Installationskonfigurationen via Docker

- reverseproxy mit 100 Jahre gültigem SSL Zertifikat

reverseproxy mit 100 Jahre gültigem SSL Zertifikat

Beschreibung:

Diese Konfiguration dient zum hinzufügen bestehender Docker Anwendungen um diese mit einem selbst signierten SSL Zertifikat via HTTPS zu sichern

Installation

docker compose datei.
Den parameter :
 depends_on:
      - web

```
services:
  web:
  ...
  irgendein webdienst der auf port 80 läuft.
  hier bei den ports unbedingt die Port binding für port 80 und 443 deaktivieren falls vorhanden.
  zu finden in der Port Sektion falls definiert
  ...

  nginx:
    image: nginx:stable
    container_name: nginx-proxy
    volumes:
      - ./nginx-proxy.conf:/etc/nginx/nginx.conf:ro
      - ./certs/selfsigned.crt:/etc/ssl/certs/selfsigned.crt:ro
      - ./certs/private.key:/etc/ssl/private/private.key:ro
    ports:
      - "80:80"
      - "443:443"
    depends_on:
      - web
    restart: always
...
```

```
fortsetzung der composer datei
```

Nun ein unterverzeichnis certs im Projektverzeichnis erstellen

```
mkdir /root/<projektname>/certs
```

Nun die nginx config erstellen

```
nano /root/<projektname>/nginx-proxy.conf
```

Inhalt

Die Parameter :

proxy_pass http://web:80; mit dem Namen des Container Dienstes ersetzten
client_max_body_size 100M; die Größe für maximales Post Upload, sprich wie groß eine Upload Datei sein darf defienieren

```
events {
  worker_connections 1024;
}

http {
  server {
    listen 80;
    return 301 https://$host$request_uri;
  }

  server {
    listen 443 ssl;
    ssl_certificate /etc/ssl/certs/selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/private.key;

    location / {
      proxy_pass http://web:80;
      proxy_set_header Host $host;
      proxy_set_header X-Real-IP $remote_addr;
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_set_header X-Forwarded-Proto $scheme;
      proxy_set_header Upgrade websocket;
      proxy_set_header Connection Upgrade;
```

```
      client_max_body_size 100M;
    }
  }
}
```

Nun das Zertifikat erstellen

```
openssl req -newkey rsa:4096 -x509 -sha256 -days 365000 -nodes -out /root/<projektname>/certs/selfsigned.crt
-keyout /root/<projektname>/certs/private.key
```

Fragen beantworten

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
```

Nun den den container starten und fertig ist der reverse proxy

```
docker-compose down
docker-compose up -d
```