

O'REILLY®

Helion 

Poznaj Microsoft Azure

Praktyczny przewodnik
po chmurze obliczeniowej
i programowaniu



Jonah Andersson

Tytuł oryginału: Learning Microsoft Azure: Cloud Computing and Development Fundamentals

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-289-1347-9

© 2024 Helion S.A.

Authorized Polish translation of the English edition of *Learning Microsoft Azure* ISBN 9781098113322 © 2024 Jonah Carrio Andersson.

This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same.

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

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

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

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

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<https://helion.pl/user/opinie/pomiaz>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:

<https://ftp.helion.pl/przyklady/pomiaz.zip>

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: <https://helion.pl> (księgarnia internetowa, katalog książek)

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Przedmowa — Magnus Mårtensson	21
Przedmowa — Thomas Maurer	23
Wprowadzenie	25

Część I. Podstawy przetwarzania w chmurze i zastosowanie platformy Microsoft Azure 37

1. Podstawy przetwarzania w chmurze obliczeniowej	39
Czym jest chmura obliczeniowa?	39
Korzyści z zastosowania chmury obliczeniowej w inżynierii oprogramowania i usługach IT	40
Chmura obliczeniowa a wirtualizacja	42
Cloud Hypervisor — klucz do wirtualizacji w chmurze	43
Ewolucja chmur obliczeniowych	44
Podróż do nowoczesnej chmury	46
Modele wdrażania chmury obliczeniowej	47
Chmura publiczna	48
Chmura prywatna	49
Chmura społecznościowa	50
Chmura hybrydowa	52
Czym jest konfiguracja wielochmurowa?	53
Chmura hybrydowa a konfiguracja wielochmurowa	54
Dostawcy publicznej chmury obliczeniowej	56
Microsoft Azure	56
Amazon (AWS)	56
Google Cloud Platform	57
Oracle Cloud	57
Alibaba Cloud	57

Modele usług w chmurze	58
IaaS — infrastruktura jako usługa	58
PaaS — platforma jako usługa	58
SaaS — oprogramowanie jako usługa	59
Przetwarzanie bezserwerowe — funkcja jako usługa (FaaS) i zaplecze jako usługa (BaaS)	60
Kontenery jako usługa	62
Dane jako usługa	62
Model wspólnej odpowiedzialności w chmurze obliczeniowej i Azure	63
Model współodpowiedzialności oferuje korzyści w zakresie bezpieczeństwa w chmurze	64
Wydatki kapitałowe i wydatki operacyjne	65
Korzyści z wykorzystania nowoczesnych technologii chmurowych	66
Chmura obliczeniowa biznesu i klientów	66
Chmura obliczeniowa dla firm z branży IT	66
Podsumowanie	68
Sprawdź swoją wiedzę	68
Gdzie warto zajrzeć?	69
2. Podstawy Microsoft Azure	70
Microsoft Azure jako dostawca chmury publicznej	71
Microsoft Azure pomaga organizacjom zminimalizować koszty początkowe migracji	71
Zalety chmury obliczeniowej	72
Portal Azure	73
Funkcje portalu Azure	75
Usługi platformy Microsoft Azure	75
Przegląd podstawowych usług Azure	77
Usługi obliczeniowe na platformie Azure	77
Usługi sieciowe na platformie Azure	77
Podstawowe usługi Azure Storage	79
Podstawowe usługi Azure Database	80
Zarządzanie tożsamościami i usługi zabezpieczeń	80
Narzędzia dla deweloperów, monitorowanie i usługi DevOps	81
Migracja do chmury oraz usługi hybrydowe i wielochmurowe	82
Podstawowa architektura i koncepcje zarządzania zasobami w Microsoft Azure	83
Grupy zarządzania platformy Azure	83
Subskrypcje Azure	84
Grupy zasobów platformy Azure	84
Zasoby platformy Azure	85
Azure Resource Manager	86

Lokalizacje geograficzne, regiony, pary regionów i strefy dostępności platformy Azure	87
Lokalizacje geograficzne Azure	87
Regiony platformy Azure	87
Pary regionów Azure	88
Strefy dostępności platformy Azure	89
Zarządzanie kosztami w Microsoft Azure	90
Tożsamości użytkowników, role i usługa Active Directory na platformie Azure	91
Kontrola dostępu oparta na rolach Azure	92
Zrób to sam!	94
Microsoft Azure Portal — ćwiczenia praktyczne	94
Podsumowanie	95
Sprawdź swoją wiedzę	96
Gdzie warto zajrzeć?	96

Część II. Obliczenia, sieci, pamięć masowa i bazy danych **99**

3. Usługi obliczeniowe w chmurze Microsoft Azure	101
Usługi Azure Compute do tworzenia w pełni zarządzanych systemów	101
Maszyny wirtualne platformy Azure i zestawy skalowania maszyn wirtualnych	103
Maszyny wirtualne Azure	104
Zestawy skalowania maszyn wirtualnych platformy Azure	106
Opcje skalowania dla zestawów skalowania maszyn wirtualnych Azure	107
Usługa Azure App Service	108
Usługa Azure Web App for Containers	111
Usługa Static Web Apps	113
Kluczowe korzyści i zastosowania statycznych aplikacji internetowych na platformie Azure	113
Bezserwerowe usługi obliczeniowe	115
Korzyści z architektury bezserwerowej w chmurze	115
Usługa Azure Functions	116
Azure Durable Functions	117
Uruchamianie funkcji trwałych za pomocą wyzwalaczy orkiestracji	125
Typy funkcji trwałych — stanowe czy bezstanowe?	127
Usługi kontenerowe w Azure	134
Usługi Azure Containers i Azure Kubernetes	135
Usługa Azure Container Apps (ACA)	136
Obliczenia kwantowe na platformie Azure	141
Azure Quantum	142
Zrób to sam!	142

Podsumowanie	143
Sprawdź swoją wiedzę	144
Gdzie warto zajrzeć?	144
4. Usługi sieciowe Microsoft Azure Cloud Networking	145
Usługi sieciowe Azure	145
Kategorie usług sieciowych na platformie Azure	146
Usługi łączności	147
Usługi ochrony aplikacji	159
Usługi sieciowe platformy Azure na potrzeby dostarczania aplikacji	168
Usługi sieciowe Azure do monitorowania sieci	173
Usługa Azure Space — tworzenie sieci ponad chmurami	174
Zrób to sam!	176
Podsumowanie	177
Sprawdź swoją wiedzę	177
Gdzie warto zajrzeć?	177
5. Magazyny i bazy danych w chmurze Azure	179
Przechowywanie danych i bazy danych w chmurze	179
Zarządzanie przechowywaniem danych w chmurze	180
Zalety cyfrowej pamięci masowej w chmurze	181
Big data, strukturalne i niestrukturalne bazy danych	181
Usługi magazynu i baz danych w chmurze Azure	183
Usługa Azure Storage	183
Usługi bazodanowe na platformie Azure	184
Usługi magazynu	184
Usługa Azure Blob Storage	184
Usługa Azure Files	186
Usługa Azure Queue Storage	187
Usługa Azure Table Storage	188
Usługa Azure Managed Disks	189
Wskazówki dotyczące najlepszych praktyk w zakresie bezpieczeństwa usługi Azure Storage	189
Usługa Azure Database Services	190
Azure SQL jako w pełni zarządzana usługa bazy danych	191
Azure Cosmos DB	192
Zrób to sam!	199
Podsumowanie	199
Sprawdź swoją wiedzę	199
Gdzie warto zajrzeć?	200

6. Sztuczna inteligencja, uczenie maszynowe i usługi kognitywne na platformie Azure	203
Sztuczna inteligencja na platformie Azure — wprowadzenie	203
Usługa Azure OpenAI i ewolucja Chat-GPT	205
Innowacje w zakresie technologii AI i pojęcia, które powinienś znać	205
Dlaczego warto poznawać systemy sztucznej inteligencji?	207
Korzyści ze sztucznej inteligencji dla biznesu	208
Uczenie maszynowe	209
MLOps i DevOps — jaka jest między nimi różnica?	211
Głębokie uczenie	212
Etyczna i odpowiedzialna sztuczna inteligencja na platformie Azure	212
Platforma Azure AI i usługi Azure Cognitive Services	214
Usługa Azure Machine Learning	216
Usługa Azure Machine Learning Studio	217
Zautomatyzowane uczenie maszynowe (AutoML)	218
Usługa AI Builder dla platformy Microsoft Power Platform	219
Usługa Azure Applied AI Services	220
Zrób to sam!	222
Podsumowanie	223
Sprawdź swoją wiedzę	223
Gdzie warto zajrzeć?	224
 7. Usługi big data, raportowanie i usługi analityczne na platformie Azure	 226
Usługi big data, raportowania i analizy na platformie Azure	226
Czym jest big data?	227
Rozwiązania big data na platformie Azure	229
Scenariusze użycia big data na platformie Azure	229
Narzędzia do tworzenia złożonych potoków big data na platformie Azure	230
Tworzenie, konfigurowanie i wdrażanie rozwiązań big data na platformie Azure	231
Przygotowanie środowiska produkcyjnego	233
Analityka danych	233
Usługi big data i analiza danych na platformie Azure	235
Usługa Azure Data Lake	236
Azure NoSQL dla rozwiązań big data i analityki	236
Usługa Azure Stream Analytics	236
Usługa Azure Synapse Analytics	237
Usługa Azure Databricks	238
Usługa Azure Data Lake Storage	238

Usługa Azure HDInsight dla klastrów Hadoop, R Server, HBase, Spark i Storm	238
Usługa Azure Data Factory	239
Usługi Azure Analysis Services	240
Osadzona analityka Power BI	240
Usługa Microsoft Purview	241
Końcowe uwagi na temat zarządzania danymi i analityki na platformie Azure	242
Zrób to sam!	242
Podsumowanie	243
Sprawdź swoją wiedzę	243
Gdzie warto zajrzeć?	243
8. Usługi Azure IoT i Azure Maps	245
IoT — internet rzeczy	245
Jak zrozumieć technologię IoT?	246
Komponenty składowe rozwiązań IoT	247
Różne rodzaje zastosowań IoT	248
Wyzwania związane z technologią IoT	249
Rozwiązania IoT na platformie Azure	251
Usługa Azure Maps	257
Zakres geograficzny usługi Azure Maps	259
Uwierzytelnianie i zabezpieczenia w Azure Maps	259
Integracja usługi Azure Maps z usługą Azure Event Grid	260
Tworzenie aplikacji wykorzystujących usługę Azure Maps	261
Zrób to sam!	262
Podsumowanie	263
Sprawdź swoją wiedzę	263
Gdzie warto zajrzeć?	264
9. Bezpieczeństwo platformy Azure, zarządzanie tożsamością i DevSecOps	265
Cyberbezpieczeństwo i jego znaczenie	266
Znaczenie cyberbezpieczeństwa w infrastrukturze chmurowej	270
Metodologia Zero Trust w chmurze	271
Cyberbezpieczeństwo, DevSecOps i zabezpieczanie infrastruktury Azure	273
Odpowiedzialność za strategię bezpieczeństwa to wspólne zadanie	274
Praktyki inżynieryjne w chmurze — shift-left lub shift-right w DevSecOps	275
Zabezpieczenia platformy Azure dla aplikacji, baz danych i sieci	278
Azure IAM — zarządzanie tożsamościami i dostępem	279
Tożsamości zarządzane na platformie Azure	287
Usługa Azure Key Vault	289
Zabezpieczenia sieci na platformie Azure	290
Microsoft Sentinel	291
Microsoft Defender dla chmury	292

Najlepsze praktyki bezpieczeństwa dla platformy Azure	296
Walidacja danych wejściowych aplikacji	296
Implementacja skanowania i sprawdzania zabezpieczeń w kodzie źródłowym i potokach CI/CD	296
Bezpieczna komunikacja i integracja między aplikacjami i interfejsami API	297
Poważne traktowanie obsługi błędów — nie tylko debugowanie, ale także zapewnienie bezpieczeństwa	297
DevSecOps — bezpieczeństwo w rozwoju, DevOps i infrastrukturze	297
Zaadaptowanie bezpieczeństwa w praktykach DevOps	298
Zrób to sam!	300
Podsumowanie	301
Sprawdź swoją wiedzę	301
Gdzie warto zajrzeć?	302

Część IV. Integracja, infrastruktura i DevSecOps **303**

10. Usługi i narzędzia integracji w chmurze Azure	305
Integracja w chmurze — wprowadzenie	305
Rodzaje integracji w chmurze na platformie Azure	306
Korzyści z integracji w chmurze	307
Niezawodność i skalowalność aplikacji	307
Większa wydajność pracy i oszczędność kosztów	309
Sprawność biznesowa i lepsze procesy biznesowe	309
Integracja w chmurze na platformie Azure	309
Wprowadzenie do interfejsów Web API	310
Różne typy interfejsów Web API	310
Cykl życia interfejsu API	311
Usługa Azure API Management	313
Zalety korzystania z usługi Azure API Management	314
Komponenty usługi Azure API Management	316
Usługa Azure Logic Apps	317
Korzyści z zastosowania Azure Logic Apps	318
Warstwy cenowe usługi Azure Logic Apps	318
Komponenty usługi Azure Logic Apps	320
Usługa Azure Service Bus — broker komunikatów w chmurze	321
Komponenty składowe usługi Azure Service Bus	324
Wybór odpowiedniej implementacji obsługi komunikatów na platformie Azure	327
Usługa Azure Web PubSub	327
Wzorzec architektury używany w usłudze Azure Web PubSub	329
Zalety korzystania z usługi Azure Web PubSub	330
Podstawy działania usługi Azure Web PubSub	330
Typowy przepływ pracy usługi Azure Web PubSub	332

Azure Event Grid	332
Zrób to sam!	333
Podsumowanie	334
Sprawdź swoją wiedzę	334
Gdzie warto zajrzeć?	335

11. Infrastruktura chmury, DevOps i monitorowanie na platformie Azure 336

Wprowadzenie	336
Natywna infrastruktura chmurowa	336
Nowoczesne tworzenie aplikacji i metodyka DevOps	339
Podstawy metodyki DevOps i jej funkcja w rozwoju aplikacji	340
Ciągła integracja, wdrażanie, testowanie i monitorowanie	340
Azure DevOps	345
Rozwiązania Azure DevOps w chmurze i lokalnie	346
Usługa Azure DevTest Labs do szkoleń, testowania i demonstracji	347
Rozwój w chmurze i DevOps z wykorzystaniem serwisu GitHub	348
GitHub dla edukacji	349
Automatyzacja i zarządzanie infrastrukturą w chmurze	350
Infrastruktura jako kod	350
Infrastruktura jako kod na platformie Azure	
z wykorzystaniem oprogramowania Hashicorp Terraform	352
Infrastruktura jako kod z wykorzystaniem usługi Azure Resource Manager	
i języka Bicep	353
Kiedy warto rozważyć użycie Azure Terraform zamiast Azure Bicep lub ARM	355
Konfiguracja jako kod	356
Zasady platformy jako kod	357
Monitorowanie infrastruktury na platformie Azure i zarządzanie nią	359
Zrób to sam	361
Podsumowanie	361
Sprawdź swoją wiedzę	362
Gdzie warto zajrzeć?	362

Część V. Zarządzanie, migracja, architektura i narzędzia deweloperskie 365

12. Zarządzanie chmurą i utrzymywanie ładu na platformie Azure 367

Zarządzanie infrastrukturą w chmurze i zapewnianie ładu	367
Azure Resource Manager	370
Organizowanie zasobów przy użyciu Azure Resource Groups i zarządzanie nimi	371
Blokowanie zasobów platformy Azure w celu ochrony infrastruktury	372
Azure Blueprints (wersja zapoznawcza)	373
Tworzenie i wdrażanie strategii usługi Azure Blueprints	374
Azure Blueprints w modelu Zero Trust Security dla migracji do chmury	375

Usługa Azure Monitor	376
Usługa Azure Automation	378
Usługa Azure Policy do zarządzania politykami i zgodnością w chmurze	379
Operacje finansowe i zarządzanie kosztami w Azure	381
Narzędzia do zarządzania kosztami platformy Azure	381
Najlepsze praktyki w zakresie zarządzania kosztami platformy Azure	382
Optymalizacja zarządzania kosztami na platformie Azure	383
Ewolucja zarządzania ładem w chmurze	385
Zrób to sam!	386
Podsumowanie	387
Sprawdź swoją wiedzę	387
Gdzie warto zajrzeć?	387
13. Migracja do chmury, rozwiązania hybrydowe i wielochmurowe na platformie Azure	389
Wdrażanie i modernizacja chmury	389
Modernizacja starszych aplikacji i tradycyjnej infrastruktury	391
Majątek cyfrowy i warunki migracji do chmury	392
Racjonalizacja chmury	394
Antywzorce migracji do chmury	395
Pięć filarów modelu Well-Architected Framework (WAF) dla platformy Azure	396
Filar nr 1 — doskonałość operacyjna	397
Filar nr 2 — bezpieczeństwo	399
Filar nr 3 — niezawodność	400
Filar nr 4 — efektywność działania	402
Filar nr 5 — optymalizacja kosztów	403
Przewodnik Cloud Adoption Framework dla Azure	404
Korzyści z Cloud Adoption Framework for Azure	407
Zalecane metody wdrażania chmury Azure	408
Azure Well-Architected Review	410
Zalety korzystania z Azure Well-Architected Review	410
Platforma Microsoft Assessments	411
Przydatne narzędzia platformy Microsoft Assessments	412
Chmura hybrydowa i rozwiązania wielochmurowe na platformie Azure	413
Azure Arc	413
Azure Arc-Enabled Kubernetes	414
Azure Stack	414
Azure VMware Solution	414
Azure ExpressRoute	415
Azure Site Recovery	415
Azure VPN Gateway	415
Rozwiązania wielochmurowe i hybrydowe na platformie Azure	415

Zrób to sam!	416
Podsumowanie	417
Sprawdź swoją wiedzę	417
Gdzie warto zajrzeć?	417
14. Narzędzia deweloperskie do pracy w chmurze Azure	419
Znaczenie narzędzi programistycznych dla produktywności deweloperów	420
Narzędzia programistyczne Azure dla inżynierów	421
Visual Studio i Visual Studio Code	421
Alternatywne środowiska IDE do programowania w języku Java i tworzenia aplikacji międzyplatformowych lub mobilnych	424
Pakiety Azure SDK	425
Narzędzia wiersza poleceń platformy Azure	427
Azure Cloud Shell	427
Azure CLI	428
Azure PowerShell	431
Predykcyjna funkcja IntelliSense w Azure Cloud Shell	432
Azure Developer CLI (azd)	433
Microsoft Dev Box	434
Azure Deployment Environments w usłudze Microsoft Dev Box	436
Azure DevOps i GitHub dla deweloperów	438
Azure DevOps	438
GitHub	439
GitHub Codespaces	439
GitHub CLI	440
GitHub Enterprise	442
Zrób to sam!	443
Podsumowanie	443
Sprawdź swoją wiedzę	444
Gdzie warto zajrzeć?	444
Postówie — Maxim Salnikov	447
Słowo końcowe od autorki	449
Dodatek. Sprawdź swoją wiedzę — odpowiedzi na pytania	451
Skorowidz	459

Podstawy Microsoft Azure

Chmura obliczeniowa zrewolucjonizowała sposób, w jaki firmy obsługują swoje obciążenia IT. Rozwiązania chmurowe umożliwiają organizacjom nie tylko tworzenie i wdrażanie aplikacji w nowoczesny sposób przy użyciu nowoczesnych usług PaaS/SaaS, ale także korzystanie z zalet chmur obliczeniowych, takich jak wysoka dostępność, skalowalność, bezpieczeństwo i optymalizacja kosztów. Zrozumienie podstaw funkcjonowania środowiska chmurowego ma kluczowe znaczenie dla nabycia podstawowej wiedzy na temat Microsoft Azure, którą później można wykorzystać do tworzenia złożonych obciążeń i zarządzania nimi. Jeżeli dopiero zaczynasz swoją karierę w chmurze lub chcesz pogłębić swoją wiedzę na temat Microsoft Azure, zacznij od podstaw!

— Tiago Costa, architekt i doradca ds. rozwiązań chmurowych, Microsoft Azure MVP,
Microsoft Certified Trainer

W rozdziale 1. poznałeś najważniejsze koncepcje chmury obliczeniowej i dowiedziałeś się, że organizacje korzystają z zasobów chmury obliczeniowej z elastycznymi modelami cenowymi, aby wykorzystać globalną skalę, niezawodność i bezpieczeństwo oferowane przez takie rozwiązania.

W tym rozdziale poszerzysz swoją wiedzę na temat przetwarzania w chmurze, zagłębiając się w świat Azure, czyli platformy chmurowej firmy Microsoft. Poznasz tutaj podstawowe koncepcje platformy Azure jako dostawcy usług w chmurze i dowiesz się jak powstała, jaki jest jej cel i w jaki sposób może zainspirować Cię do innowacyjności podczas tworzenia nowoczesnych rozwiązań spełniających potrzeby i wymagania Twojej organizacji.

Dowiesz się, czym są *lokalizacje geograficzne*, *regiony* i *strefy dostępności* platformy Azure, a także poznasz usługę Azure Resource Manager, która zapewnia przegląd infrastruktury chmury platformy Azure.

W tym rozdziale znajdziesz kompleksowy przegląd podstawowych usług platformy Azure. Każda z tych usług zostanie szczegółowo objaśniona wraz z zastosowaniami i przykładami w kolejnych rozdziałach tej książki.



Chmura publiczna to rodzaj modelu wdrażania, w którym infrastruktura chmury jest dostępna publicznie lub dla dowolnej organizacji, a zasoby są współdzielone z innymi organizacjami lub innymi użytkownikami chmury.

Microsoft Azure jako dostawca chmury publicznej

Platformą chmurową firmy Microsoft jest Microsoft Azure (<https://azure.microsoft.com>), nazywana często po prostu Azure (nazwa nie jest tutaj przypadkowa, ponieważ w języku angielskim słowo „azure” oznacza błękit, który jest typowym kolorem nieba, co w oczywisty sposób kojarzy się również z chmurami). Historycznie rzecz biorąc, pierwsza platforma Windows Azure była oparta na systemie Windows Server 2008 i przeznaczona dla programistów, którzy chcieli hostować swoje aplikacje w środowisku Windows w chmurze¹.



Platforma Windows Azure była fundamentem dla nowoczesnych rozwiązań chmurowych i z biegiem stała się naprawdę świetną i potężną platformą chmurową firmy Microsoft. W 2014 roku zmieniono jej nazwę na Microsoft Azure (co ciekawe, pierwotnie platforma Azure nosiła nazwę kodową Red Dog).

Zdolność platformy Azure do tworzenia, budowania, wdrażania aplikacji organizacji i zarządzania nimi w skali globalnej sprawiła, że stała się ona jednym z najlepszych rozwiązań chmurowych na świecie. Warto zauważyć, że platforma Microsoft Azure jest dostawcą chmury publicznej dla 95% firm z listy Fortune 500 (<https://www.extremetech.com/deals/307468-microsoft-azure-is-used-by-95-percent-of-fortune-500-companies-learn-to-use-their-cloud-services-now>).

Microsoft Azure pomaga organizacjom zminimalizować koszty początkowe migracji

Chmura publiczna ma funkcje, które są bardzo przydatne dla wielu użytkowników. Obejmuje to między innymi brak konieczności ponoszenia z góry kosztów kapitałowych (CapEx) w celu skalowania zasobów, szybkie udostępnianie i usuwanie aplikacji oraz elastyczność kosztów, dzięki której organizacje płacą tylko za to, czego naprawdę używają.

Azure jest dostawcą chmury publicznej, ale oferuje również użytkownikom rozwiązania prywatne, hybrydowe i wielochmurowe. Usługi Azure zostały tak zaprojektowane, aby pomóc użytkownikom w tworzeniu innowacyjnych rozwiązań w chmurze, które pomogą rozwiązać stawiane przed nimi wyzwania.

Usługi chmurowe Azure umożliwiają tworzenie, rozwijanie i uruchamianie zasobów takich jak serwery, bazy danych, pamięć masowa lub aplikacje w wielu środowiskach chmurowych, a także zarządzanie nimi. Można z nich korzystać w różnych scenariuszach zastosowań w chmurze przy użyciu preferowanych narzędzi, języków programowania i frameworków.

W czasie kiedy powstawała ta książka, platforma Azure oferowała ponad 200 usług, podzielonych na różne kategorie, takie jak usługi obliczeniowe, sieciowe i pamięci masowej, bazy danych, analityka, uczenie maszynowe i sztuczna inteligencja, internet rzeczy (IoT), kontenery i bezpieczeństwo.

¹ Windows Azure: Microsoft's Cloud Platform, dokumentacja Microsoft Azure, <https://docs.microsoft.com/en-us/archive/blogs/aniyer/windows-azure-microsofts-cloud-platform> (tylko w wersji ang.).

Warto zauważyć, że firma Microsoft regularnie wprowadza nowe funkcje i usługi do platformy Azure, więc ich liczba może z czasem wzrosnąć.

Platforma Azure zapewnia również usługi przetwarzania brzegowego, sztucznej inteligencji i uczenia maszynowego (ang. *machine learning* — ML), które umożliwiają tworzenie inteligentnych rozwiązań za pomocą istniejących lub nowych aplikacji. Bez technologii przetwarzania w chmurze nie byłoby to możliwe.

Zalety chmury obliczeniowej

Istnieje kilka zalet, które środowisko chmury obliczeniowej ma w porównaniu z tradycyjnym lokalnym środowiskiem fizycznym, jak pokazano w tabeli 2.1.

Tabela 2.1. Zalety chmury obliczeniowej w porównaniu ze środowiskiem lokalnym

Zaleta	Opis
Wysoka dostępność usług	Microsoft Azure zapewnia wysoką dostępność i nadmiarowość we wszystkich swoich centrach danych na całym świecie, oferując umowę SLA (ang. <i>service-level agreement</i>), która zapewnia dostępność usługi na poziomie 99,95%.
Geodystrybucja	Platforma Azure pomaga globalnym przedsiębiorstwom, udostępniając funkcje aplikacji rozproszonych geograficznie. Punkty końcowe specyficzne dla danego regionu geograficznego umożliwiają międzynarodowym przedsiębiorstwom zachowanie zgodności z lokalnymi przepisami i regulacjami obowiązującymi w danym regionie.
Skalowalność na żądanie	Gdy zapotrzebowanie na obciążenie, ruch sieciowy i dane rośnie, Azure oferuje szybki i elastyczny sposób na zaspokojenie takich potrzeb.
Niezawodność	Hostowane systemy i aplikacje działają poprawnie nawet w obliczu przeciwności losu (usterki sprzętu lub oprogramowania, a nawet błędów użytkowników).
Skalowalność	Możliwość automatycznego skalowania zasobów w chmurze w oparciu o żądaną konfigurację lub zapotrzebowanie.
Odzyskiwanie danych po awarii	Gdy aplikacje, dane i systemy są hostowane na platformie Azure, można mieć pewność, że potrzeby tworzenia kopii zapasowych i odzyskiwania danych po awarii są kompleksowo zabezpieczone.
Elastyczność kosztów	Usługi w chmurze na platformie Azure zapewniają organizacjom pełną elastyczność, umożliwiając korzystanie z elastycznych planów cenowych i pełnego, samoobsługowego zarządzania, dostępnego z dowolnego miejsca na świecie.
Narzędzia do zarządzania kosztami	Narzędzia do zarządzania kosztami na platformie Azure umożliwiają użytkownikom ustawianie alertów budżetowych dla poszczególnych grup i zasobów.
Zgodność z normami i standardami	Platforma Azure bardzo poważnie traktuje bezpieczeństwo informacji i zgodność z normami i standardami, aby spełniać wymagania swoich użytkowników.
Wysoki poziom bezpieczeństwa w chmurze	Platforma Azure chroni wszystkie przechowywane dane za pomocą wysokiej klasy zabezpieczeń. Dane przechowywane na platformie Azure są chronione za pomocą zaawansowanych technologii szyfrowania. Wszystkie centra danych Microsoft są wyposażone w nowoczesne zabezpieczenia ze skanerami biometrycznymi, wielopoziomowym uwierzytelnianiem i wieloma innymi technologiami.
OpEx kontra CapEx	Hosting w chmurze oznacza, że organizacja może oszczędzać pieniądze na wydatkach kapitałowych (CapEx) i ponosić tylko koszty operacyjne (OpEx).

Tabela 2.1. Zalety chmury obliczeniowej w porównaniu ze środowiskiem lokalnym (ciąg dalszy)

Zaleta	Opis
Model cenowy oparty na rzeczywistym zużyciu zasobów	Platforma Azure zapewnia użytkownikom elastyczność zarządzania kosztami, oferując model cenowy oparty na rzeczywistym zużyciu zasobów (model <i>pay-as-you-go</i>) dla większości swoich usług w chmurze.
Nie wymaga zaawansowanych umiejętności technicznych	Aby korzystać z platformy chmurowej, ani użytkownicy, ani organizacja nie muszą posiadać żadnych zaawansowanych umiejętności technicznych. Microsoft Azure zapewnia elastyczne i zróżnicowane opcje, które ułatwiają korzystanie z niej.

Portal Azure

Portal do zarządzania platformą chmurową firmy Microsoft nosi nazwę *Azure Portal* i jest dostępny dla użytkowników za pośrednictwem przeglądarki internetowej lub *aplikacji mobilnej Azure*. Jest to rozbudowany, internetowy portal administracyjny dla użytkowników platformy Azure, wyposażony w szereg narzędzi i funkcji do zarządzania usługami swojej firmy lub organizacji w chmurze Microsoft Azure. Na przykład w portalu Azure można zarządzać grupami zasobów, zasobami w grupach, subskrypcjami Azure, zabezpieczeniami, usługami i użytkownikami oraz wykonywać wiele innych operacji.



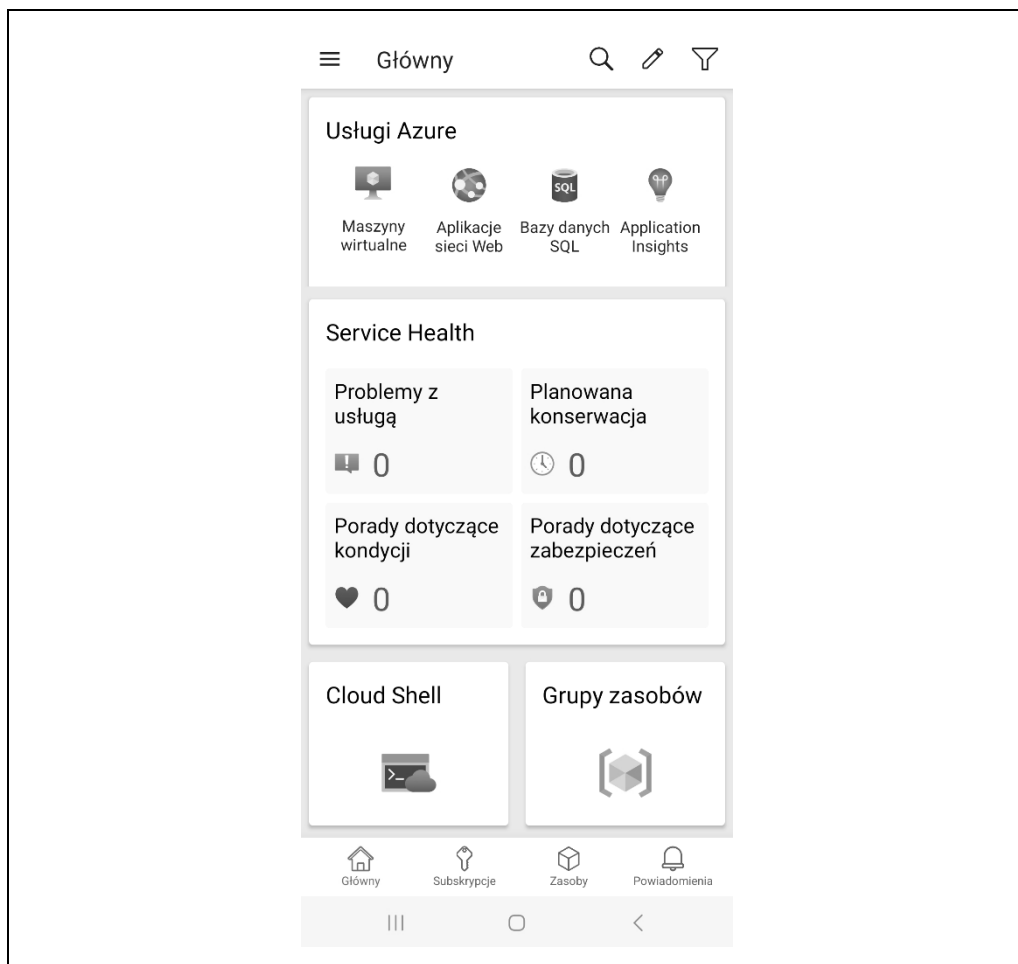
- Dostęp do portalu Microsoft Azure można uzyskać za pomocą aplikacji mobilnej Azure. Aby dowiedzieć się, jak ją pobrać i zainstalować, powinieneś zajrzeć do dokumentacji Microsoft Azure (<https://azure.microsoft.com/pl-pl/get-started/azure-portal/mobile-app/>).
- Dostęp do portalu Microsoft Azure (<https://portal.azure.com>) możesz uzyskać za pomocą ulubionej przeglądarki internetowej na dowolnym urządzeniu.

Portal Azure został zbudowany tak, aby był przenośny i dostępny z dowolnego miejsca na dowolnym urządzeniu. Na rysunku 2.1 pokazano interfejs użytkownika aplikacji mobilnej Azure, za pomocą której można zarządzać subskrypcjami i usługami Azure w podróży.



Adres URL portalu Azure zależy od chmury, w której dana firma czy organizacja została wdrożona na platformie Microsoft Azure.

- Portal Azure do użytku komercyjnego lub chmury publicznej (*Azure Public Cloud*): <https://portal.azure.com>.
- Portal Azure dla instytucji rządowych USA (*Azure United States Government Cloud*): <https://portal.azure.us>.
- Portal Azure Chiny (*Azure China*): <https://portal.azure.cn>.



Rysunek 2.1. Strona startowa aplikacji mobilnej Azure

Oprócz różnych lokalizacji i różnych zakresów wdrażania Azure jako platformy chmurowej w sektorze rządowym USA i zastosowaniach komercyjnych firma Microsoft oferuje również usługę o nazwie Microsoft Cloud for Sovereignty (<https://learn.microsoft.com/pl-pl/industry/sovereignty/cloud-for-sovereignty>). Jest to rozwiązanie, które pomaga użytkownikom platformy Azure w sektorach rządowych i publicznych innych krajów wykorzystać chmurę obliczeniową przy jednoczesnym zapewnieniu pełnej suwerenności cyfrowej i kontroli nad danymi oraz zapewnieniu zgodności ze specyficznymi i unikalnymi wymaganiami formalno-prawnymi ich krajów. Wdrożenie takiego rozwiązania pomaga tym sektorom uzyskać lepszą kontrolę nad ich danymi, prywatnością, zgodnością i potrzebami w zakresie zarządzania.

Funkcje portalu Azure

Portal Azure oferuje wiele ciekawych funkcji dla wszystkich typów użytkowników tej platformy. Dzięki niemu firmy i organizacje mają pełną kontrolę nad swoimi zasobami w chmurze i mogą globalnie nimi zarządzać. Deweloperzy oprogramowania lub inżynierowie chmury mogą tworzyć i monitorować dowolne typy aplikacji w chmurze, od prostych do złożonych, niezależnie od architektury aplikacji i użytych języków programowania, oraz zarządzać nimi. Poniżej przedstawiono niektóre funkcje portalu Azure:

- Tworzenie, kompilowanie usług Azure i zasobów w chmurze, monitorowanie ich i zarządzanie nimi w jednym miejscu, w dowolnym czasie i miejscu, w dogodny dla siebie sposób.
- Możliwość używania narzędzi wiersza poleceń i powłoki chmury do szybkiego tworzenia i wdrażania rozwiązań.
- Zarządzanie subskrypcjami platformy Azure oraz tworzenie grup, które pomagają w strukturyzowaniu zasobów platformy Azure i zarządzaniu nimi.
- Wykorzystanie Microsoft Entra ID do zarządzania tożsamościami, dostępem i uprawnieniami do zasobów na platformie Azure.
- Konfigurowanie ustawień i zarządzanie prywatnością, danymi, zabezpieczeniami, zasadami i zgodnością niezbędnymi do zarządzania organizacją.
- Możliwość dostosowywania pulpitu nawigacyjnego portalu, co umożliwia szybki przegląd stanu zasobów zaraz po zalogowaniu.
- Pełna kontrola nad miesięcznymi kosztami, monitorowanie zasobów za pomocą limitów wydatków i alertów budżetowych przy użyciu usługi Azure Cost Management.
- Możliwość łatwego wyszukiwania wszystkiego, co jest potrzebne do tworzenia, kompilowania i zarządzania przy użyciu funkcji globalnego wyszukiwania.
- Wysyłanie zgłoszeń bezpośrednio do działu pomocy technicznej platformy Azure (<https://learn.microsoft.com/pl-pl/azure/azure-portal/supportability/how-to-create-azure-support-request>), gdy potrzebujesz pomocy lub wsparcia technicznego.



Azure Marketplace (<https://azuremarketplace.microsoft.com/pl-pl/marketplace/>) to rynek dla klientów platformy Azure umożliwiający wyszukiwanie, kupowanie i wypróbowywanie aplikacji oraz usług od innych dostawców, w tym partnerów firmy Microsoft. Wszystkie usługi oferowane na Azure Marketplace są zweryfikowane i certyfikowane do współpracy z platformą chmurową Azure.

Usługi platformy Microsoft Azure

W czasie kiedy powstawała ta książka, wszystkie usługi Azure podzielone były według przeznaczenia na 21 kategorii (<https://azure.microsoft.com/pl-pl/products/>), co powoduje, że początkujący użytkownicy, a często nawet ci bardziej doświadczeni mogą być nieco przytłoczeni liczbą dostępnych usług w chmurze takiej jak Azure. Jednak każda usługa Azure ma swoje przeznaczenie i została utworzona w celu rozwiązywania konkretnych problemów technicznych. Usługi platformy Azure można płynnie integrować z innymi usługami.

Usługi Azure pomagają tworzyć i integrować rozwiązania chmurowe w oparciu o konkretne wymagania lub potrzeby biznesowe użytkowników. Na przykład utworzenie aplikacji internetowej z integracją interfejsów API, usługami kognitywnymi i funkcjami raportowania wymaga użycia kilku usług Azure: sztucznej inteligencji/uczenia maszynowego, obliczeń, analizy biznesowej, baz danych, integracji, narzędzi programistycznych itp.

W tabeli 2.2 zamieszczono opis wybranych, popularnych usług platformy Azure. Aby wyświetlić zaktualizowaną listę usług według kategorii, powinieneś zajrzeć na stronę <https://azure.microsoft.com/pl-pl/products/>. Wybrane usługi Azure zostaną omówione w kolejnych rozdziałach tej książki.

Tabela 2.2. Przegląd kategorii usług Microsoft Azure

Kategoria	Opis	Usługi Azure
Sztuczna inteligencja (AI) i uczenie maszynowe (ML)	Tworzenie nowoczesnych aplikacji w chmurze z inteligencją kognitywną i uczeniem maszynowym.	Azure Boot Service, Azure Cognitive Services, Azure Machine Learning, Azure AI Anomaly Detector, Azure DataBricks, Azure Open Datasets, Computer Vision, Face API, Azure AI Immersive Reader, Azure AI Document Intelligence, Kinect DK, Microsoft Genomics, Azure Health Boot, Azure Applied AI Services, Azure Percept, Speech Services itd.
Analizy	Zbieranie i wizualizacja dowolnego typu danych niezależnie od ich ilości.	Azure Analysis Services, Azure Data Explorer, Azure Data Lake Storage, Azure Data Share, Azure Databricks, Azure Stream Analytics, HDInsight, PowerBI Embedded, Azure Synapse Analytics, Data Factory, Event Hubs, R Server for HDInsight, Microsoft Graph Data Connect, Azure Purview itd.
Obliczenia	Tworzenie niezawodnych, skalowalnych aplikacji z wydajnym przetwarzaniem w chmurze.	API Apps, App Service, Azure Cycle Cloud, Azure Functions, Azure Kubernetes Service (AKS), Azure Quantum Preview, Azure Spot Virtual Machines, Azure Spring Cloud, Azure VMware Solution, Azure Batch, Cloud Services, Linux Virtual Machines, Azure Container Instances, Azure Static Web Apps, VM Scale Sets, Azure Virtual Machines, Azure Virtual Desktop, Web Apps, Azure Dedicated Host, Azure VM Image Builder itd.
Kontenery	Tworzenie i rozwijanie aplikacji konteneryzowanych oraz zarządzanie nimi za pomocą nowoczesnych narzędzi integracyjnych.	Azure Kubernetes Services (AKS), Azure Container Instances, Azure Container Registry, Azure Service Fabric, Web App for Containers.
Bazy danych	W pełni zarządzane i bezpieczne usługi baz danych w chmurze.	Azure SQL Database, Azure Cosmos DB, Azure Cache for Redis, Azure Database for PostgreSQL, Azure Database for MySQL, Apache Cassandra MI, SQL Server on Virtual Machines, Azure Database Migration Service, Table Storage, Azure API for FHIR, Azure SQL Database Edge itd.
Narzędzia deweloperskie	Usługi i narzędzia deweloperskie dla inżynierów i deweloperów pracujących nad rozwojem rozwiązań w chmurze i DevOps dla Azure.	Azure DevOps, Azure DevTest Labs, App Configuration, Azure SDKs, Azure Lab Services, Azure Pipelines, Visual Studio, Visual Studio Code.
Integracja	Usługi dla różnych typów integracji na platformie Azure, w chmurze hybrydowej i w konfiguracji wielochmurowej.	Azure API Management (APIM), Azure Event Grid, Azure Service Bus, Azure Logic Apps, Azure Web PubSub Preview, Azure Healthcare APIs Preview.

Tabela 2.2. Przegląd kategorii usług Microsoft Azure (ciąg dalszy)

Kategoria	Opis	Usługi Azure
Sieć	Łączenie infrastruktury lokalnej i zasobów w chmurze przy użyciu usług sieciowych.	Application Gateway, Azure Bastion, Azure DNS, Azure Express Route, Azure Content Delivery Network, Load Balancer, Azure Front Door, Azure Firewall, Internet Analyzer, Azure Orbital, Private Link, VPN Gateway, Virtual WAN, Virtual Network, Traffic Manager.
Internet rzeczy (IoT)	Tworzenie rozwiązań w chmurze dla urządzeń IoT.	Azure IoT Hub, Azure IoT Central, Azure Sphere, Azure IoT Edge, Azure RTOS.
Tożsamość i zabezpieczenia	Ochrona zasobów, danych i tożsamości w chmurze.	Microsoft Entra ID, Microsoft Defender for Cloud, Azure Security Center, Azure Key Vault, Azure Sentinel, Information Protection, DDoS Protection itd.

Przegląd podstawowych usług Azure

Firma Microsoft ciągle pracuje nad nowymi rozwiązaniami oraz stale aktualizuje i ulepsza usługi Azure.

Usługi obliczeniowe na platformie Azure

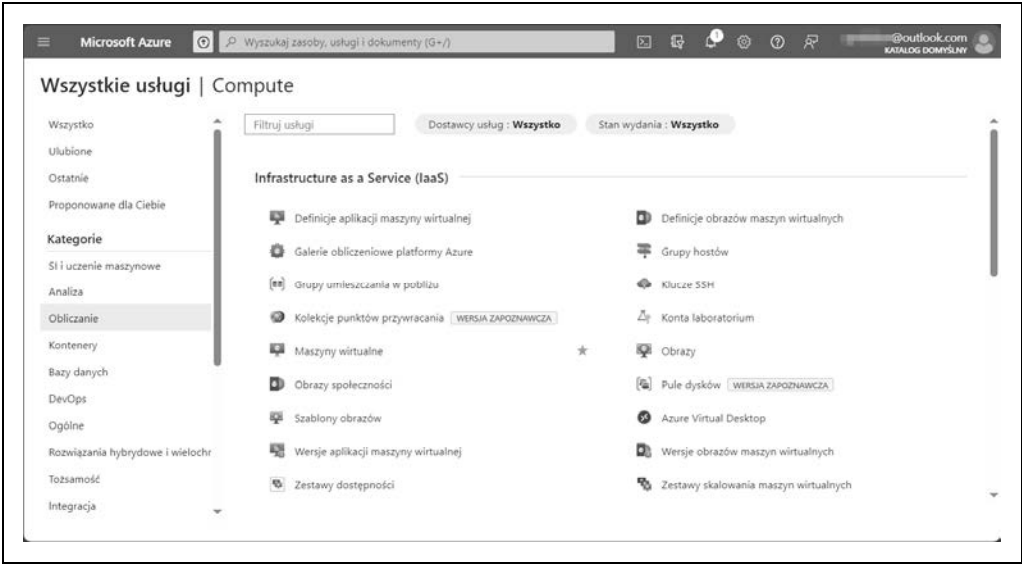
Obliczanie to nazwa kategorii używana w odniesieniu do usług oferujących korzystanie z mocy obliczeniowej i skalowania na żądanie. Usługi obliczeniowe platformy Azure zapewniają użytkownikom dostęp do zasobów takich jak systemy operacyjne, sieci, dyski, procesory i pamięć. Zasoby obliczeniowe są dostępne w każdej chwili na żądanie użytkowników. Każda aplikacja jest unikatowa i może generować wiele obciążeń, które będą wymagały więcej niż jednej usługi obliczeniowej.

W czasie kiedy powstawała ta książka, na platformie Azure dostępnych było ponad 25 usług obliczeniowych. Usługi obliczeniowe platformy Azure umożliwiają tworzenie aplikacji internetowych i mobilnych, wdrażanie maszyn wirtualnych i zarządzanie nimi, tworzenie aplikacji w kontenerach w chmurze, tworzenie zadań wsadowych i nie tylko. Na rysunku 2.2 przedstawiono przegląd usług obliczeniowych dostępnych w portalu Azure. Dodatkowo w tabeli 2.3 zamieszczono przegląd niektórych typowych usług obliczeniowych platformy Azure i ich przeznaczenia.

Szczegóły techniczne, scenariusze użycia i sposoby rozpoczęcia pracy z usługami obliczeniowymi platformy Azure omówiono w rozdziale 3.

Usługi sieciowe na platformie Azure

Usługi sieciowe pomagają zabezpieczyć zarówno prywatną, jak i publiczną infrastrukturę chmury. Użytkownicy mogą dostosować konfigurację sieci w chmurze i zarządzać zasobami sieciowymi na żądanie.



Rysunek 2.2. Przegląd usług obliczeniowych w portalu Azure

Tabela 2.3. Przegląd usług obliczeniowych platformy Azure

Usługa obliczeniowa Azure	Przeznaczenie
Azure App Service	Tworzenie i rozwijanie aplikacji internetowych i mobilnych we w pełni zarządzanym środowisku chmury.
Azure Static Web Apps	Szybkie tworzenie nowoczesnych aplikacji internetowych z pełnym stosem na platformie Azure z repozytorium kodu.
Azure Virtual Machines	Szybkie i łatwe w zarządzaniu wdrażanie maszyn wirtualnych (Azure VM) z różnymi systemami operacyjnymi, takimi jak Windows lub Linux.
Azure Virtual Machine Scale Sets	Tworzenie i aprowizowanie zestawów maszyn wirtualnych (Azure VM) w celu zrównoważenia obciążenia i zapewnienia wysokiej dostępności.
Azure Spot Virtual Machines	Oszczędzanie pieniędzy dzięki dużym rabatom na wykorzystanie nieużywanej mocy obliczeniowej platformy Azure do obsługi przerywanych, skalowanych obciążeń.
Azure Functions	Tworzenie aplikacji bezserwerowych, aplikacje sterowane zdarzeniami i stanowe przepływy pracy
Azure Container Apps	Tworzenie i wdrażanie w pełni zarządzanych, nowoczesnych aplikacji i mikrousług przy użyciu kontenerów bezserwerowych.
Azure Kubernetes Service (AKS)	Tworzenie zarządzanych kontenerów Kubernetes w chmurze.
Service Fabric	Tworzenie mikrousług i zarządzanie kontenerami w różnych systemach operacyjnych, takich jak Windows i Linux.

Usługi sieciowe platformy Azure umożliwiają użytkownikom platformy Azure spełnienie wymagań obciążeń w ich infrastrukturze lokalnej przy użyciu podejścia hybrydowego lub w chmurze z wysoką dostępnością i zabezpieczeniami opartymi na modelu Microsoft Zero Trust wdrożonym na poziomie całej firmy lub organizacji (<https://www.microsoft.com/pl-pl/security/business/zero-trust>). W tabeli 2.4 przedstawiono niektóre z typowych usług sieciowych platformy Azure.

Tabela 2.4. Przegląd usług sieciowych platformy Azure

Usługa sieciowa Azure	Opis
Azure Virtual Network	Łączenie maszyn wirtualnych przy użyciu połączeń VPN.
Azure Bastion	Bezpieczny i łatwy dostęp do maszyn wirtualnych przy użyciu w pełni zarządzanych, prywatnych protokołów RDP i SSH.
Azure Private Link	Dostęp do usług hostowanych w chmurze platformy Azure z zachowaniem prywatności.
Azure Firewall	Ochrona zasobów w chmurze przy użyciu łatwo zarządzalnej zapory sieciowej o wysokiej dostępności.
Azure Load Balancer	Równoważenie obciążenia połączeń i żądań aplikacji, zarówno przychodzących, jak i wychodzących.
Azure ExpressRoute	Tworzenie prywatnych połączeń sieciowych między centrami danych platformy Azure a infrastrukturą lokalną.
Azure Traffic Manager	Zarządzanie ruchem sieciowym w celu uzyskania lepszej wydajności.
Azure VPN Gateway	Bezpieczne łączenie sieci lokalnych z platformą Azure za pomocą połączeń VPN.

Więcej informacji na temat szczegółów technicznych i sposobu rozpoczęcia pracy z usługą Azure Networking możesz znaleźć w rozdziale 4.

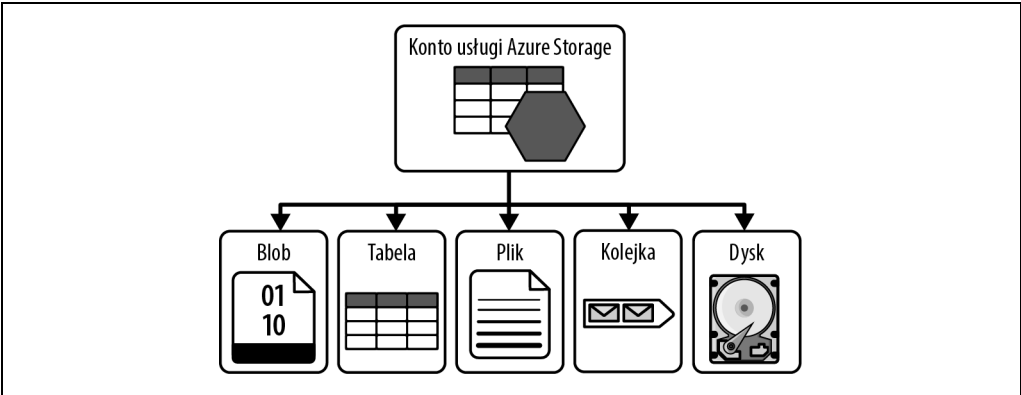
Podstawowe usługi Azure Storage

Usługi Azure Storage oferują doskonały magazyn dla różnych obiektów danych, magazyn dyskowy maszyn wirtualnych platformy Azure, niezawodny magazyn komunikatów i innych, nowoczesnych typów danych. Wykorzystanie magazynów danych na platformie Azure zapewnia wiele korzyści, takich jak wysoka dostępność, trwałość, bezpieczeństwo i łatwość zarządzania. W tabeli 2.5 przedstawiono niektóre z popularnych usług magazynu platformy Azure.

Tabela 2.5. Przegląd usług Azure Storage

Usługa Azure Storage	Opis
Azure Blobs	Przechowywanie skalowalnych danych binarnych, tekstu lub danych big data dla usługi Data Lake Storage Gen2.
Azure Files	W pełni zarządzane udziały sieciowe plików dla wdrożeń lokalnych lub w chmurze, dostępne z dowolnego miejsca za pośrednictwem protokołu Server Message Block (SMB).
Azure Queues	Usługa służąca do przechowywania dużej liczby komunikatów, do których można uzyskać dostęp za pośrednictwem uwierzytelnionych żądań HTTP lub HTTPS.
Azure Managed Disks	Dyski zarządzane platformy Azure to woluminy magazynu na poziomie bloku zarządzane przez platformę Azure i używane z usługą Azure Virtual Machines.

Każda z wymienionych usług Azure musi być zintegrowana i skojarzona z kontem usługi Azure Storage. Konto usługi Azure Storage jest kontenerem dla wszystkich obiektów danych usługi Azure Storage, takich jak obiekty blob, pliki, tabele i kolejki (rysunek 2.3).



Rysunek 2.3. Konto Azure Storage jest wymagane dla wszystkich podstawowych usług Azure Storage

Podstawowe usługi Azure Database

Azure ma ogromną kolekcję usług baz danych, które można dobierać w zależności od struktury danych potrzebnych w organizacji: bazy relacyjne, bazy NoSQL, bazy danych przechowywane w pamięci i inne nowoczesne typy baz danych. W tabeli 2.6 przedstawiono wybrane, typowe usługi baz danych platformy Azure.

Tabela 2.6. Przegląd usług baz danych platformy Azure

Usługa Azure Database	Opis
Azure SQL Database	Bazy danych SQL hostowane w chmurze, które są w pełni zarządzane, inteligentne i bezpieczne.
Azure Cosmos DB	Tworzenie i migrowanie obciążeń NoSQL do chmury z wykorzystaniem baz danych takich jak Cassandra, MongoDB i inne bazy danych NoSQL.
Azure Cache for Redis DB	Tworzenie szybkich i skalowalnych aplikacji przy użyciu magazynu danych Redis w pamięci.
Azure Database for PostgreSQL, MySQL i MariaDB	Tworzenie w pełni zarządzanych i skalowalnych baz danych dla PostgreSQL, MySQL i MariaDB.
Azure SQL Edge	Silnik bazy danych SQL z wbudowaną sztuczną inteligencją i zoptymalizowany pod kątem brzegowych urządzeń IoT.

Więcej szczegółowych informacji na temat innych rozwiązań magazynów i baz danych oraz szczegóły techniczne znajdziesz w rozdziale 5.

Zarządzanie tożsamościami i usługi zabezpieczeń

Korzystając z usług zarządzania tożsamościami i zabezpieczeń na platformie Azure (ang. *Azure Identity Management and Security Services*), możesz zabezpieczyć przed zagrożeniami zasoby swojej organizacji w chmurze. W tabeli 2.7 przedstawiono typowe usługi zarządzania tożsamościami i zabezpieczeń na platformie Azure.

Tabela 2.7. Przegląd usług tożsamości i zabezpieczeń platformy Azure

Usługa Azure Identity Management and Security Services	Opis
Microsoft Entra ID	Zabezpieczanie tożsamości i ochrona użytkowników całej organizacji przy użyciu logowania SSO i uwierzytelniania wieloskładnikowego.
Azure Information Protection	Ochrona poufnych informacji w chmurze
Azure Key Vault	Możliwość kontrolowania i zabezpieczania kluczy, zarządzanie nimi oraz bezpieczne przechowywanie ciągów połączeń i sekretów.
Microsoft Defender for Cloud	Ochrona i wykrywanie zagrożeń dla obciążeń na platformie Azure, w infrastrukturze lokalnej, a nawet u innych dostawców usług w chmurze.
Microsoft Sentinel	Microsoft Sentinel to skalowalne rozwiązanie natywne dla chmury, które zapewnia zarządzanie informacjami o zabezpieczeniach i zdarzeniach (SIEM) ² oraz orkiestrację zabezpieczeń, automatyzację i reagowanie (SOAR) ³ .
Azure DDoS Protection	Ochrona aplikacji na platformie Azure przed atakami typu rozproszona odmowa usługi (ang. <i>Distributed Denial of Service</i> — DDoS) ⁴ .



SIEM to akronim od *Security Information and Event Management*, komputerowego systemu zarządzania informacjami i zdarzeniami zabezpieczeń, który może być używany jako narzędzie do gromadzenia, analizowania i wykonywania operacji bezpieczeństwa w systemach komputerowych, zarówno w aplikacjach, jak i na urządzeniach sprzętowych. Systemy SIEM mają takie funkcje jak zbieranie i rejestrowanie danych z zasobów w środowisku, tworzenie alertów dotyczących potencjalnych anomalii bezpieczeństwa, zarządzanie incydentami i wizualizacja dzienników danych.

Więcej informacji na temat szczegółów technicznych i sposobu rozpoczęcia pracy z platformą tożsamości użytkowników platformy Azure i usługami zabezpieczeń możesz znaleźć w rozdziale 9.

Narzędzia dla deweloperów, monitorowanie i usługi DevOps

Platforma Azure oferuje różne narzędzia i usługi dla programowania w chmurze, rozwiązywania problemów, monitorowania, praktyk DevOps, infrastruktury jako kodu (ang. *Infrastructure as Code* — IaC) oraz ciągłej integracji czy ciągłego dostarczania (ang. *Continuous Integration/Continuous Delivery* — CI/CD). W tabeli 2.8 przedstawiono typowe narzędzia deweloperskie i usługi DevOps platformy Azure.

² Wikipedia, *Security information and event management*, https://en.wikipedia.org/wiki/Security_information_and_event_management.

³ Rapid7.com, *Security Orchestration Automation and Response (SOAR) Tools and Solutions*, <https://www.rapid7.com/solutions/security-orchestration-and-automation/>.

⁴ Cybersecurity & Infrastructure Security Agency, *Security Tip (ST04-015) — Understanding Denial-of-Service Attacks*, <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>.

Tabela 2.8. Przegląd narzędzi deweloperskich i usług DevOps platformy Azure

Narzędzia deweloperskie Azure	Opis
Azure DevOps	Kompleksowe narzędzie z doskonałymi usługami DevOps dla zespołów deweloperów, przeznaczone do współpracy, udostępniania kodu, śledzenia postępów zadań i dostarczania projektów oprogramowania.
Azure DevTestLabs	Szybkie tworzenie środowisk testowych na potrzeby wdrażania i testowania aplikacji, realizowane przy użyciu szablonów wielokrotnego użytku i artefaktów.
App Configuration	Szybki i skalowalny magazyn parametrów na potrzeby konfigurowania aplikacji.
Visual Studio	Opracowywanie, debugowanie, wdrażanie, diagnozowanie aplikacji w chmurze na platformie Azure i zarządzanie nimi przy użyciu w pełni funkcjonalnego środowiska IDE.
Visual Studio Code	Tworzenie i debugowanie kodu za pomocą lekkiego, szybkiego edytora kodu, który działa w systemach operacyjnych takich jak Windows i Linux oraz innych obsługiwanych systemach operacyjnych.

Inne narzędzia programistyczne dla platformy Azure, takie jak Azure Developer CLI (azd), GitHub CLI, GitHub Copilot i Microsoft Dev Box, zostały omówione w rozdziale 14.

W tabeli 2.9 przedstawiono typowe usługi monitorowania na platformie Azure.

Tabela 2.9. Przegląd wybranych narzędzi do monitorowania platformy Azure

Narzędzia do monitorowania platformy Azure	Opis
Azure Monitor	Doskonałe narzędzie do maksymalizowania wydajności aplikacji poprzez zbieranie, analizowanie, wizualizowanie i automatyzowanie danych telemetrycznych na platformie Azure i w środowiskach lokalnych.
Application Insights	Udostępnia funkcje przydatne do zarządzania wydajnością aplikacji (APM), takie jak monitorowanie na żywo i automatyczne wykrywanie problemów z wydajnością.
Azure Advisor	Innowacyjne rozwiązanie w chmurze na platformie Azure, które pomaga ulepszyć procesy wdrażania, zalecając przydatne i wykonalne rozwiązania w celu zabezpieczenia zasobów, obniżenia kosztów i poprawy wydajności.
Log Analytics	Umożliwia edytowanie, uruchamianie zapytań dziennika i analizowanie danych zebranych przez dzienniki usług Azure Monitor (https://learn.microsoft.com/pl-pl/azure/azure-monitor/logs/data-platform-logs).

Podstawowe narzędzia deweloperskie, obsługiwane języki programowania dla platformy Azure, monitorowanie, sposoby rozwiązywania problemów i usługi DevOps zostaną szczegółowo omówione w rozdziale 11.

Migracja do chmury oraz usługi hybrydowe i wielochmurowe

Platforma Azure oferuje rozwiązania migracyjne i hybrydowe, które pomagają organizacjom w procesie migracji do chmury obliczeniowej.

W tabeli 2.10 przedstawiono typowe usługi migracji oraz rozwiązania hybrydowe i wielochmurowe platformy Azure.

Tabela 2.10. Przegląd usług platformy Azure dla migracji, chmury hybrydowej i konfiguracji wielochmurowej

Narzędzia wspomagające migrację do platformy Azure	Opis
Azure Database Migration Service	Pozwala uzyskać wskazówki i przydatne narzędzia do migracji baz danych z różnych zasobów lokalnych do Azure.
Azure Data Box	Rozwiązanie pozwalające na przesyłanie dużych ilości danych na platformę Azure i wykonywanie obliczeń brzegowych.
Azure Migrate	Wszystkie przewodniki i narzędzia potrzebne do migracji na platformę Azure.
Azure Arc	Zabezpieczanie, rozwijanie i obsługiwanie infrastruktury lokalnej, hybrydowej i wielochmurowej oraz aplikacji i usług platformy Azure w dowolnym miejscu.
Azure Stack	Tworzenie i uruchamianie aplikacji hybrydowych w centrach danych, lokalizacjach brzegowych, biurach zdalnych i w chmurze.

Więcej o szczegółach technicznych i o tym, jak rozpocząć proces migracji na platformę Azure oraz jak korzystać z rozwiązań chmury hybrydowej, dowiesz się w rozdziale 13.

Na tym zakończymy omawianie głównych kategorii i podstawowych usług na platformie Microsoft Azure. Wszystkie wymienione kategorie usług wraz z niektórymi innymi kategoriami przedstawionymi w tabeli 2.2 zostaną szczegółowo opisane wraz z przykładami w kolejnych rozdziałach.

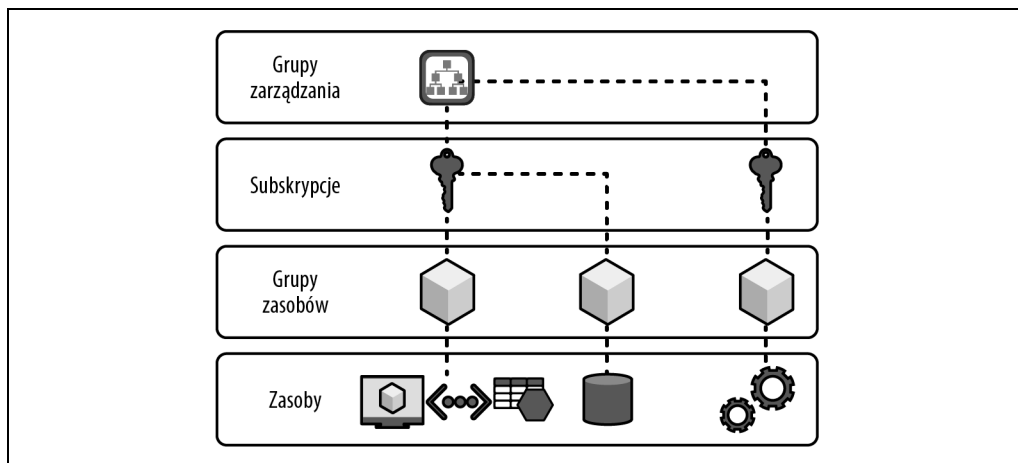
Podstawowa architektura i koncepcje zarządzania zasobami w Microsoft Azure

Organizacja korzystająca z platformy Microsoft Azure musi mieć administratora Azure, którego zadaniem będzie utworzenie i odpowiednie skonfigurowanie podstawowej struktury zarządzania zasobami. Jest to pierwsza i najważniejsza struktura, której utworzenie jest wymagane przed dodaniem innych zasobów do chmury. Utworzenie odpowiedniej struktury zarządzania zasobami jest bardzo korzystnym rozwiązaniem dla firm i organizacji podzielonych na różne działy i posiadających użytkowników spełniających różne role.

Istnieją cztery poziomy organizacji zasobów w Microsoft Azure. Jak pokazano na rysunku 2.4, patrząc od góry do dołu, mamy kolejno grupy zarządzania platformy Azure (ang. *management groups*), subskrypcje Azure (ang. *subscriptions*), grupy zasobów (ang. *resource groups*) i zasoby (ang. *resources*).

Grupy zarządzania platformy Azure

Grupy zarządzania platformy Azure to najwyższy poziom podstawowej struktury zarządzania zasobami w chmurze na platformie Azure. W grupach zarządzania administratorzy platformy Azure zarządzają wszystkim, co dotyczy dostępu użytkowników, zgodności i zasad dla subskrypcji. Subskrypcje w grupie zarządzania automatycznie dziedziczą ustawienia, warunki i ograniczenia dodane w grupie.



Rysunek 2.4. Cztery poziomy zasobów platformy Azure

Kontrola dostępu oparta na rolach platformy Azure (ang. *role-based access control* — RBAC) dla wszystkich zasobów i definicji ról jest obsługiwana w głównych grupach zarządzania (<https://learn.microsoft.com/pl-pl/azure/governance/management-groups/overview>). Osoba w organizacji z przydzieloną dowolną rolą Azure może zostać przypisana do grupy zarządzania platformy Azure. Osoby, które mają dostęp i prawa do grupy zarządzania, mogą grupować subskrypcje platformy Azure, wyświetlać grupy zarządzania i hierarchię organizacji, a przede wszystkim mogą kontrolować dostęp do dowolnej usługi lub zasobu platformy Azure, tworząc i stosując odpowiednią kontrolę ładu i zasady dostępu.

Subskrypcje Azure

Subskrypcje na platformie Azure są jak duży kontener dla wszystkich kont użytkowników i zasobów, do których uzyskali oni dostęp lub z których korzystali w ramach subskrypcji. Każda subskrypcja ma limit zasobów, które dany użytkownik może tworzyć i których może używać. Jako organizacja możesz używać subskrypcji do kontrolowania miesięcznych rachunków i kosztów zasobów w organizacji lub na własnym koncie Azure. Korzystając z subskrypcji platformy Azure, organizacja może również kontrolować zasoby tworzone, aktualizowane lub usuwane przez użytkowników.

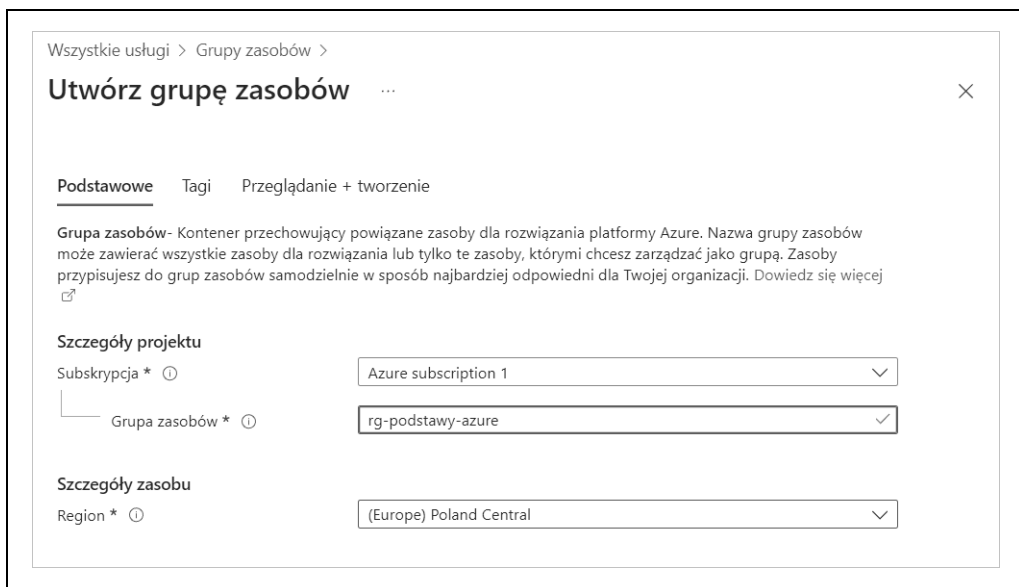
Grupy zasobów platformy Azure

Użytkownicy platformy Azure mogą grupować swoje usługi lub zasoby przy użyciu grup zasobów platformy Azure. Grupy zasobów w Microsoft Azure działają jako logiczne kontenery, w których wdrażane, zarządzane i przechowywane są różne zasoby, takie jak serwery, aplikacje internetowe, bazy danych, magazyn, monitorowanie itp. Nie należy mylić grup zasobów z zestawami dostępności na platformie Azure. Zestawy dostępności (<https://learn.microsoft.com/pl-pl/azure/virtual-machines/availability-set-overview>) to logiczne grupy maszyn wirtualnych.

Zasoby platformy Azure

Bazy danych, serwery, maszyny wirtualne lub aplikacje internetowe utworzone na platformie Azure są uważane za zasoby platformy Azure. Wszystkie utworzone zasoby lub usługi muszą zostać dodane do odpowiednich grup zasobów, które działają jako kontenery logiczne. W danej grupie zasobów można w jednym miejscu mieć aplikacje internetowe, serwery, monitorowanie, usługi obliczeniowe itp.

Podczas tworzenia nowych zasobów Azure, jak pokazano na rysunku 2.5, powinieneś najpierw wybrać subskrypcję Azure, a następnie grupę zasobów i region Azure, w którym mają zostać dodane zasoby, na przykład *(Europe) Poland Central*.



Wszystkie usługi > Grupy zasobów >

Utwórz grupę zasobów

Podstawowe Tagi Przeglądanie + tworzenie

Grupa zasobów - Kontener przechowujący powiązane zasoby dla rozwiązania platformy Azure. Nazwa grupy zasobów może zawierać wszystkie zasoby dla rozwiązania lub tylko te zasoby, którymi chcesz zarządzać jako grupą. Zasoby przypisujesz do grup zasobów samodzielnie w sposób najbardziej odpowiedni dla Twojej organizacji. Dowiedz się więcej

Szczegóły projektu

Subskrypcja * ⓘ Azure subscription 1

Grupa zasobów * ⓘ rg-podstawy-azure

Szczegóły zasobu

Region * ⓘ (Europe) Poland Central

Rysunek 2.5. Tworzenie grupy zasobów w portalu Azure

Zasoby platformy Azure można również grupować w różne kategorie, dodając odpowiednie tagi (<https://learn.microsoft.com/pl-pl/azure/azure-resource-manager/management/tag-resources>), jak pokazano na rysunku 2.6. Tagi zasobów (inaczej mówiąc, znaczniki zasobów) to zestawy par klucz-wartość składające się z nazwy tagu i przypisanej do niego wartości. Znaczniki zasobów można ustawiać w celu podzielenia zasobów na różne kategorie na potrzeby rozliczeń. Na przykład można zastosować odpowiednie tagi dla zasobów dla poszczególnych środowisk, takich jak zasoby Dev, Test, UAT czy Produkcja.

Przypisuj tagi do swoich zasobów platformy Azure, aby grupować je logicznie według kategorii. Tag składa się z klucza (nazwy) i wartości. W nazwach tagów wielkość liter nie jest uwzględniana, natomiast w wartościach tagów jest. Dowiedz się więcej [🔗](#)

Nazwa [ⓘ]	Wartość [ⓘ]	Zasób
Rozliczenia	: Demo	Grupa zasobów 
	:	Grupa zasobów

Rysunek 2.6. Wykorzystanie tagów do podziału zasobów platformy Azure na kategorie

Azure Resource Manager

Usługa Azure Resource Manager (ARM) jest bardzo ważnym elementem zarządzania zasobami na platformie Azure. ARM to usługa zarządzania i wdrażania, która zapewnia użytkownikom możliwość dodawania, edytowania i usuwania zasobów na platformie Azure. Korzystając z menedżera zasobów ARM, firma lub organizacja może zarządzać kontrolą dostępu użytkowników i bezpiecznie organizować zasoby również po wdrożeniu.

Szablony ARM są powszechnie używane do automatyzacji wdrożeń i implementacji usługi IaC (ang. *Infrastructure as Code*; infrastruktura jako kod, zobacz <https://learn.microsoft.com/pl-pl/devops/deliver/what-is-infrastructure-as-code>). Platforma Azure zapewnia natywną obsługę IaC przy użyciu szablonów ARM, a także języka Azure Bicep (<https://learn.microsoft.com/pl-pl/azure/azure-resource-manager/bicep/overview?tabs=bicep>) w Azure Resource Manager.

Na platformie Azure jest również obsługiwane narzędzie o nazwie Terraform (<https://learn.microsoft.com/pl-pl/azure/developer/terraform/overview>). Jest to narzędzie typu open source IaC służące do konfigurowania i wdrażania infrastruktury w chmurze, które znakomicie ułatwia automatyzację tego procesu. Korzystając z infrastruktury jako kodu, można zautomatyzować wdrażanie, generując za każdym razem odpowiednie szablony dla danego środowiska. Proces IaC (<https://learn.microsoft.com/pl-pl/devops/deliver/what-is-infrastructure-as-code>) minimalizuje problemy związane z dryfem środowiska podczas publikowania kolejnych wydań deweloperskich.

Platforma Azure zapewnia również obsługę innych zautomatyzowanych platform IaC, takich jak Terraform (<https://learn.microsoft.com/pl-pl/azure/developer/terraform/>), Red Hat Ansible (<https://www.redhat.com/en/technologies/management/ansible>), Chef Automate (https://docs.chef.io/azure_marketplace/) i Pulumi (<https://www.pulumi.com/azure/>).

Język Azure Bicep wykorzystuje deklaratywną, zwięzłą i bezpieczną składnię do wdrażania zasobów platformy Azure i jest uważany za język specyficzny dla domeny (ang. *domain-specific language* — DSL), który oferuje wysokiej klasy środowisko programistyczne, znakomicie ułatwiające tworzenie rozwiązań IaC na platformie Azure. Więcej szczegółowych informacji na temat aspektów technicznych znajdziesz w kolejnych rozdziałach tej książki.

Lokalizacje geograficzne, regiony, pary regionów i strefy dostępności platformy Azure

Globalna infrastruktura platformy Azure została zaprojektowana i zbudowana tak, aby zapewnić użytkownikom najlepszą możliwą odporność na awarię i wysoką dostępność zasobów w chmurze. Infrastruktura Azure składa się z różnych lokalizacji geograficznych, regionów i stref dostępności w wielu krajach na całym świecie, dlatego wiedza o tym, gdzie aprowizować zasoby w globalnej infrastrukturze Azure, znakomicie może ułatwić firmie czy organizacji zarządzanie zasobami w chmurze, zapewnienie zgodności, bezpieczeństwa i szybkości działania wdrażanych rozwiązań chmurowych.

Lokalizacje geograficzne Azure

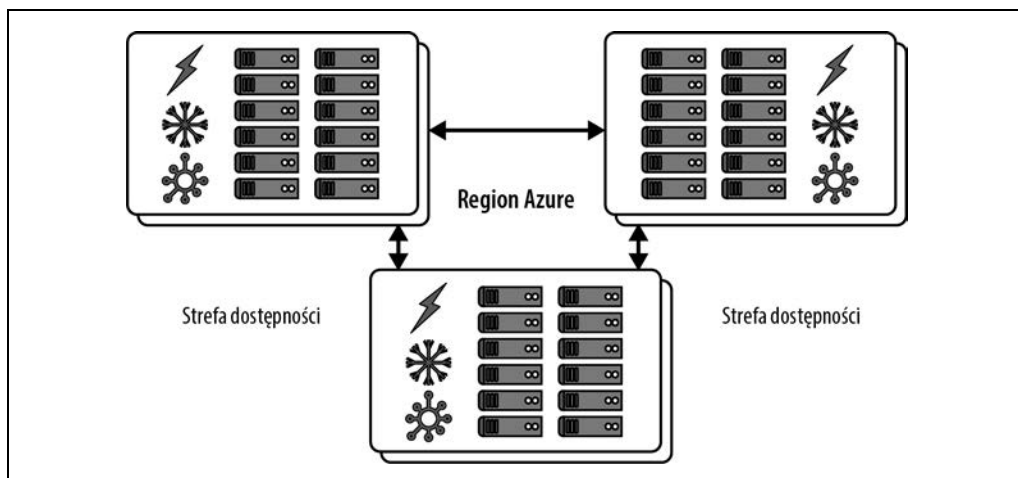
W czasie kiedy powstawała ta książka, platforma Microsoft Azure wykorzystywała fizyczne centra danych w 140 krajach na całym świecie. Globalna infrastruktura platformy Azure (<https://datacenters.microsoft.com/>), która obejmuje również infrastrukturę platformy chmury obliczeniowej firmy Microsoft, spełnia niezmiernie ważną rolę dla zapewnienia niezawodnych, bezpiecznych i innowacyjnych inteligentnych rozwiązań chmurowych. Jeżeli chciałbyś się dowiedzieć, gdzie znajdują się najbliższe centra danych platformy Azure, które spełniają Twoje wymagania, powinieneś zajrzeć na stronę <https://azure.microsoft.com/pl-pl/explore/global-infrastructure/geographies/#overview>, gdzie znajdziesz informacje o lokalizacjach geograficznych platformy Azure.

Regiony platformy Azure

Jak widać na przykładzie lokalizacji geograficznych platformy Azure, centra danych znajdują się w różnych regionach i krajach na całym świecie. Regiony Azure odgrywają istotną rolę w chmurze obliczeniowej, ponieważ każdy kraj lub region ma swoje unikalne ograniczenia, zasady, wymagania zgodności oraz reguły i przepisy prawne. Na rysunku 2.7 przedstawiono przykład regionu Azure z trzema strefami dostępności.

Spośród wszystkich wiodących dostawców chmury na świecie to właśnie platforma Azure ma najwięcej globalnych regionów geograficznych. Przy obecnym globalnym, międzynarodowym rynku biznesowym, możliwość wyboru lokalizacji geograficznej i regionalizacji zasobów zapewnia ogromną elastyczność i niezawodność działania. Wybór odpowiedniego regionu geograficznego Azure jest również ważny ze względu na konieczność zapewnienia zgodności z regulacjami i przepisami prawa dotyczącymi przetwarzania danych, takimi jak ogólne rozporządzenia o ochronie danych, takie jak RODO (GDPR) w Europie (<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr>).

Przed dodaniem zasobów na platformie Azure firma czy organizacja powinna najpierw sprawdzić, czy w danym obszarze geograficznym istnieją jakieś specyficzne normy prawne, rozporządzenia lub inne regulacje wymagające spełnienia i zapewnienia zgodności. Microsoft Azure publikuje listę ofert rozwiązań dla zapewnienia zgodności (<https://learn.microsoft.com/pl-pl/azure/compliance/>) dla różnych sektorów na całym świecie, którą możesz przejrzeć, aby dowiedzieć się czegoś więcej na ten temat.



Rysunek 2.7. Przykład regionu Azure z trzema strefami dostępności

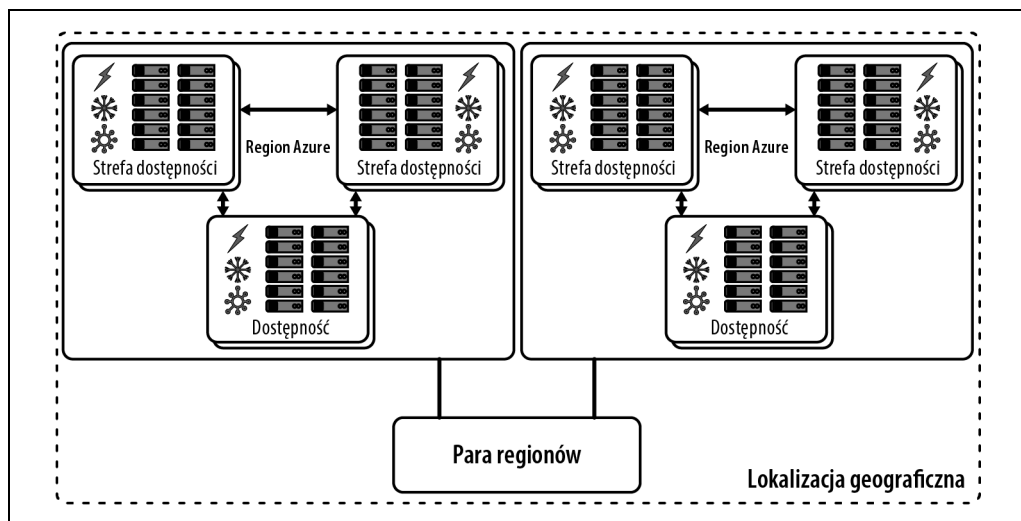
Pary regionów Azure

Zazwyczaj strefy dostępności są tworzone przy użyciu jednego lub większej liczby centrów danych. W każdym regionie znajdują się co najmniej trzy strefy. Co się jednak dzieje, jeżeli dwie z tych trzech stref przestaną działać z powodu ogromnej awarii? Gdyby jednocześnie dwa centra danych znajdujące się w tym samym regionie Azure nagle przestały działać, utrzymanie zasobów w działaniu na odpowiednim poziomie byłoby niezwykle trudne. Z tego właśnie względu użytkownicy platformy Azure mają również możliwość korzystania z par regionów platformy Azure (ang. *Azure region pairs*).

Mechanizm parowania regionów platformy Azure, jak pokazano na rysunku 2.8, pozwala na replikowanie zasobów regionu podstawowego z innym regionem (tzw. regionem pomocniczym), znajdującym się w tej samej lokalizacji geograficznej. Dzięki parowaniu regionów w tej samej lokalizacji użytkownicy mogą replikować swoje zasoby, takie jak serwery, maszyny wirtualne, bazy danych i magazyn, w innej lokalizacji, co zapewnia dodatkową ochronę w przypadku awarii zasilania, klęsk żywiołowych itp.

Jeżeli dany region w parze ulegnie awarii, usługi zostaną automatycznie przełączone do drugiego regionu w parze.

Regiony platformy Azure są zwykle parowane z innymi regionami tej samej lokalizacji geograficznej. Na przykład, jeżeli dany region znajduje się w Europie, oczekuje się, że jego region pomocniczy, z którym jest sparowany, również znajduje się w Europie, ale w odległości co najmniej 300 mil (ok. 483 km). Taka minimalna odległość między fizycznymi centrami danych Azure w parze regionalnej jest preferowana (o ile to oczywiście możliwe) ze względu na konieczność zapewnienia bezpieczeństwa i działania w przypadku klęsk żywiołowych, rozległych przerw w dostawie prądu itp. Para regionów platformy Azure powinna znajdować się w tej samej lokalizacji geograficznej, aby zapewnić niezawodność działania w przypadku nieoczekiwanych przerw, zakłóceń i awarii.



Rysunek 2.8. Pary regionów platformy Azure



Aby dowiedzieć się czegoś więcej, powinieneś zapoznać się z informacjami na temat sposobów zapewniania ciągłości działania i odzyskiwania po awarii (ang. *business continuity and disaster recovery* — BCDR) oraz replikowania danych między sparowanymi regionami platformy Azure (<https://learn.microsoft.com/pl-pl/azure/reliability/cross-region-replication-azure>).

Strefy dostępności platformy Azure

Jeżeli firma czy organizacja chce zapewnić nadmiarowość aplikacji i zasobów w chmurze w celu ochrony przed awariami lub innymi problemami, rozwiązaniem są strefy dostępności platformy Azure (ang. *Azure availability zones*). Takie strefy są unikalnymi fizycznymi lokalizacjami lub centrami danych w regionie Azure, które zapewniają SLA na poziomie 99,99% dla czasu pracy maszyn wirtualnych.

Należy jednak pamiętać, że strefy dostępności nie są dostępne we wszystkich regionach i dla wszystkich usług platformy Azure. W strefach dostępności obsługiwane są takie usługi jak SQL Managed Identity, Azure App Services i Azure Virtual Machines (Azure VMs).

Usługi platformy Azure obsługiwane w strefach dostępności pozwalają na zapewnienie odporności, wydajności, minimalnych opóźnień działania, elastyczności i skalowalności. Więcej informacji na temat usług obsługiwanych w strefach dostępności platformy Azure w poszczególnych regionach można znaleźć w dokumentacji platformy Azure (<https://learn.microsoft.com/pl-pl/azure/reliability/availability-zones-service-support>).

Strefa dostępności składa się z jednego lub wielu centrów danych z niezależnymi systemami zasilania, obsługi sieci, systemami chłodzenia i wsparcia. Celem takiej izolacji stref jest zapewnienie, że w przypadku, gdy jedna ze stref ulegnie awarii, druga strefa nadal będzie działać poprawnie. Takie strefy

dostępności są ze sobą połączone za pomocą bezpiecznych, szybkich sieci, co jest ważne przy uruchamianiu krytycznych zasobów obliczeniowych, sieciowych, pamięci masowej i danych.

Czym różnią się strefy dostępności i zestawy dostępności dla maszyn wirtualnych (<https://learn.microsoft.com/pl-pl/azure/virtual-machines/availability#availability-sets>)? Strefy dostępności służą do ochrony zasobów przed poważnymi awariami systemu w centrum danych platformy Azure, podczas gdy zestawy dostępności zapewniają ochronę aplikacji przed awariami sprzętu w centrum danych platformy Azure.



Jeżeli Twoja organizacja ma takie wymagania, to za dodatkową opłatą (zgodnie z cennikiem usług Azure) możesz replikować lub przenosić dane i zasoby do innej strefy dostępności. Przykładem zasobów, które można przenieść do strefy dostępności w innym regionie, są maszyny wirtualne Azure (<https://learn.microsoft.com/pl-pl/azure/site-recovery/move-azure-vms-avset-azone>).

Zarządzanie kosztami w Microsoft Azure

Oprócz organizowania zasobów w chmurze przy użyciu mechanizmów zarządzania platformy Azure, grup zasobów, tagów i upewniania się, że zasoby znajdują się we właściwym regionie, możliwe jest również zarządzanie finansowymi aspektami wykorzystania usług chmurowych przez firmę czy organizację.

Narzędzia do zarządzania kosztami platformy Azure pomagają firmom i organizacjom monitorować koszty wykorzystywania zasobów i usług w chmurze. Można to zrobić, ustawiając odpowiednie poziomy alertów budżetowych i powiadomień dla zespołu rozliczeniowego lub księgowego, a także szacując z wyprzedzeniem możliwe miesięczne lub roczne koszty związane z użytkowaniem chmury, co pomaga w dokładnym zaplanowaniu kosztów i przygotowaniu budżetu. Do wyboru mamy tutaj między innymi następujące narzędzia:

Usługa Azure Cost Management + Billing

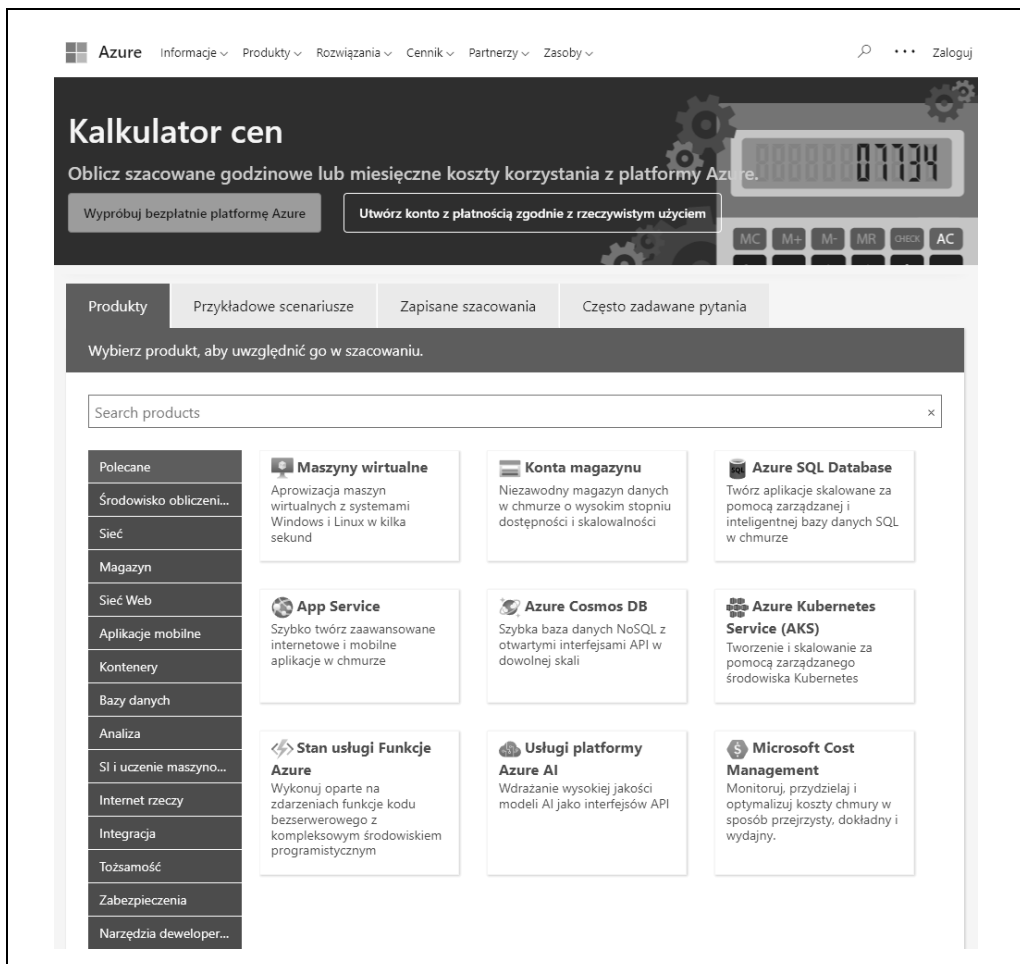
Usługa Microsoft Azure, która pozwala na kontrolowanie i monitorowanie rozliczeń oraz zarządzanie kosztami (<https://learn.microsoft.com/pl-pl/azure/cost-management-billing/cost-management-billing-overview>).

Kalkulator całkowitego kosztu posiadania (TCO)

Narzędzie, które pomaga firmom i organizacjom oszacować oszczędności kosztów wynikające z migracji obciążeń na platformę Azure (<https://azure.microsoft.com/pl-pl/pricing/tco/calculator/>).

Kalkulator cen platformy Azure

Dedykowana witryna internetowa, która pozwala na obliczanie szacowanych godzinowych lub miesięcznych kosztów produktów i usług platformy Azure (<https://azure.microsoft.com/pl-pl/pricing/calculator/>) na podstawie określonych scenariuszy użycia w projektach. Wyniki szacowania kosztów można zapisywać, eksportować i udostępniać, jak pokazano na rysunku 2.9.



Rysunek 2.9. Szacowanie kosztów usług lub wykorzystania zasobów Azure przy użyciu kalkulatora kosztów

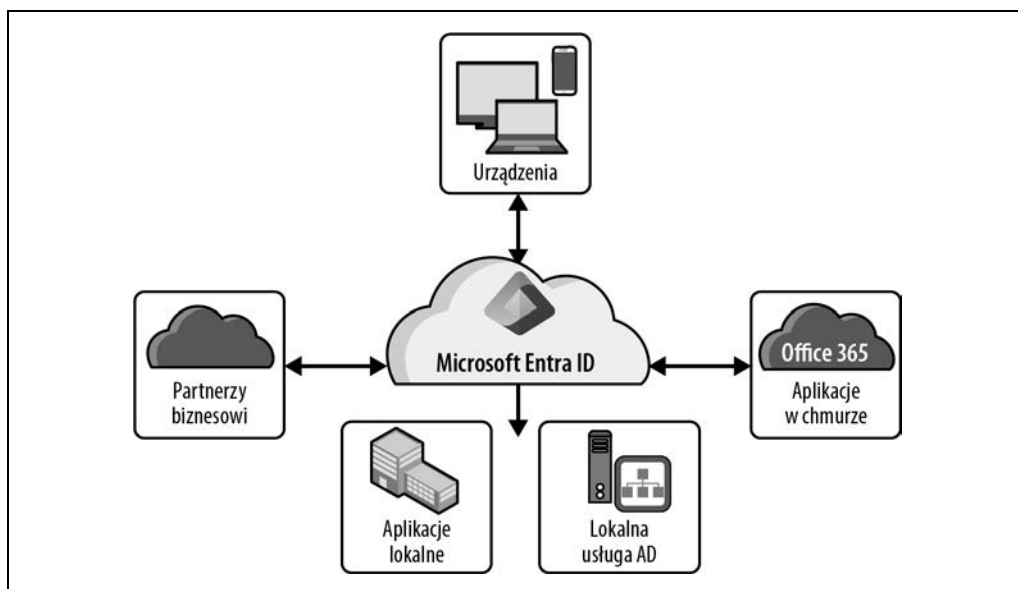


Więcej szczegółowych informacji na temat najlepszych praktyk w zakresie rozliczeń i zarządzania kosztami platformy Azure znajdziesz w dokumentacji firmy Microsoft (<https://learn.microsoft.com/pl-pl/azure/cost-management-billing/>).

Tożsamości użytkowników, role i usługa Active Directory na platformie Azure

Oprócz strukturyzowania zasobów w chmurze przy użyciu grup zarządzania, subskrypcji i grup zasobów niezmiernie ważnym czynnikiem jest również odpowiednie kontrolowanie tożsamości użytkowników i dostępu do zasobów.

Microsoft Entra ID, jak pokazano na rysunku 2.10, jest usługą firmy Microsoft przeznaczoną do zarządzania tożsamościami i dostępem użytkowników. Użytkownicy Microsoft Entra ID mogą zarządzać swoimi tożsamościami, rolami, kontami i dostępem do zasobów wewnętrznych, a także uprawnieniami do usług zewnętrznych, takich jak portal Azure, Office 365 i inne aplikacje.



Rysunek 2.10. Usługa Microsoft Entra ID do zarządzania tożsamościami i dostępem użytkowników

Kontrola dostępu oparta na rolach Azure

Niezmiernie ważną sprawą dla każdej firmy i organizacji jest to, aby mieć możliwość zarządzania dostępem użytkowników do zasobów w chmurze i grup zasobów na platformie Microsoft Azure. Kontrola dostępu oparta na rolach (ang. *Azure Role-based Access Control* — RBAC) pomaga w autoryzacji i zarządzaniu dostępem użytkowników do zasobów na platformie Azure. Zarządzanie tożsamościami przy użyciu Azure RBAC pomaga kontrolować, co użytkownicy mogą robić, a czego nie, w zależności od roli, jaką pełnią w organizacji.

Na przykład dzięki wykorzystaniu Azure RBAC możemy zezwolić administratorom baz danych na zarządzanie tylko zasobami platformy Azure związanymi z bazami danych w ramach grupy zasobów. Inny poziom dostępu możemy skonfigurować np. dla programistów lub inżynierów oprogramowania, którzy pracują nad rozwojem aplikacji na platformie chmurowej.

Aby dowiedzieć się czegoś więcej o Azure RBAC, obejrzyj film o kontroli dostępu opartej na rolach Azure (<https://www.youtube.com/watch?v=1OBi93apLdo>).

Role na platformie Azure

Aby kontrolować dostęp do zasobów na platformie Azure, należy skonfigurować i wymusić uprawnienia użytkowników, przypisując im odpowiednie *role platformy Azure* (ang. *Azure roles*). Aby

przypisać rolę Azure, musisz wybrać takie elementy jak podmiot zabezpieczeń (ang. *security principal*), definicja roli i jej zakres (rysunek 2.10).

Podmiot zabezpieczeń

Podmiot zabezpieczeń to obiekt reprezentujący tożsamość zabezpieczeń, która może być uwierzytelniana i autoryzowana do uzyskiwania dostępu do zasobów. Role Azure mogą przyznawać lub odbierać uprawnienia do zasobów wskazanym podmiotom zabezpieczeń. Podmiotami zabezpieczeń mogą być użytkownicy, grupy, jednostki usług (ang. *service principal*) lub procesy, które działają w kontekście konta komputera. Podmiot zabezpieczeń lub grupę można zidentyfikować w systemie operacyjnym komputera przy użyciu unikatowego identyfikatora SID (ang. *Security Identifier*; zobacz <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers#how-security-identifiers-work>). Przypisując odpowiednie role do podmiotu zabezpieczeń, udzielasz lub odmawiasz mu uprawnień dostępu do określonych zasobów na platformie Azure. Na przykład możesz ustawić rolę „współautor” (ang. *contributor*) dla danego użytkownika, umożliwiając mu tworzenie zasobów i zarządzanie nimi w określonej subskrypcji platformy Azure. Zrozumienie ról platformy Azure ma kluczowe znaczenie dla zapewnienia bezpieczeństwa i zgodności środowiska platformy Azure. Więcej szczegółowych informacji na temat bezpieczeństwa i zarządzania tożsamościami na platformie Azure znajdziesz w rozdziale 9.

Definicja roli

Definicja roli ustawia uprawnienia dla użytkowników platformy Azure lub innych podmiotów zabezpieczeń do korzystania z zasobów platformy Azure. Każda definicja roli ma zestaw kontroli dostępu lub akcji określających, które działania związane z zasobami platformy Azure są dozwolone. Definicja roli może zezwalać na odczytywanie, zapisywanie i usuwanie zasobów subskrypcji platformy Azure. Uprawnienia roli podmiotu zabezpieczeń mają zastosowanie do przypisanych zasobów. Wbudowane, domyślne definicje ról, takich jak współautor (ang. *contributor*) i czytelnik (ang. *reader*), dotyczą typowych scenariuszy dostępu do zasobów, ale w razie potrzeby można dostosować ich opisy lub utworzyć role o zupełnie nowych nazwach. Oczywiście istnieje również możliwość odpowiedniego zdefiniowania ról, co pozwala precyzyjnie dopasować poziom dostępu do indywidualnych potrzeb firmy. Definicje ról platformy Azure umożliwiają elastyczne i szczegółowe zarządzanie dostępem do zasobów.

Zakres

Zakres roli określa poziom, na którym ma zastosowanie przypisanie roli, i definiuje zestaw zasobów, do których ma zastosowanie dana rola. Zakres roli można ustawić na różnych poziomach w hierarchii zasobów platformy Azure, w tym na poziomie grupy zarządzania, subskrypcji, grupy zasobów i poszczególnych zasobów. Określając zakres przypisania roli, można zminimalizować ryzyko nieautoryzowanego i przypadkowego dostępu do określonych zasobów oraz wynikające z tego konsekwencje. Zarządzanie dostępem do zasobów platformy Azure oraz zapewnianie bezpieczeństwa i zgodności wymaga dobrego zrozumienia zakresów przypisania roli.

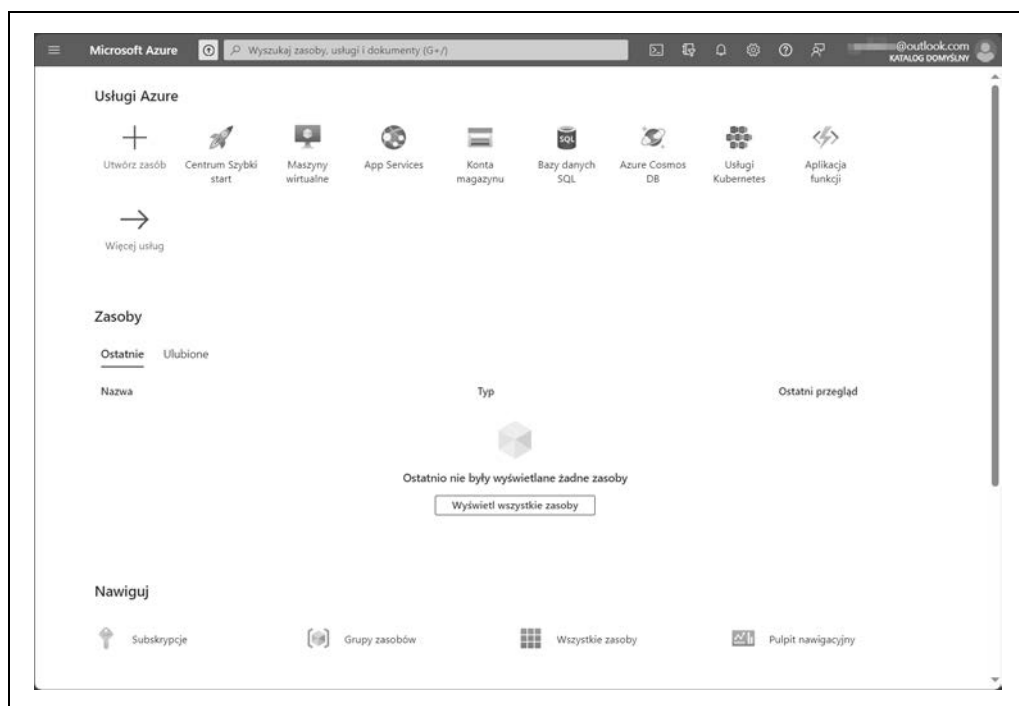
Jak wspominałam już wcześniej w tej sekcji, zakresy w Microsoft Azure mają czteropoziomową strukturę hierarchiczną i działają zgodnie z regułami dziedziczenia z poziomów nadrzędnych do podrzędnych.

Zrób to sam!

W tym rozdziale poznałeś już kilka podstawowych usług w chmurze platformy Azure, a w tej sekcji znajdziesz kilka praktycznych ćwiczeń, które pomogą lepiej zrozumieć omawiane zagadnienia i utrwalić zdobytą wiedzę.

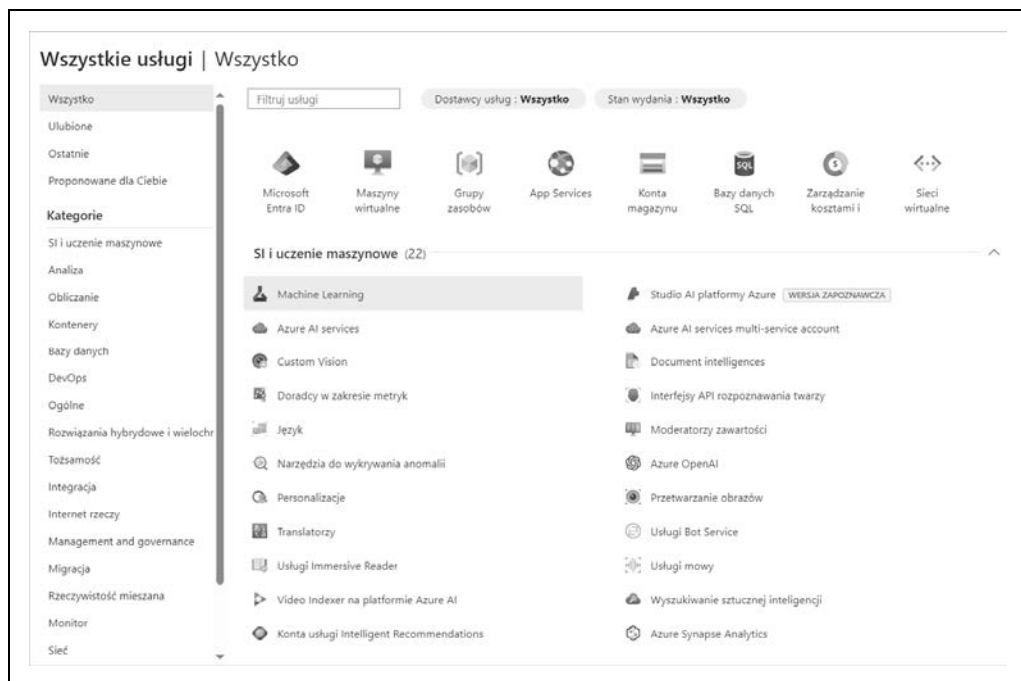
Microsoft Azure Portal — ćwiczenia praktyczne

1. Jeżeli masz już subskrypcję Microsoft Azure, wejdź na stronę <https://portal.azure.com>.
2. Jeżeli nie masz jeszcze subskrypcji, utwórz bezpłatne konto Azure na stronie <https://azure.microsoft.com/pl-pl/free>.
3. Po zalogowaniu przyjrzyj się głównej stronie portalu Azure, pokazanej na rysunku 2.11. Po lewej stronie znajdziesz pasek nawigacyjny z domyślną listą usług Azure; na stronie głównej znajduje się również pulpit nawigacyjny i pasek wyszukiwania. Na pasku narzędzi w prawym górnym rogu okna portalu możesz uzyskać dostęp do usług *Cloud Shell*, *Katalogi* i *subskrypcje*, *Powiadomienia*, *Ustawienia* oraz *Pomoc techniczna i rozwiązywanie problemów*, a także do opcji zarządzania swoim kontem.



Rysunek 2.11. Wygląd portalu Azure po utworzeniu nowego konta i zalogowaniu się

4. Kliknij opcję *Wszystkie usługi*, znajdującą się w menu po lewej stronie okna, i zapoznaj się z listą dostępnych usług Azure (rysunek 2.12).



Rysunek 2.12. Wszystkie usługi w portalu Azure

5. Znajdź listę bezpłatnych usług na platformie Microsoft Azure lub po prostu od razu przejdź na stronę https://portal.azure.com/#view/Microsoft_Azure_Billing/FreeServicesBlade, gdzie znajdziesz listę bezpłatnych usług dostępnych przez 12 miesięcy na bezpłatnym koncie Azure.

Podsumowanie

W tym rozdziale omawialiśmy szereg podstawowych zagadnień związanych z funkcjonowaniem chmury publicznej Microsoft Azure. Poznałeś wiele usług Azure podzielonych na różne kategorie, np. obliczenia, magazyn, sieci, bazy danych, narzędzia deweloperskie, integracja, analiza i inne. Zasoby na platformie Azure można organizować na różnych poziomach: grupy zarządzania Azure, subskrypcje, grupy zasobów i same zasoby. Platforma Azure oferuje wygodne narzędzia do zarządzania kosztami, a także wykorzystuje strefy dostępności i parowanie regionów w celu zapewnienia wysokiego poziomu ochrony danych i zasobów w przypadku awarii. Usługa Microsoft Entra ID umożliwia zarządzanie użytkownikami i tożsamościami i pozwala na kontrolowanie dostępu i wykorzystania zasobów platformy Azure.

Kontrola dostępu oparta na rolach na platformie Azure (RBAC) to jedna z metod kontroli dostępu użytkowników i zarządzania tożsamościami, gdzie podczas tworzenia roli musisz podać trzy ważne elementy: podmiot zabezpieczeń, definicję roli i zakres. Dowiedziałeś się również, że szablony Azure Resource Manager (ARM) i Terraform służą do automatyzacji wdrożeń na platformie Azure i implementacji infrastruktury jako kodu (IaC).

Najważniejsze usługi Azure, które poznałeś w tym rozdziale, zostaną szczegółowo opisane w kolejnych rozdziałach tej książki.

Sprawdź swoją wiedzę

1. Czy można mieć dwie pary regionów Azure w różnych lokalizacjach geograficznych? (prawda czy fałsz)
2. Azure Marketplace to miejsce, gdzie użytkownicy platformy Azure mogą kupować i wypróbować aplikacje i usługi od innych dostawców usług i firm partnerskich Microsoft (prawda czy fałsz).
3. Jakie są najważniejsze kategorie podstawowych usług na platformie Azure?
4. Zestawy skalowania maszyn wirtualnych platformy Azure (ang. *Azure Virtual Machine Scale Sets*) to usługi obliczeniowa potrzebna do tworzenia aplikacji sterowanych zdarzeniami w środowisku bezserwerowym (prawda czy fałsz).
5. Jaka jest różnica między *regionem platformy Azure* a *zestawem dostępności*?

Odpowiedzi na powyższe pytania znajdziesz w „Dodatku”.

Gdzie warto zajrzeć?

- *Co to jest platforma Azure?*, dokumentacja Microsoft Azure; <https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-is-azure/>.
- *Dokumentacja usługi Azure Blob Storage*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/azure/storage/blobs/>.
- *Globalna infrastruktura platformy Azure*, dokumentacja Microsoft Azure; <https://azure.microsoft.com/pl-pl/explore/global-infrastructure/>.
- Kleppman Martin, *Designing Data-Intensive Applications*, O'Reilly Media, Sebastopol, CA, 2017.
- *Kontrolowanie i porządkowanie zasobów platformy Azure za pomocą usługi Azure Resource Manager*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/training/modules/control-and-organize-with-azure-resource-manager/>.
- Microsoft Azure, *What Is Azure Role-Based Access Control (RBAC)? | One Dev Question: Arturo Lucatero*, YouTube, 23 czerwca 2020; https://www.youtube.com/watch?v=Dzhm-garKBM&ab_channel=MicrosoftAzure.
- O'Connell Ryan, *Azure Real World Hand-on Training for Beginners*, Udemy; <https://www.udemy.com/course/azure-real-world-hand-on-training-for-beginners/>.
- *Podstawy platformy Microsoft Azure: opis architektury i usług platformy Azure*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/training/paths/azure-fundamentals-describe-azure-architecture-services/>.
- *Podstawy platformy Microsoft Azure: opis pojęć związanych z chmurą*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/training/paths/microsoft-azure-fundamentals-describe-cloud-concepts/>.

- *Podstawy platformy Microsoft Azure: opis zarządzania i ładu na platformie Azure*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/training/paths/describe-azure-management-governance/>.
- Polkovnikov Alexey, *Welcome to Azure Charts!*, Azure Charts; <https://azurecharts.com/>.
- *Produkty platformy Azure*, dokumentacja Microsoft Azure; <https://azure.microsoft.com/pl-pl/products/>.
- *Szybki start: sprawdzanie dostępu użytkownika do pojedynczego zasobu platformy Azure*, Microsoft Learn; <https://learn.microsoft.com/pl-pl/azure/role-based-access-control/check-access>.
- *Tworzenie w chmurze za pomocą bezpłatnego konta platformy Azure*, dokumentacja Microsoft Azure; <https://azure.microsoft.com/pl-pl/free/>.

A

- Active Directory, 91
 - usługi federacyjne, 283
- Agile, 41
- AI, artificial intelligence, 203
- AI Builder, 219
- Alibaba Cloud, 57
- Amazon Web Services, AWS, 53, 56
- analiza danych, data analytics, 233, 235–42
 - deskryptywna, 234
 - diagnostyczna, diagnostic data analytics, 234
 - Power BI, 240
 - predykcyjna, predictive data analytics, 234
 - preskryptywna, prescriptive data analytics, 234
- antywzorce migracji, 395
- API, Application Programming Interface, 310
- aplikacja
 - Azure IoT Plug and Play, 253
 - mobilna Azure, 74
- aplikacje
 - internetowe statyczne, 113
 - jednostronicowe, SPA, 111, 113
 - niezawodność i skalowalność, 307
 - skonteneryzowane, 134
 - środowiska IDE, 421
 - wykorzystujące Azure Maps, 261
- App Configuration, 82
- Application Insights, 359
- architektura chmurowa dla mikrousług, 338
- atak typu
 - DDoS, 267
 - Man-in-the-middle, 269
 - ransomware, 266
 - SQL injection, 269
- automatyzacja, 299
 - infrastruktury, 350
 - procesów, 398
- AutoML, Automated Machine Learning, 218
- autoryzacja, 279
- Azure, 63
 - Advisor, 82, 360
 - AI, 214
 - Analysis Services, 240
 - API Management, APIM, 313
 - brama interfejsu API, 316
 - komponenty usługi, 316
 - modele cenowe, 313
 - platforma zarządzania, 317
 - zalety, 314
 - zasoby platformy, 315
 - App Service, 108
 - implementacja usługi, 110
 - korzyści, 110, 111
 - plan usługi, 111
 - Application Gateway, 169
 - Applied AI Services, 220
 - Arc, 83, 413
 - Arc-Enabled Kubernetes, 414
 - Automation, 378
 - automatyzacja DevOps, 379
 - korzyści, 378
 - przegląd usługi, 378
 - scenariusze użycia, 379
 - Bastion, 158, 290
 - korzyści, 158
 - zastosowania, 158
 - Blob Storage, 184, 185
 - składniki usługi, 185
 - Blueprints, 373
 - automatyzacja wdrażania, 373
 - korzyści, 374

- Blueprints
 - wdrażanie strategii usługi, 374
 - Zero Trust Security, 375
- CDN, 172
- CLI, 428
 - zalety interfejsu, 429
- Cloud Networking, 145
- Cloud Shell, 427
 - funkcja IntelliSense, 432
- Cognitive Services, 214
 - kategorie usług, 215
- Compute, 101
- Container Apps, ACA, 136
 - korzyści, 138
 - struktura usługi, 138
 - zastosowania, 138
- Container Instances, ACI, 136
- Container Registry, ACR, 135
 - tworzenie rejestru, 135
- Cosmos DB, 192
 - globalna dystrybucja, 196, 198
 - interfejsy API, 195
 - korzyści, 192
 - poziomy spójności, 194
 - replikacja, 196
 - wybór rozwiązań, 193
- Data Box, 83
- Data Catalog, 231
- Data Factory, ADF, 230, 239
- Data Lake, 236
- Data Lake Storage, 238
- Database, 80
 - Azure Cache for Redis DB, 80
 - Azure Cosmos DB, 80
 - Azure Database for PostgreSQL, 80
 - Azure SQL Database, 80
 - Azure SQL Edge, 80
- Database Migration Service, 83
- Database Services, 190
- Databricks, 238
- DDoS Protection, 160, 290
- Deployment Environ, 436
- Developer CLI, 433
- DevOps, 41, 82, 345, 438
- DevTest Labs, 82, 104, 347
- Digital Twins, 253
 - wdrażanie usługi, 256
- DNS, 157
- Durable Functions, 117
 - cechy i zalety, 118
 - komponenty składowe, 118
 - tworzenie stanowych przepływów pracy, 127
 - wzorce aplikacji, 127
- Event Grid, 260, 332
- ExpressRoute, 415
 - bezpieczne połączenie sieciowe, 152
 - funkcje, 152
 - modele połączeń, 153
- Files, 185
 - zalety, 187
 - zastosowania, 187
- Firewall, 159, 290
- Front Door, 168
- Functions, 116
- HDInsight, 235, 238
- Hypervisor, 43
- IAM, 279
- Identity Management and Security Services
 - Azure DDoS Protection, 81
 - Azure Information Protection, 81
 - Azure Key Vault, 81
 - Microsoft Defender for Cloud, 81
 - Microsoft Entra ID, 81
 - Microsoft Sentinel, 81
- IoT, 245, 251
 - aprowizacja urządzeń, 252
 - komponenty, 252
- IoT Central, 252
- IoT Hub, 252
- IoT Plug and Play, 253
- Key Vault, 289
 - scenariusze użycia usługi, 289
- Kubernetes, 135
- Kubernetes Service, AKS, 135, 139
 - architektura mikrousług, 141
- Load Balance, 164
 - działanie usługi, 165
 - komponenty składowe, 166
 - równoważenie obciążenia, 167
- Log Analytics, 359
- Logic Apps, 41, 317
 - komponenty, 320
 - korzyści, 318
 - modele cenowe, 318

- Machine Learning, 216
 - cykl rozwoju usługi, 216
- Machine Learning Studio, 217
 - zastosowania, 217
- Managed Disks, 185, 189
 - zalety, 190
 - zastosowania, 190
- Maps, 257
 - aplikacje korzystające z usługi, 261
 - integracja z Azure Event Grid, 260
 - mapowanie geoprzestrzenne, 257
 - pakiety SDK, 262
 - uwierzytelnianie, 259
 - zabezpieczenia, 259
 - zakres geograficzny usługi, 259
- Maps Android SDK, 262
- Maps iOS SDK, 262
- Maps Search, 261
- Maps Web SDK, 262
- Migrate, 83
- Monitor, 82, 359, 376
 - korzyści, 376
 - przegląd usługi, 377
- Monitor Network Insights, 174
- MXCHIP IoT DevKit, 253
- NAT, 155
 - funkcje usługi, 155
- Network Watcher, 173, 359
- NoSQL, 236
- OpenAI, 205
 - technologie AI, 205
- Policy, 379
 - zarządzanie politykami, 379
 - zarządzanie zgodnością, 379
 - zastosowania, 380
- Portal, 73, 94
- PowerShell, 431
- Private Link, 161
- Quantum, 142
- Queue Storage, 187
- Queues, 185
- Resource Groups, 371
- Resource Locks, 372
- Resource Manager, ARM, 70, 86, 353, 370
 - blokowanie zasobów, 372
 - grupowanie zasobów, 371
 - szablony, 86
 - zarządzanie zasobami, 370
- SDK, 425
- Service Bus, 321
 - kolejki, queues, 325
 - przestrzenie nazw, namespaces, 324
 - subskrypcje, subscriptions, 325
 - tematy, topics, 325
- Site Recovery, 415
- Space, 174
- SQL, 80, 191
 - opcje wdrażania, 191
- Stack, 83, 414
- Static Web Apps, 113
 - korzyści, 113
 - plany cenowe, 114
 - zastosowania, 113
- Storage, 79, 183
 - bezpieczeństwo usługi, 189
 - opcje usługi, 185
 - Azure Blobs, 79
 - Azure Files, 79
 - Azure Managed Disks, 79
 - Azure Queues, 79
- Stream Analytics, 236
- Synapse Analytics, 237
- Table Storage, 188
- Tables, 185
- Traffic Manager, 170
 - użycie usługi, 171
 - zalety, 170
- Virtual Network NAT, 155
- Virtual WAN, 150
 - wdrożenie usługi, 151
- VMware Solution, 414
- VNet
 - karty VNIC, 147
 - komunikacja, 148
- VNet Peering
 - komunikacja, 149
- VNet, Azure Virtual Network, 147
- VNet Peering, Azure Virtual Network
 - Peering, 148
- VPN Gateway, 415
- Web App for Containers, 111
 - architektura usługi, 112
- Web Application Firewall, 162
- Web PubSub, 327
 - działanie usługi, 330
 - modele cenowe, 327

Web PubSub

- obsługa komunikatów, 327
- przepływ pracy, 332
- wzorzec architektury, 329
- zalety, 330

Well-Architected Review, 410

B

BaaS, zaplecze jako usługa, 59, 60

baza danych NoSQL, 192

bazy danych, 179

- niestrukuralne, 181
- strukuralne, 181

bezpieczeństwo, 80, 265

aplikacji, 297

DevSecOps, 275, 297

infrastruktury Azure, 273

metodologia Zero Trust, 271

Microsoft Sentinel, 291

najlepsze praktyki, 296

protokołów komunikacji, 297

przesunięcie w lewo, 276, 277

przesunięcie w prawo, 276, 277

rodzaje zagrożeń, 266

usługi Azure Storage, 189

w chmurze, 64

zabezpieczenia

- dla aplikacji, 278
- dla baz danych, 278
- dla sieci, 278, 290

biblioteka DTFx, 118

big data, 181, 226, 235

Azure NoSQL, 236

korzyści, 235

scenariusze użycia, 229

środowisko produkcyjne, 233

tworzenie złożonych potoków, 230

wdrażanie rozwiązań, 231

błędna konfiguracja zasobów w chmurze, 268

boty konwersacyjne, 206

brama

interfejsu API, 316

NAT, 155

VPN, Azure VPN Gateway, 154

typy połączeń, 154

broker komunikatów, 321

C

CaaS, kontenery jako usługa, 62

CaC, configuration as code, 356

CAP, Conditional Access Policies, 285

CD, continuous delivery, 340

CDN, Content Delivery Network, 57, 172

centrum danych, 42

Chat-GPT, 205

chmura obliczeniowa, cloud computing, 39

hybrydowa, hybrid cloud, 47, 52, 54, 413

konfiguracja wielochmurowa, 53

prywatna, private cloud, 47, 49

publiczna, public cloud, 47–49, 56

rozwiązania wielochmurowe, 413

społecznościowa, community cloud, 47, 50

- infrastruktura, 51

chmury obliczeniowe

automatyzacja infrastruktury, 338

bazy danych, 179

bezpieczeństwo, 64

biznesu i klientów, 66

dla firm z branży IT, 66

dostawcy, 56, 71

Alibaba Cloud, 57

Amazon Web Services, AWS, 53, 56

Google Cloud Platform, GCP, 53, 57

IBM Cloud, 53

Microsoft Azure, 53, 56, 71

Oracle Cloud, 57

etapy wdrażania, 390

klastry obliczeniowe, 45

konteneryzacja aplikacji, 338

model wspólnej odpowiedzialności, 63

modele usług, 58

modele wdrażania, 47

orkiestracja i skalowalność, 338

przechowywanie danych, 179

przetwarzanie danych, 39

przetwarzanie rozproszone, 46

racjonalizacja, 394

systemy klasy mainframe, 45

wdrażanie aplikacji, 338

wykorzystanie hiperwizorów, 43

zalety, 72, 73

zalety pamięci masowej, 181

zarządzanie przechowywaniem danych, 180

CI/CD, Continuous Integration/Continuous Delivery, 41, 300, 340
 sprawdzanie zabezpieczeń, 296
ciągła integracja, CI, 41, 340
ciągle
 doskonalenie, 299
 dostarczanie, CD, 300, 340
 monitorowanie, 299, 340, 344
 testowanie, 299, 340, 343
 wdrażanie, 340, 342
CLI, Command-Line Interface, 428, 440
Cloud
 Adoption Framework, CAF, 404
 komponenty, 405
 korzyści, 407
 Hypervisor, 43
CRM, customer relationship management, 305
cykl życia
 interfejsu API, 311
 MLOps, 216

D

DaaS, dane jako usługa, 62
 wyzwania, 63
 zalety, 63
dane
 niestrukturalne, nonstructured data, 181, 182
 strukturalne, structured data, 181
 syntetyczne, 206
 typu blob, 184
debugowanie, 297
DevOps, 81, 211, 339
 analitka, 346
 ciągła integracja, 340
 ciągle monitorowanie, 299, 340, 344
 ciągle testowanie, 299, 340, 343
 ciągle wdrażanie, 340, 342
 integracja bezpieczeństwa, 298
 komponenty, 340
 raportowanie, 346
 rozwój aplikacji, 340
 tworzenie aplikacji, 339
 usługa Microsoft Defender, 294
 zasady bezpieczeństwa, 298
DevSecOps, 275
 przesunięcie w lewo, shift-left, 275
 przesunięcie w prawo, shift-right, 275
DNS, Domain Name System, 157
dostarczanie aplikacji, Application Delivery, 168

dostęp
 do platformy, 92
 warunkowy, 285
DSL, domain-specific language, 86
DTFx, Durable Task Framework, 118

E

ELT, extract, load, transform, 230
ERP, enterprise resource planning, 305
exploity typu zero-day, 269

F

FaaS, funkcja jako usługa, 59, 60
framework Azure Functions, 119
funkcja
 IntelliSense, 432
 orkiestracji, 130
funkcje
 działania, activity functions, 122
 jednostki, entity functions, 123
 klienta, client function, 118
 łańcuchowanie, 128
 orkiestratora, orchestrator function, 120
 ograniczenia, 126
 tworzenie przepływu pracy, 126
 portalu Azure, 75
 trwałe, 119
 interfejsy API, 131
 stany, 127
 uruchamianie, 125
 zabezpieczeń, 280

G

GenAI, Generative AI, 207
GitHub, 348, 438
 CLI, 440
 Codespaces, 439
 Copilot, 423
 dla edukacji, 349
 Enterprise, 442
głębokie uczenie, deep learning, 212
Google Cloud Platform, GCP, 53, 57
grupy
 zabezpieczeń sieci, NSG, 163
 zarządzania, 83
 zasobów, 84

H

Hashicorp Terraform, 352
zastosowania, 355
hiperwizor, 43

I

IaaS, infrastruktura jako usługa, 58
IaC, Infrastructure as Code, 41, 86, 300, 350
IAM, Azure Identity and Access Management, 279
IBM Cloud, 53
IDE, *Patrz* środowisko IDE
implementacja
obsługi komunikatów, 327
skanowania, 296
infrastruktura
chmurowa
automatyzacja, 338, 350
monitorowanie infrastruktury, 359
natywna, 336
tworzenie, 338
zarządzanie infrastrukturą, 350, 367
jako kod, IaC, 41, 86, 300, 350
program Hashicorp Terraform, 352
przepływ pracy, 351
integracja w chmurze, 305
hybrydowej, 306
integracja danych, 306
integracja środowiska lokalnego, 306
korzyści, 307
na platformie Azure, 309
niezawodność aplikacji, 307
oszczędność kosztów, 309
skalowalność aplikacji, 307
sprawność biznesowa, 309
typu
aplikacja-aplikacja, 306
chmura-biznes, 307
chmura-chmura, 306
chmura-urządzenia mobilne, 306
wydajność pracy, 309
zabezpieczenia, 299
interfejsy API
Cassandra API, 196
Core (SQL) API, 195
Gremlin API, 195
luki i podatności w zabezpieczeniach, 269

MongoDB API, 196
REST API, 261
Table API, 196
Web API, 310
cykl życia, 311
partnerskie, 310
publiczne, 310
wewnętrzne, 310
złożone, 311

internet rzeczy, *Patrz* IoT

IoT, Internet of Things, 40, 206, 245
komponenty składowe, 247, 248
na platformie Azure, 251
usługa Defender for IoT, 256
wady, 250
zabezpieczanie rozwiązań, 256
zalety, 249
zastosowania, 248

J

język
ARM, 354
Bicep, 86, 353, 354
Power Fx, 220

K

KEDA, 139
klastry obliczeniowe, 45
komunikacja internetowa, 328
użycie wzorca wydawca-subskrybent, 329
konfiguracja
jako kod, CaC, 356
wielochmurowa, multi-cloud, 53, 54
konteneryzacja, containerization, 44, 134
kontrola dostępu, 92
oparta na rolach, RBAC, 92, 279, 283
koszty, 90, 381
migracji, 71

L

Log Analytics, 82
lokalizacje geograficzne, 87
low-code/no-code, 41
luki i podatności
w zabezpieczeniach interfejsów, 269

M

- magazyny, 179
- maszyny wirtualne, 103, 104
 - opcje skalowania, 107
 - przegląd, 105
 - typu Azure Spot, 107
 - zestawy skalowania, 103, 106
- metodologia
 - DevSecOps, 275
 - Zero Trust, 271
- metodyka
 - DevOps, 81, 211, 339
 - MLOps, 211
- Microsoft Assessments, 411
 - narzędzia platformy, 412
- Microsoft Azure, 53, 56, 70
 - analiza danych, 235
 - automatyzacja, 350
 - bazy danych, 179
 - bezpieczeństwo platformy, 265
 - DevOps, 345
 - funkcje trwałe, 119
 - infrastruktura
 - chmurowa, 336
 - globalna, 87
 - jako kod, 352, 353
 - integracja w chmurze, 309
 - kategorie usług, 76, 77
 - koszty migracji, 71
 - magazyny, 179
 - model Well-Architected Framework, 396
 - monitorowanie infrastruktury, 359
 - narzędzia
 - deweloperskie, 82, 419
 - do monitorowania, 82
 - integracji, 305
 - obsługa komunikatów, 327
 - operacje finansowe, 381
 - rozwiązania hybrydowe, 415
 - rozwiązania wielochmurowe, 415
 - sztuczna inteligencja, 203
 - tworzenie aplikacji, 339
 - uczenie maszynowe, 209
 - usługi
 - big data, 229, 235
 - hybrydowe, 82
 - kognitywne, 215
 - obliczeniowe, 77, 78, 101
 - sieciowe, 77, 79, 145
 - wielochmurowe, 82
 - zabezpieczeń, 80
 - zalety, 72
 - zapewnianie ładu, 367
 - zarządzanie
 - infrastrukturą, 350, 367
 - kosztami, 90, 381
 - ładem, 385
 - tożsamościami, 80
 - zasobami, 83
- Microsoft Defender
 - for App Service, 295
 - for Cloud, 292
 - for Containers, 294
 - for DevOps, 294
 - for Endpoint, 293
 - for IoT, 256
- Microsoft Dev Box, 434
 - Azure Deployment Environments, 436
 - komponenty, 435
 - przepływ pracy, 437
- Microsoft Entra Connect, 281
 - synchronizacja skrótów haseł, 282
- Microsoft Entra ID, 92, 280
 - tożsamości zarządzane, 287
- Microsoft Entra ID Protection, 280
- Microsoft Purview, 241
- Microsoft Sentinel, 291
- migracja do chmury, 82
 - tryb lift-and-shift, 103
 - typu Big Bang, 396
- ML, machine learning, 40, 209
- MLOps, 211
- model Well-Architected Framework, 396
- monitorowanie, 81
 - alertów, 377
 - infrastruktury, 359
 - kondycji systemu, 379
 - proaktywne, 344
 - scentralizowane, 376
 - sieci, 173
 - usługi, 360

N

naruszenia danych, 266
narzędzia
 deweloperskie, 81, 419
 do monitorowania, 82
 do zarządzania kosztami, 381
 integracji, 305
 platformy Microsoft Assessments, 412
 programistyczne, 421
 wiersza poleceń, 427
narzędzie
 App Configuration, 82
 Application Insights, 82
 Azure
 Advisor, 82
 Arc, 83
 CLI, 428
 Data Box, 83
 Database Migration Service, 83
 Developer CLI, 433
 DevOps, 82
 DevTest Labs, 82, 104, 347
 Migrate, 83
 Monitor, 82
 PowerShell, 431
 Stack, 83
 Well-Architected Review, 410
 Business Intelligence, BI, 234
 Hashicorp Terraform, 352
 IntelliCode, 423
 Log Analytics, 82
 Orchestrator, 120
 Terraform, 86
 Visual Studio, 82, 421
 Visual Studio Code, 82, 421
NAT, 155
NLP, natural language processing, 206
NSG, network security groups, 163, 290

O

obliczanie, Azure Compute, 101
obliczenia kwantowe, 141
obsługa
 błędów, 297
 komunikatów, 327
ochrona tożsamości, 80

optymalizacja zasobów, 398
Oracle Cloud Platform, 57
orkiestracja, 120, 125

P

PaaS, platforma jako usługa, 58
PaC, Policy as Code, 357
pakiety Azure SDK, 425
pary regionów, Azure region pairs, 88
planowanie zasobów przedsiębiorstwa, ERP, 305
połączenia VPN, 154
portal Azure, 73
 funkcje, 75
 uzyskanie dostępu, 73
Power
 Apps, 41
 BI, 240
przechowywanie danych w chmurze, 180
przepływy pracy
 CI, 342
 stanowe, 127
 usługi Azure Web PubSub, 332
 w IaC, 351
przetwarzanie
 bezserwerowe, serverless computing, 56, 60, 115
 brzegowe, edge computing, 40
 gridowe, 46
 języka naturalnego, NLP, 206
 klastrowe, 45
 kwantowe, quantum computing, 40
 obrazów, computer vision, 206
 rozproszone, grid computing, 46
 w centrach danych, 42
 w chmurze obliczeniowej, 39, 46
 wsadowe, 45
PTA, pass-through authentication, 282

R

racjonalizacja chmury
 etapy, 394
raportowanie, 240
RBAC, Role-based Access Control, 92, 135, 279, 283
regiony, 87
rejestr kontenerów ACR, 135

- role, 92
- rozwiązania wielochmurowe,
 - multi cloud, 47, 53, 54
- równoważenie obciążenia, load balancing, 164

S

- SaaS, oprogramowanie jako usługa, 59
- sieciowe grupy zabezpieczeń, NSG, 290
- SIEM, Security Information and Event Management, 291
- single-page application, 111
- skalowanie maszyn wirtualnych, 103, 106
- SNAT, source network address translation, 155
- SPA, Single-Page Application, 113
- Static Web Apps
 - tworzenie, 113
- strefy dostępności, Azure availability zones, 89
- subskrypcje, 84
- system
 - Oryx, 114
 - zarządzania treścią, CMS, 111
- systemy
 - brzegowe AI, 207
 - klasy mainframe, 45
- szablony ARM, 86, 353
- sztuczna inteligencja, AI, 203
 - etyczna, ethical AI, 212, 214
 - korzyści, 208
 - technologie, 205

Ś

- środowisko IDE
 - Android Studio, 425
 - Eclipse, 425
 - IntelliJ IDEA, 425
 - JetBrains Rider, 425
 - Visual Studio, 421
 - Visual Studio Code, 421
 - Xcode, 425

T

- technologia hiperwizora, 43
- tożsamości
 - hybrydowe, 281
 - użytkowników, 91
 - ochrona, 80
 - zarządzanie, 279
 - zarządzane, managed identities, 287

- translacja adresów NAT, 155
- tworzenie
 - aplikacji, 421
 - łańcuchów funkcji, 128
 - sieci, 174

U

- uczenie maszynowe, ML, 40, 209
 - głębokie, 212
 - nadzorowane, supervised learning, 210
 - nienadzorowane, unsupervised learning, 210
 - ze wzmocnieniem, reinforcement learning, 210
 - zautomatyzowane, 218
- usługa
 - Active Directory, 91
 - Active Directory Federation Services, 283
 - AI Builder, 219
 - Application Insights, 359
 - Azure
 - Advisor, 360
 - API Management, 313
 - App Service, 108
 - Application Gateway, 169
 - Arc, 413
 - Arc-Enabled Kubernetes, 414
 - Automation, 378
 - Bastion, 158, 290
 - Blob Storage, 184
 - Blueprints, 373
 - Boards, 345
 - CDN, 172
 - Container Apps, 136
 - Container Instances, 136
 - Containers, 135
 - Data Catalog, 231
 - Data Factory, 230, 239
 - Data Lake, 236
 - Data Lake Storage, 238
 - Database Services, 190
 - Databricks, 238
 - DDoS Protection, 160, 290
 - DevOps Server, 347
 - DevOps Services, 346
 - DevTest Labs, 82, 104, 347
 - DNS, 157
 - Event Grid, 260, 332
 - ExpressRoute, 151, 415
 - Files, 186

usługa

- Firewall, 159, 290
- Front Door, 168
- HDInsight, 235, 238
- Identity Management and Security Services, 81
- IoT, 245, 251
- Key Vault, 289
- Kubernetes, 135
- Kubernetes Service, 135, 139
- Lab Services, 104
- Load Balancer, 164
- Log Analytics, 359
- Logic Apps, 317
- Machine Learning, 216
- Machine Learning Studio, 217
- Managed Disks, 189
- Maps, 257
- Monitor, 344, 359, 376
- Monitor Network Insights, 174
- NAT, 155
- Network Watcher, 173, 359
- OpenAI, 205
- Pipelines, 345
- Policy, 379
- Private Link, 161
- Queue Storage, 187
- Repos, 346
- Resource Manager, 70, 86, 353, 370
- Service Bus, 321
- Site Recovery, 415
- Space, 174
- Stack, 414
- Static Web Apps, 113
- Storage, 183
- Stream Analytics, 236
- Synapse Analytics, 237
- Table Storage, 188
- Testing, 346
- Traffic Manager, 170
- Virtual Network, 147
- Virtual WAN, 150
- VM Scale Sets, 103
- VMware Solution, 414
- VNet Peering, 148
- VPN Gateway, 415
- Web App for Containers, 111
- Web Application Firewall, 162
- Web PubSub, 327

- CaC, 356
- GitHub Copilot, 423
- IaC, 350
- Microsoft Defender
 - for App Service, 295
 - for Cloud, 292
 - for Containers, 294
 - for DevOps, 294
 - for Endpoint, 293
 - for IoT, 256
- Microsoft Dev Box, 434
- Microsoft Entra Connect, 281
- Microsoft Entra ID, 92, 280
- Microsoft Entra ID Protection, 280
- Microsoft Purview, 241
- PaC, 357

usługi

- analityczne, 235–42
- Azure
 - Analysis Services, 240
 - Applied AI Services, 220
 - Cognitive Services, 214
 - Database, 80, 83, 190
 - Storage, 79, 183
- baz danych, 80, 184, 191
- bezszyfrowe, serverless computing, 59
- big data, 226, 235
- do monitorowania sieci, 173
- dostarczania aplikacji, 146, 168–73
- kontenerowe, 134
- łączności, 146–59
- magazynu, 183, 184
- Microsoft Azure, 75, 77
- monitorowania sieci, 146
- obliczeniowe, 77, 101–44
 - Azure Container Apps
 - Azure Kubernetes Service, AKS, 78
 - Azure Spot Virtual Machines, 78
 - Azure Static Web Apps, 78
 - Azure Virtual Machine Scale Sets, 78
 - Azure Virtual Machines, 78
 - kategoria Obliczanie, Compute, 102
 - Service Fabric, 78
 - technologie obliczeniowe, 102, 115
- obliczeniowe bezszyfrowe
 - Azure Container Apps, 78, 136
 - Azure Durable Functions, 117
 - Azure Functions, 78, 116
 - korzyści, 115

- ochrony aplikacji, 146, 159–67
- sieciowe, 77, 145–78
 - Azure Bastion, 79
 - Azure ExpressRoute, 79
 - Azure Firewall, 79
 - Azure Load Balancer, 79
 - Azure Private Link, 79
 - Azure Traffic Manager, 79
 - Azure Virtual Network, 79
 - Azure VPN Gateway, 79
- kategorie, 146
- w chmurze, 58
- zabezpieczeń, 80
- zarządzania tożsamościami, 80
- uwierzytelnianie, 279
 - przekazywane, PTA, 282
 - typu pass-through, 282
- wieloskładnikowe, MFA, 272, 283, 284

V

- Visual Studio, 82, 421
 - edycje i wersje, 423
 - zalety programu, 422
- Visual Studio Code, 82, 421

W

- WAF, Web Application Firewall, 162
- walidacja danych, 296
- wdrażanie chmury, 47, 389
 - antywzorce migracji, 395
 - Azure CAF, 404
 - identyfikacja zasobów cyfrowych, 393
 - majątek cyfrowy, 392
 - migracja, 390
 - model WAF, 396
 - modernizacja
 - starszych aplikacji, 391
 - tradycyjnej infrastruktury, 391
 - operacje w chmurze, 390
 - planowanie, 390
 - platforma Microsoft Assessments, 411
 - racjonalizacja chmury, 394
 - warunki migracji, 392
 - zalecane metody, 408
- WebSockets, 329
- Well-Architected Framework, WAF, 396
 - bezpieczeństwo, 399
 - doskonałość operacyjna, 397

- efektywność działania, 402
- niezawodność, 400
- optymalizacja kosztów, 403
- wielochmurowość, 53
- wiersz poleceń
 - narzędzia, 427
- wirtualizacja, 42
 - w chmurze, 43
- wydatki
 - kapitałowe, CapEx, 65
 - operacyjne, OpEx, 66
- wyszukiwanie w Azure Maps, 261
- wyzwalacze orkiestracji, 125
- wzorzec
 - agregator, 134
 - Async HTTP APIs, 131
 - fan-out/fan-in, 129, 130
 - interakcji z człowiekiem, 133
 - monitor, 132
 - tworzenia łańcucha funkcji, 128
 - wydawca-subskrybent, 329

Z

- zagrożenia wewnętrzne, 267
- zapora
 - aplikacji internetowej, WAF, 162
 - sieciowa, 159
- zarządzanie
 - dostępem oparte na rolach, RBAC, 135
 - informacjami i zdarzeniami zabezpieczeń, 291
 - infrastrukturą, 350, 367
 - interfejsami API, 317
 - kosztami, 381, 382
 - najlepsze praktyki, 382
 - narzędzia, 381
 - optymalizacja, 383
 - ładem, 385
 - relacjami z klientami, CRM, 305
 - tożsamościami, 80, 92
 - tożsamościami i dostępem, IAM, 279
 - zmianami, 400
- zasady
 - dostępu warunkowego, CAP, 285
 - platformy jako kod, PaC, 357
 - projektowania aplikacji, 338
- zasoby platformy, 85
- Zero Trust, 271, 375
- zestawy dostępności, 90
- złośliwe oprogramowanie, 267

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 

Azure: zrób pierwszy krok do chmury!

Microsoft konsekwentnie doskonali się w tworzeniu wyjątkowych technologii i Azure jest tego świetnym przykładem. Pozwala nie tylko na rozwijanie natywnych aplikacji chmurowych, ale również na efektywną migrację starszych systemów, wdrażanie rozwiązań hybrydowych i modernizację istniejącego oprogramowania pod kątem skalowalności. Skorzystanie z pełni możliwości Azure wymaga jednak dobrego zrozumienia koncepcji przetwarzania w chmurze.

Dzięki tej praktycznej, przystępnie napisanej książce przyswoisz modele przetwarzania w chmurze i zrozumiesz sedno nowoczesnych technologii chmurowych. Zorientujesz się, jak optymalnie używać Microsoft Azure w różnych sytuacjach biznesowych, i płynnie przystąpisz do budowania aplikacji na tej platformie. Znajdziesz tu wyczerpujące informacje o kontenerach Azure, bezserwerowych technologiach obliczeniowych i narzędziach zwiększających produktywność deweloperów. Dowiesz się ponadto, jak korzystać z funkcji współpracy zespołowej, w jaki sposób dokonać bezpiecznej migracji aplikacji, jej transformacji, a także jak ją rozwijać z użyciem narzędzi Azure.

W książce między innymi:

- podstawy przetwarzania w chmurze Microsoft Azure
- wybór usług w chmurze Azure i dostosowanie scenariuszy do wymagań
- tworzenie usług, aplikacji i rozwiązań w chmurze
- zabezpieczenia chmury w infrastrukturze IT
- najlepsze praktyki migracji na platformę Azure

Jonah Carrio Andersson jest szwedzką programistką i prelegentką. Posiada tytuły MVP w zakresie Azure i MCT. Jest również inżynierką DevOps. W pracy zajmuje się rozwojem chmury z wykorzystaniem .NET i infrastruktury w ramach platformy Azure. Prowadzi podcast *Extend Women in Tech*.

Ta książka to pasjonująca podróż w świat Microsoft Azure!

Peter T. Lee, Capgemini America, Inc.

Helion	KOD KORZYŚCI Sięgnij po więcej! ▶	
 helion.pl	ISBN 978-83-289-1347-9	
 HELION S.A. ul. Kosciuszki 1c 44-100 Gliwice tel.: 32 220 98 63 helion@helion.pl		
Cena: 119,00 zł		