

# 申请阿里云 SSL 证书

前置条件.....	2
操作步骤.....	2
1、开通阿里云 SSL 证书产品.....	2
2、进入证书控制台申请证书.....	3
3、下载证书.....	7
配置 Nginx.....	9
1、增加 443 端口监听.....	9
2、刷新 NGINX.....	10

## 文档说明

如今 HTTPS 已成为浏览器标准配置、非 HTTPS 环境使用下，会有一些安全限制，如：不能正常考试截屏、无法录音等、资源无法正常下载等，本文将引导您在阿里云申请一个免费的 SSL 证书；

# 前置条件

- 1、需要有您自己的域名
- 2、需要注册好阿里云账号并登录

# 操作步骤

## 1、开通阿里云 SSL 证书产品

<https://www.aliyun.com/product/cas>



【公告】证书增值服务灰度上线，预计7月12日全量发布，届时将对证书部分策略进行调整[点击查看详情](#)。

商品类型: **SSL证书** | SSL快捷购买 | 网站代理https

SSL证书服务: **SSL证书** | DV单域名证书【免费试用】

原DigiCert 免费单域名证书，建议用于测试、个人试用等场景，org、jp等特殊域名存在无法申请的情况，正式环境建议使用付费证书。  
 每个实名认证个人/企业，一个自然年内可以领取一次数量为20的云盾单域名试用证书，如需更多云盾单域名试用证书需要额外付费购买。  
 云盾单域名试用证书在自然年结束时，会自动清除未签发的数量（每个自然年12月31日24:00）  
 云盾单域名试用证书不支持续费补齐时间

数量: **20** | 40 | 50 | 100

每个实名认证个人/企业，一个自然年内可以领取一次数量为20的免费证书资源包  
 免费资源包到自然年结束时，会自动清除未签发的数量（每个自然年12月31日24:00）

证书个数是指可以签发证书的数量  
 例如，证书个数为1，将签发一张有效期为1年的证书  
 证书个数支持同时签发多张证书或者1张证书托管多年的服务

配置费用 **¥0.00** **立即购买** 加入购物车

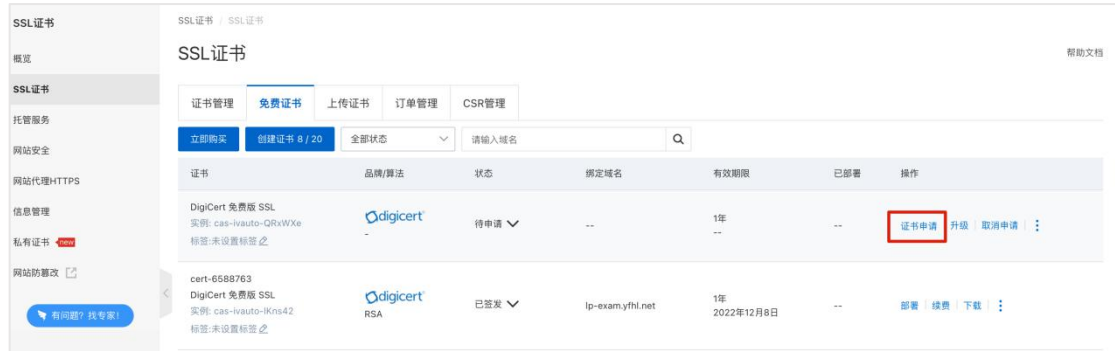
## 2、进入证书控制台申请证书

<https://yundun.console.aliyun.com/?spm=5176.b45069876.favorite.dcas.f36b2b72E>  
[XSUa1&p=cas#/overview/cn-hangzhou](#)

证书	品牌/算法	状态	绑定域名	有效期限	已部署	操作
cert-6588763 DigiCert 免费版 SSL 实例: cas-ivauto-ikns42 标签:未设置标签	DigiCert RSA	已签发	lp-exam.yfhl.net	1年 2022年12月8日	--	部署   续费   下载   ⋮
cert-6496086 DigiCert 免费版 SSL 实例: cas-ivauto-NyOIKG 标签:未设置标签	DigiCert RSA	已签发	doc-m.yfhl.net	1年 2022年11月22日	--	部署   续费   下载   ⋮
cert-6494407 DigiCert 免费版 SSL	DigiCert RSA	已签发			--	部署   续费   下载   ⋮

点击左侧 SSL 证书-->创建证书

此时下方会出现一个待申请状态的证书



点击证书申请

### 证书申请

1 填写申请 2 验证信息

申请证书需要将您提供的个人/公司信息提交给CA机构，请知悉。注意：非国产证书，申请证书时，证书申请信息将出境提交CA机构。国密算法证书只能在国密浏览器下显示可信。

• 证书绑定域名: pc.yfhl.net  
请输入完整的单个域名，域名格式例如：www.aliyun.com，IP证书仅Globalsign的OV单域名证书支持。

• 域名验证方式: 自动DNS验证

• 联系人: 杨高权, 18710213152, 626264481@qq.com

• 所在地: 中国大陆 / 浙江省 / 杭州市

• 密钥算法:  RSA

• CSR生成方式:  系统生成  手动填写  选择已有的CSR

为保障您的证书顺利申请，建议您使用默认生成CSR的方式，手动上传将无法部署到阿里云产品。  
建议您使用系统创建的CSR，避免因内容不正确而导致的审核失败。  
使用已创建的CSR申请证书，请不要在证书签发完成前删除CSR。

下一步 取消

填写好信息，继续下一步

### 证书申请

1 填写申请 2 验证信息

三步完成DNS验证

- 1 登录域名管理控制台**

如果域名在阿里云，请登录[阿里云DNS控制台](#)操作。如果您使用其他厂商的域名，请登录对应的域名管理控制台
- 2 在域名控制台添加DNS解析记录**

请按以下提示，在您的域名控制台添加DNS解析配置

配置项目	配置项值
域名授权验证类型	DNS
记录类型	TXT <a href="#">?</a>
主机记录	_dnsauth.pc <a href="#">?</a> <a href="#">复制</a>
记录值	202112150000004q1ttg4fv1utavlmjtv6i4o591rb41nkh51sj5g2xqrgolny2 <a href="#">?</a> <a href="#">复制</a>
- 3 验证DNS信息是否填写正确**

如果您已在域名控制台配置好DNS解析，请点击“验证”检查信息是否正确

[验证](#)

[上一步](#) [提交审核](#) [取消](#)

此处注意，如果您的域名是在本账号下面的，则直接点击验证即可，阿里云已经自动帮您加好的解析，如果域名是在其他账号或者其他平台下，则需要您自行解析后再点此处的验证，解析类型为 TXT，具体值按指引操作即可。

## 证书申请

✕

✓ 填写申请
2 验证信息

三步完成DNS验证

- 1 登录域名管理控制台**

如果域名在阿里云, 请登录[阿里云DNS控制台](#)操作。如果您使用其他厂商的域名, 请登录对应的域名管理控制台
- 2 在域名控制台添加DNS解析记录**

请按以下提示, 在您的域名控制台添加DNS解析配置

配置项目	配置项值
域名授权验证类型	DNS
记录类型	TXT <sup>?</sup>
主机记录	_dnsauth.pc <sup>?</sup> <a href="#">复制</a>
记录值	202112150000004q1ttg4fv1utavlmjtv6i4o591rb41nkh51sj5g2xqrgolny2 <sup>?</sup> <a href="#">复制</a>
- 3 验证DNS信息是否填写正确**

如果您已在域名控制台配置好DNS解析, 请点击“验证”检查信息是否正确

验证

✓ 域名验证成功, 域名验证记录在证书签发后再删除, 否则会因没有解析记录导致证书签发失败。

上一步
提交审核
取消

验证通过后, 提交审核按钮变为可用, 点击提交审核

### SSL证书

证书管理 **免费证书** 上传

[立即购买](#) [创建证书 8 / 20](#)

证书

DigiCert 免费版 SSL  
实例: cas-ivauto-QRxWXe  
标签:未设置标签

cert-6588763  
DigiCert 免费版 SSL  
实例: cas-ivauto-Kns42  
标签:未设置标签

cert-6496086  
DigiCert 免费版 SSL  
实例: cas-ivauto-NyDIKG  
标签:未设置标签

✓ 填写申请

三步完成DNS验证

**提示**

已经成功提交到CA公司, 请您保持电话畅通, 并及时查阅邮箱中来自CA公司的电子邮件。

确定
取消

配置项目	配置项值
域名授权验证类型	DNS
记录类型	TXT <sup>?</sup>
主机记录	_dnsauth.pc <sup>?</sup> <a href="#">复制</a>
记录值	202112150000004q1ttg4fv1utavlmjtv6i4o591rb41nkh51sj5g2xqrgolny2 <sup>?</sup> <a href="#">复制</a>

### 3、下载证书

提交审核后，过一段时间证书状态变成已签发（审核时间最快为几分钟）



The screenshot shows the 'SSL证书' (SSL Certificate) management page. It features a navigation bar with tabs for '证书管理', '免费证书', '上传证书', '订单管理', and 'CSR管理'. Below the navigation bar, there are buttons for '立即购买' and '创建证书 8 / 20', along with a search bar and a dropdown menu for '全部状态'. The main content area is a table with columns for '证书', '品牌/算法', '状态', '绑定域名', '有效期限', '已部署', and '操作'. A single certificate is listed with the following details: 'cert-6633430', 'DigiCert 免费版 SSL', '实例: cas-ivauto-QRvWXe', '品牌/算法: DigiCert RSA', '状态: 已签发', '绑定域名: pcyfhl.net', '有效期限: 1年 2022年12月16日', and '已部署: --'. The '操作' column contains links for '部署', '续费', '下载', and a three-dot menu icon. A red arrow points to the '下载' (Download) link.

证书	品牌/算法	状态	绑定域名	有效期限	已部署	操作
cert-6633430 DigiCert 免费版 SSL 实例: cas-ivauto-QRvWXe 标签:未设置标签	DigiCert RSA	已签发	pcyfhl.net	1年 2022年12月16日	--	部署   续费   下载   ⋮

我们点击下载，因为我们是用 nginx 代理，所以下载 nginx 版本

## 证书下载 ×

请根据您的服务器类型选择证书下载：

服务器类型	操作
Tomcat	<a href="#">帮助</a>   <a href="#">下载</a>
Apache	<a href="#">帮助</a>   <a href="#">下载</a>
<b>Nginx</b>	<a href="#">帮助</a>   <a href="#">下载</a>
IIS	<a href="#">帮助</a>   <a href="#">下载</a>
JKS	<a href="#">帮助</a>   <a href="#">下载</a>
其他	<a href="#">下载</a>
根证书下载	<a href="#">下载</a>

**网站代理HTTPS服务**

不用安装证书，不用纠结各种安全套件的选择，不用担心私钥泄露，网站代理HTTPS服务帮助 [立即使用](#) 您解决网站HTTPS问题。

下载后得到 zip 文件，解压后如下：



将此两个文件上传到服务器的任意位置，如我传到服务器的/data/ssl 目录下



# 配置 Nginx

## 1、增加 443 端口监听

```
server {  
    listen      80;  
    server_name pc.yfhl.net;  
    listen 443 ssl;  
    ssl_certificate /data/ssl/6803566_pc.yfhl.net.pem;  
    ssl_certificate_key /data/ssl/6803566_pc.yfhl.net.key;  
    ssl_session_timeout 5m;  
    ssl_ciphers  
ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
    ssl_prefer_server_ciphers on;  
    proxy_set_header X-Real-IP $remote_addr;  
    proxy_set_header Host $host;  
    proxy_set_header X-Forward-For $proxy_add_x_forwarded_for;  
    proxy_http_version 1.1;  
    proxy_set_header Upgrade $http_upgrade;  
    proxy_set_header Connection 'upgrade';  
    client_max_body_size 200m;  
    location / {  
        root /data/run/exam-vue/dist;  
        try_files $uri $uri/ /index.html last;  
    }  
    location ~/(api|upload/file){  
        proxy_pass http://localhost:8101;  
    }  
}
```

以上：

红色文字为增加的证书配置，只需保证证书文件位置正确即可

## 2、刷新 NGINX

重启或者刷新 NGINX 即可完整配置，此时域名支持 https 访问，如：<https://pc.yfhl.net>

刷新 nginx 命令一般为：`/usr/sbin/nginx -s reload`