Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM

Poziom: zaawansowany

Dotyczy: Active Directory Domain Services, Windows Server Backup, restic 0.19.1, rest-server na bkp01, dc01, dc02, dc03 (propozycja), ntdsutil, Windows LAPS

Czas: ~60 min

Kopia kontrolera domeny różni się od kopii zwykłego serwera: baza katalogu jest otwarta i replikowana, a stara kopia przywrócona bez zastanowienia potrafi zepsuć więcej, niż naprawi. Ta strona opisuje, jak robimy kopię stanu systemu na kontrolerach i wysyłamy ją restic na `bkp01`, oraz cztery drogi odtwarzania: kosz AD, odtworzenie nieautorytatywne, autorytatywne i odtworzenie całego lasu. Wracamy tu po każdym „ktoś usunął konto” i przy corocznym teście odtwarzania.

Skróty użyte na tej stronie (12)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
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
FSMO	Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz
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
REST	sposób budowania API przez zwykłe żądania HTTP (GET, POST) zamiast osobnego protokołu
RID	Relative Identifier: końcowa, unikalna w domenie część identyfikatora bezpieczeństwa (SID) każdego konta; RID Master to kontroler domeny rozdzielający pule tych numerów
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
SYSVOL	system volume: udział sieciowy na kontrolerze domeny z politykami GPO i skryptami logowania, replikowany między kontrolerami tak jak reszta katalogu

Skrót	Co znaczy
UTC	Coordinated Universal Time: uniwersalny czas bez strefy, punkt odniesienia dla wszystkich stref czasowych na świecie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
VSS	Volume Shadow Copy Service: mechanizm Windows do tworzenia spójnych migawek danych mimo działających w tle usług, wykorzystywany też przy kopiach zapasowych kontrolera domeny

Zanim zaczniemy

> **Z ŻYCIA WZIĘTE**
>
> Czwartek, 15:20. Tomek porządkuje jednostkę `Wylaczone` i zaznacza myszką o jedną jednostkę za dużo: znika `OU=Magazyn,OU=Uzytkownicy` z 46 kontami zmiany porannej. Ochrona przed przypadkowym usunięciem była na niej wyłączona od zeszłotygodniowej przeprowadzki kont. Na szczęście kosz AD jest włączony, więc o 15:35 konta wracają z grupami i hasłami, a Marek nie dowiaduje się o niczym. Wieczorem Tomek pyta, co by było bez kosza. Odpowiedź zajmuje resztę tej strony.

Strategia kopii całej firmy, poziomy retencji i serwery kopii są opisane w książce o kopiach: Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje i Serwery kopii bkp01 i bkp02: restic, kopia krzyżowa i niezmienność. Tu zajmujemy się tylko tym, co jest specyficzne dla Active Directory.

Wymaganie	Uwaga
osobny wolumen na kopię na każdym kontrolerze	u nas dysk `E:` o wielkości około dwukrotności stanu systemu; nie dysk `C:`
rola Windows Server Backup	instalacja w pierwszej fiszce przebiegu
restic dla Windows	plik `C:\Program Files\restic\restic.exe`, ta sama wersja co na serwerach linuksowych
konto REST `ad` na `bkp01` i repozytorium `ad`	zakładamy według strony o serwerach kopii (`htpasswd -B`, ścieżka `/ad`)
hasło repozytorium i hasło konta REST	w plikach dostępnych tylko dla SYSTEM i Administrators, kopia w Vaultwardenie i w kopercie w sejfie
hasło DSRM każdego kontrolera	w Vaultwardenie i w sejfie; bez niego odtwarzanie stanu systemu się nie zacznie

> Kopia stanu systemu kontrolera zawiera całą bazę katalogu, z hasłami wszystkich kont w postaci, z której napastnik potrafi korzystać. Dlatego repozytorium `ad`, serwer `bkp01` i hasła do nich należą do tej samej warstwy co kontrolery (warstwa 0 na stronie o hartowaniu). Kto ma dostęp do kopii AD, ma w praktyce domenę.

Przebieg

Komendy wykonujemy w PowerShellu uruchomionym jako administrator na kontrolerze, chyba że opis mówi inaczej.

Instalacja Windows Server Backup: Install-WindowsFeature

```
Install-WindowsFeature Windows-Server-Backup
```

Rola daje polecenie `wbadmin` i przystawkę Windows Server Backup. Instalujemy na każdym kontrolerze.

Kopia stanu systemu: wbadmin start systemstatebackup

```
wbadmin start systemstatebackup -backupTarget:LiteraWolumenu -quiet
```

> (gdzie `LiteraWolumenu` to dysk przeznaczony na kopie, u nas `E:`)

Stan systemu kontrolera to baza katalogu `ntds.dit` z dziennikami, udział SYSVOL, rejestr, pliki rozruchowe i baza rejestracji COM+. Polecenie korzysta z VSS, więc kopia jest spójna mimo działającej usługi katalogu. Opis parametrów jest też na stronie o pierwszym kontrolerze.

Przykład zakończenia:

```
Summary of the backup operation:
------------------
The backup of the system state successfully completed [19.10.2026 01:14].
```

```
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-19-10-2026_01-00-03.log
```

Lista wersji kopii: wbadmin get versions

```
wbadmin get versions -backupTarget:E:
```

Przykład:

```
Backup time: 18.10.2026 01:00
Backup target: Fixed Disk labeled E:
Version identifier: 10/18/2026-23:00
Can recover: Application(s), System State

Backup time: 19.10.2026 01:00
Backup target: Fixed Disk labeled E:
Version identifier: 10/19/2026-23:00
Can recover: Application(s), System State
```

Identyfikator wersji jest zapisany w czasie UTC i w formacie amerykańskim (miesiąc, dzień, rok), dlatego kopia z 1:00 polskiego czasu ma identyfikator z 23:00 dnia poprzedniego. Ten identyfikator podajemy przy odtwarzaniu.

Usunięcie starszych wersji z wolumenu: wbadmin delete systemstatebackup

```
wbadmin delete systemstatebackup -backupTarget:E: -keepVersions:3 -quiet
```

Na dysku `E:` trzymamy trzy ostatnie wersje, a resztę historii daje repozytorium restic na `bkp01`. Bez tego wolumen zapełni się po kilku tygodniach.

Skrypt nocnej kopii z wysyłką do bkp01: kopia-ad-restic.ps1

```
# Kopia stanu systemu kontrolera domeny i kopia GPO, wysylane restic na bkp01.
# Uruchamia zadanie zaplanowane jako SYSTEM, codziennie o 01:00 (dc01), 01:10 (dc02), 01:20
```

```
(dc03).
$ErrorActionPreference = 'Stop'
$Cel      = 'E:'
$KatGpo   = 'E:\GPO\' + (Get-Date -Format 'yyyy-MM-dd')
$Restic   = 'C:\Program Files\restic\restic.exe'
$Log      = 'C:\Skrypty\logi\kopia-ad.log'

function Zapisz($tekst) {
    Add-Content -Path $Log -Value ("{0} {1}" -f (Get-Date -Format 's'), $tekst)
}

try {
    Zapisz 'start kopii stanu systemu'
    wbadmin start systemstatebackup -backupTarget:$Cel -quiet | Out-Null
    if ($LASTEXITCODE -ne 0) { throw "wbadmin zakonczyl sie kodem $LASTEXITCODE" }
    wbadmin delete systemstatebackup -backupTarget:$Cel -keepVersions:3 -quiet | Out-Null

    Zapisz 'kopia GPO'
    New-Item -ItemType Directory -Path $KatGpo -Force | Out-Null
    Backup-GPO -All -Path $KatGpo | Out-Null
    Get-ChildItem 'E:\GPO' -Directory |
        Where-Object LastWriteTime -lt (Get-Date).AddDays(-14) |
        Remove-Item -Recurse -Force

    Zapisz 'wysylka restic do bkp01'
    $env:RESTIC_REPOSITORY    = 'rest:https://bkp01.ad.zielona.example:8000/ad'
    $env:RESTIC_REST_USERNAME = 'ad'
    $env:RESTIC_REST_PASSWORD = (Get-Content 'C:\Skrypty\restic\rest-haslo.txt' -Raw).Trim()
    $env:RESTIC_PASSWORD_FILE = 'C:\Skrypty\restic\restic-haslo.txt'
    & $Restic backup "$Cel\WindowsImageBackup" $KatGpo --host $env:COMPUTERNAME --tag ad --tag
$env:COMPUTERNAME
    if ($LASTEXITCODE -ne 0) { throw "restic zakonczyl sie kodem $LASTEXITCODE" }
    Zapisz 'koniec, sukces'
}
catch {
    Zapisz ("BLAD: " + $_.Exception.Message)
    exit 1
}
```

Plik zapisujemy jako `C:\Skrypty\kopia-ad-restic.ps1` na każdym kontrolerze. Kopię GPO robi każdy kontroler, bo GPO są wspólne, ale dzięki temu kopia jest także wtedy, gdy jeden kontroler leży; repozytorium i tak przechowuje tylko zmienione bloki. Retencję robi `bkp01`, bo konto REST jest w trybie tylko do dopisywania i `forget` z kontrolera zostałby odrzucony.

Zadanie zaplanowane dla skryptu: Register-ScheduledTask

```
$Akcja    = New-ScheduledTaskAction -Execute 'powershell.exe' -Argument '-NoProfile -
ExecutionPolicy Bypass -File C:\Skrypty\kopia-ad-restic.ps1'
$Wyzwal   = New-ScheduledTaskTrigger -Daily -At GodzinaStartu
$Konto    = New-ScheduledTaskPrincipal -UserId 'SYSTEM' -LogonType ServiceAccount -RunLevel
Highest
Register-ScheduledTask -TaskName 'Kopia AD do bkp01' -Action $Akcja -Trigger $Wyzwal -
Principal $Konto
```

> (gdzie `GodzinaStartu` to `01:00` na `dc01`, `01:10` na `dc02` i `01:20` na `dc03`, żeby kontrolery nie robiły migawek naraz)

Godziny mieszczą się w harmonogramie nocy z książki o kopiach: po kopiach baz o 00:30 i przed katalogiem Swarm o 02:15. Wynik zadania (kod 0 albo 1) odczytuje Zabbix, a brak wpisu „koniec, sukces” w logu z danej nocy daje alarm.

Sprawdzenie migawek w repozytorium: restic snapshots

```
& 'C:\Program Files\restic\restic.exe' snapshots --tag ad
```

Przykład:

```
ID        Time                 Host  Tags          Paths
----------------------------------------------------------------------------
3f9a2c17  2026-10-19 01:14:52  DC01  ad,DC01       E:\GPO\2026-10-19, E:\WindowsImageBackup
8b04d6e1  2026-10-19 01:24:10  DC02  ad,DC02       E:\GPO\2026-10-19, E:\WindowsImageBackup
```

Włączenie kosza AD: Enable-ADOptionalFeature

```
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -
Target 'NazwaLasu'
```

Kosz AD wymaga poziomu lasu co najmniej Windows Server 2008 R2 (mamy 2016) i, tak jak Privileged Access Management, nie da się go wyłączyć. Najpierw sprawdzamy, czy nie jest już włączony:

```
Get-ADOptionalFeature -Filter "Name -eq 'Recycle Bin Feature'" | Select-Object Name,
EnabledScopes
```

Pusta kolumna `EnabledScopes` oznacza, że kosz jest wyłączony. Obiekty usunięte przed włączeniem kosza nie dają się z niego przywrócić.

Odszukanie usuniętego obiektu w koszu: Get-ADObject -IncludeDeletedObjects

```
Get-ADObject -Filter 'isDeleted -eq $true -and Name -like "*NazwaFragment*"' -
IncludeDeletedObjects -Properties whenChanged, lastKnownParent
```

Przykład:

```
Deleted           : True
DistinguishedName : CN=Jan Nowak\0ADEL:0f3c8f1e-6a41-4d1b-9a0e-2b7c1d5e8f90,CN=Deleted
Objects,DC=ad,DC=zielona,DC=example
LastKnownParent   : OU=Magazyn,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
Name              : Jan Nowak
DEL:0f3c8f1e-6a41-4d1b-9a0e-2b7c1d5e8f90
ObjectClass       : user
WhenChanged       : 16.10.2026 15:21:07
```

Przywrócenie obiektu z kosza: Restore-ADObject

```
Get-ADObject -Filter 'isDeleted -eq $true -and Name -like "*NazwaFragment*"' -
IncludeDeletedObjects | Restore-ADObject
```

Obiekt wraca z identyfikatorem SID, członkostwem w grupach i hasłem. Przy całej jednostce organizacyjnej najpierw przywracamy samą jednostkę, potem obiekty, które w niej były (filtr po `lastKnownParent`), bo obiekt nie wróci do rodzica, którego jeszcze nie ma.

Przykład dla jednostki i jej zawartości:

```
Get-ADObject -Filter 'isDeleted -eq $true -and Name -like "Magazyn*" -and ObjectClass -eq
"organizationalUnit"' -IncludeDeletedObjects | Restore-ADObject
Get-ADObject -Filter 'isDeleted -eq $true -and lastKnownParent -eq
"OU=Magazyn,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example"' -IncludeDeletedObjects | Restore-
ADObject
```

Start kontrolera w trybie DSRM: bcdedit /set safeboot dsrepair

```
bcdedit /set "{default}" safeboot dsrepair
Restart-Computer
```

Po restarcie kontroler wstaje bez usługi katalogu. Logujemy się kontem `.\Administrator` z hasłem DSRM tego kontrolera. Po zakończeniu pracy zawsze wracamy do zwykłego startu:

```
bcdedit /deletevalue "{default}" safeboot
Restart-Computer
```

Na Windows Server od 2008 alternatywą dla pojedynczego odtwarzania bez restartu jest zatrzymanie usługi `NTDS` (`Stop-Service NTDS -Force`), ale odtwarzanie stanu systemu `wbadmin` wymaga trybu DSRM.

Odtworzenie stanu systemu w DSRM: wbadmin start systemstaterecovery

```
wbadmin start systemstaterecovery -version:IdentyfikatorWersji -backupTarget:E: -quiet
```

> (gdzie `IdentyfikatorWersji` to wartość z `wbadmin get versions`, np. `10/19/2026-23:00`)

To jest odtworzenie nieautorytatywne: kontroler wraca do stanu z kopii, a po zwykłym restarcie pobiera od partnerów wszystko, co zmieniło się od tamtej pory. Gdy pliki kopii są tylko na `bkp01`, najpierw pobieramy je restic na dysk `E:` (`restic restore` z identyfikatorem migawki i `--target E:\`), a dopiero potem uruchamiamy `wbadmin`. Gdy odtwarzamy jedyny działający kontroler i SYSVOL ma wrócić jako wersja wzorcowa, dokładamy przełącznik `-authsysvol`.

Oznaczenie obiektów jako autorytatywnych: ntdsutil authoritative restore

```
ntdsutil
activate instance ntds
authoritative restore
restore subtree "OU=NazwaJednostki,OU=NazwaRodzica,DC=ad,DC=zielona,DC=example"
quit
quit
```

Wykonujemy w DSRM, po odtworzeniu nieautorytatywnym, a przed restartem do zwykłego trybu. Polecenie podnosi numery wersji wskazanych obiektów tak bardzo, że po restarcie to ich stan rozejdzie się na pozostałe kontrolery, zamiast zostać nadpisanym informacją o usunięciu. Pojedynczy obiekt wskazujemy poleceniem `restore object` zamiast `restore subtree`. `ntdsutil` zapisuje w bieżącym katalogu pliki z członkostwem w grupach, które po restarcie importujemy poleceniem `ldifde -i -f NazwaPliku.ldf`, bo samo odtworzenie użytkownika nie przywraca jego obecności w grupach z innych jednostek.

Zmiana hasła DSRM: ntdsutil set dsrm password

```
ntdsutil
set dsrm password
reset password on server null
quit
quit
```

`null` oznacza kontroler, na którym pracujemy; w miejsce `null` można podać nazwę innego kontrolera. Hasło DSRM zmieniamy po odejściu każdej osoby, która je znała, i po każdym użyciu w awarii.

Weryfikacja

1. Następnego dnia rano sprawdzamy w logu `C:\Skrypty\logi\kopia-ad.log` wpis „koniec, sukces” i w `restic snapshots --tag ad` migawki wszystkich kontrolerów.
2. Raz na kwartał robimy test w laboratorium: pobieramy z `bkp01` migawkę `dc02`, odtwarzamy ją w izolowanej sieci na maszynie bez połączenia z produkcją i sprawdzamy, że katalog wstaje w DSRM i po restarcie. Wynik zapisujemy według strony Testy odtwarzania: plik, maszyna, baza i cała lokalizacja.
3. Raz w miesiącu przywracamy z kosza testowe konto `test.kosz`, które dzień wcześniej usunęliśmy.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: konsola Windows Server Backup na `dc01` po nocnej kopii, widoczna lista wersji na dysku `E:` z trzema ostatnimi kopiami stanu systemu i statusem Successful.

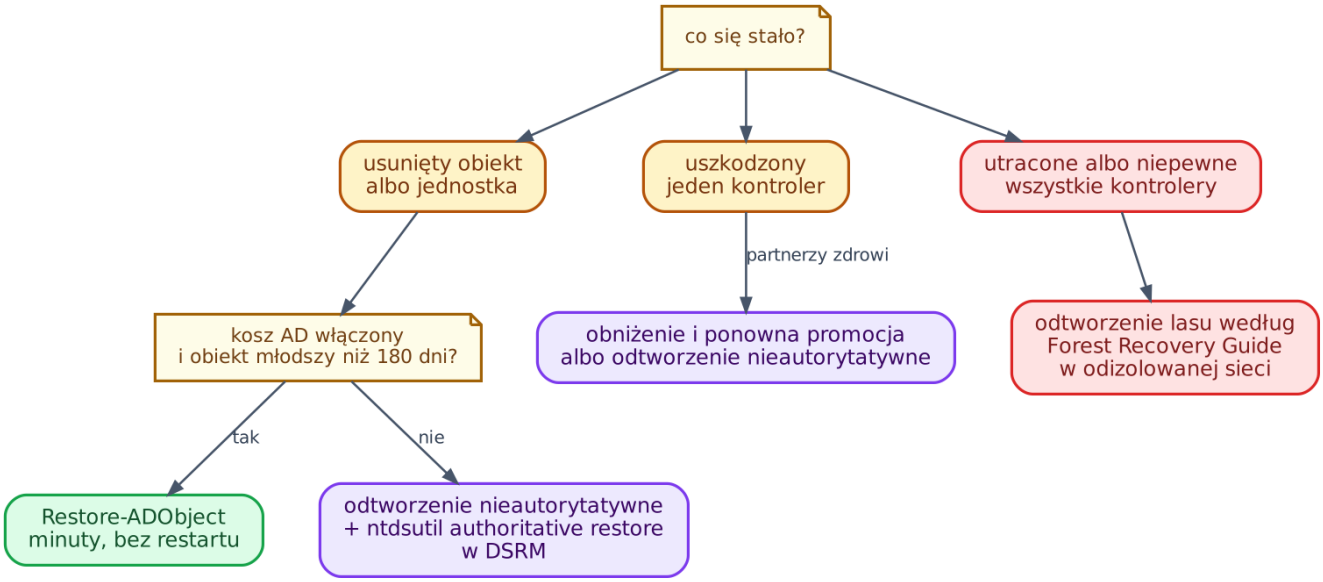
Wycofanie zmian

Kopia sama w sobie nic nie zmienia, więc wycofanie dotyczy tylko zadania i plików: wyłączamy zadanie `Kopia AD do bkp01`, a wolumen `E:` czyścimy poleceniem `wbadmin delete systemstatebackup`. Kosza AD i odtworzenia autorytatywnego wycofać się nie da: kosz zostaje włączony na zawsze, a obiekt przywrócony autorytatywnie usuwamy ponownie, jeśli wrócił przez pomyłkę.

Jak to działa

◫ Rozwiń: jak to działa pod spodem

Cztery drogi odtwarzania



Rysunek 1. Drzewo decyzji odtwarzania AD: usunięty obiekt z koszem to Restore-ADObject, bez kosza to odtworzenie autorytatywne, uszkodzony jeden kontroler to ponowna promocja albo odtworzenie nieautorytatywne, utrata wszystkich kontrolerów to odtworzenie lasu (kliknięcie otwiera pełny rozmiar)

Co się stało	Droga	Ile to trwa w Zielonej	Czego potrzebujemy
usunięty obiekt albo jednostka, kosz włączony	`Restore-ADObject`	minuty	kosz AD, obiekt młodszy niż 180 dni
usunięty obiekt, kosz wyłączony albo obiekt starszy	odtworzenie nieautorytatywne i autorytatywne na jednym kontrolerze	godzina do dwóch, z restartami	kopia stanu systemu młodsza niż czas życia nagrobka, hasło DSRM
uszkodzona baza jednego kontrolera, reszta zdrowa	obniżenie i ponowna promocja albo odtworzenie nieautorytatywne	godzina	zdrowi partnerzy; kopia nie zawsze potrzebna
zła zmiana w GPO	`Restore-GPO` z kopii	minuty	katalog `E:\GPO` albo migawka restic
wszystkie kontrolery utracone (pożar klastra, atak szyfrujący)	odtworzenie lasu	dzień i dłużej	kopia, której jesteśmy pewni, że jest sprzed włamania, i plan w sejfie

Pojęcie: odtworzenie nieautorytatywne. Kontroler wraca do stanu z kopii jako jeden z wielu: po starcie przyjmuje od partnerów wszystkie nowsze zmiany. Dobre, gdy problem dotyczy samego kontrolera, a nie danych.

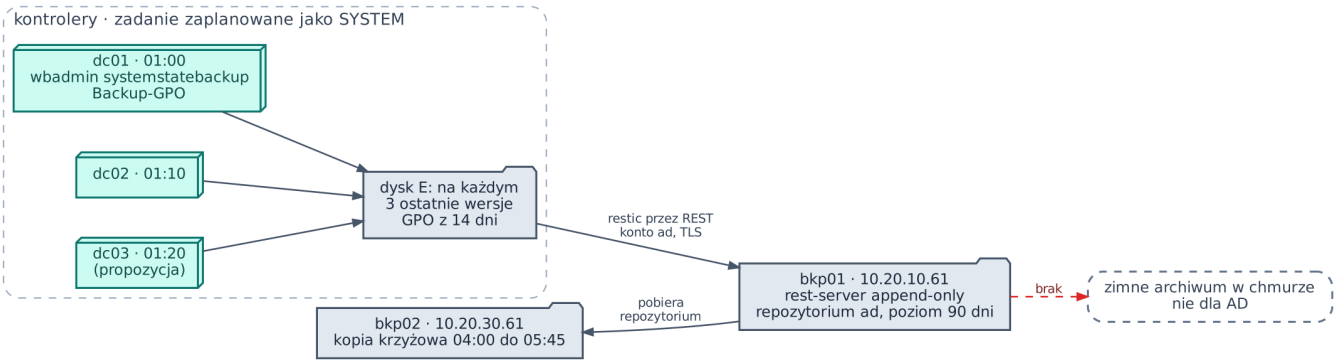
Pojęcie: odtworzenie autorytatywne. Odtworzenie nieautorytatywne plus oznaczenie wybranych obiektów jako ważniejszych niż to, co mają partnerzy. Bez tego partnerzy po restarcie odesłaliby informację, że obiekt jest usunięty, i obiekt zniknąłby ponownie.

Pojęcie: czas życia nagrobka (tombstone lifetime). Czas, przez który katalog pamięta usunięty obiekt, żeby informacja o usunięciu zdążyła dotrzeć do wszystkich kontrolerów. W lasach założonych na nowszych systemach wynosi 180 dni. Kopia starsza niż ten czas nie nadaje się do odtwarzania kontrolera, bo przywróciłaby obiekty, o których usunięciu reszta lasu już zapomniała.

Pojęcie: kosz AD (Active Directory Recycle Bin). Funkcja lasu, dostępna od Windows Server 2008 R2, dzięki której usunięty obiekt przez czas życia obiektu usuniętego (domyślnie tyle samo co czas życia nagrobka) zachowuje wszystkie atrybuty, w tym członkostwo w grupach. Przywrócenie nie wymaga kopii ani restartu.

Kopia w Zielonej

Kopie płyną tak samo jak reszta kopii firmy: kontroler zapisuje lokalnie, wysyła restic do `bkp01` w trybie tylko do dopisywania, a `bkp02` pobiera repozytorium w nocnej kopii krzyżowej.



Rysunek 2. Przepływ kopii AD: dc01, dc02 i dc03 robią o 1:00 kopię stanu systemu i GPO na dysk E:, wysyłają ją restic przez REST do repozytorium ad na bkp01, a bkp02 pobiera je w kopii krzyżowej; do chmury paczki AD nie idą (kliknięcie otwiera pełny rozmiar)

Proponujemy osobne repozytorium `ad` z poziomem retencji 90 dni: dzienne kopie z 7 dni i tygodniowe przez 90 dni, bez paczek w zimnym archiwum. Uzasadnienie:

- Kopia kontrolera starsza niż 180 dni nie nadaje się do odtwarzania, więc poziomy 180 dni i wyższe nie dają nic poza kosztem.
- Do usuniętych obiektów z ostatnich 180 dni mamy kosz AD, a do kopii sprzed tygodnia czy miesiąca wystarczy poziom 90 dni.
- Repozytorium zawiera skróty haseł wszystkich kont, więc im mniej kopii w mniej miejscach, tym mniej do pilnowania; z tego powodu nie wysyłamy jej też do chmury.

Do zatwierdzenia przez autora: wpis `[ad]=90` w pliku `/etc/restic/poziomy.sh` na `bkp01` i `bkp02`, konto REST `ad` i nowy wiersz w harmonogramie nocy (01:00 do 01:30, kopia AD). Kopia maszyn Hyper-V (repozytorium `maszyny`, 30 dni) obejmuje `dc01` i `dc02` jako całe maszyny i jest uzupełnieniem, a nie zastępstwem: maszynę kontrolera odtwarzamy z niej tylko w całości i tylko wtedy, gdy nie ma żadnego zdrowego partnera.

Odtworzenie lasu

Odtworzenie lasu to ostateczność: wszystkie kontrolery są utracone albo nie można im ufać po włamaniu. Microsoft opisuje je w osobnym przewodniku „Active Directory Forest Recovery Guide”, a jego główne kroki to:

1. Wybór kopii jednego kontrolera, o której wiemy, że jest sprzed włamania i młodsza niż czas życia nagrobka.
2. Odtworzenie tego kontrolera w odizolowanej sieci, oznaczenie SYSVOL jako wzorcowego, przejęcie ról FSMO.
3. Sprzątanie metadanych wszystkich pozostałych kontrolerów i podniesienie puli identyfikatorów RID, żeby nowe konta nie dostały numerów nadanych po wykonaniu kopii.
4. Dwukrotna zmiana hasła konta `krbtgt` i haseł kont uprzywilejowanych.
5. Promocja nowych kontrolerów od zera i dopiero wtedy połączenie z siecią firmy.

Przed odtworzeniem czytamy aktualną wersję przewodnika na Microsoft Learn, bo zmienia się z każdą wersją systemu. Wydruk przewodnika i listy haseł do kopii leżą w sejfie razem z hasłami DSRM: w dniu takiej awarii nie będzie działał ani Vaultwarden, ani VPN.

DSRM i Windows LAPS

> **Pojęcie: DSRM (Directory Services Restore Mode).** Tryb startu kontrolera bez usługi katalogu, z lokalnym kontem administratora i osobnym hasłem. Definicja jest też na stronie o pierwszym kontrolerze.

Hasło DSRM jest jedynym hasłem lokalnym na kontrolerze i łatwo o nim zapomnieć na lata. Windows LAPS potrafi zarządzać nim tak samo jak hasłem lokalnego administratora na stacjach: dokumentacja wymaga poziomu domeny co najmniej 2016 i włączonego szyfrowania haseł, a funkcja działa na kontrolerach z Windows Server 2019 i nowszym. Zielona spełnia oba warunki, więc proponujemy włączenie zarządzania DSRM przez Windows LAPS na kontrolerach, z prawem odszyfrowania tylko dla grupy administratorów warstwy 0. Konfigurację polityki opisuje strona Windows LAPS: hasło lokalnego administratora w Active Directory.

Hasło zapisane w katalogu ma jedną słabość: w dniu, w którym nie działa żaden kontroler, nie ma go skąd odczytać. Dokumentacja Microsoftu opisuje odczyt z zamontowanej kopii bazy narzędziem `dsamain.exe` i poleceniem `Get-LapsADPassword` z parametrem `-Port`, a tryb, w którym nie jest potrzebny żaden kontroler (`-RecoveryMode`), według tej samej dokumentacji jest dostępny w kompilacjach Windows Insider 27695 i nowszych. Dlatego przy zarządzaniu przez LAPS i tak trzymamy w sejfie aktualny wydruk haseł DSRM po każdej rotacji (do decyzji autora, czy rotacja ma być miesięczna, czy rzadsza).

Gdy coś nie zadziała

Objaw	Przyczyna	Co robimy
`wbadmin` kończy się błędem, że wolumen docelowy jest krytyczny	kopię wskazano na dysk z systemem albo z bazą katalogu	osobny dysk `E:` bez plików systemu
`wbadmin start systemstaterecovery` odmawia pracy	kontroler nie jest w trybie DSRM	`bcdedit /set "{default}" safeboot dsrepair` i restart
Przywrócony z kopii użytkownik po restarcie znowu znika	odtworzenie nieautorytatywne bez `ntdsutil authoritative restore`	powtarzamy z oznaczeniem obiektu jako autorytatywnego
Przywrócony użytkownik nie ma grup z innych jednostek	nie zaimportowano pliku `.ldf` z łączami zwrotnymi	`ldifde -i -f` z plikiem wygenerowanym przez `ntdsutil`
`Restore-ADObject` zwraca błąd, że rodzic nie istnieje	najpierw trzeba przywrócić jednostkę, potem jej zawartość	przywracamy od góry drzewa, filtrujemy po `lastKnownParent`
Nie znamy hasła DSRM	hasło ustawione przy promocji i nigdzie nie zapisane	na działającym kontrolerze `ntdsutil set dsrm password`; na kontrolerze, który już nie startuje, zostaje ponowna instalacja
`restic` z kontrolera kończy się błędem 403	ścieżka repozytorium nie zgadza się z nazwą konta REST (`--private-repos`)	konto `ad` i ścieżka `/ad` na `bkp01`
Kopia GPO zajmuje coraz więcej miejsca na `E:`	brak sprzątania katalogów starszych niż 14 dni	sprawdzamy fragment skryptu z `Remove-Item` i uprawnienia SYSTEM do `E:\GPO`

Ćwiczenia

1. Ktoś usunął grupę `GG_Ksiegowosc` trzy tygodnie temu, a kosz AD jest włączony. Jak ją przywracamy i co sprawdzamy potem?

Odpowiedź

`Get-ADObject -Filter 'isDeleted -eq $true -and Name -like "GG_Ksiegowosc*"' -IncludeDeletedObjects | Restore-ADObject`. Kosz przywraca grupę z jej członkami i SID, więc uprawnienia do udziałów oparte na tym SID zaczynają działać. Sprawdzamy członków (`Get-ADGroupMember`) i, po replikacji, dostęp pani Haliny do folderu księgowości.

1. Dlaczego nie trzymamy kopii stanu systemu kontrolerów przez 5 lat, skoro dla Optimy trzymamy 10?

Odpowiedź

Kopii kontrolera starszej niż czas życia nagrobka (180 dni) nie wolno odtwarzać, bo przywróciłaby obiekty usunięte dawno temu i rozjechała katalog. Długa retencja nic więc nie daje, a zwiększa liczbę miejsc, w których leżą skróty haseł całej firmy. Dane, które trzeba trzymać latami, są w bazach i plikach, nie w katalogu.

1. `dc02` ma uszkodzoną bazę po awarii dysku, `dc01` i `dc03` działają. Co jest najprostsze?

Odpowiedź

Wyłączyć `dc02`, posprzątać jego metadane albo obniżyć go siłą, zainstalować system na nowo i promować od zera; całą zawartość katalogu dostanie od partnerów. Odtworzenie nieautorytatywne z kopii też zadziała, ale przy zdrowych partnerach ponowna promocja jest prostsza i nie niesie ryzyka starej kopii.

1. Napastnik zaszyfrował `hv01`, `hv02` i `dc03`. Repozytorium `ad` na `bkp01` jest w trybie tylko do dopisywania. Od czego zaczynamy odtwarzanie i czego nie robimy?

Odpowiedź

Od wyboru kopii sprzed włamania (data włamania z logów w Graylogu, jeśli przetrwał, albo z kopii krzyżowej na `bkp02`) i od przewodnika odtworzenia lasu w odizolowanej sieci. Nie podłączamy odtworzonego kontrolera do sieci firmy przed dwukrotną zmianą hasła `krbtgt`,

zmianą haseł kont uprzywilejowanych i sprawdzeniem, czy napastnik nie zostawił sobie kont ani zadań zaplanowanych.

Powiązane: Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie · Active Directory od zera: pierwszy i drugi kontroler domeny · GPO od środka: tworzenie, łączenie, kolejność i diagnostyka · Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje · Serwery kopii bkp01 i bkp02: restic, kopia krzyżowa i niezmienność · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt

Źródła: Microsoft Learn, „wbadmin start systemstatebackup”, „wbadmin start systemstaterecovery” (przełącznik `-authsysvol`), „wbadmin get versions”, „wbadmin delete systemstatebackup” (`-keepVersions`) · Microsoft Learn, „Active Directory Recycle Bin” i `Enable-ADOptionalFeature`, `Restore-ADObject`, `Get-ADObject -IncludeDeletedObjects` · Microsoft Learn, „Performing an authoritative restore of Active Directory objects” (`ntdsutil authoritative restore`, pliki `.ldf` z łączami zwrotnymi) · Microsoft Learn, „Active Directory Forest Recovery Guide” · Microsoft Learn, „Useful shelf life of a system-state backup of Active Directory” (czas życia nagrobka 180 dni) · Microsoft Learn, „Windows LAPS scenarios for Windows Server Active Directory” (zarządzanie hasłem DSRM: poziom domeny 2016, kontrolery od Windows Server 2019, odczyt z kopii przez `dsamain.exe` i `Get-LapsADPassword -Port`, `-RecoveryMode` w kompilacjach Insider 27695 i nowszych; odczyt 19.10.2026) · Microsoft Learn, „Ntdsutil set dsrm password” · restic.readthedocs.io, „Backing up” i „Restoring from backup” · github.com/restic/rest-server (tryb `--append-only`, `--private-repos`)

Revision #3
Created 2026-10-18 22:59:53 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:32 UTC by Tomasz Konieczny