

Spis treści

Przedmowa	19
Wstęp	21
1. Rewolucja chmurowa	25
Tworzenie chmury	25
Czas kupowania	26
Infrastruktura jako usługa	27
Początki DevOps	27
Nikt nie rozumie DevOps	28
Przewaga biznesowa	29
Infrastruktura w postaci kodu	30
Wspólna nauka	30
Nadejście kontenerów	31
Stan aktualny	31
Myślenie pudełkowe	31
Umieszczanie oprogramowania w kontenerach	32
Aplikacje Plug and Play	33
Uruchomienie orkiestratora	33
Kubernetes	34
Od Borga do Kubernetes	34
Co sprawia, że Kubernetes jest tak cenny?	35
Czy Kubernetes zniknie?	36
Kubernetes nie załatwia wszystkiego	37
Model Cloud Native	38
Przyszłość operacji	39
Rozproszone DevOps	40
Niektóre rzeczy pozostaną scentralizowane	40

Produktywni programiści	40
Jesteś przyszłością	41
Podsumowanie	41

2. Pierwsze kroki z Kubernetes 43

Uruchamianie pierwszego kontenera	43
Instalowanie Docker Desktop	43
Co to jest Docker?	44
Uruchamianie obrazu kontenera	44
Aplikacja demonstracyjna	45
Oglądamy kod źródłowy	45
Wprowadzenie do języka Go	46
Jak działa aplikacja demonstracyjna?	46
Budowanie kontenera	46
Opis plików Dockerfile	47
Minimalne obrazy kontenerów	47
Uruchamianie skompilowanego obrazu Docker	48
Nazywanie obrazów	48
Przekierowanie portów (ang. port forwarding)	49
Rejestry kontenerowe	49
Uwierzytelnianie w rejestrze	49
Przydzielanie nazwy i dodawanie obrazu	50
Uruchamianie obrazu	50
Cześć, Kubernetes	50
Uruchamianie aplikacji demonstracyjnej	50
Jeśli kontener się nie uruchamia	51
Minikube	52
Podsumowanie	52

3. Opis Kubernetes 53

Architektura klastrowa	53
Warstwa sterowania	54
Elementy węzła	54
System wysokiej niezawodności (ang. high availability)	55
Koszty samodzielnego hostingu Kubernetes	56
To więcej pracy niż myślisz	57
Nie chodzi tylko o początkową konfigurację	58
Narzędzia nie wykonają za Ciebie całej pracy	58
Kubernetes jest trudny	58

Koszty administracyjne	59
Zacznij od usług zarządzanych	59
Zarządzane usługi Kubernetes	60
Google Kubernetes Engine (GKE)	60
Automatyczne skalowanie klastra	61
Usługa Amazon Elastic Container Service dla Kubernetes (EKS)	61
Usługa Azure Kubernetes Service (AKS)	61
OpenShift	62
Usługa IBM Cloud Kubernetes Service	62
Rozwiązania Kubernetes pod klucz	62
Containership Kubernetes Engine (CKE)	62
Instalatory Kubernetes	63
kops	63
Kubespray	63
TK8	63
Kubernetes The Hard Way	64
kubeadm	64
Tarmak	64
Rancher Kubernetes Engine (RKE)	64
Moduł Puppet dla Kubernetes	65
Kubeformation	65
Kup lub zbuduj: nasze rekomendacje	65
Uruchom mniej oprogramowania	65
Skorzystaj z zarządzanych usług Kubernetes, jeśli możesz	66
A co z uzależnieniem od jednego dostawcy?	66
Jeśli trzeba, użyj standardowych narzędzi do samodzielnego hostingu Kubernetes	67
Gdy Twoje wybory są ograniczone	67
Bare-metal i on-premise	67
Bezklastrowe usługi kontenerowe	68
Amazon Fargate	68
Azure Container Instances (ACI)	69
Podsumowanie	69
4. Praca z obiektami Kubernetes	71
Zasoby Deployment	71
Nadzór i planowanie	72
Restart kontenerów	72
Zapytania obiektów Deployment	72

Pody	73
ReplicaSet	74
Utrzymanie pożądanego stanu	74
Scheduler	75
Manifesty zasobów w formacie YAML	76
Zasoby są danymi	76
Manifesty obiektu Deployment	76
Polecenie kubectl apply	77
Serwis	77
Odpytywanie klastra za pomocą polecenia kubectl	80
Przenoszenie zasobów na wyższy poziom	80
Helm: menadżer pakietów Kubernetes	81
Instalacja Helm	81
Instalacja wykresu Helm	81
Wykresy, repozytoria i wydania	82
Wyświetlanie listy wydań Helm	82
Podsumowanie	83
5. Zarządzanie zasobami	85
Zrozumienie działania zasobów	85
Jednostki zasobów	86
Żądania zasobów	86
Limity zasobów	86
Utrzymuj małe kontenery	87
Zarządzanie cyklem życia kontenera	88
Sondy żywotności	88
Opóźnienie i częstotliwość sondy	89
Inne typy sond	89
Sondy gRPC	89
Sondy gotowości	90
Sondy gotowości na podstawie pliku	90
minReadySeconds	91
Budżety zakłóceń Poda	91
Korzystanie z przestrzeni nazw	92
Praca z przestrzeniami nazw	93
Jakich przestrzeni nazw powinieneś używać?	93
Adresy serwisów	94
Przydziały zasobów (ang. Resource Quotas)	94
Domyślne żądania zasobów i limity	96

Optymalizacja kosztów klastra	96
Optymalizacja obiektów Deployment	97
Optymalizacja Podów	97
Vertical Pod Autoscaler	98
Optymalizacja węzłów	98
Optymalizacja przestrzeni dyskowej	99
Czyszczenie nieużywanych zasobów	100
Sprawdzanie wolnej pojemności	102
Korzystanie z instancji zastrzeżonych	102
Korzystanie z instancji w trybie wyłączeniowym	103
Utrzymywanie równowagi obciążeń	105
Podsumowanie	106
6. Operacje na klastrach	109
Rozmiar i skalowanie klastra	109
Planowanie pojemności	109
Węzły i instancje	112
Skalowanie klastra	114
Sprawdzanie zgodności	116
Certyfikat CNCF	116
Testy zgodności z Sonobuoy	118
Walidacja i audyt	118
K8Guard	118
Copper	119
kube-bench	119
Dziennik kontroli Kubernetes (ang. Kubernetes audit log)	119
Testowanie chaosu	120
Tylko produkcja jest produkcją	120
chaoskube	121
kube-monkey	121
PowerfulSeal	122
Podsumowanie	122
7. Narzędzia Kubernetes	125
Znowu o kubectl	125
Alias powłoki	125
Używanie przełączników	126
Skracanie typów zasobów	126
Automatyczne uzupełnianie poleceń kubectl	126

Uzyskiwanie pomocy	127
Uzyskiwanie pomocy na temat zasobów Kubernetes	127
Bardziej szczegółowe wyniki	127
Praca z JSON Data i jq	128
Oglądanie obiektów	129
Opisywanie obiektów	129
Praca z zasobami	129
Imperatywne polecenia kubectl	130
Kiedy nie należy używać poleceń imperatywnych?	130
Generowanie manifestów zasobów	131
Eksportowanie zasobów	131
Śledzenie różnic w zasobach	132
Praca z kontenerami	132
Przeglądanie dzienników kontenera	132
Przylączanie do kontenera	134
Oglądanie zasobów Kubernetes za pomocą kubespy	134
Przekierowanie portu kontenera	134
Wykonywanie poleceń w kontenerach	135
Rozwiązywanie problemów w kontenerach	135
Korzystanie z poleceń BusyBox	136
Dodawanie BusyBox do kontenerów	137
Instalowanie programów w kontenerze	138
Debugowanie w czasie rzeczywistym za pomocą kubesquash	138
Konteksty i przestrzenie nazw	139
kubectx i kubens	140
kube-ps1	140
Powłoki i narzędzia Kubernetes	141
kube-shell	141
Click	141
kubed-sh	141
Stern	142
Budowanie własnych narzędzi Kubernetes	142
Podsumowanie	143

8. Uruchamianie kontenerów145

Kontenery i Pody	145
Co to jest kontener?	146
Co należy do kontenera?	147
Co należy do Poda?	147

Manifesty kontenera	148
Identyfikatory obrazu	149
Tag latest	149
Skróty kontenerów	150
Podstawowe tagi obrazu	150
Porty	151
Żądania i limity dotyczące zasobów	151
Polityka pobierania obrazu	151
Zmienne środowiskowe	152
Bezpieczeństwo kontenerów	152
Uruchamianie kontenerów jako użytkownik inny niż root	153
Blokowanie kontenerów z uprawnieniami root	153
Ustawianie systemu plików tylko do odczytu	154
Wyłączanie eskalacji uprawnień	154
Mechanizm właściwości	155
Konteksty bezpieczeństwa Poda	156
Polityka bezpieczeństwa Poda	156
Konta usług Poda	157
Woluminy	157
Woluminy emptyDir	158
Woluminy trwałe	159
Restart polityk	160
Uwierzytelnianie przy pobieraniu obrazu	160
Podsumowanie	160
9. Zarządzanie Podami	163
Etykiety	163
Co to są etykiety?	163
Selektory	164
Bardziej zaawansowane selektory	164
Inne zastosowania etykiet	165
Etykiety i adnotacje	166
Koligacje węzłów	167
Koligacje twarde	167
Koligacje miękkie	168
Koligacje Podów i antykoligacje	168
Trzymanie Podów razem	169
Trzymanie Podów oddzielnie	169

Antykoligacje miękkie	170
Kiedy korzystać z koligacji Podów?	170
Skazy i tolerancje	171
Kontrolery Podów	172
DaemonSet	172
StatefulSet	173
Kontroler Job	174
CronJob	175
Horizontal Pod Autoscaler	176
PodPreset	177
Operatory i niestandardowe definicje zasobów (CRD)	178
Zasoby Ingress	179
Reguły Ingress	180
Zarządzanie połączeniami TLS za pomocą Ingress	180
Kontroler Ingress	181
Istio	182
Envoy	182
Podsumowanie	183

10. Konfiguracja i obiekty Secret185

ConfigMap	185
Tworzenie ConfigMap	186
Ustawianie zmiennych środowiskowych z obiektu ConfigMap	186
Ustawianie środowiska za pomocą ConfigMap	188
Używanie zmiennych środowiskowych w argumentach poleceń	189
Tworzenie plików konfiguracji z ConfigMaps	190
Aktualizacja Podów po zmianie konfiguracji	191
Obiekty Secret aplikacji Kubernetes	192
Używanie obiektów Secret jako zmiennych środowiskowych	192
Zapisywanie obiektów Secret do plików	193
Odczyt obiektów Secret	194
Dostęp do obiektów Secret	195
Szyfrowanie w stanie spoczynku	195
Przechowywanie obiektów Secret	195
Strategie zarządzania obiektami Secret	195
Szyfrowanie Secret w systemach kontroli wersji	196
Zdalne przechowywanie Secret	197
Dedykowane narzędzie do zarządzania obiektami Secret	197
Rekomendacje	198

Szyfrowanie obiektów Secret za pomocą Sops	198
Przedstawiamy Sops	199
Szyfrowanie pliku za pomocą Sops	199
Korzystanie z zaplecza KMS	201
Podsumowanie	201
11. Bezpieczeństwo i kopia zapasowa	203
Kontrola dostępu i uprawnienia	203
Zarządzanie dostępem przez klaster	203
Kontrola dostępu oparta na rolach (RBAC)	204
Role	204
Wiązanie ról z użytkownikami	205
Jakich ról potrzebuję?	206
Ochrona dostępu do Cluster-Admin	206
Aplikacje i wdrażanie	206
Rozwiązywanie problemów z RBAC	207
Skanowanie bezpieczeństwa	208
Clair	208
Aqua	208
Anchore Engine	209
Kopie zapasowe	209
Czy muszę wykonać kopię zapasową?	209
Tworzenie kopii zapasowej etcd	210
Kopia zapasowa stanu zasobów	210
Tworzenie kopii zapasowej stanu klastra	210
Duże i małe katastrofy	211
Velero	211
Monitorowanie statusu klastra	214
kubectl	214
Wykorzystanie procesora i pamięci	216
Konsola dostawcy chmury	216
Pulpit Kubernetes (ang. Kubernetes Dashboard)	216
Weave Scope	218
kube-ops-view	218
node-problem-detector	218
Dalsza lektura	219
Podsumowanie	220

12. Wdrażanie aplikacji Kubernetes221

 Budowanie manifestów za pomocą wykresu Helm221

 Co znajduje się w wykresie narzędzia Helm?222

 Szablony Helm223

 Zmienne interpolacyjne223

 Wartości tekstowe w szablonach224

 Określanie zależności225

 Wdrażanie wykresów Helm225

 Ustawianie zmiennych225

 Określanie opcji podczas instalacji Helm226

 Aktualizowanie aplikacji za pomocą Helm226

 Powrót do poprzednich wersji227

 Tworzenie repozytorium wykresów Helm227

 Zarządzanie obiektami Secret wykresów Helm za pomocą Sops228

 Zarządzanie wieloma wykresami za pomocą Helmfile229

 Co znajduje się w pliku Helmfile?230

 Metadane wykresu231

 Stosowanie pliku Helmfile231

 Zaawansowane narzędzia do zarządzania manifestami232

 Tanka232

 kapitan233

 kustomize233

 kompose233

 Ansible234

 kubeval234

 Podsumowanie235

13. Proces tworzenia oprogramowania237

 Narzędzia programistyczne237

 Skaffold237

 Draft238

 Telepresence238

 Knative238

 Strategie wdrażania239

 Rolling Updates239

 Recreate240

 maxSurge i maxUnavailable240

 Wdrożenia niebiesko-zielone241

Wdrożenia rainbow	242
Wdrożenia kanarkowe	242
Obsługa migracji za pomocą Helm	242
Funkcja hook wykresu Helm	243
Obsługa nieudanych funkcji hook	243
Inne funkcje hook	244
Kolejność wykonywania funkcji hook	244
Podsumowanie	244
14. Ciągłe wdrażanie w Kubernetes	247
Co to jest ciągle wdrażanie?	247
Z którego narzędzia CD powinienem skorzystać?	248
Jenkins	248
Drone	248
Google Cloud Build	248
Concourse	249
Spinnaker	249
GitLab CI	249
Codefresh	249
Azure Pipelines	249
Komponenty CD	250
Docker Hub	250
Gitkube	250
Flux	250
Keel	250
Potok CD z wykorzystaniem Google Cloud Build	250
Konfigurowanie Google Cloud i GKE	251
Kopiowanie repozytorium demo	251
Wprowadzenie do Cloud Build	251
Budowanie kontenera testowego	252
Uruchamianie testów	252
Budowanie kontenera aplikacji	253
Walidacja manifestów Kubernetes	253
Publikowanie obrazu	253
Tagi Git SHA	254
Tworzenie pierwszego triggera kompilacji	254
Testowanie triggera	254
Wdrożenie z potoku CD	256

Tworzenie triggera wdrażania	258
Optymalizacja potoku kompilacji	258
Dostosowanie przykładowego potoku	259
Podsumowanie	259
15. Obserwowalność i monitorowanie	261
Co to jest obserwowalność?	261
Co to jest monitorowanie?	261
Monitorowanie typu czarna skrzynka	261
Co oznacza określenie „działa”?	263
Zapisywanie logów	264
Przedstawiamy metryki	265
Śledzenie	267
Obserwowalność	267
Potok obserwowalności	268
Monitorowanie w Kubernetes	269
Zewnętrzny monitoring typu czarna skrzynka	269
Wewnętrzna kontrola aplikacji	271
Podsumowanie	272
16. Metryki w Kubernetes	275
Czym są metryki?	275
Seria danych w czasie	275
Liczniki i mierniki	276
Co mogą powiedzieć metryki?	277
Wybór dobrych metryk	277
Usługi: wzorzec RED	278
Zasoby: wzorzec USE	279
Metryki biznesowe	279
Metryki Kubernetes	280
Analizowanie metryk	283
Dlaczego nie korzystać z wartości średniej?	284
Średnie arytmetyczne, mediany i wartości odstające	284
Odkrywanie percentyli	284
Stosowanie percentyli do danych metryk	285
Zwykle chcemy zobaczyć to, co najgorsze	287
Co zamiast percentylów?	287

Tworzenie wykresów metryk w pulpicie	288
Użyj standardowego układu graficznego dla wszystkich serwisów	288
Zbuduj radiator informacji za pomocą pulpitu	289
Umieszczanie na pulpicie rzeczy, które ulegają awarii	291
Alarmy na podstawie metryk	291
Jakie są problemy związane z alarmami?	291
Bezbolesna reakcja na żądanie	292
Pilne, ważne i przydatne alarmy	293
Śledź swoje alarmy, powiadomienia poza godzinami pracy i pobudki	294
Narzędzia i usługi metryczne	294
Prometheus	294
Google Stackdriver	296
AWS Cloudwatch	297
Azure Monitor	297
Datadog	297
New Relic	298
Podsumowanie	299
Postowie	301