

Projekt i konfiguracja środowiska domenowego Active Directory w systemie Windows Server 2019

Cel Projektu

Celem projektu jest zaprojektowanie i wdrożenie środowiska domenowego opartego na Active Directory Domain Services (AD DS) w systemie Windows Server 2019. Projekt zakłada stworzenie infrastruktury pozwalającej na centralne zarządzanie użytkownikami, komputerami, uprawnieniami i politykami grupowymi (GPO) w sieci firmowej.

Dzięki wdrożeniu Active Directory możliwe będzie:

- kontrolowanie dostępu do zasobów sieciowych (foldery, drukarki, udziały SMB),
- nadawanie ról i uprawnień użytkownikom w zależności od działu,
- zarządzanie komputerami i kontami użytkowników z jednego miejsca,
- zwiększenie poziomu bezpieczeństwa danych i sieci lokalnej.

Zakres projektu

Projekt obejmuje następujące etapy:

1. Przygotowanie środowiska wirtualnego (serwer + klient).
2. Instalacja i konfiguracja Windows Server 2019.
3. Instalacja roli Active Directory Domain Services (AD DS) i DNS.
4. Utworzenie domeny firma.local.
5. Stworzenie jednostek organizacyjnych (OU) odpowiadających strukturom działów firmy.
6. Dodanie użytkowników i grup domenowych.
7. Dołączenie klienta z systemem Windows 10 Pro do domeny.
8. Konfiguracja folderów współdzielonych (SMB) i uprawnień NTFS.
9. Utworzenie polityk grupowych (GPO) w celu centralnego zarządzania.
10. Konfiguracja polityk haseł, bezpieczeństwa i delegowania uprawnień.
11. Backup i przywracanie.
12. Testy poprawności działania środowiska.

Opis środowiska laboratoryjnego

Projekt został wykonany w środowisku wirtualnym z wykorzystaniem oprogramowania Oracle VirtualBox. Utworzono dwie maszyny wirtualne — serwer domeny oraz stację roboczą-klienta.

Nazwa	System Operacyjny	Funkcja	Adres IP	Uwagi
DC1	Windows Server 2019 GUI	Kontroler Domeny, DNS	192.168.1.19	Serwer Główny
Klient01	Windows 10 Pro	Klient w domenie	192.168.1.20	Stacja robocza użytkownika

Topologia sieci:

- Sieć typu: Host-Only Adapter (lub NAT + wewnętrzna).
- Maska podsieci: 255.255.255.0
- Brama domyślana: brak (sieć testowa).
- Serwer DNS: 192.168.1.19 (czyli sam serwer domeny).

Etapy realizacji projektu

1. Przygotowanie i konfiguracja serwera DC1

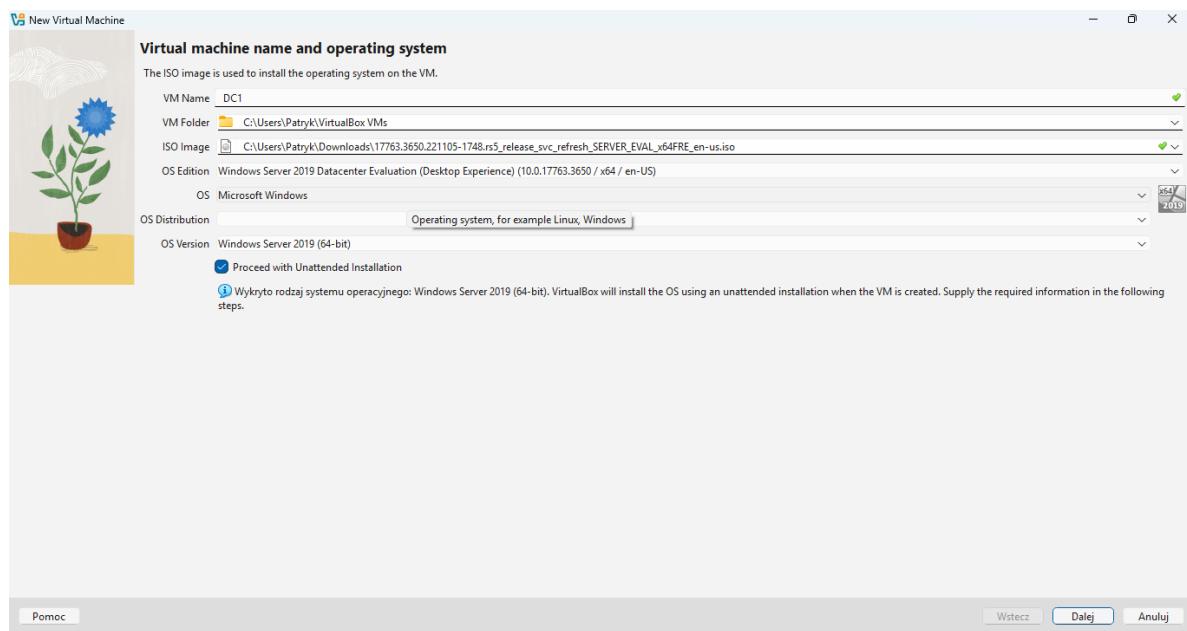
Pierwszym etapem projektu było przygotowanie środowiska serwerowego, które posłuży jako kontroler domeny Active Directory. Do tego celu wykorzystano oprogramowanie Oracle VirtualBox oraz obraz systemu Windows Server 2019 Datacenter Evaluation (x64).

1.1. Tworzenie nowej maszyny wirtualnej

Na początku w VirtualBox utworzono nową maszynę o nazwie DC1.

Na rysunku (Rys. 1) przedstawiono ustawienia podstawowe maszyny:

- Nazwa: DC1
- Typ systemu: Microsoft Windows
- Wersja: Windows Server 2019 (64-bit)
- Obraz ISO: Windows Server 2019 Datacenter Evaluation (Desktop Experience)
- Folder docelowy: C:\Users\Patryk\VirtualBox VMs
- Zaznaczono opcję Proceed with Unattended Installation, co umożliwia automatyczną instalację systemu.



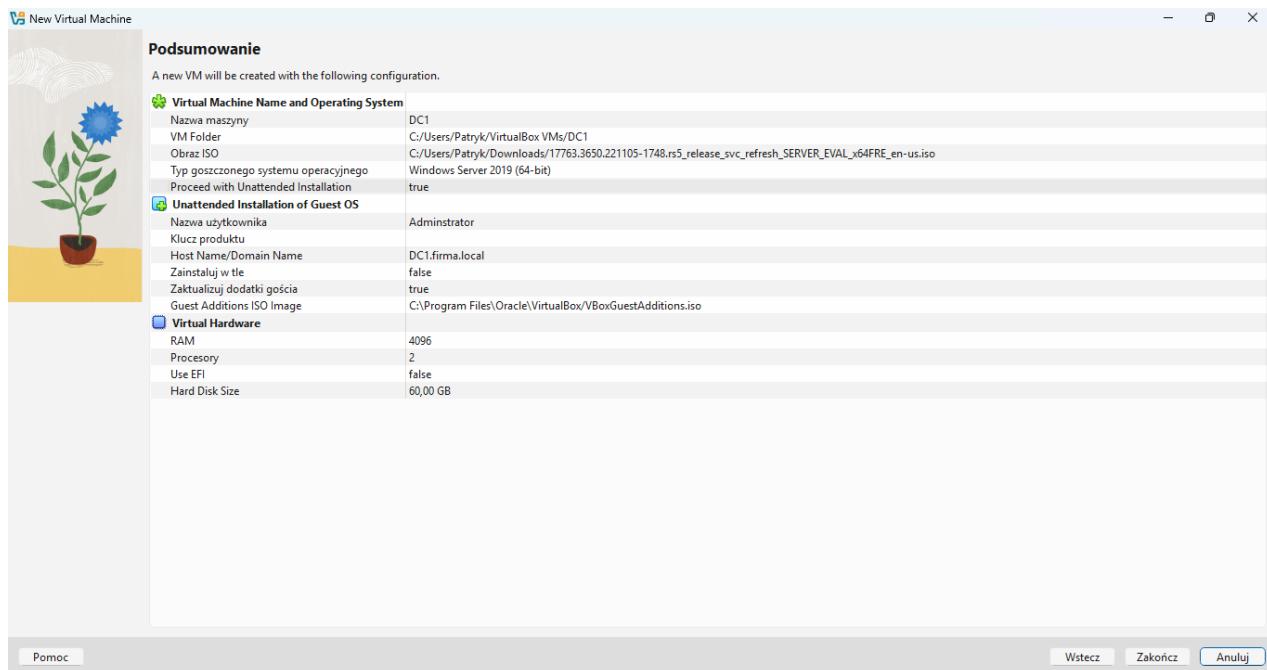
Rysunek 1 Ustawienia tworzenia maszyny wirtualnej – wybór systemu

1.2. Parametry sprzętowe maszyny wirtualnej

W kolejnym kroku przydzielono maszynie odpowiednie zasoby sprzętowe:

- Pamięć RAM: 4096 MB,
- Liczba rdzeni procesora: 2,
- Dysk twardy: 60 GB,
- Tryb EFI: wyłączony (Use EFI: false),
- Instalacja dodatków gościa VirtualBox (Guest Additions): włączona.

System został automatycznie zainstalowany w trybie Unattended Installation, z nazwą użytkownika Administrator oraz nazwą hosta DC1.firma.local.



Rysunek 2 Podsumowanie konfiguracji maszyny wirtualnej

1.3.Uruchomienie systemu po instalacji

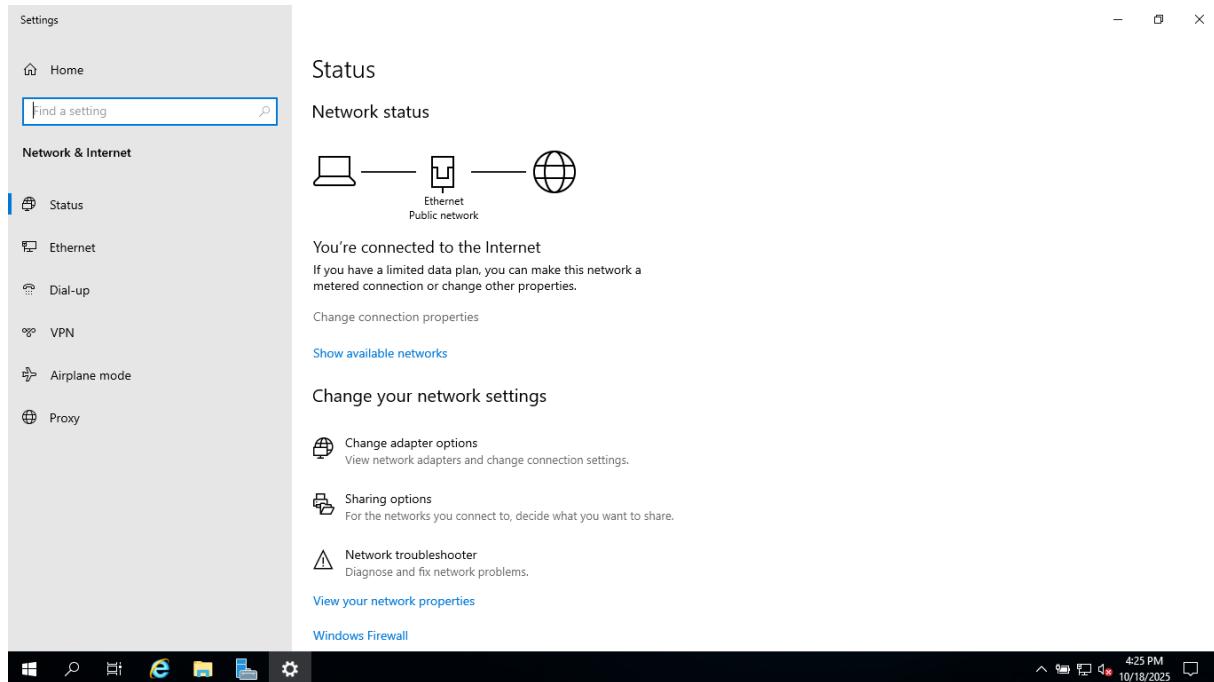
Po zakończeniu instalacji i pierwszym uruchomieniu systemu pojawił się pulpit środowiska graficznego Windows Server 2019. Na pasku zadań widoczny jest aktywny stan sieci – Connected, co potwierdza poprawną konfigurację karty sieciowej.



Rysunek 3 Ekran po pierwszym uruchomieniu systemu Windows Server 2019

1.4. Weryfikacja połączenia sieciowego

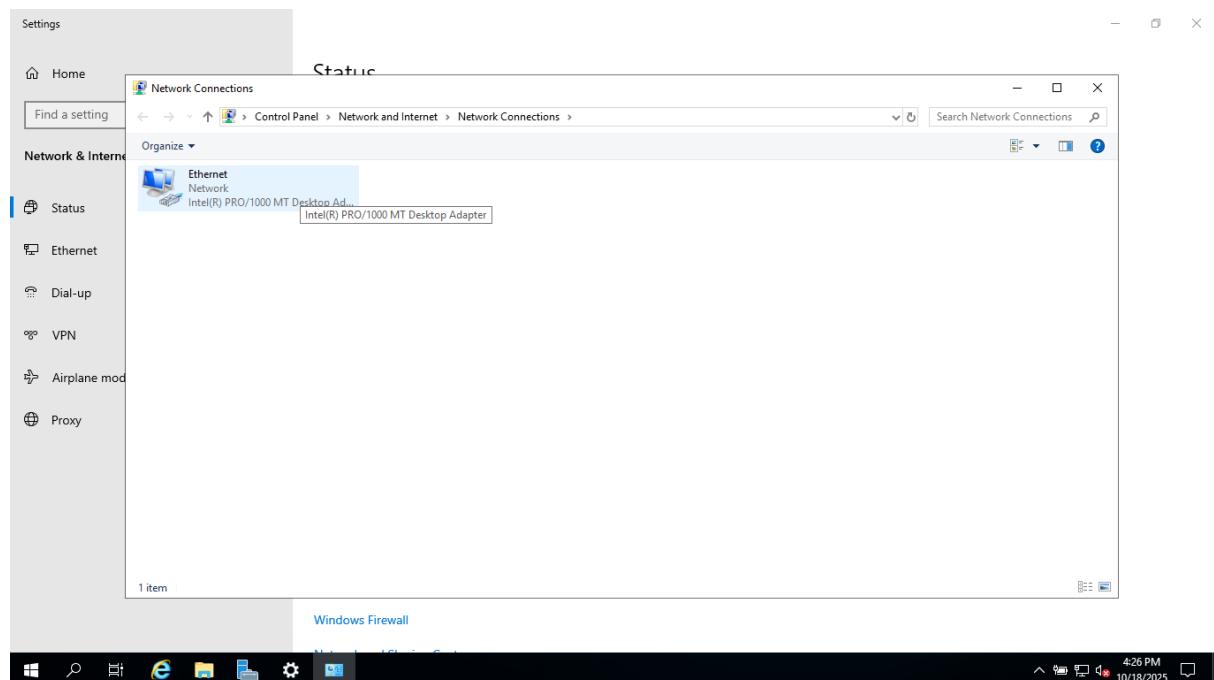
W ustawieniach systemowych (Network & Internet → Status) sprawdzono, że serwer posiada połączenie z siecią Ethernet (Public Network). W razie potrzeby możliwe było przełączenie typu sieci na Private w celu późniejszego udostępniania plików.

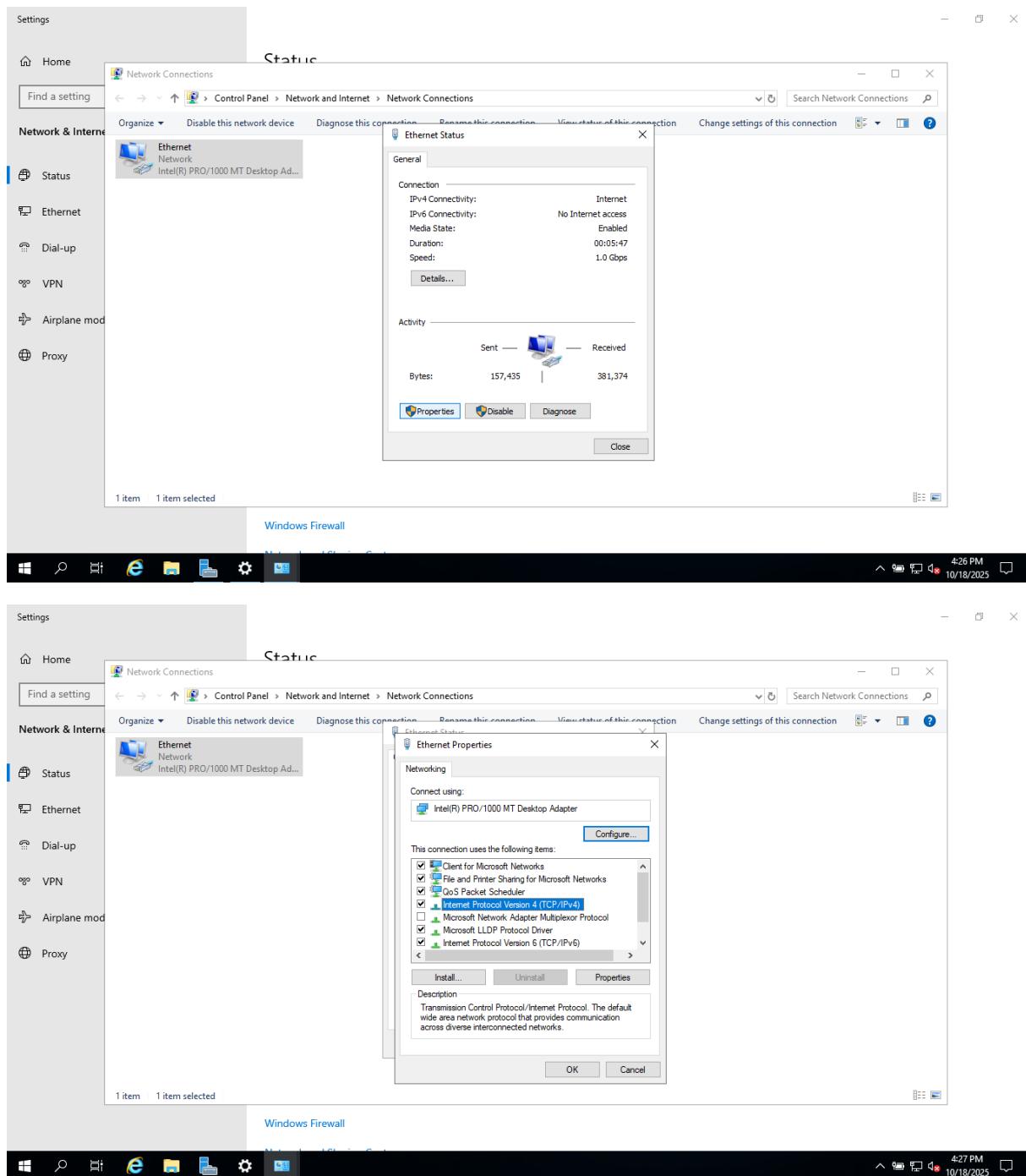


Rysunek 4 Okno statusu połączenia sieciowego

1.5. Konfiguracja interfejsu sieciowego

W celu zapewnienia stabilnej pracy serwera domenowego konieczne było przypisanie statycznego adresu IP. W panelu Network Connections wybrano adapter „Ethernet”, a następnie otwarto jego właściwości.





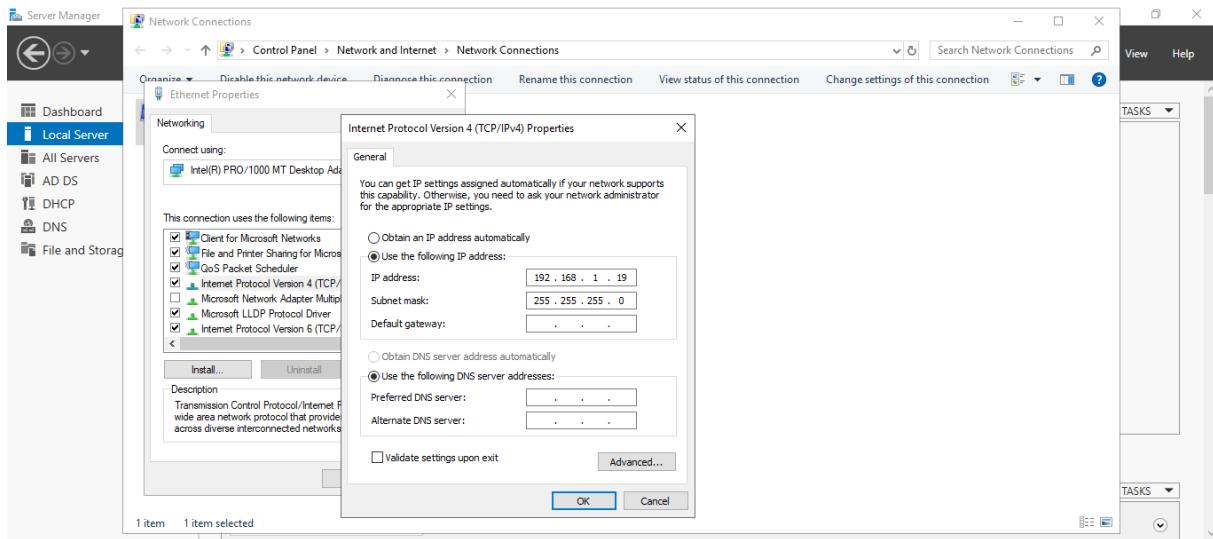
Rysunek 5 Właściwości karty sieciowej Ethernet

W sekcji Internet Protocol Version 4 (TCP/IPv4) wybrano opcje:

- “Use the following IP address”

i przypisano wartości:

- IP address: 192.168.1.19
- Subnet mask: 255.255.255.0
- Default gateway: (puste)
- Preferred DNS server: (puste – zostanie uzupełnione po instalacji roli DNS)



Rysunek 6 Ustawienia statycznego adresu IP

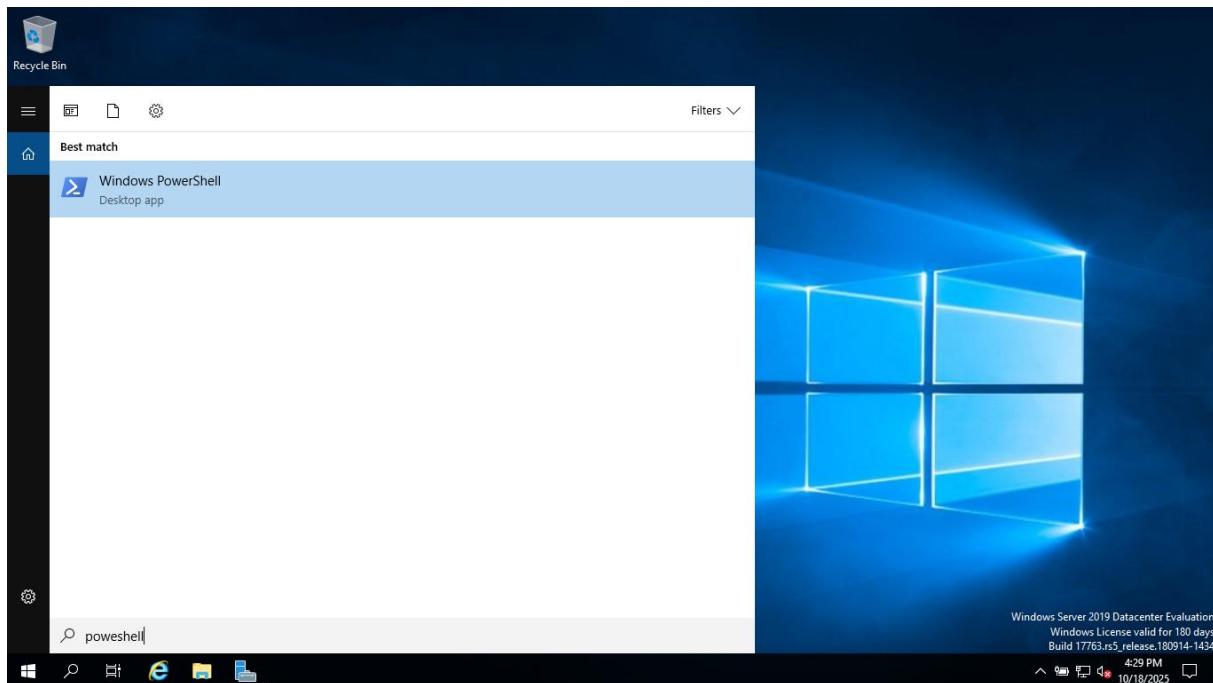
1.6. Test połączenia z siecią

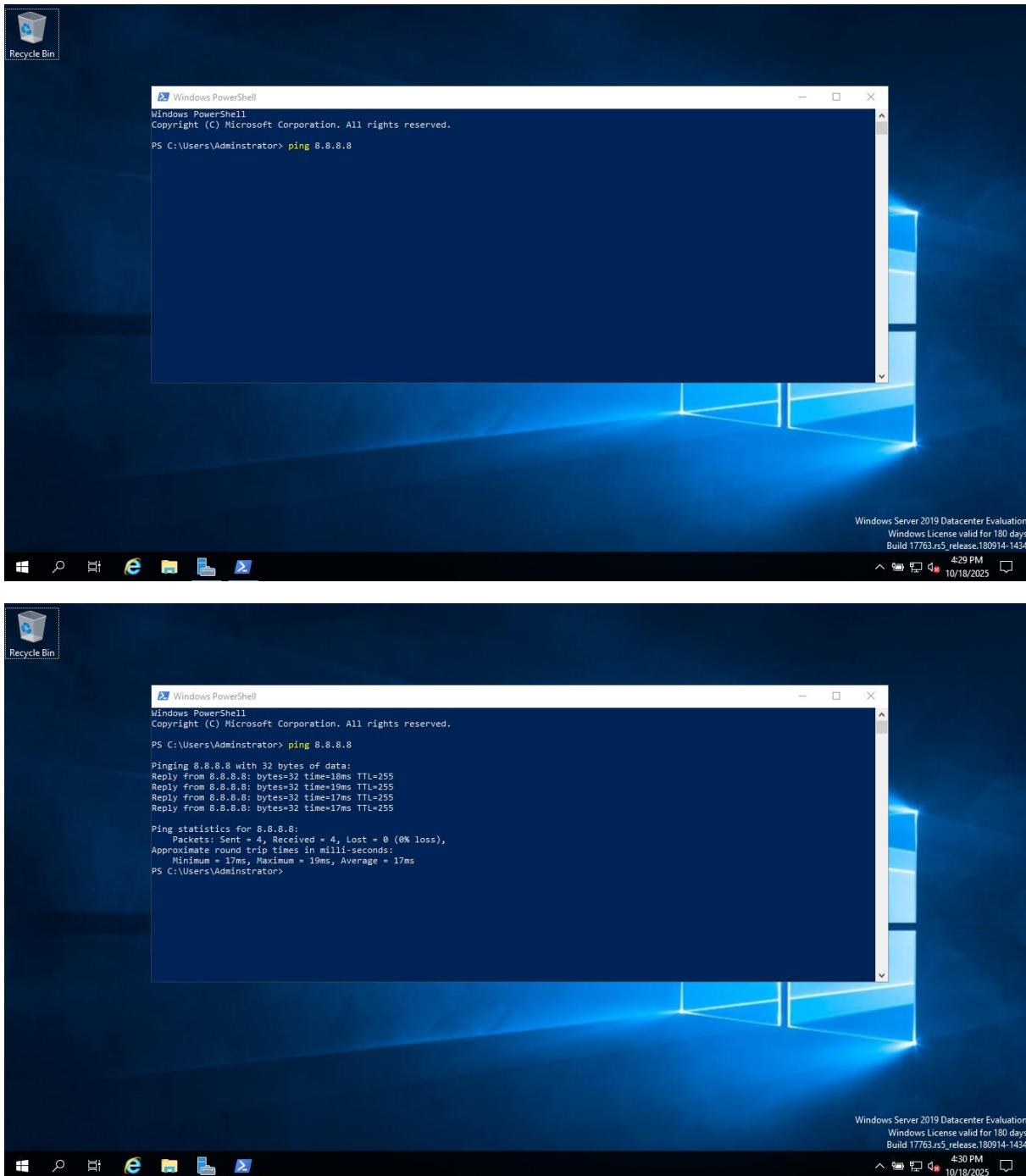
W celu potwierdzenia poprawnego działania interfejsu sieciowego uruchomiono Windows PowerShell z uprawnieniami administratora.

Poleceniem:

- ping 8.8.8.8

sprawdzono komunikację z serwerem DNS Google, co potwierdziło aktywne połączenie sieciowe.





Rysunek 7 Test polaczenia z siecią

1.7. Wnioski z etapu 1

W wyniku przeprowadzonych czynności przygotowano w pełni działający serwer DC1 z systemem Windows Server 2019 Datacenter Evaluation, posiadający:

- zainstalowany system w trybie Desktop Experience,
- skonfigurowaną kartę sieciową z adresem statycznym,
- poprawne połączenie z siecią zewnętrzną.

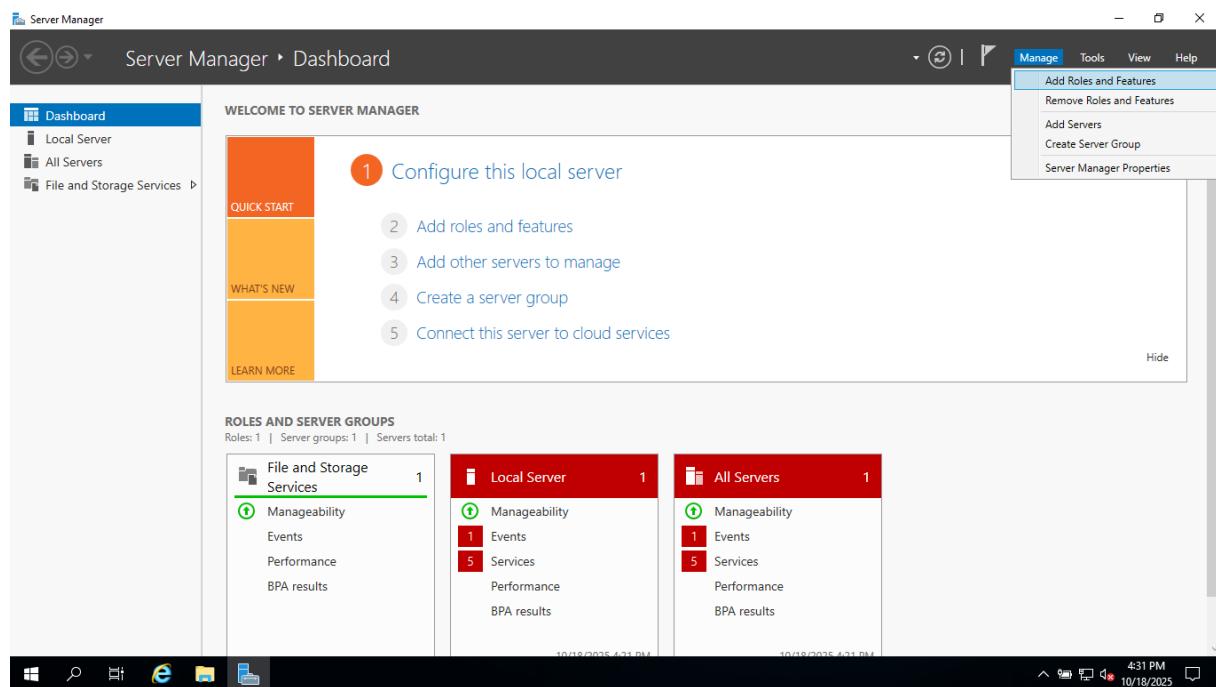
Serwer jest gotowy do instalacji ról Active Directory Domain Services (AD DS) oraz DNS, co stanowi kolejny etap projektu.

2. Instalacja roli Active Directory Domain Services (AD DS) i DNS

Po przygotowaniu serwera DC1 i konfiguracji sieci przystąpiono do instalacji roli Active Directory Domain Services (AD DS), która umożliwia utworzenie i zarządzanie strukturą domenową w sieci Windows. Dodatkowo automatycznie zainstalowana została rola DNS, niezbędna do prawidłowego działania kontrolera domeny.

2.1. Uruchomienie Server Managera i wybór instalacji roli

Po zalogowaniu na konto Administrator, otwarto narzędzie Server Manager, które uruchamia się domyślnie po starcie systemu. Z menu Manage wybrano opcję Add Roles and Features, co uruchamia kreator instalacji ról serwera.



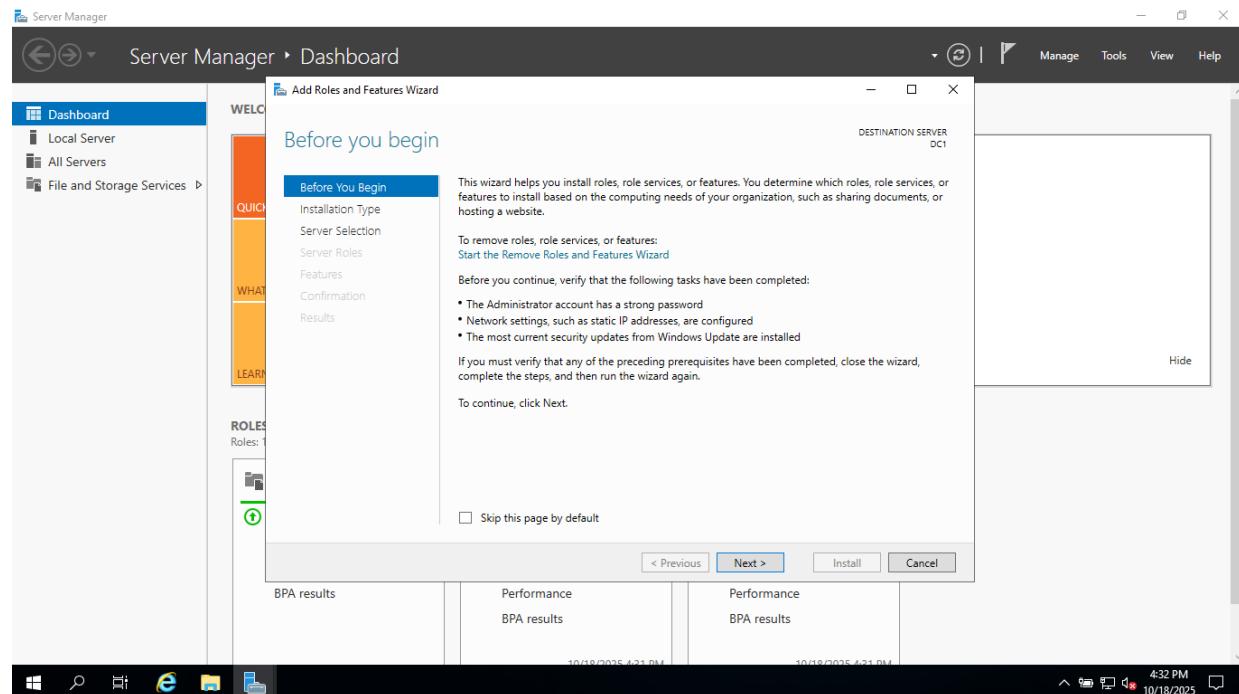
Rysunek 8 Widok głównego panelu Server Manager i wybór „Add Roles and Features”

2.2. Wprowadzenie do kreatora instalacji

W pierwszym kroku kreatora pojawia się ekran informacyjny Before You Begin, przypominający o wstępnych wymaganiach:

- Użycie konta z uprawnieniami administratora,
- Skonfigurowanie adresu IP (statycznego),
- Aktualizacja systemu Windows do najnowszej wersji.

Po ich potwierdzeniu kliknięto Next.



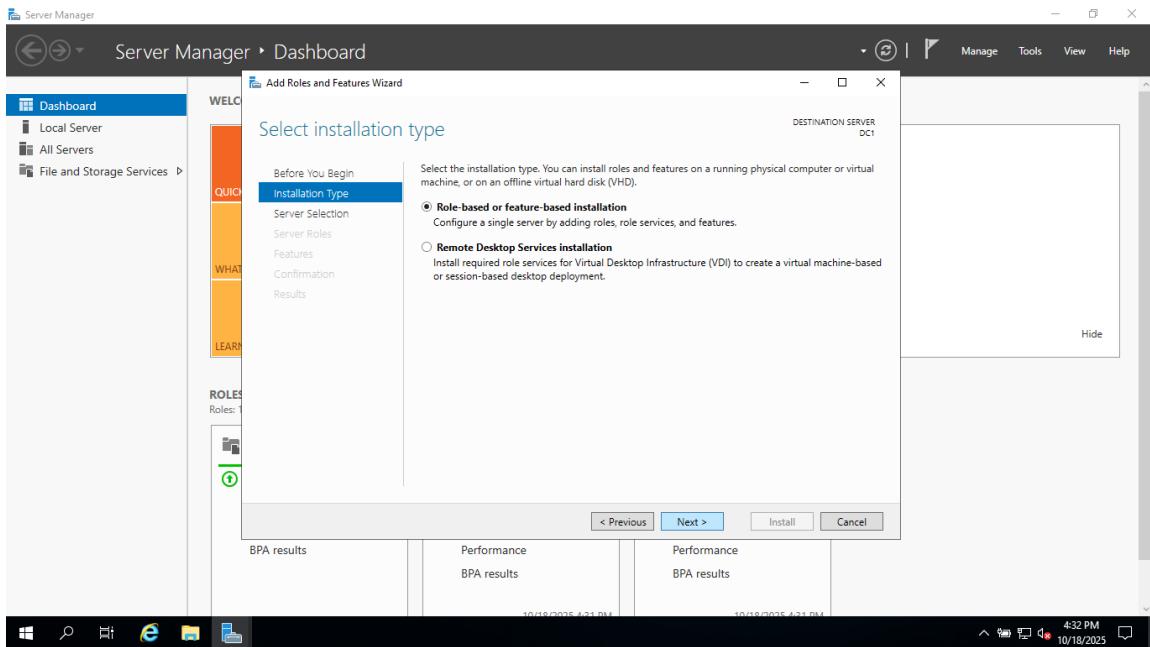
Rysunek 9 Ekran wstępny kreatora instalacji

2.3. Wybór typu instalacji

W kolejnym kroku wybrano domyślną opcję:

- Role-based or feature-based installation

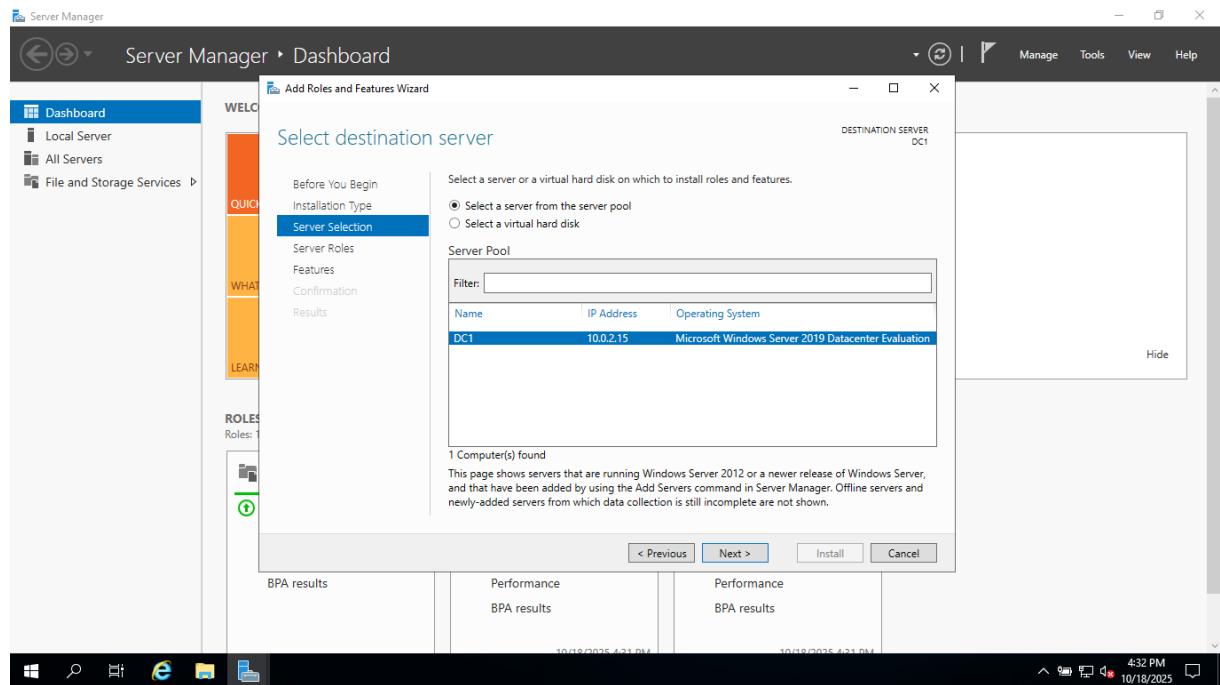
Opcja ta pozwala zainstalować role i funkcje lokalnie na bieżącym serwerze.



Rysunek 10 Wybór typu instalacji – instalacja lokalna

2.4. Wybór serwera docelowego

Z listy serwerów dostępnych w puli wybrano maszynę lokalną DC1, posiadającą adres IP 10.0.2.15 i system Windows Server 2019 Datacenter Evaluation.

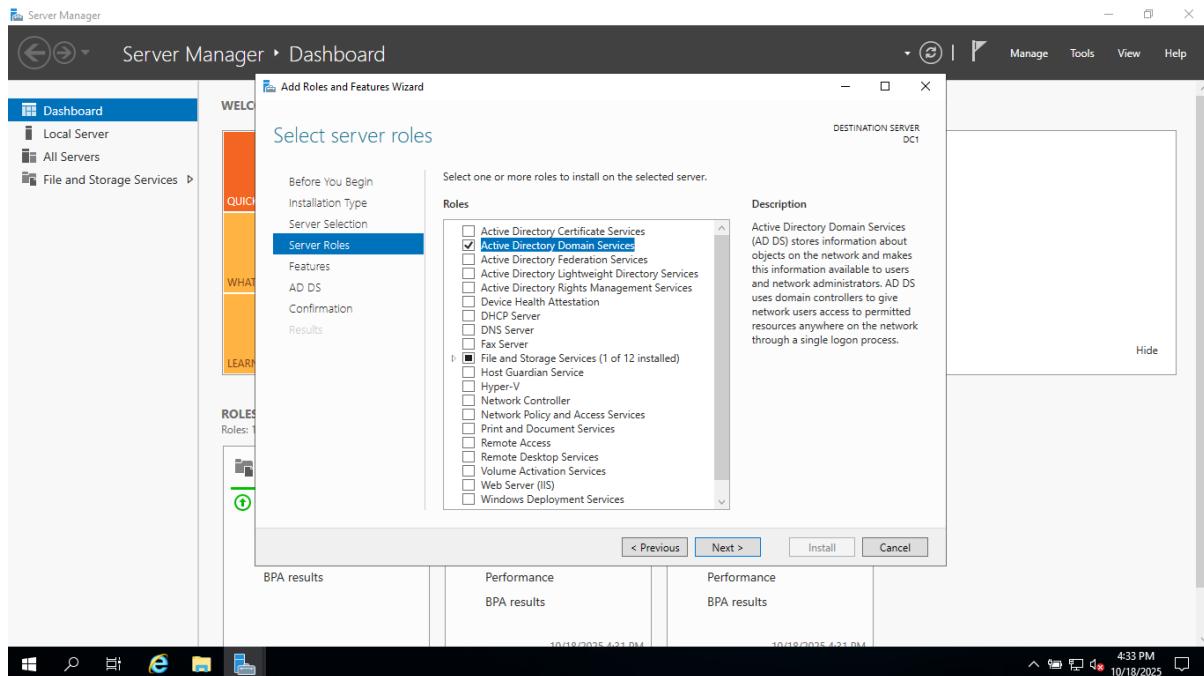


Rysunek 11 Wybór serwera DC1 do instalacji roli

2.5. Wybór roli Active Directory Domain Services

Na liście dostępnych ról zaznaczono:

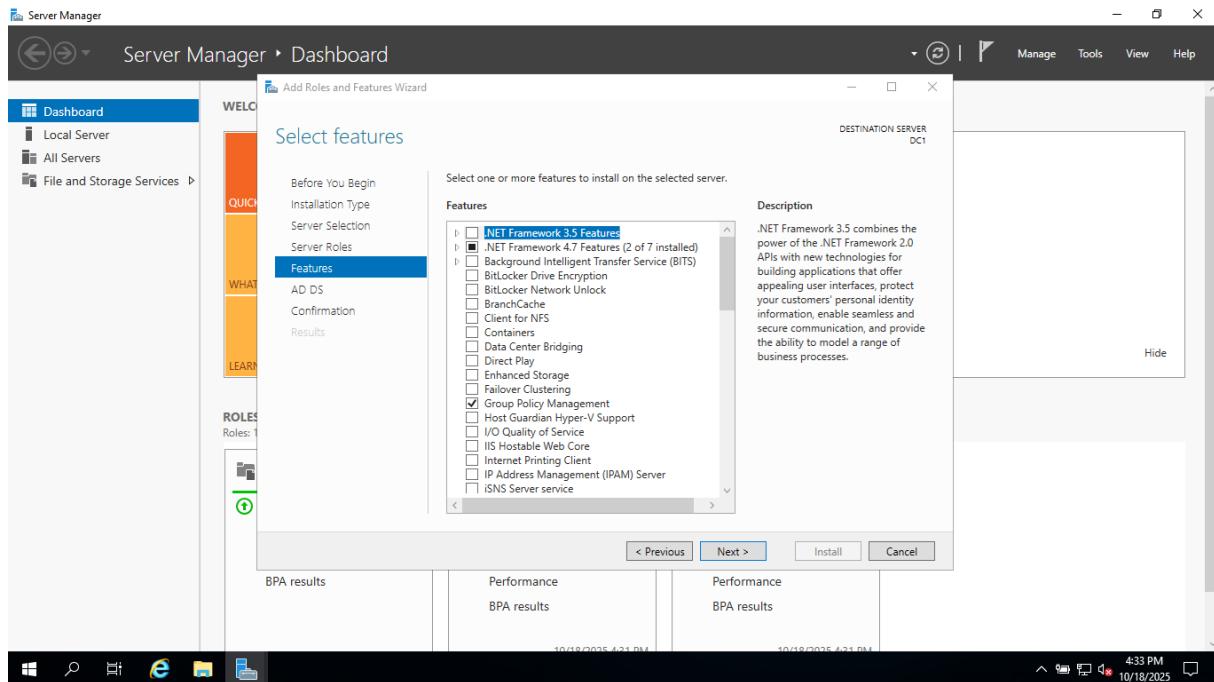
- Active Directory Domain Services, co automatycznie dodało wymagane komponenty, w tym:
- Group Policy Management,
- DNS Server (zostanie zainstalowany automatycznie w kolejnym kroku).



Rysunek 12 Wybór roli AD DS z listy dostępnych funkcji

2.6. Instalacja dodatkowych funkcji

W sekcji Select features pozostawiono domyślnie zaznaczone składniki, w tym Group Policy Management oraz biblioteki .NET Framework 4.7 i 4.8, niezbędne do działania narzędzi administracyjnych.

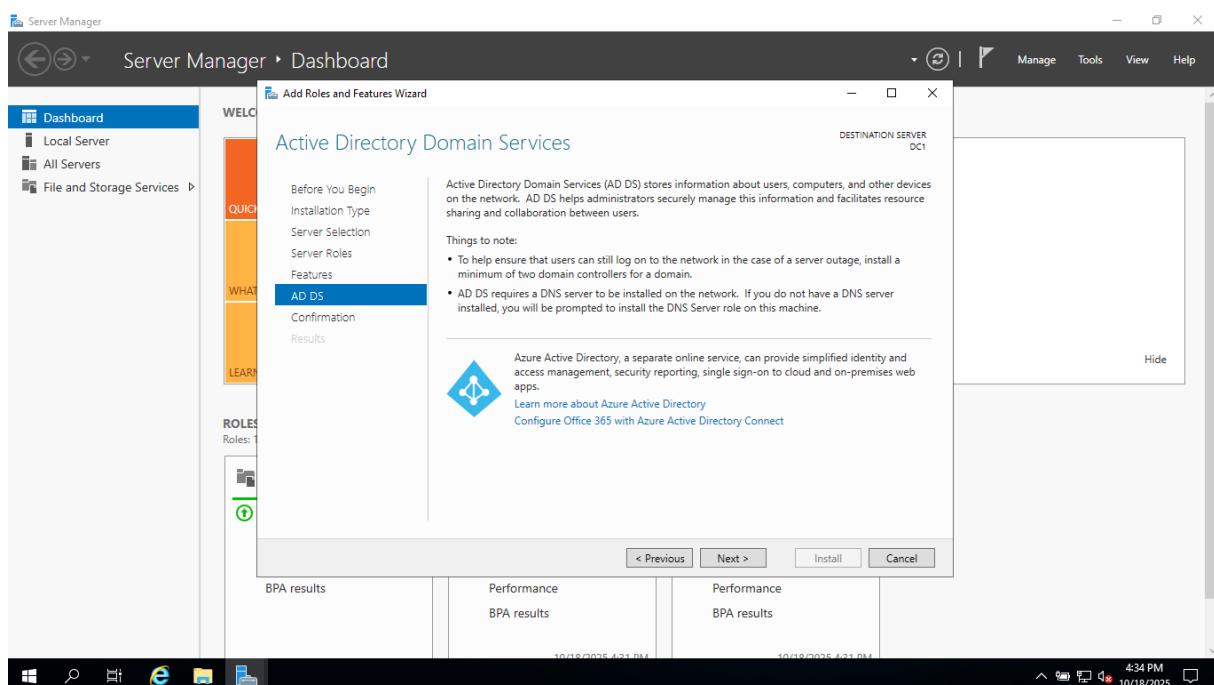


Rysunek 13 Okno wyboru funkcji dodatkowych

2.7. Informacje o roli AD DS.

Kreator wyświetlił krótkie podsumowanie dotyczące roli Active Directory Domain Services, w którym opisano:

- Przechowywanie informacji o użytkownikach, grupach i zasobach,
- Możliwość logowania się użytkowników do domeny,
- Konieczność posiadania usługi DNS dla poprawnej pracy domeny.



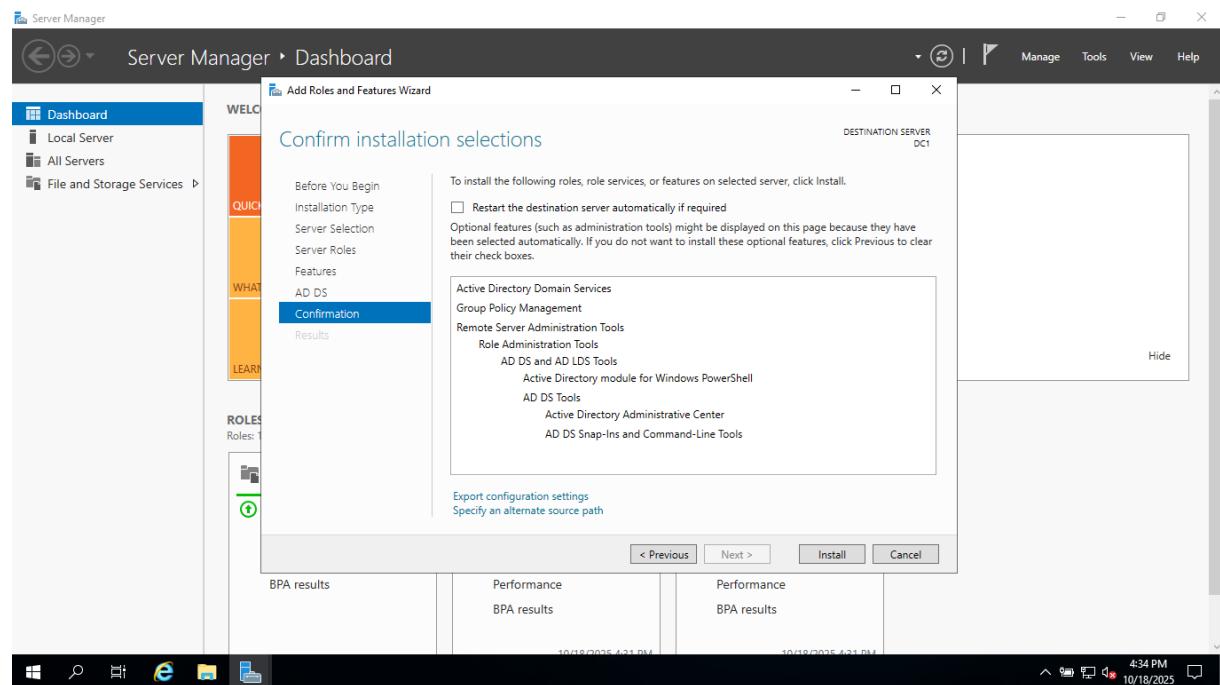
Rysunek 14 Informacje o roli AD DS

2.8.Potwierdzenie wyboru i rozpoczęcie instalacji

Na etapie Confirmation wyświetcono listę elementów, które zostaną zainstalowane:

- Active Directory Domain Services,
- Group Policy Management,
- AD DS Tools,
- Active Directory Administrative Center,
- AD DS Snap-Ins and Command-Line Tools.

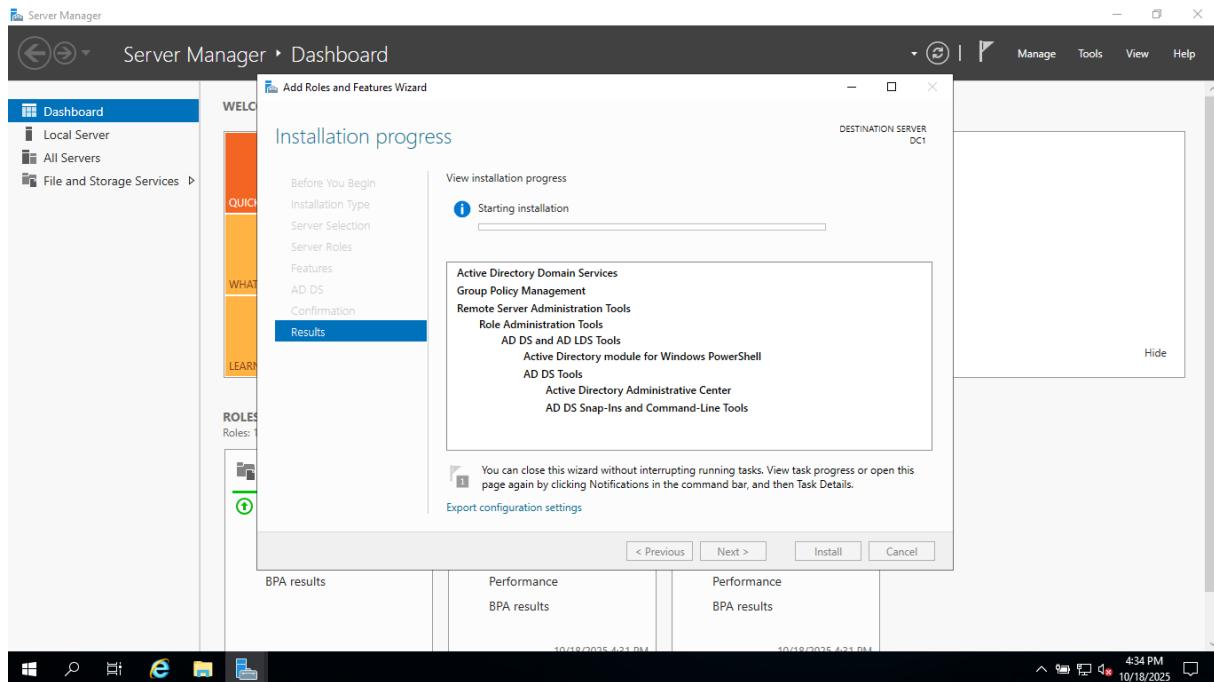
Po weryfikacji kliknięto Install.



Rysunek 15 Potwierdzenie wyboru i rozpoczęcie instalacji roli AD DS

2.9.Postęp instalacji ról serwera

Po rozpoczęciu instalacji kreator na bieżąco wyświetlał pasek postępu. Proces instalacji trwał kilka minut, a wszystkie komponenty zostały zainstalowane pomyślnie.



Rysunek 16 Postęp instalacji ról AD DS i DNS

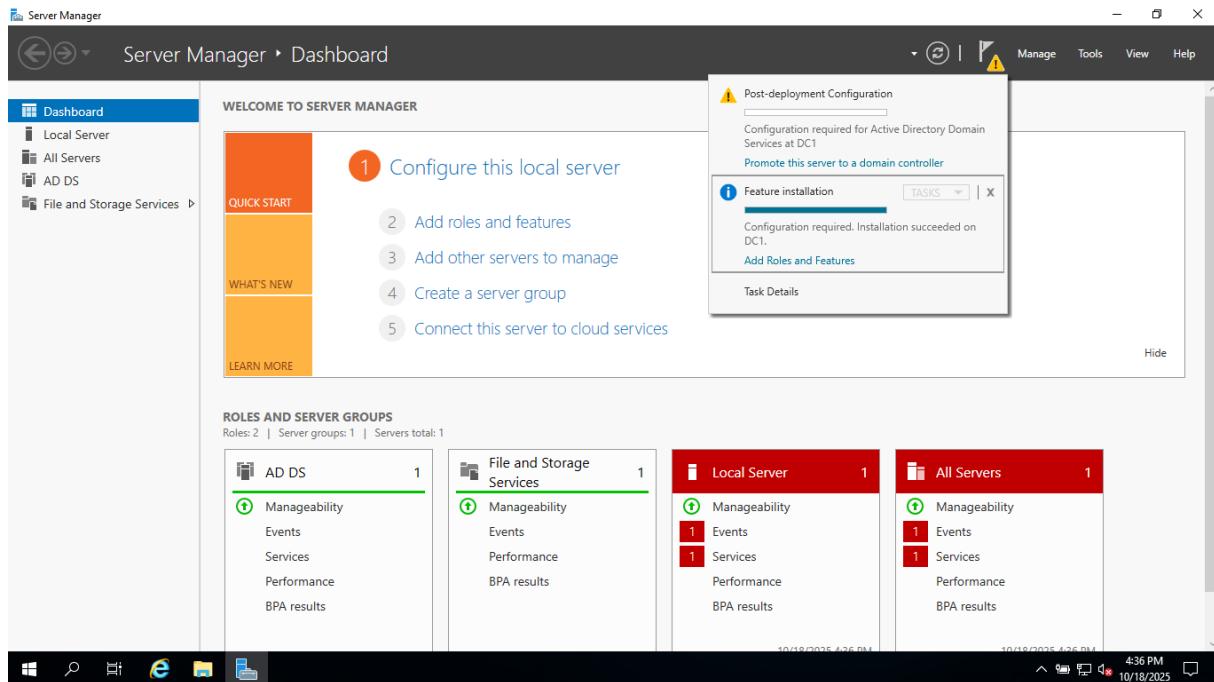
2.10. Zakończenie instalacji i wstępna konfiguracja AD DS.

Po zakończeniu procesu w górnej części Server Managera pojawiło się powiadomienie:

- Post-deployment Configuration
„Configuration required for Active Directory Domain Services at DC1.”

W tym miejscu dostępna jest opcja Promote this server to a domain controller, która uruchamia proces konfiguracji nowej domeny.

Ta czynność zostanie wykonana w następnym etapie projektu.



Rysunek 17 Zakończenie instalacji roli AD DS – serwer gotowy do promocji

2.11. Wnioski z etapu 2

W wyniku przeprowadzonego procesu:

- Zainstalowano rolę Active Directory Domain Services wraz z komponentami zarządzania,
- Włączono narzędzia administracyjne AD DS oraz GPO,
- System jest gotowy do konfiguracji nowej domeny w kolejnym etapie (promocja do kontrolera domeny).

Serwer DC1 jest w tym momencie pełnoprawnym serwerem z usługami AD DS i DNS zainstalowanymi lokalnie.

3. Promocja serwera do kontrolera domeny i utworzenie domeny „firma.local”

Po zakończeniu instalacji ról AD DS i DNS, kolejnym etapem było utworzenie nowej domeny Active Directory oraz promocja serwera DC1 do kontrolera domeny.

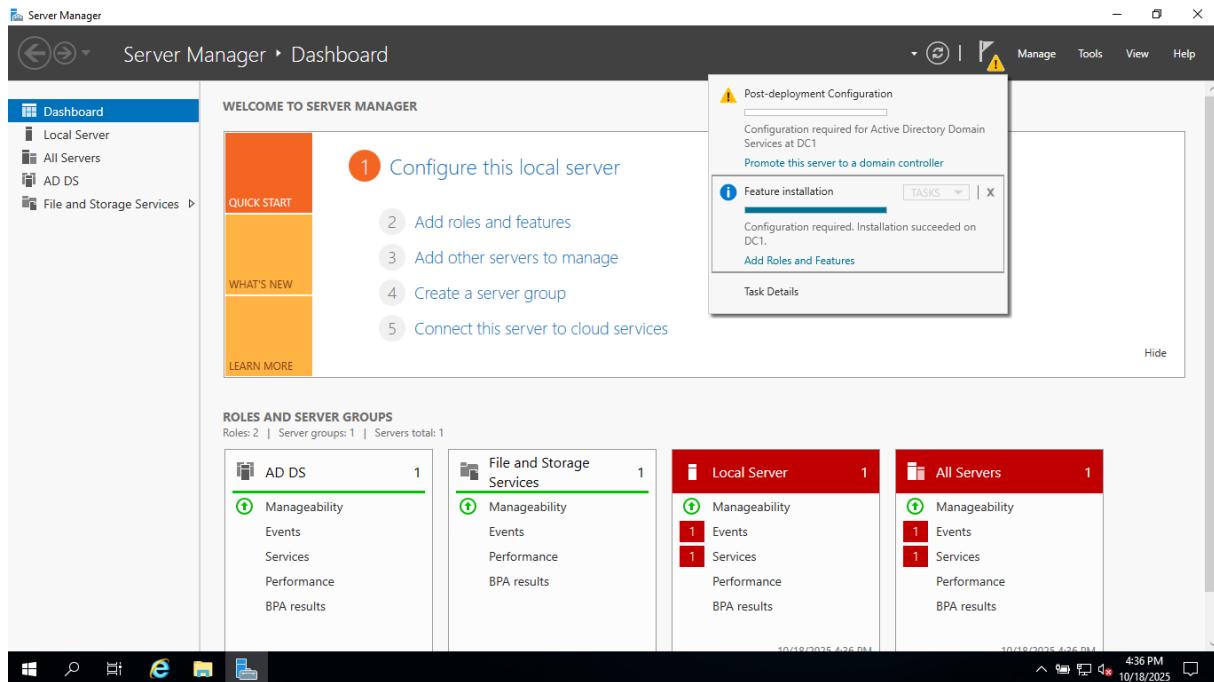
Proces przeprowadzono przy użyciu kreatora Active Directory Domain Services Configuration Wizard dostępnego w narzędziu Server Manager.

3.1. Uruchomienie kreatora konfiguracji AD DS.

Po zakończonej instalacji w Server Managerze pojawiło się ostrzeżenie o konieczności przeprowadzenia konfiguracji usługi AD DS.

Z rozwijanego menu powiadomień wybrano opcję:

- Promote this server to a domain controller

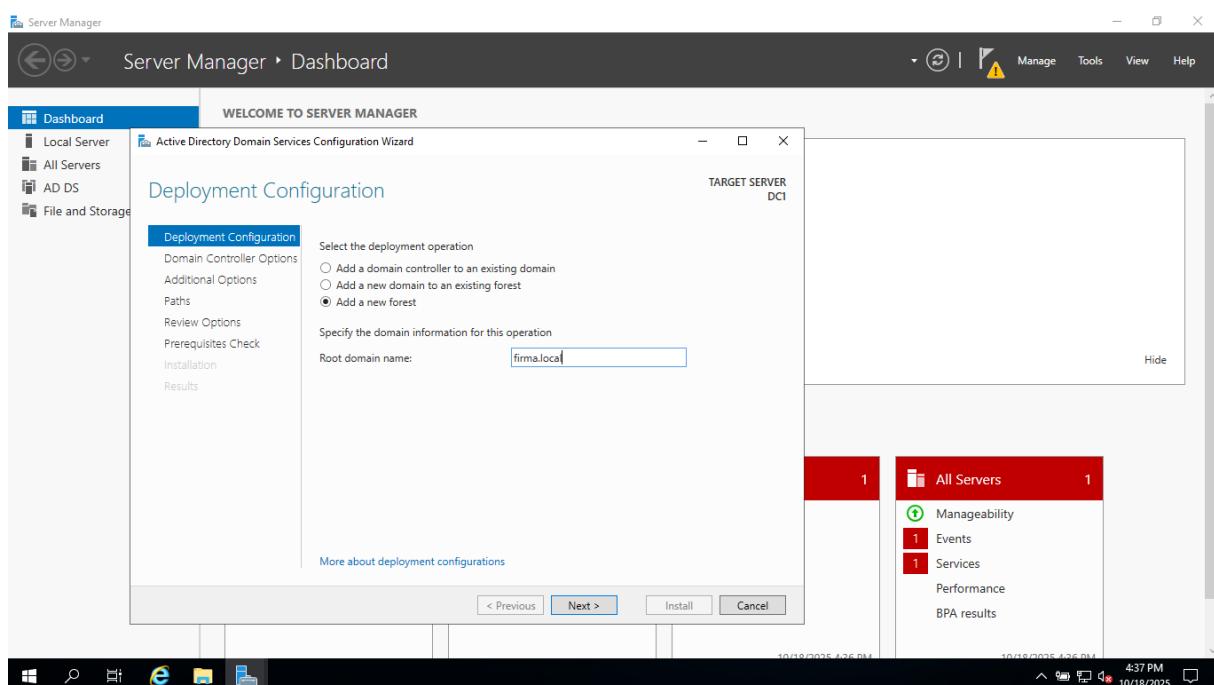


Rysunek 18 Komunikat o wymaganej konfiguracji AD DS i uruchomienie kreatora

3.2. Wybór typu wdrożenia

W pierwszym kroku kreatora (Deployment Configuration) określono sposób utworzenia domeny. Zaznaczono opcję:

- Add a new forest
czyli utworzenie nowego lasu domenowego, którego główną domeną będzie firma.local.



Rysunek 19 Wybór typu instalacji i nazwa nowej domeny

3.3.Ustawienia kontrolera domeny

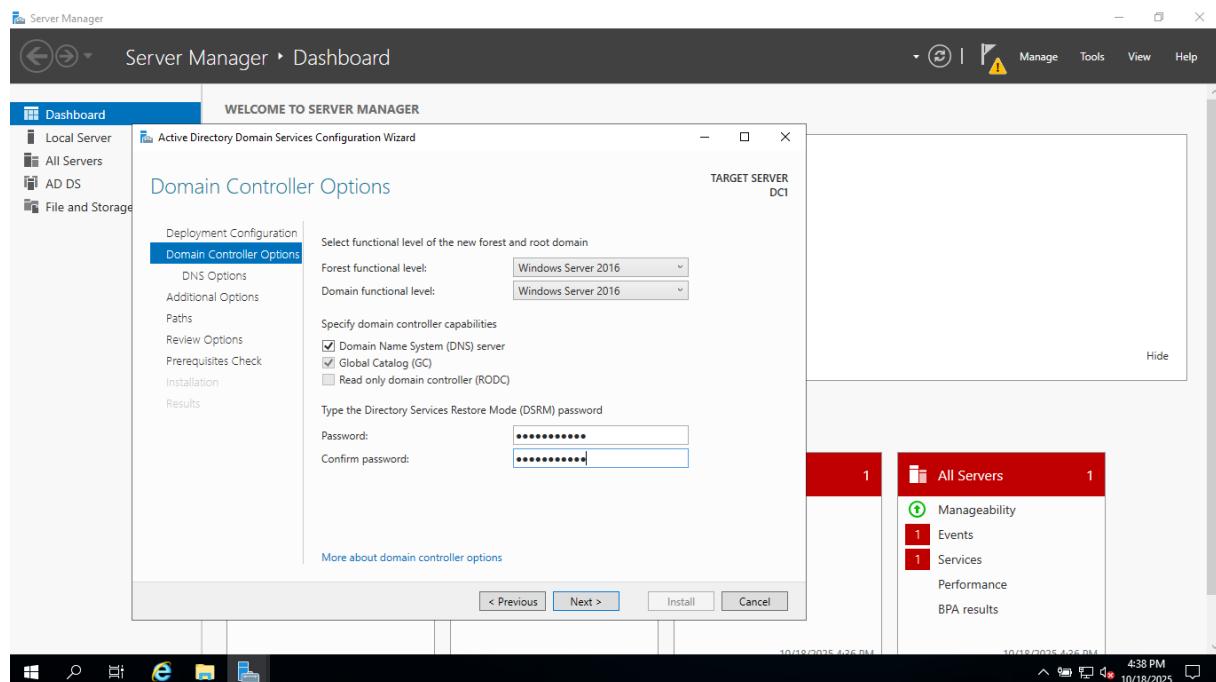
W kolejnym kroku (Domain Controller Options) skonfigurowano poziom funkcjonalny lasu i domeny:

- Forest functional level: Windows Server 2016
- Domain functional level: Windows Server 2016

Dodatkowo zaznaczono następujące opcje:

- Domain Name System (DNS) server
- Global Catalog (GC)

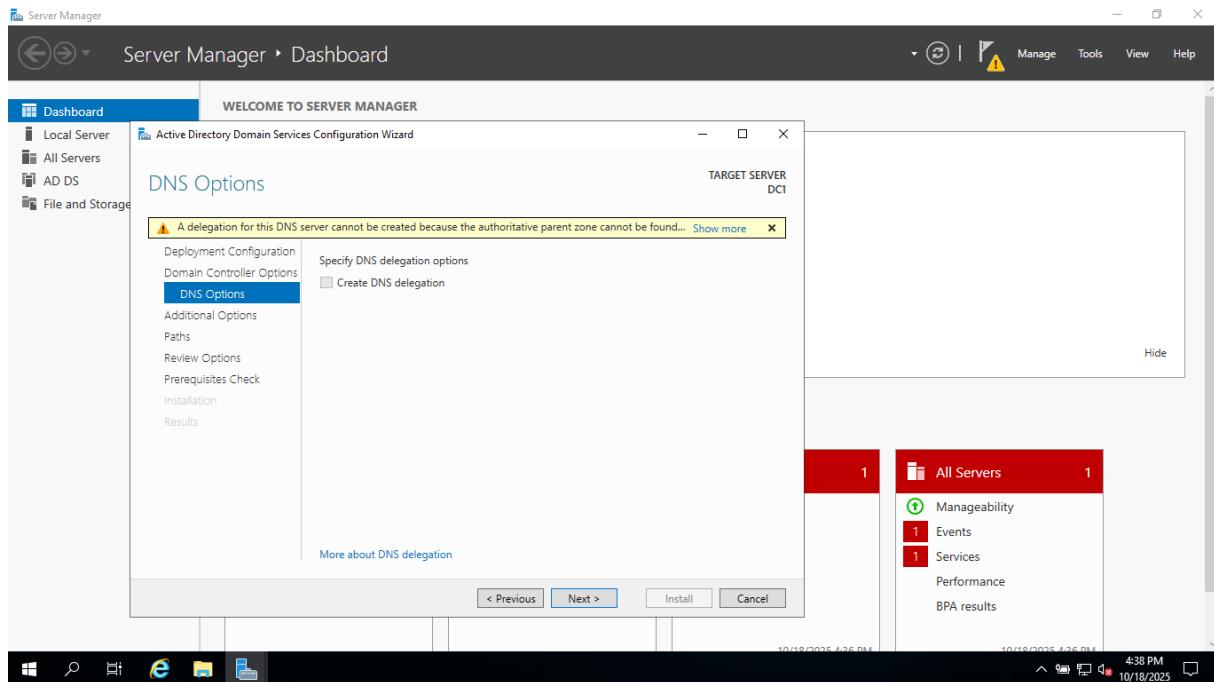
Na tym etapie ustalono również hasło dla trybu awaryjnego usługi katalogowej (DSRM), które będzie wymagane w razie konieczności przywracania usług katalogowych.



Rysunek 20 Konfiguracja kontrolera domeny i poziomów funkcjonalnych

3.4.Konfiguracja usługi DNS

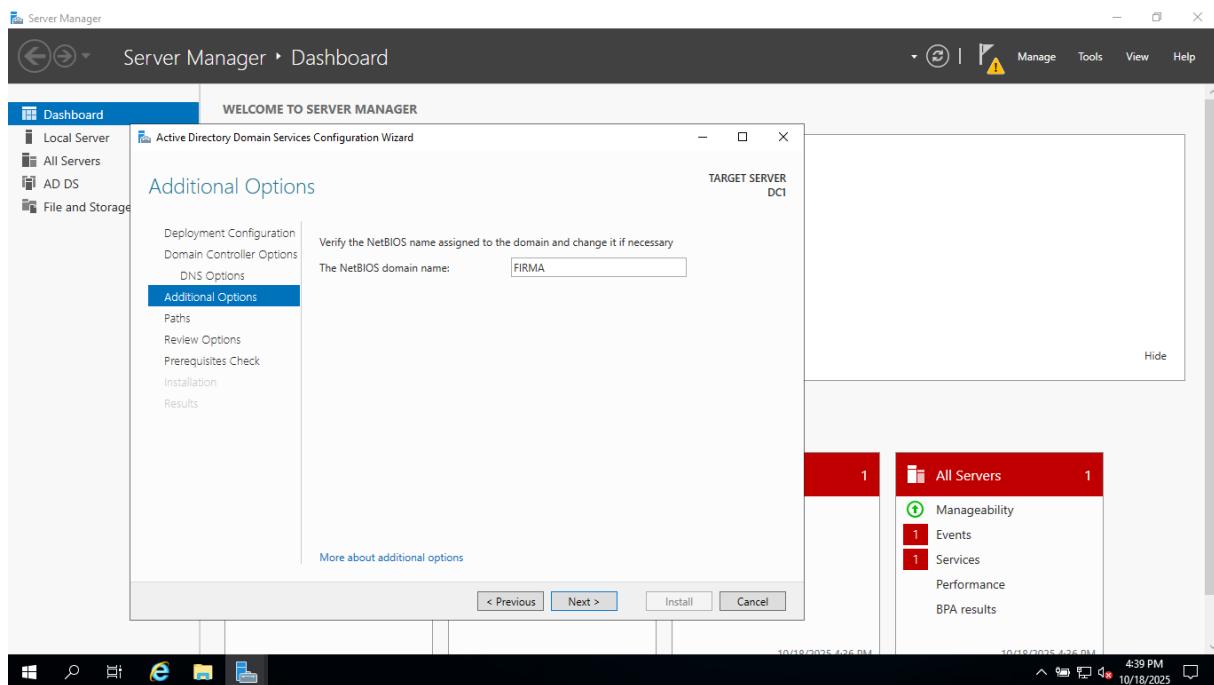
Kreator automatycznie przechodzi do zakładki DNS Options. Wyświetlony został komunikat informujący, że nie można utworzyć delegacji DNS, ponieważ nie istnieje nadrzędna strefa DNS - jest to sytuacja typowa przy tworzeniu nowej domeny od podstaw. Pozostawiono ustawienia domyślne i kliknięto Next.



Rysunek 21 Informacja o braku delegacji DNS

3.5. Weryfikacja nazwy NetBIOS

Na karcie Additional Options automatycznie została wygenerowana nazwa NetBIOS domeny - w tym przypadku FIRMA. Nazwa ta będzie używana do starszych aplikacji i procesów logowania w starszych wersjach systemów Windows.

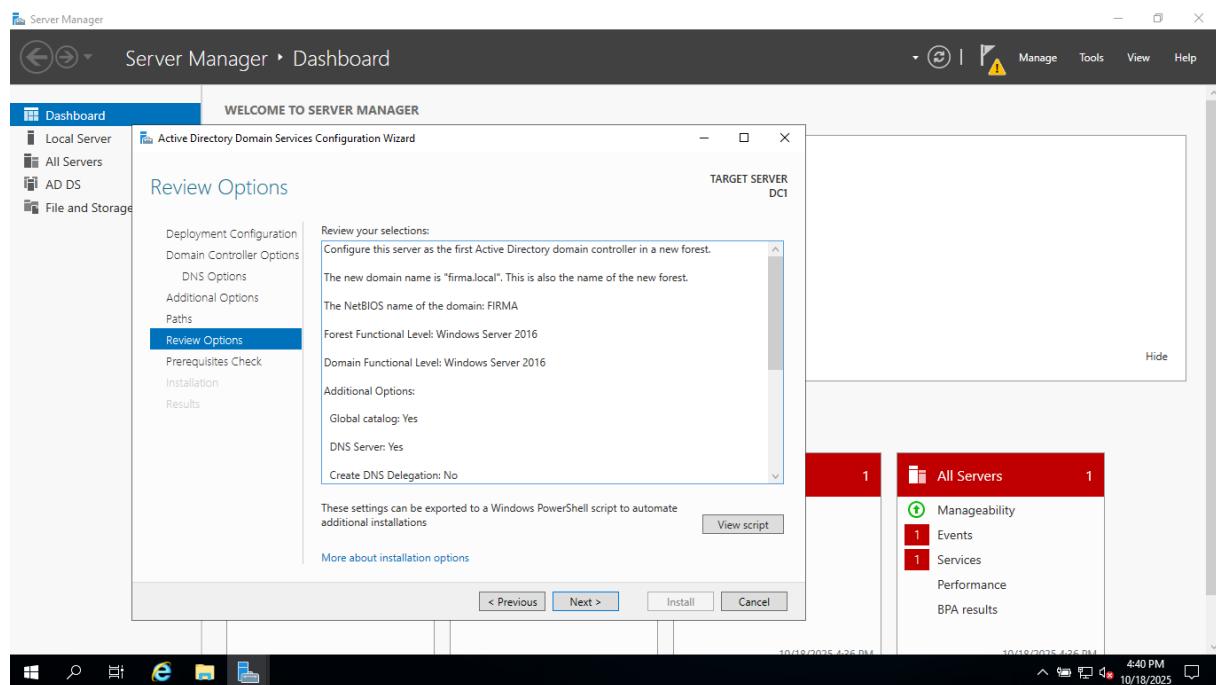


Rysunek 22 Potwierdzenie nazwy NetBIOS dla domeny

3.6. Weryfikacja i przegląd konfiguracji

W kroku Review Options wyświetlono pełne podsumowanie ustawień:

- Domena główna: firma.local
- Nazwa NetBIOS: FIRMA
- Poziom lasu i domeny: Windows Server 2016
- Global Catalog: Tak
- DNS Server: Tak



Rysunek 23 Przegląd konfiguracji domeny przed instalacją

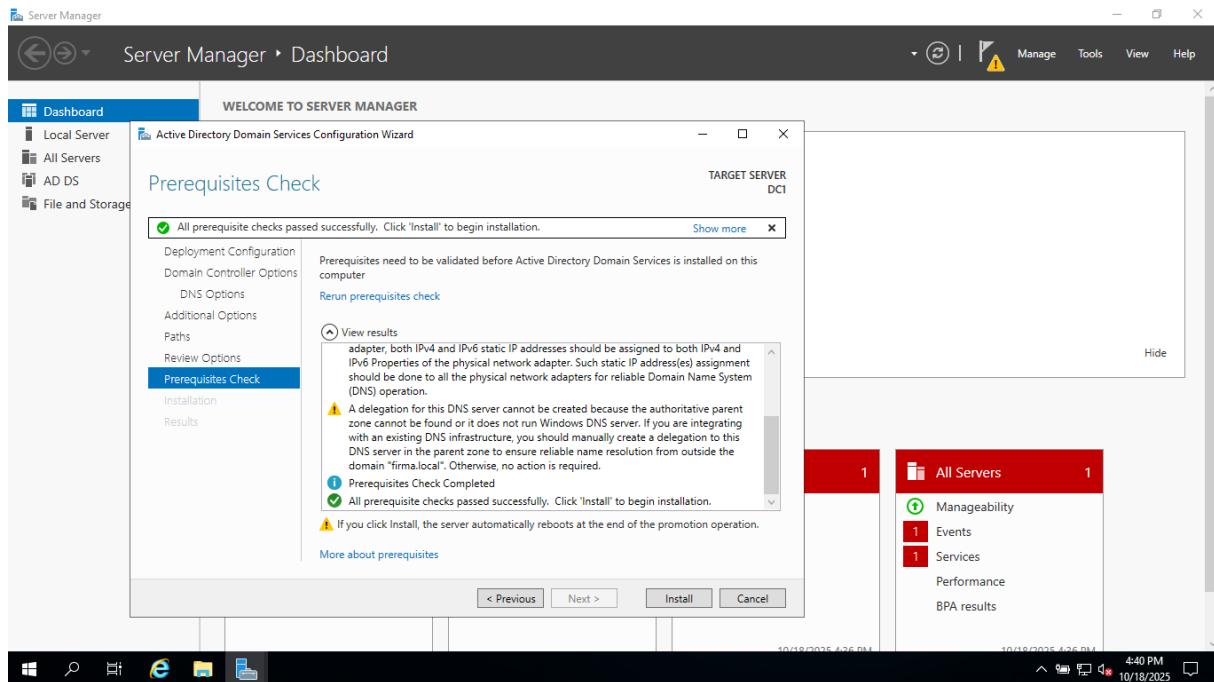
3.7. Sprawdzenie wymagań wstępnych

Przed rozpoczęciem instalacji kreator przeprowadza automatyczną weryfikację wymagań systemowych (Prerequisites Check).

Wszystkie testy zakończyły się pomyślnie — status:

- All prerequisite checks passed successfully.

Zignorowano jedynie ostrzeżenie dotyczące delegacji DNS, które nie jest błędem blokującym instalację.

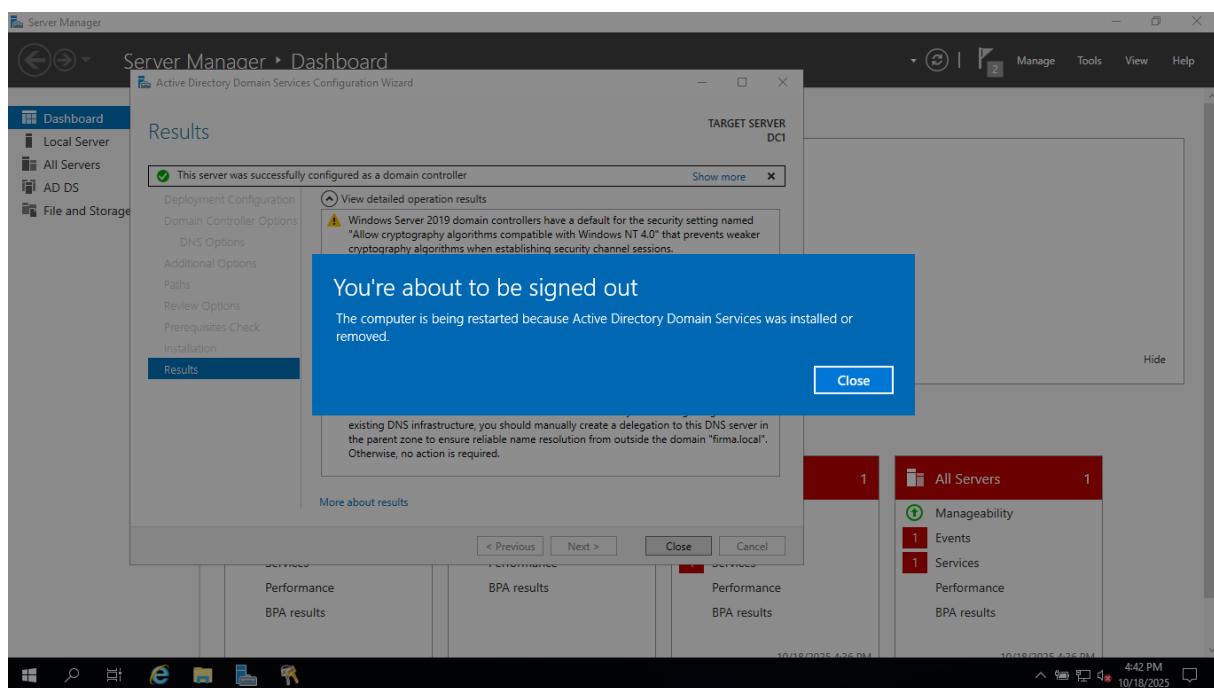


Rysunek 24 Wyniki sprawdzenia wymagań wstępnych

3.8. Instalacja i automatyczny restart systemu

Po kliknięciu Install, kreator rozpoczął proces tworzenia struktury domeny i promocji serwera do roli Domain Controller.

Po zakończeniu operacji system automatycznie uruchomił się ponownie, aby zastosować zmiany.



Rysunek 25 Komunikat o restarcie po zakończonej instalacji AD DS

3.9. Wnioski z etapu 3

W wyniku przeprowadzonego procesu:

- Utworzono nową domenę firma.local,
- Serwer DC1 został promowany do kontrolera domeny (Domain Controller),
- Automatycznie skonfigurowano usługę DNS, obsługującą nazwę domenową,
- Utworzono podstawowe jednostki organizacyjne i struktury AD DS.

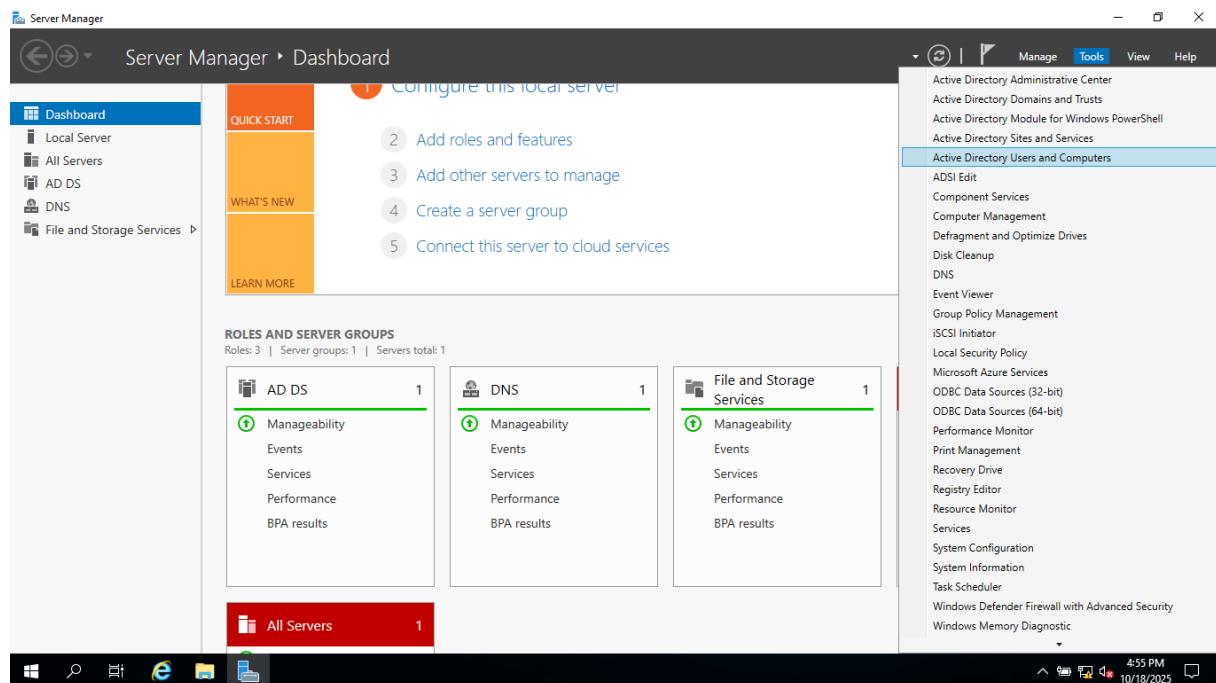
Serwer DC1 pełni teraz rolę głównego kontrolera domeny i jest gotowy do przyłączania stacji roboczych oraz zarządzania kontami użytkowników i zasobami sieciowymi.

4. Zarządzanie domeną i tworzenie kont użytkowników w Active Directory

Po pomyślnej instalacji i konfiguracji kontrolera domeny DC1 z domeną firma.local, kolejnym krokiem było utworzenie struktury organizacyjnej oraz kont użytkowników i grup w narzędziu Active Directory Users and Computers (ADUC).

4.1. Uruchomienie konsoli Active Directory Users and Computers

Z poziomu narzędzia Server Manager wybrano z menu Tools → Active Directory Users and Computers, aby otworzyć konsolę zarządzania strukturą domeny.

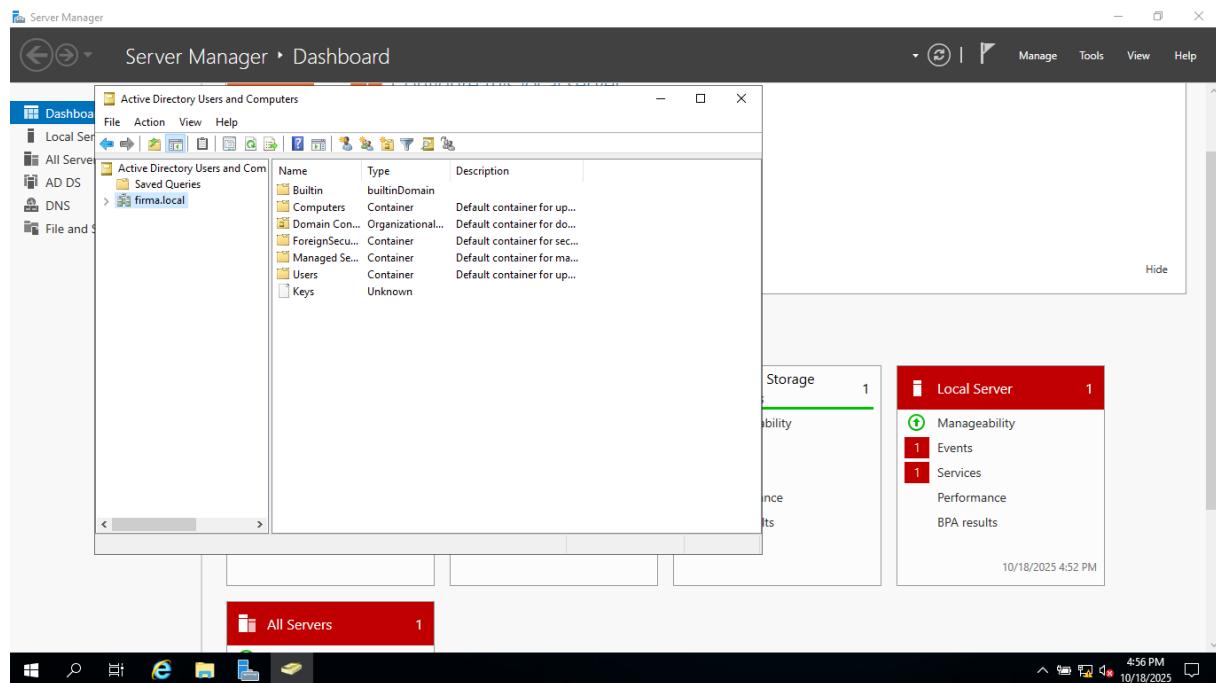


Rysunek 26 Uruchomienie narzędzia ADUC z poziomu Server Manager

4.2. Widok struktury domeny firma.local

Po uruchomieniu konsoli wyświetlono pełną strukturę katalogową domeny firma.local, zawierającą m.in. domyślne kontenery:

- Builtin – wbudowane grupy systemowe,
- Computers – konta komputerów dołączonych do domeny,
- Domain Controllers – serwery pełniące rolę kontrolerów domeny,
- Users – konta i grupy użytkowników domyślnych.



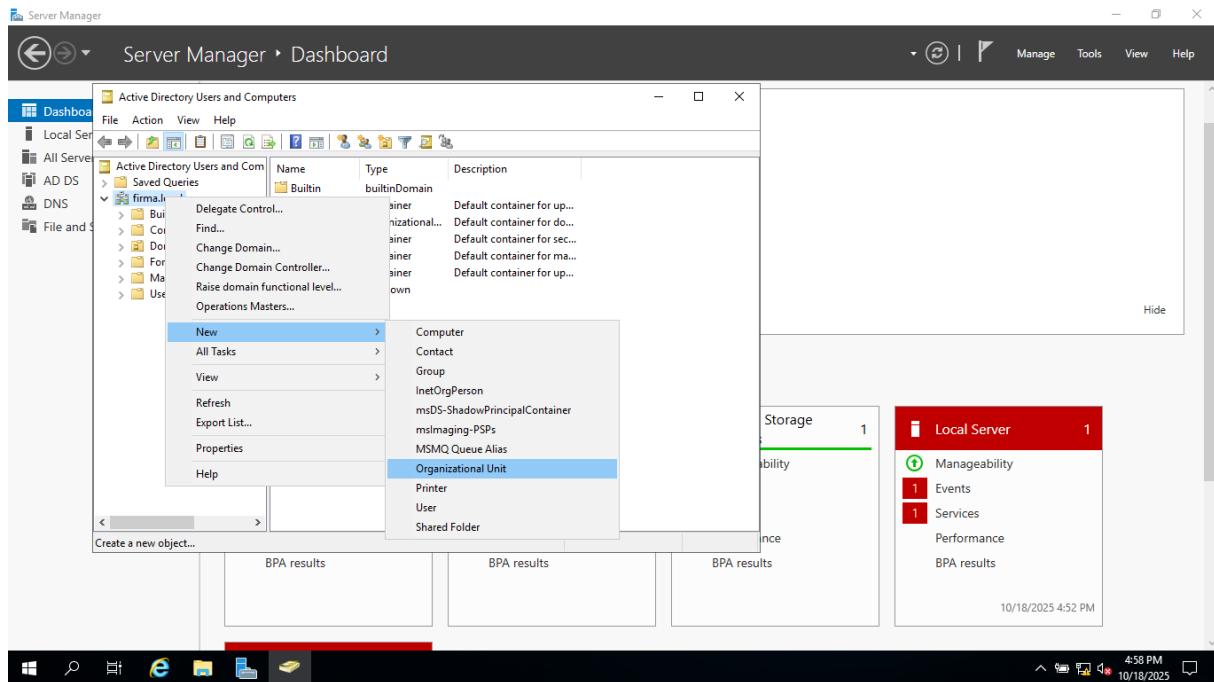
Rysunek 27 Widok podstawowej struktury domeny w konsoli ADUC

4.3. Tworzenie jednostki organizacyjnej (OU)

W celu uporządkowania obiektów domenowych utworzono nową jednostkę organizacyjną (Organizational Unit) o nazwie Dział_IT.

Aby to zrobić, kliknięto prawym przyciskiem myszy na nazwę domeny i wybrano:

- New → Organizational Unit



Rysunek 28 Tworzenie nowej jednostki organizacyjnej

Nowa jednostka pojawiła się w strukturze domeny i posłużyła do grupowania użytkowników oraz komputerów należących do działu IT.

4.4. Tworzenie grupy użytkowników

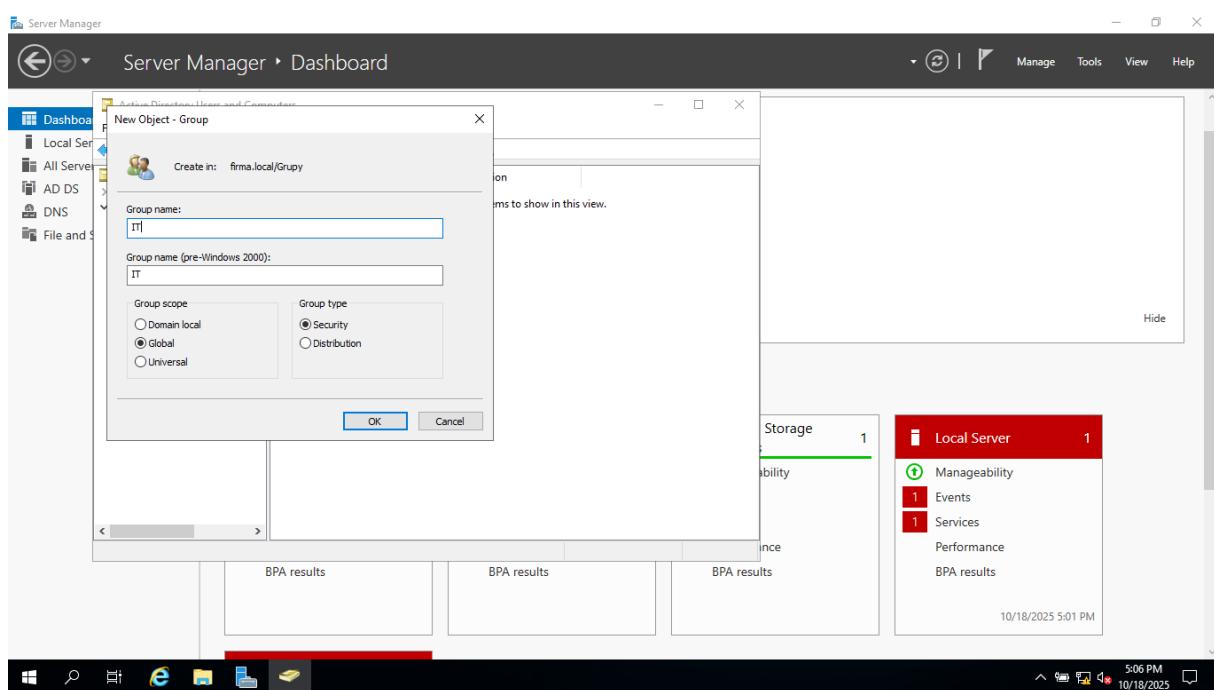
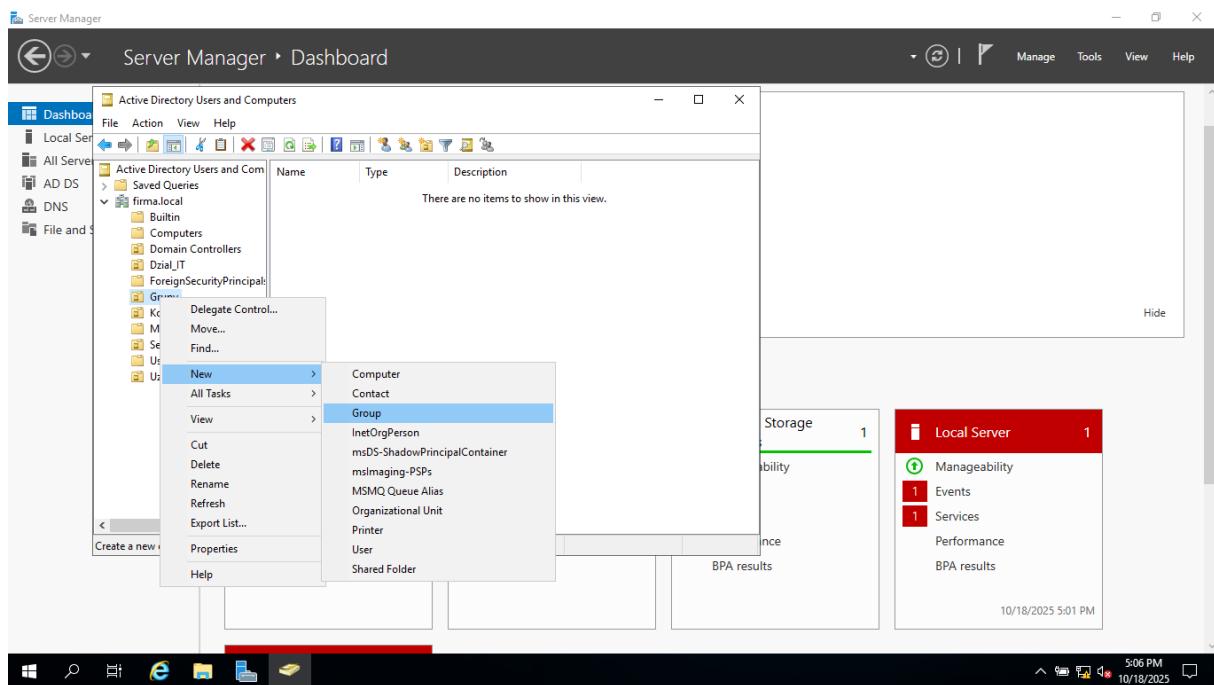
W ramach nowej jednostki organizacyjnej utworzono grupę domenową IT.

Z poziomu katalogu Dział_IT wybrano:

- New → Group

W oknie New Object – Group wprowadzono:

- Group name: IT
- Group scope: Global
- Group type: Security

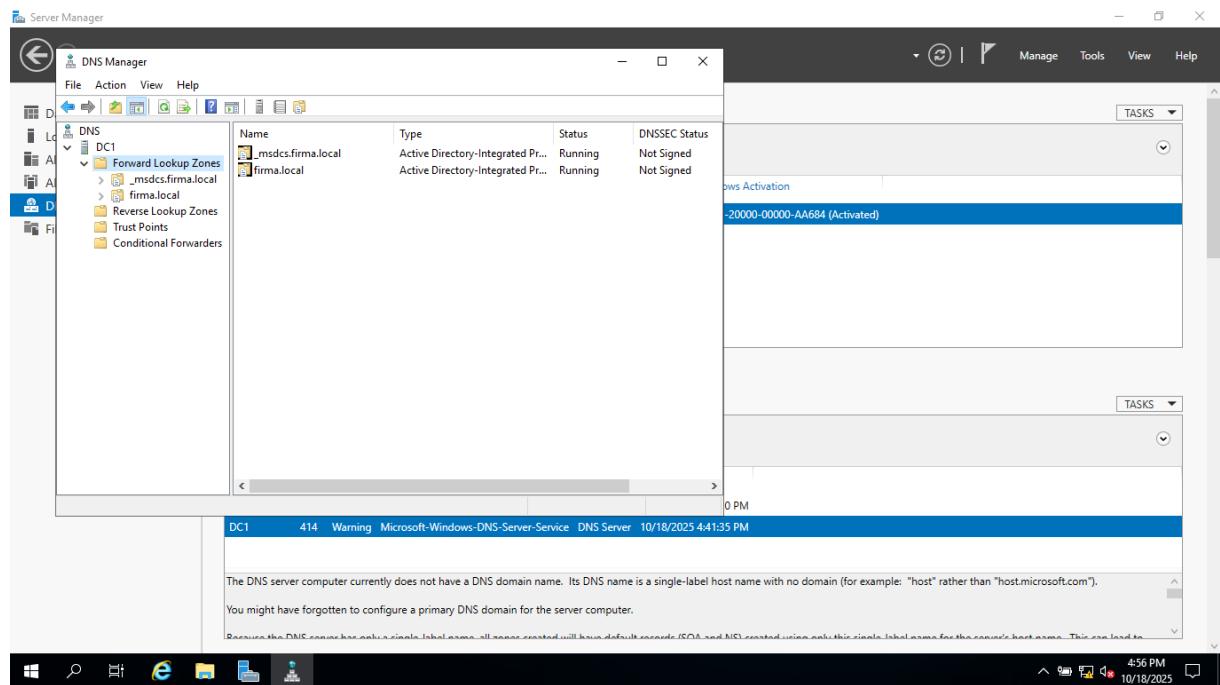


Rysunek 29 Tworzenie grupy domenowej IT

4.5. Weryfikacja konfiguracji DNS po promocji domeny

Po utworzeniu domeny sprawdzono poprawność działania usługi DNS w konsoli DNS Manager. W folderze Forward Lookup Zones znajdowały się dwie strefy:

- `_msdc.s.firma.local` – strefa usługowa dla kontrolera domeny,
- `firma.local` – strefa główna domeny, przechowująca rekordy A, NS i SRV.



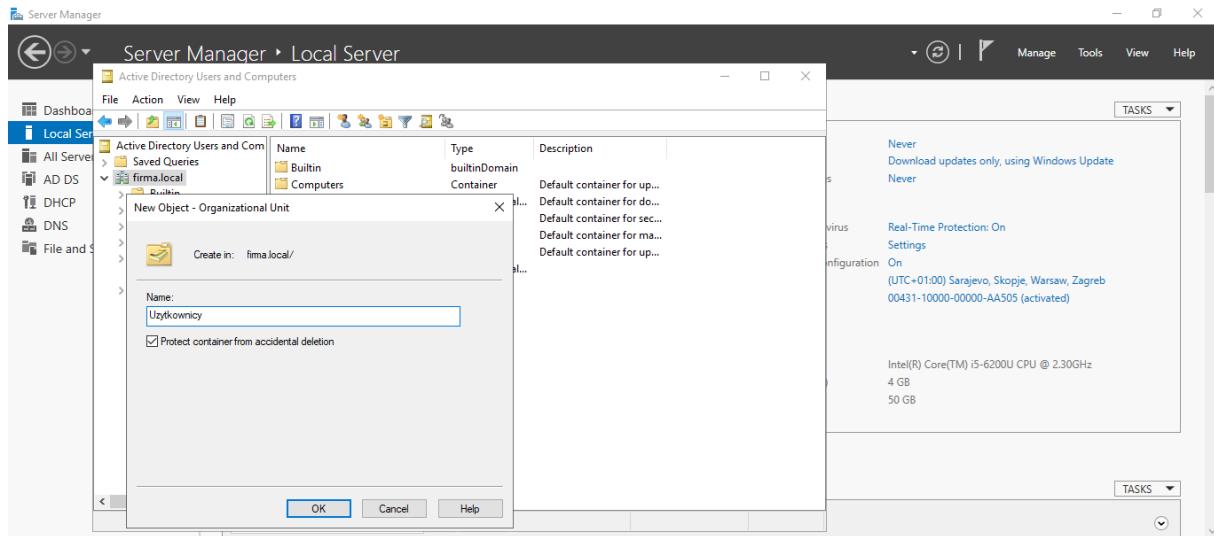
Rysunek 30 Struktura stref DNS utworzonej domeny

4.6. Tworzenie folderu na użytkowników domenowych

Dla lepszej organizacji zasobów stworzono nowy folder (OU) o nazwie Użytkownicy, który będzie zawierał konta osób należących do domeny.

Wybór:

- New → Organizational Unit → Użytkownicy



Rysunek 31 Utworzenie jednostki organizacyjnej dla użytkowników domenowych

4.7. Tworzenie konta użytkownika domenowego

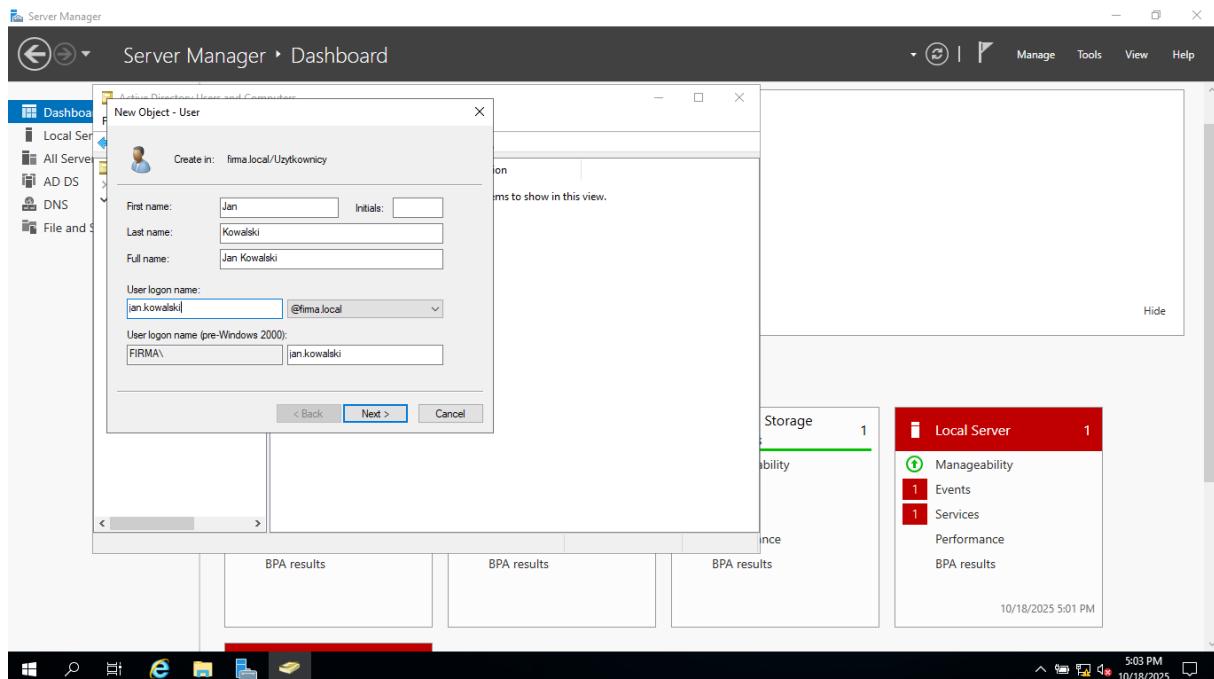
W folderze Użytkownicy utworzono konto użytkownika o danych:

- Imię: Jan
- Nazwisko: Kowalski
- Login domenowy: jan.kowalski@firma.local

W tym celu wybrano:

- New → User

i wypełniono formularz New Object – User.



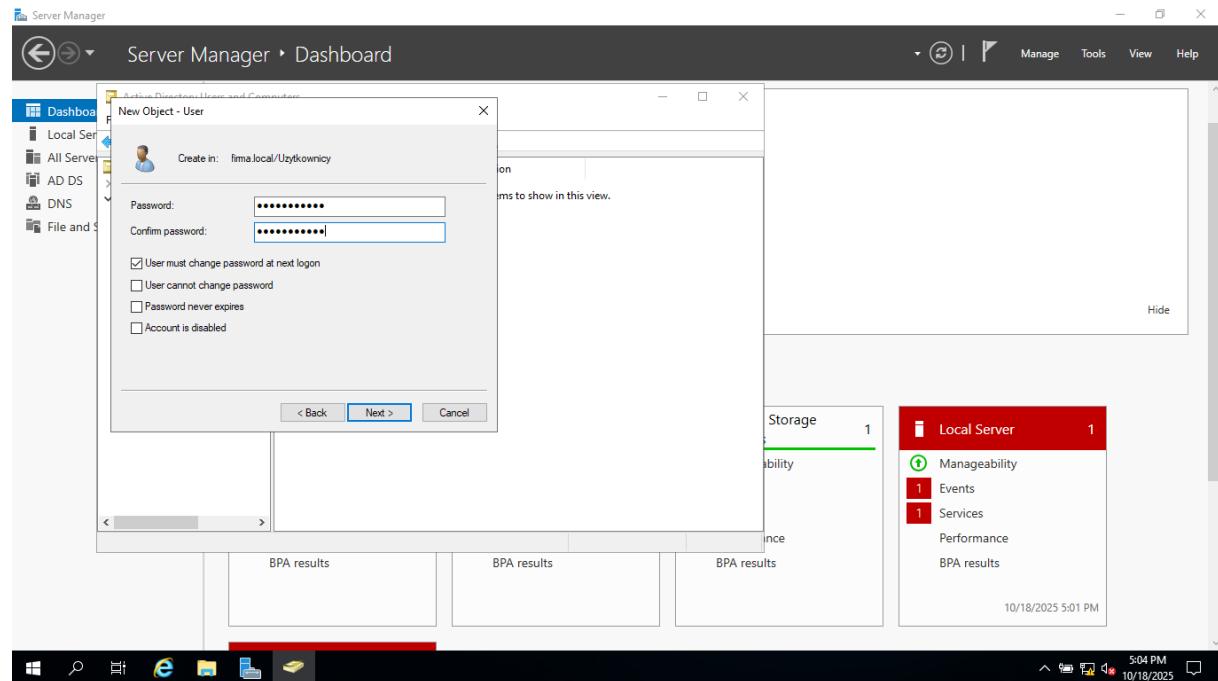
Rysunek 32 Tworzenie nowego użytkownika domenowego Jan Kowalski

4.8.Ustawienie hasła i zasad logowania

W kolejnym kroku ustalono hasło początkowe dla użytkownika oraz wymuszono jego zmianę przy pierwszym logowaniu.

Zaznaczono opcję:

- User must change password at next logon

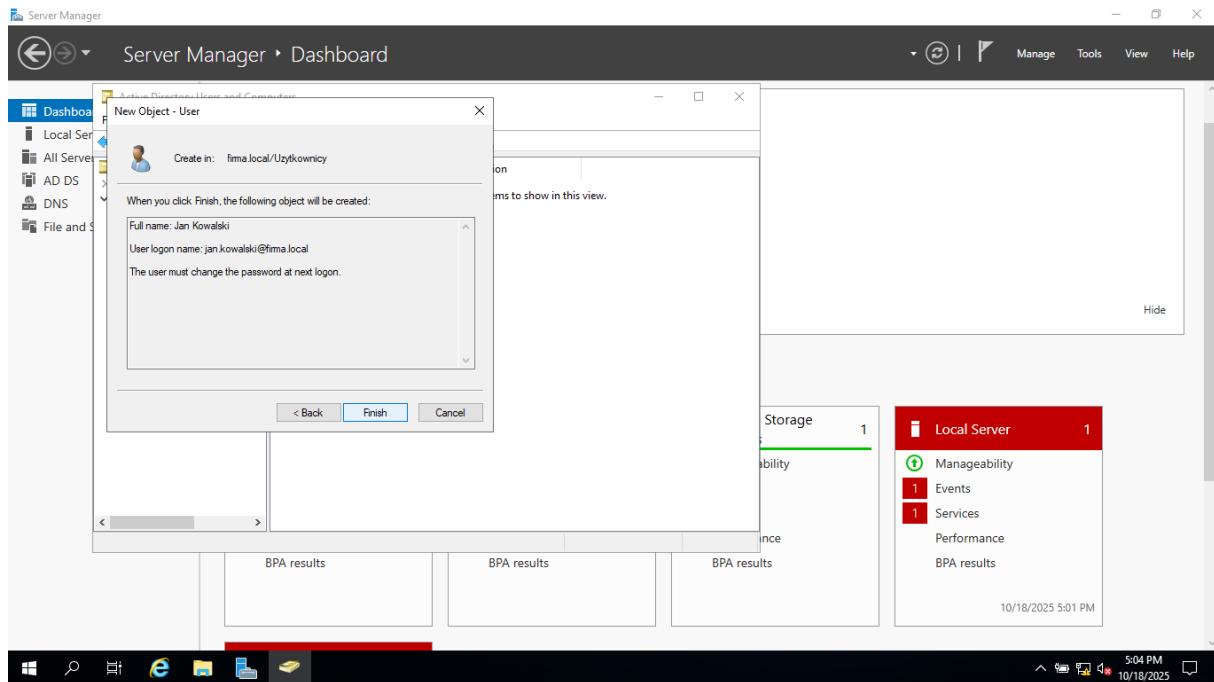


Rysunek 33 Ustalanie hasła użytkownika i opcji logowania

4.9.Podsumowanie tworzenia użytkownika

Po zakończeniu kreatora wyświetlono ekran podsumowujący utworzenie konta użytkownika:

- Pełna nazwa: Jan Kowalski,
- Login domenowy: jan.kowalski@firma.local ,
- Wymagana zmiana hasła przy pierwszym logowaniu.



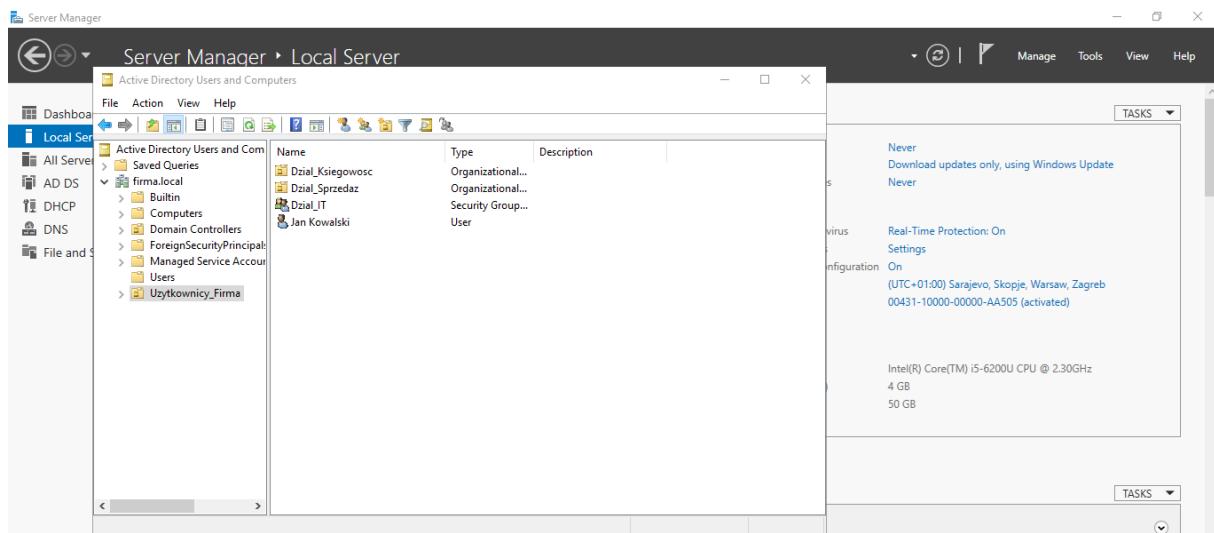
Rysunek 34 Potwierdzenie utworzenia konta użytkownika

4.10. Weryfikacja utworzonych obiektów domenowych

W końcowym etapie sprawdzono w konsoli ADUC, że w domenie firma.local znajdują się:

- jednostki organizacyjne: Dział_IT, Użytkownicy,
- grupa domenowa: IT,
- użytkownik: Jan Kowalski.

Wszystkie obiekty zostały poprawnie zarejestrowane w katalogu Active Directory.



Rysunek 35 Widok końcowy struktury domeny po utworzeniu obiektów

4.11. Wnioski z etapu 4

W wyniku wykonanych czynności:

- Utworzono logiczną strukturę domeny z jednostkami organizacyjnymi,
- Skonfigurowano grupę i konto użytkownika,
- Zweryfikowano poprawne działanie usługi DNS oraz AD DS,
- System jest gotowy do dalszej konfiguracji polityk bezpieczeństwa (GPO) i przyłączania komputerów klienckich do domeny.

Serwer DC1 w domenie firma.local funkcjonuje poprawnie jako pełny kontroler domeny z działającą strukturą Active Directory.

5. Przyłączanie komputera klienckiego do domeny firma.local

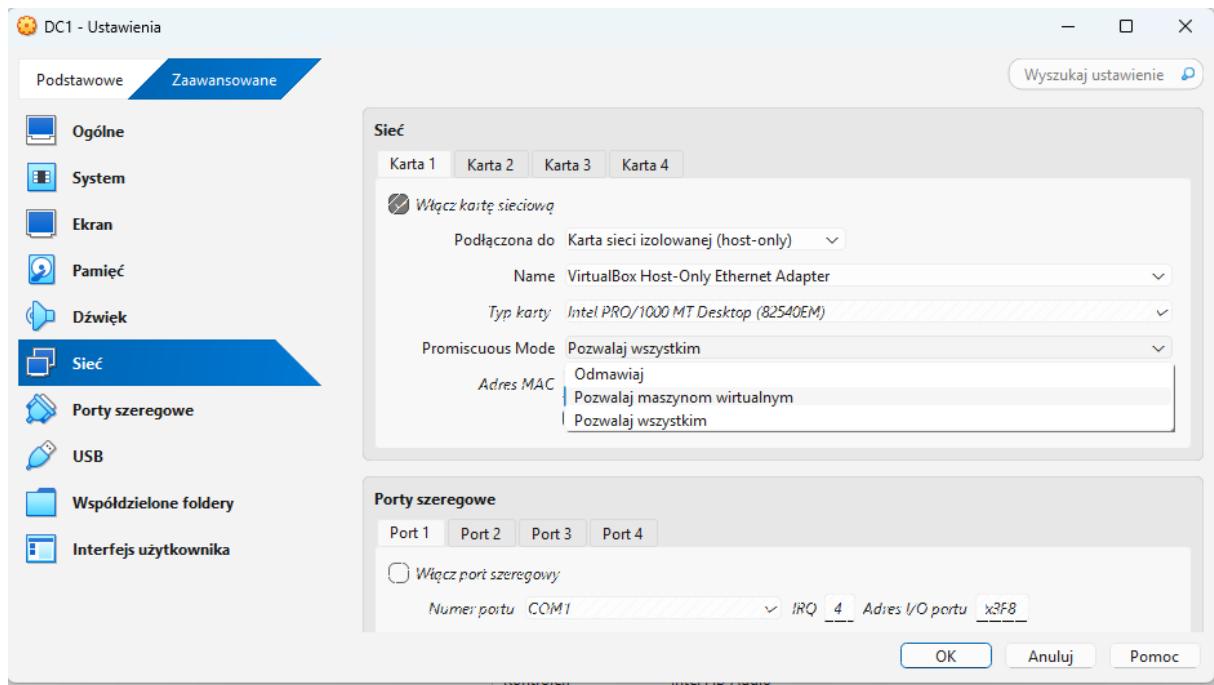
Po utworzeniu domeny firma.local oraz skonfigurowaniu struktury użytkowników i grup w serwerze DC1, przystąpiono do podłączenia komputera klienckiego (system Windows 10) do domeny. Dzięki temu użytkownicy domenowi będą mogli logować się na komputerach klienckich z użyciem swoich kont domenowych.

5.1. Sprawdzenie konfiguracji sieci kontrolera domeny

Aby komputer kliencki mógł połączyć się z domeną, konieczne było upewnienie się, że kontroler domeny DC1 jest poprawnie skonfigurowany sieciowo i pełni rolę serwera DNS w sieci wirtualnej.

W ustawieniach maszyny w VirtualBox wybrano tryb:

- Karta sieci izolowanej (Host-Only Adapter)
oraz tryb promiscuous ustawiono na Pozwalaj wszystkim.

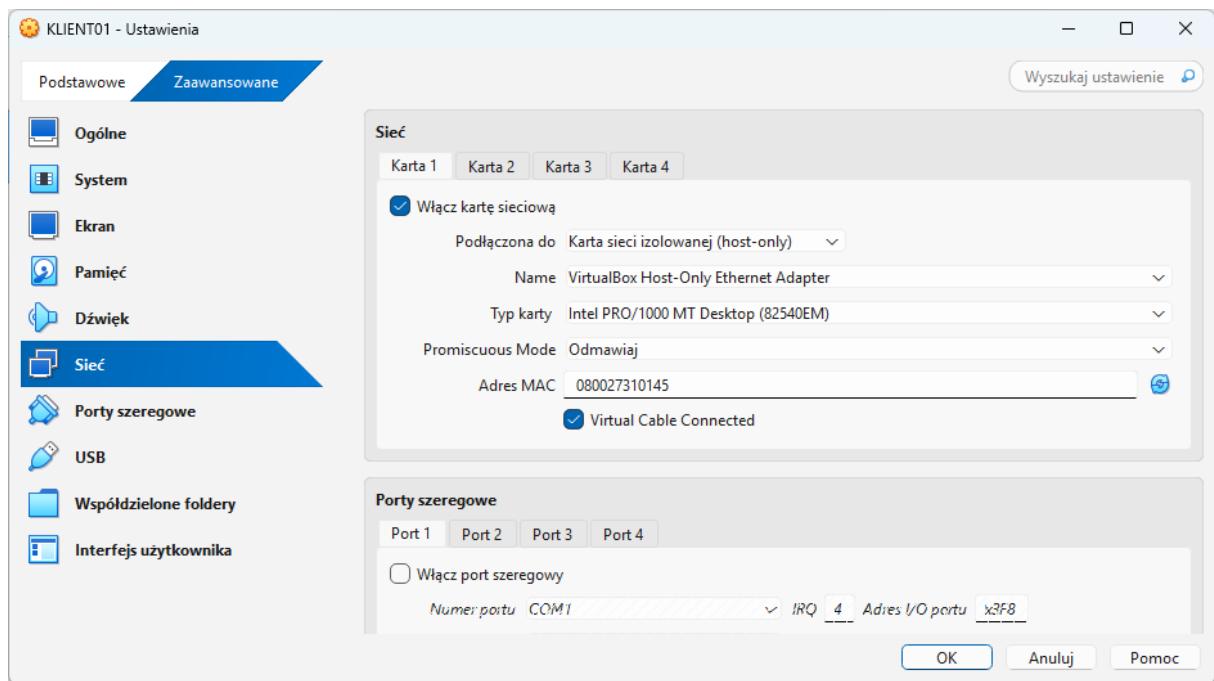


Rysunek 36 Konfiguracja sieci serwera DC1 w środowisku VirtualBox

5.2. Konfiguracja sieci komputera klienckiego

Analogicznie skonfigurowano sieć komputera klienckiego o nazwie KLIENT01, ustawiając:

- Typ połączenia: Karta sieci izolowanej (Host-Only)
- Karta sieciowa: Intel PRO/1000 MT Desktop (82540EM)
- Opcja „Virtual Cable Connected” – aktywna



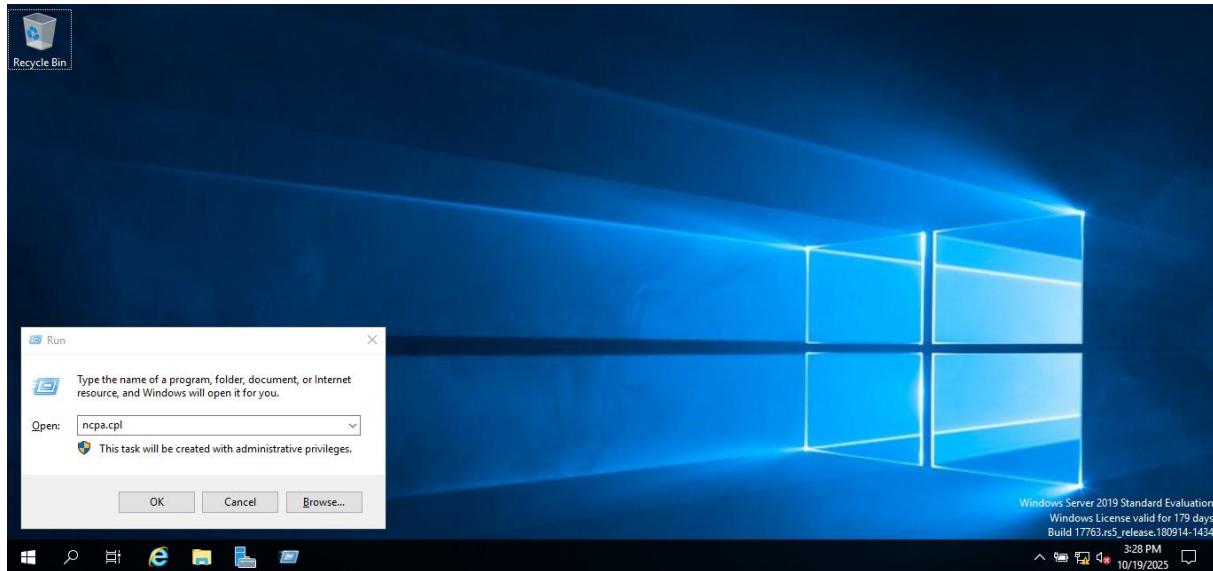
Rysunek 37 Ustawienia sieciowe komputera klienckiego w VirtualBox

5.3.Uruchomienie klienta i otwarcie konfiguracji sieci

Po uruchomieniu systemu Windows 10 na komputerze KLIENT01, w celu ustawienia adresacji IP, otwarto okno uruchamiania (Win + R) i wpisano polecenie:

- ncpa.cpl

co otworzyło panel połączeń sieciowych.



Rysunek 38 Uruchomienie konfiguracji sieci przez polecenie

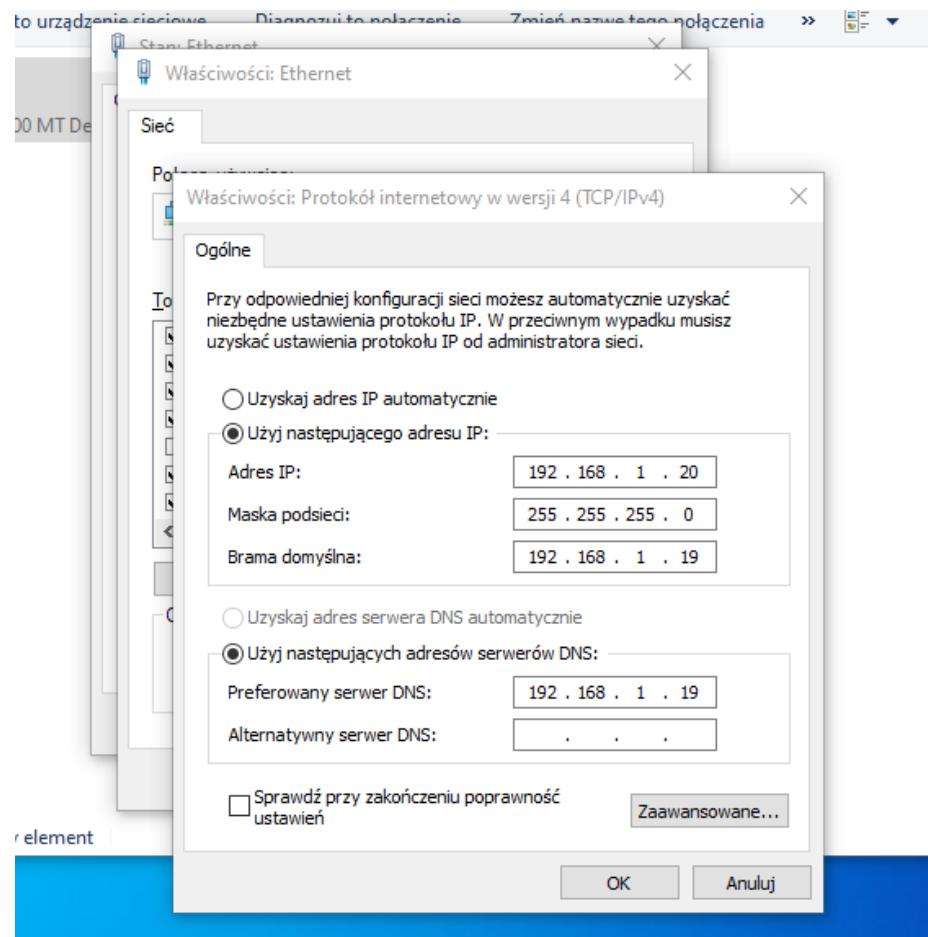
5.4.Ustawienie statycznego adresu IP

W oknie właściwości połączenia Ethernet wybrano:

- Properties → Internet Protocol Version 4 (TCP/IPv4)

i wprowadzono następujące dane:

- Adres IP: 192.168.1.20
- Maska podsieci: 255.255.255.0
- Brama domyślna: 192.168.1.19
- Preferowany serwer DNS: 192.168.1.19 (adres serwera DC1)



Rysunek 39 Ustawienia protokołu IPv4 dla komputera klienckiego

5.5. Sprawdzenie połączenia z serwerem DC1

W celu weryfikacji komunikacji między klientem a kontrolerem domeny, uruchomiono Wiersz poleceń i wykonano test:

- ping DC1
ping 192.168.1.19

Odpowiedź serwera potwierdziła prawidłowe połączenie sieciowe.

```

Wiersz polecenia
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\anna.nowak>ping 192.168.1.19

Pinging 192.168.1.19 with 32 bytes of data:
Reply from 192.168.1.19: bytes=32 time<1ms TTL=128
Reply from 192.168.1.19: bytes=32 time=2ms TTL=128
Reply from 192.168.1.19: bytes=32 time=3ms TTL=128
Reply from 192.168.1.19: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Users\anna.nowak>pind DC1
'pind' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\anna.nowak>ping DC1

Pinging DC1.firma.local [192.168.1.19] with 32 bytes of data:
Reply from 192.168.1.19: bytes=32 time<1ms TTL=128
Reply from 192.168.1.19: bytes=32 time=2ms TTL=128
Reply from 192.168.1.19: bytes=32 time=2ms TTL=128
Reply from 192.168.1.19: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\anna.nowak>_

```

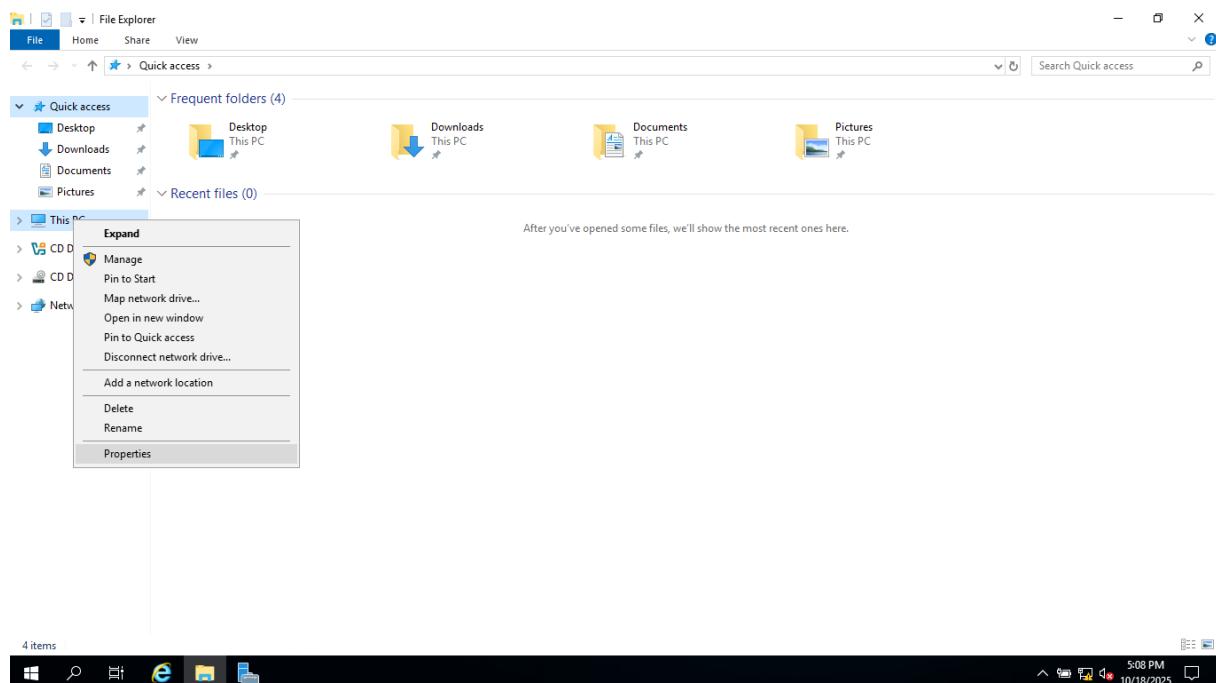
Rysunek 40 Sprawdzenie łączności z serwerem domeny

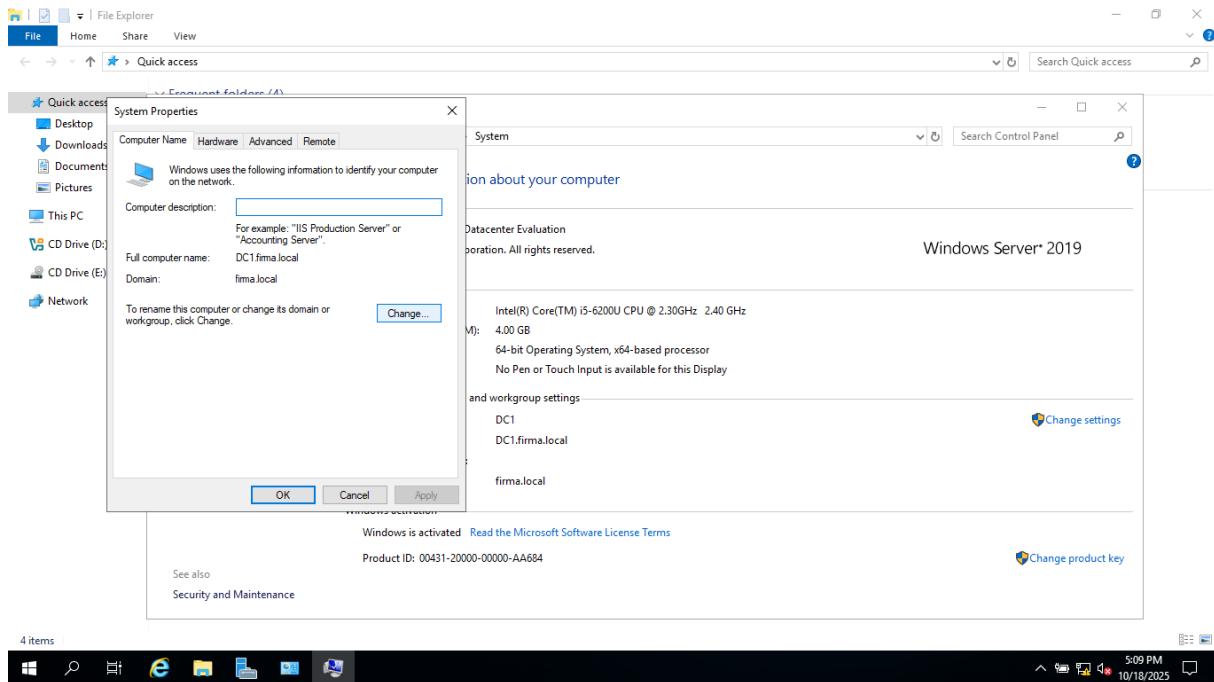
5.6. Sprawdzenie informacji o domenie na serwerze

Na serwerze DC1 otwarto właściwości systemu w celu potwierdzenia, że serwer jest już członkiem domeny firma.local.

W zakładce Computer Name widniały wpisy:

- Full computer name: DC1.firma.local
- Domain: firma.local

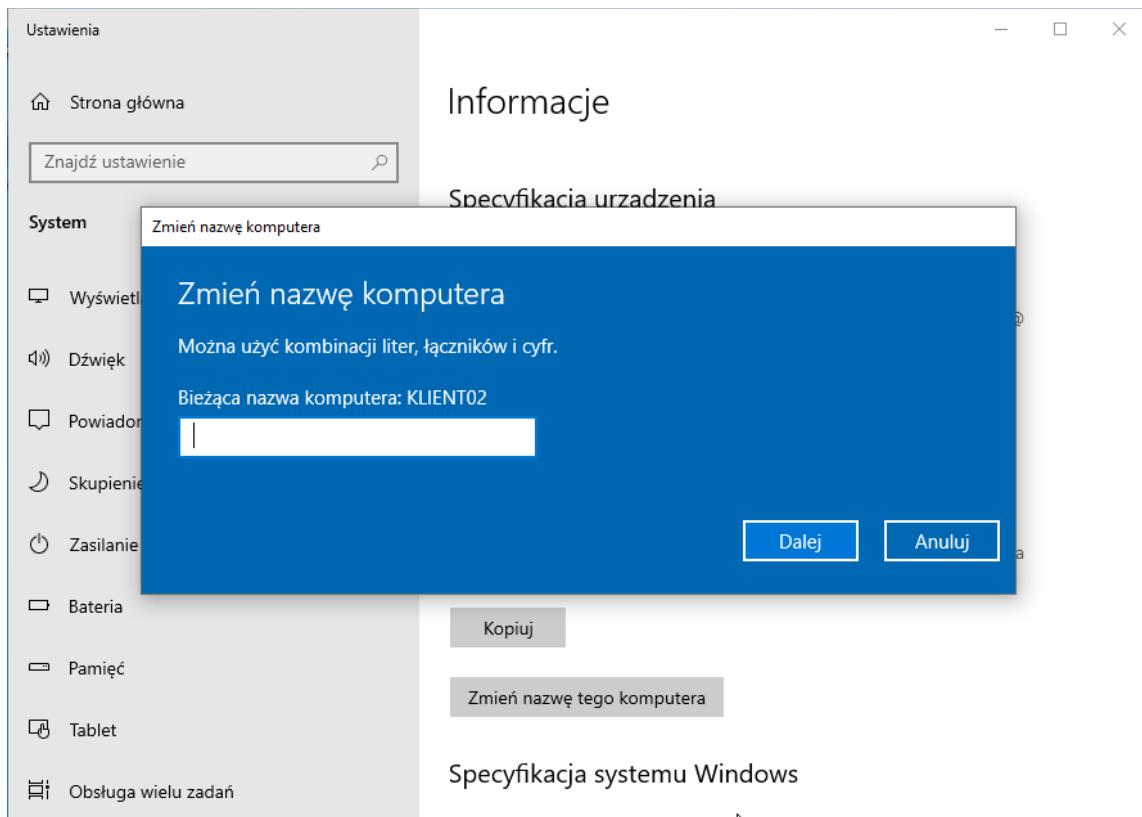




Rysunek 41 Potwierdzenie przynależności serwera DC1 do domeny

5.7.Uruchomienie konfiguracji systemu klienta

Na komputerze klienckim otwarto This PC → Properties → Advanced system settings → Computer Name, a następnie kliknięto przycisk Change w celu zmiany grupy roboczej na domenę.



Rysunek 42 Przejście do ustawień domeny komputera klienckiego

5.8. Dołączenie komputera do domeny firma.local

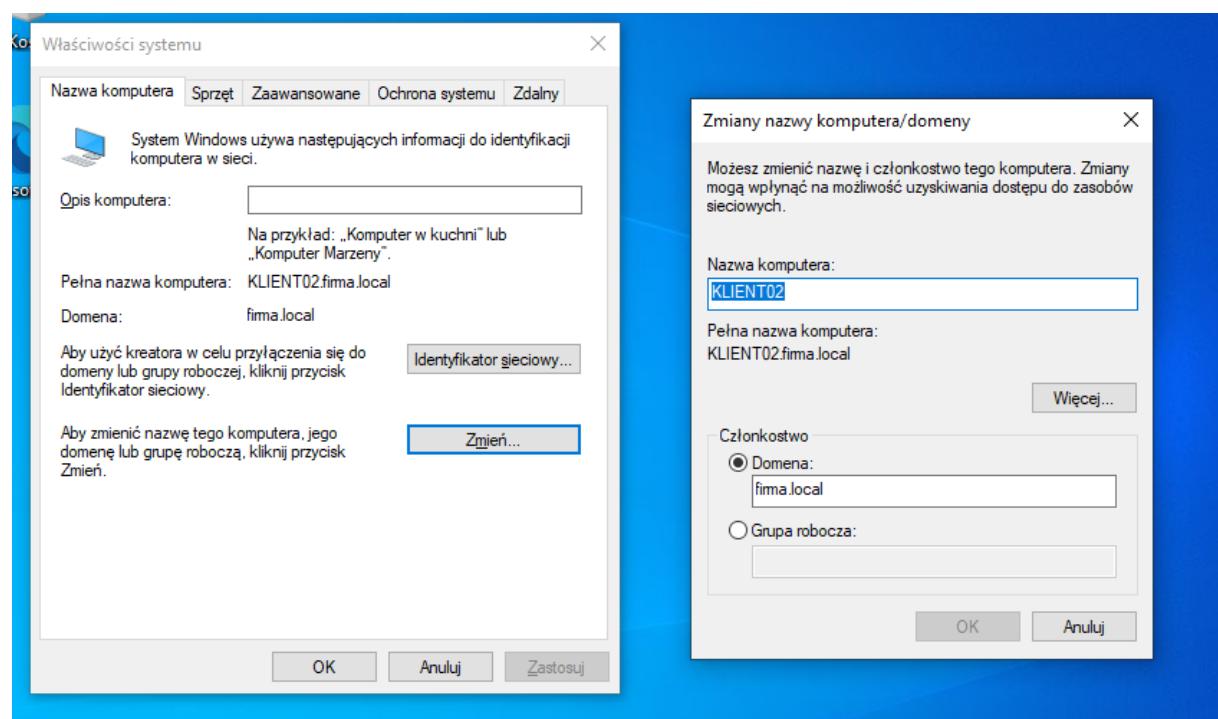
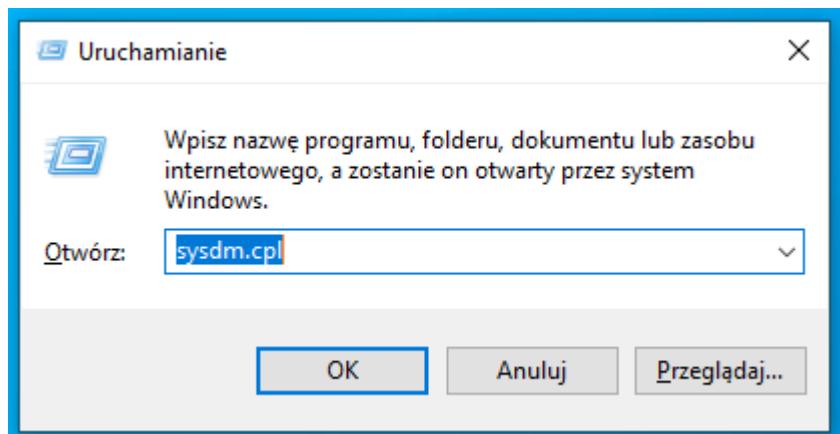
W otwartym oknie System Properties zaznaczono opcję:

- Member of → Domain

i wpisano nazwę domeny:

- firma.local

Po zatwierdzeniu system poprosił o dane konta domenowego z uprawnieniami administracyjnymi (np. Administrator domeny).



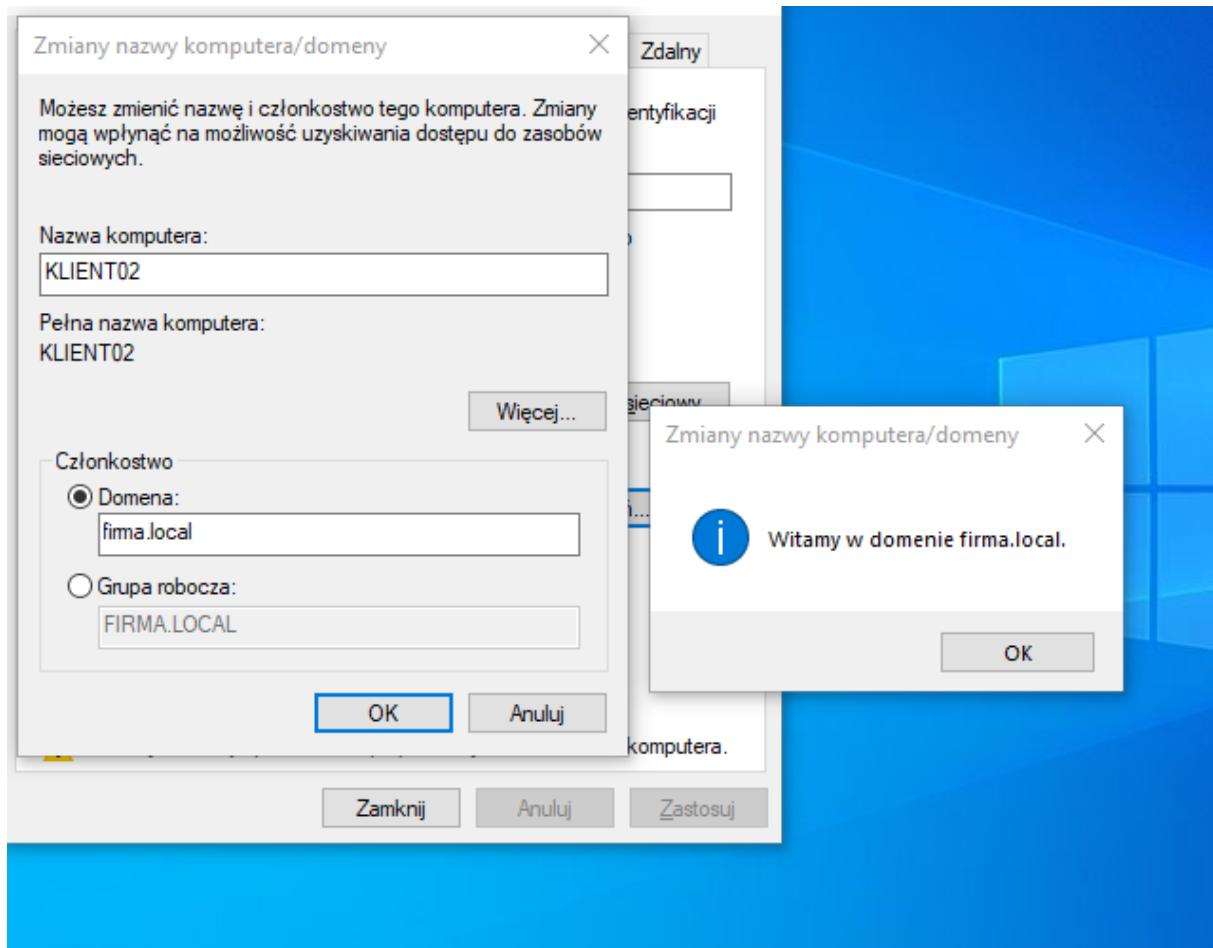
Rysunek 43 Przejście do ustawień domeny komputera klienckiego

5.9. Potwierdzenie dołączenia komputera do domeny

Po pomyślnym uwierzytelnieniu pojawił się komunikat:

- Welcome to the firma.local domain.

Po jego zaakceptowaniu komputer został automatycznie zrestartowany.



Rysunek 44 Potwierdzenie przyłączenia komputera do domeny

5.10. Weryfikacja w konsoli ADUC

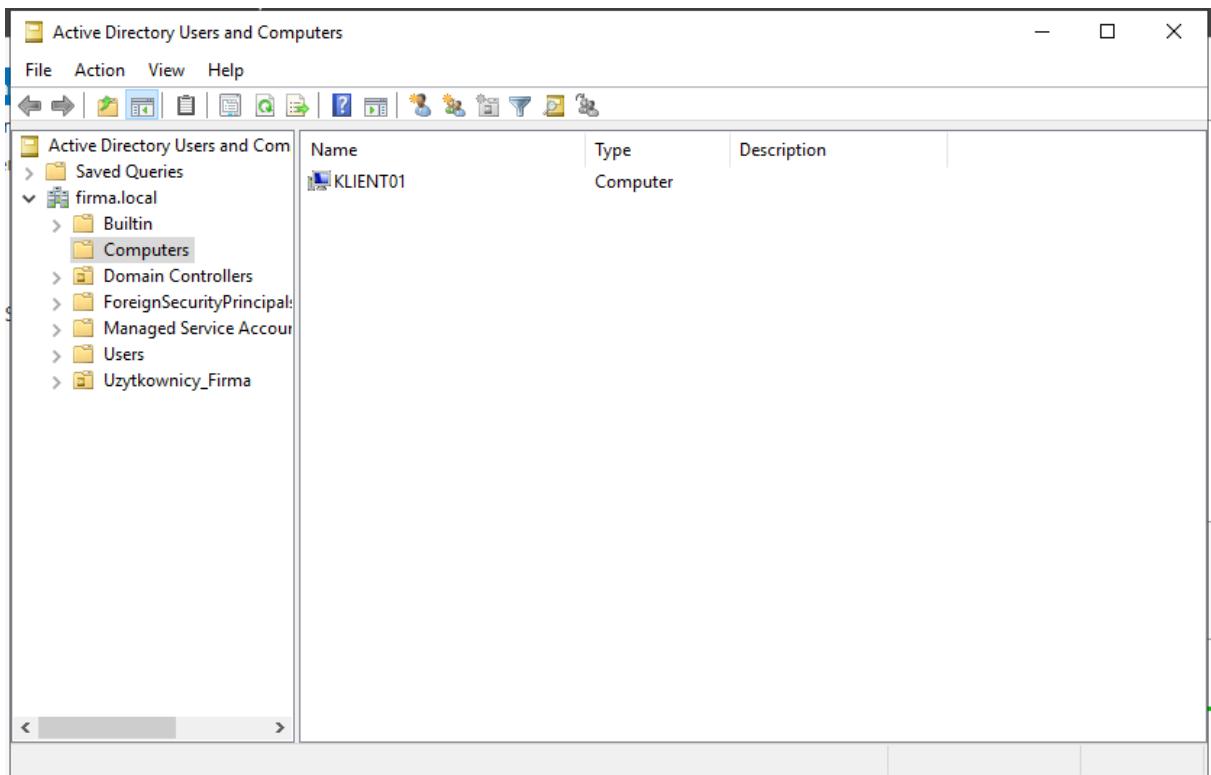
Po ponownym uruchomieniu komputera klienta, w konsoli Active Directory Users and Computers na serwerze DC1 w folderze Computers pojawił się nowy obiekt:

- KLIENT01

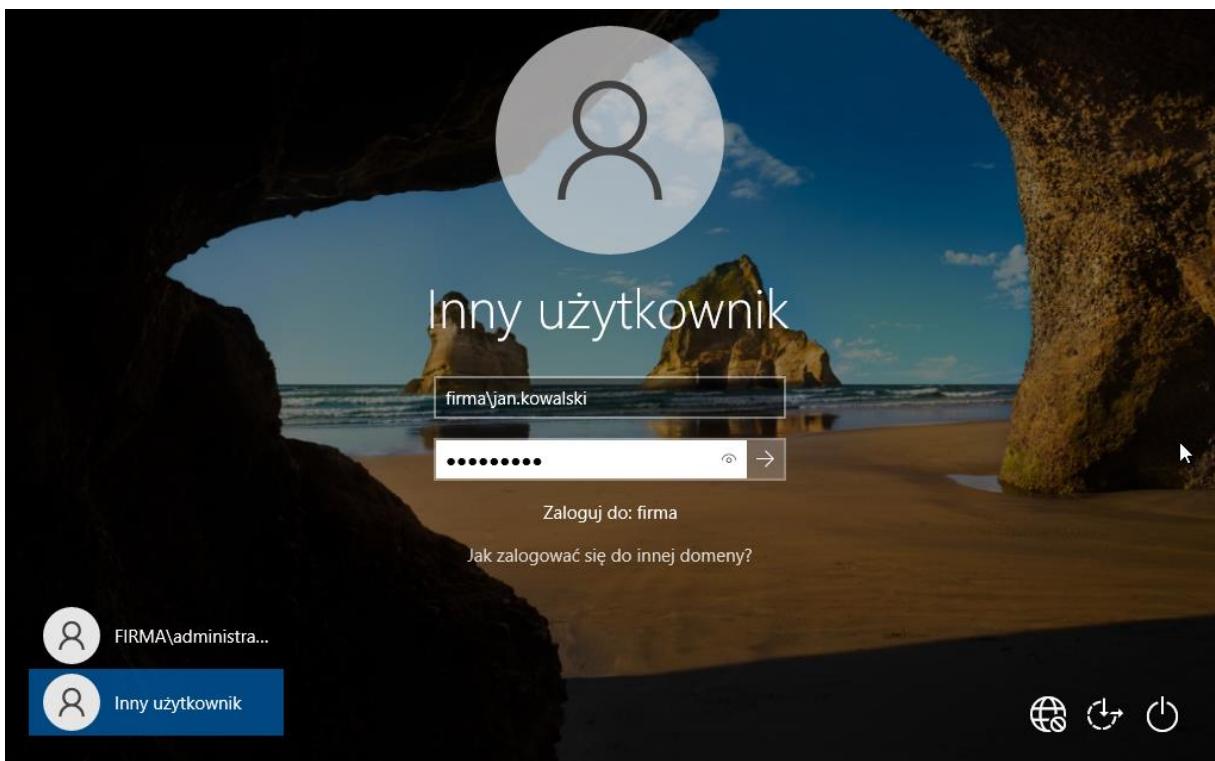
oznaczający, że komputer został prawidłowo zarejestrowany w domenie.

Po restarcie systemu użytkownik mógł wybrać opcję Inny użytkownik i zalogować się do domeny za pomocą konta:

- firma\jan.kowalski



Rysunek 45 Widok przyłączonego komputera w domenie



5.11. Wnioski z etapu 5

W wyniku przeprowadzonego procesu:

- Komputer kliencki KLIENT01 został pomyślnie przyłączony do domeny firma.local,
- Została skonfigurowana poprawna komunikacja z kontrolerem domeny (DC1),
- Użytkownicy domenowi (np. Jan Kowalski) mogą teraz logować się na komputerze klienckim, korzystając z konta domenowego,
- Usługa DNS działa prawidłowo, umożliwiając rozpoznawanie nazw domenowych w sieci.

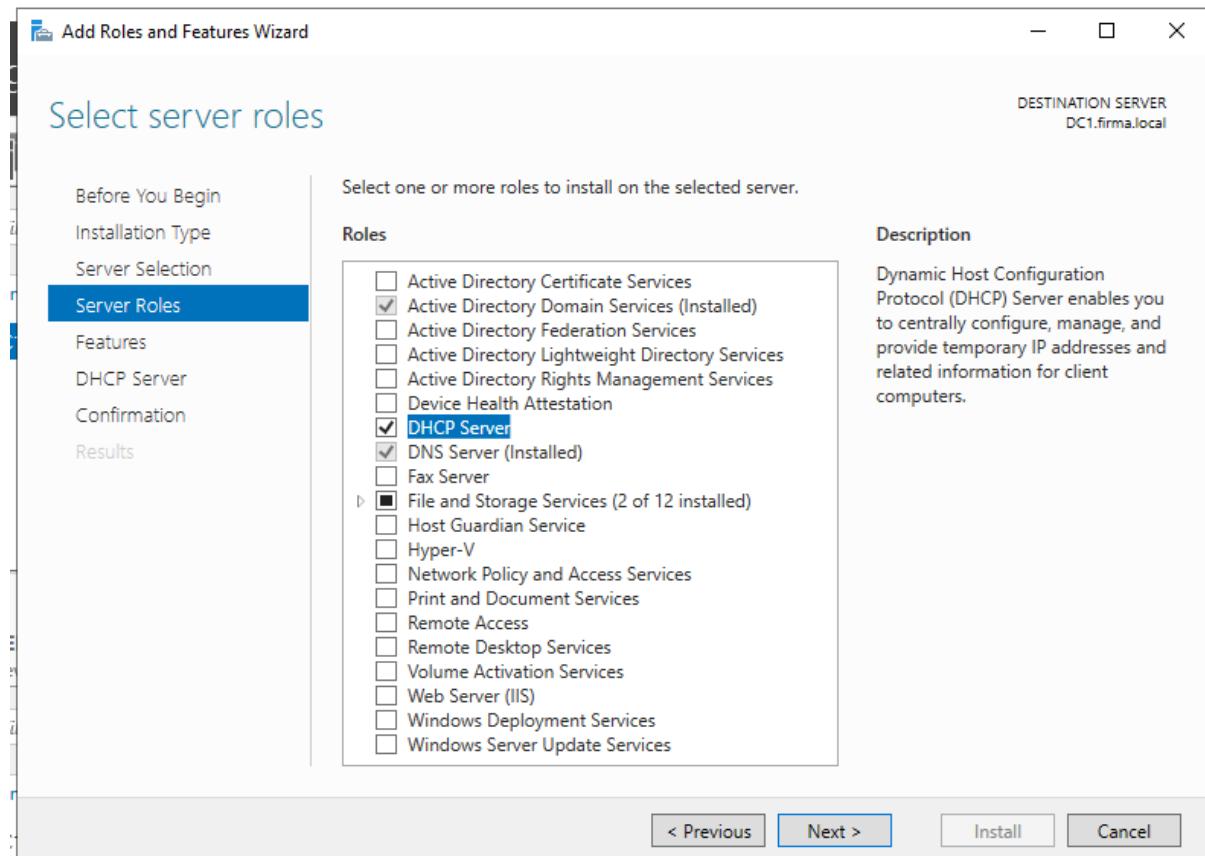
System domenowy jest w pełni funkcjonalny i gotowy do dalszej konfiguracji.

6. Konfiguracja serwera DHCP

Po poprawnym przyłączeniu komputera klienckiego KLIENT01 do domeny firma.local przystąpiono do uruchomienia usługi DHCP na serwerze DC1. Dzięki serwerowi DHCP (Dynamic Host Configuration Protocol) klienci sieci mogą automatycznie otrzymywać adresy IP, maskę podsieci, bramę domyślną i adresy DNS bez potrzeby ręcznej konfiguracji.

6.1. Dodanie roli serwera DHCP

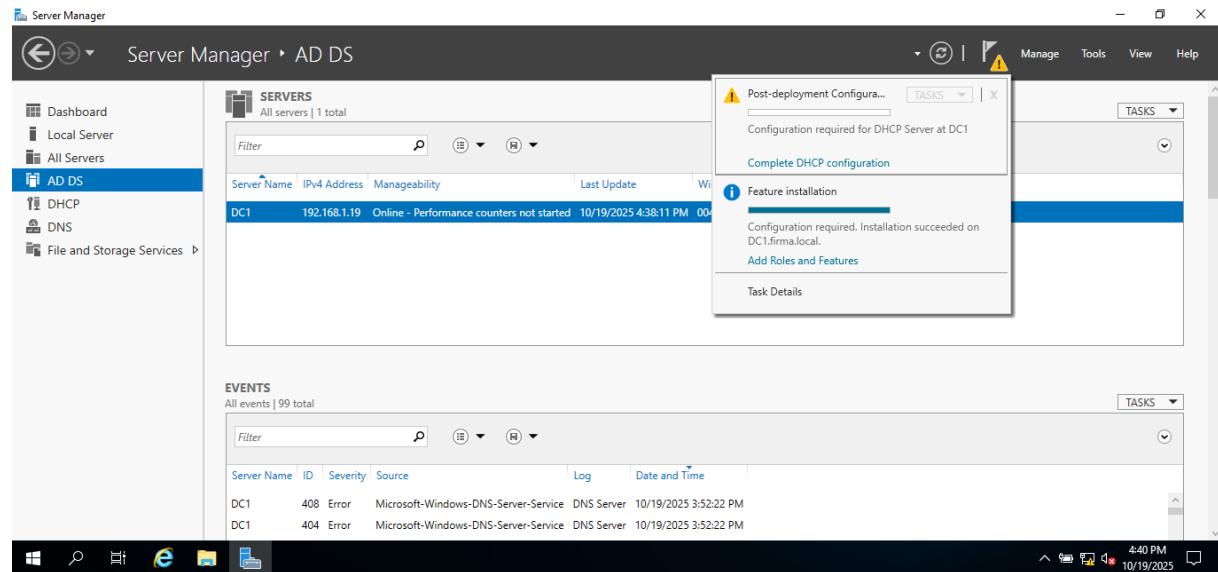
W konsoli Server Manager wybrano opcję Add Roles and Features i uruchomiono kreator dodawania ról. W sekcji Server Roles zaznaczono pozycję DHCP Server, po czym kliknięto Next i zatwierdzono instalację



Rysunek 46 Wybór roli DHCP Server w kreatorze instalacji

6.2.Zakończenie instalacji i konfiguracja końcowa

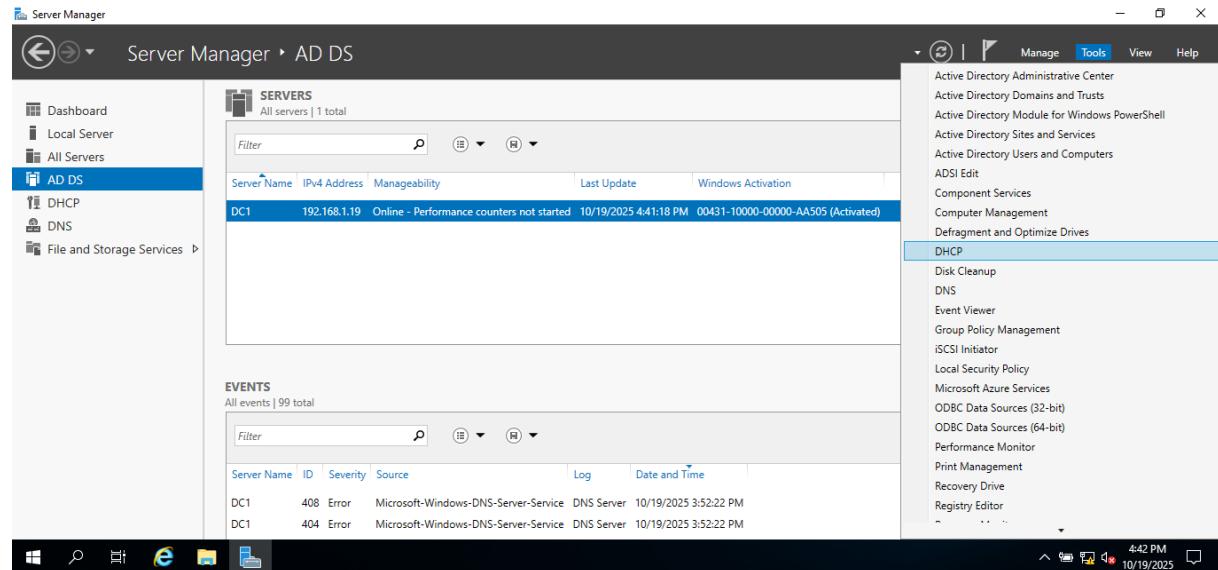
Po zakończeniu instalacji system wyświetlił komunikat o konieczności wykonania konfiguracji końcowej („Post-deployment configuration”). Kliknięto łącze Complete DHCP configuration, aby autoryzować serwer DHCP w domenie firma.local.



Rysunek 47 Komunikat o konieczności konfiguracji końcowej DHCP

6.3.Otwarcie konsoli zarządzania DHCP

Po zakończeniu konfiguracji w Server Manager → Tools wybrano pozycję DHCP, co otworzyło konsolę zarządzania usługą DHCP. W drzewie po lewej stronie widoczny był serwer dc1.firma.local oraz sekcje IPv4 i IPv6.



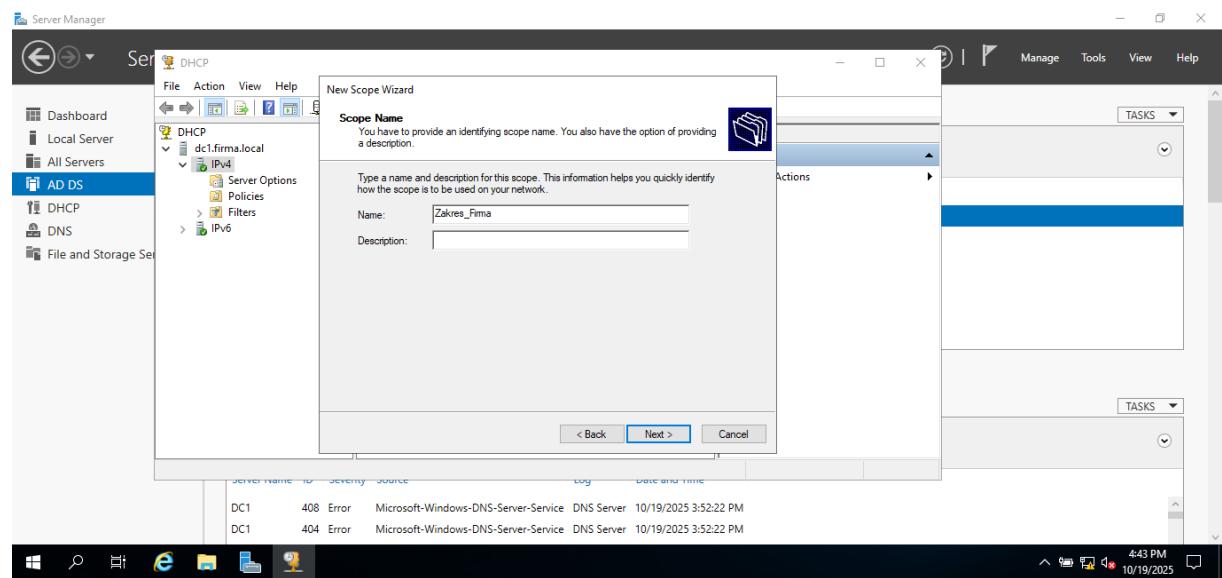
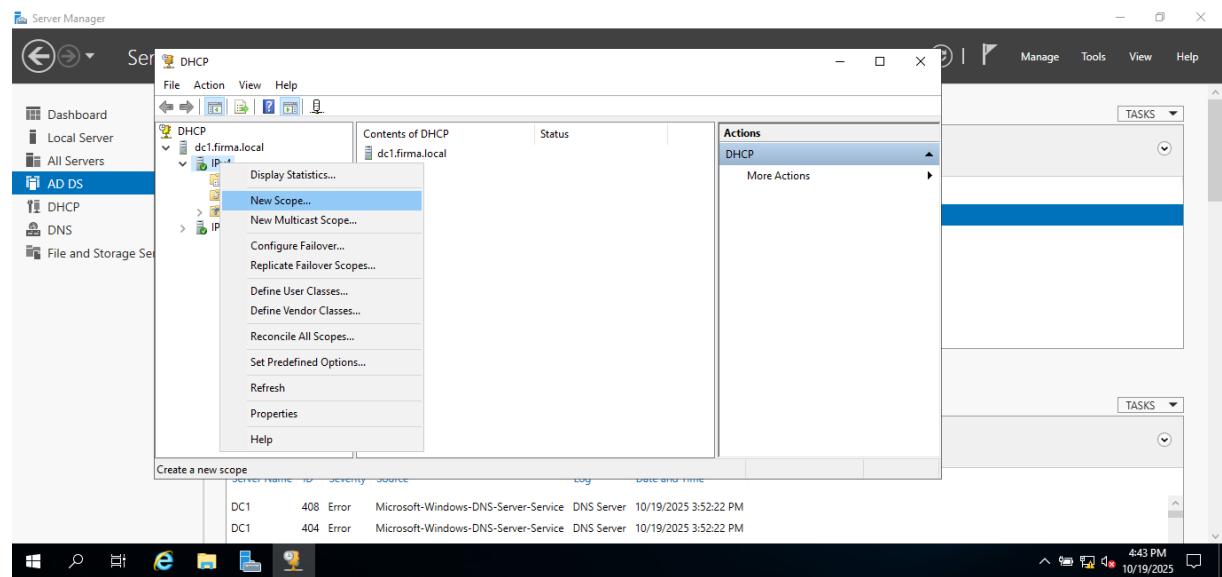
Rysunek 48 Otwarcie konsoli DHCP z poziomu Server Managera

6.4. Tworzenie nowego zakresu adresów (New Scope)

Kliknięto prawym przyciskiem myszy na sekcję IPv4 i wybrano opcję New Scope....

Uruchomiony kreator poprosił o nazwę nowego zakresu – wprowadzono:

- Nazwa zakresu: Zakres_Firma

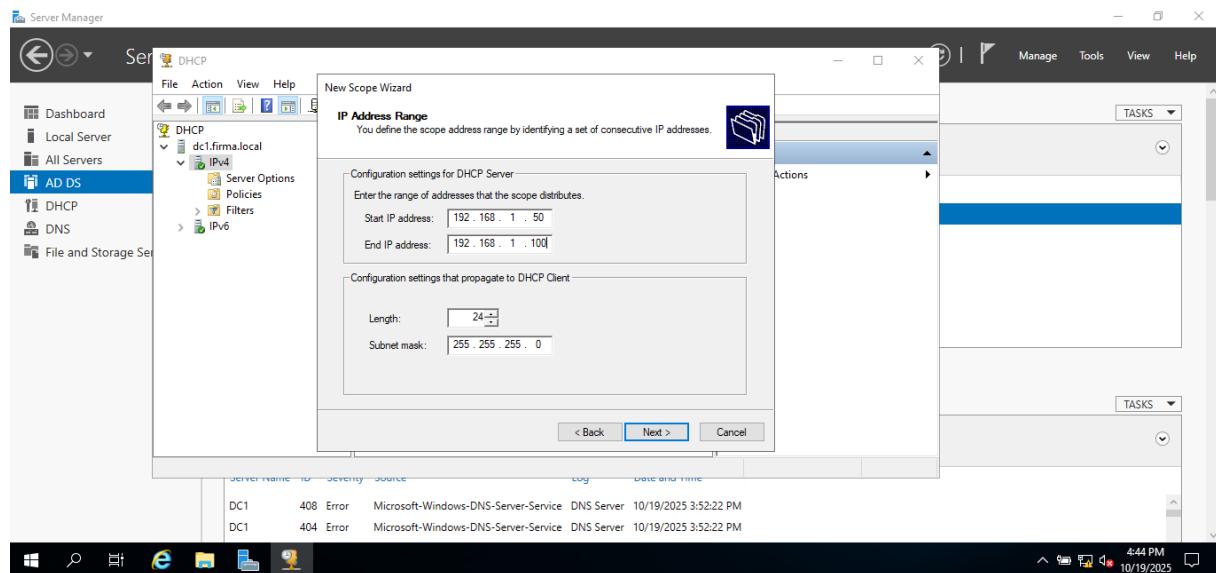


Rysunek 49 Tworzenie nowego zakresu adresów IP

6.5. Definicja zakresu adresów IP

W kolejnym oknie określono przedział adresów, jakie DHCP ma przydzielać klientom:

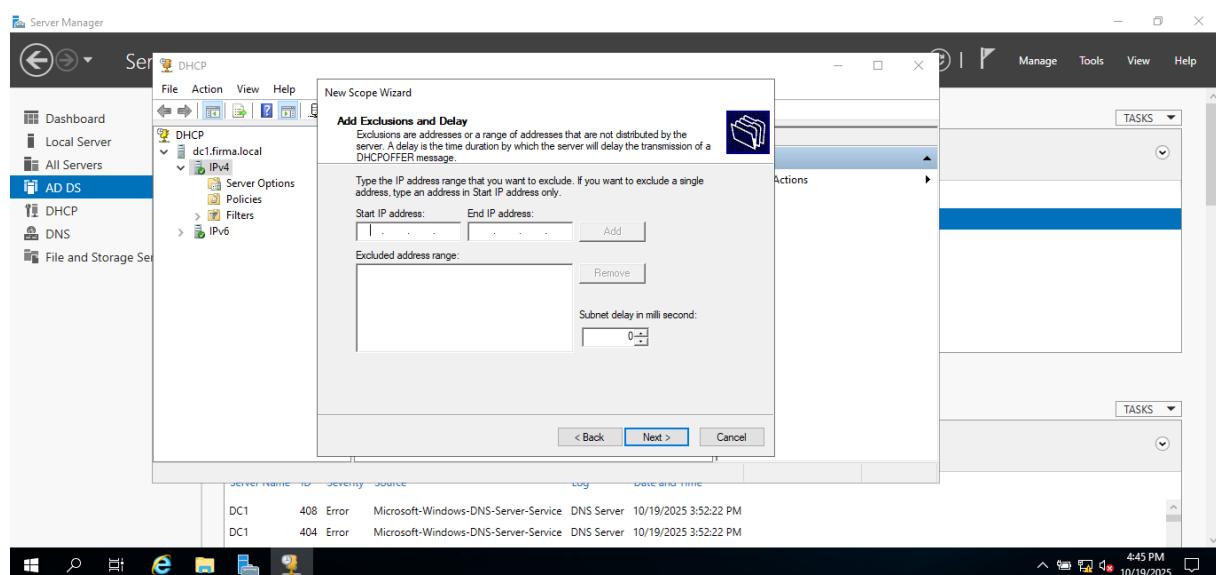
- Początek zakresu: 192.168.1.50
- Koniec zakresu: 192.168.1.100
- Maska podsieci: 255.255.255.0



Rysunek 50 Ustawienia zakresu adresów IP w kreatorze

6.6. Wykluczenia i opóźnienia

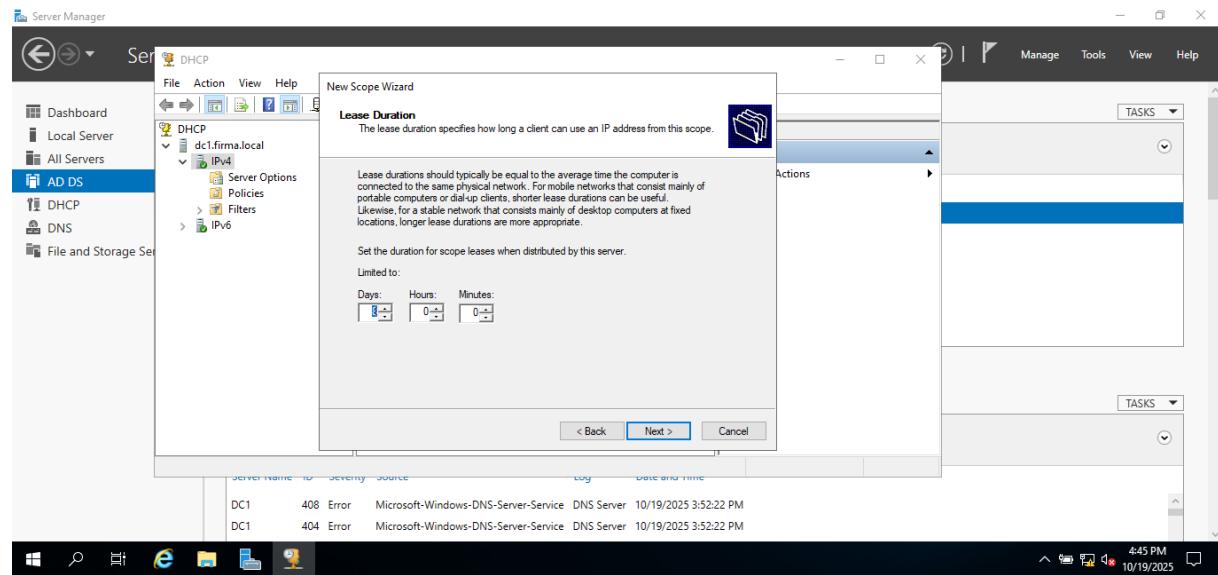
Nie wprowadzono żadnych wykluczeń ani opóźnień. Serwer będzie mógł przydzielać dowolny adres z określonego zakresu.



Rysunek 51 Pominięcie konfiguracji wykluczeń

6.7.Czas dzierżawy adresu IP

Czas dzierżawy (lease duration) ustawiono na 8 dni, co oznacza, że komputer kliencki może korzystać z przydzielonego adresu przez 8 dni, zanim konieczne będzie odnowienie dzierżawy.

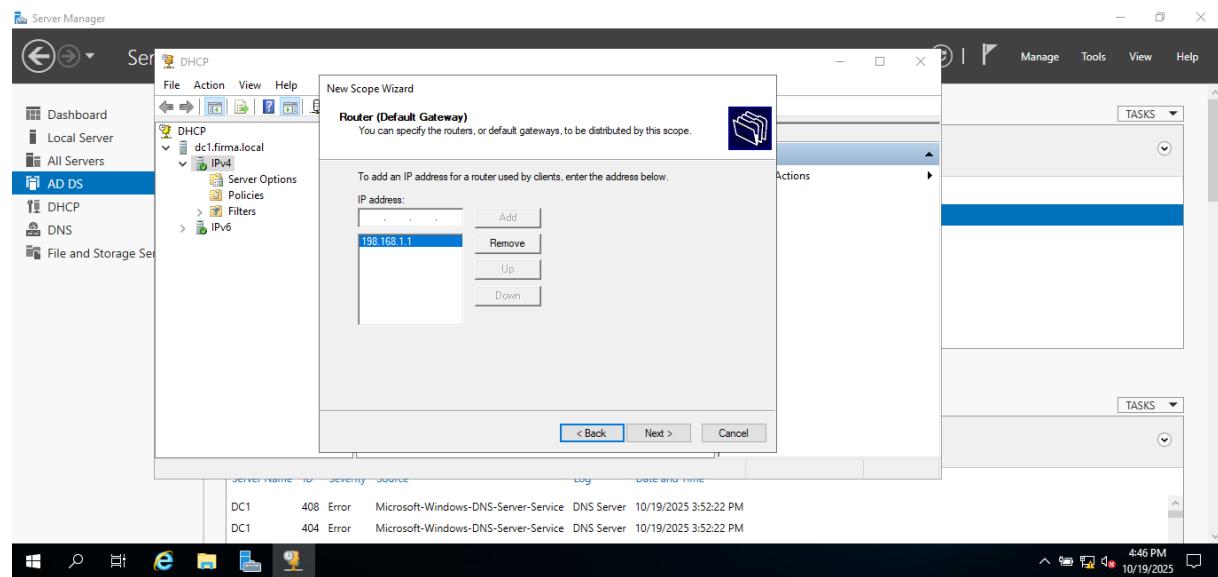


Rysunek 52 Określenie długości dzierżawy adresu IP

6.8.Ustawienie bramy domyślnej

W sekcji Router (Default Gateway) podano adres routera w sieci lokalnej:

- 192.168.1.1

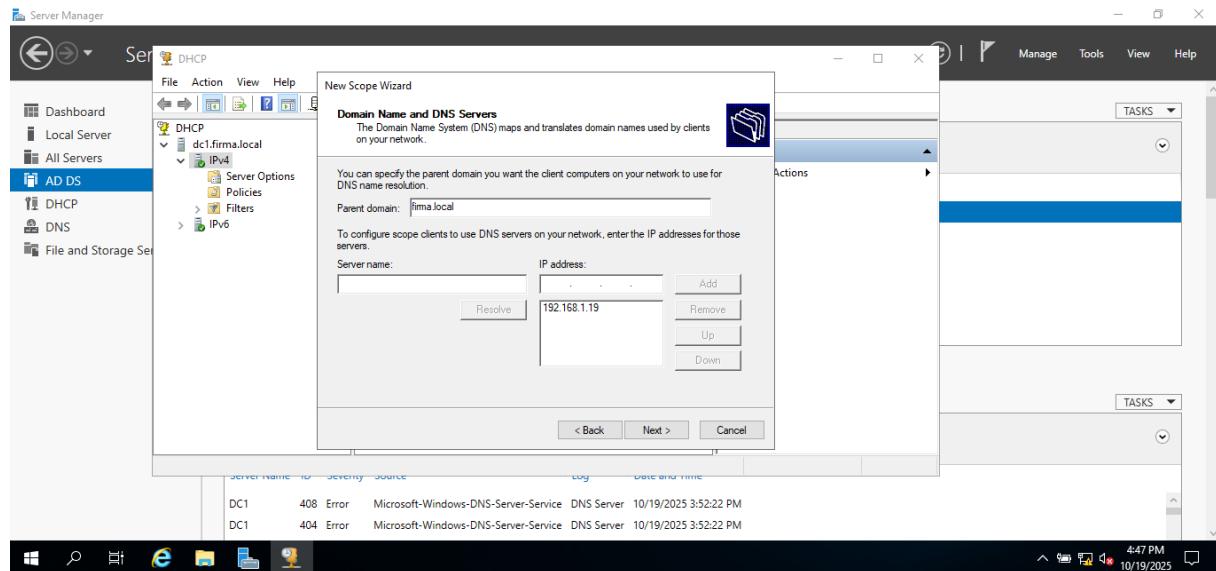


Rysunek 53 Wprowadzenie adresu bramy domyślnej

6.9. Konfiguracja DNS i domeny

Wprowadzono dane domeny oraz adres serwera DNS (czyli kontrolera domeny DC1):

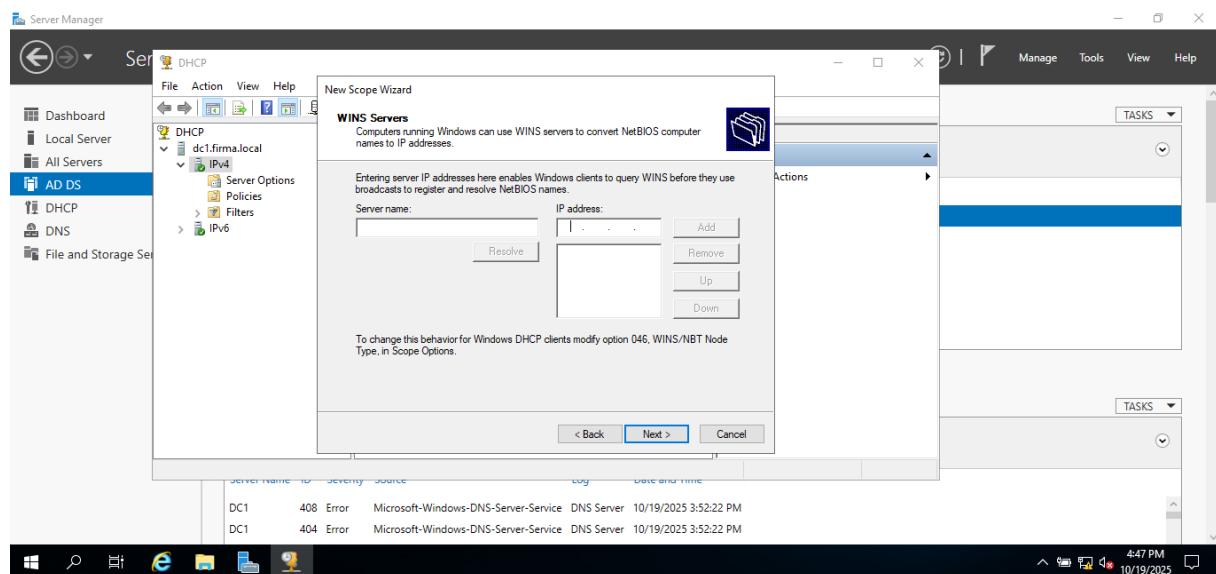
- Nazwa domeny: firma.local
- Adres DNS: 192.168.1.19



Rysunek 54 Ustawienia serwera DNS i nazwy domeny

6.10. Pominiecie konfiguracji WINS

Kreator zaproponował konfigurację serwera WINS — została pominięta, ponieważ ta funkcja nie jest używana w nowoczesnych środowiskach domenowych.



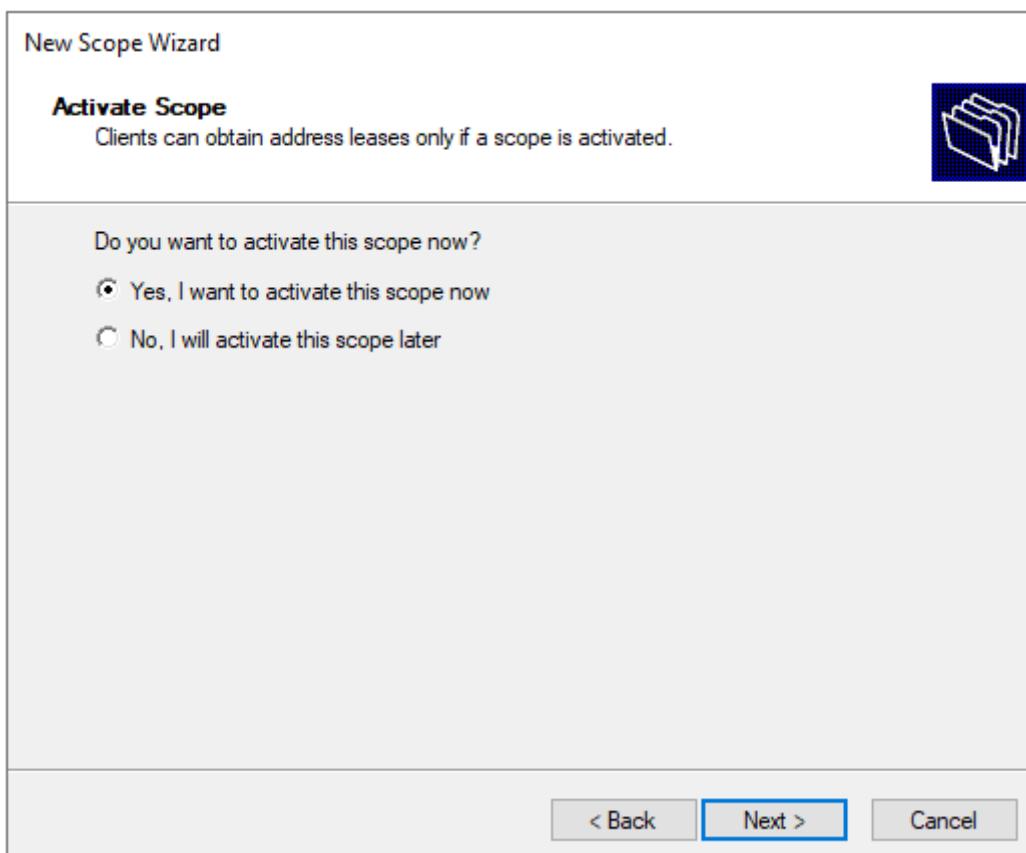
Rysunek 55 Pominiecie konfiguracji WINS

6.11. Aktywacja nowego zakresu

W ostatnim kroku kreatora zaznaczono opcję:

- Yes, I want to activate this scope now,

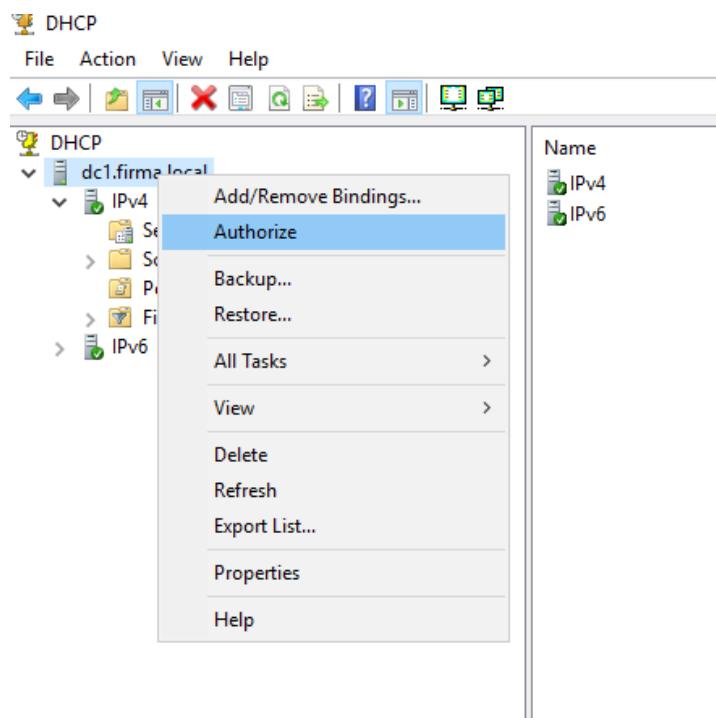
a następnie kliknięto Finish, co aktywowało zakres Zakres_Firma.



Rysunek 56 Aktywacja utworzonego zakresu DHCP

6.12. Autoryzacja serwera DHCP

Po zakończeniu konfiguracji kliknięto prawym przyciskiem myszy nazwę serwera dc1.firma.local i wybrano Authorize. Po chwili serwer został autoryzowany w domenie, co potwierdzała zielona ikona statusu.



Rysunek 57 Autoryzacja serwera DHCP w domenie

6.13. Test działania usługi DHCP

Na komputerze klienckim KLIENT01 otwarto wiersz poleceń i wykonano komendy:

- ipconfig /release
- ipconfig /renew

Klient otrzymał automatycznie adres IP z puli 192.168.1.50–100, z bramą 192.168.1.1 i DNS-em 192.168.1.19. W konsoli DHCP (zakładka Address Leases) pojawił się nowy wpis z nazwą KLIENT01 i przydzielonym adresem IP.

Ważne jest aby zaznaczyć opcje:

- Uzyskaj adres IP automatycznie
oraz Uzyskaj adres serwera DNS automatycznie

do prawidłowego działania.

```
ca Wiersz polecenia
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\jan.kowalski>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ab82:c721:b738:e601%14
Default Gateway . . . . . :

C:\Users\jan.kowalski>ipconfig /renew

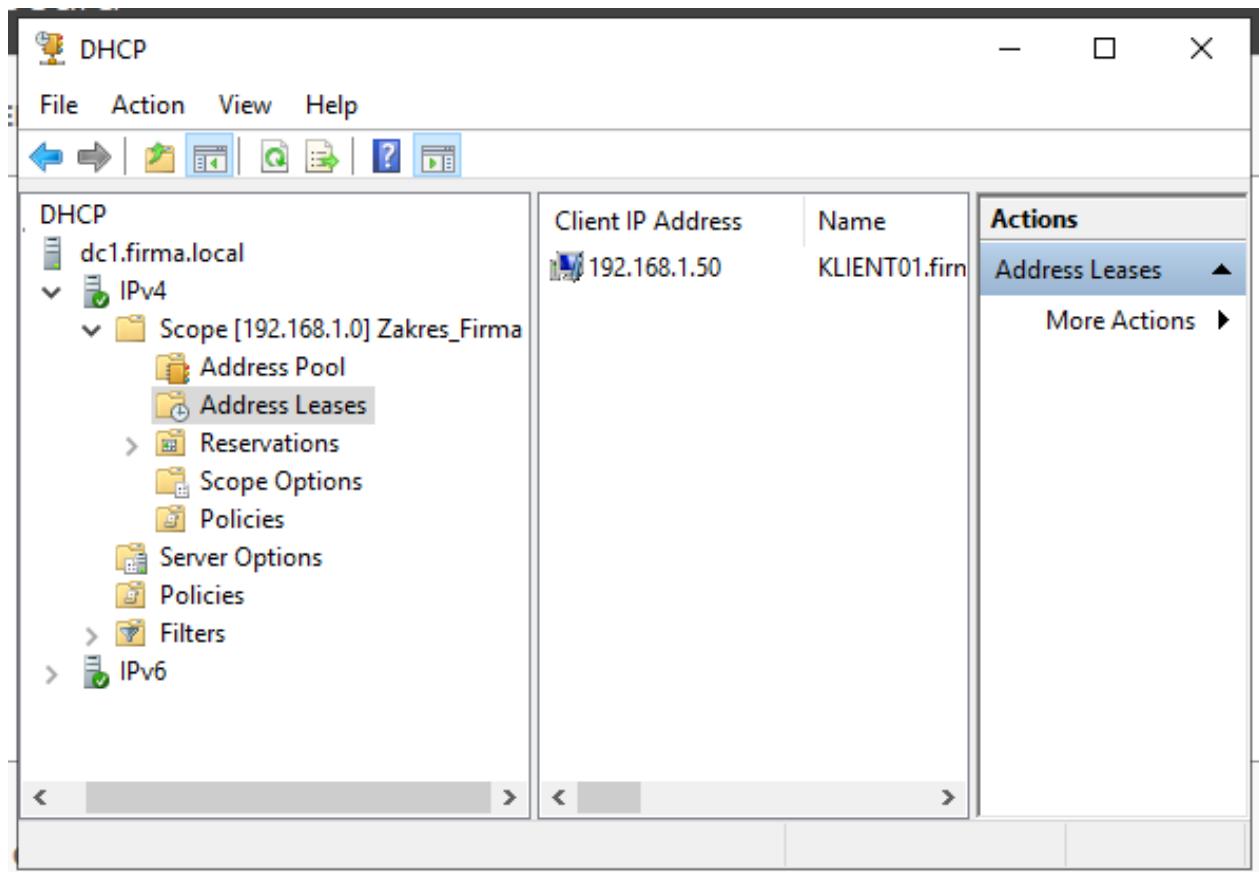
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : firma.local
Link-local IPv6 Address . . . . . : fe80::ab82:c721:b738:e601%14
IPv4 Address. . . . . : 192.168.1.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 198.168.1.1

C:\Users\jan.kowalski>
```

Rysunek 58 Wynik działania usługi DHCP – przydzielony adres IP



Rysunek 59 Wpis klienta w dzierżawach adresów (Address Leases)

6.14. Weryfikacja poprawności działania

Na serwerze DC1 widoczny był aktywny zakres Zakres_Firma, a klienci w domenie automatycznie pobierali adresy IP. Dzięki temu infrastruktura sieciowa domeny firma.local działa w pełni automatycznie.

6.15. Wnioski z etapu 6

W wyniku konfiguracji serwera DHCP:

- Serwer DC1 pełni teraz rolę kontrolera domeny, serwera DNS oraz serwera DHCP.
- Klienci sieci firmowej automatycznie otrzymują poprawne adresy IP, maskę, bramę i adres DNS.
- Zmniejszono ryzyko błędów konfiguracji adresacji IP.
- System firma.local jest w pełni funkcjonalny i gotowy do wdrażania polityk grupowych (GPO).

7. Wdrażanie zasad grupowych (GPO)

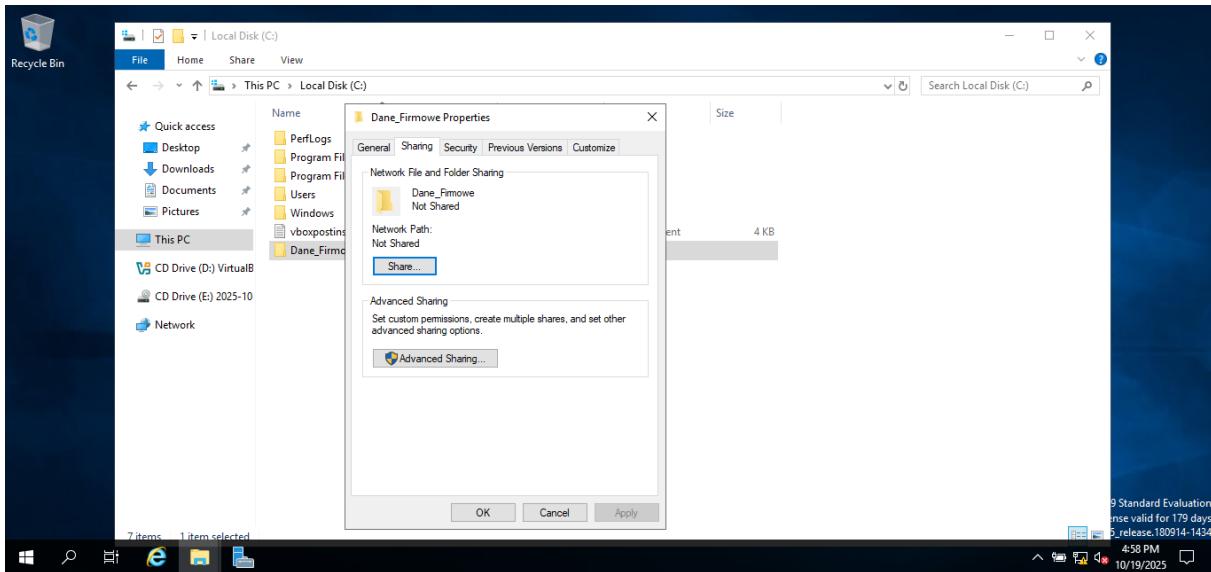
Po skonfigurowaniu domeny firma.local, usług DNS i DHCP, kolejnym krokiem było wdrożenie zasad grupowych (Group Policy Objects – GPO). Zasady GPO umożliwiają centralne zarządzanie ustawieniami użytkowników i komputerów w sieci domenowej. Dzięki nim administrator może np. automatycznie mapować dyski sieciowe, blokować dostęp do panelu sterowania, wymuszać politykę haseł lub udostępniać wspólne foldery dla działów firmy.

7.1.Utworzenie folderu współdzielonego „Dane_Firmowe”

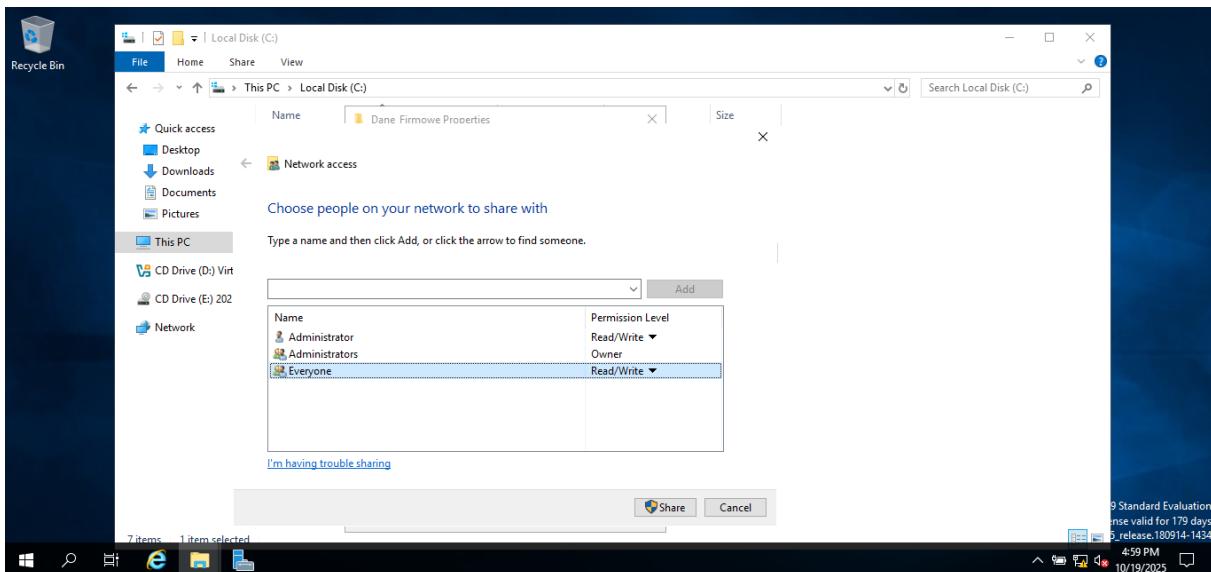
Na serwerze DC1 utworzono folder, który będzie pełnił funkcję wspólnego zasobu dla użytkowników domeny.

- W lokalizacji C:\ utworzono folder Dane_Firmowe.
- Kliknięto prawym przyciskiem myszy na folder → Properties → zakładka Sharing.
- Wybrano przycisk Share... i dodano grupę Everyone, ustawiając poziom uprawnień na Read/Write.

Dzięki temu folder będzie widoczny i dostępny w sieci dla wszystkich użytkowników.



Rysunek 60 Udostępnienie folderu Dane_Firmowe w sieci



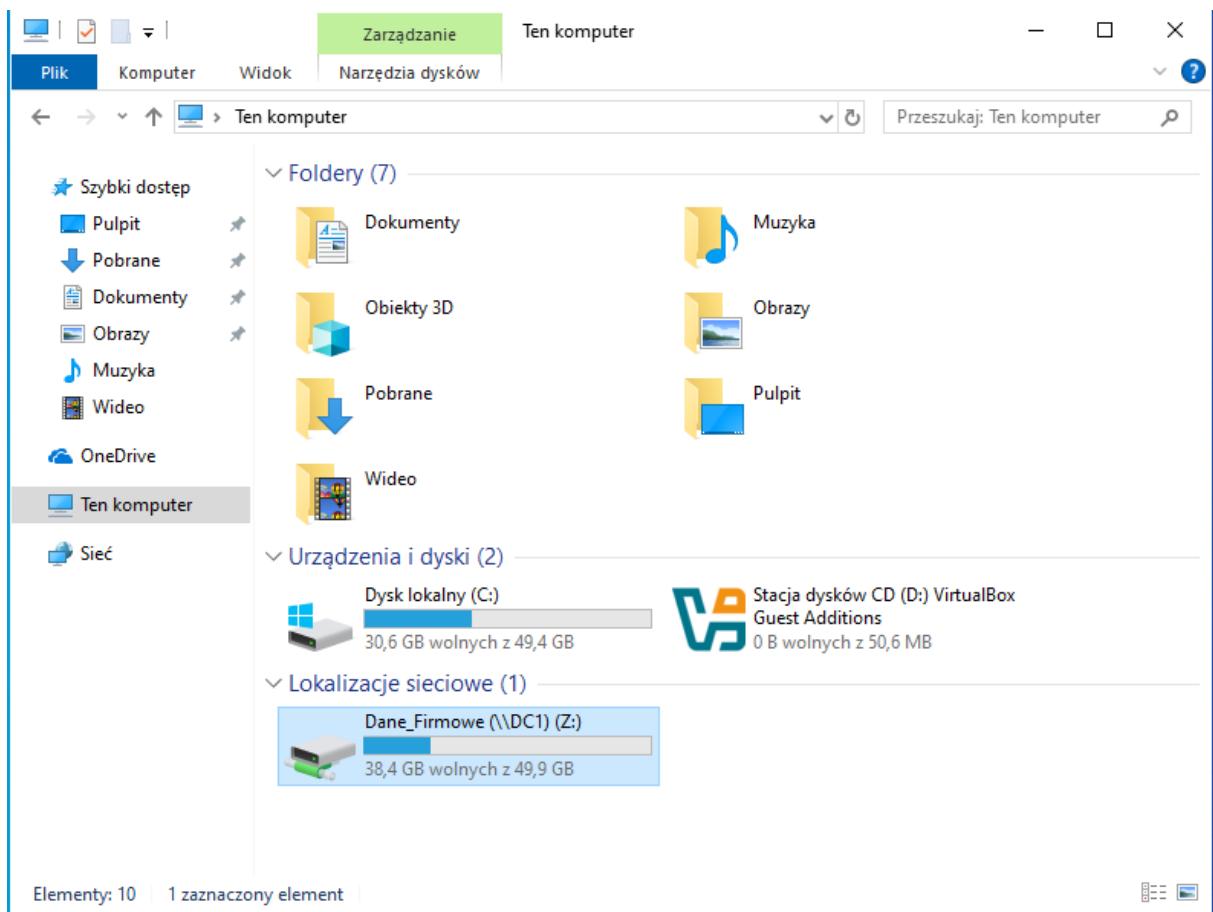
Rysunek 61 Nadanie uprawnień Read/Write dla grupy Everyone

7.2. Sprawdzenie widoczności folderu w sieci

Po udostępnieniu folderu sprawdzono jego dostępność z komputera klienckiego KLIENT01. W eksploratorze plików wpisano ścieżkę:

- \\DC1\\Dane_Firmowe

Folder otworzył się poprawnie, co potwierdziło prawidłowe działanie udostępnienia w sieci. Następnie zamapowano go ręcznie jako dysk sieciowy Z:, co ułatwia użytkownikom dostęp do wspólnych danych.

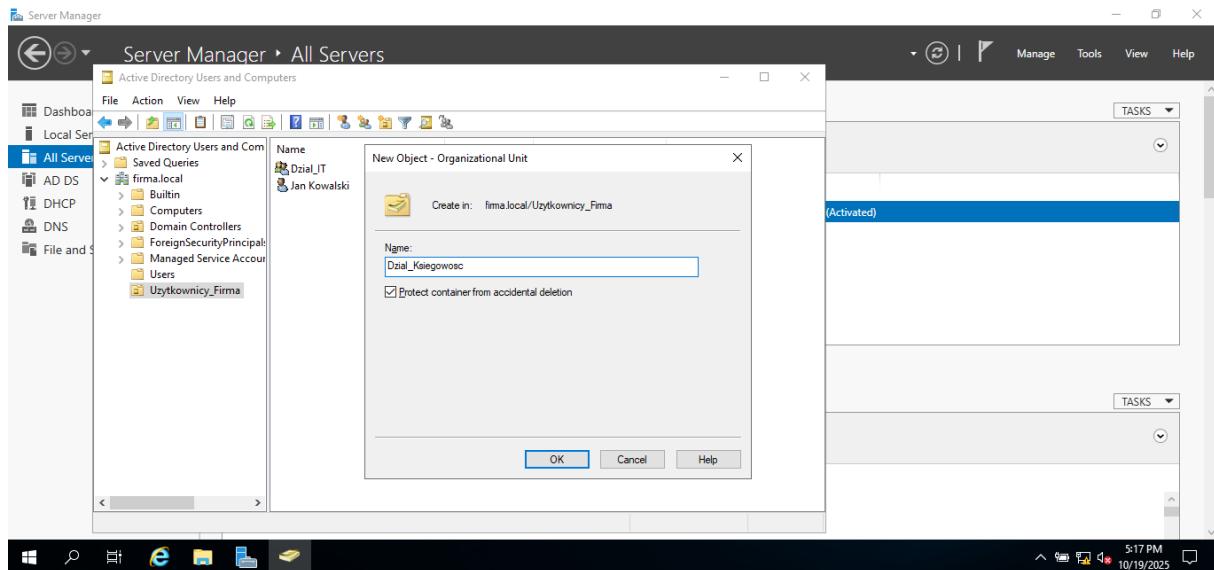


Rysunek 62 Widoczny folder sieciowy Dane_Firmowe jako dysk Z

7.3. Tworzenie jednostek organizacyjnych (OU)

W konsoli Active Directory Users and Computers (ADUC) utworzono strukturę jednostek organizacyjnych (Organizational Units – OU), aby uporządkować użytkowników i przypisywać im różne polityki grupowe.

- W drzewie domeny firma.local utworzono jednostkę nadziedną Użytkownicy_Firma.
- W niej dodano podjednostki:
 - Dział_IT
 - Dział_Księgowość
 - Dział_Sprzedaż
- Każdy dział będzie miał przypisaną własną politykę GPO.

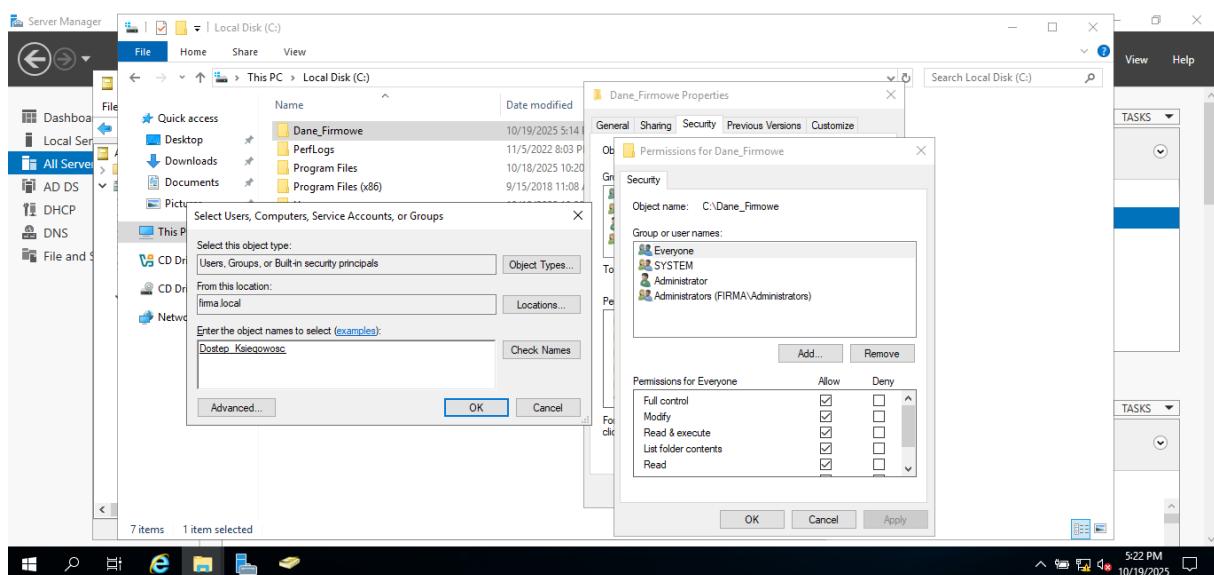


Rysunek 63 Tworzenie jednostki organizacyjnej Dział_Księgowość w ADUC

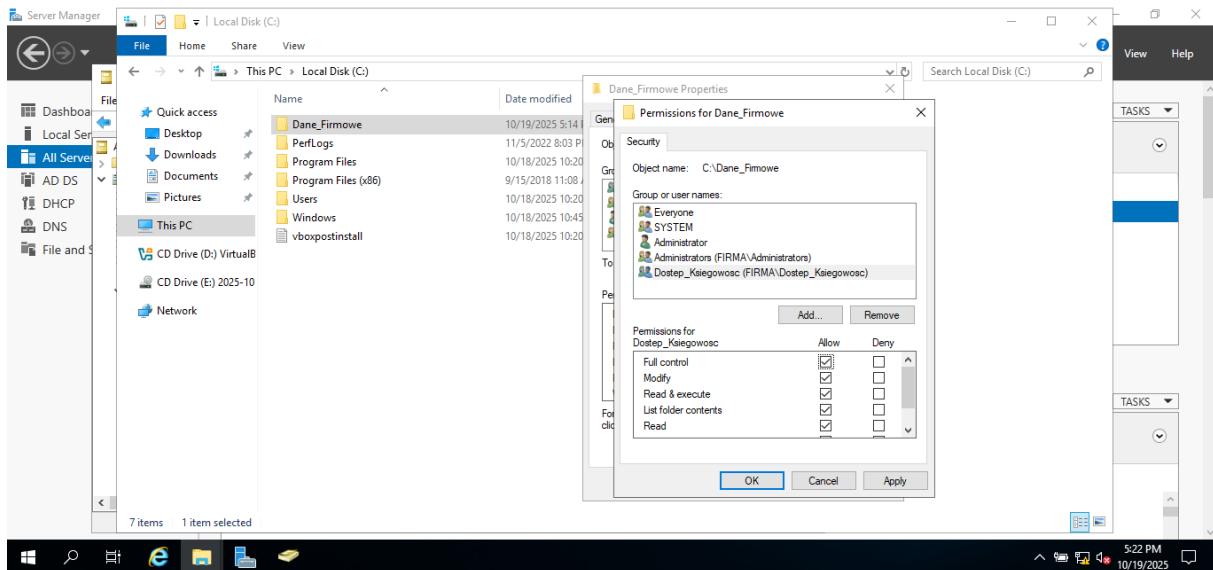
7.4.Utworzenie grupy zabezpieczeń i nadanie uprawnień

W celu kontrolowania dostępu do folderu firmowego utworzono grupę zabezpieczeń Dostęp_Ksiegowosc i przypisano jej pełne uprawnienia do folderu.

- W jednostce Dział_Księgowość kliknięto prawym przyciskiem myszy → New → Group.
- Nadano nazwę: Dostęp_Ksiegowosc, typ: Security, zakres: Global.
- W folderze C:\Dane_Firmowe otwarto zakładkę Security → Edit → Add.
- Wpisano nazwę grupy Dostęp_Ksiegowosc i zatwierdzono.
- Przyznano jej pełne prawa (Full Control).



Rysunek 64 Dodanie grupy Dostęp_Ksiegowosc do listy uprawnień folderu



Rysunek 65 Nadanie pełnych uprawnień dostępu grupie księgowości

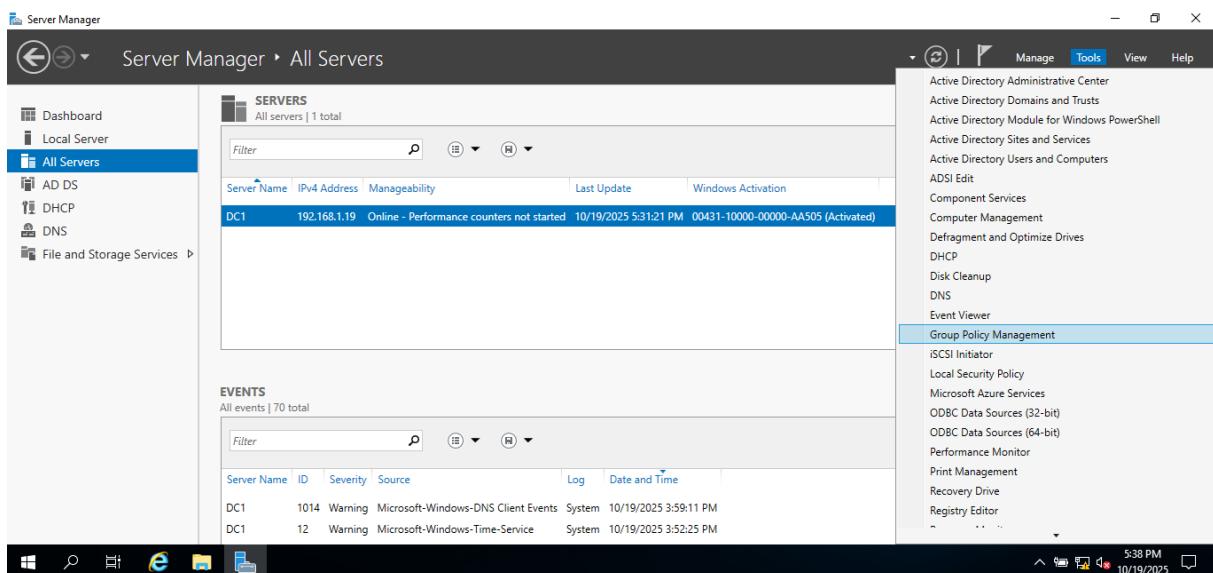
7.5. Weryfikacja dostępu

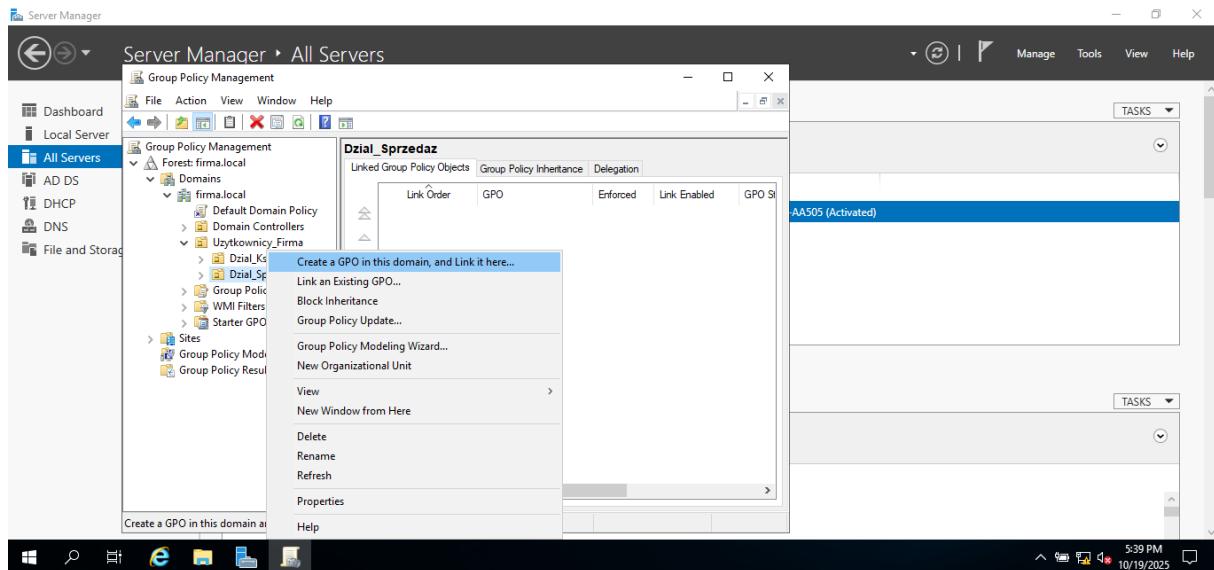
Członkowie grupy Dostęp_Księgowość po zalogowaniu do domeny uzyskują pełen dostęp do folderu Dane_Firmowe. Dzięki integracji z domeną i Active Directory uprawnienia są nadawane centralnie, bez potrzeby indywidualnej konfiguracji każdego komputera.

7.6.Uruchomienie konsoli Group Policy Management

Aby zautomatyzować mapowanie dysku sieciowego, uruchomiono narzędzie Group Policy Management (GPMC):

- W Server Manager → Tools wybrano Group Policy Management.
 - W drzewie domeny rozwinięto gałąź firma.local → Użytkownicy_Firma → Dział_Sprzedaż.
 - Kliknięto prawym przyciskiem myszy → Create a GPO in this domain, and Link it here...





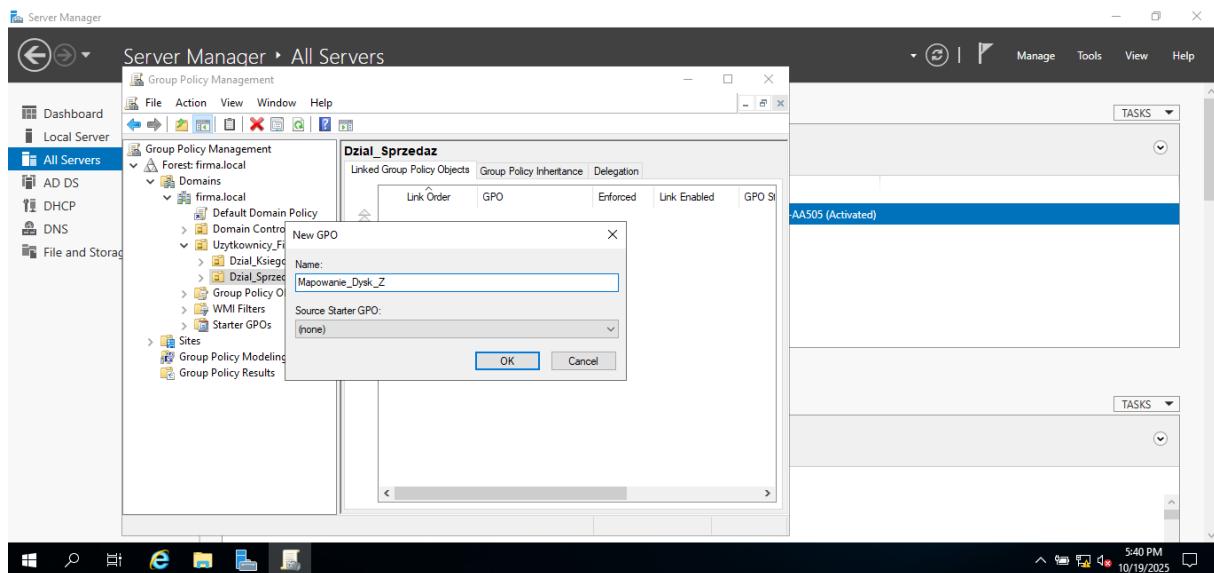
Rysunek 66 Utworzenie nowego obiektu zasad GPO w domenie

7.7. Tworzenie obiektu zasad GPO

W wyświetlonym oknie nadano nazwę dla nowego obiektu:

- Mapowanie_Dysk_Z

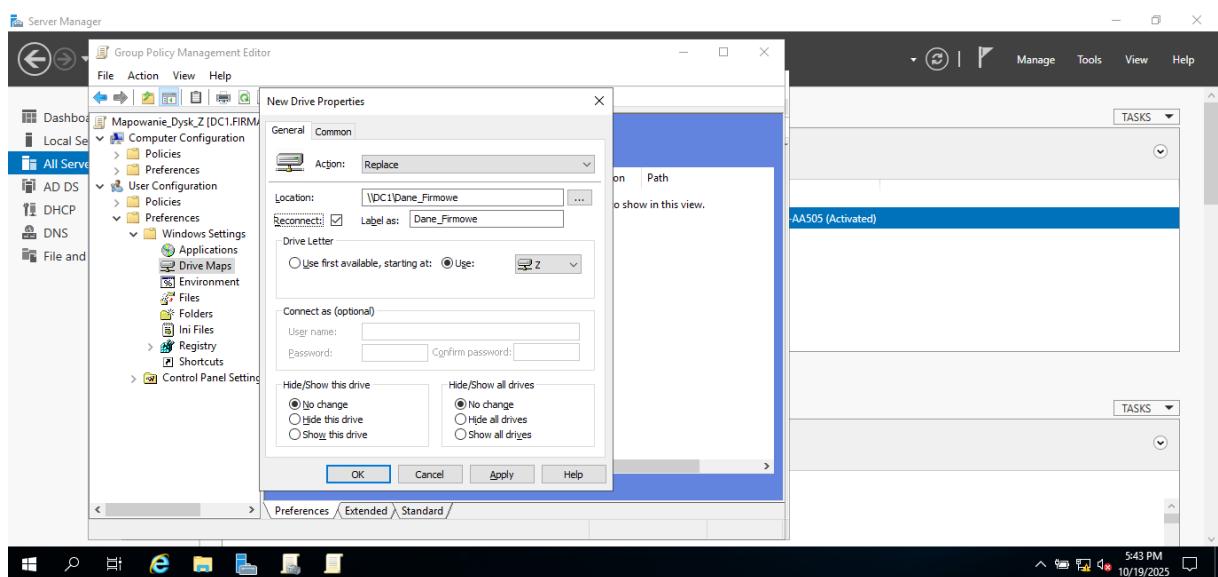
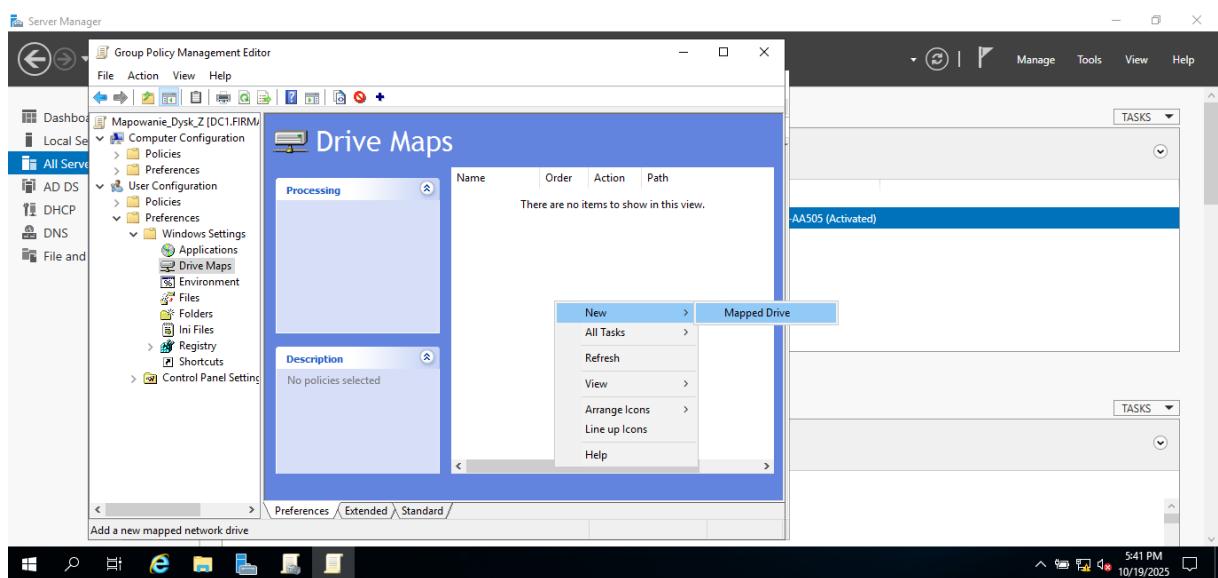
Nazwa odzwierciedla funkcję polityki — automatyczne mapowanie dysku sieciowego Z: dla użytkowników działu sprzedaży.



Rysunek 67 Tworzenie obiektu zasad Mapowanie_Dysk_Z

7.8. Edycja zasad GPO – konfiguracja mapowania dysku sieciowego

- Kliknięto prawym przyciskiem myszy na utworzony obiekt Mapowanie_Dysk_Z i wybrano Edit.
- W edytorze wybrano: User Configuration → Preferences → Windows Settings → Drive Maps.
- Kliknięto New → Mapped Drive i wprowadzono następujące dane:
 - Location: \\DC1\Dane_Firmowe
 - Drive Letter: Z:
 - Reconnect: zaznaczone (dysk łączy się automatycznie przy logowaniu)
 - Label as: Dane Firmowe
- Zapisano ustawienia i zamknięto edytor.



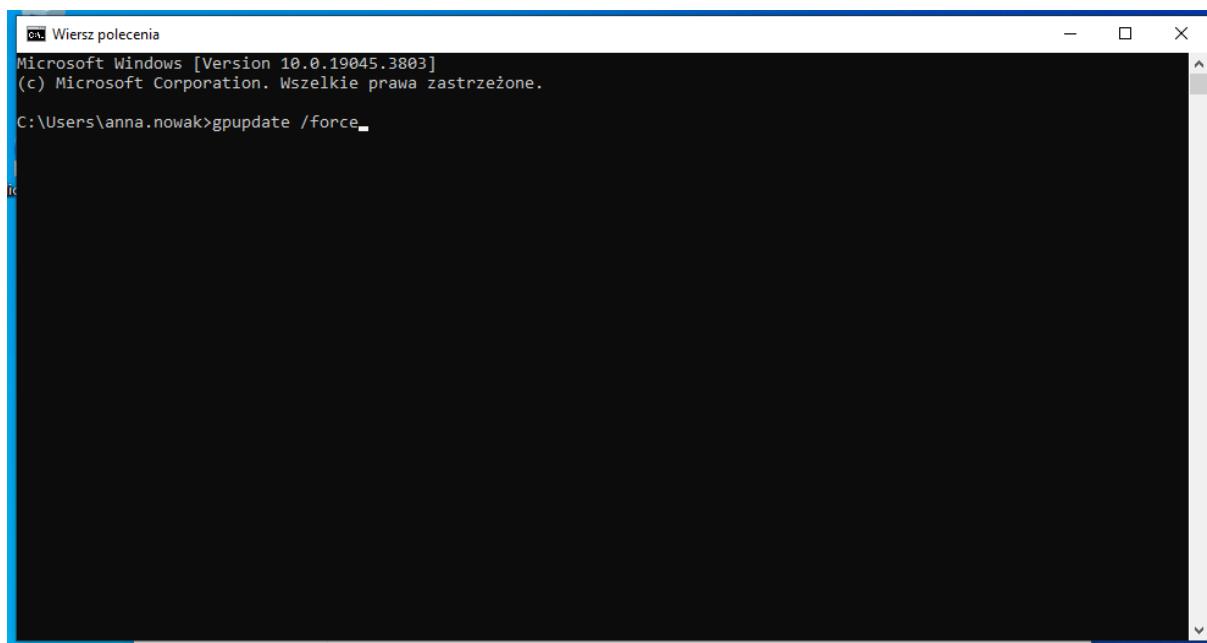
Rysunek 68 Konfiguracja mapowania dysku sieciowego Z w GPO

7.9.Zastosowanie zasad na komputerze klienckim

Na komputerze Klient01, należącym do domeny, zalogowano się na konto użytkownika przypisanego do działu sprzedaży. W wierszu poleceń wykonano aktualizację zasad:

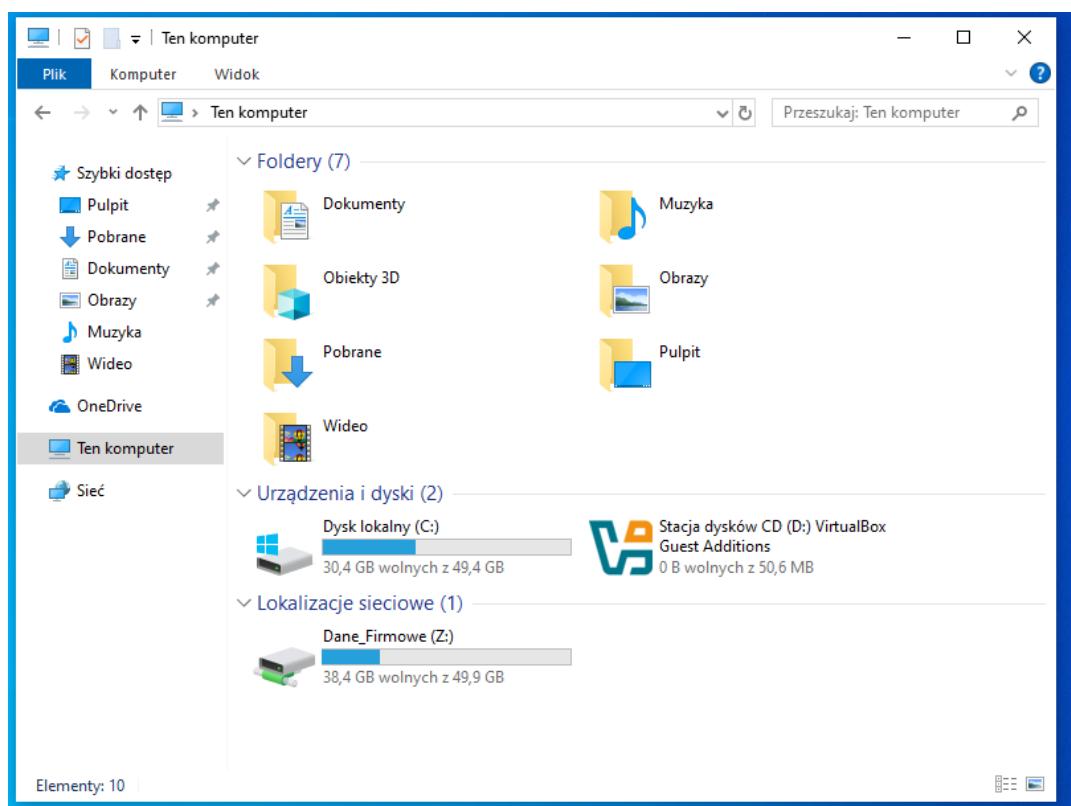
- gpupdate /force

Po ponownym zalogowaniu dysk sieciowy Z: został automatycznie podłączony do folderu \DC1\Dane_Firmowe.



```
C:\ Wiersz polecenia
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

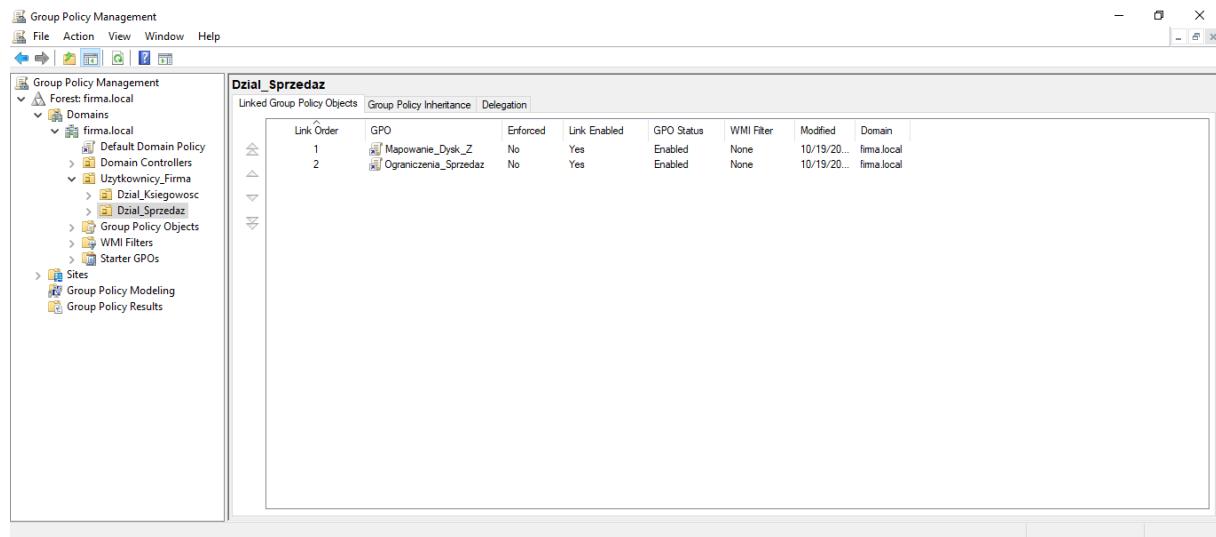
C:\Users\anna.nowak>gpupdate /force
```



Rysunek 69 Widoczny zamapowany dysk sieciowy Z na komputerze klienckim

7.10. Weryfikacja w konsoli GPMC

W konsoli Group Policy Management sprawdzono przypisanie obiektu GPO do jednostki Dział_Sprzedaz. Polityka była aktywna i poprawnie powiązana, co potwierdzało skuteczne zastosowanie zasad w domenie.



Rysunek 70 Widok aktywnego obiektu GPO w konsoli

7.11. Wnioski z etapu 7

W wyniku wdrożenia zasad grupowych:

- Utworzono strukturę jednostek organizacyjnych i grup bezpieczeństwa dla działów firmy.
- Skonfigurowano automatyczne mapowanie dysku sieciowego Z dla użytkowników domeny.
- Zastosowano centralne zarządzanie dostępem i automatyzację konfiguracji użytkowników.
- Środowisko firma.local zostało przygotowane do dalszego wdrażania polityk bezpieczeństwa i personalizacji pracy użytkowników.

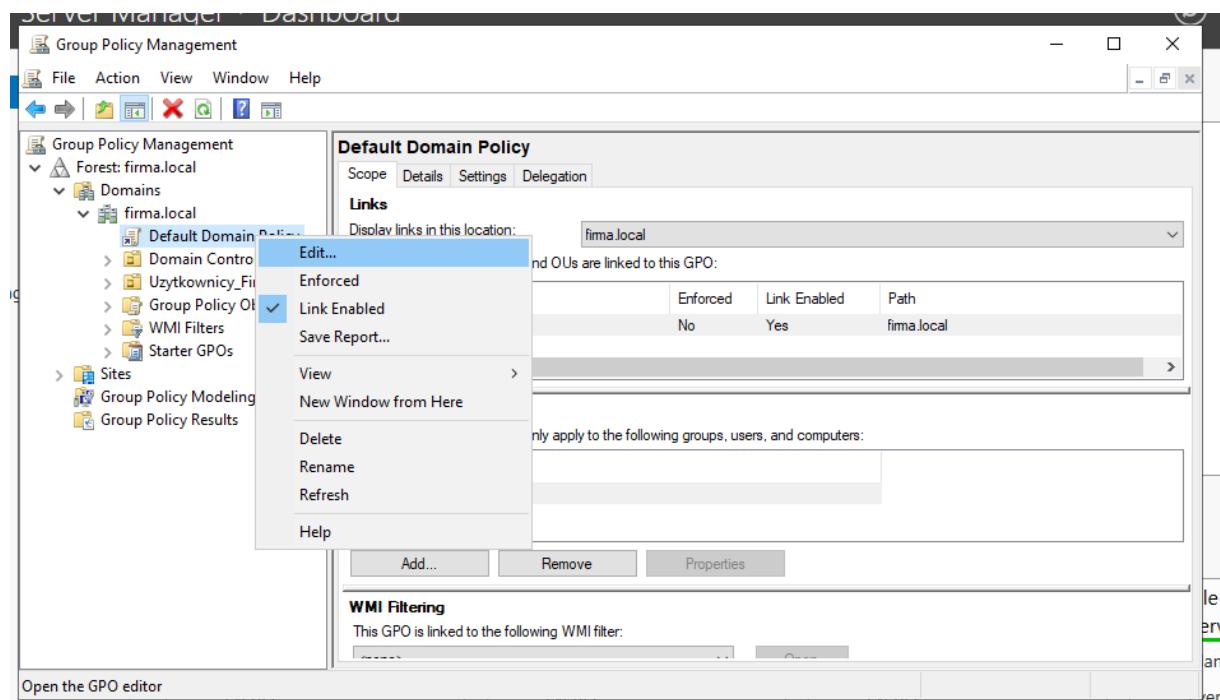
8. Wdrażanie zasad bezpieczeństwa w domenie (GPO Security Policies)

Po skonfigurowaniu automatycznego mapowania dysku sieciowego w domenie firma.local, przystąpiono do wdrażania zasad bezpieczeństwa (Group Policy Security Settings). Celem tego etapu było zwiększenie ochrony danych i ujednolicenie polityki zabezpieczeń dla wszystkich komputerów i użytkowników domeny. W ramach wdrożenia skonfigurowano m.in. politykę haseł, blokadę konta po błędnych logowaniach oraz ograniczenia dostępu do panelu sterowania i ustawień systemu.

8.1.Uruchomienie konsoli Group Policy Management

Aby rozpocząć konfigurację zasad bezpieczeństwa, otwarto konsolę Group Policy Management (GPMC):

- W Server Manager → Tools wybrano pozycję Group Policy Management.
- Rozwinięto drzewo domeny firma.local i kliknięto prawym przyciskiem myszy na pozycję Default Domain Policy.
- Wybrano opcję Edit, aby edytować globalną politykę bezpieczeństwa domeny.

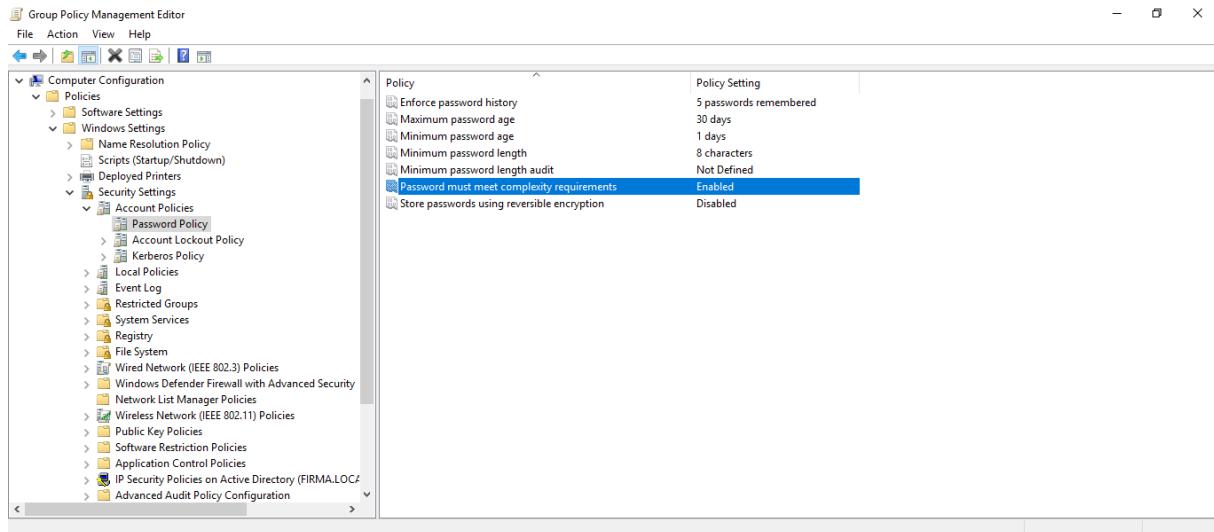


Rysunek 71 Uruchomienie konsoli Group Policy Management i edycja Default Domain Policy

8.2.Konfiguracja zasad dotyczących haseł użytkowników

W celu zwiększenia poziomu bezpieczeństwa kont domenowych, wprowadzono wymóg stosowania silnych haseł oraz ich okresowej zmiany.

- W edytorze zasad rozwinęto:
 - Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy
- Skonfigurowano następujące ustawienia:
 - Enforce password history: 5 poprzednich haseł
 - Maximum password age: 30 dni
 - Minimum password age: 1 dzień
 - Minimum password length: 8 znaków
 - Password must meet complexity requirements: Enabled (hasło musi zawierać duże litery, małe litery, cyfry i znaki specjalne)

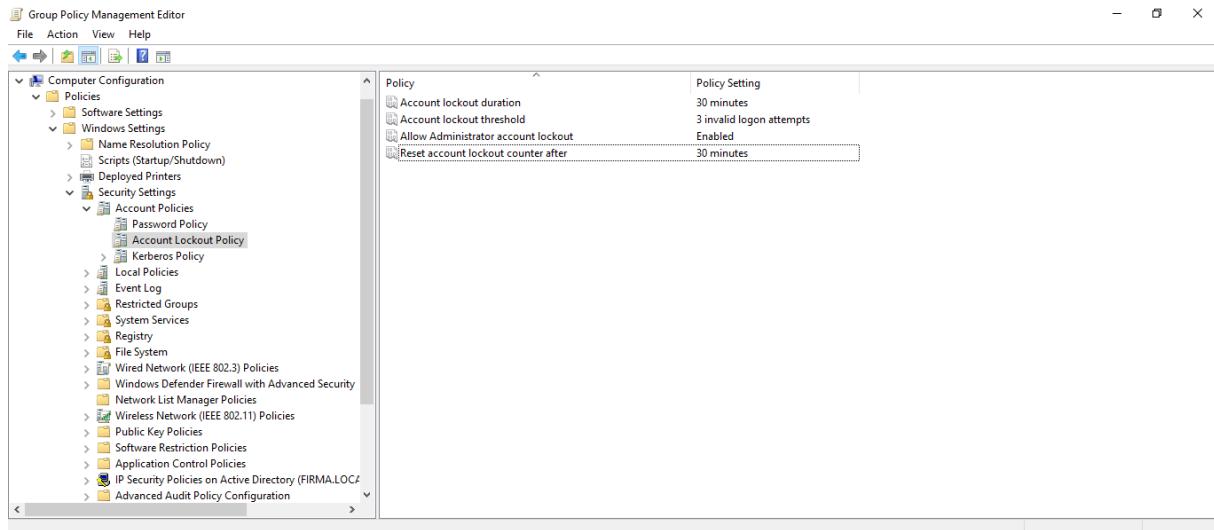


Rysunek 72 Konfiguracja polityki haseł użytkowników domeny

8.3. Blokada konta po błędnych próbach logowania

Wdrożono mechanizm blokady konta użytkownika po kilku nieudanych próbach logowania, co chroni przed próbami siłowego łamania haseł.

- W tym samym drzewie zasad otwarto:
 - Account Lockout Policy
- Skonfigurowano:
 - Account lockout threshold: 3 błędne próby logowania
 - Account lockout duration: 30 minut
 - Reset account lockout counter after: 30 minut

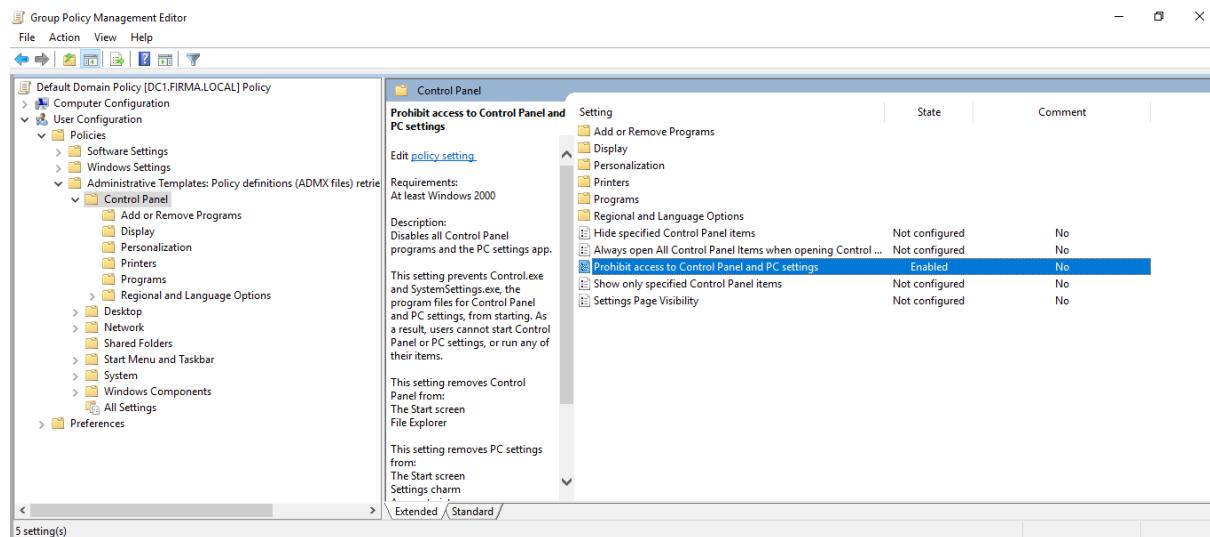


Rysunek 73 Ustawienia blokady konta użytkownika po błędnych logowaniach

8.4.Ograniczenie dostępu do Panelu sterowania i ustawień systemowych

Aby zapobiec nieautoryzowanym zmianom w konfiguracji systemu przez użytkowników, wdrożono politykę blokującą dostęp do Panelu sterowania i personalizacji pulpitu.

- W edytorze zasad przełączono do:
 - User Configuration → Policies → Administrative Templates → Control Panel
- Aktywowano opcję:
 - Prohibit access to Control Panel and PC settings: Enabled

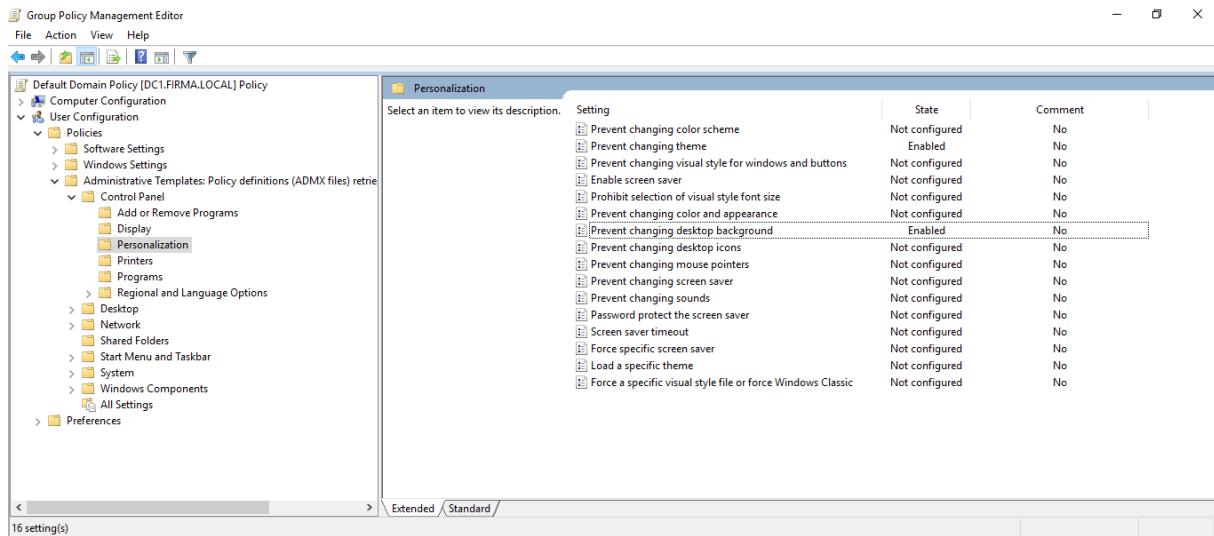


Rysunek 74 Włączenie blokady dostępu do Panelu sterowania

8.5.Blokada zmian wyglądu pulpitu i motywów

Aby zachować jednolity wygląd środowiska firmowego, włączono blokadę możliwości zmiany motywów i tła pulpitu przez użytkowników.

- W sekcji:
 - User Configuration → Policies → Administrative Templates → Control Panel → Personalization
- Aktywowano ustawienia:
 - Prevent changing desktop background: Enabled
 - Prevent changing theme: Enabled

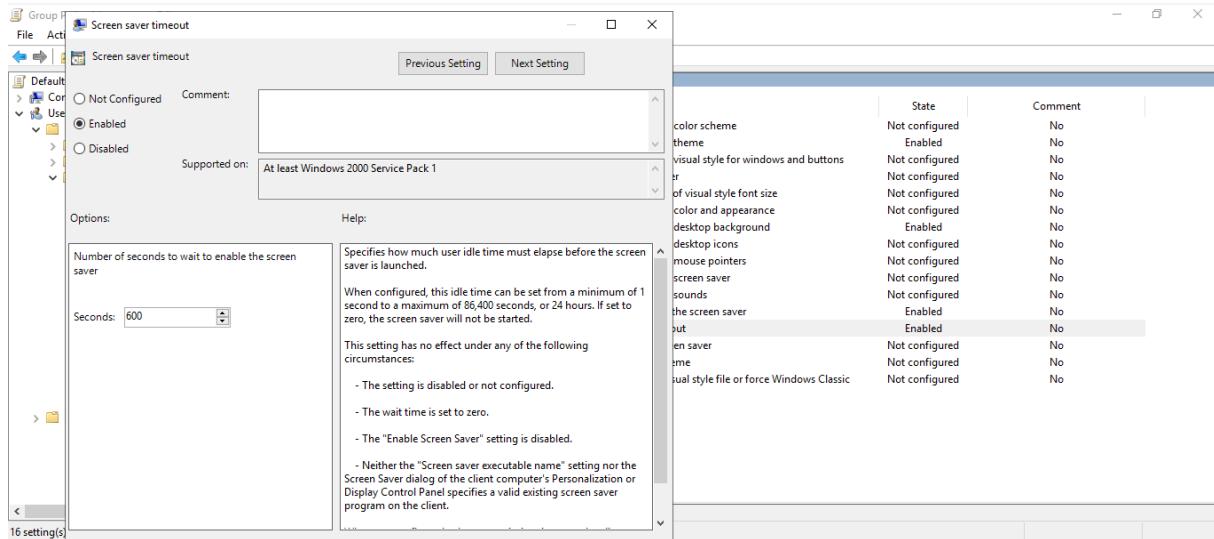


Rysunek 75 Blokada personalizacji pulpitu i motywów

8.6. Włączenie automatycznego blokowania ekranu po czasie bezczynności

W celu zwiększenia bezpieczeństwa danych firmowych skonfigurowano automatyczne blokowanie sesji użytkownika po 10 minutach nieaktywności.

- W edytorze zasad otwarto:
 - User Configuration → Policies → Administrative Templates → Control Panel → Personalization
- Aktywowano opcje:
 - Password protect the screen saver: Enabled
 - Screen saver timeout: 600 sekund (10 minut)



Rysunek 76 Włączenie automatycznego blokowania ekranu po czasie bezczynności

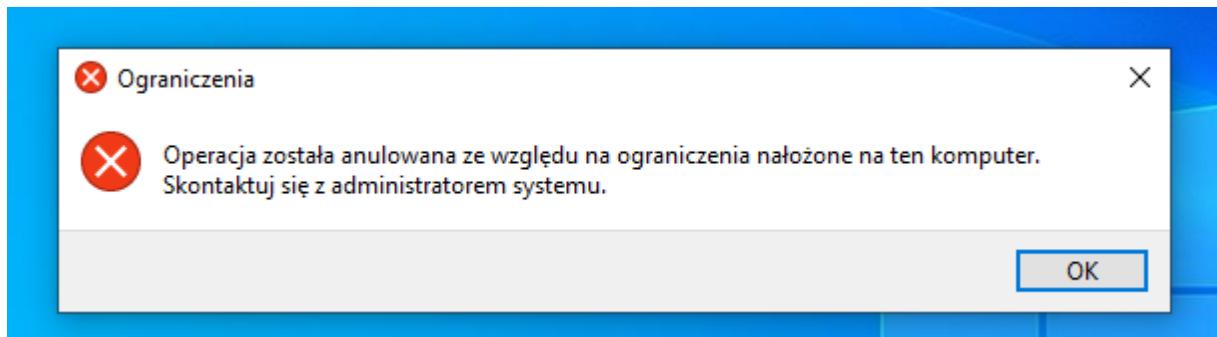
8.7. Aktualizacja zasad na komputerach klienckich

Po wprowadzeniu wszystkich zmian uruchomiono aktualizację zasad na komputerze klienckim Klient01 w celu ich natychmiastowego zastosowania.

W wierszu poleceń wpisano:

- gpupdate /force

Po ponownym zalogowaniu się użytkownika polityki bezpieczeństwa zaczęły obowiązywać — panel sterowania był zablokowany, a po 10 minutach bezczynności system automatycznie blokował ekran.



Rysunek 77 Aktualizacja zasad grupowych na komputerze klienckim

8.8. Wnioski z etapu 8

W wyniku wdrożenia zasad bezpieczeństwa:

- Zdefiniowano jednolitą politykę haseł wymuszającą stosowanie silnych zabezpieczeń.
- Włączono blokadę kont po błędnych próbach logowania, zwiększając odporność na ataki brute-force.
- Ograniczono dostęp użytkowników do panelu sterowania i personalizacji pulpitu, stabilizując środowisko pracy.
- Włączono automatyczne blokowanie ekranu po czasie bezczynności, co zabezpiecza dane w przypadku nieobecności użytkownika.
- Wszystkie zmiany zostały wdrożone centralnie przez GPO, bez potrzeby lokalnej konfiguracji komputerów.

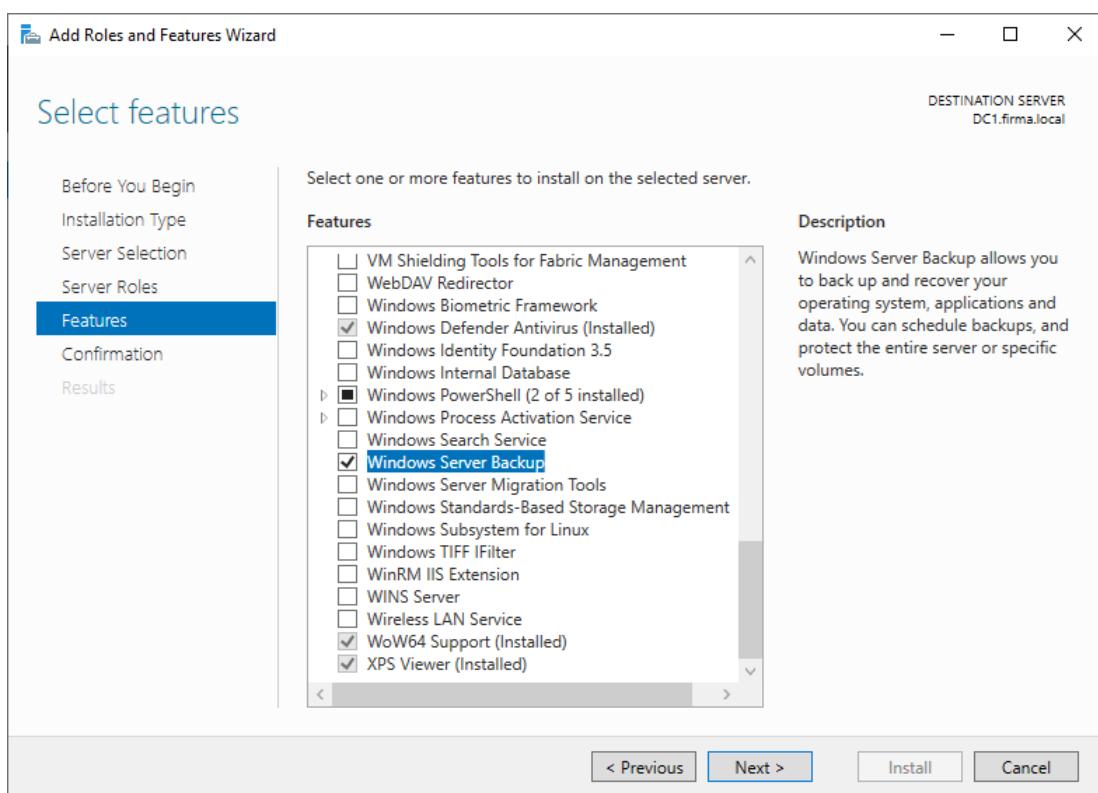
9. Kopia zapasowa i odzyskiwanie konfiguracji domeny (Backup & Restore Active Directory)

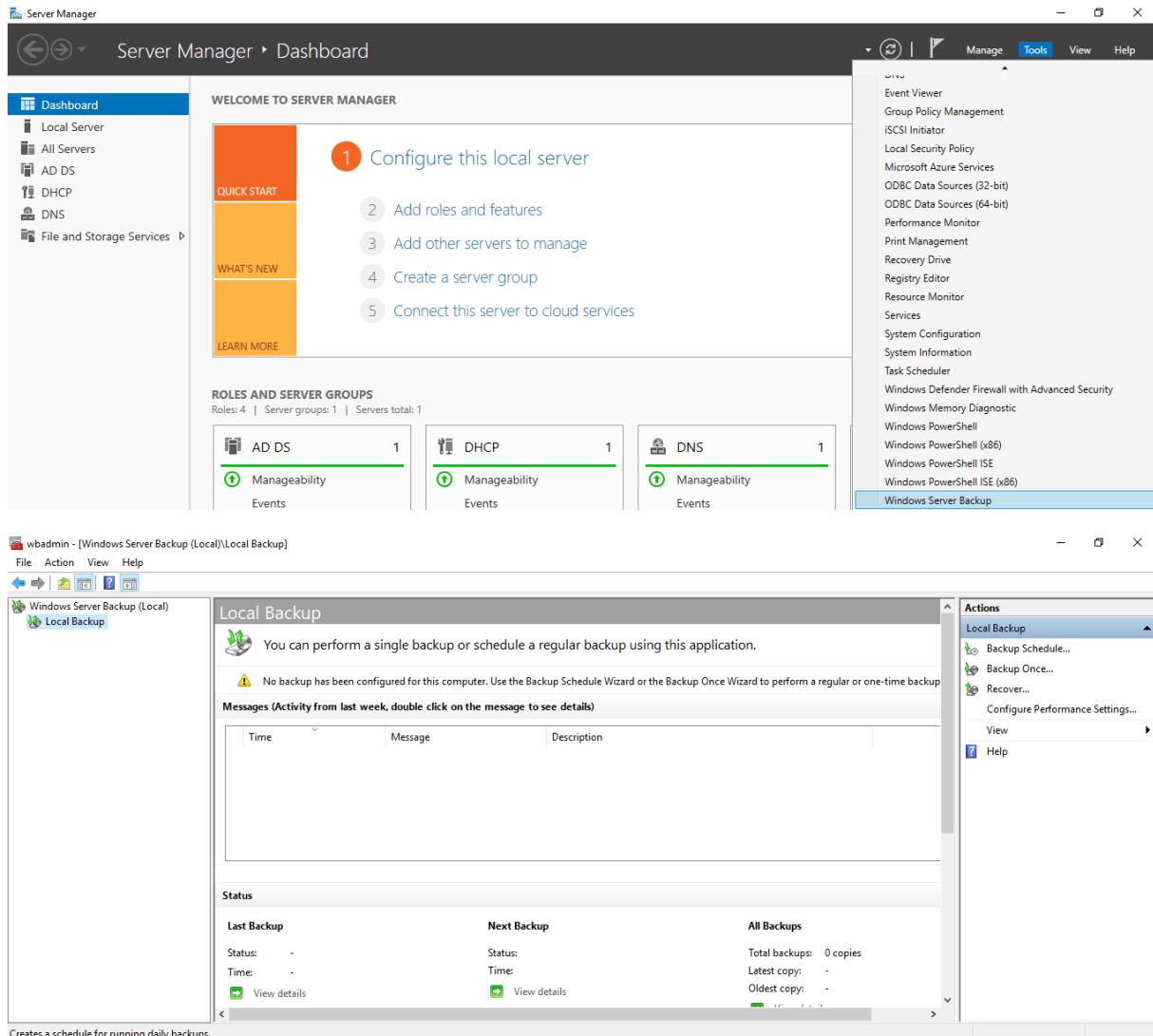
Po wdrożeniu usług domenowych, DHCP, DNS oraz zasad GPO, ostatnim etapem projektu była konfiguracja kopii zapasowej systemu domenowego. Backup jest kluczowym elementem utrzymania ciągłości działania infrastruktury IT — umożliwia szybkie odzyskanie danych po awarii, uszkodzeniu plików lub błędach administracyjnych. W tym etapie wykonano pełną kopię zapasową kontrolera domeny DC1, obejmującą: bazę Active Directory, DNS, GPO oraz rejestr systemu.

9.1.Uruchomienie narzędzia Windows Server Backup

W celu wykonania kopii zapasowej zainstalowano i uruchomiono narzędzie Windows Server Backup, dostępne w roli administracyjnej systemu Windows Server.

- W konsoli Server Manager → Tools wybrano opcję Windows Server Backup.
- Po uruchomieniu aplikacji kliknięto Local Backup, a następnie Backup Schedule..., aby utworzyć automatyczny harmonogram kopii zapasowych.





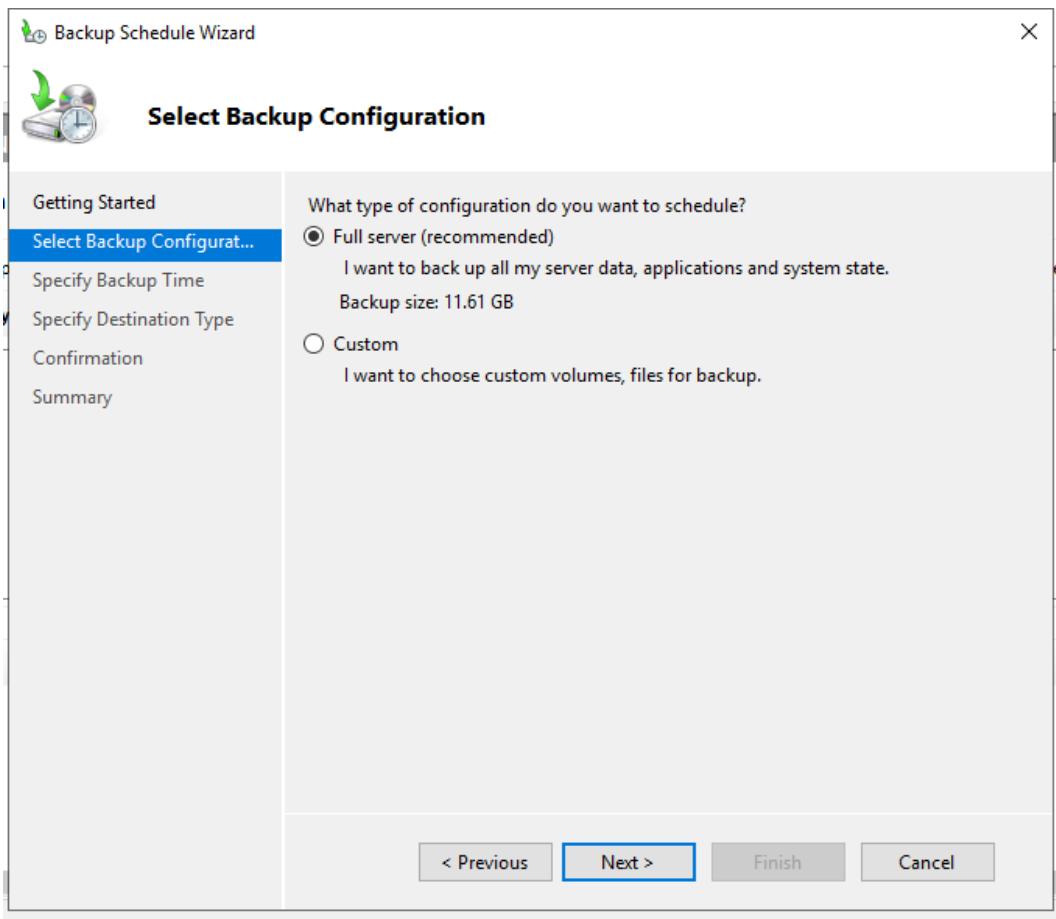
Rysunek 78 Uruchomienie konsoli Windows Server Backup

9.2. Wybór trybu tworzenia kopii zapasowej

W kreatorze wybrano opcję:

Full Server (zalecane) – obejmuje wszystkie dyski systemowe, usługi oraz dane konfiguracji domenowej.

Ten tryb gwarantuje pełną możliwość przywrócenia serwera DC1 do stanu sprzed awarii, włącznie z Active Directory i DNS.



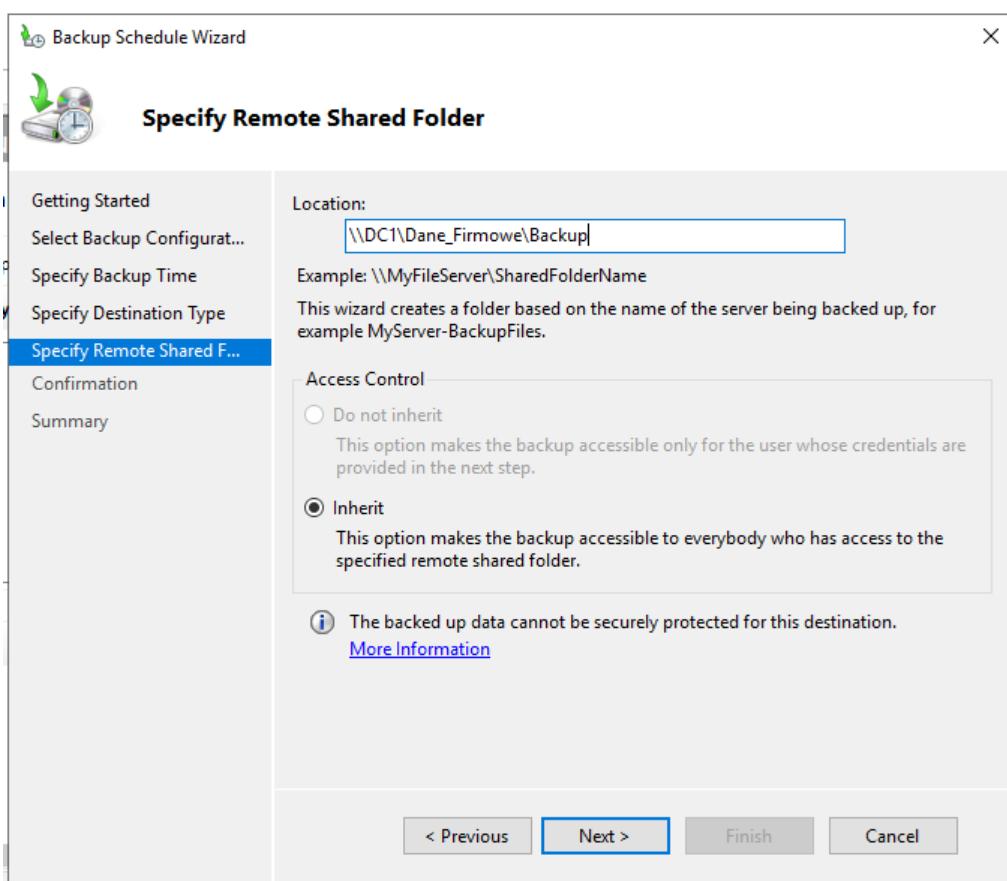
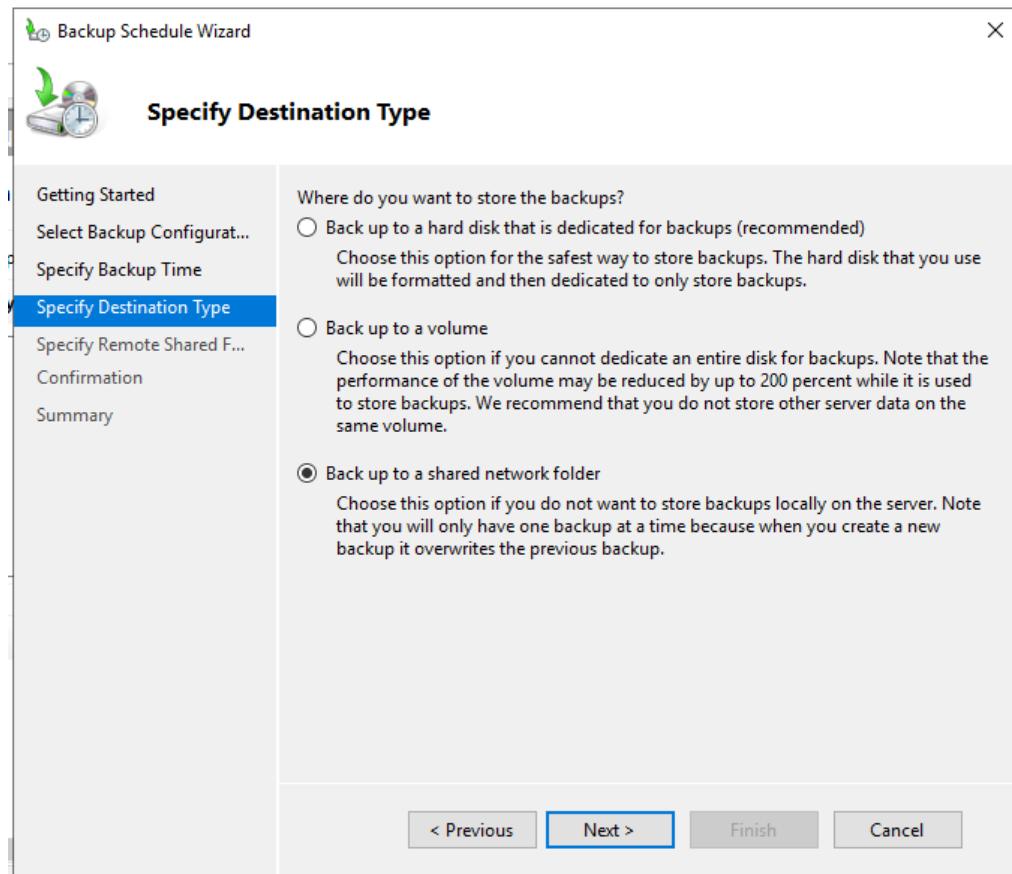
Rysunek 79 Wybór trybu tworzenia pełnej kopii zapasowej serwera

9.3. Wybór miejsca zapisu kopii zapasowej

Kopię zapasową zapisano na osobnym dysku sieciowym, co zabezpiecza dane przed utratą w przypadku awarii lokalnego dysku serwera.

Wybrano opcję:

- Backup to a shared network folder.
- Wprowadzono ścieżkę:
\\DC1\Dane_Firmowe\Backup
- Wskazano konto z uprawnieniami administratora domeny do zapisu w tej lokalizacji.



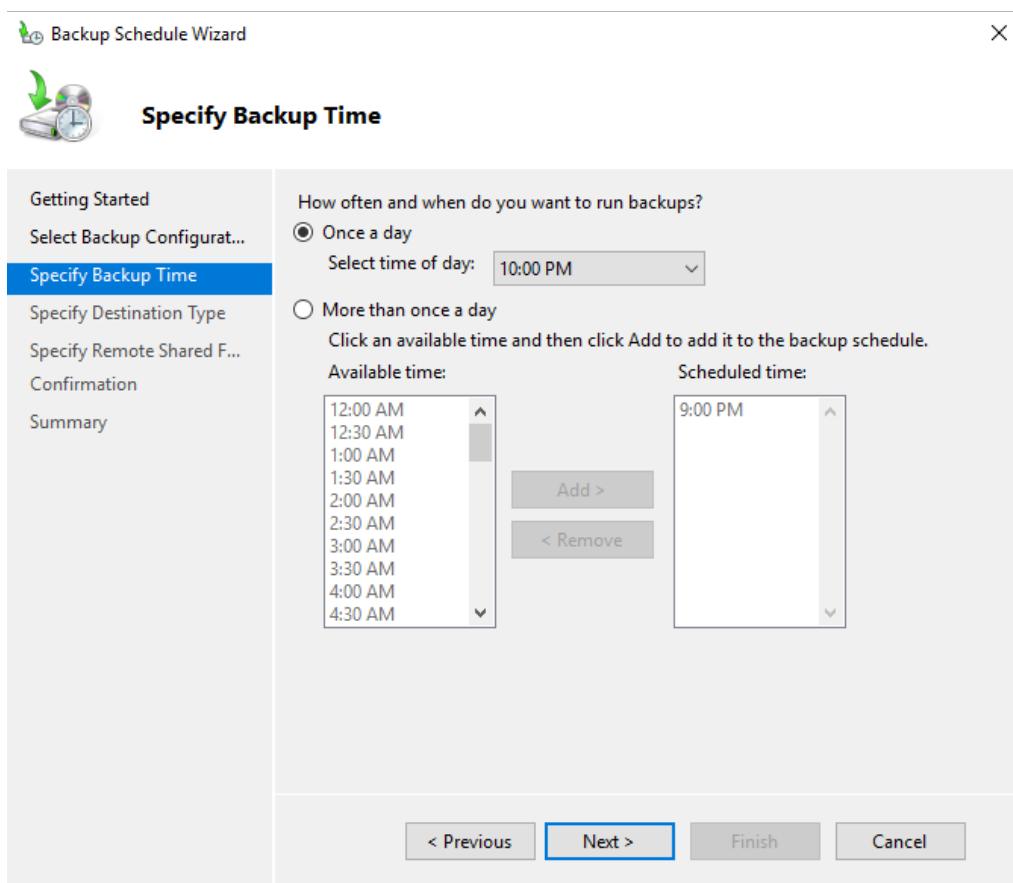
Rysunek 80 Wybór lokalizacji kopii zapasowej na udziale sieciowym

9.4.Ustawienie harmonogramu kopii zapasowej

W celu automatyzacji procesu kopii zapasowej ustawiono harmonogram wykonywania backupu:

- Częstotliwość: codziennie
- Godzina uruchomienia: 22:00
- Typ kopii: pełna (Full Backup)

Dzięki temu każdej nocy system automatycznie wykonuje aktualną kopię konfiguracji serwera DC1 i zapisuje ją w udziale sieciowym.

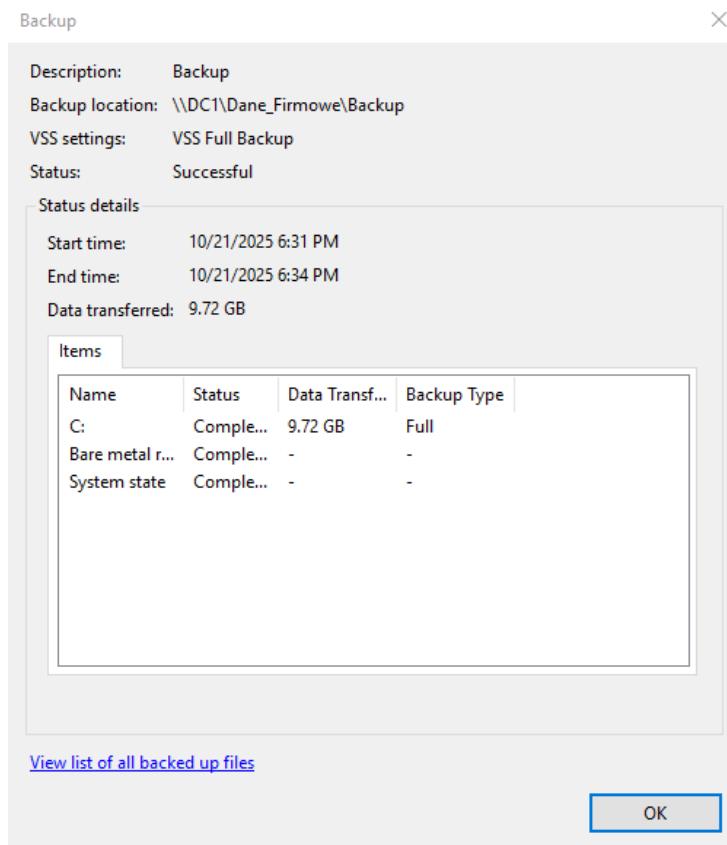


Rysunek 81 Ustawienie harmonogramu automatycznych kopii zapasowych

9.5.Zawartość kopii zapasowej

Po zakończeniu procesu w logach programu Windows Server Backup pojawił się raport potwierdzający pomyslnie wykonanie backupu. Kopia obejmowała:

- Pliki systemowe Windows Server 2019
- Bazy danych Active Directory Domain Services (NTDS.dit)
- Ustawienia DNS Server
- Polityki GPO (Group Policy Objects)
- Rejestr systemowy i pliki rozruchowe

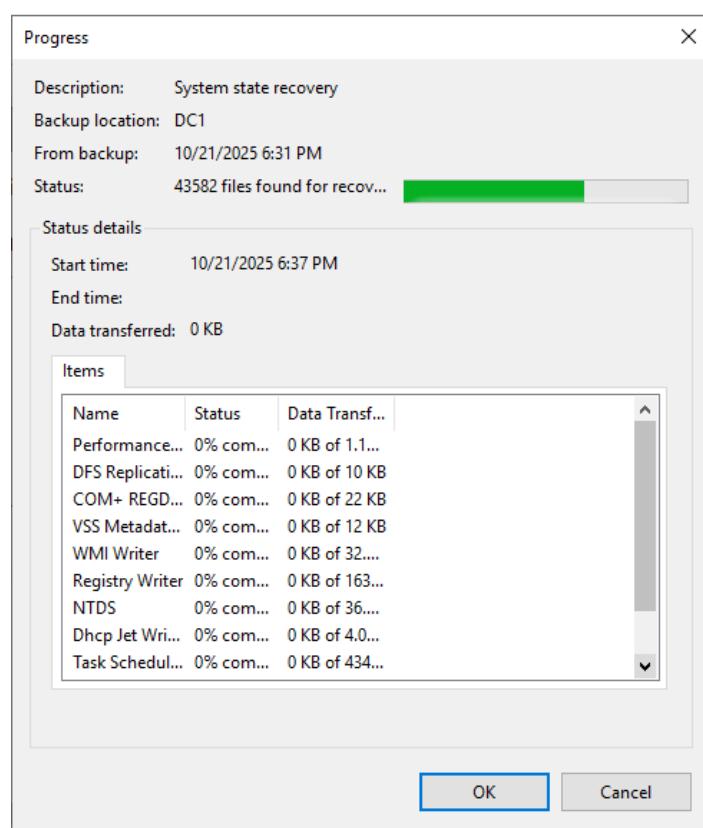
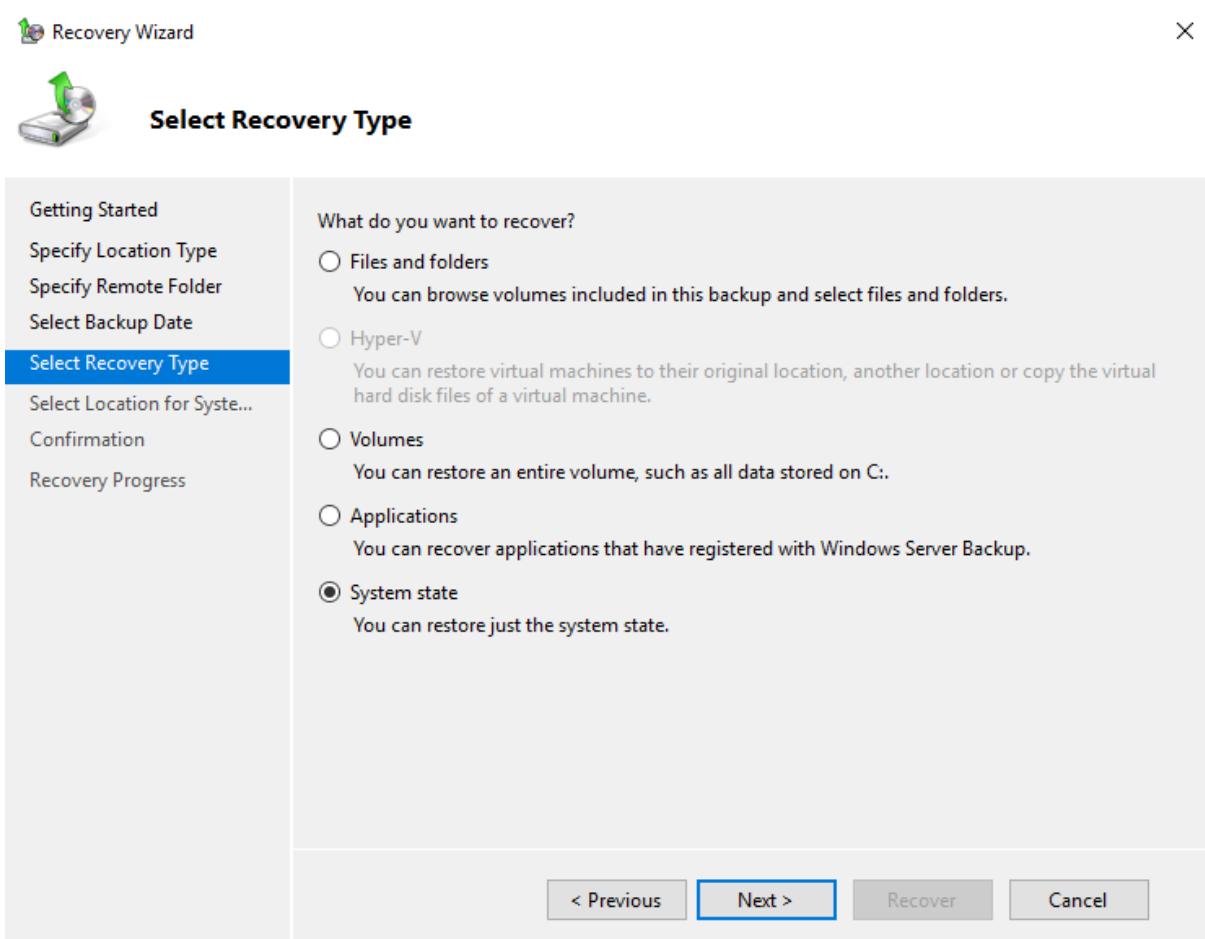


Rysunek 82 Raport wykonania kopii zapasowej systemu domenowego

9.6. Test przywracania danych (AD Restore Test)

Aby zweryfikować skuteczność kopii zapasowej, przeprowadzono testowe przywracanie elementów Active Directory w trybie awaryjnym.

- Uruchomiono serwer DC1 w trybie Directory Services Restore Mode (DSRM).
- W konsoli Windows Server Backup wybrano opcję Recover....
- Wskazano źródło kopii: folder \\DC1\盛行_Firmowe\Backup.
- Wybrano tryb przywracania:
 - System State Recovery – przywraca tylko kluczowe elementy systemu (AD DS, DNS, GPO).
- Po zakończeniu testu serwer został uruchomiony ponownie w trybie normalnym.



Rysunek 83 Okno przywracania stanu systemu w Windows Server Backup

9.7. Weryfikacja integralności usługi Active Directory

Po przywróceniu systemu sprawdzono poprawność działania domeny firma.local:

- Użytkownicy mogli logować się do domeny.
- Konsola Active Directory Users and Computers działała poprawnie.
- Polityki GPO i mapowanie dysków Z były aktywne.
- Serwer DNS rozwiązywał nazwy w sieci lokalnej bez błędów.

9.8. Wnioski z etapu 9

W wyniku wdrożenia kopii zapasowej i testu przywracania:

- Skonfigurowano automatyczny system backupu domeny w oparciu o Windows Server Backup.
- Utworzono bezpieczną kopię danych systemowych, obejmującą wszystkie kluczowe elementy infrastruktury IT.
- Przeprowadzono test przywracania Active Directory, który potwierdził pełną integralność danych.
- Zwiększoñ odporoñść systemu firma.local na awarie, utratę danych i błędy administracyjne.

10. Wnioski końcowe

Projekt wdrożenia domeny firma.local zakończył się pełnym powodzeniem. Zaprojektowane i zrealizowane środowisko sieciowe jest stabilne, bezpieczne i skalowalne — gotowe do dalszej rozbudowy o dodatkowe serwery, konta użytkowników i zasady GPO. Wdrożenie potwierdziło, że wykorzystanie technologii Windows Server 2019 pozwala na efektywne zarządzanie zasobami w małej lub średniej firmie, zapewniając wysoki poziom bezpieczeństwa oraz centralną kontrolę nad wszystkimi elementami sieci.