Active Directory - Mise en place de Windows LAPS

Difficulté : Intermédiaire

Notions : Active directory, schema active directory, ADSI edit, GPO.

> **Attention** : Microsoft LAPS est désormais déprécié, il faut maintenant utiliser le module Windows LAPS disponible sur AD et le module client disponible nativement sur Windows 10 (depuis la mise à jour d'avril 2023) et Windows 11.

I. Introduction

Dans le cadre de la sécurisation du parc, il peut être intéressant de déployer LAPS.

LAPS (**L**ocal **A**dministrator **P**assword **S**olution) est, comme son nom l'indique, une solution permettant de gérer les mot de passe des administrateurs locaux.

Sur le principe, un agent est installé sur les poste et paramétré par GPO. Une fois cela fait, les mots de passe des Administrateurs locaux seront automatiquement gérés par l'active directory et

enregistrés dans les attributs du compte machine.

Cela permet les choses suivantes :

- Ils seront définis suivant la politique de mot de passe choisis.
- Ils seront changés automatiquement sur une période définie.
- Ils seront générés aléatoirement et stockés de façon sécurisé dans les attributs Active Directory de la machine.

Pour les consulter, il sera possible pour les administrateurs autorisés d'utiliser le client LAPS ou d'aller voir les attributs active Directory.

II. Installation sur le DC

> **Prerequis** : Vérifier les prérequis suivants.

- schéma du DC en 2008R2 ou plus
- .Net 4.0 ou plus
- Powershell 2.0 ou plus.
- la mise à jour kb5025230 (avril 2023) est déployée sur les DC et l'ensemble des postes concernés.
  - Disponible ICI ou sur WSUS / windows update

2.1 Préparer le schéma AD

Vérifier que les commandes du module sont disponible avec la commande :

```
Get-Command -Module LAPS
```

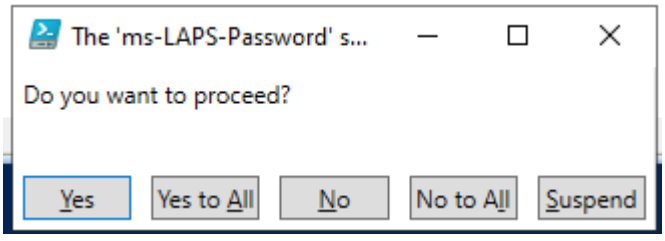
```
PS C:\Users\Administrator> Get-Command -Module LAPS

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Get-LapsAADPassword                                1.0.0.0    LAPS
Function        Get-LapsDiagnostics                                1.0.0.0    LAPS
Cmdlet          Find-LapsADExtendedRights                          1.0.0.0    LAPS
Cmdlet          Get-LapsADPassword                                 1.0.0.0    LAPS
Cmdlet          Invoke-LapsPolicyProcessing                        1.0.0.0    LAPS
Cmdlet          Reset-LapsPassword                                 1.0.0.0    LAPS
Cmdlet          Set-LapsADAuditing                                 1.0.0.0    LAPS
Cmdlet          Set-LapsADComputerSelfPermission                   1.0.0.0    LAPS
Cmdlet          Set-LapsADPasswordExpirationTime                   1.0.0.0    LAPS
Cmdlet          Set-LapsADReadPasswordPermission                   1.0.0.0    LAPS
Cmdlet          Set-LapsADResetPasswordPermission                  1.0.0.0    LAPS
Cmdlet          Update-LapsADSchema                                1.0.0.0    LAPS
```

Lancer la préparation du schéma :

```
Update-LapsADSchema -Verbose
```

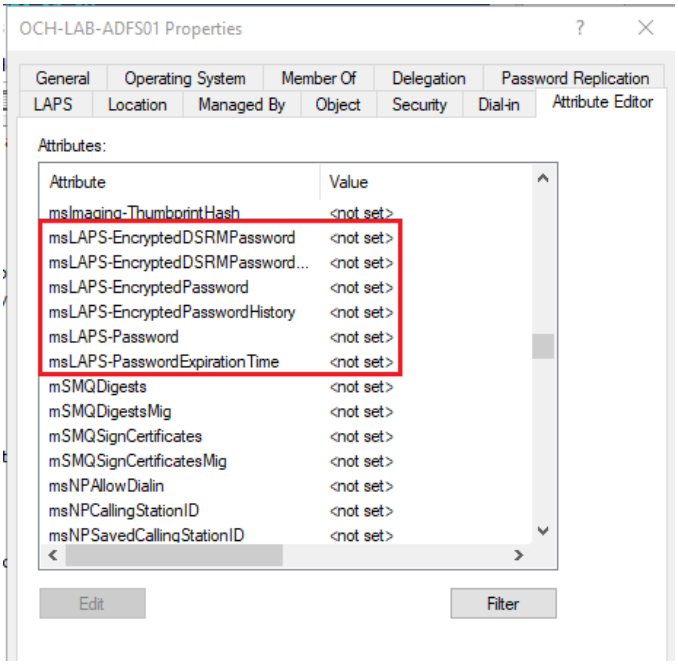
```
PS C:\Users\Administrator> Update-LapsADSchema -Verbose
VERBOSE: BeginProcessing started
VERBOSE: Verifying that current machine is AD domain-joined
VERBOSE: Success: current machine is domain-joined to 'LABS404'
VERBOSE: Creating LDAP binding to specified domain controller 'localhost'
VERBOSE: Port not specified - will default to 389
VERBOSE: Successfully created LDAP binding
VERBOSE: Calling DC-locator to locate a DC in the  domain
VERBOSE: DC-locator succeeded:
VERBOSE: Name:OCH-LAB-ADDS01.labs404.fr Address:\\172.20.0.1 AddressType:1 DomainGuid:0dcecb63-8fd7-489d-a322-0c0a444fa6a7 DomainDnsName:labs404.f
r ForestDnsName:labs404.fr Flags:0xe003f3fd DcSiteName:SC-Datacenter ClientSiteName:SC-Datacenter
VERBOSE: Binding to domain controller OCH-LAB-ADDS01.labs404.fr
VERBOSE: Bound LDAP connection to schema FSMO OCH-LAB-ADDS01.labs404.fr
VERBOSE: Successfully bound to domain controller:
VERBOSE:  DC: OCH-LAB-ADDS01.labs404.fr
VERBOSE:  DC functional level: 7
VERBOSE:  Domain info:
VERBOSE:    Domain DNS name: labs404.fr
VERBOSE:    Domain NC: DC=labs404,DC=fr
VERBOSE:    Domain functional level: 7
VERBOSE:  Forest info:
VERBOSE:    Forest DNS name: labs404.fr
VERBOSE:    Forest NC: DC=labs404,DC=fr
VERBOSE:    Config NC: CN=Configuration,DC=labs404,DC=fr
VERBOSE:    Schema NC: CN=Schema,CN=Configuration,DC=labs404,DC=fr
VERBOSE:    Forest functional level: 7
VERBOSE: BeginProcessing completed
```

Si le message suivant apparaît, faire '***Yes to All***'.

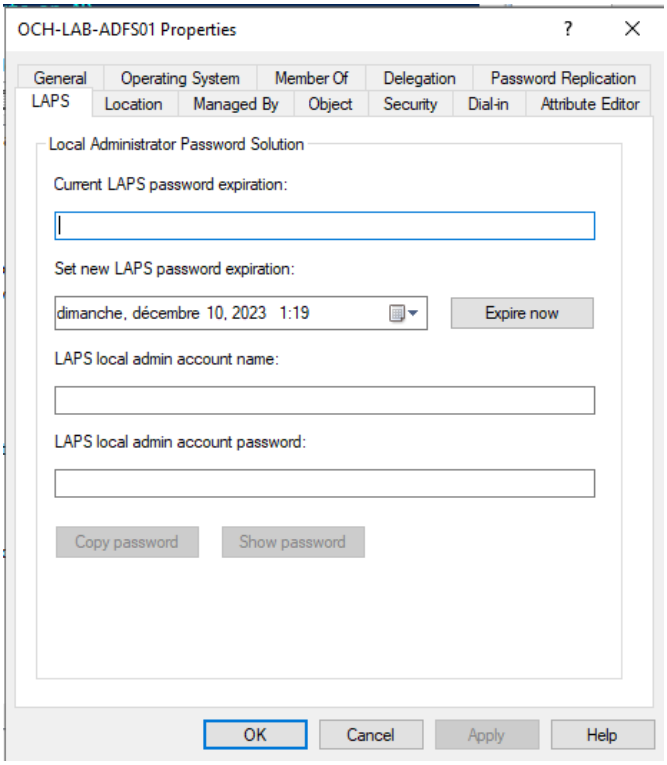


Vérifier sur le verbose que tout ce soit bien déroulé.

Puis vérifier la présence des éléments suivants sur les objets machines :



Présence des attributs dans les objets AD sur une machine.



*Ajout de l'onglet '**LAPS**'*

2.2 Créer les délégations machines

Pour que les machines puissent avoir le droit de mettre à jour le mot de passe dans leurs attributs respectifs, il va falloir leur ajouter une délégation sur les OU machines.

Cela se fait avec la commande :

```
Set-LapsADComputerSelfPermission -Identity "OU=<votreOU>,DC=<domain>,DC=<ext>"
```

> **Note** : Les autorisations sont récursives et s'appliquent sur les OU enfants.

```
PS C:\Users\Administrator> Set-LapsADComputerSelfPermission -Identity "OU=Machines,OU=LABS404,DC=LABS404,DC=FR"

Name     DistinguishedName
----     -----------------
Machines OU=Machines,OU=LABS404,DC=labs404,DC=fr
```

III. Mise en place des GPO

3.1 Ajout des templates de GPO

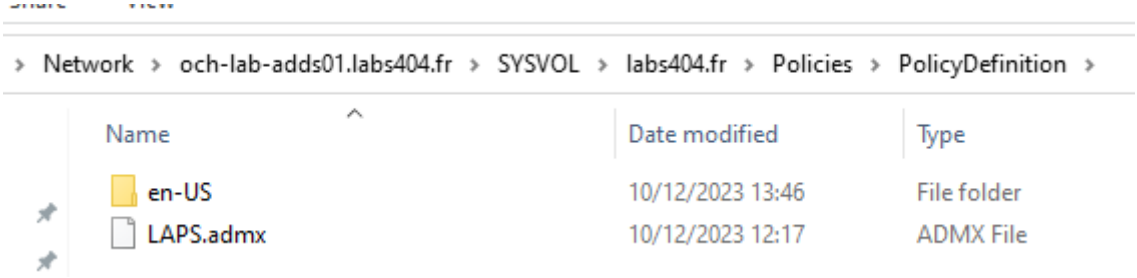
Pour une mise en place efficace de l'outil, il est bon de les configurer par GPO. Cela évitera une gestion manuelle des clients.

Pour cela, il faut importer les ADMX LAPS.

Créer dans '***\\<FQDN.du.pdc>\SYSVOL\labs404.fr\Policies***' le dossier '***PolicyDefinition***'.

Créer dans ce dossier le dossier correspondant à la localisation voulue : fr-FR ou en-US par exemple.

Aller dans '***C:\Windows\PolicyDefinitions***' et copier les fichiers '***LAPS.admx***' et le fichier de traduction correspondant dans les répertoires créés précédemment.

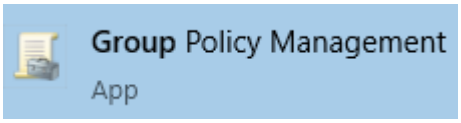


3.2 Création de la GPO

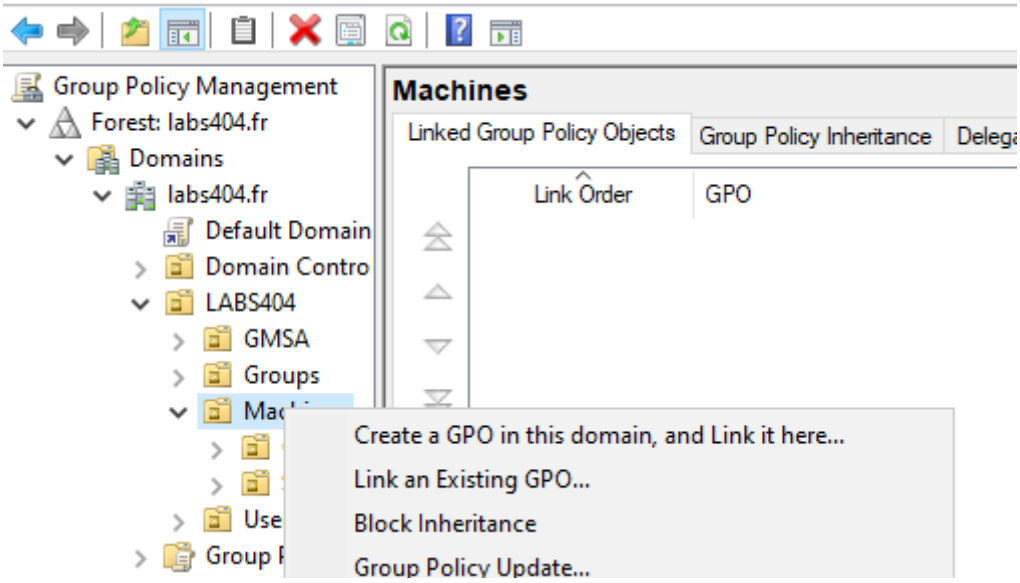
Il va falloir créer une GPO Ordinateur pour l'appliquer sur les systèmes.

> **Astuce** : Pour le nom des GPO dans le labs404, se référer à Noms des GPO

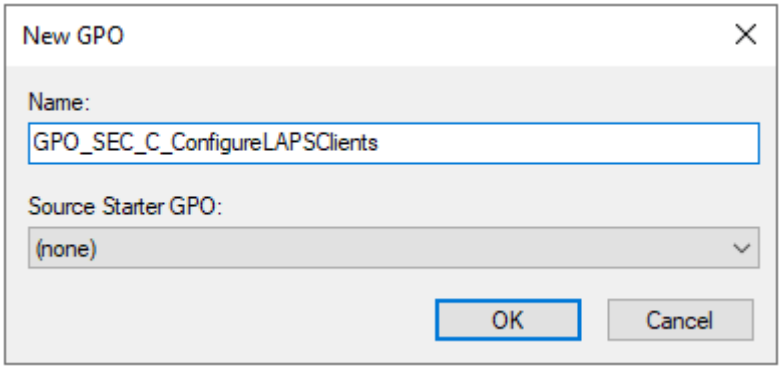
Dans la console '***Group Policy Management***'



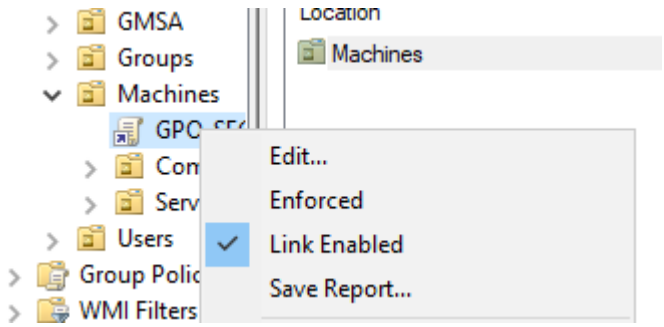
Faire un clic droit sur l'OU contenant les machines puis '***Create a GPO in this domain, and Link it here***'



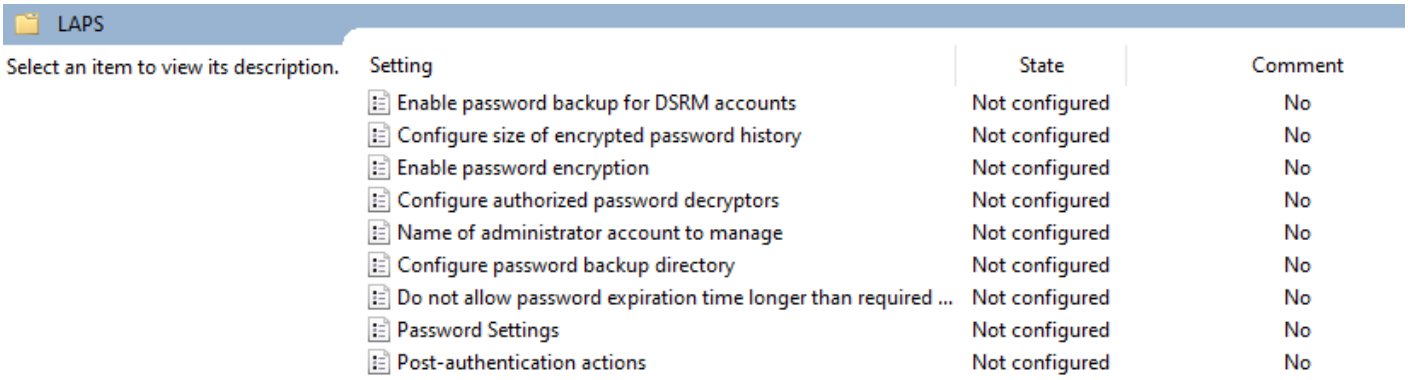
Nommer la GPO et valider.



Puis clic droit sur la GPO créée er '***Edit***'.



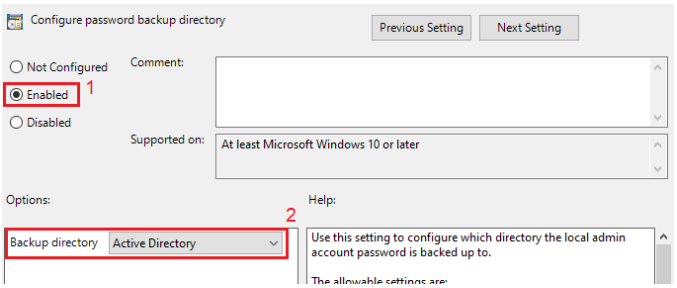
Les paramètres à modifier sont dans : '***Computer Configuration --> Policies --> Administratives Tmplates --> System --> LAPS***'



Voici la liste des paramètres :

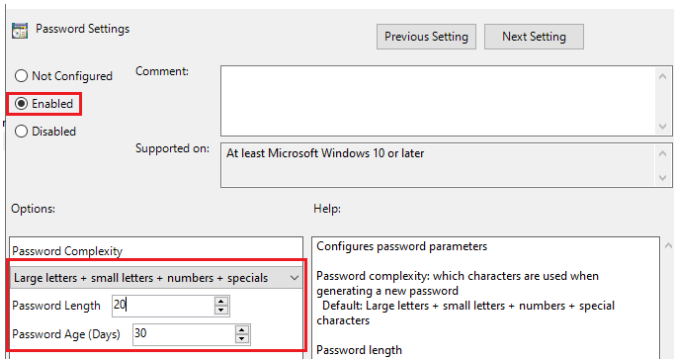
Configure '***password backup directory***' :

1. Enabled
2. Active directory



Configurer '***Password Setting***'

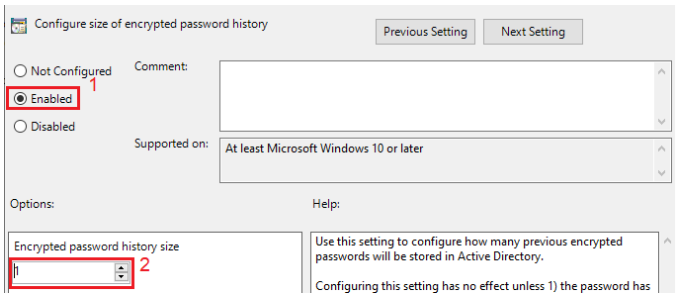
1. Enabled
2. Complexity
3. Password Length
4. Password Age (Days)



Configurer '***Size of encrypted password history***'

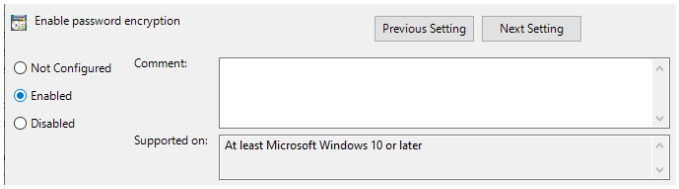
1. Enabled
2. 1

Cela permettra si jamais un mot de passe est mal renouvelé par une machine, d'accéder à l'ancien mot de passe.



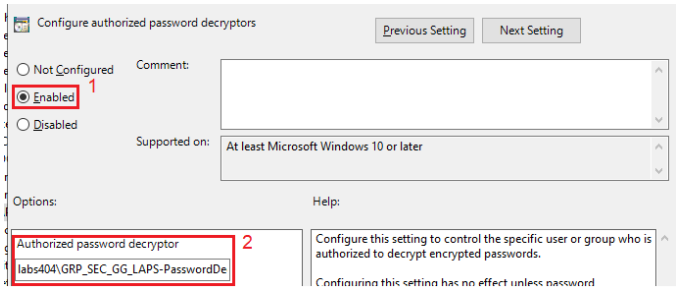
Configurer '***Enable Password Encryption***'

1. Enabled



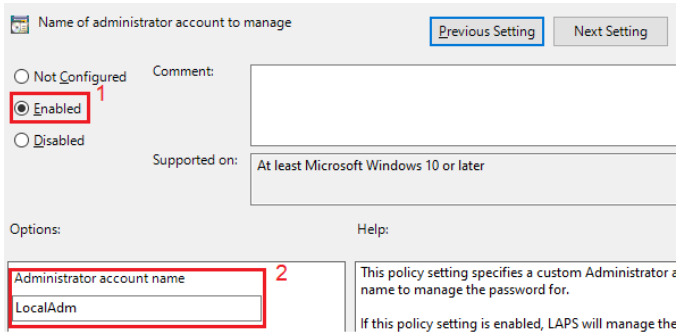
Configurer '***Authorized password decryptors***'

1. Enabled
2. Nom du groupe AD au format <dom\group>



(optionnel)
Si un compte autre que Administrator est utilisé
Configurer '***Name of the administrator account***'

1. Enabled
2. Nom du compte local



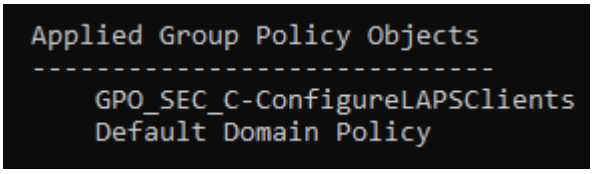
Enregistrer la GPO.

IV. Appliquer sur les clients

Pour appliquer la GPO sur les clients, 2 solutions :

Appliquer la GPO de manière classique et redémarrer.

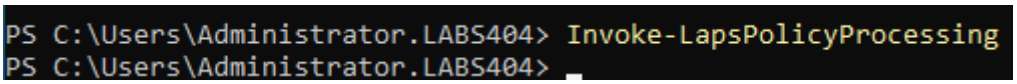
```
gpupdate /force
```



OU

Forcer l'enrôlement de la device avec

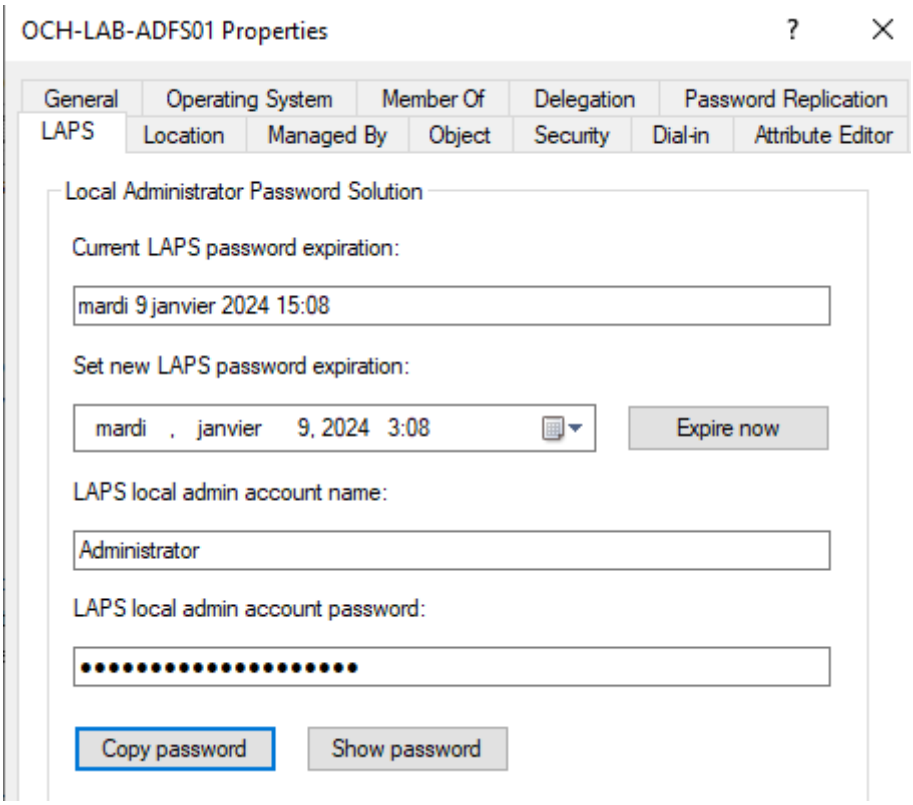
```
Invoke-LapsPolicyProcessing
```



V. Opérations supplémentaires

5.1 Consulter les mots de passes

Sur '***Active directory user & computer***' faire un clic droit sur l'ordinateur et aller dans l'onglet '***LAPS***'.



Les boutons 'Copy password' et 'show password' seront utilisables pour manipuler le mot de passe stocké.

Le boutton 'Expire Now' va forcer l'expiration et donc le renouvellement d'un mot de passe. Cel est utile si un mot de passe est compromis.

Le mot de passe peut également être récupéré en powershell avec l'applet :

```
Get-LapsADPassword "<NomDePoste>" -AsPlainText
```

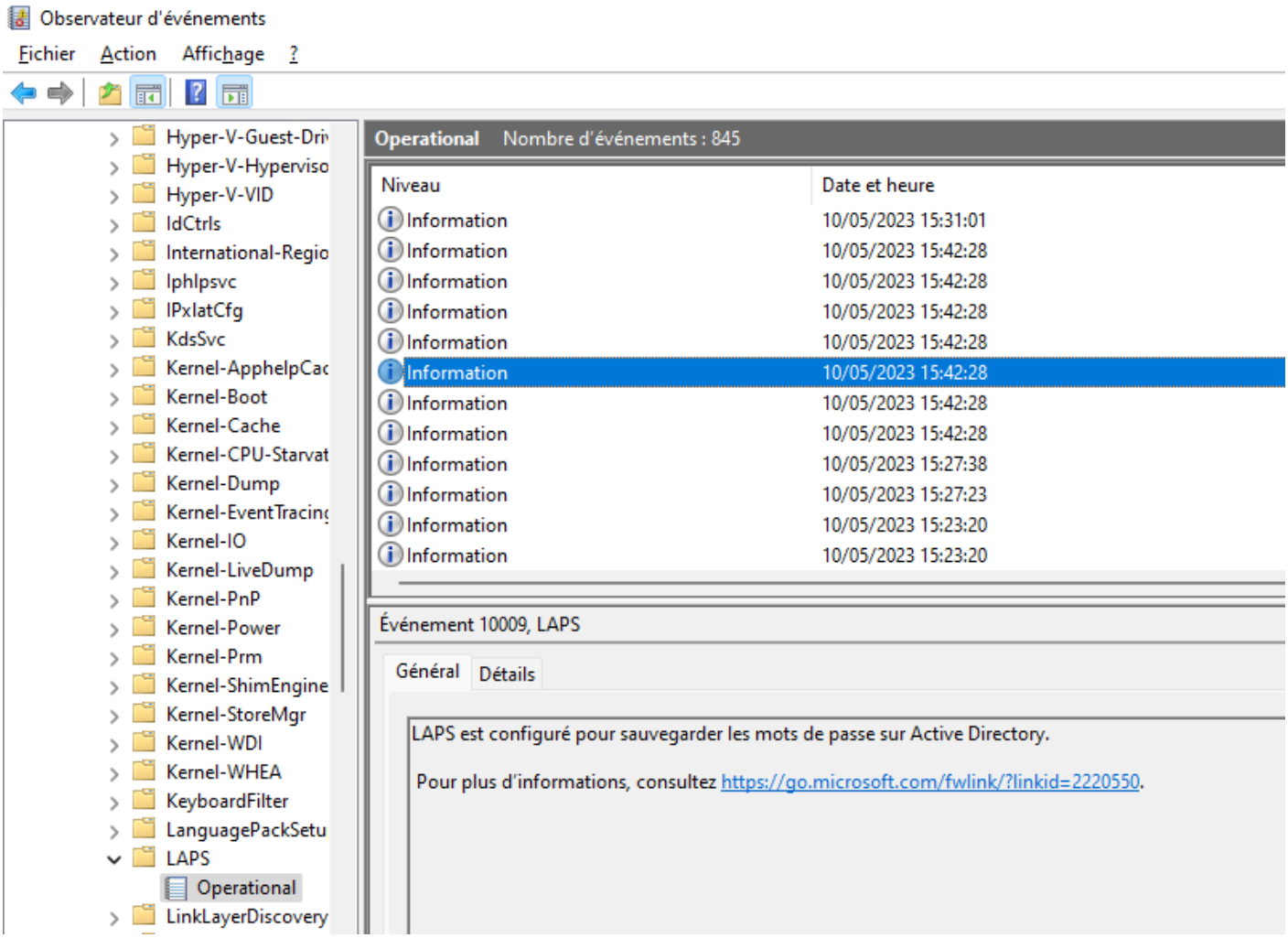
Pour voir le mot de passe ainsi que les précédents :

```
Get-LapsADPassword "PC-01" -AsPlainText -IncludeHistory
```

5.2 Consulter les événements LAPS

Les évènements LAPS sont enregistrés dans le journal d'événement windows suivant :

Applications and security --> Microsoft --> Windows --> LAPS --> Operational



> Ces journaux d'événements sont présents à la fois côté serveur et côté client.

Revision #2
Created 2026-07-30 08:30:08 UTC by Olivier
Updated 2026-07-30 08:33:03 UTC by Olivier