?????????

Официальный сайт

Docker:

Для 26 версии:

```
docker run
    -p 8080:8080
    -e KC_BOOTSTRAP_ADMIN_USERNAME=admin
    -e KC_BOOTSTRAP_ADMIN_PASSWORD=admin
    quay.io/keycloak/keycloak:26.2.5 start-dev
```

Для 22 версии:

```
 docker run
    -e KEYCLOAK_ADMIN=admin
    -e KEYCLOAK_ADMIN_PASSWORD=admin
    -p 8080:8080 quay.io/keycloak/keycloak:22.0.0
    start-dev
```

Можно еще напрямую через JDK.

Упрощенный compose

```
services:
  keycloak:
    image: quay.io/keycloak/keycloak:26.3.2
    container_name: keycloak
    environment:
      KC_BOOTSTRAP_ADMIN_USERNAME: admin
      KC_BOOTSTRAP_ADMIN_PASSWORD: SecretPassword123
    ports:
      - '0.0.0.0:8180:8080'
    command: start-dev
    volumes:
      - ~/kk/data:/opt/keycloak/data
```

Для хранения данных либо встроенная база (H2), либо нужно отдельно поднять postgresql:

Обязательно изменить константу KC_HOSTNAME, происходит перенаправление

```
services:
  postgres:
    image: postgres:15
    container_name: keycloak_postgres
    environment:
      POSTGRES_DB: keycloak
      POSTGRES_USER: keycloak
      POSTGRES_PASSWORD: keycloak
    ports:
      - "5433:5432"
    volumes:
      - ./postgres_data:/var/lib/postgresql/data
    networks:
      - keycloak_net

  keycloak:
    image: quay.io/keycloak/keycloak:26.2
    container_name: keycloak
    command: start-dev
    environment:
      KC_DB: postgres
      KC_DB_URL_HOST: postgres
      KC_DB_URL_DATABASE: keycloak
      KC_DB_USERNAME: keycloak
      KC_DB_PASSWORD: keycloak
      KC_HOSTNAME: localhost
      KEYCLOAK_ADMIN: admin
      KEYCLOAK_ADMIN_PASSWORD: admin
    ports:
      - "9090:8080"
    depends_on:
      - postgres
    networks:
      - keycloak_net

networks:
```

```
  keycloak_net:
```

Dev / prod режимы

Параметр start-dev запускает в режиме dev, предназначен для локальной разработки и тестирования.

- Упрощенный запуск: автоматически применяются настройки, не требующие сложной конфигурации.
- Включён HTTP: можно запускать без HTTPS.
- Отключена проверка сертификатов: удобно для работы с самоподписанными сертификатами.
- Включены developer-friendly endpoints: например, доступ к /admin API может быть менее защищен.
- Более подробные логи: включая stack trace.
- Слабые требования к паролям и политике безопасности.
- Нет ограничений на CORS и Content-Security-Policy, если не заданы явно.

prod - предназначен для развертывания в боевой среде.

- Требуется HTTPS: нельзя запустить без конфигурации TLS.
- Политики безопасности применяются строго (например, CSP, CORS, защита от CSRF).
- Проверка конфигурации при старте: ошибки в настройке вызовут отказ запуска.
- Пароли и другие секреты не должны быть слабыми.
- Отключены "удобные" фичи, потенциально опасные в проде (dev endpoints и т.д.).
- Подразумевается использование внешней базы данных (а не H2).
- Повышенные требования к производительности и отказоустойчивости.

Revision #4
Created 2 June 2025 05:10:17 by Admin
Updated 10 April 2026 17:39:08 by Admin