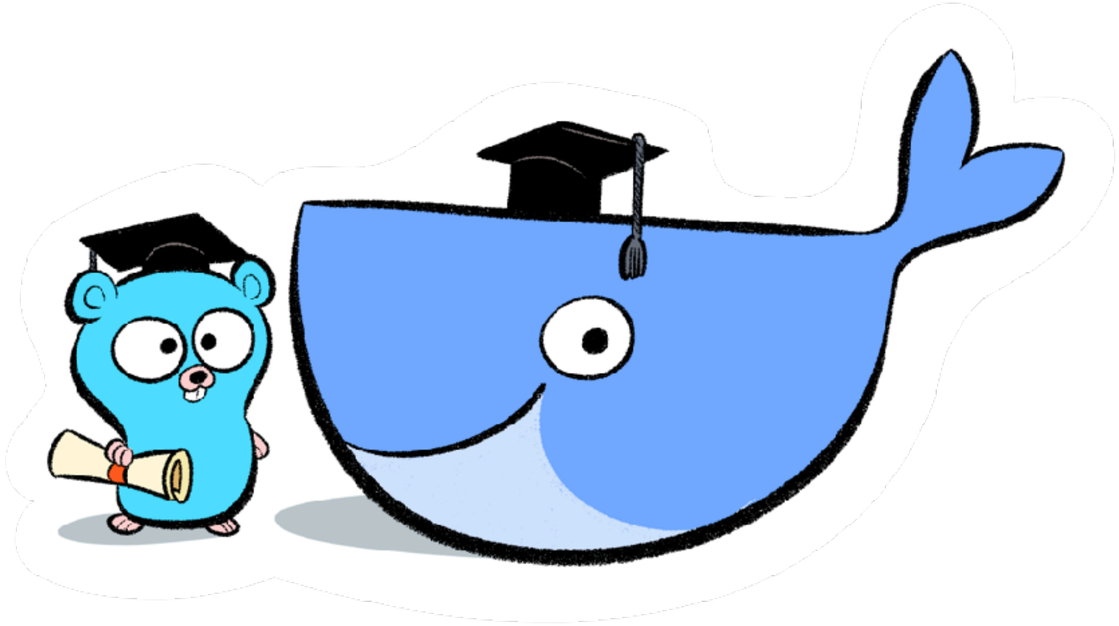


Введение в Docker

Олег Федосеев
olegfedoseev

docker
NOVOSIBIRSK

17 марта 2018

docker

Основные понятия

- Контейнеры
- Образы
- Хранение данных
- Сети
- Сервисы
- Секреты
- Swarm

docker

Что такое контейнер?

- Процесс в Linux-системе и его окружение
- С ограничениями по ресурсам (RAM, CPU, IO, Net)
- С ограниченным доступом и правами
- С Docker'ом в качестве супервизора

Что такое контейнер?

- **cgroups** для ресурсов (cpu, blkio, devices)
- **namespaces** для области видимости (pid, mnt, uts, user и т.д.)
- **AppArmor**, **seccomp**, **SELinux** и т.д. для ограничения прав и безопасности

Что такое контейнер?

```
$ docker run --help
Usage:  docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Run a command in a new container

Options:
      --add-host list              Add a custom host-to-IP mapping (host:ip) (default [])
  -a, --attach list                Attach to STDIN, STDOUT or STDERR (default [])
      --blkio-weight uint16        Block IO (relative weight), between 10 and 1000
      --blkio-weight-device list   Block IO weight (relative device weight) (default [])
      --cap-add list               Add Linux capabilities (default [])
      --cap-drop list              Drop Linux capabilities (default [])
      --cgroup-parent string       Optional parent cgroup for the container
      --cidfile string             Write the container ID to the file
      --cpu-period int             Limit CPU CFS (Completely Fair Scheduler) period
      --cpu-quota int              Limit CPU CFS (Completely Fair Scheduler) quota
      --cpu-rt-period int          Limit CPU real-time period in microseconds
      --cpu-rt-runtime int         Limit CPU real-time runtime in microseconds
  -c, --cpu-shares int             CPU shares (relative weight)
      --cpus decimal               Number of CPUs (default 0.000)
      --cpuset-cpus string         CPUs in which to allow execution (0-3, 0,1)
      --cpuset-mems string         MEMs in which to allow execution (0-3, 0,1)
  -d, --detach                     Run container in background and print container ID
      --detach-keys string         Override the key sequence for detaching a container
      --device list                Add a host device to the container (default [])
      --device-cgroup-rule list    Add a rule to the cgroup allowed devices list (default [])
```

Что такое образ?

- Окружение для процесса
- Файловая система, которую видит процесс
- Метаданные для контейнера
- **Образ это шаблон** для запуска контейнера

Особенности образов Docker'а

- Стандартизированный формат (OCI Image Format)
- Файловая система состоящая из слоёв дополняющих друг друга
- Можно собирать без Docker'а

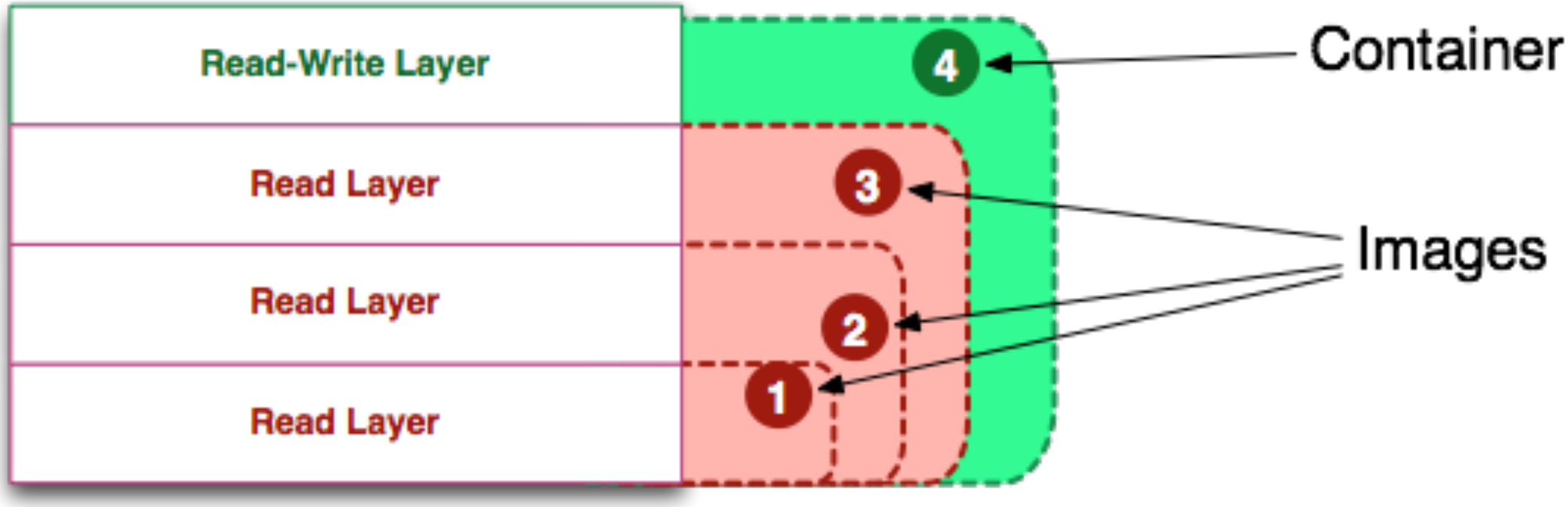
Dockerfile

```
FROM alpine:3.6

RUN apk add --no-cache mysql-client

ENTRYPOINT ["mysql"]
CMD ["--help"]
```

Образ и контейнер



Хранение данных и volume'ы

- Можно использовать локальную ФС
- Есть десятки плагинов для сетевых и не очень файловых систем
- Docker в процессе перехода на CSI, есть плагины дающие поддержку CSI

Хранение данных и volume'ы

```
$ docker container run \
    --mount type=bind,source=/path/on/host,target=/path/in/container \
    alpine
```

Хранение данных и volume'ы

```
$ docker container run \
    -v /path/on/host:/path/in/container \
    alpine
```

Сеть

- Container Network Model (CNM) и libnetwork
- Есть десятки плагинов
- Из коробки bridge, overlay, macvlan, ipvlan
- Встроенный DNS и service discovery для сервисов в Swarm

Сеть

- Проброс отдельных портов
- Полный доступ к хостовой сети
- Серый IP для внутренней сети
- Выделение отдельного IP-адреса на контейнер во внешней сети

Сеть

```
$ docker network create \
    --driver=overlay \
    --attachable=true \
    frontend

$ docker container run \
    --net frontend \
    --network-alias node1
    ...
    container-name
```

Сервисы и stack'и

- Сервис это набор одинаковых контейнеров
- Используется только вместе с Swarm
- Один общий VIP и хост в DNS на сервис
- Stack это набор сервисов, описывается в compose.yml

Сервисы и stack'и

```
$ docker service create --name opentsdb \
    --restart-condition on-failure --restart-max-attempts 5 --replicas 1 \
    --limit-memory 8G --limit-cpu 2.0 \
    --mount type=tmpfs,tmpfs-size=1G,destination=/tmp/opentsdb \
    --log-driver json-file --log-opt max-size=50m --log-opt max-file=10 \
    --label traefik.port=4242 --label traefik.frontend.rule=Host:tsdb.dev \
    --label traefik.docker.netwrok=traefik-net \
    --network traefik-net --network opentsdb --hostname opentsdb \
    -e TIMEZONE=Asia/Novosibirsk \
    olegfedoseev/opentsdb:2.3.0
```

Сервисы и stack'и

```
$ cat compose.yml

version: "3.1"
services:
  validator:
    image: swaggerapi/swagger-validator
    networks:
      - traefik-net
    deploy:
      mode: replicated
      replicas: 1
      restart_policy:
        condition: on-failure
      labels:
        - "traefik.port=8080"
        - "traefik.frontend.rule=Host:swagger-validator.dev"

networks:
  traefik-net:
    external: true
```

Сервисы и stack'и

```
$ docker stack deploy \
    --compose-file=compose.yaml \
    swagger-validator
```

docker stack vs docker-compose

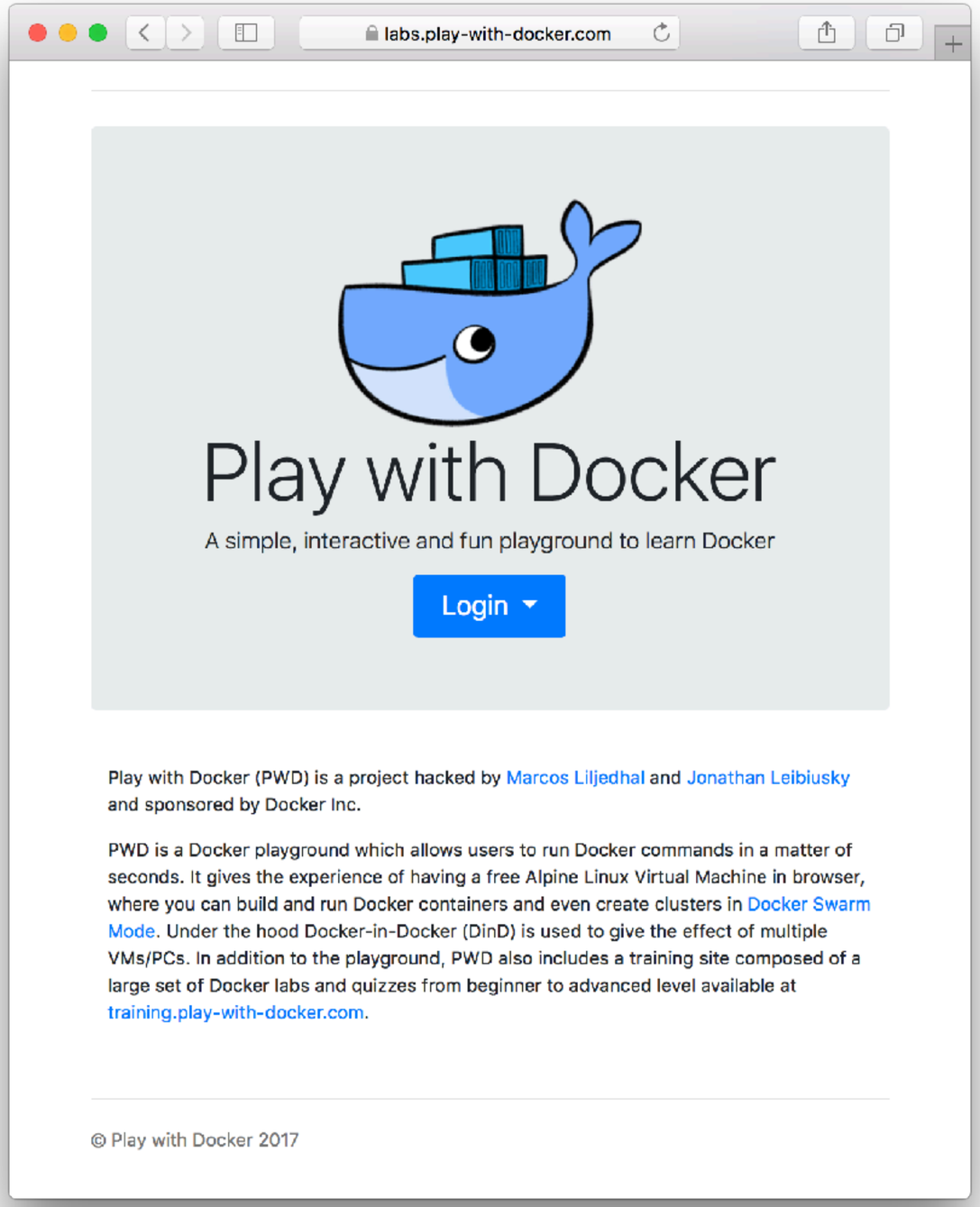
- Для использования сервисов и stack'а compose.yml должен быть версии 3+
- В compose.yml можно описать сборку образов, но команда **docker stack** их игнорирует
- **`docker-compose up`** для локального запуска dev-окружения, **`docker stack deploy`** для запуска продакшен-окружения в **swarm**

docker™

NOVOSIBIRSK

От теории к практике!

docker

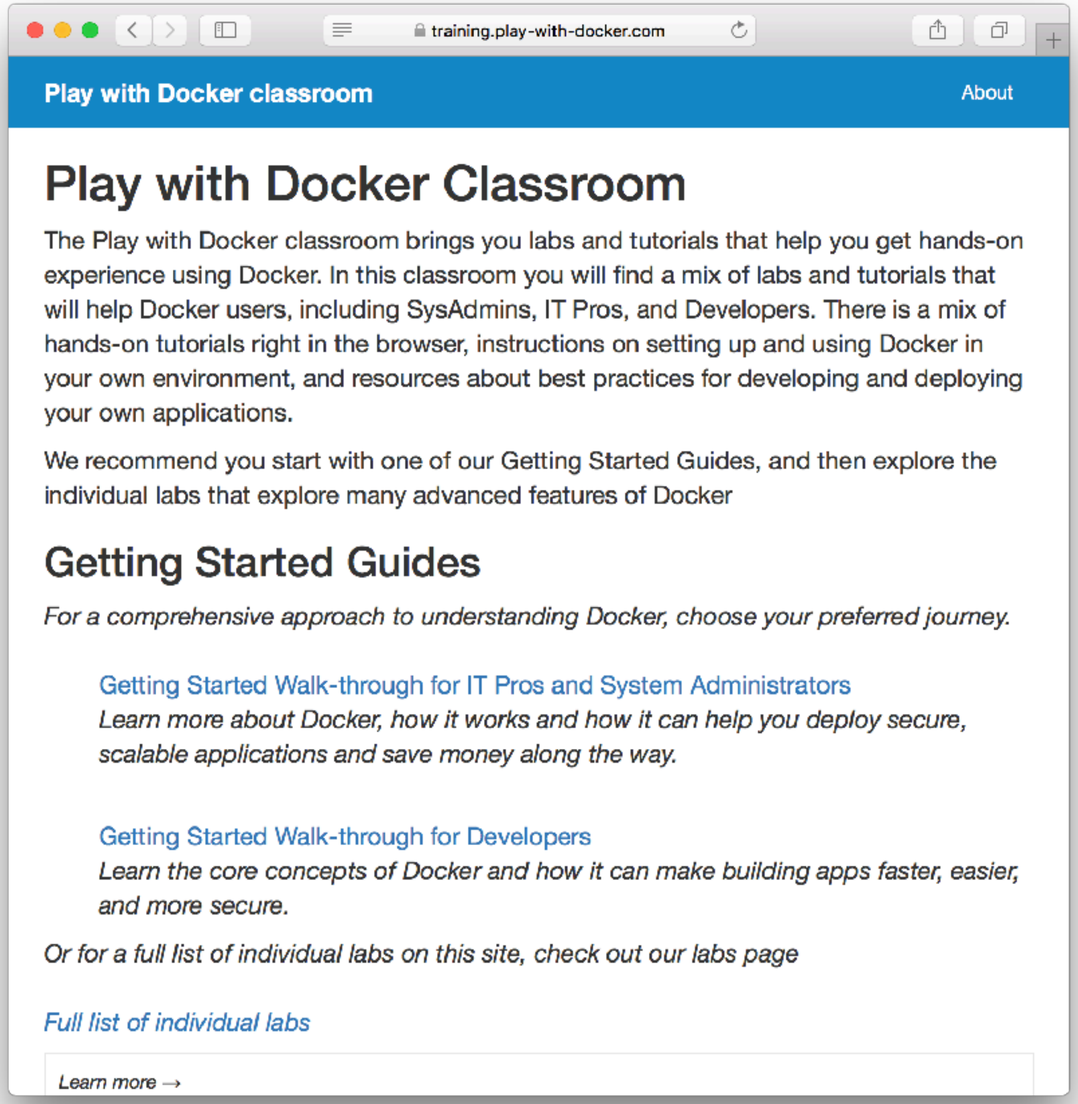


labs.play-with-docker.com

- Docker в браузере
- Требует авторизации через Docker ID или GitHub
- Можно делать кластера

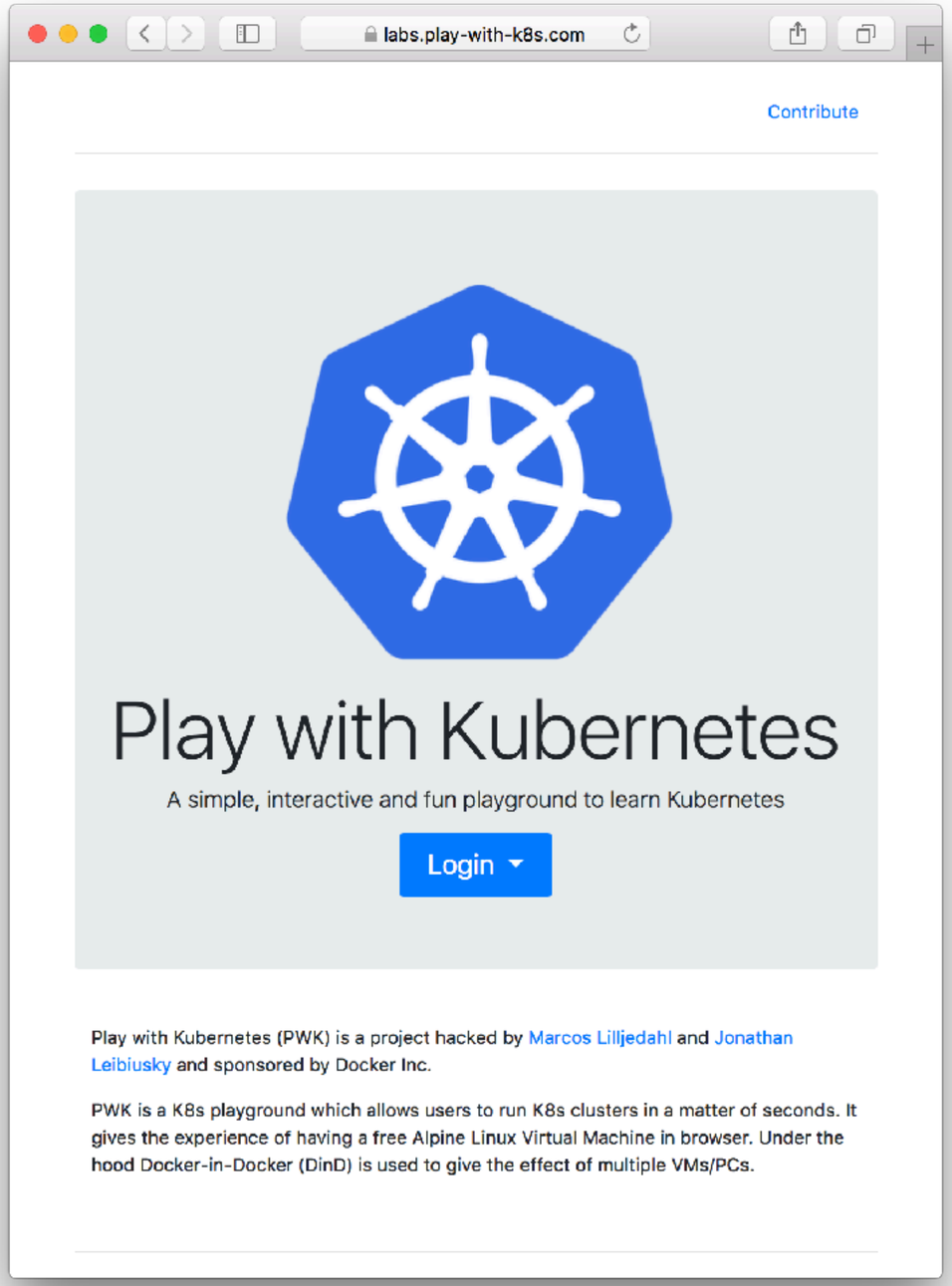
docker

training.play-with-docker.com



- Тот же Docker в браузере
- Требует авторизации через Docker ID или GitHub
- Множество разных интерактивных “уроков” на разные уровни и темы
- https://training.play-with-docker.com/alacart/

docker

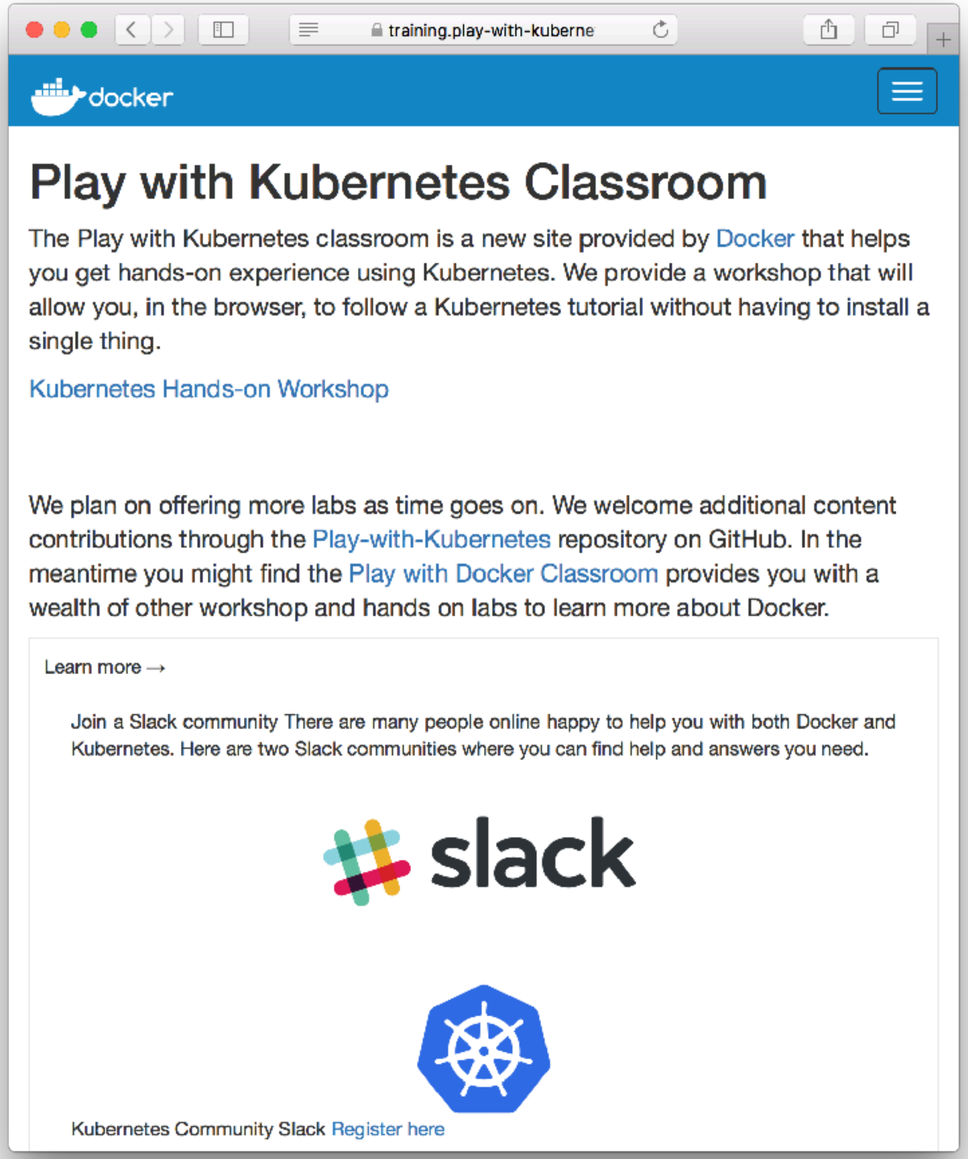


labs.play-with-k8s.com

- Kubernetes в браузере
- Требует авторизации через Docker ID или GitHub

docker

training.play-with-kubernetes.com



- Тот же Kubernetes в браузере
- Требует авторизации через Docker ID или GitHub
- Множество разных интерактивных “уроков” на разные уровни и темы
- https://training.play-with-kubernetes.com

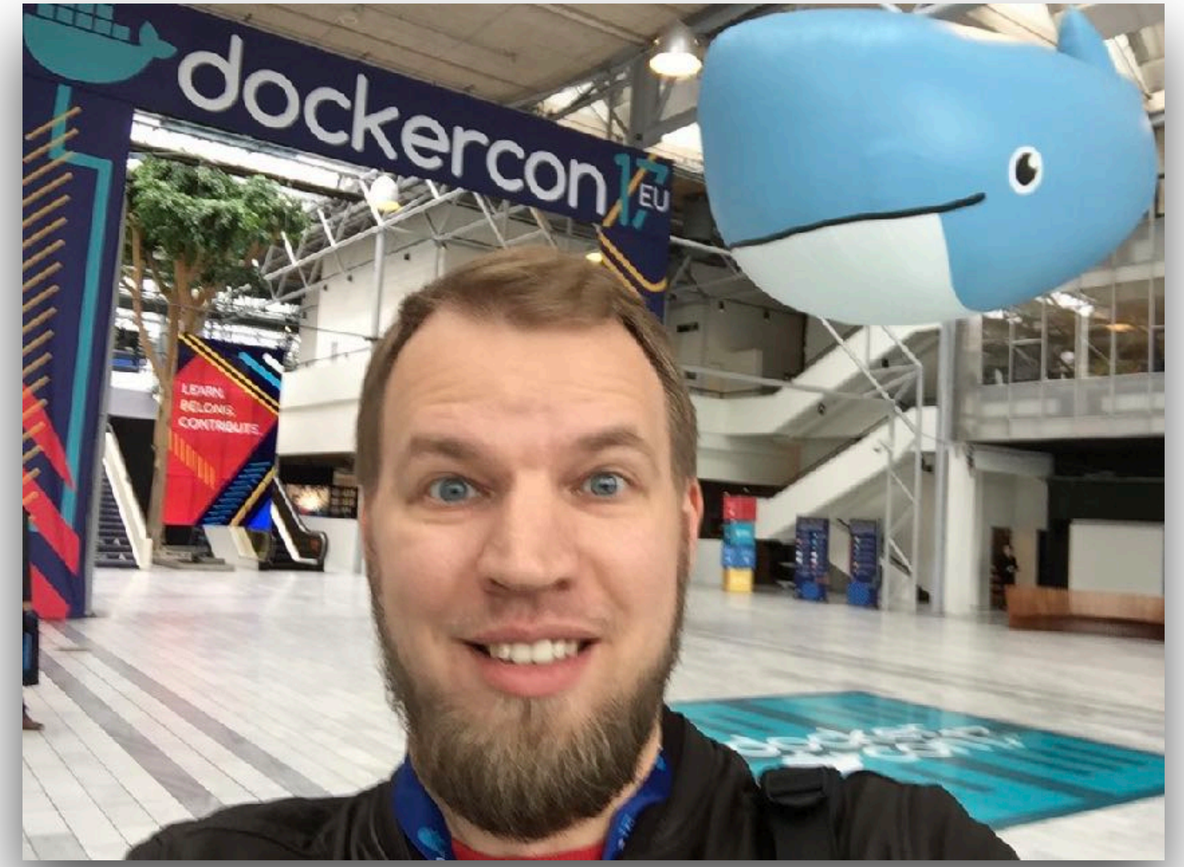
docker

Ссылки

- https://training.play-with-docker.com - уроки по Docker'у
- https://training.play-with-kubernetes.com - уроки по Kubernetes
- https://github.com/docker/labs - официальные примеры для обучения от Docker
- https://container.training/ - много слайдов и видео с подробных курсов от Jérôme Petazzoni

docker
NOVOSIBIRSK

docker



Вопросы?

Олег Федосеев
olegfedoseev
t.me/olegfedoseev
oleg.fedoseev@me.com

docker
NOVOSIBIRSK

docker