

Nginx 安装 SSL 证书

1. 找到 Nginx 的配置文件

首先确认您的 Nginx 安装目录所在位置, 打开该安装目录下的 conf 目录, 并在 conf 目录下找到 nginx.conf 文件, 这个文件就是 Nginx 的配置文件, 您可以文本方式打开该文件并进行编辑。

2. 获取证书文件

请打开我司向您交付的 Nginx 证书, 后缀为 pem 或者 crt 格式, 这个证书链包含了服务器证书、中级根证书, 将他们复制到 Nginx 安装目录 conf 文件夹下, 下面就可以来修改配置文件了。

3. 修改配置文件

打开 nginx.conf 文件后找到#HTTPS server 所标识的段落, 该段落即为配置您的证书所相关的段落, 内容如下所示:

```
# HTTPS server

#

#server {

#   listen    443 ssl;

#   server_name localhost;

#   ssl_certificate    cert.pem;
```

```
# ssl_certificate_key cert.key;

# ssl_session_cache shared:SSL:1m;

# ssl_session_timeout 5m;

# ssl_ciphers HIGH:!aNULL:!MD5;

# ssl_prefer_server_ciphers on;

# location / {

#     root html;

#     index index.html index.htm;

# }

#}
```

请按照如下所示内容修改您的配置文件中的对应段落的内容:

```
# HTTPS server

#

server {

    listen 443 ssl;

    server_name www.ihuandu.com; # www.ihuandu.com 修改为您证书绑定的域

    名

    ssl on; #设置为 on 启用 SSL 功能,如果是 nginx1.5 以前的版本就需要加上 ssl on,
```

如是 nginx1.5 以后的版本就不需要加。

```
ssl_certificate    server.pem;    #将 server.pem 替换成您证书的文件名。

ssl_certificate_key  server.key;    #将 server.key 替换成您证书的密钥文件名。。

ssl_session_cache  shared:SSL:1m;

ssl_session_timeout 5m;

ssl_protocols TLSv1.1 TLSv1.2 TLSv1.3;#使用该协议进行配置

ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4; #使用此加密套件

ssl_prefer_server_ciphers on;

location / {

    root html;#站点目录

    index index.html index.htm;

}

}
```

修改完毕保存退出后, 您可以尝试启动 Nginx 服务, 测试是否可以正常通过 https 方式访问您的域名。 测试后请务必妥善备份您的证书私钥文件以及服务器证书 (链) 文件。