

原创

hobby云说

2020-04-15 15:09:54

1715

收藏 5

版权

分类专栏：

openssl

安全

openssl

同时被 2 个专栏收录

0 订阅

2 篇文章

订阅专栏

【前言】

说来惭愧，干了快一年的运维，能力还是很欠缺，前些天因为ToB项目需求，需要用nginx搭建一个正向代理，研究了一番，在本地环境搭建一套七层代理，[请移步这里查看](#)。自认为理解了，其实不然，真正到ToB客户环境搭建的时候还是无从下手。听我扯了这么多，这些和本文有什么关系呢？当然有，这个七层代理的是https，中间人代理的话，就需要用到自建CA证书，那么问题来了，CA证书是什么呢？[请移步这里查看](#)。CA证书如何获取呢？请听我细细道来.....

【OpenSSL自签普通证书】

大致流程如下

一、创建index.txt、serial文件

二、生成CA根证书

1.创建根证书私钥

2.使用根证书私钥创建一个自签根证书的申请

3.使用申请和私钥签发根证书

三、生成自签证书

1.创建自签证书私钥

2.创建一个自签证书申请

3.使用自签的根证书对自签证书申请进行签署

在造证书之前我们先来看看配置文件openssl.conf的一些说明吧

#CA配置相关说明：

```
1 [ ca ]
2
3 default_ca = CA_default # The default ca section 默认CA
4 #####
5 [ CA_default ] 默认CA包含的信息
6 dir = /etc/pki/CA # Where everything is kept CA的公共目录
7 certs = $dir/certs # Where the issued certs are kept
8 #被发布的证书&旧的证书存放目录
9 crl_dir = $dir/crl # Where the issued crl are kept
10 #被吊销的证书存放目录
11 database = $dir/index.txt # database index file.
12 #存放颁发证书的数据库文件.默认不存在需要手动先创建
13 #unique_subject = no # Set to 'no' to allow creation of
14 # several ctificates with same subject.
15 new_certs_dir = $dir/newcerts # default place for new certs.
16 #新颁发的证书存放目录
```

分类专栏

	安全	19篇
	安全测试	2篇
	win/mac/linux系统安装	3篇
	nginx	6篇
	linux日常小操作	33篇
	运维开发系统学习	22篇
	漏洞复现	3篇
	openssl	2篇
	Linux三剑客sed、awk...	3篇
	Django	1篇
	kali_linux	1篇
	nodejs+npm+pm2	3篇
	密码学	
	数据库	2篇
	ELK	9篇
	windows日常小操作	1篇
	rabbitmq	4篇
	rsync	2篇
	马坡岭小甜甜专栏	1篇
	日常碎碎念	
	openldap	3篇
	python学习	14篇
	其他	3篇
	计算机网络	14篇
	个人项目	1篇
	zabbix监控	22篇

```
17 certificate = $dir/cacert.pem # The CA certificate 自签名证书，局域网内的根CA自证证书
18 serial      = $dir/serial      # The current serial number
19 下一个证书颁发的编号 16进制数,默认不存在需要手动先创建，并且指定第一个证书的开始编号，serial为16进制数00开始
20 crlnumber   = $dir/crlnumber    # the current crl number    下一个吊销证书的编号
21                                     # must be commented out to leave a V1 CRL
22 crl         = $dir/crl.pem      # The current CRL          证书吊销列表
23 private_key = $dir/private/akey.pem # The private key      CA的私钥文件
24 RANDFILE    = $dir/private/.rand # private random number file 私钥随机数文件
25 x509_extensions = usr_cert     # The extensions to add to the cert
26                                     要添加到证书的扩展
27 default_days = 365              # how long to certify for 默认ca有效期
28 default_crl_days= 30            # how long before next CRL
29                                     定义多少天公布新的吊销证书名单
30 default_md   = sha256           # use SHA-256 by default 默认加密算法
31 preserve     = no               # keep passed DN ordering
32
```

#创建CA和申请证书选项说明：

```
1 policy = policy_match
2 # For the CA policy
3 [ policy_match ]
4 countryName = match match的参数意味着签发的证书和根证书必须保持一致
5 #stateOrProvinceName = match
6 #organizationName = match
7 stateOrProvinceName = optional
8 organizationName = optional 申请非根自证书时组织必填项，即用户是什么组织
9 organizationalUnitName = optional optional 不关心是否一样
10 commonName = supplied supplied是必须提供的，即网站域名
11 emailAddress = optional
```

一、创建index.txt、serial文件

从配置文件可以看到，存放颁发证书的数据库文件index.txt和证书颁发的编号serial两个文件是必须要手动创建的。从配置文件里看到，默认公共目录是/etc/pki/CA，当然你也可以复制openssl.conf自定义配置到其他的路径也行。这点在后面的创建多IP/域名的自签证书里我会讲到，这里先用自带的默认配置文件生成根文件。

```
1 [root@VM118 CA]# touch index.txt
2
3 [root@VM118 CA]# echo 00 > serial
```

二、生成CA根证书

1、创建根证书私钥

这里openssl用到的是rsa算法，业界公认2048位是最安全的

```
openssl genrsa -out scwiperoot.key 2048
```

你可以选择一步到位，不创建申请文件，直接创建根证书

```
openssl req -x509 -new -sha512 -days 36500 -subj "/C=cn/ST=shenzhen/L=shenzhen/O=example/OU=Personal/CN=scwipe.com"
-key scwiperoot.key -out scwipetestroot.crt
```

2、使用生成的根私钥创建一个根申请证书（.csr格式）

Common Name必填，表明你创建的这个CA根的机构名字

```
1 [root@VM118 CA]# openssl req -new -key scwiperoot.key -out scwiperoot.csr
2
3 You are about to be asked to enter information that will be incorporated
4 into your certificate request.
5 What you are about to enter is what is called a Distinguished Name or a DN.
6 There are quite a few fields but you can leave some blank
7 For some fields there will be a default value,
8 If you enter '.', the field will be left blank.
9 -----
10 Country Name (2 letter code) [XX]:CN
11 State or Province Name (full name) []:
12 Locality Name (eg, city) [Default City]:
13 Organization Name (eg, company) [Default Company Ltd]:
14 Organizational Unit Name (eg, section) []:
15 Common Name (eg, your name or your server's hostname) []:scwipe.com
16 Email Address []:
17
18 Please enter the following 'extra' attributes
19 to be sent with your certificate request
20 A challenge password []:
21 An optional company name []:
```

3、使用根证书私钥签发申请证书

```
1 [root@VM118 CA]# openssl x509 -req -days 36500 -in scwiperoot.csr -signkey scwiperoot.key -out scwiperoot.crt
2
3 Signature ok
4 subject=C=CN/L=Default City/O=Default Company Ltd/CN=scwipe.com
5 Getting Private key
```

三、生成自签证书

1、创建自签证书的私钥

```
[root@VM118 CA]# openssl genrsa -out scwipeserver.key 2048
```

2、创建自签证书申请（.csr格式）（此为单域名签发，多域名签发将在另外一篇文章讲解）

自签SSL证书时，**申请组织（Organization Name）**必填项，**Country**必须和根证书一致，这里我填的CN

```
1 [root@VM118 CA]# openssl req -new -key scwipeserver.key -out scwipeserver.csr
2
3 You are about to be asked to enter information that will be incorporated
4 into your certificate request.
5 What you are about to enter is what is called a Distinguished Name or a DN.
6 There are quite a few fields but you can leave some blank
7 For some fields there will be a default value,
8 If you enter '.', the field will be left blank.
9 -----
10 Country Name (2 letter code) [XX]:CN
11 State or Province Name (full name) []:GuangDong
12 Locality Name (eg, city) [Default City]:ShenZhen
```



```
13 Organization Name (eg, company) [Default: Company Ltd]:
14 Organizational Unit Name (eg, section) []:
15 Common Name (eg, your name or your server's hostname) []:www.scwipe.com
16 Email Address []:
17
18 Please enter the following 'extra' attributes
19 to be sent with your certificate request
20 A challenge password []:
21 An optional company name []:
```

3、使用根证书和私钥签发server申请证书

```
[root@VM118 CA]# openssl ca -in scwipeserver.csr -cert scwiperoot.crt -keyfile scwiperoot.key -out scwipeserver.crt -days 36500
```

4、验证自签SSL证书是否ok

```
1 [root@VM118 CA]# openssl verify -verbose -CAfile scwiperoot.crt scwipeserver.crt
2
3 scwipeserver.crt: OK
```

至此，我们就完成了根证书的自签，以及使用自签的根证书签发单域名SSL证书，后面还会继续更新用自签的根证书签发多域名/IP的SSL证书。

欢迎联系我：

邮箱：zghobby@163.com

订阅号搜索“hobby云说”

里面有我的技术、人生等分享记录哟~



https://blog.csdn.net/qq_245011199

有关蓝牙耳机市场的详细分析

01-04

此文对蓝牙耳机市场进行了详细分析,包括市场,用户,产业结构等.

基于OpenSSL的CA建立及证书签发 (签发多域名/IP)

hobby云说 1180

自签SSL证书 (多域名/IP) 本文基于以下环境：内核信息：Linux zabbix 3.10.0-957.el7.x86_64 #1 SMP Thu Nov 8 23:39:32 UTC 2018 x86_64 x86_64...



优质评论可以帮助作者获得更高权重



评论



hobby云说

码龄7年  暂无认证

134	3w+	1w+	12w+	
原创	周排名	总排名	访问	等级

2732	118	168	84	484
积分	粉丝	获赞	评论	收藏












私信

关注

搜博主文章



热门文章

永久开启或关闭某些iptables开机自启规则  11652

HTTPS建立连接详细过程  7982

Kali Linux2021.1安装详细教程  5824

Python画图之浪漫樱花  5406

补码(为什么按位取反再加一):告诉你一个其实很简单的问题  5276

最新评论

Python画图之浪漫樱花
m0_62553950: 想问一下一直提示错误: At
tribute Error:'Screen'. object has no attr...

Python画图之浪漫樱花
敲敲代码吃吃饭: 好好看

Python画图之浪漫樱花
疯狂的魔王: 棒棒!

关于zabbix-proxy (原理)
hobby云说: ahhhhh, 少了个0, 多谢提醒



关于zabbix-proxy (原理)
qq1187228784: 50°50'=2500 🤔



您愿意向朋友推荐“博客详情页”吗？



    

强烈不推荐 不推荐 一般般 推荐 强烈推荐

最新文章

 小松漫步时: 赞啊 1 年前 [回复](#) ...  1

 TrueDei: 加油 1 年前 [回复](#) ... 

 扬帆向海: 加油 1 年前 [回复](#) ... 

基于OpenSSL 的 CA 建立及证书签发_林三的专栏	10-18
基于OpenSSL 的 CA 建立及证书签发 下文详细记录了基于 OpenSSL 的 CA 建立及证书签发过程。 建立CA 建立CA 目录结构 按照OpenSSL 的默认配置...	
OpenSSL自签发配置有多域名或ip地址的证书_山鬼谣的专栏	9-30
用OpenSSL配置带有SubjectAltName的ssl请求 对于多域名,只需要一个证书就可以保护非常多的域名。 SubjectAltName是X509 Version 3 (RFC 2459)的...	
OpenSSL 自建CA及签发证书	scuyxi 的专栏 2万+
ref: http://rhythm-zju.blog.163.com/blog/static/310042008015115718637/利用 OpenSSL 建立 CA 及自行签发证书。1. 创建CA目录结构在CA的配置文件...	
基于 OpenSSL 的 CA 建立及证书签发	先做个码农 248
转自http://rhythm-zju.blog.163.com/blog/static/310042008015115718637/ 建立 CA 建立 CA 目录结构 按照 OpenSSL 的默认配置建立 CA ,需要在文件...	
Linux:openssl创建CA及颁发证书_杜达达的博客	10-9
工具:openssl enc, gpg 算法:3des, aes, blowfish, twofish 帮助:man enc1、 加密:enc对称算法加密 -e加密 -des3算法加密 -a base64编码 -salt加盐打乱顺...	
openssl 自签证书(带ip或者域名)_cloudfantasy的博客	10-20
4、根证书签发下级证书: 4.1、普通什么都没有,不带x509v3 openssl x509 -req -CA myCA.crt -CAkey myCA.key -CAcreateserial -days 3560 -inmycert.cs...	
openssl 创建ca 签发证书	10-10
openssl创建自己的ca 签发证书 创建多级ca 有具体例子	
OpenSSL自签发配置有多域名或ip地址的证书 热门推荐	山鬼谣的专栏 2万+
环境翻译加实践概述HTTPS服务是工作在SSL/TLS上的HTTP。 首先简单区分一下HTTPS, SSL, TLS, OpenSSL这四者的关系: SSL: (Secure Soc...	
使用 openssl 创建自签发证书, 含 IP证书 及 泛域名证书	onebird_lmx 的博客 2798
web里面需要使用ssl才能使用, 所以需要使用域名证书: 1. 创建根证书 创建秘钥 openssl genrsa -out LocalRootCA.key 2048 生成证书并自签名, node...	
基于 OpenSSL 的 CA 建立及证书签发 【转】	dkyptnz538386的博客 28
建立 CA 建立 CA 目录结构 按照 OpenSSL 的默认配置建立 CA ,需要在文件系统中建立相应的目录结构。相关的配置内容一般位于/usr/ssl/openssl.cnf内...	
OpenSSL生成根证书CA及签发子证书	lipviolet 的博客 2360
系统: CentOS7 32位 目标: 使用OpenSSL生成一个CA根证书, 并用这个根证书颁发两个子证书server和client。 先确保系统中安装了OpenSSL, 若没安...	
OpenSSL的配置文件	ayang1986的专栏 7988
许多OpenSSL命令(例如,req和ca)带有一个-config参数用于指定openssl配置文件的位置. 本节提供配置文件格式的简短描述和它怎么应用于req和ca命令....	
SSL数字证书之CA根证书、CA中间证书和SSL证书	hobby云说 2271
【前言】说一大背景吧,我们的一个后台服务需要部署在一个没法上外网的环境,但是我们的后台服务需要访问七牛云进行对象存储,于是乎,需要一...	
基于openssl的ca建立及证书签发	weixin_34357962的博客 34
OpenSSL为网络通信提供安全及数据完整性的一种安全协议,囊括了主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议,并提供了丰富的应...	
使用openssl签发证书、签发服务器证书、多域名证书	qiqiangnie 的博客 659
使用openssl签发证书、签发服务器证书、多域名证书 1、openssl.cnf的配置 openssl.cnf位置在 /usr/local/ssl/openssl.cnf 修改【CA_default】标签下的 ...	
OpenSSL--Window生成证书实战	weixin_33754913的博客 915
为什么80%的码农都做不了架构师?>>> ...	
OpenSSL自建CA和签发二级CA及颁发SSL证书	走马行酒醺,驱车布鱼肉 4186
自己签发CA证书再签发服务器证书的场景非常简单。把根CA证书导入到浏览器后,就可以信任由这个根CA直接签发的服务器证书。但是实际上网站使用...	
Linux 使用openssl ca方式签发证书	QianLiStudent的博客 421
前言 客户端到服务端或服务端到服务端的请求方式通常是http居多(这里只考虑一般的系统),但是考虑到安全性的问题,我们会采用给系统添加一个证...	
OpenSSL生成根证书CA及签发证书	skytering 的博客 3786
OpenSSL生成根证书CA及签发证书1.系统环境2.准备工作2.1.OpenSSL的配置3.生成根证书3.1.生成根证书私钥3.2.生成证书请求 (ca.csr)3.3.检查证书请...	



闲谈安全测试之IAST

闲谈安全测试左移三板斧

2021年 11篇	2020年 42篇
2019年 76篇	2018年 1篇
2017年 6篇	

使用 openssl 创建自签发证书，含 泛域名证书和IP证书 最新发布

Arlingtonroad的博客 311

1. 创建根证书 创建秘钥openssl genrsa -out LocalRootCA.key 2048 生成证书并自签名，nodes是不用密码openssl req -sha256 -new -nodes -x509 -day...

©2021 CSDN 皮肤主题: 书香水墨 设计师:CSDN官方博客 返回首页

关于我们 招贤纳士 广告服务 开发助手 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00



hobby云说

关注



10



7



5





专栏目录