```
# Nextcloud basierend auf https://github.com/sethforprivacy/self-hosted-services
# und https://goneuland.de/nextcloud-server-mit-docker-compose-und-traefik-installieren/

version: '3.7'
services:

### Proxy fuer den externen Zugriff
  traefik:
    env_file:
      - .env
    # The official v2 Traefik docker image
    image: traefik:${TRAEFIK_VERSION}
    container_name: "traefik"
    restart: unless-stopped
    command:
      - --global.checkNewVersion=true
      - --global.sendAnonymousUsage=false
      - "--entrypoints.web.address=:80"
      - "--entrypoints.websecure.address=:443"
      - --entrypoints.https.http.tls.options=tls-opts@file
      - "--api=true"
      - "--api.dashboard=true"
      - --ping=true
      - "--log.level=${TRAEFIK_LOG_LEVEL}"
      - --log.filePath=/logs/traefik.log
      - --accessLog.bufferingSize=100 # Configuring a buffer of 100 lines
      - --accessLog.filters.statusCodes=204-299,400-499,500-599
      - "--providers.docker=true"
      - "--providers.docker.exposedbydefault=false"
      - "--providers.docker.network=web"
      - --providers.docker.swarmMode=false
     # forward port 80 -> 443
      - "--entrypoints.web.http.redirections.entryPoint.to=websecure"
```

```
    - "--entrypoints.web.http.redirections.entryPoint.scheme=https"
    # cert resolver config
    - --entrypoints.https.http.tls.certresolver=myresolver
#     - --certificatesResolvers.myresolver.acme.caServer=https://acme-staging-v02.api.letsencrypt.org/directory # LetsEncrypt Staging Server - uncomment when testing
    # wildcard certificate
    - "--certificatesresolvers.myresolver.acme.email=${TRAEFIK_LE_CERT_MAILADRDRESS}"
    - "--certificatesresolvers.myresolver.acme.storage=/acme.json"
    - "--certificatesresolvers.myresolver.acme.httpchallenge=true"
    - "--certificatesresolvers.myresolver.acme.httpchallenge.entrypoint=web"
    - "--certificatesresolvers.myresolver.acme.tlschallenge=true"
    - "--certificatesresolvers.myresolver.acme.dnschallenge=true"
    - "--certificatesresolvers.myresolver.acme.dnschallenge.provider=desec"
    - "--certificatesresolvers.myresolver.acme.dnschallenge.delayBeforeCheck=100"
    - "--certificatesresolvers.myresolver.acme.dnschallenge.resolvers=${TRAEFIK_DOMAIN_REGISTRAR_DNS},1.1.1.1:53,8.8.8.8:53"
    - "--entrypoints.websecure.http.tls.domains[0].main=${MY_DOMAIN_NAME}"
    - "--entrypoints.websecure.http.tls.domains[0].sans=*.${MY_DOMAIN_NAME}"
  ports:
    - "80:80"
    - "443:443"
  volumes:
    - ./rules:/rules # file provider directory
    - /var/run/docker.sock:/var/run/docker.sock:ro # Use Docker Socket Proxy instead for improved security
    - ./acme/acme.json:/acme.json # cert location - you must create this emtpy file and change permissions to 600
    - ./logs:/logs # for fail2ban or crowdsec
    - ./shared:/shared
    - "/etc/localtime:/etc/localtime:ro"
  labels:
    - "traefik.enable=true"
    - "traefik.http.routers.api.rule=Host(`${TRAEFIK_HOST}.${DOMAIN}`)"
    - "traefik.http.routers.api.service=api@internal"
    - "traefik.http.routers.api.middlewares=auth"
    - "traefik.http.middlewares.auth.basicauth.users=${BASIC_AUTH_USERS}:${BASIC_AUTH_HASH}"
```

```
    - "traefik.http.routers.api.entrypoints=websecure"
#     - "traefik.http.routers.api.tls.certresolver=myresolver"  ### auskommentieren nach erstem Lauf
    - "traefik.frontend.redirect.permanent: 'true'"
    - traefik.http.routers.api.tls=true
    - "traefik.http.routers.api.tls.domains[0].main=${MY_DOMAIN_NAME}"
    - "traefik.http.routers.api.tls.domains[0].sans=*.${MY_DOMAIN_NAME}"
    - "traefik.http.middlewares.api.headers.stsSeconds=155520011"
    - "traefik.http.middlewares.api.headers.stsIncludeSubdomains=true"
    - "traefik.http.middlewares.api.headers.stsPreload=true"
    - TZ=$TZ

  networks:
    - "web"
    - "traefik-proxy"
  healthcheck:
    test: ["CMD", "traefik", "healthcheck", "--ping"]
    interval: 15s
    retries: 3
    timeout: 1s
    start_period: 15s

 nextcloud:
  env_file:
    - .env
  image: nextcloud:${NEXTCLOUD_VERSION}
  container_name: nextcloud
  restart: always
  volumes:
    - ./cloud/nextcloud:/var/www/html
    - ./cloud/nextcloud/data:/var/www/html/data
    - ./cloud/nextcloud/apps:/var/www/html/apps
    - ./cloud/nextcloud/config:/var/www/html/config
#     - ./cloud/nextcloud/db:/var/lib/mysql  ###### Nach Hinweis auskommentiert
```

```
  - ./logs:/logs # for fail2ban or crowdsec
environment:
  - MYSQL_DATABASE=${MYSQL_DATABASE}
  - MYSQL_USER=${MYSQL_USER}
  - MYSQL_PASSWORD=${MYSQL_PW}
  - MYSQL_HOST=${MYSQL_HOST}
  - NEXTCLOUD_ADMIN_USER=${NEXTCLOUD_ADMIN_USER}
  - NEXTCLOUD_ADMIN_PASSWORD=${NEXTCLOUD_ADMIN_PW}
  - NEXTCLOUD_DATA_DIR=/var/www/html/data
  - NEXTCLOUD_TRUSTED_DOMAINS='${NEXTCLOUD_HOST}.${DOMAIN}' '${DOMAIN}' 'localhost' '${NEXTCLOUD_HOST}.localhost'
  - TRUSTED_PROXIES=172.18.0.2/16  ### Abfrage durch docker inspect traefik (IPAddress und IPPrefixLen)
  - OVERWRITEHOST=${NEXTCLOUD_HOST}.${DOMAIN}
  - OVERWRITEPROTOCOL=https
  - OVERWRITECLIURL=https://${NEXTCLOUD_HOST}.${DOMAIN}
  - REDIS_HOST=${REDIS_HOST}
  - REDIS_PORT=6379
  - DEFAULT_PHONE_REGION=DE
  - DEFAULT_LANGUAGE=de
  - DEFAULT_LOCALE=de_DE
  - NEXTCLOUD_UPDATE=1
depends_on:
  - nextcloud_db
  - redis
labels:
  - "traefik.enable=true"
  - "traefik.http.routers.nextcloud.rule=Host(`${NEXTCLOUD_HOST}.${DOMAIN}`)"
  - "traefik.http.routers.nextcloud.entrypoints=websecure"
  - "traefik.http.routers.nextcloud.tls.certresolver=myresolver"
  - "traefik.http.routers.nextcloud.middlewares=nextcloud,nextcloud_redirect"
  - "traefik.http.routers.nextcloud.tls=true"

  - "traefik.http.middlewares.nextcloud.headers.stsSeconds=155520011"
  - "traefik.http.middlewares.nextcloud.headers.stsIncludeSubdomains=true"
```

```
    - "traefik.http.middlewares.nextcloud.headers.stsPreload=true"
    - "traefik.http.middlewares.nextcloud.headers.forceSTSHeader=true"
    - "traefik.http.middlewares.nextcloud.headers.customFrameOptionsValue=ALLOW-FROM https://${NEXTCLOUD_HOST}.${DOMAIN}"
    - "traefik.http.middlewares.nextcloud.headers.contentSecurityPolicy=frame-ancestors 'self' ${NEXTCLOUD_HOST}.${DOMAIN} *.${NEXTCLOUD_HOST}
${DOMAIN}"
    - "traefik.http.middlewares.nextcloud.headers.customresponseheaders.X-Frame-Options=SAMEORIGIN"
    - "traefik.http.middlewares.nextcloud_redirect.redirectregex.permanent=true"
    - "traefik.http.middlewares.nextcloud_redirect.redirectregex.regex=https://(.*)/.well-known/(card|cal)dav"
    - "traefik.http.middlewares.nextcloud_redirect.redirectregex.replacement=https://$${1}/remote.php/dav/"
  networks:
   - "web"

 nextcloud_db:
  env_file:
   - .env
  image: mariadb:${DB_VERSION}
  container_name: nextcloud_db
  command: --transaction-isolation=READ-COMMITTED --binlog-format=ROW --innodb-file-per-table=1 --skip-innodb-read-only-compressed
  restart: always
  volumes:
   - ./cloud/nextcloud/db:/var/lib/mysql
  environment:
   - MYSQL_DATABASE=${MYSQL_DATABASE}
   - MYSQL_ROOT_PASSWORD=${MYSQL_ROOT_PW}
   - MYSQL_USER=${MYSQL_USER}
   - MYSQL_PASSWORD=${MYSQL_PW}
  healthcheck:
   test: ["CMD", "mysqladmin", "ping", "--silent"]
  networks:
   - "web"

 redis:
  env_file:
```

```
    - .env
  image: redis:latest
  container_name: redis
  restart: unless-stopped
  volumes:
    - ./logs:/logs # for fail2ban or crowdsec
    - ./cloud/redis-data:/var/lib/redis
  networks:
    - "web"
  healthcheck:
    test: ["CMD", "redis-cli", "ping"]
    interval: 15s
    timeout: 3s
    retries: 30

cron:
  env_file:
    - .env
  image: nextcloud:${NEXTCLOUD_VERSION}
  restart: always
  volumes:
    - "./cloud/nextcloud:/var/www/html"
    - "./cloud/nextcloud/apps:/var/www/html/apps"
    - "./cloud/nextcloud/config:/var/www/html/config"
    - "./cloud/nextcloud/db:/var/lib/mysql"
  entrypoint: /cron.sh
  depends_on:
    nextcloud_db:
      condition: service_healthy
    redis:
      condition: service_healthy
  networks:
   - "web"
```

```
volumes:
  redis-data:
  nextcloud_db:
  nextcloud:

networks:
  web:
    external: false
  traefik-proxy:
    external: true
```