Centos7下使用openssl生成CA及用户证书(测试用途)

证书 PKI **薛佳宇** 2021-01-12 发表

组网及说明

测试环境:

[root@xjyasia_cn CAs]# openssl version

OpenSSL 1.0.2k-fips 26 Jan 2017

[root@xjyasia_cn CAs]#

[root@xjyasia_cn CAs]# cat /etc/redhat-release

CentOS Linux release 7.9.2009 (Core)

[root@xjyasia_cn CAs]#

命令参数简介:

-aes256	使用AES算法（256为密钥）对产生的私钥加密
-key	密钥
-new	表示新的请求
-out	输出路径
-subj	指定用户信息
Ca	签发证书命令
Genrsa	产生RSA密钥命令
pkcs12	PKCS#12编码格式证书命令
Rand	随机数命令
Req	产生证书签发申请命令
x509	签发X.509格式证书命令
-Cacreateserial	表示创建CA证书序列号
-Cakey	表示CA证书密钥
-Caserial	表示CA证书序列号文件
-CA	表示CA证书
-cert	表示证书文件
-clcerts	表示仅导出客户证书
-days	表示有效天数
-export	表示导出证书
-extensions	表示按OpenSSL配置文件v3_ca项添加扩展
-extensions	表示按OpenSSL配置文件v3_req项添加扩展
-inkey	表示输入文件
-in	表示输入文件
-keyfile	表示根证书密钥文件
-req	表示证书输入请求
-sha1	表示证书摘要算法,这里为SHA1算法
-signkey	表示自签名密钥

配置步骤

(1)　生成CA证书

过程大致为：生成CA私钥-->生成CA证书请求-->自签名得到CA根证书（.crt）

1、生成CA私钥，名为ca-Private-Key.pem

```
[root@xjyasia_cn CAs]# openssl genrsa -out ca-Private-Key.pem 2048
Generating RSA private key, 2048 bit long modulus
.............................+++
.........................................+++
e is 65537 (0x10001)
```

2、使用CA的私钥生成CA证书请求ca-Req.csr

```
[root@xjyasia_cn CAs]# openssl req -new -key ca-Private-Key.pem -out ca-Req.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ".", the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN                    //国家
State or Province Name (full name) []:ZJ                //省份
Locality Name (eg, city) [Default City]:HZ              //城市
Organization Name (eg, company) [Default Company Ltd]:xjyasia.cn            //所属组织或公司
Organizational Unit Name (eg, section) []:xjyasia.cn                        //所属部门
Common Name (eg, your name or your server"s hostname) []:xjyasia.cn         //域名
Email Address []:                                       //邮件地址

Please enter the following "extra" attributes
to be sent with your certificate request
A challenge password []:***                             //密码
An optional company name []:                            //可选公司名称

[root@xjyasia_cn CAs]#
```

3、自签名得到CA根证书(生成 x509V3版本)

```
[root@xjyasia_cn CAs]# openssl x509 -req -extfile /etc/pki/tls/openssl.cnf -extensions v3_ca -in ca-Req.csr -out ca-cert.pem -signkey ca-Private-Key.pem -days 3650
// /etc/pki/tls/openssl.cnf是openssl的配置文件，其中包含了对于扩展参数v3_ca的定义
Signature ok
subject=/C=CN/ST=ZJ/L=HZ/O=xjyasia.cn/OU=xjyasia.cn/CN=xjyasia.cn
Getting Private key
[root@xjyasia_cn CAs]#
[root@xjyasia_cn CAs]# ll
total 12
-rw-r--r-- 1 root root 1318 Jan 12 13:21 ca-cert.pem
-rw-r--r-- 1 root root 1675 Jan 12 13:18 ca-Private-Key.pem
-rw-r--r-- 1 root root 1037 Jan 12 13:21 ca-Req.csr
[root@xjyasia_cn CAs]#
```

(2)　生成服务端证书

过程大致为：生成私钥-->生成证书请求-->用CA根证书签名得到证书

1、生成服务端证书的私钥server-Private-Key.pem

```
[root@xjyasia_cn CAs]# openssl genrsa -out server-Private-Key.pem 2048
Generating RSA private key, 2048 bit long modulus
....+++
..........+++
e is 65537 (0x10001)
[root@xjyasia_cn CAs]#
```

2、使用服务端证书的私钥生成服务端证书请求

```
[root@xjyasia_cn CAs]# openssl req -new -key server-Private-Key.pem -out server-Req.csr
You are about to be asked to enter information that will be incorporated
```

into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ".", the field will be left blank.

配置关键点

部分openssl配置文件

```
[v3_server]
basicConstraints       = critical, CA:FALSE
keyUsage               = critical, nonRepudiation, digitalSignature, keyEncipherment, keyAgreement
extendedKeyUsage       = critical, serverAuth                  //指定用途为服务端验证

[v3_client]
basicConstraints       = critical, CA:FALSE
keyUsage               = critical, nonRepudiation, digitalSignature, keyEncipherment, keyAgreement
extendedKeyUsage       = critical, clientAuth                  //指定用途为客户端验证
```

Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:ZJ
Locality Name (eg, city) [Default City]:HZ
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, your name or your server"s hostname) []:xjyasia.cn
Email Address []:

to be sent with your certificate request
A challenge password []:*****
An optional company name []:
[root@xjyasia_cn CAs]#
[root@xjyasia_cn CAs]#