forum.openmediavault.org /index.php

SWAG, Let’s Encrypt and Web GUI

HI

-
  - May 20th 2021
  - #1

I got Portainer installed and running. As OMV no longer has a plugin for Let’s Encrypt, I installed a SWAG container. As far I can see everything runs fine, I got a certificate. But now I run into an issue. I don’t know how to tell the web GUI of OMV (5.6.7-1) to use it. I changed the ports to 81 and 444, so ports 80 and 443 can be used by the SWAG container. When I open my URL on port 443 I got the website of the container. So I think I have to configure the reverse proxy to redirect to the OMV GUI. But how to do this?

BTW I’m running IPv6

Thanks

-
  - May 21st 2021
  - #2

You have to navigate to the config folder and create a file in nginx/proxy-confs. I didn't externalize omv itself or I would share my file, but for a bunch of apps there are samples there. Maybe copy one of those and customize it for omv. You need to restart swag after.

-
  - May 23rd 2021
  - #3

I've made a proxy-conf to use with my SWAG in SUBDOMAIN mode. You'll have to edit it to fit your IP/port/servername.

Go to the folder of the "proxy-confs" (/path-to-swag/nginx/proxy-confs/) and create a file named:

`nano omv.subdomain.conf.sample` and copy/paste the following code but be sure to edit it with the IP and Port you have assigned

to OMV:

Code

```
# Conf Sample to be used by SWAG Reverse Proxy for access via HTTPS to OpenMediaVault.yourdomain.url
# Example: 'h**ps://omv.yoursubdomain.duckdns.org/'
# If 2 or more instances of OMV are running on the same network, it is necessary to create a .conf
# to each one, with different names and pointing to the proper IPs.

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name omv.*; # note: Set this with a unique name IF running 2 or more OMV servers eg: omvraspi.*

    include /config/nginx/ssl.conf;

    client_max_body_size 0;

    # enable for ldap auth, fill in ldap details in ldap.conf
    #include /config/nginx/ldap.conf;

    # enable for Authelia
    #include /config/nginx/authelia-server.conf;

#
    location / {
        # enable the next two lines for http auth
        #auth_basic "Restricted";
        #auth_basic_user_file /config/nginx/.htpasswd;

        # enable the next two lines for ldap auth
        #auth_request /auth;
        #error_page 401 =200 /login;

        # enable for Authelia
        #include /config/nginx/authelia-location.conf;

        include /config/nginx/proxy.conf;
        resolver 127.0.0.11 valid=30s;
        set $upstream_app 192.168.1.200; # note: edit with the LAN IP of your OpenMediaVault server.
        set $upstream_port 35000;      # note: same port used on the server for OpenMediaVault. Here is port:35000
        set $upstream_proto http;
        proxy_pass $upstream_proto://$upstream_app:$upstream_port;
```

```
            access_log off;

        }

    }
```

Display Less

Now save the file and rename it to `cp omv.subdomain.conf.sample omv.subdomain.conf` and just restart SWAG with `docker restart swag`

After this, just go to a browser and you'll access via "https://omv.yourdomainurl"

KM0201 Care to test this one?!? 😉

-
  - May 24th 2021
  - #4

hmm, never seen one like that. Interesting

-
  - May 24th 2021
  - #5

Quote from Soma

> I've made a proxy-conf to use with my SWAG in SUBDOMAIN mode.

I had to comment in this thread, mainly so I could easily find it and come back to it at a later date and try this out in combination with KM0201 's "cheap" domain name/Nextcloud setup. Good stuff.

-
  - May 24th 2021
  - #6

I may have to try that. But I'm still having a helluva time setting up subdomains for calibre and airsonic, and they have preset services also.

-
  - May 24th 2021
  - #7

Well... you ever look at the statue "The Thinker", and wonder what he's thinking and maybe how it could apply to your life? Well, tonight I thought he was thinking "Ken, if you just sit down and put your mind on this, you'd have it figured out in no time"...

So I did.

Freaking network mode issue. I really should have caught that a couple weeks ago. I tried adding network modes to their individual stacks to connect them to the swag network (nextcloud_default in my case)... but kept getting an error. Ended up just moving those compose files to my nextcloud stack, deleted the old containers and redeployed...

blammo.. music and most importantly, MY BOOKS! are now securely accessed.

-
  - May 24th 2021
  - #8

For anyone else who might be so inclined.. here's how it ended up looking in the end... I guess if I decide to reverse proxy anymore services, I'll just add them to the nextcloud stack to keep the headaches to a minimum. Only other one I'm thinking now is probably syncthing for my offset backup

Code

```
version: "2"
services:
  nextcloud:
    image: ghcr.io/linuxserver/nextcloud:latest
    container_name: nextcloud
    environment:
      - PUID=1000
      - PGID=100
    volumes:
      - /srv/dev-disk-by-label-D1/AppData/nextcloud:/config
      - /srv/dev-disk-by-label-D1/Disk_1/Media/.Nextcloud:/data
      - /etc/localtime:/etc/localtime:ro
    depends_on:
      - mariadb
    #ports:
      #- 450:443
    restart: unless-stopped
  mariadb:
    image: ghcr.io/linuxserver/mariadb:latest
    container_name: nextclouddb
    environment:
      - PUID=1000
      - PGID=100
      - MYSQL_ROOT_PASSWORD="it's super secret"
    volumes:
      - /srv/dev-disk-by-label-D1/AppData/nextclouddb:/config
      - /etc/localtime:/etc/localtime:ro
    restart: unless-stopped
  swag:
    image: ghcr.io/linuxserver/swag
    container_name: swag
    cap_add:
      - NET_ADMIN
    environment:
      - PUID=1000
      - PGID=100
      - URL=mydomain.xyz
      - SUBDOMAINS=www,nextcloud,airsonic,calibre-web
      - VALIDATION=http
      - EMAIL=oops@aol.com
    volumes:
      - /srv/dev-disk-by-label-D1/AppData/swag:/config
      - /etc/localtime:/etc/localtime:ro
    ports:
      - 444:443
      - 81:80
    restart: unless-stopped
  airsonic:
    image: ghcr.io/linuxserver/airsonic
    container_name: airsonic
    environment:
      - PUID=1000
      - PGID=100
    volumes:
      - /NAS/AppData/airsonic:/config
      - /NAS/Media/Music:/music
      - /NAS/Media/Music/.Playlists:/playlists
      - /NAS/Media/Music/.Podcasts:/podcasts
      - /etc/localtime:/etc/localtime:ro
    ports:
      - 4040:4040
    restart: unless-stopped
  calibre-web:
    image: ghcr.io/linuxserver/calibre-web
    container_name: calibre-web
    environment:
      - PUID=1000
      - PGID=100
    volumes:
      - /NAS/AppData/calibre:/config
      - /NAS/Media/eBooks:/books
      - /etc/localtime:/etc/localtime:ro
    ports:
      - 8083:8083
    restart: unless-stopped
```

Display More

-
  - May 24th 2021
  - #9

KM0201 why do you use calibre-web instead of calibre? Just curious.

-
  - May 24th 2021
  - #10

> Quote from Agricola
>
> KM0201 why do you use calibre-web instead of calibre? Just curious.

I had some issues w/ regular calibre on my phone for some reason... I can't even remember what the issue was it's been so long ago.... I switched to calibre-web, and it's worked like a charm. Being a creature of habit, it hasn't changed since.

-
  - May 24th 2021
  - #11

After all this time, I'm finally getting a complete handle on this reverse proxy. Usually I just fumbled through it via google, searching here, etc.. and it eventually I'd get it to work.

Now I actually understand what I'm doing. (Although the OMV one didn't work, used port 35000 and modified it with my IP, then forwarded 35000 to my server in my router and set up the CNAME.. would fail authentication)... but I've set up like 7-8 random things w/ zero issue. Most I don't even need reverse proxied, I just did it to try it.

-
  - May 24th 2021
  - #12

Quote from KM0201

> I tried adding network modes to their individual stacks to connect them to the swag network (nextcloud_default in my case)... but kept getting an error.

Here is an example with trilium, that I added to the nextcloud_default network (last 5 lines).

Code

```
version: '2.1'
services:
  trilium:
    image: zadam/trilium:0.46-latest
    container_name: trilium
    user: 1002:100
    restart: unless-stopped
    environment:
      - TRILIUM_DATA_DIR=/home/node/trilium-data
    ports:
      - "8088:8080"
    volumes:
      - /srv/dev-disk-by-label-
dataos/docker/trilium:/home/node/trilium-data
    networks:
        - nextcloud_default
networks:
 nextcloud_default:
   external: true
```

Display More

-
    - May 24th 2021
    - #13

Thanks... I'll look into that when I have some time Wednesday

-
    - May 24th 2021
    - #14

Maybe this is a useful if you want to juggle different networks in a compose file:

> Quote from Morlan
>
> Inspired by this thread I continued a project, which I had on my list for some time now. I wanted to put all my docker containers into a single docker-compose file. Just for

inspiration these are my `docker-compose.yml` and my `.env`. All I need to do is run a `docker-compose up -d` in the folder containing both files.

Code: .env

```
UID=1000
GID=100
TZ=Europe/Berlin
APPDIR=/srv/dev-disk-by-label-ssd/appdata
BACKUPDIR=/srv/dev-disk-by-label-ssd/backup
SYNCDIR=/srv/dev-disk-by-label-ssd/sync
RESTART=unless-stopped
```

Code: docker-compose.yml

```
version: "2.3"

services:
#################################
#PIHOLE
#
#
    pihole:
        container_name: pihole
        image: pihole/pihole:latest
        ports:
            - "53:53/tcp"
            - "53:53/udp"
            - "67:67/udp"
            - "80:80/tcp"
            - "443:443/tcp"
        environment:
            TZ: '${TZ}'
            WEBPASSWORD: 'myPW'
            ServerIP: '192.168.188.201'
            IPv6: 'false'
            DNS1: '1.1.1.1'
            DNS2: 'no'
        volumes:
            - ${APPDIR}/pihole:/etc/pihole/
            - ${APPDIR}/pihole/dnsmasq:/etc/dnsmasq.d/
        dns:
            - 127.0.0.1
#        cap_add:
```

```
#        - NET_ADMIN
        restart: ${RESTART}
        networks:
            pihole:
                ipv4_address: 192.168.188.201
#################################
#BITWARDEN
#
#
    bitwarden:
        image: bitwardenrs/server:raspberry
        container_name: bitwarden
        volumes:
            - ${APPDIR}/bitwarden:/data
            - ${APPDIR}/letsencrypt/log/bitwarden:/log
#Logfile is mounted to swag container for fail2ban
        environment:
            WEBSOCKET_ENABLED: 'true' # Required to use
websockets
            ADMIN_TOKEN: 'mytoken'
            LOG_FILE: 'log/bitwarden.log'
            LOG_LEVEL: 'warn'
            EXTENDED_LOGGING: 'true'
            TZ: '${TZ}'
        restart: ${RESTART}
        networks:
            my-net:
    bw_backup:
        image: bruceforce/bw_backup:rpi3
        container_name: bw_backup
        restart: ${RESTART}
        depends_on:
            - bitwarden
        volumes:
            - ${APPDIR}/bitwarden:/data/
            - /etc/timezone:/etc/timezone:ro
            - /etc/localtime:/etc/localtime:ro
            - ${BACKUPDIR}/bitwarden:/backup_folder/    #This
is where the db-backup is stored
        environment:
            - DB_FILE=/data/db.sqlite3
            - BACKUP_FILE=/backup_folder/backup.sqlite3
            - CRON_TIME=30 2 * * *
            - TIMESTAMP=true
            - DELETE_AFTER=30
            - UID=0
            - GID=0
            - TZ=${TZ}
        network_mode: "none"
#################################
#LETSENCRYPT - SWAG
#
#
    swag:
        image: linuxserver/swag
        container_name: swag
        cap_add:
            - NET_ADMIN
        environment:
            - PUID=${UID}
            - PGID=${GID}
            - TZ=${TZ}
            - URL=mydomain
            - SUBDOMAINS=mysubdomains
            - VALIDATION=http
            - EMAIL=myemail
        volumes:
            - ${APPDIR}/letsencrypt:/config
        ports:
            - 450:443
            - 90:80
        restart: ${RESTART}
        networks:
            my-net:
#################################
#NEXTCLOUDPI
#
#
    nextcloudpi:
        image: ownyourbits/nextcloudpi-armhf
        command: "url_of_my_ncp"
        container_name: nextcloudpi
        ports:
            - "4443:4443"
        volumes:
            - ${APPDIR}/nextcloudpi:/data
            - /etc/localtime:/etc/localtime:ro
            - ${SYNCDIR}:/mnt/sync     #This folder is mounted
as an external storage
            - ${BACKUPDIR}/calcardbackup:/ccb   #Backups of my
```

```
calendar and contacts via calcardbackup
            - ${BACKUPDIR}/ncp_backup:/ncp_backup  #Location
where the ncp-backups are stored
        restart: ${RESTART}
        networks:
            my-net:
#################################
#RESILIO_SYNC
#
#
    resilio-sync:
        image: linuxserver/resilio-sync
        container_name: resilio-sync
        environment:
            - PUID=33
            - PGID=33
            - TZ=${TZ}
            - UMASK_SET=000
        volumes:
            - ${APPDIR}/resilio-sync:/config
            - ${APPDIR}/resilio-sync/downloads:/downloads
            - ${SYNCDIR}:/sync
        ports:
            - 8888:8888
            - 55555:55555
        logging:
            options:
                max-size: "50m"
                max-file: "1"
        restart: ${RESTART}
        network_mode: "bridge"
#################################
#PORTAINER
#
#
    portainer:
        image: portainer/portainer
        container_name: portainer
        command: -H unix:///var/run/docker.sock
        restart: always
        ports:
            - 9000:9000
            - 8000:8000
        volumes:
            - /var/run/docker.sock:/var/run/docker.sock
            - ${APPDIR}/portainer:/data
networks:
    pihole:
        driver: macvlan
        driver_opts:
            parent: enx001e063676f8
        ipam:
            driver: default
            config:
                - subnet: 192.168.188.0/24
                  gateway: 192.168.188.1
                  ip-range: 192.168.188.201/32
    my-net:
        name: my-net
```

Display More

- May 24th 2021
- #15

Quote from KM0201

> Ended up just moving those compose files to my nextcloud stack, deleted the old containers and redeployed...

This was the way I had when I run everything in just one OMV: one single YML launching all services in order to have SWAG proxying those services.

But there's really no need to have any issues with the network or lack of communication between containers, if you edit the confs. (Of course, linuxserver did a excellent job with the proxy-confs and what is done here is just for specific cases)

Quote from KM0201

> After all this time, I'm finally getting a complete handle on this reverse proxy....
>
> Now I actually understand what I'm doing. (Although the OMV one didn't work, used port 35000 and modified it with my IP, then forwarded 35000 to my server in my router and set up the CNAME.. would fail authentication)... but I've set up like 7-8 random things w/ zero issue. Most I don't even need reverse proxied, I just did it to try it.

I should had explain a bit better why I created the "conf" and the real use of it:

My previously case scenario was:

1 RPi4 with OMV and Wireguard (let's call it by server name "omv1") with dockerized "SWAG/Nextcloud/MariaDB/Redis/Motioneye/Bitwarden".

Wireguard was my previously way to access the LAN and manipulate it (it still is for SSH).

Those services were accessed via WEB with the pre-made "*.subdomain.conf" from SWAG. ("motioneye.subdomain.conf" was created by me from a "trilium.subdomain..." after some tips from macom)

Since all services were on the same server (and same YML), it was easy and flawless to run without any need of editing files.

With this setup, only 2 ports needed to be open on the router (the one's for SWAG) and nothing else. (well 3 ports counting wireguard)

But after a while, I created a new NAS and the situation changed as my current scenario:

1 RPi4 **omv1** became OMV/Wireguard with only dockerized Motioneye (this was/is on an IP **192.168.1.86**)

1 RPi4 **omv2** became a NAS with the migrated services from the previous server (became IP **192.168.1.200**)

With this, I lost the reverse-proxy to "Motioneye". But that's when I decided to edit the conf on omv2 to point to the omv1 and see how it would work (these are the lines on the conf that matter) :

Code

```
    server_name motioneye.*; # NOTE: This is what will became the sub.subdomain.url
.......
        set $upstream_app 192.168.1.86; # NOTE: Edit with the LAN IP of where your service is running. Was "motioneye"
        set $upstream_port 8765;      # NOTE: Same port used on the service you want. Here is port:8765
        set $upstream_proto http; # NOTE: This is originally from "Trillium". Maybe can be changed to "https"
```

Restarted SWAG on omv2 and *presto*, I had again motioneye access via https://motioneye.mysubdomain.url

One problem solved: SWAG running on a server on LAN but also reversing services in another server on the same LAN.

After seeing people asking for access to OMV with https, I set my noodle to HOW this would be possible with SWAG since OMV is NOT on docker and on a complete diferent nginx.

Since I always changed the OMV port to something on the 5 digits area (hence the port:35000) I decided to just edit it as on post #3.

And, as explained, I now have 2 omv, so I created 2 equal confs (with different names) pointing each one to the proper IP/port to access the OMVs.

And it's working, I have https access to each of them without any need of opening more ports via WEB. (or wireguarding)

Honestly, there was no need (to me, due to wireguard) for this but, just to see how would it go, 🙂

- - May 24th 2021
  - #16

Just for completeness. You don’t need the resolver line in your conf file. This line is needed for the docker dns resolution. But since you are hard coding the ip, it’s not necessary.

-
- - May 24th 2021
  - #18

Quote from Morlan

> Just for completeness. You don’t need the resolver line in your conf file. This line is needed for the docker dns resolution. But since you are hard coding the ip, it’s not necessary.

You're absolutely right.

I can clean it better but, was just testing it without changing too much of the original 😉

- - May 24th 2021
  - #19

> Quote from Agricola
>
> I had to comment in this thread, mainly so I could easily find it and come back to it at a later date and try this out in combination with KM0201 ’s “cheap” domain name/Nextcloud setup. Good stuff.

I don't know if I ever updated it since I originally set it up, but I broke away from cloudflare. For some reason I kept losing my connection. It would work for a while, then I'd get the "cloudflare error screen" showing my server was disconnected. I'd restart the container, and it would be fine. I couldn't come up with any rhyme or reason as to why this was happening.

This has not happened to me since I stopped using cloudflare. The compose (specifically the swag part) I put in post #8 is the one I'm currently using and I've had zero issues with it.

-
  - May 24th 2021
  - #20

Thanks for the clarification KM0201

That is pretty much what I have with airsonic for audio books, Navidrome for music, ubooquity for ebooks (instead of calibre), and of course Nextcloud.

I won’t mess with it any time soon because it is all working so well, even though I have already bought a domain name for it.

Participate now!