

# Оглавление

Об авторе.....	17
О рецензентах.....	18
Предисловие .....	19
Для кого предназначена книга .....	19
Темы, рассмотренные в книге.....	20
Как извлечь из книги максимальную пользу.....	21
Полноцветные изображения.....	21
Условные обозначения.....	21
<b>Глава 1. Архитектура Kubernetes.....</b>	<b>23</b>
Что такое Kubernetes .....	23
Чем Kubernetes не является .....	24
Оркестрация контейнеров .....	24
Контейнеры на физических и виртуальных устройствах.....	24
Преимущества контейнеров.....	25
Контейнеры в облаке .....	25
От мелких домашних животных к крупному рогатому скоту .....	26
Концепции, лежащие в основе Kubernetes.....	26
Кластер .....	28
Узел.....	28
Ведущий узел .....	28
Под .....	28
Метка.....	29
Аннотации .....	29
Селекторы меток.....	30
Контроллеры репликации и наборы реплик.....	30
Сервисы.....	31
Том .....	31

StatefulSet .....	32
Конфиденциальная информация .....	32
Имена .....	32
Пространства имен .....	33
Углубленное рассмотрение архитектуры Kubernetes .....	33
Шаблоны проектирования распределенных систем .....	33
API Kubernetes .....	35
Категории ресурсов .....	36
Ведущие компоненты Kubernetes .....	38
API-сервер .....	38
Etcд .....	38
Диспетчер контроллеров Kube .....	38
Диспетчер облачных контроллеров .....	39
kube-scheduler .....	40
DNS .....	40
Узловые компоненты .....	40
Прокси-сервер .....	40
Kubelet .....	41
Среды выполнения, совместимые с Kubernetes .....	41
Интерфейс среды выполнения контейнеров (CRI) .....	41
Docker .....	43
Rkt .....	44
Контейнеры Nureg .....	46
Непрерывная интеграция и разработка .....	46
Цепочка CI/CD .....	46
Проектирование цепочки CI/CD для Kubernetes .....	48
Резюме .....	48
<b>Глава 2. Создание кластеров Kubernetes .....</b>	<b>49</b>
Быстрое создание одноузлового кластера с помощью Minikube .....	49
Подготовка .....	50
В Windows .....	50
В macOS .....	50
Создание кластера .....	51
Отладка .....	53
Проверка кластера .....	54
Выполнение работы .....	54
Исследование кластера с помощью панели управления .....	55

Создание многоузлового кластера с помощью kubeadm.....	57
Чего следует ожидать .....	57
Подготовка к работе.....	57
Подготовка кластера виртуальных машин на основе vagrant.....	57
Установка необходимого программного обеспечения.....	58
Создание кластера .....	61
Настройка pod-сети.....	62
Добавление рабочих узлов.....	63
Создание кластеров в облаке (GCP, AWS и Azure).....	64
Интерфейс cloud-provider.....	64
Google Cloud Platform .....	65
Amazon Web Services .....	65
Azure .....	66
Alibaba Cloud .....	67
Создание аппаратного кластера с нуля .....	68
Сценарии использования «голого железа».....	68
Когда создание аппаратного кластера имеет смысл.....	68
Процесс создания кластера.....	69
Использование инфраструктуры частного виртуального облака.....	69
Резюме.....	70
<b>Глава 3. Мониторинг, журналирование и решение проблем .....</b>	<b>71</b>
Мониторинг Kubernetes с помощью Heapster .....	71
Установка Heapster .....	72
Хранилище InfluxDB.....	74
Структура хранилища .....	74
Визуализация с помощью Grafana.....	77
Анализ производительности с помощью панели управления.....	78
Представление верхнего уровня.....	78
Добавление централизованного журналирования.....	84
Обнаружение неисправностей на узлах.....	86
Node Problem Detector .....	86
DaemonSet .....	87
Демоны для обнаружения проблем .....	87
Примеры потенциальных проблем.....	87
Проектирование устойчивых систем .....	88
Аппаратные сбои.....	88

Квоты, общие ресурсы и лимиты .....	89
Плохая конфигурация.....	90
Соотношение затрат и производительности .....	91
Использование Prometheus .....	92
Что такое операторы .....	92
Prometheus Operator .....	92
Установка Prometheus с помощью kube-prometheus.....	93
Мониторинг кластера с помощью Prometheus .....	94
Резюме.....	96
<b>Глава 4. Высокая доступность и надежность.....</b>	<b>97</b>
Концепции, связанные с высокой доступностью.....	97
Избыточность.....	98
Горячая замена.....	98
Выбор лидера.....	98
Умная балансировка нагрузки .....	99
Идемпотентность .....	99
Автоматическое восстановление .....	99
Рекомендуемые методики достижения высокой доступности .....	100
Создание высокодоступных кластеров .....	100
Как сделать узлы надежными.....	101
Как обезопасить состояние кластера .....	101
Сохранность данных .....	105
Избыточные API-серверы.....	106
Выбор лидера в Kubernetes.....	106
Высокая доступность в тестовой среде .....	108
Тестирование высокой доступности.....	109
Обновление кластера на лету .....	110
Плавающие обновления .....	111
Сине-зеленые обновления .....	112
Управление изменениями в контрактах данных .....	113
Миграция данных .....	113
Устаревание API .....	114
Производительность, расходы и компромиссы архитектуры крупных кластеров.....	114
Требования к доступности.....	115
Отсутствие гарантий.....	115

Периоды обслуживания .....	115
Быстрое восстановление .....	116
Нулевое время простоя.....	116
Производительность и согласованность данных.....	118
Резюме.....	119
<b>Глава 5. Конфигурация безопасности, ограничений и учетных записей</b> в Kubernetes.....	120
Проблемы безопасности, стоящие перед Kubernetes .....	120
Потенциальные уязвимости узлов .....	121
Потенциальные уязвимости образов .....	123
Потенциальные проблемы с конфигурацией и развертыванием.....	124
Потенциальные уязвимости подов и контейнеров .....	125
Потенциальные организационные и культурные проблемы.....	125
Как закаляется Hardening.....	126
Службные учетные записи в Kubernetes .....	127
Доступ к API-серверу .....	128
Защита подов.....	134
Управление сетевыми политиками .....	139
Использование объектов secret.....	142
Многопользовательские кластеры.....	145
Необходимость в многопользовательских кластерах.....	145
Безопасная мультиарендность на основе пространств имен.....	146
Подводные камни работы с пространствами имен .....	147
Резюме.....	148
<b>Глава 6. Использование критически важных ресурсов Kubernetes.....</b>	149
Проектирование системы Hue.....	149
Область применения Hue .....	149
Планирование рабочих процессов.....	153
Использование Kubernetes для построения системы Hue .....	154
Эффективное применение kubect1.....	154
Файлы конфигурации ресурсов в kubect1.....	155
Развертывание долгоиграющих микросервисов в подах .....	157
Разделение внутренних и внешних сервисов.....	160
Развертывание внутреннего сервиса.....	161
Создание сервиса hue-reminders .....	162
Выведение сервиса наружу .....	163

Ограничение доступа с помощью пространства имен .....	165
Запуск заданий.....	166
Параллельное выполнение заданий .....	167
Удаление завершенных заданий.....	168
Планирование регулярных заданий с помощью crontab .....	168
Интеграция с внешними компонентами.....	170
Компоненты вне сети кластера .....	170
Компоненты внутри сети кластера.....	170
Управление системой Hue с помощью Kubernetes.....	171
Управление зависимостями с помощью проверок готовности .....	172
Применение контейнеров инициализации для упорядоченного запуска подов.....	173
Развитие системы Hue с помощью Kubernetes.....	174
Применение Hue на предприятиях.....	175
Двигаем научный прогресс с помощью Hue.....	175
Hue — будущее системы образования .....	175
Резюме.....	176
<b>Глава 7. Работа с хранилищем данных в Kubernetes .....</b>	<b>177</b>
Подробное знакомство с постоянными томами .....	177
Тома .....	178
Создание постоянных томов.....	182
Запрос постоянного тома .....	184
Подключение запросов в качестве томов .....	186
Тома на основе блочных устройств .....	186
Классы хранилищ .....	188
Пример работы с постоянным томом от начала до конца .....	189
Типы томов в облачных хранилищах GCE, AWS и Azure.....	192
AWS Elastic Block Store (EBS) .....	193
AWS Elastic File System.....	193
Постоянный диск в GCE.....	195
Диски в Azure .....	195
Файловое хранилище Azure.....	196
Тома GlusterFS и Ceph в Kubernetes.....	197
Использование GlusterFS .....	197
Использование Ceph.....	200
Управление томами внутрикластерных контейнеров с помощью Flocker.....	202
Интеграция промышленного хранилища в Kubernetes.....	204

Отображение томов.....	204
Использование сторонних хранилищ с помощью FlexVolume.....	205
Container Storage Interface.....	206
Резюме.....	208
<b>Глава 8. Запуск приложений с сохранением состояния.....</b>	<b>209</b>
Состояние приложений в Kubernetes.....	209
Активная работа с данными в распределенных приложениях.....	209
Зачем управлять состоянием в Kubernetes.....	210
Зачем выносить управление состоянием за пределы Kubernetes.....	210
Механизм обнаружения: общие переменные окружения или DNS-записи.....	211
Обращение к внешним хранилищам данных через DNS.....	211
Обращение к внешним хранилищам данных через переменные окружения.....	211
Использование ConfigMap в виде переменной окружения.....	212
Резервная копия состояния в памяти.....	213
Использование DaemonSet в качестве резервного постоянного хранилища.....	214
Подключение постоянных томов.....	214
Применение StatefulSet.....	214
Выполнение кластера Cassandra в Kubernetes.....	216
Краткое введение в Cassandra.....	216
Docker-образ Cassandra.....	217
Интеграция Kubernetes и Cassandra.....	222
Создание неуправляемого сервиса Cassandra.....	224
Использование контроллера StatefulSet для создания кластера Cassandra.....	225
Распределение Cassandra с помощью контроллера репликации.....	228
Использование DaemonSet для распределения Cassandra.....	232
Резюме.....	232
<b>Глава 9. Плавающие обновления, масштабирование и квоты.....</b>	<b>234</b>
Горизонтальное автомасштабирование подов.....	234
Объявление горизонтального автомасштабирования подов.....	235
Нестандартные показатели.....	237
Автомасштабирование с помощью kubectl.....	238
Плавающие обновления с автомасштабированием.....	240
Ограничение ресурсов с помощью лимитов и квот.....	241
Включение квот на ресурсы.....	242
Типы квот.....	242
Области действия квот.....	244

Запросы и ограничения .....	245
Работа с квотами .....	245
Выбор и регулирование мощности кластера.....	249
Типы узлов .....	250
Выбор решений для хранения данных .....	250
Компромисс между денежными затратами и временем отклика.....	251
Эффективное использование узлов с разной конфигурацией .....	251
Преимущества эластичных облачных ресурсов.....	252
Hyper.sh и AWS Fargate в качестве альтернативы.....	253
Экстремальные нагрузки в Kubernetes.....	254
Улучшение производительности и масштабируемости Kubernetes.....	255
Измерение производительности и масштабируемости Kubernetes.....	258
Тестирование Kubernetes в крупномасштабных кластерах .....	262
Резюме.....	263
<b>Глава 10. Продвинутая организация сети в Kubernetes.....</b>	<b>264</b>
Сетевая модель Kubernetes.....	264
Взаимодействие между контейнерами внутри пода.....	264
Взаимодействие между подами .....	265
Взаимодействие между подами и сервисами .....	265
Внешний доступ .....	266
Сетевые возможности Kubernetes и Docker .....	266
Поиск и обнаружение.....	268
Сетевые дополнения к Kubernetes.....	270
Сетевые решения для Kubernetes.....	276
Создание мостов в аппаратных кластерах .....	277
Contiv .....	277
Open vSwitch .....	278
Nuage Networks VCS.....	279
Canal .....	279
Flannel .....	280
Проект Calico.....	282
Romana.....	282
Weave Net .....	284
Эффективное использование сетевых политик .....	284
Архитектура сетевой политики в Kubernetes .....	284
Сетевые политики и CNI-дополнения .....	285
Конфигурация сетевых политик .....	285
Реализация сетевых политик.....	285



Способы балансирования нагрузки.....	286
Внешний балансировщик нагрузки .....	287
Балансирование нагрузки с помощью внутреннего сервиса .....	290
Ingress.....	291
Traffic .....	294
Написание собственного дополнения для CNI .....	294
Знакомство с дополнением loopback.....	295
Сборка CNI-дополнения на основе готового каркаса .....	297
Обзор дополнения-моста .....	298
Резюме.....	299
<b>Глава 11. Запуск Kubernetes в нескольких облаках и многокластерном режиме.....</b>	<b>301</b>
Многокластерный режим.....	301
Важные сценарии использования многокластерного режима.....	302
Федеративный управляющий уровень .....	304
Федеративные ресурсы.....	306
Сложности.....	312
Управление многокластерным режимом Kubernetes.....	316
Настройка многокластерного режима с нуля .....	316
Начальная настройка.....	317
Использование официального образа Hyperkube.....	317
Запуск федеративного управляющего уровня .....	317
Регистрация кластеров Kubernetes в федерации.....	318
Обновление KubeDNS .....	319
Отключение многокластерного режима .....	319
Настройка многокластерного режима с помощью Kubefed.....	319
Каскадное удаление ресурсов.....	322
Балансировка нагрузки между несколькими кластерами.....	323
Переключение на другие кластеры в случае сбоя .....	324
Выполнение федеративных рабочих нагрузок .....	326
Создание федеративного сервиса.....	326
Добавление подов .....	327
Проверка общедоступных записей DNS.....	327
Обнаружение федеративного сервиса.....	328
Обработка отказов подов и целых кластеров.....	330
Решение проблем .....	331
Резюме.....	331

<b>Глава 12. Настройка Kubernetes: API и дополнения</b> .....	333
Работа с API Kubernetes .....	333
OpenAPI .....	333
Настройка прокси .....	334
Непосредственный доступ к API Kubernetes .....	334
Создание пода с помощью API Kubernetes .....	337
Доступ к API Kubernetes через клиент Python .....	338
Расширение API Kubernetes .....	344
Понимание структуры пользовательского ресурса .....	344
Определение пользовательских ресурсов .....	345
Интеграция пользовательских ресурсов .....	346
Агрегация API-серверов .....	348
Использование каталога сервисов .....	349
Написание дополнений Kubernetes .....	350
Создание пользовательского дополнения-планировщика .....	350
Проверим, запланированы ли наши поды с помощью пользовательского планировщика .....	355
Использование веб-хуков для контроля доступа .....	355
Веб-хуки для аутентификации .....	355
Веб-хуки для авторизации .....	357
Веб-хуки для контроля входа .....	359
Предоставление пользовательских показателей для горизонтального автомасштабирования подов .....	359
Добавление в Kubernetes пользовательского хранилища .....	360
Резюме .....	361
<b>Глава 13. Работа с диспетчером пакетов Kubernetes</b> .....	363
Знакомство с Helm .....	363
Преимущества .....	363
Архитектура .....	364
Компоненты .....	364
Использование Helm .....	365
Установка Helm .....	365
Поиск схем .....	367
Установка пакетов .....	369
Работа с репозиториями .....	374
Управление схемами с помощью Helm .....	375

Создание своих собственных схем.....	376
Файл Chart.yaml.....	376
Файлы метаданных схемы.....	377
Управление зависимостями схемы.....	378
Использование шаблонов и значений.....	380
Резюме.....	384
<b>Глава 14. Будущее Kubernetes.....</b>	<b>385</b>
Дорога в будущее.....	385
Версии и этапы развития Kubernetes.....	385
Особые интересы и рабочие группы Kubernetes.....	386
Конкуренция.....	386
Значимость контейнеризации.....	387
Docker Swarm.....	387
Mesos/Mesosphere.....	388
Облачные платформы.....	388
AWS.....	388
Azure.....	389
Alibaba Cloud.....	389
Время Kubernetes.....	390
Сообщество.....	390
GitHub.....	390
Конференции и встречи.....	390
Осведомленность потребителей.....	391
Экосистема.....	391
Провайдеры публичных облаков.....	391
Обучение и подготовка.....	392
Модулирование и дополнения «вне дерева».....	394
Технология service mesh и serverless-фреймворки.....	395
Технология service mesh.....	395
Serverless-фреймворки.....	395
Резюме.....	396