Helion

<packt>

WYDANIE IV

Windows Server 2025

Kompendium administratora i przygotowanie do egzaminu AZ-800

BEKIM DAUTI

Tytuł oryginału: Windows Server 2025 Administration Fundamentals:
A beginner's guide to managing and administering
Windows Server environments, 4th Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-289-3329-3

First published in the English language under the title 'Windows Server 2025 Administration Fundamentals – Fourth Edition – (9781836205005)'

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/ws25k4
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

CZĘŚĆ 2. Konfiguracja systemu Windows Server 2025

CZĘŚĆ 3. Konfiguracja systemu Windows Server 2025

CZĘŚĆ 4. Nowe i ulepszone funkcje w Windows Server 2025

CZĘŚĆ 5. Konserwacja systemu Windows Server 2025 i zarządzanie nim

CZĘŚĆ 6. Nauka i przygotowanie do egzaminu certyfikacyjnego AZ-800

Usługi katalogowe w systemie Windows Server 2025

Rozdział 4

W tym rozdziale pogłębisz swoją wiedzę na temat infrastruktury IT w organizacji, koncentrując się na usługach domenowych, które są kluczowe w zarządzaniu siecią opartą na systemie Windows. Poznasz usługi **AD DS** (ang. *Active Directory Domain Services*) i **DNS** (ang. *Domain Name System*) i zrozumiesz ich fundamentalne znaczenie dla struktury i funkcjonowania środowiska sieciowego. Zdobędziesz wiedzę na temat kluczowych pojęć, takich jak **domeny**, **lasy**, **drzewa domen**, **domeny podrzędne** i **kontrolery domeny** (ang. *domain controllers* — DC). Dowiesz się, czym są poziomy funkcjonalności i relacje zaufania, które ułatwiają integrację różnych segmentów sieci oraz efektywne udostępnianie zasobów. Dodatkowo poznasz zasady działania DNS, w tym konfigurację stref wyszukiwania w przód i wstecz oraz typy rekordów DNS, które są niezbędne do rozwiązywania nazw domenowych i zapewnienia stabilnej komunikacji sieciowej.

Dowiesz się również, jak wykorzystać **jednostki organizacyjne** (ang. *Organizational Unit* — OU), **kontenery domyślne**, **konta użytkowników** oraz różne typy i zakresy grup do efektywnego zarządzania **kontami użytkowników i komputerów** w środowisku domenowym. Zrozumienie tych mechanizmów pozwoli Ci usprawnić zarządzanie zasobami domeny i poprawić strukturę organizacyjną sieci. Rozdział kończy się ćwiczeniem praktycznym, w którym zainstalujesz role AD DS i DNS, a następnie wypromujesz serwer do roli kontrolera domeny. Dzięki temu zdobędziesz niezbędne umiejętności potrzebne do wdrożenia domeny Windows Server i zarządzania nią oraz przygotujesz grunt pod bardziej zaawansowane zarządzanie środowiskiem sieciowym.

W tym rozdziale omówimy między innymi następujące zagadnienia:

- Analiza infrastruktury **Active Directory** (**AD**) w środowisku Windows Server 2025.
- Dodawanie i konfigurowanie roli AD DS.
- Podstawy działania usługi DNS i jej konfiguracja w systemie Windows Server 2025.
- Zarządzanie jednostkami organizacyjnymi (OU) i kontenerami domyślnymi.
- Zarządzanie kontami użytkowników i grupami w Active Directory.
- Instalacja ról AD DS i DNS oraz promowanie serwera do roli kontrolera domeny.

Wymagania techniczne

Aby zrealizować ćwiczenia zawarte w tym rozdziale, powinieneś mieć następujące środowisko sprzętowe:

- **komputer z systemem Windows 11 Pro**, wyposażony w co najmniej 16 GB pamięci RAM, dysk twardy o pojemności 1 TB oraz stabilne połączenie internetowe;
- maszyna wirtualna z systemem **Windows Server 2025 Standard** (Desktop Experience), oznaczona jako *Virtual Machine 1*, skonfigurowana w drzewie domeny `Dautti.local`, mająca co najmniej 4 GB pamięci RAM, 100 GB wolnej przestrzeni dyskowej i dostęp do internetu;
- druga maszyna wirtualna z systemem Windows Server 2025 Standard (Desktop Experience), oznaczona jako *Virtual Machine 2*, skonfigurowana w drzewie domeny `ITTrainings.local`, mająca minimum 4 GB pamięci RAM, 100 GB wolnej przestrzeni dyskowej i dostęp do internetu;
- trzecia maszyna wirtualna z systemem Windows Server 2025 Standard (Desktop Experience), oznaczona jako *Virtual Machine 3*, skonfigurowana w domenie podrzędnej `Programming.Dautti.local`, mająca co najmniej 4 GB pamięci RAM, 100 GB wolnej przestrzeni dyskowej i dostęp do internetu.

Takie środowisko zapewni Ci wszystkie niezbędne zasoby i ustawienia do sprawnego wykonania zaplanowanych ćwiczeń.

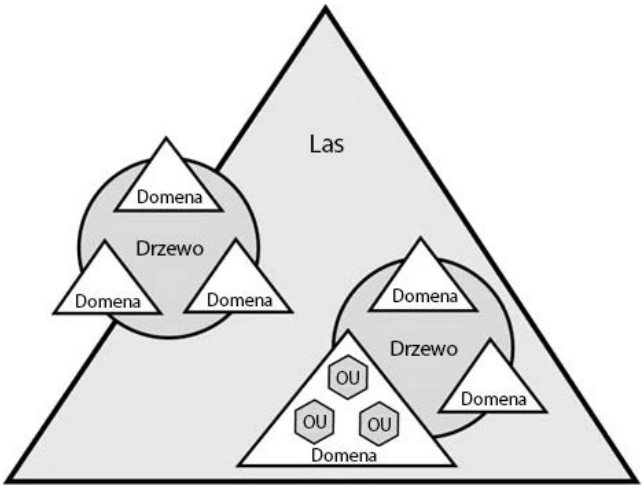
Analiza infrastruktury Active Directory w środowisku Windows Server 2025

Active Directory (AD) to kluczowa technologia firmy Microsoft, pełniąca funkcję rozproszonej usługi katalogowej. Umożliwia hierarchiczne i bezpieczne zarządzanie zasobami sieciowymi w środowisku Windows Server. Stanowi scentralizowane repozytorium, w którym przechowywane są kluczowe obiekty — takie jak konta użytkowników, komputery, drukarki oraz usługi sieciowe — każdy z przypisanymi indywidualnymi ustawieniami zabezpieczeń.

Unikalne atrybuty każdego obiektu w AD dają możliwość szczegółowego zarządzania zasobami oraz efektywnego administrowania w obrębie całej infrastruktury sieciowej. Niezależnie od tego, czy pracujesz z kontem użytkownika, komputerem, drukarką czy usługą sieciową — każdy z tych obiektów ma zestaw charakterystycznych atrybutów, takich jak **identyfikator bezpieczeństwa** (ang. *Security Identifier* — SID), przynależność do grup czy listy kontroli dostępu (ang. *Access Control List* — ACL). Dzięki tym atrybutom możesz definiować indywidualne uprawnienia, przypisywać role oraz wdrażać polityki dostępu, które są dostosowane do specyfiki danego obiektu.

Architektura Active Directory, jak pokazano na rysunku 4.1, opiera się na trzech podstawowych poziomach organizacyjnych:

- **Domena** (ang. *domain*) — podstawowa jednostka administracyjna, wyznaczająca granice obowiązywania polityk i ustawień bezpieczeństwa.
- **Drzewo** (ang. *tree*) — zbiór domen połączonych ciągłą przestrzenią nazw, odzwierciedlający hierarchiczne relacje między nimi.
- **Las** (ang. *forest*) — reprezentuje najwyższy poziom organizacji. Może obejmować wiele drzew domen i pełni funkcję nadrzędnej warstwy integrującej całą usługę katalogową Active Directory.



Rysunek 4.1. Architektura Active Directory (źródło: Websentra)

Warstwowa struktura usługi Active Directory ułatwia efektywne zarządzanie zasobami oraz zapewnia wysoką skalowalność, umożliwiając zarazem obsługę złożonych struktur organizacyjnych. Dzięki niej możesz precyzyjnie dopasować infrastrukturę sieciową do specyfiki operacyjnej swojej firmy, nie rezygnując przy tym z rygorystycznych standardów bezpieczeństwa i kontroli administracyjnej.

W dalszej części przyjrzymy się szczegółowym funkcjom i konfiguracjom AD. W ten sposób nabędziesz wiedzy i praktycznych umiejętności niezbędnych do skutecznego wdrażania usług katalogowych i zarządzania nimi w Twojej organizacji.

Rola i znaczenie Active Directory

Active Directory to znacznie więcej niż tylko usługa katalogowa — odgrywa fundamentalną rolę w nowoczesnych infrastrukturach IT i w zarządzaniu środowiskami opartymi na systemie Windows. Jeżeli dopiero zaczynasz swoją drogę zawodową w branży IT, musisz zrozumieć znaczenie Active Directory, by poznać jego funkcje oraz korzyści, jakie oferuje w codziennym zarządzaniu systemami:

- **Scentralizowane zarządzanie** — jedną z głównych zalet Active Directory jest możliwość centralizacji zarządzania. Dzięki temu administratorzy IT mogą zarządzać kontami użytkowników, komputerami i zasobami z jednego miejsca, co znacząco redukuje złożoność operacyjną i ogranicza nakład pracy administracyjnej. Takie podejście usprawnia proces przydzielania i odbierania uprawnień użytkownikom, co ułatwia utrzymanie uporządkowanej i wydajnej infrastruktury sieciowej.
- **Zwiększone bezpieczeństwo** — Active Directory zwiększa bezpieczeństwo przez wykorzystanie identyfikatorów SID oraz list kontroli dostępu (ACL). Dzięki odpowiedniemu przypisywaniu uprawnień zapewnia dostęp do określonych zasobów wyłącznie autoryzowanym użytkownikom; chroni w ten sposób poufne informacje i minimalizuje ryzyko nieuprawnionego dostępu. Ten model bezpieczeństwa odgrywa kluczową rolę w ochronie danych organizacji oraz zachowaniu zgodności z normami regulacyjnymi.
- **Skalowalność** — hierarchiczna struktura Active Directory wspiera skalowalność organizacji. Wraz z jej rozwojem AD umożliwia bezproblemową integrację nowych użytkowników i zasobów bez negatywnego wpływu na wydajność czy poziom bezpieczeństwa. Taka elastyczność umożliwia dynamiczne dopasowanie infrastruktury IT do bieżących potrzeb biznesowych oraz jej skalowanie zgodnie z rozwojem organizacji.
- **Egzekwowanie zasad** — Active Directory umożliwia centralne zarządzanie zasadami grupowymi w obrębie całej infrastruktury sieciowej, wspierając organizację w jednolitym wdrażaniu polityk bezpieczeństwa oraz standardów zgodności. Dzięki tej funkcjonalności możliwe jest skuteczne egzekwowanie ustalonych reguł wobec wszystkich użytkowników i urządzeń, co przekłada się na wyższy poziom ochrony danych oraz zwiększoną efektywność operacyjną.

Dobre zrozumienie podstawowych zasad działania usługi Active Directory pozwala docenić jej kluczową rolę w zarządzaniu oraz ochronie zasobów sieciowych, tworząc fundament dla efektywnego zarządzania środowiskiem IT organizacji.

Podstawowe protokoły i usługi wspierające Active Directory

Usługa Active Directory opiera się na kilku kluczowych protokołach i usługach, które zapewniają jej sprawne i niezawodne działanie i z których każdy wspiera inny aspekt zarządzania siecią oraz bezpieczeństwa:

- **Protokół LDAP** (ang. *Lightweight Directory Access Protocol*) — to podstawowy protokół komunikacyjny, umożliwiający użytkownikom oraz aplikacjom wysyłanie zapytań i nawiązywanie interakcji z danymi przechowywanymi w bazie AD. LDAP zapewnia ustandaryzowaną metodę dostępu do informacji przechowywanych w AD i zarządzania nimi, co czyni go kluczowym elementem w realizowaniu operacji związanych z usługą katalogową.

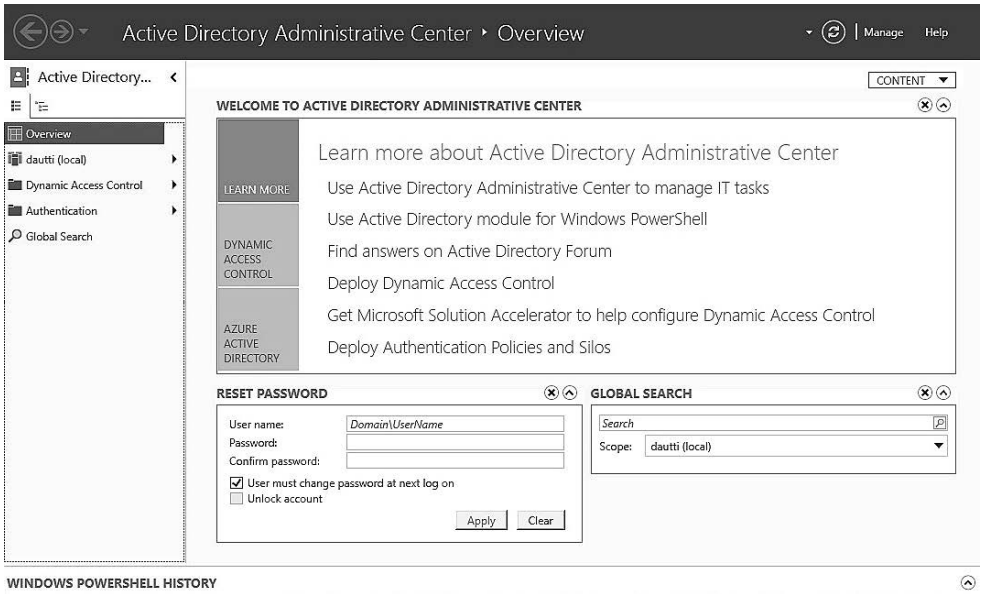
- **Protokół Kerberos** — to zaawansowany mechanizm uwierzytelniania, stanowiący fundament architektury bezpieczeństwa w Active Directory. Kerberos opiera się na systemie biletów, które umożliwiają bezpieczną weryfikację tożsamości użytkowników oraz serwerów w obrębie sieci, co zapobiega nieuprawnionemu dostępowi i gwarantuje, że wszystkie podmioty komunikujące się ze sobą w sieci są prawidłowo uwierzytelnione. Protokół ten odgrywa kluczową rolę w utrzymaniu integralności oraz poufności środowiska sieciowego.
- **DNS** — protokół ten stanowi integralną część funkcjonalności Active Directory. DNS pełni funkcję katalogu zarówno dla internetu, jak i sieci wewnętrznych. Dokonuje translacji przyjaznych dla użytkownika nazw domen na odpowiadające im numeryczne adresy IP. Proces ten jest kluczowy w skutecznym lokalizowaniu zasobów sieciowych i uzyskiwaniu do nich dostępu. W środowisku Active Directory DNS nie tylko zajmuje się rozwiązywaniem nazw domen, ale również wspiera funkcje specyficzne dla AD, takie jak lokalizowanie kontrolerów domeny oraz zapewnianie dostępności usług w infrastrukturze sieciowej.

Wymienione wyżej protokoły i usługi stanowią fundament działania usługi Active Directory. Umożliwiają świadczenie bezpiecznej, skalowalnej oraz wydajnej usługi katalogowej, która wspiera złożone wymagania organizacyjne.

Narzędzia i role do zarządzania usługą Active Directory

Active Directory to stabilne i zaawansowane środowisko, które zapewnia kompleksowy zestaw usług umożliwiających scentralizowane zarządzanie zasobami sieciowymi i znacząco ułatwiających pracę administratorów w złożonych środowiskach IT. Aby skutecznie zarządzać różnymi funkcjami usługi Active Directory, firma Microsoft oferuje zestaw specjalistycznych konsol administracyjnych dostępnych w ramach środowiska **Microsoft Management Console (MMC)** (*mmc.exe*). Każdą z tych konsol tworzono z myślą o realizacji określonych zadań związanych z obsługą usługi katalogowej:

- **Active Directory Administrative Center** (*dsac.exe*) — kluczowe narzędzie, pokazane na rysunku 4.2, służące do kompleksowego zarządzania usługami katalogowymi w środowisku Windows Server. Nowoczesny interfejs konsoli łączy wiele funkcji administracyjnych, które pozwalają na efektywne nadzorowanie dostępnych usług katalogowych. W skład konsoli wchodzi przystawka **Active Directory Users and Computers** (*dsa.msc*), która jest niezbędna do zarządzania kontami użytkowników, obiektami komputerów, jednostkami organizacyjnymi (OU) oraz ich właściwościami. Narzędzie to stanowi podstawę codziennych zadań administracyjnych, takich jak tworzenie kont użytkowników i zarządzanie nimi, tworzenie i modyfikowanie grup i urządzeń oraz organizowanie ich w strukturze AD.



Rysunek 4.2. Active Directory Administrative Center w systemie Windows Server 2025

- **Konsola Active Directory Domains and Trusts** (*domain.msc*) — konsola służy do realizacji zadań związanych z zarządzaniem domenami w środowisku Active Directory. Umożliwia administratorom konfigurowanie oraz nadzorowanie relacji zaufania między domenami, które są kluczowe dla zapewnienia bezpiecznej komunikacji oraz współdzielenia zasobów między domenami należącymi do tego samego lasu lub różnych lasów. Konsola umożliwia również konfigurowanie **poziomów funkcjonalności domen** (ang. *Domain Functional Levels* — DFL), które określają funkcje dostępne w domenie w zależności od używanej wersji systemu Windows Server, i zarządzanie nimi.
- **Konsola Active Directory Sites and Services** (*dssite.msc*) — stanowi kluczowe narzędzie do zarządzania replikacją danych między różnymi lokacjami w środowisku AD. Lokacje w AD odzwierciedlają fizyczną strukturę sieci, a konsola pozwala administratorom optymalizować i kontrolować sposób replikowania informacji katalogowych między różnymi lokalizacjami geograficznymi, by zapewnić spójność i dostępność danych w całej organizacji. Narzędzie to obsługuje również konfigurację usług takich jak serwery katalogu globalnego oraz umożliwia efektywne kierowanie żądań uwierzytelniania w zależności od lokalizacji użytkownika.
- **Moduł AD dla Windows PowerShell** — nie jest narzędziem graficznym, ale oferuje interfejs wiersza poleceń umożliwiający realizację zaawansowanych i zautomatyzowanych zadań administracyjnych. Zestaw poleceń dostępnych w powłoce PowerShell pozwala administratorom na tworzenie skryptów obsługujących złożone operacje, automatyzowanie powtarzalnych zadań i zarządzanie obiektami AD na dużą skalę, co czyni go nieocenionym narzędziem w dużych lub wysoce spersonalizowanych środowiskach sieciowych.

Aby wdrożyć usługi katalogowe w środowisku organizacji, musisz zainstalować i odpowiednio skonfigurować rolę AD DS na serwerze Windows Server. AD DS stanowi podstawę środowiska Active Directory: umożliwia przechowywanie i organizowanie informacji o zasobach sieciowych, takich jak konta użytkowników, grupy, komputery i zasady, oraz zarządzanie nimi. AD DS obsługuje również zaawansowane mechanizmy zabezpieczeń, takie jak scentralizowane uwierzytelnianie i autoryzacja, które odgrywają kluczową rolę w utrzymaniu integralności systemu i zapewnieniu wysokiego poziomu bezpieczeństwa sieci.

Uwaga

Rozbudowany zbiór darmowych skryptów PowerShell możesz znaleźć w Microsoft Script Center (*https://technet.microsoft.com/en-us/scriptcenter/bb410849.aspx*) oraz PowerShell Gallery (*https://www.powershellgallery.com/*). Obie platformy są cenionymi repozytoriami, w których specjaliści IT mogą wyszukiwać i udostępniać skrypty do różnych zadań administracyjnych. Zawierają bogate kolekcje skryptów przeznaczonych między innymi do usług Active Directory i DNS, co czyni je niezwykle przydatnymi narzędziami do automatyzowania i upraszczania złożonych zadań związanych z zarządzaniem środowiskiem sieciowym.

Szczegółowy przewodnik dotyczący konfiguracji usług Active Directory Domain Services, obejmujący między innymi instalację roli DNS oraz promocję serwera do roli kontrolera domeny, znajdziesz w rozdziale 5., „Dodawanie ról serwera w systemie Windows Server 2025”. Rozdział ten zawiera zestaw praktycznych ćwiczeń, które krok po kroku przeprowadzą Cię przez cały proces wdrożenia, co umożliwi Ci dogłębne zrozumienie poszczególnych etapów niezbędnych do zintegrowania usług AD DS w Twojej infrastrukturze sieciowej.

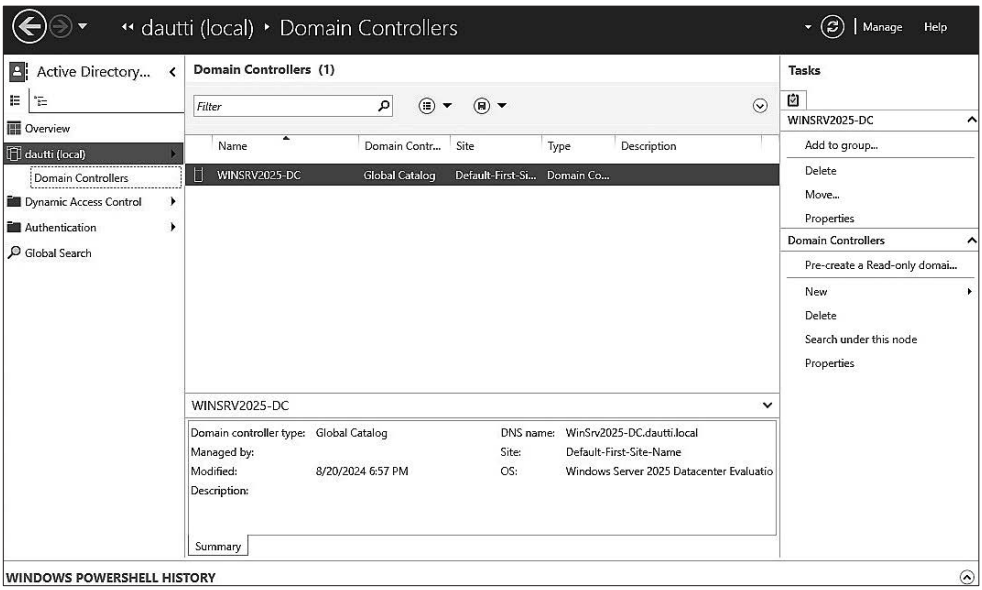
W następnym podrozdziale omówimy kluczowe komponenty infrastruktury Active Directory, począwszy od szczegółowej analizy kontrolerów domeny, które stanowią fundament każdego środowiska AD.

Dodawanie i konfigurowanie roli AD DS

W środowiskach opartych na Windows Server rola AD DS (ang. *Active Directory Domain Services*) ma fundamentalne znaczenie w zapewnianiu scentralizowanych usług katalogowych, które ułatwiają zarządzanie siecią i wspierają procesy uwierzytelniania. Skupimy się tutaj na procesie dodawania i konfigurowania roli AD DS i omówimy kluczowe zagadnienia, takie jak wdrażanie kontrolerów domeny, definiowanie i konfigurowanie domen oraz tworzenie struktur hierarchicznych, takich jak drzewa i domeny podrzędne. Ponadto przyjrzymy się koncepcji przestrzeni nazw, która umożliwia logiczne uporządkowanie zasobów katalogowych, oraz sprawdzimy, w jaki sposób lokacje poprawiają **wydajność** sieci i efektywność replikacji. Opanowanie tych zagadnień stanowi fundament skutecznego wdrożenia oraz zarządzania skalowalną i niezawodną infrastrukturą AD DS, zapewniający wysoką funkcjonalność i wydajność w środowisku informatycznym firmy.

Kontrolery domeny

Kontroler domeny (ang. *domain controller* — DC), pokazany na rysunku 4.3, to serwer odgrywający kluczową rolę w zarządzaniu tożsamością użytkowników oraz weryfikowaniu ich uprawnień w sieci. Jego głównym zadaniem jest uwierzytelnianie użytkowników i autoryzacja dostępu do zasobów sieciowych na podstawie zasad bezpieczeństwa zdefiniowanych w domenie. W starszych środowiskach Windows, a zwłaszcza Windows NT, zarządzanie domeną opierało się na architekturze z **głównym kontrolerem domeny** (ang. *Primary Domain Controller* — PDC), który odpowiadał za obsługę najważniejszych funkcji domeny. Redundancję zapewniały **zapasowe kontrolery domeny** (ang. *Backup Domain Controller* — BDC), które przejmowały część zadań w razie awarii PDC. Jednak model ten został zastąpiony przez wprowadzony w systemie Windows 2000 mechanizm replikacji wielowęzłowej (ang. *multi-master replication*), który umożliwia zarządzanie funkcjami domeny przez wiele kontrolerów. W takim rozwiązaniu każdy kontroler domeny ma możliwość wykonywania operacji odczytu i zapisu, co znacząco zwiększa niezawodność oraz dostępność usług katalogowych i uwierzytelniania w całej infrastrukturze sieciowej.



Rysunek 4.3. Kontrolery domeny w Active Directory Administrative Center

Windows Server 2025 wprowadził istotne zmiany w podejściu do kontrolerów domeny: wyeliminował tradycyjny podział na role główne i zapasowe. Zamiast tego kontrolery domeny są teraz identyfikowane za pomocą kolejnych oznaczeń, takich jak **DC1** i **DC2**, które wskazują jedynie ich kolejność, a nie przypisaną funkcję. To nowoczesne rozwiązanie umożliwia tworzenie bardziej elastycznego i skalowalnego środowiska zarządzania domeną, w którym wszystkie kontrolery domeny funkcjonują jako równorzędne węzły i dzielą odpowiedzialność za uwierzytelnianie i usługi katalogowe. Dzięki tej ewolucji możesz, jako specjalista IT, efektywnie wdrażać i utrzymywać środowiska zgodne z najnowszymi standardami i rozwiązaniami w obszarze zarządzania tożsamością i usługami katalogowymi.

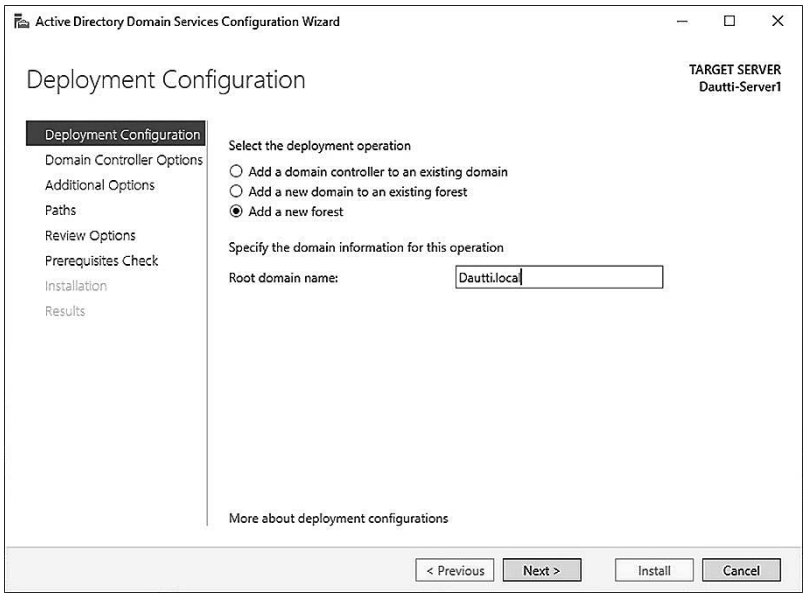
Uwaga

Gdy serwer zostaje dołączony do domeny, lecz nie pełni funkcji kontrolera domeny, klasyfikowany jest jako **serwer członkowski** (ang. *member server*). Serwery członkowskie działają zgodnie z obowiązującymi politykami domeny oraz mechanizmami kontroli dostępu, ale nie obsługują żądań uwierzytelniania ani zadań związanych z zarządzaniem domeną.

Biorąc pod uwagę, że kontrolery domeny odgrywają kluczową rolę w zapewnianiu dostępu do zasobów domeny oraz realizacji procesów uwierzytelniania, zrozumienie koncepcji domen jest nie tylko ważne, ale wręcz niezbędne do pełnego opanowania zasad działania infrastruktury Active Directory. Jako specjalista IT, odgrywasz istotną rolę w interpretowaniu i wdrażaniu struktur domenowych oraz ich funkcji w zarządzaniu siecią, dlatego w następnym punkcie szczegółowo omówimy związane z tym zagadnienia.

Domeny

Domeny stanowią kluczowy element w zarządzaniu siecią. Umożliwiają logiczne grupowanie kont użytkowników, komputerów, urządzeń oraz usług sieciowych w ramach spójnej struktury administracyjnej. Taka organizacja pozwala na zcentralizowanie zarządzania zasobami oraz wdrażanie jednolitych polityk bezpieczeństwa w całym środowisku IT. W tej architekturze istotną funkcję pełni kontroler domeny, a usługi Active Directory Domain Services (AD DS) odgrywają fundamentalną rolę w tworzeniu domeny i zapewnianiu ciągłości jej działania. Na rysunku 4.4 pokazano proces konfiguracji domeny w oknie kreatora **Active Directory Domain Services Configuration Wizard**. Widać na nim etapy tworzenia domen w środowisku Windows Server i zarządzania nimi.



Rysunek 4.4. Konfigurowanie domeny głównej w systemie Windows Server 2025

Uwaga

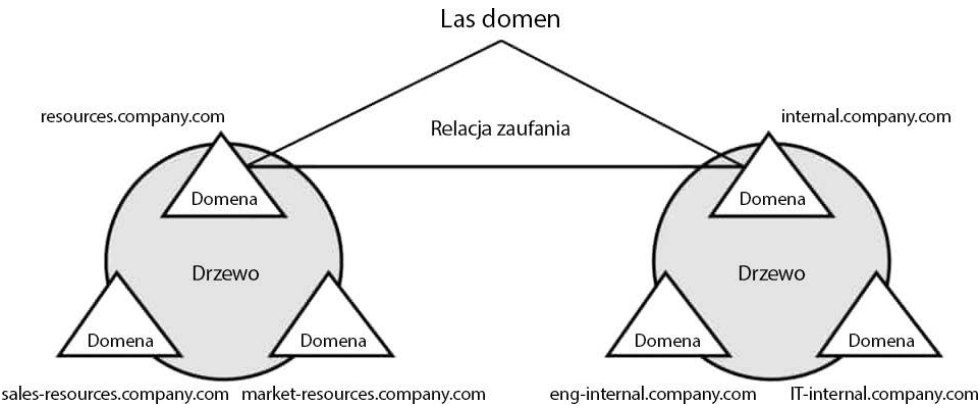
Trzeba wprowadzić rozróżnienie między domeną katalogową (ang. *directory domain*) a nazwą domeny (ang. *domain name*). W kontekście usług katalogowych termin domena odnosi się do ustrukturyzowanej bazy danych zasobów sieciowych, obejmującej zasoby sieciowe, takie jak konta użytkowników, serwery i urządzenia. Elementy te są zarządzane wspólnie według określonych zasad administracyjnych. Taka domena umożliwia efektywne zarządzanie infrastrukturą IT organizacji oraz zwiększa poziom jej bezpieczeństwa. Z kolei nazwa domeny jest częścią systemu DNS, będącego hierarchicznym systemem nazewnictwa służącym do identyfikowania i lokalizowania zasobów w internecie, takich jak strony internetowe czy serwery poczty elektronicznej.

Ponadto domeny mogą być zorganizowane w **drzewo domen** (ang. *domain tree*), które reprezentuje hierarchiczną strukturę wielu powiązanych ze sobą domen. Taka struktura pozwala na tworzenie relacji typu domena nadrzędna/ domena podrzędna (ang. *parent-child relationship*), gdzie każda domena w obrębie drzewa może dziedziczyć zasady i ustawienia od swojej domeny nadrzędnej, zachowując własną, niezależną konfigurację. W następnym punkcie szczegółowo omówimy koncepcję drzew domen. Między innymi wyjaśnimy, w jaki sposób rozszerzają one strukturę domeny oraz umożliwiają tworzenie bardziej złożonych i skalowalnych modeli organizacyjnych.

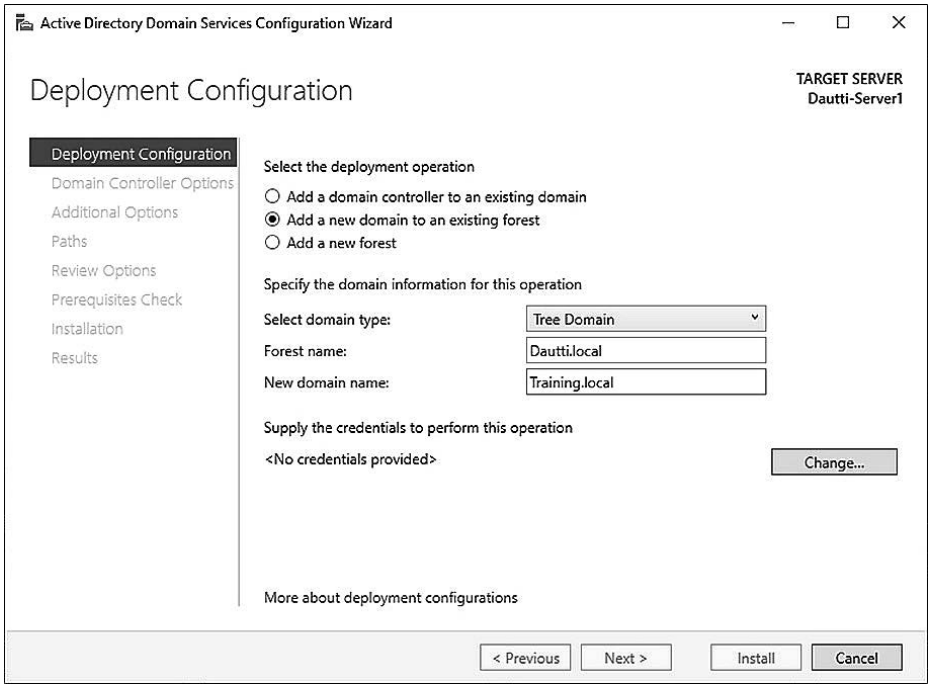
Drzewa domen

Aby w pełni zrozumieć architekturę Active Directory, trzeba dogłębnie poznać i dobrze zrozumieć koncepcję drzewa domen. Drzewo domen reprezentuje logiczną strukturę w AD, składającą się z jednej lub więcej domen, które współdzielą przestrzeń nazw i są zorganizowane w układzie hierarchicznym. Taka struktura nie tylko porządkuje domeny, ale także zapewnia ich wzajemne zaufanie dzięki domyślnej, przechodniej relacji zaufania (ang. *transitive trust relationship*). W Active Directory relacja zaufania (zobacz rysunek 4.5) umożliwia użytkownikom jednej domeny uwierzytelnianie się i dostęp do zasobów znajdujących się w innej domenie bez konieczności posiadania odrębnych poświadczeń. Zaufanie przechodnie oznacza, że jeżeli domena A ufa domenie B, a domena B ufa domenie C, to domena A automatycznie ufa domenie C. Taki mechanizm znacząco upraszcza proces udostępniania zasobów i uwierzytelniania między domenami w tym samym drzewie domen. Podczas dodawania nowej domeny do istniejącego drzewa należy podczas procesu promocji serwera wskazać nazwę odpowiedniej domeny nadrzędnej tak, aby prawidłowo osadzić nową domenę w strukturze hierarchicznej.

Proces ten polega na wskazaniu domeny nadrzędnej (ang. *parent domain*) podczas etapu promocji serwera, co umożliwia zintegrowanie nowej domeny z istniejącym drzewem domen. Takie działanie umożliwia osadzenie nowej domeny w hierarchicznej strukturze Active Directory, co umożliwia jej dziedziczenie zasad i ustawień administracyjnych od domeny nadrzędnej przy zachowaniu własnej, odrębnej tożsamości w ramach drzewa. Na rysunku 4.6 pokazano proces tworzenia domeny podrzędnej w środowisku Windows Server 2025. Grafika ukazuje sposób, w jaki nowa domena zostaje włączona do istniejącej struktury drzewa oraz jak zostaje zintegrowana z całą przestrzeń nazw.



Rysunek 4.5. Hierarchiczna architektura lasu domen (źródło: Websentra)



Rysunek 4.6. Konfigurowanie domeny drzewa w systemie Windows Server 2025

Koncepcja drzewa domen nabiera szerszego znaczenia w momencie, gdy wiele drzew domen zostaje połączonych w jedną strukturę i tym samym tworzy tzw. las (ang. *forest*). Las domen stanowi nadrzędną strukturę organizacyjną w architekturze Active Directory, która grupuje wszystkie drzewa domen w obrębie przedsiębiorstwa, co umożliwia centralne zarządzanie zasobami w całym środowisku. Las pełni w AD funkcję najwyższego poziomu hierarchii, zapewniając ramy do zarządzania wieloma drzewami domen i ich wzajemnymi relacjami. Szczegółowa struktura lasu i jego kluczowe funkcje są omówione w następnym punkcie.

Lasy domen

W środowisku Active Directory koncepcja **lasu** jest porównywalna do naturalnego lasu, który składa się z wielu drzew. Las AD może obejmować pojedyncze drzewo domenowe lub zbiór wzajemnie powiązanych drzew domenowych. Każde drzewo w obrębie lasu współdzieli wspólny schemat i globalny katalog, jednak nie musi korzystać z tej samej przestrzeni nazw. Domena główna (ang. *root domain*) jest pierwszą domeną utworzoną w drzewie domeny i stanowi podstawę dla całej jego struktury. Zazwyczaj pełni ona kluczowe funkcje, takie jak funkcja wzorca schematu (ang. *schema master*) oraz wzorca nazw domen (ang. *domain naming master*). Drzewo domeny pełniące funkcję domeny głównej może istnieć samodzielnie w obrębie lasu. Jednak gdy drzew jest wiele, las odgrywa rolę nadrzędnej struktury organizacyjnej, integrującej wszystkie drzewa i zarządzającej nimi, dzięki czemu możliwe jest utworzenie spójnego, skalowalnego i centralnie zarządzanego środowiska katalogowego.

Las stanowi najwyższy poziom hierarchii w strukturze Active Directory. Zapewnia spójny system katalogowy umożliwiający współdzielenie zasobów oraz centralne zarządzanie administracyjne wszystkimi domenami w jego obrębie. Choć na pierwszy rzut oka koncepcja lasu jako domeny nadrzędnej i zarazem struktury obejmującej inne domeny może sprawiać wrażenie nieco sprzecznej, to jednak znakomicie odzwierciedla jego podwójną rolę w organizowaniu i łączeniu ze sobą różnych domen.

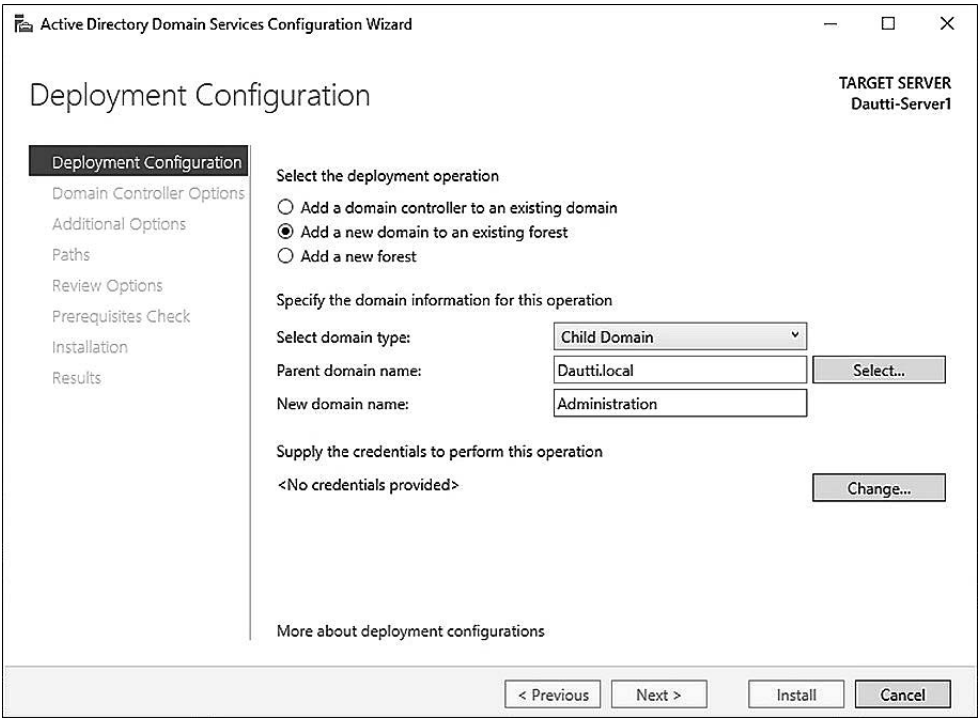
Aby utworzyć i skonfigurować las w środowisku Windows Server 2025, możesz wykorzystać kreatora konfiguracji usług domenowych AD DS (ang. *Active Directory Domain Services Configuration Wizard*), który służy również do definiowania struktury domen w obrębie drzewa. Kreator prowadzi administratora przez niezbędne kroki i ustawienia, co znacząco upraszcza proces tworzenia lasu (zobacz rysunek 4.6).

W ramach struktury drzewa domenowego możliwe jest tworzenie dodatkowych poddomen, które nazywamy domenami podrzędnymi. Stanowią one logiczne rozszerzenia domeny nadrzędnej, które umożliwiają bardziej precyzyjne odwzorowanie struktury organizacyjnej oraz efektywne zarządzanie zasobami. W następnym punkcie szczegółowo omówimy ich rolę, sposób konfiguracji oraz funkcjonalność, a także znaczenie, jakie mają w ogólnej strukturze Active Directory.

Domeny podrzędne

Domena podrzędna to domena podporządkowana w strukturze drzewa domen w Active Directory. Jak pokazano na rysunku 4.6, w naszym przykładowym środowisku istnieją dwa niezależne drzewa domenowe: `Dautti.local` i `Training.local`. `Dautti.local` pełni funkcję domeny głównej lasu, definiując podstawową przestrzeń nazw dla całej struktury. W tej konfiguracji drzewo `Training.local` zawiera domenę podrzędną o nazwie `Administration.Dautti.local`. Jest ona rozszerzeniem przestrzeni nazw domeny nadrzędnej, co pozwala zachować spójną i logicznie uporządkowaną hierarchię katalogu.

W systemie Windows Server 2025 domenę podrzędną tworzy się za pomocą kreatora konfiguracji usług AD DS, który jest również używany do konfiguracji innych typów domen. Narzędzie to prowadzi administratora przez wszystkie wymagane etapy konfiguracji, co zapewnia spójność i przejrzystość całego procesu, jak pokazano na rysunku 4.7.



Rysunek 4.7. Konfigurowanie domeny podrzędnej w Windows Server 2025

Struktura drzew i domen podrzędnych w Active Directory przypomina klasyczną strukturę danych typu drzewo, w której każda domena stanowi węzeł powiązany relacją nadrzędny-podrzędny. Taki hierarchiczny układ sprzyja efektywnemu zarządzaniu zasobami oraz umożliwia skuteczne delegowanie zadań administracyjnych w ramach organizacji. Domena nadrzędna pełni funkcję kontrolną wobec swoich domen podrzędnych, które z kolei dziedziczą z domeny macierzystej określone atrybuty i zasady polityki, zarazem zachowując własną, odrębną tożsamość.

Zrozumienie hierarchicznej struktury Active Directory stanowi fundament skutecznego zarządzania środowiskiem katalogowym. W następnym punkcie omówimy role operacyjne, które są niezbędne do utrzymania stabilności, spójności i funkcjonalności infrastruktury AD.

Role głównych operacji (role operacyjne)

Active Directory Domain Services (AD DS) to złożona i zaawansowana usługa katalogowa, której skuteczne wdrożenie wymaga przemyślanego zaplanowania, tak aby można było w pełni wykorzystać jej możliwości. Po zakończeniu wdrożenia korzyści operacyjne stają się coraz bardziej zauważalne. Jednym z kluczowych komponentów AD DS są **role głównych operacji** (ang. *operations master roles*), nazywane również rolami operacyjnymi, które są niezbędne do utrzymania pełnej funkcjonalności usług katalogowych i zarządzania nimi.

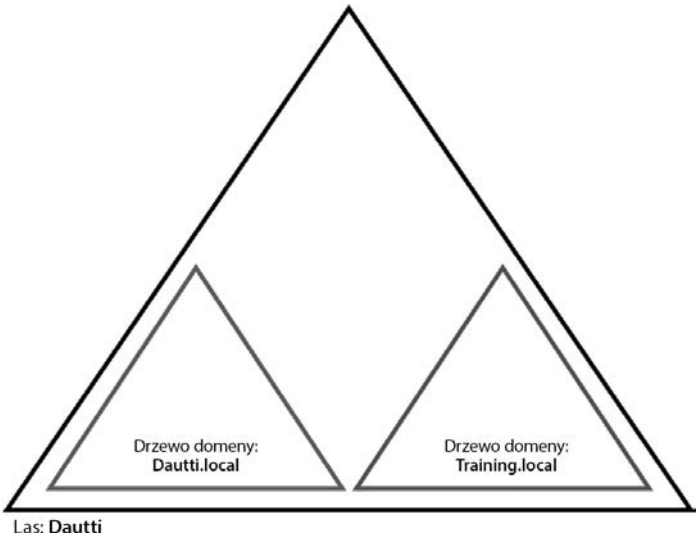
W poprzednim punkcie utworzyliśmy domenę główną `Dautti.local`, pełniącą funkcję podstawowej domeny dla całego lasu Active Directory. Domena ta jest hostowana na serwerze, który odgrywa również rolę kontrolera domeny (ang. *domain controller* — DC) i odpowiada za nadzorowanie i obsługę usług katalogowych w naszym środowisku sieciowym.

Gdy rola Active Directory Domain Services (AD DS) zostaje zainstalowana, a serwer wypromowany do rangi kontrolera domeny, usługa AD DS automatycznie przypisuje pięć kluczowych, głównych ról operacyjnych. Role te możemy podzielić na dwie kategorie:

- **Role obejmujące cały las** (ang. *forest-wide roles*) — do takich ról zaliczamy rolę **wzorca schematu** (ang. *schema master*) oraz rolę **wzorca nazw domen** (ang. *domain naming master*). Rola wzorca schematu zarządza schematem katalogu, który definiuje atrybuty i klasy obiektów dostępnych w katalogu, co zapewnia integralność i spójność struktury katalogu w całym lesie. Z kolei wzorzec nazw domen nadzoruje przestrzeń nazw domen i gwarantuje, że wszystkie nazwy domen w lesie są unikalne i nie powodują konfliktów nazw.
- **Role obejmujące domenę** (ang. *domain-wide roles*) — pozostałe trzy role: **wzorzec RID** (ang. *RID master*), **emulator kontrolera głównego** (ang. *PDC emulator*) i **wzorzec infrastruktury** (ang. *infrastructure master*), obejmują całą domenę. Wzorzec RID odpowiada za przydzielanie identyfikatorów SID dla kontrolerów domeny, umożliwiając im tworzenie nowych obiektów zabezpieczeń (ang. *security principals*). Emulator PDC obsługuje między innymi zmiany haseł i zarządza synchronizacją czasu w domenie, służąc zarazem jako pomost dla wstecznej kompatybilności z wcześniejszymi wersjami systemu Windows. Wzorzec infrastruktury odpowiada za utrzymanie i aktualizację odniesień do obiektów z innych domen, by zapewnić, że odwołania międzydomenowe pozostają aktualne i dokładne.

W przedstawionym przykładzie, zilustrowanym na rysunku 4.8, domena główna `Dautti.local` odgrywa role wzorca schematu i wzorca nazw domen dla całego lasu `Dautti`. Każde drzewo domenowe w tym lesie, takie jak `Dautti.local` czy `Training.local`, dysponuje własnymi rolami wzorca RID, emulatora kontrolera PDC i wzorca infrastruktury, które odpowiadają za realizację zadań i operacji specyficznych dla danej domeny.

Wymienione wyżej role są w środowisku Active Directory znane jako **role FSMO** (ang. *Flexible Single Master Operations*). Termin „flexible" (elastyczny) odnosi się do możliwości przenoszenia tych ról pomiędzy kontrolerami domeny w zależności od potrzeb administracyjnych lub operacyjnych. Z kolei określenie „single" (pojedynczy) podkreśla, że każda z ról może być w danym momencie przypisana tylko jednemu kontrolerowi domeny, co zapobiega konfliktom i zapewnia spójność działania usług katalogowych. Znajomość ról FSMO oraz ich funkcji ma kluczowe znaczenie dla skutecznego zarządzania infrastrukturą Active Directory oraz diagnozowania i rozwiązywania problemów w takich środowiskach. W następnym punkcie skupimy się na różnicach między domenami a grupami roboczymi i omówimy wybrane koncepcje związane z zarządzaniem siecią.



Rysunek 4.8. Struktura AD DS.

Różnice między domenami a grupami roboczymi

Aby móc właściwie rozróżnić domenę i grupę roboczą, trzeba zrozumieć podstawowe modele architektury sieciowej reprezentowane przez te struktury: **sieci równorzędnej** (ang. *peer-to-peer* — P2P) oraz **sieci typu klient-serwer**, które zostały pokrótce omówione w rozdziale 1., „Podstawy sieci komputerowych i wprowadzenie do systemu Windows Server 2025".

W sieci typu peer-to-peer (P2P), powszechnie określanej jako **grupa robocza** (ang. *workgroup*), każdy komputer działa niezależnie i samodzielnie zarządza własnymi zasobami. Taka architektura jest rozwiązaniem idealnym szczególnie do mniejszych sieci, typowych dla środowisk domowych lub małych biur, gdzie priorytetem jest prostota konfiguracji oraz bezpośrednie udostępnianie zasobów. W grupie roboczej każde urządzenie przechowuje własne, lokalne konta użytkowników i ich uprawnienia, bez scentralizowanego zarządzania czy kontroli. Takie zdecentralizowane podejście może być efektywne w przypadku prostych konfiguracji, ale wraz ze wzrostem liczby komputerów coraz trudniej jest utrzymać spójność konfiguracji oraz kontrolę dostępu. Brak centralnego zarządzania zwiększa ryzyko pojawiania się niespójnych polityk bezpieczeństwa oraz problemów związanych z zarządzaniem kontami użytkowników, co czyni grupy robocze rozwiązaniem nieadekwatnym do większych lub bardziej wymagających środowisk, szczególnie tam, gdzie przetwarzane są dane wrażliwe.

Z kolei architektura klient-serwer, obecna w środowisku domenowym, zapewnia bardziej zorganizowane i scentralizowane podejście do zarządzania zasobami i mechanizmami bezpieczeństwa. W środowisku domenowym centralny serwer, nazywany kontrolerem domeny (DC), nadzoruje zadania administracyjne i egzekwuje polityki bezpieczeństwa w całej sieci. Taki scentralizowany model zarządzania umożliwia efektywne uwierzytelnianie użytkowników, wdrażanie ujednoliconych polityk i kontrolowaną alokację zasobów, co ma kluczowe znaczenie w przypadku większych organizacji oraz

rozbudowanych środowisk sieciowych, takich jak **sieci metropolitalne** (**MAN**) czy **rozległe** (**WAN**). Domeny obsługują struktury hierarchiczne oraz zaawansowane mechanizmy bezpieczeństwa, co zapewnia wysoką skalowalność, efektywne zarządzanie i jednolite egzekwowanie zasad na wszystkich urządzeniach sieciowych. W rezultacie środowiska domenowe stanowią optymalne rozwiązanie dla dużych, złożonych środowisk, w których przetwarzane są dane wrażliwe, podczas gdy grupy robocze mogą być wystarczające dla mniejszych podmiotów, charakteryzujących się mniej restrykcyjnymi wymaganiami w zakresie zarządzania i bezpieczeństwa.

W tabeli 4.1 zamieszczono zestawienie najważniejszych różnic pomiędzy domenami a grupami roboczymi, uwzględniając ich mocne strony i ograniczenia w zależności od skali środowiska sieciowego i wymagań związanych z zarządzaniem. Przedstawione porównanie może być pomocne w wyborze najbardziej odpowiedniej architektury sieciowej dla danego środowiska.

Tabela 4.1. Domena a grupa robocza

Domena	Grupa robocza
Usługi są realizowane za pośrednictwem oddzielnego serwera	Komputery udostępniają zasoby na równych zasadach, bez konieczności korzystania z centralnego serwera
Przykład: sieć klient-serwer	Przykład: sieć peer-to-peer (P2P)

Zrozumienie przedstawionych różnic może Ci pomóc w podejmowaniu świadomych decyzji w zakresie projektowania infrastruktury sieciowej i zarządzania nią. W następnym punkcie omówimy koncepcję relacji zaufania między komputerem a kontrolerem domeny, co pozwoli Ci na pogłębienie wiedzy dotyczącej mechanizmów bezpieczeństwa oraz zarządzania środowiskiem sieciowym.

Relacje zaufania między domenami

Jednym z kluczowych pojęć w architekturze Active Directory jest relacja zaufania, omówiona wstępnie w podrozdziale dotyczącym drzewa domeny. Relacje zaufania odgrywają fundamentalną rolę w komunikacji między komputerami, kontrolerami domeny oraz samymi domenami. Kiedy komputer zostaje dołączony do domeny, przestaje używać do uwierzytelniania użytkowników **lokalnego menedżera kont zabezpieczeń** (ang. *Security Accounts Manager* — SAM). Zamiast tego proces uwierzytelniania zostaje przekazany kontrolerowi domeny, który zazwyczaj wykorzystuje protokół Kerberos. Ta zmiana ma istotne znaczenie, ponieważ centralizuje mechanizm uwierzytelniania użytkowników i zapewnia weryfikację poświadczeń przez zaufany kontroler domeny, a nie lokalną maszynę. Takie rozwiązanie nie tylko usprawnia proces logowania i dostępu do zasobów, ale również znacząco podnosi poziom bezpieczeństwa przez egzekwowanie spójnych polityk bezpieczeństwa w całym środowisku sieciowym.

Relacje zaufania w środowisku Active Directory wykraczają poza pojedyncze komputery i obejmują całe domeny funkcjonujące w ramach lasu, czyli logicznego zbioru wielu drzew domen. W obrębie lasu każda domena automatycznie uznaje mechanizmy uwierzytelniania stosowane przez inne domeny, co pozwala na tworzenie jednolitych

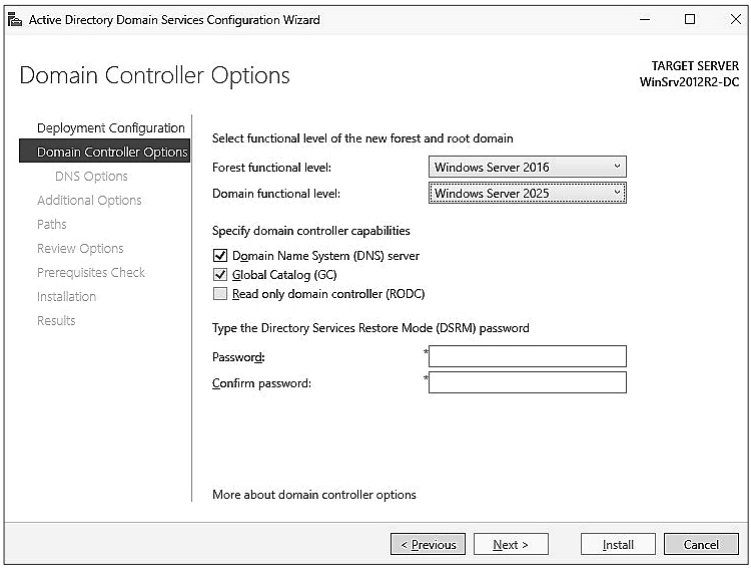
i spójnych ram bezpieczeństwa. Na przykład, jak pokazano na rysunku 4.6, jeżeli domena `Dautti.local` przeprowadzi pomyślne uwierzytelnienie użytkownika, to wynik tego procesu jest domyślnie akceptowany przez inną domenę w tym samym lesie, taką jak `Training.local`. Mechanizm ten opiera się na wspólnej infrastrukturze lasu, w której domeny — takie jak `Dautti.local` — stanowią integralne elementy połączonej i zaufanej sieci.

Zrozumienie mechanizmu działania relacji zaufania stanowi fundament dla analizy szerszych struktur administracyjnych i komunikacyjnych, które wspierają bezpieczne i wydajne działanie środowiska Active Directory. Relacje zaufania odgrywają kluczową rolę w umożliwieniu użytkownikom dostępu do zasobów zlokalizowanych w różnych domenach bez konieczności każdorazowego uwierzytelniania, co bardzo usprawnia współpracę między jednostkami organizacyjnymi oraz udostępnianie zasobów.

W następnym punkcie skupimy się na omówieniu poziomów funkcjonalnych domen i lasów, które określają możliwości i kompatybilność środowiska Active Directory. Przedstawimy również metody weryfikacji oraz konfiguracji poziomów funkcjonalnych, koncentrując się na aspektach wpływających na wydajność i poziom bezpieczeństwa środowiska sieciowego.

Poziomy funkcjonalne domen

Poziomy funkcjonalne domeny w Active Directory stanowią istotny komponent określający zakres dostępnych funkcji, kompatybilność wersji oraz ogólne zachowanie środowiska usług katalogowych. Umożliwiają precyzyjne wskazanie funkcjonalności, które mogą być wykorzystywane w danym środowisku, a także gwarantują, że wszystkie kontrolery domeny pracują na zgodnych wersjach systemu Windows Server. Wyróżniamy dwa podstawowe poziomy funkcjonalne domen, których zrozumienie jest niezbędne do prawidłowego zarządzania infrastrukturą (zobacz rysunek 4.9):



Rysunek 4.9. Poziomy funkcjonalne domen w opcjach kontrolera domeny Windows Server 2025

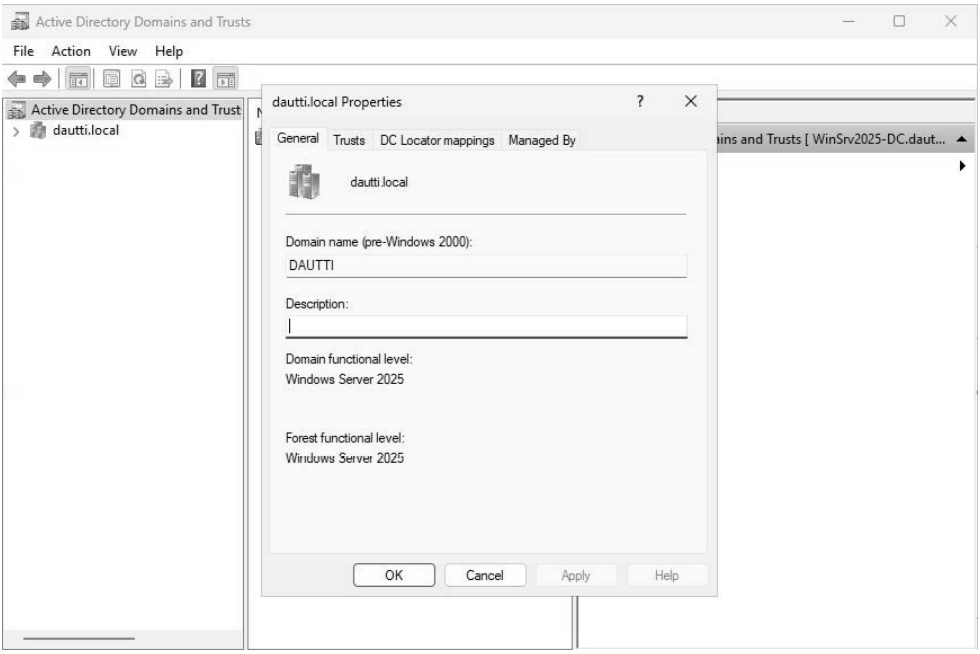
- **Poziom funkcjonalny lasu** (ang. *Forest Functional Level* — FFL) — odgrywa kluczową rolę w określaniu, które wersje systemu Windows Server mogą działać na kontrolerach domeny w obrębie całego lasu, czyli najwyższej struktury w Active Directory, obejmującej jedną lub wiele domen. Ustawienie poziomu FFL pozwala nie tylko ustawić minimalną dopuszczalną wersję systemu operacyjnego serwera, ale również aktywować określone funkcje dostępne na poziomie całego lasu, które zwiększają poziom bezpieczeństwa, usprawniają procesy replikacji oraz rozszerzają możliwości zarządzania we wszystkich domenach należących do danego lasu. Na przykład niektóre zaawansowane mechanizmy, takie jak kosz Active Directory czy szczegółowe zasady dotyczące haseł, są dostępne tylko na wyższych poziomach funkcjonalnych domeny.
- **Poziom funkcjonalny domeny** (ang. *Domain Functional Level* — DFL) — odnosi się do poszczególnych domen w obrębie lasu. Określa, które wersje systemu Windows Server są obsługiwane na kontrolerach domeny w danej domenie, oraz umożliwia korzystanie z funkcji przeznaczonych dla tej domeny. Podniesienie poziomu DFL pozwala na odblokowanie ulepszeń w zakresie funkcjonalności specyficznych dla domeny, takich jak zaawansowane mechanizmy uwierzytelniania, rozszerzone możliwości zarządzania zasadami grup oraz efektywniejsze metody replikacji. Taki poziom kontroli pozwala administratorom na stopniową modernizację części infrastruktury Active Directory bez konieczności natychmiastowej zmiany konfiguracji całego lasu, co zapewnia większą elastyczność w procesie aktualizacji.

W środowisku Windows Server 2025 minimalne poziomy funkcjonalne lasu (FFL) i domeny (DFL) można ustawić na system Windows Server 2016. Takie ograniczenie zapewnia, że las pozostanie kompatybilny z nowoczesnymi funkcjami, zarazem umożliwiając pewną wsteczną kompatybilność ze starszymi wersjami systemu. Zarówno FFL, jak i DFL można podnieść do poziomu systemu Windows Server 2025, co pozwala na pełne wykorzystanie najnowszych funkcji oraz optymalizacji oferowanych w najnowszej technologii serwerowej. Należy przy tym pamiętać, że po podniesieniu poziomu funkcjonalnego nie można go już obniżyć. Z tego względu trzeba starannie zaplanować proces aktualizacji, tak aby uniknąć problemów z kompatybilnością w przypadku środowisk, w których nadal wykorzystywane są starsze wersje systemu.

Weryfikowanie poziomów DFL i FFL oraz zarządzanie nimi

Aby zweryfikować poziomy funkcjonalne lasu (FFL) i domeny (DFL) oraz zarządzać nimi w systemie Windows Server 2025, powinieneś wykonać następujące czynności:

1. Naciśnij przycisk *Start*, a następnie z menu wybierz polecenie *Server Manager*.
2. W oknie menedżera serwera kliknij polecenie *Tools*, znajdujące się na pasku menu, a następnie wybierz opcję *Active Directory Domains and Trusts*.
3. W oknie *Active Directory Domains and Trusts* kliknij prawym przyciskiem myszy domenę główną i z menu podręcznego wybierz polecenie *Properties*.
4. W oknie dialogowym *Properties*, na karcie *General*, znajdziesz informacje o bieżących poziomach funkcjonalnych domeny i lasu, jak pokazano na rysunku 4.10.



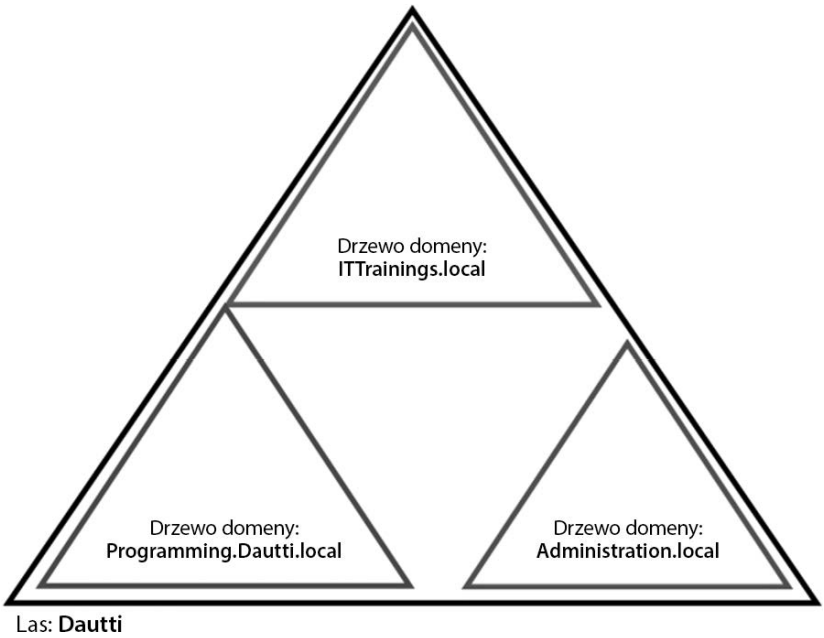
Rysunek 4.10. Weryfikowanie poziomów funkcjonalnych domeny i lasu

Zrozumienie poziomów funkcjonalnych lasu (FFL) i domeny (DFL) oraz właściwe zarządzanie nimi ma kluczowe znaczenie w zapewnieniu stabilnego, bezpiecznego i wydajnego działania środowiska Active Directory, z pełnym dostępem do wszystkich funkcji niezbędnych do realizacji potrzeb organizacji. Poziomy funkcjonalne odgrywają również istotną rolę w projektowaniu architektury oraz strategii wdrażania Active Directory, ponieważ umożliwiają elastyczne skalowanie i dostosowywanie infrastruktury do zmieniających się wymagań operacyjnych.

Znajomość wpływu poziomów funkcjonalnych na środowisko Active Directory otwiera drogę do zgłębienia koncepcji ciągłej przestrzeni nazw. Jest ona niezbędna do utrzymania logicznego i płynnego połączenia między domenami podrzędnymi a ich domenami nadrzędnymi w obrębie jednej struktury drzewa i zapewnia możliwość efektywnego i uporządkowanego zarządzania hierarchią AD.

Koncepcja przestrzeni nazw AD DS

W usłudze Active Directory Domain Services (AD DS) koncepcja przestrzeni nazw jest fundamentalna dla organizacji oraz zarządzania domenami i lasami w środowisku sieciowym. Przestrzeń odgrywa rolę logicznego identyfikatora, który jednoznacznie określa domenę lub las, zapewniając przejrzystą i uporządkowaną strukturę środowiska AD DS. Na przykład na rysunku 4.11 domena `Dautti.local` pełni funkcję zarówno domeny głównej, jak i nadrzędnego lasu. W ramach tego lasu domeny `ITTrainings.local` oraz `Administration.local` tworzą odrębne drzewa domen, reprezentujące niezależne



Rysunek 4.11. Koncepcja przestrzeni nazw w AD DS.

gałęzie w tej samej hierarchicznej strukturze. Dodatkowo w drzewie domeny `Dautti.local` znajduje się domena podrzędna o nazwie `Programming.Dautti.local`. Wspólny komponent `Dautti.local` występujący w nazwach tych domen wskazuje na ciągłość przestrzeni nazw, co oznacza, że wszystkie domeny w tym lesie są logicznie powiązane poprzez wspólną konwencję nazewnictwa.

Ciągła przestrzeń nazw jest kluczowa w utrzymaniu spójnej i zorganizowanej struktury Active Directory Domain Services (AD DS). Zapewnia ona logiczne powiązanie wszystkich domen w obrębie lasu, co znacząco ułatwia zarządzanie oraz nawigację w środowisku sieciowym. Wspólna konwencja nazewnictwa nie tylko upraszcza identyfikowanie domen i zarządzanie nimi, ale także odzwierciedla hierarchiczną naturę środowiska AD DS, w której każda domena stanowi integralny element większego, wzajemnie powiązanego systemu.

Aby lepiej zrozumieć koncepcję przestrzeni nazw, warto posłużyć się analogią do systemu **Uniform Resource Locator** (**URL**), stosowanego w internecie. Podobnie jak URL jednoznacznie identyfikuje i lokalizuje na serwerze konkretną stronę internetową, tak przestrzeń nazw w AD DS jednoznacznie identyfikuje i organizuje domeny w obrębie lasu. Taka logiczna struktura pozwala administratorom na efektywne zarządzanie zasobami oraz wdrażanie polityki bezpieczeństwa i utrzymywanie go na wysokim poziomie w całym środowisku sieciowym.

Zrozumienie roli przestrzeni nazw jest niezbędne do efektywnego zarządzania środowiskiem Active Directory Domain Services, ponieważ bezpośrednio wpływa na to, jak domeny są strukturyzowane, nazywane i powiązane ze sobą w obrębie lasu. Posiadając klarowną wiedzę na temat przestrzeni nazw, administratorzy mogą tworzyć dobrze

zorganizowane i łatwe do nawigowania środowisko AD DS. W następnym punkcie omówimy koncepcję lokacji w domenie, które reprezentują fizyczne lub logiczne lokalizacje w sieci. Jest to element infrastruktury AD DS o kluczowym znaczeniu w optymalizowaniu ruchu sieciowego oraz procesów replikacji.

Lokacje w Active Directory

Oprócz struktury logicznej Active Directory wykorzystuje również strukturę fizyczną odzwierciedlającą geograficzny lub organizacyjny układ sieci, znaną jako **lokacje** (ang. *sites*). Lokacja reprezentuje konkretną fizyczną lokalizację w infrastrukturze sieciowej organizacji i może obejmować pojedynczą domenę lub większą liczbę domen połączonych szybkimi łączami transmisji danych. Definiowanie lokacji w Active Directory ma na celu optymalizację ruchu sieciowego oraz poprawę ogólnej wydajności środowiska, szczególnie przez bardziej efektywne zarządzanie replikacją danych i ruchem związanym z uwierzytelnianiem pomiędzy różnymi lokacjami.

Lokacje odgrywają kluczową rolę w ograniczaniu zbędnego ruchu sieciowego, szczególnie w **sieciach rozległych** (**WAN**), gdzie przepustowość może być ograniczona lub może generować wysokie koszty. Dzięki temu, że ruch związany z replikacją — wykorzystywany do synchronizacji danych katalogowych między kontrolerami domeny — jest kierowany przez szybkie, lokalne łącza sieciowe, Active Directory pozwala na utrzymanie spójności danych bez przeciążania wolniejszych połączeń sieciowych. Jest to szczególnie ważne w dużych, rozproszonych środowiskach, gdzie kontrolery domeny mogą być rozmieszczone w wielu miastach, regionach, a nawet krajach.

Co więcej, lokacje w AD nie tylko służą do zwiększania efektywności replikacji, ale także odgrywają kluczową rolę w procesach uwierzytelniania. Podczas logowania się użytkownika usługa AD kieruje żądanie uwierzytelnienia do kontrolera domeny znajdującego się w tej samej witrynie, co użytkownik. Takie rozwiązanie przyspiesza proces uwierzytelniania oraz zmniejsza obciążenie zdalnych serwerów. Lokalizacja działań związanych z uwierzytelnianiem i replikacją znacząco zwiększa komfort pracy użytkownika oraz niezawodność świadczonych usług sieciowych.

Znajomość zasad działania lokacji Active Directory oraz ich wpływu na replikację jest kluczowa dla administratorów odpowiedzialnych za projektowanie infrastruktury AD lub zarządzanie nią. Odpowiednio zaprojektowane lokacje umożliwiają efektywne wykorzystanie zasobów sieciowych, minimalizują opóźnienia odczuwane przez użytkowników oraz zapewniają odporność i stabilność działania środowiska sieciowego nawet podczas jego dynamicznego skalowania. Zanim przejdziemy do szczegółowego omówienia mechanizmów działania replikacji w AD, które odpowiadają za utrzymanie spójności danych w domenach, warto zrozumieć, w jaki sposób lokacje wpływają na niezawodność i wydajność środowiska AD, szczególnie w rozbudowanych i złożonych strukturach sieciowych.

Replikacja w AD

Replikacja w Active Directory (AD) jest jedną z podstawowych funkcji zapewniających spójność oraz integralność danych dla wszystkich kontrolerów domeny w obrębie lasu. Proces ten odgrywa kluczową rolę w utrzymaniu aktualnej i zsynchronizowanej usługi katalogowej, dzięki czemu wszelkie modyfikacje — dotyczące kont użytkowników, polityk bezpieczeństwa czy ustawień konfiguracyjnych — są natychmiast odzwierciedlane w całej sieci kontrolerów domeny. Mechanizm replikacji działa w sposób ciągły, przekazując zmiany pomiędzy serwerami i zapobiegając powstawaniu potencjalnych konfliktów lub niespójności, które mogłyby wystąpić, gdyby różne fragmenty środowiska sieciowego przechowywały rozbieżne wersje danych katalogowych.

Efektywność replikacji jest zarządzana przez topologię replikacji — czyli logiczną sieć tras, którymi replikowane dane przemieszczają się między kontrolerami domeny. Ta topologia nie jest tworzona przypadkowo; jest starannie generowana i optymalizowana przez **proces KCC** (ang. *Knowledge Consistency Checker*), który automatycznie analizuje strukturę i dynamikę sieci. Na podstawie tej analizy KCC generuje zoptymalizowaną ścieżkę replikacji, która wyważa szybkość propagacji danych i rozkład obciążenia między serwerami, dzięki czemu aktualizacje katalogu są rozpowszechniane sprawnie i bez nadmiernego obciążania zasobów sieciowych. Ten zautomatyzowany proces jest szczególnie istotny w dużych, rozproszonych środowiskach Active Directory, gdzie ręczne zarządzanie replikacją byłoby niepraktyczne, nieefektywne i podatne na błędy.

Dodatkowo AD obsługuje replikację zarówno wewnątrz, jak i między lokacjami. Replikacja wewnątrz lokacji (ang. *intra-site replication*) odbywa się w obrębie tej samej lokacji, zazwyczaj z użyciem szybkich połączeń sieciowych, i jest realizowana z dużą częstotliwością, co zapewnia synchronizację danych niemal w czasie rzeczywistym. Z kolei replikacja między lokacjami (ang. *inter-site replication*) zachodzi pomiędzy różnymi lokacjami i odbywa się rzadziej. Jest ona zoptymalizowana pod kątem minimalizacji wpływu na przepustowość, szczególnie w przypadku wolniejszych lub droższych łączy WAN. Administratorzy mają możliwość konfigurowania harmonogramów replikacji między lokacjami oraz ustawienia kompresji danych, co pozwala efektywnie zarządzać tym procesem, wyważając potrzebę posiadania aktualnych danych i ograniczenia zasobów sieciowych.

Zrozumienie replikacji w Active Directory to nie tylko znajomość mechanizmów synchronizacji danych, lecz także świadomość jej kluczowego znaczenia dla utrzymania stabilności i wydajności całego środowiska AD. W razie awarii lub błędnego skonfigurowania replikacji mogą wystąpić poważne konsekwencje — od nieaktualnych lub sprzecznych informacji w kontrolerach po problemy z uwierzytelnianiem użytkowników czy nieprawidłowe stosowanie polityk i zasad grupy.

Po opanowaniu zagadnień związanych z replikacją kolejnym istotnym krokiem w zarządzaniu Active Directory jest zrozumienie schematu AD — kompleksowego planu określającego strukturę wszystkich obiektów i atrybutów w katalogu. Schemat ma fundamentalne znaczenie dla sposobu, w jaki AD organizuje i przechowuje dane. Określa, jakie typy obiektów (np. użytkownicy, grupy czy komputery) mogą istnieć w katalogu oraz jakie atrybuty mogą mieć. Znajomość schematu pozwala administratorom na rozszerzanie lub modyfikowanie katalogu w sposób zgodny z przyjętymi standardami tak, aby sprostać specyficznym wymaganiom organizacji, a zarazem zapewnić kompatybilność i stabilność całej infrastruktury AD.

Schemat AD

Schemat (ang. *schema*) w Active Directory jest kluczowym elementem, który stanowi podstawę organizowania danych w ramach usługi katalogowej i zarządzania nimi. Pełni funkcję ustrukturyzowanego modelu, który określa sposób przechowywania, organizowania i udostępniania informacji w całej infrastrukturze AD. Schemat składa się z trzech głównych elementów:

- **Obiekty** (ang. *objects*) — Obiekty stanowią odrębne jednostki w katalogu, takie jak użytkownicy, komputery, drukarki czy grupy zabezpieczeń, które reprezentują rzeczywiste zasoby lub funkcje w środowisku sieciowym.
- **Klasy** (ang. *classes*) — Obiekty są przypisane do konkretnych klas, które określają typ obiektu i ramy tego, co może reprezentować w katalogu. Na przykład obiekt użytkownika może należeć do klasy `User`, która określa konkretny zestaw atrybutów, takich jak nazwa użytkownika, hasło, adres e-mail czy dział.
- **Atrybuty** (ang. *attributes*) — Są to właściwości lub cechy przypisane do obiektów, zawierające szczegółowe informacje na ich temat. W przypadku obiektu `user` mogą to być między innymi pełne imię i nazwisko, stanowisko, numer telefonu oraz dane logowania.

Schemat nie tylko określa, jakie obiekty i atrybuty są dostępne w Active Directory, ale także ustala zasady ich tworzenia, modyfikowania oraz zarządzania nimi w środowisku AD. Zapewnia to utrzymanie integralności i spójności danych w całej infrastrukturze sieciowej. Wszelkie zmiany w schemacie podlegają ścisłej kontroli i są replikowane w obrębie całej sieci. Takie podejście gwarantuje synchronizację wszystkich kontrolerów domeny w ramach lasu, co pozwala utrzymać jednolitą strukturę, a także sprawnie zarządzać danymi katalogowymi w różnych domenach i lokacjach oraz efektywnie je wyszukiwać. Zrozumienie tego procesu jest niezbędne do zapewnienia stabilności i niezawodności środowiska sieciowego.

W następnym punkcie omówimy Microsoft Passport, nowoczesną metodę uwierzytelniania, która podnosi poziom bezpieczeństwa, gdyż pozwala użytkownikom na logowanie bez użycia tradycyjnych haseł. Zamiast nich stosowane są bezpieczniejsze opcje, takie jak uwierzytelnianie biometryczne czy kod PIN. Takie rozwiązanie nie tylko wzmacnia bezpieczeństwo, ale także jest wygodne dla użytkownika, ponieważ upraszcza i przyspiesza proces logowania.

Microsoft Passport

W dzisiejszym środowisku cyfrowym zarządzanie rosnącą liczbą haseł do różnych aplikacji, serwisów internetowych oraz usług stanowi znaczące wyzwanie. Tradycyjny model uwierzytelniania oparty na hasłach jest nie tylko niewygodny, ale także podatny na liczne zagrożenia bezpieczeństwa, ponieważ hasła można łatwo zapomnieć, odgadnąć, przechwycić lub wyłudzić w wyniku ataków phishingowych. W odpowiedzi na te problemy firma Microsoft opracowała rozwiązanie o nazwie **Microsoft Passport**, które jest obecnie zintegrowane z usługą Windows Hello for Business. Ten nowoczesny system uwierzytelniania bez użycia haseł zaprojektowano z myślą zarówno o bezpieczeństwie, jak i wygodzie użytkownika.

Microsoft Passport wykorzystuje standard **Fast ID Online** (**FIDO**) **Alliance**, powszechnie uznany framework służący do bezpiecznego uwierzytelniania bez użycia hasła. System działa w modelu uwierzytelniania dwuskładnikowego, który integruje usługę pojedynczego logowania z funkcjonalnością cyfrowego portfela. W praktyce oznacza to, że zamiast polegać na haśle, użytkownik potwierdza swoją tożsamość za pomocą elementu, który posiada — na przykład zaufanego urządzenia (takiego jak smartfon lub klucz bezpieczeństwa) — oraz czegoś, co jest dla niego unikalne, jak dane biometryczne (odcisk palca czy rysy twarzy) lub bezpieczny PIN. Połączenie tych dwóch elementów gwarantuje, że nawet w razie złamania jednego z nich drugi pozostaje bezpieczny, co znacząco ogranicza ryzyko nieuprawnionego dostępu.

Przyjęcie uwierzytelniania bez użycia hasła w ramach Windows Hello for Business pozwala organizacjom zwiększyć poziom bezpieczeństwa, a zarazem uprościć obsługę z punktu widzenia użytkownika. Rezygnacja z tradycyjnych haseł zmniejsza ryzyko incydentów związanych z bezpieczeństwem, ponieważ hasła są często podatne na zapomnienie, odgadnięcie lub kradzież, szczególnie gdy nie są wspierane przez **uwierzytelnianie wieloskładnikowe** (ang. *multi-factor authentication* — MFA). Użytkownicy nie muszą już zapamiętywać złożonych haseł ani zarządzać wieloma zestawami poświadczeń, co w oczywisty sposób przekłada się na zmniejszenie liczby incydentów związanych z hasłami i spadek liczby zgłoszeń do działu pomocy technicznej. Takie podejście wpisuje się w szerszy trend branżowy, promujący bardziej bezpieczne i przyjazne dla użytkownika metody uwierzytelniania. Przez wdrażanie rozwiązań zapewniających uwierzytelnianie bez użycia hasła organizacje mogą skutecznie ograniczyć luki związane z zarządzaniem hasłami i zbudować solidniejsze fundamenty bezpieczeństwa, obejmujące rozwiązania wieloskładnikowe i technologie biometryczne.

W tym punkcie omówiliśmy kluczowe komponenty infrastruktury Active Directory, takie jak domeny, lasy, drzewa, lokacje, schematy oraz przestrzenie nazw. Przedstawiliśmy również sposób konfigurowania i weryfikowania poziomów funkcjonalności domeny i lasu w środowisku Windows Server 2025. Zrozumienie tych elementów jest niezbędne dla każdego, kto zarządza środowiskiem AD. W następnym punkcie przyjrzymy się systemowi DNS i jego kluczowej roli w funkcjonowaniu Active Directory i zarządzaniu nim — temu, jak zapewnia sprawne rozwiązywanie nazw i działanie usług katalogowych w całym środowisku sieciowym.

Podstawy działania i konfiguracja DNS w Windows Server 2025

System DNS wywodzi się z projektu ARPANET z lat 60. XX wieku. Odpowiadał na potrzebę stworzenia bardziej przyjaznego dla użytkownika sposobu identyfikowania urządzeń sieciowych, wykraczającego poza numeryczne adresy IP. Koncepcja ta na początku lat 80. ewoluowała do znanego nam obecnie systemu DNS, wraz z publikacją podstawowych specyfikacji technicznych w **dokumentach RFC** (ang. *Request for Comments*). DNS ma strukturę hierarchiczną przypominającą drzewo, gdzie strefa główna rozgałęzia się na odpowiednie domeny i poddomeny, zawierające rekordy zasobów z kluczowymi informacjami o zasobach sieciowych. Nazwa domeny składa się z wielu

segmentów zwanych etykietami, oddzielonych kropkami — na przykład *packtpub.com*. System ten opiera się na rozproszonej bazie danych wykorzystującej architekturę klient-serwer, w której hosty sieciowe pełnią funkcję serwerów nazw. Serwery te tłumaczą nazwy domen na odpowiadające im adresy IP, co zapewnia płynną nawigację i sprawną komunikację w internecie. Takie hierarchiczne i rozproszone podejście zwiększa skalowalność, wydajność i niezawodność w zarządzaniu nazwami domen i zasobami sieciowymi.

Podstawy działania systemu DNS

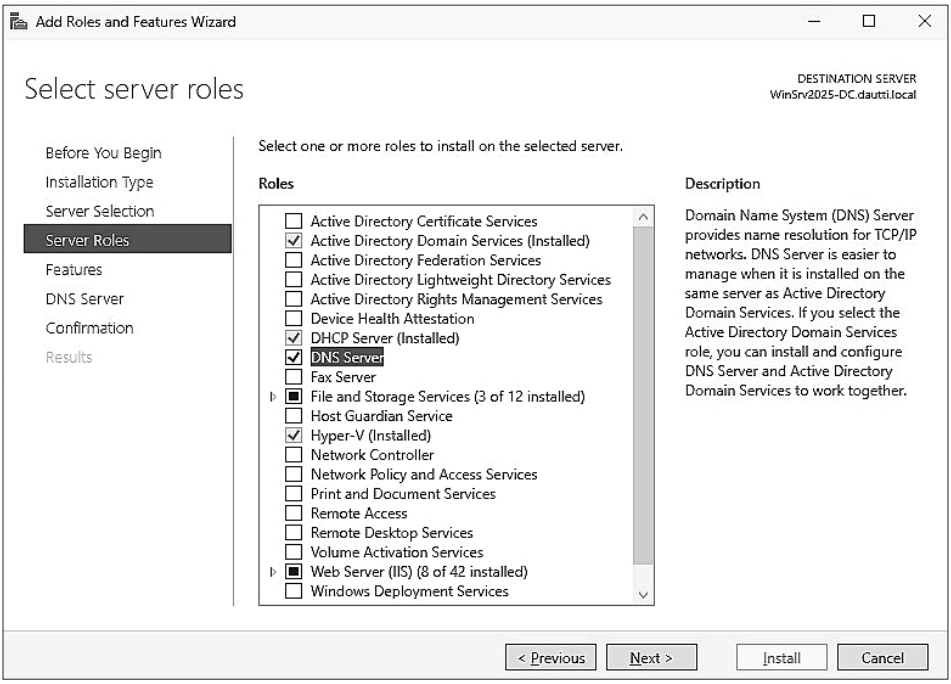
Aby w pełni zrozumieć, jak działa system DNS, warto przeanalizować sekwencję działań, które mają miejsce podczas próby dostępu do wybranej strony internetowej. DNS odgrywa kluczową rolę w tłumaczeniu nazw domen zrozumiałych dla człowieka na adresy IP interpretowane przez komputery, co umożliwia komunikację pomiędzy użytkownikami a witryną internetową. Poniżej opisano, jak przebiega proces rozwiązywania nazw DNS, czyli w jaki sposób przeglądarka ustala odpowiedni adres IP, z którym należy się połączyć po wpisaniu adresu internetowego, na przykład *www.packtpub.com*:

1. **Wprowadzanie adresu URL:** po wpisaniu adresu *www.packtpub.com* w pasku adresu przeglądarki sieciowej i naciśnięciu klawisza *Enter* przeglądarka wysyła żądanie połączenia z tą domeną.
2. **Rekursywny serwer DNS:** żądanie trafia najpierw do kluczowego komponentu infrastruktury DNS, czyli **rekursywnego serwera DNS** (ang. *recursive resolver*). Zazwyczaj jest on zarządzany przez dostawcę usług internetowych (ang. *Internet Service Provider* — ISP) i odpowiada za obsługę zapytań DNS w imieniu użytkownika.
3. **Serwery główne:** rekursywny serwer DNS kontaktuje się następnie z **globalnymi serwerami głównymi DNS** (ang. *global root servers*), które przechowują informacje o **domenach najwyższego poziomu** (ang. *top-level domains* — TLD), takich jak domeny z rozszerzeniem *.com*. Choć serwery główne DNS nie mają pełnych danych DNS, kierują serwer rekursywny do odpowiednich serwerów TLD.
4. **Serwery TLD:** serwery domen najwyższego poziomu (TLD) odpowiadają na zapytanie przez dostarczenie informacji umożliwiających serwerowi rekursywnemu dotarcie do autorytatywnych serwerów nazw dla konkretnej domeny, takiej jak *packtpub.com*.
5. **Autorytatywne serwery nazw:** serwer rekursywny wysyła zapytanie do autorytatywnych serwerów nazw, aby uzyskać dokładny adres IP przypisany do domeny *packtpub.com*. Serwery autorytatywne przechowują właściwe rekordy DNS, które odwzorowują nazwy domen na odpowiadające im adresy IP.
6. **Zwracanie adresu IP:** po uzyskaniu adresu IP serwera WWW hostującego domenę *packtpub.com* serwer rekursywny przekazuje tę informację z powrotem do przeglądarki.
7. **Łączenie z serwerem WWW:** dysponując adresem IP, przeglądarka nawiązuje połączenie z odpowiednim serwerem WWW i pobiera zawartość strony do wyświetlenia.

Ten proces krok po kroku ilustruje złożony mechanizm działania DNS, podkreślając jego kluczową rolę w przekształcaniu nazw domen na odpowiadające im adresy IP, co umożliwia płynną komunikację w internecie. Zrozumienie tego procesu unaocznia znaczenie poprawnej konfiguracji roli DNS w infrastrukturze sieciowej. Właściwie skonfigurowany system DNS zapewnia efektywne rozwiązywanie nazw domen, co jest kluczowe zarówno w sprawnym funkcjonowaniu wewnętrznych procesów sieciowych, jak i zapewnieniu niezawodnego dostępu do zasobów internetowych.

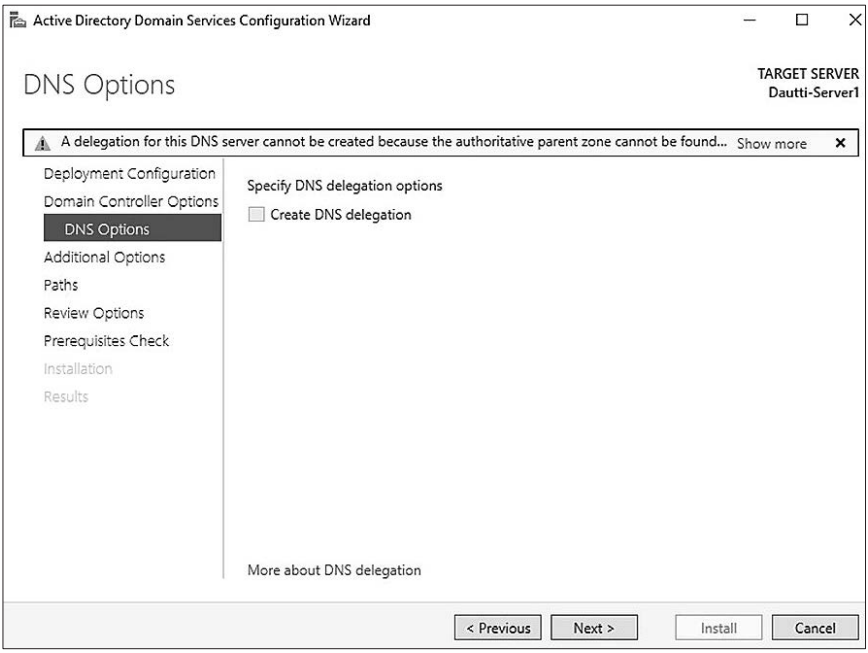
Instalowanie roli DNS

W systemie Windows Server 2025 rola DNS jest kluczowa. Umożliwia serwerowi tłumaczenie nazw domen na odpowiadające im adresy IP, co zapewnia płynną komunikację sieciową oraz dostęp do zasobów. Rolę tę można skonfigurować za pomocą narzędzia **Server Manager**, które udostępnia prosty interfejs do zarządzania rolami i funkcjami serwera. Jak pokazano na rysunku 4.12, proces konfiguracji rozpoczyna się od uruchomienia aplikacji Server Manager oraz wybrania opcji dodawania ról i funkcji.



Rysunek 4.12. Instalowanie roli DNS

Rolę DNS można zainstalować jako niezależną usługę lub w połączeniu z usługą AD DS. Gdy jest zainstalowana samodzielnie, działa autonomicznie i obsługuje rozwiązywanie nazw domen. Integracja DNS z AD DS, jak przedstawiono na rysunku 4.13, rozszerza funkcjonalność sieci: umożliwia serwerowi DNS realizowanie operacji związanych z Active Directory, takich jak lokalizowanie kontrolerów domeny czy wyszukiwanie rekordów usług. Takie połączenie jest szczególnie korzystne w środowiskach o dużej skali, gdzie współpraca AD i DNS znacząco usprawnia działanie infrastruktury sieciowej.



Rysunek 4.13. Instalowanie roli DNS wraz z usługą AD DS

Warto zauważyć, że rolę DNS często uwzględnia się w procesie instalacji AD DS, co zapewnia spójną konfigurację wspierającą rozwiązywanie nazw domen w środowisku Active Directory. Takie zintegrowane podejście gwarantuje, że usługi DNS są odpowiednio skonfigurowane do obsługi wymagań AD, w tym automatycznego tworzenia niezbędnych rekordów DNS.

Po pomyślnym zainstalowaniu i skonfigurowaniu roli DNS będziesz dobrze przygotowany do zarządzania rozwiązywaniem nazw domen oraz zwiększania funkcjonalności sieci. Następnym krokiem jest zrozumienie, w jaki sposób pliki *hosts* i *lmhosts* (ang. *LAN Manager hosts*) wspierają lokalne rozwiązywanie nazw, jako uzupełnienie roli DNS w konfiguracji sieci.

Rola plików hosts i lmhosts

W każdym środowisku sieciowym skuteczne odwzorowywanie nazw odgrywa kluczową rolę w zapewnieniu płynnej komunikacji między urządzeniami. Pliki *hosts* i *lmhosts* pełnią istotną funkcję w tym procesie. Zazwyczaj znajdują się w katalogu *C:\Windows\system32\drivers\etc* i zapewniają prosty, ale bardzo skuteczny mechanizm rozwiązywania nazw sieciowych, nawet w razie braku oddzielnych usług odwzorowywania nazw:

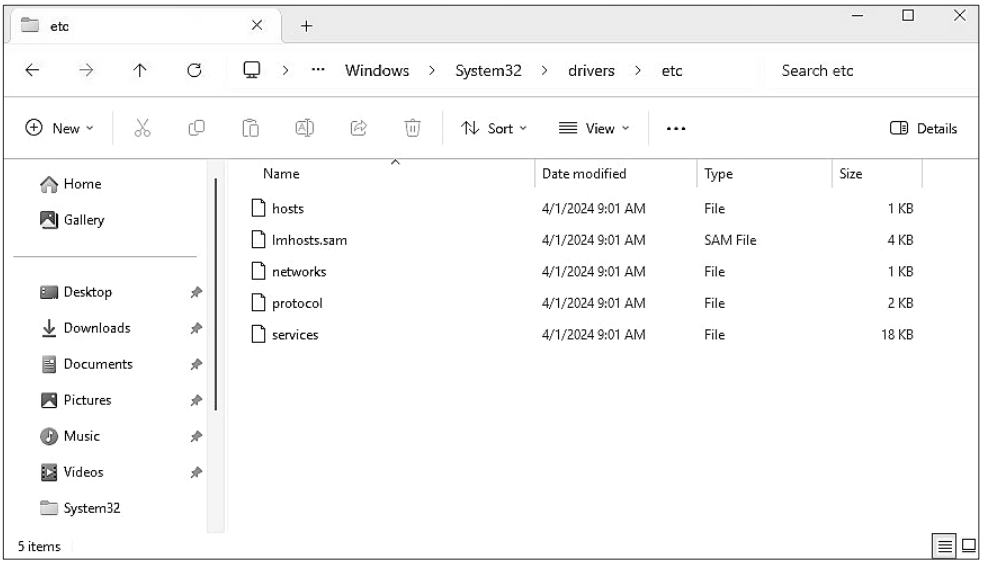
- **Plik *hosts:*** ten plik działa jako statyczne i konfigurowalne narzędzie mapowania, które umożliwia przypisywanie konkretnych adresów IP do nazw hostów. Dzięki temu możliwe staje się lokalne rozwiązywanie nazw DNS, co pozwala identyfikować urządzenia w sieci za pomocą przyjaznych dla użytkownika

nazw zamiast numerycznych adresów IP. Jest to szczególnie korzystne w środowiskach, gdzie usługi DNS mogą być niedostępne lub zawodne, lub gdy konieczne jest ręczne nadpisywanie wpisów, na przykład w celach testowych i administracyjnych. Przez edycję pliku *hosts* administratorzy mogą kontrolować sposób rozwiązywania nazw w sieci lokalnej, by zapewnić, że krytyczne systemy zawsze będą dostępne pod przypisanymi im nazwami.

- **Plik *lmhosts:*** służy do mapowania adresów IP na nazwy komputerów **NetBIOS**. Choć jego znaczenie w nowoczesnych sieciach jest mniejsze, nadal może być przydatny w określonych scenariuszach, szczególnie w starszych środowiskach, które do rozwiązywania nazw wykorzystują protokół NetBIOS. Plik ten umożliwia lokalne rozwiązywanie nazw NetBIOS nawet wtedy, gdy **serwer WINS** (ang. *Windows Internet Name Service*) jest niedostępny. Jednak ze względu na rosnące znaczenie DNS jako głównej metody rozwiązywania nazw w systemie Windows Server 2025 oraz stopniowe wycofywanie WINS praktyczne zastosowanie pliku *lmhosts* w większości współczesnych środowisk jest już mocno ograniczone.

Zarówno plik *hosts*, jak i *lmhosts* wymagają ręcznego wprowadzania wpisów, przy czym każde mapowanie powinno być zapisywane w osobnym wierszu dla zachowania przejrzystości i uporządkowania danych. Taka ręczna konfiguracja zapewnia administratorom sieci lepszą kontrolę nad rozwiązywaniem nazw, a tym samym umożliwia prawidłowe i efektywne kierowanie ruchem sieciowym.

Na rysunku 4.14 przedstawiono lokalizację plików *hosts* i *lmhosts* w środowisku Windows Server 2025, która podkreśla ich znaczenie w kontekście konfiguracji sieci.

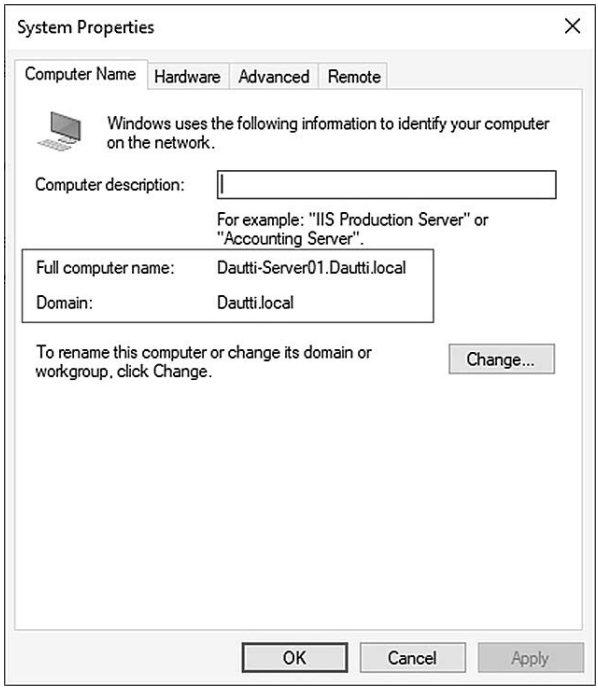


Rysunek 4.14. Pliki hosts i lmhosts w systemie Windows Server 2025

Warto zauważyć, że koncepcja nazwy hosta, pełniącej funkcję identyfikatora danego komputera w sieci lokalnej, ma kluczowe znaczenie dla rozpoznawania urządzeń w obrębie sieci. Zrozumienie tego pojęcia, omówionego wcześniej w tym rozdziale, jest niezbędne do zrozumienia mechanizmów identyfikowania urządzeń w środowisku sieciowym oraz komunikacji między nimi. Dzięki efektywnemu zarządzaniu plikami *hosts* i *lmhosts* administratorzy mogą zapewnić spójne i niezawodne rozwiązywanie nazw, co jest niezmiernie ważne dla sprawnego działania usług sieciowych i aplikacji.

Nazwy hostów i ich rola w sieci

Znajomość nazw hostów to podstawowa umiejętność każdego specjalisty IT odpowiedzialnego za sprawne funkcjonowanie sieci. Nazwy hostów są kluczowym elementem identyfikacji urządzeń i komunikacji w sieci, jak pokazano na rysunku 4.15. Nazwa hosta to logiczna etykieta przypisana do konkretnego urządzenia, pozwalająca jednoznacznie je zidentyfikować w środowisku sieciowym i umożliwiająca bezproblemową interakcję, szczególnie w **ramach sieci lokalnej** (**LAN**). Ten identyfikator jest bardzo ważny nie tylko dla operacji w sieci lokalnej, ale również w szerszej komunikacji sieciowej, ponieważ często pełni funkcję nazwy domenowej. Stosowanie przejrzystych i jednoznacznych nazw hostów znacząco ułatwia zarządzanie zasobami sieciowymi i rozwiązywanie problemów technicznych oraz gwarantuje, że każde urządzenie pozostaje łatwo rozpoznawalne i dostępne.



Rysunek 4.15. Nadawanie nazwy hosta w systemie Windows Server 2025

Przypisywanie nazw hostów to kluczowy etap konfiguracji urządzeń sieciowych, szczególnie w środowiskach takich jak Windows Server 2025, gdzie poprawna identyfikacja serwerów i innych urządzeń sieciowych jest niezbędna do utrzymania porządku i efektywności działania całej infrastruktury sieciowej. Dobrze dobrana nazwa hosta znacząco ułatwia zarządzanie siecią, ponieważ umożliwia administratorom sprawne lokalizowanie urządzeń w infrastrukturze sieciowej i zarządzanie nimi.

Oprócz świadomości znaczenia nazw hostów równie istotne jest zrozumienie koncepcji stref DNS, które pełnią funkcję segmentów administracyjnych w systemie DNS. Ich charakterystyka i zastosowanie są bardziej szczegółowo omówione w następnym punkcie.

Zasada działania i znaczenie stref DNS

Dobre zrozumienie koncepcji **stref DNS** (ang. *DNS zones*) ma nie tylko znaczenie teoretyczne, lecz przede wszystkim praktyczne. Taki poziom wiedzy jest niezbędny do skutecznego zarządzania infrastrukturą sieciową. Strefy DNS tworzą podstawę hierarchicznej struktury systemu DNS, która określa sposób rozwiązywania nazw domen w sieci. Są one integralną częścią przestrzeni nazw Active Directory, która jest ściśle powiązana z globalną przestrzenią nazw DNS oraz zapewnia uporządkowane i skalowalne podejście do zarządzania danymi domenowymi. Dzięki segmentacji stref DNS administratorzy mogą efektywniej przechowywać informacje o konkretnych domenach i sprawnie nimi zarządzać, co przekłada się na skuteczne rozwiązywanie nazw w środowisku sieciowym.

Istnieją trzy główne typy stref DNS, z których każda pełni odrębną funkcję:

- **Strefa podstawowa** (ang. *primary zone*) — stanowi autorytatywne źródło danych DNS dla danej domeny. Zawiera główną, edytowalną kopię bazy danych DNS i odpowiada za zarządzanie wszystkimi rekordami DNS w przypisanym zakresie. Pełni w procesie rozwiązywania nazw domen funkcję centralnego punktu odniesienia, który gwarantuje poprawne i spójne odpowiedzi na zapytania DNS.
- **Strefa pomocnicza** (ang. *secondary zone*) — funkcjonuje jako kopia zapasowa strefy podstawowej i przechowuje kopię rekordów DNS w trybie tylko do odczytu. Odgrywa istotną rolę w zapewnieniu redundancji, ponieważ umożliwia ciągłość rozwiązywania nazw DNS nawet po tym, jak strefa podstawowa stanie się niedostępna. Strefa pomocnicza jest synchronizowana ze strefą podstawową, co gwarantuje, że odzwierciedla najbardziej aktualne informacje DNS.
- **Strefa szkieletowa** (ang. *stub zone*) — stanowi wyspecjalizowany wariant strefy pomocniczej. W odróżnieniu od niej nie zawiera pełnej kopii bazy danych DNS, lecz jedynie kluczowe informacje — przede wszystkim adresy IP **autorytatywnych serwerów DNS** (ang. *authoritative DNS servers*) dla danej strefy — umożliwiające przekierowanie zapytań do odpowiedniego serwera autorytatywnego. Takie rozwiązanie upraszcza zarządzanie DNS oraz optymalizuje ruch sieciowy dzięki ograniczeniu konieczności pełnej replikacji danych DNS.

Rola serwerów DNS w zarządzaniu strefami jest kluczowa. Autorytatywny serwer DNS, który obsługuje rekordy DNS dla określonej domeny, odgrywa krytyczną rolę w tej strukturze. Może być konfigurowany ręcznie przez administratora systemu, co pozwala na precyzyjne zarządzanie wpisami DNS, lub dynamicznie, poprzez transfery i aktualizacje stref realizowane przez inne serwery DNS. Serwer autorytatywny stanowi ostateczne źródło odpowiedzi na zapytania DNS dla swojej domeny, gwarantując ich dokładność i aktualność. W odróżnieniu od niego **nieautorytatywny serwer DNS** (ang. *non-authoritative DNS server*) pracuje na danych przechowywanych w pamięci podręcznej, pochodzących z wcześniejszych zapytań DNS, i nie przechowuje oryginalnych rekordów DNS. Choć nieautorytatywne serwery DNS mogą dostarczać szybkich odpowiedzi na podstawie informacji z pamięci podręcznej, nie są one ostatecznym źródłem rozwiązywania nazw DNS. W przypadku niewłaściwego zarządzania pamięcią podręczną może to skutkować udzielaniem nieaktualnych lub niedokładnych odpowiedzi.

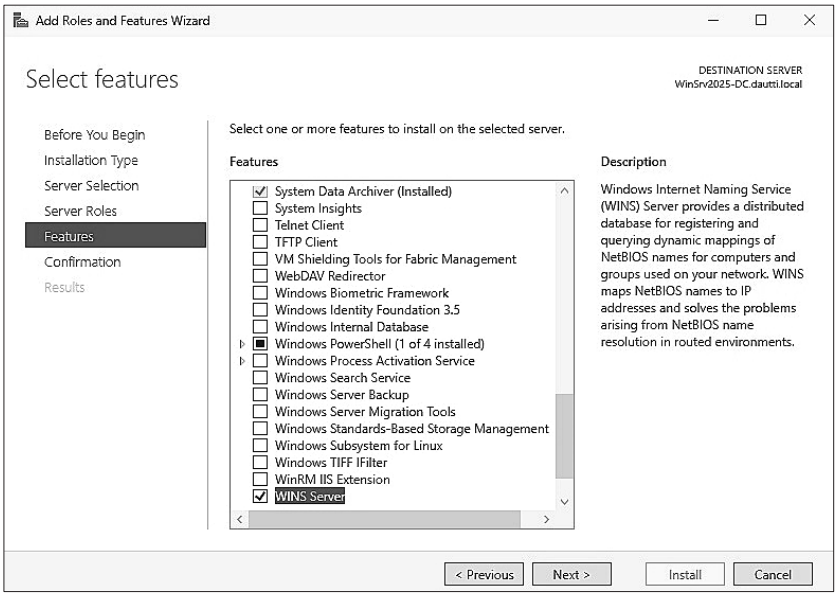
Oprócz skonfigurowania stref DNS istotne jest także poznanie działania usługi WINS, będącej wcześniejszym mechanizmem mapowania nazw NetBIOS na adresy IP. Mimo że w nowoczesnych środowiskach sieciowych funkcję tę w dużej mierze przejął DNS, WINS nadal odgrywa ważną rolę tam, gdzie wykorzystuje się starsze systemy i aplikacje zależne od NetBIOS. Znajomość WINS może okazać się szczególnie ważna w środowiskach sieciowych, które wciąż wykorzystują starszą infrastrukturę, ponieważ umożliwia sprawną komunikację między wszystkimi systemami, zarówno starszymi, jak i nowymi.

Poznaj WINS

Zrozumienie działania usługi WINS jest kluczowe dla automatyzacji procesu rozwiązywania nazw NetBIOS na adresy IP, który stanowi podstawę sprawnego funkcjonowania infrastruktury sieciowej. Twoja rola w tym procesie nabiera szczególnego znaczenia w środowiskach, w których nadal wykorzystywane są nazwy NetBIOS. WINS umożliwia efektywne mapowanie tych nazw na odpowiadające im adresy IP, co zapewnia płynny dostęp do współdzielonych zasobów sieciowych, takich jak foldery czy drukarki sieciowe. WINS zarządza tym procesem rozwiązywania nazw i zapewnia, że zasoby sieciowe są ciągle dostępne dla użytkowników.

W systemie Windows Server 2025 usługa WINS jest dostępna jako funkcja, którą można zainstalować za pomocą aplikacji Server Manager z wykorzystaniem kreatora *Add Roles and Features Wizard*, pokazanego na rysunku 4.16. Integracja z narzędziami administracyjnymi systemu ułatwia konfigurowanie usługi WINS i bieżące zarządzanie nią, co umożliwia administratorom sieci efektywne nadzorowanie jej działania. Baza danych serwera WINS jest aktualizowana dynamicznie w trakcie rejestrowania nazw NetBIOS, dzięki czemu dostarcza aktualnych informacji o rozwiązywaniu nazw w czasie rzeczywistym.

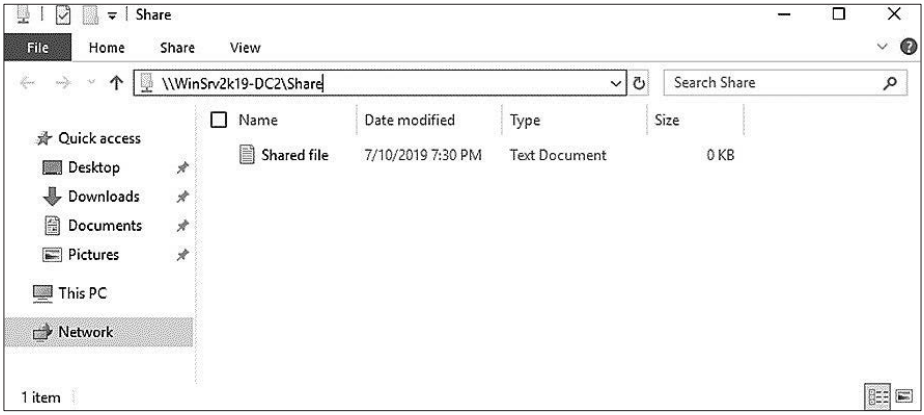
Oprócz zasad działania usługi WINS warto również poznać **konwencję UNC** (ang. *Universal Naming Convention*), która jest szczegółowo omówiona w następnym punkcie.



Rysunek 4.16. Instalowanie usługi WINS w systemie Windows Server 2025

Poznaj ścieżki UNC

Zrozumienie konwencji ścieżek **UNC** (ang. *Universal Naming Convention*) jest niezbędne do efektywnego zarządzania zasobami sieciowymi oraz sprawnego poruszania się w ich strukturze. UNC wprowadza jednolity sposób identyfikowania udostępnionych zasobów sieciowych w różnych systemach operacyjnych, w tym w środowiskach Unix, przez stosowanie ustandaryzowanego formatu nazw. Nazwa zasobu w tym formacie rozpoczyna się od dwóch lewych ukośników, po których następuje nazwa serwera oraz nazwa udostępnionego folderu, na przykład *nazwaserwera**folder* (jak pokazano na rysunku 4.17). Dzięki spójnej i czytelnej strukturze konwencja UNC znacząco ułatwia nawigację w sieci i dostęp do zasobów.



Rysunek 4.17. Przykładowa ścieżka UNC

Wcześniej opisywaliśmy system DNS, analizując jego kluczowe komponenty i sposób działania. Teraz przejdziemy do omówienia jednostek organizacyjnych (OU) i kontenerów. Jednostki organizacyjne pełnią istotną funkcję w strukturyzowaniu środowisk Active Directory i zarządzaniu nimi, ponieważ mogą zawierać inne kontenery i umożliwiają powiązanie z obiektami zasad grupy (GPO). Z kolei kontenery służą do przechowywania obiektów Active Directory, ale nie obsługują powiązań z GPO. To rozróżnienie ma fundamentalne znaczenie dla skutecznego zarządzania strukturą AD i budowania przejrzystej hierarchii katalogowej.

Zarządzanie jednostkami organizacyjnymi i kontenerami domyślnymi

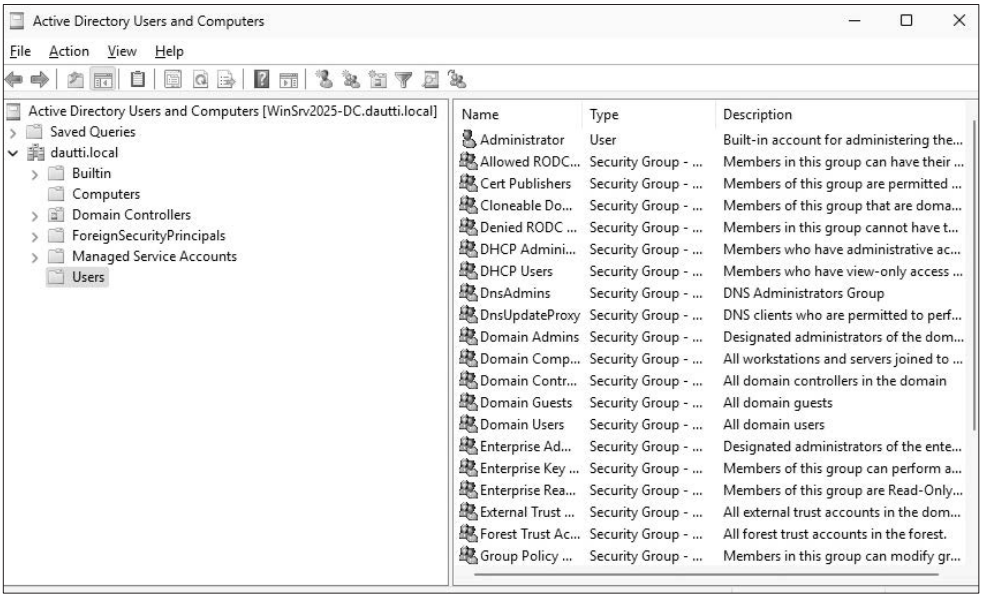
Dobra znajomość funkcji jednostek organizacyjnych (ang. *Organizational Units* — OU) i kontenerów jest niezbędna do efektywnego zarządzania usługą Active Directory. Oba komponenty, dostępne za pośrednictwem konsoli **Active Directory Users and Computers**, są niezbędne do organizowania obiektów katalogu i zarządzania nimi. Jednostki organizacyjne zapewniają elastyczną strukturę, umożliwiając administratorom tworzenie hierarchicznej organizacji w środowisku AD, co ułatwia stosowanie zasad grupy (GPO) oraz zarządzanie uprawnieniami w obrębie różnych działów lub grup użytkowników. Z kolei domyślne kontenery pełnią funkcję predefiniowanych lokalizacji dla określonych typów obiektów, takich jak użytkownicy czy komputery, lecz nie zapewniają takiego samego poziomu personalizacji ani kontroli zasad jak jednostki organizacyjne. W kolejnych punktach omówimy bardziej szczegółowo te zagadnienia, skupiając się na praktycznym zastosowaniu jednostek organizacyjnych w tworzeniu przejrzystej i bezpiecznej struktury Active Directory, z uwzględnieniem ograniczeń oraz roli kontenerów domyślnych. Zrozumienie tych zagadnień pozwoli administratorom poprawić efektywność zarządzania środowiskami AD oraz ich zabezpieczania, co zaowocuje utworzeniem dobrze zorganizowanego katalogu, który będzie prosty w obsłudze i po którym będzie łatwo się poruszać.

Czym są jednostki organizacyjne w AD?

Jednostki organizacyjne (ang. *Organizational Units* — OU) są istotnym elementem infrastruktury Active Directory, który umożliwia logiczne i przejrzyste zarządzanie zasobami katalogowymi, takimi jak użytkownicy, grupy, komputery i inne obiekty. Ich działanie przypomina strukturę folderów w systemie plików, co pozwala administratorom na tworzenie hierarchii zasobów w sposób odpowiadający strukturze organizacyjnej. Taka organizacja obiektów ma kluczowe znaczenie w usprawnianiu zadań administracyjnych, takich jak wdrażanie zasad grupy (GPO), oraz zarządzaniu uprawnieniami w obrębie poszczególnych działów, zespołów czy lokalizacji geograficznych w ramach struktury organizacyjnej.

Organizacje zazwyczaj projektują struktury swoich jednostek organizacyjnych w sposób odzwierciedlający ich wewnętrzną hierarchię biznesową. To pozwala na dostosowanie podejścia do zarządzania zgodnie z przyjętymi ramami operacyjnymi. Każda

domena w lesie Active Directory może definiować własną, unikalną strukturę jednostek organizacyjnych, co pozwala na utworzenie elastycznego i skalowalnego systemu, który dostosowuje się do zmieniających się potrzeb firmy. Taka elastyczność jest szczególnie cenna w złożonych środowiskach, gdzie poszczególne domeny mogą wymagać odmiennych zasad i praktyk zarządzania, jak pokazano na rysunku 4.18.

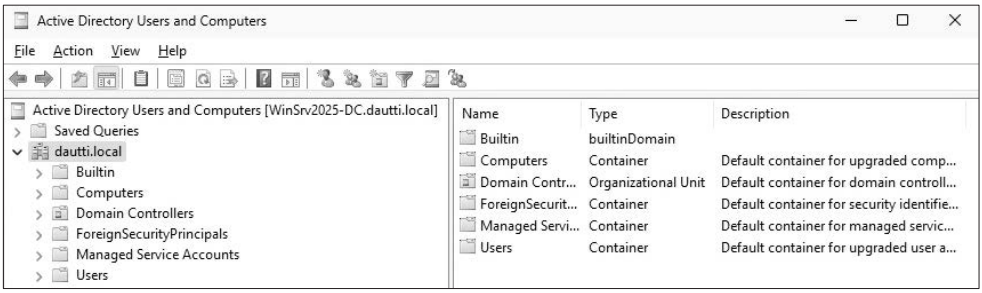


Rysunek 4.18. Przykładowa hierarchia jednostek organizacyjnych (OU) w Windows Server 2025

Poza jednostkami organizacyjnymi warto również zrozumieć rolę kontenerów domyślnych w Active Directory. Są to predefiniowane lokalizacje, do których automatycznie trafiają nowo utworzone obiekty, takie jak użytkownicy, komputery i inne zasoby. Bardziej szczegółowe omówienie kontenerów znajdziesz w następnym punkcie.

Czym są kontenery domyślne w AD?

Dobre zrozumienie roli **predefiniowanych kontenerów** jest kluczowe podczas promowania serwera do roli kontrolera domeny (DC). W trakcie tego procesu automatycznie tworzonych jest kilka domyślnych kontenerów, które pokazano na rysunku 4.19. Pełnią one istotną funkcję w strukturze Active Directory i charakteryzują się niezmienną naturą — nie można zmienić ich nazwy, usunąć ich ani odtworzyć, a także nie da się ich powiązać z obiektami zasad grupy (GPO). Ta celowa niezmienność gwarantuje spójność i bezpieczeństwo podstawowych komponentów AD oraz chroni i zachowuje integralność strukturalną całego katalogu.



Rysunek 4.19. Kontenery domyślne AD w systemie Windows Server 2025

Kontenery domyślne w Active Directory pełnią określone funkcje, umożliwiając uporządkowane rozmieszczanie użytkowników, komputerów oraz innych obiektów katalogowych w sposób zgodny z przyjętymi standardami. Zapewniają stabilne środowisko dla podstawowych operacji AD, co gwarantuje, że kluczowe obiekty są zawsze przechowywane w przewidywalnym miejscu. Choć nie oferują takiej elastyczności jak jednostki organizacyjne (OU), które można dostosować do indywidualnych potrzeb organizacji, kontenery domyślne nadal pozostają nieodzownym elementem struktury AD, wspierającym jej spójność i niezawodność.

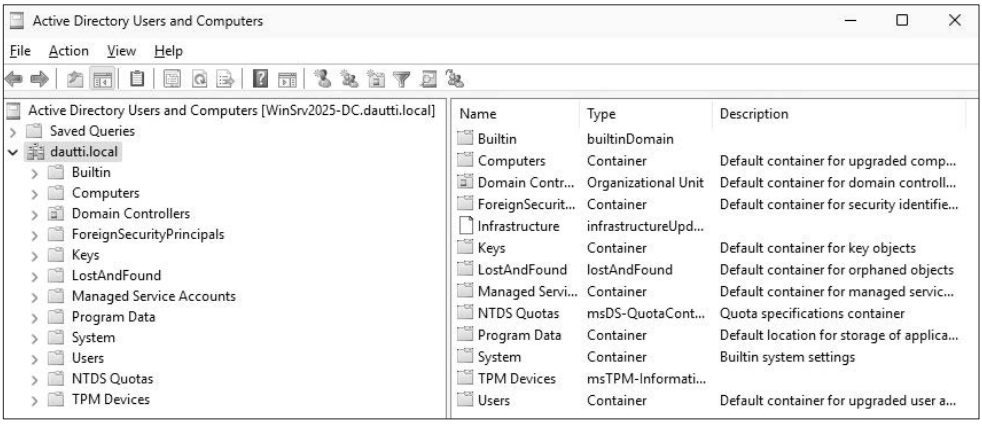
W kolejnych punktach skupimy się na koncepcji ukrytych kontenerów domyślnych. Choć nie są one widoczne w standardowym interfejsie Active Directory, odgrywają istotną rolę w działaniach systemowych i ogólnym funkcjonowaniu AD. Zrozumienie zarówno **jawnych, jak i ukrytych kontenerów domyślnych** pozwala uzyskać pełny obraz tego, jak Active Directory utrzymuje swoją integralność strukturalną i skutecznie wspiera zarządzanie obiektami katalogu.

Jak działają ukryte kontenery domyślne w AD?

Zrozumienie roli ukrytych kontenerów domyślnych w Active Directory jest niezmiernie ważne dla każdego administratora systemów, nawet jeśli nie mają bezpośredniego wpływu na jego codzienne zadania. Kontenery takie są istotne w utrzymaniu przejrzystości i porządku w konsoli **Active Directory Users and Computers**; zapobiegają niepotrzebnemu bałaganowi, który mógłby utrudnić zarządzanie obiektami AD. Dzięki ukryciu niektórych kontenerów domyślnych Active Directory zapewnia bardziej intuicyjny i uporządkowany interfejs, co ma szczególne znaczenie zwłaszcza w dużych, złożonych środowiskach sieciowych.

Ukrywanie tych kontenerów wynika również ze względów bezpieczeństwa. Ich zadaniem jest ochrona wrażliwych obiektów systemowych tak, aby dostęp do nich mieli wyłącznie użytkownicy, którzy mają odpowiednie uprawnienia oraz potrzebną wiedzę techniczną. Taka dodatkowa warstwa zabezpieczeń pomaga chronić integralność katalogu i zmniejsza ryzyko przypadkowych modyfikacji lub nieuprawnionego dostępu do krytycznych komponentów systemu.

Aby uzyskać dostęp do ukrytych kontenerów domyślnych, administratorzy muszą włączyć opcję *Advanced features* w menu *View*, jak pokazano na rysunku 4.20. Włączenie tej funkcji odsłania ukryte kontenery, co umożliwia pełniejszy wgląd w strukturę katalogu oraz lepszą kontrolę nad jego zasobami. To okazuje się szczególnie przydatne w zaawansowanych zadaniach administracyjnych, takich jak audyty bezpieczeństwa, dostrajanie ustawień zabezpieczeń czy zarządzanie obiektami, które zwykle nie są widoczne w standardowym widoku konsoli.



Rysunek 4.20. Ukryte kontenery domyślne w systemie Windows Server 2025

Po zapoznaniu się z ukrytymi kontenerami domyślnymi warto przyjrzeć się ich praktycznym zastosowaniom oraz roli, jaką odgrywają w środowisku AD. Kontenery te często przechowują kluczowe informacje systemowe, takie jak obiekty infrastrukturalne, komponenty zabezpieczeń czy informacje związane z replikacją, które są niezbędne do sprawnego działania Active Directory. Umiejętność uzyskania dostępu do tych ukrytych kontenerów oraz skutecznego zarządzania nimi pozwala administratorom utrzymać bezpieczną, wydajną i dobrze zorganizowaną infrastrukturę katalogową.

Przeznaczenie domyślnych typów kontenerów

Domyślne kontenery w systemie Windows Server 2025 odgrywają kluczową rolę w organizowaniu obiektów Active Directory i zarządzaniu nimi. Każdy z nich pełni specyficzną funkcję i każdy wspiera różne aspekty działania AD:

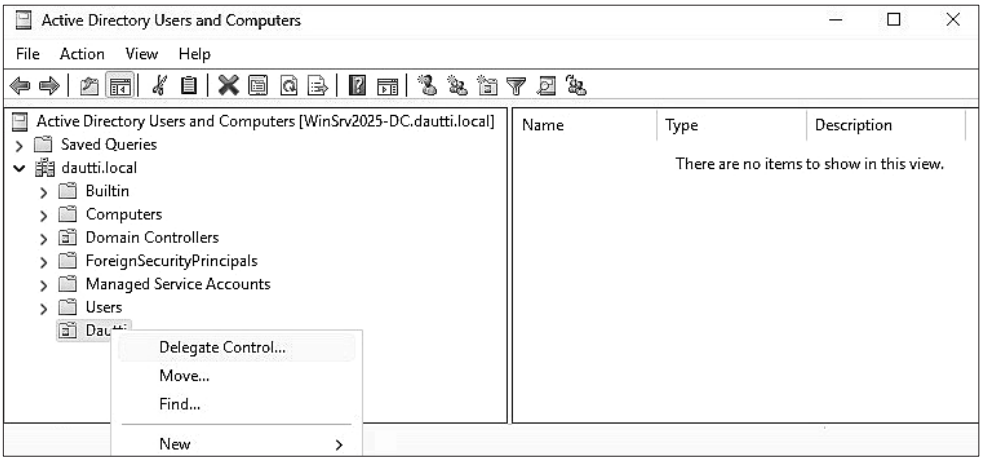
- **Computers** — domyślny kontener przeznaczony do przechowywania nowo utworzonych kont komputerów, zapewniający centralne miejsce do przechowywania tych obiektów.
- **Domain Controllers** — specjalnie zaprojektowany kontener służący do przechowywania kont kontrolerów domeny. Ułatwia ich organizację oraz zapewnia do nich szybki dostęp.

- **ForeignSecurityPrincipals** — kontener przeznaczony do przechowywania identyfikatorów SID pochodzących z zewnętrznych domen. Ułatwia zarządzanie uprawnieniami i zabezpieczeniami w środowiskach wielodomenowych.
- **Keys** — kontener przechowujący obiekty kluczy kryptograficznych, niezbędnych do zapewnienia bezpiecznej komunikacji oraz mechanizmów szyfrowania w sieci.
- **LostAndFound** — ten kontener odgrywa istotną rolę w zachowaniu integralności katalogu. Przechowuje osierocone obiekty, które utraciły powiązanie ze swoimi pierwotnymi kontenerami, dzięki czemu zapobiega potencjalnym problemom związanym z błędnymi odwołaniami do obiektów.
- **Managed Service Accounts** — kontener przeznaczony do przechowywania kont usług zarządzanych (ang. *managed service accounts*), wykorzystywanych do uruchamiania usług na serwerach z zapewnieniem wyższego poziomu bezpieczeństwa i niezawodności.
- **Users** — domyślny kontener przeznaczony do przechowywania nowo utworzonych lub zaktualizowanych kont użytkowników. Ułatwia zarządzanie obiektami związanymi z kontami użytkowników.

Po zapoznaniu się z domyślnymi kontenerami w AD kolejnym krokiem jest zrozumienie koncepcji delegowania kontroli nad jednostką organizacyjną (OU). Delegowanie kontroli polega na przyznawaniu określonych uprawnień administracyjnych wybranym użytkownikom lub grupom w obrębie konkretnej jednostki organizacyjnej, co umożliwia im zarządzanie obiektami w ramach tej jednostki bez konieczności posiadania pełnych uprawnień administracyjnych w całym środowisku Active Directory. Proces ten odgrywa kluczową rolę w utrzymaniu bezpiecznej i uporządkowanej struktury katalogu. Pozwala administratorom efektywnie rozdzielać obowiązki przy jednoczesnym ograniczeniu zakresu dostępu wyłącznie do zasobów i funkcji niezbędnych do realizacji przydzielonych zadań. Takie podejście umożliwia zachowanie równowagi między kontrolą administracyjną a bezpieczeństwem: zapewnia użytkownikom odpowiedni poziom uprawnień do realizacji ich zadań bez ryzyka naruszenia integralności całej infrastruktury AD.

Delegowanie uprawnień w jednostce organizacyjnej

Zrozumienie funkcji jednostek organizacyjnych (OU) w usłudze Active Directory jest niezbędne do efektywnego zarządzania katalogiem. OU umożliwiają logiczne i systematyczne grupowanie obiektów AD i zarządzanie nimi. Aby zwiększyć efektywność zarządzania, można delegować kontrolę nad wybranymi użytkownikami lub grupami w ramach konkretnej jednostki OU. Taki proces umożliwia rozdzielenie obowiązków administracyjnych bez konieczności przypisywania **pełnych uprawnień administracyjnych** w całym środowisku AD. Delegowanie kontroli wymaga uprzedniego przeniesienia użytkowników lub grup do odpowiedniej jednostki organizacyjnej, co zilustrowano na rysunku 4.21.



Rysunek 4.21. Delegowanie uprawnień do jednostki organizacyjnej (OU) w systemie Windows Server 2025

Delegowanie kontroli polega na przydzielaniu określonych uprawnień administracyjnych, takich jak zarządzanie kontami użytkowników, resetowanie haseł czy modyfikowanie członkostwa w grupach w ramach danej jednostki OU. Takie ukierunkowane delegowanie pomaga zapewnić, że odpowiedni personel wykonuje zadania administracyjne, a zarazem pozwala utrzymać bezpieczeństwo i porządek. Ograniczywszy uprawnienia do konkretnych jednostek OU, administratorzy mogą efektywniej zarządzać zasobami przy mniejszym ryzyku nieuprawnionego dostępu lub niezamierzonych zmian.

Delegowanie kontroli umożliwia również wdrożenie administracji opartej na rolach, co może poprawić efektywność operacyjną i odpowiedzialność. Każdemu delegowanemu administratorowi można przypisać zadania odpowiednie do jego roli, co ułatwia śledzenie zmian i zarządzanie obiektami katalogu zgodnie z polityką organizacji.

W następnym podrozdziale bardziej szczegółowo omówimy zarządzanie kontami użytkowników, kontami komputerów i grupami w usłudze AD. Między innymi przeanalizujemy, w jaki sposób te elementy współdziałają z jednostkami OU i przyczyniają się do tworzenia dobrze ustrukturyzowanego i bezpiecznego środowiska katalogowego.

Zarządzanie użytkownikami i grupami w Active Directory

Zrozumienie kont użytkowników i komputerów oraz grup odgrywa kluczową rolę w zarządzaniu dostępem do zasobów sieciowych w środowisku opartym na domenie Windows. Elementy te stanowią fundament usługi Active Directory. Umożliwiają skuteczne uwierzytelnianie zarówno użytkowników, jak i urządzeń w obrębie całej infrastruktury sieciowej. W tym scentralizowanym systemie szczególne znaczenie mają grupy, które znacząco upraszczają proces przydzielania uprawnień i zarządzania nimi. Dzięki możliwości łączenia wielu kont w jedną strukturę administratorzy mogą stosować

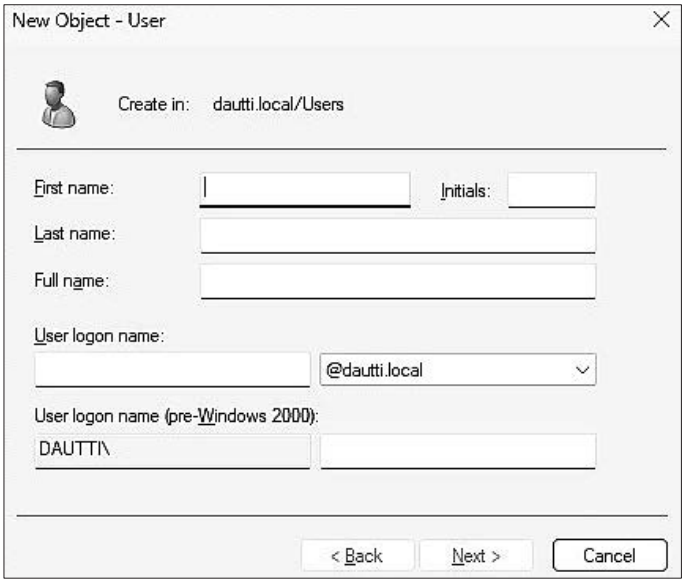
zasady i przydzielać uprawnienia zbiorczo, zamiast konfigurować je indywidualnie. Takie podejście przekłada się na większą efektywność operacyjną oraz podnosi poziom bezpieczeństwa. W kolejnych punktach szczegółowo omówimy różne typy kont i grup oraz ich funkcje i praktyczne zastosowanie w Active Directory. Analiza tych komponentów pozwoli pełniej zrozumieć ich przeznaczenie i rolę w efektywnym zarządzaniu zasobami sieciowymi.

Czym są konta domenowe?

Zrozumienie kont domenowych jest kluczowe w skutecznym zarządzaniu dostępem do zasobów sieciowych w środowisku Active Directory. Konta domenowe są uwierzytelniane przez usługę AD, co pozwala użytkownikom na dostęp zarówno do zasobów lokalnych, jak i sieciowych, zgodnie z uprawnieniami przypisanymi do konta lub odziedziczonymi z grup. Scentralizowany mechanizm uwierzytelniania w Active Directory zapewnia usprawnione i bezpieczne zarządzanie dostępem do usług i aplikacji w całym środowisku sieciowym.

Aby utworzyć konto domenowe w systemie Windows Server 2025, powinieneś wykonać następujące polecenia:

1. Otwórz konsolę *Active Directory Users and Computers*, którą znajdziesz w sekcji *Windows Tools* w menu *Start* systemu Windows.
2. W panelu po lewej stronie kliknij prawym przyciskiem myszy kontener *Users*, a następnie wybierz opcję *New/User*.
3. Wprowadź wymagane dane użytkownika, jak pokazano na rysunku 4.22, a następnie naciśnij przycisk *Next*.



Rysunek 4.22. Tworzenie konta domenowego w systemie Windows Server 2025

4. Ustaw tymczasowe hasło, potwierdź je, a następnie naciśnij przycisk *Next*.
5. Naciśnij przycisk *Finish*, aby zakończyć proces tworzenia konta domenowego.
6. Wykonanie tej operacji spowoduje utworzenie konta w domenie oraz zintegrowanie go ze strukturą Active Directory, co zapewni użytkownikowi dostęp do zasobów sieciowych zgodnie z przydzielonymi uprawnieniami.

W następnym punkcie omówimy proces tworzenia kont lokalnych i zarządzanie nimi. Konta lokalne odgrywają istotną rolę w kontroli dostępu użytkowników i zapewnianiu bezpieczeństwa zarówno na pojedynczych komputerach, jak też w wybranych środowiskach lokalnych.

Czym są konta lokalne?

Znajomość zasad działania kont lokalnych jest niezbędna do skutecznego zarządzania dostępem na poszczególnych komputerach. W odróżnieniu od kont domenowych, które są uwierzytelniane przez usługę Active Directory i zapewniają dostęp w całej sieci, konta lokalne są przypisane wyłącznie do komputera, na którym je utworzono, i są zarządzane przez lokalną usługę **Security Accounts Manager (SAM)** systemu Windows. Umożliwiają korzystanie z zasobów dostępnych na lokalnym komputerze i pozwalają na współpracę z zasobami udostępnionymi w sieciach peer-to-peer bez konieczności dodatkowych uprawnień na poziomie domeny.

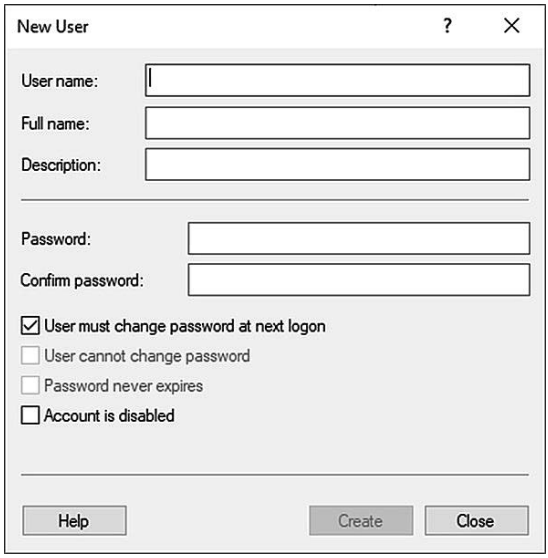
Konta lokalne są szczególnie przydatne w sytuacjach, gdy komputer działa poza domeną lub gdy dostęp do niej jest niemożliwy. Tworzy się je i zarządza nimi bezpośrednio na danym urządzeniu, co pozwala na szczegółową kontrolę uprawnień i dostępu użytkowników na poziomie pojedynczego komputera. Rozwiązanie to sprawdza się szczególnie w zarządzaniu małymi grupami roboczymi lub samodzielnymi komputerami, kiedy scentralizowane zarządzanie na poziomie domeny nie jest możliwe.

Aby utworzyć konto lokalne w systemie Windows Server 2025, wykonaj następujące czynności:

1. Otwórz konsolę *Computer Management*, którą znajdziesz w sekcji *Windows Tools*. Ta konsola zapewnia scentralizowany interfejs umożliwiający zarządzanie różnymi komponentami systemu, w tym kontami użytkowników.
2. Przejdź do sekcji *System tools*, rozwiń sekcję *Local Users and Groups*, kliknij prawym przyciskiem myszy kontener *Users* i z menu podręcznego wybierz polecenie *New*, a następnie *User*.
3. Wprowadź wymagane dane użytkownika, takie jak nazwa i hasło, jak pokazano na rysunku 4.23, a następnie naciśnij przycisk *Create*, aby zakończyć proces.

Ważna uwaga

Tworząc konto lokalne w Windows Server 2025, należy pamiętać, że serwer nie może być kontrolerem domeny. Jeżeli serwer odgrywa rolę kontrolera domeny, przejmuje funkcje związane z obsługą domeny oraz zarządzaniem Active Directory Domain Services (AD DS), co znacząco utrudnia proces zarządzania kontami lokalnymi. Jeśli się upewnisz, że serwer nie jest kontrolerem domeny, unikniesz komplikacji związanych z zarządzaniem domeną, co pozwala prosto tworzyć konta lokalne i nimi zarządzać bez dodatkowego obciążenia usługami domenowymi.



Rysunek 4.23. Tworzenie lokalnego konta w systemie Windows Server 2025

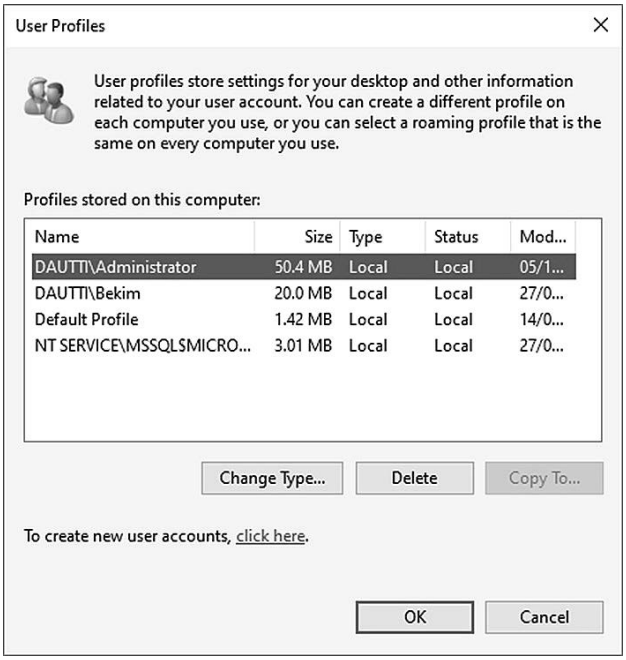
Konta lokalne są przechowywane i uwierzytelniane przez menedżera SAM na lokalnym komputerze, co zapewnia egzekwowanie kontroli dostępu i uprawnień niezależnie od domeny sieciowej. Takie rozwiązanie jest szczególnie przydatne w sytuacjach, w których potrzebna jest lokalna administracja i lokalne zarządzanie dostępem.

W dalszych podrozdziałach zajmiemy się profilami użytkowników, które są niezbędne do przechowywania informacji o poszczególnych użytkownikach i zarządzania nimi. Profil użytkownika zawiera kluczowe dane, które umożliwiają personalizację środowiska pracy użytkownika oraz efektywne zarządzanie nim zarówno w systemach lokalnych, jak i środowiskach sieciowych.

Czym są profile użytkowników?

Dobra znajomość różnych typów **profili użytkowników** (ang. *user profiles*) w środowiskach Windows Server jest niezbędna do efektywnego zarządzania kontami użytkowników i ich personalizacji. W Active Directory wyróżniamy trzy podstawowe typy profili użytkowników: profile lokalne, które są przypisane do konkretnego urządzenia; profile mobilne, zapewniające elastyczność pracy na wielu urządzeniach; profile obowiązkowe, zapewniające stałą konfigurację, której użytkownik nie może zmieniać. Przyjrzyjmy się im bliżej:

- **Profil lokalny** (ang. *local user profile*) — gdy użytkownik loguje się do komputera po raz pierwszy, tworzony jest profil lokalny, który jest przechowywany na tym konkretnym urządzeniu (zobacz rysunek 4.24). Profil ten zawiera ustawienia użytkownika, dokumenty oraz dane aplikacji dostosowane do tego komputera. Profil lokalny jest idealnym rozwiązaniem dla indywidualnego użytkownika korzystającego z jednego urządzenia, jednak nie zapewnia elastyczności w sytuacjach, gdy użytkownik potrzebuje dostępu do swojego środowiska na wielu komputerach.



Rysunek 4.24. Przykładowe profile użytkowników w systemie Windows Server 2025

- **Profil mobilny** (ang. *roaming user profile*) — ten typ profilu zapewnia większą elastyczność, umożliwia bowiem użytkownikom dostęp do ich spersonalizowanych ustawień oraz plików z dowolnego komputera w sieci. Jest to w zasadzie kopia profilu lokalnego przechowywana na udziale sieciowym. Kiedy użytkownik loguje się z innego urządzenia, jego profil mobilny jest pobierany z sieci, co gwarantuje spójne środowisko pracy na różnych komputerach. Rozwiązanie to jest szczególnie przydatne w organizacjach, w których użytkownicy regularnie korzystają z wielu stacji roboczych.
- **Profil obowiązkowy** (ang. *mandatory user profile*) — narzuca stałą konfigurację środowiska użytkownika. Profile obowiązkowe są przechowywane na udziałach sieciowych i opierają się na wcześniej przygotowanych szablonach. Zmiany wprowadzane przez użytkownika podczas sesji nie są zapisywane po wylogowaniu, dzięki czemu każde logowanie rozpoczyna pracę w identycznym środowisku. Rozwiązanie to jest szczególnie przydatne w środowiskach wymagających jednolitości oraz tam, gdzie nie przewiduje się zmian w konfiguracji wprowadzanych przez użytkowników.

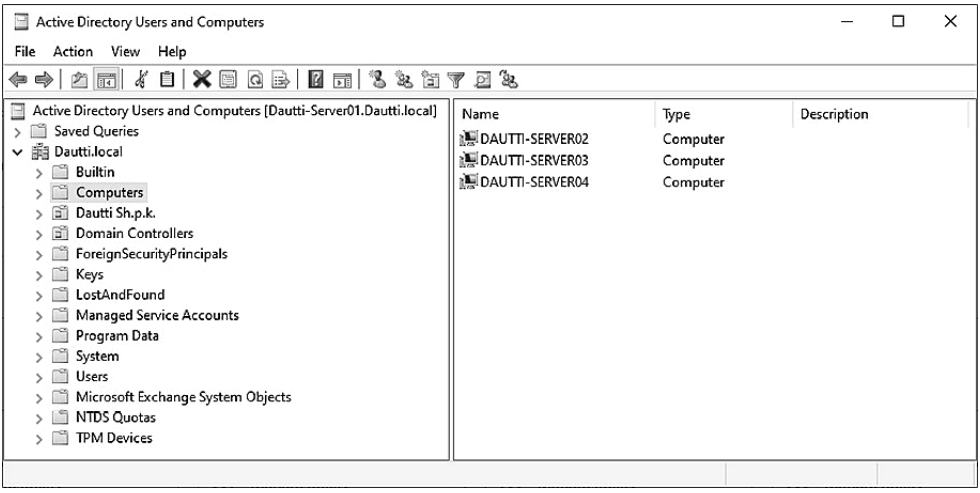
Podsumowując, profile lokalne są przypisane do pojedynczych komputerów, profile mobilne zapewniają elastyczność dzięki dostępności z dowolnego urządzenia w sieci, a profile obowiązkowe gwarantują spójność, ponieważ odrzucają wszelkie zmiany wprowadzane przez użytkownika i opierają się na stałym szablonie. Każdy z tych typów profili pełni określoną funkcję i wspiera administratorów w efektywnym zarządzaniu środowiskami użytkowników w zależności od potrzeb organizacji.

W następnym punkcie omówimy konta komputerów. Konta te odgrywają kluczową rolę w identyfikowaniu komputerów i zarządzaniu nimi zarówno w systemach lokalnych, jak i scentralizowanych środowiskach domenowych. Konta te są niezbędne do utrzymania bezpieczeństwa sieci i zapewnienia właściwej kontroli dostępu w całym środowisku sieciowym.

Czym są konta komputerów?

W środowisku Active Directory **konta komputerów** (ang. *computer accounts*) odgrywają kluczową rolę w procesie identyfikowania komputerów w domenie i zarządzaniu nimi. Przed dołączeniem do domeny każdy komputer musi mieć unikalną nazwę hosta, co pozwala uniknąć konfliktów i umożliwia jednoznaczną identyfikację w sieci. Ten unikalny identyfikator zapewnia, że komputer może być dokładnie monitorowany i zarządzany w środowisku sieciowym. Po pomyślnym dołączeniu komputera do domeny zachowuje on swoją nazwę hosta, co umożliwia nieprzerwane korzystanie z innych zasobów domeny, takich jak pliki, aplikacje czy usługi. Dzięki takiemu rozwiązaniu możliwa jest płynna komunikacja oraz pełna integracja komputera z domeną.

Konsola **Active Directory Users and Computers** stanowi podstawowe narzędzie do zarządzania kontami komputerów, jak pokazano na rysunku 4.25. Umożliwia ona administratorom przeglądanie kont komputerów i zarządzanie nimi, konfigurowanie ich właściwości, a także stosowanie odpowiednich zasad bezpieczeństwa. Do typowych zadań realizowanych z użyciem tego narzędzia należą między innymi resetowanie haseł, włączanie i wyłączanie kont oraz zmiana ich ustawień.



Rysunek 4.25. Przykładowe konta komputerów w systemie Windows Server 2025

Aby utrzymać integralność sieci i skutecznie kontrolować dostęp do zasobów, trzeba dobrze zrozumieć działanie i przeznaczenie kont komputerów. To właśnie one odpowiadają za uwierzytelnianie i autoryzację w domenie, co przekłada się na efektywność zarządzania całą infrastrukturą sieciową oraz jej bezpieczeństwo.

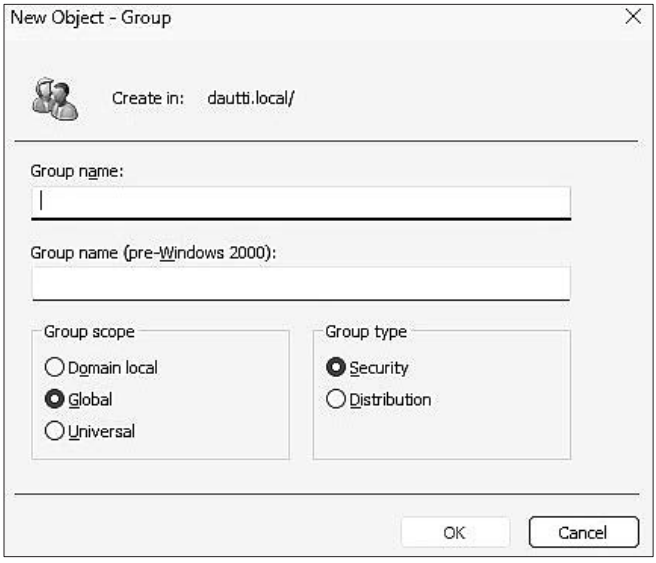
W następnym punkcie skupimy się na grupach w usłudze Active Directory. Są one integralną częścią zarządzania uprawnieniami i prawami dostępu, upraszczają przydzielanie ról i uprawnień oraz usprawniają realizowanie zadań administracyjnych. Grupy pomagają w organizowaniu użytkowników i komputerów, stosowaniu jednolitych zasad zabezpieczeń oraz zwiększaniu ogólnego bezpieczeństwa całego środowiska sieciowego.

Typy grup w usłudze AD

Aby zoptymalizować zarządzanie siecią i zapewnić jej bezpieczeństwo, trzeba dobrze zrozumieć **typy grup** dostępne w usłudze Active Directory. Grupy AD ułatwiają administrowanie uprawnieniami dzięki temu, że pozwalają na jednoczesne zarządzanie wieloma obiektami zamiast konfigurowania każdego z nich z osobna. Takie rozwiązanie nie tylko zwiększa efektywność pracy, ale także pomaga utrzymać spójne zasady bezpieczeństwa w całym środowisku sieciowym. Co więcej, same grupy również są obiektami AD, dzięki czemu mogą być przenoszone lub organizowane w różnych jednostkach organizacyjnych, co zapewnia elastyczność w dostosowywaniu ich do zmieniających się wymagań operacyjnych.

Jak pokazano na rysunku 4.26, grupami zarządza się za pomocą konsoli **Active Directory Users and Computers**. W AD wyróżniamy dwie główne kategorie grup:

- **Grupy zabezpieczeń** (ang. *security groups*) — służą do zarządzania dostępem do współdzielonych zasobów sieciowych, takich jak pliki, foldery i drukarki. Umożliwiają przydzielanie uprawnień i egzekwowanie zasad bezpieczeństwa w sieci. Grupy zabezpieczeń mogą być zagnieżdżane w innych grupach tego typu, co pozwala tworzyć hierarchiczną strukturę uprawnień i zapewnia bardziej precyzyjną kontrolę dostępu do zasobów.



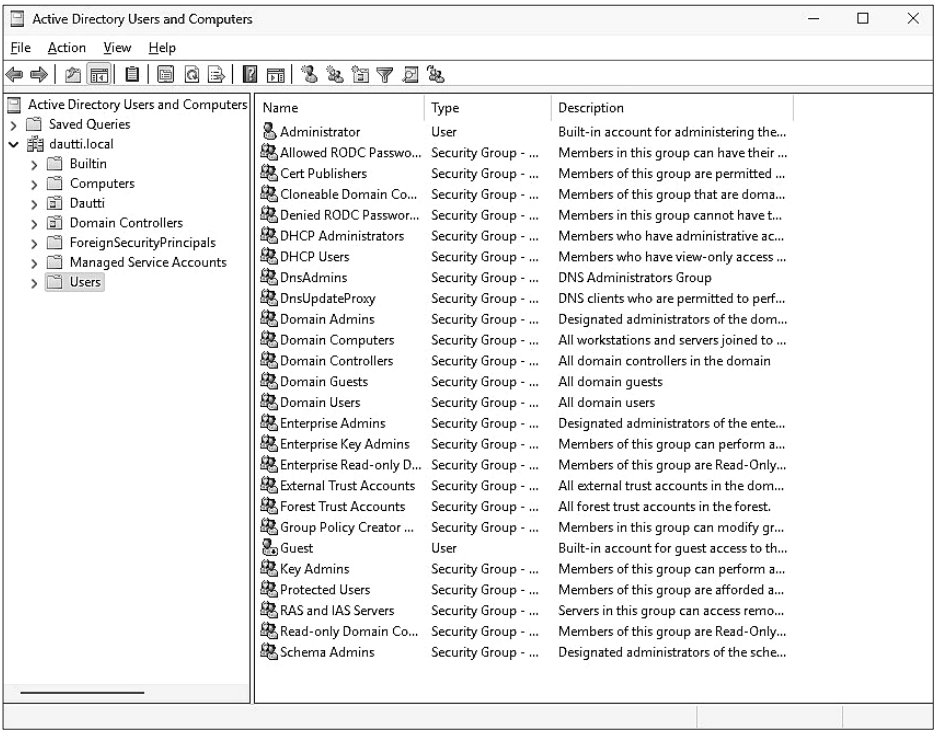
Rysunek 4.26. Typy grup w systemie Windows Server 2025

- **Grupy dystrybucyjne** (ang. *distribution groups*) — wykorzystuje się je do ułatwienia dystrybucji wiadomości e-mail w organizacji. Ułatwiają wysyłanie komunikatów do dużych grup użytkowników (działają podobnie jak listy mailingowe). Choć grupy dystrybucyjne nie mają przypisanych uprawnień i nie mogą być używane do kontrolowania dostępu do zasobów, odgrywają istotną rolę w usprawnianiu komunikacji wewnętrznej.

Znajomość typów grup oraz ich funkcji pozwala administratorom skutecznie zarządzać zasobami i komunikacją w środowisku sieciowym. W dalszych punktach omówimy grupy domyślne, które są predefiniowane i dostarczane w ramach AD, a także opiszemy proces tworzenia nowych grup. Ta wiedza jest niezbędna do odpowiedniego przydzielania ról użytkownikom, zarządzania dostępem do zasobów oraz efektywnego delegowania zadań administracyjnych w środowisku Active Directory.

Grupy domyślne w AD

Dobra znajomość domyślnych grup w usłudze Active Directory jest niezbędna do efektywnego zarządzania infrastrukturą sieciową. Gdy serwer zostaje wypromowany do roli kontrolera domeny, system Windows Server 2025 automatycznie tworzy zestaw domyślnych grup, pokazany na rysunku 4.27. Domyślne grupy AD są zaprojektowane tak, aby konsolidować powiązane obiekty katalogu. Dzięki temu administratorzy mogą efektywnie przypisywać prawa i uprawnienia oraz sprawniej kontrolować dostęp do zasobów.



Rysunek 4.27. Domyślne grupy AD w systemie Windows Server 2025

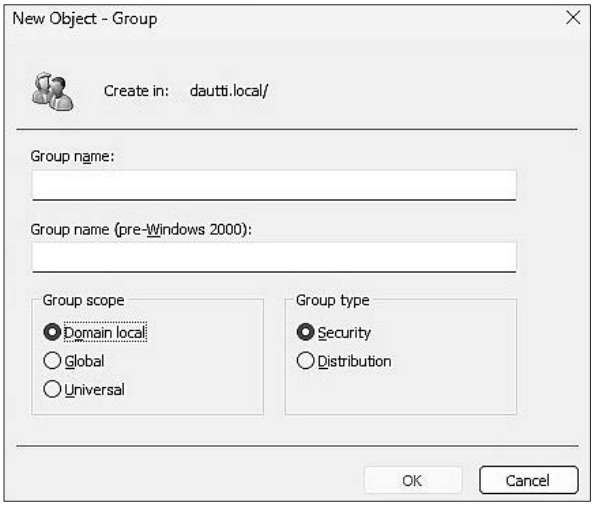
Domyślne grupy są wstępnie skonfigurowane z określonymi rolami i uprawnieniami, co znacznie usprawnia zarządzanie środowiskiem sieciowym. Na przykład grupy takie jak **Domain Admins**, **Enterprise Admins** i **Schema Admins** mają predefiniowane poziomy uprawnień administracyjnych, które są kluczowe w zarządzaniu różnymi aspektami środowiska AD. Z wykorzystaniem tych grup administratorzy mogą efektywnie zarządzać dostępem użytkowników i egzekwować polityki bezpieczeństwa bez konieczności ręcznego przypisywania uprawnień dla każdego użytkownika czy obiektu.

Ponadto domyślne grupy umożliwiają jednolite stosowanie polityk oraz uprawnień w całej sieci, co przekłada się zarówno na wyższy poziom bezpieczeństwa, jak i na zwiększoną efektywność operacyjną. Ułatwiają one również delegowanie zadań administracyjnych dzięki predefiniowanym rolom, które można przypisywać użytkownikom zgodnie z zakresem ich obowiązków. W następnym punkcie przyjrzymy się koncepcji zakresów grup i omówimy ich dostępne typy. Zrozumienie sposobu działania zakresów grup jest niezbędne do optymalizacji zarządzania grupami w środowisku Active Directory, ponieważ określają one sposób interakcji grup z obiektami AD oraz wpływają na zakres uprawnień i polityk stosowanych w całej sieci.

Zakresy grup w AD

Dobra znajomość koncepcji zakresów grup jest fundamentalnym aspektem efektywnego zarządzania środowiskiem Active Directory, ponieważ bezpośrednio wpływają one na sposób nadawania uprawnień i egzekwowania polityk w środowisku sieciowym organizacji. Zakresy grup definiują obszar obowiązywania członkostwa w grupach w strukturze Active Directory, co ma zasadnicze znaczenie dla bezpieczeństwa oraz sprawnego zarządzania zasobami.

W Active Directory wyróżniamy trzy główne zakresy grup, z których każdy pełni odrębną funkcję i znajduje zastosowanie w określonych scenariuszach administracyjnych, jak pokazano na rysunku 4.28:



Rysunek 4.28. Zakresy grup w systemie Windows Server 2025

- **Grupy lokalne domeny** (ang. *domain local group scope*) — zakres ten jest przeznaczony do zarządzania dostępem do zasobów znajdujących się w obrębie domeny lokalnej. Umożliwia dodawanie kont użytkowników, grup lokalnych domeny, grup globalnych oraz grup uniwersalnych, co pozwala administratorom efektywnie przydzielać uprawnienia do lokalnych zasobów. Grupy lokalne domeny są szczególnie użyteczne w kontrolowaniu dostępu do zasobów takich jak udziały plików, drukarki i inne zasoby specyficzne dla danej domeny, gdy chcemy ograniczyć dostęp wyłącznie do użytkowników i grup działających w obrębie tej domeny.
- **Grupy globalne** (ang. *global group scope*) — zakres grupy globalnej służy do organizowania użytkowników i grup z tej samej domeny, którzy mają wspólne wymagania dotyczące dostępu. Ten zakres obejmuje konta i grupy globalne przypisane do grupy globalnej domeny nadrzędnej. Grupy globalne są najczęściej wykorzystywane do przydzielania uprawnień do zasobów znajdujących się w różnych domenach w obrębie tego samego lasu, dzięki czemu są idealnym rozwiązaniem w scenariuszach, w których użytkownicy z wielu domen potrzebują dostępu do współdzielonych zasobów.
- **Grupy uniwersalne** (ang. *universal group scope*) — zakres grupy uniwersalnej jest najszerszy i pozwala na dodawanie kont, grup globalnych i grup uniwersalnych z dowolnej domeny w obrębie lasu. Taki zakres jest niezbędny do zarządzania uprawnieniami w wielu domenach, dzięki czemu jest szczególnie użyteczny w rozbudowanych środowiskach wielodomenowych. Grupy uniwersalne są bardzo przydatne zwłaszcza w zastosowaniach wymagających jednolitego nadawania uprawnień w całym lesie Active Directory. Dzięki nim użytkownicy z różnych domen mogą korzystać z zasobów niezależnie od tego, do której domeny należą.

Każdy z opisanych zakresów grup jest niezbędny do tego, by uprawnienia i polityki w środowisku Active Directory były stosowane we właściwy i spójny sposób. Ich zrozumienie i umiejętne wykorzystanie pozwala administratorom zwiększyć efektywność i zarazem bezpieczeństwo procesów zarządzania w całym środowisku sieciowym.

Co więcej, właściwe stosowanie zakresów grup pozwala uniknąć typowych problemów, takich jak nadmierne uprawnienia, gdy użytkownicy otrzymują prawa dostępu wykraczające poza ich rzeczywiste potrzeby, lub niewystarczające uprawnienia, gdy zostają pozbawieni uprawnień niezbędnych do wykonywania swoich obowiązków. Zachowanie tej równowagi jest kluczowe w utrzymaniu bezpiecznego i dobrze funkcjonującego środowiska Active Directory.

W następnym punkcie przyjrzymy się koncepcji zagnieżdżania grup. Mechanizm ten opiera się na zasadach zakresów grup i pozwala administratorom tworzyć bardziej złożone i elastyczne struktury grupowe. Zagnieżdżanie grup dodatkowo usprawnia zarządzanie uprawnieniami i prawami dostępu. Dzięki temu administratorzy otrzymują skuteczne narzędzie do pracy w dużych środowiskach Active Directory.

Zagnieżdżanie grup w AD

Zagnieżdżanie grup w Active Directory to kluczowy element skutecznego i bezpiecznego zarządzania uprawnieniami w złożonych środowiskach IT. Dzięki hierarchicznej organizacji grup administratorzy mogą efektywniej przydzielać prawa dostępu z zastosowaniem wielopoziomowego, ustrukturyzowanego podejścia. Takie rozwiązanie nie tylko upraszcza zarządzanie kontrolą dostępu, ale także ogranicza redundancję i minimalizuje ryzyko wystąpienia błędów, które mogłyby wynikać z ręcznego nadawania uprawnień dla wielu kont użytkowników.

W praktyce proces zagnieżdżania grup opiera się na sprawdzonych metodach i najlepszych praktykach, takich jak metodyki **AGDLP** (ang. *Accounts, Global, Domain Local, Permissions*) i **AGUDLP** (ang. *Accounts, Global, Universal, Domain Local, Permissions*), opracowane przez firmę Microsoft. Oba podejścia zapewniają uporządkowany sposób zarządzania członkostwem w grupach i odpowiednią kontrolę uprawnień w środowisku sieciowym:

- W modelu AGDLP konta użytkowników są najpierw przypisywane do grup globalnych, które zazwyczaj reprezentują określone role lub działy w organizacji. Następnie grupy globalne są umieszczane w grupach lokalnych domeny, które odpowiadają za kontrolę dostępu do konkretnych zasobów w domenie lokalnej. Uprawnienia są przydzielane grupom lokalnym domeny, co automatycznie zapewnia dostęp wszystkim członkom powiązanych grup globalnych. Takie rozwiązanie sprawdza się szczególnie w środowiskach, gdzie użytkownicy potrzebują jednolitego dostępu do zasobów w obrębie jednej domeny.
- Metodyka AGUDLP rozwija koncepcję AGDLP przez dodanie grupy uniwersalnej do struktury zagnieżdżania. W tym rozwiązaniu grupa globalna jest najpierw dodawana do grupy uniwersalnej, która może obejmować wiele domen w obrębie lasu. Następnie grupa uniwersalna zostaje umieszczona w grupie lokalnej domeny, która odpowiada za kontrolę dostępu do zasobów. Takie podejście sprawdza się szczególnie w dużych środowiskach wielodomenowych, gdzie użytkownicy wymagają dostępu do zasobów znajdujących się w różnych domenach. Dzięki wykorzystaniu grup uniwersalnych administratorzy mogą utrzymać spójną strukturę uprawnień w obrębie całego lasu, zapewniając użytkownikom niezbędny dostęp niezależnie od domeny, w której działają.

Opisane metodyki nie tylko usprawniają proces zarządzania uprawnieniami, ale także podnoszą poziom bezpieczeństwa i skalowalności środowiska Active Directory. Dzięki ograniczeniu liczby indywidualnych przypisań uprawnień i scentralizowaniu kontroli w ramach dobrze zdefiniowanych struktur grupowych administratorzy zyskują możliwość skutecznego egzekwowania polityk bezpieczeństwa, prowadzenia audytów dostępu oraz szybkiego reagowania na zmiany organizacyjne.

Po opanowaniu wiedzy na temat podstawowych elementów Active Directory, takich jak DNS, jednostki organizacyjne (OU), kontenery oraz klasyfikacja kont komputerów i grup, następnym krokiem jest instalacja ról AD DS i DNS. Ten etap jest kluczowy, ponieważ tworzy fundament konfigurowania środowiska Active Directory i zarządzania nim, gwarantując jego zgodność z wymaganiami organizacji w zakresie bezpieczeństwa, skalowalności i zarządzania.

Ćwiczenie 4.1 — instalacja ról AD DS i DNS oraz promocja serwera do roli kontrolera domeny

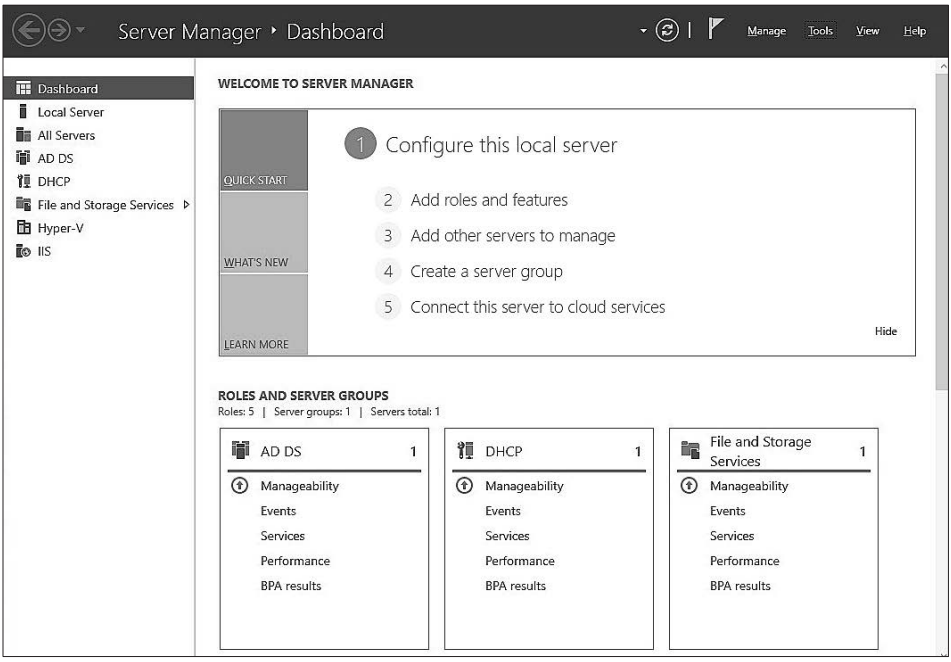
W ramach tego ćwiczenia przejdziesz przez najważniejsze etapy instalowania ról AD DS i DNS, zakończone promowaniem serwera do roli pełnoprawnego kontrolera domeny. Proces ten stanowi fundament budowy bezpiecznej i wydajnej infrastruktury sieciowej w każdej organizacji wykorzystującej usługę Active Directory.

Ćwiczenie rozpoczyna się od zainstalowania usługi Active Directory Domain Services (AD DS), będącej podstawą zarządzania tożsamościami i dostępem w środowiskach Windows Server. Następnie skonfigurujemy usługę DNS, odpowiedzialną za rozwiązywanie nazw w domenie. Ostatnim etapem będzie promowanie serwera do roli kontrolera domeny, który pełni kluczową funkcję w zakresie bezpieczeństwa, uwierzytelniania użytkowników oraz egzekwowania polityk w całej domenie.

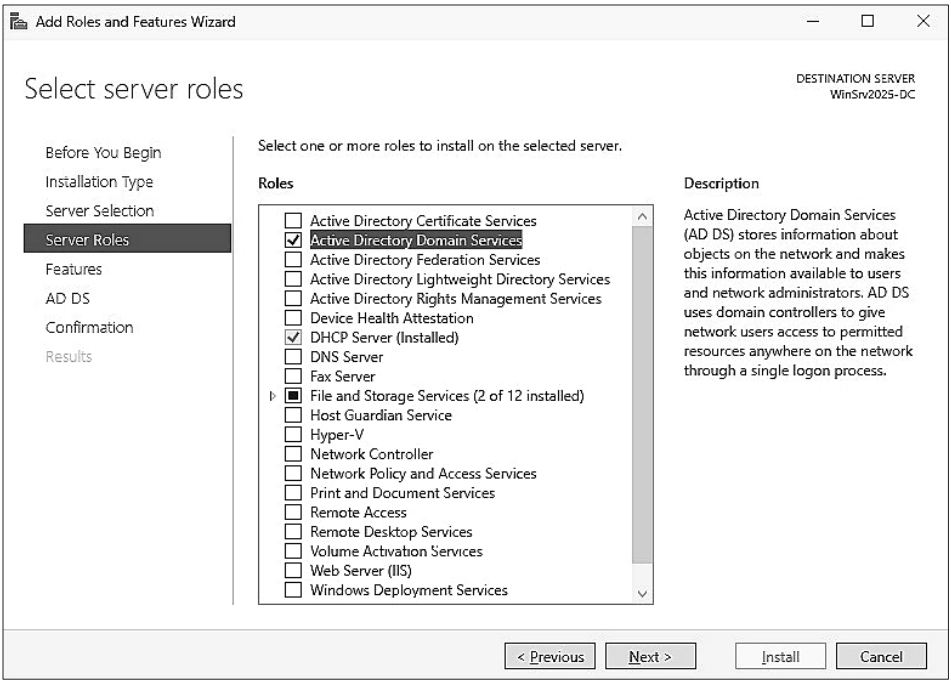
Postępując zgodnie ze szczegółowymi instrukcjami zamieszczonymi poniżej, zdobędziesz niezbędną wiedzę na temat wdrażania i konfiguracji ról AD DS i DNS, co pozwoli Ci na zbudowanie solidnej i dobrze zorganizowanej infrastruktury sieciowej. Ćwiczenie to nie tylko rozwija umiejętności praktyczne, ale również pogłębia wiedzę teoretyczną, co przygotuje Cię do bardziej złożonych zadań administracyjnych.

Aby rozpocząć proces instalacji ról AD DS i DNS oraz przeprowadzić promowanie serwera do roli kontrolera domeny, wykonaj następujące czynności:

1. Uruchom aplikację *Server Manager*. Aby to zrobić, naciśnij przycisk *Start* i z menu wybierz opcję *Server Manager*.
2. W oknie *Server Manager* przejdź do sekcji *WELCOME TO SERVER MANAGER* i wybierz opcję *Add Roles and Features*, jak pokazano na rysunku 4.29. Spowoduje to uruchomienie kreatora *Add Roles and Features Wizard*. Aby przejść dalej, naciśnij przycisk *Next*.
3. Wybierz opcję *Role-based or feature-based installation* i naciśnij przycisk *Next*.
4. Sprawdź, czy zaznaczona jest opcja *Select a server from the server pool*, po czym ponownie naciśnij przycisk *Next*.
5. Z listy dostępnych ról wybierz *Active Directory Domain Services*, jak pokazano na rysunku 4.30, i przejdź dalej za pomocą przycisku *Next*.
6. Kiedy na ekranie pojawi się okno *Add features that are required for Active Directory Domain Services*, wybierz opcję *Add Features*, a następnie naciśnij przycisk *Next*.
7. W oknie *Select Features* pozostaw ustawienia domyślne i ponownie wybierz *Next*.
8. Zapoznaj się z opisem i kluczowymi informacjami dotyczącymi instalacji roli AD DS, po czym naciśnij przycisk *Next*.
9. Potwierdź wybrane opcje instalacji roli AD DS i naciśnij przycisk *Install*. Możesz zamknąć okno kreatora lub poczekać na zakończenie procesu instalacji.

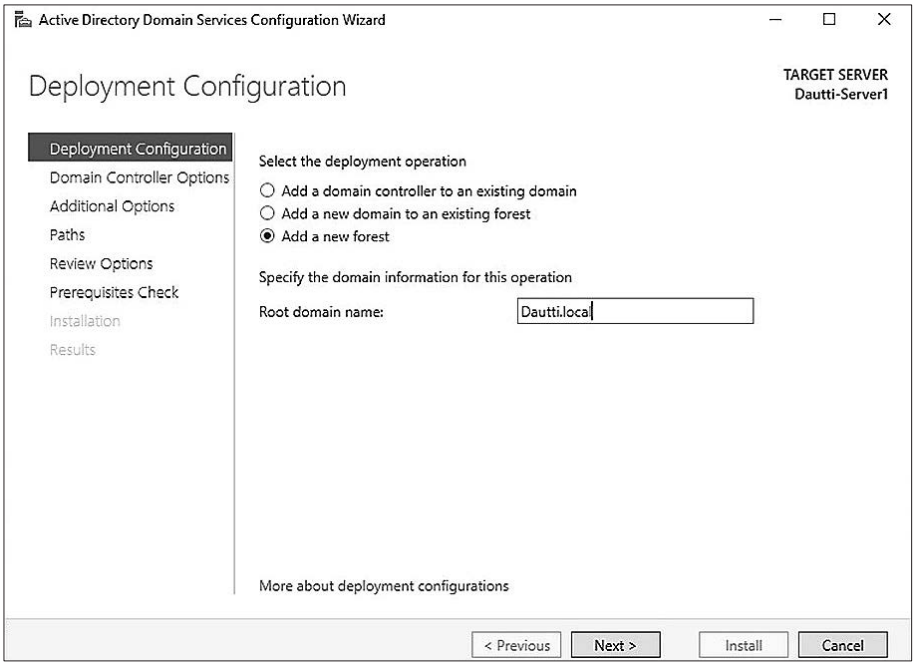


Rysunek 4.29. Dodawanie ról i funkcji do serwera z użyciem aplikacji Server Manager



Rysunek 4.30. Instalowanie roli AD DS w systemie Windows Server 2025

10. Po zakończeniu instalacji naciśnij przycisk *Close*, aby wyjść z kreatora *Add Roles and Features Wizard*.
11. W sekcji *Notifications* pojawi się opcja *Promote this server to a domain controller*. Kliknij ją, aby uruchomić kreator konfiguracji AD DS.
12. Wybierz opcję *Add a new forest*, jak pokazano na rysunku 4.31, i w polu *Root domain name* wpisz wybraną nazwę domeny głównej. Naciśnij przycisk *Next*, aby kontynuować.



Rysunek 4.31. Okno kreatora konfiguracji roli AD DS

13. Pozostaw domyślne ustawienia lasu i poziomów funkcjonalności domeny, a następnie ustaw hasło dla trybu *Directory Services Restore Mode (DSRM)*. Naciśnij przycisk *Next*.
14. Jeżeli w Twojej sieci działa już serwer DNS, być może będziesz musiał ręcznie utworzyć delegację dla tego serwera DNS, aby zapewnić prawidłowe rozwiązywanie nazw spoza domeny. W przeciwnym razie nie są wymagane żadne działania. Naciśnij przycisk *Next*.
15. Zaakceptuj domyślną nazwę *NetBIOS* lub wprowadź własną. Naciśnij przycisk *Next*.
16. Pozostaw domyślne ścieżki dla bazy danych AD DS, plików dziennika i katalogu *SYSVOL* albo dostosuj je do własnych potrzeb. Naciśnij przycisk *Next*.
17. Sprawdź podsumowanie wybranych opcji konfiguracji i naciśnij przycisk *Next*.
18. Jeżeli kreator potwierdzi, że wszystkie wymagania wstępne zostały spełnione, naciśnij przycisk *Install*. System automatycznie uruchomi serwer ponownie, aby zakończyć proces promowania do roli kontrolera domeny.

To ćwiczenie dostarczyło Ci praktycznych wskazówek dotyczących instalowania ról AD DS i DNS oraz promowania serwera do roli kontrolera domeny. Wykonanie tych kroków pozwoliło Ci zdobyć podstawowe umiejętności potrzebne do efektywnego zarządzania środowiskiem sieciowym w organizacji i zabezpieczania go.

Podsumowanie

Rozdział ten dostarczył Ci kompleksowej wiedzy na temat usług katalogowych i zasad rozwiązywania nazw, które są niezbędne do sprawnego zarządzania środowiskiem sieciowym i zabezpieczania go. Poznałeś rolę AD DS, solidny fundament zarządzania tożsamością w sieci, umożliwiający uwierzytelnianie użytkowników i urządzeń, oraz rolę DNS, odgrywającą kluczową rolę w tłumaczeniu przyjaznych dla człowieka nazw domen na adresy IP, co zapewnia płynną komunikację w całej sieci. Przyjrzeliśmy się także strukturze i funkcjonalności jednostek organizacyjnych (OU) w Active Directory, które umożliwiają logiczne grupowanie zasobów i delegowanie uprawnień. Dzięki temu nauczyłeś się, jak efektywnie delegować uprawnienia w ramach jednostki organizacyjnej, i zyskałeś umiejętność efektywnego rozdzielania zadań administracyjnych w celu zwiększenia wydajności i bezpieczeństwa całego środowiska AD. Rozdział objął również konfigurowanie grup i kont użytkowników oraz zarządzanie nimi, co jest kluczowe w utrzymywaniu uporządkowanej i bezpiecznej bazy użytkowników opartej na ich rolach i obowiązkach.

Na koniec przeprowadziliśmy ćwiczenie, które zapewniło Ci praktyczne doświadczenie w instalowaniu roli AD DS i promowaniu serwera do roli kontrolera domeny. Dzięki temu mogłeś połączyć teorię z praktyką i zdobyć kompetencje niezbędne do wdrożenia tych usług w rzeczywistym środowisku.

W następnym rozdziale skupimy się na dalszym rozszerzaniu możliwości serwera przez dodawanie i konfigurowanie dodatkowych ról w systemie Windows Server 2025, co jeszcze bardziej zwiększy Twoje umiejętności, a także pozwoli Ci skuteczniej zarządzać infrastrukturą sieciową oraz podnosić jej wydajność i poziom bezpieczeństwa.

Pytania

1. **Prawda czy fałsz?** Active Directory jest rozproszoną bazą danych, która przechowuje obiekty w sposób hierarchiczny, ustrukturyzowany i bezpieczny.
2. **Uzupełnij zdanie:** _____ pozwala ograniczyć liczbę uprawnień nadawanych bezpośrednio użytkownikom lub grupom.
3. Wskaż, które z poniższych profili użytkownika są najczęściej stosowane w sieciach domenowych opartych na systemie Windows.
   - **A.** Profil domenowy użytkownika
   - **B.** Profil zabezpieczeń użytkownika
   - **C.** Profil mobilny użytkownika
   - **D.** Profil obowiązkowy użytkownika

4. **Prawda czy fałsz?** Serwer WINS odpowiada za mapowanie adresów IP na nazwy NetBIOS.
5. **Uzupełnij zdanie:** _____ to zestaw połączeń komunikacyjnych wykorzystywanych do przesyłania danych replikacji między kontrolerami domeny.
6. Które z poniższych stanowią zakresy grup w Active Directory?
   A. Jednostka organizacyjna (OU)
   B. Grupa zabezpieczeń
   C. Grupa globalna
   D. Grupa uniwersalna
7. **Prawda czy fałsz?** UNC jest standardem służącym do identyfikowania udziałów w sieci komputerowej.
8. **Uzupełnij zdanie:** _____ to serwer odpowiedzialny za bezpieczne uwierzytelnianie żądań dostępu do zasobów domenowych w organizacji.
9. Które z poniższych przystawek MMC służą do zarządzania usługą Active Directory?
   A. Active Directory Administrative Center
   B. Active Directory Users and Computers
   C. UNC
   D. OU
10. **Prawda czy fałsz?** Typowym przykładem domeny jest środowisko klient-serwer, w którym usługi w sieci świadczy oddzielny serwer.
11. **Uzupełnij zdanie:** _____ przechowuje główną kopię bazy danych DNS i odpowiada za zarządzanie wszystkimi rekordami stref DNS.
12. Które z poniższych określeń są nazwami ról wzorców operacji obejmującymi cały las Active Directory?
    A. Master schema
    B. Domain naming master
    C. LAN manager hosts
    D. Default containers
13. Omów role usług AD DS i DNS oraz sposoby ich implementowania.
14. Przedstaw zalecenia firmy Microsoft dotyczące przydzielania uprawnień, znane jako AGDLP i AGUDLP.

Gdzie warto zajrzeć?

- Wdrażanie usługi AD DS: *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-deployment*
- System nazw domenowych (DNS): *https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview*
- Tworzenie struktury jednostek organizacyjnych: *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-an-organizational-unit-design*
- Zarządzanie grupami: *https://learn.microsoft.com/en-us/windows/win32/ad/managing-groups*

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Kompletny przewodnik po Windows Server 2025 — od podstaw do certyfikacji!

Windows Server 2025 wprowadza szereg istotnych usprawnień w zakresie bezpieczeństwa, skalowalności i integracji z chmurą. W dobie dynamicznej transformacji cyfrowej i rosnącego znaczenia rozwiązań hybrydowych umiejętność efektywnego zarządzania środowiskami serwerowymi staje się kluczową kompetencją dla specjalistów IT. Książka oferuje praktyczne podejście do administracji systemem Windows Server z uwzględnieniem najnowszych funkcji, takich jak hotpatching, SMB over QUIC czy rozszerzone możliwości Active Directory. To niezbędne kompendium dla każdego, kto chce profesjonalnie zarządzać infrastrukturą serwerową w organizacji.

Autor prowadzi czytelnika przez wszystkie aspekty pracy z Windows Server 2025 — od podstaw sieci komputerowych, przez instalację i konfigurację początkową, po zaawansowane zagadnienia dotyczące wirtualizacji, zarządzania pamięcią masową i zabezpieczeń. Szczegółowo omawia usługi katalogowe Active Directory, konfigurację ról serwerowych i zasady grupy, a także prezentuje nowe funkcjonalności systemu i mechanizmy automatycznego instalowania poprawek. Ponadto proponuje liczne ćwiczenia praktyczne, pytania kontrolne i sekcję przygotowującą do egzaminu certyfikacyjnego AZ-800, co czyni tę książkę kompleksowym przewodnikiem zarówno dla początkujących administratorów, jak i doświadczonych specjalistów IT.

Dr Erdal Ozkaya, CISO Xcitium, autor przedmowy do książki, podkreśla jej wartość jako bezcennego przewodnika dla wszystkich pragnących zgłębić tajniki Windows Server.

W książce:

- Instalacja i konfiguracja Windows Server 2025 w różnych scenariuszach
- Zarządzanie usługami Active Directory Domain Services z nowymi funkcjami
- Konfiguracja protokołu SMB over QUIC w celu bezpiecznego i wydajnego udostępniania plików
- Wirtualizacja z Hyper-V, zarządzanie maszynami wirtualnymi i kontenerami
- Implementacja zaawansowanych mechanizmów bezpieczeństwa, uwierzytelniania wieloskładnikowego i szyfrowania
- Hotpatching z Azure Arc — instalowanie aktualizacji bez ponownego uruchamiania serwera
- Przygotowanie do egzaminu certyfikacyjnego AZ-800 z praktycznymi wskazówkami i przykładami

Bekim Dauti to ceniony specjalista IT z ponad 20-letnim doświadczeniem w branży. Posiada doktorat z informatyki, jest certyfikowanym trenerem Microsoft (MCT) i instruktorem Cisco Academy (CCAI). Pracuje jako trener w firmie TeKnowledge, jest założycielem InfoTech Academy i Dautti. Ma na koncie blisko 20 książek i liczne artykuły publikowane w prestiżowych magazynach IT.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-3329-3
9 788328 933293
Cena: 139,00 zł