2019-06-06-openssl生成自签名ssl证书及证书链制作

Gswu 关注
2019.06.06 16:09:43 字数 813 阅读 3,703

openssl 是目前最流行的 SSL 密码库工具，其提供了一个通用、健壮、功能完备的工具套件，用以支持SSL/TLS 协议的实现。

以下为测试正式生成过程而做的实验，基本模拟了整个证书的生成过程。

第一步，为服务器端和客户端准备公钥、私钥

生成服务器端私钥
命令：

```
openssl genrsa -out server_pri.key 1024
```

// 生成服务器端公钥

命令：

```
openssl rsa -in server_pri.key -pubout -out server_pub.pem
```

第二步，生成 CA 证书

// 生成 CA 私钥
命令：

```
openssl genrsa -out ca.key 1024
```

命令：

```
openssl req -new -key ca.key -out ca.csr
```

//会出来一个填写资料的界面,Common Name这一项，是最后可以访问的域名
命令：

```
openssl x509 -req -in ca.csr -signkey ca.key -out ca.crt
```

第三步，生成服务器端证书

// 服务器端需要向 CA 机构申请签名证书，在申请签名证书之前依然是创建自己的 CSR 文件
命令：

```
openssl req -new -key server_pri.key -out server.csr
```

// 向自己的 CA 机构申请证书，签名过程需要 CA 的证书和私钥参与，最终颁发一个带有 CA 签名的证书
命令：

```
openssl x509 -req -CA ca.crt -CAkey ca.key -CAcreateserial -in server.csr -out server.crt
```

同样会有信息填写，照旧写就好了

第四步，生成cer文件

//使用openssl 进行转换
命令：

```
openssl x509 -in server.crt -out server.cer -outform der
```

如果完成，就会得到这么9个文件

第五步 配置到服务器端nginx

```
server {
    listen 80;
    server_name www.cc.com;
    rewrite ^(.*)$ https://www.bb.com $1 permanent;
}
server {
    listen 80;
    server_name www.bb.com;
    rewrite ^(.*)$ https://${server_name}$1 permanent;
}
server {
    listen 443;
    server_name www.test.com;
    ssl on;
    ssl_certificate /data/csr/server.crt;
    ssl_certificate_key /data/csr/server_pri.key;
    location / {
        root /data/bb;
        index  index.html index.htm;
    }
}
```

解决证书链问题

证书链可以有任意环节的长度，所以在三节的链中，信任锚证书CA 环节可以对中间证书签名；中间证书的所有者可以用自己的私钥对另一个证书签名。CertPath API 可以用来遍历证书链以验证有效性，也可以用来构造这些信任链。

Web 浏览器已预先配置了一组浏览器自动信任的根 CA 证书。来自其他证书授权机构的所有证书都必须附带证书链，以检验这些证书的有效性。证书链是由一系列 CA 证书发出的证书序列，最终以根 CA 证书结束。

我们一般会有三种证书：RootCA.crt(rCA，被信任的根证书)、IntermediateCA.crt(mCA，某些厂商有多个中间证书)、server.crt(sCA，通过CSR签下来的证书)

为了让浏览器能够信任我们的证书，我们需要配置一条完整的证书链，证书链由sCA和mCA构成就好，rCA是浏览器内置，不需要服务器给提供。

nginx配置证书链的时候，就是指定一个证书文件，这个文件中含有我们整个证书链的所有证书就好，证书合并的时候，正确的合并方法是把 mCA 合并到 sCA 中。当有多个 mCA 文件时，mCA 从下级到上级（根证书为最上级）依次合并到 sCA 中。

```
-----BEGIN CERTIFICATE-----
------ sCA ------
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
------ mCA (lower) ------
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
------ mCA (upper) ------
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
[ROOT CERTIFICATE]
-----END CERTIFICATE-----
```


Gswu
总资产2 共写了9552字 获得22个赞 共9个粉丝 关注

推荐阅读
TLS握手 阅读 103
Http1.0、Http1.1和Http2.0以及Https 阅读 197
二进制安装-k8s高可用集群03-kubectl命令行工具 阅读 204
iOS 网络数据安全(防止抓包) 阅读 721
Doker开启远程安全访问(x.x.x.x:2376) 阅读 224

全部评论 0 只看作者

按时间倒序 按时间正序

被以下专题收入，发现更多相似内容

运维工程师的进阶之路

推荐阅读 更多精彩内容 >

openssl 自签名证书 - 制作证书(二)

【上一篇：openssl 自签名证书 - 安装openssl(一)】事前准备 相关:pem、key:私钥文件，对...

码师和_夏尼 阅读 5,093 评论 0 赞 4

自签名数字证书的使用

写这篇文章的起因是遇到了需要本机配置支持HTTPS协议的情况。我们知道，因为HTTPS的安全性，越来越多的网络应...

Jason_M_Ho 阅读 8,959 评论 1 赞 8

关于证书的那些事：自签名证书和私有CA签名证书等

证书的三个作用 加密通信和身份验证(验证对方确实是对方声称的对象)和数据完整性(无法被修改，修改了会被知)证...

SuperRoot 阅读 10,084 评论 1 赞 11

mosquitto:SSL-CA-Server-Client 证书生成

一、Mosquitto安装 1.下载安装http://www.eclipse.org/downloads/down...

FocusBiao 阅读 1,479 评论 0 赞 0

《向往的生活》：我们的蘑菇屋

一开始点击这个综艺，是因为当时没觉得有什么好看的电影电视剧，看到何炅、黄磊以及Henry都在里面，看起来好像挺好玩...

行走的唇毛 阅读 410 评论 2 赞 3

抽奖

写下你的评论...

评论0 赞