Windows LAPS: hasło lokalnego administratora w Active Directory

Poziom: średniozaawansowany

Dotyczy: Windows LAPS, Windows Server 2019+ (schemat), Windows 10/11

Czas: ~30 min

Windows LAPS nadaje każdemu komputerowi inne, losowe hasło konta lokalnego administratora i rotuje je automatycznie, zamiast trzymać jedno wspólne hasło na całej flocie. Hasła trafiają do Active Directory, a o to, kto może je odczytać, decydujemy sami przez uprawnienia.

> Komputery zarządzane z Intune, zwłaszcza te rzadko widujące kontroler domeny, mogą trzymać hasło w Microsoft Entra ID zamiast w Active Directory, a politykę ustawiamy wtedy w Intune, nie w GPO. Opisuje to strona Windows LAPS z Intune: hasło lokalnego administratora w Entra ID albo AD.

Skróty użyte na tej stronie (5)

Skrót	Co znaczy
DSRM	Directory Services Restore Mode: awaryjny tryb startu kontrolera domeny, w którym usługa Active Directory się nie uruchamia, używany do naprawy albo przywrócenia bazy katalogu
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
LAPS	Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery

Fiszka

◫◫ ZMIENIA SYSTEM

Rozszerzenie schematu Active Directory: Update-LapsADSchema

```
Update-LapsADSchema
```

Uruchamiamy raz na cały las, kontem z uprawnieniami Schema Admins, zwykle bezpośrednio na kontrolerze domeny pełniącym rolę Schema Master. Polecenie dokłada do schematu atrybuty przechowujące hasło i jego historię, których wcześniej w katalogu po prostu nie było.

Przykład:

```
Atrybut schematu ms-LAPS-Password zostanie dodany do lasu ad.zielona.example.
Czy chcesz kontynuować?
[T] Tak  [W] Tak na wszystkie  [N] Nie  [?] Pomoc (domyślnie „T"):
```

◫◫ ZMIENIA SYSTEM

Nadanie komputerom prawa zapisu własnego hasła: Set-LapsADComputerSelfPermission

```
Set-LapsADComputerSelfPermission -Identity "OU=Komputery,DC=ad,DC=zielona,DC=example"
```

Bez tego uprawnienia komputer, mimo poprawnej polityki, nie zapisze swojego hasła do katalogu, bo konto komputera nie ma prawa zapisu do własnego atrybutu `ms-LAPS-Password`. Wykonujemy raz na każdą jednostkę organizacyjną, w której stoją komputery objęte Windows LAPS.

◫◫ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu · **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

◫◫ ZMIENIA SYSTEM

Nadanie prawa odczytu hasła: Set-LapsADReadPasswordPermission

```
Set-LapsADReadPasswordPermission -Identity "OU=Komputery,DC=ad,DC=zielona,DC=example" -
AllowedPrincipals "ZIELONA\Helpdesk"
```

Grupa albo konto podane w `-AllowedPrincipals` dostaje prawo odczytu haseł komputerów z całej jednostki organizacyjnej wskazanej w `-Identity`. Zasada najmniejszych uprawnień działa tu tak samo jak przy koncie technicznym LDAP z Gitea: prawo odczytu dostaje tylko grupa, która faktycznie potrzebuje haseł do pracy.

LDAP = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) · **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

TYLKO ODCZYT

Sprawdzenie, kto już ma prawo odczytu: Find-LapsADExtendedRights

```
Find-LapsADExtendedRights -Identity "OU=Komputery,DC=ad,DC=zielona,DC=example"
```

Przydatne przed pierwszym wdrożeniem i przy audycie: pokazuje, komu już dziś nadano rozszerzone prawo odczytu hasła w danej jednostce organizacyjnej, zanim dołożymy kolejną grupę.

Przykład:

```
ObjectDN                                                ExtendedRightHolders
--------                                                --------------------
OU=Komputery,DC=ad,DC=zielona,DC=example                {ZIELONA\Domain Admins,
                                                        ZIELONA\Helpdesk}
```

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

TYLKO ODCZYT

Odczyt hasła lokalnego administratora: Get-LapsADPassword

```
Get-LapsADPassword -Identity NazwaKomputera -AsPlainText
```

`-AsPlainText` pokazuje hasło wprost na ekranie zamiast jako zaszyfrowany obiekt `SecureString`, więc używamy go tylko wtedy, gdy faktycznie potrzebujemy hasła do wpisania na konsoli, nie przy rutynowym audycie.

Przykład:

```
DistinguishedName : CN=RDS01,OU=Komputery,DC=ad,DC=zielona,DC=example
Account           : Administrator
Password          : 7h!kP9qLmR2z
Expiration        : 21.10.2026 09:00:00
```

> `-Identity` w `Get-LapsADPassword` przyjmuje zwykłą nazwę komputera i to ona zadziała w zdecydowanej większości przypadków. Ale `Set-LapsADComputerSelfPermission`, `Set-LapsADReadPasswordPermission` i `Find-LapsADExtendedRights` operują na jednostce organizacyjnej, nie na komputerze, i w większym katalogu z zagnieżdżonymi jednostkami o podobnych nazwach przyjazna nazwa OU potrafi się okazać niejednoznaczna albo nie trafić tam, gdzie zamierzaliśmy. W `-Identity` tych trzech poleceń wpisujemy zawsze pełny `DistinguishedName` jednostki organizacyjnej, tak jak w przykładach wyżej, zamiast polegać na samej nazwie.

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery

ZMIENIA SYSTEM

Wymuszenie natychmiastowej rotacji hasła: Reset-LapsPassword

```
Reset-LapsPassword
```

Polecenie uruchamiamy lokalnie na samym komputerze, którego hasło chcemy zmienić od razu, bez czekania na najbliższy cykl rotacji z polityki. Typowe zastosowanie: ktoś poznał hasło, które powinien był znać tylko przez chwilę.

Z życia wzięte

Z ŻYCIA WZIĘTE

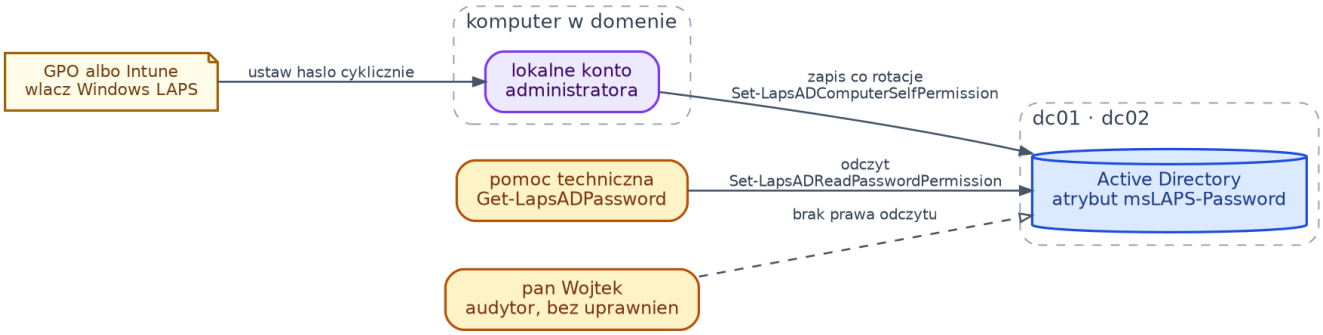
Pan Wojtek, coroczny audytor, pyta o hasła lokalnych administratorów na wszystkich 180 komputerach Zielonej. Tomek przez chwilę zastanawia się, czy to jedno hasło z arkusza Excela sprzed czterech lat wciąż obowiązuje, zanim przypomina sobie, że od miesiąca każdy komputer ma już inne, losowe hasło z Windows LAPS. Odpowiedź dla audytora brzmi: hasła są różne na każdej maszynie, rotują automatycznie, a kto je odczytał, zapisuje log zabezpieczeń kontrolera domeny.

Jak to działa

Rozwiń: jak to działa pod spodem

> **Pojęcie: Windows LAPS.** Wbudowana w Windows Server 2019 i nowsze (po aktualizacji) oraz w Windows 10/11 funkcja, która ustawia każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisuje je jako atrybut konta komputera w Active Directory, razem z datą następnej rotacji. Zastępuje starszy, niewspierany już dodatek LAPS (`Legacy Microsoft LAPS`), który trzymał hasło w osobnym, ręcznie dokładanym atrybucie `ms-Mcs-AdmPwd` i wymagał osobnego instalatora na każdej maszynie.
>
> **Pojęcie: Windows LAPS kontra stary LAPS.** Stary LAPS był dodatkiem do pobrania, wycofanym (deprecjacja od 23 października 2023, bez zmian w kodzie), z jednym stałym formatem hasła. Windows LAPS jest częścią systemu, umie też zapisywać hasło do Microsoft Entra ID zamiast do Active Directory (dla komputerów Entra joined i hybrid joined, nie dla `Entra registered`; patrz Windows LAPS z Intune: hasło lokalnego administratora w Entra ID albo AD), i pozwala ustawić długość, złożoność oraz historię hasła z poziomu jednej polityki.

Po co to całe rozszerzanie schematu i osobne uprawnienia, zamiast po prostu włączyć funkcję: zapis hasła do katalogu wymaga miejsca w schemacie, którego w starszym lesie Active Directory po prostu nie ma, więc `Update-LapsADSchema` dokłada je raz na zawsze. Samo dołożenie atrybutu nie wystarcza: komputer musi jeszcze dostać prawo zapisu do własnego rekordu (`Set-LapsADComputerSelfPermission`), a osoby, które mają czytać hasła, prawo odczytu (`Set-LapsADReadPasswordPermission`), bo domyślnie nikt, łącznie z administratorami domeny, takiego prawa nie ma.



Komputer zapisuje haslo do Active Directory, pomoc techniczna je odczytuje, audytor bez uprawnien widzi tylko odmowe (kliknięcie otwiera pełny rozmiar)

Politykę włączającą Windows LAPS konfigurujemy jednym z dwóch sposobów: przez GPO (`Computer Configuration → Administrative Templates → System → LAPS`) na komputerach w domenie z łącznością do kontrolera, albo przez profil konfiguracyjny Intune na komputerach zarządzanych w chmurze. Oba prowadzą do tego samego atrybutu w katalogu, jeśli tylko komputer ma jeszcze łączność z Active Directory; różnica jest tylko w miejscu, z którego przychodzi ustawienie.

> **Pojęcie: szyfrowanie haseł w Active Directory.** Windows LAPS może zapisać hasło w atrybucie komputera w postaci zaszyfrowanej, a nie jawnym tekstem. Ustawienie `ADPasswordEncryptionEnabled` jest domyślnie włączone, ale działa tylko wtedy, gdy domena pracuje na poziomie funkcjonalnym 2016 lub wyższym; poziom sprawdzamy poleceniem `Get-ADDomain | Select-Object DomainMode`. Hasło odszyfrowuje wyłącznie podmiot wskazany w `ADPasswordEncryptionPrincipal`, a gdy go nie ustawimy, są to członkowie grupy Domain Admins. Samo prawo odczytu atrybutu (to z `Set-LapsADReadPasswordPermission`) więc nie wystarcza: konto bez prawa odszyfrowania dostaje w wyniku `Get-LapsADPassword` status `DecryptionStatus : Unauthorized` zamiast hasła.

Na kontrolerach domeny z Windows Server 2019 i nowszym Windows LAPS może zarządzać także hasłem trybu DSRM (wymaga poziomu domeny 2016 i włączonego szyfrowania).

Propozycję dla Zielonej i odczyt hasła z kopii bazy opisuje strona Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM.

> Jeśli `Get-LapsADPassword` kończy się statusem `Unauthorized`, choć `Find-LapsADExtendedRights` pokazuje naszą grupę, dopisujemy ją do `ADPasswordEncryptionPrincipal` w polityce (GPO albo Intune) albo

> wykonujemy odczyt z konta z grupy Domain Admins.

Częste błędy

Objaw	Przyczyna	Co robimy
`Get-LapsADPassword` zwraca `Unable to retrieve password. Verify current user context has rights`	brak prawa odczytu w jednostce organizacyjnej komputera	uruchamiamy `Find-LapsADExtendedRights` na tej jednostce i w razie potrzeby dokładamy grupę przez `Set-LapsADReadPasswordPermission`
Komputer zgodnie z polityką powinien już mieć nowe hasło, a `Get-LapsADPassword` pokazuje puste albo bardzo stare	brak prawa zapisu komputera do własnego atrybutu	uruchamiamy `Set-LapsADComputerSelfPermission` na jednostce organizacyjnej tego komputera, potem `gpupdate /force` na maszynie
`Set-LapsADReadPasswordPermission` z przyjazną nazwą jednostki organizacyjnej zwraca błąd albo trafia w złe miejsce	niejednoznaczna nazwa w rozbudowanym katalogu z zagnieżdżonymi jednostkami	podajemy pełny `DistinguishedName` jednostki w `-Identity`, tak jak w ostrzeżeniu przy fiszce wyżej
Po `Update-LapsADSchema` nowsze kontrolery domeny widzą atrybut, starsze nie	replikacja schematu jeszcze nie doszła do wszystkich kontrolerów	czekamy na pełny cykl replikacji albo sprawdzamy go `repadmin /replsummary`, zanim zgłosimy problem jako błąd LAPS

□□ Ćwiczenia

1. Dlaczego `Get-LapsADPassword -Identity NazwaKomputera` działa bez podawania pełnego `DistinguishedName`, a `Set-LapsADReadPasswordPermission -Identity NazwaOU` w dużym katalogu już nie jest bezpiecznym wyborem?

Odpowiedź

`Get-LapsADPassword` szuka konkretnego konta komputera po nazwie, a nazwy komputerów w rozsądnie zarządzanym katalogu są unikalne. `Set-LapsADReadPasswordPermission` i pozostałe polecenia od uprawnień szukają jednostki organizacyjnej po samej nazwie, a w katalogu z zagnieżdżoną strukturą (na przykład osobne jednostki dla każdego działu w każdej lokalizacji) ta sama nazwa potrafi się powtórzyć w kilku miejscach naraz, więc bezpieczniej wskazać jednostkę pełnym `DistinguishedName`.

1. Zespół włączył Windows LAPS przez GPO na całej jednostce organizacyjnej z komputerami, ale zapomniał uruchomić `Set-LapsADComputerSelfPermission`. Co zobaczymy w `Get-LapsADPassword` i dlaczego?

Odpowiedź

Zobaczymy pusty wynik albo błąd braku dostępu, mimo że polityka jest poprawnie włączona: komputer próbuje zapisać nowe hasło do własnego atrybutu w katalogu, ale bez nadanego wcześniej prawa zapisu Active Directory odrzuca ten zapis, więc atrybut pozostaje pusty albo nieaktualny.

Powiązane: Skrypty audytowe Active Directory · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt · Intune obok domeny: audyt GPO i plan migracji

Źródła: Microsoft Learn, „Get started with Windows LAPS and Windows Server Active Directory" · Microsoft Learn, „Windows LAPS schema and rights extensions for Windows Server Active Directory" · dokumentacja modułu PowerShell `LAPS` (`Get-Help Get-LapsADPassword`, `Get-Help Set-LapsADReadPasswordPermission`, `Get-Help Find-LapsADExtendedRights`, `Get-Help Reset-LapsPassword`)

Revision #30
Created 2026-09-28 06:14:59 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:46 UTC by Tomasz Konieczny