

nginx 配置 https-云服务器真实环境演示

主讲教师: (大地)

合作网站: www.itying.com (IT 营)

我的专栏: https://www.itying.com/category-79-b0.html

一、	为什么要使用 https	1
	· ·	
_,	配置 https	1

一、为什么要使用 https

HTTPS (全称: Hyper Text Transfer Protocol over Secure Socket Layer),是以安全为目标的 HTTP 通道,简单讲是 HTTP 的安全版。

HTTPS 是在 HTTP 的基础上添加了安全层,从原来的明文传输变成密文传输,当然加密与解密是需要一些时间代价与开销的,不完全统计有 10 倍的差异。在当下的网络环境下可以忽略不计,已经成为一种必然趋势。

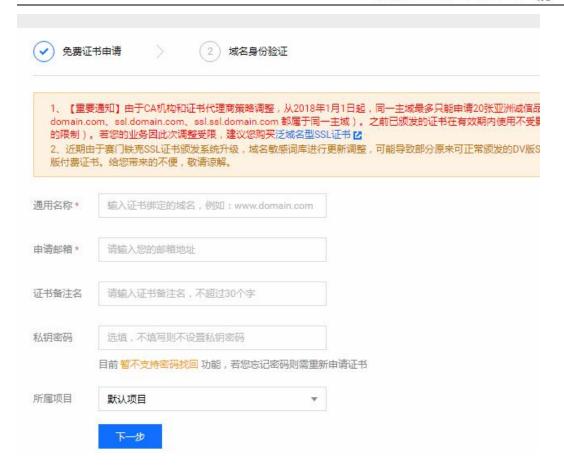
目前微信小程序请求 Api 必须用 https、los 请求 api 接口必须用 https

二、配置 https

1、证书类型

- 1、域名型 https 证书(DVSSL):信任等级一般,只需验证网站的真实性便可颁发证书保护网站;
- 2、企业型 https 证书(OVSSL):信任等级强,须要验证企业的身份,审核严格,安全性更高;
- 3、增强型 https 证书(EVSSL):信任等级最高,一般用于银行证券等金融机构,审核严格,安全性最高,同时可以激活绿色网址栏。

2、创建证书



3、证书验证

可以是域名验证,也可以是文件验证,看教程演示

4、配置 web 服务器

https://cloud.tencent.com/document/product/400/4143#2.-nginx-.E8.AF.81.E4.B9.A6.E9.83. A8.E7.BD.B2

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:

```
listen 443;
      server_name www.domain.com; #填写绑定证书的域名
      ssl on;
      ssl_certificate 1_www.domain.com_bundle.crt;
      ssl_certificate_key 2_www.domain.com.key;
      ssl_session_timeout 5m;
      ssl_protocols TLSv1.1 TLSv1.2; #按照这个协议配置
      ssl_ciphers
ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;#按照这个套件配置
      ssl_prefer_server_ciphers on;
      location / {
                html; #站点目录
          root
          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。就可以使用 https://www.domain.com 来访问。



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
ssl_session_timeout	连接超时时间