Mise en place de PKI

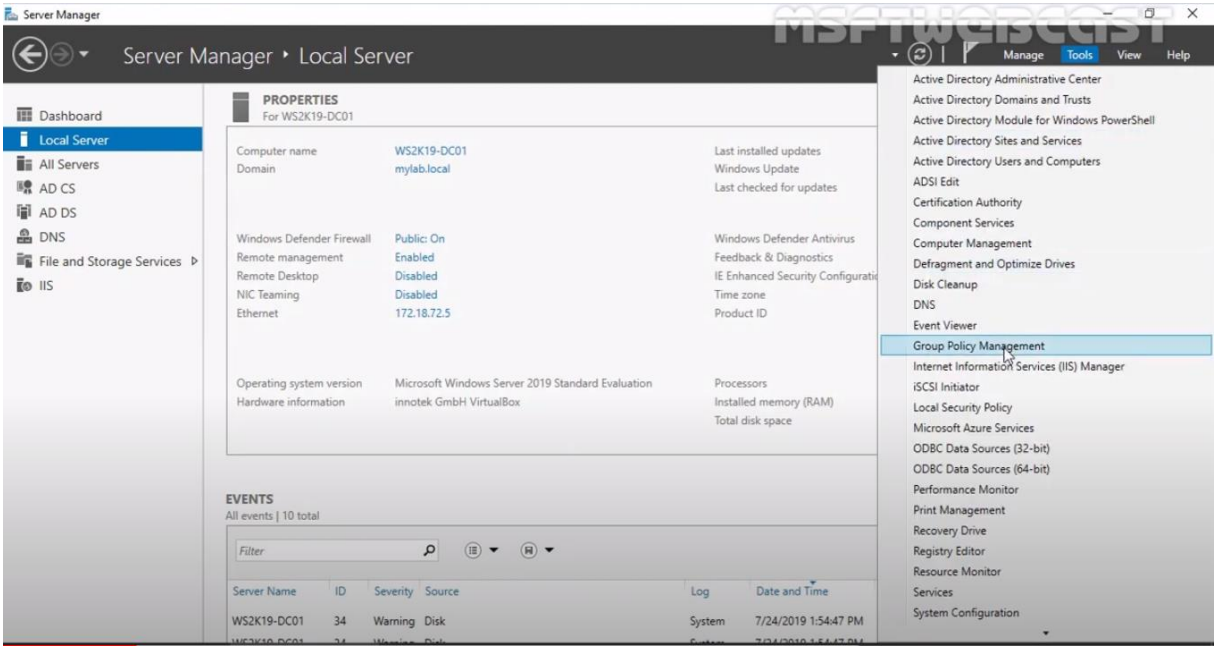
Prérequis

Pour l'installation et la configuration de PKI il y a quelques prérequis qui sont les suivants :

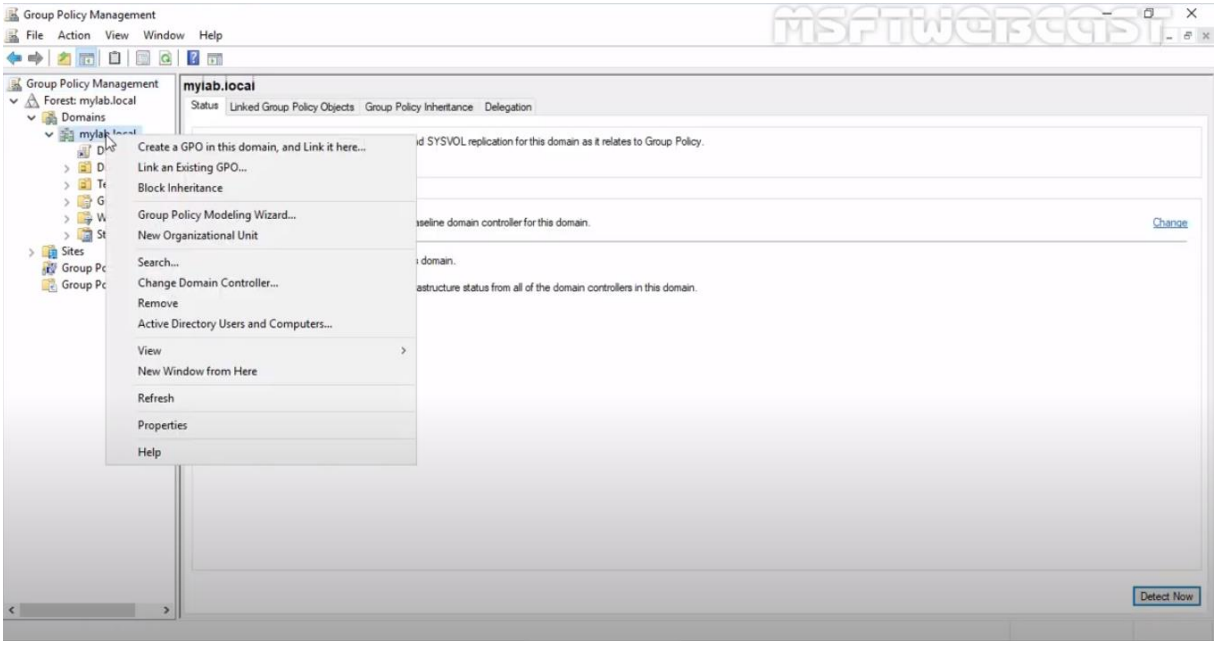
- Un poste Windows server qui est contrôleur de domaine d'un active directory
- Un poste Windows client qui est dans l'active directory du serveur

Configuration PKI

On va commencer par lancer le logiciel Group Policy Management depuis le Server Manager en cliquant sur Tools et sur Group Policy Management comme sur l'image ci-dessous :

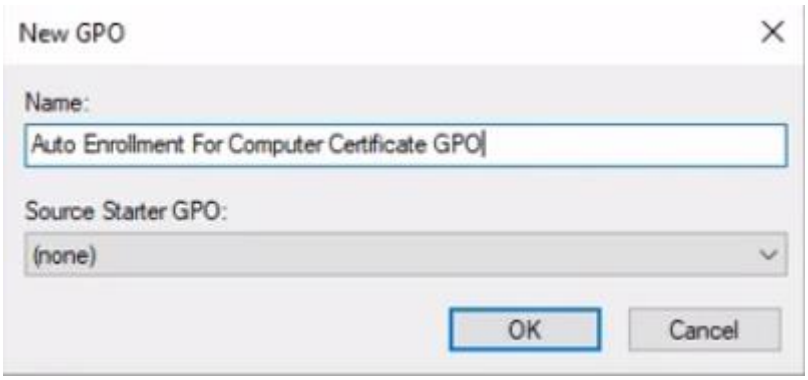


Une fois dans le logiciel il faudra dérouler la forêt, puis les domaines et de faire clic droit sur notre domaine comme sur l'image ci-dessous :



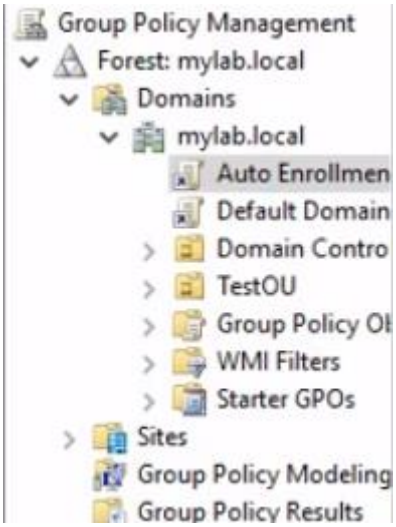
Il faudra alors ensuite cliquer sur « Create a GPO in this domain, and lin kit here… ».

La fenêtre suivante va s'ouvrir :

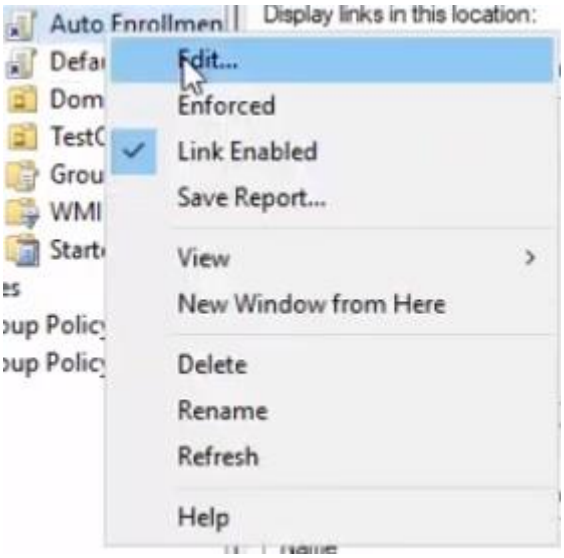


Ici il faudra mettre un nom clair pour la GPO, afin d'éviter les confusions, puis cliquer sur OK.

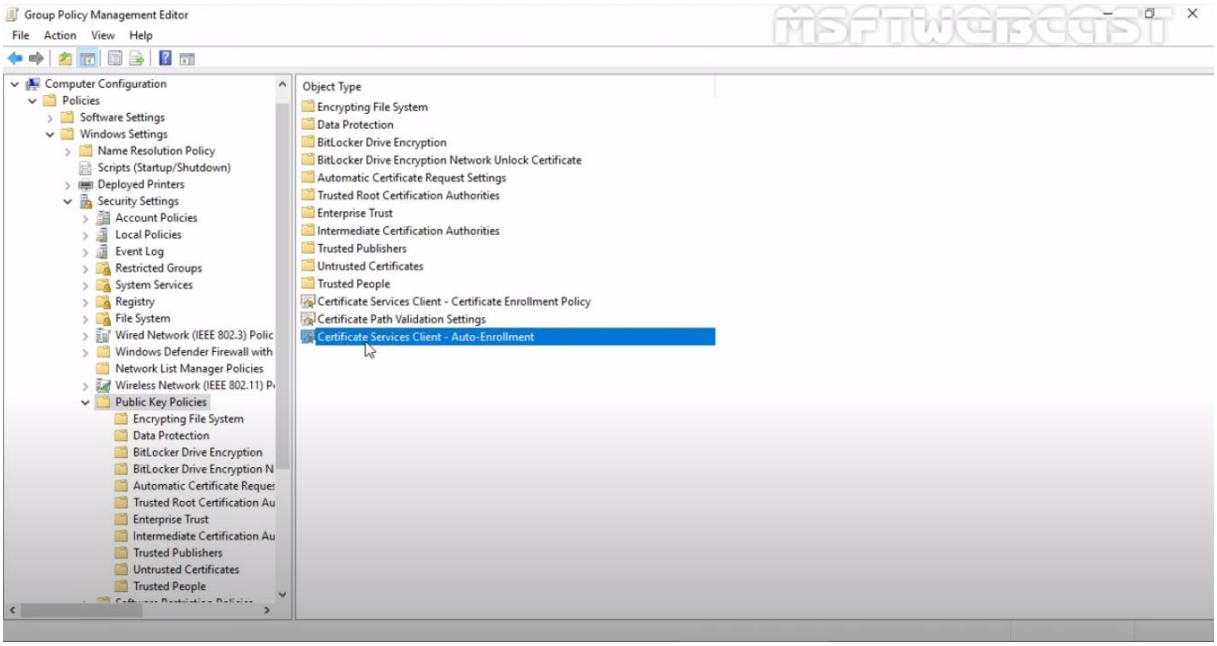
Vous aurez donc votre GPO qui va apparaitre comme ci-dessous :



Il faudra cliquer dessus une fois pour le sélectionner, puis faire clic droit sur ce dernier et cliquer sur edit comme sur le screen si dessous :



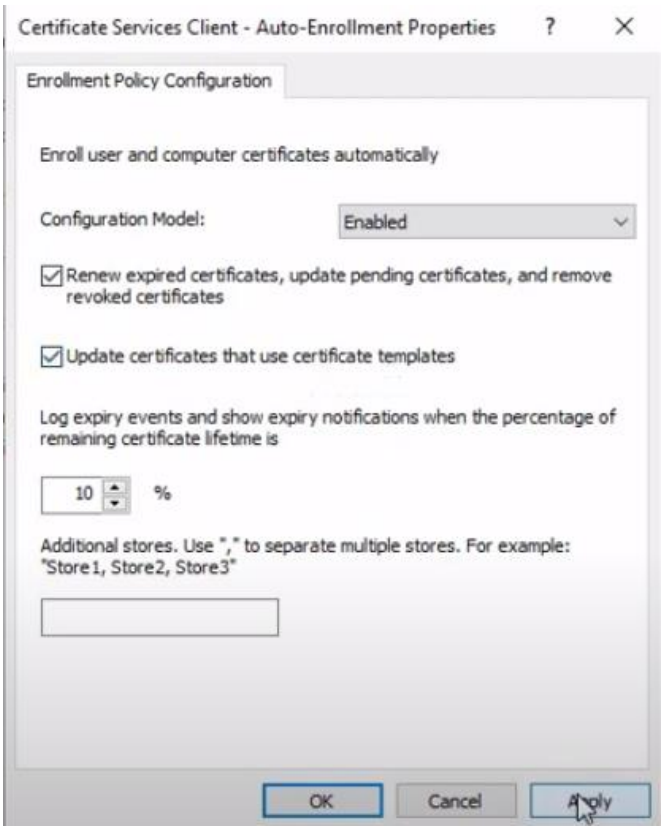
Vous aurez donc le group policy management editor qui va s'ouvrir comme ci-dessous :



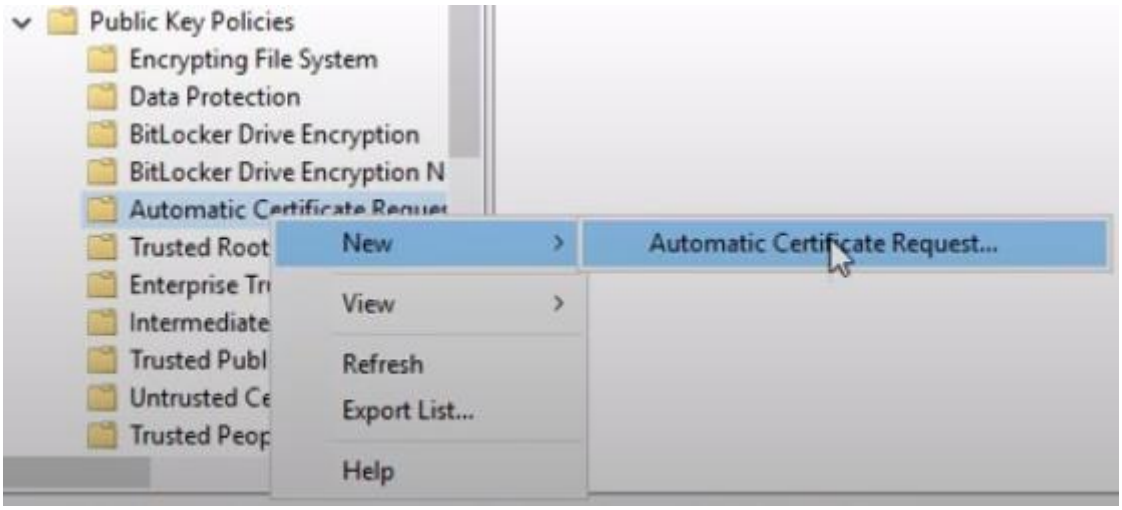
Comme sur le screen ci-dessus vous devrez rester dans « computer configuration », dérouler « Policies », dérouler » Windows Settings », dérouler « Public Key Policies » et vous aurez des objets qui vont s'afficher comme sur le screen. Vous devrez donc trouver « Certicate Service Client – Auto Enrollment » et double cliquer dessus.

Vous aurez la fenêtre suivante qui va s'ouvrir :

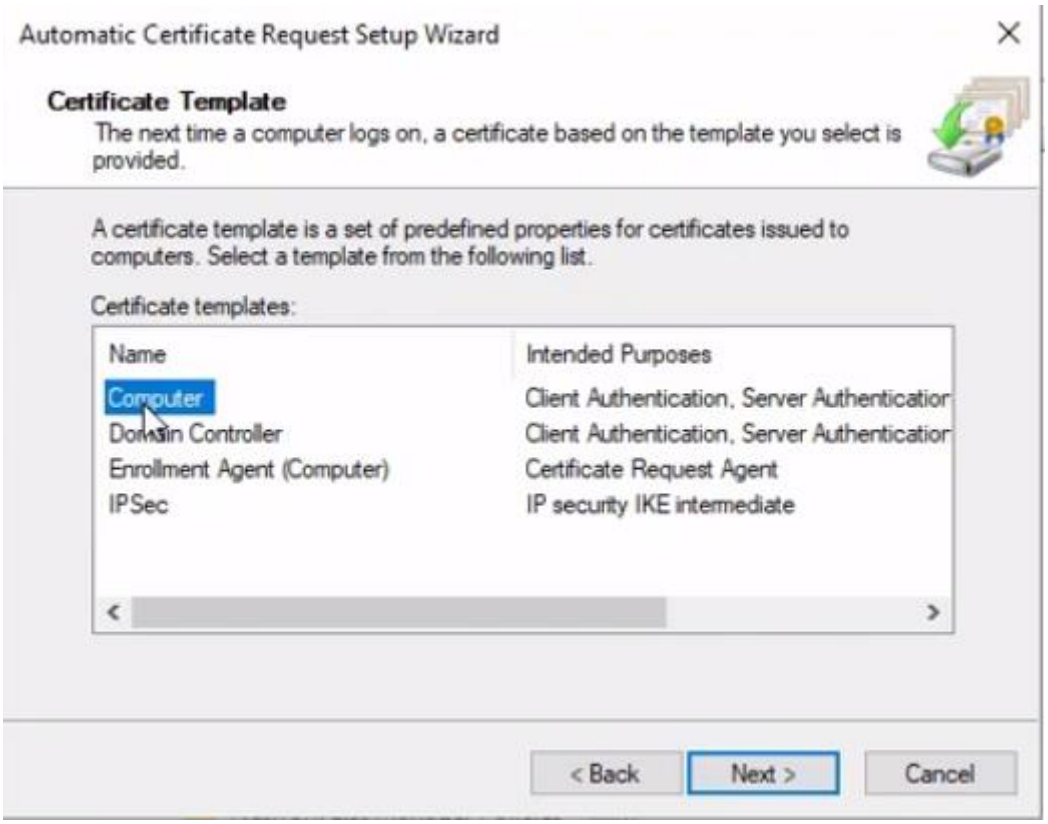
Vous devrez ici mettre « Enabled » pour configuration model qui va afficher de nouvelles options. Vous devrez cocher les deux cases et cliquer sur appliquer et sur ok comme sur l'image ci-dessous :



Ensuite il faudra trouver le dossier « Automatic Certificate Request Settings » toujours dans « Security Settings », clic droit dessus, faire nouveau et « Automatic Certificate Request… » comme le montre l'image ci-dessous :



Une fenêtre va s'ouvrir et vous devrez cliquer sur suivant et vous arriverez sur cette fenêtre :



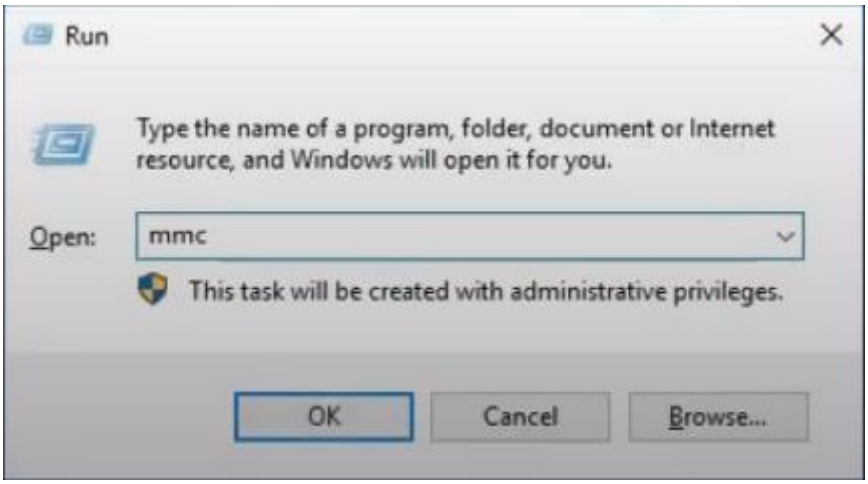
Ici il faudra sélectionner « Computer » qui est pour la connexion client-serveur donc exactement ce qu'il nous faut. Ensuite il faudra cliquer sur suivant et sur finish.

Vous pourrez voir le template de certificat que vous avez choisi pour être celui de base comme ci-dessous :

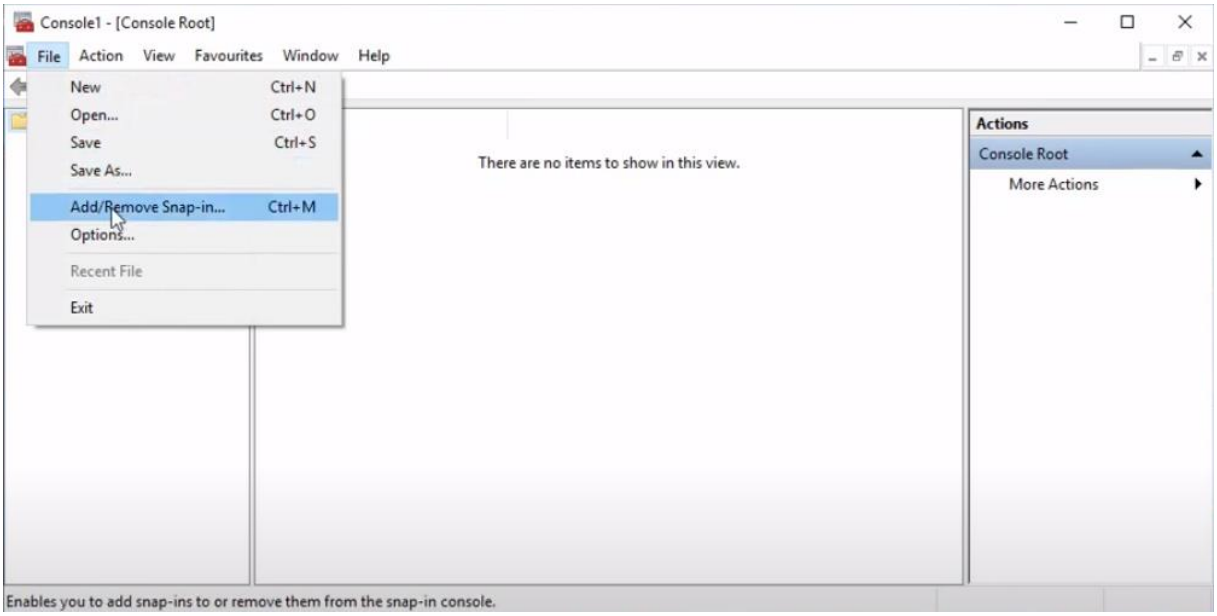
Ensuite on va devoir forcer la mise à jour des user policy sur notre contrôleur de domaine avec la commande ci-dessous :

```
C:\Users\Administrator>gpupdate /force
```

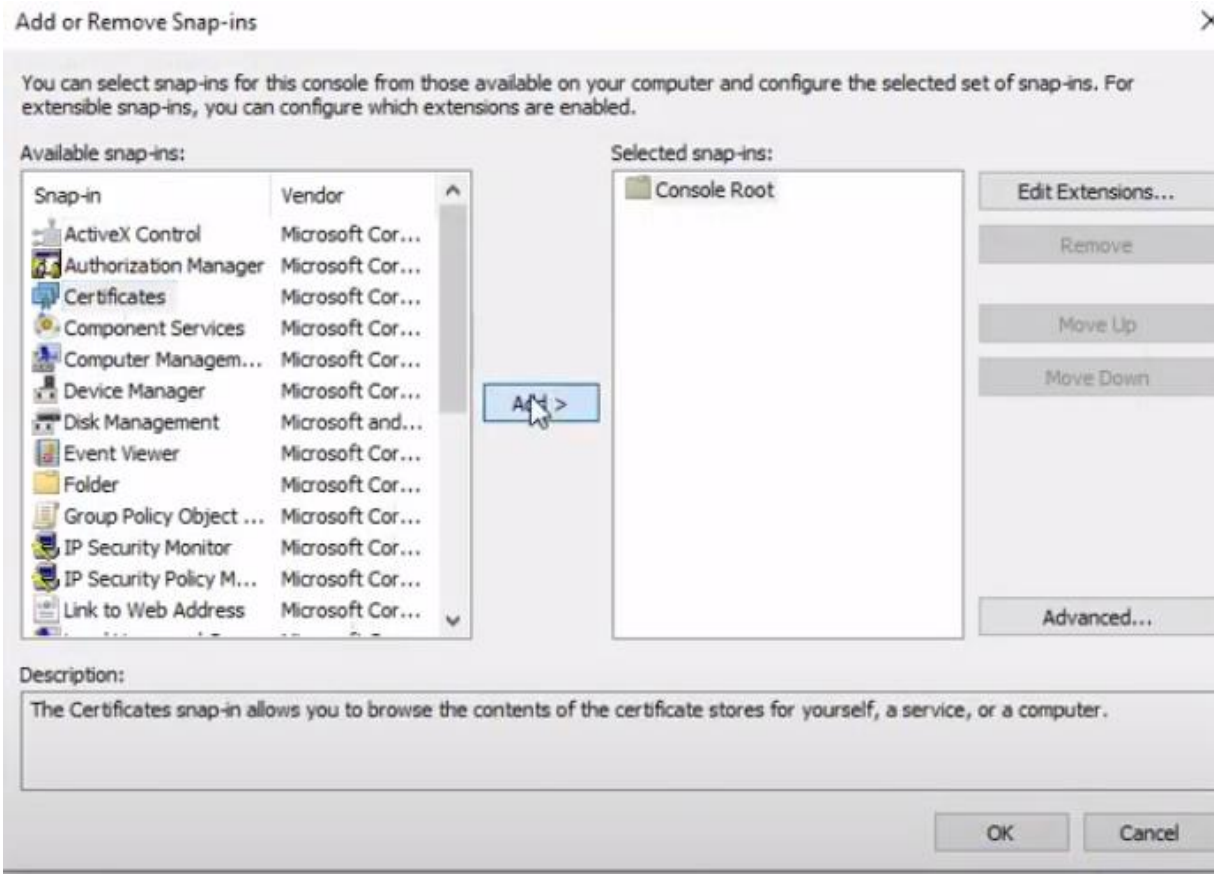
Ensuite il va falloir tester sur un client. Dans le meilleur des cas un Windows 10 et il faut qu'il soit connecté en tant qu'administrateur du poste. Vous aurez alors à aller dans exécuter en faisant Windows + r et taper mmc puis cliquer sur ok comme sur l'image ci-dessous :



Vous arriverez alors sur le logiciel mmc et devrez cliquer sur file, puis sur « Add/Remove Snap-in… » comme sur l'image ci-dessous :

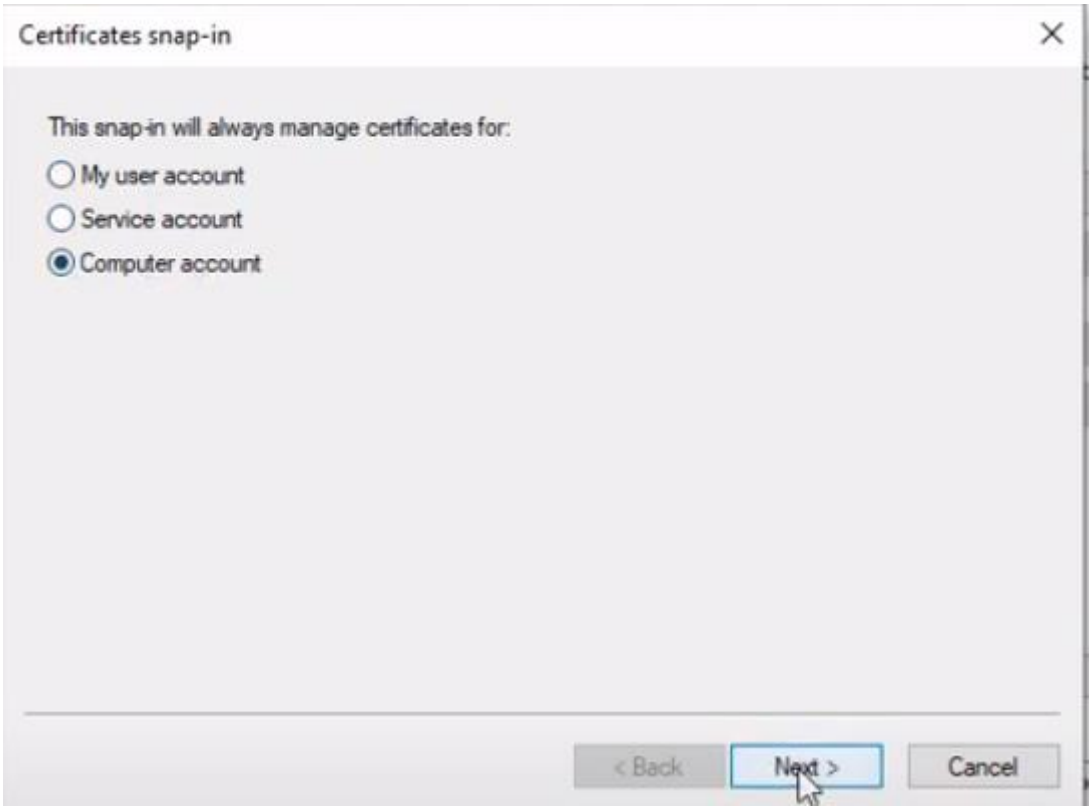


Vous aurez alors la fenêtre suivante qui va s'afficher :



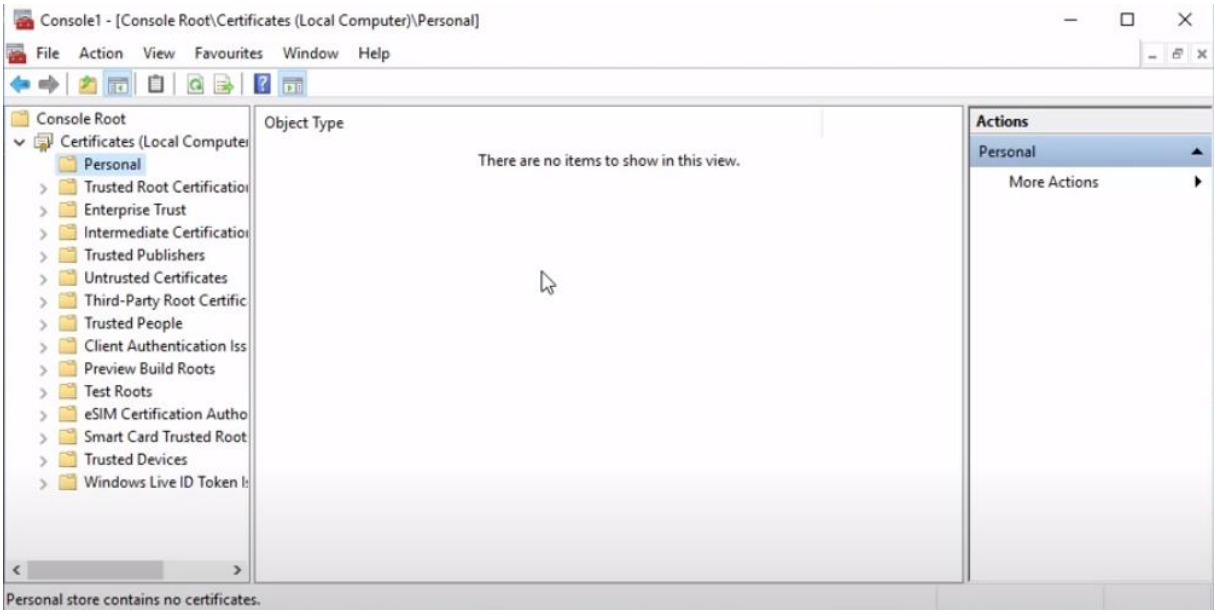
Vous aurez ici à cliquer sur Certificates et cliquer sur Add.

Une nouvelle fenêtre va s'afficher et vous devrez cocher « Computer account » et cliquer sur suivant.



Ensuite cliquer sur finish sans rien changer sur la dernière fenêtre.

Revenu sur la fenêtre principale du logiciel, déroulez « Certificates » et cliquer sur « Personal » comme sur le screen ci-dessous.

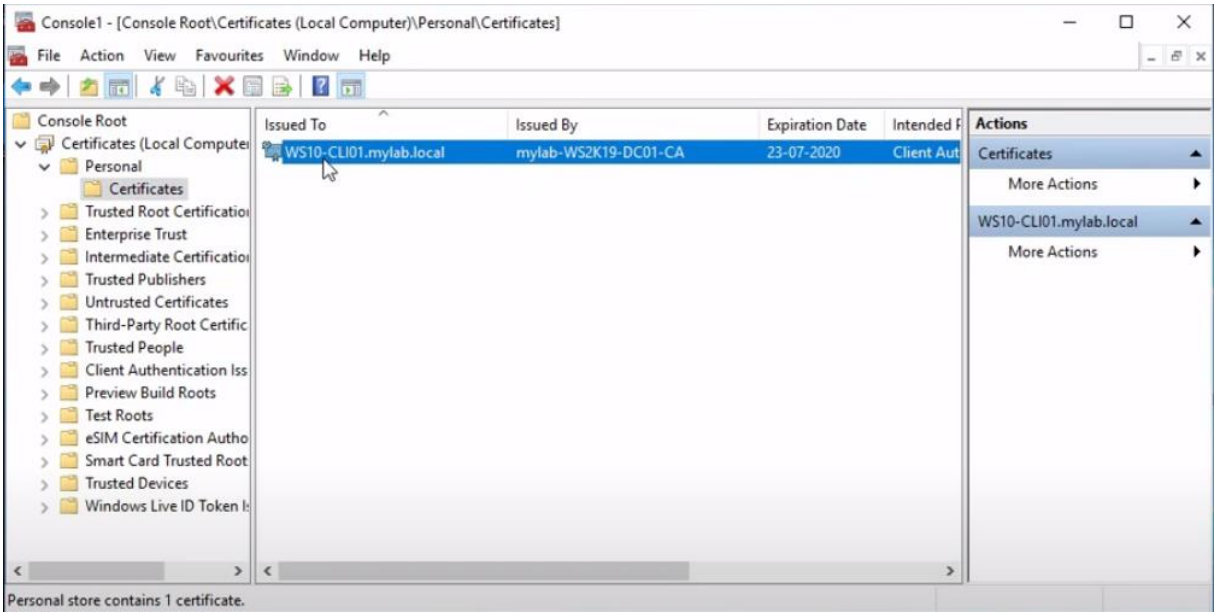


Vous verrez alors qu'il n'y a rien parce que la mise à jour ne s'est pas encore faite du côté du client.

Il faudra donc, pour remédier à cela, forcer la mise à jour comme sur le contrôleur avec la commande suivante :

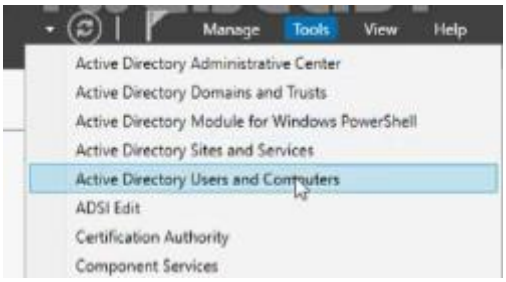
```
C:\Users\Administrator>gpupdate /force
```

Maintenant revenez sur le logiciel et rafraichissez et vous verrez qu'il y a un dossier « Certificates » qui s'est créé dans « Personal » et qui aura un certificat à l'intérieur comme sur le screen ci-dessous :

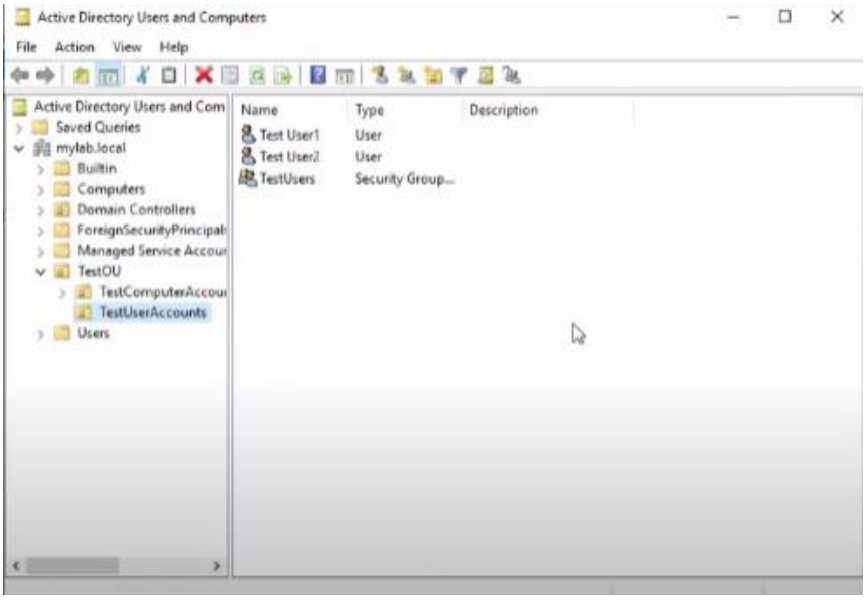


Vous pourrez ensuite si vous le souhaiter aller vérifier sur le serveur contrôleur de domaine dans « Issued ceritifactes » que le certificat de type « Computer » a bien été créé et délivré. Maintenant il faut créer et paramétrer des utilisateurs.

Pour créer et paramétrer notre premier utilisateur. Pour faire cela, nous devons tout d'abord ouvrir l'onglet *Tools* et ensuite ouvrir la partie du menu déroulant *Active Directory Users and Computers*.



Cet onglet s'affichera :



Nous pouvons alors remarquer que les utilisateurs sont créés, nous pouvons alors minimiser la fenêtre est ouvrir une autre fenêtre en suivant le chemin suivant : *Tools/Certification Authority.*

Une fois cette page ouverte nous pouvons cliquer sur la partie en dessous de :

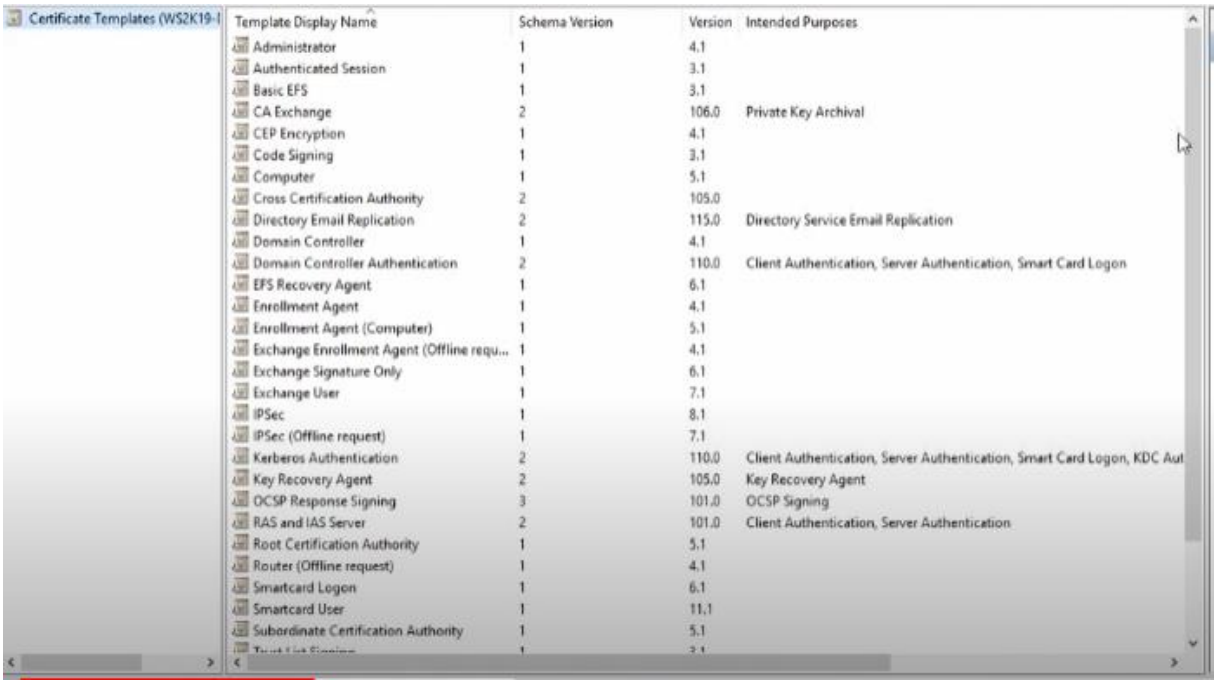
Certification Authority (local).

Un menu déroulant apparaîtra comme ceci :

Nous pouvons alors cliquer sur *Certificate Template.*

Nous voulons créer un Certificat modifier mais c'est pour cette raison que nous devons d'abord prendre un template. Pour faire cela nous allons faire clic droit sur *Certificate template* et cliquer sur *manage*.

La console de management de certificat va alors s'ouvrir.



Pour notre cas nous allons séléctionner *User* et en cliquant droit sur celui nous pouvons dupliquer le certificat.

En dupliquant le template une page s'ouvrira nous permettant de paramétrer notre nouveau template sur la base du template user déjà existant ce qui nous laisser un plus large éventail de paramètres possibles.

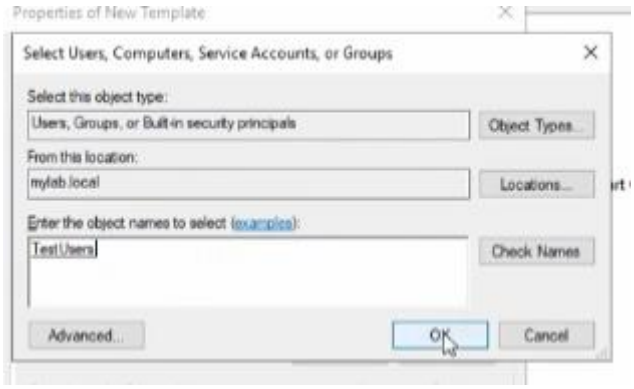
La première chose à faire et d'aller dans les paramètres généraux et de modifier le nom du template ce qui permettra une meilleure différenciation avec les autres templates.

Nous pouvons de plus remarquer que la période de validité est modifiable ce qui n'était pas le cas auparavant.

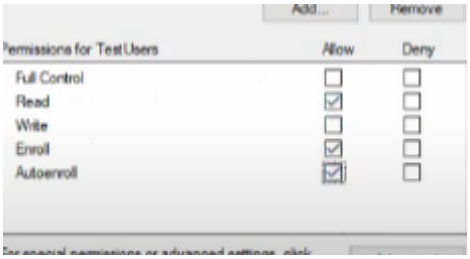
Nous pouvons ainsi remarquer que notre encryption de fichier, notre sécurisation de mail et notre authentification de client est alors disponible.

Nous pouvons une fois toutes ses étapes faites, regarder dans l'onglet *Security* et décocher la case *Enroll* pour notre *Domain Users.* Ensuite nous pouvons cliquer sur *Add* pour créer un nouveau groupe de sécurité.

Pour notre exemple nous allons alors appeler notre groupe TestUsers.

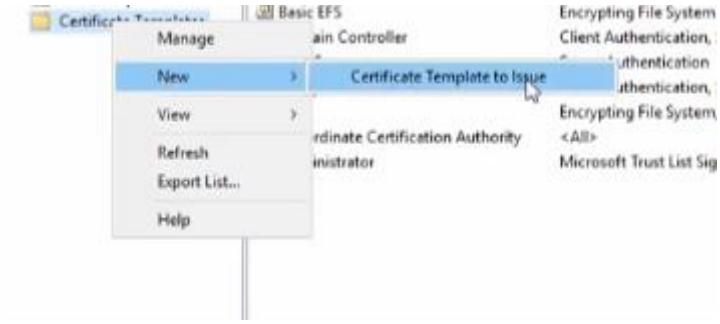


Notre groupe une fois créé, nous pouvons alors modifier ses permissions en cochant toutes les cases nécessaires comme ci-contre :



Une fois ceci fait nous pouvons alors cliquer sur *apply* puis *ok*.

Notre nouveau certificat est maintenant créé que nous pourrons modifier à tout moment.



Nous devons ensuite cliquer *Certificate Template to Issue* en cliquant droit sur *Certificate Template*.

Nous pouvons alors sélectionner notre certificat pour l'activer dans notre console.

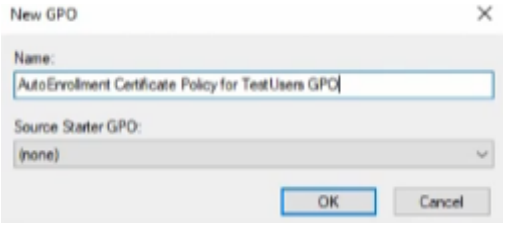
Il s'affichera ainsi dans notre console des *Certificate Template*.

Pour la prochaine étape, nous devons ouvrir dans *Tools* la partie *Group Policy Management*.

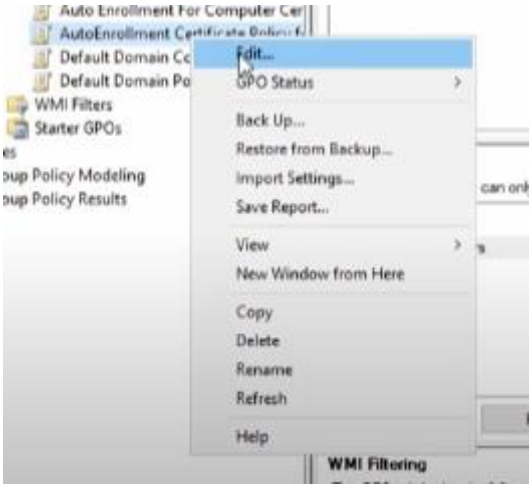
Une nouvelle console s'ouvrira donc. Dans cette nouvelle console il faut ouvrir le menu *Group Policy Object.* En cliquant dessus des sous-catégories apparaitront.

Il faudra alors cliquer droit sur *GPO* et ensuite cliquer sur *New*.

Nous pouvons ensuite donner un nom à notre GPO.

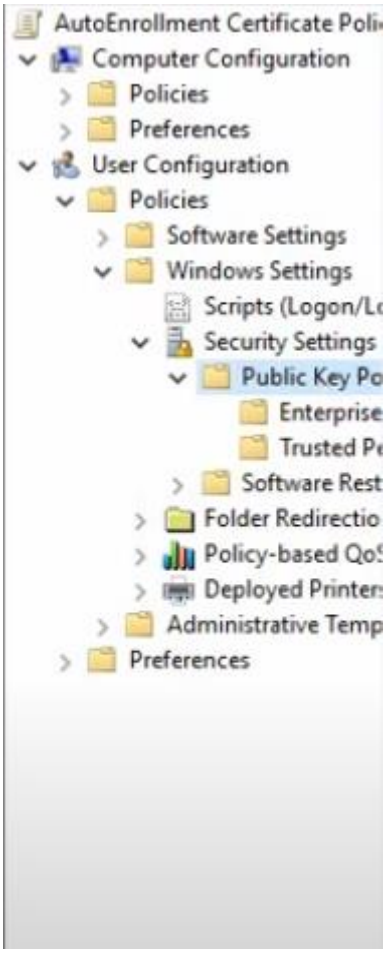


La modification de notre GPO est ainsi disponible.

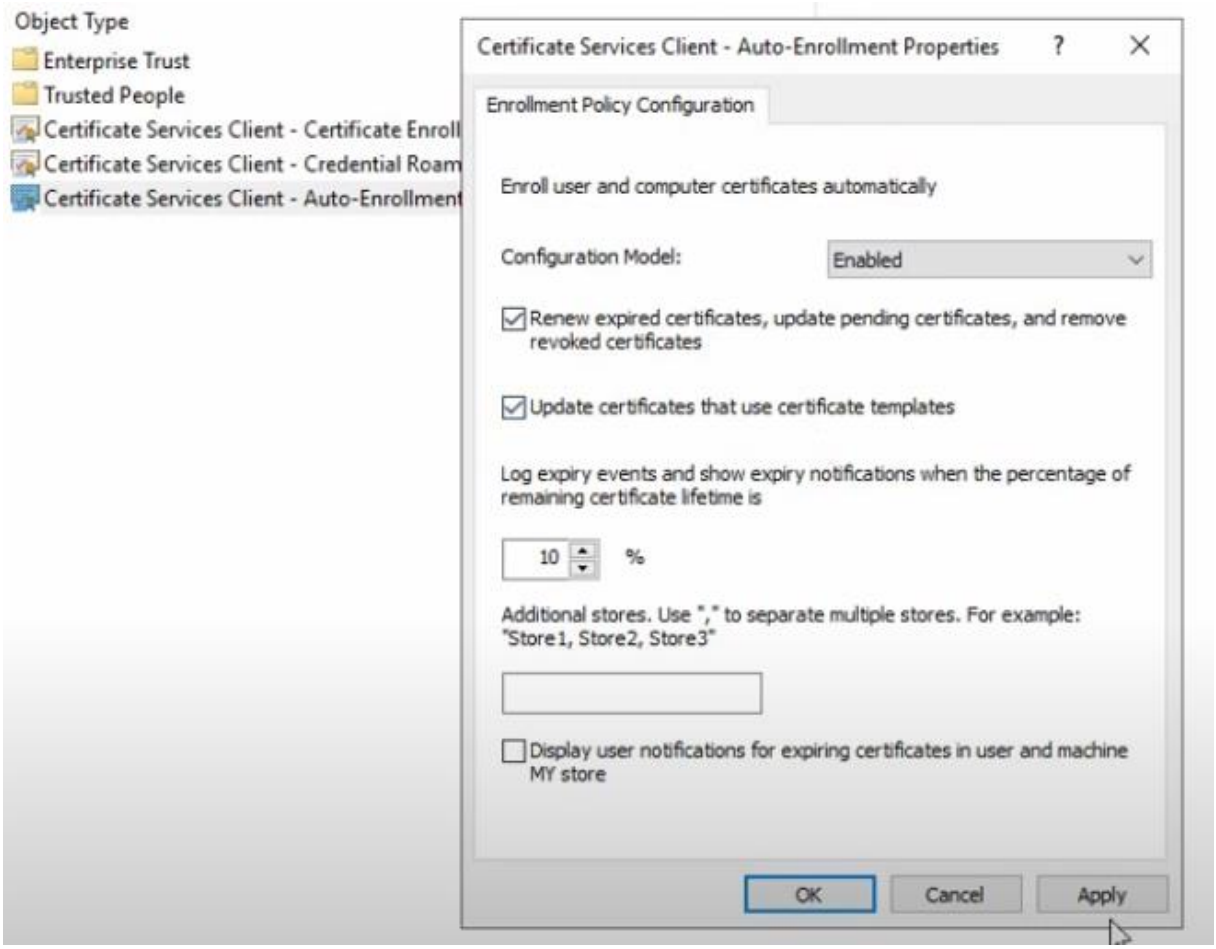


En cliquant sur *Edit* un nouvel onglet s'affichera.

Il faut ainsi suivre le chemin suivant :

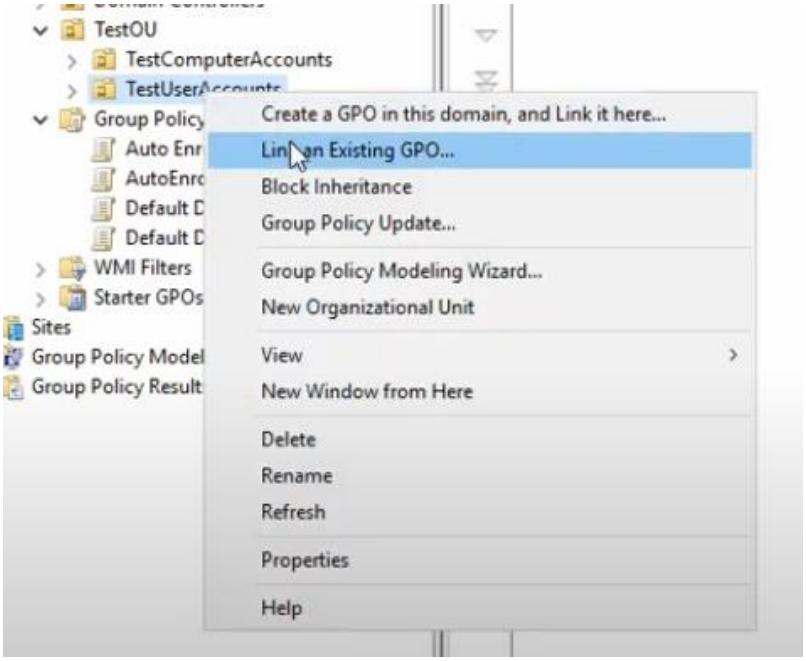


Nous pouvons ainsi ouvrir *Certificate Services Client – Auto-Enrollment.* Et paramétrer comme ci-dessous :



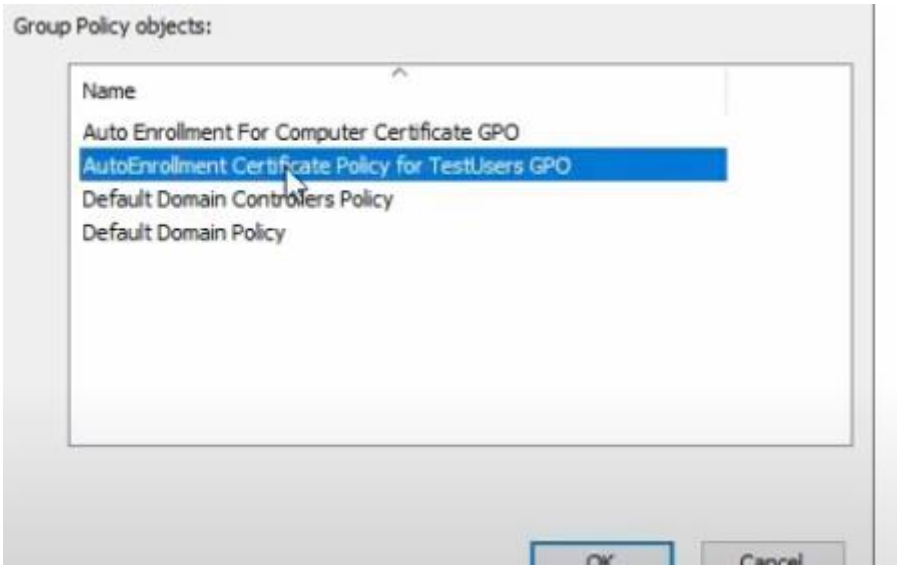
Une fois ces paramètres mis en place nous pouvons alors cliquer sur appliquer et quitter la page.

Nous devons alors retourner sur la page pour notre GPO précédemment utilisé.

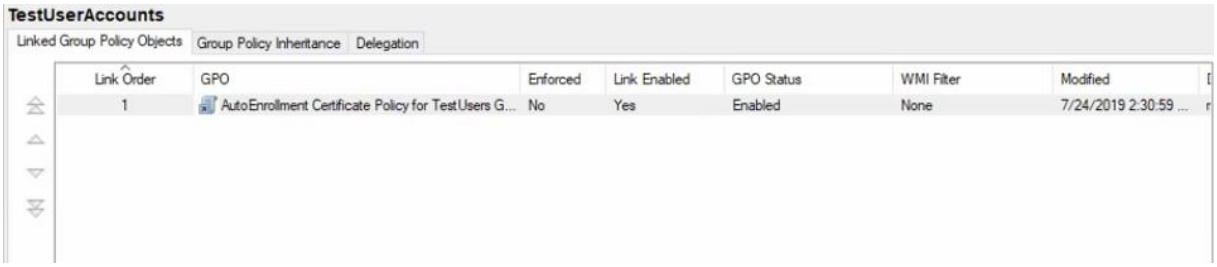


Nous pouvons ainsi aller dans *TestOU* puis *TestUserAccounts* puis *Link an Existing GPO…*

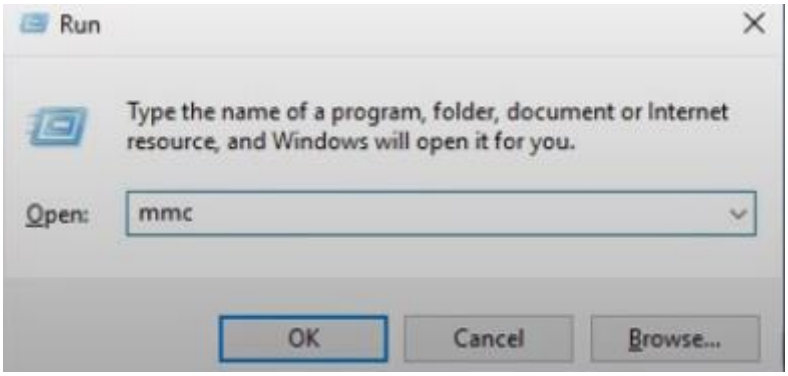
Dans la catégorie GPO la sélections du GPO créé précédemment est ainsi disponible.



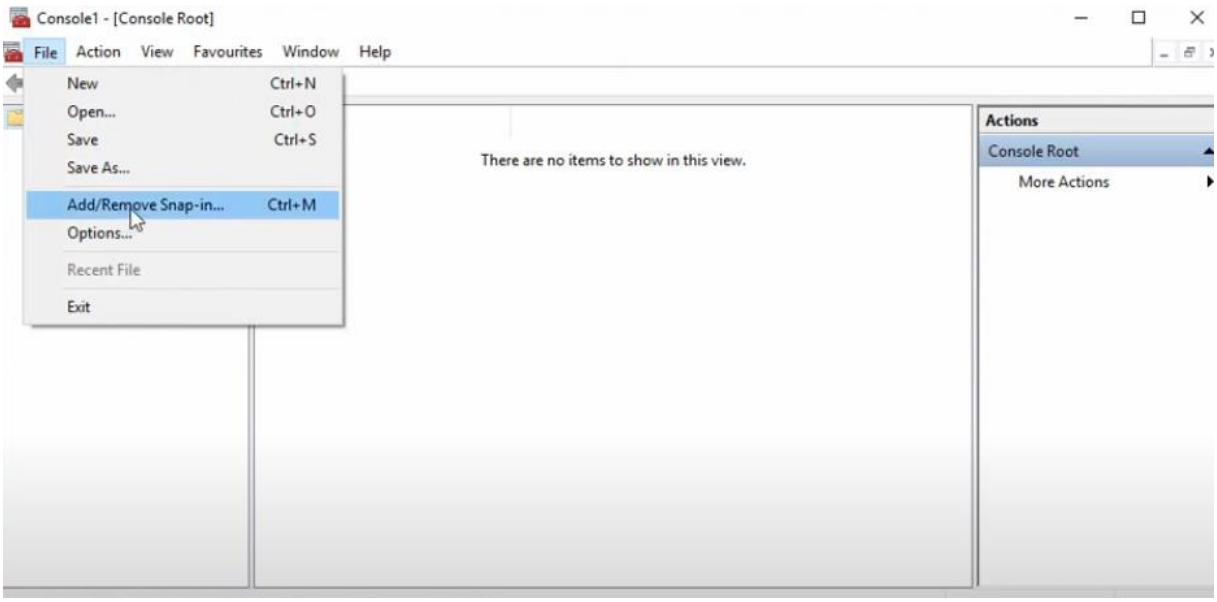
Notre lien à été correctement fait car en cliquant sur OK nous avons bien le lien qui s'affiche dans notre console :



Une fois toutes ces étapes faites nous pouvons alors retourner sur le bureau de l'ordinateur et appuyer sur Win + R et entrer *mmc* dedans :

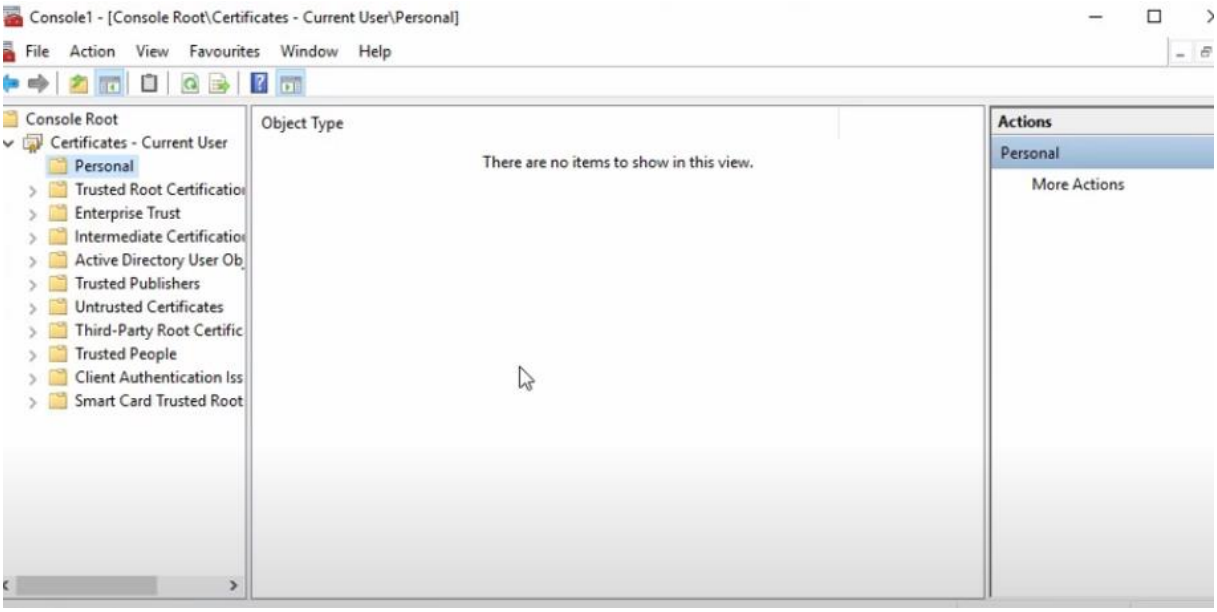


La microsoft management console va ainsi s'ouvrir.

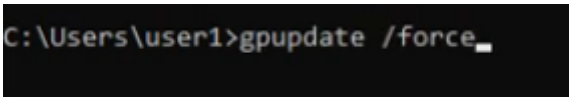


En suivant ce procédé, un nouvel onglet va s'ouvrir, nous pouvons alors sélectionner *Certificates* et cliquer sur *Add.*

Dans la partie certificat nous pouvons remarquer que rien n'apparaît :



Nous allons alors ouvrir notre cmd.



Cette commande permet alors de mettre à jour nos *Computer Policy* et *User Policy.*

Une fois cette étape faite, il faut alors se déconnecter puis se reconnecter à son compte pour que les changements soient pris en compte.

Après s'être déconnecté si les changements n'apparaissent toujours pas. L'erreur provient de notre *certificate template*. Pour régler l'erreur il faut retourner sur notre certificat, cliquer sur *manage* et dans la partie *Subject Name* nous pouvons alors décocher toutes les box en rapport avec un email.

Nous pouvons ainsi voir que notre user a ainsi un certificat associer à son compte.