

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	YmFsU21nbjETMBEGA1UEAxMKR2xvYmFsU21nbjAeFw0yMDA3MjgwMDAwMDBaFw0y
5	OTAzMTgwMDAwMDBaMFMxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWdu
6	省略部分,此段应存放中级证书内容
7	i00194TWvH3XWZGXZ6ByxTUIv1+kAIq1/Mt29PmKraTT5jrzcVzQ5A9jw16yysuR
8	XRrLOD1kS1hyBjsfyTNZrmL1h117IFgntBA5SQNV19ckedq5r4RSAU85jV8XK5UL
9	REjRZt2I6M9Po9QL7guFLu4sPFJpwR1sPJvubS2THeo7SxYoNDtdyBHs7euaGcMa
10	D/fayQ==
11	END CERTIFICATE
12	BEGIN CERTIFICATE
13	MIIETjCCAzagAwIBAgINAe5fFp3/1zUrZGXWajANBgkqhkiG9w0BAQsFADBXMQsw
14	CQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU21nbiBudi1zYTEQMA4GA1UECxMH
15	Um9vdCBDQTEbMBkGA1UEAxMSR2xvYmFsU21nbiBSb290IENBMB4XDTE4MDkxOTAw
16	省略部分,此段应存放交叉证书内容
17	fR4uUfaNU9OrH0Abio7tfftPeVZwXwzTjhuzp3ANNyuXlava4BJrHEDOxcd+7cJi
18	WOx37XMiworlhkOIreoTbv3Y/kIvuXlerRjvlJDKPSerJpSZdcfL03v3ykzTrlEh
19	kluEfSufFT90ylHonoMOFm8b50b0I7355KKL0jlrqnkckSziYSQtjipIcJDEHsXo
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。

- ui	的新作用	創建证书 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
▼ 产品与服务	30.00-300	1 mman is a World Jo.20s		
₩ 元服祭職 ECS	本例留3章	证书名称		
🐨 ziblikult RDS 🕷	征书管理		长度探测为1-80个字符,只允许包含字母、数字、字、字、字、字、	
🗛 casear	标签管理	*iEttiregion :	豆太东南1(新加坡) 24北1 差回东部1(南吉尼亚)	
	操作日志		 ・ \$\$ ・ \$\$ ・ \$\$	
🕀 🕊	产品文档		当前地域为(亚大东南 1 (新印稿))	
C ZARAFI DNS		*证书积型:	 ● 展与器运书 ○ CA正书 	
🖸 宏数振车 MongoDB 版			(1年4)時間22月間時に低から2014月2日間間からから、他から2014月24日の第二日になるか、二日の時につけ	
	4	"订书内容:		
9 39990	-			
- Ярфо О				
L 账号管理				
③ 幽田中心				
👗 纳朗智雅				
11月1日日 11月1日 11月11日 11月11日 11月11日 11月11日 11月11日 11月11日 11月1111 11月11111 11月11111111				
/ I#82				
9 #252			(pen4883)	
0 #252		*私班:	1	

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。



ш	A HULKI	(10年)正式 A 2	JF 同プニエ F Inter
	201461340	LOOM GL TO T 3	When Z. 114.74
Ξ 元配完存 ECS	实利管理	证书名称:	GlobalSign
🖤 \Xi 2018014 ROS NE	证书管理		长期限制为1-80个字符,只允许包含字母。数字、2、2、2、2、
	6552	*i£†\$ragion :	豆式东南1(新加坡) 目 华北1 目 美国东部1(秀肯尼亚)
👄 \Xi 20185145 Rectis Alia	操作日志		● \$2%2 ● \$26 2 ● \$28 1 ● 雪港 ● 美国西部1(社会)
() xia	产品文档		如 年朱 1 当前時期(均(型太东南 1 (新加坡])
🛞 EMRET DAS		"证书架型:	 ※ 展明器運動 ◎ CA運動
D EXHIBIT MongoDB &			
(空 1000日本(1000日)			征卡编辑器里面的格式化验功能只能到情報的功能,格式化验患过不能代表证书格式一定能被识别
1 4:00 00 00 00 00 00 00 00 00 00 00 00 00	=	"证他内容;	■ 2 征形代码 3 ·····END CERTIFICATE
- R++0 0			
A 16000			
③ 20用≠0			
A #021172			
□ 消息中心			
/ 1983			
© 5202			(pam编码) 尋入推測
0 #25R		*648 i	1

- 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