

# Alibaba Cloud

## ##均衡

証明書管理

Document Version20200227

# 目次

---

|                                             |    |
|---------------------------------------------|----|
| 1 証明書の要件.....                               | 1  |
| 2 証明書の作成.....                               | 4  |
| 2.1 証明書の作成.....                             | 4  |
| 2.2 SSL Certificates Service からの証明書の選択..... | 8  |
| 2.3 サードパーティ証明書のアップロード.....                  | 10 |
| 3 証明書のアップロード.....                           | 14 |
| 4 CA証明書の生成.....                             | 16 |
| 5 証明書形式の変換.....                             | 20 |
| 6 証明書の交換.....                               | 21 |

# 1 証明書の要件

---

**Server Load Balancer** では、**PEM** 形式の証明書にのみ対応しています。証明書をアップロードする前に、証明書、証明書チェーン、秘密鍵が、このセクションで説明されている規則に準拠していることを確認してください。

## ルート CA 発行の証明書

ルート **CA** 発行の証明書の場合、**Server Load Balancer** にアップロードする必要があるのは、受け取った証明書だけです。この証明書が設定された **Web** サイトは、追加の証明書を設定しなくても **Web** ブラウザーから信頼されます。

証明書の形式は、次の要件を満たす必要があります。

- ・ 証明書の内容は、-----BEGIN CERTIFICATE-----, -----END CERTIFICATE----- の間に記載されています。証明書をアップロードする際、このヘッダーとフッターも含めます。
- ・ 各行 (最後の行を除く) は **64** 文字にする必要があります。最後の行は、**64** 文字以下にすることができます。
- ・ 内容に空白文字を含めることはできません。

ルート **CA** 発行の証明書のサンプルを以下に示します。

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tELMAKGAIUEBhmMCVmxvFzAVBGnVBaoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcncvdCB0ZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiBic2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYS9oYykwOTEmMCA0GA1UEAxM=
VmVyaVNPZ24uQ2xhc3MgMyBTZWNNcmUgU2VydmdVYIENBIC0gRzIwHlcNMNTAxMDA4
MDAwMDAwHicNMNTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzEETMBEGA1UECBMK
V2FzaGlUeDZ3Rvb3JlEQMA4GA1UEBxBHUHVhdHRsZTEYMByGA1UEChQPQW1hem9uLmNv
bSBjbmuMRRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLnNvb3R1bGVzANBgkqhkiG9w0B
AQEFAAOBjQAwwYkCgYEAXb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCzdruCrW1eN/P9wbfqMMZ
X964CjVov3NrF5AuxU8jgtwEu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcc
AwEAAAoAcEdwgghHNMAKA1UdEwQCMACwYDVGR0PBAQDAgwMEUA1UdHwQ+MDwv
Oa4AoDaGNgh0dHA6Ly9TVlJTZWNNcmUteRzItY3JsLnZlcm1zaWduLmNhbWVS9TVlJT
ZWNNcmVMi5jcmmwRAYDVR0gBD0wOzA5BgtghkgBhvFAQCXAzMGMCGCCSGAUF
BwIBFBxodHRwcovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCCCS
GAUFBwMBBgrBgEFBQcDAjAFBgNVHSMEGDAwBS17wsRzsBBAGNKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAyIKwYBBQUHMAggGGGH0dHA6Ly9vY3NwLnZlcm1z
aWduLmNvbTBABgrBgEFBQcwAoY0aHR0cDovL1NWU1NlY3VyZS1HMi1haWEudmVyaXNp
Z24uY29tL1NWU1NlY3VyZUcyLmN1c2BuBgrBgEFBQcBDARIMGChXqbCMFow
WDBWFglpbWFnZS9naWYwTTFaMACGBS0AwIAaBBRLa7kolgYMu9BS0JsprEsHiyEF
GDAmFiRodHRwOi8vbG9nb352ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsttGwEE9zbCVcuKjrsl3dWK1dFiq30P4y/Bi
ZBYEywbT8znUYfUE2SUb/zmvmppe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mkrs3IQ
3gaE1an2BSUIHXGLn9NAF09hYwwbeEZAcfBiLEIodNwzcvgJ+2LDWGJOGrNI
NM856xjqhJCPxYzk9buuCL1B4Kzu0CTbexz/iEgYV+DiuTxcFA4uhwMDSe0nybn
1qiwrk450mConqH4ly4P4Lxo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5XRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

## 中間 CA 発行の証明書

中間 **CA** 発行の証明書の場合、複数の中間証明書を受け取ります。サーバー証明書と中間証明書の両方を結合して **SLB** にアップロードする必要があります。

証明書チェーンの形式は、以下の要件を満たす必要があります。

- ・ サーバー証明書を先頭部分に記載し、その後ろに空白文字を入れずに中間証明書を記載します。
- ・ 内容に空白文字を含めることはできません。
- ・ 内容に空白の行を含めることはできません。各行 (最後の行を除く) は **64** 文字にする必要があります。詳細は『[RFC1421](#)』をご参照ください。
- ・ 証明書の説明に記載されている証明書の要件に準拠しています。一般的に、中間 **CA** は証明書の発行時に証明書の形式に関する説明文書を提供します。証明書チェーンは、その形式の要件に従う必要があります。

証明書チェーンのサンプルを以下に示します。

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

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

## RSA 秘密鍵

サーバー証明書をアップロードする際、証明書の秘密鍵もアップロードする必要があります。

RSA 秘密鍵の形式は、以下の要件を満たす必要があります。

- ・ 鍵は、-----BEGIN RSA PRIVATE KEY-----，-----END RSA PRIVATE KEY----- の間に記載されています。鍵をアップロードする際、このヘッダーとフッターも含めます。
- ・ 内容に空白文字を含めることはできません。各行(最後の行を除く)は 64 文字にする必要があります。最後の行は、64 文字以下にすることができます。詳細は『RFC1421』をご参照ください。

秘密鍵が暗号化されている場合、たとえばヘッダーとフッターが -----BEGIN PRIVATE KEY-----，-----END PRIVATE KEY-----、または -----BEGIN ENCRYPTED PRIVATE KEY-----，-----END ENCRYPTED PRIVATE KEY----- であるか、秘密鍵に Proc-Type: 4, ENCRYPTED が含まれている場合、以下のコマンドを実行して秘密鍵を変換してから、**Server Load Balancer** にアップロードしてください。

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

RSA 秘密鍵のサンプルを以下に示します。

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzVSSChH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMjclva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qn9n957ZEPhtUpVZuhS3409DDM/tJ3Tl8aaNYWHRPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUypdcfXzN5WM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHRFi
laF6+Wen8ZvNqkm0hAMQwIj1h1Vp1f174//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGPcwUshSfXewfbAYGf3ur8W0xq0uU07BAxaKHnCMNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoieYs111ah1AJvICVgTc3+LzG2pIpM7I+K0nHC5eswM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKfVWjLUnhf6WcQFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhgqHu0edU
ZXIHRJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/Hc9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhMZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4led0Sa/uKRao4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAERmtJf2yS
ICRkbQaB3gPSe/LCgzy1nhtaFOUbNxeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kV106MZCFAdqirAjiQWapKh9Bxbp2eHCrB81MFAWLRQSl0k79b/jVmZMC3upd
EJ/iSWjZKPBw7hCFAeRtPhxyNTJ5idEiU9U8EQid8111giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFYGRfEWWrrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

## 2 証明書の作成

---

### 2.1 証明書の作成

HTTPS リスナーを設定するには、**SSL Certificate Service** の証明書を直接使用するか、**SLB** に必要なサードパーティサーバー証明書と **CA** 証明書をアップロードします。これにより、バックエンドサーバーで証明書を設定する必要がなくなります。

**SLB** は、以下の 2 つのリソースからの証明書に対応しています。

- ・ **Alibaba Cloud SSL Certificate Service** により発行またはホストされる証明書: **Alibaba Cloud SSL Certificate Service** の証明書を選択することができます。証明書が期限切れに近づくと通知が来ます。証明書の更新は簡単にできます。

現在、クライアント **CA** 証明書には対応していません。

- ・ サードパーティ証明書: サードパーティ証明書をアップロードするには、証明書の公開鍵/秘密鍵が必要です。

**HTTPS** サーバー証明書とクライアント **CA** 証明書に対応しています。

証明書を作成する前に、以下の点に注意してください。

- ・ 複数のリージョンで証明書を使用するには、証明書の作成時に複数のリージョンを選択する必要があります。
- ・ 1 アカウントで最大 **100** の証明書を作成できます。

#### SSL Certificate Service からの証明書の選択

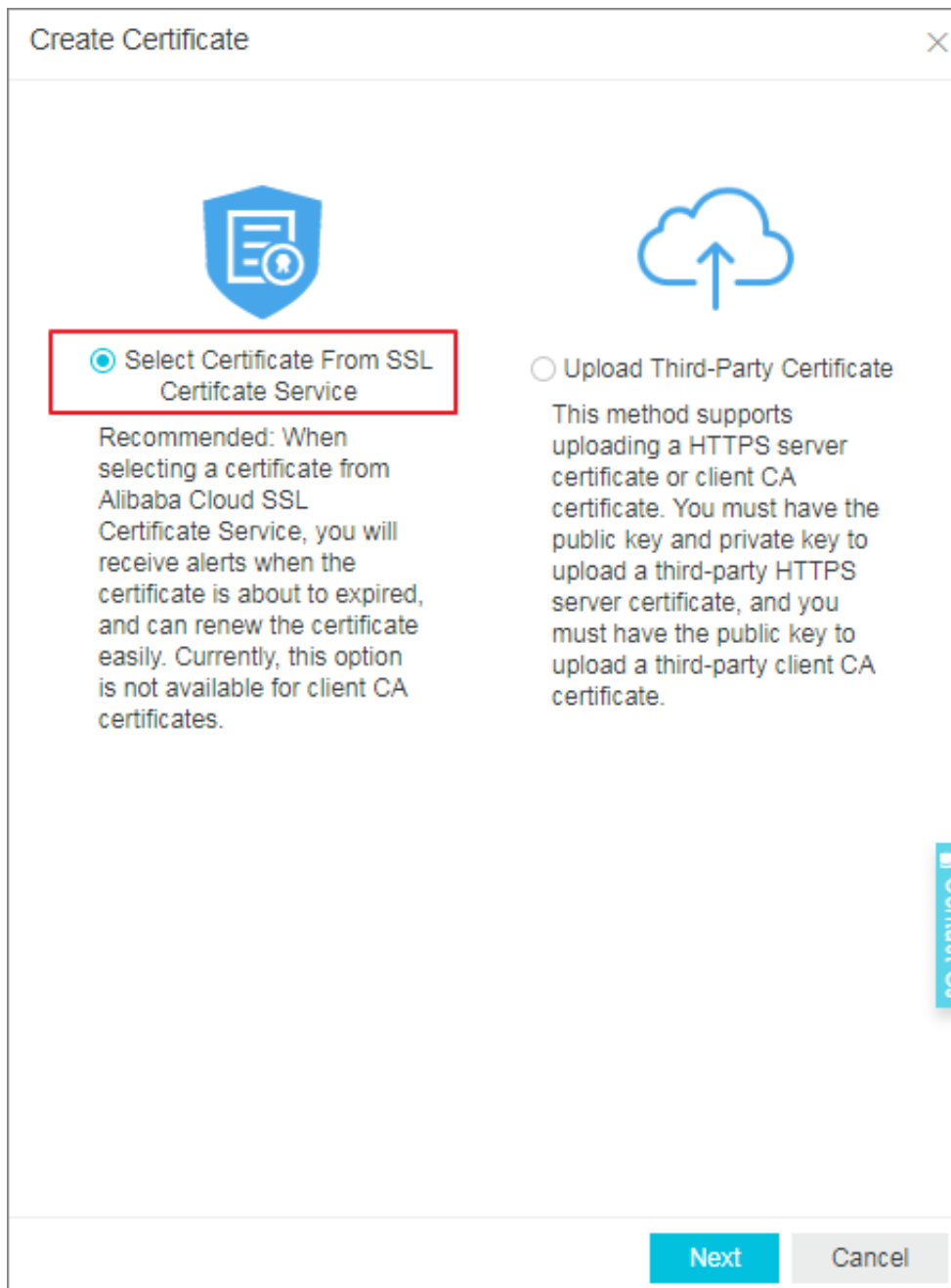
**Alibaba Cloud SSL Certificate Service** は、**Web** サイトの **HTTPS** 化のために、さまざまな種類のデジタル証明書を発行します。これにより、**Web** サイトが信頼できるものになり、乗っ取り、改ざん、傍受を防止することができます。また、証明書のライフサイクルが一律に管理され、証明書のデプロイが簡略化されます。詳細は、「[SSL Certificate Service](#)」をご参照ください。

**SSL Certificate Service** で証明書を使用するには、[SSL Certificate コンソール](#) にログインして証明書を購入するか、サードパーティ証明書を **SSL Certificate Service** にアップロードする必要があります。

**SSL Certificate Service** から証明書を選択するには、以下の手順を実行します。

1. [SLB コンソール](#) にログインします。
2. 左側のナビゲーションウィンドウで、[証明書] をクリックします。

3. [証明書の作成] をクリックします。証明書の作成ページで、[SSL Certificate Service から証明書を選択] をクリックします。



4. [次へ] をクリックします。SSL Certificate Service から証明書を選択ページで、証明書をデプロイするリージョンを選択し、証明書リストから使用する SSL 証明書を選択します。

1つの証明書を複数のリージョンにまたがって使用することはできません。複数のリージョンで証明書を使用する場合は、それらのリージョンをすべて選択する必要があります。

5. [OK] をクリックします。

## サードパーティ証明書のアップロード

サードパーティ証明書をアップロードする前に、次の条件が満たされていることを確認してください。

- ・ サーバー証明書を購入していること。
- ・ CA 証明書とクライアント証明書を生成していること。詳細は、「[CA証明書の生成](#)」をご参照ください。

サードパーティ証明書をアップロードするには、次の手順を実行します。

1. [SLB コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、[証明書] をクリックします。
3. [証明書の作成] をクリックします。

4. 証明書の作成ページで、[サードパーティ証明書のアップロード] をクリックします。

**Create Certificate**

☐ Select Certificate From SSL Certificate Service

Recommended: When selecting a certificate from Alibaba Cloud SSL Certificate Service, you will receive alerts when the certificate is about to expired, and can renew the certificate easily. Currently, this option is not available for client CA certificates.

☒ Upload Third-Party Certificate

This method supports uploading a HTTPS server certificate or client CA certificate. You must have the public key and private key to upload a third-party HTTPS server certificate, and you must have the public key to upload a third-party client CA certificate.

[Contact Us](#)

**Next** **Cancel**

5. [次へ] をクリックします。サードパーティ証明書のアップロードページで、証明書の内容をアップロードします。

| 設定項目 | 説明                                                                                 |
|------|------------------------------------------------------------------------------------|
| 証明書名 | <p>証明書名を入力します。</p> <p>名前は、<b>1～80</b> 文字です。英数字、および以下の特殊文字を使用できます。</p> <p>_/. -</p> |

| 設定項目    | 説明                                                                                                                                                                                                                                                                 |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リージョン   | <p>証明書をアップロードするリージョンを <b>1</b> つ以上選択します。</p> <p><b>1</b> つの証明書を複数のリージョンにまたがって使用することはできません。複数のリージョンで証明書を使用する場合は、それらのリージョンをすべて選択する必要があります。</p>                                                                                                                       |
| 証明書のタイプ | <p>アップロードする証明書のタイプを選択します。</p> <ul style="list-style-type: none"> <li>・ <b>[サーバー証明書]: HTTPS</b> 片方向認証の場合、サーバー証明書と秘密鍵のみが必須です。</li> <li>・ <b>[CA 証明書]: HTTPS</b> 双方向認証の場合、サーバー証明書と <b>CA</b> 証明書の両方が必要です。</li> </ul>                                                  |
| 証明書の内容  | <p>証明書の内容をエディターに貼り付けます。</p> <p>[サンプル証明書を見る] をクリックして、正しい証明書形式を確認します。詳細は、「<a href="#">証明書の要件</a>」をご参照ください。</p>                                                                                                                                                       |
| 秘密鍵     | <p>サーバー証明書の秘密鍵をエディターに貼り付けます。</p> <p>[サンプル証明書を見る] をクリックして、正しい証明書形式を確認します。詳細は、「<a href="#">証明書の要件</a>」をご参照ください。</p> <div>  :         秘密鍵は、サーバー証明書をアップロードする場合にのみ必要です。       </div> |

6. [OK] をクリックします。

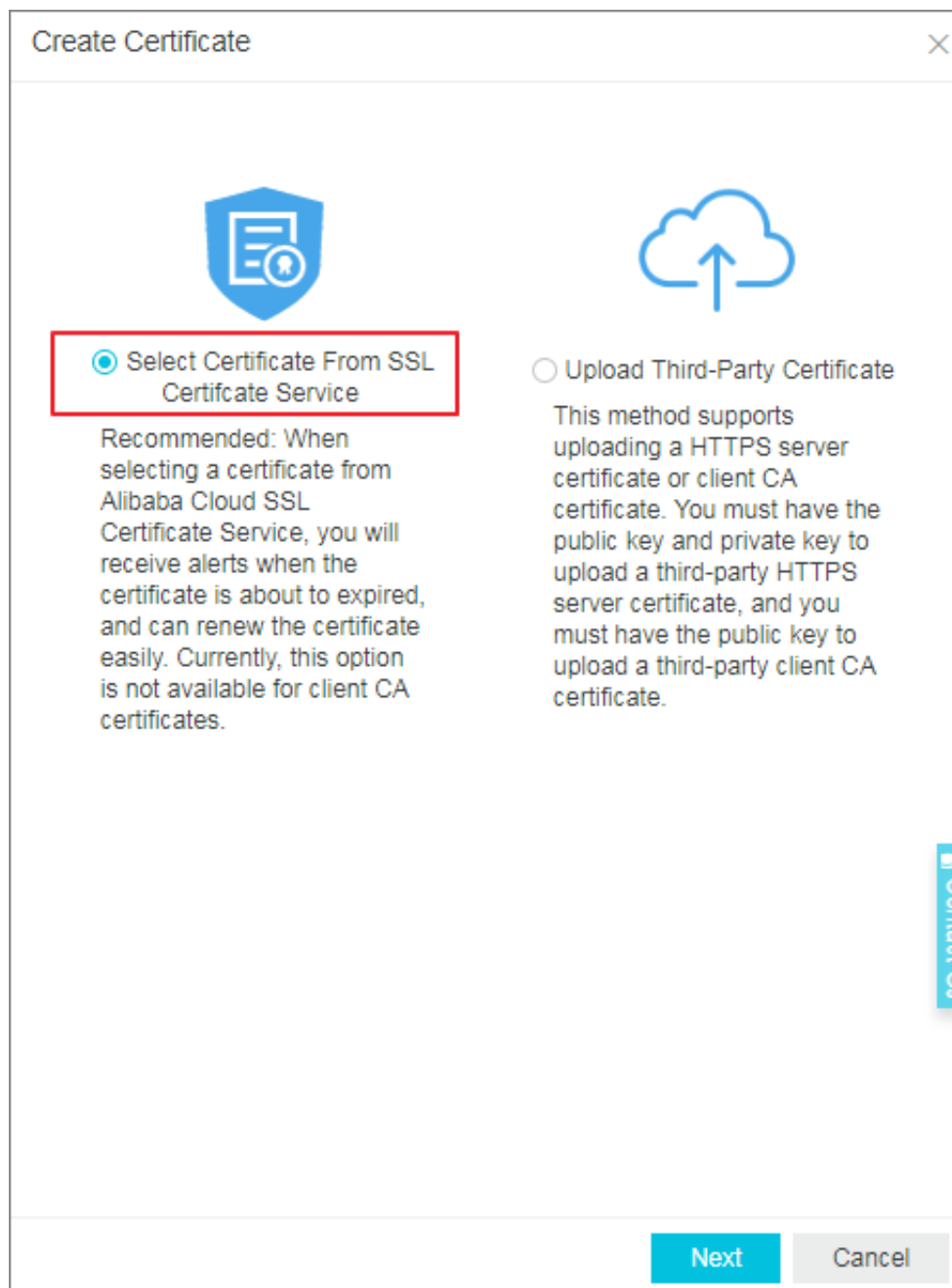
## 2.2 SSL Certificates Service からの証明書の選択

このトピックでは、**SSL Certificates Service** から証明書を選択する方法について説明します。**SSL Certificates Service** は、さまざまな機関のデジタル証明書を発行して信頼できる **HTTPS** サービスを提供し、ハイジャック、改ざん、傍受などから **Web** サイトを保護します。**SSL Certificates Service** を使用すると、証明書のライフサイクルを一元管理して、証明書のデプロイを簡素化できます。

**SSL Certificates Service** で証明書を使用するには、[SSL Certificates Service コンソール](#) にログインし、証明書を購入するか、サードパーティの証明書を **SSL Certificates Service** にアップロードする必要があります。

**SSL Certificates Service** の詳細については、[SSL Certificates Service](#) をご参照ください。

1. [SLB コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、[証明書] をクリックします。
3. [証明書の作成] をクリックします。[証明書の作成] ページで、[**SSL Certificate Service** から証明書の選択] をクリックします。



Create Certificate

 ☒ Select Certificate From SSL Certificate Service

Recommended: When selecting a certificate from Alibaba Cloud SSL Certificate Service, you will receive alerts when the certificate is about to expired, and can renew the certificate easily. Currently, this option is not available for client CA certificates.

 ☐ Upload Third-Party Certificate

This method supports uploading a HTTPS server certificate or client CA certificate. You must have the public key and private key to upload a third-party HTTPS server certificate, and you must have the public key to upload a third-party client CA certificate.

Next Cancel

4. [次へ] をクリックします。[SSL Certificate Service から証明書の選択] ページで、証明書をデプロイするリージョンを選択します。証明書リストから、使用する **SSL** 証明書を選択します。

1 つの証明書を複数のリージョンにまたがって使用することはできません。複数のリージョンで証明書を使用する場合、必要なリージョンをすべて選択する必要があります。

5. [OK] をクリックします。

#### 関連情報

[#unique\\_6](#)

## 2.3 サードパーティ証明書のアップロード

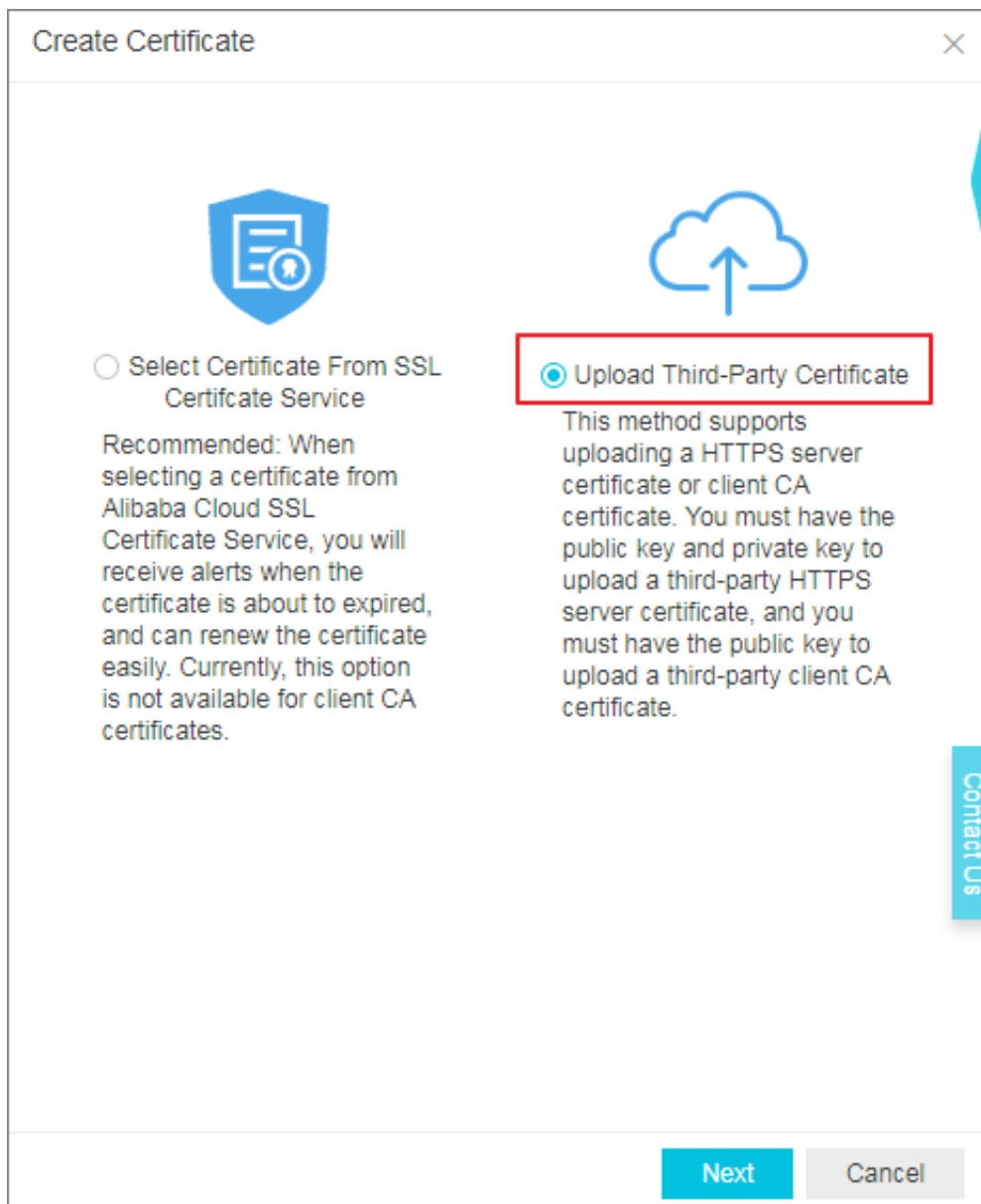
サードパーティの証明書をアップロードする前に、証明書の公開鍵ファイルと秘密鍵ファイルを取得しておく必要があります。

サードパーティ証明書をアップロードする前に、次の条件が満たされていることを確認してください。

- ・ サーバー証明書を購入済みであること。
- ・ CA 証明書とクライアント証明書が生成されていること。詳細については、「[#unique\\_8](#)」をご参照ください。

1. [SLB コンソール](#) にログインします。
2. 左側のメニューで [証明書] をクリックします。
3. [証明書の作成] をクリックします。

4. [証明書の作成] ページで、[サードパーティ証明書のアップロード] をクリックします。



**Create Certificate**

☐ Select Certificate From SSL Certificate Service

Recommended: When selecting a certificate from Alibaba Cloud SSL Certificate Service, you will receive alerts when the certificate is about to expired, and can renew the certificate easily. Currently, this option is not available for client CA certificates.

☒ Upload Third-Party Certificate

This method supports uploading a HTTPS server certificate or client CA certificate. You must have the public key and private key to upload a third-party HTTPS server certificate, and you must have the public key to upload a third-party client CA certificate.

[Contact Us](#)

**Next** Cancel

5. [次へ] をクリックします。[サードパーティ証明書のアップロード] ページで、証明書をアップロードします。

| 設定項目 | 説明                                                                                            |
|------|-----------------------------------------------------------------------------------------------|
| 証明書名 | <p>アップロードする証明書の名前を入力します。</p> <p>名前の長さは 1 から 80 文字です。英数字、および以下の特殊文字を使用できます。</p> <p>_ / . -</p> |

| 設定項目    | 説明                                                                                                                                                                                                             |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リージョン   | <p>アップロードする証明書を使用する <b>1</b> つ以上のリージョンを選択します。</p> <p><b>1</b> つの証明書を複数のリージョンにまたがって使用することはできません。複数のリージョンで証明書を使用する必要がある場合は、必要なすべてのリージョンを選択します。</p>                                                               |
| 証明書のタイプ | <p>アップロードする証明書のタイプを選択します。</p> <ul style="list-style-type: none"><li>・ <b>[サーバー証明書]: HTTPS</b> 片方向認証の場合、サーバー証明書と秘密鍵のみが必須です。</li><li>・ <b>[CA 証明書]: HTTPS</b> 双方向認証の場合、サーバー証明書と <b>CA</b> 証明書の両方が必要です。</li></ul> |
| 証明書の内容  | <p>証明書の内容をエディターに貼り付けます。</p> <p><b>[サンプル証明書を見る]</b> をクリックして、正しい証明書の形式を確認します。詳細については、「<a href="#">証明書の要件</a>」をご参照ください。</p>                                                                                       |

| 設定項目 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 秘密鍵  | <p>サーバー証明書の秘密鍵をエディターに貼り付けます。</p> <p>[サンプル証明書を見る] をクリックして、正しい証明書の形式を確認します。詳細については、「<a href="#">証明書の要件</a>」をご参照ください。</p> <p><b>SLB</b> がサポートする秘密鍵の形式は、次の 2 種類です。</p> <pre>-----BEGIN RSA PRIVATE KEY----- 秘密鍵の内容 (BASE64 エンコーディング) -----END RSA PRIVATE KEY-----</pre> <p>または</p> <pre>-----BEGIN EC PARAMETERS----- 秘密鍵の内容 (BASE64 エンコーディング) -----END EC PARAMETERS----- -----BEGIN EC PRIVATE KEY----- 秘密鍵の内容 (BASE64 エンコーディング) -----END EC PRIVATE KEY-----</pre> <p> :</p> <ul style="list-style-type: none"> <li>秘密鍵は、サーバー証明書をアップロードする場合にのみ必要です。</li> <li>現在、EC 形式のキーは次の地域でサポートされています。 <ul style="list-style-type: none"> <li>- イギリス (ロンドン)</li> <li>- 中国 (青島)</li> <li>- 中国 (フフホト)</li> <li>- 中国 (成都)</li> <li>- 日本 (東京)</li> <li>- インド (ムンバイ)</li> <li>- オーストラリア (シドニー)</li> <li>- マレーシア (クアラルンプール)</li> <li>- 米国 (シリコンバレー)</li> <li>- 米国 (バージニア)</li> <li>- ドイツ (フランクフルト)</li> <li>- <b>UAE</b> (ドバイ)</li> </ul> </li> </ul> |

6. [OK] をクリックします。

[#unique\\_9](#)

[#unique\\_6](#)

## 3 証明書のアップロード

HTTPS リスナーを作成する前に、必要なサーバー証明書とCA証明書をSLBにアップロードする必要があります。証明書をSLBにアップロードすれば、バックエンドサーバーに証明書を設定する必要はなくなります。

- ・ サーバー証明書を購入済みです。
- ・ CA 証明書とクライアント証明書を生成済みです。詳細は次を参照ください[CA証明書の生成](#)。

証明書をアップロードする前に、次の事項を注意してください：

- ・ 1つの証明書を複数のリージョンで使用する場合は、すべてのリージョンに証明書をアップロードする必要があります。
- ・ 1つのアカウントにつき、最大 **100** の証明書をアップロードできます。

1. [SLBコンソール](#)にログインします。
2. 左側のメニューで、証明書をクリックします。
3. 証明書の作成をクリックします。
4. 証明書の作成ページで、証明書の内容をアップロードし、**OK**をクリックします。

| 構成    | 説明                                                                                                                    |
|-------|-----------------------------------------------------------------------------------------------------------------------|
| 証明書名  | 証明書の名前を入力します。<br><br>名前は、 <b>1～80</b> 文字です。英字、数字、および以下の特殊文字を使用できます。<br><br>_/. -                                      |
| リージョン | 証明書がアップロードされるリージョンを <b>1</b> つ、或いは複数選択します。<br><br>証明書はクロスリージョンで使用することはできません。複数のリージョンで証明書を使用する場合は、該当するすべてのリージョンを選択します。 |

| 構成      | 説明                                                                                                                                                                                                                                    |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書のタイプ | 証明書のタイプを選択します。 <ul style="list-style-type: none"><li>・ サーバー証明書：HTTPS片方向認証の場合、サーバー証明書と秘密鍵のみが必須となります。</li><li>・ CA証明書：HTTPS双方向認証の場合、サーバー証明書とCA証明書の両方が必須となります。</li></ul>                                                                 |
| 証明書内容   | 証明書内容をエディターに貼り付けます。<br><br>有効な証明書の形式を表示するには、サンプルをインポートをクリックします。 PEM 形式の証明書のみに対応しています。 詳細は次を参照ください <a href="#">証明書の要件</a> 。                                                                                                            |
| 秘密鍵     | サーバー証明書の秘密鍵をエディターに貼り付けます。<br><br>有効な形式を表示するには、サンプルをインポートをクリックします。 詳細は次を参照ください <a href="#">証明書</a> の要件。<br><br> :<br>秘密鍵は、サーバー証明書をアップロードする場合にのみ必要です。 |

期限切れの証明書を一括削除するには、期限切れ証明書を全削除をクリックします。

## 4 CA証明書の生成

HTTPS リスナーを設定する際、自己署名 CA 証明書を使用できます。このドキュメントの手順に従って、CA証明書を生成し、作成されたCA証明書を使用してクライアント証明書に署名します。

### Open SSL を使用してCA 証明書を生成する

1. 次のコマンドを実行して、/rootディレクトリにcaフォルダーを作成し、caフォルダーに 4 つのサブフォルダーを作成します。

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

- ・ newcertsフォルダーには、CA 証明書によって署名されたデジタル証明書が保存されます。
- ・ privateフォルダーには、CA 証明書の秘密鍵が保存されます。
- ・ confフォルダーには、設定ファイルが保存されます。
- ・ serverフォルダーには、サーバー証明書が保存されます。

2. confディレクトリにopenssl.confファイルを作成し、次の情報を入力します。

```
[ 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. 次のコマンドを実行して、秘密鍵を生成します。

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

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

秘密鍵を生成する例を以下に示します。

```
root@iZbp1hfvivcqx1jwap31iZ:~/ca/conf# cd /root/ca
root@iZbp1hfvivcqx1jwap31iZ:~/ca# sudo openssl genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
.....+++
..+++
e is 65537 (0x10001)
```

4. 次のコマンドを実行し、プロンプトに従って必要な情報を入力します。 **Enter** キーを押すと、csrファイルが生成されます。

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



注:

**Common Name**は、SLB インスタンスのドメイン名です。

```
root@iZbp1hfvivcqx1jwap31iZ:~/ca# sudo openssl req -new -key private/ca.key -out 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@iZbp1hfvivcqx1jwap31iZ:~/ca#
```

5. 次のコマンドを実行して、`crt`ファイルを生成します。

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

6. 次のコマンドを実行して、秘密鍵の開始シーケンス番号を設定します。シーケンス番号には、任意の4文字を使用できます。

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

7. 次のコマンドを実行して、**CA**キーライブラリを作成します。

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

8. 次のコマンドを実行して、クライアント証明書を削除するための証明書失効リストを作成します。

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

次のレスポンスが返されます。

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

### クライアント証明書に署名する

1. 次のコマンドを実行して、`ca`ディレクトリの下に、クライアントキーを保存する`users`ディレクトリを生成します。

```
$ sudo mkdir users
```

2. 次のコマンドを実行して、クライアント証明書のキーを作成します。

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



注：

キーを作成する際、パスフレーズを入力します。パスフレーズは、不正なアクセスから秘密鍵を保護するためのパスワードです。入力されたパスフレーズは、このキーのパスワードになります。

3. 次のコマンドを実行して、証明書署名要求のための`csr`ファイルを作成します。

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

プロンプトが表示されたら、前の手順で設定したパスフレーズを入力します。



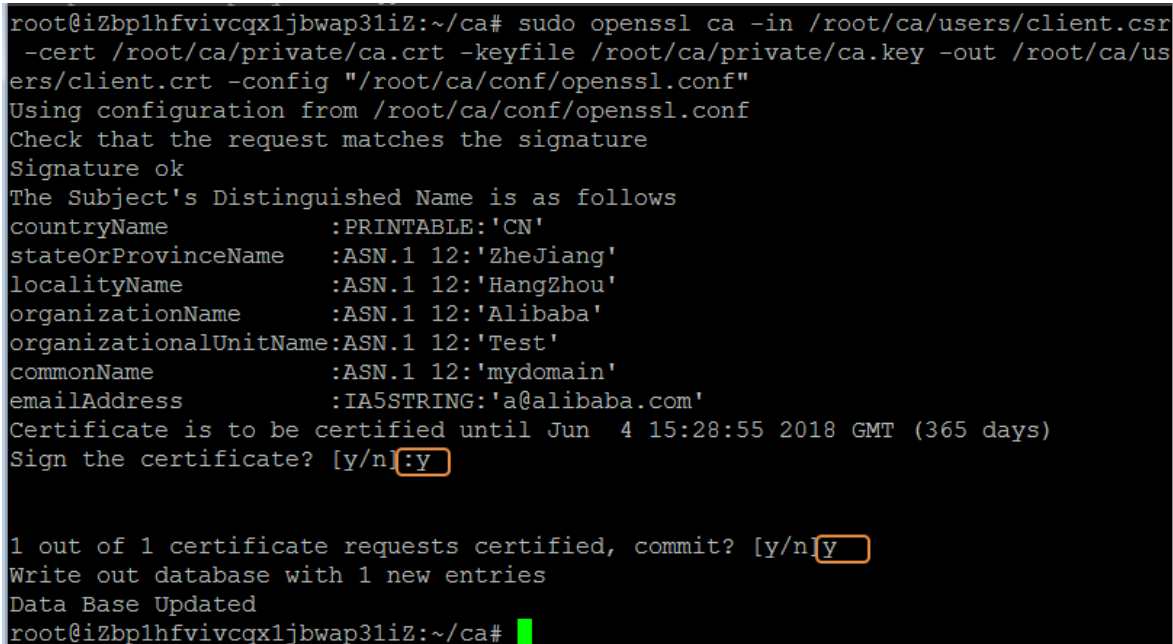
注：

チャレンジパスワードは、クライアント証明書のパスワードです。クライアントキーのパスワードではありません。

4. 次のコマンドを実行して、クライアントキーに署名します。

```
$ 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"
```

プロンプトが表示されたら、どちらのプロンプトにもyと入力します。



```
root@izbp1hfvivcqx1jwap3liZ:~/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@izbp1hfvivcqx1jwap3liZ:~/ca#
```

5. 次のコマンドを実行して、証明書をPKCS12ファイルに変換します。

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

プロンプトが表示されたら、クライアントキーのパスワードを入力します。そしてクライアント証明書のエクスポートに使用するパスワードを入力します。これはクライアント証明書を保護するためのパスワードで、クライアント証明書をインストールするときに必要です。

6. 生成されたクライアント証明書を表示するには、次のコマンドを実行します。

```
cd users
ls
```

## 5 証明書形式の変換

---

**Server Load Balancer** は、**PEM** 証明書のみに対応します。他の形式の証明書は、**PEM** 形式に変換してから、**Server Load Balancer** にアップロードする必要があります。形式の変換には、**Open SSL** を使用することを推奨します。

### DER を PEM に変換

**DER:** 一般的に、この形式は **Java** プラットフォームで使用されます。この証明書の拡張子は一般的に **.der**、**.cer** または **.crt** です。

- ・ 次のコマンドを実行して、証明書の形式を変換します。

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

- ・ 次のコマンドを実行して、秘密鍵を変換します。

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

### P7B を PEM に変換

**P7B:** 一般的に、この形式は **Windows Server** および **Tomcat** で使用されます。

次のコマンドを実行して、証明書の形式を変換します。

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

### PFX を PEM に変換

**PFX:** 一般的に、この形式は **Windows Server** で使用されます。

- ・ 次のコマンドを実行して、証明書を取り出します。

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

- ・ 次のコマンドを実行して、秘密鍵を取り出します。

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

## 6 証明書の交換

---

証明書期限切れによりサービスに与える影響を避けるには、証明書が期限切れになる前に証明書を交換してください。

1. 新しい証明書を作成し、アップロードします。

詳細は、[証明書のアップロード](#)と[CA証明書の生成](#)を参照してください。

2. **HTTPS**リスナー構成で新しい証明書を構成します。
3. 証明書ページで、対象証明書を検索し、削除をクリックします。
4. 表示されるダイアログボックスで、**OK**をクリックします