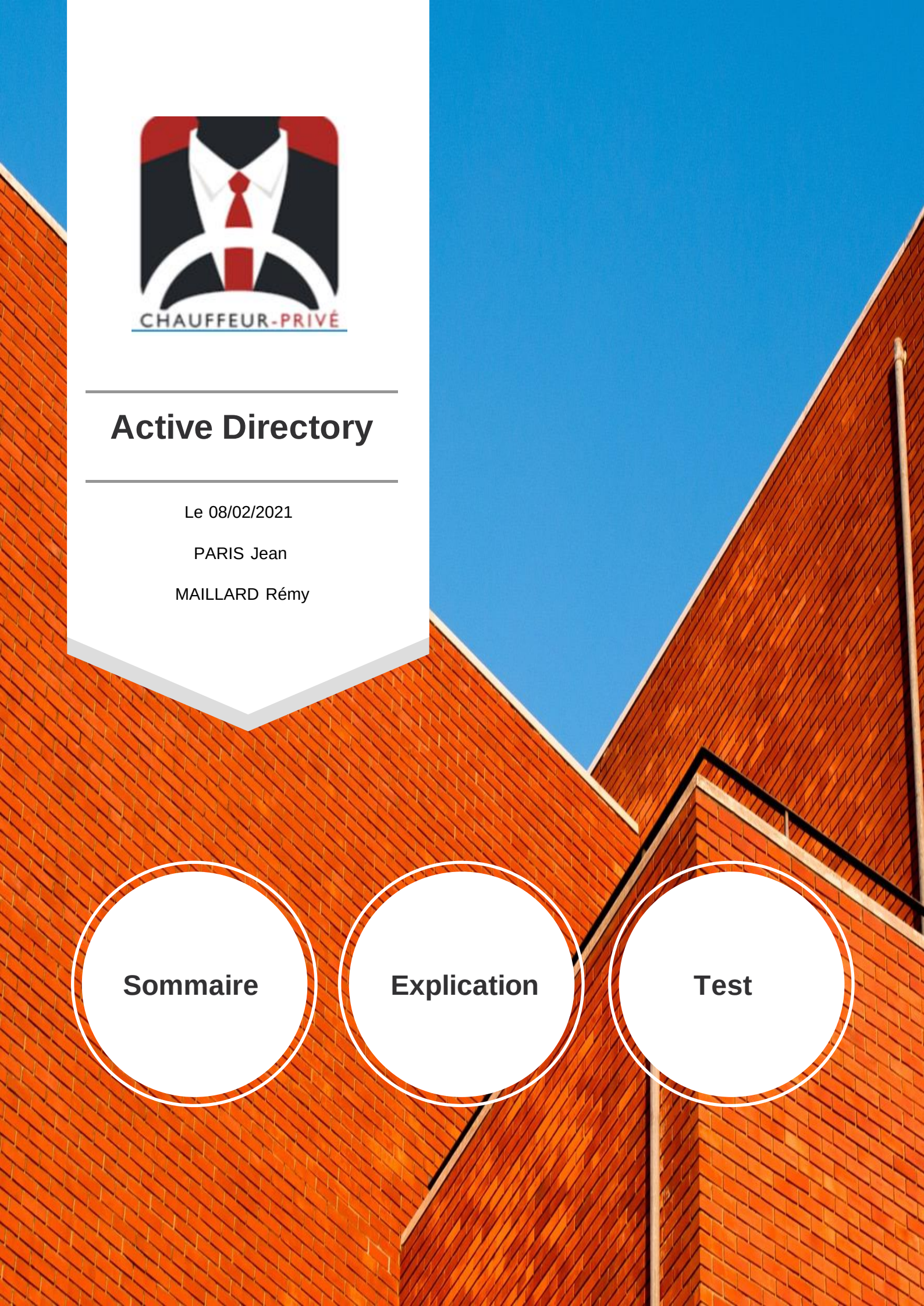


Active Directory

Le 08/02/2021

PARIS Jean

MAILLARD Rémy

Sommaire

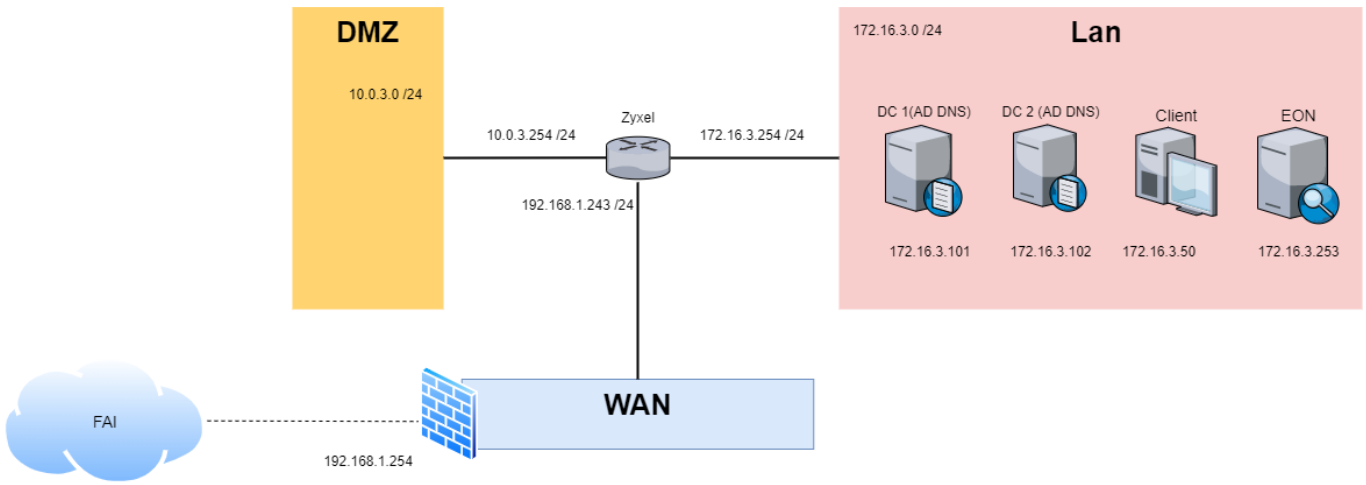
Explication

Test

Table des matières

Visio de l'infrastructure (mission 3) 2
I] Active Directory : 3
Le rôle d'un AD : 3
II] Installation et création de la forêt 3
Installation : 3
Configuration : 4
Les groupes et users : 5
Les profils (Itinérants) 7
Les types de profils : 7
1]Création du fichier partagé sur le SDF : 8
2] Configuration du chemin du profil : 9
Test profil : 10
Redondance de l'AD : 11
Stratégies de groupes (GPO) : 12
III] Tests 17

Visio de l'infrastructure (mission 3)



I] Active Directory :

Le rôle d'un AD :

Un active directory est un service s'appuyant sur un annuaire LDAP, permettant de faire de la gestion de session, de mettre en place de la sécurité et d'appliquer des stratégies de groupes (GPO) sur des UO (Unité d'Organisation). Il en existe une infinité comme la stratégie de mot de passe, stratégie de fond d'écran ….

II] Installation et création de la forêt

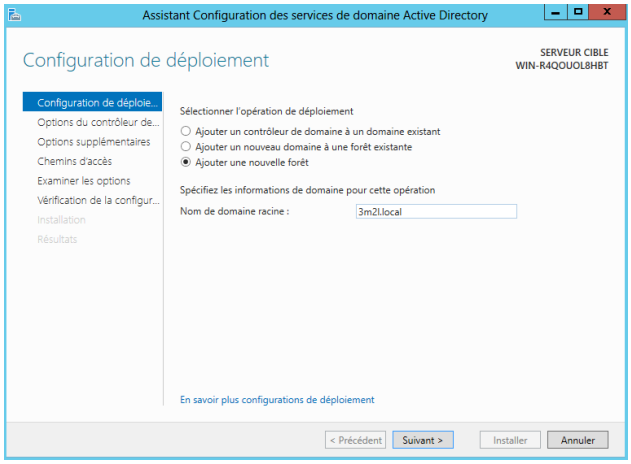
Installation :

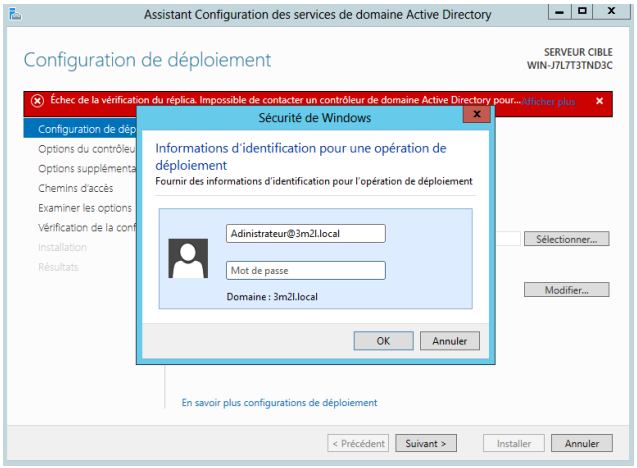
Tuto expliquant l'installation du service AD sur un Windows server :

https://techexpert.tips/fr/windows-fr/installation-dactive-directory-sur-windows-server/#:~:text=Ouvrez%20l'application%20Server%20Manager,le%20bouton%20Ajouter%20des%20fonctionnalit%C3%A9s.

Configuration :

Pour la mise en place de l'Active Directory nous devons créer une nouvelle forêt car il n'y en a pas encore d'existante. On indique le domaine racine c'est-à-dire sur quel domaine la forêt va s'appuyer : le domaine 3m2l.local



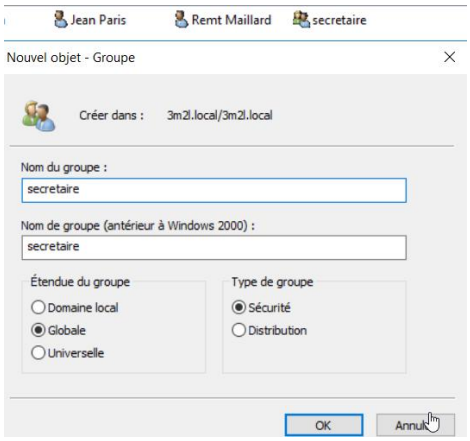


Afin de rallier notre AD au domaine nous devons avoir l'autorisation d'un Domain Controller, c'est celui qui dispose des droits d'entrée dans le domaine. Administrateur@3m2l.local mdp : Admin123$

Les groupes et users :

Afin de gérer nos utilisateurs il faut déjà les créer et les renseigner dans des groupes pour faciliter la compréhension et gérer les droits plus facilement : on définit les droits à un groupe et non à chaque user. Dans notre cas nous allons créer des groupes par secteur dans l'entreprise.

ex : secrétaire, commercial, technicien …

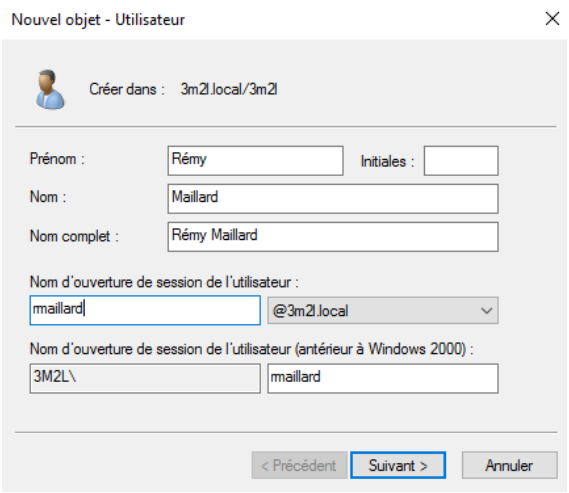


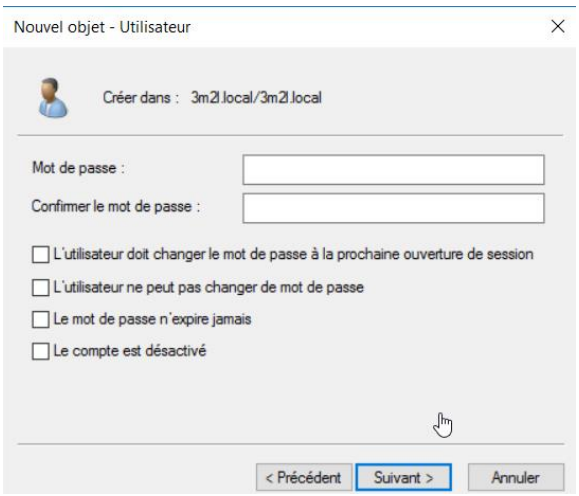
Le groupe « secretaire » maintenant présent nous allons créer nos users (nouveau > utilisateurs).

Comme dans notre architecture nous créons que quelques utilisateurs, nous faisons le tout à la main mais à savoir que dans un contexte d'entreprise comportant un grand nombre d'employés, il est plus intéressant d'automatiser la création de ces utilisateurs à l'aide d'un scrypt PowerShell comme nous avons fait en début d'année.

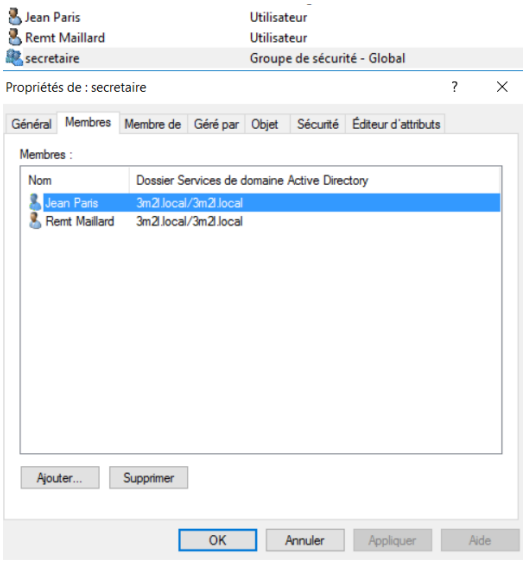
Un exemple d'utilisateur crée :

Le mot de passe des users sera « Admin123$ » afin de le retenir plus facilement. Il est également possible de définir une stratégie de mot de passe directement depuis la création du user.





Une fois les users crées, il faut les placer dans les groupes. Afin de se faciliter la tâche il est plus intéressant de faire par le biais du « drag and drop » (glisser déposer) qu'on active dans « affichage » et en activant «utilisateurs, contacts et ordinateurs en tant que conteneurs ».



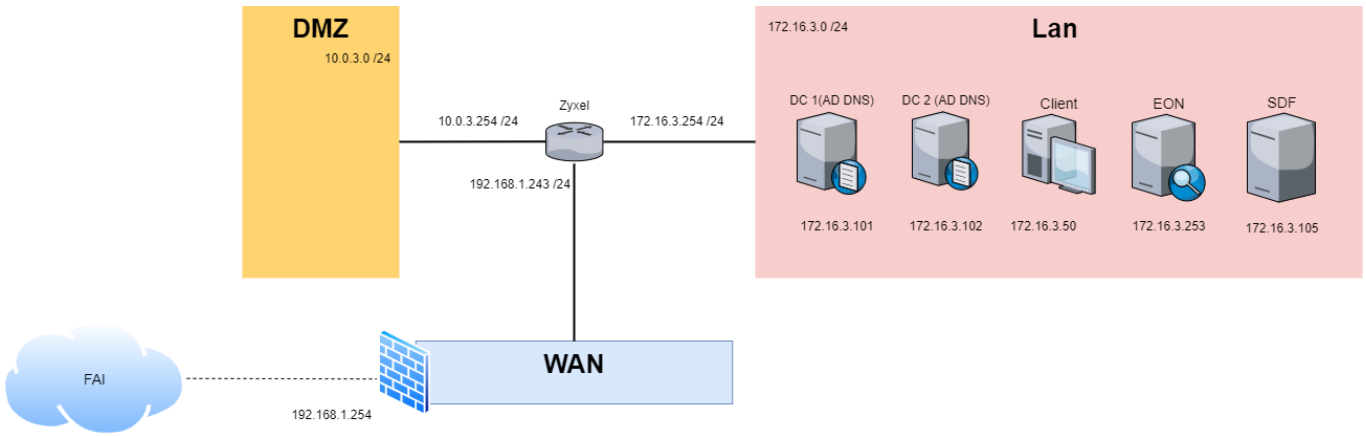
Les profils (Itinérants)

Les types de profils :

Il existe plusieurs types de profils :

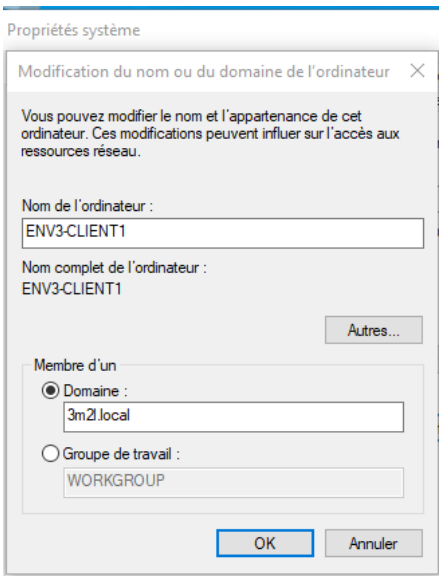
- Profil **local** : chargé localement sur la machine
- Profil **itinérant** = stocké dans un fichier partagé sur un serveur (il y a une copie en local).
- Profil **temporaire** = lorsque le profil itinérant ne peut être chargé. Une fois la session fermée toutes les données seront supprimées.
- Profil **Obligatoire** = On définit un profil à l'utilisateur (par exemple si on met un fond d'écran et que l'on éteint l'ordinateur, il se rallumera avec un bureau vierge).

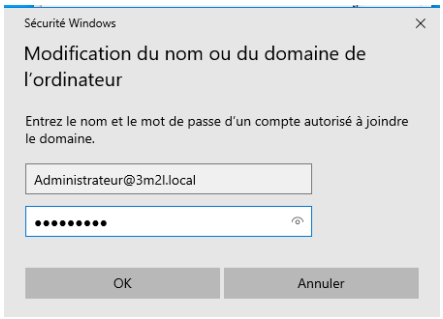
Pour mettre en place nos profils itinérants, on rajoute à notre infrastructure un Serveur De Fichier pour qu'il puisse stocké les profils.



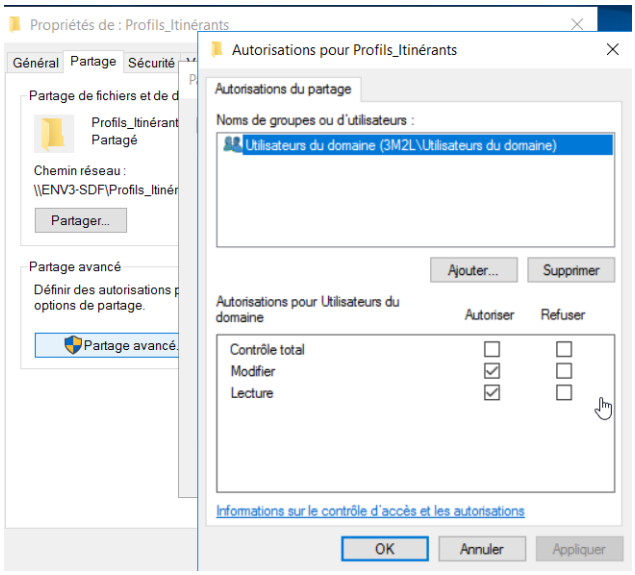
1]Création du fichier partagé sur le SDF :

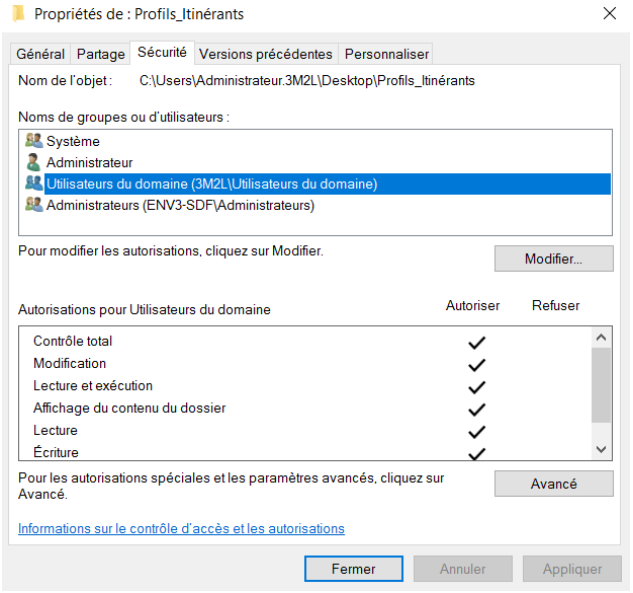
La première étape est de mettre le serveur de fichier dans le domaine 3m2l.local pour qu'il puisse gérer la sécurité de partage et les droits d'écriture.





La 2e étape est de mettre en place la sécurité. On autorise les utilisateurs du domaine à accéder au dossier partagé et on autorise également le fait qu'il puisse écrire dessus pour y mettre le contenu de leur profil.



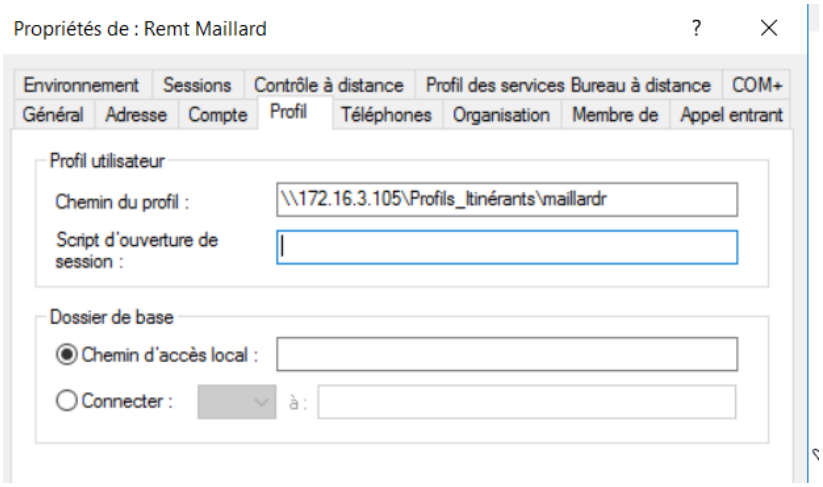


2] Configuration du chemin du profil :

Définir le chemin de profil permet de définir où sera stocké le contenu du profil. Ici on définit que le profil contenu dans le dossier maillardr sera stocké dans le dossier partagé « Profils_Itinérants » sur le serveur de fichier. Afin de ne pas rajouter à la main à chaque fois le nom du fichier qui devra être crée, on peut sélectionner tout nos users et dans le chemin du profil inscrire :

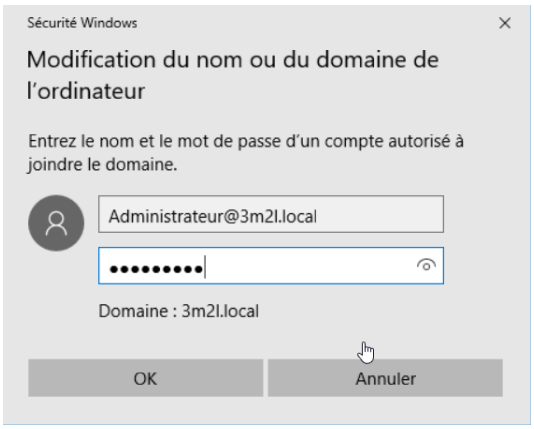
« \\172.16.3.105\Profils_Itinérants\%username% »

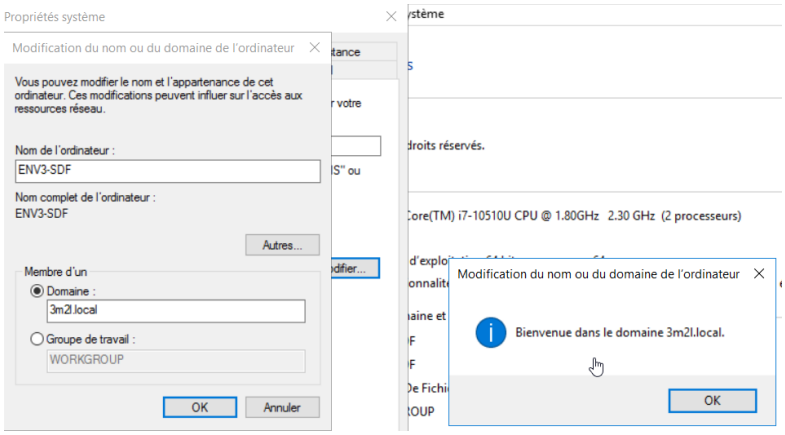
Ainsi le « %username% remplacera automatiquement par le nom du profil correspondant.



Test profil :

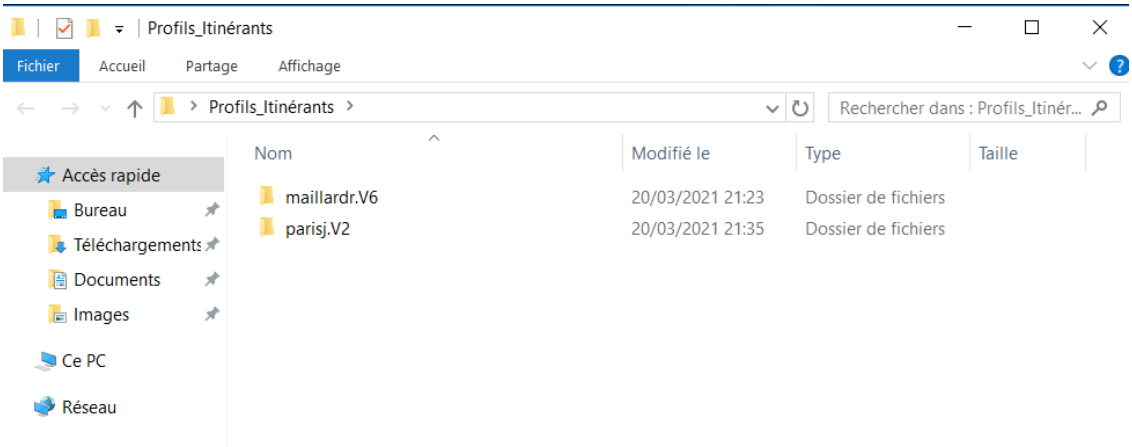
Afin de tester si notre profil arrive bien à charger il faut d'abord inscrire l'hôte dans le domaine pour qu'il comprenne qu'il doit charger le profil depuis le domaine et non en local.





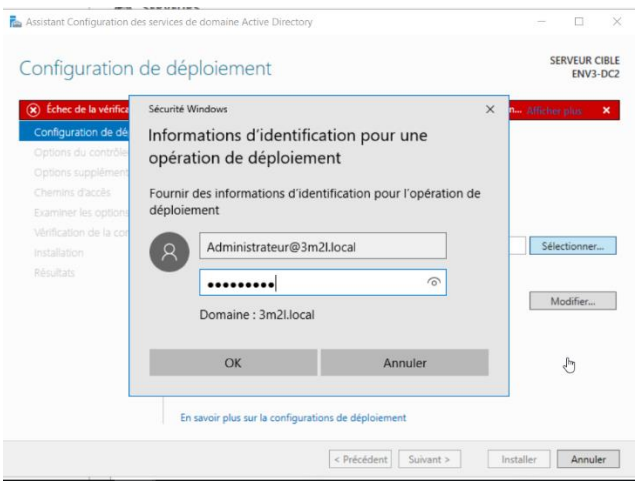
Peut importe si le profil est chargé sur un Windows 10 ou Windows 7 le résultat doit être le même. Les Login et Mots de passes sont ceux que nous avons ajouté lors de la création des users.

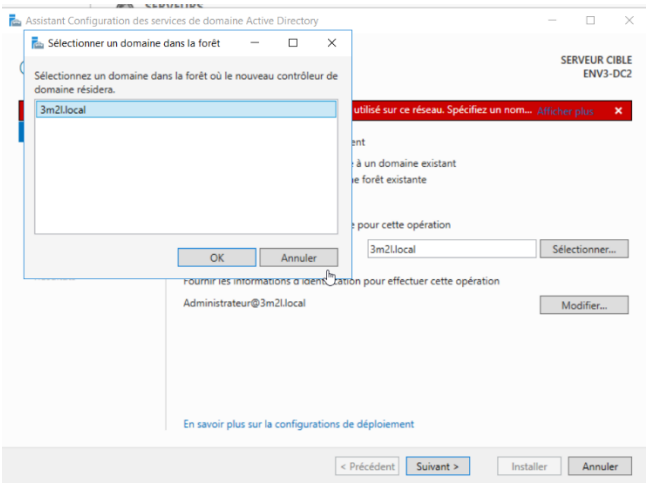
Pour vérifier si le profil s'est bien chargé depuis le serveur de fichier, on doit voir le dossier du profil sur le dossier partagé. Le dossier du profil est crée lors de sa première connexion.



Redondance de l'AD :

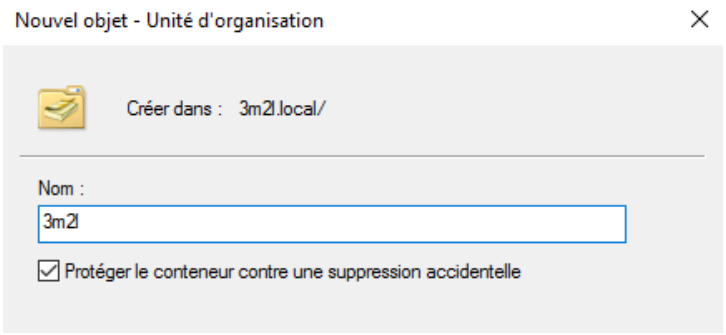
Pour rajouter un nouveau Domain Controller il faut tout comme le serveur maître installer le service DNS en plus du service AD, celui-ci est indispensable car le service AD s'appuie sur le service DNS. Il faut donc d'abord redonder le DNS. Il est possible de configurer les 2 en même temps pour gagner du temps. Pour rajouter un domain controller il faut lors de la configuration indiquer vers quel domaine il va devoir s'appuyer, soit dans notre cas le domaine : 3m2l.local. Pour pouvoir y accéder il faut l'autorisation d'un utilisateur faisant autorité, pour cela on indique login et mot de passe du domain controller : Administrateur@3m2l.local mdp : Admin123$



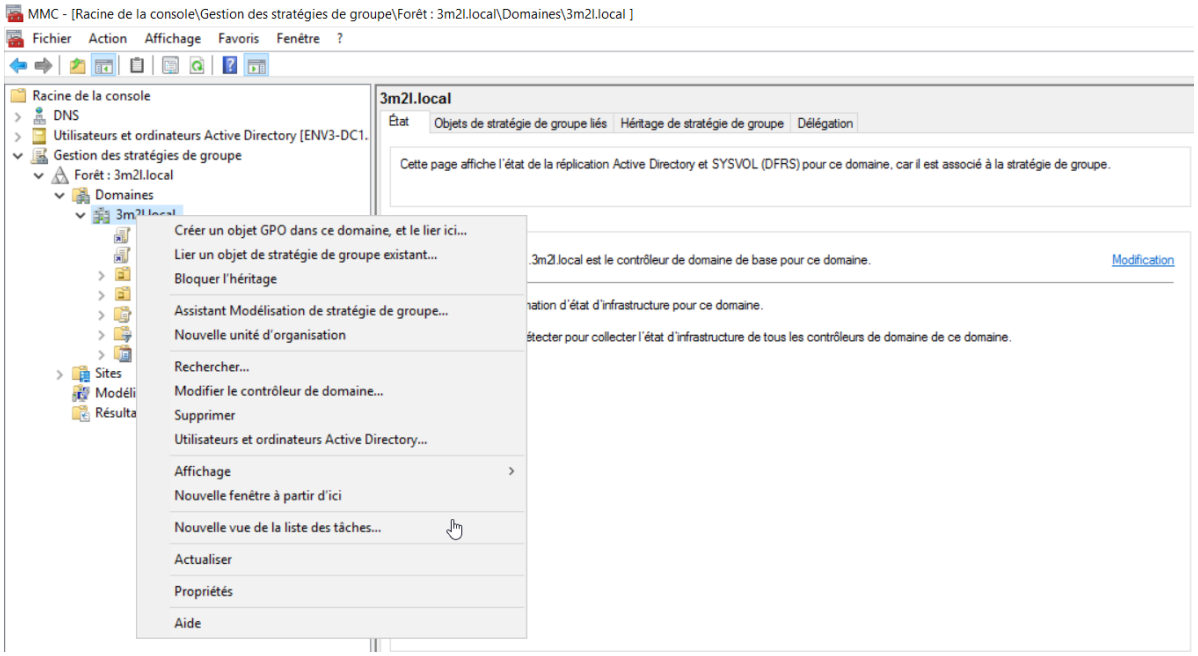


Stratégies de groupes (GPO) :

Afin de mettre en place des GPOS, il faut commencer par créer nos UO (Unité d'Organisation) sur lesquelles va s'appuyer la GPO. / !\ une GPO fait autorité sur une UO et non un groupe.

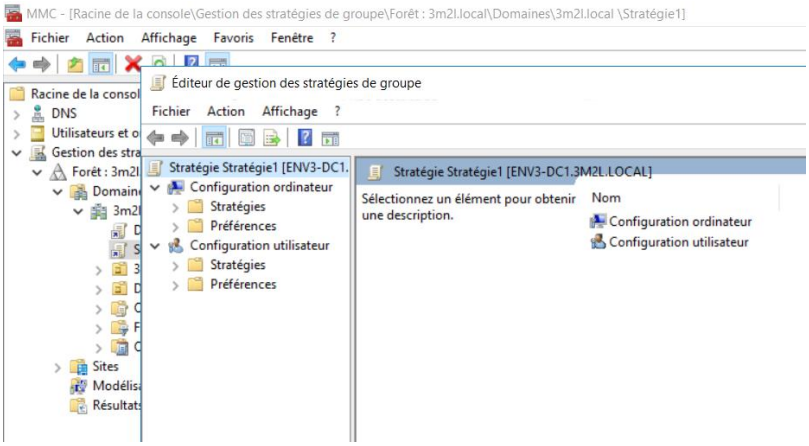


Une fois nos Unités d'organisations créées, nous devons créer notre GPO.



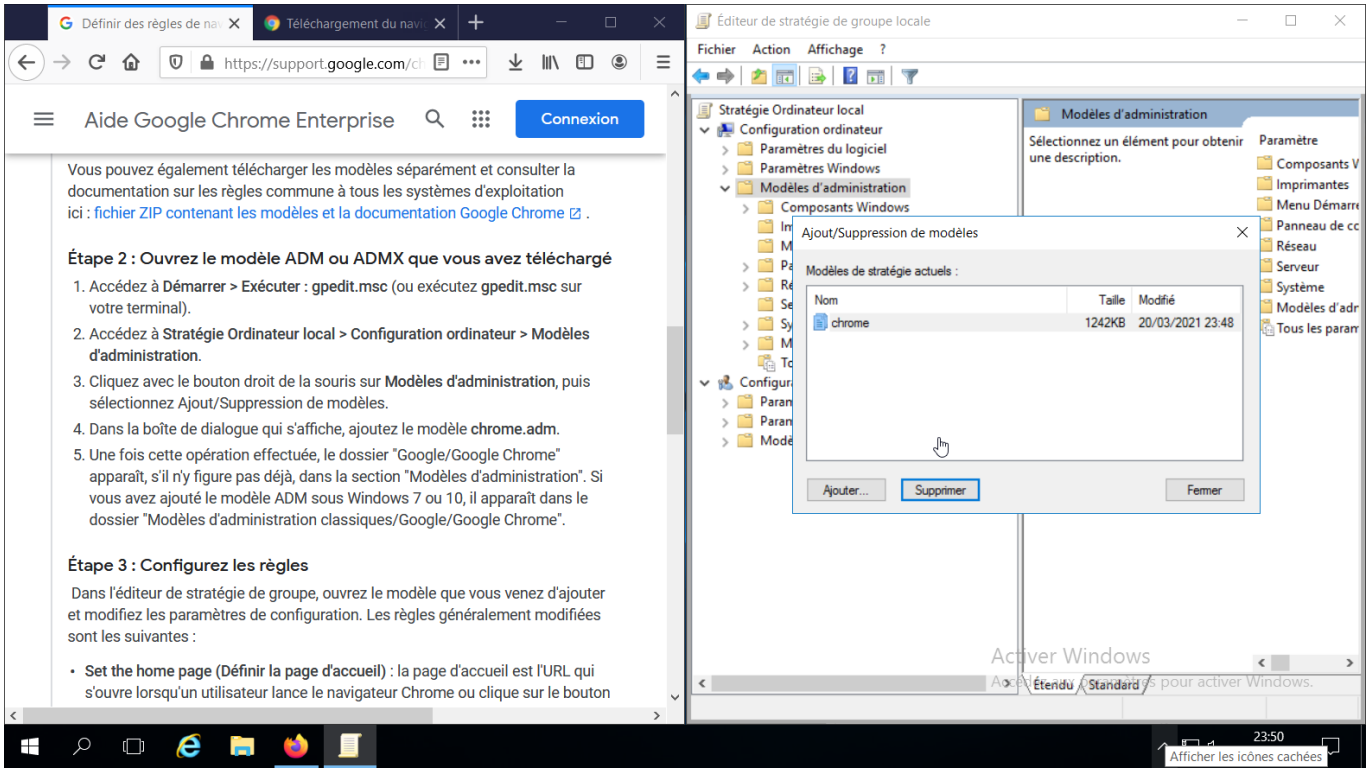
Il existe 2 types de GPO :

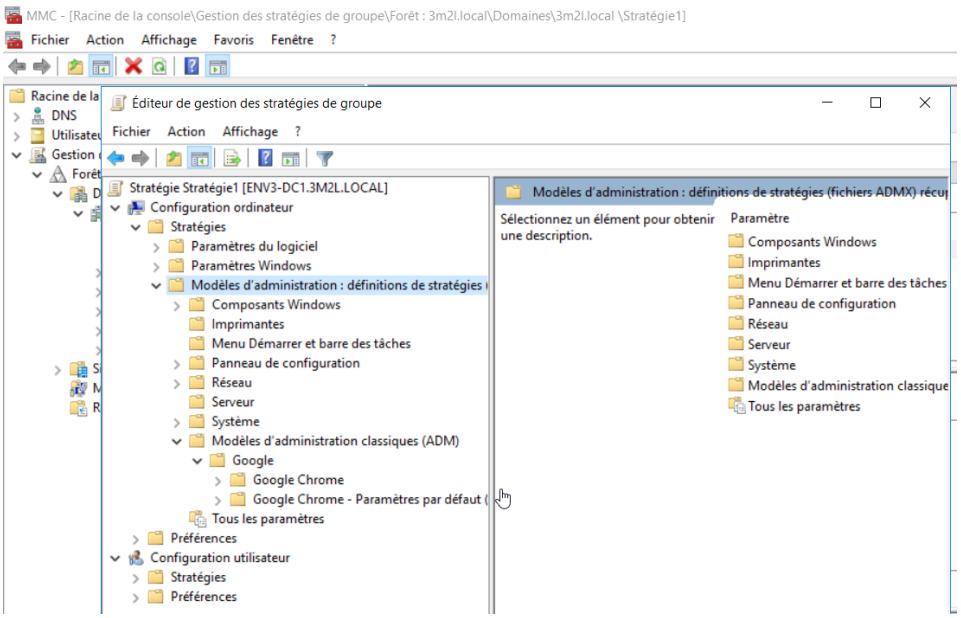
- Les stratégies d'ordinateurs : Se portent sur l'ordinateur peu importe l'utilisateur.
- Les stratégies d'utilisateurs : Se portent sur l'utilisateur peu importe l'ordinateur du domaine utilisé.
- On peut également voir des stratégies qui se portent sur les 2 objets présentés juste avant mais souvent on essaye de les dissocier au maximum



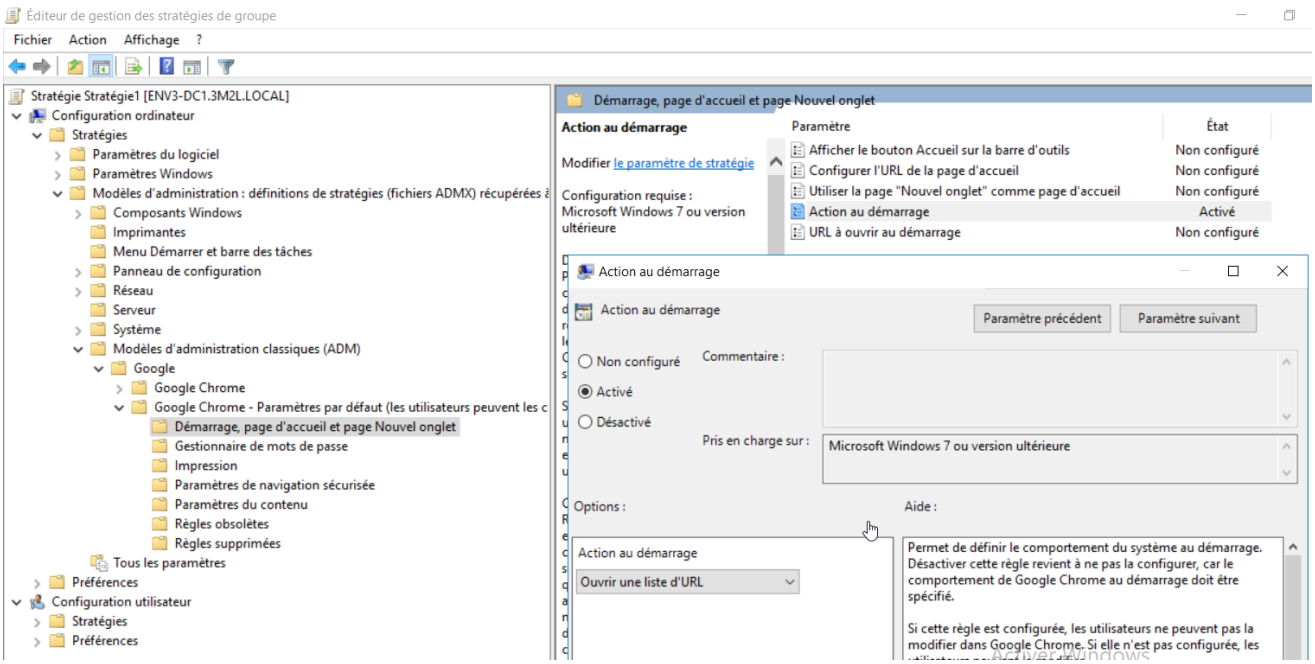
Pour notre part on va mettre en place une GPO consistant à charger des pages définies sur chrome au chargement de l'application. Pour cela il faut d'abord télécharger les modèles ADM ou ADMX qui permettent de définir les règles de Chrome. Une fois ajouté le modèle dans « ajouter ou supprimer un modèle », on peut retrouver les stratégies liées à chrome et les mettre en place.

https://support.google.com/chrome/a/answer/187202?hl=fr#zippy=%2Cwindows

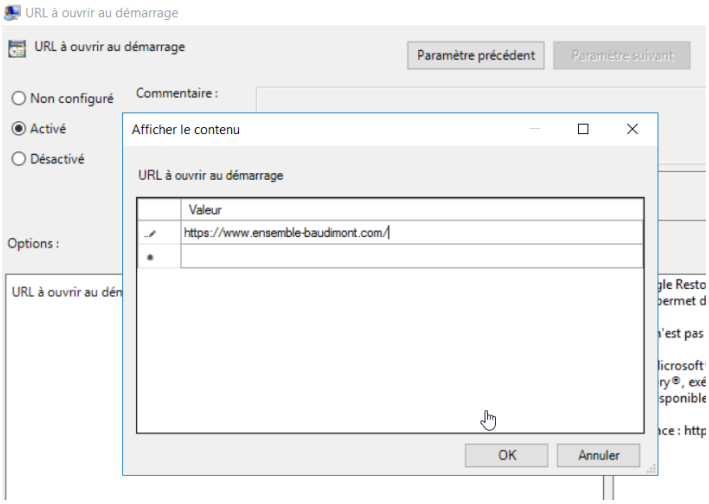




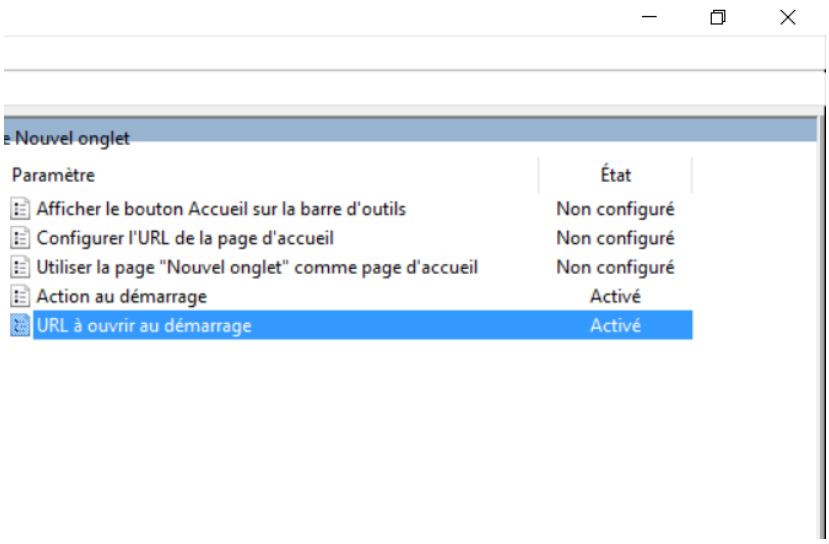
Pour notre stratégie nous allons activer les « actions au démarrage » et les « URL à ouvrir au démarrage ».



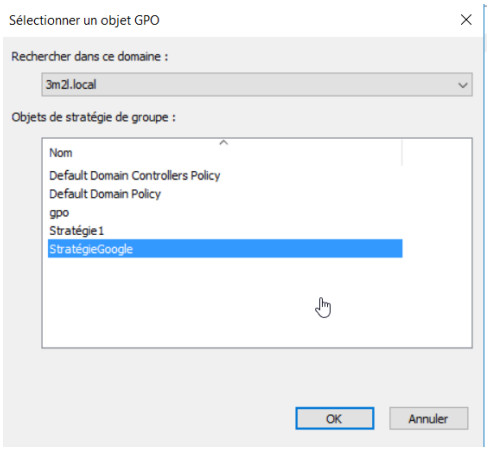
On peut renseigner autant de pages à charger au démarrage que l'on veut. Dans notre exemple nous allons juste définir de charger la page de Baudimont.

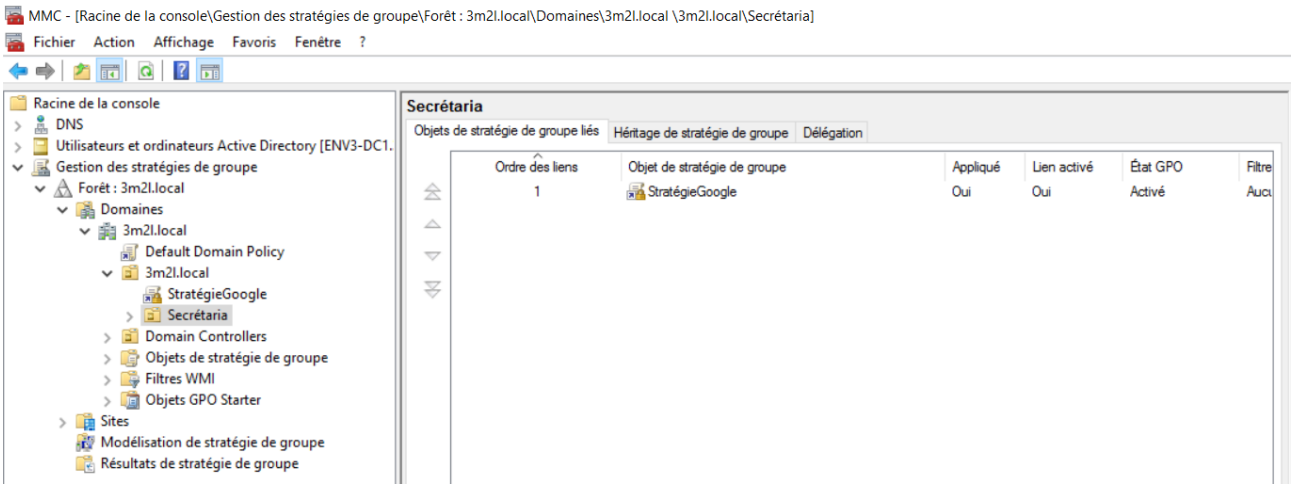


On peut voir ici l'état des stratégies afin de vérifier si les bonnes stratégies sont activées. Il en existe une infinité notamment avec google et autres applications. De ce fait il faut faire très attention avec les GPO que nous voulons mettre en place. Pour une compréhension plus simple et pour éviter toutes confusions il faut essayer de structurer au mieux notre plan de stratégie.



Une fois notre stratégie configurée, nous devons la lier à l'objet sur lequel nous voulons faire autorité. Dans notre cas nous allons choisir notre UO qui contient notre domaine afin d'appliquer cette stratégie de pages qui se lancent à l'ouverture de chrome à l'ensemble des users du domaine.

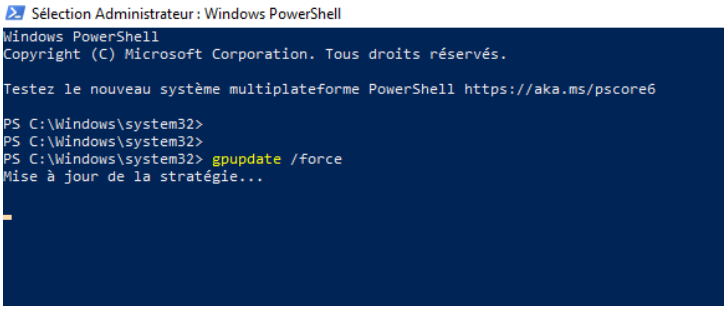




III] Tests

D'après le paramétrage par défaut, l'actualisation des GPO se fait toutes les 15 minutes. On peut choisir de changer cette variable afin d'éviter que tout le monde sur le réseau fasse la mise à jour en même temps. Dans ce cas nous pouvons forcer la mise à jour des GPO depuis le client pour éviter d'attendre ce laps de temps.

On utilise donc la commande « gpupdate/force » sur l'invite de commande powershell en mode administrateur. Ou encore « gpedit/force »



Aussi, pour que nos GPO puissent se charger correctement nous devons vérifier que les dates et heures soient coordonnées.