ALIBABA CLOUD

阿里云

负载均衡

证书管理

文档版本：20210115

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.证书要求

负载均衡只支持PEM格式的证书。在上传证书前，确保您的证书、证书链和私钥符合格式要求。

Root CA机构颁发的证书

如果是通过Root CA机构颁发的证书，您拿到的证书是唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。

证书格式必须符合如下要求：

- 以 -----BEGIN CERTIFICATE-----, -----END CERTIFICATE----- 开头和结尾。
- 每行64个字符，最后一行长度可以不足64个字符。
- 证书内容不能包含空格。

中级机构颁发的证书

如果是通过中级CA机构颁发的证书，您拿到的证书文件包含多份证书，需要将服务器证书与中级证书合并在一起上传。

证书链格式必须符合如下要求：

- 服务器证书放第一位，中级证书放第二位，中间不能有空行。
- 证书内容不能包含空格。
- 证书之间不能有空行，并且每行64字节。更多信息，请参见RFC1421。
- 符合证书的格式要求。一般情况下，中级机构在颁发证书时会有对应说明，证书要符合证书机构的格式要求。

中级机构颁发的证书链示例。

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

证书公钥

目前阿里云负载均衡支持如下公钥算法：

- RSA 1024
- RSA 2048
- RSA 4096
- ECDSA P-256
- ECDSA P-384
- ECDSA P-521

RSA私钥格式要求

在上传服务器证书时，您也需要上传证书的私钥。

RSA私钥格式必须符合如下要求：

- 以 -----BEGIN RSA PRIVATE KEY-----, -----END RSA PRIVATE KEY----- 开头和结尾，请将这些内容一并上传。
- 字串之间不能有空行，每行64字符，最后一行长度可以不足64字符。更多信息，请参见RFC1421。

如果您的私钥是加密的，例如私钥的开头和结尾是 -----BEGIN PRIVATE KEY-----, -----END PRIVATE KEY----- 或 -----BEGIN ENCRYPTED PRIVATE KEY-----, -----END ENCRYPTED PRIVATE KEY----- ，或者私钥中包含 Proc-Type: 4,ENCRYPTED ，需要先运行以下命令进行转换：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

EC私钥格式要求

> **说明** 目前仅英国（伦敦）地域支持。

在上传服务器证书时，您也需要上传证书的私钥。

EC私钥格式必须符合如下要求：

- 以 -----BEGIN EC PARAMETERS-----, -----END EC PARAMETERS----- 开头和结尾，请将这些内容一并上传。
- 字串之间不能有空行，每行64字符，最后一行长度可以不足64字符。更多信息，请参见RFC1421。

如果您的私钥是加密的，例如私钥的开头和结尾是 -----BEGIN EC PRIVATE KEY-----, -----END EC PRIVATE KEY----- 或者私钥中包含 Proc-Type: 4,ENCRYPTED ，需要先运行以下命令进行转换：

```
openssl ec -in old_server_key.pem -out new_server_key.pem
```

下图为EC私钥示例。

```
-----BEGIN EC PARAMETERS-----
Bggq**********Bw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEICo9b+vQUhqFUWgWjE0YY4h0b3bE/udcubxVwcVY99MuoAoGCCqGSM49
**************************4xz0SHsuQc/7XBmgmrMpAmE80c0DR
5HcMHFxRPtGLv22T62e5KqN1W3uN9Hplgg==
-----END EC PRIVATE KEY-----
```

2.创建证书

2.1. 概述

配置HTTPS监听，您可以直接使用SSL证书服务中的证书或者将所需的第三方签发的服务器证书和CA证书上传到负载均衡。上传后，无需在后端服务器再配置证书。

负载均衡支持两种来源的证书：

- 在阿里云SSL证书服务中签发或托管的证书：从阿里云SSL证书服务选择，可实现证书到期提醒和一键续期。

  暂未支持客户端CA证书。

- 第三方签发的证书：上传第三方签发证书，您需要持有证书的公钥/私钥文件。

  支持HTTPS服务器证书及客户端CA证书。

在创建证书前，注意：

- 如果一个证书要在多个地域使用，那么创建证书时就需要选择多个地域。
- 每个账号最多可以创建100个证书。

2.2. 选择阿里云签发证书

阿里云提供的证书签发服务是指在云上签发各品牌数字证书，实现网站HTTPS化，使网站具备可信、防劫持、防篡改和防监听等特点，并对证书进行统一生命周期管理，简化证书部署。

前提条件

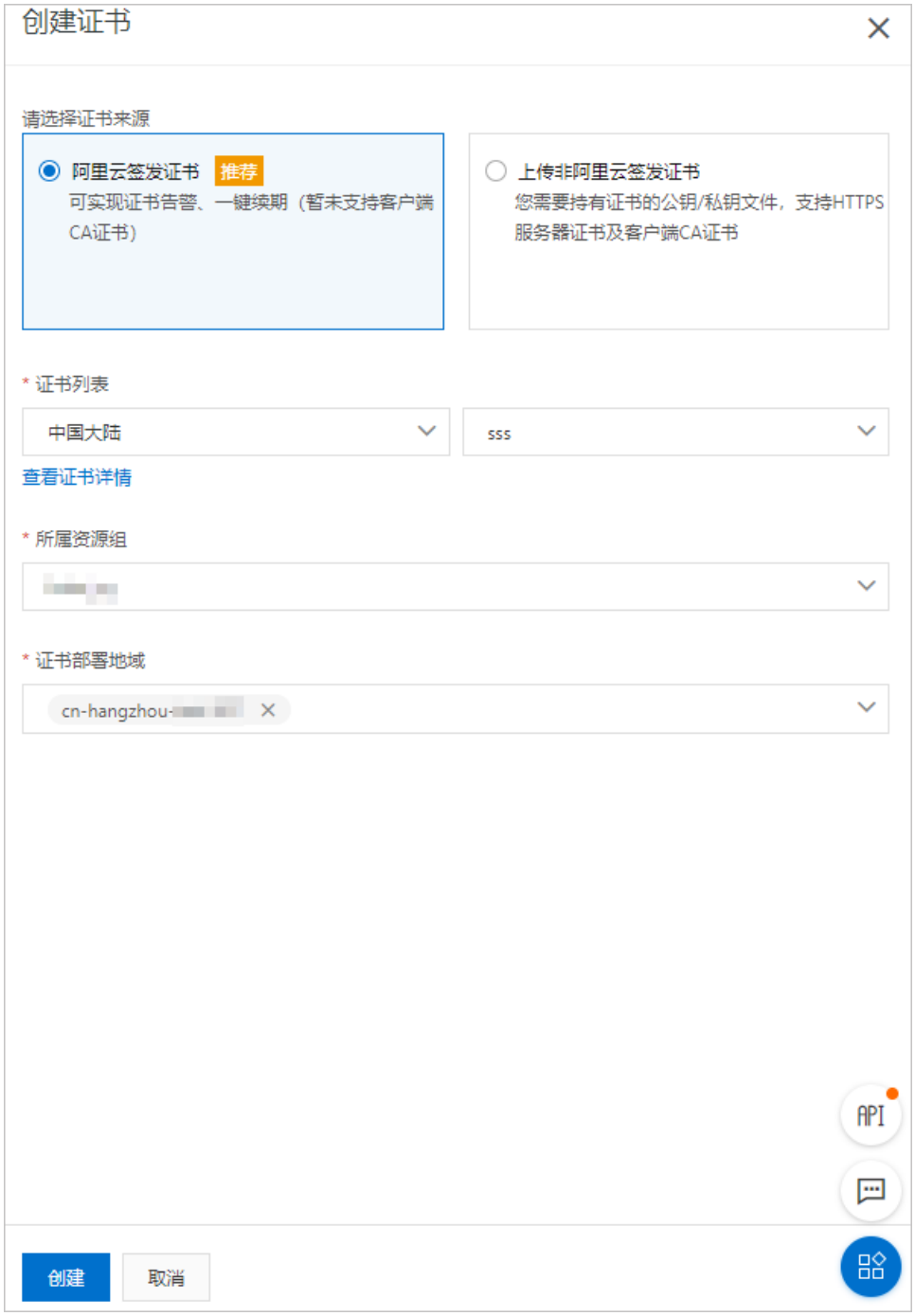
如果您需要使用SSL证书服务中的证书，您需要登录SSL证书控制台，购买证书或者上传第三方证书到SSL证书服务。

背景信息

SSL证书服务详情请参见SSL证书。

操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击**证书管理**。
3. 在**证书管理**页面，单击**创建证书**。
4. 在**创建证书**页面，选择**阿里云签发证书**，设置证书部署地域、所属资源并从证书列表中选择使用的SSL证书。证书不支持跨地域使用。如果该证书需要在多个地域使用，选择所有需要的地域。



5. 单击**创建**。

相关文档

- UploadServerCertificate

2.3. 上传非阿里云签发证书

上传非阿里云签发证书，您需要持有证书的公钥或私钥文件。

前提条件

上传非阿里云签发证书前，您必须：

- 已经购买了服务器证书。
- 已经生成了CA证书和客户端证书，详情请参见生成CA证书。

操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击**证书管理**。
3. 单击**创建证书**。
4. 在**创建证书**页面，选择**上传非阿里云签发证书**。

5. 在**上传非阿里云签发证书**页签下，上传证书内容。

配置	说明
证书名称	输入证书名称。 名称在1~80个字符之间，只能包含字母、数字和以下特殊符号：冒号（:）、下划线（_）、斜杠（/）、点号（.）和连接号（-）。
所属资源组	选择证书所属的资源组。
证书部署地域	选择证书的地域。 证书不支持跨地域使用。如果该证书需要在多个地域使用，选择所有需要的地域。
证书类型	选择要上传的证书类型： ○ **服务器证书**：配置HTTPS单向认证，只需要上传服务器证书和私钥。 ○ **CA证书**：配置HTTPS双向认证，除了上传服务器证书外，还需要上传CA证书。
公钥证书	复制服务器或者CA证书内容，公钥证书包含证书的公钥和签名等信息。 负载均衡使用NGINX格式的证书，通常从证书提供商获取到的NGINX格式的证书文件，以.pem为后缀，也有可能以.crt或其他为后缀。 单击**查看样例**查看正确的证书样式。详情参见证书要求。

配置	说明
私钥	复制服务器证书的私钥内容，通常从证书提供商获取到NGINX格式的证书文件，以.key为后缀。 单击**查看样例**查看正确的证书样式。详情参见证书要求。 负载均衡支持以下两种格式的私钥： -----BEGIN RSA PRIVATE KEY----- 证书私钥(BASE64编码) -----END RSA PRIVATE KEY----- 或者： -----BEGIN EC PARAMETERS----- 证书私钥(BASE64编码) -----END EC PARAMETERS----- -----BEGIN EC PRIVATE KEY----- 证书私钥(BASE64编码) -----END EC PRIVATE KEY----- **注意** ○ 只有上传服务器证书时，才需要上传私钥。 ○ EC格式的密钥目前支持的地域如下： ■ 英国（伦敦） ■ 华北1（青岛） ■ 华北5（呼和浩特） ■ 西南1（成都） ■ 日本（东京） ■ 印度（孟买） ■ 澳大利亚（悉尼） ■ 马来西亚（吉隆坡） ■ 美国（硅谷） ■ 美国（弗吉利亚） ■ 德国（法兰克福） ■ 阿联酋（迪拜）

6. 单击**新建**。

相关文档

相关文档

- UploadCACertificate

- UploadServerCertificate

3.生成CA证书

在配置HTTPS监听时，您可以使用自签名的CA证书，并且使用该CA证书为客户端证书签名。

使用Open SSL生成CA证书

1. 执行以下命令，在 /root 目录下新建一个ca文件夹，并在ca文件夹下创建四个子文件夹。

```
sudo mkdir ca
cd ca
sudo mkdir newcerts private conf server
```

   - newcerts目录将用于存放CA签署过的数字证书。
   - private目录用于存放CA的私钥。
   - conf目录用于存放一些简化参数用的配置文件。
   - server目录存放服务器证书文件。

2. 在 conf 目录下新建一个包含以下信息的openssl.conf文件。

```
[ ca ]
default_ca = foo
[ foo ]
dir = /root/ca
database = /root/ca/index.txt
new_certs_dir = /root/ca/newcerts
certificate = /root/ca/private/ca.crt
serial = /root/ca/serial
private_key = /root/ca/private/ca.key
RANDFILE = /root/ca/private/.rand
default_days = 365
default_crl_days= 30
default_md = md5
unique_subject = no
policy = policy_any
[ policy_any ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = match
localityName = optional
commonName     = supplied
emailAddress   = optional
```

3. 执行以下命令，生成私钥Key文件。

```
cd /root/ca
sudo openssl genrsa -out private/ca.key
```

执行结果如下图所示。

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca/conf# cd /root/ca
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....+++
..+++
e is 65537 (0x10001)
```

4. 执行以下命令，按照提示输入所需信息，然后按下回车键生成证书请求csr文件。

```
sudo openssl req -new -key private/ca.key -out private/ca.csr
```

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl req -new -key private/ca.key -ou
t private/ca.csr
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) [AU]:CN
State or Province Name (full name) [Some-State]:ZheJiang
Locality Name (eg, city) []:HangZhou
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alibaba
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:mydomain
Email Address []:a@alibaba.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@iZbp1hfvivcqx1jbwap31iZ:~/ca#
```

> 说明
>
> Common Name需要输入负载均衡的域名。

5. 执行以下命令，生成凭证crt文件。

```
sudo openssl x509 -req -days 365 -in private/ca.csr -signkey private/ca.key -out private/ca.crt
```

6. 执行以下命令，为CA的Key设置起始序列号，可以是任意四个字符。

```
sudo echo FACE > serial
```

7. 执行以下命令，创建CA键库。

```
sudo touch index.txt
```

8. 执行以下命令，为移除客户端证书创建一个证书撤销列表。

```
sudo openssl ca -gencrl -out /root/ca/private/ca.crl -crldays 7 -config "/root/ca/conf/openssl.conf"
```

输出为：

```
Using configuration from /root/ca/conf/openssl.conf
```

为客户端证书签名

1. 执行以下命令，在 `ca` 目录内创建一个存放客户端Key的目录 `users` 。

```
sudo mkdir users
```

2. 执行以下命令，为客户端创建一个Key。

```
sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

> **说明**
>
> 创建Key时要求输入pass phrase，这个是当前Key的口令，以防止本密钥泄漏后被人盗用。两次输入同一个密码。

3. 执行以下命令，为客户端Key创建一个证书签名请求csr文件。

```
sudo openssl req -new -key /root/ca/users/client.key -out /root/ca/users/client.csr
```

输入该命令后，根据提示输入STEP 2中输入的pass phrase，然后根据提示输入对应的信息。

> **说明**
>
> A challenge password是客户端证书口令。注意将它和client.key的口令进行区分。

4. 执行以下命令，使用CA证书的Key为客户端Key签名。

```
sudo openssl ca -in /root/ca/users/client.csr -cert /root/ca/private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/users/client.crt -config "/root/ca/conf/openssl.conf"
```

当出现确认是否签名的提示时，两次都输入*y*。

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl ca -in /root/ca/users/client.csr
 -cert /root/ca/private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/us
ers/client.crt -config "/root/ca/conf/openssl.conf"
Using configuration from /root/ca/conf/openssl.conf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :ASN.1 12:'ZheJiang'
localityName          :ASN.1 12:'HangZhou'
organizationName      :ASN.1 12:'Alibaba'
organizationalUnitName:ASN.1 12:'Test'
commonName            :ASN.1 12:'mydomain'
emailAddress          :IA5STRING:'a@alibaba.com'
Certificate is to be certified until Jun  4 15:28:55 2018 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@iZbp1hfvivcqx1jbwap31iZ:~/ca#
```

5. 执行以下命令，将证书转换为PKCS12文件。

```
sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt -inkey /root/ca/users/client.key -out /r
oot/ca/users/client.p12
```

按照提示输入客户端client.key的pass phrase。再输入用于导出证书的密码。这个是客户端证书的保护密码，在安装客户端证书时需要输入这个密码。

6. 执行以下命令，查看生成的客户端证书。

```
cd users
ls
```

4.转换证书格式

负载均衡只支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到负载均衡。建议使用Open SSL进行转换。

DER转换为PEM

DER格式通常使用在Java平台中，证书文件后缀一般为*.der*、*.cer*或者*.crt*。

- 运行以下命令进行证书转化：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

- 运行以下命令进行私钥转化：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

P7B转换为PEM

P7B格式通常使用在Windows Server和Tomcat中。

运行以下命令进行证书转化：

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

PFX转换为PEM

PFX格式通常使用在Windows Server中。

- 运行以下命令提取证书：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

- 运行以下命令提取私钥：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

5.替换证书

为避免证书过期对您的服务产生影响，请在证书过期前替换证书。

操作步骤

1. 新建并上传一个新的证书。 详情请参见概述。
2. 在HTTPS监听中配置新的证书。 详情请参见添加HTTPS监听。
3. 打开**证书管理**页面，找到过期目标证书，然后单击**删除**。
4. 在弹出的对话框中，单击**确认**。

6.批量替换证书

您可以通过批量替换证书功能批量更新监听或扩展域名上的证书，一键替换即将过期的证书。

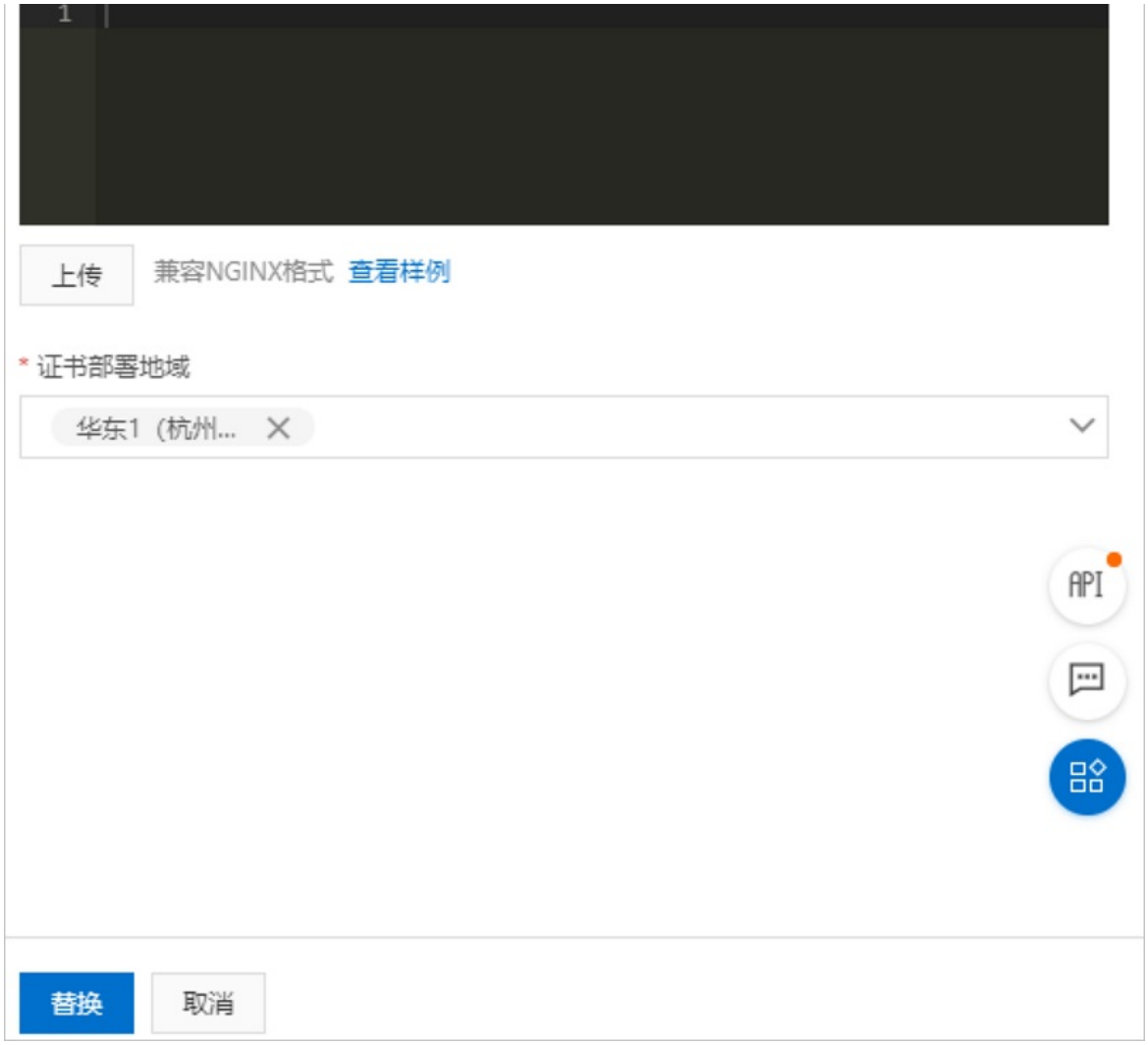
操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击**证书管理**。
3. 在**证书管理**页面，单击需要替换证书**操作**列的**替换**。

   > **说明** 至少关联了一个监听或者域名扩展的证书才能被替换。

4. 在**替换服务器证书**页面，修改证书。相关参数配置说明如下表所示。

参数	说明
替换方式为**新建一个证书并替换**	
选择阿里云签发证书	选择**证书部署地域**和**所属资源组**，在**证书列表**选择新的证书。
上传非阿里云签发证书	选择第三方签发证书，详细配置说明请参见上传非阿里云签发证书。
替换方式为**使用已有证书替换**	
选择用来替换的服务器证书	在已有证书列表中选择用来替换的服务器证书。



5. 单击**替换**。
6. 单击**去证书列表查看**，在**证书管理**页面，可以查看关联监听或者扩展域名对应的证书变成新替换的证书。