L A P S

MARGAUX TANET
BTS 2 SIO

Introduction:

Nous allons installer la fonctionnalité windows LAPS sur un réseau.
Laps (Local Administrator Password Solution) permet de faire la gestion des mots de passe administrateurs locaux de nos postes clients/administrateur. Cela permet de centraliser et ainsi de sécuriser les mots de passe utilisés pour les administrateurs locaux des membres du domaine.

Pré requis:

- windows server 2019 mise à jour
- poste client mise à jour
- procédé à une sauvegarde avant

1) Préparer le schéma

Le schéma correspond aux attributs que l'on peut utiliser. Les attributs sont les paramètres par objet. On peut leur donner une valeur. Cette manipulation va permettre de rajouter des attributs dédiés à LAPS.

Mise à jour de schéma:

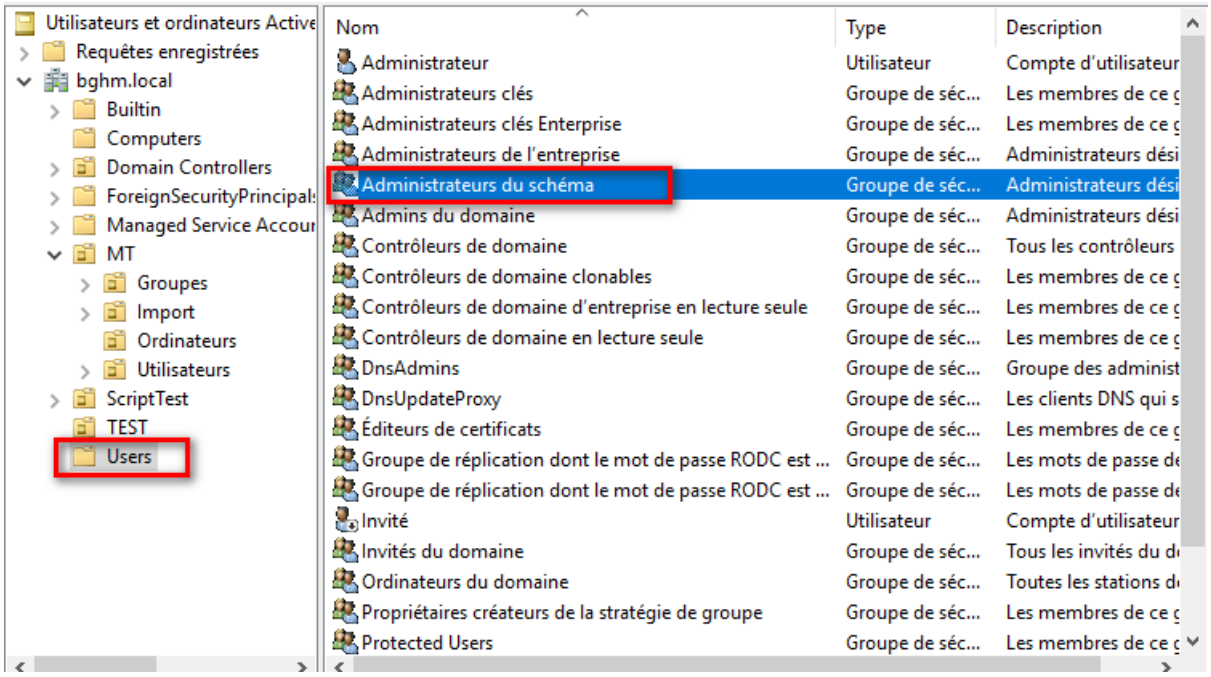
Lancer le powershell en Administrateur:
Taper la commande: update-lapsADSchema

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> update-LapsADSchema

The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») :
```

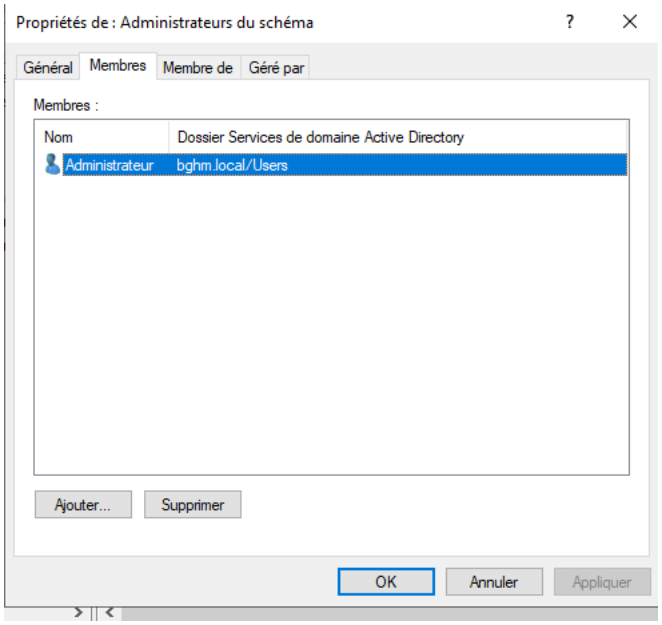
Nous remarquons que nous n'avons pas les droits. C'est normal car on ne laisse pas tout le temps la possibilité aux administrateurs de modifier le schéma.

```
The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o
AVERTISSEMENT : Add request for 'CN=ms-LAPS-Password,CN=Schema,CN=Configuration,DC=bghm,DC=local' threw exception:
AVERTISSEMENT : System.DirectoryServices.Protocols.DirectoryOperationException: Une erreur de fonctionnement s'est
produite.
   à System.DirectoryServices.Protocols.LdapConnection.ConstructResponse(Int32 messageId, LdapOperation operation,
ResultAll resultType, TimeSpan requestTimeOut, Boolean exceptionOnTimeOut)
   à System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request, TimeSpan requestTimeout)
   à Microsoft.Windows.LAPS.UpdateLapsADSchema.AddSchemaAttribute(String schemaAttributeDN, LAPSSchemaAttribute
lapsSchemaAttribute)
update-LapsADSchema : Une erreur de fonctionnement s'est produite.
Au caractère Ligne:1 : 1
+ update-LapsADSchema
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Update-LapsADSchema], DirectoryOperationException
    + FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,Microsoft.Windows.LAPS.Up
   dateLapsADSchema

PS C:\Users\Administrateur>
```

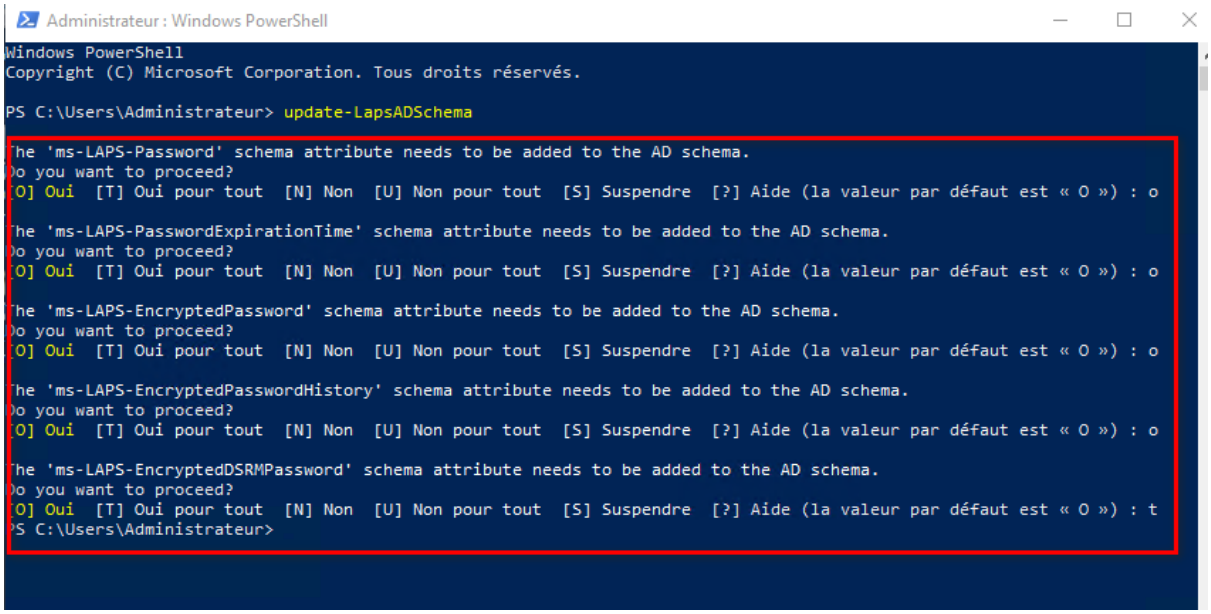
Il suffit de rajouter Administrateur dans le groupe des Administrateur du schéma.
Se rendre dans l'AD et dans Utilisateurs et sélectionnez Administrateurs du schéma:



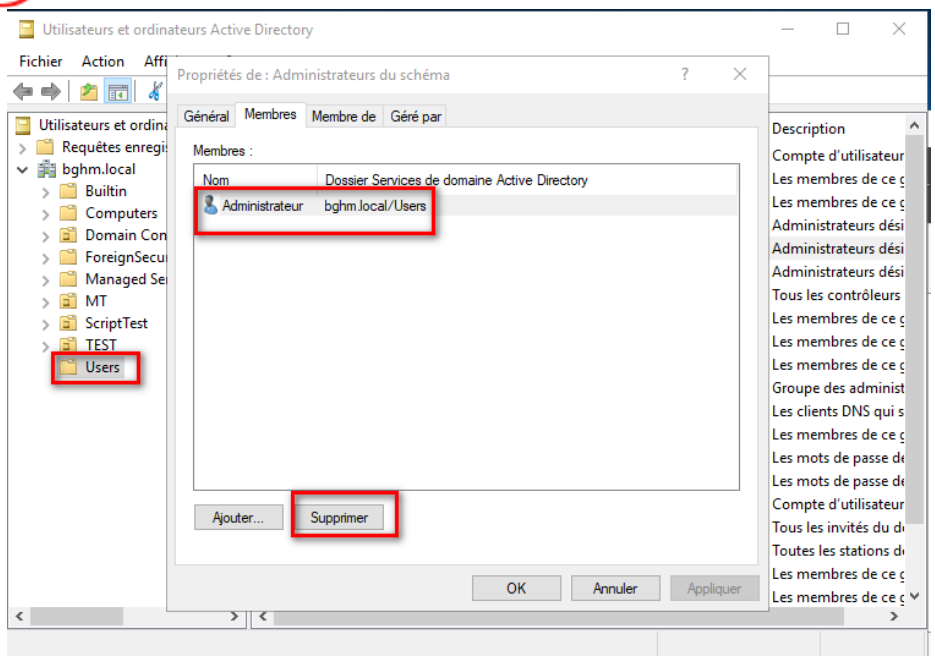
Se rendre dans l'onglet "Membre" et ajouter votre Administrateur:



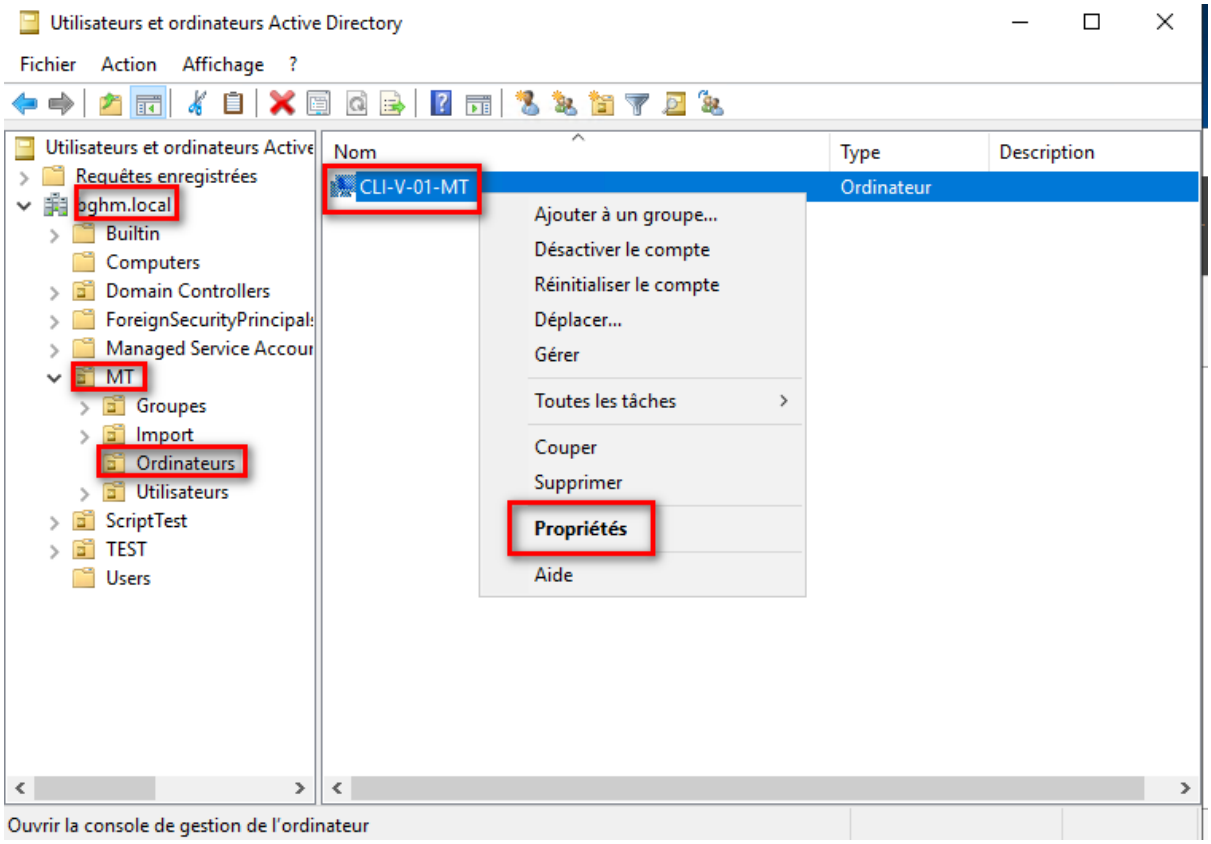
Pour pouvoir prendre en compte la modification il faut fermer puis rouvrir la session. Rouvrir l'invite de commande powershell et refaire la même commande qu'au début. Et cette fois-ci aucune erreur est ressortie:



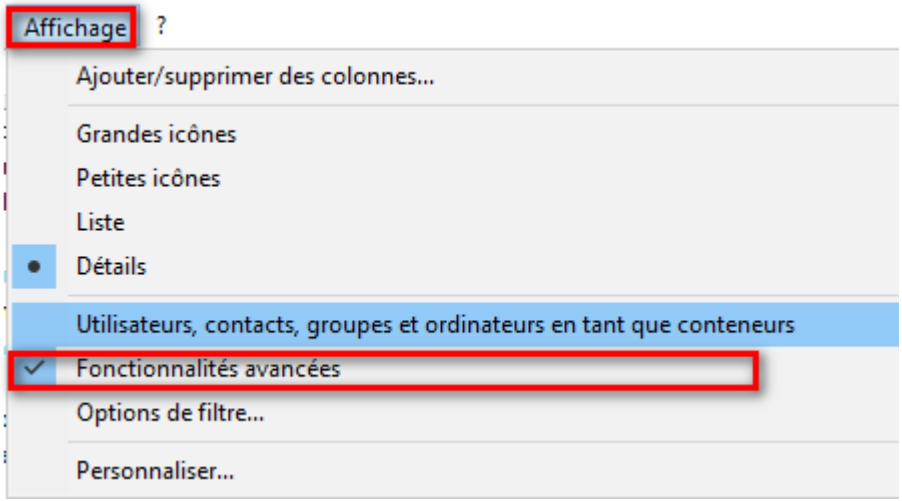
Ne pas oublier d'aller retirer à nouveau votre administrateur des membres d'administrateur du schéma:



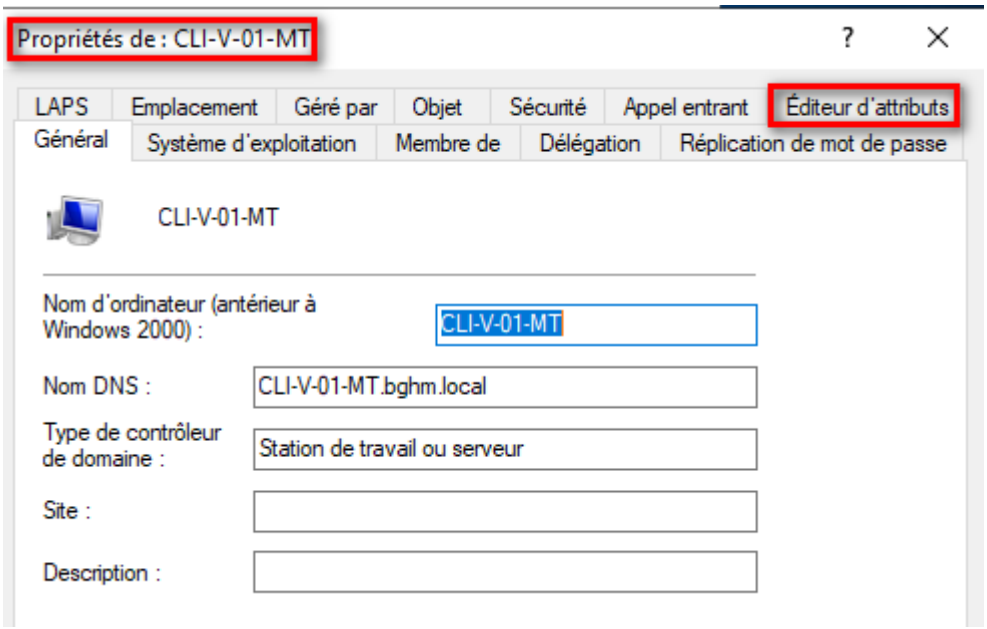
Vérifier que la mise à jour du schéma a bien été faite en allant vérifier un objet active directory:
Pour cela se rendre dans l'OU "ordinateur" sous l'AD. Clic droit sur notre PC client puis propriété:



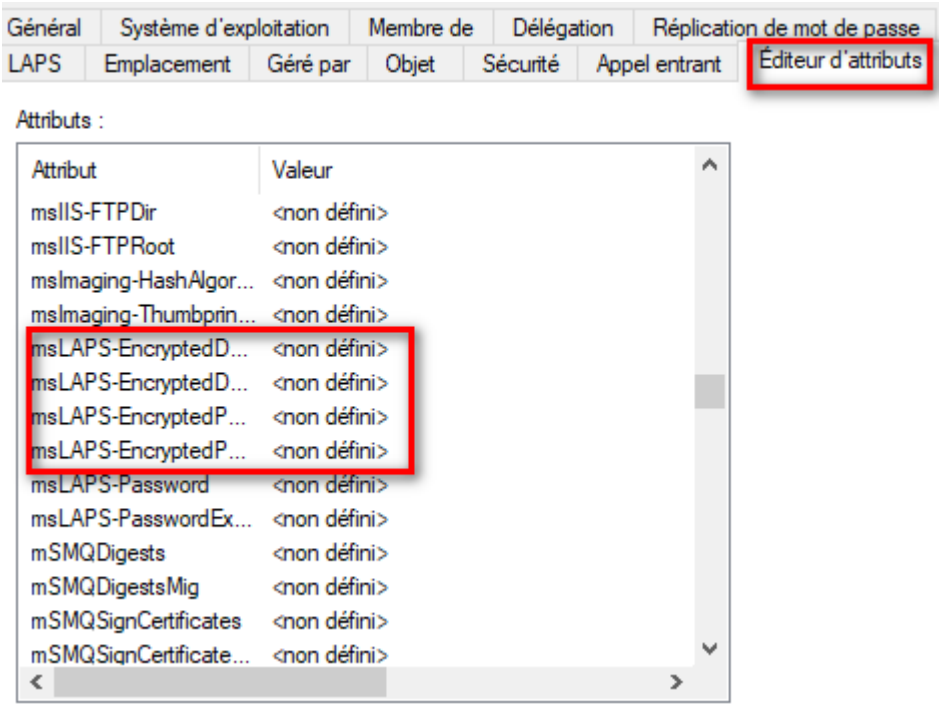
Juste avant, sur certains ordinateurs l'onglet "éditeurs d'attributs" n'apparaît pas. Pour cela, dans "Affichage" sélectionner "fonctionnalités avancées" pour que cet onglet apparaît.



Se rendre dans l'onglet "éditeur d'attributs":



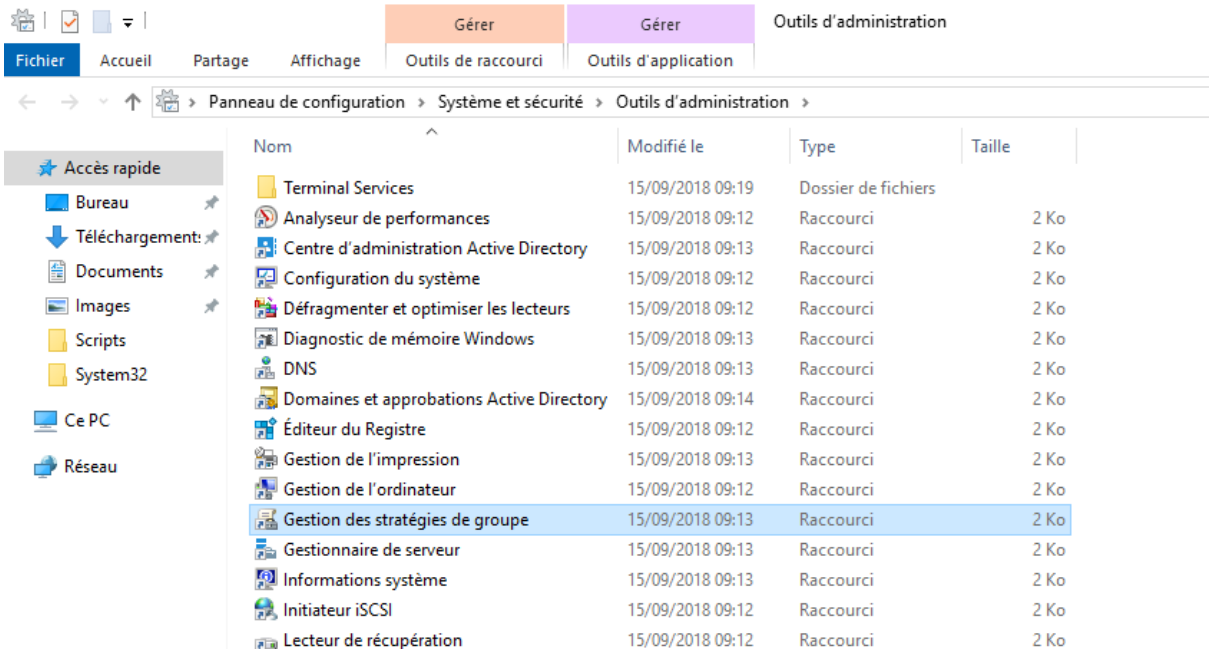
Je retrouve bien les attributs msLaps:



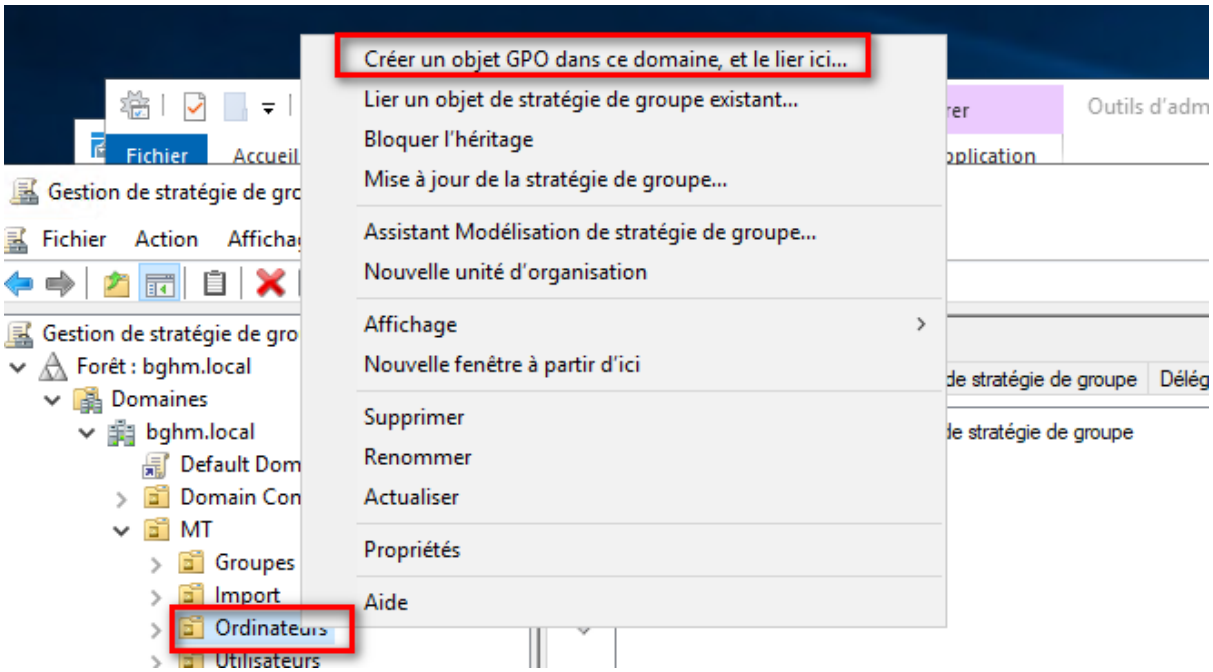
Cela permet de stocker les mots de passe chiffrer, l'historique de mot de passe, le mot de passe si on ne souhaite pas le chiffrer et le temps ou le mot de passe est valide.

2) Paramétrage de la stratégie de groupe LAPS

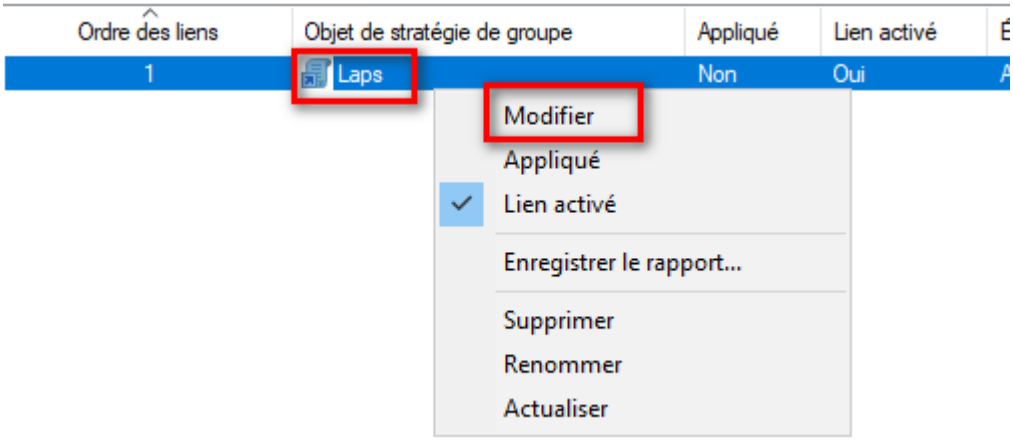
Administrer LAPS c'est donner les paramètres qu'on veut appliquer pour le cas, cela va se faire par stratégies. Se rendre dans "gestion de stratégies de groupes":



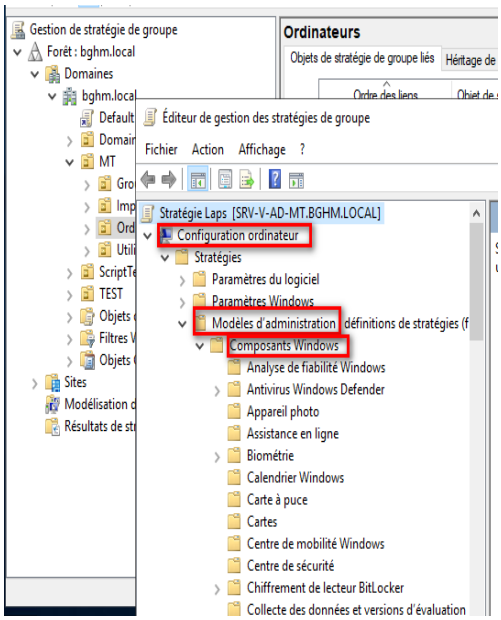
On veut appliquer LAPS sur notre unité d'organisation d'ordinateurs .Pour se faire , on va créer une GPO. Se rendre dans l'AD, se mettre sur l'OU "ordinateurs", clic droit "créer un objet GPO:

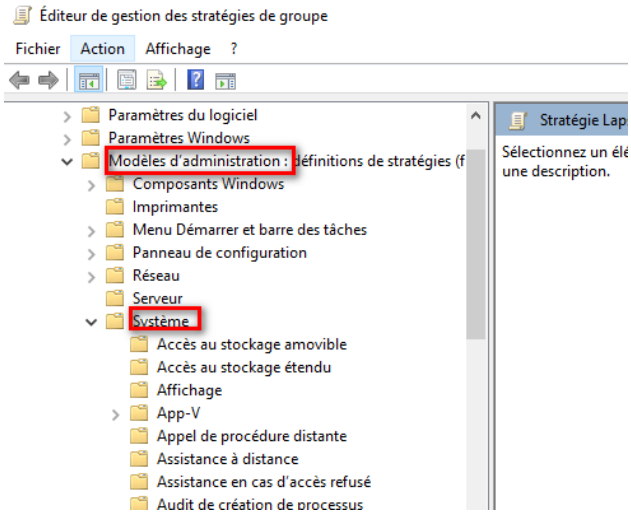


Pour modifier la stratégie, clic droit “modifier”:

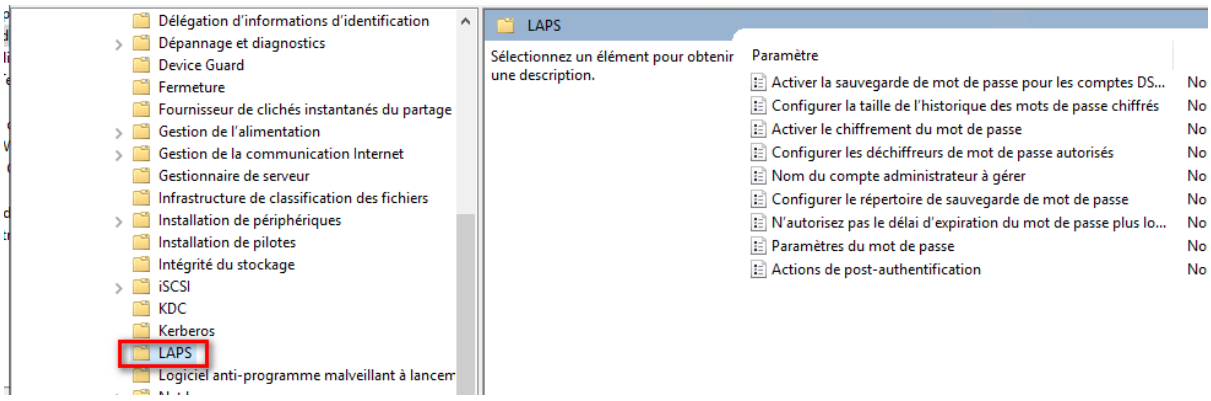


Puis se rendre dans “configuration ordinateur” > “modèles d’administrateur” > “Système”



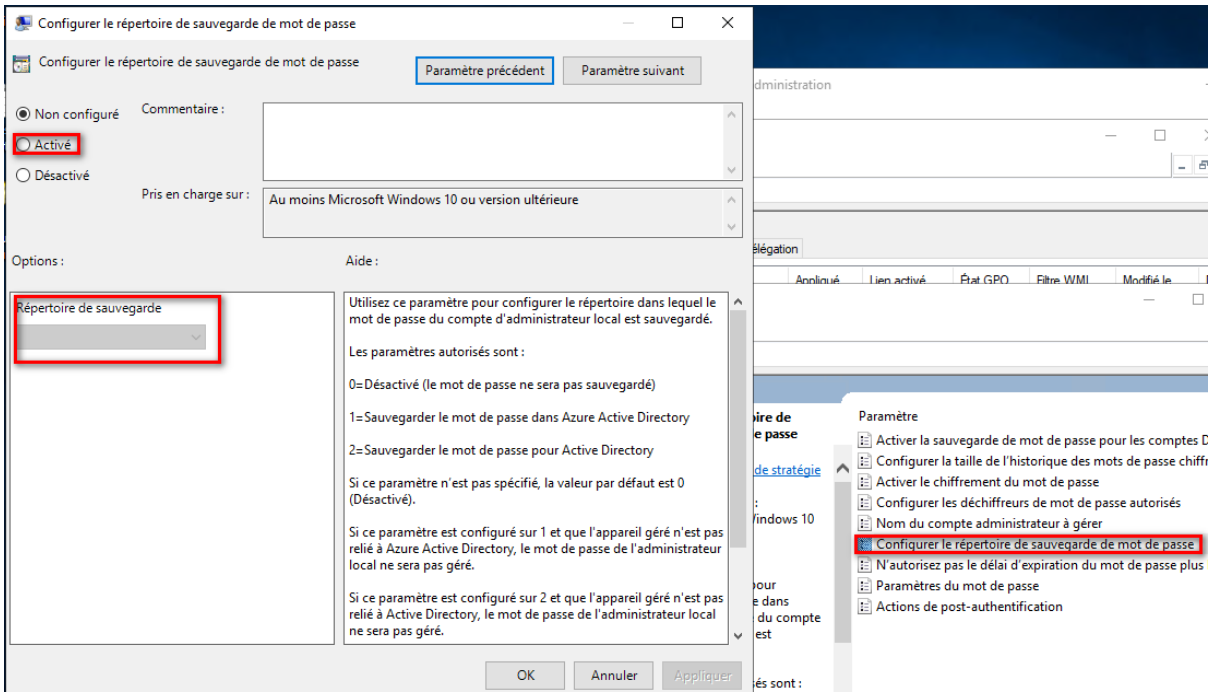


On retrouve dans cette liste “LAPS”:



Nous allons activer LAPS en configurant le répertoire de sauvegarde de mot de passe LAPS tant qu'on active pas cela, nous n'activons pas LAPS car il est installé mais pas utilisé.

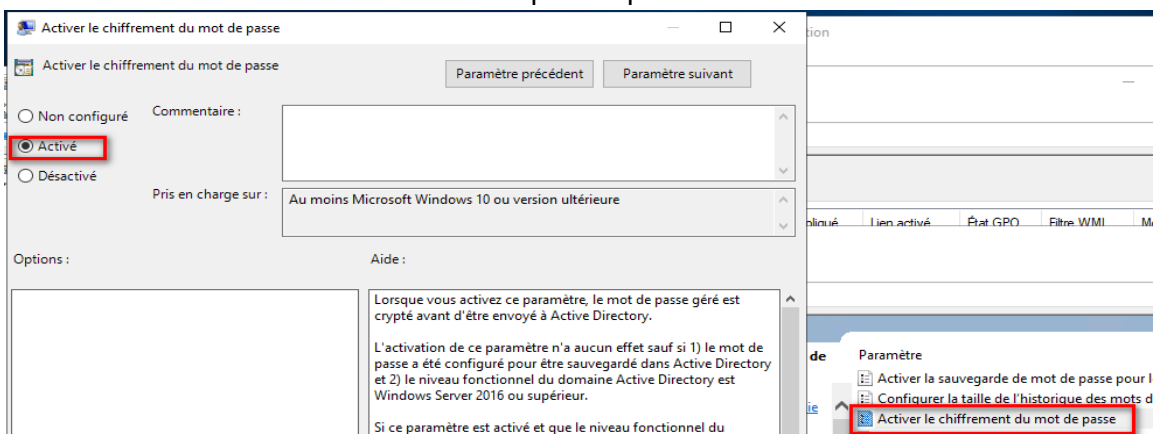
Pour ce faire, clique droit "configurer le répertoire de sauvegarde de mot de passe" et cliquer sur "activer" et sélectionner comme répertoire de sauvegarde "active directory" comme nous sommes en local.



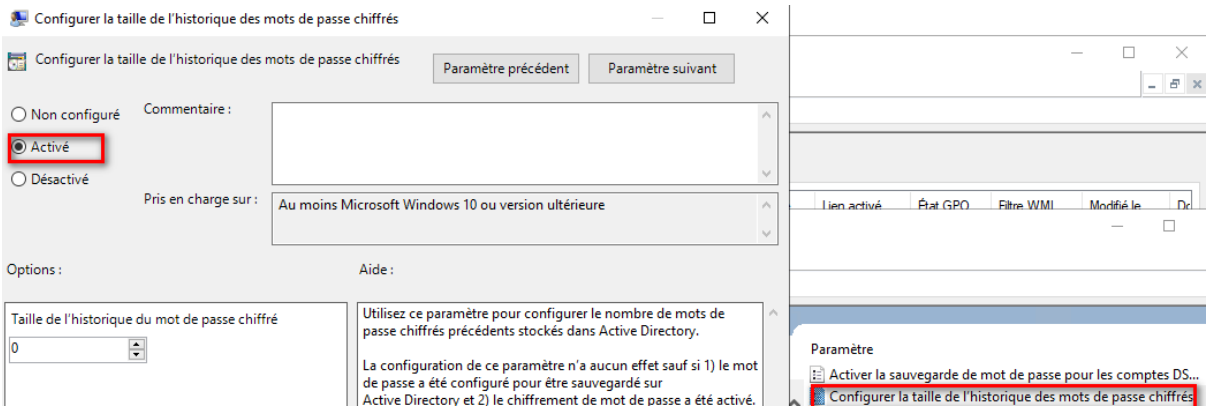
Grâce à cela tous les ordinateurs membres de l'unité d'organisation "ordinateurs" pourront stocker leur mot de passe administrateur locaux dans l'AD. Nous avons activé LAPS.

Dans un deuxième temps, nous allons décider de quel administrateur et de qui on veut gérer. Par défaut si on n'active pas cette stratégie, le compte administrateur en local c'est le compte administrateur.

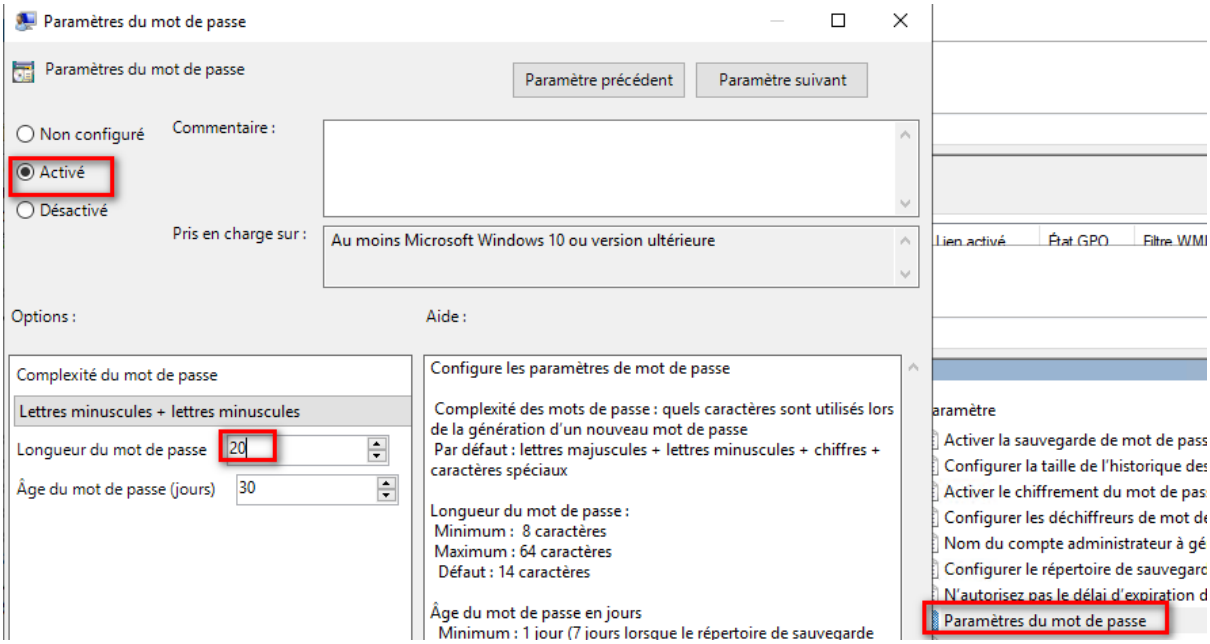
On va chiffrer le mot de passe. Par défaut, il n'est pas chiffré il est en clair:
Choisir "activer le chiffrement du mot de passe" puis "activé":



Cliquer “configurer la taille de l’historique des mots de passes chiffrés” et activé et mettre “2” en taille:



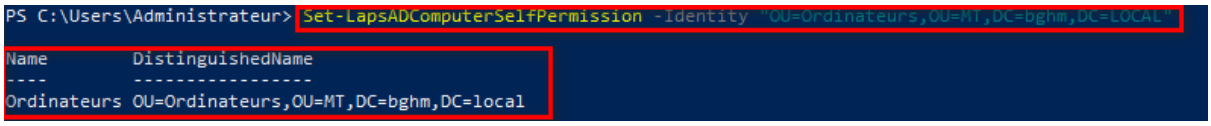
Cliquer sur “paramètres du mot de passe” puis “activer” et mettre en longueur du mot de passe “20”.



3) Modification des droits d'accès à l'OU ordinateurs pour LAPS

Il faut donc que le pc client ait le droit d'écrire sur *msLAPS* par défaut il n'a pas le droit. On va lui donner les droits et donc de pouvoir les communiquer à Active Directory.

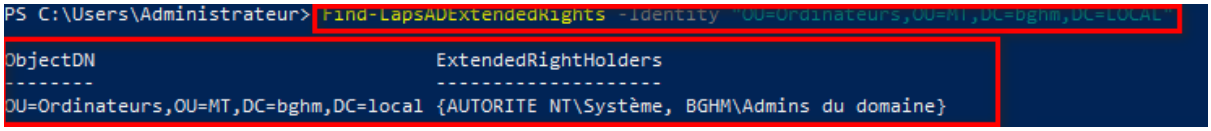
Ouvrir une invite de commande Powershell en admin, taper la commande "***Set -LapsADComputerSelfPermission"***. Cela donne à l'ordinateur de modifier les droits lui même ses attributs LAPS. Et indiquer l'OU dans laquelle se faire en ajoutant ***"- Identity OU=Ordinateurs, OU=MT, DC=bghm, DC=local".***



Les droits ont bien été modifiés.

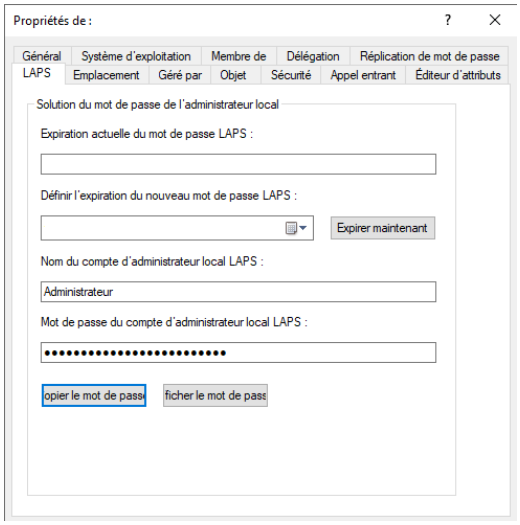
Conseil : Bien vérifier qu'il n'y a pas de droits complémentaires en amont sur l'OU: commande: "find-LapsADExtendedRights "***- Identity OU=Ordinateurs, OU=MT, DC=bghm, DC=local"***

Nous pouvons regarder que le laps a bien été activé sur notre poste client:



Se rendre sur le poste client et faire la mise à jour de la stratégie en faisant "*gpupdate /force*".

En se rendant sur les propriétés puis dans l'onglet éditeurs d'attributs, il est renseigné le mot de passe LAPS pour le compte Administrateur.



Conclusion :

On a donc paramétré LPAS sur notre serveur AD en mettant à jour le schéma, on a paramétré les stratégies de groupes. Nous avons défini comment on voulait chiffrer le mot de passe et la complexité du mot de passe. Nous avons mis les droits de modifications du mot de passe LAPS sur l'OU ordinateurs. Enfin nous avons pu se rendre compte que cela fonctionnait bien.