

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

Copyright © Packt Publishing 2025.

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

Polish edition copyright © 2026 by Helion S.A.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści |

Przedmowa	21
O autorze	22
O recenzencie	22
Wstęp	23

CZĘŚĆ 1. Wprowadzenie do Windows Server i instalacja Windows Server 2025

ROZDZIAŁ 1

Podstawy sieci komputerowych

i wprowadzenie do systemu Windows Server 2025	31
Wymagania techniczne	32
Podstawy infrastruktury sieciowej: hosty, węzły, architektura klient-serwer	32
Czym jest sieć komputerowa?	33
Rodzaje sieci komputerowych	34
Kluczowe elementy sieci komputerowych	37
Architektura sieci komputerowych	39
Przegląd adresowania IP i podsieci	41
Adresy sieciowe IPv4	41
Adresy sieciowe IPv6	42
Podsieci IPv4	42
Poznajemy serwer	43
Poznanie sprzętu i oprogramowania serwerowego	44
Rozmiary, formy i typy serwerów	45
Podstawy sieciowych systemów operacyjnych	46
Przegląd systemu Windows Server	47
Przegląd systemu Linux Server	47
Przegląd systemu macOS Server	49
Przegląd systemu Windows Server 2025 i jego edycje	49
Ewolucja systemu Windows Server — przegląd wersji	50

Przegląd systemu Windows Server 2025	50
Edycje systemu Windows Server 2025	53
Kluczowe różnice między Windows Server 2025 a Windows Server 2022	53
Minimalna i zalecana konfiguracja sprzętowa dla Windows Server 2025	55
Ćwiczenie 1.1 — pobieranie Windows Server 2025	56
Pobieranie systemu Windows Server 2025	57
Ćwiczenie 1.2 — pobieranie Windows Admin Center	58
Pobieranie Windows Admin Center	58
Podsumowanie	59
Pytania	60
Gdzie warto zajrzeć?	61

ROZDZIAŁ 2

Instalowanie systemu Windows Server 2025	62
Wymagania techniczne	62
Podstawy partycjonowania dysków i dostępne opcje przechowywania danych	63
Schematy partycjonowania dysków	63
Przegląd opcji przechowywania danych	65
Jak uzyskać dostęp do zaawansowanych opcji uruchamiania?	66
Konfiguracja rozruchu i opcje uruchamiania systemu	68
Opcje uruchamiania dostępne w UEFI	68
Poznajemy proces uruchamiania w BIOS-ie	69
Alternatywne oprogramowanie firmware do uruchamiania współczesnych komputerów	70
Jak działa TPM?	71
POST — test o kluczowym znaczeniu dla serwera	72
GPT i programy rozruchowe	73
BCD — baza danych do uruchamiania systemu Windows	74
Czym jest bootloader?	75
Czym jest sektor rozruchowy?	75
Jak korzystać z menu rozruchowego?	76
Jak działa tryb Safe Mode?	77
Błędy instalacji systemu Windows i konfiguracji dysków	78
Opcje instalacji dla Windows Server 2025	79
Zrozumienie roli Twojego serwera	79
Przygotowanie do instalacji — sprawdzenie zgodności sprzętu i zasobów	80
Którą opcję instalacji systemu Windows Server 2025 powinienem wybrać?	81
Porównanie Nano Server i Server Core	82
Wykorzystanie logów do diagnozowania problemów z instalacją	83

Połączenia sieciowe i dołączanie do domeny	85
Problemy z aktywacją i licencjonowaniem	86
Metody wdrażania systemu Windows Server 2025	87
Czysta instalacja	87
Wdrażanie systemu Windows Server 2025 za pomocą MDT	93
Aktualizacja w miejscu	98
Migracja	100
Wdrażanie systemu Windows Server 2025 na platformie Azure	102
Podsumowanie	105
Pytania	105
Gdzie warto zajrzeć?	106

ROZDZIAŁ 3

Co zrobić po zainstalowaniu systemu Windows Server 2025?	107
Wymagania techniczne	108
Zarządzanie urządzeniami oraz sterownikami, w tym technologia Plug and Play, przerwania IRQ i podpisywanie sterowników	108
Zrozumienie urządzeń komputerowych i sterowników	108
Zarządzanie urządzeniami i sterownikami	109
Dostosowywanie menu Start w celu usprawnienia nawigacji	110
Praca z urządzeniami i programem Device Manager	111
PnP, IRQ, DMA i podpisywanie sterowników — co warto wiedzieć?	118
Zarządzanie wpisami rejestru oraz kontami usługowymi	120
Rejestr systemu Windows Server	120
Service Control Manager i usługi Windows Server	121
Dostęp do usług i rejestru systemu Windows Server 2025 oraz zarządzanie nimi	122
Wstępna konfiguracja serwera w celu zoptymalizowania wydajności i bezpieczeństwa	135
Wstępna konfiguracja systemu Windows Server	135
Zarządzanie konfiguracją z wykorzystaniem PowerShell Desired State Configuration	137
Weryfikowanie stabilności sprzętu z użyciem testerów pamięci i aplikacji do testów obciążeniowych	138
Ćwiczenie 3.1 — wstępna konfiguracja systemu Windows Server	139
Konfigurowanie początkowych ustawień systemu Windows Server za pomocą aplikacji Server Manager	139
Jak skonfigurować system Windows Server za pomocą programu Server Configuration?	147
Podsumowanie	152
Pytania	152
Gdzie warto zajrzeć?	153

CZĘŚĆ 2. Konfiguracja systemu Windows Server 2025

ROZDZIAŁ 4

Usługi katalogowe w systemie Windows Server 2025	157
Wymagania techniczne	158
Analiza infrastruktury Active Directory w środowisku Windows Server 2025	158
Rola i znaczenie Active Directory	159
Podstawowe protokoły i usługi wspierające Active Directory	160
Narzędzia i role do zarządzania usługą Active Directory	161
Dodawanie i konfigurowanie roli AD DS	163
Kontrolery domeny	164
Domeny	165
Drzewa domen	166
Lasy domen	168
Domeny podrzędne	168
Role głównych operacji (role operacyjne)	169
Różnice między domenami a grupami roboczymi	171
Relacje zaufania między domenami	172
Poziomy funkcjonalne domen	173
Koncepcja przestrzeni nazw AD DS	175
Lokacje w Active Directory	177
Replikacja w AD	178
Schemat AD	179
Microsoft Passport	179
Podstawy działania i konfiguracja DNS w Windows Server 2025	180
Podstawy działania systemu DNS	181
Instalowanie roli DNS	182
Rola plików hosts i lmhosts	183
Nazwy hostów i ich rola w sieci	185
Zasada działania i znaczenie stref DNS	186
Poznaj WINS	187
Poznaj ścieżki UNC	188
Zarządzanie jednostkami organizacyjnymi i kontenerami domyślnymi	189
Czym są jednostki organizacyjne w AD?	189
Czym są kontenery domyślne w AD?	190
Jak działają ukryte kontenery domyślne w AD?	191
Przeznaczenie domyślnych typów kontenerów	192
Delegowanie uprawnień w jednostce organizacyjnej	193

Zarządzanie użytkownikami i grupami w Active Directory	194
Czym są konta domenowe?	195
Czym są konta lokalne?	196
Czym są profile użytkowników?	197
Czym są konta komputerów?	199
Typy grup w usłudze AD	200
Grupy domyślne w AD	201
Zakresy grup w AD	202
Zagnieżdżanie grup w AD	204
Ćwiczenie 4.1 — instalacja ról AD DS i DNS oraz promocja serwera do roli kontrolera domeny	205
Podsumowanie	208
Pytania	208
Gdzie warto zajrzeć?	210

ROZDZIAŁ 5

Dodawanie ról serwera w systemie Windows Server 2025 211

Wymagania techniczne	212
Analiza ról i funkcji serwera w systemie Windows Server 2025	212
Przegląd dostępnych ról i funkcji	212
Czym są usługi ról?	213
Poznawanie funkcji serwera	214
Przegląd aplikacji Server Manager	215
Przegląd ról serwera aplikacji i ich wdrażanie	216
Serwer poczty elektronicznej w systemie Windows Server 2025	216
Rola serwera baz danych	218
Role i funkcje serwerów ułatwiających współpracę	220
Rola serwera monitorującego	221
Serwery wspomagające ochronę danych	222
Konfigurowanie usług sieciowych i ich funkcji w systemie Windows Server 2025	223
Serwery IIS	224
Wprowadzenie do sieci WWW	227
FTP	228
Czym są procesy robocze i jak uzyskać do nich dostęp?	229
Instalowanie dodatkowych funkcji IIS	230
Witryny internetowe	230
Porty	232
Czym jest SSL?	233
Jak działają certyfikaty?	234

Konfigurowanie ról dostępu zdalnego oraz ich funkcjonalności	236
Jak korzystać z funkcji Remote Assistance?	238
Jak działa RSAT?	239
Rola Remote Desktop Services (RDS)	240
Jak zarządzać licencjami CAL dla roli RDS?	241
Konfigurowanie usługi Remote Desktop Gateway	242
Tunele VPN	243
Usługa App-V	244
Wykorzystywanie wielu portów	245
Wdrażanie usług plikowych i drukowania w środowiskach sieciowych	246
Rola File Services	246
Rola Print and Document Services (PDS)	247
Czym jest drukarka lokalna?	249
Drukarki sieciowe	249
Printer pooling	250
Drukowanie przez internet	251
Zarządzanie drukowaniem w sieci	252
Wdrażanie sterowników drukarek	253
Zarządzanie uprawnieniami i prawami dostępu użytkowników	254
Uprawnienia NTFS	254
Uprawnienia dostępu do udziałów sieciowych	256
Prawa użytkownika	257
Monitorowanie aktywności serwera plików	258
Ćwiczenie 5.1 — instalowanie ról Web Server (IIS) i PDS	259
Instalowanie roli Web Server (IIS)	259
Instalowanie roli PDS	261
Podsumowanie	262
Pytania	263
Gdzie warto zajrzeć?	264

CZĘŚĆ 3. Konfiguracja systemu Windows Server 2025

ROZDZIAŁ 6

Zasady grupy w systemie Windows Server 2025	267
Wymagania techniczne	268
Podstawy zasad grupy w systemie Windows Server 2025	268
Domyślna lokalizacja GPO	268
Zarządzanie obiektami zasad grupy (GPO)	270
Zarządzanie szablonami administracyjnymi	271

Najlepsze praktyki zarządzania zasadami grupy	274
Praktyczne zastosowania zasad grupy	275
Analiza mechanizmów przetwarzania GP i kolejności wykonywania operacji	276
Konfiguracja ustawień GPO	277
Stosowanie zasad grupy	278
Przegląd edytorów Group Policy	280
Edytor lokalnych zasad grupy	281
Stosowanie lokalnych zasad grupy	282
Przegląd kategorii ustawień GPO	283
Ćwiczenie 6.1 — przykładowe zasady grupy (GPO) dla administratorów systemów	287
Zmiana nazwy konta administratora	287
Zmiana nazwy konta gościa	288
Blokowanie korzystania z kont Microsoft	289
Blokowanie dostępu do panelu sterowania i ustawień komputera	290
Blokowanie dostępu do wszystkich klas wymiennych nośników pamięci	291
Podsumowanie	292
Pytania	293
Gdzie warto zajrzeć?	294

ROZDZIAŁ 7

Wirtualizacja w systemie Windows Server 2025	295
Wymagania techniczne	296
Podstawy wirtualizacji w systemie Windows Server 2025	296
Związek między technologią Hyper-V a chmurą obliczeniową	296
Tryby wirtualizacji	298
Aspekty wydajnościowe w wirtualizacji	300
Dodawanie i konfigurowanie roli Hyper-V w systemie Windows Server 2025	301
Architektura Hyper-V	302
Wymagania instalacyjne Hyper-V	303
Wirtualizacja zagnieżdżona	304
Zarządzanie maszynami wirtualnymi za pomocą aplikacji Hyper-V Manager	305
Podstawowe funkcje aplikacji Hyper-V Manager	306
Ustawienia konfiguracyjne w Hyper-V	308
Jak tworzyć i modyfikować dyski wirtualne VHD?	310
Przydzielanie pamięci RAM dla maszyny wirtualnej	311
Konfigurowanie sieci wirtualnych z użyciem aplikacji Hyper-V Manager	313
Punkty kontrolne	316

Formaty VHD i VHDX	318
Migracja z VMware do Hyper-V	321
Dostosowywanie ustawień maszyny wirtualnej	323
Praca z maszynami wirtualnymi	325
Najlepsze praktyki dotyczące ustawień uruchamiania i odzyskiwania maszyn wirtualnych	326
Praktyczne zastosowania Hyper-V we współczesnych środowiskach IT	328
Ćwiczenie 7.1 — instalowanie roli Hyper-V w systemie Windows Server 2025	330
Podsumowanie	332
Pytania	333
Gdzie warto zajrzeć?	334

ROZDZIAŁ 8

Przechowywanie danych w systemie Windows Server 2025	335
Wymagania techniczne	336
Technologie pamięci masowej i ich rozwój w systemie Windows Server 2025	336
Przegląd różnych typów pamięci masowej	337
Interfejsy ATA i SCSI	338
Przegląd standardów PCI i PCIe	340
Pamięć lokalna	341
Analiza architektur pamięci masowej i ich wpływu na środowiska sieciowe	342
Pamięci masowe na poziomie bloków i plików	344
Zasady działania adapterów i kontrolerów	345
Transmisja danych w urządzeniach pamięci masowej	346
Przegląd protokołów pamięci masowej oraz ich znaczenie w przesyłaniu i udostępnianiu danych	347
Protokoły komunikacyjne w urządzeniach pamięci masowej	347
Protokoły udostępniania plików	348
Karty HBA i przełączniki FC	350
Sprzęt iSCSI	351
Technologia S2D	352
Wprowadzenie do deduplikacji	353
Wielowarstwowe pamięci masowe	354
Wprowadzenie do sieciowego systemu automatycznego zarządzania warstwową pamięcią masową w Windows Server 2025	355
Praktyczne zastosowania technologii przechowywania danych u dostawców zarządzanych usług bezpieczeństwa	356

Zarządzanie pamięcią masową serwera z użyciem aplikacji Server Manager i powłoki Windows PowerShell	358
Zarządzanie pamięcią masową z użyciem aplikacji Server Manager	358
Zarządzanie pamięcią masową z poziomu powłoki Windows PowerShell	359
Macierze RAID — zasady działania i konfiguracja	361
Warianty macierzy RAID	362
Metody implementowania RAID	363
Technologia SDS	364
Odporność na awarie dzięki technologii S2D	365
Koncepcja wysokiej dostępności	366
Podstawowe koncepcje i optymalizacja rozwiązań pamięci masowej w systemie Windows Server 2025	367
Tradycyjne dyski twarde (HDD)	368
Dyski półprzewodnikowe (SSD)	369
Napędy dysków optycznych i dyski optyczne	370
Dyski podstawowe	372
Dyski dynamiczne	372
Konwersja dysku podstawowego na dysk dynamiczny	373
Optymalizacja wydajności dysku	374
Punkty montowania	376
Systemy plików	376
Montowanie wirtualnych dysków twardych (VHD)	378
DFS — rozproszony system plików	379
Ćwiczenie 8.1 — włączanie deduplikacji w systemie Windows Server 2025	380
Podsumowanie	382
Pytania	383
Gdzie warto zajrzeć?	384

CZĘŚĆ 4. Nowe i ulepszone funkcje w Windows Server 2025

ROZDZIAŁ 9

Rozszerzenia i ulepszenia

usługi Active Directory Domain Services (AD DS)	387
Wymagania techniczne	388
Przegląd rozszerzeń i ulepszeń usługi Active Directory w systemie Windows Server 2025	388
Najważniejsze ulepszenia usługi Active Directory Domain Services w systemie Windows Server 2025	389

Najważniejsze ulepszenia zabezpieczeń i mechanizmów uwierzytelniania w systemie Windows Server 2025	392
Integracja z usługami chmurowymi i środowiskami hybrydowymi	394
Wdrażanie 32-kilobajtowych stron w bazach danych AD —	
lepsza skalowalność	397
Optymalizowanie replikacji dla środowisk wielkoskalowych	398
Ulepszone mechanizmy tworzenia kopii zapasowych i odzyskiwania danych	399
Aktualizacje schematów Active Directory i rozszerzanie ich funkcjonalności	401
Zarządzanie wersjami schematów i eliminowanie konfliktów	402
Najlepsze praktyki projektowania i utrzymywania schematów Active Directory	403
Wykorzystanie mechanizmów naprawy obiektów AD do lepszego zarządzania obiektami	405
Identyfikowanie i diagnozowanie problemów z obiektami Active Directory	406
Naprawianie i odzyskiwanie obiektów AD	407
Najlepsze praktyki zarządzania obiektami Active Directory i ich odzyskiwania	409
Praktyczne zastosowania narzędzi diagnostycznych w Active Directory	410
Najważniejsze narzędzia diagnostyczne do zarządzania Active Directory	411
Ćwiczenie 9.1 — implementacja 32-kilobajtowej strony bazy danych AD w systemie Windows Server 2025	413
Podsumowanie	415
Pytania	416
Gdzie warto zajrzeć?	417

ROZDZIAŁ 10

Konfigurowanie protokołu SMB over QUIC

w systemie Windows Server 2025	418
Wymagania techniczne	419
Wprowadzenie do protokołu SMB over QUIC w systemie Windows Server 2025	419
Przegląd protokołów SMB i QUIC	419
Kontekst historyczny i rozwój	422
Kluczowe korzyści z wdrożenia SMB over QUIC	424
Najważniejsze zagadnienia związane z bezpieczeństwem danych i protokołami szyfrowania	426
Infrastruktura klucza publicznego (PKI)	426
Jak PKI zabezpiecza komunikację sieciową?	428

Wdrażanie infrastruktury klucza publicznego (PKI) w środowisku Windows Server 2025	430
Najlepsze praktyki zarządzania infrastrukturą klucza publicznego (PKI)	430
Mechanizmy szyfrowania w protokole SMB over QUIC	431
Konfigurowanie zabezpieczeń	433
Najlepsze praktyki bezpieczeństwa	435
Optymalizowanie wydajności protokołu SMB over QUIC	437
Konfigurowanie sieci w celu zapewnienia optymalnej wydajności	437
Zagadnienia sprzętowe	439
Monitorowanie i optymalizowanie wydajności	440
Rozwiązywanie problemów z wdrożeniami protokołu SMB over QUIC	443
Rozpoznawanie typowych problemów	443
Rozwiązania i poprawki	445
Działania prewencyjne	447
Znaczenie protokołu SMB over QUIC w różnych środowiskach sieciowych	449
Ćwiczenie 10.1 — włączanie i konfigurowanie protokołu SMB over QUIC w systemie Windows Server 2025	452
Podsumowanie	455
Pytania	455
Gdzie warto zajrzeć?	457

ROZDZIAŁ 11

Przegląd nowych mechanizmów bezpieczeństwa

w systemie Windows Server 2025	458
Wymagania techniczne	459
Przegląd nowych i ulepszonych mechanizmów bezpieczeństwa w systemie Windows Server 2025	459
Ulepszone mechanizmy kontroli dostępu	459
Przegląd mechanizmów zaawansowanego wykrywania zagrożeń	464
Microsoft Defender Antivirus dla systemu Windows Server 2025	468
Czym są zautomatyzowane systemy reagowania na zagrożenia?	469
Ulepszanie mechanizmów uwierzytelniania i autoryzacji	472
Uwierzytelnianie biometryczne	473
Wdrażanie uwierzytelniania biometrycznego	475
Przegląd zasad dostępu warunkowego	476
Konfigurowanie zasad dostępu warunkowego	477
Integracja OAuth 2.0 w systemie Windows Server 2025	478
Wdrażanie protokołu OAuth 2.0	480

Zabezpieczanie kanałów komunikacyjnych za pomocą TLS i innych protokołów	481
Protokół TLS	481
Przegląd innych protokołów bezpieczeństwa (HTTPS, IPsec i SSH)	483
Jak monitorować bezpieczne kanały komunikacji?	485
Zaawansowane mechanizmy bezpieczeństwa systemu	
Windows Server 2025 w integracji z platformą Azure	486
Licencjonowanie i koszty związane z wdrożeniem zaawansowanych funkcji zabezpieczeń	488
Usługa Microsoft Defender for Servers — Plan 1 i Plan 2	489
Wdrażanie najlepszych praktyk bezpieczeństwa w systemie	
Windows Server 2025	490
Zarządzanie aktualizacjami	491
Rejestrowanie zdarzeń audytowych	493
Dlaczego regularne oceny bezpieczeństwa są tak ważne?	494
Wymagania i proces integracji usługi Microsoft Defender for Endpoint w systemie Windows Server 2025	495
Komentarz na temat bazowych konfiguracji zabezpieczeń i monitorowania dryfu ustawień	497
Ćwiczenia — konfigurowanie reguł zapory sieciowej, włączanie szyfrowania TLS oraz konfigurowanie dzienników audytu	498
Ćwiczenie 11.1 — konfigurowanie reguł zapory sieciowej	499
Ćwiczenie 11.2 — włączanie szyfrowania TLS	500
Ćwiczenie 11.3 — konfigurowanie dzienników inspekcji	501
Podsumowanie	502
Pytania	503
Gdzie warto zajrzeć?	504

ROZDZIAŁ 12

Zarządzanie aktualizacjami w systemie Windows Server 2025:

hotpatching, Azure Arc i inne rozwiązania	506
Wymagania techniczne	507
Wprowadzenie do aktualizowania serwerów „na gorąco” z użyciem Azure Arc w systemie Windows Server 2025	507
Hotpatching — instalowanie aktualizacji w locie	508
Dlaczego warto korzystać z Azure Arc?	510
Kompatybilność systemu Windows Server 2025	511
Hotpatching — instalowanie poprawek i aktualizacji w locie	513
Przygotowania do instalowania aktualizacji w locie	514
Instalowanie poprawek i aktualizacji w locie	517
Weryfikacja po zainstalowaniu aktualizacji	519

Efektywne zarządzanie aktualizacjami i cyklem życia serwerów	522
Strategie zarządzania cyklem życia serwerów	522
Automatyzacja zarządzania aktualizacjami	524
Monitorowanie i raportowanie	526
Rozwiązywanie problemów z instalowaniem aktualizacji w locie	528
Typowe problemy i ich rozwiązania	529
Narzędzia i techniki diagnostyczne	530
Najlepsze praktyki rozwiązywania problemów	533
Ćwiczenie 12.1 — konfigurowanie Azure Arc w systemie Windows Server 2025	535
Podsumowanie	538
Pytania	538
Gdzie warto zajrzeć?	540

CZĘŚĆ 5. Konserwacja systemu Windows Server 2025 i zarządzanie nim

ROZDZIAŁ 13

Optymalizacja i konserwacja systemu Windows Server 2025	543
Wymagania techniczne	544
Komponenty sprzętowe serwera i ich funkcje w systemie Windows Server 2025	544
Procesor	544
Pamięć operacyjna	546
Dyski twarde	547
Interfejsy sieciowe	548
Różnice między architekturą 32- i 64-bitową	549
Dyski zewnętrzne	550
Wpływ zewnętrznych dysków USB na wydajność serwera	551
Karty graficzne	552
Układy chłodzenia	553
Zasilacze	554
Porty fizyczne	555
Narzędzia i metody monitorowania wydajności w systemie Windows Server 2025	556
Metodyczne podejście do monitorowania wydajności	557
Wdrażanie procedur monitorowania wydajności	558
Określanie punktu odniesienia wydajności serwera	559

Wykorzystanie monitora wydajności, monitora zasobów i menedżera zadań do optymalizacji wydajności	560
Performance Monitor	560
Resource Monitor	562
Task Manager	564
Monitorowanie serwerów z użyciem Azure Monitor na platformie Arc ...	565
Wykorzystanie liczników wydajności do optymalizacji pracy serwera	567
Tworzenie zestawów Data Collector Set	567
Rola dzienników wydajności i alertów	569
Ćwiczenie 13.1 — usługa dzienników wydajności i alertów	570
Uruchamianie usługi Performance Logs & Alerts	570
Folder PerfLogs	571
Tworzenie dzienników danych wydajności	572
Tworzenie alertów dla liczników wydajności	573
Podsumowanie	574
Pytania	575
Gdzie warto zajrzeć?	576

ROZDZIAŁ 14

Aktualizowanie Windows Server 2025

i rozwiązywanie problemów z systemem 577

Wymagania techniczne	578
Zarządzanie aktualizacjami systemu operacyjnego, sterowników i aplikacji w środowisku Windows Server 2025	578
Aktualizacje systemu Windows Server	578
Instalowanie aktualizacji w systemie Windows Server 2025	580
Aktualizowanie aplikacji firmy Microsoft	581
Aktualizowanie programów innych firm	582
Aktualizowanie aplikacji z użyciem polecenia Winget	583
Konfigurowanie usługi Windows Update do sprawdzania i aktualizowania sterowników urządzeń	585
Usługa WSUS	587
Metodyka i najlepsze praktyki rozwiązywania problemów	588
Najlepsze praktyki, wytyczne i procedury	589
Jak skutecznie rozwiązywać problemy techniczne?	589
Porównanie systematycznego i ukierunkowanego podejścia do rozwiązywania problemów	590
Procedury rozwiązywania problemów	591
Czym jest ITIL?	592

Wdrażanie strategii ciągłości działania	
w środowiskach Windows Server 2025	592
Czym jest DRP?	593
Różnice między ciągłością działania a odzyskiwaniem po awarii	594
Jak działa redundancja danych?	595
Czym jest klastrowanie?	595
Zapewnienie ciągłości działania przez tworzenie kopii zapasowych, odtworzenie danych i planowanie odzyskiwania po awarii	596
Tworzenie kopii zapasowych i odzyskiwanie danych	597
Odzyskiwanie danych Active Directory	599
Jak działa usługa Volume Shadow Copy?	601
Przekierowanie folderów	602
Redundancja zasilania	603
Wdrażanie planu odzyskiwania po awarii w środowisku Windows Server 2025	604
Wykorzystanie programu Event Viewer do monitorowania dzienników systemowych i rozwiązywania problemów	606
Event Viewer	606
Ćwiczenie 14.1 — wykorzystanie programu Event Viewer do monitorowania dzienników zdarzeń i zarządzania nimi	608
Konfigurowanie scentralizowanego monitorowania w systemie Windows Server 2025	608
Jak stosować filtry dzienników w programie Event Viewer?	610
Jak zmienić domyślną lokalizację plików dziennika?	611
Podsumowanie	612
Pytania	612
Gdzie warto zajrzeć?	613

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

ROZDZIAŁ 15

Certyfikacje Microsoft i przygotowanie do egzaminu AZ-800	617
Wartość certyfikacji Microsoft	618
Wpływ certyfikacji Microsoft opartych na rolach	619
Określenie grupy docelowej certyfikacji Microsoft	620
Umiejętności sprawdzane na egzaminach certyfikacyjnych Microsoft	622
Przygotowanie do egzaminu AZ-800	622
Wdrażanie usług Active Directory Domain Services (AD DS) i zarządzanie nimi w środowiskach lokalnych i chmurowych (30 – 35%) ...	624

Zarządzanie serwerami Windows i obciążeniami w środowisku hybrydowym (10 – 15%)	625
Zarządzanie maszynami wirtualnymi i kontenerami (15 – 20%)	627
Wdrażanie infrastruktury sieciowej oraz zarządzanie nią w środowiskach lokalnych i hybrydowych (15 – 20%)	628
Zarządzanie usługami pamięci masowej i plików (15 – 20%)	630
Strategie sukcesu i wskazówki dotyczące przygotowania do certyfikacji Microsoft	631
Źródła wiedzy przydatne w przygotowaniu do certyfikacji Microsoft	632
Jak zarejestrować się na egzamin certyfikacyjny Microsoft?	634
Wskazówki na dzień egzaminu certyfikacyjnego	635
Nowe wymagania dotyczące ważności i odnawiania certyfikatów Microsoft	636
Podsumowanie	637
Gdzie warto zajrzeć?	638

DODATEK

Odpowiedzi na pytania	639
Rozdział 1. Podstawy sieci komputerowych i wprowadzenie do systemu Windows Server 2025	639
Rozdział 2. Instalowanie systemu Windows Server 2025	640
Rozdział 3. Co zrobić po zainstalowaniu systemu Windows Server 2025? ...	641
Rozdział 4. Usługi katalogowe w systemie Windows Server 2025	641
Rozdział 5. Dodawanie ról serwera w systemie Windows Server 2025	642
Rozdział 6. Zasady grupy w systemie Windows Server 2025	643
Rozdział 7. Wirtualizacja w systemie Windows Server 2025	644
Rozdział 8. Przechowywanie danych w systemie Windows Server 2025	645
Rozdział 9. Rozszerzenia i ulepszenia usługi Active Directory Domain Services (AD DS)	646
Rozdział 10. Konfigurowanie protokołu SMB over QUIC w systemie Windows Server 2025	647
Rozdział 11. Przegląd nowych mechanizmów bezpieczeństwa w systemie Windows Server 2025	648
Rozdział 12. Zarządzanie aktualizacjami w systemie Windows Server 2005: hotpatching, Azure Arc i inne rozwiązania	649
Rozdział 13. Optymalizacja i konserwacja systemu Windows Server 2025 ...	650
Rozdział 14. Aktualizowanie Windows Server 2025 i rozwiązywanie problemów z systemem	651
Skorowidz	653

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 rolę 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.

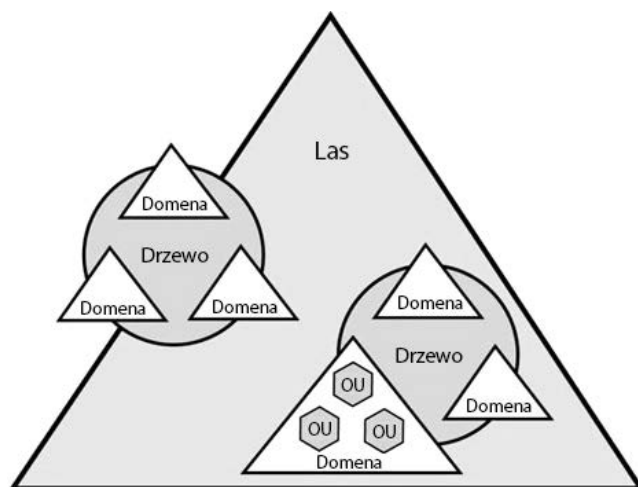
Analiza infrastruktury Active Directory w środowisku Windows Server 2025

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 urzędzeń 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 lokalizacjami 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.

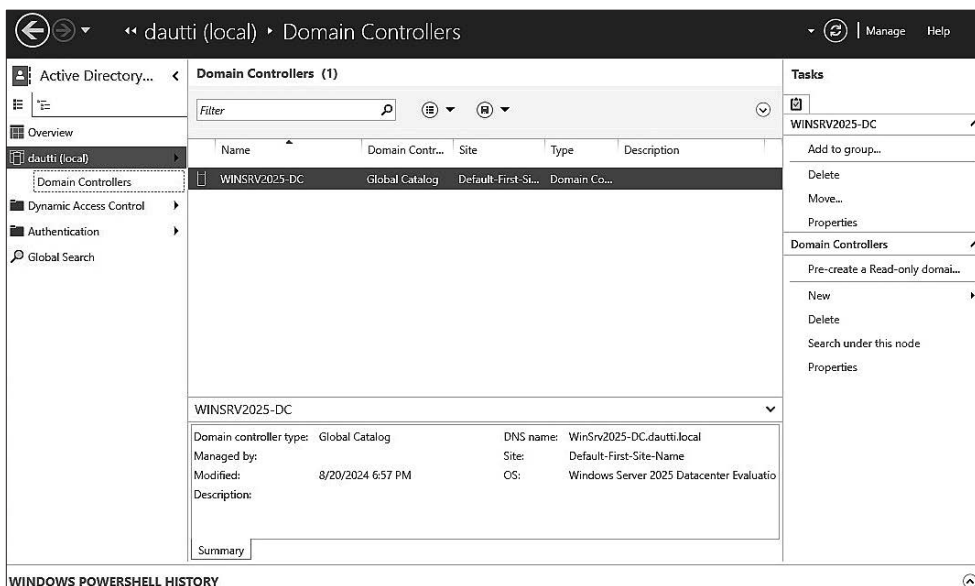
W następnym podrozdziale omówimy kluczowe komponenty infrastruktury Active Directory, począwszy od szczegółowej analizy kontrolerów domeny, które stanowią fundament każdego środowiska AD.

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 lokalizacje 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.

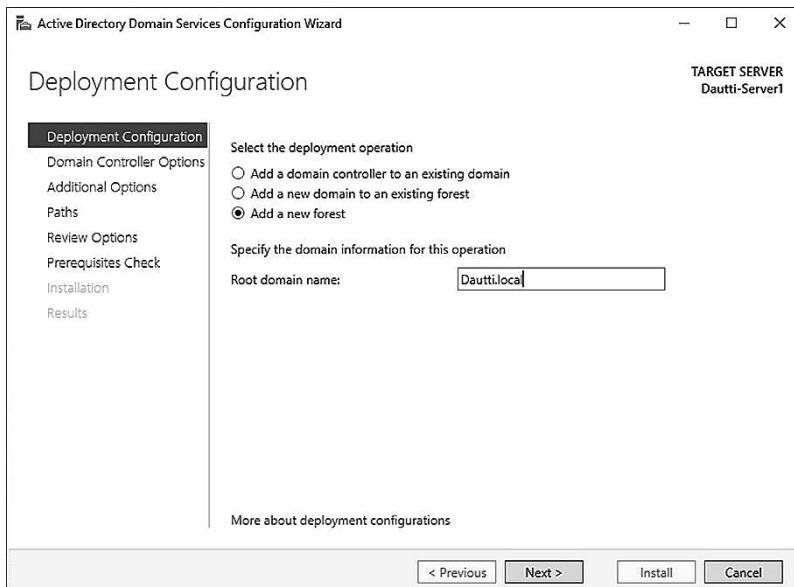
Uwaga

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

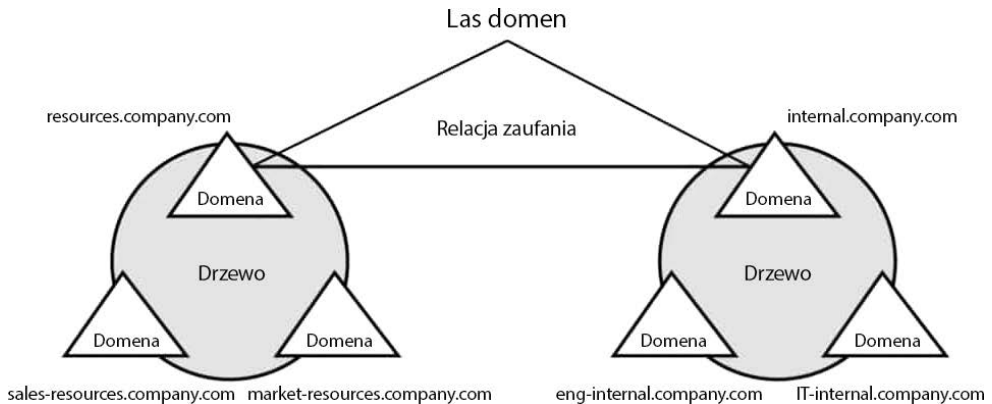
Trzeba wprowadzić rozróżnienie między domeną katalogową (ang. *directory domain*) a nazwą domeny (ang. *domain name*). W kontekście usług katalogowych termin domena odnosi się do ustrukturyzowanej bazy danych zasobów sieciowych, obejmującej zasoby sieciowe, takie jak konta użytkowników, serwery i urządzenia. 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.

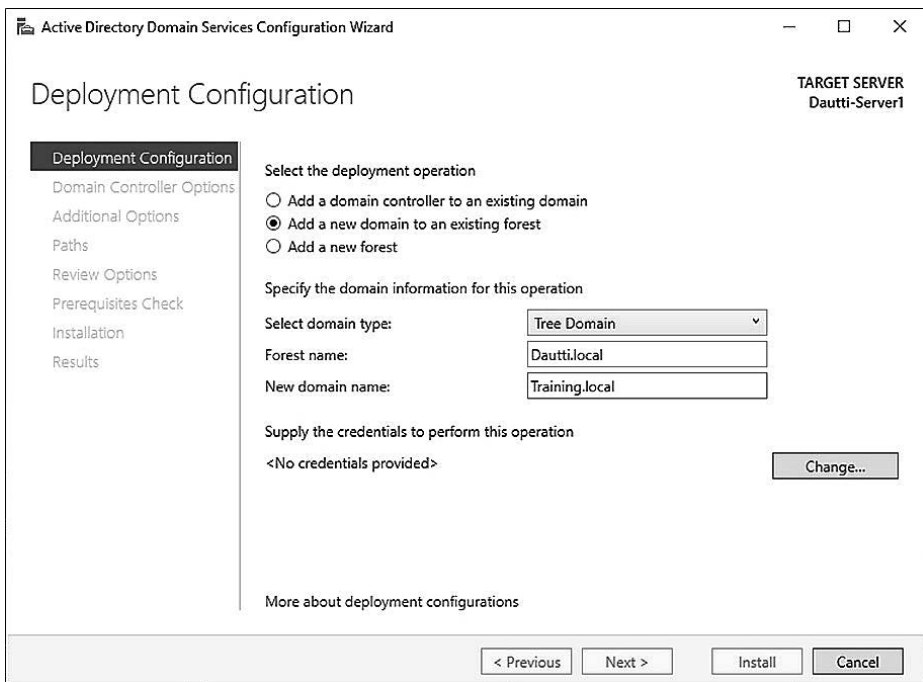
Drzewa domen

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.

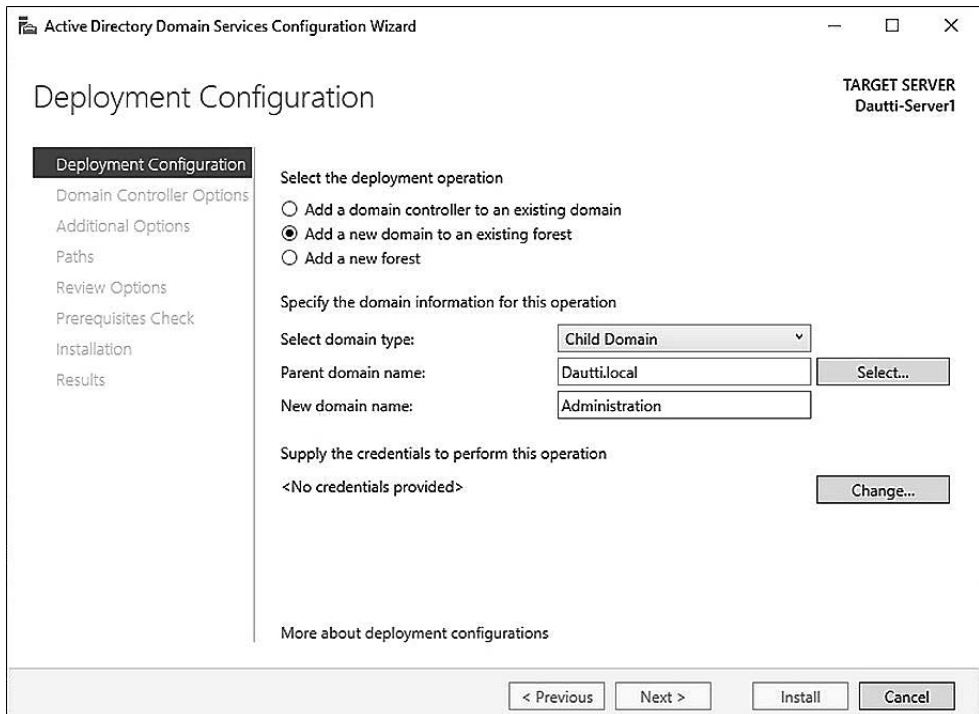
Aby utworzyć i skonfigurować las w środowisku Windows Server 2025, możesz wykorzystać kreatora konfiguracji usług domenowych AD DS (ang. *Active Directory Domain Services Configuration Wizard*), który służy również do definiowania struktury domen w obrębie drzewa. Kreator prowadzi administratora przez 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.

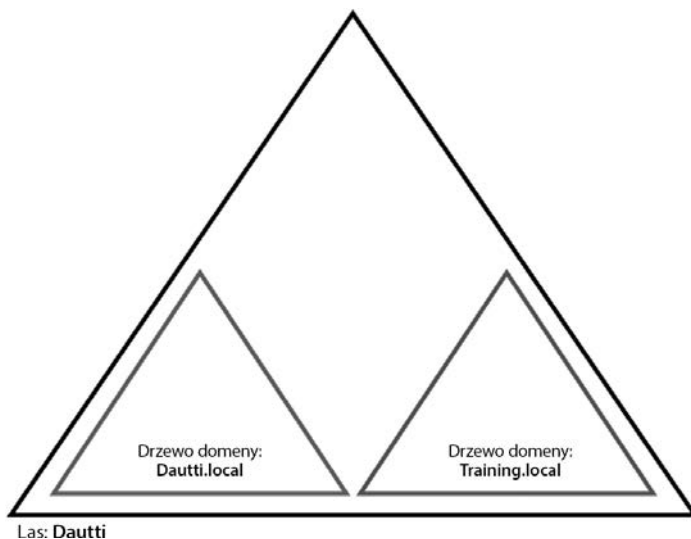
W poprzednim punkcie utworzyliśmy domenę główną `Dautti.local`, pełniącą funkcję podstawowej domeny dla całego lasu Active Directory. Domena ta jest hostowana na serwerze, który odgrywa również rolę kontrolera domeny (ang. *domain controller* — DC) i odpowiada za nadzorowanie i obsługę usług katalogowych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

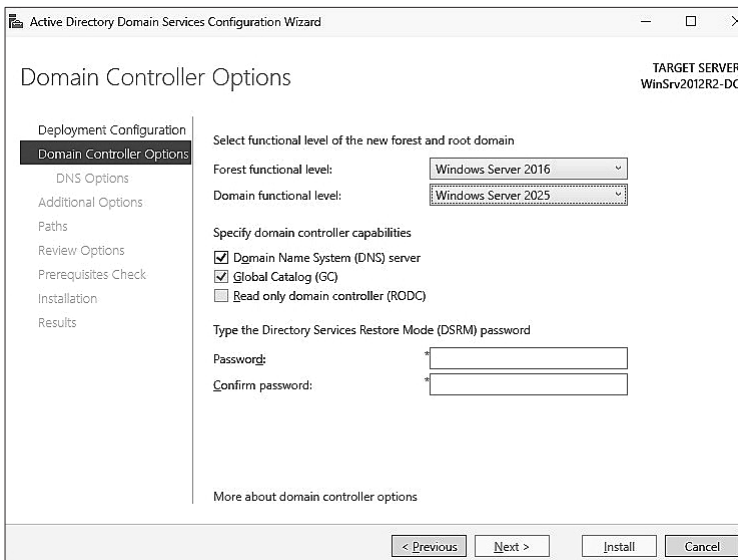
i spójnych ram bezpieczeństwa. Na przykład, jak pokazano na rysunku 4.6, jeżeli domena `Dautti.local` przeprowadzi pomyślne uwierzytelnienie użytkownika, to wynik tego procesu jest domyślnie akceptowany przez inną domenę w tym samym lesie, taką jak `Training.local`. Mechanizm ten opiera się na wspólnej 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

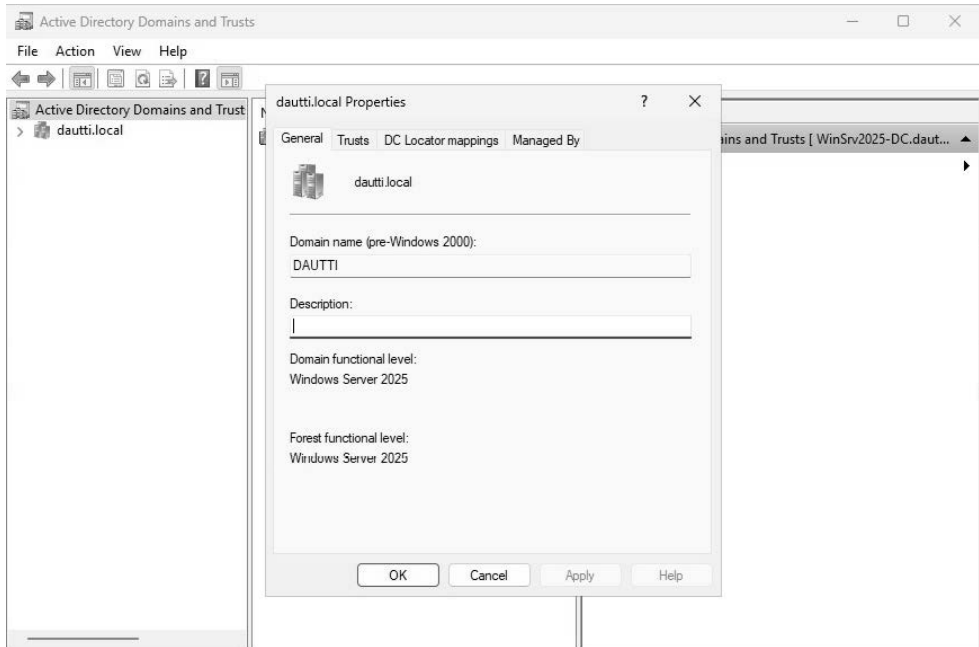
- **Poziom funkcjonalny lasu** (ang. *Forest Functional Level* — FFL) — odgrywa kluczową rolę w określaniu, które wersje systemu Windows Server mogą działać na kontrolerach domeny w obrębie całego lasu, czyli najwyższej struktury w Active Directory, obejmującej jedną lub wiele domen. Ustawienie poziomu 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 koszt 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.



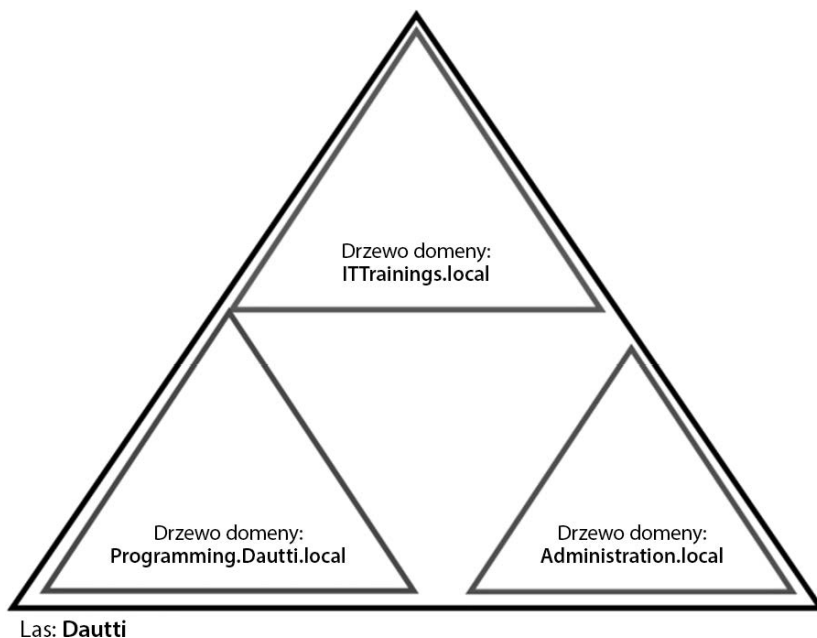
Rysunek 4.10. Weryfikowanie poziomów funkcjonalnych domeny i lasu

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 hasle, 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 przyjrzemy 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

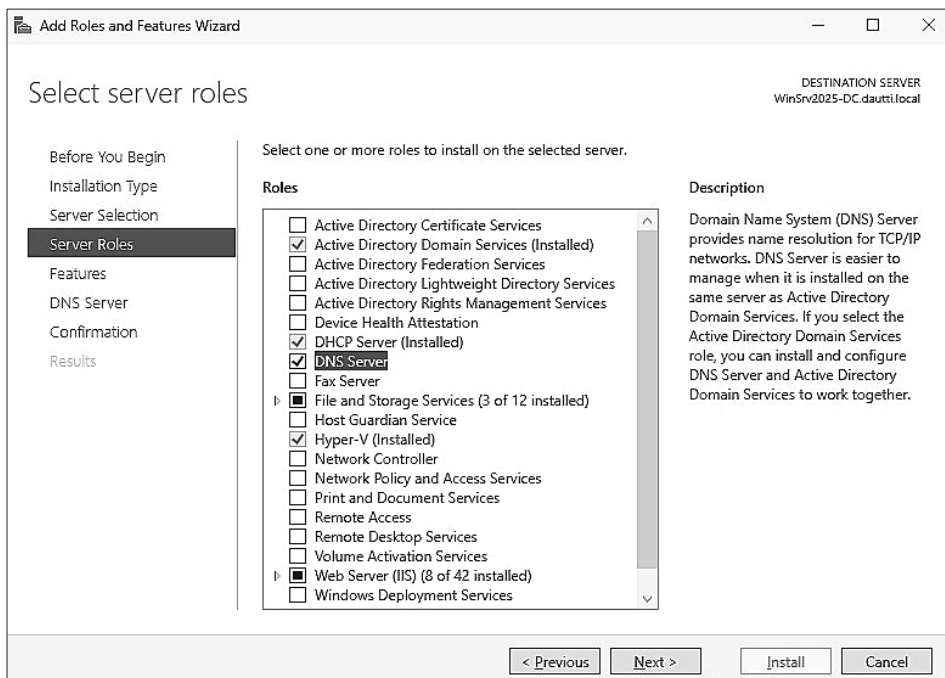
Aby w pełni zrozumieć, jak działa system DNS, warto przeanalizować sekwencję działań, które mają miejsce podczas próby dostępu do wybranej strony internetowej. DNS odgrywa kluczową rolę w tłumaczeniu nazw domen zrozumiałych dla człowieka na adresy IP interpretowane przez komputery, co umożliwia komunikację 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 w zapewnieniu niezawodnego dostępu do zasobów internetowych.

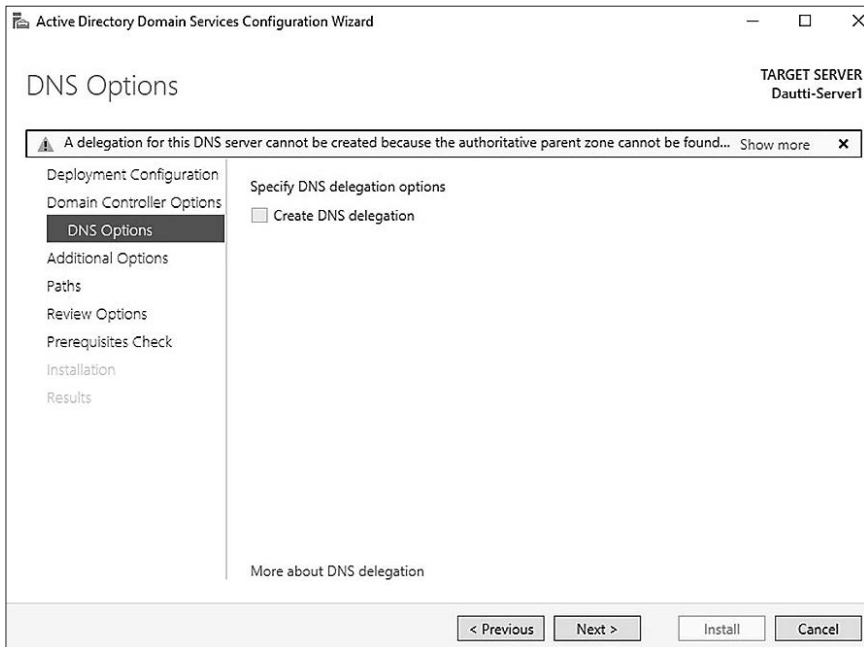
Instalowanie roli DNS

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:

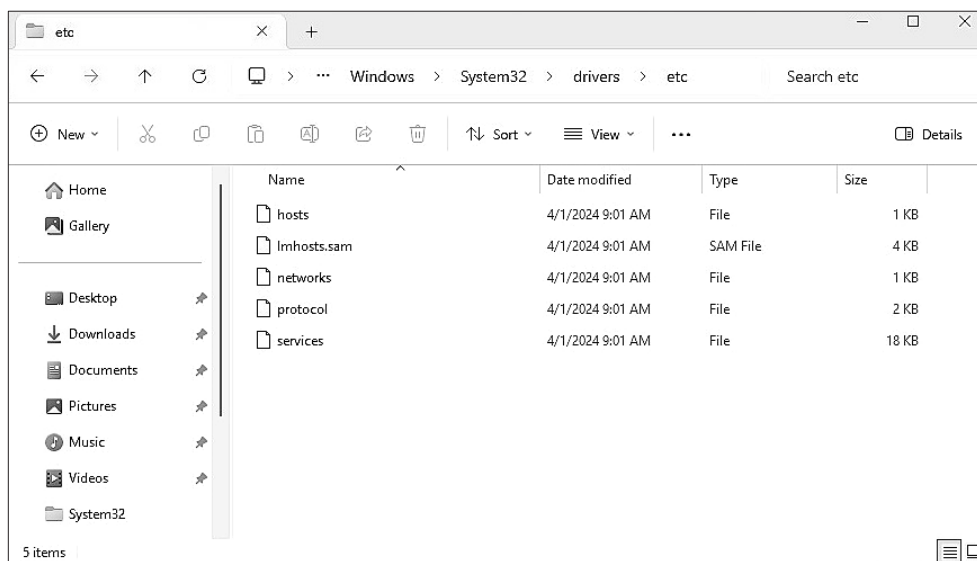
- **Plik *hosts*:** ten plik działa jako statyczne i konfigurowalne narzędzie mapowania, które umożliwia przypisywanie konkretnych adresów IP do nazw hostów. Dzięki temu możliwe staje się lokalne rozwiązywanie nazw DNS, co pozwala identyfikować urządzenia w sieci za pomocą przyjaznych dla użytkownika

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 umożliwi 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 skonfigurowany 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.

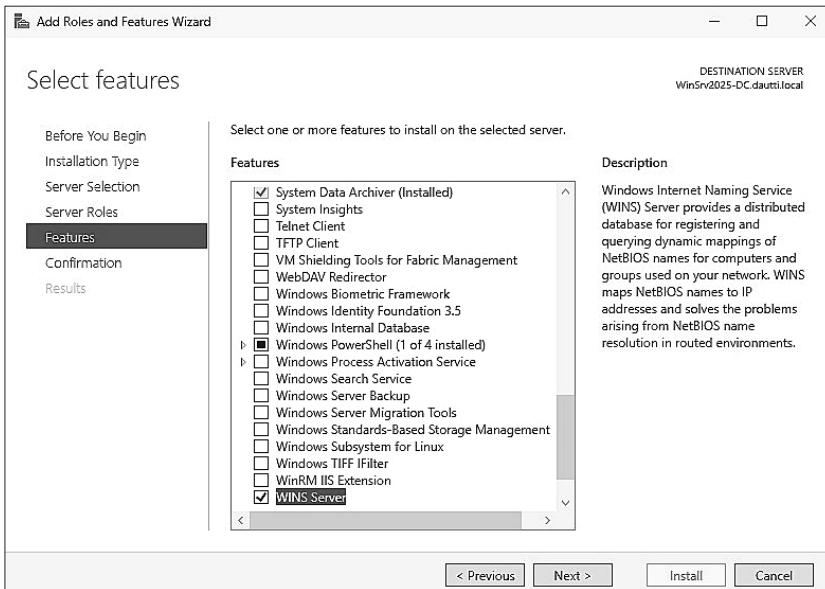
Oprócz skonfigurowania stref DNS istotne jest także poznanie działania usługi WINS, będącej wcześniejszym mechanizmem mapowania nazw NetBIOS na adresy IP. Mimo że w nowoczesnych środowiskach sieciowych funkcję tę w dużej mierze przejął DNS, WINS nadal odgrywa ważną rolę tam, gdzie wykorzystuje się starsze 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.

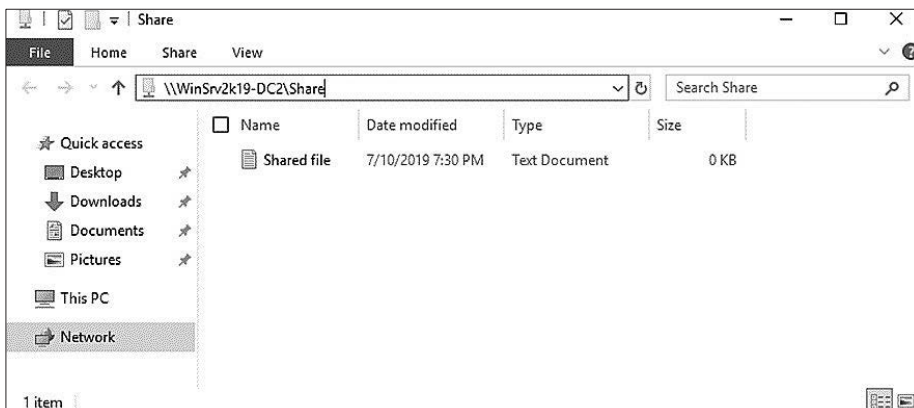
Oprócz zasad działania usługi WINS warto również poznać **konwencję UNC** (ang. *Universal Naming Convention*), która jest szczegółowo omówiona w następnym punkcie.



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 środowiska 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

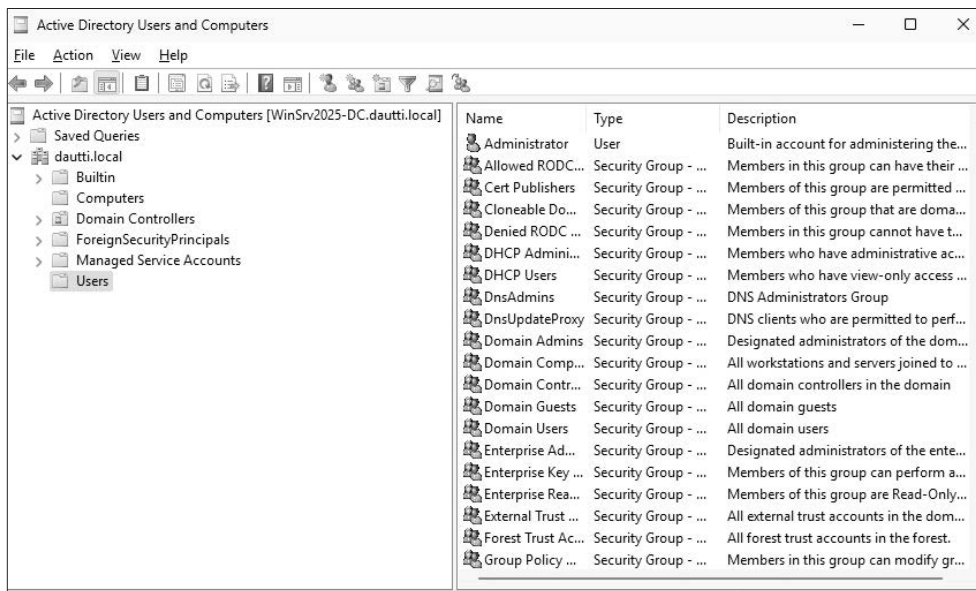
Dobra znajomość funkcji jednostek organizacyjnych (ang. *Organizational Units* — OU) i kontenerów jest niezbędna do efektywnego zarządzania usługą Active Directory. Oba komponenty, dostępne za pośrednictwem konsoli **Active Directory Users and Computers**, są niezbędne do organizowania obiektów katalogu 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.

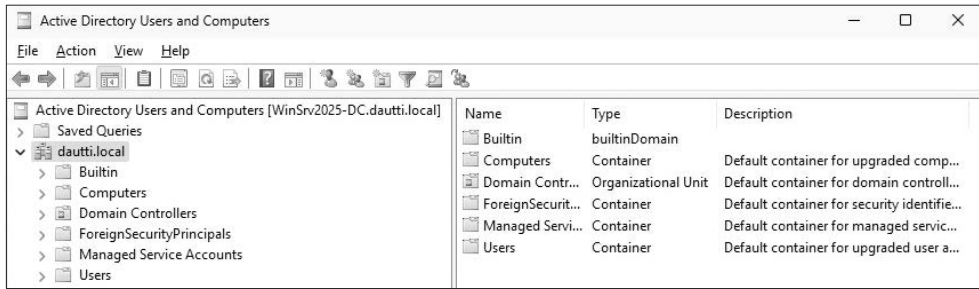


Rysunek 4.18. Przykładowa hierarchia jednostek organizacyjnych (OU) w Windows Server 2025

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 niezmiennosc 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.

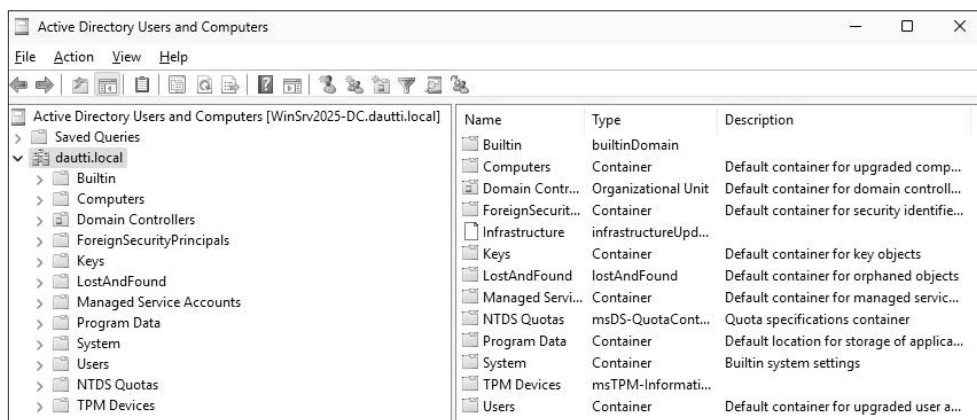
W kolejnych punktach skupimy się na koncepcji ukrytych kontenerów domyślnych. Choć nie są one widoczne w standardowym interfejsie Active Directory, odgrywają istotną rolę w działaniach systemowych i ogólnym funkcjonowaniu AD. Zrozumienie zarówno **jawnych, jak i ukrytych kontenerów domyślnych** pozwala 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:

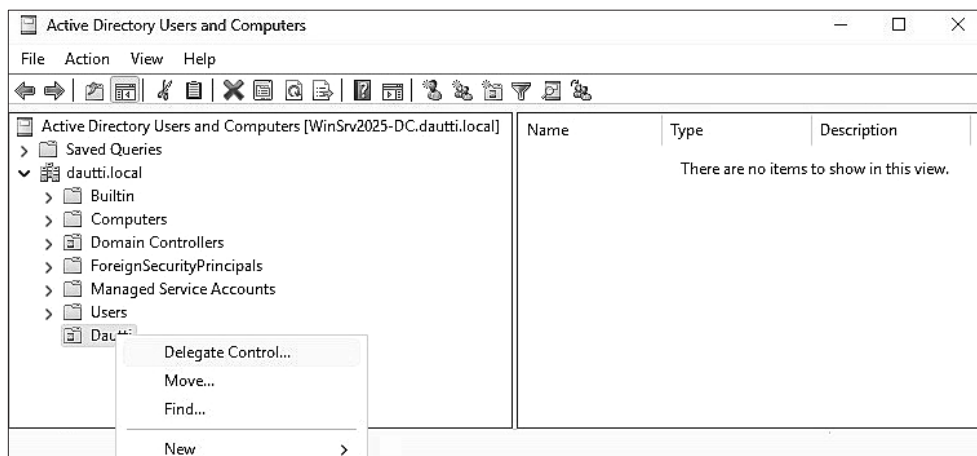
- **Computers** — domyślny kontener przeznaczony do przechowywania nowo utworzonych kont komputerów, zapewniający centralne miejsce do przechowywania tych obiektów.
- **Domain Controllers** — specjalnie zaprojektowany kontener służący do przechowywania kont kontrolerów domeny. Ułatwia ich organizację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

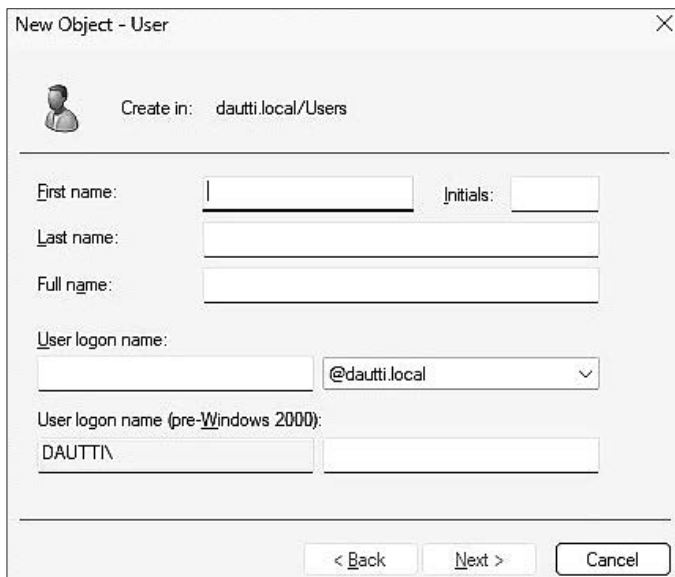
zasady i przydzielać uprawnienia zbiorczo, zamiast konfigurować je indywidualnie. Takie podejście przekłada się na większą efektywność operacyjną oraz podnosi poziom bezpieczeństwa. W kolejnych punktach szczegółowo omówimy różne typy kont i grup oraz ich funkcje i praktyczne zastosowanie w Active Directory. 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*.



New Object - User

Create in: dautti.local/Users

First name: Initials:

Last name:

Full name:

User logon name: @dautti.local

User logon name (pre-Windows 2000): DAUTTI\

< Back Next > Cancel

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

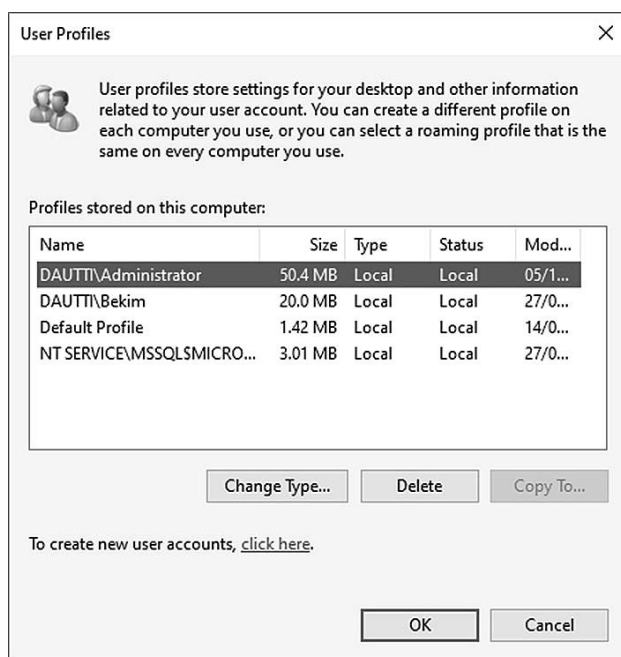
Konta lokalne są przechowywane i uwierzytelniane przez menedżera SAM na lokalnym komputerze, co zapewnia egzekwowanie kontroli dostępu i uprawnień niezależnie od domeny sieciowej. Takie rozwiązanie jest szczególnie przydatne w sytuacjach, w których potrzebna jest lokalna administracja i lokalne zarządzanie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

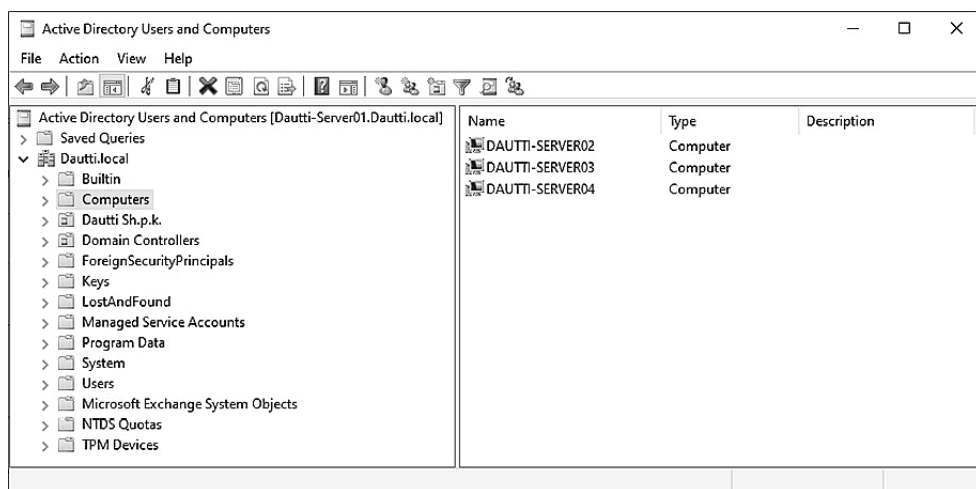
Podsumowując, profile lokalne są przypisane do pojedynczych komputerów, profile mobilne zapewniają elastyczność dzięki dostępności z dowolnego urządzenia w sieci, a profile obowiązkowe gwarantują spójność, ponieważ odrzucają wszelkie zmiany wprowadzane przez użytkownika i opierają się na stałym szablonie. 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 hasła, 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.

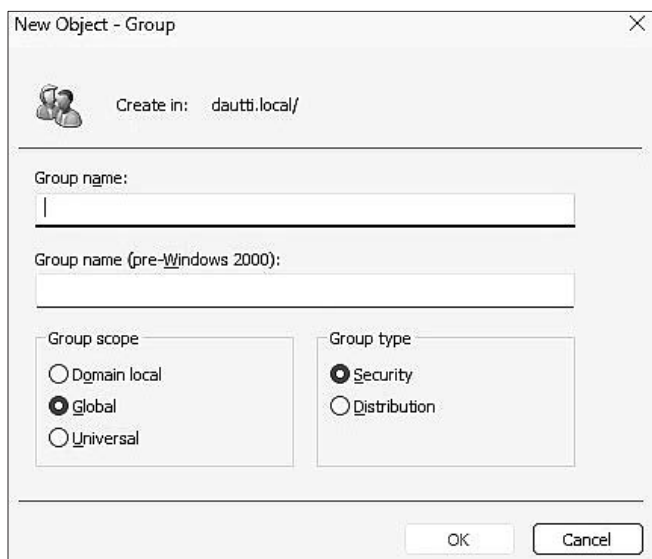
W następnym punkcie skupimy się na grupach w usłudze Active Directory. Są one integralną częścią zarządzania uprawnieniami i prawami dostępu, upraszczają przydzielanie ról i uprawnień oraz usprawniają realizowanie zadań administracyjnych. Grupy pomagają w organizowaniu użytkowników i komputerów, stosowaniu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



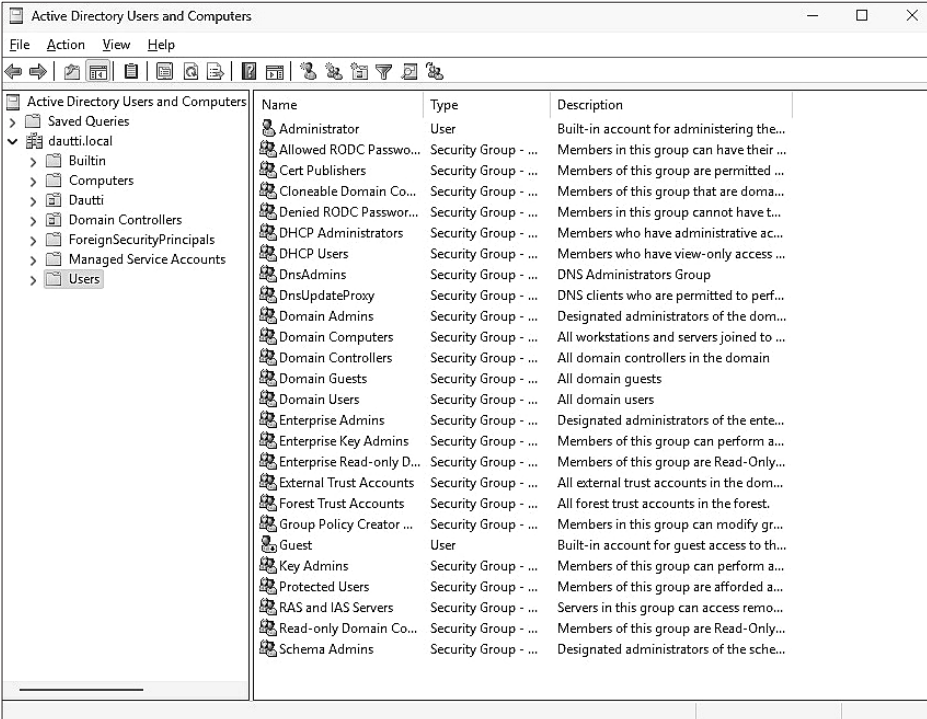
Rysunek 4.26. Typy grup w systemie Windows Server 2025

- **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.



Name	Type	Description
Administrator	User	Built-in account for administering the...
Allowed RODC Passwo...	Security Group - ...	Members in this group can have their ...
Cert Publishers	Security Group - ...	Members of this group are permitted ...
Cloneable Domain Co...	Security Group - ...	Members of this group that are doma...
Denied RODC Passwor...	Security Group - ...	Members in this group cannot have t...
DHCP Administrators	Security Group - ...	Members who have administrative ac...
DHCP Users	Security Group - ...	Members who have view-only access ...
DnsAdmins	Security Group - ...	DNS Administrators Group
DnsUpdateProxy	Security Group - ...	DNS clients who are permitted to perf...
Domain Admins	Security Group - ...	Designated administrators of the dom...
Domain Computers	Security Group - ...	All workstations and servers joined to ...
Domain Controllers	Security Group - ...	All domain controllers in the domain
Domain Guests	Security Group - ...	All domain guests
Domain Users	Security Group - ...	All domain users
Enterprise Admins	Security Group - ...	Designated administrators of the ente...
Enterprise Key Admins	Security Group - ...	Members of this group can perform a...
Enterprise Read-only D...	Security Group - ...	Members of this group are Read-Only...
External Trust Accounts	Security Group - ...	All external trust accounts in the dom...
Forest Trust Accounts	Security Group - ...	All forest trust accounts in the forest.
Group Policy Creator ...	Security Group - ...	Members in this group can modify gr...
Guest	User	Built-in account for guest access to th...
Key Admins	Security Group - ...	Members of this group can perform a...
Protected Users	Security Group - ...	Members of this group are afforded a...
RAS and IAS Servers	Security Group - ...	Servers in this group can access remo...
Read-only Domain Co...	Security Group - ...	Members of this group are Read-Only...
Schema Admins	Security Group - ...	Designated administrators of the sche...

Rysunek 4.27. Domyślne grupy AD w systemie Windows Server 2025

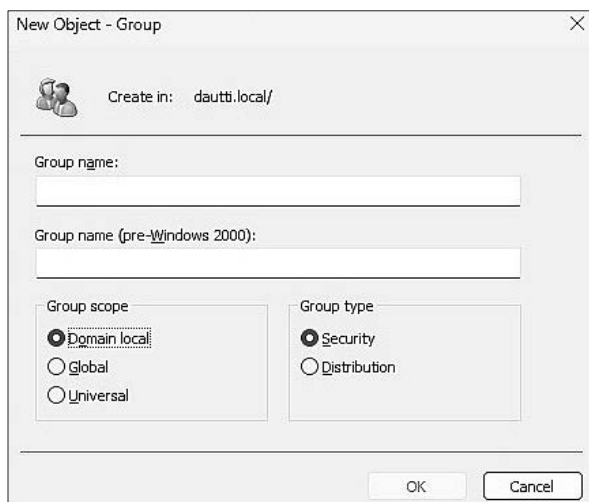
Domyślne grupy są wstępnie skonfigurowane z określonymi rolami i uprawnieniami, co znacznie usprawnia zarządzanie środowiskiem sieciowym. Na przykład grupy takie jak **Domain Admins**, **Enterprise Admins** i **Schema Admins** mają predefiniowane poziomy uprawnień administracyjnych, które są kluczowe 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 zagnieżdżenia 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

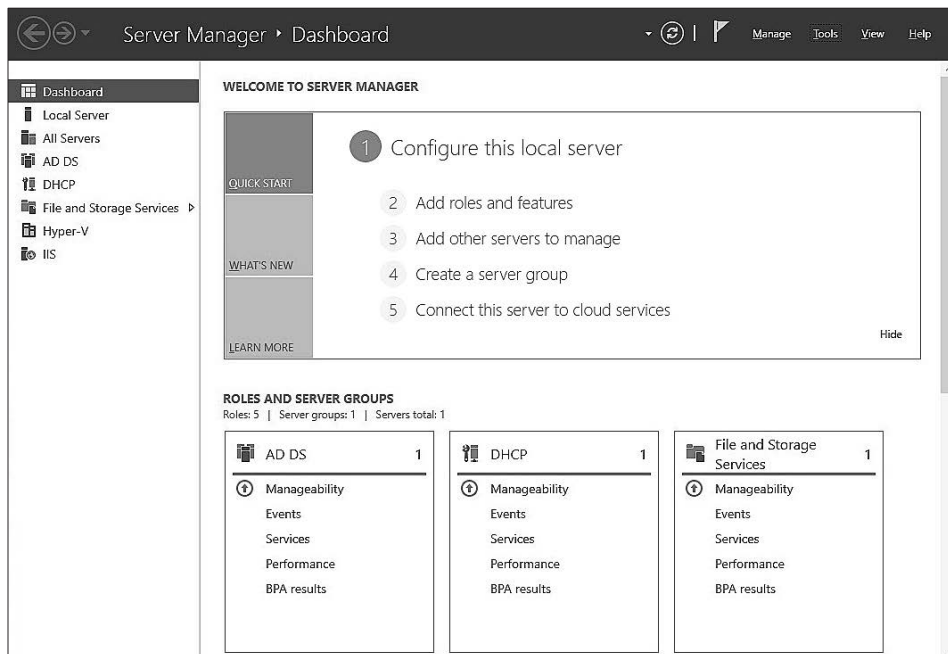
W ramach tego ćwiczenia przejdziesz przez najważniejsze etapy instalowania ról AD DS i DNS, zakończone promowaniem serwera do roli pełnoprawnego kontrolera domeny. Proces ten stanowi fundament budowy bezpiecznej i wydajnej infrastruktury sieciowej w każdej organizacji wykorzystującej usługę Active Directory.

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.

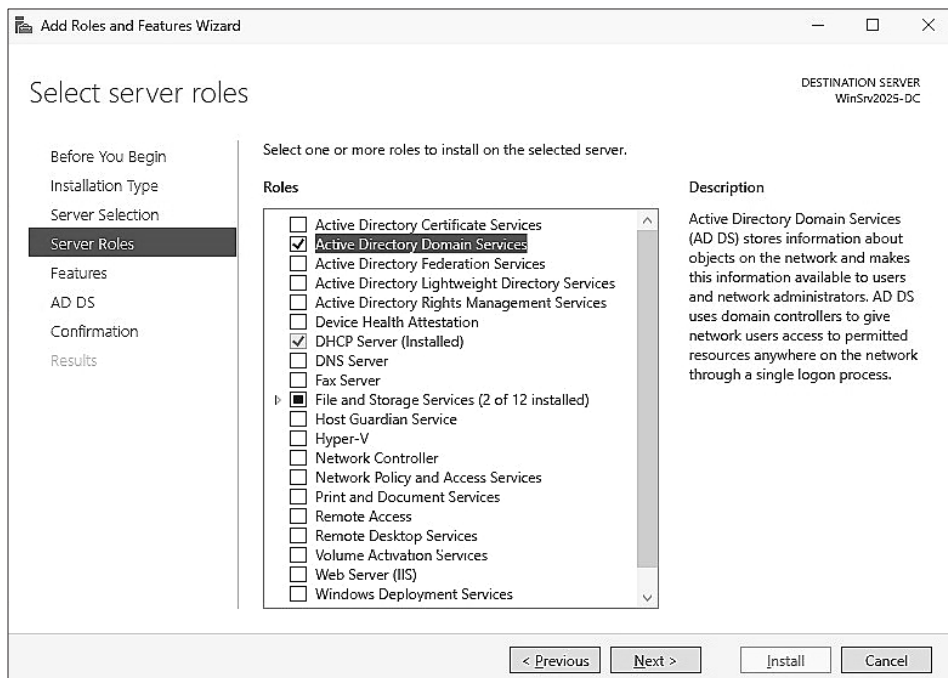
Postępując zgodnie ze szczegółowymi instrukcjami zamieszczonymi poniżej, zdobędziesz niezbędną wiedzę na temat wdrażania i konfiguracji ról AD DS i DNS, co pozwoli Ci na zbudowanie solidnej i dobrze zorganizowanej infrastruktury sieciowej. Ćwiczenie to nie tylko rozwija umiejętności praktyczne, ale również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

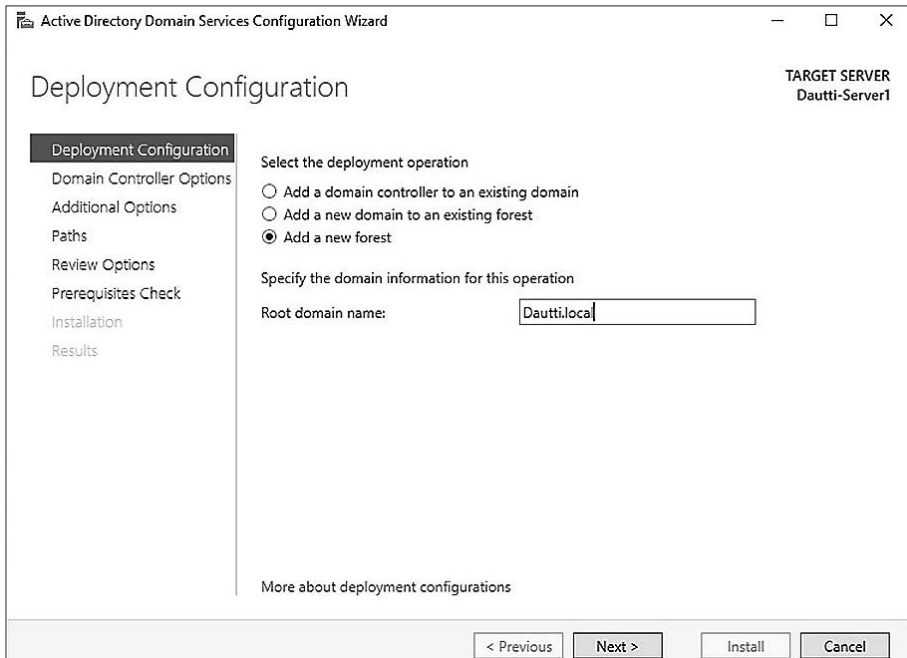


Rysunek 4.29. Dodawanie ról i funkcji do serwera z użyciem aplikacji Server Manager



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, umożliwiającą 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. Przyjrzeliliśmy 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

- Active Directory, AD, 158
 - aktualizacje schematów, 401
 - diagnozowanie problemów, 406
 - dla Windows PowerShell, 162
 - DNS, 161
 - domeny podrzędne, 168
 - drzewa domen, 166
 - działanie systemu, 181
 - grupy domyślne, 201
 - instalowanie roli, 182
 - jednostki organizacyjne, 189
 - konfigurowanie roli, 163
 - konta
 - domenowe, 195
 - komputerów, 199
 - lokalne, 196
 - kontenery domyślne, 190
 - lasy domen, 168
 - lokacje, 177
 - narzędzia diagnostyczne, 410
 - odzyskiwanie danych, 599
 - profile użytkowników, 197
 - projektowanie schematów, 403
 - protokół
 - Kerberos, 161
 - LDAP, 160
 - replikacja, 178
 - schemat, 179
 - typy grup, 200
 - ukryte kontenery domyślne, 191
 - usługi wspierające, 160
 - utrzymywanie schematów, 403
 - zagnieżdżanie grup, 204
 - zakresy grup, 202
 - zarządzanie
 - grupami, 194
 - obiektami, 405
 - usługą, 161
 - użytkownikami, 194
- Active Directory Administrative Center, AD AC, 161
- Active Directory Certificate Services, AD CS, 213
- Active Directory Domain Services, AD DS, 51, 54, 157, 169, 387
 - koncepcja przestrzeni nazw, 175
 - odzyskiwanie danych, 399
 - replikacje, 398
 - role głównych operacji, 169
 - skalowalność, 397
 - tworzenie kopii zapasowych, 399
 - ulepszenia, 389
 - ulepszenia zabezpieczeń, 392
- Active Directory Federation Services, AD FS, 237
- adres
 - IPv4, 38, 41
 - konfiguracja, 142, 149
 - IPv6, 42
 - URL, 227
- aktualizacje, 143, 150, 491, 506, *Patrz także*
 - hotpatching
 - automatyzacja zarządzania, 524
 - instalowanie, 580
 - usługa Windows Update, 578
 - zarządzanie, 578
 - zarządzanie efektywne, 522
- aktualizowanie
 - aplikacji, 581
 - innych firm, 582
 - z użyciem polecenia Winget, 583
 - sterowników urządzeń, 585
- aktywacja systemu, 146, 151
- alerty, 569, 570, 573
- analiza plików dzienników, 84
- antywirus, 468
- aplikacja, *Patrz* narzędzie
- App-V, 244
- architektura
 - 32-bitowa, 549
 - 64-bitowa, 549

architektura
 Hyper-V, 302, 303
 klient-serwer, 32, 40
 OAuth, 479
 peer-to-peer, 39
 ASP, Active Server Pages, 224
 atrybuty, attributes, 179
 ATSC, Automated Tiered Storage Control, 355
 audyt, 258, 493
 wydajności, 441
 zasady, 258
 autoryzacja, 472
 awarie usług, 126
 Azure, 102
 Arc, 506
 aktualizacje w locie, 508
 integrowanie platformy, 510
 klastry Kubernetes, 512
 konfigurowanie, 509, 535
 Monitor, 565
 Update Manager, 524

B

BaaS, backup as service, 598
 baza danych
 AD, 397, 413
 BCD, 74
 BCD, Boot Configuration Data, 73
 bezpieczeństwo, 54, 135, 458
 aktualizacje, 491
 bazowe konfiguracje zabezpieczeń, 497
 cyfrowe, 433
 danych, 426
 dostęp warunkowy, 476
 kontrola dostępu, 459
 koszty, 488
 Microsoft Defender
 Antivirus, 468
 for Endpoint, 495
 for Servers, 489
 monitorowanie, 485
 najlepsze praktyki, 435, 490
 protokół
 HTTPS, 483
 IPsec, 483
 OAuth 2.0, 478, 480
 SSH, 484
 TLS, 481, 500
 regularne oceny, 494
 reguły zapory sieciowej, 498
 rejestrowanie zdarzeń audytowych, 493
 uwierzytelnianie biometryczne, 473, 475

uwierzytelnianie i autoryzacja, 472
 zaawansowane mechanizmy, 486
 zaawansowane wykrywanie zagrożeń, 464
 zasady dostępu warunkowego, 477
 zautomatyzowane systemy reagowania, 469
 BIOS, Basic Input/Output System, 65
 opcje uruchamiania, 69
 BitLocker, 64, 71
 błędy
 instalacji systemu, 78
 konfiguracji dysków, 78
 Boot Manager, 73
 bootloader, 73, 75

C

CA, certificate authority, 427
 certyfikacje Microsoft, 618
 grupa docelowa, 620
 oparte na rolach, 619
 ważności i odnawiania, 636
 certyfikaty
 cyfrowe, digital certificates, 234, 427
 unieważnione, CRL, 427
 chmura obliczeniowa, 296
 ciągła integracja i ciągłe dostarczanie, CI/CD, 526
 ciągłość działania, business continuity, 594, 596
 CPU, Central Processing Unit, 44, 544
 CRL, certificate revocation list, 427
 CSM, Compatibility Support Module, 76
 cykl życia serwerów, 522

D

DAS, Direct-Attached Storage, 341
 DC, domain controller, 164
 deduplikacja danych, data deduplication, 353, 380
 Device Manager, 109, 111
 DFS, Distributed File System, 379
 DHCP, 214
 DHCP Server, 101
 Disk Management, 64, 78
 DMA, 118
 DNS, Domain Name System, 157, 180, 214
 działanie stref, 186
 pliki hosts i lmhosts, 183
 dołączanie do domeny, 85, 148

domena, domain, 159, 165, 171, 172
 poziomy funkcjonalne, 173
 relacje zaufania, 172

dostęp
 do opcji uruchamiania, 66
 do pamięci, DMA, 118
 do rejestru systemu, 122
 do udziałów sieciowych, 256
 do usług, 124
 warunkowy, 476
 konfigurowanie zasad, 477
 zdalny, 236

DRP, disaster recovery plan, 593

drukarka
 lokalna, local printer, 249
 sieciowa, network printer, 249

drukowanie przez internet, 251

dryf
 konfiguracji, configuration drift, 137
 ustawień, 497

drzewa domen, 166

drzewo, tree, 159

DSC, Desired State Configuration, 137

DSRM, Directory Services Restore Mode, 599

dyski
 dynamiczne, 372, 373
 lokalne, 300
 NVMe, 337, 439
 optyczne, 337, 370
 podstawowe, 372, 373
 półprzewodnikowe SSD, 44, 337, 369, 439
 twarde HDD, 44, 337, 368, 439, 547
 USB, 551
 wirtualne VHD, 310
 wymienne, removable drives, 550

dzienniki
 aplikacji, Application, 606
 danych wydajności, 572
 inspekcji, 501
 instalacji, Setup, 84, 606
 przekazanych zdarzeń, Forwarded
 Events, 607
 systemowe, System, 607
 wydajności, 569
 zabezpieczeń, Security, 606
 zdarzeń, 608

E

edytor lokalnych zasad grupy, 267, 278, 281

egzamininy certyfikacyjne Microsoft, 622
 przygotowania, 631
 rejestracja, 634

wdrażanie
 infrastruktury sieciowej, 628
 usług AD DS, 624

wskazówki, 635

zarządzanie
 infrastrukturą sieciową, 628
 maszynami wirtualnymi
 i kontenerami, 627
 serwerami Windows, 625
 usługami AD DS, 624
 usługami pamięci masowej i plików,
 630
 źródła wiedzy, 632

enkawy VBS, 52, 509

Event Viewer, 606
 filtry dzienników, 610
 konfigurowanie monitorowania, 608
 monitorowanie dzienników zdarzeń, 608

exFAT, Extended File Allocation Table, 377

F

FAT, File Allocation Table, 377

FC, Fibre Channel, 348

FCoE, Fibre Channel over Ethernet, 348

FFL, Forest Functional Level, 174

File Services, 246

File and Storage Services, 214

format
 VHD, 318
 VHDX, 318

framework ITIL, 592

FTP, File Transfer Protocol, 224, 228, 349

FTPS, FTP Secure, 224

funkcja
 IE Enhanced Security Configuration, 135,
 144
 Internet Printing, 248
 Remote Assistance, 238
 Remote Desktop, 141
 SMTP Server, 217

funkcje
 IIS, 230
 jednokrotnego logowania, 394
 serwera
 serwera, server features, 212, 214

G

gałęzie rejestru, registry hives, 120

główny kod rozruchowy, MBC, 76

GP, Group Policy, 267

GPM, Group Policy Management, 392
 GPO, Group Policy Objects, 267, 602
 GPT, GUID Partition Table, 73, 75
 graficzny interfejs użytkownika, GUI, 47
 grupy
 domyślne w AD, 201
 dystrybucyjne, distribution groups, 201
 globalne, 203
 lokalne domeny, 203
 robocze, workgroups, 171, 172
 uniwersalne, 203
 zabezpieczeń, security groups, 200
 zagnieżdżanie, 204
 GUID Partition Table, GPT, 64

H

HA, High Availability, 366
 HAN, Home Area Network, 34
 HCI, Hyper-Converged Infrastructure, 355, 300
 hosty, 32, 38, 185
 hotpatching, 52, 54, 508
 instalowanie poprawek, 513, 517
 przygotowania do instalowania, 514, 516
 rozwiązywanie problemów, 528, 533
 weryfikacja po zainstalowaniu, 519
 HTML, HyperText Markup Language, 227
 HTTP, HyperText Transfer Protocol, 349
 HTTPS, HyperText Transfer Protocol
 Secure, 483
 Hype-V, 214, 296
 architektura, 303
 wymagania instalacyjne, 303
 Hype-V Manager, 295, 305
 dyski wirtualne VHD, 310
 funkcje, 306
 konfigurowanie sieci wirtualnych, 313
 przydzielanie pamięci RAM, 311
 punkty kontrolne, 316
 ustawienia konfiguracyjne, 308
 zarządzanie maszynami wirtualnymi, 305
 Hype-V Replica, 328

I

IIS, Internet Information Services, 224
 implementacja strony bazy danych AD, 413
 infrastruktura
 hiperkonwergentna, hyper-converged
 infrastructure, 300
 klucza publicznego, 426, 430

instalowanie
 aktualizacji, 580
 pakietu
 MDT, 95
 Windows ADK, 94
 Windows PE, 94
 roli
 Hyper-V, 330
 IIS, 225, 230
 PDS, 261
 Web Server, 259
 ról AD DS, 205
 sterowników, 112
 systemu, 62
 aktualizacja w miejscu, 98
 aktywacja i licencjonowanie, 86
 czysta instalacja, 87
 Desktop Experience, 81
 diagnozowanie problemów, 83
 dołączanie do domeny, 85
 Nano Server, 82
 opcje, 79
 połączenia sieciowe, 85
 Server Core, 82, 150
 wymagania systemowe, 80
 z wykorzystaniem MDT, 93
 integralność danych, 428
 interfejs
 ATA, 338
 ISA, 340
 PATA, 339
 SAS, 339
 SATA, 339
 SCSI, 339
 SPI, 339
 interfejsy sieciowe, 45, 548
 Internet
 Information Services, IIS, 211
 Rzeczy, IoT, 42
 IOPS, Input/Output Operations Per Second, 356
 IP, Internet Protocol, 38
 IPsec, Internet Protocol Security, 483
 IRQ, 118
 iSCSI, Internet Small Computer System
 Interface, 335, 351
 w środowiskach wirtualnych, 357
 ITIL, ITIL core books, 592

J

jednostki organizacyjne, Organizational
 Units, 189
 delegowanie uprawnień, 193

język

HTML, 227

XML, 223

K

kafelki, 111

kanały komunikacji, 485

karty

graficzne, 552

HBA, 350

sieciowe, NIC, 439, 548

KCC, Knowledge Consistency Checker, 178

klastrowanie, clustering, 595

klastry rozciągnięte, stretched clusters, 66

klasy, classes, 179

klienci, 37

klucz

prywatny, 427

publiczny, 426, 427

wdrażanie infrastruktury, 430

zarządzanie infrastrukturą, 430

komponenty sprzętowe serwera, 544

komputer osobisty, PC, 37

komunikacja

równoległa, parallel communication, 346

szeregową, serial communication, 346

konfigurowanie

adresu IP, 142, 149

Azure Arc, 509, 535

DNS, 180

domeny

drzewa, 167

głównej, 165

podrzędnej, 169

dzienników inspekcji, 501

mechanizmu RBAC, 462

początkowych ustawień, 139

reguł zapory sieciowej, 498

rozruchu, 68

ról dostępu zdalnego, 236

scentralizowanego monitorowania, 608

serwera

DHCP, 102

w trybie CLI, 136

za pomocą Server Manager, 136, 139

sieci wirtualnej, 313, 314

systemu za pomocą Server

Configuration, 147

usług sieciowych, 223

usługi

Remote Desktop Gateway, 242

Windows Update, 585

ustawień GPO, 277

uwierzytelniania wieloskładnikowego,
463

wstępne systemu, 135

wykrywania zagrożeń, 466

zabezpieczeń, 433

żądanego stanu, 137

konsola

Active Directory Domains and Trusts, 162

Active Directory Sites and Services, 162

Disk Management, 78

GPM, 272, 273

GPMC, 270

konta

domenowe, 195

komputerów, computer accounts, 199

lokalne, 196

kontenery

domyślne, 190, 192

domyślne ukryte, 191

konto

administratora, 287

gościa, 288

usługowe, service account, 133

kontrola dostępu, 459

oparta na rolach, RBAC, 460

konfigurowanie, 462

kontroler

domeny, domain controller, 140, 164

dysku, disk controller, 345

konwencja UNC, 187

konwersja dysku podstawowego, 373

kopia

przyrostowa, incremental backup, 400,
597

różnicowa, differential backup, 597

zapasowa, 399, 596

zapasowa pełna, full backup, 597

zapasowa w chmurze, 598

Kubernetes, 55, 512

L

LAN, Local Area Network, 34

las, forest, 159

lasy domen, 167, 168

licencja RDS CAL, 241

liczniki wydajności, 567

Linux Server, 46, 47

logi, 84

lokacje, sites, 177

M

macierz RAID, 357, 361
 macOS Server, 46, 49
 MAN, Metropolitan Area Network, 35
 Master Boot Record, MBR, 63
 maszyny wirtualne, virtual machines, 103, 295, 305

- dostosowywanie ustawień, 323
- kopie zapasowe, 329
- punkty kontrolne, 329
- tworzenie, 104
- ustawienia uruchamiania i odzyskiwania, 326
- zarządzanie, 325

 MBC, Master Boot Code, 76
 MBR, 75
 MDT, Microsoft Deployment Toolkit, 62

- instalowanie systemu, 93

 mechanizm dwuportowy, dual-port system, 228
 menedżer zadań, 560
 menu

- Advanced Boot Options, 77
- rozruchowe, boot menu, 76
- Start, 110
- Start systemu, 51

 metodyka

- AGDLP, 204
- AGUDLP, 204

 MFA, multi-factor authentication, 460
 Microsoft

- Defender Antivirus, 468
- Defender for Endpoint, 495
- Defender for Servers, 489
- Passport, 179

 migracja, 319

- usług sieciowych, 100
- z VMware do Hyper-V, 321, 328

 model

- klient-serwer, 39, 228
- równorzędny, 39, 171

 moduł

- CSM, 76
- TPM, 71

 monitor

- wydajności, 560
- zasobów, 560

 monitorowanie, 526

- aktywności serwera plików, 258
- dryfu ustawień, 497
- dzienników systemowych, 606
- dzienników zdarzeń, 608

- kanałów komunikacji, 485
- procesu instalowania aktualizacji, 528
- serwerów, 565
- wydajności, 440, 556–558

 MSSP, managed security service providers, 356
N

napędy dysków optycznych, 370
 narzędzia

- diagnostyczne, 410, 411, 530
- migracyjne, 322
- RSAT, 52

 narzędzie

- Ansible, 532
- Azure Monitor, 565
- Azure Update Manager, 524
- bcdedit.exe, 74
- dcdiag, 411
- Device Manager, 109
- Disk2vhd, 319
- dsac.exe, 161
- DTrace, 412
- ELK Stack, 531
- Event Viewer, 606
- Git, 532
- Hyper-V Manager, 305
- Intune, 526
- MDT, 62
- Nagios, 531
- Nessus, 532
- OpenVAS, 532
- Performance Monitor, 441, 560
- PowerShell DSC, 137
- Red Hat Satellite, 524
- Registry Editor, 122
- repadmin, 412
- Resource Monitor, 562
- RSAT, 239
- SCCM, 526
- Server Configuration, 147
- Server Manager, 101, 136, 139, 215
- Service Control Manager, 121
- SolarWinds, 531
- Splunk, 531
- Task Manager, 564
- Tripwire, 532
- VMware, 321
- Windows Admin Center, 395
- Windows Settings, 109
- WSIM, 93
- WSMT, 100

NAS, Network-Attached Storage, 342, 598
nazwa
 hosta, 185
 konta
 administratora, 287
 gościa, 288
NetBIOS, 184
Network Policy Server, NPS, 213
NFS, Network File System, 349
NIC, Network Interface Card, 439, 548
niezaprzeczalność, non-repudiation, 429
NNTP, Network News Transfer Protocol, 224
NOS, Network Operating System, 46
NT Loader, 73
NTFS, New Technology File System, 47, 63, 377

O

OAuth, Open Authorization, 478
obiekty, objects, 179
 AD, 406
 diagnozowanie problemów, 406
 najlepsze praktyki zarządzania, 409
 naprawianie, 407
 odzyskiwanie, 407, 409
 zasad grupy, GPO, 267, 602
 blokowanie dostępu, 290, 291
 blokowanie kont Microsoft, 289
 dla administratorów systemów, 287
 kategorie ustawień, 283
 konfiguracja ustawień, 277, 279
 lokalne, 278
 na poziomie domeny, 279
 na poziomie jednostek organizacyjnych OU, 279
 na poziomie lokalizacji, 279
OCSP, Online Certificate Status Protocol, 427
odzyskiwanie
 danych, 400, 597
 tryb DSRM, 599
 po awarii, 357, 593–596
 kopie zapasowe, 597
 typy ośrodków zapasowych, 605
 wdrażanie planu, 604
opcje
 instalacji systemu, 79
 przechowywania danych, 65
 uruchamiania systemu, 66, 68
 dostępne w UEFI, 68
 oprogramowanie firmware, 70
 w BIOS-ie, 69

oprogramowanie
 firmware, 70
 serwerowe, 44
organizacja IANA, 232
ośrodek zapasowy
 ciepły, warm site, 605
 gorący, hot site, 605
 zimny, cold site, 605
OU, Organizational Units, 189

P

P2P, peer-to-peer, 39, 171
pamięć
 DAS, 341
 lokalna, 341
 masowa, 65, 300, 337
 definiowana programowo, SDS, 357
 optymalizacja rozwiązań, 367
 warstwowa, 354, 355
 zarządzanie, 358, 359
 na poziomie bloków, 344
 na poziomie plików, 344
 NAS, 342
 nieulotna, non-volatile memory, 547
 operacyjna RAM, 44, 546
 SAN, 343
 ulotna, volatile memory, 546
 USB, 550
PAN, Personal Area Network, 34, 39
panel
 szczegółów, details pane, 215
 zakresu, scope pane, 215
partycja
 główna, root partition, 302
 podrzędna, child partition, 302
 systemowa EFI, 76
partycjonowanie dysków, 63
PC, Personal Computers, 37
PCI, 340
PCIe, 340
Performance
 Logs & Alerts, 570
 Monitor, 560
PKI, public key infrastructure, 235, 426
platforma
 Confluence, 532
 Docker, 532
 Slack, 532
 VMware, 532
plik
 hosts, 183, 184
 lmhosts, 183, 184

- odpowiedzi, answer file, 93
- setupact.log, 84
- setuperr.log, 84
- pliki dziennika, 611
- PnP, Plug and Play, 118
- podłączanie do domeny, 140
- podpis cyfrowy, digital signature, 119
- podsieci, 41, 42
- polecenia powłoki PowerShell, 100
- połączenia sieciowe, 85
- porty, ports, 232
 - dobrze znane, 232
 - dynamiczne lub prywatne, 232
 - fizyczne, 555
 - programowe, software ports, 232
 - sprzętowe, hardware ports, 232
 - zarejestrowane, 232
- POST, Power-On Self-Test, 72
- PowerShell, 498
- PowerShell DSC, 137
- powiadomienie o przeciążeniu, 438
- poziom funkcjonalny
 - domeny, DFL, 174
 - lasu, FFL, 174
- prawa
 - dostępu użytkowników, 254
 - użytkownika, 257
- Print and Document Services, PDS, 211, 247
- proces
 - KCC, 178
 - roboczy, worker process, 229
- procesor, 44, 544
- profile użytkowników, user profiles, 197
- program rozruchowy, bootloader, 73, 75
 - BOOTMGR, 73, 75
 - NTLDR, 73, 75
- protokoły
 - bezpieczeństwa, 483
 - komunikacyjne, 216, 347
 - pamięci masowej, 347
 - szyfrowania, 426
 - udostępniania plików, 348
- protokół
 - AES, 433
 - FC, 348
 - FCoE, 348
 - FTP, 224, 228, 349
 - FTPS, 224
 - HTTP, 349
 - HTTPS, 483
 - IPsec, 483
 - iSCSI, 348, 351
 - Kerberos, 392
 - NFS, 349
 - NNTP, 224
 - OAuth 2.0, 478
 - wdrażanie, 480
 - OCSP, 427
 - QUIC, 420, 423
 - SCSI, 347
 - SMB, 349, 419, 422
 - SMB over QUIC, 52, 54, 418–455
 - działania prewencyjne, 447
 - konfigurowanie protokołu, 452
 - konfigurowanie zabezpieczeń, 433
 - mechanizmy szyfrowania, 431
 - optymalizowanie wydajności, 437
 - rozpoznawanie problemów, 443
 - rozwiązania problemów, 445
 - udostępnianie danych, 438
 - wdrażanie, 424, 443
 - włączanie protokołu, 452
 - znaczenie protokołu, 449
 - SOAP, 223
 - SSH, 349, 484
 - SSL, 233
 - TLS, 235, 481
 - zabezpieczanie kanałów komunikacyjnych, 481
- przechowywanie danych
 - u dostawcy MSSP, 356
 - zgodność z przepisami, 356
- przeglądarka
 - Internet Explorer, 135
 - Microsoft Edge, 224
- przekierowanie folderów, folder redirection, 602
- przełączniki FC, 350
- przerwania sprzętowe, IRQ, 118
- przetwarzanie w chmurze, cloud computing, 295
- przystawka Active Directory Users and Computers, 161
- przywracanie
 - autorytatywne, authoritative restore, 600
 - nieautorytatywne, non-authoritative restore, 600
- PT, Partition Table, 76
- pula drukarek, printer pooling, 250
- pulpit, 51
 - zdalny, 148
- punkt montowania, mount point, 376
- punkty kontrolne, checkpoints, 316, 329

Q

QoS, quality of service, 437

R

RA, registration authority, 427
 RAID, Redundant Array of Independent
 Disks, 357, 361
 0, 362
 1, 362
 10, 363
 5, 362
 metody implementowania, 363
 RAM, Random Access Memory, 44, 546
 raportowanie, 526
 RBAC, role-based access control, 460
 Red Hat Satellite, 524
 redundancja
 danych, data redundancy, 595
 zasilania, 603
 ReFS, Resilient File System, 47, 63, 377
 Registry Editor, 122
 regularne oceny bezpieczeństwa, 494
 rejestr systemu Windows Server, 120, 122
 modyfikowanie wartości, 123
 tworzenie klucza, 132
 usuwanie wartości, 124
 zmiana nazwy wartości, 123
 rejestrowanie zdarzeń, 393, 493
 rekord Protective MBR, 76
 Remote
 Assistance, 238
 Desktop, 135, 141, 148
 Desktop Services, RDS, 240
 replikacja między lokalizacjami, 66
 Resource Monitor, 562
 Rights Management Services, RMS, 213
 rola
 File Services, 246
 Hyper-V, 301
 Print and Document Services, 247
 Remote Desktop Licensing, 241
 Remote Desktop Services, 240
 role
 dostępu zdalnego, 236
 serwera, 212, 216
 ROM, Read-Only Memory, 546
 rozwiązywanie problemów,
 troubleshooting, 588
 ITIL, 592
 najlepsze praktyki, 589
 problemy techniczne, 589

procedury, 591
 systematyczne i ukierunkowane, 590
 RSAT, 239

S

S2D, Storage Spaces Direct, 335, 352, 365
 SAM, Security Accounts Manager, 172, 196
 SAN, Storage Area Network, 343, 598
 schemat, schema, 179
 schematy AD, 401–403
 SCSI, Small Computer System Interface, 335
 SDS, Software-Defined Storage, 352, 357, 364
 Secure Boot, 64
 sektor rozruchowy, 75
 Server
 Configuration, 147
 Manager, 136, 139, 215
 zarządzanie pamięcią masową, 358
 Service Control Manager, 121, 122
 serwer, 43
 aplikacji, 216
 baz danych, 218
 IIS, 224
 monitorujący, 221
 nieautorytatywny DNS, 187
 plików, 258
 poczty elektronicznej, 216
 WINS, 184
 wspomagający ochronę danych, 222
 współpracy, 220
 serwery, 37
 do montażu w szafach rack, 45
 fizyczne, 319, 320
 role, 79
 typu blade, 45
 typu wieża, 46
 wirtualne, 319, 320
 sieciowy system operacyjny, NOS, 46
 sieć
 domowa, HAN, 34
 klient-serwer, 40, 171
 komputerowa, 33
 lokalna, LAN, 34
 metropolitalna, MAN, 35, 172
 osobista, PAN, 34
 P2P, 39, 171
 pamięci masowej, SAN, 300
 rozległa, WAN, 35, 36172
 wirtualna, 313
 WWW, 227
 skalowalność usługi AD DS, 397

SMB, Server Message Block, 349
 SMTP, 224
 SOAP, Simple Object Access Protocol, 223
 SOHO, Small Office/Home Office, 46
 spójność danych, data consistency, 595
 SQL Server, 219
 SSD, Solid-State Drives, 44, 369
 SSH, Secure Shell, 349, 484
 SSL, Secure Sockets Layer, 233
 sterownik

- aktualizowanie, 113
- odinstalowywanie, 114
- podpisywanie, 118, 119
- przywracanie, 116
- rozwiązywanie problemów, 117
- urządzenia, device driver, 109
- wyłączanie, 115

 sterowniki drukarek, 253
 Storage

- Replica, 66
- Spaces, 65
- Spaces Direct, 65

 strefa DNS, DNS zones, 186

- podstawowa, primary zone, 186
- szkieletowa, stub zone, 186

 System Center Configuration Manager, SCCM, 105
 system

- operacyjny
 - Linux Server, 47
 - macOS Server, 49
 - sieciowy, NOS, 46
 - Windows Server, 47
- plików, filesystem, 376
 - DFS, 379
 - exFAT, 377
 - FAT, 377
 - NTFS, 47, 63, 377
 - ReFS, 47, 63, 377

 systemy wykrywania zagrożeń, 356
 szablony administracyjne, administrative templates, 271

- aktualizowanie, 271
- instalowanie, 271
- zarządzanie, 271

 szafa rack, 45
 szyfrowanie, 431

- i poufność, 429
- TLS, 500

T

tabela partycji, PT, 76
 Task Manager, 564
 TCP handshake, 420
 technologia

- S2D, 352, 365
- SDS, 364

 technologie pamięci masowej, 336
 Terminal Services, 240
 test POST, 72
 testery pamięci, 138
 testy obciążeniowe, 138
 TLS, Transport Layer Security, 481

- handshake, 420
- włączanie szyfrowania, 500

 TPM, 71
 tryb

- awaryjny, Safe Mode, 77
- CLI, 136

 tunele VPN, 243
 tworzenie maszyny wirtualnej, 104

U

UDDI, Universal Description, Discovery and Integration, 223
 udostępnianie plików, 420
 UEFI, Unified Extensible Firmware Interface, 65, 68, 70

- opcje uruchamiania, 68

 układy chłodzenia, 553
 UNC, Universal Naming Convention, 187

- ścieżki, 188

 uprawnienia, 254

- dostępu do udziałów sieciowych, 256
- NTFS, NTFS permissions, 254

 URL, Uniform Resource Locator, 176, 227
 urząd

- certyfikacji, CA, 427
- rejestracji, RA, 427

 urządzenia

- aktualizowanie sterowników, 113
- peryferyjne, 108
- podłączanie, 112
- rozwiązywanie problemów, 117
- sieciowe, 109
- usuwanie, 114
- wewnętrzne, 108
- zarządzanie, 115
- zewnętrzne, 108

usługa

- Active Directory Domain Services,
 - AD DS, 51, 54, 157, 169, 387
- App-V, 244, 245
- Azure Update Manager, 525
- DirectAccess, 236
- drukowania, 246
- dzienników wydajności i alertów, 570
- Line Printer Daemon, 248
- Microsoft Defender for Endpoint, 495
- Microsoft Defender for Servers, 489
- odzyskiwania po awarii, 598
- Performance Logs & Alerts, 570
- Print Server, 248
- Remote Desktop Gateway, 242
- Routing and Remote Access, 236
- SAM, 196
- udostępniania plików, 246
- VSS, 601
- Web Application Proxy, 237
- Windows Deployment Service, WDS, 62
- Windows Update, 578, 585
- WINS, 187
- WSUS, 587
- usługi, services, 121, 124
 - chmurowe, 394
 - dodawanie zależności, 134
 - katalogowe, 157
 - oparte na SOAP, 224
 - opóźnianie uruchomienia, 127
 - ponowne uruchamianie, 131
 - przywracanie, 126
 - ról, role services, 213
 - sieciowe
 - konfigurowanie, 223
 - tryby uruchamiania, 121, 129
 - tworzenie konta, 133
 - typu RESTful, 224
 - ustawienia logowania, 128
 - Windows Server, 121
 - Windows, Windows services, 120
 - zależności, 131
 - zatrzymywanie, 129
- ustawienia rozruchu, boot settings, 65
- uwierzytelnianie, 392, 428, 472
 - biometryczne, biometric authentication, 473
 - wdrażanie, 475
 - wieloskładnikowe, multi-factor authentication, 180, 392, 460, 476
 - konfigurowanie, 463

V

- VBS, Virtualization-Based Security Enclaves, 509
- VHD, Virtual Hard Disk, 318, 378
- VHDX, Virtual Hard Disk Extended, 318
- VMware, 321
- VPN, virtual private network, 212, 243, 420
- VSS, Volume Shadow Copy Service, 601

W

- WAN, Wide Area Network, 35
- warstwowanie pamięci, storage tiering, 354
- wdrażanie
 - infrastruktury
 - klucza publicznego, 430
 - sieciowej, 628
 - protokołu
 - OAuth 2.0, 480
 - SMB over QUIC, 443
 - sterowników drukarek, 253
 - systemu, 87
 - aktualizacja w miejscu, 98
 - czysta instalacja, 87
 - migracja, 100
 - na platformie Azure, 102
 - opcja System Center Configuration Manager, 105
 - za pomocą MDT, 93
 - usług AD DS, 624
 - uwierzytelniania biometrycznego, 475
- wersje systemu Windows Server, 50
- wersjonowanie schematów, schema versioning, 402
- węzły, 32, 38
- wielosystemowość, multi-booting, 76
- Windows
 - Admin Center, 55, 58, 239, 395
 - pobieranie, 58
 - Assessment and Deployment Kit, 62
 - PowerShell
 - zarządzanie pamięcią masową, 359
 - Recovery Environment, 74
 - Server, 46, 47
 - Server 2022, 53
 - Server 2025, 50
 - aktualizacje systemu, 577, 578
 - dodawanie ról serwera, 211
 - edycje, 49
 - edycje systemu, 53
 - instalacja systemu, 62

- kompatybilność systemu, 511
 - konfiguracja sprzętowa, 55
 - konserwacja systemu, 543
 - optymalizacja systemu, 543
 - pobieranie systemu, 57
 - Server dla chmury, 50
 - Server Migration Tool, 100
 - Server Update Services, WSUS, 214, 276, 587
 - Settings, 109, 111
 - System Image Manager, 93
 - Update, 578
 - konfigurowanie usługi, 585
 - Virtual PC, 296
 - WINS, Windows Internet Name Service, 184
 - działanie usługi, 187
 - wirtualizacja, virtualization, 295
 - tryby, 298
 - wydajność, 300
 - zagnieżdżona, nested virtualization, 304
 - wirtualne
 - dyski twarde, VHD, 310, 378
 - sieci prywatne, VPN, 212
 - witryny internetowe, sites, 230
 - wolumin
 - lustrzany, mirrored volume, 373
 - prosty, simple volume, 372
 - RAID 5, 373
 - rozłożony, striped volume, 373
 - rozpięty, spanned volume, 373
 - WWW, World Wide Web, 227
 - wydajność, 135, 551
 - dysku, 374
 - dzienniki, 569, 570
 - liczniki, 567, 573
 - monitorowanie, 556, 557
 - narzędzia, 556, 560
 - określanie punktu odniesienia, 559
 - optymalizacja, 440, 560, 567
 - procedury monitorowania, 558
 - protokołu SMB over QUIC, 437
 - tworzenie dzienników, 572
 - wykrywanie zagrożeń, 464
 - wysoka dostępność, High Availability, 366
- X**
- XML, Extensible Markup Language, 223
- Z**
- zabezpieczenia, 392, 433
 - zagrożenia
 - analizowanie, 467
 - automatyczne systemy reagowania, 469, 471
 - dostosowywanie
 - wdrażanie, 470
 - konfigurowanie mechanizmów wykrywania, 464, 466
 - zapora sieciowa
 - konfigurowanie reguł, 498
 - zarządzanie
 - aktualizacjami, 491, 506, 522, 578
 - automatyczne aktualizacjami, 524
 - cyklem życia serwerów, 522
 - dostępem w chmurze, 396
 - drukowaniem, 252
 - infrastrukturą
 - klucza publicznego, 430
 - sieciową, 628
 - kontenerami, 627
 - maszynami wirtualnymi, 305, 325, 627
 - obciążeniami w środowisku hybrydowym, 625
 - obiektami, 405, 409
 - obiektami zasad grupy, 270
 - pamięcią masową, 358, 359
 - rejestr systemu, 122
 - serwerami Windows, 625
 - sterownikami, 109
 - szablonami administracyjnymi, 271
 - tożsamością, 396
 - uprawnieniami, 254
 - urządzeniami, 109, 115
 - usługami, 124
 - Active Directory, 161
 - AD DS, 411, 624
 - pamięci masowej i plików, 630
 - użytkownikami i grupami, 194
 - warstwową pamięcią masową, 355
 - wersjami schematów, 402
 - zasadami grupy, GPM, 274, 392
 - zasobami hybrydowymi, 395
 - zasady
 - dostępu warunkowego, 476, 477
 - grupy, Group Policy, 267, 268
 - edytory, 280
 - lokalne, 282
 - proces przetwarzania, 276
 - stosowanie, 278
 - zarządzanie, 274
 - zastosowania, 275
 - zasilacze, 554
 - zaufane urzędy certyfikacji, 233
 - zestawy Data Collector Set, 567

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

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 serwowymi 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 Xcitiem, 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 (CCA). 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.

	KOD KORZYŚCI Sięgnij po więcej! ▶	
 helion.pl	ISBN 978-83-289-3329-3	
 HELION S.A. ul. Kościuszki 1c 44-100 Gliwice tel.: 32 250 98 63 helion@helion.pl	 9 788328 933293	
Cena: 139,00 zł		