Администрирование виртуализации в Deckhouse Platform

Онлайн-курс 5 дней

Аудитория курса

- DevOps-инженеры
- Системные инженеры Kubernetes
- Администраторы инфраструктуры виртуализации

Требования к участникам

- Знать Linux на уровне пользователя
- Знать основные понятия и сущности Kubernetes (pod, deployment, service, ingress, PV/PVC, StorageClass)
- Знать принцип работы и основные понятия TCP/IP (уровень CCNA)
- Иметь общее представление о виртуализации (KVM/QEMU, libvirt)

Цели курса

- Получить знания о принципах работы и архитектуре виртуализации как части Deckhouse Platform
- Приобрести базовые навыки развёртывания, настройки и эксплуатации виртуализации Deckhouse Platform, включая управление виртуальными машинами, дисками, образами, хранилищами и сетями

Формат

- Курс состоит из теоретического материала и практической части с выполнением лабораторных работ на учебном стенде
- Теоретический материал включает вебинары и онлайн-демонстрации работы в кластере

Важно:

- Курс сфокусирован на виртуализации. Платформа и сеть разбираются в объёме, нужном для работы с виртуальными машинами. Для углублённого изучения:
  - администрирования всей Deckhouse Platform — курс «Администрирование Deckhouse Platform»;
  - сетевых возможностей платформы — курс «Сетевые возможности Deckhouse Platform».

Deckhouse Platform

План работы

Тема 01

Основы виртуализации в Deckhouse Platform: архитектура, установка, образы и диски

Продолжительность: 8 ак. часов

Цель: получить знания об архитектуре виртуализации в Deckhouse Platform, научиться развёртывать её поверх кластера Deckhouse Platform и управлять образами и дисками виртуальных машин.

Теория:

- Kubernetes и Deckhouse Platform как основа для виртуализации
- Оркестрация ВМ в Kubernetes и проект KubeVirt
- Стек гипервизора: KVM + QEMU + libvirt
- Что не устраивает в «чистом» KubeVirt и что добавляет виртуализация Deckhouse Platform. Назначение и сценарии использования виртуализации Deckhouse Platform
- Архитектура виртуализации Deckhouse Platform
- Виртуализация как часть Deckhouse Platform. Порядок установки
- Включение виртуализации. Ресурс ModuleConfig для модуля virtualization
- Способы взаимодействия с платформой
- Зачем в виртуализации Deckhouse Platform отдельные ресурсы для образов и дисков
- Ресурсы образов. Импорт образов
- Источники данных для образов и дисков
- Ресурсы образов. Импорт образов
- Варианты хранения образов. DVCR: внутренний реестр образов ВМ, настройка
- Ресурс VirtualDisk. Перемещение диска между StorageClass'ами
- Жизненный цикл образов и дисков

Практика:

- Проектирование подсети для виртуальных машин (virtualMachineCIDRs)
- Проверка кластера и готовности узлов к виртуализации
- Подготовка SDS-хранилища под DVCR и диски ВМ с маркировкой блочных устройств
- Включение модуля virtualization
- Контроль развёртывания компонентов виртуализации Deckhouse Platform
- Работа с командами d8 k и d8 v, проверка установки через веб-интерфейс
- Подготовка проекта для образов и дисков
- Создание VirtualImage из HTTP-источника с хранением в DVCR
- Создание ClusterVirtualImage
- Сравнение вариантов хранения образа (DVCR против PVC) и ограничения локального хранилища
- Создание VirtualDisk из образа и пустого диска
- Проверка и диагностика образов и дисков

Тема 02

Виртуальные машины в виртуализации в Deckhouse Platform. Снимки

Продолжительность: 8 ак. часов

Цель: научиться создавать виртуальные машины и управлять их жизненным циклом в виртуализации в Deckhouse Platform, работать со снимками дисков и ВМ.

Теория:

- Как виртуальная машина исполняется «под капотом»
- Ресурс VirtualMachine
- VirtualMachineClass
- Provisioning ВМ
- Подключение блочных устройств
- Проброс USB-устройств
- Развёртывание ВМ
- Сеть и IP-адреса ВМ (обзорно)
- Live-миграция
- Доступ к ВМ
- Снимки в виртуализации Deckhouse Platform

Практика:

- Создание VirtualMachineClass
- Развёртывание Debian из готового образа с cloud-init
- Доступ к ВМ через консоль/VNC/SSH
- Подключение диска на лету
- Установка ALT Linux p11 с ISO
- Управление жизненным циклом через VMOP
- Работа с IP-адресами ВМ
- Live-миграция
- Проверка возможностей хранилища для снимков и создание снимков

Тема 03

Хранилища для виртуализации в Deckhouse Platform: SDS, CSI, разновидности и особенности

Продолжительность: 8 ак. часов

Цель: изучить варианты поддерживаемых хранилищ для виртуализации в Deckhouse Platform и их особенности, выбрать и настроить оптимальное хранилище под задачи виртуализации.

Теория:

- Как данные хранятся на дисках: блочное устройство как базовая абстракция; файловая система поверх блочного устройства; разделы и менеджеры томов (LVM); толстое и тонкое выделение места (Thick vs Thin)
- Модель хранения в Kubernetes: PV, PVC, StorageClass, CSI, VolumeSnapshot; ключевые параметры StorageClass для виртуализации Deckhouse Platform
- Требования виртуализации Deckhouse Platform к хранилищу
- Software-Defined Storage (SDS) в Deckhouse Platform
- sds-node-configurator
- sds-local-volume
- sds-replicated-volume
- sds-elastic
- Внешние и CSI-варианты хранения
- Влияние выбора хранилища в виртуализации Deckhouse Platform
- Эксплуатация SDS

Практика:

- Анализ текущего хранилища и доступных дисков
- Включение модуля sds-replicated-volume
- Подготовка Volume Group с thin-пулом под репликацию
- Создание ReplicatedStoragePool и ReplicatedStorageClass
- Перевод дисков ВМ на реплицируемое хранилище на лету
- Live-миграция ВМ на реплицируемом хранилище
- Снимки на реплицируемом хранилище
- Имитация отказа узла для проверки отказоустойчивости

Тема 04

Сеть в виртуализации в Deckhouse Platform. Модуль sdn

Продолжительность: 8 ак. часов

Цель: научиться организовывать сетевое взаимодействие виртуальных машин в виртуализации Deckhouse Platform с использованием модуля sdn.

Теория:

- Сетевая модель виртуализации Deckhouse Platform
- Две плоскости сети ВМ: основная сеть кластера (Main) и дополнительные сети
- IPAM основной сети
- Дополнительные интерфейсы ВМ
- Модуль sdn от Deckhouse Platform
- VLAN для виртуальных машин
- IPAM для дополнительных сетей
- Разграничение трафика между портами и сетями
- Публикация сервисов ВМ
- Диагностика сети ВМ

Практика:

- Работа с основной сетью ВМ и IPAM
- Публикация сервиса ВМ через Service
- Публикация через Ingress
- Публикация через Gateway API
- Включение и подготовка модуля sdn
- Создание VLAN-сети для ВМ
- Подключение второго интерфейса ВМ в VLAN
- Разграничение трафика и проверка изоляции
- Диагностика сети ВМ

Важно:

Сетевые возможности платформы (Cilium, внутренняя сеть, DNS, MetalLB, NLB в облаке, ingress-nginx, alb, сетевая сегментация, Istio service mesh) подробно разбираются в курсе «Сетевые возможности Deckhouse Platform».

Тема 05

Эксплуатация и мультитенантность в виртуализации в Deckhouse Platform

Продолжительность: 8 ак. часов

Цель: научиться эксплуатировать и сопровождать кластер виртуализации Deckhouse Platform в production-окружении, организовывать мультитенантную работу нескольких команд и проектов, настраивать мониторинг и диагностику.

Теория:

- Почему неймспейс сам по себе не является изоляцией
- Механизмы Deckhouse Platform для изоляции
- Модуль multitenancy-manager
- Штатные шаблоны проектов
- Изоляция тенантов в контексте виртуализации Deckhouse Platform
- Доступ: RBAC для виртуализации
- Кастомизация: собственный ProjectTemplate
- Встроенный мониторинг
- Диагностика типовых проблем ВМ

Практика:

- Проверка модуля multitenancy-manager
- Разбор штатных шаблонов проектов
- Создание тенант-проекта из шаблона default
- Проверка изоляции тенанта
- Защита от «голых» неймспейсов и перевод существующего неймспейса под управление проекта
- Разработка собственного ProjectTemplate под виртуализацию
- Создание проекта из своего шаблона
- Работа со встроенным мониторингом ВМ и проекта
- Диагностика ВМ

Важно:
Администрирование всей платформы (установка и обновление, модули, мониторинг, аутентификация и авторизация) подробно разбирается в курсе «Администрирование Deckhouse Platform».