

Chmura Azure Praktyczne wprowadzenie dla administratora

Implementacja, monitorowanie i zarządzanie
ważnymi usługami i komponentami IaaS/PaaS



Packt 

Mustafa Toroman

Tytuł oryginału: Hands-On Cloud Administration in Azure: Implement, monitor, and manage important Azure services and components including IaaS and PaaS

Tłumaczenie: Andrzej Watrak

ISBN: 978-83-283-6483-7

Copyright © Packt Publishing 2018. First published in the English language under the title 'Hands-On Cloud Administration in Azure – (9781789134964)'

Polish edition copyright © 2020 by Helion SA
All rights reserved.

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

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

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

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

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
<ftp://ftp.helion.pl/przyklady/chmazu.zip>

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

Printed in Poland.

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

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

Spis treści

Przedmowa	9
O autorze	11
O korektorze merytorycznym	12
Wstęp	13
Rozdział 1. Chmura obliczeniowa — podstawowe pojęcia	17
Pojęcia stosowane w chmurze obliczeniowej	17
Rodzaje chmur obliczeniowych	18
Historia Azure w skrócie (od ASM do ARM)	21
Modele usług chmurowych	23
Zalety i wady modeli usług chmurowych	25
Inne zalety chmury	27
Model subskrypcji w chmurze Azure	29
Rodzaje subskrypcji w chmurze Azure	31
Wybór między modelami IaaS i PaaS	33
Opłaty za zasoby w chmurze Azure	35
Rewolucja ARM	36
Podsumowanie	38
Pytania	38
Rozdział 2. Sieci — podstawa modelu IaaS	41
Wymagania techniczne	41
Podstawy sieci Azure	42
Utworzenie sieci w chmurze Azure	42
Opcje sieci wirtualnej Azure	45

Urządzenia w sieci	50
Tworzenie maszyny wirtualnej	50
Typy adresów IP	54
Prywatne adresy IP	55
Sieciowe grupy zabezpieczeń	57
Publiczny adres IP	60
Inne usługi Azure	61
Szablony ARM	62
Podsumowanie	69
Pytania	69
Rozdział 3. Infrastruktura jako usługa — pierwsza warstwa chmury obliczeniowej	71
Wymagania techniczne	72
Wdrażanie maszyn wirtualnych	72
Tworzenie maszyny wirtualnej	72
Podstawowe parametry maszyny wirtualnej	73
Rozmiar maszyny wirtualnej	74
Zaawansowane ustawienia maszyny wirtualnej	76
Zarządzanie maszynami wirtualnymi	79
Ustawienia maszyny wirtualnej	80
Obsługa i monitorowanie maszyny wirtualnej	81
Moduł równoważenia obciążenia	87
Tworzenie modułu równoważenia obciążenia	87
Konfigurowanie modułu równoważenia obciążenia	89
Szablon ARM modułu równoważenia obciążenia	93
Zestaw skalowania maszyn wirtualnych	96
Tworzenie zestawu skalowania maszyn wirtualnych	97
Zarządzanie zestawem skalowania maszyn wirtualnych	100
Szablon zestawu skalowania maszyn wirtualnych	102
Podsumowanie	109
Pytania	109
Rozdział 4. Azure App Service	
— udostępnianie aplikacji internetowych bez serwera	111
Wymagania techniczne	111
Plan usługi aplikacji i aplikacje internetowe	112
Tworzenie aplikacji usługi	112
Tworzenie aplikacji internetowej	114
Zarządzanie aplikacją internetową	116
Konfigurowanie aplikacji internetowej	116
Ogólne ustawienia aplikacji internetowej	118
Domeny niestandardowe, certyfikaty i skalowanie aplikacji	122
Narzędzia programistyczne	126
Monitorowanie aplikacji internetowej	128
Usługa Application Insights	128
Plan usługi aplikacji	132

Wysoka dostępność aplikacji internetowej	133
Tworzenie menedżera ruchu	134
Konfiguracja i ustawienia menedżera ruchu	135
Uruchamianie aplikacji internetowych w dedykowanym środowisku	138
Podsumowanie	139
Pytania	139
Rozdział 5. Platforma danych Azure	141
Wymagania techniczne	141
Rodzaje baz danych w chmurze Azure	141
Serwer SQL Server w modelu IaaS	142
Tworzenie maszyny wirtualnej z serwerem SQL Server	142
Zarządzanie serwerem SQL Server w maszynie wirtualnej	146
Wysoka dostępność serwera SQL Server w maszynie wirtualnej	148
Serwer SQL Server w modelu PaaS	148
Tworzenie bazy danych Azure SQL Database	148
Zarządzanie bazą Azure SQL Database	151
Tworzenie wysokodostępnej bazy Azure SQL Database	154
Bezpieczeństwo bazy Azure SQL Database	157
Monitorowanie i diagnostyka bazy Azure SQL Database	162
Tworzenie kopii zapasowej bazy Azure SQL Database	164
Inne usługi przetwarzania danych w chmurze Azure	165
Podsumowanie	166
Pytania	166
Rozdział 6. Przenoszenie danych do Azure: magazyn, kopie zapasowe i usługa Site Recovery	169
Wymagania techniczne	169
Usługa magazynu Azure	170
Tworzenie konta magazynu	170
Ustawienia konta magazynu	173
Migracja bazy danych do chmury	175
Umieszczanie zapasowej kopii bazy danych w magazynie	176
Migracja bazy danych do Azure SQL	178
Sprawdzanie bazy danych	180
Usługi Recovery Services	184
Tworzenie magazynu usług Recovery Services	185
Tworzenie kopii zapasowych zasobów Azure	185
Tworzenie kopii zapasowych lokalnych zasobów	186
Usługa Site Recovery	192
Przystosowanie usługi Site Recovery do lokalnych zasobów	192
Usługa Site Recovery jako narzędzie migracyjne	198
Tryb failover i migracja maszyny wirtualnej	200
Inne opcje	201
Podsumowanie	203
Pytania	203

Rozdział 7. Chmura hybrydowa	
— rozszerzenie lokalnej infrastruktury na chmurę Azure	205
Wymagania techniczne	205
Chmura hybrydowa	206
Łączenie sieci lokalnej i wirtualnej w chmurze Azure	206
Tworzenie połączenia typu lokacja – lokacja	207
Konfigurowanie połączenia typu lokacja – lokacja w chmurze Azure	211
Konfigurowanie połączenia typu lokacja – lokacja w lokalnej bramie	212
Konfigurowanie usług w chmurze hybrydowej	213
Łączenie sieci wirtualnych wewnątrz chmury Azure	214
Lokalna brama danych	214
Instalacja bramy na lokalnym serwerze	216
Tworzenie w chmurze połączenia z lokalną bramą danych	218
Azure Stack	218
Podsumowanie	220
Pytania	221
Rozdział 8. Azure Active Directory — tożsamość w chmurze	223
Wymagania techniczne	223
Usługa Azure Active Directory	224
Tworzenie nowego katalogu	224
Dostosowanie domeny	226
Synchronizacja usługi AAD z lokalnym kontrolerem domeny	228
Instalacja programu Azure AD Connect	229
Zarządzanie usługą AAD	234
Tworzenie nowego konta użytkownika	234
Zarządzanie opcjami i uprawnieniami użytkowników	236
Rejestrowanie aplikacji w usłudze AAD	237
Mechanizm RBAC	240
Podsumowanie	242
Pytania	242
Rozdział 9. Bezpieczeństwo i administracja w chmurze Azure	245
Wymagania techniczne	246
Fakty i mity o bezpieczeństwie w chmurze	246
Ochrona tożsamości	247
Włączenie uwierzytelnienia wieloskładnikowego	247
Inne zabezpieczenia tożsamości	248
Zabezpieczenia sieci	248
Zapora sieciowa	249
Inne zabezpieczenia sieciowe	255
Szyfrowanie danych	256
Magazyn kluczy	256
Szyfrowanie magazynu danych	260
Szyfrowanie baz danych	261
Szyfrowanie dysków maszyn wirtualnych	263

Centrum zabezpieczeń Azure	264
Ogólne informacje o centrum zabezpieczeń Azure	264
Zalecenia	265
Alerty zabezpieczeń	267
Dostęp just in time	268
Podsumowanie	270
Pytania	271
Rozdział 10. Dobre praktyki	273
<hr/>	
Wymagania techniczne	273
Dobre praktyki	274
Konwencja nazewnictwa	274
Publiczne punkty końcowe	275
Inne kwestie	277
Model IaC	279
Instalacja narzędzi	280
Tworzenie zasobów w modelu IaC	282
Konfiguracja jako kod	292
Korzystanie z Azure Automation i DSC	292
Podsumowanie	297
Pytania	297
Odpowiedzi	299
<hr/>	

Platforma danych Azure

Najważniejszą częścią każdego systemu informatycznego są dane. Systemy i aplikacje bez danych są niczym. Z poprzednich rozdziałów wiesz, jak wdrażać aplikacje w modelach IaaS i PaaS, ale jak tworzy się bazy danych? Teraz poznasz różnego rodzaju bazy danych i dowiesz się, jak tworzyć środowiska dla nich.

W tym rozdziale zostały omówione następujące zagadnienia:

- Wdrażanie serwera SQL Server na maszynie wirtualnej Azure
- Model DaaS (ang. *Database as a Service* — baza danych jako usługa)
- Baza danych Azure SQL Database
- Usługi przetwarzania i analizowania danych w chmurze Azure

Wymagania techniczne

W tym rozdziale będą potrzebne:

- subskrypcja Azure,
- oprogramowanie SQL Server Management Studio.

Rodzaje baz danych w chmurze Azure

Poznanie dostępnych rodzajów baz danych jest bardzo ważnym etapem naszej podróży po chmurze Azure. Wszystkie wdrażane usługi muszą gdzieś przechowywać swoje dane. Chmura Azure oferuje wiele różnego rodzaju baz danych i usług umożliwiających korzystanie z nich. Zaczniemy od tradycyjnego systemu RDBMS (ang. *Relational Database Management System* — system zarządzania relacyjną bazą danych), a następnie zajmiemy się serwerem Microsoft SQL Server umożliwiającym korzystanie z chmurowego systemu RDBMS.

Serwer SQL Server można wdrożyć w chmurze Azure, wykorzystując IaaS lub PaaS. Baza danych w tym drugim modelu jest często określana mianem modelu DaaS. W niniejszym rozdziale poznasz oba modele wraz z dodatkowymi usługami związanymi z obsługą baz danych.

Serwer SQL Server w modelu IaaS

Uruchomienie serwera SQL Server w modelu IaaS wymaga utworzenia maszyny wirtualnej. W tym celu można utworzyć „czystą” maszynę, zawierającą jedynie system operacyjny, a następnie zainstalować w niej SQL Server. Inną opcją jest użycie gotowego obrazu maszyny z zainstalowanym serwerem. Zarządzanie bazą w obu przypadkach nie różni się zbytnio od zarządzania w lokalnym środowisku — dostępna jest pełna wersja serwera SQL Server ze wszystkimi opcjami.

Zacznijmy od utworzenia krok po kroku maszyny wirtualnej z serwerem SQL Server.

Tworzenie maszyny wirtualnej z serwerem SQL Server

Jak wspomniałem, można najpierw utworzyć maszynę wirtualną, a następnie zainstalować w niej serwer SQL Server lub utworzyć maszynę od razu, wykorzystując gotowy obraz z serwerem. W tym przykładzie użyjemy obrazu z serwerem SQL Server 2017 Enterprise Edition i systemem operacyjnym Windows Server 2016.

Aby utworzyć maszynę, kliknij ikonę *Utwórz zasób*, następnie odnośnik *Obliczeniowe* i ikonę *SQL Server 2017 Enterprise Windows Server 2016*. Większość dostępnych opcji jest takich samych jak w maszynie bez serwera. Trzeba podać podstawowe informacje, takie jak nazwa maszyny, typ dysku, nazwa użytkownika, hasło, subskrypcja, grupa zasobów i region. W przypadku maszyny z serwerem SQL Server bardzo zalecane jest użycie dysków SSD, ponieważ wydajność bazy w dużym stopniu zależy od szybkości operacji dyskowych. Oto przykładowe ustawienia maszyny (zobacz pierwszy rysunek na następnej stronie).

Kolejnym krokiem jest wybranie rozmiaru maszyny. Zalecany jest rozmiar z większą liczbą rdzeni i większą ilością pamięci, ponieważ SQL Server wymaga większych zasobów i od rozmiaru maszyny zależy jego wydajność. Jeżeli w przyszłości okaże się, że wybrany rozmiar jest zbyt mały lub zbyt duży, będzie go można zmienić. Jest to jedna z zalet chmury — początkowo wybrana wielkość zasobu nie jest wiążąca dla użytkownika. Oto lista dostępnych rozmiarów maszyn z dyskami SSD (zobacz drugi rysunek na następnej stronie).

Subskrypcja * ⓘ

Grupa zasobów * ⓘ
 [Utwórz nowy](#)

Szczegóły wystąpienia

Nazwa maszyny wirtualnej * ⓘ

Region * ⓘ

Opcje dostępności ⓘ

Obraz * ⓘ
 [Przeglądaj wszystkie obrazy publiczne i prywatne](#)

Wystąpienie usługi Azure Spot ⓘ Tak Nie

Wybieranie rozmiaru maszyny wirtualnej ✕

Przejrzyj dostępne rozmiary maszyn wirtualnych i ich funkcje

[Przywróć filtry domyślne](#)

Wysświetlanie 268 rozmiarów maszyn wirtualnych. | Subskrypcja: Płatność zgodnie z rzeczywistym użyciem | Region: Europa Zachodnia | Bieżący rozmiar: Standard_DS13_v2

Rozmi...↕	Oferta ↕	Rodzina ↕	Proc...↕	Pamię...↕	Dyski z d...↕	Maks. IO...↕	Tymczasowy m...↕	Pomoc technic...↕	Koszt/miesiąc (...↕)
A2	Standardowa	Ogólnego przeznac...	2	3,5	4	4x500		Nie	112,93 €
A2	Podstawowa	Ogólnego przeznac...	2	3,5	4	4x300		Nie	75,92 €
A2_v2	Standardowa	Ogólnego przeznac...	2	4	4	4x500	20	Nie	81,56 €
A2m_v2	Standardowa	Ogólnego przeznac...	2	16	4	4x500	20	Nie	117,95 €
A3	Standardowa	Ogólnego przeznac...	4	7	8	8x500		Nie	225,87 €
A3	Podstawowa	Ogólnego przeznac...	4	7	8	8x300		Nie	203,28 €
A4	Standardowa	Ogólnego przeznac...	8	14	16	16x500		Nie	451,74 €
A4	Podstawowa	Ogólnego przeznac...	8	14	16	16x300		Nie	406,57 €
A4_v2	Standardowa	Ogólnego przeznac...	4	8	8	8x500	40	Nie	171,91 €
A4m_v2	Standardowa	Ogólnego przeznac...	4	32	8	8x500	40	Nie	247,20 €

Podane ceny to szacowane wartości w walucie lokalnej, które obejmują tylko koszty infrastruktury platformy Azure i uwzględniają rabaty dla danej subskrypcji oraz lokalizacji. Ceny nie zawierają żadnych kosztów odpowiedniego oprogramowania. Ostateczne opłaty będą widoczne w walucie lokalnej w widokach analizy kosztów i rozliczeń. Wyświetl kalkulator cen platformy Azure.

Pozostałe opcje są takie same jak opisane w poprzednim rozdziale. Można pozostawić ich domyślne wartości. Jeżeli potrzebna jest wysoka dostępność serwera, strefę i zestaw dostępności należy wybrać już teraz, ponieważ tych ustawień nie można później zmienić. Zwróć uwagę na wybraną sieć, podsieć i sieciową grupę zabezpieczeń. Serwera SQL Server nie należy umieszczać w podsieci DMZ. Ponadto należy użyć innej sieciowej grupy zabezpieczeń niż wykorzystywana przez serwer WWW. Ustawienia te można później zmienić. Oto przykładowe parametry sieci:

Interfejs sieciowy

Podczas tworzenia maszyny wirtualnej interfejs sieciowy zostanie utworzony za Ciebie.

Sieć wirtualna * ⓘ MojaSiec ▼
 Utwórz nowy

Podsieć * ⓘ default (10.1.0.0/24) ▼
 Zarządzaj konfiguracją podsieci

Publiczny adres IP ⓘ (nowy) BazaDanych-ip ▼
 Utwórz nowy

Sieciowa grupa zabezpieczeń karty sieciowej ⓘ Brak Basic Zaawansowane

Publiczne porty ruchu przychodzącego * ⓘ Brak Zezwalaj na wybrane porty

Wybierz porty wejściowe * RDP (3389) ▼

W zakładce *Ustawienia programu SQL Server* znajdują się ustawienia charakterystyczne dla obrazu z zainstalowanym serwerem SQL Server. Można tu określić łączność SQL, uwierzytelnienie, konfigurację magazynu danych, automatyczne stosowanie poprawek, automatyczne tworzenie kopii zapasowych, integrację z usługą Azure Key Vault oraz ustawienia języka R (zaawansowane funkcje analityczne).

Ustawienie *Łączność SQL* określa rodzaj połączenia z serwerem i wykorzystywany do tego celu port. Można wybrać połączenie *Lokalne (tylko wewnątrz maszyny wirtualnej)*, *Prywatne (wewnątrz sieci wirtualnej)* lub *Publiczne (Internet)*. Nie zaleca się jednak stosować ostatniej opcji. Jeżeli bowiem baza danych będzie dostępna w Internecie, każdy będzie mógł do niej się dostać i przeprowadzić atak. Pierwszy wybór też nie jest właściwy, chyba że cała aplikacja będzie uruchomiona na jednej maszynie. Najczęściej wybierane jest drugie ustawienie, umożliwiające odwoływanie się do bazy wyłącznie z maszyn znajdujących się w tej samej sieci wirtualnej. Domyślnie serwer wykorzystuje port nr 1433, który można w razie potrzeby zmienić.

Domyślnie w serwerze SQL jest stosowane takie samo uwierzytelnienie jak w systemie Windows. Jeżeli w ustawieniu *Uwierzytelnianie SQL* wybierze się wartość *Włącz*, będzie można określić nazwę użytkownika i hasło niezbędne do zalogowania się do serwera.

Zautomatyzowane stosowanie poprawek jest domyślnie wykonywane w niedzielę, o godzinie 2.00. Ustawienie to można zmieniać lub wyłączać, aczkolwiek wyłączenie nie jest zalecane, ponieważ dzięki poprawkom oprogramowanie serwera będzie zawsze aktualne i zabezpieczone. Czasami jednak trzeba sprawdzić poprawki przed ich zainstalowaniem, aby można je było ewentualnie zablokować. W takim przypadku aktualizacją serwera musi zajmować się administrator.

Ustawienie *Automatyczne tworzenie kopii zapasowych* jest domyślnie wyłączone. Po jego włączeniu pojawiają się dodatkowe ustawienia, służące do określenia konta magazynu, w którym będą umieszczane kopie. Domyślnie kopie są przechowywane przez 30 dni. Minimalny okres wynosi 1 dzień, a maksymalny 30 dni. Kopie można szyfrować, jak również umieszczać w nich bazę systemową.

Kolejne ustawienie dotyczy harmonogramu tworzenia kopii zapasowych. Domyślnie kopia jest tworzona raz na tydzień, ale może być wykonywana codziennie. Można określić godzinę tworzenia kopii bazy oraz częstotliwość tworzenia kopii dziennika (minimalnie co 5 minut, maksymalnie co godzinę).

Ostatnie ustawienia to *Integracja usługi Azure Key Vault i Usługi języka R (zaawansowane funkcje analityczne)*. Można je włączyć lub wyłączyć. Pierwsze wymaga podania dodatkowych informacji, a drugie skutkuje zainstalowaniem dodatkowych funkcjonalności.

Oto przykładowe ustawienia serwera SQL Server:

Zabezpieczenia i sieć

Łączność SQL *

Port *

Uwierzytelnianie SQL

Uwierzytelnianie SQL Wyłącz Włącz

Integracja usługi Azure Key Vault Wyłącz Włącz

Konfiguracja magazynu

Dostosuj wydajność, rozmiar i typ obciążenia, aby zoptymalizować magazyn dla tej maszyny wirtualnej. W celu uzyskania optymalnej wydajności domyślnie zostaną utworzone oddzielne dyski dla danych i magazynu dziennika. Dowiedz się więcej o najlepszych rozwiązaniach w zakresie wydajności programu SQL Server.

Magazyn **Optymalizacja magazynu: Przetwarzanie transakcji**
 SQL Dane: 1024 GiB, 5000 operacji we/wy na sekundę, 200 MB/s
 SQL Dziennik: 1024 GiB, 5000 operacji we/wy na sekundę, 200 MB/s
 SQL TempDb: Użyj lokalnego dysku SSD
[Zmień konfigurację](#)

Licencja na program SQL Server

Oszczędź do 43% dzięki licencjom, które już masz. Masz już licencję na program SQL Server? [Dowiedz się więcej](#)

Zautomatyzowane stosowanie poprawek

Ustaw okno stosowania poprawek, w ciągu którego zostaną zastosowane wszystkie poprawki systemu Windows i języka SQL.

Zautomatyzowane stosowanie poprawek **Włączono**
 Niedziela o 2:00
[Zmień konfigurację](#)

Automatyczne tworzenie kopii zapasowych

Automatyczne tworzenie kopii zapasowych Wyłącz Włącz

Usługi języka R (zaawansowane funkcje analityczne)

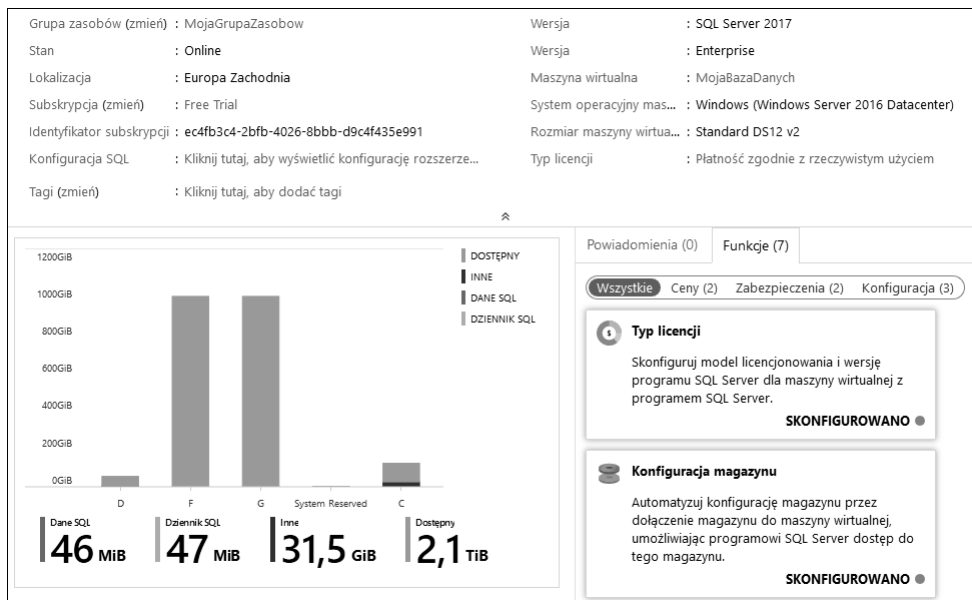
SQL Server Machine Learning Services (In-Database) Wyłącz Włącz

Wdrożenie maszyny z serwerem SQL Server trwa nieco dłużej niż zwykłej maszyny, ponieważ dodatkowo jest uruchamiany i konfigurowany serwer.

Zarządzanie serwerem SQL Server w maszynie wirtualnej

Ustawienia utworzonej maszyny wirtualnej z serwerem SQL Server są bardzo podobne do ustawień zwykłej maszyny. Jedyną różnicą polega na tym, że w sekcji *Ustawienia* znajduje się dodatkowa opcja *Konfiguracja serwera SQL*, zawierająca ustawienia bardzo podobne do określonych w ostatnim kroku procesu tworzenia maszyny.

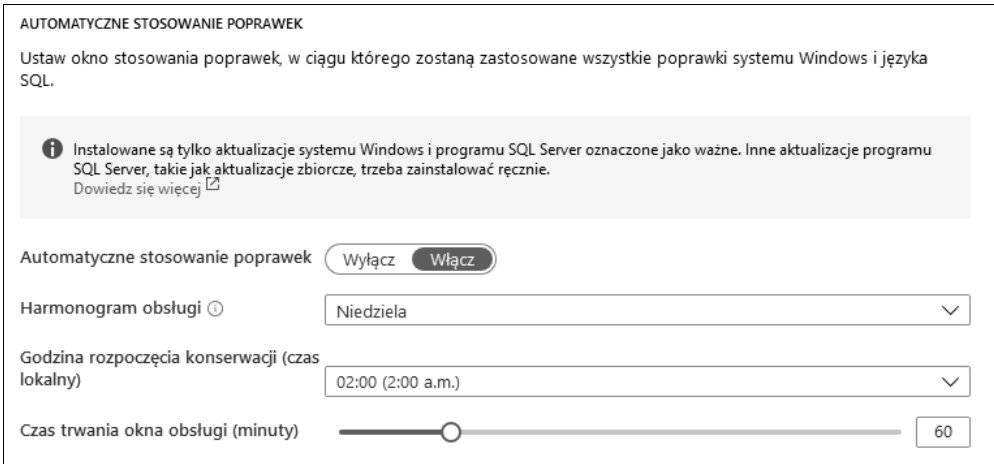
Oto ogólne informacje o serwerze SQL:



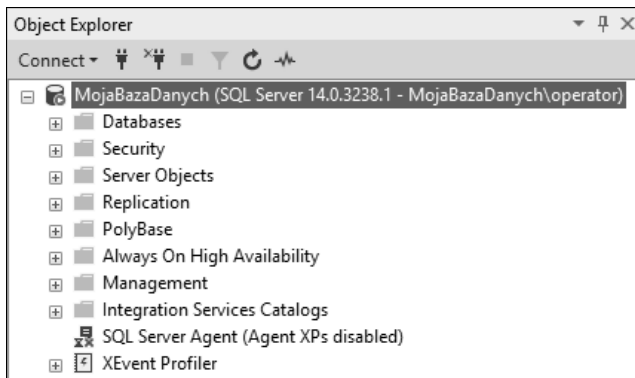
Pierwsze dwie dostępne opcje to *Typ licencji* i *Konfiguracja magazynu*. Otwierają one widok, w którym można zmienić ustawienia licencji i dysków.

Kolejna opcja to *Łączność SQL*, za pomocą której można zmieniać sposób dostępu do serwera, numer portu, uwierzytelnianie (włączone lub wyłączone) oraz integrację z usługą Azure Key Vault.

Pozostałe opcje konfiguracyjne to *Integracja usługi Azure Key Vault*, *Automatyczne stosowanie poprawek*, *Automatyczne kopie zapasowe* i *Usługi języka R (zaawansowane funkcje analityczne)*. Wszystkie zawierają te same ustawienia jak w widoku do tworzenia maszyny. Oto ustawienia dostępne w widoku opcji *Automatyczne stosowanie poprawek*:



Serwerem można zarządzać za pomocą programu SQL Server Management Studio zainstalowanego w maszynie wirtualnej. Można również użyć lokalnego komputera, o ile został skonfigurowany publiczny dostęp do serwera. Po nawiązaniu połączenia dostępne są takie same opcje i funkcjonalności jak w serwerze wdrożonym w lokalnym środowisku. Pod tym względem utrzymywanie baz danych i administrowanie nimi w chmurze niczym się różni od zarządzania w lokalnym serwerze lub maszynie wirtualnej. Można wykonywać dowolne operacje i wprowadzać wszelkie zmiany. Poniższy rysunek pokazuje, że w serwerze SQL Server uruchomionym w maszynie wirtualnej w chmurze Azure dostępne są takie same opcje jak w lokalnym serwerze:



Maszyna wirtualna z serwerem SQL Server niczym się różni pod względem utrzymania i administrowania od zwykłej maszyny Azure. Wszystkie opcje konfiguracyjne są takie same. Dodatkowo dostępna jest opcja *Konfiguracja serwera SQL*.

Wysoka dostępność serwera SQL Server w maszynie wirtualnej

Administrowanie maszyną wirtualną z serwerem SQL Server i utrzymywanie jej niczym się nie różni od zwykłej maszyny. Tak samo jest w przypadku konfigurowania wysokiej dostępności. Do dyspozycji mamy kilka opcji:

- utworzenie klastra zawsze dostępnych maszyn pracujących w trybie failover;
- utworzenie grupy zawsze dostępnych maszyn;
- utworzenie lustrzanej bazy danych;
- wysyłanie dzienników.

Aby uzyskać wysoką dostępność maszyn, należy je umieścić w strefie lub zestawie dostępności.

Teraz zajmiemy się serwerem SQL Server w modelu PaaS i porównamy dostępne opcje i funkcjonalności.

Serwer SQL Server w modelu PaaS

Tworząc serwer SQL Server w modelu PaaS, można korzystać ze wszystkich zalet tego modelu. Oznacza to, że dostępnych jest mniej opcji konfiguracyjnych, ale też mniejszy jest nakład pracy związanej z utrzymywaniem serwera. Administrator nie ma bezpośredniego dostępu do serwera, dlatego wielu operacji nie może wykonać samodzielnie, ale do dyspozycji ma wiele innych opcji.

Zacznijmy od utworzenia bazy danych Azure SQL Database, a następnie przejrzymy dostępne opcje.

Tworzenie bazy danych Azure SQL Database

Aby utworzyć bazę, kliknij ikonę *Utwórz zasób*, następnie odnośnik *Bazy danych* i ikonę *SQL Database*. W widoku, który się pojawi, podaj standardowe informacje, takie jak nazwa zasobu, subskrypcja, grupa zasobów. Dodatkowe wymagane informacje są charakterystyczne dla bazy danych: źródło, nazwa serwera i warstwa cenowa. Ustawienie *Chcesz użyć puli elastycznej SQL?* jest bezpośrednio związane z warstwą cenową (zajmiemy się nim za chwilę). Ustawienie *Źródło danych* może przyjąć wartość *Brak* (zostanie utworzona pusta baza), *Kopia zapasowa* (dane zostaną skopiowane z zapasowej kopii umieszczonej we wskazanym magazynie) lub *Przykład* (w bazie zostaną umieszczone przykładowe dane *AdventureWorkLT*). Ustawienie *Sortowanie* ma wartość *SQL_Latin1_General_CP1_CI_AS* i nie można go zmieniać. Oto przykładowe ustawienia bazy:

Podstawowe Sieć Ustawienia dodatkowe Tagi Przeglądanie + tworzenie

Utwórz bazę danych SQL z preferowanymi konfiguracjami. Wypełnij kartę Podstawy, a następnie przejdź do obszaru Przegląd i tworzenie, aby aprowizować z użyciem inteligentnych wartości domyślnych, lub przejdź na każdą z kart, aby dostosować ustawienia. [Dowiedz się więcej](#)

Szczegóły projektu

Wybierz subskrypcję, aby zarządzać wdrożonymi zasobami i kosztami. Użyj grup zasobów jak folderów, aby organizować wszystkie Twoje zasoby i zarządzać nimi.

Subskrypcja * ⓘ Płatność zgodnie z rzeczywistym użyciem ▼

Grupa zasobów * ⓘ MojaGrupaZasobow ▼
Utwórz nowy

Szczegóły bazy danych

Podaj wymagane ustawienia dla tej bazy danych, w tym wybierania serwera logicznego oraz konfigurowania zasobów obliczeniowych i magazynowych

Nazwa bazy danych * MojaBazaDanych ▼

Serwer * ⓘ (nowe) moj-serwer ((Europa) Europa Zachodnia) ▼
Utwórz nowy

Chcesz użyć puli elastycznej SQL? * ⓘ Tak Nie

Obliczenia i magazyn * ⓘ
Przeznaczenie ogólne
 Gen5, 2 Rdzenie wirtualne, Magazyn 32 GB
 Konfigurowanie bazy danych

Baza danych nie może istnieć bez serwera. Dlatego podczas tworzenia bazy trzeba wprowadzić parametry serwera. Jeżeli go nie ma, należy utworzyć nowy. Konieczne jest podanie nazwy serwera (która musi być unikatowa, ponieważ zostanie użyta w publicznym punkcie dostępu), nazwy użytkownika, hasła i regionu.

Naliczanie opłat za bazę Azure SQL Database jest dość skomplikowane, gdyż istnieją dwa modele cenowe. Pierwszy dotyczy pojedynczej bazy danych. Opłata jest naliczana za bazę, a sam serwer jest bezpłatny. Jeżeli na jednym lub kilku serwerach jest uruchomionych kilka baz, opłata zależy od ich liczby, a nie od liczby serwerów. Załóżmy, że mamy dziesięć baz. Opłata będzie taka sama, niezależnie od tego, czy bazy będą się znajdowały na jednym czy na dziesięciu serwerach. Sprawa zaczyna się komplikować, gdy opłata jest określana na podstawie **jednostek DTU** (ang. *Database Transaction Unit* — jednostka transakcyjna bazy danych). Liczba jednostek zależy od liczby rdzeni procesora, wielkości pamięci oraz liczby transakcji danych i dzienników. W środowisku lokalnym te składniki są znane i można je przeliczyć na jednostki, choć nie jest to proste zadanie. W chmurze Azure można zmieniać modele cenowe na bieżąco. Jeżeli po pewnym czasie wydajność bazy okaże się niewystarczająca lub zasoby nie będą w pełni wykorzystywane, będzie je można w każdej chwili odpowiednio zmienić. W modelu opartym na jednostkach DTU dostępne są trzy warstwy cenowe: *Podstawowa*, *Standardowa* i *Premium*.

Liczba jednostek waha się od 5 w warstwie podstawowej do 4000 w warstwie premium P15. Oto widok umożliwiający wybranie liczby jednostek w warstwie standardowej:

Podstawowa
Dla mniej wymagających obciążeń

Standardowa
Dla obciążeń z typowymi wymaganiami w zakresie wydajności

Premium
Dla obciążeń intensywnie korzystających z operacji wejścia/wyjścia.

Opcje zakupu oparte na rdzeniach wirtualnych
Kliknij tutaj, aby dostosować wydajność za pomocą rdzeni wirtualnych

Jednostki DTU Co to jest jednostka DTU? ⓘ

10 20 50 100 200 400 800 1600 3000 10 (50)

Maksymalny rozmiar danych

100 MB 250 GB 250 GB

Podsumowanie kosztów

Koszt na DTU (w EUR)	1,27
Liczba wybranych: Jednostki DTU	x 10
SZACOWANY KOSZT MIESIĘCZNY	12,65 EUR

Ponieważ model oparty na jednostkach DTU okazał się zbyt skomplikowany dla użytkowników, Microsoft wprowadził inny model, oparty na wirtualnych rdzeniach procesorów. W tym modelu użytkownik może wybrać liczbę rdzeni i ilość pamięci przeznaczoną dla bazy danych. Liczba rdzeni waha się od 2 do 80, a ilość pamięci od 5,5 do 408 GB (w zależności od wybranej liczby rdzeni). Oto widok umożliwiający wybranie liczby rdzeni:

Warstwa obliczeniowa

Obsługiwane administracyjnie

Zasoby obliczeniowe są wstępnie przydzielane

Rozliczane co godzinę na podstawie skonfigurowanych rdzeni wirtualnych

Bezserwerowe

Zasoby obliczeniowe są skalowane automatycznie

Rozliczane co godzinę na podstawie użytych rdzeni wirtualnych

Sprzęt do obliczeń

Kliknij pozycję „Zmień konfigurację”, aby wyświetlić szczegóły dotyczące wszystkich dostępnych generacji sprzętu, w tym opcji zoptymalizowanych pod kątem pamięci i obliczeń

Konfiguracja sprzętu

5. generacji

do 80 rdzeni wirtualnych, do 408 GB pamięci

Zmień konfigurację

Oszczędność pieniędzy

Oszczędzaj do 55% dzięki licencji, którą już masz. Masz już licencje na program SQL Server? ⓘ

Tak Nie

Rdzenie wirtualne Czym różnią się rdzenie wirtualne od jednostek DTU? ⓘ

2 4 6 8 10 12 14 16 18 20 24 32 40 80 2 Rdzenie wirtualne

Maksymalny rozmiar danych ⓘ

1 GB 1 TB 1 GB

Podsumowanie kosztów

5. generacji — Przeznaczenie ogólne (GP_Gen5_2)

Koszt na rdzeń wirtualny (w EUR) **167.77**

Liczba wybranych: **Rdzenie wirtualne** **x 2**

Koszt na GB (w EUR) **0.12**

Wybrano: **Max storage** (w GB) **x 1.3**

SZACOWANY KOSZT MIESIĘCZNY **335,70 EUR**



307,2 MB PRZYDZIELONE MIEJSCE NA DZIENNIKI

Jak wspomniałem, z opłatami jest związane ustawienie *Chcesz użyć puli elastycznej SQL?*. Jeżeli zostanie wybrane, wówczas opłata będzie naliczana nie na podstawie liczby baz danych, lecz wielkości puli. Podobnie jak w przypadku pojedynczej bazy, można wybrać sposób wyceniania zasobów w puli na podstawie jednostek DTU lub wirtualnych rdzeni. Różnica między pojedynczą bazą a pulą polega na tym, że zasoby w puli są współdzielone z innymi bazami. Jeżeli na przykład pula będzie zawierała 4000 jednostek DTU, będą one wykorzystywane przez wszystkie bazy znajdujące się w puli. Gdy wszystkie bazy są intensywnie wykorzystywane w tym samym czasie, ten model nie jest najbardziej efektywny i lepiej jest wybrać wycenianie oparte na pojedynczej bazie. Doskonale za to sprawdza się w sytuacji, kiedy szczytowe obciążenia poszczególnych baz wypadają w różnych porach dnia.

Wyobraźmy sobie, że mamy aplikację, z której korzystają użytkownicy z całego świata. Okresy zwiększonego obciążenia baz danych zdarzają się w różnych momentach, w zależności od strefy czasowej, w której znajdują się użytkownicy. Baza danych obsługująca użytkowników z Europy jest bardziej obciążona w europejskich godzinach pracy, a mniej w amerykańskich. Natomiast baza obsługująca użytkowników ze Stanów Zjednoczonych jest bardziej obciążona w amerykańskich godzinach pracy, mniej zaś w europejskich. Jeżeli obie bazy umieści się w elastycznej puli, będą współdzieliły dostępne zasoby. W efekcie obie będą miały do dyspozycji więcej zasobów, choć w różnych przedziałach czasu.

Czas wdrażania bazy Azure SQL Database zależy od wybranej warstwy i źródła danych. Od źródła zależą ilość danych i rodzaje wykonywanych operacji. Oczywiście krócej trwa utworzenie pustej bazy niż odtworzenie kopii zapasowej o wielkości rzędu giga- lub terabajtów.

Po wdrożeniu bazy pojawiają się dwa nowe zasoby, mianowicie *Serwer SQL* i *Baza danych SQL*:

<input type="checkbox"/> Nazwa ↑↓	Typ ↑↓	Lokalizacja ↑↓
<input type="checkbox"/>  moj-serwer	Serwer SQL	Europa Zachodnia ...
<input type="checkbox"/>  MojaBazaDanych (moj-serwer/MojaBazaDanych)	Baza danych SQL	Europa Zachodnia ...

Zarządzanie bazą Azure SQL Database

Zarządzanie bazą Azure SQL Database należy zacząć od skonfigurowania zapory. Domyślnie z bazą mogą się łączyć jedynie usługi Azure. Aby baza mogła obsługiwać połączenia pochodzące od określonych adresów IP, należy skonfigurować regułę zapory. W tym celu w widoku serwera SQL kliknij opcję *Zapory i sieci wirtualne*, a następnie przycisk *Dodaj adres IP klienta*. Portal wykryje adres IP Twojego komputera i użyje go w nowej regule. Pamiętaj, aby po wprowadzeniu zmian kliknąć *Zapisz*. Jeżeli tego nie zrobisz, reguła nie zostanie utworzona. Taka sytuacja zdarzyła mi się kilkakrotnie — dodałem nowy adres IP, zapomniałem kliknąć *Zapisz*, a potem trwonilem czas na dociekanie, dlaczego nie mogłem nawiązać połączenia z bazą. Oto przykładowe ustawienia zapory:

Zapisz ✕ Odrzuć + Dodaj adres IP klienta

i Połączenia z adresów IP określonych poniżej umożliwiają dostęp do wszystkich baz danych w lokalizacji moj-serwer.

Zezwalaj usługom i zasobom platformy Azure na dostęp do tego serwera

WŁ. **WYŁ.**

Adres IP klienta 78.11.214.75

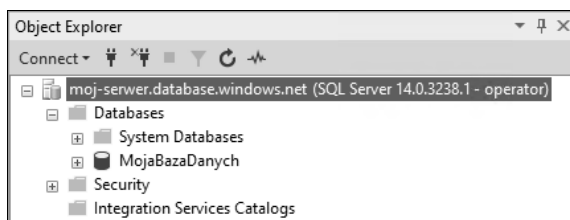
Nazwa reguły	Początkowy adres IP	Końcowy adres IP	
<input type="text"/>	<input type="text"/>	<input type="text"/>	...
ClientIPAddress_2020-1-22_1...	78.11.214.75	78.11.214.75	...

i Połączenia z sieci wirtualnych/podsieci określonych poniżej umożliwiają dostęp do wszystkich baz danych w lokalizacji moj-serwer.

Sieci wirtualne + Dodaj istniejącą sieć wirtualną + Utwórz nową sieć wirtualną

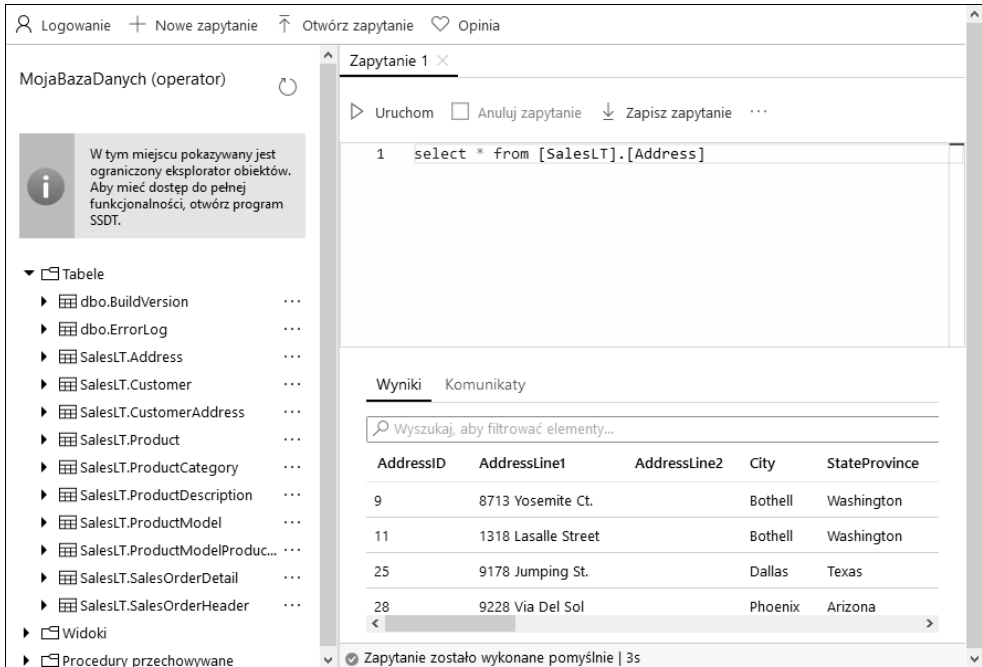
Nazwa reguły	Sieć wirtual...	Podsieć	Zakres adr...	Stan punkt...	Grupa zasob...	Subskrypcja	Stan
Brak reguł sieci wirtualnej dla tego serwera.							

Po skonfigurowaniu adresu można połączyć się z bazą za pomocą programu SQL Server Management Studio. Należy zwrócić uwagę, że tym razem dostępnych będzie mniej opcji niż w przypadku bazy wdrożonej lokalnie. W programie będą widoczne tylko trzy sekcje: *Databases*, *Security* i *Integration Services Catalogs*. Ilustruje to poniższy rysunek:



Na szczęście portal Azure oferuje mnóstwo opcji do zarządzania bazą, więc większość potrzebnych funkcjonalności jest dostępna. Dzięki temu zarządzanie bazą Azure SQL Database i utrzymanie jej jest wyjątkowo proste.

Pierwszą unikatową opcją w widoku bazy danych SQL jest *Edytor zapytań (wersja zapoznawcza)*. Dzięki edytorowi nie jest potrzebny program SQL Server Management Studio, ponieważ za pomocą przeglądarki można wysyłać do bazy dowolne zapytania, jak również wykonywać inne operacje. Oto widok edytora zapytań:



W sekcji *Ustawienia* znajdują się typowe opcje: *Konfiguruj*, *Właściwości*, *Blokady* i *Eksportuj szablon*, jak również unikatowe: *Replikacja geograficzna*, *Parametry połączeń*, *Synchronizuj z innymi bazami danych* oraz *Dodawanie usługi Azure Search*. Za pomocą opcji *Synchronizuj z innymi bazami danych* tworzy się grupy synchronizacji. Umieszczone w tych grupach bazy są automatycznie synchronizowane. Opcja *Dodawanie usługi Azure Search* służy do łączenia bazy z usługą oferującą wyszukiwanie pełnotekstowe, dodatkowe formaty kodowania i rozszerzone opcje konfiguracyjne.

Po wybraniu opcji *Konfiguruj* można zmienić warstwę cenową. Pojawi się taki sam widok jak podczas tworzenia bazy. Ilustruje to rysunek na następnej stronie.

W opcji *Parametry połączeń* znajdują się ciągi służące do nawiązywania połączeń z bazą za pomocą programów napisanych w różnych językach. Przykładowy ciąg dla platformy ADO.NET wygląda następująco:

```
Server=tcp:moj-serwer.database.windows.net,1433;Initial
↳Catalog=MojaBazaDanych;Persist Security Info=False;User
↳ID=operator;Password={your_password};MultipleActiveResultSets=False;Encrypt=True;
↳TrustServerCertificate=False;Connection Timeout=30;
```

Warstwa obliczeniowa

Obsługiwane administracyjnie

Zasoby obliczeniowe są wstępnie przydzielane

Rozliczane co godzinę na podstawie skonfigurowanych rdzeni wirtualnych

Bezserwerowe

Zasoby obliczeniowe są skalowane automatycznie

Rozliczane co godzinę na podstawie użytych rdzeni wirtualnych

Sprzęt do obliczeń

Kliknij pozycję „Zmień konfigurację”, aby wyświetlić szczegóły dotyczące wszystkich dostępnych generacji sprzętu, w tym opcji zoptymalizowanych pod kątem pamięci i obliczeń

Konfiguracja sprzętu

5. generacji

do 80 rdzeni wirtualnych, do 408 GB pamięci

Zmień konfigurację

Oszczędność pieniędzy

Oszczędzaj do 55% dzięki licencji, która już masz. Masz już licencję na program SQL Server? Tak Nie


Rdzenie wirtualne Czym różnią się rdzenie wirtualne od jednostek DTU? [id](#)

2 Rdzenie wirtualne

Maksymalny rozmiar danych

1 GB 1 TB 1 GB

307,2 MB PRZYDZIELONE MIEJSCE NA DZIENNIKI



Podsumowanie kosztów

5. generacji — Przeznaczenie ogólne (GP_Gen5_2)	
Koszt na rdzeń wirtualny (w EUR)	167,77
Liczba wybranych: Rdzenie wirtualne	x 2
Koszt na GB (w EUR)	0,12
Wybrano: Max storage (w GB)	x 1,3
SZACOWANY KOSZT MIESIĘCZNY	335,70 EUR


Tworzenie wysokodostępnej bazy Azure SQL Database

Tworzenie wysokodostępnego serwera SQL Server jest skomplikowaną operacją, a konfiguracja i utrzymanie samego serwera oraz zarządzanie nim to trudne zadanie. Natomiast osiągnięcie wysokiej dostępności bazy Azure SQL Database jest o wiele prostsze, a sama baza niemal nie wymaga utrzymania.

Aby utworzyć wysokodostępną bazę danych, kliknij opcję *Replikacja geograficzna*. Pojawi się widok z mapą świata, na której będą zaznaczone centra danych, z których wszystkie można wykorzystać do replikowania bazy. Centra, w których znajdują się utworzone bazy, są wyróżnione kolorem niebieskim, a centra zalecane do replikacji — fioletowym. Widoczna jest też informacja o bazie podstawowej. Oto widok opcji *Replikacja geograficzna* (zobacz pierwszy rysunek na następnej stronie).

Aby utworzyć replikę bazy, kliknij na liście dowolne centrum. Otworzy się nowy widok, w którym musisz wskazać docelowy serwer (jeżeli go nie ma, utwórz go). W polu *Nazwa bazy danych* będzie widoczna nazwa oryginalnej bazy, której nie można zmieniać. Warstwa cenowa również będzie taka sama jak oryginalna, ale możesz wpisać inną. Oto przykładowe ustawienia zapasowej bazy danych (zobacz drugi rysunek na następnej stronie).

i Możesz teraz automatycznie zarządzać replikacją, łącznością i przechodzeniem w tryb failover tej bazy danych, dodając ją do grupy trybu failover.



	Serwer/Baza danych	Zasady pracy w trybie failover	Stan
Podstawowy			
<input checked="" type="checkbox"/>	Europa Zachodnia	moj-serwer/MojaBazaDanych	Brak
			Online

Tworzenie pomocniczej b...

Utwórz replikowane geograficznie pomocnicze bazy danych, aby zapewnić ochronę przed długimi przestojami centrum danych. Pomocnicze bazy danych mają wpływ na cenę. [Dowiedz się więcej?](#)

Region

Nazwa bazy danych

*Typ pomocniczej bazy danych

*Serwer docelowy

Pula elastyczna

*Warstwa cenowa

Czas wdrażania repliki bazy zależy od wielkości oryginalnej bazy. W trakcie procesu w wskazanym centrum tworzona jest pusta baza, do której następnie są kopiowane dane z bazy podstawowej. Na koniec na mapie pojawia się połączenie między bazami podstawową i zapasową. Oto zreplikowana baza danych:

i Możesz teraz automatycznie zarządzać replikacją, łącznością i przechodzeniem w tryb failover tej bazy danych, dodając ją do grupy trybu failover.



	Serwer/Baza danych	Zasady pracy w trybie failover	Stan
Podstawowy			
<input checked="" type="checkbox"/>	Europa Zachodnia	moja-baza/MojaBazaDanych	Brak
Pomocnicze bazy danych			
<input checked="" type="checkbox"/>	East US	moj-serwer2/MojaBazaDanych	Możliwość... ***

Pamiętaj, że kopia bazy podstawowej jest dostępna tylko w trybie do odczytu. W razie awarii lub niedostępności bazy podstawowej trzeba ręcznie przestawić bazę zapasową w tryb odczytu i zapisu, jak również zastosować inny ciąg umożliwiający łączenie się z bazą. Rozwiązanie to nie zapewnia więc wysokiej dostępności. W tym celu trzeba wykonać dodatkową operację — utworzyć grupę trybu *failover*. Aby to zrobić, w widoku serwera kliknij opcję *Grupy trybu failover*, a następnie ikonę *Dodaj grupę*. Pojawi się widok *Grupa trybu failover*, w którym musisz podać nazwę grupy i serwer pomocniczy i wybrać zasadę trybu, okres prologaty odczytu i zapisu oraz bazę danych w grupie. Nazwa grupy musi być unikatowa, ponieważ zostanie użyta w punkcie końcowym umożliwiającym odwoływanie się do bazy. Odwołania do grupy będą automatycznie kierowane do serwera podstawowego. Jeżeli nie będzie on dostępny, odwołania będą kierowane do serwera zapasowego. Przełączanie pomiędzy obydwojema serwerami będzie się odbywać automatycznie. Oto przykładowe ustawienia grupy trybu *failover* (zobacz rysunek na następnym stronie).

Jak widać, tworzenie wysokodostępnej bazy Azure SQL Database jest proste i szybkie. Jeżeli konfigurowałeś podobne rozwiązanie w lokalnym środowisku, przyznasz, że jest to skomplikowany proces.

Grupa trybu failover
□ ×

Utwórz grupę trybu failover w celu automatycznego przełączania w tryb failover znajdujących się w niej baz danych.

Nazwa grupy trybu failover *
 ✓
 .database.windows.net

*Serwer pomocniczy >

Zasady trybu failover odczytu/zapisu
 ▼

Okres prolongaty odczytu/zapisu (w godzinach)
 ▼

Baza danych w grupie >
 1 / 1

Bezpieczeństwo bazy Azure SQL Database

Bezpieczeństwo danych jest bardzo ważne (co nie oznacza, że inne zasoby mogą pozostać niezabezpieczone). W widoku bazy danych SQL znajduje się sekcja *Zabezpieczenia*, zawierająca opcje *Advanced Data Security* (zaawansowane bezpieczeństwo danych), *Inspekcja*, *Dynamiczne maskowanie danych* i *Transparent Data Encryption* (przezroczyste szyfrowanie danych). Opcje *Advanced Data Security*, *Inspekcja* i *Transparent Data Encryption* można stosować na poziomie serwera (dotyczą wtedy wszystkich wdrożonych w nim baz) lub pojedynczej bazy.

W widoku opcji *Advanced Data Security* znajdują się trzy panele:

- *Odnajdywanie i klasyfikacja danych*,
- *Ocena luk w zabezpieczeniach*,
- *Zaawansowana ochrona przed zagrożeniami*.

Funkcjonalności oferowane w panelu *Odnajdywanie i klasyfikacja danych* są bardzo przydatne. Skanują bazę danych i rekomendują kolumny do sklasyfikowania. Jest to szczególnie użyteczna funkcjonalność, jeżeli baza zawiera dane osobowe podlegające przepisom RODO.

Panel *Ocena luk w zabezpieczeniach* umożliwia skanowanie bazy pod kątem bezpieczeństwa i dostarcza rekomendacji w tym zakresie, np. włączenie śledzenia reguł zapory lub sklasyfikowanie poufnych danych.

W funkcjonalnościach dostępnych w panelu *Zaawansowana ochrona przed zagrożeniami* wykorzystane są techniki uczenia maszynowego, które analizują działanie bazy i alarmują o odstępstwach od normy. Jeżeli na przykład logowanie do bazy zazwyczaj odbywa się w godzinach pracy i ktoś zaloguje się o innej porze, zostanie zgłoszony alarm. Innym przykładem anomalii jest próba zalogowania się do bazy za pomocą komputera, którego adres IP jest inny niż uznany za bezpieczny, bo na przykład znajduje się w innej części świata. W takim wypadku też może być zgłaszany alarm.

Oto widok opcji *Advanced Data Security*:

The screenshot displays three panels from the Advanced Data Security interface:

- Odnajdywanie i klasyfikacja danych:** Shows 0 total findings. Below is a table of recommended columns for classification:

Kolumna	Etykieta poufności
FirstName	Confidential - GDPR
LastName	Confidential - GDPR
EmailAddress	Confidential
- Ocena luk w zabezpieczeniach:** Shows 7 total findings. It includes a section for 'Sprawdzenia zakończone niepowodzeniem' (Checks completed with failure) with a table:

SPRAWDZANIE ZABEZPIECZEŃ	RY...
Auditing should be enabled at the server...	High
Server-level firewall rules should be track...	High
'dbo' user should not be used for norma...	Me...
- Zaawansowana ochrona przed zagrożeniami:** Shows 0 total alerts. It includes a table for 'Alerty zabezpieczeń' (Security alerts) with columns for 'Opis' (Description) and 'Data' (Date). A note indicates 'Brak alertów i zaleceń do wyświetlenia.' (No alerts or recommendations to display).

Opcja *Inspekcja* służy do śledzenia zdarzeń i rejestrowania ich w magazynie. Można określić okres przechowywania informacji o zdarzeniach oraz włączyć lub wyłączyć inspekcję na poziomie serwera. Ponieważ wiele firm i instytucji podlega obowiązkowemu audytowaniu pod kątem zgodności z różnymi standardami, opcja ta może okazać się dla nich szczególnie przydatna. Oto widok opcji *Inspekcja*:

The screenshot shows the 'Rekordy inspekcji' (Inspection Records) page with the following details:

- Buttons: Odśwież, Filtruj, Log Analytics, Wyświetl pulpit nawigacyjny
- Information: Kliknij tutaj, aby dowiedzieć się więcej o metodach wyświetlania i analizowania rekordów inspekcji.
- Source: Źródło inspekcji (Inspekcja serwera, Inspekcja bazy danych)
- Display: Wyświetlanie rekordów inspekcji do Wed, 22 Jan 2020 12:21:18 UTC.
- Action: Uruchom w edytorze zapytań
- Table of records:

Czas zdarzenia (UTC)	Nazwa główna	Typ zdarzenia	Stan akcji
1/22/2020 5:21:15 PM	operator	RPC COMPLETED	Succeeded
1/22/2020 5:21:15 PM	operator	RPC COMPLETED	Succeeded

Zanim zajmiemy się opcją *Dynamiczne maskowanie danych*, wyślijmy do bazy proste zapytanie zwracające 1000 pierwszych wierszy z tabeli SalesLT.Customers. Tabela ta zawiera różnego rodzaju dane o klientach, do których nie wszyscy powinni mieć dostęp. Przykładem jest numer telefonu (kolumna Phone). Jak pokazuje poniższy rysunek, zapytanie zwraca numery telefonów klientów:

The screenshot shows a SQL query execution interface. At the top, there are buttons for 'Uruchom', 'Anuluj zapytanie', 'Zapisz zapytanie', 'Eksportuj dane jako .json', and a menu icon. Below the buttons is the SQL query:

```

1 SELECT TOP (1000) [CustomerID]
2     , [NameStyle]
3     , [Title]
4     , [FirstName]
5     , [MiddleName]
6     , [LastName]
7     , [Suffix]
8     , [CompanyName]
9     , [SalesPerson]
10    , [EmailAddress]
11    , [Phone]
12    , [PasswordHash]
13    , [PasswordSalt]
14    , [Password]

```

Below the query, there are tabs for 'Wyniki' and 'Komunikaty'. The 'Wyniki' tab is active, showing a table with the following data:

CompanyName	SalesPerson	EmailAddress	Phone
A Bike Store	adventure-works\pamela0	orlando0@adventure-works.com	245-555-0173
Progressive Sports	adventure-works\david8	keith0@adventure-works.com	170-555-0127
Advanced Bike Components	adventure-works\jillian0	donna0@adventure-works.com	279-555-0130
Modular Cycle Systems	adventure-works\jillian0	janet1@adventure-works.com	710-555-0173
Metropolitan Sports Supply	adventure-works\shu0	lucy0@adventure-works.com	828-555-0186
Aerobic Exercise Company	adventure-works\linda3	rosmarie0@adventure-works.com	244-555-0112
Associated Bikes	adventure-works\shu0	dominic0@adventure-works.com	192-555-0173

Opcja *Dynamiczne maskowanie danych* zawiera listę kolumn, których maskowanie jest zalecane. Można tu również zdefiniować własne reguły maskowania. Zwróć uwagę, że zabezpieczenie to nie dotyczy administratora. Można wskazać innych użytkowników, którzy będą wykluczeni z maskowania. Oto widok opcji *Dynamiczne maskowanie danych* (zobacz pierwszy rysunek na następnej stronie).

Aby zdefiniować nową regułę, należy wskazać schemat bazy, tabelę, kolumnę i format pola z maskowaniem. Ostatnie ustawienie określa, jak mają wyglądać w wynikach zapytania zamaskowane dane. Oto przykładowa reguła maskująca kolumnę zawierającą numery telefonów (zobacz drugi rysunek na następnej stronie)

Zapisz Odrzuć Dodaj maskę Opinia

Dowiedz się więcej — przewodnik Wprowadzenie

Reguły maskowania

Nazwa maski	Funkcja maskowania
Nie utworzono żadnych reguł maskowania.	

Użytkownicy SQL wykluczeni z maskowania (administratorzy są zawsze wykluczeni)

Użytkownicy SQL wykluczeni z maskowania (administratorzy są zawsze wykluczeni) ✓

Zalecane pola do zamaskowania

Schemat	Tabela	Kolumna	
SalesLT	Customer	FirstName	Dodaj maskę
SalesLT	Customer	LastName	Dodaj maskę
SalesLT	Customer	EmailAddress	Dodaj maskę
SalesLT	Customer	Phone	Dodaj maskę

Dodaj regułę masko...

Dodaj Odrzuć Usuń

Nazwa maski
SalesLT_Customer_Phone

Wybierz, co ma być maskowane

Schemat
SalesLT

Tabela
Customer

Kolumna
Phone (nvarchar)

Wybierz sposób maskowania

Format pola z maskowaniem
Ciąg niestandardowy (prefiks [dopeł...

Ujawniany prefiks
0

Ciąg wypełnienia
xxx

Ujawniany sufiks
0

Po zdefiniowaniu reguły należy ponownie wykonać zapytanie. Jak pokazuje poniższy rysunek, po zastosowaniu reguły maskującej zapytanie zwraca inne wyniki niż poprzednio — teraz kolumna Phone zawiera znaki xxx:

▶ Uruchoń Anuluj zapytanie ↓ Zapisz zapytanie ↓ Eksportuj dane jako .json ...

```

1 SELECT TOP (1000) [CustomerID]
2     , [NameStyle]
3     , [Title]
4     , [FirstName]
5     , [MiddleName]
6     , [LastName]
7     , [Suffix]
8     , [CompanyName]
9     , [SalesPerson]
10    , [EmailAddress]
11    , [Phone]
12    , [PasswordHash]
13    , [PasswordSalt]
14    , [Password]
    
```

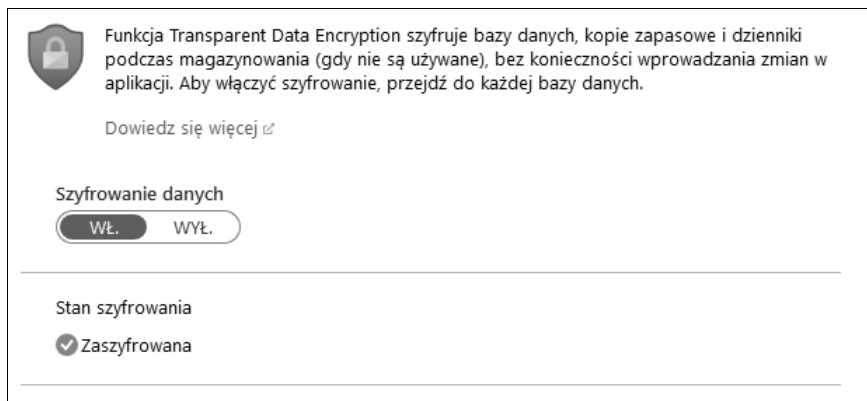
Wyniki Komunikaty

CompanyName	SalesPerson	EmailAddress	Phone
A Bike Store	adventure-works\pamela0	orlando0@adventure-works.com	xxx
Progressive Sports	adventure-works\david8	keith0@adventure-works.com	xxx
Advanced Bike Components	adventure-works\jillian0	donna0@adventure-works.com	xxx
Modular Cycle Systems	adventure-works\jillian0	janet1@adventure-works.com	xxx
Metropolitan Sports Supply	adventure-works\shu0	lucy0@adventure-works.com	xxx
Aerobic Exercise Company	adventure-works\linda3	rosmarie0@adventure-works.com	xxx
Associated Bikes	adventure-works\shu0	dominic0@adventure-works.com	xxx

Za pomocą opisanej opcji można kontrolować dostęp użytkowników do danych i ograniczać im wgląd w poufne informacje. Załóżmy, że mamy w bazie tabelę zawierającą numery kart kredytowych i informacje kontaktowe klientów. Pracownicy działu sprzedaży mogą widzieć adresy e-mail i numery telefonów, ale nie mogą widzieć numerów kart kredytowych. Natomiast pracownicy działu finansowego mogą mieć wgląd w numery kart. W takim przypadku doskonale sprawdzają się reguły dynamicznego maskowania danych, dzięki którym różni użytkownicy mający dostęp do tej samej tabeli będą widzieć różne dane.

Opcja *Transparent Data Encryption* służy do szyfrowania bazy danych, kopii zapasowych i dzienników. Można ją stosować, gdy baza nie jest używana. Funkcjonalność szyfrowania jest dostępna w lokalnie wdrożonym serwerze SQL Server, jednak zaimplementowanie jej nie jest proste. Natomiast wszystkie tworzone bazy Azure SQL Database mają domyślnie włączone

szyfrowanie. W przeszłości szyfrowanie nie było stosowane, ale wystarczyło użyć tej opcji, aby je włączyć. Oto widok opcji *Transparent Data Encryption*:



Monitorowanie i diagnostyka bazy Azure SQL Database

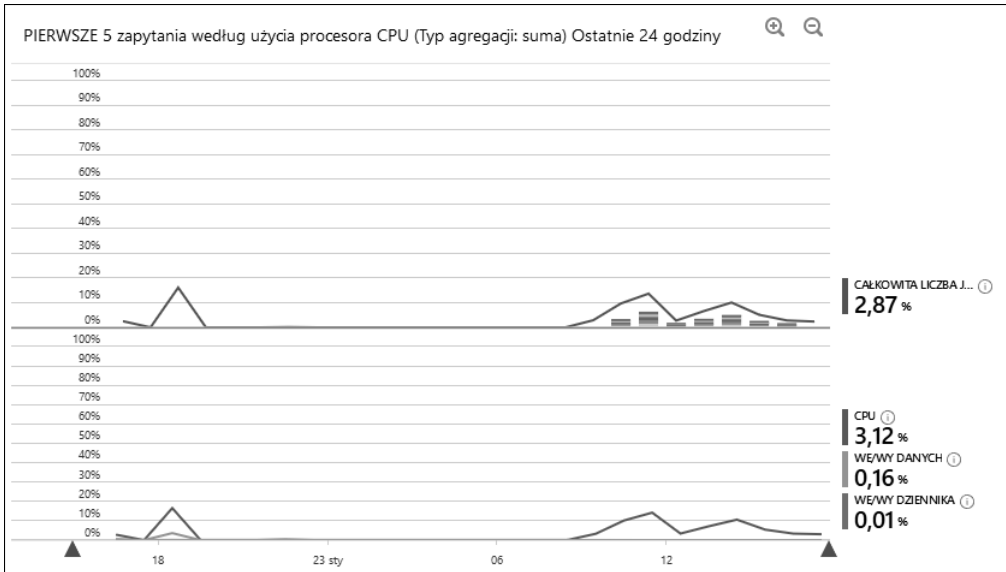
Sekcja *Monitorowanie* w widoku bazy Azure SQL Database jest bardzo podobna do analogicznej sekcji w innych zasobach. Dostępne są w niej opcje *Alerty*, *Metryki*, *Ustawienia diagnostyczne* i *Dzienniki*, takie same jak w maszynach wirtualnych i aplikacjach internetowych opisanych w poprzednich rozdziałach.

Sekcja *Pomoc i rozwiązywanie problemów* zawiera opcje *Kondycja zasobu* i *Nowy wniosek o pomoc techniczną*, identyczne jak w innych zasobach.

Sekcją charakterystyczną dla bazy Azure SQL Database jest *Inteligentna wydajność* zawierająca opcje *Przegląd wydajności*, *Zalecenie dotyczące wydajności*, *Szczegółowe informacje o wydajności zapytań* oraz *Dostrajanie automatyczne*.

Opcja *Przegląd wydajności* zawiera ogólne informacje o wydajności zapytań. Znajdują się tu wykresy przedstawiające wykorzystanie zasobów przez zapytania: liczbę zużytych jednostek DTU, obciążenie procesora oraz liczbę wykonanych operacji wejścia/wyjścia dla danych i dzienników. Uwzględnione są tu zapytania, które wykorzystują najwięcej zasobów. Ponieważ dane są zagregowane, na wykresie mogą znajdować się zapytania, które zużywają niewiele zasobów, ale są często wykonywane. Oto widok obciążenia procesora znajdujący się w zakładce *Przegląd wydajności* (zobacz pierwszy rysunek na następnej stronie).

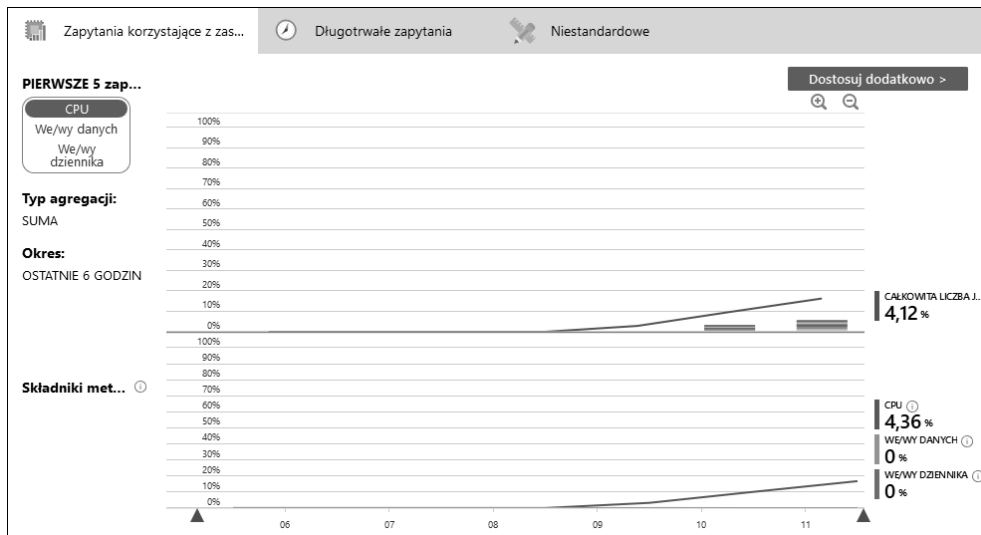
W opcji *Zalecenie dotyczące wydajności* znajdują się zalecenia dotyczące poprawy wydajności bazy, które można od razu zastosować. Zalecenia są tworzone na podstawie historii wydajności. Widok opcji zawiera listy zaleceń nowych i zastosowanych (zobacz drugi rysunek na następnej stronie).



Zalecenia							
Akcja	↑↓	Opis rekomendacji	↑↓	Wpływ			
Przeanalizowaliśmy Twoją bazę danych i stwierdziliśmy, że została ona niedawno utworzona. W tej chwili nie mamy żadnych rekomendacji do przedstawienia.							
Historia dostrajania							
Akcja	↑↓	Opis rekomendacji	↑↓	Stan	↑↓	Czas	↑↓
Brak operacji do wyświetlenia. Po zastosowaniu rekomendacji jej stan będzie widoczny w tym miejscu.							

W opcji *Szczegółowe informacje o wydajności zapytań* znajduje się zakładka *Zapytania korzystające z zasobów*, która zawiera bardzo podobne informacje jak w opcji *Przegląd wydajności*. Różnica polega jedynie na tym, że w tej zakładce można dostosowywać wykresy i tabele, np. wybierać inne wskaźniki i przedziały czasu. Dzięki temu można obserwować wydajność bazy w dłuższych okresach. Zakładka *Długotrwałe zapytania* zawiera listę zapytań, które są wykonywane dłużej niż inne. Zazwyczaj tego rodzaju zapytania zużywają więcej zasobów, więc odpowiednio je modyfikując można zwiększyć ich wydajność i w konsekwencji w dłuższej perspektywie zaoszczędzić pieniądze. Oto przykładowy widok opcji *Szczegółowe informacje o wydajności zapytań* (zobacz pierwszy rysunek na następnej stronie).

Opcja *Dostrajanie automatyczne* zawiera funkcjonalności, o których marzą wszyscy administratorzy baz danych. Wykorzystując techniki uczenia maszynowego, obserwują przez dłuższy czas działanie bazy danych i stosują rozwiązania zwiększające jej wydajność. Dostępne są następujące opcje dostrajania automatycznego: **WYMUSZ PLAN**, **UTWÓRZ INDEKS** i **USUŃ INDEKS**. Ustawienia te można włączać na poziomie serwera lub subskrypcji, jak również włączać i wyłączać indywidualnie dla poszczególnych baz. Oto widok opcji *Dostrajanie automatyczne* (zobacz drugi rysunek na następnej stronie).



Dostrajanie automatyczne

Zastosuj | Przywróć wartości domyślne

Wbudowane funkcje inteligentne usługi Azure SQL Database automatycznie dostrajają bazy danych w celu zoptymalizowania wydajności. Kliknij tutaj, aby dowiedzieć się więcej na temat automatycznego dostrajania.

Dziedzicz z: Serwer Ustawienia domyślne platformy Azure Bez dziedziczenia

i Baza danych dziedziczy konfigurację dostrajania automatycznego z serwera. Można ustawić konfigurację, która ma być dziedziczona, przechodząc do: Ustawienia dostrajania serwera

⚠ Baza danych dziedziczy ustawienia z serwera, ale serwer jest w stanie nieokreślonym. Określ stan automatycznego dostrajania na serwerze.

Skonfiguruj opcje dostrajania automatycznego

Opcja	Żądany stan	Bieżący stan
WYMUSZ PLAN	WŁ. WYŁ. DZIEDZICZ	OFF Dziedziczone z serwera
UTWÓRZ INDEKS	WŁ. WYŁ. DZIEDZICZ	OFF Dziedziczone z serwera
USUŃ INDEKS	WŁ. WYŁ. DZIEDZICZ	OFF Dziedziczone z serwera

Tworzenie kopii zapasowej bazy Azure SQL Database

Bardzo ważnym zadaniem każdego administratora bazy danych jest tworzenie jej kopii zapasowej. Kopie bazy Azure SQL Database są tworzone automatycznie. Jest to bezpłatna funkcjonalność. Wraz z nową bazą tworzony jest geograficznie nadmiarowy magazyn, w którym zapisywane są kopie pełne, różnicowe i transakcyjne. Kopie transakcyjne są tworzone co 12 godzin, a różnicowe co 5 – 10 minut, w zależności od wielkości i aktywności bazy. Dzięki temu można przywracać bazę do stanu, w jakim znajdowała się w określonym punkcie czasu.

Najpierw dane odtwarza się z pełnej kopii, następnie dane zmienione od chwili wykonania pełnej kopii do zadanego punktu odtwarza się z kopii różnicowej i na koniec dane zmienione od chwili wykonania kopii różnicowej do zadanego punktu odtwarza się z kopii transakcyjnej.

Okres przechowywania kopii zapasowej zależy od wybranej warstwy cenowej i waha się od 7 do 35 dni. Dostępna jest też opcja *długoterminowego* przechowywania kopii, nawet do 10 lat. Jest ona bardzo przydatna, ponieważ zdarzają się sytuacje, w których wymagany jest długi czas przechowywania danych. Opcja ta jest płatna, jednak zważywszy na niskie koszty magazynu, nie wpływa znacząco na wysokość rachunku.

Inną funkcjonalnością bezpośrednio związaną z kopią zapasową jest eksport bazy. Dzięki niemu można tworzyć dodatkowe kopie w osobnych magazynach i odtwarzać je na innych serwerach lub w osobnych subskrypcjach. Podczas eksportu tworzony jest plik BACPAC zawierający schemat bazy i właściwe dane.

Inne usługi przetwarzania danych w chmurze Azure

Maszyna wirtualna z serwerem SQL Server oraz baza Azure SQL Database to tylko fragment oferty przetwarzania danych w chmurze Azure.

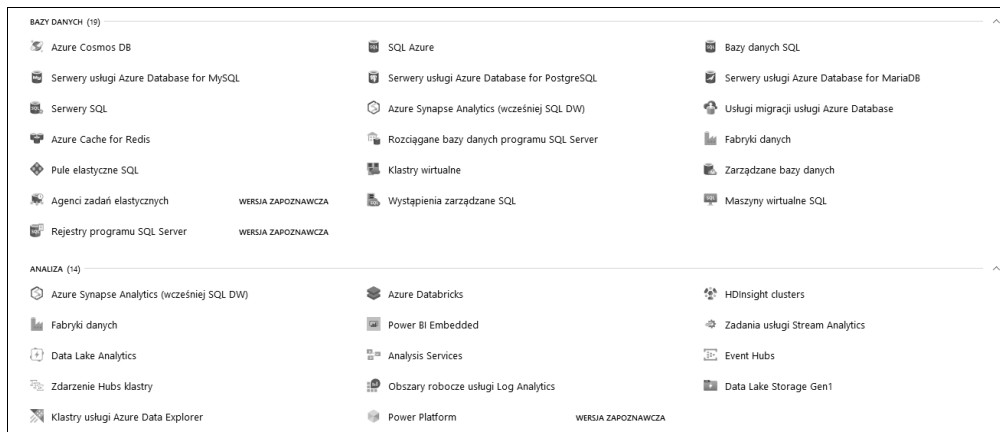
Relacyjne bazy danych tworzone w modelu IaaS nie mają żadnych ograniczeń. Można wdrażać dowolne maszyny oparte na różnych systemach operacyjnych i instalować w nich dowolne oprogramowanie, np. Oracle, MySQL czy PostgreSQL. Dostępnych jest też wiele obrazów maszyn z już zainstalowanym oprogramowaniem. Podobnie jest z bazami typu NoSQL: można je samodzielnie instalować w maszynach wirtualnych albo użyć gotowego obrazu z bazą MongoDB, CouchDB lub inną.

W modelu PaaS dostępne są relacyjne bazy danych takie jak MySQL, PostgreSQL, hurtownie danych i inne. Można też korzystać z baz typu NoSQL, np. Cosmos DB lub MongoDB.

Ponadto chmura Azure oferuje szeroki wachlarz usług analitycznych dostępnych zarówno w modelu IaaS, jak i PaaS.

Na platformie Microsoft Azure dostępnych jest wiele funkcjonalności przetwarzania i analizowania danych, migrowania istniejących baz oraz tworzenia nowych. Można stosować dowolne kombinacje usług w modelach IaaS i PaaS, dostosowywać je do specyficznych wymagań i uzyskiwać w ten sposób najlepsze możliwe efekty.

Oto część opcji służących do przetwarzania i analizowania danych w chmurze Azure:



Podsumowanie

Platforma Azure oferuje wiele opcji przetwarzania danych w modelach IaaS i PaaS. Pierwszy model daje większą kontrolę nad bazą, ale wymaga większego nakładu pracy związanego z administrowaniem i utrzymywaniem. Natomiast model PaaS oferuje więcej funkcjonalności ułatwiających pracę, ale nie pozwala na korzystanie ze starszych funkcjonalności i aplikacji. Dokonując wyboru modelu dla tworzonego rozwiązania, należy więc rozważyć wymagane i dostępne opcje.

Chmura Azure oferuje wiele funkcjonalności analizy danych rozszerzających tworzone rozwiązania. Tutaj też można wybierać między modelami IaaS i PaaS.

W poprzednich rozdziałach opisałem możliwości tworzenia nowych aplikacji i baz danych w chmurze Azure. Choć są to niewątpliwie bardzo ważne funkcjonalności, nie zawsze są przydatne. Najczęściej podróż ku chmurze polega na przenoszeniu do niej rozwiązań istniejących w lokalnym środowisku. W następnym rozdziale zajmiemy się dostępnymi opcjami migrowania aplikacji i baz danych do chmury Azure.

Pytania

1. Bazy danych w chmurze Azure można tworzyć w modelu:
 - a) IaaS
 - b) PaaS
 - c) w obu

2. Maszyna wirtualna z serwerem SQL Server różni się od maszyny bez serwera:
 - a) konfiguracją
 - b) wielkością pamięci i liczbą rdzeni procesora
 - c) nazwą
3. Baza Azure SQL Database jest również określania mianem modelu:
 - a) Database as a Service
 - b) SQL as a Service
 - c) Data as a Service
4. Warstwę cenową bazy Azure SQL Database określa:
 - a) liczba jednostek DTU
 - b) liczba wirtualnych rdzeni procesora
 - c) oba powyższe
5. Zapytania do bazy Azure SQL Database można wysyłać za pomocą:
 - a) programu SQL Server Management Studio
 - b) edytora zapytań w portalu Azure
 - c) obu narzędzi
6. Aby połączyć się z bazą Azure SQL Database, należy:
 - a) utworzyć regułę zapory zawierającą adres IP
 - b) wskazać legalny adres IP w ustawieniach sieci wirtualnej
 - c) wskazać legalny adres IP w ustawieniach głównej bazy danych
7. Aby utworzyć replikę bazy Azure SQL Database, należy:
 - a) utworzyć kopię bazy
 - b) wyeksportować bazę
 - c) skonfigurować replikację geograficzną bazy
8. Aby uzyskać wysoką dostępność bazy Azure SQL Database, należy:
 - a) utworzyć grupę trybu *failover*
 - b) utworzyć klaster trybu *failover*
 - c) użyć opcji *Zawsze włączone*
9. Do maskowania kolumn danych w bazie Azure SQL Database wykorzystuje się:
 - a) przezroczyste szyfrowanie danych
 - b) dynamiczne maskowanie danych
 - c) klasyfikowanie danych
10. Do wykrywania potencjalnych zagrożeń bazy danych stosuje się:
 - a) ocenę luk w zabezpieczeniach
 - b) zaawansowaną ochronę przed zagrożeniami
 - c) obie funkcjonalności

PROGRAM PARTNERSKI

— GRUPY HELION —

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

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

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

GRUPA
Helion 

Chmura Azure: przenieś swój system na wyższy poziom!

Decyzja o przeniesieniu zasobów informatycznych do chmury jest podejmowana najczęściej wtedy, gdy niezawodność i bezpieczeństwo systemu są dla firmy sprawą kluczową. Jeśli chodzi o rozwiązania oparte na chmurze obliczeniowej, warto zainteresować się Azure. Azure udostępnia takie usługi, by umożliwić rozbudowę i monitorowanie aplikacji, baz danych czy innych usług oraz zarządzanie nimi w sposób globalny. Pozwala na ciągłe dostarczanie znakomitych, innowacyjnych rozwiązań. Umożliwia wirtualizację rozmaitych systemów, takich jak Windows, Linux, dystrybucje serwerowe, strony WWW, aplikacje ASP .NET, systemy CMS, bazy danych czy rozproszone klastry obliczeniowe.

Oto praktyczne wprowadzenie do Azure. Wyjaśniono tu wiele pojęć potrzebnych w pracy administratora, takich jak sieci wirtualne oraz koncepcja IaaS. Omówiono zasady pracy z Azure oraz pokazano, jak można przygotować platformę do wdrożenia własnego systemu. Od strony praktycznej przedstawiono tworzenie zaawansowanych usług w Azure. Sporo miejsca poświęcono najważniejszym kwestiom bezpieczeństwa i administracji, zaprezentowano też szereg dobrych praktyk, a także sporo technik ułatwiających rozwiązywanie najczęstszych problemów. Książka jest napisana w zwięzły i przystępny sposób. Dzięki niej szybko i skutecznie zaczniesz administrować zasobami w chmurze Azure.

W tej książce między innymi:

- podstawowe pojęcia, koncepcje i modele związane z chmurą obliczeniową
- tworzenie i konfiguracja wirtualnej maszyny Azure
- praca z bazami danych, usługi IaaS i PaaS
- usługi hybrydowe, implementacja i zarządzanie
- tożsamość i bezpieczeństwo zasobów w chmurze Azure

Mustafa Toroman jest architektem oprogramowania z wieloletnim doświadczeniem w projektowaniu i monitorowaniu rozwiązań infrastrukturalnych. Obecnie zajmuje się wdrażaniem systemów opartych na chmurze. Interesuje się procesami DevOps, jest entuzjastą koncepcji IaC. Posiada ponad 30 certyfikatów Microsoft, od niemal dekady jest certyfikowanym trenerem. Często występuje na międzynarodowych konferencjach poświęconych technologiom chmurowym. Kilukrotnie otrzymał tytuł MVP w dziedzinie platformy Microsoft Azure.

	<i>Sprawdź nasze szkolenia!</i>	KOD KORZYŚCI Sięgnij po więcej! ▶	
 helion.pl	 AKADEMIA IT & BUSINESS	ISBN 978-83-283-6483-7	
 0 801 339900		WWW.SZKOLENIA.HELION.PL	
 0 601 339900	INFORMATYKA W NAJLEPSZYM WYDANIU	Cena: 67,00 zł	

Packt