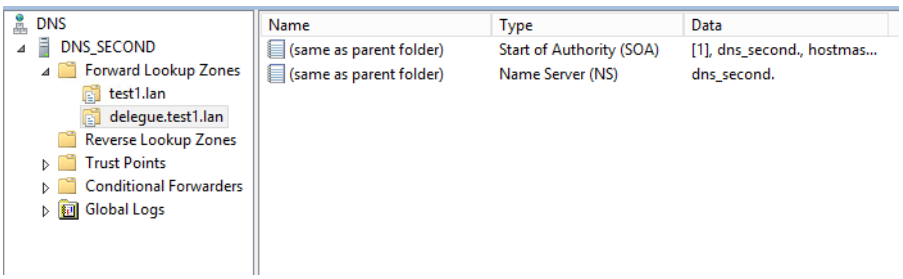

Figure 44 : Délégation de zone - création zone primaire.

Dans cette zone nous allons créer un hôte correspondant à notre serveur primaire « ***dcroot2irt*** ».

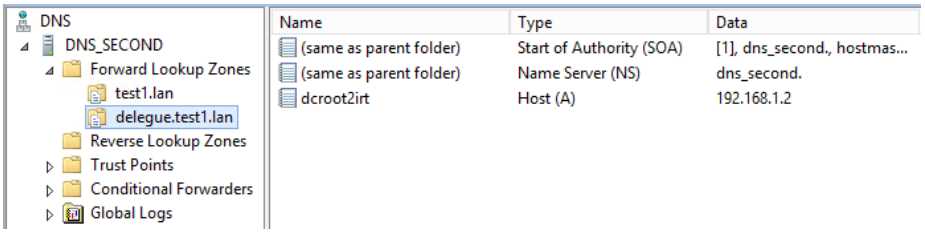

Figure 45 : Délégation de zone - Nouvel hôte.

Maintenant nous allons créer la délégation de zone sur le serveur parent (dcroot2irt). Pour ce faire, il faut sélectionner la zone primaire « ***test1.lan*** », faire un clic droit et sélectionner « ***Nouvelle délégation*** ».
L'assistant nous demande d'entrer le domaine que l'on désire déléguer (***delegue.test1.lan***).

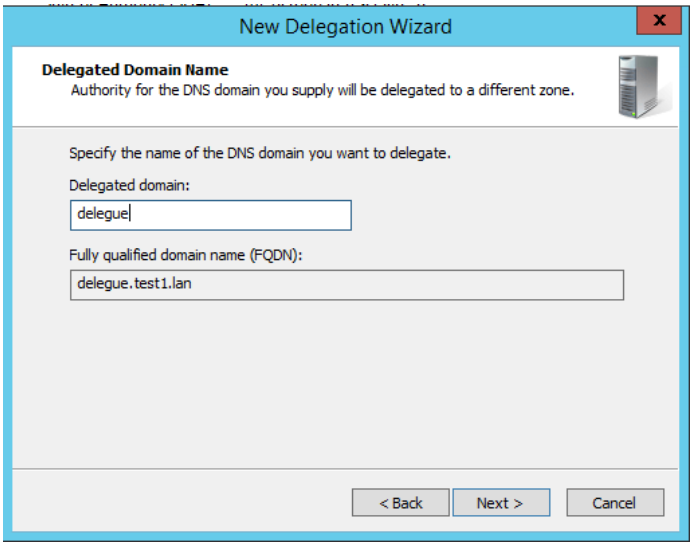

Figure 46 : Domaine délégué.

Ensuite, nous allons devoir choisir le serveur qui héberge la zone délégué. Nous allons donc cliquer sur le bouton « ***Add*** » et spécifier le FQDN du serveur secondaire ainsi que son adresse IP.

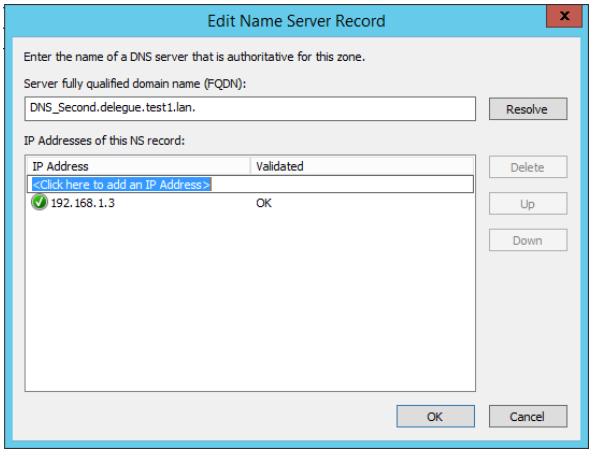

Figure 47 : FQDN du serveur secondaire.

Afin de tester si notre délégation fonctionne correctement, nous allons créer un alias « ***www*** » sur notre serveur secondaire.

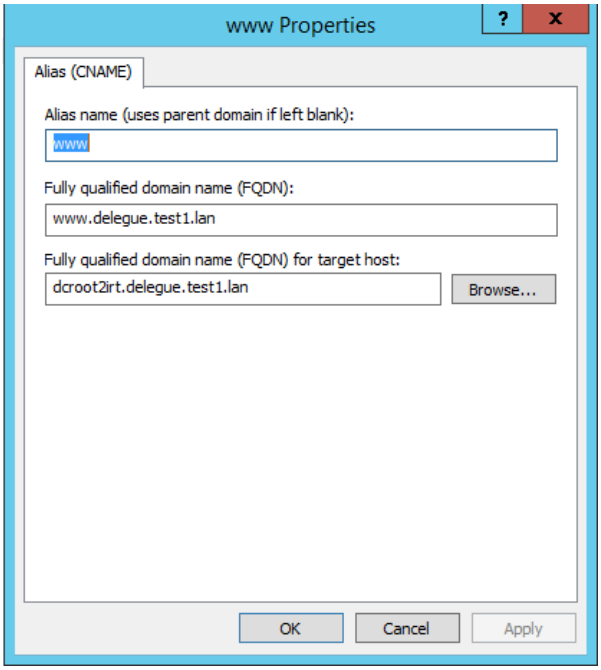

Figure 48 : Délégation de zone - création d'un alias.

Nous allons maintenant réaliser la commande « ***nslookup*** » sur notre serveur primaire pointant sur www.delegue.test1.lan.

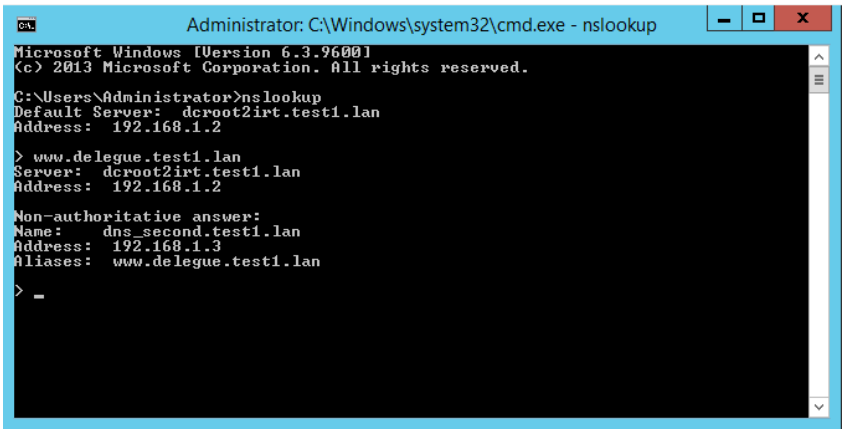

Figure 49 : Délégation de zone - NSLOOKUP

Nous pouvons constater, que le serveur répondant à la requête ***«www.delegue.test1.lan»*** est bien le serveur gérant la zone « ***delegue.test1.lan*** ».
Par contre, nous constatons que le serveur qui répond ne fait pas autorité.

6 Active directory

6.1 Installation du rôle AD-DS :

Comme pour l'installation du rôle DNS, il suffit de cocher l'option « ***Active Directory Domain Services*** » et de cliquer sur « ***Install*** ».

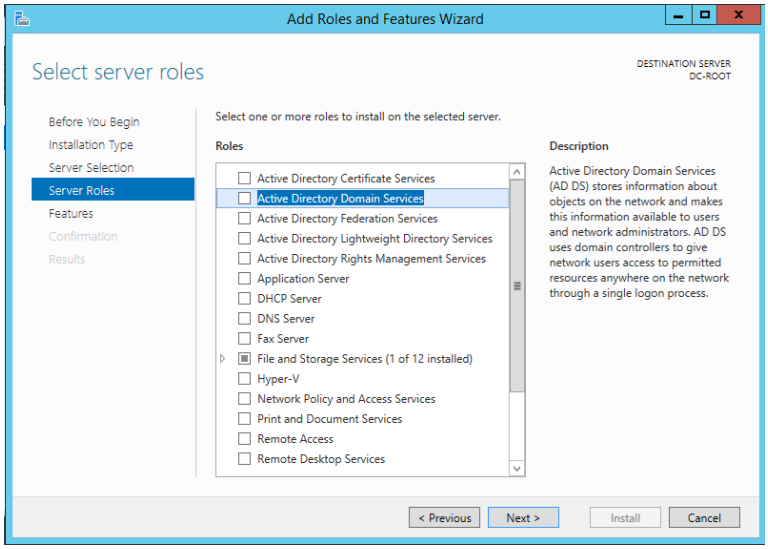

Figure 50 : Installation du rôle ADDS.

Une fois le rôle installé, on peut constater une alerte dans le panneau de notification. Il vous suffit de cliquer sur « ***Promote this server to a domain controller*** ».

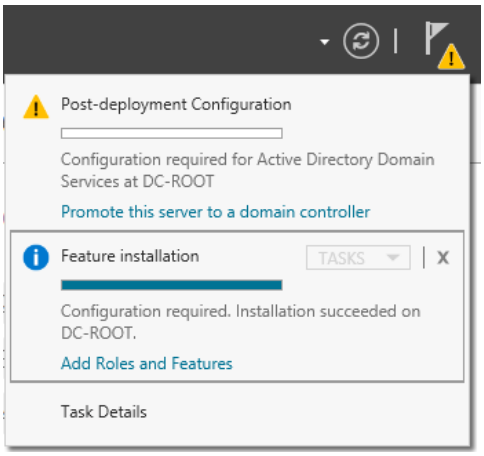

Figure 51 : Promouvoir votre serveur.

Vous serez amené à configurer ensuite votre domaine. Dans un premier temps, il faudra créer une nouvelle forêt et donner un nom à votre domaine.

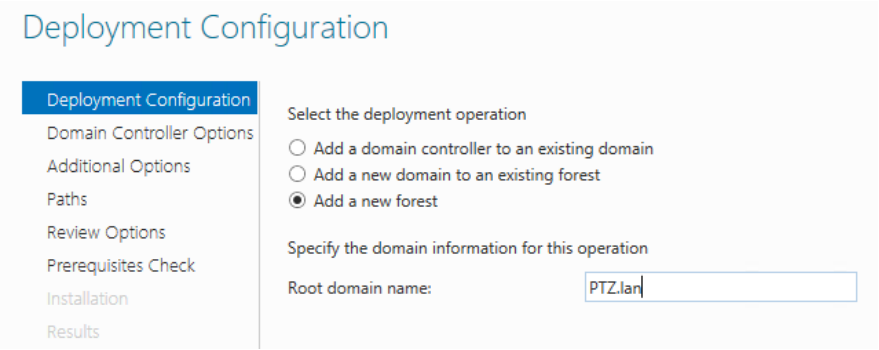

Figure 52 : Création de la forêt et du nom de domaine.

Ensuite il vous sera demandé d'entrer un mot de passe pour le DSRM.

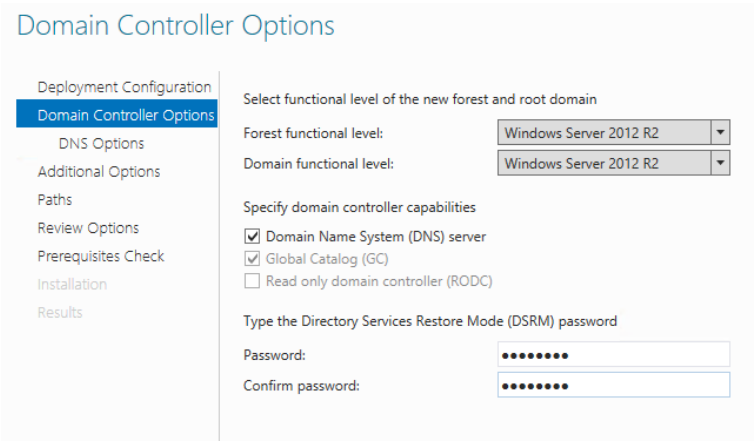

Figure 53 : DSRM.

Une fois l'installation terminée, n'oubliez pas de redémarrer votre serveur si ce n'est fait automatiquement.

6.2 Sites Active-Directory :

Un site a pour objectif de gérer le trafic de réplication inter-sites et de faciliter la localisation des services. La gestion des sites se fait via l'outil d'administration « ***Sites et services Active Directory*** ». Cette console permet de gérer les éléments suivants :

- Les sous-réseaux
- Les protocoles de transports
- Les sites
- Les topologies de réplication
- Les planifications de réplication
- Les liens inter sites
- Les serveurs de catalogue global.

Lors de la création du premier domaine d'une forêt, les services de domaines Active Directory créent automatiquement un site par défaut « ***Default-First-Site-Name*** ».

Il est recommandé de renommer le site par défaut afin de lui donner un nom plus représentatif.
Pour ce faire vous devez, dans « ***Sites et service Active Directory*** », cliquer droit sur « ***Default-First-Site-Name*** » et choisir « ***Renommer*** ».

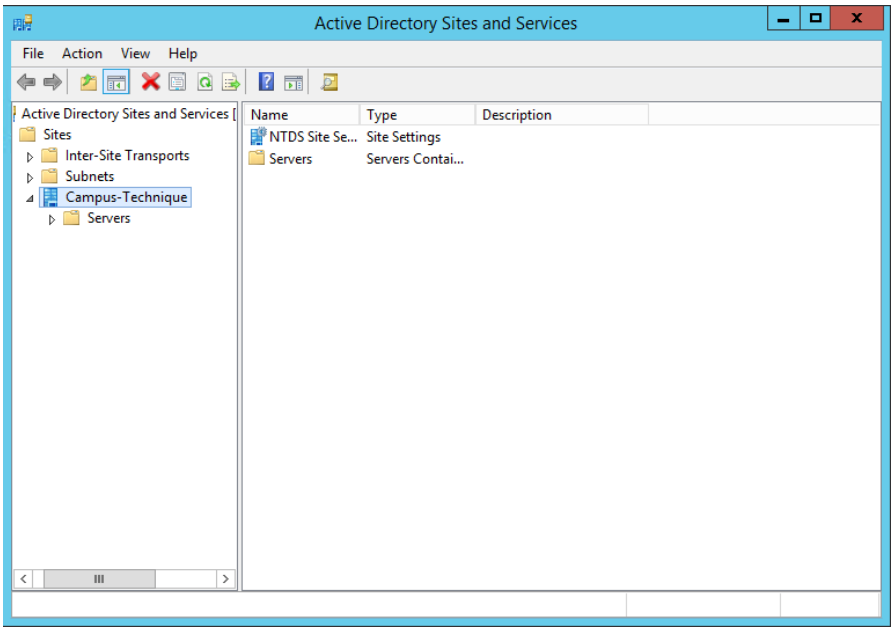

Figure 54 : Default-First-Site-Name.

6.3 Ajout d'une UO et d'un utilisateur :

Les unités d'organisation (OU – Organizational Unit) sont les objets conteneurs les plus communément utilisés au sein d'un domaine Active Directory.
Ce conteneur peut contenir de multiples types d'objets tels que les utilisateurs, des contacts, des ordinateurs, des imprimantes, des dossiers partagés.

Vous pouvez effectuer toutes ces modifications à partir de la console « ***Active Directory Users and computers*** »

6.4 Modifier la complexité du mot de passe:

Par défaut, la complexité du mot de passe sur votre serveur est la suivante :

- Doit contenir minimum 7 caractères ;
- Doit contenir minimum une majuscule ;
- Doit contenir minimum une minuscule ;
- Doit contenir minimum un chiffre ;
- Doit contenir minimum 1 caractère spécial.

Les paramètres de sécurités des mots de passe Active Directory se gèrent dans « ***Outils d'administration*** », « ***Gestion des stratégies de groupes*** ».
Attention à ne pas confondre avec la sécurité du contrôleur de domaine qui ne concerne que les comptes locaux du serveur.
Dans l'arborescence, déployer « ***Group Policy Management*** », « ***Forest*** », « ***Domains*** », « ***nom de domaine*** ».

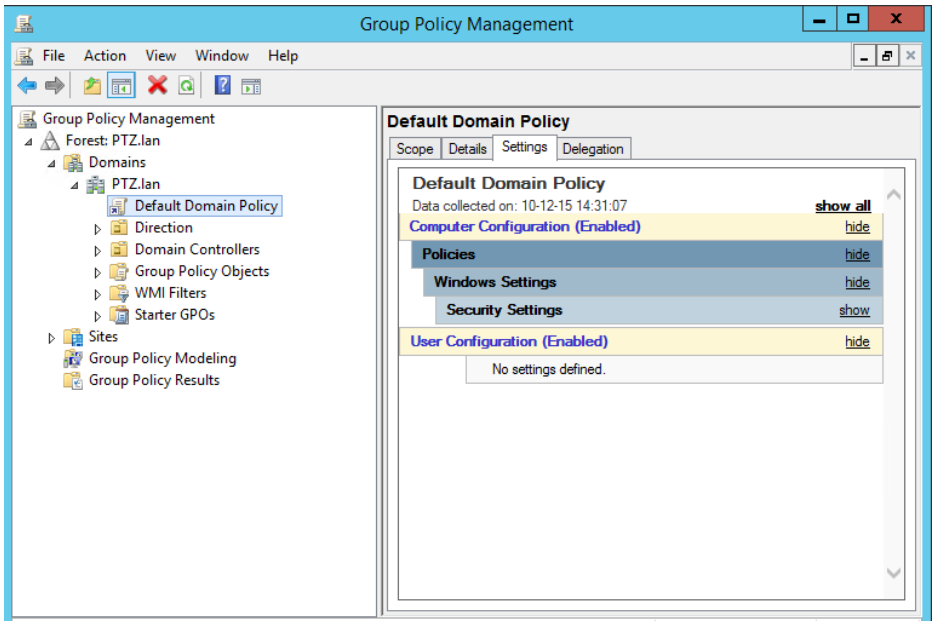

Figure 55 : Group Policy Management.

Faites un clic droit sur « ***Default Domain Policy*** » et sélectionnez « ***Edit*** ». La fenêtre « ***Group Policy Management Editor*** » s'ouvre.

Dans cette fenêtre vous disposez de deux catégories :

- Computer configuration
- User Configuration

Déployez la catégorie « ***Computer configuration*** » afin d'atteindre « ***Sécurity Settings*** ».

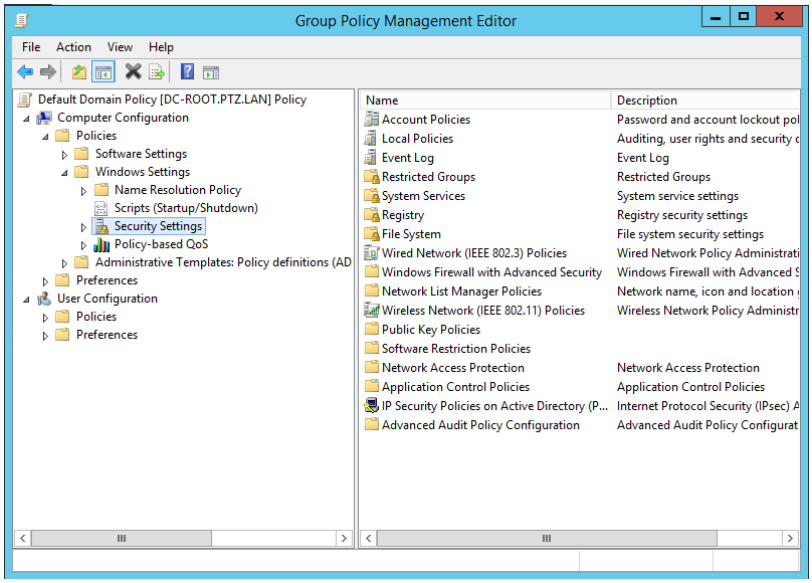

Figure 56 : Security Settings.

Dans cet onglet, sélectionnez « ***Account Policy*** » et ensuite « ***Password Policy*** ».

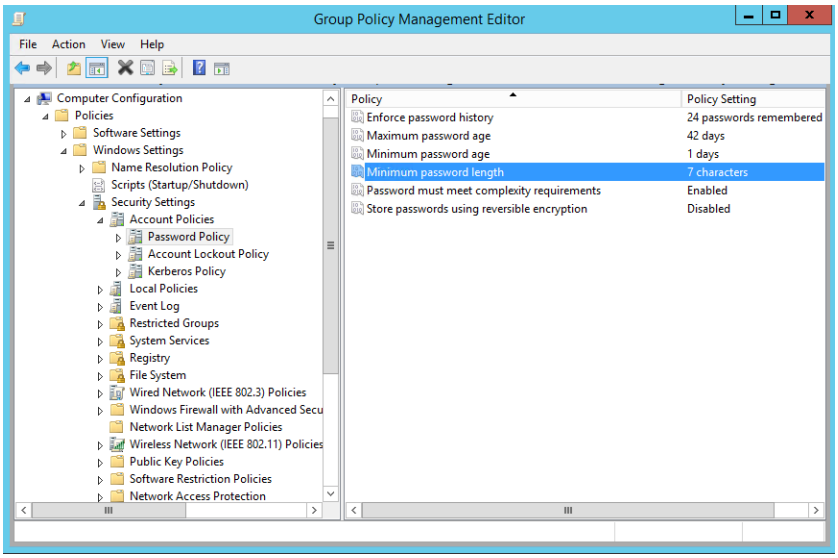

Figure 57 : Modifier la complexité de mot de passe.

6.5 Configurer des horaires de connexion :

Les horaires de connexions permettent de préciser les plages horaires ainsi que les jours de la semaine pendant lesquelles les utilisateurs peuvent se connecter via leur session.

Afin de modifier les horaires de connexions, il suffit de vous rendre dans les propriétés d'un compte utilisateur et de sélectionner l'onglet « ***Account*** » et de cliquer sur « ***Logon Hours*** ». Dans la fenêtre « ***Logon Hours*** » (voir figure 58), il vous suffit de sélectionner les périodes autorisées et les périodes refusées.

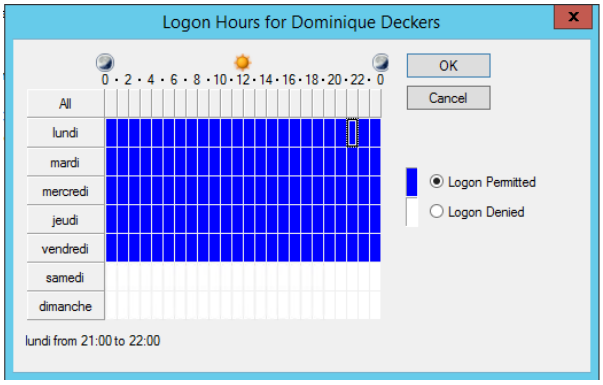

Figure 58 : Modification des horaires de connexion.

6.6 Créer des profils itinérants :

Le profil itinérant permet à l'utilisateur de conserver ses documents, son environnement de travail, … quel que soit l'ordinateur sur lequel il se trouve. Un autre avantage c'est que vous pourrez par la suite effectuer des backups des profils afin de minimiser la perte d'informations, de documents, …

Pour configurer le profil itinérant d'un utilisateur, il faut au préalable effectuer quelques prérequis.

- Dans un premier temps, si vous avez mis des quotas, vérifier que ceux-ci soit assez conséquent pour les profils. Si vous mettez un quota trop faible, vous ne pourrez pas copier l'entièreté de vos données.
- Il ne faut pas utiliser le système de chiffrage « ***Encrypted File System (EFS)*** » avec vos comptes itinérants.
- Pour éviter les problèmes d'ouverture de synchronisation lors des ouvertures et fermetures de session, il est nécessaire de désactiver les fichiers hors connexion.
- Créer un dossier partagé qui contiendra l'ensemble des profils.

Nous allons donc dans un premier temps créer un dossier partagé. Par sécurité on peut cacher ce dossier en ajoutant un $ au nom du ***partage*** comme par exemple : « ***profils$*** ».

Ensuite il faudra donner les accès pour le partage. Vous trouverez ci-dessous les droits devant être mis en place sur le dossier.

Compte d'utilisateur	Permission
Créateur propriétaire	Contrôle total sur les dossiers enfants et les fichiers
Administrateur	Aucune permission
Tout le monde	Aucune permission
System	Contrôle total sur le dossier et les dossiers enfants et les fichiers
Groupe de sécurité / Utilisateur	Listage du dossier / Lecture, création de dossier dans le dossier de l'utilisateur ou du groupe.

Tableau 1 : Permission du dossier partagé pour les profils itinérants.

ATTENTION, il ne faut surtout pas créer les dossiers de profils manuellement, c'est le système qui les créera lors de la première connexion de l'utilisateur. Si vous créer manuellement les dossiers, vous risquez d'avoir des doublons ce qui engendrera de gros problèmes.

Voici ci-dessous les permissions qui seront effectives lorsque le système aura créé le dossier de profil :

Comptes utilisateur	Permission
%username%	Contrôle total sur le dossier, les dossiers enfants et les fichiers. Propriétaires du dossier.
Administrateur	Aucune permission
Tout le monde	Aucune permission
Local System	Contrôle total sur le dossier, sur les dossiers enfants et les fichiers.

Tableau 2 : Permission pour le dossier de profil itinérant d'un utilisateur.

Une fois le dossier partagé, il faut indiquer le chemin où les informations de l'utilisateur seront stockées. Pour ce faire, dans les propriétés du compte utilisateur, dans l'onglet « ***Profile*** », tapez le chemin du partage dans le champ « ***Profile path*** ».

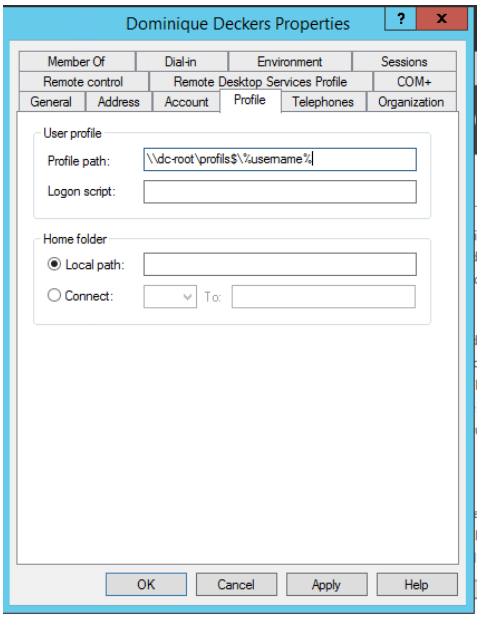

Figure 59 : Chemin du profil itinérant.

L'utilisation de la variable « ***%Username%*** » permet de créer un dossier portant le nom de l'utilisateur. Il reste maintenant à effectuer une connexion avec l'utilisateur en question pour voir si tout est opérationnel. Attention, si vous êtes déjà connecté avec l'utilisateur, il faudra au préalable se déconnecter et se reconnecter pour que le profil soit pris en compte.

6.7 Ajouter un suffixe UPN :

Par défaut, lorsque l'on édite les propriétés d'un compte utilisateur, seul le suffixe de nom correspondant au nom de domaine apparait.
On peut ajouter des suffixes afin de faciliter les processus d'administration et d'ouverture de session
Pour ajouter un suffixe, il faut ouvrir la console « ***Active Directory – Domains and trusts*** ». Dans l'arborescence de cette console, effectuez un clic droit sur « ***Active Directory domains and trusts*** », et sélectionnez « ***Propertie***s ». Dans celles-ci, vous avez la possibilité d'ajouter un suffixe. Dans l'exemple ci-dessous, nous avons ajouté un suffixe pour l'unité d'organisation direction.

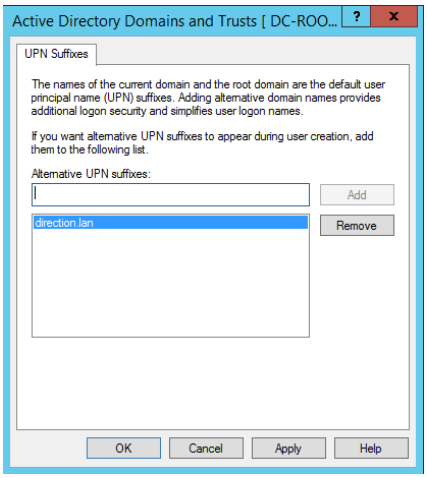

Figure 60 : Ajout d'un suffixe UPN.

Maintenant que le suffixe est ajouté, il faut l'associé aux utilisateurs. Pour ce faire, ouvrez la console « ***Active Directory – Users and Computers*** », éditez les propriétés d'un utilisateur, dans l'onglet « Account » modifiez l'UPN à l'aide de la liste déroulante.

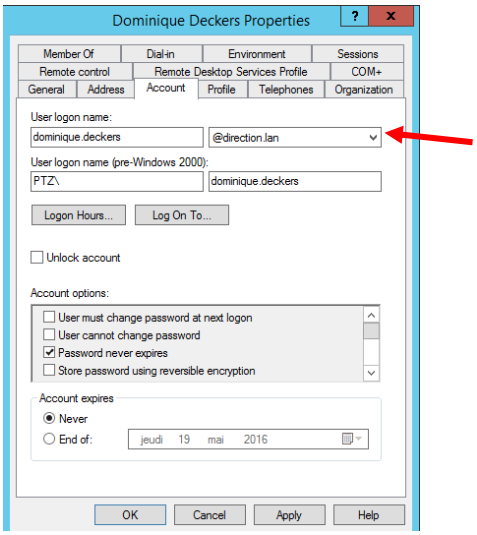

Figure 61 : Associer un UPN à un utilisateur.

6.8 Les groupes :

Windows Serveur 2012 gère plusieurs types de groupes. Ceux-ci peuvent être définis selon 3 types d'étendues de groupe et deux types de groupe.

- Etendues de groupe :
  - Domaine local
  - Globale
  - Universelles
- Groupe :
  - Sécurité
  - Distribution

Etant donné que les groupes de sécurité sont des objets Active Directory, ils possèdent également un SID unique dans le domaine.

Définition des différents types de groupes :

- ***Les groupes de distribution*** : Essentiellement utilisés par les applications de messagerie. La sécurité n'y est pas activée car il ne possède pas de SID et ne peuvent donc pas recevoir d'autorisations vers des ressources. Envoyer un message à un groupe de distribution revient à envoyer un message à chacun des membres de ce groupe.
- **Les groupes de sécurité** : ce sont des entités de sécurité dotées d'un SID. Donc ils peuvent faire office d'entrée d'autorisation dans des ACL pour contrôler la sécurité de l'accès aux ressources. Les groupes de sécurités peuvent être utilisés comme groupe de distribution par les applications de messagerie.

Ces groupes peuvent être gérés à partir de la console « ***Active Directory – Users and Computers*** ».

6.8.1 Les groupes globaux :

Cette étendue de groupe ne sert qu'à regrouper divers objets du domaine afin d'en centraliser la gestion. Ce type de groupe ne peut contenir que des objets ordinateurs, utilisateurs ou des groupes globaux issus du même domaine. Ces groupes sont répliqués vers l'ensemble des contrôleurs de domaine.

6.8.2 Les groupes universels :

Ce type de groupe s'utilise surtout dans les environnements multi-domaine. Il peut accueillir des objets tels que des ordinateurs, des utilisateurs ou des groupes issus de toute la forêt. Ils peuvent servir à gérer des ressources dans des contextes multi

domaine. Ils sont répliqués sur les contrôleurs de domaine hébergeant le catalogue global.

Pour créer un groupe, dans la console « ***Active Directory – Users and Computers*** », effectuez un clic droit sur l'UO dans laquelle vous voulez créer le groupe et sélectionnez « ***New*** », « ***Group*** ».

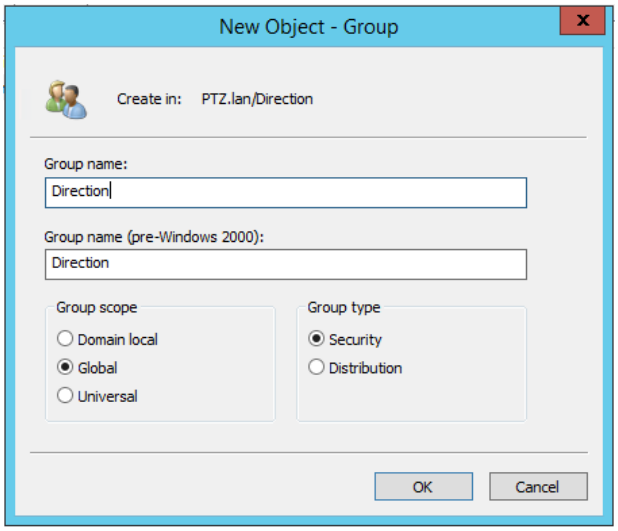

Figure 62 : Création d'un groupe.

6.9 Délégation de contrôle :

Cette méthode permet de donner des autorisations à un utilisateur d'une UO afin de gérer certaines tâches. De cette manière, des opérations de base peuvent être assurées par un autre utilisateur que l'administrateur.

Ce genre de contrôle peut être effectué à partir de l'assistant « ***Délégation de contrôle*** » ou de la console « ***Gestionnaire d'autorisations*** ». Ces deux outils permettent d'attribuer des droits et des autorisations à des groupes ou des utilisateurs spécifiques.

Si par exemple nous voulons déléguer la gestion d'une UO à un utilisateur de celle-ci, il suffit de sélectionner l'UO en question, effectuer un clic droit et sélectionner « ***Delegate Control …***».

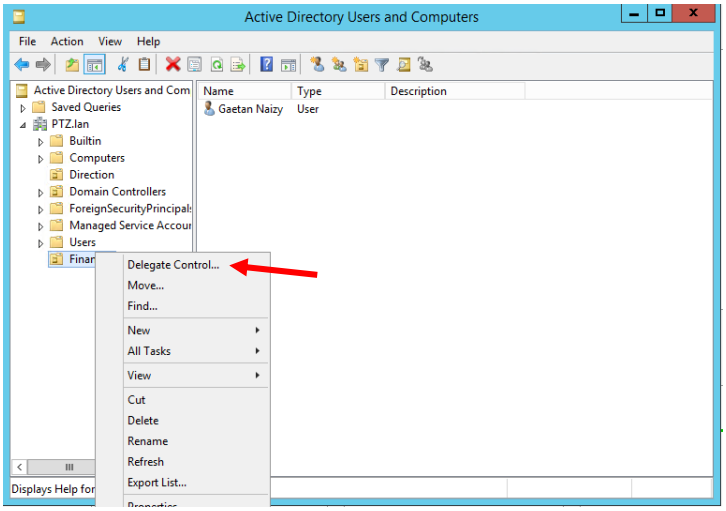

Figure 63 : Delegate Control …

Cette étape ouvrira l'assistant délégation de contrôle.
Dans celui-ci, il faudra stipuler l'utilisateur auquel nous allons attribuer des tâches, sélectionner la tâche à attribuer (il est également possible de créer une tâche personnalisée)

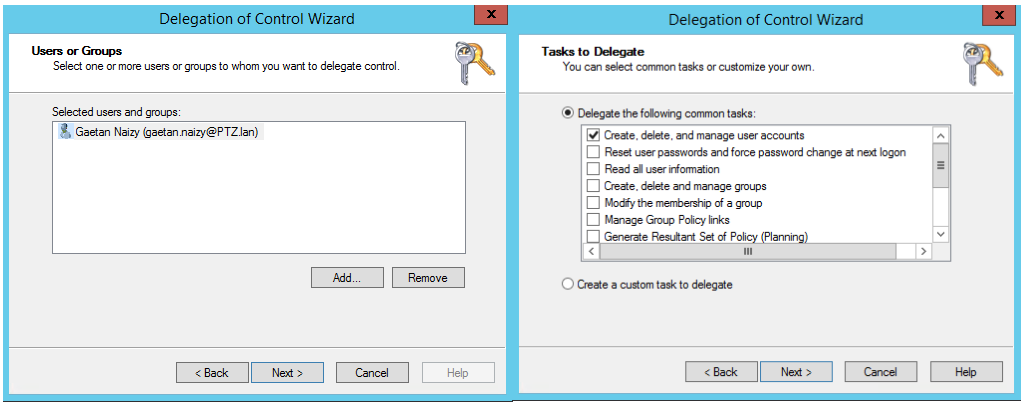

Figure 64 : Délégation de contrôle – User and Task.

Il est possible de vérifier les droits afin de vérifier si tout est correct selon vos besoins. Pour ce faire, dans l'onglet « ***View*** », sélectionnez l'option « ***Advanced Features*** ». Ensuite, effectuez un clic droit sur l'UO en question (ici Finances), « ***Properties*** ». Dans l'onglet « ***Security*** », cliquez sur « ***Advanced*** ». On peut constater que l'utilisateur choisi auparavant possède bien les accès pour créer ou supprimer des utilisateurs.

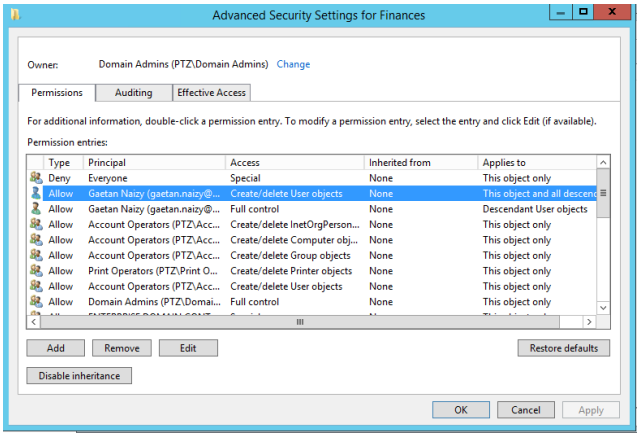

Figure 65 : Vérification des permissions.

Maintenant que la délégation est réalisée, il serait intéressant de mettre en place une console afin que l'utilisateur puisse gérer de manière plus simple ses tâches.

Pour ce faire dans « ***Run*** », tapez la commande « ***mmc*** ». Nous disposons maintenant d'une console vide. Il faut donc ajouter les éléments dont nous avons besoin dans celle-ci. Pour ce faire, dans l'onglet « ***File*** », sélectionnez « ***Add or remove Snap-ins*** ». Ajoutez l'élément « ***Active Directory Users and Computers*** ».

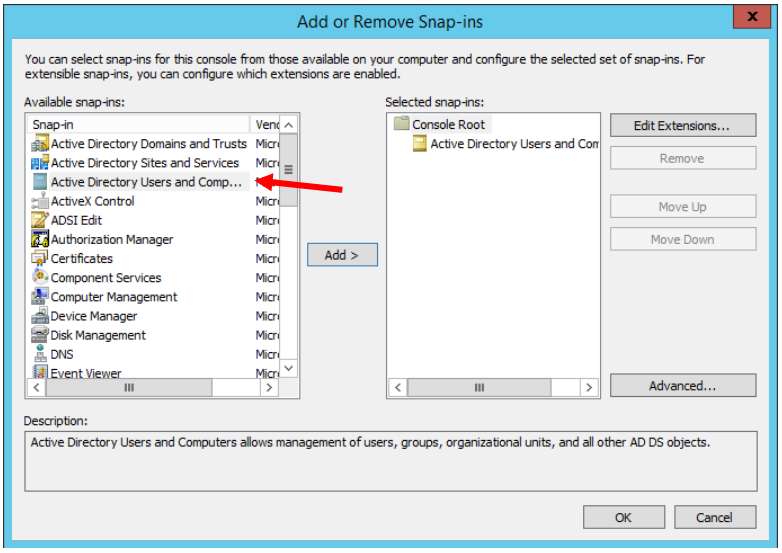

Figure 66 : Ajouter un logiciel composant enfichable.

Actuellement, nous avons accès à toute l'arborescence. Hors, nous ne devons avoir accès qu'à une seule UO. Pour ce faire, nous allons sélectionner l'UO, effectuer un clic droit et sélectionner l'option « ***New Window from here*** ».

Il vous est également possible de personnaliser la console, pour ce faire, il suffit de cliquer sur l'icône à côté de « ***File*** » et de sélectionner « ***Customize View*** ». Une fois que la console vous satisfait, il suffit simplement d'enregistrer celle-ci et de la placer sur le poste client.

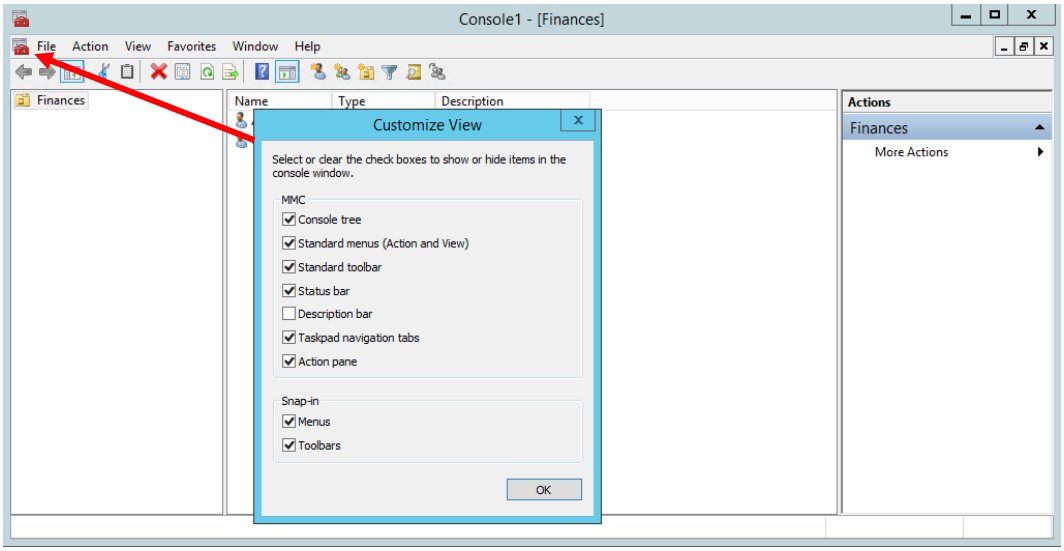

Figure 67 : Console mmc personnalisée.

Lorsque vous allez lancer la console sur le client vous risquez d'avoir l'erreur suivante :

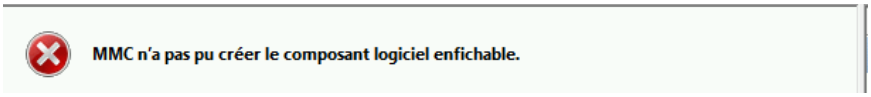

Figure 68 : Erreur MMC sur poste client.

Pour pallier à ce problème vous devez installer les outils d'administration de serveur distant et ajouter des fonctionnalités Windows.
Pour ce dernier, sur le poste client, vous devez aller dans « ***Panneau de configuration*** », « ***Programmes et fonctionnalités*** », « ***Activer ou désactiver des fonctionnalités Windows*** ».
Ensuite, sélectionnez les fonctionnalités suivantes :

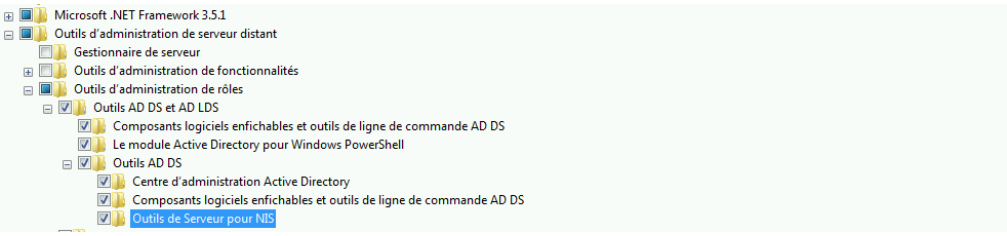

Figure 69 : Activation des outils d'administration de rôle.

7 Les dossiers partagés

Les répertoires partagés permettent un accès à une ressource stockée sur un serveur. Bien entendu cet accès s'effectue depuis le réseau. Lorsque l'on partage un dossier, celui-ci devient disponible pour tous les utilisateurs connectés sur le réseau.
Il faut donc limiter les accès pour assurer la confidentialité des informations. Pour ce faire, il faut mettre en place des autorisations de sécurité. Ces dernières peuvent être placées sur un dossier ou sur un fichier.

L'accès au dossier partagé s'effectue à partir d'un chemin UNC[4]. Celui-ci est composé du nom du serveur qui contient la ressource ainsi que du nom du partage (\\DC-root\partages).

Pour cacher un partage et le transformer en partage administratif, il suffit simplement d'ajouter un « ***$*** » à la fin du partage (\\DC-root\paratages$).

Remarque : Seul le dossier parent doit être partagé. Les sous-dossiers de « partages » ne doivent pas être partagés.

7.1 L'héritage :

Le système NTFS[5] utilise l'héritage pour transmettre les permissions d'accès. Lorsque vous allez créer un dossier ou un fichier, celui-ci va récupérer automatiquement les permissions de sécurité qui sont appliquées à son dossier parent. Dans certain cas, il peut arriver que l'administrateur ait besoin de mettre en place des autorisations autres que celle définit par l'héritage. Afin d'éviter des conflits entre les autorisations héritées et les autorisations déclarées par l'administrateur, il faut bloquer l'héritage.
Vous pouvez le réaliser en cliquant droit sur le répertoire, « ***Properties*** », « ***Security*** », « ***Advanced*** » et cliquer sur « ***Disable inheritance*** »

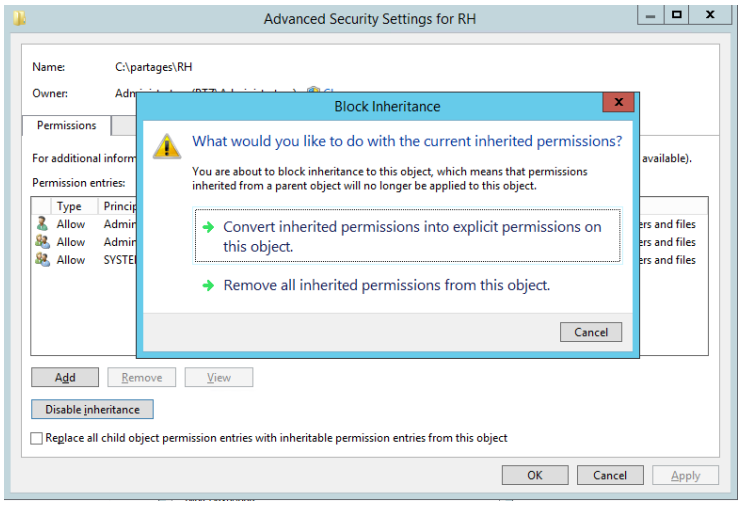

Figure 70 : Désactiver l'héritage.

7.2 Les permissions :

Deux types de permissions peuvent être configurés :

- Les permissions standards
- Les permissions avancées.

[4] UNC : Universal Naming Convention.
[5] NTFS : New Technology File System, système de fichier développé par Microsoft.

7.2.1 Les permissions standards :

Elles sont celles qui sont le plus souvent utilisées.

Permissions	Descriptions
Contrôle total / Full Control	Donne à l'objet concerné (utilisateur, groupe ou ordinateur) les droits complets sur le fichier ou le dossier. Dont la possibilité de modifier les autorisations ou de devenir propriétaire.
Modification / Modify	Permet de lire, écrire et supprimer un fichier ou un dossier. L'objet peut également exécuter un fichier ou en créer un.
Lecture et exécution / Read and execute	Permet de lire un fichier et d'exécuter un programme.
Ecriture / Write	Permet d'écrire dans un fichier
Affichage du contenu du dossier / List folder contents	Permet uniquement de lister les dossiers et les fichiers sans avoir la possibilité de les ouvrir ou de lire le contenu des fichiers.

Tableau 3 : Permissions standards.

7.2.1 Les permissions avancées :

Les permissions avancées permettent la mise en place d'autorisations beaucoup plus fine.

Permissions	Descriptions
Parcours du dossier/exécuter le fichier **Traverse folder / execute file**	Permet à l'objet de parcourir une arborescence. On peut accéder à un fichier sans pouvoir le lire. L'autorisation exécuter permet d'autoriser ou non l'exécution des programmes.
Liste du dossier/lecture de données **List folder/read data**	Contrairement à l'autorisation parcours du dossier, celle-ci s'applique uniquement au dossier et à son contenu. Lecture de données permet d'autoriser ou de refuser un utilisateur à lire les fichiers.
Attributs de lecture / Read Attributes	Permet la lecture des attributs de base d'un fichier ou d'un dossier (lecture seul, caché, …).
Création de fichier/écriture de données **Create files/write data**	Création de fichier : s'applique uniquement au dossier et donne l'autorisation d'écrire à l'intérieur de ce dossier. Ecriture de données : permet à l'utilisateur d'écraser le contenu existant d'un fichier.
Création de dossier / Ajout de données **Create folders / append data**	Création de dossier : donne l'autorisation de créer des dossiers à l'intérieur du répertoire sur lequel est positionnée la permission d'accès.

	Ajout de données : permet l'ajout de données à la fin du fichier. L'utilisateur ne pourra ni modifier ni supprimer les données existantes.
Lecture et exécution, Lecture	Permet seulement de voir le contenu d'un fichier ou d'un dossier.
Attributs d'écriture / Write attributes	Donne l'autorisation de modifier les attributs de base.
Suppression de sous-dossier et fichier Delete subfolders and files	Donne la possibilité de supprimer les sous-dossiers et les fichiers. Ne s'applique qu'au dossier.
Suppression / Delete	Permet de supprimer les dossiers et les fichiers. L'utilisateur doit posséder la permission suppression de sous-dossier et fichier sur le dossier parent.
Autorisations de lecture Read permissions	Autorise l'objet qui possède cette permission à lire les droits positionnés sur une ressource.
Modifier les autorisations Change permissions	Permet de modifier les autorisations.
Approbation Take ownership	Autorise l'utilisateur à devenir propriétaire de la ressource, il aura la possibilité de modifier les permissions.

Tableau 4 : Permissions avancées.

7.3 Les quotas :

Les quotas vous permettre de :

- Limiter l'espace autorisé pour un volume ou un dossier et générer des notifications lorsque les limites de quota approchent ou sont dépassées ;
- On peut aussi générer des quotas automatiques qui vont s'appliquer à tous les sous-dossiers existants dans un volume ou un dossier, ainsi qu'à tous les sous-dossiers qui seront créés ultérieurement ;
- Vous pourrez également définir des modèles de quota facilement applicables aux nouveaux volumes ou dossiers. Ceux-ci seront disponibles pour toute l'organisation.

Dans un premier temps, il faut vérifier si l'outil « ***File Server Ressource Manager*** » est bien installé. Pour ce faire, sélectionnez dans « ***Server manager*** », le rôle « ***Files and Storage Services*** » et l'option « ***Shares*** ». Dans celle-ci vous pouvez voir dans la partie quota si l'outil « ***File Server Ressource Manager*** » est installé. Si pas il vous suffit de cliquer sur le lien présent dans la fenêtre.

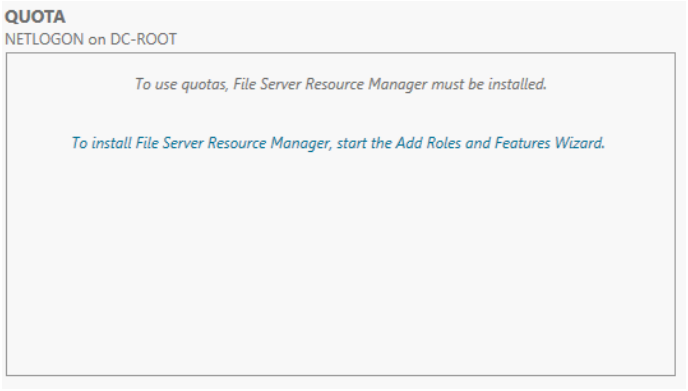

Figure 71 : Installation de File Server Ressource Manager.

Une fois le rôle installé, ouvrez l'outil « ***File Server Ressource Manager*** » et sélectionnez dans celui-ci « ***Quota Management*** ».

7.3.1 Création d'un quota à partir d'un modèle :

Dans l'outil « ***Quota Management*** », sélectionnez l'onglet « ***Quota Templates*** » et sélectionnez l'un des modèles présents dans la fenêtre. Faites un clic droit sur celui-ci et choisissez « ***Create quota from template …*** ».

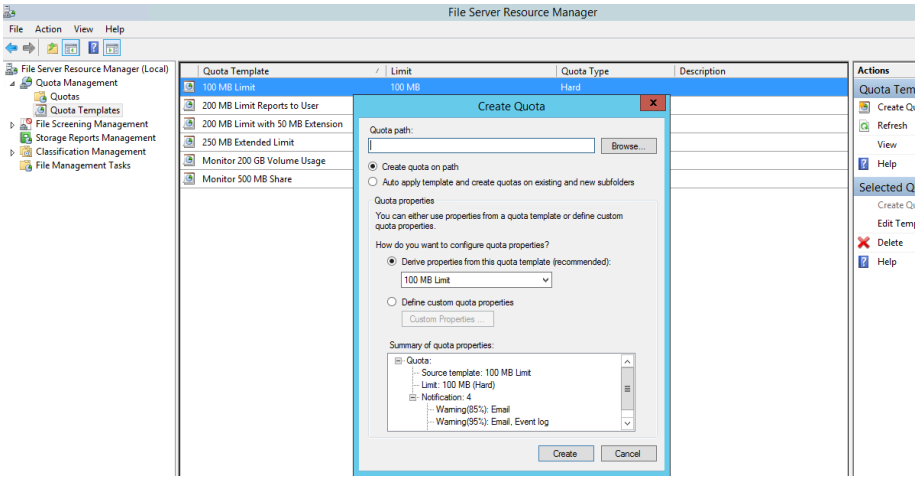

Figure 72 : Créer un quota à partir d'un modèle.

Dans la fenêtre « ***Create Quota*** » il faut indiquer le dossier sur lequel vous désirez mettre le quota et cliquer sur « ***Create*** ».
Pour vérifier si le quota est bien mis en place, il suffit de sélectionner l'onglet « ***Quotas*** ».

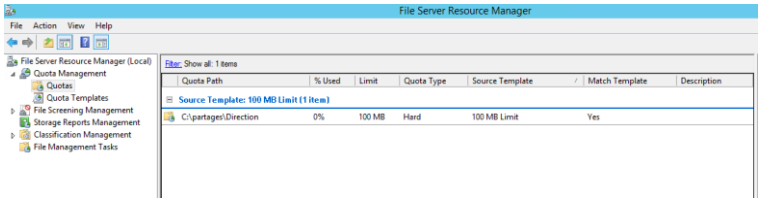

Figure 73 : Vérification de la création du quota.

7.3.2 Création d'un quota automatique :

Dans l'outil « ***Quota Management*** », sélectionnez l'onglet « ***Quotas*** », effectuez un clic droit sur celui-ci et sélectionnez « ***Create Quota*** ». Dans cette dernière, choisissez le chemin du ***dossier parent*** sur lequel vous allez mettre en place le quota.

Afin d'effectuer un quota automatique, c'est-à-dire que le quota soit également effectif sur tous les dossiers enfants, il faut cocher l'option « ***Auto apply template and create quotas on existing and new subfolders*** ».

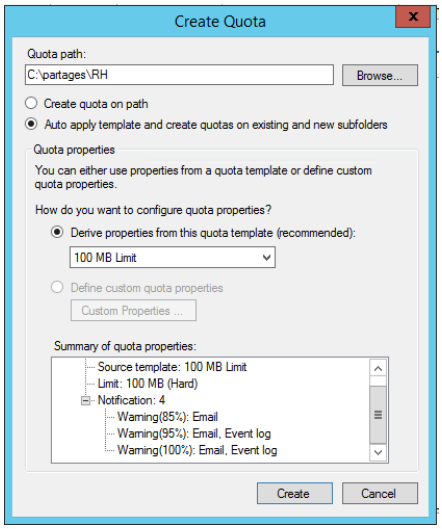

Figure 74 : Créer un quota automatique.

Il vous est également possible de modifier les propriétés du quota automatique en cliquant droit sur celui-ci, « ***Edit Quotas properties*** ». Attention, la seule modification que vous pourrez apporter, sera le changement de modèle. Vous ne pourrez pas définir vous-même les limites du quota, …

7.3.3 Création d'un modèle de quota :

Dans l'outil « ***Quota Management*** », sélectionnez l'onglet « ***Quota Templates*** », effectuez un clic droit sur celui-ci et cliquez sur « ***Create quota template*** ».
Dans cette fenêtre, donnez un nom à votre modèle, éventuellement une description mais surtout définir les limitations et les alertes.

Vous avez également la possibilité de choisir entre deux options « Hard Quota » ou « Soft Quota » :

- Hard Quota : Empêche les utilisateurs à enregistrer leur fichier lorsque la limite d'espace est atteinte et génère des notifications lorsque le volume de données atteint un seuil configuré.

- Soft Quota : Permet aux utilisateurs d'enregistrer leur fichier mais génère tout de même toutes les notifications configurées.

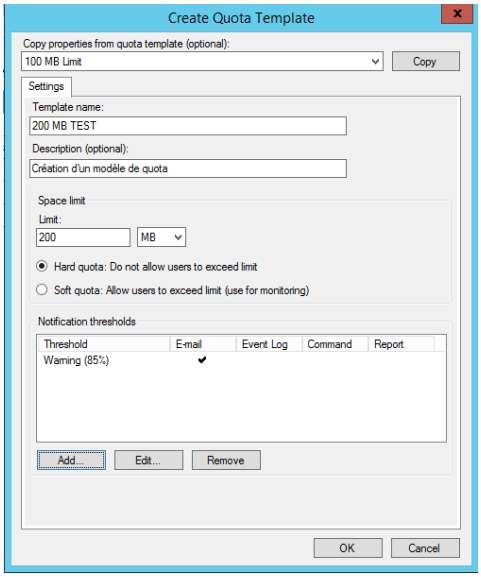

Figure 75 : Créer un modèle de quota.

7.4 Volume Shadow Copy :

Shadow copy permet de réaliser un instantanée des fichiers/ dossiers du partage.

Cette outil permet de :

- Récupérer les fichiers accidentellement effacés ;
- Récupérer les fichiers malencontreusement écrasés ou mis à jour ;
- D'implémenter la notion de version sur les documents sur lesquels les utilisateurs travaillent.
- Limiter les accès physiques aux serveurs pour effectuer des backups de fichiers à restaurer en offrant des possibilités de récupération de fichier directement sur un poste client.

Afin d'activer cette option, vous devez effectuer un clic droit sur votre disque C et sélectionner « ***Configure Shadow Copy …*** ».
Dans la fenêtre « ***Shadow Copy*** » sélectionnez le disque C et cliquez sur « ***Enable*** ».

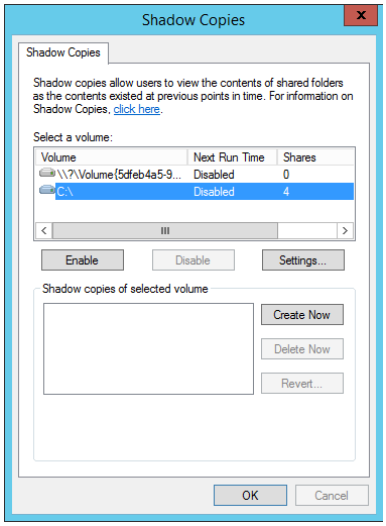

Figure 76 : Activer Shadow Copy.

Maintenant il faut planifier les sauvegardes pour ce faire cliquer sur « ***Settings*** ».
Dans ces paramètres, vous pouvez modifier la taille maximum que Shadow Copy va utiliser pour ses instantanées. Il vous est également possible de planifier les instantanées en cliquant sur « ***Schedule*** ».

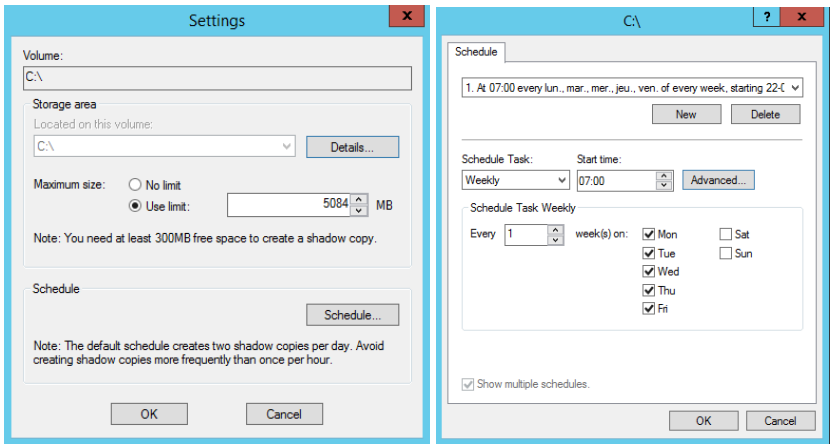

Figure 77 : Paramètres de Shadow Copy.

On peut maintenant accéder aux dossiers partagés et voir les versions précédentes en allant dans les propriétés de celui-ci et en sélectionnant l'onglet « ***Previous Versions*** ». Vous pouvez à partir de cette onglet, effectuer une restauration ou supprimer un instantanées.

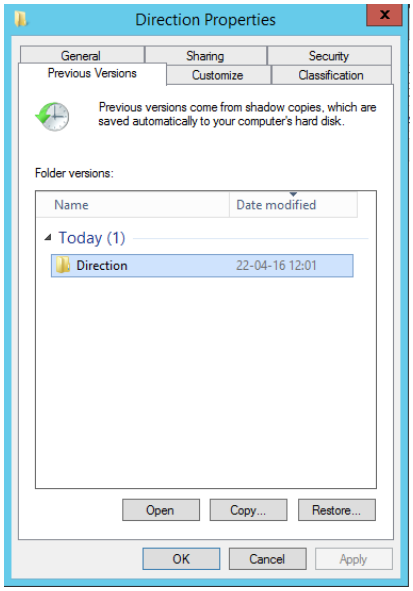

Figure 78 : Instantanées via Shadow Copy.

8 Windows Server Backup

Afin de réaliser différents types de sauvegarde, nous allons utiliser le rôle « ***Windows Server Backup*** ». Il vous faudra donc installer ce rôle.

Avant toute chose, nous allons configurer les performances de notre backup. Pour ce faire, il faut, dans l'onglet « ***Actions*** », sélectionner « ***Configure Performance Settings …*** ».

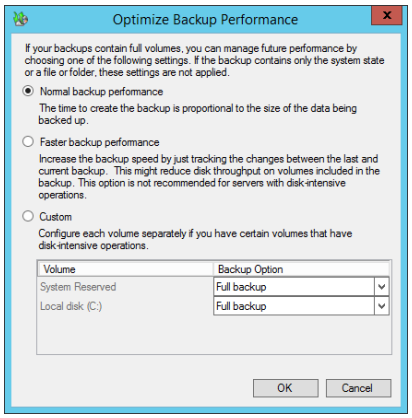

Figure 79 : Optimisation des performances du backup.

Il existe deux types de sauvegardes :

- ***Normal backup performance*** : Les sauvegardes qui seront réalisées seront des sauvegardes complètes. Dans ce cas, Windows transfère l'intégralité du contenu du volume faisant l'objet de la sauvegarde. L'espace utilisé au niveau de l'emplacement de stockage de la sauvegarde correspond uniquement aux blocs modifiés sur la source.

- ***Faster backup performance*** : Il s'agit dans ce cas d'une sauvegarde incrémentielle. Windows conserve un cliché instantané sur le volume source afin de pouvoir faire le suivi des modifications. Lors de la prochaine sauvegarde, seules les modifications apportées depuis la dernière sauvegarde seront transférées. L'espace de stockage de la sauvegarde correspond uniquement aux blocs modifiés détectés sur la source.

Dans le rôle « ***Windows Server Backup*** », il est possible d'effectuer plusieurs actions :

- Backup Schedule ;
- Backup Once ;
- Recover.

8.1 Backup Schedule :

Cette option vous permet de planifier des sauvegardes (par exemple journalière) de votre serveur de manière automatique. La première chose qui vous sera demandée, c'est de choisir un emplacement pour effectuer votre sauvegarde. Il est préférable de dédier un disque complet pour un backup plutôt que de créer un volume ou autre. En effet, si vous n'utilisez pas un disque complet, vous pourrez constater une diminution des performances d'E/S au niveau de l'écriture.

Lorsque vous choisissez l'option « ***Backup Schedule*** », vous avez 2 types de sauvegardes possibles.

- Soit vous effectuez un backup complet du serveur
- Soit vous effectuez un backup personnalisé dans lequel vous allez pouvoir sélectionner les éléments à sauvegarder.
  Dans cette dernière option vous pouvez par exemple sauvegarder que le « ***System State***[6] ».

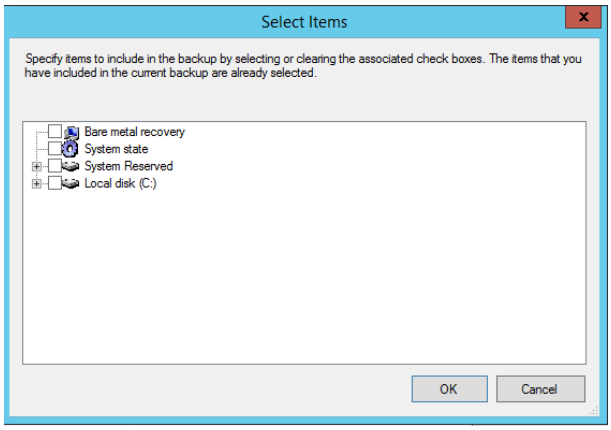

Figure 80 : Eléments disponibles lors d'un backup personnalisé.

[6] Le System State contient les registres, les différentes configurations des rôles mis en place (DHCP, DNS,…) mais aussi tout le contenu de la configuration de l'Active Directory.

8.2 Backup Once :

Cette option vous permet d'effectuer soit :

- Un backup complet de votre machine.
- Un backup personnalisé comme vu dans le point précédent.

La différence avec l'option « ***Backup Schedule*** » réside dans le fait que vous ne pouvez pas planifier la sauvegarde. Ce qui veut dire que la sauvegarde ne peut s'effectuer qu'une seule fois et de manière manuelle.

8.3 Recover :

L'option « ***Recover*** » permet de restaurer des fichiers, des applications, des volumes à partir d'un backup réalisé au préalable.

L'option « ***Select recovery types*** » vous permettra de choisir le type de fichiers que vous voulez sauvegarder (fichiers, applications, …).

9 Les Stratégies de groupe

Une stratégie de groupe est un objet qui contient un ou plusieurs paramètres de stratégie. Ceux-ci peuvent appliqués des paramètres de configuration à des ordinateurs, des utilisateurs ou éventuellement les deux.

Les stratégies de groupe sont divisées en deux parties :

- Les stratégies locales :
  Utilisées lors d'une approche individuelle des postes de travail.
- Les stratégies du domaine :
  Celles-ci sont indispensables pour configurer les postes clients d'un réseau de grande taille. Ce sont ces dernières que nous allons principalement utilisées.

Les paramètres des utilisateurs et des ordinateurs ont chacun trois domaines de configuration.

Domaine de configuration	Description
Paramètres logiciels	Comprennent les paramètres logiciels qui peuvent être déployés pour l'utilisateur ou l'ordinateur. Les logiciels qui sont déployés pour un utilisateur sont spécifiques à cet utilisateur. Les logiciels qui sont déployés pour l'ordinateur sont à la disposition de tous les utilisateurs de cet ordinateur.

Paramètres du système d'exploitation Windows	Comprennent les paramètres de script et les paramètres de sécurité pour l'utilisateur et l'ordinateur et la maintenance Internet Explorer pour la configuration utilisateur.
Modèles d'administration	Comprennent des centaines de paramètres qui modifient le Registre afin de contrôler les divers aspects de l'environnement de l'utilisateur et de l'ordinateur. De nouveaux modèles d'administration peuvent être créés par Microsoft ou d'autres fournisseurs.

Tableau 5 : Domaines de configuration des paramètres de stratégie de groupe.

Pour ce qui est des stratégies du domaine, il existe 3 niveaux d'applications différents dans l'AD.

- ***Les GPO actives au niveau Site :***
  Celles-ci affectent les utilisateurs en fonction du lieu de connexion.
- ***Les GPO actives au niveau Domaine :***
  Celles-ci affectent tous les utilisateurs et ordinateurs du domaine, toutes les UO et tous les sous-conteneurs UO.
- ***Les GPO actives au niveau UO :***
  Celles-ci affectent les utilisateurs et ordinateurs présente dans l'UO ainsi que les objets créés dans les UO enfants.

Les stratégies de groupes s'appliquent dans l'ordre suivant :

- Stratégies locales
- Sites
- Domaine
- Unité d'organisation

Lorsqu'une GPO est liée à une OU dans l'AD, les objets situés en dessous héritent des paramètres de stratégies de groupes venant du niveau supérieur.

9.1 La console GPMC[7] :

Il existe plusieurs manières d'accéder à la console GPMC.

- Via la boîte de dialogue « ***Exécuter*** », en tapant la commande « ***gpmc.msc*** ».

- Via la console « ***Server Manager*** », « ***Tools*** », « ***Group Policy Management*** ».

Une fois la console démarrée, on peut constater que celle-ci possède une arborescence qui débute au niveau de la forêt Active Directory et continue au niveau du domaine. Cette console

[7] ***GPMC*** : Group Policy Management Console – Console de gestion des stratégies de groupe.

GMPC est identique à celle de la console « ***Active Directory – Users and computers*** » mais sans les conteneurs « ***Builtin*** », « ***Computers*** » et « ***Users*** ». Ceux-ci n'étant pas des UO, on ne peut donc pas les liés à des stratégies de groupe.

On peut également constater que par défaut il existe déjà deux stratégies « ***Default Domain Controlers Policy*** » et « ***Default Domain Policy*** ».

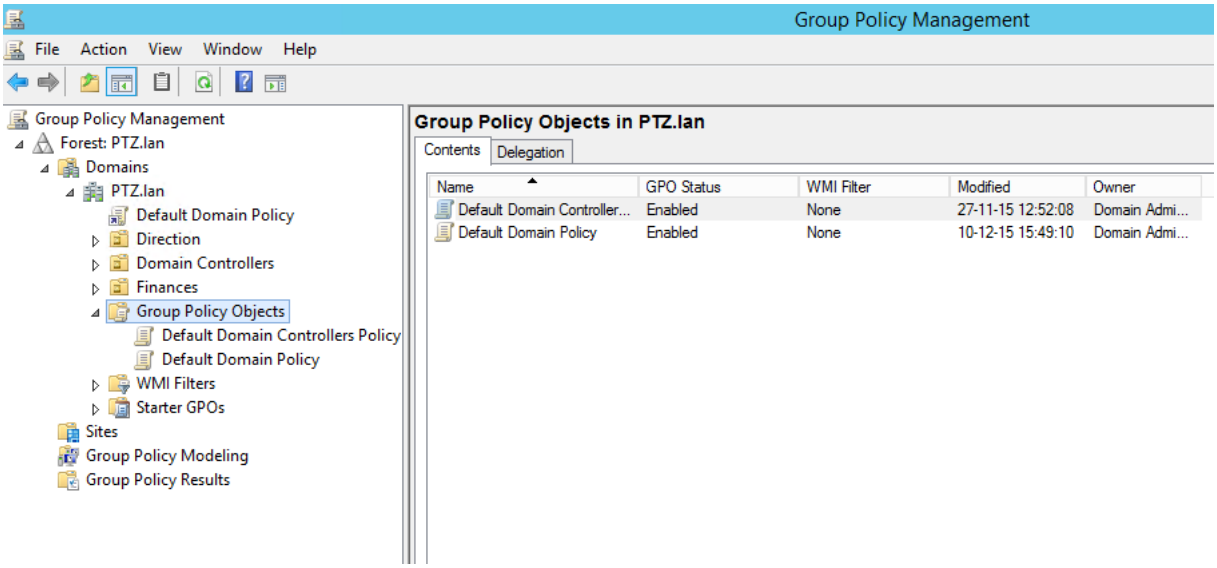

Figure 81 : Console Group Policy Management.

Afin de se familiariser avec cette console, nous allons créer une première stratégie.
Pour créer celle-ci, il suffit d'effectuer un clic droit dans la partie vide du conteneur « ***Group Policy Objects*** » et cliquer sur « ***New*** ». Dans la fenêtre suivante, il vous faudra préciser un nom à cette stratégie.

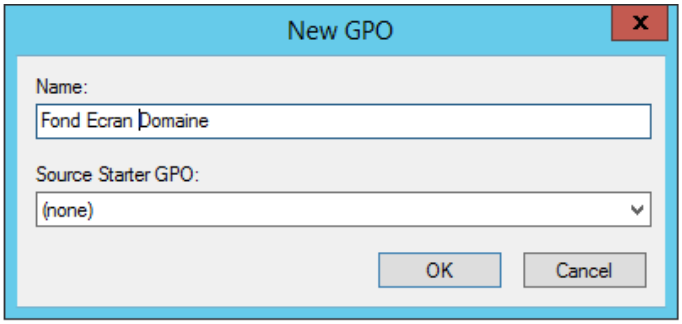

Figure 82 : Créer une GPO.

ATTENTION : Cette étape ne doit pas être négligée car le nom fait partie des informations d'identification des objets de stratégie sur le réseau. Lorsqu'une stratégie doit être identifiée rapidement, le nom donné à l'objet constitue le premier critère de recherche.

Maintenant que la GPO est créé, nous allons pouvoir paramétrer celle-ci. ***ATTENTION*** : Plus il y aura des critères configurés dans une stratégie, plus sera complexe la résolution de problème et le dépannage de celle-ci.

Pour éditer la stratégie, cliquez droit sur celle-ci et choisissez « ***Edit*** ». L'éditeur de gestion des stratégies de groupe s'ouvre. Celle-ci permet d'accéder aux paramètres de configuration des stratégies de groupe.

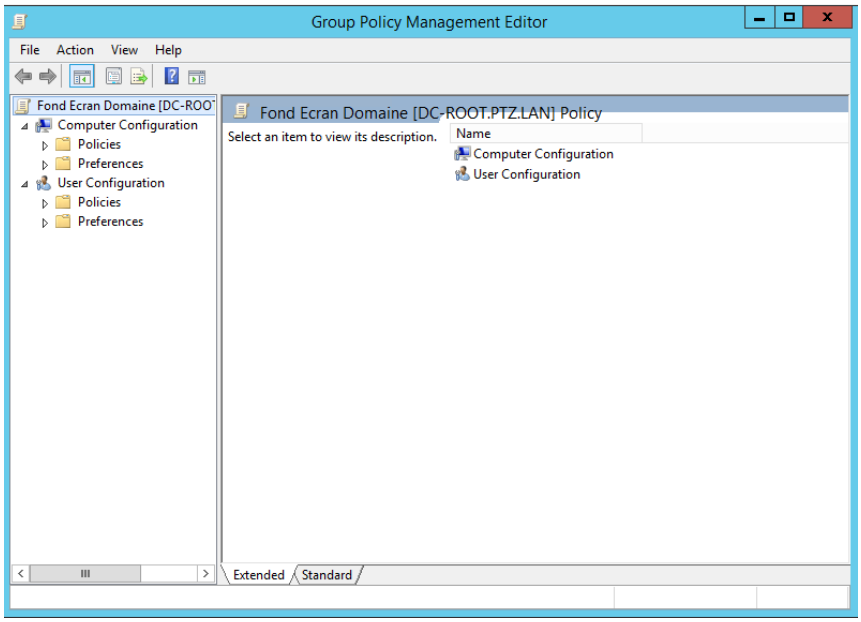

Figure 83 : Group Policy Management Editor.

Le but de notre GPO étant de modifier le fond d'écran des postes de travail, il faut au préalable placer le fichier dans un dossier partagé.

Nous allons dans un premier temps créer un paramètre de préférence afin que le fichier image soit copié sur les postes distants. Pour ce faire dans « ***Computer Configuration*** », « ***Preferences*** », « ***Windows settings*** » et « ***Files*** ». Effectuez un clic droit sur ce dernier et sélectionnez « ***New*** », « ***File*** ».

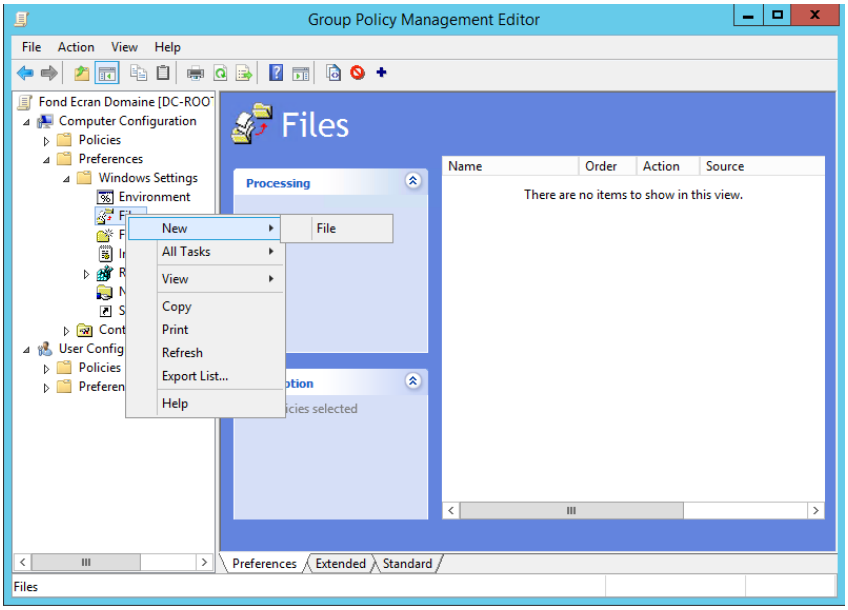

Figure 84 : Ajouter un fichier dans une GPO.

La fenêtre suivante nous permet de stipuler l'endroit où est stockée le fichier, l'endroit où le fichier doit être placé sur la machine distante (Par défaut le dossier où Windows stocke tous les fonds d'écran est le suivant : « ***C:\Windows\Web\Wallpaper\wallpaper.png*** ») ainsi que l'action qui doit être entreprise (dans ce cas ce sera « ***Create*** » étant donné que le fichier n'existe pas sur le poste distant).

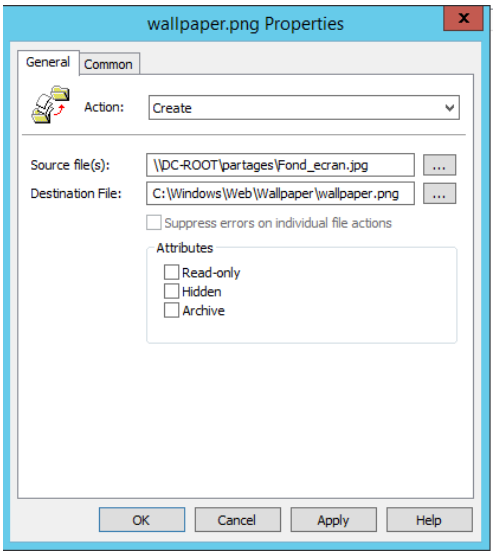

Figure 85 : Propriétés du fichier.

Ensuite, il faut aller dans l'onglet « ***Common*** » afin de préciser que l'action ne doit se réaliser qu'une seule fois.

L'étape suivante consiste à appliquer le fond d'écran sur les machines distante.
Pour ce faire, dans « ***User configurations*** », « ***Policies*** », « ***Adminsitrative Templates*** », « ***Desktop*** », sélectionnez « ***Desktop Wallpaper*** ».

Dans la fenêtre suivante, il faut activer cette option et préciser le chemin vers lequel on pourra trouver le fond d'écran.

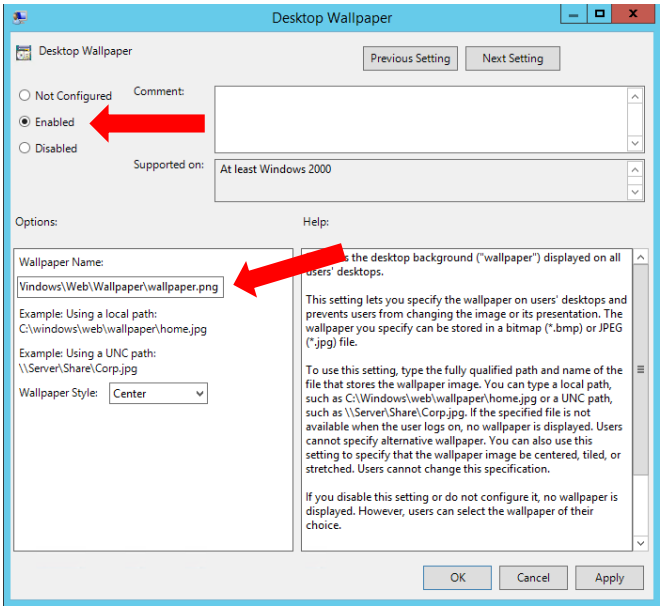

Figure 86 : Desktop Wallpaper Activation.

Avant de voir si le fond d'écran est effectif sur le poste distant, il faut appliquer la GPO sur l'UO concernée. Dans ce cas, je veux l'appliquer au domaine.
Pour appliquer la GPO, il faut effectuer un clic droit sur l'emplacement concerné et choisir « ***Link an existing GPO …*** ». Dans cette fenêtre il suffira de choisir la GPO que l'on vient de créer.

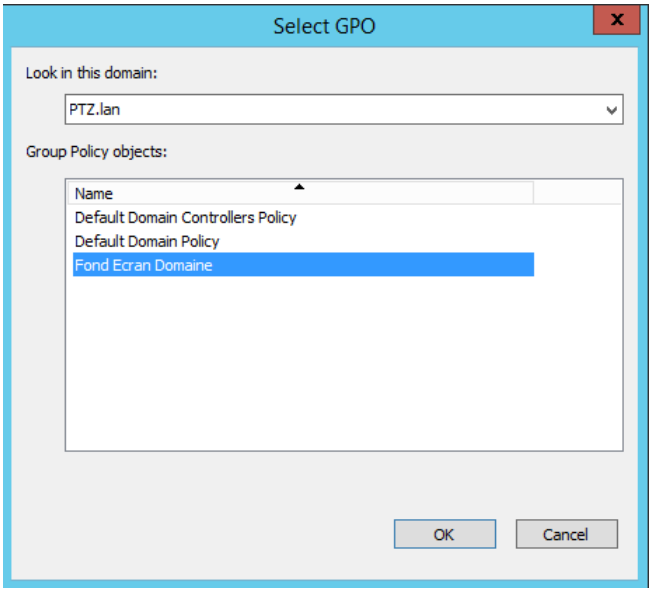

Figure 87 : Appliquer une GPO.

9.2 Redirection du dossier « Mes documents » sur le serveur de fichier :

Nous allons maintenant créer une GPO permettant de rediriger le dossier « ***Mes Documents*** » vers un dossier du partage.

Dans un premier temps créez la GPO (n'oubliez pas de lui donner un nom correcte), ensuite éditez celle-ci.

La redirection de dossier s'effectue dans la rubrique « ***User Configuration*** », « ***Windows Settings*** » et « ***Folder Redirection*** ».

Dans ce dernier, vous retrouvez différents dossiers. Celui qui nous intéresse est forcément « ***Documents*** ». Effectuez un clic droit sur celui-ci et sélectionnez « ***Propertie***s ».

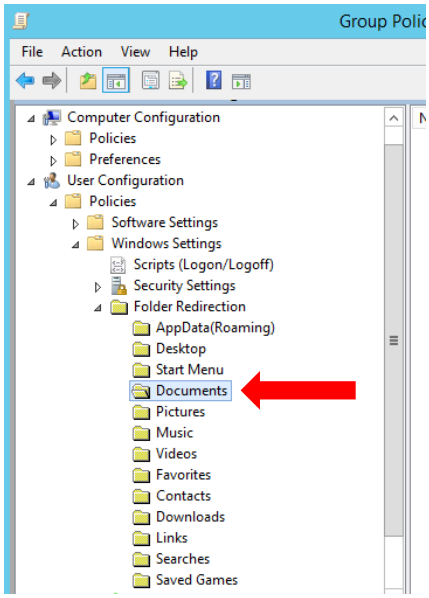

Figure 88 : Redirection de dossier.

Dans les propriétés de l'objet, nous allons dans un premier temps sélectionner l'option « ***Basic – Redirect everyone's folder to the same location*** ». Ensuite nous allons stipuler l'emplacement dans lequel ce dossier devra être copié et de quelle manière (Dans ce cas, nous créons un dossier pour chaque utilisateur dans le dossier parent stipulé).

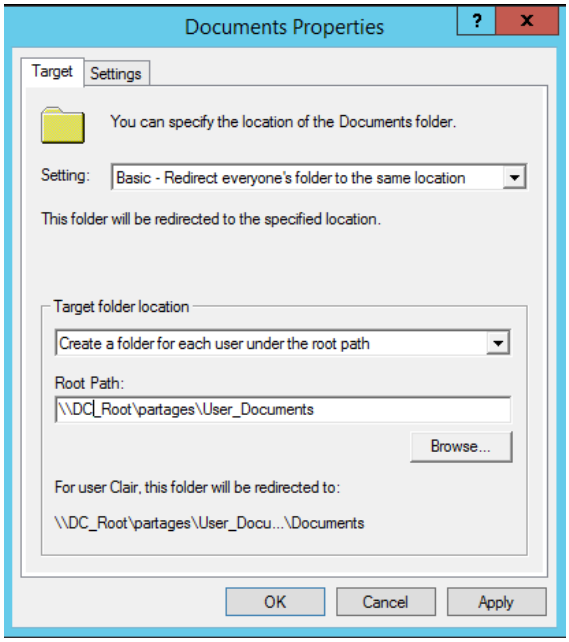

Figure 89 : Redirection de dossier – Propriétés.

N'oubliez pas une fois les paramètres validés d'activer la GPO et de tester le bon fonctionnement de celle-ci.

10 Bibliographie

- BONNET N., *Préparation à la certification MCSA Windows Server 2012 – Installation et Configuration*, Editions ENI, France, Avril 2013
- ASIMANE A., *Préparation à l'examen MCSA Windows Server 2012 – Configurations des services avancés*, Editions ENI, France, Octobre 2013
- BENICHOU J. & BEZET-TORRES J., *Les stratégies de groupe (GPO) sous Windows Server 2012 – Planification, déploiement, dépannage*, Editions ENI, France, Octobre 2013

11 Table des illustrations

12 Liste des tableaux