Alibaba Cloud Server Load Balancer

Certificate management

Issue: 20190816

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Certificate requirements

Server Load Balancer (SLB) only supports certificates in the PEM format. Before you upload a certificate, make sure that the certificate content, certificate chain, and private key conform to the corresponding format requirements.

Certificates issued by a root CA

If the certificate is issued by a root CA, the received certificate is the only one required to be uploaded to SLB. In this case, the website that is configured with the certificate will be regarded as a trusted website and does not require additional certificates.

The certificate format must meet the following format requirements:

- The certificate must start with `----- BEGIN CERTIFICAT E -----`, and end with `----- END CERTIFICAT E -----`, and both parts must be uploaded together.
- Each line except the last line must contain exactly 64 characters. The last line can contain 64 or fewer characters.
- Spaces are not allowed in the certificate content.

The following is a sample certificate issued by a root CA.

Certificates issued by an intermediate CA

If the certificate is issued by an intermediate CA, you are able to obtain multiple intermediate certificates. You must upload both the server certificate and the required number of immediate certificates to SLB.

The format of the certificate chain must meet the following requirements:

- Paste the server certificate content first, and then paste the content of the one or more required intermediate certificates directly underneath without any blank lines in between the certificates.
- Spaces are not allowed in the content.
- Blank lines are not allowed in the content. Each line must contain exactly 64 characters. For more information, see RFC1421.
- The certificate must conform to the corresponding format requirements. Generally , the intermediate CA will provide instructions about the certificate format when issuing the certificate. The certificate chain must conform to the format requirements.

The following is a sample certificate chain.

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

RSA private keys

When you upload the server certificate, you also need to upload the private key of the certificate.

The RSA private key format must meet the following requirements:

- The private key must start with `-----BEGIN RSA PRIVATE KEY-----`, and end with `-----END RSA PRIVATE KEY-----`, and both parts must be uploaded together.
- Blank lines are not allowed in the content. Each line except the last line must contain exactly 64 characters. The last line can contain 64 or fewer characters. For more information, see RFC1421.

If your private key is encrypted (for example, the content at the beginning and end of the private key is `-----BEGIN PRIVATE KEY-----`, `-----END PRIVATE KEY-----` or `-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----END ENCRYPTED PRIVATE KEY-----`, or the private key contains `Proc-Type: 4,ENCRYPTED`), you must first run the following command to convert the private key:

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

The following is a sample RSA private key.

EC private key

> **Note:**
> Currently, EC private keys are supported only in the UK (London) region.

When you upload the server certificate, you also need to upload the private key of the certificate.

The EC private key format must meet the following requirements:

- The private key must start with `----- BEGIN EC PARAMETERS -----`, and end with -----END EC PARAMETERS-----, and both parts must be uploaded together.
- Blank lines are not allowed in the content. Each line except the last line must contain exactly 64 characters. The last line can contain 64 or fewer characters. For more information, see RFC1421.

If your private key is encrypted (for example, the content at the beginning and end of the private key is `----- BEGIN EC PRIVATE KEY -----`, `----- END`

`EC PRIVATE KEY -----`, or the private key contains `Proc-Type: 4,ENCRYPTED`), you must first run the following command to convert the private key:

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

The following is a sample EC private key.

```
-----BEGIN EC PARAMETERS-----
Bggq**********Bw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIC o9b+vQUhqFUWgW jE0YY4h0b3 bE/udcubxVwcV
Y99MuoAoGC CqGSM49
AwEHoUQDQg AEgpla3Bj9 rX**********4xz0SHsuQc/7XBmgmrMpA
mE80c0DR
5HcMHFxRPt GLv22T62e5 KqN1W3uN9H plgg==
-----END EC PRIVATE KEY-----
```

2 Create a certificate

2.1 Create a certificate

To configure an HTTPS listener, you can directly use a certificate from Alibaba Cloud SSL Certificate Service or upload a third-party server certificate and CA certificate to Server Load Balancer (SLB). After you upload the certificate to SLB, you do not need to configure certificates on backend servers.

SLB supports certificates from the following two sources:

- Certificates issued or hosted by Alibaba Cloud SSL Certificate Service: You can select the required certificate from Alibaba Cloud SSL Certificate Service. When the certificate is about to expire, Alibaba Cloud will send alerts notifying you to renew the certificate to ensure its validity.

  Currently client CA certificates are not supported.
- Third-party certificates: To upload a third-party certificate, you must have the public key and private key files of the certificate.

  HTTPS server certificates and client CA certificates are supported.

Before you create a certificate, note the following:

- If you need to use a certificate in multiple regions, you must select all the required regions when creating the certificate.
- Each Alibaba Cloud account can create up to 100 certificates.

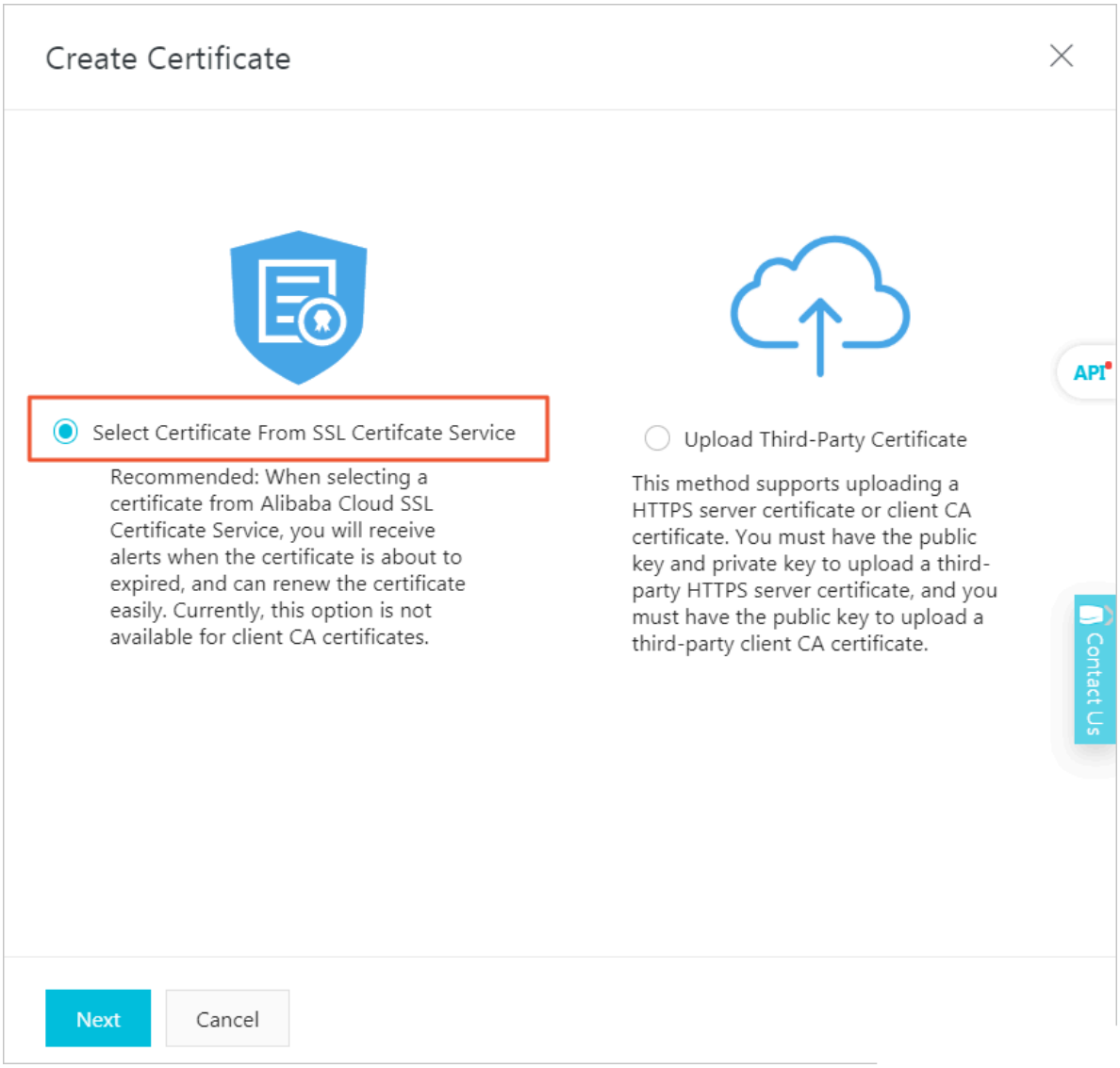
Select a certificate from SSL Certificate Service

Alibaba Cloud SSL Certificate Service issues digital certificates of a variety of authorities to provide HTTPS services. Additionally, Alibaba Cloud SSL Certificate Service can uniformly manage the life cycles of certificates to simplify certificate deployment. For more information, see SSL certificate service.

To use a certificate in SSL Certificate Service, you must log on to the SSL Certificate console to buy a certificate or upload a third-party certificate to SSL Certificate Service.

To use a certificate from SSL Certificate Service, follow these steps:

1. Log on to the SLB console.
2. In the left-side navigation pane, click Certificates.
3. Click Create Certificate. On the Create Certificate page, select Select Certificate From SSL Certificate Service.



4. Click Next. On the Select Certificate From SSL Certificate Service page, select the region to deploy the certificate and then select the SSL certificate to use from the certificate list.

   A certificate cannot be used across regions. If you need to use a certificate in multiple regions, you must select all the required regions.
5. Click OK.

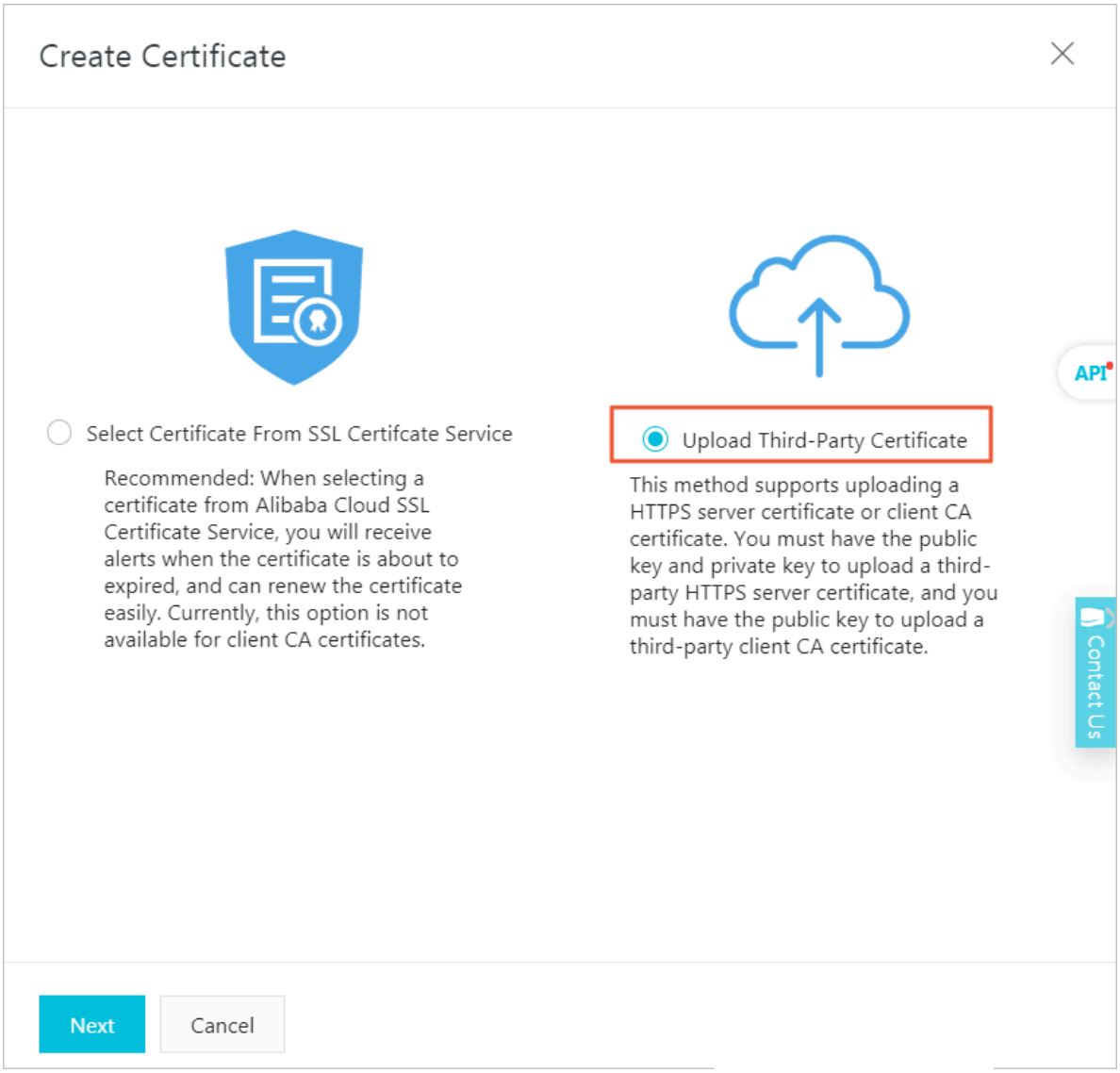
Upload a third-party certificate

Before you upload a third-party certificate, make sure that the following conditions are met:

- A server certificate is purchased.
- A CA certificate and a client certificate are generated. For more information, see #unique_6.

To upload a third-party certificate to SLB, follow these steps:

1. Log on to the SLB console.
2. In the left-side navigation pane, click Certificates.
3. Click Create Certificate.
4. On the Create Certificate page, select Upload Third-Party Certificate.



5. Click Next. On the Upload Third-Party Certificate page, upload the certificate content.

Configuration	Description
Certificate Name	Enter a name for the certificate to be uploaded. The name must be 1 to 80 characters in length, and can contain letters, numbers, and the following special characters: _ / . -
Regions	Select one or more regions to which the certificate to be uploaded belongs. A certificate cannot be used across regions. If you need to use a certificate in multiple regions, you must select all the required regions.
Certificate Type	Select the type of the certificate to be uploaded: · Server Certificate: For HTTPS one-way authentication, only the server certificate and the private key are required. · CA Certificate: For HTTPS mutual authentication, both the server certificate and the CA certificate are required.
Certificate Content	Paste the certificate content into the text editor. Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_7.

Configuration	Description

Private Key	Paste the private key of the server certificate into the text editor.
	Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_7.
	SLB supports the following two private key formats:
	`----- BEGIN RSA PRIVATE KEY -----`
	`Private key content ( BASE64 encoding )`
	`----- END RSA PRIVATE KEY -----`
	or
	`----- BEGIN EC PARAMETERS -----`
	`Private key content ( BASE64 encoding )`
	`----- END EC PARAMETERS -----`
	`----- BEGIN EC PRIVATE KEY -----`
	`Private key content ( BASE64 encoding )`
	`----- END EC PRIVATE KEY -----`
	Notice:
	· A private key is required only when you upload a server certificate.
	· Currently, EC private keys are supported only in the UK (London) region.

6. Click OK.

2.2 Select a certificate from Alibaba Cloud SSL Certificates Service

Alibaba Cloud SSL Certificates Service issues digital certificates of a variety of authorities to provide HTTPS services which are reliable and protect websites from being hijacked, tampered with, or listened to. Through Alibaba Cloud SSL Certificates Service, you can manage the life cycles of certificates in a centralized way to simplify certificate deployment.

Prerequisites

To use a certificate in SSL Certificates Service, you must log on to the SSL Certificate console to buy a certificate or upload a third-party certificate to SSL Certificates Service.

Context

For more information about SSL Certificates Service, see SSL Certificates Service.

Procedure

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, click Certificates.
3. Click Create Certificate. On the Create Certificate page, select Select Certificate From SSL Certificate Service.

4. Click Next. On the Select Certificate From SSL Certificate Service page, select the region to deploy the certificate and then select the SSL certificate to use from the certificate list.

   A certificate cannot be used across regions. If you need to use a certificate in multiple regions, you must select all the required regions.
5. Click OK.

More information
#unique_9

2.3 Upload a third-party certificate

Before you upload a third-party certificate, you must obtain the public and private key file of the certificate.

Prerequisites

Before you upload a third-party certificate, make sure that the following conditions are met:

- A server certificate is purchased.
- A CA certificate and a client certificate are generated. For more information, see #unique_11.

Procedure

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, choose Certificates.
3. Click Create Certificate.

4. On the Create Certificate page, select Upload Third-Party Certificate.

5. Click Next. On the Upload Third-Party Certificate page, upload the certificate.

Configuration	Description
Certificate Name	Enter a name for the certificate to be uploaded. The name must be 1 to 80 characters in length, and can only contain letters, numbers, and the following special characters: _ / . -
Regions	Select one or more regions to which the certificate to be uploaded belongs. A certificate cannot be used across regions. If you need to use a certificate in multiple regions, select all the required regions.
Certificate Type	Select the type of the certificate to be uploaded: · Server Certificate: For HTTPS one-way authentication, only the server certificate and the private key are required. · CA Certificate: For HTTPS mutual authentication, both the server certificate and the CA certificate are required.
Certificate Content	Paste the certificate content into the text editor. Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_12.

Configuration	Description

Private Key	Paste the private key of the server certificate into the text editor.
	Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_12.
	SLB supports the following two private key formats:
	`----- BEGIN RSA PRIVATE KEY -----`
	`Private key content ( BASE64 encoding )`
	`----- END RSA PRIVATE KEY -----`
	or
	`----- BEGIN EC PARAMETERS -----`
	`Private key content ( BASE64 encoding )`
	`----- END EC PARAMETERS -----`
	`----- BEGIN EC PRIVATE KEY -----`
	`Private key content ( BASE64 encoding )`
	`----- END EC PRIVATE KEY -----`
	Notice:
	· A private key is required only when you upload a server certificate.
	· Currently, keys in the EC format are supported in the following regions:
	- UK (London)
	- China (Qingdao)
	- China (Hohhot)
	- China (Chengdu)
	- Japan (Tokyo)
	- India (Mumbai)
	- Australia (Sydney)
	- Malaysia (Kuala Lumpur)
	- US (Silicon Valley)
	- US (Virginia)
	- Germany (Frankfurt)
	- UAE (Dubai)

6. Click OK.

#unique_13
#unique_9

3 Upload a certificate

Before you create an HTTPS listener, you must upload the required server certificate and CA certificate to SLB. You no longer need to configure certificates on backend servers after uploading the certificates to SLB.

Prerequisites

- A server certificate is purchased.
- A CA certificate and a client certificate are generated. For more information, see #unique_6.

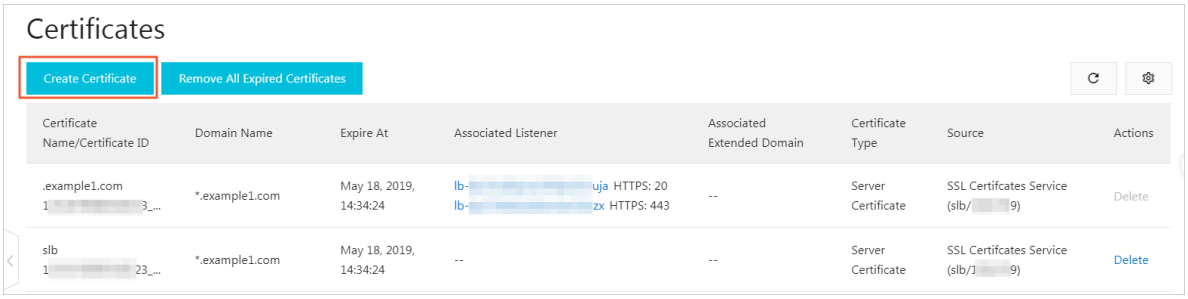
Context

Before you upload a certificate, note the following:

- If you want to use a certificate in multiple regions, you must select all the required regions.
- Up to 100 certificates can be uploaded under one account.

Procedure

1. Log on to the SLB console.
2. In the left-side navigation pane, choose Certificates.
3. Click Create Certificate.



4. On the Create Certificate page, upload the certificate and then click OK.

Configuration	Description
Certificate Name	Enter a name for the certificate to be uploaded. The name must be 1 to 80 characters in length, and can only contain letters, numbers, and the following special characters: _ / . -
Regions	Select one or more regions to which the certificate to be uploaded belongs. A certificate cannot be used across regions. If you need to use a certificate in multiple regions, select all the required regions.
Certificate Type	Select the type of the certificate to be uploaded: · Server Certificate: For HTTPS one-way authentication, only the server certificate and the private key are required. · CA Certificate: For HTTPS mutual authentication, both the server certificate and the CA certificate are required.
Certificate Content	Paste the certificate content in the editor. Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_7.
Private Key	Paste the private key of the server certificate in the editor. Click View Sample Certificate to view the valid certificate formats. For more information, see #unique_7.  Notice: A private key is required only when you upload a server certificate.

To delete expired certificates in batches, click Remove All Expired Certificates.

4 Generate a CA certificate

When configuring HTTPS listeners, you can use self-signed CA certificates. Follow the instructions in this document to generate a CA certificate and use the CA certificate to sign a client certificate.

Generate a CA certificate by using Open SSL

1. **Run the following commands to create a *ca* folder in the */ root* directory and then create four sub folders under the *ca* folder.**

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

   - ***newcerts* is used to store the digit certificate signed by a CA certificate.**
   - ***private* is used to store the private key of the CA certificate.**
   - ***conf* is used to store the configuration files.**
   - ***server* is used to store the server certificate.**

2. **Create an *openssl . conf* file that contains the following information in the *conf* directory.**

```
[ ca ]
default_ca = foo
[ foo ]
dir = / root / ca
database = / root / ca / index . txt
new_certs_ dir = / root / ca / newcerts
certificat e = / root / ca / private / ca . crt
serial = / root / ca / serial
private_ke y = / root / ca / private / ca . key
RANDFILE = / root / ca / private /. rand
default_da ys = 365
default_cr l_days = 30
default_md = md5
unique_sub ject = no
policy = policy_any
[ policy_any ]
countryNam e = match
stateOrPro vinceName = match
organizati onName = match
organizati onalUnitNa me = match
localityNa me = optional
commonName = supplied
emailAddre ss = optional
```

3. **Run the following command to generate a private key.**

```
$ cd / root / ca
```

```
$ sudo openssl genrsa -out private/ca.key
```

The following figure is an example of key generation.

```
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. Run the following command and input the required information according to the prompts. Press Enter to generate a *csr* file.

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

Note:

Common Name is the domain name of the SLB instance.

```
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#
```

5. Run the following command to generate a *crt* file.

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

6. Run the following command to set the start sequence number for the private key, which can be any four characters.

```
$ sudo echo FACE > serial
```

7. Run the following command to create a CA key library.

```
$ sudo touch index.txt
```

8. Run the following command to create a certificate revocation list for removing the client certificate.

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

The response is as follows:

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

Sign the client certificate

1. Run the following command to generate a *users* folder under the *ca* directory to store the client key.

```
$ sudo mkdir users
```

2. Run the following command to create a key for the client certificate.

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

> **Note:**
> Enter a pass phrase when creating the key. It is the password to protect the private key from unauthorized access. The pass phrase entered is the password for this key.

3. Run the following command to create a *csr* file for requesting certificate sign.

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

Enter the pass phrase set in the previous step when prompted.

> **Note:**
> A challenge password is the password of the client certificate. Note that it is not the password of the client key.

4. Run the following command to sign the client key.

```
$ 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"
```

Enter y twice when prompted.

```
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. Run the following command to convert the certificate to a *PKCS12* file.

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

Enter the password of the client key when prompted. Then, enter the password used for exporting the client certificate. This password is used to protect the client certificate, which is required when installing the client certificate.

6. **Run the following command to view the generated client certificate.**

```
cd   users
ls
```

5 Convert the certificate format

Server Load Balancer supports PEM certificates only. Certificates in other formats must be converted to the PEM format before they can be uploaded to Server Load Balancer. We recommend that you use Open SSL for conversion.

Convert DER to PEM

DER: This format is usually used on a Java platform. The certificate file suffix is generally . *der* , . *cer* , or . *crt* .

- Run the following command to convert the certificate format:

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

-
- Run the following command to convert the private key:

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

Convert P7B to PEM

P7B: This format is usually used in a Windows server and Tomcat.

Run the following command to convert the certificate format:

```
openssl pkcs7 - print_cert s - in incertific ate . p7b - out
  outcertifi cate . cer
```

Convert PFX to PEM

PFX: This format is usually used in a Windows server.

- Run the following command to extract the certificate:

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

- Run the following command to extract the private key:

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

6 Replace a certificate

To avoid the impact of certificate expiration on your service, we recommend that you replace the certificate before the certificate expires.

Procedure

1. Create and upload a new certificate.

   For more information, see #unique_6 and #unique_18.
2. Configure the new certificate in HTTPS listener configuration.

   For more information, see #unique_19.
3. On the Certificates page, find the target certificate, and then click Delete.
4. In the displayed dialog box, click OK.