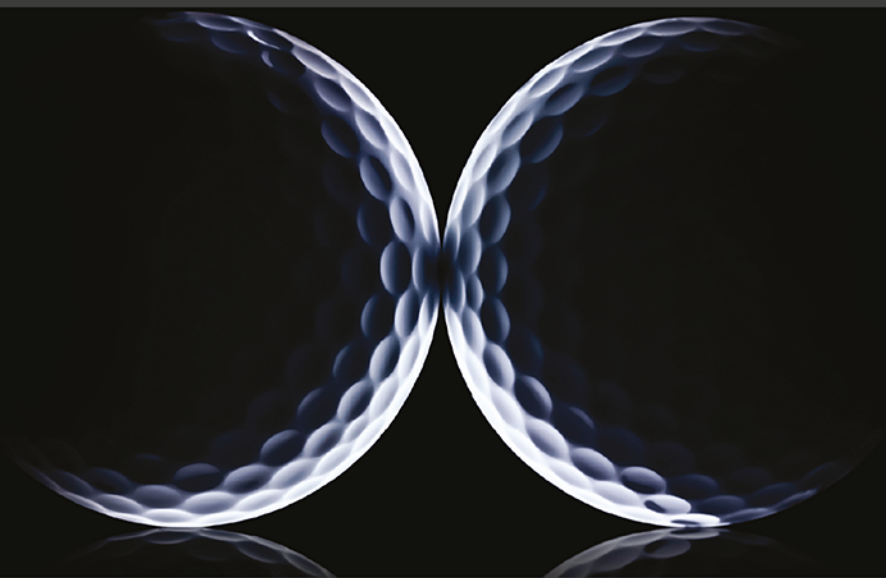


DevOps

w praktyce

Wydanie II

Wdrażanie narzędzi Terraform, Azure DevOps,
Kubernetes i Jenkins



Mikael Krief

Helion 



Tytuł oryginału: Learning DevOps: A comprehensive guide to accelerating DevOps culture adoption with Terraform, Azure DevOps, Kubernetes, and Jenkins, 2nd Edition

Tłumaczenie: Łukasz Wójcicki

ISBN: 978-83-8322-198-4

Copyright © Packt Publishing 2022. First published in the English language under the title 'Learning DevOps - Second Edition – (9781801818964)'

Polish edition copyright © 2023 by Helion S.A.

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/devpr2>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

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

Spis treści |

O autorze	15
O recenzentach	16
Przedmowa	17

CZĘŚĆ 1. DevOps i infrastruktura jako kod

Rozdział 1

Kultura DevOps i praktyki kodowania infrastruktury	25
Pierwsze kroki z DevOps	25
Wdrażanie CI/CD i ciągłe wdrażanie	29
Ciągła integracja (CI)	29
Ciągłe dostarczanie (CD)	31
Ciągłe wdrażanie	33
Zrozumienie praktyk IaC	35
Korzyści IaC	36
Języki i narzędzia IaC	36
Topologia IaC	39
Ewolucja kultury DevOps	44
Podsumowanie	45
Pytania	45
Dalsza lektura	46

Rozdział 2

Udostępnianie infrastruktury chmury za pomocą Terraform	47
Wymagania techniczne	48
Instalacja Terraform	48
Instalacja ręczna	49
Instalacja za pomocą skryptu	49
Integracja Terraform z Azure Cloud Shell	53

Konfigurowanie Terraform dla platformy Azure	55
Tworzenie jednostki usługi Azure SP	55
Konfiguracja dostawcy Terraform	57
Konfiguracja Terraform w celu rozwoju aplikacji i testowania	58
Tworzenie skryptu Terraform w celu wdrożenia infrastruktury Azure	60
Postępowanie zgodnie z dobrymi praktykami Terraform	63
Uruchamianie Terraform w celu wdrożenia	66
Inicjalizacja	67
Podgląd zmian	69
Stosowanie zmian	70
Zrozumienie cyklu życia Terraform z różnymi opcjami wiersza polecenia	72
Używanie polecenia destroy w celu przebudowy	72
Formatowanie i walidacja konfiguracji	74
Cykl życia Terraform w procesie CI/CD	75
Ochrona pliku stanu za pomocą zdalnego zaplecza	77
Podsumowanie	82
Pytania	82
Dalsza lektura	83

Rozdział 3

Używanie Ansible do konfigurowania infrastruktury IaaS	84
Wymagania techniczne	85
Instalacja Ansible	86
Instalacja Ansible za pomocą skryptu	86
Integracja Ansible z Azure Cloud Shell	88
Artefakty Ansible	89
Konfiguracja Ansible	90
Tworzenie pliku inwentarza Ansible	92
Plik inwentarza	93
Konfigurowanie hostów w pliku inwentarza	94
Testowanie pliku inwentarza	95
Uruchomienie pierwszego playbooka	97
Tworzenie prostego playbooka	97
Opis modułów Ansible	98
Ulepszanie playbooków za pomocą ról	99
Uruchomienie Ansible	100
Korzystanie z podglądu lub z opcji testowej pracy (ang. dry run)	102
Zwiększanie poziomu logowania	104

Ochrona danych za pomocą Ansible Vault	104
Używanie zmiennych w Ansible w celu lepszej konfiguracji	105
Ochrona wrażliwych danych za pomocą Ansible Vault	108
Korzystanie z dynamicznego pliku inwentarza dla infrastruktury Azure	110
Podsumowanie	115
Pytania	115
Dalsza lektura	115

Rozdział 4

Optymalizacja wdrażania infrastruktury za pomocą Packera	117
Wymagania techniczne	118
Opis Packera	119
Instalacja Packera	119
Tworzenie szablonów Packera dla maszyn wirtualnych Azure za pomocą skryptów	125
Struktura szablonu Packera	125
Tworzenie obrazu platformy Azure za pomocą szablonu Packera	130
Tworzenie szablonów Packera przy użyciu Ansible	133
Tworzenie playbooka Ansible	134
Integracja playbooka Ansible z szablonem Packera	135
Uruchamianie Packera	136
Konfigurowanie Packera do uwierzytelniania na platformie Azure	136
Sprawdzanie poprawności szablonu Packera	137
Uruchamianie Packera w celu wygenerowania naszego obrazu maszyny wirtualnej	138
Tworzenie szablonów Packera w formacie HCL	140
Korzystanie z obrazów utworzonych przez Packera za pomocą Terraform	143
Podsumowanie	145
Pytania	145
Dalsza lektura	146

Rozdział 5

Tworzenie środowiska programistycznego z Vagrantem	147
Wymagania techniczne	148
Instalacja Vagranta	148
Instalacja ręczna (w systemie Windows)	148
Instalowanie Vagranta za pomocą skryptu w systemie Windows	150
Instalowanie Vagranta za pomocą skryptu w systemie Linux	151

Tworzenie pliku konfiguracyjnego Vagranta	152
Używanie Vagrant Cloud dla boksów Vagranta	152
Tworzenie pliku konfiguracyjnego Vagranta	154
Tworzenie lokalnej maszyny wirtualnej za pomocą interfejsu Vagrant CLI	156
Tworzenie maszyny wirtualnej	156
Łączenie z maszyną wirtualną	158
Podsumowanie	159
Pytania	160
Dalsza lektura	160

CZĘŚĆ 2. Potok CI/CD

Rozdział 6

Zarządzanie kodem źródłowym za pomocą Gita	163
Wymagania techniczne	164
Przegląd Gita i jego głównych poleceń	164
Instalacja Gita	166
Konfiguracja Gita	176
Terminologia Gita	176
Polecenia Gita	177
Zrozumienie procesu Gita i wzorca Gitflow	181
Zaczynamy od procesu Gita	181
Izolacja kodu za pomocą gałęzi	190
Strategia tworzenia gałęzi z Gitflow	195
Podsumowanie	198
Pytania	198
Dalsza lektura	199

Rozdział 7

Ciągła integracja i ciągłe wdrażanie	200
Wymagania techniczne	201
Zasady CI/CD	201
CI	201
CD	202
Korzystanie z menedżera pakietów w procesie CI/CD	203
Prywatne repozytorium NuGet i npm	205
Repozytorium Nexusa OSS	205
Azure Artifacts	206

Używanie Jenkinsa do implementacji CI/CD	208
Instalowanie i konfigurowanie Jenkinsa	208
Konfiguracja webhooka GitHuba	210
Konfiguracja zadania CI w Jenkinsie	211
Wykonywanie zadania Jenkinsa	215
Korzystanie z Azure Pipelines dla CI/CD	216
Wersjonowanie kodu za pomocą Gita w Azure Repos	218
Tworzenie potoku CI	219
Tworzenie potoku CD — nowa wersja aplikacji	228
Tworzenie pełnej definicji potoku w pliku YAML	234
Korzystanie z GitLab CI	240
Uwierzytelnianie w GitLabie	241
Tworzenie nowego projektu i zarządzanie kodem źródłowym	242
Tworzenie potoku CI	245
Dostęp do szczegółów wykonania potoku CI	247
Podsumowanie	249
Pytania	249
Dalsza lektura	249

Rozdział 8

Wdrażanie infrastruktury jako kodu za pomocą potoku CI/CD	251
Wymagania techniczne	252
Uruchamianie Packera w Azure Pipelines	252
Uruchamianie Terraform i Ansible w Azure Pipelines	255
Podsumowanie	260
Pytania	261
Dalsza lektura	261

CZĘŚĆ 3. Konteneryzowane mikrouслуги wykorzystujące platformę Docker i Kubernetes

Rozdział 9

Konteneryzacja aplikacji za pomocą Dockera	265
Wymagania techniczne	266
Instalowanie Dockera	267
Rejestracja w Docker Hubie	267
Instalacja Dockera	268
Przegląd elementów Dockera	272

Tworzenie pliku Dockerfile	273
Tworzenie pliku Dockerfile	273
Przegląd instrukcji Dockerfile	274
Budowanie i uruchamianie kontenera na komputerze lokalnym	276
Tworzenie obrazu Dockera	276
Tworzenie nowego kontenera obrazu	278
Lokalne testowanie kontenera	279
Wysyłanie obrazu do Docker Huba	279
Wysyłanie obrazu Dockera do rejestru prywatnego (ACR)	283
Wdrażanie kontenera do ACI za pomocą potoku CI/CD	285
Tworzenie kodu Terraform dla ACI	286
Tworzenie potoku CI/CD dla kontenera	287
Korzystanie z Dockera przy użyciu narzędzi wiersza poleceń	294
Pierwsze kroki z Docker Compose	296
Instalowanie Docker Compose	297
Tworzenie pliku konfiguracyjnego dla Docker Compose	298
Wykonywanie Docker Compose	299
Wdrażanie kontenerów Docker Compose w ACI	300
Podsumowanie	303
Pytania	303
Dalsza lektura	304

Rozdział 10

Efektywne zarządzanie kontenerami za pomocą Kubernetesa

Wymagania techniczne	306
Instalacja Kubernetesa	306
Przegląd architektury Kubernetesa	307
Instalacja Kubernetesa na komputerze lokalnym	307
Instalacja pulpitu nawigacyjnego Kubernetesa	309
Pierwszy przykład wdrożenia aplikacji w Kubernetesie	312
Używanie Helma jako menedżera pakietów	316
Instalacja klienta Helma	316
Korzystanie z publicznego pakietu Helma, dostępnego w Artifact Hubie	317
Tworzenie niestandardowego charta Helma	321
Publikowanie charta Helma w rejestrze prywatnym (ACR)	323
Korzystanie z AKS	325
Tworzenie usługi AKS	326
Konfigurowanie pliku kubeconfig dla AKS	327
Zalety AKS	328
Tworzenie potoku CI/CD dla Kubernetesa za pomocą Azure Pipelines	329

Monitorowanie aplikacji i metryk w Kubernetesie	330
Korzystanie z wiersza poleceń kubectl	330
Korzystanie z interfejsu webowego	331
Korzystanie z narzędzi	332
Podsumowanie	334
Pytania	334
Dalsza lektura	335

CZĘŚĆ 4. Testowanie aplikacji

Rozdział 11

Testowanie interfejsów API za pomocą Postmana	339
Wymagania techniczne	340
Tworzenie kolekcji żądań Postmana	340
Instalacja Postmana	341
Tworzenie kolekcji	342
Tworzenie pierwszego żądania	343
Wykorzystywanie środowisk i zmiennych do dynamizowania żądań	346
Tworzenie testów Postmana	349
Wykonywanie lokalnych testów za pomocą żądań Postmana	351
Zrozumienie koncepcji Newmana	354
Przygotowywanie kolekcji Postmana dla Newmana	356
Eksportowanie kolekcji	356
Eksportowanie środowisk	357
Korzystanie z wiersza poleceń Newmana	359
Integracja Newmana z procesem potoku CI/CD	361
Budowa i udostępnianie konfiguracji	362
Wykonanie potoku	366
Podsumowanie	367
Pytania	368
Dalsza lektura	368

Rozdział 12

Statyczna analiza kodu za pomocą SonarQube	369
Wymagania techniczne	370
Odkrywanie SonarQube	370
Instalacja SonarQube	371
Przegląd architektury SonarQube	371
Instalacja SonarQube	372

Analiza w czasie rzeczywistym za pomocą SonarLint	378
Wykonywanie SonarQube w procesie CI	380
Konfigurowanie SonarQube	381
Tworzenie potoku CI dla SonarQube w Azure Pipelines	381
Podsumowanie	385
Pytania	385
Dalsza lektura	385

Rozdział 13

Testy bezpieczeństwa i wydajności	386
Wymagania techniczne	386
Stosowanie zabezpieczeń internetowych i testów penetracyjnych za pomocą narzędzia ZAP	387
Korzystanie z ZAP-a w celu testowania bezpieczeństwa	388
Sposoby automatyzacji wykonywania ZAP-a	390
Uruchamianie testów wydajności za pomocą Postmana	392
Podsumowanie	395
Pytania	395
Dalsza lektura	395

CZĘŚĆ 5. Więcej informacji na temat DevOps

Rozdział 14

Bezpieczeństwo w procesie DevOps z wykorzystaniem DevSecOps	399
Wymagania techniczne	400
Testowanie infrastruktury Azure za pomocą InSpec	400
Omówienie InSpec	401
Instalacja InSpec	402
Konfigurowanie platformy Azure dla InSpec	403
Tworzenie testów InSpec	405
Wykonywanie InSpec	408
Ochrona poufnych danych dzięki Vault od HashiCorp	410
Lokalna instalacja programu Vault	411
Uruchamianie serwera Vault	413
Zapisywanie haseł w Vault	415
Odczytywanie sekretów z Vault	416
Korzystanie z interfejsu webowego (UI) programu Vault	418
Pobieranie sekretów Vault w Terraform	421

Podsumowanie	425
Pytania	425
Dalsza lektura	425

Rozdział 15

Skrócenie czasu przestoju wdrażania	426
Wymagania techniczne	427
Skrócenie czasu przestojów we wdrażaniu dzięki Terraform	427
Zrozumienie zielono-niebieskich koncepcji i wzorców wdrażania	429
Korzystanie z wdrożenia zielono-niebieskiego w celu ulepszenia środowiska produkcyjnego	430
Opis wzorca Canary release	430
Badanie wzorca Dark launch	432
Stosowanie wdrożeń zielono-niebieskich na platformie Azure	432
Używanie App Service z gniazdami	433
Korzystanie z usługi Azure Traffic Manager	434
Wprowadzenie flag funkcjonalności	436
Używanie frameworka open source dla flag funkcjonalności	438
Korzystanie z narzędzia LaunchDarkly	443
Podsumowanie	447
Pytania	448
Dalsza lektura	448

Rozdział 16

DevOps dla projektów open source	449
Wymagania techniczne	450
Przechowywanie kodu źródłowego w GitHubie	451
Tworzenie nowego repozytorium na GitHubie	451
Przyczynianie się do rozwoju projektu w GitHubie	453
Przyczynianie się do rozwoju projektów open source przy użyciu żądań pobierania	455
Zarządzanie plikiem dziennika zmian i informacjami o wydaniu	459
Udostępnianie plików binarnych w wydaniach GitHuba	461
Wprowadzenie do GitHub Actions	464
Analiza kodu za pomocą SonarCloud	468
Wykrywanie luk w zabezpieczeniach za pomocą narzędzia WhiteSource Bolt	473
Podsumowanie	476
Pytania	477
Dalsza lektura	478

Rozdział 17**Najlepsze praktyki DevOps479**

Pełna automatyzacja	480
Wybór odpowiedniego narzędzia	480
Tworzenie całej konfiguracji za pomocą kodu	481
Projektowanie architektury systemu	482
Budowanie dobrego potoku CI/CD	484
Testy integracyjne	485
Przesunięcie bezpieczeństwa w lewo dzięki DevSecOps	486
Monitorowanie systemu	487
Ewoluuujące zarządzanie projektami	488
Podsumowanie	489
Pytania	489
Dalsza lektura	490

Odpowiedzi491

Rozdział 1. Kultura DevOps i praktyki kodowania infrastruktury	491
Rozdział 2. Udostępnianie infrastruktury chmury za pomocą Terraform	491
Rozdział 3. Używanie Ansible do konfigurowania infrastruktury IaaS	492
Rozdział 4. Optymalizacja wdrażania infrastruktury za pomocą Packera	492
Rozdział 5. Tworzenie środowiska programistycznego z Vagrantem	493
Rozdział 6. Zarządzanie kodem źródłowym za pomocą Gita	493
Rozdział 7. Ciągła integracja i ciągłe wdrażanie	494
Rozdział 8. Wdrażanie infrastruktury jako kodu za pomocą potoku CI/CD	494
Rozdział 9. Konteneryzacja aplikacji za pomocą Dockera	494
Rozdział 10. Efektywne zarządzanie kontenerami za pomocą Kubernetesa	495
Rozdział 11. Testowanie interfejsów API za pomocą Postmana	495
Rozdział 12. Statyczna analiza kodu za pomocą SonarQube	495
Rozdział 13. Testy bezpieczeństwa i wydajności	496
Rozdział 14. Bezpieczeństwo w procesie DevOps z wykorzystaniem DevSecOps	496
Rozdział 15. Skrócenie czasu przestoju wdrażania	496
Rozdział 16. DevOps dla projektów open source	497
Rozdział 17. Najlepsze praktyki DevOps	497

Skorowidz499

Kultura DevOps i praktyki kodowania infrastruktury

Rozdział
1

DevOps, termin, który coraz częściej słyszymy w przedsiębiorstwach z frazami typu „stosujemy DevOps” czy „używamy narzędzi DevOps”, to skrót pochodzący od słów „Development” i „Operations”.

DevOps to kultura, która różni się od tradycyjnych kultur korporacyjnych i wymaga zmiany sposobu myślenia, procesów i narzędzi. Często wiąże się to z praktykami **ciągłej integracji** (ang. *continuous integration* — CI) i **ciągłego dostarczania** (ang. *continuous delivery* — CD), które są związane z inżynierią oprogramowania, ale także z **infrastrukturą jako kod** (ang. *Infrastructure as Code* — IaC), polegającą na *kodyfikacji* struktury i konfiguracji infrastruktury.

W tym rozdziale zobaczymy, czym jest kultura DevOps, jakie są zasady DevOps i jakie korzyści przynoszą firmie. Następnie wyjaśnimy praktyki CI/CD, a na koniec omówimy szczegółowo IaC z jej wzorcami i praktykami.

W tym rozdziale omówimy następujące tematy:

- pierwsze kroki z DevOps,
- wdrażanie CI/CD i ciągłe wdrażanie,
- zrozumienie praktyk IaC.

Obejrzyj następujący film na kanale Code in Action: <https://bit.ly/3JJAMAb>.

Pierwsze kroki z DevOps

Termin *DevOps* został wprowadzony w latach 2007 – 2009 przez Patricka Debois, Gene’a Kima i Johna Willisa i reprezentuje połączenie słów *Development* (Dev) i *Operations* (Ops). Dało to początek ruchowi, który opowiada się za łączeniem razem programistów i operacji. Zapewnia to użytkownikom dodaną wartość biznesową dużo szybciej, co czyni ją bardziej konkurencyjną na rynku.

Kultura DevOps to zestaw praktyk zmniejszających bariery między *programistami*, którzy chcą szybciej wprowadzać innowacje i dostarczać, a *zespołami operacyjnymi*, które chcą zagwarantować stabilność systemów produkcyjnych i jakość wprowadzanych zmian systemowych.

Kultura DevOps to także rozszerzenie zwinnych (ang. *agile*) procesów (scrum, XP itd.), co pozwala skrócić czas dostawy, angażując programistów i zespoły biznesowe. Procesy te są często trudne do przeprowadzenia z powodu niewłączania operacji do tych samych zespołów.

Komunikacja i to połączenie między Dev i Ops umożliwiają lepsze śledzenie kompleksowych wdrożeń produkcyjnych i częstsze wdrożenia o wyższej jakości, co pozwala zaoszczędzić pieniądze dla firmy.

Aby ułatwić tę współpracę i poprawić komunikację między programistami a zespołami operacyjnymi, w procesach należy wprowadzić kilka kluczowych elementów, jak pokazano poniżej:

- Częstsze wdrożenia aplikacji z integracją i ciągłym dostarczaniem (tzw. **CI/CD**).
- Wdrażanie i automatyzacja testów jednostkowych i integracyjnych z procesem skoncentrowanym na **projektowaniu opartym na zachowaniu** (ang. *behavior-driven design* — **BDD**) lub **projektowaniu opartym na testach** (ang. *test-driven design* — **TDD**).
- Wdrożenie sposobu zbierania informacji zwrotnych od użytkowników.
- Monitorowanie aplikacji i infrastruktury.

Ruch DevOps opiera się na trzech założeniach:

- **Kultura współpracy.** To jest istota DevOps — fakt, że zespoły nie są już rozdzielone (jeden zespół programistów, jeden zespół Ops, jeden zespół testerów itd.). Ludzie ci łączą się, tworząc multidyscyplinarne zespoły, które mają ten sam cel: jak najszybsze dostarczenie wartości dodanej do produktu.
- **Procesy.** Aby oczekiwać szybkiego wdrożenia, zespoły te muszą śledzić procesy rozwoju oparte na metodologiach agile z iteracyjnymi fazami, które pozwalają na lepszą funkcjonalność, wyższą jakość i szybszą informację zwrotną. Te procesy powinny być zintegrowane nie tylko z przepływem pracy programistycznej z ciągłą integracją, ale także z przepływem pracy wdrażania z ciągłym dostarczaniem i wdrażaniem. Proces DevOps podzielony jest na kilka faz:
 - A. Planowanie i ustalanie priorytetów funkcjonalności.
 - B. Rozwój.
 - C. Ciągła integracja i dostarczanie.

- D. Ciągłe wdrażanie.
- E. Ciągłe monitorowanie.

Fazy te są przeprowadzane cyklicznie i iteracyjnie przez cały czas trwania projektu.

- **Narzędzia.** Wybór narzędzi i produktów używanych przez zespoły jest bardzo ważny w DevOps. W rzeczywistości, kiedy zespoły zostały podzielone na Dev i Ops, każdy zespół używał swoich specyficznych narzędzi — narzędzi do wdrażania dla programistów i narzędzi infrastruktury dla Ops — co jeszcze bardziej zwiększyło luki komunikacyjne.

W zespołach, które łączą programowanie i operację, oraz w tej kulturze jednoci używane narzędzia muszą być użyteczne i możliwe do wykorzystania przez wszystkich członków.

Deweloperzy muszą zapoznać się z narzędziami monitorującymi używanymi przez zespoły Ops w celu jak najwcześniejszego wykrywania problemów z wydajnością i z narzędziami bezpieczeństwa dostarczanych przez Ops w celu ochrony dostępu do różnych zasobów.

Ops z kolei musi zautomatyzować proces tworzenia i aktualizacji infrastruktury oraz zintegrować kod z menedżerem kodu. Wszystkie te czynności tworzą praktyki IaC. Można je jednak wykonać tylko we współpracy z programistami, którzy znają infrastrukturę potrzebną dla aplikacji. Zadania zespołów operacyjnych należy również zintegrować z procesami i narzędziami wydawania aplikacji.

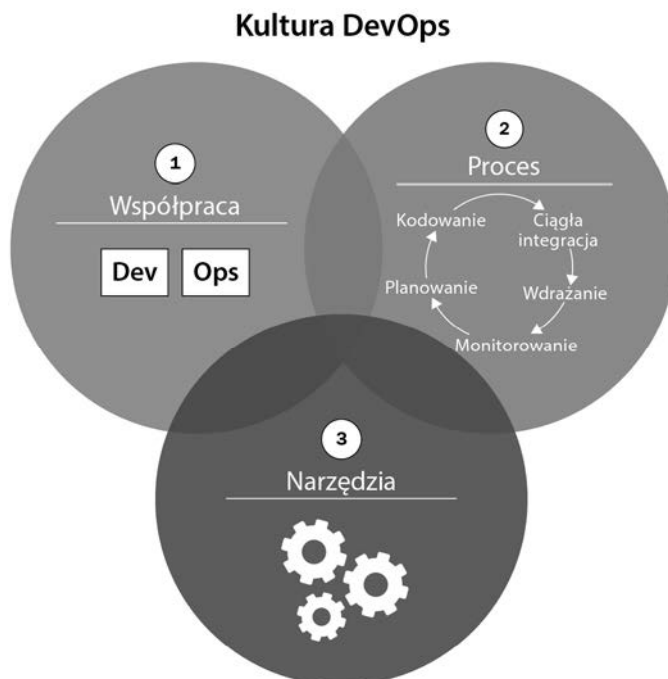
Poniższy diagram ilustruje trzy założenia kultury DevOps — współpracę między Dev i Ops, procesy i wykorzystanie narzędzi.

Możemy nawiązać do kultury DevOps za pomocą definicji Donovan Brown (http://donovanbrown.com/post/what-is-devops):

„DevOps to połączenie ludzi, procesów i produktów, które umożliwia ciągłe dostarczanie wartości naszym użytkownikom końcowym”.

Korzyści z ustanowienia kultury DevOps w przedsiębiorstwie są następujące:

- Lepsza współpraca i komunikacja w zespołach, co ma wpływ na ludzi i na społeczne więzi w firmie.
- Krótsze czasy realizacji produkcji, co skutkuje lepszą wydajnością i satysfakcją użytkownika końcowego.
- Zmniejszone koszty infrastruktury dzięki IaC.



Rysunek 1.1. Kultura DevOps

- Znaczna oszczędność czasu dzięki cyklom iteracyjnym zmniejszającym liczbę błędów aplikacji i narzędziom automatyzacji, które ograniczają liczbę zadań wykonywanych ręcznie, dzięki czemu zespoły skupiają się bardziej na opracowywaniu nowych funkcji o wartości dodanej dla biznesu.

Uwaga

Aby uzyskać więcej informacji na temat kultury DevOps i jej wpływu na transformację przedsiębiorstw, przeczytaj książki *The Phoenix Project: A Novel about IT, DevOps and Helping Your Business Win* Gene'a Kima i Kevina Behra oraz *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations* Gene'a Kima, Jeza Humble'a, Patricka Debois i Johna Willisa.

W tej sekcji poznaliśmy podstawowe pojęcia kultury DevOps. Przyjrzyjmy się teraz pierwszej praktyce kultury DevOps: implementacji CI/CD i ciągłemu wdrażaniu.

Wdrażanie CI/CD i ciągłe wdrażanie

Wcześniej dowiedzieliśmy się, że jedną z kluczowych praktyk DevOps jest proces ciągłej integracji i ciągłego dostarczania, znany również jako **CI/CD**. W rzeczywistości za akronimami CI/CD kryją się trzy praktyki:

- **ciągła integracja (CI),**
- **ciągłe dostarczanie (CD),**
- **ciągłe wdrażanie.**

Czemu odpowiada każda z tych praktyk? Jakie są ich wymagania wstępne i które z nich są najlepsze? Gdzie mają zastosowanie?

Przyjrzyjmy się szczegółowo każdej z tych praktyk, zaczynając od ciągłej integracji.

Ciągła integracja (CI)

W poniższej definicji podanej przez Martina Fowlera wymienia się trzy kluczowe rzeczy: *członkowie zespołu integrują się i to jak najszybciej*:

„Ciągła integracja to praktyka tworzenia oprogramowania, w której członkowie zespołu często integrują swoją pracę... Każda integracja jest weryfikowana przez zautomatyzowaną kompilację (w tym test), aby jak najszybciej wykryć błędy integracji”.

Oznacza to, że CI to automatyczny proces, który pozwala na sprawdzenie kompletności kodu aplikacji za każdym razem, gdy członek zespołu dokona zmiany. Tę weryfikację należy przeprowadzić jak najszybciej.

Kulturę DevOps w CI widzimy bardzo wyraźnie, w duchu współpracy i komunikacji, ponieważ realizacja CI wpływa na wszystkich członków pod względem metodologii pracy, a tym samym współpracy; ponadto CI wymaga implementacji procesów (wprowadzanie zmian, zatwierdzanie, pobieranie i przegląd kodu itd.) wykorzystujących automatyzację za pomocą narzędzi dostosowanych do całego zespołu (Git, Jenkins, Azure DevOps itd.). Wreszcie CI musi działać szybko, aby jak najszybciej zebrać informacje zwrotne na temat integracji kodu, a tym samym być w stanie szybciej dostarczać nowe funkcje użytkownikom.

Wdrażanie CI

Dlatego aby skonfigurować CI, konieczne jest posiadanie **menedżera kodu źródłowego** (ang. *Source Code Manager* — **SCM**), który scentralizuje kod wszystkich członków. Ten menedżer może być dowolnego typu: Git, SVN lub *Team Foundation Version Control* (**TFVC**). Ważne jest również posiadanie automatycznego menedżera kompilacji (serwera CI), który obsługuje ciągłą integrację, takiego jak Jenkins, GitLab CI, TeamCity, Azure Pipelines, GitHub Actions, Travis CI i Circle CI.

Uwaga

W tej książce jako SCM użyjemy Gita i przyjrzymy się nieco dokładniej jego konkretnym zastosowaniom.

Każdy członek zespołu będzie pracował nad kodem aplikacji codziennie, iteracyjnie i przyrostowo (np. w metodach agile i scrum). Każde zadanie lub funkcja musi być oddzielona od innych rozwiązań za pomocą stosowania gałęzi (ang. *branch*).

Regularnie, nawet kilka razy dziennie, członkowie archiwizują lub zatwierdzają (ang. *commit*) swój kod, najlepiej za pomocą małych paczek (ang. *trunks*), które można łatwo naprawić w przypadku błędu. Zostanie on zintegrowany z resztą kodu aplikacji, z resztą zatwierdzeń innych członków.

Integracja wszystkich zatwierdzeń jest punktem wyjścia procesu CI.

Ten proces, który jest wykonywany przez serwer CI, musi być zautomatyzowany i uruchamiany przy każdym zatwierdzeniu. Serwer pobierze kod, a następnie wykona następujące czynności:

- Zbuduje pakiet aplikacji — kompilacja, transformacja plików itd.
- Wykona testy jednostkowe (z testem pokrycia — ang. *code coverage*).

Uwaga

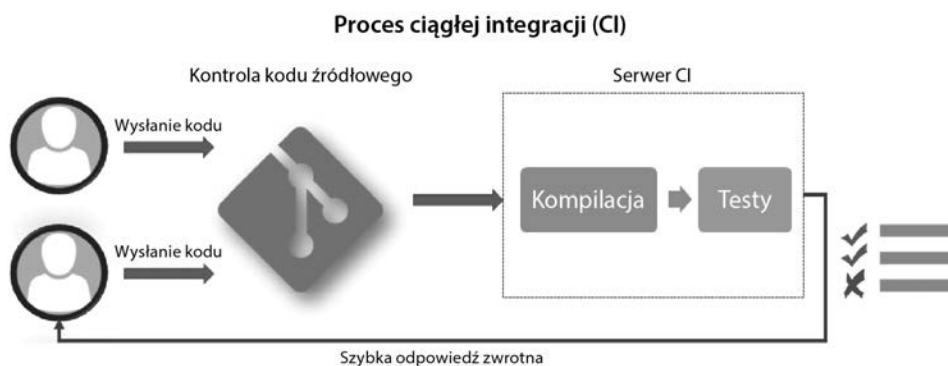
Możliwe jest również wzbogacenie tego procesu o statyczną analizę kodu i podatności. Przyjrzymy się temu w rozdziale 12., „Statyczna analiza kodu za pomocą SonarQube”, który jest poświęcony testom.

Proces CI musi zostać zoptymalizowany najwcześniej, jak to możliwe, aby mógł działać natychmiast, a programiści mogli szybko zebrać informacje zwrotne na temat integracji ich kodu. Na przykład kod, który został zarchiwizowany i nie kompiluje się lub dla którego test kończy się niepowodzeniem, może wpływać na cały zespół i blokować go.

Czasami złe praktyki mogą spowodować niepowodzenie testów podczas CI. Przed dezaktywacją wykonania tego testu musisz wziąć pod uwagę to, że *nie jest ważne, aby koniecznie zadbać o szybkie dostarczenie kodu*.

Wręcz przeciwnie, ta praktyka może mieć poważne konsekwencje, gdy błędy wykryte przez testy zostaną ujawnione w produkcji. Czas zaoszczędzony podczas CI zostanie stracony na naprawianie błędów za pomocą poprawek i ich szybkie ponowne wdrażanie, co może powodować stres. Jest to przeciwieństwo kultury DevOps, ponieważ użytkownicy końcowi otrzymują niską jakość aplikacji i nie ma prawdziwych informacji zwrotnych; zamiast opracowywać nowe funkcje, spędzamy czas na poprawianiu błędów.

Dzięki zoptymalizowanemu i kompletnemu procesowi CI programista może szybko naprawić swoje problemy i ulepszyć kod lub przedyskutować go z resztą zespołu i zatwierdzić swój kod do nowej integracji. Spójrzmy na poniższy diagram:



Rysunek 1.2. Proces ciągłej integracji

Ten diagram przedstawia cykliczne etapy ciągłej integracji. Obejmuje to kod przesyłany do SCM przez członków zespołu oraz kompilację i test wykonywany przez serwer CI. Celem tego procesu jest zapewnienie członkom szybkiej informacji zwrotnej.

Teraz, gdy dowiedzieliśmy się, czym jest ciągła integracja, spójrzmy na ciągłe dostarczanie.

Ciągłe dostarczanie (CD)

Po zakończeniu ciągłej integracji następnym krokiem jest automatyczne wdrożenie aplikacji w co najmniej jednym środowisku nieprodukcyjnym, określanym jako **staging**. Ten proces nazywa się **ciągłym dostarczaniem** (ang. *continuous delivery* — CD).

CD często rozpoczyna pracę z pakietem aplikacji przygotowywanym przez CI, który zostanie zainstalowany na podstawie listy zautomatyzowanych zadań. Mogą to być zadania dowolnego typu: rozpakowanie, zatrzymanie i ponowne uruchomienie usługi, skopiowanie plików, zamiana konfiguracji itd. Podczas procesu CD mogą być również wykonane testy funkcjonalne i akceptacyjne.

W przeciwieństwie do CI, CD ma na celu przetestowanie całej aplikacji ze wszystkimi jej zależnościami. Jest to szczególnie widoczne w aplikacjach mikroserwisowych składających się z kilku usług i interfejsów API; CI przetestuje tylko rozwijaną mikrousługę, podczas gdy po wdrożeniu w środowisku przejściowym będzie można przetestować i zweryfikować całą aplikację, a także interfejsy API i mikrousługi, z których się składa.

W praktyce obecnie bardzo często łączy się CI z CD w środowisku integracyjnym; oznacza to, że CI wdraża się w tym samym czasie w środowisku. Jest to konieczne, aby programiści mogli nie tylko wykonywać testy jednostkowe, ale także weryfikować aplikację jako całość (UI i funkcjonalną) przy każdym zatwierdzeniu, wraz z integracją opracowań innych członków zespołu.

Ważne jest, aby pakiet generowany podczas CI, który zostanie wdrożony również podczas CD, był tym samym, który zostanie zainstalowany we wszystkich środowiskach, i tak powinno być do czasu produkcji. Mogą jednak występować zmiany pliku konfiguracyjnego, które różnią się w zależności od środowiska, ale kod aplikacji (pliki binarne, pliki DLL, obrazy Dockera i JAR) musi pozostać niezmienny.

Niezmienny charakter kodu jest jedyną gwarancją, że aplikacja weryfikowana w środowisku będzie tej samej jakości co wersja, która została wdrożona w poprzednim środowisku, a także ta sama, która zostanie wdrożona w następnym środowisku. Jeśli zmiany (ulepszenia lub poprawki błędów) mają zostać wprowadzone w kodzie po weryfikacji w jednym z tych środowisk, po ich wykonaniu modyfikacje będą musiały ponownie przejść cykl CI i CD.

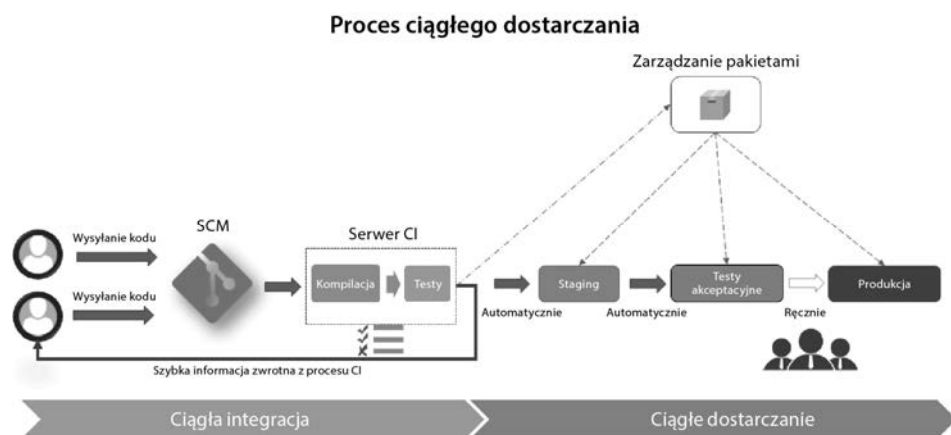
Narzędzia skonfigurowane dla CI/CD są często używane z innymi rozwiązaniami, takimi jak:

- **Menedżer pakietów** — stanowi przestrzeń przechowywania pakietów wygenerowanych przez CI i odzyskanych przez CD. Menedżery te muszą obsługiwać źródła danych, wersjonowanie i różne typy pakietów. Na rynku jest ich kilka, np.: Nexus, ProGet, Artifactory i Azure Artifacts.
- **Menedżer konfiguracji** — umożliwia zarządzanie zmianami konfiguracji podczas procesu CD; większość narzędzi CD zawiera mechanizm konfiguracyjny z systemem zmiennych.

Podczas procesu CD wdrażanie aplikacji w każdym środowisku przejściowym jest wyzwalane w następujący sposób:

- Może być wyzwolone automatycznie po pomyślnym wykonaniu w poprzednim środowisku. Na przykład możemy sobie wyobrazić przypadek, w którym wdrożenie w środowisku przedprodukcyjnym jest uruchamiane automatycznie po pomyślnym przeprowadzeniu testów integracyjnych w środowisku dedykowanym.
- Może być uruchomione ręcznie w przypadku wrażliwych środowisk, takich jak środowisko produkcyjne, po ręcznym zatwierdzeniu przez osobę odpowiedzialną za sprawdzenie poprawności działania aplikacji w środowisku.

W procesie CD ważne jest to, że wdrożenie do środowiska produkcyjnego — czyli dla użytkownika końcowego — jest uruchamiane ręcznie przez zatwierdzonych użytkowników.



Rysunek 1.3. Proces ciągłego dostarczania

Powyższy diagram wyraźnie pokazuje, że proces CD jest kontynuacją procesu CI. Reprezentuje łańcuch kroków CD, które są automatyczne dla środowisk przejściowych i ręczne dla wdrożeń produkcyjnych. Pokazuje również, że pakiet jest generowany przez CI i przechowywany w menedżerze pakietów oraz że jest to ten sam pakiet, który jest wdrażany w różnych środowiskach.

Teraz, gdy przyjrzeliliśmy się CD, przyjrzyjmy się praktykom ciągłego wdrażania.

Ciągłe wdrażanie

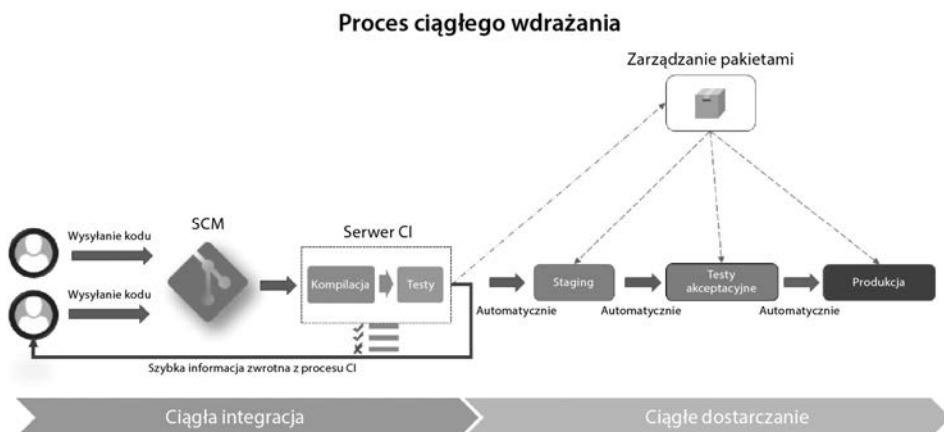
Ciągłe wdrażanie jest rozszerzeniem procesu CD. Automatyzuje cały potok CI/CD od momentu, gdy programista zatwierdzi swój kod, do wdrożenia w środowisku produkcyjnym, przez wszystkie etapy weryfikacji.

Taka praktyka jest rzadko wdrażana w przedsiębiorstwach, ponieważ wymaga wykonania różnych testów (jednostkowych, funkcjonalnych, integracyjnych, wydajnościowych itd.) dla aplikacji. Pomyślne wykonanie tych testów jest wystarczające do sprawdzenia poprawności działania aplikacji pod kątem wszystkich tych zależności. Pozwala również na automatyczne wdrażanie w środowisku produkcyjnym bez konieczności wykonywania jakichkolwiek czynności zatwierdzania.

Ciągły proces wdrażania musi również uwzględniać wszystkie etapy przywracania aplikacji w razie wystąpienia problemu produkcyjnego.

Ciągłe wdrażanie można zastosować przy użyciu i implementacji technik przełączników (ang. *feature toggle*), co obejmuje hermetyzację funkcji aplikacji i aktywowanie danej funkcjonalności na żądanie, bezpośrednio w środowisku produkcyjnym, bez konieczności ponownego wdrażania kodu aplikacji.

Inną techniką jest wykorzystanie niebiesko-zielonej infrastruktury produkcyjnej, która składa się z dwóch środowisk produkcyjnych: jednego niebieskiego i jednego zielonego. Najpierw wdrażamy się do niebieskiego środowiska, a następnie do zielonego; zapewni to, że nie będą wymagane żadne przestoje.



Rysunek 1.4. Proces ciągłego wdrażania

Uwaga

Przełącznikom i niebiesko-zielonemu wykorzystaniu wdrożeń bardziej szczegółowo przyjrzemy się w rozdziale 15., „Skrócenie czasu przestoju wdrażania”.

Powyższy diagram jest prawie taki sam jak w przypadku CD, ale z tą różnicą, że przedstawia automatyczne, kompleksowe wdrożenie.

Procesy CI/CD są zatem istotną częścią kultury DevOps, przy czym CI pozwala zespołom integrować i testować spójność kodu oraz regularnie uzyskiwać szybkie informacje zwrotne. CD automatycznie wdraża się w jednym lub kilku środowiskach staging, dzięki czemu oferuje możliwość przetestowania całej aplikacji, dopóki nie zostanie ona wdrożona w środowisku produkcyjnym.

Wreszcie ciągłe wdrażanie automatyzuje możliwość wdrażania aplikacji od zatwierdzenia do środowiska produkcyjnego.

Uwaga

W rozdziale 7., „Ciągła integracja i ciągłe wdrażanie”, dowiemy się, jak wdrożyć wszystkie te procesy we współpracy z narzędziami Jenkins, Azure DevOps i GitLab CI.

W tej sekcji omówiliśmy praktyki, które są niezbędne dla kultury DevOps, czyli ciągłą integrację, ciągłe dostarczanie i ciągłe wdrażanie.

W następnej sekcji przyjrzymy się innej praktyce DevOps, znanej jako IaC.

Zrozumienie praktyk IaC

IaC to praktyka polegająca na pisaniu kodu zasobów składających się na infrastrukturę.

Praktyka ta zaczęła przynosić efekty wraz z rozwojem kultury DevOps i modernizacją infrastruktury chmury. Rzeczywiście, zespoły operacyjne, które ręcznie wdrażają infrastrukturę, poświęcają czas na wprowadzenie zmian w infrastrukturze ze względu na niespójną obsługę i ryzyko błędów. Ponadto, wraz z modernizacją chmury i jej skalowalnością, sposób budowania infrastruktury wymaga przeglądu wyposażenia (ang. *provisioning*) i praktyki zmian poprzez dostosowanie bardziej zautomatyzowanej metody.

IaC to proces pisania kodu etapów udostępniania i konfiguracji komponentów infrastruktury, który pomaga zautomatyzować jej wdrażanie w powtarzalny i spójny sposób.

Zanim przyjrzymy się korzystaniu z IaC, zobaczmy, jakie są korzyści płynące z tej praktyki.

Korzyści IaC

Korzyści płynące z IaC są następujące:

- Standaryzacja konfiguracji infrastruktury zmniejsza ryzyko błędów.
- Kod opisujący infrastrukturę jest wersjonowany i kontrolowany w menedżerze kodu źródłowego.
- Kod jest zintegrowany z potokami CI/CD.
- Wdrożenia, które wprowadzają zmiany w infrastrukturze, są szybsze i bardziej wydajne.
- Lepsze zarządzanie, kontrola i redukcja kosztów infrastruktury.

IaC przynosi również korzyści zespołowi DevOps, umożliwiając Ops większą wydajność w zakresie zadań związanych z ulepszaniem infrastruktury zamiast poświęcania czasu na ręczną konfigurację. Daje również Dev możliwość ulepszania swojej infrastruktury i wprowadzania zmian bez konieczności proszenia o więcej zasobów operacyjnych.

IaC umożliwia też tworzenie samoobsługowych, efemerycznych środowisk, które zapewnią programistom i testerom większą elastyczność w testowaniu nowych funkcji w izolacji i niezależnie od innych środowisk.

Języki i narzędzia IaC

Języki i narzędzia używane do napisania konfiguracji infrastruktury mogą być różnych typów: **skryptowe**, **deklaratywne** i **programowe**. Zbadamy je w kolejnych sekcjach.

Typy skryptowe

Zaliczają się do nich języki skryptowe, takie jak Bash, PowerShell lub inne, które korzystają z różnych klientów (SDK) dostarczanych przez dostawcę chmury. Na przykład możesz uzyskać dostęp do zasobów platformy Azure za pomocą interfejsu wiersza poleceń platformy Azure lub programu Azure PowerShell.

Oto polecenie, które tworzy grupę zasobów na platformie Azure:

- Korzystając z interfejsu Azure CLI (dokumentacja jest dostępna pod adresem <https://bit.ly/2V10fxj>):
az group create --location westeurope --resource-group MyAppResourcegroup
- Korzystając z Azure PowerShell (dokumentacja jest dostępna pod adresem <https://bit.ly/2VcASeh>):
New-AzResourceGroup -Name MyAppResourcegroup -Location westeurope

Problem z tymi językami i narzędziami polega na tym, że wymagają one dużej ilości linii kodu. Dzieje się tak, ponieważ musimy zarządzać różnymi stanami manipulowanych zasobów i konieczne jest napisanie wszystkich kroków tworzenia lub aktualizowania pożądanej infrastruktury.

Jednak te języki i narzędzia mogą być bardzo przydatne w wypadku zadań, które automatyzują powtarzalne czynności wykonywane na liście zasobów (wybór elementu i zapytania) lub które wymagają złożonego przetwarzania z pewną logiką do wykonania na zasobach infrastruktury, np. skrypt automatyzujący maszyny wirtualne, które mają usuwany określony tag.

Typy deklaratywne

Zaliczają się do nich języki, w których wystarczy zapisać pożądany stan systemu lub infrastruktury w postaci konfiguracji i właściwości. Tak jest np. w przypadku narzędzi Terraform i Vagrant firmy HashiCorp, Ansible, szablonu Azure ARM, Azure Bicep (<https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/overview?tabs=bicep>), PowerShell DSC, Puppet i Chef. Wszystko, co użytkownik musi zrobić, to opisać ostateczny stan pożądanej infrastruktury; narzędzie zadba o jego zastosowanie.

Na przykład poniższy kod Terraform umożliwia zdefiniowanie żądanej konfiguracji grupy zasobów platformy Azure:

```
resource "azurerm_resource_group" "myrg" {
  name = "MyAppResourceGroup"
  location = "West Europe"

  tags = {
    environment = "Bookdemo"
  }
}
```

W tym przykładzie, jeśli chcesz dodać lub zmodyfikować tag, po prostu zmodyfikuj właściwość tags w poprzednim kodzie, a Terraform sam wykona aktualizację.

Oto kolejny przykład, który pozwala zainstalować i uruchomić usługę nginx na serwerze za pomocą Ansible:

```
---
- hosts: all
  tasks:
    - name: install and check nginx latest version
      apt: name=nginx state=latest
    - name: start nginx
      service:
        name: nginx
        state: started
```

Aby się upewnić, że usługa nie jest zainstalowana, po prostu zmień poprzedni kod dla elementu `service` — ustaw wartość `stopped` dla właściwości `state`:

```
---
- hosts: all
  tasks:
    - name: stop nginx
  service:
    name: nginx
    state: stopped
    - name: check nginx is not installed
  apt: name=nginx state=absent
```

W tym przykładzie wystarczyło zmienić właściwość `state`, aby wskazać pożądany stan usługi.

Uwaga

Aby uzyskać szczegółowe informacje na temat korzystania z Terraform i Ansible, zobacz rozdział 2., „Udostępnianie infrastruktury chmury za pomocą Terraform”, i rozdział 3., „Używanie Ansible do konfigurowania infrastruktury IaaS”.

Typy programowe

Od kilku lat obserwuje się, że dwa rodzaje kodu IaC, czyli języki skryptowe lub deklaratywne, używane są przez zespół **operacyjny**. Zwykle nie dotyczy to programistów.

W celu zacieśnienia więzi między programistami a operacjami widzimy pojawianie się narzędzi IaC, które są bardziej oparte na językach znanych programistom, takich jak TypeScript, Java, Python i C#.

Wśród narzędzi IaC, które pozwalają nam udostępniać infrastrukturę za pomocą języka programowania, mamy **Pulumi** (<https://www.pulumi.com/>) i **Terraform CDK** (<https://github.com/hashicorp/terraform-cdk>).

Poniżej znajduje się przykład kodu TypeScriptu napisanego za pomocą Terraform CDK:

```
import { Construct } from 'constructs';
import { App, TerraformStack, TerraformOutput } from 'cdktf';
import {
  ResourceGroup,
} from './.gen/providers/azurerm';
class AzureRgCDK extends TerraformStack {
  constructor(scope: Construct, name: string) {
    super(scope, name);
    new AzurermProvider(this, 'azureFeature', {
      features: [{}],
    });
    const rg = new ResourceGroup(this, 'cdktf-rg', {
```

```
        name: 'MyAppResourceGroup',
        location: 'West Europe',
    });
  }
}
const app = new App();
new AzureRgCDK(app, 'azure-rg-demo');
app.synth();
```

W tym przykładzie, napisanym w języku TypeScript, używamy bibliotek dwuwarstwowych: pakietu npm i Terraform CDK o nazwie `cdktf`. Pakiet npm używany do udostępniania zasobów platformy Azure nosi nazwę `'gen/providers/azurerm'`.

Następnie deklarujemy nową klasę, która inicjuje dostawcę platformy Azure, i definiujemy tworzenie grupy zasobów za pomocą metody `new ResourceGroup`.

Na koniec, aby utworzyć grupę zasobów, tworzymy wystąpienie tej klasy i wywołujemy metodę `app.synth` zestawu CDK.

Uwaga

Aby uzyskać więcej informacji na temat Terraform CDK, proponuję przeczytać następujące wpisy na blogu i obejrzeć następujący film:

<https://www.hashicorp.com/blog/cdk-for-terraform-enabling-python-and-typescript-support>,
<https://www.hashicorp.com/blog/announcing-cdk-for-terraform-0-1>,
<https://www.youtube.com/watch?v=5hSdb0nadRQ>.

Topologia IaC

W infrastrukturze chmurowej IaC dzieli się na kilka typologii:

- wdrażanie i udostępnianie infrastruktury,
- konfiguracja serwera i tworzenie szablonów,
- konteneryzacja,
- konfiguracja i wdrożenie w Kubernetesie.

Przyjrzymy się szerzej każdej z nich.

Wdrażanie i udostępnianie infrastruktury

Udostępnianie to czynność tworzenia instancji zasobów tworzących infrastrukturę. Mogą to być zasoby typu **platforma jako usługa** (ang. *Platform-as-a-Service* — PaaS) i bezserwerowe, takie jak aplikacja internetowa, funkcja platformy Azure, Event Hub, ale także cała zarządzana część sieci, taka jak sieć wirtualna, podsieci, tabele routingu

lub Azure Firewall. W przypadku zasobów maszyn wirtualnych proces udostępniania tworzy lub aktualizuje tylko zasób w chmurze maszyny wirtualnej, ale nie jego zawartość.

Dostępnych jest wiele narzędzi do udostępniania, takich jak Terraform, szablony ARM, Azure CLI, Azure PowerShell, a także Google Cloud Deployment Manager. Oczywiście jest ich znacznie więcej, ale trudno je wszystkie wymienić. W tej książce przyjrzymy się szczegółowo wykorzystaniu Terraform.

Konfiguracja serwera

Ten krok dotyczy konfigurowania maszyn wirtualnych, takich jak utwardzenie (ang. *hardening*), montowanie dysków, konfiguracja sieci (zapora ogniowa, proxy itd.) oraz instalacja middleware.

Istnieją różne narzędzia konfiguracyjne, takie jak Ansible, PowerShell DSC, Chef, Puppet i SaltStack. Oczywiście jest ich znacznie więcej, ale w tej książce szczegółowo przyjrzymy się wykorzystaniu Ansible w celu konfiguracji maszyny wirtualnej.

Aby zoptymalizować czas udostępniania i konfiguracji serwera, można tworzyć modele serwerów, zwanych obrazami, i ich używać. Zawierają one całą konfigurację (hardening, middleware itd.) serwerów. Podczas przygotowywania serwera wskażemy odpowiadający mu szablon. Tak więc za kilka minut będziemy mieli serwer, który został skonfigurowany i jest gotowy do użycia.

Istnieje również wiele narzędzi IaC do tworzenia szablonów serwerów, np. **Aminator** (używany przez Netfliksa) i **HashiCorp Packer**.

Oto przykład kodu Packera służącego do tworzenia obrazu Ubuntu z aktualizacjami pakietów:

```
{
  "builders": [{
    "type": "azure-arm",
    "os_type": "Linux",
    "image_publisher": "Canonical",
    "image_offer": "UbuntuServer",
    "image_sku": "16.04-LTS",
    "managed_image_resource_group_name": "demoBook",
    "managed_image_name": "SampleUbuntuImage",
    "location": "West Europe",
    "vm_size": "Standard_DS2_v2"
  }],
  "provisioners": [{
    "execute_command": "chmod +x {{ .Path }}; {{ .Vars }} sudo -E sh
    ↪ '{{ .Path }}'",
```

```
"inline": [  
  "apt-get update",  
  "apt-get upgrade -y",  
  "/usr/sbin/waagent -force -deprovision+user && export  
  HISTSIZE=0 && sync"  
],  
"inline_shebang": "/bin/sh -x",  
"type": "shell"  
}]  
}
```

Ten skrypt tworzy obraz szablonu dla maszyny wirtualnej Standard_DS2_V2 na podstawie systemu operacyjnego Ubuntu (sekcja `builders`). Dodatkowo podczas tworzenia obrazu Packer aktualizuje wszystkie pakiety za pomocą polecenia `apt-get update`.

Następnie Packer wyrejestruje obraz, aby usunąć wszystkie informacje o użytkowniku (sekcja `provisioners`).

Uwaga

Packer zostanie szczegółowo omówiony w rozdziale 4., „Optymalizacja wdrażania infrastruktury za pomocą Packera”.

Niezmienna infrastruktura z kontenerami

Konteneryzacja polega na wdrażaniu aplikacji w kontenerach zamiast na maszynach wirtualnych.

Obecnie najpowszechniejszym oprogramowaniem służącym do konteneryzacji jest **Docker**. Obraz Dockera jest konfigurowany za pomocą kodu w pliku *Dockerfile*. Plik ten zawiera deklarację obrazu bazowego, który reprezentuje używany system operacyjny, dodatkowe oprogramowanie middleware, pliki i binaria niezbędne dla aplikacji oraz konfigurację sieciową portów. W przeciwieństwie do maszyn wirtualnych, kontenery są uważane za niezmiennie; konfiguracja kontenera nie może być modyfikowana podczas jego wykonywania.

Oto prosty przykład pliku *Dockerfile*:

```
FROM ubuntu  
RUN apt-get update  
RUN apt-get install -y nginx  
ENTRYPOINT ["/usr/sbin/nginx","-g","daemon off;"]  
EXPOSE 80
```

W tym obrazie Dockera używamy podstawowego obrazu Ubuntu, instalujemy `nginx` i udostępniamy port 80.

Uwaga

Część dotycząca platformy Docker zostanie szczegółowo omówiona w rozdziale 9., „Konteneryzacja aplikacji za pomocą Dockera”.

Konfiguracja i wdrożenie w Kubernetesie

Kubernetes jest orkiestratorem kontenerów — to technologia, która w większości uosabia IaC (moim zdaniem) ze względu na sposób wdrażania kontenerów, architekturę sieci (równoważenie obciążenia, porty itd.) i zarządzanie woluminami. Chroni także poufne informacje, które są zapisane w plikach specyfikacji YAML.

Oto prosty przykład pliku specyfikacji YAML:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-demo
  labels:
    app: nginx
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx
template:
  metadata:
    labels:
      app: nginx
  spec:
    containers:
      - name: nginx
        image: nginx:1.7.9
    ports:
      - containerPort: 80
```

W poprzednim pliku specyfikacji możemy zobaczyć nazwę obrazu do wdrożenia (nginx), port do otwarcia (80) i liczbę replik (2).

Uwaga

Część dotycząca Kubernetesa zostanie szczegółowo omówiona w rozdziale 10., „Efektywne zarządzanie kontenerami za pomocą Kubernetesa”.

IaC, podobnie jak tworzenie oprogramowania, wymaga od nas wdrożenia praktyk i procesów, które umożliwiają ewolucję i utrzymanie kodu infrastruktury.

Wśród tych praktyk są te związane z tworzeniem oprogramowania:

- Stosuj dobre zasady nazewnictwa.
- Nie przeciążaj kodu niepotrzebnymi komentarzami.
- Używaj małych funkcji.
- Zaimplementuj obsługę błędów.

Uwaga

Aby dowiedzieć się więcej o dobrych praktykach tworzenia oprogramowania, przeczytaj doskonałą książkę związaną z tym tematem, *Clean Code* Roberta Martina.

Są jeszcze inne konkretne praktyki, które moim zdaniem zasługują na więcej uwagi:

- **Kod musi być w pełni zautomatyzowany.** Podczas wykonywania IaC należy zakodować i zautomatyzować wszystkie etapy udostępniania i nie należy pozostawiać ręcznych działań poza kodem, które zakłócają automatyzację infrastruktury — co może generować błędy. A jeśli to konieczne, nie wahać się użyć kilku narzędzi, takich jak Terraform i Bash, ze skryptami Azure CLI.
- **Kod musi się znajdować w menedżerze kodu źródłowego.** Kod infrastruktury musi również znajdować się w SCM, aby można go było wersjonować, śledzić, scalać i przywracać, a tym samym zapewniać lepszą widoczność kodu między programistami i zespołem operacyjnym.
- **Kod infrastruktury musi być trzymany z kodem aplikacji.** W niektórych przypadkach może to być trudne, ale jeśli to możliwe, znacznie lepiej jest umieścić kod infrastruktury w tym samym repozytorium co kod aplikacji. Ma to na celu zapewnienie lepszej organizacji pracy między programistami i operatorami, którzy będą dzielić ten sam obszar roboczy.
- **Oddzielenie ról i katalogów.** Dobrze jest oddzielić kod od infrastruktury — zgodnie z rolą kodu. Umożliwia to utworzenie jednego katalogu do udostępniania i konfigurowania maszyn wirtualnych i innego, który będzie zawierał kod do testowania integracji całej infrastruktury.
- **Integracja z procesem CI/CD.** Jednym z celów IaC jest możliwość automatyzacji wdrażania infrastruktury. Tak więc od początku jego implementacji konieczne jest utworzenie procesu CI/CD, który zintegruje kod, przetestuje go i wdroży w różnych środowiskach. Niektóre narzędzia, takie jak Terratest, umożliwiają tworzenie testów dla kodu infrastruktury. Jedną z najlepszych praktyk jest integracja procesu CI/CD infrastruktury w tym samym potoku co aplikacja.
- **Kod musi być idempotentny.** Wykonanie kodu wdrażania infrastruktury musi być idempotentne — czyli kod powinien być ciągle automatycznie wykonywalny. Oznacza to, że skrypty muszą uwzględniać stan infrastruktury

podczas jej uruchamiania i nie generować błędów, jeśli zasób do utworzenia już istnieje lub zasób do usunięcia został już usunięty. Zobaczymy, że języki deklaratywne, takie jak Terraform, natywnie przyjmują ten aspekt idempotencji. Kod infrastruktury raz w pełni zautomatyzowany musi umożliwiać budowę i niszczenie infrastruktury aplikacji.

- **Kod jako dokumentacja.** Kod infrastruktury musi być jasny i musi służyć jako dokumentacja. Dokumentacja infrastruktury zajmuje dużo czasu i w wielu przypadkach nie jest aktualizowana w miarę rozwoju infrastruktury.
- **Kod musi być modułowy.** W infrastrukturze komponenty często mają ten sam kod — jedyną różnicą jest wartość ich właściwości. Również te komponenty są kilkakrotnie wykorzystywane w aplikacjach firmy. Dlatego ważne jest, aby zoptymalizować czasy pisania kodu przez podzielenie go na moduły (lub role w przypadku Ansible), które będą wywoływane jako funkcje. Kolejną zaletą korzystania z modułów jest możliwość standaryzacji nazewnictwa zasobów i zgodność niektórych właściwości.
- **Posiadanie środowiska programistycznego.** Problem z IaC polega na tym, że trudno jest testować kod infrastruktury będącej w fazie rozwoju w środowiskach używanych do integracji, a także testować aplikację, ponieważ zmiana infrastruktury może wpływać na kod. Dlatego ważne jest, aby mieć środowisko programistyczne nawet dla IaC, które może w każdej chwili ulec uszkodzeniu lub nawet zostać zniszczone.

W przypadku testów infrastruktury lokalnej niektóre narzędzia symulują środowisko lokalne, np. Vagrant (od HashiCorp), więc należy ich używać do testowania skryptów kodu tak często, jak to możliwe.

Oczywiście pełna lista dobrych praktyk jest dłuższa; również wszystkie metody i procesy praktyk inżynierii oprogramowania mają zastosowanie.

Dlatego IaC, podobnie jak procesy CI/CD, jest kluczową praktyką **kultury DevOps**, która umożliwia wdrażanie i konfigurowanie infrastruktury poprzez pisanie kodu. Jednak IaC może być skuteczna tylko przy użyciu odpowiednich narzędzi i wdrażaniu dobrych praktyk.

W tej sekcji zawarliśmy omówienie niektórych najlepszych praktyk DevOps. Teraz przedstawimy krótki przegląd ewolucji kultury DevOps.

Ewolucja kultury DevOps

Z czasem i doświadczeniem zdobytym przy stosowaniu kultury DevOps możemy zaobserwować ewolucję praktyk, a także zespołów pragnących dołączyć do tego ruchu.

Tak jest np. w przypadku praktyki **GitOps**, która coraz częściej zaczyna się pojawiać w firmach.

Przepływ pracy GitOps, który jest powszechnie stosowany w Kubernetesie, polega na użyciu Gita jako jedyne źródła prawdy; oznacza to, że repozytorium Gita zawiera kod stanu infrastruktury, a także kod aplikacji do wdrożenia.

Kontroler będzie nadzorował pobieranie źródła Gita podczas zatwierdzania kodu, wykonywania testów i ponownego wdrażania aplikacji.

Uwaga

Aby uzyskać więcej informacji o kulturze, praktykach i przepływach pracy GitOps, przeczytaj oficjalny przewodnik po GitOps: <https://www.weave.works/technologies/gitops/>.

Podsumowanie

W tym rozdziale zobaczyliśmy, że kultura DevOps to złożenie współpracy, procesów i narzędzi. Następnie szczegółowo opisaliśmy poszczególne etapy procesu CI/CD i wyjaśniliśmy różnicę między ciągłą integracją, ciągłym dostarczaniem i ciągłym wdrażaniem. W ostatniej części wyjaśniliśmy, jak korzystać z IaC z jej najlepszymi praktykami, a także omówiliśmy ewolucję kultury DevOps.

Poznaliśmy podstawy kultury DevOps i jej praktyk, co nadaje ton pozostałym rozdziałom tej książki, w których omówimy, jak zastosować tę kulturę za pomocą narzędzi i praktyk.

W następnym rozdziale zaczniemy od omówienia implementacji procesu *infrastruktury jako kodu* i sposobu dostarczania infrastruktury za pomocą Terraform.

Pytania

1. Od jakich słów pochodzi skrót DevOps?
2. Czy DevOps to termin, który reprezentuje nazwę narzędzia, kulturę, społeczeństwo czy tytuł książki?
3. Jakie są trzy założenia kultury DevOps?
4. Jaki jest cel ciągłej integracji?
5. Jaka jest różnica między ciągłym dostarczaniem a ciągłym wdrażaniem?
6. Co oznacza IaC?

Dalsza lektura

Jeśli chcesz dowiedzieć się więcej o kulturze DevOps, oto kilka zasobów:

- Centrum zasobów DevOps (zasoby firmy Microsoft) — <https://docs.microsoft.com/en-us/azure/devops/learn/>.
- Raport na temat DevOps z 2020 r. (zasoby Puppeta) — <https://puppet.com/resources/report/2020-state-of-devops-report>.

Skorowidz |

A

- ACI, Azure Container Instances, 285, 305
 - wdrażanie kontenera, 285
 - Docker Compose, 300
- ACR, Azure Container Registry, 283, 305
 - obraz Dockera, 285
 - repozytorium Helma, 325
- Active Directory, 55
- agent hostowany samodzielnie, 223
- AKS, Azure Kubernetes Service, 305, 325
 - konfigurowanie pliku kubeconfig, 327
 - logi w czasie rzeczywistym, 332
 - monitorowanie, 328
 - skalowanie, 329
 - tworzenie usługi, 326
 - zalety, 328
- Aminator, 40
- analiza kodu
 - statyczna, 369
 - w czasie rzeczywistym, 378
 - za pomocą
 - SonarCloud, 468
 - SonarLint, 378
 - SonarQube, 369
- Ansible
 - artefakty, 89
 - hosty, 89
 - instalowanie za pomocą skryptu, 86
 - integrowanie z Azure Cloud Shell, 88
 - inwentarz, 89
 - maszyn wirtualnych, 113
 - katalog roles, 99, 105
 - konfigurowanie, 90
 - hostów, 94
 - infrastruktury IaaS, 84
 - korzystanie z podglądu, 102
 - moduły, 98
 - opcja testowa pracy, 102
 - PLAY Recap, 101
 - playbook, 90
 - integracja z szablonem, 135
 - tworzenie, 134
 - ulepszanie, 99
 - uruchamianie, 97
 - wykonanie testu, 103
 - wykonywanie, 101, 102
 - plik inwentarza, 93
 - testowanie, 95
 - wykonanie, 114
 - tworzenie szablonów Packera, 133
 - uruchamianie w Azure Pipelines, 255
 - używanie zmiennych, 105
 - wyświetlenie konfiguracji, 92
 - wywołanie MySQL, 107
 - zwiększanie poziomu logowania, 104
- Ansible Vault, 410
 - ochrona danych, 104
 - odszyfrowanie pliku, 109
 - szyfrowanie pliku, 108
- API, 297, 339
- aplikacje mikrousług, 305
- App Service, 433
 - sloty wdrażania, 433
- Artifact Hub, 317
 - pakiet wordpress, 319
- automatyzacja wdrożeń, 480
- Azure
 - adres IP SonarQube, 375
 - brak grupy zasobów, 67
 - klucz dostępu do magazynu, 80
 - konfigurowanie
 - platformy, 403
 - Terraform, 55
 - lista rejestracji aplikacji, 57
 - odzyskiwanie hasła SonarQube, 376
 - strona logowania, 54, 59
 - tag role, 111

- Azure
 - tworzenie
 - jednostki SP, 56
 - obrazu platformy, 130
 - SonarQube, 374
 - udostępnianie zasoby, 72
 - uwierzytelnianie, 136
 - używanie
 - Ansible, 88
 - Packera, 123
 - wdrażanie
 - SonarQube, 375
 - zielono-niebieskie, 432
 - Azure Artifacts, 206, 217
 - Azure Boards, 217
 - Azure CLI, 404
 - Azure Cloud Shell, 53, 54, 403
 - Azure DevOps
 - rozszerzenie SonarQube, 382
 - Azure Key Vault, 410
 - Azure Pipelines, 217
 - definiowanie
 - wersji, 233
 - aplikacji, 229
 - dodawanie
 - artefaktu, 230
 - zadania, 225
 - dzienniki
 - Ansible, 259
 - potoku, 255
 - Terraform, 259
 - edycja nazwy
 - usługi aplikacji, 233
 - wersji, 232
 - instalowanie npm, 364
 - klonowanie, 232
 - konfigurowanie
 - kodu źródłowego, 224
 - potoku CI/CD, 287
 - puli agentów, 224
 - wersji, 231
 - lista zadań, 223
 - przeglądanie artefaktów, 228
 - stan wdrożenia, 234
 - szablon Azure App Service deployment, 229
 - testy
 - podsumowanie wykonania, 227
 - publikowanie wyników, 365, 366
 - tworzenie potoku, 254
 - CD, 228
 - CI, 219, 381
 - CI/CD, 329
 - YAML, 236
 - tworzenie
 - wersji, 234
 - wydania, 363
 - uruchamianie, 227
 - Ansible, 255
 - Newmana, 365
 - Packera, 252
 - potoku, 239
 - Terraform, 255
 - włączanie
 - CI, 226
 - CD, 230
 - wybór
 - pliku YAML, 237, 238
 - repozytorium, 221, 237
 - szablonu, 222
 - źródła GitHuba, 288
 - wykonanie zadania, 239
 - zakładka Variables, 222
 - zapisywanie i kolejkovanie potoku, 226
 - zarządzanie potokami CI/CD, 216
 - zmienne, 255, 259
 - Azure Repos, 164, 181, 217
 - dodawanie pliku, 188
 - formularz PR, 194
 - import repozytorium, 219
 - lista gałęzi, 192
 - menu, 183
 - menu Import, 218
 - tworzenie PR, 193
 - zatwierdzenie PR, 194
 - Azure Test Plans, 217
 - Azure Traffic Manager, 434
 - konfigurowanie usługi, 435
 - punkty końcowe, 436
- ## B
- BDD, behavior-driven development, 485
 - BDD, behavior-driven design, 26
 - bezpieczeństwo, 399

C

CD, continuous delivery, 25, 31, 202
 tworzenie potoku, 228
Chocolatey, 122, 175, 402
CI, continuous integration, 25, 29, 200
 korzystanie z GitHub Actions, 465
 menedżer
 konfiguracji, 203
 repozytorium, 202
 obszary pośrednie, 202
 serwer, 202
 tworzenie potoku, 219, 245
 dla SonarQube, 381
 wykonywanie SonarQube, 380
CI/CD, ciągła integracja/ciągłe wdrażanie, 163, 484
 korzystanie
 z Azure Pipelines, 216
 z GitLab CI, 240
 z Jenkinsa, 208
 z Newmana, 361
 menedżer pakietów, 203
 narzędzia, 203
 potok
 w pliku YAML, 234
 w trybie UI, 234
 przebieg pracy, 201
 tworzenie potoku
 dla kontenera, 287
 dla Kubernetesa, 329
 wdrażanie
 infrastruktury jako kodu, 251
 kontenera do ACI, 285
ciągła integracja, CI, 25, 29, 200
ciągłe dostarczanie, CD, 25, 31, 202
ciągłe wdrażanie, 33
Collection Runner, 393

D

demon Dockera, 267
DevOps, development-operations, 25, 399
 najlepsze praktyki, 479
DevSecOps, 486
Docker, 41, 265
 dokumentacja instalacji, 271
 instalowanie, 268
 kontener, 273

 lista obrazów, 280
 narzędzia wiersza poleceń, 294
 obraz, 273
 tworzenie, 276, 278
 w ACR, 285
 plik Dockerfile, 273
 testowanie kontenera, 279
 wolumin, 273
 wysyłanie obrazu
 do rejestru prywatnego, 283
 do rejestru publicznego, 279

Docker Compose, 296
 instalowanie, 297
 lista kontenerów, 300
 plik konfiguracyjny, 298
 wdrażanie kontenerów w ACI, 300
 wykonywanie, 299
Docker Desktop, 269
 komponenty Docker Compose, 300
 logowanie do Docker Huba, 271
 włączanie Kubernetesa, 308
Docker Hub, 267
 publikowanie obrazu Dockera, 279
 sekcja Explore, 268
 strona logowania, 268
 tworzenie konta, 267
 wyszukiwanie obrazu, 282
dostęp do magazynu Azure, 80
dynamiczny plik inwentarza, 256

E

ewolucja kultury, 44

F

flagi funkcjonalności, feature flags, 432, 436
 implementacja, 439
 prezentacja przełączania, 442
 tworzenie, 444
 w LaunchDarkly, 444, 447
format
 HCL, 140
 JSON, 351, 424
 YAML, 234, 297, 482
FQDN, fully qualified domain name, 93

G

- Git, 164
 - gałąź master, 177–180
 - gałęzie, 177
 - przełączanie, 191
 - scalanie, 195
 - tworzenie, 190, 192, 197
 - zarządzanie, 195
 - instalowanie, 166
 - klonowanie, 176
 - konfigurowanie, 176
 - narzędzie
 - GitKraken, 196
 - Sourcetree, 197
 - polecenia, 177
 - przepływ danych, 182
 - repozytorium, 176
 - konfigurowanie, 182
 - tworzenie, 182
 - wersjonowanie kodu w Azure Repos, 218
 - wyświetlanie wersji, 174
 - wzorec Gitflow, 195
 - zatwierdzanie, 176
- Gitflow, 195
- GitHub
 - aktywacja Issues, 475
 - dziennik zmian, 459, 460
 - funkcje i narzędzia, 451
 - konfigurowanie webhooka, 210
 - link do wydania, 462
 - lista żądań pobierania, 457
 - operacja scalania, merge, 455
 - repozytoria publiczne, 451
 - rozwidlanie repozytorium, 454
 - rozwijanie projektu, 453
 - tworzenie
 - repozytorium, 451
 - wydania, 463
 - udostępnianie plików binarnych, 461
 - żądanie pobierania, pull request, 455
- GitHub Actions, 464
 - kod źródłowy przepływu pracy, 467
 - szablony przepływów pracy, 465
 - tworzenie potoku CI, 465
 - wybór szablonu Node.js, 466
 - wykonanie przepływu pracy, 468
 - zarządzanie potokami CI/CD, 464

GitLab

- importowanie kodu, 244
 - konfigurowanie projektu, 243
 - rejestracja, 241
 - repozytorium, 245
 - szablon projektu, 243
 - tworzenie
 - nowego projektu, 242
 - potoku CI, 245
 - uruchamianie CI/CD, 244
 - uwierzytelnianie, 241
 - wykonanie potoku CI, 247
 - zarządzanie kodem źródłowym, 242
- GitLab CI, 240

H

- HashiCorp Packer, 40
- hasła
 - zapisywanie w Vault, 415
- Helm, 316
 - charty, 317
 - publikowanie, 323
 - tworzenie, 321
 - instalowanie, 316
 - aplikacji, 320
 - pakiety
 - lista, 320, 322
 - tworzenie, 323
 - wyszukiwanie, 318
- hosty, 89

I

- IaaS, 84
- IaC, Infrastructure as Code, 25, 35, 251
 - infrastruktura z kontenerami, 41
 - konfigurowanie serwera, 40
 - narzędzia, 36
 - typy
 - deklaratywne, 37
 - programowe, 38
 - skryptowe, 36
 - udostępnianie infrastruktury, 39
 - wdrażanie
 - infrastruktury, 39
 - w Kubernetesie, 42
- infrastruktura
 - IaaS, 84
 - jako kod, IaC, 25, 35, 251

InSpec, 400
 instalowanie, 402
 konfigurowanie platformy Azure, 403
 sprawdzanie profilu, 409
 testy
 tworzenie, 405
 wykonanie, 409
 zgodności, 406
instalacja
 Ansible, 86
 Docker Compose, 297
 Dockera, 268
 Gita, 166
 Helma, 316
 InSpec, 402
 Jenkinsa, 208
 Kubernetesa, 307
 Newmana, 355
 npm, 364
 Packera, 119
 Postmana, 341
 SonarQube, 372
 Terraform, 48
 Vagranta, 148
 Vault, 411
interfejs
 programowania aplikacji, API, 297, 339
 użytkownika, UI, 234
inwentarz, 89
 dynamiczny, 92, 256
 statyczny, 92
izolacja kodu, 190

J

Java Runtime Environment, JRE, 370
jednostka Azure SP, 55
Jenkins
 implementacja CI/CD, 208
 instalowanie, 208
 konfigurowanie, 208
 GitHuba, 213
 webhooka GitHuba, 211
 zadania CI, 211
 konsola zadań, 216
 w Azure Marketplace, 209
 wtyczka integracyjna GitHuba, 209
 zadania
 historia wykonywania, 215
 tworzenie, 212
 uruchamianie, 214
 wykonywanie, 215

język Markdown, 459
języki
 IaC, 36
 skryptowe, 36
JSON, 351, 424

K

KeyPass, 410
klient Dockera, 267
konfiguracja
 Ansible, 90
 Docker Desktop, 270
 dostawcy Terraform, 57
 Gita, 176
 infrastruktury IaaS, 84
 Jenkinsa, 208
 maszyn wirtualnych, 40, 84
 Terraform, 55
 webhooka GitHuba, 210
 zadania CI, 211
konteneryzacja aplikacji, 265
kontrola kodu źródłowego
 rozproszona, 165
 scentralizowana, 165
KPI, key performance indicators, 487
Kubernetes, 42
 architektura, 307
 instalowanie, 307
 pulpitu nawigacyjnego, 309
 lista zasobów, 312
 menedżer pakietów Helm, 316
 monitorowanie
 aplikacji, 330
 metryk, 330, 333
 narzędzie
 Grafana, 334
 Lens, 332
 Octant, 332
 Prometheus, 334
 pody, 307
 serwer główny, 306
 uwierzytelnianie, 311
 wdrażanie aplikacji, 312
 węzły, nodes, 306
 robocze, 307
 zarządzanie kontenerami, 305
kultura współpracy, 26

L

LastPass, 410
LaunchDarkly, 443
 flagi funkcjonalności, 446, 447
luki w zabezpieczeniach, 473

M

magazyn Azure, 80
maszyna wirtualna, VM, 84
 publiczny adres IP, 260
 tworzenie, 156
 uzyskiwanie połączenia, 158
 wykonywanie poleceń, 159
menedżer
 hasel AWS, 410
 kodu źródłowego, SCM, 30
 konfiguracji, 32, 203
 kontroli wersji, VCM, 163
 pakietów, 32, 203
 Helm, 316
 Nexusa, 206
 NuGet, 204
 poświadczeń Gita, 172
 potoków CI/CD, 464
 repozytorium, 202
metoda zwinna, agile, 488
moduły Ansible, 98
monitorowanie systemu, 487

N

narzędzia, 27
 do konfigurowania potoku CI/CD, 203
 Gitflow, 196
 IaC, 36
Newman, 354
 instalowanie, 355
 integracja z potokiem CI/CD, 361
 publikowanie wyniku testów, 366
 w Azure Pipelines
 tworzenie wydania, 363
 uruchamianie, 365
nginx, 260, 294
npm, 205
 instalowanie w Azure Pipelines, 364

O

obraz
 Dockera, 276
 maszyny wirtualnej, 138, 143
 Azure, 139
 Terraform, 295
ochrona danych, 410
oprogramowanie jako usługa, SaaS, 202
OWASP, 387, 486
OWASP ZAP, 389
 automatyczne skanowanie, 390
 wynik skanowania, 391

P

PaaS, Platform-as-a-Service, 39
PaC, Pipeline as Code, 246, 482
Packer
 dane wyjściowe, 139
 instalowanie
 ręczne, 119
 za pomocą skryptu, 120–123
 integrowanie z Azure Cloud Shell, 123
 obraz maszyny wirtualnej, 138, 139
 sprawdzanie instalacji, 124
 szablony
 dla maszyn wirtualnych, 125
 obraz platformy Azure, 130
 struktura, 125–130
 użycie Ansible, 133
 w formacie HCL, 140
 walidacja, 137
 zmienne szablonu, 137
 tymczasowa
 grupa zasobów, 139
 maszyna wirtualna, 138
 uruchamianie, 136
 w Azure Pipelines, 252
 uwierzytelnianie w Azure, 136
paczki, charts, 316
pakiety
 Azure Artifacts, 207
 NuGet, 205
 uniwersalne, 207
 wordpress, 319
piaskownica, sandbox, 58
platforma jako usługa, PaaS, 39

- playbook, 90
 - integracja z szablonem, 135
 - tworzenie, 97, 134
 - ulepszanie, 99
 - uruchamianie, 97
 - wykonywanie, 101, 102
- plik
 - Dockerfile, 273
 - instrukcje, 274, 275
 - dziennika zmian, 459
 - inwentarza Ansible
 - dynamiczny, 110
 - konfigurowanie hostów, 94
 - statyczny, 93
 - testowanie, 95
 - konfiguracyjny
 - Ansible, 91
 - Vagranta, 152, 154
 - kubeconfig, 311, 327
 - main.tf, 286
 - profilu InSpec, 405
 - Readme.md, 185
 - stanu infrastruktury, 77
- pliki
 - JSON, 356, 424
 - YAML, 234, 297, 313
- polecenia Gita, 177
- polecenie
 - ansible
 - help, 87
 - ping, 96
 - version, 87, 159
 - config, 91
 - playbook, 101
 - docker
 - build, 276, 288
 - compose up, 302
 - help, 272
 - image, 278
 - login, 280
 - ps, 278, 300
 - pull, 295
 - push, 281
 - run, 278, 295
 - tag, 280
 - compose up -d, 299
 - git
 - add, 179, 186
 - branch, 180, 191
 - checkout, 180
 - clone, 178, 188
 - commit, 179, 186, 187
 - init, 178, 184
 - merge, 180
 - pull, 172, 180, 189
 - push, 179, 187
 - remote add, 178, 185
 - status, 186
 - helm
 - create, 321
 - delete, 321
 - help, 317
 - install, 322
 - ls, 322
 - package, 323
 - search, 318
 - inspec exec, 409
 - kubectl, 309
 - apply, 314
 - get pods, 322
 - proxy, 310
 - login, 66
 - newman run, 359
 - packer
 - help, 124
 - version, 124
 - terraform
 - apply, 70, 296, 423
 - destroy, 73
 - fmt, 74
 - init, 68, 81, 295, 423
 - plan, 69, 75, 296, 423
 - validate, 75
 - vagrant
 - destroy, 159
 - help, 156
 - ssh, 158
 - up, 157
 - vault kv get, 417
 - zap-cli
 - active-scan, 391
 - report, 391
- połączenie SSL, 209
- Postman
 - dodawanie zmiennej środowiskowej, 347
 - edytowanie
 - kolekcji, 343
 - żądania, 345
 - eksportowanie
 - kolekcji, 356
 - środowisk, 357

- instalowanie, 341
- kod testów, 350
- konfigurowanie żądania, 345
- rejestracja, 351
- testowanie interfejsów API, 339
- tworzenie
 - kolekcji, 342
 - kolekcji żądań, 340
 - środowiska, 347
 - testów, 349
 - żądania, 343
- uruchamianie testów wydajności, 392
- używanie zmiennej środowiskowej, 348
- wyniki testu, 352
- zakładka Tests, 349
- Postman Collection Runner, 352
- praktyki, 43
 - GitOps, 45
 - IaC, 35
- proces, 26
 - CI/CD Terraform, 76
 - ciągłego dostarczania, 33
 - ciągłego wdrażania, 34
 - ciągłej integracji, 31
 - Gita, 181
- projektowanie
 - architektury systemu, 482
 - oparte na testach, TDD, 26, 485
 - oparte na zachowaniu, BDD, 26, 485
- projekty open source, 449
- Pulumi, 38

R

- rejestr
 - Dockera, 267
 - prywatny, 283
- repozytorium
 - Gita, *Patrz także* Azure Repos
 - adres URL, 185
 - aktualizacja kodu, 189
 - archiwizacja, 187
 - inicjowanie, 184
 - klonowanie, 188
 - konfigurowanie, 182
 - pobieranie aktualizacji, 189
 - tworzenie, 182
 - GitLaba, 245
 - Helma, 317, 325
 - na GitHubie, 451

- Nexusa OSS, 205
- NuGet, 205
- rola, role, 99
- rozwidlenie, fork, 453

S

- SaaS, software-as-a-service, 202
- SCM, Source Code Manager, 30
- serwer
 - CI, 202
 - Vault, 413
- SonarCloud
 - analiza kodu, 468
- SonarLint, 378
 - analiza kodu, 378
- SonarQube, 370
 - analiza kodu, 369, 384
 - architektura, 371
 - instalowanie
 - na Kubernetesie, 377
 - na platformie Azure, 373
 - ręczne, 372
 - za pomocą Dockera, 373
 - integrowanie z procesem CI, 380
 - w Azure Pipelines, 383
- SP, service principal, 55
- SSL, Secure Sockets Layer, 209
- system kontroli wersji, VCS, 163, *Patrz także* Git
- szablon Packera, 252
 - playbook Ansible, 135
 - sekcja
 - builders, 125
 - provisioners, 127
 - variables, 129
 - sprawdzanie poprawności, 137
 - tworzenie obrazu platformy Azure, 130
 - użycie Ansible, 133
 - w formacie HCL, 140
- szyfrowanie pliku, 108

Ś

- środowisko programistyczne, 147

T

TDD, test-driven design, 26
TDD, test-driven development, 485
Terraform, 38, 47

- cykl życia, 72
 - w procesie CI/CD, 75
- dane wyjściowe, 424
- definiowanie architektury Azure, 60
- dobre praktyki, 63
- formatowanie kodu, 74
- inicjalizowanie, 67
- instalowanie
 - ręczne, 49
 - za pomocą skryptu, 49–52
- integrowanie z Azure Cloud Shell, 53
- jednostka Azure SP, 55
- katalog konfiguracji, 68
- konfiguracja dostawcy, 57
- korzystanie z obrazów Packera, 143
- lista udostępnionych zasobów, 72
- plik stanu, 77
- pobieranie sekretów Vault, 421
- podgląd zmian, 69
- potwierdzenie zmian, 70
- przepływ pracy CI/CD, 76
- skręcanie czasu przestoju, 427
- testowanie, 58
- udostępnianie zasobu ACI, 286
- uruchamianie w Azure Pipelines, 255
- usuwanie infrastruktury, 72
- walidacja konfiguracji, 74
- wdrażanie infrastruktury, 66
- wyświetlanie danych wrażliwych, 424

testowanie interfejsów API, 339

testy

- A/B, 443
- bezpieczeństwa, 386
- integracyjne, 485
- konfiguracji Runnera, 394
- penetracyjne, 387
- wydajności, 386, 392
- zgodności InSpec, 406

topologia IaC, 39

tworzenie

- charta, 321
- kodu Terraform, 286
- kolekcji Postmana, 340, 342
- kontenera obrazu, 278
- maszyny wirtualnej, 156
- obrazu

- Dockera, 276
- platformy Azure, 130

pakietu Helma, 323

playbooka, 97

- Ansible, 134

pliku

- Dockerfile, 273
- inwentarza dynamicznego, 110
- inwentarza statycznego, 92
- konfiguracyjnego Vagranta, 152, 154

potoku, 254

- CD, 228
- CI, 219, 245, 381
- CI/CD, 287, 329
- YAML, 234, 236

projektu LaunchDarkly, 444

repozytorium

- Gita, 182
- na GitHubie, 451

szablonów Packera

- dla maszyn wirtualnych, 125
- przy użyciu Ansible, 133
- w formacie HCL, 140

środowiska programistycznego, 147

testów

- InSpec, 405, 406
- Postmana, 349

usługi AKS, 326

żądania, 343

U

UI, user interface, 234

usługa

- ACI, 285
- AKS, 326
- App Service, 432
- Azure
 - Active Directory, 55
 - AD SP, 131, 136
 - Pipelines, 216
 - Repos, 181
 - SP, 55
 - Traffic Manager, 432, 434
- Docker Hub, 267
- zarządzania kluczami, 410

usługi Azure DevOps, 217

uwierzycznianie

- w Azure, 136
- wieloskładnikowe, MFA, 387

V

Vagrant
 inicjalizacja, 154
 instalowanie
 ręczne, 148
 za pomocą skryptu, 150, 151
 tworzenie
 pliku konfiguracyjnego, 152, 154
 środowiska programistycznego, 147
 weryfikacja konfiguracji, 156
 wyświetlanie poleceń, 157
Vagrant Box, 152
Vagrant CLI, 156
 tworzenie maszyny wirtualnej, 156
Vagrant Cloud, 152
 boksy, 153, 154
Vault, 410
 instalowanie
 automatyczne, 412
 ręczne, 412
 interfejs webowy, 418
 ochrona poufnych danych, 410
 odczytywanie sekretów, 416
 status, 415
 uruchamianie serwera, 413
 zapisywanie haseł, 415
VCM, version control manager, 163
VCS, version control system, 163
Visual Studio Code, 378, 427
 rozszerzenie SonarLint, 379
VSTS, *Patrz* Azure Pipelines

W

walidacja
 kodu, 74
 szablonu Packera, 137
wdrażanie
 CI, 30
 infrastruktury
 Azure, 60
 jako kodu, 251
 za pomocą Packera, 117
 kontenera do ACI, 285
 zielono-niebieskie, 430, 432
webhook GitHuba, 210
wersja aplikacji, release, 228

WhiteSource Bolt
 instalowanie, 475
 konfigurowanie, 475
 wykryte problemy, 476
 wykrywanie luk w zabezpieczeniach, 473
wiersz poleceń
 kubectl, 330
 Newmana, 359
 zap-cli, 391
wybór narzędzi, 480
wysyłanie obrazu Dockera
 do Docker Huba, 279
 do rejestru prywatnego, 283
wyszukiwanie
 pakietów Helma, 318
 pakietu wordpress, 319
wzorce wdrażania, 429
wzorzec
 Canary release, 430
 Dark launch, 432
 Gitflow, 181, 195

Y

YAML, YAML Ain't Markup Language, 297, 482
 tworzenie definicji potoku, 234

Z

ZAP, Zed Attack Proxy, 388, 486
 testy penetracyjne, 387
zapora aplikacji webowej, WAF, 387
zarządzanie
 kontenerami, 305
 projektami, 488
zdalne zaplecze, remote backend, 78

Ż

żądanie, request, 343
 pobierania, pull request, 455

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

Potrzebujesz efektywności? Praktykuj DevOps i wygrywaj na rynku!

DevOps jest doskonałym rozwiązaniem dla każdej organizacji, która musi zwiększyć przepływ pracy technicznej przy zachowaniu odpowiedniej jakości i niezawodności. Pozwala też na uzyskanie trwałości projektów i wzorową współpracę programistów z zespołem operacyjnym. Wiele organizacji decyduje się na wdrożenie praktyk DevOps. Pomyślne przeprowadzenie tego procesu wymaga przygotowań, w ich ramach zaś kluczowe znaczenie ma wybór odpowiednich do potrzeb wzorców i narzędzi.

To drugie, zaktualizowane i uzupełnione wydanie książki poświęconej wdrażaniu najlepszych praktyk DevOps przy użyciu nowoczesnych narzędzi. Przedstawiono w niej informacje o kulturze DevOps, opisano różne narzędzia i techniki stosowane do jej wdrażania, takie jak IaC, potoki Git i CI/CD, a także automatyzację testów i analizę kodu. Sporo miejsca poświęcono konteneryzacji aplikacji za pomocą Dockera i platformy Kubernetes. Znajdziemy tutaj również kwestię skracania przestojów podczas wdrażania oprogramowania i omówienie możliwości stosowania praktyk DevOps w projektach open source. Warto zwrócić uwagę na ostatni rozdział, w którym pokazano zasady wdrażania niektórych praktyk DevOps w całym cyklu życia projektów.

Najciekawsze zagadnienia:

- infrastruktura jako kod (IaC)
- udostępnianie i konfigurowanie infrastruktury chmurowej
- tworzenie lokalnego środowiska programistycznego i konteneryzowanie aplikacji
- zastosowanie DevSecOps do testowania zgodności i zabezpieczania infrastruktury
- potoki DevOps CI/CD i zielononiebieskie praktyki wdrażania
- praktyki DevOps dla projektów open source

Mikael Krief jest inżynierem DevOps, autorem książek technicznych i blogerem. Angażuje się w wiele różnych projektów, często występuje na prestiżowych konferencjach. Specjalizuje się w stosowaniu Terraform. Od lat rokrocznie otrzymuje tytuł Microsoft MVP, a od 2020 roku jest wybierany na ambasadora HashiCorp.

Helion	KOD KORZYŚCI Sięgnij po więcej!	
 helion.pl	ISBN 978-83-8322-198-4	
 HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	 9 788383 221984	
Cena: 109,00 zł		

Packt