1°/ Télécharger LAPS

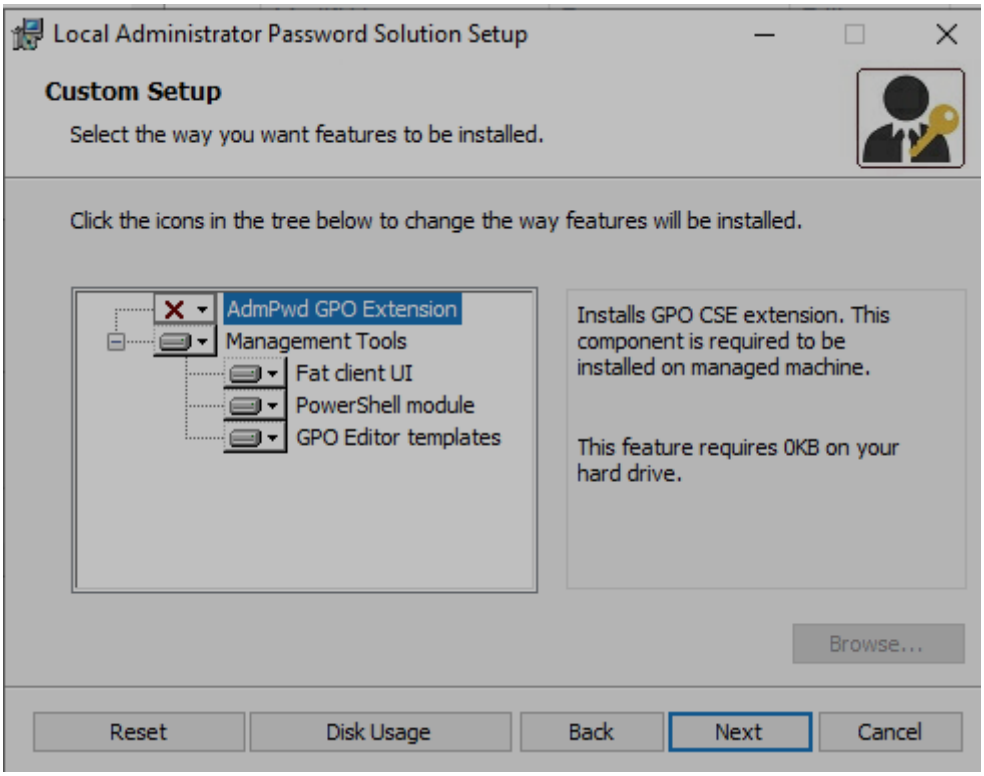
https://www.microsoft.com/en-us/download/details.aspx?id=46899

2°/ Installer LAPS

Il est possible d'installer LAPS à distance via GPO par exemple.

> msiexec /i ..\LAPS.msi /quiet

Sinon on procède à l'installation manuel avec les options suivantes sur le contrôleur de domaine :




```
Fat client UI : outil graphique pour la gestion de LAPS
PowerShell module : commandes PowerShell pour LAPS
GPO Editor templates : modèle ADMX de LAPS
```

3°/ Vérifier l'installation des éléments

FAT client UI

=> %ProgramFiles%\LAPS

- AdmPwd.UI.exe
- AdmPwd.Utils.config
- AdmPwd.Utils.dll

PowerShell module

=> %WINDIR%\System32\WindowsPowerShell\v1.0\Modules\AdmPwd.PS

- AdmPwd.PS.dll
- AdmPwd.PS.format.ps1xml

- AdmPwd.PS.psd1
- AdmPwd.Utils.config
- AdmPwd.Utils.dll

=> %WINDIR%\System32\WindowsPowerShell\v1.0\Modules\AdmPwd.PS\en-us

- AdmPwd.PS.dll-Help.xml

CSE

=> %ProgramFiles%\LAPS\CSE

- AdmPwd.dll

GPO Editor templates

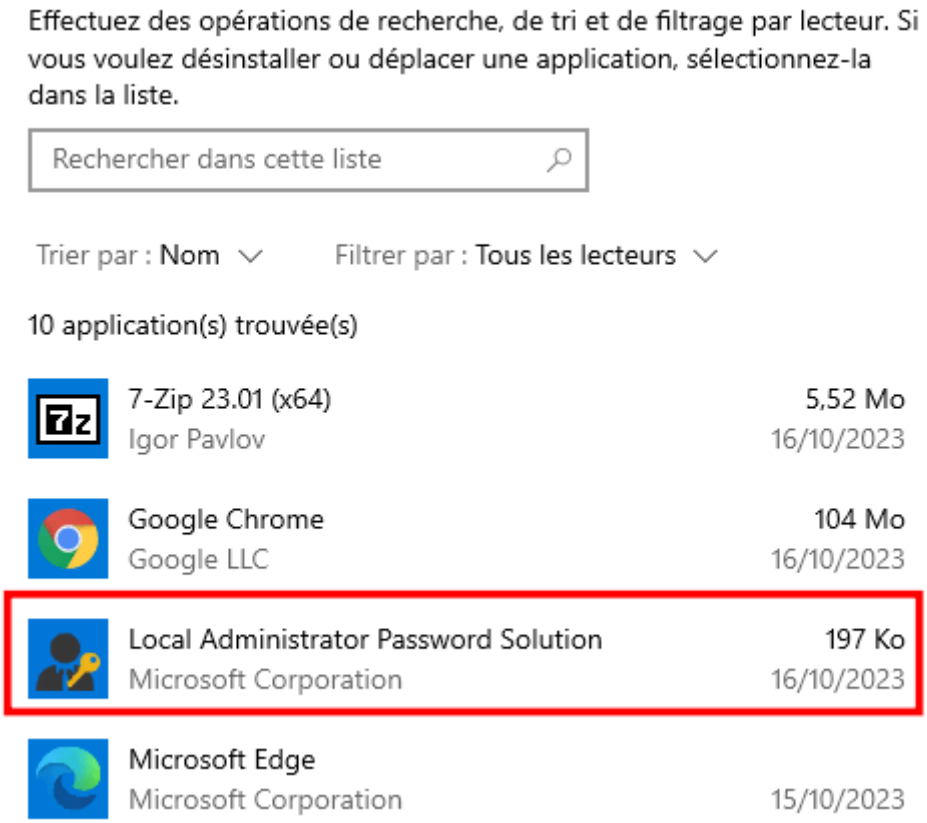
=> %WINDIR%\PolicyDefinitions

- AdmPwd.admx

=> %WINDIR%\PolicyDefinitions

- AdmPwd.adml

On peut également vérifier dans les programmes installés :



4°/ Préparation de l'Active Directory pour LAPS

a) Trouver le contrôleur de domaine qui dispose du rôle FSMO "Maître de schéma"

> Get-ADForest | Select-Object Name, SchemaMaster

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

Name        SchemaMaster
----        ------------
raisin.lab raisin-dc1.raisin.lab
```

b) Vérifié que le contrôleur de domaine possède les droits d'écriture (pas de RODC)

> nltest.exe /dsgetdc: /writable /force

```
PS C:\Users\Administrateur> nltest.exe /dsgetdc: /writable /force
          Contrôleur de domaine : \\raisin-dc1.raisin.lab
     Adresse : \\192.168.9.71
    GUID dom : bfb4b03c-60fa-4a02-bcf3-465c9215992d
    Nom dom : raisin.lab
  Nom de la forêt : raisin.lab
 Nom de site du contrôleur de domaine : Default-First-Site-Name
Nom de notre site : Default-First-Site-Name
       Indicateurs : PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10 KEYLIST
La commande a été correctement exécutée
```

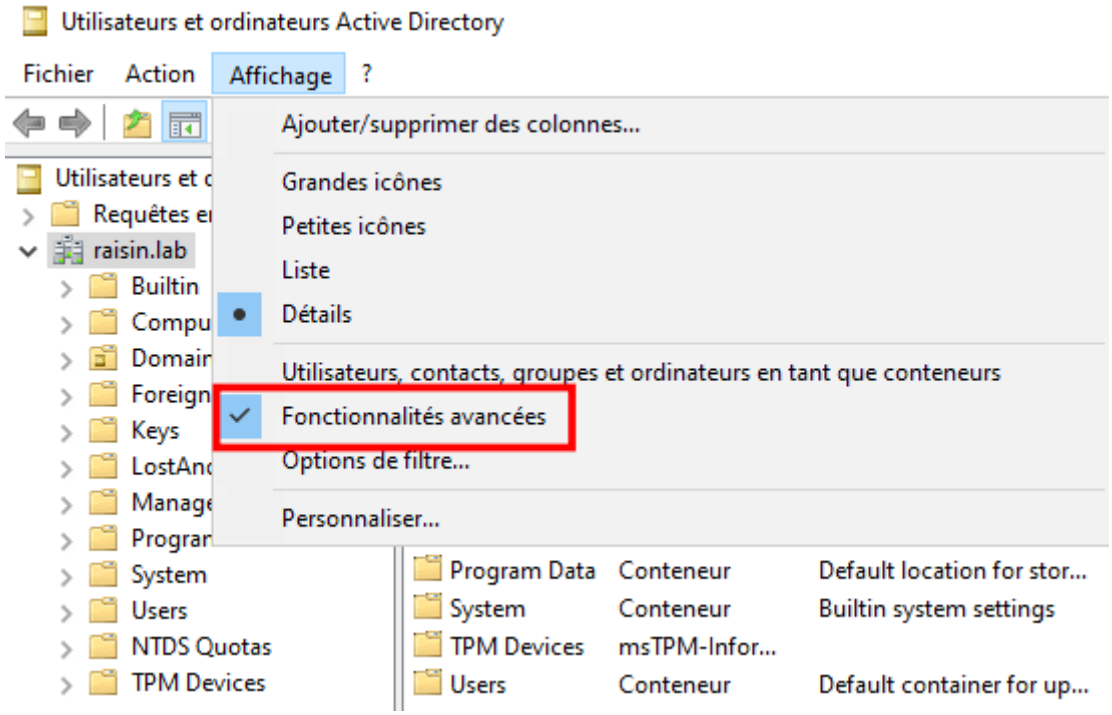
c) Mettre à jour le schéma AD

> Import-Module AdmPwd.PS
> Update-AdmPwdADSchema

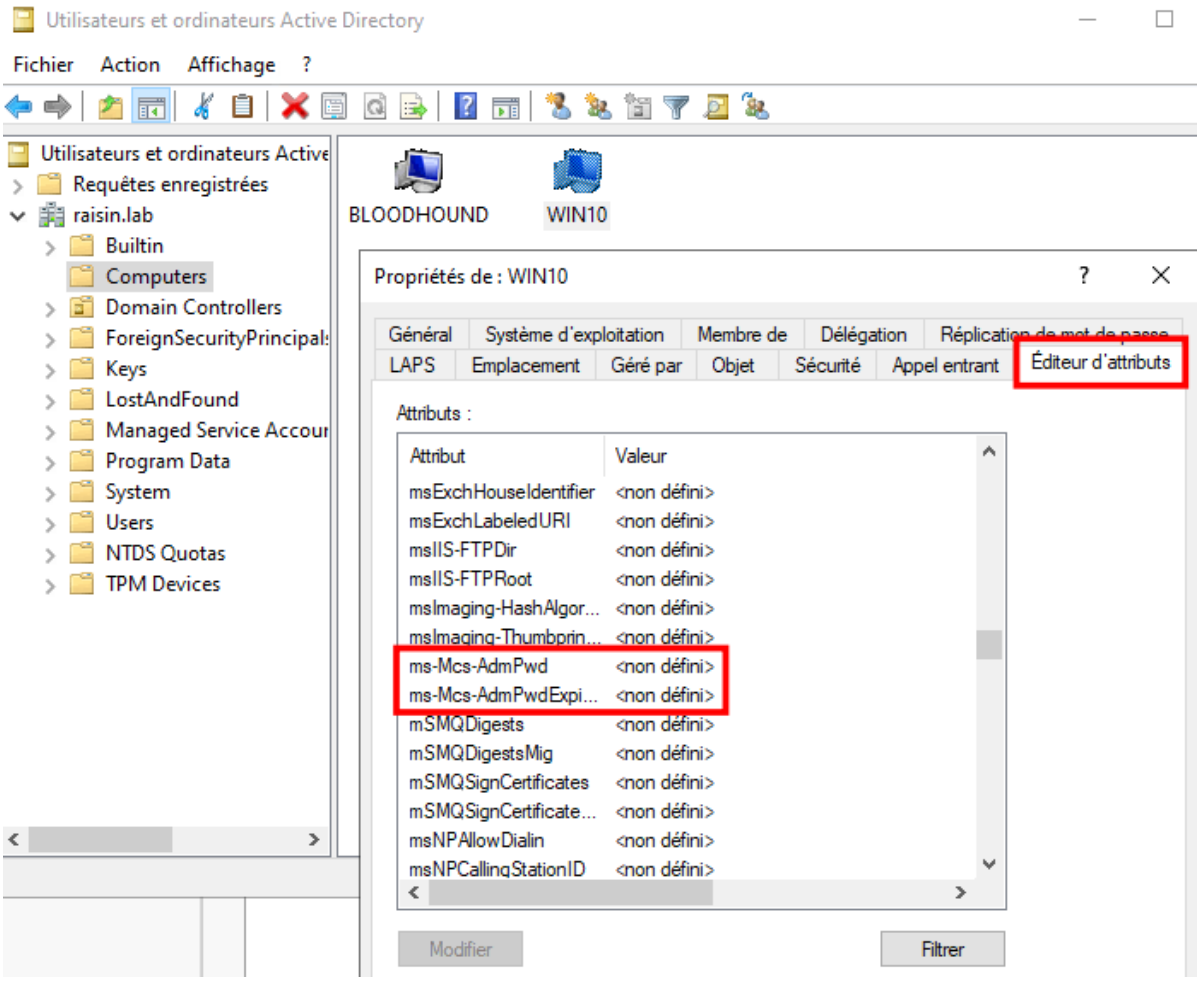
```
PS C:\Users\Administrateur> Import-Module AdmPwd.PS
PS C:\Users\Administrateur> Update-AdmPwdADSchema

Operation           DistinguishedName                                          Status
---------           -----------------                                          ------
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=r... Success
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=raisin,DC=lab    Success
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=raisin,DC=lab         Success
```

d) Vérifier l'apparition des 2 nouveaux attributs

Activer les fonctionnalités avancées



Noter la présence des attributs



e) Attribuer les droits d'écriture sur les attributs 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'AD la **date d'expiration** et le **mot de passe**.

Cela se fait via la commande PowerShell :

> **Set-AdmPwdComputerSelfPermission -OrgUnit "CN=Computers,DC=raisin,DC=lab"**

```
PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit "CN=Computers,DC=raisin,DC=lab"

Name                DistinguishedName                                                Status
----                -----------------                                                ------
Computers           CN=Computers,DC=raisin,DC=lab                                    Delegated
```

f) Gestion des permissions : restriction des droits en lecture sur les attributs étendus

Afin d'empêcher les utilisateurs ou des groupes de voir les mots de passes (stockés en clair), nous devons supprimer le droit "Tous les droits étendus" des utilisateurs et des groupes qui ne sont pas autorisés à lire la valeur de l'attribut ms-Mcs-AdmPwd. Cela est nécessaire car le droit "Tous les droits étendus" donne également la permission de lire les attributs confidentiels.

On peut déjà voir qui possède ces droits via la commande PowerShell suivante :

> **Find-AdmPwdExtendedrights -Identity "CN=Computers,DC=raisin,DC=lab" | Format-Table**

```
PS C:\Users\Administrateur> Find-AdmPwdExtendedrights -Identity "CN=Computers,DC=raisin,DC=lab" | Format-Table

ObjectDN                                ExtendedRightHolders
--------                                --------------------
CN=Computers,DC=raisin,DC=lab           {AUTORITE NT\Système, RAISIN\Admins du domaine}
```

Ici on peut voir que les membres du groupe "Admins du domaine" ont un accès à ces informations : c'est normal, c'est la configuration par défaut.

Ajouter des utilisateurs / groupes qui auront accès à ces attributs

> Set-AdmPwdReadPasswordPermission -OrgUnit "CN=Computers,DC=raisin,DC=lab" -AllowedPrincipals raisin\toto,raisin\utilisateurs33

> Set-AdmPwdResetPasswordPermission -OrgUnit "CN=Computers,DC=raisin,DC=lab" -AllowedPrincipals raisin\toto,raisin\utilisateurs33

5°/ Implication pour la sécurité de machines jointes à un environnement Active Directory

⚠️ Il est fortement recommandé de configurer l'annuaire Active Directory pour interdire aux utilisateurs d'ajouter des ordinateurs au domaine : sinon l'utilisateur disposera des droits pour lire le mot de passe de l'ordinateur qu'il a ajouté lui-même au domaine. Par défaut, chaque utilisateur peut ajouter jusqu'à 10 machines au domaine (selon un quota définit au sein de l'attribut msDS-MachineAccountQuota) sans avoir besoin des droits d'administrateur au niveau du domaine. ⚠️

> Get-ADObject -Identity "DC=raisin,DC=lab" -Properties MS-DS-MachineAccountQuota

```
PS C:\Users\Administrateur> Get-ADObject -Identity "DC=raisin,DC=lab" -Properties MS-DS-MachineAccountQuota


DistinguishedName         : DC=raisin,DC=lab
MS-DS-MachineAccountQuota : 10
Name                      : raisin
ObjectClass               : domainDNS
ObjectGUID                : bfb4b03c-60fa-4a02-bcf3-465c9215992d
```

Pour modifier le quota, on peut exécuter la commande suivante :

> Set-ADDomain -Identity "DC=raisin,DC=lab" -Replace @{"ms-DS-MachineAccountQuota"="0"}

Autre méthode, via une GPO qui modifie les autorisations par défaut :

On va dans *Configuration ordinateur* > *Stratégies* > *Paramètres Windows* > *Paramètres de sécurité* > *Stratégies locales* >> **Attribution des droits utilisateurs**

On modifie le paramètre **Ajouter des stations de travail au domaine** en supprimant ~~Utilisateurs authentifiés~~ et en le remplaçant par **Administateurs**

6°/ Configuration de la GPO 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.

Il existe deux fichiers qui ont été installés par LAPS :

> C:\Windows\PolicyDefinitions\AdmPwd.admx
> C:\Windows\PolicyDefinitions\en-US\AdmPwd.adml

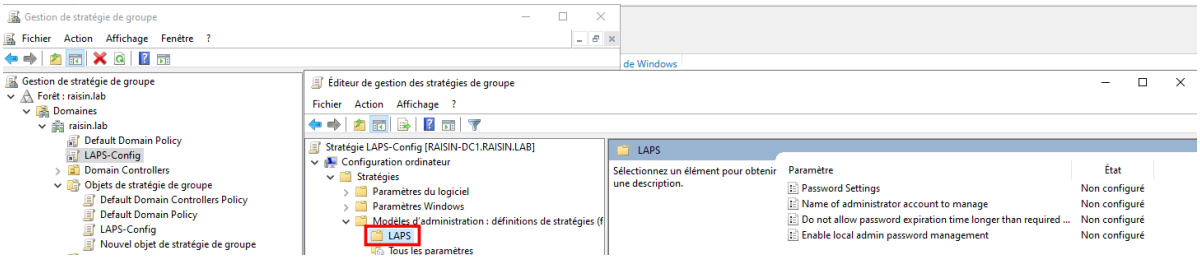
Il faut les copier vers les emplacements suivants :

> C:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions
> C:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions\en-US

On peut copier / coller les lignes suivantes :

```
cd C:/Windows/PolicyDefinitions
mkdir c:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions
mkdir c:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions\en-US
cp AdmPwd.admx c:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions
cp en-US\AdmPwd.adml c:\Windows\SYSVOL\sysvol\raisin.lab\Policies\PolicyDefinitions\en-US
```

Ensuite nous allons créer une **GPO** que nous appellerons **LAPS-Config** (à faire dans l'OU hébergeant les machines qui n'existe pas ici). Puis nous allons dans *Configuration ordinateur* > *Stratégies* > *Modèles d'administration : définitions de stratégies*. Comme nous avons précédemment importé les fichiers **ADMX** / **ADML** dans **SYSVOL**, nous pouvons voir une nouvelle catégorie : **LAPS**



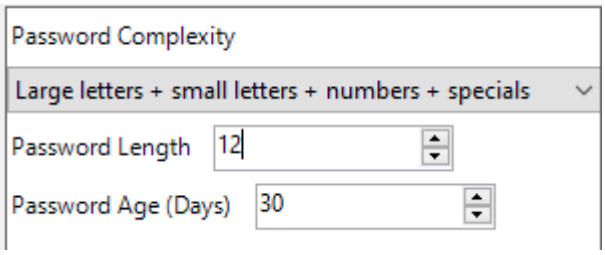
Explication des paramètres :

- **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.

a) Configuration des paramètres

Pour **Password Settings**, on l'active et on met par exemple la configuration suivante :

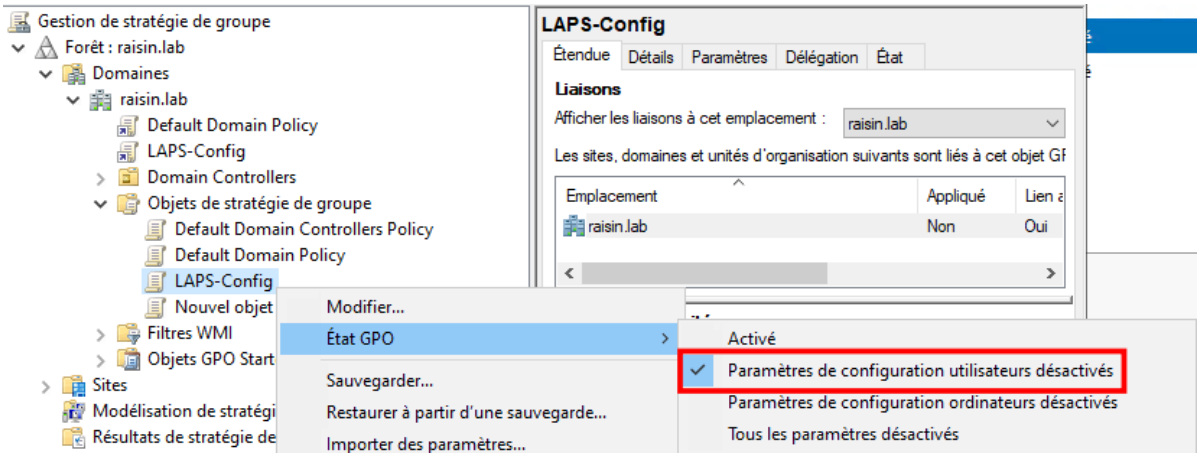


Ensuite, nous allons activer deux autres paramètres donc il suffit de les basculer sur l'état "Activé" :

```
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 sur notre poste de tests. Il conviendra de l'activer et le configurer en fonction de vos besoins. Vous pouvez fermer la GPO puisqu'elle est prête.

Comme cette GPO ne contient uniquement que des paramètres ordinateur, nous allons désactiver le traitement des paramètres utilisateurs. Pour ce faire, cliquer droit sur la GPO puis sous "Etat GPO", cliquer sur "Paramètres de configuration utilisateurs désactivés".



7°/ Déploiement sur la machine cliente

On se rend sur la machine **WIN10** et on met à jour les GPOs :

```
gpupdate /force
```

On en profite pour installer **LAPS**. On peut le faire via déploiement GPO mais ici on le fera via Chocolaley :

```
choco install laps -y
```

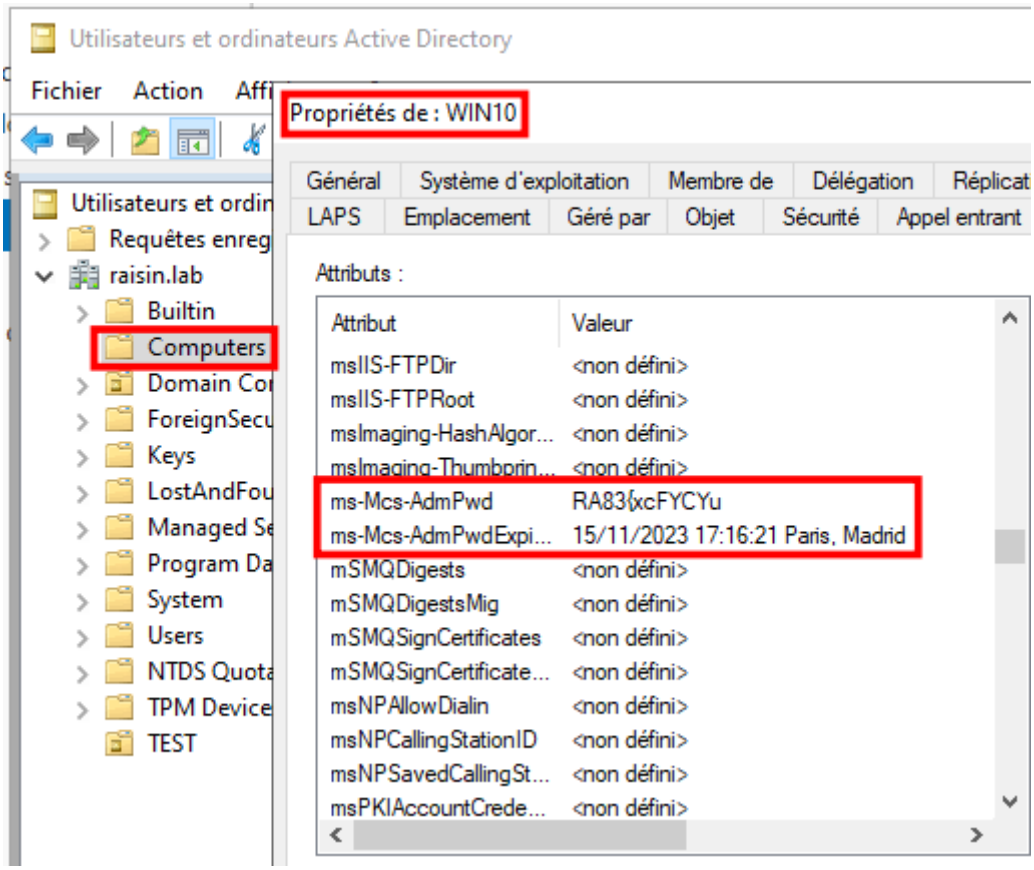
On redémarre ensuite la machine.

8°/ Utilisation de LAPS

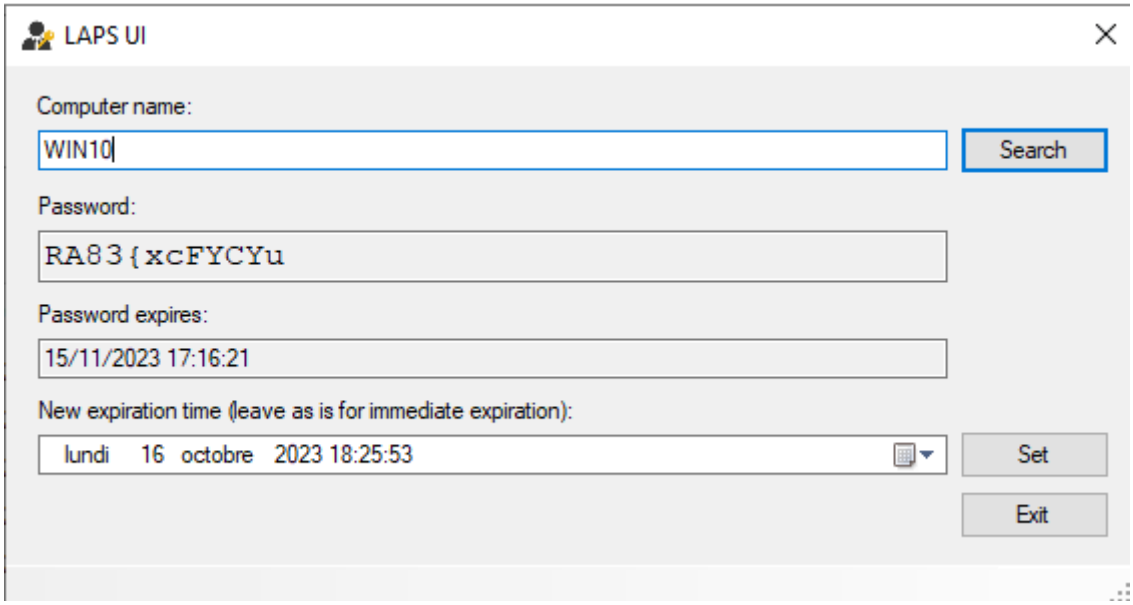
a) Afficher le mot de passe administrateur local

Si l'on se rend dans les propriétés de l'ordinateur **WIN10**, on peut voir deux nouvelles choses :

- Le mot de passe du compte administrateur local
- La date d'expiration du mot de passe



On peut retrouver ces informations en utilisant, depuis le contrôleur de domaine, LAPS UI :



Une troisième façon de récupérer le mot de passe se fait via PowerShell :

> Get-AdmPwdPassword -ComputerName WIN10

```
PS C:\Users\Administrateur> Get-AdmPwdPassword -ComputerName WIN10

ComputerName         DistinguishedName                          Password          ExpirationTimestamp
------------         -----------------                          --------          -------------------
WIN10                CN=WIN10,CN=Computers,DC=raisin,DC=lab     RA83{xcFYCYu      15/11/2023 17:16:21
```

Si l'on disposait de plusieurs machines Windows, on pourrait en une seule commande récupérer l'ensemble des mots de passe de ces machines via la commande PowerShell suivante :

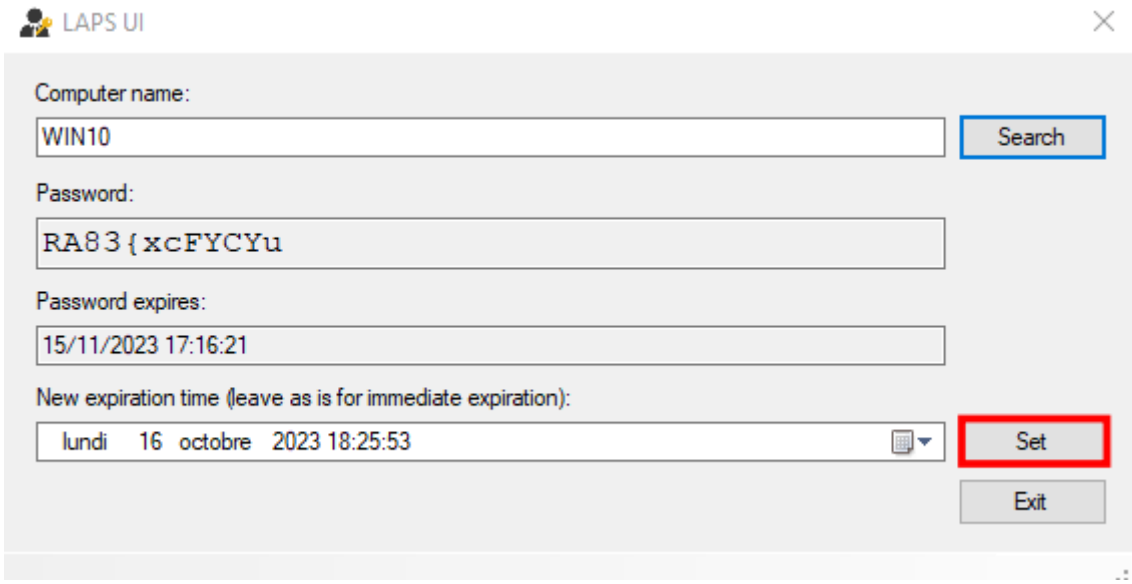
> Get-ADComputer -Filter * -SearchBase "CN=Computers,DC=raisin,DC=lab" | Get-AdmPwdPassword

```
ComputerName         DistinguishedName                          Password          ExpirationTimestamp
------------         -----------------                          --------          -------------------
WIN10                CN=WIN10,CN=Computers,DC=raisin,DC=lab     RA83{xcFYCYu      15/11/2023 17:16:21
BLOODHOUND           CN=BLOODHOUND,CN=Computers,DC=raisin,DC=lab                  01/01/0001 00:00:00
```

Ici, nous n'avons pas installé **LAPS** sur la machine **BLOODHOUND**.

b) Réinitialiser le mot de passe administrateur local

Si depuis **LAPS UI** on clique sur le bouton **Set**, alors le mot de passe expire immédiatement :



Lorsque la machine redémarrera (initialisation de la GPO Ordinateur), alors un nouveau mot de passe sera configuré.

Si l'on modifie la date d'expiration, alors on repousse l'expiration du mot de passe à une date ultérieure par rapport à celle qui était prévue.

Si on veut réinitialiser le mot de passe immédiatement en PowerShell :

```
Reset-AdmPwdPassword -ComputerName WIN10
```

Si on veut réinitialiser la date d'expiration immédiatement en PowerShell :

```
Reset-AdmPwdPassword -ComputerName WIN10 -WhenEffective "15.12.2023 07:00"
```

c) Modification du niveau de log de LAPS sur une machine cliente

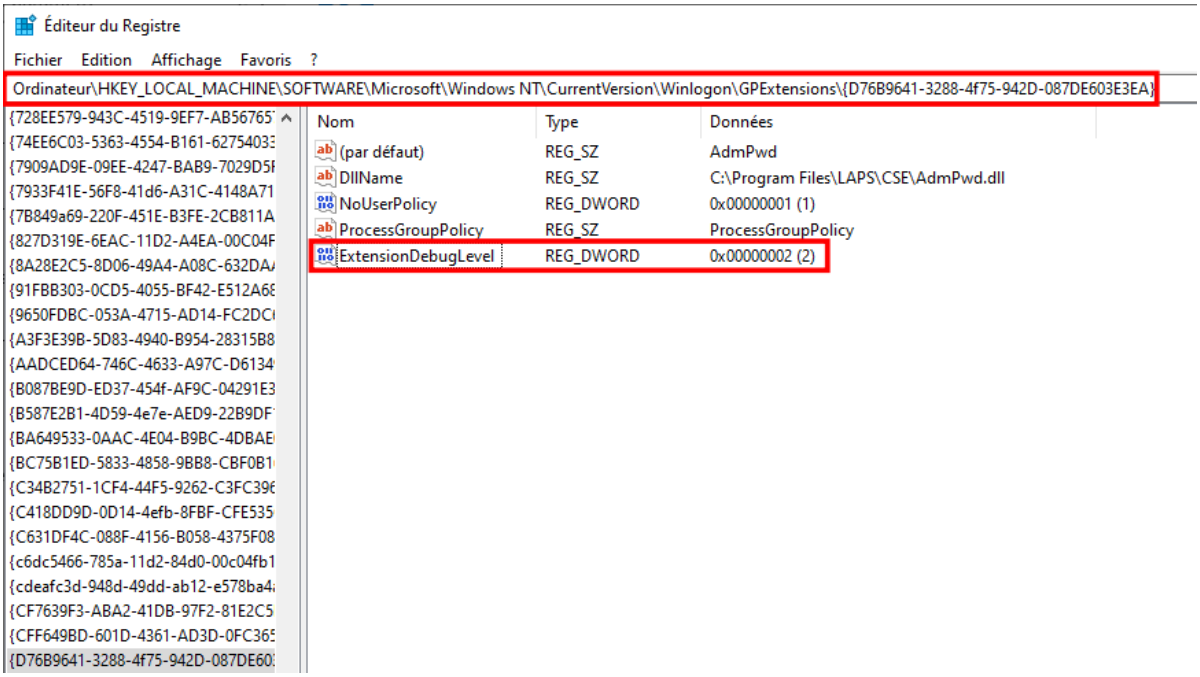
Il faut dans un premier temps utiliser RegEdit sur la machine cliente pour créer une clef de registre.

On se rend à l'adresse :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions{D76B9641-3288-4f75-942D-087DE603E3EA}
```

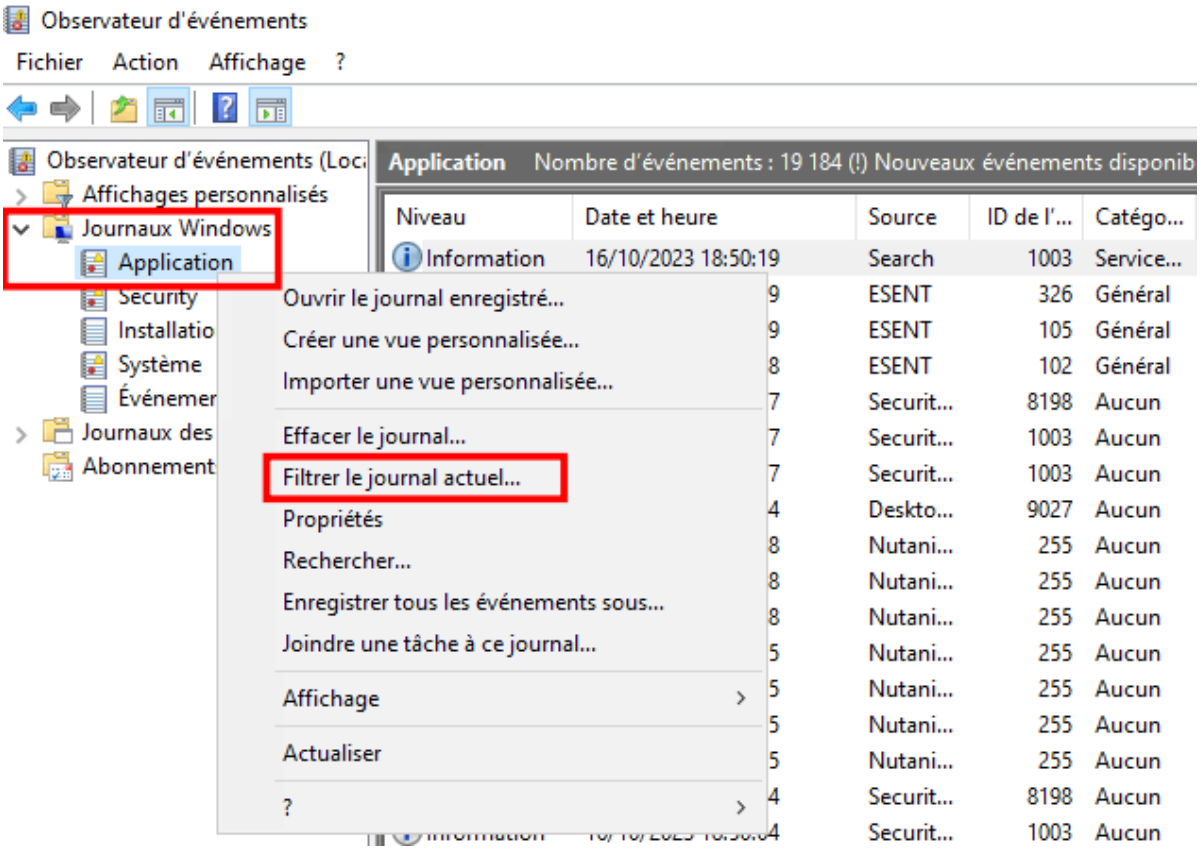
Puis on créer une valeur **DWORD 32 bits** qui se nomme **ExtensionDebutLevel**. Cette valeur peut être :

- 0 : Erreurs.
- 1 : Erreurs / Avertissements.
- 2 : Erreurs / Avertissements / Infos.

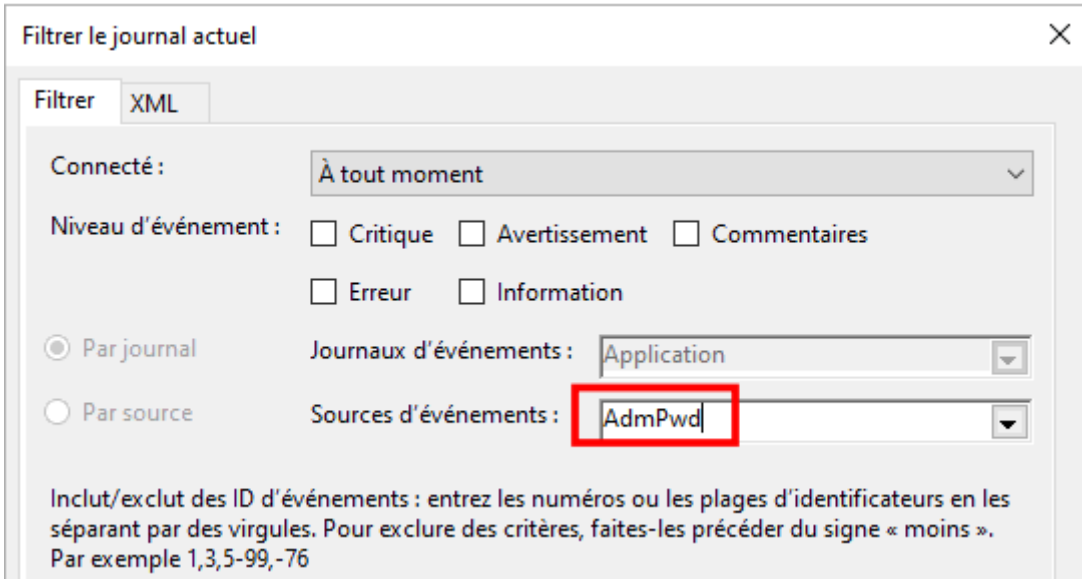


Nous allons mettre 2 pour voir ce que cela produit. Une fois que c'est fait, on redémarre la machine.

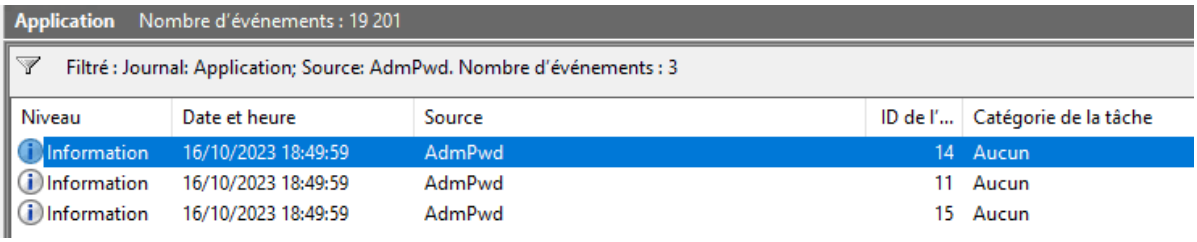
Nous ouvrons ensuite l'**observateur d'événements** :



Nous y appliquons un filtre : **AdmPwd**



Et nous obtenons :



Sur ces 3 logs, dans l'ordre nous avons comme résultats :

- **Beginning processing**
- **It is not necessary to change password yet. Days to change: 30**
- **Finished successfully**

LAPS est capable de générer des logs d'erreurs pour différents événements et notamment :

- **Le client LAPS n'est pas en mesure de réinitialiser le mot de passe Administrateur**
- **Le client LAPS ne parvient pas à écrire le nouveau mot de passe dans l'Active Directory**

d) Activer l'audit LAPS sur le contrôleur de domaine

Pour activer les logs, il faut saisir la commande suivante en PowerShell :

> Set-AdmPwdAuditing -OrgUnit "CN=Computers,DC=raisin,DC=lab" -AuditedPrincipals "Admins du domaine"

```
PS C:\Users\Administrateur> Set-AdmPwdAuditing -OrgUnit "CN=Computers,DC=raisin,DC=lab" -AuditedPrincipals "Admins du domaine"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
Computers           CN=Computers,DC=raisin,DC=lab                      Delegated
```

On peut cibler plusieurs groupes en les séparant par une virgule.

Vérifions à présent que cela fonctionne. Pour cela nous allons lancer la commande PowerShell permettant de récupérer le mot de passe du compte Administrateur local sur la machine **WIN10**.

> Get-AdmPwdPassword PC-01

Un événement va être généré depuis l'**Observateur d'événements** dans *Journaux Windows* > *Sécurité* ayant pour *ID de l'événement* **4662**