

Traefik with OID Keycloak

```
version: '2'

networks:
  traefik:
    name: traefik

volumes:
  docker_networking_keycloak_postgresdata:
    external: true
  docker_networking_traefik_acme:
    external: true
  docker_networking_traefik_rules:
    external: true
  docker_networking_traefik_logs:
    external: true
  docker_networking_keycloak_postgresbackup:
    external: true

services:
  traefik:
    image: traefik
    restart: always
    networks:
      - traefik
    command:
      - --pilot.token=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      - --entrypoints.web.address=:80
      - --entrypoints.websecure.address=:443
      - --entryPoints.ws.address=:8081
      - --entryPoints.wss.address=:8083
      - --providers.docker
      - --providers.docker.exposedByDefault=false
      - --providers.file.directory=/config/
      - --api
      - --log.filePath=logs/log.txt
```

- ```
- --log.format=json
- --log.level=DEBUG
- --accesslog=true
- --accesslog.filepath=/logs/access.log
- --certificatesresolvers.leresolver.acme.email=xxxxxxxxxxxxx@mail.com
- --certificatesresolvers.leresolver.acme.storage=/acme/acme.json
- --certificatesresolvers.leresolver.acme.dnschallenge=true
- --certificatesresolvers.leresolver.acme.dnschallenge.provider=namedotcom
- --certificatesresolvers.leresolver.acme.dnschallenge.resolvers=163.114.216.17
```

environment:

- [illegible]

```
ports:
```

- "80:80"
- "443:443"
- "8081:8081"
- "8083:8083"

volumes:

- "/var/run/docker.sock:/var/run/docker.sock:ro"
- docker\_networking\_traefik\_logs:/logs/
- docker\_networking\_traefik\_acme:/acme/
- docker\_networking\_traefik\_rules:/config/

labels:

## # Dashboard

- "traefik.enable=true"
- "traefik.http.routers.traefik.rule=Host(`traefik.domain.com`)"
- "traefik.http.routers.traefik.service=api@internal"
- "traefik.http.routers.traefik.entrypoints=websecure"
- "traefik.http.routers.traefik.middlewares=traefik-forward-auth"
- "traefik.http.routers.traefik.tls=true"

```
global redirect to https
```

- ```
- "traefik.http.routers.http-catchall.rule=hostregexp(`{host:.+}`)"
- "traefik.http.routers.http-catchall.entrypoints=web"
- "traefik.http.routers.http-catchall.middlewares=redirect-to-https"
```

```
# middleware redirect
```

- ```
- "traefik.http.middlewares.redirect-to-https.redirectscheme.scheme=https"
```

# traefik network

- "traefik.docker.network=traefik"

# global wildcard certificates

- 'traefik.http.routers.wildcard-certs.tls.certresolver=leresolver'

- 'traefik.http.routers.wildcard-certs.tls.domains[0].main=domain.com'

- 'traefik.http.routers.wildcard-certs.tls.domains[0].sans=\*.domain.com'

extra\_hosts:

- host.docker.internal:172.1.1.1

keycloak:

image: mihaibob/keycloak:15.0.1

restart: always

labels:

- "traefik.enable=true"

- "traefik.http.routers.keycloak.rule=Host(`keycloak.domain.com`)"

- "traefik.http.routers.keycloak.entrypoints=websecure"

- "traefik.http.routers.keycloak.tls=true"

- "traefik.http.services.keycloak.loadBalancer.server.port=8080"

- "traefik.docker.network=traefik"

networks:

- traefik

environment:

- KEYCLOAK\_USER=admin

- KEYCLOAK\_PASSWORD=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

- PROXY\_ADDRESS\_FORWARDING=true

- KEYCLOAK\_HOSTNAME=keycloak.domain.com

- DB\_VENDOR=POSTGRES

- DB\_ADDR=postgres

- DB\_DATABASE=keycloak

- DB\_USER=keycloak

- DB\_SCHEMA=public

- DB\_PASSWORD=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

depends\_on:

- postgres

postgres:

user: "65534:100"

image: postgres:13.4

restart: unless-stopped

volumes:

- docker\_networking\_keycloak\_postgresdata:/var/lib/postgresql/data

environment:

- PGDATA=/var/lib/postgresql/data/keycloak
- POSTGRES\_DB=keycloak
- POSTGRES\_USER=keycloak
- POSTGRES\_PASSWORD=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

networks:

- traefik

#-----Keycloak-Postgres-

Backup-----

pgbackups:

image: prodrigestivill/postgres-backup-local

restart: always

volumes:

- docker\_networking\_keycloak\_postgresbackup:/backups

links:

- postgres

depends\_on:

- postgres

environment:

- POSTGRES\_HOST=postgres
- POSTGRES\_DB=keycloak
- POSTGRES\_USER=keycloak
- POSTGRES\_PASSWORD=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- SCHEDULE=@daily
- BACKUP\_KEEP\_DAYS=7
- BACKUP\_KEEP\_WEEKS=4
- BACKUP\_KEEP\_MONTHS=6
- HEALTHCHECK\_PORT=8080

networks:

- traefik

healthcheck:

test: curl --fail http://localhost:8080 || exit 1

interval: 5m

retries: 5

start\_period: 20s

timeout: 10s

traefik-forward-auth:

image: thomseddon/traefik-forward-auth:2-arm64

restart: unless-stopped

command:

- "--default-provider=oidc"

- "--providers.oidc.issuer-url=https://keycloak.domain.com/auth/realms/master"
- "--providers.oidc.client-id=traefik-forward-auth"
- "--providers.oidc.client-secret=xxxxxxxxxxxxxxxxxxxxxxxxxxxx"
- "--secret=xxxxxxxxxxxxxxxxxxxxxxxxxxxx"
- "--insecure-cookie"
- "--cookie-domain=domain.com"
- "--auth-host=auth.domain.com"
- "--log-level=debug"

labels:

- "traefik.enable=true"
- "traefik.http.routers.traefik-forward-auth.rule=Host(`auth.domain.com`)"
- "traefik.http.services.traefik-forward-auth.loadbalancer.server.port=4181"
- "traefik.http.routers.traefik-forward-auth.entrypoints=websecure"
- "traefik.http.routers.traefik-forward-auth.tls=true"
- "traefik.docker.network=traefik"
- "traefik.http.routers.traefik-forward-auth.middlewares=traefik-forward-auth"
- "traefik.http.middlewares.traefik-forward-auth.forwardauth.address=http://traefik-forward-auth:4181"
- "traefik.http.middlewares.traefik-forward-auth.forwardauth.authResponseHeaders=X-Forwarded-User"
- "traefik.http.middlewares.traefik-forward-auth.forwardauth.trustForwardHeader=true"

networks:

- traefik

depends\_on:

- keycloak

Revision #1

Created 25 April 2022 15:51:05 by Andreas Greiner

Updated 3 January 2023 09:47:02 by Andreas Greiner