Продакшн-образы Docker

Сборка production-образа для мини-сервиса на Flask

Требования:

- Размер образа **< 150 MB**.
- Есть **HEALTHCHECK** (проверяет `GET /health`).
- Запуск под **не-root** пользователем (`USER`).
- Корректное завершение по **SIGTERM**.
- Контейнер можно запускать на `--read-only`.
- Переменная окружения `ROCKET_SIZE` влияет на ответ `/` **без пересборки**.
- В **LABEL** должны быть:
    - `org.lab.login=<ваш_dockerhub_login>`
    - `org.lab.token=<token>` (из вашего seed-файла)

---

1. Локальная сборка prod-образа

```
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ SEED_JSON=seed-dianaponomareva.json
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ LOGIN=$(jq -r .login "$SEED_JSON")
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ TOKEN=$(jq -r .token  "$SEED_JSON")
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ PREFIX=$(jq -r .prefix "$SEED_JSON")
```

```
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker build  --build-arg LAB_LOGIN="$LOG
IN"  --build-arg LAB_TOKEN="$TOKEN"  -t "$LOGIN/image-lab:$PREFIX" .
[+] Building 1.8s (16/16) FINISHED                                             docker:default
 => [internal] load build definition from Dockerfile                                    0.0s
 => => transferring dockerfile: 886B                                                    0.0s
 => [internal] load metadata for docker.io/library/python:3.12-alpine                   0.0s
 => [internal] load .dockerignore                                                       0.0s
 => => transferring context: 107B                                                       0.0s
 => [builder 1/4] FROM docker.io/library/python:3.12-alpine@sha256:02a73ead8397e904cea6d17e18516f1df3590e05dc8823  0.0s
 => => resolve docker.io/library/python:3.12-alpine@sha256:02a73ead8397e904cea6d17e18516f1df3590e05dc8823bd5b1c7f   0.0s
 => [internal] load build context                                                       0.0s
 => => transferring context: 90B                                                        0.0s
 => CACHED [stage-1 2/8] RUN apk add --no-cache curl                                     0.0s
 => CACHED [stage-1 3/8] RUN addgroup -S appuser && adduser -S appuser -G appuser        0.0s
 => [stage-1 4/8] RUN mkdir -p /app && chown appuser:appuser /app                        0.2s
 => CACHED [builder 2/4] RUN apk add --no-cache gcc musl-dev python3-dev                 0.0s
 => CACHED [builder 3/4] COPY requirements.txt .                                         0.0s
 => CACHED [builder 4/4] RUN pip install --no-cache-dir -r requirements.txt              0.0s
 => [stage-1 5/8] WORKDIR /app                                                           0.0s
 => [stage-1 6/8] COPY --from=builder /usr/local/lib/python3.12/site-packages/ /usr/local/lib/python3.12/site-pac  0.4s
 => [stage-1 7/8] COPY --from=builder /usr/local/bin/ /usr/local/bin/                    0.0s
 => [stage-1 8/8] COPY --chown=appuser:appuser app/ ./                                   0.0s
 => exporting to image                                                                   0.7s
 => => exporting layers                                                                  0.4s
 => => exporting manifest sha256:ca54d88210453f4fda0b154ff5b9e83e859a16e730a49b2fb0fe4d6c3dea21b5   0.0s
 => => exporting config sha256:1a02f02f8a4018a28311d7b05d9037fba17f874140da9037faaed7942f34d1e6     0.0s
 => => exporting attestation manifest sha256:062dfb9a6d9de01e0749cf16fba413534d5eae4fe6dbe95b00c5a4c2122343b5       0.0s
 => => exporting manifest list sha256:2c1b44e5bdcbe037054a9561a02864b07dbb47a4760bd31d6612876ca39c3d45             0.0s
 => => naming to docker.io/dianaponomareva/image-lab:285f8025                            0.0s
 => => unpacking to docker.io/dianaponomareva/image-lab:285f8025                         0.2s
```

2. Локальная проверка (быстро)

```
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker run -d --rm --read-only -e ROCKET_S
IZE=Big -p 8080:8000 "$LOGIN/image-lab:$PREFIX"
23d62b962a1afe861871960bfd4102ae0135fb18072a083d327d5581e8e03e50
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker ps --format "table {{.Names}}\t{{.P
orts}}"
NAMES          PORTS
goofy_golick   0.0.0.0:8080->8000/tcp, [::]:8080->8000/tcp
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ curl -s http://localhost:8080/health
{"status":"ok","uptime":112.04}
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ curl -s http://localhost:8080/
Hello from Docker! Rocket=Big
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker exec 23d62b962a1a touch /test.txt
touch: /test.txt: Read-only file system
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$
```

Не защищено | localhost:8080   localhost:8080

Hello from Docker! Rocket=Big

```
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker images
REPOSITORY                    TAG        IMAGE ID       CREATED          SIZE
dianaponomareva/image-lab     285f8025   2c1b44e5bdcb   9 minutes ago    97.2MB
```

3. Публикация в Docker Hub

```
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker login
Authenticating with existing credentials... [Username: dianaponomareva]

i Info → To login with a different account, run 'docker logout' followed by 'docker login'


Login Succeeded
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker push "$LOGIN/image-lab:$PREFIX"
The push refers to repository [docker.io/dianaponomareva/image-lab]
1e894ae96196: Mounted from library/python
c8b256b33da3: Pushed
ebcc377cac3c: Pushed
a8068aa9c171: Pushed
e830ac31321a: Pushed
4f4fb700ef54: Mounted from library/redis
9824c27679d3: Mounted from docker/welcome-to-docker
2be5d4a24bdd: Mounted from library/python
bd0b3be187e3: Mounted from library/python
9132eed28c5c: Pushed
277f2d0dbd71: Pushed
b65ac3f1898f: Pushed
285f8025: digest: sha256:2c1b44e5bdcbe037054a9561a02864b07dbb47a4760bd31d6612876ca39c3d45 size: 856
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$
```

4. Вывод docker history

```
diana@LAPTOP-VFHN5IBT:~$ cd /mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ SEED_JSON=seed-dianaponomareva.json
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ LOGIN=$(jq -r .login "$SEED_JSON")
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ PREFIX=$(jq -r .prefix "$SEED_JSON")
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$ docker history "$LOGIN/image-lab:$PREFIX"
IMAGE          CREATED        CREATED BY                                      SIZE      COMMENT
2c1b44e5bdcb   6 hours ago    CMD ["python" "app.py"]                         0B        buildkit.dockerfile.v0
<missing>      6 hours ago    HEALTHCHECK &{["CMD-SHELL" "curl -f http://l…   0B        buildkit.dockerfile.v0
<missing>      6 hours ago    ENV ROCKET_SIZE=Medium                          0B        buildkit.dockerfile.v0
<missing>      6 hours ago    USER appuser                                    0B        buildkit.dockerfile.v0
<missing>      6 hours ago    COPY --chown=appuser:appuser app/ ./ # build…   12.3kB    buildkit.dockerfile.v0
<missing>      6 hours ago    COPY /usr/local/bin/ /usr/local/bin/ # build…   24.6kB    buildkit.dockerfile.v0
<missing>      6 hours ago    COPY /usr/local/lib/python3.12/site-packages…   11.9MB    buildkit.dockerfile.v0
<missing>      6 hours ago    WORKDIR /app                                    4.1kB     buildkit.dockerfile.v0
<missing>      6 hours ago    RUN |2 LAB_LOGIN=dianaponomareva LAB_TOKEN=2…   8.19kB    buildkit.dockerfile.v0
<missing>      16 hours ago   RUN |2 LAB_LOGIN=dianaponomareva LAB_TOKEN=2…   41kB      buildkit.dockerfile.v0
<missing>      16 hours ago   LABEL org.lab.token=285f8025407781bf6fb07abc…   0B        buildkit.dockerfile.v0
<missing>      16 hours ago   LABEL org.lab.login=dianaponomareva             0B        buildkit.dockerfile.v0
<missing>      16 hours ago   ARG LAB_TOKEN=285f8025407781bf6fb07abcacc15e…   0B        buildkit.dockerfile.v0
<missing>      16 hours ago   ARG LAB_LOGIN=dianaponomareva                   0B        buildkit.dockerfile.v0
<missing>      16 hours ago   RUN /bin/sh -c apk add --no-cache curl # bui…   5.31MB    buildkit.dockerfile.v0
<missing>      2 months ago   CMD ["python3"]                                 0B        buildkit.dockerfile.v0
<missing>      2 months ago   RUN /bin/sh -c set -eux;  for src in idle3 p…   16.4kB    buildkit.dockerfile.v0
<missing>      2 months ago   RUN /bin/sh -c set -eux;   apk add --no-cach…   44MB      buildkit.dockerfile.v0
<missing>      2 months ago   ENV PYTHON_SHA256=c30bb24b7f1e9a19b11b55a546…   0B        buildkit.dockerfile.v0
<missing>      2 months ago   ENV PYTHON_VERSION=3.12.11                      0B        buildkit.dockerfile.v0
<missing>      2 months ago   ENV GPG_KEY=7169605F62C751356D054A26A821E680…   0B        buildkit.dockerfile.v0
<missing>      2 months ago   RUN /bin/sh -c set -eux;   apk add --no-cache…  2.98MB    buildkit.dockerfile.v0
<missing>      2 months ago   ENV LANG=C.UTF-8                                0B        buildkit.dockerfile.v0
<missing>      2 months ago   ENV PATH=/usr/local/bin:/usr/local/sbin:/usr…   0B        buildkit.dockerfile.v0
<missing>      2 months ago   CMD ["/bin/sh"]                                 0B        buildkit.dockerfile.v0
<missing>      2 months ago   ADD alpine-minirootfs-3.22.1-x86_64.tar.gz /…   8.98MB    buildkit.dockerfile.v0
diana@LAPTOP-VFHN5IBT:/mnt/c/me/programs/OS_labs/OS-labs/02_docker_image_lab$
```

5. Отчет:

Данный Dockerfile реализует многостадийную сборку, исключая инструменты компиляции из финального образа и сокращая его размер на сотни мегабайт. Использование минимального базового образа Alpine Linux и флагов `--no-cache` радикально уменьшает поверхность для атак и итоговый объем. Кэширование слоев достигается за счет раздельного копирования зависимостей и кода, что ускоряет повторные сборки. Безопасность обеспечивается запуском от имени непривилегированного пользователя и корректными правами доступа, а встроенный HEALTHCHECK с curl контролирует работоспособность. В совокупности эти подходы создают оптимизированный, безопасный и эффективный контейнер, превосходящий наивную сборку по многим важным параметрам.