Kontrolery w utrzymaniu

Replikacja, FSMO, kopia, odtwarzanie i audyt skryptami.

- Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie
- Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM
- Skrypty audytowe Active Directory

Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie

Poziom: średnio

Dotyczy: Active Directory Domain Services, Windows Server 2022 i 2025, dc01, dc02, dc03 (propozycja), repadmin, dcdiag, ntdsutil, moduł ActiveDirectory

Czas: ~50 min

Kontroler domeny po postawieniu nie wymaga wiele, dopóki replikacja działa, a role FSMO są tam, gdzie myślimy. Ta strona to codzienny i comiesięczny przegląd kontrolerów, przenoszenie i przejmowanie ról, sprzątanie po kontrolerze, który zniknął, oraz dołożenie i wycofanie kontrolera. Wracamy tu po każdym alarmie o replikacji i przed każdą wymianą serwera.

Skróty użyte na tej stronie (16)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
AD DS	Active Directory Domain Services: rola Windows Server uruchamiająca właściwą usługę katalogową Active Directory na kontrolerze domeny
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
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
FSSO	Fortinet Single Sign-On: mechanizm FortiGate, który podgląda logowania w Active Directory i sam wie, z jakiej grupy korzysta dana osoba, bez proszenia jej o dodatkowe hasło
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)

Skrót	Co znaczy
PDC	Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł
RID	Relative Identifier: końcowa, unikalna w domenie część identyfikatora bezpieczeństwa (SID) każdego konta; RID Master to kontroler domeny rozdzielający pule tych numerów
RPC	Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji
RSAT	Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej
SRV	rekord DNS wskazujący nie adres hosta, tylko usługę i port, pod którym jej szukać, np. kontroler domeny w sieci
SYSVOL	system volume: udział sieciowy na kontrolerze domeny z politykami GPO i skryptami logowania, replikowany między kontrolerami tak jak reszta katalogu
USN	Update Sequence Number: rosnący licznik zmian w bazie Active Directory na danym kontrolerze domeny, używany do śledzenia postępu replikacji

Fiszka

Komendy wykonujemy w PowerShellu uruchomionym jako administrator na kontrolerze domeny albo na stacji z RSAT, kontem z grupy Domain Admins (role lasu: Enterprise Admins, rola schematu: Schema Admins). `repadmin` i `dcdiag` są dostępne razem z rolą AD DS i z narzędziami RSAT.

□□ TYLKO ODCZYT

Podsumowanie replikacji wszystkich kontrolerów: repadmin /replsummary

```
repadmin /replsummary
```

Jedna tabela dla całej domeny: od ilu czasu każdy kontroler nie replikował się z partnerem i ile prób się nie powiodło. Pierwsza komenda porannego przeglądu.

Przykład:

```
Replication Summary Start Time: 2026-10-19 07:40:12


Beginning data collection for replication summary, this may take awhile:
```

```
  ......

Source DSA          largest delta    fails/total %%   error
 DC01                       08m:41s    0 /  10    0
 DC02                       08m:37s    0 /  10    0
 DC03                       08m:39s    0 /  10    0

Destination DSA     largest delta    fails/total %%   error
 DC01                       08m:37s    0 /  10    0
 DC02                       08m:39s    0 /  10    0
 DC03                       08m:41s    0 /  10    0
```

repadmin = CLI: podgląd i diagnostyka replikacji Active Directory między kontrolerami domeny

TYLKO ODCZYT

Szczegóły replikacji jednego kontrolera: repadmin /showrepl

```
repadmin /showrepl NazwaKontrolera
```

Pokazuje każdą partycję katalogu, każdego partnera i wynik ostatniej próby. Szukamy wierszy z `Last attempt ... failed` i numeru błędu, który potem wpisujemy w wyszukiwarkę dokumentacji.

Przykład fragmentu:

```
Pamiatkowo\DC02
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 7c1e0a52-3b0e-4b8f-9c6e-0d6c2a8f41aa

==== INBOUND NEIGHBORS ======================================

DC=ad,DC=zielona,DC=example
    Pamiatkowo\DC01 via RPC
        DSA object GUID: 2a4d9a10-5f7e-4c6b-8a51-1f3e5b6c7d80
        Last attempt @ 2026-10-19 07:31:55 was successful.
```

repadmin = CLI: podgląd i diagnostyka replikacji Active Directory między kontrolerami domeny

◫◫ ZMIENIA SYSTEM

Wymuszenie replikacji wszystkich partycji: repadmin /syncall /AdeP

```
repadmin /syncall NazwaKontrolera /AdeP
```

> (gdzie `A` to wszystkie partycje, `d` to nazwy wyróżniające w wyniku zamiast identyfikatorów, `e` to także kontrolery z innych lokacji, a `P` to wypychanie zmian z tego kontrolera do partnerów)

Używamy po ważnej zmianie (nowa polityka, zmiana grupy uprzywilejowanej), żeby nie czekać na harmonogram, i po naprawie błędu replikacji, żeby od razu sprawdzić skutek.

◫◫ **repadmin** = CLI: podgląd i diagnostyka replikacji Active Directory między kontrolerami domeny

◫◫ TYLKO ODCZYT

Kolejka i błędy replikacji w PowerShellu: Get-ADReplicationFailure

```
Get-ADReplicationFailure -Target NazwaKontrolera
Get-ADReplicationPartnerMetadata -Target NazwaKontrolera -Scope Server | Select-Object
Partner, LastReplicationSuccess, LastReplicationResult
```

Pierwsze polecenie zwraca listę nieudanych prób z liczbą błędów od pierwszego niepowodzenia, drugie datę ostatniej udanej replikacji z każdym partnerem. Wynik nadaje się do skryptu, który raz na godzinę wysyła stan do Zabbixa.

Przykład:

```
Partner                                              LastReplicationSuccess
LastReplicationResult
-------                                              ----------------------
---------------------
CN=NTDS Settings,CN=DC01,CN=Servers,CN=Pamiatkowo,... 19.10.2026
07:31:55                      0
CN=NTDS Settings,CN=DC03,CN=Servers,CN=Pamiatkowo,... 19.10.2026
07:32:10                      0
```

TYLKO ODCZYT

Test zdrowia kontrolera: dcdiag

```
dcdiag /s:NazwaKontrolera /q
```

`/q` pokazuje wyłącznie błędy, więc pusty wynik oznacza, że wszystkie testy przeszły. Pełny wynik z opisami dostajemy z `/v`, a pojedynczy test wywołujemy przełącznikiem `/test:`, na przykład `/test:Replications`, `/test:Advertising`, `/test:FsmoCheck` albo `/test:DNS`.

Przykład, gdy na `dc02` nie działa udział SYSVOL:

```
         Starting test: NetLogons
            Unable to connect to the NETLOGON share! (\\DC02\netlogon)
            ..... DC02 failed test NetLogons
```

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **SYSVOL** = system volume: udział sieciowy na kontrolerze domeny z politykami GPO i skryptami logowania, replikowany między kontrolerami tak jak reszta katalogu · **dcdiag** = CLI: zestaw testów sprawdzających zdrowie kontrolera domeny

TYLKO ODCZYT

Sprawdzenie, kto trzyma role FSMO: netdom query fsmo

```
netdom query fsmo
```

Wynik i opis jest na stronie Active Directory od zera: pierwszy i drugi kontroler domeny. Przed każdą operacją na rolach sprawdzamy stan, zamiast polegać na pamięci.

FSMO = Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz · **netdom** = CLI: starsze narzędzie do zarządzania domeną i zaufaniami, tu używane do sprawdzenia ról FSMO

ZMIENIA SYSTEM

Przeniesienie ról FSMO na działający kontroler: Move-ADDirectoryServerOperationMasterRole

```
Move-ADDirectoryServerOperationMasterRole -Identity NazwaKontroleraDocelowego -
OperationMasterRole PDCEmulator, RIDMaster, InfrastructureMaster, SchemaMaster,
```

```
DomainNamingMaster
```

Przeniesienie (transfer) to uprzejma zmiana: dotychczasowy właściciel działa, oddaje rolę i aktualny stan, nowy ją przejmuje. Robimy to przed wyłączeniem kontrolera na dłużej niż kilka godzin i przed jego wymianą. Możemy podać tylko wybrane role.

Przykład przed wymianą `dc01`:

```
Move-ADDirectoryServerOperationMasterRole -Identity dc02 -OperationMasterRole
PDCEmulator, RIDMaster, InfrastructureMaster, SchemaMaster, DomainNamingMaster
```

FSMO = Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz

OSTROŻNIE · NIEODWRACALNE

Przejęcie ról FSMO po trwałej awarii właściciela: Move-ADDirectoryServerOperationMasterRole -Force

```
Move-ADDirectoryServerOperationMasterRole -Identity NazwaKontroleraDocelowego -
OperationMasterRole NazwyRol -Force
```

Przejęcie (seize) robimy wyłącznie wtedy, gdy dotychczasowy właściciel ról nie wróci: spłonął, ma uszkodzoną bazę, której nie odtwarzamy, albo decydujemy, że stawiamy go od nowa. Polecenie najpierw próbuje zwykłego przeniesienia, a dopiero gdy stary właściciel nie odpowiada, zapisuje role na nowym kontrolerze bez jego zgody.

> Kontroler, któremu odebraliśmy role przejęciem, nigdy nie może wrócić do sieci w dawnym stanie. Wyłączamy go, nie podłączamy kabla, a po decyzji robimy sprzątanie metadanych i instalujemy system od nowa. Stary właściciel puli RID albo schematu, który wraca do sieci, może nadać zdublowane identyfikatory i zepsuć las w sposób, którego nie odkręcimy kopią.

FSMO = Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz · **RID** = Relative Identifier: końcowa, unikalna w domenie część identyfikatora bezpieczeństwa (SID) każdego konta; RID Master to kontroler domeny rozdzielający pule tych numerów

ZMIENIA SYSTEM

Ustawienie źródła czasu na PDC Emulator: w32tm /config

```
w32tm /config /manualpeerlist:"SerwerNTP1,0x8 SerwerNTP2,0x8" /syncfromflags:manual
/reliable:yes /update
Restart-Service w32time
```

Wykonujemy tylko na kontrolerze z rolą PDC Emulator. Pozostałe kontrolery i komputery biorą czas z hierarchii domeny, więc niczego na nich nie ustawiamy. Po przeniesieniu roli PDC Emulator to samo robimy na nowym właścicielu, a na starym wracamy do hierarchii domeny poleceniem `w32tm /config /syncfromflags:domhier /reliable:no /update`.

Przykład:

```
w32tm /config /manualpeerlist:"0.pl.pool.ntp.org,0x8 1.pl.pool.ntp.org,0x8"
/syncfromflags:manual /reliable:yes /update
```

PDC = Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł · **w32tm** = Windows Time: konfiguracja i diagnostyka usługi czasu, np. źródła NTP na PDC Emulator

TYLKO ODCZYT

Sprawdzenie źródła czasu: w32tm /query /status

```
w32tm /query /status
```

Przykład na `dc02`:

```
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Source: dc01.ad.zielona.example
Last Successful Sync Time: 19.10.2026 07:35:02
```

w32tm = Windows Time: konfiguracja i diagnostyka usługi czasu, np. źródła NTP na PDC Emulator

ZMIENIA SYSTEM

Promocja kolejnego kontrolera do lokacji: Install-ADDSDomainController -SiteName

```
Install-ADDSDomainController `
    -DomainName "NazwaDomeny" `
    -SiteName "NazwaLokacji" `
    -InstallDns:$true `
    -Credential (Get-Credential) `
    -SafeModeAdministratorPassword (Read-Host -AsSecureString -Prompt "Haslo DSRM")
```

To samo polecenie co przy `dc02`, z jawnie wskazaną lokacją. Pełny przebieg dla `dc03` jest niżej w sekcji „Dodanie trzeciego kontrolera”.

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

OSTROŻNIE · NIEODWRACALNE

Sprzątanie metadanych po kontrolerze, który nie wróci: ntdsutil metadata cleanup

```
ntdsutil
metadata cleanup
remove selected server
"CN=NazwaKontrolera,CN=Servers,CN=NazwaLokacji,CN=Sites,CN=Configuration,DC=ad,DC=zielon
a,DC=example"
quit
quit
```

Usuwa z katalogu obiekt kontrolera, którego nie dało się normalnie obniżyć (`Uninstall-ADDSDomainController`). Od Windows Server 2008 to samo robi usunięcie konta komputera kontrolera w konsoli Active Directory Users and Computers albo obiektu serwera w Active Directory Sites and Services, z potwierdzeniem, że kontroler jest trwale niedostępny. Po sprzątaniu zostają jeszcze rekordy DNS, które usuwamy ręcznie.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

OSTROŻNIE · NIEODWRACALNE

Obniżenie działającego kontrolera: Uninstall-ADDSDomainController

```
Uninstall-ADDSDomainController -LocalAdministratorPassword (Read-Host -AsSecureString -
Prompt "Nowe haslo lokalnego administratora")
```

Opis parametrów jest na stronie o pierwszym kontrolerze. Tu ważna jest kolejność czynności przed tym poleceniem, opisana w sekcji „Wycofanie kontrolera”.

Z życia wzięte

Z ŻYCIA WZIĘTE

Poniedziałek, 8:05. Pan Wojtek, audytor, pyta, kiedy ostatnio sprawdzaliśmy replikację kontrolerów. Tomek uruchamia `repadmin /replsummary` i widzi przy `dc02` 41 dni od ostatniej udanej replikacji z `dc01` i błąd 1722, serwer RPC niedostępny. Okazuje się, że we wrześniu ktoś dopisał na `dc01` regułę zapory dla dynamicznych portów RPC tylko z sieci biurowej, więc `dc02` przestał pobierać zmiany. Hasła zmienione od tamtej pory działały tylko dzięki PDC Emulator, a nowe konta istniały wyłącznie na `dc01`. Od tego dnia `repadmin /replsummary` wysyła wynik do Zabbixa co godzinę.

Jak to działa

Rozwiń: jak to działa pod spodem

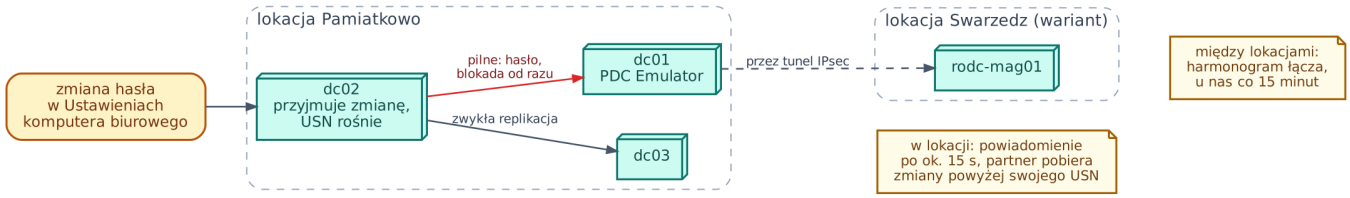
Replikacja

Pojęcie: replikacja wielomasterowa. Każdy zapisywalny kontroler przyjmuje zmiany i sam rozsyła je partnerom. Krótka definicja jest na stronie o pierwszym kontrolerze; tutaj interesuje nas, jak replikacja wie, czego partner jeszcze nie ma.

Pojęcie: USN (Update Sequence Number). Licznik zmian prowadzony osobno przez każdy kontroler. Każda zmiana dostaje kolejny numer, a partner pamięta, do którego numeru już pobrał zmiany od danego kontrolera (tak zwany high-watermark). Przy kolejnej replikacji prosi tylko o zmiany z wyższymi numerami.

Pojęcie: KCC (Knowledge Consistency Checker). Proces na każdym kontrolerze, który co 15 minut sam układa połączenia replikacji: wewnątrz lokacji pierścień z najwyżej

trzema skokami, między lokacjami połączenia przez wybrany kontroler pomostowy (bridgehead). Ręcznie nie tworzymy połączeń, chyba że wiemy dokładnie dlaczego.



Rysunek 1. Replikacja w Zielonej: zmiana hasła trafia na dc02, który powiadamia partnerów w lokacji Pamiatkowo po około 15 sekundach, a do lokacji Swarzedz zmiana idzie przez łącze lokacji co 15 minut; pilne zmiany, takie jak zablokowanie konta, idą od razu do PDC Emulator (kliknięcie otwiera pełny rozmiar)

Wewnątrz lokacji kontroler po zmianie czeka kilkanaście sekund i powiadamia partnerów, którzy pobierają zmiany. Między lokacjami replikacja idzie według harmonogramu łącza lokacji, u nas co 15 minut. Kilka rzeczy nie czeka na nikogo: blokada konta, zmiana hasła i wyłączenie konta trafiają od razu do PDC Emulator, który przy nieudanym logowaniu jest pytany o najnowsze hasło.

Pojęcie: USN rollback. Sytuacja, w której kontroler wraca do starszego stanu bazy, ale dalej używa tych samych numerów zmian. Partnerzy uważają, że te numery już znają, i ignorują nowe zmiany z tego kontrolera, a katalog po cichu przestaje być spójny. Przyczyną jest zwykle przywrócenie migawki maszyny wirtualnej albo starej kopii dysku narzędziem, które nie wie, że to kontroler domeny. Windows Server od 2012 na hiperwizorach z identyfikatorem generacji maszyny (Hyper-V go ma) wykrywa taki powrót i chroni się sam, ale migawki kontrolera i tak nie traktujemy jak kopii zapasowej.

Role FSMO: przeniesienie i przejęcie

Sytuacja	Co robimy	Czy stary właściciel może wrócić
planowany serwis `dc01` na kilka godzin	nic, role mogą chwilę poczekać	tak
serwis albo wymiana `dc01` na dłużej	przeniesienie (transfer) na `dc02` przed wyłączeniem	tak

Sytuacja	Co robimy	Czy stary właściciel może wrócić
`dc01` nie działa, naprawa potrwa dzień	czekamy, chyba że boli PDC Emulator (czas, blokady); wtedy przejęcie samej roli PDC	po przejęciu nie, trzeba go postawić od nowa
`dc01` nie wróci nigdy	przejęcie (seize) wszystkich ról na `dc02`, sprzątanie metadanych	nie

Rozmieszczenie ról w Zielonej i skutki niedostępności każdej z nich opisuje strona Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo.

Czas w domenie

> **Pojęcie: Kerberos.** Sposób logowania w domenie, w którym kontroler wydaje komputerowi i użytkownikowi bilety ważne przez określony czas, zamiast za każdym razem sprawdzać hasło. Bilet ma w sobie godzinę wystawienia, więc zegary w domenie muszą się zgadzać: domyślna tolerancja to 5 minut.

Hierarchia czasu w domenie jest prosta: PDC Emulator w domenie głównej lasu pobiera czas z zewnątrz, pozostałe kontrolery od niego, a komputery od kontrolera, do którego się logują. Dlatego źródło zewnętrzne ustawiamy tylko na PDC Emulator i przenosimy je razem z rolą. Kontrolery w maszynach wirtualnych nie powinny dodatkowo brać czasu od hosta Hyper-V; usługa integracji „Time Synchronization” na kontrolerach jest u nas wyłączona (sprawdzamy to po każdej migracji maszyny).

Dodanie trzeciego kontrolera

Zanim zaczniemy

Dokładamy `dc03` (10.20.10.114, Windows Server 2025, poza klastrem `hv01` i `hv02`), zgodnie z projektem. Sprawdziliśmy grep po całej bazie, że adres 10.20.10.114 nie jest używany.

Wymaganie	Jak sprawdzamy
poziom lasu co najmniej 2016	`(Get-ADForest).ForestMode` mówi `Windows2016Forest`
zdrowa replikacja istniejących kontrolerów	`repadmin /replsummary` bez błędów, `dcdiag /q` pusty
statyczny adres, nazwa, aktualizacje	jak przy `dc02` na stronie o pierwszym kontrolerze

Wymaganie	Jak sprawdzamy
DNS klienta na `dc03`	`10.20.10.11` i `10.20.10.12` przed promocją, po promocji najpierw partner, na końcu `127.0.0.1`
reguły zapory między kontrolerami	ruch RPC, LDAP, Kerberos, DNS, SMB między 10.20.10.11, .12 i .114
wpis w CMDB i zgłoszenie zmiany	zmiana standardowa w GLPI, okno poza zamknięciem miesiąca

Przebieg

1. Na `dc03` ustawiamy adres, nazwę i DNS klienta, instalujemy aktualizacje i rolę `Install-WindowsFeature AD-Domain-Services -IncludeManagementTools`.
2. Promujemy serwer poleceniem z fiszki z `-SiteName "Pamiatkowo"` i hasłem DSRM zapisanym w Vaultwardenie oraz w kopercie w sejfie.
3. Po restarcie zmieniamy DNS klienta na `10.20.10.11`, `10.20.10.12` i na końcu `127.0.0.1`. Kontroler, który pyta tylko sam siebie, po restarcie może czekać na własny DNS, zanim wystartuje usługa katalogu.
4. Dopisujemy `dc03` jako trzeci serwer DNS w opcji 006 zakresów DHCP i na serwerach ze statycznym adresem, opis na stronie DHCP w utrzymaniu: hot standby, rezerwacje drukarek i skanerów, opcje i DNS.
5. Dopisujemy `dc03` do kopii stanu systemu (strona o kopii AD), do monitoringu w Zabbixie i do przekazywania dzienników do Grayloga.

Weryfikacja

```
Get-ADDomainController -Filter * | Select-Object Name, Site, IPv4Address, OperatingSystem,
IsGlobalCatalog
repadmin /replsummary
dcdiag /s:dc03 /q
```

Przykład:

```
Name Site       IPv4Address  OperatingSystem                    IsGlobalCatalog
---- ----       -----------  ---------------                    ---------------
DC01 Pamiatkowo 10.20.10.11  Windows Server 2022 Standard       True
DC02 Pamiatkowo 10.20.10.12  Windows Server 2022 Standard       True
DC03 Pamiatkowo 10.20.10.114 Windows Server 2025 Standard       True
```

Wycofanie zmian

Gdy `dc03` sprawia kłopot w pierwszych dniach, obniżamy go z powrotem poleceniem `Uninstall-ADDSDomainController`, usuwamy jego adres z opcji DHCP i z ustawień DNS klientów, a po replikacji sprawdzamy, że w strefie `_msdcs.ad.zielona.example` nie zostały jego rekordy SRV.

Wycofanie kontrolera

Wycofujemy kontroler przy wymianie sprzętu albo systemu. Kolejność ma znaczenie, bo kontroler to nie tylko katalog: jest też serwerem DNS, czasem DHCP, a jego adres siedzi w dziesiątkach miejsc.

1. Sprawdzamy, co jeszcze robi kontroler: `netdom query fsmo`, `Get-DhcpServerInDC`, czy jest kolektorem FSSO dla `fw01`, czy stoi na nim AD CS (na `dc01` stoi, a urząd wyprowadzamy z niego według strony Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona, zanim kontroler pójdzie do wycofania), czy aplikacje mają jego nazwę albo adres wpisany na sztywno (LDAP w Gitea, Grafanie, NetBoksie).
2. Przenosimy role FSMO i, jeśli trzeba, źródło czasu.
3. Usuwamy jego adres z opcji 006 DHCP, ze statycznych ustawień DNS serwerów i z przekaźnika DHCP na `fw01` i `rtr-mag01`.
4. Czekamy co najmniej jeden pełny okres dzierżawy DHCP, a w Graylogu sprawdzamy, czy ktoś jeszcze pyta ten kontroler o LDAP albo DNS.
5. Obniżamy kontroler `Uninstall-ADDSDomainController`, a po restarcie odłączamy serwer od domeny albo go wyłączamy.
6. Sprawdzamy `repadmin /replsummary`, rekordy w `_msdcs` i obiekt serwera w Active Directory Sites and Services.

Gdy kontroler wymieniamy na nowy pod tą samą nazwą i adresem, najpierw kończymy wycofanie starego (z usunięciem obiektu w katalogu), a dopiero potem promujemy nowy. Dwa kontrolery o tej samej nazwie w różnym czasie są w porządku, dwa naraz nie.

Częste błędy

Objaw	Przyczyna	Co robimy
`repadmin /showrepl` pokazuje błąd 1722 (serwer RPC niedostępny)	zapora albo filtr blokuje dynamiczne porty RPC między kontrolerami	sprawdzamy reguły na kontrolerach i na `fw01`; między kontrolerami przepuszczamy cały ruch AD

Objaw	Przyczyna	Co robimy
Błąd 8524 (wyszukiwanie DSA nie powiodło się)	partner nie rozwiązuje nazwy GUID kontrolera w strefie `_msdcs`	`dcdiag /test:DNS`, rejestracja rekordów `ipconfig /registerdns` i restart usługi Netlogon na partnerze
Błąd 8614 (zbyt długo bez replikacji)	kontroler nie replikował się dłużej niż czas życia nagrobka (180 dni)	nie zmuszamy go do replikacji; obniżamy go, sprzątamy metadane i stawiamy od nowa
Zegary kontrolerów rozjeżdżają się o kilka minut	PDC Emulator bierze czas od hosta Hyper-V albo nie ma źródła zewnętrznego	`w32tm /query /status` na PDC, wyłączona synchronizacja czasu z hostem, `w32tm /config` z fiszki
Po przejęciu ról stary `dc01` wrócił po naprawie i w sieci są dwa właściciele ról	przejęcie bez odłączenia starego kontrolera	natychmiast odłączamy stary kontroler, sprawdzamy `netdom query fsmo` na każdym kontrolerze, stary instalujemy od nowa
Nowe konta na jednym kontrolerze nie powstają, błąd o puli RID	RID Master niedostępny, a lokalna pula się skończyła	przywracamy RID Master albo przejmujemy rolę, jeśli nie wróci
Po wycofaniu kontrolera część komputerów loguje się wolno	adres starego kontrolera wciąż w opcji DNS albo w statycznych ustawieniach	przegląd opcji DHCP, `Get-DnsClientServerAddress` na serwerach, zapytania DNS do starego adresu w Graylogu

□□ Ćwiczenia

1. `dc01` trzyma wszystkie role i ma iść do serwisu sprzętowego na dwa dni. Co robimy przed wyłączeniem i co po powrocie?

Odpowiedź

Przenosimy wszystkie pięć ról na `dc02` (transfer), na `dc02` ustawiamy zewnętrzne źródło czasu, a na `dc01` hierarchię domeny. Po powrocie `dc01` sprawdzamy replikację, a role możemy zostawić na `dc02` albo przenieść z powrotem; ważne, żeby projekt i dokumentacja mówiły, gdzie są.

1. Dlaczego po przejęciu ról z kontrolera, który spłonął, nie możemy przywrócić go z kopii na nowym sprzęcie i podłączyć do sieci?

Odpowiedź

Kopia zawiera stan, w którym to on był właścicielem ról. Po podłączeniu w sieci byłyby dwa kontrolery przekonane, że rozdzielają pule RID albo zmieniają schemat, co grozi zdublowanymi identyfikatorami. Po przejęciu ról stary kontroler sprzątamy z katalogu, a nowy stawiamy jako

świeży kontroler.

1. `repadmin /replsummary` pokazuje dla `dc02` largest delta 3 godziny, a dla `dc01` i `dc03` kilka minut. Od czego zaczynamy?

Odpowiedź

Od `repadmin /showrepl dc02`, żeby zobaczyć, z którym partnerem i dla której partycji ostatnia próba się nie udała, i jaki jest numer błędu. Potem `dcdiag /s:dc02 /q` i sprawdzenie sieci oraz DNS między kontrolerami. Ręczne `repadmin /syncall` robimy dopiero po usunięciu przyczyny.

1. Tomek chce przywrócić `dc02` z migawki maszyny sprzed tygodnia, „bo tak szybciej”. Co mu mówimy?

Odpowiedź

Migawka nie jest kopią zapasową kontrolera. Mechanizm identyfikatora generacji w Hyper-V chroni przed najgorszymi skutkami, ale przywracanie kontrolera robimy kopią stanu systemu albo, szybciej i czyściej, obniżamy uszkodzony kontroler i promujemy go od nowa; resztę danych dostanie z replikacji. Opis jest na stronie o kopii i odtwarzaniu AD.

Powiązane: Active Directory od zera: pierwszy i drugi kontroler domeny · Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo · Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM · DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain · Skrypty audytowe Active Directory · Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć

Źródła: Microsoft Learn, „Repadmin” i „Dcdiag” (składnia `/replsummary`, `/showrepl`, `/syncall /AdeP`, `/test:`) · Microsoft Learn, `Get-ADReplicationFailure`, `Get-ADReplicationPartnerMetadata`, `Move-ADDirectoryServerOperationMasterRole` (parametr `-Force`), `Install-ADDSDomainController`, `Uninstall-ADDSDomainController` · Microsoft Learn, „Transfer or seize Operation Master roles in Active Directory Domain Services” · Microsoft Learn, „Clean up Active Directory Domain Controller server metadata” (`ntdsutil metadata cleanup`, usuwanie przez konsole od Windows Server 2008) · Microsoft Learn, „How the Windows Time Service Works” i „Configuring an authoritative time source” (`w32tm /config /reliable:yes`) · Microsoft Learn, „Active Directory replication error 1722, 8524 i 8614” (artykuły rozwiązywania problemów) · Microsoft Learn, „Virtualized domain controller architecture” (VM-GenerationID, ochrona przed USN rollback) · Microsoft Learn, „Active Directory functional levels” (kontroler Windows Server 2025 wymaga poziomu co najmniej 2016)

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.

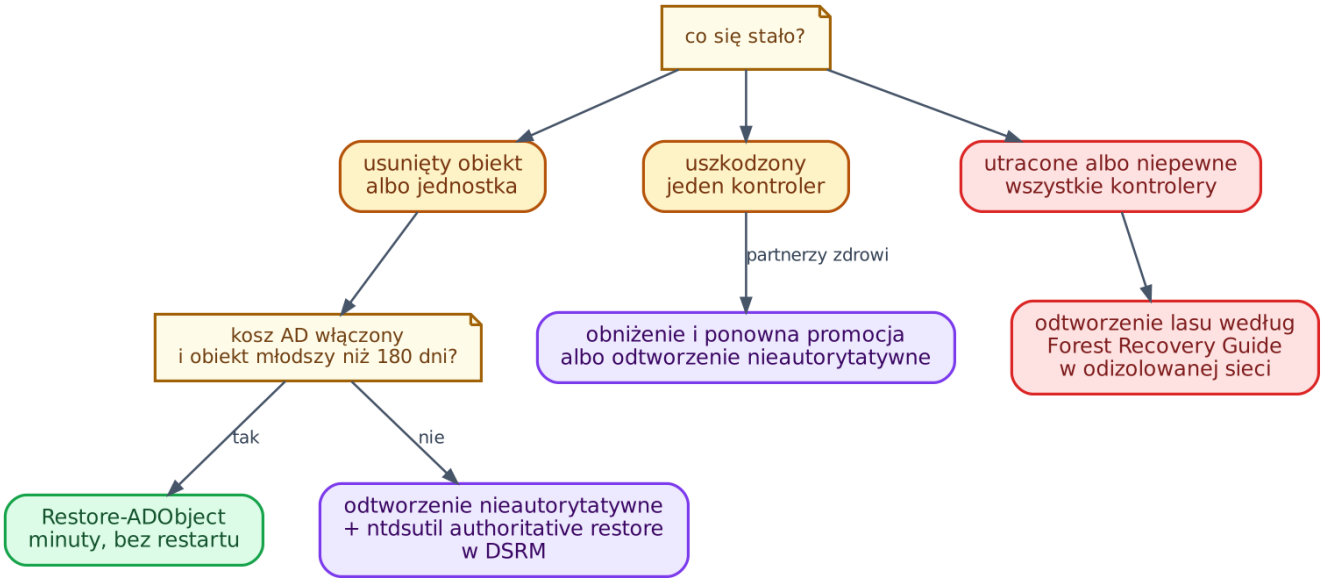
Wycofanie zmian

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.

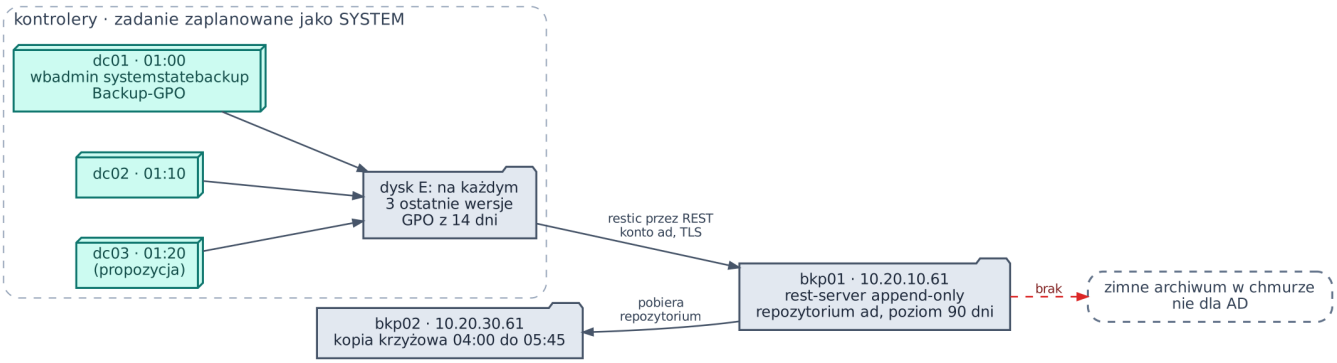
Pojęcie: odtworzenie autorytatywne. Odtworzenie nieautorytatywne plus oznaczenie wybranych obiektów jako ważniejszych niż to, co mają partnerzy. Bez tego partnerzy po restarcie odesłaliby informację, że obiekt jest usunięty, i obiekt zniknąłby ponownie.

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`)

Skrypty audytowe Active Directory

Poziom: zaawansowany **Dotyczy: Windows Server 2016+, moduł ActiveDirectory (RSAT)**

Czas: ~40 min

Sześć gotowych skryptów audytowych do skopiowania: od zagnieżdżonych grup między domenami, przez pełny zrzut DNS i GPO, po klucze BitLocker i wymuszenie synchronizacji z Entra ID.

Skróty użyte na tej stronie (14)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
CSV	w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami
DC	Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników
DN	Distinguished Name: pełny, jednoznaczny adres jednego obiektu w katalogu LDAP, na przykład konta albo grupy
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
GPMC	Group Policy Management Console: konsola do zarządzania politykami GPO w domenie
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery
RSAT	Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
XML	eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Fiszka

TYLKO ODCZYT

Audyt grupy z zagnieżdżoną grupą z innej domeny

```
# Pytaj użytkownika o nazwę grupy, kontroler domeny (DC) i poświadczenia
$Group = Read-Host -Prompt "Podaj nazwę grupy"
$DC = Read-Host -Prompt "Podaj kontroler domeny bądź jej nazwę (NazwaKontroleraDC / NazwaDomeny)"
$Credential = Get-Credential -Message "Podaj poświadczenia użytkownika do dostępu do domeny $DC"

# Pobierz członków grupy z określonego kontrolera domeny
$membership = Get-ADGroup $Group -Properties Member -Server $DC -Credential $Credential
$membership.Member | Group-Object { ($_ -split '(?=DC=)', 2)[1] } |
ForEach-Object {
    [adsi]$ldap = 'LDAP://{0}' -f $_.Name
    [string]$domain = $ldap.Name

    foreach ($member in $_.Group) {
        $obj = Get-ADObject $member -Server $domain -Credential $Credential
        [pscustomobject]@{
            MemberOf       = $membership.Name
            Domain         = $domain
            Name           = $obj.Name
            DSN            = $obj.DistinguishedName
            SamAccountName = $obj.SamAccountName
            ObjectClass    = $obj.ObjectClass
        }
    }
}
```

Komendę uruchamiamy jako Administrator w PowerShell na systemie z zainstalowanymi przystawkami RSAT. Rozwiązujemy tu problem, który zwykły `Get-ADGroupMember` nie obsługuje wprost: grupa ma wśród członków obiekty z innej domeny w tym samym lesie, a `Member` zwraca dla nich pełny `DistinguishedName` zamiast gotowego obiektu. Grupujemy członków po fragmencie DN odpowiadającym domenie (`(?=DC=)` jako wyrażenie regularne z pozytywnym wyprzedzeniem, dzielące napis tuż przed każdym „DC="), budujemy z tego fragmentu

ścieżkę LDAP, odczytujemy jej rzeczywistą nazwę domeny przez `[adsi]`, i dopiero z tak ustaloną domeną odpytujemy `Get-ADObject` dla każdego członka osobno.

Przykład:

```
MemberOf       Domain                  Name
DSN                                                    SamAccountName  ObjectClass
--------       ------                  ----           ---
                                                          --------------  -----------
GrupaProjektowa ad.zielona.example     Jan Kowalski  CN=Jan
Kowalski,OU=Users,DC=ad,DC=zielona,DC=example        jkowalski       user
GrupaProjektowa filia.ad.zielona.example Anna Nowak  CN=Anna
Nowak,OU=Users,DC=filia,DC=ad,DC=zielona,DC=example anowak          user
```

Zielona ma jedną domenę, więc w produkcji skrypt przydaje się głównie przy członkach z domen zaufanych; przykład pokazuje las laboratoryjny z domeną podrzędną `filia`.

RSAT = Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej · **DN** = Distinguished Name: pełny, jednoznaczny adres jednego obiektu w katalogu LDAP, na przykład konta albo grupy · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników · **LDAP** = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) · **DSN** = Data Source Name: nazwa gotowego połączenia do bazy danych zapisanego w konfiguracji ODBC

TYLKO ODCZYT

Audyt grupy z zagnieżdżoną grupą: wariant z zapisem do CSV

```
# Pytaj użytkownika o nazwę grupy, kontroler domeny (DC) i poświadczenia
$Group = Read-Host -Prompt "Podaj nazwę grupy"
$DC = Read-Host -Prompt "Podaj kontroler domeny bądź jej nazwę (NazwaKontroleraDC /
NazwaDomeny)"
$Credential = Get-Credential -Message "Podaj poświadczenia użytkownika do dostępu do
domeny $DC"

# Pobierz członków grupy z określonego kontrolera domeny
$membership = Get-ADGroup $Group -Properties Member -Server $DC -Credential $Credential

# Zbieramy obiekty członków grupy
$results = foreach ($domainGroup in $membership.Member | Group-Object { ($_ -split
'(?=DC=)', 2)[1] }) {
```

```
    [adsi]$ldap = "LDAP://$($domainGroup.Name)"
    [string]$domain = $ldap.Name

    foreach ($member in $domainGroup.Group) {
        $obj = Get-ADObject $member -Server $domain -Credential $Credential
        [pscustomobject]@{
            MemberOf       = $membership.Name
            Domain         = $domain
            Name           = $obj.Name
            DSN            = $obj.DistinguishedName
            SamAccountName = $obj.SamAccountName
            ObjectClass    = $obj.ObjectClass
        }
    }
}

# Pytanie do użytkownika czy zapisać wynik
$saveCsv = Read-Host -Prompt "Czy chcesz zapisać wynik do pliku CSV? (t/n)"

if ($saveCsv -eq 't') {
    $path = Read-Host -Prompt "Podaj pełną ścieżkę do pliku CSV"

    try {
        $results | Export-Csv -Path $path -NoTypeInformation -Encoding UTF8
        Write-Host "Wynik zapisano do pliku: $path" -ForegroundColor Green
    }
    catch {
        Write-Host "Wystąpił błąd podczas zapisywania pliku:" -ForegroundColor Red
        Write-Host $_.Exception.Message -ForegroundColor Red
    }
}
else {
    Write-Host "Wynik nie został zapisany do pliku." -ForegroundColor Yellow
}

# Wyświetlenie wyników na ekranie
$results
```

Ten sam mechanizm co wyżej, rozbudowany o opcjonalny zapis do CSV: wygodne, gdy audyt trzeba udokumentować albo porównać ze stanem sprzed miesiąca, zamiast tylko przejrzeć wynik na ekranie i zapomnieć.

CSV = w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami ·**DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników ·**LDAP** = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) ·**DSN** = Data Source Name: nazwa gotowego połączenia do bazy danych zapisanego w konfiguracji ODBC

TYLKO ODCZYT

Skrypt wykonujący audyt wszystkich wpisów w DNS

```
### Pobieranie argumentu adresu serwera DNS ###
if ($args.Count -eq 2) {
    $DnsServer = $args[0]
    $SavePath = $args[1]
} else {
    # Jeśli uruchomiono bez argumentów, prosimy o wpisanie ręcznie
    Write-Host "Uruchom skrypt poprzez ./NazwaSkryptu.ps1 AdresSerweraDNS
ŚcieżkaDoPliku.txt bądź podaj je teraz: "
    $DnsServer = Read-Host "Podaj adres serwera DNS"
    $SavePath = Read-Host "Podaj ścieżkę do zapisu"
}

# Sprawdzenie czy podano ścieżkę do zapisu
if (-not $SavePath) {
    Write-Host "Nie podano ścieżki do zapisu. Skrypt zostanie przerwany." -
ForegroundColor Red
    exit
}

# Pobranie stref DNS z serwera
$Zones = @(Get-DnsServerZone -ComputerName $DnsServer)

ForEach ($Zone in $Zones) {
    # Wypisywanie strefy do konsoli i pliku
    Write-Host "`n$($Zone.ZoneName)" -ForegroundColor "Green"
    "`n$($Zone.ZoneName)" | Out-File -Append -FilePath $SavePath
```

```
    # Pobranie rekordów DNS w strefie i zapis do pliku
    Get-DnsServerResourceRecord -ComputerName $DnsServer -ZoneName $Zone.ZoneName | Out-
File -Append -FilePath $SavePath
}

Write-Host "Zapis zakończony. Dane znajdują się w: $SavePath" -ForegroundColor Cyan
```

Skrypt uruchamiamy jako Administrator w PowerShell, z zainstalowanymi przystawkami RSAT DNS. Zapisuje pliki w aktualnie używanym folderze, jeśli podajemy ścieżkę względną: zamierzone, żeby ten sam skrypt dało się odpalić z różnych katalogów roboczych bez modyfikacji. Uruchomienie z argumentami (`./audyt-dns.ps1 dc01 raport.txt`) pomija oba pytania interaktywne, co czyni go gotowym do wywołania z harmonogramu zadań.

Przykładowe uruchomienie:

```
PS C:\Audyty> .\audyt-dns.ps1 dc01 dns-raport.txt

ad.zielona.example
dc01         Host (A)     10.20.10.11
app01        Host (A)     10.20.10.41

Zapis zakończony. Dane znajdują się w: dns-raport.txt
```

□□ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **RSAT** = Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej · **exit** = zakończ bieżącą powłokę albo skrypt z podanym kodem wyjścia

□□ **ZMIENIA SYSTEM**

Wariant DNS z interaktywnym oknem dla każdej strefy

```
Add-Type -AssemblyName Microsoft.VisualBasic
Add-Type -TypeDefinition @"
using System;
using System.Runtime.InteropServices;

public class WinAPI {
    [DllImport("user32.dll")]
    public static extern bool SetForegroundWindow(IntPtr hWnd);
```

```
}
"@ -Language CSharp

# Wyświetlenie okna dialogowego do wpisania adresu serwera DNS z instrukcją
$DnsServer = [Microsoft.VisualBasic.Interaction]::InputBox(
    "Podaj adres serwera DNS w formacie: NazwaSerwera.NazwaDomeny`n`nUWAGA: Skrypt musi
być uruchomiony na komputerze z zainstalowaną przystawką RSAT: DNS!`n`nUWAGA: Skrypt
otwiera nowe interaktywne okno dla każdej zony!",
    "Wprowadź adres DNS",
    "dc01.ad.zielona.example"
)

# Ustawienie okna na pierwszym planie po zamknięciu InputBox
$process = Get-Process | Where-Object { $_.MainWindowTitle -match "Wprowadź adres DNS" }
if ($process) {
    [WinAPI]::SetForegroundWindow($process.MainWindowHandle)
}

# Jeśli użytkownik nic nie wpisał i kliknął "Anuluj", skrypt się zatrzyma
if (-not $DnsServer) {
    Write-Host "Nie podano adresu serwera DNS. Skrypt zostanie zakończony." -
ForegroundColor Red
    exit
}

# Pobranie stref DNS z serwera
$Zones = @(Get-DnsServerZone -ComputerName $DnsServer)

ForEach ($Zone in $Zones) {
    Write-Host "`n$($Zone.ZoneName)" -ForegroundColor "Green"

    # Pobranie rekordów DNS w strefie
    $records = Get-DnsServerResourceRecord -ComputerName $DnsServer -ZoneName
$Zone.ZoneName

    if ($records) {
        # Wymuszenie oczekiwania na zamknięcie Out-GridView przed otwarciem kolejnego
        $records | Out-GridView -Title "Rekordy DNS - $($Zone.ZoneName)" -PassThru |
Out-Null
```

```
    } else {
        Write-Host "Brak rekordów w strefie $($Zone.ZoneName)" -ForegroundColor Yellow
    }
}

Write-Host "Koniec działania skryptu." -ForegroundColor Cyan
```

Ten sam audyt, ale zamiast pliku tekstowego każda strefa otwiera się jako osobne, interaktywne okno `Out-GridView`: okno kolejnej strefy otwiera się dopiero po zamknięciu poprzedniego, więc przy dużej liczbie stref przeklikanie się przez wszystkie może zająć sporo czasu. Przydatne do jednorazowego, ręcznego przeglądania małej liczby stref, niepraktyczne jako zadanie cykliczne bez nadzoru: do tego celu służy wariant zapisujący do pliku wyżej.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **RSAT** = Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej · **exit** = zakończ bieżącą powłokę albo skrypt z podanym kodem wyjścia

ZMIENIA SYSTEM

Skrypt dodający aliasy SMTP użytkownikom w parametrach AD

```
# Importowanie modułu Active Directory
Import-Module ActiveDirectory

# Definicja zmiennych dla domen
$oldDomain = "NazwaStarejDomeny"
$newDomain = "NazwaNowejDomeny"

# Określenie wyróżnionej nazwy (DN) docelowej jednostki organizacyjnej (OU)
$ou = "SciezkaDoOU"

# Pobranie wszystkich użytkowników (aktywnych i nieaktywnych) w określonym OU wraz z ich
UserPrincipalName i ProxyAddresses
$users = Get-ADUser -Filter * -SearchBase $ou -Properties UserPrincipalName,
ProxyAddresses, SamAccountName

# Iteracja przez każdego użytkownika (zarówno aktywnego, jak i nieaktywnego) i dodanie
aliasu
foreach ($user in $users) {
```

```
    # Upewnienie się, że użytkownik ma ustawiony UserPrincipalName kończący się na
starej domenie
    if ($user.UserPrincipalName -match "@$oldDomain$") {

        # Wyodrębnienie nazwy użytkownika poprzez usunięcie starej domeny z
UserPrincipalName
        $username = $user.UserPrincipalName -replace "@$oldDomain", ""

        # Utworzenie aliasu w formacie username@newDomain
        $alias = "smtp:$username@$newDomain"

        # Pobranie aktualnych ProxyAddresses (aliasów e-mail)
        $proxyAddresses = $user.ProxyAddresses

        # Upewnienie się, że ProxyAddresses jest zainicjalizowane
        if (-not $proxyAddresses) {
            $proxyAddresses = @()
        }

        # Sprawdzenie, czy alias już istnieje
        if ($proxyAddresses -notcontains $alias) {
            try {
                # Dodanie nowego aliasu
                Set-ADUser -Identity $user -Add @{ProxyAddresses = $alias}
                Write-Host "Dodano alias $alias dla użytkownika $username"
            } catch {
                Write-Host "Błąd podczas dodawania aliasu $alias dla użytkownika
$username: $_" -ForegroundColor Red
            }
        } else {
            Write-Host "Alias $alias już istnieje dla użytkownika $username"
        }
    } else {
        Write-Host "Pomijanie użytkownika $($user.SamAccountName), ponieważ nie ma
poprawnego UserPrincipalName kończącego się na @$oldDomain" -ForegroundColor Yellow
    }
}
```

Skrypt wykonujemy z poziomu PowerShell po zmianie zmiennych `$oldDomain`, `$newDomain` i `$ou` na wartościach właściwych dla naszego środowiska. Skrypt musi być uruchomiony na serwerze z zainstalowaną funkcją RSAT, z dostępem do domeny, w której chcemy go uruchomić. Typowy scenariusz użycia to migracja domeny pocztowej: organizacja zmienia domenę SMTP i wszyscy użytkownicy w danej jednostce organizacyjnej mają dostać nowy adres jako alias, bez usuwania starego z listy `ProxyAddresses`.

Przykład:

```
Dodano alias smtp:jkowalski@zielona.example dla użytkownika jkowalski
Alias smtp:anowak@zielona.example już istnieje dla użytkownika anowak
Pomijanie użytkownika switek, ponieważ nie ma poprawnego UserPrincipalName kończącego
się na @ad.zielona.example
```

SMTP = Simple Mail Transfer Protocol: protokół wysyłania poczty · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **RSAT** = Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej · **alias** = nadaj poleceniu własny, krótszy skrót na czas sesji powłoki

OSTROŻNIE · NIEODWRACALNE

Wyszukiwanie frazy we wszystkich GPO

```
# Definiujemy wzorzec wyszukiwania na samej górze
$searchPattern = "SzukanaFraza"

Write-Host "`nTworzę folder na raporty GPO w bieżącym katalogu..."

# Próba pobrania ścieżki skryptu, jeśli brak to używamy bieżącego katalogu
if ($MyInvocation.MyCommand.Path) {
    $scriptFolder = Split-Path -Parent $MyInvocation.MyCommand.Path
} else {
    Write-Host "Nie wykryto ścieżki skryptu, używam bieżącego katalogu."
    $scriptFolder = (Get-Location).Path
}

$folder = Join-Path $scriptFolder "GPOReports"
New-Item -Path $folder -ItemType Directory -Force | Out-Null

Write-Host "Pobieram wszystkie obiekty GPO z domeny..."
$allgpos = Get-GPO -All
```

```
# Plik do zapisania raportu z listą i wynikiem w folderze skryptu
$reportFile = Join-Path $scriptFolder "GPO_export_and_scan_report.txt"

# Czyszczenie pliku jeśli istnieje
if (Test-Path $reportFile) {
    Remove-Item $reportFile
}

Write-Host "Eksportuję wszystkie GPO do osobnych plików XML oraz zapisuję listę do pliku raportu..."
Add-Content -Path $reportFile "Lista wyeksportowanych GPO:`n"
$allgpos | ForEach-Object {
    $path = Join-Path $folder ("{0}_{1}.xml" -f $_.DisplayName, $_.Id)
    Write-Host ("Eksportuję GPO: {0}" -f $_.DisplayName)
    Get-GPOReport -Guid $_.Id -ReportType Xml -Path $path
    Add-Content -Path $reportFile $_.DisplayName
}

# Dodaj pustą linię do rozdzielenia sekcji
Add-Content -Path $reportFile "`nWyniki wyszukiwania wzorca '$searchPattern':`n"

Write-Host "Szukam wzorca '$searchPattern' we wszystkich wyeksportowanych raportach..."
$patternMatches = Select-String -Path (Join-Path $folder "*.xml") -Pattern $searchPattern
if ($patternMatches -and $patternMatches.Count -gt 0) {
    $patternMatches | ForEach-Object { Add-Content -Path $reportFile $_.ToString() }
} else {
    Add-Content -Path $reportFile "Brak wzorca '$searchPattern' w żadnym z raportów GPO."
}

Write-Host "`nGotowe! Pełny raport w pliku: $reportFile"
```

Skrypt tworzy katalog `GPOReports` w folderze, z którego jest uruchamiany, eksportuje do niego pełny raport XML każdego GPO w domenie, po czym przeszukuje wszystkie wyeksportowane pliki w poszukiwaniu ustawionej na samej górze frazy. Uruchamiamy w PowerShell z uprawnieniami administratora, na kontrolerze domeny albo na maszynie z modułem `GroupPolicy` i dostępem do domeny. Typowe zastosowanie: sprawdzenie, w którym GPO (spośród często kilkudziesięciu) skonfigurowano konkretne ustawienie rejestru, nazwę

usługi albo ścieżkę skryptu logowania, bez ręcznego otwierania każdego GPO w konsoli zarządzania.

Przykład:

```
Pobieram wszystkie obiekty GPO z domeny...
Eksportuję GPO: Polityka haseł
Eksportuję GPO: Mapowanie dysków sieciowych
Eksportuję GPO: Konfiguracja proxy

Szukam wzorca 'SzukanaFraza' we wszystkich wyeksportowanych raportach...

Gotowe! Pełny raport w pliku: GPO_export_and_scan_report.txt
```

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **XML** = eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

TYLKO ODCZYT

Pobieranie klucza BitLocker z AD

```
$objComputer = Get-ADComputer NazwaKomputera
$Bitlocker_Objects = Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'}
-SearchBase $objComputer.DistinguishedName -Properties 'msFVE-RecoveryPassword'
$Bitlocker_Objects
```

Uruchamiamy jako user z uprawnieniami do odczytu atrybutu `msFVE-RecoveryPassword`: w wielu środowiskach domyślnie ograniczonego do administratorów domeny albo do wydzielonej grupy service desk. **Pojęcie: msFVE-RecoveryInformation.** Obiekt potomny konta komputera w Active Directory, tworzony automatycznie przy włączeniu BitLockera z kopią zapasową klucza do AD: jeden komputer może mieć kilka takich obiektów, po jednym na każde szyfrowanie/odszyfrowanie wolumenu w historii.

Przykład:

```
DistinguishedName : CN={a1b2c3d4-
...},CN=NazwaKomputera,OU=Komputery,DC=ad,DC=zielona,DC=example
msFVE-RecoveryPassword : 123456-654321-123456-654321-123456-654321-123456-654321
```

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

TYLKO ODCZYT

Pobieranie klucza BitLocker: wariant z pytaniem o komputer i poświadczenia

```
# Pobieranie nazwy komputera
$ComputerName = Read-Host "Nazwa komputera [$env:COMPUTERNAME]"
if ([string]::IsNullOrWhiteSpace($ComputerName)) {
    $ComputerName = $env:COMPUTERNAME
}

# Pobieranie poświadczeń domenowych
$Credentials = Get-Credential -Message "Poświadczenia do domeny AD"

# Wyszukanie odpowiedniego komputera
$objComputer = Get-ADComputer $ComputerName -Credential $Credentials

# Pobranie kluczy BitLocker z dodatkowymi polami
$Bitlocker_Object = Get-ADObject `
    -Filter {objectclass -eq 'msFVE-RecoveryInformation'} `
    -SearchBase $objComputer.DistinguishedName `
    -Properties 'msFVE-RecoveryPassword', 'msFVE-RecoveryGuid', 'msFVE-VolumeGuid',
'whenCreated' `
    -Credential $Credentials |
    Sort-Object whenCreated -Descending |
    Select-Object `
        @{Name = 'CN'; Expression = { $ComputerName }},
        @{Name = 'Bitlocker Password'; Expression = { $_.'msFVE-RecoveryPassword' }},
        @{Name = 'Volume GUID'; Expression = { $_.'msFVE-VolumeGuid' }},
        @{Name = 'Recovery GUID'; Expression = { $_.'msFVE-RecoveryGuid' }},
        @{Name = 'Created'; Expression = { $_.whenCreated }}

# Wypisanie danych
$Bitlocker_Object | Format-Table -AutoSize
```

Rozszerzamy poprzedni wariant o pytanie interaktywne o nazwę komputera (z domyślną wartością bieżącego hosta) i o osobne poświadczenia domenowe, oraz sortujemy wynik po dacie utworzenia malejąco: jeśli komputer miał kilka cykli szyfrowania, najnowszy, aktualnie obowiązujący klucz znajdzie się na górze listy.

Przykład:

```
CN            Bitlocker Password                                          Volume
GUID                          Recovery GUID                          Created
--            ------------------                                          -----------
                          -------------                          -------
NazwaKomputera 123456-654321-123456-654321-123456-654321-123456-654321    {b2c3d4e5-
...}                       {c3d4e5f6-...}                        24.09.2026 09:12:41
```

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **CN** = Common Name: główna nazwa w certyfikacie, np. adres serwera · **GUID** = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera

ZMIENIA SYSTEM

Manualne wymuszenie synchronizacji AD on-premises z Entra ID

```
Start-ADSyncSyncCycle -PolicyType Delta
```

Komendę uruchamiamy jako Administrator w PowerShell na serwerze z zainstalowanym i skonfigurowanym Azure AD Connect (obecnie Microsoft Entra Connect, w Zielonej `sync01`), ze skonfigurowanymi odpowiednimi połączeniami do Entra ID. Cykl `Delta` synchronizuje wyłącznie zmiany od ostatniej synchronizacji: dużo szybszy niż pełny cykl i wystarczający w zdecydowanej większości przypadków, gdy trzeba natychmiast przepchnąć pojedynczą zmianę (na przykład świeżo dodany alias SMTP ze skryptu wyżej) bez czekania na najbliższy zaplanowany cykl synchronizacji.

Przykład:

```
Result
------
Success
```

Pełny cykl (`-PolicyType Initial`) przelicza cały zestaw obiektów od nowa: używamy go rzadko, głównie po zmianie reguł synchronizacji, nie jako rutynowe polecenie.

Uważaj

- `Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'}` zwraca puste wyniki, jeśli konto komputera nigdy nie zapisało klucza do AD: dotyczy to maszyn z BitLockerem skonfigurowanym bez zasady grupy wymuszającej kopię zapasową klucza do katalogu.
- Skrypt dodający aliasy SMTP modyfikuje atrybuty kont w produkcyjnym katalogu: pierwsze uruchomienie warto wykonać na pojedynczym koncie testowym albo z dopisanym na sztywno filtrem ograniczającym `$users` do jednego obiektu, zanim puścimy go na całe OU.
- `Start-ADSyncSyncCycle -PolicyType Initial` na dużym katalogu potrafi trwać wyraźnie dłużej niż `Delta` i obciążać kontroler domeny odczytem: nie uruchamiamy go odruchowo zamiast `Delta`.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **SMTP** = Simple Mail Transfer Protocol: protokół wysyłania poczty · **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery

Z życia wzięte

Z ŻYCIA WZIĘTE

Pan Wojtek pyta w listopadzie, przed corocznym audytem, na których stacjach roboczych BitLocker w ogóle zapisał klucz odzyskiwania do katalogu. Odpalamy skrypt pobierający klucz z AD dla kilkunastu komputerów po kolei i dla trzech z nich `Get-ADObject` zwraca pustą listę. Okazuje się, że te trzy laptopy dostały szyfrowanie jeszcze przed włączeniem zasady grupy wymuszającej kopię zapasową klucza, więc klucz istnieje tylko lokalnie, nigdy nie trafił do Active Directory.

Zanim zaczniemy

Wszystkie skrypty na tej stronie wymagają modułu `ActiveDirectory`, dostarczanego przez funkcję RSAT (Remote Server Administration Tools): na stacji roboczej instalujemy go poleceniem `Add-WindowsFeature RSAT-AD-PowerShell` (na serwerze) albo przez `Add-WindowsCapability -Online -Name Rsat.ActiveDirectory...` (na kliencie Windows 10/11), opisane szerzej na stronie Instalacja i usuwanie oprogramowania. Skrypt audytujący DNS wymaga dodatkowo przystawki RSAT DNS, a skrypt przeszukujący GPO wymaga modułu `GroupPolicy` z RSAT GPMC. Wszystkie skrypty uruchamiamy w PowerShell z uprawnieniami odpowiednimi do zakresu odczytu, jakiego wymaga dana operacja: audyt grup i DNS wystarczy zwykłe konto z prawem odczytu katalogu, pobranie klucza BitLocker wymaga uprawnień do odczytu atrybutu `msFVE-RecoveryPassword`, a synchronizacja

z Entra ID wymaga uprawnień administratora na serwerze z rolą Azure AD Connect.

Po co to istnieje

Audyt Active Directory ma jedną wspólną cechę we wszystkich sześciu skryptach powyżej: dane, których szukamy, technicznie istnieją w katalogu, ale żadna standardowa konsola graficzna (Active Directory Users and Computers, konsola zarządzania GPO) nie pokazuje ich w formie gotowej do przeszukania masowo: trzeba by klikać obiekt po obiekcie, GPO po GPO, strefę po strefie. PowerShell z modułem `ActiveDirectory` zamienia to z zadania ręcznego, powtarzalnego i podatnego na pominięcie czegoś, w jednorazowy skrypt, który przechodzi przez wszystko naraz i zwraca gotowy raport.

Jak to działa

Skrypt audytu grupy zagnieżdżonej rozwiązuje konkretny problem techniczny `Get-ADGroupMember`: to polecenie domyślnie odpytuje tylko bieżącą domenę i nie podąża automatycznie za członkami z innych domen tego samego lasu: zwraca dla nich błąd albo pomija ich całkowicie, w zależności od wersji. Rozbicie `DistinguishedName` członka po wzorcu `DC=` i zbudowanie z tego osobnej ścieżki LDAP pozwala ustalić, do jakiej domeny naprawdę należy dany obiekt, i odpytać właściwy kontroler domeny zamiast zakładać, że wszystko leży w tej samej domenie co grupa nadrzędna.

Wyszukiwanie frazy w GPO nie odpytuje samych zasad grupy bezpośrednio: `Get-GPOReport -ReportType Xml` generuje pełny, płaski zrzut XML każdego GPO (ustawienia, filtry zabezpieczeń, powiązania), a dopiero `Select-String` przeszukuje tekstowo te wyeksportowane pliki. To dwuetapowe podejście istnieje, bo GPO nie ma wbudowanego mechanizmu pełnotekstowego wyszukiwania po swojej zawartości: jedynym pewnym sposobem sprawdzenia, czy dana fraza (nazwa usługi, ścieżka rejestru, adres serwera) występuje gdziekolwiek w polityce, jest zrzucenie wszystkiego do formatu tekstowego i przeszukanie go standardowymi narzędziami.



Kazde GPO trafia do osobnego pliku XML, dopiero potem Select-String szuka w nich frazy (kliknięcie otwiera pełny rozmiar)

Częste błędy

Brak przystawki RSAT DNS przy próbie audytu DNS. `Get-DnsServerZone` zwraca błąd `The term 'Get-DnsServerZone' is not recognized`: moduł `DnsServer` (część RSAT DNS) nie instaluje się razem z modułem `ActiveDirectory`, trzeba go dodać osobno.

Uruchomienie skryptu SMTP na całym katalogu bez wcześniejszego testu na jednym koncie. Skrypt zmienia atrybuty realnych kont produkcyjnych: literówka w `$newDomain` albo błędnie zdefiniowany `$ou` obejmujący więcej użytkowników niż zamierzono, oznacza masową, trudną do szybkiego cofnięcia zmianę na wielu kontach naraz.

Oczekiwanie klucza BitLocker dla komputera, który nigdy nie zapisał go do AD. Pusty wynik `Get-ADObject` nie zawsze oznacza błąd skryptu: równie często oznacza, że zasada grupy wymuszająca kopię zapasową klucza do katalogu nie była włączona w momencie szyfrowania tego konkretnego dysku.

□□ Ćwiczenia

> Ćwiczenia poniżej wymagają dostępu do testowej domeny Active Directory z zainstalowanym modułem RSAT: nie wykonujemy ich na domenie produkcyjnej.

Ćwiczenie 1: rozbicie DistinguishedName po domenie

```
$przykladowyDN = "CN=Jan Kowalski,OU=Users,DC=filia,DC=ad,DC=zielona,DC=example"
$przykladowyDN -split '(?=DC=)', 2
```

Sprawdzamy, jak dokładnie wyrażenie regularne z fiszki audytu grup rozdziela DistinguishedName na część obiektu i część domeny.

Odpowiedź

Wynikiem są dwa elementy: `CN=Jan Kowalski,OU=Users,` oraz `DC=filia,DC=ad,DC=zielona,DC=example`. Pozytywne wyprzedzenie `(?=DC=)` dzieli napis dokładnie przed pierwszym wystąpieniem `DC=`, nie konsumując samego dopasowanego fragmentu: dzięki temu drugi element zawiera kompletną, gotową do użycia w `[adsi]` ścieżkę domeny, bez potrzeby ręcznego doklejania z powrotem obciętego prefiksu.

Ćwiczenie 2: bezpieczne przetestowanie skryptu SMTP

```
$testowyUser = Get-ADUser -Filter * -SearchBase "SciezkaDoOU" -Properties UserPrincipalName |
Select-Object -First 1
$testowyUser.UserPrincipalName
```

Zanim uruchomimy pełny skrypt dodawania aliasów SMTP na całym OU, wyciągamy z niego pojedynczego, przykładowego użytkownika i sprawdzamy ręcznie, czy filtr `-SearchBase` faktycznie obejmuje tylko zamierzony zakres.

Odpowiedź

Sprawdzenie pojedynczego wyniku przed uruchomieniem pętli na całym zbiorze to praktyczna metoda uniknięcia masowej, niezamierzonej zmiany: jeśli `$testowyUser` pochodzi z niewłaściwej jednostki organizacyjnej albo ma nieoczekiwany `UserPrincipalName`, oznacza to błąd w wartości `$ou` jeszcze przed uruchomieniem właściwego skryptu na wszystkich kontach.

Pytania kontrolne

1. Dlaczego skrypt audytu GPO eksportuje każdą politykę do osobnego pliku XML zamiast przeszukiwać GPO bezpośrednio przez moduł GroupPolicy?

Odpowiedź

Moduł `GroupPolicy` nie udostępnia polecenia do pełnotekstowego przeszukania zawartości ustawień GPO: `Get-GPOReport` generuje kompletny, płaski zrzut ustawień w formacie XML (albo HTML), który dopiero wtedy da się przeszukać ogólnym narzędziem tekstowym, takim jak `Select-String`. To pośredni krok wymuszony brakiem bezpośredniego API do wyszukiwania w treści polityk.

2. Skrypt pobierający klucz BitLocker zwraca pusty wynik dla komputera, o którym wiadomo, że ma włączony BitLocker. Jaka jest najbardziej prawdopodobna przyczyna, niezwiązana z samym skryptem?

Odpowiedź

BitLocker mógł zostać włączony bez skonfigurowanej wcześniej zasady grupy wymuszającej zapis klucza odzyskiwania do Active Directory: w takim przypadku klucz nigdy nie trafił do obiektu `msFVE-RecoveryInformation`, bo taki obiekt w ogóle nie powstał. Sam skrypt działa poprawnie, po prostu przeszukuje katalog, w którym nie ma czego znaleźć.

Powiązane: Zadania zaplanowane, usługi i procesy · Poświadczenia i bezpieczne hasła w skryptach · Instalacja i usuwanie oprogramowania · Konta usługowe MSA i gMSA · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt · Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID

Źródła: `Get-Help Get-ADObject` · `Get-Help Get-GPOReport` · dokumentacja Microsoft Learn, „Active Directory module for Windows PowerShell" i „Microsoft Entra Connect Sync"