

证书管理

操作指南

产品文档



腾讯云

【版权声明】

©2015-2016 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【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

文档声明.....	2
域名验证指引.....	4
证书安装指引.....	7
私钥密码指引.....	15

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. 自动DNS验证

注：仅限使用云解析的域名

系统为申请证书的域名自动解析一条记录类型为CName的DNS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。

了解具体操作原理可以参考手动DNS验证。

2. 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

例如为申请的域名 www.domain.com

添加一条记录类型为Cname的DNS记录：sr5jtl1xxxxxxxmygdps.domain.com -> CName -> s2015xxxxxxx.domain.com，

解析添加成功后如下：

<input type="checkbox"/>	主机记录	状态	记录类型	线路	记录值
<input type="checkbox"/>	sr5jtl1xxxxxxxmygdps	✔ 正常解析	CNAME	默认	s2015xxxxxxx.domain.com.

sr5jtl1xxxxxxxmygdps.domain.com

的CName记录会被定时检查，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。

注：

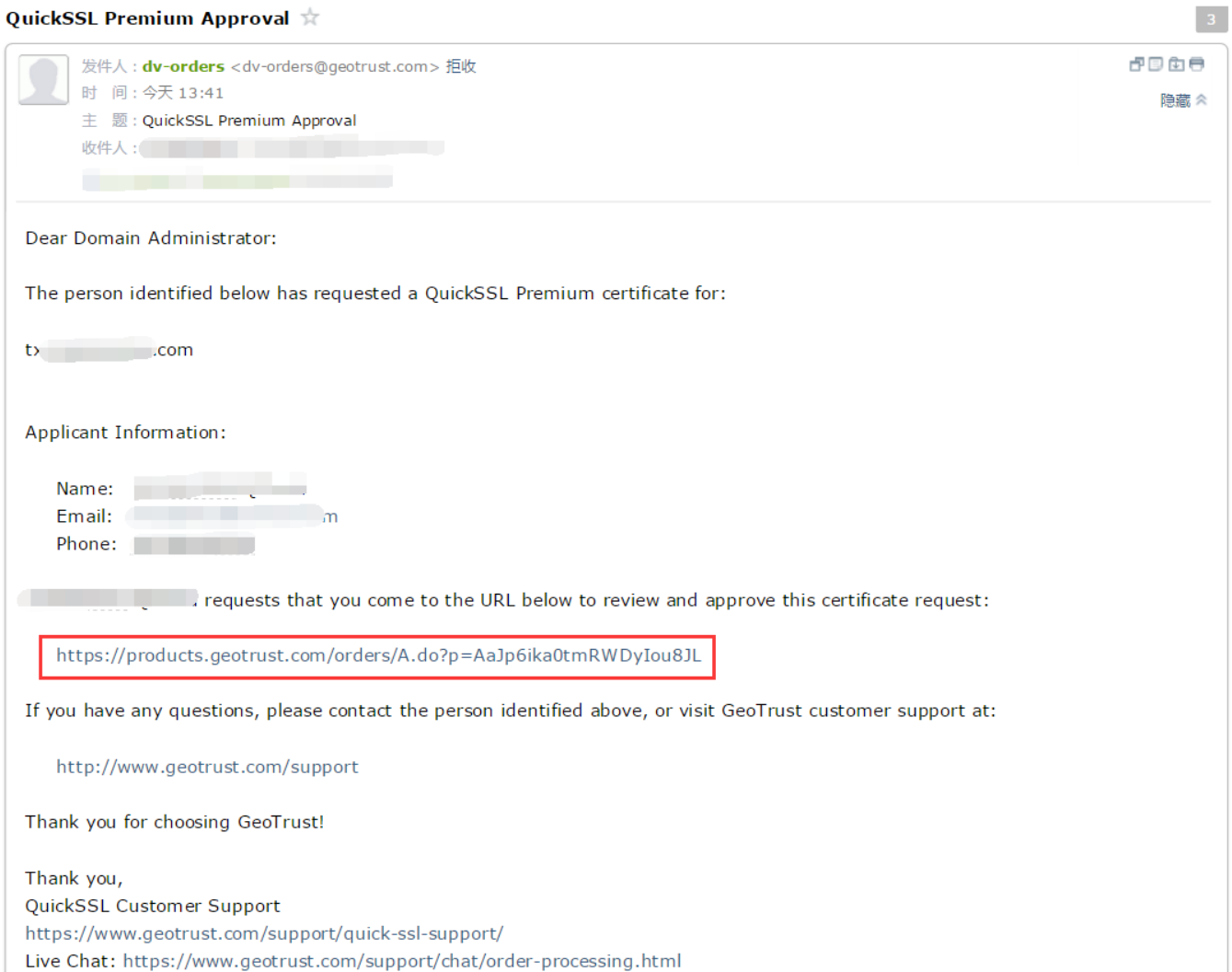
1. 主机记录填写 “.domain.com” 前面的内容，不需要填写主域名；
2. 记录类型选择为CName；

3. 记录值须完整填写。

3. 域名邮箱验证

所申请证书的CA机构将向您选择的邮箱发送验证邮件，手动验证邮件后点击其中的验证链接即可完成验证。

例如GeoTrust CA机构发送的验证邮件，点击其中的验证链接如下：



域名管理员邮箱符合以下规则，选择任意的邮箱确保您可以查收即可：

1. 域名whois管理联系人邮箱
2. 域名whois技术联系人邮箱

3. 默认管理员前缀的邮箱：

admin@domain.com

adminstrator@domain.com

hostmaster@domain.com

webmaster@domain.com

postmaster@domain.com

证书安装指引

下面提供了三类服务器证书安装方法的示例，分别是Nginx、Apache 和 IIS：

1. Nginx证书部署

1.1 获取证书

下载得到的 www.domain.com.zip 文件，解压获得SSL证书文件 1_www.domain.com_cert.crt 和私钥文件 2_www.domain.com.key,

1_www.domain.com_cert.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-----” 。

1.2 证书安装

将域名 www.domain.com 的证书文件1_www.domain.com_cert.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_cert.crt;
    ssl_certificate_key 2_www.domain.com.key;
    ssl_session_timeout 5m;
    ssl_protocols TLSv1;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
    location / {
        root html;
        index index.html index.htm;
    }
}
```

```
}
```

配置完成后，重新启动 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

2. Apache 2.x证书部署

2.1 获取证书

下载得到的 www.domain.com.zip 文件，解压获得SSL证书文件 1_www.domain.com_cert.crt 和私钥文件 2_www.domain.com.key,

1_www.domain.com_cert.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-----” 。

将1_domain.com_cert.crt 第一段代码保存成一个 crt格式的文件domain.crt ，第二段粘贴到一个文本中保存为 crt格式的文件 ca.crt。

(如果是三段式的交叉证书，将第二段、第三段保存为ca.crt)

2.2 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/domain.crt
    SSLCertificateKeyFile /usr/local/apache/conf/2_domain.com.key
    SSLCertificateChainFile /usr/local/apache/conf/ca.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

3. IIS 证书部署

3.1 获取证书

下载得到的 `www.domain.com.zip` 文件，解压获得SSL证书文件 `1_www.domain.com_cert.crt` 和私钥文件 `2_www.domain.com.key`,

`1_www.domain.com_cert.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-----” 。

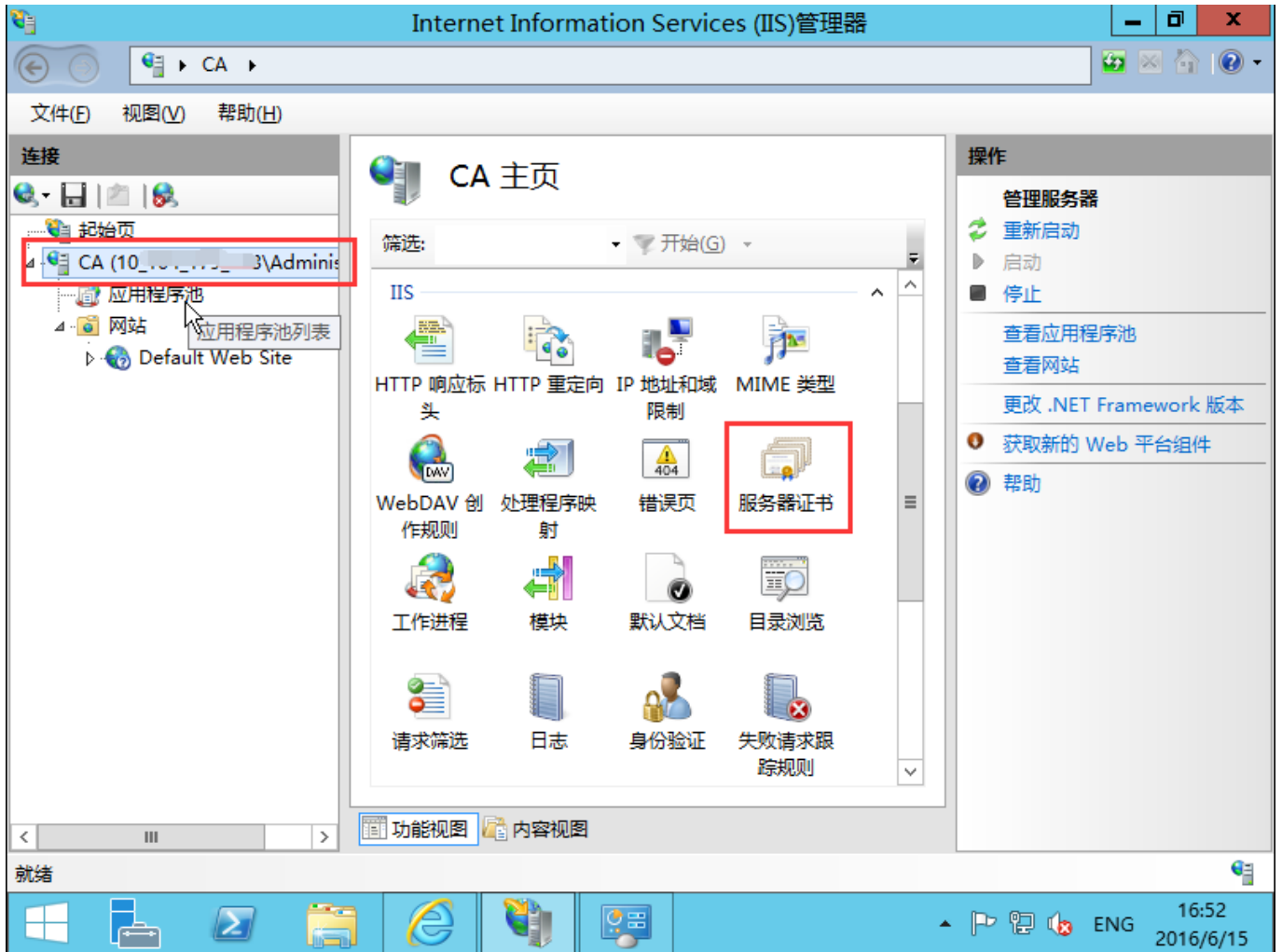
通过以下命令生成pfx格式证书文件

```
openssl pkcs12 -export -out www.domain.com.pfx -inkey 2_www.domain.com.key -in
1_www.domain.com_cert.crt
```

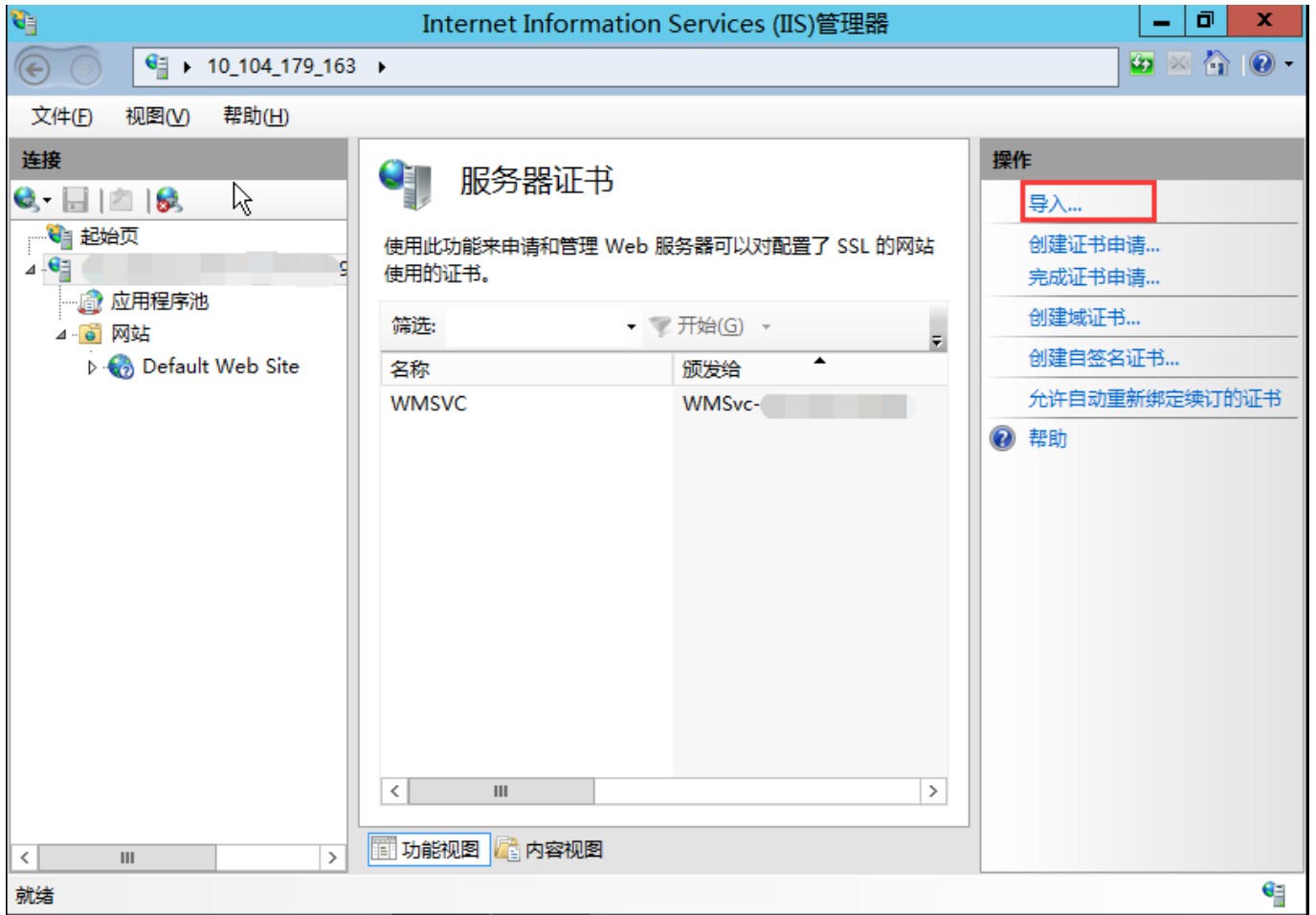
获得 `www.domain.com.pfx` 证书文件

3.2 证书安装

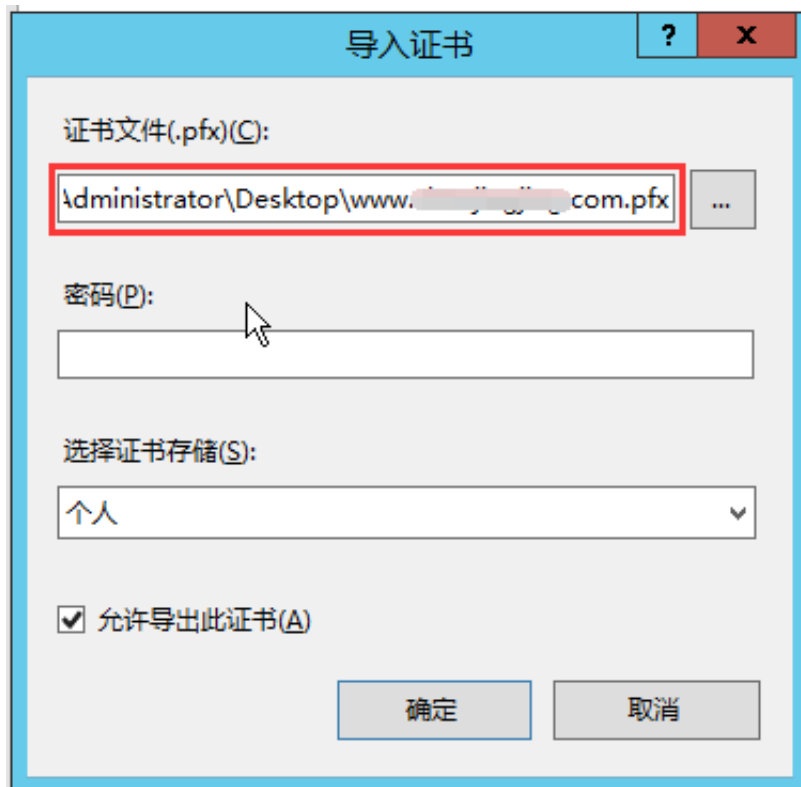
1、打开IIS服务管理器，点击计算机名称，双击‘服务器证书’



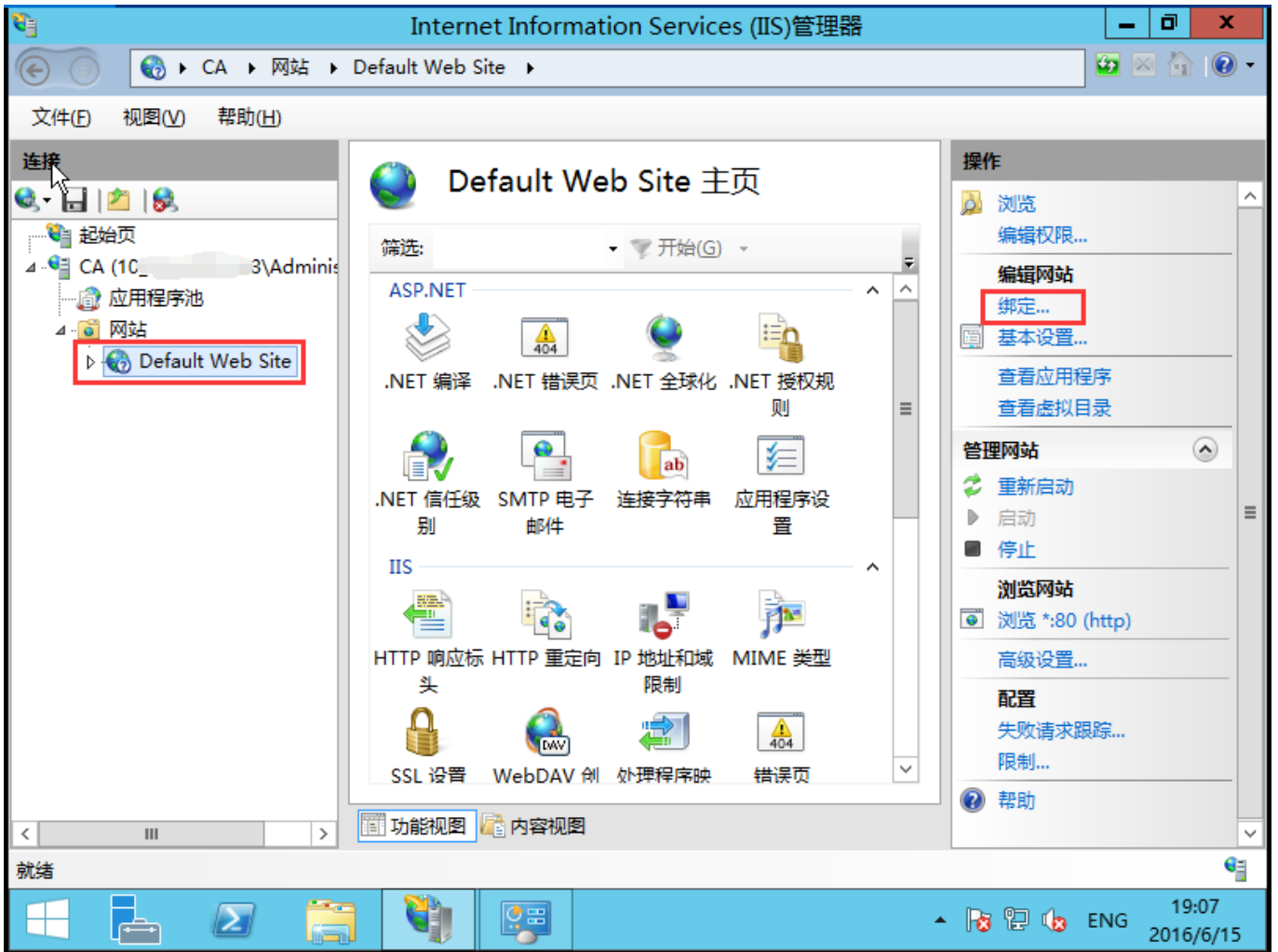
2、双击打开服务器证书后，点击右侧的导入



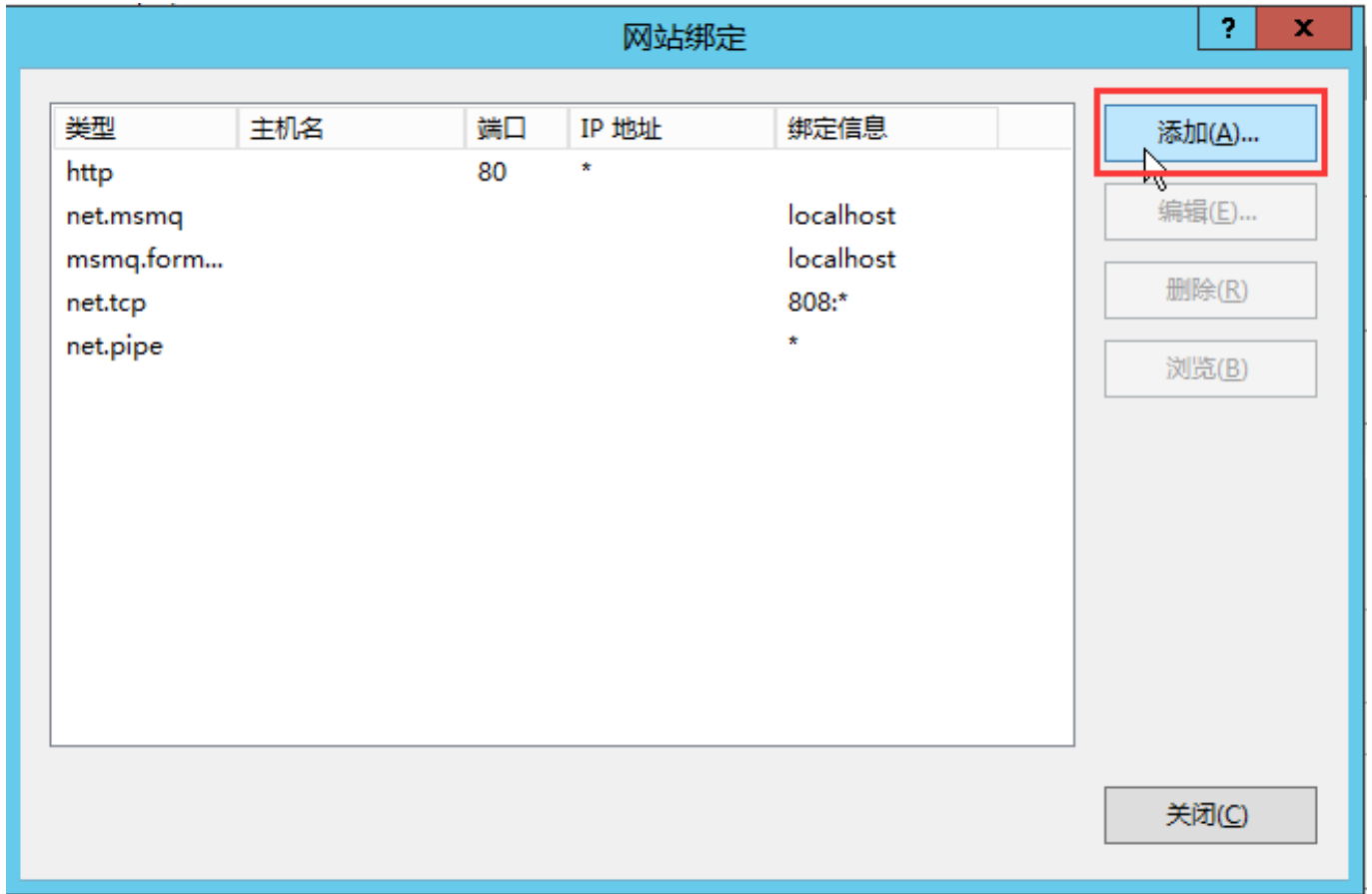
3、选择证书文件，如果输入申请证书时有填写私钥密码需要输入密码，点击确定。[参考私钥密码指引](#)



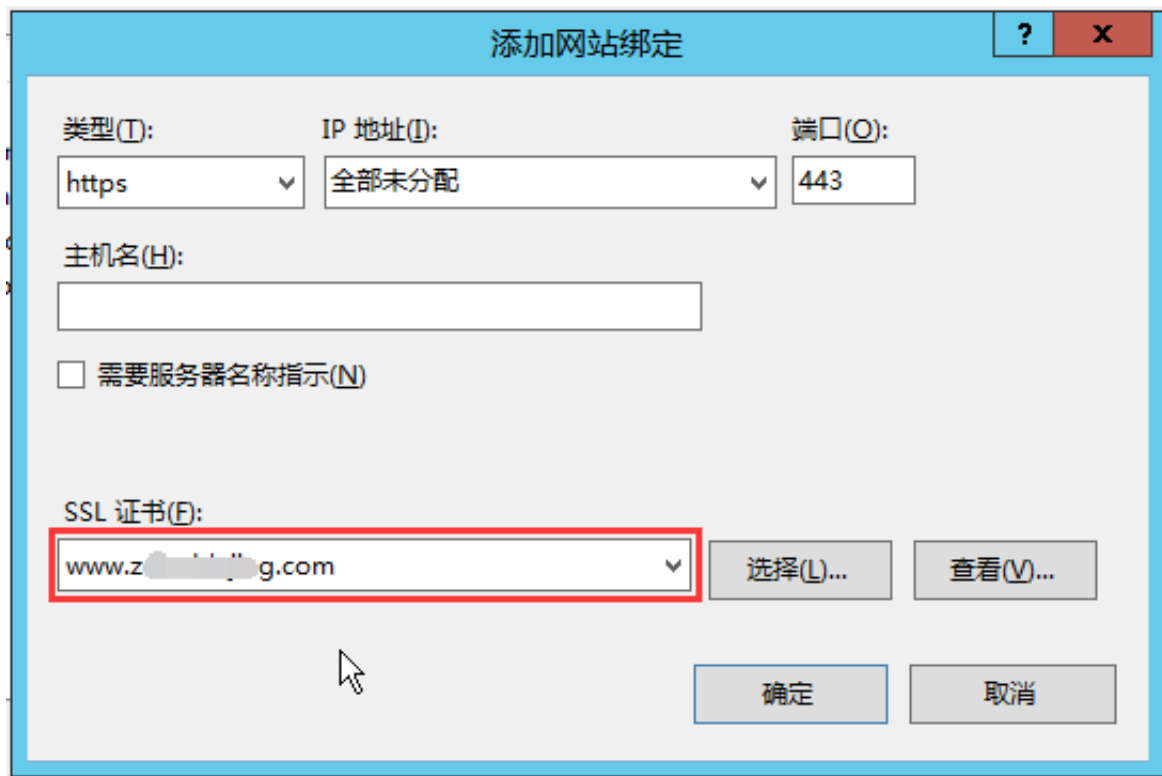
4、点击网站下的站点名称，点击右则的绑定



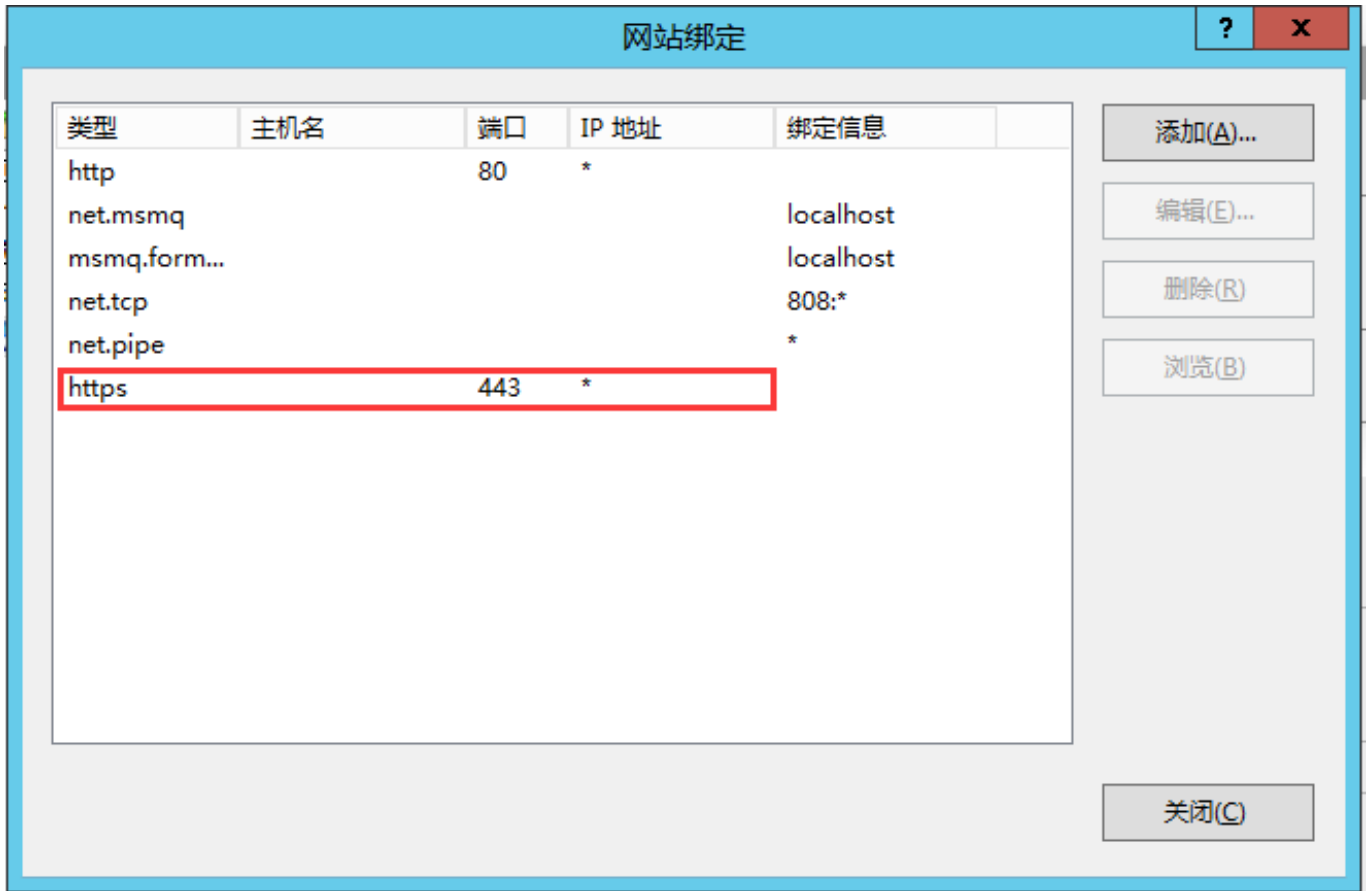
5、打开网站绑定界面后，点击添加



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



私钥密码指引

私钥密码是申请证书时的选填项，如图所示：

The screenshot shows the 'SSL证书管理' (SSL Certificate Management) console. The left sidebar has '证书管理' (Certificate Management) selected. The main area is titled '证书列表 | 证书申请' (Certificate List | Certificate Application). A green progress indicator shows '1 免费证书申请' (1 Free Certificate Application). The form includes the following fields:

- 绑定域名 * (Binding Domain): www.domain.com ✓
- 证书备注名 (Certificate Remark Name): 一个DV证书 ✓
- 私钥密码 (Private Key Password): [Redacted] (This field is highlighted with a red box in the original image)
- 确认密码 (Confirm Password): [Redacted]

Below the '私钥密码' field, there is a warning: 目前 暂不支持密码找回 功能，若您忘记密码则需重新申请证书 (Currently, the password recovery function is not supported. If you forget your password, you need to re-apply for the certificate). A blue '下一步' (Next Step) button is located at the bottom.

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、如果密码不慎遗忘，免费证书可重新申请。