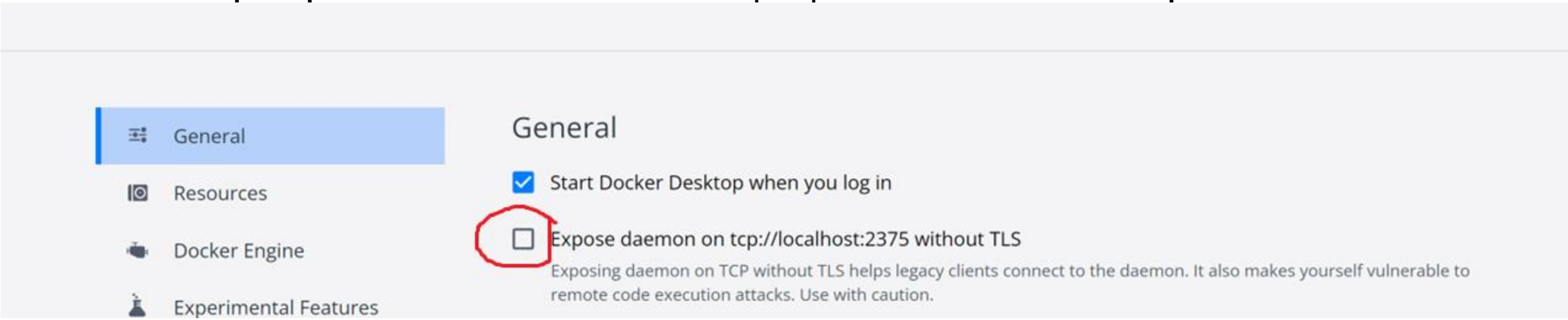
Docker security cheat sheets

Как обеспечить безопасность контейнеров?

Неавторизированный доступ к Docker

- Не пробрасывать Docker незащещённый daemon порт



~~volumes:~~
~~- "/var/run/docker.sock:/var/run/docker.sock"~~

Run always as Non root

- Запуск от рута внутри Docker контейнера – плохо

```
FROM alpine
RUN groupadd -r myuser && useradd -r -g myuser myuser
<HERE DO WHAT YOU HAVE TO DO AS A ROOT USER LIKE INSTALLING PACKAGES ETC.>
USER myuser
```

Лимиты на ресурсы

```
➜  ~ docker run --memory 50m --memory-swap 50m --rm -it progrium/stress --vm 1 --vm-bytes 62914560 --timeout 1s
stress: info: [1] dispatching hogs: 0 cpu, 0 io, 1 vm, 0 hdd
stress: dbug: [1] using backoff sleep of 3000us
stress: dbug: [1] setting timeout to 1s
stress: dbug: [1] --> hogvm worker 1 [6] forked
stress: dbug: [6] allocating 62914560 bytes ...
stress: dbug: [6] touching bytes in strides of 4096 bytes ...
stress: FAIL: [1] (416) <-- worker 6 got signal 9
stress: WARN: [1] (418) now reaping child worker processes
stress: FAIL: [1] (422) kill error: No such process
stress: FAIL: [1] (452) failed run completed in 0s
```

Всегда read only

- Запускать контейнер, даже с монтированной файловой системой как read-only

```
docker run --read-only alpine sh -c 'echo "whatever" > /tmp'
```

Используйте статичные анализаторы контейнера

- Бесплатные:
  - https://github.com/quay/clair
  - https://github.com/deepfence/ThreatMapper
  - https://github.com/aquasecurity/trivy
- Платные:
  - https://github.com/aquasecurity/microscanner
  - https://jfrog.com/xray/
  - https://www.qualys.com/apps/container-security/
  - https://anchore.com/opensource/
  - https://snyk.io/

Логи

- Устанавливать уровень логгирования на INFO

```
docker-compose --log-level info up
```