使用shell脚本生成自签名证书

下载自签名证书脚本

shell脚本的使用说明如下：

- 脚本中使用openssl命令生成证书，执行前需要保证openssl命令可用。
- 脚本在centos 7和ubuntu 16.04中已经验证通过；在windows中的git bash里无法正确执行，不要在windows上的git bash里面执行脚本。
- 脚本命令格式如下：

```
./gen-cert.sh -a 算法 -d 域名 -n 证书文件名
```

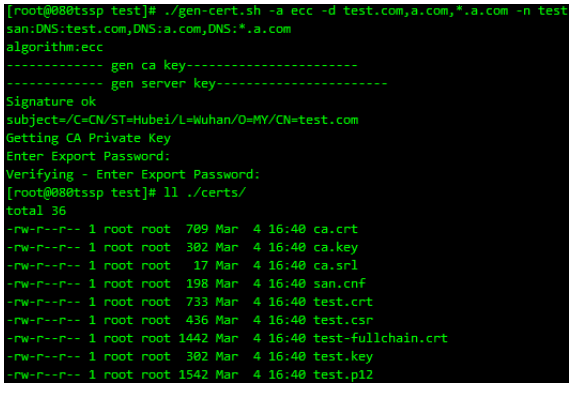
脚本中的参数说明：

- -a 生成的证书中使用的算法，有rsa和ecc两种选项，rsa会生成2048位的key，ecc生成prime256v1的key；
- -d 证书中的域名，可以支持写多个域名，多个域名使用逗号分隔。第一个域名会作为CN（common name），这个参数里面所有的域名会写入证书的SAN（通过这可以一个证书支持多个不同域名）。
- -n 生成的服务器证书文件名。脚本生成的证书文件都放在certs目录下，如果目录下已经存在同名的证书文件则会跳过。第二次执行脚本时，如果-n参数指定为与第一次不同的名称，则会使用第一次生成的CA证书签发新的服务器证书。
- -h 查看脚本帮助。

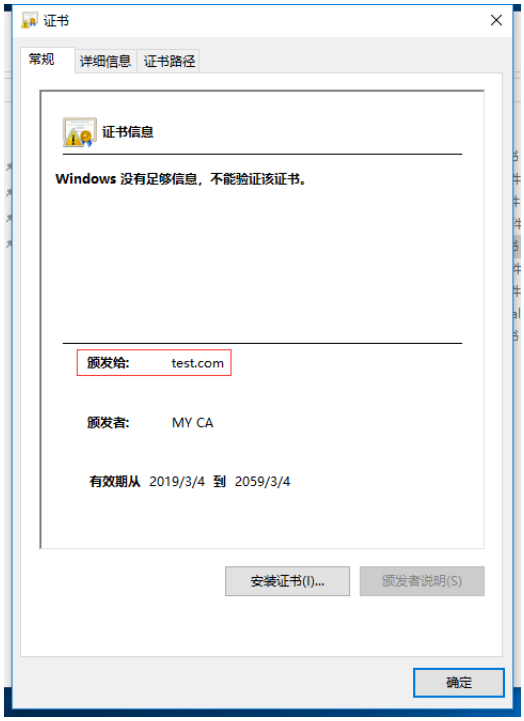
脚本执行示例

执行命令下面命令生成证书，生成pkcs12格式证书过程中会提示输入证书密码，请保持两次输入一致。虽然输入密码时可以直接回车设为空，由于某些使用证书的场景必须要密码，所以最好设置一个密码。生成的文件中ca.crt与ca.key为CA证书的公钥与私钥；test.crt与test.key为服务器证书的公钥与私钥；test.p12为pkcs12格式的文件，包含了公私钥。

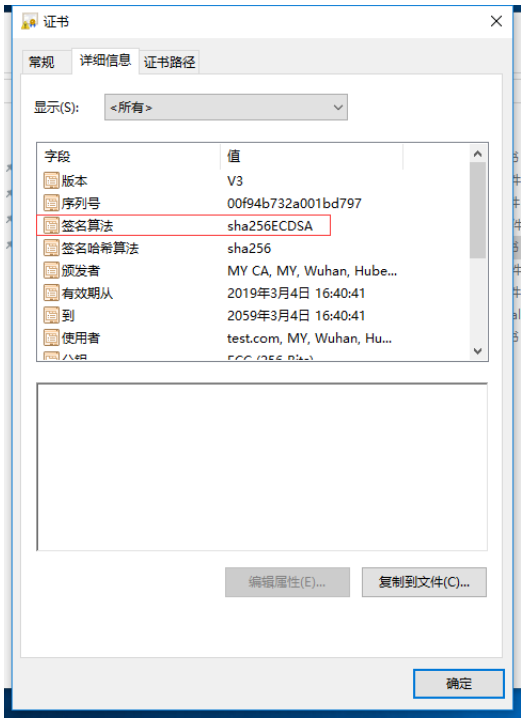
```
./gen-cert.sh -a ecc -d test.com,a.com,*.a.com -n test
```



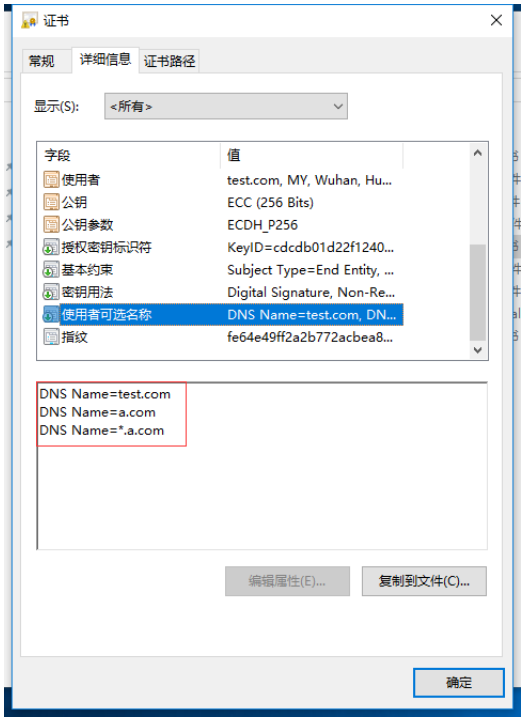
生成的服务器证书中“颁发给”为test.com，即-d参数中指定的第一个域名。



签名算法采用的ECC算法。



使用者可选名称包含了-d参数中指定的所有域名。


证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
使用者
test.com, MY, Wuhan, Hu...
公钥
ECC (256 Bits)
公钥参数
ECDH_P256
授权密钥标识符
KeyID=cdcdb01d22f1240...
基本约束
Subject Type=End Entity, ...
密钥用法
Digital Signature, Non-Re...
使用者可选名称
DNS Name=test.com, DN...
指纹
fe64e49ff2a2b772acbea8...
DNS Name=test.com
DNS Name=a.com
DNS Name=*.a.com
编辑属性(E)...
复制到文件(C)...
确定