Docker

- [Reverse Proxy](#)

Reverse Proxy

The new reverse proxy is located on the docker1 VM and consists of the following containers:

- nginx1 (Normal proxy)
- nginx2 (Secure proxy for proxying sites that need to be protected by SSO)
- oauth2-proxy (Handler proxy for authenticating users, used with nginx2)
- certbot (generates certificates)

The config can be found at /docker/reverse, and the nginx configs in nginx1/conf.d and nginx2/conf.d respectively. The oauth2-proxy.cfg should never need to be changed.

Generating a certificate:

1. Add a CNAME record for the site, it should point to proxy.tranquilit.cloud.
2. Do not add the site into the nginx config yet, if it has certificate definitions and cannot see them, the server will fail to start and will then cause the Let's Encrypt challenge to fail (needs to have HTTP running). The default nginx.conf handles the acme challenge so you won't need to add anything
3. In /docker/reverse, run create_cert.sh as sudo; it will ask you what domains you want to generate for. This is ONLY for new configs, by regenerating a certificate for a site that already exists, you will end up with the cert in a folder like {$domain}-0001 which may invalidate your nginx config.
4. Once the script has completed successfully (check the output!), it should provide you with the lines to add into the config. Make sure that the folder is correct vs the LE output further up in the script.
5. Add your nginx config with the ssl_certifcate lines, run `docker container restart nginx_proxy1` and you should be good to go.