Использование Deckhouse Kubernetes Platform: запуск и администрирование приложений

онлайн-курс | 10 дней | 85 000 руб. (+НДС)

Аудитория курса

- Будущий пользователь/администратор Deckhouse Kubernetes Platform (DKP) без навыков в Kubernetes

Цели курса

- Изучить основные понятия, сущности и механизмы Kubernetes
- Научиться запускать, публиковать и конфигурировать приложения с помощью Kubernetes в среде DKP

Требования к участникам

- Знать Linux на уровне пользователя
- Понятия DNS, HTTP, URL
- Основы Docker
- Основы создания и использования Docker-контейнеров

Формат

- Курс состоит из теоретического материала, который включает серии вебинаров, Q&A-сессии, и практической части с выполнением лабораторных работ на учебном стенде

План работы

Использование Deckhouse Kubernetes Platform: запуск и администрирование приложений

Онлайн, 10 дней

Тема	Структура
1. Знакомство с Kubernetes	**Цель:** разобрать форматы данных и научиться подключаться к кластеру с помощью kubectl **Темы урока:** • Введение в Kubernetes • Основные понятия Kubernetes • Kubernetes API, kubectl • Формат данных в Kubernetes (JSON, YAML, манифесты) **Практика:** создание kubeconfig; использование kubectl для получения различных данных.

2. Запуск и взаимодействие контейнеров	**Цель:** научиться запускать поды в кластере, настраивать их ресурсы, научиться создавать Deployment, Job и CronJob
	
	Темы урока:
	• Что собой представляет под:
	  ○ Контейнеры
	  ○ Жизненный цикл пода
	  ○ Планирование ресурсов
	• Управление группами подов:
	  ○ ReplicaSet, ReplicationController, Job
	  ○ CronJob, DaemonSet, Deployment
	
	Практика: создание Deployment, CronJob и Job.

3. Конфигурация приложений	**Цель:** научиться использовать переменные окружения, ConfigMap'ы и Secret'ы для конфигурации приложений.
	
	Теория:
	• Способы конфигурации в DKP:
	  ○ ConfigMap'ы
	  ○ Переменные окружения
	• Работа с приватными данными приложений — пароли, ключи
	
	Практика: создание ConfigMap'ов и Secret'ов и конфигурация приложений.

4. Публикация приложений и сетевое взаимодействие	**Цель:** научиться создавать сервисы разных типов, настраивать связь между приложениями и пользователями, понимать, как работает DNS в кластере.
	
	Теория:
	• Виды сетевого взаимодействия в кластере
	• Механизм Services:
	  ○ clusterIP
	  ○ nodePort
	  ○ Headless Services
	  ○ External name
	  ○ endpoints
	• Работа DNS в кластере
	
	Практика: настройка сетевого взаимодействия между приложениями

	и пользователями.
5. Механизм Ingress	**Цель:** научиться публиковать приложения по HTTP, создавать сертификаты с помощью cert-manager'а, управлять входящими HTTP-запросами. **Теория:** • Маршрутизация входящих HTTP-запросов • Конфигурирование поведения Ingress • Работа с Ingress Class и Ingress Controller • Работа с SSL-сертификатами и cert-manager'ом • Защита Ingress логином и паролем **Практика:** создание и настройка Ingress-ресурсов и сертификатов.
6. Хранение данных и stateful-приложения	**Цель:** научиться понимать связку PV, PVC и StorageClass, монтировать Volumes и создавать StatefulSet. **Теория:** • Зачем нужны Volumes • Что такое Volumes • Типы Volumes • Persistent Volumes и PVC • StorageClass • Политики переиспользования PV • Изменение размера PV • Режимы доступа • Лимитирование дисковых ресурсов • StatefulSet **Практика:** создание PV, PVC и StatefulSet.
7. Безопасность и управление доступом	**Цель:** научиться понимать механизм RBAC, создавать Service Account, распределять права доступа с использованием ролей и кластерных ролей. **Теория:** • Механизм RBAC • Service Accounts, пользователи, группы • Роли и кластерные роли • Привязка ролей и кластерных ролей **Практика:** настройка прав доступа приложений.

8. Безопасность в Kubernetes	**Цель:** изучить основные стандарты безопасности, научиться создавать и применять политики безопасности для подов, а также сетевые политики для пространств имен и других объектов кластера.
	
	Теория:
	• Стандарты безопасности
	• Безопасность пода:
	  ○ Pod Security Standards (политики безопасности и их ограничения)
	  ○ Модуль admission-policy-engine и его особенности
	  ○ Параметры безопасности пода
	• Сетевая безопасность:
	  ○ CNI. Cilium
	  ○ Cilium Network Policy
	
	Практика: настройка политик безопасности и сетевых политик.

9. Распределение подов по узлам

Цель: научиться использовать механизмы selector, affinity, taint/toleration, настраивать PDB для приложений.

Теория:

- taint/toleration
- NodeAffinity
- Pod anti-affinity
- PDB

Практика: распределение подов по узлам и настройка autoscalers.