Mireille GUETCHO YOMPA

# DÉPLOYER ET CONFIGURER MICROSOFT LAPS

## SOMMAIRE

**I – Définition et les fonctionnalités de LAPS**
**II – Les prérequis de LAPS**
**III – Mise en place de LAPS dans un service de domaine Active Directory**
**IV – La configuration de la GPO LAPS**

## I -Définition et fonctionnalités de LAPS

LAPS, pour **Local Administrator Password Solution**, est un outil gratuit proposé par Microsoft et qui va venir se greffer sur le domaine Active Directory pour renforcer la sécurité des comptes " Administrateur " locaux de vos postes de travail et serveurs.
L'objectif étant mieux gérer les identités sur les machines de votre système d'information afin de renforcer la sécurité.
La solution Microsoft LAPS va offrir aux administrateurs systèmes des fonctionnalités clés afin de gérer le mot de passe des comptes administrateurs locaux des machines :

- Générer des mots de passe uniques et robustes pour chaque compte administrateur local
- Définir la durée d'expiration des mots de passe associés à ces comptes
- Définir la complexité des mots de passe associés à ces comptes
- Régénérer automatiquement un mot de passe quand il expire

## II – Les prérequis de LAPS

Afin de pouvoir déployer la solution Microsoft LAPS, vous devez disposer d'un annuaire Active Directory et utiliser les versions de Windows (desktop) et Windows Serveur prise en charge.
Pour la suite de ce TP, vous avez besoin de deux machines au minimum, à savoir :

. Un contrôleur de domaine Active Directory
. Un poste de travail sous Windows

Pour ma part je vais utiliser les deux machines virtuelles suivantes :
Serveur (DC)

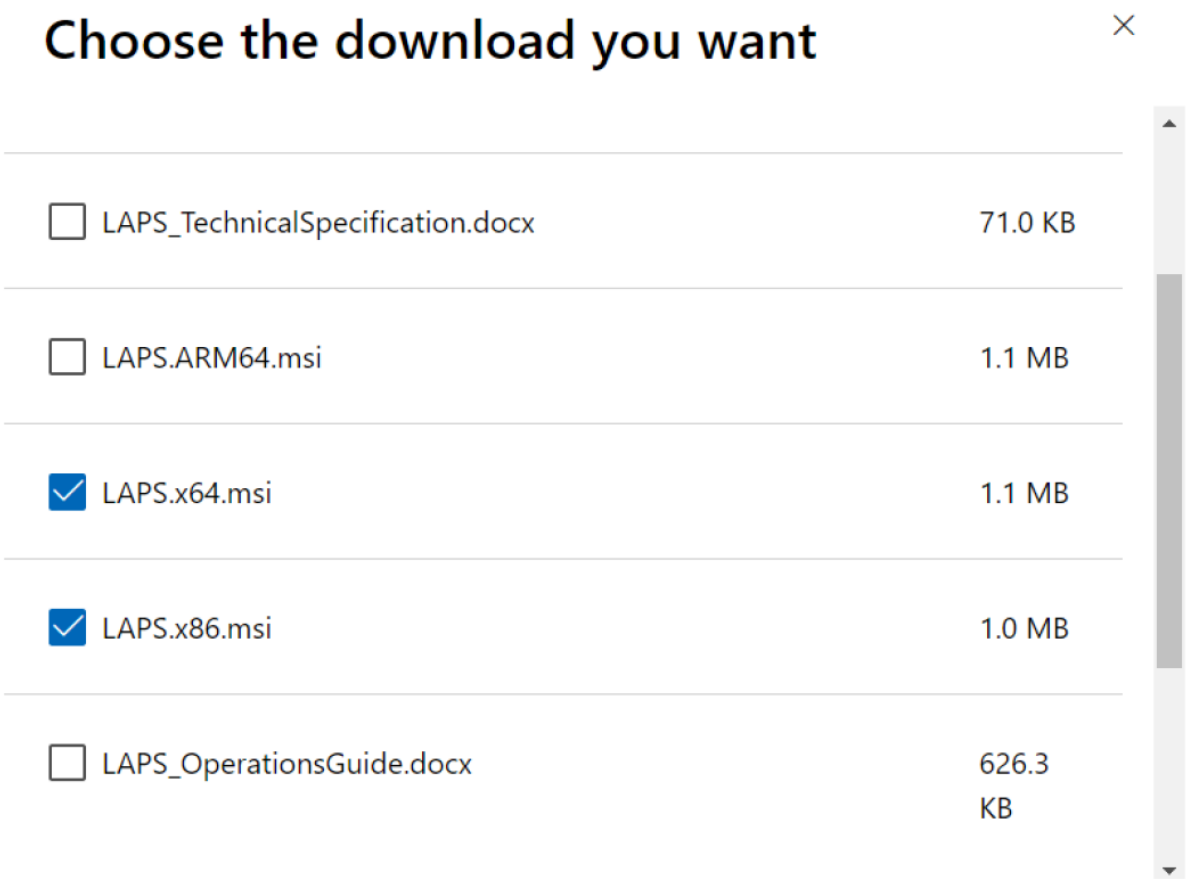
. Contrôleur de domaine Active Directory pour " btssio.fr "
. Système d'exploitation : Windows serveur 2022 standard
. Adresse IP : 10.75.19.10/24

PC -01

. Poste client intégré au domaine AD et à gérer avec LAPS
. Système d'exploitation : Windows 11
. Adresse IP : 10.75.19.101

## III – Mise en place de LAPS dans un service de domaine Active Directory

Avant de commencer, téléchargeons LAPS gratuitement sur le site de Microsoft :
nous devons télécharger à minima " **LAPS.x64.msi** " pour les machines 64 bits et " **LAPS.x86.msi** " pour les machines de 32 bits, en fonction des besoins.

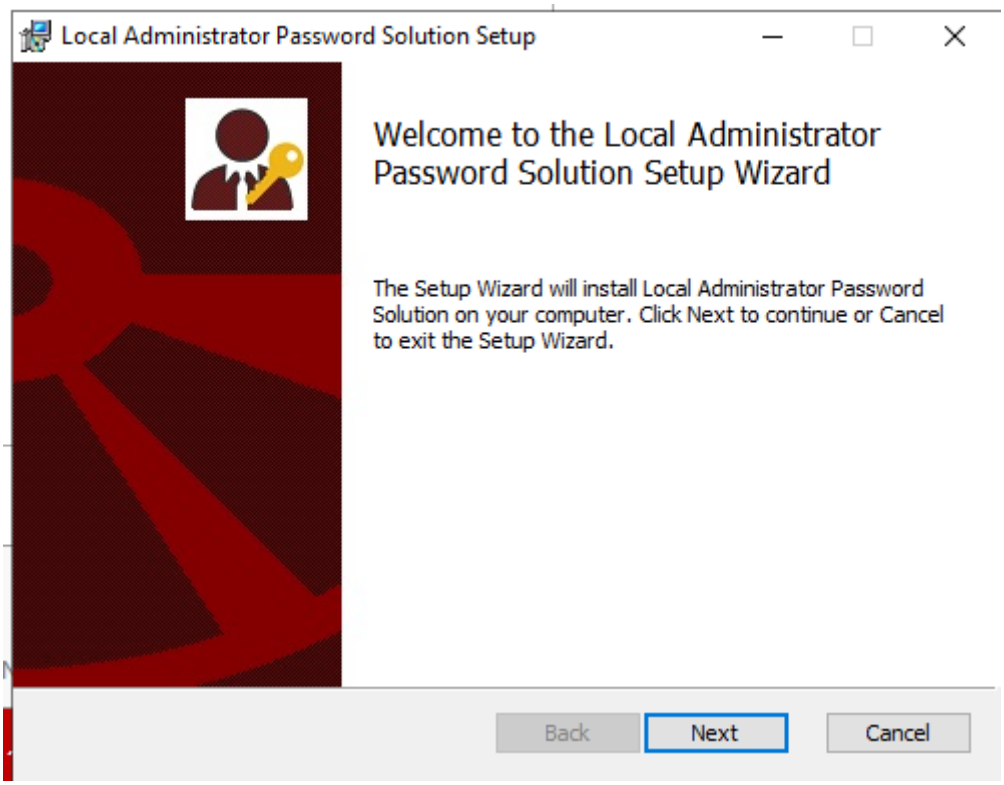



### 1 – Installation de LAPS

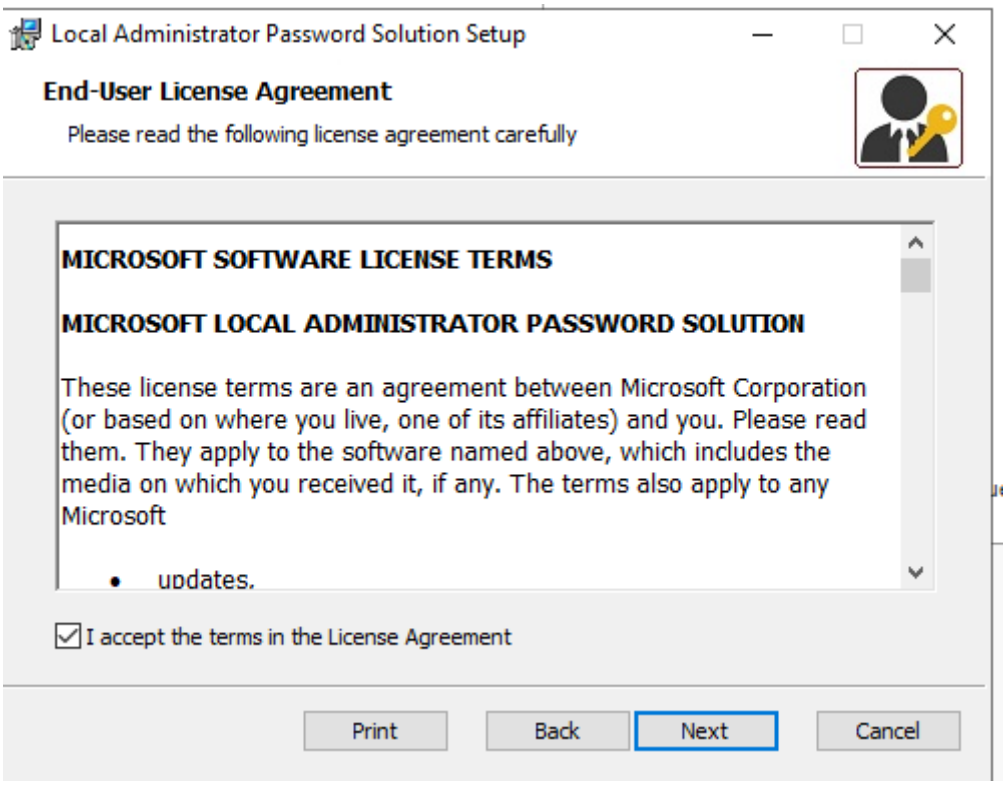
Sur le contrôleur de domaine, nous allons installer les outils de gestion LAPS. Cela pourrait être installé sur un autre serveur où vous avez les outils d'administration Active Directory installés.

Exécutons le package **MSI** correspondant à la version de votre serveur :

32 bits ou 64 bits. Vous allez voir, l'installation est simple et s'effectue en quelque clics..... Cliquez sur " **Next** " .

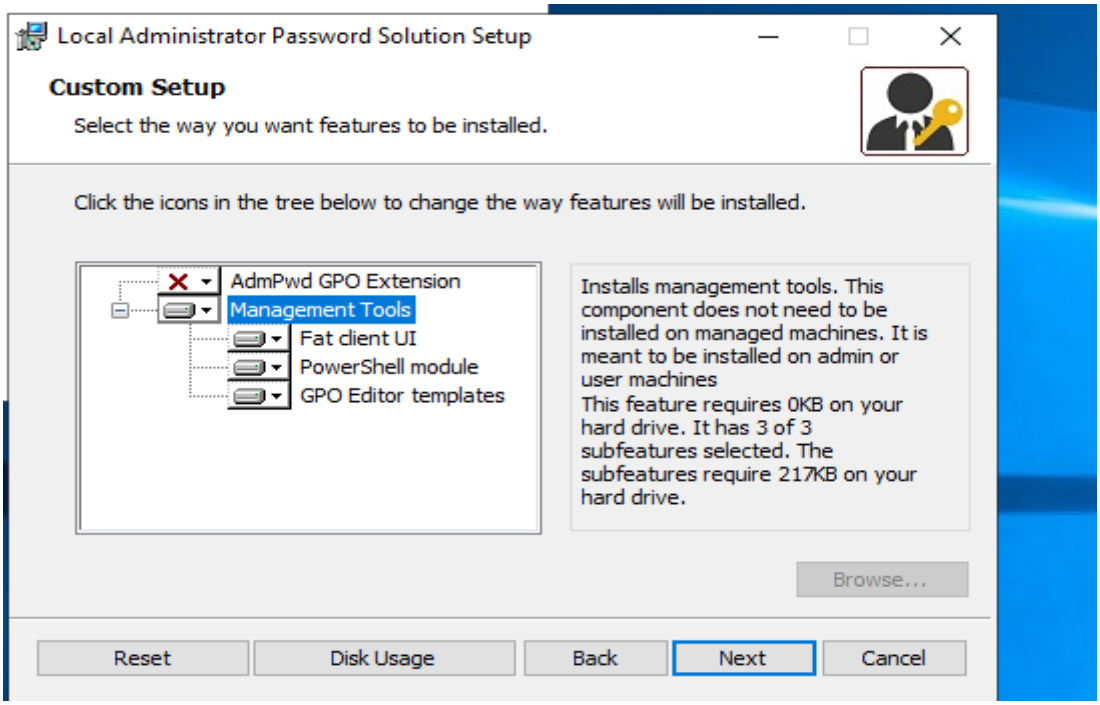



Cochons l'option " **I accept the terms in the license Agreement** " et cliquez sur " **Next** ".



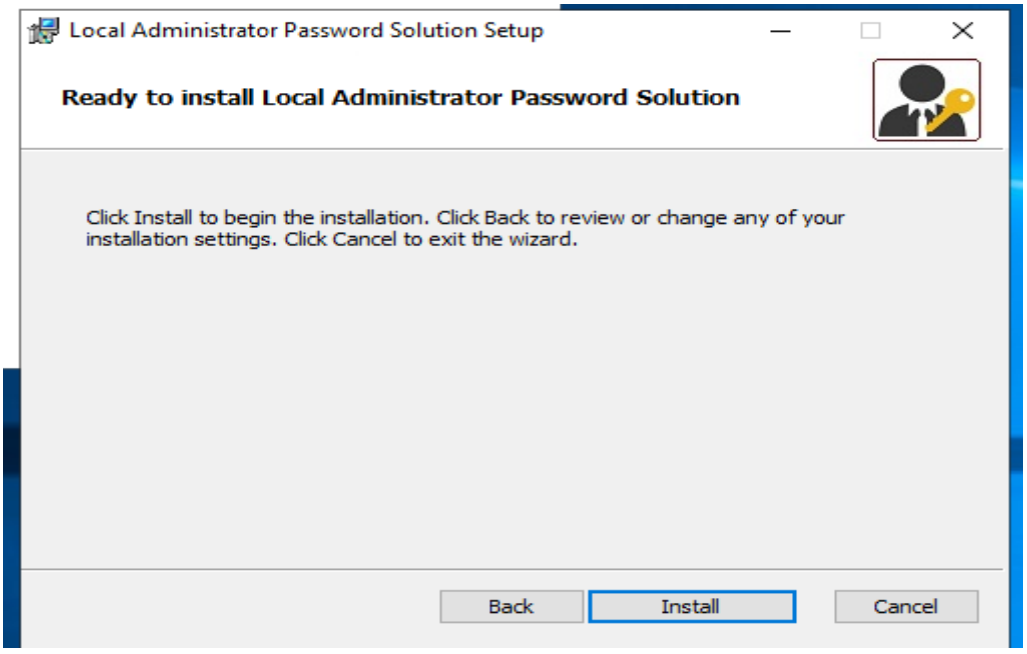

Ensuite, vous devez installer tous les outils d'administration (comme sur l'image ci-dessous ) et nous devons désélectionner l'entrée **" AdmPwd GPO Extention** " car elle n'est pas utile sur le contrôleur de domaine.

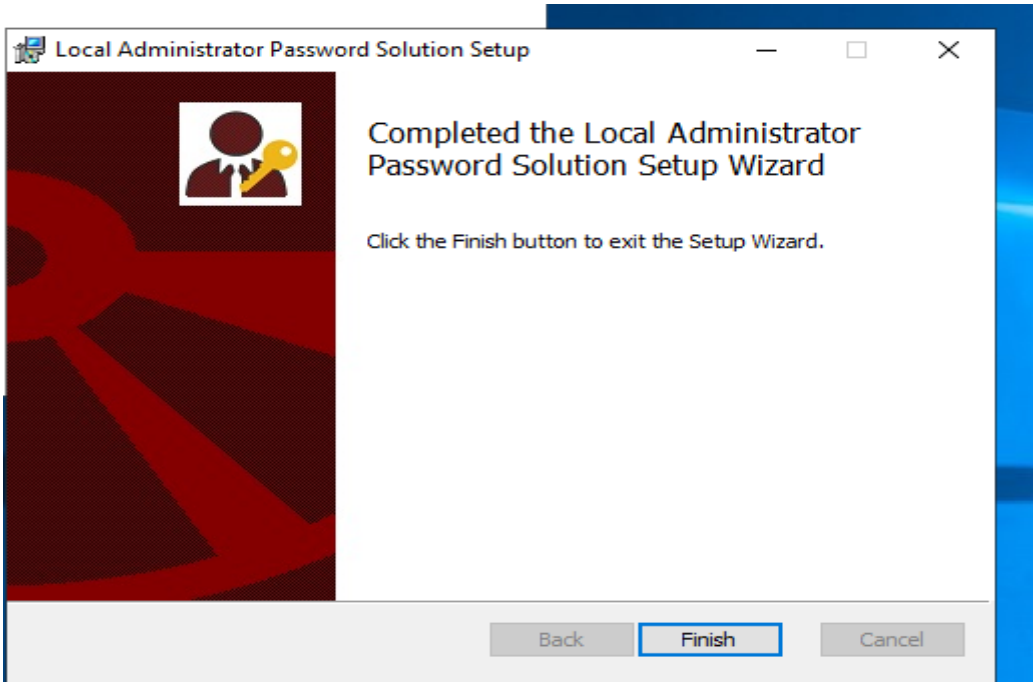
En fait, le composant “ **AdmPwd GPO Extension** ” doit être déployé sur l’ensemble des machines à gérer via LAPS.




Voici l’utilité des différents outils de gestion :

- Fat client UI : Outil graphique pour la gestion de LAPS
- PowerShell module : Commande PowerShell pour LAPS
- GPO Editor templates : Modèle ADMX de LAPS






La première étape est faite, passons à la suite.

## 2 – Présentation de l'Active Directory pour LAPS

La phase de préparation de l'Active Directory se déroule en plusieurs sous-étapes, dont voici la liste d'aperçu de ce que nous allons faire :

- Mettre à jour le schéma de Active Directory
- Déléguer l'accès à certains objets " computers " pour qu'ils puissent mettre à jour le mot de passe et la date d'expiration dans l'annuaire Active Directory
- Gérer les permissions par défaut / actuelles
- Autoriser certains utilisateurs ou groupes de sécurité à lire les mots de passe
- Autoriser certain utilisateurs ou groupes de sécurité à réinitialiser le mot de passe d'un ordinateur

### A – Mise à jour le schéma Active Directory

Ouvrez une console **Windows Powershell** sur votre contrôleur de domaine. Il faut que ce soit un contrôleur de domaine en écriture (donc pas un simple serveur !!!) et qu'il dispose du rôle FSMO " **Maître de schéma** " puisque l'on va modifier le schéma Active Directory.

Si nous avons besoins de localiser le contrôleur de domaine qui dispose du rôle FSMO, voici une commande Powershell qui nous donnera la réponse : **" Get-ADForest | Select-Object Name, SchemaMaster "**

```
PS C:\Users\Administrateur> Get-ADForest | Select-Object Name, SchemaMaster

Name        SchemaMaster
----        ------------
iticsio2.fr SCDN2.iticsio2.fr
```

Cette modification du schéma Active Directory va ajouter deux attributs au sein des objets de la class **“ computers ” :**

- ms-MCS-AdmPwd : Stocker le mot de passe en clair
- ms-MCS-AdmPwdExpirationTime : stocker la date d’expiration du mot de passe

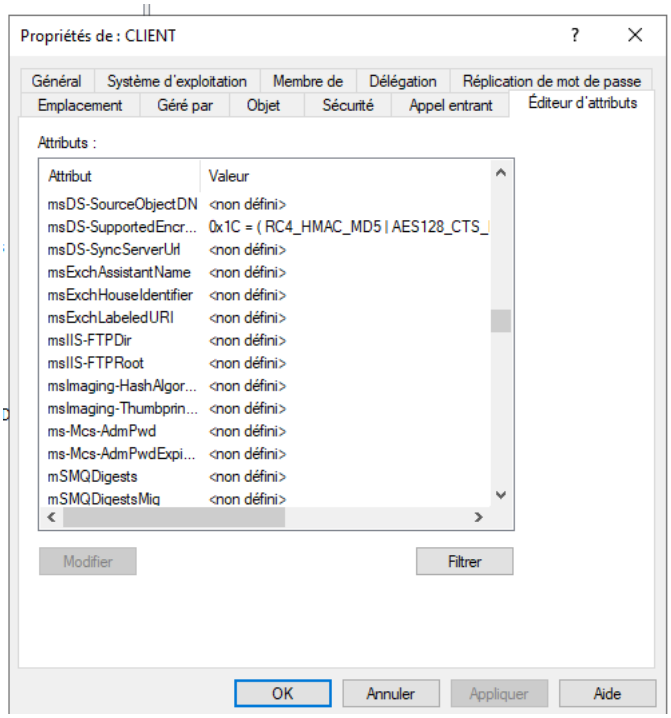
Exécutons la commande **Import-module Admpwd. PS** pour importer le module PowerShell de LAPS :
Ensuite, exécutons

```
PS C:\Users\Administrateur> Import-module AdmPwd.PS
PS C:\Users\Administrateur>
```

Ensuite, exécutons la commande **Update-AdmPwdADSchema** pour mettre à jour le Schéma de AD :

```
PS C:\Users\Administrateur> Update-AdmPwdADSchema

Operation           DistinguishedName                                          Status
---------           -----------------                                          ------
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=i... Success
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=iticsio2,DC=fr     Success
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=iticsio2,DC=fr          Success
```

Si nous ouvrons la console **“ Utilisateur et ordinateurs Active Directory ”** et que nous regardons les propriétés d’un ordinateur membre du domaine, on peut voir la présence de deux nouveaux attributs. Voici un exemple :




## B – Attribuer les droits d'écriture aux machines

Les machines qui doivent être managées via LAPS ont besoin de mettre à jour les attributs **ms-MCS-AdmPwdExpirationTime** et **ms-MCS-AdmPwd** au sein de notre annuaire Active Directory. Sinon, il ne sera pas possible de stocker dans l'Active Directory la date d'expiration et le mot de passe.

Le module LAPS de PowerShell contient un cmdlet pour réaliser cette action. Pour l'utiliser, c'est tout simple nous devonsidiquer le nom de l'OU cible. Pour nous, nous ciblons l'OU "**Ordinateur**" (visible sur la copie d'écran ci-dessus) car elle contient les machines que je souhaite gérer avec LAPS. Nous recommandons de préciser le **DistinguishedName** de l'OU pour être sûr de cibler la bonne OU, sauf s'il n'y en a qu'une seule qui a ce nom.

La commande est **Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=iticsio2,DC=fr"**

Nous devons obtenir un retour dans la console avec le statut ***" Delegated "***

```
PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=iticsio2,DC=fr"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=iticsio2,DC=fr                            Delegated


PS C:\Users\Administrateur>
```

## C – Gérer les permissions par défaut / actuelles

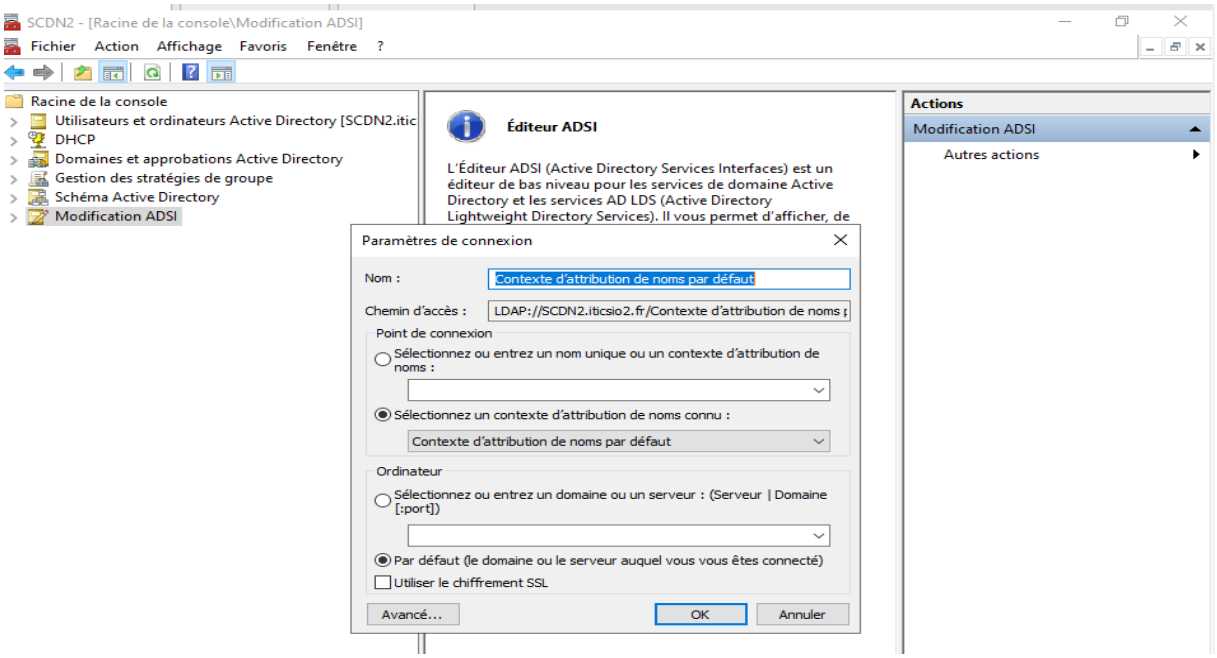
En fonction de la configuration de votre annuaire Active Directory, certains utilisateurs ou groupes ont probablement les permissions pour lire les attributs étendus. Afin d'éviter que les attributs créés par LAPS soient accessibles par n'importe qui, nous devons contrôler et adapter les permissions. Nous devons **retirer les permissions aux utilisateurs/groupes qui ont accès aux attributs étendus** sur l'OU "**PC**", s'il y a des entrées correspondantes à des utilisateurs non habilités.

Plutôt que de parcourir les droits via l'interface graphique, on peut s'appuyer sur PowerShell pour visualiser quels sont les comptes qui ont un accès à ces attributs étendus. Pour ma part, je vais auditer l'OU "PC" qui contient mes postes à manager avec LAPS.

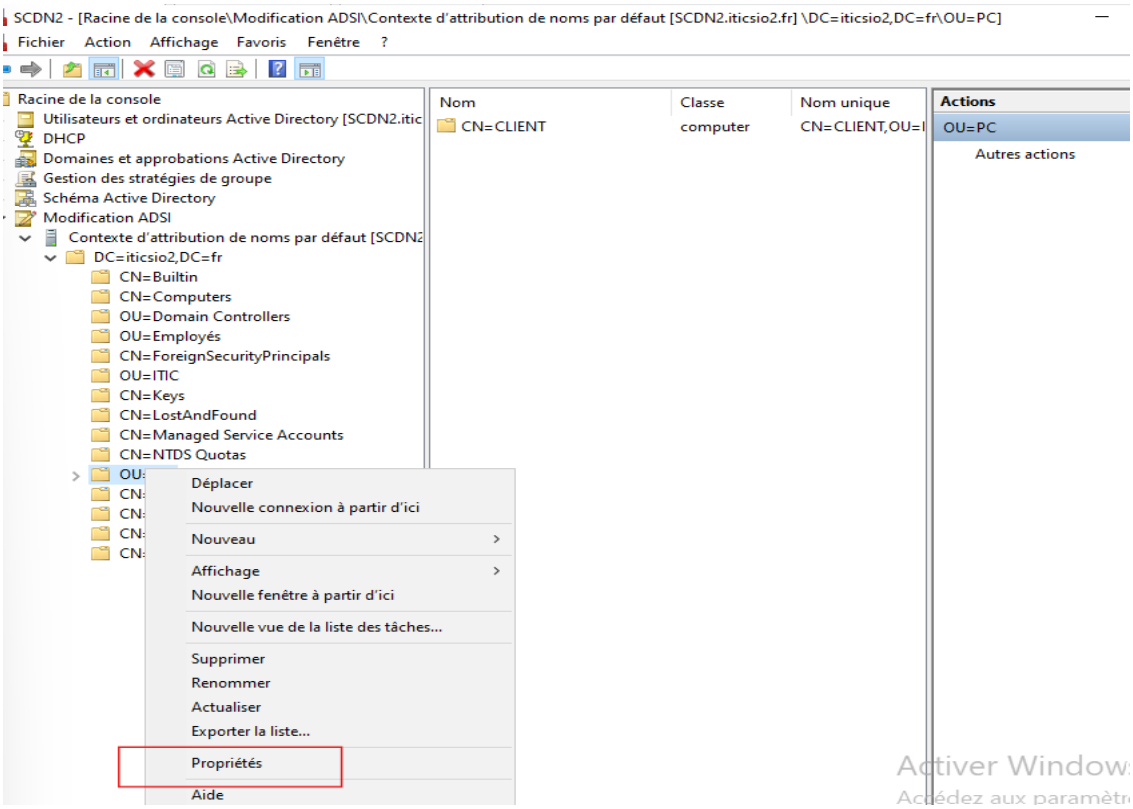
```
PS C:\Users\Administrateur> Find-AdmPwdExtendedRights -Identity "PC" | Format-Table

ObjectDN                                ExtendedRightHolders
--------                                --------------------
OU=PC,DC=iticsio2,DC=fr                 {AUTORITE NT\Système, ITICSIO2\Admins du domaine}


PS C:\Users\Administrateur>
```

Voyons comment gérer cette permission……

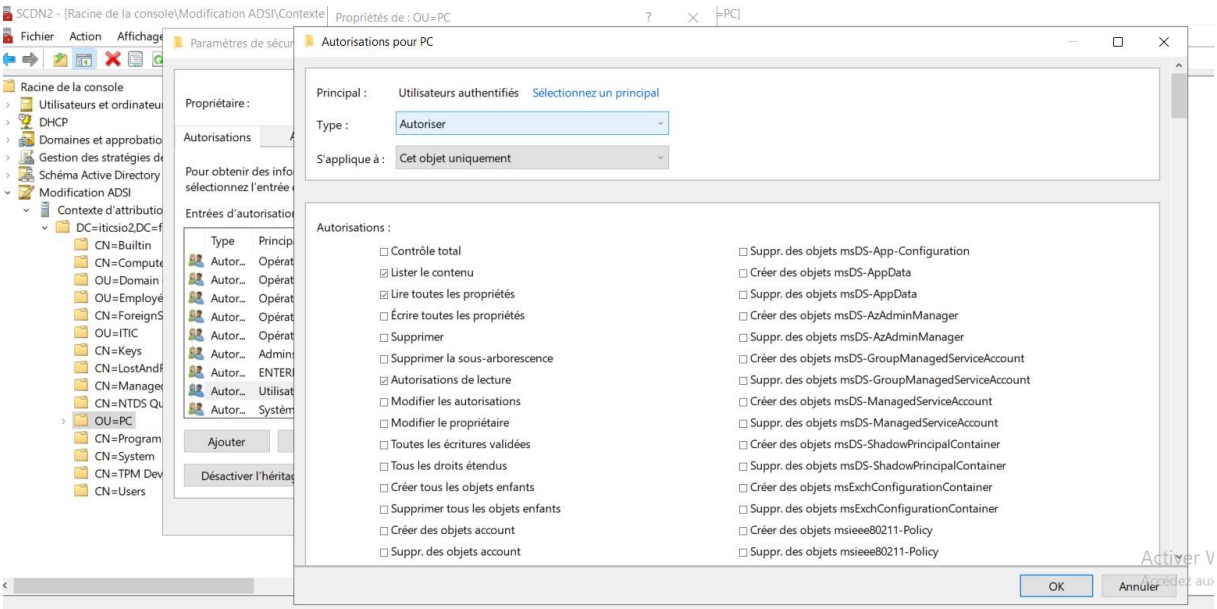
Ouvrons la console "**Modification ADSI**" puis effectuons un clic droit sur "**Modification ADSI**" afin de cliquer sur "**Connexion**". Une fenêtre s'ouvre... nous Laissons le choix par défaut, à savoir "**Contexte d'attribution de noms par défaut**" et après nous validons.



Ensuite, nous parcourons l'Active Directory jusqu'à trouver l'**OU qui contient les ordinateurs managés par LAPS** (et donc qui vont venir écrire leur mot de passe). Effectuons un clic droit sur cette OU, pour ma part c'est l'OU "**PC**" et accédons aux propriétés via un clic droit.




Cliquez sur l'onglet "**Sécurité**" puis sur le bouton "**Avancé**". Ensuite, si l'on souhaite retirer les droits, par exemple sur le groupe "**Utilisateurs authentifiés**" (même si ici ils n'ont pas les droits, c'est un exemple...), il suffit de sélectionner "**Utilisateurs authentifiés**" dans la liste et cliquer sur le bouton "**Modifier**". Il ne reste plus qu'à décocher les droits "**Tous les droits étendus**".



## D – Ajouter des autorisations de lire le mot de passe LAPS

Au sein de l'annuaire Active Directory, je dispose d'un groupe nommé "**laps**" qui contient **tous les utilisateurs qui doivent être en mesure de lire le mot de passe laps** de chaque ordinateur (correspondant au compte Administrateur local de la machine).

Pour ajouter l'autorisation de lire le mot de passe, nous allons utiliser le cmdlet "**Set-AdmPwdReadPasswordPermission**" avec deux paramètres qui vont permettre de préciser l'OU (*-Identity*) et le nom du groupe (ou l'utilisateur) à autoriser (*-AllowedPrincipals*). Ce qui donne :

```
PS C:\Users\Administrateur> Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=iticsio2,DC=fr                            Delegated


PS C:\Users\Administrateur>
```

On obtient un retour dans la console avec le statut ***“ Delegated ”***

Le tour est joué, passons à la suite.

## E – Ajouter des autorisations de réinitialisation du mot de passe LAPS

En fonction de l'organisation du service informatique de l’entreprise, peut-être que les administrateurs et les techniciens du support sont différents, et qu'ils ont des autorisations différentes. On peut imaginer avoir **deux groupes pour les autorisations LAPS** : un groupe qui permet de lire le mot de passe et un second groupe qui permet en plus la réinitialisation du mot de passe. Dans le cadre de ce TP, nous allons continuer d'utiliser le groupe "**laps**".

Le cmdlet pour cette autorisation se nomme "**Set-AdmPwdResetPasswordPermission**" et il fonctionne comme le cmdlet précédent. Ce qui donne :

```
PS C:\Users\Administrateur> Set-AdmPwdResetPasswordPermission -Identity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=iticsio2,DC=fr                            Delegated


PS C:\Users\Administrateur>
```

On obtient un retour dans la console avec le statut ***“ Delegated ”***

Les autorisations sont effectives et s’appliquent au groupe **“ LAPS** ”

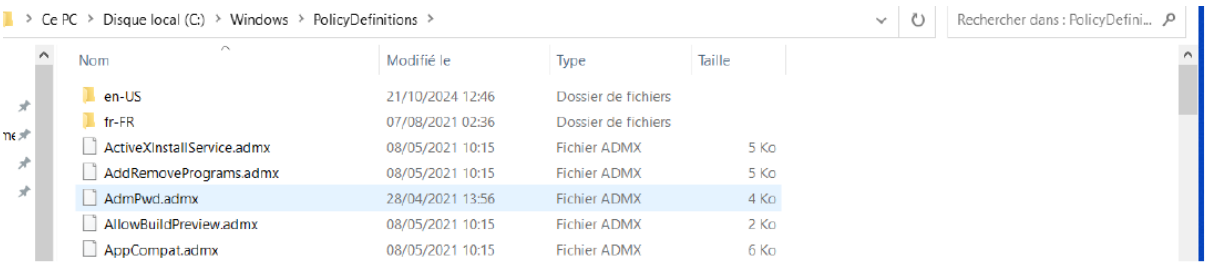
```
PS C:\Users\Administrateur> Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=iticsio2,DC=fr                            Delegated


PS C:\Users\Administrateur> Set-AdmPwdResetPasswordPermission -Identity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=iticsio2,DC=fr                            Delegated
```

# IV – Configuration de la GPO LAPS

La dernière étape de la configuration, avant que l'on déploie le client LAPS sur les postes de travail à gérer, consiste à créer une GPO de configuration de LAPS. Cette GPO va contenir différents paramètres, notamment pour activer la gestion du compte Administrateur avec LAPS, ou encore pour définir la complexité du mot de passe généré aléatoirement par LAPS.

## 1 – ADMX de LAPS

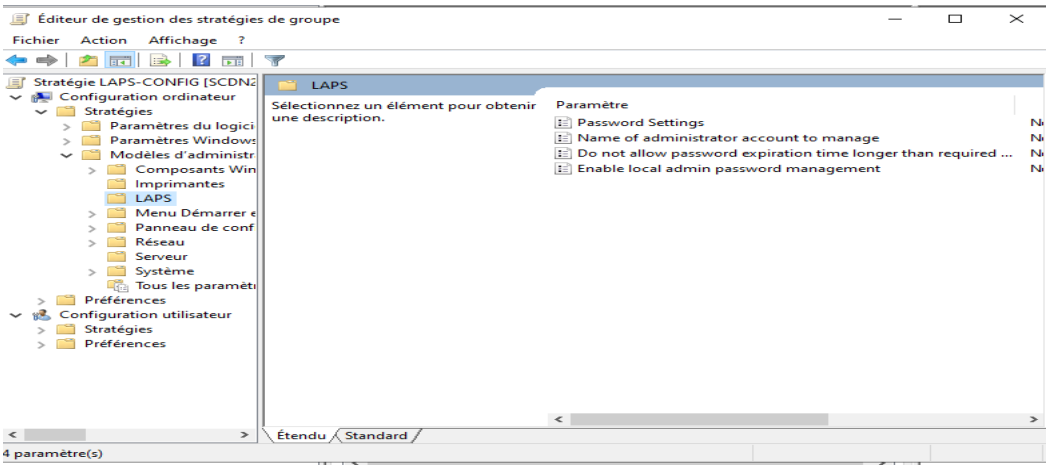
Nous devons commencer par **importer les fichiers ADMX de LAPS** sur notre contrôleur de domaine, à l'intérieur du dossier "**PolicyDefinitions**" (magasin central) puisqu'il sert à ajouter des modèles d'administration supplémentaires.
Pour récupérer le fichier ADMX et son fichier de langue ADML, nous devons aller sur le serveur où l'on a installé les outils d'administration de LAPS. Il y a un fichier à copier et a coller dans le fichier SYSVOL




Ensuite, nous pouvons passer à la configuration de la GPO.

## 2 – GPO pour LAPS

Pour créer la GPO, nous devons ouvrir la console d'édition des stratégies de groupe et créer une nouvelle GPO. Nous allons nommer cette GPO "**LAPS-Config**" et l'appliquer sur mon OU "**PC**".
**C'est important de lier la GPO sur cette OU "PC"** (*à adapter selon votre configuration, bien sûr*) et non sur une autre OU, car jusqu'ici nous avons géré les autorisations de LAPS sur cette OU.
Ensuite, modifons la GPO via un clic droit "**Modifier**" et parcourons les paramètres comme ceci :



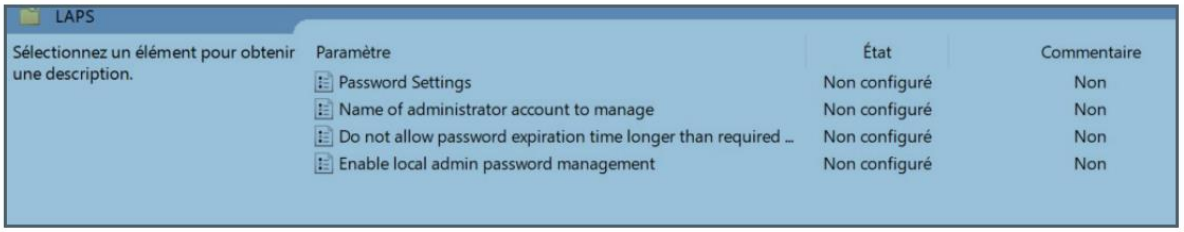
Ce modèle d'administration pour LAPS contient 4 paramètres.Voici la signification de ces différents paramètres :

- **Password Settings** : définir la complexité du mot de passe, sa longueur et sa durée de vie

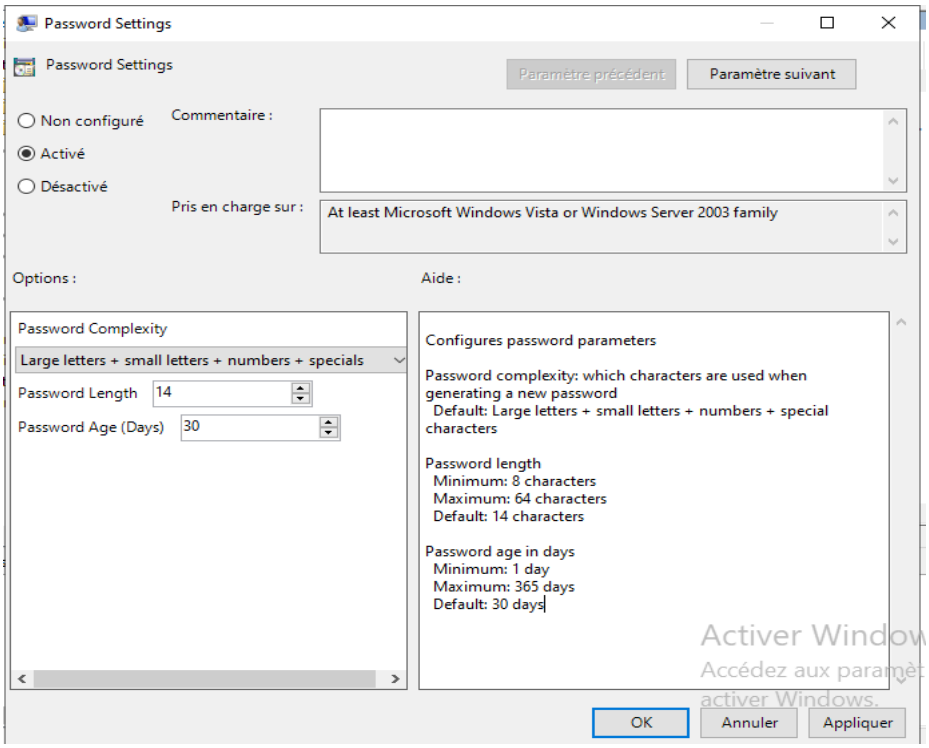
- **Name of administrator account to manage** : définir un compte administrateur à configurer autre que le compte Administrateur intégré à Windows. En effet, le compte Administrateur BUILT-IN est automatiquement détecté, grâce au SID (Identifiant de sécurité unique) même s'il est renommé. Si l'on cible le compte Administrateur intégré à Windows, il ne sera pas utile de configurer ce paramètre.

- **Do not allow password expiration longer than required by policy** : ne pas autoriser une expiration du mot de passe plus longue que le permet la stratégie définie au sein du paramètre "*Password settings*".

- **Enable local admin password management** : activer ou désactiver la gestion du mot de passe administrateur avec LAPS pour l'ordinateur cible.



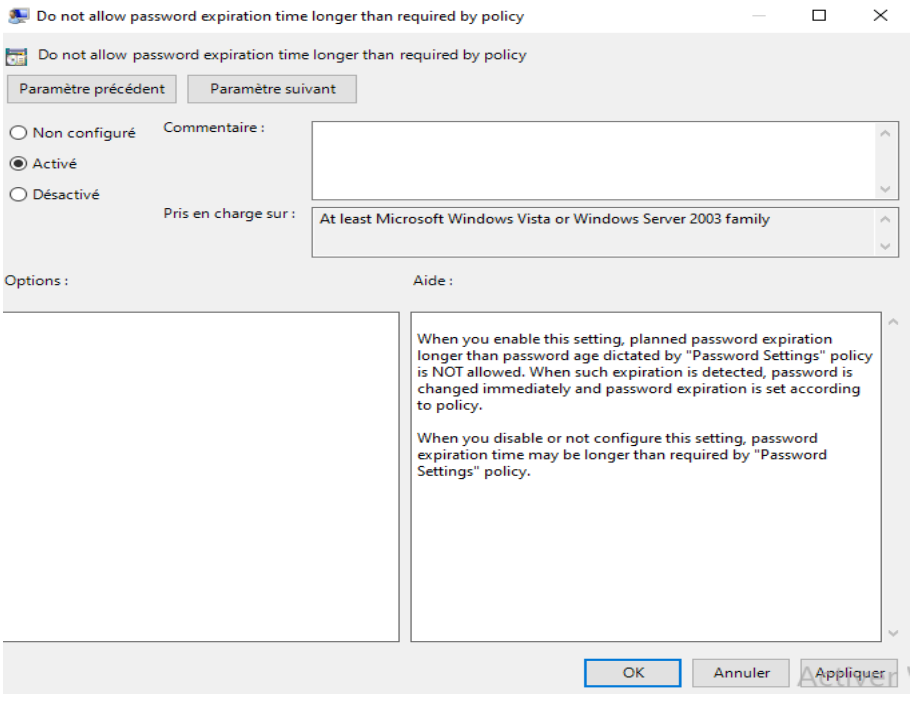

Nous allons commencer par définir une stratégie de complexité des mots de passe via le paramètre "**Password Settings**". Avec la stratégie indiquée sur la copie d'écran ci-dessous, on obtient des mots de passe très complexes et qu'il sera très difficile de mémoriser. Par exemple, on peut obtenir « *6F5g@FRlb)1KE.* »



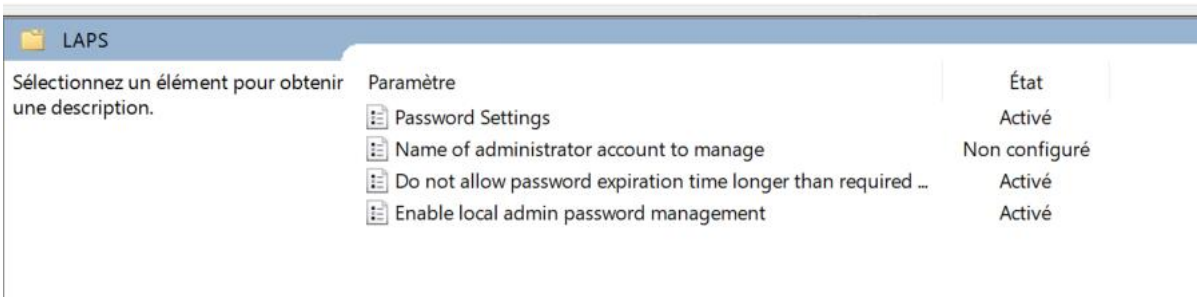

Ensuite, nous allons activer deux autres paramètres donc il suffit de les basculer sur l'état "**Activé**" :

- **Enable local admin password management** (indispensable pour activer LAPS)

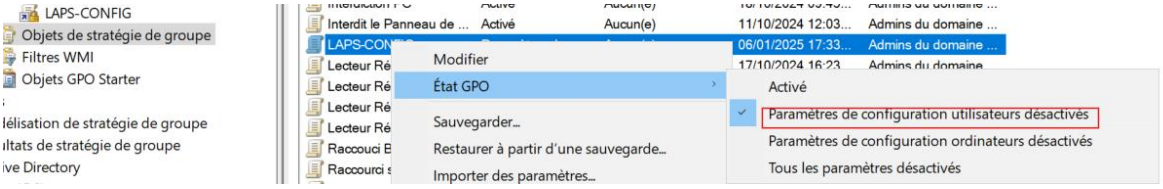
**Do not allow password expiration longer than required by policy**



Le dernier paramètre ne sera pas configuré, car le compte "Administrateur" d'origine est utilisé sur mes postes de tests. Il conviendra de l'activer et le configurer en fonction de vos besoins. Vous pouvez fermer la GPO puisqu'elle est prête. Nous obtenons la configuration suivante :

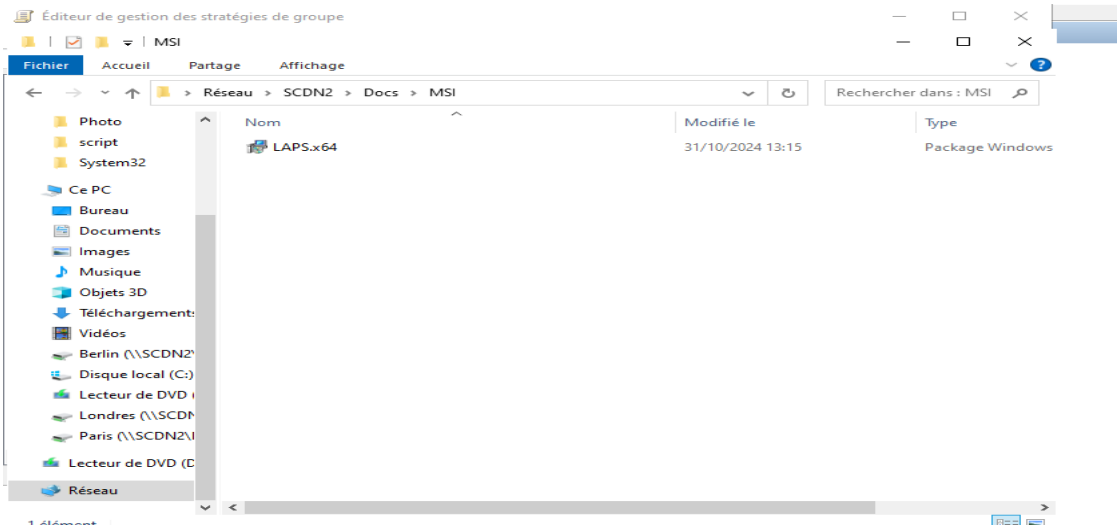



Pour finir, profitons d'être sur la configuration de la GPO pour désactiver le traitement des paramètres utilisateurs puisque cette GPO contient uniquement des paramètres ordinateurs. Effectuez un clic droit sur la GPO, puis sous "**Etat GPO**" cliquez sur "**Paramètres de configuration utilisateurs désactivés**".




## 3 – Créer la GPO pour déployer le MSI de LAPS

Avant de commencer à créer la GPO, nous devons héberger le package MSI sur un partage, accessible au travers du réseau, depuis les postes clients qui doivent pouvoir installer ce package. La solution de faciliter consiste à utiliser le dossier "DC" du partage Script lié à l'Active Directory. De notre côté, nous déposerons le package MSI à l'endroit ci-dessous :
notre chemin : **\\SCDN2\Docs\MSI**.

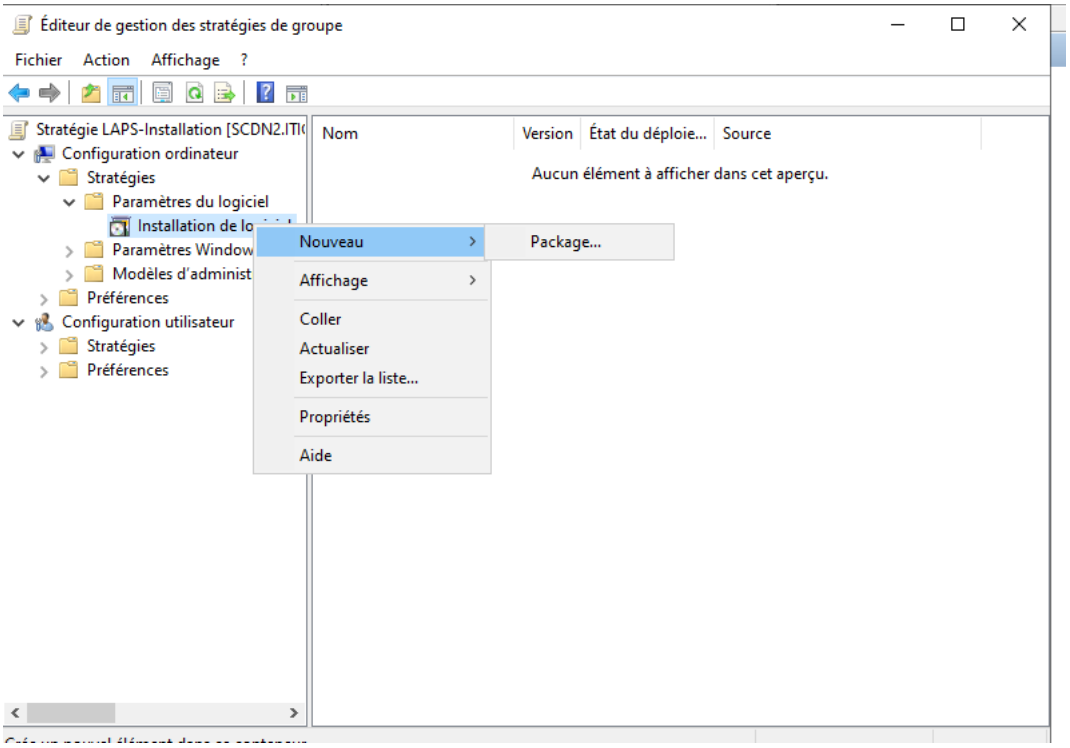


A partir de la console de gestion des stratégies de groupe, nous allons créer une GPO nommée "**LAPS-Installation**" qui sera là en complément de la GPO "**LAPS-Config**" créée précédemment. Elle sera liée également à l'OU "Computer" puisque cette OU contient tous les PC que je souhaite gérer avec LAPS.

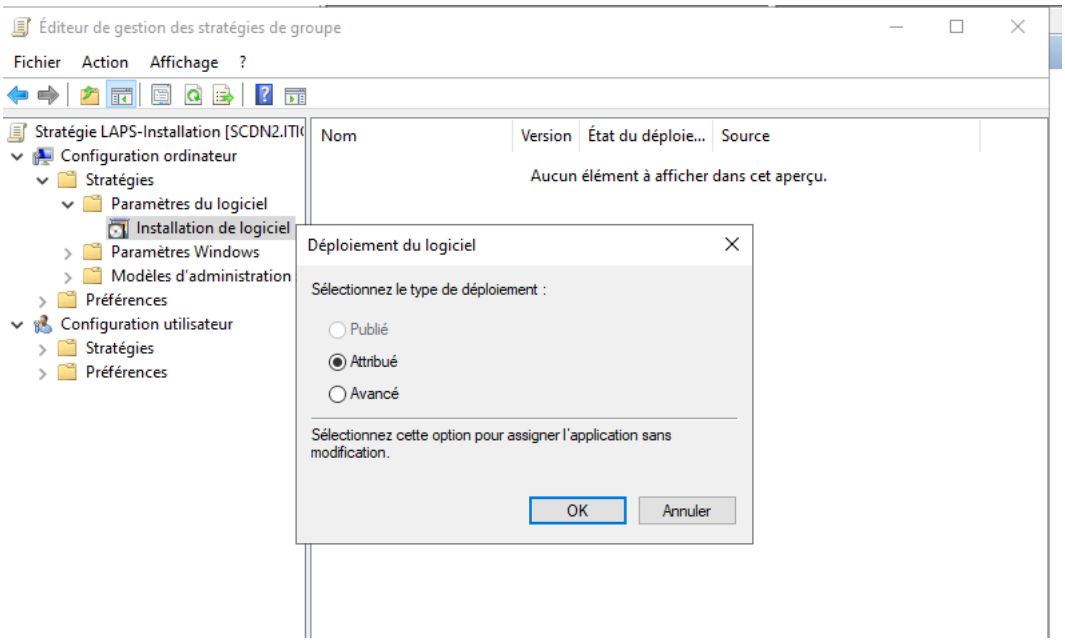
D'un point de vue technique, rien n'empêche d'utiliser la même GPO pour l'installation et la configuration. Pour utilisation d'une solution pour déployer les postes Windows, il faut penser à inclure l'installation de LAPS en ce moment afin de se passer de cette GPO d'installation.

Une fois la GPO créée, nous devons la modifiée comme suit :

**Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel**



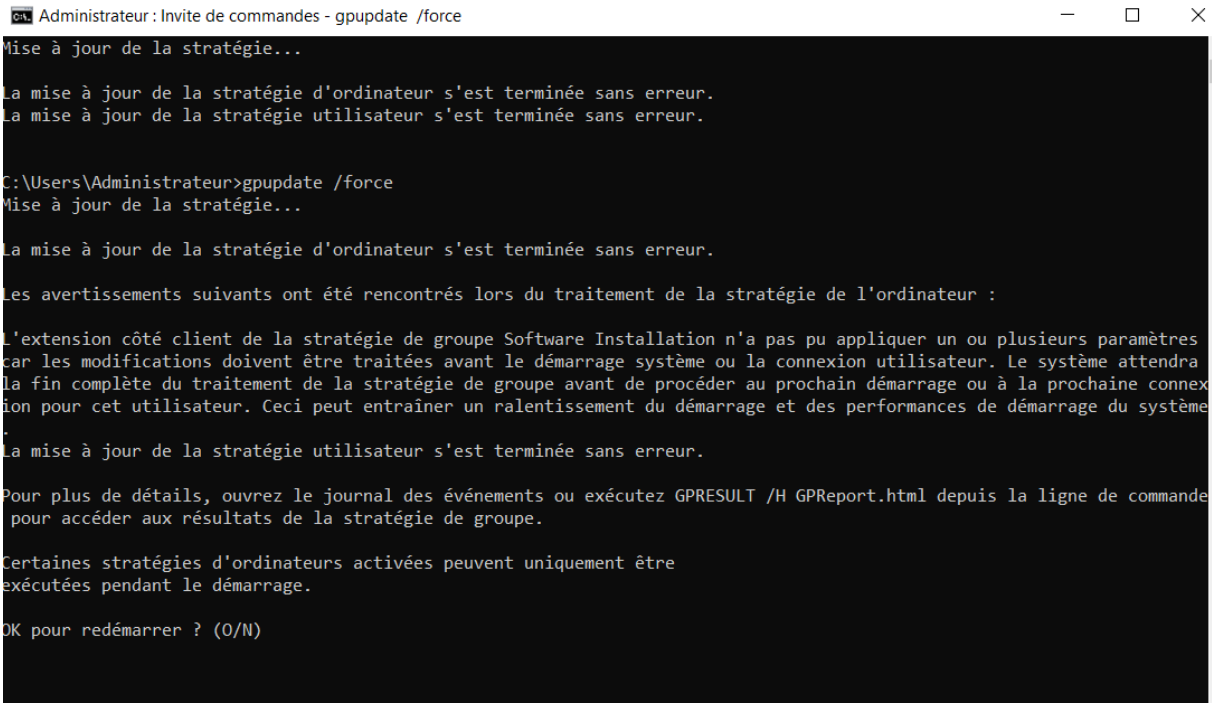

Nous devons indiquer quel est le package MSI à déployer, alors accédons à notre partage et sélectionnez le MSI de LAPS. Validons... La fenêtre ci-dessous va apparaître. Sélectionnons "**Attribué**" et cliquez sur "**OK**".



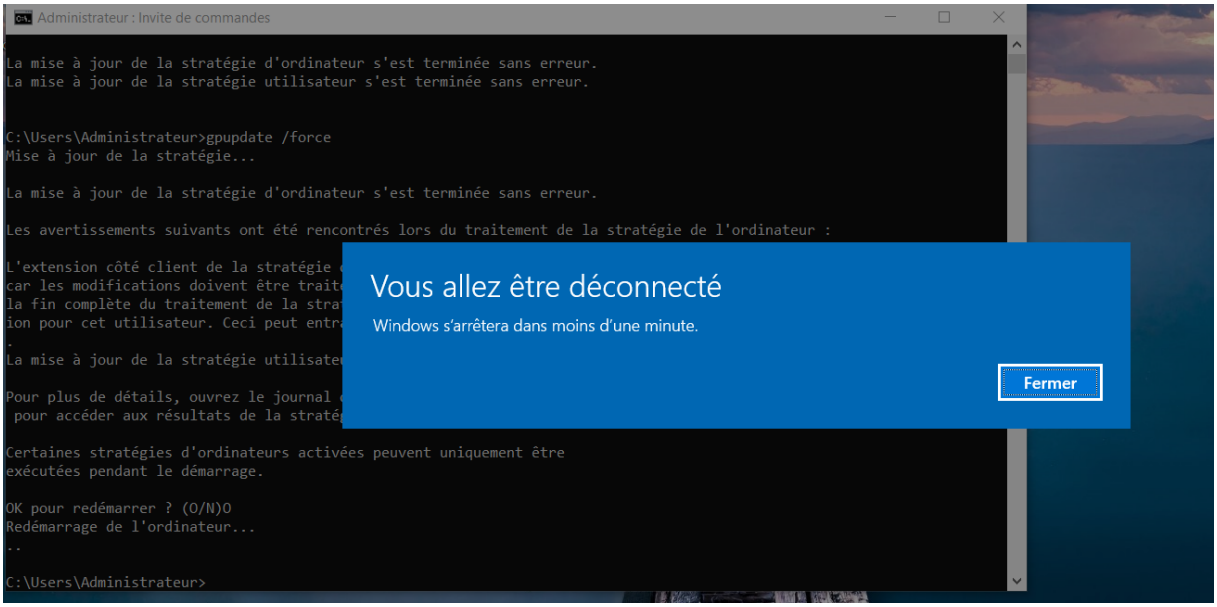

**Voilà, le package MSI est inclus à la GPO et prêt à être installé sur les postes !** Le mode "**Attribué**" permet d'utiliser les options par défaut, ce qui est satisfaisant pour l'installation de LAPS.

## 3 – Tester l'installation de LAPS sur une machine

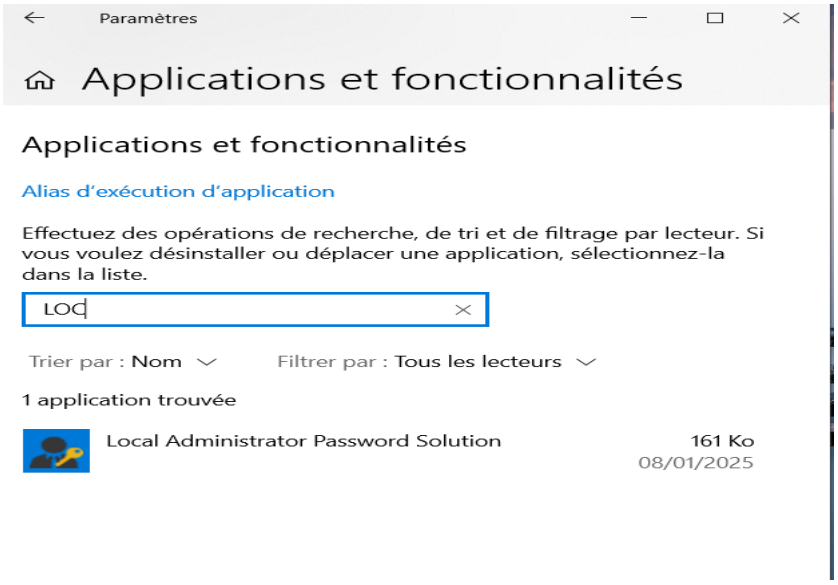
Nous allons utiliser la machine "**CLIENT**", sous Windows 10, et qui appartient à **l'OU "PC".** Après avoir ouvert une session, nous devons faire une mise à jour des GPO à partir d'une console : nous allons utiliser cette commande **gpupdate /force** dans l'Invite de commande



Un avertissement s'affiche pour me dire que l'installation du logiciel s'effectue au redémarrage et il m'est proposé de redémarrer. Il suffit d'indiquer "**O**" et de **valider pour que la machine redémarre**.



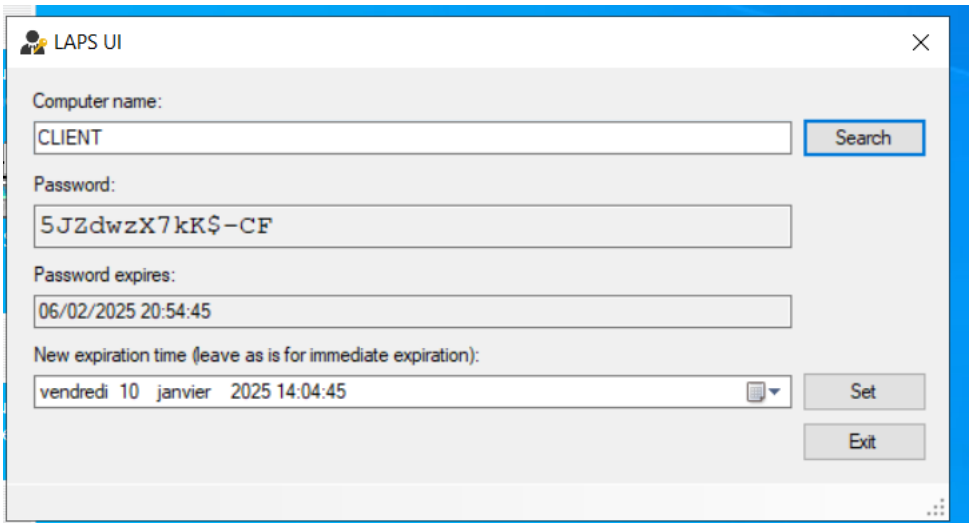

Suite au redémarrage, si l'on regarde au sein des applications et fonctionnalités, on constate quelque chose d'intéressant : "**Local Administrator Password Solution**" apparaît dans la liste ! LAPS est installé sur cette machine et cela va suivre sur les autres machines de mon parc...




Puisque le client LAPS est déployé sur au moins une machine de notre parc et que la GPO de configuration de l'outil est en place, normalement il doit y avoir du changement du côté de l'Active Directory. Autrement dit, les attributs **"ms-Mcs-AdmPwd"** et **"ms-Mcs-AdmPwdExpirationTime"** ne doivent plus être vide.

## 4 – Afficher le mot de passe avec LAPS UI

A partir du menu Démarrer de votre serveur, vous pouvez trouver l'application "**LAPS UI**" à l'intérieur d'un dossier nommé "**LAPS**". Ce petit utilitaire est très pratique et va éviter d'utiliser la console Active Directory. Il va permettre d'afficher le mot de passe et la date d'expiration d'un ordinateur.
Faisons un essai avec notre PC client :




Le mot de passe apparaît bien, et la date d'expiration est lisible du premier coup.

Merci là nous arrivons à la fin du TP, à bientôt pour un nouveau.