

HTTPS

客户端认证和使用openssl制作证书

HTTPS连接过程

客户端

服务器

Client Hello

服务器主机名 / 随机数 / 客户端支持的加密套件



选择证书

请选择证书，以在 exam.devmgr.cn:443 上对您本人进行身份验证



exam.devmgr.cn

显示证书

取消

确定

400 Bad Request

No required SSL certificate was sent

nginx/1.7.12

客户端

服务器

Client Hello

服务器主机名 / 随机数 / 客户端支持的加密套件

Server Hello

服务器随机数
服务器挑选出的加密套件

服务器的数字证书

CertificateRequest

Certificate

PreMasterKey (公钥加密)

即将使用加密通讯 FINISH

将使用加密通讯 FINISH

握手完毕，以后是应用数据协议正式报文

配置客户端认证

```
server {  
    listen 443;  
    server_name exam.devmgr.cn;
```

```
# 配置使用SSL，服务器端证书  
ssl on;  
ssl_certificate /etc/nginx/certs/1_exam.devmgr.cn_bundle.crt;  
ssl_certificate_key /etc/nginx/certs/2_exam.devmgr.cn.key;  
ssl_session_timeout 5m;  
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;  
ssl_prefer_server_ciphers on;
```

```
# 开启客户端认证  
ssl_client_certificate /etc/nginx/certs/ca.crt;  
ssl_verify_client on;
```

```
root /web/sites/exam;
```

```
}
```

获取客户端认证信息

- NGINX (ngx_http_ssl_module模块)
 - \$ssl_client_s_dn 客户端证书的主题DN
 - \$ssl_client_raw_cert 客户端证书, PEM格式
 - \$ssl_client_i_dn 客户端证书的颁发者DN

```
location /webapp {  
    proxy_pass http://127.0.0.1:8080;  
    proxy_set_header Host $host;  
    proxy_set_header X-Real-IP $remote_addr;  
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
    # 把客户端证书的主题信息作为request header (Client-Cert)传递给应用  
    proxy_set_header Client-Cert $ssl_client_s_dn;  
}
```

ngx_http_ssl_module文档: http://nginx.org/en/docs/http/ngx_http_ssl_module.html

OPENSSL自制证书

• 制作CA证书

#制作CA私钥

① openssl genrsa -out ca.key 2048

#制作CA根证书（公钥），会要求填写信息

② openssl req -new -x509 -days 3650 -key ca.key -out ca.crt

ca.key 保存的是私钥，后面签发证书会用到

ca.crt 包含了CA的公钥，验证证书会用到

服务器证书在浏览器端验证

客户端证书在服务器端验证

• 制作服务器证书

#制作服务器端私钥：

③ openssl genrsa -out server.key 2048

④ openssl rsa -in server.key -out server.public.key

#生成CSR（证书签发请求）

⑤ openssl req -new -key server.public.key -out server.csr

#用CA私钥签发证书

⑥ openssl x509 -req -sha256 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -days 3650 -out server.crt

在nginx中使用服务器端证书时，

需要证书server.crt和私钥server.key两个文件

• 制作客户端证书

#制作客户端私钥

⑦ openssl genrsa -out client.key 2048

⑧ openssl rsa -in client.key -out client.public.key

#生成CSR（签发请求）

⑨ openssl req -new -key client.public.key -out client.csr

#用CA私钥签发证书

⑩ openssl x509 -req -sha256 -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -days 365 -out client.crt

#转成pfx格式

⑪ openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.pfx

client.pfx是需要在客户端安装的证书

安装是需要这步设置的提取码