n Guastamacchia
Livio
SIO2

TP Sécurité :

10/12/2024

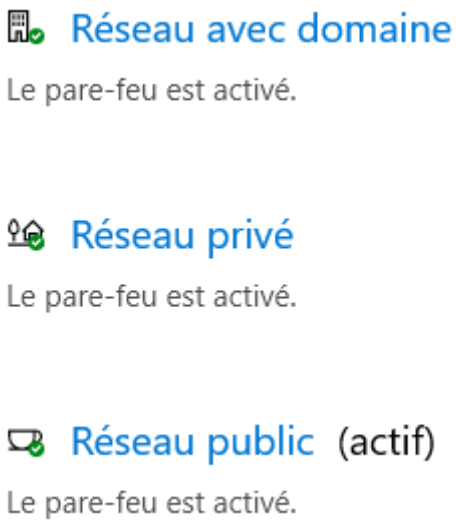
Durcissement Serveur :

Introduction :

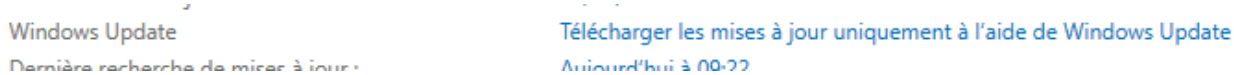
Lors de ce TP nous allons effectuer quelque paramètre de base afin de sécurisé nos serveur.

TP :

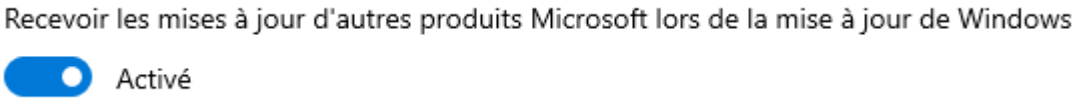
La première étape de sécurité de ce TP sera d'activé le pare-feu Windows



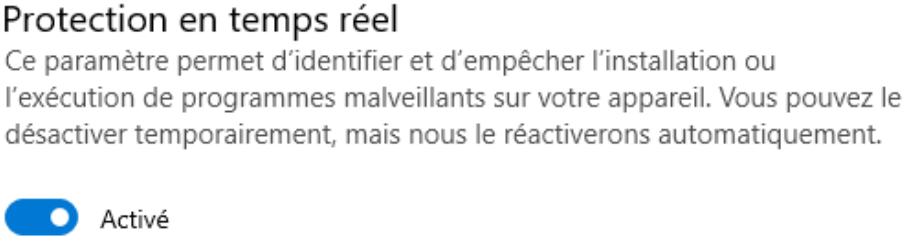
Ensuite nous allons faire en sorte que notre serveur soit a jour dans Windows update



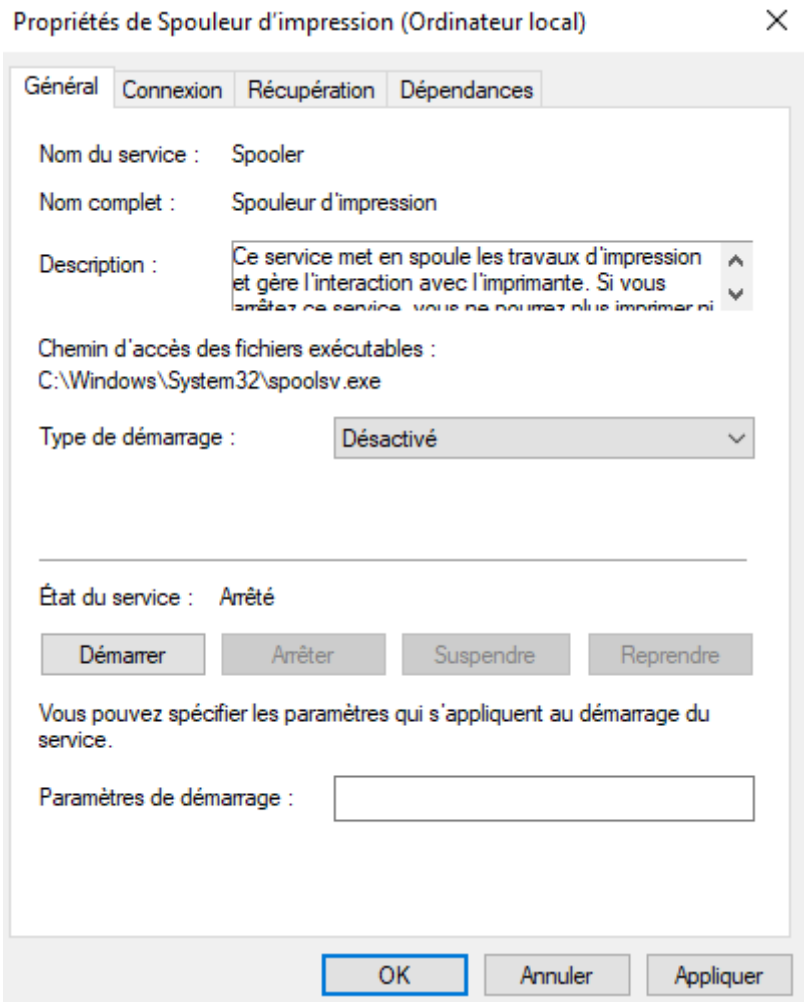
Et nous activerons aussi dans les paramètre avancer, le fait de recevoir les mises a jours des produits Microsoft qui permettra de tenir a jours tous les produits Microsoft sur notre serveur.



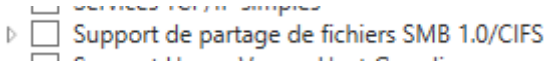
L'antivirus doit être aussi activé surtout la protection en temps réel qui montre bien que l'antivirus est actif



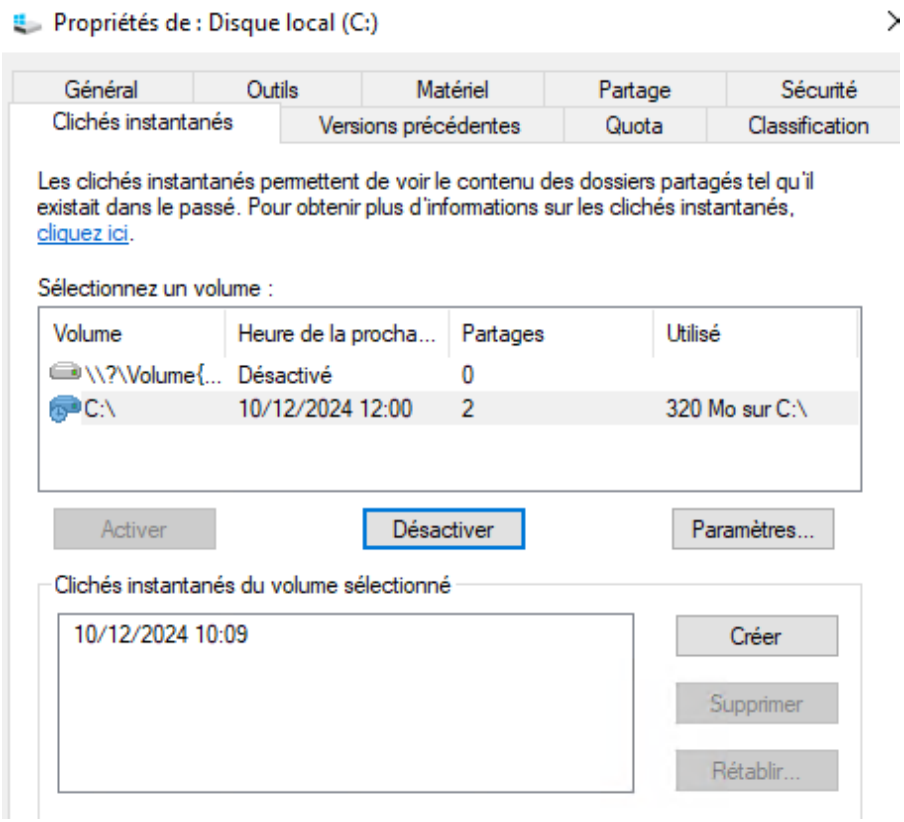
Dans les services nous pouvons arrêté le spouleur d'impression si notre serveur n'est pas un serveur d'impression afin d'évité les failles potentielles



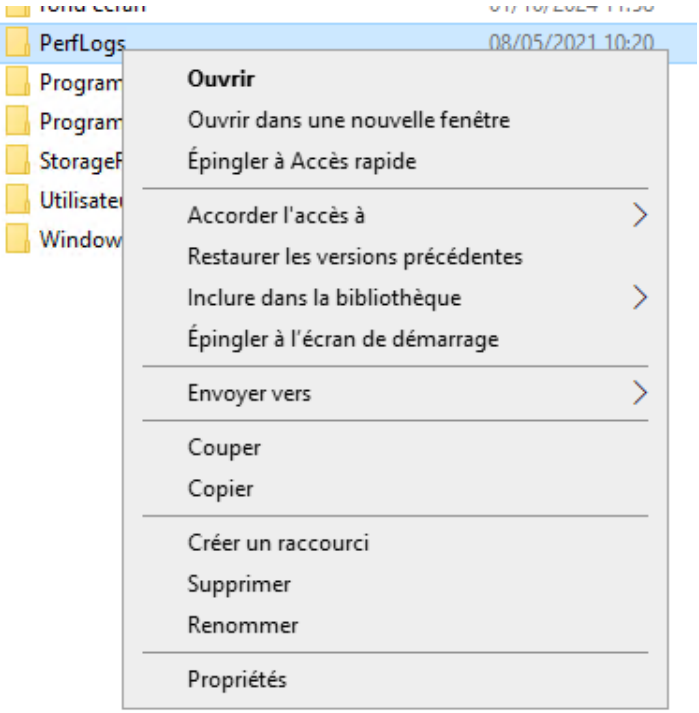
La vérification de la version du protocole SMB est important car il y a une version ancienne qui n'est plus utilisé « SMBv1 » alors si nous n'utilisons pas ce protocole, nous devons le désactiver et pour voir si il est installé par le biais de l'interface graphique. Nous allons faire ajouter un rôle et regarder dans les fonctionnalités si la case « support de partage de fichier SMB 1.0/CIFS » est cocher si elle ne l'est pas c'est qu'il n'est pas utilisé sur notre serveur. Dans l'autre cas ou elle est cocher, il est préconisé de désinstaller ce rôle et de passer a des versions plus sécurisé de ce protocole.



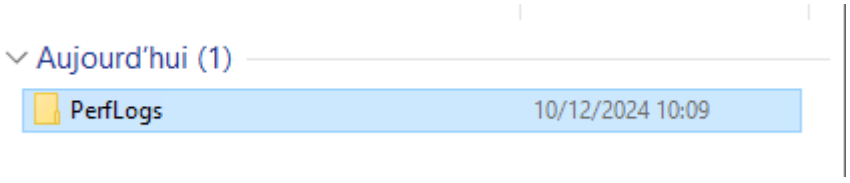
Sur notre disque local nous pouvons activé les clichés instantanés afin d'avoir une sauvegarde de l'état de notre disque a un moment donné

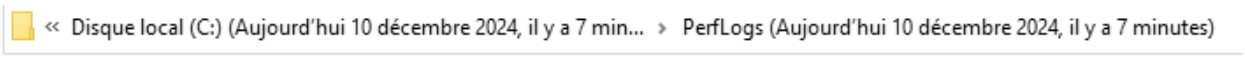


C'est dans le fichier « Perflogs » ou nous pourrons restauré les sauvegarde précédente

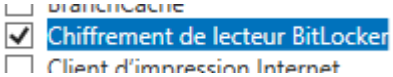


Nous pouvons voir que le cliché que j'ai créer a l'instant est affiché dans l'onglet version précédente et en rentrant dans ce dossier nous pourrons naviguer dans la sauvegarde du disque et restaurer ce qui nous intéresse

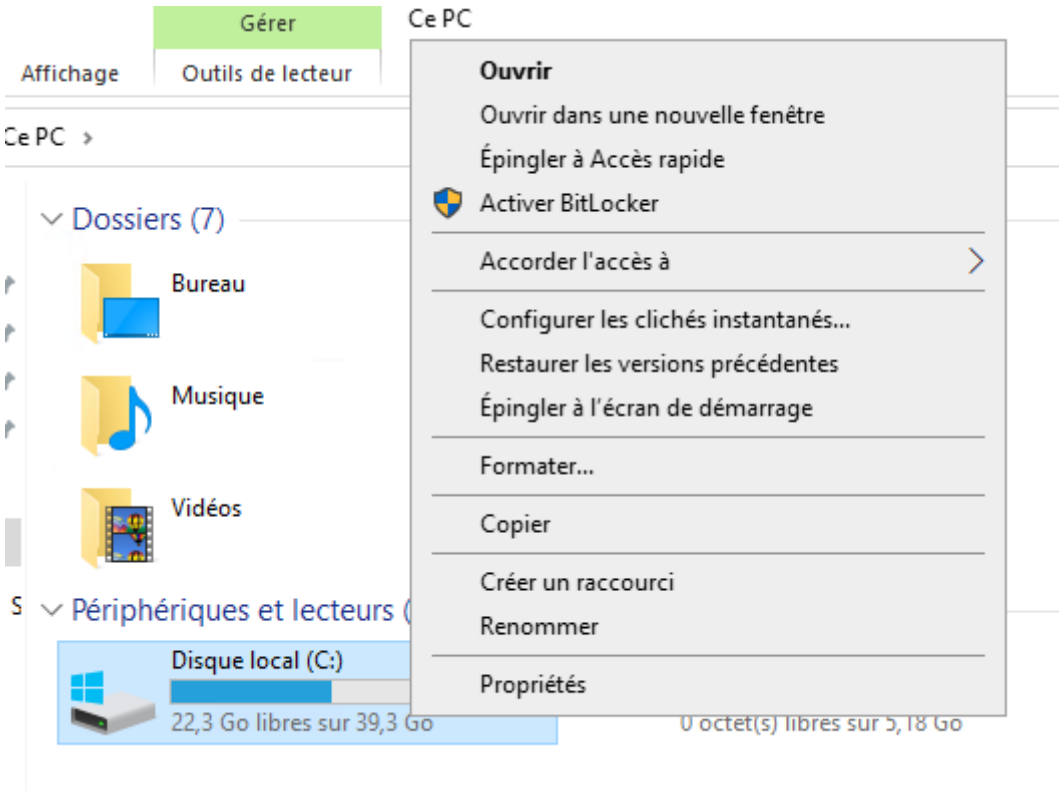




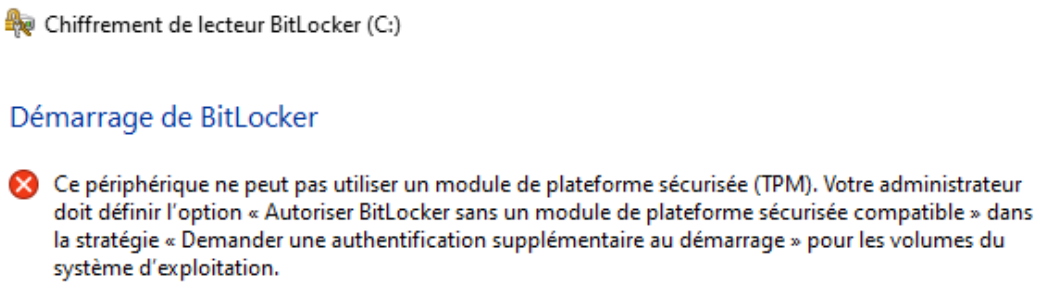
Nous passons a présent au chiffrement du disque dur via Bitlocker. Pour cela nous allons ajouté une fonctionnalité dans les rôles qui sera « chiffrement de lecteur Bitlocker »



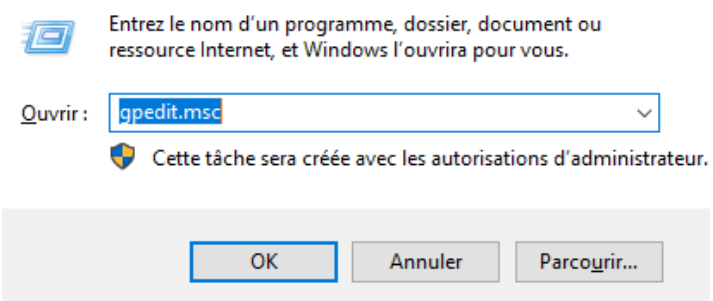
Après avoir installé la fonctionnalité, nous pouvons activé Bitlocker sur notre disque



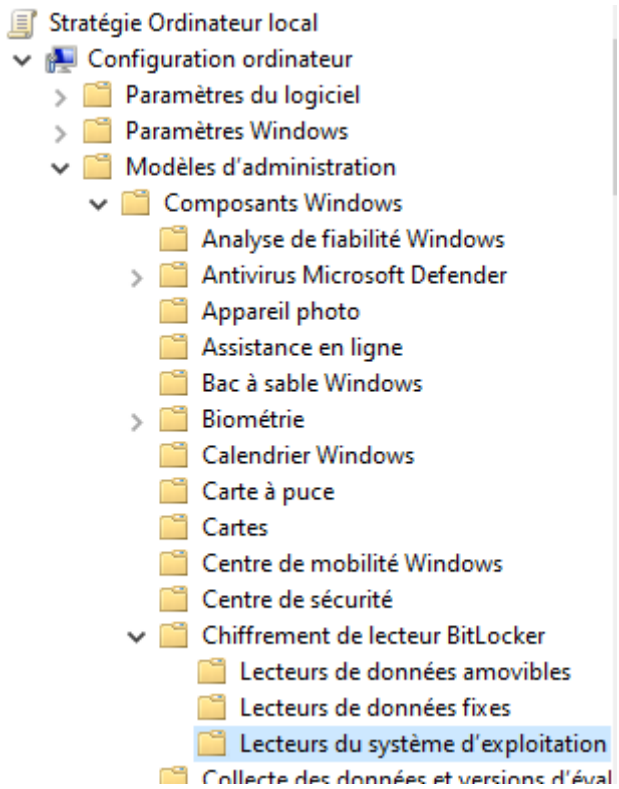
Notre poste ne contient pas de puce TPM, nous allons donc procédé a une installation sans puce TPM

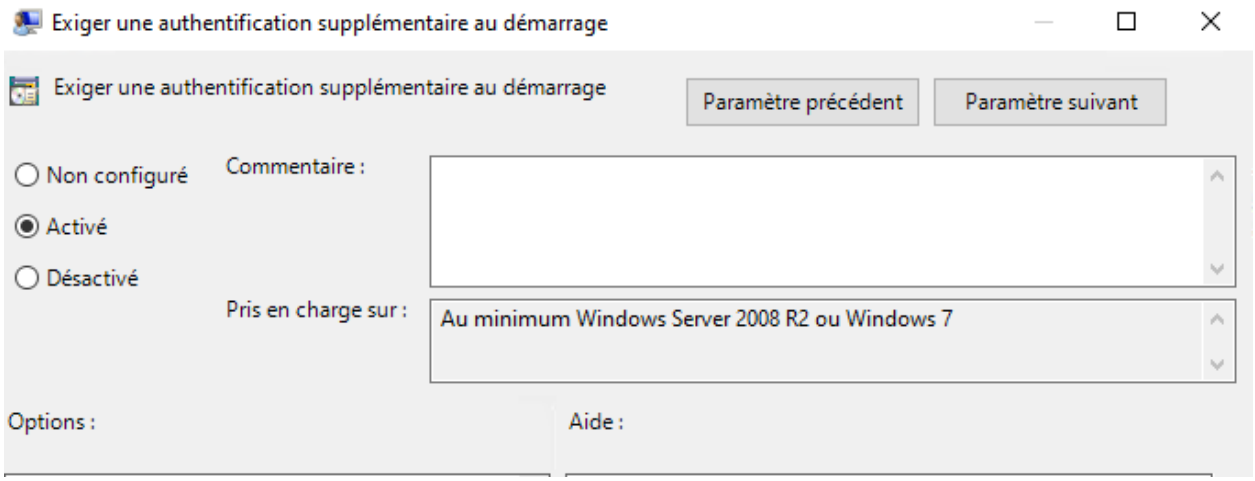


Pour cela, nous allons ouvrir l'exécuter et ouvrir l'éditeur de stratégie local « gpedit.msc »

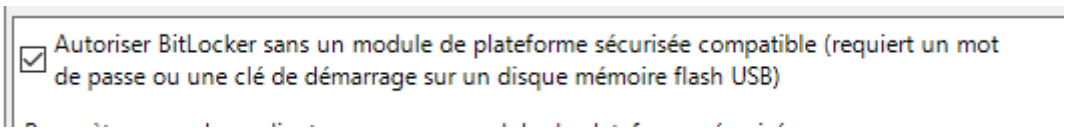


Nous nous rendons dans le chemin « configuration ordinateur » –> « modèle d'administration » –> « Composant Windows » –> « Chiffrement de lecteur Bitlocker » –> « lecteurs du système d'exploitation »
Puis nous allons activer « exiger une authentification supplémentaire au démarrage »



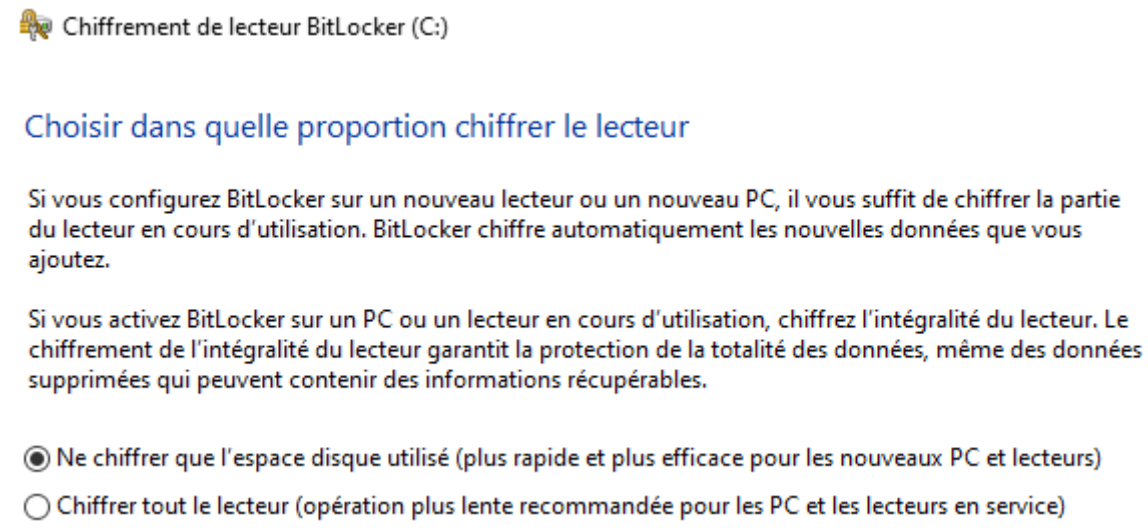


Nous cochons aussi dans la même interface « autorisé bitlocker » si cela ne s'est pas fait automatiquement

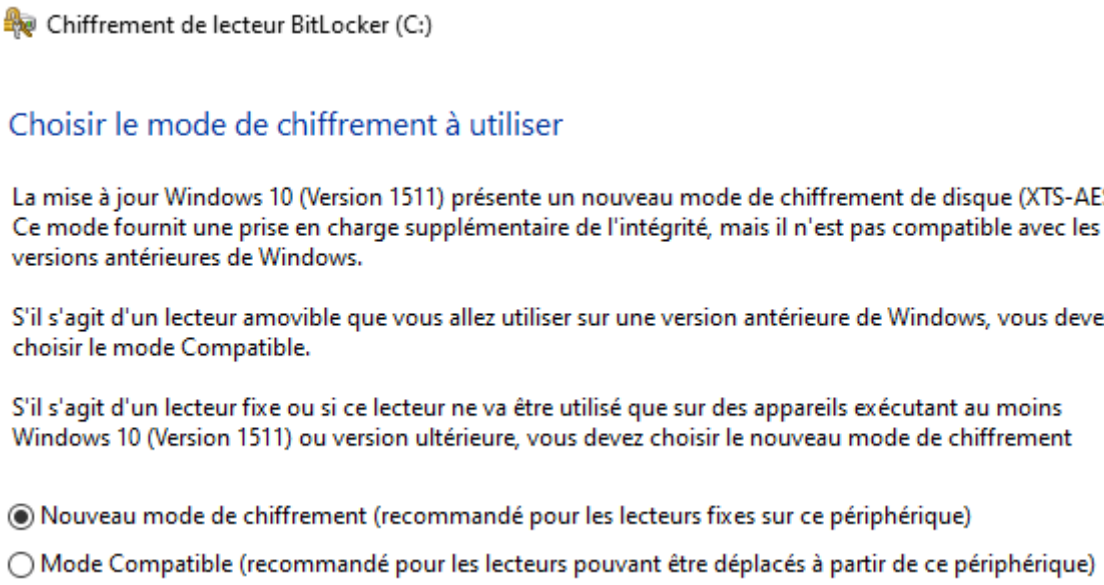


Après cela nous pouvons activer bitlocker en lui mettant un mot de passe ainsi que enregistrer sa clé de récupération.

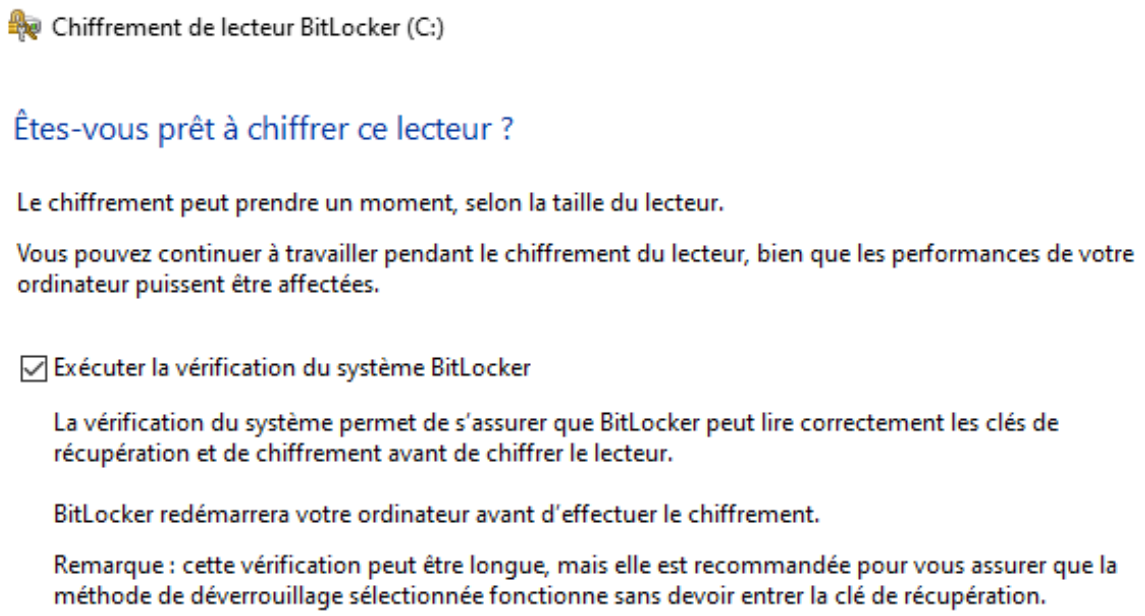
Maintenant lors de l'installation, nous pouvons choisir comment bitlocker fonction. Soit nous prenons chiffré que l'espace utilisé soit chiffrer tout le lecteur qui est meilleur lorsqu'il est en production dans notre cas nous prendrons chiffre que l'espace utilisé et même si de nouvelles données sont rajouté ils seront chiffré au fur et a mesure.



Pour le mode de chiffrement nous avons le choix entre le nouveau mode et le mode compatible, le nouveau seras principalement sur les poste récent qui possède la mise a jour bitlocker et qui puisse le faire tourner mais pour le mode compatible ce sera majoritairement pour les poste avec un système d'exploitation antérieur a windows 10. Dans notre cas nous prenons le nouveau mode car il est plus sécurisé.



Puis enfin, nous exécuterons la vérification du système bitlocker qui permettras a bitlocker de voir si il est capable de lire la clé de chiffrement et de récupération avant de chiffrer le lecteur.



Conclusion :

Le poste ne possédant pas de puce TPM, il a causé problème lors de l'activation de Bitlocker mais il y a un moyen de contourner le problème ce qui a permis de finalisé cette parti du TP

Durcissement AD :

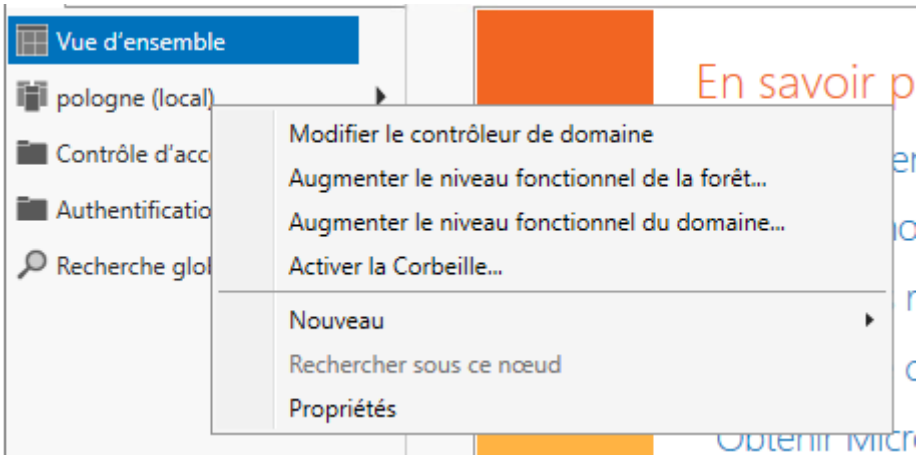
Introduction :

Le but de cette parti du TP est de procédé a une amélioration de sécurité plus centré sur Active Directory que sur un poste client

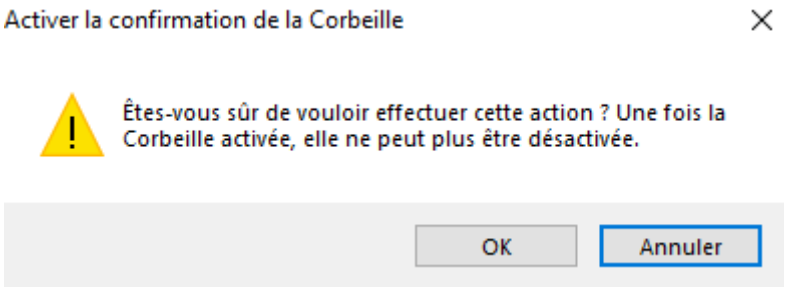
TP :

Pour commencer, nous allons activé la corbeille activé directory. Pour cela nous allons dans le centre d'administration active directory.

Sur notre domaine, nous activons la corbeille

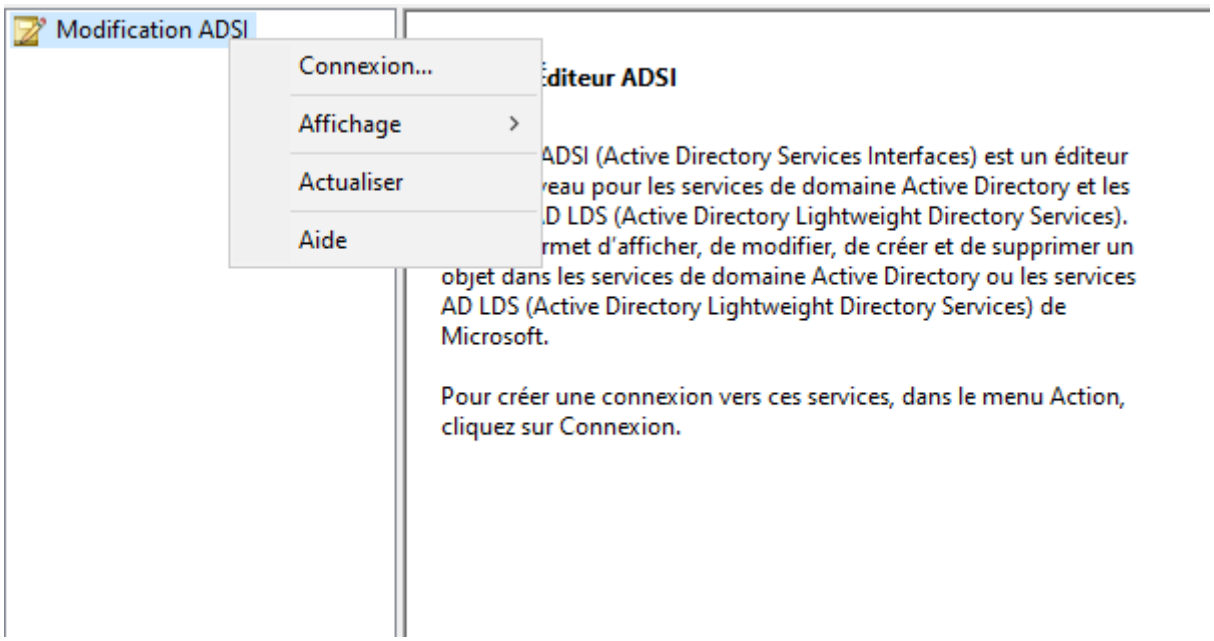


On nous précise bien que dès lors qu'on active la corbeille nous ne pourrons plus la désactiver après

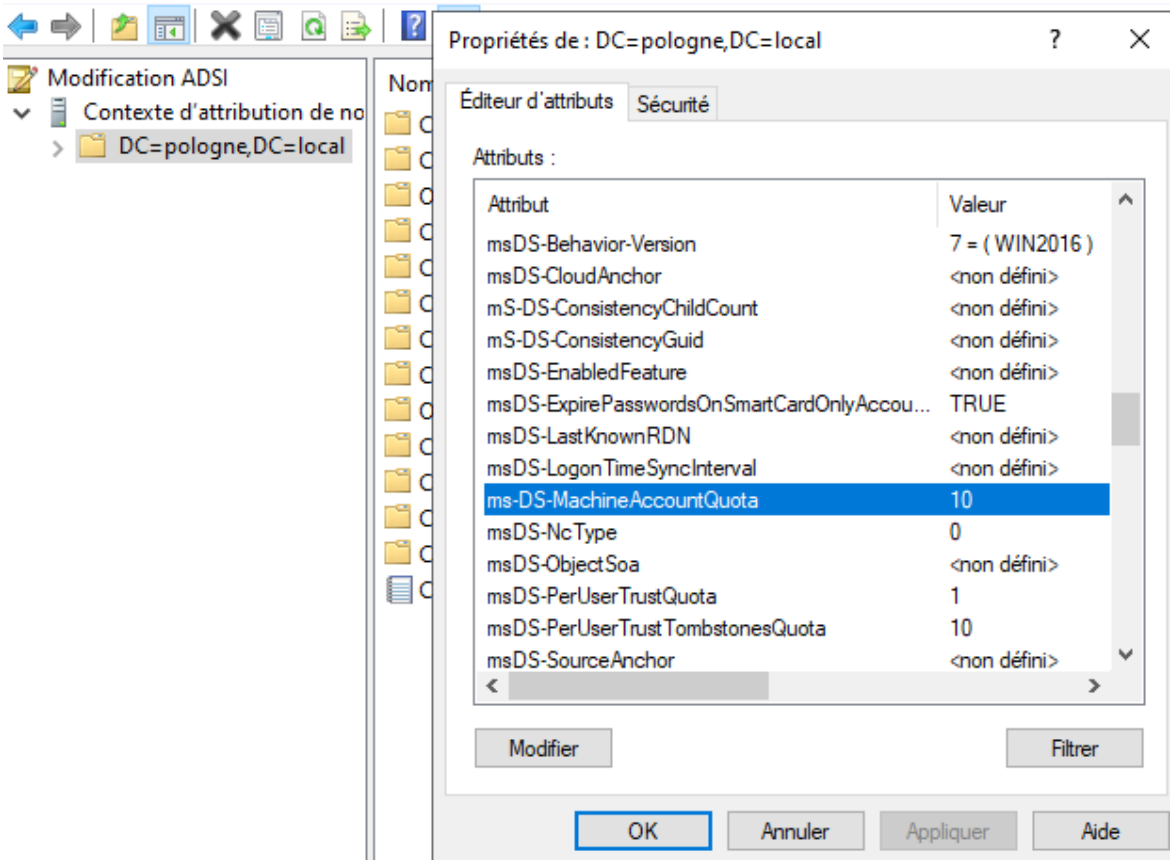


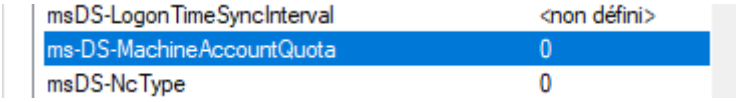
Dans les outils d'administration « modification ADSI »

Lorsque nous nous y rendons pour la première fois, nous arrivons sur une page vide. Pour y remédier nous faisons connexion sur « modification ADSI » et nous laissons par défaut les paramètre, cela nous connectera automatiquement

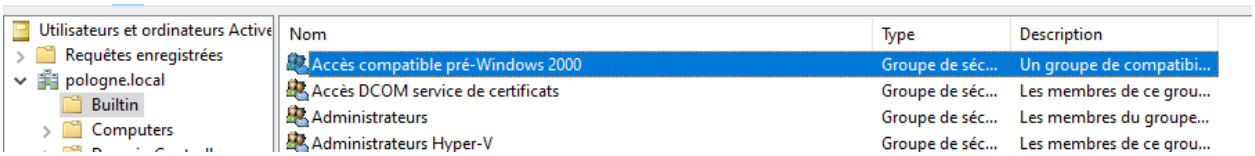


Dans les propriétés nous chercherons le paramètre « ms-DS-MachineAccountQuota » qui par défaut est a 10 et nous le mettrons a 0 car c'est le paramètre qui dit le nombre de machine maximal qu'un utilisateur peut ajouté au domaine.

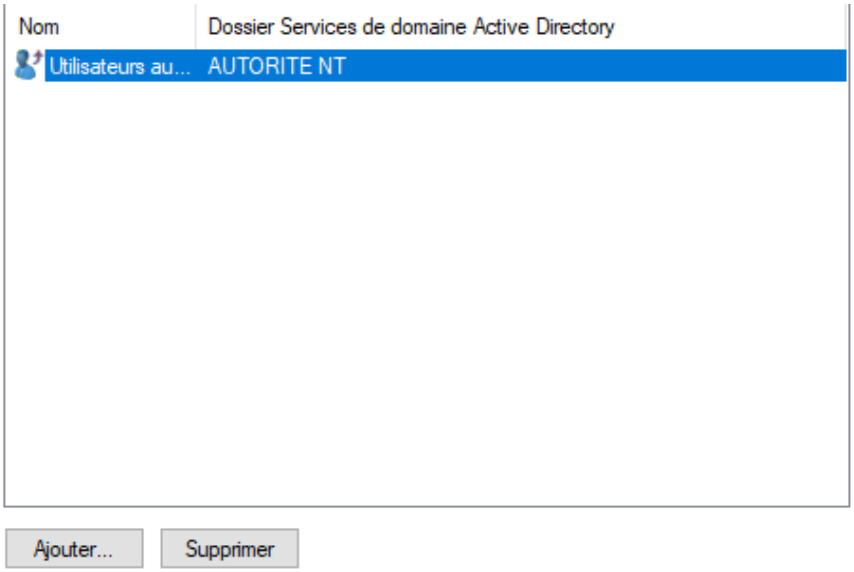




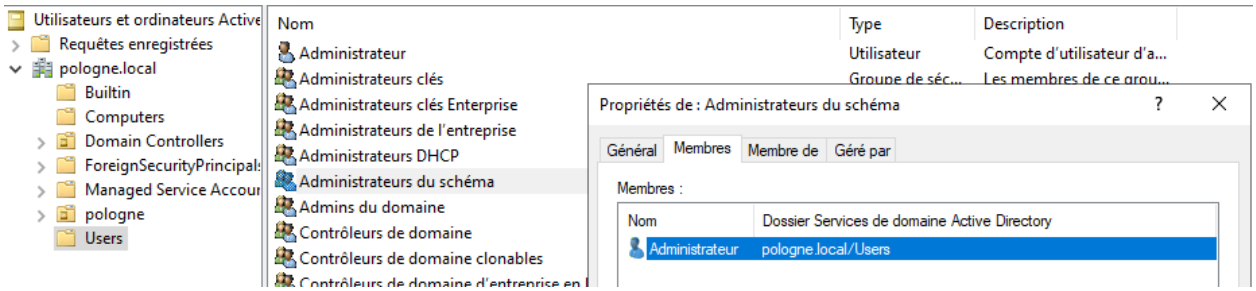
Pour poursuivre, dans les utilisateurs et ordinateurs active directory dans le dossier « builtin » nous avons le groupe « accès compatible pré-windows 2000 » qui sert a la rétrocompatibilité avec les Windows avant 2000 en leur donnant les droits de lecture



Nous irons dans les membres et nous supprimerons les utilisateurs authentifié

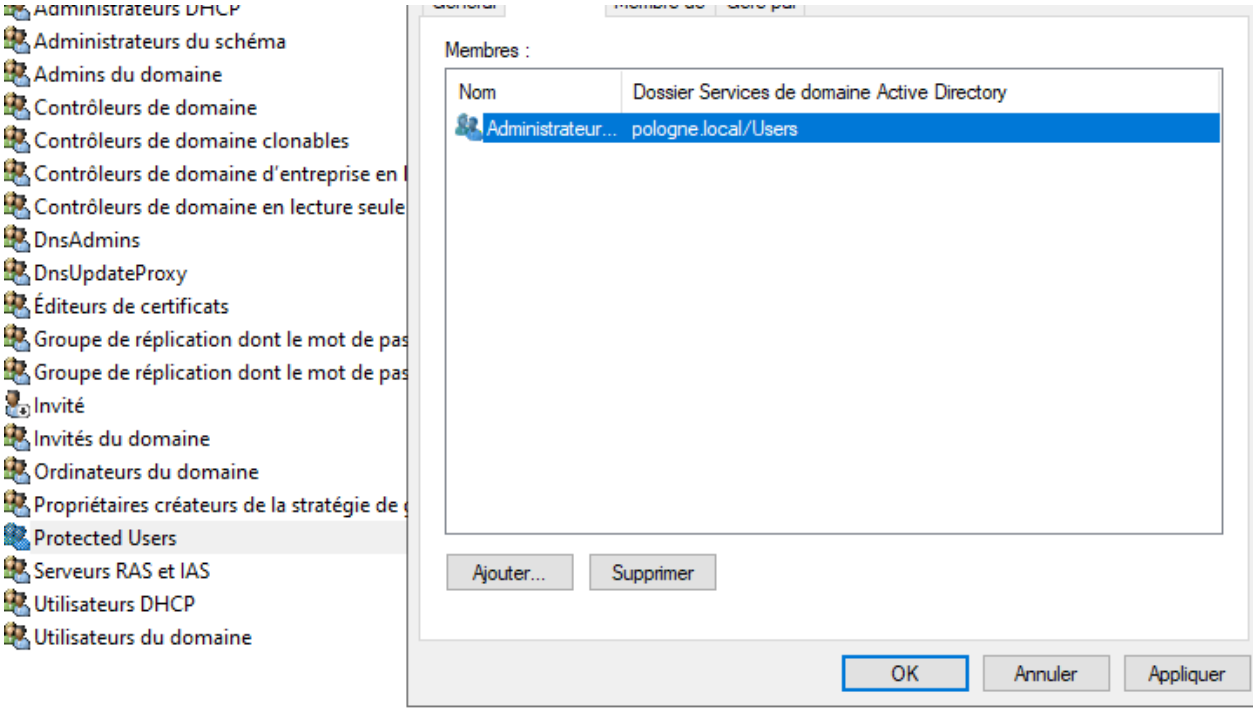


Tout en restant dans le même endroit dans « user » nous pouvons retrouvé « utilisateur du schéma » qui permet de modifier, créer ou supprimer des objets sur les serveurs donc lorsque nous n'avons pas besoin d'y toucher nous pouvons supprimé l'administrateur local et si nous aurons besoin de modifier quelque chose, il suffira de le rajouter a nouveau.

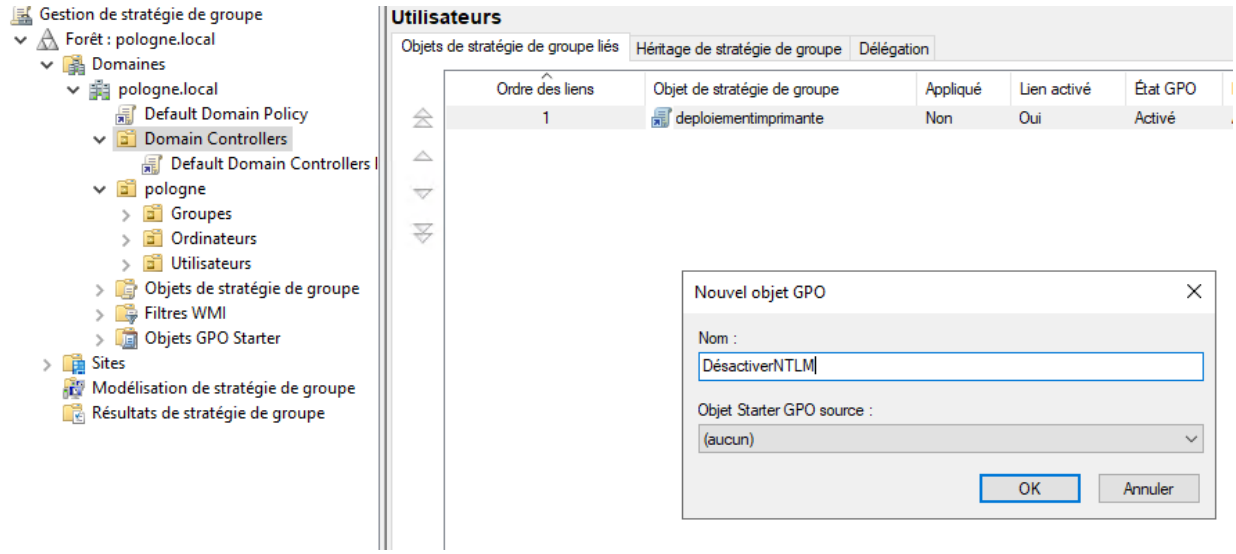


Encore une fois dans les « user » nous pouvons trouvé « protected user » qui est l'endroit ou l'on peut mettre tous les administrateur nominatif ou bien les utilisateurs sensible, ce groupe permet de ne pas enregistré dans le cache le mot de passe lors de la connection. Dans notre cas nous allons ajouté notre administrateur local.

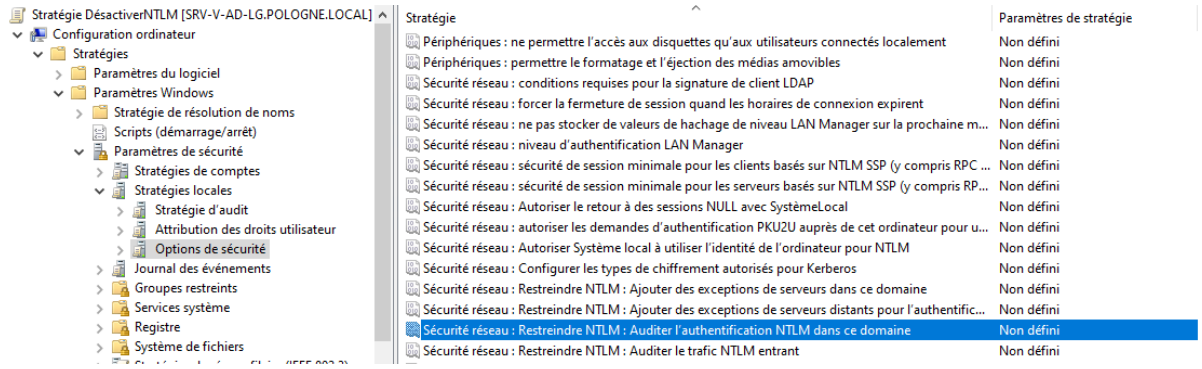
Il faut faire attention aussi lorsqu'un utilisateur protéger veux se connecter en bureau a distance il est possible qu'il doit écrire le nom complet du serveur donc : nom du srv « . » le domaine



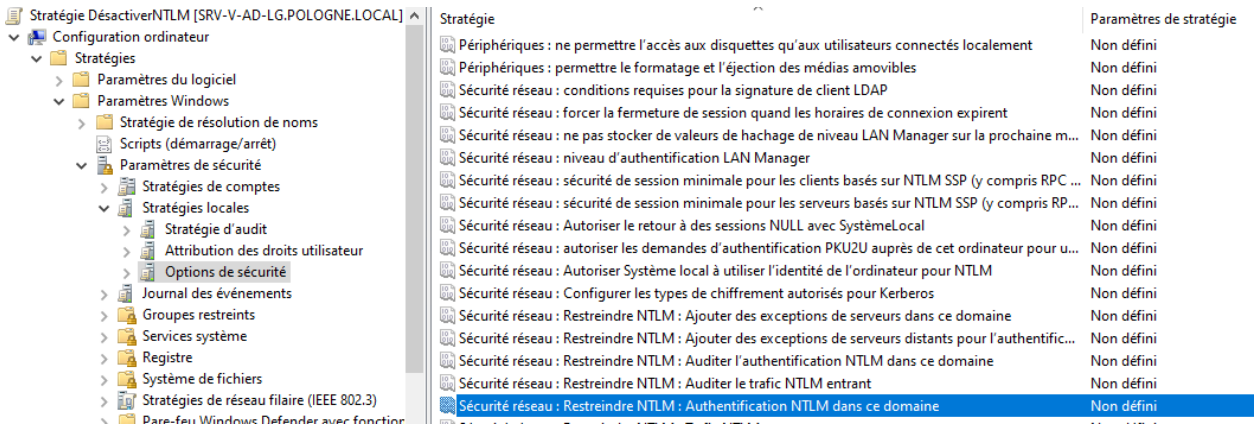
Pour continuer le durcissement de notre serveur, nous pouvons allé dans la gestion des stratégie de groupe et ajouté un GPO nommé « désactiverNTLM » qui vas nous désactivé les anciens protocoles d'authentification (NTLM v1 et v2), il est d'abord nécessaire de vérifier qu'aucun logiciel n'utilise ce protocole avant de le désactiver

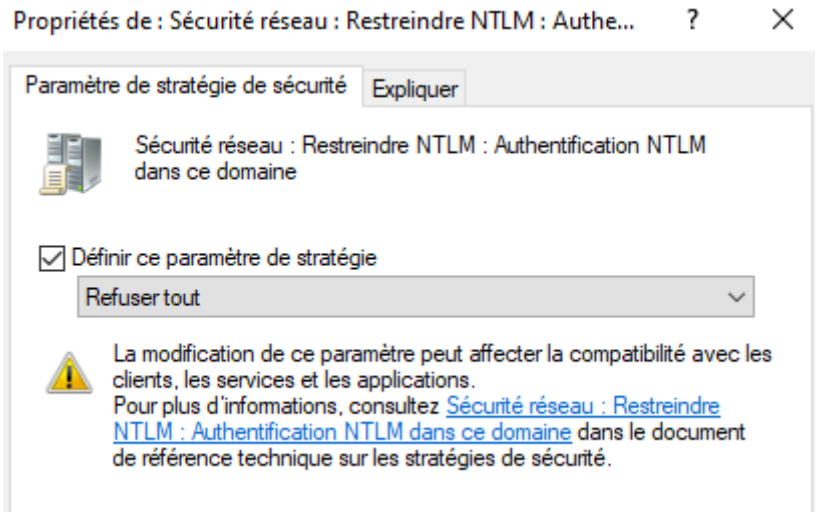


Pour vérifier si il nous reste de l'authentification via NTLM, nous pouvons laisser tourner la stratégie de groupe qui permet d'audité toute les authentifications NTLM pendant 15 jours a 1 mois afin d'être sur qu'il n'y a aucune trace du NTLM dans l'observateur d'événement.



Dès lors ou nous n'avons plus de trace de cette authentification nous pouvons a présent la restreindre





Conclusion :

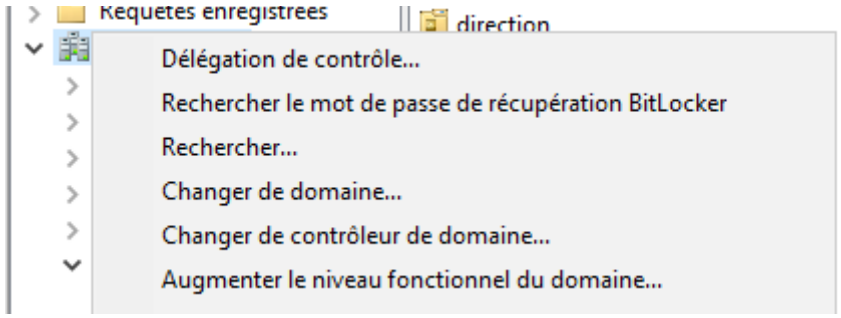
TP effectuer sans la réinitialisation du mdp Kerberos car l'utilisateur krbtgt n'était pas présent dans les utilisateurs de l'AD sinon a part ça aucun soucis rencontrer.

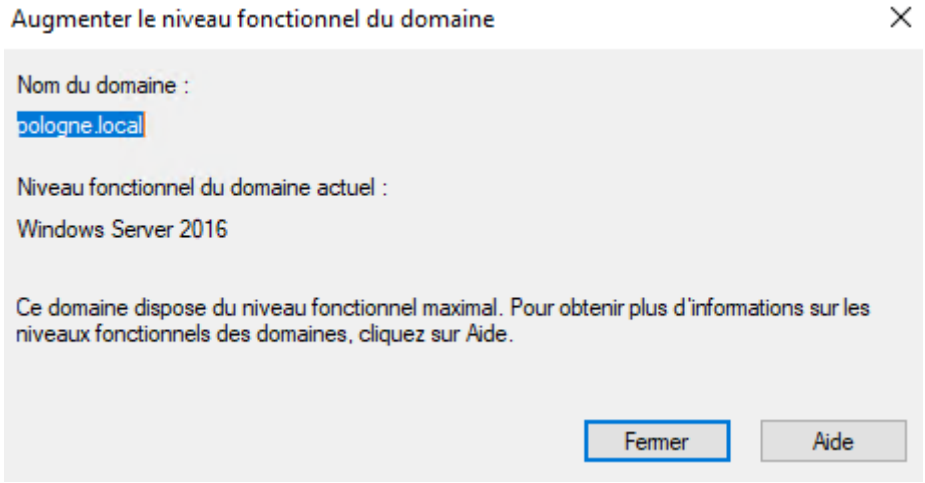
Gestion de l'authentification local LAPS :

Introduction :

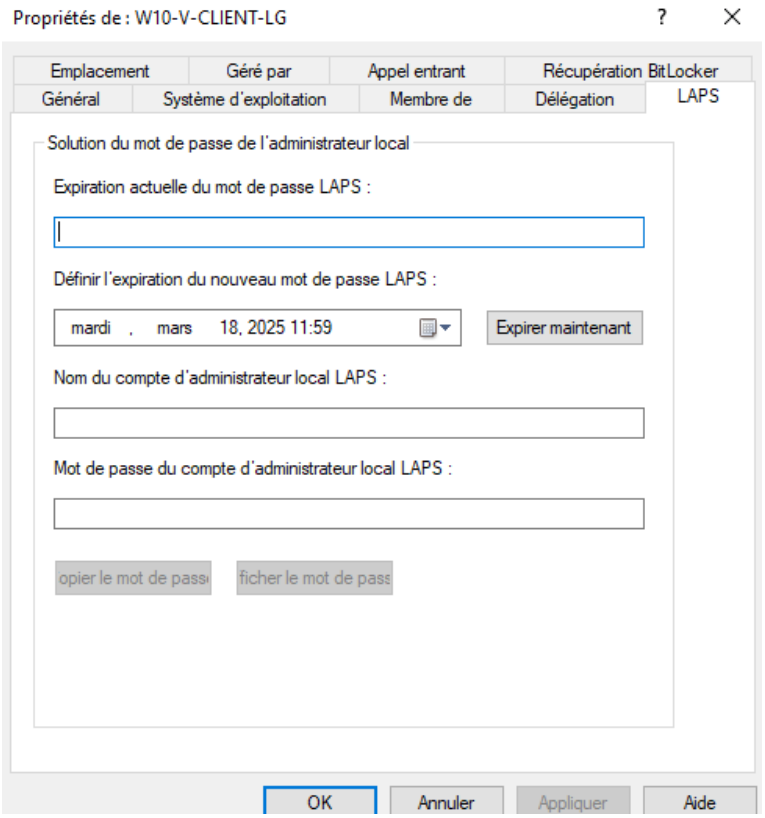
TP :

Pour débuter, nous allons voir le niveau fonctionnel de notre domaine est assez élever. Dans les utilisateur active directory nous faisons un clique droit sur le domaine et cliquons « augmenter le niveau fonctionnel du domaine »
Notre serveur a un niveau fonctionnel de 2016 ce qui est le maximum a la date du tp.

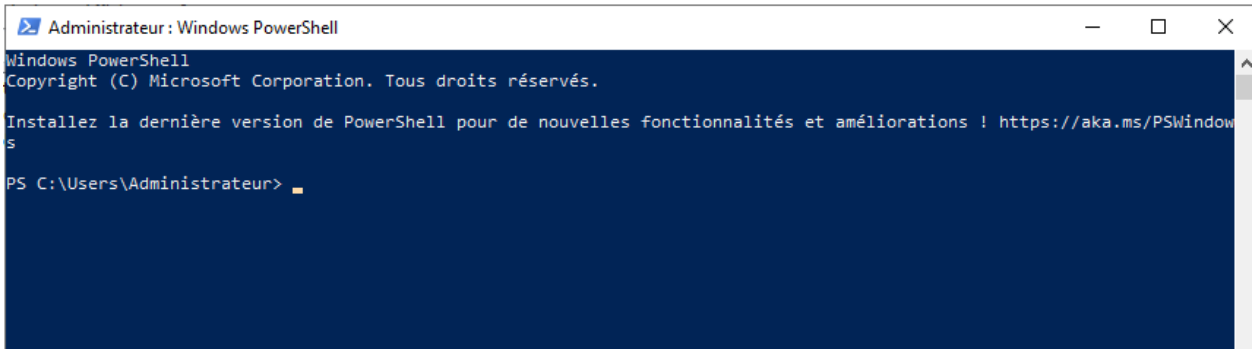




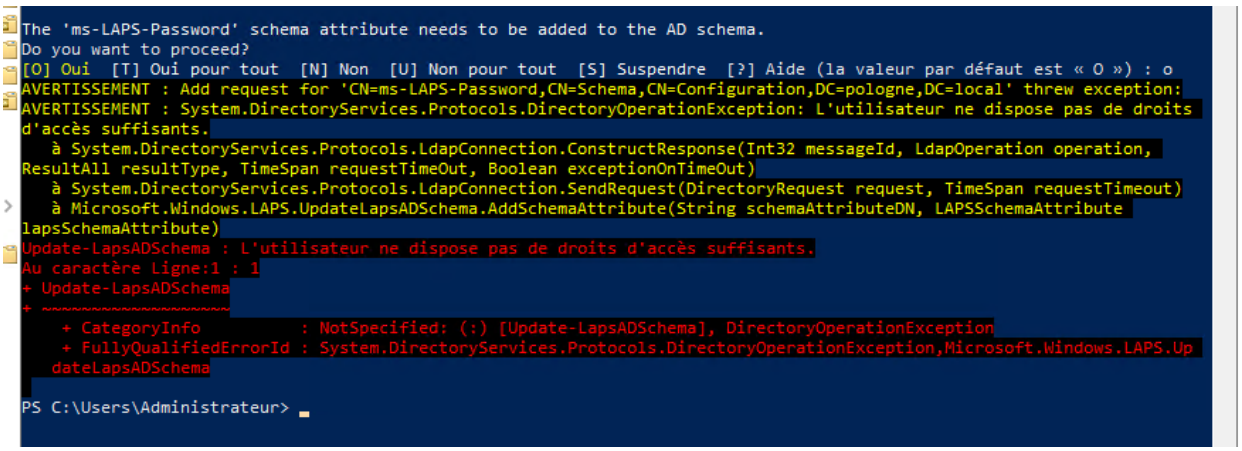
Quand nous allons dans les propriétés d'un ordinateur nous pouvons voir l'onglet LAPS qui n'est pas encore paramétrer



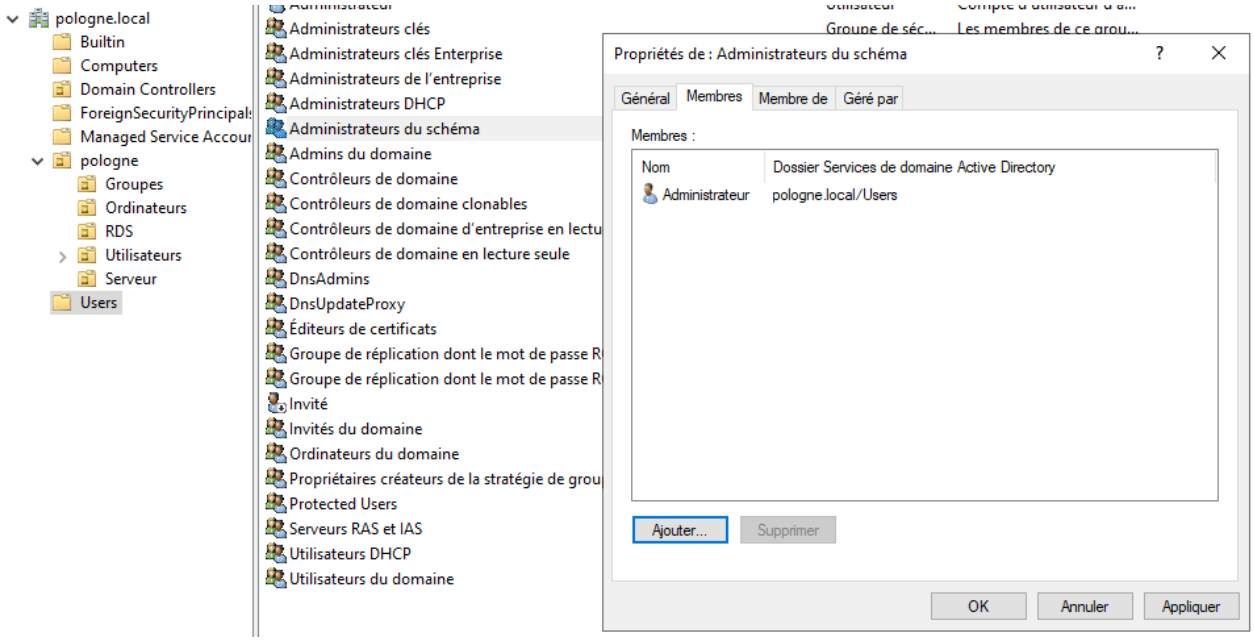
La première étape du paramétrage du schéma active directory sera lancer une fenêtre powershell en administrateur



La commande a utilisé pour mettre a jours est « Update-LapsADSchema ». Il faut bien attendre que tout les serveurs en replication, on leur replication a jour. Nous voyons que nous avons pas les droits.



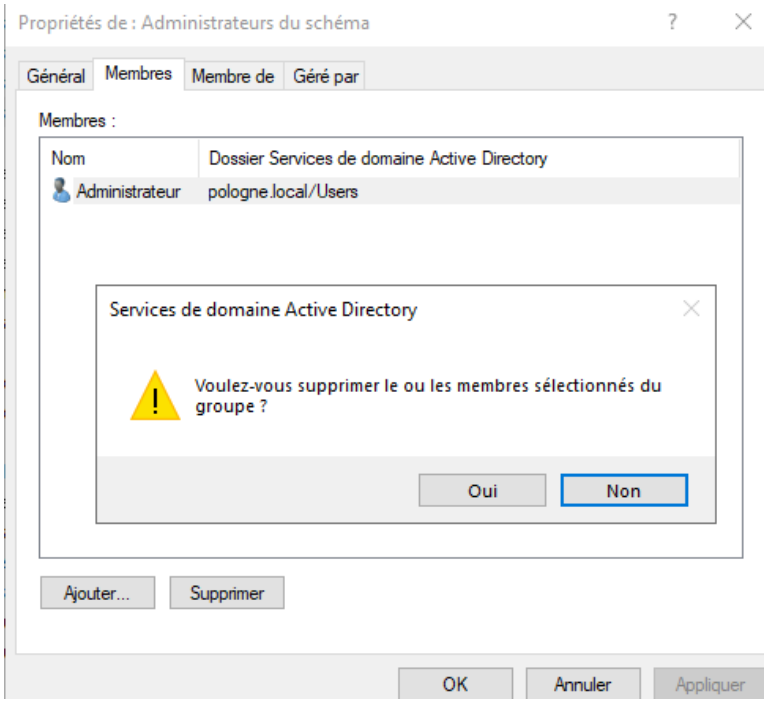
Pour y remédier, il nous suffit de rajouter l'administrateur dans les administrateurs du schéma



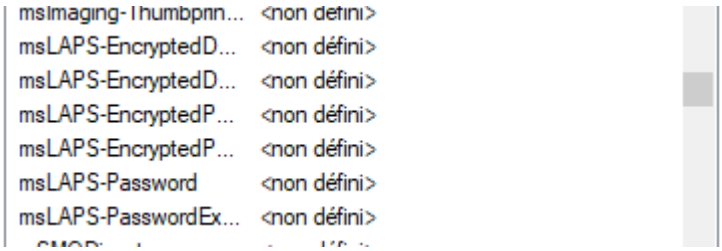
Nous voyons que nous n'avons plus d'erreur, nous pouvons mettre « t » pour dire oui a tout

```
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 ») : o

The 'ms-LAPS-PasswordExpirationTime' 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 ») : t
```

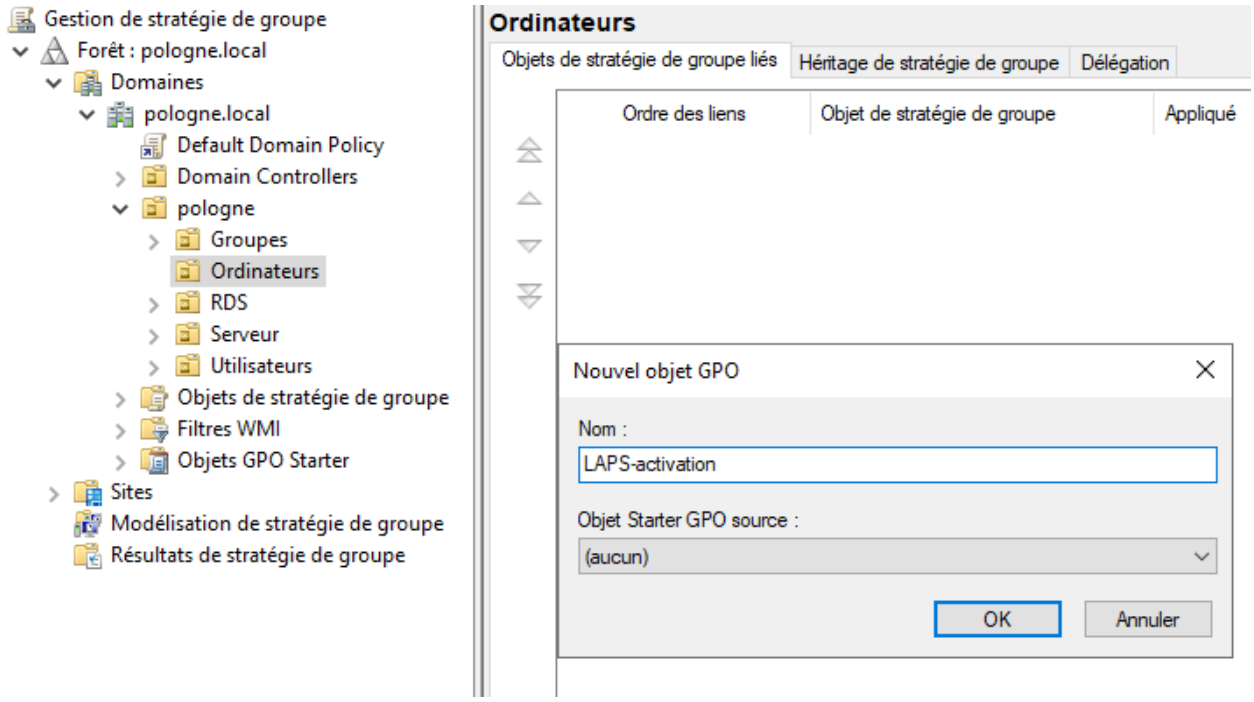
Après il ne faut pas oublier de supprimer a nouveau l'administrateur dans les administrateurs du schéma



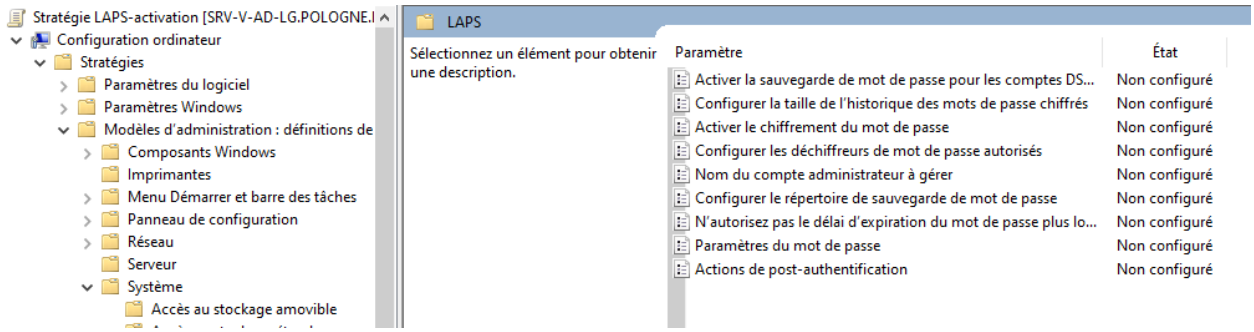
La mise a jour du schéma nous affiche maintenant dans l'éditeur d'attribut nous pouvons voir maintenant les attribut « msLAPS »



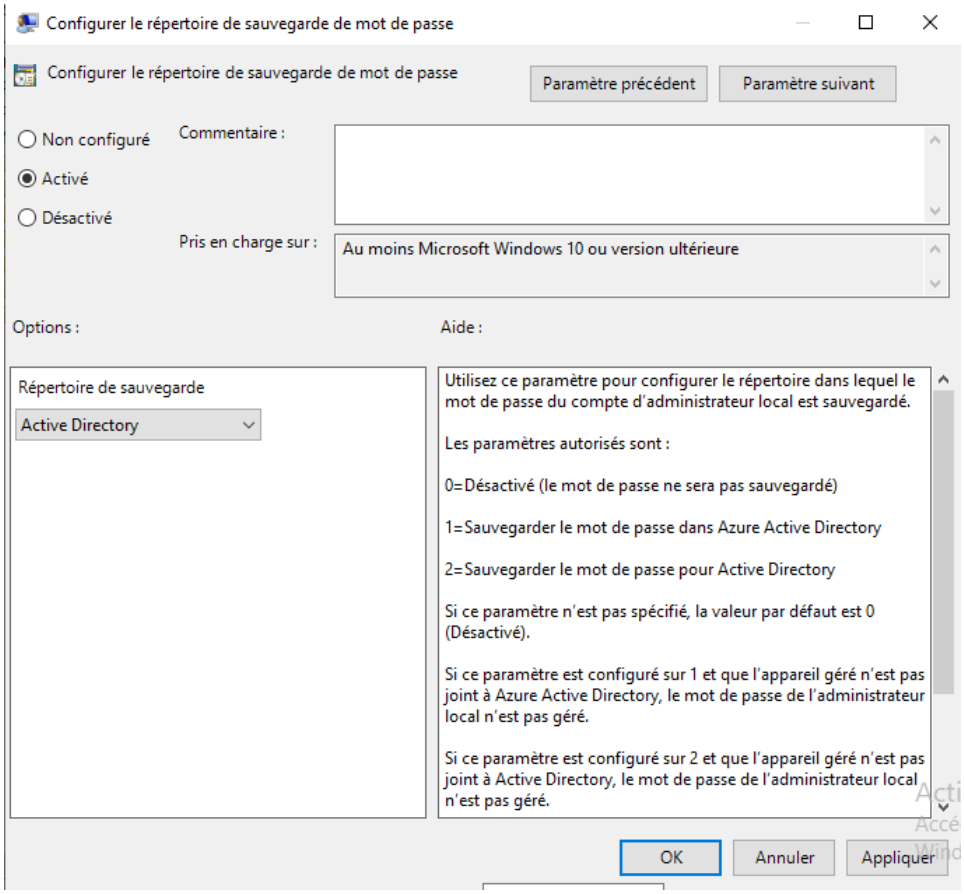
Le paramétrage a été effectué, la deuxième étape est l'administration via stratégie de groupe ou nous allons créé un GPO sur l'UO ordinateur. Je l'ai nommé « LAPS-activation ».



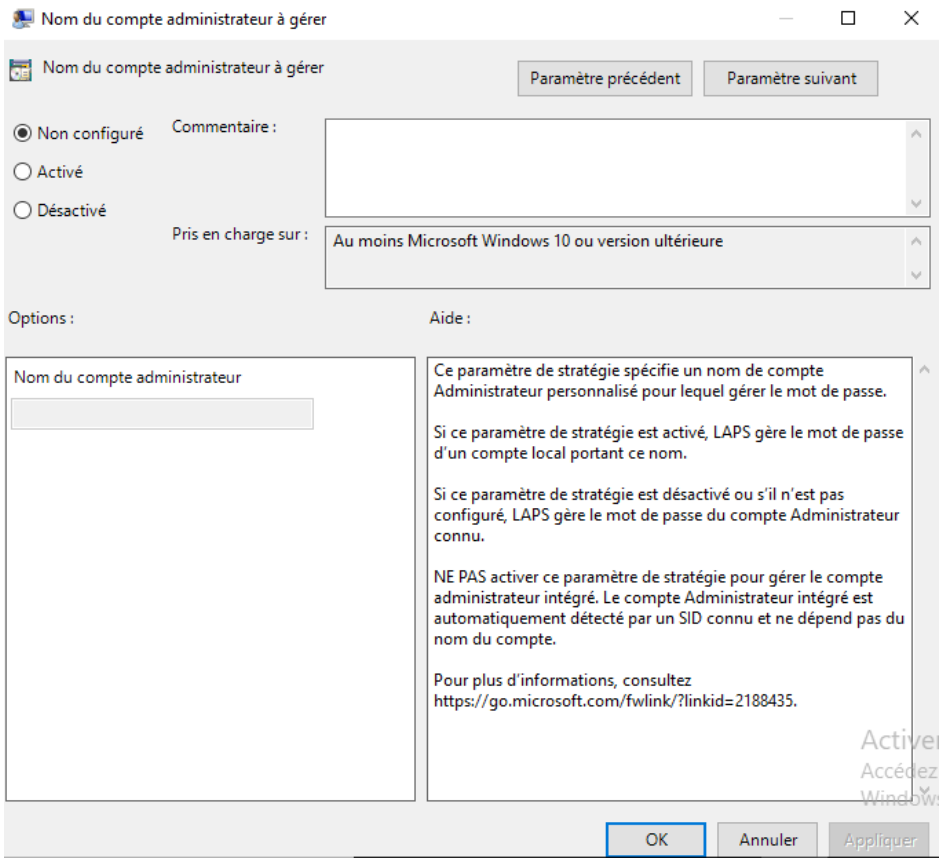
Nous la modifions et allons dans config ordi –> stratégie –> modèles d'administration –> Système –> LAPS



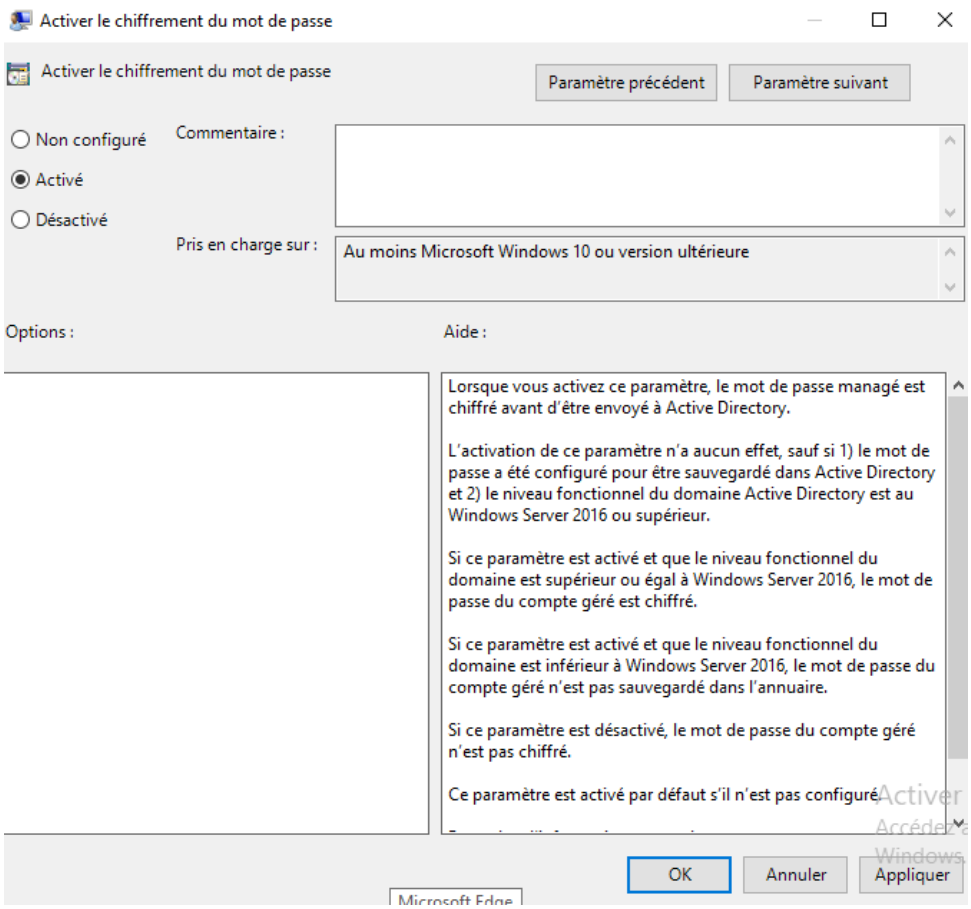
Vue que notre LAPS n'est que installé pour le moment. Il faudra donc l'activer, pour l'activer nous activerons « configurer le répertoire de sauvegarde de mot de passe » et choisissons ou stocker. Dans notre cas ce sera active directory car nous somme en local



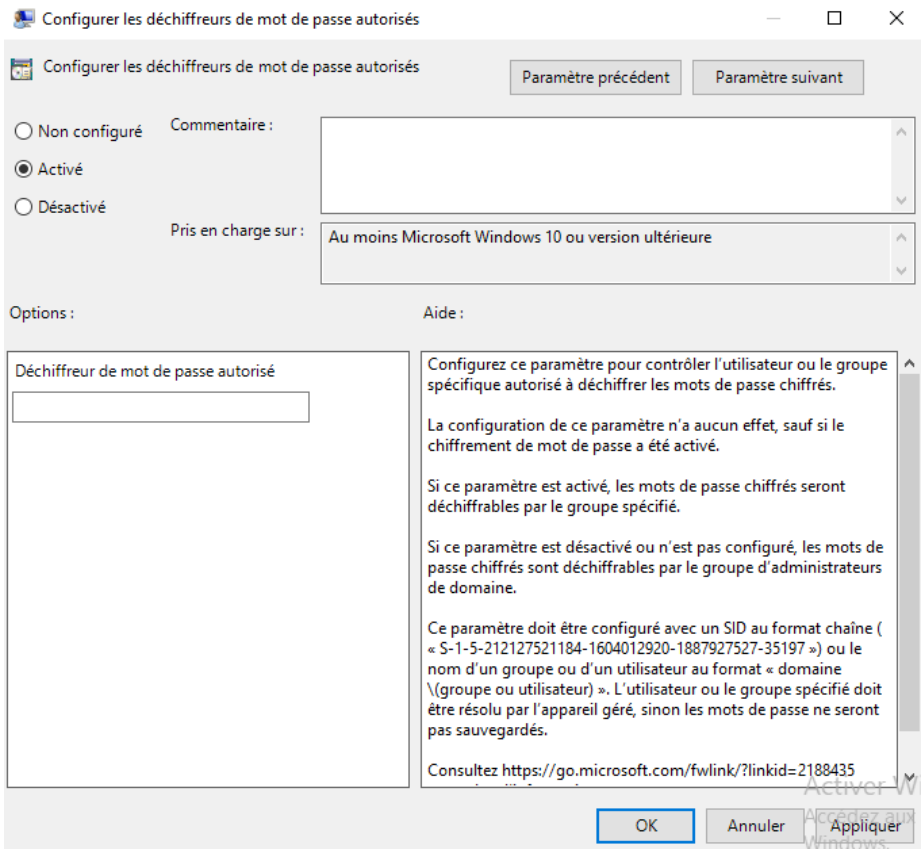
Par rapport a la configuration nous pouvons choisir l'option « nom du compte administrateur à gérer ». en l'activant nous pourrons rentré le nom que l'on a donner aux comptes administrateur sur les postes. Dans notre cas ça ne sera pas utile.



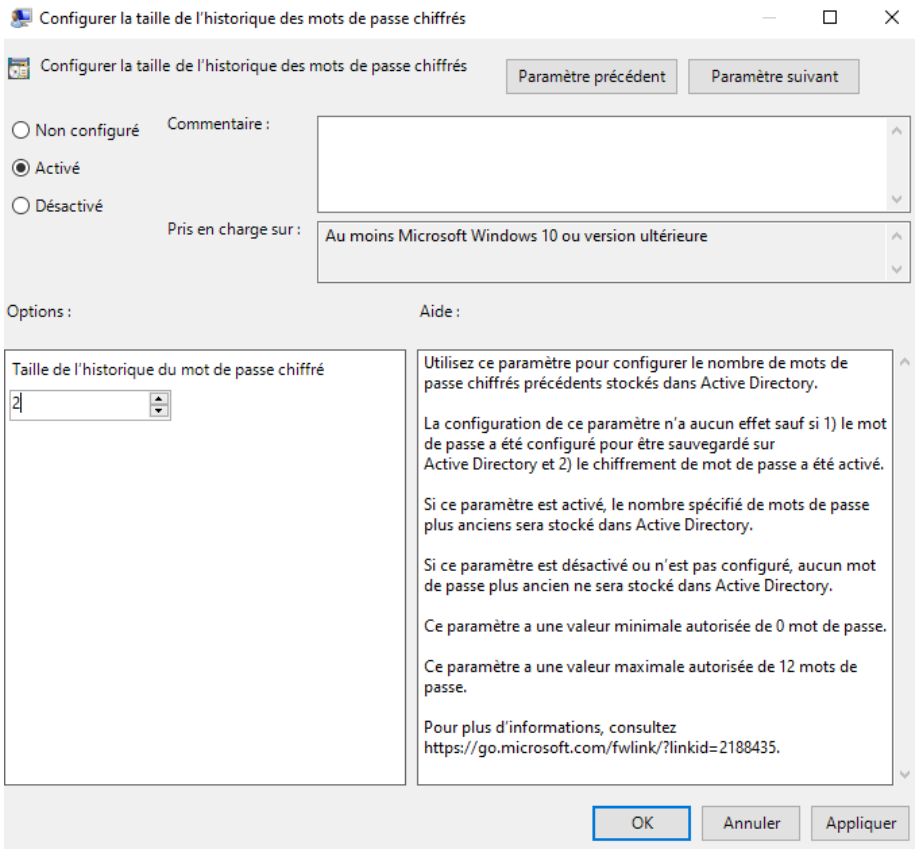
Pour sécuriser le stockage des mots de passe dans active directory, nous activons le chiffrement des mot de passe



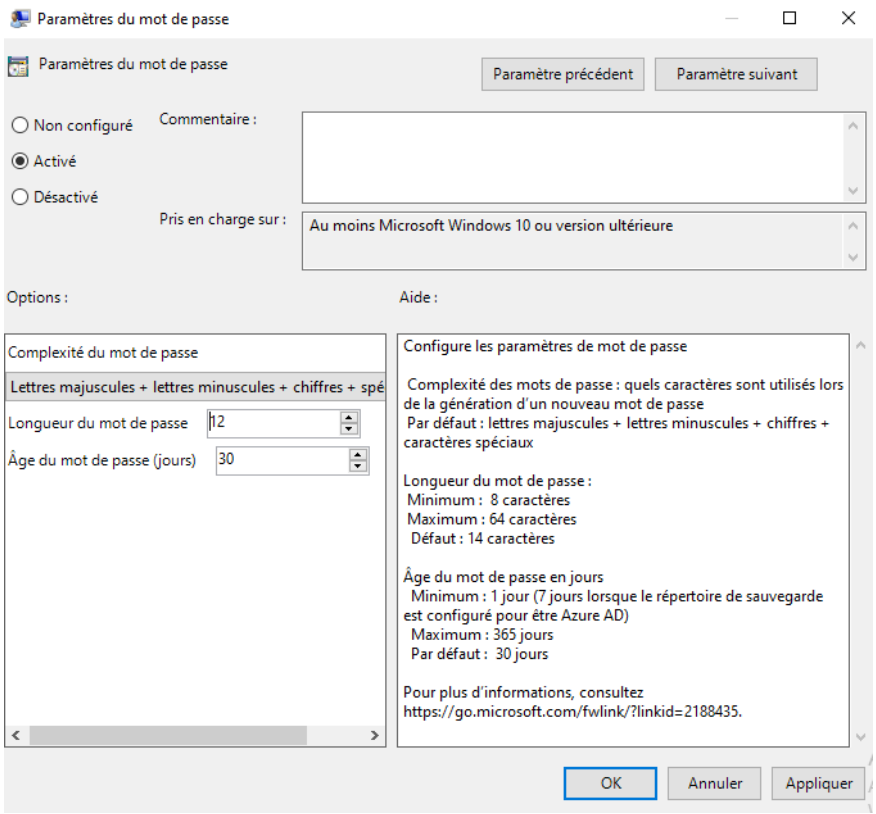
Si nous activons l'option ci-dessus, il faudra alors dire qui pourra les déchiffrer grâce à « configurer les déchiffreur de mot de passe autorisés » par defaut ce sont les admin du domaine si nous ne l'activons pas



En cas de restauration d'un poste client activer l'historique de mot de passe serait judicieux afin d'avoir encore les anciens mot de passe. La taille de l'historique sera juste le nombre de mot de passe retrouvable dans l'historique.



Passons au paramètre de la spécificité du mot de passe, nous l'activons et prenons « lettres majuscule + lettres minuscule + chiffre + cara spéciaux » la longueur nous la définissons sur 12 afin d'être dans les norme. L'age dépendera de la politique de la boite.



La dernière étape sera l’autorisation aux utilisateurs de changer leurs mot de passe et de le communiquer a active directory. Pour cela nous ouvrons a nouveau une fenêtre powershell en admin et rentrons la commande « Set-LapsADComputerSelfPermission -Identity "OU=Ordinateurs,OU=GA,DC=geek-advisor,DC=local" »