CFCA EV/OV SSL 证书域名验证指南

2020 年 2 月

目录

1 引言

申请 CFCA EV/OV SSL 证书时，除需要验证申请机构身份信息外，也需要验证域名所有权。目前 CFCA 支持邮箱验证、DNS 验证、文件验证三种域名验证方式，本文介绍上述三种验证方法及区别，申请者可根据自身实际情况选择，并在申请表中标注以何种方式进行验证。

2 验证方式

2.1 DNS 验证

下文介绍 SSL 证书 DNS 验证在各主流域名注册商下的域名解析方法，仅供参考，具体以各注册商实际为准。CFCA 会将 DNS 记录值发送到证书申请经办人邮箱，请留意查收。

注意事项：域名验证记录值有效期为 15 天，自生成时开始计算。请务必在 15 天内完成配置，如超时未进行配置或验证未通过，请联系 CFCA 工作人员，重新申请域名验证记录值并配置。

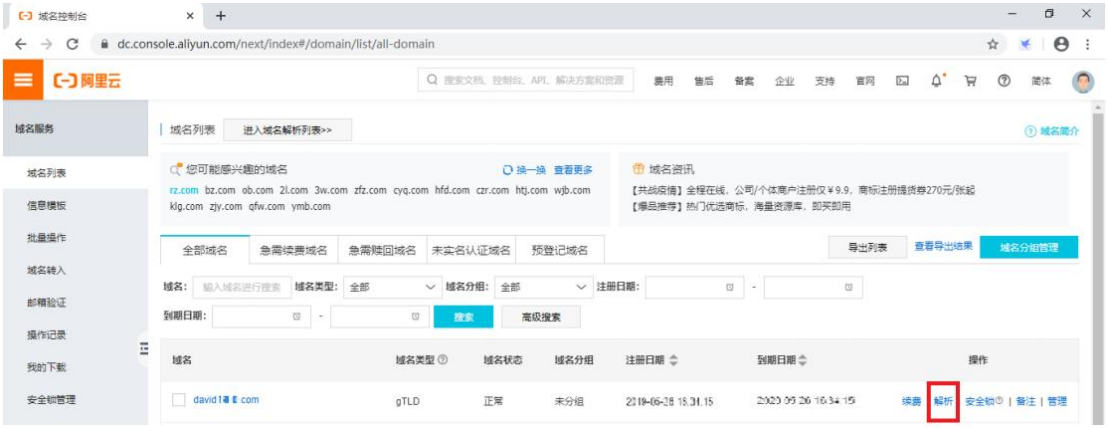
2.1.1 DNS 验证注意事项

当申请的域名不为主域名（如：domain.com），为二级域名时（如：www.domain.com），主机记录值需更新为：“_cfcachallenge.host.二级域名前缀”，即：

_cfcachallenge.host.www

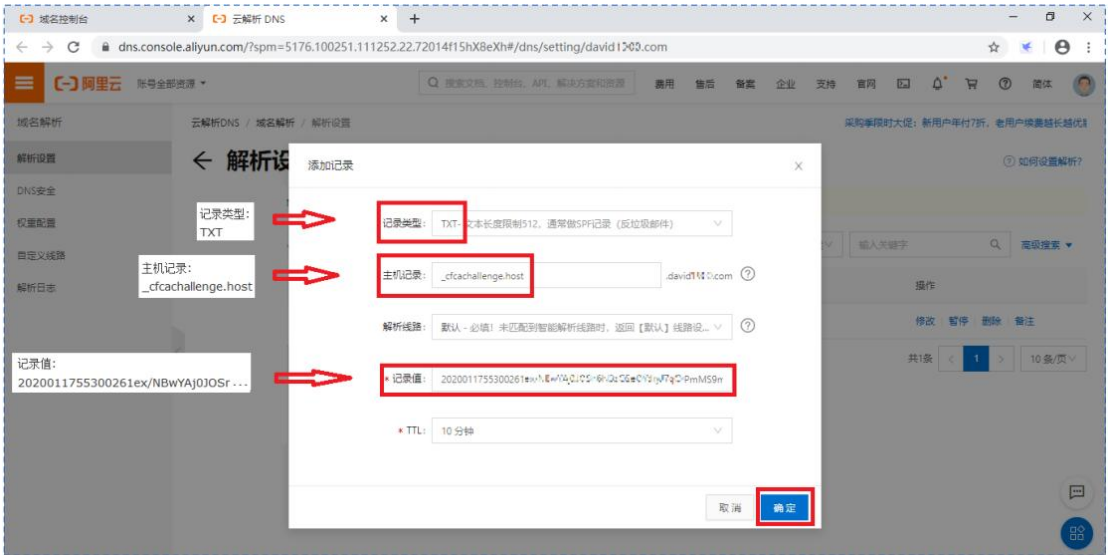
2.1.2 阿里云操作示例

（1）登陆域名管理控制台，查看【域名列表】，单击操作栏的【解析】，进入域名解析页面：



（2）单击【添加记录】

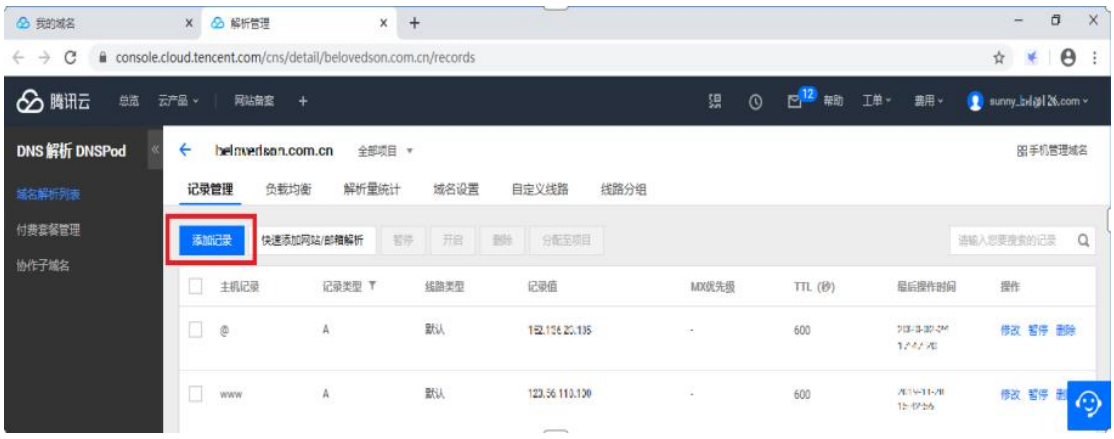
（3）添加记录类型为 TXT 的 DNS 记录，单击【确定】完成添加



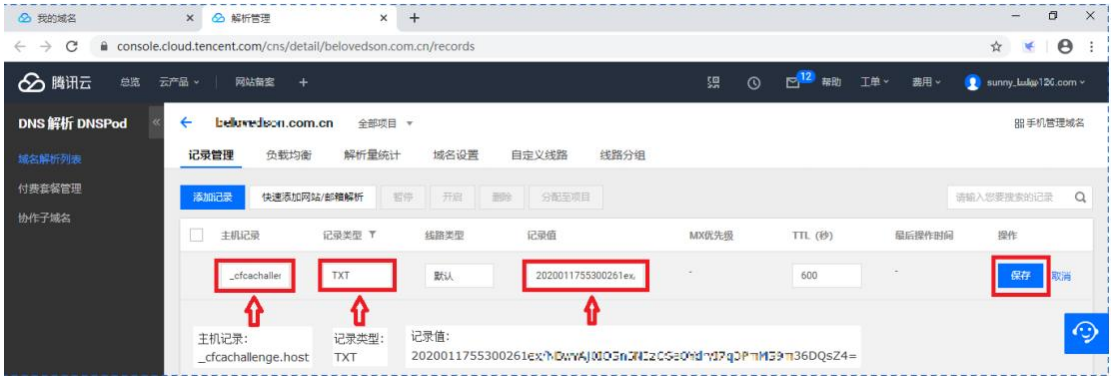
2.1.3 腾讯云操作示例

（1）登陆域名管理控制台，查看【我的域名】，单击操作栏的【解析】，进入域名解析页面：

（2）单击【添加记录】



（3）添加记录类型为 TXT 的 DNS 记录，单击【保存】完成添加



2.1.4 新网操作示例

将记录类型选择为 **TXT 纪录**，在主机记录中输入邮件中提供的**主机记录**字段信息，不包括网址信息，在记录值中输入邮件中的**记录值**字段信息，点击添加

2.2 文件验证

选择文件方式验证后，CFCA 会发送记录值至证书申请经办人邮箱，操作步骤如下：

注意事项：域名验证记录值有效期为 15 天，自生成时开始计算。请务必在 15 天内完成配置，如超时未进行配置或验证未通过，请联系 CFCA 工作人员，重新申请域名验证记录值并配置。

1、 创建文件：

本地创建名称为“cfcafileauth.txt”的 TXT 文件，将邮件中“文件内容”字段，复制到上述文件，保存（请不要增加空格等其他多余信息）；

2、创建目录：

在站点根目录下创建/.well-known/pki-validation 子目录，然后将 cfcafileauth.txt 文件上传至该目录；

注：

（1）第一层目录是带点的隐藏目录，Windows 下命令为：

mkdir .well-known

（2）如果您的站点由于某种原因无法创建隐藏目录，请选择 DNS 验证方式

3、域名解析至服务器

4、配置检测：

配置好之后，可通过浏览器访问地址，如正常输出配置的记录值，则表示配置成功。

（1）HTTP 配置检测： http://**您的域名**/.well-known/pki-validation/cfcafileauth.txt

（2）HTTPS 配置检测：https://**您的域名**/.well-known/pki-validation/cfcafileauth.txt

若申请*.domain.com 类型的通配符证书时，访问检测地址为：

（1）HTTP 配置检测：http://domain.com/.well-known/pki-validation/cfcafileauth.txt

（2）HTTPS 配置检测：https://domain.com/.well-known/pki-validation/cfcafileauth.txt

注意事项：

（1）HTTP、HTTPS 任选其一验证通过即可，HTTP 方式默认使用 80 端口，HTTPS 方式默认使用 443 端口，若使用其他端口请告知 CFCA 工作人员；

（2）文件验证需要直接响应 200 状态码和文件内容，不支持任何形式的跳转。

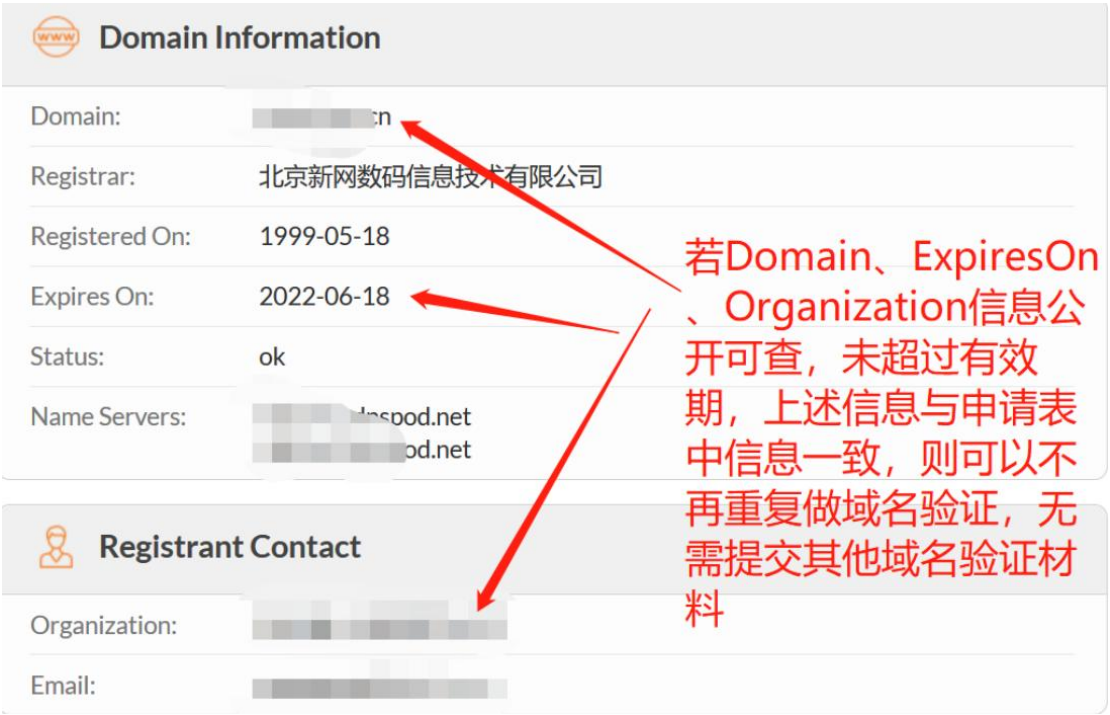
2.3 邮箱验证

邮箱验证，即通过 Whois 查询域名注册时预留的邮箱，CFCA 向该注册邮箱发送 SSL 证书申请确认信息，若 CFCA 受到确认邮件，

则可证明该邮箱被合法持有人控制，验证通过后可为其颁发服务器证书。

采用邮箱验证方式时，请确保 whois 隐私保护关闭， whois 中管理员邮箱可正常回复邮件（若开启隐私保护，我方无法查询明确的管理员邮箱，则默认向 admin 、administrator、webmaster、hostmaster、postmaster 开头 的域名邮箱发送验证邮件，例如 admin@domain.com 形式，**请 确认上述邮箱可正常回复邮件后，再选择此种验证方式。**

Whois 邮箱查询地址：https://www.whois.com/whois/



3 常见验证不通过错误情况

（1）DNS 及文件验证中记录值内容不正确；

（2）已配置但检测不到，确认是否有网名白名单限制；

（3）文件验证过程中，配置的原始地址发生了跳转；

（4）验证值内容已经过期；

（5）邮箱验证时，注册邮箱发生变更，或 5 个默认邮箱不可用，请确认绑定的管理员邮箱，确保上述邮箱可正常接受及回复邮件。