ssl\_protocols TLSv1.2;

ssl\_prefer\_server\_ciphers on;

ssl\_dhparam /etc/nginx/certs/dhparam.pem;

ssl\_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;

ssl\_ecdh\_curve secp384r1; # Requires nginx >= 1.1.0

ssl\_session\_timeout 10m;

ssl\_session\_cache shared:SSL:10m;

ssl\_session\_tickets off; # Requires nginx >= 1.5.9

# ssl\_stapling on; # Requires nginx >= 1.3.7

# ssl\_stapling\_verify on; # Requires nginx => 1.3.7

resolver 8.8.8.8 8.8.4.4 valid=300s;

resolver\_timeout 5s;

add\_header X-Frame-Options DENY;

add\_header X-Content-Type-Options nosniff;

add\_header X-XSS-Protection "1; mode=block";