



服务器证书安装配置指南

阿里云SLB

二〇二一年一月

第一步：生成证书请求文件(CSR)

进入OpenSSL 安装的目录，运行如下命令生成私钥：

```
openssl genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

该命令执行后将会生成server.key 私钥文件

运行如下命令生成证书请求文件 (CSR)

```
openssl req -new -key server.key -out server.csr
```

如是Windows 系统，请使用下面命令生成证书请求文件 (CSR)

```
set OPENSSL_CONF=openssl.cnf
openssl req -new -key server.key -out server.csr
```

接下来提示输入申请证书的详细信息

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign China Co., Ltd.

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

从Email 地址开始，下面的信息都不需要，请保留为空，直接回车即可。

需要输入的信息说明请见下表：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名称	GlobalSign China Co., Ltd.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	cn.globalsign.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成以上的操作后会在对应的目录下生成server.key 和server.csr，请妥善保存这两个文件。

第二步：提交CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。

我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

1. 获取SSL 证书（此证书由GlobalSign 系统通过Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为server.cer（文本格式）。
2. 获取CA证书（此证书由GlobalSign 系统通过Email 方式发送给用户，邮件中第二段中级证书和第三段交叉证书代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为ca.cer 内容。格式如下图所示：

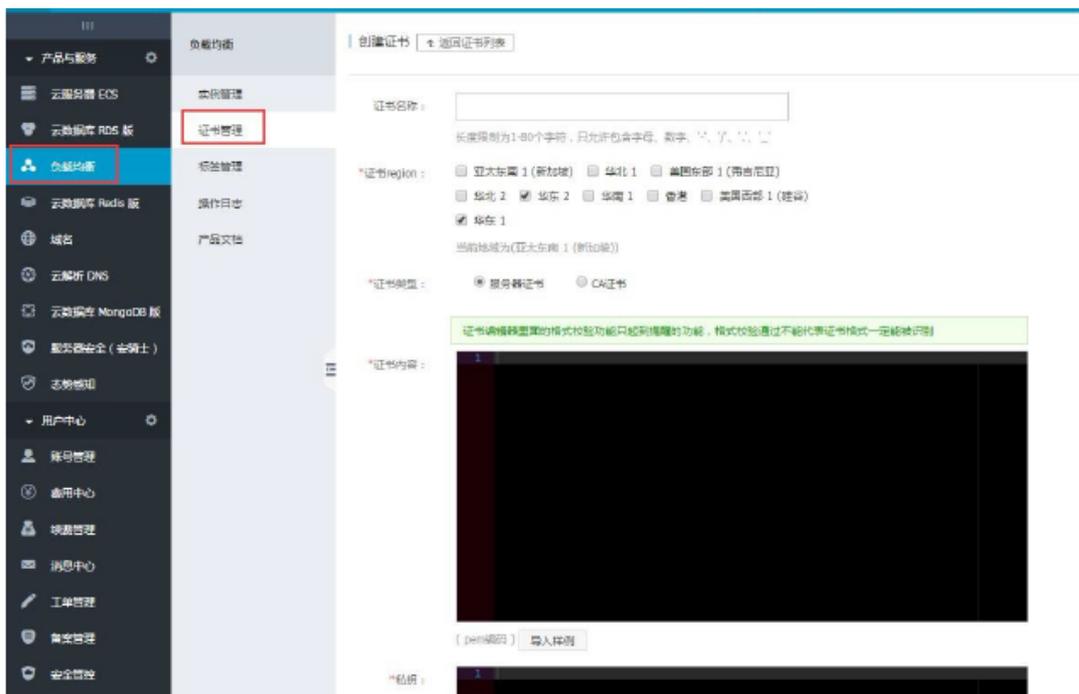
```

1 -----BEGIN CERTIFICATE-----
2 MIIEsDCCA5igAwIBAgIQd700B0LV2enQSdd00CpvmjANBgkqhkiG9w0BAQsFADBM
3 MSAwHgYDVQQLEXdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMzETMBEGA1UEChMKR2xv
4 YmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjAeFw0yMDA3MjgwMDAwMDBaFw0y
5 OTAzMTgwMDAwMDBaMFmxGzAJBgNVBAYTAkJKFMRkwFwYDVQQKEExBHBG9iYWxTaWdu
6 省略部分， 此段应存放中级证书内容
7 i00194TWvH3XWZGXZ6ByxTUIv1+kAIql/Mt29PmKraTT5jrzcVzQ5A9jw16yysuR
8 XRrLODlkS1hyBjsfyTNZrmL1h117IFgntBA5SQNV19ckedq5r4RSAU85jV8XK5UL
9 REjRzt2I6M9Po9QL7guFLu4sPFJpwr1sPJvubS2Theo7SxYoNDtdyBHs7euaGcMa
10 D/fayQ==
11 -----END CERTIFICATE-----
12 -----BEGIN CERTIFICATE-----
13 MIIEtjCCAzagAwIBAgINAe5fFp3/1zUrZGXWajANBgkqhkiG9w0BAQsFADBMQsw
14 CQYDVQQGEwJCRTEZMBcGALUEChMQR2xvYmFsU2lnbiBudilzYTEQMA4GALUECXMH
15 Um9vdCBDQTEbMBkGALUEAxMSR2xvYmFsU2lnbiBSb290IENBMB4XDTE4MDkxOTAw
16 省略部分， 此段应存放交叉证书内容
17 fR4uUfaNU9OrH0Abio7tfftPeVZwXwzTjhuzp3ANNyuXlava4BJrHED0xcd+7cJi
18 Wox37XMiworlkhOIreoTbv3Y/kIvuXlerRjv1JDKPserJpS2dcfL03v3yKzTr1Eh
19 kluEfSufFT90y1HonoMOFm8b50bOI7355KKL0jlrqnckckSziYSQtjipIcJDEHsXo
20 4HA=
21 -----END CERTIFICATE-----

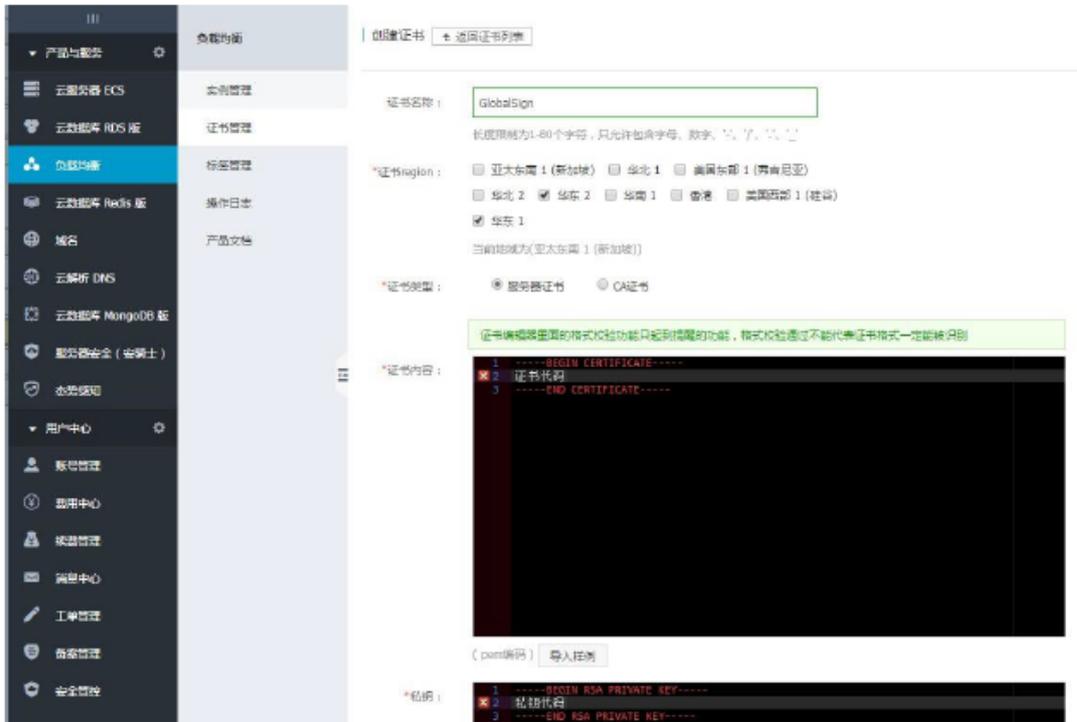
```

第四步：部署证书

1. 访问阿里云登录控制台，选择负载均衡，证书管理，创建证书。



2. 依次输入证书名称，证书region，选择服务器证书，证书内容复制server.cer 内容，私钥复制server.key 内容，然后点确定。



3. 选择CA 证书，复制ca.cer 内容，完成上传。

4. 进行端口配置。

按照以上的步骤配置完成后，就可以使用 <https://www.domain.com> 来访问了。附：

阿里官方文档

https://help.aliyun.com/knowledge_detail/39472.html?spm=5176.7839466.2.6.zl7bpr

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月