

Оглавление

Предисловие	18
Благодарности	19
Об этой книге	21
Для кого эта книга	21
Структура издания: дорожная карта.....	22
Форум LiveBook.....	23
Автор онлайн	23
Об авторе	24
Иллюстрация на обложке	25
О переводчике на русский язык	26
От издательства	26

Часть 1 ОСНОВЫ

Глава 1. Podman: контейнерный движок нового поколения	28
1.1. О терминологии.....	29
1.2. Краткое описание контейнеров.....	33

8 Оглавление

1.2.1. Образы контейнеров: новый способ доставки программного обеспечения.....	36
1.2.2. Как образы контейнеров способствуют развитию микросервисов	37
1.2.3. Формат образа контейнера	39
1.2.4. Контейнерные стандарты.....	41
1.3. Зачем использовать Podman, если есть Docker.....	42
1.3.1. Почему есть только один способ запуска контейнеров	42
1.3.2. Непривилегированные (rootless) контейнеры.....	44
1.3.3. Модель fork/exec	45
1.3.4. Podman без демонов	48
1.3.5. Дружественная командная строка	48
1.3.6. Поддержка REST API.....	49
1.3.7. Интеграция с systemd	50
1.3.8. Поды	51
1.3.9. Настраиваемые реестры.....	53
1.3.10. Множественный транспорт.....	54
1.3.11. Полная настраиваемость.....	55
1.3.12. Поддержка пользовательского пространства имен	55
1.4. Когда не следует использовать Podman	56
Резюме	56
Глава 2. Командная строка	58
2.1. Работа с контейнерами.....	59
2.1.1. Исследование контейнеров	59
2.1.2. Запуск контейнерного приложения	62
2.1.3. Остановка контейнеров	66
2.1.4. Запуск контейнеров	67
2.1.5. Список контейнеров.....	68
2.1.6. Инспектирование контейнеров.....	69

2.1.7. Удаление контейнеров.....	70
2.1.8. Выполнение команд внутри контейнера	71
2.1.9. Создание образа из контейнера.....	72
2.2. Работа с образами контейнеров	75
2.2.1. Разница между контейнером и образом.....	75
2.2.2. Вывод списка образов.....	78
2.2.3. Инспектирование образов.....	79
2.2.4. Передача образов.....	80
2.2.5. podman login: аутентификация в реестре контейнеров.....	83
2.2.6. Тегирование образов	85
2.2.7. Удаление образов.....	88
2.2.8. Загрузка образов.....	90
2.2.9. Поиск образов.....	94
2.2.10. Монтирование образов	94
2.3. Сборка образов.....	96
2.3.1. Формат Containerfile или Dockerfile	97
2.3.2. Автоматизация сборки нашего приложения	101
Резюме	104
Глава 3. Тома	105
3.1. Использование томов в контейнерах	106
3.1.1. Именованные тома	108
3.1.2. Параметры монтирования томов.....	111
3.1.3. Параметр --mount команды podman run	115
Резюме	116
Глава 4. Поды	117
4.1. Управление подами	117
4.2. Создание подов	121
4.3. Добавление контейнера в под	122

4.4. Запуск подов.....	124
4.5. Остановка пода	125
4.6. Вывод списка подов	126
4.7. Удаление подов	126
Резюме	128

Часть 2 АРХИТЕКТУРА

Глава 5. Настройка и файлы конфигурации 130

5.1. Конфигурационные файлы для хранилища	132
5.1.1. Расположение хранилища	133
5.1.2. Драйверы хранилища	136
5.2. Конфигурационные файлы реестров	139
5.2.1. registries.conf	139
5.2.2. Запрет на загрузку из реестров контейнеров	141
5.3. Конфигурационные файлы контейнерных движков.....	143
5.4. Системные файлы конфигурации.....	147
Резюме	149

Глава 6. Непривилегированные (rootless) контейнеры 150

6.1. Как работает Podman в режиме rootless?.....	153
6.1.1. Образы с содержимым, принадлежащим нескольким идентификаторам пользователей (UIDs)	154
6.1.2. Пользовательское пространство имен (user namespace).....	155
6.1.3. Пространство имен mount (mount namespace)	161
6.1.4. Пользовательское пространство имен и пространство имен mount	163
6.2. «Под капотом» Podman без root.....	164
6.2.1. Скачивание образа.....	166
6.2.2. Создание контейнера.....	167

6.2.3. Настройка сети.....	168
6.2.4. Запуск мониторинга контейнера: conmon.....	169
6.2.5. Запуск среды выполнения ОСИ.....	170
6.2.6. Контейнерное приложение работает до своего завершения.....	172
Резюме.....	172

Часть 3

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ PODMAN

Глава 7. Интеграция с systemd.....	174
7.1. Запуск systemd внутри контейнера.....	176
7.1.1. Требования к systemd в контейнерах.....	178
7.1.2. Контейнер Podman в режиме systemd.....	179
7.1.3. Запуск службы Apache в systemd-контейнере.....	180
7.2. Journald для ведения журналов и событий.....	182
7.2.1. Драйвер логирования.....	183
7.2.2. События.....	184
7.3. Запуск контейнеров при загрузке.....	185
7.3.1. Перезапуск контейнеров.....	185
7.3.2. Контейнеры Podman как службы systemd.....	186
7.3.3. Распространение юнит-файлов systemd для управления контейнерами Podman.....	190
7.3.4. Автоматическое обновление контейнеров Podman.....	191
7.4. Запуск контейнеров в юнит-файлах типа notify.....	195
7.5. Откат неисправных контейнеров после обновления.....	196
7.6. Контейнеры Podman, активируемые через сокет.....	197
Резюме.....	200
Глава 8. Работа с Kubernetes.....	201
8.1. YAML-файлы Kubernetes.....	203
8.2. Генерация YAML-файлов Kubernetes с помощью Podman.....	204

12 Оглавление

- 8.3. Генерация подов и контейнеров Podman из Kubernetes YAML..... 208
 - 8.3.1. Завершение работы подов и контейнеров на основании Kubernetes YAML-файла..... 209
 - 8.3.2. Создание образов с использованием YAML-файлов Podman и Kubernetes..... 210
- 8.4. Запуск Podman внутри контейнера 213
 - 8.4.1. Запуск Podman внутри Podman-контейнера..... 214
 - 8.4.2. Запуск Podman внутри пода Kubernetes..... 215
- Резюме 217

- Глава 9. Podman как служба 218**
 - 9.1. Знакомство со службой Podman 219
 - 9.1.1. Службы Systemd..... 221
 - 9.2. API, поддерживаемые Podman 223
 - 9.3. Библиотеки Python для работы с Podman 226
 - 9.3.1. Использование docker-py с Podman API 226
 - 9.3.2. Использование podman-py с Podman API..... 228
 - 9.3.3. Какую библиотеку Python выбрать..... 230
 - 9.4. Использование docker-compose со службой Podman 230
 - 9.5. podman --remote 234
 - 9.5.1. Локальные подключения..... 235
 - 9.5.2. Удаленные подключения 236
 - 9.5.3. Настройка SSH на клиентской машине 239
 - 9.5.4. Настройка соединения 240
 - Резюме 241

Часть 4
БЕЗОПАСНОСТЬ КОНТЕЙНЕРОВ

- Глава 10. Изоляция контейнеров 244**
 - 10.1. Read-only псевдофайловые системы ядра Linux 246

10.1.1. Снятие маскировки с путей	248
10.1.2. Маскировка дополнительных путей	249
10.2. Linux-привилегии (Linux capabilities).....	250
10.2.1. Отключенные Linux-привилегии.....	251
10.2.2. Отключение привилегии CAP_SYS_ADMIN.....	253
10.2.3. Отказ от привилегий	253
10.2.4. Добавление привилегий.....	254
10.2.5. Отключение новых привилегий	255
10.2.6. Root без привилегий по-прежнему опасен	255
10.3. Изоляция UID: Пользовательское пространство имен	255
10.3.1. Изоляция контейнеров с использованием флага --userns=auto.....	256
10.3.2. Linux-привилегии пользовательского пространства имен	258
10.3.3. Rootless Podman с флагом --userns=auto	259
10.3.4. Пользовательские тома с флагом --userns=auto	260
10.4. Изоляция процессов: пространство имен PID.....	262
10.5. Сетевая изоляция: сетевое пространство имен	263
10.6. IPC-изоляция: пространство имен IPC	264
10.7. Изоляция файловой системы: пространство имен mount.....	265
10.8. Изоляция файловой системы: SELinux	266
10.8.1. SELinux type enforcement.....	266
10.8.2. Мультикатегорийное разделение SELinux	270
10.9. Изоляция системных вызовов seccomp.....	273
10.10. Изоляция виртуальных машин	275
Резюме	275
Глава 11. Дополнительные аспекты безопасности	276
11.1. Сравнение демона с моделью fork/exec	277
11.1.1. Доступ к docker.sock.....	277
11.1.2. Логирование и аудит	278

14 Оглавление

11.2. Работа с секретами в Podman	281
11.3. Доверие к образам Podman.....	282
11.3.1. Подписание образов в Podman.....	285
11.4. Сканирование образов	289
11.4.1. Контейнеры, доступные только для чтения	290
11.5. Глубокая защита.....	291
11.5.1. Podman использует все механизмы безопасности одновременно	291
11.5.2. Где следует запускать контейнеры?	292
Резюме	292

ПРИЛОЖЕНИЯ

Приложение А. Инструменты, связанные с Podman.....	294
А.1. Skopeo	296
А.2. Buildah.....	300
А.2.1. Создание рабочего контейнера из базового образа	301
А.2.2. Добавление данных в рабочий контейнер	302
А.2.3. Выполнение команд в рабочем контейнере	303
А.2.4. Добавление содержимого в рабочий контейнер напрямую с хоста.....	303
А.2.5. Конфигурирование рабочего контейнера.....	304
А.2.6. Создание образа из рабочего контейнера	306
А.2.7. Отправка образа в реестр контейнеров	306
А.2.8. Создание образа из Containerfile	307
А.2.9. Buildah как библиотека	308
А.3. CRI-O: Container Runtime Interface для контейнеров OCI.....	308
Приложение В. Среды выполнения OCI.....	310
В.1. runc	312
В.2. crun	314

В.3. Kata.....	315
В.4. gVisor	317
Приложение С. Установка Podman	319
С.1. Установка Podman.....	319
С.1.1. macOS.....	319
С.1.2. Windows.....	321
С.1.3. Arch Linux и Manjaro Linux	321
С.1.4. CentOS.....	321
С.1.5. Debian.....	322
С.1.6. Fedora	322
С.1.7. Fedora-CoreOS, Fedora Silverblue.....	322
С.1.8. Gentoo.....	322
С.1.9. OpenEmbedded	322
С.1.10. openSUSE.....	322
С.1.11. openSUSE Kubic	322
С.1.12. Raspberry Pi OS arm64.....	322
С.1.13. Red Hat Enterprise Linux	323
С.1.14. Ubuntu	323
С.2. Сборка Podman из исходного кода.....	323
С.3. Podman Desktop.....	323
Резюме	324
Приложение D. Участие в проекте Podman.....	325
D.1. Вступление в сообщество.....	325
D.2. Podman на github.com.....	327
Приложение E. Podman на macOS	328
E.1. Использование команд podman machine	330
E.1.1. podman machine init	330
E.1.2. Настройка SSH для машины Podman	332

16 Оглавление

E.1.3. Запуск виртуальной машины.....	334
E.1.4. Остановка виртуальной машины.....	335
Резюме	335
Приложение F. Podman в Windows	336
F.1. Первые шаги.....	337
F.1.1. Предварительные условия.....	338
F.1.2. Установка Podman.....	338
F.1.3. Автоматическая установка WSL	340
F.2. Использование команды podman machine.....	340
F.2.1. podman machine init	341
F.2.2. Настройка SSH в podman machine	343
F.2.3. Запуск экземпляра WSL 2	344
F.2.4. Использование команд podman machine.....	345
Резюме	348