



Inside **OUT**

Wyczerpujący, kompletny poradnik
Setki rozwiązań oszczędzających czas
Doskonale uporządkowany
i wypełniony eksperckimi
wskazówkami

Windows Server 2019

Orin Thomas

Microsoft Cloud Operations Advocate, ekspert Cloud and Datacenter i wiodący autor

Orin Thomas

Windows Server 2019 Inside Out

Przekład: Krzysztof Kapustka, Marek Włodarz

APN Promise, Warszawa 2020

Windows Server 2019 Inside Out

Authorized Polish translation of the English language edition entitled
Windows Server 2019 Inside Out, by Orin Thomas, ISBN: 978-0-13-549227-7

Copyright © 2020 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 © 2020

Autoryzowany przekład z wydania w języku angielskim, zatytułowanego:
Windows Server 2019 Inside Out, by Orin Thomas, ISBN: 978-0-13-549227-7

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiegokolwiek 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 jakiegokolwiek 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 jakiegokolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-429-5 (druk), 978-83-7541-433-2 (ebook)

Przekład: Krzysztof Kapustka, Marek Włodarz

Korekta: Ewa Swędrowska

Skład i łamanie: MAWart Marek Włodarz

Spis treści

<i>O autorze</i>	xix
<i>Wprowadzenie</i>	xxi
1 Narzędzia administracyjne	1
Zdalnie, nie lokalnie	1
Stacje robocze z dostępem uprzywilejowanym	2
Windows Admin Center	4
Instalowanie Windows Admin Center	7
Rozszerzenia Windows Admin Center	10
Pokazywanie skryptu	11
Narzędzia zdalnej administracji serwerem	12
Konsole RSAT	13
Konsola Server Manager	16
PowerShell	19
Moduły	21
Galeria PowerShell	21
Obsługa zdalna	22
Obsługa zdalna wielu maszyn	23
PowerShell ISE	24
PowerShell Direct	27
Pulpit zdalny	28
SSH	30
2 Opcje instalacji	33
Edycje Windows Server 2019	33
Kanały obsługi Windows Server	35
LTSC	35
Semi Annual Channel	36
Kompilacje Insider Preview	37
Server Core	38
Interfejs systemu Server Core	39
Role w systemie Server Core	40
App Compatibility Features on Demand	44

Kiedy wdrażać Server Core	45
Serwer z interfejsem graficznym	47
Role i funkcje	47

3 Wdrożenie i konfiguracja

Wdrożenie fizyczne a wirtualne	51
Obrazy systemu Windows	52
Modyfikowanie obrazów Windows	53
Obsługiwanie obrazów Windows	54
Montowanie obrazów	55
Dodawanie do obrazów sterowników i aktualizacji	57
Dodawanie ról i funkcji	59
Zatwierdzanie zmian w obrazie	61
Tworzenie i przechwytywanie	61
Pliki odpowiedzi	62
Windows Deployment Services	65
Wymagania usługi WDS	65
Zarządzanie obrazami	67
Konfigurowanie serwera WDS	68
Konfigurowanie transmisji	73
Grupy i pakiety sterowników	74
Virtual Machine Manager	74
Szablony maszyn wirtualnych	75
Magazyn programu VMM	76
Sieci VMM	77
Dodawanie usługi WDS do programu VMM	82
Grupy hostów VMM	84
Konfiguracja infrastruktury jako kod	86
Desired State Configuration	88
Pliki konfiguracji DSC	89
Local Configuration Manager	90
Zasoby DSC	91
Model Push	91
Serwer ściągania	92
Chef Infra Server	93
Serwery Chef	93
Chef Development Kit	97
Wdrażanie agentów Chef	102

Wdrażanie książek kucharskich i przepisów Chef	103
Puppet	104
Puppet Master	104
Wdrażanie agenta Puppet w Windows Server	107
Zarządzanie konfiguracją Windows Server	109
Pakiet modułów Windows	110
Narzędzia zarządzania pakietami	112
Galeria PowerShell	114
Chocolatey	115
4 Active Directory	119
Zarządzanie środowiskiem Active Directory	119
Administracja zdalna zamiast lokalnej	120
Active Directory Administrative Center	121
Active Directory Users and Computers	123
Active Directory Sites and Services	125
Active Directory Domains and Trusts	127
Kontrolery domeny	128
Wdrażanie	129
Server Core	131
Serwery wykazu globalnego	132
Kontrolery domeny tylko do odczytu	133
Wirtualne klonowanie kontrolera domeny	136
Struktura środowiska AD DS	137
Domeny	137
Poziomy funkcjonalności domen	137
Lasy	139
Lasy kont i zasobów	139
Jednostki organizacyjne	140
Role wzorców operacji	141
Konta	143
Konta użytkowników	144
Konta komputerów	145
Konta grup	146
Grupy domyślne	147
Konta usług	150
Zasady grupy	152
Zarządzanie obiektami GPO	153

Przetwarzanie zasad	156
Preferencje zasad grupy	158
Szablony administracyjne	160
Przywracanie usuniętych elementów	161
Kosz usługi Active Directory	163
Przywracanie autorytatywne	164
Migawki usługi Active Directory	166
Zarządzanie usługą AD DS z poziomu programu PowerShell	168
Moduł ActiveDirectory	168
Moduł GroupPolicy	172
Moduł ADDSDeployment	173
5 DNS, DHCP i IPAM	175
DNS	175
Rodzaje stref DNS	175
Delegowanie stref	179
Usługi przesyłania dalej i warunkowego przesyłania dalej	180
Strefy skrótowe	181
Strefy GlobalNames	182
Protokół PNRP	183
Rekordy zasobów	184
Przedawianie i oczyszczanie stref	185
DNSSEC	186
Dzienniki zdarzeń DNS	188
Opcje DNS	189
Administracja delegowana	193
Zarządzanie usługą DNS za pomocą PowerShell	193
DHCP	197
Zakresy	197
Opcje serwera i zakresu DHCP	198
Zastrzeżenia	199
Filtrowanie DHCP	199
Superzakresy	200
Zakresy multitemisji	200
Podziały zakresów	201
Ochrona nazwy	201
Tryb pracy awaryjnej	202
Administracja	203

IPAM	206
Wdrażanie IPAM	206
Konfigurowanie odnajdowania serwerów	207
Administrowanie serwerem IPAM	208
Zarządzanie usługą IPAM z poziomu programu PowerShell	210
6 Hyper-V	213
Pamięć dynamiczna	214
Inteligentne stronicowanie	215
Pomiar zasobów	215
Usługi integracji dla systemów operacyjnych gościa	216
Maszyny wirtualne drugiej generacji	217
Tryb sesji rozszerzonej	218
Discrete Device Assignment	218
Wirtualizacja zagnieżdżona	220
Pamięć dynamiczna wirtualizacji zagnieżdżonej	220
Sieć wirtualizacji zagnieżdżonej	220
PowerShell Direct	221
HVC for Linux	222
Wirtualne dyski twarde	222
Dyski o stałym rozmiarze	223
Dyski dynamiczne	223
Dyski różnicowe	224
Modyfikowanie wirtualnych dysków twardych	225
Dyski przekazane	225
Zarządzanie punktami kontrolnymi	226
Wirtualne karty Fibre Channel	228
Jakość usług magazynowania	229
Optymalizacja magazynu Hyper-V	229
Deduplikacja	229
Tworzenie warstw magazynowania	230
Wirtualne przełączniki Hyper-V	230
Przełączniki zewnętrzne	230
Przełączniki wewnętrzne	231
Przełączniki prywatne	231
Karty sieciowe maszyn wirtualnych	232
Optymalizowanie wydajności sieci	232
Zarządzanie przepustowością	233

SR-IOV	233
Dynamiczna kolejka maszyn wirtualnych	233
Zespół kart interfejsu sieciowego w maszynie wirtualnej	234
Adresy MAC maszyn wirtualnych	234
Izolacja sieci	235
Hyper-V Replica	236
Konfigurowanie serwerów repliki Hyper-V	237
Konfigurowanie repliki maszyny wirtualnej	237
Przełączanie repliki w tryb failover	239
Broker funkcji Hyper-V Replica	239
Klastry Hyper-V trybu failover	239
Magazyn klastra hostów Hyper-V	239
Kworum klastra	241
Sieć klastra	243
Wymuszanie odporności kworum	244
Udostępnione woluminy klastra	244
Klastry odłączone od Active Directory	245
Preferowany właściciel i ustawienia trybu failover	246
Klastry gościa funkcji Hyper-V	246
Magazyn klastra gościa Hyper-V	247
Udostępnione wirtualne dyski twarde	248
Zestawy dysków VHD Hyper-V	249
Migracja na żywo	249
Migracja magazynu	251
Eksportowanie, importowanie i kopiowanie maszyn wirtualnych	252
Wykrywanie kondycji sieci maszyny wirtualnej	253
Opróżnianie maszyn wirtualnych przy wyłączaniu	253
Klonowanie kontrolera domeny	254
Chronione maszyny wirtualne	254
Zarządzanie Hyper-V z poziomu programu PowerShell	255
7 Usługi magazynowania	261
Miejsca do magazynowania i pule magazynu	261
Pule magazynu	262
Odporność miejsc do magazynowania	266
Tworzenie warstw magazynowania	267
Alokowanie elastyczne i przycinanie magazynu	269
Tworzenie wirtualnych dysków twardych	272

Bezpośrednie miejsca do magazynowania	273
Replika magazynu.....	281
Obsługiwane konfiguracje	282
Konfigurowanie replikacji	283
SMB 3.1.1	286
iSCSI.....	288
Serwer iSNS	292
Skalowalny w poziomie serwer plików	294
Serwer dla NFS	295
Deduplikacja.....	297
Jakość usług magazynowania.....	299
ReFS.....	301
Polecenia programu PowerShell związane z magazynowaniem.....	303
Moduł Deduplication.....	303
Moduł iSCSI.....	304
Moduł iSCSITarget	304
Moduł NFS.....	305
Moduł Storage	305
Moduł StorageReplica.....	309
8 Serwery plików	311
Uprawnienia folderów udostępnionych	312
Korzystanie z Eksploratora plików.....	313
Windows Admin Center	315
Server Manager	315
File Server Resource Manager.....	318
Przydziały na poziomie folderów	318
Osłony plików	321
Raporty magazynowania.....	325
Klasyfikacja plików	327
Zadania zarządzania plikami	329
Access-Denied Assistance.....	331
Rozproszony system plików.....	333
Obszary nazw DFS	333
Replikacja DFS.....	336
BranchCache	340
Polecenia PowerShell	343
Polecenia folderów udostępnionych.....	343

Polecenia konsoli File Server Resource Manager	345
Polecenia usługi BranchCache	347
Polecenia DFS	348
9 Internet Information Services	351
Zarządzanie witrynami	351
Dodawanie witryn	352
Katalogi wirtualne	355
Modyfikowanie ustawień witryny	356
Konfigurowanie certyfikatów TLS	357
Uwierzytelnianie witryny	360
Modyfikowanie niestandardowych odpowiedzi na błędy	362
Dodawanie lub wyłączenie domyślnego dokumentu	363
Przeglądanie katalogów	364
Filtrowanie adresów IP i nazw domen	364
Reguły autoryzacji adresów URL	366
Filtry żądań	367
Pule aplikacji	369
Tworzenie pul aplikacji	369
Konfigurowanie ustawień odtwarzania puli aplikacji	370
Użytkownicy i delegowanie w IIS	372
Konta użytkowników IIS	374
Delegowanie uprawnień administracyjnych	374
Zarządzanie serwerem FTP	375
Zarządzanie IIS za pomocą programu PowerShell	378
10 Kontenery	381
Pojęcia związane z kontenerami	381
Tryby izolacji	384
Tryb izolacji procesu	384
Tryb izolacji Hyper-V	384
Zarządzanie kontenerami poprzez Docker	385
Instalacja Docker	385
Demon.json	387
Pozyskiwanie bazowego obrazu systemu operacyjnego kontenera ..	389
Rejestry i obrazy kontenerów	390
Zarządzanie kontenerami	393
Uruchamianie kontenera	393

Modyfikowanie uruchomionego kontenera	396
Tworzenie nowego obrazu na podstawie kontenera	396
Korzystanie z plików Dockerfile	397
Zarządzanie obrazami kontenerów	399
Konta usług dla kontenerów Windows	401
Instalowanie aktualizacji	402
Sieci w kontenerach	403
Tryb NAT	405
Tryb Transparent	406
Tryb Overlay	408
Tryb Layer 2 Bridge	408
Kontenery Linux w Windows	409
Orkiestracja kontenerów	411
Kubernetes	412
Docker Swarm	412
Tworzenie klastrów Swarm	413
Tworzenie sieci nakładkowej	413
Wdrażanie i skalowanie usług klastra Swarm	414
11 Klastry i wysoka dostępność	417
Klaster pracy awaryjnej	417
Tryby kworum klastra	418
Magazyn klastra i udostępnione woluminy klastra	420
Sieci klastra	421
Aktualizacje typu cluster-aware	421
Ustawienia preferencji i praca awaryjna	422
Klastry wielolokacyjne	423
Świadek w chmurze	424
Klastrowanie awaryjne maszyn wirtualnych	425
Uaktualnianie stopniowe	427
Klastry grup roboczych	429
Zestawy klastrów	430
Zarządzanie klastrem pracy awaryjnej przy użyciu PowerShell	431
Network Load Balancing	434
Wymagania NLB	435
Tryby operacji NLB	436
Zarządzanie hostami klastra	437
Reguły portów	438

Filtrowanie i koligacja	438
Zarządzanie NLB przy użyciu PowerShell.....	439
12 Active Directory Certificate Services.....	441
Typy CA.....	441
Urząd certyfikacji przedsiębiorstwa.....	443
Autonomiczne urzędy certyfikacji.....	454
Listy odwołań certyfikatów	458
Punkty dystrybucji CRL	458
Dostęp do informacji o urzędach	459
Odwoływanie certyfikatu	460
Publikowanie CRL i delta-CRL	461
Usługi roli Certificate Services.....	463
Szablony certyfikatów	464
Właściwości szablonu	466
Dodawanie i edytowanie szablonów.....	471
Automatyczne rejestrowanie i odnawianie certyfikatów	472
Zarządzanie CA	474
Obsługa żądań certyfikatów.....	476
Kopie zapasowe i przywracanie CA.....	477
Archiwizowanie i przywracanie kluczy	479
CAPolicy.inf	483
Zarządzanie Certificate Services przy użyciu PowerShell	485
Zarządzanie usługami certyfikatów przy użyciu narzędzi Certutil.exe i Certreq.exe	487
13 Active Directory Federation Services	489
Komponenty AD FS.....	489
Oświadczenia, reguły oświadczeń i magazyny atrybutów	490
Dostawca oświadczeń	490
Jednostka zależna.....	491
Relacja zaufania jednostki zależnej.....	492
Relacja zaufania dostawcy oświadczeń.....	492
Konfigurowanie relacji certyfikatów	493
Magazyny atrybutów.....	494
Reguły oświadczeń	495
Reguły relacji zaufania jednostki zależnej	495
Reguły relacji zaufania dostawcy oświadczeń.....	496

Konfigurowanie proxy aplikacji Web	496
Workplace Join	499
Uwierzytelnianie wieloczynnikowe	500
Zarządzanie AD FS przy użyciu PowerShell	502
Zarządzanie proxy aplikacji Web przy użyciu PowerShell	506
14 Dynamic Access Control i Active Directory Rights Management Services	507
Dynamic Access Control	507
Konfigurowanie zasad grupy w celu obsługi DAC	508
Konfigurowanie oświadczeń użytkowników i urzędzeń	508
Konfigurowanie właściwości zasobów	510
Centralne reguły dostępu	512
Centralne zasady dostępu	514
Przemieszczanie	515
Access Denied Assistance	516
Instalowanie AD RMS	517
Certyfikaty i licencje AD RMS	519
Szablony AD RMS	520
Administratorzy AD RMS i super-użytkownicy	523
Zaufane domeny użytkowników i publikowania	524
Zasady wykluczania	524
Automatyczne stosowanie szablonów AD RMS	525
Zarządzanie AD RMS przy użyciu Windows PowerShell	526
Zarządzanie Dynamic Access Control przy użyciu PowerShell	528
15 Routing i dostęp zdalny	529
Remote Desktop Gateway	529
Zasady połączeń i zasobów RD Gateway	530
Konfigurowanie ustawień serwera	532
Konfigurowanie klientów do korzystania z RD Gateway	532
Wirtualne sieci prywatne	533
Protokół IKEv2 (Always On VPN)	534
Protokół SSTP	535
Protokoły L2TP/IPsec	536
Protokół PPTP	536
Uwierzytelnianie VPN	537
Wdrażanie serwera VPN	537

Wyłączanie protokołów VPN	538
Przyznawanie prawa dostępu do serwera VPN.....	539
Routing LAN.....	543
Network Address Translation (NAT).....	544
DirectAccess.....	545
Topologie DirectAccess.....	546
Serwer DirectAccess.....	547
Serwer lokalizacji sieciowej.....	549
Konfigurowanie DirectAccess.....	550
Zarządzanie dostępem zdalnym przy użyciu PowerShell.....	554
16 Usługi pulpitu zdalnego.....	557
Wdrożenie	557
Remote Desktop Connection Broker.....	559
Właściwości wdrożenia	560
Remote Desktop Session Host	561
Ustawienia kolekcji sesji	562
Osobiste sesje pulpitu	564
RemoteApp.....	564
Konfigurowanie zasad grupy	565
Remote Desktop Virtualization Host.....	567
Przygotowywanie maszyn wirtualnych.....	568
Kolekcje pulpitu wirtualnych.....	569
Pule pulpitu wirtualnych	570
Osobiste pulpity wirtualne	571
DDA oraz RemoteFX	571
Remote Desktop Web Access.....	571
Licencjonowanie pulpitu zdalnego	572
Instalowanie RDS CAL	573
Aktywowanie serwera licencji.....	574
Zarządzanie usługami pulpitu zdalnego przy użyciu PowerShell.....	574
17 Azure IaaS i usługi hybrydowe	577
Maszyny wirtualne Windows Server	577
Tworzenie maszyn wirtualnych Azure IaaS	579
Sieci maszyn wirtualnych IaaS	583
Administrowanie maszyną wirtualną IaaS	590
Azure Active Directory.....	598

Azure Active Directory Connect	599
Wymagania serwera Azure AD Connect	601
Instalowanie Azure AD Connect	604
Korzystanie z sufiksów UPN i nierutowalne domeny	612
Azure AD Connect Health	615
Wymuszanie synchronizacji	616
Konfigurowanie filtrów obiektów	619
Implementowanie i zarządzanie samodzielnym resetowaniem haseł w Azure AD	621
Azure AD Password Protection	623
Azure AD Domain Services	624
Hybrydowe usługi chmurowe Azure	626
Dołączanie Windows Admin Center	626
Tworzenie maszyn wirtualnych Azure IaaS w Windows Admin Center	628
Azure File Sync	631
Azure Arc	634
Azure Site Recovery	634
Azure Network Adapter	635
18 Windows Subsystem for Linux	637
Linux w Windows Server	637
Instalowanie WSL	638
WSL 2.0	642
19 Wzmacnianie zabezpieczeń Windows Server i Active Directory	645
Wzmacnianie zabezpieczeń Active Directory	646
Wzmacnianie zabezpieczeń kontrolerów domeny	646
Minimalne przywileje	647
Kontrola dostępu oparta na rolach	649
Zasady kont	649
Opcje zabezpieczeń konta	650
Konta chronione	652
Zasady uwierzytelniania i silosy	654
Wyłączenie NTLM	655
Blokowanie możliwości planowania zadań przez operatorów serwerów	656
Włączanie ochrony LSA	657
Hasło konta KRBTGT	658

Las administracyjny	659
Wzmacnianie zabezpieczeń Windows Server.....	661
Prawa użytkowników.....	662
Konta usługowe	668
Just Enough Administration (JEA)	671
Zarządzanie uprzywilejowanym dostępem	679
Local Administrator Password Solution	683
Zaawansowana inspekcja	685
Windows Firewall with Advanced Security.....	688
Chronione maszyny wirtualne.....	699
Chroniona sieć szkieletowa.....	702
20 Systemy i usługi zabezpieczeń.....	707
Security Compliance Toolkit	707
Policy Analyzer	708
Narzędzie Local Group Policy Object.....	710
Attack Surface Analyzer.....	710
Credential Guard.....	712
Windows Defender Application Control.....	714
Zabezpieczenia oparte na wirtualizacji.....	717
Controlled Folder Access	718
Exploit Protection	720
Windows Defender.....	723
Windows Defender SmartScreen	724
21 Monitorowanie i konserwacja	725
Zestawy modułów zbierających dane	725
Alerty.....	727
Event Viewer	727
Filtry dzienników zdarzeń.....	728
Widoki dzienników zdarzeń.....	728
Subskrypcje zdarzeń	730
Zadania sterowane zdarzeniami	731
Monitorowanie sieci	732
Resource Monitor.....	733
Message Analyzer.....	733
Azure Monitor	734
Windows Server Backup.....	736

Lokalizacje kopii zapasowych	737
Kopiowanie danych	738
Kopie zapasowe specyficzne dla ról i aplikacji	738
Przywracanie z kopii zapasowych	739
Przywracanie w lokalizacji alternatywnej	740
Azure Backup	740
Przygotowywanie Azure Backup	741
Wykonywanie kopii zapasowych przy użyciu Azure Backup Agent	743
Przywracanie z Azure Backup	743
Vssadmin	745
Windows Server Update Services	746
Produkty, klasyfikacje zabezpieczeń i języki	746
Tryby autonomiczny i repliki	747
Pliki aktualizacji	748
Role zabezpieczeń WSUS	749
Grupy WSUS	750
Zasady WSUS	750
Wdrażanie aktualizacji	752
Reguły automatycznego zatwierdzania	753
Azure Update Management	755
Polecenia cmdlet Windows PowerShell dotyczące monitorowania i konserwacji	758
Polecenia PowerShell dotyczące WSUS	760
22 Uaktualnianie i migracja	761
Obsługiwane ścieżki uaktualniania i migracji	761
Uaktualnianie ról i funkcji	763
Konwertowanie wersji próbnej do wersji licencjonowanej	765
Uaktualnianie wydań	766
Windows Server Migration Tools	766
Active Directory	770
Migrowanie FRS do DFSR	772
Migracja do nowego lasu	773
Active Directory Certificate Services	776
Przygotowania	778
Migracja	780
Weryfikacja i zadania pomigracyjne	781
DNS	781

DHCP	783
Przygotowania do migracji DHCP	783
Migracja	786
Weryfikacja i zadania pomigracyjne	786
Serwery plików i magazynowania	787
Migrowanie serwerów plików przy użyciu Storage Migration Service	787
Migrowanie serwerów plików przy użyciu WSMT	796
Uprawnienia migracji	797
Przygotowania do migracji	797
Migrowanie roli File and Storage Services	799
23 Rozwiązywanie problemów	801
Metodologia rozwiązywania problemów	801
Ponowna instalacja	802
Symptomy i diagnoza	804
Zależności	805
Ocenianie hipotetycznych rozwiązań	806
Stosowanie rozwiązania	807
Narzędzia wiersza polecenia	807
Narzędzia Sysinternals	812
Process Explorer	812
Process Monitor	814
ProcDump	815
PS Tools	815
VMMap	817
SigCheck	818
AccessChk	819
Sysmon	819
AccessEnum	824
ShellRunAs	825
LogonSessions	826
Active Directory Explorer	827
ADInsight	830
PsPing	830
RAMMap	831
Indeks	835

O autorze



Orin Thomas jest głównym promotorem operacji chmurowych w firmie Microsoft. Napisał ponad trzydzieści książek dla wydawnictwa Microsoft Press, poświęconych takim zagadnieniom, jak systemy Windows Server, Azure, System Center, Exchange Server, SQL Server i bezpieczeństwo systemów klienckich i serwerowych. Pisuje w portalu PluralSight, a także jest autorem szeregu oficjalnych kursów szkoleniowych Microsoft Official Curriculum i EdX dla rozmaitych zagadnień IT Pro. Uzyskał doktorat z informatyki na Charles Sturt University.

Można się z nim skontaktować na Twitterze: <http://twitter.com/orinthomas>.

Wprowadzenie

Książka ta została napisana dla profesjonalistów IT, którzy regularnie pracują z systemami Windows Server. Najprawdopodobniej Windows Server 2019 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 2019.

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 2019 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.

Zmiany w porównaniu do wersji *Windows Server 2016 Inside Out*

To wydanie książki zawiera kilka nowych rozdziałów oraz poprawki i uzupełnienia – od kosmetycznych po zasadnicze – rozdziałów, które były obecne w wersji dla systemu Windows Server 2016. Niektóre z tych zasadniczych zmian obejmują usunięcie treści dotyczących opcji instalacji Nano Server, która nie jest już obsługiwana; omówienie nowej konsoli Windows Admin Center; zupełnie nowe rozdziały na temat Azure IaaS i usług hybrydowych, a także Windows Subsystem for Linux. Rozdział dotyczący bezpieczeństwa z wydania 2016 został podzielony na dwa i znacząco rozbudowany.

W książce znalazło się również omówienie nowych ról i funkcji, w tym Storage Migration Services, Azure File Sync oraz Azure Update Management. Choć w niektórych rozdziałach dokonałem jedynie kosmetycznych poprawek, pod względem całkowitej liczby słów ta książka jest o około 15 procent obszerniejsza, niż wydanie poprzednie, czyli *Windows Server 2016 Inside Out*.

Podziękowania

Rick Kughen, Vince Averello, Dan Foster, Charvi Arora i Loretta Yates – wasza nieoceniona pomoc sprawiła, że udało się doprowadzić tę pracę do upragnionego finału, jakim jest druk. Chciałbym również podziękować Thomasowi Maurerowi za jego porady przy wprowadzaniu zmian i pomysły, co powinno znaleźć się w nowym wydaniu.

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:

MicrosoftPressStore.com/WindowsServer2019InsideOut/errata

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

Jeśli potrzebna jest dodatkowa pomoc, prosimy odwiedzić stronę

MicrosoftPressStore.com/Support

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



Rozdział 1

Narzędzia administracyjne

Zdalnie, nie lokalnie	1	Narzędzia zdalnej administracji serwerem	12
Stacje robocze z dostępem uprzywilejowanym.....	2	PowerShell	19
Windows Admin Center	4	Pulpit zdalny.....	28
		SSH.....	30

Zarządzanie Windows Server 2019 można realizować przy użyciu różnych narzędzi. Niektóre, takie jak PowerShell, konsole MMC (Microsoft Management Console) czy Server Manager, są wbudowane w system operacyjny. Inne, takie jak Windows Admin Center, można pobrać bezpłatnie z witryny firmy Microsoft.

Ogólna filozofia firmy Microsoft w zakresie administracji systemami mówi, że choć niemal wszystko można wykonać przy użyciu graficznej konsoli, takiej jak Windows Admin Center, Active Directory Administrative Center lub Server Manager, wszelkie powtarzane przez nas zadania powinniśmy automatyzować za pomocą Windows PowerShell. Najlepsze praktyki firmy Microsoft stwierdzają, że niemal wszystkie zadania administracyjne powinny być wykonywane zdalnie, a nie poprzez logowanie na serwerze i ich lokalną realizację.

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 2019.

Zdalnie, nie lokalnie

Windows Server projektowany był z myślą o administracji zdalnej, nie lokalnej. Tego rodzaju filozofia „najpierw zdalnie” nie powinna być zaskoczeniem dla doświadczonych administratorów. Ogromna większość wystąpień Windows Server działa jako maszyny wirtualne, albo w centrach danych, albo w chmurze i dawno minęły czasy, gdy podstawową metodą przełączania się pomiędzy różnymi serwerami, na których pracujemy, było wybieranie różnych opcji na przełącznikach KVM.

Musimy dobrze opanować zdalne korzystanie z naszych narzędzi. Powinniśmy też unikać logowania się do każdego serwera indywidualnie przy użyciu Pulpitu zdalnego i uruchamiania konsoli odpowiadającej roli czy funkcji, którą chcemy zarządzać. Powinniśmy również unikać stosowania Pulpitu zdalnego w celu połączenia się z serwerem jedynie po to, aby uruchomić skrypt PowerShell.

Głównym powodem, dla którego należy unikać stosowania Pulpitu zdalnego jest to, że umożliwia on interakcję z tylko jednym serwerem na raz. Rozważmy ilość czasu, który trzeba poświęcić na wykonanie jakiegoś zadania, takiego jak zresetowanie hasła nieuprzywilejowanego konta lokalnego użytkownika na 100 różnych serwerach. Gdybyśmy chcieli to zrobić przy użyciu Pulpitu zdalnego, musielibyśmy połączyć się kolejno z każdym serwerem, zmienić hasło, wylogować się, po czym przejść do następnego serwera. Jeśli zaś zrobimy to za pomocą zdalnych funkcji PowerShell, można osiągnąć ten sam cel pojedynczym skryptem, który można napisać i wykonać w nieznacznym ułamku tego czasu.

Od podszewki

Automatyzuj, co tylko się da

Wykonywane przez siebie zadania powinienś automatyzować tam, gdzie się da, i tam, gdzie ma to sens. Trzeba mieć na uwadze, że nie będziesz w stanie zautomatyzować *wszystkiego*. Skoncentruj się na zautomatyzowaniu tego, co można. 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 lub które opierają się automatyzacji.

Stacje robocze z dostępem uprzywilejowanym

Serwery są tak bezpieczne, jak bezpieczne są komputery wykorzystywane do zarządzania tymi serwerami. 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. 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 czytania poczty czy przeglądania Internetu, a jedynie do wykonywania zadań administracyjnych na serwerach.

Stacja robocza PAW powinna spełniać następujące wymagania:

- Skonfigurowana funkcja Windows Defender Application Control (Device Guard), zezwalająca na uruchamianie na tym komputerze wyłącznie podpisanego cyfrowo i jawnie autoryzowanego oprogramowania.

- Skonfigurowana funkcja Credential Guard w celu ochrony poświadczeń przechowywanych na komputerze.
- Użycie BitLocker do zaszyfrowania dysku 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 zarówno lokalnie, jak i na brzegowej zaporze sieciowej.
- Dostęp do Internetu na stacji roboczej PAW powinien być zablokowany. Aktualizacje oprogramowania powinny być pozyskiwane z dedykowanego, zabezpieczonego serwera aktualizacji w naszej sieci lokalnej. Narzędzia zewnętrzne powinny być uzyskiwane przy użyciu innego komputera i następnie transferowane do PAW.
- Administratorzy serwerów nie powinni logować się do stacji roboczej PAW z użyciem konta użytkownika z uprawnieniami administratora na tej stacji. W rozdziale 19, „Wzmacnianie zabezpieczeń Windows Server i Active Directory”, powiemy sobie więcej zabezpieczonych lasach kont w celu podniesienia zabezpieczeń kont.
- Tylko wybrane konta użytkownika wykorzystywane przez administratorów serwerów powinny móc logować się do stacji roboczej PAW. Rozważmy wprowadzenie dodatkowych ograniczeń, takich jak godziny logowania. Blokujemy 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. Można to zrealizować przy użyciu Windows Defender Firewall.
- 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.

- Blokujemy nieinicjowany z wewnątrz ruch przychodzący do stacji roboczych PAW przy użyciu Windows Defender Firewall.

Od podszewki

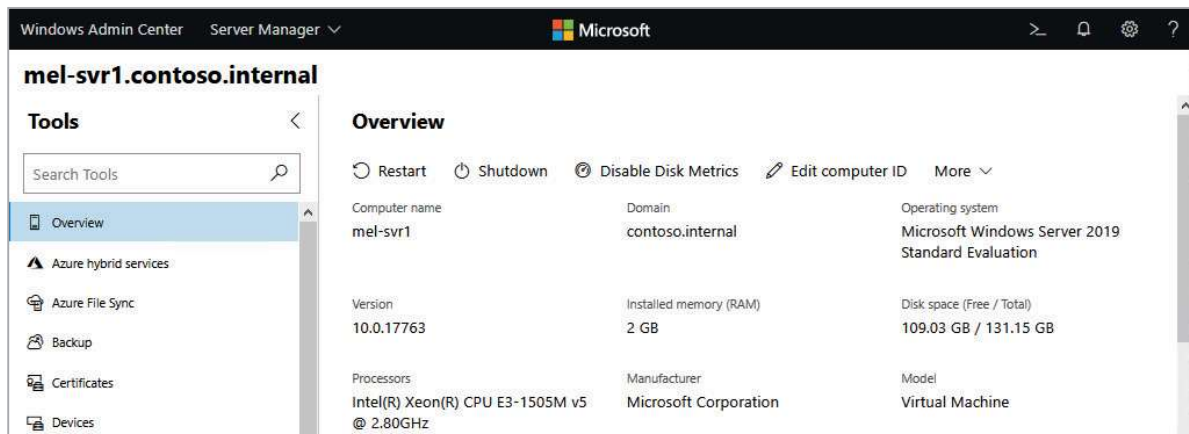
Serwery przeskoku

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.

Windows Admin Center

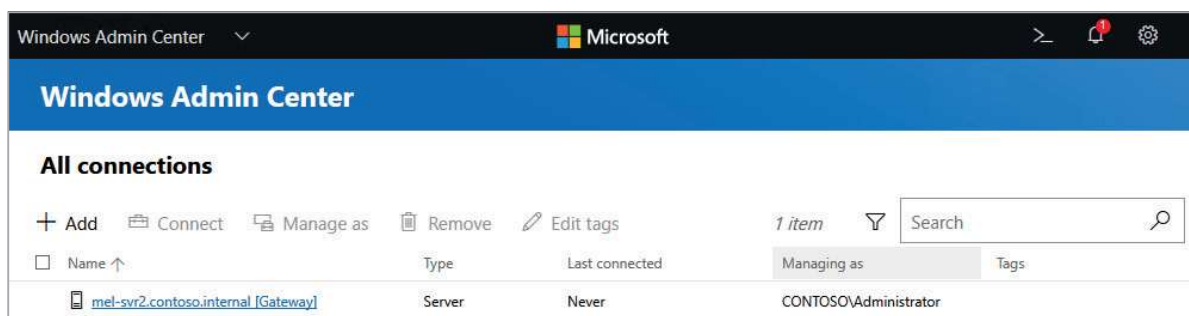
Windows Admin Center to oparta na Web konsola pozwalająca na zdalne zarządzanie Windows Server poprzez przeglądarkę. Z Windows Admin Center można się połączyć przy użyciu przeglądarek Edge, Firefox oraz Chrome (ale nie poprzez Internet Explorer). Konsolę Windows Admin Center można zainstalować na komputerach systemu Windows 10, Windows Server 2016 albo Windows Server 2019. Co istotne, Windows Admin Center można zainstalować w systemie Windows Server wdrożonych przy użyciu opcji instalacyjnej Server Core.

Konsola Windows Admin Center, pokazana na rysunku 1-1, umożliwia zarządzanie komputerami działającymi pod kontrolą Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 oraz Windows Server 2019. Konsola pozwala również na wykonywanie pewnej ograniczonej liczby zadań na komputerach systemu Windows Server 2008 R2, ale ponieważ wsparcie techniczne dla Windows Server 2008 R2 skończyło się w styczniu 2020 roku, rozsądne będzie założenie, że w przyszłych wersjach Windows Admin Center nie pojawią się żadne dodatkowe funkcjonalności dotyczące tej wersji systemu.



RYSUNEK 1-1 Windows Admin Center

Gdy jesteśmy połączeni z serwerem bramy, kliknięcie Add na stronie All Connections pokazanej na rysunku 1-2 umożliwi dołączenie dodatkowych serwerów, którymi chcemy zarządzać. Pojawi się okno dialogowe z monitem o wpisanie poświadczeń konta posiadającego lokalne uprawnienia administracyjne na dodawanym serwerze.



RYSUNEK 1-2 Windows Admin Center – strona All Connections

Konsolę Windows Admin Center (WAC) możemy wykorzystywać do realizowania zadań na serwerach w siedzibie, wyliczonych w tabeli 1-1. Zauważmy, że wiele narzędzi wewnątrz WAC pozwala obecnie na wykonywanie tylko niektórych – nie wszystkich – zadań, które można realizować przy użyciu jednej ze starszych konsoli MMC. Jednak docelowo narzędzia te będą ewoluować, aż do pełnego wyrównania funkcjonalności.

TABELA 1-1 Narzędzia WAC i ich funkcjonalności

Narzędzie WAC	Funkcja
Overview	Szczegóły serwera i kontrolowanie stanu
Active Directory	Wykonywanie pewnych zadań zarządzania Active Directory
Backup	Zarządzanie Azure Backup
Certificates	Wyświetlanie i modyfikowanie certyfikatów, włącznie z wygaszaniem certyfikatów

TABELA 1-1 Narzędzia WAC i ich funkcjonalności

Narzędzie WAC	Funkcja
Containers	Zarządzanie kontenerami
Devices	Zarządzanie urządzeniami (podobnie do konsoli Device Manager)
DHCP	Wykonywanie pewnych zadań administracji DHCP
DNS	Wykonywanie pewnych zadań administracji DNS
Events	Wyświetlanie zdarzeń. Podobne do konsoli Event Viewer
Files	Przeglądanie plików i folderów
Firewall	Zarządzanie regułami zapory
Installed Apps	Dodawanie i usuwanie programów
Local Users and Groups	Zarządzanie lokalnymi użytkownikami i grupami
Network	Zarządzanie urządzeniami sieciowymi
PowerShell	Interakcja z serwerem poprzez sesję PowerShell opartą na Web
Processes	Zarządzanie uruchomionymi procesami
Registry	Zdalne zarządzanie rejestrem
Remote Desktop	Połączenie z serwerem przy użyciu klienta pulpitu zdalnego opartego na Web
Roles and Features	Zarządzanie rolami i funkcjami serwera
Scheduled Tasks	Zarządzanie zadaniami zaplanowanymi
Services	Zarządzanie usługami
Storage	Zarządzanie urządzeniami pamięci masowej serwera
Storage Migration Service	Migrowanie serwerów plików do Azure lub Windows Server 2019
Storage Replica	Zarządzanie replikami magazynu
System Insights	Wyświetlanie danych analizy trendu dla wykorzystania procesora, dysków i sieci
Updates	Zarządzanie aktualizacjami oprogramowania
Virtual Machines	Zarządzanie maszynami wirtualnymi Hyper-V
Virtual Switches	Wyświetlanie i zarządzanie przełącznikami wirtualnymi

Windows Admin Center można również wykorzystać do zarządzania hybrydowymi usługami Azure, takimi jak Azure Backup, Azure Software Update, Azure Site Recovery, Azure Network Adapter i Azure Monitor. Więcej informacji na temat hybrydowych usług Azure dostępnych za pośrednictwem Windows Admin Center przedstawimy w rozdziale 17, „Azure IaaS i usługi hybrydowe”.

Windows Admin Center (WAC) stanowi dopełnienie – nie zaś pełny zamiennik – istniejących narzędzi RSAT. Może się wydawać, że intencją zespołu projektowego WAC było zreplikowanie wszystkich zadań, które można wykonać przy użyciu konsol obecnych w pakiecie Remote Server Administration Tools (RSAT). Jednak przy obecnym tempie – i biorąc pod uwagę konieczność objęcia przez WAC również dowolnych nowych funkcjonalności Windows Server – mało prawdopodobne jest, aby WAC mogło posłużyć jako pełny zamiennik narzędzi RSAT w dowolnym czasie przed kolejnym wydaniem Long Term Servicing Channel (LTSC) (którym może, choć nie musi być Windows Server 2022).

Od podszewki

Przyszłość to WAC

Patrząc w przyszłość, można się spodziewać, że graficzne zarządzanie nowymi funkcjami Windows Server będzie możliwe tylko za pośrednictwem WAC. Zanim jednak WAC ostatecznie zastąpi istniejące narzędzia GUI, takie jak konsole MMC i Server Management, będziemy mieli przejściowy okres kilku lat, w którym będziemy musieli używać zarówno WAC, jak i tradycyjnych konsoli, takich jak Active Directory Users and Computers oraz Active Directory Administrative Center, aby móc wykonać pewne zadania (gdyż żadne pojedyncze narzędzie obecnie nie pokrywa całej funkcjonalności). Ogólnie mówiąc, jeśli coś jest nowe w Windows Server 2019, zapewne będziemy to robić za pośrednictwem WAC albo PowerShell. Jeśli jest to coś, co wykonujemy już w Windows Server od jakiegoś czasu, istnieje spore prawdopodobieństwo, że będziemy mogli nadal używać oryginalnego przybornika narzędzi jeszcze przez kilka kolejnych lat.

Instalowanie Windows Admin Center

Konsolę Windows Admin Center (WAC) można zainstalować, pobierając ją z witryny firmy Microsoft. Dostępne są cztery opcje wdrożenia Windows Admin Center: lokalny klient, serwer bramy, zarządzany serwer oraz klaster pracy awaryjnej.

- **Lokalny klient** Po wybraniu tej opcji instalacyjnej instalujemy Windows Admin Center na swojej stacji roboczej. Z wystąpieniem WAC łączymy się lokalnie, co jest podobne do instalowania narzędzi RSAT na lokalnej stacji roboczej. Po lokalnym zainstalowaniu WAC na pulpicie umieszczany jest skrót do konsoli WAC.
- **Serwer bramy** Przy instalacji Windows Admin Center w konfiguracji serwera bramy instalacja następuje na komputerze systemu Windows Server 2016 lub Windows Server 2019, po czym wykonujemy zdalne połączenie z instancją WAC utrzymywaną na tym komputerze przy użyciu preferowanej przeglądarki. Po

połączeniu z instancją WAC można dodać serwery, którymi chcemy zarządzać. Podczas realizowania zadań administracyjnych instrukcje są wysyłane z serwera bramy i wykonywane przez docelowy serwer.

- **Zarządzany serwer** Wdrożenie zarządzanego serwera to wersja WAC dla konfiguracji bramy, ale umieszczona na węźle klastra w celu zarządzania tym klastrem.
- **Klaster pracy awaryjnej** Serwer bramy jest wdrażany jako usługa wysokiej dostępności. Wymaga to skonfigurowanie udostępnionego woluminu klastra (Cluster Shared Volume) do przechowywania trwałych danych używanych przez WAC. W witrynie firmy Microsoft dostępny jest skrypt, który upraszcza proces wdrażania w konfiguracji wysokiej dostępności.

Windows Admin Center występuje w dwóch wersjach. Istnieje wersja wstępna (*preview*), w której będziemy mieli do dyspozycji najświeższe aktualizacje funkcji, oraz wersja „szeroko walidowana”, która powinna być bardziej niezawodna (stabilna). W środowiskach produkcyjnych należy używać tylko wersji szeroko walidowanej; wersja wstępna jest przydatna w środowiskach eksperymentalnych lub testowych.

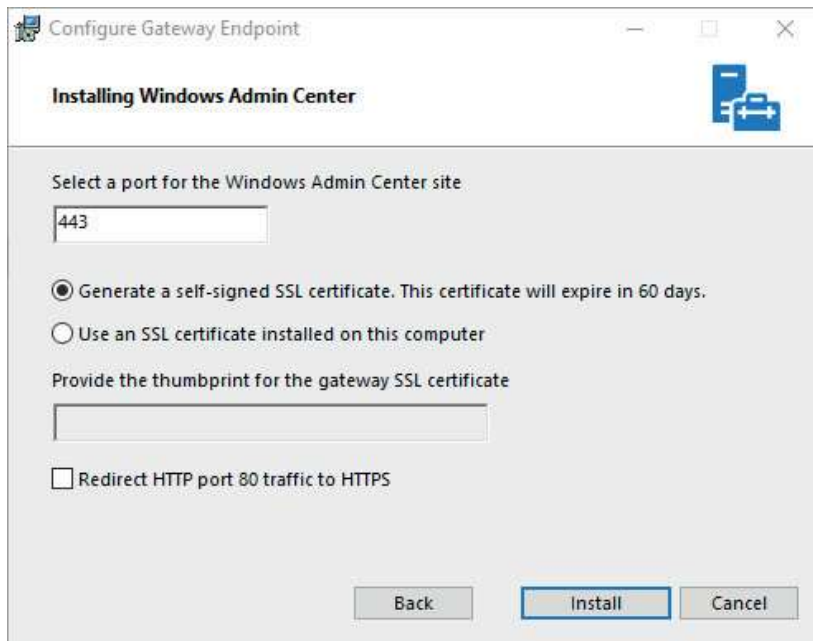
Domyślnie podczas instalacji WAC na komputerze Windows 10 usługa będzie dostępna na lokalnym porcie 6516. Zainstalowanie WAC w Windows 10 powoduje umieszczenie ikony WAC na pulpicie, stanowiącej skrót do lokalnej instancji WAC.

W przypadku instalacji na komputerze systemu Windows Server z opcją instalacji pulpitu graficznego mamy możliwość skonfigurowania portu, który będzie używany, co widać na rysunku. Dodatkowo można wybrać pomiędzy samo-podpisanym certyfikatem SSL (TLS) a certyfikatem, który jest już zainstalowany na tym komputerze. Jeśli wdrażamy serwer bramy, działania będą nieco prostsze, jeśli użyjemy certyfikatu TLS pochodzącego od zaufanego urzędu certyfikacji (CA), gdyż nie będzie potrzeby zatwierdzania zaufania do tego certyfikatu w całym mnóstwie okien dialogowych.

Instalację Windows Admin Center w wersji Server Core systemu Windows Server wykonujemy przy użyciu narzędzia `msiexec`, specyfikując port zarządzania oraz opcję certyfikatu SSL. (W istocie powinien być to certyfikat TLS, gdyż protokół SSL jest obecnie wygaszany). Składnia polecenia instalacyjnego z użyciem zaufanego certyfikatu jest następująca:

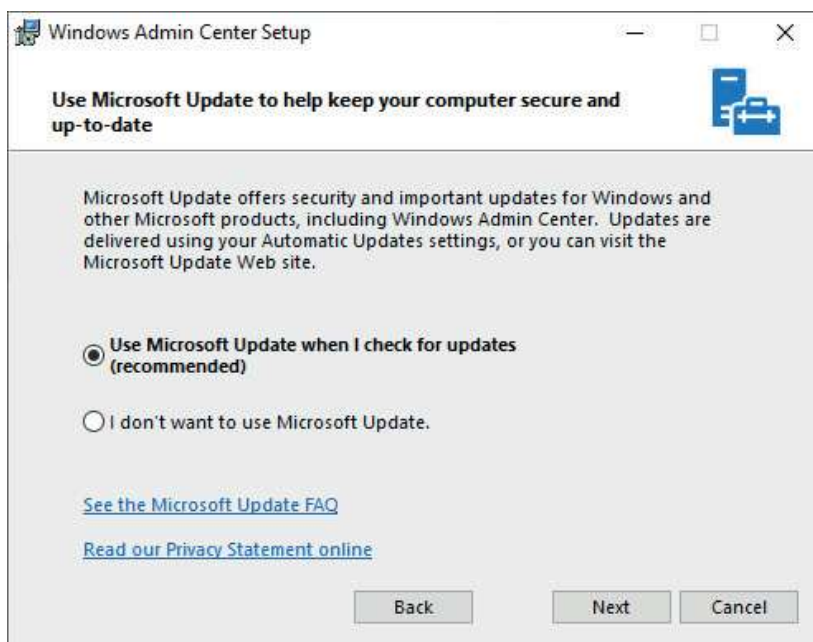
```
msiexec /i <WindowsAdminCenterInstallerName>.msi /qn /L*v log.txt  
SME_PORT=<port> SME_THUMBPRINT=<thumbprint> SSL_CERTIFICATE_OPTION=installed
```

Opcja `SME_PORT` wskazuje port, którego zamierzamy użyć, zaś `SME_THUMBPRINT` to odcisk palca zainstalowanego certyfikatu SSL (TLS).



RYSUNEK 1-3 Wybieranie portu Windows Admin Center

Domyślnie instalowanie WAC aktualizuje zaufane pliki komputera. Przy wdrażaniu WAC możemy je skonfigurować, aby aktualizowały się automatycznie lub ręcznie. W przypadku skonfigurowania automatycznego aktualizowania Windows Admin Center, jak na rysunku 1-4, nowe wersje będą instalowane, gdy staną się dostępne w usłudze Microsoft Update. Jeśli nie skonfigurujemy tej opcji, konieczne będzie ręczne instalowanie nowych wersji Windows Admin Center, gdy staną się dostępne.



RYSUNEK 1-4 Konfigurowanie aktualizacji Windows Admin Center

Dodatkowe informacje

Instalowanie Windows Admin Center

Więcej informacji na temat instalowania Windows Admin Center można znaleźć pod adresem <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/installation-options>.

Od podszewki

WAC Web Server

Windows Admin Center nie korzysta z Internet Information Services (IIS); zamiast tego używa swojego własnego serwera Web. Choć możliwe jest wdrożenie Windows Admin Center na komputerze z zainstalowanym IIS, w ogólności lepszym wyborem jest wdrożenie WAC w konfiguracji bramy i użycie serwera bramy do zdalnego zainstalowania komputera, który ma zainstalowany składnik IIS.

Rozszerzenia Windows Admin Center

Rozszerzenia Windows Admin Center pozwalają na rozbudowę funkcjonalności konsoli. Windows Admin Center zawiera rozszerzenia dla ról wbudowanych w Windows Server, takich jak Storage Migration Services, a także rozszerzenia innych firm. Microsoft zachęca innych dostawców oprogramowania, aby dodawali rozszerzenia do Windows Admin Center jako alternatywy dla wymagania od administratorów systemu, by używali konsol specyficznych dla produktu.

Domyślnie Windows Admin Center będzie prezentować rozszerzenia opublikowane w oficjalnym strumieniu NuGet firmy Microsoft. Strumień ten zawiera rozszerzenia opublikowane i zaktualizowane przez firmę Microsoft, a także te opublikowane przez zaufanych innych dostawców. Dodatkowo można skonfigurować konsolę Windows Admin Center, aby pokazywała rozszerzenia lub instalacje z dowolnego strumienia NuGet, który wspiera API NuGet V2 lub ze specjalnie skonfigurowanego sieciowego udziału plikowego dostępnego dla komputera utrzymującego Windows Admin Center.

Rozszerzenia są dostępne w Windows Admin Center po wybraniu ikony ustawień, a następnie wybraniu Extensions (Rozszerzenia). Panel Available Extension (dostępne rozszerzenia), pokazany na rysunku 1-5, wyświetla wszystkie rozszerzenia, które są dostępne, ale nie zostały jeszcze zainstalowane z aktualnie skonfigurowanego strumienia. Za pośrednictwem panelu Installed Extensions można zaktualizować aktualnie zainstalowane rozszerzenia, jeśli dostępne będą nowe ich wersje.

Dodatkowe informacje

Rozszerzenia WAC

Więcej informacji na temat rozszerzeń WAC można znaleźć pod adresem <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/using-extensions>.

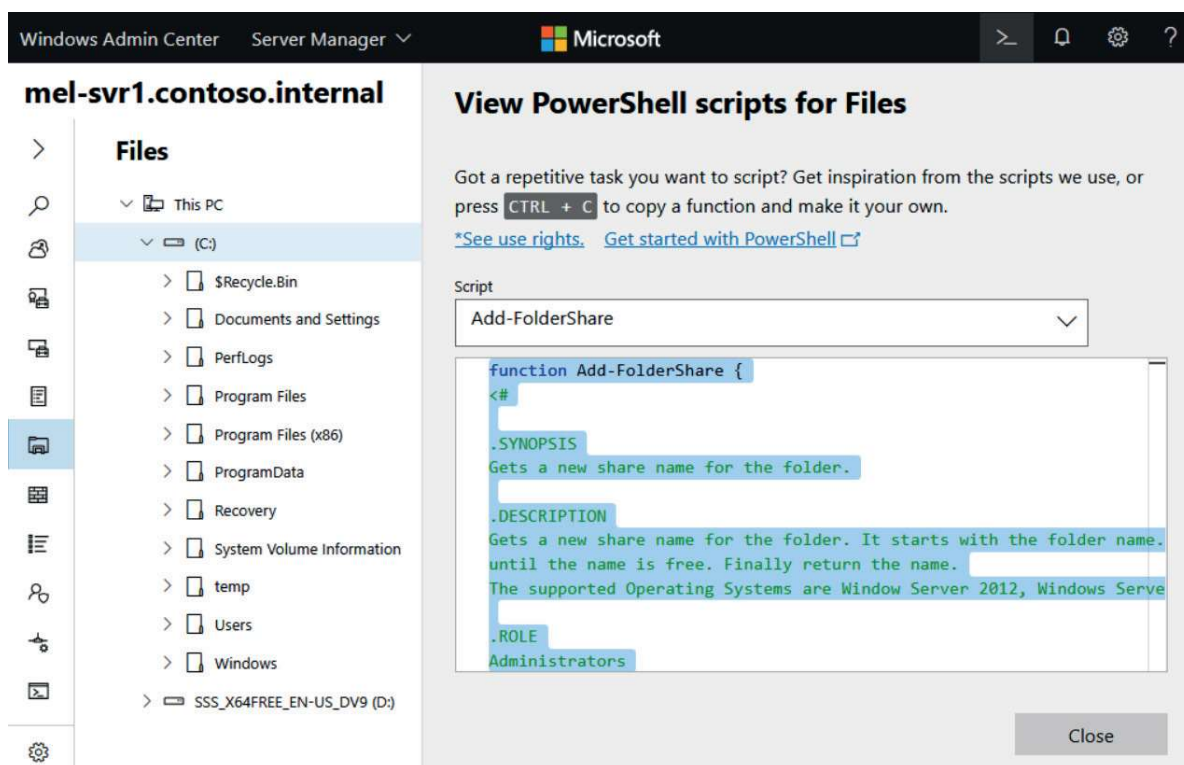
The screenshot shows the Windows Admin Center Settings page. The left sidebar contains navigation options: User (Account, Personalization, Language / Region, Suggestions, Advanced) and Gateway (Extensions, Azure, Access, Shared Connections). The main content area is titled 'Extensions' and includes a warning: 'We might have to restart the Windows Admin Center gateway after installing an extension, temporarily affecting availability for anyone else currently using this gateway.' Below the warning are tabs for 'Available extensions', 'Installed extensions', and 'Feeds'. The 'Available extensions' tab is active, showing a list of 22 items. A search box is present above the list. The list contains the following items:

Name ↑	Version	Created by	Package	Status
Active Directory (Preview)	0.63.0	Microsoft	Windo...	Available
BitOps Changes	1.0.12	BitOps	Windo...	Available
Configuration Manager Client (Preview)	1.0.0	Ken Wygant (...)	Windo...	Available
Containers	1.33.0	Microsoft	Windo...	Available
DataON MUST Visibility, Monitoring, and Man...	2.3.0	DataON	Windo...	Available
Dell EMC OpenManage Integration	1.0.0	Dell EMC	Windo...	Available
DHCP (Preview)	0.9.3	Microsoft	Windo...	Available
DNS (Preview)	0.9.5	Microsoft	Windo...	Available

RYSUNEK 1-5 Rozszerzenia Windows Admin Center

Pokazywanie skryptu

Ilekcroć wykonujemy jakieś zadanie w konsoli Windows Admin Center, możemy kliknąć ikonę PowerShell w pasku tytułu konsoli, aby wyświetlić kod źródłowy PowerShell odpowiadający temu zadaniu, co pokazuje rysunek 1-6. Pozwala to na skopiowanie i zapisanie przydatnego kodu PowerShell do ponownego użycia w późniejszym terminie.



RYSUNEK 1-6 Pokazywanie skryptu

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 2019. Konsolle RSAT można również zainstalować na komputerze z Windows Server 2019. Jeśli chcemy zainstalować wszystkie dostępne konsolle 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.

Prostsza metoda instalowania narzędzi RSAT w systemie Windows 10 wymaga wykonania poniższego polecenia w wierszu poleceń o podniesionych uprawnieniach – pod warunkiem, że zainstalowaliśmy Chocolatey:

```
choco install -y rsat
```

Chocolatey jest niezależnym menedżerem pakietów dla systemów operacyjnych Windows. Więcej informacji na temat tego (i innych) narzędzi zawiera rozdział 3, „Wdrożenie i konfiguracja”.

Od podszewki

Windows 10 dla Windows Server 2019

Podczas gdy narzędzia RSAT dla Windows 10 umożliwiają zarządzanie systemami Windows Server od wersji 2008 R2 w górę, ich zainstalowanie w systemie Windows 8.1 pozwala na zarządzanie wyłącznie serwerami pracującymi pod kontrolą systemów Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 i Windows Server 2008, ale nie Windows Server 2016 i późniejszych. Podobnie jest z narzędziami RSAT dla Windows 7, które umożliwiają zarządzanie systemami Windows Server 2008 R2 i Windows Server 2008, ale nie nowszych. Krótko mówiąc, jedynie najnowsza wersja klienckiego systemu operacyjnego Windows obsługuje wersję narzędzi SAT pozwalających na zarządzanie najnowszą wersją systemu operacyjnego Windows Server.

Konsole RSAT

Tabela 1-2 zawiera listę narzędzi RSAT, jakie dostępne są w systemie Windows Server 2019. Większość z tych narzędzi dostępnych jest z poziomu menu Tools (Narzędzia) w konsoli Server Manager.

TABELA 1-2 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

TABELA 1-2 Konsole RSAT

Konsola	Funkcja
Active Directory Sites and Services	Zarządzanie konfiguracją lokacji Active Directory, wliczając w to serwery wykazu globalnego oraz buforowanie członkostwa grup uniwersalnych
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

TABELA 1-2 Konsole RSAT

Konsola	Funkcja
Internet Information Services (IIS) Manager	Konfigurowanie i zarządzanie serwerem IIS w wersji 7 i nowszymi
iSCSI Initiator	Konfigurowanie ustawień inicjatora iSCSI
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 Services	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

TABELA 1-2 Konsole RSAT

Konsola	Funkcja
Windows Firewall with Advanced Security	Konfigurowanie i zarządzanie zaporą systemu Windows z zabezpieczeniami zaawansowanymi
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 2019 zainstalowaliśmy w ramach opcji Server with Desktop Experience (Środowisko pulpitu), wówczas na takim komputerze konsola ta uruchamiać się będzie automatycznie. Dodatkowo automatycznie będzie zachęcać do wypróbowania Windows Admin Center, udostępniając łącze do pobrania tego narzędzia.

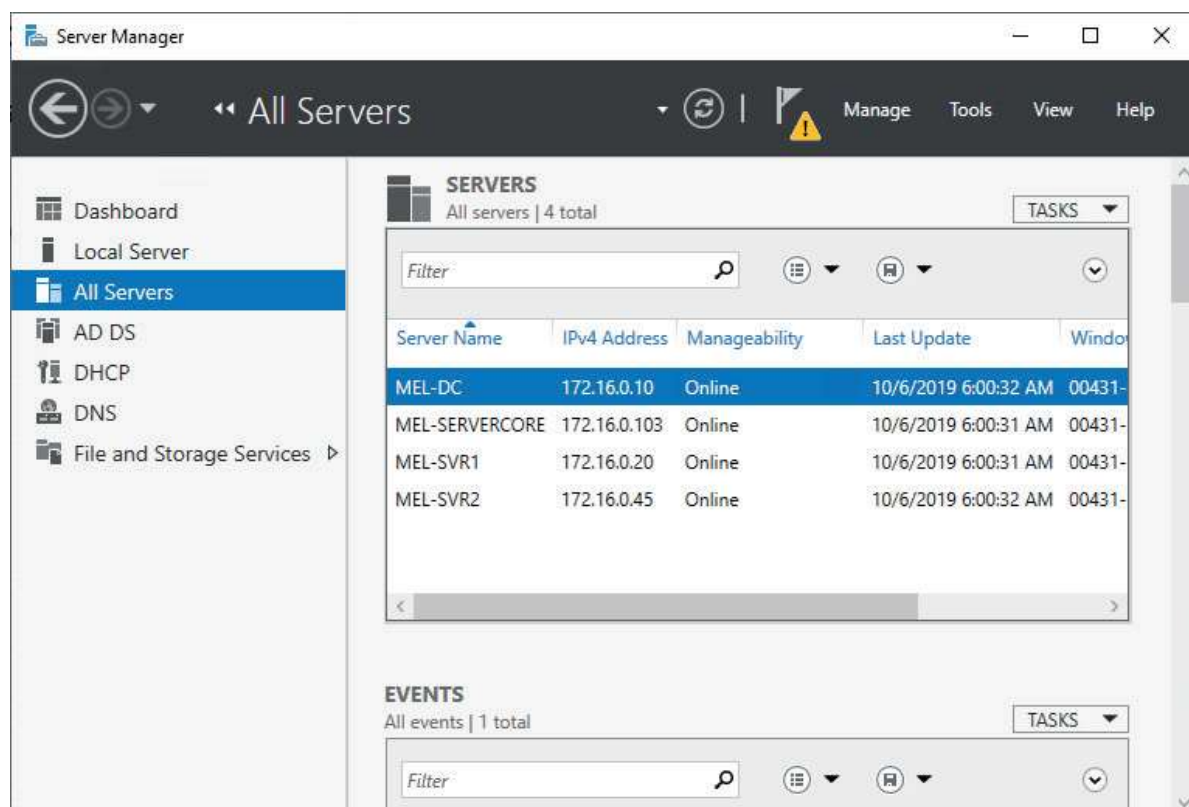
Wiele ról, dla których w poprzednich wersjach Windows Server istniały oddzielne konsole, zostały zintegrowane w konwoli Server Manager. Przykładem są zadania zarządzania magazynem oraz zadania usługi IPAM, które dotychczas wymagały użycia kilku indywidualnych konsol, a które można teraz ukończyć z poziomu konsoli Server Manager.

Od podszewki

Server Manager i Windows Admin Center

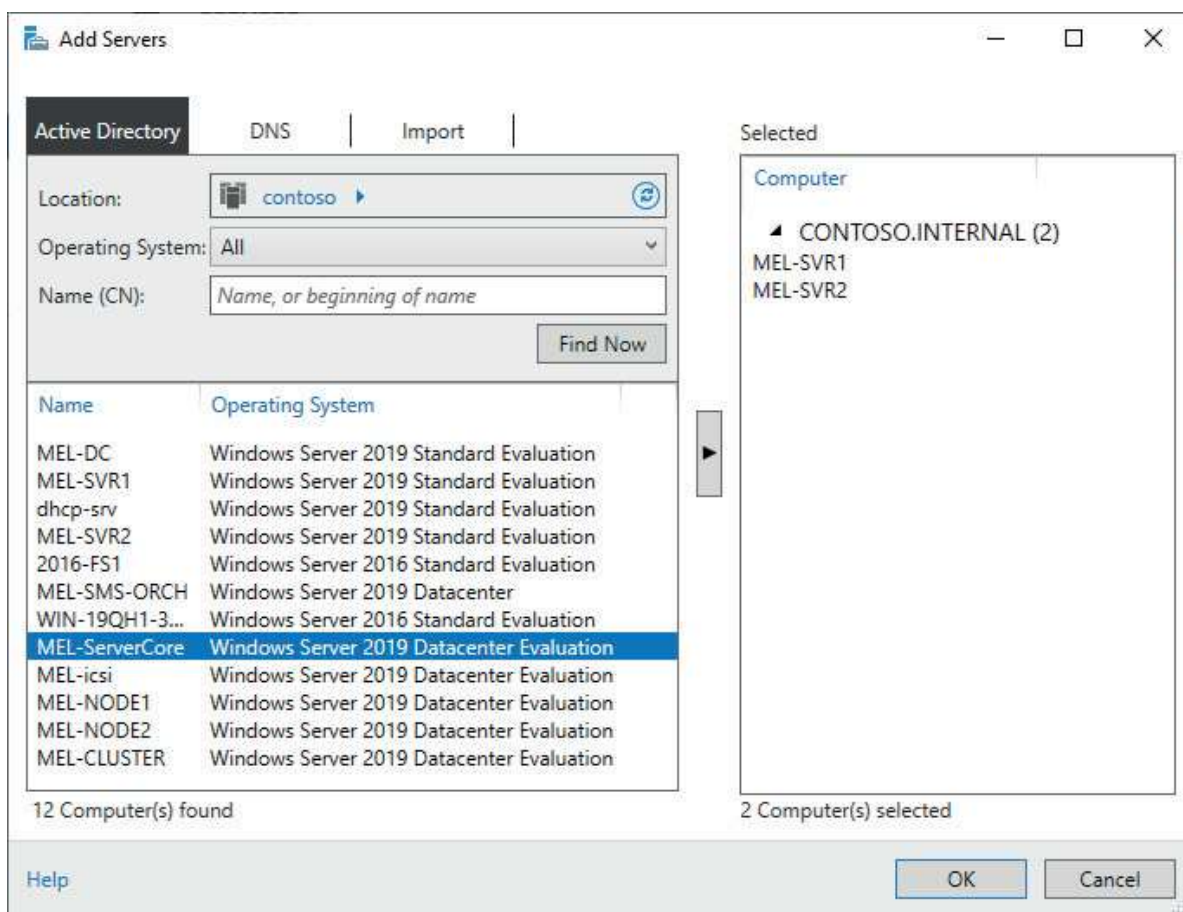
Gdy opublikowano Windows Server 2016, nowe funkcjonalności w trybie graficznym były eksponowane raczej przez Server Manager, a nie przez nowe konsole MMC. Wraz z udostępnieniem narzędzia Windows Admin Center nie będziemy już obserwować nowych funkcjonalności w konsoli Server Manager. Może się okazać, że Windows Admin Center zastąpi funkcjonalność narzędzia Server Manager, zanim zespół WAC zdoła zreplikować wszystkie funkcje starszych konsol MMC, takich jak Active Directory Users and Computers (ADUC).

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 przygotowuje i wyświetli ona odpowiednią listę kategorii. Rysunek 1-7 pokazuje grupę All Servers złożoną z serwerów MEL-DC, MEL-SERVERCORE, MEL-SVR1 i MEL-SVR2. Na serwerach tych wykryte zostały role serwera AD CS, DHCP i DNS.



RYSUNEK 1-7 Lista All Servers

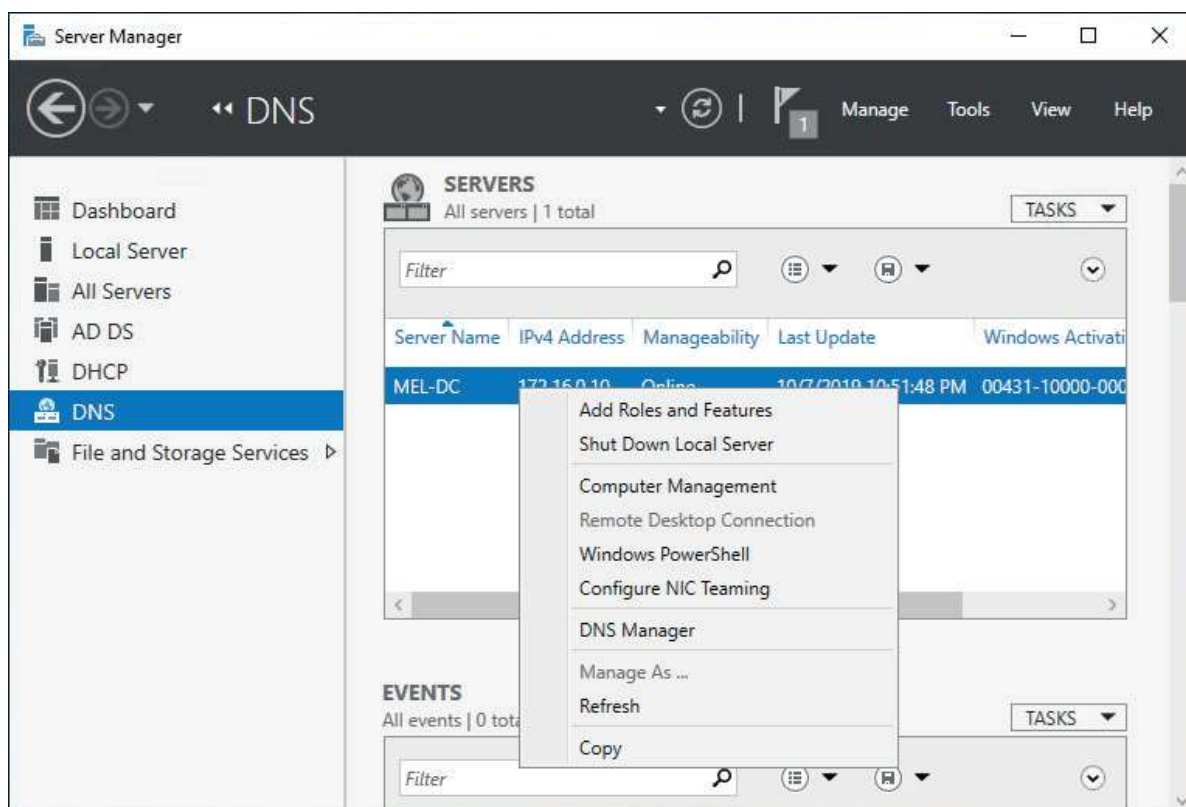
Aby dodać serwery do grupy All Servers, należy w konsoli Server Manager kliknąć prawym przyciskiem węzeł All Servers i wybrać opcję Add Servers (Dodaj serwery). W oknie dialogowym Add Servers (Dodawanie serwerów), widocznym na rysunku 1-8, wybieramy docelowe serwery, przy czym możemy to zrobić na trzy sposoby: poprzez odpytanie katalogu Active Directory, wyszukanie ich po nazwie DNS lub przez zaimportowanie tych serwerów z listy.



RYSUNEK 1-8 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 1-9 pokazuje przykład, w którym dla serwera MEL-DC na liście serwerów z rolą DNS wybierana jest opcja pozwalająca na uruchomienie konsoli DNS Manager (Menedżer DNS). 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



RYSUNEK 1-9 Menu kontekstowe indywidualnego serwera w konsoli Server Manager

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. Pomoc dla każdego polecenia można uzyskać, wpisując **help <cmdletname>**. Na przykład by uzyskać pomoc na temat polecenia cmdlet **get-service**, należy wpisać **help get-service** w sesji PowerShell.

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.

Niektóre kluczowe polecenia pozwalające rozpocząć pracę z programem PowerShell zebrane zostały w tabeli 1-3.

TABELA 1-3 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
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 systemach Windows Server 2016 i 2019 dowolny zainstalowany moduł zostanie automatycznie załadowany przy próbie wykonania któregoś 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. Tabela 1-4 zawiera polecenia, które ułatwią nam rozpoczęcie pracy z galerią PowerShell.

TABELA 1-4 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 2019 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 zbliżony do wykonywania poleceń w ramach sesji SSH.

Za pomocą poniższego polecenia będziemy mogli połączyć się w ramach sesji zdalnej z komputerem Windows Server 2019, który jest członkiem tego samego lasu Active Directory. Polecenie to prosi o podanie poświadczeń, za pomocą których będziemy mogli podłączyć się do zdalnej maszyny, jak na rysunku 1-10.

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



RYСУNEK 1-10 Podawanie poświadczeń

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 19, „Wzmacnianie zabezpieczeń Windows Server i Active Directory”, 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 obsłudze 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 wuauaserv } -computername $Computers
```

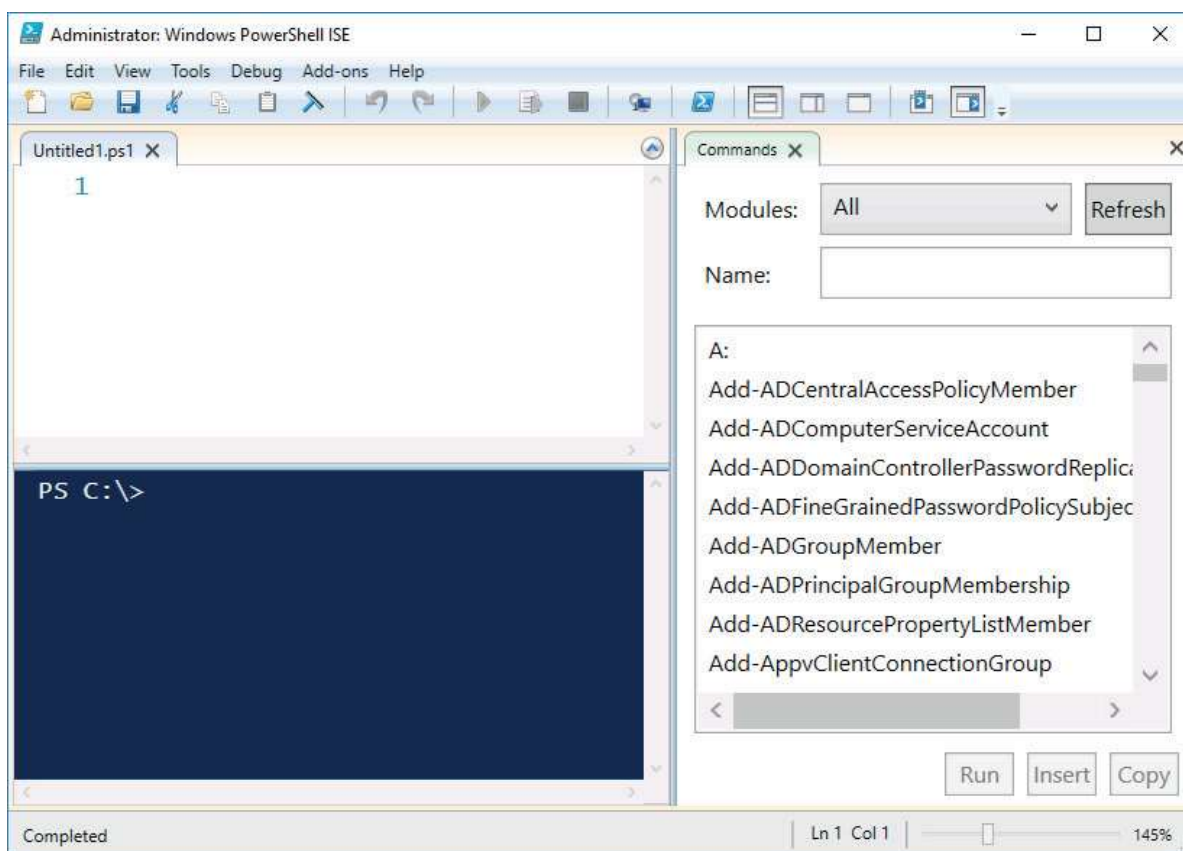
Możemy również wykorzystać polecenie **Invoke-Command** do wykonania skryptu z lokalnego komputera na dowolnej liczbie komputerów zdalnych. Przykładowo, w celu wykonania skryptu `FixStuff.ps1` na komputerach wskazanych w pliku `computers.txt` możemy wykonać poniższe polecenie:

```
$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 2019, 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 1-11.



RYSUNEK 1-11 PowerShell ISE

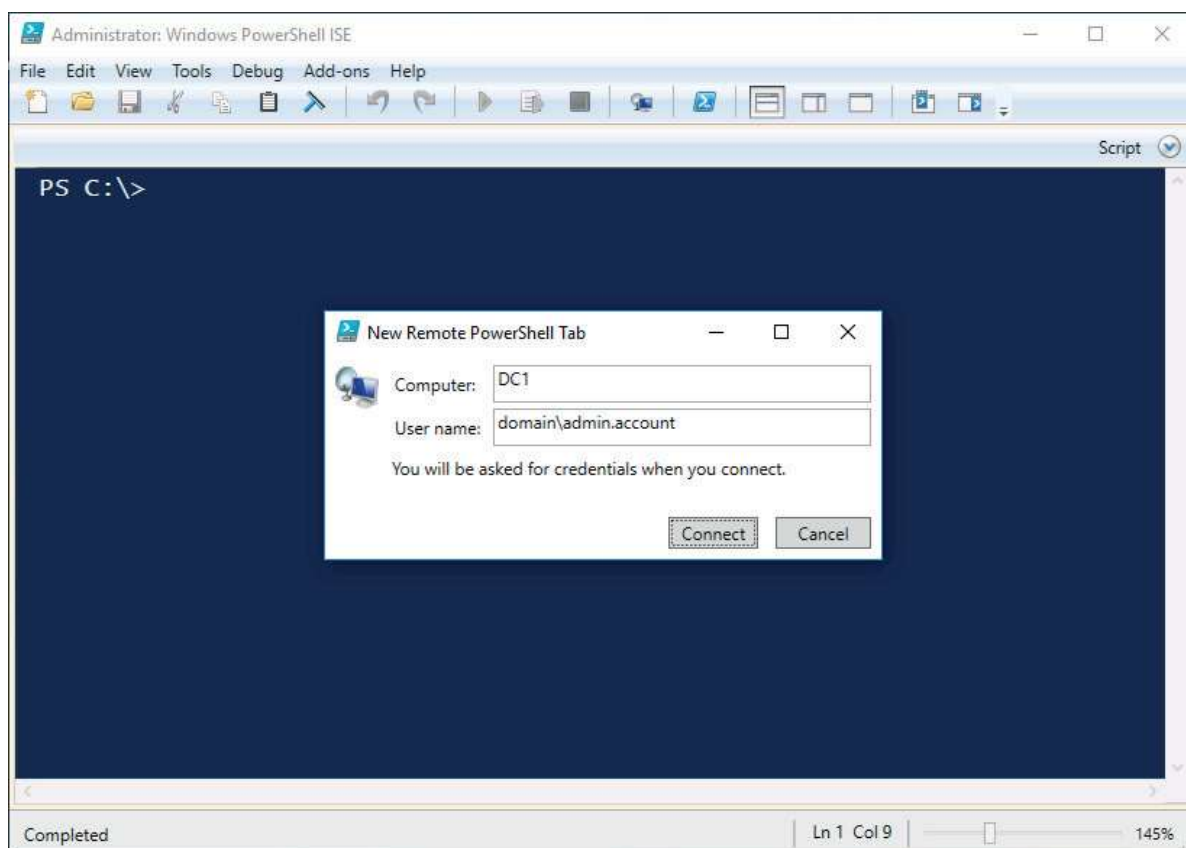
PowerShell ISE oferuje następującą funkcjonalność:

- **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 1-12.

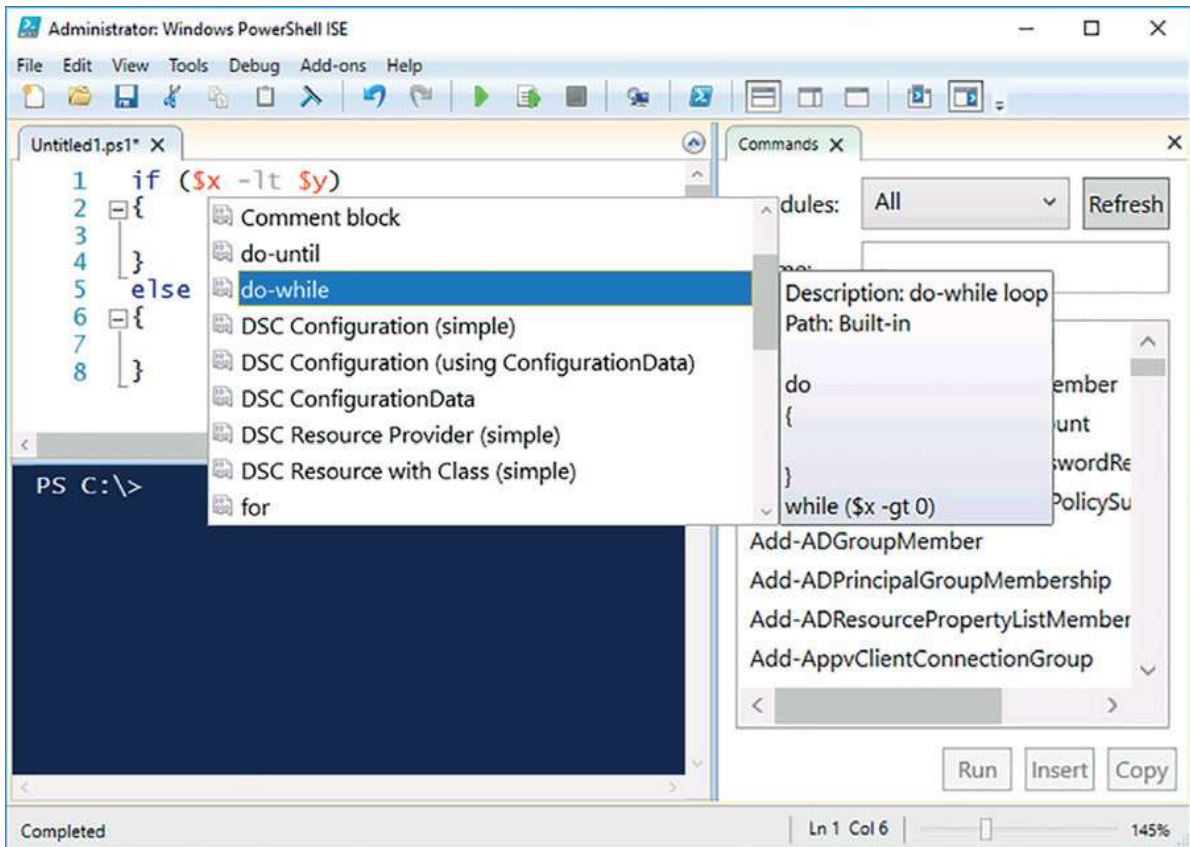


RYСУNEK 1-12 Nowa karta zdalna w programie PowerShell ISE

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 1-13 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 1-13 Wstawki kodu

Od podszewki

VSCode

Podobnie jak konsola Server Manager, PowerShell ISE jest już dinozaurem w porównaniu do nowszych opcji, które można pobrać z witryny firmy Microsoft. Visual Studio Code (VSCode) jest bezpłatnym środowiskiem programistycznym (Integrated Development Environment – IDE), wyposażonym w rozszerzenia, które ogromnie wspomagają tworzenie i debugowanie skryptów PowerShell. Podobnie jak Windows Admin Center, VSCode podlega bardzo szybkim cyklom aktualizacji, co jest jednym z powodów, dla których narzędzie to nie jest dołączone do instalacji systemu operacyjnego. Mówiąc ogólnie, należy tworzyć swoje skrypty PowerShell na stacji roboczej przy użyciu takiego narzędzia, jak VSCode z jego wszystkimi doskonałymi rozszerzeniami. Jeśli konieczne jest debugowanie skryptu PowerShell na serwerze, na którym ten skrypt jest uruchamiany, należy użyć PowerShell ISE.

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 2019 albo 2016 oraz 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`.

Aby utworzyć bezpośrednie połączenie z hosta Hyper-V do komputera działającego pod kontrolą obsługiwaną wersję systemu Linux, trzeba upewnić się, że zainstalowane są rozszerzenia wirtualizacji właściwe dla danej dystrybucji oraz serwer SSH. Po wykonaniu tych kroków można użyć polecenia `hvc.exe` w celu nawiązania połączenia. Na przykład poniższe polecenie pozwala utworzyć połączenie SSH do maszyny wirtualnej *Ubuntu-Server* i konta użytkownika *prime* z okna poleceń PowerShell o podniesionych uprawnieniach na hoście wirtualizacji:

```
Hvc.exe ssh prime@ubuntu-server -v
```

Pulpit zdalny

Wielu administratorów decyduje się wykonywać zdalnie pojedyncze zadania na serwerach działających pod kontrolą systemu Windows Server 2019 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 i 2019, pracującymi w ramach infrastruktury IaaS platformy Azure, gdy maszyny te wdrażane są z poziomu galerii PowerShell. Więcej na temat uruchamiania systemu Windows Server 2019 na platformie Azure dowiesz się w rozdziale 17, „Azure IaaS i usługi hybrydowe”.

Pulpit zdalny na komputerach z systemem Windows Server 2019 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
```

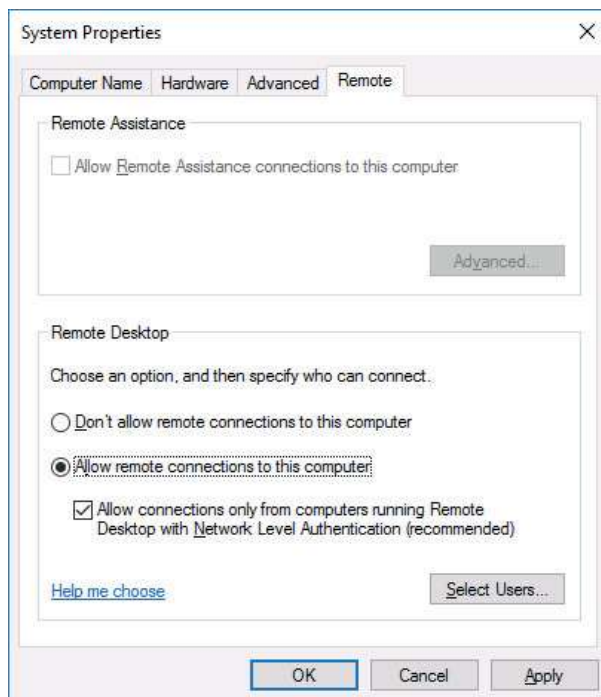
Jeśli tylko funkcja Remote Desktop została na tych komputerach włączona, połączenia pulpitu zdalnego możemy nawiązywać także z komputerami z systemem zainstalowanym w trybie Server Core.

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 1-14. 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 1-14 Karta Remote w oknie właściwości systemu

Od podszewki

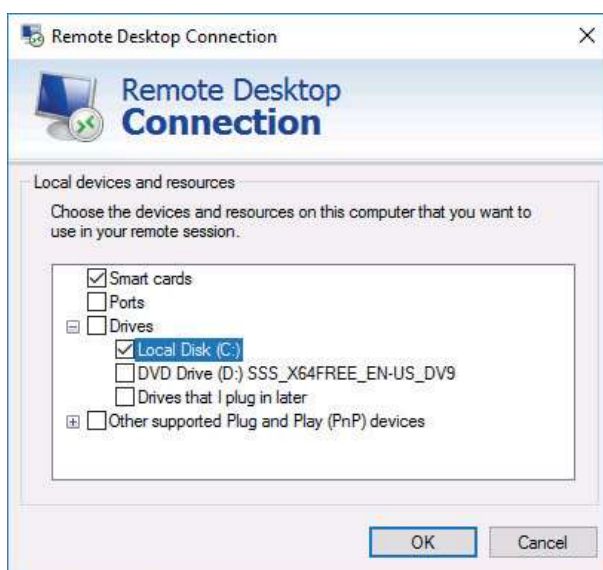
Just Enough Administration

Funkcja *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 dowiemy się w rozdziale 19, „Wzmacnianie zabezpieczeń Windows Server i Active Directory”.

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.

Poprzez skonfigurowanie widocznego na rysunku 1-15 ustawienia Local Devices and Resources (Lokalne urządzenia i zasoby) na karcie Local Resources (Zasoby lokalne) okna dialogowego Remote Desktop Connection możemy zmapować na zdalnym gości 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 1-15 Ustawienia Local Resources and Devices

SSH

Windows Server 2019 i najnowsze wersje Windows 10 zawierają możliwość zainstalowania zarówno klienta, jak i serwera SSH. Pomimo tego, że PowerShell obecnie działa również w systemach operacyjnych Linux i Mac OS, wielu administratorów hybrydowych środowisk preferuje korzystanie z SSH przy wykonywaniu zdalnych połączeń administracyjnych z użyciem interfejsów wiersza poleceń.

Aby dodać klienta i serwer SSH do systemu Windows Server 2019, należy użyć następujących poleceń PowerShell:

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Pomimo tego, że w poleceniach tych pojawia się wersja 0.0.1.0, zainstalowana zostanie najnowsza obsługiwana wersja. Wersję zainstalowanych narzędzi SSH można sprawdzić przy użyciu polecenia `SSH -v`.

Po dodaniu tej funkcjonalności musimy wykonać jeszcze kilka rzeczy, aby uzyskać działający serwer SSH. Jeśli planujemy korzystać z uwierzytelniania opartego na kluczach, a nie hasłach, trzeba również uruchomić poniższe polecenie, aby zainstalować moduł PowerShell dla OpenSSH, który zawiera narzędzia pomocne w konfigurowaniu tej funkcjonalności:

```
Install-Module -Force OpenSSHUtils -Scope AllUsers
```

Po wykonaniu tych poleceń trzeba skonfigurować domyślnie wyłączoną usługę `ssh-agent` na automatyczne uruchamianie, podobnie jak usługę `sshd`. Można to uzyskać, wykonując poniższe polecenia PowerShell commands:

```
Set-Service -Name ssh-agent -StartupType 'Automatic'  
Set-Service -Name sshd -StartupType 'Automatic'
```

Końcowym krokiem prowadzącym do uzyskania SSH działającego w systemie Windows Server 2019 jest uruchomienie poniższych poleceń w celu uruchomienia odpowiednich usług:

```
Start-Service ssh-agent  
Start-Service sshd
```

Po wykonaniu tych wszystkich zadań możemy połączyć się przy użyciu uwierzytelnienia opartego na hasłach z klienta SSH, używając poniższej składni:

```
ssh username@hostname_or_IP_address
```

W przypadku korzystania z konta domenowego, należy użyć następującego formatu:

```
ssh username@domain@hostname_or_IP_address
```

Ogromna większość osób korzystających z SSH preferuje stosowanie uwierzytelniania opartego na kluczach, a nie na hasłach. Aby uzyskać działające uwierzytelnianie tego typu w serwerze SSH w systemie Windows Server 2019, trzeba wykonać pewne dodatkowe kroki. Po stronie klienta trzeba przejść do katalogu `.ssh` i uruchomić w nim polecenie `ssh-keygen`, akceptując domyślne parametry. W ten sposób utworzymy prywatny i publiczny klucz. Klucz prywatny znajdzie się w pliku `id_rsa`, zaś klucz publiczny w pliku `id_rsa.pub`.

Kolejną rzeczą, którą trzeba zrobić, jest dodanie klucza prywatnego do naszego kontekstu zabezpieczeń Windows. Można to wykonać poprzez uruchomienie następujących trzech poleceń:

```
Set-Service ssh-agent -StartupType 'Automatic'  
Start-service ssh-agent  
Ssh-add ~\.ssh\id_rsa
```

Po wykonaniu tych czynności trzeba zainstalować klucz publiczny na serwerze Windows Server 2019, na którym chcemy korzystać z uwierzytelniania SSH opartego na kluczach. W tym celu wykonujemy poniższe kroki (gdzie `chancellor` trzeba zastąpić nazwą użytkownika, dla którego konfigurujemy uwierzytelnianie i podać adres IP konfigurowanego przez nas serwera):

```
Ssh chancellor@172.16.0.15 mkdir c:\users\chancellor\.ssh\  
Scp c:\users\chancellor\.ssh\id_rsa.pub chancellor@172.16.0.15:C:\Users\  
Administrator\.ssh\authorized_keys
```

Aby skonfigurować niektóre uprawnienia pliku autoryzowanych kluczy, trzeba wykonać poniższe polecenie PowerShell zlokalizowane we wspomnianym wcześniej module `OpenSSHUtils`. Możemy nawet użyć SSH z uwierzytelnieniem hasła, aby to wykonać:

```
Repair-AuthorizedKeyPermission C:\users\Chancellor\.ssh\authorized_keys
```

Ponieważ ten cmdlet PowerShell nie do końca działa zgodnie z oczekiwaniem, trzeba jeszcze wykonać polecenie `Icacls authorized_keys /remove "NT SERVICE\sshd"`, gdyż usługa "NT SERVICE\sshd" nie powinna mieć żadnych uprawnień do pliku `authorized_keys` (gdyby je miała, uwierzytelnianie oparte na kluczach nie będzie działać).

Finalnym wymaganym krokiem jest przeedytowanie pliku `C:\ProgramData\ssh\sshd_config` i wykomentowanie poniższych wierszy (można je znaleźć na końcu pliku):

```
# Match Group administrators  
#     AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Konieczne może być wykonanie tej operacji lokalnie na komputerze Windows Server 2019. Gdy już to zrobimy, należy zrestartować usługę `sshd` przy użyciu polecenia PowerShell `restart-service sshd`. Następnie będziemy mogli łączyć się z serwerem z naszego komputera klienckiego przy użyciu uwierzytelniania opartego na kluczach.

Dodatkowe informacje

OpenSSH w Windows Server

Więcej informacji na temat OpenSSH w Windows Server dostępnych jest pod adresem https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_server_configuration.



Edycje Windows Server 2019.....	33	Serwer z interfejsem graficznym.....	47
Kanały obsługi Windows Server	35	Role i funkcje	47
Server Core.....	38		

P przed zainstalowaniem systemu Windows Server 2019 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), czy też w wersji Server Core. Musimy też określić, czy chcemy wdrożyć wersję Windows Server należącą do Long Term Servicing Channel (kanału długoterminowej obsługi), czy do Semi Annual Channel (kanału półrocznego). W tym rozdziale zapoznamy się z różnymi edycjami systemu Windows Server 2019.

Edycje Windows Server 2019

Istnieją dwie główne oraz kilka pomniejszych edycji systemu Windows Server 2019. Do edycji głównych zaliczamy:

- **Windows Server 2019 Standard** Edycja systemu Windows Server 2019 przeznaczona dla środowisk, w których większość serwerów wdrażana jest fizycznie, a nie 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 2019 Datacenter** Ta edycja systemu Windows Server 2019 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 2019 należą:

- **Windows Server 2019 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.

- **Microsoft Hyper-V Server 2019** 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 2019.

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 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
Wystąpienia Storage Replica	2	Nielimitowane
Wliczone licencje dla kontenerów Hyper-V	2	Nielimitowane

Dla większości organizacji podstawową różnicą pomiędzy tymi dwoma systemami jest sposób licencjonowania na nich maszyn wirtualnych. Edycja Datacenter pozwala nam na hostowanie nieograniczonej liczby maszyn wirtualnych. Natomiast 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 2019 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 dziedziczną aktywację zarówno jako host, jak i maszyna wirtualna gościa. Edycja Standard wspiera aktywację dziedziczną tylko wtedy, gdy hostowana jest na maszynie wirtualnej gościa na hoście Hyper-V, który działa pod kontrolą systemu w edycji Datacenter. Aktywacja dziedziczna polega na tym, że aktywacja dokonywana jest automatycznie na podstawie edycji systemu Windows Server. W przypadku hostowania dużej liczby maszyn wirtualnych Windows Server 2019 pozwala to zaoszczędzić sporo czasu, jako że nie musimy w tym celu wykorzystywać kluczy licencyjnych ani serwerów KMS.

Kanały obsługi Windows Server

W zależności od wybranej przez nas opcji instalacji Windows Server 2019 wspierał będzie jeden z dwóch oddzielnych kanałów obsługi: długoterminowy Long Term Servicing Channel (LTSC – kanał o obsłudze długoterminowej) oraz bieżący Semi Annual Channel (SAC – kanał półroczny). Wymagają one oddzielnych nośników instalacji i nie jest możliwe zainstalowanie wydania SAC z nośnika LTSC ani odwrotnie.

LTSC

Wersje LTSC to wydania Windows Server, które można uznać za główne wersje systemu. Windows Server 2016 i Windows Server 2019 są wersjami LTSC, przy czym kolejna wersja LTSC zapewne otrzyma nazwę Windows Server 2021 albo Windows Server 2022. Wersje LTSC mogą być instalowane albo jako serwer ze środowiskiem pulpitu, albo w konfiguracji Server Core.

Kanał LTSC 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 LTSC przez co najmniej 10 lat. W przypadku wydania systemu Windows Server 2019 oznacza to, że rozszerzone wsparcie zakończy się 9 stycznia 2029 roku. Obecnie firma Microsoft oferuje dodatkowe trzy lata rozszerzonych aktualizacji zabezpieczeń dla klientów, którzy gotowi są płacić roczne opłaty za wsparcie

dla Windows Server 2008 i Windows Server 2008 R2, których standardowe wsparcie zakończyło się w styczniu 2020 roku. Coś podobnego może być również dostępne dla Windows Server 2019 w celu rozszerzenia dostępności aktualizacji zabezpieczeń poza rok 2029, ale są to czyste spekulacje.

LTSC jest jedynym kanałem obsługi, który jest dostępny dla serwerów zainstalowanych w ramach opcji instalacji Server with Desktop Experience (z graficznym środowiskiem pulpitu).

Semi Annual Channel

Wydania SAC są dostępne tylko jako instalacje Server Core i są w ogólności udostępniane dwa razy do roku. Wydania SAC nazywane są rokiem i miesiącem wydania. Na przykład wersja Windows Server 1809 została opublikowana we wrześniu roku 2018, a Windows Server 1903 w marcu 2019. Mogłoby się nawet pojawić wydanie SAC Windows Server 2003 (z marca 2020) albo Windows Server 2008 (z sierpnia 2020), co mogłoby być mylące dla osób, które nie rozumieją nowego schematu nazewnictwa i mogłyby przypuszczać, że firma Microsoft ponownie wydaje „klasyków”.

Wydania SAC zawierają nowe funkcje i możliwości opracowane od czasu ostatniego wydania LTSC, a także funkcje i możliwości, które były dostępne w tej najświeższej wersji LTSC. Zasadniczo wydanie SAC Windows Server 1903 to wersja Server Core systemu Windows Server 2019 z pewnymi nowymi funkcjami i możliwościami, ale która będzie wspierana przez firmę Microsoft tylko przez 18 miesięcy, a nie zwyczajowe 10.

Wydania SAC są odpowiednie dla organizacji, które mają zautomatyzowane potoki wdrażania systemów operacyjnych i które czują się dobrze, traktując serwery jak „zwierzęta hodowlane”, a nie „domowych pupilów”. W teorii, jeśli nasza organizacja używa wydań SAC, czuje się wygodnie przy 18-miesięcznym oknie wsparcia, gdyż ma wdrożoną dostateczną automatyzację, aby istniejące wystąpienia Windows Server były samoczynnie zastępowane za każdym razem, gdy zostanie opublikowane kolejne wydanie SAC. Jeśli pracujemy dla organizacji, która nadal ma w swojej sieci komputery systemu Windows Server 2003, zapewne zechcemy dać przepustkę wydaniom SAC Windows Server.

W większości przypadków funkcje i możliwości, które pojawiają się w wydaniach SAC, zostaną zintegrowane w kolejnym wydaniu LTSC. Niekiedy funkcje z wydań SAC nie będą częścią kolejnego wydania LTSC, ale będzie tak dlatego, że nie będą jeszcze naprawdę gotowe na wprowadzenie do wersji systemu operacyjnego, która ma być wspierana przez całą dekadę. Niekiedy nowe funkcje będą dołączane również do wydań LTSC; przykładem może być mechanizm migracji Samba w Storage Migration Services, który został dołączony do aktualizacji zbiorczej z sierpnia 2019, ale jest to raczej wyjątek, niż reguła.

Dodatkowe informacje

Kanały obsługi

Więcej informacji na temat kanałów obsługi Windows Server można znaleźć pod adresem <https://docs.microsoft.com/en-us/windows-server/get-started-19/servicing-channels-19>.

Kompilacje Insider Preview

Wewnętrzne kompilacje wstępne (Insider Preview) Windows Server to wersje oprogramowania podobne do znanych wcześniej wersji Release Candidate (kandydat na wydanie) albo Beta. Kompilacje Insider Preview przeznaczone są tylko do użytku testowego i nie powinny być wykorzystywane w środowiskach produkcyjnych. Nowe funkcje pojawiają się w tych wersjach, zanim zostaną włączone do wydań SAC. Funkcje, które pojawiają się w wydaniach SAC, zazwyczaj później pojawiają się w wydaniach LTSC.

W przeciwieństwie to wydań SAC, to, czy kompilacja wstępna zawiera środowisko graficzne, zależy od samej wersji wstępnej. Przed wydaniem kolejnej kompilacji LTSC z pewnością będą dostępne kompilacje Insider Preview, które zawierają opcję instalacji środowiska graficznego. Tym samym kompilacja Insider Preview systemu Windows Server 2021/2022 pozwoli na wdrożenie serwera ze środowiskiem pulpitu, ale hipotetyczna kompilacja wstępna wydania SAC Windows Server 2203 – nie.

Od podszewki

Na własne ryzyko

Kompilacje Insider Preview zasadniczo są ofertą typu „używaj na własną odpowiedzialność”. Niektóre z nich mogą działać doskonale, ale inne mogą być mniej wiarygodne, niż obietnica nastolatka, że pozmywa po obiedzie.

Dodatkowe informacje

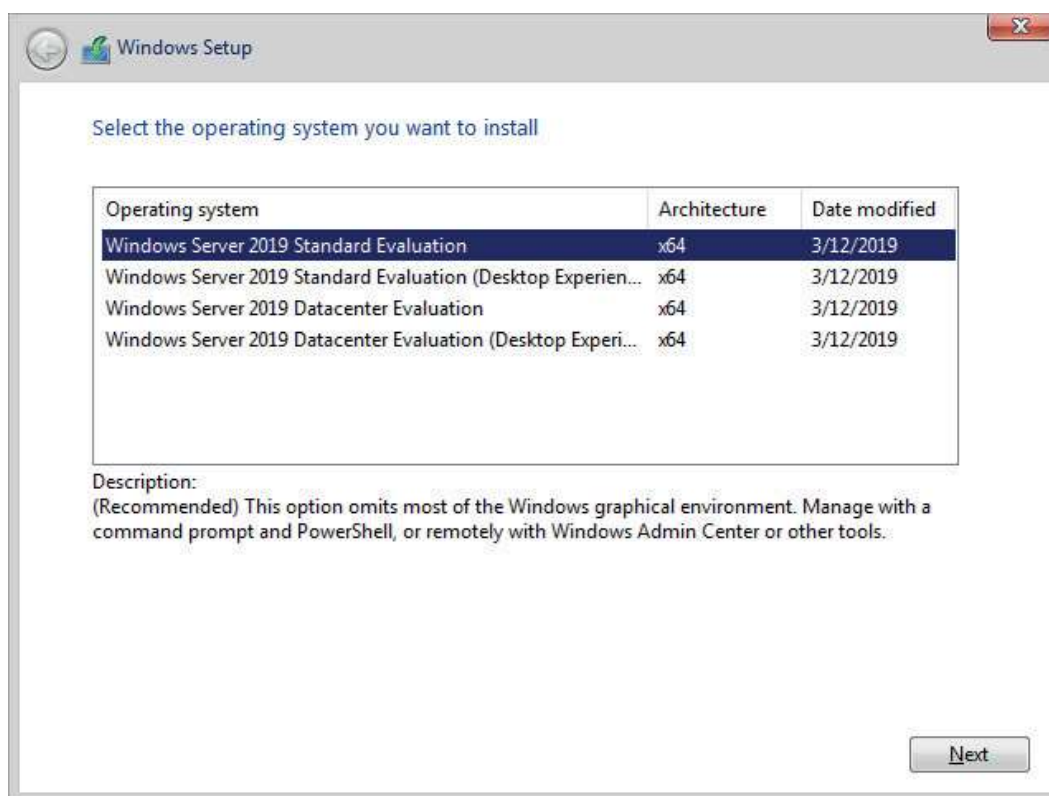
Kompilacje Insider Preview

Więcej informacji na temat kompilacji wstępnych Windows Server i możliwość dołączenia do tego programu można znaleźć pod adresem <https://www.microsoft.com/en-us/software-download/windowsinsiderpreviewserver>.

Server Core

Server Core jest domyślną opcją instalacji systemu Windows Server 2019. Jako że na Server Core składa się mniejsza 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 zawierających interfejs graficzny, cechuje go mniejsze wykorzystanie zasobów.

W systemie Windows Server 2019 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. Natomiast wersja Standard 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. Widywałem to już wiele razy, zatem Czytelnik może czuć się ostrzeżony.



RYSUNEK 2-1 Opcje instalacji systemu Windows Server 2019