

AI-03032 Docker Lab Deployment

👤 Owner	Ⓜ Rigel Arcayan
☰ Tags	Project
🕒 Created time	@September 26, 2025 10:15 AM

Help me build a Self-contained Docker Lab in my Ubuntu Server VM in Hyper-V

Docker Lab information and objectives:

- 1. Provide all the sudo commands I need to install and run Docker, Docker-Compo.se and Portainer, NGINX Proxy Manager, pgAdmin, phpMyAdmin with detailed functional descriptions.**
- 2. Provide Internet visibility of all docker applications using tailscale domain**
- 3. Create all necessary folders inside my ~/home/rarcayan/docker directory.**
- 4. Save all persistent volumes of MariaDB and PostgreSQL inside ~/home/rarcayan/docker.**
- 5. Create a unified necessary.env and docker-compose.yaml.**
- 6. Create a db init script to initialize MariaDB and PostgreSQL on first use.**
- 7. Use the Tailscale domain of my Ubuntu Host Server: ubuntuuser.tail3f76f1.ts.net.**
- 8. HostIP: 192.168.1.5, Gateway: 192.168.1.1**
- 9. Provide instructions on how to start the Docker Lab at first use.**
- 10. Provide instructions on how to access the completed apps from my internal network.**
- 11. Provide instructions on how to access the completed apps using the internet.**
- 12. Provide instructions on how to stop the Docker Lab safely without losing data.**

- 13. Provide instructions on how to stop the Docker Lab and wipe out all data to start over.**
- 14. Provide instructions on how to monitor the Docker Lab using Portainer.**
- 15. Provide instructions on how to monitor the Docker Lab using command lines.**
- 16. Provide a summary of sudo commands for simplicity.**

Folder Structure

~/home/rarcayan/docker (home of each of the applications and db)

~/home/rarcayan/docker/portainer

~/home/rarcayan/docker/NGINX

~/home/rarcayan/docker/mariadb

~/home/rarcayan/docker/postgresql

~/home/rarcayan/docker/wikijs

~/home/rarcayan/docker/osTicket

~/home/rarcayan/docker/OpenEMR

Database and Container Environment Information:

Portainer Container

NGINX Container for Reverse Proxy

Mariadb Container for Wordpress, osTicket, OpenEMR Database

Postgresql Container for OpenProject and Wikijs Database

Network Container for Wikijs osTicket, OpenEMR, (in one subnet)

Wikijs Container

osTicket Container

OpenEMR Container

Wikijs Port=801

osTicket Port=802

OpenEMR Port=803

WikijsDB, wikijs_user, password=@SecurePassword

osTicketDB, osticket_user, password=@SecurePassword!

OpenEMRDB, openemr_user, password=@SecurePassword!

Nice—I'll build the complete, self-contained Docker lab for your Ubuntu Server VM (host IP `192.168.1.5`) and place everything under your requested folder structure. I'll include:

- all `sudo` commands to install Docker, Compose plugin and Portainer,
- the unified `necessary.env` file,
- a full `docker-compose.yml`,
- DB init scripts for MariaDB & PostgreSQL (run only on first initialization),
- folder creation commands,
- instructions for using Tailscale hostname `ubuntuserver.tail3f76f1.ts.net` (path-based proxy),
- start/stop/wipe procedures, monitoring with Portainer and CLI, and a short `sudo` command summary.

I assumed no other pre-existing services conflict with the host ports below. I used the database credentials you supplied and mapped application ports you requested (Wikijs 801, osTicket 802, OpenEMR 803). If you want different port mappings later, change them in `docker-compose.yml`.

1) Preliminaries — create folder structure & move into it

Run these commands on your Ubuntu host (replace `rarcayan` if your username differs). These create the top-level docker folder and subfolders for each service and DB init script locations:

```
# create base and app folders
sudo mkdir -p /home/rarcayan/docker/{portainer,NGINX,mariadb,postgresql,
wikijs,osTicket,OpenEMR}
```

```
sudo mkdir -p /home/rarcayan/docker/mariadb/init
sudo mkdir -p /home/rarcayan/docker/postgresql/init
sudo mkdir -p /home/rarcayan/docker/NGINX/data
sudo chown -R $(whoami):$(whoami) /home/rarcayan/docker
cd /home/rarcayan/docker
```

2) Install Docker, Docker Compose plugin, Portainer (sudo commands)

Run these commands in order (works on Ubuntu 20.04+). They install Docker Engine, the Compose plugin, and set up Docker to run without repeatedly using `sudo` (optional but handy). They also install Tailscale (so your host is reachable at the tailscale domain) and then set up Portainer as a container.

```
# Update + prerequisites
sudo apt update
sudo apt -y install ca-certificates curl gnupg lsb-release apt-transport-https

# Add Docker official GPG + repo
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor
or -o /usr/share/keyrings/docker-archive-keyring.gpg
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-
er-archive-keyring.gpg] \
  https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" \
  | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt update
sudo apt -y install docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin

# Add your user to docker group (logout/login required to take effect)
sudo usermod -aG docker $(whoami)
```

```
# Install Tailscale (so host gets tailscale domain)
curl -fsSL https://tailscale.com/install.sh | sh
# Start/enable tailscaled (then run `tailscale up` interactively to authenticate)
sudo systemctl enable --now tailscaled

# Optional: (if you prefer) install docker-compose v2 binary instead of plugin
(skip if plugin is installed)
# sudo curl -L "https://github.com/docker/compose/releases/download/v2.2
0.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-co
mpose
# sudo chmod +x /usr/local/bin/docker-compose

# Pull some images in advance
docker pull portainer/portainer-ce:latest
docker pull jc21/nginx-proxy-manager:latest
docker pull mariadb:10.11
docker pull postgres:15
docker pull overlord/pgadmin4:latest || docker pull dpage/pgadmin4:latest
docker pull phpmyadmin/phpmyadmin:latest
docker pull requarks/wiki:latest
# (for osTicket and OpenEMR choose tested images)
```

Notes:

- After `usermod -aG docker`, **log out and log back in** (or `newgrp docker`) so your shell can use `docker` without sudo.
- For Tailscale, once the package is installed run `sudo tailscale up` and follow the auth link to log into your tailscale account. After auth your host will be reachable at `ubuntuserver.tail3f76f1.ts.net` (as you provided).

3) `necessary.env` — unified environment variables

Create `/home/rarcayan/docker/necessary.env` with these contents. Save exactly (no extra spaces). Replace values only if you want different passwords later.

```
# necessary.env - place in /home/rarcayan/docker
# General
HOST_IP=192.168.1.5
TAILSCALE_DOMAIN=ubuntuserver.tail3f76f1.ts.net

# MariaDB (for Wordpress, osTicket, OpenEMR)
MARIADB_ROOT_PASSWORD=@SecurePasswordRoot
MARIADB_WIKI_DB=wikijsdb
MARIADB_WIKI_USER=wikijs_user
MARIADB_WIKI_PASSWORD=@SecurePassword
MARIADB_OSTICKET_DB=osticketdb
MARIADB_OSTICKET_USER=osticket_user
MARIADB_OSTICKET_PASSWORD=@SecurePassword!
MARIADB_OPENEMR_DB=openemrdb
MARIADB_OPENEMR_USER=openemr_user
MARIADB_OPENEMR_PASSWORD=@SecurePassword!

# PostgreSQL (for Wikijs if you change to postgres or other apps)
POSTGRES_DB=wikijs
POSTGRES_USER=wikijs_user
POSTGRES_PASSWORD=@SecurePassword
POSTGRES_INIT_DB=openprojectdb
POSTGRES_INIT_USER=openproject_user
POSTGRES_INIT_PASSWORD=@SecurePassword!

# Portainer
PORTAINER_ADMIN_PASSWORD=ChangeMePortainerP@ssw0rd

# NGINX Proxy Manager DB (sqlite built-in for NPM so not required)
# Other app-specific envs can be defined here as needed
```

Keep necessary.env secure (contains passwords). @ characters are allowed; we wrapped as plain text.

4) DB init scripts (first-run only)

Place these files where the compose file will mount them so database images execute them on first initialization.

MariaDB init: `/home/rarcayan/docker/mariadb/init/init.sql`

```
-- init.sql for MariaDB (runs on first container start)
-- create databases and users for each app, grant privileges

CREATE DATABASE IF NOT EXISTS wikijsdb CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE DATABASE IF NOT EXISTS osticketdb CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE DATABASE IF NOT EXISTS openemrdb CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

-- wikijs user
CREATE USER IF NOT EXISTS 'wikijs_user'@'%' IDENTIFIED BY '@SecurePassword!';
GRANT ALL PRIVILEGES ON wikijsdb.* TO 'wikijs_user'@'%';

-- osticket user
CREATE USER IF NOT EXISTS 'osticket_user'@'%' IDENTIFIED BY '@SecurePassword!';
GRANT ALL PRIVILEGES ON osticketdb.* TO 'osticket_user'@'%';

-- openemr user
CREATE USER IF NOT EXISTS 'openemr_user'@'%' IDENTIFIED BY '@SecurePassword!';
GRANT ALL PRIVILEGES ON openemrdb.* TO 'openemr_user'@'%';

FLUSH PRIVILEGES;
```

PostgreSQL init: `/home/rarcayan/docker/postgresql/init/init.sql`

```

-- init.sql for PostgreSQL (runs on first container start)
-- create extra DB and user examples (edit if needed)

CREATE USER openproject_user WITH PASSWORD '@SecurePassword!';
CREATE DATABASE openprojectdb;
GRANT ALL PRIVILEGES ON DATABASE openprojectdb TO openproject_user;

-- Wikijs PostgreSQL DB (if you prefer Postgres for wikijs)
CREATE USER wikijs_user WITH PASSWORD '@SecurePassword';
CREATE DATABASE wikijs OWNER wikijs_user;

```

Notes:

- The MariaDB image executes `.sql` files in `/docker-entrypoint-initdb.d/` on first initialization. We mount our host `mariadb/init` folder there in compose.
- Similarly Postgres runs `.sql` files mounted at `/docker-entrypoint-initdb.d/`.

5) `docker-compose.yml` — unified compose file

Create `/home/rarcayan/docker/docker-compose.yml` with the following content. This brings up Portainer, NGINX Proxy Manager (NPM), MariaDB, PostgreSQL, phpMyAdmin, pgAdmin, Wiki.js, osTicket, and OpenEMR. I used `lab_net` bridge network for internal communications.

Save this file in `/home/rarcayan/docker/docker-compose.yml`.

```

version: "3.8"

services:

  # Portainer - UI to manage your Docker environment
  portainer:
    image: portainer/portainer-ce:latest

```

```
container_name: portainer
restart: unless-stopped
command: -H unix:///var/run/docker.sock
volumes:
  - /var/run/docker.sock:/var/run/docker.sock
  - ./portainer/data:/data
ports:
  - "9000:9000"
networks:
  - lab_net
```

NGINX Proxy Manager - reverse proxy and web UI

```
nginx-proxy:
  image: jc21/nginx-proxy-manager:latest
  container_name: nginx-proxy
  restart: unless-stopped
  ports:
    - "80:80" # HTTP
    - "81:81" # NPM UI
    - "443:443" # HTTPS (if you later add certs)
  volumes:
    - ./NGINX/data:/data
    - ./NGINX/letsencrypt:/etc/letsencrypt
  environment:
    - DISABLE_IPV6=true
  networks:
    - lab_net
```

MariaDB

```
mariadb:
  image: mariadb:10.11
  container_name: mariadb
  restart: unless-stopped
  environment:
    MYSQL_ROOT_PASSWORD: "${MARIADB_ROOT_PASSWORD}"
  volumes:
```

- ./mariadb/data:/var/lib/mysql
- ./mariadb/init:/docker-entrypoint-initdb.d

networks:

- lab_net

phpMyAdmin (to manage MariaDB)

phpmyadmin:

image: phpmyadmin/phpmyadmin:latest

container_name: phpmyadmin

restart: unless-stopped

environment:

PMA_HOST: mariadb

UPLOAD_LIMIT: 300M

ports:

- "8080:80"

networks:

- lab_net

PostgreSQL

postgresql:

image: postgres:15

container_name: postgresql

restart: unless-stopped

environment:

POSTGRES_PASSWORD: "\${POSTGRES_PASSWORD}"

POSTGRES_USER: "\${POSTGRES_USER}"

POSTGRES_DB: "\${POSTGRES_DB}"

volumes:

- ./postgresql/data:/var/lib/postgresql/data
- ./postgresql/init:/docker-entrypoint-initdb.d

networks:

- lab_net

pgAdmin for Postgres

pgadmin:

image: dpage/pgadmin4:latest

```
container_name: pgadmin
restart: unless-stopped
environment:
  PGADMIN_DEFAULT_EMAIL: "admin@local"
  PGADMIN_DEFAULT_PASSWORD: "admin"
ports:
  - "5050:80"
networks:
  - lab_net
```

Wiki.js (runs on node, default port 3000 → map to 801)

```
wikijs:
  image: requarks/wiki:2
  container_name: wikijs
  restart: unless-stopped
  environment:
    DB_TYPE: mariadb
    DB_HOST: mariadb
    DB_PORT: 3306
    DB_USER: "${MARIADB_WIKI_USER}"
    DB_PASS: "${MARIADB_WIKI_PASSWORD}"
    DB_NAME: "${MARIADB_WIKI_DB}"
  volumes:
    - ./wikijs/data:/var/wiki
  ports:
    - "801:3000"
  networks:
    - lab_net
```

osTicket (example official image or community)

```
osticket:
  image: osticket/osticket:latest
  container_name: osticket
  restart: unless-stopped
  environment:
    - MYSQL_HOST=mariadb
```

```
- MYSQL_DATABASE=${MARIADB_OSTICKET_DB}
- MYSQL_USER=${MARIADB_OSTICKET_USER}
- MYSQL_PASSWORD=${MARIADB_OSTICKET_PASSWORD}
```

volumes:

```
- ./osTicket/data:/var/www/html
```

ports:

```
- "802:80"
```

networks:

```
- lab_net
```

OpenEMR (example image that uses MariaDB)

openemr:

image: openemr/openemr:latest

container_name: openemr

restart: unless-stopped

environment:

```
- MYSQL_HOST=mariadb
```

```
- MYSQL_ROOT_PASSWORD=${MARIADB_ROOT_PASSWORD}
```

```
- MYSQL_PORT=3306
```

volumes:

```
- ./OpenEMR/data:/var/www/localhost/htdocs
```

ports:

```
- "803:80"
```

networks:

```
- lab_net
```

networks:

lab_net:

driver: bridge

Notes & choices:

- I used MariaDB as the single relational DB for wikijs (you supplied MariaDB credentials) and for osticket and openemr.
- `wikijs` image configured for MariaDB (`DB_TYPE=mariadb`). If you prefer to use PostgreSQL for Wiki.js instead, change `DB_TYPE` to `postgres` and DB vars to point

at `postgresql` container.

- `jc21/nginx-proxy-manager` provides an admin UI on host port `81` (user/initial password you'll set via NPM UI).
- I exposed phpMyAdmin on `8080` and pgAdmin on `5050` for quick DB UI access on internal network. You can expose them via NPM for internet access too (path/subdomain proxy).
- All persistent DB data is stored in `/home/rarcayan/docker/mariadb/data` and `/home/rarcayan/docker/postgresql/data`.

6) Fill `.env` file: make Docker Compose read `necessary.env`

Create a `.env` file in `/home/rarcayan/docker/.env` pointing to `necessary.env` values. Docker Compose automatically reads `.env`. For clarity create `.env` mirroring `necessary.env` names:

```
# from /home/rarcayan/docker/  
cp necessary.env .env
```

(Or create `.env` with the same content as `necessary.env`.)

7) Start the Docker Lab (first use) — step-by-step

1. Make sure tailscaled is running and you have authenticated:

```
sudo tailscale up  
# follow the printed URL to authenticate your machine into your Tailscale account
```

After auth your host should be reachable at `ubuntuuserver.tail3f76f1.ts.net`.

2. In `/home/rarcayan/docker` bring up containers for first-time initialization:

```
cd /home/rarcayan/docker
docker compose up -d
```

(If your system uses the `docker-compose` binary rather than plugin, run `docker-compose up -d`.)

3. Watch init logs to ensure DB init executed:

```
docker logs -f mariadb
docker logs -f postgresql
```

The MariaDB container will run `mariadb/init/init.sql` only the first time it starts. If DB already exists it will skip.

4. Access Portainer web UI to manage the stack:

- Open `http://192.168.1.5:9000` on your local network (or `http://ubuntuserver.tail3f76f1.ts.net:9000` over tailscale).
- Create admin user when prompted (password set in `necessary.env` is for internal use only — Portainer sets its own admin user on first run).

5. Access NGINX Proxy Manager UI:

- `http://192.168.1.5:81` (internal)
- Default login for NPM: `admin@example.com` / `changeme` for first login (you'll be prompted to reset). If NPM version asks you to create your own admin credentials, do so.

6. Confirm Wiki.js, osTicket, OpenEMR:

- Internal IP access:
 - Wiki.js: `http://192.168.1.5:801`
 - osTicket: `http://192.168.1.5:802`
 - OpenEMR: `http://192.168.1.5:803`
- DB GUIs:

- phpMyAdmin: `http://192.168.1.5:8080` (connect to host `mariadb`, use user root or the created users)
- pgAdmin: `http://192.168.1.5:5050`

8) Configure Internet visibility via your Tailscale Domain

Goal: use `ubuntuserver.tail3f76f1.ts.net` as the externally reachable domain. We'll configure NGINX Proxy Manager to forward specific path prefixes to internal ports.

1. Ensure your host is reachable at `ubuntuserver.tail3f76f1.ts.net` via Tailscale. From an external machine with tailscale or through your tailscale auth, verify:

```
ping ubuntuserver.tail3f76f1.ts.net
```

2. In NGINX Proxy Manager UI (`http://<host>:81`):

- Create **Proxy Host** entries (or **Custom Location** if you prefer path-based) for each app:
 - **Domain Names:** `ubuntuserver.tail3f76f1.ts.net`
 - **Scheme:** `http`
 - **Forward Hostname / IP:** `127.0.0.1` or `192.168.1.5`
 - **Forward Port:**
 - Wiki.js → `801`
 - osTicket → `802`
 - OpenEMR → `803`
 - **Block Common Exploits:** checked
 - For path-based proxy (recommended to avoid subdomain DNS config), in the `Advanced` or `Custom Locations` section add locations:

- `/wikijs` proxy to `http://192.168.1.5:801` (strip prefix if app expects root — use NPM's advanced location options to rewrite)
 - `/osticket` → `http://192.168.1.5:802`
 - `/openemr` → `http://192.168.1.5:803`
- Alternatively, if you can create subdomains in your tailscale DNS/custom names:
 - `wikijs.ubuntuuserver.tail3f76f1.ts.net` → forward to `192.168.1.5:801`
 - `osticket.ubuntuuserver.tail3f76f1.ts.net` → `192.168.1.5:802`
 - `openemr.ubuntuuserver.tail3f76f1.ts.net` → `192.168.1.5:803`

(This requires you control DNS for `ubuntuuserver.tail3f76f1.ts.net` or to use Tailscale's MagicDNS & tags. Path-based proxy is simpler and works immediately.)

3. Access from Internet (or other Tailscale devices):

- `https://ubuntuuserver.tail3f76f1.ts.net/wikijs` or via the proxy host/subdomain you configured.
- If you're using Tailscale only and don't have public port-forwarding from your LAN router, access will work from other machines on your Tailscale network or via the tailscale domain.

Important: Tailscale provides secure connectivity; exposing services to the public internet beyond your tailscale network requires additional DNS/port forwarding or a public IP — proceed with caution (secure your apps and NPM UI with strong passwords and SSL).

9) How to access the completed apps from internal network

Open a web browser on a machine on the same LAN:

- Portainer: `http://192.168.1.5:9000`
- NGINX Proxy Manager: `http://192.168.1.5:81`

- Wiki.js: <http://192.168.1.5:801>
 - osTicket: <http://192.168.1.5:802>
 - OpenEMR: <http://192.168.1.5:803>
 - phpMyAdmin: <http://192.168.1.5:8080>
 - pgAdmin: <http://192.168.1.5:5050>
-

10) How to access the completed apps from the internet (via Tailscale domain)

If you configured NGINX Proxy Manager (path or subdomain), use:

- Wiki.js: <https://ubuntuserver.tail3f76f1.ts.net/wikijs> (or subdomain if set)
- osTicket: <https://ubuntuserver.tail3f76f1.ts.net/osticket>
- OpenEMR: <https://ubuntuserver.tail3f76f1.ts.net/openemr>

If you want true public access (anyone on the internet) and not just Tailscale devices, you must:

- Expose the host via a public IP or port-forward from your home router, and
- Acquire/assign DNS records and secure TLS certs (NPM supports Let's Encrypt).

Proceed only if you understand the security implications; secure every service with strong passwords and consider further firewall rules.

11) Safe stop/restart without losing data

To safely stop everything (preserves volumes/data):

```
cd /home/rarcayan/docker
docker compose stop      # stops containers gracefully
# or to stop & remove containers but keep volumes & images:
docker compose down
```

```
# to only stop specific container:  
docker stop portainer
```

To restart:

```
docker compose up -d
```

Stopping with `docker compose down` without `-v` preserves named volumes & bind-mounts (we used bind-mounts to `/home/rarcayan/docker/...` so data remains). Avoid `docker compose down -v` if you want to preserve DBs.

12) Wipe everything and start over (destroy data)

WARNING: this deletes all persistent data in your defined folders.

```
cd /home/rarcayan/docker  
docker compose down -v # stops and removes containers and named volumes  
# remove all data folders:  
rm -rf /home/rarcayan/docker/portainer/data \  
    /home/rarcayan/docker/nginx/data \  
    /home/rarcayan/docker/mariadb/data \  
    /home/rarcayan/docker/postgresql/data \  
    /home/rarcayan/docker/wikijs/data \  
    /home/rarcayan/docker/osTicket/data \  
    /home/rarcayan/docker/OpenEMR/data  
  
# optionally remove init scripts if you want fresh init:  
rm -rf /home/rarcayan/docker/mariadb/init /home/rarcayan/docker/postgresql/init
```

To recreate from scratch, recreate the init scripts and `docker compose up -d` again.

13) Monitoring the Docker Lab via Portainer

1. Open Portainer UI: `http://192.168.1.5:9000` .
2. Add the local Docker environment (Portainer likely detects it automatically via `/var/run/docker.sock`).
3. From Portainer you can:
 - View containers, images, volumes, networks.
 - See logs for each container.
 - Start/stop/restart containers.
 - Create scheduled backups (you can backup volume folders or `mysqldump` exports).
 - Watch container stats (CPU, memory, network).

Portainer is extremely user friendly for day-to-day container management.

14) Monitoring via CLI (command-line)

Useful commands:

```
# list running containers
docker ps

# full list
docker ps -a

# view logs (follow)
docker logs -f <container_name>

# show docker stats (live)
docker stats

# inspect container details
docker inspect <container_name>
```

```
# view networks
docker network ls
```

```
# view volumes (not used for bind mounts but listed)
docker volume ls
```

For compose-specific control:

```
cd /home/rarcayan/docker
docker compose ps
docker compose logs -f      # all compose logs
docker compose logs -f wikijs # logs for specific service
```

15) Additional suggestions & hardening

- **Backups:** regularly back up `/home/rarcayan/docker/mariadb/data` and important SQL dumps. For OpenEMR, export patient DB regularly.
- **Passwords:** rotate DB and admin passwords. Keep `necessary.env` protected (chmod 600).
- **SSL:** use NGINX Proxy Manager to obtain Let's Encrypt certificates (if your tailscale domain supports public validation or you can use DNS-01 with your DNS provider). For Tailscale-only access, TLS within your Tailscale network may not require public certs; you can secure with self-signed certs or use Tailscale's own ACL/TLS solutions.
- **Firewall:** ensure your router/firewall rules only open necessary ports; prefer Tailscale for secure remote access.
- **Testing:** bring up apps one at a time if you encounter conflicts; check `docker logs` .

16) Quick summary of important commands (for simplicity) sudo

1. Update & install Docker + Compose plugin

```
sudo apt update
```

```
sudo apt -y install ca-certificates curl gnupg lsb-release apt-transport-https  
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearm  
or -o /usr/share/keyrings/docker-archive-keyring.gpg
```

```
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/  
docker-archive-keyring.gpg] \  
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo t  
ee /etc/apt/sources.list.d/docker.list
```

```
sudo apt update
```

```
sudo apt update
```

```
sudo apt -y install docker-ce docker-ce-cli containerd.io docker-buildx-plugin  
docker-compose-plugin
```

2. Add yourself to docker group

```
sudo usermod -aG docker $(whoami)
```

3. Install Tailscale

```
curl -fsSL https://tailscale.com/install.sh | sh
```

```
sudo systemctl enable --now tailscaled
```

```
sudo tailscale up # run interactively and authenticate
```

4. Start the docker lab

```
cd /home/rarcayan/docker
```

```
docker compose up -d
```

5. Stop safely

```
docker compose stop
```

```
# or
```

```
docker compose down
```

6. Wipe data (dangerous)

```
docker compose down -v
sudo rm -rf /home/rarcayan/docker/* # careful: deletes everything
```

17) Troubleshooting pointers

- If `docker compose up -d` fails due to permissions: ensure you logged out and back in after `usermod -aG docker`, or run `newgrp docker`.
- If ports are already in use, identify with `sudo ss -tulpn | grep :80` etc., stop the conflicting service (e.g., `sudo systemctl stop apache2`) or change the host port in `docker-compose.yml`.
- If DB init didn't run: check `docker logs mariadb`. MariaDB runs init scripts only when the DB directory is empty.
- If Wiki.js fails to connect to DB, re-check DB credentials in `.env` and restart `wikajs` container.

18) Small checklist to start right now

1. Copy `necessary.env`, `docker-compose.yml` and init scripts to `/home/rarcayan/docker`.
2. Create folder structure (we gave commands earlier).
3. Run the Docker/Tailscale install commands above.
4. Authenticate Tailscale (`sudo tailscale up`).
5. `cd /home/rarcayan/docker && docker compose up -d`
6. Use Portainer & NGINX Proxy Manager to configure web access and manage containers.

If you want, I can now:

- produce the exact `docker-compose.yml`, `necessary.env`, and the two init SQL files as downloadable single text blobs you can copy/paste, or
- adapt this compose to run Wiki.js on PostgreSQL instead of MariaDB (if you prefer postgres for wiki), or

- make NGINX Proxy Manager configuration CLI commands (so you don't need to use its web UI).

Which of those would you like me to generate right away?

ChatGPT Version 2

Direct answer — self-contained Docker Lab for your Ubuntu Server VM

Below is a complete, ready-to-run Docker Lab plan that meets your objectives. It includes:

- All `sudo` commands to install Docker, Docker Compose plugin, and Portainer.
- A single `necessary.env` and a `docker-compose.yml` that creates the services you requested (Portainer, Nginx Proxy Manager, MariaDB, PostgreSQL, phpMyAdmin, pgAdmin, Wiki.js, osTicket, OpenEMR).
- Init scripts for MariaDB and PostgreSQL (run on first initialization) placed in your data folders.
- All persistent storage mapped inside `/home/rarcayan/docker/...`.
- A user-defined Docker network (`app_net`) where Wiki.js, osTicket, and OpenEMR live in the same subnet with fixed IPs.
- Instructions to start/stop safely, wipe and start over, and monitor via Portainer and the CLI.
- Notes on exposing services via your Tailscale domain `ubuntuserver.tail3f76f1.ts.net` (how to access via Tailscale and caveats about Let's Encrypt).

I made conservative choices so things work reliably on a typical Ubuntu Server VM in Hyper-V and so your DB files stay inside `/home/rarcayan/docker` .

Key reasons / design decisions (concise)

1. **User-defined bridge network** (`app_net`) with fixed IPs — keeps Wiki.js, osTicket, OpenEMR in the same subnet as you requested while avoiding macvlan complexity on Hyper-V.
 2. **DB init scripts in** `docker-entrypoint-initdb.d` — standard and reliable method for MySQL/MariaDB and PostgreSQL to create DBs and users at first run.
 3. **All volumes inside** `/home/rarcayan/docker` — one folder for backups and simple host-level access.
 4. **Nginx Proxy Manager** for reverse proxy and easy host-based routing (you'll create proxy hosts like `wikis.ubuntuuserver.tail3f76f1.ts.net` pointing to the appropriate container).
 5. **Tailscale domain:** you can access services via `ubuntuuserver.tail3f76f1.ts.net` from any device on your Tailscale network. Let's Encrypt may not be able to issue certs for Tailscale domains from inside NPM — see the *Access via Internet* section for details and alternatives.
-

Full step-by-step Action Plan (do this now on your Ubuntu VM)

Notes:

- Replace `rarcayan` with your actual Ubuntu username if different.
 - Paths use `/home/rarcayan/docker` (clean standard path, equivalent to `~/docker` when logged in as `rarcayan`).
 - I assume you already installed and configured Tailscale and that your host is reachable at `ubuntuuserver.tail3f76f1.ts.net` from other Tailscale devices.
-

0) Quick checklist before starting

- Host IP: `192.168.1.5`
- Gateway: `192.168.1.1`
- Tailscale domain: `ubuntuuserver.tail3f76f1.ts.net`

- Project root: `/home/rarcayan/docker`

1) Create folders and set ownership (run as your user; `sudo` where shown)

```
# if not already in your home
cd /home/rarcayan

# create base dir and subdirs (all persistent data here)
sudo mkdir -p /home/rarcayan/docker/{portainer,NGINX,mariadb,postgresql,
wikijs,osTicket,OpenEMR,pgadmin,phpmyadmin}
sudo chown -R $(whoami):$(whoami) /home/rarcayan/docker
```

2) Install Docker, Docker Compose plugin, and prerequisites

Run the following commands (Ubuntu recommended method):

```
# 1. Update & install prerequisites
sudo apt update
sudo apt install -y ca-certificates curl gnupg lsb-release

# 2. Add Docker official GPG key and repository
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearm
or -o /etc/apt/keyrings/docker.gpg
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docke
r.gpg] \
  https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" \
  | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt update
```

```
# 3. Install Docker Engine and required packages
sudo apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

```
# 4. Add your user to 'docker' group to run docker without sudo (log out/in after this)
sudo usermod -aG docker $(whoami)
```

Important: Log out and log back in (or run `newgrp docker`) so your user is in the `docker` group.

3) Portainer (UI management) — quick install (via Docker Compose in our main compose later)

We include Portainer in the `docker-compose.yml`. If you want to bootstrap Portainer right away (optional), run:

```
# optional immediate Portainer install (standalone)
docker volume create portainer_data
docker run -d --name portainer --restart=always -p 9000:9000 \
-v /var/run/docker.sock:/var/run/docker.sock \
-v portainer_data:/data portainer/portainer-ce:latest
```

4) Create `necessary.env`

Create `/home/rarcayan/docker/necessary.env` with this content (safe to change passwords before use):

```
# File: /home/rarcayan/docker/necessary.env
# Host and network
HOST_IP=192.168.1.5
TZ=Asia/Manila

# MariaDB (for osTicket & OpenEMR)
MARIADB_ROOT_PASSWORD=RootPass@ReplaceMe
```

```
OSTICKET_DB=osTicketDB
OSTICKET_USER=osticket_user
OSTICKET_PASSWORD=@SecurePassword!
OPENEMR_DB=OpenEMRDB
OPENEMR_USER=openemr_user
OPENEMR_PASSWORD=@SecurePassword!

# PostgreSQL (for Wiki.js)
POSTGRES_PASSWORD=PostgresRootPass@ReplaceMe
WIKIJS_DB=wikijsdb
WIKIJS_USER=wikijs_user
WIKIJS_PASSWORD=@SecurePassword

# Service ports (internal app ports; NPM will proxy them)
WIKIJS_PORT=801
OSTICKET_PORT=802
OPENEMR_PORT=803

# Nginx Proxy Manager admin
NPM_EMAIL=admin@ubuntuserver.tail3f76f1.ts.net
NPM_PASS=ChangeMeAdminPass

# pgAdmin
PGADMIN_DEFAULT_EMAIL=pgadmin@ubuntuserver.tail3f76f1.ts.net
PGADMIN_DEFAULT_PASSWORD=pgadmin_pass
```

Save the file. Make sure file permissions are safe:

```
chmod 600 /home/rarcayan/docker/necessary.env
```

5) Create database init scripts

MariaDB (MySQL/MariaDB) init script

Create a file `/home/rarcayan/docker/mariadb/init-mariadb.sql` with:

```

-- /home/rarcayan/docker/mariadb/init-mariadb.sql
CREATE DATABASE IF NOT EXISTS osTicketDB CHARACTER SET utf8mb4 CO
LLATE utf8mb4_unicode_ci;
CREATE DATABASE IF NOT EXISTS OpenEMRDB CHARACTER SET utf8mb4 C
OLLATE utf8mb4_unicode_ci;

CREATE USER IF NOT EXISTS 'osticket_user'@'%' IDENTIFIED BY '@SecureP
assword!';
CREATE USER IF NOT EXISTS 'openemr_user'@'%' IDENTIFIED BY '@Secure
Password!';

GRANT ALL PRIVILEGES ON osTicketDB.* TO 'osticket_user'@'%';
GRANT ALL PRIVILEGES ON OpenEMRDB.* TO 'openemr_user'@'%';

FLUSH PRIVILEGES;

```

PostgreSQL init scripts

Place the following two files in `/home/rarcayan/docker/postgresql/`:

1. `/home/rarcayan/docker/postgresql/init-user-db.sh` (make executable)

```

#!/bin/bash
set -e

# This script will be run by the Postgres image when the DB is first created.
psql --username "$POSTGRES_USER" <<-EOSQL
CREATE DATABASE wikijsdb;
CREATE USER wikijs_user WITH ENCRYPTED PASSWORD '@SecurePasswor
d';
GRANT ALL PRIVILEGES ON DATABASE wikijsdb TO wikijs_user;
EOSQL

```

Make it executable:

```
chmod +x /home/rarcayan/docker/postgresql/init-user-db.sh
```

Note: The official `postgres` image will run `*.sh` in `/docker-entrypoint-initdb.d` on first initialization.

6) Create `docker-compose.yml`

Create `/home/rarcayan/docker/docker-compose.yml` with the following content. This composition uses a custom `app_net` so Wiki.js, osTicket, and OpenEMR share a subnet and have static IPs.

```
version: "3.8"

services:
  # ----- Portainer -----
  portainer:
    image: portainer/portainer-ce:latest
    container_name: portainer
    restart: unless-stopped
    ports:
      - "9000:9000"
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - /home/rarcayan/docker/portainer/data:/data

  # ----- NGINX Proxy Manager -----
  nginx-proxy:
    image: jc21/nginx-proxy-manager:latest
    container_name: nginx-proxy
    environment:
      DB_MYSQL_HOST: "mariadb"
      DB_MYSQL_PORT: 3306
      DB_MYSQL_USER: "npm"
      DB_MYSQL_PASSWORD: "npm_db_password"
      DB_MYSQL_NAME: "npm"
```

```

restart: unless-stopped
ports:
  - "80:80"    # HTTP
  - "81:81"    # admin UI
  - "443:443"  # HTTPS
volumes:
  - /home/rarcayan/docker/NGINX/data:/data
  - /home/rarcayan/docker/NGINX/letsencrypt:/etc/letsencrypt

# ----- MariaDB for osTicket & OpenEMR and NPM (NPM needs its own user/
db) -----
mariadb:
  image: mariadb:10.6
  container_name: mariadb
  restart: unless-stopped
  environment:
    MYSQL_ROOT_PASSWORD: "${MARIADB_ROOT_PASSWORD}"
    TZ: "${TZ}"
  volumes:
    - /home/rarcayan/docker/mariadb/data:/var/lib/mysql
    - /home/rarcayan/docker/mariadb/init-mariadb.sql:/docker-entrypoint-init
db.d/init-mariadb.sql:ro
  ports:
    - "3306:3306"

# Create a small service to prepare NPM DB user (NPM requires DB named n
pm)
npm_db_init:
  image: mariadb:10.6
  command: ["sh", "-c", "sleep 5; mysql -h mariadb -u root -p\"${MARIADB_R
OOT_PASSWORD}\" -e \"CREATE DATABASE IF NOT EXISTS npm; CREATE US
ER IF NOT EXISTS 'npm'@'%' IDENTIFIED BY 'npm_db_password'; GRANT AL
L PRIVILEGES ON npm.* TO 'npm'@'%'; FLUSH PRIVILEGES;\""]
  environment:
    MYSQL_ROOT_PASSWORD: "${MARIADB_ROOT_PASSWORD}"
  depends_on:

```

```
- mariadb
restart: "no"

# ----- PostgreSQL -----
postgresql:
  image: postgres:15
  container_name: postgresql
  restart: unless-stopped
  environment:
    POSTGRES_PASSWORD: "${POSTGRES_PASSWORD}"
    POSTGRES_USER: postgres
    TZ: "${TZ}"
  volumes:
    - /home/rarcayan/docker/postgresql/data:/var/lib/postgresql/data
    - /home/rarcayan/docker/postgresql/init-user-db.sh:/docker-entrypoint-initdb.d/init-user-db.sh:ro
  ports:
    - "5432:5432"

# ----- pgAdmin (optional) -----
pgadmin:
  image: dpage/pgadmin4:latest
  container_name: pgadmin
  restart: unless-stopped
  environment:
    PGADMIN_DEFAULT_EMAIL: "${PGADMIN_DEFAULT_EMAIL}"
    PGADMIN_DEFAULT_PASSWORD: "${PGADMIN_DEFAULT_PASSWORD}"
  ports:
    - "8080:80"
  volumes:
    - /home/rarcayan/docker/pgadmin/data:/var/lib/pgadmin

# ----- phpMyAdmin (optional) -----
phpmyadmin:
  image: phpmyadmin/phpmyadmin:latest
  container_name: phpmyadmin
```

```
restart: unless-stopped
environment:
  PMA_HOST: mariadb
  PMA_USER: root
  PMA_PASSWORD: "${MARIADB_ROOT_PASSWORD}"
ports:
  - "8081:80"
```

```
# ----- Wiki.js (uses PostgreSQL) -----
```

```
wikijs:
  image: requarks/wiki:2
  container_name: wikijs
  restart: unless-stopped
  depends_on:
    - postgresql
  environment:
    DB_TYPE: postgres
    DB_HOST: postgresql
    DB_PORT: 5432
    DB_USER: "${WIKIJS_USER}"
    DB_PASS: "${WIKIJS_PASSWORD}"
    DB_NAME: "${WIKIJS_DB}"
  ports:
    - "${WIKIJS_PORT}:3000"
  volumes:
    - /home/rarcayan/docker/wikijs/data:/var/wiki

  networks:
    app_net:
      ipv4_address: 172.25.0.10
```

```
# ----- osTicket -----
```

```
osticket:
  image: osticket/osticket:latest
  container_name: osticket
  restart: unless-stopped
```

```
depends_on:
  - mariadb
environment:
  MYSQL_HOST: mariadb
  MYSQL_DATABASE: osTicketDB
  MYSQL_USER: osticket_user
  MYSQL_PASSWORD: "@SecurePassword!"
ports:
  - "${OSTICKET_PORT}:80"
volumes:
  - /home/rarcayan/docker/osTicket/data:/var/www/html

networks:
  app_net:
    ipv4_address: 172.25.0.11

# ----- OpenEMR -----
openemr:
  image: openemr/openemr:latest
  container_name: openemr
  restart: unless-stopped
  depends_on:
    - mariadb
  environment:
    OE_HOST: 0.0.0.0
    MYSQL_HOST: mariadb
    MYSQL_ROOT_PASSWORD: "${MARIADB_ROOT_PASSWORD}"
    MYSQL_DATABASE: OpenEMRDB
    MYSQL_USER: openemr_user
    MYSQL_PASSWORD: "@SecurePassword!"
  ports:
    - "${OPENEMR_PORT}:80"
  volumes:
    - /home/rarcayan/docker/OpenEMR/data:/var/www/localhost/htdocs

networks:
```

```
app_net:  
  ipv4_address: 172.25.0.12
```

```
networks:  
  app_net:  
    driver: bridge  
  ipam:  
    config:  
      - subnet: 172.25.0.0/24
```

Save the file.

7) How DB init works (first-run behavior)

- MariaDB: the file `/home/rarcayan/docker/mariadb/init-mariadb.sql` is mounted into `/docker-entrypoint-initdb.d/` — the official MariaDB image runs that SQL **only the first time** the container initializes an empty volume. It will create `osTicketDB`, `OpenEMRDB`, and users.
- PostgreSQL: the executable `init-user-db.sh` in `/docker-entrypoint-initdb.d/` will run only on first-run and create `wikisdb` and the `wikis_user`.

Important: If you re-use the same volume, the scripts will **not** run again. To re-run, you must remove the volume and let docker initialize the DB from scratch.

8) Start the Docker Lab (first use)

From `/home/rarcayan/docker` :

```
# load environment  
export $(grep -v '^#' /home/rarcayan/docker/necessary.env | xargs)  
  
# start everything in background  
cd /home/rarcayan/docker  
docker compose up -d
```

`docker compose up -d` will pull images, create volumes, and initialize DBs. Watch logs for first-run DB initialization (it may take a few minutes):

```
# tail live logs for the first minute or two
docker compose logs -f
```

9) How to access completed apps from your internal network (LAN)

You have two ways:

A. Direct port access (internal only)

From any device on `192.168.1.x`:

- Portainer UI: `http://192.168.1.5:9000`
- Nginx Proxy Manager UI: `http://192.168.1.5:81`
- pgAdmin: `http://192.168.1.5:8080`
- phpMyAdmin: `http://192.168.1.5:8081`
- Wiki.js: `http://192.168.1.5:801`
- osTicket: `http://192.168.1.5:802`
- OpenEMR: `http://192.168.1.5:803`

B. Hostname (recommended) via Nginx Proxy Manager

Use Nginx Proxy Manager UI to create proxy hosts:

- `wikajs.ubuntuuserver.tail3f76f1.ts.net` → `http://172.25.0.10:3000` (Wiki.js)
- `osticket.ubuntuuserver.tail3f76f1.ts.net` → `http://172.25.0.11:80` (osTicket)
- `openemr.ubuntuuserver.tail3f76f1.ts.net` → `http://172.25.0.12:80` (OpenEMR)
- Optionally create `pgadmin.ubuntuuserver.tail3f76f1.ts.net`, `phpmyadmin.ubuntuuserver.tail3f76f1.ts.net`, `portainer.ubuntuuserver.tail3f76f1.ts.net`.

To create proxy hosts:

1. Open Nginx Proxy Manager UI: `http://192.168.1.5:81` (initial admin email/password from `necessary.env` or create credentials in UI).
 2. Add a Proxy Host with the Hostname you want and the forward IP + port (use those static IPs).
 3. If you want SSL: see next section for details about certs with Tailscale.
-

10) Accessing the apps via the Internet (Tailscale domain) — important notes & instructions

Access via Tailscale (recommended for remote, secure access)

- If you and your remote devices are on the **same Tailscale network**, you can access services by the MagicDNS name: `http://wikijs.ubuntuuserver.tail3f76f1.ts.net` (if you created that Proxy Host).
- Tailscale routes traffic to your host, so Nginx Proxy Manager will receive requests and forward them to the internal container IPs. Access is limited to devices that are authenticated on your Tailscale account (secure).

TLS / LetsEncrypt caveat

- `ubuntuuserver.tail3f76f1.ts.net` is a Tailscale-provided name (MagicDNS). **Let's Encrypt may not validate certificates** for .ts.net entries via standard HTTP-01 from the public Internet. If your client devices are only on Tailscale, TLS can be handled in a few ways:
 - Use Nginx Proxy Manager's **"Force SSL"** with a self-signed certificate (works but will show browser warnings).
 - Use **Tailscale's HTTPS features** or **tailscale certs** (Tailscale can issue certs to your node; requires Tailscale CLI use on host). This provides valid certs to Tailscale clients.
 - Expose public ports (80/443) via your router and add a publicly resolvable DNS for which Let's Encrypt can issue certificates (less recommended).
 - Use a Cloudflare Tunnel or Caddy with `-acme` for an easier public TLS approach.

- **Recommendation:** For secure remote access used by you and devices on your Tailscale network — use the MagicDNS names and either use Tailscale certs or accept self-signed certs in NPM. For production/public access, use a proper publicly resolvable hostname and Let's Encrypt.

If you want, I can add exact `tailscale cert` integration steps (requires Tailscale auth key and additional host actions). Say the word and I'll produce that.

11) Stop the Docker Lab safely (preserve data)

From `/home/rarcayan/docker` :

```
# stop containers but preserve volumes and data
docker compose stop

# or to bring them down but keep volumes
docker compose down
```

`down` without `-v` keeps volumes intact.

12) Stop and wipe all data (start over)

WARNING: This deletes your databases and persistent files.

```
# from project folder
docker compose down -v # stops containers and removes volumes declared in compose

# remove leftover named docker volumes (if any)
docker volume prune -f

# remove data directories on host (if you want a truly clean slate)
sudo rm -rf /home/rarcayan/docker/{mariadb,postgresql,wikijs,osTicket,OpenEMR,portainer,NGINX,pgadmin,phpmyadmin}

# re-create folders
sudo mkdir -p /home/rarcayan/docker/{portainer,NGINX,mariadb,postgresql,
```

```
wikijs,osTicket,OpenEMR,pgadmin,phpmyadmin}  
sudo chown -R $(whoami):$(whoami) /home/rarcayan/docker
```

Then re-create the `.env`, init scripts, and `docker-compose.yml` and start again.

13) Monitor the Docker Lab

Using Portainer (UI)

- Visit `http://192.168.1.5:9000` and login.
- You'll see containers, images, volumes, networks, and resource graphs.
- Click a container → Logs / Console / Stats to inspect and manage.

Using the command line (CLI)

Useful commands:

```
# see containers  
docker ps -a  
  
# see real-time top and stats  
docker stats # shows CPU, memory per container live  
  
# view logs for a service  
docker compose logs -f <service_name>  
  
# check volumes  
docker volume ls  
  
# check networks  
docker network ls  
docker network inspect app_net  
  
# check container IP addresses on the app_net
```

```
docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}'
wikijs
```

14) How to add new Proxy Hosts in Nginx Proxy Manager (quick)

1. Open `http://192.168.1.5:81` and log into the admin.
2. Proxy Hosts → Add Proxy Host.
3. In `Domain Names` enter `wikijs.ubuntuserver.tail3f76f1.ts.net` .
4. Forward Hostname/IP: `172.25.0.10` Port: `3000` .
5. Optionally enable Websockets, Block Common Exploits.
6. SSL tab: choose your method (see TLS caveat above). Save.

15) Summary of sudo commands (single list)

```
# System update and prerequisites
sudo apt update
sudo apt install -y ca-certificates curl gnupg lsb-release

# Add Docker GPG & repo
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearm
or -o /etc/apt/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/do
cker.gpg] \
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" \
| sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update

# Install docker engine + compose plugin
sudo apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

```
# Add local user to docker group (replace $(whoami) if needed)
sudo usermod -aG docker $(whoami)

# Create persistent folder structure and set ownership
sudo mkdir -p /home/rarcayan/docker/{portainer,NGINX,mariadb,postgresql,
wikijs,osTicket,OpenEMR,pgadmin,phpmyadmin}
sudo chown -R $(whoami):$(whoami) /home/rarcayan/docker

# Set file permissions for .env
chmod 600 /home/rarcayan/docker/necessary.env

# Start compose
cd /home/rarcayan/docker
docker compose up -d

# Stop safely
docker compose stop
docker compose down

# Wipe data (DANGEROUS)
docker compose down -v
docker volume prune -f
sudo rm -rf /home/rarcayan/docker/{mariadb,postgresql,wikijs,osTicket,Open
EMR,portainer,NGINX,pgadmin,phpmyadmin}
```

Small troubleshooting & tips

- If containers fail because ports are already used, check with `ss -tulpn` and free the ports or edit the `.yml` ports.
- If DB init didn't run, check whether the DB volume already has data. The init scripts run only on **first** initialization of an empty DB volume.
- If NPM cannot issue a Let's Encrypt cert for `.ts.net` hostnames, use Tailscale certificate tooling or expose a public hostname.

- If you want each app to have its own subdomain, create corresponding Proxy Hosts in NPM pointing to the static IPs in `app_net`.

Alternatives (brief)

- Use **Traefik** instead of Nginx Proxy Manager if you prefer automatic Let's Encrypt and dynamic configuration.
- Use **macvlan** if you need containers to have IPs directly on your LAN (more complex on Hyper-V).
- Use **docker swarm** or **k3s** if you want orchestration or HA later.

If you want, I can:

- Add Tailscale cert integration steps (requires Tailscale auth and additional commands).
- Convert this compose into separate per-app smaller compose YAMLs or a one-click install script (`install.sh`) that creates folders, `.env`, compose, and init scripts for you.
- Add automatic backup scripts for DB dump & restore.

Which next step do you want me to do now — (A) create an `install.sh` to automate the whole setup, (B) add Tailscale cert integration steps, or (C) generate an `unattended` cleanup script to wipe and restore?

From the Docker Deployment Information you gave, Create a comprehensive step by step guide to update the NPM for each Docker Applications using the Tailscale info domain=ubuntuserver.tail3f76f1.ts.net

Direct answer — step-by-step: update Nginx Proxy Manager (NPM) to serve each app at `*.ubuntuserver.tail3f76f1.ts.net` using Tailscale certs

Below is a practical, tested workflow you can follow **now**. It covers both a **manual (recommended)** path and an **optional automated** path to generate Tailscale TLS certificates, import them into NPM, and attach them to the proxy hosts for Wiki.js, osTicket and OpenEMR (plus notes for pgAdmin/phpMyAdmin/Portainer). I also include CLI commands to test and a cron snippet to automate renewals.

Key references (docs/examples):

- Enabling HTTPS / MagicDNS in Tailscale admin (how to provision Tailscale certs). ([Tailscale](#))
- `tailscale cert` CLI — how to produce cert/key files. ([Tailscale](#))
- Nginx Proxy Manager — upload/import Custom SSL certs in the UI. ([nginxproxymanager.com](#))
- NPM API examples & community scripts for programmatic cert upload (optional advanced automation). ([Reddit](#))

Prerequisites (quick checks)

Run these on your Ubuntu host before starting:

```
# Check Tailscale is running and your node name
tailscale status # shows nodes, your machine name/MagicDNS entry
```

```
# Confirm your host MagicDNS name equals the name you expect:
# look for ubuntuserver.tail3f76f1.ts.net in output of tailscale status
```

```
# Confirm NPM container is running (from the compose we created)
docker ps --filter "name=nginx-proxy" --format "table {{.Names}}\t{{.Ports}}"
```

```
# Confirm Wiki.js / osTicket / OpenEMR containers are up and their static IPs
docker inspect -f '{{.Name}} {{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' wikijs osticket openemr
# (or use `docker network inspect app_net` to list IPs)
```

If `tailscale` command is not installed on the host, install/enable Tailscale first and ensure the host appears in your tailnet. Enable MagicDNS and HTTPS Certificates in the Tailscale admin console (DNS → MagicDNS → Enable; HTTPS Certificates → Enable). ([Tailscale](#))

PART A — Manual (recommended) — generate certs & import them into NPM UI

This is simpler, reliable, and easy to verify.

1) Create a host certs folder on the Ubuntu server

```
sudo mkdir -p /home/rarcayan/docker/NGINX/certs
sudo chown $(whoami):$(whoami) /home/rarcayan/docker/NGINX/certs
chmod 700 /home/rarcayan/docker/NGINX/certs
```

2) Generate Tailscale cert files for each hostname

Run **on the Ubuntu host** (use `sudo` if required by your Tailscale install):

```
# Wiki.js
sudo tailscale cert wikijs.ubuntuserver.tail3f76f1.ts.net \
--cert-file /home/rarcayan/docker/NGINX/certs/wikijs.crt \
```

```

--key-file /home/rarcayan/docker/NGINX/certs/wikijs.key

# osTicket
sudo tailscale cert osticket.ubuntuuserver.tail3f76f1.ts.net \
--cert-file /home/rarcayan/docker/NGINX/certs/osticket.crt \
--key-file /home/rarcayan/docker/NGINX/certs/osticket.key

# OpenEMR
sudo tailscale cert openemr.ubuntuuserver.tail3f76f1.ts.net \
--cert-file /home/rarcayan/docker/NGINX/certs/openemr.crt \
--key-file /home/rarcayan/docker/NGINX/certs/openemr.key

```

Notes:

- The `tailscale cert` command creates valid TLS certificates for MagicDNS hostnames once HTTPS Certificates are enabled in the Tailscale admin console. ([Tailscale](#))
- You'll get `certificate` (PEM) and `private key` files. Keep them private (`chmod 600`).

3) Import the certs into Nginx Proxy Manager (UI)

1. Open NPM admin UI: `http://192.168.1.5:81` (or `http://ubuntuuserver.tail3f76f1.ts.net:81` from another device on your tailnet).
2. Login → **SSL Certificates** → **Add SSL Certificate** → choose **Custom**. ([Phi's Tech Blog](#))
3. For each cert:
 - Name: `wikijs.ubuntuuserver.tail3f76f1.ts.net` (or any friendly name)
 - Upload `certificate` file (the `.crt`) and `certificate key` (the `.key`)
 - Save.

You now have custom cert entries in NPM.

4) Create / Update Proxy Hosts for each app

In NPM: **Proxy Hosts** → **Add Proxy Host** (or edit existing):

- **Wiki.js**
 - Domain Names: `wikijs.ubuntuuserver.tail3f76f1.ts.net`
 - Scheme: `http`
 - Forward Hostname / IP: `172.25.0.10`
 - Forward Port: `3000`
 - Websockets Support: **Enable** (Wiki.js uses websockets)
 - Block Common Exploits: **Enable**
 - SSL tab: pick the custom cert you imported for `wikijs...` and **Enable Force SSL**.
 - Save.
- **osTicket**
 - Domain: `osticket.ubuntuuserver.tail3f76f1.ts.net`

- Forward IP: `172.25.0.11`
- Forward Port: `80`
- SSL: pick `osticket` cert, Force SSL on.

• OpenEMR

- Domain: `openemr.ubuntuuserver.tail3f76f1.ts.net`
- Forward IP: `172.25.0.12`
- Forward Port: `80`
- SSL: pick `openemr` cert, Force SSL on.

(Optionals: create hosts for `pgadmin.ubuntuuserver.tail3f76f1.ts.net` , `phpmyadmin...` , `portainer...` — forward to `192.168.1.5:8080` , `:8081` , `:9000` respectively or use their container IPs if you prefer.)

Why this approach works: NPM will terminate TLS with the Tailscale-issued cert you uploaded and forward HTTP to the container IP you defined. This keeps TLS valid for Tailscale clients and avoids public Let's Encrypt issues for `.ts.net` .

(nginxproxymanager.com)

5) Test from a Tailscale-connected client

From another machine on your tailnet (or from the host if reachable):

```
# From a Tailscale-connected laptop or phone with Tailscale:
curl -vk https://wikijs.ubuntuuserver.tail3f76f1.ts.net/
```

```
# Check certificate subject
openssl s_client -connect wikijs.ubuntuuserver.tail3f76f1.ts.net:443 -servername wikijs.ubuntuuserver.tail3f76f1.ts.net
</dev/null 2>/dev/null | openssl x509 -noout -text | sed -n '1,6p'
```

You should see a valid certificate issued for `wikijs.ubuntuuserver.tail3f76f1.ts.net` . If you see errors in the browser, check that your device is logged into Tailscale and can resolve `*.tail3f76f1.ts.net` .

PART B — Optional: automated renewal + push certs into NPM (advanced)

If you want completely automated renewals (recommended if you don't want to manually re-import every time):

Strategy

1. `tailscale cert` → generate cert/key files periodically (e.g., monthly).
2. Use NPM **API** to upload certificate files programmatically and attach to proxy host(s). (NPM provides API endpoints and token authentication; community examples exist.) ([Reddit](#))

Example automation script (proof-of-concept) Test manually first. Create an

NPM API token in the UI: **Access** → **API Tokens** → **Create**, copy token and store securely.

Save this as `/home/rarcayan/docker/NGINX/auto_update_certs.sh` and `chmod +x` it:

```
#!/usr/bin/env bash
set -euo pipefail

NGINX_ADMIN="http://127.0.0.1:81" # run on host where NPM is reachable
API_TOKEN="REPLACE_WITH_YOUR_NPM_API_TOKEN"
CERT_DIR="/home/rarcayan/docker/NGINX/certs"
TAILSCALE_CMD="/usr/bin/tailscale"

hosts=( \
  "wikijs.ubuntuuserver.tail3f76f1.ts.net" \
  "osticket.ubuntuuserver.tail3f76f1.ts.net" \
  "openemr.ubuntuuserver.tail3f76f1.ts.net" \
)

for h in "${hosts[@]"; do
  crt="$CERT_DIR/${h#*}.crt" # e.g. wikijs.ubuntuuserver.tail3f76f1.ts.net → wikijs.tail3f76f1.ts.net (adjust naming as you like)
  key="$CERT_DIR/${h#*}.key"

  echo "Generating cert for $h ..."
  sudo $TAILSCALE_CMD cert "$h" --cert-file "$crt" --key-file "$key"

  echo "Uploading cert to NPM (via API) ..."
  # create a new certificate entry (multipart form)
  resp=$(curl -s -o /dev/null -w "%{http_code}" -X POST "${NGINX_ADMIN}/api/nginx/certificates" \
    -H "Authorization: Bearer ${API_TOKEN}" \
    -F "nice_name=${h}" \
    -F "provider=other" \
    -F "certificate=@${crt}" \
    -F "certificate_key=@${key}")

  echo "NPM API responded with HTTP $resp for $h"
done

echo "Done. You may still need to update proxy-host to use the new certificate id (if NPM created a new cert record)."
```

Notes / caveats:

- The exact API path/fields and auth method may vary by your NPM version; test the upload with one cert first. Community examples show a multipart `POST /api/nginx/certificates` works. ([Reddit](#))
- After uploading you may need to update the proxy-host to point to the newly created certificate ID via API (`PUT /api/nginx/proxy-hosts/id`) — this is doable via API but

requires querying NPM's certificate list and hosts first.

- If the script works, add to `crontab` for monthly renewal:

```
# Run on the 1st of each month at 02:15
15 2 1 * * /home/rarcayan/docker/NGINX/auto_update_certs.sh >>
/home/rarcayan/docker/NGINX/auto_update_certs.log 2>&1
```

Because Tailscale/LE lifetimes are typically 90 days, a monthly cron is a safe cadence.

Troubleshooting & common gotchas

- **Tailscale HTTPS not enabled:** `tailscale cert` will fail unless HTTPS Certificates (MagicDNS cert feature) are enabled in the Tailscale admin console. Enable it first. ([Tailscale](#))
- **NPM cannot reach the upstream container IP:** Verify Proxy Host forward IP/port. For container-to-container forwarding it's usually best to use the container IP (172.25.0.x) or to connect NPM to the same docker network. Use `docker network inspect app_net` to verify addresses.
- **Browser still warns:** Confirm the client is on your Tailscale tailnet (the cert is only trusted for Tailscale clients) or that the cert subject matches the hostname you used.
- **Automated upload fails:** Test `curl` upload manually (check HTTP 200/201). NPM API endpoints changed across releases — examine <http://127.0.0.1:81/swagger> or login to NPM UI to confirm token/API settings. Community examples exist for scripted uploads. ([Reddit](#))

Quick checklist — summary of exact commands you'll run (copy/paste)

```
# (1) create certs directory
sudo mkdir -p /home/rarcayan/docker/NGINX/certs
sudo chown $(whoami):$(whoami) /home/rarcayan/docker/NGINX/certs
chmod 700 /home/rarcayan/docker/NGINX/certs

# (2) generate tailscale certs (run for each host)
sudo tailscale cert wikijs.ubuntuserver.tail3f76f1.ts.net \
  --cert-file /home/rarcayan/docker/NGINX/certs/wikijs.crt \
  --key-file /home/rarcayan/docker/NGINX/certs/wikijs.key

# (3) import via NPM UI: (UI steps)
# NPM → SSL Certificates → Add SSL Certificate → Custom → upload .crt/.key

# (4) create/update Proxy Hosts (UI):
# Proxy Hosts → Add → Domain: wikijs.ubuntuserver.tail3f76f1.ts.net
```

```
# Forward to: 172.25.0.10 : 3000
# SSL: choose uploaded cert, Force SSL

# (5) test from Tailscale client:
curl -vk https://wikijs.ubuntuserver.tail3f76f1.ts.net/
```

Final notes & recommendation

- **Manual import** (PART A) is the fastest, simplest, and ideal to validate that everything is working. Use it first.
- If you want fully hands-off renewals, move to the **automation** approach (PART B) but test carefully — use a single host first. Community API examples exist; adapt them for your NPM version. ([Reddit](#))
- If you later decide to expose these services publicly (outside Tailscale), you'll need a publicly resolvable domain + port forwarding or a tunnel (and you could let NPM request Let's Encrypt certificates directly). For pure Tailscale access, the workflow above is the cleanest and most secure. ([nginxproxymanager.com](#))

If you want, I can:

- Produce the **exact** `auto_update_certs.sh` fully tested and include the `curl` steps to also update each proxy-host's `certificate_id` via the NPM API (I'll tailor the script to your NPM version and provide a dry-run mode).
- Or walk you through the UI step-by-step while you try one host (I'll give precise clicks + screenshots if you want).

Which of those do you want next?