ALIBABA CLOUD

Alibaba Cloud

Server Load Balancer

Certificate management

Document Version: 20220427

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Certificate requirements

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

Certificates issued by a root CA

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

The certificate must meet the following format requirements:

- The certificate must start with `-----BEGIN CERTIFICATE-----` and end with -----END CERTIFICATE-----.
- Each line (except the last line) must contain 64 characters. The last line can contain 64 or fewer characters.
- The certificate content cannot contain spaces.

Certificates issued by an intermediate CA

If the certificate was issued by an intermediate CA, the received certificate file contains multiple certificates. You must upload both the server certificate and the required intermediate certificates to SLB.

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

- The server certificate must be put first and the content of the one or more required intermediate certificates must be put underneath without blank lines between the certificates.
- The certificate content cannot contain spaces.
- Blank lines are not allowed between the certificates. Each line must contain 64 characters. For more information, see RFC1421.
- Certificates must meet the corresponding format requirements. In most cases, the intermediate CA provides instructions about the certificate format when certificates are issued. The certificates must meet the format requirements.

The following section provides a sample certificate chain:

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

Public keys of certificates

SLB supports the following public key algorithms:

- RSA 1024
- RSA 2048
- RSA 4096

- ECDSA P-256
- ECDSA P-384
- ECDSA P-521

RSA private keys

When you upload a server certificate, you must upload the private key of the certificate.

An RSA private key must meet the following format requirements:

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

You may use an encrypted private key. For example, the private key starts with `----BEGIN PRIVATE KEY-----` and ends with -----END PRIVATE KEY-----, or starts with `-----BEGIN ENCRYPTED PRIVATE KEY-----` and ends with -----END ENCRYPTED PRIVATE KEY-----. The private key may also contain `Proc-Type: 4,ENCRYPTED`. In this case, you must first run the following command to convert the private key:

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

2.Create a certificate

2.1. Overview

When you configure an HTTPS listener, you can use a certificate from Certificate Management Service or upload a third-party server certificate and certification authority (CA) certificate to .

supports the following certificates:

- Certificates issued and hosted by Alibaba Cloud Certificate Management Service: After you purchase a certificate from Certificate Management Service, you will be notified when the certificate is about to expire. You can renew the certificate with one click.

  Client CA certificates are not supported.

- Third-party certificates: To upload a third-party certificate, you need the public key and private key files of the certificate.

  Server certificates and client CA certificates are supported.

Before you create a certificate, take note of the following rules:

- If you want to use a certificate in multiple regions, you must select all of the required regions when you create the certificate.
- Each region supports at most 100 server certificates.
- Each region supports at most 100 client CA certificates.

2.2. Use a certificate from Alibaba Cloud SSL Certificates Service

This topic describes how to use a certificate from Alibaba Cloud SSL Certificates Service when you specify a certificate for Classic Load Balancer (CLB) instances. To provide reliable HTTPS services, Alibaba Cloud SSL Certificates Service offers digital certificates that are issued by different authorities. This prevents eavesdropping, tampering, and man-in-the-middle (MITM) attacks. You can use Alibaba Cloud SSL Certificates Service to manage the lifecycle of different certificates and efficiently deploy certificates.

Prerequisites

To use a certificate from SSL Certificates Service, you must log on to the SSL Certificates Service console. Then, you can purchase a certificate or upload a certificate issued by a third party to SSL Certificates Service.

Context

For more information, see SSL Certificates Service.

Procedure

1.
2.
3. In the left-side navigation pane, choose **CLB (Formerly Known as SLB) > Certificates**.

4. On the **Certificates** page, click **Create Certificate**.
5. In the **Create Certificate** panel, select **Alibaba Cloud Certificates**, select the region where the certificate is deployed, and select the resource group to which the certificate belongs. Then, select the certificate from the Certificates drop-down list.

   Certificates cannot be deployed across regions. If you want to deploy a certificate across regions, you must specify the regions where you want to deploy the certificate.
6. Click **Create**.

Related information

- UploadServerCertificate

2.3. Upload a third-party certificate

This topic describes how to upload a third-party certificate. You must obtain the public key or private key file of the certificate before you can upload a third-party certificate.

Prerequisites

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

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

Procedure

1.
2.
3. In the left-side navigation pane, choose **CLB (Formerly Known as SLB) > Certificates**.
4. On the **Certificates** page, click **Create Certificate**.
5. In the **Create Certificate** panel, select **Upload Third-party Certificate**.
6. After you select **Upload Third-party Certificate**, configure the certificate.

Parameter	Description
Certificate Name	Enter a name for the certificate. The name must be 1 to 80 characters. The name can contain only letters, digits, hyphens (-), forward slashes (/), periods (.), underscores (_), and asterisks (*).
Resource Group	Select the resource group to which the certificate belongs.
Certificate Type	Select the type of certificate that you want to upload. ○ **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.

Parameter	Description
Public Key Certificate	Paste the contents of the server certificate or CA certificate into the field. The public key certificate contains the public key and signature information. SLB instances use NGINX certificates obtained from a certificate provider. In most cases, NGINX certificates are suffixed with .pem, and some certificates may be suffixed with .crt. Click **Example** to view the valid certificate formats. For more information, see Certificate requirements.

Parameter	Description

Private Key	Paste the private key of the server certificate into the field. In most cases, NGINX certificates are obtained from a certificate provider and are suffixed with .key.
	Click **Example** to view the valid certificate formats. For more information, see Certificate requirements.
	SLB supports the following private key formats:
	`-----BEGIN RSA PRIVATE KEY-----`
	`Private key (Base64 encoded)`
	`-----END RSA PRIVATE KEY-----`
	and
	`-----BEGIN EC PARAMETERS-----`
	`Private key (Base64 encoded)`
	`-----END EC PARAMETERS-----`
	`-----BEGIN EC PRIVATE KEY-----`
	`Private key (Base64 encoded)`
	`-----END EC PRIVATE KEY-----`
	Notice
	◦ A private key is required only when you upload a server certificate.
	◦ Regions that support Elliptic Curve (EC) keys:
	▪ 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)

Parameter	Description
Region	Select the region where you want to deploy the certificate. A certificate cannot be used across regions. If you want to use the certificate in multiple regions, select the regions where you want to use the certificate.

7. Click **Create**.

Related information

References

- UploadCACertificate
- UploadServerCertificate

3.Generate a CA certificate

When you configure an HTTPS listener, you can use a self-signed CA certificate. You can also use the CA certificate to sign a client certificate.

Generate a CA certificate by using OpenSSL

1. Run the following commands to create a ca folder in the `/root` directory and then create four subfolders under the ca folder:

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

   - The newcerts folder is used to store the digital certificate signed by the CA certificate.
   - The private folder is used to store the private key of the CA certificate.
   - The conf folder is used to store the configuration files used for simplifying parameters.
   - The server folder 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
   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. Run the following commands to generate a private key:

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

   The following figure shows the command output.

4. Run the following command, enter the required information as prompted, and then press Enter to generate a .csr file.

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

> **Note**
>
> Common Name specifies the domain name of the Classic Load Balancer (CLB) instance.

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 privat
e/ca.crt
```

6. Run the following command to set the initial sequence number of the CA key. The key 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"
```

Output:

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

Sign the client certificate

1. Run the following command to create the `users` directory in the `ca` directory to store client keys:

```
sudo mkdir users
```

2. Run the following command to create a client key:

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

> **Note**
>
> When you create the key, enter a passphrase to prevent unauthorized access. Enter the same password twice.

3. Run the following command to create a .csr file for the client key:

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

Enter the passphrase in Step 2 and other required information as prompted.

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

4. Run the following command to use the CA key 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* when you are prompted to confirm the following two operations.

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 passphrase of the client key as prompted and press Enter. Then, enter the password used to export the client certificate. This password is used to protect the client certificate and is required when the client certificate is installed.

6. Run the following commands to view the generated client certificate:

```
cd users
ls
```

4.Convert the certificate format

Server Load Balancer (SLB) supports PEM certificates only. Certificates in other formats must be converted to the PEM format before they can be uploaded to SLB. 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_certs -in incertificate.p7b -out outcertificate.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
```

5.Replace a certificate

This topic describes how to replace a certificate with a new certificate. We recommend that you replace certificates before they expire to avoid service interruption.

Procedure

1. Click the ID of the Server Load Balancer (SLB) instance for which you want to replace the certificate and select the **Listener** tab.
2. Find the HTTPS listener for which you want to replace the certificate and click **Manage Certificate** in the **Actions** column.
3. On the **Manage Certificate** page, select Add Server Certificate.

   You can also select **Create Server Certificate** or **Purchase Certificate**. For more information about how to create a server certificate, see Overview.
4. On the **Advanced Settings** tab, click **Modify** and select whether to enable mutual authentication and TLS security policy. For more information, see Add an HTTPS listener.
5. Click **OK**.
6. On the **Certificates** page, find the expired certificate and click **Delete**.
7. In the message that appears, click **OK**.

   > **Note** If the certificate is associated with another listener, it cannot be deleted.

Related information

- Add an HTTPS listener
- Replace multiple certificates at a time

6.Replace multiple certificates at a time

This topic describes how to replace multiple expired certificates at a time. You can replace additional certificates and certificates for listeners.

Procedure

1.
2.
3. In the left-side navigation pane, choose **CLB (Formerly Known as SLB) > Certificates**.
4. On the **Certificates** page, find the certificate that you want to replace and click **Replace** in the **Actions** column.

   > **Note** Only certificates associated with at least one listener or additional certificate can be replaced.

5. On the **Replace Server Certificate** page, replace the certificate.

   The following table describes the parameters.

Parameter	Description
Replace Mode: **Create and Replace Certificate**	
Select Certificate Source: **Alibaba Cloud Certificates**	Set **Region** and **Resource Group**, and select a certificate from **Certificates**.
Select Certificate Source: **Upload Third-party Certificate**	Upload a third-party certificate. For more information, see Upload a third-party certificate.
Replace Mode: **Replace with Saved Certificate**	
Server Certificate for Replacement	Select a server certificate from the list of existing certificates.

6. Click **Replace**.
7. Click **View Certificate**. On the **Certificates** page, you can check whether the certificates for the listeners or additional certificates are replaced with the new one.

7.FAQ about certificate upload failures

This topic provides answers to some frequently asked questions about certificate upload failures.

How can I resolve the Invalid Parameter error when I create a certificate?

On the **Certificates** page, after I click **Create Certificate**, select **Alibaba Cloud Certificates**, and then click **Create**, the message **Invalid parameter.** appears.

The error may be caused by one of the following reasons:

- The content of the public key is invalid.
- The format in which the certificate is encoded is not supported.
- To check whether the content of a public key is valid, upload the certificate to a Linux server and run the following command:

```
openssl x509 -noout -text -in myprivate.pem
```

  - If the following error is returned, it indicates that the content of the public key is invalid.

```
[root@iZ~]# openssl x509 -noout -text -in  /root/z.pem
unable to load certificate
139903831541648:error:0906D064:PEM routines:PEM_read_bio:bad base64 decode:pem_lib.c:829:
```

  - If the following message is returned, it indicates that the content of the public key is valid.

```
[root@iZ~]# openssl x509 -noout -text -in  /root/z.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:0...7b:d7:ef
    Signature Algorithm: sha...ryption
        Issuer: C=US, O=DigiCert Inc, OU=www...com, CN=...DV TLS CA - G1
        Validity
```

- Alibaba Cloud supports certificates encoded in RFC4648 Base64. To prevent upload failures, make sure that your certificate is encoded in the format supported by Alibaba Cloud.

Issue

Cause

Solution

How can I resolve the Invalid Format error when I create a server certificate?

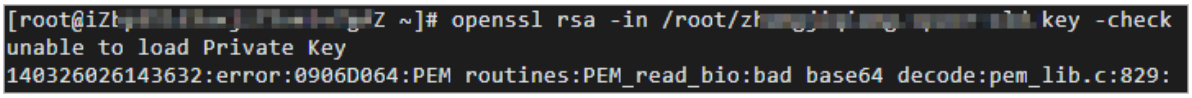
On the **Certificates** page, after I click **Create Certificate**, select **Upload Third-party Certificate**, and then click **Create**, the message **The specified Server Certificate format is invalid. Check the format and try again.** appears.

The content of the private key is invalid.

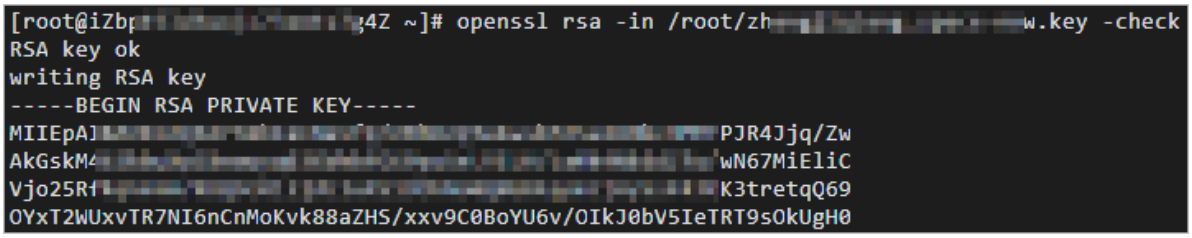
To check whether the content of a private key is invalid, upload the certificate to a Linux server and run the following command:

```
openssl rsa -in myprivate.key -check
```

- If the following error is returned, it indicates that the content of the private key is invalid.



- If the following message is returned, it indicates that the content of the private key is valid.



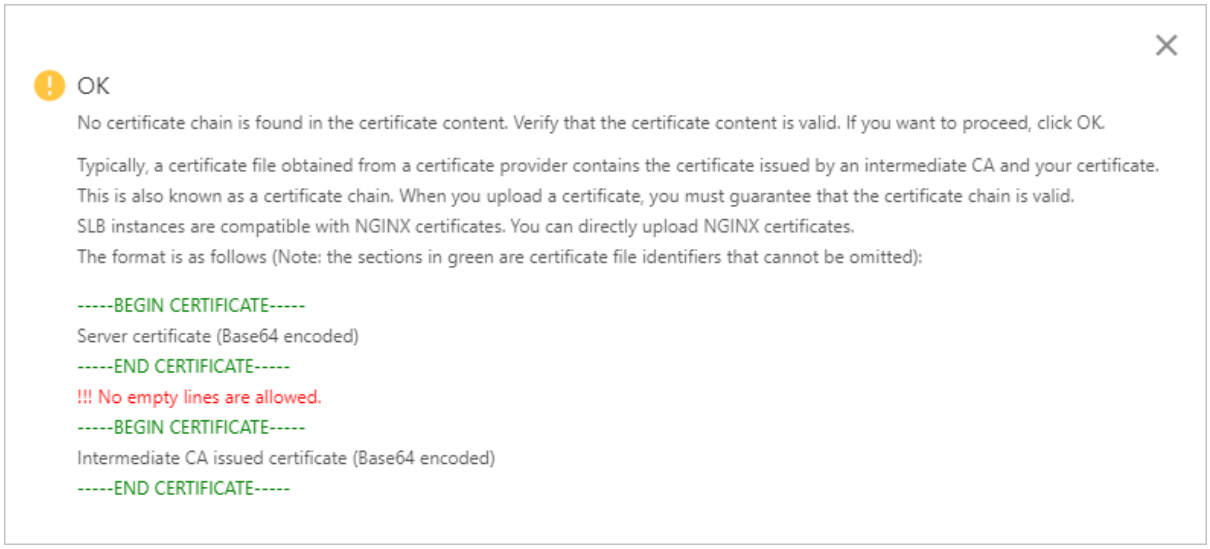
Issue

Cause

Solution

How can I resolve the Certificate Chain Not found error when I create a certificate?

On the **Certificates** page, after I click **Create Certificate**, select **Upload Third-party Certificate**, and then click **Create**, the message **No certificate chain is found.** appears.



In most cases, a certificate file obtained from a certificate provider contains a certificate issued by an intermediate certification authority (CA) and your certificate. This is also known as a certificate chain. Before you upload a certificate, you must verify that the certificate chain is valid.

Contact the CA that issues the certificate to verify the certificate chain.

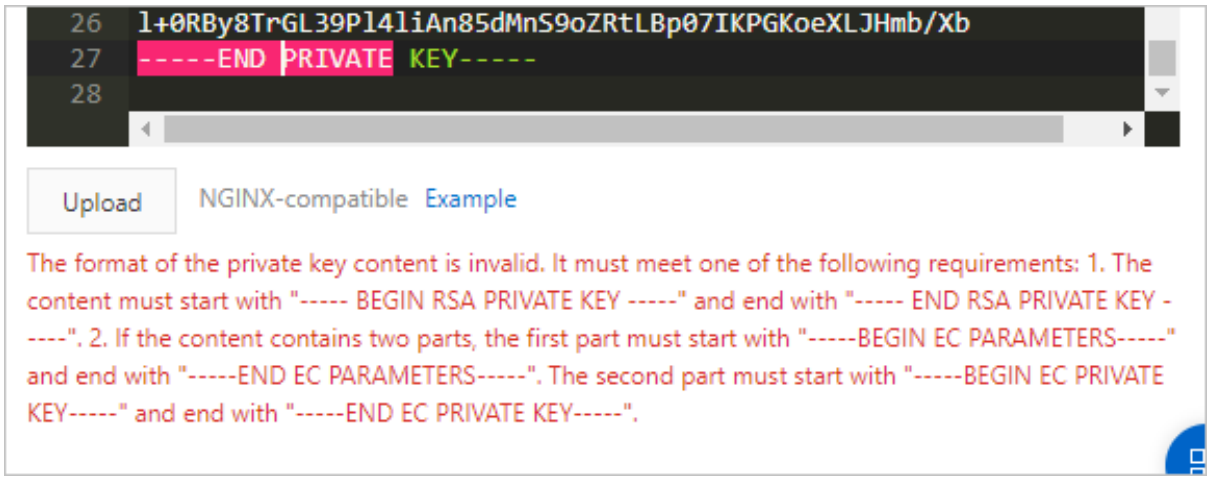
Issue

Cause

Solution

How can I resolve the Invalid Format error when I specify a private key?

On the **Certificates** page, after I click **Create Certificate**, select **Upload Third-party Certificate**, and then enter the content of a private key, the message **The format of the private key content is invalid.** appears.



The error may be caused by one of the following reasons:

- The format of the RSA private key certificate is invalid. The RSA private key must start with `-----BEG`

`IN RSA PRIVATE KEY-----` and end with `-----END RSA PRIVATE KEY-----`.

- The content of the elliptic curve (EC) private key certificate is not found. An EC private key certificate consists of two sections. The first part starts with `-----BEGIN EC PARAMETERS-----` and ends with `-----END EC PARAMETERS-----`. The second part starts with `-----BEGIN EC PRIVATE KEY-----` and ends with `-----END EC PRIVATE KEY-----`.
- If the format of the RSA private key certificate is invalid, upload the certificate to a Linux server and run the following command to convert the format:

```
openssl rsa -in myprivate.key  -out  myprivate.pem
```

- If the content of the EC private key is not found, contact the CA that issues the certificate to verify the private key.

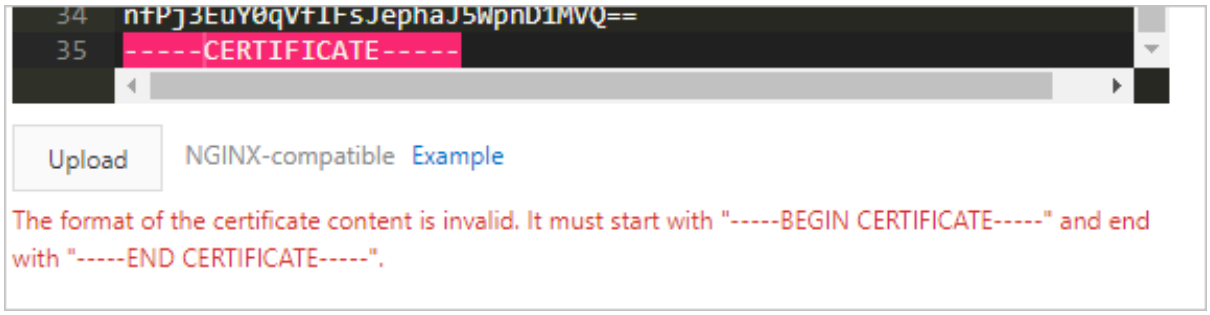
Issue

Cause

Solution

How can I resolve the Invalid Format error when I specify a public key?

On the **Certificates** page, after I click **Create Certificate**, select **Upload Third-party Certificate**, and then enter the content of a public key, the message **The format of the certificate content is invalid.** appears.



The format of the public key content is invalid. It must start with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

Contact the CA that issues the certificate to verify the public key.

Issue

Cause

Solution

How can I resolve the Certificate Not Found error when I associate a server certificate with an HTTPS listener?

When I configure an HTTPS listener, after I select a server certificate in the **SSL Certificates** step, the message **The certificate does not exist.** appears.

The HTTPS listener of the Classic Load Balancer (CLB) instance is created by using an Alibaba Cloud account. The certificate is created by using an Alibaba Finance Cloud account. Therefore, the system cannot identify the certificate that you uploaded.

Use the same account to create the CLB instance and upload the certificate.

Issue

Cause

Solution