nginx ssl 自签名证书配置

生成证书

登录主机

cd /data01/nginx/nginx/conf
mkdir cert
cd cert

创建私钥

1024 位的 在新版nginx上可能或报错 SSL_CTX_use_certificate:ee key too small
需要改成 2048以上 4096

ContinuousIntegration/TriagingTips/openssl-1.1.1 - Debian Wiki
openssl: Allow usage of insecure client certs - Server Fault

```
openssl genrsa -des3 -out server.key 4096
```

输入命令后 需要输入两遍密码 随便指定一个4位数及以上的密码

清除私钥密码

不带口令的Key (可以不要这一步，不用这一步的话以后每次重启nginx都需要输入密码)
mv server.key server.origin.key
openssl rsa -in server.origin.key -out server.key

输入命令后 需要输入上面设置的密码

生成csr 证书签名请求

```
SUBJECT="/C=CN/ST=Guangdong/L=Guangzhou/O=CM/OU=CM/CN=10.252.115.197"
SUBJECT="/C=CN/ST=Chongqing/L=Chongqing/O=AI/OU=AI/CN=localhost"

SUBJECT="/C=CN/ST=Anhui/L=Jieshou/O=AI/OU=AI/CN=localhost"
openssl req -new -subj $SUBJECT -key  server.key  -out server.csr
```

签名 100年过期

openssl x509 -req -days 36500 -in server.csr -signkey server.key -out server.crt

查看确认一下

openssl x509 -in server.crt -noout -text

配置nginx

vi /data01/nginx/nginx/conf/nginx.conf

```
listen 9001 ssl;

ssl_certificate cert/server.crt;
ssl_certificate_key  cert/server.key;
ssl_protocols        TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers          ECDHE-RSA-AES128-GCM-
SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;
ssl_prefer_server_ciphers  on;
ssl_session_cache    shared:SSL:10m;
ssl_session_timeout  10m;
```