原创 hobby云说 2020-06-09 10:06:20 1179 收藏 6 原力计划 版权
分类专栏： openssl 安全 计算机网络 文章标签： ssl
openssl 同时被 3 个专栏收录

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 x86_64 GNU/Linux

系统版本：CentOS Linux release 7.6.1810 (Core)

OpenSSL版本：OpenSSL 1.0.2k-fips 26 Jan 2017

【前言】

在基于OpenSSL的CA建立及证书签发（签发单域名/IP）一文中（后面统一称作上文中），我已经有详细的介绍如何用openssl自签一个根证书以如何用自签的根证书去签发一个SSL证书。在上文中的前言里我有说到做nginx的https代理需要一个自签SSL证书，其实这个自签SSL证书是用来跟七牛云进行传输的，众所周知，七牛云的上传和下载是走到两个域名，具体的的这里就不展开说了，后面有时间再单独出一篇关于七牛云的文章吧。那么显然在上文中签发的单一域名不满足这个需求。解决的办法有两种，第一就是再签发一个SSL证书，第二种就是签发多域名SSL证书。好了，废话不多说，我们来看看要怎么操作吧。

【OpenSSL自签多域名/IP证书】

大致流程如下

一、创建index.txt、serial等文件

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ca根证书的申请

3.使用申请和私钥签发ca根证书

三、**修改openssl配置文件**

四、用修改后的配置文件生成SSL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

如果看了我写的单域名签发就会发现在这里多了一步**修改openssl配置文件**，这一步就是为自签发多域名做准备的。这里要提及一个新名词**SubjectAltName**，简称SAN。于我个人理解，它就是X509数字证书中的一个扩展项，用来添加多个签发的域名/ip的一个扩展项，在openssl的默认配置中是没有打开的，详细解说移步这里：（https://blog.csdn.net/henter/article/details/91351800）。接下来是正式的操作步骤。

一、创建index.txt、serial等文件

```
[root@zabbix ca]# cd /etc/pki/CA

[root@zabbix CA]# touch index.txt

[root@zabbix CA]# echo 00 > serial
```

二、生成CA根证书

1、创建根证书私钥

[root@zabbix ca]# openssl genrsa -out ca.key 2048

2、创建根证书申请证书（切记，生成CA根证书的时候不能用修改的openssl.conf文件）

```
[root@zabbix ca]# openssl req -new -out ca.csr -key ca.key

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
State or Province Name (full name) []:GD
Locality Name (eg, city) [Default City]:SZ
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:scwipe.com
Email Address []:


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3、生成ca根证书

[root@zabbix ca]# openssl x509 -req -days 36500 -in ca.csr -signkey ca.key -out ca.crt

三、修改openssl配置文件

1、复制openssl配置文件

为了不破坏原始文件，我们使用带配置文件的方式来生成证书，先把证书复制到另外一个地方，这里我保存到/root/ca目录下

[root@zabbix ca]# mkdir -p /root/ca && cp /etc/pki/tls/openssl.cnf /root/ca/

2、修改[req]段落

为了让openssl处理证书请求（csr）时，带上拓展项，所以需要配置req_extensions项，此时[req]必须包含下面两行

```
[req]

basicConstraints = CA:TRUE
distinguished_name= req_distinguished_name
req_extensions = v3_req
```

3、修改[v3_req]段落

增加subjectAltName行如下

subjectAltName = @alt_names

4、增加[alt_names]模块

此处填写你需要签发的域名/ip，如下

```
[alt_names]

DNS.1=*scwipe.com
DNS.2=*.scwipe.cn
```

四、用自签ca证书签发ssl证书

1、创建ssl证书私钥

[root@zabbix ca]# openssl genrsa -out scwipe.key 2048

2、创建证书请求文件csr

（此处需要注意国家、省份、城市需要和ca根证书保持一致，当然也可以修改配置文件，具体见签发 基于OpenSSL的CA建立及证书签发（签发单域名/IP））

```
[root@zabbix ca]# openssl req -new -key scwipe.key -out scwipe.csr -config /root/ca/openssl.cnf -extensions v3_re
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
State or Province Name (full name) []:GD
Locality Name (eg, city) [Default City]:SZ
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:*.scwipe.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3、用ca根证书签发ssl证书

openssl ca -in scwipe.csr -out scwipe.crt -cert ca.crt -keyfile ca.key -extensions v3_req -days 36500 -config /root/ca/openssl.cnf

4、验证自签SSL证书是否ok

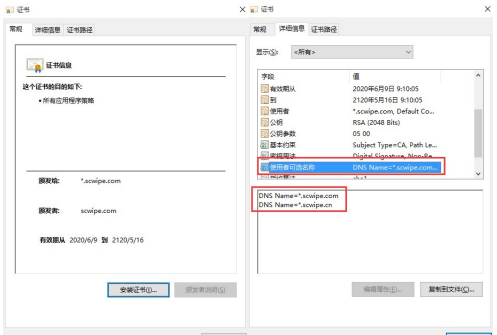
openssl verify -verbose -CAfile ca.crt scwipe.crt

scwipeserver.crt: OK

将签发的ca根证书和SSL证书导出到win上面查看，先信任自己签发的根证书，双击ca.crt

安装证书-->选择本地计算机-->将所有
证书都放入下列存储-->浏览-->受信任的根证书颁发机构-->下一步-->完成

完成上面的操作后，再双击签发的SSL证书，我这里是scwiper.crt证书，就可以看到如下，就是签发成功了



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…

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…

优质评论可以帮助作者获得更高权重 评论

凉鞋的笔记： 谢谢分享 1 年前 回复

hobby云说
码龄7年 暂无认证

134
原创
2732
积分

私信 关注

搜博主文章

3万+ 周排名 | 1万+ 总排名 | 12万+ 访问 | 等级
118 粉丝 | 168 获赞 | 84 评论 | 484 收藏

基于OpenSSL的CA建立及证书签发(签发单域名/IP)_hobby云说 10-25
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/pk…

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https证书 — zheshijieyouwo的博客 1798
生成CA私钥与CA证书 1. openssl genrsa -out cakey.pem 2048 2. openssl req -new -x509 -sha256 -key cakey.pem -out cacert.pem 生成服务端私钥与证…

openssl 生成证书及生成过程 — nsaygl的专栏 3687
1. 基本原理 公司一个项目要进行交易数据传输,因为这个项目银行那边也是刚刚开始启动,所有的支持只有一个传输字段的说明文档,好吧,总的有人做事不是…

基于openssl的ca建立及证书签发_weixin_34357962的博客 9-16
基于openssl的ca建立及证书签发 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…

openssl自签名多域名证书 — weixin_30770495的博客 307
这几天一直在研究如何使用openssl工具来生成多域名证书，今天终于有点眉目了，实现方法如下： 生成私钥 openssl genrsa -out server.key 1024 用私…

OpenSSL生成v3证书方法及配置文件 — weixin_34066347的博客 968
场景： 业务需要生成v3版的证书，而一般使用OpenSSL生成证书时都是v1版的，不带扩展属性。方法：在使用CA证书进行签署证书时加入-exfile和-exten…

openssl 生成v3证书 — wangsifu2009的专栏 5221
今天一下午都在调这个，网上也到处搜帖子，提问的一大票，能解决的暂时没有发现~~~~~ 想使用openssl生成一个只能用于签名的证书，即证书的扩展属…

生成本地测试用https证书，支持通配符和多域名，初学OpenSSL — 高坚果兄弟 3856
18-01-26在v2ex上看到一妹纸发的《身为一个 21 岁的年轻程序员，我已经腰突了（躺），哈哈，感同身受，想到这几天我左腿麻木持续了好几天，前几…

使用openssl签发证书、签发服务器证书、多域名证书 最新发布 — 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、openssn.cnf的配置 openssn.cnf位置在 /usr/local/ssl/openssl.cnf 修改【CA_default】标签下的 …

最新评论

Python画图之浪漫樱花
m0_62553950: 想问一下一直提示错误：Attribute 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: 好棒！

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

关于zabbix-proxy（原理）
qq1187228784: 50*50=2500

最新文章

浅谈系列之跨站脚本攻击（XSS）

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	

OpenSSL创建带SAN扩展的证书并进行CA自签 — liwei2633的专栏 — 1万+
什么是 SANSAN(Subject Alternative Name) 是 SSL 标准 x509 中定义的一个扩展。使用了 SAN 字段的 SSL 证书，可以扩展此证书支持的域名，使得一个…

TLS初探（4）多域名证书 — jjxojm的专栏 — 1478
在“TLS初探（2）证书简介”中提过，如想使用泛域名，可在Subject DN(Distingushed Name)的CN(Common Name)中使用*通配符，例如*.abc.com。…

openssl生成自签名泛域名（通配符）证书 — qq_21359467的博客 — 4866
openssl自签名泛域名（通配符）证书生成命令（Liunx） 首先编译openssl.cnf文件,如果没有安装openssl的话先在度娘上搜索安装方法进行安装，下面的…

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…

SSL多域名绑定证书的解决方案 — zymx(u010820135)的专栏 — 7129
转自 http://codefine.co/2786.html 之前有几篇文章已经关注过加密解密证书和HTTTPS的一些基本原理。HTTPS、SSL与数字证书介绍，公钥私钥加密…

openssl证书添加多个IP — 林三的专栏 — 1万+
前文http://blog.csdn.net/linsanhua/article/details/16878817 描述了基于 OpenSSL 的 CA 建立及证书签发过程。 这里描述怎么利用subjectAltName添加ip…

openssl 自签发证书及ssl 原理简介（一） — Vicky — 3527
提纲： 1、使用openssl自签发证书 2、配置apache 3、配置客户端 4、ssl原理分析 一、使用Openssl自签发证书 首先装openssl 。编辑配置文件/etc/ssl/o…

grpc使用ssl(tls) 通过openssl指定多个域名和IP — devotedwife的博客 — 2229
最近在使用grpc做项目，信息安全的同事提出要求，需要将来往报文加密，避免抓包。阅读grpc的文档，发现它已经支持ssl(tls)，因此直接选这种认证和…

openssl 生成X509 V3的根证书及签名证书 — 冰冻三尺非一日之寒 — 1万+
openssl 生成X509 V3的根证书及签名证书在测试的时候有时需要使用证书。因此使用OpenSSL创建自签名根证书，使用根证书签发证书显得很重要。1、…

OpenSSL命令---req — VitalityShow(网络通讯) — 1万+
本指令用来创建和处理PKCS#10格式的证书。它还能够建立自签名证书，做Root CA。