**SOMMAIRE**

[1) Administration de l’Active Directory 2](#_Toc34564)

[a) Création console mmc 2](#_Toc34565)

[b) Réplication 3](#_Toc34566)

[2) Création d’objets dans Active Directory 5](#_Toc34567)

[a) Les unités d’organisation 5](#_Toc34568)

[b) Création d’unités d’organisation 6](#_Toc34569)

[3) Création d’utilisateurs 12](#_Toc34570)

[a) Création classique A 12](#_Toc34571)

[b) Ajouter une station de travail 14](#_Toc34572)

[c) Création de dossiers de partage e affectation des permissions aux administrateurs domaines 17](#_Toc34573)

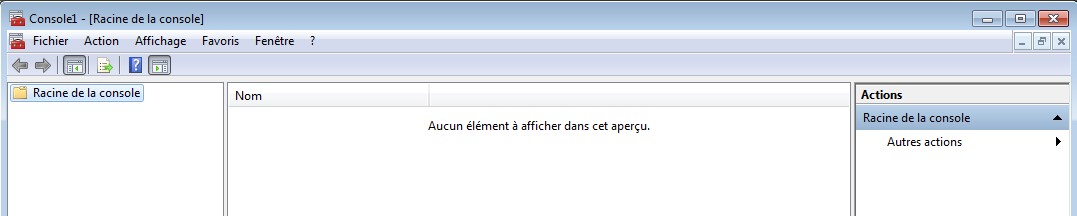
[d) Création du lecteur de travail d’un utilisateur 22](#_Toc34574)

# 1) Administration de l’Active Directory

## a) Création console mmc

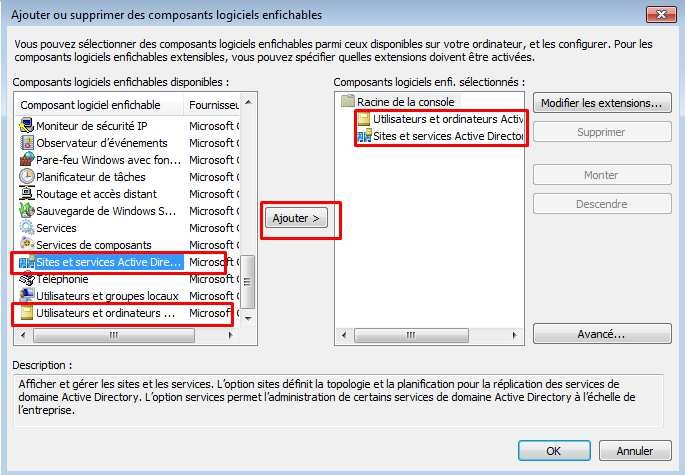
A présent vous allez pouvoir administrer votre domaine. En cliquant sur le bouton « Démarrer » puis sur « Outils d’administration » vous remarquerez le grand nombre de composants.

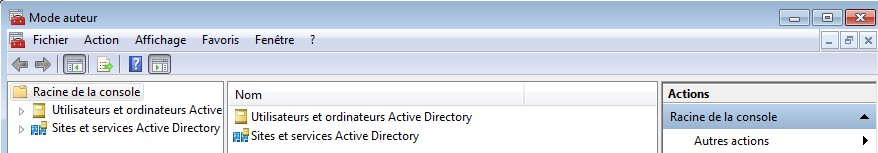
Tous on leur utilité mais certains sont très peu employés. Vous allez donc créer votre propre console d’administration **mmc** avec les **composants logiciels enfichables** les plus utilisés et la sauvegarder sur votre bureau. - Bouton « Démarrer », « Exécuter » et tapez **mmc**.



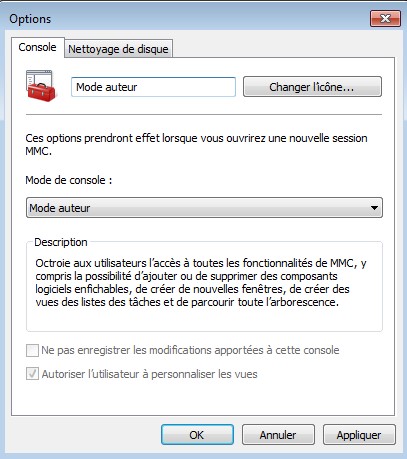
* Menu « Fichier », « Ajouter/Supprimer un composant… »
* Pour le moment choisissez les composants « Utilisateurs et ordinateurs Active

Directory » et « Sites et services Active Directory » et validez





* Avant d’enregistrer, cliquez sur le menu « Fichier » puis « Options » et choisissez le « Mode de console » = **Mode auteur**.



* Lisez la description de chaque mode de console

Mode utilisateur o Accès total o Accès limité

Fenêtre multiple

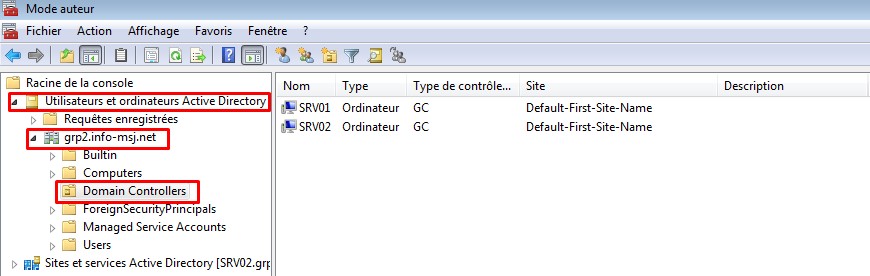
Fenêtre unique

* Enregistrez votre console sur votre bureau = « GRP02.**msc** ».

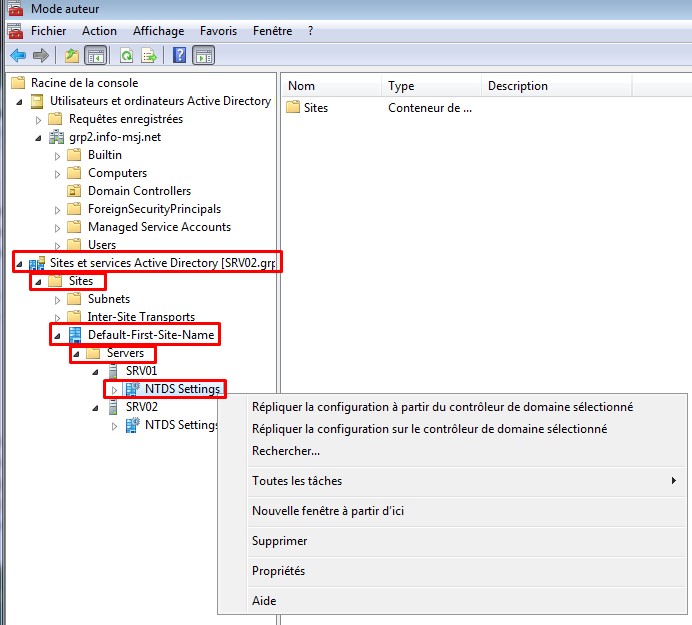
## b) Réplication

Avant de créer des objets (utilisateurs, unités d’organisation, ordinateurs) dans l’Active Directory, vous allez réaliser quelques vérifications à partir de votre console d’administration.

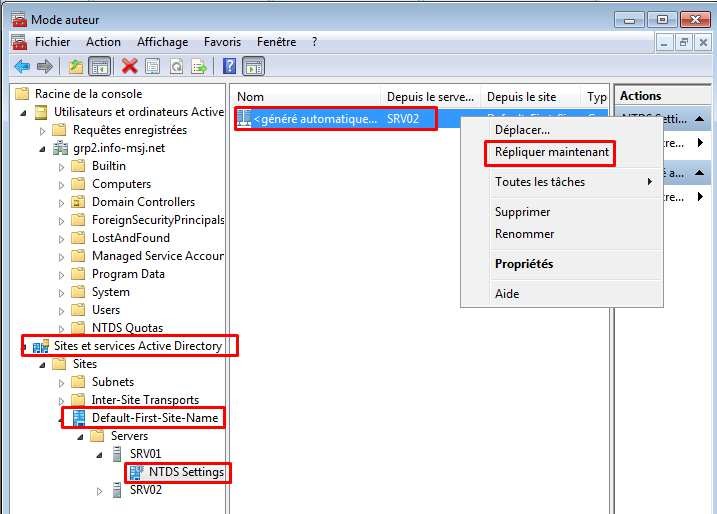
* Développez l’arborescence de votre domaine dans « Utilisateurs et ordinateurs Active Directory » et observez si les 2 contrôleurs de domaine sont bien présents dans le container « Domain Controllers ».



* Développez « **Sites et services Active Directory** » comme ci-dessous, faites un clic droit sur le connecteur et cliquez sur « **Répliquer maintenant** » et constatez la réplication réussie de l’Active Directory ou à cliquer sur réplication à partir de l’onglet « action ».



**OU**





# 2) Création d’objets dans Active Directory

## a) Les unités d’organisation

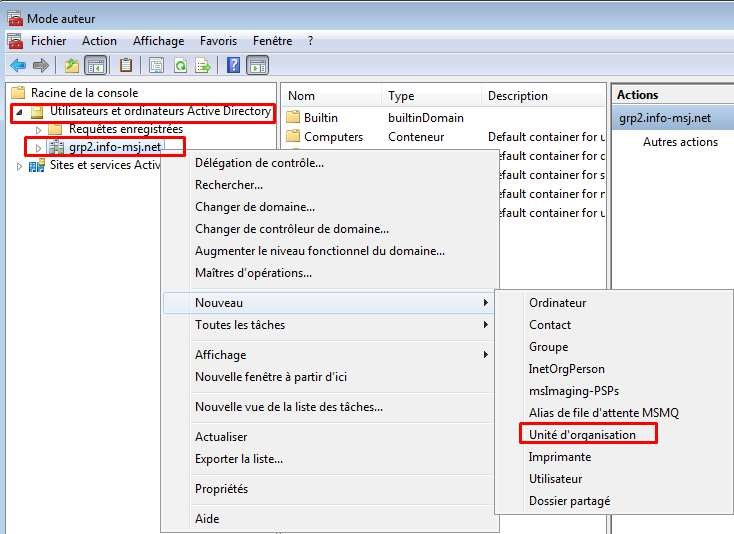
Les unités d’organisation (OU) sont uniquement des objets administratifs. C'est-à-dire qu’elles ne permettent pas aux objets contenus d’accéder aux ressources du domaine mais vont nous permettre d’organiser les objets de l’Active Directory à l’image de l’organisation de l’entreprise.

Par exemple on peut imaginer créer les unités d’organisation « Service achats », « Service comptabilité », « Service production », ensuite créer des sous unités d’organisation qui hébergeront les utilisateurs et les ordinateurs de ces services.

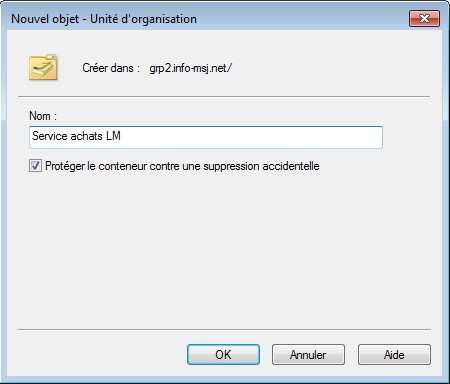
Par la suite nous appliquerons des stratégies qui différencieront les droits des utilisateurs et le comportement des ordinateurs.

## b) Création d’unités d’organisation

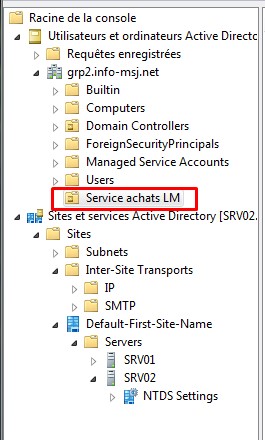
Ouvrez votre console d’administration et développez l’arborescence de votre domaine. Clic droit sur le domaine, puis sur **« Nouveau » « Unité d’organisation »**. Obtenez le même résultat que ci-dessous.



Ce qui donne :

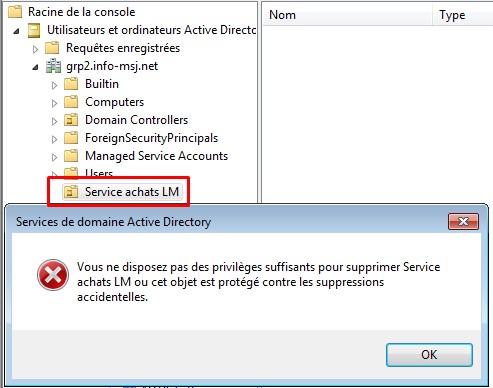


La nouvelle unité d’organisation est créée dans l’arborescence

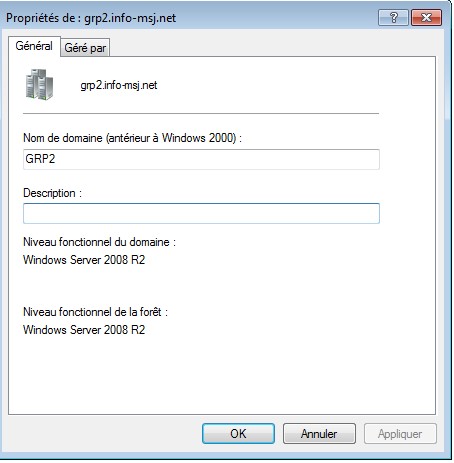
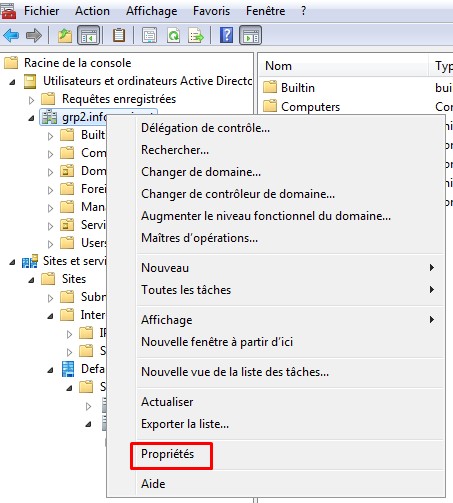


Essayez de supprimer une des Unité d’Organisation nouvellement créée : **clic droit/suprimer**

* Vous constatez qu’il est impossible de la supprimée

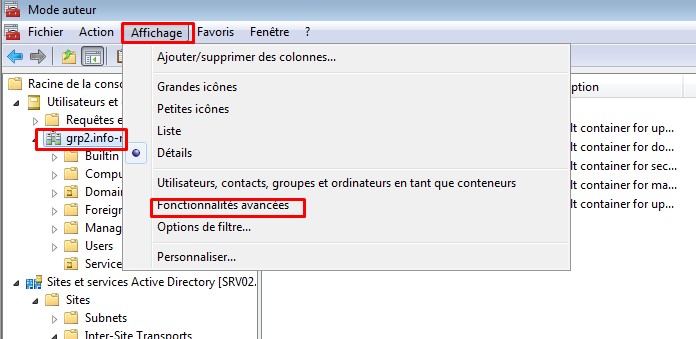


* Par un clic droit affichez les propriétés de cette Unité d’Organisation et observez les onglets

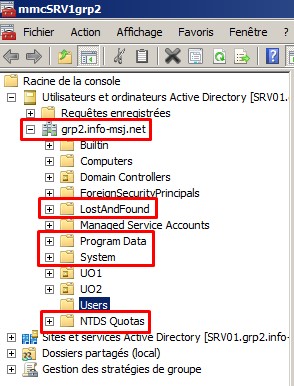


* Dans « utilisateur et ordinateur AD » cliquez sur votre domaine puis sur « affichage » et **« Fonctionnalités avancées**

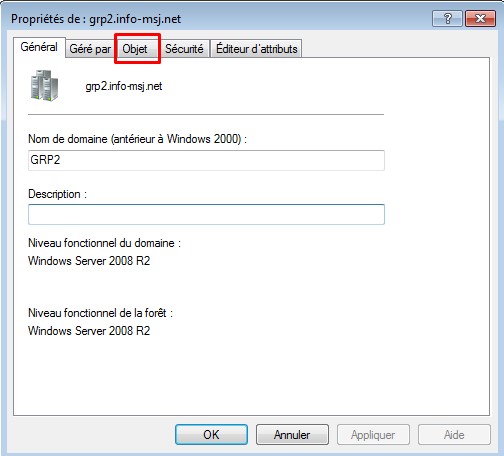
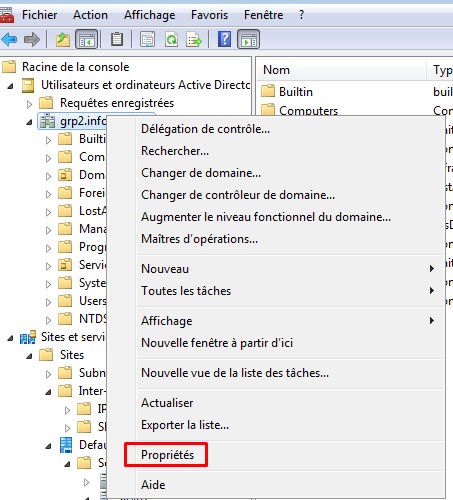
**»**



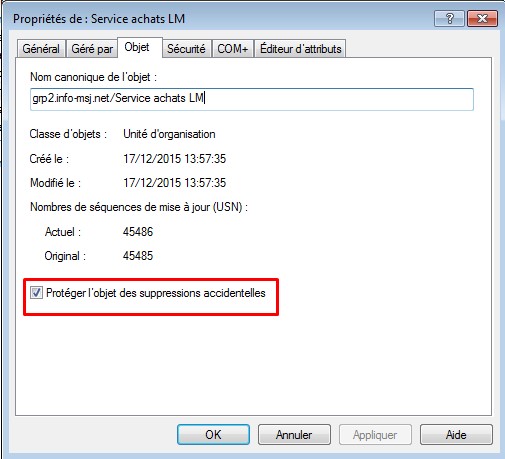
Ceci permet d’afficher les dossiers LostAndFound, Program Data, System et NTDS Quotas



* Par un clic droit affichez les propriétés de cette UO et observez à nouveau les onglets.et plus particulièrement l’onglet « **Objet** »



* Désactivez la case à cocher «**Protéger l’objet des suppressions accidentelles** » si vous désirez supprimer un tel objet



Attention si vous supprimez une UO contenant des utilisateurs ou des ordinateurs, ces objets seront orphelins. Vous venez de créer une **incohérence** dans la base de données.

# 3) Création d’utilisateurs

Vous allez maintenant peupler vos unités d’organisation. Vous utiliserez 3 méthodes de création **A), B) et C)**.

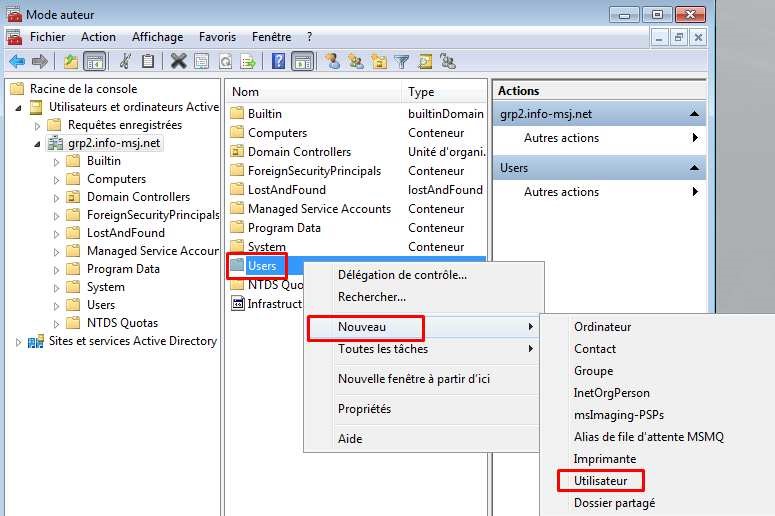
## a) Création classique A

- Créez un utilisateur de façon classique en un clic droit sur le conteneur

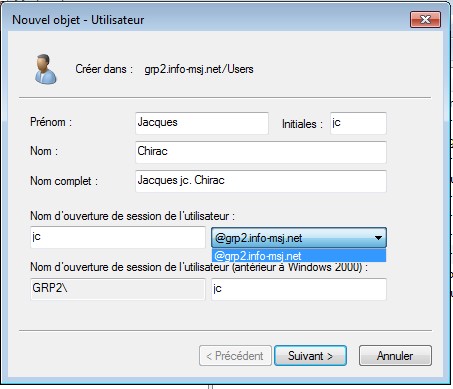
« users »

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Prénom | Nom | Nom  Complet | Nom ouverture session | Mot de passe complexe | Le mot de passe n’expire jamais |
| Jacques | Chirac | Jacques jc. Chirac | jc@grp2.info-msj.net | Tsgeri13860 | A  COCHER ! |

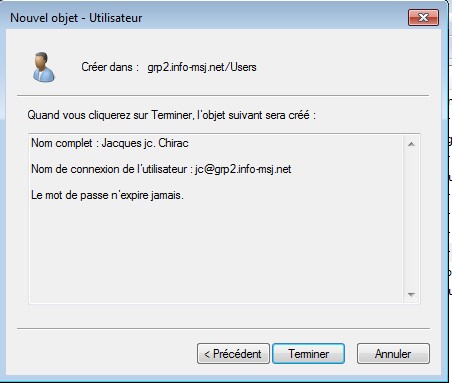
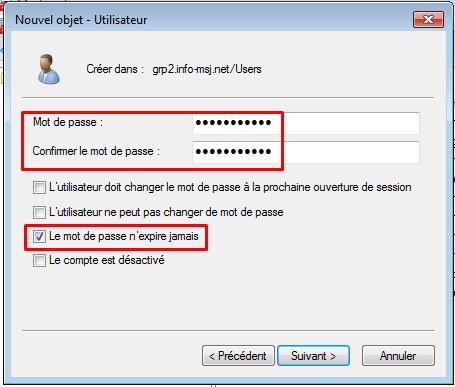
Certains utilisateurs se déplacent et se connectent sur différent postes de travail. Il est important pour eux de retrouver leur bureau (=leur profile=NtUser.dat) et leur répertoire de travail placés tous deux sur un serveur.



(Possibilité de choisir le nom de domaine d’appartenance souhaité.)



Mot de passe : Tsgeri13860



L’utilisateur est ajouté :

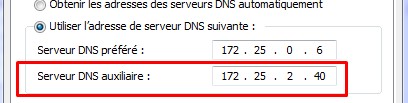
## b) Ajouter une station de travail

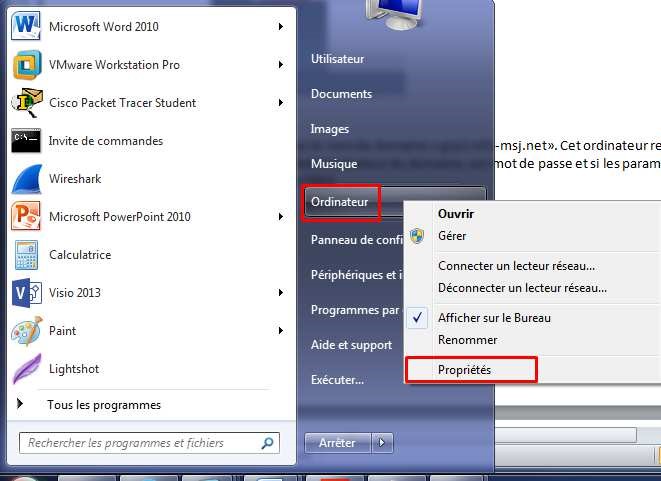
Avant de poursuivre

* Ajouter une station de travail ( sur mon poste physique) à son domaine et à un serveur.

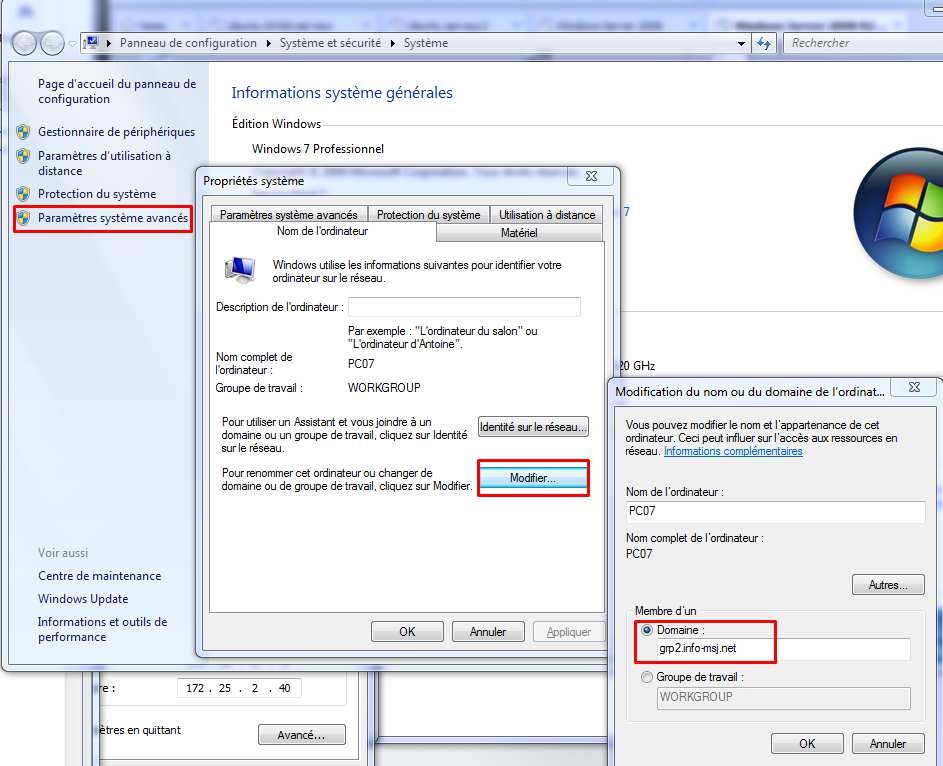
Sur mon poste physique, dans l’explorateur de fichiers, clic droit sur Ordinateur, propriété, Paramètres systèmes avancés, Nom de l’ordinateur, Modifier, cliquer sur Domaine et ajouter le nom de domaine.

**D’abord, être sûr d’avoir l’une des 2 adresses DNS remplie avec l’adresse du Serveur.** **Sinon, on ne peut pas ajouter le poste à la forêt.**





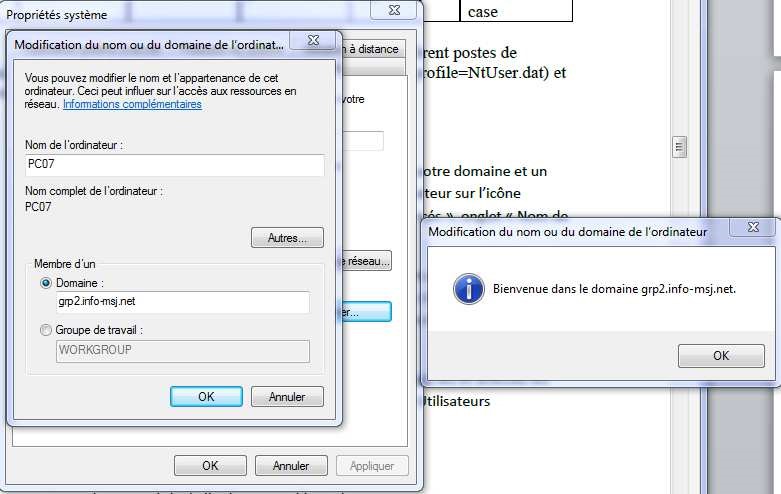
* Cliquez sur le bouton « Domaine » et entrez le nom de domaine. L’ordinateur physique rejoindra le domaine que si vous utilisez l’identité d’un Administrateur du domaine, son mot de passe et si les paramètres IP sont correctes (@IP, masque, passerelle, serveur DNS)



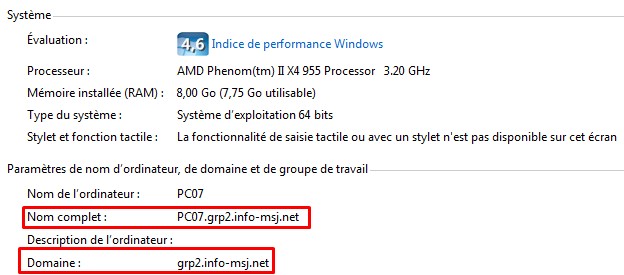
Ensuite windows demande une validation avec un compte administrateur.

Loggin=administrateur

Mot de passe=Tsgeri13860



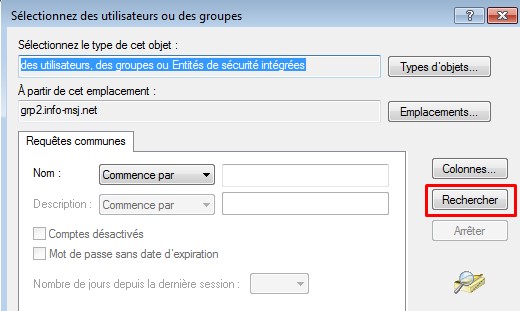
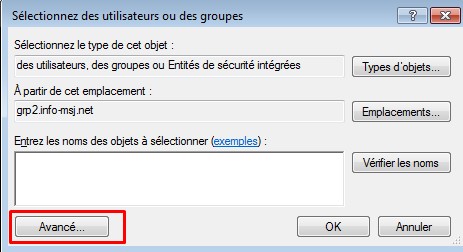
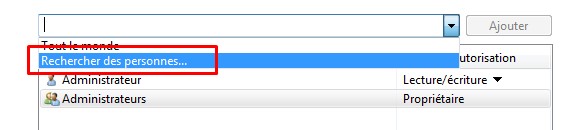
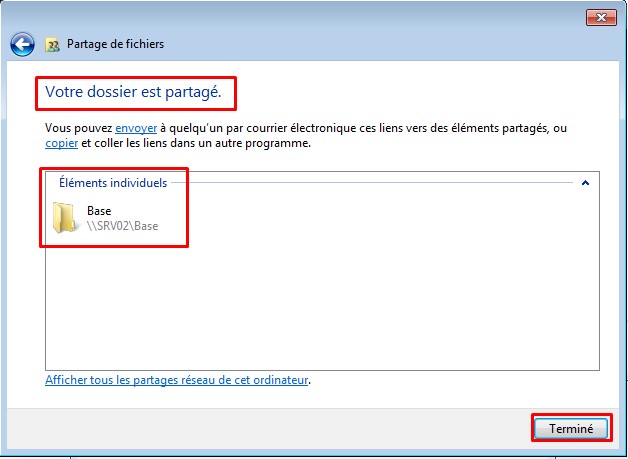
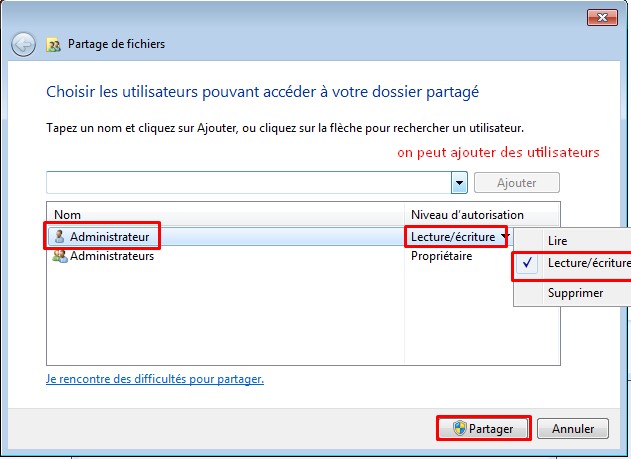
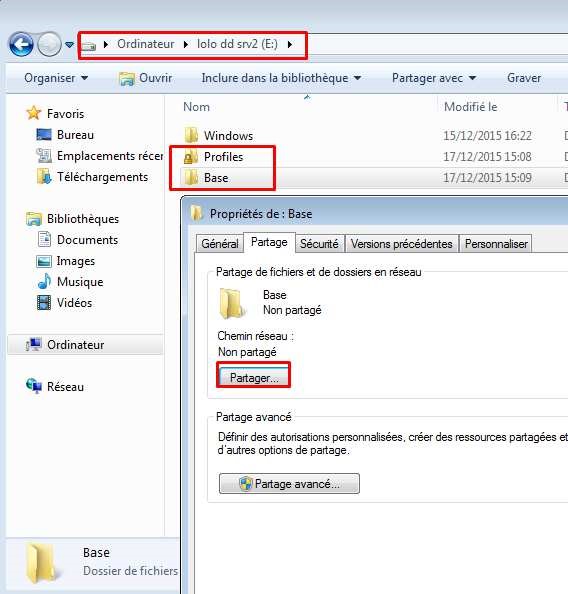
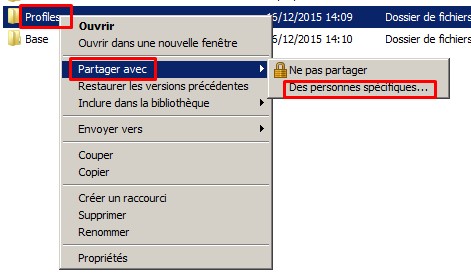
On peut vérifier la nouvelle configuration du domaine (ctrl+pause) :

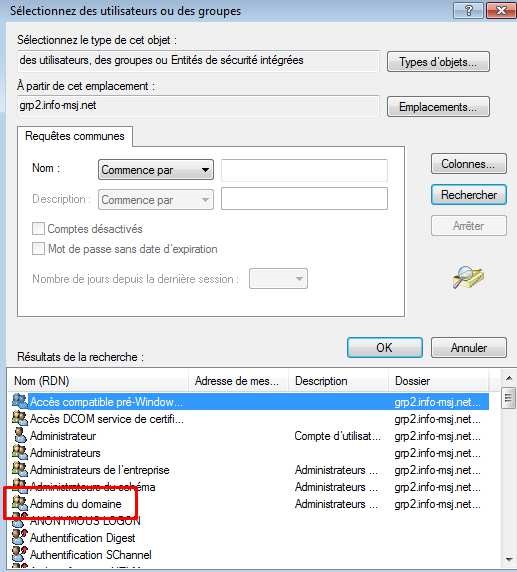


## c) Création de dossiers de partage e affectation des permissions aux administrateurs domaines

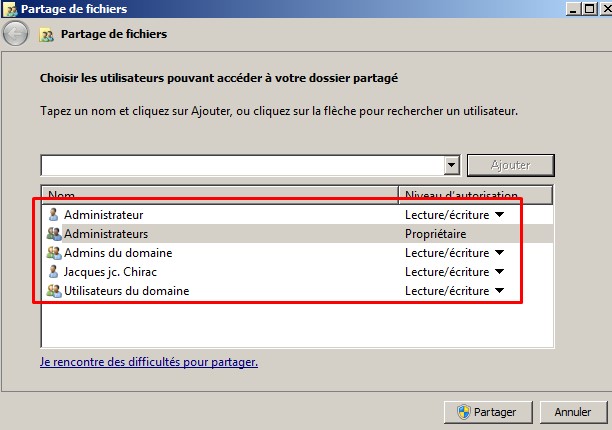
- Créez sur le serveur 2, deux répertoires (Profiles et Base), partagez-les et affectez les permissions aux «

Administrateurs du domaine » et aux « Utilisateurs authentifiés ». Supprimez le groupe tout le monde. (par défaut il n’y est pas)

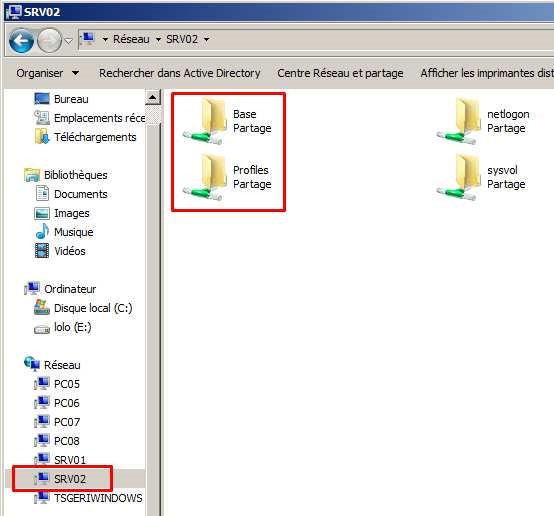
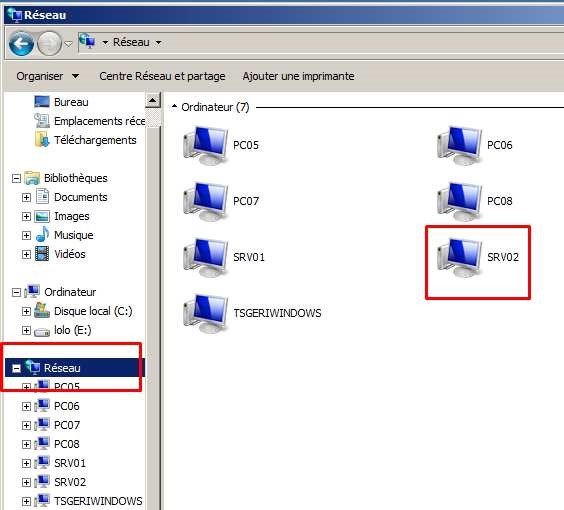




Il faut créer « utilisateur de domaine » au lieu de « utilisateurs authentifiés » sinon cela ne fonctionne pas, j’ai aussi ajouté l’utilisateur même (Jacques Chirac) pour tester, et cela fonctionne avec ou sans l’utilisateur lui-même.



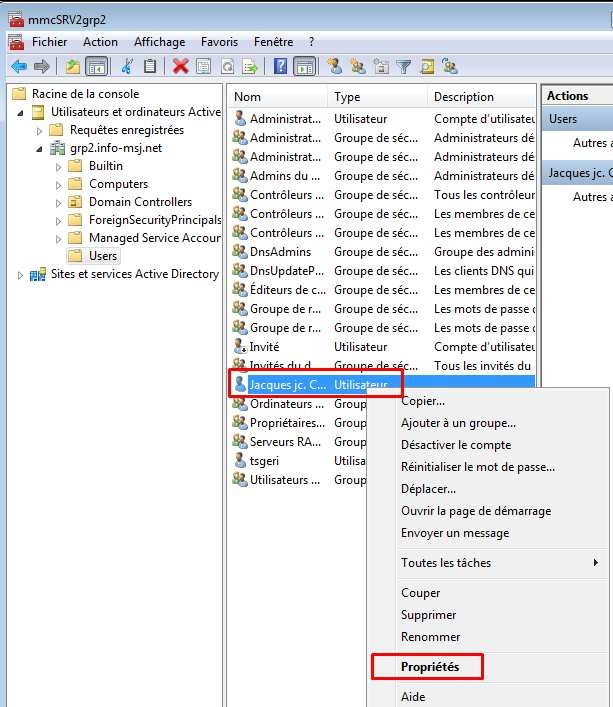
Depuis, le serveur 1, on peut accéder aux fichiers de partage du serveur 2

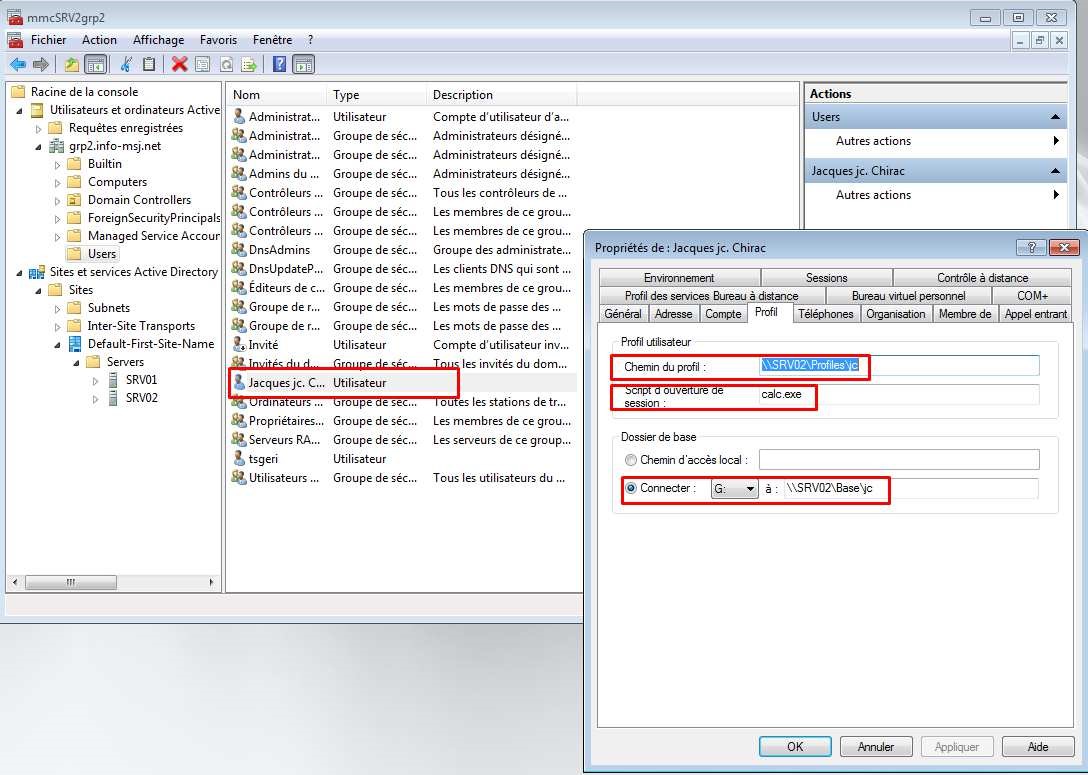


## d) Création du lecteur de travail d’un utilisateur

Maintenant poursuivons

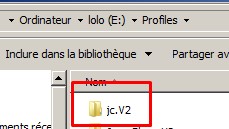
* Ouvrez les propriétés de l’utilisateur créé en A)
* Cliquez sur l’onglet « Profil » et faites comme ci-dessous sur le serveur02 (ou sur le 01) pour que cela fonctionne





Ou autre méthode (réalisée sur le serveur 1)

En faisant « appliquer » le nom d’utilisateur remplace « username » ici il sera remplacé par « jc »

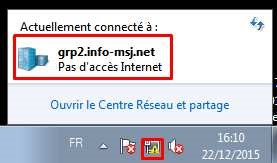
Pour vérifier que cela fonctionne, il faut que le dossier **« jc.V2 »** apparaisse dans le dossier racine **E:/Profiles,** et que **« jc »** est bien le seul à pouvoir y accéder

**Attention : Il faut administrer avec mmc sur un seul serveur (surtout ne pas ouvrir mmc sur deux consoles en même temps)**

**Ensuite il faut enregistrer, les modifications et fermer puis ré-ouvrir la session de l’ordinateur hôte.**

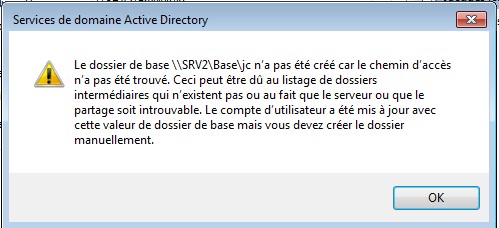
**Toujours vérifier que le nom domaine souhaité est activé.**

**Ici la connexion indiquait « pas d’accès à internet », en fait ce n’était pas le cas, le proxy a été configuré afin d’avoir l’accès à internet, mais la connexion principal du réseau local était en défaut.**



Vérifier que l’on se trouve dans le domaine, sinon le lecteur n’apparait pas.

* **Ouvrez une session sur la station de travail :**  Nom = jc@grp2.info-msj.net Mot de passe = Tsgeri13860 Problème rencontré :

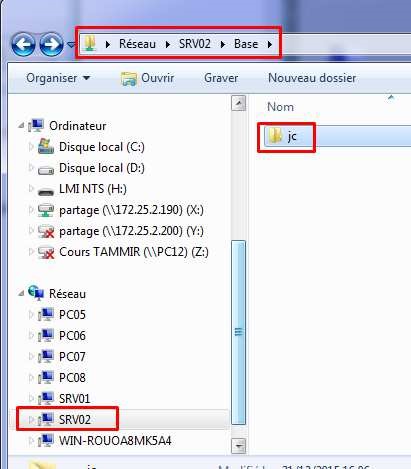


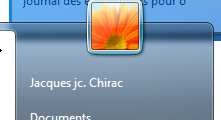
Solution : L’erreur venait du chemin d’accès, j’ai fait une erreur sur le nom du serveur au lieu de mettre SRV02, j’ai mis SRV2.

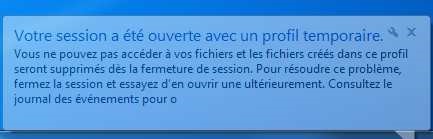
Le lecteur réseau **G:** nommé « **jc** » se créé dans « ordinateur » ainsi que le dossier « **jc** » dans le « Réseau »

Depuis ma machine physique, on peut voir apparaitre le fichier « jc » précédemment créé dans le SRV2 du réseau

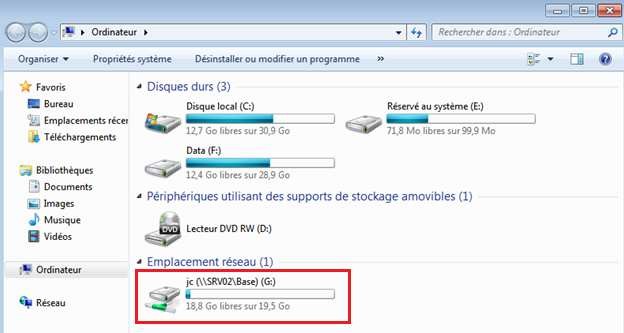




Ouverture d’une session en tant Jacques Chirac :**|** Message de windows à l’ouverture : pour des profils temporaires :



* Création de deux raccourcis dans le lecteur G: afin de vérifier que l’utilisateur possède le droit d’écriture
* Fermez la session et ré-ouvrez une nouvelle session sur une autre station de travail si possible
* Vérifiez dans l’explorateur l’existence du lecteur **« G :** » et son accessibilité pour y stocker le travail effectué par l’utilisateur.

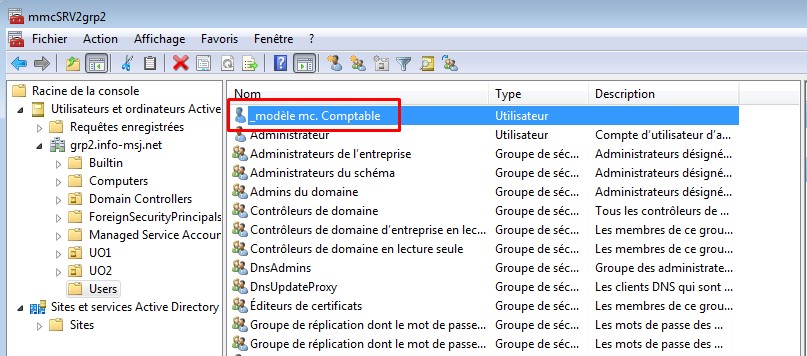


* Vérifiez la présence des 2 raccourcis C’est ce qu’on appelle un **profile errant**.

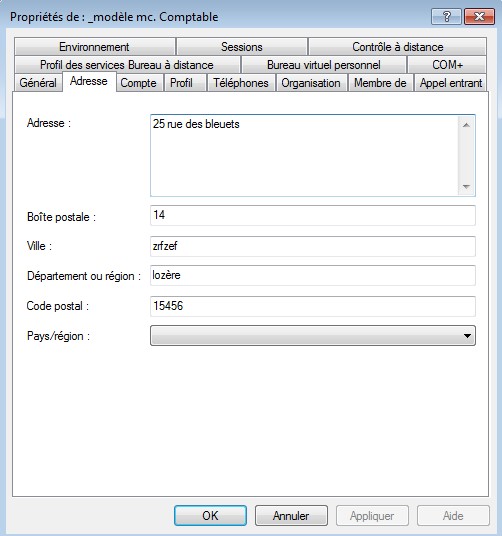
**Si l’on tente de se connecter avec un profil d’utilisateur créé qui n’a pas de droit d’admin ou de contrôleur, on ne PEUT PAS se connecter à SRV02, et il n’est apparemment pas possible de se modifier les droits de Permettre l’ouverture d’une session locale qui est dans Attributions des droits utilisateur, qui est dans stratégies locales, lui-même dans Stratégie de sécurité locale qui est dans Outils d’administration. On peut régler le problème de façon temporaire en mettant ajoutant l’utilisateur en tant qu’Admin du domaine… Ce qui n’est pas vraiment une solution.**

## e) Création d’utilisateur à partir d’un modèle :

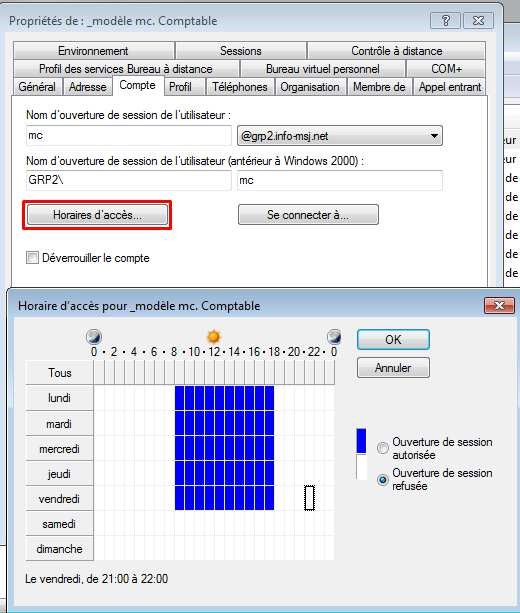
Créer un utilisateur nommé « **\_modèle Comptable** » dans le conteneur « **Users** » Renseigner les onglets et les zones de saisie comme ci-dessous.



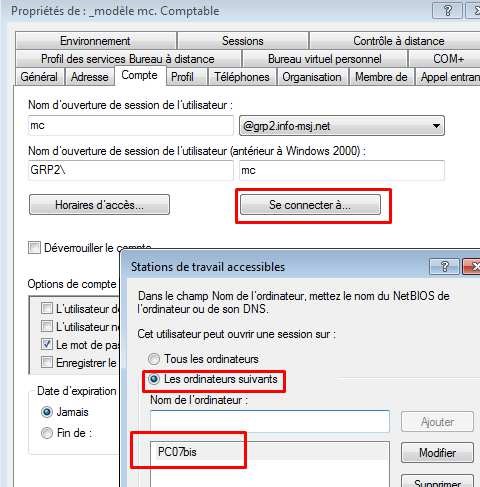
Configuration de l’adresse de l’utilisateur : **\_modèle Comptable** :



Configuration des horaires de permissions d’accès de l’utilisateur : **\_modèle Comptable** :



Configuration du ou des station(s) de travail accessible(s) (ici PC07bis) via le profil :



* Créez un nouvel utilisateur en cliquant droit sur le compte modèle et sur « Copier », cela sert à créer rapidement un nouvel utilisateur, en copiant un existant
* Ouvrez les propriétés de ce nouvel utilisateur et parcourez les onglets pour constater que **tout n’a pas été copié**

