Zasady haseł i blokady konta: polityka domeny i PSO

Poziom: średniozaawansowany

Dotyczy: moduł PowerShell ActiveDirectory (RSAT), Windows Server 2016+

Czas: ~35 min

Jedna polityka haseł domeny obowiązuje wszystkie konta domenowe naraz, a wyjątki dla wybranych grup, na przykład administratorów, ustawia się osobnym mechanizmem, nie zwykłym GPO na jednostce organizacyjnej. Tu ustawiamy obie te rzeczy i szukamy, skąd bierze się konkretna blokada konta.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
NIST	National Institute of Standards and Technology: amerykańska agencja standaryzacyjna, tu autor wytycznych SP 800-63B o hasłach
PDC	Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł
PSO	Password Settings Object: obiekt w katalogu przechowujący precyzyjną politykę haseł, przypisywaną do wybranych kont albo grup zamiast całej domeny
RSAT	Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej
SP	Special Publication: oznaczenie serii dokumentów NIST, tu wytycznych o hasłach SP 800-63B

Fiszka

TYLKO ODCZYT

Odczyt bieżącej polityki haseł domeny: Get-ADDefaultDomainPasswordPolicy

```
Get-ADDefaultDomainPasswordPolicy
```

Pokazuje aktualne wartości polityki haseł obowiązującej wszystkie konta domenowe: minimalną długość, wymóg złożoności, okres ważności hasła i próg blokady konta. Pierwsze polecenie przed jakąkolwiek zmianą, żeby wiedzieć, od czego startujemy.

Przykład:

```
ComplexityEnabled           : True
LockoutDuration              : 00:15:00
LockoutObservationWindow     : 00:15:00
LockoutThreshold             : 5
MaxPasswordAge                : 42.00:00:00
MinPasswordLength            : 8
PasswordHistoryCount         : 24
```

ZMIENIA SYSTEM

Zmiana polityki haseł domeny: Set-ADDefaultDomainPasswordPolicy

```
Set-ADDefaultDomainPasswordPolicy -Identity NazwaDomeny -MinPasswordLength DlugoscHasla
-MaxPasswordAge OkresWaznosci -LockoutThreshold LiczbaProb -LockoutDuration CzasBlokady
```

Zmienia politykę haseł dla wszystkich kont domenowych naraz. `-MaxPasswordAge` w wartości `0.00:00:00` oznacza brak wymuszonego wygasania hasła, zamiast konkretnego okresu.

Przykład:

```
Set-ADDefaultDomainPasswordPolicy -Identity ad.zielona.example -MinPasswordLength 14 -
MaxPasswordAge 0.00:00:00 -LockoutThreshold 10 -LockoutDuration 0.00:15:00
```

ZMIENIA SYSTEM

Utworzenie precyzyjnej polityki haseł: New-ADFineGrainedPasswordPolicy

```
New-ADFineGrainedPasswordPolicy -Name NazwaPolityki -Precedence WartoscPierwszenstwa -MinPasswordLength DlugoscHasla -ComplexityEnabled WartoscTakNie -LockoutThreshold LiczbaProb -LockoutDuration CzasBlokady
```

Tworzy dodatkową, osobną politykę haseł, na razie nieprzypisaną do nikogo. `-Precedence` rozstrzyga, która polityka wygrywa, gdy to samo konto miałoby kwalifikować się do kilku naraz: niższa wartość oznacza wyższy priorytet.

Przykład:

```
New-ADFineGrainedPasswordPolicy -Name "PSO-Administratorzy" -Precedence 10 -MinPasswordLength 16 -ComplexityEnabled $true -LockoutThreshold 3 -LockoutDuration 1.00:00:00
```

◫◫ ZMIENIA SYSTEM

Przypisanie polityki do grupy: Add-ADFineGrainedPasswordPolicySubject

```
Add-ADFineGrainedPasswordPolicySubject -Identity NazwaPolityki -Subjects NazwaGrupy
```

Dopiero to polecenie zaczyna faktycznie stosować politykę utworzoną wcześniej, przypisując ją do konkretnych kont albo grup zabezpieczeń. Bez tego kroku `New-ADFineGrainedPasswordPolicy` tworzy tylko obiekt w katalogu, który na nikogo nie działa.

Przykład:

```
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO-Administratorzy" -Subjects "ZIELONA\Domain Admins"
```

◫◫ TYLKO ODCZYT

Sprawdzenie, która polityka faktycznie obowiązuje konto: Get-ADUserResultantPasswordPolicy

```
Get-ADUserResultantPasswordPolicy -Identity NazwaUzytkownika
```

Rozstrzyga za nas, która polityka wygrywa dla danego konta: jeśli żadna precyzyjna polityka nie jest przypisana, wynikiem jest zwykła polityka domeny, w przeciwnym razie ta z najniższą wartością `Precedence` spośród przypisanych bezpośrednio albo przez członkostwo w grupie.

Przykład:

```
Name                 : PSO-Administratorzy
Precedence           : 10
MinPasswordLength    : 16
LockoutThreshold     : 3
LockoutDuration       : 1.00:00:00
AppliesTo            : {CN=Domain Admins,CN=Users,DC=ad,DC=zielona,DC=example}
```

TYLKO ODCZYT

Wyszukanie zablokowanych kont: Search-ADAccount

```
Search-ADAccount -LockedOut
```

Zwraca listę wszystkich aktualnie zablokowanych kont w domenie, bez przeszukiwania ręcznego jednostka po jednostce w konsoli. Pierwsze polecenie, gdy zgłoszenie brzmi „nie mogę się zalogować", zanim jeszcze wiadomo, czy to w ogóle jest blokada, czy zwykła pomyłka w haśle.

Przykład:

```
Name              SamAccountName   LockedOut
----              --------------   ---------
Halina Kowalska   halina.kowalska  True
```

TYLKO ODCZYT

Odblokowanie konta: Unlock-ADAccount

```
Unlock-ADAccount -Identity NazwaUzytkownika
```

Zdejmuje blokadę z konta natychmiast, bez czekania na upływ `LockoutDuration` z polityki. Samo odblokowanie nie usuwa przyczyny, więc jeśli źródło powtarzających się nieudanych prób nie zostanie znalezione, konto zablokuje się ponownie.

Przykład:

```
Unlock-ADAccount -Identity halina.kowalska
```

Z życia wzięte

Z ŻYCIA WZIĘTE

Pani Halina zmienia hasło w piątek przed wyjściem, zgodnie z powiadomieniem o zbliżającym się wygaśnięciu. W poniedziałek rano jej konto jest zablokowane, mimo że za każdym razem wpisuje nowe hasło poprawnie. Powodem jest telefon: aplikacja pocztowa co kilka minut próbuje zalogować się starym, zapamiętanym hasłem, aż licznik nieudanych prób w polityce domeny dobija do progu blokady.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: polityka haseł domeny. Jedna, wspólna polityka (Default Domain Policy) decydująca o długości, złożoności, historii i okresie ważności hasła dla wszystkich kont jednej domeny Active Directory (każda domena w lesie ma własną). GPO podłączone do konkretnej jednostki organizacyjnej może ustawiać własną politykę haseł, ale dla kont domenowych Windows ją ignoruje: to ustawienie stosuje się tylko z polityki podłączonej do korzenia domeny, niezależnie od tego, na jakiej jednostce stoi konto użytkownika. GPO na jednostce organizacyjnej z własną polityką haseł działa jedynie dla lokalnych kont komputerów leżących w tej jednostce, nigdy dla kont domenowych.

Pojęcie: PSO, precyzyjna polityka haseł. Fine-Grained Password Policy, w skrócie PSO od nazwy obiektu w katalogu (Password Settings Object), to sposób na wyjątek od jednej wspólnej polityki domeny, bez GPO. Przypisujemy ją bezpośrednio do wybranych kont albo grup zabezpieczeń, na przykład administratorów albo kont usługowych, którym chcemy narzucić inne wymagania niż reszcie firmy.

> **Pojęcie: blokada konta.** Mechanizm chroniący przed zgadywaniem haseł: po przekroczeniu `LockoutThreshold` nieudanych prób logowania z rzędu, w oknie czasu `LockoutObservationWindow`, konto blokuje się na czas `LockoutDuration`, niezależnie od tego, czy kolejna próba miałaby akurat poprawne hasło.

Skąd biorą się nieudane próby logowania, gdy nikt świadomie nie wpisuje złego hasła

Zablokowane konto nie musi oznaczać ataku ani pomyłki użytkownika przy klawiaturze. Najczęstszym źródłem powtarzających się nieudanych prób jest urządzenie, które w tle wciąż próbuje zalogować się starym, zapamiętanym hasłem, po tym jak użytkownik zmienił je gdzie indziej.



Stare haslo z telefonu wywoluje kolejne nieudane proby logowania, PDC emulator liczy je i zapisuje zdarzenie 4740 (kliknięcie otwiera pełny rozmiar)

Nieudana próba logowania trafia najpierw do dowolnego kontrolera domeny w pobliżu, ale to kontroler pełniący rolę PDC emulator ostatecznie liczy nieudane próby dla danego konta i zapisuje w swoim dzienniku zabezpieczeń zdarzenie o identyfikatorze 4740, razem z nazwą komputera, z którego przyszła próba, w polu Caller Computer Name.

Rozsądne wartości polityki według aktualnych zaleceń

NIST w wytycznych SP 800-63B i najnowsze zalecenia Microsoftu idą w tym samym kierunku: dłuższe hasło, mniej sztywnych reguł.

Ustawienie	Starsze podejście	Aktualne zalecenie	Dlaczego

Minimalna długość	8 znaków	co najmniej 14 znaków	długość chroni skuteczniej niż wymuszona różnorodność znaków
Złożoność (wielkie, małe, cyfry, znaki specjalne)	wymuszona	mniej istotna niż zakaz haseł ze słownika typowych, zgadywalnych haseł	reguły złożoności skłaniają ludzi do przewidywalnych wzorców, na przykład dopisania jednej cyfry na końcu
Okres ważności hasła	wymuszona zmiana co 30 do 90 dni	brak wymuszonej, okresowej zmiany, hasło zmieniamy tylko przy podejrzeniu wycieku	częsta wymuszona zmiana też prowadzi do przewidywalnych wzorców i nie chroni przed niczym, czego nie chroniłoby dłuższe hasło

W Zielonej, gdzie konta domenowe nie mają jeszcze włączonej wieloskładnikowej weryfikacji ani listy zakazanych haseł z Intune, zostawiamy `ComplexityEnabled` włączone jako jedyne wbudowane zabezpieczenie przed najsłabszymi hasłami, ale wydłużamy `MinPasswordLength` do 14 znaków i wyłączamy wymuszone wygasanie hasła, żeby nie zachęcać do haseł w rodzaju `Halina2026`, gdzie zmienia się tylko rok.

Częste błędy

Objaw	Przyczyna	Co robimy
Konto blokuje się co kilka godzin, mimo że użytkownik twierdzi, że nie loguje się nieudanie	urządzenie mobilne albo stara aplikacja w tle próbuje logować się zapamiętanym, starym hasłem	szukamy zdarzenia 4740 na kontrolerze z rolą PDC emulator i sprawdzamy pole Caller Computer Name
GPO z inną polityką haseł podłączone do jednostki organizacyjnej nie zmienia niczego dla kont domenowych	dla kont domenowych liczy się tylko polityka domeny albo PSO, GPO na jednostce organizacyjnej ustawia politykę haseł wyłącznie dla lokalnych kont komputerów	zamiast GPO na OU zakładamy precyzyjną politykę haseł (`New-ADFineGrainedPasswordPolicy`) i przypisujemy ją do właściwej grupy
`Get-ADUserResultantPasswordPolicy` pokazuje inną politykę niż spodziewana	konto należy do kilku grup, z których każda ma przypisaną inną PSO, a wygrywa ta z najniższą wartością `Precedence`	sprawdzamy `Precedence` wszystkich PSO przypisanych do grup danego konta, nie tylko tej, którą ostatnio dodaliśmy
`Unlock-ADAccount` działa, ale konto blokuje się ponownie po kilku minutach	przyczyna powtarzających się nieudanych prób wciąż działa w tle	zamiast odblokowywać w kółko, szukamy źródła przez zdarzenie 4740, zanim odblokujemy konto po raz kolejny

□□ Ćwiczenia

1. Zespół zakłada GPO z inną, surowszą polityką haseł i podłącza je do jednostki organizacyjnej z kontami działu księgowości. Dlaczego po `gpupdate /force` na komputerze księgowej nic się nie zmienia w wymaganiach dla jej hasła?

Odpowiedź

Dla kont domenowych Windows stosuje politykę haseł wyłącznie z GPO podłączonego do korzenia domeny, czyli z Default Domain Policy, albo z precyzyjnej polityki haseł przypisanej bezpośrednio do konta lub jego grupy. GPO podłączone do jednostki organizacyjnej z inną polityką haseł działa tylko dla lokalnych kont komputerów w tej jednostce, nigdy dla kont domenowych, niezależnie od tego, jak dokładnie skonfigurujemy samo GPO.

1. Konto usługowe należy jednocześnie do grupy z PSO o `Precedence 50` i do grupy z PSO o `Precedence 200`. Która polityka faktycznie obowiązuje to konto?

Odpowiedź

Wygrywa polityka z niższą wartością `Precedence`, czyli ta ustawiona na 50. `Get-ADUserResultantPasswordPolicy` uwzględnia to automatycznie i od razu pokazuje wynikową politykę, zamiast zmuszać do ręcznego porównywania wartości `Precedence` wszystkich PSO przypisanych do grup danego konta.

1. Dlaczego zdarzenie 4740 dla zablokowanego konta szukamy na kontrolerze z rolą PDC emulator, a nie na dowolnym z kontrolerów domeny, do którego akurat mamy pod ręką dostęp?

Odpowiedź

Nieudana próba logowania może trafić do dowolnego kontrolera domeny w pobliżu użytkownika czy urządzenia, ale to kontroler z rolą PDC emulator ostatecznie liczy nieudane próby dla danego konta i to on zapisuje zdarzenie 4740 w swoim dzienniku zabezpieczeń w momencie przekroczenia progu blokady. Szukanie tego zdarzenia na innym kontrolerze może nic nie znaleźć, mimo że blokada naprawdę wystąpiła.

Powiązane: GPO od środka: tworzenie, łączenie, kolejność i diagnostyka · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt · DHCP: adresy dla biura i magazynu z przełączaniem awaryjnym · Windows LAPS: hasło lokalnego administratora w Active

Directory

Źródła: Get-ADDefaultDomainPasswordPolicy · Set-ADDefaultDomainPasswordPolicy · New-ADFineGrainedPasswordPolicy · Add-ADFineGrainedPasswordPolicySubject · Get-ADUserResultantPasswordPolicy · Search-ADAccount · Unlock-ADAccount · NIST SP 800-63B, Digital Identity Guidelines · Microsoft Learn, Password policy recommendations · Account Lockout Event ID, znajdowanie źródła blokad

---

Revision #29
Created 2026-09-28 09:24:35 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:44 UTC by Tomasz Konieczny