

Vaultwarden Password Management (draft)

The first thing I self-hosted on my Docker server (after a media server, of course) and made public on a domain was a password manager. At the time, the container was called BitWarden RS, but it has since been renamed to VaultWarden.

The reason I wanted to self-host a password manager is that I believe 2 factor authentication and strong passwords are a great first step in securing our accounts online. I had been using a paid password manager for years and had even convinced others to do the same. Unfortunately, the company that I recommended to everyone switched their pricing structure to only allow for 1 device to be connected to their account on the free tier.

I regularly use 2-4 devices per day and so using a service that only allows for 1 device wasn't going to cut it.

Prerequisites for VaultWarden in Docker.

First things first, you'll need a Docker server set up. Linode has made that process very simple and you can set one up for just a few bucks a month and can add a private IP address (for free) and backups for just a couple bucks more per month.

Another thing you'll need is a domain name, which you can buy from almost anywhere online for a wide range of prices depending on where you make your purchase. Be sure to point the domains DNS settings to point to Linode. You can find more information about that here:

<https://www.linode.com/docs/guides/dns-manager/> (or link to the previous article)

You'll also want a reverse proxy set up on your Docker Server so that you can do things like route traffic and manage SSLs on your server. I made a video about the process of setting up a Docker server with Portainer and a reverse proxy called Nginx Proxy Manager that you can check out here: INSERT LINK TO THAT VIDEO/POST HERE.

Once you've got your Docker server set up, you can begin the process of setting up your VaultWarden password manager on that server.

There are 2 primary ways you can do this:

1. In the command line via SSH.
2. In Portainer via the Portainer dashboard.

We're going to take a look at how to do this in Portainer so that we can have a user interface to work with.

Head over to <http://your-server-ip-address:9000> and get logged into Portainer with the credentials we setup in our previous post/video.

On the left side of the screen, we're going to click the "Stacks" link and then, on the next page, click the "+ Add stack" button.

This will bring up a page where you'll enter the name of the stack. Below that that you can then copy and paste the following:

```
version: "2"
services:
  vaultwarden:
    image: vaultwarden/server:latest
    container_name: vaultwarden
    networks:
      - nginxproxymanager_default
    volumes:
      - /home/docker/vaultwarden:/data/
    ports:
      - 90:80
    restart: unless-stopped

networks:
  nginxproxymanager_default:
    external: true
```

This Docker compose file / stack tells the system to download the latest vaultwarden/server image to the Docker server, name the container "vaultwarden", attach it to the "nginxproxymanager_default" network, mount it to the directory "home/docker/vaultwarden", and make it available on the docker server's port 90.

You can change the path of where you'd like to store the vaultwarden data if you'd like. Just make sure that the folder has the correct permissions to be written to.

Once you're happy with the settings here, we can deploy the container by clicking the button that says "Deploy the stack".

This will start the process of downloading and deploying VaultWarden on your server. You'll know that the container has been deployed once the page reloads and you see all your running containers.

image-1646867721920.png

Now you can go to <http://your-server-ip-address:90> and you should be able to see the login screen for VaultWarden.

STOP.

In order for you to actually be able to use VaultWarden, it needs a domain name and SSL.

Setting up a domain and SSL

Head back over to your Linode dasboard and go to "Domains". Then find the domain that you added to your account. Click it and then look for the CNAME section of the domain management.

Add a CNAME to your domain by entering a hostname entry for what you'd like your subdomain to be. In the example video, I entered "pw" (without the quotes). Below that, I entered the @ symbol in the "Alias to" box and then clicked "Save".

Now that you have that done, we can head over to Nginx Proxy Manager and setup our SSL and domain.

Now you can go to <http://your-server-ip-address:81> and you should be able to see the login screen for Nginx Proxy Manager.



Log into your account.

Revision #1

Created 6 April 2022 22:17:34 by DB T3CH

Updated 6 April 2022 22:20:28 by DB T3CH