

**Durcissement Serveur :**

**Introduction :**

Lors de ce TP nous allons effectuer quelques paramètres de base afin de sécuriser nos serveurs.

**TP :**

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

 **Réseau avec domaine**  
Le pare-feu est activé.

 **Réseau privé**  
Le pare-feu est activé.

 **Réseau public (actif)**  
Le pare-feu est activé.

Ensuite nous allons faire en sorte que notre serveur soit à jour dans Windows Update

Windows Update Dernière recherche de mises à jour : [Télécharger les mises à jour uniquement à l'aide de Windows Update](#) Aujourd'hui à 00:22

Et nous activerons aussi dans les paramètres avancés, le fait de recevoir les mises à jour des produits Microsoft qui permettra de tenir à jour tous les produits Microsoft sur notre serveur.

Recevoir les mises à jour d'autres produits Microsoft lors de la mise à jour de Windows

Activé

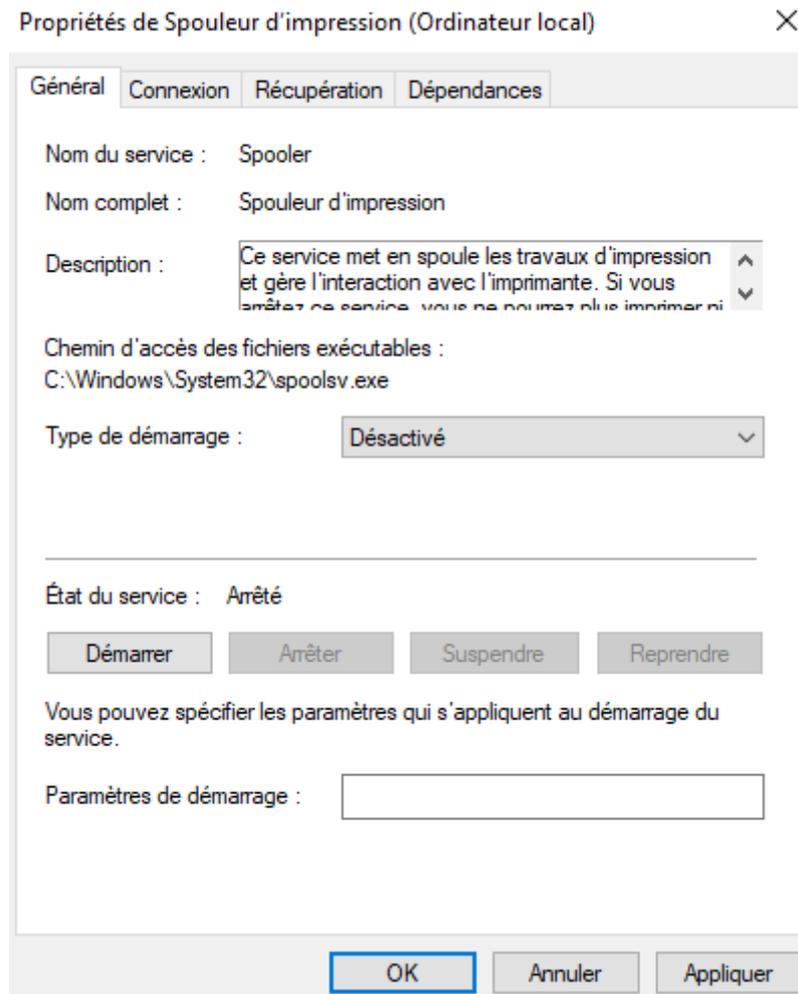
L'antivirus doit être aussi activé surtout la protection en temps réel qui montre bien que l'antivirus est actif

**Protection en temps réel**

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

Activé

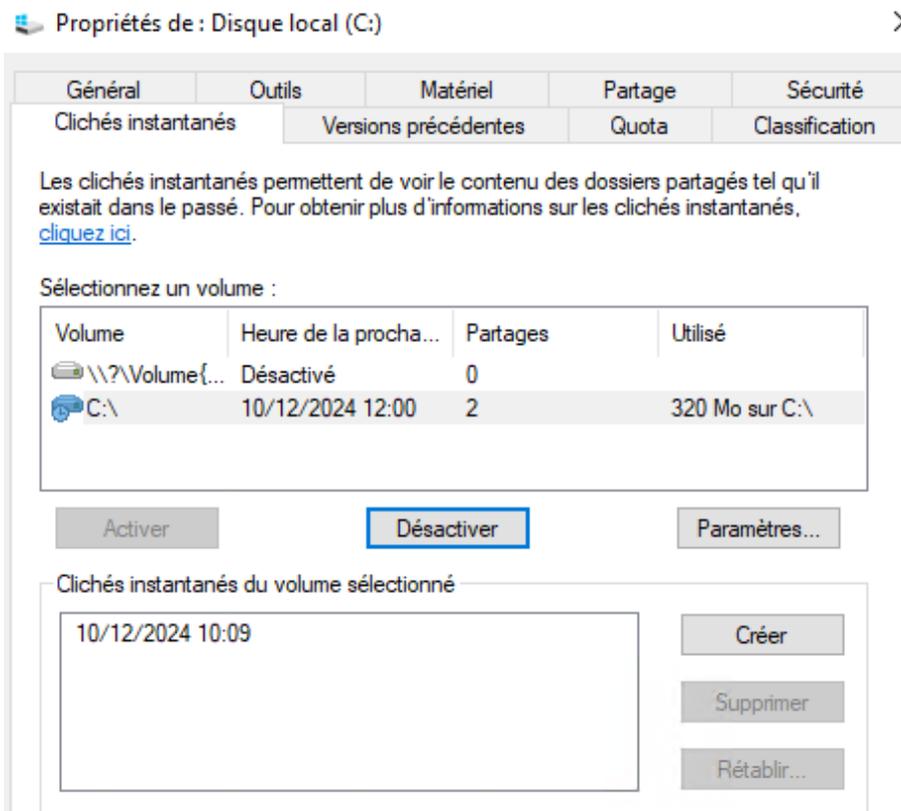
Dans les services nous pouvons arrêter le spouleur d'impression si notre serveur n'est pas un serveur d'impression afin d'éviter les failles potentielles



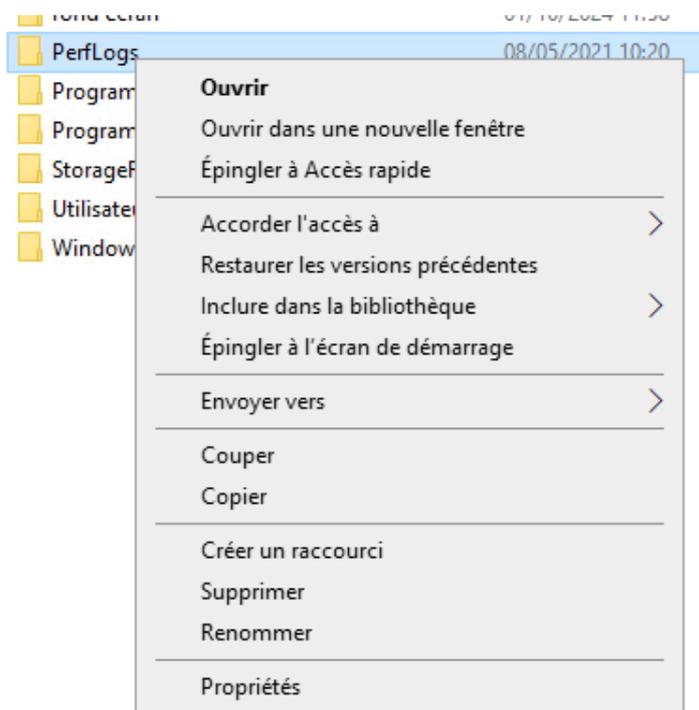
La vérification de la version du protocole SMB est important car il y a une version ancienne qui n'est plus utilisé « SMBv1 » alors si nous n'utilisons pas ce protocole, nous devons le désactiver et pour voir si il est installé par le biais de l'interface graphique. Nous allons faire ajouter un rôle 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.



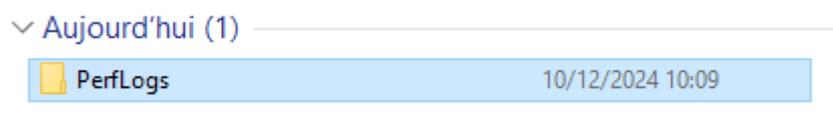
Sur notre disque local nous pouvons activé les clichs instantanés afin d'avoir une sauvegarde de l'état de notre disque a un moment donné



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



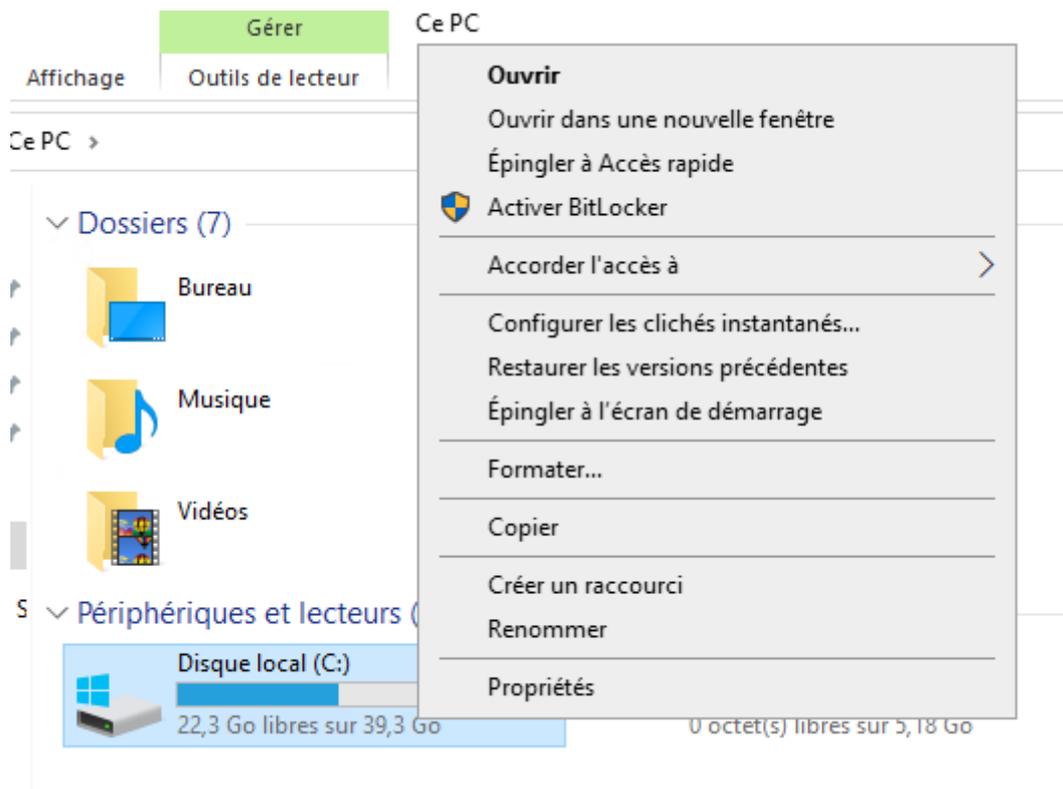
Nous pouvons voir que le cliché que j'ai créer à l'instant est affiché dans l'onglet version précédente et en rentrant dans ce dossier nous pourrons naviguer dans la sauvegarde du disque et restaurer ce qui nous intéresse



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 »

- BitLocker
- Chiffrement de lecteur BitLocker
- Client d'impression Internet

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



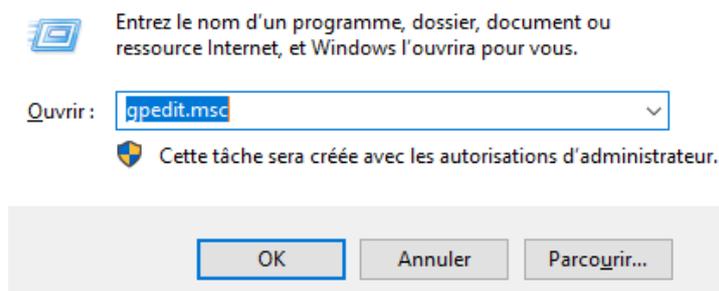
Notre poste ne contient pas de puce TPM, nous allons donc procédé a une installation sans puce TPM

 Chiffrement de lecteur BitLocker (C:)

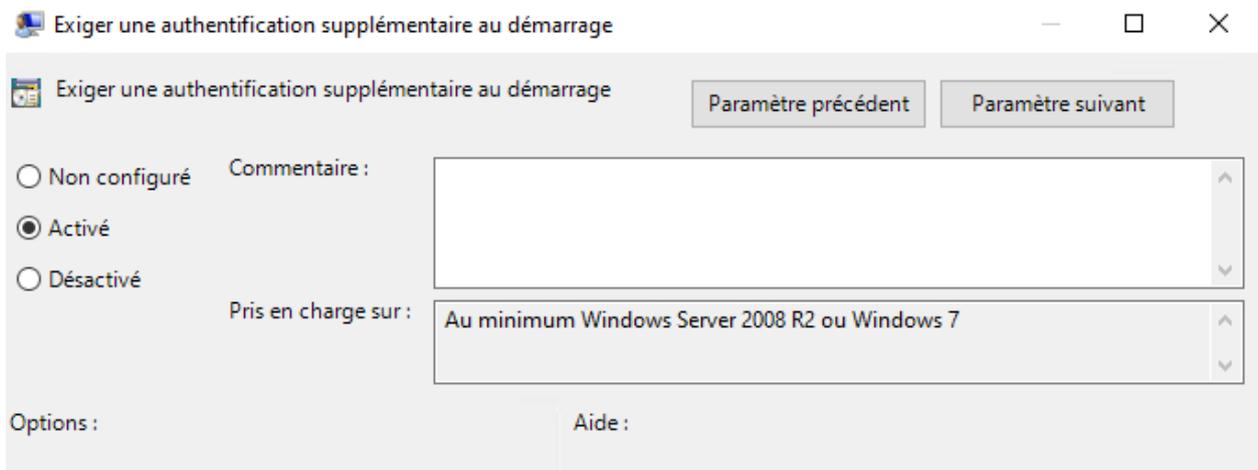
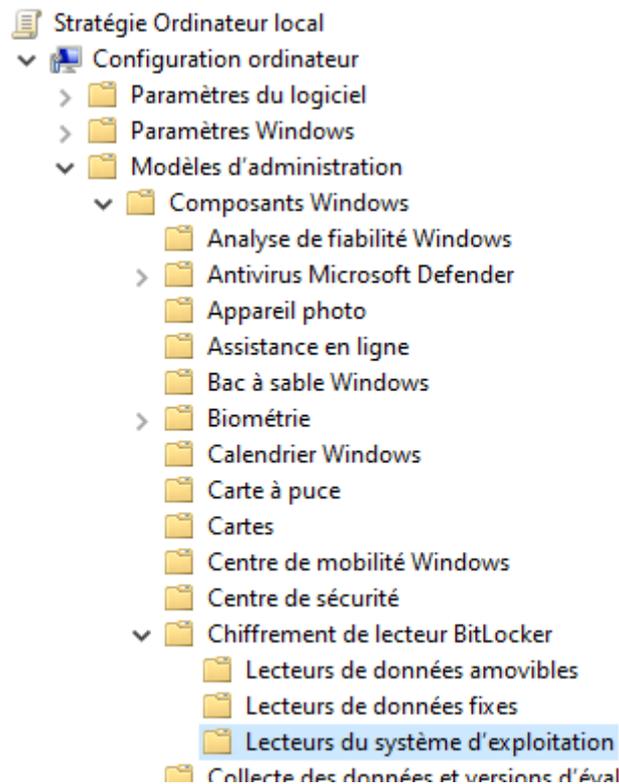
### Démarrage de BitLocker

-  Ce périphérique ne peut pas utiliser un module de plateforme sécurisée (TPM). Votre administrateur doit définir l'option « Autoriser BitLocker sans un module de plateforme sécurisée compatible » dans la stratégie « Demander une authentification supplémentaire au démarrage » pour les volumes du système d'exploitation.

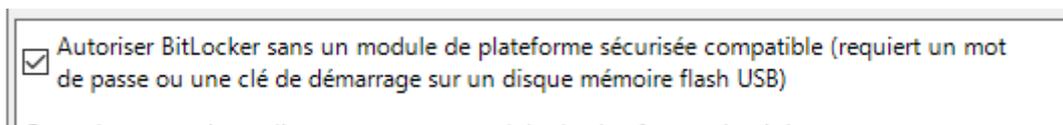
Pour cela, nous allons ouvrir l'exécuter et ouvrir l'éditeur de stratégie local « gpedit.msc »



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.

## Chiffrement de lecteur BitLocker (C:)

### Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

- Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)
- Chiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

Pour le mode de chiffrement nous avons le choix entre le nouveau mode et le mode compatible, le nouveau sera 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.

## Chiffrement de lecteur BitLocker (C:)

### Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

- Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)
- Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

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

## Chiffrement de lecteur BitLocker (C:)

### Êtes-vous prêt à chiffrer ce lecteur ?

Le chiffrement peut prendre un moment, selon la taille du lecteur.

Vous pouvez continuer à travailler pendant le chiffrement du lecteur, bien que les performances de votre ordinateur puissent être affectées.

Exécuter la vérification du système BitLocker

La vérification du système permet de s'assurer que BitLocker peut lire correctement les clés de récupération et de chiffrement avant de chiffrer le lecteur.

BitLocker redémarrera votre ordinateur avant d'effectuer le chiffrement.

Remarque : cette vérification peut être longue, mais elle est recommandée pour vous assurer que la méthode de déverrouillage sélectionnée fonctionne sans avoir à entrer la clé de récupération.

### **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 finaliser cette partie du TP

---

### **Durcissement AD :**

#### **Introduction :**

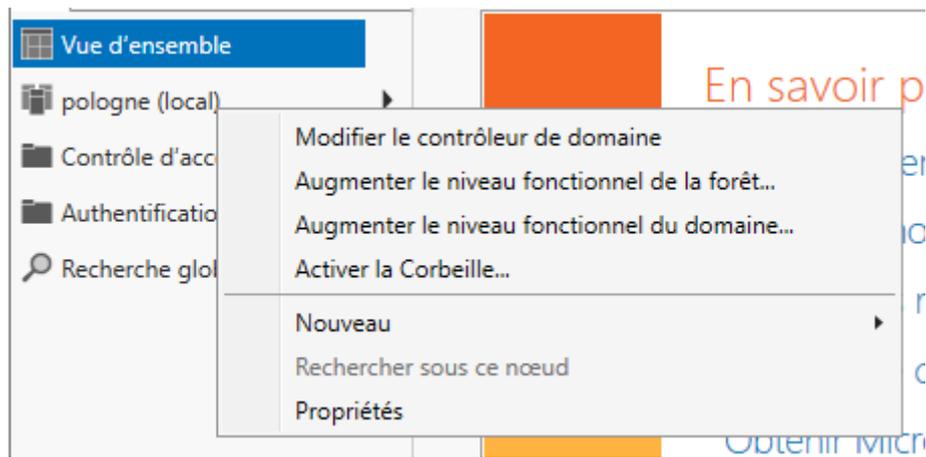
Le but de cette partie du TP est de procéder à une amélioration de sécurité plus centrée sur Active Directory que sur un poste client

#### **TP :**

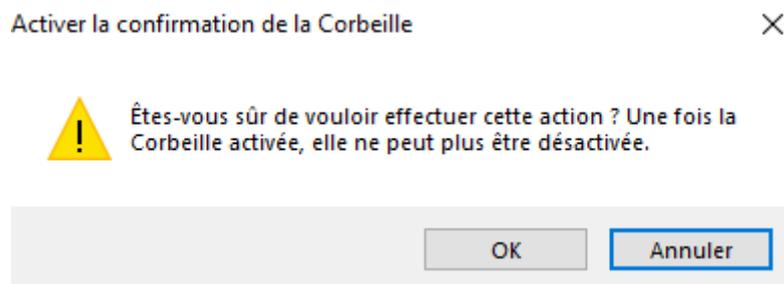
Pour commencer, nous allons activer la corbeille active directory. Pour cela nous allons dans le centre d'administration active directory.

 Centre d'administration Active Directory 08/05/2021 10:15 Raccourci 2 Ko

Sur notre domaine, nous activons la corbeille



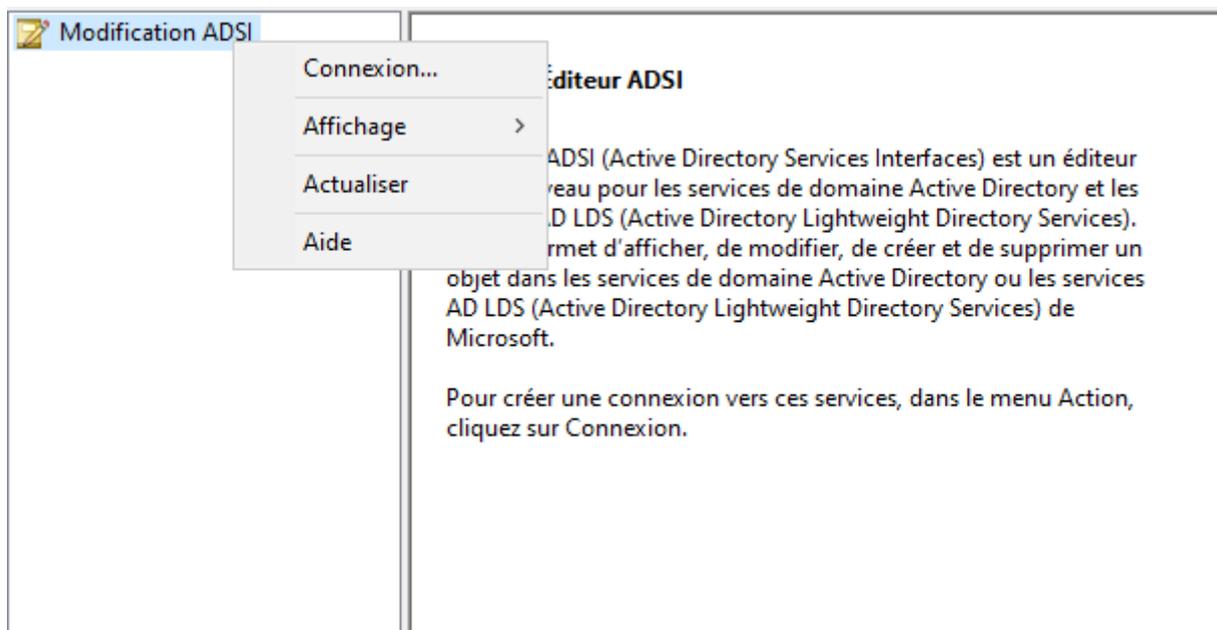
On nous précise bien que dès lors qu'on active la corbeille nous ne pourrons plus la désactiver après



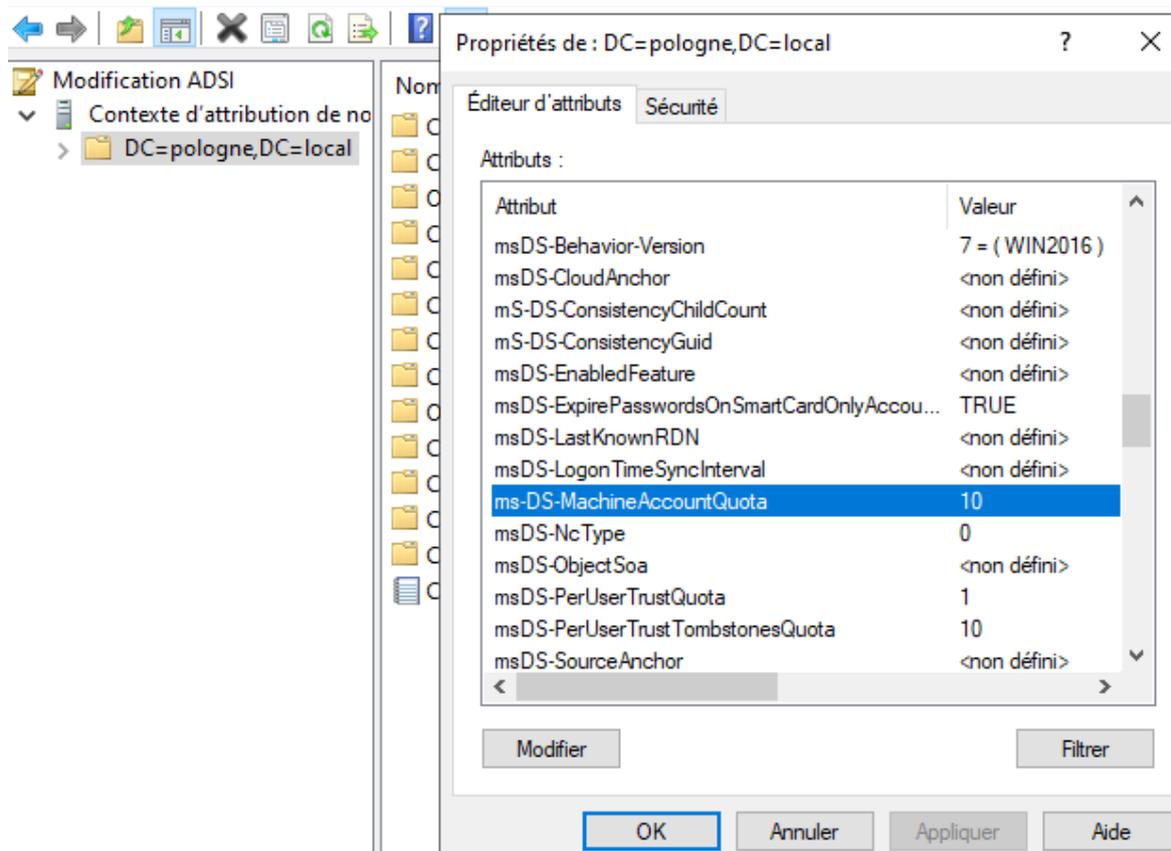
Dans les outils d'administration « modification ADSI »

Icon	Nom	Date	Type	Taille
	Modification ADSI	08/05/2021 10:15	Raccourci	2 Ko
	Module Active Directory...	08/05/2021 10:15	Raccourci	2 Ko

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 paramètres, cela nous connectera automatiquement



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

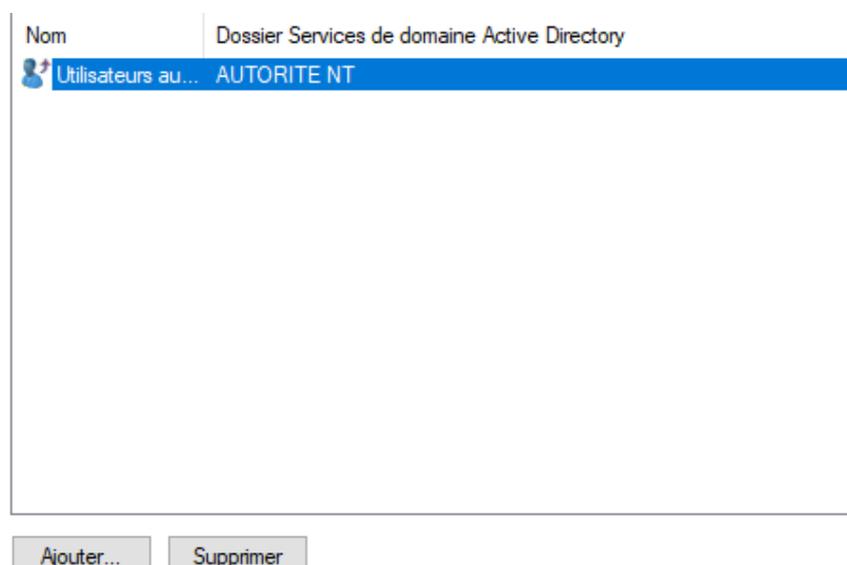


msDS-LogonTimeSyncInterval	<non défini>
<b>msDS-MachineAccountQuota</b>	<b>0</b>
msDS-NcType	0

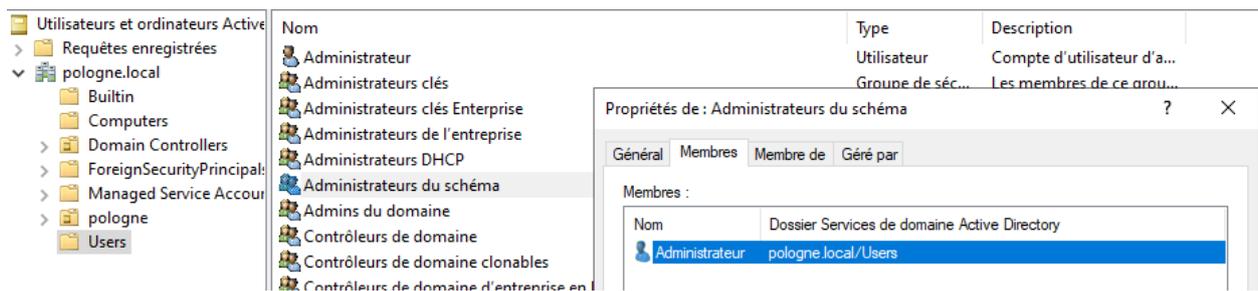
Pour poursuivre, dans les utilisateurs et ordinateurs active directory dans le dossier « builtin » nous avons le groupe « accès compatible pré-windows 2000 » qui sert à la rétrocompatibilité avec les Windows avant 2000 en leur donnant les droits de lecture

Nom	Type	Description
Accès compatible pré-Windows 2000	Groupe de séc...	Un groupe de compati...
Accès DCOM service de certificats	Groupe de séc...	Les membres de ce grou...
Administrateurs	Groupe de séc...	Les membres du groupe...
Administrateurs Hyper-V	Groupe de séc...	Les membres de ce grou...

Nous irons dans les membres et nous supprimerons les utilisateurs authentifié

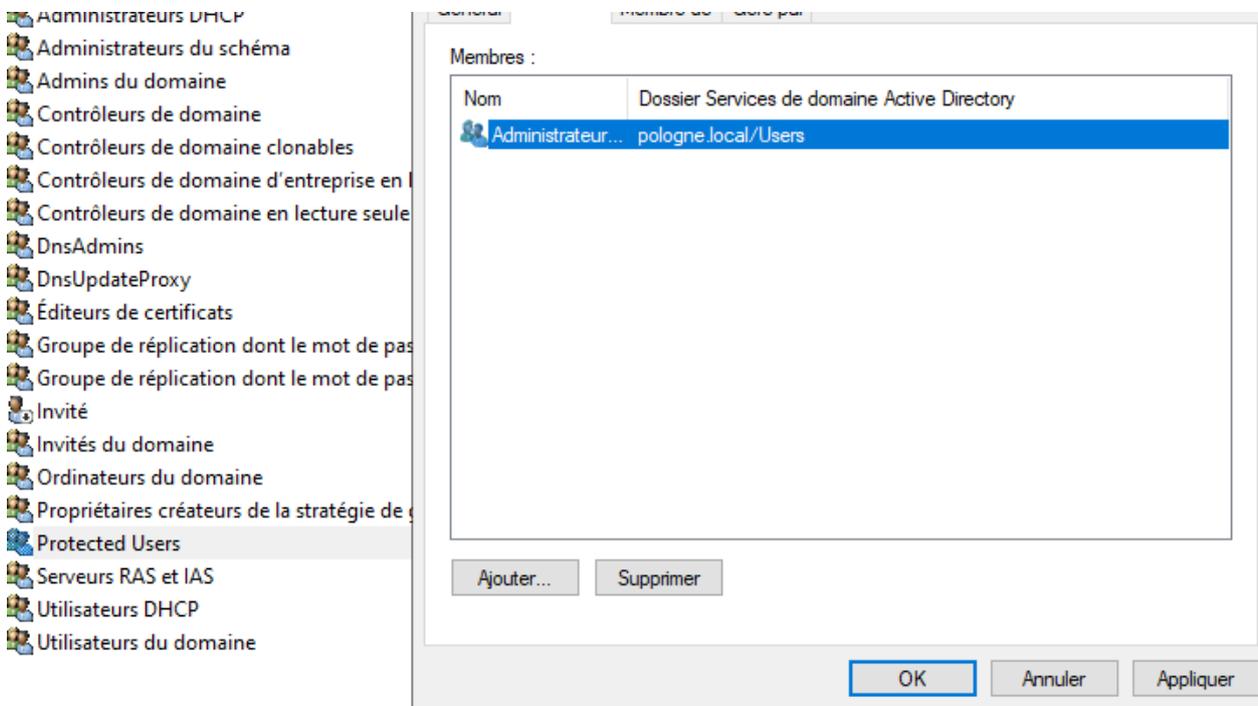


Tout en restant dans le même endroit dans « user » nous pouvons retrouver « utilisateur du schéma » qui permet de modifier, créer ou supprimer des objets sur les serveurs donc lorsque nous n'avons pas besoin d'y toucher nous pouvons supprimer l'administrateur local et si nous aurons besoin de modifier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

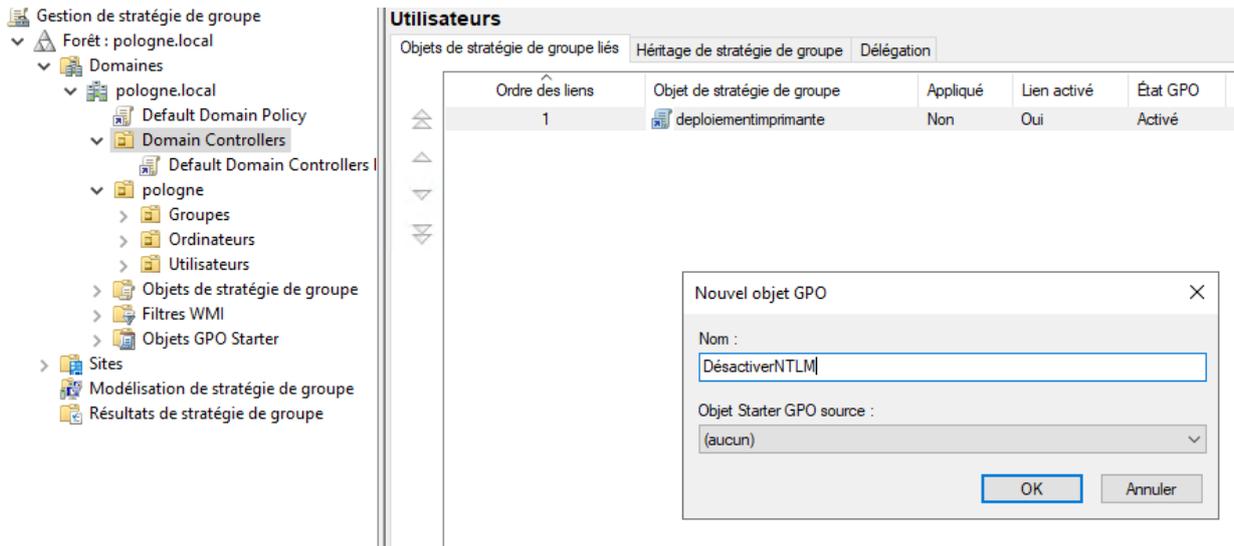


Encore une fois dans les « user » nous pouvons trouver « protected user » qui est l'endroit où l'on peut mettre tous les administrateur nominatif ou bien les utilisateurs sensible, ce groupe permet de ne pas enregistrer dans le cache le mot de passe lors de la connection. Dans notre cas nous allons ajouter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

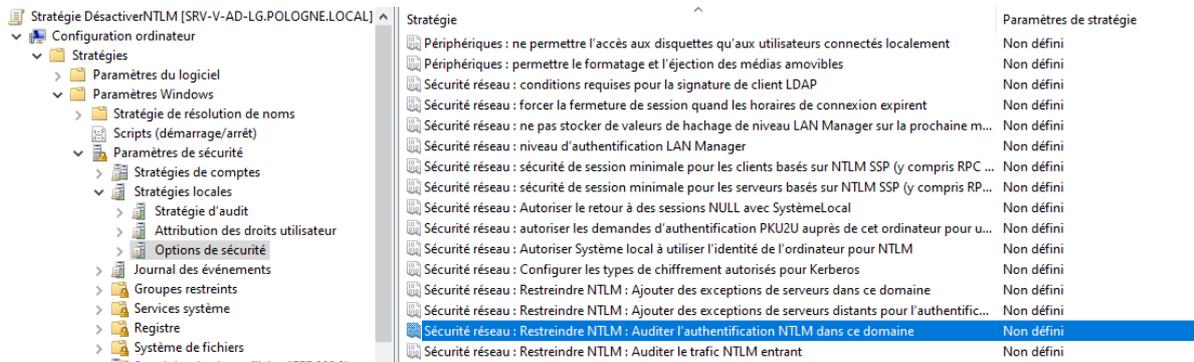
Il faut faire attention aussi lorsqu'un utilisateur protégé veut se connecter en bureau à distance il est possible qu'il doit écrire le nom complet du serveur donc : nom du srv « . » le domaine



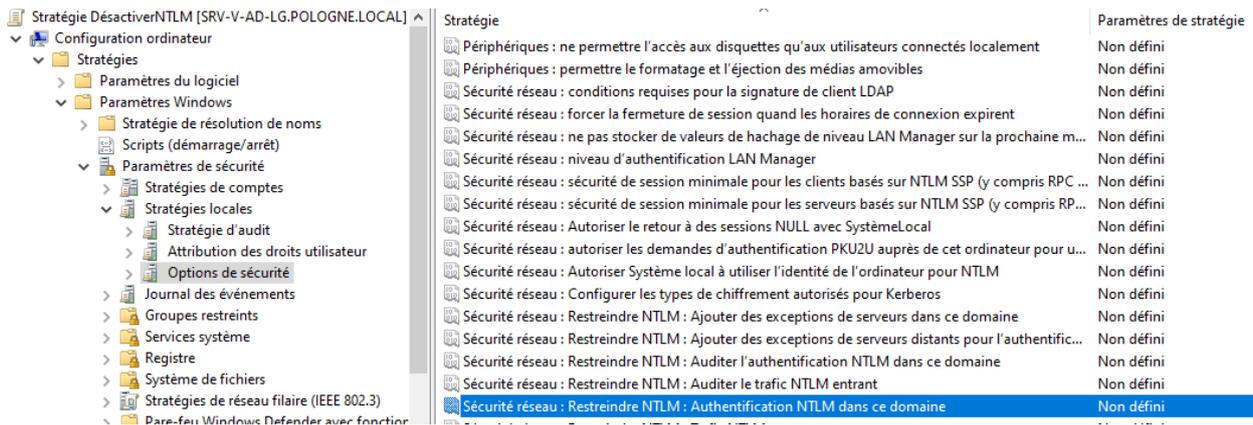
Pour continuer le durcissement de notre serveur, nous pouvons aller dans la gestion des stratégie de groupe et ajouter un GPO nommé « désactiverNTLM » qui va nous désactiver les anciens protocoles d'authentification (NTLM v1 et v2), il est d'abord nécessaire de vérifier qu'aucun logiciel n'utilise ce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

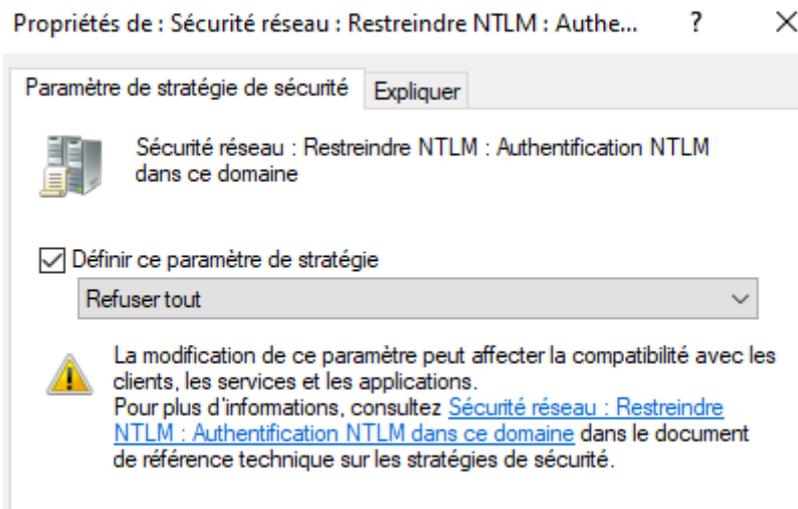


Pour vérifier si il nous reste de l'authentification via NTLM, nous pouvons laisser tourner la stratégie de groupe qui permet d'auditer toute les authentifications NTLM pendant 15 jours a 1 mois afin d'être sur qu'il n'y a aucune trace du NTLM dans l'observateur d'événement.



Dès lors ou nous n'avons plus de trace de cette authentification nous pouvons 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.

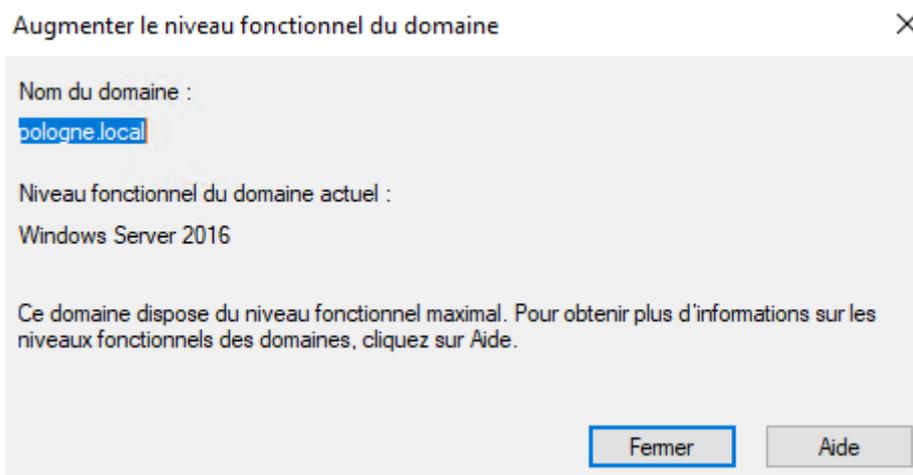
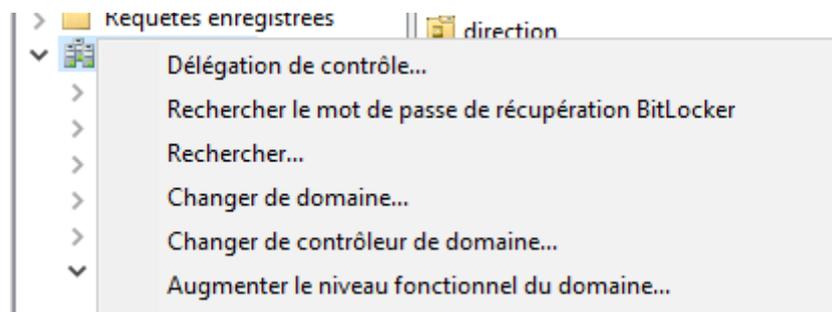
---

## Gestion de l'authentification local LAPS :

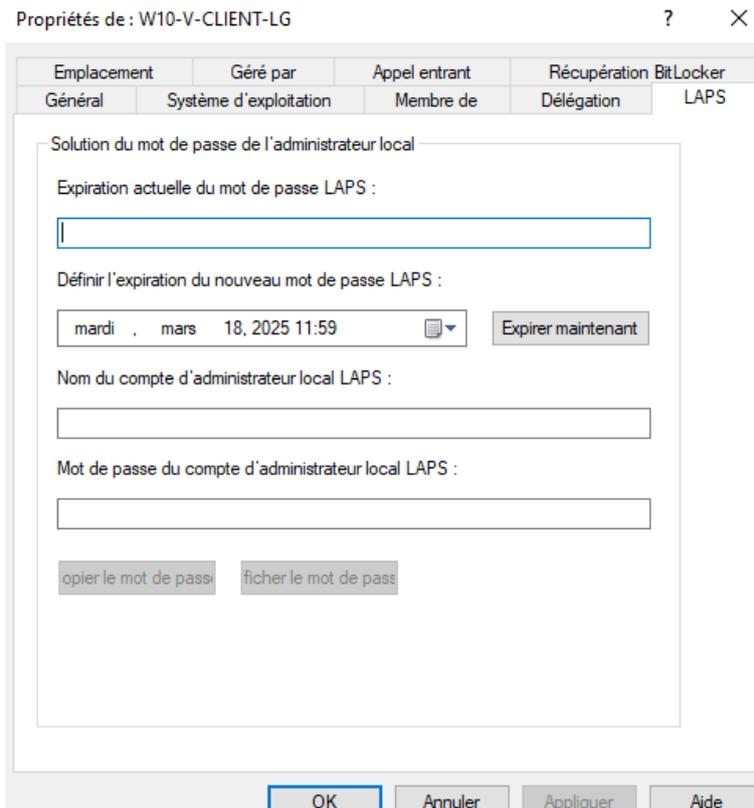
### Introduction :

### TP :

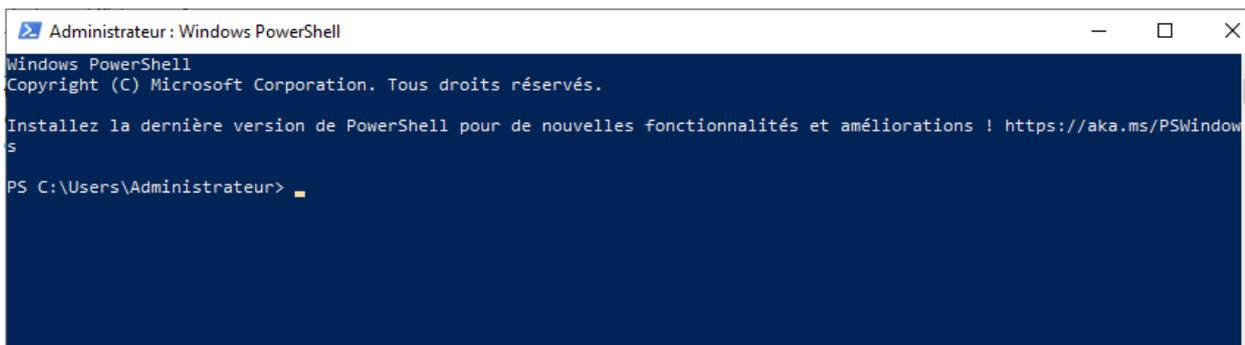
Pour débiter, nous allons voir le niveau fonctionnel de notre domaine est assez élever. Dans les utilisateur active directory nous faisons un clique droit sur le domaine et cliquons « augmenter le niveau fonctionnel du domaine » Notre serveur a un niveau fonctionnel de 2016 ce qui est le maximum a la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



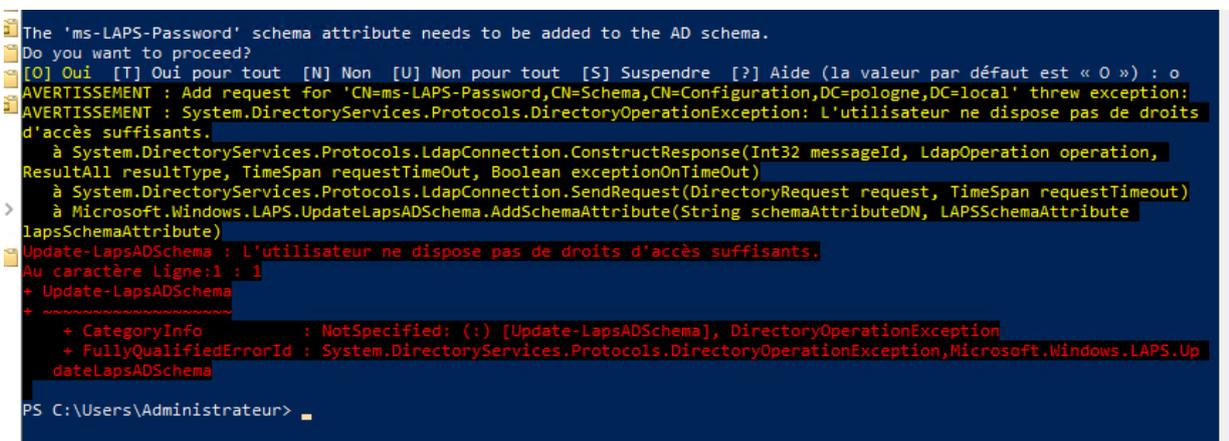
Quand nous allons dans les propriétés d'un ordinateur nous pouvons voir l'onglet LAPS qui n'est pas encore paramétré



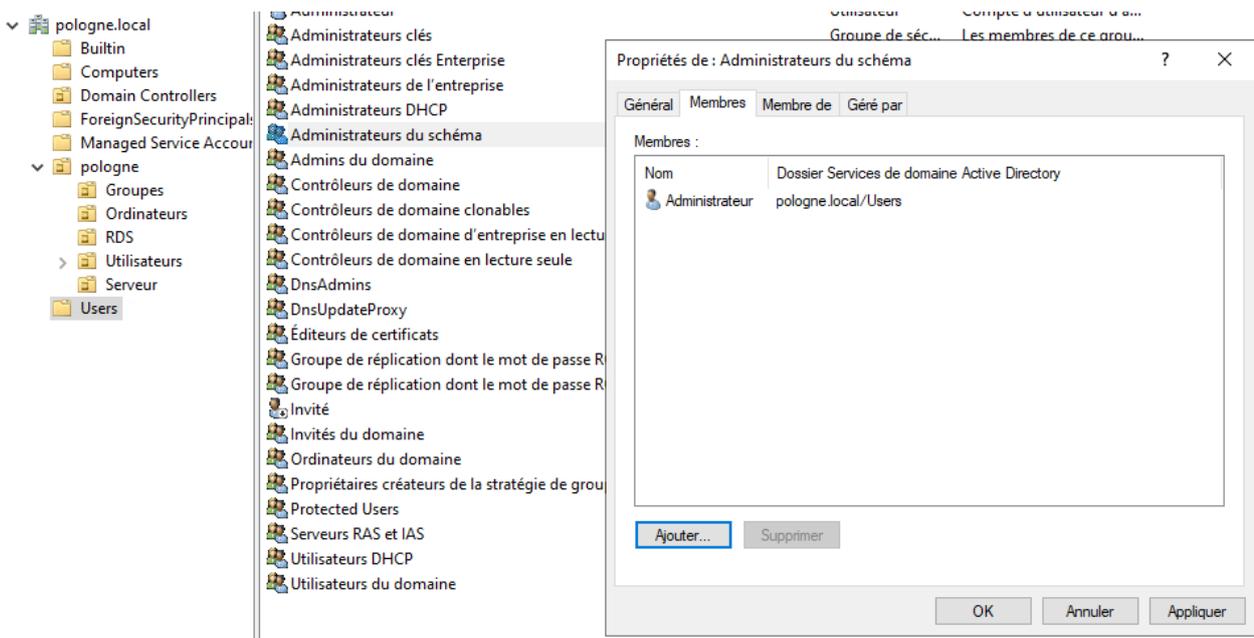
La première étape du paramétrage du schéma active directory sera lancer une fenêtre powershell en administrateur



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

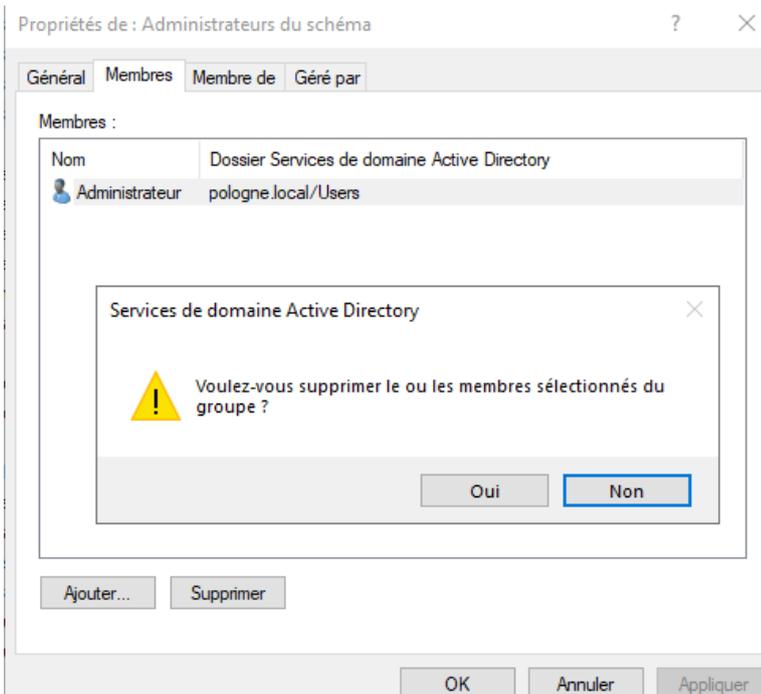


Nous voyons que nous n'avons plus d'erreur, nous pouvons mettre « t » pour dire oui à tout

```

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?
[0] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « 0 ») : o
The 'ms-LAPS-PasswordExpirationTime' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[0] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « 0 ») : t
  
```

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



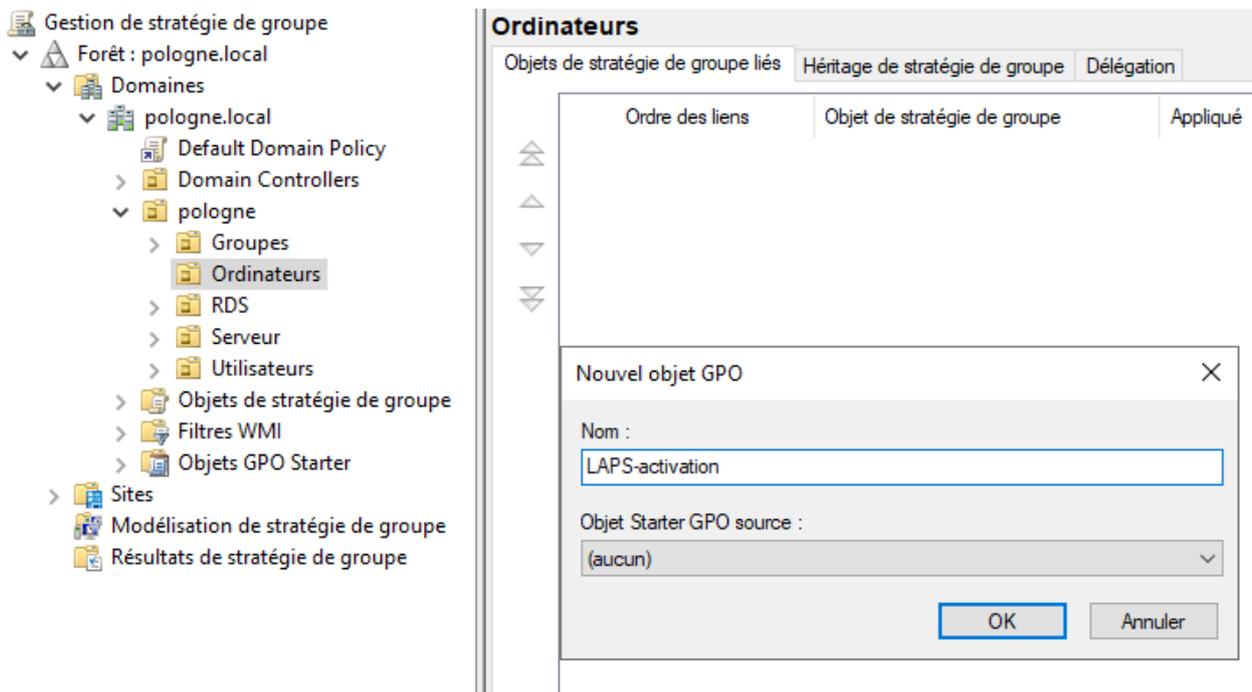
La mise a jour du schéma nous affiche maintenant dans l'éditeur d'attribut nous pouvons voir maintenant les attribut « msLAPS »

```

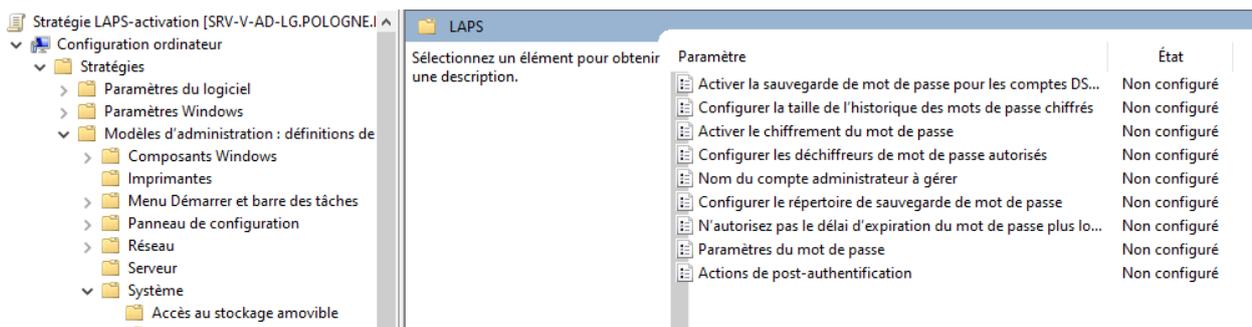
msimaging-Ihumbpnn... <non défini>
msLAPS-EncryptedD... <non défini>
msLAPS-EncryptedD... <non défini>
msLAPS-EncryptedP... <non défini>
msLAPS-EncryptedP... <non défini>
msLAPS-Password <non défini>
msLAPS-PasswordEx... <non défini>

```

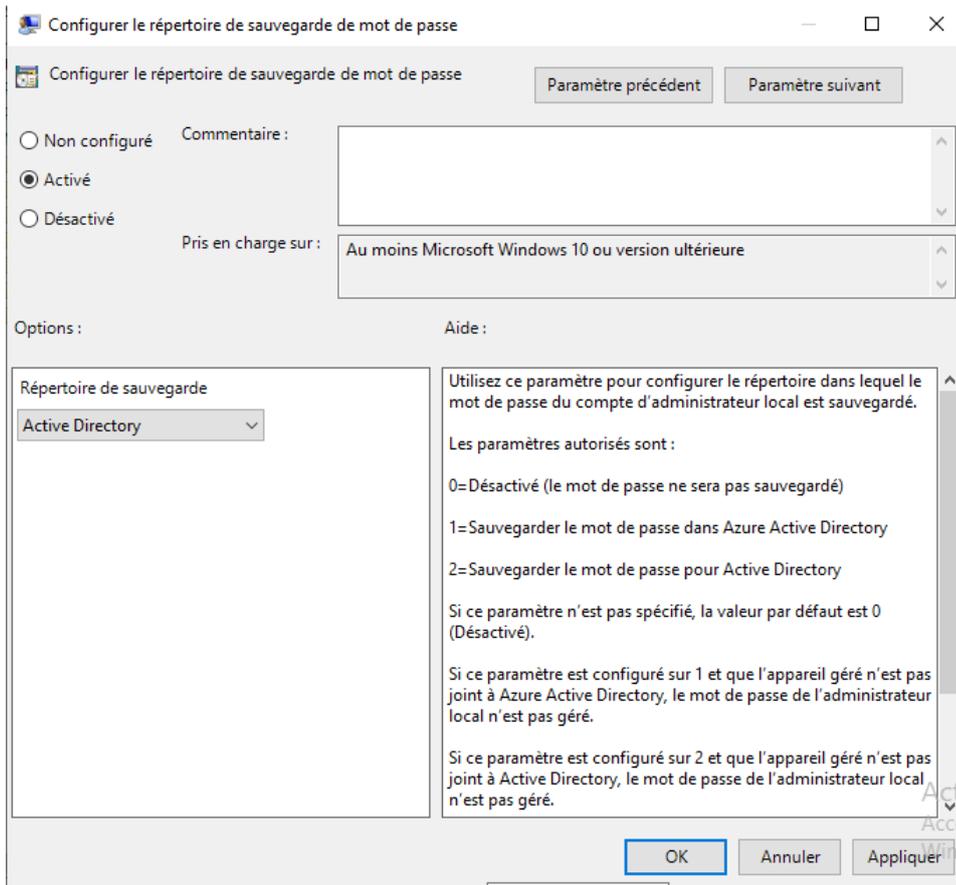
Le paramétrage a été effectué, la deuxième étape est l'administration via stratégie de groupe ou nous allons créer un GPO sur l'OU ordinateur. Je l'ai nommé « LAPS-activation ».



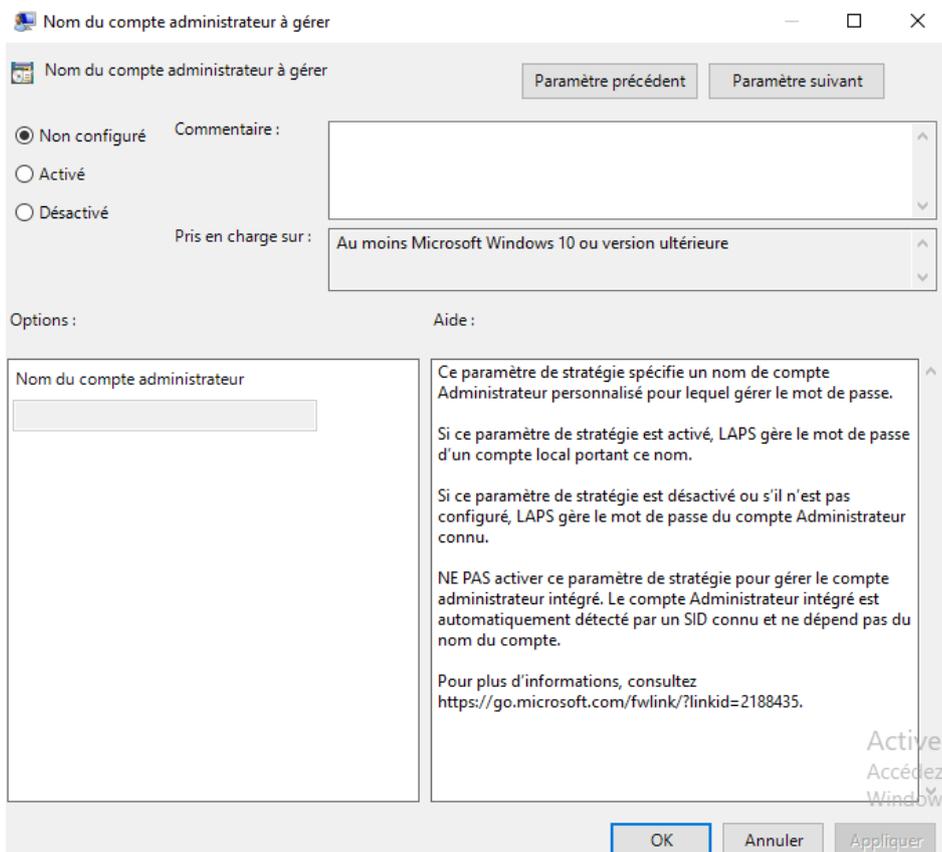
Nous la modifions et allons dans config ordi → stratégie → modèles d'administration → Système → LAPS



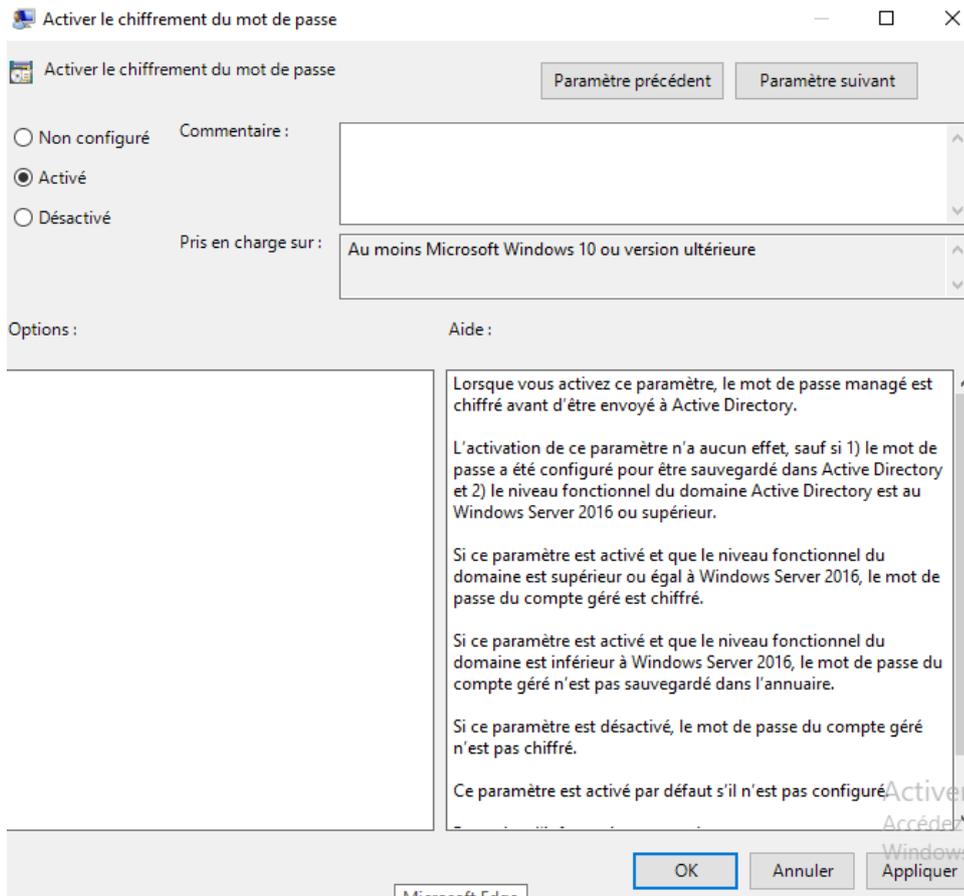
Vue que notre LAPS n'est que installé pour le moment. Il faudra donc l'activer, pour l'activer nous activerons « configurer le répertoire de sauvegarde de mot de passe » et choisissons ou stocker. Dans notre cas ce sera active directory car nous somme en local



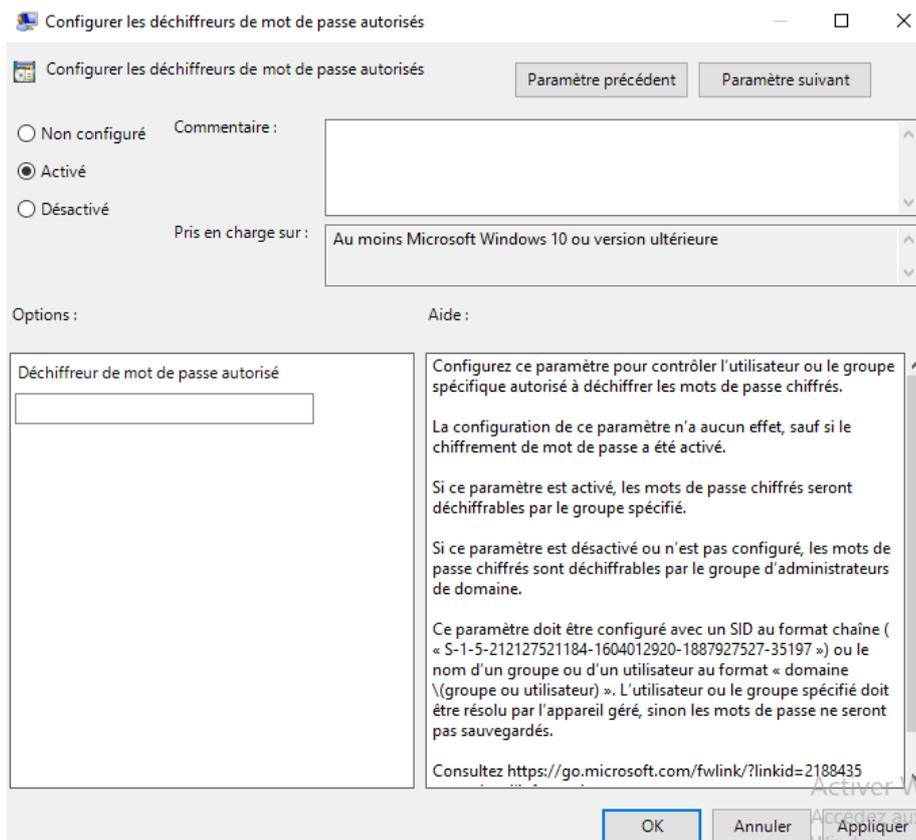
Par rapport à la configuration nous pouvons choisir l'option « nom du compte administrateur à gérer ». en l'activant nous pourrions rentrer le nom que l'on a donné aux comptes administrateur sur les postes. Dans notre cas ça ne sera pas utile.



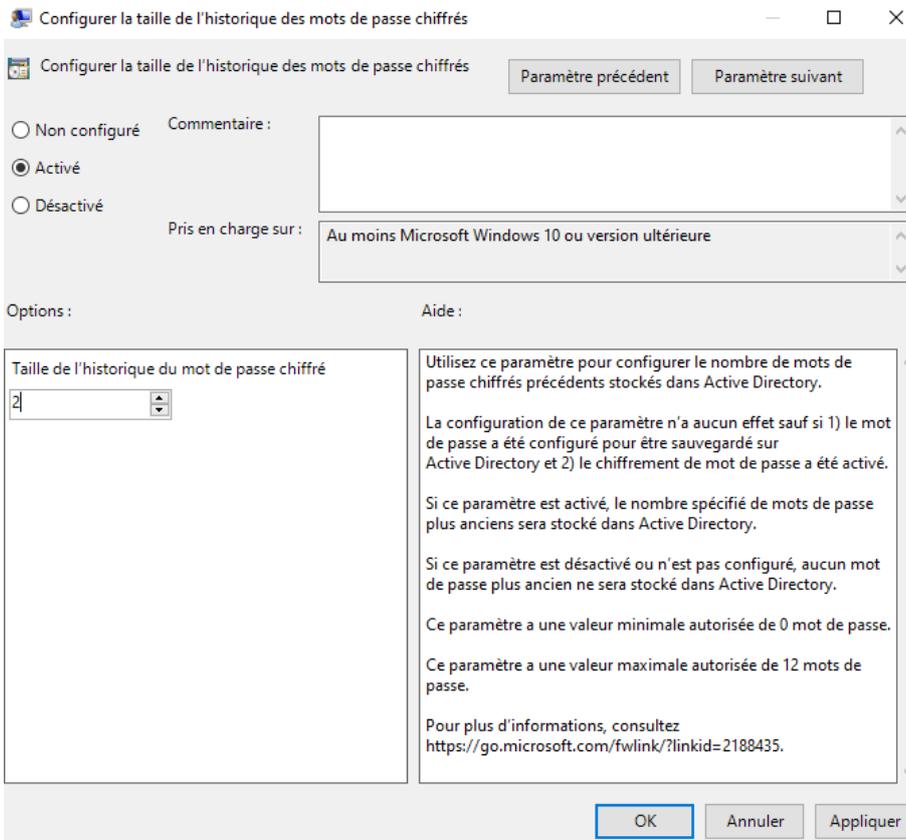
Pour sécuriser le stockage des mots de passe dans active directory, nous activons le chiffrement des mot de passe



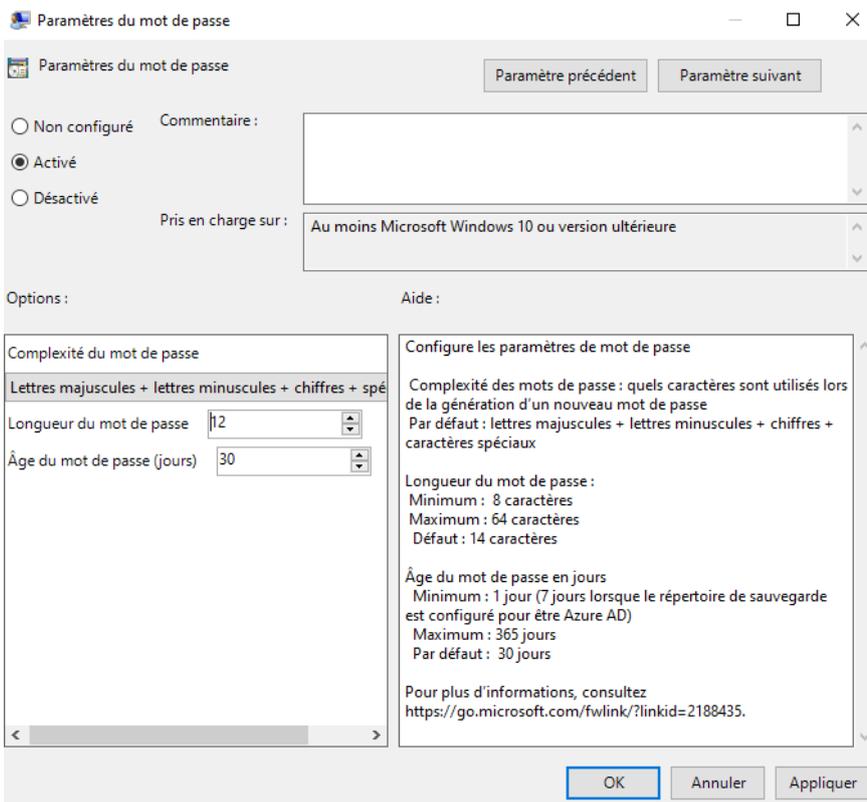
Si nous activons l'option ci-dessus, il faudra alors dire qui pourra les déchiffrer grâce à « configurer les déchiffreur de mot de passe autorisés » par défaut ce sont les admin du domaine si nous ne l'activons pas



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'âge dépendra 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" »