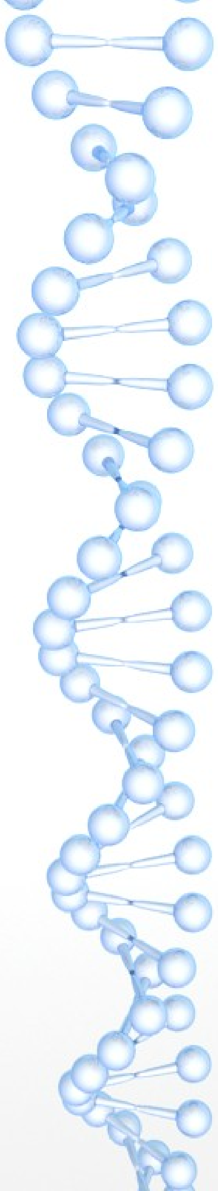
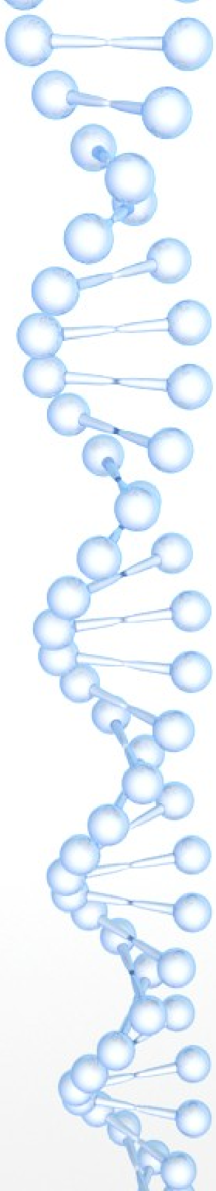


Escaping Big Tech with Traefik 2.0

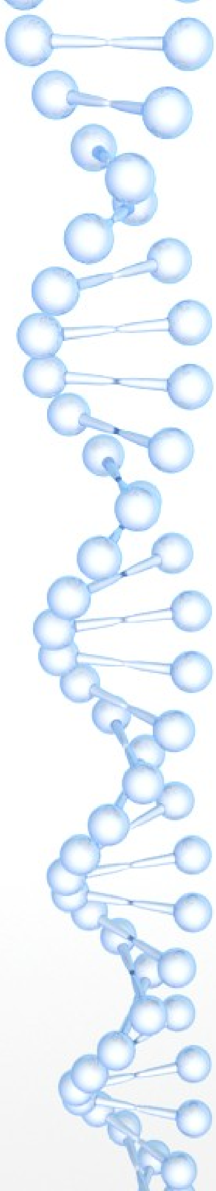


Slides and files:
http://wieg.co/traefik-meetup

About Me

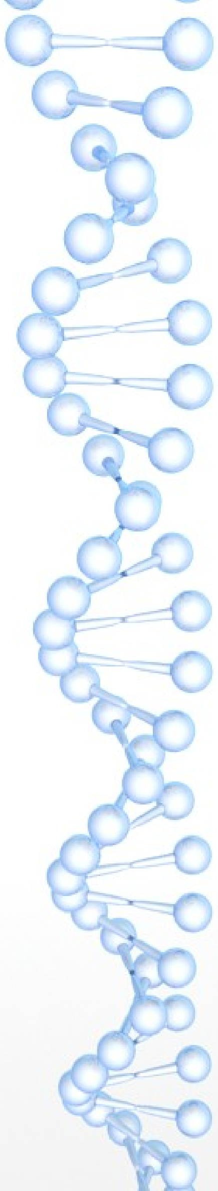
- Senior Software Engineer | WP Engine
- Plugin Developer
- Teacher
- Speaker
- Pilot
- Focus on:
- Privacy
- Development workflows
- Open web

http://chriswiegman.com



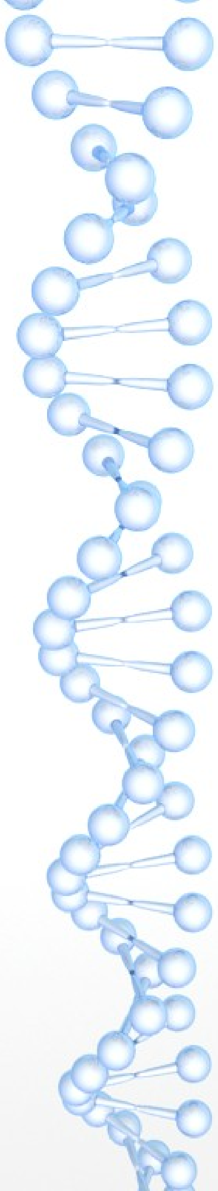
Why Escape Big Tech?

- Privacy
- Better control
- Own your own data
- Escape “walled garden”
- For fun



Services We Can Replace

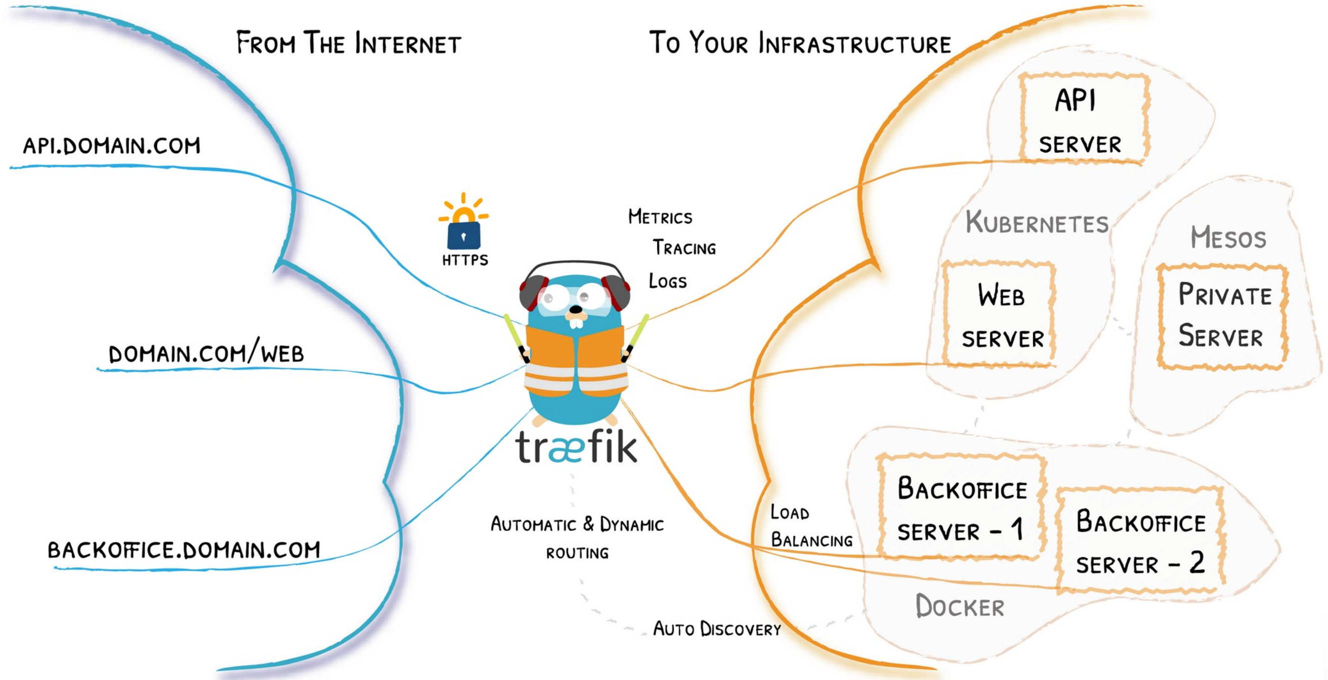
- File storage (Google Drive/iCloud/etc)
- Notes (Google Keep/Notes/etc)
- Photos
- News Reader
- Chat (Google Duo/Facetime/etc)
- Calendar/Contacts/Tasks
- *So much more...*

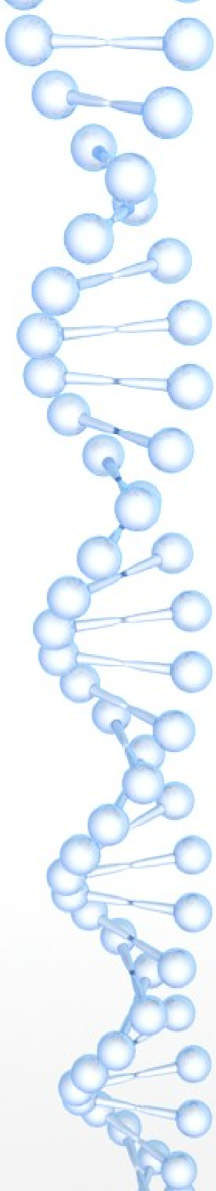


Why Traefik?

1) Reduce hosting costs
2) Simple implementation
3) Containerize all the things

Traefik Architecture

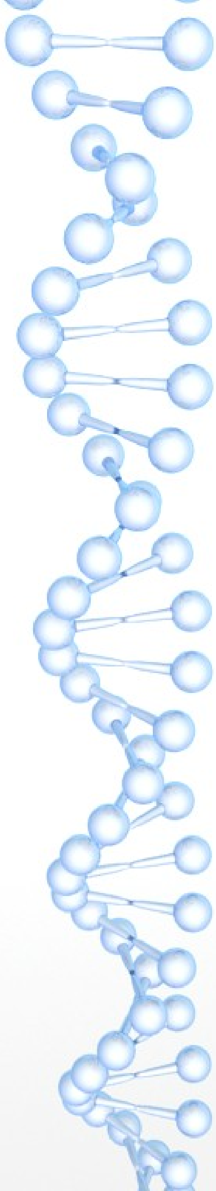




Traefik Configs

- **Static configuration**: The startup configuration
- **Dynamic configuration**: Fully dynamic routing configuration

- Most of this tutorial is dynamic configuration
- Dynamic configuration can be specified in many ways, in your traefik config or docker-compose



Traefik Concepts

- **Routers:** A router is in charge of connecting incoming requests to the services that can handle them. In the process, routers may use pieces of middleware to update the request, or act before forwarding the request to the service.
- **Middlewares**: Pieces of middleware are a means of tweaking the requests before they are sent to your service
- **Providers**: The backend provider of your application (ie, Docker)

Example Middleware

- **Enable SSL**

```
- "traefik.http.routers.service.entrypoints=web-secure"
- "traefik.http.routers.service.rule=Host(`service.url`)"
- "traefik.http.routers.service.tls=true
- "traefik.http.routers.service.tls.certresolver=default"
```

Example Middleware

- **Redirect to ssl:**

```
- "traefik.http.middlewares.service-https.redirectscheme.scheme=https"
- "traefik.http.routers.service-http.entrypoints=web"
- "traefik.http.routers.service-http.rule=Host(`http.url`)"
- "traefik.http.routers.service-http.middlewares=service-https@docker"
```

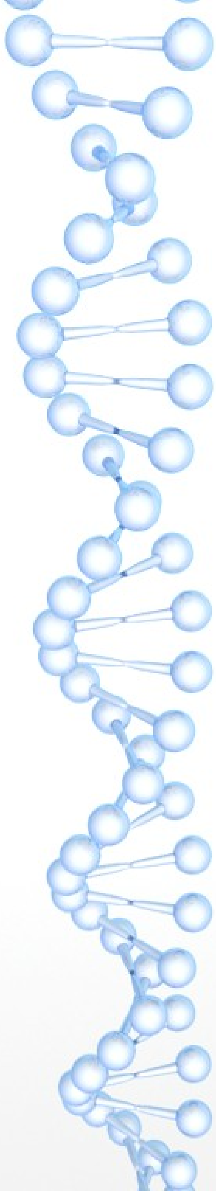
Example Middleware

- **Regex Redirect**

```
- "traefik.http.middlewares.nextcloud-caldav.redirectregex.permanent=true"
 - "traefik.http.middlewares.nextcloud-caldav.redirectregex.regex=^https://(.*)/.well-known/(card|cal)dav"
 - "traefik.http.middlewares.nextcloud-caldav.redirectregex.replacement=https://$${1}/remote.php/dav/"
```

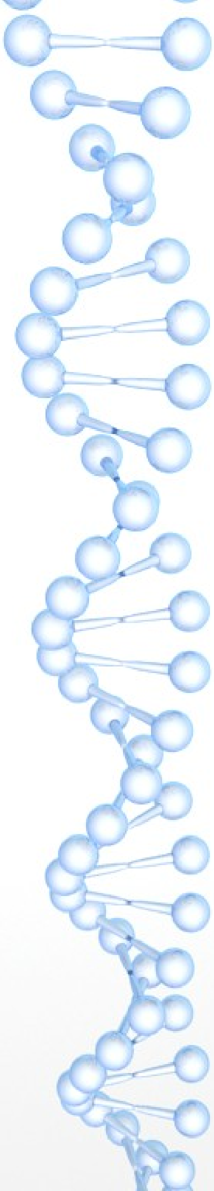
Attaching Middleware to Router

```
- "traefik.http.routers.my-router.middlewares=my-middleware@docker"
```



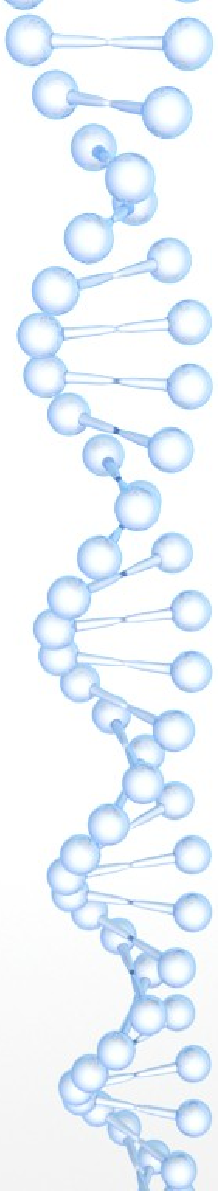
Middleware Gotchas

- Middleware can’t do multiple things (can’t set a header and handle a redirect in a single middleware)
- Only one middleware per router (https://github.com/containous/traefik/issues/5538)



Where to Host?

- Any VPS provider will do
- $5 DigitalOcean instance is “good enough” for today’s demo
- ***Make sure you use a service that offers backups!***

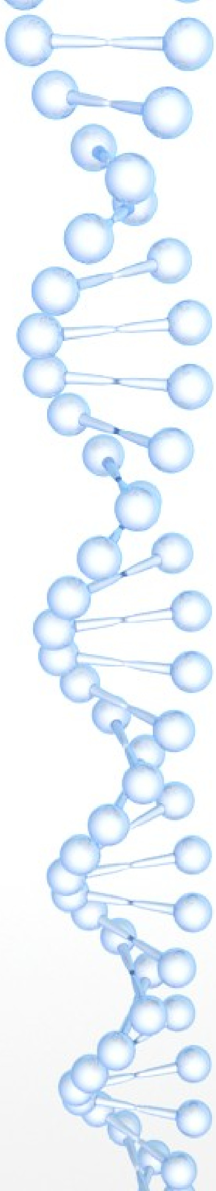


Getting Started

```
traefik:
  image: traefik:2.1
  ports:
    - 80:80
    - 443:443
  restart: always
  volumes:
    - ./data/conf/traefik/acme.json:/acme.json
    - ./data/conf/traefik/traefik.toml:/traefik.toml
    - ./data/volumes/traefik/tmp:/tmp
```

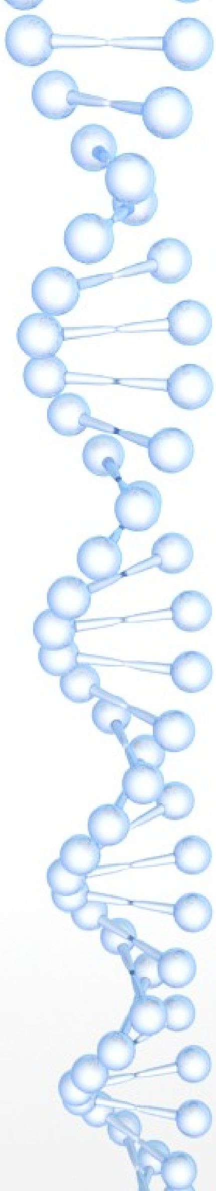
Keeping It Updated

```
watchtower:
  command: --label-enable --cleanup --interval 300
  image: containrrr/watchtower
  labels:
    - "com.centurylinklabs.watchtower.enable=true"
  network_mode: none
  restart: always
  volumes:
    - /var/run/docker.sock:/var/run/docker.sock
```



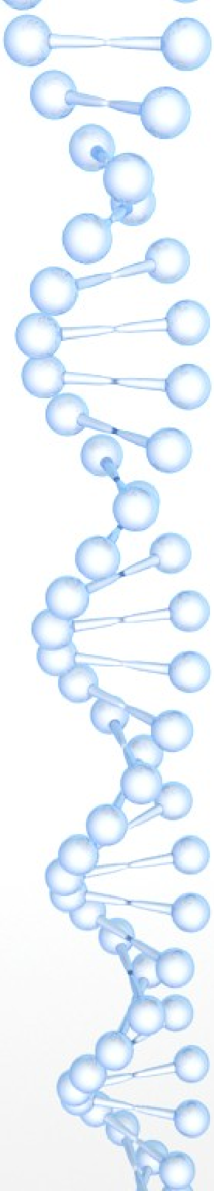
Keeping It Updated

```
traefik:
    depends_on:
      - watchtower
    labels:
      - "com.centurylinklabs.watchtower.enable=true"
```



Keeping It Secure

```
networks:
  default:
    driver: bridge
  traefik:
    internal: true
```

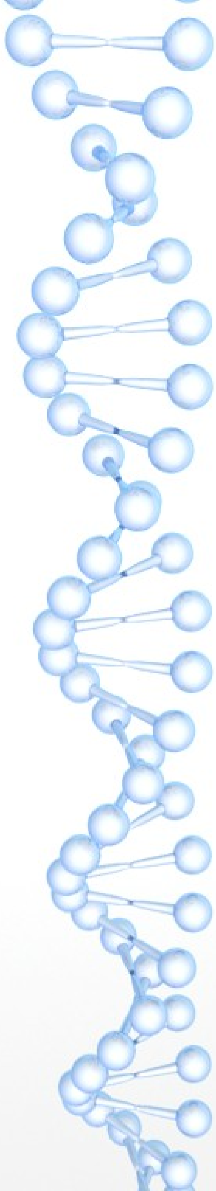


Keeping It Secure

```
dockerproxy:
  depends_on:
    - watchtower
  environment:
    CONTAINERS: 1
  image: tecnativa/docker-socket-proxy
  labels:
    - "com.centurylinklabs.watchtower.enable=true"
  networks:
    - traefik
  ports:
    - 2375
  volumes:
    - "/var/run/docker.sock:/var/run/docker.sock"
```

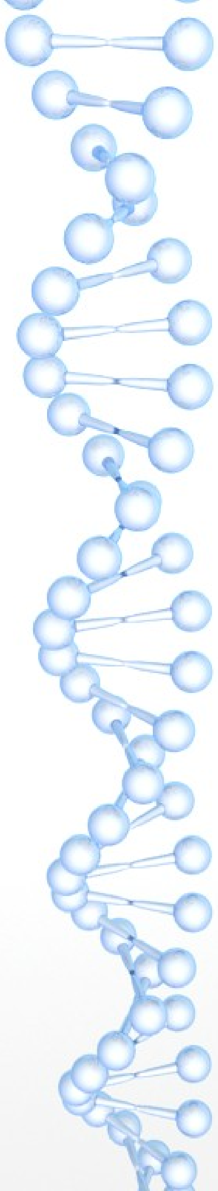
Keeping It Secure

```
traefik:
    depends_on:
      - dockerproxy
    networks:
      - default
      - traefik
```



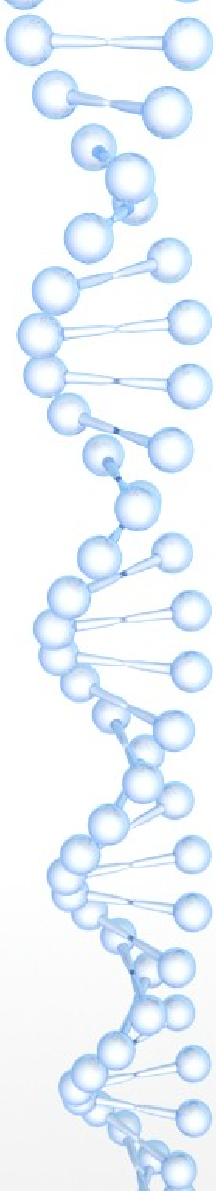
Keeping It Secure

```
[providers.docker]
  exposedByDefault = false
  endpoint = "tcp://dockerproxy:2375"
  network = "traefik"
```



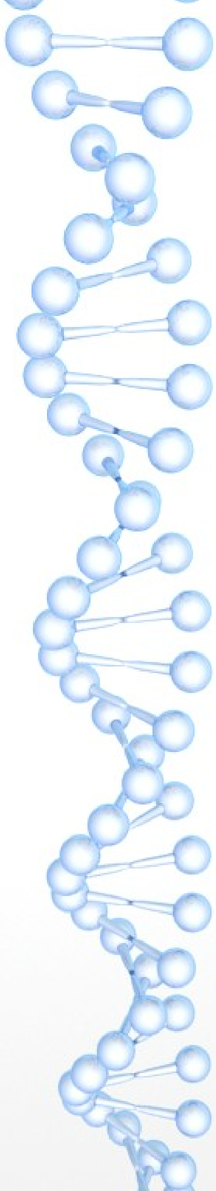
Finishing Traefik Config

```
[log]
  level = "ERROR"

[entryPoints]
  [entryPoints.web]
    address = ":80"
  [entryPoints.web-secure]
    address = ":443"

[certificatesResolvers]
  [certificatesResolvers.default.acme]
    email = "your@email.address"
    storage = "acme.json"
    [certificatesResolvers.default.acme.tlsChallenge]
```



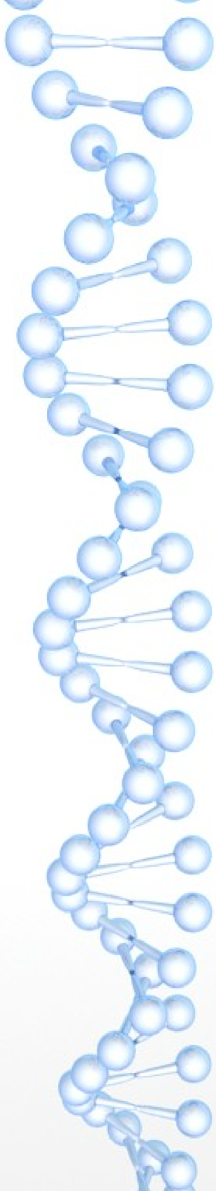
Adding Services

- File Storage, Calendar, Contacts, etc → Nextcloud
  - https://nextcloud.com
- Read it later → Wallabag
  - https://wallabag.org
- RSS/News → FreshRSS
  - https://www.freshrss.org
- ShortURLs - > YOURLs
  - https://yourls.org/



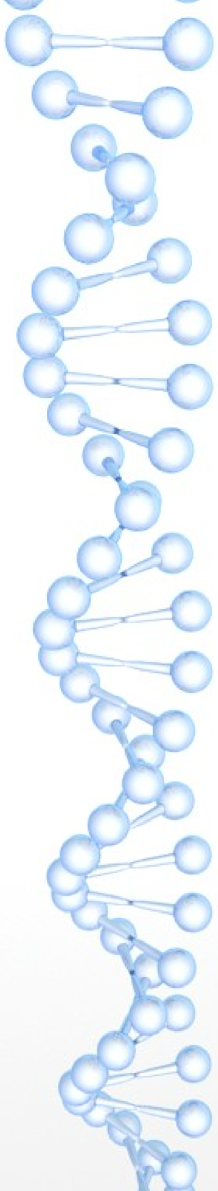
Add Supporting Services

```
mariadb:
    depends_on:
      - watchtower
    env_file: .mariadb.env
    image: mariadb:10
    labels:
      - "com.centurylinklabs.watchtower.enable=true"
    networks:
      - default
    ports:
      - 3306:3306
    restart: always
    volumes:
      - ./data/volumes/mariadb:/var/lib/mysql
```

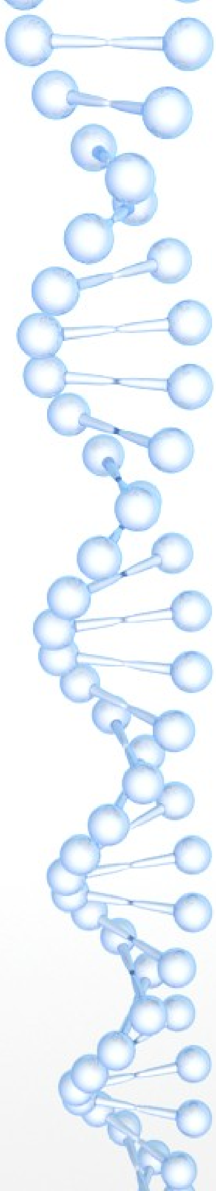


Mariadb config file

```
MYSQL_ROOT_PASSWORD=
```



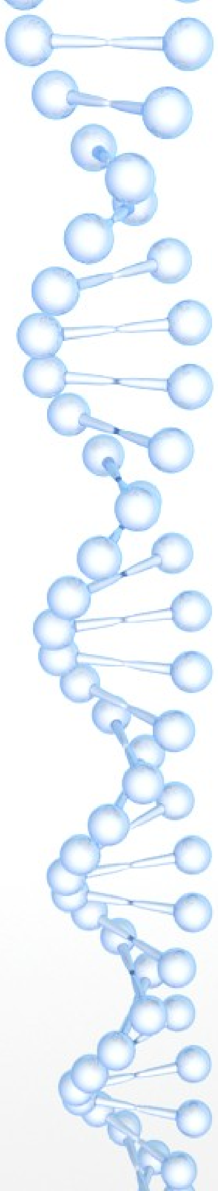
```
redis:
  depends_on:
    - watchtower
  image: redis:5
  labels:
    - "com.centurylinklabs.watchtower.enable=true"
  networks:
    - default
  restart: always
  volumes:
    - ./data/volumes/redis:/data
```



Labels We Will Need

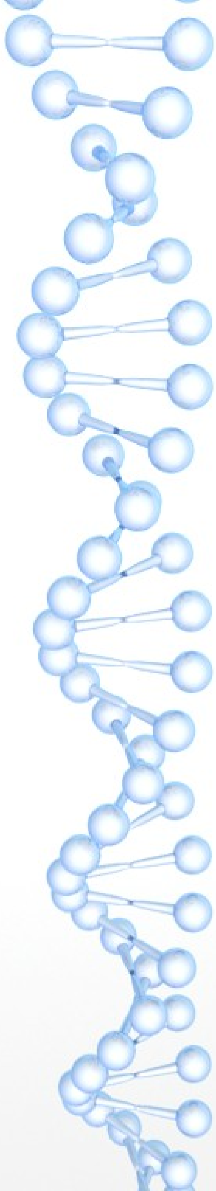
- **Enable Traefik**

```
- "traefik.enable=true"
```



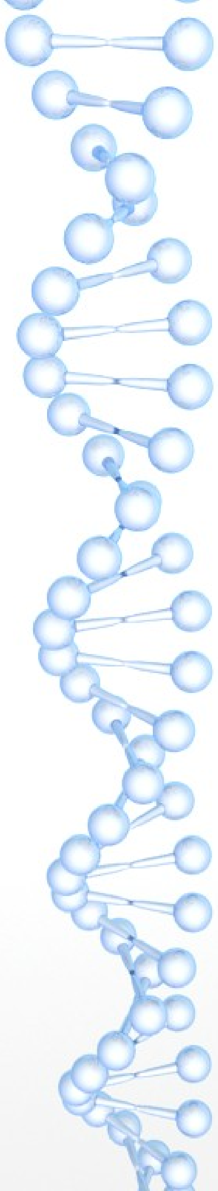
FreshRSS

```
freshrss:
  depends_on:
    - mariadb
    - traefik
    - watchtower
  env_file: .freshrss.env
  image: freshrss/freshrss
  labels:
    - "traefik.enable=true"
    - "traefik.http.middlewares.freshrss-https.redirectscheme.scheme=https"
    - "traefik.http.routers.freshrss-http.entrypoints=web"
    - "traefik.http.routers.freshrss-http.rule=Host(`my.freshrss.url`)"
    - "traefik.http.routers.freshrss-http.middlewares=freshrss-https@docker"
    - "traefik.http.routers.freshrss.entrypoints=web-secure"
    - "traefik.http.routers.freshrss.rule=Host(`my.wallabag.url`)"
    - "traefik.http.routers.freshrss.tls=true"
    - "traefik.http.routers.freshrss.tls.certresolver=default"
    - "com.centurylinklabs.watchtower.enable=true"
  networks:
    - default
  restart: always
  volumes:
    - ./data/volumes/freshrss:/var/www/FreshRSS/data
```



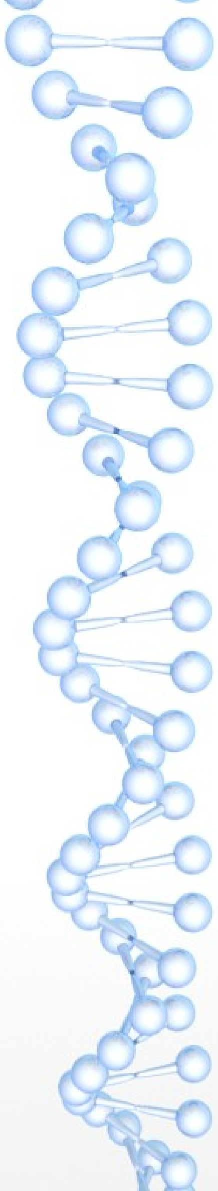
FreshRSS Config

```
CRON_MIN=*/10
TZ=America/Chicago
```



Wallabag

```
wallabag:
  depends_on:
    - mariadb
    - redis
    - traefik
    - watchtower
  env_file: .wallabag.env
  image: wallabag/wallabag:2.3.8
  labels:
    - "traefik.enable=true"
    - "traefik.http.middlewares.wallabag-https.redirectscheme.scheme=https"
    - "traefik.http.routers.wallabag-http.entrypoints=web"
    - "traefik.http.routers.wallabag-http.rule=Host(`my.wallabag.url`)"
    - "traefik.http.routers.wallabag-http.middlewares=wallabag-https@docker"
    - "traefik.http.routers.wallabag.entrypoints=web-secure"
    - "traefik.http.routers.wallabag.rule=Host(`my.wallabag.url`)"
    - "traefik.http.routers.wallabag.tls=true"
    - "traefik.http.routers.wallabag.tls.certresolver=default"
    - "com.centurylinklabs.watchtower.enable=true"
  networks:
    - default
  restart: always
  volumes:
    - ./data/volumes/wallabag/images:/var/www/wallabag/web/assets/images
    - ./data/volumes/wallabag/data:/var/www/wallabag/data
```



Wallabag Config

```
MYSQL_ROOT_PASSWORD=
SYMFONY__ENV__DATABASE_DRIVER=pdo_mysql
SYMFONY__ENV__DATABASE_HOST=mariadb
SYMFONY__ENV__DATABASE_PORT=3306
SYMFONY__ENV__DATABASE_NAME=
SYMFONY__ENV__DATABASE_USER=
SYMFONY__ENV__SECRET=
SYMFONY__ENV__DATABASE_PASSWORD=
SYMFONY__ENV__DATABASE_CHARSET=utf8mb4
SYMFONY__ENV__FOSUSER_REGISTRATION=false
SYMFONY__ENV__FOSUSER_CONFIRMATION=false
SYMFONY__ENV__DOMAIN_NAME=https://[your site here]
```

YOURLs

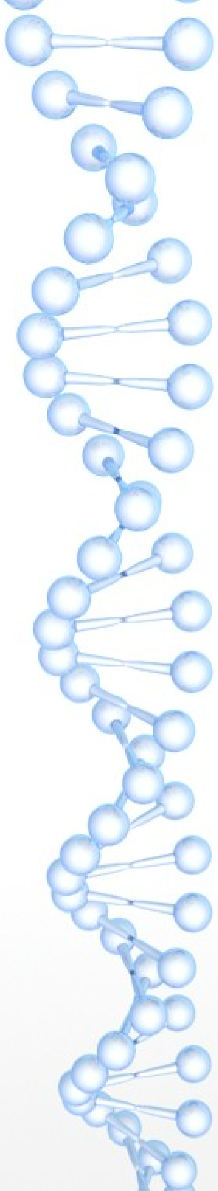
```
yourls:
    depends_on:
      - mariadb
      - traefik
      - watchtower
    env_file: .yourls.env
    image: yourls:1.7
    labels:
      - "traefik.enable=true"
      - "traefik.http.middlewares.yourls-https.redirectscheme.scheme=https"
      - "traefik.http.routers.yourls-http.entrypoints=web"
      - "traefik.http.routers.yourls-http.rule=Host(`my.yourls.url`)"
      - "traefik.http.routers.yourls-http.middlewares=yourls-https@docker"
      - "traefik.http.routers.yourls.entrypoints=web-secure"
      - "traefik.http.routers.yourls.rule=Host(`my.yourls.url`)"
      - "traefik.http.routers.yourls.tls=true"
      - "traefik.http.routers.yourls.tls.certresolver=default"
      - "com.centurylinklabs.watchtower.enable=true"
    networks:
      - default
    restart: always
    volumes:
      - ./data/conf/yourls/plugins:/var/www/html/user/plugins
      - ./data/volumes/yourls/html:/var/www/html
```

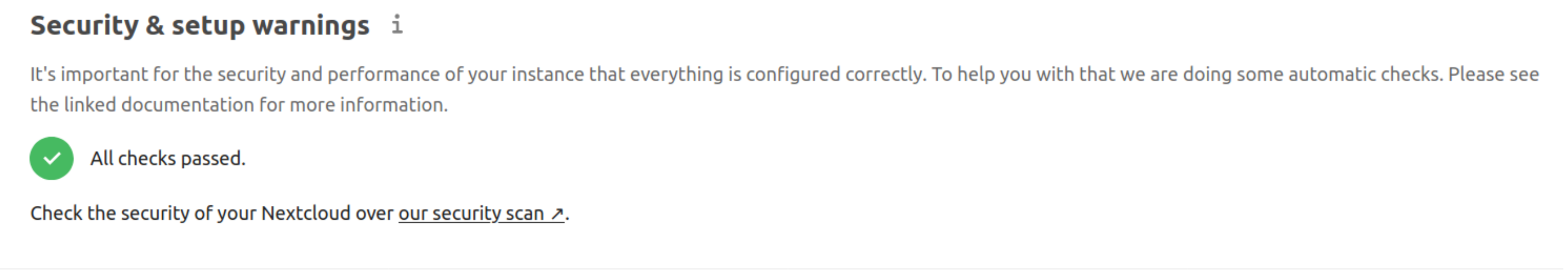
YOURLs Config

```
YOURLS_DB_HOST=mariadb
YOURLS_DB_USER=
YOURLS_DB_PASS=
YOURLS_DB_NAME=
YOURLS_SITE=https://[your site here]
YOURLS_USER=
YOURLS_PASS=
```

Nextcloud

```
nextcloud:
  depends_on:
    - mariadb
    - redis
    - traefik
    - watchtower
  env_file: .nextcloud.env
  image: nextcloud:18
  labels:
    - "traefik.enable=true"
    - "traefik.http.middlewares.nextcloud-caldav.redirectregex.permanent=true"
    - "traefik.http.middlewares.nextcloud-caldav.redirectregex.regex=^https://(.*)/.well-known/(card|cal)dav"
    - "traefik.http.middlewares.nextcloud-caldav.redirectregex.replacement=https://$${1}/remote.php/dav/"
    - "traefik.http.middlewares.nextcloud-https.redirectscheme.scheme=https"
    - "traefik.http.routers.nextcloud-http.entrypoints=web"
    - "traefik.http.routers.nextcloud-http.rule=Host(my.nextcloud.url`)"
    - "traefik.http.routers.nextcloud-http.middlewares=nextcloud-https@docker"
    - "traefik.http.routers.nextcloud.entrypoints=web-secure"
    - "traefik.http.routers.nextcloud.rule=Host(`my.nextcloud.url`)"
    - "traefik.http.routers.nextcloud.middlewares=nextcloud-caldav@docker"
    - "traefik.http.routers.nextcloud.tls=true"
    - "traefik.http.routers.nextcloud.tls.certresolver=default"
    - "com.centurylinklabs.watchtower.enable=true"
  networks:
    - default
  restart: always
  volumes:
    - ./data/volumes/nextcloud/html:/var/www/html
```





Security & setup warnings

It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information.

✓ All checks passed.

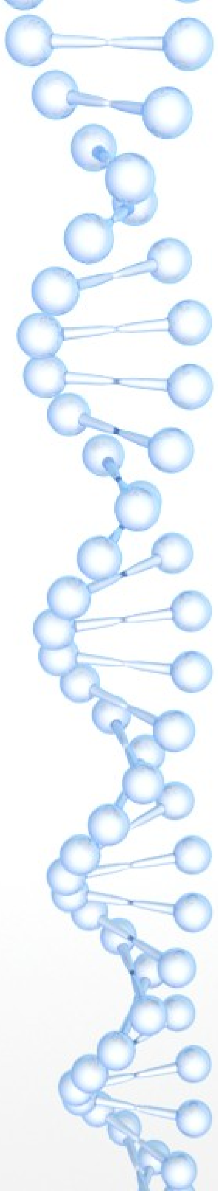
Check the security of your Nextcloud over our security scan ↗.

Nextcloud Labels

```
- "traefik.enable=true"
- "traefik.http.middlewares.nextcloud-caldav.redirectregex.permanent=true"
- "traefik.http.middlewares.nextcloud-caldav.redirectregex.regex=^https://(.*)/.well-known/(card|cal)dav"
- "traefik.http.middlewares.nextcloud-caldav.redirectregex.replacement=https://$${1}/remote.php/dav/"
- "traefik.http.middlewares.nextcloud-https.redirectscheme.scheme=https"
- "traefik.http.routers.nextcloud-http.entrypoints=web"
- "traefik.http.routers.nextcloud-http.rule=Host(`my.nextcloud.url`)"
- "traefik.http.routers.nextcloud-http.middlewares=nextcloud-https@docker"
- "traefik.http.routers.nextcloud.entrypoints=web-secure"
- "traefik.http.routers.nextcloud.rule=Host(`my.nextcloud.url`)"
- "traefik.http.routers.nextcloud.middlewares=nextcloud-caldav@docker"
- "traefik.http.routers.nextcloud.tls=true"
- "traefik.http.routers.nextcloud.tls.certresolver=default"
- "com.centurylinklabs.watchtower.enable=true"
```

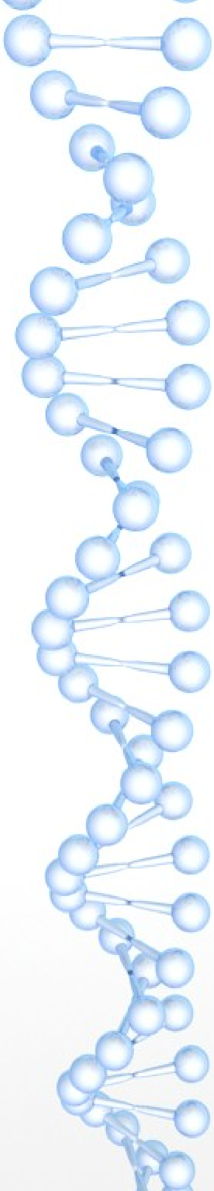
The Nextcloud Config

```
REDIS_HOST=
MYSQL_ROOT_PASSWORD=
MYSQL_PASSWORD=
MYSQL_DATABASE=
MYSQL_USER=
MYSQL_HOST=
```

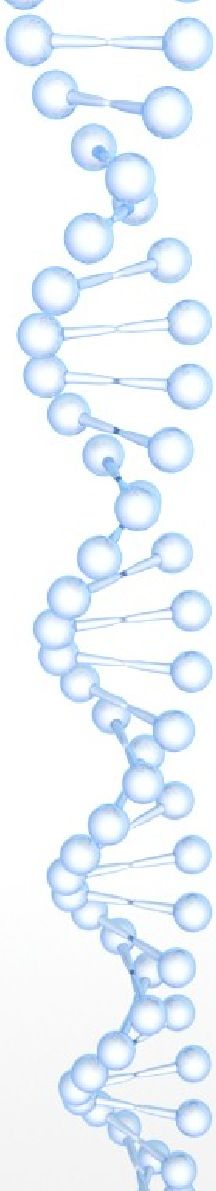


Nextcloud Middlewares

- Ideal would handle HSTS expiration AND caldav/carddav redirect
- Setup for caldav, use https://github.com/sualko/cloud_hsts for hsts header



Questions?



Slides and files:
http://wieg.co/traefik-meetup