

# 07.Nginx HTTPS

- 07.Nginx HTTPS
  - 1.HTTPS基本概述
  - 2.HTTPS配置语法
  - 3.HTTPS配置场景
  - 4.Https公有云实践

徐亮伟,江湖人称标杆徐。多年互联网运维工作经验,曾负责过大规模集群架构自动化运维管理工作。擅长Web集群架构与自动化运维,曾负责国内某大型电商运维工作。

个人博客["徐亮伟架构师之路"](#)累计受益数万人。

笔者Q:552408925、572891887

架构师群:471443208

实战构建一个满足苹果要求的HTTPS后台服务

## 1.HTTPS基本概述

为什么需要使用HTTPS,因为HTTP不安全

- 1.传输数据被中间人盗用,信息泄露
- 2.数据内容劫持,篡改

## 2.HTTPS配置语法

```
Syntax: ssl on | off;  
Default: ssl off;  
Context: http, server
```

```
Syntax: ssl_certificate file;  
Default: -  
Context: http, server
```

```
Syntax: ssl_certificate_key file;  
Default: -  
Context: http, server
```

## 3.HTTPS配置场景

## 配置苹果要求的证书

- 1.服务器所有连接使用TLS1.2以上版本(openssl 1.0.2)
- 2.HTTPS证书必须使用SHA256以上哈希算法签名
- 3.HTTPS证书必须使用RSA 2048位或ECC256位以上公钥算法
- 4.使用前向加密技术

## 秘钥生成操作步骤

- 1.生成key密钥
- 2.生成证书签名请求文件(csr文件)
- 3.生成证书签名文件(CA文件)

### 1.检查当前环境

```
//openssl必须是1.0.2
[root@Nginx ~]# openssl version
OpenSSL 1.0.2k-fips  26 Jan 2017

//nginx必须有ssl模块
[root@Nginx ~]# nginx -V
--with-http_ssl_module

[root@Nginx ~]# mkdir /etc/nginx/ssl_key -p
[root@Nginx ~]# cd /etc/nginx/ssl_key
```

### 2.创建私钥

```
[root@Nginx ssh_key]# openssl genrsa -idea -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
//记住配置密码，我这里是1234
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

### 3.生成使用签名请求证书和私钥生成自签证书

```
[root@Nginx ssl_key]# openssl req -days 36500 -x509 \
-sha256 -nodes -newkey rsa:2048 -keyout server.key -out server.crt

Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:WH
```

```
Locality Name (eg, city) [Default City]:WH
Organization Name (eg, company) [Default Company Ltd]:edu
Organizational Unit Name (eg, section) []:SA
Common Name (eg, your name or your server's hostname) []:bgx
Email Address []:bgx@foxmail.com
```

#### 4.配置 Nginx

```
[root@Nginx ~]# cat /etc/nginx/conf.d/ssl.conf
server {
    listen 443;
    server_name localhost;
    ssl on;
    index index.html index.htm;
    #ssl_session_cache share:SSL:10m;
    ssl_session_timeout 10m;
    ssl_certificate    ssl_key/server.crt;
    ssl_certificate_key    ssl_key/server.key;
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDSA:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_prefer_server_ciphers on;

    location / {
        root /soft/code;
        access_log /logs/ssl.log main;
    }
}
```

#### 5.测试访问, 由于该证书非第三方权威机构颁发, 而是我们自己签发的, 所以浏览器会警告



6.以上配置如果用户忘记在浏览器地址栏输入 https:// 那么将不会跳转至 https , 需要将访问 http 强制跳转 https

```
[root@Nginx ~]# cat /etc/nginx/conf.d/ssl.conf
server {
    listen 443;
    server_name localhost;
    ssl on;
    index index.html index.htm;
    #ssl_session_cache share:SSL:10m;
    ssl_session_timeout 10m;
    ssl_certificate    ssl_key/server.crt;
    ssl_certificate_key    ssl_key/server.key;
```

```
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;  
  
location / {  
    root /soft/code;  
}  
}  
  
server {  
    listen 80;  
    server_name localhost;  
    rewrite ^(.*) https://$server_name$1 redirect;  
}
```

## 7. 检查是否支持苹果要求 ATS 协议

```
//仅能在苹果终端上使用  
$ nscurl --ats-diagnostics --verbose https://192.168.69.113
```

## 4. Https公有云实践

在云上签发各品牌数字证书，实现网站 HTTPS 化，使网站可信，防劫持、防篡改、防监听。并进行统一生命周期管理，简化证书部署，一键分发到云上产品。

域名控制台 > Alibaba Cloud DNS > 云盾证书服务管理控制台

安全 | https://dc.console.aliyun.com/dns/domain/setting?instanceId=&domain=bjstack.com

应用 运维 开发 学习 写作 阅读 教育 公有云 翻译 Tmp 已导入 Google google

管理控制台 产品与服务 搜索 搜索 新手引导 搜索 状态 操作

添加解析 导入/导出

云计算基础服务 大数据（数加） 安全（云盾） 域名与网站（万网） 域名 云解析 DNS 云虚拟主机 企业邮箱 标准建站 弹性 Web 托管 云市场

产品详情 解析设置 网站监控 DNS 护流管理 QPS 统计 解析日志

添加解析

记录类型: A - 将域名指向一个IPv4地址

主机记录: nginx .bjstack.com

解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路...

记录值: 118.190.174.159

TTL值: 10分钟

同步默认线路

配置域名解析

确认 取消

CNAME image 默认 idux9ql.qiniudns.com 10分钟

暂停 启用 删除

10条/页 1 10条/页

域名控制台 > https://netcn.console.aliyun.com/core/domain/list?spm=5176.2020520001.aliyun\_sidebar.33.69864bd3Aign9a

安全 | https://netcn.console.aliyun.com/core/domain/list?spm=5176.2020520001.aliyun\_sidebar.33.69864bd3Aign9a

应用 运维 开发 学习 写作 阅读 教育 公有云 翻译 Tmp 已导入 Google google

管理控制台 产品与服务 搜索 搜索 163 费用 工单 备案 企业 支持与服务 5524\*\*\*\*\*@qq.com 简体中文

云计算基础服务 大数据（数加） 安全（云盾） 域名与网站（万网） 域名 云解析 DNS 云虚拟主机 企业邮箱 标准建站 弹性 Web 托管 云市场

域名服务 域名列表 [进入域名解析列表] [域名抢注] 专业通道SnapNames抢注, 限时88折优惠, 更有精品域名0元火爆预定中!

英文.com批量(≥5个)注册39元/首年, 英文.cn批量(≥5个)注册13元/首年, 英文.net批量(≥5个)注册55元/首年!

信息模板 批量操作 域名转入 邮箱验证 操作日志 我是卖家 我是买家 域名预订 帮助与文档

全部域名 急需续费域名 急需赎回域名 未实名认证域名 预登记域名 导出列表 域名分组管理

关键词: 输入域名进行搜索 域名类型: 全部 域名分组: 选择分组 域名到期日期: 至

搜索 高级搜索

域名	域名类型	域名状态	到期日期	操作
lufedu.com	国际域名	正常	2018-06-19	续费   解析   SSL证书   管理
lufzx.com	国际域名	未实名认证	2018-06-19	续费   解析   管理
ncstack.com	国际域名	正常	2019-03-03	续费   解析   SSL证书   管理
bjstack.com	国际域名	正常	2018-05-29	续费   解析   SSL证书   管理
xuliangwei.com	国际域名	正常	2019-03-10	续费   解析   SSL证书   管理

共有5条, 每页显示: 20条 1 GO

域名控制台 > 云盾证书服务管理控制台 > DV通配符证书

特别提示：一个域名下，一次只能添加一个证书，最多申请3个免费证书用于测试。免费证书无法申请带 敏感关键字 域名的证书。

要申请的域名: nginx.bjstack.com  
例如：要申请 www.abc.com，则在文本框输入中填www。

授权系统自动添加TXT解析记录，自动完成域名授权验证

免费默认签发有效时长为1年，用于个人及测试，每个证书支持一个明细域名，更多证书类型 [请点此购买](#)

已获得证书: bjstack.com

确定 放弃

域名控制台 > 云盾证书服务管理控制台 > 域名控制台 > Alibaba Cloud DNS

实例名称: cas\_idv\_00 订单状态: 待完成

填写域名信息 > 填写个人信息 > 上传相关信息

申请人姓名: 徐亮伟  
申请人手机号: 13000000000  
非常重要的，签证人员会拨打该电话号码，确认证书验证的相关事宜

所在省市: 湖北省 武汉市  
详细地址: Hangzhou China  
邮政编码: 100000

域名验证类型:  DNS  文件  
证书绑定的域名在【阿里云的云解析】产品中，授权系统自动添加一条记录以完成域名授权验证。

申请确认Email: 552408925@qq.com  
非常重要，请确保邮箱可收发邮件，证书信息的确认、变改都会发到该邮箱

系统生成CSR  自己生成CSR

取消 上一步 下一步

域名控制台 > 云盾证书服务管理控制台 > Alibaba Cloud DNS

我的证书 | 亚太东南 2 (悉尼) | 中东东部 1 (迪拜) | 德国1 (法兰克福) | 亚太东北 1 (北京)

我的订单 我的证书

使用Web应用防火墙，可有效针对HTTPS业务防御黑客攻击、过滤海量CC请求。

证书订单的流程如下图，每个环节都有对应的帮助信息，请一定仔细阅读：

补全信息 → 提交审核 → 查看进度 → 颁发证书 → 下载证书

特别提示：免费证书只要按要求配置验证文件正确，系统就可自动完成签发。后台小二无法加速免费证书。另外，免费证书用于个人测试目的，后台小二无法提供安装部署的工单咨询服务噢！

实例ID	证书绑定域名	年限	证书品牌 (所有)	到期时间	证书状态 (全部)	进度	操作
cas_idv_00	nginx.bjstack.com	1 Year	Symantec 免费版 SSL	--	审核中	进度	<a href="#">撤回</a> <a href="#">详情</a>
cas_idv_00	nginx.bjstack.com	1 Year	Symantec 免费版 SSL	2019-04-19	已签发	--	<a href="#">推送</a> <a href="#">吊销</a> <a href="#">下载</a> <a href="#">到期新购</a> <a href="#">详情</a>
cas-ubcx5f0thgwy	down.xuliangwei.com	1 Year	Symantec 免费版 SSL	2018-03-03	已过期	--	<a href="#">详情</a>
cas-ysr5xb4pcu3j	xuliangwei.com	1 Year	Symantec 免费版 SSL	2017-12-20	已过期	--	<a href="#">详情</a>
cas-7k66lt678b5m	www.xuliangwei.com	1 Year	Symantec 免费版 SSL	2017-12-20	已过期	--	<a href="#">详情</a>
cas_idv_00	*.bjstack.com	1 Year	GeoTrust 通配符 DV	--	已关闭	--	<a href="#">详情</a>

共有6条，每页显示：6条

域名控制台 > 云盾证书服务管理控制台 > Alibaba Cloud DNS

我的证书 | 亚太东南 2 (悉尼) | 中东东部 1 (迪拜) | 德国1 (法兰克福) | 亚太东北 1 (北京) | 返回上级列表

实例名称：cas\_idv\_00 订单状态：已签发

请根据您的服务器类型选择下载，关于 苹果ATS的证书配置 问题和常见的 [证书格式转换](#)，请参考相关介绍  
注：云盾证书提供的证书文件后缀是.pem，如果是系统创建的CSR，同时还会伴随证书私钥，文件后缀.key。只有是系统创建的CSR时，证书才支持不同格式的转换。可根据自己的实际需求修改扩展名，比如可将.pem修改成.crt等。

Nginx/Tengine	Apache	Tomcat	IIS 6	IIS 7/8	其他
---------------	--------	--------	-------	---------	----

① [下载证书for Nginx](#)

② 安装证书

文件说明：  
 1. 证书文件1524377920931.pem，包含两段内容，请不要删除任何一段内容。  
 2. 如果是证书系统创建的CSR，还包含：证书私钥文件1524377920931.key。

(1) 在Nginx的安装目录下创建cert目录，并且将下载的全部文件拷贝到cert目录中。如果申请证书时是自己创建的CSR文件，请将对应的私钥文件放到cert目录下并且命名为1524377920931.key；  
 (2) 打开Nginx安装目录下conf目录中的nginx.conf文件，找到：

```
# HTTPS server
# #server {
# listen 443;
# server_name localhost;
# ssl on;
# ssl_certificate cert.pem;
# ssl_certificate_key cert.key;
# ssl_session_timeout 5m;
# ssl_protocols SSLv2 SSLv3 TLSv1;
# ssl_ciphers ALL:!ADH:!EXPORTS:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
# ssl_prefer_server_ciphers on;
# location / {
```

## 上传阿里云证书，并解压

```
[root@Nginx ssl_key]# rz
rz waiting to receive.
Starting zmodem transfer. Press Ctrl+C to cancel.
Transferring 1524377920931.zip...
```

100% 3 KB 3 KB/sec 00:00:01 0 Errors

```
//解压
[root@Nginx ssl_key]# unzip 1524377920931.zip
```

配置 nginx https

```
[root@Nginx conf.d]# cat ssl.nginx.bjstack.com.conf
server {
    listen 443;
    server_name nginx.bjstack.com;
    index index.html index.htm;
    ssl on;
    ssl_session_timeout 10m;
    ssl_certificate ssl_key/1524377920931.pem;
    ssl_certificate_key ssl_key/1524377920931.key;
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDSA:HIGH:!NULL:!aNULL:!MD5::!
ADH:!RC4;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_prefer_server_ciphers on;

    location / {
        root /soft/code;
    }
}

server {
    listen 80;
    server_name nginx.bjstack.com;
    rewrite ^(.*) https://$server_name$1 redirect;
}
```

测试访问



## 使用腾讯云 ATS 检测工具检查是否满足苹果 iOS 要求

The screenshot shows the Tencent Cloud SSL Certificate management interface. On the left sidebar, there are links for various domain suffixes (.com, .net, .cn, .club, .Wang, etc.) and services like DNS Management, Cloud Resolution, Website Host, Website Backup, SSL Certificates, and Enterprise Mail. The main content area is titled "Apple ATS Detection". It displays a message about the requirement starting in January 2017 and provides a form to enter a domain name for testing. The domain "nginx.bjstack.com" is entered in the "Domain" field, and the port "443" is selected. A red box highlights the "Domain" input field. Below the form, the result is shown as "ATS Detection Passed" with a green lock icon, stating "Congratulations, your application has passed the Apple ATS feature detection." Two sections follow: "Certificate Detection Results" and "Server Detection Results", each listing four items with green checkmarks.

证书品牌 证书类型 苹果ATS检测 产品优势 产品功能 应用场景 文档 立即购买 产品价格

苹果ATS检测

2017年1月1日起，苹果强制所有 app 满足 HTTPS，即 iOS9 推出的 App Transport Security (ATS) 特性。  
输入域名，检查您的 iOS app 是否满足 ATS 特性。

域名 nginx.bjstack.com 端口 ① 443 立即检测

ATS 检测通过  
恭喜，您的应用已通过苹果 ATS 特性检测。

证书检测结果

- 安全的证书签名算法 (SHA2)
- 证书被iOS9信任
- 证书与域名匹配
- 证书时间有效

服务器检测结果

- 支持TLS1.2
- PFS (完全正向保密)

## 苹果ATS - 证书选择及配置