user www-data;

worker\_processes 4;

pid /run/nginx.pid;

daemon off;

events {

worker\_connections 2048;

multi\_accept on;

use epoll;

}

http {

server\_tokens off;

sendfile on;

tcp\_nopush on;

tcp\_nodelay on;

keepalive\_timeout 15;

types\_hash\_max\_size 2048;

client\_max\_body\_size 20M;

include /etc/nginx/mime.types;

default\_type application/octet-stream;

access\_log /dev/stdout;

error\_log /dev/stderr;

gzip on;

gzip\_disable "msie6";

# ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_protocols TLSv1.2;

ssl\_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS';

ssl\_prefer\_server\_ciphers on;

# HSTS (ngx\_http\_headers\_module is required) (15768000 seconds = 6 months)

add\_header Strict-Transport-Security max-age=15768000;

# OCSP Stapling ---

# fetch OCSP records from URL in ssl\_certificate and cache them

ssl\_stapling on;

ssl\_stapling\_verify on;

include /etc/nginx/conf.d/\*.conf;

include /etc/nginx/sites-available/\*.conf;

open\_file\_cache off; # Disabled for issue 619

charset UTF-8;

}