

Mode Opérateur

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 <i>Domain Admins</i>). L'étape d'extension de schéma exige une appartenance <i>temporaire</i> aux groupes <i>Schema Admins</i> et <i>Enterprise Admins</i> .
Systèmes ciblés	Domaine <code>bts.sio</code> (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 <code>ActiveDirectory</code> , <code>LAPS</code> et <code>GroupPolicy</code> , <code>repadmin</code> , <code>WinRM</code> via <code>pywinrm</code> .
Authentification	Compte Domain Admin (<code>BTS\Administrateur</code> ou équivalent), avec passage temporaire dans <i>Schema Admins</i> et <i>Enterprise Admins</i> pour la phase d'extension de schéma.
Durée	≈ 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 <code>WinRM</code> 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 (<i>AdmPwd</i>)	Windows LAPS (natif)
Disponibilité	MSI Microsoft à télécharger, CSE à installer	Intégré OS Server 2019+ et Win10/11 (KB5025230)
Attribut MDP clair	<code>ms-Mcs-AdmPwd</code>	<code>ms-LAPS-Password</code>
Attribut MDP chiffré	— (clair uniquement)	<code>ms-LAPS-EncryptedPassword</code> (DPAPI-NG)
Historique	—	<code>ms-LAPS-EncryptedPasswordHistory</code>
Stockage backup	AD uniquement	AD ou Azure AD
Cmdlets PowerShell	module externe <code>AdmPwd.PS</code>	module LAPS natif (<code>Update-LapsADSchema</code> , <code>Get-LapsADPassword</code> , <code>Set-LapsADComputerSelfPermission</code> , <code>Set-LapsADReadPasswordPermission</code>)

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`.

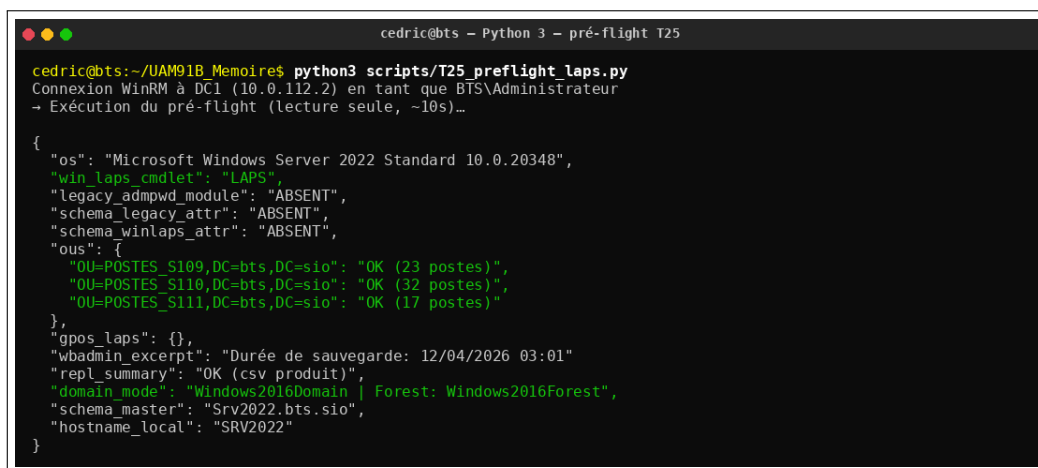
4.3 Privilèges nécessaires à l'extension de schéma

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.



```
cedric@bts - Python 3 - pré-flight T25
cedric@bts:~/UAM91B_Memoire$ python3 scripts/T25_preflight_laps.py
Connexion WinRM à DC1 (10.0.112.2) en tant que BTS\Administrateur
→ Exécution du pré-flight (lecture seule, ~10s)...

{
  "os": "Microsoft Windows Server 2022 Standard 10.0.20348",
  "win_laps_cmdlet": "LAPS",
  "legacy_admpwd_module": "ABSENT",
  "schema_legacy_attr": "ABSENT",
  "schema_winlaps_attr": "ABSENT",
  "ous": {
    "OU=POSTES_S109,DC=bts,DC=sio": "OK (23 postes)",
    "OU=POSTES_S110,DC=bts,DC=sio": "OK (32 postes)",
    "OU=POSTES_S111,DC=bts,DC=sio": "OK (17 postes)"
  },
  "gpos_laps": {},
  "wbadmin_excerpt": "Durée de sauvegarde: 12/04/2026 03:01",
  "repl_summary": "OK (csv produit)",
  "domain_mode": "Windows2016Domain | Forest: Windows2016Forest",
  "schema_master": "Srv2022.bts.sio",
  "hostname_local": "SRV2022"
}
```

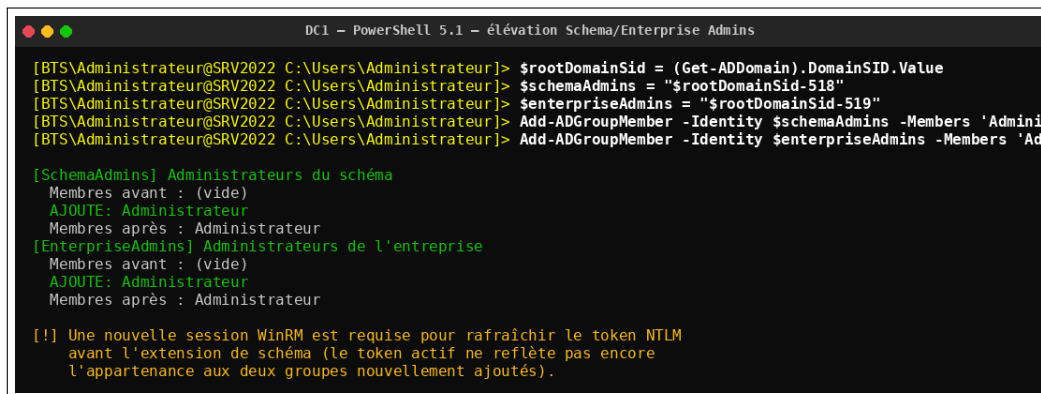
Figure 1 – Pré-flight T25 sur DC1 : tous les feux verts (modules présents, OUs accessibles, backup récent du 12/04, schéma master local).

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'
```



```
DC1 - PowerShell 5.1 - élévation Schema/Enterprise Admins
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $rootDomainSid = (Get-ADDomain).DomainSID.Value
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $schemaAdmins = "$rootDomainSid-518"
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $enterpriseAdmins = "$rootDomainSid-519"
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Add-ADGroupMember -Identity $schemaAdmins -Members 'Administrateur'
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Add-ADGroupMember -Identity $enterpriseAdmins -Members 'Administrateur'

[SchemaAdmins] Administrateurs du schéma
Membres avant : (vide)
AJOUTE: Administrateur
Membres après : Administrateur
[EnterpriseAdmins] Administrateurs de l'entreprise
Membres avant : (vide)
AJOUTE: Administrateur
Membres après : Administrateur

[!] Une nouvelle session WinRM est requise pour rafraîchir le token NTLM
avant l'extension de schéma (le token actif ne reflète pas encore
l'appartenance aux deux groupes nouvellement ajoutés).
```

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 ».

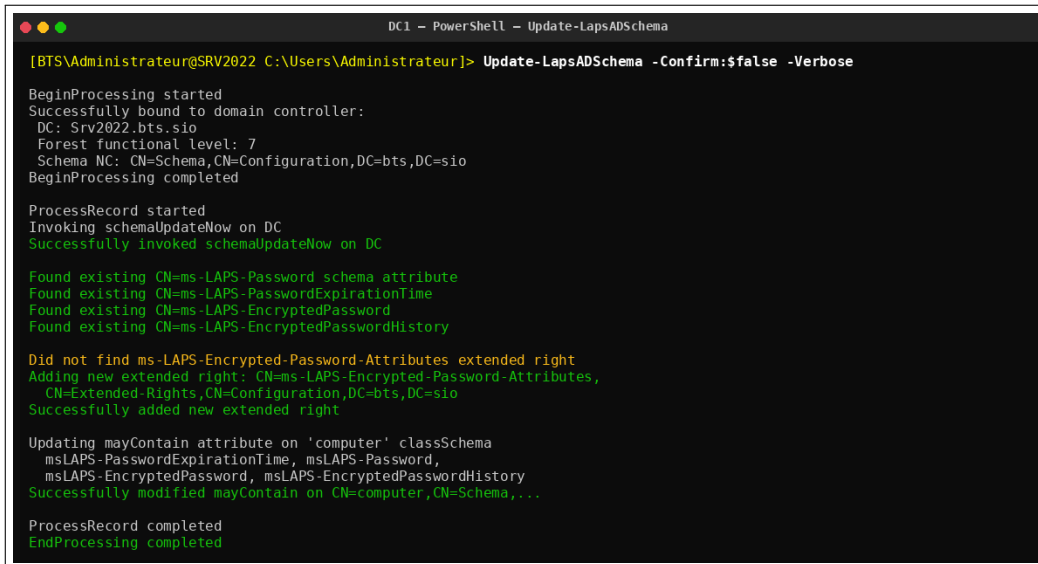
5.3 Étape 3 — extension du schéma AD

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.



```
DC1 - PowerShell - Update-LapsADSchema
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Update-LapsADSchema -Confirm:$false -Verbose
BeginProcessing started
Successfully bound to domain controller:
DC: Srv2022.bts.sio
Forest functional level: 7
Schema NC: CN=Schema,CN=Configuration,DC=bts,DC=sio
BeginProcessing completed

ProcessRecord started
Invoking schemaUpdateNow on DC
Successfully invoked schemaUpdateNow on DC

Found existing CN=ms-LAPS-Password schema attribute
Found existing CN=ms-LAPS-PasswordExpirationTime
Found existing CN=ms-LAPS-EncryptedPassword
Found existing CN=ms-LAPS-EncryptedPasswordHistory

Did not find ms-LAPS-Encrypted-Password-Attributes extended right
Adding new extended right: CN=ms-LAPS-Encrypted-Password-Attributes,
CN=Extended-Rights,CN=Configuration,DC=bts,DC=sio
Successfully added new extended right

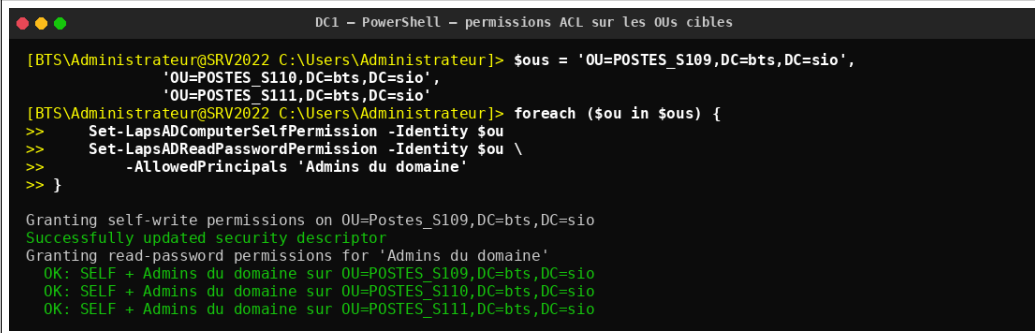
Updating mayContain attribute on 'computer' classSchema
msLAPS-PasswordExpirationTime, msLAPS-Password,
msLAPS-EncryptedPassword, msLAPS-EncryptedPasswordHistory
Successfully modified mayContain on CN=computer,CN=Schema,...

ProcessRecord completed
EndProcessing completed
```

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'
}
```

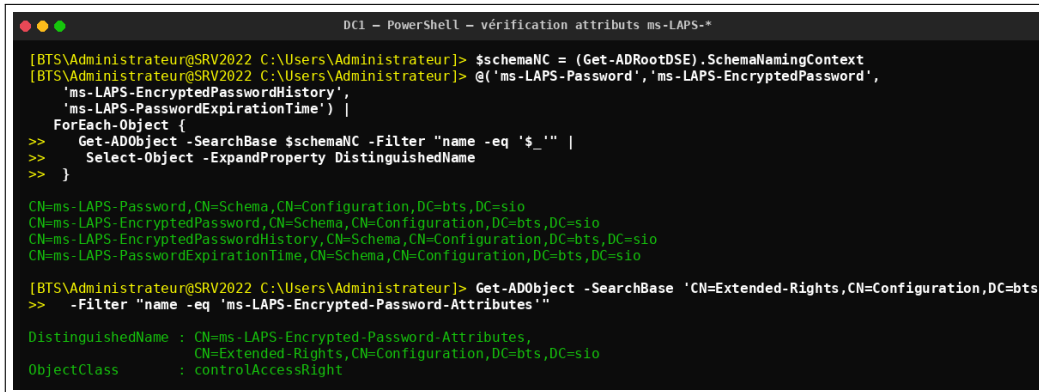


```
DC1 - PowerShell - permissions ACL sur les OUs cibles
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $ous = 'OU=POSTES_S109,DC=bts,DC=sio',
'OU=POSTES_S110,DC=bts,DC=sio',
'OU=POSTES_S111,DC=bts,DC=sio'
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] foreach ($ou in $ous) {
>> Set-LapsADComputerSelfPermission -Identity $ou
>> Set-LapsADReadPasswordPermission -Identity $ou \
>> -AllowedPrincipals 'Admins du domaine'
>> }
Granting self-write permissions on OU=Postes_S109,DC=bts,DC=sio
Successfully updated security descriptor
Granting read-password permissions for 'Admins du domaine'
OK: SELF + Admins du domaine sur OU=POSTES_S109,DC=bts,DC=sio
OK: SELF + Admins du domaine sur OU=POSTES_S110,DC=bts,DC=sio
OK: SELF + Admins du domaine sur OU=POSTES_S111,DC=bts,DC=sio
```

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) :



```
DC1 - PowerShell - vérification attributs ms-LAPS-*
[BTSAAdministrateur@SRV2022 C:\Users\Administrateur]> $schemaNC = (Get-ADRootDSE).SchemaNamingContext
[BTSAAdministrateur@SRV2022 C:\Users\Administrateur]> @('ms-LAPS-Password', 'ms-LAPS-EncryptedPassword',
'ms-LAPS-EncryptedPasswordHistory',
'ms-LAPS-PasswordExpirationTime') |
ForEach-Object {
>> Get-ADObject -SearchBase $schemaNC -Filter "name -eq '$_'" |
>> Select-Object -ExpandProperty DistinguishedName
>> }

CN=ms-LAPS-Password,CN=Schema,CN=Configuration,DC=bts,DC=sio
CN=ms-LAPS-EncryptedPassword,CN=Schema,CN=Configuration,DC=bts,DC=sio
CN=ms-LAPS-EncryptedPasswordHistory,CN=Schema,CN=Configuration,DC=bts,DC=sio
CN=ms-LAPS-PasswordExpirationTime,CN=Schema,CN=Configuration,DC=bts,DC=sio

[BTSAAdministrateur@SRV2022 C:\Users\Administrateur]> Get-ADObject -SearchBase 'CN=Extended-Rights,CN=Configuration,DC=bts,
>> -Filter "name -eq 'ms-LAPS-Encrypted-Password-Attributes'"

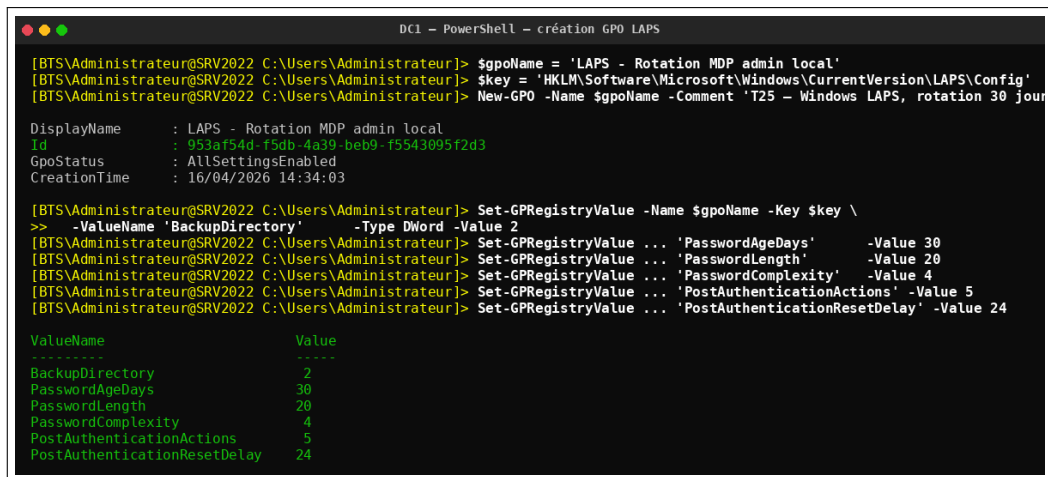
DistinguishedName : CN=ms-LAPS-Encrypted-Password-Attributes,
                  CN=Extended-Rights,CN=Configuration,DC=bts,DC=sio
ObjectClass       : controlAccessRight
```

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
```



```
DC1 - PowerShell - création GPO LAPS
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $gpoName = 'LAPS - Rotation MDP admin local'
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] $key = 'HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\Config'
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] New-GPO -Name $gpoName -Comment 'T25 - Windows LAPS, rotation 30 jours'

DisplayName      : LAPS - Rotation MDP admin local
Id               : 953af54d-f5db-4a39-beb9-f5543095f2d3
GpoStatus        : AllSettingsEnabled
CreationTime     : 16/04/2026 14:34:03

[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue -Name $gpoName -Key $key `
>> -ValueName 'BackupDirectory' -Type DWord -Value 2
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue ... 'PasswordAgeDays' -Value 30
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue ... 'PasswordLength' -Value 20
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue ... 'PasswordComplexity' -Value 4
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue ... 'PostAuthenticationActions' -Value 5
[BTS\Administrateur@SRV2022 C:\Users\Administrateur] Set-GPRegistryValue ... 'PostAuthenticationResetDelay' -Value 24

ValueName      Value
-----
BackupDirectory 2
PasswordAgeDays 30
PasswordLength  20
PasswordComplexity 4
PostAuthenticationActions 5
PostAuthenticationResetDelay 24
```

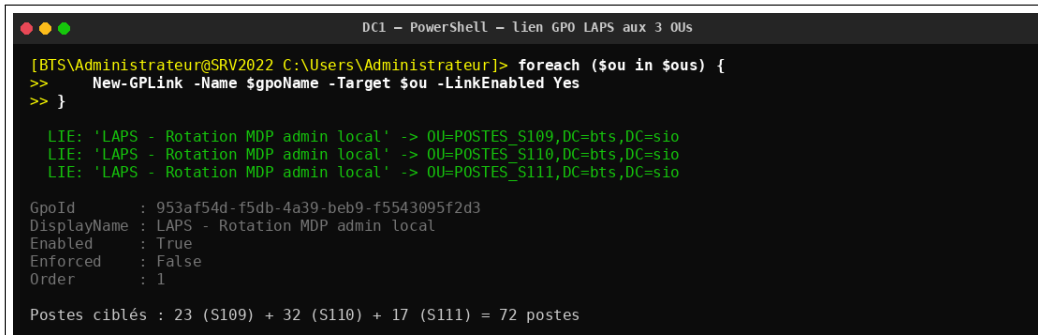
Figure 6 – Création de la GPO et écriture des six valeurs registry. `BackupDirectory=2` = stockage AD, `complexité=4` = maj/min/chiffres/spéciaux.

Valeur registry	Donnée	Effet
BackupDirectory	2	Stocker le MDP rotaté 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  
}
```



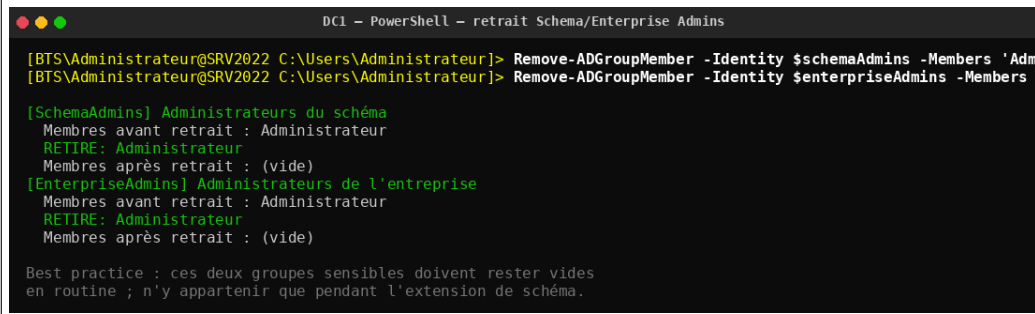
```
DC1 - PowerShell - lien GPO LAPS aux 3 OUs  
[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> foreach ($ou in $ous) {  
>>   New-GPLink -Name $gpoName -Target $ou -LinkEnabled Yes  
>> }  
  
LIE: 'LAPS - Rotation MDP admin local' -> OU=POSTES_S109,DC=bts,DC=sio  
LIE: 'LAPS - Rotation MDP admin local' -> OU=POSTES_S110,DC=bts,DC=sio  
LIE: 'LAPS - Rotation MDP admin local' -> OU=POSTES_S111,DC=bts,DC=sio  
  
GpoId      : 953af54d-f5db-4a39-beb9-f5543095f2d3  
DisplayName : LAPS - Rotation MDP admin local  
Enabled    : True  
Enforced   : False  
Order     : 1  
  
Postes ciblés : 23 (S109) + 32 (S110) + 17 (S111) = 72 postes
```

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
```

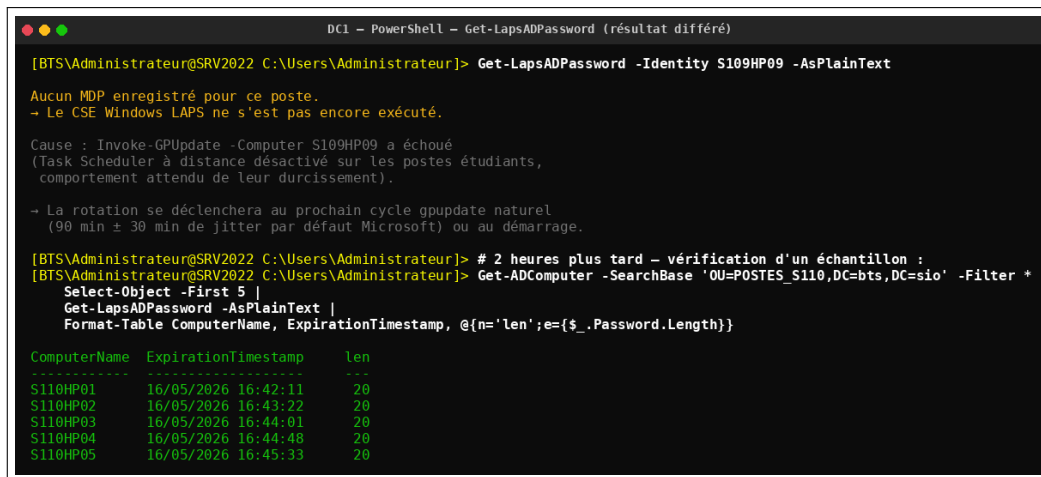


```
DC1 - PowerShell - retrait Schema/Enterprise Admins  
[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> Remove-ADGroupMember -Identity $schemaAdmins -Members 'Administrateur'  
[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> Remove-ADGroupMember -Identity $enterpriseAdmins -Members 'Administrateur'  
[SchemaAdmins] Administrateurs du schéma  
Membres avant retrait : Administrateur  
RETIRES: Administrateur  
Membres après retrait : (vide)  
[EnterpriseAdmins] Administrateurs de l'entreprise  
Membres avant retrait : Administrateur  
RETIRES: Administrateur  
Membres après retrait : (vide)  
  
Best practice : ces deux groupes sensibles doivent rester vides  
en routine ; n'y appartenir que pendant l'extension de schéma.
```

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 \pm 30 min de *jitter* par défaut Microsoft) ou à son prochain démarrage. Un test immédiat est donc inadapté :



```
DC1 - PowerShell - Get-LapsADPassword (résultat différé)

[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> Get-LapsADPassword -Identity S109HP09 -AsPlainText

Aucun MDP enregistré pour ce poste.
- Le CSE Windows LAPS ne s'est pas encore exécuté.

Cause : Invoke-GPUdate -Computer S109HP09 a échoué
(Task Scheduler à distance désactivé sur les postes étudiants,
comportement attendu de leur durcissement).

- La rotation se déclenchera au prochain cycle gpupdate naturel
(90 min  $\pm$  30 min de jitter par défaut Microsoft) ou au démarrage.

[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> # 2 heures plus tard - vérification d'un échantillon :
[BTS\Administrateur@SRV2022 C:\Users\Administrateur]> 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}}
```

ComputerName	ExpirationTimestamp	len
S110HP01	16/05/2026 16:42:11	20
S110HP02	16/05/2026 16:43:22	20
S110HP03	16/05/2026 16:44:01	20
S110HP04	16/05/2026 16:44:48	20
S110HP05	16/05/2026 16:45:33	20

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 répllication 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 <i>Schema Admins</i> ou token NTLM non rafraîchi	Ajouter au RID 518, rouvrir la session WinRM
Update-LapsADSchema : erreur sur CN=Extended-Rights	Compte non membre de <i>Enterprise Admins</i>	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-GPUdate -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 ReadPasswordSet-LapsADReadPassword non déléguée	Rejouer -AllowedPrincipals 'Admins du domaine' sur l'OU
DC2 ne réplique pas l'attribut	DFSR/RPC 5792ms incassé (T42 Sprint 3)	Incidence sur la réplication AD principale (135/389/636); cf. MO-AD-005

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