

# Installation Vaultwarden avec nginx en reverse et ssl

## DOCKER:

### **docker-compose.yml:**

```
version: "3"
services:
  vaultwarden:
    image: vaultwarden/server:latest
    container_name: vaultwarden
    restart: unless-stopped
    ports:
      - 8080:80
    volumes:
      - ./bitwarden:/data:rw
    environment:
      - ADMIN_TOKEN=${ADMIN_TOKEN}
      - WEBSOCKET_ENABLED=true
      - SIGNUPS_ALLOWED=true
      - SIGNUPS_VERIFY=true
      - SMTP_HOST=${SMTP_HOST}
      - SMTP_FROM=${SMTP_FROM}
      - SMTP_PORT=${SMTP_PORT}
      - SMTP_SSL=${SMTP_SSL}
      - SMTP_USERNAME=${SMTP_USERNAME}
      - SMTP_PASSWORD=${SMTP_PASSWORD}
      - DOMAIN=${DOMAIN}
```

### **.env:**

```
ADMIN_TOKEN=edit!
WEBSOCKET_ENABLED=true
SIGNUPS_VERIFY=true
SIGNUPS_ALLOWED=true
SMTP_HOST=
SMTP_FROM=
SMTP_PORT=587
SMTP_SSL=true
SMTP_USERNAME=
SMTP_PASSWORD=
DOMAIN=https://vault.blah.local
```

## config.json

```
{
  "domain": "https://vault.blah.local",
  "sends_allowed": true,
  "disable_icon_download": false,
  "signups_allowed": true,
  "signups_verify": true,
  "signups_verify_resend_time": 3600,
  "signups_verify_resend_limit": 6,
  "invitations_allowed": true,
  "password_iterations": 100000,
  "show_password_hint": false,
  "admin_token": "edit!",
  "invitation_org_name": "Vaultwarden",
  "ip_header": "X-Real-IP",
  "icon_cache_ttl": 2592000,
  "icon_cache_negttl": 259200,
  "icon_download_timeout": 10,
  "icon_blacklist_non_global_ips": true,
  "disable_2fa_remember": false,
  "authenticator_disable_time_drift": false,
  "require_device_email": false,
  "reload_templates": false,
  "log_timestamp_format": "%Y-%m-%d %H:%M:%S.%3f",
  "disable_admin_token": false,
```

```
"_enable_yubico": true,
"_enable_duo": false,
"_enable_smtp": true,
"smtp_host": "smtp.office365.com",
"smtp_ssl": false,
"smtp_explicit_tls": false,
"smtp_port": 587,
"smtp_from": "",
"smtp_from_name": "",
"smtp_username": "",
"smtp_password": "",
"smtp_timeout": 15,
"smtp_accept_invalid_certs": false,
"smtp_accept_invalid_hostnames": false,
"_enable_email_2fa": true,
"email_token_size": 6,
"email_expiration_time": 600,
"email_attempts_limit": 3
}
```

# NGINX:

## Générate cert ssl:

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/ssl/private/entité.key -out
/etc/ssl/certs/vault.crt
openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

## conf nginx:

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
```

```
worker_connections 768;
# multi_accept on;
}

http {

    ##
    # Basic Settings
    ##

    sendfile on;
    tcp_nopush on;
    types_hash_max_size 2048;
    # server_tokens off;

    # server_names_hash_bucket_size 64;
    # server_name_in_redirect off;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    ##
    # SSL Settings
    ##

    ##
    # Logging Settings
    ##

    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    ##
    # Gzip Settings
    ##

    gzip on;

    # gzip_vary on;
```

```

# gzip_proxied any;
# gzip_comp_level 6;
# gzip_buffers 16 8k;
# gzip_http_version 1.1;
# gzip_types text/plain text/css application/json application/javascript text/xml application/xml
application/xml+rss text/javascript;

##

# Virtual Host Configs

##

include /etc/nginx/conf.d/*.conf;

include /etc/nginx/sites-enabled/*;

server {
    listen      80;
    listen      443 ssl;
    ssl on;
    server_name  domain.local;
    include /etc/nginx/conf.d/ssl-params.conf;
    ssl_certificate /etc/ssl/certs/vault.crt;
    ssl_certificate_key /etc/ssl/private/entite.key;
    ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
    location / {
        proxy_pass http://localhost:8080;
        proxy_set_header Host          $host;
        proxy_set_header X-Real-IP      $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        client_max_body_size 100M;
    }
}
}

```

Revision #5

Created 14 October 2022 07:25:56 by garfi

Updated 14 October 2022 07:35:34 by garfi