

Spis treści

O autorze	iii
O recenzencie	iii
 Przedmowa	 1
 Rozdział 1: Poznajemy architekturę Kubernetes	 7
Czym jest Kubernetes?	8
Czym Kubernetes nie jest	8
Istota orkiestrowania kontenerów	9
Koncepcje Kubernetes	12
Klasy	12
Węzły	12
Master	14
Pody	14
Etykiety	15
Adnotacje	15
Selektory etykiet	16
Usługi	16
Woluminy	17
Kontrolery replikacji i zestawy replik	17
StatefulSet	18
Sekrety	18
Nazwy	19
Przestrzenie nazw	19
Głębsze zanurzenie w architekturę Kubernetes	19
Wzorce projektowe systemów rozproszonych	20
API Kubernetes	22
Komponenty Kubernetes	26
Mechanizmy wykonawcze w Kubernetes	30
Container Runtime Interface (CRI)	31
Docker	33
rkt	34

CRI-O.....	35
Kontenery Hyper.....	35
Ciągła integracja i wdrażanie.....	36
Projektowanie potoku CI/CD dla Kubernetes.....	37
Podsumowanie	38
Rozdział 2: Tworzenie klastrów Kubernetes.....	39
Przegląd.....	39
Tworzenie jednowęzłowego klastra za pomocą Minikube.....	40
Poznajemy kubectl.....	40
Krótkie wprowadzenie do Minikube.....	41
Przygotowanie.....	41
W systemie Windows.....	41
W systemie macOS.....	42
Tworzenie klastra	43
Rozwiązywanie problemów	44
Sprawdzanie klastra.....	45
Wykonywanie pracy.....	46
Badanie klastra za pomocą tablicy kontrolnej.....	48
Tworzenie wielowęzłowego klastra przy użyciu KinD	49
Krótkie wprowadzenie do KinD	49
Instalowanie KinD.....	50
Tworzenie klastra w KinD.....	50
Wykonywanie pracy w KinD	53
Uzyskiwanie dostępu do usług Kubernetes lokalnie poprzez proxy.....	53
Tworzenie wielowęzłowego klastra przy użyciu k3d	55
Krótkie wprowadzenie do k3s i k3d	55
Instalowanie k3d.....	56
Tworzenie klastra za pomocą k3d	56
Porównanie Minikube, KinD i k3d	59
Tworzenie klastrów w chmurze (GCP, AWS, Azure)	59
Interfejs cloud-provider	60
GCP.....	60
AWS.....	61
Azure	63
Inni dostawcy chmurowi	64
Tworzenie fizycznego klastra od podstaw	66
Przypadki użycia fizycznych maszyn.....	66

Kiedy należy rozważyć utworzenie fizycznego klastra?	66
Istota procesu	67
Używanie infrastruktury wirtualnej chmury prywatnej	67
Budowanie własnego klastra przy użyciu Kubespray	68
Budowanie klastra przy użyciu KRIB	68
Budowanie klastra przy użyciu RKE	69
Bootkube	69
Podsumowanie	69
Źródła	70

Rozdział 3: Wysoka dostępność i niezawodność.....71

Koncepcje wysokiej dostępności	72
Nadmiarowość	72
Wymiana na gorąco	72
Wybór lidera	73
Inteligentne równoważenie obciążeń	73
Idempotencja	73
Samonaprawy	74
Najlepsze praktyki wysokiej dostępności	74
Tworzenie klastrów wysokiej dostępności	75
Zapewnianie niezawodności węzłów	76
Ochrona stanu klastra	77
Ochrona danych	81
Uruchamianie nadmiarowych serwerów API	82
Realizowanie wyboru lidera w Kubernetes	82
Zapewnianie wysokiej dostępności środowiska przejściowego	83
Testowanie wysokiej dostępności	84
Planowanie wysokiej dostępności, skalowalności i pojemności	86
Instalowanie mechanizmu Cluster Autoscaler	87
Automatyczne skalowanie podów w pionie	88
Aktualizacje klastrów na żywo	89
Aktualizacje kroczące	90
Wdrożenia blue-green	93
Wdrożenia typu canary	94
Zarządzanie zmianami w kontraktach danych	95
Migrowanie danych	96
Wycofywanie przestarzałych API	96
Wydajność, koszty i kompromisy projektowe wielkich klastrów	97

Wymagania dostępności	98
Najlepsze starania	98
Okna konserwacji	99
Szybkie przywracanie	99
Zero przestojów	100
Inżynieria niezawodności lokacji	102
Wydajność i spójność danych	103
Podsumowanie	103
Źródła	104
 Rozdział 4: Zabezpieczanie Kubernetes	 105
Istota wyzwań zabezpieczeń w Kubernetes	106
Wyzwania węzłów	106
Wyzwania sieciowe	107
Wyzwania dotyczące obrazów	109
Wyzwania dotyczące konfiguracji i wdrażania	111
Wyzwania dotyczące podów i kontenerów	111
Wyzwania organizacyjne, kulturowe i procesowe	112
Wzmacnianie Kubernetes	114
Istota kont usługowych w Kubernetes	114
Uzyskiwanie dostępu do serwera API	116
Zabezpieczanie podów	123
Zarządzanie zasadami sieciowymi	130
Używanie sekretów	133
Klasy o wielu dzierżawcach	137
Przypadki użycia klastrów o wielu dzierżawcach	137
Wykorzystanie przestrzeni nazw dla bezpiecznego rozwiązywania wielu dzierżawców	138
Unikanie pułapek dotyczących przestrzeni nazw	139
Podsumowanie	140
Źródła	140
 Rozdział 5: Praktyczne używanie zasobów Kubernetes	 141
Projektowanie platformy Hue	141
Definiowanie zakresu Hue	142
Planowanie przepływów pracy	147
Używanie Kubernetes do budowania platformy Hue	149
Efektywne używanie kubectl	149
Pliki konfiguracji zasobów kubectl	150

Wdrażanie długo działających mikrouslug w podach	152
Separowanie usług wewnętrznych i zewnętrznych	157
Wdrażanie wewnętrznej usługi	158
Tworzenie usługi hue-reminders	159
Ekspozowanie usługi na zewnątrz	161
Zaawansowane rozmieszczanie	163
Selektor węzłów	163
Skazy i tolerancje	164
Koligacje i antykoligacje węzła	166
Koligacja i antykoligacja podu	166
Używanie przestrzeni nazw do ograniczania dostępu	167
Wykorzystanie kustomize do hierarchizowania struktur klastra	169
Podstawy kustomize	170
Konfigurowanie struktury katalogów	170
Aplikowanie dostosowań kustomize	172
Uruchamianie zadań	175
Równoległe uruchamianie zadań	176
Sprzątanie ukończonych zadań	177
Planowanie zadań cron	178
Mieszanie nieklastrowych komponentów	179
Komponenty poza siecią klastra	180
Komponenty wewnątrz sieci klastra	180
Zarządzanie platformą Hue przy użyciu Kubernetes	180
Używanie sond gotowości do zarządzania zależnościami	182
Stosowanie kontenerów inicjujących w celu uporządkowanego podnoszenia podów ...	183
Gotowość podu i bramki gotowości	183
Współużytkowanie przy użyciu podów DaemonSet	184
Ewolucja platformy Hue z pomocą Kubernetes	186
Wykorzystanie Hue w przedsiębiorstwie	186
Postęp naukowy w Hue	186
Kształcenie dzieci	186
Podsumowanie	187
Źródła	187
Rozdział 6: Zarządzanie magazynem	189
Przegląd trwałych woluminów	190
Woluminy	190
Wyposażanie trwałych woluminów	196

Tworzenie trwałych woluminów	197
Tworzenie żądań trwałych woluminów	200
Montowanie żądań jako woluminów	203
Surowe woluminy blokowe	204
Klasy magazynowe	206
Pełna demonstracja stosowania trwałych woluminów	207
Typy woluminów magazynów chmur publicznych – GCE, AWS i Azure	213
Amazon EBS	213
Amazon EFS	214
Trwałe dyski GCE	216
Dyski danych Azure	217
Azure Files	218
Woluminy GlusterFS oraz Ceph w Kubernetes	219
Stosowanie GlusterFS	219
Używanie Ceph	222
Flocker jako klastrowy kontenerowy menedżer woluminów danych	225
Integrowanie magazynów klasy przedsiębiorstwa z Kubernetes	227
Rook – nowy gracz na boisku	228
Rzutowanie woluminów	229
Korzystanie z wtyczek woluminów out-of-tree przy użyciu FlexVolume	230
Container Storage Interface	230
Migawki i klonowanie woluminów	232
Podsumowanie	234
 Rozdział 7: Uruchamianie aplikacji stanowych w Kubernetes	 235
Aplikacje stanowe i bezstanowe w środowisku Kubernetes	235
Wspólne zmienne środowiskowe kontra rekordy DNS dla odkrywania	237
Uruchamianie klastra Cassandra w Kubernetes	243
Podsumowanie	260
 Rozdział 8: Instalowanie i aktualizowanie aplikacji	 261
Automatyczne skalowanie podów w poziomie	262
Deklarowanie HPA	263
Niestandardowe miary	265
Automatyczne skalowanie przy użyciu kubectl	266
Wykonywanie aktualizacji kroczących przy użyciu autoskalowania	269
Obsługiwanie deficytowych zasobów za pomocą limitów i przydziałów	271
Włączanie przydziałów zasobów	272

Typy przydziałów zasobów	272
Zakresy przydziałów	275
Przydziały zasobów i klasy pierwszeństwa	276
Żądania i limity	276
Posługiwanie się przydziałami	276
Wybieranie i zarządzanie pojemnością klastra	282
Wybieranie typów węzłów	282
Wybieranie rozwiązania magazynowego	283
Kompromis pomiędzy kosztami a czasem odpowiedzi	283
Efektywne używanie wielu konfiguracji węzłów	284
Czerpanie korzyści z elastycznych zasobów chmurowych	285
Uwzględnianie rozwiązań natywnych dla kontenerów	286
Przesuwanie granic wydajności w Kubernetes	288
Podnoszenie wydajności i skalowalności Kubernetes	288
Mierzenie wydajności i skalowalności Kubernetes	291
Testowanie Kubernetes w wielkiej skali	294
Podsumowanie	296
Rozdział 9: Pakowanie aplikacji	297
Czym jest Helm	297
Umotywowanie Helm	298
Architektura Helm 2	298
Komponenty Helm 2	298
Helm 3	299
Używanie Helm	300
Instalowanie Helm	300
Wyszukiwanie schematów	301
Instalowanie pakietów	304
Posługiwanie się repozytoriami	313
Zarządzanie schematami przy użyciu Helm	314
Tworzenie własnych schematów	315
Plik Chart.yaml	316
Pliki metadanych schematu	317
Zarządzanie zależnościami schematu	317
Używanie szablonów i wartości	320
Podsumowanie	327

Rozdział 10: Poznanie zaawansowanych funkcji sieciowych	329
Model sieciowy Kubernetes	330
Komunikacja wewnątrz podu (między kontenerami)	330
Komunikacja między podami	330
Komunikacja pod-usługa	331
Dostęp z zewnątrz	331
Sieć Kubernetes a sieć Dockera	332
Wyszukiwanie i odkrywanie	334
Wtyczki sieciowe Kubernetes	336
Rozwiązania sieciowe Kubernetes	344
Mostkowanie w klastrach fizycznych	344
Contiv	345
Open vSwitch	345
Nuage Networks VCS	347
Flannel	347
Calico	348
Romana	349
Weave Net	350
Efektywne używanie zasad sieciowych	351
Istota projektu zasad sieciowych Kubernetes	351
Zasady sieciowe i wtyczki CNI	351
Konfigurowanie zasad sieciowych	352
Implementowanie zasad sieciowych	352
Opcje równoważenia obciążeń	353
Zewnętrzny mechanizm równoważący	354
Równoważenie obciążenia dla usługi	357
Ingress	358
Pisanie własnej wtyczki CNI	363
Pierwsze podejście – wtyczka loopback	363
Podsumowanie	372
 Rozdział 11: Uruchamianie Kubernetes w wielu chmurach oraz federacja klastrów	 375
Historia federacji klastrów w Kubernetes	376
Czym jest federacja klastrów	376
Ważne przypadki użycia dla federacji klastrów	378
Podstawy federacji Kubernetes	380
Warstwa sterowania KubeFed	382

Trudniejsze części	383
Zarządzanie federacją klastrów Kubernetes	388
Instalowanie kubefedctl	388
Tworzenie klastrów	389
Konfigurowanie klastra Host	390
Rejestrowanie klastrów w federacji	391
Posługiwanie się typami federacyjnego API	392
Federowanie zasobów	393
Używanie pola overrides	395
Używanie pola placement do kontrolowania federacji	396
Debugowanie błędów propagacji	397
Stosowanie zachowań wyższego rzędu	397
Wprowadzenie do projektu Gardener	402
Terminologia projektu Gardener	402
Poznajemy model koncepcyjny rozwiązania Gardener	403
Poznajemy architekturę Gardenera	404
Zarządzanie stanem klastra	404
Rozszerzanie Gardener	406
Pierścień Gardener	411
Podsumowanie	411
 Rozdział 12: Przetwarzanie bezserwerowe w Kubernetes	 413
Istota bezserwerowego przetwarzania	413
Uruchamianie długo działających usług w infrastrukturze „bezserwerowej”	414
Uruchamianie FaaS w infrastrukturze „bezserwerowej”	415
Bezserwerowa platforma Kubernetes w chmurze	416
Nie zapominajmy o autoskalowaniu klastra	416
Azure AKS oraz Azure Container Instances	416
AWS: EKS i Fargate	418
Google Cloud Run	419
Knative	420
Knative Serving	421
Knative Eventing	427
Próbna jazda z Knative	431
Frameworki FaaS w Kubernetes	435
Fission	435
Kubeless	440
Knative oraz riff	445
Podsumowanie	448

Rozdział 13: Monitorowanie klastrów Kubernetes	449
Obserwowalność	450
Rejestrowanie	450
Metryki	451
Śledzenie rozproszone	452
Raportowanie błędów aplikacji	453
Tablice kontrolne i wizualizacje	453
Alarmowanie	453
Rejestrowanie dzienników	454
Dzienniki kontenerów	454
Dzienniki komponentów Kubernetes	455
Scentralizowane rejestrowanie	456
Wykorzystanie Fluentd do gromadzenia dzienników	459
Gromadzenie metryk w Kubernetes	460
Monitorowanie przy użyciu serwera metryk	461
Przeglądanie klastra przy użyciu tablicy kontrolnej Kubernetes	463
Powstanie Prometheus	464
Rozproszone śledzenie przy użyciu Jaeger	474
Czym jest OpenTracing?	475
Przedstawiamy Jaeger	476
Instalowanie Jaegera	478
Rozwiązywanie problemów	481
Korzystanie ze środowisk pośrednich	481
Wykrywanie problemów na poziomie węzłów	482
Tablice kontrolne kontra alerty	483
Dzienniki kontra metryki kontra raporty błędów	484
Wykrywanie zakłóceń wydajności i źródłowych przyczyn za pomocą śledzenia rozproszonego	485
Podsumowanie	485
Rozdział 14: Korzystanie z Service Mesh	487
Czym jest Service Mesh?	487
Warstwa sterowania i warstwa danych	491
Wybieranie Service Mesh	491
Envoy	491
Linkerd 2	491
Kuma	492
AWS App Mesh	492

Maesh.....	492
Istio.....	492
Dołączanie Istio do klastra Kubernetes.....	493
Architektura Istio.....	493
Przygotowywanie klastra minikube dla Istio.....	496
Instalowanie Istio.....	497
Instalowanie Bookinfo.....	499
Zarządzanie ruchem.....	502
Zabezpieczenia.....	505
Zasady.....	511
Monitorowanie i obserwowalność.....	514
Podsumowanie.....	525
 Rozdział 15: Rozszerzanie Kubernetes.....	 527
Posługiwanie się API Kubernetes.....	527
Istota OpenAPI.....	528
Konfigurowanie proxy.....	528
Bezpośrednie badanie API Kubernetes.....	529
Tworzenie podu przy użyciu API Kubernetes.....	532
Uzyskiwanie dostępu do API Kubernetes poprzez klienta w Pythonie.....	533
Rozszerzanie API Kubernetes.....	540
Punkty i wzorce rozszerzania Kubernetes.....	540
Wprowadzenie do zasobów niestandardowych.....	545
Opracowywanie definicji zasobów niestandardowych.....	545
Integrowanie niestandardowych zasobów.....	547
Agregowanie serwera API.....	551
Korzystanie z wykazu usług.....	552
Tworzenie wtyczek Kubernetes.....	554
Pisanie niestandardowego schedulera.....	554
Tworzenie wtyczek dla kubectl.....	561
Pułapki związane z wtyczkami kubectl.....	564
Stosowanie webhooków kontroli dostępu.....	565
Używanie webhooka uwierzytelniania.....	566
Używanie webhooka autoryzacji.....	568
Używanie webhooka kontroli wejścia.....	570
Dostarczanie niestandardowych metryk dla autoskalowania podów.....	572
Rozszerzanie Kubernetes przy użyciu niestandardowego magazynu.....	573
Podsumowanie.....	574

Rozdział 16: Przyszłość Kubernetes	577
Dynamika Kubernetes	578
Ważność CNCF	578
Osprzęt.....	580
Powstanie zarządzanych platform Kubernetes	581
Platformy Kubernetes w chmurach publicznych.....	581
Instalacje fizyczne, chmury prywatne i KubeEdge	581
Kubernetes jako Platform as a Service (PaaS).....	582
Nowe trendy	582
Zabezpieczenia	582
Sieci.....	583
Niestandardowy sprzęt i urządzenia.....	584
Service Mesh	584
Przetwarzanie bezserwerowe	585
Kubernetes dla rozwiązań brzegowych.....	585
Natywne CI/CD	586
Operatory	586
Podsumowanie	587
Źródła	587
Indeks	589