LAPS

Introduction :

Dans ce TP, nous allons aborder la solution LAPS au sein du contexte. Une installation complète suivie d'un test de fonctionnement d'un utilisateur ayant un mot de passe généré par l'Active-Directory.

Qu'est-ce que LAPS :

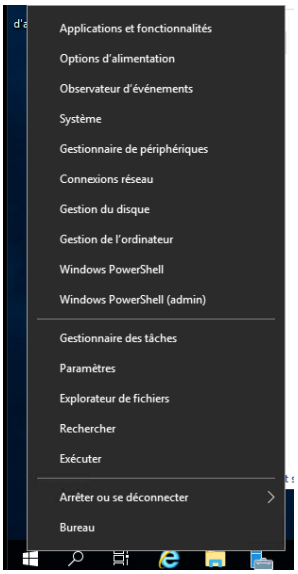
La solution LAPS permet de gérer les mots de passe aléatoires en mettant directement à jour les mots de passe de façon régulière directement dans Active Directory.

Prérequis :

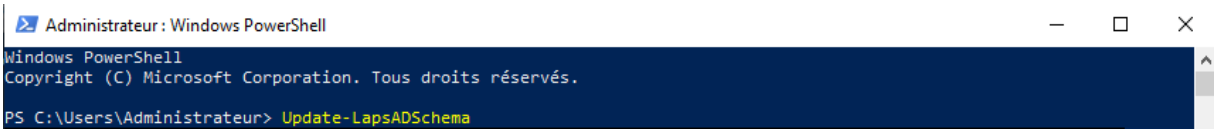
- PowerShell
- Active Directory (Windows Server 2003 ou une version supérieure)
- Stratégie de groupe

Installation de LAPS :

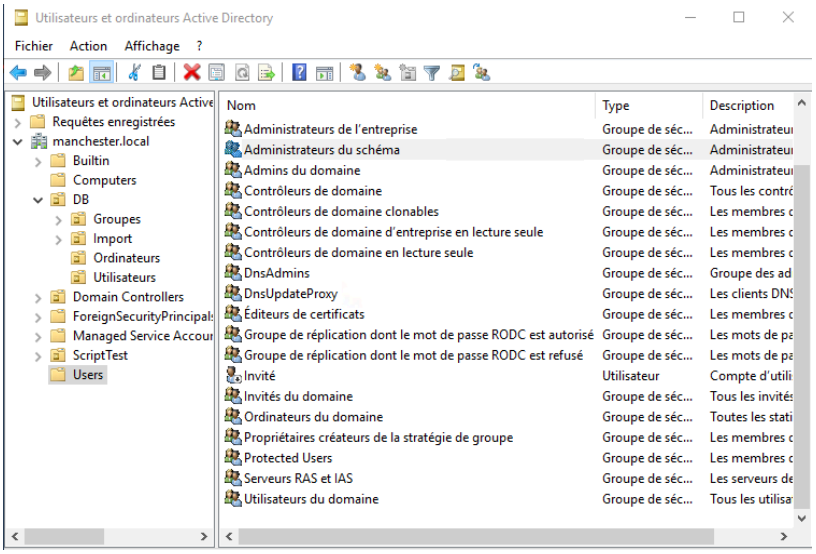
Cliquer sur Windows Powershell (admin)



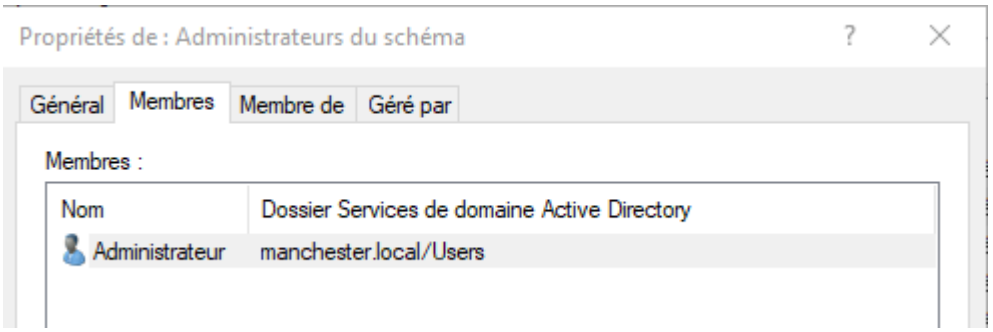
Taper : « Update-LapsADSchema »



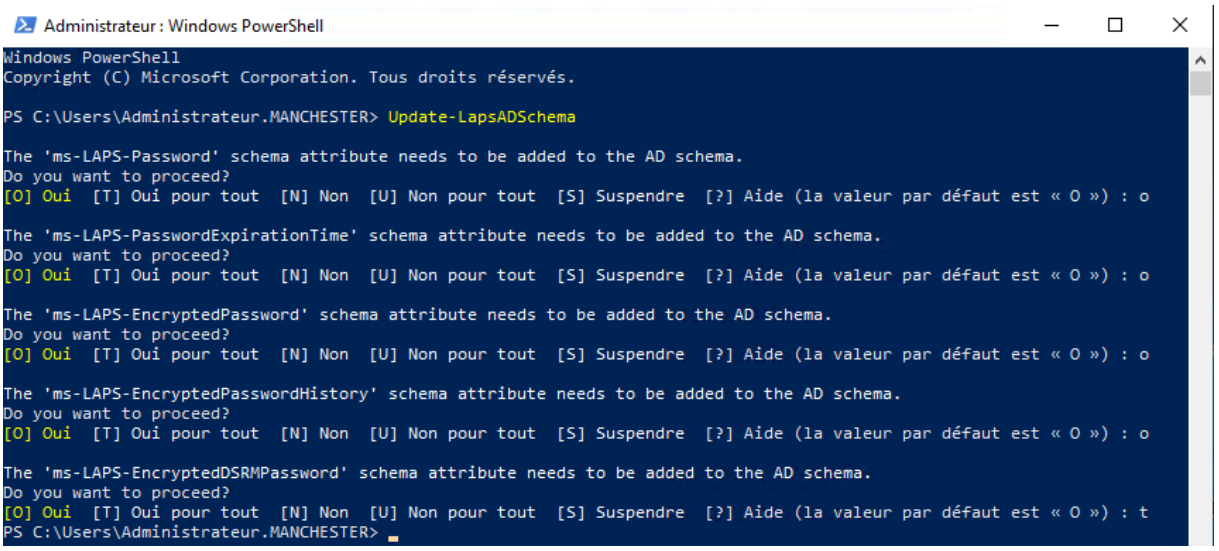
La commande est vite bloquée donc aller dans « Users » puis « Administrateur du schéma »



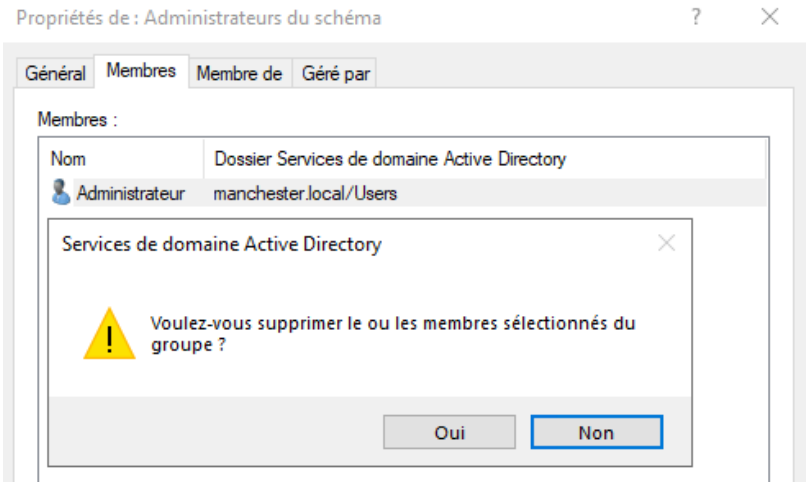
Mettre « Administrateur » dans l'onglet « Membres » et fermer et rouvrir la session.



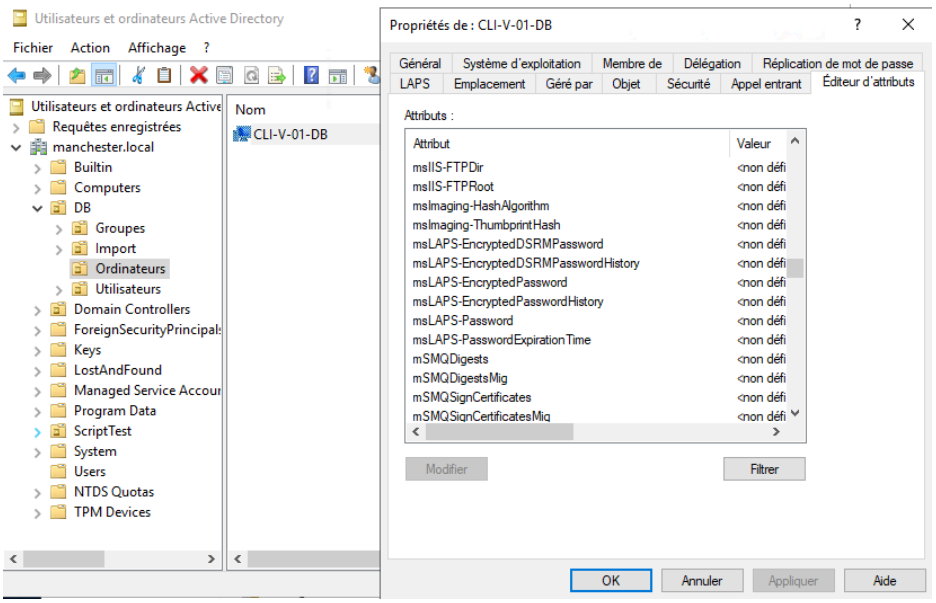
Puis retaper la commande, ensuite il faut dire 4 fois « o » et ensuite un « t »



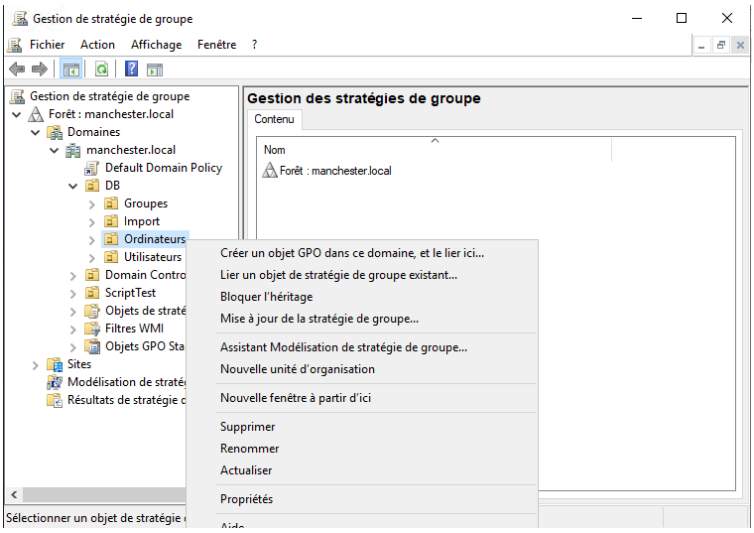
Puis enlever le membre « Administrateur » :



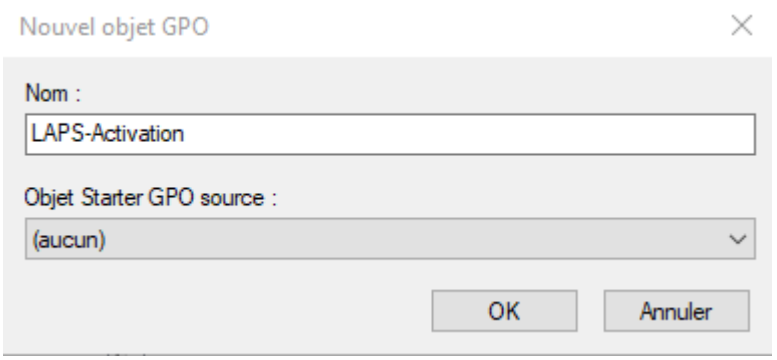
On retrouve bien les attributs LAPS dans les propriétés de l'ordinateur :



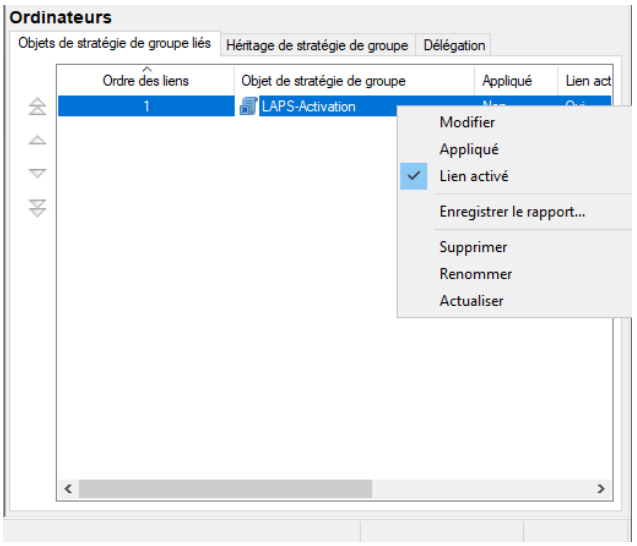
Créer une GPO dans le groupe ordinateur :



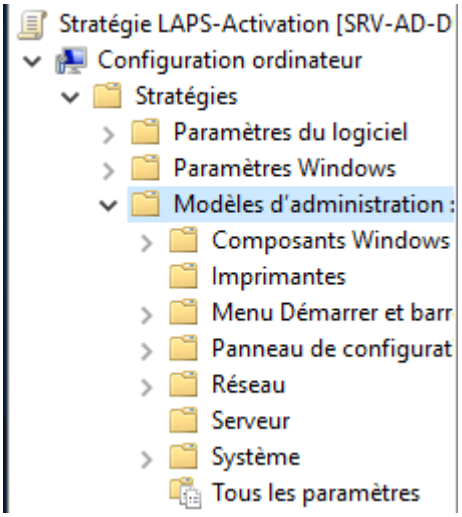
Le nommer :



Puis modifier :

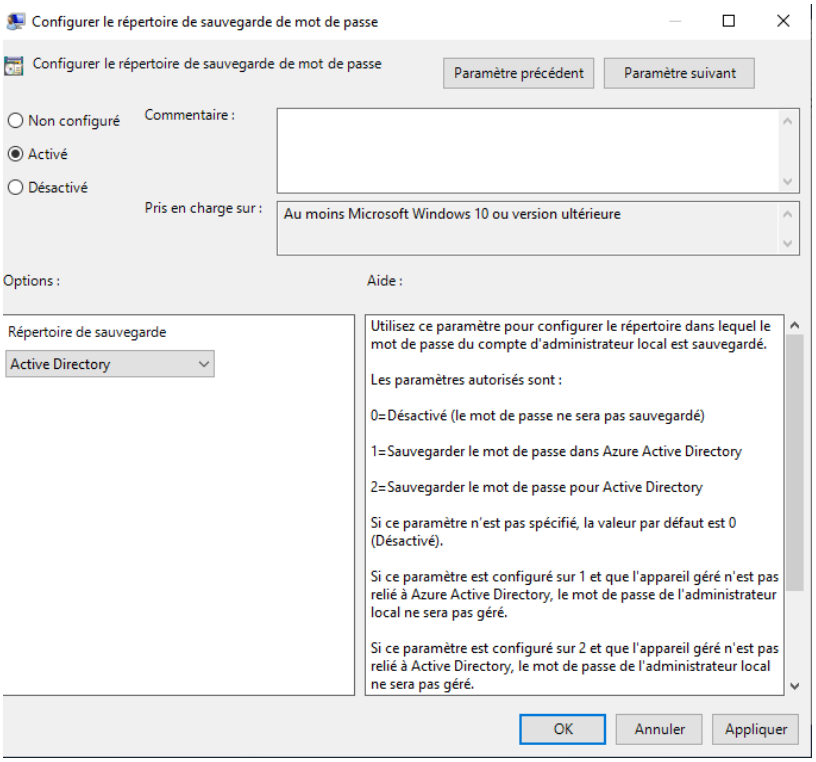


Aller dans « Configuration ordinateur », puis « Stratégies » ensuite « Modèles d'administration » puis dans « Système »

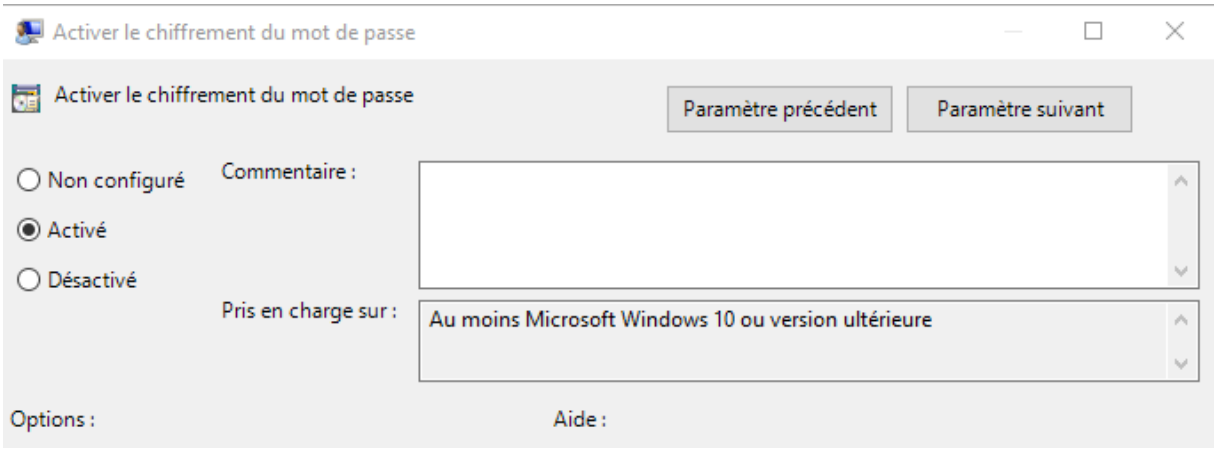


Puis cliquer dans la liste sur « LAPS » :

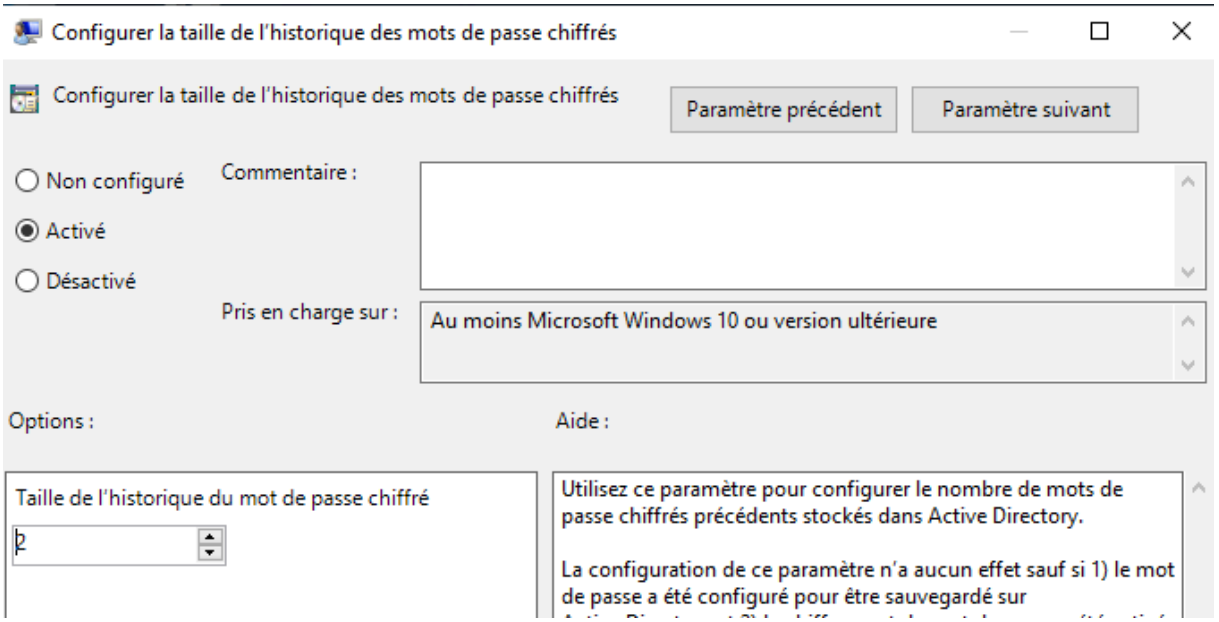
Pour l'activation de LAPS, veuillez-vous rendre dans « Configurer le répertoire de sauvegarde de mot de passe », cocher la case « Activé », puis bien indiquer dans le répertoire de sauvegarde « Active Directory » puis appliquer cela.



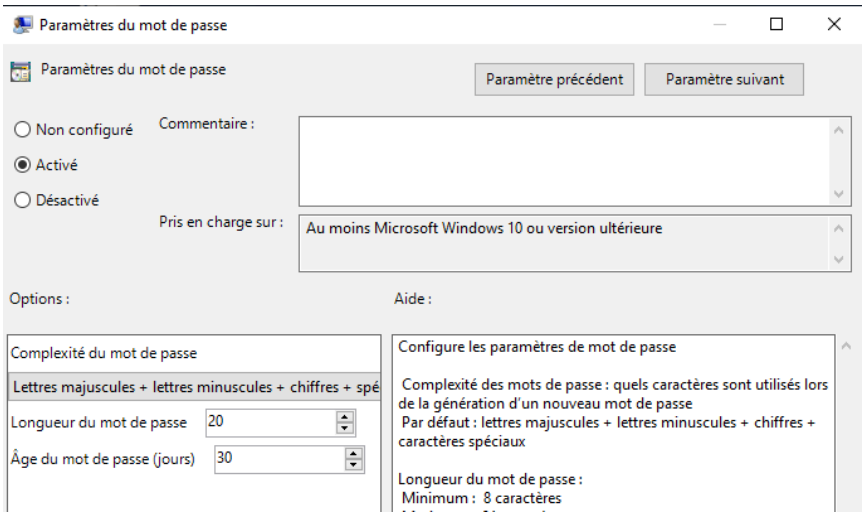
Dans « Activer le chiffrement de mot de passe », cocher la case pour l'activer :



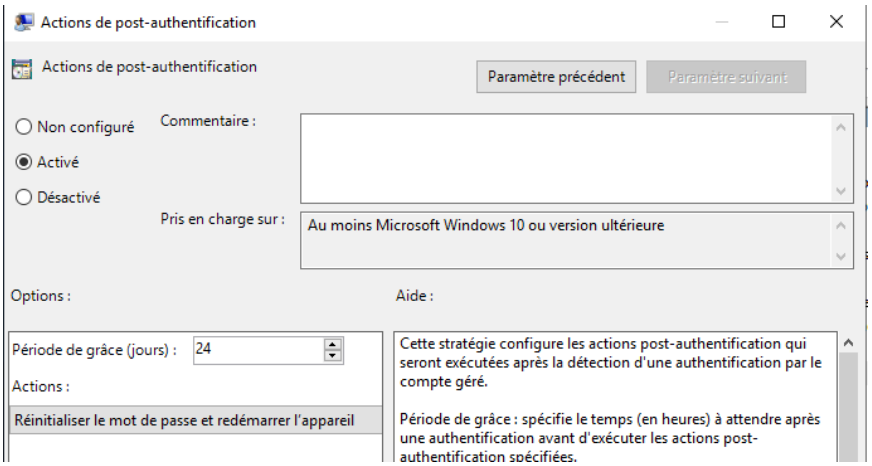
Puis dans « Configurer la taille de l'historique des mots de passe chiffrés », activer et mettre indiquer « 2 » dans la taille de l'historique du mot de passe chiffré :



Dans « Paramètres du mot de passe », activer et adapter la ligne « longueur du mot de passe » selon ses besoins et la complexité aussi :



Dans « Actions de post-authentification », activer et modifier selon ses besoins :



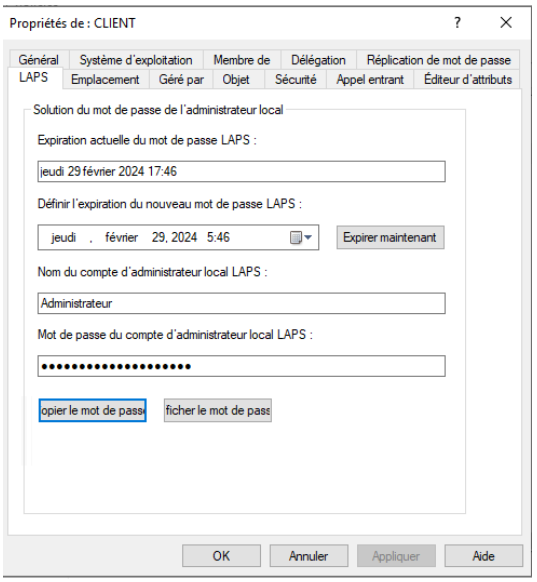
Pour donner les droits à l'utilisateur de communiquer son mot de passe à Active Directory, il faut se rendre sur Powershell et taper cette commande :

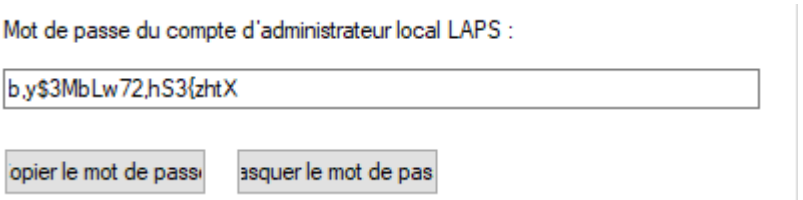
```
PS C:\Users\Administrateur.MANCHESTER> Set-LapsADComputerSelfPermission -Identity "OU=Ordinateurs,OU=DB,DC=manchester,DC=local"

Name        DistinguishedName
----        -----------------
Ordinateurs OU=Ordinateurs,OU=DB,DC=manchester,DC=local
```

Pour vérifier les autorisations il faut taper :

```
PS C:\Users\Administrateur.MANCHESTER> Find-LapsADExtendedRights -Identity "OU=Ordinateurs,OU=DB,DC=manchester,DC=local"

ObjectDN                                    ExtendedRightHolders
--------                                    --------------------
OU=Ordinateurs,OU=DB,DC=manchester,DC=local {AUTORITE NT\Système, MANCHESTER\Admins du domaine}
```

On voit bien que les seuls autorisés sont les Admins du domaine et le Système.





Conclusion :

En définitive, la solution LAPS est un bon moyen pour générer des mots de passe robustes automatiquement ce qui permet de sécuriser les comptes à privilège et donc de protéger les données. C'est une solution assez facile à mettre en place et très utile.