

# Docker Compose Template

## Guidelines

These guidelines are suggested in order to maximise reliability of hosted services.

- Store secrets and tokens in a `.env` file adjacent to the `docker-compose.yml` file.
  - The environment variables are automatically interpolated when `docker compose up` is called.
  - If multiple `.env` files are required (for separation of secrets), then use `.env.<CONTAINER_NAME>` (e.g. `.env.gitea`) and add an override in the `docker-compose.yml` file. See the [Docker documentation](#) for more details.
- Always use tagged images.
  - Avoid using `latest`. By default, Docker hub automatically tags the most recently pushed image as `latest`, unless overridden by the image maintainer. This means that you might be running bleeding edge/alpha/vulnerable versions.
  - Often images expect a specific version of a container to be running in order for DB migrations to work. This is especially important with Postgres where major versions are not always forwards compatible.
- Separate frontend and backend services using different networks.
  - Docker Compose manages the creation/destruction of these networks for you. Please see the examples below.
- Volumes should be placed in a volumes directory adjacent to the `docker-compose.yml` file.
  - Prefix volume directories with the name of the container.
  - See the directory structure below for an example.
- Mount `/etc/timezone` and `/etc/localtime` where timestamps are used by the container.
  - See below for an example.

An example directory structure is shown below:

```
.
├── .env.db
├── .env.gitea
├── .env.tunnel
├── docker-compose.yml
├── start.sh
└── volumes/
```

```
├─ gitea_config/
│  └─ ...
├─ gitea_data/
│  └─ ...
└─ postgres_data/
   └─ ...
```

See [Cloudflare Tunnel Configuration](#) for instructions on how to configure a tunnel and get a tunnel token.

# Gitea

## .env.db

```
POSTGRES_USER=gitea
POSTGRES_PASSWORD=gitea
POSTGRES_DB=gitea
```

## .env.gitea

```
GITEA__database__DB_TYPE=mysql
GITEA__database__HOST=db:3306
GITEA__database__NAME=gitea
GITEA__database__USER=gitea
GITEA__database__PASSWD=gitea
```

## .env.tunnel

```
TUNNEL_TOKEN=abc...
```

## docker-compose.yml

```
services:
  tunnel:
    image: cloudflare/cloudflared:2024.4.0    # Use version tags to ensure only stable software is used.
    restart: unless-stopped                 # This restart command helps with crashing services.
```

```
command: tunnel run
depends_on:
  - gitea                # Ensure dependencies start in the correct order.
networks:
  - frontend              # Use multiple networks to isolate services.
env_file:
  - .env.tunnel           # Use environment variables loaded via a .env file for tokens.
gitea:
  image: gitea/gitea:1.21-rootless
  restart: unless-stopped
  healthcheck:             # Use healthchecks if possible.
    test: curl --fail http://localhost:3000/api/healthz || exit 1
    interval: 60s
    retries: 5
    start_period: 20s
    timeout: 10s
  depends_on:
    - db
  networks:
    - frontend
    - backend
  volumes:
    - './volumes/gitea_data:/var/lib/gitea' # Mount volumes into the ./volumes directory.
    - './volumes/gitea_config:/etc/gitea'   # Relative volumes must be wrapped in single quotes.
    - '/etc/timezone:/etc/timezone:ro'      # Mount timezone/localtime so that timestamps are correct.
    - '/etc/localtime:/etc/localtime:ro'
  env_file:
    - .env.gitea
db:
  image: postgres:14
  restart: unless-stopped
  healthcheck:
    test: ["CMD-SHELL", "pg_isready", "-d", "db_prod"]
    interval: 60s
    retries: 5
    start_period: 20s
    timeout: 10s
  networks:
    - backend
  volumes:
    - './volumes/postgres_data:/var/lib/postgresql/data'
```

env\_file:

- .env.db

networks:

backend:

frontend:

---

Revision #8

Created 19 April 2024 10:33:50 by Jack

Updated 19 April 2024 16:14:44 by Jack