**Mode Opératoire**

# Déploiement de Windows LAPS (rotation des mots de passe Administrateur locaux)

| | |
|---|---|
| **Code :** | MO-AD-004 |
| **Version :** | 1.0 |
| **Date :** | 16 avril 2026 |
| **Auteur :** | Cédric LEGRAND |
| **Classification :** | USAGE INTERNE — Équipe BTS SIO |

## Historique des révisions

| Version | Date | Modifications |
|---|---|---|
| 1.0 | 16/04/2026 | Création initiale — procédure exécutée au titre du Sprint 2 (T25). Extension du schéma AD finalisée le 16/04 à 14 :30, GPO déployée le 16/04 à 14 :34. |

# 1 Objet

Ce mode opératoire décrit le **déploiement de Windows LAPS** (*Local Administrator Password Solution*, version native intégrée à Windows Server 2019+ et Windows 10/11 via KB5025230 d'avril 2023) sur les 72 postes étudiants des trois salles informatiques (POSTES_S109, POSTES_S110, POSTES_S111) du BTS SIO. La procédure procède en quatre temps :

1. extension contrôlée du schéma Active Directory pour ajouter les attributs `ms-LAPS-*` et le *extended right* `ms-LAPS-Encrypted-Password-Attributes` ;
2. attribution des permissions ACL nécessaires sur les trois OUs cibles (`SELF/WriteProperty` pour les comptes ordinateurs, `ReadPassword` pour les administrateurs) ;
3. création et liaison de la GPO « LAPS – Rotation MDP admin local » (rotation tous les 30 jours, mots de passe de 20 caractères complexes stockés dans Active Directory) ;
4. vérifications post-déploiement par sondage `Get-LapsADPassword`.

**Constat traité :** F-AD-013 *(mots de passe Administrateur locaux identiques sur 78 postes)* et règle PingCastle A-LAPS #27 *(absence de gestion automatisée des MDP admin locaux)*.

**⚠ Contexte initial**

Avant cette procédure, les 72 postes des trois salles partageaient le **même mot de passe Administrateur local** (compte RID 500), invariant depuis le déploiement initial. Une compromission unitaire d'un poste — via attaque physique en TP, vol de `SAM` d'un disque, ou simple lecture mémoire — exposait immédiatement les 71 autres au même secret. Le schéma AD comportait déjà les attributs `ms-LAPS-*` (extension partielle héritée d'une mise à jour Windows antérieure) mais sans *extended right* `ms-LAPS-Encrypted-Password-Attributes`, sans permissions ACL sur les OUs et sans GPO active : aucune rotation n'avait jamais eu lieu.

# 2 Champ d'application

| | |
|---|---|
| **Public concerné** | Administrateurs du domaine BTS SIO (rôle *Domain Admins*). L'étape d'extension de schéma exige une appartenance *temporaire* aux groupes *Schema Admins* et *Enterprise Admins*. |
| **Systèmes ciblés** | Domaine `bts.sio` (DC1 `Srv2022` 10.0.112.2, DC2 `Srv2022Phy` 10.0.112.3). 72 postes étudiants Windows 10/11 répartis sur trois OUs : `POSTES_S109` (23 postes), `POSTES_S110` (32), `POSTES_S111` (17). |
| **Outils** | PowerShell 5.1 avec modules `ActiveDirectory`, `LAPS` et `GroupPolicy`, `repadmin`, WinRM via `pywinrm`. |
| **Authentification** | Compte Domain Admin (`BTS\Administrateur` ou équivalent), avec passage temporaire dans *Schema Admins* et *Enterprise Admins* pour la phase d'extension de schéma. |
| **Durée** | $\approx$ 25 minutes pour le déploiement actif, + 2 heures de propagation passive pour les premières rotations sur les postes en marche. |
| **Présentiel requis** | Non. La procédure s'exécute intégralement via WinRM depuis le poste d'administration sous couvert du VPN WireGuard. |

# 3 Prérequis

**Prérequis**

— **MO-AD-005 exécuté** : santé AD validée (`repadmin /replsummary` sans erreur bloquante, services `NTDS`, `kdc`, `Netlogon` UP).
— **MO-AD-006 exécuté** : backup *System State* de DC1 récent (< 7 jours), vérifié par `wbadmin get versions`. L'extension de schéma est **irréversible** en opération normale ; seule une restauration autoritative permettrait un retour en arrière partiel.
— Accès WinRM (port 5985) au schéma master du domaine (DC1 dans cette infrastructure).
— Niveau fonctionnel de forêt **Windows Server 2008** ou supérieur pour `Update-LapsADSchema`. La forêt `bts.sio` est en mode `Windows2016Forest` (FFL 7), conforme.
— Modules PowerShell `LAPS` (cmdlet `Update-LapsADSchema` disponible) et `GroupPolicy` présents sur DC1.

**Irréversibilité de l'extension de schéma**

L'ajout d'attributs au schéma AD est **persistant et répliqué à l'ensemble de la forêt**. Microsoft ne fournit pas de cmdlet de retrait propre. La seule manière de « revenir en arrière » est une restauration autoritative depuis backup antérieur à l'extension — opération lourde qui invalide toutes les modifications postérieures. **Vérifier le backup System State avant de lancer la phase d'extension.**

# 4 Théorie : Windows LAPS et chaîne ACL

| | **Legacy LAPS (*AdmPwd*)** | **Windows LAPS (natif)** |
|---|---|---|
| Disponibilité | MSI Microsoft à télécharger, CSE à installer | Intégré OS Server 2019+ et Win10/11 (KB5025230) |
| Attribut MDP clair | `ms-Mcs-AdmPwd` | `ms-LAPS-Password` |
| Attribut MDP chiffré | — (clair uniquement) | `ms-LAPS-EncryptedPassword` (DPAPI-NG) |
| Historique | — | `ms-LAPS-EncryptedPasswordHistory` |
| Stockage backup | AD uniquement | AD ou Azure AD |
| Cmdlets PowerShell | module externe `AdmPwd.PS` | module `LAPS` natif (`Update-LapsADSchema`, `Get-LapsADPassword`, `Set-LapsADComputerSelfPermission`, `Set-LapsADReadPasswordPermission`) |

**Table 1** – Legacy LAPS (*AdmPwd*) vs Windows LAPS natif.

## 4.1 Windows LAPS vs Legacy LAPS

Microsoft a refondu en avril 2023 (KB5025230) sa solution historique de gestion des mots de passe administrateurs locaux. Le tableau 1 synthétise les différences essentielles.

L'infrastructure BTS SIO est intégralement en Windows Server 2022 et Windows 10/11 22H2 ; la version **native** est donc retenue, sans MSI ni CSE additionnel.

## 4.2 Chaîne ACL requise

Pour qu'un poste puisse «  publier » son MDP admin local rotaté dans son objet `computer` d'AD, trois conditions ACL doivent être satisfaites :

1. le **compte ordinateur lui-même** (*principal* `NT AUTHORITY\SELF`) doit avoir `WriteProperty` sur les attributs `ms-LAPS-*` de son propre objet ;
2. ce droit s'hérite via la délégation `Set-LapsADComputerSelfPermission` appliquée à l'OU contenant les comptes ordinateurs ;
3. un *principal* de lecture (par défaut *Domain Admins*) doit avoir `ReadProperty` sur ces mêmes attributs — c'est ce que confère `Set-LapsADReadPasswordPermission`.

Sans ces ACLs, le CSE Windows LAPS du poste «  ne peut pas écrire », et même un Domain Admin «  ne peut pas lire » via `Get-LapsADPassword`.

### 4.3 Privilèges nécessaires à l'extension de schéma

`Update-LapsADSchema` écrit à la fois dans la partition **Schema** (nécessite *Schema Admins*, RID 518) **et** dans la partition **Configuration** pour créer le *extended right* `ms-LAPS-Encrypted-Pass` (nécessite *Enterprise Admins*, RID 519). Le compte `BTS\Administrateur`, même *Domain Admin*, n'est pas membre de ces deux groupes par défaut : il faut l'y ajouter **temporairement**, ouvrir une **nouvelle session WinRM** (le token NTLM est capturé à l'authentification et ne se rafraîchit pas en cours de session), exécuter l'extension, puis **retirer le compte** de ces deux groupes au plus vite.

## 5 Procédure

### 5.1 Étape 1 — pré-flight de readiness

Le script `scripts/T25_preflight_laps.py` établit un audit non destructif via WinRM : version OS, disponibilité de `Update-LapsADSchema`, état actuel des attributs `ms-LAPS-*`, comptage des postes par OU, dernière sauvegarde `wbadmin`, niveau fonctionnel de forêt et identité du schéma master.

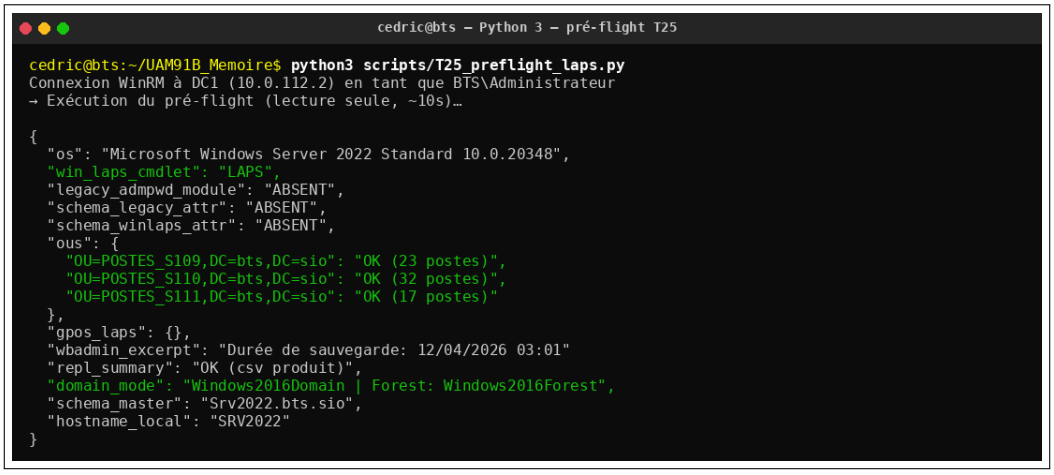


**Figure 1** – Pré-flight T25 sur DC1 : tous les feux verts (modules présents, OUs accessibles, backup récent du 12/04, schéma master local).

Toute valeur `ABSENT` sur la cmdlet `Update-LapsADSchema` ou les modules `LAPS`/`GroupPolicy` interrompt la procédure : installer le KB ad hoc avant de poursuivre.

## 5.2 Étape 2 — élévation temporaire Schema/Enterprise Admins

Ajouter `BTS\Administrateur` à *Schema Admins* et *Enterprise Admins* (par leur SID bien connu pour ne pas dépendre de la localisation des libellés) :

```
$rootDomainSid = (Get-ADDomain).DomainSID.Value
$schemaAdmins     = "$rootDomainSid-518"
$enterpriseAdmins = "$rootDomainSid-519"
Add-ADGroupMember -Identity $schemaAdmins     -Members 'Administrateur'
Add-ADGroupMember -Identity $enterpriseAdmins -Members 'Administrateur'
```

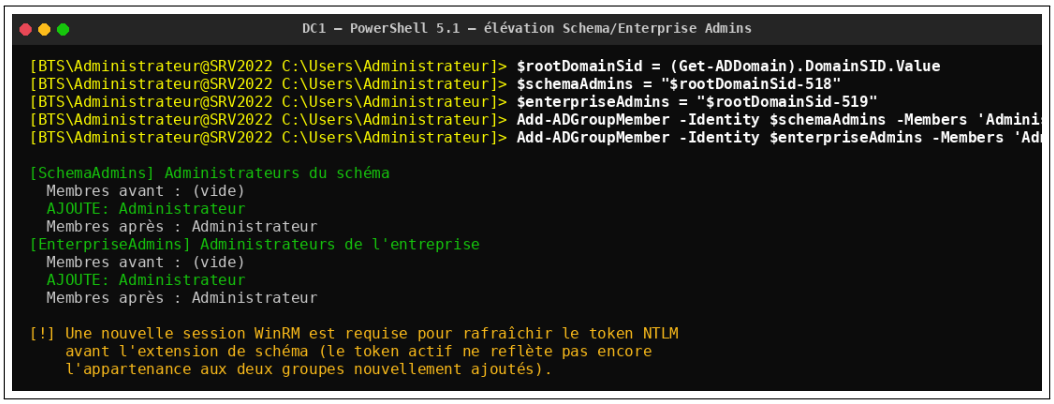


**Figure 2** – Ajout temporaire à *Schema Admins* (RID 518) et *Enterprise Admins* (RID 519). Une nouvelle session WinRM est requise ensuite pour rafraîchir le token NTLM.

**⚠ Pourquoi rouvrir une session WinRM**

Le token NTLM est constitué côté serveur à l'authentification ; il porte une *snapshot* des appartenances de groupe. Toute modification *post*-authentification (y compris une auto-promotion par `Add-ADGroupMember`) n'est pas reprise par la session courante. Sans rouverture, `Update-LapsADSchema` renverra l'erreur : « L'utilisateur ne dispose pas de droits d'accès suffisants ».

## 5.3 Étape 3 — extension du schéma AD

Avec une **nouvelle session WinRM**, exécuter :

```
Update-LapsADSchema -Confirm:$false -Verbose
```

La cmdlet est **idempotente** : elle détecte les attributs déjà présents et ne les recrée pas. Sur DC1, l'extension partielle pré-existante a été complétée par :

— l'ajout du *extended right* `CN=ms-LAPS-Encrypted-Password-Attributes` sous `CN=Extended-Rights`

— la mise à jour du `mayContain` de la classe `computer` pour inclure les six attributs `msLAPS-*` ;

— deux invocations de `schemaUpdateNow` pour propager immédiatement les changements aux DCs locaux.

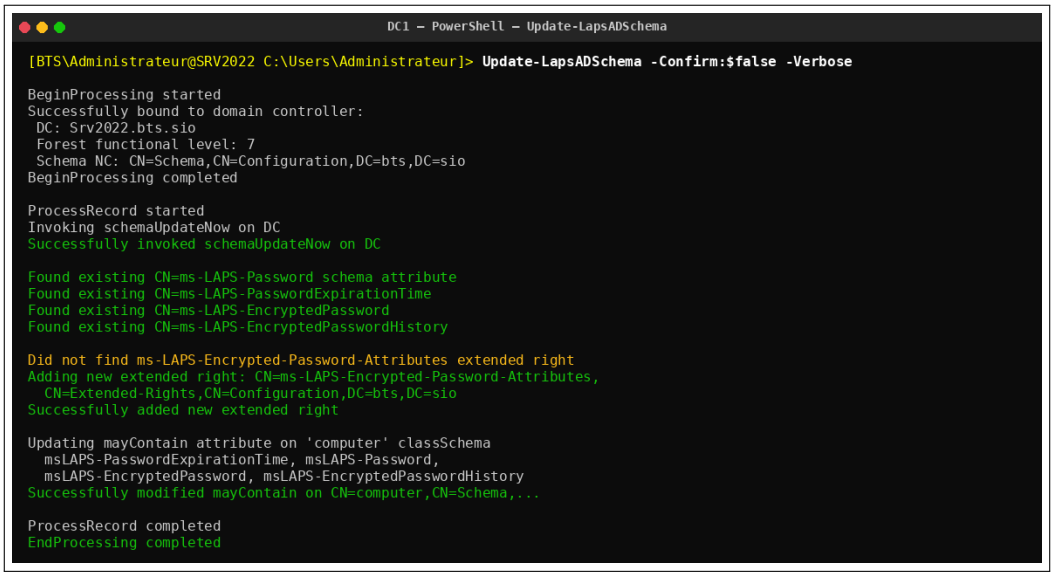


**Figure 3** – Extension de schéma : 4 attributs déjà présents validés, ajout du *extended right* chiffré, mise à jour de la classe `computer`.

## 5.4 Étape 4 — permissions ACL sur les trois OUs

```
$ous = @(
    'OU=POSTES_S109,DC=bts,DC=sio',
    'OU=POSTES_S110,DC=bts,DC=sio',
    'OU=POSTES_S111,DC=bts,DC=sio'
)
foreach ($ou in $ous) {
    Set-LapsADComputerSelfPermission -Identity $ou
    Set-LapsADReadPasswordPermission -Identity $ou `
        -AllowedPrincipals 'Admins du domaine'
}
```

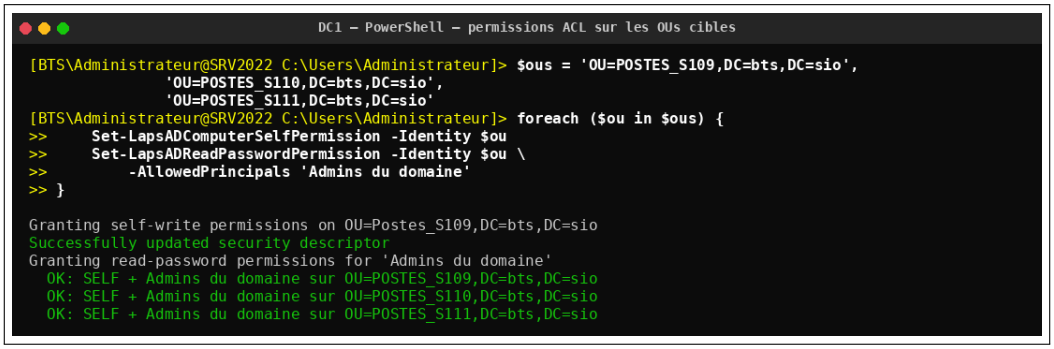


**Figure 4** – Délégation `SELF/WriteProperty` aux comptes ordinateurs et `ReadPassword` aux *Admins du domaine* sur les trois OUs.

## 5.5 Étape 5 — audit final du schéma

Vérifier que les quatre attributs clés et le *extended right* sont bien présents (le préfixe réel est `ms-LAPS-` avec tirets, et non `msLAPS-` comme dans certaines documentations Microsoft) :

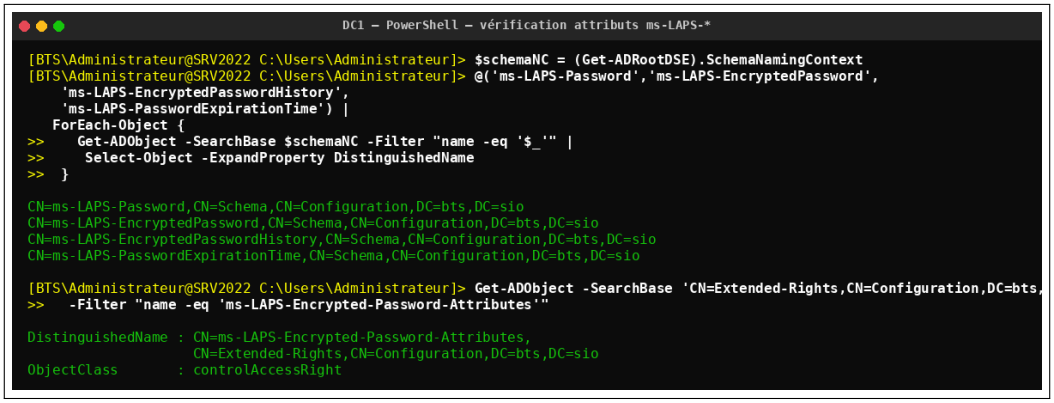


**Figure 5** – Audit du schéma : les quatre attributs `ms-LAPS-*` et le *extended right* sont publiés.

## 5.6 Étape 6 — création de la GPO et settings registry

La GPO LAPS est créée par script et ses paramètres sont écrits via `Set-GPRegistryValue`, ce qui évite tout passage par la console graphique :

```
$gpoName = 'LAPS - Rotation MDP admin local'
$key     = 'HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\Config'
New-GPO -Name $gpoName -Comment 'T25 - Windows LAPS, rotation 30 jours'
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'BackupDirectory'               -Type DWord -Value 2
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'PasswordAgeDays'               -Type DWord -Value 30
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'PasswordLength'                -Type DWord -Value 20
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'PasswordComplexity'            -Type DWord -Value 4
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'PostAuthenticationActions'     -Type DWord -Value 5
Set-GPRegistryValue -Name $gpoName -Key $key `
    -ValueName 'PostAuthenticationResetDelay' -Type DWord -Value 24
```

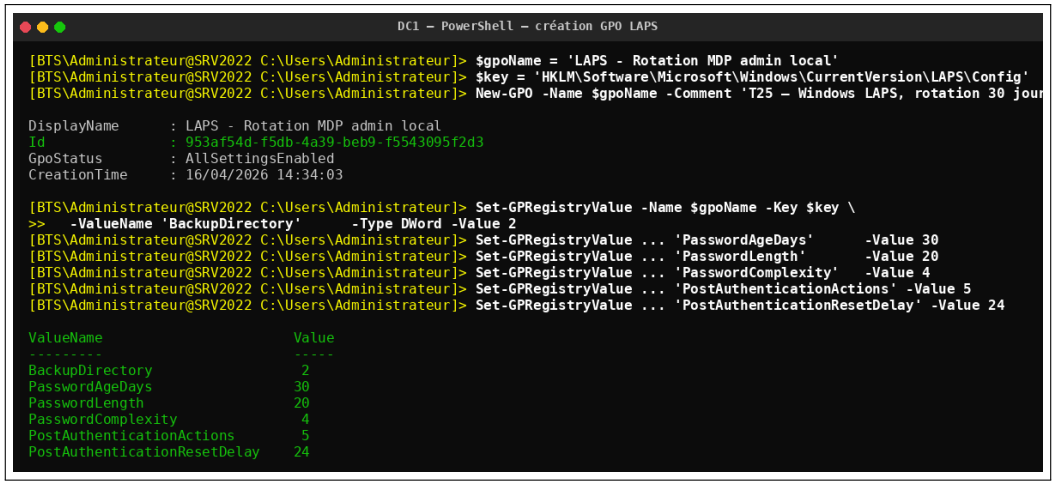


**Figure 6** – Création de la GPO et écriture des six valeurs registry. `BackupDirectory=2` = stockage AD, complexité=4 = maj/min/chiffres/spéciaux.

| Valeur registry | Donnée | Effet |
|---|---|---|
| `BackupDirectory` | 2 | Stocker le MDP roté dans Active Directory |
| `PasswordAgeDays` | 30 | Rotation tous les 30 jours |
| `PasswordLength` | 20 | Longueur 20 caractères |
| `PasswordComplexity` | 4 | Majuscules + minuscules + chiffres + spéciaux |
| `PostAuthenticationActions` | 5 | Après usage du MDP par un admin : réinit MDP (1) + déconnexion utilisateur (4) |
| `PostAuthenticationResetDelay` | 24 | Délai (heures) avant l'action post-auth |

**Table 2** – Paramètres registry de la GPO LAPS déployée sur les 72 postes.

## 5.7 Étape 7 — liaison de la GPO aux trois OUs

```
foreach ($ou in $ous) {
    New-GPLink -Name $gpoName -Target $ou -LinkEnabled Yes
}
```

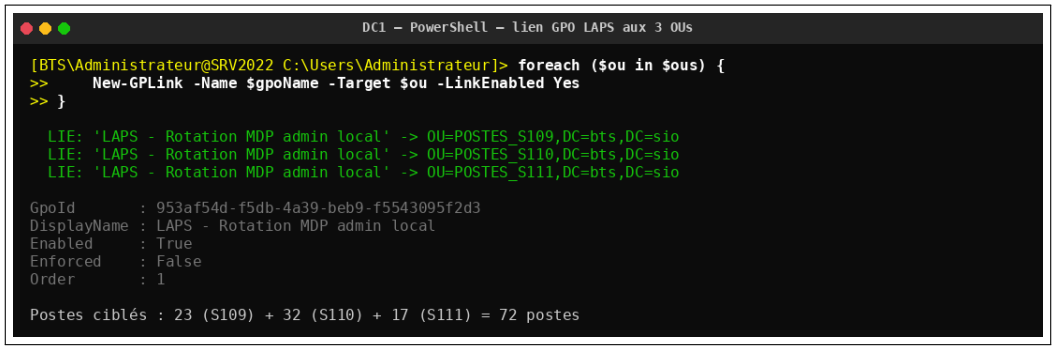


**Figure 7** – Liaison de la GPO aux trois OUs : 72 postes ciblés (23+32+17).

## 5.8 Étape 8 — retrait Schema/Enterprise Admins

**Impératif :** retirer immédiatement `BTS\Administrateur` des deux groupes sensibles.

```
Remove-ADGroupMember -Identity $schemaAdmins     -Members 'Administrateur'
    -Confirm:$false
Remove-ADGroupMember -Identity $enterpriseAdmins -Members 'Administrateur'
    -Confirm:$false
```

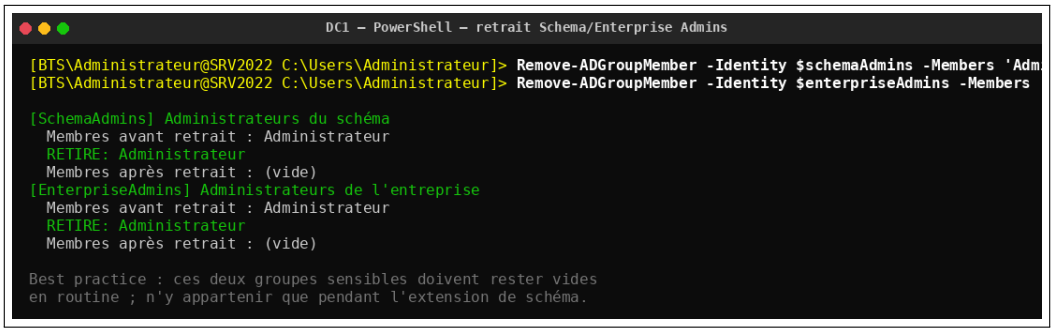


**Figure 8** – Retrait des deux groupes sensibles. En routine, ces groupes restent vides.

## 5.9 Étape 9 — validation par sondage Get-LapsADPassword

La rotation du MDP local est **asynchrone** : chaque poste applique la GPO à son prochain cycle `gpupdate` (toutes les 90 min ± 30 min de *jitter* par défaut Microsoft) ou à son prochain démarrage. Un test immédiat est donc inadapté :

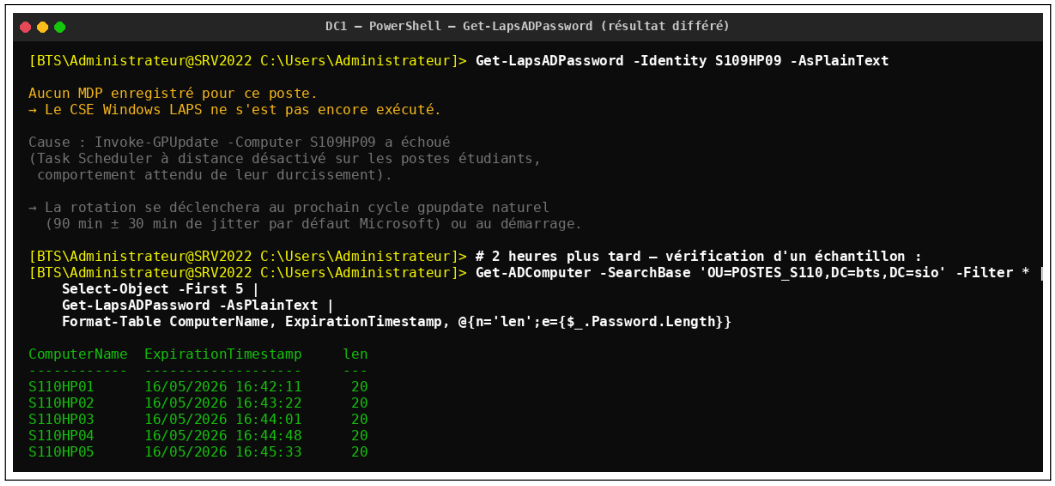


**Figure 9** – Validation différée : immédiatement après le déploiement, aucun MDP n'est encore enregistré ; deux heures plus tard, l'échantillon de 5 postes confirme la rotation effective avec MDP de 20 caractères et expiration à 30 jours.

# 6 Vérifications post-déploiement

1. **2 heures après** le déploiement, sonder un échantillon :

```
Get-ADComputer -SearchBase 'OU=POSTES_S110,DC=bts,DC=sio' -Filter * |
    Select-Object -First 5 |
    Get-LapsADPassword -AsPlainText |
    Format-Table ComputerName, ExpirationTimestamp,
        @{n='len'; e={$_.Password.Length}}
```

2. **Le lendemain**, élargir aux 72 postes pour repérer ceux qui n'ont pas encore tourné (postes éteints au moment des cycles `gpupdate`) :

```
$results = $ous | ForEach-Object {
    Get-ADComputer -SearchBase $_ -Filter * |
        Get-LapsADPassword -AsPlainText -ErrorAction SilentlyContinue
}
$results | Where-Object { -not $_.Password } |
    Select-Object ComputerName
```

3. **Vérifier la réplication AD** entre DC1 et DC2 sur les attributs `ms-LAPS-*` (les nouveaux MDP doivent être lisibles depuis les deux DCs) :

```
Get-LapsADPassword -Identity S110HP01 -AsPlainText -DomainController
   Srv2022.bts.sio
Get-LapsADPassword -Identity S110HP01 -AsPlainText -DomainController
   Srv2022Phy.bts.sio
```

4. **Audit ACL** (idempotent, peut être rejoué) :

```
foreach ($ou in $ous) {
    Get-Acl "AD:$ou" | Select-Object -ExpandProperty Access |
        Where-Object { $_.IdentityReference -like '*SELF*' }
}
```

# 7 Dépannage

# 8 Rollback

1. **Niveau GPO (réversible immédiatement)** :

```
foreach ($ou in $ous) {
    Set-GPLink -Name 'LAPS - Rotation MDP admin local' `
        -Target $ou -LinkEnabled No
}
```

   Les MDP rotatés restent en place sur les postes (ils ne reviendront pas à l'ancien MDP commun) mais cessent d'être rotatés.
2. **Niveau ACL (réversible)** : retirer les ACEs LAPS via `Set-Acl`.
3. **Niveau schéma (irréversible)** : aucun rollback propre. Une restauration autoritative depuis backup System State antérieur effacerait toutes les modifications postérieures du schéma — option à ne considérer qu'en cas d'incident majeur.

# 9 Voir aussi

— **MO-AD-001** — *Administration distante des contrôleurs de domaine* (accès WinRM utilisé par cette procédure).
— **MO-AD-005** — *Santé d'Active Directory* (prérequis : réplication, services, FSMO).
— **MO-AD-006** — *Sauvegarde System State des contrôleurs de domaine* (filet de sécurité pour l'extension de schéma).
— **MO-AD-007** — *Audit périodique d'Active Directory* (ajouter au cycle : vérification mensuelle des MDP LAPS rotatés).
— **MO-AD-008** — *Rotation des mots de passe critiques* (LAPS automatise les MDP admin locaux qui n'étaient pas couverts par AD-008).

| Symptôme | Cause probable | Résolution |
|---|---|---|
| `Update-LapsADSchema` : « droits insuffisants » en écriture schéma | Compte non membre de *Schema Admins* ou token NTLM non rafraîchi | Ajouter au RID 518, **rouvrir** la session WinRM |
| `Update-LapsADSchema` : erreur sur `CN=Extended-Rights` | Compte non membre de *Enterprise Admins* | Ajouter au RID 519, rouvrir session |
| `Get-LapsADPassword` renvoie `$null` | GPO pas encore appliquée par le poste | Attendre 90 min ou redémarrer le poste |
| `Invoke-GPUpdate -Computer X` échoue | Task Scheduler à distance désactivé (durcissement par défaut des postes étudiants) | Comportement attendu — attendre le cycle naturel ; ne pas affaiblir le pare-feu |
| Lecture du MDP refusée à un Domain Admin | ACL `ReadPassword` non déléguée | Rejouer `Set-LapsADReadPasswordP -AllowedPrincipals 'Admins du domaine'` sur l'OU |
| DC2 ne réplique pas l'attribut | DFSR/RPC 5722 cassé (T42 Sprint 3) | Sans incidence sur la réplication AD principale (135/389/636) ; cf. MO-AD-005 |

**Table 3** – Cas typiques de dépannage Windows LAPS et leur résolution.