LAPS

LAPS (Local Administrator Password Solution) est un outil développé par Microsoft qui permet de gérer automatiquement les mots de passe du compte administrateur local des ordinateurs dans un domaine Active Directory.

Installer laps sur l'adsecure1

Mettre à jour le schéma AD en ajoutant LAPS via PowerShell :

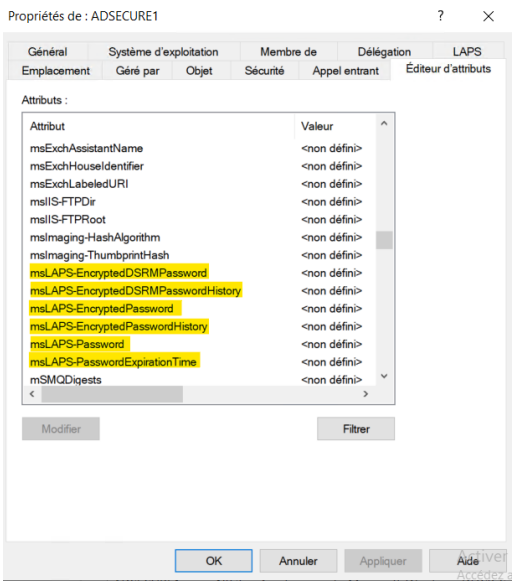
Get-Command -Module LAPS

Import-Module LAPS

Update-LapsADSchema -Verbose > oui à tout

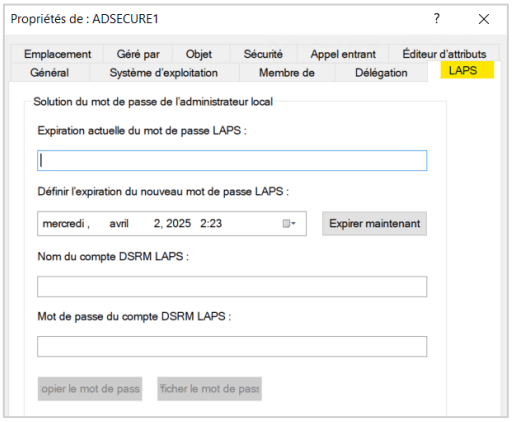
Dans **utilisateurs et ordinateurs active directory**, on fait un clic droit sur l'ordinateur ADSecure1 et on se rend dans les propriétés, dans éditeur d'attributs, et on vérifie que tout s'est bien installé.

(Si l'onglet « Éditeur d'attributs » n'apparaît pas, il faut activer les fonctionnalités avancées en cochant l'option « Fonctionnalités avancées » dans le menu « Affichage » de la console Utilisateurs et ordinateurs Active Directory.)



On peut voir en jaune sur la capture ci-contre que les attributs liés à LAPS sont bien présents et ont bien été installés.

L'onglet LAPS est également apparu :



Autorisation pour la machine de réécrire son objet sur active directory

Lorsqu'un poste de travail doit effectuer une rotation du mot de passe du compte administrateur géré par Windows LAPS, il doit sauvegarder ce mot de passe dans l'Active Directory. Pour cela, la machine doit avoir les permissions nécessaires pour écrire/modifier son propre objet dans l'Active Directory.

Les commandes suivantes permettent d'accorder cette autorisation sur l'unité d'organisation "PC", qui se trouve dans l'OU "Administration" et « Entrepôt », elles-mêmes situées dans l'OU "roncenoir" du domaine roncenoir.local.

Afin d'éviter toute confusion, notamment en cas d'unités d'organisation portant le même nom, il est recommandé d'utiliser le DistinguishedName complet de l'OU ciblée :

Set-LapsADComputerSelfPermission -Identity "OU=PC,OU=Administration,OU=roncenoir,DC=roncenoir,DC=local"

Set-LapsADComputerSelfPermission -Identity "OU=PC,OU=Entrepôt,OU=roncenoir,DC=roncenoir,DC=local"

```
PS C:\Users\Administrateur> Set-LapsADComputerSelfPermission -Identity "OU=PC,OU=Administration,OU=roncenoir,DC=roncenoir,DC=local"

Name DistinguishedName
---- -----------------
PC   OU=PC,OU=Administration,OU=Roncenoir,DC=roncenoir,DC=local


PS C:\Users\Administrateur> Set-LapsADComputerSelfPermission -Identity "OU=PC,OU=Entrepôt,OU=roncenoir,DC=roncenoir,DC=local"

Name DistinguishedName
---- -----------------
PC   OU=PC,OU=Entrepôt,OU=Roncenoir,DC=roncenoir,DC=local
```

Création GPO LAPS

La prochaine étape consiste à configurer Windows LAPS via une stratégie de groupe (GPO). Cette GPO définira la politique de mots de passe du compte administrateur géré, son emplacement de sauvegarde (Active Directory ou Azure AD) et le nom du compte concerné.

Avant cela, il faut importer les modèles d'administration (ADMX) de Windows LAPS. Si un magasin central existe dans le domaine, Windows ne lira pas les modèles locaux, donc l'importation est nécessaire. Sur le contrôleur de domaine, on récupère les deux fichiers suivants :

C:\Windows\PolicyDefinitions\LAPS.admx → Modèle d'administration de Windows LAPS

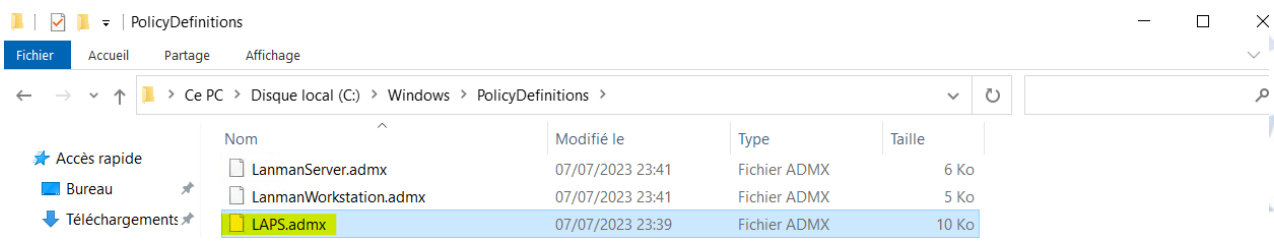
C:\Windows\PolicyDefinitions\fr-FR\LAPS.adml → Fichier de langue FR associé

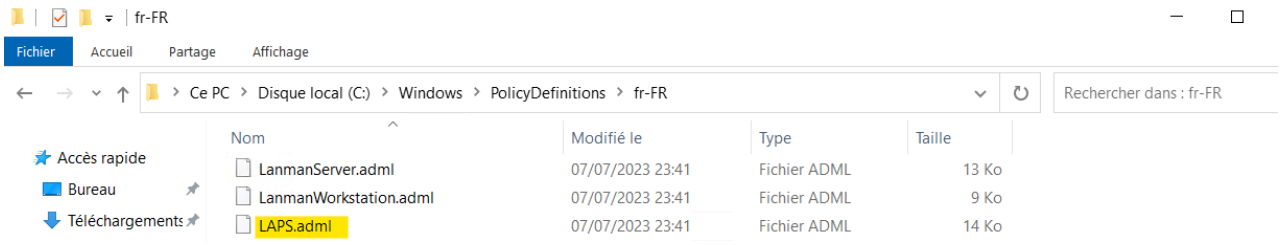
On les dépose dans le magasin central de votre partage SYSVOL :

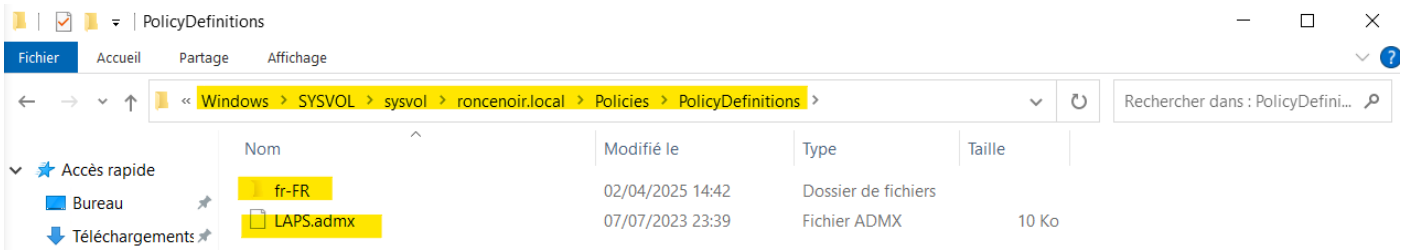
LAPS.admx → à la racine du dossier PolicyDefinitions

LAPS.adml → dans le sous-dossier fr-FR

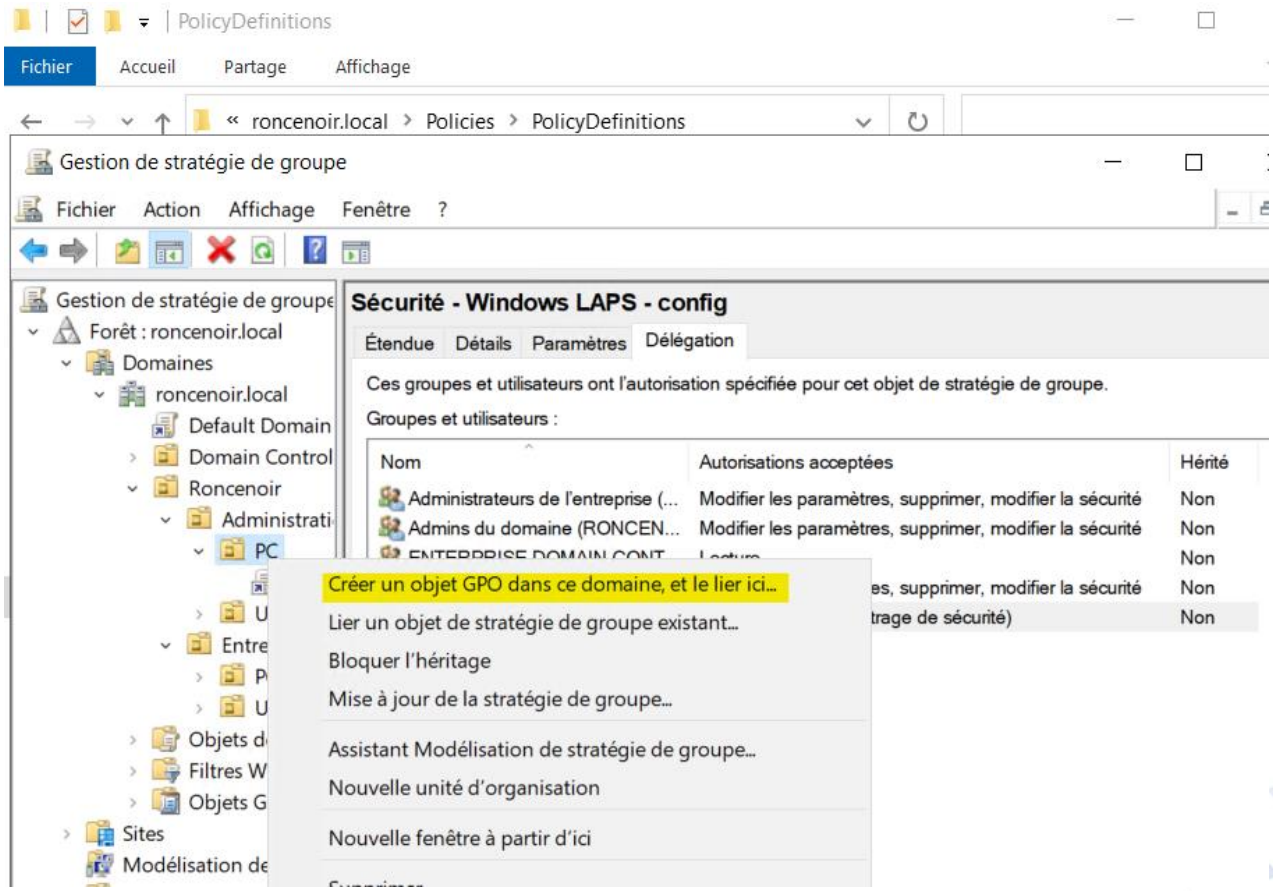
Cela permettra à la stratégie de groupe de prendre en charge Windows LAPS correctement.

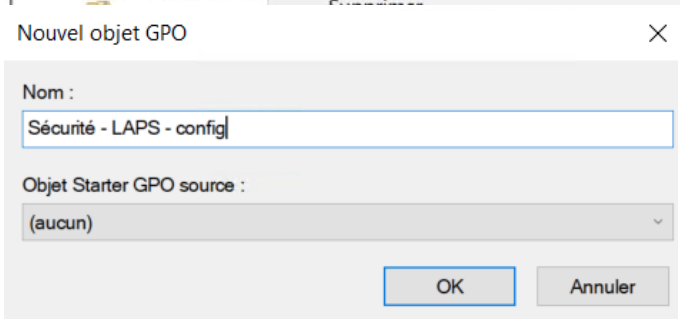


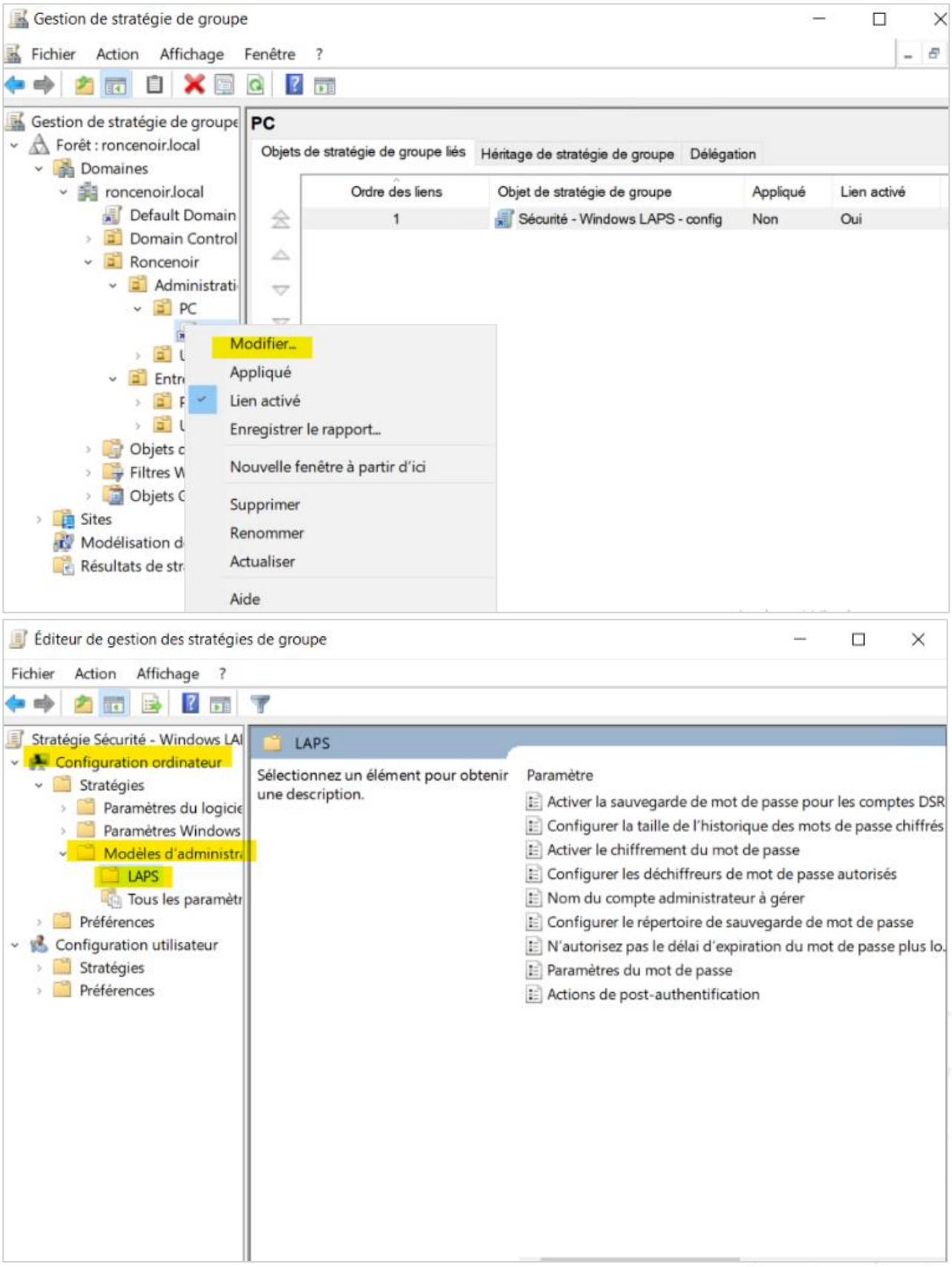




Une fois cette étape terminée, on crée une nouvelle GPO via Gestion de stratégies de groupe. Elle contiendra des paramètres de configuration ordinateur.





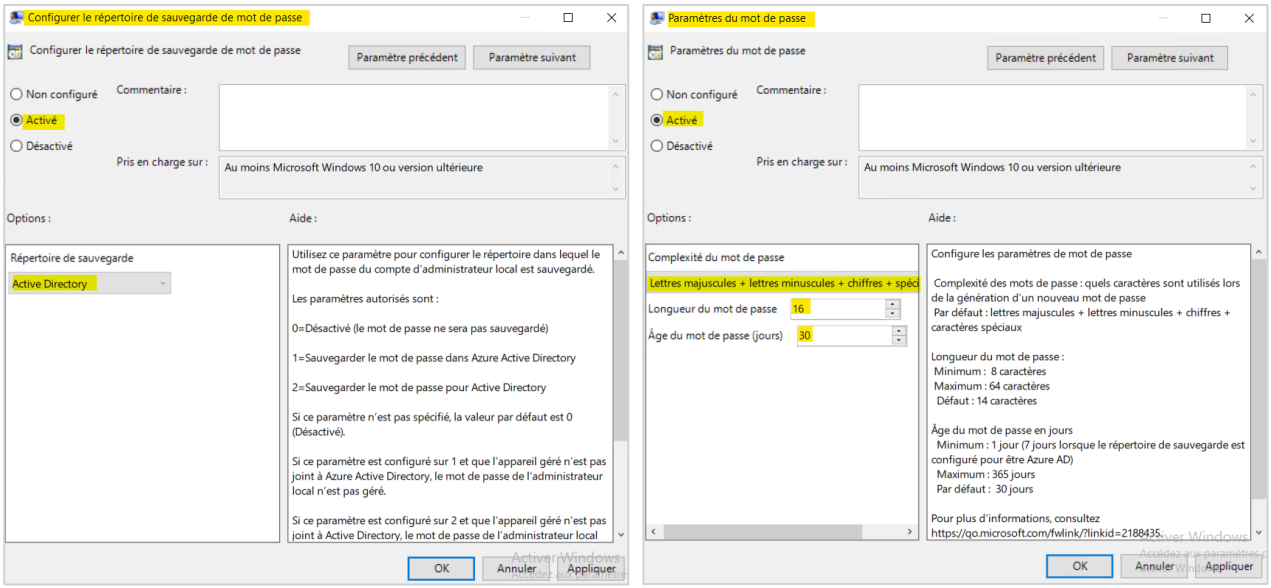


On commence par activer le paramètre "**Configurer le répertoire de sauvegarde de mot de passe**", indispensable pour activer Windows LAPS sur la machine. Il faut le passer à "Activé" et choisir "Active Directory".

Le deuxième paramètre à configurer est **"Paramètres du mot de passe"**, qui permet de définir la complexité du mot de passe pour le compte administrateur géré par Windows LAPS. Il faut l'activer et définir la politique de mot de passe.

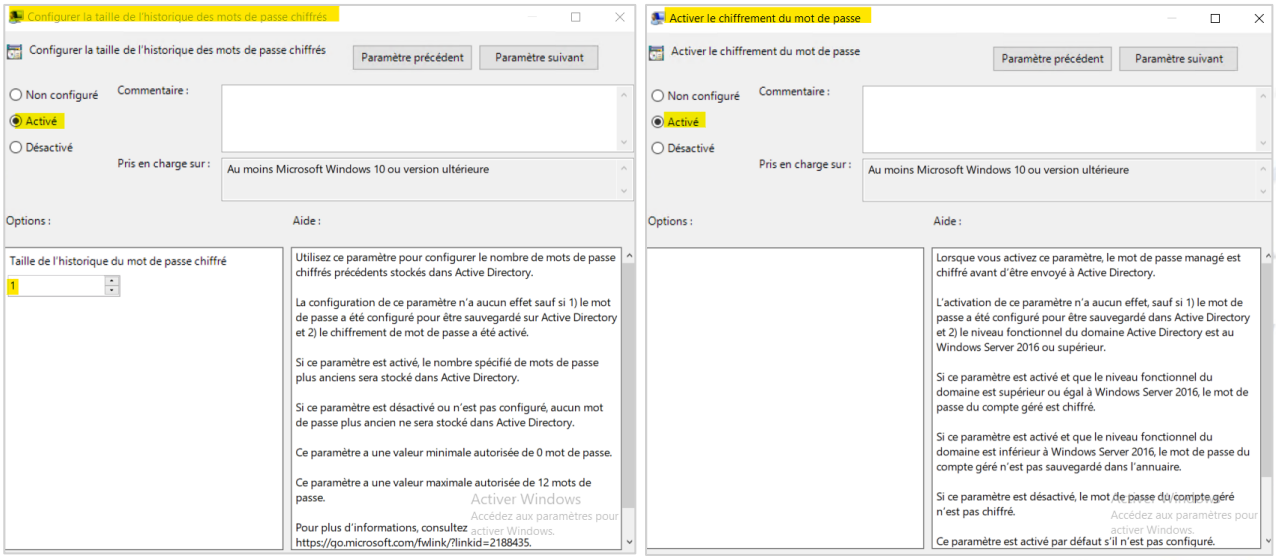
Pour un mot de passe fort, on recommande :

- **Complexité** : Majuscules + minuscules + chiffres + caractères spéciaux
- **Longueur** : 16 caractères
- **Âge** : 30 jours (valeur par défaut)



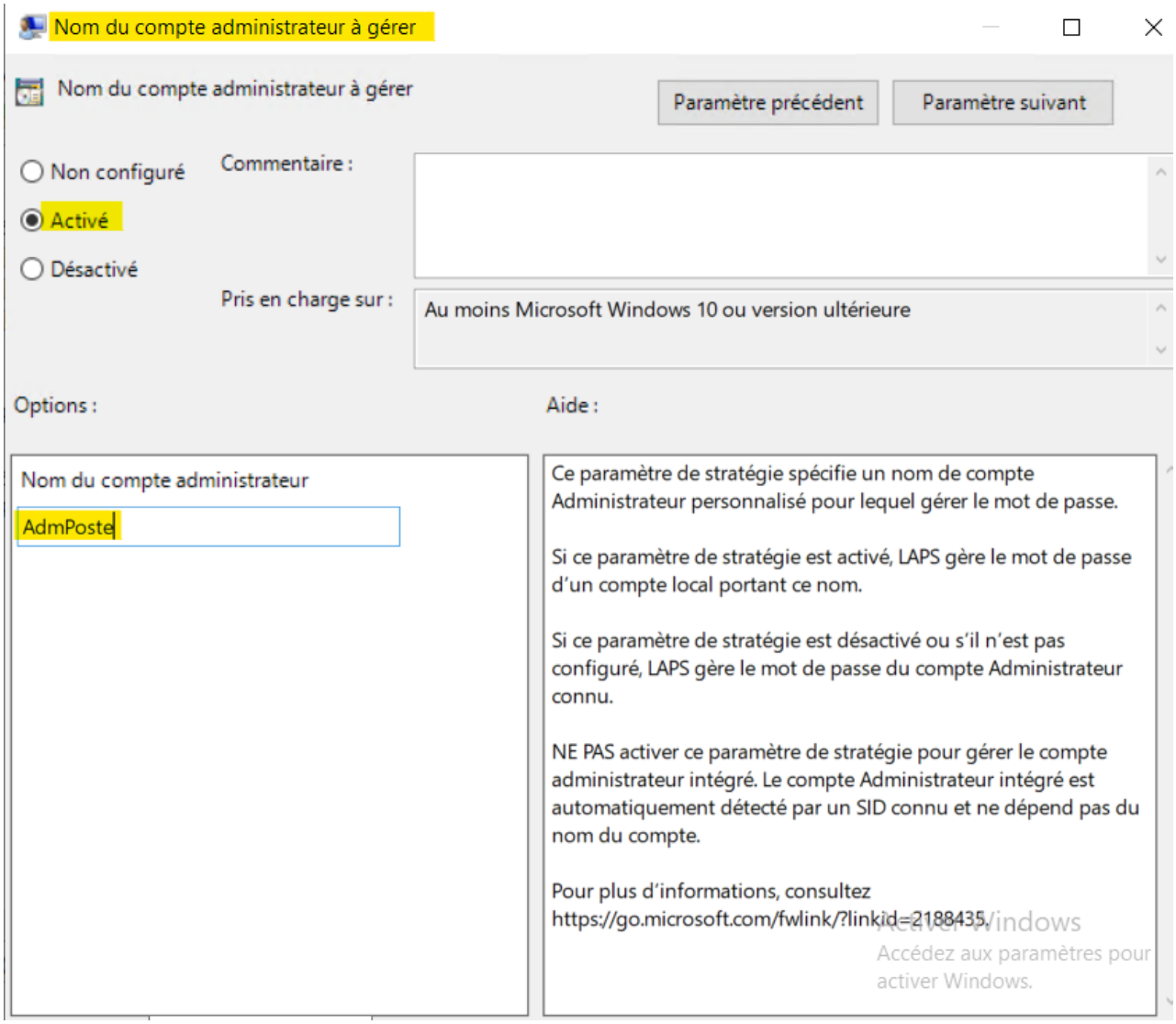
Configurer la taille de l'historique des mots de passe chiffrés : Ce paramètre est facultatif mais utile, car il permet d'activer l'historique des mots de passe. En l'activant et en définissant la taille de l'historique à 1, on peut toujours lire le mot de passe actuel et le précédent. En cas de problème où le mot de passe est mis à jour dans l'AD mais pas sur le poste, cela évite de perdre l'accès.

Le quatrième paramètre à activer est "**Activer le chiffrement du mot de passe**". Même si c'est le comportement par défaut, mieux vaut le forcer. Comme son nom l'indique, il garantit que le mot de passe stocké dans l'Active Directory soit chiffré.

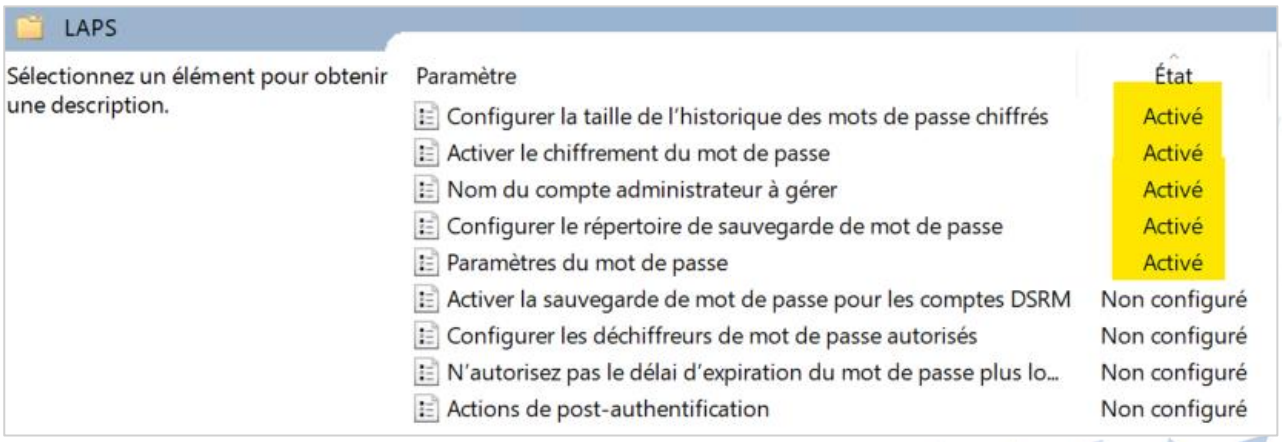


Par défaut, Windows LAPS gère automatiquement le compte "Administrateur" intégré à Windows, sans configuration supplémentaire, grâce à son SID connu.

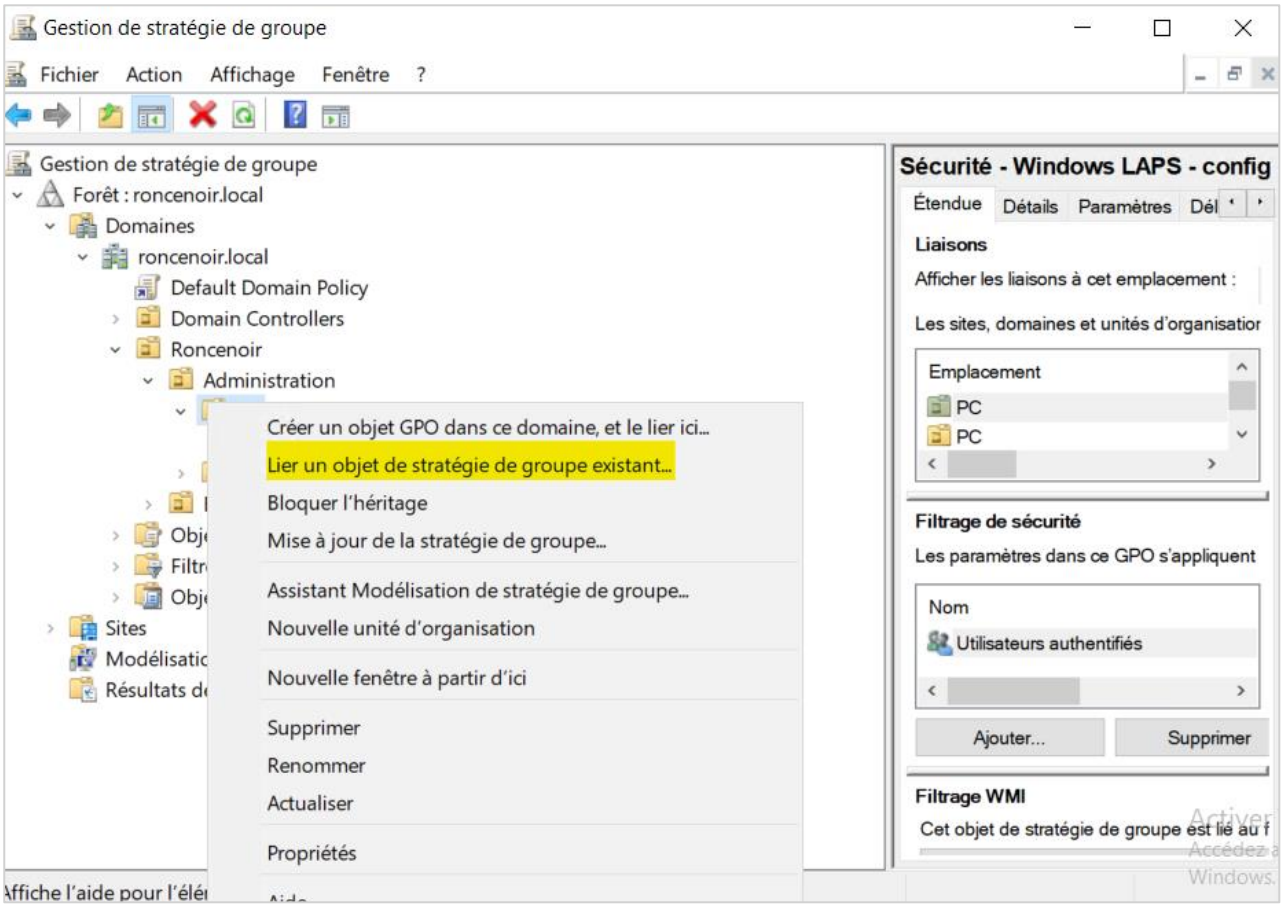
Si l'on veut gérer un autre compte avec un nom personnalisé, il faut activer le paramètre "**Nom du compte administrateur à gérer**" et préciser le nom du compte cible.

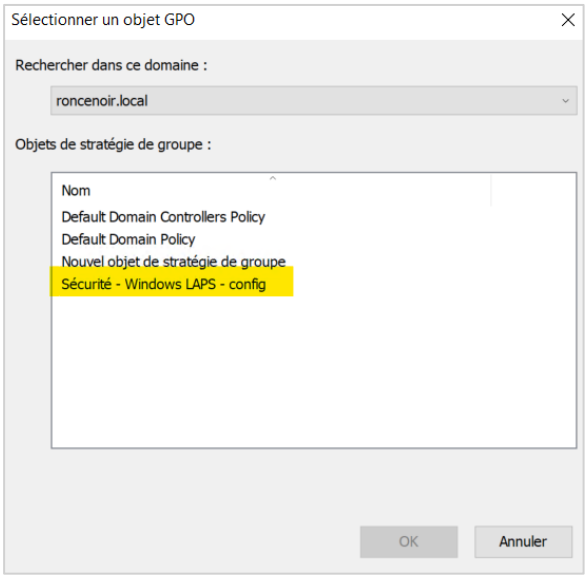


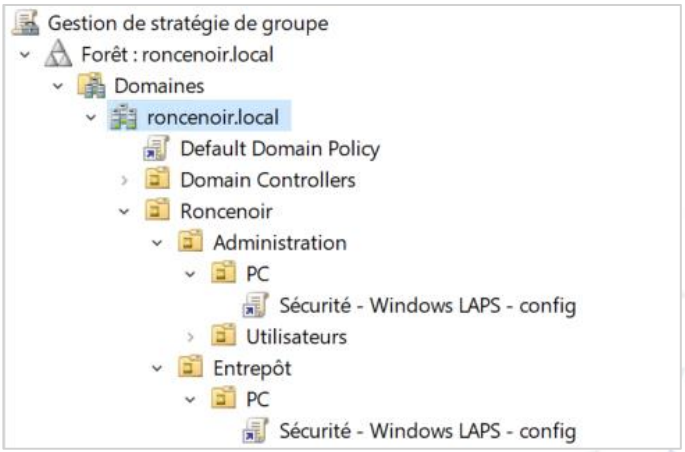
Au final, notre **stratégie de groupe** est configurée ainsi :



J’attribue ma GPO à mes deux OU PC dans les OU entrepôt et Administration comme ci-dessous :

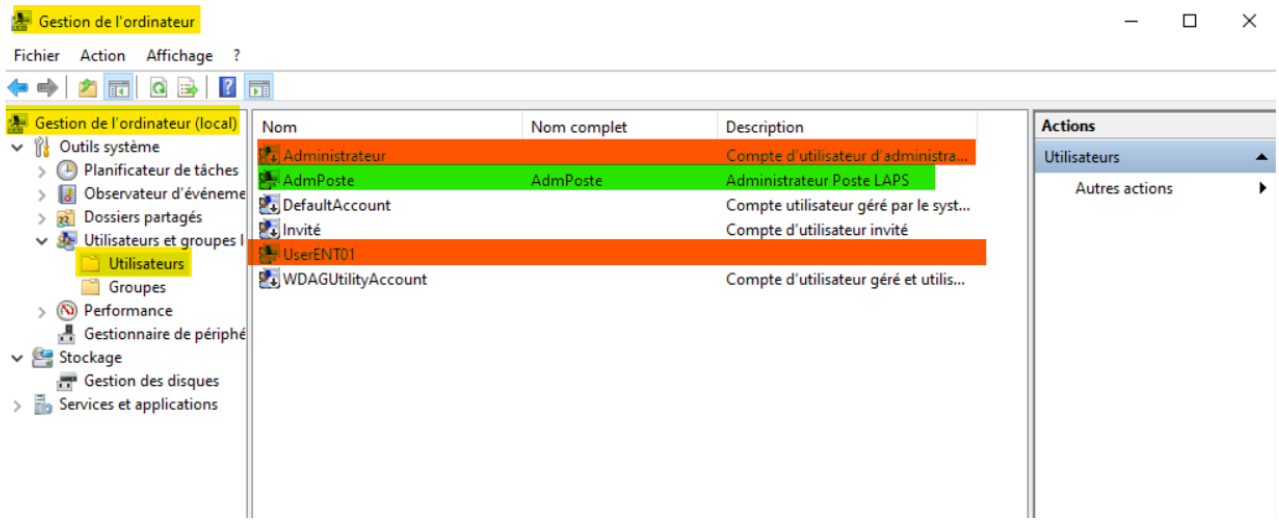




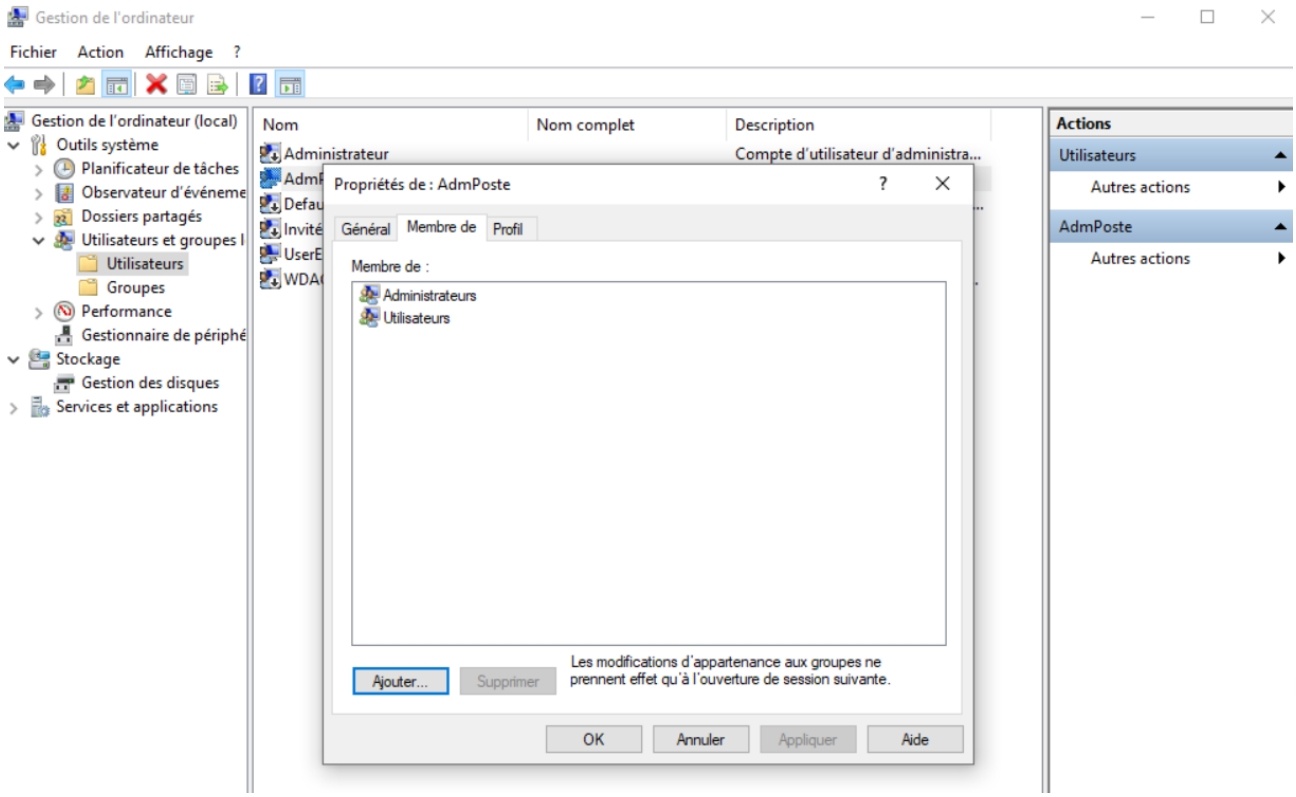


Tester laps sur mon poste client

Je me connecte à mon pc client entrepôt en local.



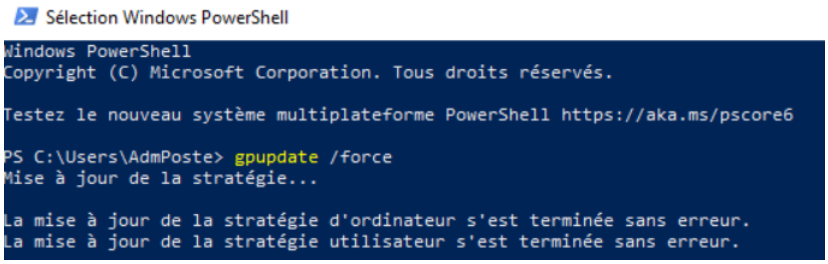
Dans Gestion de l'ordinateur, je crée un utilisateur AdmPoste qui me servira d'administrateur local lié à l'AD et je supprime les deux autres comptes qui me servaient d'administrateurs (ne pouvant supprimer le compte Administrateur, je me contente de le laisser désactivé comme il est censé l'être de base).



Je fais bien attention à ce que mon nouvel administrateur local fasse partie des administrateurs locaux de l'ordinateur.

Je me connecte à ce nouveau compte administrateur local.

Sur PowerShell, je mets à jour la stratégie de groupe : gpupdate /force



- J'ai dû mettre ma vm Windows10 à jour avant de lancer la prochaine commande. La commande dont j'ai besoin n'est disponible qu'à partir de la version 22h2.

Toujours sur ma VM client, sur le profil administrateur local, je lance PowerShell en administrateur et lance la commande : Invoke-LapsPolicyProcessing

Ensuite, je retourne sur ma VM ADSecure1 (ou 2 peu importe) et je peux voir que dans les propriétés de l'ordinateur, le LAPS s'est appliqué.