BTS Services Informatiques aux Organisations
Option Solutions d'Infrastructure, Systèmes et Réseaux

Epreuve E4 : Conception et Maintenance de solutions Informatiques

Documentation technique

Projet 1 : Mise en place d'un contrôleur de domaine sous Windows Server 2012 avec les services AD-DS, DHCP, DNS et mise en place de GPO

JORDA Ludovic

Session 2018

Table des matières

Table des figures

Nature de l'activité
Contexte : Mise en place d'un serveur de domaine sous Windows Server 2012 avec les services AD-DS, DHCP, DNS et mise en place GPOs pour la Maison des Ligues (M2L)
Objectifs : Contrôleur de domaine, Active Directory, DHCP, DNS, GPOs fonctionnels

<table>
<tr><th colspan="2">Environnement technologique</th></tr>
<tr><td>Matériels :

• Ordinateur sous Windows Server 2012
• Ordinateur sous Windows 10</td><td rowspan="2">Durée de réalisation : 45 minutes</td></tr>
<tr><td>Logiciels :

• Oracle VirtualBox
• Windows Server 2012 R2
• Windows 10
• IPCOP
• DNS
• DHCP</td></tr>
</table>

1. Installation des services Active Directory

Pour commencer, nous allons nous connecter à la machine Windows Server 2012 ; ce qui ouvrira automatiquement le **Gestionnaire de serveur**. Nous allons donc cliquer sur : **Gérer → Ajouter des rôles et des fonctionnalités**.

Figure 1 : Le gestionnaire de serveur

De là, nous allons nous rendre dans l'onglet « **Rôles de serveurs** » pour y cocher exclusivement les **services AD DS** (permettent la création d'un contrôleur de domaine).

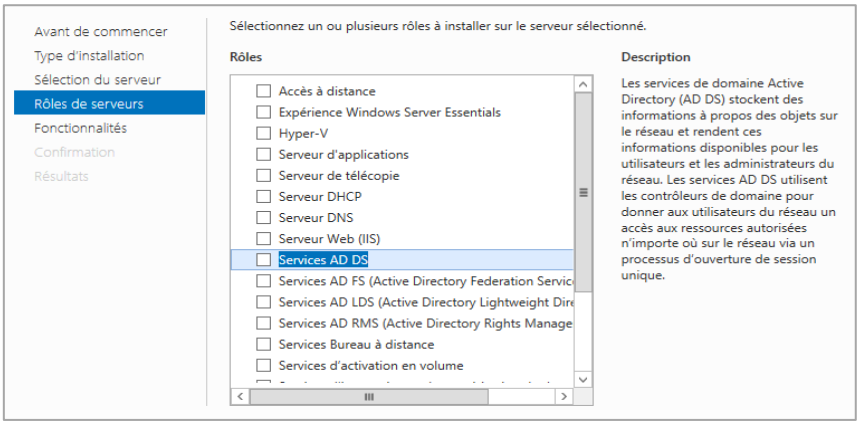

Figure 2 : Sélection des rôles de serveurs

A la fin de l'opération, le contrôleur de domaine va redémarrer. Nous profiterons du temps d'installation des services pour renommer le serveur **M2L-Serveur** via **Propriétés Système → Modifier les paramètres → Modifier** (voir page 17).

2. Création du domaine « M2L »

Une fois l'installation terminée, nous devons nous rendre sur l'interface du **Gestionnaire de serveur** pour cliquer sur le **drapeau à côté de** « **Gérer** » ; ce qui va nous permettre de **promouvoir le serveur en tant que contrôleur de domaine**. Nous arrivons ensuite à la configuration du déploiement et de la création d'une nouvelle forêt. De là, nous pouvons ajouter un nom de domaine avec pour fin «.local ». Nous allons donc cocher « **Ajouter une nouvelle forêt** », entrer un nom de domaine et un mot de passe.

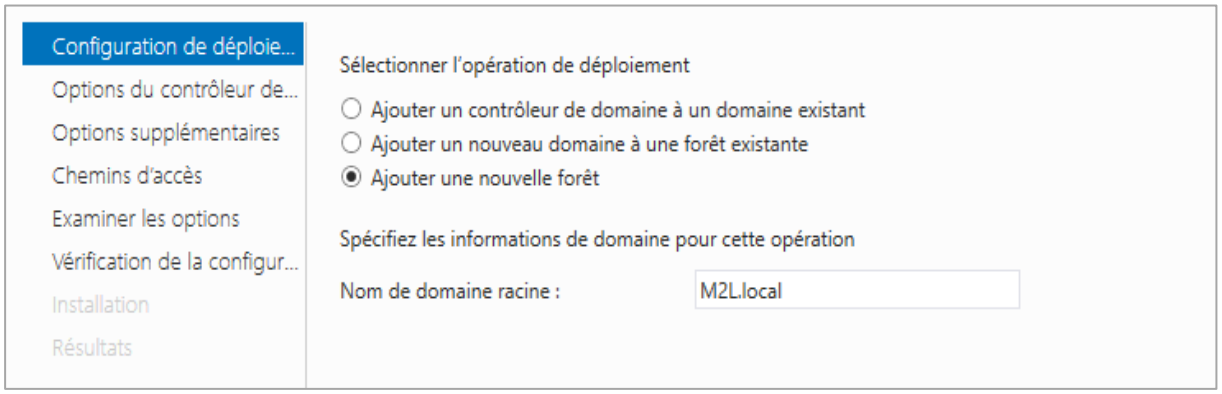

Figure 3 : Configuration de déploiement

Il nous faut par la suite saisir le **nom de domaine du NetBIOS** en majuscule. Nous laisserons les chemins par défauts.

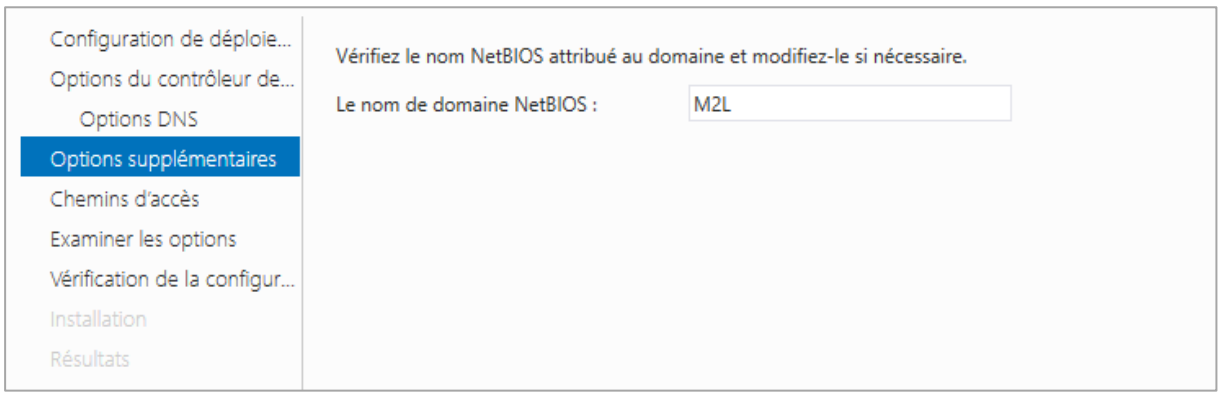

Figure 4 : Choix du nom de domaine NetBIOS

Nous devons maintenant vérifier que le serveur DNS a bel et bien été installé. Une fois ceci fait, le serveur devra redémarrer pour pouvoir prendre en compte les modifications système effectuées.

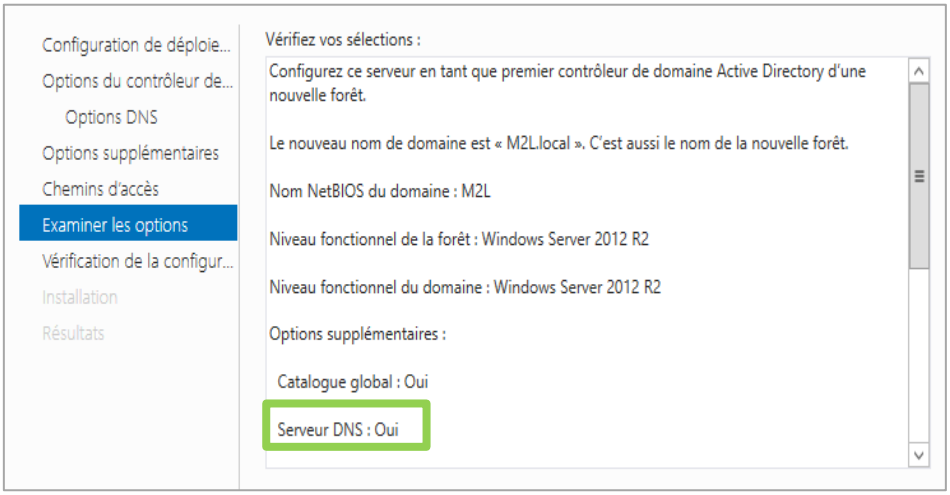

Figure 5 : Rapport des options installées

3. Configuration du serveur DNS

Dans le **Gestionnaire de serveur** cliquons sur **Adresse IPv4 attribuée par DHCP → Protocole Internet version 4 → Propriétés** ; nous allons déterminer une adresse IP fixe de classe B. L'adresse de passerelle par défaut correspond à l'adresse du routeur soit 172.16.6.1 (relevée avec la commande DOS « ipconfig/all »).

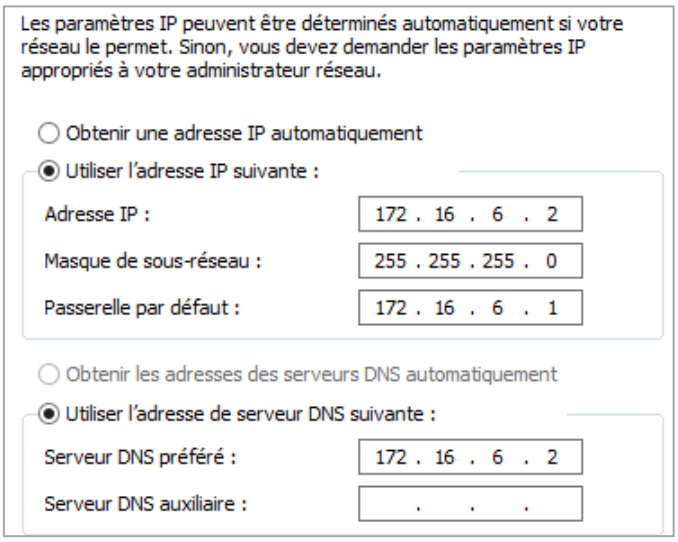

Figure 6 : Paramètres IP du contrôleur de domaine

Nous allons maintenant aller dans **Outils d'administration → DNS** ; puis faire afficher les **propriétés** de notre serveur. On remarque que l'adresse IP du serveur DNS correspond à celle que l'on vient de saisir.

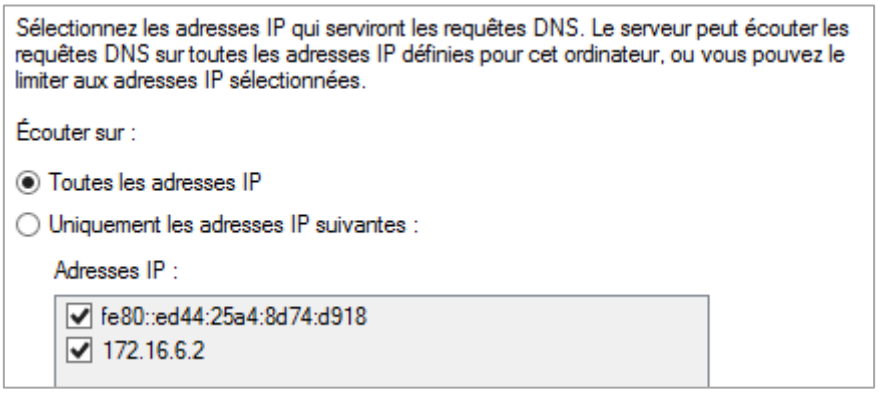

Figure 7 : Vérification des paramètres IP du serveur DNS

Dans la plupart des recherches DNS (Domain Name System), les clients effectuent des recherches directes, à savoir des recherches basées sur le nom DNS d'un autre ordinateur stocké dans un enregistrement de ressource hôte. Ce type de requête attend une adresse IP comme données de ressource pour la réponse.

Rendons-nous dans **Outils d'administration -> DNS -> Clic droit sur Zones de recherche inversées -> Nouvelle zone**. C'est ainsi que nous sommes invités à saisir l'ID du réseau (172.16. 0).

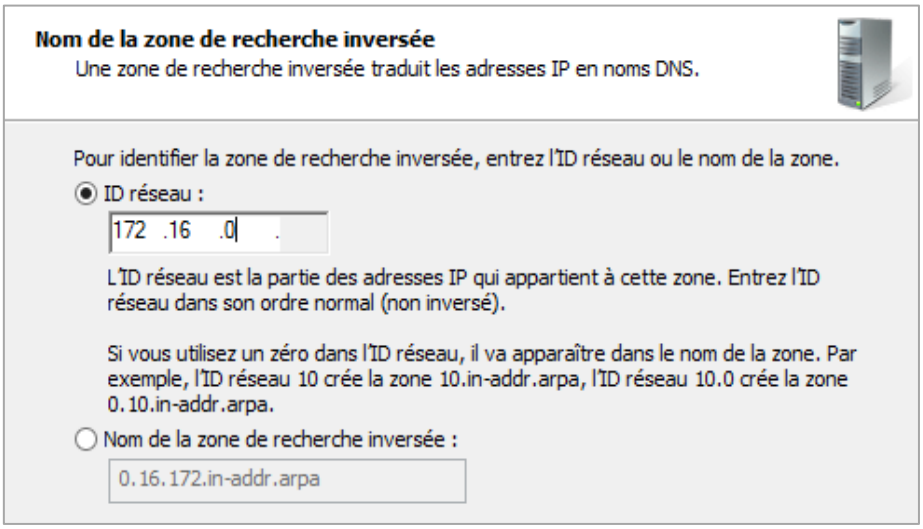

Figure 8 : Identification de la zone de recherche inversée

4. Configuration du serveur DHCP

Nous allons maintenant installer le service DHCP qui nous permettra de distribuer des paramètres IP de manière automatique.
Après avoir ajouté au serveur le rôle « **Serveur DHCP** » de la même manière que l'on a ajouté les services AD DS (voir page 4), nous allons nous en terminer la configuration. Pour ce faire nous allons cliquer sur le **drapeau jaune** puis sur « **Terminer la configuration DHCP** » et enfin sur « Valider ».

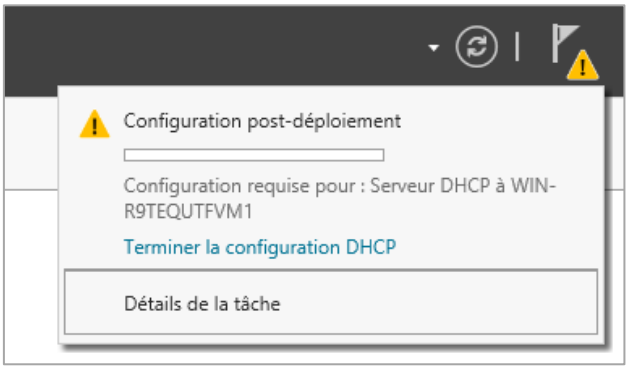

Figure 9 : Finalisation de la configuration du serveur DHCP

La première étape de la configuration du DHCP sera la création d'une étendue pour chaque bâtiment. Pour ce faire, il nous faut ouvrir le « **DHCP** » via « **Outils d'administration** ».

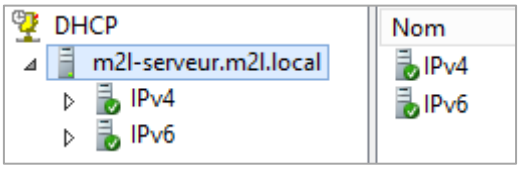

Figure 10 : DHCP

Nous allons donc créer une nouvelle étendue pour chacun des bâtiments en faisant un **clic droit sur IPv4 → Nouvelle étendue**.

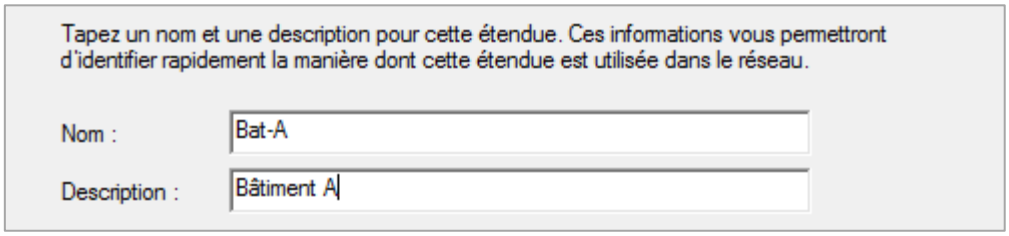

Figure 11 : Création des étendues DHCP pour chacun des bâtiments

Puis, nous il nous faut renseigner les plages d'adresses IP à partir du schéma réseau du contexte M2L.

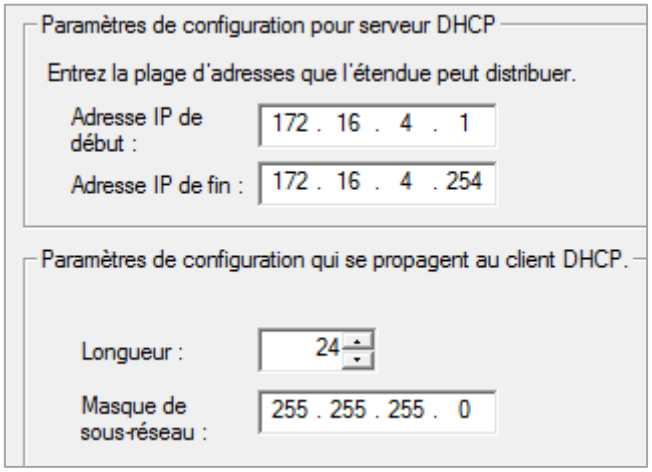

Figure 12 : Définition de la plage d'adresses pour la bâtiment A

Nous devons par la suite définir la durée du bail qui spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue. Nous allons la limiter à **sept jours** dans la mesure où un renouvellement trop fréquemment des baux peut surcharger le serveur suivant sa fréquence d'utilisation en entreprise.

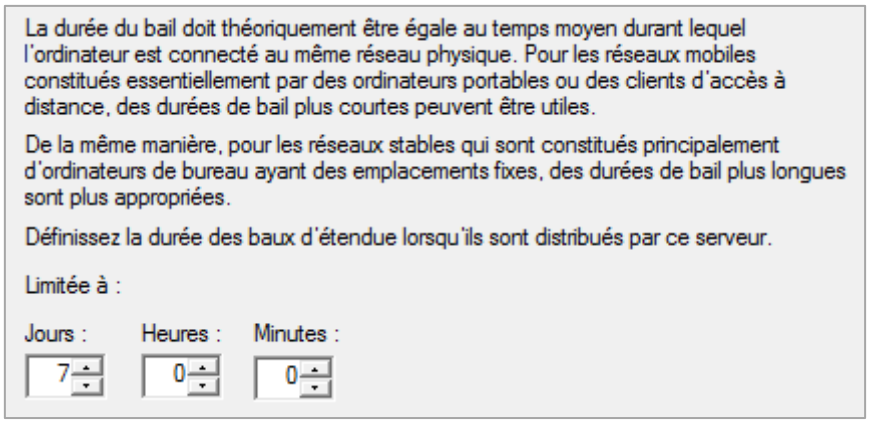

Figure 13 : Définition de la durée des baux d'étendue

Puis, nous allons configurer les options DHCP les plus courantes de façon à ce que les clients puissent utiliser leurs étendues respectives. ; Nous allons donc indiquer **l'adresse du routeur** (192.161.12.1) qui sera distribuée par le service DHCP.

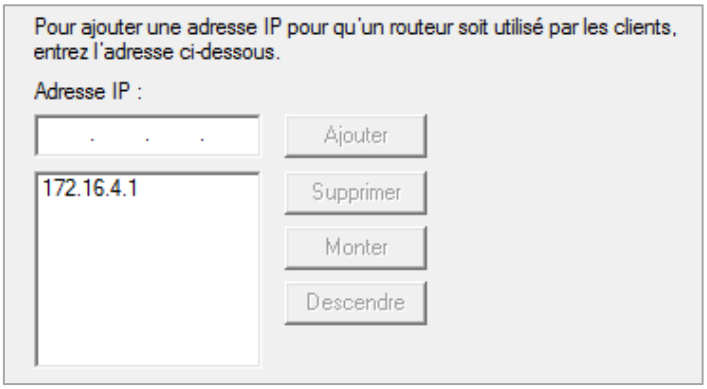

Figure 14 : Ajout de l'adresse du routeur

Nous pouvons ainsi saisir **l'adresse IP du serveur DNS** afin de le lier au serveur DHCP via le domaine parent à savoir M2L.local

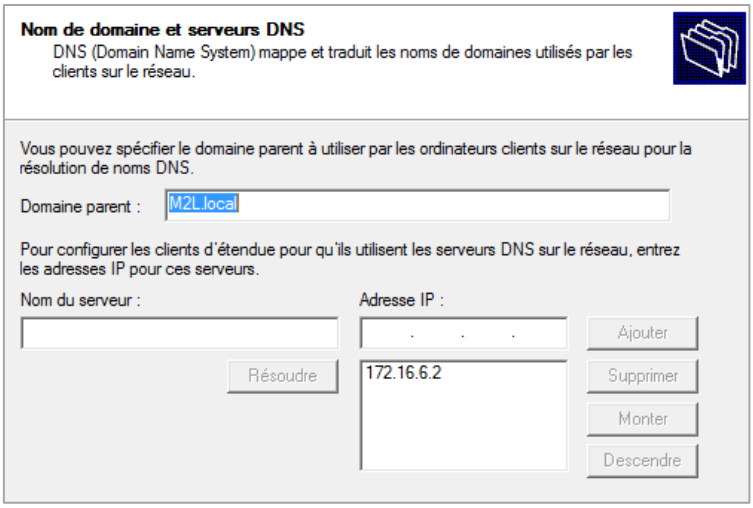

Figure 15 : Liaison du DHCP et du DNS via le domaine

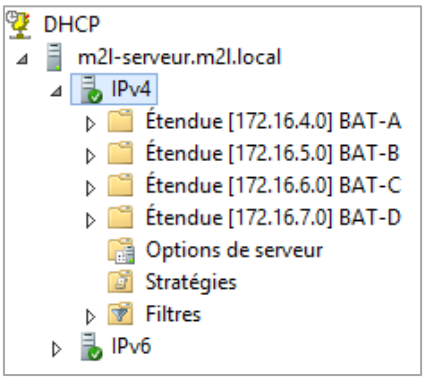

Figure 16 : Vérification de la création des étendues

5. Configuration du serveur Active Directory

Pour configurer le serveur Active Directory comme il se doit, nous devons commencer par ouvrir « **Sites et services Active Directory** » via « **Outils d'administration** » ; pour enfin renommer le site « Default-First-Site-Name » en « **M2L** ».

Puis, après avoir ouvert le « **Centre d'administration Active Directory** » toujours via « **Outils d'administration** » ; nous allons créer une nouvelle unité d'organisation nommée **M2L**. Pour ce faire, nous allons cliquer droit sur **M2L (local) → Nouveau → Unité d'organisation**

.

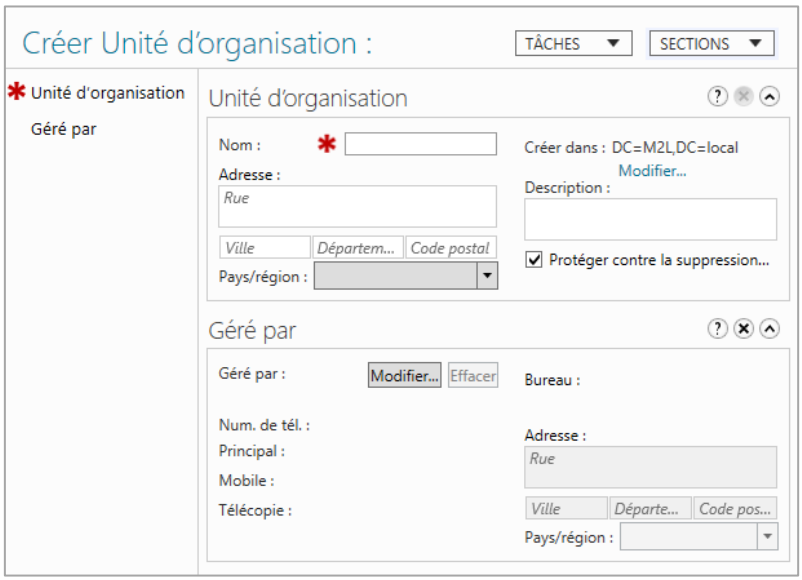

Figure 17 : Utilitaire de création d'une unité d'organisation

Nous pouvons de ce fait **créer les quatre unités d'organisation correspondantes aux quatre bâtiments** de la Maison des Ligues. Leur création se fera donc de la même manière que l'unité précédente à l'exception qu'il faudra les créer à l'intérieur de celle-ci.

Cliquons droit sur M2L → Nouveau → Unité d'organisation. C'est ainsi que nous allons créer nos unités (bâtiments) respectivement nommées :

- **Bat_A**
- **Bat_B**
- **Bat_C**
- **Bat_D**

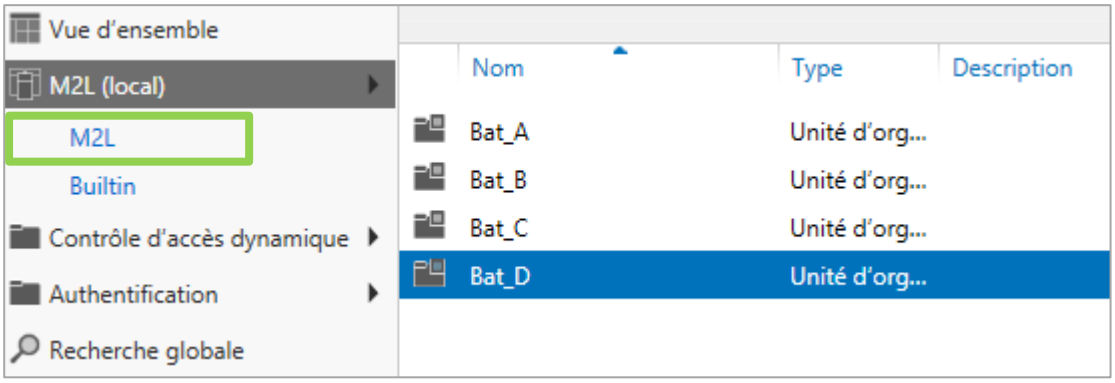

Figure 18 : Résultat de la création des quatre unités d'organisation

Nous devons par la suite pouvoir affecter des utilisateurs aux bâtiments à l'aide de groupes. Dans l'idéal, il serait plus judicieux de créer, pour chaque bâtiment, des groupes en fonctions des ligues et des services mais cela nous prendrais beaucoup plus de temps. Nous allons donc rester simple et **créer un groupe par bâtiment (unité d'organisation)** afin de pouvoir y ajouter des futurs utilisateurs.

Pour ce faire nous allons **cliquer droit sur un bâtiment → Nouveau → Groupe** ; respectivement nommés :

- **Bat_A_utilisateur**
- **Bat_B_utilisateur**
- **Bat_C_utilisateur**
- **Bat_D_utilisateur**

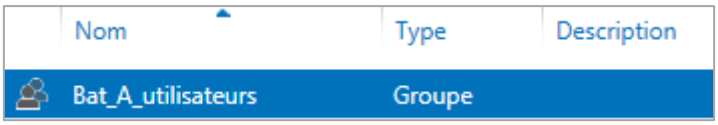

Figure 19 : Résultat d'un ajout d'un groupe au sein d'une unité d'organisation

Nous allons maintenant créer un utilisateur par bâtiment ainsi qu'un utilisateur administrateur du domaine. Afin d'effectuer la manipulation, nous devons ouvrir « **Utilisateurs et ordinateurs Active Directory** ».

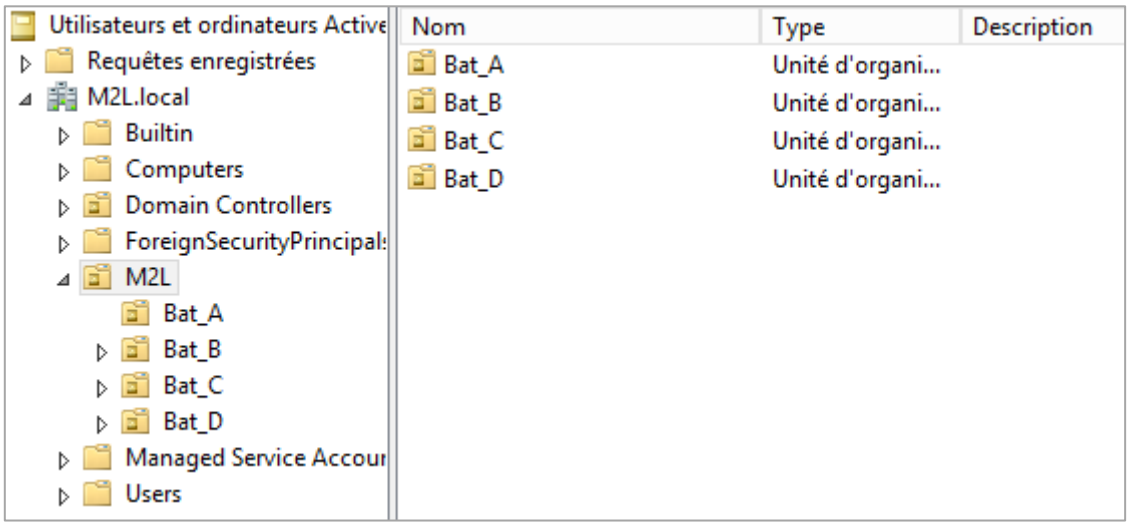

Figure 20 : Utilisateurs et ordinateurs Active Directory

Pour chaque bâtiment, nous allons **cliquer droit → Nouveau → Utilisateur** ; et saisir les informations les plus utiles à savoir :

- **Prénom**
- **Nom**
- **Nom d'ouverture de session de l'utilisateur**

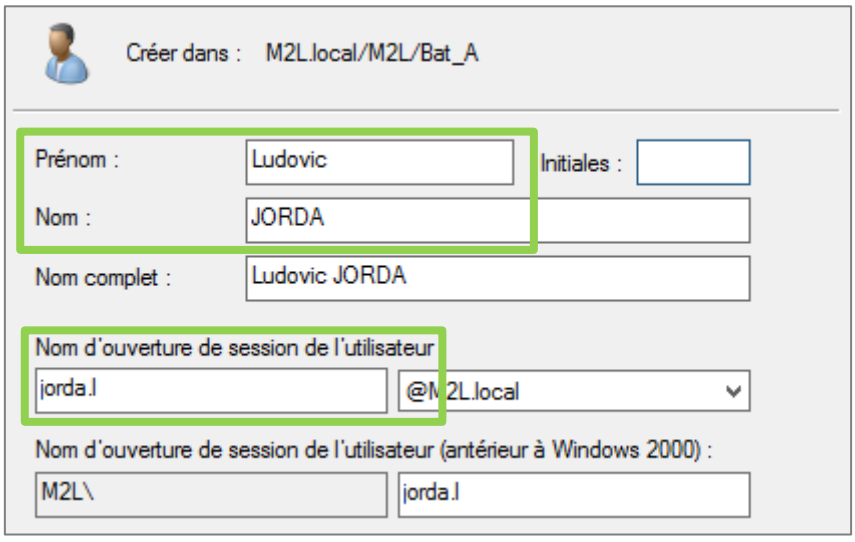

Figure 21 : Création d'un nouvel utilisateur

C’est ainsi que nous devons créer un utilisateur administrateur du domaine qui sera affecté à l’unité d’organisation du **bâtiment C** car c’est à ce bâtiment que se trouve l’administration du réseau M2L.Pour ce faire, rendons-nous dans **Users → Clic droit sur « Admins du domaine » → Propriétés → Membre → Ajouter**. De là, nous allons saisir le nom de l’administrateur puis le vérifier.

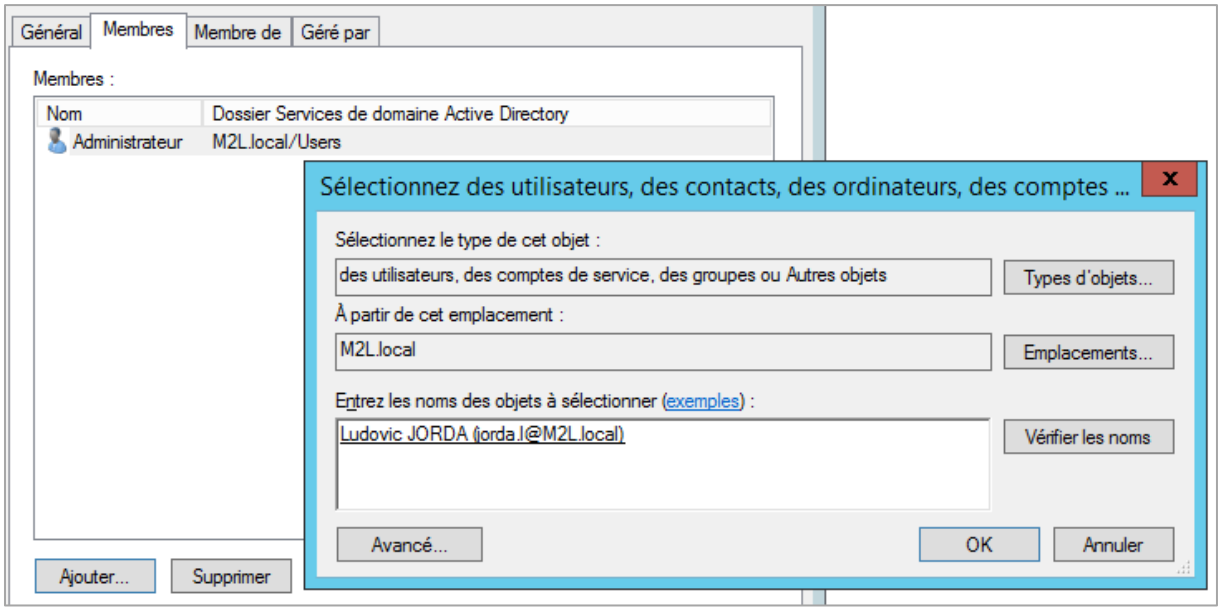

Figure 22 : Ajout d'un utilisateur administrateur du domaine

6. Jonction d'un client au domaine M2L

Pour qu'un client puisse profiter des configurations du serveur, nous devons le rattacher au domaine M2L précédemment créée. Pour ce faire, nous devons nous connecter sur la machine cliente ; ouvrir : **Ce PC → Propriétés Système → Modifier les paramètres**

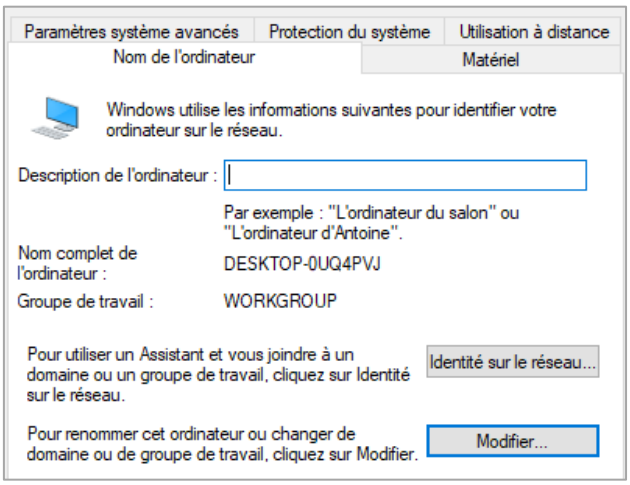

Figure 23 : Propriétés d'identification de la machine

Une fois cette fenêtre affichée nous allons cliquer sur **Modifier** puis saisir **le nom de l'ordinateur** ainsi que **le domaine** ci-dessous

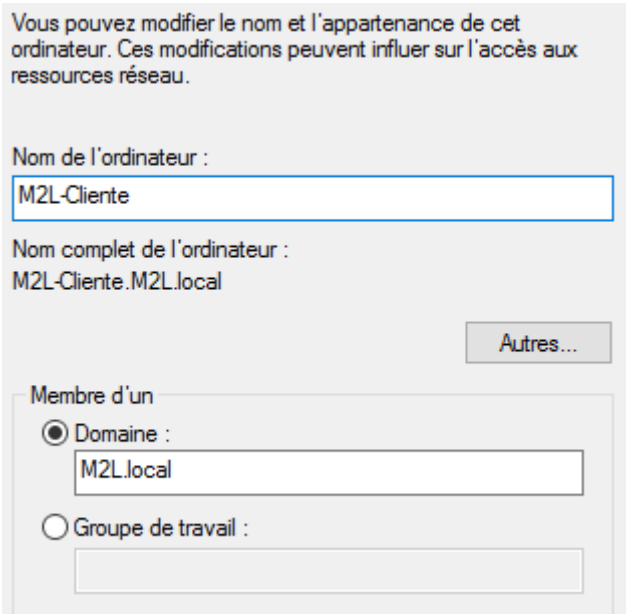

Figure 24 : Saisie des informations permettant l'accès au domaine

Le pare-feu Windows interdit par défaut les connexions entrantes ; ce qui fait que deux machines sur le même réseau ne peuvent communiquer. Pour résoudre ce problème nous allons, pour le contrôleur de domaine ainsi que pour la machine cliente, configurer le pare-feu afin d'autoriser les communications.

Pour ce faire, nous devons nous rendre au: **Panneau de configuration → Système et sécurité → Pare-feu Windows → Paramètres avancés**. De là, nous pouvons faire un **clic droit sur « Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local → Propriétés**

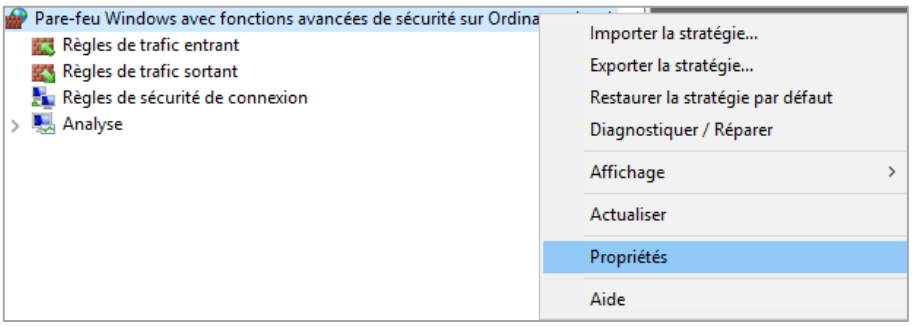

Figure 25 : Accès aux propriétés du pare-feu Windows

C'est ainsi que nous pouvons **autoriser les connexions entrantes**.

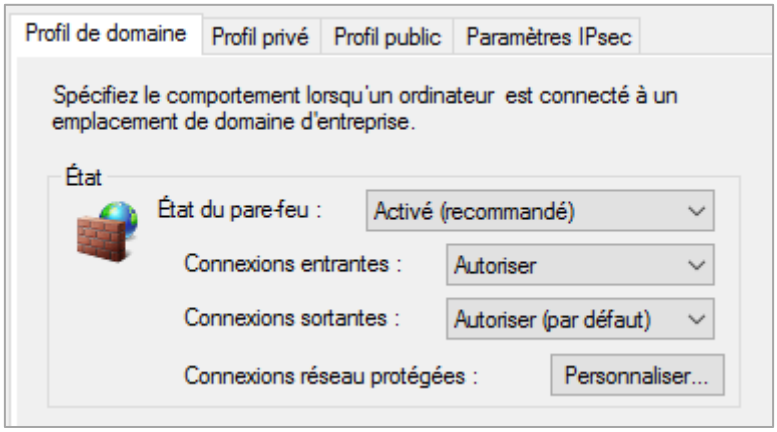

Figure 26 : Autorisation des connexions entrantes via le Pare-feu Windows

Dans la mesure où nous devons effectuer le paramétrage des connexions de façon manuelle, il serait judicieux de créer une GPO nous permettant d'automatiser cette tâche. Pour ce faire, nous allons ouvrir : **Outils d'administration → Gestion de stratégies de groupe**. De là, on déroule jusqu'à retrouver les unités d'organisation M2L ; puis on **clique droit sur M2L → Créer un objet GPO dans ce domaine et le lier ici …**

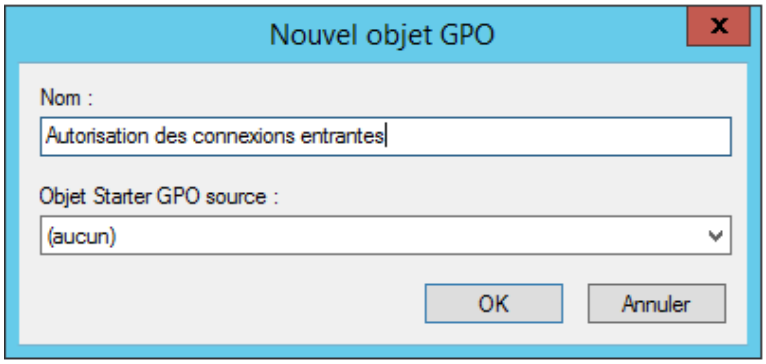

Figure 27 : Création d'un nouvel objet GPO

Une fois l'objet créé, nous pouvons faire un **clic droit sur la GPO → Modifier**. C'est ainsi que l'on va pouvoir choisir le type de GPO que l'on va créer ainsi que ceux qui vont en hériter. Nous allons donc dérouler **Configuration ordinateur→ Paramètres Windows → Paramètres de sécurité → Pare-feu Windows avec fonctions avancées de sécurité**. On constate que le pare-feu n'est pas configuré, ce qui est normal puisque l'on vient de créer une GPO « vierge ».

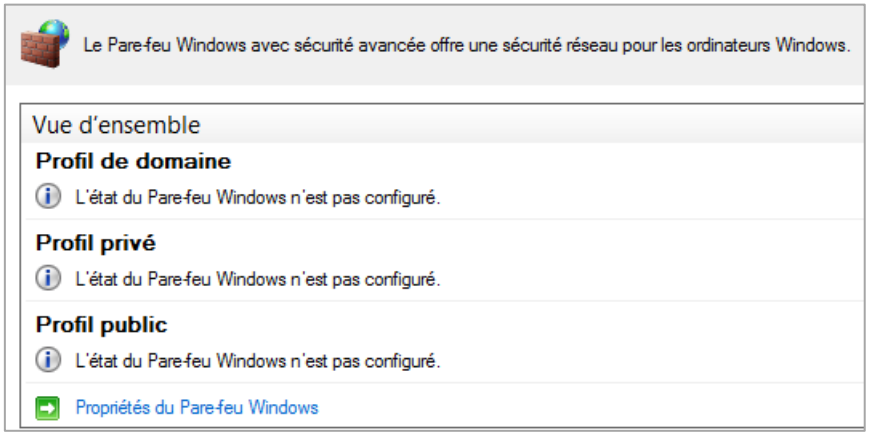

Figure 28 : Vue d'ensemble sur la configuration du pare-feu

Nous pouvons dès à présent cliquer sur « **Propriétés du Pare-feu Windows** » et **autoriser les connexions pour tous les profils**.

Nous pouvons par la suite retourner sur : **Gestion de stratégies de groupe** pour activer la GPO. Nous allons donc **cliquer droit → Appliqué.**

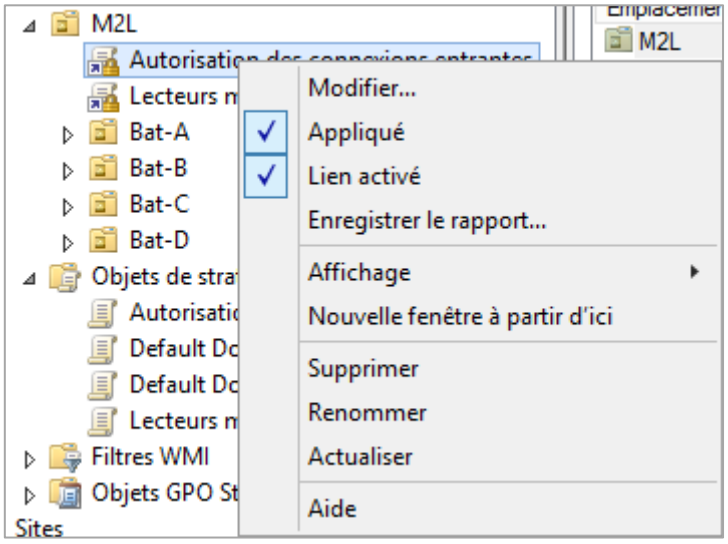

Figure 29 : Application de la GPO aux unités d'organisation

Nous terminons en ouvrant un « **invite de commande** » pour y saisir la commande « **gpupdate /force** » qui nous permettra de forcer les mises à jours des modifications effectuées par la mise en place de la GPO. Il faudra redémarrer la session de la machine cliente pour que la stratégie soit prise en compte.

```
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.


C:\Users\Administrateur>
```

Figure 30 : Forcer la mise à jour des modifications par GPO

7. Création des dossiers partagés et des lecteurs mappés (GPO)

Nous allons déployer un objet GPO sur un poste client pour ajouter des lecteurs réseau et installer des applications automatiquement à l'ouverture de la session.
Conformément au contexte M2L, nous allons donc créer **un dossier partagé par bâtiment ainsi qu'un dossier commun** (le tout dans **un dossier « Partage » que l'on crée à la racine du disque dur**).

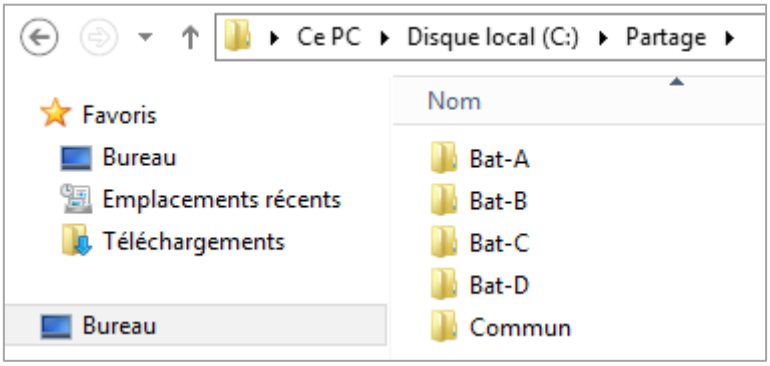

Figure 31 : Création des futurs dossiers partagés

Ensuite, pour chacun des cinq dossiers créés, il nous faut ouvrir les **Propriétés → Partage → Partager →** On choisit l'utilisateur souhaité.

Dans la mesure où le bâtiment C est l'administration du réseau M2L, chacun de ses utilisateurs doit pouvoir accéder les dossiers partagés. Par exemple, Ludovic Jorda (du bâtiment C) devra être renseigné dans chacun de ces dossiers.

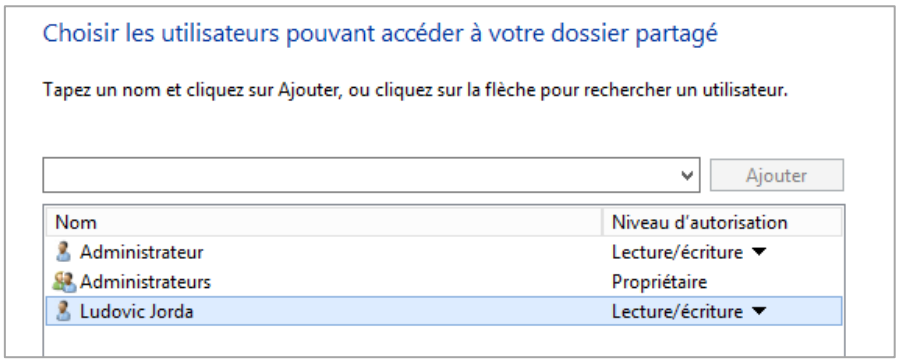

Figure 32 : Choix des utilisateurs pouvant accéder au dossier partager

Vient ensuite le moment de la création d'une GPO. Dans notre cas, nous allons mettre en place des lecteurs mappés (attribution d'une lettre à une ressource réseau pour y accéder plus rapidement) qui permettrons le stockage des logiciels à installer via le déploiement de la GPO.

Pour ce faire, rendez-vous dans **Outils d'administration → Gestion de stratégies de groupe** pour créer un nouvel objet GPO (voir page 18).

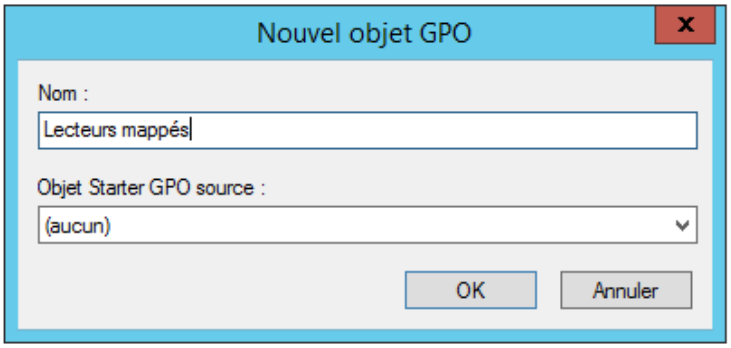

Figure 33 : Création d'un nouvel objet GPO

Une fois l'objet créé, nous pouvons faire un **clic droit sur la GPO → Modifier**. C'est ainsi que l'on va pouvoir choisir le type de GPO que l'on va créer ainsi que ceux qui vont en hériter. Nous allons donc dérouler **Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs → clic droit → Nouveau → Lecteur mappé**

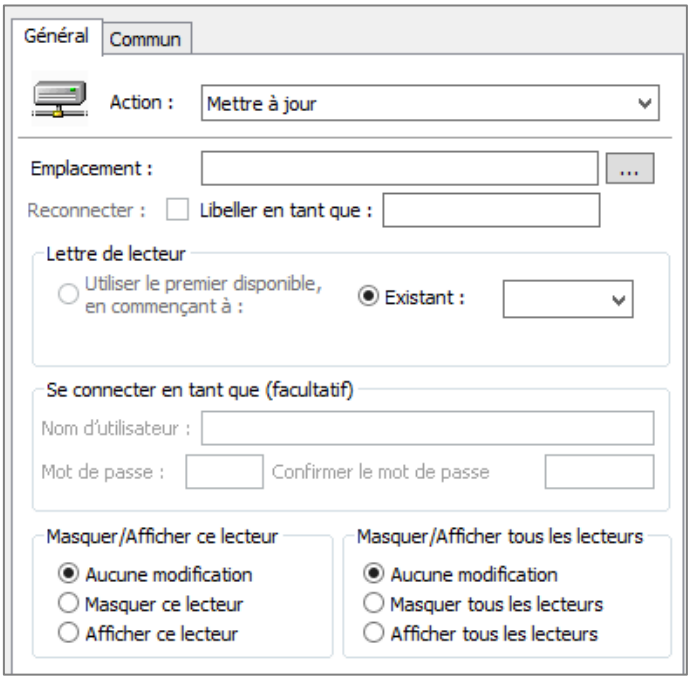

Figure 34 : Création et modifications de propriétés d'un lecteur mappé

Une fois arrivé sur l'utilitaire de création, nous allons :

- **Sélectionner l'emplacement**
- **Cocher « Reconnecter »**
- **Libeller en tant que : Bat- ?**
- **Cocher « Afficher ce lecteur »**
- **Cocher « Afficher tous les lecteurs »**

Bien entendu, il nous faudra **créer un lecteur mappé par bâtiment.**

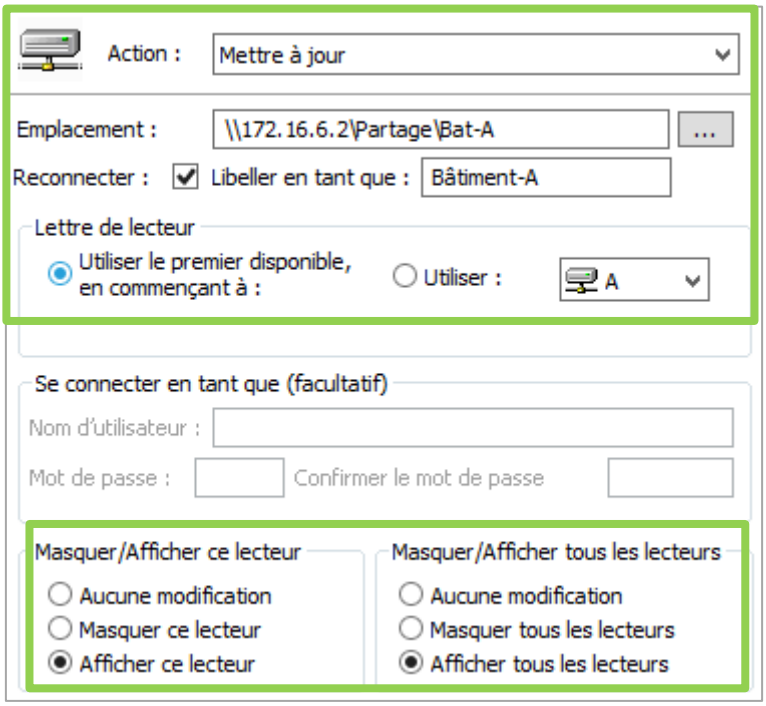

Figure 35 : Propriétés de base pour chaque lecteur mappé

Ainsi nous obtenons l'affichage suivant :

Figure 36 : Résultat de la création des lecteurs mappés

De ce fait, nous pouvons appliquer la GPO (voir page 19) ; lancer la commande **« gpupdate /force »** ; puis **redémarrer les sessions ciblées par la stratégie mise en place**.

Il ne suffit plus que d'ouvrir « Ce PC » pour constater que les emplacements réseaux ont bel et bien été créés.

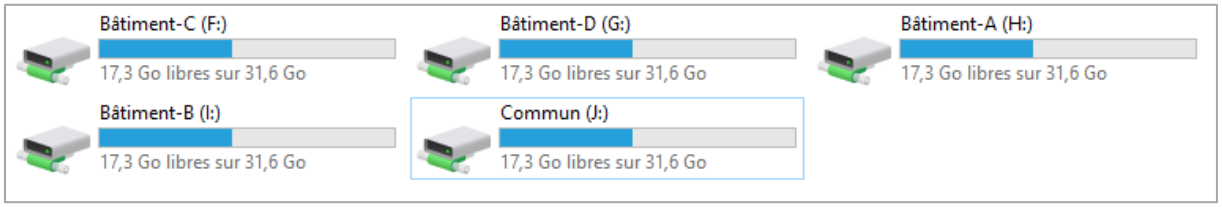

Figure 37 : Accès aux ressources partagées

8. Activation du « Bureau à distance »

Nous allons activer le service « Bureau à distance » qui permettra aux utilisateurs autorisés de prendre le contrôle du serveur depuis un autre poste à distance. Depuis le **Gestionnaire de serveur**, on **clique sur l'onglet Serveur Local et on active le service Bureau à distance** :

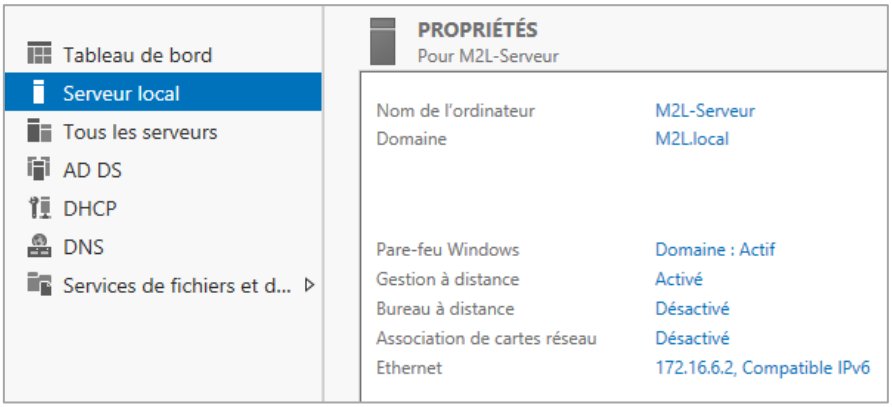

Figure 38 : Activation du service "Bureau à distance"

C'est ainsi que l'on peut lancer depuis une machine cliente, l'utilitaire « **Connexion bureau à distance** » via « **Accessoires Windows** » pour y saisir le nom du serveur que l'on veut contrôler. Par exemple, notre contrôleur de domaine :

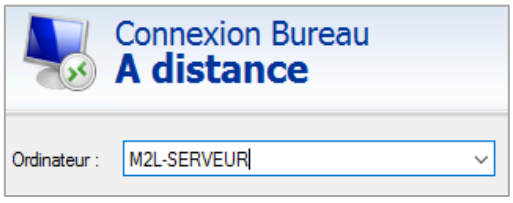

Figure 39 : Champ de saisir du nom de la machine à prendre en main

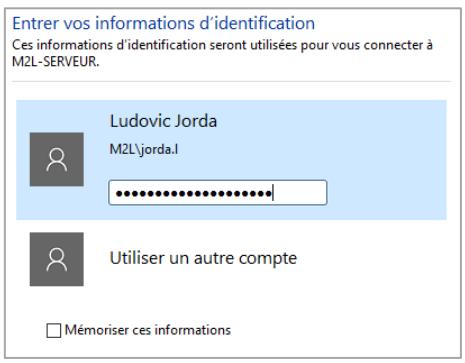

Figure 40 : Saisie des informations d'identification

9. Mise en place d'un pare-feu IPCop

IPCop est une distribution Linux open source distribuée sous les termes de Public licence, permettant la mise en place simplifiée d'un pare-feu. Travaillant sur des machines virtuelles, notre serveur ainsi que les machines clientes sont isolées du réseau local et ne disposent pas de connexion internet. Nous allons donc mettre en place un pare-feu (IPCop) afin de fournir une connexion internet sécurisée à notre serveur. De plus, mettre en place cette solution nous permettra de déplacer le réseau sans pour autant modifier l'adressage IP (pour examen BTS SIO).

Dans IPCop, on peut définir jusqu'à quatre interfaces réseau définies par les couleurs selon les besoins :

- Interface **Rouge**: Ce réseau correspond au réseau Internet.
- Interface **Verte**: Correspond au réseau local (LAN) protégé par IPCOP.
- Interface **Orange**: Ce réseau est une DMZ (Zone Démilitarisée).
- Interface **Bleu**: C'est une interface spécifique aux réseaux sans fil.

Dans notre cas, il convient de lui attribuer deux interfaces : **Rouge** et **Verte**. Après avoir saisi le nom d'hôte ainsi que le nom du domaine, nous devons à présent sélectionner me type de configuration pour l'interface **rouge**. Nous allons donc choisir une configuration **statique**, ce qui nous permet de la modifier à tout moment.

Figure 41 : Choix du type de configuration pour l'interface rouge

Nous allons maintenant passer à l'affectation des cartes. Pour ce faire, nous devons assigner « Green » à une carte et « Red » à l'autre afin d'avoir un côté LAN et un autre « Internet ».

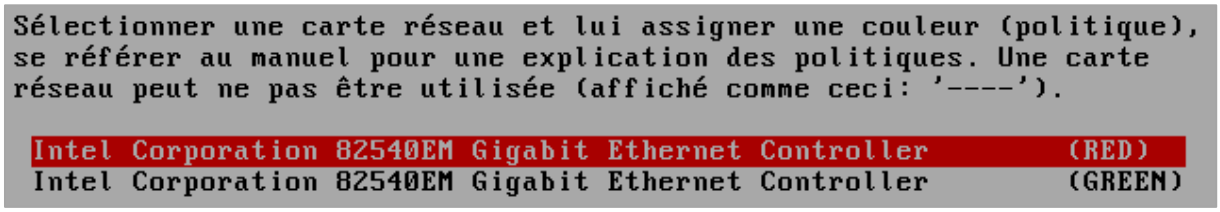

Figure 42 : Affectation des politiques aux cartes

C'est ainsi qu'il nous faut indiquer les paramètres IP pour chacune des interfaces auxquelles nous avons attribué une politique. Pour l'interface Green : Les paramètres IP seront quasi-identiques à ceux du serveur AD (172.16.12.2). Ici l'adresse IP sera 172.16.12.1

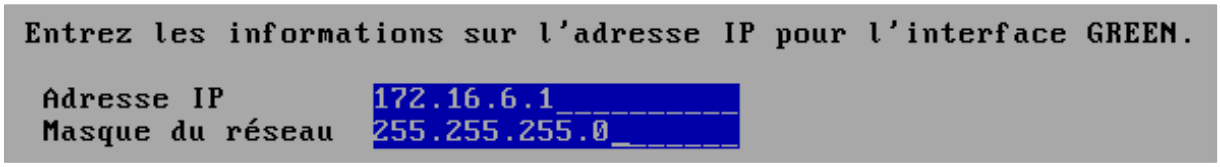

Figure 43 : Paramètres IP pour la politique Green

Pour l'interface Red : Nous devons d'abord déterminer les paramètres IP permettant au Windows hôte de se connecter à Internet. Pour ce faire, nous allons ouvrir un Invite de commande puis saisir ipconfig /all. Puis, il nous faut relever les paramètres IP de la carte Wifi car c'est cette carte là que l'on a affecté à VirtualBox. Une fois l'adresse trouvée, il nous faut ajouter +1 à son dernier octet.

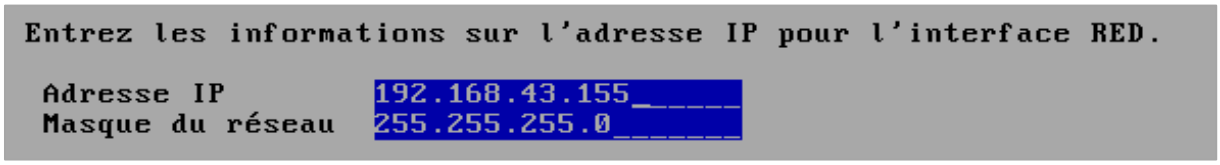

Figure 44 : Paramètres IP pour la politique Red

Pour ce qui est de la configuration DNS, nous pouvons également retrouver les informations grâce à la commande cmd :

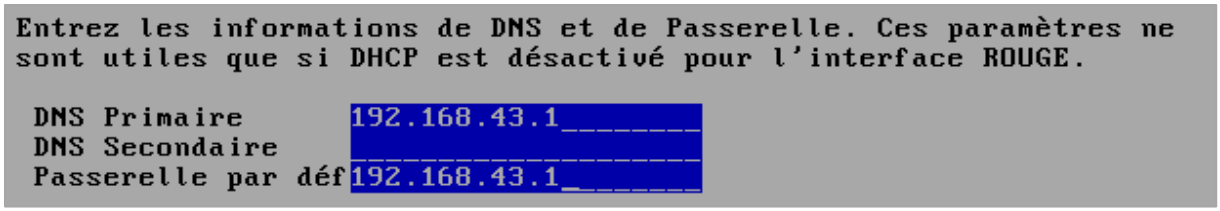

Figure 45 : Saisie des paramètres DNS

Nous pouvons ainsi tester la connexion Internet du pare-feu grâce à un ping …

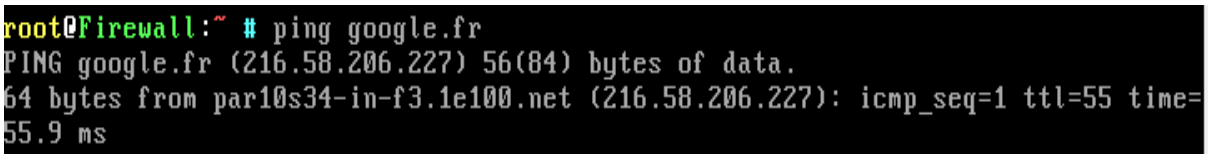

Figure 46 : Test de la connectivité Internet du pare-feu

… ainsi que la connexion avec le contrôleur de domaine :

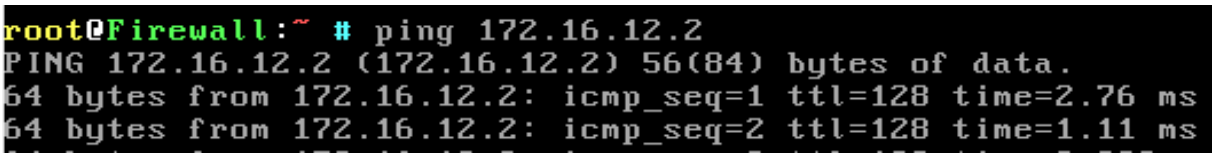

Figure 47 : Test de la connectivité du pare-feu au contrôleur de domaine

Une fois la configuration terminée, nous allons pouvoir nous connecter à l'interface web d'IPCop, qui nous permettra de le configurer comme bon nous semble, tout dépend des besoins de l'administrateur. Dans notre cas, conformément au contexte M2L, nous n'allons toucher à aucun paramètre dans la mesure où le pare-feu Windows est laissé actif. Ce qui veut dire que notre IPCop nous sert de routeur tant que nous ne touchons pas à son pare-feu. En effet, configuré comme précédemment, IPCop assure bel et bien le routage des paquets ; et pour cause, si IPCop n'est pas démarré, ni nos serveurs, ni nos machines ne bénéficieront de connexion Internet :

Figure 48 : Test de ping du contrôleur de domaine avec IPCop inactif

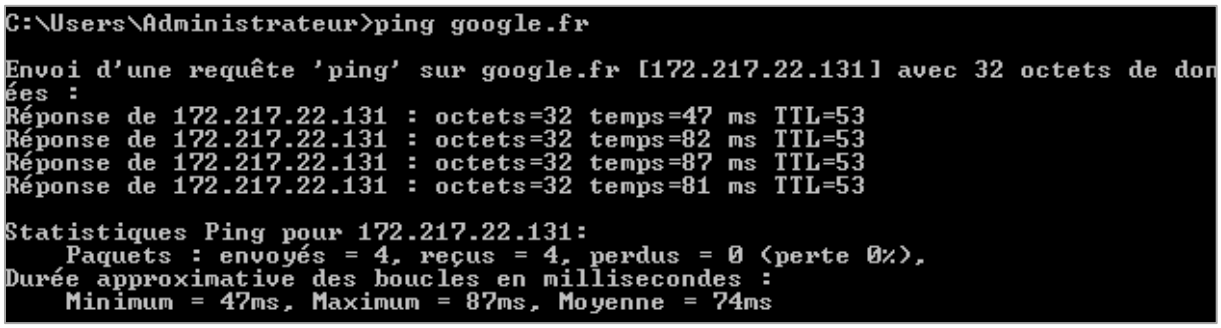

Figure 49 : Test de ping du contrôleur de domaine avec IPCop actif

Pour pouvoir accéder à l'interface web d'IPCop, nous allons nous connecter au contrôleur de domaine (avec IPCOP actif), **ouvrir un navigateur Internet** pour y saisir l'adresse IP « **Green** » d'IPCop à savoir **: https://172.16.6.1:8443/** (voir page 26).

C'est ainsi que des identifiants de connexion nous sont demandés. Il est important de savoir que **l'identifiant utilisateur « admin » ci-dessous est obligatoirement celui à utiliser !** En revanche, le mot de passe est celui saisi lors de l'installation d'IPCop.

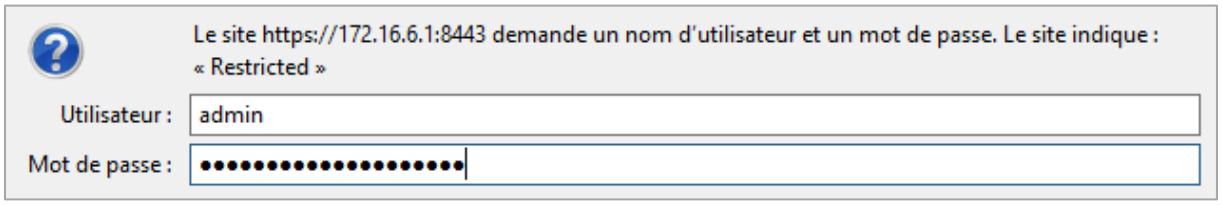

Figure 50 : Connexion à l'interface web d'IPCop

Figure 51 : Interface web d'IPCop

11. Conclusion

Nous avons maintenant un contrôleur de domaine sous Windows Server 2012 prêt à être utilisé. Les postes clients peuvent être ajoutés au domaine M2L.local et les utilisateurs vont pouvoir profiter des dossiers partagés sur celui-ci. Le pare-feu IPCop est parfaitement configuré pour fournir une connexion internet sécurisé à notre serveur. Ainsi, le serveur DHCP attribuera des adresses IP automatiquement aux postes clients et ils pourront se connecter au réseau sur la plage d'adresse qu'on a défini sur le DHCP. Les groupes d'accès ont été créé selon les bâtiments de la Maison des Ligues de Lorraine. Chaque utilisateur aura les droits d'accès sur les dossiers partagés spécifiquement créés pour leur bâtiment respectif. A l'ouverture de la session de l'utilisateur, les logiciels seront installés automatiquement grâce à des objets GPO ainsi que les lecteurs réseau.