Моим родителям,
которые всегда ставили потребности своих детей
выше собственных

Оглавление

Вступительное слово от компании ITSumma

Любимой кофейной кружке придется подвинуться – эта книга займет центральное место на вашем столе и станет главным навигатором в контейнерных технологиях. Мы очень рады, что книга выходит на русском языке. После своего триумфального появления в 2014 году Kubernetes основательно утвердился в качестве лидирующей программы для оркестровки контейнеров в мире. Но в России до сих пор не было ресурса, который бы дал о нём исчерпывающую информацию.

Данная книга дает пошаговое разъяснение принципов работы контейнеризации и устройства модулей в Kubernetes. Вы узнаете все о создании объектов верхнего уровня, развертывании кластера Kubernetes на собственной рабочей машине и построении федеративного кластера в нескольких дата-центрах.

Автор книги – инженер-программист с двадцатилетним стажем Марко Лукша. Последние пять лет он курировал новые разработки Kubernetes для компании Red Hat и изучил все тонкости создания приложений в данной среде. Сложные рабочие схемы Лукша преподносит в очень занимательной и последовательной манере. Вы узнаете о трех способах обеспечить доступ к службам извне и разберете варианты перехода к процессу обновления с нулевым временем простоя. А также сравните размещение в Kubernetes классических контейнеризированных микросервисов и систем, использующих внутреннее состояние.

Нас приятно удивило, что Лукша уделяет особое внимание извечному спору сисадминов и разработчиков и в том числе рассказывает о практике NoOps, которая разрешает конфликты двух лагерей. Отдельное спасибо автору за то, что он детально анализирует задачи обеспечения безопасности в Kubernetes – крайне актуальную и малоисследованную на сегодня задачу.

Наглядные схемы и «разбор полетов» в книге создают впечатление индивидуального мастер-класса. Автор предвосхищает большинство вопросов, заранее объясняя, в каком направлении двигаться, если что-то пойдет не так. Те, кто только начал знакомство с платформой, смогут уверенно перейти к практической работе в Kubernetes. А «бывалые» специалисты узнают причины и пути решения для ранее безвыходных ситуаций.

Эта книга – отличный компас в увлекательном изучении облачных технологий, которые с каждым годом набирают все больше последователей. Надеемся увидеть вас в их числе.

Ваша ITSumma

Описанные/рассмотренные в книге ресурсы Kubernetes

	Ресурс (сокр.) [версия API]	Описание	Раздел
	Namespace* (ns) [v1]	Позволяет организовывать ресурсы в неперекрывающиеся группы (например, для каждого потребителя ресурсов)	3.7
Развертывающие рабочие нагрузки	**Pod** (po) [v1]	Основная развертываемая единица, содержащая один или более процессов в расположенных рядом контейнерах	3.1
	ReplicaSet (rs) [apps/v1beta2**]	Поддерживает одну или несколько реплик модуля	4.3
	ReplicationController (rc) [v1]	Более старый, менее мощный эквивалент ресурса ReplicaSet	4.2
	Job [batch/v1]	Запускает модули, выполняющие завершаемую задачу	4.5
	CronJob [batch/v1beta1]	Запускает назначаемое задание один раз или периодически	4.6
	DaemonSet (ds) [apps/v1beta2**]	Запускает одну реплику модуля в расчете на узел (на всех узлах или только на тех, которые соответствуют селектору узлов)	4.4
	StatefulSet (sts) [apps/v1beta1**]	Запускает модули, имеющие внутреннее состояние, со стабильной идентичностью	10.2
	Deployment (deploy) [apps/v1beta1**]	Декларативное развертывание и обновление модулей	9.3
Службы	**Service** (svc) [v1]	Предоставляет доступ к одному или нескольким модулям на одной и стабильной паре IP-адреса и порта	5.1
	Endpoints (ep) [v1]	Определяет, к каким модулям (или другим серверам) предоставляется доступ через службу	5.2.1
	Ingress (ing) [extensions/v1beta1]	Предоставляет внешним клиентам доступ к одной или нескольким службам через один доступный извне IP-адрес	5.4
Конфигурация	**ConfigMap** (cm) [v1]	Словарь в формате «ключ-значение» для хранения незащищенных параметров конфигурации приложений и предоставления им доступа к ним	7.4
	Secret [v1]	Как и словарь конфигурации ConfigMap, но для конфиденциальных данных	7.5
Хранение	**PersistentVolume*** (pv) [v1]	Указывает на постоянное хранилище, которое можно смонтировать в модуль посредством заявки PersistentVolumeClaim	6.5
	PersistentVolumeClaim (pvc) [v1]	Запрос и заявка на PersistentVolume	6.5
	StorageClass* (sc) [storage.k8s.io/v1]	Определяет тип динамически резервируемого хранилища, заявляемого в PersistentVolumeClaim	6.6

(Окончание)

	Ресурс (сокр.) [версия API]	Описание	Раздел
Масштабирование	**HorizontalPodAutoscaler** (hpa) [autoscaling/v2beta1**]	Автоматически масштабирует количество реплик модулей на основе использования ЦП или другой метрики	15.1
	PodDisruptionBudget (pdb) [policy/v1beta1]	Определяет минимальное количество модулей, которые должны оставаться запущенными при эвакуации узлов	15.3.3
Ресурсы	**LimitRange** (limits) [v1]	Определяет мин, макс, ограничения и запросы по умолчанию (default) для модулей в пространстве имен	14.4
	ResourceQuota (quota) [v1]	Определяет объем вычислительных ресурсов, доступных для модулей в пространстве имен	14.5
Состояние кластера	**Node*** (нет)[v1]	Представляет рабочий узел Kubernetes	2.2.2
	Cluster* [federation/v1beta1]	Кластер Kubernetes (используемый в федерации кластеров)	Прил. D
	ComponentStatus* (cs) [v1]	Статус компонента контрольной панели	11.1.1
	Event (ev) [v1]	Отчет о том, что произошло в кластере	11.2.3
Безопасность	**ServiceAccount** (sa) [v1]	Учетная запись, используемая приложениями, запущенными в модулях	12.1.2
	Role [rbac.authorization.k8s.io/v1]	Определяет, какие действия субъект может выполнять с какими ресурсами (в расчете на пространство имен)	12.2.3
	ClusterRole* [rbac.authorization.k8s.io/v1]	Как Role, но для ресурсов уровня кластера или для предоставления доступа к ресурсам во всех пространствах имен	12.2.4
	RoleBinding [rbac.authorization.k8s.io/v1]	Определяет, кто может выполнять действия, определенные в Role или ClusterRole (в пространстве имен)	12.2.3
	ClusterRoleBinding* [rbac.authorization.k8s.io/v1]	Как RoleBinding, но по всем пространствам имен	12.2.4
	PodSecurityPolicy* (psp) [extensions/v1beta1]	Ресурс уровня кластера, который определяет, какие чувствительные для безопасности особенности могут использовать модули	13.3.1
	NetworkPolicy (netpol) [networking.k8s.io/v1]	Изолирует сеть между модулями, указывая, какие модули могут подключаться друг к другу	13.4
	CertificateSigningRequest* (csr) [certificates.k8s.io/v1beta1]	Запрос на подписание сертификата открытого ключа	5.4.4
Расш.	**CustomResourceDefinition*** (crd) [apiextensions.k8s.io/v1beta1]	Определяет настраиваемый ресурс, позволяющий пользователям создавать экземпляры настраиваемого ресурса	18.1

* Ресурс уровня кластера (без пространства имен).

** Также в других версиях API; указанная версия использована в этой книге.

Благодарности

Издательство «ДМК Пресс» благодарит компанию «ITSumma» и ее генерального директора Евгения Потапова за неоценимую помощь в подготовке этой книги.

Без них вы, возможно, не так хорошо поняли бы Kubernetes, но теперь мы полностью уверены, что все термины стоят на своих местах.

Предисловие

После работы в Red Hat в течение нескольких лет, в конце 2014 года я был назначен в недавно созданную команду под названием Cloud Enablement. Нашей задачей было вывести линейку продуктов компании промежуточного уровня на OpenShift Container Platform, которая затем разрабатывалась поверх платформы Kubernetes. В то время Kubernetes все еще находилась в зачаточном состоянии – версия 1.0 еще даже не была выпущена.

Наша команда должна была узнать все входы и выходы Kubernetes, чтобы быстро установить правильное направление для нашего программного обеспечения и воспользоваться всем, что система Kubernetes должна была предложить. Когда мы сталкивались с проблемой, нам было трудно сказать, делаем ли мы что-то неправильно или просто попали на одну из ранних ошибок Kubernetes.

С тех пор и Kubernetes, и мое понимание этой платформы прошли долгий путь. Когда я впервые начал ее использовать, большинство людей даже не слышало о Kubernetes. Теперь об этой платформе знает практически каждый инженер-программист, и она стала одним из самых быстрорастущих и широко распространенных способов запуска приложений как в облаке, так и в локальных центрах обработки данных.

В первый месяц работы с Kubernetes я написал двухсоставной блог-пост о том, как запускать кластер сервера приложений Jboss WildFly в OpenShift/Kubernetes. В то время я совсем не мог себе представить, что простой пост в блоге в конечном итоге приведет к тому, что представители издательства Manning свяжутся со мной по поводу того, хочу ли я написать книгу о Kubernetes. Конечно, я не мог сказать «нет» такому предложению, хотя я был уверен, что они также обратились к другим специалистам и в конечном итоге выбрали кого-то другого.

И все же вот мы здесь. После более чем полутора лет написания и исследования книга закончена. Это было потрясающее путешествие. Написание книги о технологии является идеальным способом узнать ее гораздо подробнее, чем если вы узнаете ее как простой пользователь. По мере того как во время процесса написания книги мои знания о Kubernetes расширялись, а сама платформа Kubernetes эволюционировала, я постоянно возвращался к предыдущим, уже написанным главам и добавлял дополнительную информацию. Я перфекционист, поэтому никогда не буду абсолютно доволен книгой, но я рад узнать, что многие читатели программы раннего доступа Manning (MEAP) считают ее отличным путеводителем по Kubernetes.

Моя цель состоит в том, чтобы помочь читателю понять саму технологию и научить их использовать ее инструментарий для эффективной и действенной разработки и развертывания приложений в кластерах Kubernetes. В книге я не уделяю особого внимания тому, как на самом деле создавать и поддерживать надлежащий высокодоступный кластер Kubernetes, но последняя часть должна дать читателям очень четкое понимание того, из чего состоит такой кластер, и должна позволить им легко разбираться в дополнительных ресурсах, которые касаются этой темы.

Очень надеюсь, что вам понравится читать эту книгу и что она научит вас получать максимальную отдачу от удивительной системы под названием Kubernetes.