Microsoft

Orin Thomas

Windows Server 2016 Inside Out

Przekład: Krzysztof Kapustka, Marek Włodarz

APN Promise, Warszawa 2017

Windows Server 2016 Inside Out

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

Polish language edition published by APN PROMISE SA Copyright © 2017

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

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

ISBN: 978-83-7541-335-9 (druk), 978-83-7541-359-5 (ebook)

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

Spis treści

Wprowadzenie

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

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

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

Dla kogo jest ta książka

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

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

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

Konwencje używane w książce

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

Konwencje tekstowe

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

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

Stałe elementy

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

Dodatkowe informacje

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

Pomoc i informacje zwrotne

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

Errata i pomoc

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

https://aka.ms/WinServ2016CBS/errata

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

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

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

Rozdział 1

Narzędzia administracyjne

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

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

Zdalnie, nie lokalnie

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

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

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

Od podszewki

Automatyzuj, gdzie tylko się da

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

Stacje robocze z dostępem uprzywilejowanym

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

Stacja robocza PAW powinna zostać skonfigurowana w następujący sposób:

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

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

Od podszewki

Serwery przeskoku

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

Narzędzia zdalnej administracji serwerem

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

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

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

Od podszewki

Windows 10 dla Windows Server 2016

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

Konsole RSAT

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

Tabela 1-1 Konsole RSAT

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

Tabela 1-1 Konsole RSAT

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

Tabela 1-1 Konsole RSAT

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

Tabela 1-1 Konsole RSAT

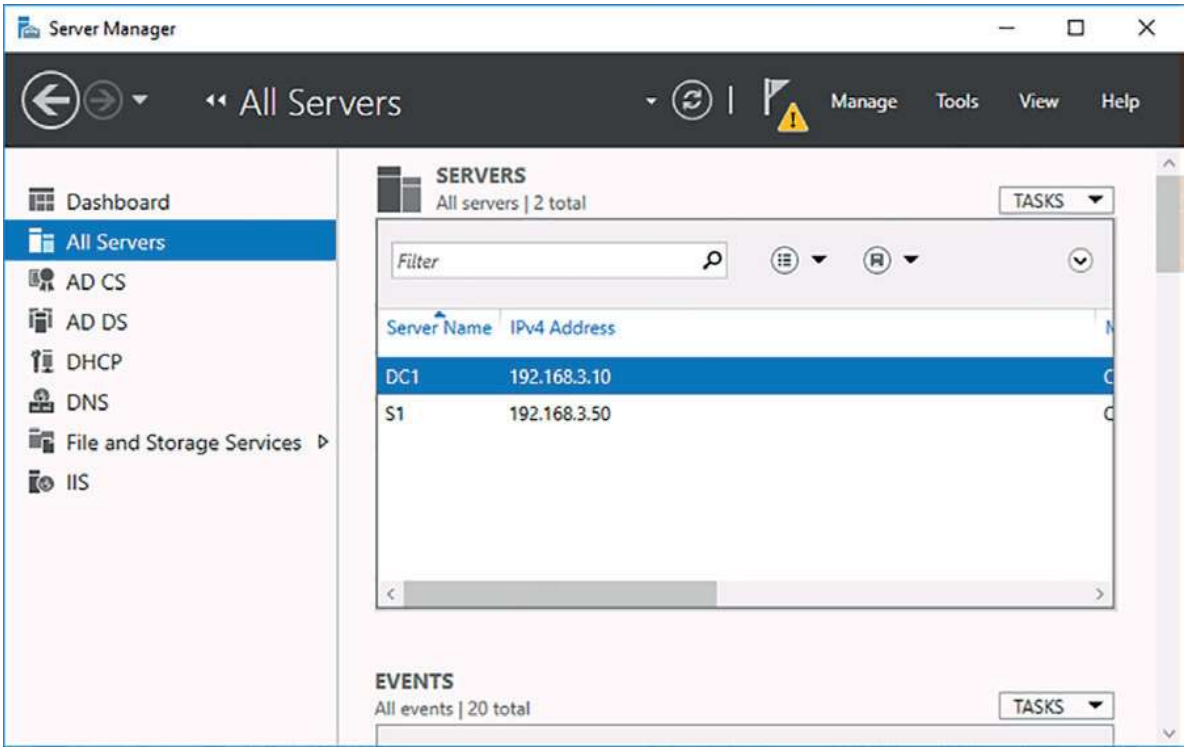
Konsola	Funkcja
Windows Memory Diagnostics	Wykonywanie diagnostyki pamięci w celu sprawdzenia, czy pamięć serwera nie jest uszkodzona. Może wymagać ponownego uruchomienia
Windows Server Backup	Konfigurowanie i zarządzanie funkcją Windows Server Backup
Windows Server Update Services	Konfigurowanie i zarządzanie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

Konsola Server Manager

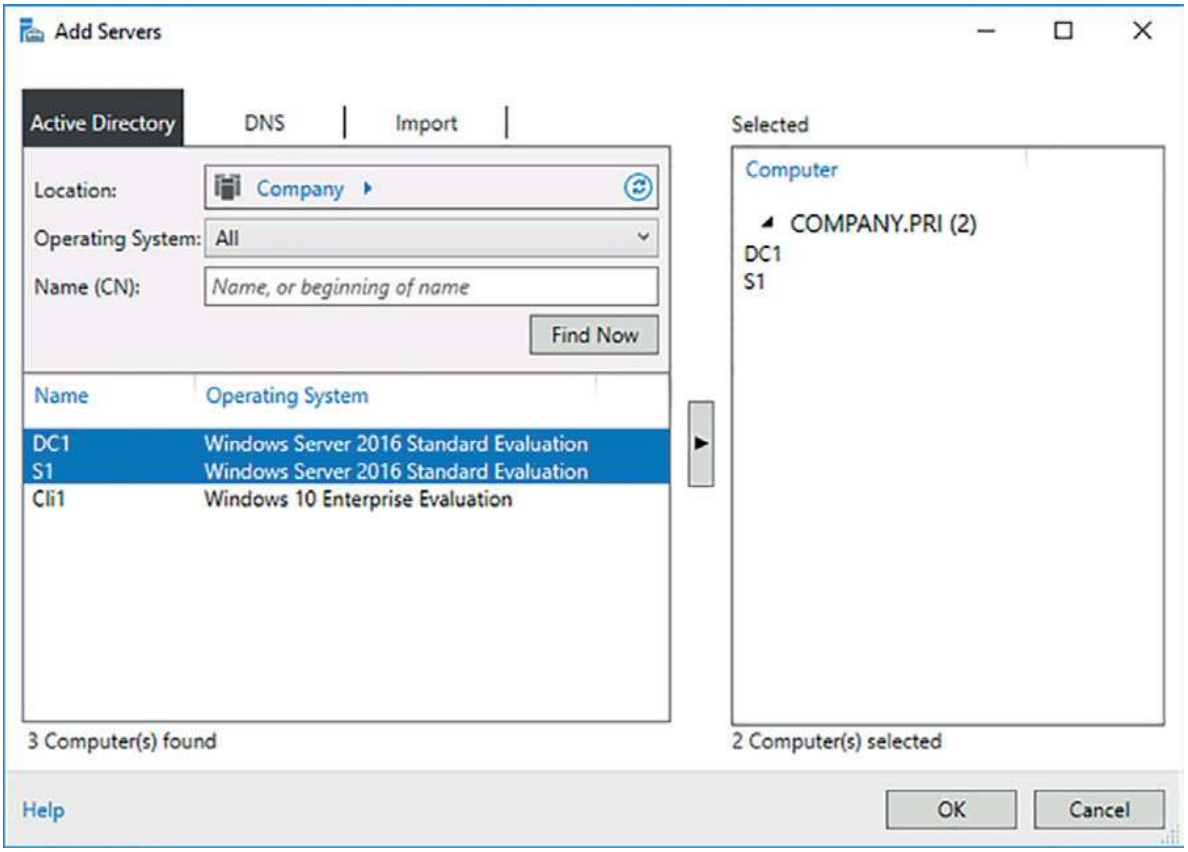
Prawdopodobnie najważniejszą konsolą oferowaną w ramach narzędzi RSAT jest konsola Server Manager. Jeśli system Windows Server 2016 zainstalowaliśmy w ramach opcji Server with Desktop Experience (Środowisko pulpitu), wówczas na takim komputerze konsola ta uruchamiać się będzie automatycznie. Część ról,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

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

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

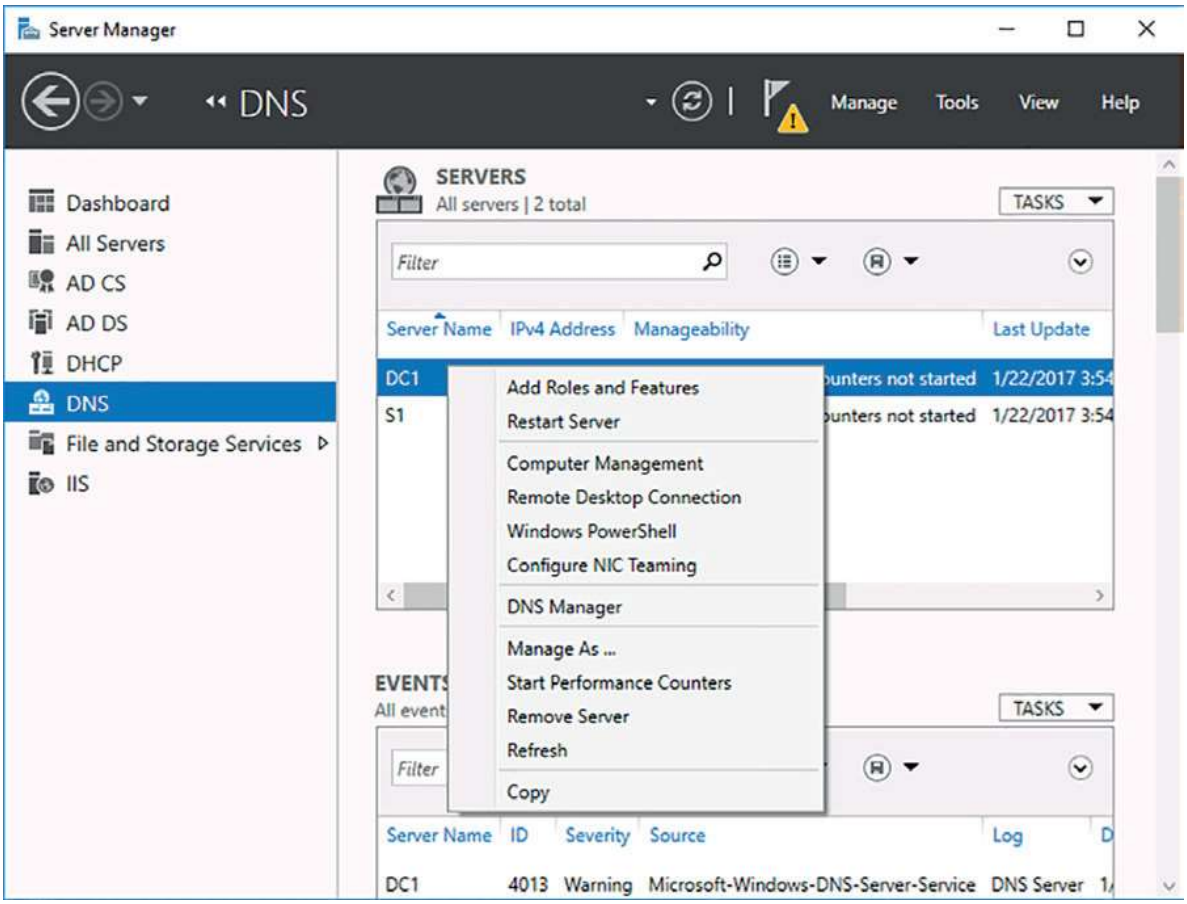


Rysunek 1-1 Lista All Servers



Rysunek 1-2 Dodawanie serwerów do listy All Servers

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



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

Menu kontekstowego wywoływanego prawym przyciskiem myszy możemy również używać do:

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

PowerShell

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

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

Od podszewki

Najnowsza dokumentacja

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

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

Tabela 1-2 Polecenia pomocy PowerShell

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

Tabela 1-2 Polecenia pomocy PowerShell

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

Moduły

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

Galeria PowerShell

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

Tabela 1-3 Podstawowe polecenia galerii PowerShell

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

Obsługa zdalna

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

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

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

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

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

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

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

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

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

```
Help about_Remote_faq -ShowWindow
```

Obsługa zdalna wielu maszyn

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

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

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

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

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

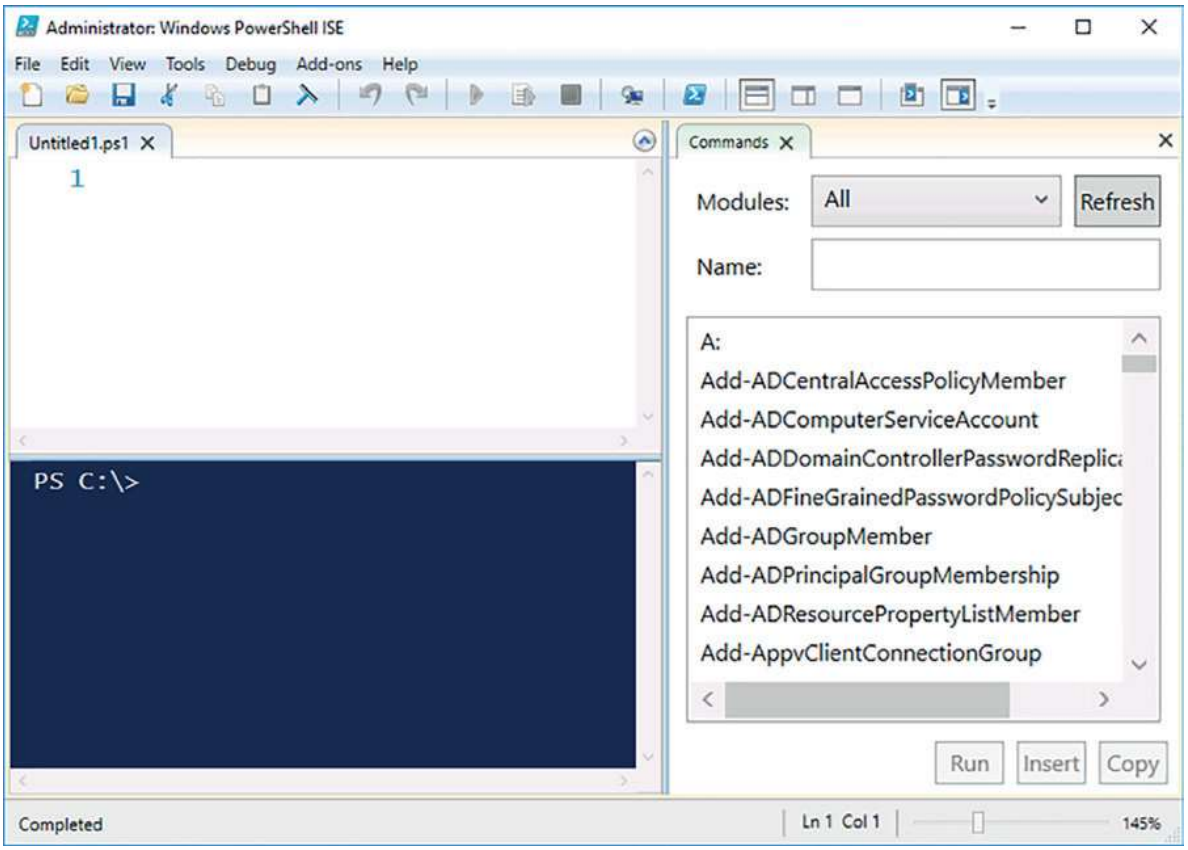
Możemy również wykorzystać polecenie `Invoke-Command` do wykonania skryptu z lokalnego komputera na dowolnej liczbie komputerów zdalnych. Przykładowo, w celu wykonania skryptu FixStuff.ps1 na komputerach wskazanych w pliku computers.txt możemy wykonać poniższe polecenie:

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

PowerShell ISE

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

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



Rysunek 1-4 PowerShell ISE

PowerShell ISE oferuje następującą funkcjonalność:

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

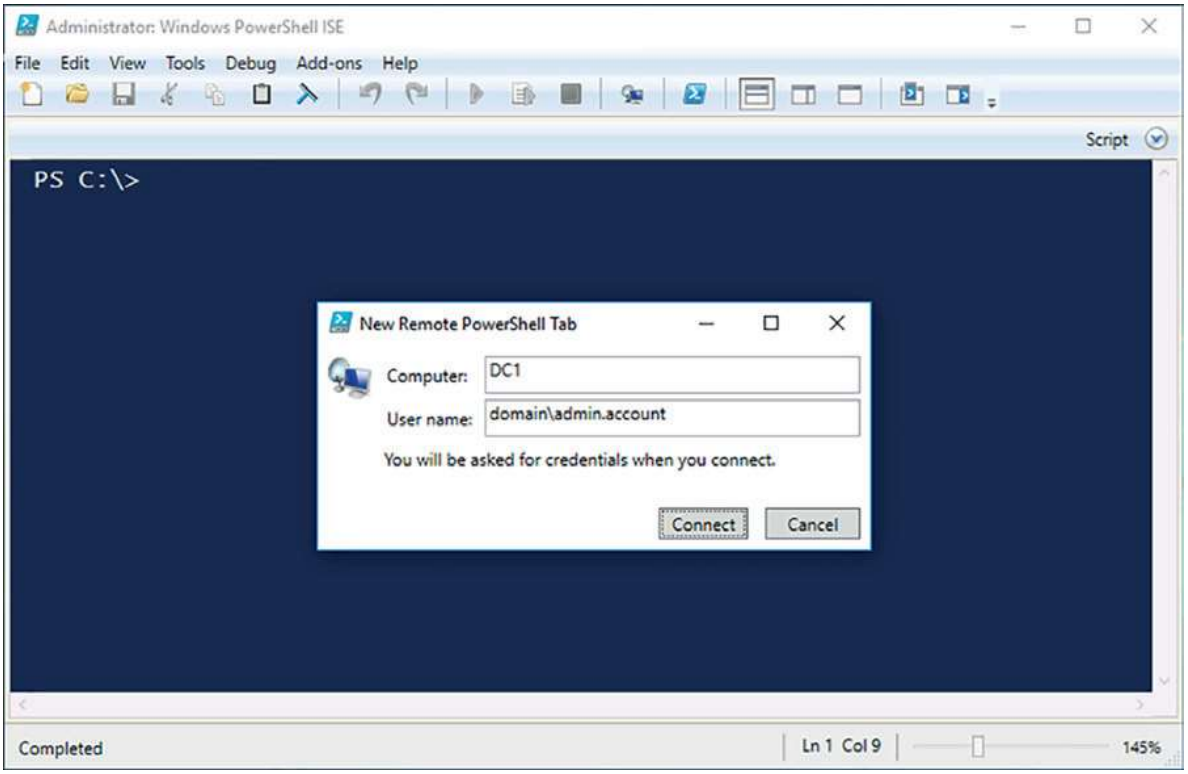
Karty zdalne

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

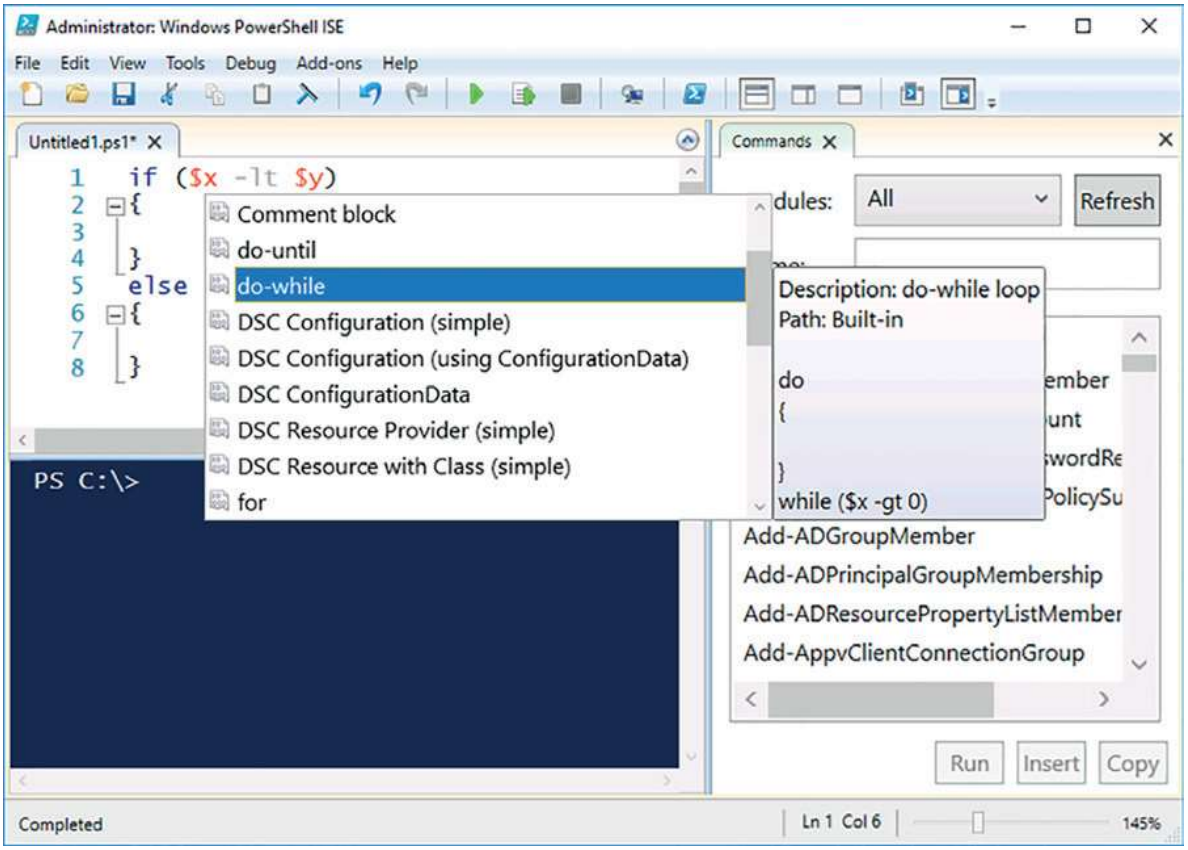
Gdy sesja jest już ustanowiona, z poziomu panelu skryptu konsoli PowerShell ISE możemy zdalnie uruchamiać skrypty i fragmenty kodu dokładnie w taki sam sposób, jak to robimy to na komputerze lokalnym.

Wstawki kodu

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



Rysunek 1-5 Nowa karta zdalna w programie PowerShell ISE



Rysunek 1-6 Wstawki kodu

PowerShell Direct

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

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

Pulpit zdalny

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

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

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

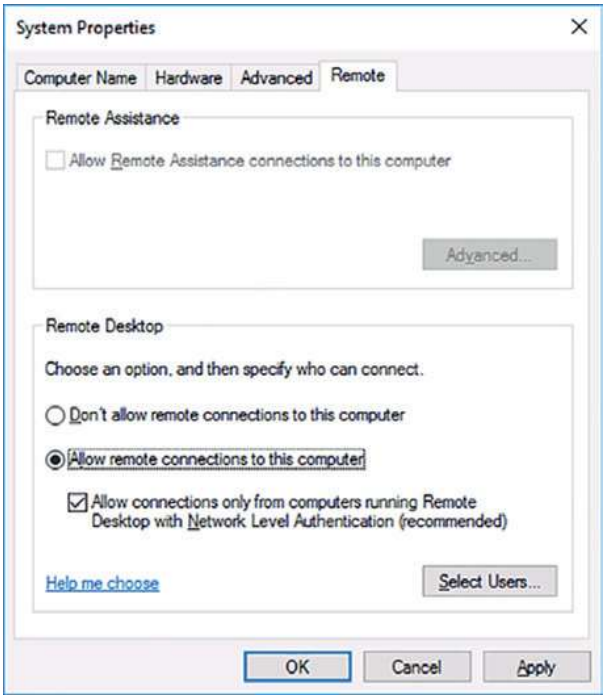
```
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal
  Server" -Name "fDenyTSConnections" –Value 0
```

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

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

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

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



Rysunek 1-7 Karta Remote w oknie właściwości systemu

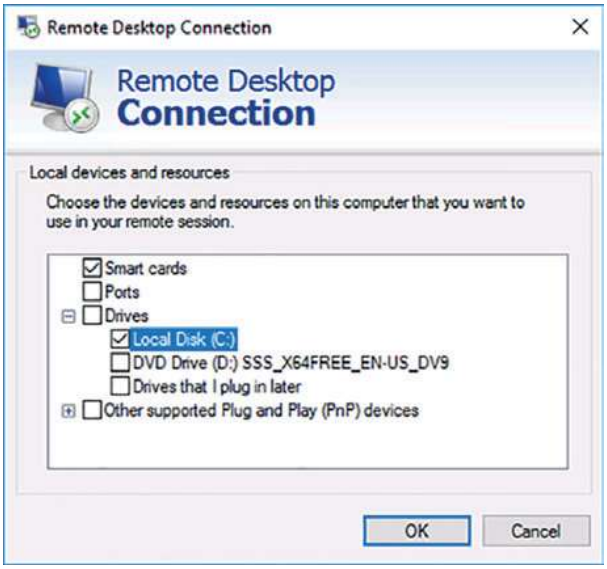
Tylko użytkownicy będący członkami lokalnej grupy administratorów oraz członkowie lokalnej grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego) mogą nawiązywać połączenia za pomocą Pulpitu zdalnego. Jeśli chcemy przyznać komuś uprawnienia dostępu do serwera bez przyznawania mu pełnych uprawnieńadministracyjnych,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

Od podszewki

Just Enough Administration

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

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



Rysunek 1-8 Ustawienia Local Resources and Devices