ANTRI Mohamed
Antrimohamed.fr

Stratégies de mot de passe affinées (FGPP)

Description

Avant l'apparition de Windows Server 2008 il n'était possible de créer qu'une seule stratégie de mot de passe par domaine Active Directory. Ainsi, certaines entreprises qui avaient besoin de plusieurs stratégies, allèrent jusqu'à créer des nouveaux domaines. C'est ainsi que Microsoft créa les stratégies de mots de passe affinées souvent appelés FGPP pour Fine Grained Password Policy. Ces stratégies vont nous permettre de créer plusieurs exigences de mot de passe pour l'ensemble de notre domaine.

Prérequis

1. Niveau fonctionnel du domaine en 2008
2. S'appliquent seulement aux groupes de **sécurités Globaux !**
3. Par défaut, être membre du groupe Admin du domaine pour crée la FGPP
4. Préparer les valeurs pour tous les attributs nécessaires.
5. Nom du groupe ou utilisateur sur lequel sera appliquée la stratégie.

Ordres d'applications (PSO Résultant)

Nous allons maintenant voir la manière dont s'appliquent les stratégies de mot de passe affinées.

Premièrement, il faut savoir que vous pouvez appliquer une stratégie de mot de passe seulement à un utilisateur ou à un groupe. Vous ne pouvez pas appliquer ce type de stratégie à une unité d'organisation directement. Vous devez créer un « **shadow group** ». Un **shadow group** est un groupe logique contenant l'ensemble des objets d'une O.U. L'inconvénient de ce type de groupe est qu'il faut maintenir manuellement le **shadow group** car lorsque vous ajoutez un utilisateur à une unité d'organisation, il ne s'ajoute pas automatiquement à un groupe. Vous pouvez bien évidemment développer des scripts afin de corriger cela.

Une stratégie appliquée directement à un utilisateur est prioritaire sur celle appliquée à un groupe. Pour exemple, si une stratégie s'applique à un utilisateur du nom de « Mohamed » et qu'une autre stratégie s'applique à un groupe contenant l'utilisateur Mohamed, alors la première stratégie sera prise en compte car elle s'applique directement à l'utilisateur en question.

ANTRI Mohamed

Si nous avons plusieurs FGPP qui sont appliquées à un utilisateur ou à un groupe la stratégie qui sera appliquée sera celle qui possède la plus petite valeur pour l'attribut « **msDS-PasswordSettingsPrecedence** ». Si deux stratégies possèdent la même valeur à cet attribut alors la stratégie qui sera appliquée sera celle qui possède le plus petit GUID.

Les FGPP s'appliquent aussi aux groupes imbriqués. C'est-à-dire que si notre groupe contient d'autres groupes, alors la stratégie de mot de passe s'appliquera à l'ensemble des utilisateurs. J'ai personnellement testé à une profondeur de groupe à N+3.

Si, à tout moment, vous souhaitez connaître la stratégie qui est appliquée à un utilisateur vous pouvez regarder la valeur de l'attribut « msDS-ResultantPso ». Cet attribut vous permettra ainsi de déterminer la stratégie résultante.

Impact stratégies de mot de passe

Avant de déployer vos stratégies de mot de passe en production, vous pouvez les tester en pré production. Lorsqu'une stratégie de mot de passe est appliquée elle prendra effet sur l'utilisateur seulement lorsque celui-ci devra réinitialiser son mot de passe. Par exemple, si votre « default domain policy » force tous les utilisateurs à réinitialiser leurs mots de passe tous les 42 jours, alors lorsque le 42ème jour arrivera et que l'utilisateur changera son mot de passe, à ce moment-là, la stratégie sera appliquée. Bien évidemment vous pouvez encore une fois réaliser un script Powershell pour forcer les utilisateurs à changer leurs mots de passe à la prochaine connexion. Mais dans ces cas-là, faîtes attention à vos comptes de services ! Privilégiez donc les comptes de services managés.

De toute manière, si à un moment vous rencontrez un souci avec les stratégies de mot de passe affinées, alors il vous faudra simplement retirer le groupe ou l'utilisateur de cette stratégie. Une fois retirée, la stratégie ne fera plus effet.

Paramètres

Une stratégie de mot de passe affinée est un objet de type PSO (Password Settings Objects). Voici les paramètres que vous aurez besoin de définir.

1. Stratégie Name [Unicode-String] (Nom de la stratégie de mot de passe)
2. Password Settings Precedence [int] (Valeur utilisée en cas de conflit de FGPP)
3. Password Reversible encryption [Boolean] (Mot de passe chiffré en mode réversible.)
4. Password History Length [int] (Nombre de conservation des anciens mots de passe.)
5. Password Complexity Status [Boolean] (Respecter les exigences de complexités.)
6. Minimum Password Length [int] (Taille minimum du mot de passe)
7. Minimum Password Age [Duration] (Durée de validité minimum du mot de passe)
8. Maximum Password Age [Duration] (Durée de validité maximum du mot de passe)
9. LockoutThreshold [int] (Seuil de verrouillage des comptes utilisateurs)
10. LockoutObservationWindows [Duration] (Durée compteur mauvais mot de passe)
11. LockoutDuration [Duration] (Durée de verrouillage du compte)

ANTRI Mohamed

Voici les valeurs que nous utiliserons pour notre exemple.

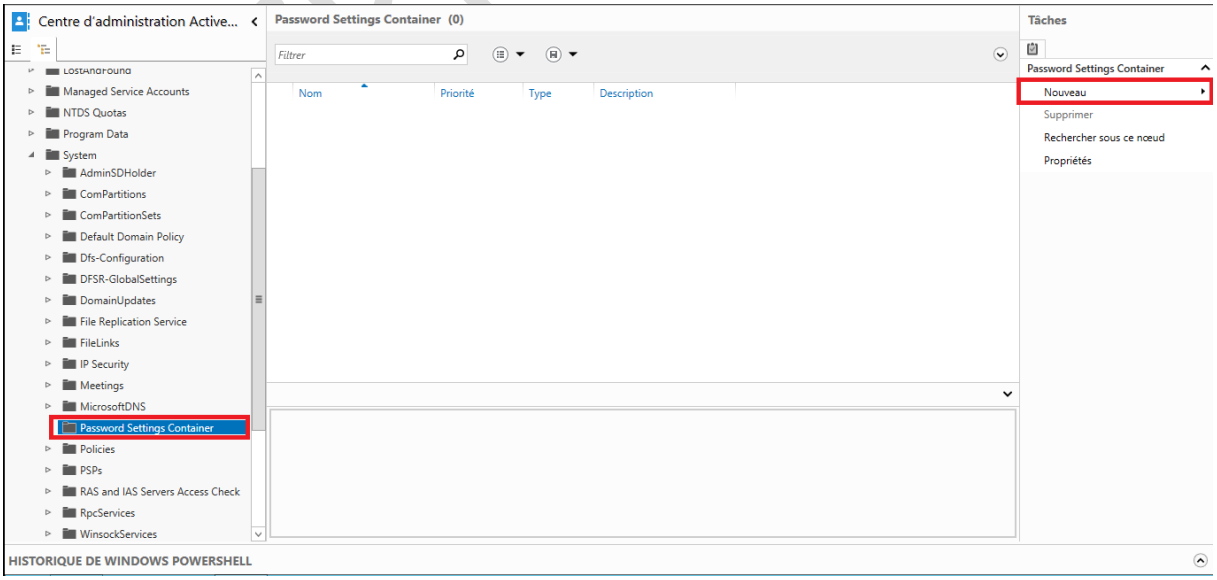
Proposition de valeurs possibles :

1. Stratégie Name : Première FGPP
2. Password Settings Precedence : 10
3. Password Reversible encryption : FALSE
4. Password History Length : 24
5. Password Complexity Status : TRUE
6. Minimum Password Length : 15
7. Minimum Password Age : 1 :00 :00 :00 soit 1 Jour
8. Maximum Password Age : 30 :00 :00 :00 soit 30 Jours
9. LockoutThreshold : 7
10. LockoutObservationWindows : 0 :00 :30 :00 soit 30 minutes
11. LockoutDuration : 1 :00 :00 :00 soit 1 jour

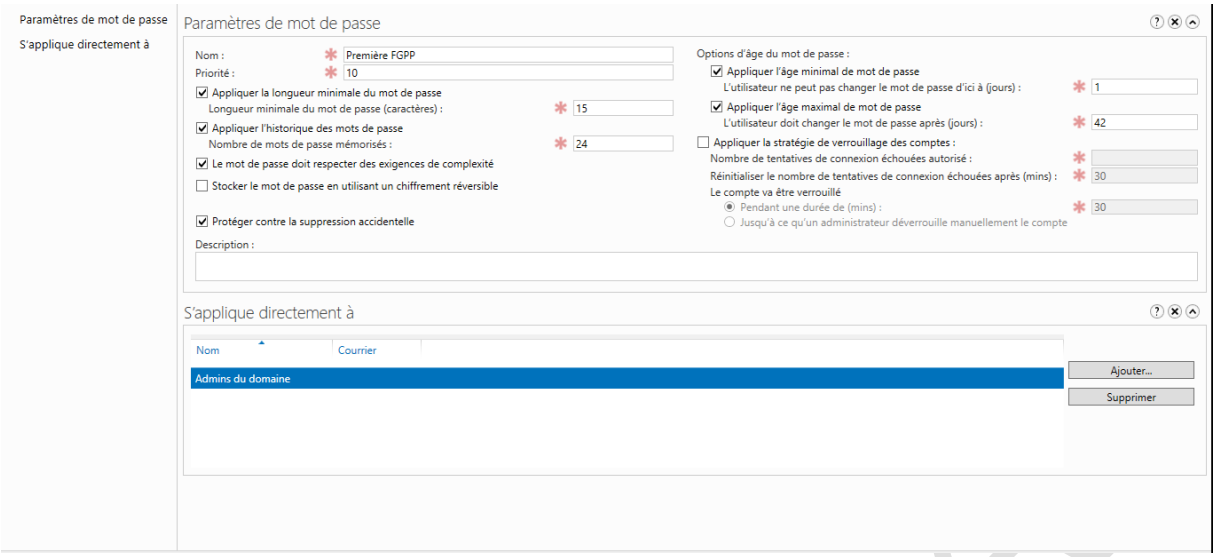
Une fois tous ces paramètres définis, nous devrons modifier la valeur de l'attribut « **msds-PSOAppliedTo** » afin d'appliquer la FGPP à notre groupe.

Réalisation

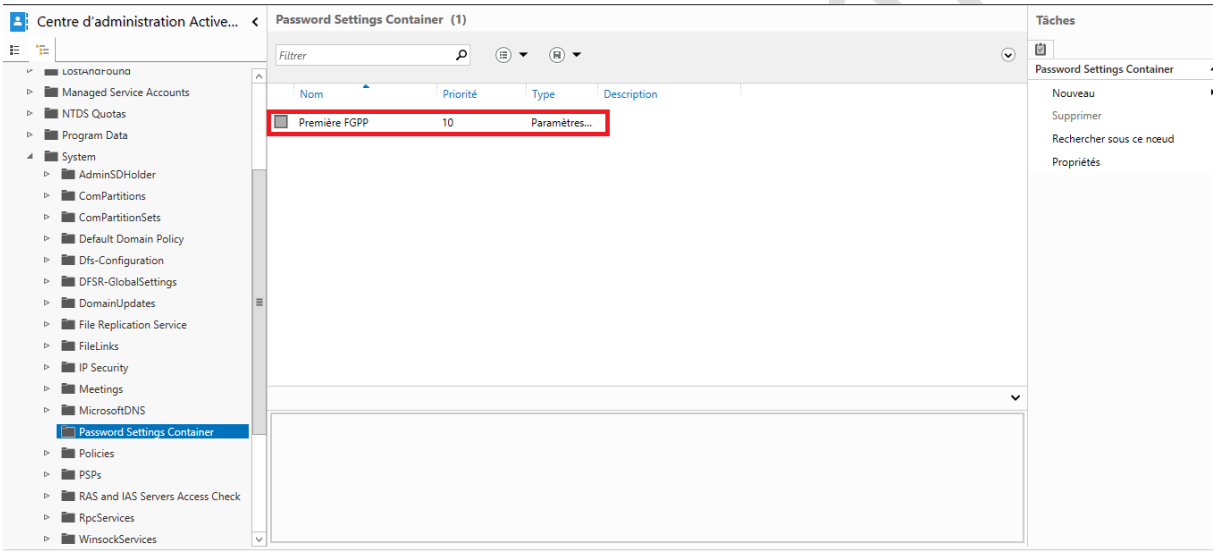
Nous allons commencer par créer une stratégie de mot de passe affinée. Depuis Windows Serveur 2012 nous pouvons créer des FGPP directement en interface graphique. Pour cela, nous allons lancer la console Active Directory Administrative Center. Ensuite, nous nous rendons sur le « **Password Settings Container** » et nous cliquons sur nouveau puis paramètres de mot de passe.



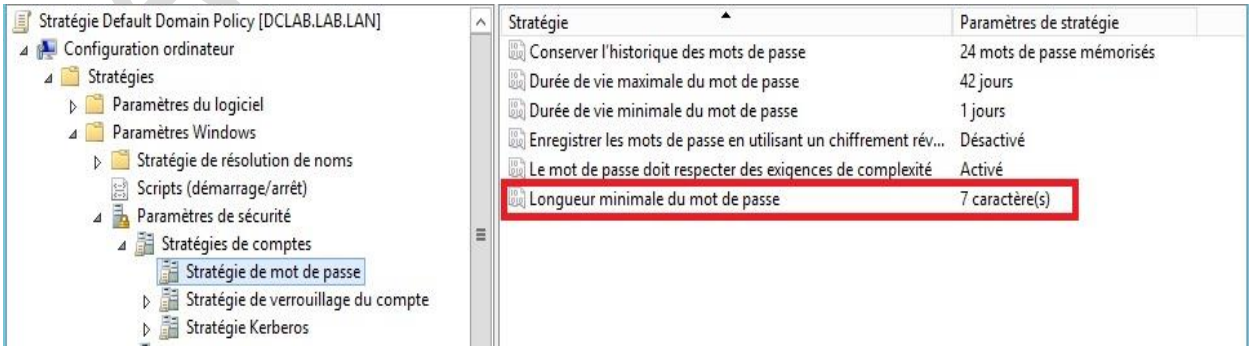
Ensuite nous inscrivons des valeurs pour les différents paramètres et le plus important c'est qu'il faut indiquer l'objet sur lequel s'appliquera notre stratégie puis, nous validons. Pour notre exemple, nous choisirons le groupe « Admins du domaine »



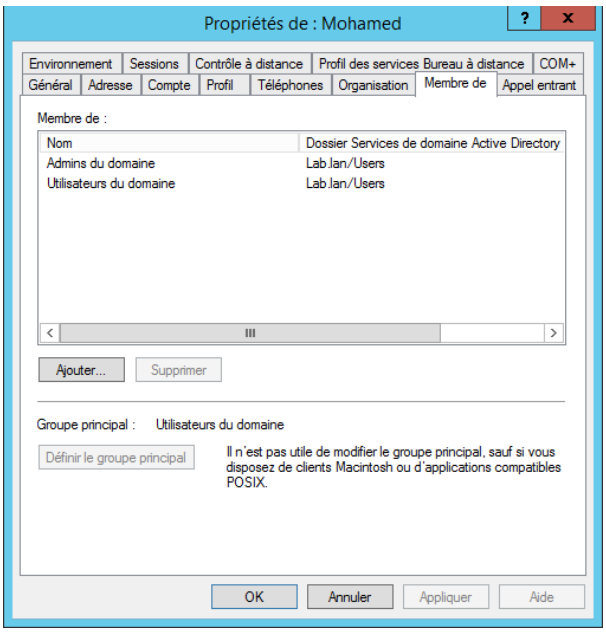
Une fois la stratégie appliquée vous devrez la voir apparaître comme ci-dessous :



Nous allons maintenant voir si notre stratégie de mot de passe est appliquée. Avant cela nous allons d'abord regarder la stratégie du domaine. Pour cela nous lançons la mmc « Group Policy Management Console » Ensuite, nous pouvons voir, par exemple, que la longueur du mot de passe est actuellement définie à 7.

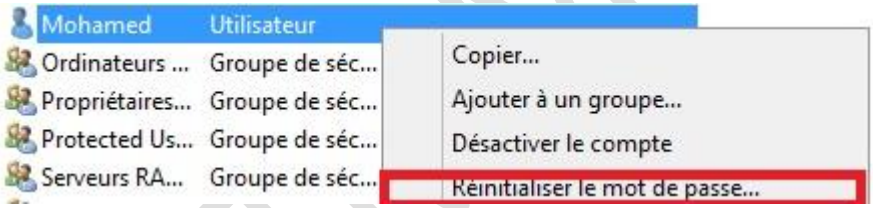


Nous allons alors essayer de changer le mot de passe pour un membre du groupe « Admins du domaine ».

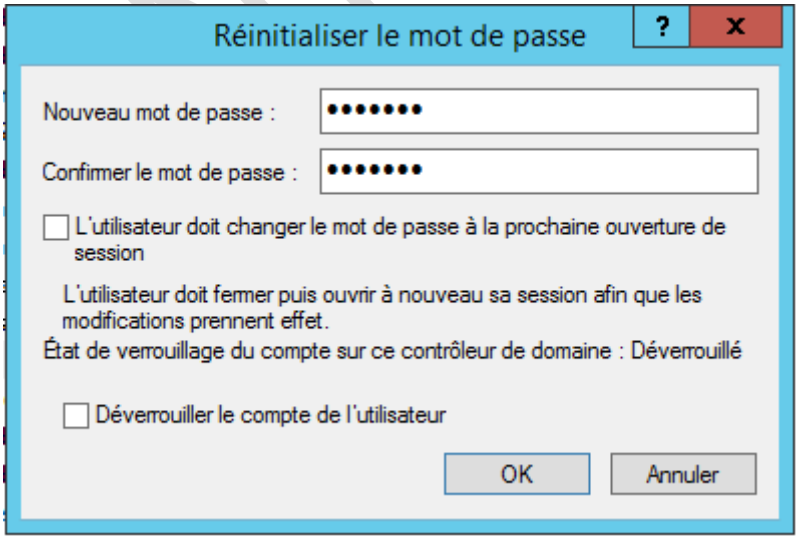


L'utilisateur Mohamed est donc membre du groupe Admins du domaine. Nous allons tentez de lui spécifier un mot de passe de moins de 15 caractères (15 étant la valeur définie dans la FGPP).

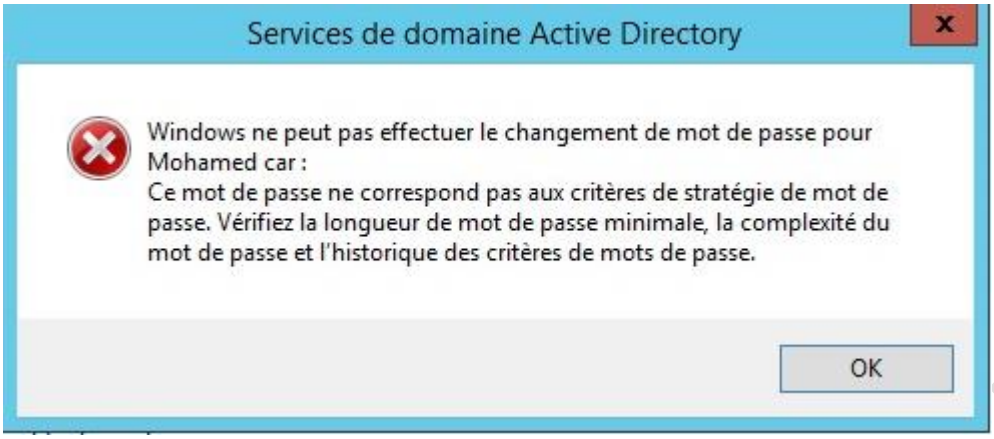
Pour cela, nous réalisons un clic droit sur l'objet utilisateur puis nous sélectionnons « réinitialiser le mot de passe »



Ensuite nous entrons un mot de passe de 7 caractères puis nous validons.

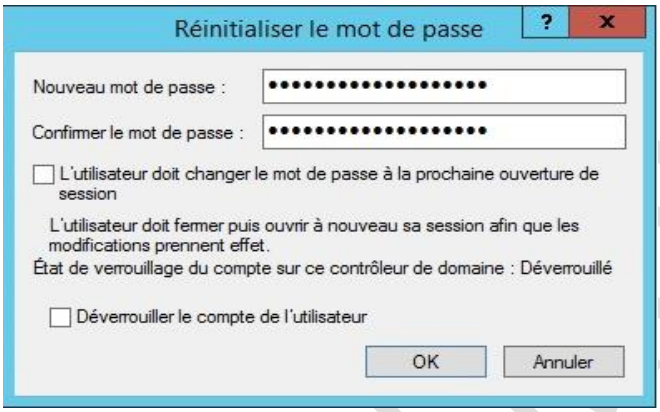


ANTRI Mohamed

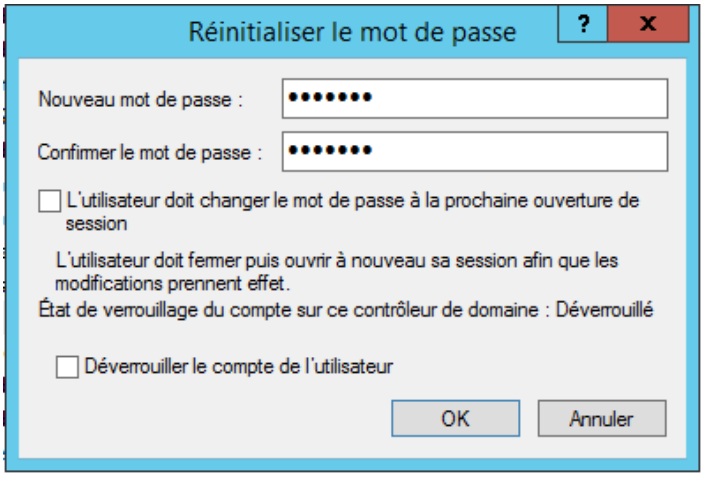


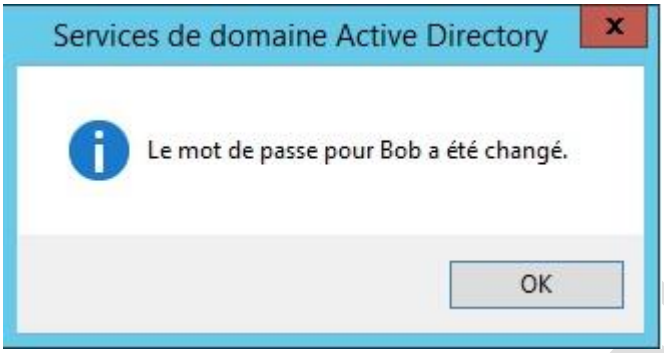
Nous pouvons voir que nous ne pouvons pas valider ce mot passe pour les raisons mentionnées ci-dessus.

Nous entrons maintenant un mot de passe d'au moins 15 caractères puis nous validons.



Par contre si nous tentons maintenant de mettre un mot de passe de 7 caractères pour un simple utilisateur :





Vous avez donc pu constater que la nouvelle stratégie de mot de passe s'applique actuellement seulement pour le groupe « Admins du domaine ». Vous pouvez ainsi créer plusieurs stratégies et les appliquer à différents groupes à privilèges.

Nous pouvons aussi créer la stratégie de mot de passe en Powershell grâce à la commande « **New-AdFinegrainedPasswordPolicy** » :

```
New-ADFineGrainedPasswordPolicy -Name SecondeFGPP -Precedence 10 -ComplexityEnabled
$true -Description "Seconde FGPP" `
-MaxPasswordAge 42 -MinPasswordAge 1 -MinPasswordLength 15 -PasswordHistoryCount 24
-ProtectedFromAccidentalDeletion $true `
-LockoutDuration "0:02:00:00" -LockoutObservationWindow "0:01:00:00"
```

```
PS C:\Users\Administrateur> New-ADFineGrainedPasswordPolicy -Name SecondeFGPP -Precedence 10 -ComplexityEnabled $true -Description "Seconde FGPP" `
-MaxPasswordAge 42 -MinPasswordAge 1 -MinPasswordLength 15 -PasswordHistoryCount 24 -ProtectedFromAccidentalDeletion $true `
-LockoutDuration "0:02:00:00" -LockoutObservationWindow "0:01:00:00"
```

N'oubliez pas que vous disposez toujours de la commande Get-help pour vous aider à créer vos commandes.

Une fois notre stratégie créée, nous allons l'ajouter à un groupe grâce à la commande « **Add-ADFinegrainedPasswordPolicy**

```
Add-ADFineGrainedPasswordPolicySubject SecondeFGPP "Admins du domaine"
```

```
PS C:\Users\Administrateur> Add-ADFineGrainedPasswordPolicySubject SecondeFGPP "Admins du domaine"
```

ANTRI Mohamed

Bravo ! Vous savez maintenant configurer une stratégie de mot de passe affinée en GUI et en Powershell.

Roll Back

A tout moment, vous pourrez revenir en arrière en cas d'erreur. Pour retirer une stratégie de mot de passe affinée, il suffit simplement de retirer l'objet figurant dans l'attribut « **msds-PSOAppliedTo** ». Dans notre exemple, il suffit simplement de retirer le groupe « Admins du domaine » de la stratégie de mot de passe. Ainsi, vous pourrez de nouveau spécifier des mots de passe de 7 caractères par défaut.

Ou en Powershell grâce à la commande « **Remove-FineGrainedPasswordPolicySubject** »

```
Remove-ADFineGrainedPasswordPolicySubject SecondeFGPP -Subjects "Admins du domaine"
```

```
PS C:\Users\Administrateur> Remove-ADFineGrainedPasswordPolicySubject SecondeFGPP -Subjects "Admins du domaine"
```

Merci à vous d'avoir suivi cette procédure.

ANTRI Mohamed