



**数安时代科技股份有限公司**

**Nginx SSL 服务器证书部署指南**

修订日期：2017/12/12

## 目 录

一、	部署前特别说明.....	2
二、	获取服务器证书.....	2
1.	获取证书 .....	2
2.	私钥文件 .....	3
三、	安装服务器证书.....	3
1.	配置 ssl 证书.....	3
四、	访问测试.....	4
五、	备份和恢复 .....	4
1.	备份服务器证书.....	4
2.	恢复服务器证书.....	4
六、	证书遗失处理 .....	4








## 一、部署前特别说明

1. GDCA 信鉴易® SSL 服务器证书部署指南(以下简称“本部署指南”)主要描述如何通过 GDCA 在线系统产生密钥对证书部署到 Nginx 服务器
2. 本部署指南适用于 linux、windows 系统下 Nginx 1.4 及以上版本;
3. Nginx 服务器部署恒信企业 EV SSL 和睿信 SSL 证书的操作步骤一致, 区别在于: 前者在 IE7 以上浏览器访问时, 浏览器会显示安全锁标志, 地址栏会变成绿色; 而后者在浏览器访问时, 浏览器显示安全锁标志, 但地址栏不会变成绿色。
4. 本部署指南使用 testweb.95105813.cn 作为样例进行安装配置, 实际部署过程请用户根据正式的域名进行配置。


## 二、获取服务器证书

### 1. 获取证书

在您完成申请数安时代 GDCA 服务器证书的流程后, 登录系统将会下载一个压缩文件, 使用压缩文件里面的 NginxServer.zip 文件

 ApacheServer.zip	2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 IISServer.zip	2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 NginxServer.zip ← 解压此文件	2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 OtherServer.zip	2017/12/4 13:40	好压 ZIP 压缩文件	5 KB
 README.txt	2017/12/4 13:40	文本文档	1 KB

解压之后获得证书如下图:

名称	修改日期	类型
 testweb.95105813.cn_bundle.crt	2017/12/4 13:40	安全证书



## 2. 私钥文件

请找到之前提交 `csr` 时生成的 `.key` 私钥文件，该文件为证书的私钥，请找到此文件，后面配置要用到此文件；

# 三、安装服务器证书

## 1. 配置 ssl 证书

打开 `nginx` 安装目录下 `conf` 目录中的 `nginx.conf` 文件，找到被注释掉的 `server` 配置，进行修改：

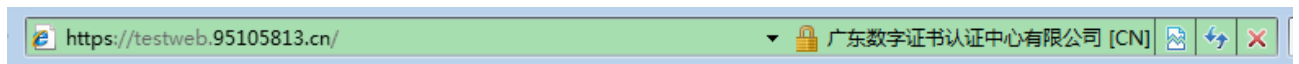
```
server {  
    listen          443 ssl;  
    server_name    www.yourdomian.com;  
    ssl            on;  
    ssl_certificate /usr/local/nginx/conf/testweb.95105813_bundle.cn.crt;#证书  
    ssl_certificate_key /usr/local/nginx/conf/testweb.95105813.cn.key; #私钥  
    ssl_session_cache    shared:SSL:1m;  
    ssl_session_timeout  5m;  
    ssl_protocols    TLSv1 TLSv1.1 TLSv1.2;  
    ssl_ciphers    ECDH:AESGCM:HIGH:!RC4:!DH:!MD5:!3DES:!aNULL:!eNULL;  
    ssl_prefer_server_ciphers    on;  
  
    location / {  
        root    html;  
        index  index.html index.htm;  
    }  
}
```



把服务器证书 `testweb.95105813.cn.crt` 和私钥 `testweb.95105813.cn.key` 上传到配置文件指向的目录 `/usr/local/nginx/conf/`（具体文件路径可以自行指定）  
保存退出，并重起 `nginx` 配置 `nginx -s reload` 后通过 `https` 方式访问您的站点，测试站点证书的安装配置。

## 四、 访问测试

服务器若部署了 SSL 证书，浏览器访问时将出现安全锁标志；若部署了 EV SSL 证书，IE 浏览器除了显示安全锁标志，地址栏会变成绿色，（*如果访问不通，请查看防火墙是否拦截 443 端口*）如下图：



## 五、 备份和恢复

### 1. 备份服务器证书

备份服务器证书私钥文件 `testweb.95105813.cn.key`，服务器证书文件 `testweb.95105813.cn_bundle.crt`，即可完成服务器证书的备份操作。

### 2. 恢复服务器证书

参照步骤“三、安装服务器证书”即可完成恢复操作。

## 六、 证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件，请联系 GDCA（客服热线 95105813）办理遗失补办业务，重新签发服务器证书。

