HTTPS aktivieren

Die bisherige Konfiguration von Traefik ist noch unsicher, da keine Verschlüsselung verwendet wird. Diese lässt sich jedoch nachrüsten, indem die Konfiguration angepasst wird. Traefik kann von Haus aus mit Let's Encrypt umgehen, was die Verwaltung von Zertifikaten recht einfach macht. Es sind keine zusätzlichen Tools notwendig.

> Bei der Konfiguration der Challenge für die Zertifikate wird hinter certificatesresolvers der Name festgelegt. Im folgenden Beispiel wird der Name des Resolvers auf *einzelzertifikat* festgelegt, indem dieser einfach mit einem Punkt getrennt angehängt wird. Der Name ist wichtig, denn dieser wird später in allen Containern als Label angegeben werden müssen, die mit Zertifikaten von diesem Resolver versorgt werden sollen.

```
services:
  traefik:
    image: traefik
    container_name: traefik
    restart: unless-stopped
    ports:
      - 80:80
      - 443:443
      - 8080:8080
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock:ro
      - ${TRAEFIK_PFAD}/traefik_data:/traefik
    command:
      - --api.dashboard=true
      - --api.insecure=true
      - --providers.docker=true
      - --providers.docker.exposedbydefault=false
      - --providers.docker.network=traefik
      - --entrypoints.webinsecure.address=:80
      - --entrypoints.websecure.address=:443
      - --entrypoints.traefik.address=:8080
# Challenge für die Zertifikate festlegen
      - --certificatesresolvers.einzelzertifikat.acme.tlschallenge=true
      - --certificatesresolvers.einzelzertifikat.acme.email=${ACME_EMAIL}
      - --
```

```
certificatesresolvers.einzelzertifikat.acme.storage=/traefik/certs_einzelzertifikat/acme.json
    labels:
      - traefik.enable=true
      # HTTPS Umleitung
      - traefik.http.routers.http-catchall.entrypoints=webinsecure
      - traefik.http.routers.http-catchall.rule=HostRegexp(`{host:.+}`)
      - traefik.http.routers.http-catchall.middlewares=redirect-to-https
      - traefik.http.middlewares.redirect-to-https.redirectscheme.scheme=https
      # HTTP Router
      - traefik.http.routers.traefik-secure.entrypoints=websecure
      - traefik.http.routers.traefik-secure.tls=true
      - traefik.http.routers.traefik-secure.tls.domains[0].main=*.${DOMAIN}
      - traefik.http.routers.traefik-secure.tls.domains[0].sans=${DOMAIN}
      - traefik.http.routers.traefik-secure.service=api@internal
    networks:
      - traefik

networks:
  traefik:
    name: traefik
    external: true
```

> In der oben gezeigten Konfiguration ist noch das Dashboard verfügbar, welches alle Interna von Traefik anzeigt. Für ein produktives Setup, dass von außen erreichbar ist, sollte dieses besser abgeschaltet werden. Dazu die folgenden Zeilen löschen:
>
> - 8080:8080
> - --entrypoints.traefik.address=:8080
> - traefik.http.routers.traefik-secure.rule=Host(`traefik.${DOMAIN}`)

In dieser Compose Konfiguration werden Variablen verwendet, um die Einstellung zu vereinfachen. Nachdem die docker-compose.yml erstellt wurde, gilt es noch folgende .env Datei zu erstellen und anzupassen.

```
TRAEFIK_PFAD=/pfad/zu/traefik
ACME_EMAIL=email@beispiel.de
DOMAIN=beispiel.de
```

Bevor nun die Konfiguration angewendet wird, müssen schon der Ordner traefik_data und darin der Unterordner für die Zertifikate erstellt werden. Zusätzlich ist die Datei für die Zertifikatskonfiguration zu erstellen und die Berechtigung anzupassen. Dazu kann das folgende Skript verwendet werden, wobei der Pfad anzupassen ist.

```
pfad=/pfad/zu/traefik/traefik_data/certs_einzelzertifikat
mkdir $pfad
touch mkdir $pfad/acme.json
chmod 600 $pfad/acme.json
```

Um die Docker Compose Konfiguration auszuführen, kann am besten in das Verzeichnis der YAML Datei gewechselt werden. Danach wird je nach nach gewählter Installation `sudo docker-compose up -d` oder `sudo docker compose up -d` (keine Bindestrich zwischen docker und compose) eingegeben, um die Standard Konfiguration `docker-compose.yml` zu starten. Compose erstellt dann die gewünschten Container mit den angegeben Optionen. Sollten die Container bereits mit dieser Compose Konfiguration erstellt worden sein, so werden die Container in dieser neu erstellt, dessen Konfiguration geändert wurde.

Anschließend müssen nur noch die gewünschten Dienst konfiguriert werden, damit diese von Traefik verwaltet werden können.

> In der Konfiguration ist noch die Konfigurationsübersicht unter Port 8080 erreichbar. Diese sollte in einer produktiven Umgebung deaktiviert werden.

Version #7
Erstellt: 16 März 2024 13:39:05 von Marcel
Zuletzt aktualisiert: 17 März 2024 10:54:07 von Marcel