Microsoft



Inside OUT

Wyczerpujący, kompletny poradnik

Setki rozwiązań oszczędzających czas

Doskonale uporządkowany i wypełniony eksperckimi wskazówkami

Windows Server 2016

Orin Thomas

Microsoft MVP, RD, Cloud and Datacenter Specialist

Microsoft

Orin Thomas

Windows Server 2016 Inside Out

Przekład: Krzysztof Kapustka, Marek Włodarz

APN Promise, Warszawa 2017

Windows Server 2016 Inside Out

Authorized Polish translation of the English language edition entitled
Windows Server 2016 Inside Out, by Orin Thomas, ISBN: 978-1-5093-0248-2

Copyright © 2017 by Orin Thomas

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 Pearson Education, Inc.

Polish language edition published by APN PROMISE SA Copyright © 2017

Autoryzowany przekład z wydania w języku angielskim, zatytułowanego:
Windows Server 2016 Inside Out, by Orin Thomas, ISBN: 978-1-5093-0248-2

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiejkolwiek formie i w jakikolwiek sposób (elektroniczny, mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu innych systemów bez pisemnej zgody wydawcy.

APN PROMISE SA, ul. Domaniewska 44a, 02-672 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

Książka ta przedstawia poglądy i opinie autora. Przykłady firm, produktów, osób i wydarzeń opisane w niniejszej książce są fikcyjne i nie odnoszą się do żadnych konkretnych firm, produktów, osób i wydarzeń, chyba że zostanie jednoznacznie stwierdzone, że jest inaczej. Ewentualne podobieństwo do jakiejkolwiek rzeczywistej firmy, organizacji, produktu, nazwy domeny, adresu poczty elektronicznej, logo, osoby, miejsca lub zdarzenia jest przypadkowe i niezamierzone.

Microsoft oraz znaki towarowe wymienione na stronie *http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx* są zastrzeżonymi znakami towarowymi grupy Microsoft. Wszystkie inne znaki towarowe są własnością ich odnośnych właścicieli.

APN PROMISE SA dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej publikacji. Jednakże nikomu nie udziela się rękojmi ani gwarancji.
APN PROMISE SA nie jest w żadnym wypadku odpowiedzialna za jakiekolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-335-9

Przekład: Krzysztof Kapustka, Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Wprowadzenie xix

1 Narzędzia administracyjne 1

Zdalnie, nie lokalnie 1
Stacje robocze z dostępem uprzywilejowanym 2
Narzędzia zdalnej administracji serwerem 4
Konsole RSAT 5
Konsola Server Manager 8
PowerShell 11
Moduły 12
Galeria PowerShell 12
Obsługa zdalna 13
Obsługa zdalna wielu maszyn 14
PowerShell ISE 15
PowerShell Direct 18
Pulpit zdalny 18

2 Opcje instalacji 21

Edycje Windows Server 2016 21
Gałęzie obsługi Windows Server 23
LTSB 23
CBB 24
Server Core 24
Interfejs systemu Server Core 25
Role w systemie Server Core 26
Kiedy wdrażać Server Core 30
Serwer z interfejsem graficznym 32
Role i funkcje 32
Nano Server 34
Konsola Nano Server 35
Obsługiwane role i funkcje 36
Przyłączanie do domeny 37
Tworzenie obrazów systemu Nano Server 38

3 Wdrożenie i konfiguracja 45
Wdrożenie fizyczne a wirtualne 45
Obrazy systemu Windows 46
Modyfikowanie obrazów Windows 48
Obsługiwanie obrazów Windows 48
Montowanie obrazów 49
Dodawanie do obrazów sterowników i aktualizacji 52
Dodawanie ról i funkcji 54
Zatwierdzanie zmian w obrazie 55
Tworzenie i przechwytywanie 56
Pliki odpowiedzi 57
Windows Deployment Services 59
Wymagania usługi WDS 60
Zarządzanie obrazami 62
Konfigurowanie serwera WDS 63
Konfigurowanie transmisji 67
Grupy i pakiety sterowników 68
Virtual Machine Manager 69
Szablony maszyn wirtualnych 69
Magazyn programu VMM 70
Sieci w programie VMM 72
Dodawanie usługi WDS do programu VMM 77
Grupy hostów 78
Konfiguracja infrastruktury w postaci kodu 80
Desired State Configuration 82
Pliki konfiguracji DSC 84
Local Configuration Manager 85
Zasoby DSC 86
Model Push 86
Serwer ściągania 87
Chef 87
Serwery Chef 88
Chef Development Kit 91
Wdrażanie agentów Chef 97
Wdrażanie książek kucharskich i przepisów Chef 98
Puppet 100
Puppet master 100
Wdrażanie agenta Puppet w Windows Server 104

Zarządzanie konfiguracją Windows Server 106
Pakiet modułów Windows 107
Narzędzia zarządzania pakietami 109
Galeria PowerShell 111
Dostawca pakietów Nano Server 111
Chocolatey 112

4 Active Directory 117

Zarządzanie środowiskiem Active Directory 117
Administracja zdalna zamiast lokalnej 118
Active Directory Administrative Center 119
Active Directory Users and Computers 121
Active Directory Sites and Services 123
Active Directory Domains and Trusts 125
Kontrolery domeny 126
Wdrażanie 127
Server Core 129
Serwery wykazu globalnego 130
Kontrolery domeny tylko do odczytu 131
Klonowanie wirtualnego kontrolera domeny 134
Struktura środowiska AD DS 135
Domeny 135
Poziomy funkcjonalności domen 135
Lasy 136
Lasy kont i zasobów 137
Jednostki organizacyjne 138
Role FSMO 139
Konta 142
Konta użytkownika 142
Konta komputera 143
Konta grup 144
Grupy domyślne 145
Konta usług 148
Zasady grupy 150
Zarządzanie obiektami GPO 150
Przetwarzanie zasad 153
Preferencje zasad grupy 155
Szablony administracyjne 158

Przywracanie usuniętych elementów . . . 158
Kosz usługi Active Directory . . . 160
Przywracanie autorytatywne . . . 162
Migawki usługi Active Directory . . . 164
Zarządzanie usługą AD DS z poziomu programu PowerShell . . . 165
Moduł ActiveDirectory . . . 165
Moduł GroupPolicy . . . 169
Moduł ADDSDeployment . . . 170

5 DNS, DHCP i IPAM . . . 171

DNS . . . 171
Rodzaje stref DNS . . . 171
Delegowanie stref . . . 175
Usługi przesyłania dalej i warunkowego przesyłania dalej . . . 176
Strefy skrótowe . . . 177
Strefy GlobalNames . . . 178
Protokół PNRP . . . 179
Rekordy zasobów . . . 180
Przedawnianie i oczyszczanie stref . . . 181
DNSSEC . . . 182
Dzienniki zdarzeń DNS . . . 184
Opcje DNS . . . 185
Administracja delegowana . . . 189
Zarządzanie usługą DNS za pomocą programu PowerShell . . . 190
DHCP . . . 193
Zakresy . . . 193
Opcje serwera i zakresu DHCP . . . 194
Zastrzeżenia . . . 195
Filtrowanie . . . 195
Superzakresy . . . 196
Zakresy multiemisji . . . 196
Podziały zakresów . . . 197
Ochrona nazwy . . . 197
Tryb failover . . . 198
Administracja . . . 199
IPAM . . . 202
Wdrażanie IPAM . . . 203
Konfigurowanie odnajdowania serwerów . . . 203

Administrowanie serwerem IPAM 204
Zarządzanie usługą IPAM z poziomu programu PowerShell 206

6 Hyper-V 209

Pamięć dynamiczna 209
Inteligentne stronicowanie 210
Pomiar zasobów 211
Usługi integracji dla systemów operacyjnych gościa 212
Maszyny wirtualne drugiej generacji 212
Tryb sesji rozszerzonej 213
RemoteFX 214
Wirtualizacja zagnieżdżona 214
Pamięć dynamiczna wirtualizacji zagnieżdżonej 214
Sieć wirtualizacji zagnieżdżonej 215
PowerShell Direct 215
Wirtualne dyski twarde 216
Dyski o stałym rozmiarze 216
Dyski dynamiczne 217
Dyski różnicowe 217
Modyfikowanie wirtualnych dysków twardych 218
Dyski przekazane 219
Zarządzanie punktami kontrolnymi 220
Wirtualne karty Fibre Channel 221
Jakość usług magazynowania 222
Optymalizacja magazynu Hyper-V 222
Deduplikacja 222
Tworzenie warstw magazynowania 223
Wirtualne przełączniki Hyper-V 224
Przełączniki zewnętrzne 224
Przełączniki wewnętrzne 224
Przełączniki prywatne 225
Karty sieciowe maszyn wirtualnych 225
Optymalizowanie wydajności sieci 226
Zarządzanie przepustowością 226
SR-IOV 226
Dynamiczna kolejka maszyn wirtualnych 227
Zespół kart interfejsu sieciowego w maszynie wirtualnej 227
Adresy MAC maszyn wirtualnych 228

Izolacja sieci . . . 228
Hyper-V Replica . . . 229
Konfigurowanie serwerów repliki Hyper-V . . . 230
Konfigurowanie repliki maszyny wirtualnej . . . 230
Przełączanie repliki w tryb failover . . . 232
Broker funkcji Hyper-V Replica . . . 232
Klastry trybu failover . . . 232
Magazyn klastra hostów Hyper-V . . . 233
Kworum klastra . . . 234
Sieć klastra . . . 236
Wymuszanie odporności kworum . . . 237
Udostępnione woluminy klastra . . . 237
Klastry odłączone od Active Directory . . . 238
Preferowany właściciel i ustawienia trybu failover . . . 238
Klastry gościa funkcji Hyper-V . . . 239
Magazyn klastra gościa Hyper-V . . . 240
Udostępnione wirtualne dyski twarde . . . 240
Migracja na żywo . . . 241
Migracja magazynu . . . 243
Eksportowanie, importowanie i kopiowanie maszyn wirtualnych . . . 244
Wykrywanie kondycji sieci maszyny wirtualnej . . . 245
Opróżnianie maszyn wirtualnych przy wyłączaniu . . . 245
Klonowanie kontrolera domeny . . . 246
Chronione maszyny wirtualne . . . 246
Zarządzanie Hyper-V z poziomu programu PowerShell . . . 247

7 Usługi magazynowania . . . 253

Miejsca do magazynowania i pule magazynu . . . 253
Pule magazynu . . . 253
Odporność miejsc do magazynowania . . . 258
Tworzenie warstw magazynowania . . . 259
Alokowanie elastyczne i przycinanie magazynu . . . 260
Tworzenie wirtualnych dysków twardych . . . 262
Bezpośrednie miejsca do magazynowania . . . 264
Replika magazynu . . . 265
Obsługiwane konfiguracje . . . 267
Konfigurowanie replikacji . . . 268
SMB 3.1.1 . . . 271

iSCSI . . . 273
Serwer iSNS . . . 276
Serwer plików skalowalny w poziomie . . . 279
NFS . . . 280
Deduplikacja . . . 281
Jakość usług magazynowania . . . 284
ReFS . . . 286
Polecenia programu PowerShell związane z magazynowaniem . . . 288
Moduł Deduplication . . . 288
Moduł iSCSI . . . 288
Moduł iSCSITarget . . . 289
Moduł NFS . . . 289
Moduł Storage . . . 290
Moduł StorageReplica . . . 294

8 Serwery plików . . . 295

Uprawnienia folderów udostępnionych . . . 296
Korzystanie z Eksploratora plików . . . 297
Server Manager . . . 299
Konsola File Server Resource Manager . . . 301
Przydziały na poziomie folderów . . . 301
Osłony plików . . . 303
Raporty magazynowania . . . 307
Klasyfikacja plików . . . 309
Zadania zarządzania plikami . . . 312
Rozproszony system plików . . . 314
Obszary nazw DFS . . . 314
Replikacja DFS . . . 317
BranchCache . . . 321
Polecenia PowerShell . . . 324
Polecenia folderów udostępnionych . . . 324
Polecenia konsoli File Server Resource Manager . . . 325
Polecenia usługi BranchCache . . . 327
Polecenia DFS . . . 329
Polecenia funkcji Dynamic Access Control . . . 331

9 Internet Information Services . . . 333

Zarządzanie witrynami . . . 333

Dodawanie witryn 334
Katalogi wirtualne 337
Dodawanie aplikacji sieci Web 339
Konfigurowanie certyfikatów TLS 339
Uwierzytelnianie witryny 342
Modyfikowanie niestandardowych odpowiedzi na błędy 344
Dodawanie lub wyłączanie domyślnego dokumentu 345
Przeglądanie katalogów 346
Filtrowanie adresów IP i nazw domen 346
Reguły autoryzacji adresów URL 348
Filtry żądań 348
Pule aplikacji 351
Tworzenie pul aplikacji 351
Konfigurowanie ustawień odtwarzania puli aplikacji 352
Użytkownicy i delegowanie w IIS 354
Konta użytkowników IIS 355
Delegowanie uprawnień administracyjnych 355
Zarządzanie serwerem FTP 356
Zarządzanie IIS za pomocą programu PowerShell 359

10 Kontenery 363

Pojęcia związane z kontenerami 363
Rodzaje kontenerów 365
Kontenery Windows Server 365
Kontenery Hyper-V 366
Server Core i obrazy Nano 367
Zarządzanie kontenerami poprzez Docker 367
Instalacja silnika Docker 368
Demon.json 369
Pozyskiwanie bazowego obrazu systemu operacyjnego kontenera . . 372
Rejestry i obrazy kontenerów 373
Zarządzanie kontenerami 376
Uruchamianie kontenera 376
Modyfikowanie uruchomionego kontenera 379
Tworzenie nowego obrazu na podstawie kontenera 379
Korzystanie z plików Dockerfile 380
Zarządzanie obrazami kontenerów 381
Konta usług dla kontenerów Windows 383

Stosowanie aktualizacji . . . 384
Sieci w kontenerach . . . 385
Tryb NAT . . . 387
Tryb Transparent . . . 388
Tryb Overlay . . . 390
Tryb Layer 2 Bridge . . . 390
Tryb roju . . . 391
Tworzenie klastrów roju . . . 391
Tworzenie sieci Overlay . . . 392
Wdrażanie i skalowanie usług roju . . . 392

11 Klastrowanie i wysoka dostępność . . . 395

Klaster pracy awaryjnej . . . 395
Tryby kworum klastra . . . 396
Magazyn klastra i udostępnione woluminy klastra . . . 397
Sieć klastra . . . 398
Aktualizacje typu cluster-aware . . . 399
Ustawienia preferencji i praca awaryjna . . . 400
Klastry wielolokacyjne i świadek w chmurze . . . 401
Klastrowanie awaryjne maszyn wirtualnych . . . 402
Uaktualnianie stopniowe . . . 404
Zarządzanie klastrem pracy awaryjnej przy użyciu PowerShell . . . 406
Network Load Balancing . . . 409
Wymagania NLB . . . 409
Tryby operacji NLB . . . 410
Zarządzanie hostami klastra . . . 411
Reguły portów . . . 412
Filtrowanie i koligacja . . . 412
Zarządzanie NLB przy użyciu PowerShell . . . 413

12 Active Directory Certificate Services . . . 415

Typy CA . . . 415
Urząd certyfikacji przedsiębiorstwa . . . 417
Autonomiczne CA . . . 430
Listy odwołań certyfikatów . . . 434
Punkty dystrybucji CRL . . . 434
Dostęp do informacji o urzędach . . . 435
Odwoływanie certyfikatu . . . 436

Publikowanie CRL i delta-CRL 437
Usługi roli Certificate Services. 439
Szablony certyfikatów 440
Właściwości szablonu 442
Dodawanie i edytowanie szablonów. 447
Automatyczne rejestrowanie i odnawianie certyfikatów 448
Zarządzanie CA 450
Obsługa żądań certyfikatów. 452
Kopie zapasowe i przywracanie CA. 453
Archiwizowanie i przywracanie kluczy 455
CAPolicy.inf 459
Zarządzanie Certificate Services przy użyciu PowerShell 460
Zarządzanie usługami certyfikatów przy użyciu narzędzi Certutil.exe i Certreq.exe 462

13 Active Directory Federation Services 465

Komponenty AD FS. 465
Oświadczenia, reguły oświadczeń i magazyny atrybutów 466
Dostawca oświadczeń 466
Jednostka zależna. 467
Relacja zaufania jednostki zależnej 468
Relacja zaufania dostawcy oświadczeń. 468
Konfigurowanie relacji certyfikatów 469
Magazyny atrybutów. 470
Reguły oświadczeń 471
Reguły relacji zaufania jednostki zależnej 471
Reguły relacji zaufania dostawcy oświadczeń 472
Konfigurowanie proxy aplikacji Web 472
Workplace Join 475
Uwierzytelnianie wieloczynnikowe. 476
Zarządzanie AD FS przy użyciu PowerShell 478
Zarządzanie proxy aplikacji Web przy użyciu PowerShell 482

14 Dynamic Access Control i Active Directory Rights Management Services. 483

Dynamic Access Control. 483
Konfigurowanie zasad grupy w celu obsługi DAC 484
Konfigurowanie oświadczeń użytkowników i urządzeń. 484

Konfigurowanie właściwości zasobów 486
Centralne reguły dostępu 488
Centralne zasady dostępu 490
Przemieszczanie 491
Access Denied Assistance 492
Instalowanie AD RMS 492
Certyfikaty i licencje AD RMS 494
Szablony AD RMS 495
Administratorzy AD RMS i super-użytkownicy 499
Zaufane domeny użytkowników i publikowania 500
Zasady wykluczania 500
Automatyczne stosowanie szablonów AD RMS 501
Zarządzanie AD RMS przy użyciu Windows PowerShell 502

15 Zasady sieciowe i usługi dostępu 505

Remote Desktop Gateway 505
Zasady połączeń i zasobów RD Gateway 506
Konfigurowanie ustawień serwera 508
Konfigurowanie klientów do korzystania z RD Gateway 508
Wirtualne sieci prywatne 509
Protokół IKEv2 510
Protokół SSTP 511
Protokoły L2TP/IPsec 512
Protokół PPTP 512
Uwierzytelnianie VPN 513
Wdrażanie serwera VPN 513
Wyłączanie protokołów VPN 514
Przyznawanie prawa dostępu do serwera VPN 514
Routing LAN 519
Network Address Translation (NAT) 520
DirectAccess 521
Topologie DirectAccess 522
Serwer DirectAccess 523
Serwer lokalizacji sieciowej 525
Konfigurowanie DirectAccess 526
Zarządzanie dostępem zdalnym przy użyciu PowerShell 530

16 Usługi pulpitu zdalnego 533
Wdrożenie 533
Remote Desktop Connection Broker 535
Właściwości wdrożenia 536
Remote Desktop Session Host 537
Ustawienia kolekcji sesji 538
Osobiste sesje pulpitu 540
RemoteApp 540
Konfigurowanie zasad grupy 541
Remote Desktop Virtualization Host 543
Przygotowywanie maszyn wirtualnych 544
Kolekcje pulpitów wirtualnych 545
Pule pulpitów wirtualnych 547
Osobiste pulpity wirtualne 547
RemoteFX 547
Remote Desktop Web Access 547
Licencjonowanie pulpitu zdalnego 548
Instalowanie RDS CAL 549
Aktywowanie serwera licencji 550
Zarządzanie usługami pulpitu zdalnego przy użyciu PowerShell 550

17 Windows Server 2016 i Azure IaaS 553
Czym jest IaaS? 553
Grupy zasobów 554
Konta magazynu 555
Wirtualne sieci Azure 558
Typy maszyn wirtualnych 560
Wdrażanie maszyny wirtualnej w IaaS 561
Adresowanie IP 565
Grupy zabezpieczeń sieci 567
Pulpit zdalny 569
Przyłączanie do domeny Azure AD 569
Szyfrowane maszyny wirtualne 570
Wysoka dostępność 571
Monitorowanie i diagnostyka 572
VPN i ExpressRoute 573
Połączenia lokacja-lokacja 573
Połączenia punkt-lokacja 573

ExpressRoute . . . 574
Importowanie obrazów maszyn wirtualnych . . . 574
Azure Site Recovery . . . 575

18 Bezpieczeństwo . . . 577

Minimalne przywileje . . . 578
Kontrola dostępu oparta na rolach . . . 579
Zasady kont . . . 580
Prawa użytkowników . . . 581
Opcje zabezpieczeń konta . . . 587
Konta usługowe . . . 589
Konta chronione . . . 592
Zasady uwierzytelniania i silosy . . . 594
Credential Guard . . . 595
Just Enough Administration (JEA) . . . 597
Pliki możliwości ról . . . 599
Pliki konfiguracji sesji . . . 602
Punkty końcowe JEA . . . 603
Las administracyjny . . . 605
Zarządzanie uprzywilejowanym dostępem . . . 607
Korzyści wynikające ze stosowania PAM . . . 608
Komponenty PAM . . . 608
Użytkownicy i grupy PAM . . . 609
Role PAM . . . 610
Local Administrator Password Solution . . . 611
WSUS . . . 614
Produkty, klasyfikacje zabezpieczeń i języki . . . 614
Tryby autonomiczny i repliki . . . 614
Pliki aktualizacji . . . 616
Role zabezpieczeń WSUS . . . 617
Grupy WSUS . . . 617
Zasady WSUS . . . 618
Wdrażanie aktualizacji . . . 619
Reguły automatycznego zatwierdzania . . . 620
Device Guard . . . 622
Chronione maszyny wirtualne . . . 624
Chroniona sieć szkieletowa . . . 627
Windows Defender . . . 632

Windows Firewall with Advanced Security 633
Profile zapory 633
Reguły ruchu przychodzącego 635
Tworzenie reguł dla ruchu wychodzącego 636
Konfigurowanie IPsec 636
Reguły zabezpieczeń połączeń 639

19 Monitorowanie i konserwacja 645

Zestawy modułów zbierających dane 645
Alerty 647
Event Viewer 647
Filtry dzienników zdarzeń 648
Widoki dzienników zdarzeń 648
Subskrypcje zdarzeń 650
Zadania sterowane zdarzeniami 652
Monitorowanie sieci 653
Resource Monitor 653
Message Analyzer 653
Zaawansowane opcje inspekcji 654
Zasady inspekcji oparte na wyrażeniach 655
Inspekcja plików i folderów 655
Korzystanie z narzędzia auditpol 656
Windows Server Backup 657
Lokalizacje kopii zapasowych 658
Kopiowanie danych 659
Kopie zapasowe specyficzne dla roli i aplikacji 660
Przywracanie z kopii zapasowych 660
Przywracanie w lokalizacji alternatywnej 661
Azure Backup Agent 662
Przygotowywanie na potrzeby Azure Backup Agent 662
Wykonywanie kopii zapasowych przy użyciu Azure Backup Agent . . 663
Przywracanie z Azure Backup 664
Vssadmin 664
Safe Mode i Last Known Good Configuration 666
Konfigurowanie magazynu Boot Configuration Data 667
Polecenia cmdlet Windows PowerShell dotyczące monitorowania i konserwacji 667

20 Aktualizowanie i migracja 669
Obsługiwane ścieżki aktualizacji i migracji 669
Aktualizowanie ról i funkcji 671
Konwertowanie wersji próbnej do wersji licencjonowanej 673
Aktualizowanie wydań 674
Windows Server Migration Tools 674
Active Directory 679
Migrowanie FRS do DFSR 680
Migracja do nowego lasu 681
Active Directory Certificate Services 684
Przygotowania 686
Migracja 688
Weryfikacja i zadania pomigracyjne 689
DNS 689
DHCP 691
Przygotowania do migracji DHCP 691
Migracja 694
Weryfikacja i zadania pomigracyjne 694
Serwery plików 695
Uprawnienia migracji 696
Przygotowania do migracji 696
Migrowanie roli File and Storage Services 698
Kompatybilność aplikacji 699

21 Rozwiązywanie problemów 701
Metodologia rozwiązywania problemów 701
Ponowna instalacja 702
Symptomy i diagnoza 704
Ocenianie hipotetycznych rozwiązań 705
Stosowanie rozwiązania 706
Operations Management Suite Log Analytics 706
Narzędzia Sysinternals 708
Process Explorer 708
Process Monitor 710
ProcDump 711
PS Tools 711
VMMap 713
SigCheck 714

AccessChk 715
Sysmon 716
AccessEnum 721
ShellRunAs 722
LogonSessions 723
Active Directory Explorer 723
ADInsight 726
PsPing 727
RAMMap 728

Indeks 731

Wprowadzenie

Windows Server 2016 to więcej, niż po prostu kolejna iteracja systemu operacyjnego Windows Server. Nie tylko zawiera stertę nowych funkcji oraz zupełnie nową metodę wdrażania obciążeń poprzez kontenery Windows Server i Hyper-V, ale oferuje także wersję Nano Server, odchudzoną i przekonstruowaną wersję Windows Server o minimalnych wymaganiach dotyczących przestrzeni dyskowej i pamięci RAM.

Choć firma Microsoft skupia się ostatnio głównie na chmurze, innowacje obecne w Windows Server 2016 demonstrują, że firma nie lekceważy klientów, którzy chcą samodzielnie utrzymywać swoje rozwiązania u siebie. Windows Server 2016 nie tylko jest w stanie hostować tradycyjne role wewnętrzne, takie jak kontroler domeny, serwer DNS i DHCP, urząd certyfikacji, serwer Pulpitu zdalnego, serwer Web, plików czy host wirtualizacji, ale jest stabilnym i niezawodnym środowiskiem dla zaawansowanych obciążeń serwerowych, w tym SQL Server, Exchange Server, SharePoint czy pakiet System Center.

Książka ta ma na celu przedstawić wyczerpujący przegląd funkcjonalności Windows Server 2016. Pokażę w niej bieżące podejście do technik wdrażania i zarządzania systemem Windows Server 2016. Zademonstruję też, jak używać instalacji Server Core zamiast tradycyjnej wersji „pełnego pulpitu" i jak posługiwać się funkcjonalnością Just Enough Administration („Wystarczające uprawnienia administracyjne") środowiska PowerShell. Nadal ważne jest, aby wiedzieć, jak obsługiwać system Windows Server 2016, niezależnie od tego, czy został zainstalowany w serwerowni w piwnicy budynku, w lokalnym centrum danych, czy też w chmurze jako maszyna wirtualna Azure Infrastructure as a Service.

Dla kogo jest ta książka

Książka została napisane dla profesjonalistów IT, którzy regularnie pracują z systemami Windows Server. Najprawdopodobniej Windows Server 2016 nie będzie pierwszą wersją systemu, za którego obsługę Czytelnik jest odpowiedzialny. Większość administratorów Windows Server pracuje z różnymi wersjami systemu więcej niż dekadę, a spory odsetek ma doświadczenia sięgające wstecz do czasów Windows NT 4. Mając to na uwadze, nie poświęciłem zbyt wiele czasu i miejsca na omówienie wstępnych koncepcji czy technik, a zamiast tego skupiłem się na średnio- i bardzo zaawansowanym omówieniu najważniejszych ról i funkcji dostępnych w Windows Server 2016.

Książka została również napisana przy założeniu, że jako doświadczony profesjonalista IT, Czytelnik wie, jak użyć wyszukiwarek w celu znalezienia niezbędnych informacji technicznych. Prowadzi to do oczywistego pytania: „dlaczego miałbym kupować książkę, jeśli mogę znaleźć potrzebne informacje w wyszukiwarce?" Odpowiedź jest taka, że nawet jeśli ktoś naprawdę jest dobry w śledzeniu informacji technicznych i ma doświadczenie w odsiewaniu użytecznej wiedzy od zmyśleń, skutecznie można poszukiwać czegoś tylko wtedy, gdy ma się już jakieś pojęcie o tym, *czego* się szuka.

Podczas wystąpień na konferencjach i zjazdach użytkowników poświęconych tematyce Windows Server regularnie spotykam profesjonalistów IT, którzy spędzili wiele lat na pracy z Windows Server i nadal są nieświadomi pewnych funkcjonalności lub technik tego produktu, nawet jeśli taka funkcjonalność jest dostępna od wielu lat. Można to wytłumaczyć tym, że Windows Server 2016 zawiera tak wiele ról, faktów i ruchomych elementów, że mało prawdopodobne jest, aby ktokolwiek używał ich wszystkich w codziennej pracy, a tym samym niektóre elementy znikają z pola widzenia. Moim celem podczas pisania tej książki było zapewnienie wyczerpującego omówienia, tak by Czytelnik mógł szybko opanować zagadnienia, których dotychczas nie potrzebował znać, ale teraz musi sobie poradzić z jakimś krytycznym problemem albo po prostu rozszerzyć funkcjonalność swojego środowiska.

Konwencje używane w książce

W książce używanych jest kilka konwencji tekstowych i projektowych, które powinny pomóc w szybkim odszukaniu potrzebnych informacji.

Konwencje tekstowe

- **Skrótowe polecenia menu** Dla uproszczenia w książce używane są skrócone formy poleceń menu. Na przykład „Kliknij Tools, Track Changes, Highlight Changes" oznacza, że należy kliknąć menu Tools, wskazać pozycję Track Changes, po czym kliknąć polecenie Highlight Changes.
- **Wytłuszczona czcionka** W ten sposób wyróżniany jest tekst, który ma zostać wpisany przez czytelnika.
- **Kursywa** Nowe lub szczególnie istotne terminy wyróżniane są *kursywą*.
- **Czcionka stałopozycyjna** Taką czcionką wyróżnione są `nazwy poleceń cmdlet` (w tekście) oraz fragmenty kodu i skryptów.
- **Znak plus (+) w skrótach klawiszowych** Umieszczenie znaku plus (+) pomiędzy nazwami klawiszy oznacza, że należy nacisnąć jednocześnie klawisze połączone tym znakiem. Na przykład Ctrl+Alt+Delete oznacza, że należy jednocześnie wcisnąć klawisze Ctrl, Alt i Delete.

- **Nazwy poleceń, opcji i menu** Nazwy podawane są w wersji angielskiej. Przy pierwszym użyciu jakiegoś terminu podawany jest polski odpowiednik. Warto zauważyć, że niektóre komponenty systemu nie mają wersji spolonizowanej – w takim przypadku zostanie to zaznaczone przypisem.

Stałe elementy

> **Od podszewki**
>
> Tak oznaczone są wskazówki dla Czytelnika. W tych notkach znaleźć można pogłębione wyjaśnienia, dlaczego coś działa tak, jak działa, a także poręczne metody obejścia różnorodnych problemów.

Dodatkowe informacje

W tych notatkach zazwyczaj wskazywane są lokalizacje w Internecie, w których można znaleźć więcej informacji o bieżącym zagadnieniu. Zazwyczaj jest to łącze do odpowiedniego artykułu TechNet lub prezentacji z jakiejś konferencji.

Pomoc i informacje zwrotne

Poniższe podpunkty zawierają informacje na temat erraty, wsparcia dla książki, informacji zwrotnych i kontaktowych.

Errata i pomoc

Dokonaliśmy wszelkich starań, aby zapewnić dokładność informacji zawartych w tej książce. Dowolne błędy zgłoszone po opublikowaniu książki zostaną zamieszczone w naszej witrynie Microsoft Press pod adresem:

https://aka.ms/WinServ2016CBS/errata

W razie znalezienia błędu, który nie został jeszcze wymieniony, można go zgłosić za pośrednictwem tej samej strony.

Jeśli potrzebna jest dodatkowa pomoc, prosimy o e-mail do Microsoft Press Book Support pod adresem *mspinput@microsoft.com*.

Proszę zauważyć, że pod tymi adresami nie jest oferowana pomoc techniczna dotycząca produktów firmy Microsoft.



Rozdział 1

Narzędzia administracyjne

Zdalnie, nie lokalnie 1
Stacje robocze z dostępem uprzywilejowanym. 2
Narzędzia zdalnej administracji serwerem . 4
PowerShell 11
Pulpit zdalny. 18

Windows Server 2016 dostarczany jest z zestawem wbudowanych narzędzi, za pomocą których możemy zarządzać tym systemem operacyjnym. Choć te same zadania mogą być często wykonywane z poziomu wielu różnych narzędzi, a do tego prawie wszystko możemy zrealizować z użyciem konsoli graficznej, takiej jak Active Directory Administrative Center czy Server Manager, to zgodnie z ogólną filozofią Microsoft w zakresie administracji systemami wszelkie powtarzane przez nas zadania powinniśmy automatyzować za pomocą programu Windows PowerShell.

W tym rozdziale powiemy sobie o tym, dlaczego zadania administracyjne powinniśmy wykonywać zdalnie, co należy wziąć pod uwagę przy tworzeniu naszego zestawu narzędzi do administracji zdalnej, a także przyjrzymy się różnym narzędziom, za pomocą których możemy zdalnie administrować systemem Windows Server 2016.

Zdalnie, nie lokalnie

Windows Server 2016 projektowany był z myślą o administracji zdalnej, nie lokalnej. Przykładowo, w ramach opcji wdrożenia Nano Server, o której powiemy sobie więcej w rozdziale 2, „Opcje instalacji", z poziomu konsoli możemy wykonywać tylko podstawowe zadania konfiguracyjne. W celu wykonania jakichkolwiek bardziej zaawansowanych czynności konieczne będzie nawiązanie sesji zdalnej PowerShell lub sesji konsoli Remote Server Administration Tool (RSAT).

Tego rodzaju filozofia „najpierw zdalnie" nie powinna być zaskoczeniem dla doświadczonych administratorów. Choć niekiedy może zajść potrzeba uzyskania fizycznego dostępu do sprzętu, wykorzystywane dziś serwery i obciążenia robocze stają się coraz bardziej zwirtualizowane i skonteneryzowane. Obecnie rzadko się zdarza, aby serwery umiejscowione były w lokalnych serwerowniach, gdyż coraz częściej są one lokalizowane w odległych centrach danych lub w chmurze. Jest więc coraz mniej prawdopodobne, że jako administratorzy serwerów będziemy znajdować się w pobliżu zarządzanych przez nas maszyn. Nasza strategia administracji serwerami Windows Server 2016 powinna bazować na założeniu, że przypadek, w którym zarządzany przez nas serwer znajduje się bezpośrednio przed nami, będzie raczej wyjątkiem niż regułą.

To wymusza na nas konieczność zaznajomienia się ze sposobami wykorzystywania naszych narzędzi zdalnie, zamiast logowania się do każdego serwera indywidualnie za pomocą Pulpitu zdalnego i uruchamiania na nim określonej konsoli, odpowiedniej dla roli lub funkcji, którą chcemy zarządzać.

Od podszewki

Automatyzuj, gdzie tylko się da

Rola administratora serwerów coraz częściej uwzględnia tworzenie i wdrażanie rozwiązań automatyzacji. Gdy został wydany system Windows NT4, przeciętny administrator Windows Server odpowiedzialny był zazwyczaj za mniej niż 10 fizycznych serwerów. Dzisiaj, za sprawą automatyzacji, typowy administrator Windows Server zarządza setkami, jeśli nie tysiącami serwerów. Wykonywane przez siebie zadania powinieneś automatyzować tam, gdzie się da, i tam, gdzie ma to sens. Na dłuższą metę zredukuje to czas potrzebny na wykonywanie znanych Ci zadań, dzięki czemu będziesz mógł poświęcić więcej czasu na realizację tych zadań, których jeszcze nie potrafisz wykonać rutynowo.

Stacje robocze z dostępem uprzywilejowanym

Serwery są tak bezpieczne, jak bezpieczne są komputery wykorzystywane do zarządzania tymi serwerami. Stacje robocze z dostępem uprzywilejowanym (*Privileged Access Workstations, PAW*) są specjalnie skonfigurowanymi komputerami, które wykorzystywane są do wykonywania zadań administracji zdalnej. Koncepcja stacji roboczej PAW polega na tym, że jest to komputer z odpowiednio zabezpieczoną konfiguracją, który służy nam wyłącznie do wykonywania zadań związanych ze zdalną administracją serwerami. Nie wykorzystujemy tego komputera do odczytywania poczty elektronicznej czy przeglądania Internetu, a jedynie do wykonywania zadań administracyjnych na serwerach. W ostatnim czasie coraz częściej dochodzi do incydentów naruszenia bezpieczeństwa bezpośrednio spowodowanych tym, że komputer uprzywilejowanego użytkownika został zainfekowany złośliwym oprogramowaniem, a następnie ten sam komputer wykorzystywany był później do wykonywania zadań administracyjnych.

Stacja robocza PAW powinna zostać skonfigurowana w następujący sposób:

- Skonfigurowana funkcja Device Guard w celu zezwolenia na uruchamianie na tym komputerze wyłącznie podpisanego cyfrowo i jawnie autoryzowanego oprogramowania
- Skonfigurowana funkcja Credential Guard w celu ochrony przechowywanych na komputerze poświadczeń

- Funkcja BitLocker wykorzystywana do zaszyfrowania magazynu komputera i ochrony środowiska rozruchowego
- Komputer nie powinien być wykorzystywany do przeglądania Internetu lub sprawdzania poczty e-mail. Do wykonywania jakichkolwiek innych zadań administratorzy serwerów powinni wykorzystywać oddzielne komputery. Przeglądanie Internetu z poziomu stacji roboczej PAW należy blokować nie tylko lokalnie, ale również na zaporze sieciowej.
- Dostęp do Internetu jest na stacji roboczej PAW zablokowany. Aktualizacje oprogramowania powinny być pozyskiwane z dedykowanego, zabezpieczonego serwera aktualizacji w naszej sieci lokalnej.
- Administratorzy serwerów nie powinni logować się do stacji roboczej PAW z użyciem konta użytkownika z uprawnieniami administratora na tej stacji. W rozdziale 18, „Bezpieczeństwo", powiemy sobie o sposobach poprawiania bezpieczeństwa kont poprzez wykorzystywanie zabezpieczonych lasów kont.
- Tylko wybrane konta użytkownika wykorzystywane przez administratorów serwerów powinny być w stanie zalogować się do stacji roboczej PAW. Rozważmy wprowadzenie dodatkowych ograniczeń, takich jak godziny logowania. Blokujmy uprzywilejowane konta przed logowaniem się do komputerów, które nie są stacjami roboczymi PAW lub serwerami do zarządzania. Przykładem tego rodzaju maszyn są chociażby komputery wykorzystywane na co dzień przez pracowników IT.
- Serwery konfigurujemy w taki sposób, aby akceptowały połączenia administratora wyłącznie z poziomu stacji roboczych PAW.
- Konfigurację stacji roboczej PAW monitorujemy za pomocą narzędzi zarządzania konfiguracją. Niektóre organizacje całkowicie przebudowują swoje stacje robocze PAW co 24 godziny, aby mieć absolutną pewność, że ich konfiguracje nie zostały zmienione. Wykorzystajmy te narzędzia do ograniczenia członkostwa w grupach lokalnych i upewnijmy się, że stacja robocza PAW została wyposażona w najnowsze aktualizacje oprogramowania.
- Upewnijmy się, że dzienniki inspekcji ze stacji roboczych PAW przekierowywane są do osobnych i zabezpieczonych lokalizacji.
- Wyłączamy możliwość korzystania z nieautoryzowanych urządzeń magazynowania. Na przykład, możemy skonfigurować zasady w taki sposób, aby na komputerze można było korzystać jedynie z tych urządzeń magazynowania USB, które mają określony identyfikator organizacyjny BitLocker.
- Za pomocą zapory sieciowej Windows blokujemy nieoczekiwany ruch przychodzący do stacji roboczych PAW.

Od podszewki

Serwery przeskoku

Serwery przeskoku (*jump servers*) są kolejną procedurą zabezpieczeń, która może być wykorzystywana w połączeniu ze stacjami roboczymi z dostępem uprzywilejowanym. Koncepcja serwerów przeskoku polega na tym, że serwerom zezwala się na przyjmowanie połączeń administracyjnych wyłącznie od określonych hostów. Przykładowo możesz sprawić, że kontrolery domeny będą mogły być zarządzane tylko z poziomu komputerów dysponujących określonymi adresami IP oraz certyfikatami wydanymi przez określony urząd certyfikacji. Serwery przeskoku możesz skonfigurować w taki sposób, aby przyjmowały połączenia wyłącznie od stacji roboczych PAW. Z kolei swoje serwery, którymi zarządzasz, możesz skonfigurować tak, by akceptowały wyłącznie połączenia pochodzące od serwerów przeskoku. Niektóre organizacje wykorzystujące serwery przeskoku przebudowują je i wdrażają je ponownie co 24 godziny, co pozwala upewnić się, że ich konfiguracja w żaden sposób nie odbiega od konfiguracji zatwierdzonej.

Narzędzia zdalnej administracji serwerem

Narzędzia Remote Server Administration Tools (RSAT) stanowią zbiór konsol, które możemy zainstalować na komputerze z systemem Windows 10 w celu umożliwienia nam zarządzania komputerami z systemem Windows Server 2016. Konsole RSAT można również zainstalować na komputerze z Windows Server 2016. Jeśli chcemy zainstalować wszystkie dostępne konsole RSAT, możemy to zrobić za pomocą poniższego polecenia PowerShell:

```
Install-WindowsFeature -IncludeAllSubFeature RSAT
```

Instalacja narzędzi RSAT na komputerze z systemem Windows 10 polega na pobraniu ich najnowszej wersji bezpośrednio z witryny Microsoft. Lokalizację tych narzędzi można łatwo ustalić za pomocą dowolnej wyszukiwarki internetowej.

Od podszewki

Windows 10 dla Windows Server 2016

Narzędzia RSAT dla Windows 10 umożliwiają zarządzanie systemami Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 oraz Windows Server 2008 R2. Pakiety narzędzi RSAT dla Windows 8.1 pozwalają na zarządzanie wyłącznie serwerami pracującymi pod kontrolą systemów Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 i Windows Server 2008, nie uwzględniając przy tym systemu Windows Server 2016. Podobnie jest z narzędziami RSAT dla Windows 7, które umożliwiają zarządzanie systemami Windows Server 2008 R2 i Windows Server 2008, ale nie mogą być wykorzystywane do zarządzania serwerami Windows Server 2012, Windows Server 2012 R2 i Windows Server 2016. Krótko mówiąc, jedynie najnowsza wersja klienckiego systemu operacyjnego Windows otrzymuje wersję narzędzi SAT pozwalających na zarządzanie najnowszą wersją systemu operacyjnego Windows Server.

Konsole RSAT

Tabela 1-1 zawiera listę narzędzi RSAT, jakie dostępne są w systemie Windows Server 2016. Większość z tych narzędzi dostępnych jest z poziomu menu Tools (Narzędzia) w konsoli Server Manager.

Tabela 1-1 Konsole RSAT

Konsola	Funkcja
Active Directory Administrative Center	Zaawansowana konsola do zarządzania użytkownikami, komputerami, domenami i lasami Active Directory, jak również funkcją Dynamic Access Control i zasadami uwierzytelniania. Pozwala na wykonywanie większości zadań dostępnych w tradycyjnych konsolach zarządzania Active Directory, jakie używane były we wcześniejszych wersjach systemu Windows Server
Active Directory Domains and Trust	Konsola do konfigurowania i zarządzania relacjami zaufania pomiędzy domenami i lasami
Active Directory Rights Management Services	Zarządzanie i konfigurowanie usługami Active Directory Rights Management Services
Active Directory Sites and Services	Zarządzanie konfiguracją lokacji Active Directory, wliczając w to serwery wykazu globalnego oraz buforowanie członkostwa grup uniwersalnych

Tabela 1-1 Konsole RSAT

Konsola	Funkcja
ADSI Edit	Edytor obiektów i atrybutów Active Directory
Certification Authority	Zarządzanie usługami Active Directory Certificate Services
Cluster-Aware Updating	Zarządzanie aktualizacją typu cluster-aware
Component Services	Zarządzanie usługami składowymi, przeglądanie dziennika zdarzeń i zarządzanie usługami
Computer Management	Konsola podobna do konsoli Computer Management w systemie Windows Server 2008 R2. Pozwala na zarządzanie zadaniami, folderami udostępnionymi, użytkownikami i grupami lokalnymi, wydajnością oraz urządzeniami i usługami, umożliwiając przy tym również podgląd zdarzeń
Connection Manager Administration Kit	Umożliwia tworzenie i wdrażanie połączeń dostępu zdalnego
Defragment and Optimize Drives	Umożliwia zarządzanie defragmentacją i optymalizacją dysków
DFS Management	Zarządzanie rozproszonym systemem plików Distributed File System
DHCP	Zarządzanie serwerami Dynamic Host Configuration Protocol
Disk Cleanup	Umożliwia usuwanie plików i folderów, które nie są już dłużej potrzebne, takich jak stare aktualizacje czy pliki tymczasowe
DNS	Konfigurowanie i zarządzanie serwerami DNS
Event Viewer	Przeglądanie i zarządzanie dziennikami zdarzeń
Failover Cluster Manager	Konfigurowanie i zarządzanie klastrami pracy awaryjnej
Fax Service Manager	Konfigurowanie i zarządzanie usługą faksu
File Server Resource Manager	Konsola do zarządzania serwerami plików, wliczając w to klasyfikacje plików, raporty magazynowania oraz przydziały
Group Policy Management	Konsola do zarządzania zasadami grupy, wliczając w to uruchamianie raportów wynikowego zestawu zasad
Hyper-V Manager	Konfigurowanie i zarządzanie wirtualizacją Hyper-V
Internet Information Services (IIS) 6.0 Manager	Konfigurowanie i zarządzanie serwerem IIS w wersji 6
Internet Information Services (IIS) Manager	Konfigurowanie i zarządzanie serwerem IIS w wersji 7 i nowszymi
iSCSI Initiator	Konfigurowanie ustawień inicjatora iSCSI

Tabela 1-1 Konsole RSAT

Konsola	Funkcja
Local Security Policy	Konfigurowanie i zarządzanie ustawieniami zasad zabezpieczeń lokalnych
Network Load Balancing Manager	Konfigurowanie i zarządzanie równoważeniem obciążenia sieciowego
Network Policy Server	Zarządzanie serwerem zasad sieciowych
ODBC Data Sources (32-bit)	Zarządzanie 32-bitowymi źródłami danych ODBC
ODBC Data Sources (64-bit)	Zarządzanie 64-bitowymi źródłami danych ODBC
Online Responder Management	Konfigurowanie i zarządzanie macierzami Online Certificate Status Protocol
Performance Monitor	Przeglądanie informacji o wydajności
Print Management	Konfigurowanie i zarządzanie serwerami wydruku
Remote Access Management	Konfigurowanie i zarządzanie dostępem zdalnym
Remote Desktop Services	Konfigurowanie i zarządzanie usługami Remote Desktop Services
Resource Monitor	Monitorowanie na żywo wykorzystania zasobów pamięci, procesora, dysku i sieci
Routing and Remote Access	Konfigurowanie oraz zarządzanie usługami routingu i dostępu zdalnego, wliczając w to funkcję DirectAccess
Services	Konfigurowanie i zarządzanie usługami
Services for Network File System (NFS)	Konfigurowanie i zarządzanie sieciowym systemem plików Network File System
Shielding Data File Wizard	Zarządzanie plikami i zasadami danych ochrony
System Configuration	Zarządzanie konfiguracją systemu
System Information	Przeglądanie informacji systemowych
Task Scheduler	Konfigurowanie i zarządzanie zaplanowanymi zadaniami
Template Disk Wizard	Konfigurowanie i zarządzanie szablonowymi wirtualnymi dyskami twardymi dla chronionych maszyn wirtualnych
Volume Activation Tools	Konfigurowanie i zarządzanie licencjonowaniem grupowym
Windows Deployment Services	Konfigurowanie i zarządzanie usługami Windows Deployment Services
Windows Firewall with Advanced Security	Konfigurowanie i zarządzanie zaporą systemu Windows z zabezpieczeniami zaawansowanymi

Tabela 1-1 Konsole RSAT

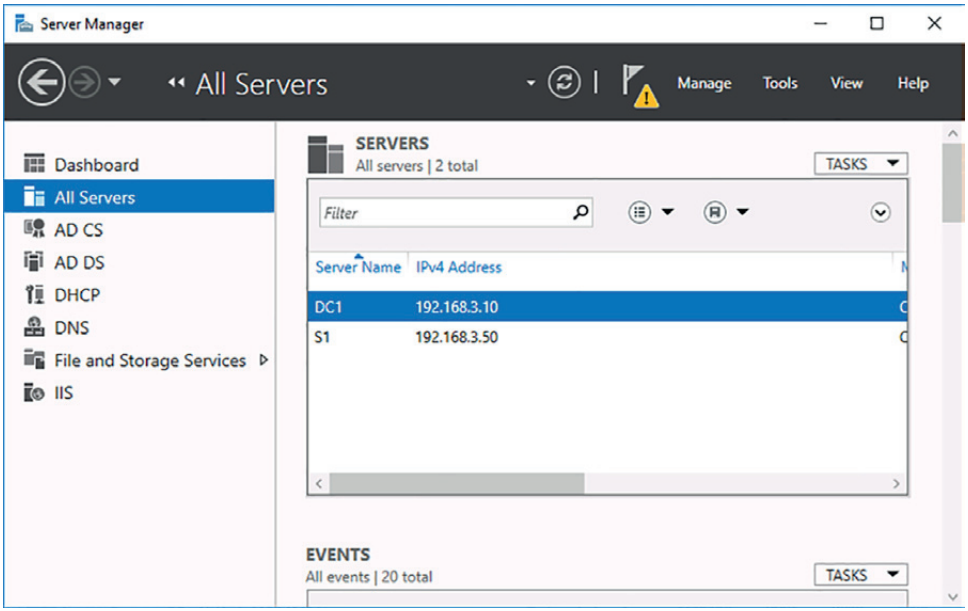
Konsola	Funkcja
Windows Memory Diagnostics	Wykonywanie diagnostyki pamięci w celu sprawdzenia, czy pamięć serwera nie jest uszkodzona. Może wymagać ponownego uruchomienia
Windows Server Backup	Konfigurowanie i zarządzanie funkcją Windows Server Backup
Windows Server Update Services	Konfigurowanie i zarządzanie serwerem aktualizacji Windows Server Update Services
WINS	Konfigurowanie i zarządzanie serwerem nazw Windows Internet Naming Services

Konsola Server Manager

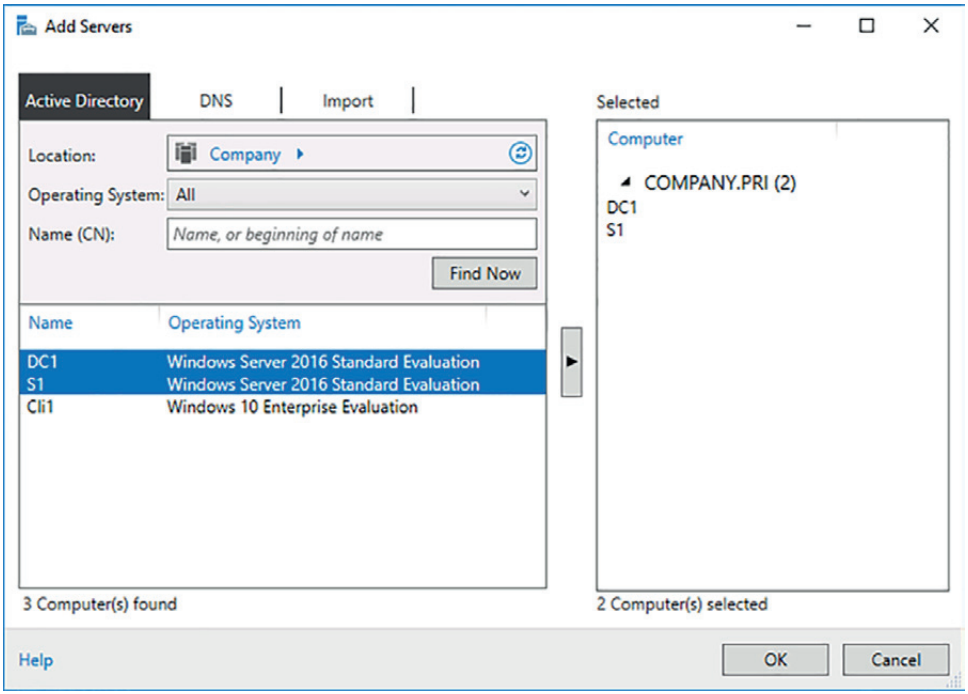
Prawdopodobnie najważniejszą konsolą oferowaną w ramach narzędzi RSAT jest konsola Server Manager. Jeśli system Windows Server 2016 zainstalowaliśmy w ramach opcji Server with Desktop Experience (Środowisko pulpitu), wówczas na takim komputerze konsola ta uruchamiać się będzie automatycznie. Część ról, dla których w poprzednich wersjach systemu Windows Server dostępne były oddzielne konsole zarządzania, ma teraz tę funkcjonalność zintegrowaną w konsoli Server Manager. Na przykład, wiele zadań zarządzania magazynem oraz zadań usługi IPAM wykonywanych dotychczas za pomocą kilku indywidualnych konsol można teraz ukończyć z poziomu konsoli Server Manager.

Po uruchomieniu konsoli Server Manager odpyta ona poszczególne serwery, które dodaliśmy do grupy All Servers (Wszystkie serwery), w celu ustalenia ról i funkcji, jakie są na tych serwerach zainstalowane. Następnie na bazie wykrytych ról przygotuje i wyświetli ona odpowiednią listę kategorii. Rysunek 1-1 pokazuje grupę All Servers złożoną z serwerów DC1 i S1. Na serwerach tych wykryte zostały role serwera AD CS, AD DS, DHCP, DNS i IIS.

Aby dodać serwery do grupy All Servers, należy w konsoli Server Manager kliknąć prawym przyciskiem węzeł All Servers i wybrać opcję Add Servers (Dodaj serwery). W oknie dialogowym Add Servers (Dodawanie serwerów), widocznym na rysunku 1-2, wybieramy docelowe serwery, przy czym możemy to zrobić na trzy sposoby: poprzez odpytanie katalogu Active Directory, wyszukanie ich po nazwie DNS lub przez zaimportowanie tych serwerów z listy.

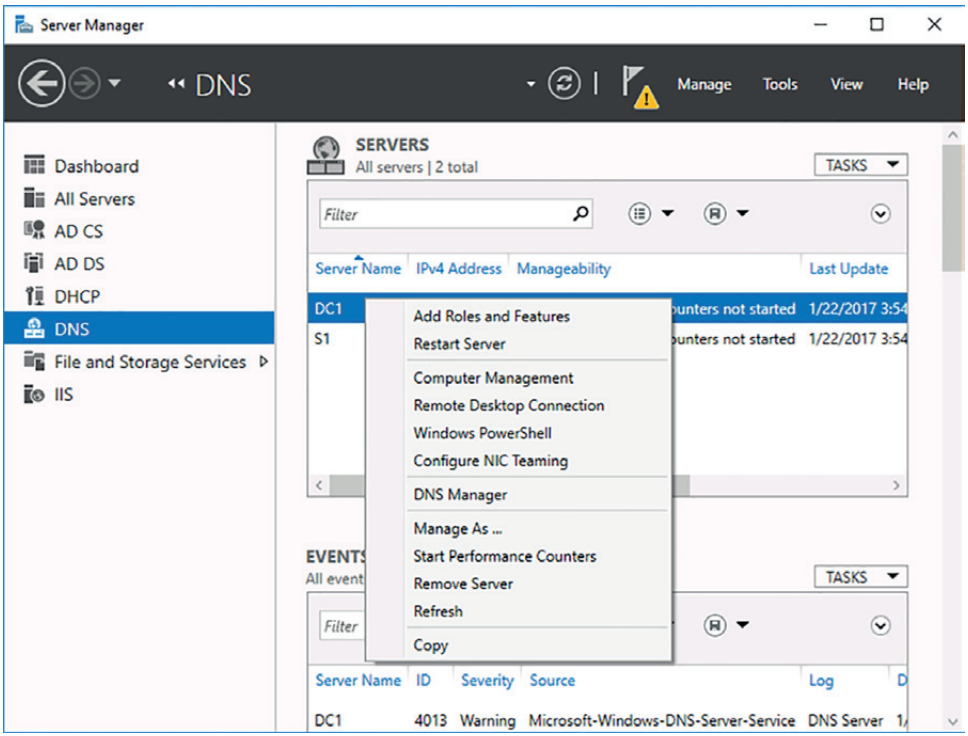


Rysunek 1-1 Lista All Servers



Rysunek 1-2 Dodawanie serwerów do listy All Servers

Mając już listę ról w konsoli Server Manager, poprzez kliknięcie wybranego serwera prawym przyciskiem myszy możemy zacząć wykonywać na nim powiązane z konkretną rolą zadania administracyjne. Gdy to zrobimy, uruchomiona zostanie odpowiednia konsola RSAT, skonfigurowana do zarządzania wybranym serwerem. Rysunek 1-3 pokazuje przykład, w którym dla serwera DC1 na liście serwerów z rolą DNS wybierana jest opcja pozwalająca na uruchomienie konsoli DNS Manager (Menedżer DNS).



Rysunek 1-3 Menu kontekstowe indywidualnego serwera w konsoli Server Manager

Menu kontekstowego wywoływanego prawym przyciskiem myszy możemy również używać do:

- Dodawania ról i funkcji do docelowego serwera
- Restartowania docelowego serwera
- Otwierania konsoli Computer Management
- Otwierania sesji pulpitu zdalnego do docelowego serwera
- Otwierania sesji Windows PowerShell na docelowym serwerze
- Konfigurowania na docelowym serwerze zespołu kart interfejsu sieciowego
- Zarządzania serwerem przy użyciu alternatywnego zestawu poświadczeń

PowerShell

PowerShell jest podstawowym narzędziem firmy Microsoft wykorzystywanym do tworzenia i wykonywania skryptów, automatyzacji oraz zarządzania. Nie jest przesadą stwierdzenie, że PowerShell jest najważniejszą umiejętnością, jaką muszą obecnie posiadać administratorzy Windows Server. Prawie we wszystkich przypadkach PowerShell zapewnia nam dostęp do znacznie szerszej funkcjonalności niż w przypadku korzystania z konsol RSAT.

PowerShell zawiera bardzo obszerną dokumentację, która szczegółowo wyjaśnia nam, co każde polecenie może dla nas zrobić i jak możemy z niego skorzystać. W każdym rozdziale tej książki będziemy poznawać nazwy poleceń PowerShell, które powiązane są z daną rolą. Gdy znamy już nazwę polecenia umożliwiającego wykonanie konkretnego zadania, wykorzystując wbudowaną pomoc programu PowerShell możemy zapoznać się ze szczegółami umożliwiającymi wykorzystanie tego polecenia do realizacji tego zadania.

Od podszewki

Najnowsza dokumentacja

Pierwszą rzeczą, jaką powinieneś zrobić na serwerze podłączonym do Internetu w przypadku korzystania z pomocy dla poleceń PowerShell, jest wykonanie polecenia Update-Help. Wykonanie tego polecenia spowoduje pobranie z serwerów Microsoft na Twój serwer lokalny najnowszej dokumentacji programu PowerShell. Jako że dokumentacja ta jest niemal zawsze taka sama, jak dokumentacja poleceń dostępna w witrynie Microsoft, nie będziesz już musiał dłużej wyszukiwać tych informacji w swojej ulubionej wyszukiwarce internetowej.

Kluczowe polecenia ułatwiające pracę z programem PowerShell zebrane zostały w tabeli 1-2.

Tabela 1-2 Polecenia pomocy PowerShell

Polecenie	Funkcjonalność
Update-Help	Aktualizuje dokumentację pomocy dla wszystkich poleceń do najnowszej dostępnej wersji
Get-Command	Wyświetla wszystkie dostępne na komputerze polecenia PowerShell

Tabela 1-2 Polecenia pomocy PowerShell

Polecenie	Funkcjonalność
Get-Command -Module <nazwa modułu>	Wyświetla wszystkie polecenia dostępne w określonym module PowerShell. Na przykład, w celu wyświetlenia wszystkich poleceń serwera DNS należy wykonać polecenie `Get-Command -Module DNSServer`
Get-Command -Noun <rzeczownik>	Każde polecenie PowerShell zbudowane jest na bazie kombinacji czasownik-rzeczownik. Za pomocą tego polecenia można przejrzeć wszystkie polecenia powiązane z określonym rzeczownikiem. Na przykład, aby wyświetlić wszystkie polecenia zawierające rzeczownik DNSServer, należy wykonać polecenie `Get-Command -Noun DNSserver`
Help <nazwa cmdlet>	Wyświetla podsumowanie dokumentacji pomocy dla określonego polecenia PowerShell
Help -detailed <nazwa cmdlet>	Wyświetla szczegółową dokumentację pomocy dla określonego polecenia PowerShell
Help -examples <nazwa cmdlet>	Wyświetla przykłady wykorzystania określonego polecenia PowerShell w celu realizacji zadań

Moduły

Moduły są kolekcjami poleceń PowerShell. Aby móc skorzystać z jakiegoś polecenia z danego modułu, w poprzednich wersjach programu PowerShell moduł ten musieliśmy wczytywać ręcznie. W systemie Windows Server 2016 dowolny zainstalowany moduł zostanie automatycznie załadowany przy próbie wykonania któregokolwiek z powiązanych z nim poleceń. Poprzez wyświetlenie poleceń dla danego modułu z użyciem polecenia `Get-Command -Module <NazwaModułu>`, możemy zapoznać się z poleceniami, które powiązane są z określoną rolą lub funkcją.

Galeria PowerShell

Galeria programu PowerShell jest zbiorem modułów opublikowanych przez społeczność, które rozszerzają standardową funkcjonalność programu PowerShell dostępną w domyślnej instalacji systemu Windows Server 2016. Tabela 1-3 zawiera polecenia, które ułatwią nam rozpoczęcie pracy z galerią PowerShell.

Tabela 1-3 Podstawowe polecenia galerii PowerShell

Polecenie	Funkcja
Find-Module -Repository PSGallery | out--host -paging	Wyświetla listę dostępnych modułów w galerii PowerShell w formacie stronicowanym. Do nawiązania komunikacji z galerią PowerShell wymagana będzie instalacja dostawcy NugetProvider
Find-Module -Repository PSGallery -Name <nazwa modułu>	Wyświetla listę modułów zawierających określoną nazwę. Można używać symboli wieloznacznych. Na przykład, aby wyświetlić wszystkie moduły rozpoczynające się od słów AzureRM, należy wykonać polecenie `Find-Module -Repository PSGallery -Name AzureRM*`
Install-Module -Repository PSGallery -Name <nazwa modułu>	Instaluje moduł o wskazanej nazwie. Na przykład, w celu zainstalowania modułu AzureRM należy wykonać polecenie `Install-Module -Repository PSGallery -Name AzureRM`
Update-Module	Dokonuje aktualizacji wszystkich modułów, które zostały zainstalowane poleceniem `Install-Module`
Get-InstalledModule	Wyświetla wszystkie moduły zainstalowane z galerii PowerShell

Obsługa zdalna

W systemie Windows Server 2016 obsługa zdalna programu PowerShell jest domyślnie włączona, przy czym standardowo wymaga ona, aby połączenie realizowane było w obrębie sieci prywatnej, z wykorzystaniem konta będącego członkiem lokalnej grupy administratorów. Sesja zdalna PowerShell pozwala na uruchamianie poleceń na komputerze zdalnym w sposób bardzo zbliżony do wykonywania poleceń w ramach sesji zdalnej SSH.

Za pomocą poniższego polecenia będziemy mogli połączyć się w ramach sesji zdalnej z komputerem Windows Server 2016, który jest członkiem tego samego lasu Active Directory. Polecenie to prosi o podanie poświadczeń, za pomocą których będziemy mogli podłączyć się do zdalnej maszyny.

```
$cred = Get-Credential
Enter-PSSession -computername <computername> -Credential $cred
```

Jeśli funkcja obsługi zdalnej PowerShell została wyłączona, możemy ją włączyć za pomocą polecenia `Enable-PSRemoting`. Obsługa zdalna PowerShell bazuje na technologii

zarządzania Web Server Management (WSMan). Usługa WSMan wykorzystuje port 5985 i może być skonfigurowana pod obsługę protokołu TLS na porcie 5986.

Połączenia zdalne PowerShell wykonywane są do odpowiednio zdefiniowanego, zazwyczaj domyślnego punktu końcowego. Konto wykorzystywane do nawiązywania połączenia z takim zdalnym punktem końcowym musi dysponować na komputerze docelowym uprawnieniami lokalnego administratora. W ramach koncepcji Just Enough Administration (JEA), o której powiemy sobie więcej w rozdziale 18, nauczymy się tworzyć dodatkowe punkty końcowe, umożliwiające nawiązywanie połączeń w ramach sesji z ograniczonymi uprawnieniami.

Aby włączyć obsługę zdalną PowerShell na komputerach, które nie są przyłączone do domeny, na komputerze klienckim, z którego zamierzamy nawiązywać te zdalne sesje, należy skonfigurować listę zaufanych hostów. Dokonujemy tego za pomocą polecenia `Set-Item`. Na przykład, aby zdefiniować zaufanie dla komputera o adresie IP 192.168.3.100, należy wykonać poniższe polecenie:

```
Set-Item wsman:\localhost\Client\TrustedHosts -Value 192.168.3.200
  -Concatenate
```

Po skonfigurowaniu klienta powyższym poleceniem będziemy mogli ustanowić sesję zdalną PowerShell ze wskazanym komputerem za pomocą polecenia `Enter-PSSession`. Jeśli potrzebujemy dodatkowych informacji na temat obsługi zdalnej, możemy wykonać poniższe polecenie, które wyświetli nam treści pomocnicze.

```
Help about_Remote_faq -ShowWindow
```

Obsługa zdalna wielu maszyn

PowerShell pozwala wykonywać pojedyncze polecenia na wielu maszynach jednocześnie. Jest to tzw. obsługa zdalna wielokierunkowa (one to many remoting), nazywana niekiedy administracją rozdysponowującą (*fan out administration*). Wielokierunkowej obsługi zdalnej możemy używać do wykonywania tego samego polecenia na dowolnej liczbie docelowych komputerów. Przykładowo, zamiast logować się na każdej z tych maszyn z osobna w celu sprawdzenia, czy dana usługa jest na tym komputerze uruchomiona, możemy z poziomu obsługi zdalnej PowerShell uruchomić jedno polecenie, które dokona sprawdzenia stanu tej usługi na każdym z komputerów objętych zakresem tego polecenia.

Na przykład, za pomocą poniższego polecenia możemy wczytać listę komputerów z pliku tekstowego o nazwie computers.txt:

```
$Computers = Get-Content c:\Computers.txt
```

po czym przy użyciu polecenia Get-Service możemy pozyskać właściwości usługi Windows Update:

```
Invoke-Command -ScriptBlock { get-service wuauserv } -computername $Computers
```

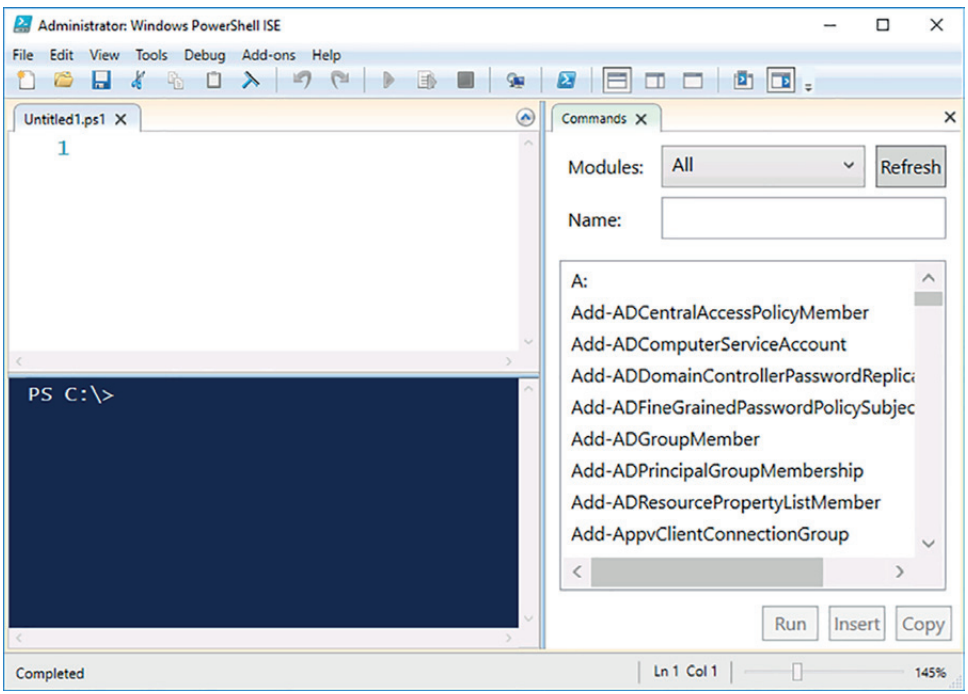
Możemy również wykorzystać polecenie `Invoke-Command` do wykonania skryptu z lokalnego komputera na dowolnej liczbie komputerów zdalnych. Przykładowo, w celu wykonania skryptu FixStuff.ps1 na komputerach wskazanych w pliku computers.txt możemy wykonać poniższe polecenie:

```
$Computers = Get-Content c:\Computers.txt
Invoke-Command -FilePath c:\FixStuff.ps1 -computername $Computers
```

PowerShell ISE

PowerShell Integrated Scripting Environment (ISE) jest narzędziem dostępnym na komputerach z systemem Windows 10 oraz graficzną instalacją systemu Windows Server 2016, za pomocą którego możemy tworzyć, zarządzać i uruchamiać skrypty oraz polecenia PowerShell.

PowerShell ISE zawiera panel skryptu i okno poleceń, a przy tym daje nam możliwość przeglądania listy dostępnych poleceń, które posortowane są według poszczególnych modułów, jak to pokazano na rysunku 1-4.



Rysunek 1-4 PowerShell ISE

PowerShell ISE oferuje następującą funkcjonalność:

- **IntelliSense** Dostarcza funkcję uzupełniania kodu. Wyświetla możliwe polecenia, parametry, wartości parametrów, pliki i foldery. Funkcjonalność uzupełniania kodu dostępna jest również w oknie poleceń.
- **Kolorowanie składni** Kod PowerShell jest odpowiednio kolorowany, co ma na celu zwiększenie jego czytelności. Kolorowanie składni dostępne jest również w oknie poleceń.
- **Debugowanie wizualne** Umożliwia krokowe wykonywanie kodu PowerShell oraz konfigurowanie i zarządzanie punktami przerwania.
- **Dopasowywanie nawiasów** Umożliwia lokalizowanie pasujących nawiasów, aby zagwarantować, że wszystkie otwarte nawiasy zostały poprawnie zamknięte.
- **Pomoc kontekstowa** Umożliwia przeglądanie informacji na temat poleceń, parametrów i wartości.
- **Wykonywanie całego kodu lub jego fragmentu** Zamiast wykonywać cały kod PowerShell w panelu skryptu, pozwala wykonywać tylko jego podświetlony fragment.

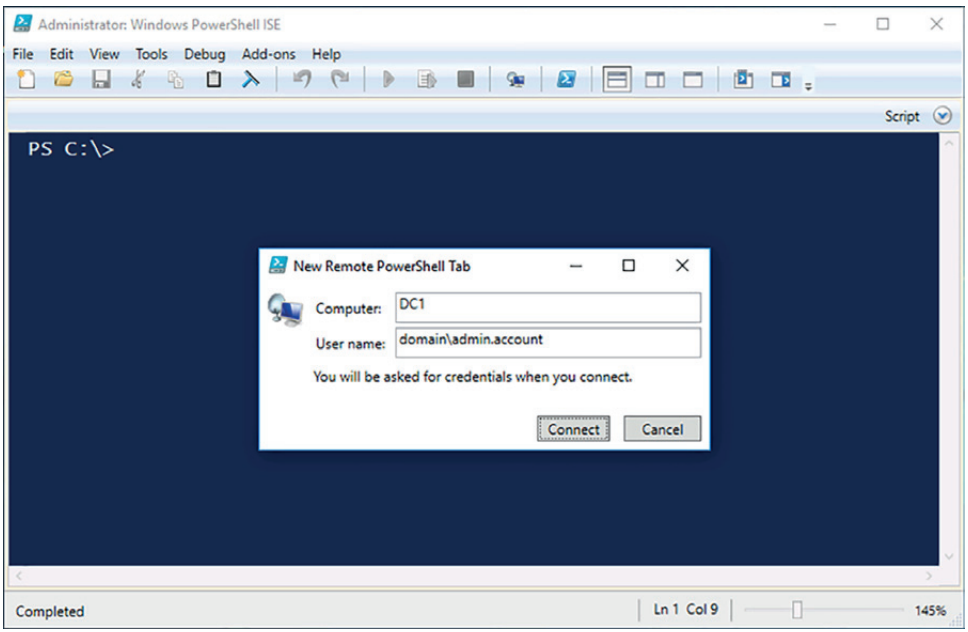
Karty zdalne

Karty zdalne umożliwiają nam nawiązywanie sesji zdalnych PowerShell z poziomu programu PowerShell ISE zamiast korzystania z polecenia `Enter-PSSession`. Aby nawiązać sesję zdalną, należy wybrać z menu File polecenie New Remote PowerShell Tab (Nowa karta zdalna PowerShell). Zostaniemy poproszeni o podanie adresu komputera, z którym chcemy się połączyć, a także nazwy konta użytkownika, w kontekście którego chcemy utworzyć sesję, jak to pokazano na rysunku 1-5.

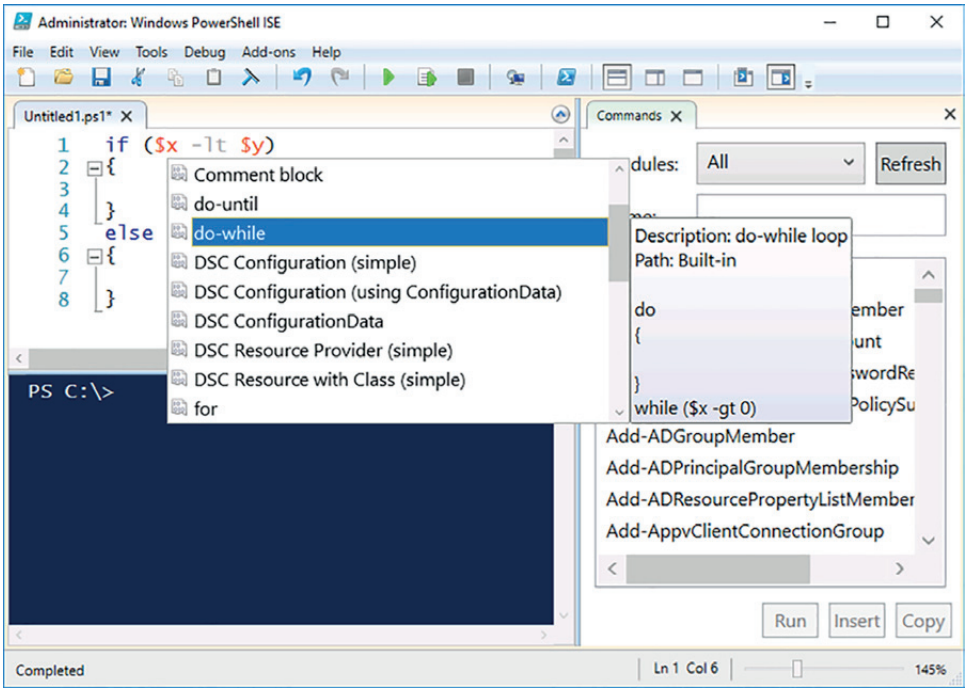
Gdy sesja jest już ustanowiona, z poziomu panelu skryptu konsoli PowerShell ISE możemy zdalnie uruchamiać skrypty i fragmenty kodu dokładnie w taki sam sposób, jak to robimy to na komputerze lokalnym.

Wstawki kodu

Wstawki kodu (*snippets*) są niewielkimi fragmentami kodu, które możemy wstawiać do naszych skryptów PowerShell. Rysunek 1-6 pokazuje wstawioną już do kodu wstawkę `If-Else`, wraz z wyświetlonymi właściwościami wstawki `Do-While`. Nowe wstawki możemy dodawać do programu PowerShell ISE za pomocą polecenia `New-Snippet`.



Rysunek 1-5 Nowa karta zdalna w programie PowerShell ISE



Rysunek 1-6 Wstawki kodu

PowerShell Direct

PowerShell Direct pozwala na utworzenie połączenia z hosta wirtualizacji do działającej na nim maszyny wirtualnej. Aby móc skorzystać z funkcji PowerShell Direct, na hoście Hyper-V musimy dysponować uprawnieniami administratora Hyper-V, zaś na maszynie wirtualnej, z którą się łączymy, musimy dysponować uprawnieniami administratora. PowerShell Direct daje nam możliwość nawiązywania połączeń z maszynami wirtualnymi, które nie zostały skonfigurowane pod obsługę połączeń zdalnych.

PowerShell Direct działa wyłącznie z hostami Hyper-V oraz systemami operacyjnymi gościa Windows Server 2016 i Windows 10. Do pozyskania listy maszyn wirtualnych działających na serwerze Hyper-V możemy użyć polecenia `Get-VM`. Aby połączyć się z wybraną maszyną w ramach funkcji PowerShell Direct, należy skorzystać z polecenia `Enter-PSSession` z parametrem `-VMName`.

Pulpit zdalny

Wielu administratorów decyduje się wykonywać zdalnie pojedyncze zadania na serwerach działających pod kontrolą systemu Windows Server 2016 z graficznym interfejsem użytkownika za pomocą Pulpitu zdalnego (*Remote Desktop*). Choć coraz częstszą praktyką staje się wykorzystywanie do administracji zdalnej programu PowerShell, czasem łatwiej i szybciej jest po prostu nawiązać sesję pulpitu zdalnego, by następnie móc wykonać określone zadania na serwerze zdalnym w sposób zbliżony do wykonywania ich po bezpośrednim zalogowaniu.

> Od podszewki
>
> **Pulpit zdalny i Azure**
>
> Pulpit zdalny pozostaje domyślną metodą łączenia się z maszynami wirtualnymi Windows Server 2016 pracującymi w ramach infrastruktury IaaS platformy Azure, gdy maszyny te wdrażane są z poziomu galerii. Więcej na temat uruchamiania systemu Windows Server 2016 na platformie Azure dowiesz się w rozdziale 17, „Windows Server 2016 i Azure IaaS".

Pulpit zdalny na komputerach z systemem Windows Server 2016 jest domyślnie wyłączony. Możemy włączyć go albo z poziomu karty Remote (Zdalny) w oknie dialogowym System Properties (Właściwości systemu), albo poniższym poleceniem PowerShell:

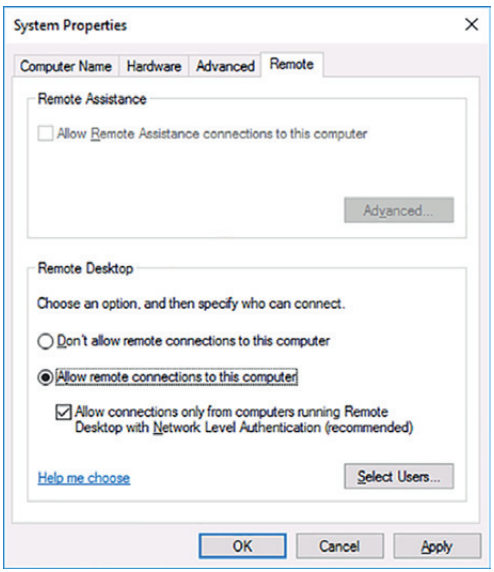
```
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal
  Server" -Name "fDenyTSConnections" –Value 0
```

Jeśli tylko funkcja Remote Desktop została na tych komputerach włączona, połączenia pulpitu zdalnego możemy nawiązywać także z komputerami z systemem zainstalowanym w trybie Server Core. Na komputerach z systemem Windows Server zainstalowanym w trybie Nano Server funkcja Remote Desktop nie jest dostępna.

Domyślnie funkcja Remote Desktop Connection (Podłączanie pulpitu zdalnego) łączy się z usługami pulpitu zdalnego na porcie 3389. W przypadku włączenia funkcji Remote Desktop z poziomu graficznego interfejsu użytkownika, powiązana z nią reguła zapory sieciowej zostanie automatycznie włączona. Jeśli jednak funkcję pulpitu zdalnego włączymy z poziomu programu PowerShell, będziemy musieli ręcznie włączyć tę regułę zapory w celu umożliwienia nawiązywania połączeń. Możemy to zrobić za pomocą poniższego polecenia PowerShell:

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Domyślnie zaznaczona jest opcja „Allow connections only from computers running Remote Desktop with Network Level Authentication" (Zezwalaj na połączenia tylko z komputerów, na których Pulpit zdalny jest uruchomiony z uwierzytelnianiem na poziomie sieci), widoczna na rysunku 1-7. Uwierzytelnianie na poziomie sieci wymaga, aby użytkownik został uwierzytelniony zanim jeszcze sesja pulpitu zdalnego zostanie nawiązana. Uwierzytelnianie na poziomie sieci obsługiwane jest przez klientów Podłączania pulpitu zdalnego na wszystkich systemach operacyjnych Windows, ale może nie być wspierane przez klientów pulpitu zdalnego zewnętrznych dostawców.



Rysunek 1-7 Karta Remote w oknie właściwości systemu

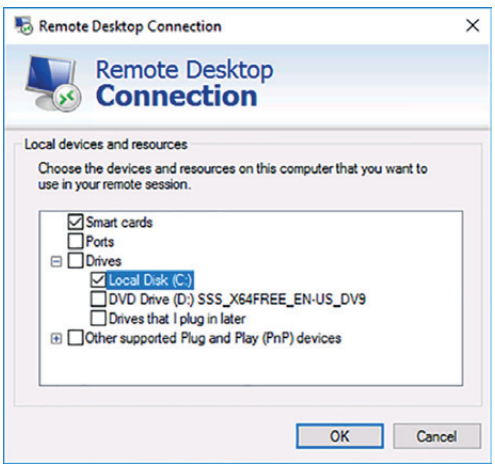
Tylko użytkownicy będący członkami lokalnej grupy administratorów oraz członkowie lokalnej grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego) mogą nawiązywać połączenia za pomocą Pulpitu zdalnego. Jeśli chcemy przyznać komuś uprawnienia dostępu do serwera bez przyznawania mu pełnych uprawnień administracyjnych, możemy dodać takiego użytkownika do lokalnej grupy Remote Desktop Users.

Od podszewki

Just Enough Administration

Technologia wystarczających uprawnień administracyjnych Just Enough Administration (JEA) pozwala na przyznawanie za pośrednictwem punktów końcowych PowerShell dostępu wyłącznie do określonych poleceń i parametrów programu PowerShell. Jest to znacznie bardziej efektywny sposób przyznawania komuś ograniczonego dostępu administracyjnego, niż przyznawanie mu dostępu Pulpitu zdalnego do serwera. Więcej na temat administracji JEA dowiesz się w rozdziale 18.

Poprzez skonfigurowanie widocznego na rysunku 1-8 ustawienia Local Devices and Resources (Lokalne urządzenia i zasoby) na karcie Local Resources (Zasoby lokalne) okna dialogowego Remote Desktop Connection możemy zmapować na zdalnym hoście nasze woluminy lokalne. Choć funkcja ta będzie mało efektywna w przypadku połączeń o niskiej przepustowości, umożliwi nam ona łatwe przesyłanie plików z naszego komputera klienckiego do serwera zdalnego, bez konieczności konfigurowania serwera FTP lub wykorzystywania innej metody transferu plików.



Rysunek 1-8 Ustawienia Local Resources and Devices



Rozdział 2

Opcje instalacji

Edycje Windows Server 2016. 21
Gałęzie obsługi Windows Server. 23
Server Core. 24
Serwer z interfejsem graficznym. 32
Role i funkcje 32
Nano Server 34

Przed zainstalowaniem systemu Windows Server 2016 będziemy musieli podjąć szereg różnych decyzji. Dokonywane przez nas wybory podyktowane będą rolą, jaką nasz serwer ma odgrywać w ramach hostowania obciążeń roboczych w naszej organizacji. Będziemy musieli wybrać, którą edycję systemu Windows Server chcemy zainstalować, a także zdecydować, czy zamierzamy zainstalować ten system w wersji Server with Desktop Experience (Serwer ze środowiskiem pulpitu) – znanej również jako Server with GUI (Serwer z interfejsem graficznym) – w wersji Server Core, czy też w wersji Nano Server. W tym rozdziale zapoznamy się z różnymi edycjami systemu Windows Server 2016, a także nauczymy się konfigurować obraz systemu Nano Server w celu jego wdrożenia.

Edycje Windows Server 2016

Istnieją dwie główne oraz kilka pomniejszych edycji systemu Windows Server 2016. Do edycji głównych zaliczamy:

- **Windows Server 2016 Standard** Edycja systemu Windows Server 2016 przeznaczona dla środowisk, w których większość serwerów wdrażana jest fizycznie zamiast w postaci maszyn wirtualnych. Licencjonowana jest w oparciu o liczbę rdzeni procesora i wymaga licencji dostępowych Client Access Licenses (CAL) dla Windows Server.
- **Windows Server 2016 Datacenter** Ta edycja systemu Windows Server 2016 jest odpowiednia dla centrów danych o wysokim stopniu wirtualizacji. Systemy w tej edycji licencjonowane są w oparciu o liczbę rdzeni procesora i wymagają licencji dostępowych CAL dla Windows Server.

Do pomniejszych edycji systemu Windows Server 2016 należą:

- **Windows Server 2016 Essentials** Ta edycja systemu Windows Server przeznaczona jest dla małych firm. Edycja ta obsługuje do 25 użytkowników i 50 urządzeń, a przy tym licencjonowana jest w oparciu o liczbę procesorów. Z uwagi

na ograniczenia co do liczby użytkowników i urządzeń, systemy w tej edycji nie wymagają licencji dostępowych CAL.

- **Windows Server 2016 Multipoint Premium Server** Edycja przeznaczona dla sektora edukacyjnego i dostępna wyłącznie dla klientów w ramach licencjonowania akademickiego. Umożliwia podłączenie wielu terminalów do specjalnie skonfigurowanego serwera usług pulpitu zdalnego i jest licencjonowana w oparciu o liczbę procesorów.
- **Windows Storage Server 2016** Funkcjonuje jako rozwiązanie magazynowania i dostępna jest wyłącznie w ramach kanałów dystrybucji OEM. Licencjonowana jest w oparciu o liczbę procesorów i nie wymaga licencji dostępowych CAL.
- **Microsoft Hyper-V Server 2016** Oferowany za darmo hiperwizor, który nie wymaga zakupu licencji serwera lub licencji dostępowych CAL.

Tabela 2-1 zawiera listę różnych ograniczeń obecnych w edycjach Standard i Enterprise systemu Windows Server 2016.

Tabela 2-1 Ograniczenia edycji

Element	Edycja Standard	Edycja Datacenter
Maksymalna liczba użytkowników	Określana liczbą posiadanych licencji dostępowych	Określana liczbą posiadanych licencji dostępowych
Maksymalna liczba połączeń SMB	16 777 216	16 777 216
Maksymalna liczba połączeń routingu i dostępu zdalnego	Brak limitu	Brak limitu
Maksymalna liczba połączeń usługi uwierzytelniania internetowego Internet Authentication Service	2 147 483 647	2 147 483 647
Maksymalna liczba połączeń pulpitu zdalnego Remote Desktop Services	65 535	65 535
Maksymalna liczba gniazd procesora x64	64	64
Maksymalna ilość pamięci RAM	24 TB	24 TB
Wliczone licencje dla zwirtualizowanych gości	2 wliczone licencje maszyn wirtualnych, jak również licencja dla hosta Hyper-V	Nielimitowane licencje maszyn wirtualnych, plus licencja dla hosta Hyper-V
Wliczone licencje dla kontenerów Windows	Nielimitowane	Nielimitowane
Wliczone licencje dla kontenerów Hyper-V	2	Nielimitowane

Podstawową różnicą pomiędzy tymi dwoma systemami jest sposób licencjonowania na nich maszyn wirtualnych. Edycja Datacenter pozwala nam na hostowanie nieograniczonej liczby maszyn wirtualnych. Z kolei edycja Standard zezwala na hostowanie dwóch maszyn wirtualnych, a jakakolwiek dodatkowa liczba tych maszyn będzie wymagać zakupienia dla nich odrębnych licencji. Warto zapoznać się z bieżącym cennikiem licencjonowania, jednak zazwyczaj jest tak, że w przypadku hostowania więcej niż sześciu maszyn wirtualnych z systemem Windows Server (lub więcej niż sześciu kontenerów Hyper-V), lepiej na tym wyjdziemy, jeśli zakupimy edycję Datacenter.

Na poziomie ról wspieranych w edycjach Standard i Datacenter systemu Windows Server 2016 jedyną różnicą jest to, że edycja Datacenter obsługuje hostowanie chronionych maszyn wirtualnych, a więc coś, czego nie można osiągnąć przy wykorzystaniu edycji Standard. Chronione maszyny wirtualne są maszynami wirtualnymi szyfrowanymi technologią BitLocker, dzięki czemu nie mogą być one modyfikowane przez administratora wirtualizacji.

Kolejną różnicą pomiędzy tymi dwoma edycjami jest to, że edycja Datacenter wspiera dziedziczoną aktywację zarówno jako host, jak i maszyna wirtualna gościa. Edycja Standard wspiera aktywację dziedziczoną tylko wtedy, gdy hostowana jest na maszynie wirtualnej gościa na hoście Hyper-V, który działa pod kontrolą systemu w edycji Datacenter. Aktywacja dziedziczona polega na tym, że aktywacja dokonywana jest automatycznie na podstawie edycji systemu Windows Server. W przypadku hostowania dużej liczby maszyn wirtualnych Windows Server 2016, pozwala to zaoszczędzić sporo czasu, jako że nie musimy w tym celu wykorzystywać kluczy licencyjnych lub serwerów KMS.

Gałęzie obsługi Windows Server

W zależności od wybranej przez nas opcji instalacji, Windows Server 2016 wspierał będzie jedną z dwóch oddzielnych gałęzi obsługi: długoterminową gałąź Long Term Servicing Branch (LTSB) oraz gałąź bieżącą Current Branch for Business (CBB).

LTSB

Gałąź LTSB oferuje pięć lat głównego wsparcia oraz pięć lat wsparcia rozszerzonego. Jest to więc wsparcie zbliżone do wsparcia świadczonego w poprzednich wersjach systemu Windows Server, jak na przykład systemu Windows Server 2012 R2. Ten rodzaj wsparcia oznacza, że Microsoft będzie dostarczał aktualizacje dla komputerów korzystających z LTSB przez co najmniej 10 lat licząc od momentu wydania systemu Windows Server 2016.

LTSB jest jedyną gałęzią obsługi, która dostępna jest dla serwerów zainstalowanych w ramach opcji instalacji Server Core i Server with GUI.

CBB

Wydanie CBB dostarczane będzie ze wsparciem i aktualizacjami oprogramowania od Microsoft, które obowiązywać będą do momentu wydania następnej+1 wersji gałęzi bieżącej. W dowolnym momencie wsparcie CBB może być oferowane wyłącznie dla dwóch gałęzi bieżących i ma zastosowanie tylko do komputerów wdrożonych w ramach opcji instalacji Nano Server. Na przykład, jeśli nasza organizacja dokona wdrożenia wersji CBB#1 serwera Nano Server, wówczas ta wersja serwera Nano nadal otrzymywać będzie aktualizacje i wsparcie aż do momentu wydania wersji CBB#3.

Wsparcie LTSB nie jest dostępne dla serwera Nano, zaś wsparcie CBB nie jest dostępne dla serwerów wdrożonych w ramach opcji instalacji Server Core i Server with GUI. Nano Server wspierany jest w produkcji wyłącznie w obrębie organizacji, które podpisały z firmą Microsoft umowę Software Assurance.

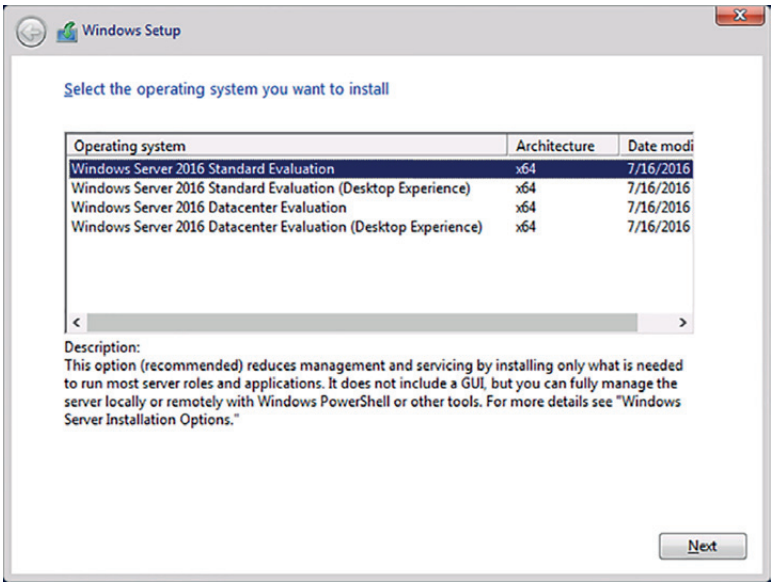
> Od podszewki
>
> **Nano Server jest krótkoterminowy**
>
> Choć dokładny czas uzależniony jest od tego, kiedy poszczególne wersje CBB serwera Nano zostaną wydane, wdrożenie serwera Nano będzie prawdopodobnie objęte 18-miesięcznym wsparciem, zaś po tym okresie konieczne będzie dokonanie uaktualnienia do nowej wersji systemu Nano Server. Zamiast uaktualniania w miejscu Microsoft wydaje się preferować migrowanie obciążeń roboczych, tak więc na hostach działających pod kontrolą systemu Nano Server powinieneś unikać wdrażania obciążeń długoterminowych.

Server Core

Server Core jest domyślną opcją instalacji systemu Windows Server 2016. Ponieważ na Server Core składa się mała liczba komponentów, system ten nie musi być tak często aktualizowany, jak na przykład opcja instalacji Server with GUI. Ponieważ niektóre komponenty, takie jak wbudowana przeglądarka internetowa są z tego systemu usunięte, Server Core jest mniej podatny na zagrożenia niż opcja instalacji Server with GUI. Co więcej, ponieważ system ten nie wymaga do pracy wszystkich komponentów, cechuje go mniejsze wykorzystanie zasobów.

W przeciwieństwie do poprzednich wersji instalatora, w systemie Windows Server 2016 opcja instalacji Server Core nie jest jawnie określona, co zostało pokazane na rysunku 2-1. Wersja oznaczona jako Desktop Experience (Środowisko pulpitu) jest opcją serwera z interfejsem graficznym. Z kolei wersja pozbawiona tego dodatku jest wersją Server Core. Może się więc zdarzyć, że przy odrobinie nieuwagi niechcący

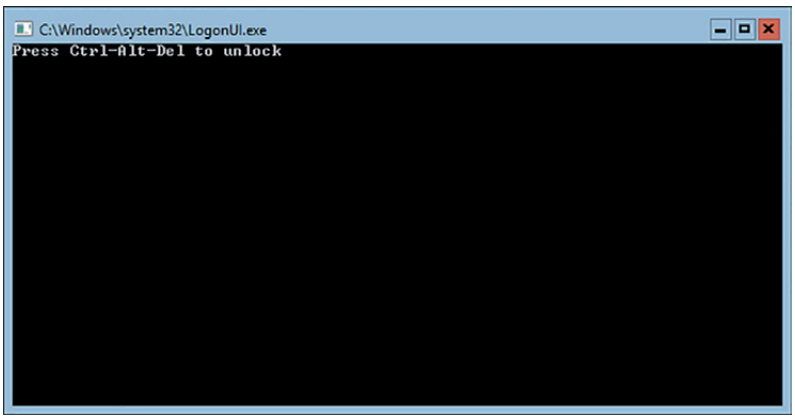
dokonamy wdrożenia systemu w wersji Server Core, zamiast serwera z interfejsem graficznym.



Rysunek 2-1 Opcje instalacji systemu Windows Server 2016

Interfejs systemu Server Core

Interfejs systemu Server Core oparty jest na wierszu polecenia. Jak pokazano na rysunku 2-2, aby móc zacząć wydawać polecenia, musimy najpierw odblokować komputer za pomocą klawiszy Ctrl+Alt+Del, a następnie zalogować się za pomocą lokalnego lub domenowego konta administratora.



Rysunek 2-2 Pulpit systemu Server Core

Gdy się już zalogujemy, za pomocą polecenia PowerShell.exe możemy uruchomić lokalną sesję programu PowerShell. Server Core jest przede wszystkim tekstowym środowiskiem wiersza poleceń, przy czym dostępne są pewne narzędzia graficzne, które mogą być uruchamiane z poziomu wiersza poleceń lub menedżera zadań. Są to:

- **Task Manager (Menedżer zadań)** Funkcjonuje tak samo jak Menedżer zadań dostępny w interfejsie graficznym Windows Server lub Windows 10. Możemy wykorzystać go do uruchamiania zadań poprzez skorzystanie z opcji Run New Task (Uruchom nowe zadanie) dostępnej w menu File (Plik).
- **Notepad (Notatnik)** Uruchamiany poleceniem Notepad.exe umożliwia edytowanie i przeglądanie zawartości plików tekstowych.
- **MSInfo32.exe** Pozwala przeglądać informacje na temat bieżącej instalacji systemu.
- **Regedit.exe i Regedt32.exe** Pozwalają na edytowanie rejestru na komputerze Server Core.
- **TimeDate.cpl** Otwiera aplet Time and Date (Data i godzina) panelu sterowania.
- **Intl.cpl** Otwiera aplet ustawień regionalnych panelu sterowania.
- **Iscsicpl.exe** Otwiera aplet iSCSI Initiator Properties (Właściwości: Inicjator iSCSI) panelu sterowania. Umożliwia połączenie z magazynem danych udostępnionym poprzez iSCSI.

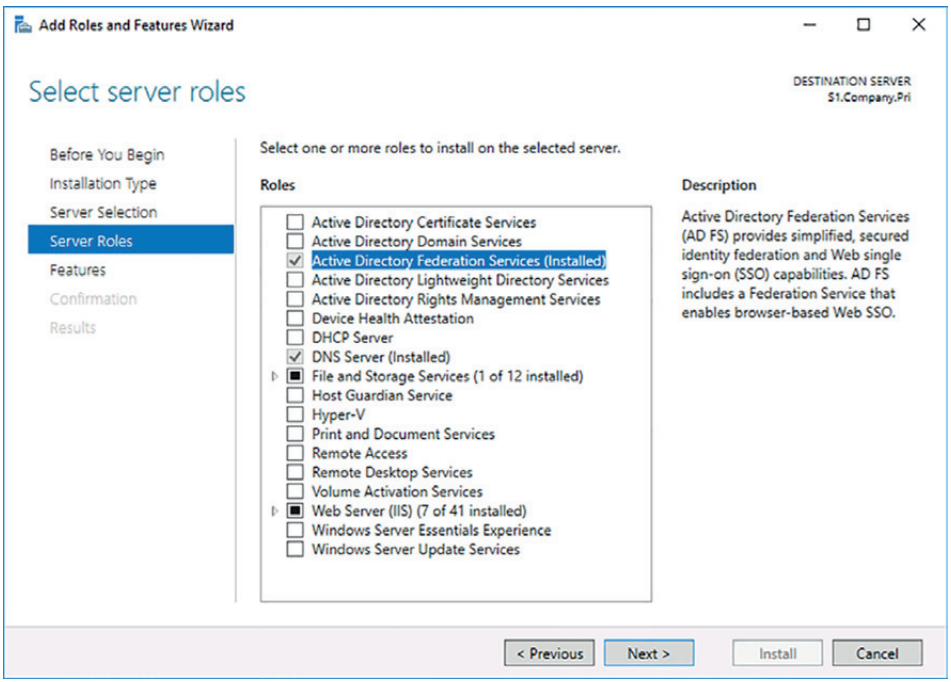
Od podszewki

Ups...

Jeśli w wierszu poleceń systemu Server Core wpiszesz Exit, okno wiersza poleceń zostanie zamknięte. W celu jego przywrócenia wielu administratorów ponownie uruchamia swój serwer, jednak istnieje na to znacznie prostszy sposób. Jeśli przypadkowo zamknąłeś wiersz polecenia, wciśnij skrót Ctrl+Alt+Del, wybierz Task Manager, następnie kliknij More Details (Więcej szczegółów), File oraz Run New Task, po czym wpisz `cmd.exe`. W ten sposób przywrócisz wiersz polecenia, bez konieczności wylogowywania się lub ponownego uruchamiania komputera.

Role w systemie Server Core

Server Core obsługuje następujące role serwera, które możemy zainstalować za pomocą polecenia PowerShell o nazwie `Add-WindowsFeature` lub z poziomu kreatora Add Roles and Features Wizard (Kreator dodawania ról i funkcji). Rysunek 2-3 pokazuje role systemu Server Core, jakie dostępne są w konsoli Server Manager wyświetlającej listę roli na komputerze zdalnym.



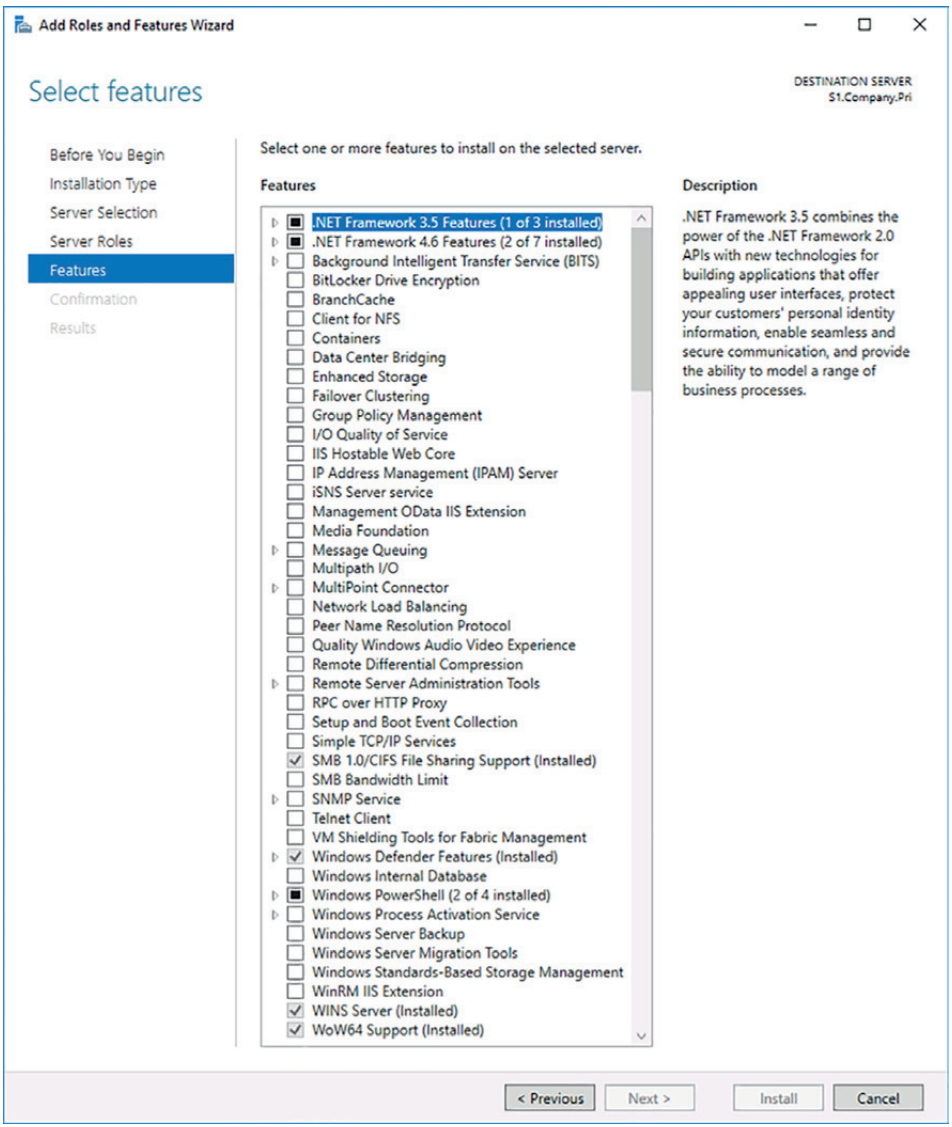
Rysunek 2-3 Role serwera Server Core

- Active Directory Certificate Services (Usługi certyfikatów Active Directory)
- Active Directory Domain Services (Usługi domenowe Active Directory)
- Active Directory Federation Services (Usługi federacyjne Active Directory)
- Active Directory Lightweight Directory Services (Usługi LDS w usłudze Active Directory)
- Active Directory Rights Management Services (Usługi zarządzania prawami dostępu w usłudze Active Directory)
- Device Health Attestation (Zaświadczanie o kondycji urządzeń)
- DHCP Server (Serwer DHCP)
- DNS Server (Serwer DNS)
- File and Storage Services (Usługi plików i magazynowania)
- Host Guardian Service (Usługa Ochrona hosta)
- Hyper-V
- Print and Document Services (Usługi drukowania i zarządzania dokumentami)
- Routing and Remote Access Server (Usługi routingu i dostępu zdalnego)
- Remote Desktop Services Connection Broker (Broker połączeń usług pulpitu zdalnego)

- Web Server (Serwer sieci Web, w tym również części ASP.NET)
- Windows Server Essentials Experience (Środowisko systemu Windows Server Essentials)
- Windows Server Update Services

Server Core wspiera ponadto następujące funkcje, pokazane również na rysunku 2-4.

- .NET Framework 3.5 (Funkcje programu .NET Framework 3.5)
- .NET Framework 4.6 (Funkcje programu .NET Framework 4.6)
- Background Intelligent Transfer Service (Usługa inteligentnego transferu w tle)
- BitLocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker)
- BranchCache
- Client for NFS (Klient systemu plików NFS)
- Containers (Kontenery)
- Data Center Bridging (Mostkowanie centrum danych)
- Enhanced Storage (Magazyn rozszerzony)
- Failover Clustering (Klaster pracy w trybie Failover)
- Group Policy Management (Zarządzanie zasadami grupy)
- I/O Quality of Service
- IIS Hostable Web Core (Obsługiwane podstawowe funkcje usług IIS)
- IP Address Management Server (Serwer zarządzania adresami IP, IPAM)
- iSNS Server service (Usługa serwera iSNS)
- Management OData IIS Extension (Rozszerzenie usług IIS OData dla usługi zarządzania)
- Media Foundation
- Message Queuing (Kolejkowanie komunikatów)
- Multipath I/O (Wielowejściowe We/Wy)
- MultiPoint Connector
- Network Load Balancing (Równoważenie obciążenia sieciowego)
- Peer Name Resolution Protocol (Protokół rozpoznawania nazw równorzędnych)
- Quality Windows Audio Video Experience
- Remote Differential Compression (Kompresja RDC)
- Remote Server Administration Tools (Narzędzia administracji zdalnej serwera)
- RPC over HTTP Proxy (Zdalne wywoływanie procedur za pośrednictwem serwera proxy)



Rysunek 2-4 Funkcje systemu Server Core

- Setup and Boot Event Collection (Kolekcja zdarzeń instalacji i rozruchu)
- Simple TCP/IP Services (Usługi Simple TCP/IP)
- SMB 1.0/CIFS File Sharing Support (Obsługa udostępniania plików SMB 1.0/CIFS)
- SMB Bandwidth Limit
- SNMP Service (Usługa SNMP)

- Telnet Client (Klient Telnet)
- VM Shielding Tools for Fabric Management (Narzędzia ochrony maszyn wirtualnych na potrzeby zarządzania siecią szkieletową)
- Windows Defender Features (Funkcje usługi Windows Defender)
- Windows Internal Database (Wewnętrzna baza danych systemu Windows)
- Windows PowerShell
- Windows Process Activation Service (Usługa aktywacji procesów systemu Windows)
- Windows Server Backup (Kopia zapasowa systemu Windows Server)
- Windows Server Migration Tools (Narzędzia migracji systemu Windows Server)
- Windows Standards-Based Storage Management (Zarządzanie magazynami systemu Windows oparte na standardach)
- WinRM IIS Extension (Rozszerzenie WinRM usług IIS)
- WINS Server (Serwer WINS)
- WoW64 Support (Obsługa emulatora WoW64)

Choć powyższe role i funkcje mogą być instalowane i zarządzane z poziomu programu PowerShell – czy to lokalnie, czy też w ramach sesji zdalnej – większość administratorów będzie raczej wdrażać i zarządzać tymi składnikami za pośrednictwem konsol administracji zdalnej.

Jak dowiedzieliśmy się w rozdziale 1, „Narzędzia administracyjne", Microsoft zachęca organizacje do tego, aby wszystkimi swoimi serwerami zarządzały zdalnie. Nie ma więc znaczenia, że Server Core nie oferuje graficznego interfejsu użytkownika, gdyż do serwerów prawie nigdy nie będziemy logować się bezpośrednio, a zamiast tego będziemy się z nimi łączyć za pomocą narzędzi administracji zdalnej.

Kiedy wdrażać Server Core

Podstawą wdrożenia systemu Server Core w naszej organizacji powinno być ustalenie, czy nadaje się on do wykorzystania pod konkretne obciążenie robocze. Server Core jest idealny dla ról z zakresu infrastruktury, takich jak kontrolery domeny, serwery DNS, serwery DHCP i serwery plików, natomiast nieco słabiej wypada w kontekście hostowania aplikacji o złożonych zależnościach.

Jeśli rozważamy wdrożenie systemu Server Core, powinniśmy najpierw wykonać odpowiednie testy, aby mieć pewność, że wszystkie rozpatrywane przez nas obciążenia robocze działają na nim zgodnie z oczekiwaniami. Mimo że Server Core jest obecnie opcją instalacji, jaka zalecana jest przez Microsoft, hostowane na serwerze aplikacje firm trzecich mają często pewne zależności, które do poprawnego działania wymagają graficznego interfejsu użytkownika.

Od podszewki

Blokada opcji instalacji

Systemy Windows Server 2012 i Windows Server 2012 R2 umożliwiały przełączanie się pomiędzy opcjami instalacji Server Core i Server with GUI, pozwalając administratorom na wdrożenie serwera z interfejsem graficznym, a następnie zredukowanie go do wersji Server Core w celu pozbycia się wszystkich niepotrzebnych komponentów, jakie uruchamiane są w środowisku graficznym. Administratorzy, którzy wdrożyli opcję Server Core, mieli również pewne wyjście awaryjne. Gdy okazywało się, że nie mogą oni uruchamiać konkretnej aplikacji w środowisku Core, mogli w dowolnym momencie przekształcić ten serwer w opcję instalacji Server with GUI. Windows Server 2016 nie oferuje już takiej możliwości, tak więc opcja instalacji wybierana jest w tym systemie na stałe. Takie podejście jest co prawda zgodne z filozofią firmy Microsoft, według której w przypadku chęci wprowadzenia szerszych zmian zamiast modyfikować istniejące wdrożenie powinno się przeprowadzić wdrożenia od nowa, ale jednak może to oznaczać, że na wdrożenie opcji Server Core zdecyduje się mniejsza liczba administratorów. Może tak być, ponieważ wiedzą oni, że wykorzystywane przez nich aplikacje zawsze będą działać na serwerze z interfejsem graficznym, ale już nikt nie zagwarantuje im działania tych aplikacji w systemie Server Core.

Od podszewki

Wget

Często jest tak, że w celu wykonania na serwerze pewnego zadania administratorzy muszą pobrać na niego określony plik z lokalizacji sieciowej lub internetowej. W przypadku, gdy serwer ten znajduje się w sieci brzegowej, proces ten może się okazać dość skomplikowany, jako że administrator nie ma możliwości bezpośredniego przekopiowania takiego pliku (lub plików) z udziału sieciowego. Systemy Server Core i Nano Server nie są wyposażone w przeglądarkę, tak więc nie ma możliwości pozyskania takich plików z poziomu programu Internet Explorer. W takim przypadku można jednak skorzystać z polecenia `Wget` programu PowerShell (będącego aliasem dla polecenia `Invoke-WebRequest`) i za jego pomocą pobrać wybrany plik z lokalizacji internetowej wprost do systemu plików komputera, na którym polecenie to zostało uruchomione.

Wersję Server Core można zainstalować przy użyciu nośnika instalacyjnego systemu Windows Server 2016, jak również wdrożyć go za pomocą wielu różnych metod przy wykorzystaniu pliku install.wim, który zlokalizowany jest na nośniku instalacyjnym.

Więcej informacji na temat wdrażania i konfigurowania systemu Windows Server 2016 znajduje się w rozdziale 3, „Wdrożenie i konfiguracja".

Serwer z interfejsem graficznym

Opcja instalacji Server with GUI, oficjalnie znana jako Server with Desktop Experience (Serwer ze środowiskiem pulpitu), jest wersją systemu Windows Server, którą profesjonaliści IT znali i zarządzali już w latach 90-tych ubiegłego wieku, a tym samym są z nią najbardziej zaznajomieni. Serwer ten oferowany jest z pełnym środowiskiem graficznym, wliczając w to również przeglądarkę internetową. Na serwerze z interfejsem graficznym możemy także zainstalować oprogramowanie, które standardowo zainstalowalibyśmy na komputerze z systemem operacyjnym Windows 10.

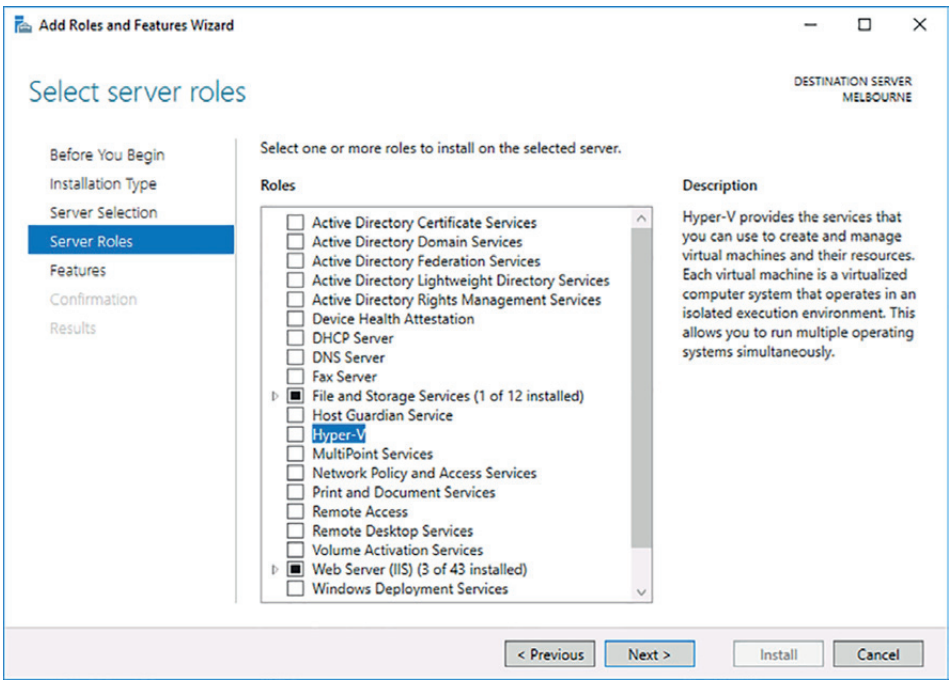
Serwery z interfejsem graficznym wdrażamy przeważnie wtedy, gdy zachodzi potrzeba hostowania serwerów sesji pulpitu zdalnego, a także wtedy, gdy potrzebujemy zainstalować aplikację, której zależności nie są dostępne w systemie Server Core.

Microsoft zaleca, aby system Windows Server 2016 wdrażany był z interfejsem graficznym tylko w sytuacjach, w których wdrożenie systemu Server Core lub Nano Server byłoby niepraktyczne. Obecnie wielu administratorów, którzy z systemem Windows Server pracowali przez lata, wybierze zapewne opcję instalacji Server with GUI, chociażby z samego przyzwyczajenia. W przyszłości jednak serwer ze środowiskiem pulpitu będziemy raczej wdrażać tylko w sytuacjach wyjątkowych.

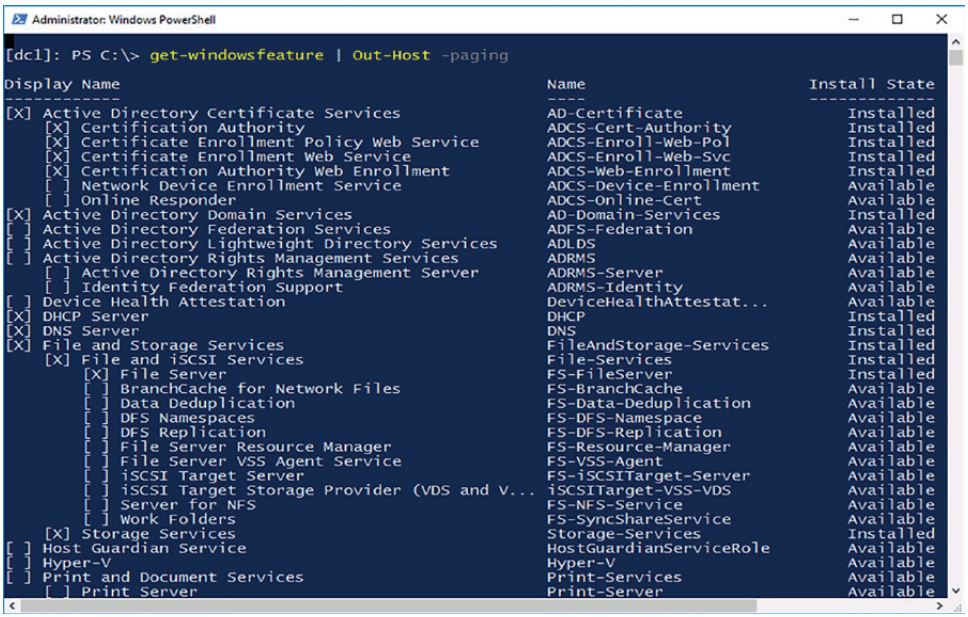
Role i funkcje

Jeśli nie zapoznaliśmy się jeszcze dobrze z systemem Windows Server 2016, to zapewne w celu dodania lub usunięcia roli lub funkcji z komputera wdrożonego w ramach opcji instalacji Server with GUI posłużymy się kreatorem Add Roles and Features Wizard, przedstawionego na rysunku 2-5. Choć narzędzie to może być wykorzystywane zarówno zdalnie, jak i lokalnie, to za jego pomocą w danej chwili będziemy mogli zarządzać rolami i funkcjami tylko jednego serwera.

Program PowerShell dostarcza znacznie lepszych narzędzi umożliwiających dodawanie, usuwanie i sprawdzanie stanu funkcji w postaci poleceń `Add-WindowsFeature`, `Get-WindowsFeature` i `Remove-WindowsFeature`. Rysunek 2-6 pokazuje fragment listy wszystkich możliwych do zainstalowania na serwerze funkcji. Niektóre z nich, takie jak Active Directory Certificate Services, Active Directory Domain Services, DHCP Server, DNS Server czy File and Storage Services, są już zainstalowane.



Rysunek 2-5 Kreator dodawania ról i funkcji



Rysunek 2-6 Przegląd zainstalowanych funkcji z poziomu programu PowerShell

Przykładowo, za pomocą poniższych poleceń rolę Hyper-V możemy zainstalować na wszystkich komputerach, jakie wylistowane zostały w pliku tekstowym virt-servers.txt. Po zakończeniu instalacji tej roli komputer zostanie automatycznie zrestartowany:

```
$Computers = Get-Content c:\virt-servers.txt
$Invoke-Command -ScriptBlock { Add-WindowsFeature Hyper-V -Restart }
  -Computername $Computers
```

Od podszewki

Żądany stan

Dodawanie lub usuwanie ról i funkcji z poziomu konsoli Server Manager lub programu PowerShell będzie rozsądnym wyjściem w przypadku, gdy do zmodyfikowania będziesz mieć niewielką liczbę serwerów. Jeśli musisz dokonać wdrożenia dużej liczby serwerów o identycznej konfiguracji ról i funkcji, lepiej będzie, jeśli posłużysz się w tym celu specjalnymi narzędziami zarządzania konfiguracją, takimi jak Chef, Puppet czy PowerShell Desired State Configuration. Za pomocą tych narzędzi będziesz mógł dokonać wdrożenia serwerów, zaś system zarządzania konfiguracją skonfiguruje na nich odpowiednie role, funkcje i ustawienia, zgodnie z podaną specyfikacją. Więcej informacji na temat wykorzystywania tych narzędzi znajdziesz w rozdziale 3.

Nano Server

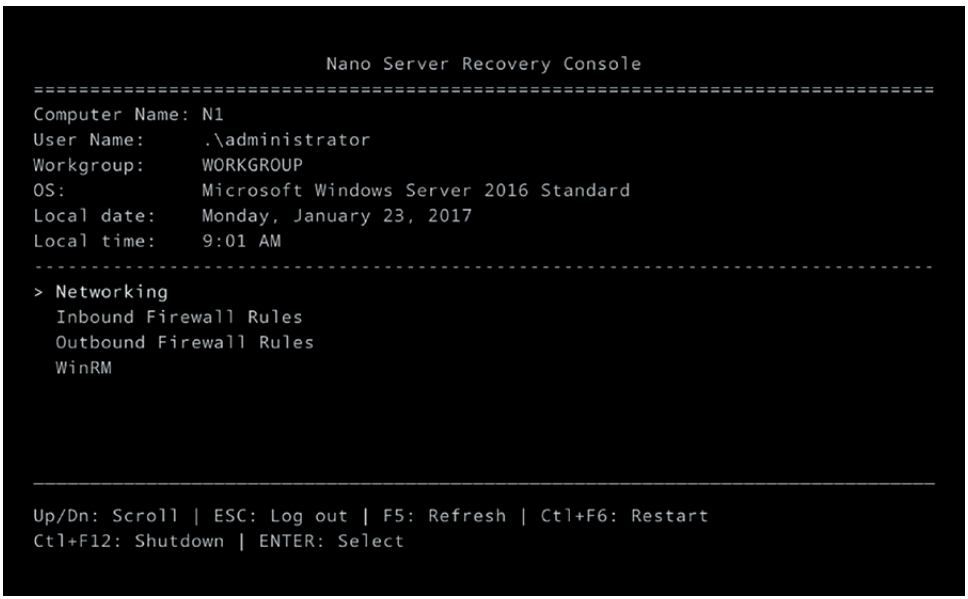
Nano Server jest okrojoną wersją systemu Windows Server 2016, która wymaga do pracy minimalnej ilości pamięci RAM i przestrzeni dyskowej. Dzięki temu, że Nano Server zawiera wyłącznie te elementy, które są niezbędne do wykonywania określonych zadań, systemowi temu do pracy wystarcza już kilkaset megabajtów pamięci RAM i kilkaset megabajtów przestrzeni dyskowej. Oznacza to, że na jednym hoście Hyper-V możemy uruchamiać znacznie więcej maszyn wirtualnych z systemem Nano Server, niż możemy uruchamiać instancji Windows Server w opcjach instalacji Server Core i Server with GUI, które do swojego działania wymagają dużo większej ilości zasobów.

W ramach tradycyjnego procesu wdrażania systemu Windows Server 2016 dokonujemy najpierw wdrożenia takiego serwera, a następnie w miarę potrzeb dodajemy do niego odpowiednie role i funkcje. Jest to możliwe, ponieważ wszystkie pliki pozwalające na zainstalowanie tych składników są już zawarte we wdrożonym systemie. Dostępność tych plików zapewnia nam co prawda znacznie większą elastyczność w zakresie możliwości modyfikowania konfiguracji wdrożonego serwera, jednak odbywa się to kosztem zwiększonej ilości danych, jakie muszą być na tym serwerze przechowywane.

Podstawową różnicą pomiędzy systemem Nano Server a pozostałymi serwerowymi systemami operacyjnymi firmy Microsoft jest to, że dostarczana w nim konsola tekstowa istnieje tylko po to, aby umożliwić nam dostęp zdalny do takiego serwera. Zamiast logować się na tym serwerze lokalnie i wykonywać na nim zadania administracyjne, Nano Server został zaprojektowany w taki sposób, aby po wykonaniu konfiguracji wstępnej wszystkie zadania administracyjne na tej maszynie wykonywane były zdalnie.

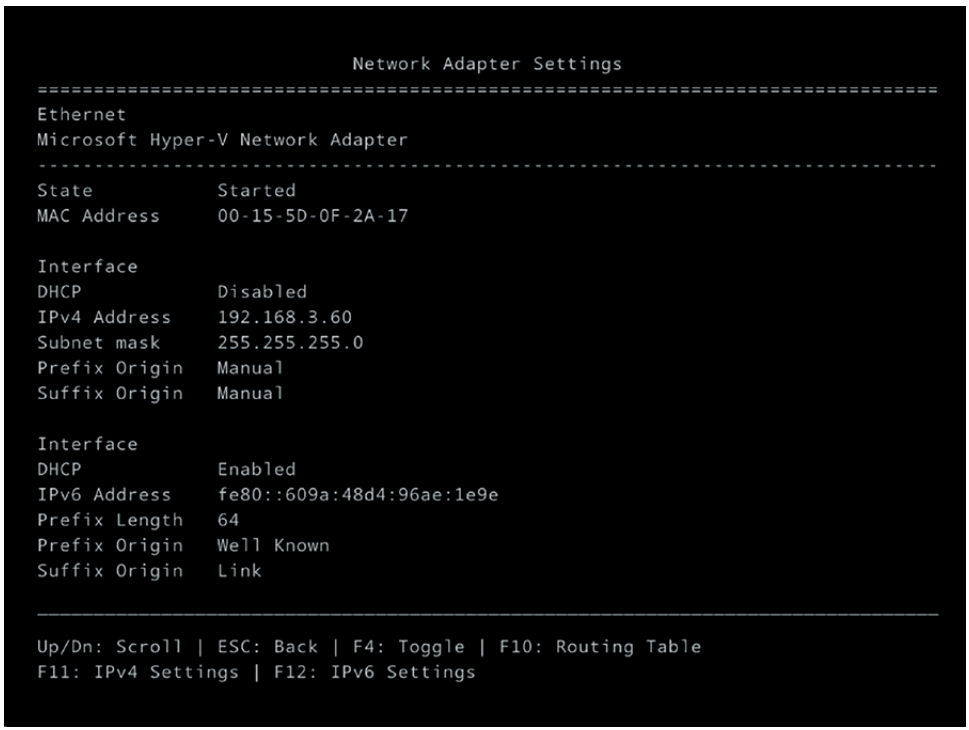
Konsola Nano Server

Jak pokazuje rysunek 2-7, konsola Nano Server daje nam dostęp jedynie do kilku prostych narzędzi, za pomocą których możemy skonfigurować podstawowe ustawienia sieciowe, określić aktywne reguły zapory sieciowej i ustawienia WinRM. Zadaniem tego interfejsu jest więc umożliwić nam skonfigurowanie naszego serwera w takim stopniu, aby możliwe było połączenie się z nim w ramach zdalnej sesji PowerShell, w celu zdalnego wykonywania na nim wszystkich pozostałych zadań administracyjnych.



Rysunek 2-7 Interfejs konsoli odzyskiwania systemu Nano Server

Za pomocą konsoli Nano Server Recovery Console możemy odpowiednio skonfigurować opcje sieciowe, jak to pokazano na rysunku 2-8. Nano Server obsługuje zarówno statyczną konfigurację IP, jak i dynamiczną konfigurację adresów z użyciem serwera DHCP. Konsola odzyskiwania umożliwia nam także włączenie lub wyłączenie usługi zdalnego zarządzania systemem WinRM oraz skonfigurowanie przychodzących i wychodzących reguł zapory sieciowej.



Rysunek 2-8 Ustawienia karty sieciowej w systemie Nano Server

Obsługiwane role i funkcje

Jednym z powodów, dla których Nano Server wykorzystuje wsparcie CBB zamiast wsparcia LTSB jest to, że Microsoft zamierza regularnie rozszerzać funkcjonalność tego systemu. Poprzez ograniczenie wsparcia oferowanego dla gałęzi bieżącej do przedziału od 18 do 24 miesięcy, będziemy zmuszeni regularnie aktualizować ten system do jego nowszej wersji.

Nano Server obsługuje obecnie następujące role i funkcje:

- Containers (Kontenery)
- Data Center Bridging (Mostkowanie centrum danych)
- DNS Server (Serwer DNS)
- Failover Clustering (Klaster pracy w trybie failover)
- File Server (Serwer plików)
- Hyper-V
- Web Server (Serwer sieci Web, IIS)

Od podszewki

Przyszłość systemu Windows Server

Jeffrey Snover, architekt systemu Nano Server i pomysłodawca programu PowerShell, niejednokrotnie podkreślał, że Nano Server stanowi przyszłość systemu Windows Server. Snover spodziewa się, że w miarę jak Nano Server będzie stawał się coraz bardziej funkcjonalny, system w opcji Server with GUI będzie wdrażany coraz rzadziej. Wierzy on, że administratorzy będą decydować się na budowanie szczuplejszych serwerów hostujących konkretne obciążenia robocze, zamiast wdrażać masywne serwery o ogólnym przeznaczeniu, dla których konfiguracja może zostać zmieniona w dowolnym czasie już po ich wdrożeniu. Choć w 2017 roku znaczenie systemu Nano Server nie jest zbyt duże, firma Microsoft głęboko wierzy, że w ciągu kilku kolejnych lat będzie on stanowił większość wdrożeń systemu Windows Server.

Bieżące ograniczenia systemu Nano Server są następujące:

- Obsługuje wyłącznie 64-bitowe aplikacje, narzędzia oraz agentów.
- Nie ma wsparcia dla zasad grupy (choć obsługuje funkcję Desired State Configuration).
- Nie może zostać skonfigurowany pod dostęp do Internetu za pośrednictwem serwera proxy.
- PowerShell w systemie Nano Server oferowany jest w wersji Core, zamiast w pełnej wersji, jaka dostępna jest w systemach Server Core, Server with GUI i Windows 10.

Przyłączanie do domeny

Proces przyłączania serwera Nano do domeny Active Directory nie należy do najprostszych. Nie możemy posłużyć się poleceniem `Add-Computer`, za pomocą którego możliwe jest przyłączenie do domeny komputera z systemem Server Core, Server with GUI i Windows 10.

Aby przyłączyć system Nano Server do domeny Active Directory, w ramach przyłączania do domeny w trybie offline musimy najpierw utworzyć nowy blob. Procesu tego dokonujemy na komputerze, który jest już przyłączony do domeny, wykorzystując konto użytkownika posiadające uprawnienie przyłączania komputerów do domeny.

Na przykład w celu przygotowania blobu dla komputera z systemem Nano Server o nazwie NS1, który ma być przyłączony do domeny contoso.interlan, na już przyłączonym do domeny komputerze możemy wykonać poniższe polecenie:

```
Djoin.exe /provision /domain contoso.internal /machine NS1
  /savefile .\odjblob
```

Następnie musimy przenieść wygenerowany plik odjblob na docelowy serwer NS1. Możemy to zrobić za pomocą poniższych poleceń, które umieszczą plik odjblob w katalogu głównym serwera NS1. Po wykonaniu pierwszego wiersza zostaniemy poproszeni o podanie poświadczeń administracyjnych dla serwera NS1.

```
$cred = Get-Credential
$session = New-PSSession -Computername NS1 -Credential $cred
Copy-Item c:odjblob -Destination 'C:' -ToSession $Session
```

Teraz za pomocą polecenia `Enter-PSSession` możemy nawiązać sesję zdalną PowerShell z serwerem Nano NS1.

Wcześniej jednak adres serwera NS1 będziemy musieli dodać do listy zaufanych hostów TrustedHosts, co możemy zrealizować poniższym poleceniem:

```
Set-Item wsman:\localhost\Client\TrustedHosts -Value NS1 -Concatenate
```

Teraz możemy już połączyć się z tym serwerem, wykorzystując do tego wspomniane polecenie `Enter-PSSession` oraz zmienną `$cred`:

```
Enter-PSSession -ComputerName NS1 -Credential $cred
```

Po nawiązaniu sesji zdalnej do serwera NS1 możemy skorzystać z poniższego polecenia, które dokona przyłączenia tego serwera do domeny:

```
Djoin /requestodj /loadfile c:\odjblob /windowspath c:\windows /localos
```

Na koniec uruchamiamy ponownie serwer Nano w celu zakończeniu operacji przyłączania do domeny. Możemy to przykładowo zrobić poleceniem `Restart-Computer`.

Tworzenie obrazów systemu Nano Server

Systemu Nano Server nie możemy po prostu zainstalować poprzez dokonanie rozruchu komputera z poziomu nośnika instalacyjnego Windows Server 2016. Zamiast tego musimy odpowiednio zaprojektować obraz instalacyjny, tak aby zawierał on wyłącznie te role, funkcje i sterowniki, które są właściwe dla dokonywanego przez nas wdrożenia. Na przykład, jeśli chcielibyśmy wdrożyć instancję systemu Nano Server w postaci maszyny wirtualnej hostującej kontenery Windows, dodalibyśmy do obrazu systemu Nano Server odpowiedni pakiet sterowników pozwalający systemowi Nano na pracę w postaci maszyny wirtualnej, a także sterownik umożliwiający hostowanie na tym systemie kontenerów. Zgodnie z filozofią wdrożenia systemu Nano Server, do obrazu tego systemu dodawać będziemy tylko te komponenty, z których faktycznie będziemy korzystać. Jeśli będziemy potrzebowali czegoś więcej, wtedy zamiast rozszerzać o ten nowy element obraz już wdrożonego systemu, będziemy tworzyć nowy obraz systemu Nano, w którym ten komponent zostanie zawarty.

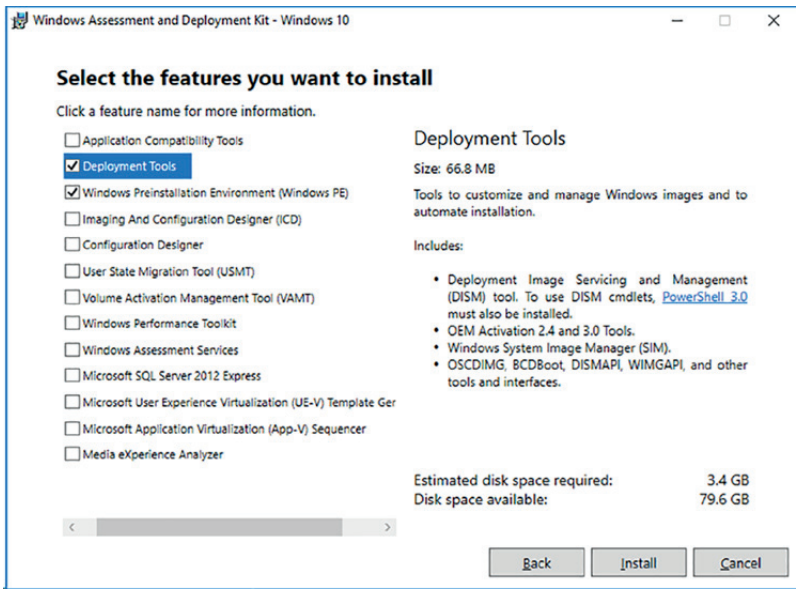
Nano Server Image Builder

Nano Server Image Builder jest graficznym narzędziem umożliwiającym budowanie nowych obrazów systemu Nano Server dla wdrożeń fizycznych i wirtualnych. W przypadku budowania obrazu dla wdrożenia fizycznego, Nano Server Image Builder utworzy rozruchowy nośnik USB, za pomocą którego będziemy mogli dokonać instalacji serwera Nano na fizycznym sprzęcie. Narzędzie Nano Server Image Builder możemy również wykorzystać do utworzenia wirtualnego dysku twardego Nano Server, którego będziemy mogli użyć w roli dysku systemu operacyjnego dla maszyny wirtualnej.

Aby móc utworzyć nowy obraz serwera Nano za pomocą programu Nano Server Image Builder, musimy mieć:

- Dostęp do foldera NanoServer na nośniku instalacyjnym Windows Server 2016. Folder ten może być przechowywany lokalnie lub w udziale sieciowym dostępnym dla komputera, na którym uruchamiamy narzędzie Nano Server Image Builder.
- Listę nazw, które zamierzamy wykorzystać dla poszczególnych komputerów z systemem Nano Server.
- Dostęp do niezbędnych sterowników, jeśli zamierzamy utworzyć obraz, który będzie wdrażany bezpośrednio na fizycznym sprzęcie.

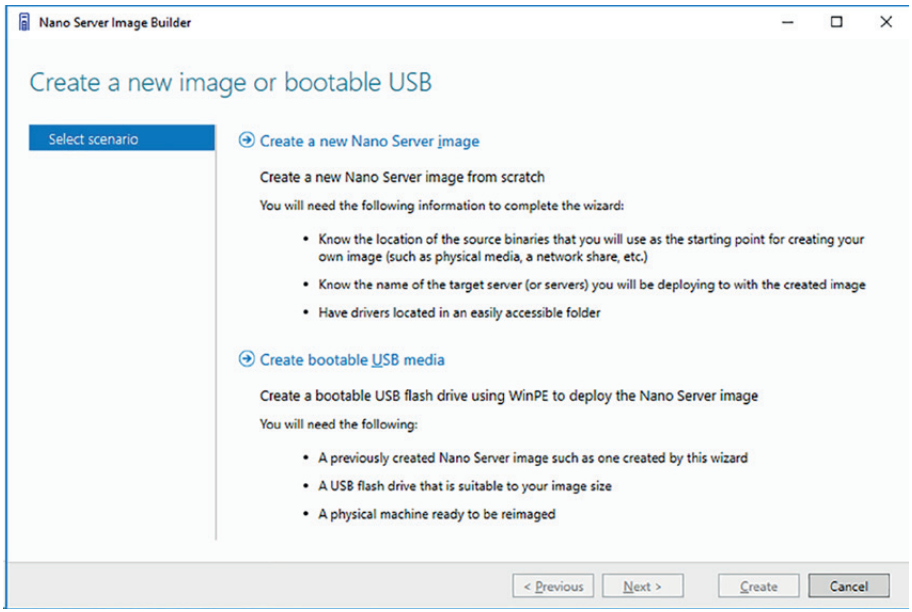
Program Nano Server Image Builder dostępny jest do pobrania ze stron Microsoft. Do poprawnej pracy narzędzie to wymaga komponentów Deployment Tools oraz Windows Preinstallation Environment (Windows PE), będących częścią pakietu Windows Assessment and Deployment Kit (Windows ADK), widocznego na rysunku 2-9.



Rysunek 2-9 Wymagania wstępne narzędzia Nano Server Image Builder

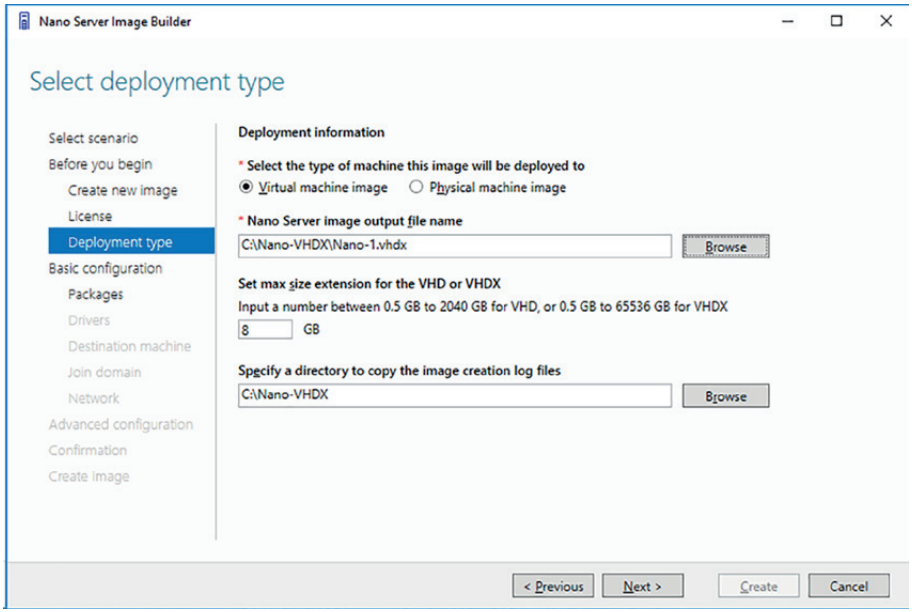
W celu utworzenia nowego obrazu systemu Nano Server za pomocą narzędzia Nano Server Image Builder, wykonaj poniższe czynności:

1. Zainstaluj i uruchom narzędzie Nano Server Image Builder.
2. Na stronie Select Scenario (Wybierz scenariusz), widocznej na rysunku 2-10, wybierz opcję Create a new Nano Server image (Utwórz nowy obraz Nano Server).

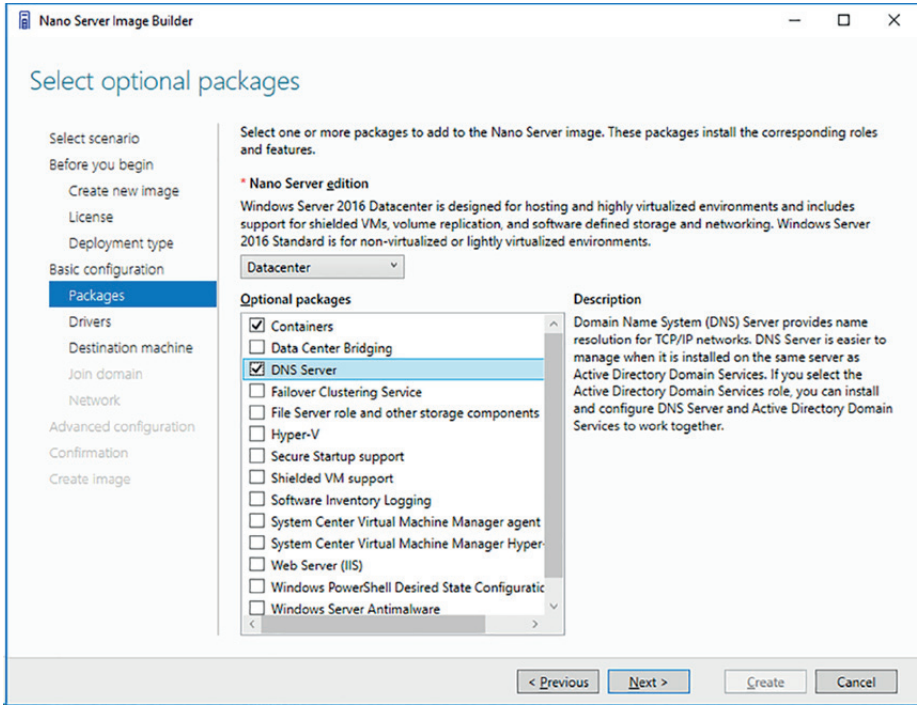


Rysunek 2-10 Wybieranie scenariusza w programie Nano Server Image Builder

3. Na stronie Select Installation Media (Wybierz nośnik instalacyjny) podaj lokalizację do folderu NanoServer, który przekopiowałeś z nośnika instalacyjnego Windows Server 2016.
4. Na stronie License (Licencja) przejrzyj i zaakceptuj warunki umowy.
5. Na stronie Deployment Information (Informacje dotyczące wdrożenia), widocznej na rysunku 2-11, określ, czy chcesz utworzyć obraz maszyny wirtualnej, czy obraz maszyny fizycznej. Jeśli tworzysz obraz maszyny wirtualnej, to poprzez zastosowanie rozszerzenia .vhd lub .vhdx możesz w tym miejscu określić rodzaj wykorzystywanego wirtualnego dysku twardego. Na stronie tej możesz również skonfigurować maksymalny rozmiar wirtualnego dysku twardego, a także określić lokalizację, do której przekopiowane zostaną pliki dziennika tworzenia obrazu.
6. Na stronie Packages (Pakiety) określ edycję systemu Windows Server 2016, dla której tworzony jest nowy obraz Nano Server. Możesz również zaznaczyć role serwera, które chcesz zainstalować. W przykładzie na rysunku 2-12 do obrazu Nano Server dodawane są role Containers i DNS Server.

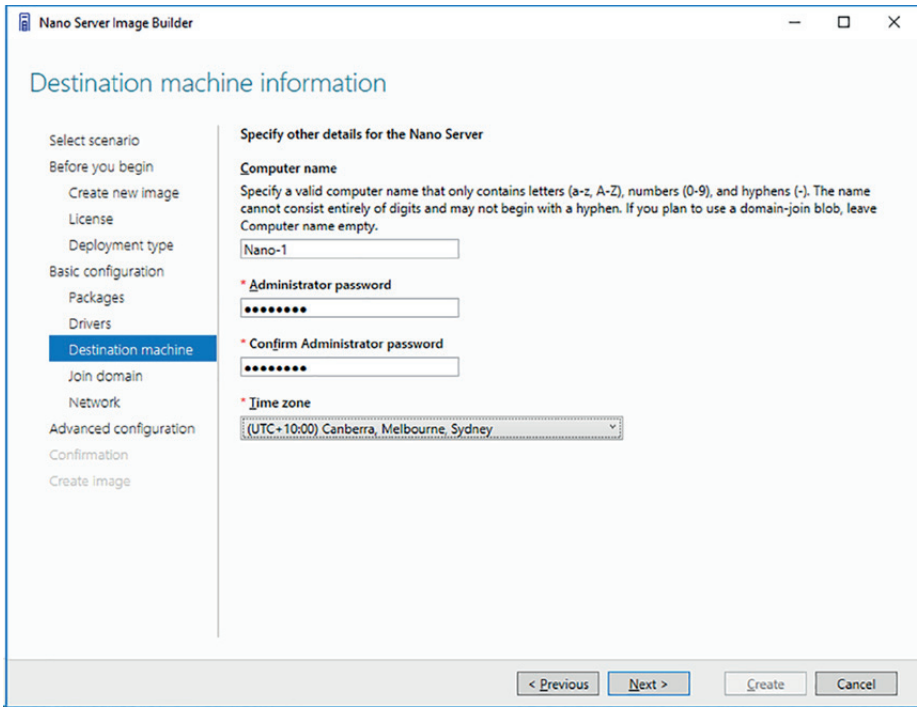


Rysunek 2-11 Konfigurowanie wdrożenia



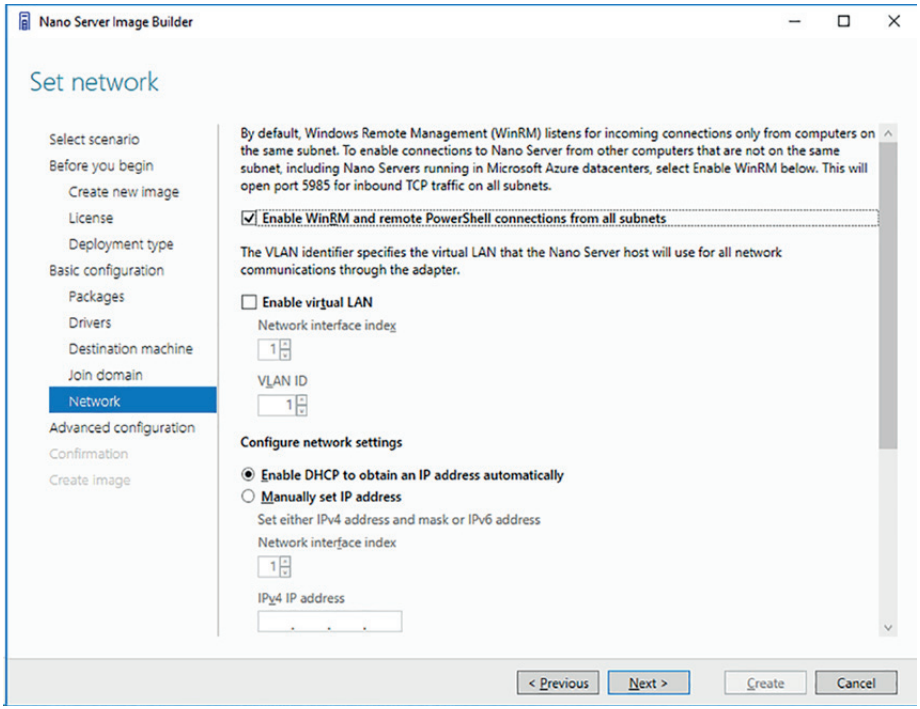
Rysunek 2-12 Wybieranie pakietów opcjonalnych

7. Na stronie Drivers (Sterowniki) określ jakiekolwiek dodatkowe sterowniki, które będą wymagane dla tego obrazu Nano Server. Jeśli wdrażasz serwer Nano w postaci maszyny wirtualnej, niezbędne sterowniki Hyper-V są już uwzględnione.



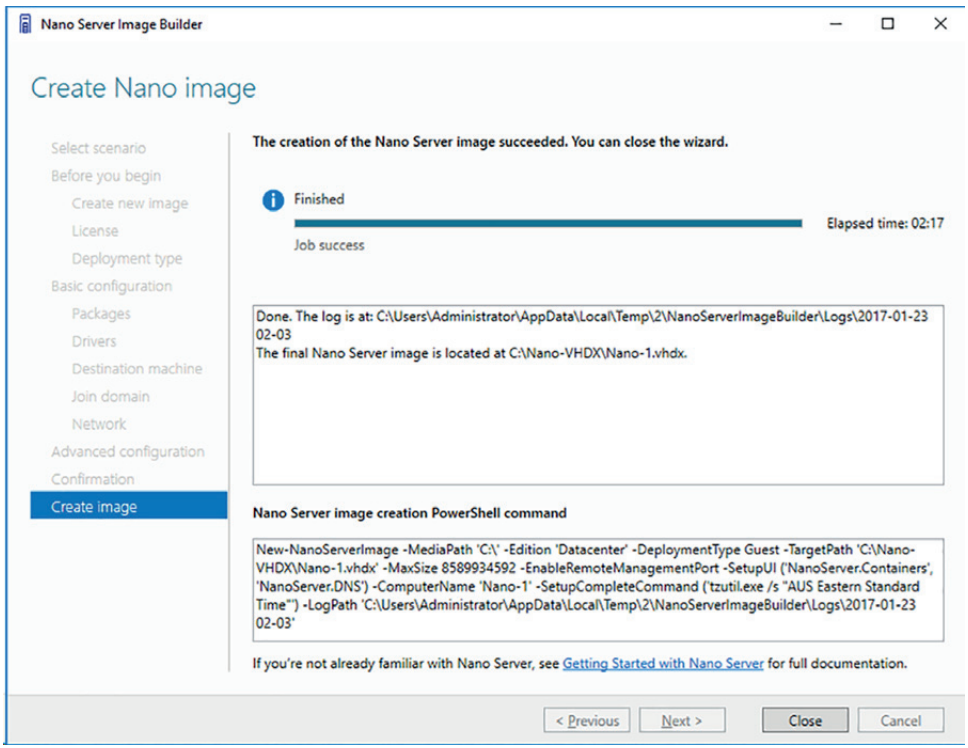
Rysunek 2-13 Właściwości komputera docelowego

8. Na stronie Destination machine (Maszyna docelowa), widocznej na rysunku 2-13, podaj nazwę docelowego komputera, hasło administratora oraz strefę czasową.
9. Jeśli skonfigurowałeś już blob przyłączenia do domeny, możesz wskazać go na stronie Join domain (Przyłącz do domeny).
10. Na widocznej na rysunku 2-14 stronie Network (Sieć) skonfiguruj następujące ustawienia:
    - ❏ Zaznacz lub odznacz pole wyboru Enable WinRM and remote PowerShell connections from all subnets (Zezwól na połączenia usługi WinRM i zdalne połączenia programu PowerShell ze wszystkich podsieci)
    - ❏ Skonfiguruj ustawienia sieci VLAN
    - ❏ Określ, czy adres IP serwera Nano będzie pozyskiwany z serwera DHCP, czy też podany zostanie ręcznie



Rysunek 2-14 Ustawienia sieciowe

11. Na stronie Advanced configuration (Zaawansowana konfiguracja) możesz utworzyć podstawowy obraz systemu Nano lub też skonfigurować dla niego dodatkowe opcje, wliczając w to aktualizacje oprogramowania, skrypty, pliki i binaria, a także metody debugowania.
12. Na stronie Confirmation (Potwierdzenie) kliknij Create (Utwórz). Jak pokazano na rysunku 2-15, narzędzie Nano Server Image Builder dostarcza także odpowiednie polecenie PowerShell, za pomocą którego został wygenerowany obraz systemu Nano Server.



Rysunek 2-15 Tworzenie obrazu

Polecenia PowerShell dla obrazu systemu Nano Server

Folder NanoServer na nośniku instalacyjnym Windows Server 2016 zawiera moduł PowerShell o nazwie `NanoServerImageGenerator`. Moduł ten oferuje następujące polecenia umożliwiające zarządzanie obrazem systemu Nano Server:

- **New-NanoServerImage** Polecenie do tworzenia nowego obrazu systemu Nano Server.
- **Edit-NanoServerImage** Polecenie do modyfikowania istniejącego obrazu systemu Nano Server.
- **Get-NanoServerPackage** Polecenie do przeglądania dostępnych pakietów systemu Nano Server.



Rozdział 3

Wdrożenie i konfiguracja

Wdrożenie fizyczne a wirtualne 45
Obrazy systemu Windows 46
Pliki odpowiedzi. 57
Windows Deployment Services. 59
Virtual Machine Manager 69
Konfiguracja infrastruktury w postaci kodu. 80
Desired State Configuration 82
Chef 87
Puppet. 100
Narzędzia zarządzania pakietami 109

W zależności od rozmiaru naszej organizacji, wdrożone przez nas serwery pozostawiać będziemy w środowisku produkcyjnym na całe lata, a niekiedy nawet na dłużej niż dekadę, jak choćby w przypadku (trwającego nadal) okresu wycofywania serwerów Windows Server 2003. Inne organizacje mogą wdrażać serwery z większą lub mniejszą częstotliwością. Niektóre z nich wykorzystują w tym celu proces, w ramach którego zamiast stosować aktualizacje oprogramowania bezpośrednio do serwera produkcyjnego, wymuszając w ten sposób przestój takiego serwera do momentu zainstalowania na nim aktualizacji i jego ponownego uruchomienia, wdrażają zupełnie nowy, już odpowiednio zaktualizowany komputer. Następnie na tak przygotowany serwer migrują istniejące obciążenia robocze, a na koniec likwidują serwer oryginalny.

Taki rodzaj przyrostowego wdrażania możliwy jest dzięki temu, że narzędzia zarządzania konfiguracją serwerów przeszły pewną ewolucję. Dzisiaj proces wdrażania i konfigurowania nowego serwera nie jest wcale trudniejszy od typowego procesu wdrażania aplikacji, jakiego dokonalibyśmy dziesięć lat temu. W tym rozdziale nauczymy się korzystać z obrazów systemu Windows Server, usługi Windows Deployment Services, konsoli Virtual Machine Manager, funkcji Desired State Configuration oraz narzędzi Puppet i Chef, za pomocą których będziemy wdrażać i zarządzać konfiguracją naszych komputerów oraz maszyn wirtualnych, działających pod kontrolą systemu operacyjnego Windows Server 2016.

Wdrożenie fizyczne a wirtualne

Dzisiaj prawie wszystkie nowe obciążenia robocze są zwirtualizowane. Dla większości organizacji hosty wirtualizacji pozostają praktycznie jedynymi fizycznie wdrażanymi serwerami, zaś wszystkie pozostałe obciążenia robocze uruchamiane są na tych hostach w postaci maszyn wirtualnych. O ile nie mamy żadnych konkretnych powodów, dla których nie powinniśmy wirtualizować danego obciążenia roboczego, zamiast wdrażać

system Windows Server 2016 w formie serwera fizycznego, powinniśmy uruchamiać go w postaci maszyny wirtualnej.

Zabezpieczenia dostępne w chronionych maszynach wirtualnych usuwają jedną z ostatnich przeszkód, jakie stały organizacjom na drodze do wdrażania serwerów w postaci wirtualnej zamiast fizycznej. Dzięki chronionym maszynom wirtualnym możemy zapewnić naszym obciążeniom roboczym taki sam poziom zabezpieczeń, z jakim mieliśmy do czynienia w przypadku serwerów fizycznych, wdrażanych w zamkniętych centrach danych.

Najlepszym sposobem wdrażania hostów wirtualizacji jest skorzystanie z opcji instalacji Server Core, jako że system w tej wersji, w porównaniu do opcji Server with Desktop Experience, cechuje się dużo mniejszym zapotrzebowaniem na zasoby oraz zmniejszoną powierzchnią ataku. Po wdrożeniu hosta wirtualizacji Server Core, dostępną na nim funkcją Hyper-V będziemy mogli zarządzać zdalnie z poziomu stacji roboczej z dostępem uprzywilejowanym lub za pomocą odpowiednich narzędzi, takich jak konsola Virtual Machine Manager.

Od podszewki

Host wirtualizacji Nano

Nadejdzie taki czas, że większość organizacji za najbardziej odpowiednią wersję hosta wirtualnych obciążeń roboczych uzna opcję instalacji Nano Server. Obecnie wiele organizacji wzbrania się przed wdrażaniem serwera Nano jako hosta dla ról infrastruktury, ponieważ system ten dostępny jest jedynie w gałęzi obsługi Current Branch, a nie w długoterminowej gałęzi Long Term Servicing Branch.

Obrazy systemu Windows

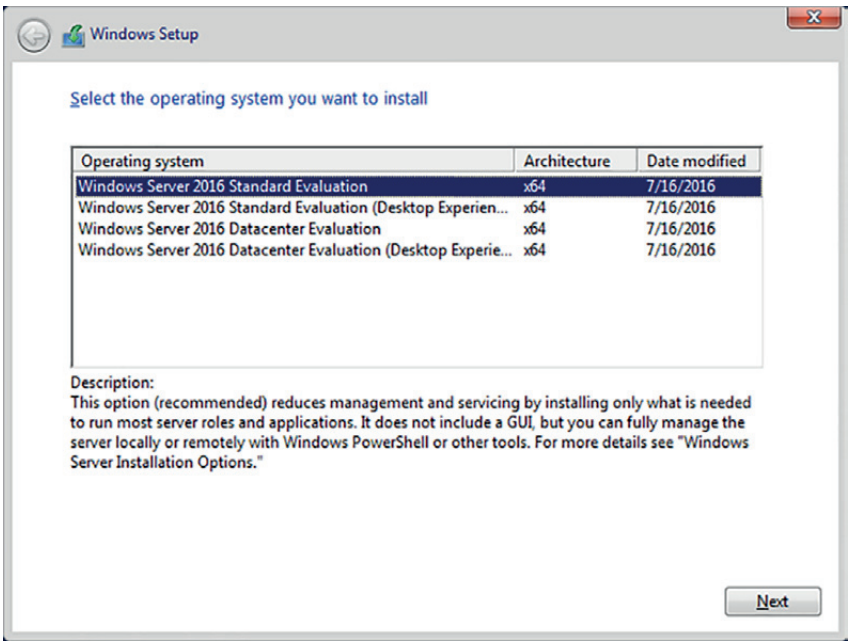
Cały system operacyjny Windows, wraz z powiązanymi sterownikami, aktualizacjami i aplikacjami, przechowywany jest w pojedynczym pliku, który podczas instalacji zostaje zastosowany na docelowym woluminie. Plik ten znany jest jako plik obrazu. Windows wykorzystuje pliki obrazu w formacie Windows Imaging (WIM), który przynosi następujące korzyści:

- **Kilka metod wdrażania** Obrazy systemu Windows możemy wdrażać na kilka sposobów. Pliki .wim możemy wdrożyć za pomocą tradycyjnego nośnika DVD, z poziomu pamięci masowej USB, z poziomu udziału sieciowego, a także przy wykorzystaniu specjalnych technologii wdrożeniowych, takich jak usługi Windows Deployment Services (WDS) czy program System Center Virtual Machine Manager. Choć możliwe jest wdrożenie systemu Windows Server z poziomu programu

System Center Configuration Manager, to jednak program ten wykorzystywany jest głównie w celu konfiguracji systemów klienckich, a nie serwerowych systemów operacyjnych.

- **Możliwość edycji** Obraz systemu możemy zamontować w celu jego edycji, co pozwala nam wyłączać, włączać lub usuwać z niego wybrane role i funkcje.
- **Możliwość aktualizacji** Obraz systemu możemy zaktualizować bez konieczności przechwytywania obrazu istniejącego systemu operacyjnego.

Nośnik instalacyjny Windows Server 2016 zawiera dwa pliki .wim zlokalizowane w folderze Sources. Są to pliki Boot.wim oraz Install.wim. Plik Boot.wim wykorzystywany jest do załadowania środowiska preinstalacyjnego, którego używamy do wdrażania systemu Windows Server 2016. Z kolei plik Install.wim przechowuje jeden lub więcej obrazów systemu operacyjnego. Jak możemy przykładowo zobaczyć na rysunku 3-1, plik Install.wim dostępny w ramach wersji ewaluacyjnej systemu Windows Server 2016 zawiera cztery różne edycje tego systemu.



Rysunek 3-1 Edycje Windows Server 2016

Modyfikowanie obrazów Windows

Narzędzie Deployment Image Servicing and Management (DISM) jest narzędziem wiersza poleceń, za pomocą którego możemy zarządzać obrazami systemu w trybie offline. Narzędzie Dism.exe umożliwia nam wykonywanie następujących zadań na obrazie Windows:

- Włączanie lub wyłączanie ról i funkcji
- Listowanie ról i funkcji
- Dodawanie, usuwanie lub listowanie aktualizacji oprogramowania
- Dodawanie, usuwanie lub listowanie sterowników
- Dodawanie, usuwanie lub listowanie pakietów oprogramowania w formacie .appx

Na przykład, po pozyskaniu pliku Install.wim z nośnika instalacyjnego Windows Server możemy zamontować go za pomocą programu Dism.exe. Do tak zamontowanego obrazu możemy dodać nowe sterowniki i najnowsze aktualizacje oprogramowania. Po zakończeniu będziemy mogli zapisać w tym obrazie wszystkie wprowadzone zmiany, bez konieczności wykonywania samego wdrożenia. Korzyści z tego są takie, że gdy przyjdzie nam wykorzystać ten obraz podczas faktycznego wdrożenia, wszystkie sterowniki i aktualizacje, które dodaliśmy do tego obrazu narzędziem Dism.exe, będą już w nim obecne, tak więc nie będziemy musieli instalować ich w ramach standardowego procesu konfiguracji.

W celu wyszukania sterowników dla obrazów wykorzystywanych do wdrażania serwerów fizycznych możemy posłużyć się katalogiem Microsoft Update Catalog (*https://catalog.update.microsoft.com*). Witryna ta przechowuje wszystkie certyfikowane sterowniki sprzętu, aktualizacje oprogramowania oraz poprawki opublikowane przez Microsoft. Gdy już pobierzemy odpowiednie sterowniki i aktualizacje oprogramowania, będziemy mogli je dodać do istniejących obrazów instalacyjnych za pomocą narzędzia Dism.exe lub odpowiednich poleceń programu PowerShell zebranych w module DISM.

Obsługiwanie obrazów Windows

Jako profesjonaliści IT odpowiedzialni za wdrażanie systemu Windows Server musimy się upewnić, że wdrażane przez nas obrazy będą zawsze aktualne. Obraz systemu Windows Server powinien uwzględniać zarówno najnowsze aktualizacje oprogramowania, jak i wszelkie nowe sterowniki dla najczęściej wykorzystywanego sprzętu serwerowego.

W naszej strategii obsługiwania obrazów możemy wyróżnić dwa podstawowe cele:

- Upewnić się, że wszystkie najnowsze aktualizacje oprogramowania i poprawki zostaną uwzględnione w obrazie, zanim zostanie on wykorzystany do wdrożenia nowych serwerów.

- Upewnić się, że w obrazie uwzględnione zostaną najnowsze sterowniki, zanim obraz ten zostanie wykorzystany do wdrożenia nowych serwerów.

Jeśli nie wykonamy powyższych kroków, wówczas sterowniki i aktualizacje oprogramowania będziemy mogli zainstalować w systemie dopiero po zakończeniu jego wdrażania. Choć obecnie aktualizacje są kumulowane, przez co nie musimy już spędzać wielu godzin na aktualizowaniu obrazu z wersji RTM, to jednak znacznie szybciej będzie zastosować najnowsze aktualizacje bezpośrednio na obrazie systemu, zamiast czekać na zakończenie wdrożenia, pozyskanie najnowszych aktualizacji i ich późniejsze zainstalowanie. Zastosowywanie aktualizacji już po wdrożeniu systemu nie tylko konsumuje znaczną ilość czasu, ale też znacząco zwiększa ruch sieciowy. Pamiętajmy, że jednym z naszych celów podczas wykonywania wdrożenia powinno być jak najszybsze skonfigurowanie i przygotowanie serwera do obsługi docelowych obciążeń roboczych.

Narzędzia DISM lub odpowiadających mu poleceń PowerShell wchodzących w skład modułu DISM możemy użyć nie tylko do serwisowania offline konkretnego obrazu Windows, ale również do serwisowania bieżącego systemu operacyjnego w stanie online.

Proces obsługi obrazu sprowadza się do wykonania następujących kroków:

1. Zamontowanie obrazu w celu jego modyfikacji.
2. Obsługiwanie obrazu.
3. Zatwierdzenie lub odrzucenie zmian wprowadzonych do obrazu.

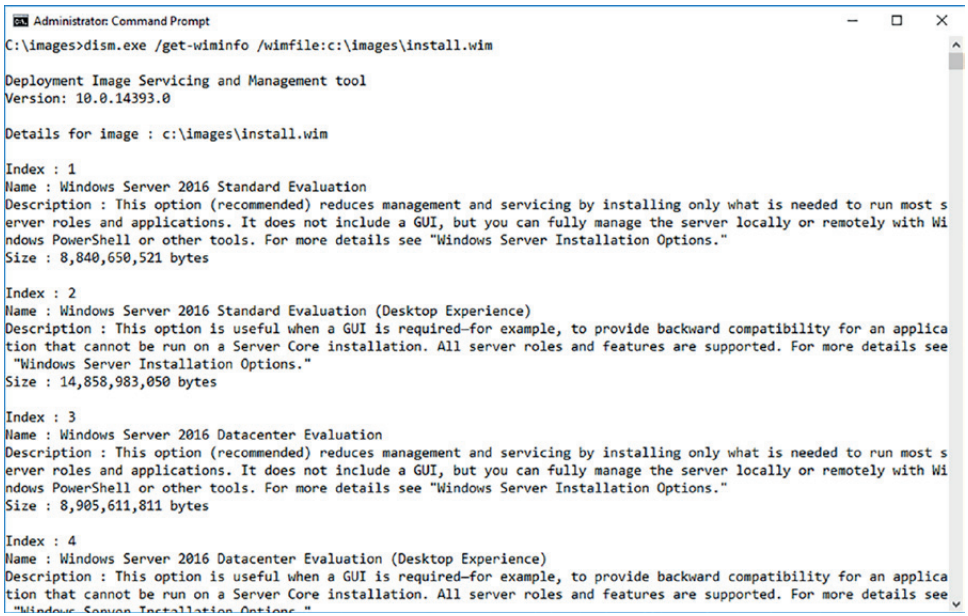
Montowanie obrazów

Po zamontowaniu obrazu możemy zacząć wprowadzać do niego zmiany. Operacja montowania obrazu polega na jego podlinkowaniu do wskazanego folderu. Za pomocą Eksploratora plików, programu Windows PowerShell lub konsoli wiersza polecenia możemy nawigować po strukturze tego folderu i pracować z nim dokładne tak samo, jak pracujemy z każdym innym folderem zlokalizowanym w systemach plików Windows. Gdy obraz jest już zamontowany, możemy posłużyć się narzędziem `Dism.exe` lub programem PowerShell w celu wykonania zadań serwisowania, takich jak dodanie lub usunięcie sterowników i aktualizacji.

Pojedynczy plik WIM może zawierać kilka obrazów systemu operacyjnego, z których każdy ma przypisany odpowiedni numer indeksu. Zanim będziemy mogli taki obraz zamontować, musimy poznać numer jego indeksu. Numer indeksu możemy ustalić za pomocą narzędzia `Dism.exe` uruchomionego z przełącznikiem `/Get-WIMInfo`. Na przykład, jeśli dysponujemy obrazem Install.wim zlokalizowanym w folderze C:\Images, za pomocą poniższego polecenia będziemy mogli pozyskać listę zawartych w nim systemów operacyjnych.

```
Dism.exe /get-wiminfo /wimfile:c:\images\install.wim
```

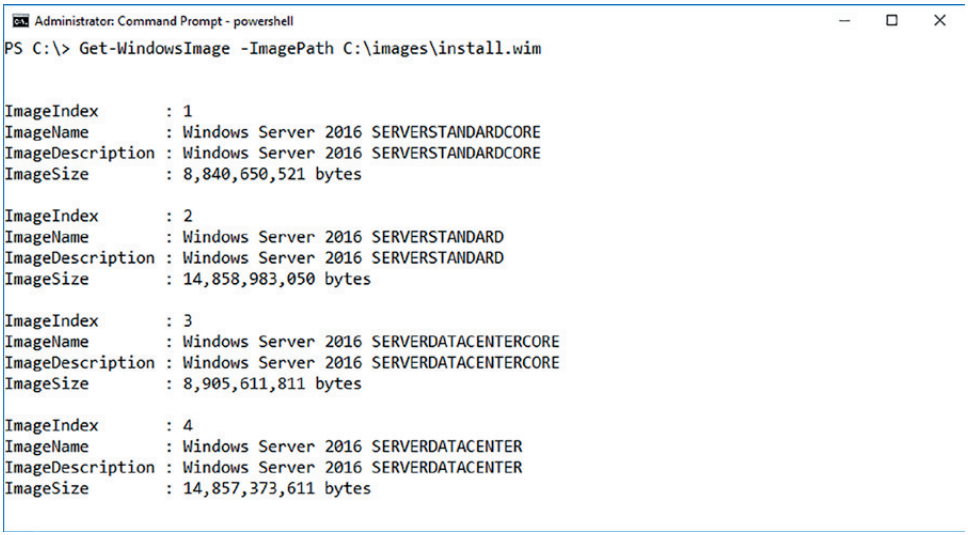
Rysunek 3-2 pokazuje wynik działania tego polecenia na przykładzie obrazu systemu Windows Server 2016. Edycja ewaluacyjna Standard systemu Windows Server 2016 z opcją instalacji Server Core ma nadany numer indeksu 1, edycja ewaluacyjna Standard z pulpitem graficznym ma nadany numer indeksu 2, edycja ewaluacyjna Datacenter z opcją instalacji Server Core ma przypisany numer indeksu 3, zaś edycja ewaluacyjna Datacenter z pulpitem graficznym na nadany numer indeksu 4.



Rysunek 3-2 Szczegóły obrazu systemu operacyjnego

To samo zadanie możemy również zrealizować za pomocą polecenia PowerShell o nazwie `Get-WindowsImage`. Na przykład, w celu przejrzenia zawartości obrazu Install.wim w folderze C:\Images należy wykonać poniższe polecenie, którego wynik przedstawiony został na rysunku 3-3:

```
Get-WindowsImage -ImagePath c:\images\install.wim
```



Rysunek 3-3 Szczegóły obrazu systemu Windows

Od podszewki

DISM i PowerShell

Zarządzanie obrazami możliwe jest zarówno za pośrednictwem narzędzia DISM, jak i poleceń programu PowerShell, ponieważ wielu profesjonalistów IT przyzwyczajonych jest do narzędzia DISM i nadal wykorzystuje go w swoich skryptach. Warto jednak skupić się na korzystaniu z poleceń PowerShell, ponieważ narzędzie DISM może kiedyś przestać być obsługiwane.

Gdy już ustaliliśmy, który obraz systemu operacyjnego chcemy obsłużyć, możemy zamontować go za pomocą polecenia `Dism.exe` z przełącznikiem `/Mount-Image`. Przykładowo, w celu zamontowania edycji Standard systemu Windows Server 2016 z pliku Install.wim dostępnego w folderze C:\Mount możemy wydać poniższe polecenie:

```
Dism.exe /mount-image /imagefile:c:\images\install.wim /index:2
  /mountdir:c:\mount
```

Alternatywnie ten sam cel możemy osiągnąć za pomocą polecenia `Mount-WindowsImage`:

```
Mount-WindowsImage -ImagePath c:\images\install.wim -index 2 -path c:\mount
```

Dodawanie do obrazów sterowników i aktualizacji

Po zamontowaniu obrazu możemy rozpocząć proces jego obsługi. W ramach obsługiwania obrazów służących do wdrażania systemu Windows Server będziemy najczęściej dodawać do nich sterowniki urządzeń oraz aktualizacje oprogramowania. W celu dodania do obrazu wybranego sterownika możemy posłużyć się poleceniem `Dism.exe` z przełącznikiem `/Add-Driver`. W przypadku użycia tego przełącznika musimy podać również ścieżkę do lokalizacji pliku .inf danego sterownika. Zamiast jednak dodawać do obrazu po jednym sterowniku na raz, możemy skorzystać z opcji `/Recurse`, która umożliwi nam dodanie do obrazu wszystkich sterowników zlokalizowanych we wskazanym folderze oraz jego podfolderach. Na przykład, aby do obrazu zamontowanego w folderze C:\Mount dodać wszystkie sterowniki zlokalizowane wewnątrz folderu C:\Drivers, możemy wykonać poniższe polecenie.

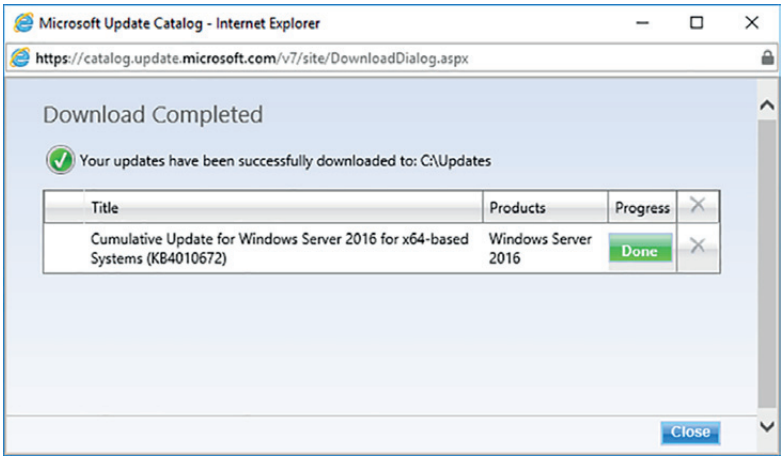
```
Dism.exe /image:c:\mount /Add-Driver /driver:c:\drivers\ /recurse
```

Podobny rezultat moglibyśmy otrzymać za pomocą cmdlet PowerShell o nazwie `Add-WindowsDriver`:

```
Add-WindowsDriver -Path c:\mount -Driver c:\drivers -Recurse
```

Przy użyciu przełącznika `/Get-Driver` możemy podejrzeć listę wszystkich sterowników, jakie zostały dodane do obrazu, zaś poprzez zastosowanie przełącznika `/Remove-Driver` możemy dany sterownik usunąć z obrazu. Odpowiednikami tych przełączników w programie PowerShell są polecenia `Get-WindowsDriver` oraz `Remove-WindowsDriver`. Możemy usuwać tylko te sterowniki, które dodane zostały do obrazu przez kogoś innego lub przez nas samych. Nie ma możliwości usunięcia sterownika, który obecny był w obrazie w momencie jego publikacji przez Microsoft. Potrzeba usunięcia istniejącego sterownika może pojawić się wtedy, gdy dodany przez nas w przeszłości sterownik został już zaktualizowany do nowej wersji.

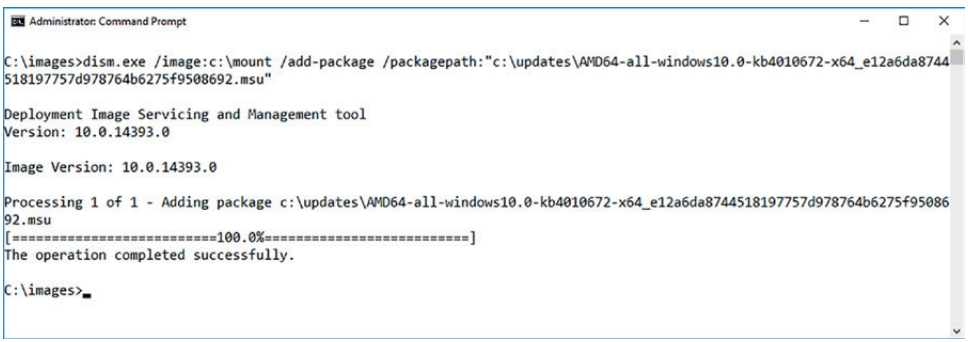
W celu dodania do obrazu pakietów zawierających aktualizacje oprogramowania lub pakietów w formacie .cab i .msu możemy posłużyć się narzędziem `Dism.exe` z przełącznikiem `/Add-Package`. Aktualizacje oprogramowania dostępne są do pobrania z witryny Microsoft Update Catalog w formacie .msu. Rysunek 3-4 pokazuje przykład pobierania z witryny Microsoft Update Catalog do folderu C:\Updates na naszym komputerze aktualizacji zbiorczej Cumulative Update for Windows Server 2016 for x64-based Systems (KB4010672).



Rysunek 3-4 Pobieranie aktualizacji zbiorczej

Jeśli obraz WIM systemu Windows Server 2016 zamontowaliśmy w folderze C:\Mount, moglibyśmy zastosować na nim tę aktualizację za pomocą poniższego polecenia, którego wynik przedstawiony został na rysunku 3-5:

```
Dism.exe /image:c:\mount /Add-Package /PackagePath:"c:\updates\AMD64-all-
windows10.0-kb4010672-x64_e12a6da8744518197757d978764b6275f9508692.msu"
```



Rysunek 3-5 Zastosowywanie aktualizacji na obrazie

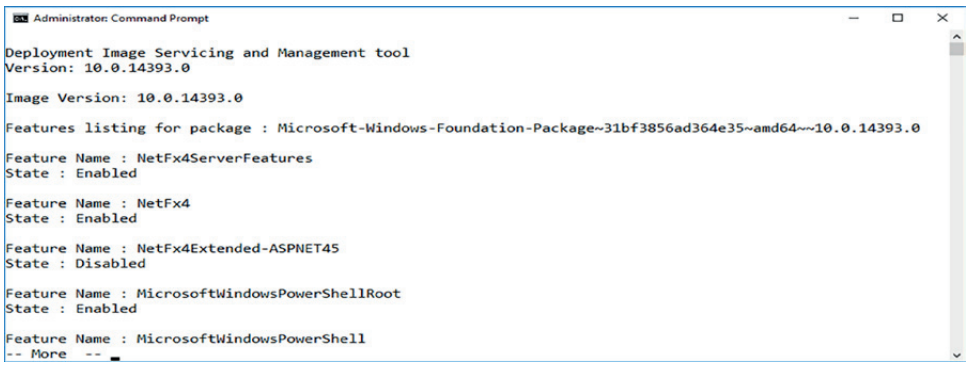
Ten sam rezultat możemy otrzymać za pomocą poniższego polecenia `Add-WindowsPackage`:

```
Add-WindowsPackage -path c:\mount -packagepath "c:\updates\AMD64-all-
windows10.0-kb4010672-x64_e12a6da8744518197757d978764b6275f9508692.msu"
```

Dodawanie ról i funkcji

Poprzez zastosowanie przełącznika `/Get-Features` możemy określić, które z funkcji są dostępne w zamontowanym obrazie systemu operacyjnego. W tym wypadku funkcje odnoszą się nie tylko do funkcji systemu Windows Server 2016, ale także do jego ról serwera. Aby przykładowo dowiedzieć się, które funkcje dostępne są w obrazie zamontowanym w folderze C:\Mount, możemy skorzystać z poniższego polecenia, którego wynik przedstawiony został na rysunku 3-6.

```
Dism.exe /image:c:\mount /Get-Features
```



Rysunek 3-6 Przeglądanie funkcji

Daną funkcję możemy włączyć lub wyłączyć za pomocą przełącznika `/Enable-Feature`. Przykładowo, aby włączyć funkcję NetFx3ServerFeatures, która odpowiada za włączenie w obrazie funkcji serwera .NET Framework 3.5, należy wykonać poniższe polecenie:

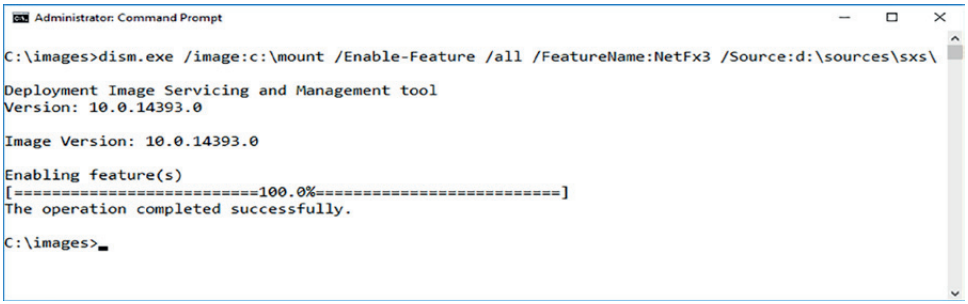
```
Dism.exe /image:c:\mount /Enable-Feature /all
  /FeatureName:NetFx3ServerFeatures
```

Oznaczenie niektórych funkcji wskazuje, że ich ładunki zostały usunięte, co oznacza, że pliki instalacyjne tych funkcji nie zostały uwzględnione w obrazie. Jeśli spróbujemy zainstalować funkcję, której ładunek w momencie wdrożenia systemu operacyjnego był niedostępny, system będzie mógł pobrać te pliki przez Internet bezpośrednio z serwerów aktualizacji Microsoft. Lokalizację tych plików instalacyjnych możemy określić ręcznie. Pliki instalacyjne funkcji, których ładunek został z systemu usunięty, znajdują się w folderze \Sources\sxs na woluminie zawierającym pliki nośnika instalacyjnego.

Te pozbawione ładunku funkcje możemy dodać do obrazu za pomocą polecenia `Dism.exe`, określając przy tym ścieżkę do katalogu źródłowego. Na przykład, w celu zmodyfikowania obrazu zamontowanego w folderze C:\Mount w taki sposób, aby zawierał on gotową do zainstalowania funkcję Microsoft .NET Framework 3.5, należy posłużyć się poniższym poleceniem, którego rezultat przedstawiony został

na rysunku 3-7. Zakładamy tutaj, że zawartość nośnika instalacyjnego Windows Server znajduje się na woluminie oznaczonym literą D.

```
Dism.exe /image:c:\mount /Enable-Feature /all /FeatureName:NetFx3
  /Source:d:\sources\sxs
```



Rysunek 3-7 Włączanie funkcji

Od podszewki

.NET Framework 3.5

Choć niektóre starsze funkcje, takie jak WINS czy SMB w wersji 1, nadal pozostają dostępne w systemie Windows Server 2016, to funkcja .NET Framework 3.5 nie tylko nie jest domyślnie zainstalowana, ale też została wydzielona do osobnego folderu instalacyjnego. Można się jedynie domyślać, że Microsoft starał się nieco utrudnić instalację tego komponentu. Problem polega na tym, że nadal wiele programów (wliczając w to również stosunkowo nowe oprogramowanie) wykorzystuje funkcje komponentu .NET Framework 3.5, przez co takie zachowanie tworzy tylko dodatkowy kłopot.

Zatwierdzanie zmian w obrazie

Po zakończeniu obsługiwania obrazu możemy zachować nasze zmiany poprzez zastosowanie przełącznika `/Unmount-WIM` z opcją `/Commit`. W celu odrzucenia zmian stosujemy opcję `/Discard`. Na przykład, aby dokonać zmian i zatwierdzić je w obrazie zamontowanym w folderze C:\Mount, należy wykonać poniższe polecenie.

```
Dism.exe /Unmount-Wim /MountDir:c:\mount /commit
```

Jeśli chcemy zapisać zmiany w obrazie bez jego odmontowywania, możemy posłużyć się poleceniem PowerShell o nazwie `Save-WindowsImage`. Z kolei w celu zapisania wprowadzonych w obrazie modyfikacji i jego odmontowania należy skorzystać z polecenia

`Dismount-WIMImage` z parametrem `Save`. Na przykład, aby odmontować i zapisać obraz zamontowany w folderze C:\Mount, należy wykonać polecenie:

```
Dismount-WimImage -Path c:\mount -Save
```

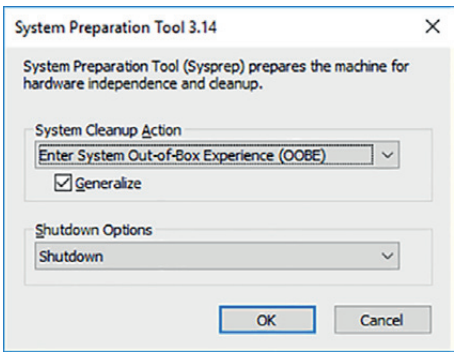
Gdy zmiany zostały już wprowadzone, zamontowany przez nas plik .wim zostanie odpowiednio zaktualizowany. Teraz będziemy mogli zaimportować ten plik .wim do serwera WDS, wykorzystać go do budowy wirtualnego dysku twardego lub też użyć go w nośniku instalacyjnym USB w celu przeprowadzenia fizycznego wdrożenia systemu Windows Server 2016, uwzględniając przy tym wszystkie zastosowane w tym systemie aktualizacje i modyfikacje.

Tworzenie i przechwytywanie

Operacja tworzenia i przechwytywania odnosi się do procesu, w którym najpierw wdrażamy nowy system operacyjny, następnie przygotowujemy ten system pod kątem odpowiednich aktualizacji, aplikacji i sterowników, a na końcu przechwytujemy ten system do postaci obrazu w celu umożliwienia jego wdrożenia. Tworzenie i przechwytywanie na systemach serwerowych nie jest stosowane zbyt często, ponieważ systemy te rzadko kiedy wymagają takich metod wdrażania aplikacji, jakie stosowane są w systemach klienckich. Jeśli istnieje możliwość ściągnięcia na serwer gotowego kontenera ze zaktualizowaną aplikacją, wtedy nie ma większego powodu, aby umieszczać taką aplikację w obrazie tego systemu. Dodatkowo, dzięki takim narzędziom jak Desired State Configuration, Chef czy Puppet wiele zadań konfiguracyjnych może zostać całkowicie zautomatyzowanych, co znacznie upraszcza proces konfiguracji systemu po jego instalacji.

Jeśli nasza strategia wdrażania uwzględnia utworzenie i przechwycenie istniejącego systemu Windows Server 2016, należy pamiętać, że przed przechwyceniem tego systemu będziemy musieli dokonać jego uogólnienia, usuwając w ten sposób wszelkie informacje, które są unikalne dla tej instalacji. Zadanie to możemy wykonać za pomocą narzędzia `Sysprep.exe`. Program ten dostępny jest na nośniku instalacyjnym systemu Windows Server 2016 w folderze C:\Windows\System32\Sysprep. W ramach przygotowywania obrazu narzędziem Sysprep możemy przywrócić ten obraz do systemowego trybu Out-of-Box Experience (OOBE), jak to pokazano na rysunku 3-8. System w trybie OOBE znajduje się w dokładnie takim samym stanie, w jakim znajduje się podczas swojego pierwszego uruchomienia, z tym że w tym przypadku wszystkie aktualizacje, aplikacje i sterowniki zawarte w przechwyconym obrazie będą już zainstalowane.

Aby przechwycić obraz, należy posłużyć się narzędziem `Dism.exe` z przełącznikiem `/Capture-Image` lub poleceniem PowerShell o nazwie `New-Windows Image`.



Rysunek 3-8 Narzędzie Sysprep

Pliki odpowiedzi

Pliki odpowiedzi stanowią tradycyjną metodę wdrażania i konfigurowania systemu operacyjnego. Choć nie są one tak wszechstronne, jak niektóre nowsze technologie – jak choćby Desired State Configuration, która wspomaga nie tylko sam proces wdrażania, ale też zapewnia konfigurację ciągłą – pliki odpowiedzi pozwalają nam zautomatyzować proces wdrażania systemu Windows Server.

Zamiast ręcznego instalowania nowego serwera i wykonywania na nim określonych zadań poinstalacyjnych, takich jak przyłączanie serwera do domeny AD DS, możemy zautomatyzować te czynności za pomocą plików odpowiedzi. Podczas uruchamiania programu instalatora system Windows Server sprawdza lokalne i zewnętrzne nośniki danych pod kątem obecności pliku Autounattend.xml. Jeśli plik ten zostanie znaleziony, Windows Server automatycznie wykorzysta zawarte w nim ustawienia w celu skonfigurowania nowego serwera.

Jak wskazuje jego nazwa, plik Autounattend.xml wykorzystuje format pliku XML. Choć możliwe jest ręczne edytowanie tego pliku za pomocą zwykłego edytora tekstowego, takiego jak Notatnik, proces ten jest dosyć skomplikowany, przez co jest wysoce prawdopodobne, że w którymś miejscu popełnimy w nim jakiś błąd, który uniemożliwi nam automatyczne zainstalowanie systemu z wykorzystaniem tego pliku. Do utworzenia pliku odpowiedzi możemy wykorzystać narzędzie graficzne Windows System Image Manager, znane również jako Windows SIM. Przy korzystaniu z tego narzędzia musimy określić docelowy obraz, dla którego chcemy utworzyć plik odpowiedzi. Wtedy Windows SIM utworzy specjalny plik katalogu dla wszystkich opcji, które możemy skonfigurować dla tego obrazu. Po skonfigurowaniu wszystkich ustawień, które mają być zautomatyzowane podczas instalacji i późniejszej konfiguracji, możemy wykorzystać to narzędzie do wygenerowania pliku odpowiedzi z poprawną składnią XML. Narzędzie Windows SIM zawarte jest w pakiecie Windows Assessment and Deployment Kit (Windows ADK), który dostępny jest do pobrania z witryny Microsoft.