### Настройка генерации сертификата (<https://certbot.eff.org/#ubuntuxenial-nginx>)

Устанавливаем certbot

$ sudo add-apt-repository ppa:certbot/certbot

$ sudo apt-get update

$ sudo apt-get install certbot

Для выпуска сертификатов используем ["webroot" plugin](https://certbot.eff.org/docs/using.html#webroot), который может работать с webroot директорией любого веб-сервера:

$ certbot certonly --webroot -w /var/www/example -d example.com -d www.example.com -w /var/www/thing -d thing.is -d m.thing.is

Эта команда выпустит единый сертификат для **example.com**, **www.example.com**, **thing.is**, и **m.thing.is**, находящийся в **/var/www/example** для первых двух доменов и в **/var/www/thing** для второй пары. Для проверки права владения доменом, на который выпускается сертификат необходимо указать корень сайта, к которому будет полный доступ. Чтобы не засорять корень сайта лишними каталогами говорим nginx, чтобы при обращении по соответствующему адресу обращался в отдельную директорию

location ~/.well-known {

root /home/user/web/sitename.ru;

}

Certbot устанавливается вместе с заданием cron, которое будет автоматически продлять сертификаты до того, как они просрочатся. Пока Let's Encrypt выдает сертификаты на 90 дней. Протестировать автоматическое обновление сертификатов можно командой:

certbot renew --dry-run

Готовые сертификаты находятся в папке /etc/letsencrypt/live/имя\_сайта/

### Настройка nginx на работу по https (<https://www.alexeykopytko.com/2017/free-ssl-from-letsencrypt/>, <https://habrahabr.ru/post/252821/>, <https://gist.github.com/plentz/6737338>)

Редактируем настройки nginx:

sudo nano /etc/nginx/sites-available/default

добавляя строки

server {

listen 80;

listen [::]:80;

listen 443 ssl spdy;

ssl\_certificate /etc/letsencrypt/live/bot.online-gymnasium.ru/fullchain.pem;

ssl\_certificate\_key /etc/letsencrypt/live/bot.online-gymnasium.ru/privkey.pem;

ssl\_trusted\_certificate /etc/letsencrypt/live/bot.online-gymnasium.ru/chain.pem;

ssl\_session\_timeout 10m;

ssl\_session\_cache shared:SSL:5m;

ssl\_dhparam /var/ssl/dhparam.pem;

ssl\_prefer\_server\_ciphers on;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers "ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-SHA:DES-CBC3-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4";

resolver 77.88.8.8;

ssl\_stapling on;

add\_header Strict-Transport-Security "max-age=31536000; includeSubdomains;";

root /var/www/bot;

index index.html index.htm index.php;

server\_name BOT.ONLINE-GYMNASIUM.RU;

…

Проверка качества, например, в <https://www.ssllabs.com/ssltest/index.html> должна показывать A+

Лучше, чтобы стоял локальный кеширующий DNS-сервер. Чтобы использовать его необходимо поменять

resolver 127.0.0.1;

и установить, например, dnsmasq:

sudo apt-get install dnsmasq

запрещаем ему отвечать посторонним

sudo tee /etc/dnsmasq.d/localhost <<EOF

listen-address=127.0.0.1

bind-interfaces

EOF

Проверяем конфиг и перезапускаем

dnsmasq --test

service dnsmasq restart