PROCEDURE STRATEGIE PSO ACTIVE DIRECTORY ET AUGMENTATION NIVEAU FONCTIONNEL FORET

Cette procédure à pour but de montrer étape par étape comment créer une stratégie de mot de passe dans active directory et comment élever le niveau d'une forêt et le niveau d'un domaine dans active directory

Active directory

PROCEDURE STRATEGIE PSO ACTIVE DIRECTORY ET AUGMENTATION NIVEAU FONCTIONNEL FORET

Table des matières

Niveau Fonctionnel

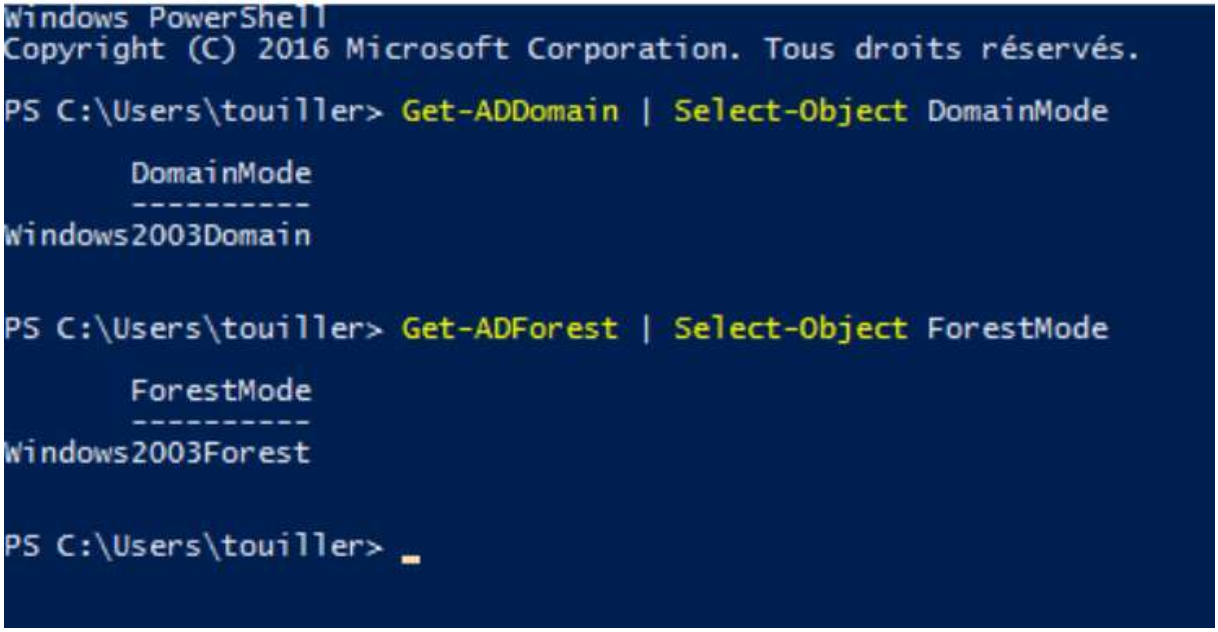
Vérifier le niveau fonctionnel de notre domaine active directory et de sa forêt. Pour rappel, nous ne pouvons créer une stratégie de mot passe dans l'active directory qu'après les versions 2003 de Windows.

Copier la commande suivante dans PowerShell pour vérifier notre niveau de forêt et de domaine.

```
Get-ADDomain | Select-Object DomainMode

Get-ADForest | Select-Object ForestModemodules
```

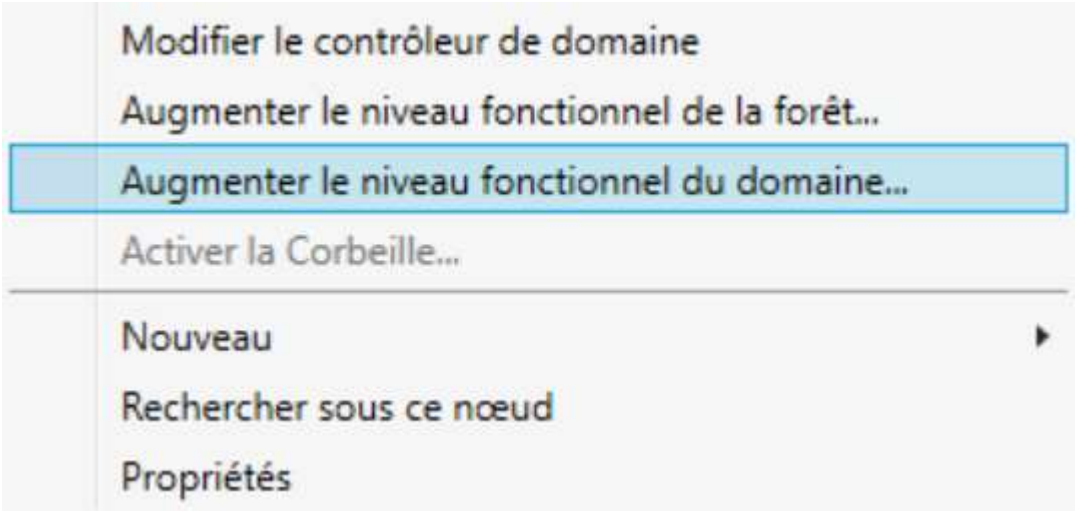
Vous devirez avoir un écran semblable (n'oublier pas d'ouvrir PowerShell en administrateur)

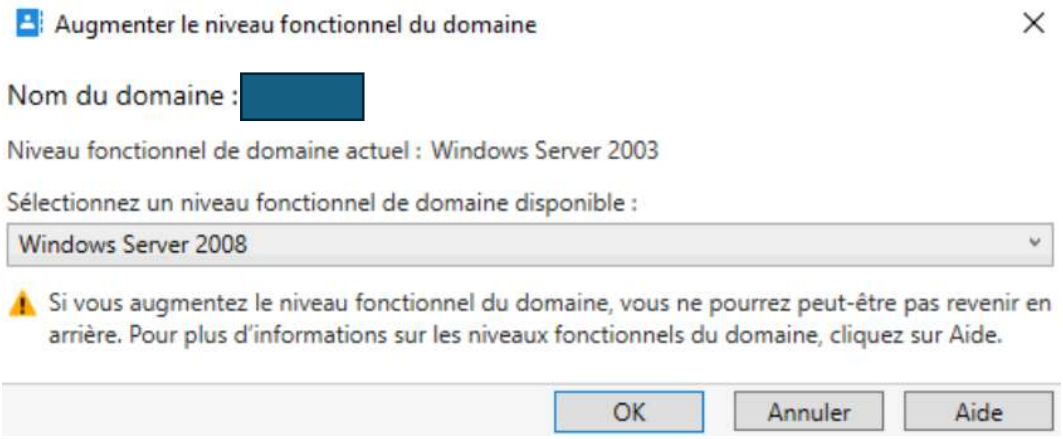


Relever le niveau fonctionnel de la forêt et du domaine

Se rendre dans le centre d'administration active directory

Clic droit sur le domaine





Augmenter le niveau de domaine par version ! Ne pas passer d'une version trop veille jusqu'à la version actuelle de l'OS si trop de version d'écart ! préférer un upgrade version par version !

Nous allons maintenant répéter l'opération pour le niveau fonctionnel de la forêt

Une fois le niveau fonctionnel de domaine augmenté jusqu'à la version souhaité, réalisé la même opération pour le niveau fonctionnel de forêt !

ATTENTION, tester au préalable le bon fonctionnement version par version de l'augmentation du niveau fonctionnel de domaine.

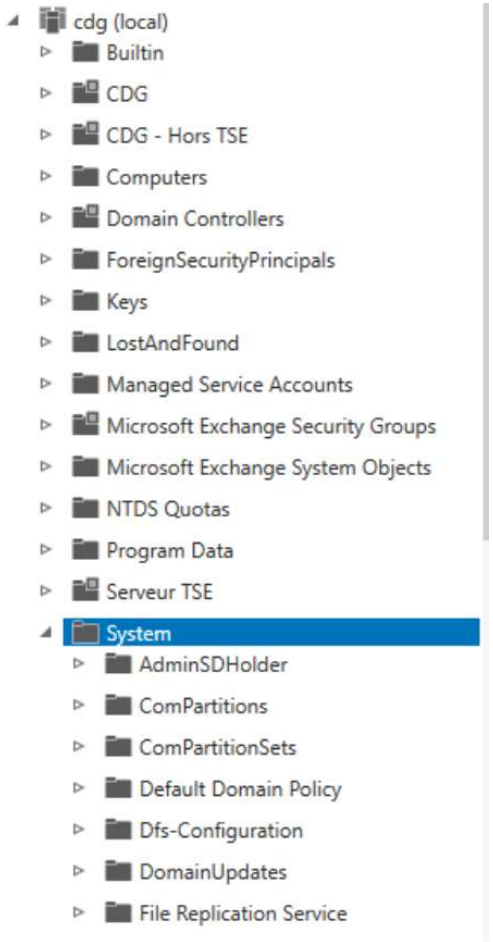
TOUTE AUGMENTER DU NIVEAU EST IRREVERSIBLE. Certains logiciels comme sage peuvent rencontrer des difficultés si les versions ne supportent pas un niveau fonctionnel de domaine élevé. (Ou certains logiciels utilisant une base de données)

Il est important à noter que à chaque augmentation de niveau, il faut réaliser une phase de test pour voir si l'augmentation est opérationnelle au niveau des utilisateurs et des groupes.

Création d'une PSO

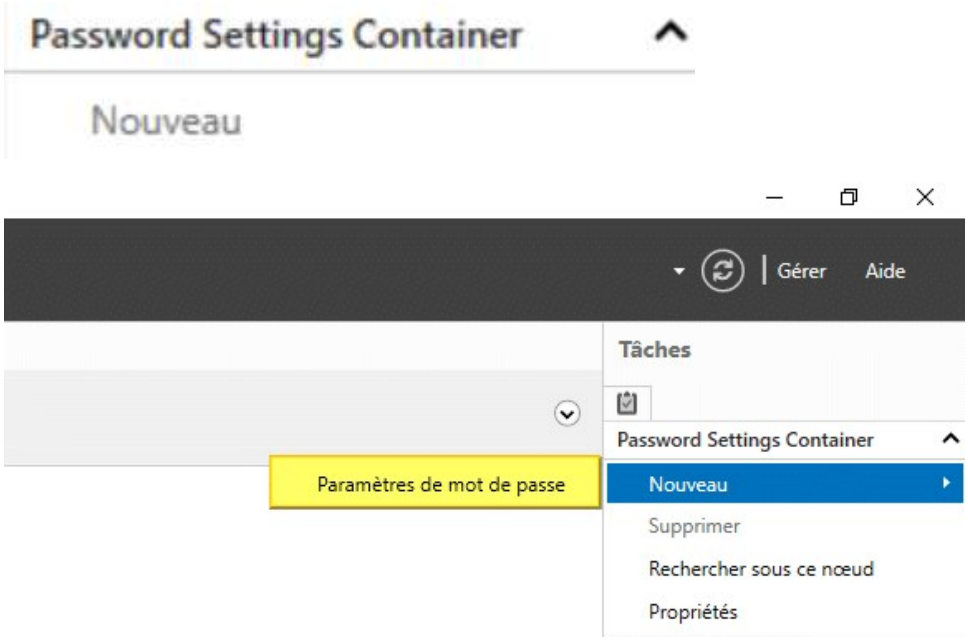
Une fois le niveau fonctionnel de domaine et de forêt augmenté, nous allons maintenant créer une PSO (stratégie de mot de passe unifié) pour les utilisateurs du domaine.

Ouvrer le centre d'administration active directory



Dérouler system en dessous du domaine concerné, puis cliquer sur

Aller sur Password settings container, puis cliquer sur nouveau



Nous allons maintenant détailler chaque étape de la création de la PSO :

Etape 1 :

- Nommer la nouvelle politique de mot de passe
- Metter une Priorité (

Valeur supérieure à 0 qui servira à faire l'arbitrage en cas de conflit entre deux PSO qui s'appliquent sur un même objet.)

- La valeur la plus faible sera prioritaire sur la valeur la plus haute.
- En cas de priorité identique, c'est la politique avec le GUID le plus faible qui sera appliqué
- Un PSO appliqué au niveau d'un utilisateur sera prioritaire appliqué au niveau du groupe.
- Appliquer la longueur minimale du mot de passe
- Appliquer l'historique des mots de passe
- Le mot de passe doit respecter des exigences de sécurité (indiquer si oui ou non le mot de passe doit respecter ces exigences
- Stocker le mot de passe en utilisant un chiffrement réversible (

il est préférable de ne pas activer cette option, là aussi par sécurité. Si vous activez cette option, cela signifie que le mot de passe stocké dans l'AD peut être récupéré en clair, ce qui n'est pas souhaitable

- Protéger contre la suppression accidentelle
- Appliquer l'âge minimal du mot de passe (permet d'empêcher à un utilisateur de changer successivement son mot de passe)
- Appliquer l'âge maximal du mot de passe (durée de vie du mot de passe avant prochain changement)
- Nombre de tentatives échouées autorisées (évite les attaques par brut force)
- Pendant une durée minimum

Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

Nous allons maintenant appliqué cette nouvelle stratégie de mot de passe à l'OU qui nous intéresse

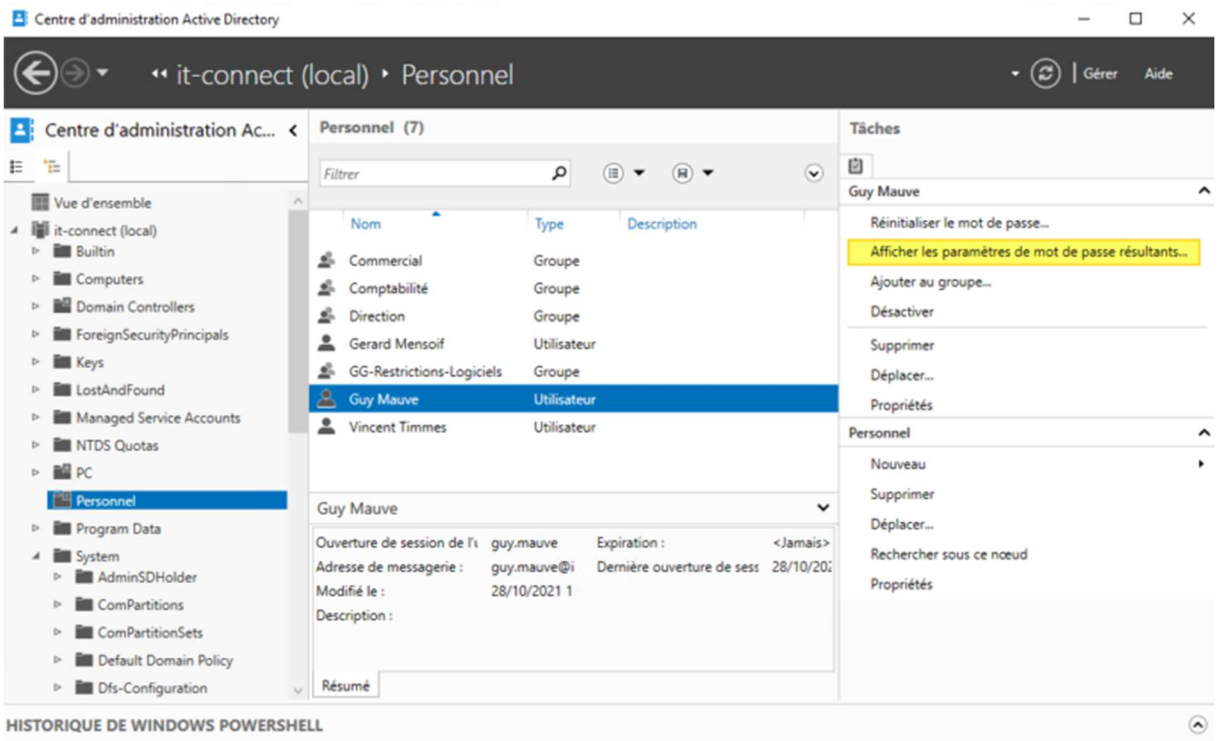
Se placer sur l'OU concerné dans le centre d'administration active directory.

- Sélectionné tous les utilisateurs
- Appliquer la stratégie de mot de passe préalablement créé
- Tester en amont sur une OU créer pour vérifier le bon fonctionnement de la stratégie.

Appliquer la PSO

Nous allons maintenant appliquer la PSO

Aller sur le centre d’administration Active Directory



Sélectionner tous les utilisateurs voulus et appliquer la PSO préalablement Créer.

Les utilisateurs seront donc invités à leur prochaine connexion de changer leur mot de passe suivant cette nouvelle politique de mot de passe !

Changement de mot de passe pour tous les utilisateurs

```
Get-ADUser -Filter * -SearchBase "CN=Fabrina
LEFEUVRE,OU=GPO,OU=Utilisateurs,OU=CDG,DC=cdg,DC=local" | ForEach-Object {
Set-ADUser -Identity $_.DistinguishedName -ChangePasswordAtLogon $true }
```

```
Get-ADUser -Filter * -SearchBase "OU=Utilisateurs,DC=CDG,DC=local" | ForEach-
  Object { Set-ADUser -Identity $_.DistinguishedName -ChangePasswordAtLogon
                                    $true }
```

Commande pour ajouter tous les utilisateurs à un groupe

```
Get-ADUser -Filter * -SearchBase "CN=Fabrina
LEFEUVRE,OU=GPO,OU=Utilisateurs,OU=CDG,DC=cdg,DC=local" | ForEach-Object {
Add-ADGroupMember -Identity
"CN=PSO_password,OU=GPO,OU=Utilisateurs,OU=CDG,DC=cdg,DC=local" -Members
```

```
Get-ADUser -Filter * -SearchBase "OU=Utilisateurs,OU=CDG,DC=cdg,DC=local" |
                ForEach-Object { Add-ADGroupMember -Identity
  "CN=PSO_password,OU=GPO,OU=Utilisateurs,OU=CDG,DC=cdg,DC=local" -Members
```