BitLocker z kluczem odzyskiwania w Active Directory

Poziom: średniozaawansowany
Dotyczy: BitLocker, Windows 10/11, Active Directory na dc01/dc02 **Czas: ~30 min**

BitLocker szyfruje dysk, ale klucz odzyskiwania musi gdzieś trafić, zanim zapomnimy go razem z dyskiem. Konfigurujemy politykę wymuszającą kopię do Active Directory, uczymy się jednego błędu, który potrafi to po cichu zablokować, i sprzątamy po latach zbierania się duplikatów w katalogu.

> Komputery zarządzane z Intune mogą zapisywać klucz odzyskiwania w Microsoft Entra ID, a przejście z kopii w Active Directory i zasady unikania podwójnego zarządzania opisuje strona BitLocker z Intune: ciche szyfrowanie i klucze odzyskiwania w Entra ID.

Skróty użyte na tej stronie (7)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
ADMX	format plików szablonów administracyjnych GPO, następca starszego formatu ADM
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
GUID	Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera
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
RMM	Remote Monitoring and Management: platforma do zdalnego zarządzania i monitorowania stacji roboczych

Fiszka

□□ TYLKO ODCZYT

Wymuszenie kopii klucza do Active Directory przed szyfrowaniem

```
Konfiguracja komputera → Szablony administracyjne → Składniki systemu Windows →
Szyfrowanie dysków funkcją BitLocker → Dyski systemu operacyjnego →
„Wybierz metodę odzyskiwania dysków systemu operacyjnego chronionych przez BitLocker"
→ Włączone
→ zaznaczone: „Nie włączaj funkcji BitLocker, dopóki informacje odzyskiwania nie zostaną
   zapisane w usłudze AD DS dla dysków systemu operacyjnego"
```

Ta sama polityka istnieje osobno dla dysków stałych innych niż systemowy (`Dyski danych stałych`) i dla dysków wymiennych. Zaznaczenie „Nie włączaj funkcji BitLocker, dopóki..." jest tym, co faktycznie wymusza kopię: bez tej opcji polityka tylko pozwala na zapis do katalogu, ale nie blokuje szyfrowania bez niego.

□□ TYLKO ODCZYT

Odświeżenie polityk przed kopią klucza

```
gpupdate /force /target:computer
```

Wymuszamy odświeżenie polityk komputera zaraz przed próbą kopii klucza, żeby mieć pewność, że urządzenie już wie o włączonej polityce zapisu do AD, zanim zaczniemy szukać przyczyny nieudanej kopii gdzie indziej.

□□ **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **gpupdate** = group policy update: wymuś odświeżenie GPO

□□ TYLKO ODCZYT

Kopia klucza z komputera, na którym BitLocker już działa

```
manage-bde -protectors -adbackup C: -id "{NumerGuidProtektora}"
```

Numer GUID protektora hasła odzyskiwania sprawdzamy wcześniej poleceniem `manage-bde -protectors -get C:`. Tego polecenia używamy, gdy dysk był szyfrowany zanim polityka

wymuszająca kopię w ogóle istniała, i chcemy dogonić zaległość bez odszyfrowywania dysku.

GUID = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera · **manage-bde** = BitLocker Drive Encryption: zarządzanie szyfrowaniem dysków

TYLKO ODCZYT

To samo z poziomu PowerShella

```
Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId "{NumerGuidProtektora}"
```

Ten sam efekt co `manage-bde -adbackup`, wygodniejszy w skrypcie, bo nie wymaga parsowania tekstowego wyniku `manage-bde`. `BackupToAAD-BitLockerKeyProtector` wygląda podobnie, ale zapisuje protektor do Microsoft Entra ID, nie do Active Directory on premises: te dwa polecenia mylą się łatwo po samej nazwie, a używamy zupełnie innego z nich w zależności od tego, gdzie komputer jest zarządzany.

> Odczyt zapisanego klucza z katalogu opisaliśmy już na stronie Skrypty audytowe Active Directory, fiszka „Pobieranie klucza BitLocker z AD". Tu skupiamy się na tym, co potrafi ten zapis zablokować, i na porządkach po latach działania.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

Z życia wzięte

Z ŻYCIA WZIĘTE

Laptop Kasi pada w hotelu w środę wieczorem, tydzień przed targami. Nowy laptop startuje w tryb odzyskiwania BitLockera i prosi o klucz, którego Kasia oczywiście nie zna na pamięć. Tomek otwiera Active Directory Users and Computers, szuka konta komputera i nie znajduje żadnego obiektu z kluczem: polityka wymuszająca kopię do katalogu weszła w życie dopiero miesiąc po tym, jak dysk Kasi już był zaszyfrowany.

Jak to działa

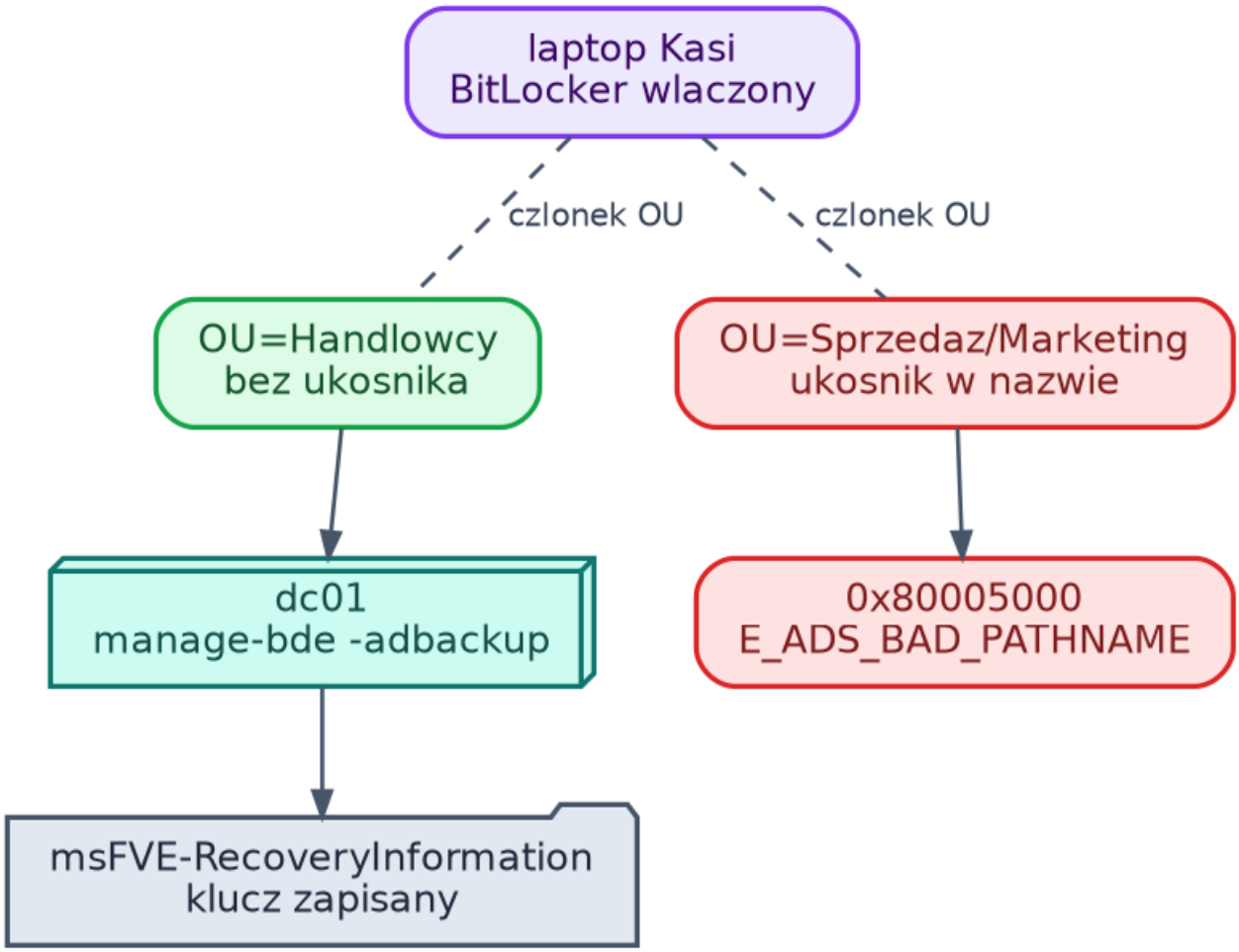
Rozwiń: jak to działa pod spodem

> **Pojęcie: msFVE-RecoveryInformation.** Obiekt potomny konta komputera w Active Directory, w którym BitLocker zapisuje hasło odzyskiwania. Jeden komputer może mieć ich kilka, po jednym na każdy cykl szyfrowania i odszyfrowania w swojej historii; dokładnie opisaliśmy to pojęcie na stronie Skrypty audytowe Active Directory.

> **Pojęcie: ADsPath.** Wewnętrzna, tekstowa ścieżka, którą Windows buduje z `DistinguishedName` obiektu w katalogu, żeby dostać się do niego przez interfejs ADSI (`Active Directory Service Interfaces`). `manage-bde -adbackup` buduje taką ścieżkę z lokalizacji konta komputera, żeby wiedzieć, gdzie w katalogu dopisać nowy obiekt `msFVE-RecoveryInformation`.

Błąd, na który trafiamy najczęściej, ma swój własny kod i swoją własną, dość nieoczywistą przyczynę.

> ⚠ Kopia klucza kończy się błędem `0x80005000` (`E_ADS_BAD_PATHNAME`, czyli „nieprawidłowa ścieżka ADSI"), gdy komputer stoi w jednostce organizacyjnej, której nazwa zawiera ukośnik (`/`). `manage-bde` buduje `ADsPath` z `DistinguishedName` komputera, a ukośnik w nazwie jednostki organizacyjnej rozjeżdża tę ścieżkę w sposób, którego interfejs ADSI nie potrafi już poprawnie odczytać. W Zielonej problem dotyczy jednostki `OU=Sprzedaż/Marketing,OU=Komputery,DC=ad,DC=zielona,DC=example`, założonej dawno temu na wzór nazwy działu w firmowym systemie kadrowym.



Komputer w OU bez ukosnika zapisuje klucz poprawnie, ten sam zapis z OU z ukosnikiem konczy sie bledem 0x80005000 (kliknięcie otwiera pełny rozmiar)

Naprawa polega na zmianie nazwy jednostki organizacyjnej na taką bez ukośnika:

```
Rename-ADObject -Identity "OU=Sprzedaż/Marketing,OU=Komputery,DC=ad,DC=zielona,DC=example"
-NewName "Sprzedaz i Marketing"
```

Zmiana nazwy zachowuje powiązania GPO i wszystkie nadane uprawnienia, bo obiekt jednostki organizacyjnej fizycznie zostaje ten sam, zmienia się tylko jego atrybut `name` i w efekcie `DistinguishedName`. Trzeba jednak poprawić wszystko, co wcześniej odwoływało się do starego, pełnego `DistinguishedName`: zapytania `-Identity` z tej i z poprzedniej strony o Windows LAPS, `-SearchBase` w istniejących skryptach audytowych, oraz reguły kierujące polityki w RMM, jeśli filtrują komputery po ścieżce jednostki organizacyjnej zamiast po samej nazwie.

Porządki z duplikatami po latach działania

Każdy cykl szyfrowania i odszyfrowania dopisuje nowy obiekt `msFVE-RecoveryInformation`, a stare nie znikają same. Po latach niektóre komputery mają po kilkanaście takich obiektów, z których żywy jest tylko ten najnowszy. Zasada porządków: dla każdego komputera zostawiamy najnowszy obiekt (po `whenCreated`), a starsze usuwamy, zawsze najpierw oglądając, co konkretnie usuniemy.

Szkic zapytania do podglądu duplikatów w jednej jednostce organizacyjnej:

```
Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} `
    -SearchBase "OU=Komputery,DC=ad,DC=zielona,DC=example" `
    -Properties whenCreated |
    Group-Object { ($_.DistinguishedName -split ',', 2)[1] } |
    Where-Object Count -gt 1 |
    ForEach-Object {
        $_.Group | Sort-Object whenCreated -Descending | Select-Object -Skip 1
    }
```

Grupujemy obiekty po fragmencie `DistinguishedName` wskazującym konto komputera nadrzędnego, zostawiamy w wyniku wszystko poza najnowszym obiektem w każdej grupie, i dopiero ten wynik oglądamy, zanim cokolwiek usuniemy.

```
$doUsuniecia | Remove-ADObject -WhatIf
```

`-WhatIf` pokazuje, co polecenie by zrobiło, bez faktycznego usunięcia. Dopiero po spokojnym przejrzeniu tej listy zdejmujemy `-WhatIf` i usuwamy naprawdę, jednostka po jednostce, nigdy jednym zamachem na cały katalog.

Częste błędy

Objaw	Przyczyna	Co robimy
`manage-bde -adbackup` kończy się `0x80005000`	komputer stoi w jednostce organizacyjnej z ukośnikiem w nazwie	zmieniamy nazwę jednostki `Rename-ADObject`, potem poprawiamy wszystkie zapytania i reguły odwołujące się do starego `DistinguishedName`

Objaw	Przyczyna	Co robimy
`Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'}` zwraca puste wyniki dla komputera z aktywnym BitLockerem	polityka wymuszająca kopię nie była włączona w chwili szyfrowania tego dysku	włączamy politykę z fiszki wyżej, potem uruchamiamy `manage-bde -adbackup` albo `Backup-BitLockerKeyProtector` ręcznie na tym komputerze
Klucz w AD jest, ale nie pasuje do żadnego z kluczy, o które prosi ekran odzyskiwania	w katalogu leży kilka starych obiektów `msFVE-RecoveryInformation`, a odczytaliśmy nie ten, co trzeba	sortujemy wynik po `whenCreated` malejąco i bierzemy najnowszy obiekt, tak jak w skrypcie z tej strony i na stronie o audycie AD
Po zmianie nazwy jednostki organizacyjnej skrypt audytowy przestaje znajdować komputery	skrypt miał na sztywno wpisany stary `DistinguishedName` w `-SearchBase`	aktualizujemy `-SearchBase` na nowy `DistinguishedName`, dokładnie tak jak przy regułach RMM

□□ Ćwiczenia

1. Dlaczego zmiana nazwy jednostki organizacyjnej z ukośnikiem naprawia błąd `0x80005000`, a nie tylko go maskuje?

Odpowiedź

Przyczyną błędu jest sam znak ukośnika w `DistinguishedName` jednostki organizacyjnej: `manage-bde` buduje z tego `DistinguishedName` ścieżkę `ADsPath`, a interfejs ADSI odczytuje ukośnik jako część własnej składni ścieżki, nie jako zwykły znak w nazwie. Usunięcie ukośnika z nazwy usuwa problem u źródła, zamiast obchodzić go inną metodą zapisu klucza.

1. Skrypt porządkujący duplikaty `msFVE-RecoveryInformation` z tej strony grupuje obiekty po fragmencie `DistinguishedName` rodzica. Co się stanie, jeśli uruchomimy go z `-SearchBase` ustawionym na cały katalog zamiast na jedną jednostkę organizacyjną, i dlaczego mimo to zaczynamy zawsze od małego zakresu?

Odpowiedź

Zapytanie technicznie zadziała na całym katalogu tak samo poprawnie, ale wynik do przejrzenia urośnie do wszystkich komputerów w firmie naraz, co przy pierwszym uruchomieniu utrudnia sprawdzenie, czy grupowanie i sortowanie faktycznie wybrały właściwe obiekty do zachowania. Zaczynamy od jednej, znanej jednostki organizacyjnej, żeby ręcznie zweryfikować kilka wyników, zanim zaufamy temu samemu zapytaniu na całym katalogu.

Powiązane: Skrypty audytowe Active Directory · Windows LAPS: hasło lokalnego administratora w Active Directory

Źródła: Microsoft Learn, „BitLocker recovery overview" · Microsoft Learn, „Choose how BitLocker-protected operating system drives can be recovered" (ADMX) · `Get-Help Backup-BitLockerKeyProtector` · `Get-Help manage-bde-protectors`

Revision #30
Created 2026-09-28 06:15:00 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:47 UTC by Tomasz Konieczny