Эта книга посвящается
моим любимым родителям:
Шримати Таре Деви и Шри Баскиту Саху.
А также
моей жене Гитешри Ананде и моему сыну Найтику.

– Дхирендра Кумар

Как мы учимся и развиваемся в жизни

आचार्यत् पद्मादत्ते पादम् पादम् शष्यि स्वमेधायः

पादम् सब्रह्मचारभ्यिःपादम् कालक्रमेण च

Четверть знаний ученик получает от своего учителя,
четверть – благодаря собственному разуму,
четверть – от своих сокурсников
и еще четверть – со временем (от жизненного опыта).

– Ишан Кхаре

Оглавление

Об авторах 22

О техническом рецензенте 23

Признательности 24

Предисловие 25

От издательства 28

Глава 1. Введение в виртуализатор KubeVirt для виртуализации на базе платформы OpenShift 29

Введение 29
Содержание главы 29
Эволюция виртуализации и облачно-ориентированных приложений 30
Эволюция виртуализации 30
Появление облачных вычислений 31
Сдвиг в сторону облачно-ориентированных приложений 32
Трудности управления унаследованными и облачно-ориентированными рабочими нагрузками 33
Введение в виртуализатор KubeVirt: наведение мостов 33
Выгоды виртуализатора KubeVirt в облачных средах 34
Этапы освоения виртуализатора 34
Виртуализатор KubeVirt и его актуальность 35
Эволюция виртуализации и расцвет контейнеров 36
Трудности управления унаследованными рабочими нагрузками на базе виртуальных машин 36
Ключевые компоненты виртуализатора KubeVirt 37
Выгоды от объединения Kubernetes и виртуальных машин 38
Обзор виртуализации на базе платформы OpenShift 39
Эволюция виртуализации и контейнеризации 39
Ключевые компоненты виртуализации на базе платформы OpenShift 40
Ключевые варианты использования виртуализатора KubeVirt в гибридных рабочих нагрузках 41
Наведение мостов между унаследованными приложениями и облачно-ориентированными средами 42
Развертывание в гибридном облаке 42
Среды разработки и тестирования для унаследованных приложений 42
Многоарендность и защищенная изоляция рабочих нагрузок 43
Восстановление после аварийных отказов и высокая доступность 43

Сравнение с традиционными платформами виртуализации 43
Архитектура и модель развертывания 44
Производительность и потребление ресурсов 45
Управление и автоматизация 46
Безопасность и изоляция 46
Заключение 47

Глава 2. Настройка среды 48

Введение 48
Содержание главы 48
Предварительные условия для развертывания виртуализатора KubeVirt 48
Совместимость платформ 49
Аппаратные требования 50
Аспекты сетевого взаимодействия 51
Программные зависимости 51
Безопасность и контроль доступа 51
Проверка готовности системы к установке 52
Установка оператора виртуализации OpenShift 52
Предварительные условия 53
Шаг 1: доступ к веб-консоли платформы OpenShift 53
Шаг 2: установка оператора виртуализации OpenShift 54
Шаг 3: проверка корректности установки 55
Шаг 4: активация виртуализации OpenShift 55
Шаг 5: конфигурирование хранилища и сетевого взаимодействия 55
Пример из реальной практики: развертывание виртуальной машины 56
Конфигурирование ресурсов кластера для виртуализации 57
Понимание выделения ресурсов в виртуализации OpenShift 57
Конфигурирование вычислительных ресурсов 57
Конфигурирование хранилища для виртуализации 58
Использование ODF для долговременного хранения 58
Сетевое взаимодействие для виртуализации 59
Политики масштабирования и планирования 60
Настройка и интеграция сетевого взаимодействия 60
Обзор сетевого взаимодействия в виртуализаторе KubeVirt 61
Настройка сетевого взаимодействия в OpenShift с виртуализатором KubeVirt 61
CNI-плагин Multus для нескольких сетевых интерфейсов 62
Аппаратная виртуализация SR-IOV для высокопроизводительных сетей 63
Проверка корректности установки и устранение неисправностей 64
Проверка корректности установки 64
Устранение типичных неисправностей при установке 65
Инструменты для подготовки среды 66
Инструменты подготовки инфраструктуры 67
Инструменты управления кластерами Kubernetes 68
Инструменты для сетевого взаимодействия и балансировки нагрузки 68

Инструменты управления хранилищем 68
Инструменты обеспечения безопасности и соблюдения нормативных требований 69
Заключение 69

Глава 3. Понимание архитектуры виртуализатора KubeVirt 71

Введение 71
Содержание главы 71
Важнейшие компоненты 72
Компонент virt-api: центральный API-сервер виртуализатора KubeVirt 72
Компонент virt-controller: стержневой компонент плоскости управления 74
Компонент virt-handler: агент на каждом узле 76
Мониторинг работоспособности узлов 77
Архитектура и процесс общения 77
Компонент virt-launcher: менеджер процессов в каждом экземпляре ВМ 79
Описания собственных ресурсов виртуализатора KubeVirt: приоритетный обзор 80
Ресурс VirtualMachineInstance (VMI) 81
Ресурс VirtualMachine (VM) 81
Ресурс DataVolume 82
Ресурс VirtualMachineInstanceReplicaSet (VMIRS) 82
Ресурс instancetype 83
Менее распространенные описания собственных ресурсов 83
Важнейшая роль инструментария libvirt и эмулятора QEMU в KubeVirt 84
Инструментарий libvirt: API виртуализации 84
QEMU: эмулятор и виртуализатор виртуальных машин 84
Взаимодействие инструментария libvirt, эмулятора QEMU и виртуализатора KubeVirt 85
Заключение 87

Глава 4. Управление виртуальными машинами 88

Введение 88
Содержание главы 88
Определение манифестов виртуальных машин 89
Конфигурирование спецификаций ВМ 90
Конфигурирование ЦП 90
Количество виртуальных ЦП 90
Топология ЦП 91
Модель ЦП 92
Функции ЦП 92
Конфигурирование памяти 92
Выделение памяти 93
Конфигурирование хранилища 93
Ресурсы PersistentVolumeClaim 93
Сводный пример 94
Управление заготовками и репликами виртуальных машин 94

Выгоды от использования заготовок виртуальных машин ... 95
Создание заготовок виртуальных машин ... 95
Управление заготовками виртуальных машин ... 96
Реплики виртуальных машин в виртуализаторе KubeVirt ... 96
Ресурсы DataVolume для хранения данных виртуальных машин ... 97
Понимание контейнеризированного импортера данных (CDI) ... 97
Альтернативные варианты хранения ... 98
Использование ресурсов DataVolume в виртуализаторе KubeVirt ... 99
Характеристики и нюансы использования ресурсов DataVolume ... 100
Закачивание образов дисков с помощью команды virtctl image-upload ... 101
Практические варианты использования ресурсов DataVolume ... 101
Преимущества и ограничения ресурсов DataVolume ... 102
Управление жизненным циклом ... 102
Заключение ... 104

Глава 5. Сетевое взаимодействие в среде виртуализации на базе OpenShift ... 105

Введение ... 105
Содержание главы ... 105
Обзор архитектуры сетевого взаимодействия в виртуализаторе KubeVirt ... 106
Основы сетевого взаимодействия в KubeVirt ... 106
Глоссарий по сетевому взаимодействию в виртуализации в среде OpenShift ... 107
Виртуальный сетевой контроллер (vNIC) ... 108
Сеть пода ... 108
Специфичный для KubeVirt механизм сетевой привязки ... 108
Распространенные модели сетевого взаимодействия ... 108
Сетевое взаимодействие с маскировкой (NAT) ... 108
CNI-плагин Multus для многосетевых подключений ... 109
Технология SR-IOV для высокопроизводительных сетей ... 109
Аспекты сетевого взаимодействия и лучшие образцы практики ... 109
Сценарий развертывания из реальной практики ... 110
Конфигурирование сетевого плагина Multus для продвинутого сетевого взаимодействия в виртуализации в среде OpenShift ... 110
Понимание сетевого плагина Multus в виртуализации в среде OpenShift ... 110
Ключевые выгоды сетевого плагина Multus ... 111
Установка и конфигурирование сетевого плагина Multus в OpenShift ... 111
Варианты использования из реальной практики ... 113
Устранение неполадок сетевого плагина Multus ... 113
Подсоединение виртуальных машин к сервисам Kubernetes ... 113
Сетевые стратегии для обеспечения соединяемости виртуальных машин и сервисов Kubernetes ... 114
Сервисная сетка Istio для интеграции в нее виртуальных машин ... 114
Гибридные сетевые политики ... 115
Модели сетевого взаимодействия через сетевой мост и трансляцию сетевых адресов (NAT) ... 116
Сетевое взаимодействие через сетевой мост ... 116

Вариант использования в виртуализации OpenShift 117
Сетевое взаимодействие через трансляцию сетевых адресов (NAT) 117
Вариант использования 118
Устранение проблем сетевой связности в KubeVirt для виртуализации в среде OpenShift 118
Распространенные проблемы сетевой связности в KubeVirt 119
Пошаговый подход к устранению неполадок 119
Отладка проблем связности между подами 119
Устранение неполадок в работе сервисов и балансировщиков нагрузки 120
Отладка преобразования имен DNS 120
Выявление проблем с максимальным размером пакета (MTU) и фрагментацией пакетов 121
Устранение проблем с производительностью и потерей пакетов 121
Вопросы обеспечения безопасности сетевой изоляции 121
Понимание сетевой изоляции в виртуализаторе KubeVirt 121
Ключевые модели сетевой изоляции 122
Риски для безопасности при сетевой изоляции 122
Лучшие образцы практики обеспечения сетевой изоляции 123
Вариант использования из реальной практики: обеспечение безопасности многоарендной среды виртуализации OpenShift 124
Заключение 125

Глава 6. Интеграция хранилищ 126

Введение 126
Содержание главы 126
Долговременное хранилище в виртуальных машинах 127
Традиционные решения по хранению данных 127
Основополагающие элементы хранилища в Kubernetes 127
Использование основополагающих элементов в виртуализаторе KubeVirt 128
Режимы хранения 129
Гибкая подготовка хранилища с помощью CDI-импортера и примитивов Kubernetes 131
Проект контейнеризированного импорта данных (CDI) 132
Собственный ресурс DataVolume 132
Импорт из URL-адресов по протоколам HTTP/HTTPS 132
Импорт контейнерных дисков из реестров контейнеров 133
Эффективное клонирование ресурсов PVC 133
Закачивание локальных образов дисков 134
Создание пустых дисков для виртуальных машин KubeVirt 134
Импорт из сред виртуализации oVirt (источник imageio) 135
Импорт из среды виртуализации VMware (источник vddk) 135
Специализированная обработка типов содержимого 136
Контейнерные диски в виртуализаторе KubeVirt 136
CSI-драйверы для расширенной поддержки хранилищ 138
Задействование CSI-драйверов в виртуализаторе KubeVirt 138
Повышенная гибкость и выбор бэкендов хранилищ 140

Популярные CSI-драйверы и их интеграция с виртуализатором KubeVirt ... 140
CSI-драйверы облачных провайдеров ... 140
Локальные CSI-драйверы ... 141
Управление производительностью и масштабируемостью хранилищ ... 141
Запаздывание в операциях на томах ... 142
Выявление и измерение запаздывания у хранилища ... 143
Лимиты соединений с хостом и давление на соединения ... 143
Стратегии минимизации рисков ... 144
Вопросы масштабируемости при использовании локальных и топологически ограниченных хранилищ ... 144
Проблемы масштабируемости локальных хранилищ ... 145
Вопросы масштабируемости топологически ограниченных хранилищ ... 145
Решения и лучшие образцы практики ... 146
Влияние режимов доступа на живую миграцию ... 146
Определение режимов доступа к хранилищу ... 146
Влияние режима RWO на живую миграцию ... 147
Влияние режима ROX на живую миграцию ... 147
Влияние режима RWX на живую миграцию ... 147
Устранение распространенных проблем с хранилищем ... 148
Отказы при монтировании томов ... 148
Распространенные причины ... 148
Шаги по устранению неполадок ... 149
Узкие места в производительности хранилища ... 149
Распространенные причины ... 149
Диагностика и устранение узких мест ... 150
Проблемы с повреждением данных ... 150
Выявление и устранение повреждений данных ... 150
Проблемы с сетевой связностью ... 151
Влияние на доступ к хранилищу и способы решения ... 151
Лучшие образцы практики интеграции хранилищ ... 151
Выбор подходящих типов хранилищ ... 152
Блочное, файловое и объектное хранилища ... 152
Рекомендации в зависимости от рабочей нагрузки ... 152
Конфигурации, рекомендуемые для классов хранилищ и долговременных томов ... 152
Конфигурация спецификации класса хранения ... 153
Конфигурация ресурсов PersistentVolume и PersistentVolumeClaim ... 153
Рекомендации по мониторингу ... 153
Инструменты и метрики мониторинга ... 153
Проактивное выявление проблем ... 154
Заключение ... 154

Глава 7. Обеспечение безопасности и соблюдение нормативных требований ... 155

Введение ... 155
Содержание главы ... 155

Управление доступом на основе ролей (RBAC) в виртуальных машинах 156
Понимание управления доступом на основе ролей в KubeVirt 156
Ключевые компоненты управления доступом на основе ролей 156
Реализация управления доступом на основе ролей в KubeVirt 156
Продвинутые варианты использования метода RBAC 158
Лучшие образцы практики управления на основе ролей в среде виртуализации на базе OpenShift 159
Использование профилей механизмов SELinux и Seccomp для усиления безопасности 160
Введение в механизмы SELinux и Seccomp 160
Обзор механизма SELinux 160
Обзор механизма Seccomp 160
Варианты использования из реальной практики 161
Конфигурирование политик безопасности OpenShift 161
Доступ к кластеру OpenShift 161
Обзор доступа к кластеру OpenShift 162
Вариант использования из реальной практики 162
Механизмы аутентификации 162
Доступ через командный интерфейс и веб-консоль 163
Управление доступом на основе ролей (RBAC) 163
Роли и привязки ролей 163
Ограничения контекста безопасности 164
Сетевые политики для защиты виртуализированных рабочих нагрузок 164
Соблюдение нормативных требований и аудит 165
Аудит и мониторинг активности виртуальных машин 166
Важность аудита и мониторинга 166
Журналирование активности виртуальных машин в KubeVirt 166
Захватывание журналов виртуальных машин 166
Журналирование аудита в целях обеспечения безопасности и соблюдения нормативных требований 167
Пример: обнаружение несанкционированного доступа 167
Мониторинг метрик производительности виртуальных машин 167
Настройка системы Prometheus для мониторинга виртуальных машин 168
Мониторинг сетевого трафика 168
Захватывание журналов сетевого трафика 168
Аспекты безопасности 169
Движок политик Kyverno: чем он полезен для KubeVirt и OpenShift 169
Ключевые функциональные возможности Kyverno 169
Применение движка политик Kyverno в KubeVirt 170
Повышение безопасности OpenShift с помощью движка Kyverno 171
Обеспечение соблюдения сетевых политик 171
Применение политик ограничения контекста безопасности в OpenShift 172
Практические вызовы и решения в области обеспечения безопасности для KubeVirt и виртуализации на базе OpenShift 172
Изоляция рабочих нагрузок и риски многоарендности 172
Сетевая безопасность и защита горизонтального трафика 173

Безопасность хранилищ и защита данных ... 173
Безопасность цепочки поставок и целостность образов ... 174
Управление доступом на основе идентичности ... 174
Лучшие образцы практики по обеспечению безопасности в среде виртуализации на базе OpenShift ... 174
Заключение ... 175

Глава 8. Автоматизация процесса виртуализации посредством операционной модели GitOps ... 176

Введение ... 176
Содержание главы ... 177
Введение в операционную модель GitOps для виртуализации ... 177
Определение операционной модели GitOps в контексте виртуализатора KubeVirt и среды OpenShift ... 177
Преимущества операционной модели GitOps для виртуализированных рабочих нагрузок ... 178
Архитектура операционной модели GitOps для виртуализатора KubeVirt на базе OpenShift ... 179
Пример из реальной практики: подход к разработке с внедрением практики безопасности (DevSecOps) для виртуальных машин в финансовой организации ... 179
Интеграция долговременных томов и томов данных в операционную модель GitOps ... 180
Расширение операционной модели GitOps на мультиоблачные среды и развертывания виртуальных кластеров (vCluster) ... 180
Управление конфигурациями виртуальных машин с помощью инструментов операционной модели GitOps ... 181
Декларативное управление виртуальными машинами с помощью KubeVirt ... 181
Принципы операционной модели GitOps в управлении жизненным циклом виртуальных машин ... 181
Пример из реальной практики ... 182
Интеграция собственных ресурсов VMConfig ... 183
Конвейеры GitOps для развертываний виртуальных машин ... 183
Управление секретами и SSH-ключами ... 184
Наблюдаемость и аудитоспособность ... 184
Проблемы и лучшие образцы практики ... 184
Автоматизация развертывания и обновлений с использованием конвейеров ... 185
Понимание конвейерных принципов в виртуализации на базе операционной модели GitOps ... 185
Архитектурное исполнение конвейеров виртуализации ... 186
Пример из реальной практики: автоматизация развертывания виртуальной машины Windows ... 187
Задействование инструментов Tekton и Argo CD для полной автоматизации жизненного цикла ... 187
Контроль версий и продвижение между средами ... 188

Защищенная обработка секретов и конфигураций виртуальных машин ... 188
Пример: инъекция SSH-ключа в конфигуратор cloud-Init ... 189
Мониторинг, наблюдаемость и отказоустойчивость конвейеров ... 189
Поддержание согласованности между кластерами ... 190
Сложности многокластерной согласованности ... 190
Операционная модель GitOps как основание для согласованности ... 190
Архитектура многокластерной согласованности с использованием виртуализатора KubeVirt ... 191
Управление специфичными для виртуализатора KubeVirt ресурсами ... 192
Пример из реальной практики: развертывание виртуальных машин Windows в двух кластерах ... 192
Синхронизация ролей RBAC и кластерных политик ... 193
Интеграция CI/CD для виртуализированных рабочих нагрузок ... 194
Архитектурные вопросы ... 194
Конструктивные шаблоны конвейеров ... 195
Пример из реальной практики: операционная модель GitOps для сред разработки на базе Ubuntu ... 196
Рекомендации по инструментарию ... 196
Вопросы безопасности и соблюдения нормативных требований ... 197
Устранение неполадок в автоматизации GitOps ... 197
Понимание пути исполнения в рамках операционной модели GitOps ... 197
Распространенные категории отказов автоматизации ... 198
Инструментарий диагностики и наблюдаемость ... 199
Лучшие образцы практики создания отказоустойчивых конвейеров GitOps ... 200
Сценарий устранения неполадок из реальной практики ... 200
Заключение ... 201

Глава 9. Мониторинг и оптимизация производительности ... 203

Введение ... 203
Содержание главы ... 204
Настройка мониторинга рабочих нагрузок KubeVirt ... 204
Необходимость наблюдаемости виртуальных машин в Kubernetes ... 204
Активация мониторинга KubeVirt в среде OpenShift ... 204
Конфигурирование системы Prometheus под сбор метрик виртуализатора KubeVirt ... 205
Конфигурирование RBAC для сбора метрик ... 205
Визуализация метрик с помощью информационных панелей платформы Grafana ... 206
Импорт информационных панелей для виртуализатора KubeVirt ... 206
Продвинутые методы обеспечения наблюдаемости ... 207
Использование платформ Prometheus и Grafana для визуализации ... 207
Архитектурный обзор мониторинга в OpenShift под управлением KubeVirt ... 207
Конфигурирование системы Prometheus под мониторинг компонентов виртуализатора KubeVirt ... 208

Понимание ключевых метрик виртуализатора KubeVirt 209
Интеграция и индивидуальная настройка информационных панелей платформы Grafana 209
Сценарий из реальной практики: мониторинг соблюдения соглашения об уровне обслуживания (SLA) в отношении виртуализированных рабочих нагрузок 209
Лучшие образцы практики обеспечения наблюдаемости в кластерах OpenShift с поддержкой KubeVirt 210
Конфигурирование оповещений для проактивного мониторинга 211
Архитектура системы оповещения в средах OpenShift-KubeVirt 211
Определение эффективных правил оповещения 211
Статус виртуальной машины 211
Исчерпание ресурсов 212
Узкие места дискового ввода-вывода 212
Интеграция с компонентом Alertmanager с целью маршрутизации уведомлений 213
Настройка чувствительности оповещений и предотвращение усталости от оповещений 213
Лучшие образцы практики управления жизненным циклом оповещений 214
Анализ метрик производительности для оптимизации 214
Архитектура наблюдаемости для виртуализатора KubeVirt в среде OpenShift 215
Ключевые оптимизируемые метрики производительности 215
Пример оптимизации 215
Установка базовых уровней производительности 217
Выявление узких мест производительности 217
Оповещения и автоматизация при деградации производительности 218
Устранение узких мест производительности 218
Понимание анатомии узкого места 218
Каркас поиска неисправностей на основе симптомов 219
Инструменты и методы 219
Сценарий возникновения узкого места № 1: исчерпание ЦП на узлах виртуализатора KubeVirt 219
Сценарий возникновения узкого места № 2: давление на память и раздувание памяти 220
Сценарий возникновения узкого места № 3: производительность диска и ввода-вывода 221
Сценарий возникновения узкого места № 4: сетевое запаздывание и пропускная способность сети 222
Методы оптимизации ресурсов виртуальных машин 223
Понимание моделей выделения ресурсов в KubeVirt 223
Подбор правильного размера виртуальных машин 224
Задействование механизма HugePages для оптимизации памяти 224
Привязка ЦП и планирование с учетом архитектуры NUMA 225
Оптимизация дискового ввода-вывода 225
Сетевая оптимизация виртуальных машин 226

Стратегическое использование живой миграции ... 227
Автоматизация оптимизации с помощью операционной модели GitOps и конвейеров ... 227
Заключение ... 228

Глава 10. Программирование функциональности виртуализатора KubeVirt ... 229

Введение ... 229
Содержание главы ... 229
Настройка среды и клиента Go для виртуализатора KubeVirt ... 229
Роль файлов kubeconfig ... 230
Внекластерная аутентификация с помощью библиотеки client-go ... 230
Внутрикластерная аутентификация с использованием объектов ServiceAccount ... 231
Использование функции k8s.io/client-go/rest.InClusterConfig() ... 231
Клиентские библиотеки Go для KubeVirt ... 232
Сравнение библиотек kubevirt.io/client-go и k8s.io/client-go ... 233
Инициализация объекта clientset виртуализатора KubeVirt ... 233
Использование клиента controller-runtime вместо типизированных ... 234
Взаимодействие с объектами API KubeVirt ... 235
Выполнение операций CRUD на ресурсах виртуализатора KubeVirt ... 236
Примеры операций CRUD на ресурсах виртуализатора KubeVirt ... 236
Операции CRUD с использованием клиента controller-runtime ... 239
Продвинутые операции ... 242
Программное масштабирование ресурсов ... 242
Создание платформ вокруг виртуализатора KubeVirt ... 243
Преимущества ... 246
Заключение ... 247

Глава 11. Сравнений технологий KubeVirt и vCluster ... 248

Введение ... 248
Содержание главы ... 248
Подробный архитектурный обзор ... 248
Технология KubeVirt ... 249
Пояснение элементов диаграммы и рабочего процесса ... 250
Ключевая философия и цели технологии vCluster ... 252
Ключевые архитектурные компоненты технологии vCluster ... 253
Пояснение элементов диаграммы и рабочих процессов ... 254
Подготовка изолированных экземпляров виртуального кластера vCluster ... 257
Задействование командного интерфейса vCluster ... 257
Продвинутое развертывание с помощью менеджера Helm и файла vCluster.yaml ... 258
Доступ к виртуальному кластеру vCluster через конфигурационный файл Kubeconfig ... 258
Проверка успешности развертывания виртуального кластера vCluster ... 259
Защищенный демонтаж: удаление виртуального кластера vCluster ... 259

Оптимизация ресурсов: приостановка (режим сна) и возобновление виртуального кластера vCluster 260
Сравнение производительности и использования ресурсов 260
Гибридные рабочие нагрузки и многоарендные среды 262
Преимущества гибридных контекстов 262
Интеграция технологий KubeVirt и vCluster 263
Выгоды и лимиты комбинированного подхода 263
Каркас принятия решений 266
Когда выбирать виртуализатор KubeVirt 267
Когда выбирать технологию vCluster 267
Заключение 269

Глава 12. Клонирование виртуальных машин, золотые образы и контейнеризированный импортер данных (CDI)..... 270

Введение 270
Содержание главы 270
Выгоды и варианты использования 271
Преимущества клонирования виртуальных машин в KubeVirt 271
Ускорение подготовки и развертывания виртуальных машин 272
Обеспечение согласованности, единообразия и стандартизации по всем средам 272
Обеспечение эффективной масштабируемости виртуализированных рабочих нагрузок 272
Укрепление способностей по восстановлению после аварийных отказов 273
Создание золотых образов и управление ими 273
Золотой образ диска в экосистеме виртуализатора KubeVirt 273
Центральная роль ресурсов PersistentVolumeClaim 274
Клонирование на базе контейнеризированного импортера данных (CDI) 274
Использование API VirtualMachineClone со снимками виртуальных машин 275
Ссылка на золотые образы в описаниях ресурсов VirtualMachine 275
Лучшие образцы практики управления жизненным циклом золотых образов 277
Обновление живых виртуальных машин новыми версиями золотых образов 277
Контейнеризированный импортер данных (CDI) и его роль в управлении образами 278
Ключевые компоненты 278
Поток взаимодействия при обработке описания собственного ресурса DataVolume 279
Ключевые функциональности контейнеризированного импортера данных (CDI) по управлению образами 282
Импорт образов виртуальных машин из различных источников 282
Клонирование существующих ресурсов PersistentVolumeClaim 284
Понимание поля contentType 284

Шаблоны создания, обслуживания и потребления ... 285
Создание ... 285
Обслуживание и обновление ... 286
Индивидуальная настройка клонов виртуальных машин под уникальные требования рабочих нагрузок ... 287
Обеспечение уникальности: MAC-адреса и серийные номера SMBIOS ... 287
Изменение конфигурации виртуального оборудования ... 288
Подключение к описаниям сетевых подключений NetworkAttachmentDefinition (NAD) ... 289
Типы интерфейсов (masquerade, bridge, slirp, SR-IOV) ... 289
Аспекты использования статических IP- и MAC-адресов ... 290
Использование конфигуратора cloud-init для виртуальных машин Linux (пользовательские данные, SSH-ключи и сеть) ... 291
Заключение ... 293

Глава 13. Виртуализатор KubeVirt в гибридных и мультиоблачных средах ... 294

Введение ... 294
Содержание главы ... 294
Понимание гибридной и мультиоблачной архитектур ... 295
Деловые драйверы перехода на гибридные и мультиоблачные архитектуры ... 296
Архитектурные шаблоны для развертываний гибридных облаков и мультиоблаков ... 297
Сетевые аспекты и вопросы хранения данных ... 297
Роль виртуализатора KubeVirt в гибридных и мультиоблачных экосистемах ... 298
Сложности и лучшие образцы практики ... 298
Переносимость рабочих нагрузок: миграция виртуальных машин между облаками с помощью виртуализатора KubeVirt ... 299
Понимание переносимости рабочих нагрузок в контексте виртуализации ... 300
Архитектурные основы для мультиоблачной миграции виртуальных машин ... 300
Пошаговый процесс межоблачной миграции виртуальных машин ... 301
Пример из реальной практики: миграция из локального кластера OpenShift в управляемый кластер AWS ROSA ... 302
Рекомендации и лучшие образцы практики ... 302
Перспективы на будущее: живая миграция и периферийные вычисления ... 303
Аспекты сетевого взаимодействия для гибридных и мультиоблачных сред ... 303
Введение в гибридное и мультиоблачное сетевое взаимодействие ... 303
Конструктивные принципы сети ... 304
Архитектура сетевого взаимодействия в KubeVirt ... 304
Межкластерное сетевое взаимодействие ... 304
Система доменных имен (DNS) и обнаружение сервисов ... 305

Балансировка нагрузки и управление трафиком ... 305
Безопасность и управление политиками ... 306
Наблюдаемость и устранение неполадок ... 306
Стратегии масштабирования мультиоблачных рабочих нагрузок и восстановления после аварийных отказов ... 306
Понимание мультиоблачного масштабирования и его сложностей ... 307
Масштабирование виртуальных рабочих нагрузок в мультиоблачных кластерах OpenShift ... 307
Горизонтальное масштабирование по всем кластерам ... 307
Вертикальное масштабирование внутри узлов ... 308
Восстановление после аварийных отказов для виртуальных машин в мультиоблачных средах ... 308
«Холодное» восстановление после аварийных отказов с использованием операционной модели GitOps и немутируемых определений виртуальных машин ... 308
«Теплое» восстановление после аварийных отказов с использованием долговременных томов и периодической синхронизации ... 309
«Горячее» восстановление после аварийных отказов с непрерывной репликацией ... 309
Практическая архитектура для мультиоблачного масштабирования и восстановление после аварийных отказов ... 310
Лучшие образцы практики и рекомендации ... 311
Сложности обеспечения безопасности и лучшие образцы практики в гибридных и мультиоблачных средах ... 311
Вызовы в области безопасности в гибридных и мультиоблачных архитектурах ... 311
Лучшие образцы практики безопасности для KubeVirt в гибридных и мультиоблачных средах ... 313
Варианты использования виртуализатора KubeVirt в гибридных и мультиоблачных средах из реальной практики ... 314
Модернизация унаследованных приложений при обеспечении непрерывности процессов ... 315
Восстановление после аварийных отказов и высокая доступность через границы облаков ... 315
Периферийные вычисления и виртуализация телекоммуникационных сетевых функций ... 316
Межоблачное расширение для сезонного спроса ... 317
Среды разработки и тестирования для разнородных стеков приложений ... 317
Рабочие нагрузки с повышенными требованиями к безопасности в регулируемых средах ... 318
Заключение ... 318

Глава 14. Продвинутые темы в виртуализаторе KubeVirt ... 320

Введение ... 320
Содержание главы ... 320

Рабочие нагрузки на графических процессорах 321
Типы виртуализации графических процессоров 322
Плагины устройств Kubernetes для поддержки графических ЦП 322
Поддержка графических процессоров NVIDIA 323
Поддержка графических процессоров AMD 324
Сквозная передача графических процессоров для виртуальных машин KubeVirt 325
Подготовка хоста 325
Активация контроллера IOMMU 325
Настройка параметров ядра 326
Загрузка драйвера vfio-pci и привязка ГП 326
Конфигурирование собственного ресурса (CR) KubeVirt для списка разрешенных устройств permittedHostDevices 326
Спецификация экземпляра ВМ (VirtualMachineInstance) для сквозной передачи графических процессоров 327
Лучшие образцы практики настройки производительности рабочих нагрузок графических процессоров 328
Задействование механизмов выравнивания с учетом архитектуры NUMA и привязки ЦП 328
Использование дробных ресурсов графических процессоров 329
Производительность хранилища 329
Механизм HugePages для виртуальных машин 329
Управление ресурсами графических процессоров и мониторинг использования 329
Мониторинг метрик графических процессоров с помощью инструментов Prometheus и Grafana 330
Инструментарий для мониторинга и управления графическими процессорами NVIDIA (DCGM) 330
Экспортер DCGM 331
Настройка системы Prometheus 331
Информационные панели платформы Grafana 331
Ключевые метрики графических процессоров для мониторинга 331
Проблемы и устранение неполадок при работе с графическими процессорами в виртуализаторе KubeVirt 333
Проблемы с привязкой драйвера vfio-pci 333
Неправильные конфигурации контроллера IOMMU 333
Неправильная конфигурация собственного ресурса permittedHostDevices виртуализатора KubeVirt 334
Нарезка, коллективизация использования времени графических процессоров и многоэкземплярный ГП (MIG) 334
Нарезка/коллективизация использования времени графических процессоров (преимущественно в контексте NVIDIA) 334
Многоэкземплярный ГП (MIG) (специфика NVIDIA) 335
Виртуальные графические процессоры NVIDIA (опосредованные устройства) в KubeVirt 336
Заключение 337

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru