سامانه کاتب

نصب و راه اندازی keycloak

در این سند طریقه نصب و تنظیم نرم افزار keycloak جهت راه اندازی سیستم احراز هویت کاربران شرح داده شده است.

نکته: برای آشنایی بیشتر با این ابزار و معماری آن و ساختار سیستم های مبتنی بر sso می‌توانید به سند (SSO_solution) مراجعه فرمایید.

۱- نصب و اجرا

۱-۱- ایجاد docker-compose

در این حالت از postgres برای دیتابیس داده های ساخته شده توسط keycloak استفاده می‌شود مانند: کاربران و گروه ها و قلمرو های ساخته شده در خود نرم افزار.

keycloak یک دیتابیس ساده و داخلی نیز دارد ولی پیشنهاد می‌شود در محیط های عملیاتی از دیتابیسی مجزا و پیشرفته استفاده شود.

```yaml
version: '3.8'

services:
  postgres:
    image: postgres:latest
    container_name: postgres-sso
    restart: always
    environment:
      POSTGRES_DB: ${POSTGRES_DB}
      POSTGRES_USER: ${POSTGRES_USER}
      POSTGRES_PASSWORD: ${POSTGRES_PASSWORD}
    ports:
      - '5432:5432'
    volumes:
      - ./keycloak_data/postgres:/var/lib/postgresql/data
    networks:
      - keycloak-network

  keycloak:
    image: quay.io/keycloak/keycloak:latest
    container_name: keycloak-sso
    restart: always
    environment:
      DB_VENDOR: ${DB_VENDOR}
      DB_ADDR: ${DB_ADDR}
      DB_DATABASE: ${DB_DATABASE}
      DB_USER: ${DB_USER}
      DB_PASSWORD: ${DB_PASSWORD}
      KEYCLOAK_ADMIN: ${KEYCLOAK_ADMIN}
      KEYCLOAK_ADMIN_PASSWORD: ${KEYCLOAK_ADMIN_PASSWORD}
      KC_HTTPS_CERTIFICATE_FILE: /etc/keycloak/certs/tls.crt.pem
      KC_HTTPS_CERTIFICATE_KEY_FILE: /etc/keycloak/certs/tls.key.pem
    command: ["start-dev", "--http-port", "8080", "--https-port", "8443"]
    ports:
      - "8080:8080"
      - "8443:8443"
```

```
    volumes:
      - ./keycloak_data/certs:/etc/keycloak/certs
    depends_on:
      - postgres
    networks:
      - keycloak-network

networks:
  keycloak-network:
    driver: bridge
```

پس از ایجاد این compose file در یک مسیر دلخواه فایل مورد نیاز متغیر های محیطی آن را نیز در کنار فایل با نام .env ایجاد کنید. درون این فایل نام های کاربری و رمز های عبور keycloak و postgres قرار دارد.

```
POSTGRES_DB=keycloak
POSTGRES_USER=keycloak
POSTGRES_PASSWORD=password

DB_VENDOR=postgres
DB_ADDR=postgres
DB_DATABASE=keycloak
DB_USER=keycloak
DB_PASSWORD=password

KEYCLOAK_ADMIN=admin
KEYCLOAK_ADMIN_PASSWORD=admin
```

بعد از ساخت هر دو فایل اقدام به اجرای آن کنید:

```
docker-compose -f <file.yml> up -d
```

پس از ایجاد دایرکتوری داده های keycloak در مسیر جاری می‌توان در دایرکتوری certs فایل های key و crt خود را قرار دهید.

> **نکته: keycloak فقط از فایل‌هایی با فرمت .pem پشتیبانی می‌کند.**

```
./keycloak_data/
├── certs/
│   ├── tls.crt.pem    # certificate
│   └── tls.key.pem    # Private key
└── postgres/
```

سپس سطح دسترسی هر دو فایل را تغییر دهید تا در دسترس سرویس نرم افزار باشند.

```
chmod 644 tls.*.pem
```

پس از اضافه کردن certificate کانتینر keycloak را ری استارت کنید تا تغییرات اعمال شود، بعد از این کار

۱-۱-۱ کاربرد آزمایشگاهی

در مدل های تستی و آزمایشگاهی می‌توان بدون دسترسی به https نیز از نرم افزار استفاده کرد. برای این منظور قبل از اجرای فایل compose متغیر های مربوط به https را کامنت کنید.

```
      # KC_HTTPS_CERTIFICATE_FILE: /etc/keycloak/certs/tls.crt.pem
      # KC_HTTPS_CERTIFICATE_KEY_FILE: /etc/keycloak/certs/tls.key.pem
```

و پس از اجرا وارد کانتینر keycloak شده و در مسیر ذکر شده اقدام به اجرای دستورات کنید. در زمان اجرا رمز عبور تعریف شده برای کاربر admin درخواست می‌شود که مطابق فایل .env برابر مقدار ذکر شده در آن است.

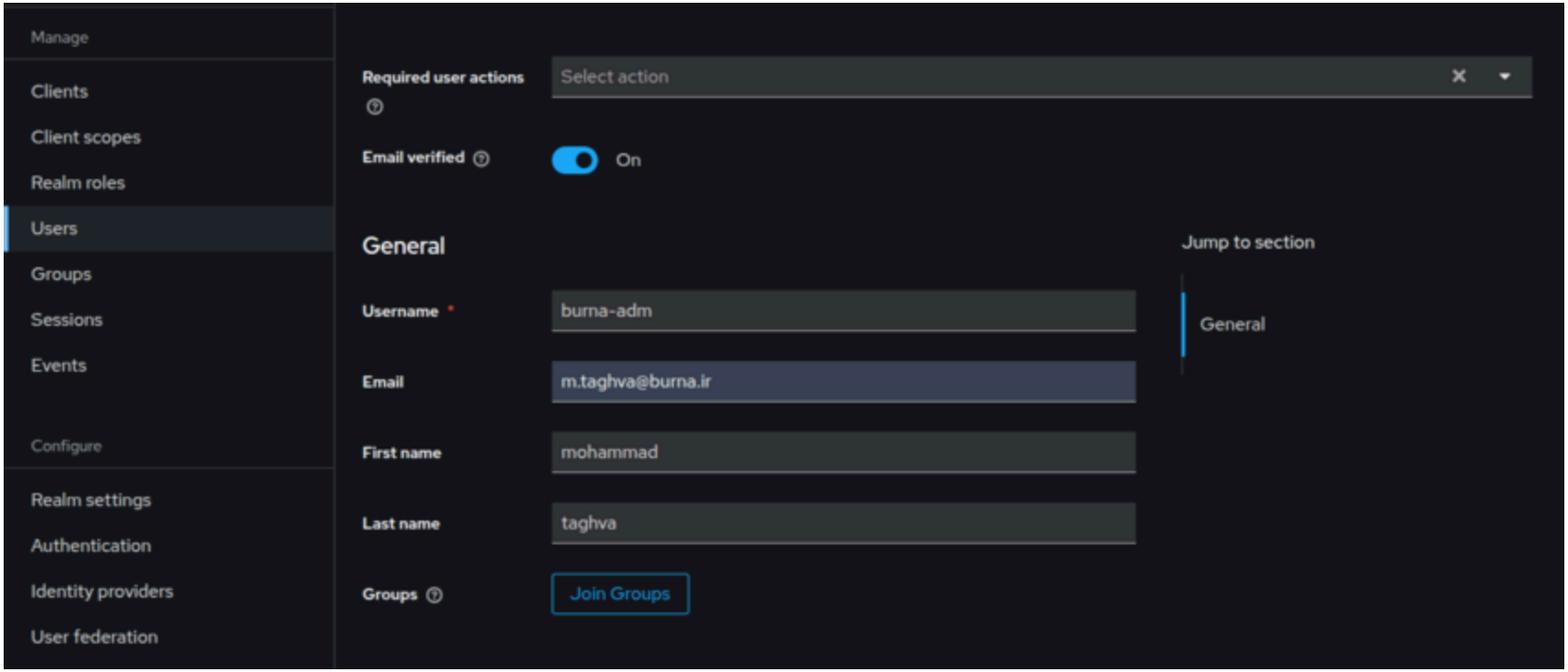
```
docker exec -it -u root keycloak-sso bash
cd /opt/keycloak/bin
./kcadm.sh config credentials --server http://localhost:8080 --realm master --user admin
./kcadm.sh update realms/master -s sslRequired=NONE
```

۱-۲- تنظیمات اولیه

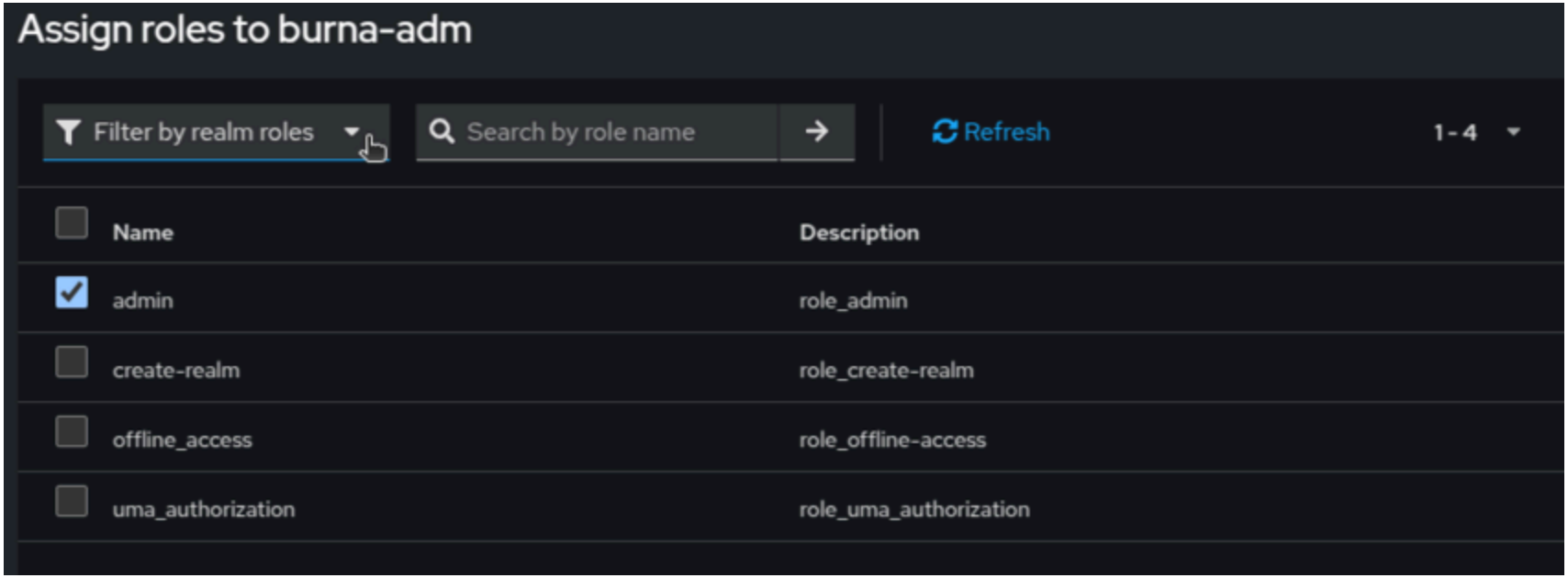
پس از انجام مراحل قبل پنل وب نرم افزار در آدرسی مشابه در دسترس است: **https://<IP or domain>:8443/admin** یا **http://<IP or domain>:8080/admin**

برای login بار اول می‌توان از user و pass موقت ذکر شده در فایل .env استفاده کرد ولی پس از آن باید کاربر ادمین اصلی را مشابه روند زیر تعریف کرد.

۱- پس از اولین ورود به realm master به تب client رفته و کاربر ادمین جدید را ایجاد کنید. مشابه تصویر:



۲- بعد از ایجاد کاربر در بخش تنظیمات آن در قسمت role mapping با استفاده گزینه assign role به منو نقش های موجود رفته و تغییر فیلتر به realm roles دسترسی به نقش ادمین را فعال کنید. مشابه تصویر:



حال می‌توان از حساب کاربری موقت خارج شد و با ادمین جدید مجدد وارد شد و کاربر ادمین موقت را از لیست کاربران حذف کرد.

برگرفته از «https://kateb.burna.ir/w/index.php?title=نصب_و_راه_اندازی_keycloak&oldid=106791»

مشارکت‌کنندگان:محمد تقوا (100),

مشاهده‌گر: محمد تقوا (۱۱)

▪