

Installation hinter Reverse Proxy

Die auf der vorherigen Seite erklärte Installation ist aufgrund der fehlenden Verschlüsselung unsicher. Statt beim Container SSL zu aktivieren und ein Zertifikat einzuspielen, kann am besten ein sog. Reverse Proxy verwendet werden.

Im folgenden werden die notwendigen Anpassungen an Zitadel beschrieben, jedoch wird davon ausgegangen, dass bereits ein Reverse Proxy im Einsatz und mit einem gültigen SSL-Zertifikat ausgestattet ist. Außerdem wird angenommen, dass der Reverse Proxy die Domäne id.beispiel.de nutzt auf Port 443 (Standard HTTPS Port).

Die Compose Konfiguration ist wie folgt anzupassen.

```
services:
  zitadel:
    image: 'ghcr.io/zitadel/zitadel:latest'
    container_name: zitadel
    command: 'start-from-setup --init-projections --masterkey
"MasterkeyNeedsToHave32Characters"'
    environment:
      - 'ZITADEL_DATABASE_POSTGRES_HOST=zitadel-db'
      - 'ZITADEL_DATABASE_POSTGRES_PORT=5432'
      - 'ZITADEL_DATABASE_POSTGRES_DATABASE=zitadel'
      - 'ZITADEL_DATABASE_POSTGRES_USER_USERNAME=zitadel'
      - 'ZITADEL_DATABASE_POSTGRES_USER_PASSWORD=PasswortFuerZitadel'
      - 'ZITADEL_DATABASE_POSTGRES_USER_SSL_MODE=disable'
      - 'ZITADEL_DATABASE_POSTGRES_ADMIN_USERNAME=postgres'
      - 'ZITADEL_DATABASE_POSTGRES_ADMIN_PASSWORD=PasswortFuerDenPostgresChef'
      - 'ZITADEL_DATABASE_POSTGRES_ADMIN_SSL_MODE=disable'
      - 'ZITADEL_EXTERNALSECURE=true'
      - 'ZITADEL_EXTERNALPORT=443'
      - 'ZITADEL_TLS_ENABLED=false'
      - 'ZITADEL_EXTERNALDOMAIN=beispiel.de'
    depends_on:
      zitadel-db:
```

```
    condition: 'service_healthy'
  restart: unless-stopped

zitadel-db:
  image: postgres:16-alpine
  container_name: zitadel-db
  environment:
    - 'POSTGRES_USER=postgres'
    - 'POSTGRES_PASSWORD=PasswortFuerDenPostgresChef'
  volumes:
    - /root/Docker/zitadel/data:/var/lib/postgresql/data
  healthcheck:
    test: ["CMD-SHELL", "pg_isready", "-d", "db_prod"]
    interval: '10s'
    timeout: '30s'
    retries: 5
    start_period: '20s'
  restart: unless-stopped
```

Anschließend den Container einfach über *sudo docker-compose up -d* neu erstellen lassen.

Nicht vergessen: Im Reverse Proxy ist natürlich Zitadel mit der dazugehörigen Domäne zu hinterlegen und an diesen Container weiterzuleiten.

Danach ist die Weboberfläche unter folgender Adresse erreichbar: <https://beispiel.de/ui/console>

Durch die Domäne verändert sich der Standard-Login wie folgt:

Benutzername: `zitadel-admin@zitadel.beispiel.de`

Passwort: `Password1!`

Version #3

Erstellt: 2024-03-09 20:26:07 CET von Marcel

Zuletzt aktualisiert: 2024-03-09 22:15:41 CET von Marcel