



链滴

Nginx 反向配置,SSL 证书配置

作者: [monwon](#)

原文链接: <https://ld246.com/article/1572769529632>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)



Nginx 安装、配置

安装

CentOS 6/7安装Nginx

添加镜像源

```
sudo rpm -Uvh http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.e7.ngx.noarch.rpm
```

通过 `yum search nginx` 看看是否已经添加源成功。如果成功则执行下列命令安装Nginx

```
sudo yum install -y nginx
```

Ubuntu 16/18 安装Nginx

```
sudo apt-get install nginx
```

浏览器输入 `http://IP` 如果出现 `Welcome to nginx !` 字样表示安装成功。

默认安装位置: `/usr/local/nginx`

```
root@instance-89i1mzb4:/usr/local/nginx# pwd
/usr/local/nginx
root@instance-89i1mzb4:/usr/local/nginx# ll
total 48
drwxr-xr-x 12 root  root 4096 Oct 31 18:58 ./
drwxr-xr-x 14 root  root 4096 Jul 13 23:34 ../
drwxr-xr-x  2 root  root 4096 Jul 13 23:34 conf/
drwxr-xr-x  2 root  root 4096 Nov  1 23:14 conf.d/
drwxr-xr-x  2 root  root 4096 Oct 31 18:59 crt/
drwx----- 2 nobody root 4096 Jul 13 23:34 fastcgi_temp/
drwxr-xr-x  2 root  root 4096 Jul 13 23:34 html/
drwxr-xr-x  2 root  root 4096 Nov  2 00:00 logs/
drwx----- 4 nobody root 4096 Nov  1 23:07 proxy_temp/
drwxr-xr-x  2 root  root 4096 Jul 13 23:34 sbin/
drwx----- 2 nobody root 4096 Jul 13 23:34 scgi_temp/
drwx----- 2 nobody root 4096 Jul 13 23:34 uwsgi_temp/
root@instance-89i1mzb4:/usr/local/nginx#
```

Nginx目录下文件夹含义：

conf: nginx所有配置文件

conf.d: 默认的主配置文件

sbin: 存放主程序

html: 默认的静态页面

logs: 日志

scgi_temp: 临时目录

uwsgi_temp: 临时目录

Nginx重启、停止、启动

#重启

```
service nginx restart
```

#停止

```
/usr/local/nginx/sbin/nginx -s stop
```

```
service nginx stop
```

#启动

```
/usr/local/nginx/sbin/nginx
```

```
service nginx start
```

#重新加载配置文件

```
/usr/local/nginx/sbin/nginx -c /usr/local/nginx/conf/nginx.conf
```

Nginx配置Http

编辑conf/nginx.con http下添加 **include /usr/local/nginx/conf.d/*.conf;**

```
vim /usr/local/nginx/conf/nginx.conf
```

```

error_log logs/error.log error;
pid logs/nginx.pid;
user www;
worker_processes auto;
worker_rlimit_nofile 51200;

events {
    use epoll;
    worker_connections 51200;
}

http {
    client_body_buffer_size 32k;
    client_header_buffer_size 2k;
    client_max_body_size 2m;
    default_type application/octet-stream;
    log_not_found off;
    server_tokens off;
    include mime.types;
    gzip on;
    gzip_min_length 1k;
    gzip_buffers 4 16k;
    gzip_http_version 1.0;
    gzip_comp_level 2;
    gzip_types text/plain text/css text/xml text/javascript application/x-javascript application/xml application/rss+xml application/xhtml+xml application/atom+xml;
    gzip_vary on;
    #error_page 500 502 503 504 /50x.html;
    log_format access '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" $http_x_forwarded_for';
    include /ewomail/nginx/conf.d/*.conf;
}

```

接着到 `conf.d` 下,新建任意以`.conf`结尾的文件

```

cd /usr/local/nginx/conf.d/
touch tomcat.conf
vim tomcat.conf

```

如果`cd`到 `conf.d`目录下提示`-bash: cd: /usr/local/nginx/conf.d/: No such file or directory`, 需要建`conf.d`文件夹,再进到 `conf.d`下。

```
mdkir -p /usr/local/nginx/conf.d/
```

接下来配置http协议 80端口

eg: 博客地址: <http://127.0.0.1/blogs/>

使用Nginx反向代理8080端口 blogs项目

```

upstream blogs{
    ip_hash; #session共享
    server 127.0.0.1:8080 max_fails=3 fail_timeout=600s;
}
server {
    listen 80 backlog=65535;
    server_tokens off;
    server_name 127.0.0.1;
    #access_log /gs/nginx-logs/teach.access.log;
    #proxy_set_header Host $host:$server_port;
    proxy_set_header Host $host;
    # 获取真实IP
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header REMOTE-HOST $remote_addr;
    # 获取代理者的真实ip
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_http_version 1.1;
    #proxy_set_header Connection "";
    proxy_buffering off;
    proxy_redirect off;
    location / {
        #这两个方法都可, 转发地址栏显示http://127.0.0.1, 重定向显示http://127.0.0.1/blogs
    }
}

```

```
#    rewrite "/" http://127.0.0.1/blogs; #重定向
proxy_pass http://mblogs; #转发
}
location /blogs {
proxy_next_upstream http 502 http 504 error timeout invalid_header;
set $origin '*';#写入需要跨域的请求地址
if ($request_method = 'OPTIONS') {
add_header 'Access-Control-Allow-Origin' $origin;
add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
add_header 'Access-Control-Max-Age' 17280000;
#add_header 'Content-Type' 'multipart/form-data';
#add_header 'Content-Type' 'text/plain charset=UTF-8';
add_header 'Content-Length' 0;
return 204;
}
if ($request_method = 'POST') {
add_header 'Access-Control-Allow-Origin' $origin;
#add_header 'Content-Type' 'multipart/form-data';
add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
add_header 'Access-Control-Allow-Headers' 'DNT,X-CustomHeader,Keep-Alive,User-Agent,X
Requested-With,If-Modified-Since,Cache-Control,Content-Type';
}
if ($request_method = 'GET') {
add_header 'Access-Control-Allow-Origin' $origin;
add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
add_header 'Access-Control-Allow-Headers' 'DNT,X-CustomHeader,Keep-Alive,User-Agent,X
Requested-With,If-Modified-Since,Cache-Control,Content-Type';
}
proxy_pass http://blogs;
}
}
```

Http协议访问

<http://127.0.0.1>

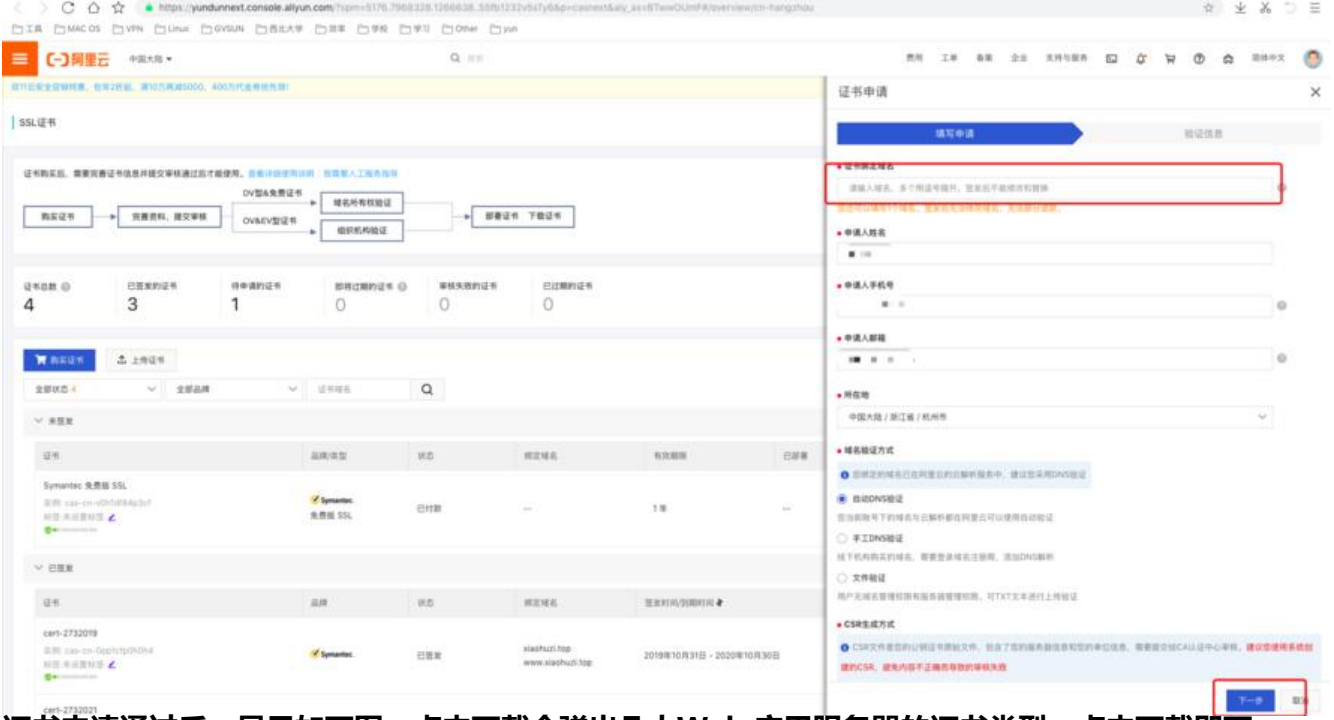
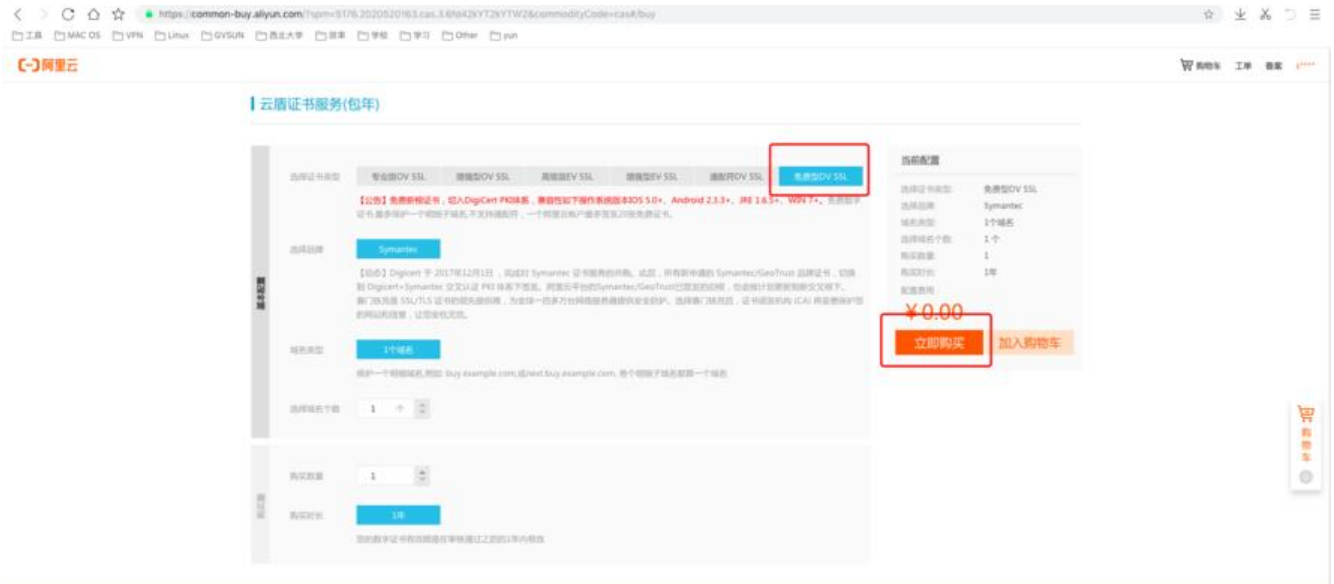
至此，http协议的反向代理就配置完成，下面是配置https协议。

申请ssl证书(阿里云为例)

[阿里云传送带](#)

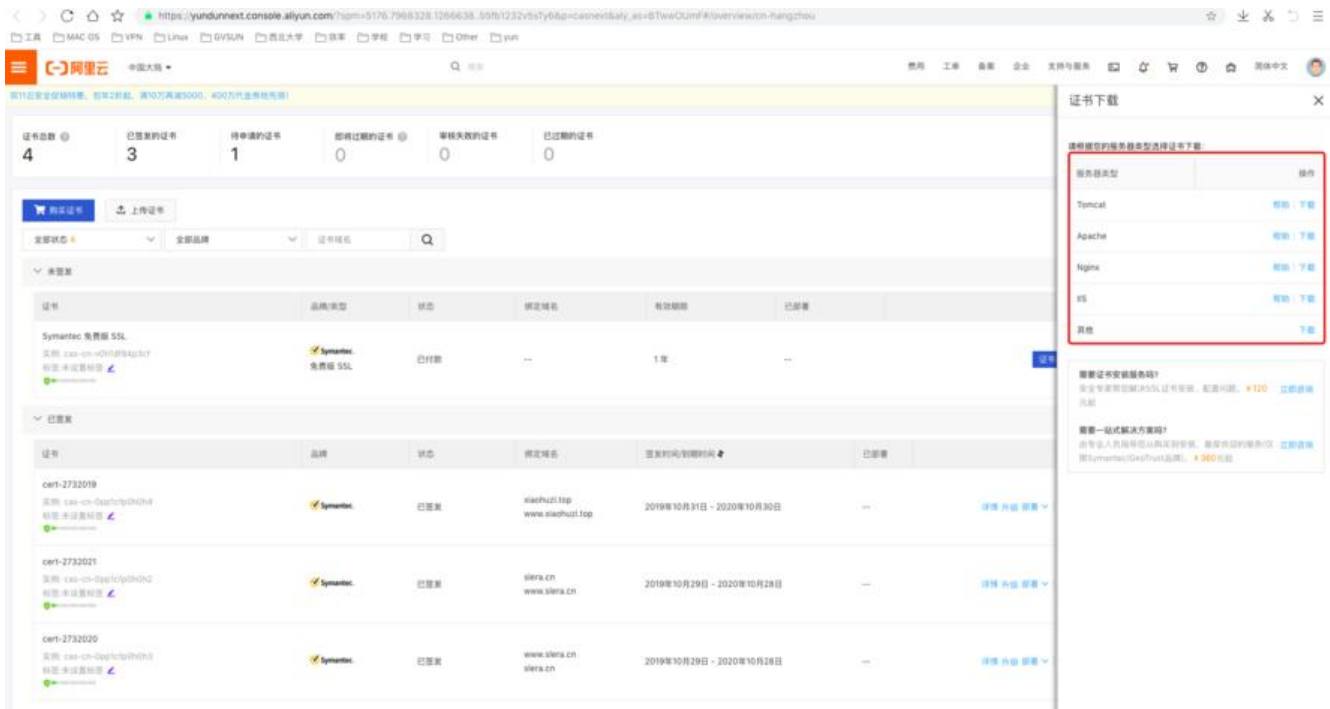
[腾讯云传送带](#)

购买后在阿里云SSL证书管理控制台可以看到一个证书，未签发状态需要点击证书申请,填写绑定的域和个人信息后，点击下一步等待申请，差不多不到一天就可以通过。



证书申请通过后，显示如下图；点击下载会弹出几大Web 应用服务器的证书类型；点击下载即可，情





配置SSL

准备工作

将下载的SSL证书上传到服务器上面到nginx的根目录/usr/local/nginx/下

```
cd /usr/local/nginx/
#创建crt文件夹
mkdir crt
#剪切到crt目录下
mv 3006543_sll.cn_tomcat.zip crt/

# 安装unzip gzip 如果已安装, 跳过这一步
yum install unzip gzip #Centos安装
apt-get yum install unzip gzip #Ubuntu 安装

#解压
unzip 3006543_sll.cn_tomcat.zip
```

解压完成后可以看到.pem和.key结尾的文件

.pem是SSL的证书

.key是SSL的密钥

Nginx配置Https

进入到conf.d目录下

```
cd /usr/local/nginx/conf.d
#编辑配置文件tomcat.conf
vim tomcat.conf
```

完整文件如下:

注意修改 `ssl_certificate`和`ssl_certificate_key`证书的路径和证书名字, 127.0.0.1 改为你的域名

```
upstream blogs{
    ip_hash;
    server 127.0.0.1:8080 max_fails=3 fail_timeout=600s;
}
server {
    listen 80 backlog=65535;
    server_tokens off;
    server_name 127.0.0.1;
    #access_log /gs/nginx-logs/teach.access.log;
    #proxy_set_header Host $host:$server_port;
    proxy_set_header Host $host;
    # 获取真实IP
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header REMOTE-HOST $remote_addr;
    # 获取代理者的真实ip
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_http_version 1.1;
    #proxy_set_header Connection "";
    proxy_buffering off;
    proxy_redirect off;
    location / {
        rewrite "/" https://127.0.0.1;
    }
}

server {
    listen 443;
    #ssl on;
    server_tokens off;
    server_name 127.0.0.1;
    #access_log /gs/nginx-logs/teach.access.log;
    #proxy_set_header Host $host:$server_port;
    proxy_set_header Host $host;
    # 获取真实IP
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header REMOTE-HOST $remote_addr;
    # 获取代理者的真实ip
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_http_version 1.1;
    #proxy_set_header Connection "";
    proxy_buffering off;
    # proxy_redirect off;
    ssl_certificate /usr/local/nginx/crt/a.pem;#证书文件名称
    ssl_certificate_key /usr/local/nginx/crt/a.key;#私钥文件名称
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #请按照这个协议配置
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;#请按照这
    套件配置
    ssl_prefer_server_ciphers on;
    location / {
        proxy_pass http://blogs;
    }
}
```



```

}
location /blogs {
    proxy_next_upstream http_502 http_504 error timeout invalid_header;
    set $origin '*';#写入需要跨域的请求地址
    if ($request_method = 'OPTIONS') {
        add_header 'Access-Control-Allow-Origin' $origin;
        add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
        add_header 'Access-Control-Max-Age' 17280000;
        #add_header 'Content-Type' 'multipart/form-data';
        #add_header 'Content-Type' 'text/plain charset=UTF-8';
        add_header 'Content-Length' 0;
        return 204;
    }
    if ($request_method = 'POST') {
        add_header 'Access-Control-Allow-Origin' $origin;
        #add_header 'Content-Type' 'multipart/form-data';
        add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
        add_header 'Access-Control-Allow-Headers' 'DNT,X-CustomHeader,Keep-Alive,User
Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type';
    }
    if ($request_method = 'GET') {
        add_header 'Access-Control-Allow-Origin' $origin;
        add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
        add_header 'Access-Control-Allow-Headers' 'DNT,X-CustomHeader,Keep-Alive,User
Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type';
    }
    proxy_pass http://blogs;
}
}

```

配置完成后重启Nginx

#重启

/usr/local/nginx/sbin/nginx -s stop

/usr/local/nginx/sbin/nginx

#或者

service nginx restart

服务器需要关闭防火墙，云服务器需要在控制台开放 80，443端口

Https访问

<https://127.0.0.1>