Active Directory od zera: pierwszy i drugi kontroler domeny

Typ: procedura **Dotyczy: Active Directory Domain Services, Windows Server 2022 / 2025**

Czas: ~90 min

Efekt: dwa kontrolery domeny, `dc01` i `dc02`, obsługujące jedną domenę Active Directory `ad.zielona.example`, replikujące się nawzajem i gotowe przyjmować logowania komputerów Zielonej z dowolnej lokalizacji. Od tego zaczyna się cała reszta rozdziału o infrastrukturze Windows.

ZAŁOŻENIA SCENARIUSZA

`dc01` i `dc02` stoją w VLAN 10 w centrali, a domena ma jedną witrynę AD (`Default-First-Site-Name`), więc magazyn w Swarzędzu korzysta z nich przez sieć centrali za `fw01`. Przy magazynie jako osobnej lokalizacji z tunelem (IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy) rozważamy osobną witrynę AD z podsiecią 10.20.30.0/24; tutaj tego nie robimy.

Skróty użyte na tej stronie (18)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD DS	Active Directory Domain Services: rola Windows Server uruchamiająca właściwą usługę katalogową Active Directory na kontrolerze domeny
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
FQDN	Fully Qualified Domain Name: pełna nazwa hosta razem z domeną, np. docker01.ad.zielona.example
FSMO	Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz

Skrót	Co znaczy
GPMC	Group Policy Management Console: konsola do zarządzania politykami GPO w domenie
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
mDNS	Multicast DNS: sposób, w którym urządzenia w jednej sieci lokalnej ogłaszają swoją nazwę (np. esp01.local) zapytaniami na adres multicast, bez serwera DNS; nie przechodzi między podsieciami
NetBIOS	Network Basic Input/Output System: stara warstwa nazw w sieciach Windows; nazwa komputera w niej ma najwyżej 15 znaków, co ogranicza długość nazwy punktu dostępu klastra
PDC	Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł
RDS	Remote Desktop Services: zdalne pulpity i aplikacje Windows Server
RID	Relative Identifier: końcowa, unikalna w domenie część identyfikatora bezpieczeństwa (SID) każdego konta; RID Master to kontroler domeny rozdzielający pule tych numerów
SYSVOL	system volume: udział sieciowy na kontrolerze domeny z politykami GPO i skryptami logowania, replikowany między kontrolerami tak jak reszta katalogu
TLD	Top Level Domain: najwyższy poziom nazwy domeny internetowej, część po ostatniej kropce, np. `.com` albo `.example`
UPN	User Principal Name: login w formie adresu, np. jan.nowak@zielona.example
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Pojęcia

Pojęcie: las. Najwyższy poziom struktury Active Directory. Jedna albo więcej domen, które dzielą wspólny schemat katalogu, wspólną konfigurację i wspólny katalog globalny. Las jest też granicą zaufania: administrator jednej domeny w lesie automatycznie nie zarządza inną domeną w innym lesie, dopóki ktoś nie skonfiguruje osobnego zaufania między lasami.

Pojęcie: domena. Grupa komputerów i kont użytkowników zarządzana z jednego miejsca, z jednym wspólnym hasłem do wielu systemów zamiast osobnego konta na każdej maszynie. Zielona ma jedną domenę, `ad.zielona.example`, w jednym lesie.

Pojęcie: kontroler domeny. Serwer trzymający bazę Active Directory: konta, komputery, grupy i uprawnienia całej domeny. `dc01` i `dc02` to dwa kontrolery tej samej domeny Zielonej,

każdy z pełną kopią tej samej bazy.

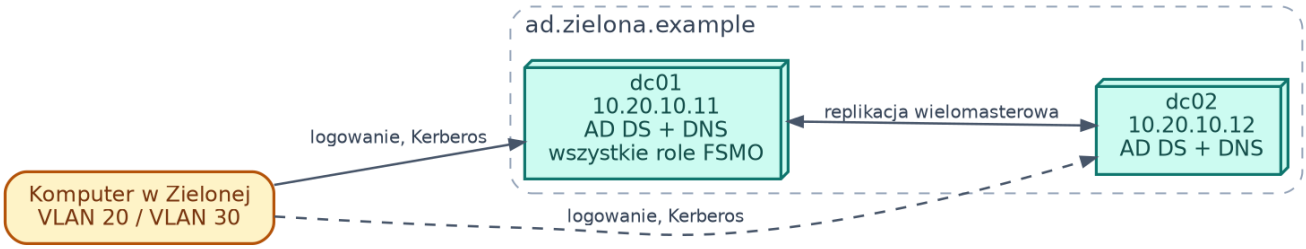
Pojęcie: poziom funkcjonalności. Ustawienie lasu i osobno domeny, które mówi, jak starą wersję Windows Server dopuszczamy jeszcze jako kontroler domeny. Im wyższy poziom, tym nowsze funkcje Active Directory są dostępne, ale tym starszy system nie wejdzie już do tej domeny jako kontroler. Poziomu nie da się obniżyć bez poważnych ograniczeń, więc wybieramy go raz, świadomie.

Pojęcie: FSMO (Flexible Single Master Operations). Pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz, żeby uniknąć sprzeczności: dwa kontrolery nie mogą jednocześnie nadawać tych samych identyfikatorów kont. Dwa zadania (Schema Master, Domain Naming Master) dotyczą całego lasu, trzy (PDC Emulator, RID Master, Infrastructure Master) dotyczą jednej domeny. Pierwszy kontroler domeny w nowym lesie dostaje automatycznie wszystkie pięć ról.

Pojęcie: katalog globalny (Global Catalog). Kontroler domeny oznaczony jako katalog globalny trzyma dodatkowo częściową, ale przeszukiwalną kopię obiektów z każdej domeny całego lasu, nie tylko własnej. W lesie z jedną domeną, tak jak w Zielonej, różnica jest mniej widoczna, ale logowanie kontem UPN (`jan.nowak@ad.zielona.example`) i wyszukiwanie w całym katalogu i tak korzystają z tej roli.

Pojęcie: DSRM (Directory Services Restore Mode). Specjalny tryb startu kontrolera domeny, w którym usługa Active Directory w ogóle się nie uruchamia. Wchodzimy w niego, gdy baza katalogu na danym kontrolerze jest uszkodzona i trzeba ją naprawić albo przywrócić z kopii, zanim serwer znów zacznie odpowiadać na logowania. Hasło do konta administratora DSRM ustawiamy raz, przy tworzeniu każdego kontrolera domeny, i trzymamy osobno od haseł domenowych.

Pojęcie: replikacja. Automatyczna, wielomasterowa synchronizacja bazy Active Directory między kontrolerami domeny. Wielomasterowa znaczy, że zmianę (nowego użytkownika, zmienione hasło) można zapisać na dowolnym kontrolerze, a on sam rozgłosi ją do reszty; nie ma jednego „głównego" kontrolera do zapisu, jak bywa w niektórych bazach danych.



Dwa kontrolery domeny ad.zielona.example replikujace sie nawzajem, komputer Zielonej loguje sie do dowolnego z nich (kliknięcie otwiera pełny rozmiar)

Zanim zaczniemy

> **Z ŻYCIA WZIĘTE**
>
> Tomek, drugi tydzień pracy, dostaje od starszego administratora zadanie: postawić w odizolowanej sieci testowej domenę bliźniaczą do produkcyjnej Zielonej, krok po kroku, zanim w ogóle dotknie czegokolwiek na prawdziwych `dc01` i `dc02`. „Jak coś spartolisz na testowej maszynie, nikt tego nie zauważy poza tobą. Jak spartolisz na produkcji, zauważy to sto osiemdziesiąt osób naraz" - słyszy w odpowiedzi na pytanie, po co to całe ćwiczenie.

Zakładamy nowy las Active Directory od zera na serwerze, który jeszcze nie należy do żadnej domeny, i dokładamy mu drugiego bliźniaka. W Zielonej odpowiadają temu `dc01` (10.20.10.11) i `dc02` (10.20.10.12), oba Windows Server 2022, w sieci serwerowej VLAN 10 (`10.20.10.0/24`).

Wymaganie	Uwaga
Świeży Windows Server, jeszcze bez roli AD DS	zarówno na przyszłym `dc01`, jak i na przyszłym `dc02`
Konto lokalnego administratora na obu serwerach	do momentu utworzenia lasu nie ma jeszcze żadnego konta domenowego
Statyczny adres IP dla każdego serwera	kontroler domeny z adresem przydzielanym przez DHCP to źródło problemów z DNS po każdej zmianie adresu
Zarezerwowana nazwa FQDN domeny	w Zielonej `ad.zielona.example`, poddomena domeny publicznej `zielona.example`, którą firma faktycznie posiada
Łączność sieciowa między przyszłymi `dc01` i `dc02`	replikacja wymaga otwartych portów RPC, LDAP, Kerberos i DNS między obiema maszynami

> Nazwy domeny i NetBIOS ustawiamy raz, na starcie. Zmiana nazwy domeny istniejącego lasu jest możliwa (`rendom`), ale to osobna, dużo bardziej ryzykowna procedura, nie temat tej strony. Warto dobrze przemyśleć nazwę, zanim uruchomimy `Install-ADDSForest`.

Przebieg

1. Przygotowanie dc01: nazwa i adres IP

Ustawiamy statyczny adres w sieci serwerowej i nazwę hosta, zanim zaczniemy instalować cokolwiek:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.20.10.11 -PrefixLength 24 -
DefaultGateway 10.20.10.1
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 127.0.0.1
Rename-Computer -NewName "dc01" -Restart
```

Adres serwera DNS klienta ustawiamy od razu na `127.0.0.1`: po instalacji roli AD DS ten sam serwer będzie też serwerem DNS domeny, więc od początku każe sobie pytać samego siebie zamiast zewnętrznego DNS. Instalujemy też dostępne aktualizacje systemu i restartujemy jeszcze raz, zanim przejdziemy dalej: kontroler domeny lepiej zakładać na w miarę świeżym systemie, procedurę aktualizacji opisaliśmy osobno na stronie Windows Update z wiersza poleceń.

Weryfikujemy adres i nazwę:

```
ipconfig /all
```

Przykład:

```
Nazwa hosta . . . . . . . . . . . . : dc01
Karta Ethernet Ethernet:
   Adres IPv4. . . . . . . . . . . . : 10.20.10.11(Preferowane)
   Maska podsieci . . . . . . . . . . : 255.255.255.0
   Brama domyślna . . . . . . . . . . : 10.20.10.1
   Serwery DNS . . . . . . . . . . . . : 127.0.0.1
```

2. Instalacja roli Active Directory Domain Services

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

`-IncludeManagementTools` dokłada razem z rolą przystawki administracyjne (konsolę Active Directory Users and Computers, moduł PowerShell `ActiveDirectory`, GPMC), bez których i tak zaraz będziemy zarządzać świeżo utworzoną domeną. Sama instalacja roli jeszcze niczego w sieci nie zmienia: dopiero kolejny krok, `Install-ADDSForest`, faktycznie zakłada las i promuje ten serwer na kontroler domeny.

Przykład:

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Grup...
```

3. Utworzenie nowego lasu i domeny: Install-ADDSForest

```
Install-ADDSForest `
    -DomainName "ad.zielona.example" `
    -DomainNetbiosName "ZIELONA" `
    -DomainMode WinThreshold `
    -ForestMode WinThreshold `
    -InstallDns:$true `
    -SafeModeAdministratorPassword (Read-Host -AsSecureString -Prompt "Haslo DSRM dla dc01") `
    -Force:$true
```

`-DomainName` to pełna nazwa FQDN nowej domeny, `-DomainNetbiosName` to jej krótki, stary format sprzed DNS, używany dziś głównie w loginach `ZIELONA\jan.nowak`. `-InstallDns:$true` instaluje razem z lasem rolę serwera DNS na tym samym serwerze: w małej firmie jak Zielona to naturalny wybór, bo i tak potrzebujemy DNS zintegrowanego z AD, opisanego osobno na stronie DNS w domenie: strefy, rekordy, przekazywanie.

`-DomainMode` i `-ForestMode` na `WinThreshold` ustawiają poziom funkcjonalności na Windows Server 2016. To najwyższy poziom, na którym mogą pracować kontrolery z Windows Server 2019 i 2022, bo te wersje nie wprowadziły własnych poziomów. Windows Server 2025 wprowadził nowy poziom Windows Server 2025, ale dopuszcza on jako kontrolery wyłącznie Windows Server 2025, więc dla `dc01` i `dc02` z Windows Server 2022 `WinThreshold` jest właściwym wyborem. Poziom 2016 jest też minimum, przy którym do domeny da się dołożyć kontroler z Windows Server 2025. Plan przejścia na nowszy poziom opisuje strona Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo.

Polecenie samo sprawdza wymagania wstępne, zanim cokolwiek zmieni, i prosi o potwierdzenie:

Przykład:

```
Sprawdzanie wymagan wstepnych...
Wszystkie testy zakonczone powodzeniem. Mozna kontynuowac instalacje.

Podaj i potwierdz haslo trybu przywracania uslug katalogowych (DSRM):
```

Po zatwierdzeniu instalacja tworzy las, domenę, bazę Active Directory i strefę DNS, po czym sama uruchamia ponownie serwer, bo `-NoRebootOnCompletion` nie zostało podane. Po restarcie `dc01` wraca już jako pierwszy kontroler domeny `ad.zielona.example`, z wszystkimi pięcioma rolami FSMO na sobie.

4. Przygotowanie i promowanie dc02

Na drugim serwerze powtarzamy przygotowanie z kroku 1 (statyczny adres `10.20.10.12`, nazwa `dc02`), z jedną różnicą: adres DNS klienta ustawiamy od razu na `dc01`, bo w chwili startu `dc02` żadnego własnego DNS jeszcze nie ma:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.20.10.12 -PrefixLength 24 -
DefaultGateway 10.20.10.1
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.20.10.11
Rename-Computer -NewName "dc02" -Restart
```

Instalujemy rolę tak samo jak na `dc01`:

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Promujemy serwer do istniejącej już domeny, zamiast zakładać nową:

```
$Poswiadczenia = Get-Credential -UserName "ZIELONA\Administrator" -Message "Poswiadczenia
administratora domeny ad.zielona.example"

Install-ADDSDomainController `
    -DomainName "ad.zielona.example" `
    -Credential $Poswiadczenia `
    -InstallDns:$true `
    -SafeModeAdministratorPassword (Read-Host -AsSecureString -Prompt "Haslo DSRM dla dc02") `
    -Force:$true
```

`-Credential` przyjmuje konto z uprawnieniami do dołączania kontrolerów domeny, zwykle administratora domeny; samo konto lokalnego administratora serwera tu nie wystarczy, bo

operacja dotyczy już istniejącej domeny, nie tylko lokalnej maszyny. Hasło DSRM dla `dc02` jest osobnym hasłem od hasła DSRM `dc01`: każdy kontroler domeny ma własne. Po zakończeniu i automatycznym restarcie `dc02` staje się drugim, pełnoprawnym kontrolerem domeny `ad.zielona.example`, na razie bez żadnej roli FSMO, bo wszystkie zostały na `dc01`.

> Przenoszenie ról FSMO na `dc02` (na przykład, gdyby `dc01` miał zejść do serwisu na dłużej) robimy poleceniem `Move-ADDirectoryServerOperationMasterRole`, ale to już osobna operacja, nie część samego stawiania kontrolera. Opisuje ją strona Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie.

Weryfikacja

Sprawdzamy ogólny stan zdrowia obu kontrolerów, najlepiej po pełnym cyklu replikacji od promocji `dc02` (kilka do kilkunastu minut):

```
dcdiag /v
```

Uruchamiamy na każdym kontrolerze osobno. `/v` (verbose) rozszerza standardowy zestaw testów (łączność, replikacja, DNS, role FSMO, SYSVOL) o dodatkowe szczegóły diagnostyczne, przydatne, gdy któryś z podstawowych testów akurat zawiedzie i trzeba wiedzieć dlaczego, a nie tylko że.

Sprawdzamy stan samej replikacji między `dc01` i `dc02`:

```
repadmin /replsummary
```

Przykład:

```
Zrodlo DSA          largest delta    failures/total   %%   error
dc01                 00m:03s            0 /   2    0
dc02                 00m:05s            0 /   2    0

DSA docelowe          largest delta    failures/total   %%   error
dc01                 00m:03s            0 /   2    0
dc02                 00m:05s            0 /   2    0
```

Kolumna `largest delta` pokazuje, ile czasu minęło od ostatniej udanej replikacji z danym partnerem; `failures/total` przy zerze błędów znaczy, że wszystkie próby replikacji się powiodły.

Sprawdzamy, który kontroler trzyma które role FSMO:

```
netdom query fsmo
```

Przykład:

```
Schema Master               dc01.ad.zielona.example
Domain naming Master        dc01.ad.zielona.example
PDC                         dc01.ad.zielona.example
RID Pool Manager            dc01.ad.zielona.example
Infrastructure Master       dc01.ad.zielona.example

Polecenie zostalo wykonane pomyslnie.
```

Sprawdzamy oba kontrolery z poziomu modułu `ActiveDirectory`:

```
Get-ADDomainController -Filter *
```

Przykład:

```
Name  Site                 IPv4Address   OperatingSystem        IsGlobalCatalog
----  ----                 -----------   ---------------        ---------------
dc01  Default-First-Site-Name  10.20.10.11   Windows Server 2022    True
dc02  Default-First-Site-Name  10.20.10.12   Windows Server 2022    True
```

Obie maszyny powinny pojawić się na liście, obie z `IsGlobalCatalog : True`: przy pierwszym kontrolerze dzieje się to automatycznie, przy drugim `Install-ADDSDomainController` też domyślnie włącza tę rolę, o ile nie wyłączymy jej wprost parametrem `-NoGlobalCatalog`.

Dlaczego nie .local

Domena Zielonej nazywa się `ad.zielona.example`, poddomena `zielona.example`, którą firma faktycznie zarejestrowała i posiada, a nie `zielona.local` czy `ad.local`. To nie estetyka, tylko dwa konkretne problemy, które `.local` sprowadza na kontroler domeny.

Po pierwsze, `.local` jest zarezerwowany dla mDNS (`multicast DNS`, mechanizmu, którym urządzenia w tej samej sieci lokalnej same się sobie ogłaszają, bez centralnego serwera DNS). Komputer, telefon albo drukarka próbujące rozwiązać nazwę kończącą się na `.local` najpierw czekają na odpowiedź mDNS, a dopiero potem pytają zwykły DNS, co potrafi zauważalnie wydłużać czas logowania i inne operacje domenowe, szczególnie na urządzeniach Apple.

Po drugie, publiczne urzędy certyfikacji od listopada 2015 roku nie wystawiają już certyfikatów dla nazw w domenach, których nikt nie może wykazać jako swoich w internecie, a `.local` nigdy nie

jest taką domeną. Każda usługa Zielonej, która kiedyś będzie chciała publicznie zaufanego certyfikatu na nazwę wewnętrzną (na przykład serwer RDS albo bramkę VPN), utyka na tym problemie, jeśli nazwa domeny kończy się na `.local`. `zielona.example` jako realnie zarejestrowana domena (a w prawdziwym świecie każdy odpowiednik `zielona.example` z realnym TLD) tego ograniczenia nie ma: `ad.zielona.example` to zwykła poddomena, dla której da się wystawić poprawny certyfikat, gdyby taka potrzeba się pojawiła.

Kopia stanu systemu kontrolera domeny

Baza Active Directory, `SYSVOL` z politykami GPO i rejestr systemowy razem tworzą tak zwany stan systemu (`system state`). Zwykła kopia plików tego nie obejmuje w spójny sposób, bo baza `ntds.dit` jest cały czas otwarta przez usługę AD DS. Kopię wykonujemy narzędziem `wbadmin`, które potrafi zrobić spójny zrzut mimo działającej usługi:

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

`-backupTarget` wskazuje dysk albo wolumen, na którym ma powstać kopia, koniecznie inny niż dysk systemowy `C:`; `-quiet` pomija pytania kontrolne, przydatne przy uruchamianiu z harmonogramu zadań. Pełną procedurę w Zielonej, z wysyłką kopii restic na `bkp01`, retencją i odtwarzaniem, opisuje strona Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM. Kopię stanu systemu wykonujemy na obu kontrolerach domeny osobno, bo każdy ma własną, choć zreplikowaną, bazę na dysku, i to właśnie ona jest tu najważniejsza: to jedyny sposób na przywrócenie kontrolera domeny do działania bez stawiania go od zera, gdyby baza uległa uszkodzeniu, a nie samej maszyny wirtualnej.

> Backup samej maszyny wirtualnej na poziomie hiperwizora (migawka, kopia dysków) też działa dla kontrolera domeny, o ile jest wykonywany narzędziem świadomym Active Directory (`VSS writer` dla AD DS) - inaczej ryzykujemy przywrócenie bazy w niespójnym stanie, znane jako `USN rollback`.

Wycofanie zmian

Jeśli `dc02` okazał się niepotrzebny albo coś poszło nie tak i chcemy go zdjąć z domeny, obniżamy go z powrotem do zwykłego serwera:

```
Uninstall-ADDSDomainController -Force
```

Bez dodatkowych parametrów polecenie zakłada, że w domenie zostaje jeszcze co najmniej jeden kontroler, i samo poprosi o hasło nowego lokalnego administratora zdegradowanego serwera. Jeśli demontujemy naprawdę ostatni kontroler całej domeny (rzadka sytuacja, bo w Zielonej to oznaczałoby likwidację domeny), dokładamy `-LastDomainControllerInDomain`, a jeśli ten kontroler wciąż trzyma role FSMO, których nikt jeszcze nie przeniósł, dokładamy `-DemoteOperationMasterRole`, żeby degradacja mimo to poszła do końca.

Cofnięcie całego lasu, czyli zdjęcie roli AD DS z jedynego kontrolera nowo założonej domeny, wykonujemy tym samym poleceniem na tej jednej maszynie; po demontażu domena `ad.zielona.example` przestaje istnieć, a serwer wraca do bycia zwykłym, niezależnym Windows Server.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
`Install-ADDSForest` kończy się błędem o nierozwiązywalnej nazwie domeny	serwer nie ma jeszcze ustawionego statycznego adresu i poprawnego DNS klienta	wracamy do kroku 1, sprawdzamy `ipconfig /all`, powtarzamy instalację
`dcdiag /v` na `dc02` zgłasza błędy testu `Replications` zaraz po promocji	replikacja jeszcze nie zdążyła się w pełni zsynchronizować	czekamy kilkanaście minut i sprawdzamy ponownie `repadmin /replsummary`, zanim uznamy to za realny problem
`Install-ADDSDomainController` odrzuca podane poświadczenia	konto w `-Credential` nie ma uprawnień do dołączania kontrolerów domeny (wymagana grupa Domain Admins albo delegacja)	logujemy się kontem faktycznego administratora domeny, nie lokalnym administratorem serwera
Po restarcie `dc02` komputery w biurze nie widzą domeny	klient DNS na stacjach roboczych wciąż wskazuje na router zamiast na `dc01`/`dc02`	poprawiamy ustawienia DHCP albo klienta DNS, szerzej na stronie DNS w domenie: strefy, rekordy, przekazywanie
`netdom query fsmo` pokazuje różne kontrolery dla różnych ról po ręcznym przenoszeniu	to normalne po świadomym przeniesieniu pojedynczej roli, nie błąd	sprawdzamy, czy rozkład ról odpowiada temu, co faktycznie planowaliśmy, zamiast zakładać, że wszystkie pięć musi trzymać jeden serwer

□□ Ćwiczenia

1. Dlaczego `Install-ADDSForest` dla Zielonej używa `-ForestMode WinThreshold`, skoro `dc01` i `dc02` to Windows Server 2022, wydany kilka lat po Windows Server 2016?

Odpowiedź

Windows Server 2019 i 2022 nie wprowadziły własnych poziomów funkcjonalności i używają poziomu 2016 (`WinThreshold`) jako najwyższego. Nowy poziom Windows Server 2025 istnieje, ale wymaga, żeby wszystkie kontrolery miały Windows Server 2025, więc `dc01` i `dc02` z Windows Server 2022 by go nie obsłużyły. Poziom 2016 nie ogranicza niczego, czego Zielona dziś potrzebuje, i dopuszcza dołożenie kontrolera z Windows Server 2019, 2022 albo 2025.

1. `dc02` promujemy poleceniem `Install-ADDSDomainController`, nie `Install-ADDSForest`. Co by się stało, gdybyśmy przez pomyłkę użyli na `dc02` tego drugiego polecenia z tą samą nazwą domeny `ad.zielona.example`?

Odpowiedź

`Install-ADDSForest` zakłada zupełnie nowy las i nową domenę, więc próba użycia go z nazwą domeny, która już istnieje w sieci, kończy się błędem: polecenie sprawdza w ramach wymagań wstępnych, czy taka nazwa nie jest już zajęta, i odmawia dalszego działania zamiast przypadkowo dołączyć się do istniejącej domeny albo ją nadpisać. Do dołączenia kolejnego kontrolera do już istniejącej domeny służy właśnie `Install-ADDSDomainController`.

Powiązane: Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo · Struktura OU Zielonej i delegowanie uprawnień · DNS w domenie: strefy, rekordy, przekazywanie · Skrypty audytowe Active Directory · Konta usługowe MSA i gMSA

Źródła: Microsoft Learn, „Install-ADDSForest (ADDSDeployment)" · Microsoft Learn, „Install-ADDSDomainController (ADDSDeployment)" · Microsoft Learn, „Uninstall-ADDSDomainController (ADDSDeployment)" · Microsoft Learn, „Active Directory Domain Services functional levels" (odczyt 19.10.2026: obsługiwane poziomy 2012 R2, 2016 i 2025) · Microsoft Learn, „Install Active Directory Domain Services on Windows Server" · Microsoft Learn, „wbadmin start systemstatebackup" · Microsoft TechNet Wiki, „Active Directory Domain Naming Considerations" · `Get-Help dcdiag` · `Get-Help repadmin`

Revision #30
Created 2026-09-28 09:24:25 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:25 UTC by Tomasz Konieczny