Seafile + Nginx + SSL

Nginx

```
# vi /etc/nginx/sites-available/seafile

server {
    listen 80;
    server_name seafile.tst-amo.net.ua;
    server_tokens off;
    location /seafile {
       rewrite ^ https://$http_host$request_uri? permanent; #
force redirect http to https
    }
}

server {
    listen 443 ssl http2;
    server_name seafile.tst-amo.net.ua;
    server_tokens off;

    root /home/www/seafile;

# Let'sCript
include acme.conf;
include /etc/nginx/conf.d/hsts.conf;
include /etc/nginx/conf.d/ssl.conf;

     location / {
         proxy_pass http://127.0.0.1:8999;
         proxy_set_header Host $host;
         proxy_connect_timeout 36000s;
         proxy_read_timeout 36000s;
         proxy_send_timeout 36000s;
         send_timeout 36000s;

          # used for view/edit office file via Office Online
Server
         client_max_body_size 0;
```

```
        access_log /var/log/nginx/seahub.access.log;
        error_log /var/log/nginx/seahub.error.log;
      }

    location /seafhttp {
        rewrite ^/seafhttp(.*)$ $1 break;
        proxy_pass http://127.0.0.1:8082;
        client_max_body_size 0;
        proxy_connect_timeout 36000s;
        proxy_read_timeout 36000s;
        proxy_send_timeout 36000s;
        send_timeout 36000s;
        proxy_request_buffering off;
        proxy_http_version 1.1;
     }

    location /seafmedia {
        rewrite ^/seafmedia(.*)$ /media$1 break;
        root /home/www/seafile/seafile-server-latest/seahub;
     }

    location /seafdav {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
                    proxy_set_header  X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Host $server_name;
        proxy_set_header X-Forwarded-Proto https;
        proxy_http_version 1.1;
        proxy_connect_timeout 36000s;
        proxy_read_timeout 36000s;
        proxy_send_timeout 36000s;
        send_timeout 36000s;

        # This option is only available for Nginx >= 1.8.0.
        client_max_body_size 0;
        proxy_request_buffering off;

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

```
        }
}
```

```
# ln -s /etc/nginx/sites-available/seafile /etc/nginx/sites-enabled
# nginx -t
# nginx -s reload
```

Letsencrypt

Добавляем сертификат для субдомена, проверяем:

```
# certbot certonly --dry-run -d tst-amo.net.ua -d www.tst-amo.net.ua -d mail.tst-amo.net.ua -d cloud.tst-amo.net.ua -d seafile.tst-amo.net.ua
```

Если все нормально выполняем без –dry-run:

```
# certbot certonly -d tst-amo.net.ua -d www.tst-amo.net.ua -d mail.tst-amo.net.ua -d cloud.tst-amo.net.ua -d seafile.tst-amo.net.ua
```

Seafile

Внесем правки в наши конфиги. У меня владелец nginx:www-data, поэтому гружусь под ним (предварительно поправив vipw)

```
# su nginx
$ vi /home/www/seafile/conf/ccnet.conf
[General]
#SERVICE_URL = http://192.168.1.41/
SERVICE_URL = https://seafile.tst-amo.net.ua/
```

```
$ vi /home/www/seafile/conf/gunicorn.conf.py
...
# default localhost:8000
bind = "127.0.0.1:8999"
```

```
$ vi /home/www/seafile/conf/seahub_settings.py
FILE_SERVER_ROOT = 'https://seafile.tst-amo.net.ua/seafhttp'
```

```
$ cd /home/www/seafile/seafile-server-latest
```

```
$ ./seafile.sh restart
```

```
$ ./seahub.sh restart 8999
```

Возможно понадобится очистить /tmp/seahub_cache.

Проверяем:

https://seafile.tst-amo.net.ua