Амиму Кнаббену (Amim Knabben), Рикардо Кацу (Ricardo Katz), Мэтту Фенвику (Matt Fenwick), Антонио Охеа (Antonio Ojea), Раджасу Какодару (Rajas Kakodar) и Микаэлю Клюзо (Mikael Cluseau) за многочасовые исследования K8s по ночам и выходным и увлекательные соревнования по крику. Эндрю Стойокосу (Andrew Stoyocos), возглавлявшему группу политик в SIG Network. Моей жене и семье, позволившим мне писать эту книгу по субботам. Гари (Gary), Роне (Rona), Норе (Nora) и Джинджину (Gingin) за помощь моей маме.

– Джей

Кейт (Kate) и всем моим близким, поддерживавшим меня в этом путешествии. Спасибо команде LionKube, особенно Одри (Audrey) за организацию работы и Шарифу (Sharif) за помощь и поддержку. Также моему соавтору Джею (Jay), предложившему мне принять участие в работе над этой книгой вместе с ним, я благодарю тебя за это! Без твоей целеустремленности и упорства у нас ничего не получилось бы.

– Крис

Оглавление

Содержание

Предисловие

Мы написали эту книгу для всех, кто хочет получить новые знания о K8s (Kubernetes) и сразу же углубиться в различные темы, связанные с хранением, сетевыми взаимодействиями и использованием разнообразных инструментов.

Мы не ставили перед собой цель написать исчерпывающее руководство по всем возможностям K8s API (это просто невозможно), но искренне верим, что, прочитав эту книгу, пользователи обретут понимание, которое поможет им по-новому взглянуть на сложные задачи организации инфраструктуры в промышленных кластерах и увидеть общее развитие ландшафта Kubernetes в более широком контексте.

Конечно, есть немало книг, позволяющих пользователям изучить основы Kubernetes, но мы хотели написать книгу, рассказывающую об основных технологиях, составляющих Kubernetes. Здесь мы расскажем вам все тонкости организации сети и плоскости управления, а также некоторые другие темы, чтобы вы смогли понять внутренние особенности работы Kubernetes. Понимание этих деталей сделает вас лучшим инженером DevOps и программистом.

Мы также надеемся вдохновить новых пользователей Kubernetes. Свяжитесь с нами в Твиттере (@jayunit100, @chrislovcnm), если решите принять участие в жизни сообщества Kubernetes или помочь нам добавить больше примеров для этой книги.

Благодарности

Мы хотим поблагодарить сообщество и компании, поддерживающие Kubernetes. Без них и их постоянных усилий не было бы этого замечательного программного обеспечения. Мы хотели бы упомянуть всех причастных, но боимся, что кого-то упустим, поэтому извиняемся заранее.

Спасибо нашим друзьям и наставникам в SIG Network (Микаэлю Клюзо (Mikael Cluseau), Халеду Хендиаку (Khaled Hendiak), Тиму Хокинсу (Tim Hockins), Антонио Охеа (Antonio Ojea), Рикардо Кацу (Ricardo Katz), Мэтту Фенвику (Matt Fenwick), Дэну Уиншипу (Dan Winship), Дэну Уильямсу (Dan Williams), Кейси Календеро (Casey Calendero), Кейси Девенпорт (Casey Davenport), Эндрю Си (Andrew Sy) и многим, многим другим); неутомимым разработчикам открытого исходного кода в сообществах SIG Network и SIG Windows (Марку Розетти (Mark Rosetti), Джеймсу Стареванту (James Sturevant), Клаудио Белу (Claudio Belu), Амиму Кнаббену (Amim Knabben)); первым основателям Kubernetes (Джо Беду (Joe Beda), Брендану Барнсу (Brendan Burns), Вилле Айкасу (Ville Aikas) и Крейгу Маклаки (Craig McLuckie)); а также инженерам из Google, включая Брайана Гранта (Brian Grant) и Тима Хокина (Tim Hockin), присоединившимся к ним вскоре после этого.

Мы благодарны духовным лидерам сообщества: Тиму Сент-Клеру (Tim St. Clair), Джордану Лиггиту (Jordan Liggit), Бриджит Кромхаут (Bridget Kromhaut) и многим другим. Мы также хотели бы поблагодарить Раджаса Какодара (Rajas Kakodar), Анушу Хедж (Anusha Hedge) и Неху Лохию (Neha Lohia) за создание потрясающей команды SIG Network India, внесших колоссальное количество предложений, которые мы надеемся учесть в следующем издании (или возможном продолжении) этой книги, где мы предполагаем подробнее рассказать о приемах организации сети и о прокси-сервере `kube-proxy`.

Джей также хотел бы поблагодарить Клинта Китсона (Clint Kitson) и Аарти Ганесана (Aarthi Ganesan), давших возможность работать над этой книгой, будучи сотрудником VMware, а также его коллег в VMware (Амима (Amim) и Зака (Zac)), постоянно остававшихся рядом и по-

могавших советами. И конечно же, спасибо Фрэнсису Бурану (Frances Buran), Карен Миллер (Karen Miller) и многим другим сотрудникам Manning Publications, помогавшим готовить эту книгу к печати.

Наконец, спасибо всем нашим рецензентам: Алу Кринкеру (Al Krinker), Алессандро Кампейсу (Alessandro Campeis), Александру Эрциу (Alexandru Herciu), Аманде Деблер (Amanda Debler), Андреа Косентино (Andrea Cosentino), Андресе Сакко (Andres Sacco), Анупаму Сенгупте (Anupam Sengupta), Бену Фенвику (Ben Fenwick), Борко Джурковичу (Borko Djurkovic), Дарье Василенко (Daria Vasilenko), Элиасу Рангелю (Elias Rangel), Эрике Хоулу (Eric Hole), Эриксу Зеленке (Eriks Zelenka), Ойгену Кокалеа (Eugen Cocalea), Ганди Раджану (Gandhi Rajan), Ирине Романенко (Iryna Romanenko), Джареду Дункану (Jared Duncan), Джеффу Лиму (Jeff Lim), Джиму Амрайну (Jim Amrhein), Хуану Хосе Дурильо Барриону́эво (Juan José Durillo Barrionuevo), Мэтту Фенвику (Matt Fenwick), Мэтту Велке (Matt Welke), Михалю Рутке (Michał Rutka), Риккардо Маротти (Riccardo Marotti), Робу Пачеко (Rob Pacheco), Робу Рютчу (Rob Ruetsch), Роману Левченко (Roman Levchenko), Райану Бартлетту (Ryan Bartlett), Убальдо Пескаторе (Ubaldo Pescatore) и Уэсли Рольнику (Wesley Rolnick). Ваши предложения помогли сделать эту книгу лучше.

О книге

Кому адресована эта книга

Всем желающим узнать больше о внутреннем устройстве Kubernetes, о том, как рассуждать о его режимах отказа и возможности расширения под нужды пользователей. Если вы не знаете, что такое Pod, то, конечно, можете приобрести эту книгу, но прежде прочтите какую-нибудь другую книгу, где вы сможете поближе познакомиться с терминологией.

Также книга пригодится операторам, желающим общаться на едином языке с сотрудниками ИТ-отделов, техническими директорами и другими руководителями о том, как внедрить Kubernetes, сохранив при этом основные принципы построения инфраструктуры, существовавшие до появления контейнеров. Эта книга действительно поможет преодолеть разрыв между новыми и старыми решениями по проектированию инфраструктуры. По крайней мере, мы на это надеемся!

Организация книги

Эта книга состоит из 15 глав:

- глава 1. Дает общий обзор Kubernetes для новичков;
- глава 2. Рассматривает идею модуля Pod как атомарного строительного блока для приложений и закладывает основы для последующих глав, подробно рассматривающих низкоуровневые детали Linux;
- глава 3. Углубляется в детали использования в Kubernetes низкоуровневых примитивов Linux для реализации концепций более высокого уровня, включая модули Pod;
- глава 4. Здесь начинается изучение внутренних особенностей процессов и их изоляции в Linux, которые являются одними из менее известных деталей ландшафта Kubernetes;
- глава 5. После подробного знакомства с модулями Pod углубляется в организацию сетевых взаимодействий между ними и рассказывает, как они соединяются друг с другом через разные узлы;

- глава 6. Вторая глава, посвященная сетевым взаимодействиям, описывающая более широкие аспекты работы модулей Pod и прокси-сервера (`kube-proxy`), а также приемы их настройки и сопровождения;
- глава 7. Первая глава, посвященная вопросам организации хранилища. Здесь дается широкое введение в теоретические основы хранилищ Kubernetes, контейнерный интерфейс хранилища (Container Storage Interface, CSI) и его взаимодействия с kubelet;
- глава 8. Вторая глава, посвященная вопросам организации хранилища. Здесь рассматриваются некоторые более практические аспекты хранения данных, включая особенности emptyDir, Secrets и PersistentVolumes/Dynamic storage;
- глава 9. Углубляется в kubelet и рассматривает некоторые детали запуска модулей Pod и управления ими, включая такие понятия, как CRI, жизненный цикл узла и ImagePullSecrets;
- глава 10. DNS в Kubernetes – сложный механизм, используемый почти всеми контейнерными приложениями для локального доступа к внутренним сервисам. Здесь рассматривается CoreDNS – реализация сервиса DNS для Kubernetes – и порядок выполнения DNS-запросов разными модулями Pod;
- глава 11. Подробно обсуждает плоскость управления, упоминавшуюся в предыдущих главах, включая тонкости работы планировщика, диспетчера контроллеров и сервера API. Они образуют «мозг» Kubernetes и объединяют вместе все низкоуровневые концепции, обсуждавшиеся в предыдущих главах;
- глава 12. После обсуждения логики плоскости управления мы углубимся в etcd, надежный механизм консенсуса для Kubernetes, и особенности его настройки для удовлетворения потребностей плоскости управления Kubernetes;
- глава 13. Представляет обзор NetworkPolicies, RBAC и безопасности на уровне модулей Pod и узлов, о которых должен знать каждый администратор. В этой главе также обсуждается общее развитие политик безопасности модулей Pod;
- глава 14. Здесь рассматривается настройка безопасности на уровне узла и облака, а также другие аспекты безопасности Kubernetes, ориентированные на инфраструктуру;
- глава 15. Эта заключительная глава дает общий обзор прикладных инструментов на примере Carvel, набора инструментов для управления файлами YAML, создания приложений и долгосрочного управления жизненным циклом приложений.

О примерах программного кода

Для этой книги мы подготовили несколько примеров, которые вы найдете в репозитории GitHub (https://github.com/jayunit100/k8sprototypes/), в том числе примеры:

- использования `kind` для настройки реалистичной сети в локальных кластерах с помощью Calico, Antrea или Cillium;
- анализа метрик Prometheus в реальном мире;
- создания приложений с помощью набора инструментов Carvel;
- различных экспериментов, связанных с RBAC.

Эта книга также содержит множество примеров программного кода. Они оформлены `шрифтом фиксированной ширины`, чтобы вам было проще отличать его от основного текста.

Во многих случаях исходный код переформатирован, чтобы уместить его по ширине книжной страницы. В частности, мы добавили разрывы строк и отступы. В редких случаях даже этого было недостаточно, и мы добавили маркеры продолжения строки (➥). Многие листинги сопровождаются комментариями в тексте, подчеркивающими важные понятия. Получить выполняемые фрагменты кода можно из электронной версии книги по адресу https://livebook.manning.com/book/core-kubernetes и в репозитории GitHub https://github.com/jayunit100/k8sprototypes/.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Manning Publications очень серьезно от-

носятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторах

Джей Вьяс, д-р наук (Jay Vyas, PhD), в настоящее время – штатный инженер в VMware. Работал над несколькими коммерческими дистрибутивами и платформами Kubernetes с открытым исходным кодом, включая OpenShift, VMware Tanzu, внутренними коллективными платформами Black Duck для Kubernetes и установкой Kubernetes для клиентов его консалтинговой компании Rocket Rudolf, LLC. В течение нескольких лет был членом комитета по управлению проектами (Project Management Committee, PMC) в Apache Software Foundation, где работал над несколькими проектами в области больших данных. Он был связан с Kubernetes на различных должностях с момента его создания и в настоящее время уделяет большое внимание сообществам SIG-Windows и SIG-Network. Начинал с создания распределенных систем, одновременно защитив докторскую диссертацию по витринам данных в сфере биоинформатики (объединявшим базы данных в платформы для анализа человеческих и вирусных белковых карт – протеомов). Это привело его в мир больших данных и масштабируемых систем обработки данных и, наконец, в Kubernetes.

Связаться с Джеем можно по адресу @jayunit100 в Твиттере, если вы заинтересованы в сотрудничестве… по какой угодно теме. Уделяет большое внимание спорту, ежедневно пробегает одну милю в спринтерском темпе и подтягивается до отказа. Также увлекается музыкой и имеет несколько синтезаторов, в том числе Prophet-6, который звучит как космический корабль.

Крис Лав (Chris Love) – сертифицированный сотрудник Google Cloud и соучредитель Lionkube. Больше 25 лет занимался разработкой программного обеспечения в таких компаниях, как Google, Oracle, VMware, Cisco, Johnson & Johnson и др. Как идейный лидер в Kubernetes и в сообществе DevOps, Крис Лав участвовал во многих проектах с открытым исход-

ным кодом, включая Kubernetes, kops (в должности руководителя AWS SIG), Bazel (внес вклад в разработку правил для Kubernetes) и Terraform (один из первых разработчиков плагина VMware). В число его профессиональных интересов входят: трансформация ИТ-культуры, технологии контейнеризации, методы и средства автоматизированного тестирования, Kubernetes, Golang (он же Go) и другие языки программирования. Лав обожает заниматься популяризацией DevOps, Kubernetes и технологий, а также обучать людей в сфере ИТ и программного обеспечения.

Вне работы любит кататься на лыжах, играть в волейбол, заниматься йогой и участвовать в мероприятиях на свежем воздухе. Кроме того, вот уже 20 лет занимается боевыми искусствами.

Если вы решите пообщаться с Крисом и задать ему свои вопросы, то сможете связаться с ним по адресу @chrislovenm в Twitter или LinkedIn.

Об иллюстрации на обложке

Изображение на обложке книги называется «Штерн, матрос у руля корабля». Оно взято с гравюры картины Альфредо Луксоро (Alfredo Luxoro), опубликованной в журнале «L'Illustrazione Italiana», № 19, от 9 мая 1880 года.

В те дни по одежде было легко определить, где живет человек, чем занимается и какое положение занимает в обществе. Мы в издательстве Manning славим изобретательность, предприимчивость и радость компьютерного бизнеса обложками книг, изображающими богатство региональных различий многовековой давности, оживших благодаря иллюстрациям, таким как эта.

1 Почему появился Kubernetes

В этой главе:

- почему появился Kubernetes;
- основные термины Kubernetes;
- конкретные примеры использования Kubernetes;
- высокоуровневые функции Kubernetes;
- когда нежелательно использовать Kubernetes.

Kubernetes – это платформа с открытым исходным кодом для размещения контейнеров и определения прикладных API для управления облачной семантикой обеспечения этих контейнеров хранилищами данных, сетевыми услугами, поддержкой безопасности и другими ресурсами. Kubernetes обеспечивает непрерывную синхронизацию всего пространства состояний ваших приложений, в том числе способов доступа к ним из внешнего мира.

Зачем внедрять Kubernetes в свое окружение? Не проще ли выделить все необходимые ресурсы вручную с помощью инструмента управления инфраструктурой, связанного с DevOps? Ответ зависит от того, как мы определяем процесс DevOps и его интеграцию в общий жизненный цикл приложения. DevOps продолжает расширяться и включает в себя процессы, инженеров и инструменты, которые поддерживают более автоматизированное администрирование приложений в центре обработки данных. Одно из условий успешного