



清园

沉没的Atlantis

签发SSL多域名自签证书

本文章在CentOS7下操作通过.

多域名证书, 有两种配置方式:

1. 使用openssl.cnf进行配置

2. 直接命令行内内置生成

下面使用一个例子, 来具体说明一下两种方式的做法.

一. 复制并修改openssl配置文件(openssl.cnf)

```
#CentOS的配置文件在/etc/pki/tls/下
mv /etc/pki/tls/openssl.cnf ./
```

修改配置文件并保存.

```
#这3个是取消注释并修改
copy_extensions = copy
req_extensions = v3_req
subjectAltName = @alt_names
#新增alt_names节点并配置需要的域名和IP
[alt_names]
DNS.1 = *.org.example.com
DNS.2 = *.abc.com
IP.1 = 127.0.0.1
IP.2 = 2.0.12.10
```

二. 生成根证书(CA) - 使用配置文件方式生成

```
#生成CA key文件
openssl genrsa -out ca.key 2048

#使用配置文件生成自签名CA证书
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 \
    -subj "/C=CN/ST=ZHEJIANG/L=HANGZHOU/O=WANMA/OU=COMPANY/CN=127.0.0.1" \
    -config ./openssl.cnf -extensions v3_req \
    -out ca.pem
```

导航

[博客园](#) [首页](#) [联系](#) [订阅](#) [管理](#)

2021年10月						
日	一	二	三	四	五	六
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

公告

昵称: [太清](#)
园龄: [12年4个月](#)
粉丝: [58](#)
关注: [0](#)
[+加关注](#)

统计

随笔 - 80 文章 - 0 评论 - 29 阅读 - 76万


搜索

随笔分类

[DB\(13\)](#)
[Docker\(2\)](#)
[Java\(9\)](#)
[JavaScript\(2\)](#)
[Linux\(28\)](#)
[MVC\(2\)](#)
[Other\(3\)](#)
[Revision Control\(6\)](#)
[Web Server\(10\)](#)
[Windows\(9\)](#)

随笔档案

[2021年9月\(2\)](#)
[2021年7月\(1\)](#)
[2021年6月\(1\)](#)
[2021年3月\(1\)](#)
[2020年7月\(2\)](#)
[2020年6月\(6\)](#)
[2020年5月\(1\)](#)
[2020年4月\(1\)](#)
[2020年3月\(1\)](#)
[2020年1月\(1\)](#)
[2019年12月\(1\)](#)
[2019年10月\(1\)](#)
[2019年8月\(3\)](#)

# 直接命令行生成ca.pem , 该命令可以不用复制openssl.cnf

```
openssl req -x509 -new -nodes -key ./ca.key -sha256 -days 3650 \
    -subj "/C=CN/ST=ZHEJIANG/L=HANGZHOU/O=WANMA/OU=COMPANY/CN=127.0.0.1" \
    -reqexts SAN \
    -config <(cat /etc/pki/tls/openssl.cnf <(printf "\n[SAN]\nsubjectAltName=DNS:*.abc.com,IP:0.0.0.0")) \
    -out ca.pem
```

#使用这个命令可以查看生成的CA证书是否支持多域名

```
openssl x509 -text -in ca.pem -noout
```

三 . 生成服务器端证书 - 使用配置文件方式生成

#生成Server端 Key文件

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

#生成签名请求

```
openssl req -new -key ./server.key \
    -subj "/C=CN/ST=ZHEJIANG/L=HANGZHOU/O=WANMA/OU=COMPANY/CN=127.0.0.1" \
    -config ./openssl.cnf -extensions v3_req \
    -out server.csr
```

#使用CA证书签名Server端证书

```
openssl x509 -req -in ./server.csr -CA ca.pem -CAkey ca.key -CAcreateserial \
    -extfile ./openssl.cnf -extensions v3_req \
    -days 3650 -sha256 -out server.pem
```

#使用这个命令可以查看生成的Server端证书是否支持多域名

```
openssl x509 -text -in server.pem -noout
```

四 . 生成客户端证书 - 使用命令行直接生成

注意 : 配置中的DNS和IP,没有配置文件中的1.2

#生成Client端 Key文件

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

#生成签名请求 - 直接嵌入命令方式

```
openssl req -new -key ./client.key \
    -subj "/C=CN/ST=ZHEJIANG/L=HANGZHOU/O=WANMA/OU=COMPANY/CN=127.0.0.1" \
    -reqexts SAN \
    -config <(cat /etc/pki/tls/openssl.cnf <(printf "\n[SAN]\nsubjectAltName=DNS:*.org.example.com,DNS:*.abc.com,IP:127.0.0.1,IP:2.0.12.10")) \
    -out client.csr
```

#使用CA证书签名Client端证书

```
openssl x509 -req -in ./client.csr -CA ca.pem -CAkey ca.key -CAcreateserial \
    -extensions SAN \
    -extfile <(cat /etc/pki/tls/openssl.cnf <(printf "\n[SAN]\nsubjectAltName=DNS:*.org.example.com,DNS:*.abc.com,IP:127.0.0.1,IP:2.0.12.10")) \
    -days 3650 -sha256 -out client.pem
```

#使用这个命令可以查看生成的Server端证书是否支持多域名

```
openssl x509 -text -in client.pem -noout
```

[2019年6月\(2\)](#)

[2019年5月\(3\)](#)

[更多](#)

阅读排行榜

- [1. redis.conf配置详细解析\(177648\)](#)
- [2. JS ES6中export和import详解\(147211\)](#)
- [3. CentOS7安装iptables防火墙\(119484\)](#)
- [4. SpringMVC 基于注解的Controller详解\(80148\)](#)
- [5. CentOS7安装配置redis5集群\(37629\)](#)

评论排行榜

- [1. SpringMVC 基于注解的Controller详解\(6\)](#)
- [2. CentOS7安装配置redis5集群\(5\)](#)
- [3. redis.conf配置详细解析\(5\)](#)
- [4. CentOS7安装iptables防火墙\(5\)](#)
- [5. JS ES6中export和import详解\(4\)](#)

推荐排行榜

- [1. JS ES6中export和import详解\(25\)](#)
- [2. redis.conf配置详细解析\(8\)](#)
- [3. CentOS7安装iptables防火墙\(8\)](#)
- [4. SpringMVC 基于注解的Controller详解\(7\)](#)
- [5. Tomcat调优\(3\)](#)

最新评论

- [1. Re:部署EMQX集群](#)

可以不用ssl证书吗

--tomjoy

- [2. Re:CentOS7安装iptables防火墙](#)

@hudeyong_1 你就是不写文章还通通的那种家伙...

--黑色的小蚂蚁

- [3. Re:JS ES6中export和import详解](#)

怎么收藏啊

--TXJ0115

- [4. Re:CentOS7安装iptables防火墙](#)

666 谢谢博主 注释很清晰,好用

--三里林

- [5. Re:JS ES6中export和import详解](#)

强啊

--拾荒_encoded

Powered by:

[博客园](#)

Copyright © 2021 太清

Powered by .NET 6 on Kubernetes

五. 转成jks证书(Java相关的程序使用, 带密码, 安全一点)

#CA根证书生成, 相当于把 ca.pem > ca.jks

```
keytool -import -noprompt -file ca.pem -keystore ca.jks -storepass capassword
```



#Client证书生成, 相当于 client.key + client.pem > client.jks

#首先需要先转成p12格式的证书

```
openssl pkcs12 -export -in client.pem -inkey client.key -out client.p12 -passout pass:clientpassword
```

#把p12证书转成jks证书, 密码就不改了

```
keytool -importkeystore -srckeystore client.p12 -srcstoretype PKCS12 -destkeystore client.jks -srcstorepass clientpassword -deststorepass clientpassword
```



六. Java中调用jks证书例子(以paho.client.mqttv3.MqttClient为例子)



```
package test.mqtt;
```

```
import org.eclipse.paho.client.mqttv3.MqttClient;
import org.eclipse.paho.client.mqttv3.MqttConnectOptions;
import org.eclipse.paho.client.mqttv3.MqttException;
import org.eclipse.paho.client.mqttv3.internal.security.SSLSocketFactoryFactory;
import org.eclipse.paho.client.mqttv3.persist.MemoryPersistence;

import java.util.Properties;

/**
 * @author kreo
 * @description
 * @date 2020-6-23 23:15:16
 */
public class MqttConnection {

    private final static String broker = "ssl://2.0.12.10:8883";
    private final static String clientId = "LOCAL_JAVA_CLIENT";
    private final static MemoryPersistence persistence = new MemoryPersistence();

    private static MqttClient client;

    public static MqttClient getClient() {
        try {
            if (client == null) {
                client = new MqttClient(broker, clientId, persistence);

                // MQTT 连接选项
                MqttConnectOptions connOptions = new MqttConnectOptions();
                connOptions.setUserName("guest");
                connOptions.setPassword("123456".toCharArray());
                Properties sslProperties = new Properties();
                sslProperties.put(SSLSocketFactoryFactory.KEYSTORE, "/usr/var/certs/client.jks");
                sslProperties.put(SSLSocketFactoryFactory.KEYSTOREPWD, "client.wanmagroup.com");
                sslProperties.put(SSLSocketFactoryFactory.KEYSTORETYPE, "JKS");

                sslProperties.put(SSLSocketFactoryFactory.TRUSTSTORE, "/usr/var/certs/ca.jks");
                sslProperties.put(SSLSocketFactoryFactory.TRUSTSTOREPWD, "wanmagroup.com");
                sslProperties.put(SSLSocketFactoryFactory.TRUSTSTORETYPE, "JKS");
                sslProperties.put(SSLSocketFactoryFactory.CLIENTAUTH, true);

                connOptions.setSSLProperties(sslProperties);
                // 保留会话
                connOptions.setCleanSession(true);
            }
        } catch (MqttException e) {
            e.printStackTrace();
        }
        return client;
    }
}
```

```
// 设置回调
client.setCallback(new OnMessageCallback());

// 建立连接
System.out.println("尝试建立连接... Broker >> " + broker);
client.connect(connOptions);

System.out.println("建立连接成功");
}
} catch (MqttException me) {
    System.out.println("原因代码 " + me.getReasonCode());
    System.out.println("信息 " + me.getMessage());
    System.out.println("LOC " + me.getLocalizedMessage());
    System.out.println("原因 " + me.getCause());
    me.printStackTrace();
}
return client;
}

public static void close() {
    try {
        client.disconnect();
        System.out.println("断开连接");
        client.close();
        System.out.println("连接关闭");
    } catch (MqttException me) {
        System.out.println("原因代码 " + me.getReasonCode());
        System.out.println("信息 " + me.getMessage());
        System.out.println("LOC " + me.getLocalizedMessage());
        System.out.println("原因 " + me.getCause());
        me.printStackTrace();
    }
}
```

-sha256 -days 3650

分类: [Linux](#)

好文要顶

关注我

收藏该文

太清

关注 - 0

粉丝 - 58

[+加关注](#)

« 上一篇: [Redis迁移备份工具redis-shake使用](#)
» 下一篇: [部署EMQX集群](#)

posted on 2020-06-28 17:56 [太清](#) 阅读(1592) 评论(0) [编辑](#) [收藏](#) [举报](#)

0

推荐

0

反对

[刷新评论](#) [刷新页面](#) [返回顶部](#)

登录后才能查看或发表评论, 立即 [登录](#) 或者 [逛逛](#) [博客园首页](#)

穿山甲

App开发者高效成长

增长变现闭环

收入提升 **28%**

立即注册

增长变现闭环
收入提升 28%

立即注册

编辑推荐：

- [带团队后的日常思考（五）](#)
- [聊聊我在微软外服的工作经历及一些个人见解](#)
- [死磕 NIO — Reactor 模式就一定意味着高性能吗？](#)
- [消息队列那么多，为什么建议深入了解下RabbitMQ？](#)
- [技术管理进阶——管人还是管事？](#)

最新新闻：

- [现在的年轻人，已经不愿意为钻石缴纳“智商税”了 \(2021-10-26 10:11 \)](#)
 - [遭苹果“虐哭”，Snap还能收割Z世代吗？ \(2021-10-26 10:03 \)](#)
 - [微软称俄罗斯黑客自5月以来至少入侵了14家IT供应链公司 \(2021-10-26 09:55 \)](#)
 - [新东方已“躺平” 教培百万从业者都去哪了？ \(2021-10-26 09:47 \)](#)
 - [Redmi智能手环Pro将于10月28日上市 官方渲染图泄露 \(2021-10-26 09:46 \)](#)
- » [更多新闻...](#)