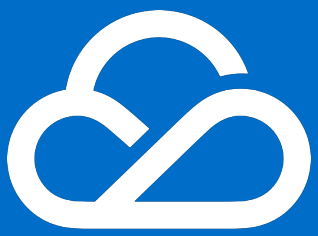
SSL证书

操作指南

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

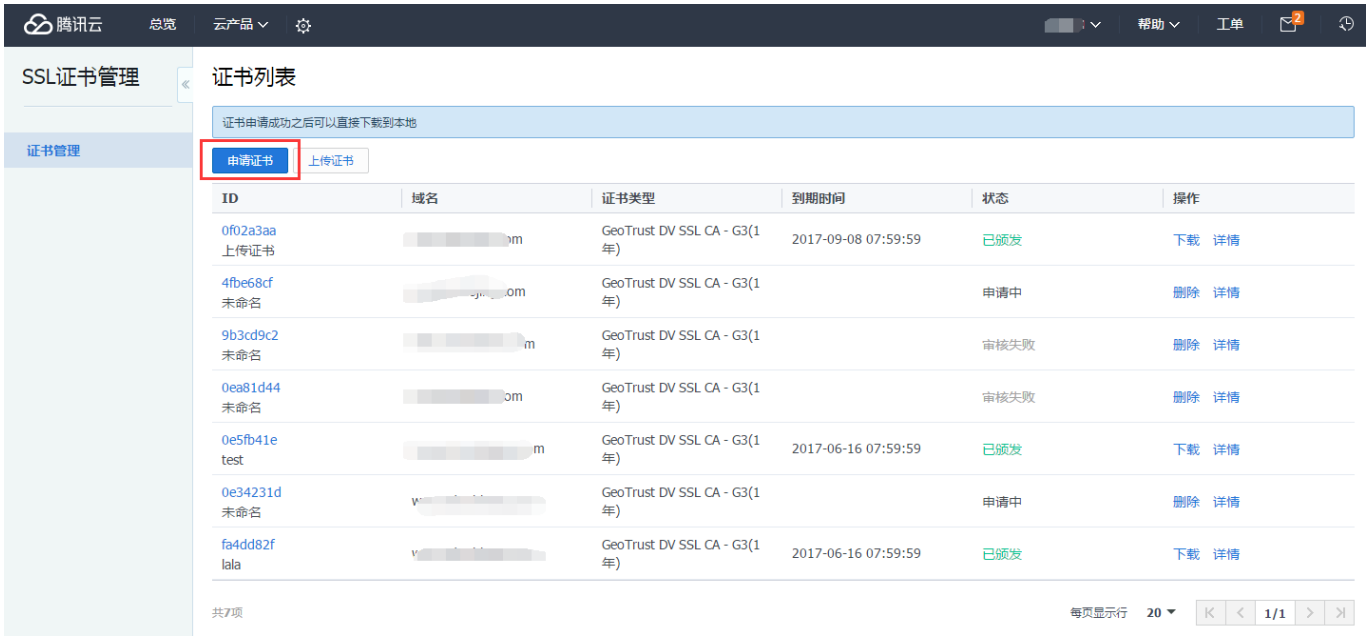
域名型证书申请流程

申请域名型（DV）SSL证书

1. 申请入口

进入SSL证书管理控制台

点击【申请证书】



查看申请域名型证书型号，点击【确定】

2. 填写申请

填写申请域名，注意不支持一级域名申请（例如qcloud.com），请填写例如www.qcloud.com，demo.test.qlcoud.com形式二级、三级等域名。

3.1 手动DNS验证方式

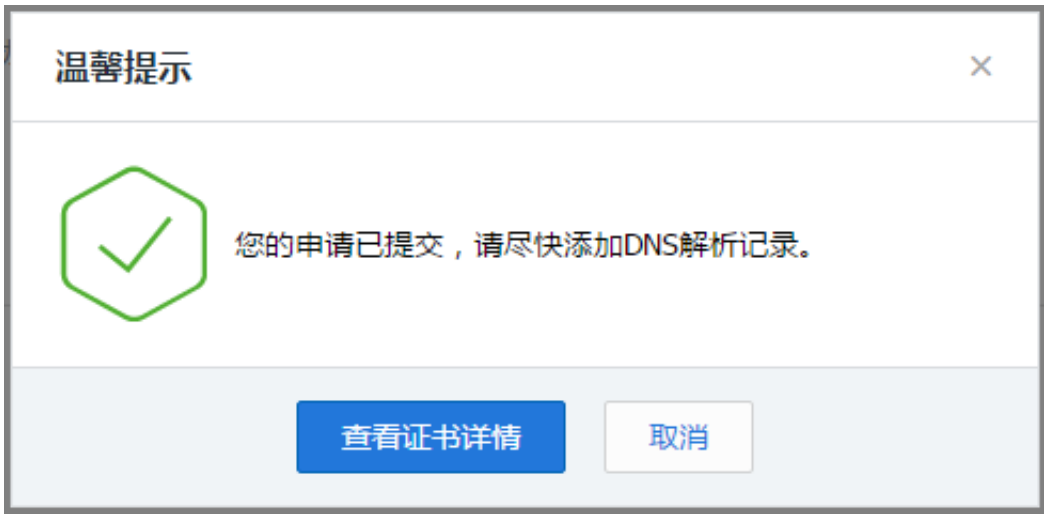
证书默认支持收到DNS验证，验证方法可查看详情。

3.2 选择自动DNS验证方式

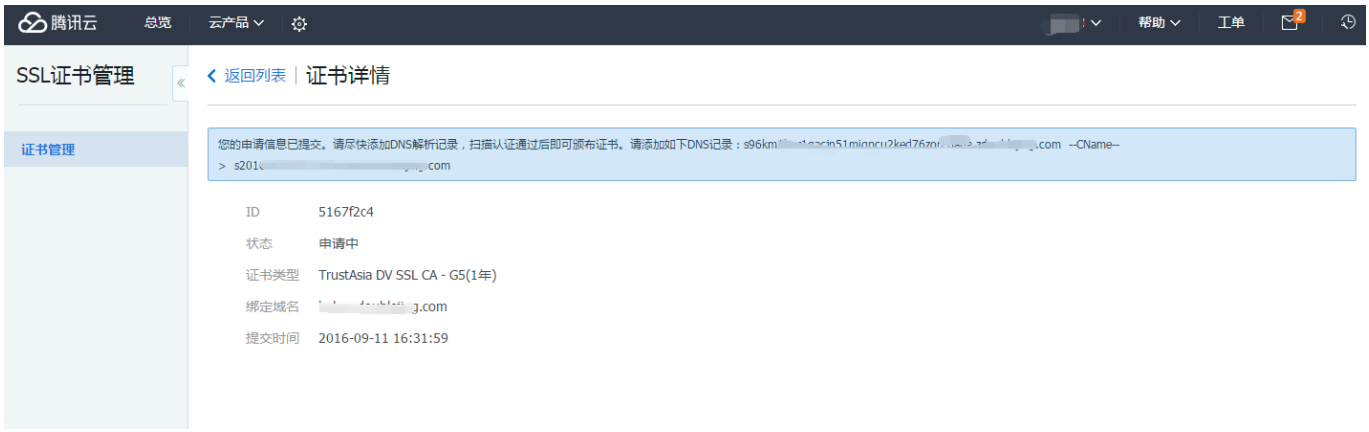
如果所申请域名成功添加云解析平台，可以支持自动DNS验证，验证方法可查看详情。

4.1 提交申请后验证身份

提交申请成功后弹窗提示如下，需要前往【证书详情页】获取CName记录添加解析：



获取CName记录如Tips中显示，需要尽快成功添加解析，方可通过CA机构审核：



4.2 提交申请失败

如遇到下图所示弹窗，是提交域名未通过CA机构安全审核，具体原因参考安全审核失败原因。

域名验证指引

申请域名型证书，可以通过以下方式验证域名的所有权：

1. 手动DNS验证

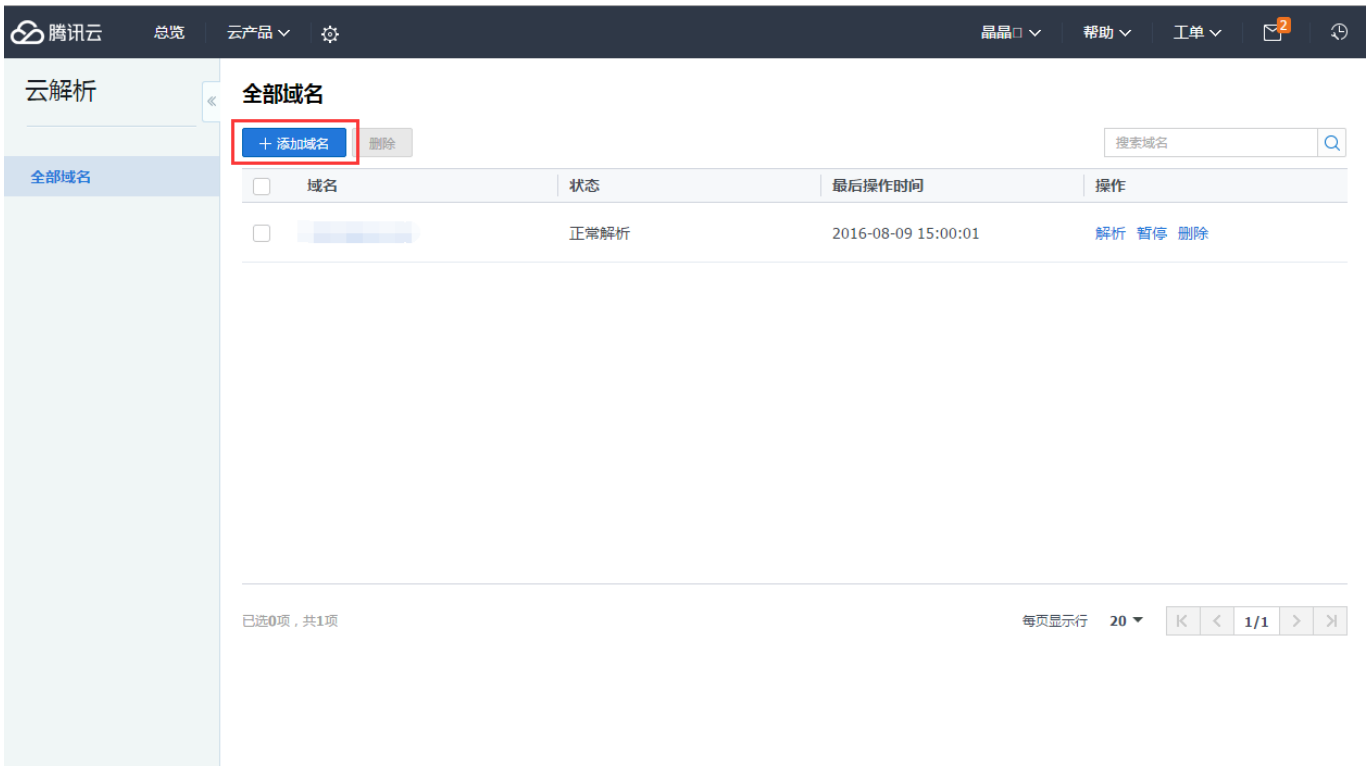
通过解析指定的DNS记录验证您的域名所有权，指定的解析格式如下：

主机记录 –> CName记录类型 –> 记录值

例如为申请证书的域名 www.domain.com
添加一条记录类型为CNAME的DNS记录：sr5jtl1xxxxxxxmygdps.domain.com –> CNAME –> s2015xxxxxxxx.domain.com，以云解析平台为例说明如何进行操作：

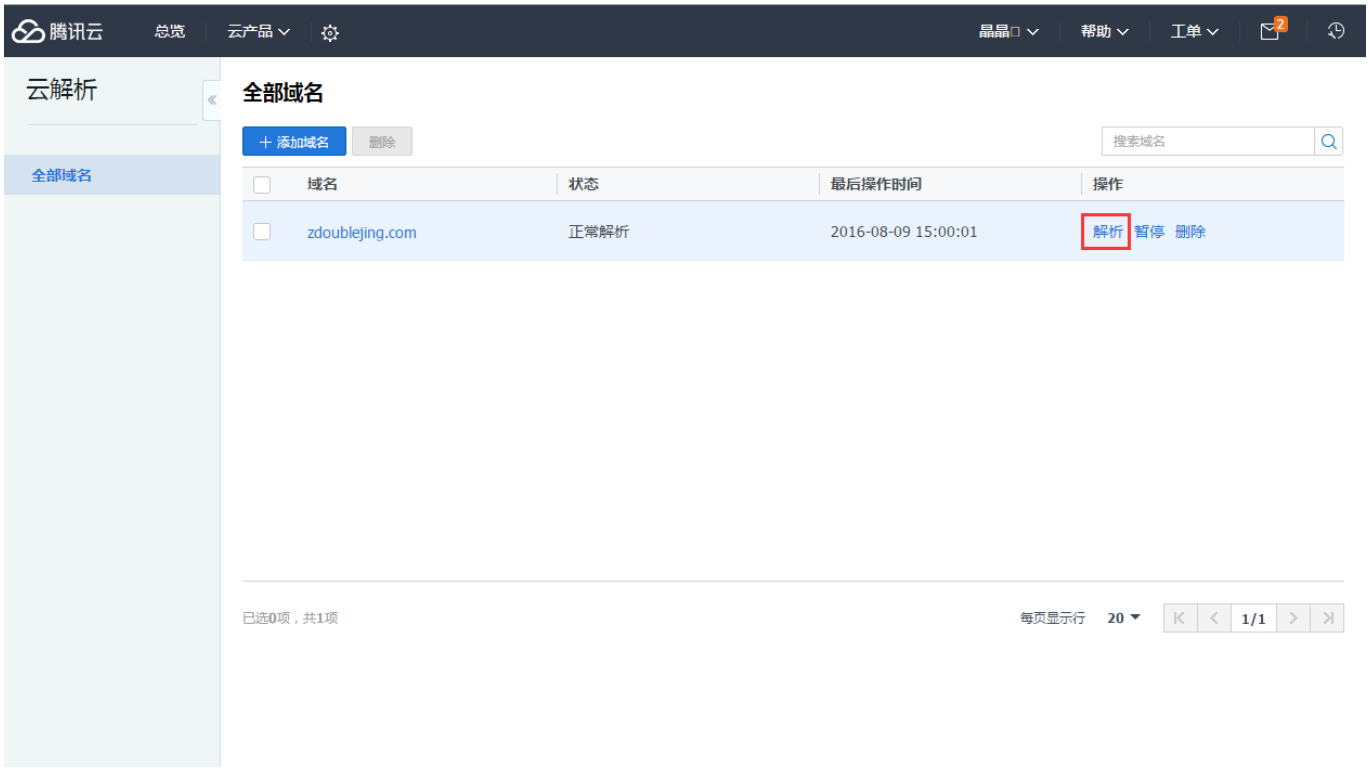
1.1 添加域名

点击【添加域名】，输入您要解析域名的主域名domain.com，并点【确定】

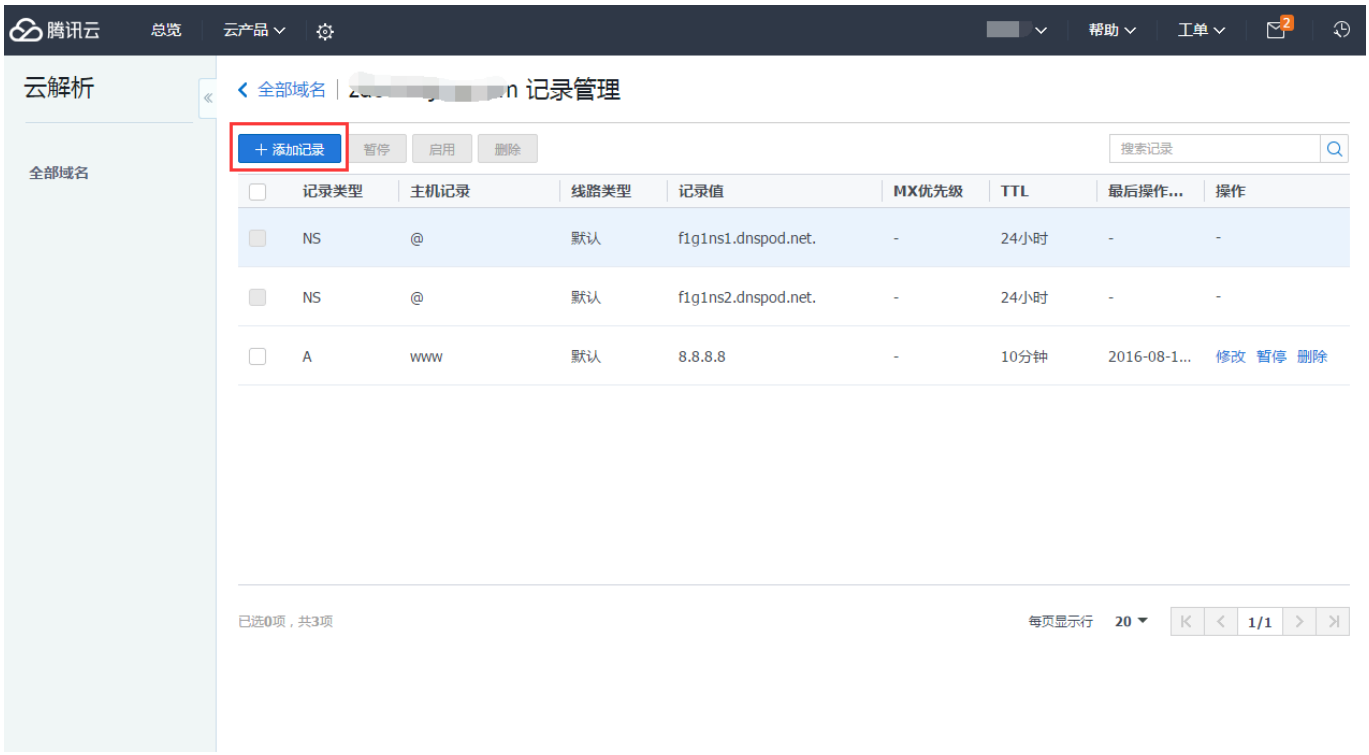


1.2 添加解析记录

点击刚添加的域名【解析】



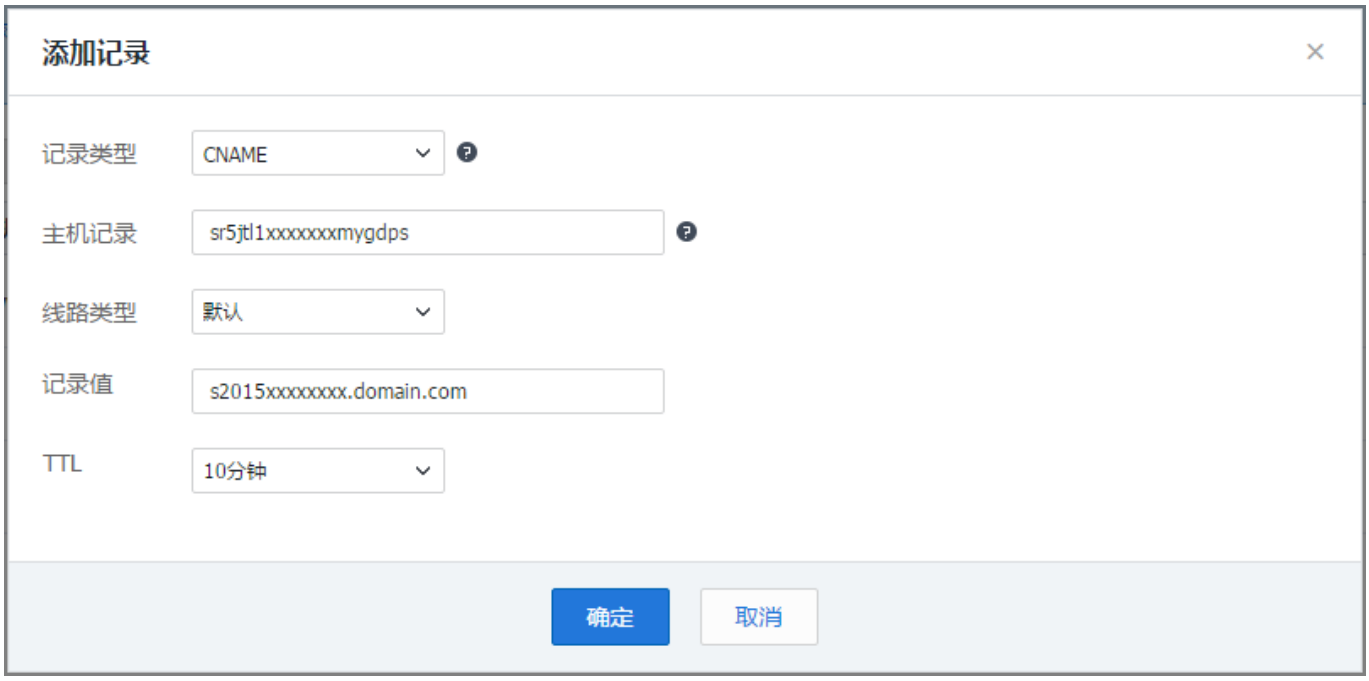
点击【添加记录】



1.3 完成指定的CNAME记录添加

CNAME记录即将域名指向另一个域名，再由另一个域名提供ip地址：

- 记录类型选择为CNAME
- 主机记录处填子域名，比如需要添加sr5jtl1xxxxxxxmygdps.domain.com的解析，只需要在主机记录处填写sr5jtl1xxxxxxxmygdps即可，不需要填写主域名domain.com
- 线路类型选择默认
- 记录值为
  CNAME指向的域名，只可以填写域名，此处为s2015xxxxxxxx.domain.com，注意记录值须完整填写
- TTL选择默认值10分钟即可



解析添加成功后如下：

sr5jtl1xxxxxxxmygdps.domain.com
的指向系统会定时检查，若能检测到并且与指定的值匹配，即可完成域名所有权验证。

2. 自动DNS验证

注：仅限使用云解析的域名

如果申请证书的域名已经在云解析平台进行解析，可以选择自动验证。

系统为将为该域名自动添加指定的DNS解析记录，记录被检测匹配成功，完成域名所有权验证后，该记录将自动清除。

域名身份如何自动验证

1. 自动DNS验证原理

提交证书申请后，CA机构会指定添加一条CNAME解析记录来验证域名的所有权，如果该域名在腾讯云云解析平台进行解析，则可以立即自动添加指定的CNAME解析记录，等待CA机构的定时扫描审核，以最快最便捷的方式完成证书申请。

2. 云解析添加域名

如果您的域名不在云解析平台进行解析，可以参考如下流程将域名加入云解析：
添加域名到云解析

3. 修改DNS服务器

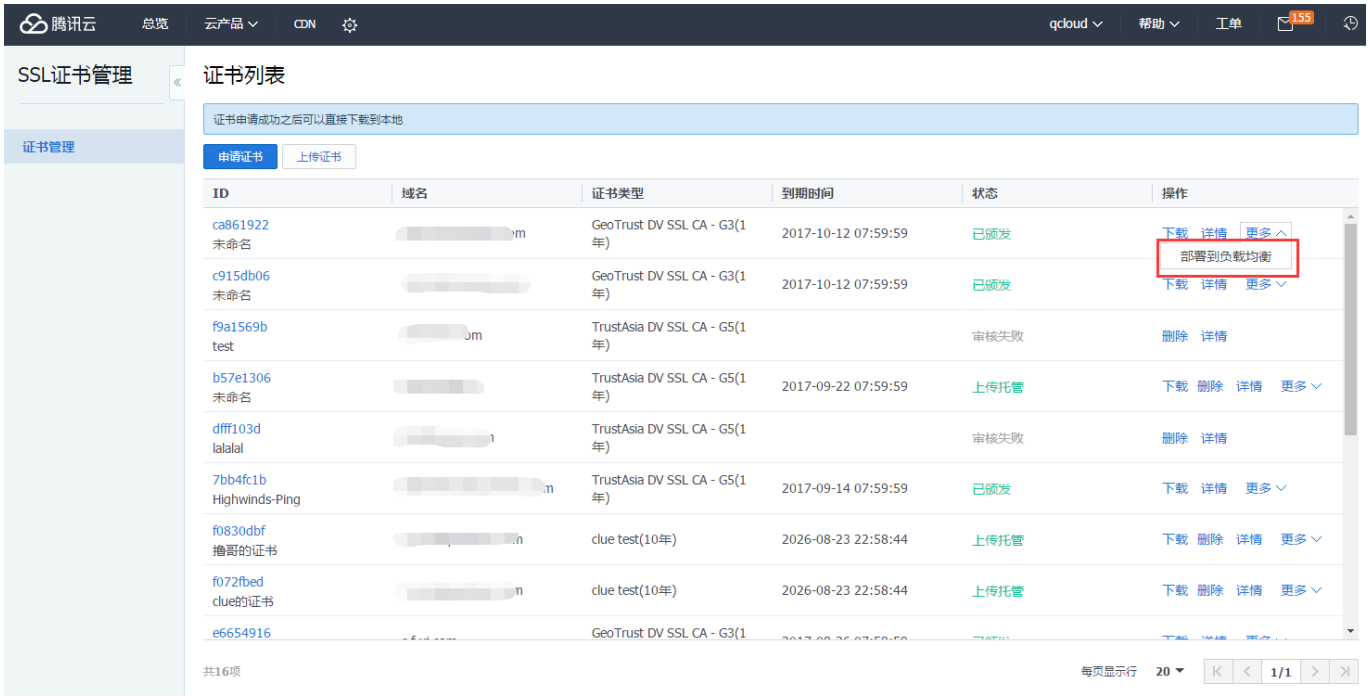
切记，完成添加域名后，需要修改域名的DNS服务器为腾讯云指定的DNS地址，解析方可生效。
参考 修改域名DNS指引

部署证书到负载均衡指引

SSL证书支持部署到负载均衡，步骤如下所示：

1. 选择证书

首先成功申请获取证书（参考[如何免费申请域名型证书]
），或者选择上传的证书，展开【更多】操作，选择【部署到负载均衡】。

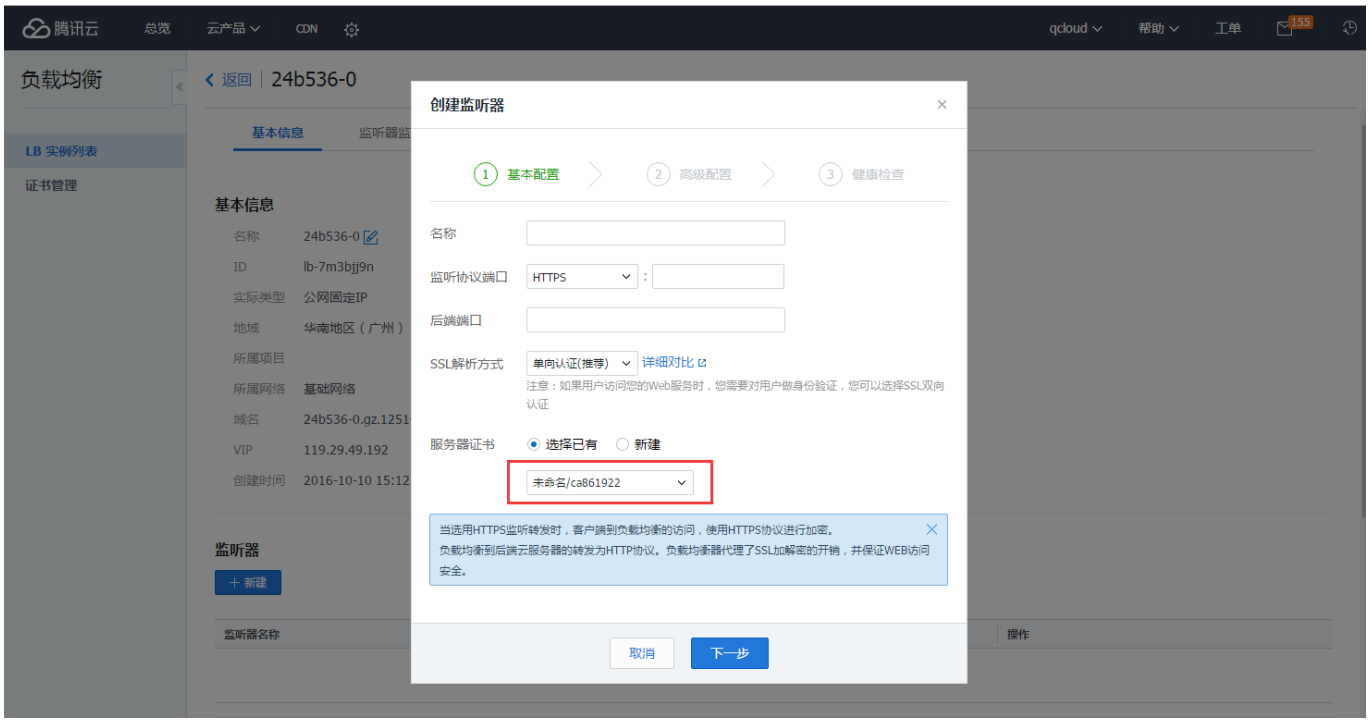


2. 选择LB实例

根据项目和地区筛选LB实例（目前不支持华南地区-深圳金融），且只能选择一个实例。

3. 创建监听器

跳转到负载均衡控制台，打开创建监听器弹窗，并且监听协议端口已切换到Https，服务器证书为已选中的证书，然后完成剩余的基本配置。



4. 继续完成配置

继续完成创建监听器的其他配置，即可实现负载均衡的Https。

私钥密码指引

私钥密码是申请证书时的选填项，如图所示：

注意事项：

1、如果填写了私钥密码，请您牢记该密码，该密码不支持找回和修改；

2、该密码在证书下载完成进行解压时需要输入；

3、在您的服务器上进行证书导入、导出、安装等操作时可能会需要输入；

4、如果私钥密码不慎遗忘，请工单联系客服删除该证书，然后重新申请该域名证书。

证书安装指引

下载得到的 www.domain.com.zip 文件，解压获得3个文件夹，分别是Apache、IIS、Nginx 服务器的证书文件，

下面提供了3类服务器证书安装方法的示例：

1. Apache 2.x证书部署

1.1 获取证书

Apache文件夹内获得证书文件 1_root_bundle.crt，2_www.domain.com_cert.crt 和私钥文件 3_www.domain.com.key,

1_root_bundle.crt 文件包括一段证书代码 “-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，

2_www.domain.com_cert.crt 文件包括一段证书代码 “-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，

3_www.domain.com.key 文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

1.2 证书安装

编辑Apache根目录下 conf/httpd.conf 文件，

找到 #LoadModule ssl_module modules/mod_ssl.so 和 #Include conf/extra/httpd-ssl.conf，去掉前面的#号注释；

编辑Apache根目录下 conf/extra/httpd-ssl.conf 文件，修改如下内容：

```
<VirtualHost www.domain.com:443>
    DocumentRoot "/var/www/html"
    ServerName www.domain.com
    SSLEngine on
    SSLCertificateFile /usr/local/apache/conf/2_www.domain.com_cert.crt
    SSLCertificateKeyFile /usr/local/apache/conf/3_www.domain.com.key
    SSLCertificateChainFile /usr/local/apache/conf/1_root_bundle.crt
</VirtualHost>
```

配置完成后，重新启动 Apache 就可以使用https://www.domain.com来访问了。

注：

配置文件参数	说明
SSLEngine on	启用SSL功能
SSLCertificateFile	证书文件
SSLCertificateKeyFile	私钥文件
SSLCertificateChainFile	证书链文件

2. Nginx证书部署

2.1 获取证书

Nginx文件夹内获得SSL证书文件 1_www.domain.com_bundle.crt 和私钥文件 2_www.domain.com.key,
1_www.domain.com_bundle.crt 文件包括两段证书代码 “-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，
2_www.domain.com.key 文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

2.2 证书安装

将域名 www.domain.com 的证书文件1_www.domain.com_bundle.crt
、私钥文件2_www.domain.com.key保存到同一个目录，例如/usr/local/nginx/conf目录下。
更新Nginx根目录下 conf/nginx.conf 文件如下：

```
server {
        listen 443;
        server_name www.domain.com; #□□□□□□□□□□
        ssl on;
        ssl_certificate 1_www.domain.com_bundle.crt;
        ssl_certificate_key 2_www.domain.com.key;
        ssl_session_timeout 5m;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #□□□□□□□□□
        ssl_ciphers
```

```
ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;#□□□□□□□□□
        ssl_prefer_server_ciphers on;
        location / {
            root   html; #□□□□
            index  index.html index.htm;
        }
    }
```

配置完成后，先用bin/nginx –t来测试下配置是否有误，正确无误的话，重启nginx。就可以使https://www.domain.com 来访问了。

注：

配置文件参数	说明
listen 443	SSL访问端口号为443
ssl on	启用SSL功能
ssl_certificate	证书文件
ssl_certificate_key	私钥文件
ssl_protocols	使用的协议
ssl_ciphers	配置加密套件，写法遵循openssl标准

2.3 使用全站加密，http自动跳转https（可选）

对于用户不知道网站可以进行https访问的情况下，让服务器自动把http的请求重定向到https。
在服务器这边的话配置的话，可以在页面里加js脚本，也可以在后端程序里写重定向，当然也可以在web服务器来实现跳转。Nginx是支持rewrite的（只要在编译的时候没有去掉pcre）
在http的server里增加rewrite ^(.*) https://$host$1 permanent;
这样就可以实现80进来的请求，重定向为https了。

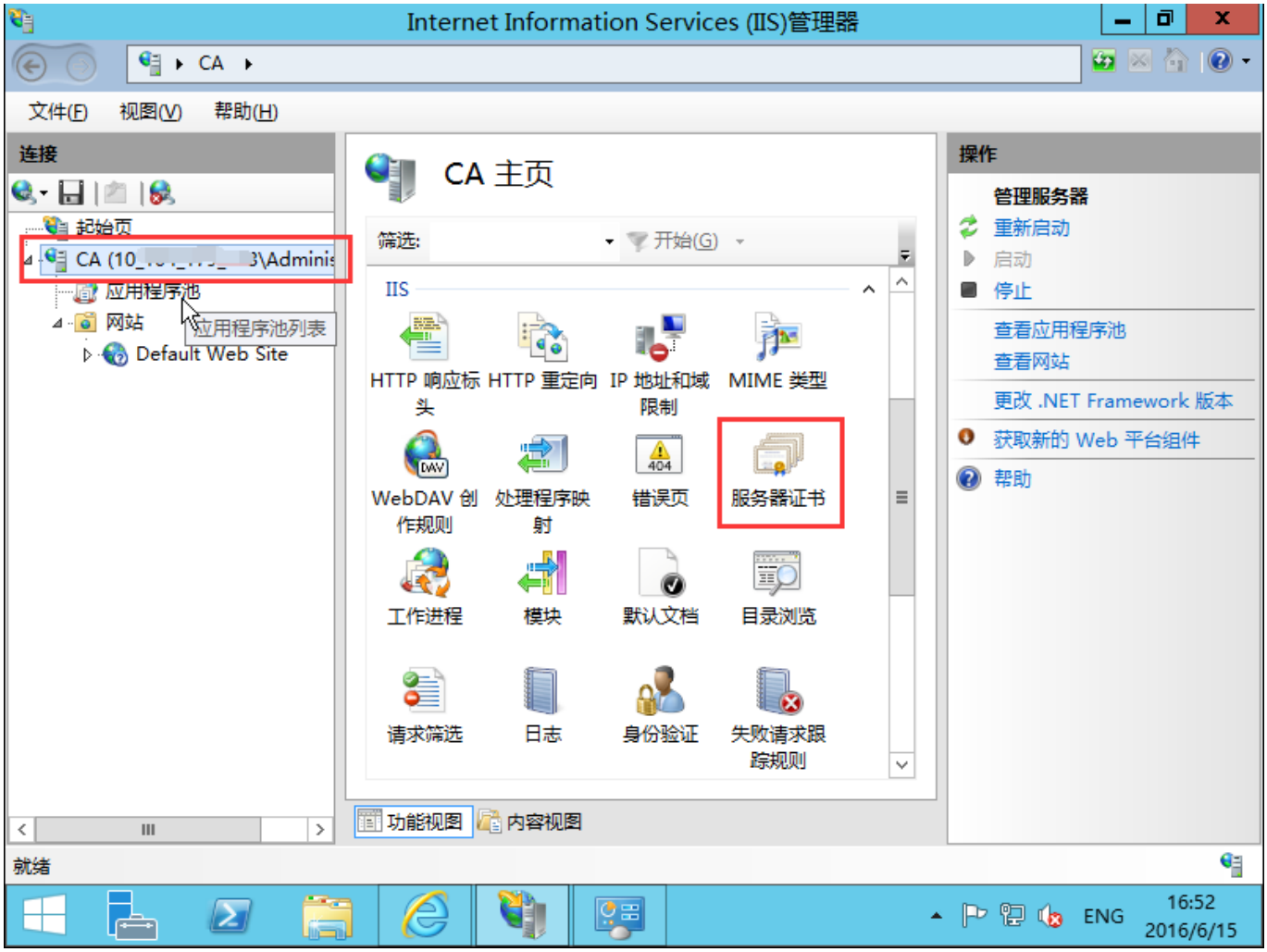
3. IIS 证书部署

3.1 获取证书

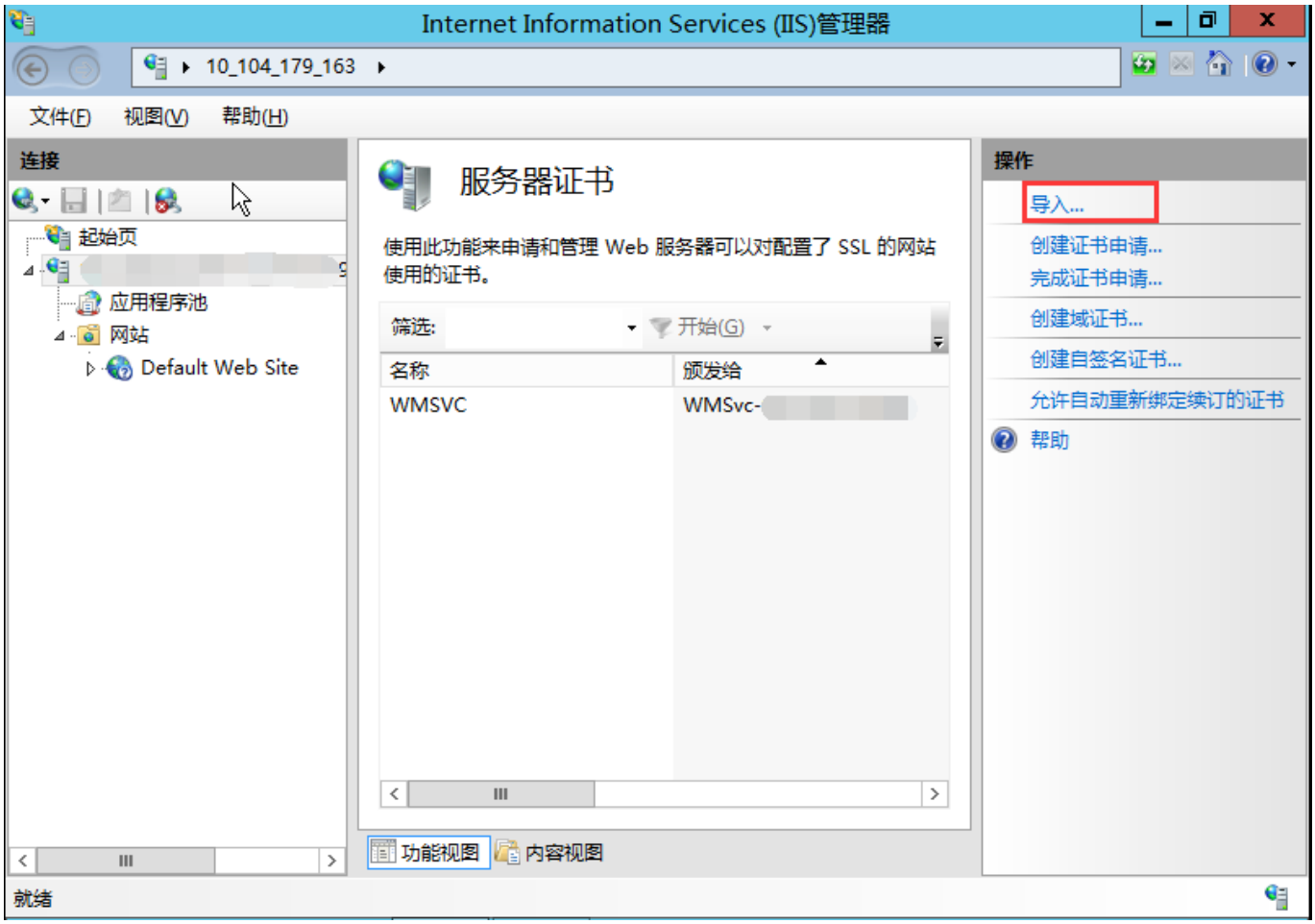
IIS文件夹内获得SSL证书文件 www.domain.com.pfx。

3.2 证书安装

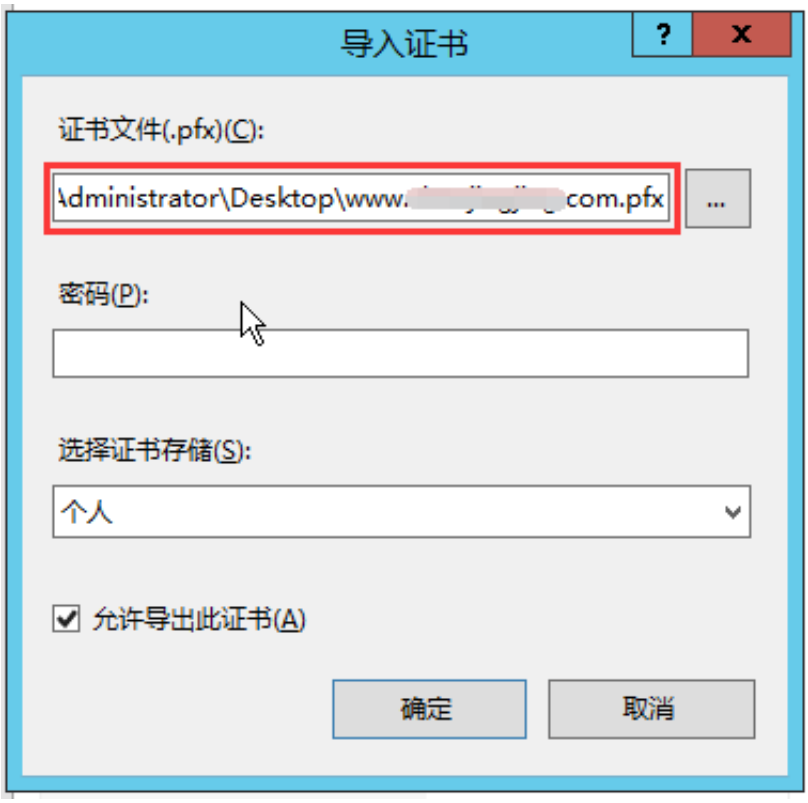
1、打开IIS服务管理器，点击计算机名称，双击‘服务器证书’



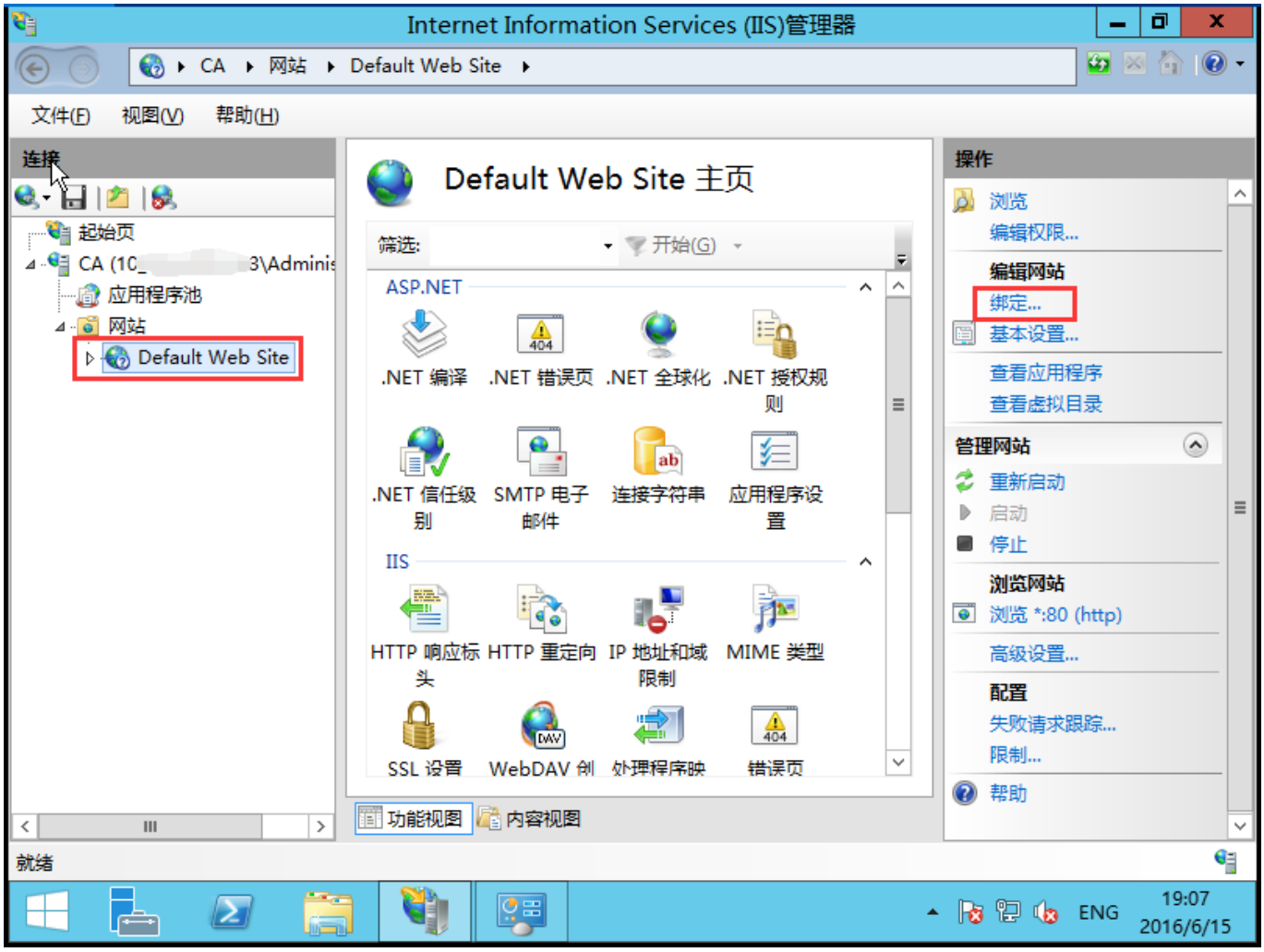
2、双击打开服务器证书后，点击右则的导入



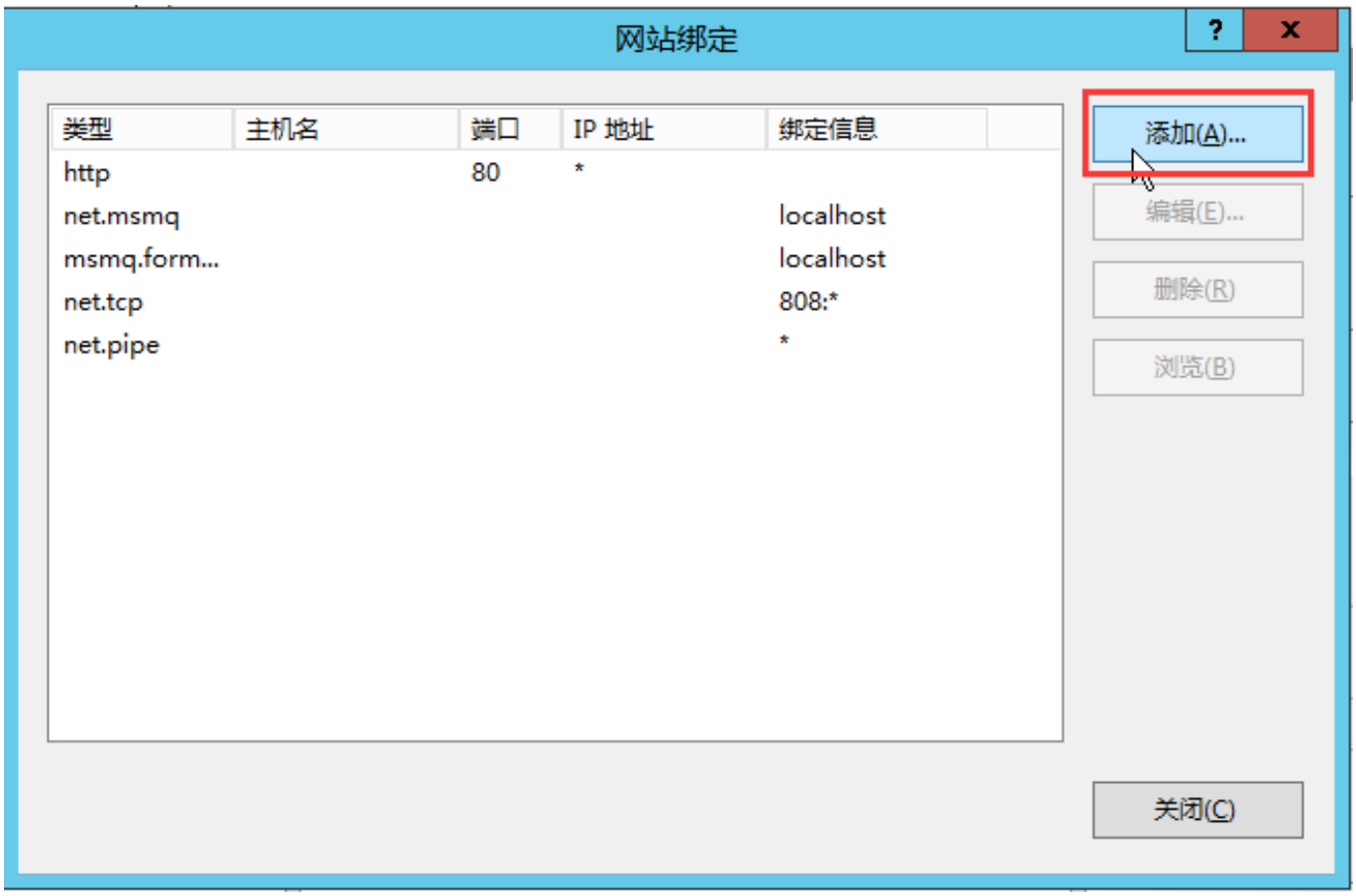
3、选择证书文件，如果输入申请证书时有填写私钥密码需要输入密码，点击确定。[参考私钥密码指引]



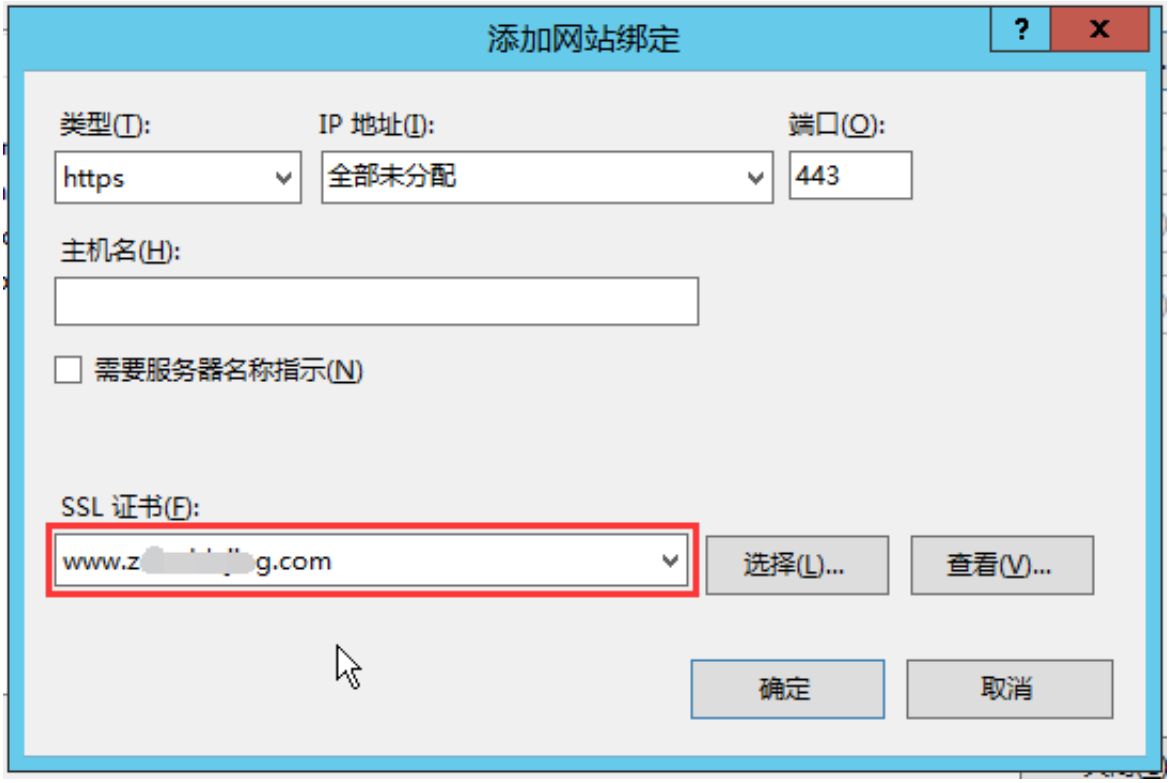
4、点击网站下的站点名称，点击右则的绑定



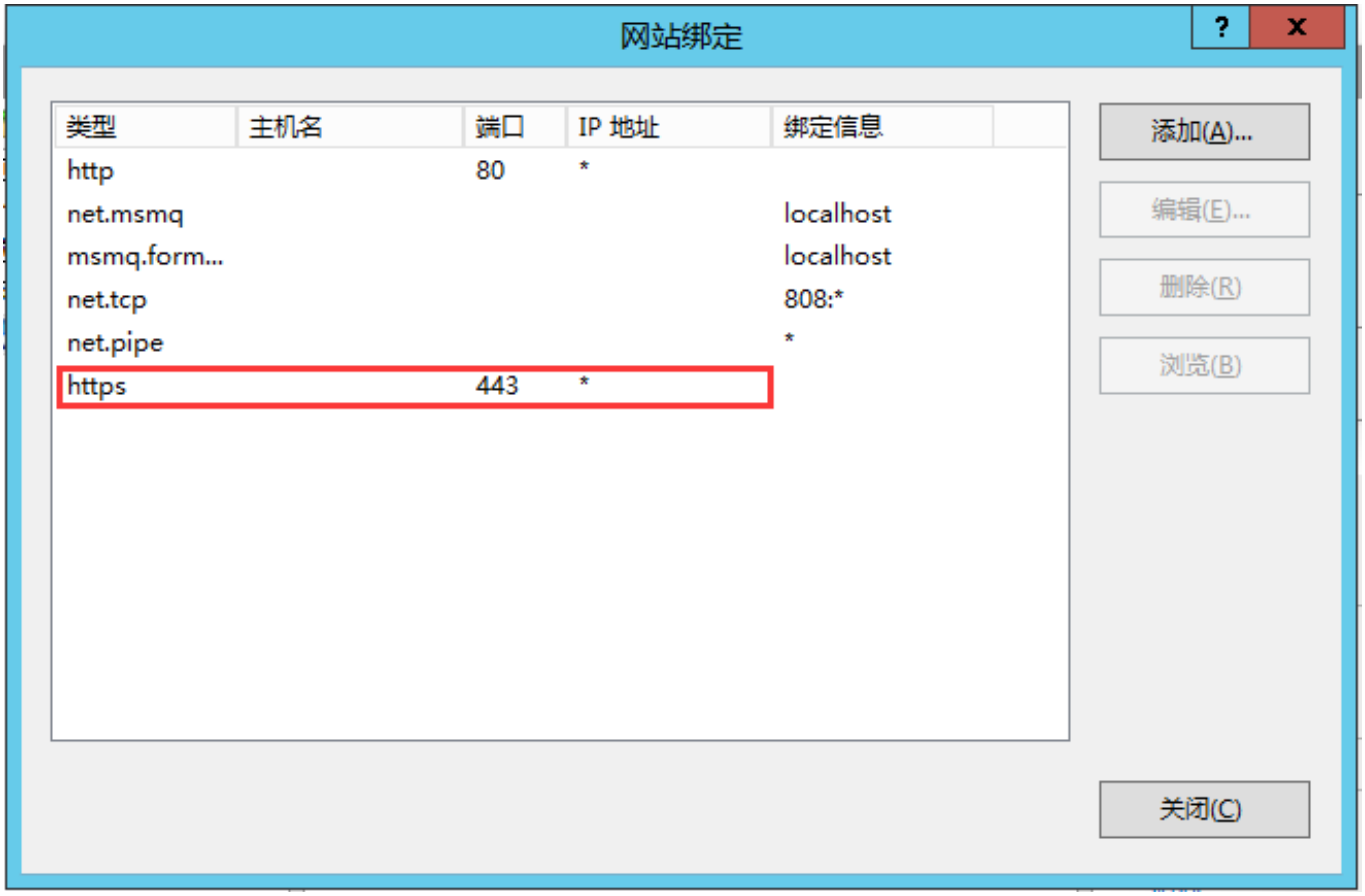
5、打开网站绑定界面后，点击添加



6、添加网站绑定内容：选择类型为https，端口443和指定对应的SSL证书，点击确定



7、添加完成后，网站绑定界面将会看到刚刚添加的内容



域名型证书吊销指引

1. 提交工单

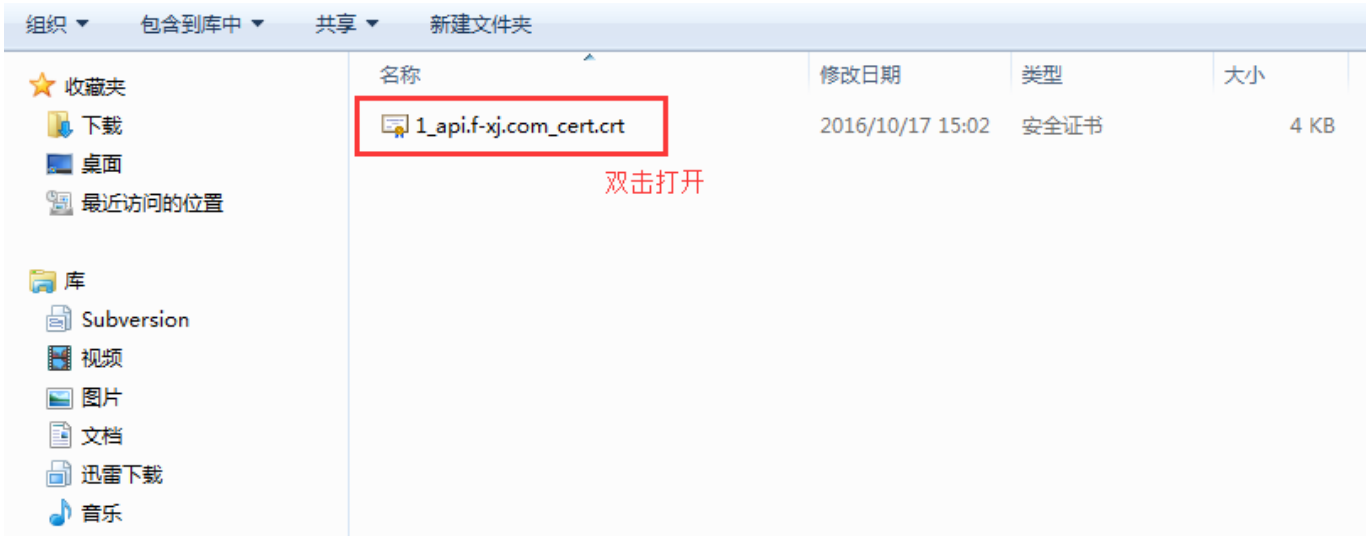
提交工单 寻求腾讯云工程师协助您完成证书吊销。

2. 提供相关信息

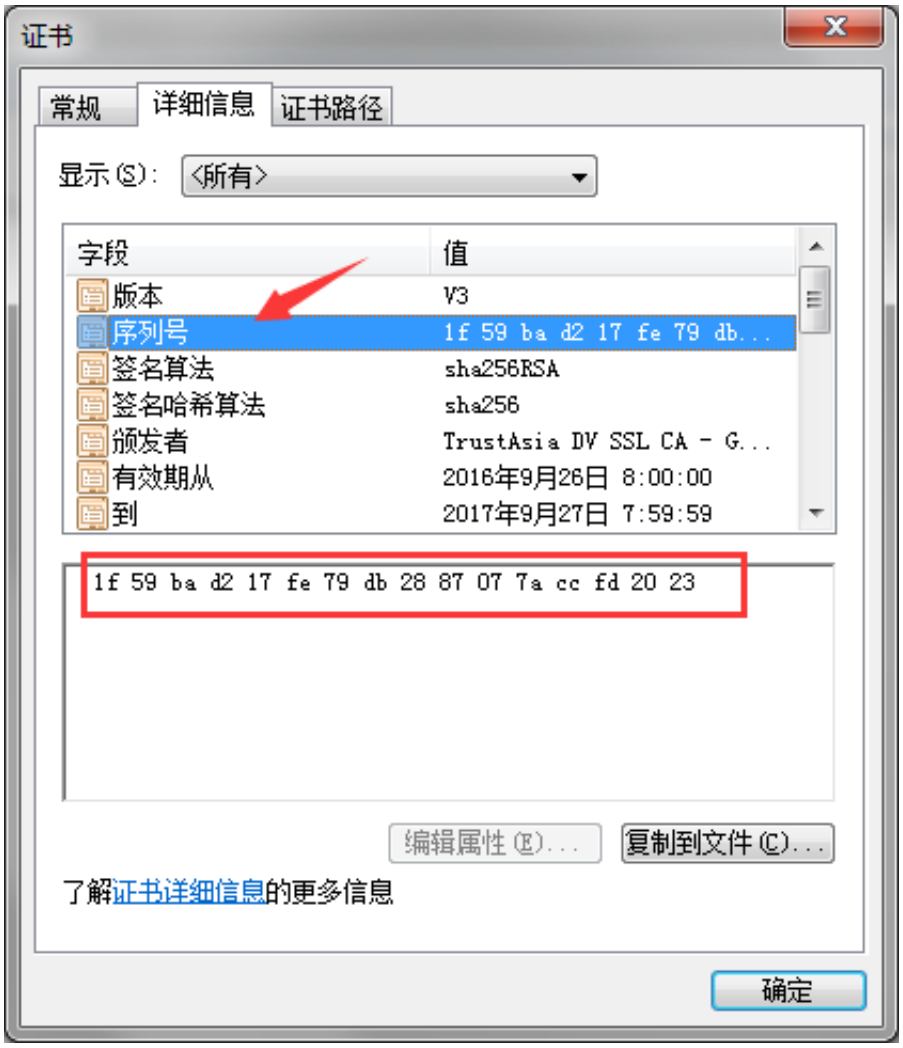
提供证书信息：包括证书ID、域名、证书序列号。

3. 证书序列号获取方法

3.1 下载证书到本地，双击打开



3.2 切换到【详细信息】，获取证书序列号



4. 重新验证域名身份

腾讯云工程师会要求您完相应的DNS验证或者文件验证，完成身份验证后，CA机构方可继续完成证书吊销流程。

苹果ATS特性服务器配置指南

配置指南：

1. 需要配置符合PFS规范的加密套餐，目前推荐配置：
   ECDHE-RSA-AES128-GCM-SHA256:ECDH:AES:HIGH:!aNULL:!MD5:!ADH:!DH
2. 需要在服务端TLS协议中启用TLS1.2，目前推荐配置：
   TLSv1 TLSv1.1 TLSv1.2

1.Nginx 证书配置

更新Nginx根目录下 conf/nginx.conf 文件如下：

```
server {
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDH:AES:HIGH:!aNULL:!MD5:!ADH:!DH;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
}
```

2.Apache 证书配置

更新Apache根目录下 conf/httpd.conf 文件如下：

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
        SSLProtocol TLSv1 TLSv1.1 TLSv1.2
        SSLCipherSuite ECDHE-RSA-AES128-GCM-
SHA256:ECDH:AES:HIGH:!aNULL:!MD5:!ADH:!DH
        </VirtualHost>
</IfModule>
```

3.Tomcat 证书配置

更新 %TOMCAT_HOME%\conf\server.xml 文件如下：

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
    scheme="https" secure="true"
    SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
    SSLCipherSuite="ECDHE-RSA-AES128-GCM-
SHA256:ECDH:AES:HIGH:!aNULL:!MD5:!ADH:!DH" />
```