O'REILLY®

Kubernetes для DevOps

развертывание, запуск и масштабирование в облаке

Джон Арундел
Джастин Домингус

Краткое содержание

Предисловие 21
Введение 22
Глава 1. Революция в облаке 27
Глава 2. Первые шаги с Kubernetes 51
Глава 3. Размещение Kubernetes 64
Глава 4. Работа с объектами Kubernetes 89
Глава 5. Управление ресурсами 107
Глава 6. Работа с кластерами 137
Глава 7. Продвинутые инструменты для работы с Kubernetes 157
Глава 8. Работа с контейнерами 183
Глава 9. Управление pod-оболочками 205
Глава 10. Конфигурация и объекты Secret 234
Глава 11. Безопасность и резервное копирование 257
Глава 12. Развертывание приложений Kubernetes 280
Глава 13. Процесс разработки 300
Глава 14. Непрерывное развертывание в Kubernetes 311
Глава 15. Наблюдаемость и мониторинг 328
Глава 16. Показатели в Kubernetes 346
Заключение 379
Об авторах 381
Об обложке 382

Оглавление

Предисловие 21

Введение 22
- Чему вы научитесь 22
- Для кого предназначена книга 23
- На какие вопросы отвечает книга 23
- Условные обозначения 24
- Использование примеров кода 25
- Благодарности 26
- От издательства 26

Глава 1. Революция в облаке 27
- Создание облака 28
  - Покупаем время 28
  - Инфраструктура как услуга 29
- Расцвет DevOps 30
  - Никто не понимает DevOps 31
  - Бизнес-преимущество 32
  - Инфраструктура как код 33
  - Учимся вместе 34
- Пришествие контейнеров 34
  - Последние веяния 34
  - «Коробочное» мышление 35
  - Размещение программного обеспечения в контейнерах 36
  - Динамически подключаемые приложения 38

Дирижирование оркестром контейнеров ... 38
Kubernetes ... 39
От Borg до Kubernetes ... 39
Что делает платформу Kubernetes такой ценной ... 40
Не исчезнет ли Kubernetes? ... 42
Kubernetes не решает все проблемы ... 42
Облачная ориентированность ... 44
Будущее системного администрирования ... 46
Распределенный DevOps ... 47
Некоторые элементы останутся централизованными ... 47
Планирование продуктивности разработчиков ... 48
Вы — будущее ... 49
Резюме ... 49

Глава 2. Первые шаги с Kubernetes ... 51
Запускаем наш первый контейнер ... 51
Установка Docker Desktop ... 52
Что такое Docker ... 52
Запуск образа контейнера ... 53
Демонстрационное приложение ... 53
Рассмотрение исходного кода ... 54
Введение в Go ... 54
Как работает демонстрационное приложение ... 55
Построение контейнера ... 55
Что собой представляет Dockerfile ... 56
Минимальные образы контейнеров ... 56
Выполнение команды docker image build ... 57
Выбор имен для ваших образов ... 57
Перенаправление портов ... 58
Реестры контейнеров ... 59
Аутентификация в реестре ... 59
Выбор имени для вашего образа и загрузка его в реестр ... 60
Запуск вашего образа ... 60

Здравствуй, Kubernetes ... 60
Запуск демонстрационного приложения ... 61
Если контейнер не запускается ... 62
Minikube ... 62
Резюме ... 63

Глава 3. Размещение Kubernetes ... 64
Архитектура кластера ... 65
Управляющий уровень ... 65
Компоненты узла ... 66
Высокая доступность ... 67
Стоимость самостоятельного размещения Kubernetes ... 69
Это сложнее, чем вам кажется ... 69
Начальная настройка — это далеко не все ... 70
Инструменты не сделают за вас всю работу ... 71
Kubernetes — это сложно ... 72
Накладные расходы на администрирование ... 72
Начните с управляемых сервисов ... 72
Управляемые сервисы Kubernetes ... 74
Google Kubernetes Engine (GKE) ... 74
Amazon Elastic Container Service для Kubernetes ... 75
Azure Kubernetes Service (AKS) ... 76
OpenShift ... 76
IBM Cloud Kubernetes Service ... 77
Heptio Kubernetes Subscription (HKS) ... 77
Решения для Kubernetes под ключ ... 77
Stackpoint ... 78
Containership Kubernetes Engine (CKE) ... 78
Установщики Kubernetes ... 78
kops ... 78
Kubespray ... 79
TK8 ... 79
Kubernetes: трудный путь ... 80

kubeadm ... 80
Tarmak ... 80
Rancher Kubernetes Engine (RKE) ... 81
Модуль Puppet для Kubernetes ... 81
Kubeformation ... 81
Покупать или строить: наши рекомендации ... 81
Не используйте слишком много ПО ... 82
По возможности используйте Kubernetes в виде управляемого сервиса ... 82
Но что насчет привязки к поставщику? ... 83
При необходимости используйте стандартные инструменты Kubernetes для самостоятельного размещения ... 84
Если ваш выбор ограничен ... 84
Локально размещенные физические серверы ... 84
Бескластерные контейнерные сервисы ... 85
Amazon Fargate ... 86
Azure Container Instances (ACI) ... 86
Резюме ... 87

Глава 4. Работа с объектами Kubernetes ... 89
Развертывания ... 89
Надзор и планирование ... 90
Перезапуск контейнеров ... 90
Обращение к развертываниям ... 91
Pod-оболочки ... 92
Объекты ReplicaSet ... 93
Поддержание желаемого состояния ... 94
Планировщик Kubernetes ... 95
Манифесты ресурсов в формате YAML ... 95
Ресурсы являются данными ... 96
Манифесты развертываний ... 96
Использование команды kubectl apply ... 97
Ресурсы типа «сервис» ... 97
Обращение к кластеру с помощью kubectl ... 100
Выводим ресурсы на новый уровень ... 101

Helm: диспетчер пакетов для Kubernetes ... 102
Установка Helm ... 102
Установка чарта Helm ... 103
Чарты, репозитории и выпуски ... 104
Вывод списка выпусков Helm ... 104
Резюме ... 105

Глава 5. Управление ресурсами ... 107
Понимание ресурсов ... 107
Единицы измерения ресурсов ... 108
Запросы ресурсов ... 108
Лимиты на ресурсы ... 109
Делайте контейнеры небольшими ... 110
Управление жизненным циклом контейнера ... 111
Проверки работоспособности ... 111
Задержка и частота проверки ... 112
Другие типы проверок ... 112
Проверки gRPC ... 113
Проверки готовности ... 113
Проверки готовности на основе файла ... 114
Поле minReadySeconds ... 115
Ресурс PodDisruptionBudget ... 115
Использование пространств имен ... 117
Работа с пространствами имен ... 117
Какое пространство имен следует использовать ... 118
Адреса сервисов ... 119
Квоты на ресурсы ... 119
Запросы и лимиты на ресурсы по умолчанию ... 121
Оптимизация стоимости кластера ... 122
Оптимизация развертываний ... 122
Оптимизация pod-оболочек ... 123
Vertical Pod Autoscaler ... 124
Оптимизация узлов ... 124

Оптимизация хранилища ... 126
Избавление от неиспользуемых ресурсов ... 127
Проверка резервной мощности ... 129
Использование зарезервированных серверов ... 129
Использование прерываемых (spot) серверов ... 130
Балансировка вашей рабочей нагрузки ... 133
Резюме ... 134

Глава 6. Работа с кластерами ... 137
Масштабирование и изменение размеров кластера ... 137
Планирование мощности ... 138
Узлы и серверы ... 141
Масштабирование кластера ... 144
Проверка на соответствие ... 146
Сертификация CNCF ... 147
Проверка на соответствие с помощью Sonobuoy ... 148
Проверка конфигурации и аудит ... 149
K8Guard ... 150
Copper ... 150
kube-bench ... 151
Ведение журнала аудита для Kubernetes ... 151
Хаотическое тестирование ... 152
Промышленные условия только в промышленной среде ... 152
chaoskube ... 153
kube-monkey ... 154
PowerfulSeal ... 154
Резюме ... 155

Глава 7. Продвинутые инструменты для работы с Kubernetes ... 157
Осваиваем kubectl ... 157
Псевдонимы командной оболочки ... 157
Использование коротких флагов ... 158
Сокращение названий типов ресурсов ... 158
Автодополнение команд kubectl ... 159

Справка ... 159
Справка по ресурсам Kubernetes ... 160
Отображение более подробного вывода ... 160
Работа с jq и данными в формате JSON ... 161
Наблюдение за объектами ... 162
Описание объектов ... 162
Работа с ресурсами ... 163
Императивные команды kubectl ... 163
Когда не следует использовать императивные команды ... 164
Генерация манифестов ресурсов ... 165
Экспорт ресурсов ... 165
Сравнение ресурсов ... 166
Работа с контейнерами ... 166
Просмотр журнальных записей контейнера ... 167
Подключение к контейнеру ... 168
Наблюдение за ресурсами Kubernetes с помощью kubespy ... 168
Перенаправление порта контейнера ... 169
Выполнение команд внутри контейнеров ... 169
Запуск контейнеров с целью отладки ... 170
Использование команд BusyBox ... 171
Добавление BusyBox в ваш контейнер ... 172
Установка программ в контейнер ... 173
Отладка в режиме реального времени с помощью kubesquash ... 173
Контексты и пространства имен ... 174
kubectx и kubens ... 176
kube-ps1 ... 177
Командные оболочки и инструменты Kubernetes ... 177
kube-shell ... 177
Click ... 178
kubed-sh ... 178
Stern ... 178
Создание собственных инструментов для работы с Kubernetes ... 179
Резюме ... 180

Глава 8. Работа с контейнерами ... 183
Контейнеры и pod-оболочки ... 183
Что такое контейнер ... 184
Что должно находиться в контейнере ... 185
Что должно находиться в pod-оболочке ... 186
Манифесты контейнеров ... 187
Идентификаторы образов ... 188
Тег latest ... 189
Контрольные суммы контейнеров ... 190
Теги базового образа ... 190
Порты ... 191
Запросы и лимиты на ресурсы ... 191
Политика загрузки образов ... 191
Переменные среды ... 192
Безопасность контейнеров ... 192
Запуск контейнеров от имени обычного пользователя ... 193
Блокирование контейнеров с администраторскими привилегиями ... 194
Настройка файловой системы только для чтения ... 195
Отключение повышения привилегий ... 195
Мандаты ... 196
Контексты безопасности pod-оболочки ... 197
Политики безопасности pod-оболочки ... 198
Служебные учетные записи pod-оболочек ... 199
Тома ... 199
Тома emptyDir ... 200
Постоянные тома ... 201
Политики перезапуска ... 202
imagePullSecrets ... 202
Резюме ... 203

Глава 9. Управление pod-оболочками ... 205
Метки ... 205
Что такое метки ... 206
Селекторы ... 206

Более сложные селекторы 207
Дополнительные способы использования меток 208
Метки и аннотации 209
Принадлежность к узлам 210
Жесткая принадлежность 211
Мягкая принадлежность 211
Принадлежность и непринадлежность pod-оболочек 212
Размещение pod-оболочек вместе 213
Размещение pod-оболочек порознь 214
Мягкая непринадлежность 214
Когда использовать правила принадлежности pod-оболочек 215
Ограничения и допуски 215
Контроллеры pod-оболочек 217
Объекты DaemonSet 218
Объект StatefulSet 219
Запланированные задания 220
Задания Cronjob 222
Горизонтальное автомасштабирование pod-оболочек 222
PodPreset 224
Операторы и определение пользовательских ресурсов 225
Ресурсы Ingress 226
Правила Ingress 227
Терминация TLS с помощью Ingress 228
Контроллеры Ingress 229
Istio 230
Envoy 231
Резюме 231

Глава 10. Конфигурация и объекты Secret 234
Объекты ConfigMap 235
Создание ConfigMap 235
Задание переменных среды из ConfigMap 236
Установка всей среды из ConfigMap 238

Использование переменных среды в аргументах командной строки....239
Создание конфигурационных файлов из объектов ConfigMap....240
Обновление pod-оболочек при изменении конфигурации....243
Конфиденциальные данные в Kubernetes....243
Использование объектов Secret в качестве переменных среды....244
Запись объектов Secret в файлы....245
Чтение объектов Secret....245
Доступ к объектам Secret....247
Пассивное шифрование данных....247
Хранение конфиденциальных данных....248
Стратегии управления объектами Secret....248
Шифрование конфиденциальных данных в системе контроля версий....248
Удаленное хранение конфиденциальных данных....250
Использование специального инструмента для управления конфиденциальными данными....250
Рекомендации....251
Шифрование конфиденциальных данных с помощью Sops....252
Знакомство с Sops....252
Шифрование файла с помощью Sops....253
Использование внутреннего механизма KMS....255
Резюме....255

Глава 11. Безопасность и резервное копирование....257
Управление доступом и права доступа....257
Управление доступом в кластере....258
Введение в управление доступом на основе ролей....258
Понимание ролей....259
Привязка ролей к пользователям....260
Какие роли вам нужны....261
Обращение с ролью cluster-admin....261
Приложения и развертывание....262
Решение проблем с RBAC....262

Сканирование безопасности ... 263
Clair ... 263
Aqua ... 264
Anchore Engine ... 265
Резервное копирование ... 265
Нужно ли выполнять резервное копирование в Kubernetes ... 265
Резервное копирование etcd ... 266
Резервное копирование состояния ресурсов ... 267
Резервное копирование состояния кластера ... 267
Крупные и мелкие сбои ... 268
Velero ... 268
Мониторинг состояния кластера ... 271
kubectl ... 272
Загруженность процессора и памяти ... 274
Консоль облачного провайдера ... 274
Kubernetes Dashboard ... 275
Weave Scope ... 277
kube-ops-view ... 277
node-problem-detector ... 278
Дополнительный материал ... 278
Резюме ... 278

Глава 12. Развертывание приложений Kubernetes ... 280
Построение манифестов с помощью Helm ... 280
Что внутри у чарта Helm ... 281
Шаблоны Helm ... 282
Интерполяция переменных ... 283
Цитирование значений в шаблонах ... 284
Задание зависимостей ... 285
Развертывание чартов Helm ... 285
Задание переменных ... 285
Задание значений в выпуске Helm ... 286
Обновление приложения с помощью Helm ... 287
Откат к предыдущей версии ... 287

Создание репозитория с чартами Helm ... 288
Управление конфиденциальными данными чартов Helm с помощью Sops ... 289
Управление несколькими чартами с помощью Helmfile ... 291
Что такое Helmfile ... 291
Метаданные чарта ... 292
Применение Helmfile ... 293
Продвинутые инструменты управления манифестами ... 294
ksonnet ... 294
kapitan ... 296
kustomize ... 296
kompose ... 297
Ansible ... 297
kubeval ... 298
Резюме ... 298

Глава 13. Процесс разработки ... 300
Инструменты разработки ... 300
Skaffold ... 301
Draft ... 301
Telepresence ... 301
Knative ... 302
Стратегии развертывания ... 302
Плавающие обновления RollingUpdate ... 303
Стратегия Recreate ... 304
Параметры maxSurge и maxUnavailable ... 304
Сине-зеленые развертывания ... 305
Rainbow-развертывания ... 306
Канареечные развертывания ... 306
Выполнение миграции с помощью Helm ... 307
Хуки Helm ... 307
Обработка неудачных хуков ... 308
Другие хуки ... 308
Создание цепочки хуков ... 309
Резюме ... 309

Глава 14. Непрерывное развертывание в Kubernetes 311
Что такое непрерывное развертывание 311
Какие инструменты следует использовать для CD 312
Jenkins 313
Drone 313
Google Cloud Build 313
Concourse 314
Spinnaker 314
GitLab CI 314
Codefresh 314
Azure Pipelines 315
Компоненты непрерывного развертывания 315
Docker Hub 315
Gitkube 315
Flux 315
Keel 316
Процесс CD с использованием Cloud Build 316
Настройка Google Cloud и GKE 316
Создание копии репозитория demo 317
Знакомство с Cloud Build 317
Сборка контейнера с тестами 317
Выполнение тестов 318
Собираем контейнер приложения 319
Проверка манифестов Kubernetes 319
Публикация образа 320
Теги на основе Git SHA 320
Создание первого триггера сборки 320
Проверка триггера 322
Развертывание из конвейера CD 322
Создание триггера развертывания 325
Оптимизация процесса сборки 326
Адаптация демонстрационного конвейера 326
Резюме 326

Глава 15. Наблюдаемость и мониторинг 328
Что такое наблюдаемость 328
Что такое мониторинг 328
Мониторинг методом черного ящика 329
Что означает «работает» 330
Ведение журнала 332
Введение в показатели 334
Трассировка 336
Наблюдаемость 337
Процесс наблюдаемости 338
Мониторинг в Kubernetes 340
Внешние проверки методом черного ящика 340
Внутренние проверки работоспособности 342
Резюме 344

Глава 16. Показатели в Kubernetes 346
Что на самом деле представляют собой показатели 346
Хронологические данные 347
Счетчики и измерители 348
О чем нам могут поведать показатели 348
Выбор подходящих показателей 348
Сервисы: шаблон RED 349
Ресурсы: шаблон USE 350
Бизнес-показатели 351
Показатели Kubernetes 353
Анализ показателей 357
Что не так с простым средним значением 357
Средние значения, медианы и выбросы 358
Вычисление перцентилей 358
Применение перцентилей к показателям 359
Обычно нас интересуют наихудшие показатели 361
Не перцентилями едиными 361
Визуализация показателей с помощью информационных панелей 362
Использование стандартной компоновки для всех сервисов 363

Информационный излучатель на основе обобщенных панелей данных 364
Отслеживайте то, что может сломаться 366
Уведомления о показателях 366
Что не так с уведомлениями 367
Дежурство не должно быть пыткой 368
Уведомления неотложные, важные и требующие принятия мер 369
Отслеживайте свои уведомления и их последствия 370
Инструменты и сервисы для работы с показателями 370
Prometheus 371
Google Stackdriver 373
AWS Cloudwatch 374
Azure Monitor 374
Datadog 374
New Relic 376
Резюме 377

Заключение 379
Что дальше? 379
Добро пожаловать на борт 380

Об авторах 381

Об обложке 382