

```
1  ssl on;
2  ssl_certificate /etc/letsencrypt/live/nc.c-rieger.de/fullchain.pem;
3  ssl_certificate_key /etc/letsencrypt/live/nc.c-rieger.de/privkey.pem;
4  ssl_trusted_certificate /etc/letsencrypt/live/nc.c-rieger.de/fullchain.pem;
5  ssl_dhparam /etc/ssl/certs/dhparam.pem;
6  ssl_protocols TLSv1.2;
7  ssl_ciphers
   'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384
   :ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kED
   H+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
   ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SH
   A:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA25
   6:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!D
   ES:!RC4:!3DES:!MD5:!PSK:!AES128';
8  ssl_ecdh_curve secp384r1;
9  ssl_prefer_server_ciphers on;
10 ssl_stapling on;
11 ssl_stapling_verify on;
12 ssl_session_timeout 24h;
13 ssl_session_cache shared:SSL:50m;
14 ssl_session_tickets off;
15 resolver 192.168.2.1;
16 resolver_timeout 10s;
17 add_header Strict-Transport-Security "max-age=15768000; includeSubDomains" always;
18 add_header X-Content-Type-Options "nosniff" always;
19 add_header Referrer-Policy "same-origin" always;
20 add_header X-Frame-Options "SAMEORIGIN" always;
21 add_header X-Xss-Protection "1; mode=block" always;
22 add_header X-Robots-Tag none;
23 add_header X-Download-Options noopen;
24 add_header X-Permitted-Cross-Domain-Policies none;
25
```