<https://blog.csdn.net/abld99/article/details/74011487>

2017年06月30日 18:32:30 [向上爬的蜗牛](https://me.csdn.net/abld99) 阅读数：14945 标签： [https](http://so.csdn.net/so/search/s.do?q=https&t=blog) 更多

个人分类： [服务器部署](https://blog.csdn.net/abld99/article/category/6600985)

版权声明：本文为博主原创文章，未经博主允许不得转载。 https://blog.csdn.net/abld99/article/details/74011487

## Question

1.HTTPS证书支持覆盖二级域名吗？

2.如何选择证书提供商(CA)？

3.如何申请免费的证书？

4.使用https后对原来的应用有哪些影响？

5.使用https后怎么通过charles抓包分析？

## 概念

1. https证书的类型：

DV SSL证书：域名型

OV SSL证书：企业型

EV SSL证书：增强型

* 1
* 2
* 3

**DV SSL**证书：指只验证网站域名所有权的简易型SSL证书，此类证书仅能起到网站机密信息加密的作用，无法向用户证明网站的真实身份。所以，不推荐在电子商务网站部署 DV SSL证书，因为电子商务首先需要的是在线信任，其次才是在线安全。

**OV SSL** 是 Organization Validation SSL 的缩写，指需要验证网站所有单位的真实身份的标准型SSL证书，此类证书也就是正常的SSL证书，不仅能起到网站机密信息加密的作用，而且能向用户证明网站的真实身份。所以，推荐在所有电子商务网站使用，因为电子商务需要的是在线信任和在线安全。从 SSL 证书的诞生史可以看出：标准型 SSL 证书就是 OV SSL证书(Organization Validation SSL)。

**EV SSL** 是 Extended Validation SSL 的缩写，指遵循全球统一的严格身份验证标准颁发的SSL证书，是目前业界最高安全级别的SSL证书。用户访问部署了EV SSL证书的网站，不仅浏览器地址栏会显示安全锁标志，而且浏览器地址栏会变成绿色。所以，推荐所有电子商务网站都部署EV SSL证书，因为电子商务首先需要的是在线信任，其次才是在线安全。EV SSL证书，绿色安全通道，增强在线信任，促成更多在线订单！

1. 证书按覆盖范围分为：
   * **单域名证书**：只能用于单一域名
   * **通配符证书**：可以用于某个域名及其所有一级子域名。
   * **多域名证书**：可以用于多个域名
2. 选择证书提供商(CA)

浏览器和操作系统支持程度（即公网受信）

证书类型

维护成本

1. 申请免费的https证书

[腾讯云免费证书](https://console.qcloud.com/ssl)

let’s encrypt：推荐比较多的，但是实际操作起来还是比较繁琐。

#### 腾讯云的免费DV证书申请

申请地址：<https://console.qcloud.com/ssl>

免费证书是由亚洲诚信TrustAsia提供的免费版DVSSL证书，有效期是一年。

免费的DV证书只支持单域名，支持多域名和通配符的证书需要付费购买，所以如果有多个子域名，需要一个个的申请。

申请的流程也特别的简单，如果选择的是文件验证，添加文件后等待CA来验证就好了，大概几分钟左右验证通过后就会颁发证书，就可以在腾讯云的后台管理里下载证书了。

下载证书后怎么配置nginx呢，可以参考腾讯云的[证书安装指引](https://www.qcloud.com/document/product/400/4143)

## Nginx配置https

server{

listen 443*;*

server\_name xxx.xxx.com*;*

root /opt/https/*;*

ssl on*;*

ssl\_certificate vhost/keys/xxx.xxx.com.crt*;*

ssl\_certificate\_key vhost/keys/xxx.xxx.com.key*;*

ssl\_session\_timeout 5m*;*

ssl\_protocols TLSv1 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 / {

index index.html*;*

root /opt/https*;*

}

}

* 1
* 2
* 3
* 4
* 5
* 6
* 7
* 8
* 9
* 10
* 11
* 12
* 13
* 14
* 15
* 16
* 17
* 18

| **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 |

##### 使用全站加密,http自动跳转https

server{

listen 80;

server\_name xxx.xxx.com;

rewrite ^(.\*) https://$host$1 permanent;

}

* 1
* 2
* 3
* 4
* 5

## 使用HTTPS可能带来的问题

1. https网站中存在http外部接口
2. CDN静态资源使用了http
3. charles抓包调试

#### 参考链接

[SSL证书有哪几种？如何识别这几种SSL证书](http://www.wosign.com/FAQ/SSL_type_check.htm)

[Let’s Encrypt 给网站加 HTTPS 完全指南](https://ksmx.me/letsencrypt-ssl-https/)

[HTTPS 升级指南](http://www.ruanyifeng.com/blog/2016/08/migrate-from-http-to-https.html)