云证书管理服务

常见问题

文档版本 37

发布日期 2025-08-21

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 证书咨询

1.1 SSL 证书管理与私有证书管理的区别?

概念

SSL证书管理（SSL Certificate Manager，SCM）是一个SSL（Secure Sockets Layer）证书管理平台。它是由华为云联合全球知名数字证书服务机构（CA，Certificate Authority），在华为云平台上为您提供一站式SSL证书的全生命周期管理，实现网站的可信认证与安全数据传输。

私有证书管理（Private Certificate Authority，PCA）是一个私有CA和私有证书管理平台。您可以通过简单的可视化操作，建立自己完整的CA层次体系并使用它签发证书，实现了在组织内部签发和管理自签名私有证书。主要用于对组织内部的应用身份认证和数据加解密。

SCM 与 PCA 的区别

SCM与PCA的主要区别如**表1-1**所示。

表 1-1 SCM 与 PCA 的区别

服务名称	作用	应用场景	安全等级	是否可以配置到内网
SSL证书管理（SCM）	SSL证书采用SSL协议进行通信，SSL证书部署到服务器后，服务器端的访问将启用HTTPS协议。您的网站将会通过HTTPS加密协议来传输数据，可帮助服务器端和客户端之间建立加密链接，从而保证数据传输的安全。 ● 网站身份验证，确保数据发送到正确的客户端和服务器。 ● 在客户端和服务器端之间建立加密通道，保证数据在传输过程中不被窃取或篡改。	● 网站可信认证 SSL证书如同网站在互联网中的“身份证”，网站没有安装SSL证书，浏览器将会将其列为不安全的网站，网站用户也就无法信任您网站的安全性，安装了SSL证书就代表您的网站是“安全”的，网站用户可以放心访问您的网站。特别是OV或EV型证书，CA颁发机构在签发证书前会验证域名所有者及其企业信息，可以有效提升网站可信度。 ● 网站数据加密 通常网站数据传输使用的HTTP协议，无法加密数据，导致数据有泄露和被窃听、篡改的风险，SSL证书可以让您的网站采用HTTPS加密通讯，有效提升数据传输安全性。 ● 在华为云WAF、ELB、CDN等服务上使用HTTPS协议 如果您购买了华为云WAF、ELB、CDN等服务，可以在SSL证书管理页面中将购买的证书一键部署至这些云产品中，为云产品提供HTTPS数据传输安全保障。 ● 提高网站访问速度 SSL 证书全面兼容 HTTP2.0 协议，快速动态加载网页内容，可以为网站服务提速。	高	不可以，SSL证书只能用于公网域名。

服务名称	作用	应用场景	安全等级	是否可以配置到内网
私有证书管理（PCA）	• 支持用户建立完整的CA层次体系，包括根及多级中间CA等。 • 为用户提供高可用高安全的私有CA托管能力。 • 支持用户方便快捷地创建和管理私有证书，用于识别和保护组织内的应用程序、服务、设备和用户等资源。	• 企业对内实行应用数据安全管控 您可以通过私有证书管理建立企业内部的证书管理体系，在企业内部签发和管理自签名私有证书，实现企业内部的身份认证、数据加解密、数据安全传输。 • 车联网应用 车企TSP使用私有证书管理服务，为每台车辆终端颁发证书，提供车-车、车-云、车-路多场景交互时鉴权、认证、加密等安全能力。 • 物联网应用 IoT平台使用私有证书管理服务，为每台IoT设备颁发证书，并通过IoT平台联动PCA，实现IoT设备的身份校验与认证，保障IoT场景下设备接入安全。	较低	可以，私有证书可以部署到内网使用。

1.2 哪些网站必须启用 HTTPS 加密?

在越来越重视信息安全的今天，HTTPS协议站点无疑已经成为主流。就目前形势而言，以下网站必须启用HTTPS协议加密：

- 电商平台及其相关支付系统网站
- 银行系统、金融机构等高私密性网站
- 政府、高校、科研机构及其相关网站
- 以搜索引擎为主要流量来源的网站
- 以邮箱为主的企业交流平台

长远来看，HTTPS协议网站已是必然趋势。启用HTTPS协议加密是当今网站建设的关键要点。不仅局限于上述网站类型，启用HTTPS协议加密既是网站安全的必然需要，也是公司发展的提前布局。

1.3 HTTPS 与 HTTP 协议有什么不同?

HTTPS 与 HTTP 的区别

HTTP是在过去很长一段时间经常用到的一种传输协议。HTTP协议传输的数据都是未加密的，这就意味着用户填写的密码、账号、交易记录等机密信息都是明文，随时可能被泄露、窃取、篡改，被黑客加以利用，因此使用HTTP协议传输隐私信息非常不安全。

HTTPS是一种基于SSL协议的网站加密传输协议，网站安装SSL证书后，使用HTTPS加密协议访问，可激活客户端浏览器到网站服务器之间的“SSL加密通道”（SSL协议），实现高强度双向加密传输，防止传输数据被泄露或篡改。简单讲HTTPS=HTTP+SSL，是HTTP的安全版。

如何将网站协议由 HTTP 换成 HTTPS

如果您需要实现网站HTTPS化，可通过购买SSL证书并部署在网站对应的服务器上来实现。

SSL证书采用SSL协议进行通信，SSL证书部署到服务器后，服务器端的访问将启用HTTPS协议。您的网站将会通过HTTPS加密协议来传输数据，可帮助服务器端和客户端之间建立加密链接，从而保证数据传输的安全。

1.4 什么是公钥和私钥?

公钥和私钥就是俗称的不对称加密方式。公钥（Public Key）与私钥（Private Key）是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。

通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，则必须用另一个密钥才能解密。比如用公钥加密的数据就必须用私钥才能解密，如果用私钥进行加密也必须用公钥才能解密，否则将无法成功解密。

说明

私钥一般情况都是由证书持有者在自己本地生成或委托受信的第三方生成的。华为云云证书管理中申请证书时，既支持生成私钥（“证书请求文件”选择“系统生成CSR”），也支持使用用户自己生成的私钥（“证书请求文件”选择“自己生成CSR”）。建议您申请证书时，选择“系统生成CSR”，其安全性更高，也更便于统一管理。如果您选择“自己生成CSR”，则生成的私钥需要符合**创建私钥**中的要求，并自行妥善保管。一旦发生证书私钥丢失的事件，请立刻吊销已有证书并对相关域名重新申购证书。以避免因私钥丢失导致网站信息泄露等恶性事件的发生。

数字证书的原理

数字证书采用公钥体制，即利用一对互相匹配的密钥对进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。

数字证书是一个经证书授权中心（CA）数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书还有一个重要的特征就是只在特定的时间段内有效。

创建私钥

华为云云证书管理对您的私有密钥的加密算法和长度有如下要求：

- 加密算法使用RSA算法
- 加密长度至少2048位

  说明

  建议您使用2048位加密长度的SHA256摘要算法。

您可以通过以下两种方式创建您的私钥：

- 使用OpenSSL工具生成私钥

  OpenSSL是一个强大且应用广泛的安全基础库工具，您可以从“http://www.openssl.org/source/”下载最新的OpenSSL工具安装包。

  须知

  要求OpenSSL版本必须是1.0.1g或以上版本。

  安装OpenSSL工具后，在命令行模式下运行**openssl genrsa -out myprivate.pem 2048**即可生成您的私钥文件。
  - “myprivate.pem”即为您的私钥文件。
  - “2048”指定加密长度。
- 使用Keytool工具导出私钥

  Keytool工具是JDK中自带的密钥管理工具，可以制作Keystore（jks）格式的证书文件，您可以从“http://www.oracle.com/technetwork/java/javase/downloads/index.html”下载JDK工具包来获取Keytool工具。

  由于使用Keytool工具制作的公钥和私钥默认是不可以导出的，需要您从已经创建好的“.keystore”文件中导出私钥。

  在导出的文件中，以下部分的内容即是您的私钥：

  ```
  -----BEGIN RSA PRIVATE KEY-----
  ......
  -----END RSA PRIVATE KEY-----
  ```

  或者

  ```
  -----BEGIN PRIVATE KEY-----
  ......
  -----END PRIVATE KEY-----
  ```

  须知

  无论您通过哪种方式生成密钥，请您完善地保管好您的私钥文件，私钥文件一旦丢失或者损坏，您申请的对应的公钥、及数字证书都将无法使用。

1.5 公钥、私钥、数字证书的关系是什么?

根据非对称密码学的原理，每个证书持有人都有一对公钥和私钥，这两把密钥可以互为加解密。

公钥是公开的，不需要保密，而私钥是由证书持有人自己特有，并且必须妥善保管和注意保密。数字证书则是由证书认证机构（CA）对证书申请者真实身份验证之后，用CA的根证书对申请人的一些基本信息以及申请人的公钥进行签名（相当于加盖发证书机构的公章）后形成的一个数字文件。

数字证书就是经过CA认证过的公钥，因此数字证书和公钥一样是公开的。

可以这样说，数字证书就是经过CA认证过的公钥，而私钥一般情况都是由证书持有者在自己本地生成或委托受信的第三方生成的，由证书持有者自己负责保管或委托受信的第三方保管。

华为云的SSL证书管理中，如果您申请证书时，“证书请求文件”选择的是“系统生成CSR”，则在您的证书签发成功后，私钥和证书文件将统一放在证书文件夹内，您可通过下载证书进行获取。

如果您申请证书时，“证书请求文件”选择的是“自己生成CSR”，则在您的证书签发成功后，下载的证书仅包含一个名为“server.pem”的文件（文件中已经包含两段证书代码，分别是服务器证书和CA中间证书）。私钥为用户自行保存的，华为云SSL证书管理不提供。

1.6 为什么要使用无密码保护的私钥?

因为私钥是加载密码保护的，且华为云其他云产品在使用数字证书的过程中需要使用您提供的私钥，所以如果您的私钥是加载密码保护的，那么其它云产品在加载您的数字证书时将无法使用您的私钥，可能导致数字证书解密失败，HTTPS服务失效。因此，需要您提供无密码保护的私钥。

在您生成私钥时，请去掉密码保护后再进行上传。

如何去除私钥密码保护

如果您的密钥已经加载密码保护，可以通过OpenSSL工具运行以下命令去掉密码保护：

openssl rsa -in encryedprivate.key -out unencryed.key

其中，“encryedprivate.key”是带密码保护的私钥文件；“unencryed.key”是去掉了密码保护的私钥文件，扩展名为key或pem均可。

如果您的证书使用的是除密码保护的私钥，当需要将该证书部署给CDN时，需要检查证书文件的格式。因为CDN要求证书文件必须是RSA加密的，即私钥是以“-----BEGIN RSA PRIVATE KEY-----”开头并以“-----END RSA PRIVATE KEY-----”结尾的格式。如果证书文件不是此格式，则需要使用工具转换证书的格式。具体转换方式，请参考**主流数字证书有哪些格式?**。

什么样的私钥是有密码保护的

使用文本编辑器打开您的私钥文件，如果私钥文件是如下样式，则说明您的私钥是已加载密码保护的：

- PKCS#8私钥加密格式
```
-----BEGIN ENCRYPTED PRIVATE KEY-----
.....BASE64 私钥内容.....
-----END ENCRYPTED PRIVATE KEY-----
```
- Openssl ASN格式
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,4D5D1AF13367D726
.....BASE64 私钥内容.....
-----END RSA PRIVATE KEY-----
```

说明

用Keytool工具生成的密钥都是带有密码保护的，您可以转换成无密码的密钥文件。关于具体转换方式，请参考**主流数字证书有哪些格式？**。

1.7 主流数字证书有哪些格式?

主流的Web服务软件，通常都基于OpenSSL和Java两种基础密码库。

- Tomcat、Weblogic、JBoss等Web服务软件，一般使用Java提供的密码库。通过Java Development Kit（JDK）工具包中的Keytool工具，生成Java Keystore（JKS）格式的证书文件。
- Apache、Nginx等Web服务软件，一般使用OpenSSL工具提供的密码库，生成PEM、KEY、CRT等格式的证书文件。
- IBM的Web服务产品，如Websphere、IBM Http Server（IHS）等，一般使用IBM产品自带的iKeyman工具，生成KDB格式的证书文件。
- 微软Windows Server中的Internet Information Services（IIS）服务，使用Windows自带的证书库生成PFX格式的证书文件。

查看证书文件的格式

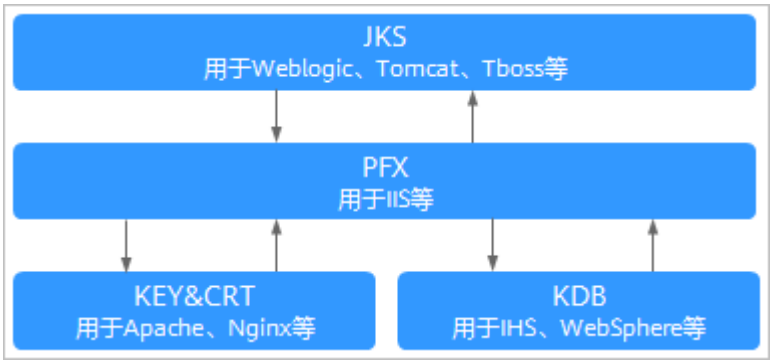
- 您可以使用以下方法简单区分带有后缀扩展名的证书文件：
  - *.DER或*.CER文件：这样的证书文件是二进制格式，只含有证书信息，不包含私钥。
  - *.CRT文件：这样的证书文件可以是二进制格式，也可以是文本格式，一般均为文本格式，功能与*.DER及*.CER证书文件相同。
  - *.PEM文件：这样的证书文件一般是文本格式，可以存放证书或私钥，或者两者都包含。*.PEM文件如果只包含私钥，一般用*.KEY文件代替。
  - *.PFX或*.P12文件：这样的证书文件是二进制格式，同时包含证书和私钥，且一般有密码保护。
- 您也可以使用记事本直接打开证书文件。如果显示的是规则的数字和字母，则表示该证书文件是文本格式。

  举例：
```
—–BEGIN CERTIFICATE—–
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
—–END CERTIFICATE—–
```
  - 如果存在“——BEGIN CERTIFICATE——”，则说明这是一个证书文件。
  - 如果存在“—–BEGIN RSA PRIVATE KEY—–”，则说明这是一个私钥文件。

证书格式转换

证书格式之间是可以互相转换的，如**图1-1**所示。

图 1-1 证书格式转换



您可使用以下方式实现证书格式之间的转换：

- 将JKS格式证书转换为PFX格式

  您可以使用JDK中自带的Keytool工具，将JKS格式证书文件转换成PFX格式。

  例如，您可以执行以下命令将“server.jks”证书文件转换成“server.pfx”证书文件：

  keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -srcstoretype JKS -deststoretype PKCS12

- 将PFX格式证书转换为JKS格式

  您可以使用JDK中自带的Keytool工具，将PFX格式证书文件转换成JKS格式。

  例如，您可以执行以下命令将“server.pfx”证书文件转换成“server.jks”证书文件：

  keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks -srcstoretype PKCS12 -deststoretype JKS

- 将PEM/KEY/CRT格式证书转换为PFX格式

  您可以使用**OpenSSL**工具，将KEY格式密钥文件和CRT格式公钥文件转换成PFX格式证书文件。

  例如，将您的KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）复制至OpenSSL工具安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pfx”证书文件：

  openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt

- 将PFX格式证书转换为PEM/KEY/CRT格式

  您可以使用**OpenSSL**工具，将PFX格式证书文件转化为PEM格式证书文件、KEY格式密钥文件和CRT格式公钥文件。

  例如，将您的PFX格式证书文件复制至OpenSSL安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pem”证书文件、KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）：

  openssl pkcs12 -in server.pfx -nodes -out server.pem

  openssl rsa -in server.pem -out server.key

  openssl x509 -in server.pem -out server.crt

须知

此转换步骤是专用于通过OpenSSL工具生成私钥和CSR申请证书文件，并且通过此方法您还可以在获取到PEM格式证书公钥的情况下，分离出私钥。在您实际部署数字证书时，请使用通过此转换步骤分离出来的私钥和您申请得到的公钥证书匹配进行部署。

1.8 SSL 证书中包含哪些信息?

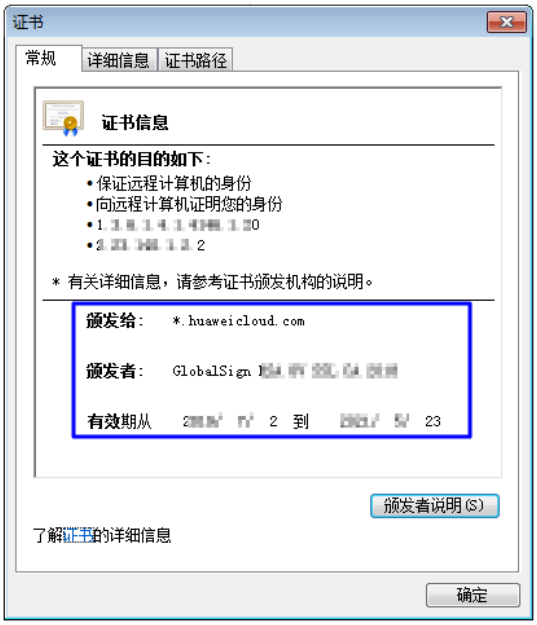
签发并部署成功后的证书包含的信息如下：

1. 地址栏：安全锁、Https标志、企业名称（仅EV类型证书）。
   示例：增强型EV证书在Chrome浏览器的显示效果

2. 常规：证书的使用者、颁发者和有效期。

   图 1-2 证书常规信息示例

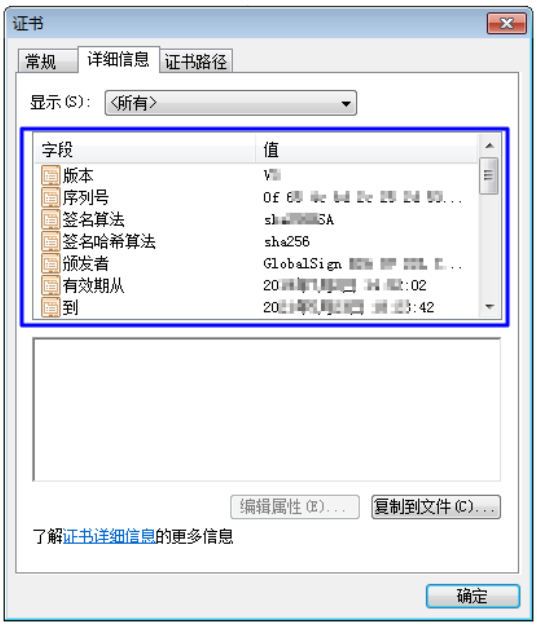
   

3. 详细信息：证书版本、序列号、签名算法、加密算法、公钥、有效期及使用者的详细信息（如省市、企业名称、部门等）等。

   说明

   在申请证书时，填写的“公司联系人/授权人信息”（联系人姓名、手机号码），涉及用户个人信息的内容，证书签发后不会包含在证书中。

图 1-3 证书详细信息示例



1.9 SSL 证书可以跨区域、跨账号或跨平台使用吗?

SSL 证书是否可以跨区域使用

可以。

SSL证书管理服务是全局服务，不论是在哪个区域购买的证书，均可在其他区域进行使用。

SSL 证书是否可以跨账号使用

可以。

SSL证书签发后，可跨账号进行使用。

- 示例1：

  A账号购买的SSL证书，证书签发后可以给B账号的服务器使用。

  因为证书是绑定域名，所以，要求域名和证书绑定的域名一致，否则会报不安全。

- 示例2：

  A账号下的证书可以使用部署功能将证书部署到A账号下的其他云产品，比如WAF、ELB、CDN等。

  但是，A账号下的证书不能跨账号部署到B账号下的产品。

  如需在B账号下使用A账号中申请的证书，则可先将A账号中申请的证书下载后，再在B账号中进行使用。

SSL 证书是否可以跨平台使用

可以。

SSL证书不限定使用平台。

SSL证书签发后，即可在SSL证书管理服务中下载证书文件。

获取证书文件后，用户可根据自己的需求部署到网站对应的服务器上，或对应的云产品中。

对于部署环境，可以部署在华为云服务器上，也可以部署在非华为云的服务器上。

1.10 SSL 证书购买后一直未使用，是否还可以使用?

证书有效期从签发日开始计算。证书签发时间是指申请证书、并通过了CA中心的审核验证后，证书最终签发的时间。

多域名类型的证书，如果是新增附加域名，证书有效期是从第一次签发日开始计算。

请根据您的情况进行查看证书是否可用：

- 如果您购买了证书，但未申请证书，证书未签发：

  可以使用。

  证书有效期是从签发日开始计算的，因此，您可以在申请证书后进行使用。申请证书详细操作请参见**提交SSL证书申请**。
- 如果您购买了证书，证书已签发，但仍在有效期内：

  证书在有效期内可以继续使用。
- 如果您购买了证书，证书已签发，且证书已过期：

  无法继续使用。

1.11 SSL 证书是否支持升级?

不支持。

证书签发后，证书类型将不可升级，且证书信息将不可修改（如证书绑定的域名、证书有效期、证书品牌等）。

如需绑定其他域名、更换证书品牌或修改证书有效期，请重新申请新的证书。

1.12 SSL 证书对服务器端口是否有限制?

没有限制。SSL证书是绑定域名使用的，和服务器端口没有任何关系。

1.13 在控制台访问 SSL 证书管理服务时，为什么服务显示没有权限访问或操作按钮显示为灰色?

在控制台访问SSL证书管理服务时，出现服务显示没有权限访问或操作按钮显示为灰色的情况，请参照以下步骤进行处理：

在SSL证书管理服务中，无论是您的账号权限不足还是账号欠费，系统均会提示您没有执行此操作的权限。

- 如果您的权限不足，请联系您的管理员开通权限。开通后，再执行相应操作。
- 如果您的账号已欠费，请您进行充值。充值后，再执行相应操作。

2 区域与可用区

2.1 什么是区域和可用区?

什么是区域、可用区?

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图2-1阐明了区域和可用区之间的关系。

图 2-1 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2.2 哪些区域提供 SSL 证书管理?

SSL证书管理服务属于全局服务，所有区域都提供SSL证书管理服务。

由于SSL证书的签发是由证书CA机构平台签发的，而非华为云直接签发，因此，证书的使用不受购买区域的限制，购买后可全球使用。

3 SSL 证书申购

3.1 SSL 证书选型类

3.1.1 如何选择 SSL 证书?

购买证书时，需要根据您的需要选择对应的证书，本章节将介绍如何选择证书类型、证书品牌、域名类型。

各证书之间的区别，请参考**各证书之间的区别**。

如何选择证书类型

购买SSL证书时，SSL证书管理服务支持的“证书类型”分为“OV”、“OV Pro”、“EV”、“EV Pro”、“DV（Basic）”5种类型。

- 对于一般企业，建议购买OV及以上类型的数字证书。对于金融、支付类企业，建议购买EV型证书。
- 移动端网站或接口调用，建议您使用OV及以上类型的证书。
- 如果您的网站主体是个人（即没有企业营业执照），只能申请DV（Basic）基础版数字证书。

如何选择证书品牌

目前云证书管理支持购买的证书品牌及不同品牌支持签发的证书类型如下表所示：

表 3-1 证书品牌说明

证书品牌	说明	是否支持DV（域名型）SSL证书	是否支持OV（企业型）SSL证书	是否支持EV（增强型）SSL证书
DigiCert	DigiCert（原Symantec）是全球最大、最权威的数字证书颁发机构。全球著名的数字证书提供商，服务范围超过150多个国家，拥有超过10万客户。 优势：安全、稳定、兼容性好。受银行、金融等行业青睐，适用于高安全性要求的数字交易场景。	是 支持单域名、泛域名。	是 支持单域名、多域名、泛域名和IP地址。	是 支持单域名、多域名。
GeoTrust	GeoTrust是全球第二大数字证书颁发机构，也是身份认证和信任认证领域的领导者。公司服务于各大中小型企业，一直致力于用最低的价格来为客户提供最好的服务。 优势：该品牌是DigiCert旗下的子品牌。安全、稳定、兼容性好、HTTPS防护门槛低、性价比高。	是 支持单域名、泛域名。	是 支持单域名、多域名、泛域名和IP地址。	是 支持单域名、多域名。
GlobalSign	GlobalSign成立于1996年，是全球最早的数字证书认证机构之一。它是一家声誉卓著，备受信赖的CA中心和SSL数字证书提供商，并在全球拥有众多合作伙伴。 优势：签发速度快、验证速度快。该品牌是华为云、大型电商企业都在用的证书，全系标配的RSA+ECC算法，资源占用少。	否	是 支持单域名、多域名、泛域名和IP地址。	是 支持单域名、多域名。

惠赠活动：

- 单域名：以域名www.a.com和根域名a.com为例进行说明

图 3-1 品牌惠赠活动

- 泛域名：以域名*.a.com和*.a.b.com为例进行说明

图 3-2 品牌惠赠活动

如何选择域名类型

购买SSL证书时，需要根据您的域名类型，选择对应的域名类型证书。SSL证书管理服务支持的“域名类型”有“单域名”、“多域名”和“泛域名”3种类型。

表 3-2 域名类型

参数名称	参数说明
单域名	单域名类型证书。 仅支持绑定1个普通域名。 如果您仅有一个域名，则选择单域名类型。

参数名称	参数说明
多域名	多域名类型证书 • 可以绑定多个不同的域名，域名可包含多个单域名。如购买多域名类型证书，域名数量为3的场景，可同时支持example.com、example.cn、test.com3个域名。 • 有几个域名需要绑定在同一个SSL证书里，则需要选择对应的域名数量。 • 由于各个证书品牌针对www型域名有不同的惠赠活动，具体的详见**如何选择证书品牌**，导致多域名证书在绑定www型域名时，有如下限制（以下以域名www.a.com和根域名a.com为例进行说明）。 – DigiCert和GeoTrust品牌，为www.a.com或者a.com购买的证书，该证书同时支持防护另一个域名，即如果您购买的是这两个品牌的多域名证书，且同时需要防护www.a.com和a.com，只需要且只能绑定其中一个域名即可。 • 域名数量范围为“2~250”，支持最多绑定250个域名。 如果您有多个域名，则选择多域名类型。需要根据域名个数，在购买页面购买对应的域名数量。
泛域名（通配符域名）	泛域名类型证书，也叫通配符证书 • 仅支持绑定1个泛域名。 • 泛域名一般格式带1个通配符“*”且以“*.”开头，例如，*.huaweicloud.com、 *.example.huaweicloud.com等。 • 仅支持同级匹配，例如：绑定*.huaweicloud.com通配符域名的数字证书，支持p1.huaweicloud.com，但不支持p2.p1.huaweicloud.com。如果需要支持p2.p1.huaweicloud.com的泛域名证书，则还需要购买一张*.p1.huaweicloud.com的泛域名证书。更多级别匹配规则请参见**表3-3**。 如果您的域名未跨级别，则选择泛域名类型。

说明

如果您有≥1个泛域名和≥1个普通域名需要绑定在同一个SSL证书里，具体操作方法请参见**多泛域名和混合域名证书的申请方法**。

购买泛域名证书，需要注意泛域名证书匹配域名的规则。只能匹配同级别的子域名，不能跨级匹配，具体示例如**表3-3**所示。

表 3-3 泛域名匹配规则示例

域名	匹配的域名	不匹配的域名
*.huaweicloud.com	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名
*.test.huaweicloud.com	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名	abc.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名

须知

- 泛域名的数字证书中，仅根域名包含域名主体本身。泛域名证书只能匹配同级别的子域名，不能跨级匹配。匹配规则具体如下：
  - 如果泛域名证书的主域名为一级域名，云证书管理服务默认赠送主域名。例如：您购买的泛域名证书为*.huaweicloud.com其包含了huaweicloud.com，为您默认赠送huaweicloud.com域名，无需再购买证书绑定huaweicloud.com。
  - 如果泛域名证书的主域名不是一级域名，例如：您购买的泛域名证书为*.p1.huaweicloud.com其不包含p1.huaweicloud.com，则不会赠送p1.huaweicloud.com或huaweicloud.com，只能匹配同级别的域名。如果需要绑定p1.huaweicloud.com或huaweicloud.com，则需要购买证书来进行绑定。
- 具体的域名中如果填写的是www的三级域名，则包含了主域名本身。例如：www.huaweicloud.com域名绑定的数字证书包含了huaweicloud.com，无需再购买证书绑定huaweicloud.com。
- 您的数字证书一旦颁发后，将无法修改域名信息等。

具体选择示例如表3-4所示：

表 3-4 选择域名类型示例

场景示例	域名情况示例	选择域名类型	选择域名数量
您仅有一个域名	示例1：huaweicloud.com	单域名	单域名类型，“域名数量”固定为“1”
	示例2：test.huaweicloud.com	单域名	
	示例3：p1.test.huaweicloud.com	单域名	

场景示例	域名情况示例	选择域名类型	选择域名数量
您有多个域名	示例1：2个域名 huaweicloud.com、p1.huawei.com	多域名	2
	示例2：3个域名 huaweicloud.com、p1.huawei.com和p1.test.huaweicloud.cn	多域名	3
	示例3：4个域名 huaweicloud.com、test.huaweicloud.cn、p1.test.huaweicloud.cn和p1.test.yun.huaweicloud.com	多域名	4
您有多个域名，且在同一个级别	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等，均在一个级别，在*.huaweicloud.com的包含范围内	泛域名	泛域名类型，“域名数量”固定为“1”

3.1.2 如何申请入门级 SSL 证书?

该任务指导用户如何申请入门级SSL证书

华为云SSL证书管理服务中，GeoTrust品牌提供有入门级SSL证书。

前提条件

购买证书的IAM用户已被授予SCM Administrator/SCM FullAccess和BSS Administrator权限。

步骤一：购买证书

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理”，并在SSL证书管理界面右上角，单击“购买证书”，进入购买证书页面。

步骤3 在购买证书页面，配置购买参数，具体参数说明如**表3-5**所示。

表 3-5 购买证书参数配置

参数名称	参数说明
证书类型	选择证书类型。 此处请选择“DV（Basic）”。

参数名称	参数说明
证书品牌	选择证书品牌。 此处请选择“GeoTrust”。
域名类型	选择域名类型，可选择“单域名”和“泛域名”，请根据需要进行选择。 • 单域名：即单个证书只支持绑定1个域名。该域名可以是二级域名domain.com，也可以是三级域名example.domain.com，都可以支持。但不支持一级域名下的所有子域名，例如：domain.com、ssl.domain.com、ssl.ssl.domain.com分别为一个域名，domain.com不包含ssl.domain.com等子域名。 • 泛域名：即单个证书支持绑定一个且只有一个泛域名。泛域名只允许添加一个通配符，例如*.domain.com，*.example.domain.com。*.*.domain.com多个通配符的泛域名是不支持的。 泛域名类型支持的域名请参见**泛域名证书支持哪些域名?**。
域名数量	选择域名数量。 此处无需配置，域名数量限制为1个。
有效期	选择证书的有效期。 SSL证书目前支持“1年”的有效期。证书有效期从签发日开始计算。证书签发时间是指申请证书、并通过了CA中心的审核验证后，证书最终签发的时间。证书到期后，需要重新购买。
购买量	设置购买的证书个数。您可以根据您的需要设置购买量。

步骤4 确认参数配置无误后，在页面右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

步骤5 确认订单无误后，阅读并勾选“我已阅读并同意《云证书管理服务（CCM）免责声明》”，单击“去支付”。

步骤6 在购买页面，请选择付款方式进行付款。

成功付款后，可以在“SSL证书管理 > SSL证书列表”，查看已购买的证书。

- 查看已购买**付费**证书，请单击“SSL证书”页签。
- 查看已购买**测试**证书，请单击“测试证书”页签。

----结束

步骤二：提交证书申请

成功购买证书后，您需要为证书绑定域名、填写证书申请人的详细信息并提交审核。

提交SSL证书申请的详细操作请参见**提交SSL证书申请**。

须知

“域名信息”中，“域名验证方式”仅可选择“DNS验证”。

步骤三：DNS 验证

DNS验证，是指在域名管理平台通过解析指定的DNS记录，验证域名所有权。

在您提交证书申请后，需要按照证书列表页面的提示完成域名授权验证配置，否则证书将一直处于“待完成域名验证”状态，且您的证书将无法通过审核。

DNS验证方式详细操作请参见**域名DNS解析**。

步骤四：签发证书

DNS验证通过之后，CA机构将还需要一段时间进行处理，请您耐心等待。

CA机构审核通过后，将会签发证书。证书签发后便立即生效，即可部署证书到华为云其他云产品或下载证书并部署到服务器上进行使用。

3.1.3 多泛域名和混合域名证书的申请方法

如果您需要一张证书中包含一个或一个以上的泛域名和一个或一个以上的普通域名，请按照本章节进行操作。

关于域名类型的解释，请参考**域名的相关概念**。

购买证书前，请注意以下问题：

整理需要绑定的域名，泛域名数量、普通域名数量，该证书要求至少要有2个或2个以上的域名。

关于泛域名的匹配关系，请参考**泛域名证书支持哪些域名？** 。

操作步骤

以下操作将以1个泛域名和2个普通域名为例进行说明。

步骤1 登录**云证书管理服务控制台**。

步骤2 在界面右上方，选择“工单 > 新建工单”，进入“新建工单”页面。

图 3-3 新建工单

步骤3 在“新建工单”页面，填写工单后提交工单。

请在“问题描述”中按照以下方式进行填写：

问题描述：

标题：组合证书购买

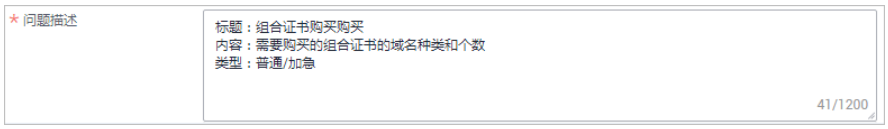
购买内容：需要购买的组合证书的域名种类和个数

类型：普通/加急

示例：

如果您需要购买1个泛域名和2个普通域名，则填写如图3-4所示。

图 3-4 问题描述



提交工单后，请耐心等待3~5个工作日，期间请保持手机畅通，工程师将会与您联系。

----结束

后续处理

证书购买后，还需要进行**提交证书申请**、**域名验证**、**组织验证**操作，请根据提示进行操作。

3.1.4 SSL 证书购买后，可以修改证书品牌、证书类型、域名类型等信息吗?

在CCM中成功购买SSL证书后，将无法修改证书品牌、证书类型、域名类型、有效期等信息。

如修改证书品牌、证书类型等信息，则需要重新进行购买。

3.2 域名填写类

3.2.1 申请 SSL 证书时，如何填写证书中绑定的域名?

SSL证书管理中的证书是绑定域名的，因此购买证书时，需要根据您的域名情况，选择对应的域名类型。

如果您想了解域名的相关概念，请参见**域名的相关概念**。

选择域名类型并成功购买证书后，需要将对应的域名绑定给已购买的证书，即需要在SSL证书管理控制台补全证书审核资料。而申请证书的第一步就是填写域名信息，将对应的域名绑定给已购买的证书。

SSL证书管理控制台会根据您购买的证书提示您需要输入的域名类型。

如果您申请的DV证书，绑定的域名含有edu、gov、bank、live等敏感词，可能无法通过安全审核，建议选择OV或EV证书，目前已知敏感词请参见**敏感词**。

各域名类型具体说明如**表3-6**所示，更多参考内容可查看具体示例。

表 3-6 绑定域名

参数名称	参数说明
单域名	仅可绑定1个普通域名。 绑定域名时，绑定1个普通域名即可。
多域名	• 可绑定多个域名（购买的域名数量为几，则可绑定几个域名）。 • 申请证书时，需要将其中一个域名设置为“主域名”，其他域名则设置为“附加域名”。您可根据自己实际情况进行选择。 例如，您购买的域名数量为3，则将其中1个域名设置为主域名，其他2个域名则设置为附加域名。 **须知** • 主域名和附加域名的关系（主从关系）对添加的域名没有影响。
泛域名	仅可绑定1个泛域名。 绑定域名时，绑定1个含*的泛域名即可。

具体示例：

- 单域名型证书

  当您购买的是单域名型证书，则仅支持绑定一个普通域名。

  示例：您的域名为huaweicloud.com

  申请证书时，则在“绑定域名”中填写huaweicloud.com即可，如图3-5所示。

  图 3-5 单域名绑定域名

- 多域名型证书

  当您购买的是多域名型证书，则可绑定多个域名（购买的域名数量为几，则可绑定几个域名）。

  申请证书时，需要将其中一个域名设置为“主域名”，其他域名则设置为“附加域名”。您可根据自己实际情况进行选择。附加域名可分批次多次录入，具体操作请参见**新增附加域名**。

  须知

  - 主域名和附加域名的关系（主从关系）对添加的域名没有影响。

  示例：如果购买的域名数量为3，且您的域名为huaweicloud.com、test.huaweicloud.com和huaweicloud.cn

  申请证书时，则在“绑定主域名”中填写huaweicloud.com，“绑定附加域名”填写test.huaweicloud.com和huaweicloud.cn。多个附加域名需要换行输入，如图3-6所示。

图 3-6 多域名绑定域名

- 泛域名型证书

  当您购买的是泛域名型证书，则支持绑定一个泛域名。

  示例：您的域名为test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com、good.huaweicloud.com等，均在同一个级别

  申请证书时，则在“绑定域名”中填写“*.huaweicloud.com”，如图3-7所示。

图 3-7 泛域名绑定域名

3.2.2 SSL 证书管理服务中，单域名、多域名、泛域名的区别是什么？

SSL证书管理服务支持的“域名类型”有“单域名”、“多域名”和“泛域名”3种类型。

表 3-7 域名类型

参数名称	参数说明
单域名	仅支持绑定1个普通域名。 如果您仅有一个域名，则选择单域名类型。
多域名	• 可以绑定多个不同的域名，域名可包含多个单域名。如购买多域名类型证书，域名数量为3的场景，可同时支持example.com、example.cn、test.com3个域名。 • 有几个域名需要绑定在同一个SSL证书里，则需要选择对应的域名数量。 • 由于各个证书品牌针对www型域名有不同的惠赠活动，具体的详见**如何选择SSL证书？**，导致多域名证书在绑定www型域名时，有如下限制（以下以域名www.a.com和根域名a.com为例进行说明）。 – DigiCert和GeoTrust品牌，为www.a.com或者a.com购买的证书，该证书同时支持防护另一个域名，即如果您购买的是这两个品牌的多域名证书，且同时需要防护www.a.com和a.com，只需要且只能绑定其中一个域名即可。 • 域名数量范围为“2~250”，支持最多绑定250个域名。 如果您有多个域名，则选择多域名类型。需要根据域名个数，在购买页面购买对应的域名数量。

参数名称	参数说明
泛域名	• 仅支持绑定1个泛域名。 • 泛域名一般格式带1个通配符“*”且以“*.”开头，例如，*.huaweicloud.com、 *.example.huaweicloud.com等。 • 仅支持同级匹配，例如：绑定*.huaweicloud.com通配符域名的数字证书，支持p1.huaweicloud.com，但不支持p2.p1.huaweicloud.com。如果需要支持p2.p1.huaweicloud.com的通配符域名数字证书，则还需要购买一张*.p1.huaweicloud.com的通配符域名证书。更多级别匹配规则请参见**表3-8**。 如果您的域名在同一个级别，且未跨级别，均在一个级别，则选择泛域名类型。

购买泛域名证书，需要注意泛域名证书匹配域名的规则。只能匹配同级别的子域名，不能跨级匹配，具体示例如**表3-8**。

表 3-8 泛域名匹配规则示例

域名	匹配的域名	不匹配的域名
*.huaweicloud.com	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名
*.test.huaweicloud.com	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名	abc.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名

须知

- 泛域名的数字证书中，仅根域名包含域名主体本身。泛域名证书只能匹配同级别的子域名，不能跨级匹配。匹配规则具体如下：
  - 如果泛域名证书的主域名为一级域名，云证书管理服务默认赠送主域名。例如：您购买的泛域名证书为*.huaweicloud.com其包含了huaweicloud.com，为您默认赠送huaweicloud.com域名，无需再购买证书绑定huaweicloud.com。
  - 如果泛域名证书的主域名不是一级域名，例如：您购买的泛域名证书为*.p1.huaweicloud.com其不包含p1.huaweicloud.com，则不会赠送p1.huaweicloud.com或huaweicloud.com，只能匹配同级别的域名。如果需要绑定p1.huaweicloud.com或huaweicloud.com，则需要购买证书来进行绑定。
- 具体的域名中如果填写的是www的三级域名，则包含了主域名本身。例如：

  www.huaweicloud.com域名绑定的数字证书包含了huaweicloud.com，无需再购买证书绑定huaweicloud.com。
- 您的数字证书一旦颁发后，将无法修改域名信息等。

具体选择示例如表3-9所示：

表 3-9 选择域名类型示例

场景示例	域名情况示例	选择域名类型	选择域名数量
您仅有一个域名	示例1：huaweicloud.com	单域名	单域名类型，“域名数量”固定为“1”
	示例2：test.huaweicloud.com	单域名	
	示例3：p1.test.huaweicloud.com	单域名	
您有多个域名	示例1：2个域名 huaweicloud.com、p1.huawei.com	多域名	2
	示例2：3个域名 huaweicloud.com、p1.huawei.com和p1.test.huaweicloud.cn	多域名	3
	示例3：4个域名 huaweicloud.com、test.huaweicloud.cn、p1.test.huaweicloud.cn和p1.test.yun.huaweicloud.com	多域名	4
您有多个域名，且在同一个级别	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等，均在一个级别，在*.huaweicloud.com的包含范围内	泛域名	泛域名类型，“域名数量”固定为“1”

3.2.3 SSL 证书与域名的关系?

SSL证书需要绑定域名使用，故您在购买证书时需要确认证书类型、证书品牌、域名类型，并在申请证书时，根据已选择的域名类型，正确填写需要绑定目标SSL证书的域名。

一个 SSL 证书能够绑定几个域名

用户在购买证书时，需要根据实际情况选择域名类型。域名类型不同，支持绑定的域名数量也差异。具体的情况如**表3-10**所示。

表 3-10 不同的域名类型可绑定的域名数量

证书类型	支持的域名类型	可绑定的域名数量
OV、OV Pro	单域名	1个。
	多域名	域名数量范围为“2~250”，支持最多绑定250个域名。
	泛域名	1个。 泛域名类型支持的域名请参见**泛域名证书支持哪些域名?** 。
EV、EV Pro	单域名	1个。
	多域名	域名数量范围为“2~250”，支持最多绑定250个域名。
DV基础版（GeoTrust入门级SSL证书）	单域名	1个。
	泛域名	1个。 泛域名类型支持的域名请参见**泛域名证书支持哪些域名?** 。
DV基础版（DigiCert免费SSL证书）	单域名	1个。

一个域名能绑定几张 SSL 证书

没有限制，即同一个域名，您可以根据需要购买多张证书绑定该域名，您选择应用到服务产品中或者安装到服务器使用的证书，即该证书生效。

证书是一次性的，当目前的证书不能满足您的要求或者证书即将过期，您可以再购买新的可匹配该域名类型的证书，将新证书配置到目标域名使用。

相关操作:

- **如何将SSL证书应用到华为云产品?**

- 如何在服务器上安装SSL证书?

3.2.4 泛域名证书支持哪些域名?

华为云SSL证书管理服务支持申请泛域名类型的证书，用户可以通过泛域名证书保护服务器的单个域名和该域名下同级别的所有子域名。OV企业型、OV Pro企业型专业版和DV基础版（GeoTrust入门级SSL证书）类型证书支持泛域名。

如果您拥有多个同级别子域名服务器，使用泛域名证书即可，无需为每个子域名单独购买和安装证书。

须知

- 泛域名的数字证书中，仅根域名包含域名主体本身。泛域名证书只能匹配同级别的子域名，不能跨级匹配。匹配规则具体如下：
  - 如果泛域名证书的主域名为一级域名，云证书管理服务默认赠送主域名。例如：您购买的泛域名证书为*.huaweicloud.com其包含了huaweicloud.com，为您默认赠送huaweicloud.com域名，无需再购买证书绑定huaweicloud.com。
  - 如果泛域名证书的主域名不是一级域名，例如：您购买的泛域名证书为*.p1.huaweicloud.com其不包含p1.huaweicloud.com，则不会赠送p1.huaweicloud.com或huaweicloud.com，只能匹配同级别的域名。如果需要绑定p1.huaweicloud.com或huaweicloud.com，则需要购买证书来进行绑定。
- 您的数字证书一旦颁发后，将无法修改域名信息等。

购买泛域名证书，需要注意泛域名证书匹配域名的规则。只能匹配同级别的子域名，不能跨级匹配，域名级别说明请参见**域名的相关概念**。

匹配示例如**表3-11**所示。

表 3-11 泛域名匹配规则示例

域名	匹配的域名	不匹配的域名
*.example.com	abc.example.com、sport.example.com、good.example.com等域名	mycard.good.example.com、mycalc.good.example.com等域名
*.good.example.com	mycard.good.example.com、mycalc.good.example.com等域名	abc.example.com、sport.example.com、good.example.com等域名

3.2.5 申请 SSL 证书时应该使用哪个域名?

关于申请SSL数字证书时应该如何选择申请域名，本文将通过一个简单的示例进行描述。

例如，您的网站为“www.domain.com”。其中，有一个用户登录页面“http://www.domain.com/login.asp”，您想要申请一张SSL数字证书确保用户输入用户名和密码时的安全，确保用户信息不会在传输过程中被非法窃取。同时，还有一个用户登

录的信息管理页面“http://www.domain.com/oa/manage.asp”，您也希望使用SSL数字证书来保障内部管理系统中的机密信息的安全。这种情况下，您使用域名“www.domain.com”申请SSL数字证书即可实现对这类页面的保护。

如果您的网站访问量较大，建议您为需要使用SSL数字证书的页面设置一个独立的Web服务器（HTTP server），并使用一个独立的域名来申请SSL数字证书，例如：secure.domain.com或ssl.domain.com。

须知

“https://”的使用必须与申请SSL数字证书的域名一致，否则浏览器可能会出现“安全证书上的名称无效,或者与站点名称不匹配”警告。请根据您网站的具体情况使用合适的域名来申请SSL数字证书。

3.2.6 主域名绑定后，是否可以修改?

请根据实际情况进行处理：

- 证书未签发：

  可以。

  如果证书未签发，且需要修改主域名，则可撤回证书申请，绑定新的主域名后，再重新提交证书申请。

- 证书已签发：

  不可以。

  证书已签发，暂不支持修改已绑定的主域名。如果需要修改主域名，则需要重新购买证书。

3.2.7 主域名和附加域名的关系对域名有没有什么影响?

当证书域名类型为“多域名”时，申请证书时，您可以添加1个主域名、至少添加1个附加域名，多个附加域名间需要换行输入。

例如，您购买的域名数量为3，则将其中1个域名设置为主域名，其他2个域名则设置为附加域名。

须知

- 主域名和附加域名的关系（主从关系）对添加的域名没有影响。

具体如何填写请参见**申请SSL证书时，如何填写证书中绑定的域名?** 。

3.2.8 如何制作 CSR 文件?

在申请数字证书之前，您必须先生成证书私钥和证书请求文件（Certificate Signing Request，简称CSR）。CSR文件是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给CA认证中心进行审核。

说明

建议您使用系统提供的创建CSR功能，避免出现内容不正确而导致的审核失败。关于审核失败详细信息，请参考**如何解决“审核失败 - 主域名不能为空”的问题？**。

手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥。

此处提供2种制作方法，请根据您的需要进行选择：

- **使用OpenSSL工具生成CSR文件**
  如果您需要输入中文信息，建议您使用Keytool工具生成CSR文件。
- **使用Keytool工具生成CSR文件**

须知

证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。

使用 OpenSSL 工具生成 CSR 文件

步骤1 安装**OpenSSL**工具。

步骤2 执行以下命令生成CSR文件。

openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout *myprivate.key* -out *mydomain.csr*

- -new：指定生成一个新的CSR。
- -nodes：指定私钥文件不被加密。
- -sha256：指定摘要算法。
- -newkey rsa:2048：指定私钥类型和长度。
- -keyout：生成私钥文件，名称可自定义。
- -out：生成CSR文件，名称可自定义。

步骤3 生成CSR文件“mydomain.csr”。

图 3-8 生成 CSR 文件

```
Generating a 2048 bit RSA private key
....+++
.....................................................................+++
writing new private key to 'myprivate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
[Country Name (2 letter code) [CN]:CN
[State or Province Name (full name) []:ZheJiang
[Locality Name (eg, city) [Default City]:HangZhou
[Organization Name (eg, company) [Default Company Ltd]:HangZhou xxx Technologies,Inc.
[Organizational Unit Name (eg, section) []:IT Dept.
[Common Name (eg, your name or your server's hostname) []:www.example.com
[Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
[A challenge password []:
[An optional company name []:
```

需要输入的信息说明如下：

字段	说明	示例
Country Name	申请单位所属国家，只能是两个字母的国家码。例如，中国只能是CN。	CN
State or Province Name	申请单位所在省名或州名，可以是中文或英文。	ZheJiang
Locality Name	申请单位所在城市名，可以是中文或英文。	HangZhou
Organization Name	申请单位名称法定名称，可以是中文或英文。	HangZhou xxx Technologies, Inc.
Organizational Unit Name	申请单位的所在部门，可以是中文或英文。	IT Dept.
Common Name	申请证书的具体网站域名。 **说明** • 多域名类型的证书，请填写需要绑定的主域名。 • 泛域名类型的证书，请填写泛域名。示例：*.example.com	www.example.com
Email Address	申请单位的邮箱。 无需输入，请直接按“Enter”。	-
A challenge password	设置CSR文件密码。 无需输入，请直接按“Enter”。	-

须知

- 在使用OpenSSL工具生成中文证书时，需要注意中文编码格式必须使用UTF8编码格式。同时，需要在编译OpenSSL工具时指定支持UTF8编码格式。
- 证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。

完成命令提示的输入后，会在当前目录下生成myprivate.key（私钥文件）和mydomain.csr（CSR，证书请求文件）两个文件。

----结束

使用 Keytool 工具生成 CSR 文件

步骤1 安装Keytool工具，Keytool工具一般包含在Java Development Kit（JDK）工具包中。

步骤2 使用Keytool工具生成keystore证书文件。

说明

Keystore证书文件中包含密钥，导出密钥方式请参考**主流数字证书有哪些格式？**。

1. 执行以下命令生成keystore证书文件。

   keytool -genkey -alias mycert -keyalg RSA -keysize 2048 -keystore ./mydomain.jks

   - -keyalg：指定密钥类型，必须是RSA。
   - -keysize：指定密钥长度为2,048。
   - -alias：指定证书别名，可自定义。
   - -keystore：指定证书文件保存路径，证书文件名称可自定义。

   图 3-9 生成 keystore 证书文件

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  www.example.com
What is the name of your organizational unit?
  [Unknown]:  IT Dept.
What is the name of your organization?
  [Unknown]:  HangZhou xxx Technologies,Inc.
What is the name of your City or Locality?
  [Unknown]:  HangZhou
What is the name of your State or Province?
  [Unknown]:  ZheJiang
What is the two-letter country code for this unit?
  [Unknown]:  CN
Is CN=www.example.com, OU=IT Dept., O="HangZhou xxx Technologies,Inc.", L=HangZhou, ST=Zhe
Jiang, C=CN correct?
  [no]:  Y

Enter key password for <mycert>
        (RETURN if same as keystore password):
```

2. 输入证书保护密码，然后根据下表依次输入所需信息：

问题	说明	示例
What is your first and last name?	申请证书的域名。 **说明** - 多域名类型的证书，请填写需要绑定的主域名。 - 泛域名类型的证书，请填写泛域名。示例：*.example.com	www.example.com
What is the name of your organizational unit?	申请单位的所在部门名称。	IT Dept
What is the name of your organization?	申请单位的所在公司名称。	HangZhou xxx Technologies,Ltd
What is the name of your City or Locality?	申请单位的所在城市。	HangZhou
What is the name of your State or Province?	申请单位的所在省份。	ZheJiang

问题	说明	示例
What is the two-letter country code for this unit?	申请单位所属国家，ISO国家代码（两位字符）。	CN

输入完成后，确认输入内容是否正确，输入Y表示正确。

3. 根据提示输入密钥密码。可以与证书密码一致，如果一致直接按回车键即可。

步骤3 通过证书文件生成证书请求。

1. 执行以下命令生成CSR文件。

   keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr

   - -sigalg：指定摘要算法，使用SHA256withRSA。
   - -alias：指定别名，必须与**•-alias**中keystore文件中的证书别名一致。
   - -keystore：指定证书文件。
   - -file：指定证书请求文件（CSR），名称可自定义。

2. 根据提示输入证书密码即可以生成“mydomain.csr”。

----结束

3.2.9 系统生成的 CSR 和自己生成 CSR 的区别?

证书请求文件（Certificate Signing Request，CSR）即证书签名申请，获取SSL证书，需要先生成CSR文件并提交给CA中心。CSR包含了公钥和标识名称（Distinguished Name），通常从Web服务器生成CSR，同时创建加解密的公钥私钥对。

申请证书时，需要设置“证书请求文件”，您可以选择“系统生成的CSR”，也可手动生成CSR文件并将文件内容复制到CSR文件内容对话框中。两者之间的区别如**表3-12**所示。

表 3-12 CSR 的比较

证书请求文件	说明	区别
系统生成的CSR	系统将自动帮您生成证书私钥，并且您可以在证书申请成功后直接在证书管理页面下载您的证书和私钥。	• 选择“系统生成CSR”，在数字证书颁发后还可以支持不同格式的证书下载。 • “系统生成CSR”，下载证书后，证书文件“server.jks”和密码文件“keystorePass.txt”已自动生成好，可以直接安装使用。

证书请求文件	说明	区别
自己生成CSR	手动生成CSR文件并将文件内容复制到CSR文件内容对话框中。 详细操作请参见**如何制作CSR文件?** 。	• “自己生成CSR”的证书**不支持**一键部署到云产品。 • 手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥文件。私钥和数字证书一一对应，一旦丢失了私钥，您的数字证书也将不可使用。华为云不负责保管您的私钥，如果您的私钥丢失，您需要重新购买并替换您的数字证书。 • “自己生成CSR”，下载证书后，需要使用OpenSSL工具，将pem格式证书转换为PFX格式证书，得到“server.pfx”文件，再使用Keytool工具，将PFX格式证书文件转换成JKS格式，得到“server.jks”证书文件和“keystorePass.txt”密码文件，然后才可以安装部署。

根据以上的比较，建议您选择“系统生成CSR”，可以规避CSR内容不正确而导致证书审核失败。

3.2.10 如何导出已创建 CSR 文件?

CSR（Certificate Signing Request）即证书签名请求文件，用于证书申请者发给证书颁发机构（CA）申请SSL证书。

创建CSR的具体操作步骤请参见**创建CSR**。

导出已创建 CSR 文件

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理 >SSL证书证书列表 > CSR管理”，进入CSR管理界面。

步骤3 在已创建的CSR列表，单击目标CSR名称，如**图 CSR列表**，右侧出现目标CSR详情信息的弹框，如**图 CSR详情**。

图 3-10 CSR 列表

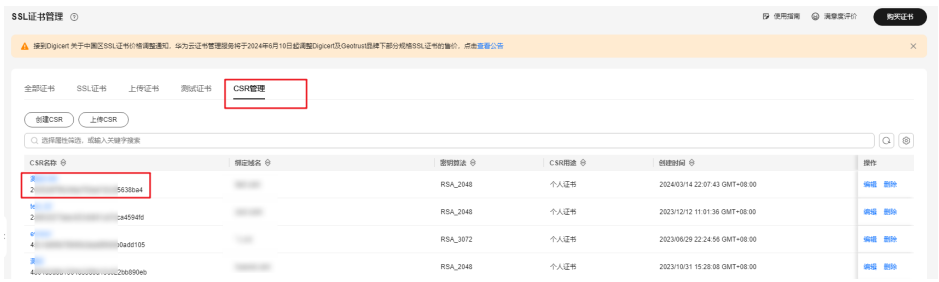
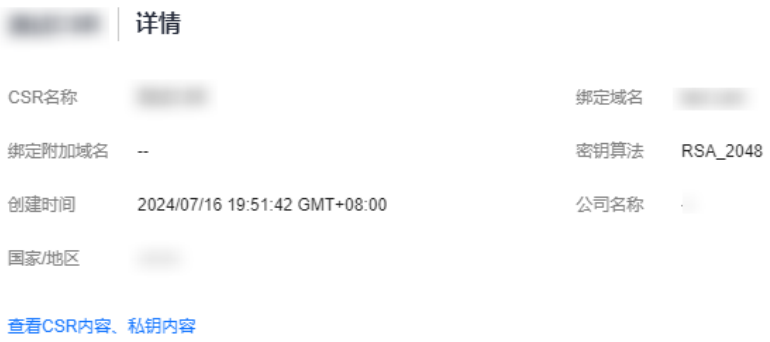


图 3-11 CSR 详情



步骤4 单击CSR详情页面“查看CSR内容、私钥内容”，如**图 查看CSR、私钥内容**。

须知

请注意妥善保管您已创建的CSR和密钥。

图 3-12 查看 CSR、私钥内容

步骤5 单击CSR文件内容框右侧“复制”。可以复制当前已创建的CSR文件内容，用于申请证书时填写，如**图 复制CSR文件**。

须知

私钥内容由用户自行保管，请避免外发。

图 3-13 复制 CSR 文件

----结束

3.2.11 域名的相关概念

- 泛域名
  泛域名是指带1个通配符“*”且以“*.”开头的域名。
  例如：“*.a.com”是正确的泛域名，但“*.*.a.com”则是不正确的。

  说明

  一个泛域名算一个域名。关于泛域名的匹配关系，请参考**泛域名证书支持哪些域名？**。
- 普通域名
  普通域名是相对泛域名来说的，是一个具体的域名或者说不是通配符域名。
  例如：“www.a.com”或“a.com”都算一个普通域名。
  普通域名能绑定的数量，取决于您证书订单中选择的域名个数。

说明

如“buy.example.com”或“next.buy.example.com”各个明细子域名都算一个域名。

- 域名级别

  域名由一或多个部分组成，这些部分通常连接在一起，并由点分隔，例如www.huaweicloud.com。最右边的一个标签是顶级域名，一个域名的层次结构，从右侧到左侧隔一个点依次下降一层。

  域名的第一级是顶级域名，顶级域名下一层是二级域名，一级一级地往下。域名层次结构具体划分情况如**表3-13**所示。

表 3-13 域名层级结构

参数名称	参数说明
顶级域名	域名中最高的一级，每个域名都以顶级域结尾。它包括通用顶级域（例如.com、.net、.org等）、国际和地区顶级域（例如.us、.cn、.tk等）和新通用顶级域名（例如.info、.biz等）。
二级域名	顶级域名下面是二级域名，它位于顶级域名的左侧。例如，在example.com中，example是二级域名。
三级域名	二级域名下面是三级域名，它位于二级域的左侧。例如，在www.example.com中，www是三级域名。
以此类推，在上一级域名最左侧进行域名级别的拓展。	

以abc.huaweicloud.com为例，进行域名层次结构说明：

.com为顶级域名。

huaweicloud.com为1个二级域名。

abc.huaweicloud.com为1个三级域名。

3.2.12 域名相关问题，该如何解决?

SSL 证书可以绑定中文域名吗?

如需绑定中文域名，请单击访问**Punycode官网**使用**Punycode编码**工具将中文域名编码，再使用编码后信息来申请证书。

示例：**华为云.com** Punycode 编码后：**xn--siq1ht8k.com**

申请证书时，绑定域名则填写**xn--siq1ht8k.com**。

申请证书时，SSL 证书绑定的域名是否需要备案通过后才能绑定?

- 证书申请时，为SSL证书绑定的域名可以没有通过备案，但是在后续域名访问中，没有备案的域名会被拦截，导致域名无法访问，所以建议您搭建好网站后立即完成域名备案。
- 无论是个人备案的域名（网站是个人网站，不含有企业、单位等非个人网站的信息），还是企业备案的域名（网站是企业或者公司网站），都支持绑定SSL证书。

华为云 SSL 证书服务中是否有通配符类型的证书?

有。

华为云SSL证书管理服务中，提供有单域名、多域名、泛域名类型的证书。

通配符类型的证书在华为云SSL证书管理服务中对应的就是泛域名类型的证书。

泛域名证书匹配域名的规则是什么，或者是否支持跨级匹配?

SSL证书管理服务中，支持购买“泛域名”类型的证书。

泛域名是指带1个通配符“*”且以“*.”开头的域名。

例如：“*.a.com”是正确的泛域名，但“*.*.a.com”则是不正确的。

购买泛域名证书，需要注意泛域名证书匹配域名的规则。只能匹配同级别的子域名，不能跨级匹配，具体示例如表3-14所示。

表 3-14 泛域名匹配规则示例

域名	匹配的域名	不匹配的域名
*.huaweicloud.com	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名
*.test.huaweicloud.com	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名	abc.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名

SCM 中，单域名类型证书，支持绑定哪些域名?

SSL证书管理服务支持的“域名类型”有“单域名”、“多域名”和“泛域名”3种类型。

其中，单域名类型的证书，仅支持绑定1个普通域名，如example.com、test.example.com分别为一个域名。

需要注意的是，example.com不包含test.example.com等子域名。如果需要支持所有二级或三级域名，请购买泛域名证书。

SCM 中，多域名类型证书，支持绑定哪些域名?

SSL证书管理服务支持的“域名类型”有“单域名”、“多域名”和“泛域名”3种类型。

其中，多域名类型的证书，可以绑定多个不同的域名，域名可包含多个单域名。如购买多域名类型证书，域名数量为3的场景，可同时支持example.com、example.cn、test.com3个域名。

有几个域名需要绑定在同一个SSL证书里，则需要选择对应的域名数量。

域名数量范围为“2~250”，支持最多绑定250个域名。

SCM 中，泛域名类型证书，支持绑定哪些域名?

SSL证书管理服务支持的“域名类型”有“单域名”、“多域名”和“泛域名”3种类型。

其中，泛域名类型的证书，仅支持绑定1个泛域名。

- 泛域名一般格式带1个通配符“*”且以“*.”开头，例如， *.huaweicloud.com、*.example.huaweicloud.com等。
- 仅支持同级匹配，例如：绑定*.huaweicloud.com通配符域名的数字证书，支持p1.huaweicloud.com，但不支持p2.p1.huaweicloud.com。如果需要支持p2.p1.huaweicloud.com的通配符域名数字证书，则还需要购买一张*.p1.huaweicloud.com的通配符域名证书。更多级别匹配规则请参见**表3-15**。

购买泛域名证书，需要注意泛域名证书匹配域名的规则。只能匹配同级别的子域名，不能跨级匹配，具体示例如**表3-15**所示。

表 3-15 泛域名匹配规则示例

域名	匹配的域名	不匹配的域名
*.huaweicloud.com	test.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名
*.test.huaweicloud.com	abc.test.huaweicloud.com、yun.test.huaweicloud.com、example.test.huaweicloud.com等域名	abc.huaweicloud.com、yun.huaweicloud.com、example.huaweicloud.com等域名

须知

- 泛域名的数字证书中，仅根域名包含域名主体本身。例如：
  - *.huaweicloud.com的泛域名数字证书包含了huaweicloud.com，还可匹配同级别的域名。无需再购买证书绑定huaweicloud.com。
  - *.p1.huaweicloud.com的泛域名数字证书不包含p1.huaweicloud.com，只能匹配同级别的域名。如果需要绑定p1.huaweicloud.com，则需要购买证书来进行绑定。
- 具体的域名中如果填写的是www的三级域名，则包含了主域名本身。例如：

  www.huaweicloud.com域名绑定的数字证书包含了huaweicloud.com，无需再购买证书绑定huaweicloud.com。
- 您的数字证书一旦颁发后，将无法修改域名信息等。

3.3 信息填写类

3.3.1 申请 SSL 证书时，个人用户如何填写企业组织信息?

华为云当前提供的OV、OV Pro、EV、EV Pro型证书均需要填写组织信息，个人将无法填写。

如果购买的是DV（Basic）型证书，则无需填写企业组织信息。

如需要个人使用的免费证书，请购买对应品牌的证书，具体操作请参见**申请免费证书**。

3.3.2 申请 SSL 证书时，“银行开户许可”和“企业营业执照”是否必须上传?

不是。

两个内容均为**可选项**，您可以根据自己的实际情况进行处理。

不上传“银行开户许可”和“企业营业执照”会延长证书的签发周期，具体延长时间取决于CA机构验证时间。

申请证书时，OV、EV类型的证书需要填写“企业组织信息”。需要填写的企业组织信息中则包含“银行开户许可”和“企业营业执照”。

图 3-14 企业组织信息

两个内容均为**可选项**，请根据自己的实际情况进行处理：

- 银行开户许可：
  如需上传，则请单击“上传文件”，上传银行开户许可证电子件。

  须知

  - 上传的文件大小限制为2MB以下，格式须为png或jpg，且仅支持上传一个文件。
  - 不上传银行开户许可会延长证书的签发周期，具体延长时间取决于CA机构验证时间。

    为了避免延长证书的签发周期，建议您上传文件。

- 企业营业执照
  如需上传，则请单击“上传文件”，上传企业营业执照电子件。
  - 中国大陆：上传企业营业执照。
  - 其他地区：上传当地的商业登记证。

  须知

  - 上传的文件大小限制为2MB以下，格式须为png或jpg，且仅支持上传一个文件。
  - 不上传企业经营许可会延长证书的签发周期，具体延长时间取决于CA机构验证时间。

    为了避免延长证书的签发周期，建议您上传文件。

3.4 问题排查类

3.4.1 免费 SSL 证书在购买、申请、安装或使用过程中，遇到问题如何处理?

免费证书的签发由系统自动完成，申请者按要求完成配置后即可获得证书。同时，免费证书建议只用于测试，如果您需要您的服务器与客户端之间建立更加安全的数据传输，建议您购买其他类型的证书。

相关操作可参见对应资料进行解决：

- **申请免费证书**
- **如何进行手动DNS验证?**
- **如何在服务器上安装SSL证书?**
- **如何将SSL证书应用到华为云产品?**

3.4.2 “提交申请”按钮灰显如何处理?

问题描述

申请证书时，“提交申请”按钮灰显，无法操作。

问题原因

- 可能原因一：欠费
- 可能原因二：权限不足

解决方法

请根据可能原因选择操作步骤：

- **原因一：欠费**

  解决方法：请您先充值，充值后再执行申请证书操作。
- **原因二：权限不足**

  解决方法：请联系您的管理员授予执行申请证书的操作权限。权限申请成功后，再执行操作。

3.4.3 提交 SSL 证书申请后，发现证书信息填写错误或变更怎么办?

哪些信息填写错误或变更会影响 SSL 证书的审核

除“联系人名字”之外，其他信息错误都会影响证书审核。

哪些信息变更或填写错误会影响 SSL 证书的使用

表 3-16 信息错误或变更的影响

填写的信息	信息错误或变更是否影响SSL证书的使用
域名	是

填写的信息	信息错误或变更是否影响SSL证书的使用
联系人姓名	否 **说明** 申请证书时，填写的“公司联系人/授权人信息”（联系人姓名、手机号码），仅用于申请证书时进行验证，证书签发后不会包含在证书中。 如果此类信息发生变更，不影响证书使用，无需处理。
联系人手机号码	
公司的信息地址	是
公司的营业范围	是

提交 SSL 证书申请后，发现证书信息错误或变更怎么办

1. 判断错误的信息是否会影响证书的审核或使用。
   - 是，执行**2**。
   - 否，请根据实际情况进行处理。
     - 未签发：请继续执行后续操作，等待证书的审核。
     - 已签发：无需处理，可正常使用证书。
2. 查看证书是否签发。
   - 证书未签发

     提交证书申请后，发现证书信息填写错误或变更，可撤回申请。

     具体的操作请参见**撤回证书申请**。
   - 证书已签发
     - 证书已签发且在规定时间内（DigiCert品牌和GeoTrust品牌：证书签发后的25天内），如果发现证书信息填写错误或变更，“单域名”和“泛域名”证书可通过重新签发功能来进行修改，具体操作请参见**重新签发**，“多域名”证书、免费证书不支持重新签发，您需要重新购买证书，具体操作请参见**购买证书**。
     - 证书已签发且已超过规定时间（DigiCert品牌和GeoTrust品牌：证书签发后的25天内），如果发现证书信息填写错误或变更，则需要重新购买证书。

3.4.4 申请 SSL 证书过程中遇到的问题，该如何解决?

申请证书时，可能遇到以下问题，请根据自己的实际情况进行处理：

申请证书时，公司联系人可以填写自己吗?

可以。

联系人仅做联系用，并非人工审核联系人。

DNS 验证时，添加的解析记录能否删除?

DNS配置记录用于验证域名，解析记录须在证书域名验证完成后才能删除。删除后对证书的审核和使用没有影响。

在华为云云解析服务上进行域名解析操作，添加记录集中的值时，是否需要引号?

提交SSL证书申请后需要进行域名授权验证。

当您是在华为云的云解析服务上进行域名解析操作，添加记录集的值时，需要填写该域名对应的主机记录值。输入时，必须用双引号（英文状态下）引用该记录值。

示例：

"201807040000001v0p73k28ruec3am17s0wl6z7angvqlesyipf65k7347knjm7h"

更多详细操作请参见**步骤三：在华为云云解析服务上进行DNS验证**。

申请证书时，如何选择“证书请求文件”？

证书请求文件（Certificate Signing Request，CSR）即证书签名申请，获取SSL证书，需要先生成CSR文件并提交给CA中心。CSR包含了公钥和标识名称（Distinguished Name），通常从Web服务器生成CSR，同时创建加解密的公钥私钥对。

SSL证书管理中，申请证书时，“证书请求文件”可选择“系统生成CSR”或“自己生成CSR”。

- 系统生成CSR：系统将自动帮您生成证书私钥，并且您可以在证书申请成功后直接在证书管理页面下载您的证书和私钥。
- 自己生成CSR：手动生成CSR文件。详细操作请参见**如何制作CSR文件?** 。

说明

建议您选择“系统生成CSR”，避免出现内容不正确而导致的审核失败。两种证书文件的区别请参见**系统生成的CSR和自己生成CSR的区别?** 。

申请证书时，“企业营业执照”需要上传哪个企业的营业执照?

申请证书时，用户可根据自己的实际情况选择是否上传“企业营业执照”。

如需上传“企业营业执照”，上传时，需要上传使用该证书的企业的营业执照，即系统的使用单位的营业执照，而不是系统的开发单位的营业执照。

如果不上传，可能会延长证书的签发周期，具体延长时间取决于CA机构验证时间。

4 测试证书相关

4.1 CCM 是否提供免费的 SSL 证书?

CCM中，DigiCert品牌提供有证书类型为DV（Basic）、域名类型为单域名的免费测试证书。

测试证书申请操作请参见**申请测试证书**。

接Digicert厂商通知，**2023年11月15日**起 Digicert DV(Basic) 单域名证书（即测试证书）有效期将从**12个月**缩短至**3个月**。

- 对于2023年11月15日前，在华为云创建和签发的免费测试证书（规格为Digicert DV(Basic)单域名），证书有效期仍为12个月。
- 对于2023年11月15日后，在华为云创建和签发的免费测试证书（规格为Digicert DV(Basic)单域名），证书有效期将改为3个月。
- 对于在华为云上通过付费购买Digicert DV(Basic)扩容包签发的测试证书，有效期仍为12个月，不受此变动影响。

测试（免费）证书使用须知

- 测试证书一个账号最多可以申请20张。同时，为了减少证书资源的浪费，CCM只支持单次申请一张测试证书。

  须知

  - 20张的测试证书额度包括：已删除或已吊销证书，即测试证书申请后进行吊销或删除的操作其额度不会恢复。
  - 同一个账号不区分主账号和子账号。例如，主账号已使用了20张的额度，则主账号和子账号均无测试证书额度。
  - 如果您华为云账号下的20张测试SSL证书额度已用完，还需继续使用测试证书，可以购买Digicert DV(basic) 单域名扩容包，对测试证书额度进行扩容。详细操作请参见**测试证书额度已用完，该如何处理?**

- 一张测试证书仅支持绑定一个单域名。
- 测试证书不支持保护IP和泛域名（通配符域名）。

- 测试证书的信任等级和安全性都较低，所以建议只用于测试。
- 由于DigiCert品牌的DV（Basic）免费证书是无偿提供给个人用户用于测试或个人业务，因此**不支持**任何免费的人工技术支持或安装指导。
- 测试证书签发后，不支持续费和续期，到期之后，将无法继续使用。如需继续使用SSL证书，请在控制台重新创建。

4.2 测试（免费）证书与收费证书的区别

所有SSL证书都具备SSL加密传输功能，都可通过https访问网站，在浏览器上显示安全锁标志。

本章节将介绍免费证书和收费证书的区别。

表 4-1 测试证书和收费证书的区别

区别项	测试证书	收费证书
安全等级	一般	高
证书运行环境的兼容性	一般	高
CA中心对证书的安全保险赔付	不支持	支持
证书数量限制	每个账号（不区分主账号和子账号）仅限20张	不限制
支持保护的网站域名类型	仅支持保护一个单域名	支持保护单域名、多域名、泛域名
支持的证书类型	仅DV	DV、OV、EV
人工客服支持	不支持	支持
OCSP（Online Certificate Status Protocol，在线证书状态协议）	无本地OCSP，可能会有网络延时或超时情况	除DV (Basic)，其他付费证书均支持OCSP加速访问

测试证书一般仅用于个人网站或测试使用，不建议业务成熟的企业类型网站使用。

如果您是企业类型网站，建议您购买收费证书。对于政府、金融、电子商务、医疗等组织或机构，推荐使用OV型证书或安全等级最高的EV型证书，不仅让您的用户更信赖您的网站，同时对您的网站数据和身份认证安全提供更强的保障。关于收费证书选型的更多建议，请参见**如何选择SSL证书？**。

4.3 如何申请测试证书?

华为云云证书管理服务中，**DigiCert品牌**提供有证书类型为**DV（Basic）**、域名类型为**单域名**、有效期为**3个月**的测试证书。

前提条件

购买证书的IAM用户已被授予“SCM Administrator”/“SCM FullAccess”、“BSS Administrator”和“DNS Administrator”权限。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- DNS Administrator：云解析服务（DNS）的所有执行权限。

具体操作请参见**权限管理**。

约束条件

- 测试证书一个账号最多可以申请20张。同时，为了减少证书资源的浪费，CCM只支持单次申请一张测试证书。

  须知

  - 20张的测试证书额度包括：已删除或已吊销证书，即测试证书申请后进行吊销或删除的操作其额度不会恢复。
  - 同一个账号不区分主账号和子账号。例如，主账号已使用了20张的额度，则主账号和子账号均无测试证书额度。
  - 如果您华为云账号下的20张测试SSL证书额度已用完，还需继续使用测试证书，可以购买Digicert DV(basic) 单域名扩容包，对测试证书额度进行扩容。详细操作请参见**测试证书额度已用完，该如何处理?**

- 一张测试证书仅支持绑定一个单域名。
- 测试证书不支持保护IP和泛域名（通配符域名）。
- 测试证书的域名验证默认使用DNS验证。
- 测试证书的信任等级和安全性都较低，所以建议只用于测试。
- 由于DigiCert品牌的DV（Basic）免费证书是无偿提供给个人用户用于测试或个人业务，因此**不支持**任何免费的人工技术支持或安装指导。
- 测试证书签发后，不支持续费和续期，到期之后，将无法继续使用。如需继续使用SSL证书，请在控制台重新创建。

步骤一：创建免费证书（方式一）

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

步骤3 在证书列表选择“测试证书”页签，单击“创建测试证书”，进入创建测试证书对话框界面。

“创建测试证书”按钮处显示的数字表示测试证书剩余可创建数量和可累计创建总数量。例如数字显示为“13/20”，表示剩余可创建13张测试证书，可累计创建20张测试证书。

步骤4 阅读并勾选“我已阅读并同意《云证书管理服务（CCM）免责声明》”，单击“确认”。

步骤5 您在SSL证书列表的“测试证书”页签中可查看到创建成功的免费测试证书。

说明

测试证书下发可能存在延迟，如果证书列表中未看到创建的测试证书，建议您刷新当前页面。

----结束

步骤一：创建免费证书（方式二）

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

步骤3 在界面右上角，单击“购买证书”，进入购买证书页面。

步骤4 在购买证书页面，配置购买参数。

- “域名类型：”选择“单域名”。
- “证书类型”：选择“DV（Basic）”。
- “证书品牌”：选择“DigiCert”。
- “证书类型”和“证书品牌”选择后，“域名数量”、“有效期”、“购买量”将自动生成，无需配置。

图 4-1 免费证书购买信息

步骤5 确认参数配置无误后，在页面右下角，单击“立即购买”。

步骤6 确认订单无误后，阅读并勾选“我已阅读并同意《云证书管理服务（CCM）免责声明》”，单击“去支付”。

步骤7 在购买页面，请选择付款方式进行付款。

成功付款后，在SSL证书列表的“测试证书”页签中可查看到创建成功的免费测试证书。

----结束

步骤二：提交证书申请

成功创建免费的测试证书后，您需要为证书绑定域名、填写证书申请人的详细信息并提交审核。

1. 在SSL证书列表中选择“测试证书”页签，在您已创建的测试证书所在行的“操作”列，单击“申请证书”。
2. 在“申请证书”页面，填写域名信息和联系人信息。
   a. 填写域名信息，参数配置如表4-2所示。

图 4-2 配置域名信息

表 4-2 域名信息参数说明

参数名称	参数说明	取值样例
证书请求文件	证书请求文件（Certificate Signing Request，CSR）即证书签名申请，获取SSL证书，需要先生成CSR文件并提交给CA中心。CSR包含了公钥和标识名称（Distinguished Name），通常从Web服务器生成CSR，同时创建加解密的公钥私钥对。 选择证书请求文件生成方式： • 系统生成CSR：系统将自动帮您生成证书私钥，并且您可以在证书申请成功后直接在证书管理页面下载您的证书和私钥。 • 自己生成CSR：手动生成CSR文件并将文件内容复制到CSR文件内容对话框中。详细操作请参见**如何制作CSR文件？**。	系统生成CSR

参数名称	参数说明	取值样例
绑定域名	输入证书需要绑定的单域名。 填写示例：您的域名为www.domain.com，则在“绑定域名”中填写www.domain.com 如果需要绑定中文域名，请单击访问**Punycode官网**使用**Punycode编码**工具将中文域名编码，再填写编码后信息。 示例：**华为云.com** Punycode 编码后：**xn--siq1ht8k.com**，则在“绑定域名”中填写xn--siq1ht8k.com	www.domain.com

b. 单击“下一步”，进入“授权信息”页面。
c. 填写公司联系人信息，参数配置如**表4-3**所示。

图 4-3 配置授权信息

表 4-3 授权信息参数说明

参数名称	参数说明	取值样例
公司联系人/授权人信息	仅需要填写联系人的姓名、电话、邮箱。 为了使证书能够快速的签发，此处填写的电话、邮箱必须真实有效。	--
技术联系人信息（选填）	可选项。可以不填。	--

3. 确认填写的信息无误后，阅读《云证书管理服务（CCM）免责声明》、《隐私政策声明》和信息授权声明，并勾选声明内容前面的框。
4. 单击“提交申请”。

   系统会将您的申请提交到CA认证机构，请您**保持电话畅通**，并**及时查阅**邮箱中来自CA认证机构的电子**邮件**。

步骤三：DNS 验证

DNS验证，是指在域名管理平台通过解析指定的DNS记录，验证域名所有权，即您需要到该域名的管理平台为该域名添加一条DNS记录。例如：如果您购买的是A公司的域名，您需要到A公司的域名管理平台添加DNS记录文件。有关DNS验证方式详细操作请参见**域名DNS解析**。

- 如果您是在华为云上申请的域名，且域名已使用华为云云解析服务，则无需进行任何操作，系统将自动添加DNS记录验证。
- 如果您是在其他域名管理平台（如万网、新网、DNSPod等）管理您的域名，则需要前往域名的DNS解析服务商进行操作。

  详细操作请参见**DNS验证**。

须知

- 在您提交证书申请后，需要按照证书列表页面的提示完成DNS验证，否则证书将一直处于“待完成域名验证”状态，且您的证书将无法通过审核。
- DNS验证通过后，您需要耐心等待CA机构审核。

步骤四：签发证书

DNS验证通过之后，CA机构将还需要一段时间进行处理，请您耐心等待。CA机构审核通过后，将会签发证书。

证书签发后便立即生效，即可部署证书到华为云其他云产品或下载证书并部署到服务器上进行使用。

须知

CA机构针对已提交申请的证书的审核检测频率为：

- 提交申请后0-1h：15分钟轮询一次，如果配置没有问题，一般情况，10-20分钟签发证书。
- 提交申请后1-4h：30分钟轮询一次。
- 提交申请后4h-24h：1小时轮询一次。
- 提交申请后1-7天：4小时轮询一次。
- 提交申请后7天以上认定为订单超时，自动取消。此时，请参照**为什么“证书状态”长时间停留在审核中？**排查并解决问题。

4.4 如何查询免费测试证书剩余额度?

免费的SSL证书一个账号最多可以申请20张。同时，为了减少证书资源的浪费，SCM只支持单次申请一张免费证书。

须知

- 20张的测试证书额度包括：已删除或已吊销证书，即测试证书申请后进行吊销或删除的操作其额度不会恢复。
- 同一个账号不区分主账号和子账号。例如，主账号已使用了20张的额度，则主账号和子账号均无测试证书额度。
- 如果您华为云账号下的20张测试SSL证书额度已用完，还需继续使用测试证书，可以购买Digicert DV(basic) 单域名扩容包，对测试证书额度进行扩容。详细操作请参见**测试证书额度已用完，该如何处理?**

关于免费测试证书额度使用情况，您可以通过以下方式查询：

步骤1 登录**云证书管理服务控制台**。

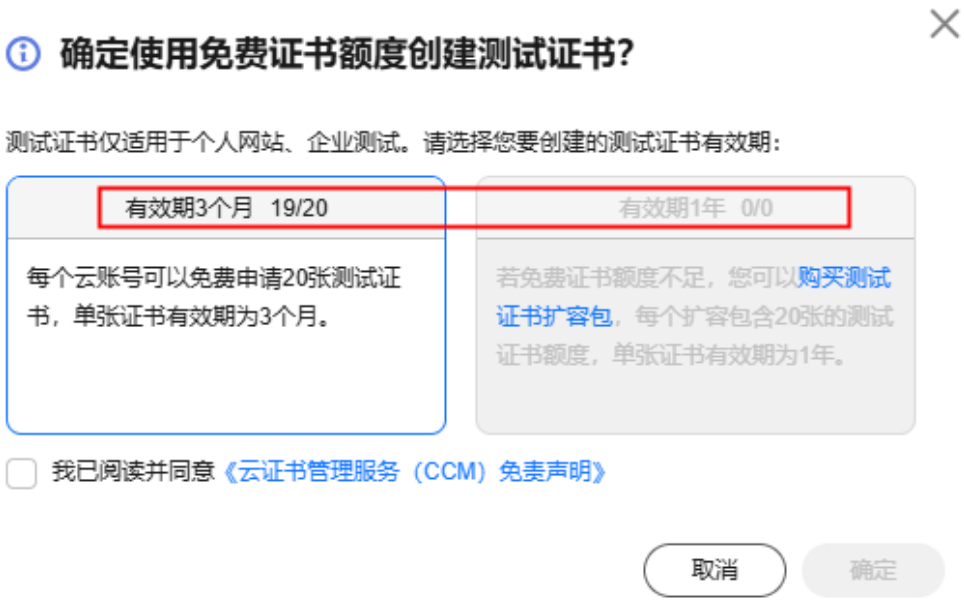
步骤2 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

步骤3 单击“测试证书”页签，进入测试证书列表页面。

步骤4 单击列表上方的“创建测试证书”，在弹出的对话框中，可以查看测试证书剩余额度，如**图 免费SSL证书额度**所示。

如果20张测试证书额度已使用完，可以单击“购买扩容包”，购买成功后，将增加20张测试证书使用额度。

图 4-4 免费 SSL 证书额度



----结束

4.5 测试证书额度已用完，该如何处理?

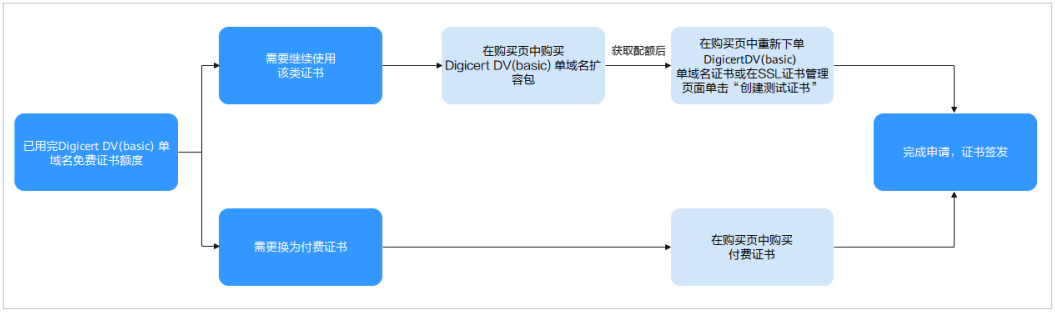
当您申请测试证书时遇到以下情况，请参照本章节进行处理。

- 您通过单击CCM控制台“创建测试证书”按钮创建Digicert DV(Basic)单域名证书（免费证书）时，出现“创建测试证书”按钮置灰不能使用的情况。
- 您通过CCM控制台购买页面购买Digicert DV(Basic)单域名证书（免费证书）时，出现界面提示“当前用户证书数量已经达到最大值，不能继续添加”的情况。

测试证书额度说明

如果您华为云账号下的20张测试证书额度已用完，具体情况如图4-5所示。请根据您实际情况进行处理：

图 4-5 证书额度说明



- 还需继续使用测试证书，可以购买Digicert DV(basic) 单域名扩容包，增加Digicert DV(basic) 单域名证书的使用额度。

本章节将介绍此情况下的操作步骤。

- 需要更换为付费证书，在购买页面选购付费证书即可。

购买和使用单域名扩容包的约束与限制

- Digicert DV(basic) 单域名扩容包属于增值服务类产品，需支付一定的费用，该费用是针对已领取过华为云提供的20张免费证书额度的用户，收取的扩容服务费用。
- 发票将按照购买Digicert DV(basic) 单域名扩容包时的实付金额开具等额发票，之后使用Digicert DV(basic) 单域名扩容包额度申请的免费证书不再开具发票。
- Digicert DV(basic) 单域名扩容包一经购买，则不支持退款、退货、换货。
- Digicert DV(basic) 单域名扩容包每个扩容包中包含20张测试证书额度，单张证书有效期为12个月。扩容包无使用期限限制，待包内测试证书额度全部用完后，请按需购买。

操作步骤

该操作步骤为需**继续使用测试证书**的操作方法，如需购买付费证书，详细操作请参见**购买SSL证书**。

步骤1 购买单域名扩展包。

1. 登录**云证书管理服务控制台**。
2. 在左侧导航栏选择“SSL证书管理”，并在SSL证书管理界面右上角，单击“购买证书”，进入购买证书页面。
3. 在购买证书页面，配置购买参数。
   - “证书类型”：选择“DV（Basic）”。
   - “证书品牌”：选择“DigiCert”。
   - “域名类型”：选择“单域名扩展包”。

   “证书类型”、“证书品牌”和“域名类型”选择后，“证书数量”、“有效期”、“购买量”将自动生成，无需配置。

图 4-6 扩容包购买信息

4. 确认参数配置无误后，在页面右下角，单击“立即购买”。
5. 确认订单无误后，阅读并勾选“我已阅读并同意《云证书管理服务（CCM）免责声明》”，单击“去支付”。
6. 在购买页面，请选择付款方式进行付款。

步骤2 申请测试证书。

详细操作请参见**如何申请测试证书？**。

----结束

5 验证域名所有权

5.1 如何进行域名验证?

按照CA中心的规范，如果您申请了SSL数字证书，您必须配合完成域名验证来证明您对所申请绑定的域名的所有权。

当您按照要求正确配置域名验证信息，待域名授权验证完成，CA系统中心审核通过后，才会签发证书。

华为云SSL证书管理提供的域名验证方式具体说明如**表5-1**所示，请根据您申请证书时选择的验证方式进行操作。

表 5-1 域名验证

参数名称	参数说明
自动DNS验证	DNS验证指在域名管理平台通过解析指定的DNS记录，验证域名所有权。 自动DNS验证则系统自动添加DNS记录验证，无需您进行任何操作。以下条件必须**全部满足**系统才会进行自动DNS验证： • 购买的是DV（域名型）证书 • 绑定域名是在华为云上申请的域名，且已使用华为云云解析服务
手动DNS验证	DNS验证指在域名管理平台通过解析指定的DNS记录，验证域名所有权。 手动DNS验证则您需要前往域名的DNS解析服务商进行操作。具体操作请参见**如何进行手动DNS验证?** 。
邮箱验证	指通过回复邮件的方式来验证域名所有权。具体操作请参见**如何进行邮箱验证?** 。
文件验证	指通过在服务器上创建指定文件的方式来验证域名所有权。具体操作请参见**如何进行文件验证?** 。

参数名称	参数说明

须知
• DV（域名型）证书默认通过“DNS验证”方式进行验证。
  • 如果您是在华为云上申请的域名，且域名已使用华为云云解析服务，则系统将进行**自动DNS验证**，您无需进行任何操作。
  • 如果您是在其他域名管理平台（如万网、新网、DNSPod等）管理您的域名，则需要进行**手动DNS验证**。	

5.2 如何进行手动 DNS 验证?

DNS验证，是指在域名管理平台通过解析指定的DNS记录，来验证域名所有权的一种方式。SSL证书管理中支持自动DNS验证和手动DNS验证两种DNS验证方式。

本章节将介绍如何在华为云平台进行手动DNS验证。

手动DNS验证是指您需要前往域名的DNS解析服务商进行操作。

图 5-1 手动 DNS 验证场景图

约束与限制

手动DNS验证的域名解析只能在您的域名管理平台上进行操作，具体的解析方法以域名服务商提供的解析方法为准。

步骤一：确认验证步骤

DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析。请根据域名管理平台类型执行验证步骤：

域名管理平台类型	验证步骤
域名管理平台是华为云	继续执行后续所有步骤。
域名管理平台不是华为云	请确认是否愿意把域名从其他服务商迁移到华为云DNS? • 是。请执行以下操作步骤: 1. 请把域名从其他服务商迁移到华为云DNS。 2. 继续执行后续所有步骤。 • 否。请在相应的平台上进行DNS验证。例如，域名托管在阿里云，则需要到阿里云的云解析DNS控制台进行相关配置。

步骤二：获取验证信息

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理”，并在SSL证书页面中待进行域名验证的证书所在行的“操作”列，单击“域名验证”，系统从右面弹出域名验证详细页面。

步骤3 在证书的域名验证页面，查看并记录“主机记录”、“记录类型”和“记录值”，如**图5-2**所示。

如果界面未显示，则请登录邮箱（申请证书时填写的邮箱）进行查看。

图 5-2 查看主机记录

----结束

步骤三：在华为云云解析服务上进行 DNS 验证

步骤1 登录**云证书管理服务控制台**。

步骤2 选择“网络 > 云解析服务”，并在云解析页面左侧导航栏，选择“公网域名”，进入“公网域名”页面。

步骤3 在“公网域名”页面的域名列表中，单击待添加记录集的域名，并在解析记录页面右上角单击“添加记录集”，进入“添加记录集”页面。

须知

- 不同域名类型的证书做DNS验证时，需要添加记录集的域名如下：
  - 单域名证书，为证书绑定的域名添加记录集（域名带www时例外，域名带www时为其上一级域名添加记录集。例如证书绑定的域名为www.example.com，为域名example.com添加记录集）。
  - 多域名证书，需要为证书绑定的所有域名添加记录集。
  - 泛域名证书，为泛域名相应的上一级域名添加记录集。

    例如：证书绑定的域名为*.example.com，只需为域名example.com添加记录集。
- 如果在“解析记录”的域名列表中，已存在带解析域名且相同记录类型的记录值，直接在目标域名的“操作”列，单击“修改”，进入“修改记录集”页面。

图 5-3 添加记录集

表 5-2 添加记录集参数说明

参数名称	参数说明
主机记录	证书的“域名验证”页面，域名服务商返回的“主机记录”。
类型	证书的“域名验证”页面，域名服务商返回的“记录类型”。
别名	选择“否”。
线路类型	选择“全网默认”。
TTL (秒)	一般建议设置为5分钟。TTL值越大，则DNS记录的同步和更新越慢。
值	证书的“域名验证”页面，域名服务商返回的“记录值”。 **说明** 记录值必须用英文引号引用后粘贴在文本框中。
其他的设置保持不变。	

步骤4 单击“确定”，记录集添加成功。

当记录集的状态显示为“正常”时，表示记录集添加成功。

须知

该记录集在证书签发后才可以删除。

----结束

步骤四：查看域名验证是否生效

步骤1 在Windows系统中，单击“开始”，输入“cmd”，进入命令提示符对话框。

步骤2 根据不同的记录类型，选择执行**表 验证命令**所示命令，查看DNS验证配置是否已经生效。

表 5-3 验证命令

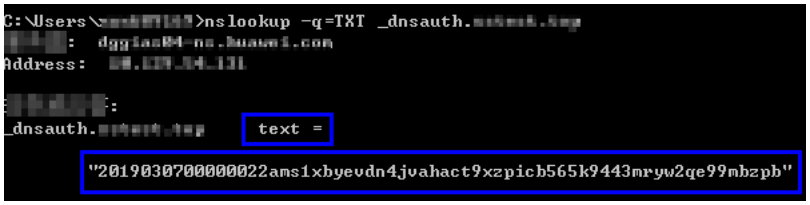
记录类型	验证命令
TXT	**nslookup -q=TXT** *xxx*
CNAME	**nslookup -q=CNAME** *xxx*

说明

*xxx*代表域名服务商返回的“主机记录”值。

- 如果界面回显的记录值（text的值）与域名服务商返回的“记录值”一致，如**图 5-4**所示，说明域名授权验证配置已经生效。

图 5-4 域名授权验证配置生效



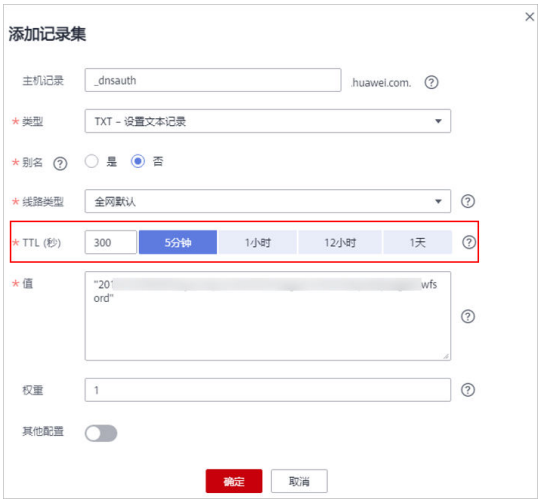
- 如果界面未回显记录值，显示为“Non-existent domain”，说明域名授权验证配置未生效。

图 5-5 域名授权验证配置未生效

步骤3 如果DNS验证配置未生效，请根据以下可能原因进行排除修改，直至验证生效。

表 5-4 排查处理

可能原因	处理方法
域名管理平台选择错误	DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析，请确认您进行DNS验证的平台是否为您的域名托管平台。
旧解析记录未删除	证书签发后添加的解析记录即可删除。 如您上一次申请证书时添加的解析记录未删除，本次申请证书添加的解析记录将不会生效，请您确认是否未删除上一次解析记录。
记录配置出错	请您检查“主机记录”、“类型”或“记录值”是否填写正确。 **图 5-6** 配置记录 

可能原因	处理方法
配置的生效时间过长，生效时间还未到，因此无法查询到数据。	请您检查生效时间（TTL）是否设置过长，建议将生效时间修改为5分钟。不同的域名提供商的DNS配置不一样，如华为云的DNS（云解析服务）默认是5分钟后生效，如下图所示。 如配置的生效时间未到，请等时间到了后再进行验证。 **图 5-7** 生效时间 

----结束

步骤五：DNS 验证结果审核

- **OV、EV证书**

  按CA机构审核邮件要求完成验证后，请耐心等待，CA机构需要2-3个工作日对DNS验证信息进行审核，审核通过后，才会签发证书。

  如遇验证失败或其他问题，请根据CA机构审核邮件中提供的联系方式，与CA机构联系。

- **DV证书**

  您可以在域名验证页面，手动验证结果。

  a. 登录**云证书管理服务控制台**。

  b. 在左侧导航栏选择“SSL证书管理”，并SSL证书页面中待域名验证的证书所在行的“操作”列，单击“域名验证”，系统从右面弹出域名验证详细页面。

  c. 单击“验证”，验证DNS解析配置。

  - 界面提示“验证成功，证书签发审核中，请等待”：证书将在1分钟内签发，请您及时刷新页面查看证书状态。
  - 验证失败，请参照**DV证书DNS验证失败如何处理?** 排查并修改问题后，等待3-5分钟重新验证。

DV 证书 DNS 验证失败如何处理?

失败提示信息	解决方案
提交验证频繁，请稍后再试	验证过于频繁，建议您等待3-5分钟后，执行验证操作。
DNS记录值不匹配	您配置的DNS记录值不正确，请参照**步骤二：获取验证信息**获取正确记录值后，重新配置。
DNS验证失败，请稍后再试。	请排查是否存在以下问题： • 可能问题一：DNS记录值配置未生效。 解决方案：DNS记录值配置完后不会立即生效（具体生效时间为您域名服务器中设置的TTL缓存时间），建议您等待3-5分钟后，执行验证操作。 • 可能问题二：DNS记录值正确配置，且一段时间后验证依然失败。 解决方案：CA验证服务器位于国外，部分时间可能存在网络问题，导致验证DNS失败，请等待1-2小时，或尝试重新发起申请。 • 可能问题三：域名未完成备案或实名认证。 解决方案：请完成域名备案和实名认证后，进行域名所有权验证。 • 可能问题四：域名存在CAA类型的解析记录。 解决方案：CAA记录会导致验证失败，您需要在域名解析记录中删除所有CAA类型的记录。 • 可能问题五：CA验证服务器没有检测到DNS解析记录。 解决方案：CA验证服务器位于国外，需要您放开该域名国外的访问限制。

5.3 如何进行文件验证?

文件验证指通过在服务器上创建指定文件的方式来验证域名所有权。

在您成功申请证书后，需要按照订单进度提示完成域名授权验证配置，否则证书将一直处于“待完成域名验证”状态，且您的证书将无法通过审核。

文件验证方式一般需要由您的服务器管理人员进行操作。本章节将介绍如何进行文件验证。

须知

该验证文件在证书颁发或吊销后方可删除。

前提条件

服务器开放了80或443端口。

说明

目前CA机构仅支持向80或443端口发起认证请求。

约束与限制

- 仅DV单域名证书支持文件验证。

步骤一：获取验证信息

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理”，并SSL证书页面中待域名验证的证书所在行的“操作”列，单击“域名验证”，系统从右面弹出域名验证详细页面。

步骤3 在域名验证页面中，查看此处的“记录值”。

如果界面未显示，则请按照页面中的提示，登录邮箱（申请证书时填写的邮箱）查看“记录值”。

图 5-8 文件验证

----结束

步骤二：创建指定文件

步骤1 登录您的服务器，并且确保域名已指向该服务器并且对应的网站已正常启用。

步骤2 在网站根目录下，创建指定的文件。该文件包括文件目录、文件名、文件内容。

说明

网站根目录是指您在服务器上存放网站程序的文件夹，大致有这几种表示名称：wwwroot、htdocs、public_html、webroot等。请您根据实际情况进行操作。

如下以服务器操作系统为“Windows”，网站根目录为“/www/htdocs”,为例进行说明：

1. 在Windows系统中，单击“开始”，输入“cmd”，进入命令提示符对话框。
2. 执行以下命令，进入网站根目录所在磁盘，此处以网站根目录所在磁盘为D盘为例。

   d:
3. 执行以下命令，在网站根目录下，创建“.well-known/pki-validation”子目录。

   此处则在“/www/htdocs”目录下进行创建，请您根据实际情况进行操作。

   ```
   cd /www/htdocs
   mkdir .well-known
   cd .well-known
   mkdir pki-validation
   cd pki-validation
   ```
4. 执行以下命令，在“.well-known/pki-validation”子目录下，创建一个名称为“fileauth.txt”的文件。

   echo off>fileauth.txt
5. 执行以下命令，打开“fileauth.txt”文件。

   start fileauth.txt
6. 将**步骤一：获取验证信息**中的记录值放在“fileauth.txt”文件内，在左上角选择“文件>保存”。

----结束

步骤三：查看验证配置是否生效

步骤1 打开浏览器，访问URL地址“https://yourdomain/.well-known/pki-validation/fileauth.txt”或“http://yourdomain/.well-known/pki-validation/fileauth.txt”。

请将URL地址中的yourdomain替换成您申请证书时绑定的域名。

- 如果您的域名是普通域名，则请参照以下方法进行操作：

  例如，如果您的域名为example.com，则访问的URL地址为：https://example.com/.well-known/pki-validation/fileauth.txt或http://example.com/.well-known/pki-validation/fileauth.txt
- 如果您的域名为泛域名，则请参照以下方法进行操作：

  例如，如果您的域名为*.domain.com，则访问的URL地址为：https://domain.com/.well-known/pki-validation/fileauth.txt或http://domain.com/.well-known/pki-validation/fileauth.txt

步骤2 确认验证URL地址在浏览器中是否可正常访问，且页面中显示的内容和订单进度页面中的记录值是否内容一致。

- 如果界面回显的记录值与SSL证书管理控制台的域名验证页面中显示记录值中显示的记录值一致，则说明域名授权验证已生效。
- 如果界面回显信息不一致，则说明域名授权验证未生效。

步骤3 如果配置未生效，请从以下几方面进行排查和处理：

- 检查该验证URL地址是否在HTTPS可访问的地址中存在。如果存在，请在浏览器中使用HTTPS重新访问，如果浏览器提示“证书不可信”或者显示的内容不正确，请您暂时关闭该域名的HTTPS服务。

- 确保该验证URL地址在任何一个地方都能正确访问。由于有些品牌的检测服务器均在国外，请确认您的站点是否有国外镜像，或者是否使用了智能DNS服务。
- 检查该验证URL地址是否存在301或302跳转。如存在此类重定向跳转，请取消相关设置关闭跳转。

  您可使用**wget -S** *URL地址*命令检测该验证URL地址是否存在跳转。

----结束

5.4 如何进行邮箱验证?

邮箱验证指通过回复邮件的方式来验证域名所有权。

在您提交证书申请后，需要按照订单进度提示完成域名授权验证配置，否则证书将一直处于“待完成域名验证”状态，且您的证书将无法通过审核。

操作步骤

步骤1 登录您申请域名的域名管理员邮箱。

步骤2 打开来自CA机构的域名确认邮件。

步骤3 单击邮件中的认证按钮，完成域名验证。

验证完成后，CA机构可能还需要一段时间审核域名信息。在此期间，证书状态为“待完成域名验证”。

如您已完成域名验证操作，由于CA机构需要2-3个工作日对您提交的信息进行验证，请您耐心等待。CA机构审核通过后，证书审核才可以进入“待完成组织验证”状态。

----结束

5.5 如何查看域名验证是否生效?

如果您已经完成了域名授权验证配置，可查看域名验证是否生效。本章节将介绍如何查看域名验证是否生效。

操作指引如下：

- 如果您的域名验证方式是“DNS验证”，请参见**DNS验证方式的检查**。
- 如果您的域名验证方式是“文件验证”，请参见**文件验证方式的检查**。

前提条件

- 已完成域名授权验证配置，具体操作请参见**域名验证**。
- 已完成域名备案。如果未进行域名备案将导致域名验证失败，请先完成域名备案。

DNS 验证方式的检查

步骤1 获取主机记录和记录值。

1. 登录**云证书管理服务控制台**。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

3. 在待完成域名验证的证书所在行的“操作”列，单击“域名验证”，系统从右面弹出域名验证详细页面。
4. 在证书的域名验证页面，查看并记录“主机记录”、“记录类型”和“记录值”，如图5-9所示。

   如果界面未显示，则请登录邮箱（申请证书时填写的邮箱）进行查看。

图 5-9 查看主机记录

步骤2 根据不同的记录类型、操作系统，选择以下方式验证DNS配置是否生效。

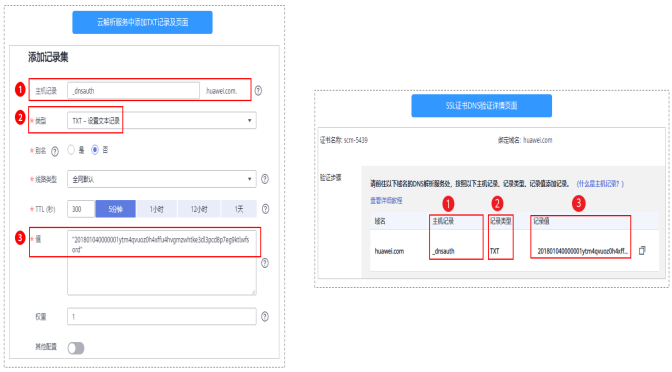
本文档以主机记录值为“_dnsauth.domain.com”为例。

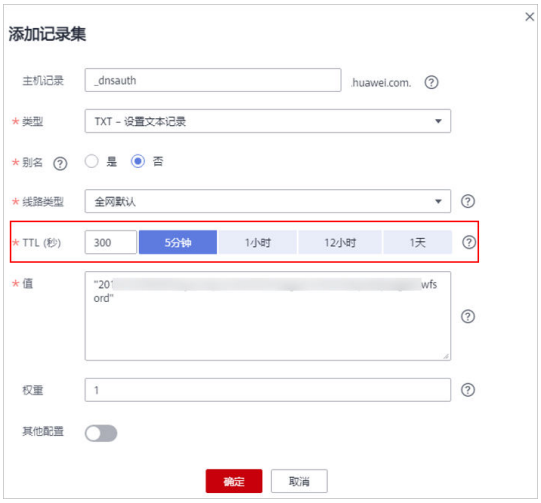
- 记录类型为“TXT”
  - Windows系统：
    i. 在Windows系统中，单击“开始”，输入“cmd”，进入命令提示符对话框。
    ii. 输入命令 **nslookup -q=TXT _dnsauth.domain.com** 。
  - Linux系统：
    i. 在桌面单击鼠标右键，选择“terminal”，进入命令提示符对话框。
    ii. 输入命令 **dig TXT _dnsauth.domain.com** 。
  - MACOS系统：
    i. 选择“前往>实用工具”,，单击“终端”，进入命令提示符对话框。
    ii. 输入命令 **dig TXT _dnsauth.domain.com** 。
- 记录类型为“CNAME”
  - Windows系统：
    i. 在Windows系统中，单击“开始”，输入“cmd”，进入命令提示符对话框。
    ii. 输入命令 **nslookup -q=CNAME _dnsauth.domain.com** 。
  - Linux系统：
    i. 在桌面单击鼠标右键，选择“terminal”，进入命令提示符对话框。
    ii. 输入命令 **dig CNAME _dnsauth.domain.com** 。
  - MACOS系统：
    i. 选择“前往>实用工具”,，单击“终端”，进入命令提示符对话框。
    ii. 输入命令 **dig CNAME _dnsauth.domain.com** 。

如果界面回显的记录值（text的值）与域名服务商返回的“记录值”一致，说明域名授权验证配置已经生效。

步骤3 如果DNS验证配置未生效，请根据以下可能原因进行排除修改，直至验证生效。

表 5-5 排查处理

可能原因	处理方法
域名管理平台选择错误	DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析，请确认您进行DNS验证的平台是否为您的域名托管平台。
旧解析记录未删除	证书签发后添加的解析记录即可删除。 如您上一次申请证书时添加的解析记录未删除，本次申请证书添加的解析记录将不会生效，请您确认是否未删除上一次解析记录。
记录配置出错	请您检查“主机记录”、“类型”或“记录值”是否填写正确。 **图 5-10** 配置记录 

可能原因	处理方法
配置的生效时间过长，生效时间还未到，因此无法查询到数据。	请您检查生效时间（TTL）是否设置过长，建议将生效时间修改为5分钟。不同的域名提供商的DNS配置不一样，如华为云的DNS（云解析服务）默认是5分钟后生效，如下图所示。 如配置的生效时间未到，请等时间到了后再进行验证。 **图 5-11** 生效时间 

----结束

文件验证方式的检查

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理”，并SSL证书页面中待域名验证的证书所在行的“操作”列，单击“域名验证”，系统从右面弹出域名验证详细页面。

步骤3 在域名验证页面中，查看此处的“记录值”。

如果界面未显示，则请按照页面中的提示，登录邮箱（申请证书时填写的邮箱）查看“记录值”。

图 5-12 文件验证

步骤4 打开浏览器，访问URL地址“https://yourdomain/.well-known/pki-validation/fileauth.txt”或“http://yourdomain/.well-known/pki-validation/fileauth.txt”。

请将URL地址中的yourdomain替换成您申请证书时绑定的域名。

- 如果您的域名是普通域名，则请参照以下方法进行操作：

  例如，如果您的域名为example.com，则访问的URL地址为：https://example.com/.well-known/pki-validation/fileauth.txt或http://example.com/.well-known/pki-validation/fileauth.txt

- 如果您的域名为泛域名，则请参照以下方法进行操作：

  例如，如果您的域名为*.domain.com，则访问的URL地址为：https://domain.com/.well-known/pki-validation/fileauth.txt或http://domain.com/.well-known/pki-validation/fileauth.txt

步骤5 确认验证URL地址在浏览器中是否可正常访问，且页面中显示的内容和订单进度页面中的记录值是否内容一致。

- 如果界面回显的记录值与SSL证书管理控制台的域名验证页面中显示记录值中显示的记录值一致，则说明域名授权验证已生效。
- 如果界面回显信息不一致，则说明域名授权验证未生效。

步骤6 如果配置未生效，请从以下几方面进行排查和处理：

- 检查该验证URL地址是否在HTTPS可访问的地址中存在。如果存在，请在浏览器中使用HTTPS重新访问，如果浏览器提示“证书不可信”或者显示的内容不正确，请您暂时关闭该域名的HTTPS服务。
- 确保该验证URL地址在任何一个地方都能正确访问。由于有些品牌的检测服务器均在国外，请确认您的站点是否有国外镜像，或者是否使用了智能DNS服务。
- 检查该验证URL地址是否存在301或302跳转。如存在此类重定向跳转，请取消相关设置关闭跳转。

您可使用**wget -S** *URL地址*命令检测该验证URL地址是否存在跳转。

----结束

5.6 Windows 系统如何验证 DNS 解析生效?

如果您使用的是Windows操作系统，可参考本章节验证DNS验证是否生效。

提交证书申请后，您可以参考域名验证页面的提示完成域名DNS验证。

步骤1 在Windows系统中，单击“开始”，输入“cmd”，进入命令提示符对话框。

步骤2 根据不同的记录类型，选择执行**表 验证命令**所示命令，查看DNS验证配置是否已经生效。

表 5-6 验证命令

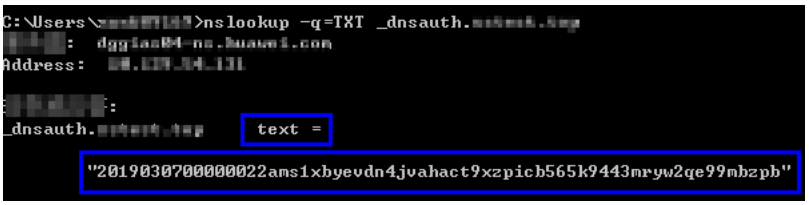
记录类型	验证命令
TXT	**nslookup -q=TXT** *xxx*
CNAME	**nslookup -q=CNAME** *xxx*

说明

*xxx*代表域名服务商返回的“主机记录”值。

- 如果界面回显的记录值（text的值）与域名服务商返回的“记录值”一致，如**图 5-13**所示，说明域名授权验证配置已经生效。

图 5-13 域名授权验证配置生效



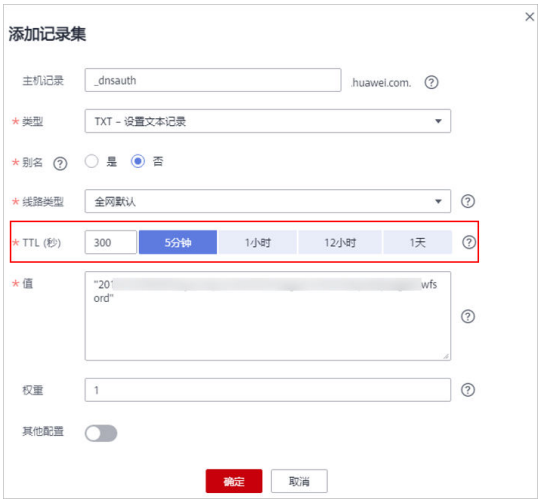
- 如果界面未回显记录值，显示为“Non-existent domain”，说明域名授权验证配置未生效。

图 5-14 域名授权验证配置未生效

步骤3 如果DNS验证配置未生效，请根据以下可能原因进行排除修改，直至验证生效。

表 5-7 排查处理

可能原因	处理方法
域名管理平台选择错误	DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析，请确认您进行DNS验证的平台是否为您的域名托管平台。
旧解析记录未删除	证书签发后添加的解析记录即可删除。 如您上一次申请证书时添加的解析记录未删除，本次申请证书添加的解析记录将不会生效，请您确认是否未删除上一次解析记录。
记录配置出错	请您检查“主机记录”、“类型”或“记录值”是否填写正确。 **图 5-15** 配置记录 

可能原因	处理方法
配置的生效时间过长，生效时间还未到，因此无法查询到数据。	请您检查生效时间（TTL）是否设置过长，建议将生效时间修改为5分钟。不同的域名提供商的DNS配置不一样，如华为云的DNS（云解析服务）默认是5分钟后生效，如下图所示。 如配置的生效时间未到，请等时间到了后再进行验证。 **图 5-16** 生效时间 

----结束

5.7 域名验证未生效如何处理?

如果您已经完成了域名授权验证配置，且域名验证未生效，请参照本章节进行处理。

操作指引如下：

- 如果您的域名验证方式是“DNS验证”，且配置未生效，请参见**DNS验证后，配置未生效**进行操作。
- 如果您的域名验证方式是“文件验证”，且配置未生效，请参见**文件验证后，配置未生效**进行操作。

前提条件

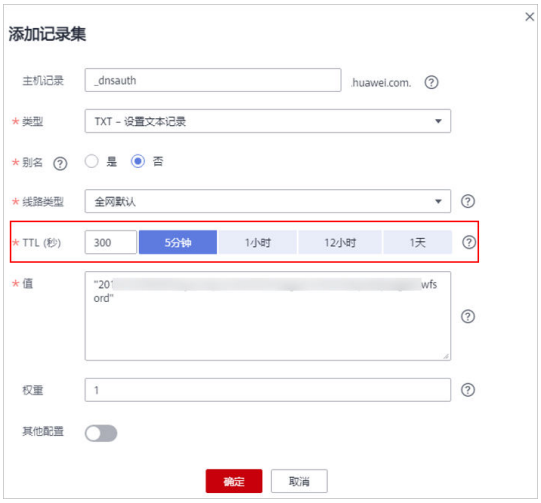
- 已完成域名备案。如果未进行域名备案将导致域名验证失败，请先完成域名备案。
- 已完成域名授权验证配置，具体操作请参见**域名验证**。
- 已查看域名验证是否生效，具体作请参见**如何查看域名验证是否生效?** 。

DNS 验证后，配置未生效

域名授权验证配置未生效可能有以下原因，请根据实际情况进行处理：

表 5-8 排查处理

可能原因	处理方法
域名管理平台选择错误	DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析，请确认您进行DNS验证的平台是否为您的域名托管平台。
旧解析记录未删除	证书签发后添加的解析记录即可删除。 如您上一次申请证书时添加的解析记录未删除，本次申请证书添加的解析记录将不会生效，请您确认是否未删除上一次解析记录。
记录配置出错	请您检查“主机记录”、“类型”或“记录值”是否填写正确。 **图 5-17** 配置记录 

可能原因	处理方法
配置的生效时间过长，生效时间还未到，因此无法查询到数据。	请您检查生效时间（TTL）是否设置过长，建议将生效时间修改为5分钟。不同的域名提供商的DNS配置不一样，如华为云的DNS（云解析服务）默认是5分钟后生效，如下图所示。 如配置的生效时间未到，请等时间到了后再进行验证。 **图 5-18** 生效时间 

文件验证后，配置未生效

域名授权验证配置未生效，请从以下几方面进行排查：

- 如果界面回显的记录值与SSL证书管理控制台的域名验证页面或邮件中显示的记录值一致，则说明域名授权验证已生效。
- 如果界面回显信息不一致，则说明域名授权验证未生效。

  如果配置未生效，请从以下几方面进行排查和处理：
  - 检查该验证URL地址是否在HTTPS可访问的地址中存在。如果存在，请在浏览器中使用HTTPS重新访问，如果浏览器提示“证书不可信”或者显示的内容不正确，请您暂时关闭该域名的HTTPS服务。
  - 确保该验证URL地址在任何一个地方都能正确访问。由于有些品牌的检测服务器均在国外，请确认您的站点是否有国外镜像，或者是否使用了智能DNS服务。
  - 检查该验证URL地址是否存在301或302跳转。如存在此类重定向跳转，请取消相关设置关闭跳转。

    您可使用**wget -S** *URL地址*命令检测该验证URL地址是否存在跳转。

5.8 如何查询域名提供商?

用户可以通过查询域名注册信息，确认域名所属的DNS服务器信息，然后再根据域名所属的DNS服务器信息进行DNS验证的相关操作。

操作步骤

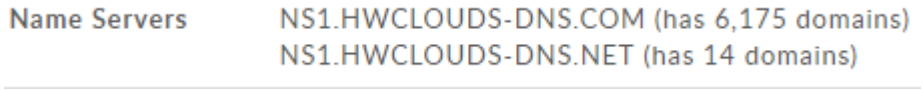
步骤1 打开浏览器，访问“https://whois.domaintools.com/”网站。

步骤2 输入需要查询的域名，单击“Search”，进入域名注册信息详情页面。

步骤3 在注册信息中，查看“Name Servers”，确认域名所属的DNS服务器。

当“Name Servers”显示如所图5-19示时，则表示域名所属的“DNS服务器”为华为云DNS。

图 5-19 Name Servers



请根据域名所属的DNS服务器进行DNS验证，执行以下操作：

- 域名所属的“DNS服务器”为华为云DNS：请参见**如何进行DNS验证?**，在华为云的云解析服务上进行DNS验证。
- 域名所属的“DNS服务器”不是华为云DNS：请确认是否愿意把域名从其他服务商迁移到华为云DNS?
  - 是：请执行以下操作步骤：
    i. 请把域名从其他服务商迁移到华为云DNS。
    ii. 参见**如何进行手动DNS验证?**，在华为云的云解析服务上进行DNS验证。
  - 否：请在相应的平台上进行DNS验证。例如，域名托管在阿里云，则需要到阿里云的云解析DNS控制台进行相关配置。

----结束

5.9 如何查询域名管理员邮箱并进行验证?

本章节介绍如何在证书审核过程中，查询域名管理员邮箱并根据邮件提示进行验证。

操作步骤

步骤1 打开浏览器，访问“http://whois.domaintools.com/”网站，输入需要查询的域名。

步骤2 在查询结果中，查看域名管理员邮箱。

步骤3 如果邮箱无误，用户申请证书后，CA机构将会给该邮箱发送验证邮件，收到邮件后单击邮件中的确认链接即可完成验证。

----结束

5.10 域名不在华为云平台管理，如何进行 DNS 验证?

域名不在华为云平台管理，在进行DNS验证时，请确认是否愿意把域名从其他服务商迁移到华为云DNS?

- 是：请执行以下操作步骤：
  a. 请把域名从其他服务商迁移到华为云DNS。
  b. 参见**如何进行手动DNS验证？**，在华为云的云解析服务上进行DNS验证。
- 否：请在相应的平台上进行DNS验证。例如，域名托管在阿里云，则需要到阿里云的云解析DNS控制台进行相关配置。

5.11 域名验证完成后，为什么 SSL 证书还是停留在“待完成域名验证（申请进度为 40%）”的状态?

申请证书时，如果已完成域名验证，但证书状态还是停留在“待完成域名验证”，请参照以下步骤进行处理：

1. 证书申请中填写的域名是否已做实名认证。
   - 如果域名已做实名认证，请执行**2**。
   - 如果域名未做实名认证，请前往您的域名服务商处完成域名实名认证。
2. 确认是否已完成域名验证。
   - 如果已完成，请执行**3**。
   - 如果未完成，请按照提示进行操作。
     域名验证详细操作请参见**域名验证**。
3. 查看域名验证是否生效。
   具体验证方法请参见**如何查看域名验证是否生效？**。
   - 如果已生效，请执行**4**。
   - 如果未生效，请按照**域名验证未生效如何处理？**进行处理。

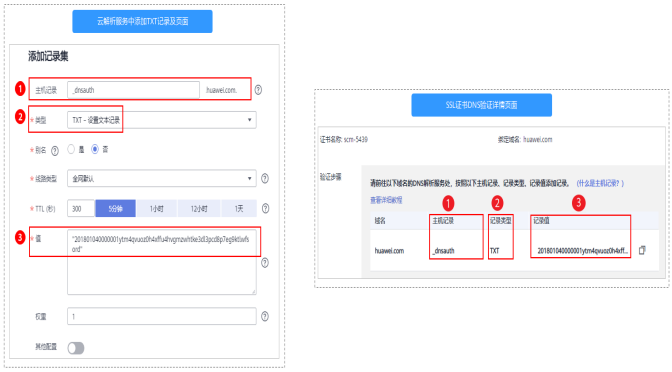
   本章节将详细介绍DNS验证的排查方法，具体操作请参见**DNS验证后，配置未生效**。
4. 请您耐心等待。
   验证完成后，CA机构可能还需要一段时间审核域名信息。在此期间，证书状态为“待完成域名验证”。
   如果您已完成域名验证操作，由于CA机构需要2-3个工作日对您提交的信息进行验证，请您耐心等待。CA机构审核通过后，才会签发证书。

DNS 验证后，配置未生效

域名授权验证配置未生效可能有以下原因，请根据实际情况进行处理：

表 5-9 排查处理

可能原因	处理方法
域名管理平台选择错误	DNS验证只能在域名管理平台（即您的域名托管平台）上进行解析，请确认您进行DNS验证的平台是否为您的域名托管平台。

可能原因	处理方法
旧解析记录未删除	证书签发后添加的解析记录即可删除。 如您上一次申请证书时添加的解析记录未删除，本次申请证书添加的解析记录将不会生效，请您确认是否未删除上一次解析记录。
记录配置出错	请您检查“主机记录”、“类型”或“记录值”是否填写正确。 **图 5-20** 配置记录 
配置的生效时间过长，生效时间还未到，因此无法查询到数据。	请您检查生效时间（TTL）是否设置过长，建议将生效时间修改为5分钟。不同的域名提供商的DNS配置不一样，如华为云的DNS（云解析服务）默认是5分钟后生效，如下图所示。 如配置的生效时间未到，请等时间到了后再进行验证。 **图 5-21** 生效时间 

5.12 当 SSL 证书状态为“待完成域名验证”时，如何修改域名验证方式?

当SSL证书状态为“待完成域名验证”，则需要根据申请证书时选择的“域名验证方式”进行域名验证。

此时，如果需要修改域名验证方式，可先撤回证书申请，并修改域名验证方式后，再提交申请。

须知

- DV基础版证书（GeoTrust入门级SSL证书和DigiCert免费SSL证书）仅支持通过“DNS验证”方式进行验证，暂不支持修改域名验证方式。

步骤1 撤回证书申请。

1. 登录**云证书管理服务控制台**。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。
3. 在目标证书所在行的“操作”列，单击“撤回申请”，如**图5-22**所示。

图 5-22 撤回申请

4. 在弹出的“取消申请流程”对话框中，单击“确定”，页面右上角弹出“取消申请流程成功”，则说明取消证书的申请流程提交成功。

   此时，证书的状态为“CA审核中（撤回申请）”，待服务审核撤销证书申请流程通过后，撤销成功，证书的状态切换为“待申请”。

步骤2 提交证书申请。

将撤回成功，状态处于为“待申请”的证书重新提交申请。提交申请时，修改域名验证方式。

更多详细操作请参见**提交SSL证书申请**。

步骤3 根据证书流程进行处理。

根据页面提示完成申请证书操作。

----结束

5.13 DV 证书 DNS 验证失败该如何处理?

DV证书通过云证书管理控制台“验证”功能校验**DNS解析**结果时，验证失败，请参照下表提示进行排查处理后重新验证：

失败提示信息	解决方案
提交验证频繁，请稍后再试	验证过于频繁，建议您等待3-5分钟后，执行验证操作。
DNS记录值不匹配	您配置的DNS记录值不正确，请参照**步骤二：获取验证信息**获取正确记录值后，重新配置。
DNS验证失败，请稍后再试。	请排查是否存在以下问题： ● 可能问题一：DNS记录值配置未生效。 解决方案：DNS记录值配置完后不会立即生效（具体生效时间为您域名服务器中设置的TTL缓存时间），建议您等待3-5分钟后，执行验证操作。 ● 可能问题二：DNS记录值正确配置，且一段时间后验证依然失败。 解决方案：CA验证服务器位于国外，部分时间可能存在网络问题，导致验证DNS失败，请等待1-2小时，或尝试重新发起申请。 ● 可能问题三：域名未完成备案或实名认证。 解决方案：请完成域名备案和实名认证后，进行域名所有权验证。 ● 可能问题四：域名存在CAA类型的解析记录。 解决方案：CAA记录会导致验证失败，您需要在域名解析记录中删除所有CAA类型的记录。 ● 可能问题五：CA验证服务器没有检测到DNS解析记录。 解决方案：CA验证服务器位于国外，需要您放开该域名国外的访问限制。

6 SSL 证书审核

6.1 SSL 证书审核需要多久时间?

证书审核时间取决于您和CA机构之间的配合。请留意您在申请证书时预留的邮箱和电话。CA机构将通过您预留的邮箱和电话与您进行联系。

不同的证书类型审核周期有所区别，按照证书申请流程，CA机构（证书的签发方）需要对提交的信息进行确认，通过后才会签发证书。证书签发后立即生效。

一般情况下，各证书类型的审核周期说明如表6-1所示。

表 6-1 证书审核周期

证书类型	审核周期
增强型（EV）、增强型企业版（EV Pro）	CA机构人工审核信息，在信息正确的情况下审核周期一般为7～10个**工作日**。
企业型（OV）、企业型专业版（OV Pro）	CA机构人工审核信息，在信息正确的情况下审核周期一般为3～5个**工作日**。
基础版（DV）	CA机构签发系统自动检查域名授权配置，无人工审核，DNS配置正确的情况下可在数小时内快速颁发。 免费证书包含在此类型证书中。证书申请过程中，CA机构签发系统自动检查域名授权配置，无人工审核，DNS配置正确的情况下可在数小时内快速颁发。

如果资料信息完备，并且与CA机构配合积极，审核时间将大大缩减。签发证书的审核流程依赖于您的配合，为了快速签发证书，希望您做到以下两点：

- 提交信息准确，避免因为信息不正确反复修改。
- 及时接听来自CA机构的电话或确认来自CA机构的邮件等。

须知

13个月内再次购买DigiCert、GeoTrust品牌的OV证书且资料信息无更改，将免组织验证即人工审核。

相关操作

- **域名验证完成后，为什么SSL证书还是停留在“待完成域名验证（申请进度为40%）”的状态?**
- **如何查看域名验证是否生效?**
- **域名验证未生效如何处理?**
- **为什么“证书状态”长时间停留在审核中?**

6.2 为什么“证书状态”长时间停留在审核中?

在您成功补全证书信息后，CA机构（证书的签发机构）将审核您的域名和提交的证书信息。为了确保您的证书能够尽快签发，请您仔细阅读以下说明。

说明

不同品牌的证书，实际的签发时间可能有所不同，具体审核时间请参见**SSL证书审核需要多久时间?** 。

操作步骤

步骤1 证书申请中填写的域名是否已做实名认证。

- 如果域名已做实名认证，请执行**步骤2**。
- 如果域名未做实名认证，请前往您的域名服务商处完成域名实名认证。

步骤2 确认您已正确填写和提交证书申请订单。

- 如果填写确认无误，请执行**步骤3**。
- 如果填写的信息有误，您可以取消申请。取消成功后，再提交证书申请。修改后，再执行**步骤3**。

  撤回申请详细操作请参见**撤回证书申请**。

  提交证书申请详细操作请参见**提交SSL证书申请**。

步骤3 确认您已按照SSL证书管理控制台该证书的“状态/申请进度”提示，完成“域名验证”、“组织验证”。

- 如果已完成，请执行**4**。
- 如果未完成，请按照提示进行操作。

  域名验证详细操作请参见**域名验证**，域名验证完成后，请查看验证是否生效。

  组织验证详细操作请参见**组织验证**。组织验证仅OV、OV Pro、EV、EV Pro类型证书需要。

步骤4 查看域名验证是否生效。

具体验证方法请参见**如何查看域名验证是否生效?** 。

- 如果已生效，请执行**步骤5**。
- 如果未生效，请按照**域名验证未生效如何处理？**进行处理。

步骤5 检查是否CAA（Certification Authority Authorization，证书颁发机构授权限制）限制了CA证书颁发。

- 是，您可以取消限制或者参考**设置CAA记录防止错误颁发HTTPS证书**添加一条CAA解析记录。
- 否，请执行**步骤6**。

步骤6 请您耐心等待。

申请证书后，CA机构将对您提交的信息进行审核。请您耐心等待。

审核期间，CA机构会通过电话联系您并指导您进行相关操作，请您务必保持手机畅通。如果CA机构无法及时联系到您，该订单的审核进度可能会延迟。

- OV、EV类型证书审核时长

  如果您购买的是OV或EV类型证书，请您需要耐心等待3~7个**工作日**。CA中心会在3~7个工作日内完成您的证书订单审核。

  如果审核期间有任何问题，CA中心的客服人员会通过电话联系您并指导您进行相关操作，请务必确保您的联系电话在审核期间保持畅通。如果CA中心无法及时联系到您，那么该订单的审核进度将可能会延迟。您的及时回复将能有效缩短SSL证书的验证时间。
- DV类型或免费证书审核时长

  域名授权验证完成后，CA中心将会在1~2个工作日内签发您的证书。

  如果您的域名中包含某些敏感词（例如bank、pay、live等），可能会触发人工审核机制，审核时间会比较长，请您耐心等待。

须知

免费证书申请后会在1~2个工作日内签发。根据CA中心审核流程耗时不同，您的证书有可能会在几个小时内就完成签发，也有可能需要2个工作日才能完成签发，请您耐心等待。

----结束

6.3 SSL 证书提交申请后需要做什么？

SSL证书购买后，需要申请证书并提交审核，审核通过后才能使用该证书。

当证书订单提交审核后，您可以在SSL证书管理控制台的证书管理列表中，在该证书的“状态/申请进度”中查看您接下来需要做什么。以下为几个重要操作的示例：

- 待完成域名验证：已提交申请证书的请求，需要按照CA机构的要求完成域名授权验证，具体操作请参见**域名验证**。此时，证书申请进度为40%。
- 待完成组织验证：如果您申请的是OV或EV类型的证书，域名验证完成后，CA机构将还会确认组织是否发起了此次的证书订单申请。具体操作请参见**组织验证**。此时，证书申请进度为70%。
- 即将签发：已完成域名验证、组织验证等操作，等待CA机构审核中，请您耐心等待。此时，证书申请进度为90%。

待所有信息验证通过后，证书“状态”更新为“已签发”。

OV、OVPro 型或 EV、EV Pro 型证书

如果您购买的是OV、OVPro或EV、EV Pro类型证书，成功购买证书后，您需要按照SSL证书管理控制台该证书的“状态/申请进度”提示，完成“申请证书”、“域名验证”、“组织验证”。

以上操作完成后，您只需要耐心等待，CA机构（证书的签发方）可能还需要一段时间审核。CA机构审核通过后，您的数字证书将会签发。

如果审核期间有任何问题，CA中心的客服人员会通过电话联系您并指导您进行相关操作，请务必确保您的联系电话在审核期间保持畅通。

DV（Basic）型证书

如果您购买的是DV（Basic）证书，您需要按照SSL证书管理控制台该证书的“状态/申请进度”提示，完成“申请证书”、“域名验证”。

当域名验证完成后，您的SSL证书将会在1-2个工作日内签发。

如果您的域名中包含某些敏感词（例如bank、pay、live等），可能会触发人工审核机制，审核时间会比较长，请您耐心等待。

6.4 收到 CA 机构的邮件或电话如何处理?

SSL证书申请过程中，如果收到证书相关的邮件或电话，请在确认是CA机构的邮件或电话后，尽快根据邮件或电话内容进行相应处理，以免影响证书审核进度。

以下几种情况CA机构可能会给您发送邮件或打电话：

- 验证域名所有权
  - 原因：证书申请过程中，按照CA中心的规范，您必须配合完成域名授权验证来证明您对所申请绑定的域名的所有权。
  - 处理方法：请根据邮件内容进行验证域名所有权操作。详细操作可参见**域名验证**。
- 组织验证
  - 原因：申请OV和EV类型证书时，CA机构将联系组织的公开电话，确认组织是否发起了此次的证书订单申请。
  - 处理方法：CA机构将通过组织的公开电话与您联系，请您留意并及时进行处理。

6.5 新购买的 SSL 证书是否需要重新审核?

需要。

不论之前是否申请过证书，购买证书后，均需要审核。证书的申请流程是一样的，都是需要申请并通过CA机构审核的。

新证书签发后即可替换，替换过程不会影响业务。

6.6 域名未通过安全审核该怎么办?

问题描述

如果您申请DV证书的订单审核结果失败，您可能收到以下失败结果描述：

该域名未通过CA安全审核，无法申请DV证书，请尝试使用其他域名，或选择购买OV、EV类型的证书。

问题原因

一般这种情况的审核失败，可能是由于您的域名中包含某些敏感词。

目前已知的可能无法通过DV数字证书审核的域名敏感词包括：

- live（不包含 .live顶级域名）
- bank
- banc
- ban.c
- alpha
- example
- credit
- pw（包含 .pw顶级域名）
- apple
- ebay
- trust
- root
- amazon
- android
- visa
- google
- discover
- financial
- wordpress
- pal
- hp
- lv
- free
- SCP
- edu
- .edu.cn
- gov

- onion

解决方法

根据CA中心给出的建议，在这种情况下您可以选择：

- 购买OV或EV类型的数字证书来绑定您的域名。
- 使用该DV证书绑定您的其它不包含上述敏感词的域名。

6.7 如何解决“审核失败 - 主域名不能为空”的问题?

问题描述

如果您在申请数字证书时选择自己上传CSR文件，可能收到“审核失败 – 主域名不能为空”的返回结果。

问题原因

在创建CSR文件时，未正确填写Common Name字段。

解决方法

重新制作并上传CSR文件，确保正确填写Common Name字段。

须知

Common Name字段必须是证书绑定的主域名。

为保证CSR文件内容正确，强烈建议您使用系统提供的系统生成CSR文件功能。同时，使用系统自动生成CSR文件功能，在数字证书颁发后还可支持不同格式的证书下载。

7 SSL 证书下载/安装与应用

7.1 SSL 证书下载类

7.1.1 已签发的 SSL 证书可以多次下载并使用吗?

- 证书在有效期内，可多次下载并使用，下载后即可在服务器（华为云的或非华为云的均可）上进行部署。
- 重新下载并安装部署后，对已部署的服务器没有影响，且在浏览器上通过域名进行访问时，对浏览器也没有影响。

须知

待安装证书的服务器上需要运行的域名，必须与证书的域名一一对应，即购买的是哪个域名的证书，则用于哪个域名。否则安装部署后，浏览器将提示不安全。

7.1.2 如何获取 SSL 证书私钥文件 server.key?

根据申请证书时，选择的“证书请求文件”方式（系统生成CSR和自己生成CSR）的不同，获取方式不一样。

- 系统生成CSR

  系统生成CSR的情况，重新下载证书文件即可。下载证书详细操作请参见**下载证书**。
- 自己生成CSR

  自己生成CSR的情况，server.key是用户自行保存，无法下载或从SSL证书管理服务获取。

7.1.3 SSL 证书下载失败如何处理?

问题描述

在SSL证书管理服务中申请了证书，且证书已签发，下载证书时，无法下载。

问题原因

- 可能原因一：账号欠费或权限不足
- 可能原因二：浏览器缓存较多

解决方法

请根据可能原因选择操作步骤：

- **原因一：账号欠费或权限不足**

  解决方法：如果欠费，请您进行充值；如果您的权限不足，请联系您的管理员开通权限。

- **原因二：浏览器缓存较多**

  解决方法：请清除浏览器缓存或者更换浏览器重试。

  如果仍未解决，请您提工单联系我们，并在工单中进行描述（例如：非上传的已签发的证书无法下载，华为云账号未欠费且有下载的操作权限）。

7.1.4 SSL 证书下载后文件为空如何处理?

问题描述

在SSL证书管理服务中下载了证书，且证书已下载成功，本地打开证书下载压缩文件时，文件为空无内容。

问题原因

部分 Windows 系统的默认压缩软件存在兼容性问题，无法正常解压下载的证书文件，导致文件内容为空。

解决方法

更换解压缩工具：使用其他解压缩软件对文件进行解压操作，验证是否能正常提取证书文件内容。

7.2 SSL 证书安装类

7.2.1 SSL 证书支持在哪些服务器上部署?

SSL证书对部署的服务器没有任何限制，无论是华为云或其他云厂商的服务器，还是线下云服务器。

获取证书文件后，您可根据自己的需求将SSL证书部署到网站对应的服务器上，或将证书应用到WAF、ELB、CDN等云产品中。具体的部署操作请参考以下文档：

- **如何在服务器上安装SSL证书?**
- **如何将SSL证书应用到华为云产品?**

7.2.2 如何在服务器上安装 SSL 证书?

如何在服务器上安装 SSL 证书

SSL证书签发后，即可下载并安装Web服务器，在Tomcat、Nginx、Apache、IIS等服务器上安装证书，您可以参考表7-1。

表 7-1 安装 SSL 证书操作示例

服务器类型	操作示例
Tomcat	在Tomcat服务器上安装SSL证书
Nginx	在Nginx服务器上安装SSL证书
Apache	在Apache服务器上安装SSL证书
IIS	在IIS服务器上安装SSL证书
Weblogic	在Weblogic服务器上安装SSL证书
Resin	在Resin服务器上安装SSL证书

说明

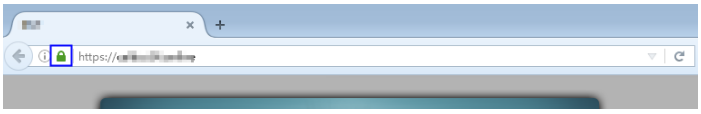
由于服务器系统版本或服务器环境配置不同，在安装SSL证书过程中使用的命令或修改的配置文件信息可能会略有不同，云证书管理服务提供的安装证书示例，仅供参考，请以您的实际情况为准。

效果验证

验证证书安装是否正确。

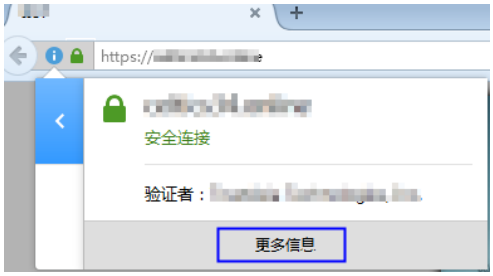
1. 在浏览器的地址中输入“https://域名”，按“Enter”。
2. 单击，查看证书，如图7-1所示。

图 7-1 查看证书



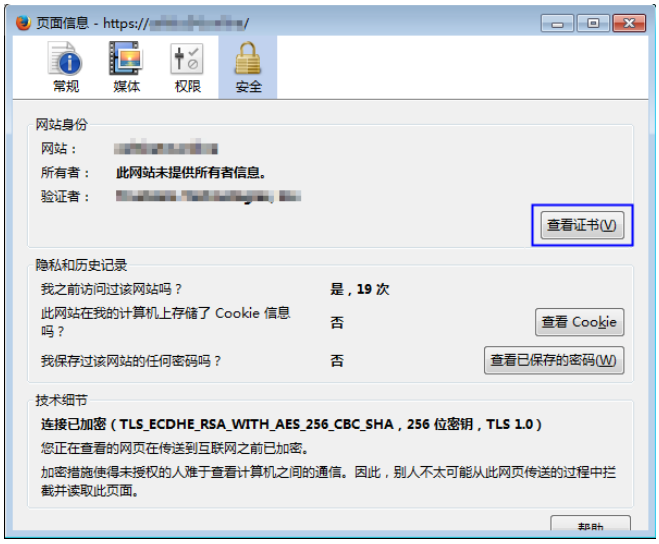
3. 单击“更多信息”，如图7-2所示。

图 7-2 更多信息



4. 在弹出的“页面信息”窗口中，单击“安全 > 查看证书”，如图7-3所示。

图 7-3 查看证书信息



5. 在弹出的“证书查看器”中，单击“常规”和“详细信息”，通过查看证书常规信息和详细信息，确认证书是否安装成功。

图 7-4 证书信息

如果证书信息确认无误，则表示证书安装正确。

7.2.3 如何验证部署的 SSL 证书是否生效?

SSL数字证书必须由浏览器中受信任的根证书颁发机构在验证服务器身份后颁发，具有网站身份验证和加密传输双重功能。

配置完成SSL数字证书后，如果您能使用浏览器通过“https://”方式访问您的网站，则表示SSL证书已正常工作。

操作步骤

在浏览器地址栏中，输入“https://您的数字证书绑定的域名”（如https://www.huaweicloud.com），通过HTTPS方式访问您的网站。

如果网站页面能正常访问，且浏览器地址栏中显示安全锁标志，说明您的SSL数字证书已在正常工作，如图7-5所示。

图 7-5 数字证书正常工作

7.2.4 服务器 IP 地址变更后，原 SSL 证书是否仍可用?

可以的。

SSL证书都是绑定域名的，和服务器更换IP地址没有任何关系。

只要域名不变，重新解析到新的IP地址即可，原来的SSL证书照样可以用，不需要更换新的证书。

7.2.5 SSL 证书支持在哪些地域部署?

SSL证书对地理位置没有任何限制，可以部署在国内的服务器上，也可以部署在海外的服务器上。

获取证书文件后，您可根据自己的需求将SSL证书部署到网站对应的服务器上，或将证书应用到WAF、ELB、CDN等云产品中。具体的部署操作请参考以下文档：

- **如何在服务器上安装SSL证书?**
- **如何将SSL证书应用到华为云产品?**

7.2.6 宝塔搭建的网站如何在后台添加 SSL 证书?

安装证书前，需要获取证书文件和密码文件，请根据申请证书时选择的“证书请求文件”生成方式来选择操作步骤：

- 如果申请证书时，“证书请求文件”选择“系统生成CSR”，具体操作请参见：**系统生成CSR**。
- 如果申请证书时，“证书请求文件”选择“自己生成CSR”，具体操作请参见：**自己生成CSR**。

系统生成 CSR

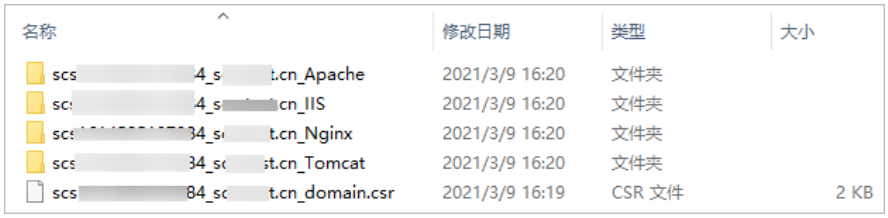
宝塔面板一般包含Apache环境和Nginx环境。

- **Nginx环境配置SSL证书的方法**

  a. 在本地解压已下载的证书文件。

  下载的文件包含了“Apache”、“IIS”、“Nginx”、“Tomcat”4个文件夹和1个“domain.csr”文件，如**图7-6**所示。

  图 7-6 本地解压 SSL 证书

  b. 从“*证书ID_证书绑定的域名*_Nginx”文件夹内获得证书文件“*证书ID_证书绑定的域名*_server.crt”和私钥文件“*证书ID_证书绑定的域名*_server.key”。

  - “*证书ID_证书绑定的域名*_server.crt”文件包括两段证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，分别为服务器证书和中级CA。
  - “*证书ID_证书绑定的域名*_server.key”文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

  c. 打开宝塔网站的“SSL”界面。

  - 将“*证书ID_证书绑定的域名*_server.key”的内容复制粘贴到“密钥(KEY)”的配置框中。

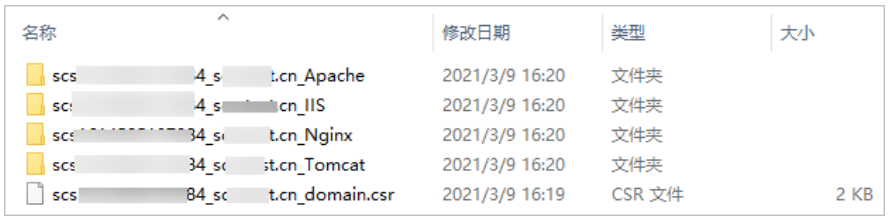
- 将“*证书ID_证书绑定的域名*_server.crt”的内容复制粘贴到“证书(PEM格式)”的配置框中。

- **Apache环境配置SSL证书的方法**

  a. 在本地解压已下载的证书文件。

  下载的文件包含了“Apache”、“IIS”、“Nginx”、“Tomcat”4个文件夹和1个“domain.csr”文件，如图7-6所示。

  图 7-7 本地解压 SSL 证书

  b. 从“*证书ID_证书绑定的域名*_Apache”文件夹内获得证书文件“*证书ID_证书绑定的域名*_ca.crt”，“*证书ID_证书绑定的域名*_server.crt”和私钥文件“*证书ID_证书绑定的域名*_server.key”。

  - “*证书ID_证书绑定的域名*_ca.crt”文件包括一段中级CA证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
  - “*证书ID_证书绑定的域名*_server.crt”文件包括一段服务器证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
  - “*证书ID_证书绑定的域名*_server.key”文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

  c. 打开宝塔网站的“SSL”界面。

  - 将“*证书ID_证书绑定的域名*_server.key”的内容复制粘贴到“密钥(KEY)”的配置框中。
  - “*证书ID_证书绑定的域名*_server.crt”文件和“*证书ID_证书绑定的域名*_ca.crt”文件合并后录入到“证书(PEM格式)”的配置框中。

  须知

  - “server.crt”文件和“ca.crt”文件合并时，一定是“server.crt”内容在前，“ca.crt”内容在后，顺序不正确会导致Apache无法正常启动。
  - 如果您的证书不是通过SCM签发的，下载的crt文件对应的名称是“_public.crt”和“_chain.crt”，与SCM签发的证书文件的对应关系是：
    - “_public.crt”文件对应“server.crt”文件。
    - “_chain.crt”文件对应“ca.crt”文件。

    合并时，“_public.crt”文件内容在前，“_chain.crt”文件内容在后。

自己生成 CSR

此时，不区分Apache环境和Nginx环境，均按以下步骤进行操作。

1. 解压已下载的证书压缩包，获得“*证书ID_证书绑定的域名*_server.pem”文件。

   “*证书ID_证书绑定的域名*_server.pem”文件包括两段证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，分别为服务器证书和中级CA证书。

2. 打开宝塔网站的“SSL”界面。
   - 将生成CSR时的私钥“server.key”的内容复制粘贴到“密钥(KEY)”的配置框中。
   - 将“*证书ID_证书绑定的域名*_server.pem”的内容复制粘贴到“证书(PEM格式)”的配置框中。

7.2.7 SSL 证书安装配置或使用中的相关问题，该如何解决?

一个服务器上可以配置多张 SSL 证书吗?

可以。一个服务器上可以同时配置多个证书。

一张 SSL 证书是否可以部署到多台服务器?

证书是与域名绑定的，对服务器的数量没有限制。如果您购买的证书绑定的域名用于多台服务器，则购买的证书需要在每台服务器上进行部署才能生效。

SSL 证书必须安装在华为云的服务器上吗?

不是。

华为云的或非华为云的均可。

证书在有效期内，可多次下载并使用，下载后即可在服务器（华为云的或非华为云的均可）上进行部署。

SSL 证书是否可以用在中国香港的云虚拟主机或者网站上?

可以用。

证书使用不受地理位置的限制。

已签发或已上传的 SSL 证书，为什么在 WAF、ELB、CDN 等云产品的配置中，找不到新的证书呢?

SSL证书签发后或成功上传后，可以在华为云的其他云产品中使用，如WAF、ELB、CDN等。

目前，SSL证书管理支持将证书一键部署到WAF、ELB、CDN。其他产品则需要下载证书后，再在对应的云产品控制台上传数字证书并进行部署。

将证书应用到WAF、ELB、CDN中：

SSL证书管理支持将证书一键部署到WAF、ELB、CDN中。部署成功后，可以帮助您提升云产品访问数据的安全性。

详细操作请参见**部署证书**。

已购买 SSL 证书和 WAF 服务，怎样将证书的密钥导出到 WAF 中使用呢?

在配置WAF时需要使用SSL证书中密钥，具体操作请参见**WAF证书配置**。

配置过程中如有问题，请参考相应服务文档进行处理或咨询对应服务。

7.3 SSL 证书应用类

7.3.1 非华为云 SSL 证书如何配置到华为云服务中?

非华为云证书是指在非华为云处申请的、并由CA机构签发的SSL证书，例如，在其他云服务提供商或线下证书供应商处申请的、并由CA机构签发的SSL证书。

SSL证书是由CA机构签发的，不论什么平台申请的都是一样的。

任何平台申请的或者任何品牌的SSL证书，只要是CA机构签发的均可在华为云中进行使用。但是，无法一键部署到WAF、ELB、CDN等云产品。因此，建议您使用在华为云平台申请的SSL证书，以便一键部署证书到对应云服务。部署后，可以帮助您提升云产品访问数据的安全性。

如需将非华为云SSL证书配置到华为云服务中，请根据需要选择具体操作：

表 7-2 场景说明

场景	操作方法
将证书放在华为云的SSL证书管理中统一管理	上传到SSL证书管理中，详细操作请参见**上传证书**。
将证书配置到WAF、ELB、CDN中	SSL证书管理支持将证书一键部署到WAF、ELB、CDN，详细操作请参见**部署证书**。
将证书配置到其他华为云产品中	先将证书下载到本地，然后再到对应的云产品控制台上传数字证书并进行部署。 配置过程中如有问题，请参考相应服务文档进行处理或咨询对应服务。

另外，如果您需要将证书配置到服务器上，请根据服务器类型进行配置。具体操作请参见**如何在服务器上安装SSL证书?** 。

7.3.2 如何将 SSL 证书应用到华为云产品?

SSL证书签发后或成功上传后，可以在华为云的其他云产品中使用，如WAF、ELB、CDN等。

目前，SSL证书管理支持将证书一键部署到WAF、ELB、CDN。其他产品则需要下载证书后，再在对应的云产品控制台上传数字证书并进行部署。

约束条件

- 更新SSL证书到ELB时，有以下几点限制条件，请您提前确认：

  - 您已在ELB中配置过证书，即您需要先在ELB服务中完成**首次**证书的配置，才能通过SCM服务更新证书。ELB中创建证书详细操作请参见**创建证书**。
  - 通过SCM更新ELB中的证书，可以更新部署在ELB监听器下证书，即在SCM控制台更新对应ELB中证书的内容及私钥，更新成功后，ELB将自动对该证书部署的监听器实例完成证书内容及私钥的更新。
  - ELB中使用的证书，需要指定域名，才可在SCM中完成更新证书的操作。
  - ELB中使用的证书如果指定了多个域名，更新证书前需要注意SCM证书的域名与其是否完全匹配。如果不完全匹配，则在SCM中执行更新证书操作后，会同时将ELB中使用的证书域名更新为当前SCM中证书的域名。

    示例：SCM中证书的主域名及附加域名为example01.com，example02.com，ELB中证书的域名为example01.com，example03.com，在SCM中执行更新证书操作后，会将该ELB中证书的域名更新为example01.com，example02.com。
- 目前，SCM证书仅支持一键部署到WAF的“default”企业项目下。如果您使用的是其他项目，则无法直接部署，您可以先将证书下载到本地，然后再到WAF控制台上传证书并进行部署。
- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，那么签发的证书**不支持**一键部署到云产品。如需在对应云产品中使用证书，可以先将证书下载到本地，然后再到对应云产品中上传证书并进行部署。

将证书应用到 WAF、ELB、CDN 中

SSL证书管理支持将证书一键部署到WAF、ELB、CDN中。部署成功后，可以帮助您提升云产品访问数据的安全性。

详细操作请参见**部署证书**。

将证书应用到其他云产品

如果您需要将您的数字证书部署到其他产品中，您可以先将证书下载到本地，然后再到对应的云产品控制台上传数字证书并进行部署。

7.3.3 一键部署 SSL 证书到云产品时，会部署到哪些地域?

通过华为云SSL证书管理购买数字证书，支持一键部署到华为云的弹性负载均衡（Elastic Load Balance，ELB）、Web应用防火墙（Web Application Firewall，WAF）、CDN（Content Delivery Network，内容分发网络）产品中。

部署时，根据产品的不同，部署区域也会有所不同：

- 当部署/更新证书到ELB和WAF时，用户可以自行选择部署到哪个区域，选择并部署后，SSL证书管理会将数字证书部署到用户所选择的区域。
- 当部署证书到CDN时，无需选择区域，SSL证书管理会将数字证书部署到CDN服务中。

如果您没有购买对应的云产品，或您的数字证书所绑定的域名没有在对应的云产品中开通服务，请不要将数字证书部署到对应的云产品中，如果部署将可能导致部署失败。

7.3.4 一键部署 SSL 证书到云产品后，HTTPS 服务就自动启用了吗?

是。

使用CCM一键部署证书到云产品后，HTTPS服务就自动启用了，不需要进行其他参数配置。

7.3.5 在 WAF/ELB/CDN 等服务中使用证书时，出现问题如何处理?

在WAF/ELB/CDN等服务中使用证书时，出现问题请直接提单至WAF/ELB/CDN产品中进行咨询。

SSL证书管理支持将已签发的证书一键部署到WAF、ELB、CDN产品中，配置过程中如有问题，请参考WAF/ELB/CDN服务文档进行处理或咨询WAF/ELB/CDN服务。

如果仍未解决您的问题，需提工单咨询，请直接提单至WAF/ELB/CDN产品中进行咨询，以便能更快更准确解决您的问题。

相关操作：

一键部署到WAF、ELB、CDN产品，详细操作请参见**部署证书到云产品**。

7.3.6 为什么在 CDN 中进行 HTTPS 配置时，提示证书链不齐全?

当在CDN（Content Delivery Network，内容分发网络）中使用SSL证书进行HTTPS配置时，如果出现HTTPS配置证书失败，提示证书链不齐全的情况，请参照以下方式进行排查、处理：

请您查看证书链是否填写完整，是否按照格式添加，是否将所有证书填写完整，证书顺序是否正确。

如果证书顺序不对，请按照“服务器证书-证书链”的顺序依次排列。

如果是证书链不完整，请参见**如何解决SSL证书链不完整?** 操作补齐证书链。

通过华为云SSL证书管理购买的数字证书，支持一键部署到CDN产品中，部署后，可以帮助您提升云产品访问数据的安全性。无需再手动导入证书，避免了此类报错。因此建议您在华为云SSL证书管理中购买证书。

7.3.7 “自己生成 CSR”方式申请的 SSL 证书，部署到 WAF/ELB/CDN 等服务中报错，该如何处理?

如果申请证书时，“证书请求文件”选择的是“自己生成CSR”，证书签发后，证书文件中不包含证书私钥文件，因此将出现一键部署证书到WAF/ELB/CDN等服务中出现报错的问题。

手动生成CSR文件的同时会生成私钥文件，上传“证书请求文件”时，无需上传私钥文件，私钥文件由用户自行保管。

如需在WAF/ELB/CDN等服务中使用证书，请参照以下方法进行操作：

- 使用SCM的一键部署功能
  a. 下载证书。
     将已签发的证书下载到本地，具体操作请参见**下载证书**。
  b. 上传证书。
     将**a**下载的证书和本地保存的私钥一起上传到SCM中，具体操作请参见**上传证书**。
  c. 一键部署证书到WAF/ELB/CDN。

将上传的证书部署到WAF/ELB/CDN等服务中，具体操作请参见**部署证书到云产品**。

- 不使用SCM的一键部署功能

  a. 下载证书。

  将已签发的证书下载到本地，具体操作请参见**下载证书**。

  b. 在WAF/ELB/CDN等服务中上传证书。

  请在WAF/ELB/CDN等服务中，上传**a**下载的证书，具体操作请参照对应服务文档。

7.3.8 SSL 证书签发后，如何使用?

CA机构审核通过后，将签发证书。证书签发后，即可使用。

- 通过华为云SCM签发的证书。
  - 将产品用于华为云WAF、ELB、CDN云产品中。通过一键部署证书到具体的服务，具体的方法请参考**部署证书到云产品**。
  - 将证书部署到其他云产品中。先将证书下载到本地，再到对应的云产品控制台上传数字证书并进行部署。
  - 将证书配置到服务器上。先将证书下载到本地，再参照**如何在服务器上安装SSL证书?** 将证书部署到对应的服务器上。
- 非华为云签发的证书。
  - 将证书部署到云产品中，先将证书下载到本地，再到对应的云产品控制台上传数字证书并进行部署。
  - 将证书配置到服务器上。先将证书下载到本地，再参照**如何在服务器上安装SSL证书?** 将证书部署到对应的服务器上。

7.3.9 SSL 证书部署失败怎么办?

证书管理支持将上传的证书和通过SCM签发的证书一键部署到弹性负载均衡（Elastic Load Balance，ELB）、Web应用防火墙（Web Application Firewall，WAF）、CDN（Content Delivery Network，内容分发网络）等其它华为云产品中。但是以下情况会导致部署失败：

- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，那么签发的证书**不支持**部署到云产品。

  解决方法：

  先将证书下载到本地，然后再到对应的云产品控制台上传数字证书并进行部署。

- 没有购买对应的云产品，或数字证书所绑定的域名没有在对应的云产品中开通服务，部署将可能导致部署失败。

  解决方法：

  没有购买对应的云产品或在对应的云产品中开通服务

- 如果您已将证书部署或者上传到对应的云产品中，即目标证书在对应的云产品中已存在，再次通过SCM平台部署时，将会部署失败。

  解决方法：

  查看是否已部署，如果SSL已部署则无需再次部署。

7.3.10 上传 SSL 证书相关问题

上传证书相关问题，请根据您的情况选择具体解决方法：

上传证书到 SSL 证书管理中，需要上传什么格式的?

目前SSL证书管理平台只支持上传PEM格式的证书。

其他格式的证书需要转化成PEM格式后才能上传，具体操作请参见**如何将证书格式转换为PEM格式?** 。

上传证书会影响原平台使用吗?

不会影响原平台的使用。

上传可以理解为把用户本地的证书，复制一份到华为云来，复制操作是不会影响证书使用的。

为什么上传证书成功后，访问域名仍然提示不安全?

证书上传成功后，还需要部署证书到对应的云产品中，并在对应的云产品中进行配置。

SSL证书管理支持将证书一键部署到WAF、ELB、CDN中。部署成功后，可以帮助您提升云产品访问数据的安全性。

详细操作请参见**部署证书**。

什么是公钥和私钥?

SSL证书管理支持上传原有的证书和私钥，您需要确认证书和私钥是一一对应的。关于公钥和私钥的详细说明，以及如何创建私钥请参见**什么是公钥和私钥?** 。

为什么要使用无密码保护的私钥?

在云产品使用数字证书，需要保证您的私钥无密码保护。关于为什么需要使用无密码保护的私钥，详情请参见**为什么要使用无密码保护的私钥?** 。

为什么在 CDN 中进行 HTTPS 配置时，提示证书链不齐全?

向CDN、ELB、WAF等云产品推送数字证书时，需要正确上传证书文件及证书链文件。当在CDN中进行HTTPS配置时，提示证书链不齐全，请参考**如何正确上传证书?** 。

7.3.11 上传 SSL 证书时可能有哪些报错，如何解决?

您可以将您所拥有的SSL证书（已在其他平台购买并签发的SSL证书）上传到云证书管理平台，以便在云证书管理平台对您的证书进行统一管理。关于上传证书具体的操作步骤，请参考**上传已有SSL证书**。

本章节为您介绍上传证书过程中可能出现的报错提示及如何解决报错。

表 7-3 证书上传报错

报错类型	错误码	报错信息详情	解决措施
解析证书链报错	SCM.0053	证书格式错误，应该以特定的字符串开头或结尾	证书格式错误，要以-----BEGIN CERTIFICATE-----开头和以-----END CERTIFICATE-----结尾。
	SCM.0054	证书内容缺失	证书前后缀之间内容有缺失，需要补充前后缀之间的内容。
检查证书链报错	SCM.0079	CaCert的主题与证书的签发者不匹配	确保证书链中的证书签发关系正确，证书链的顺序为用户证书到底层CA。 例如：证书链现有两个证书：签发证书A、被签发证书B，需要确保证书A的subjectDN和证书B的issuerDN一致。
	SCM.0109	证书链长度必须大于1	请上传长度大于1的证书链。
国际标准SSL证书上传报错	SCM.0012	上传私钥解析不正确，请确保填写已签发证书	请检查您的私钥内容，需上传正确的私钥。
	SCM.0114	私钥格式错误，应该以特定字符串开头或结尾	检查私钥格式，需要以*开头和以*结尾。
	SCM.0115	私钥不是Base64编码	检查私钥格式，需要为Base64编码。
	SCM.0116	生成私钥失败	请输入正确的的私钥内容。
国密证书上传报错	SCM.0059	国密私钥为空	请输入正确的国密私钥。
	SCM.0115	私钥不是Base64编码	检查私钥格式，需要为Base64编码。
	SCM.0116	生成私钥失败	请输入正确的的私钥内容。
	SCM.0114	私钥格式错误，应该以特定字符串开头或结尾	检查私钥格式，需要以*开头和以*结尾。
	SCM.0012	国密私钥解析失败	请输入正确的私钥内容。
	SCM.0118	国密证书长度必须为1	国密证书-加密证书链长度必须为1。
	SCM.0055	证书内容不是Base64编码	请检查证书内容，需要为Base64编码。

报错类型	错误码	报错信息详情	解决措施
	SCM.0058	生成X509证书失败	请输入正确的证书内容。
	SCM.0119	写入加密证书或私钥内容失败	请输入正确的加密证书或私钥内容。
	SCM.0117	写入私钥或证书内容失败	请输入正确的证书或私钥内容。

7.4 SSL 证书问题排查类

7.4.1 浏览器提示 SSL 证书不可信怎么办?

如果遇到电脑浏览器或手机浏览器提示证书不可信的问题，请确认您所购买的数字证书品牌和提示证书不可信的终端类型。

部分品牌的数字证书在某些终端上是不被支持的，请参考该品牌的数字证书的官网中的相关介绍。

目前市场上的主流设备都是兼容DigiCert、GeoTrust品牌的数字证书的。

说明

Chrome53版本存在已知的问题导致不兼容DigiCert、GeoTrust品牌证书：

- Chrome 53 Bug Affecting DigiCert SSL/TLS Certificates
- Warning | Certificate Transparency error with Chrome 53

排查步骤

排除数字证书与终端不兼容的问题后，建议您按以下步骤进行检查：

1. 首先建议您使用**GlobalSign SSL Server Test**工具进行检查：
   - 如果检查结果中的证书品牌、证书类型、域名与您购买的不一致，请仔细检查服务器上数字证书的配置。
   - 如果检查结果显示证书链不完整，请检查数字证书相关配置是否正确。

   须知

   证书服务提供的PEM格式数字证书包含两段内容，两段内容中的任何一段都不能丢失。如果两段内容之间存在空白行，请删除空白行。配置修改完成后重启Web服务，并重新检查。
2. 确保您的数字证书配置中已关闭了不安全的协议，如SSLv3等有已知隐患的协议。
3. 检查您的网页中是否引用了一些HTTP资源。部分浏览器对HTTPS站点引用HTTP资源的情况会认为是不安全的。
4. 如果一个域名有多台服务器，请您确认是否每台服务器都正确部署了证书。

7.4.2 部署了 SSL 证书后，为什么网站仍然提示不安全?

问题描述

配置好HTTPS后，访问网站，仍然出现拦截，并提示不安全。

问题原因

- 可能原因一：访问的域名与证书域名不一致
- 可能原因二：网站内使用了非HTTPS素材，包括图片、CSS、js等
- 可能原因三：SSL证书已到期
- 可能原因四：浏览器缓存较多
- 可能原因五：网站接入了Web应用防火墙（Web Application Firewall，WAF），WAF中网站绑定的证书未更新

解决方法

请根据可能原因选择操作步骤：

- **原因一：访问的域名与证书域名不一致**
  例如，您访问的是“https://yun.huaweicloud.com/”，但是您使用的证书是“huaweicloud.com”的，您的证书信息如图7-8所示。

  图 7-8 证书域名信息

  您购买证书是绑定域名“huaweicloud.com”的，不能用于“yun.huaweicloud.com”的。“huaweicloud.com”和

“yun.huaweicloud.com”都是一个单独的域名，每个明细子域名都算一个域名，不能使用同一个证书。

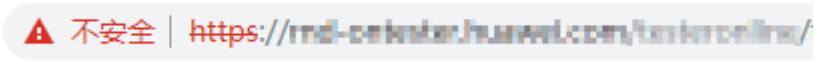
解决方法：

建议购买并申请对应域名的SSL证书。例如，此处可购买证书并绑定“yun.huaweicloud.com”域名，即可通过“https://yun.huaweicloud.com/”进行访问。

如果您的域名在同一个级别，未跨级别，如yun.huaweicloud.com、test.huaweicloud.com、example.huaweicloud.com等，均在一个级别，在“*.huaweicloud.com”的包含范围内，则可购买泛域名证书，绑定泛域名“*.huaweicloud.com”即可。

- **原因二：网站内使用了非HTTPS素材，包括图片、CSS、js等**

  当HTTPS网页中被引入了HTTP协议的不安全元素，如：图片、js、css文件、音频、视频、Flash资源、CSS中引用的HTTP图片、js脚本写入的不安全元素等，默认就会被浏览器拦截。如果强制载入，则会出现不安全提示，如下图所示。

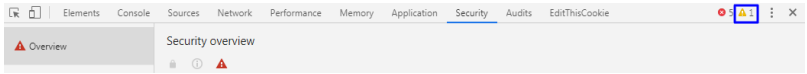
  

  解决方法：

  a. 打开浏览器（Chrome浏览器74版本为例），登录需要检查的网页。

  b. 按“F12”进入开发者模式。在右上角看到是哪些非安全链接影响了网站。

  图 7-9 不安全链接

  c. 找到所提示的链接，可以看到确实是http的素材路径。

  图 7-10 不安全素材

  - 如果这个链接内容是没什么作用的链接，请直接删除该链接。删除后可以继续查看，确认是否清除了非安全链接。
  - 如果这个链接的内容是至关重要且不能删除的，请将http的素材路径改为https的素材路径。

  须知

  如果您的网站涉及API等数据类网站，建议和数据调用厂商联系。因为API非常重要，不能随便修改。如果厂商没有做https认证，建议您也不要做认证，防止调用的数据出现问题。具体请与您的相关厂商进行沟通。

  d. 处理完成后，请清除浏览器缓存，再次访问网站。

- **原因三：SSL证书已到期**

  您的SSL证书已到期，登录时将会提示不安全。

解决方法：

SSL证书到期后需要重新购买证书，详细描述请参见**SSL证书过期了怎么办？**。

- **原因四：浏览器缓存较多**

  解决方法：请清除浏览器缓存或者更换浏览器重试。

- **原因五：网站接入了Web应用防火墙（Web Application Firewall， WAF），WAF中网站绑定的证书未更新**

  解决办法：

  - 如需继续使用WAF，请同步更新WAF中网站绑定的证书，详细操作请参见**在WAF更新证书**。
  - 如不再使用WAF，请将DNS解析到源站。

7.4.3 部署了 SSL 证书后，为什么通过域名无法访问网站?

问题描述

当在服务器上成功部署SSL证书后，通过“https://+域名”的方式访问网站时，显示无法打开网站。

问题原因

- 可能原因一：未开启443端口
- 可能原因二：配置文件未配置正确

解决方法

请根据可能原因选择操作步骤：

- **原因一：未开启443端口**

  解决方法：

  在安装SSL证书的服务器上开启“443”端口，同时在安全组增加“443”端口，避免安装后仍然无法启用HTTPS。

- **原因二：配置文件未配置正确**

  解决方法：请根据安装配置操作进行排查。

7.4.4 为什么安装了 SSL 证书后，https 访问速度变慢了?

安装了SSL证书后，访问网站时，HTTPS比HTTP要多几次握手的时间，HTTPS协议握手阶段比较费时，同时还要进行RSA校验，因此使用了SSL证书后，相较于HTTP访问，访问速度变慢了。

另外，会增加服务器CPU的处理负担，因为要为每一个SSL链接实现加密和解密，但一般不会影响太大。

为了减轻服务器的负担，建议注意以下几点：

1. 仅为需要加密的页面使用SSL，如“https://www.domain.com/login.asp”，不要把所有页面都使用“https://”，特别是访问量大的首页。
2. 尽量不要在使用了SSL的页面上设计大块的图片文件或者其他大文件，尽量使用简洁的文字页面。

7.4.5 为什么配置了 SSL 证书仍存在用户访问时提示不受信任?

问题现象

用户已将购买的SSL证书配置到ELB中，访问域名时，存在部分电脑访问提示不受信任，且同一办公网络部分电脑反馈“Windows没有足够信息，不能验证证书”。

原因

电脑终端浏览器版本未及时更新，无法识别根证书。

解决方案

将浏览器版本更新至最新版本。为了更加稳定的访问您的服务器，建议您使用Chrome、IE等这些主流的浏览器。

7.4.6 浏览器提示“您的连接不是私密链接”错误怎么办?

问题描述:

2016年11月左右，部分浏览器用户反馈，通过53版本的Chrome浏览器或9.5.1版本的QQ浏览器（内置Chrome53内核）访问HTTPS网站时，出现“NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED”的错误，导致显示HTTPS网站异常。

解决办法:

- 如果为53版本的Chrome浏览器，则请使用非53版本的Chrome浏览器进行HTTPS网站访问，便可避免上述问题。

  Chrome浏览器版本查看方法如下:

  a. 打开Chrome浏览器，单击浏览器右上角的更多图标 ，并选择“帮助 > 关于 Google Chrome(G)”，进入Chrome帮助页面。
  b. 在帮助页面中，查看Chrome的版本，如图7-11所示。

  图 7-11 Chrome 版本

- 如果为9.5.1版本的QQ浏览器（内置Chrome53内核），且请将QQ浏览器更新到最新版本，便可避免上述问题。该问题已经在新版本中修复，使用了旧版本QQ浏览器的用户也建议更新到最新版本。

  QQ浏览器版本查看方法如下:

a. 打开QQ浏览器，单击浏览器右上角的三，并选择“帮助 > 关于”。
b. 在弹出的浏览器版本信息框中，查看QQ浏览器的版本。

其他浏览器暂无此问题，可正常访问。

7.4.7 SSL 证书部署后，浏览器是否会弹出不安全提示?

不会。

免费测试证书会对网站域名进行简易验证，能起到加密传输的作用。如果证书安装正确，且在有效期内，在使用时，浏览器不会弹出不安全提示。

另外，收费证书不仅会对申请者做严格的身份审核验证，还会提供高强度通信链路加密功能，保护内外部网络上敏感数据传输。如果证书安装正确，且在有效期内，在使用时，浏览器也不会弹出不安全提示。

8 证书有效期

8.1 SSL 证书过期了怎么办?

SSL证书存在有效期限制。证书过期之后，将无法继续使用，您需要在证书到期前进行续费。

在华为云SSL证书管理中购买的，已签发且即将到期的付费SSL证书支持续费操作。证书续费详细操作请参见**续费SSL证书**。

SCM会在证书到期前30天提醒您证书即将到期。

须知

上传证书和在华为云购买的SSL证书，系统会默认为您配置到期提醒并默认打开到期提醒开关，此时系统会自动为您发送邮件和短信提醒，如您需要关闭或更换具体配置，请参见**如何配置SSL证书到期提醒?** 。

- 已签发的证书，系统还会在证书到期前两个月、一个月、一周、三天、一天和到期时，发送邮件和短信提醒用户。
- 上传的第三方证书过期后，如您需要继续使用，请重新购买并上传，上传证书操作具体请参考**上传已有SSL证书**。

重新购买或续费证书成功后（重新购买、手动续费时您需要重新提交证书审核申请），您将获得一张新的证书，您需要在您的服务器上安装新证书来替换即将过期的证书，或在对应的云产品中替换新的证书。

新证书签发后即可替换，替换过程不会影响业务。

说明

- 如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到验证通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。
- 证书续费后，新旧证书有效期说明如下：
  - 续费证书信息不变

    在证书信息不变情况下，新申请的证书的到期时间=原证书到期时间+新申购证书的有效期。**最多累加30天**，如果您未开通自动续费，建议您提前30天开始申请证书。

    示例：您的原有证书到期时间是2019年10月1号，您于2019年8月31号申请同品牌、同类型SSL证书，有效期为1年。新证书于2019年9月1号签发，签发有效期将为2019年9月1号~2020年9月30号。

    此条规则由证书签发CA制定、解释和澄清，如有疑问，华为云将配合您与CA机构进行沟通和协商。
  - 手动续费过程中修改了新证书信息（如域名、证书类型或公司名称等不同于旧证书）

    新旧证书有效期分别计算。

    新签发证书不影响之前旧证书，旧证书到期前均可使用，两张证书均可使用。

- 安装证书详细操作，您可以参考**表 安装SSL证书操作示例**。

  表 8-1 安装 SSL 证书操作示例

服务器类型	操作示例
Tomcat	**在Tomcat服务器上安装SSL证书**
Nginx	**在Nginx服务器上安装SSL证书**
Apache	**在Apache服务器上安装SSL证书**
IIS	**在IIS服务器上安装SSL证书**
Weblogic	**在Weblogic服务器上安装SSL证书**
Resin	**在Resin服务器上安装SSL证书**

- 在其他云产品中使用证书操作请参见**如何将SSL证书应用到华为云产品？**。

8.2 SSL 证书的有效期是多久？

SSL证书的有效期为1年，即证书在审核通过之后的1年内有效，到期后将无法继续使用。

您可以在SSL证书即将到期前进行续费，具体操作请参见**续费SSL证书**。

如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到短信通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。

证书有效期从什么时候开始计算?

证书有效期从签发日开始计算。证书签发时间是指申请证书、并通过了CA中心的审核验证后，证书最终签发的时间。

多域名类型的证书，如果是新增附加域名，证书有效期是从第一次签发日开始计算。

证书到期前多久会发送通知?

SCM会在证书到期前30天提醒您证书即将到期。

- 已签发的证书，系统还会在证书到期前两个月、一个月、一周、三天、一天和到期时，发送邮件和短信提醒用户。
- 上传的第三方证书过期后，如您需要继续使用，请重新购买并上传，上传证书操作具体请参考**上传已有SSL证书**。

在华为云SSL证书管理中购买的，已签发且即将到期的付费SSL证书支持续费操作。证书续费详细操作请参见**续费SSL证书**。

8.3 SSL 证书即将到期，该如何处理?

SSL证书存在有效期限制。证书过期前必须及时续费，否则将导致证书过期后不被信任，已安装证书的网站业务会受到影响（提示访问不安全或无法访问）。

SSL证书即将到期前，可在控制台设置开通自动续费或手动执行续费操作。手动续费操作入口将在SSL证书到期前30个自然日内开放，其余时间不支持操作。

SCM会在证书到期前30天提醒您证书即将到期。

- 已签发的证书，系统还会在证书到期前两个月、一个月、一周、三天、一天和到期时，发送邮件和短信提醒用户。若到期前已续费新证书，则新证书续费成功并签发后，系统将不会再发送邮件和短信提醒用户旧证书即将过期，如需系统发送旧证书到期提醒，具体配置操作请参见**如何配置SSL证书到期提醒?** 。
- 上传的第三方证书过期后，如您需要继续使用，请重新购买并上传，上传证书操作具体请参考**上传已有SSL证书**。

重新购买或续费证书成功后（重新购买、手动续费时您需要重新提交证书审核申请），您将获得一张新的证书，您需要在您的服务器上安装新证书来替换即将过期的证书，或在对应的云产品中替换新的证书。

新证书签发后即可替换，替换过程不会影响业务。

说明

- 如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到验证通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。
- 证书续费后，新旧证书有效期说明如下：
  - 续费证书信息不变

    在证书信息不变情况下，新申请的证书的到期时间=原证书到期时间+新申购证书的有效期。**最多累加30天**，如果您未开通自动续费，建议您提前30天开始申请证书。

    示例：您的原有证书到期时间是2019年10月1号，您于2019年8月31号申请同品牌、同类型SSL证书，有效期为1年。新证书于2019年9月1号签发，签发有效期将为2019年9月1号~2020年9月30号。

    此条规则由证书签发CA制定、解释和澄清，如有疑问，华为云将配合您与CA机构进行沟通和协商。
  - 手动续费过程中修改了新证书信息（如域名、证书类型或公司名称等不同于旧证书）

    新旧证书有效期分别计算。

    新签发证书不影响之前旧证书，旧证书到期前均可使用，两张证书均可使用。

8.4 SSL 证书购买后多久生效?

证书购买后，需要申请证书，CA机构将对用户提交的申请进行审核，审核通过后才会签发证书。

证书签发后立即生效。

证书的有效期为1年，即证书在审核通过之后的1年内有效，到期后将无法继续使用。如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到验证通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。

多域名类型的证书，如果是新增附加域名，证书有效期是从第一次签发日开始计算。

8.5 新旧 SSL 证书相关问题

新旧 SSL 证书有效期说明

证书续费成功，新证书签发后，旧证书仍在有效期内，新增证书有效期和使用说明如下：

- 续费证书信息不变

  在证书信息不变情况下，新申请的证书的到期时间=原证书到期时间+新申购证书的有效期。**最多累加30天**，如果您未开通自动续费，建议您提前30天开始申请证书。

  示例：您的原有证书到期时间是2019年10月1号，您于2019年8月31号申请同品牌、同类型SSL证书，有效期为1年。新证书于2019年9月1号签发，签发有效期将为2019年9月1号~2020年9月30号。

  此条规则由证书签发CA制定、解释和澄清，如有疑问，华为云将配合您与CA机构进行沟通和协商。

  此时，两张证书视为同一张证书，均在使用中。

- 手动续费过程中修改了新证书信息（如域名、证书类型或公司名称等不同于旧证书）

  新旧证书有效期分别计算。

  新签发证书不影响之前旧证书，旧证书到期前均可使用，两张证书均可使用。

新旧 SSL 证书替换对业务有影响吗?

重新购买或续费证书成功后（重新购买、手动续费时您需要重新提交证书审核申请），您将获得一张新的证书，您需要在您的服务器上安装新证书来替换即将过期的证书，或在对应的云产品中替换新的证书。

新证书签发后即可替换，替换过程不会影响业务。

8.6 SSL 证书是一次性产品，到期后如何申请?

SSL证书是一次性产品，且存在有效期限制。证书到期后将无法继续使用。如需继续使用证书，您可以在证书到期前进行续费。证书续费详细操作请参见**续费SSL证书**。

SCM会在证书到期前30天提醒您证书即将到期。

- 已签发的证书，系统还会在证书到期前两个月、一个月、一周、三天、一天和到期时，发送邮件和短信提醒用户。
- 上传的第三方证书过期后，如您需要继续使用，请重新购买并上传，上传证书操作具体请参考**上传已有SSL证书**。

重新购买或续费证书成功后（重新购买、手动续费时您需要重新提交证书审核申请），您将获得一张新的证书，您需要在您的服务器上安装新证书来替换即将过期的证书，或在对应的云产品中替换新的证书。

新证书签发后即可替换，替换过程不会影响业务。

说明

- 如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到验证通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。
- 证书续费后，新旧证书有效期说明如下：
  - 续费证书信息不变

    在证书信息不变情况下，新申请的证书的到期时间=原证书到期时间+新申购证书的有效期。**最多累加30天**，如果您未开通自动续费，建议您提前30天开始申请证书。

    示例：您的原有证书到期时间是2019年10月1号，您于2019年8月31号申请同品牌、同类型SSL证书，有效期为1年。新证书于2019年9月1号签发，签发有效期将为2019年9月1号~2020年9月30号。

    此条规则由证书签发CA制定、解释和澄清，如有疑问，华为云将配合您与CA机构进行沟通和协商。
  - 手动续费过程中修改了新证书信息（如域名、证书类型或公司名称等不同于旧证书）

    新旧证书有效期分别计算。

    新签发证书不影响之前旧证书，旧证书到期前均可使用，两张证书均可使用。

新证书获取后，需要在服务器上安装新的证书来替换即将过期的证书，或在对应的云产品中替换新的证书。具体可参照以下步骤进行处理：

- 安装证书详细操作，您可以参考**表 安装SSL证书操作示例**。

表 8-2 安装 SSL 证书操作示例

服务器类型	操作示例
Tomcat	在Tomcat服务器上安装SSL证书
Nginx	在Nginx服务器上安装SSL证书
Apache	在Apache服务器上安装SSL证书
IIS	在IIS服务器上安装SSL证书
Weblogic	在Weblogic服务器上安装SSL证书
Resin	在Resin服务器上安装SSL证书

- 在其他云产品中使用证书操作请参见**如何将SSL证书应用到华为云产品?** 。

8.7 如何配置 SSL 证书到期提醒?

背景

SSL证书存在有效期限制，到期后将无法继续使用，所以如果您未开通自动续费，证书到期前您需预留**3-10个工作日**重新购买或手动续费，如果您已开通自动续费，请注意查收验证提醒的短信通知，您收到验证通知后请提前**3-10个工作日**配合完成相关的验证操作，以免证书审核还未完成之前现有证书已经过期。

为了防止您的证书到期后给您的业务造成风险，CCM提供了以下到期提醒的方式：

- 控制台提醒方式，即上传的证书和已签发的证书到期前30天，SSL证书管理控制台会提示您有即将到期的证书。如图8-1所示。

图 8-1 证书列表

- 消息提醒方式。在SSL证书管理服务中签发的证书和上传的证书支持证书到期前消息提醒功能，即在证书即将到期前两个月、一个月、一周、三天、一天及证书过期当天，系统将默认向证书申请人或配置的消息接收人发送证书到期提醒信息。如果您想增加或者修改消息通知接收人，可以参考**配置消息接收人**进行配置。

如果您的证书即将到期，在收到系统的消息提醒时，请参考**SSL证书即将到期，该如何处理？**进行处理。

配置消息接收人

步骤1 登录**云证书管理服务控制台**。

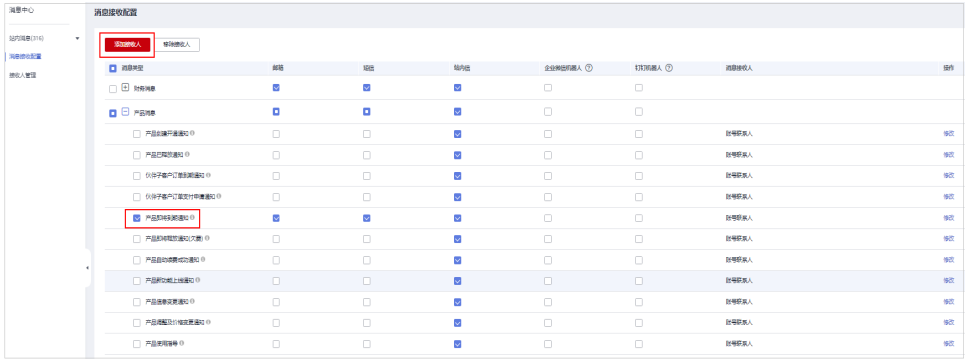
步骤2 单击页面右上角的，打开通知窗口。

步骤3 单击“更多”，进入“消息中心”服务页面。

步骤4 在左侧导航树中，选择“消息接收配置”，进入“消息接收配置”页面。

步骤5 在“产品消息”页签中勾选“产品即将到期通知”，在页面左上方单击“添加接收人”。

图 8-2 添加接收人



步骤6 在弹出的“添加接收人”对话框中，勾选已有的账号联系人或者单击“添加接收人”，填入新增消息接收人的姓名、邮箱和手机号码并单击“保存”填写的信息。

图 8-3 添加接收人

步骤7 单击“确定”。

在添加完消息接收人信息后，系统将自动发送验证信息到所填手机号和邮箱，通过验证后方可接收消息。

----结束

后续操作

配置成功后，“到期提醒”开关默认为打开状态，如需关闭该提醒，请单击证书名称进入证书详情页，并单击  关闭，如需再次打开，单击  即可，如**图 到期提醒开关**所示。

须知

“到期提醒”开关只在证书已签发、已到期和托管中三个状态展示，其中已到期状态开关不可修改。

图 8-4 到期提醒开关

8.8 SSL 证书到期未更新新证书，会影响业务吗？

SSL证书到期了，如果后续不再进行使用，则无需再次购买，不会影响业务。

另外，需要注意的是，如果SSL证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。黑客等不法分子可以利用过期的SSL证书，篡改或窃取浏览器和服务器之间传输的信息和数据，从而影响用户的数据安全。

当浏览器用户发现网站服务器证书过期，会对该网站不信任，从而为企业的品牌形象带来负面的影响。网站服务器过期后，用户可能会为了避免出现个人损失，而选择停止访问该网站。

8.9 私有证书有效期相关问题

私有证书的有效期是多久?

- 设置有效期

  私有证书的有效期根据您申请证书时所设置的有效期而定，如图8-5所示。具体操作请参见**申请私有证书**。

  须知

  私有证书由处于激活状态的CA进行签发，所以，设置私有证书有效期时须满足：私有证书有效期 ≤ 签发的私有CA有效期。

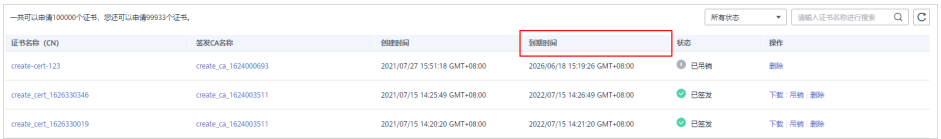
  图 8-5 设置有效期

- 查看到期时间

  私有证书申请成功后，您可以登录管理控制台，在私有证书列表页面查看证书到期时间，如图8-6所示。具体操作请参见**查看私有证书详情**。

  图 8-6 查看私有证书到期时间

如何配置私有证书和私有 CA 到期提醒?

通过配置产品即将到期的消息通知，当私有CA在即将到期前半年、3个月、1个月，私有证书在即将到期前30天、7天时，系统将默认向您配置的消息接收人发送到期提醒。配置步骤如下：

步骤1 登录**云证书管理服务控制台**。

步骤2 单击右上角的  ，进入消息中心。

步骤3 在左侧导航栏，选择“消息接收配置”，进入“消息接收配置”页面。

步骤4 在“产品消息”下方，勾选“产品即将到期通知”，单击页面上方的“绑定接收人”。

步骤5 在弹出的“绑定接收人”对话框中，在手机邮箱页签下，按实际需要勾选接收人姓名。

- 您可以在手机邮箱、企业微信机器人、钉钉机器人、飞书机器人等页签下分别勾选需要添加的接收人。可以同时设置多个接收人，以及多种通知方式。
- 您也可以单击“添加接收人”，添加并选择新的接收人。系统会自动发送验证信息到新添加的接收人的手机号和邮箱中，通过验证后，该接收人方可接收消息。

步骤6 单击“确定”，完成配置。

----结束

私有证书的有效期快到了，怎么避免业务中断?

为了避免证书过期，导致业务中断，请参考如下步骤进行处理。

步骤1 申请新证书。

私有证书到期不支持续费，当私有证书到期后将无法继续使用，建议在证书到期前提前申请新证书。具体操作请参见**申请私有证书**。

步骤2 替换过期证书。

在旧证书过期前，用新签发的证书提前替换旧证书。详细的轮换方案请参见最佳实践**私有CA轮换**和**私有证书轮换**。

----结束

8.10 购买证书后未立即申请，订单多久后会失效?

您购买SSL证书后如果未申请证书，订单将一直保留，不会失效，您在需要使用时申请即可。

8.11 如何查询证书还有多久到期?

SCM会在证书到期前30天提醒您证书多久到期。

- 已签发的证书，系统还会在证书到期前两个月、一个月、一周、三天、一天和到期时，发送邮件和短信提醒用户。

- 上传的第三方证书过期后，如您需要继续使用，请重新购买并上传，上传证书操作具体请参考**上传已有SSL证书**。

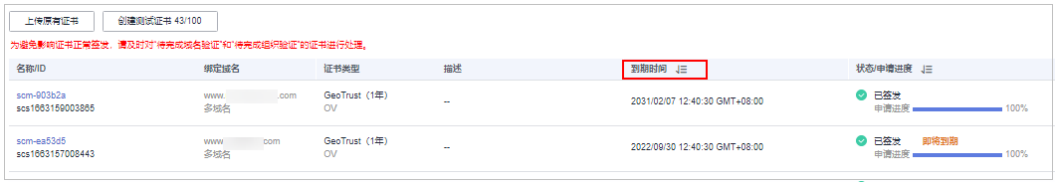
除此之外，您可以在华为云云证书管理控制台查看SSL证书的到期时间，具体步骤如下：

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理”，进入SSL证书管理页面。

步骤3 在待查询证书的“到期时间”列，查看证书的到期时间。

图 8-7 证书到期时间



----结束

9 计费、续费与退订

9.1 SSL 证书是如何收费的?

SSL证书管理服务为您提供了一种证书品牌为DigiCert品牌、证书类型为DV（Basic）、域名类型为单域名的用于测试的免费证书。关于免费证书的相关信息请参考**如何申请免费证书?** 。

除此之外，SSL证书管理服务会根据您选择的证书类型、证书品牌、域名类型、域名数量和购买时长进行收费。

详细的服务资费费率标准，请参见**产品价格详情**。

上传证书到SSL证书管理中进行集中管理，管理上传证书暂不收费。

9.2 SSL 证书是否支持续费?

支持。

CA机构签发的SSL证书默认有效期为1年，证书到期后服务器将无法进行HTTPS加密通信，您可以在证书到期前进行续费。

证书续费详细操作请参见**续费SSL证书**。

续费限制说明

- 手动续费操作入口仅在SSL证书到期前**30个自然日内**开放，其余时间不支持操作。
- 仅支持对在华为云SSL证书管理中购买的，已签发且即将到期的付费SSL证书进续费，**上传的证书**、**免费证书**、**单域名扩容包**暂不支持续费。
- 手动续费相当于在控制台重新购买一张与原证书规格（即证书品牌、证书类型、域名类型、域名数量、主域名）**完全相同**的证书。
- 开启自动续费后，系统会在原证书即将到期前30天内自动为您购买一张相同规格的新证书，并且以原证书的申请信息提交证书申请，由于证书申请需要校验申请者的域名所有权、身份，因此您需要配合CA机构完成**域名验证**、**组织验证**后续费证书才会签发。
- 续费证书与原证书为独立的两张证书，因此续费证书签发后您需要**安装到Web服务器或部署到华为云产品。**

- 续费签发的新证书有效期为续费有效期（如1年）加上原证书剩余有效期。例如，您已签发的1年有效期证书将于2022年11月30日过期，如果您在2022年11月25日完成续费购买和签发，则续费签发证书的有效期将在2023年11月25日的基础上再加上5天，即2023年11月30日。

须知

- Digicert DV(basic) 泛域名证书的续费入口仅在到期前**15个自然日内**开放。
- Digicert DV(basic) 泛域名证书续费签发的新证书不支持补齐原证书剩余有效期，新证书有效期为实际续费时长。
- 如果通过**手动续费**购买入口购买的证书与原证书规格（即证书品牌、证书类型、域名类型、域名数量、主域名）不完全相同，则新签发证书的有效期为一年（可能与原证书过期前未使用的有效期存在重合），**无法自动补齐**原证书剩余的有效期。

9.3 SSL 证书支持退订吗?

SCM支持7天无理由退款。

约束与限制

- 满足以下条件（必须全部满足）的SSL证书订单，可申请退订：
  - 您通过华为云SSL证书管理控制台购买了SSL证书。
  - 距离SSL证书订单下单时间（完成支付的时间）不超过7个自然日，即距离SSL证书订单完成支付时间顺延不超过7*24小时。

    例如，12月1日12:00完成SSL证书订单支付，则在12月8日11:59前可以退订，12月8日11:59后将不支持退订。

    ⚠ 注意

    购买7天后不支持退款。
  - 已购买的SSL证书符合以下情况之一：
    - 未提交证书申请，证书状态为“待申请”。
    - 提交过证书申请，证书未签发，且已取消申请，证书状态为“待申请”。
    - 提交过证书申请，证书已签发，且在下单后7个自然日内完成了证书吊销流程（不仅是提交了吊销申请，须完成吊销流程），证书状态为“已吊销”。
- 全额退款将退还您在购买SSL证书时所支付的费用。

> **注意**
>
> 退款仅限于退还您在购买或续费SSL证书或相关服务订单时所支付的费用，代金券、优惠券抵扣的部分不支持退回。

操作步骤

步骤1 登录**云证书管理服务控制台**。

步骤2 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

步骤3 在需要退订的证书所在行的“操作”列中，单击“退订”，如**图9-1**所示。

图 9-1 退订

步骤4 在“退订信息确认”页面确认待退订证书信息，确认信息无误后，勾选退订提示信息。

步骤5 在页面右下角，单击“退订”。

> **须知**
>
> - 退订后，证书将被删除且无法恢复，请谨慎操作。
> - 退订提交后，系统将对您提交的退订进行审核。审核通过后，证书才不会显示在控制台证书列表中。在此期间，请勿对SSL证书做任何操作，避免审核失败。

在页面的右上角弹出“证书退订成功”，表示证书退订成功，已支付的费用将按照原支付路径退还给您。

退订成功后，可在“费用中心 > 订单管理 > 我的订单”中查看已退订的证书订单。

----结束

9.4 私有证书管理服务是如何收费的?

私有CA支持按需和包年/包月计费，私有证书支持按需计费，按需计费将根据您的私有CA数量、私有证书数量进行收费，包年/包月根据您购买的私有CA时长进行收费。具体收费情况以购买页面显示为准。

> **须知**
>
> 当前私有CA的按需计费模式只能通过调用API来实现，无法在管理控制台页面直接创建按需支付订单。

如何停止私有 CA 或私有证书的计费?

私有CA和私有证书支持按需计费。其中，根CA创建后即开始计费；子CA创建后不收费，激活后才开始计费。

如需停止计费，删除申请的私有CA和私有证书即可。

⚠ 注意

- 私有CA禁用期间也将保持收费。
- 用户执行删除私有CA操作后，私有CA不会立即删除。计划删除最快7天生效（根据您设置的推迟时间为准）。在此期间收费情况说明如下：
  - 如果用户未取消计划删除，私有CA被删除了，则在计划删除期间的私有CA不会收费；
  - 如果用户在计划删除期间，取消了计划删除，私有CA未被删除，则在计划删除期间的私有CA将保持收费。

  例如：您在2022年01月01日00:00执行了删除私有CA的操作，且设置的私有CA计划删除推迟时间为7天，7天后私有CA被删除，那么，PCA服务将不收取这7天的费用；如果您在2022年01月04日00:00取消了计划删除，私有CA未被删除，那么，PCA服务将补齐2022年01月01日00:00至2022年01月04日00:00期间的费用。

9.5 续费 SSL 证书后，还需要重新安装 SSL 证书吗?

需要重新安装SSL证书。

CA机构签发的每张SSL证书有效期最长只有1年，SSL证书到期后就会失效。

SSL证书续费操作相当于重新购买一张与原证书规格（即证书品牌、证书类型、域名类型、域名数量、主域名）**完全相同**的证书。因此，您需要将续费签发的新证书安装到您的Web服务器或部署到您在使用中的华为云产品（WAF/ELB/CDN）替换已过期的旧证书。

在华为其他云产品部署证书操作详情请参考**如何将SSL证书应用到华为云产品?**

在Tomcat、Nginx、Apache、IIS等服务器上安装证书，您可以参考**表 安装SSL证书操作示例**。

表 9-1 安装 SSL 证书操作示例

服务器类型	操作示例
Tomcat	**在Tomcat服务器上安装SSL证书**
Nginx	**在Nginx服务器上安装SSL证书**
Apache	**在Apache服务器上安装SSL证书**
IIS	**在IIS服务器上安装SSL证书**

服务器类型	操作示例
Weblogic	**在Weblogic服务器上安装SSL证书**
Resin	**在Resin服务器上安装SSL证书**

10 其他

10.1 SSL 证书管理类

10.1.1 吊销证书和删除证书的区别是什么?

华为云SSL证书管理服务支持对证书进行吊销，也支持对证书进行删除。

证书的吊销和删除操作都不影响您再次购买证书。

两者的不同主要表现在以下两方面：

- 含义：
  - 证书吊销：指将已签发的证书从CA签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。
  - 证书删除：指将证书资源从华为云系统中删除。证书仍然有效，浏览器信任该证书。
- 限制条件：
  - 证书吊销：

    当您的证书状态为“已签发”，且您不需要使用证书，在证书私钥已丢失，或出于安全因素考虑等情况下，可申请吊销证书。

    须知

    进入续费期的证书无法吊销，即证书到期前一个月内不支持吊销。
  - 证书删除：

    当您的证书状态为“已到期”、“托管中”、“已签发”的状态，可以在SCM的操作控制台执行删除操作。

10.1.2 提交了吊销或删除证书的申请，是否可以取消?

不可以。

吊销申请提交后或删除证书的操作执行后，将无法取消，请谨慎操作。

- 证书吊销指将已签发的证书从CA签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。

  提交吊销申请后，将由CA机构审核，审核通过后，吊销操作才算完成。

  因为吊销过程中无需用户执行任何操作，且CA机构审核流程较快，所以，提交吊销申请后，将无法取消，请谨慎操作。
- 证书删除指将证书资源从华为云系统中删除。证书仍然有效，浏览器信任该证书。

  提交删除操作后，华为云将直接执行删除操作，无需CA机构审核，将立即被删除。因此，执行删除操作后，将无法取消，请谨慎操作。

10.1.3 如何将证书格式转换为 PEM 格式?

证书格式之间是可以互相转换的。

如果您需要将其他格式的证书/私钥需要转换成PEM格式，建议通过**OpenSSL**工具进行转换。下面是几种比较流行的证书格式转换为PEM格式的方法。

证书格式转换为 PEM 格式

表 10-1 证书转换命令

格式类型	转换方式（通过**OpenSSL**工具进行转换）
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	• 提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out key.pem** • 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • 提取证书命令，以“cert.cer”转换为“cert.pem”为例。 **openssl x509 -inform der -in cert.cer -out cert.pem**

证书编码格式为 PKCS8 时

由于华为云WAF、ELB、CDN服务暂时不支持PKCS8编码格式，因此，当您将PKCS8编码格式的证书上传到SSL证书管理平台，再部署至WAF、ELB、CDN三个服务时，会报错。

说明

- 如果证书私钥文件以“-----BEGIN PRIVATE KEY-----”开头，则说明该证书是PKCS8编码格式。
- 如果证书私钥文件以“-----BEGIN RSA PRIVATE KEY-----”开头，则说明该证书是PKCS1编码格式。

当您的公钥或者私钥的编码格式是PKCS8格式时，需要执行如下操作，才能将PKCS8编码格式的证书成功地运用到WAF、ELB、CDN服务。

步骤1 证书格式是否为PEM格式。

- 是，执行**步骤2**。
- 否，参照**证书格式转换为PEM格式**将证书格式转换为PEM后，再执行**2**。

步骤2 执行如下命令将PKCS8编码格式转换为PKCS1编码格式。

- PKCS8格式私钥转换为PKCS1格式

  openssl rsa -in pkcs8.pem -out pkcs1.pem
- PKCS8公钥转PKCS1公钥

  openssl rsa -pubin -in public.pem -RSAPublicKey_out

步骤3 将转换后的证书上传至SSL证书管理平台，详细的操作请参见**上传证书**。

步骤4 再将证书部署到对应的华为云服务，详细的操作请参见**部署证书到云产品**。

----结束

10.1.4 上传证书时，“证书文件”该如何填写?

CCM支持用户将所拥有的证书上传到SSL证书管理平台，以便在SSL证书管理平台对您的证书进行统一管理。

上传已有证书到CCM中时，需要上传“证书文件”，如**图10-1**所示。

图 10-1 证书文件

目前CCM只支持上传PEM格式的证书文件。

上传证书文件时，以文本方式打开待上传证书里的PEM格式的文件（后缀名为“.pem”），将证书内容复制到**图10-1**的“证书文件”中即可。

如果上传时，系统提示证书链不完整，请参见以下方式进行处理：

一般情况下，中级机构颁发的证书文件包含多份证书，如包含服务器证书和证书链2个*.PEM格式的证书内容。在CCM中上传证书文件时，需要将所有证书拼接在一起组成一份完整的证书后再上传。更多证书链相关介绍请参见**证书链配置说明**。

拼接时，须按照“**服务器证书-证书链**”的顺序进行拼接，具体方法如下：

1. 通过记事本打开所有*.PEM格式的证书文件。
2. 将**服务器证书**放在首位，再放置**证书链**。

   一般情况下，中级机构在颁发证书的时候会有对应说明，请注意查阅相关规则。通用的规则如下：

   - 证书之间没有空行。
   - 证书链的格式如下：

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

拼接后的证书文件如**图10-2**所示。

图 10-2 拼接后的 PEM 证书文件

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj4lj5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZIdWF3ZWkxCzAJBgNVBAsMAklUMS4wLAYDVQQD
DCVIdWF3ZWkgV2ViIFNlY3VyZSBJbnRlcm5ldCBHYXRld2F5IENBMB4XDTE3MTAx
ODAwNDA0NloXDTE4MTAxODAwNDA0NlowgZoxCzAJBgNVBAYTAkNOMRAwDgYDVQQI
DAdqaWFuZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVIdWF3ZWkgU29m
dHdhcmUgVGVjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLDBBDbG91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPfLT/IV6UnvMLnxJQBavqauykCSkadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhRfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNn4c37kwjJeKf+b2F/IqO/KF+9zF
[redacted]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZWlj
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZWljbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOFl3U0ROnMeHSKSxJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsdDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJVDEuMCwGA1UEAwwlSHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJ
VDEuMCwGA1UEAwwlSHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBD
[redacted]
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9kSjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqiLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3dujlFuRJgSvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhRAHezyfLrvimxI0Ky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu67lliddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHBlB2HJ3DU5gE=
-----END CERTIFICATE-----
```

10.1.5 证书链配置说明

上传证书到SSL证书管理中进行统一管理时，需要单独导入证书、证书链和私钥，并需要以PEM格式进行编码。

以下将以示例方式对证书文件格式进行说明。

须知

如果您在编辑PEM文件时，将PEM文件中的任何字符编辑错误，或者在任何行的末尾添加一个或多个空格，则将导致证书、证书链或私钥无效，因此，请谨慎操作。

- 示例1：PEM编码的证书

  图 10-3 PEM 编码的证书

  ```
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  ```

- 示例2：PEM编码的证书链

  一个证书链包含一个或多个证书。您可以使用文本编辑器将您的证书文件连接成一个链。证书必须按顺序连接，以便每个证书都直接证明前一个证书。

  以下示例包含三个证书，您的证书链可能包含更多或更少。

  图 10-4 PEM 编码的证书链

  ```
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  ```

- 示例3：PEM编码的私钥（仅限私有证书）

  X.509版本3的证书使用公钥算法，因此，当您创建X.509证书或证书请求时，需要指定必须用于创建私钥-公钥对的算法和密钥位大小，并且需要将公钥放置在证书或请求中。

  同时，您需要自行保留私钥密码。在导入证书时需要私钥，此时，私钥必须是未加密的，更多详细介绍请参见**为什么要使用无密码保护的私钥？**。

  以下示例为PEM编码的RSA私钥：

  ```
  -----BEGIN RSA PRIVATE KEY-----
  Base64-encoded private key
  -----END RSA PRIVATE KEY-----
  ```

  以下示例为PEM编码的椭圆曲线私钥。根据您创建密钥的方式，可能不包括参数块。如果包含参数块，在导入过程中使用密钥之前将其删除。


```
-----BEGIN EC PARAMETERS-----
Base64-encoded parameters
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
Base64-encoded private key
-----END EC PRIVATE KEY-----
```

10.1.6 SSL 证书为什么没有在证书列表中显示?

CCM控制台的SSL证书列表会展示以下两种证书：

- 直接通过CCM控制台购买的SSL证书。
- 上传到CCM控制台进行管理的SSL证书。

除此之外，通过其它平台购买的SSL证书（包括在云市场购买的证书），都需要将证书上传至CCM控制台后，CCM才能帮您管理证书，具体的操作请参见**上传证书**。

10.1.7 吊销证书需要多长时间

DV证书在您提交证书吊销申请后，1个工作日内完成吊销。

OV、EV证书在您提交证书吊销申请后，CA中心会在1个工作日内向您的联系人邮箱（即申请该证书时提交的联系人邮箱地址）发送一封确认邮件。您需要及时登录该邮箱并确认吊销证书，当您完成邮件确认后，OV、EV证书将会吊销成功。

10.1.8 SSL 单向认证和双向认证说明

HTTPS在HTTP的基础上加入了SSL协议（Secure Sockets Layer）即“安全套接层”协议，对信息、数据加密，用来保证数据传输的安全，SSL支持单向认证和双向认证两种认证方式。

- 单向认证：客户端与服务端连接时，客户端需要验证所连接的服务端是否正确。
- 双向认证：客户端与服务端连接时，除了客户端需要验证所连接的服务器是否正确之外，服务端也需要验证接入的客户端是否正确。

应用场景

SLL单向认证适用于客户端只需验证服务端身份的场景，如网站访问这类无需在通讯层做用户身份验证，而应用逻辑层足以保障安全的情况。

SSL双向认证机制保证服务器端与客户端能互相验证对方的身份，主要目的是防止中间人攻击，确保通信的安全性和可靠性。这种机制一般使用在需要高安全性的场景中，例如银行、金融服务、物联网、企业内部服务或政府服务等涉及隐私信息，或只对特定客户端提供服务的场景中。

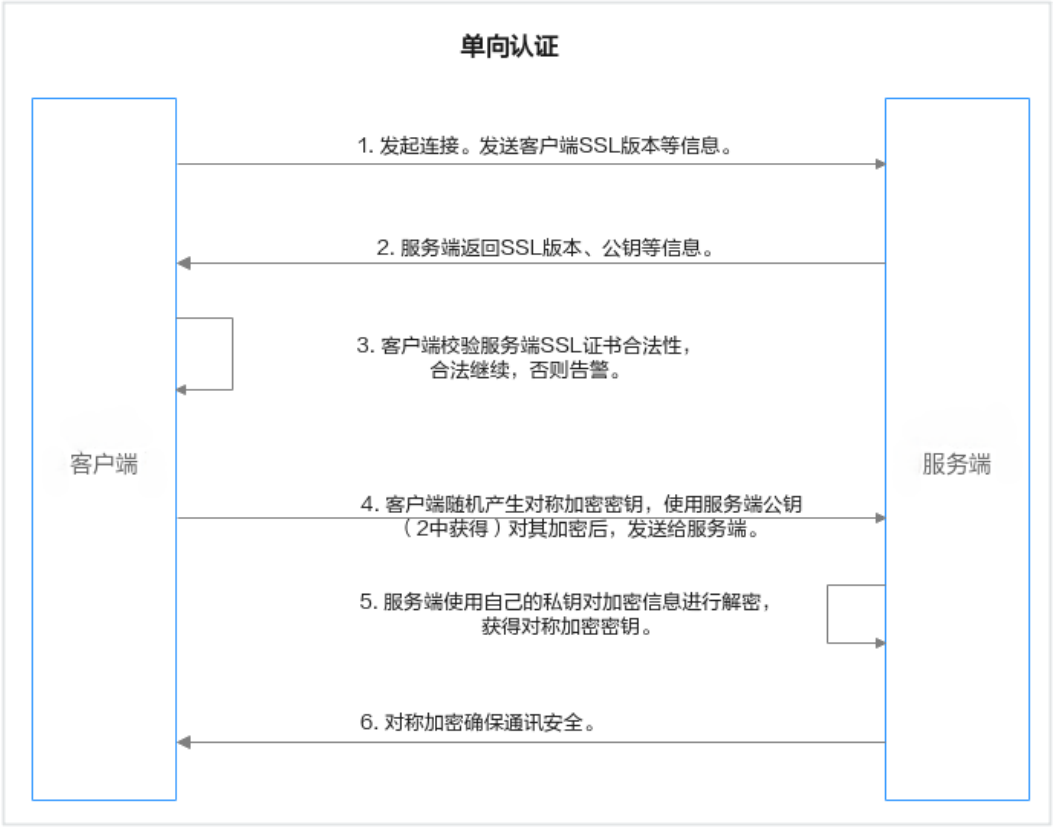
说明

弹性负载均衡 ELB 可在创建HTTPS监听器时，配置单向认证或双向认证，具体操作请参见**通过ELB部署HTTPS单向认证或双向认证**。

功能原理

- SSL单向认证

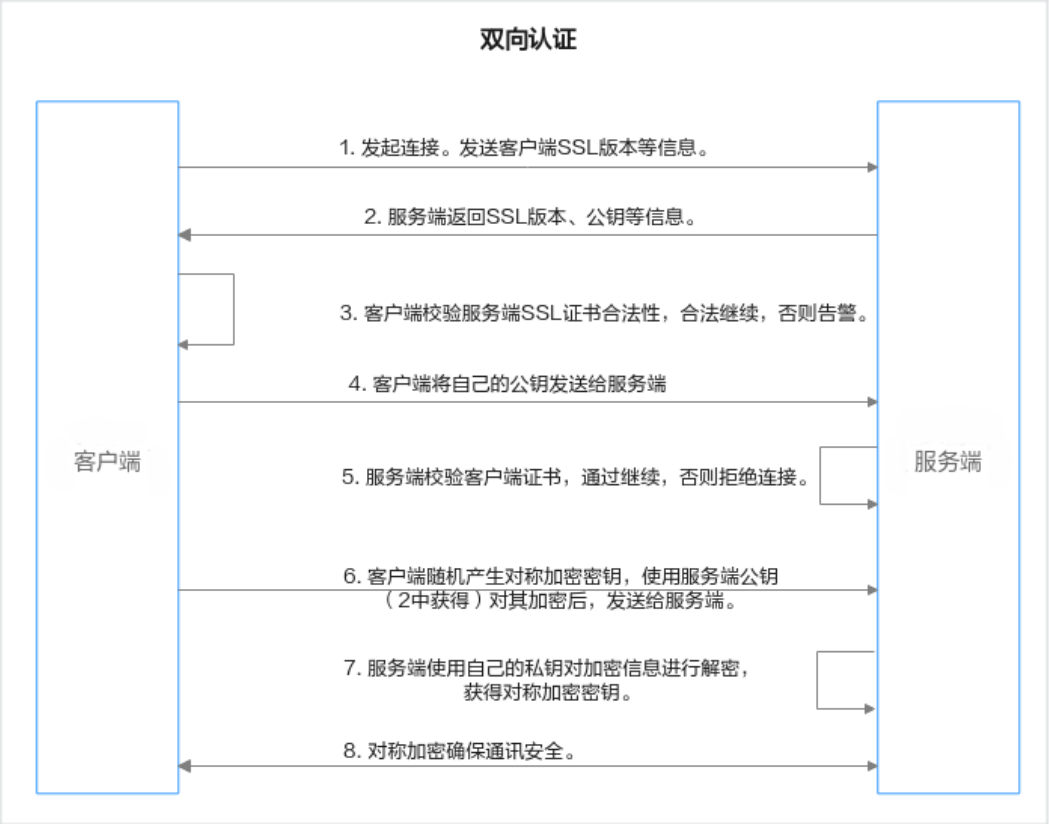
  图 10-5 单向认证



  a. 客户端向服务端发送SSL协议版本号、加密算法种类、随机数等信息。
  b. 服务端给客户端返回SSL协议版本号、加密算法种类、随机数等信息，以及服务端的证书，即公钥证书。
  c. 客户端使用服务端返回的信息验证服务端SSL证书的合法性，包括：证书是否过期、发行服务器证书的CA是否可靠、返回的公钥是否能正确解开返回证书中的数字签名、服务器证书上的域名是否和服务器的实际域名相匹配，验证通过后，将继续进行通信，否则终止通信。
  d. 客户端随机产生对称加密密钥，并用服务端的公钥（服务端的公钥从步骤2中的服务端的证书中获得）对其加密，然后发送给服务端。
  e. 服务端收到客户端发送的加密信息后，使用私钥进行解密，获取对称加密密钥。
  f. 在接下来的会话中，客户端和服务端将会使用该对称加密密钥进行通信，保证通信过程中信息的安全。

- SSL双向认证

图 10-6 双向认证



a. 客户端向服务端发送SSL协议版本号、加密算法种类、随机数等信息。
b. 服务端给客户端返回SSL协议版本号、加密算法种类、随机数等信息，以及服务端的证书，即公钥证书。
c. 客户端使用服务端返回的信息验证服务端SSL证书的合法性，包括：证书是否过期、发行服务器证书的CA是否可靠、返回的公钥是否能正确解开返回证书中的数字签名、服务器证书上的域名是否和服务器的实际域名相匹配，验证通过后，将继续进行通信，否则终止通信。
d. 服务端要求客户端发送客户端的证书，客户端将自己的证书和公钥发送至服务端。
e. 服务端验证客户端的证书，通过继续进行通信，否则断开连接。
f. 客户端随机产生对称加密密钥，并用服务端的公钥（服务端的公钥从步骤2中的服务端的证书中获得）对其加密，然后发送给服务端。
g. 服务端收到客户端发送的加密信息后，使用服务端的私钥进行解密，获取对称加密密钥。
h. 在接下来的会话中，客户端和服务端将会使用该对称加密密钥进行通信，保证通信过程中信息的安全。

10.2 问题排查定位类

10.2.1 如何增加、解绑、替换或修改 SSL 证书域名?

请根据您的实际情况选择对应的处理方式。

增加 SSL 证书绑定的域名

- 如果您购买的是**单域名**类型的SSL证书：

  需要重新购买证书。

- 如果您购买的是**多域名**类型的SSL证书：
  - 该证书有可追加附加域名的额度，则可为该证书增加附加域名。具体操作请参见**新增附加域名**。
  - 该证书没有可追加附加域名的额度，需要重新购买证书。
- 如果您购买的是**泛域名**类型的SSL证书：
  - 如果需要增加的域名与证书绑定的域名在同一级别，则无需增加该域名，直接使用即可。

    示例：证书绑定的域名为*.example.com，此次想要绑定test.example.com，则无需绑定，直接使用已有证书即可。
  - 如果需要增加的域名与证书绑定的域名不在同一级别，则需要重新购买证书。

    示例：证书绑定的域名为*.example.com，此次想要绑定abc.test.example.com，则需要重新购买证书来绑定该域名。

解绑 SSL 证书绑定的域名

- 证书未签发

  如果证书未签发，需要解绑当前证书绑定的域名并绑定新的域名，可以撤回证书申请，具体操作请参见**撤回证书申请**。

- 证书已签发

  如果您的证书在已签发后，需要解绑当前证书绑定的域名并绑定新的域名，“单域名”和“泛域名”证书可以重新签发证书，“多域名”证书不支持解绑证书绑定的域名，您需要重新购买证书。

  证书签发后，各证书品牌针对“单域名”和“泛域名”证书重新签发的时间有以下限制：

  - DigiCert品牌和GeoTrust品牌：25天。

  在规定时间内，“单域名”和“泛域名”证书可重新签发的次数不限，超过各证书品牌的规定的时间，将不能执行重新签发的操作。

  重新签发证书的具体操作请参见**重新签发**。

替换或修改 SSL 证书绑定的域名

- 证书未签发

  如果证书未签发，需要替换或修改当前证书绑定的域名，可以撤回证书申请，具体操作请参见**撤回证书申请**。

- 证书已签发

  如果您的证书在已签发后，需要替换或修改当前证书绑定的域名，“单域名”和“泛域名”证书可以重新签发证书，“多域名”证书不支持替换或修改证书绑定的域名，您需要重新购买证书。

  证书签发后，各证书品牌针对“单域名”和“泛域名”证书重新签发的时间有以下限制：

  - DigiCert品牌和GeoTrust品牌：25天。

在规定时间内，“单域名”和“泛域名”证书可重新签发的次数不限，超过各证书品牌的规定的时间，将不能执行重新签发的操作。

重新签发证书的具体操作请参见**重新签发**。

10.2.2 内网域名可以申请 SSL 证书吗?

内网域名不能申请公网数字证书。

如果您需要在内网使用证书，建议您申请私有证书，更多关于私有证书的信息请参考**申请私有证书**。

10.2.3 如何解决 SSL 证书链不完整?

如果证书机构提供的证书在用户平台内置信任库中查询不到，且证书链中没有颁发机构，则证明该证书是不完整的证书。使用不完整的证书，当用户访问防护域名对应的浏览器时，因不受信任而不能正常访问防护域名对应的浏览器。

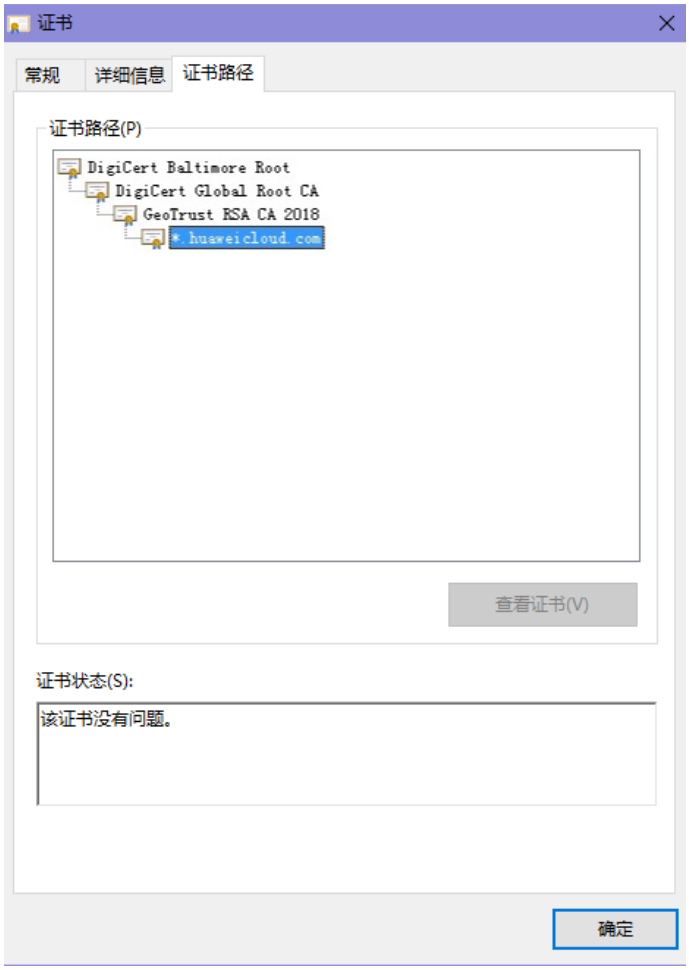
可通过手动构造完整证书链解决此问题。Chrome最新版本一般是支持自动验证信任链，以华为的证书为例，手工构造完整的证书链步骤如下：

步骤1 **查看证书**。单击浏览器前的锁，可查看证书状况，如**图10-7**所示。

图 10-7 查看证书

步骤2 **查看证书链**。单击“证书”，并选中“证书路径”页签，可单击证书名称查看证书状态，如**图10-8**所示。

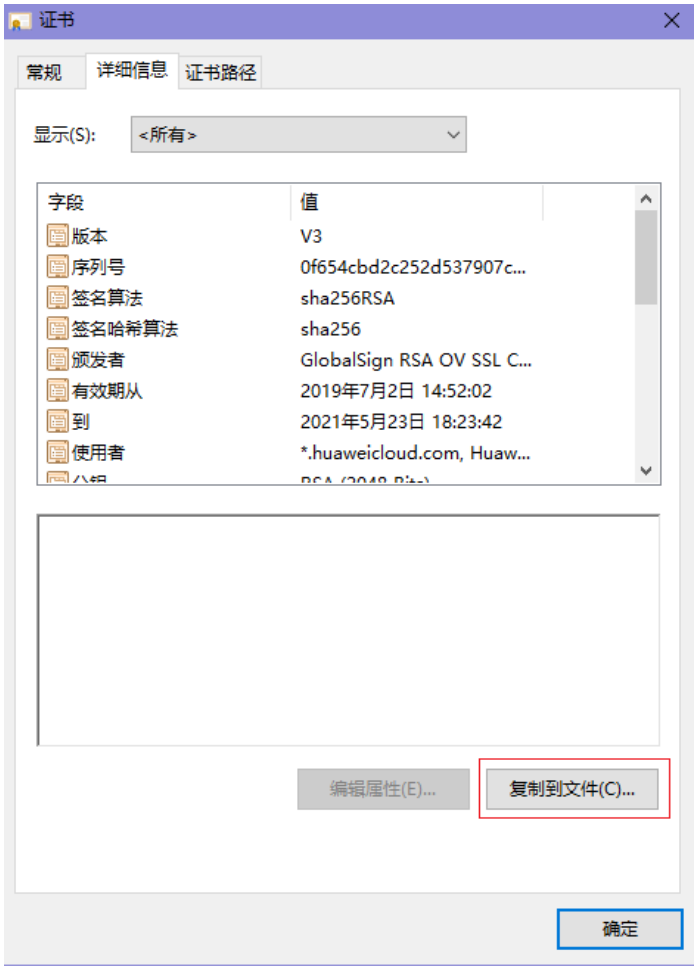
图 10-8 查看证书链



步骤3 逐一将证书另存到本地。

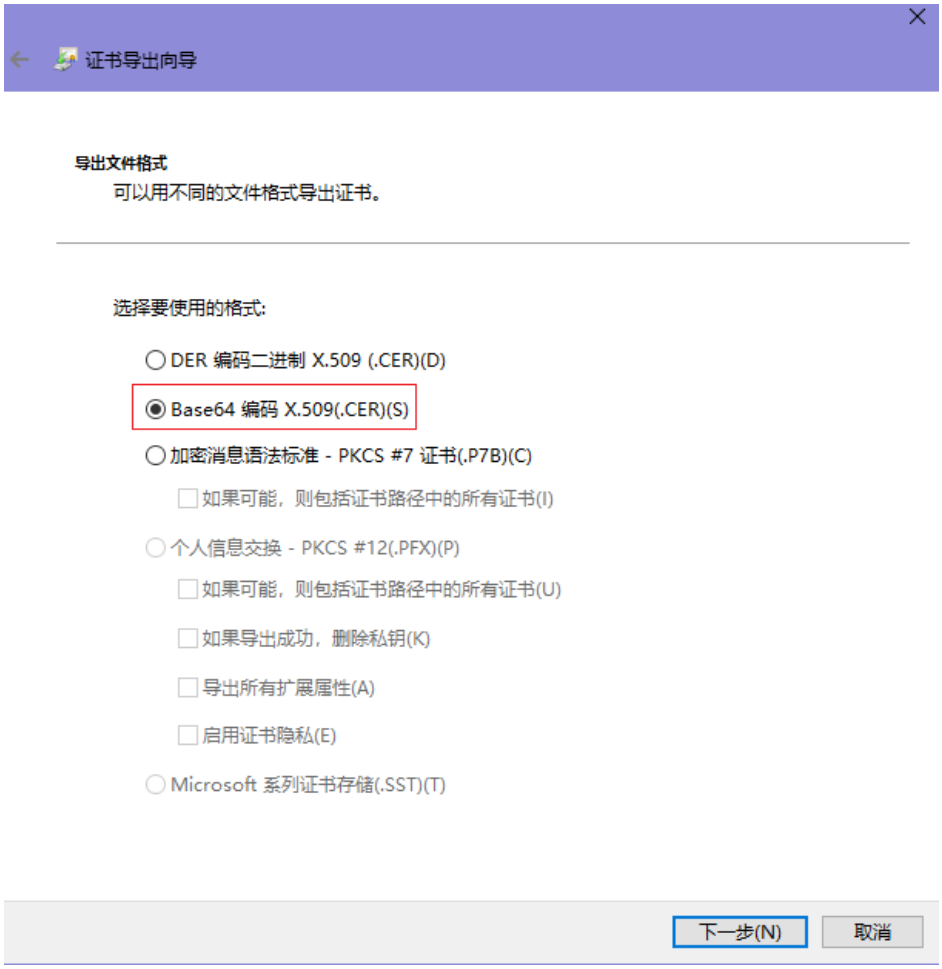
1. 选中证书名称，单击“详细信息”页签，如图10-9所示。

图 10-9 详细信息



2. 单击“复制到文件”，按照界面提示，单击“下一步”。
3. 选择“Base64编码”，单击“下一步”，如**图10-10**所示。

图 10-10 证书导出向导



步骤4 证书重构。证书全部导出到本地后，用记事本打开证书文件，按图10-11重组证书顺序，完成证书重构。

图 10-11 证书重构

步骤5 重新上传证书。

----结束

10.3 私有证书使用类

10.3.1 私有证书签发后，能否停用私有 CA?

您可以根据实际情况选择以下方法停用私有CA的部分功能或者停用私有CA：

- 如果您不再需要使用某个私有CA来签发证书，但需要保留其吊销证书和签发证书吊销列表的功能，您可以禁用该私有CA。禁用私有CA后，其下所有证书使用不受影响。禁用私有CA详细操作请参见**禁用私有CA**。

  ⚠ 注意

  私有CA禁用期间也将持续计费。

- 如果您不再需要使用某个私有CA，您可以删除该私有CA。删除私有CA后，将不再计费，其下已经导出的证书（未被吊销）仍可使用，但该私有CA下的所有证书都将无法执行“吊销”操作，无法再更新证书吊销列表，并且该私有CA和其子CA下所有私有证书将无法执行“导出”操作。删除私有CA详细操作请参见**计划删除私有CA**。