Mode Opératoire

Politiques de mots de passe différenciées (FGPP)

Code :	MO-AD-003
Version :	1.0
Date :	31 mars 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	31/03/2026	Création initiale après déploiement des 3 FGPP

1 Objet

Ce mode opératoire décrit la création et la gestion de politiques de mots de passe différenciées (*Fine-Grained Password Policies*, FGPP) dans le domaine Active Directory `bts.sio`. Les FGPP permettent d'appliquer des exigences de mots de passe proportionnelles au niveau de privilège de chaque profil utilisateur, conformément aux recommandations de l'ANSSI (modèle d'administration en tiers, 2023).

2 Champ d'application

— **Système cible :** domaine Active Directory `bts.sio`
— **Serveur :** DC1 — Srv2022 (`10.0.112.2`)
— **Profils concernés :** administrateurs (4), enseignants (9), étudiants (57)
— **Durée estimée :** 15 minutes
— **Intervenants :** administrateur du domaine

3 Concepts

3.1 Politique par défaut vs FGPP

La *Default Domain Password Policy* s'applique à tous les utilisateurs du domaine. Elle constitue le socle minimal. Les FGPP (*Password Settings Objects*, PSO) permettent de surcharger cette politique pour des groupes ou utilisateurs spécifiques.

Précédence

Chaque FGPP possède une valeur de **précédence** (entier positif). Plus la valeur est basse, plus la politique est prioritaire. Si un utilisateur est couvert par plusieurs FGPP, celle avec la précédence la plus basse l'emporte.

3.2 Architecture déployée

Trois niveaux de politique sont configurés, conformément au modèle ANSSI :

FGPP	Groupes	Min. chars	Lockout	Expiration
FGPP-Admins	Admins du domaine (4)	**16**	5 / 60 min	90 j
FGPP-Staff	GGPROFS (9)	**12**	10 / 30 min	180 j
FGPP-Etudiants	GGPromoSio1+2 (57)	**10**	10 / 15 min	365 j
Default	*Tous (baseline)*	*10*	*10 / 30 min*	*180 j*

4 Prérequis

Prérequis

— Niveau fonctionnel du domaine ≥ Windows Server 2008
— Module PowerShell `ActiveDirectory` disponible
— Droits *Domain Admins* ou délégation sur le conteneur PSC
— Accès WinRM au contrôleur de domaine (`bts winrm dc1` ou `pywinrm`)

5 Procédure

5.1 Vérifier le niveau fonctionnel

Étape 1 — Vérifier que le domaine supporte les FGPP

Les FGPP nécessitent un niveau fonctionnel ≥ Windows Server 2008. Exécuter sur DC1 :

```
(Get-ADDomain).DomainMode
```

Le résultat doit afficher `Windows2016Domain` ou supérieur.

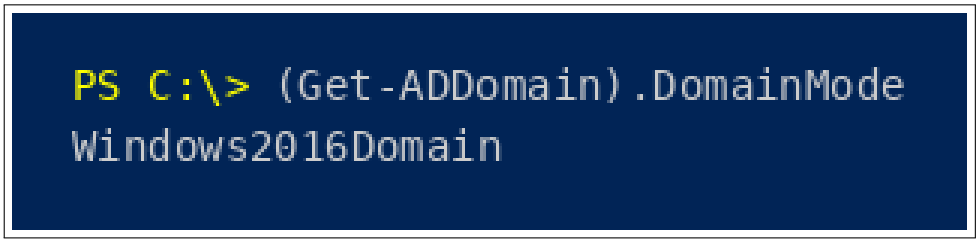

Figure 1 – Vérification du niveau fonctionnel du domaine

5.2 Créer une FGPP

Étape 2 — Créer la politique avec `New-ADFineGrainedPasswordPolicy`

Exemple pour la politique administrateurs (FGPP-Admins) :

```
New-ADFineGrainedPasswordPolicy -Name "FGPP-Admins" `
    -Precedence 10 `
    -MinPasswordLength 16 `
    -PasswordHistoryCount 24 `
    -ComplexityEnabled $true `
    -MaxPasswordAge "90.00:00:00" `
    -MinPasswordAge "1.00:00:00" `
    -LockoutThreshold 5 `
    -LockoutDuration "01:00:00" `
    -LockoutObservationWindow "01:00:00" `
    -ReversibleEncryptionEnabled $false
```

⚠ Paramètres critiques

- **Precedence** : valeur unique par FGPP. Plus basse = plus prioritaire.
- **MaxPasswordAge** : format `jours.heures:minutes:secondes`.
- **ReversibleEncryptionEnabled** : toujours `$false` (stockage en clair sinon).

Étape 3 — Assigner la FGPP à un groupe

La FGPP ne s'applique qu'après assignation explicite à un groupe ou utilisateur :

```
Add-ADFineGrainedPasswordPolicySubject `
    -Identity "FGPP-Admins" `
    -Subjects "Admins du domaine"
```

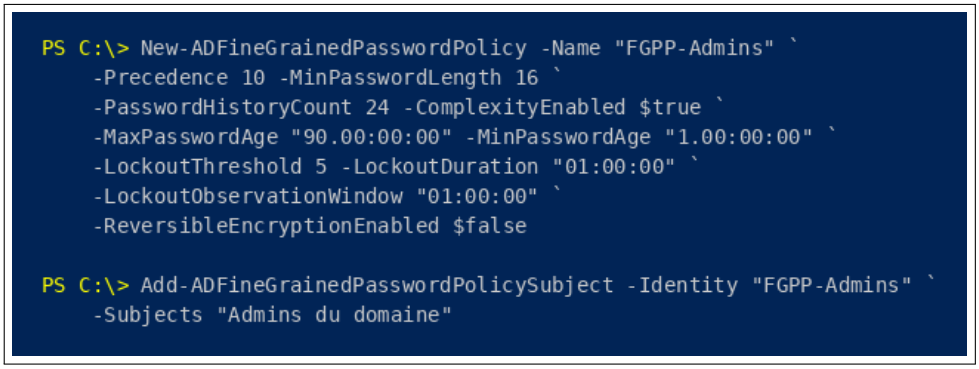

Figure 2 – Création et assignation d'une FGPP

Groupes uniquement

Les FGPP s'appliquent aux **groupes globaux de sécurité** ou aux **utilisateurs individuels**, jamais aux OU.

5.3 Vérifier les FGPP déployées

Étape 4 — Lister toutes les FGPP du domaine

```
Get-ADFineGrainedPasswordPolicy -Filter * |
    Format-List Name, Precedence, MinPasswordLength,
    LockoutThreshold, MaxPasswordAge, AppliesTo
```

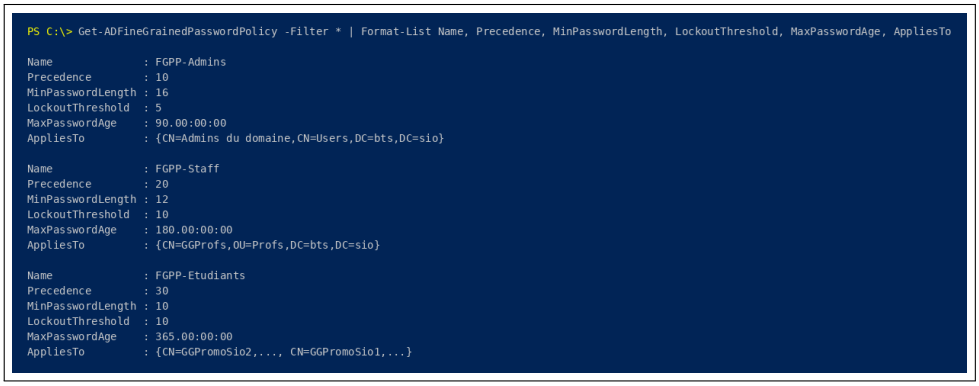

Figure 3 – Liste des 3 FGPP déployées sur le domaine bts.sio

Étape 5 — Vérifier la politique résultante d'un utilisateur

Pour confirmer qu'un utilisateur reçoit bien la bonne FGPP :

```
Get-ADUserResultantPasswordPolicy -Identity "clegrand"
```

Si la commande ne retourne rien, l'utilisateur est soumis à la politique par défaut du domaine (Default Domain Policy).

Figure 4 – Politique résultante pour 3 profils utilisateurs

5.4 Modifier ou supprimer une FGPP

Étape 6 — Modifier les paramètres d'une FGPP existante

```
# Exemple : passer le seuil de lockout de 5 a 3
Set-ADFineGrainedPasswordPolicy -Identity "FGPP-Admins" `
    -LockoutThreshold 3
```

La modification prend effet immédiatement pour les prochains changements de mot de passe.

Étape 7 — Retirer un groupe d'une FGPP

```
Remove-ADFineGrainedPasswordPolicySubject `
    -Identity "FGPP-Admins" `
    -Subjects "Admins du domaine" -Confirm:$false
```

Le groupe revient alors à la politique par défaut du domaine.

Étape 8 — Supprimer complètement une FGPP

```
Remove-ADFineGrainedPasswordPolicy `
    -Identity "FGPP-Admins" -Confirm:$false
```

⚠ Impact

La suppression d'une FGPP fait immédiatement basculer tous les utilisateurs et groupes concernés vers la politique de niveau supérieur (autre FGPP ou Default Domain Policy).

6 Vérification

Vérification

- ☐ 3 FGPP visibles dans `Get-ADFineGrainedPasswordPolicy -Filter *`
- ☐ FGPP-Admins appliquée à `Admins du domaine` (précédence 10)
- ☐ FGPP-Staff appliquée à `GGPROFS` (précédence 20)
- ☐ FGPP-Etudiants appliquée à `GGPromoSio1` et `GGPromoSio2` (précédence 30)
- ☐ `Get-ADUserResultantPasswordPolicy clegrand` retourne FGPP-Admins
- ☐ `Get-ADUserResultantPasswordPolicy a.verrier` retourne FGPP-Etudiants
- ☐ Un enseignant (ex. `fghoua`) reçoit FGPP-Admins s'il est DA, sinon FGPP-Staff

7 Dépannage

Problème	Solution
`New-ADFineGrainedPasswordPolicy` échoue	Vérifier le niveau fonctionnel du domaine ($\geq$ 2008). Vérifier les droits (Domain Admins requis).
FGPP créée mais non appliquée	Vérifier l'assignation avec `Get-ADFineGrainedPasswordPolicySubject`. Les FGPP ne s'appliquent pas aux OU, uniquement aux groupes globaux.
Utilisateur reçoit la mauvaise FGPP	Vérifier les appartenances de groupe (`Get-ADUser -Properties MemberOf`). La FGPP avec la précédence la plus basse l'emporte.
Lockout inattendu d'un compte admin	FGPP-Admins a un seuil de 5 tentatives (1h lockout). Déverrouiller : `Unlock-ADAccount -Identity <sam>`

Références

— ANSSI — *Administration sécurisée des systèmes d'information — Modèle en tiers* (2023)
— ANSSI — *Guide d'hygiène informatique*, mesure 10 (2017)
— CIS — *Microsoft Windows Server 2019 Benchmark*, section 1.1 (2024)
— Microsoft — `New-ADFineGrainedPasswordPolicy` (documentation PowerShell)
— Audit BTS SIO — Constats F-AD-003, F-AD-004 / Recommandations R-011, R-012