

Traefik v2

- [Neuen Service zu Traefik hinzufügen](#)
- [Traefik v2 als Reverse Proxy installieren](#)

Neuen Service zu Traefik hinzufügen

Einleitung

Mithilfe von Traefik ist es möglich einen zentralen Proxy Server für alle Web Applikationen zu verwenden. Dieser nimmt alle Anfragen standardgemäß auf Port **80** und **443** an und leitet diese anhand der **Subdomain** in die entsprechenden **Docker Container**. Dies hat den Vorteil das die Applikationen nur über die Domains aufgerufen werden können, und so keine speziellen Ports mehr angegeben werden müssen oder Anwendungen auf andere Ports umgeleitet werden müssen.

Anwendung

Um eine Anwendung hinzuzufügen, musst du Traefik installieren. Wie du das erledigst erfährst du HIER (Folgt noch...)

Nun öffnest du die **docker-compose.yml** und fügst folgende Label ein:

```
labels:
  - "traefik.enable=true"
  - "traefik.docker.network=traefik"
  - "traefik.http.routers.service.entrypoints=http"
  - "traefik.http.routers.service.rule=Host(`domain.de`,`www.domain.de`)"
  - "traefik.http.middlewares.service-https-redirect.redirectscheme.scheme=https"
  - "traefik.http.routers.service.middlewares=service-https-redirect"
  - "traefik.http.routers.service-secure.entrypoints=https"
  - "traefik.http.routers.service-secure.rule=Host(`domain.de`,`www.domain.de`)"
  - "traefik.http.routers.service-secure.tls=true"
  - "traefik.http.routers.service-secure.tls.certresolver=http"
  - "traefik.http.routers.service-secure.service=service"
  - "traefik.http.services.service.loadbalancer.server.port=80"
  - "traefik.http.routers.service-secure.middlewares=secHeaders@file"
  - "com.centurylinklabs.watchtower.enable=true"
```

Dort musst du nur noch die Domains anpassen, den Ziel-Port angeben, das Traefik Netzwerk angeben und dem Service einen Namen geben. Du veränderst dann das Schlüsselwort service in den entsprechenden App-Namen. Zuletzt startest du den Docker Container, und dein Container

ist nun Ã¼ber Traefik erreichbar!

Notiz: Der letzte Label dient dazu Ã¼ber **Watchtower** automatisch **Image Updates** der service zu installieren. Wenn du kein Watchtower verwendest, kannst du dieses entfernen.

Traefik v2 als Reverse Proxy installieren

Einleitung

Traefik ist ein sogenannter **Reverse Proxy**. Das bedeutet, dieser nimmt alle Anfragen auf den angegebenen *Entrypoints* an und routet die Anfragen in die entsprechenden *Docker Container*. Dies hat den Vorteil das keine *Virtuellen Hosts* oder du dir unterschiedliche *Port-Nummern* merken musst. Deine Anfragen kannst du automatisch auf einen angegebenen Port routen.

Mehr Informationen: https://hub.docker.com/_/traefik/

Installation

Wenn wir nun **Traefik** installieren wollen, musst du **Docker** installiert haben. Wie du das machst, habe ich **hier** erklärt. Im ersten Schritt installieren wir das Tool **htpasswd**.

```
sudo apt-get update
sudo apt-get install apache2-utils
```

Im nächsten Schritt legen wir ein Verzeichnis für **Traefik** an. In meinem Beispiel haben wir unter dem root Verzeichnis, ein Verzeichnis mit dem Namen **_docker**. Dort liegen alle Daten für die **Docker Container**. In diesem Verzeichnis legen wir einen Ordner für **Traefik** an.

```
sudo mkdir -p /_docker/traefik
```

Im nächsten Schritt erstellen wir ein paar Verzeichnisse und Dateien die zur späteren Konfiguration oder Dateiablage benötigt werden.

```
sudo mkdir -p /_docker/traefik/data && \
sudo touch /_docker/traefik/data/acme.json && \
sudo chmod 600 /_docker/traefik/data/acme.json && \
sudo touch /_docker/traefik/data/traefik.yml
```

im vierten Schritt bearbeiten wir nun die **traefik.yml**. Dies ist eine *Konfigurationsdatei*. Mit dieser kannst du **Traefik** konfigurieren damit es so arbeitet wie du es brauchst. Dort musst du nur die E-Mail Adresse verändern. Da die Zertifikate per **Let's Encrypt** beantragt werden, kannst du damit deine E-Mail gleich für weitere Rückfragen hinterlegen. Dort fügst du dann folgende

Konfiguration ein.

```
sudo nano /_docker/traefik/data/traefik.yml
```

```
api:
  dashboard: true
entryPoints:
  http:
    address: ":80"
  https:
    address: ":443"
providers:
  docker:
    endpoint: "unix:///var/run/docker.sock"
    exposedByDefault: false
  file:
    filename: "./dynamic_conf.yml"
certificatesResolvers:
  http:
    acme:
      email: beispiel@beispiel.de # <--- E-Mail Adresse für Rückfragen
      storage: acme.json
      httpChallenge:
        entryPoint: http
```

Im Anschluss erstellen wir die **docker-compose.yml**. Diese Datei ist quasi die Konfigurationsdatei von *Applikationen* die du mit Docker erstellst. Aus dieser Datei erstellst du Anwendungen und gibst die entsprechenden Parameter mit.

```
sudo nano /_docker/traefik/docker-compose.yml
```

```
version: '3'
services:
  traefik:
    image: traefik:latest
    container_name: traefik
    restart: unless-stopped
    security_opt:
      - no-new-privileges:true
    networks:
```

```

- traefik
ports:
- 80:80
- 443:443
volumes:
- /etc/localtime:/etc/localtime:ro
- /var/run/docker.sock:/var/run/docker.sock:ro
- ./data/traefik.yml:/traefik.yml:ro
- ./data/acme.json:/acme.json
- ./data/dynamic_conf.yml:/dynamic_conf.yml
labels:
- "traefik.enable=true"
- "traefik.http.routers.traefik.entrypoints=http"
- "traefik.http.routers.traefik.rule=Host(`traefik.beispiel.de`)"
- "traefik.http.middlewares.traefik-auth.basicauth.users=admin:Pa$$w0rd"
- "traefik.http.middlewares.traefik-https-redirect.redirectscheme.scheme=https"
- "traefik.http.routers.traefik.middlewares=traefik-https-redirect"
- "traefik.http.routers.traefik-secure.entrypoints=https"
- "traefik.http.routers.traefik-secure.rule=Host(`traefik.beispiel.de`)"
- "traefik.http.routers.traefik-secure.tls=true"
- "traefik.http.routers.traefik-secure.tls.certresolver=http"
- "traefik.http.routers.traefik-secure.service=api@internal"
- "providers.file.filename=/dynamic_conf.yml"
- "traefik.http.routers.traefik-secure.middlewares=secHeaders@file,traefik-auth"
networks:
traefik:
external: true

```

Jetzt erstellen wir einen Benutzer und geben dem ein entsprechendes Passwort mit. Es wird **dringend** empfohlen dieses zu Ändern! In der Konfigurationsdatei sind momentan die Platzhalter **admin** und **Pa\$\$w0rd** dort eingetragen. Der Benutzername und das Kennwort werden durch ein : voneinander getrennt. Wir generieren jetzt ein neues Kennwort mit dem Tool **htpasswd**. Dort ersetzt du den Benutzernamen und das Kennwort durch deine eigenen Daten.

```
echo $(htpasswd -nb admin Pa$$w0rd) | sed -e s/\$/\$/g
```

Du bekommst beim ausführen dieses Befehls eine Ausgabe, diese Ausgabe trägst du in das entsprechende Label in der **docker-compose.yml** ein.

Vorher:

```
- "traefik.http.middlewares.traefik-auth.basicauth.users=admin:Pa$$w0rd"
```

Nachher:

```
- "traefik.http.middlewares.traefik-auth.basicauth.users=admin:$apr1$$ofCridn5$$94xGJcgJ0qoS0tZUHN.gP/"
```

Als nächstes erstellen wir eine weitere **Konfigurationsdatei**. Diese erstellen wir mit dem folgenden Befehl und fügen dann wieder einen Inhalt ein.

```
sudo nano /_docker/traefik/data/dynamic_conf.yml
```

```
tls:
  options:
    default:
      minVersion: VersionTLS12
      cipherSuites:
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256
      curvePreferences:
        - CurveP521
        - CurveP384
      sniStrict: true
http:
  middlewares:
    secHeaders:
      headers:
        browserXssFilter: true
        contentTypeNosniff: true
        frameDeny: true
        sslRedirect: true
        #HSTS Configuration
        stsIncludeSubdomains: true
        stsPreload: true
        stsSeconds: 31536000
        customFrameOptionsValue: "SAMEORIGIN"
```

Im vorletzten Schritt legen wir das **Docker Netzwerk** an indem Traefik mit den anderen Containern kommuniziert.

```
sudo docker network create traefik
```

Und im letzten Schritt starten wir den Container mit dem **docker-compose** Befehl.

```
sudo docker-compose -f /_docker/traefik/docker-compose.yml up -d
```

Wenn du jetzt deinen Webbrowser öffnest und auf den entsprechenden Hostnamen navigierst, wirst du dich mit den vorhin angegebenen Daten anmelden müssen. Wenn du das gemacht hast, bist du auf dem Traefik Dashboard angemeldet. Dort findest du alle Informationen über Verbindungen, Entrypoints und andere Dienste.