# Table des matières

# PRESENTATION

Pour mettre en place cette GPO, il existe 2 solutions développés par Microsoft : Windows LAPS et LAPS Legacy.

Windows LAPS est un composant intégré à Windows, c'est la nouvelle solution développée par Microsoft pour la gestion des mots de passes d'Administrateur locaux des postes. Elle fait suite à LAPS Legacy. Windows LAPS apporte plusieurs nouveautés comme le fait qu'il est intégré directement à Windows, il n'y a pas d'agent à installer contrairement à LAPS Legacy

Nouveautés de Windows LAPS :

- Pas d'agent à installer
- Les mots de passe peuvent être stockés dans l'AD et être chiffrés
- Possibilité de configurer l'historique des mots de passe
- La possibilité de mettre en place une rotation de mots de passe
- Le mot de passe de restauration des services d'annuaire Active Directory (DSRM) peut être géré
- Un nouvel onglet « LAPS » prendra place dans les propriétés des objets ordinateurs
- Nouvelle GPO pour Windows LAPS
- Un nouveau module Powershell

Les Prérequis pour Windows LAPS :

Les systèmes d'exploitation **compatibles**

- Windows 11 21H2 et Windows 11 22H2 (Pro, Education, Enterprise)
- Windows 10 (Pro, Education, Enterprise)
- Windows Server 2022 (y compris en mode Core)
- Windows Server 2019

A Savoir : Malgré que l'OS soit compatible il faut surtout installer la mise à jour cumulative d'avril 2023, c'est elle qui a pour effet d'ajouter le composant Windows LAPS

Ce qui implique d'installer au minima les mises à jour suivantes :

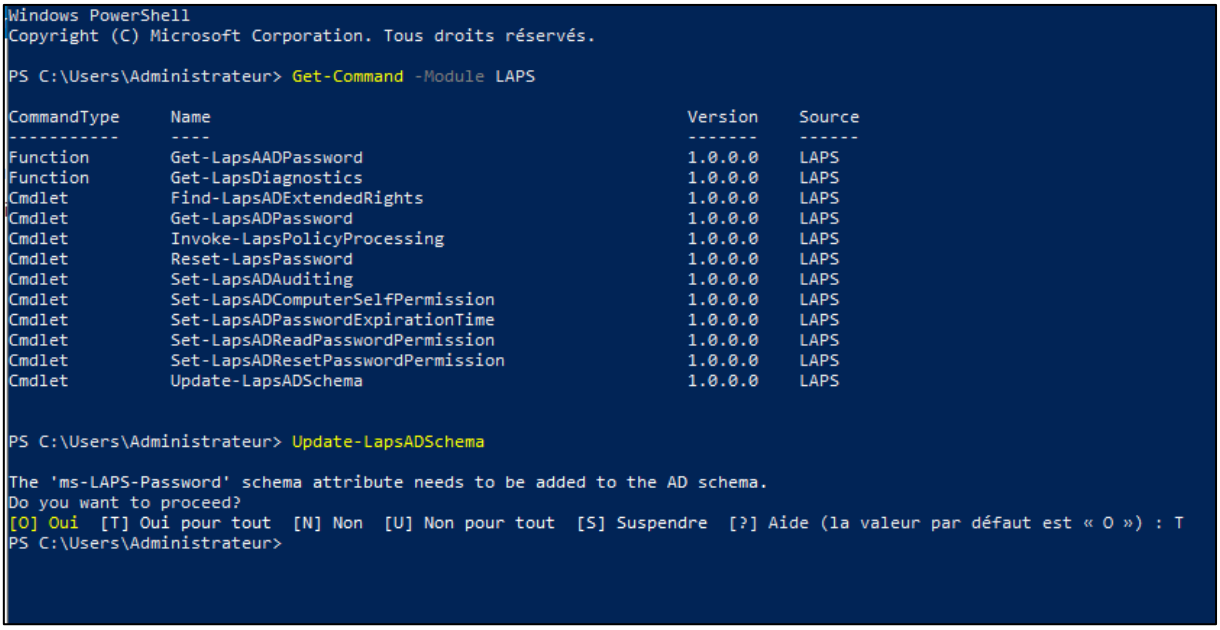
- Windows 11 22H2 : KB5025239
- Windows 11 21H2 : KB5025224
- Windows 10 20H2, 21H1, 21H2 et 22H2 : KB5025221
- Windows Server 2022 : KB5025230
- Windows Server 2019 : KB5025229

Il est conseillé de mettre à jour les machines à gérer avec Windows LAPS et aussi de mettre à jour les contrôleurs de domaine.

# 1. CONFIGURATION DE WINDOWS LAPS

## 1.1/ Mettre à jour le schéma Active Directory pour Windows LAPS

Maintenant que tous les systèmes sont à jour, il faut mettre à jour le schéma de l'AD, d'abord il faut vérifier que le module LAPS soit installé. Pour cela il faut entrer cette suite de commande et avoir le même résultat que moi.




Si le module n'est pas installé :

On importe ensuite le module LAPS avec les commandes suivantes :

« Install-Module LAPS » & « Import-Module LAPS »

Pour terminer nous allons lancer l'update du schéma de l'AD, bien penser à faire une sauvegarde de l'Active Directory pour éviter d'éventuels problèmes, pour cela entrer cette commande :

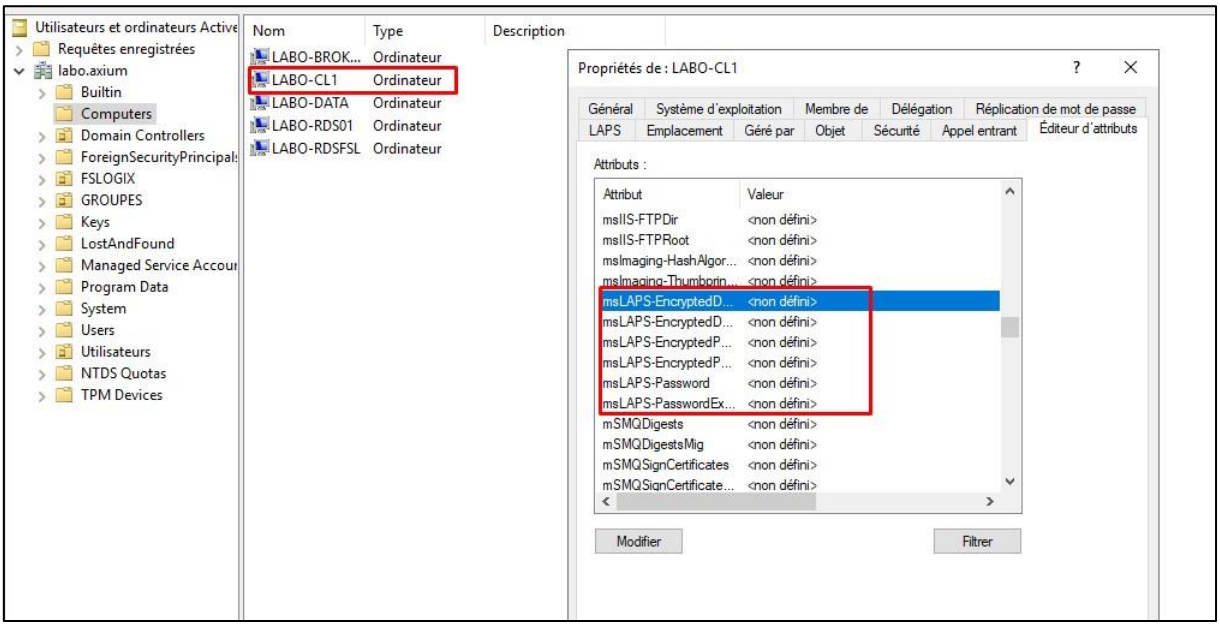
« Update-LapsADSchema »

## 1.2/ Vérification de l'ajout des attributs LAPS

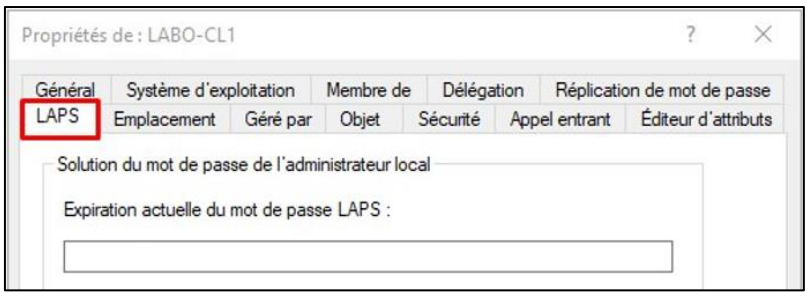
Normalement le schéma à été mis à jour, on peut désormais aller dans les propriétés d'un poste pour vérifier :

Les attributs ci-dessous apparaissent :

- msLAPS-PasswordExpirationTime
- msLAPS-Password
- msLAPS-EncryptedPassword
- msLAPS-EncryptedPasswordHistory
- msLAPS-EncryptedDSRMPassword
- msLAPS-EncryptedDSRMPasswordHistory




Aussi, il y a un onglet « LAPS » qui a apparu dans les mêmes propriétés, c'est ici que les infos sur le compte Administrateur se retrouveront (mot de passe, nom du compte, et expiration du mot de passe).



## 1.3/ Attribuer les droits d'écriture aux machines

Pour permettre aux postes de transmettre leurs informations lié à Windows LAPS à l'AD, il faut leurs attribuer des droits d'écriture et de modification dans leurs objets correspondants.

Dans mon cas je vais utiliser mon dossier « Computers » ou sont tous mes postes pour leurs attribuer des droits

La commande ci-dessous donne la permission au dossier « Computers » ou sont tous mes postes, j'ai renseigné le DN (DistinguishedName) pour éviter d'éventuels erreurs.

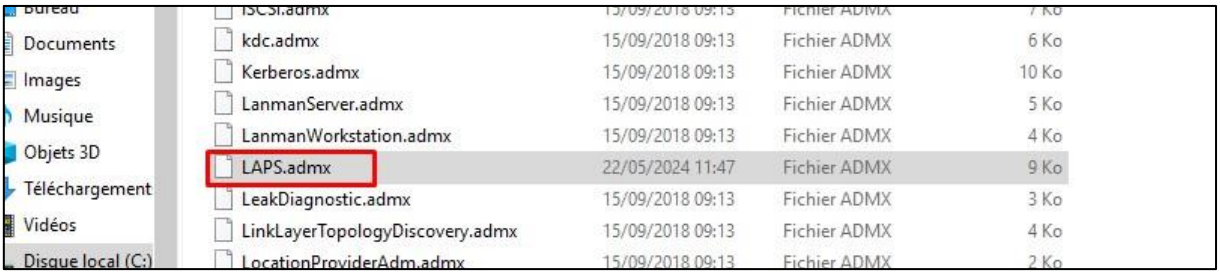
```
PS C:\Users\Administrateur> Set-LapsADComputerSelfPermission -Identity "CN=Computers,DC=labo,DC=axium"

Name      DistinguishedName
----      -----------------
Computers CN=Computers,DC=labo,DC=axium
```

## 1.4/ Importation des modèles d'administration Windows LAPS

La prochaine étape consiste à paramétrer Windows LAPS à l'aide d'une stratégie de groupe. Cette GPO permettra de définir la politique de mots de passe à appliquer sur le compte administrateur géré, l'emplacement de sauvegarde du mot de passe (Active Directory dans notre cas), ainsi que le nom du compte administrateur à gérer avec Windows LAPS.

En premier lieu, il est nécessaire d'importer les modèles d'administration (ADMX) de Windows LAPS (*ceci est requis s'il existe déjà un magasin central dans votre domaine, car Windows ne lira pas le magasin local*). Ce processus n'est pas automatique. Sur le contrôleur de domaine, on doit récupérer deux fichiers:

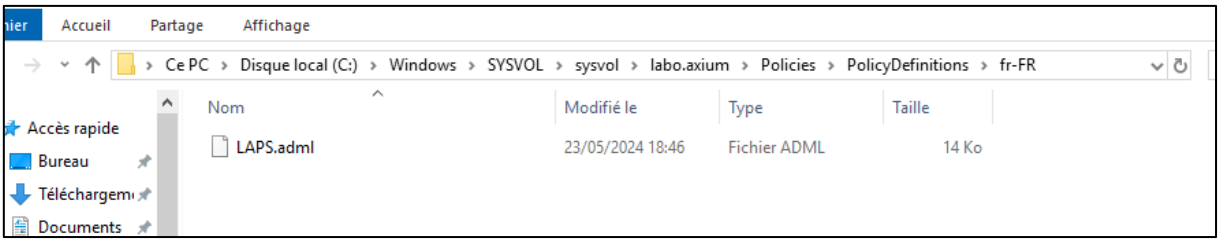
1er fichier : Dans « C:\Windows\PolicyDefinitions\LAPS.admx » qui correspond aux modèles d'administration de Windows LAPS



Ce fichier est à déposer dans le magasin central du partage SYSVOL, dans mon cas ici :


2ième fichier : Dans « C:\Windows\PolicyDefinitions\fr-FR\LAPS.adml » qui correspond au fichier de langue FR du fichier ADMX

Déposer ce fichier ici : dans le répertoire "fr-FR" pour le fichier de langue.




Désormais, une nouvelle GPO est disponible et peut être configuré.

## 1.5/ Configuration de la GPO

Je crée une GPO nommé « Windows LAPS », je parcours ce chemin et je configure comme tel :

Dans l'éditeur de gestion des stratégies de groupe -> Configuration Ordinateur -> Stratégies -> Modèle d'administration -> Système -> LAPS

- **Configurer le répertoire de sauvegarde de mot de passe** – Activer et choisir comme répertoire de sauvegarde « Active Directory »

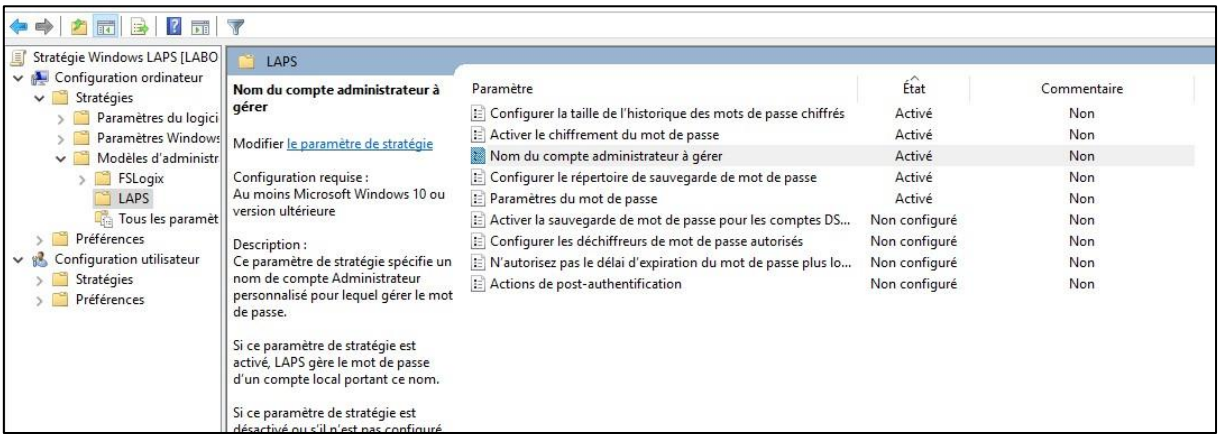
- **Paramètres du mot de passe** – Activer et définir la longueur et l'âge du mot de passe souhaité

- **Configurer la taille de l'historique des mots de passe chiffrés** – Activer et définir sur 1, permet de lire le mot de passe actuel et le précèdent, pratique en cas de bug.

- **Activer le chiffrement du mot de passe** -- Activer, le mot de passe ne sera pas stocké en clair

- **Nom du compte administrateur à gérer** – Activer, permet de spécifier un nom de compte Administrateur personnalisé pour lequel gérer le mot de passe, le compte Administrateur intégré est automatiquement reconnu grâce à son SID. Dans mon cas je rentre « Utilisateur ». Windows LAPS est capable de gérer uniquement 1 compte par poste.

Voici à quoi ressemble la GPO :



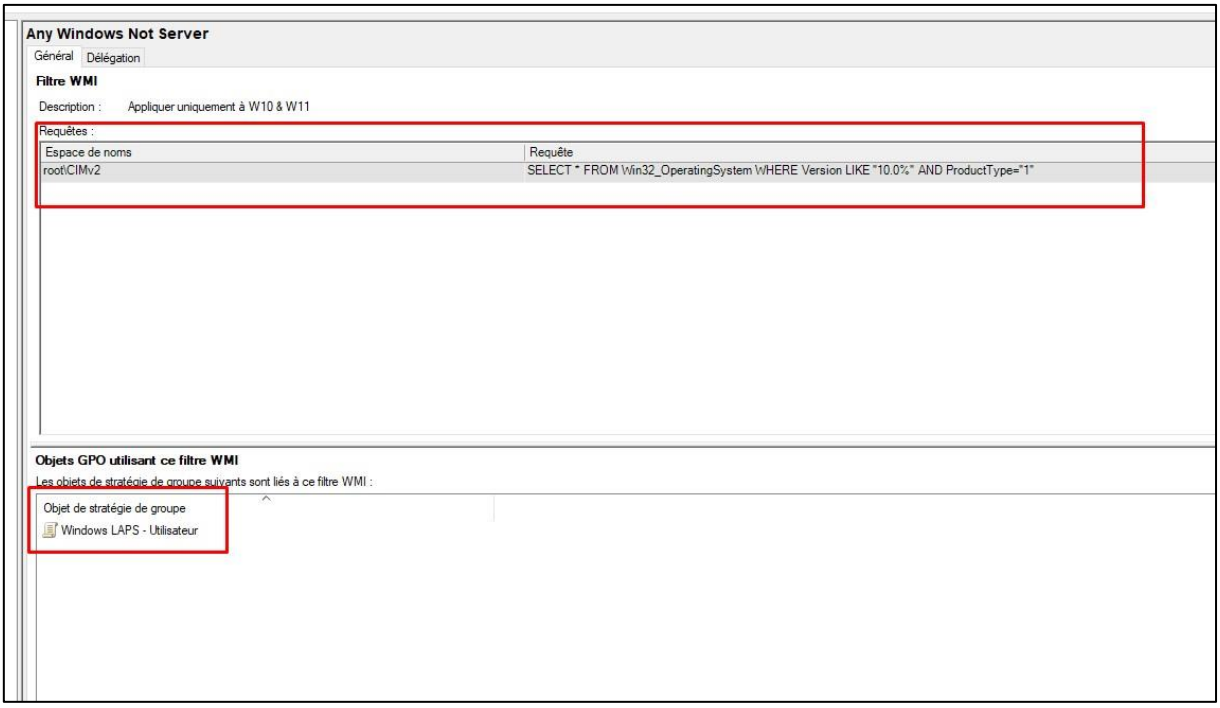

La GPO est placé à la racine du domaine.

## 1.6/ Filtrage WMI

Etant donné que ma GPO agit sur la totalité des machines de mon domaine, je dois mettre en place un filtrage WMI pour que celui-ci filtre les OS concerné par la GPO.

Nous voulons contrôler uniquement les mots de passe des postes clients W11 – W10 dans notre cas en excluant les différents serveurs Windows que composent l'infra AXIUM.

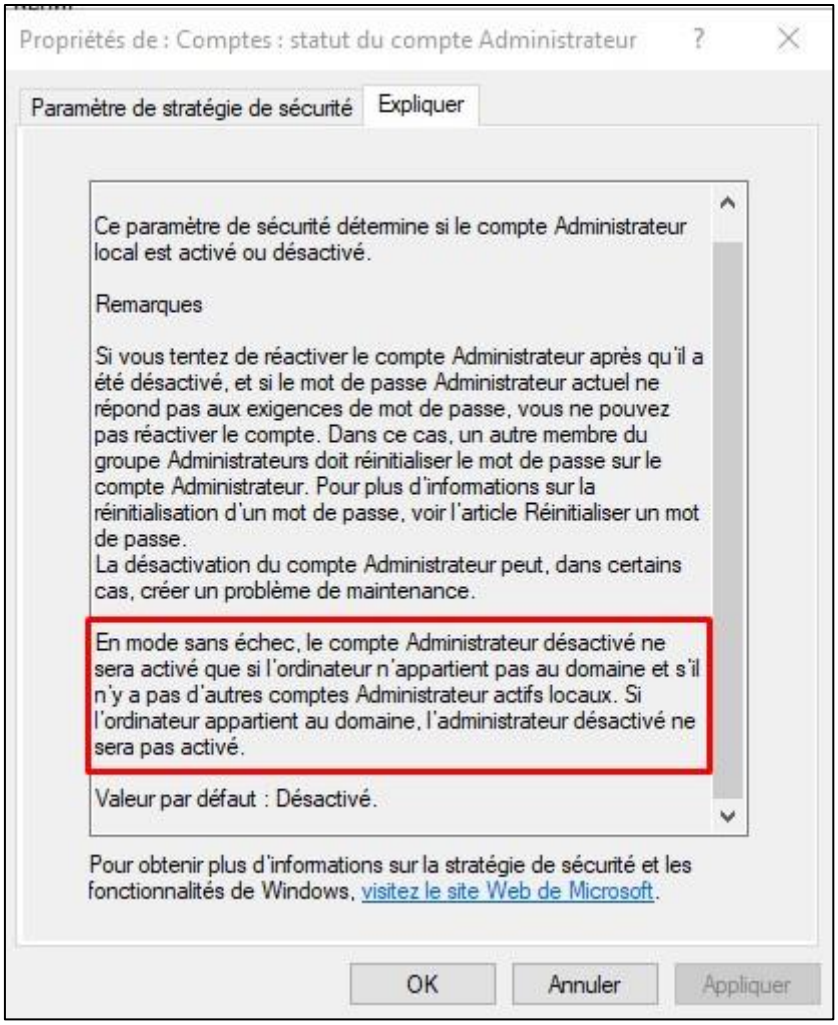
Pour cela le filtre WMI suivant a été mis en place pour que la GPO s'applique uniquement aux O.S Windows 10 et 11.



**A SAVOIR** :

Dans mon cas sur les postes il y'a generalement 2 utilisateurs membres du groupe « Administrateurs » local, par défaut le compte Administrateur intégré à Windows est désactivé et peut-être activé en mode sans echec. Donc le resonnement classique est de dire que c'est un grosse faille de sécurité, oui mais non car le compte Administrateur intégré est désactivé et ne peut pas être réactive en mode sans echec si un autre utilisateur local est présent dans le groupe « Administrateurs » des postes.

Explication de Microsoft :

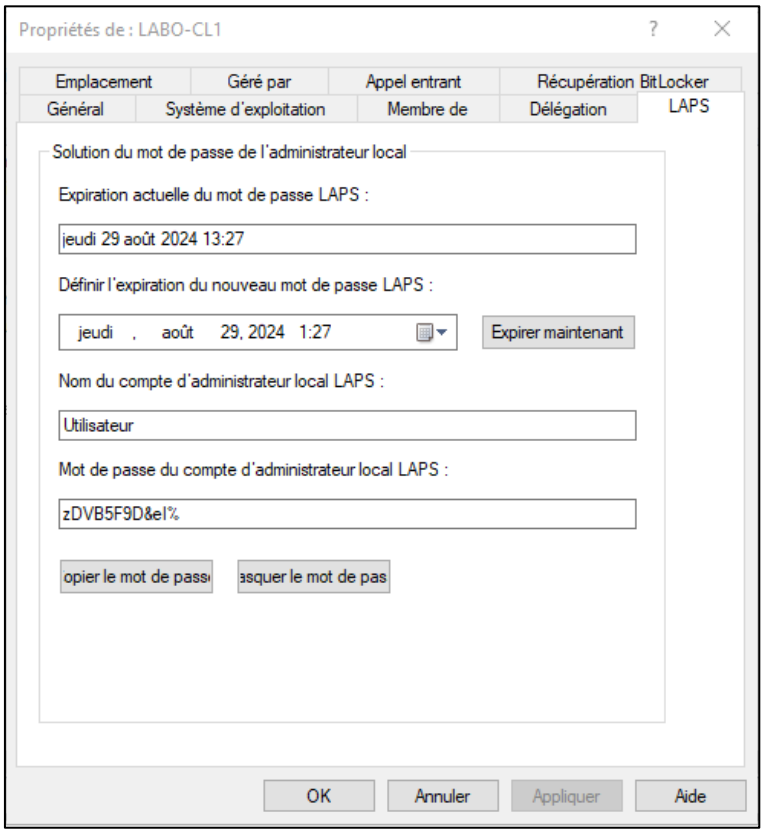


## 1.7/ Résultats

Le temps d'application de Windows LAPS dépend de celui de la GPO, donc si l'on veut forcer la mise en place de la GPO sur un poste on doit faire un « gpupdate /force » puis un redémarrage.

**Récupération des informations de Windows LAPS :**

Dans les propriétés d'un poste puis dans l'onglet « LAPS », on peut apercevoir le mot de passe du compte « Utilisateur » dans mon cas (voir image), il faut être autorisé à déchiffrer le mot de passe car celui-ci est chiffré.




On peut également consulter la date d'expiration du mot de passe, mais aussi forcer la réinitialisation de celui-ci via le bouton « Expirer maintenant ». Le mot de passe sera remplacé au prochain démarrage du poste client.

Windows LAPS est desormais configuré et fonctionnel.

## 1.8/ Divers Commandes Powershell

**Forcer le changement de mot de passe LAPS :** Sur le poste client après un « gpupdate /force », il faut entrer cette commande pour forcer la mise en place de Windows LAPS :

« Invoke-LapsPolicyProcessing » ou “Reset-LapsPassword”

**Récupérer le mot de passe généré par Windows LAPS :** Depuis le contrôleur de domaine, entrer cette commande pour récuperer le mot de passe LAPS d’un poste souhaité (dans ce cas « LABO-CL1 »). L’option « -AsPlainText » permet d’affiche le mot de passe en clair car de base il est chiffré (neccesite une autorisation). L’option « -IncludeHistory » permet d’afficher l’historique des mots de passe selon le paramètrage de la GPO.

« Get-LapsADPassword " LABO-CL1 " -AsPlainText -IncludeHistory »

```
PS C:\Users\Administrateur> Get-LapsADPassword "LABO-CL1" -AsPlainText -IncludeHistory


ComputerName        : LABO-CL1
DistinguishedName   : CN=LABO-CL1,CN=Computers,DC=labo,DC=axium
Account             : Utilisateur
Password            : zDVB5F9D&eI%
PasswordUpdateTime  : 31/05/2024 13:27:13
ExpirationTimestamp : 29/08/2024 13:27:13
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : LABO\Admins du domaine

ComputerName        : LABO-CL1
DistinguishedName   : CN=LABO-CL1,CN=Computers,DC=labo,DC=axium
Account             : Utilisateur
Password            : iQ2R7w}q07YI
PasswordUpdateTime  : 31/05/2024 13:02:38
ExpirationTimestamp :
Source              : EncryptedPasswordHistory
DecryptionStatus    : Success
AuthorizedDecryptor : LABO\Admins du domaine
```

**Autoriser une entité à déchiffrer les mots de passe Windows LAPS :** Par défaut seuls les membres du groupe « Admins du domaine » sont autorisés à déchiffrer les mots de passes, pour changer cela entrer cette commande :

« Set-LapsADReadPasswordPermission -Identity "OU=X,DC=labo,DC=axium" “

Ce n’est pas terminé, il est aussi necessaire de modifier la GPO, le paramètre "Configurer les déchiffreurs de mot de passe autorisés" doit être activé.