云证书管理服务

SSL 证书用户指南

文档版本 36

发布日期 2024-12-17

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。

目 录

1 SSL 证书使用概述

华为云SSL证书提供多个品牌和类型的证书，详情请参见**各证书之间的区别**。本文档介绍如何购买和使用华为云SSL证书。

您的网站使用SSL证书后，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。

相关流程如**图 证书使用流程**所示，具体说明如**表 证书使用流程说明**所示。

图 1-1 证书使用流程

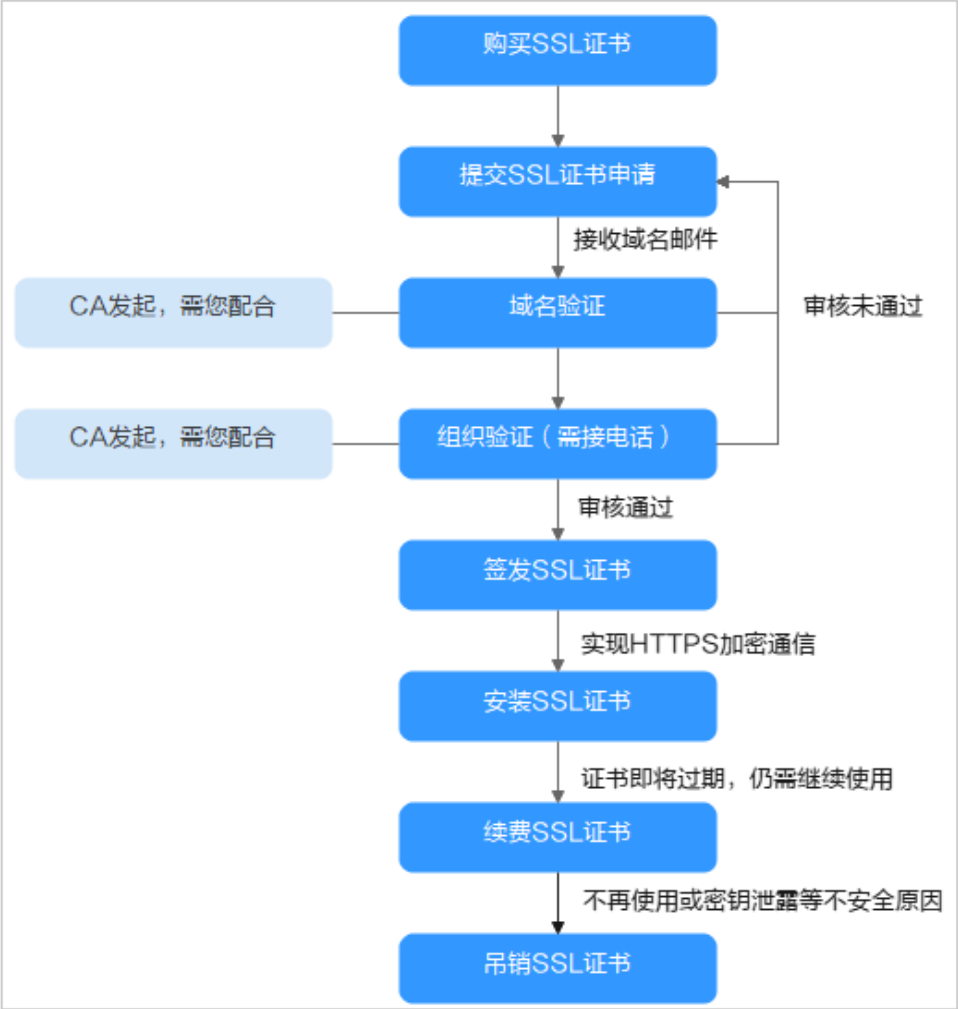


表 1-1 证书使用流程说明

步骤	操作	说明
1	**购买SSL证书**	在SSL证书管理平台，根据您的域名类型选购对应的证书。 各类型证书之间的区别以及选择请参见**各类型SSL证书之间的区别**、**如何选择SSL证书?** 。
2	**提交SSL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。
3	**域名验证**	按照CA中心的规范，证书提交申请后您需要配合完成域名授权验证来证明您对所申请绑定域名的所有权。 SCM提供有以下几种验证方式： • 自动DNS验证：符合**条件**的证书可选。 • 手动DNS验证：所有类型证书均可选。 • 邮箱验证：仅OV、EV型证书可选。 • 文件验证：仅IP证书支持。

步骤	操作	说明
4	**组织验证（OV、EV）**	仅当申请OV、OV Pro、EV和EV Pro类型证书时，需要该操作。 域名验证完成后，CA机构需要确认企业/组织是否发起了此次的证书订单申请。
5	**签发SSL证书**	验证完成后，CA机构还需要一段时间进行处理，请您耐心等待。具体申请时间请参见**各证书的申请时长**。 CA机构审核通过后，将签发证书。证书自签发之时开始生效，有效期为1年。
6	**安装SSL证书**	证书签发后，您可以一键部署证书到华为云其他云产品或下载证书并安装到服务器上进行使用。 ● 将证书部署到其他云产品后，将帮助您提升对应云产品访问数据的安全性。 ● SSL证书安装到Web服务器后，您的Web服务器才能实现HTTPS加密通信，实现通信安全。
7	**续费SSL证书**	自2020年9月1日起，全球CA机构颁发的SSL证书有效期最长为一年，证书到期后将不再被浏览器信任，建议您提前开通自动续费或在证书即将到期前三十天进行手动续费，避免因证书过期对您的业务产生影响。 SSL证书续费操作相当于重新申请了一张与原证书规格（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。证书续费后，您需要将续费签发的新证书重新安装到您的Web服务器或部署到华为云其他云产品，替换即将过期的旧证书。
8	**吊销SSL证书**	如果您不再需要某张已签发的SSL证书或某张SSL证书密钥丢失或出于其他安全因素考虑，可以在SSL证书管理控制台申请吊销证书。 吊销证书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。

2 购买 SSL 证书

华为云云证书管理服务提供多个品牌和类型的证书，您可以根据需求购买SSL证书。

前提条件

购买证书的账号拥有“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

特殊企业不支持申请OV、EV类型的证书。例如：军队、政府的一些特殊机构、国家保密单位等。

原因：全国组织机构统一社会信用代码公示查询平台无法在查询到特殊企业的相关信息，因而无法完成组织身份验证，所以特殊企业无法使用OV、EV类型的SSL证书。

操作步骤

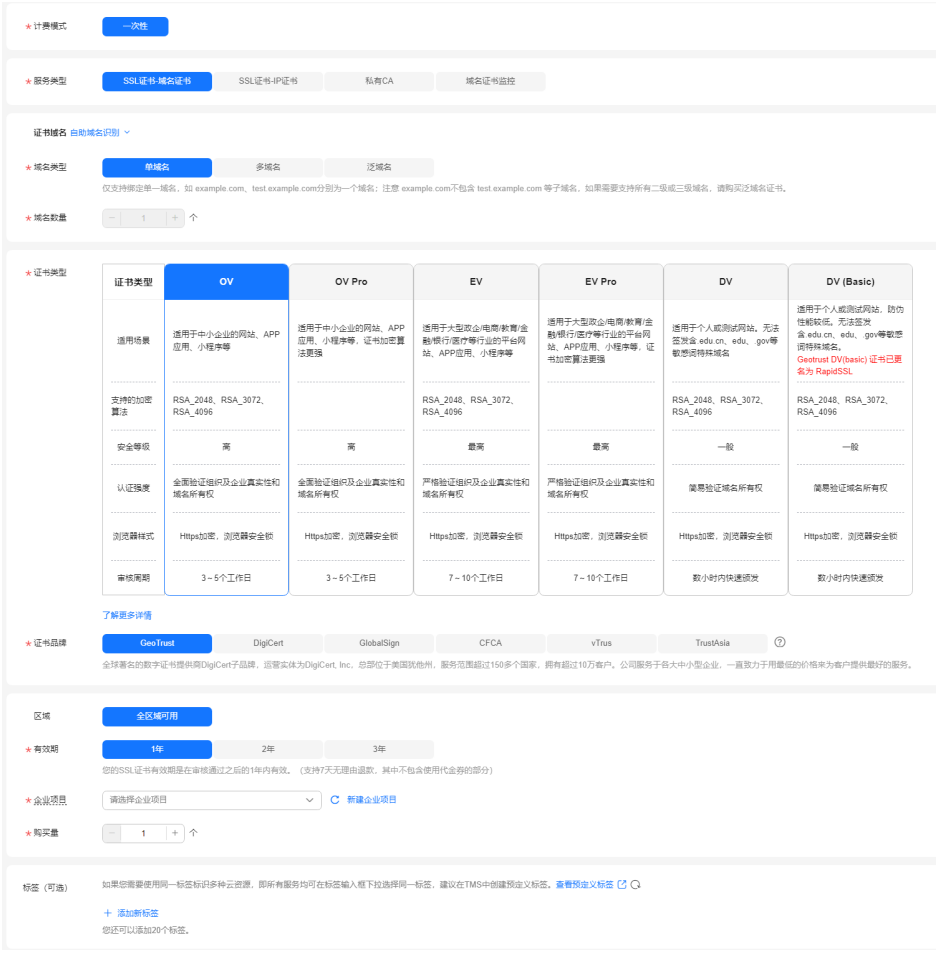
步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在购买证书页面，选择“服务类型”、“域名类型”、“域名数量”、“证书类型”、“证书品牌”、“有效期”、“企业项目”、“购买量”，“标签”如**图 证书选型**所示。

图 2-1 证书选型



1. 选择“服务类型”：

   证书服务类型，支持购买“域名证书”和“IP证书”两类证书。

   说明

   当您服务类型选择IP证书时，只需在购买证书页面再另行选择“有效期”、“企业项目”和“购买量”即可，其余项均为默认，无需配置。

2. 选择“域名类型”：

   域名的类型，域名证书支持“单域名”、“多域名”和“泛域名”。具体参数说明如**表 域名类型**所示。

   表 2-1 域名类型

域名类型	说明
单域名	即单个SSL证书只支持绑定1个单域名。例如，example.com

域名类型	说明
多域名	即单个SSL证书可以同时绑定多个域名。 – 最多可以支持250个域名。 – 仅当证书类型为OV、OV Pro时，多个域名中可包含泛域名。其他类型的证书，仅支持绑定多个单域名。 – 多个域名可以分批次绑定。例如，购买多域名类型证书，域名数量为3的场景，首次申请证书时仅填写了2个域名，证书签发后可再追加填写1个域名。 – 当购买多域名类型证书，域名数量为3的场景，仅支持绑定3个域名。如果后续还需添加，则需要重新购买证书。
泛域名	即单个SSL证书支持绑定一个且只有一个泛域名。*.*.example.com多个通配符的泛域名不支持。 泛域名只允许添加一个通配符域名，例如*.example.com（包含a.example.com、b.example.com、.....，但是不包含a.a.example.com）。
更多关于如何选择域名类型，详情请参见**如何选择域名类型?**	

3. 设置“域名数量”：
   – “域名类型”选择“单域名”和“泛域名”时，域名数量限制为1个。
   – “域名类型”选择“多域名”时，域名数量范围为“2~250”。域名数量须满足以下条件：
     - **主域名**数量固定为1个。
     - **附加单域名**数量≥1个（当证书类型为OV、OV Pro时，**附加单域名**数量+**附加泛域名**数量≥1）。

   图 2-2 域名类型

   须知

   GeoTrust品牌的域名数量范围为“5~250”，其中，单域名数量需≥5个。

4. 选择“证书类型”：
   域名证书可选择的证书类型以及区别如**表 证书类型**所示，请根据您的需要进行选择。

表 2-2 证书类型

证书类型	典型应用场景	认证强度	安全等级	审核周期
EV Pro	证书加密算法更强，适用于大型政企/电商/教育/金融/银行/医疗等行业的平台网站、APP应用、小程序等。	严格验证组织及企业真实性和域名所有权	最高	7～10个**工作日**
EV	适用于大型政企/电商/教育/金融/银行/医疗等行业的平台网站、APP应用、小程序等	严格验证组织及企业真实性和域名所有权	最高	7～10个**工作日**
OV Pro	证书加密算法更强，适用于中小企业的网站、APP应用、小程序等	验证组织及企业真实性和域名所有权	高	3～5个**工作日**
OV	适用于中小企业的网站、APP应用、小程序等	验证组织及企业真实性和域名所有权	高	3～5个**工作日**
DV、DV（Basic）	适用于个人网站、企业测试	简易验证域名所有权	一般	数小时内快速颁发
更多关于证书类型的区别，请参见**各证书之间的区别**。				

5. 选择“证书品牌”：

   当前支持的品牌包括“GeoTrust”、“DigiCert”、“GlobalSign”、“CFCA（国产）”、“TrustAsia（国产）”和“vTrus（国产）”。关于证书类型的区别，请参见**各证书之间的区别**。

   说明

   Digicert、Geotrust证书于2024年12月1日起将使用Digicert Global Root G2根签发，相关证书链变化，请参见**【2024年10月28日】关于DigiCert品牌根证书的切换公告**。

6. 选择“有效期”：

   自2020年09月01日起，全球所有CA中心签发的SSL证书的有效期为1年，华为云云证书管理服务提供购买多年期（2年-3年）证书的解决方案，满足您1次下单即可完成2年、3年证书服务购买操作的需求，不同有效期的区别说明如**表 有效期说明**所示。您可以在SSL证书列表查看您购买的多年期证书剩余年数。

   证书有效期从证书**最终签发的时间**开始计算，到期后，需要重新购买并完成证书申请流程。

   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邮件通知，您收到邮件通知后请提前**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。

⚠ 注意

- 多年期（2年-3年）证书续期过程中，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**，CA机构会向您首次申请证书时填写的邮箱发送一封验证邮件告知您具体的验证事宜，收到邮件后请您尽快完成相关验证操作，避免因延误而导致上一张证书已过期，新证书还未签发，让您的网站处于不安全的状态。
- 为了避免多年期证书自动申请失败，**请勿取消隐私授权**。

表 2-3 有效期说明

有效期	生效说明
1年	CA机构签发的SSL证书默认有效期为1年。
2年	- 有效期为“2年”的证书实际包含2张有效期为1年且规格相同的SSL证书。在第一张证书到期前30天，系统自动以您第一张证书的信息为您申请第二张证书。您需要及时完成域名或组织验证，避免影响第二张证书的及时签发。 - 第二张证书签发后，您需要手动将第二张证书安装到您的Web服务器或部署到华为云产品，替换旧证书。详细操作请参考**安装SSL证书**。 如果您未安装或未部署第二张证书，则在第一张证书过期后，您的服务器或华为云产品将无法正常使用HTTPS服务。 - 原证书未用完的时间会**自动补齐**到新证书里面。
3年	- 有效期为“3年”的证书实际包含3张有效期为1年且规格相同的SSL证书。在第一张证书到期前30天，系统自动以您第一张证书的信息为您申请第二张证书，在第二张证书到期前30天，系统自动以您第一张证书的信息为您申请第三张证书。您需要及时完成域名或组织验证，避免影响第二或第三张证书的及时签发。 - 第二或第三张证书签发后，您需要手动将第二或第三张证书安装到您的Web服务器或部署到华为云产品，替换旧证书。详细操作请参考**安装SSL证书**。 如果您未安装或未部署第二或第三张证书，则在第一或第二张证书过期后，您的服务器或华为云产品将无法正常使用HTTPS服务。 - 原证书未用完的时间会**自动补齐**到新证书里面。

7. 在“企业项目”下拉列表中选择您所在的企业项目。

   企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。

   如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

   说明

   “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。

8. 设置“购买量”：设置购买的证书个数。
9. （可选）设置“标签”：为当前购买的证书添加新标签，关于标签设置详情，请参见**创建标签**。

步骤5 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6 若购买GeoTrust和DigiCert品牌的证书，系统将弹出提示框，请仔细阅读提示内容后，单击“确定”。

步骤7 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8 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

后续处理

成功购买SSL证书后，您需要申请证书，即为证书绑定域名或IP、填写证书申请人的详细信息并提交审核。所有信息通过审核后，证书颁发机构才签发证书，更多详细操作请参考**提交SSL证书申请**。

3 申请 SSL 证书

3.1 提交 SSL 证书申请

成功购买证书后，您需要申请证书，即为证书绑定域名或IP、填写证书申请人的详细信息并提交审核。所有信息通过审核后，证书颁发机构才签发证书。

本章节将介绍申请证书的详细操作。

前提条件

已购买SSL证书且状态为“待申请”，购买证书详细操作请参见**购买SSL证书**。

约束限制

- 绑定域名时，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，再使用编码后信息来申请证书。
- 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**。
- 由于各个证书品牌针对www型域名有不同的惠赠活动，具体请参见**证书品牌**。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，并在SSL证书列表待申请证书所在行的“操作”列，单击“申请证书”，系统从右面弹出申请证书详细页面。

- 提交付费证书申请，请单击“SSL证书”页签，选择待申请的证书进行提交。
- 提交测试证书申请，请单击“测试证书”页签，选择待申请的证书进行提交。

步骤4 在弹出申请证书详细页面中，填写域名、企业组织和申请人等信息。

图 3-1 域名及其他信息

1. **证书请求文件**

   证书请求文件（Certificate Signing Request，CSR）即证书签名申请，包含了您的服务器信息和公司信息。申请证书时需要将您证书的CSR文件提交给CA认证中心审核。

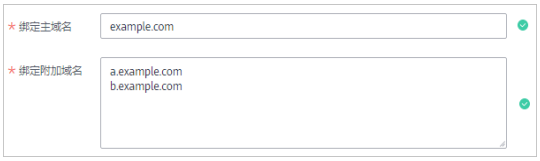
   选择证书请求文件生成方式：

   - 系统生成CSR（**推荐**）：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。
   - 选择已有CSR：手动选择您在CSR管理列表已创建或已上传的CSR文件，创建CSR的详细操作请参见**创建CSR**，上传CSR的详细操作请参见**上传CSR**。
   - 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?** 。

   两种证书请求文件的区别请参见**系统生成的CSR和自己生成CSR的区别?** 。

2. **绑定域名或IP**
   - 当“证书请求文件”选择“自己生成CSR”时，域名将根据CSR文件自动解析出来，不需要手动输入域名或IP。
   - 当“证书请求文件”选择“系统生成CSR”时，需要手动输入证书需要绑定的域名或IP。

表 3-1 绑定域名或 IP

类型	填写说明
单域名	填写需要绑定的1个域名。 例如，需要绑定域名为example.com，则填写如下图所示： 
单IP	填写需要绑定的1个公网IP。 例如，需要绑定的域名为192.168.1.1，则填写如下图所示： 
多域名	需要绑定**主域名**和**附加域名**。 例如，需要绑定域名为example.com、a.example.com和b.example.com，则填写如下图所示：  **说明** ■ 附加域名须**大于等于1个**。附加域名可分批次进行录入，具体操作请参见**新增附加域名**。 ■ 多个附加域名请换行输入。 ■ 如果购买的是组合证书（单域名+泛域名），**主域名同时支持绑定单域名和泛域名**。 ■ 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。 ■ 仅当证书类型为OV、OV Pro时，多个域名中可包含泛域名。其他类型的证书，仅支持绑定多个单域名。
泛域名	填写需要绑定的1个泛域名。 例如，需要绑定域名为*.example.com，则填写如下图所示： 

类型	填写说明
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**	

3. **密钥算法**

   选择待申请证书的加密算法，加密算法默认为“RSA_2048”。可选择的加密算法类型：

   - **RSA**：目前在全球应用广泛的非对称加密算法，兼容性在三种算法中最好，支持主流浏览器和全平台操作系统。一般采用2048位或3072位的加密长度。
   - **ECC**：椭圆曲线加密算法。相比于RSA，ECC加密速度快、效率更高、服务器资源消耗低，目前已在主流浏览器中得到推广，成为新一代主流算法。一般采用256位加密长度。
   - **SM2**：中国国家密码管理局发布的ECC椭圆曲线加密算法，在中国商用密码体系中用来替代RSA算法。

   各类证书支持的加密算法详情请参见**证书支持的加密算法**。

   须知

   申请国密证书时，加密算法请选择“SM2”。

4. **企业组织信息**

   请根据界面提示填写您的企业组织信息。

   说明

   - 仅OV、EV类型的证书需要填写此项。
   - 公司名称请填写营业执照注册公司的全称。

5. **申请人信息**
   - 请确保此处填写的申请人电话和邮箱填写准确，CA机构人员会在审核过程中通过邮箱和电话联系您。
   - 申请人信息涉及用户个人信息的内容，证书签发后**不会**包含在证书中。

6. **技术联系人信息**

   此项信息为选填项，如填写，请确保填写的技术联系人姓名、电话和邮箱信息准确。

步骤5 确认填写信息无误后，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勾选框。

步骤6 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**。

----结束

后续处理

- 补充申请资料
  - CFCA品牌的证书提交证书申请后，CFCA机构将在1-2个工作日内给您提交申请时填写的邮箱发送一封邮件要求您提供盖**公司公章**的CFCA证书申请表（确保控制台申请信息与申请表申请信息一致）、营业执照复印件和经办人身份证复印件进行组织身份验证。请您按照要求提供相关资料。
  - vTrus品牌的国际标准（RSA）证书提交证书申请后，vTrus机构将在1-2个工作日内给您提交申请时填写的邮箱发送一封邮件要求您提供盖**公司公章**或**部门章**的授权函、经办人身份证复印件进行组织身份验证。请您按照要求提供相关资料。
- 提交审核后，CA颁发机构将在2-3个工作日内对您提交的申请进行处理并给您填写的邮箱发送一封验证邮件。

  您需要按照要求进行域名验证。具体操作请参见**域名验证**。
- 如果已提交了证书申请，发现信息填写错误，可撤销申请，修改信息后重新提交证书申请，撤回申请具体操作请参见**撤回证书申请**。

3.2 域名验证

3.2.1 域名验证概述

证书提交申请后，您需要进行域名授权验证。按照CA中心的规范，如果您申请了SSL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。

如果不完成域名验证，您的证书将无法通过审核，且您的证书申请将会一直显示“待完成域名验证”的状态。

华为云SSL证书管理提供以下几种方式，根据您申请证书时，选择的验证方式进行操作：

表 3-2 域名验证方式

验证方式	说明	适用场景
自动DNS验证	指您授权SCM服务修改域名的DNS解析记录，自动在解析记录中添加一条用于验证记录，无需您手动修改域名解析记录。	• 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**（Domain Name Service）； 以上条件必须**全部满足**系统才会进行自动DNS验证。

验证方式	说明	适用场景
手动DNS验证	指您需要在域名的DNS解析服务商手动修改域名的DNS解析记录，在解析记录中添加一条用于验证的记录。	• 您有权限修改域名的DNS解析设置（即拥有域名管理权限）； • 申请证书时，域名验证方式选择了手动DNS验证（DV型证书无需此项）。
邮箱验证	即您登录域名管理员邮箱，接收域名确认邮件并回复CA机构发送的域名确认邮件。	您有权限登录域名管理员邮箱（即拥有域名管理权限）。
文件验证	指由您手动从SCM控制台获取证书验证文件，然后在服务器的网站根目录下创建指定文件。	• 购买的是IP证书 • 您有权限向网站所在服务器的根目录写入内容（即拥有服务器管理权限）。 • 服务器开放了80或443端口，支持监听HTTP、HTTPS访问。 **注意** 目前CA机构仅支持向80或443端口发起认证请求。如果您的服务器未开放80或443端口，则请勿使用文件验证方式。

3.2.2 方式一：自动 DNS 验证（DV 证书）

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

自动DNS验证是指授权SCM服务修改域名的DNS解析记录，自动在解析记录中添加一条用于验证的记录，无需您手动修改域名解析记录。CA机构添加的记录能被解析，则表示验证通过。

本章节将介绍如何进行自动DNS验证。

约束与限制

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

操作步骤

如果您在申请证书时域名验证方式选择了自动DNS验证，则无需您进行任何操作。

请您耐心等待系统进行自动DNS验证。DNS验证完成后，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。

3.2.3 方式二：手动 DNS 验证

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

手动DNS验证，是指您需要在域名的DNS解析服务商手动修改域名的DNS解析记录，在解析记录中添加一条用于验证的记录。CA机构验证添加的记录能被解析，则表示验证通过。

如果您在申请证书时域名验证方式选择了手动DNS验证，请参照本章节进行处理。

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。

前提条件

绑定的域名须做实名认证，如果未做实名认证，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. 请参见**怎样把域名从其他服务商迁移到华为云DNS?**，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**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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3-2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 3-2 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 登录管理控制台。

步骤2 单击页面左上方的 ☰，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。

说明

- 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 3-3 添加记录集

表 3-3 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。

说明

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 3-4 验证命令

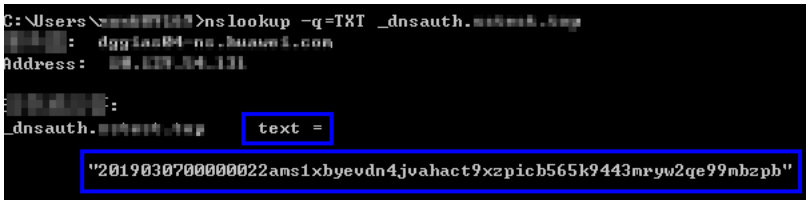
记录类型	验证命令
TXT	**nslookup -q=TXT** *xxx*
CNAME	**nslookup -q=CNAME** *xxx*

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3-4所示，说明域名授权验证配置已经生效。

  图 3-4 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。

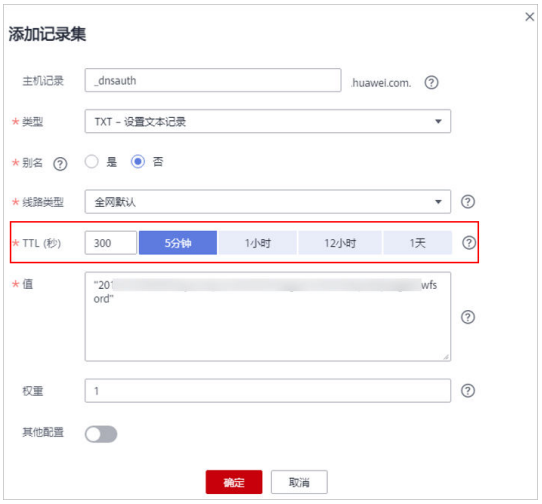
  图 3-5 域名授权验证配置未生效

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 3-5 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。

可能原因	处理方法
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 3-6** 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 3-7** 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**管理控制台**。

  b. 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

  c. 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。

  d. 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。

3.2.4 方式三：文件验证（IP 证书&DV 证书）

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

文件验证，是指您手动从SCM控制台获取证书验证文件，然后在服务器的网站根目录下创建指定文件。CA机构验证文件路径可以被访问，则表示验证通过。

如果您购买的IP证书或DV证书，您需要完成文件验证，请参照本章节进行处理。

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IP证书和DV证书支持文件验证。
- 泛域名证书不支持文件验证。

步骤一：获取验证信息

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 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 3-8 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。

   说明

   此处以GeoTrust证书颁发机构返回“fileauth.txt”为例进行说明，请以您CA机构实际返回的文件名为准。

echo off>fileauth.txt

5. 执行以下命令，打开“fileauth.txt”文件。

   start fileauth.txt

6. 将步骤4中的记录值放在“fileauth.txt”文件内，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

3.2.5 方式四：邮箱验证

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

邮箱验证，是指您登录域名管理员邮箱，接收域名确认邮件并回复CA机构发送的域名确认邮件。CA机构验证邮件由域名管理员邮箱回复认证信息，则表示验证通过。

如果您在申请证书时域名验证方式选择了邮箱验证，请参照本章节进行处理。

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。

说明

CA机构发送域名确认邮件需要大约一个工作日。如您短时间内未收到域名确认邮件，请耐心等待。如一个工作日后仍未收到邮件，请检查域名管理员邮箱正确性。

- 预留域名管理员邮箱地址配置错误：需要您撤回当前SSL证书申请，并重新配置邮箱地址信息，具体操作请参见**撤回SSL证书申请**，是否撤回成功以华为云SSL证书列表呈现最终状态为准。
- 预留域名管理员邮箱地址配置无误：一个工作日后仍未收到邮件，请您提工单联系我们，并在工单中进行描述。

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

3.3 组织验证（OV、EV）

申请OV、OV Pro、EV和EV Pro类型证书时，域名验证完成后，CA机构将向您填写的邮箱发送一封组织验证邮件。CA机构将根据您选择的验证方式与企业/组织进行联系，确认企业/组织是否发起了此次的证书订单申请。

须知

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

前提条件

证书的状态为“待完成组织验证”。

约束与限制

申请OV、OV Pro、EV和EV Pro四种类型的证书需要完成组织验证。

操作步骤

步骤1 请登录您在申请证书时填写的联系人邮箱。

步骤2 打开来自CA机构的组织验证邮件。

步骤3 回复CA机构的邮件以选择组织验证方式。

组织验证包括电话、企业邮箱、律师函方式等，其中律师函方式需要额外收费500元。请根据您的实际情况进行选择。

如果需要更改组织验证方式，请直接回复CA中心的邮件。

步骤4 请您留意所选择的验证方式，配合CA机构进行处理。

例如，您选择的组织验证方式为电话验证，则CA机构将通过企业/组织的公开电话与您联系，请您留意并及时进行处理。

----结束

3.4 签发 SSL 证书

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

- DV型证书在确认完成DNS验证且验证结果无误后，请您耐心等待，CA机构将还需要一段时间进行处理。CA机构审核通过后，将会签发证书。
- OV、EV型证书在确认完成组织验证后，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。

不同的SSL证书类型审核周期有所区别，一般情况下，各证书类型的审核周期说明如**表3-6**所示。

表 3-6 证书审核周期

证书类型	审核周期
EV	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**。
OV	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**。
DV	无人工审核。 CA机构签发系统自动检查域名授权配置，DNS配置正确的情况下（需要您自行排查DNS配置是否正确）可在数小时内快速颁发。

操作步骤

CA机构审核通过后，将会签发证书，证书签发后便立即生效。

证书签发后，可一键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。

部署证书操作请参见**部署证书到云产品**。

下载证书操作请参见**下载证书**。

4 安装 SSL 证书

4.1 安装国际标准 SSL 证书到 Web 服务器

4.1.1 下载 SSL 证书

SSL证书签发后，需要将SSL证书下载到本地。下载后，还需要将已下载的证书上传到Web服务器并修改服务器的相关配置，才能使SSL证书生效。

该任务介绍如何在SSL证书管理平台下载证书。

前提条件

“证书状态”为“已签发”或“托管中”。

约束条件

- 仅支持在证书有效期内，不限次数的下载证书，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。
- “证书请求文件”选择的是“系统生成CSR”，下载的文件包含了“Apache”、“IIS”、“Nginx”、“Tomcat”4个文件夹和1个“domain.csr”文件。
- “证书请求文件”选择的是“自己生成CSR”，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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要下载的证书所在行的“操作”列，单击“下载”，如图4-1所示。

图 4-1 下载证书

步骤5 在证书详情页面，确认证书信息无误后，单击“下载证书”。

步骤6 证书下载后，需要安装到对应的服务器上，才能使SSL证书生效。

不同Web服务器安装SSL证书的具体操作不同，以下介绍了几种在主流Web服务器上安装SSL证书的方法，请根据您的需要进行选择：

- **在Tomcat服务器上安装SSL证书**
- **在Nginx服务器上安装SSL证书**
- **在Apache服务器上安装SSL证书**
- **在IIS服务器上安装SSL证书**
- **在Weblogic服务器上安装SSL证书**
- **在Resin服务器上安装SSL证书**

----结束

下载的证书文件说明

下载文件说明：根据申请证书时，选择的“证书请求文件”方式的不同，下载文件也有所不同。

- 申请证书时，如果“证书请求文件”选择的是“系统生成CSR”，则下载文件说明如下：

  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4-2所示，具体文件说明如表4-1所示。

图 4-2 解压 SSL 证书

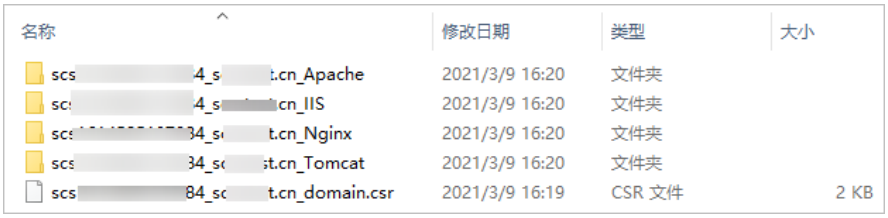


表 4-1 下载文件说明

文件夹/文件名称	文件夹内容
Tomcat	keystorePass.txt：证书密码。 server.jks：证书文件。
Nginx	server.crt：证书文件，包含两段证书代码，分别为服务器证书和CA中间证书。 server.key：证书私钥文件，包含一段证书私钥代码。

文件夹/文件名称	文件夹内容
Apache	ca.crt：证书链文件，包含一段中级CA代码。 server.crt：证书文件，包含一段服务器证书代码。 server.key：证书私钥文件，包含一段证书私钥代码。
IIS	keystorePass.txt：证书密码。 server.pfx：证书文件。
domain.csr	证书请求文件。

- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，则下载文件说明如下：

  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。在各个服务器上安装证书时，需要填写对应私钥的位置。

  说明

  “自己生成CSR”的证书不支持一键部署到云产品。

4.1.2 下载根证书

如果您的业务用户通过浏览器访问您的web业务，您下载并安装SSl证书即可，SSL证书文件中已包含相应的根证书，无需再单独配置。

如果您的业务用户通过Java等客户端访问您的web业务，您需要下载根证书并手动安装到对应的客户端，保证客户端能够校验您web服务器的加密信息。例如，如果您的web服务器安装了GeoTrust EV型SSL证书，则对应的客户端需要安装GeoTrust EV型根证书，才能保证您业务用户能通过客户端访问您的web业务。

约束条件

您的业务用户通过Java等客户端访问您的web业务。

下载地址

目前仅支持下载部分品牌和证书类型的根证书，具体的下载地址如下：

- DigiCert-DV-TLS-CA-G1
- DigiCert-EV-root
- DigiCert-OV-DV-root
- GeoTrust-CN-RSA-CA-G1
- GeoTrust-EV-CN-RSA-G1
- GlobalSign-R3-root
- DigiCert Global Root G2

- DigiCert Global RootCA

4.1.3 在 Tomcat 服务器上安装 SSL 证书

本文以Linux操作系统中的Tomcat7服务器为例介绍SSL证书的安装步骤，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。
- 已安装OpenSSL工具。

  您可以从“https://www.openssl.org/source/”下载最新的OpenSSL工具安装包（要求OpenSSL版本必须是1.0.1g或以上版本）。
- 已安装Keytool工具。

  Keytool工具一般包含在Java Development Kit（JDK）工具包中。
- 待安装证书为国际标准证书。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。

操作步骤

在Tomcat7服务器上安装SSL证书的流程如下所示：

①获取文件 → **②创建目录** → **③修改配置文件** → **④重启Tomcat** → **⑤效果验证**

步骤一：获取文件

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**。

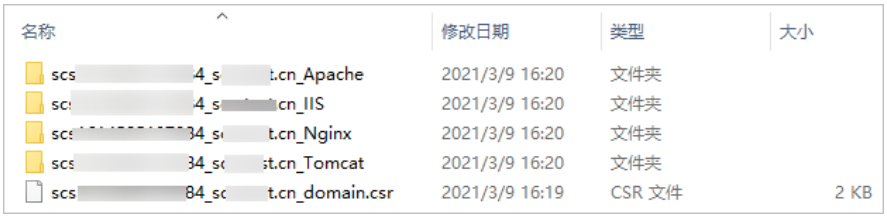
具体操作如下：

- **系统生成CSR**

  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4-3所示。

  图 4-3 本地解压 SSL 证书

  b. 从“*证书ID_证书绑定的域名*_Tomcat”文件夹内获得证书文件“*证书ID_证书绑定的域名*_server.jks”和密码文件“*证书ID_证书绑定的域名*_keystorePass.txt”。

- **自己生成CSR**

  a. 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。

  b. 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。

  i. “pem”文件和生成CSR时的私钥“server.key”放在OpenSSL工具安装目录的bin目录下。

  ii. 在OpenSSL工具安装目录的bin目录下，执行以下命令将pem格式证书转换为PFX格式证书，按“Enter”。

  openssl pkcs12 -export -out server.pfx -inkey server.key -in *证书ID_证书绑定的域名*_**server.pem**

  回显信息如下：

  ```
  Enter Export Password:
  ```

  iii. 输入PFX证书密码，按“Enter”。

  此处输入的密码为用户自定义密码，请根据自己的需求进行设置并输入密码。

  回显信息如下：

  ```
  Verifying - Enter Export Password:
  ```

  说明

  请牢记此处输入的PFX证书密码。后续设置JKS密码需要与此处设置的PFX密码保持一致，否则可能会导致Tomcat启动失败。

  为提高用户密码安全性，建议按以下复杂度要求设置密码：

  - 密码长度为8～32个字符。
  - 至少需要包含大写字母、小写字母、数字、空格、特殊字符~`!@#$%^&*()_+|{}:"<>?-=\[];',./中的3种类型字符。

  iv. 再次输入PFX证书密码，按“Enter”。

当系统没有回显任何错误信息，表示已在OpenSSL工具安装目录下成功生成“server.pfx”文件。

c. 使用Keytool工具，将PFX格式证书文件转换成JKS格式，得到“server.jks”文件。

i. 将**b**中生成的“server.pfx”文件复制到“%JAVA_HOME%/jdk/bin”目录下。

ii. 在“%JAVA_HOME%/jdk/bin”目录下，执行以下命令，按“Enter”。

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

回显信息如下：

```
输入目标密钥库口令:
```

iii. 输入JKS证书密码，按“Enter”。

须知

请将JKS密码设置为与PFX证书密码相同的密码，否则可能会导致Tomcat启动失败。

回显信息如下：

```
再次输入新口令:
```

iv. 再次输入JKS证书密码，按“Enter”。

回显信息如下：

```
输入源密钥库口令:
```

v. 输入**b.iii**中设置PFX证书密码，按“Enter”。

回显类似如下信息时，则表示转换成功，已在OpenSSL工具安装目录下成功生成“server.jks”文件。

```
已成功导入别名 1的条目。
已完成导入命令：1个条目成功导入，0个条目失败或取消
```

vi. 在“%JAVA_HOME%/jdk/bin”目录下新建一个“keystorePass.txt”文件，将JKS的密码保存在该文件中。

d. 将转换后的证书文件“server.jks”和新建的密码文件“keystorePass.txt”放在同一目录下。

步骤二：创建目录

在Tomcat的安装目录下创建“cert”目录，并且将证书文件“server.jks”和密码文件“keystorePass.txt”复制到“cert”目录中。

步骤三：修改配置文件

须知

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

在Tomcat7安装证书的具体操作如下：

1. 在Tomcat安装目录conf目录下“server.xml”文件中找到如下参数：

```
<!--
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
              maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS" />
   -->
```

2. 找到以上参数，去掉<!- - 和 - ->这对注释符。
3. 增加以下2个参数，请根据表4-2修改参数的值。

```
keystoreFile="cert/server.jks"
keystorePass="证书密码"
```

完整配置参考如下，其余参数请根据实际情况进行修改：

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
              maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    keystoreFile="cert/server.jks"
    keystorePass="证书密码"
    clientAuth="false" sslProtocol="TLS" />
```

须知

不要直接复制所有配置，只需添加“keystoreFile”，“keystorePass”参数即可，其它参数请根据自己的实际情况修改。

表 4-2 参数说明（一）

参数	参数说明
port	指定服务器要使用的端口号，建议配置为“443”。
protocol	设置HTTP协议，保持缺省值即可。
keystoreFile	“server.jks”文件存放路径，绝对路径和相对路径均可。示例：cert/server.jks
keystorePass	“server.jks”的密码。填写“keystorePass.txt”文件内的密码。 **须知** 如果密码中包含**“&”**，请将其替换成**“&”**，以免配置不成功。 示例： 如果keystorePass="Ix6**&**APWgcHf72DMu"，则修改为keystorePass="Ix6**&**APWgcHf72DMu"。
clientAuth	是否要求所有的SSL客户出示安全证书，对SSL客户进行身份验证，保持缺省值即可。

4. 在Tomcat安装目录conf目录下“server.xml”文件中找到如下参数：

```
<Host name="localhost"  appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

5. 将“Host name”改为证书绑定的域名。

完整配置如下（以“www.domain.com”为例）：

```
<Host name="www.domain.com"  appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

6. 修改完成后保存配置文件。

步骤四：重启 Tomcat

在Tomcat bin目录下执行**./shutdown.sh**命令停止Tomcat服务；

等待10秒后，再执行**./startup.sh**命令（如进程被守护进程自动拉起，则无需手动启动），启动Tomcat服务。

步骤五：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.1.4 在 Nginx 服务器上安装 SSL 证书

本文以CentOS 7操作系统中的Nginx 1.7.8服务器为例介绍SSL证书的安装步骤，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国际标准证书。

操作步骤

在CentOS 7操作系统中的Nginx 1.7.8服务器上安装SSL证书的流程如下所示：

①获取文件 → **②创建目录** → **③上传证书文件** → **④修改配置文件** → **⑤验证配置是否正确** → **⑥重启Nginx** → **⑦效果验证**

步骤一：获取文件

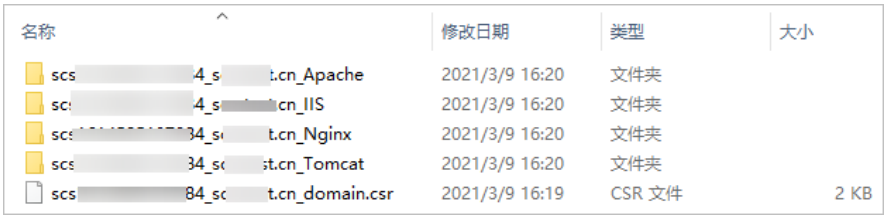
安装证书前，需要获取证书文件和密码文件，请根据申请证书时选择的“证书请求文件”生成方式来选择操作步骤：

- 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**。

具体操作如下：

- **系统生成CSR**
  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 本地解压SSL证书**所示。

  图 4-4 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-----”。
- **自己生成CSR**
  a. 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。
  b. 将“*证书ID_证书绑定的域名*_server.pem”的后缀名修改为“crt”，即“server.crt”。

c. 将“server.crt”和生成CSR时的私钥“server.key”放在任意文件夹内。

步骤二：创建目录

在Nginx的安装目录conf下，创建“cert”目录用于存放证书文件。

1. 执行以下命令，进入到Nginx的安装目录conf下。

   此处以Nginx默认配置文件目录“/usr/local/nginx/conf”为例进行命令演示，请以您实际的conf目录进行调整。

   cd /usr/local/nginx/conf

2. 执行以下命令，创建“cert”目录。

   mkdir cert

步骤三：上传证书文件

将步骤一中获取到的本地“server.key”和“server.crt”证书文件上传到Nginx服务器的证书目录下（步骤二创建的“cert”目录）。

上传方法：

- 如果您使用的是弹性云服务器ECS，如何上传文件，请参见**上传文件到云服务器**。
- 其他服务器，可以使用远程登录工具（PuTTy、Xshell等）自带的本地文件上传功能进行上传。

步骤四：修改配置文件

须知

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

配置Nginx中“conf”目录下的“nginx.conf”文件。

1. 找到如下配置内容：

```
#server {
#    listen       443 ssl;
#    server_name  localhost;
#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;
#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;
#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;
#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
```

2. 删除行首的配置语句注释符号#。

```
server {
            listen              443 ssl;
            server_name         localhost;
            ssl_certificate     cert.pem;
            ssl_certificate_key cert.key;
```

```
        ssl_session_cache    shared:SSL:1m;
        ssl_session_timeout 5m;
        ssl_ciphers          HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers  on;
        location / {
                root     html;
                index    index.html index.htm;
                 }
}
```

3. 修改如下参数，具体参数修改说明如**表 参数说明**所示。

```
ssl_certificate          cert/server.crt;
ssl_certificate_key      cert/server.key;
```

完整的配置如下，其余参数根据实际情况修改：

```
server {
    listen       443 ssl; #配置HTTPS的默认访问端口为443。如果在此处未配置HTTPS的默认访问端口，可能会导致Nginx无法启动。
    server_name  www.domain.com; #修改为您证书绑定的域名。
    ssl_certificate      cert/server.crt; #替换成您的证书文件的路径。
    ssl_certificate_key  cert/server.key; #替换成您的私钥文件的路径。
    ssl_session_cache    shared:SSL:1m;
    ssl_session_timeout  5m;
    ssl_ciphers  HIGH:!aNULL:!MD5; #加密套件。
    ssl_prefer_server_ciphers  on;
    location / {
        root   html; #站点目录。
        index  index.html index.htm; #添加属性。
            }
}
```

须知

不要直接复制所有配置，参数中“ssl”开头的属性与证书配置有直接关系，其它参数请根据自己的实际情况修改。

表 4-3 参数说明

参数	参数说明
listen	SSL访问端口号，设置为“443”。 配置HTTPS的默认访问端口为443。如果未配置HTTPS的默认访问端口，可能会导致Nginx无法启动。
server_name	证书绑定的域名。示例：www.domain.com
ssl_certificate	证书文件“server.crt”。 设置为“server.crt”文件的路径，且路径中不能包含中文字符，例如“cert/server.crt”。
ssl_certificate_key	私钥文件“server.key”。 设置为“server.key”的路径，且路径中不能包含中文字符，例如“cert/server.key”。

4. 修改完成后保存配置文件。

步骤五：验证配置是否正确

进入Nginx执行目录下，执行以下命令：

sbin/nginx -t

当回显信息如下所示时，则表示配置正确：

```
nginx.conf syntax is ok
nginx.conf test is successful
```

步骤六：重启 Nginx

执行以下命令，重启Nginx，使配置生效。

cd /usr/local/nginx/sbin

./nginx -s reload

步骤七：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示?** 进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站?** 进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.1.5 在 Apache 服务器上安装 SSL 证书

本文以CentOS 7操作系统中的Apache 2.4.6服务器为例介绍SSL证书的安装步骤，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。
- Apache服务器上已安装了mod_ssl.so模块（启用SSL功能）。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。

- 待安装证书为国际标准证书。

操作步骤

在CentOS 7操作系统中的Apache 2.4.6服务器上安装SSL证书的流程如下所示：

①获取文件 → **②创建目录** → **③修改配置文件** → **④重启Apache** → **⑤效果验证**

步骤一：获取文件

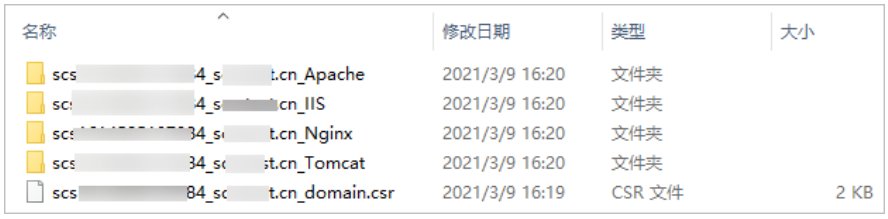
安装证书前，需要获取证书文件和密码文件，请根据申请证书时选择的“证书请求文件”生成方式来选择操作步骤：

- 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**。

具体操作如下：

- **系统生成CSR**
  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 本地解压SSL证书**所示。

     图 4-5 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-----”。
- **自己生成CSR**
  a. 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。

b. 复制“*证书ID_证书绑定的域名*_server.pem”文件的第一段证书代码（服务器证书），并另存为“server.crt”文件。
c. 复制“*证书ID_证书绑定的域名*_server.pem”文件的第二段证书代码（中级CA），并另存为“ca.crt”文件。
d. 将“ca.crt”、“server.crt”和生成CSR时的私钥“server.key”放在任意文件夹内。

步骤二：创建目录

在Apache的安装目录下创建“cert”目录，并且将“server.key”、“server.crt”和“ca.crt”复制到“cert”目录下。

步骤三：修改配置文件

须知

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

1. 打开Apache根目录下“conf.d/ssl.conf”文件。
2. 配置证书绑定的域名。

   找到并修改如下参数：

   ```
   ServerName www.example.com:443
   ```

   完整配置如下（以“www.domain.com”为例）：

   ```
   ServerName www.domain.com:443 #用户服务器的域名
   ```

3. 配置证书公钥。

   找到并修改如下参数：

   ```
   SSLCertificateFile "${SRVROOT}/conf/server.crt"
   ```

   设置证书公钥文件“server.crt”文件的路径，且路径中不能包含中文字符，例如“cert/server.crt”。

   完整配置如下：

   ```
   SSLCertificateFile "cert/server.crt"
   ```

4. 配置证书私钥。

   找到并修改如下参数：

   ```
   SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
   ```

   设置为“server.key”文件的路径，且路径中不能包含中文字符，例如“cert/server.key”。

   完整配置如下：

   ```
   SSLCertificateKeyFile "cert/server.key"
   ```

5. 配置证书链。

   找到并修改如下参数：

   ```
   #SSLCertificateChainFile "${SRVROOT}/conf/server-ca.crt"
   ```

   删除行首的配置语句注释符号“#”，并设置为“ca.crt”文件的路径，且路径中不能包含中文字符，例如“cert/ca.crt”。

   完整配置如下：


```
SSLCertificateChainFile "cert/ca.crt"
```

6. 修改后，保存“ssl.conf”文件并退出编辑。

步骤四：重启 Apache

执行以下操作重启Apache，使配置生效。

1. 执行**service httpd stop**命令停止Apache服务。
2. 执行**service httpd start**命令启动Apache服务。

步骤五：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.1.6 在 IIS 服务器上安装 SSL 证书

本章节介绍将国际标准证书安装到IIS服务器，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国际标准证书。

操作步骤

在IIS服务器上安装SSL证书的流程如下所示：

①获取文件 → **②配置IIS** → **③效果验证**

步骤一：获取文件

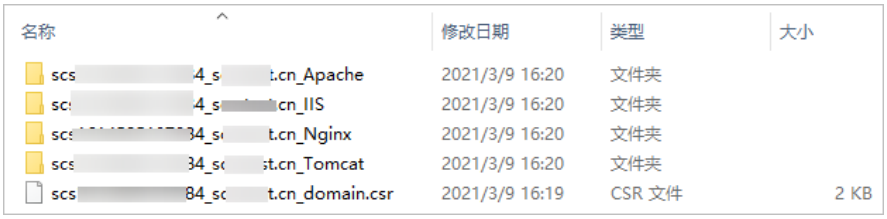
安装证书前，需要获取证书文件和密码文件，请根据申请证书时选择的“证书请求文件”生成方式来选择操作步骤：

- 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**。

具体操作如下：

- **系统生成CSR**
  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4-6所示。

     图 4-6 本地解压 SSL 证书

  b. 从“*证书ID_证书绑定的域名*_IIS”文件夹内获得SSL证书文件“*证书ID_证书绑定的域名*_server.pfx”和密码文件“*证书ID_证书绑定的域名*_keystorePass.txt。”
- **自己生成CSR**
  a. 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。
  b. 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。
     i. “pem”文件和生成CSR时的私钥“server.key”放在OpenSSL工具安装目录的bin目录下。
     ii. 在OpenSSL工具安装目录的bin目录下，执行以下命令将pem格式证书转换为PFX格式证书，按“Enter”。
     openssl pkcs12 -export -out server.pfx -inkey server.key -in *证书ID_证书绑定的域名*_**server.pem**
     回显信息如下：

```
Enter Export Password:
```

iii. 输入PFX证书密码，按“Enter”。

此处输入的密码为用户自定义密码，请根据自己的需求进行设置并输入密码。

回显信息如下：

```
Verifying - Enter Export Password:
```

说明

请牢记此处输入的PFX证书密码。后续设置JKS密码需要与此处设置的PFX密码保持一致，否则可能会导致IIS启动失败。

为提高用户密码安全性，建议按以下复杂度要求设置密码：

- 密码长度为8～32个字符。
- 至少需要包含大写字母、小写字母、数字、空格、特殊字符~`!@#$%^&*()_+|{}:"<>?-=\[];',./中的3种类型字符。

iv. 再次输入PFX证书密码，按“Enter”。

当系统没有回显任何错误信息，表示已在OpenSSL工具安装目录下成功生成“server.pfx”文件。

v. 在OpenSSL工具安装目录下，新建一个“keystorePass.txt”文件，将PFX的密码保存在该文件中。

步骤二：配置 IIS

1. 安装IIS，请参照IIS相关安装指导进行安装。
2. 打开IIS管理控制台，双击“服务器证书”，如图4-7所示。

图 4-7 服务器证书

3. 在弹出的窗口中，单击“导入”，如图4-8所示。

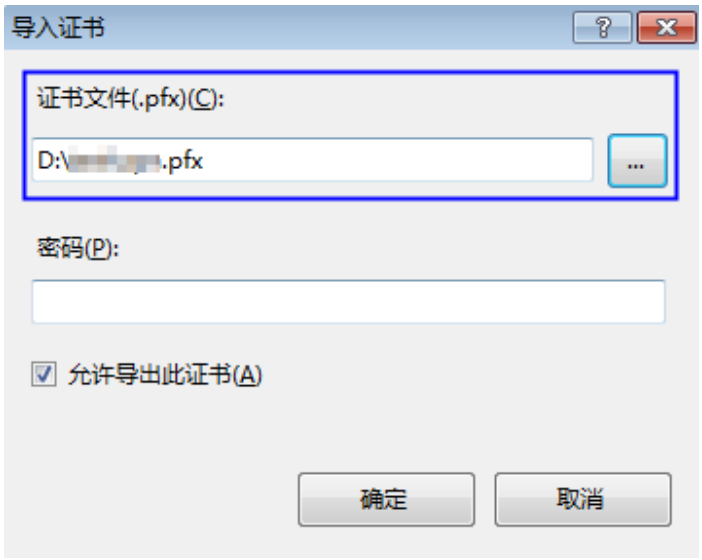
图 4-8 导入

4. 导入“server.pfx”证书文件，单击“确定”。

   说明

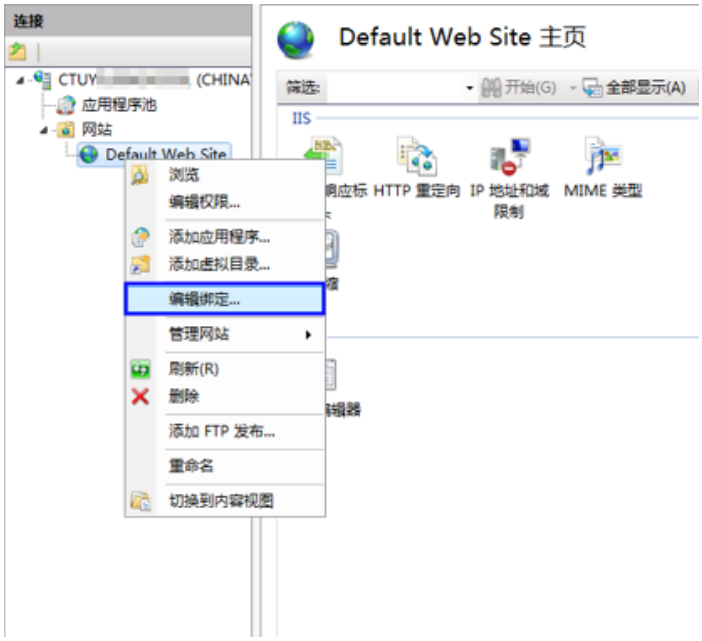
   “密码”配置框内需要输入“keystorePass.txt”文件内的密码。

   图 4-9 导入 pfx 证书文件



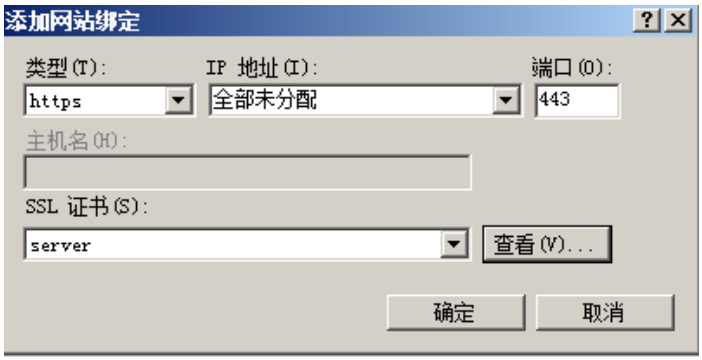
5. 鼠标右键单击目标站点（这里以默认站点为例），选择“编辑绑定”，如图4-10所示。

   图 4-10 编辑绑定



6. 在弹出的窗口中，单击“添加”，并填写以下信息。

图 4-11 添加网站绑定



- 类型：选择“https”。
- 端口：保持默认的“443”端口即可。
- SSL证书：选择4导入的证书。

7. 填写完成后，单击“确定”。

步骤三：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示?** 进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站?** 进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.1.7 在 Weblogic 服务器上安装 SSL 证书

Weblogic基于JAVAEE架构的中间件，Weblogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。将Java的动态功能和Java Enterprise标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

目前Weblogic 10.3.1及其以上的版本支持所有主流品牌的SSL证书，10.3.1之前的版本不支持各品牌SSL证书。

本章节介绍将国际标准证书安装到Weblogic服务器，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。
- 已安装JDK。

  Weblogic安装后自带JDK安装。如果未安装，则请安装**Java SE Development Kit (JDK)**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国际标准证书。

操作步骤

在Weblogic服务器上安装SSL证书的流程如下所示：

①获取文件 → **②配置Weblogic** → **③效果验证**

步骤一：获取文件

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**。

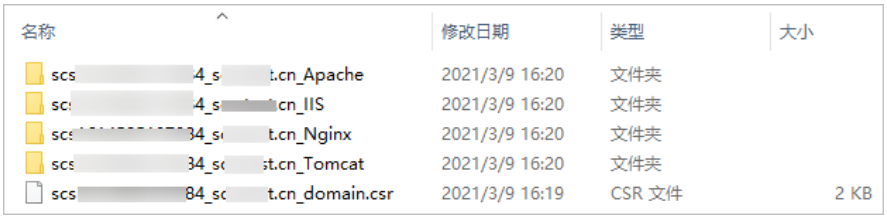
具体操作如下：

- **系统生成CSR**

  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4-12**所示。

  图 4-12 本地解压 SSL 证书

  b. 从“*证书ID_证书绑定的域名*_Tomcat”文件夹内获得证书文件“*证书ID_证书绑定的域名*_server.jks”和密码文件“*证书ID_证书绑定的域名*_keystorePass.txt”。

- **自己生成CSR**

  a. 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。

  b. 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。

  i. “pem”文件和生成CSR时的私钥“server.key”放在OpenSSL工具安装目录的bin目录下。

  ii. 在OpenSSL工具安装目录的bin目录下，执行以下命令将pem格式证书转换为PFX格式证书，按“Enter”。

  openssl pkcs12 -export -out server.pfx -inkey server.key -in *证书ID_证书绑定的域名*_**server.pem**

  回显信息如下：

  ```
  Enter Export Password:
  ```

  iii. 输入PFX证书密码，按“Enter”。

  此处输入的密码为用户自定义密码，请根据自己的需求进行设置并输入密码。

  回显信息如下：

  ```
  Verifying - Enter Export Password:
  ```

  说明

  请牢记此处输入的PFX证书密码。后续设置JKS密码需要与此处设置的PFX密码保持一致，否则可能会导致Weblogic启动失败。

  为提高用户密码安全性，建议按以下复杂度要求设置密码：

  - 密码长度为8～32个字符。
  - 至少需要包含大写字母、小写字母、数字、空格、特殊字符~`!@#$%^&*()_+|{}:"<>?-=\[];',./中的3种类型字符。

  iv. 再次输入PFX证书密码，按“Enter”。

  当系统没有回显任何错误信息，表示已在OpenSSL工具安装目录下成功生成“server.pfx”文件。

  c. 使用Keytool工具，将PFX格式证书文件转换成JKS格式，得到“server.jks”文件。

  i. 将**b**中生成的“server.pfx”文件复制到“%JAVA_HOME%/jdk/bin”目录下。

  ii. 在“%JAVA_HOME%/jdk/bin”目录下，执行以下命令，按“Enter”。

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

  回显信息如下：

  ```
  输入目标密钥库口令:
  ```

  iii. 输入JKS证书密码，按“Enter”。

须知

请将JKS密码设置为与PFX证书密码相同的密码，否则可能会导致Weblogic启动失败。

回显信息如下：

```
再次输入新口令:
```

iv. 再次输入JKS证书密码，按“Enter”。

回显信息如下：

```
输入源密钥库口令:
```

v. 输入2.c中设置PFX证书密码，按“Enter”。

回显类似如下信息时，则表示转换成功，已在OpenSSL工具安装目录下成功生成“server.jks”文件。

```
已成功导入别名 1的条目。
已完成导入命令：1个条目成功导入，0个条目失败或取消
```

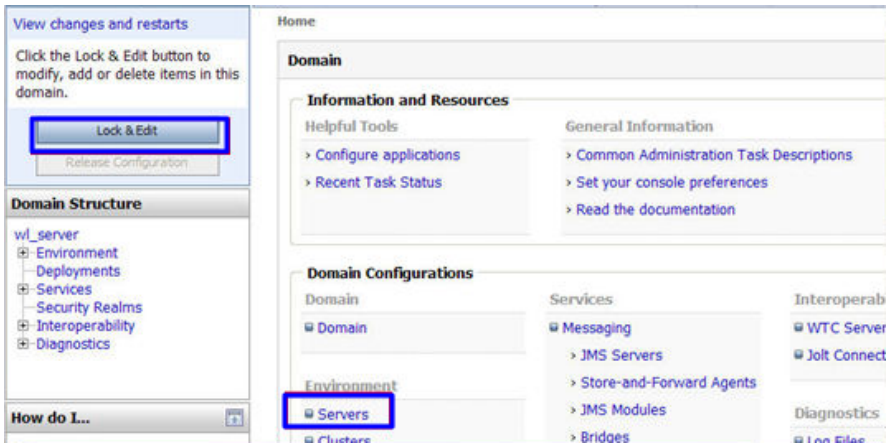
vi. 在“%JAVA_HOME%/jdk/bin”目录下新建一个“keystorePass.txt”文件，将JKS的密码保存在该文件中。

d. 将转换后的证书文件“server.jks”和新建的密码文件“keystorePass.txt”放在同一目录下。

步骤二：配置 Weblogic

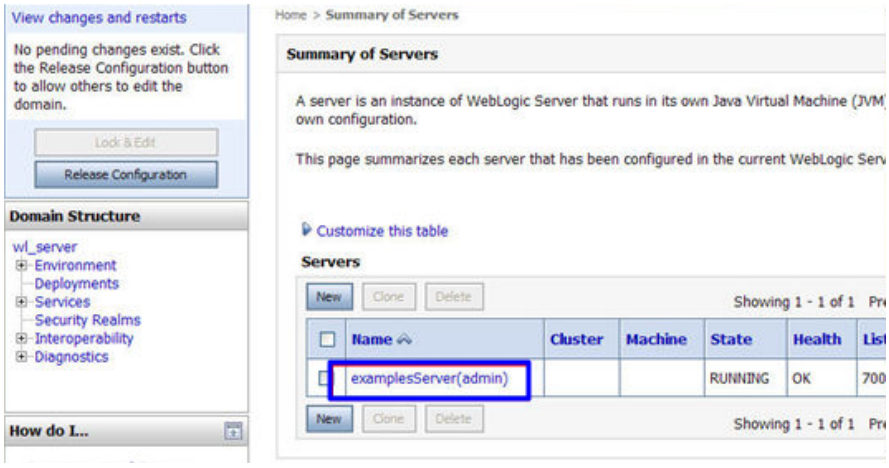
1. 登录Weblogic服务器管理控制台。
2. 单击页面左上方“Lock & Edit”，解锁配置。
3. 在“Domain Configurations”中，单击“Servers”。

图 4-13 服务器



4. 在服务器列表中，选择您需要配置服务器证书的Server，进入服务器的设置页面。

图 4-14 目标服务器

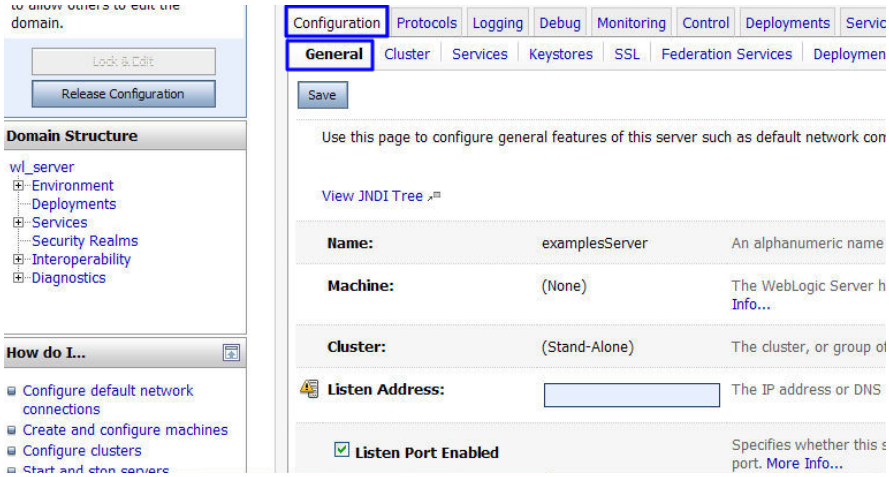


5. 修改HTTPS端口。

   在服务器的配置页面，选择“General”页签，配置是否启用HTTP和HTTPS，以及访问端口号。

   请勾选“Listen SSL Port Enabled”，并修改端口号为“443”。

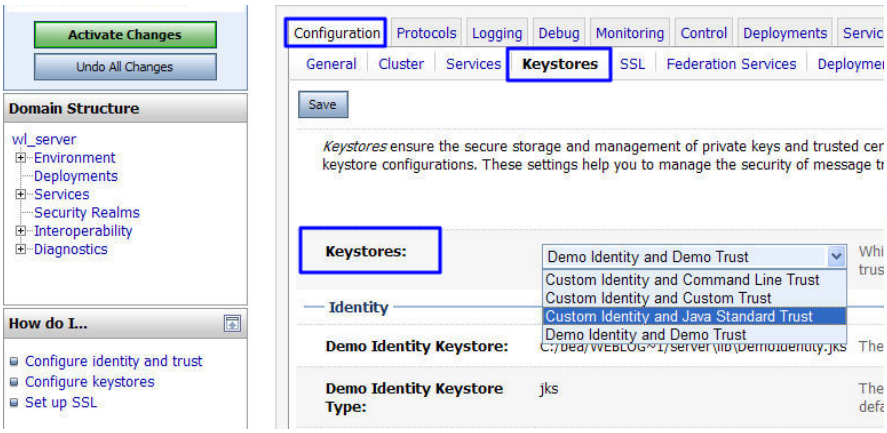
图 4-15 端口



6. 配置认证方式和密钥。

   a. 在服务器的配置页面，选择“Keystores”页签，配置认证方式。

图 4-16 认证方式

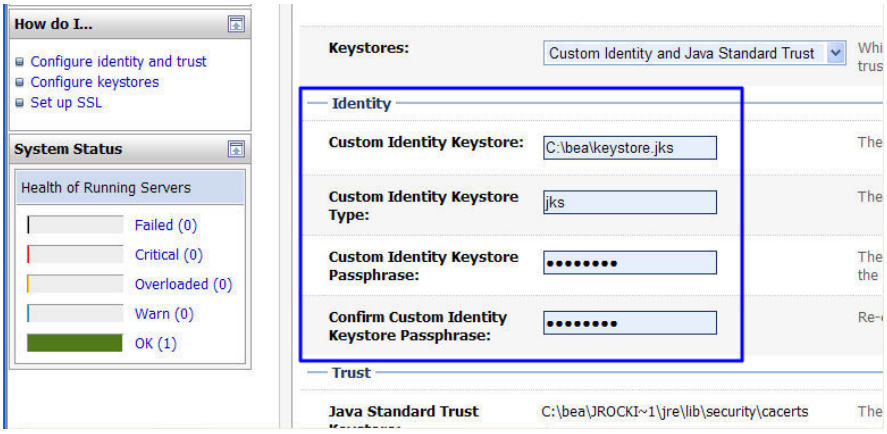


- 服务器身份认证请选择“Custom identity and Java Standard Trust”。
- 双向认证请选择“Custom Identity and Custom Trust”。

b. 在“Identity”区域中，配置密钥。

配置密钥库文件server.jks所保存的服务器上的路径，并填写密钥库文件密码。

图 4-17 密钥

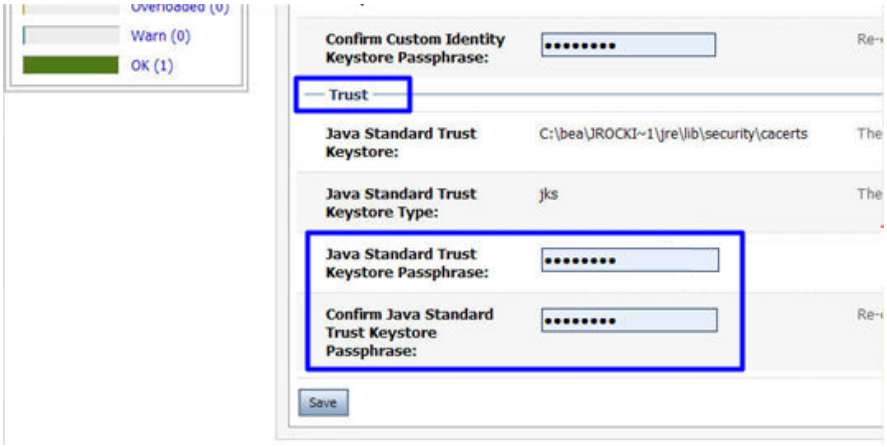


- **Custom Identity Keystore**：请填写jks文件保存路径。示例：C:\bea\server.jks
- **Custom Identity Keystore Type**：文件格式请填写“jks”。
- **Custom Identity Keystore Passphrase**：请填在证书密码，即“keystorePass.txt”中的密码。
- **Confirm Custom Identity Keystore Passphrase**：请再次填写证书密码。

c. 在单向认证中，需要配置JRE默认信任库文件cacerts。

Cacerts默认密码为changeit。

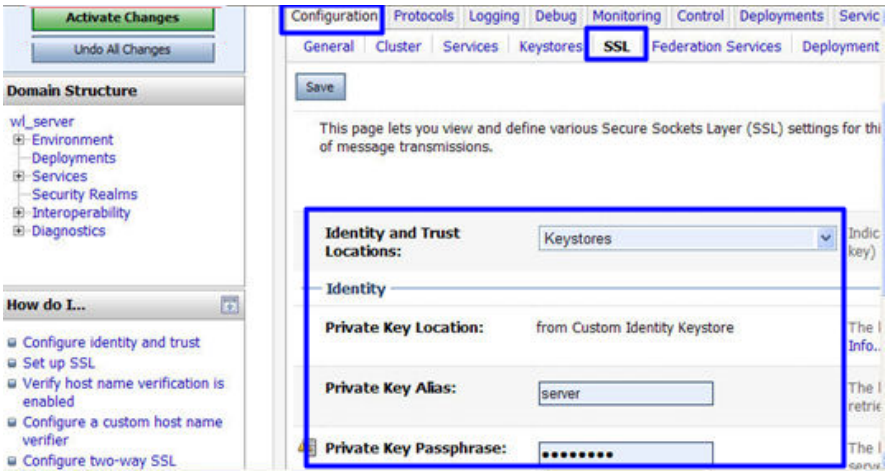
图 4-18 信任库文件



- **Java Standard Trust Keystore Passphrase**：输入默认密码changeit。
- **Confirm Java Standard Trust Keystore Passphrase**：再次输入默认密码。

7. 配置服务器证书私钥别名。
   在服务器的配置页面，选择“SSL”页签，配置以下参数：

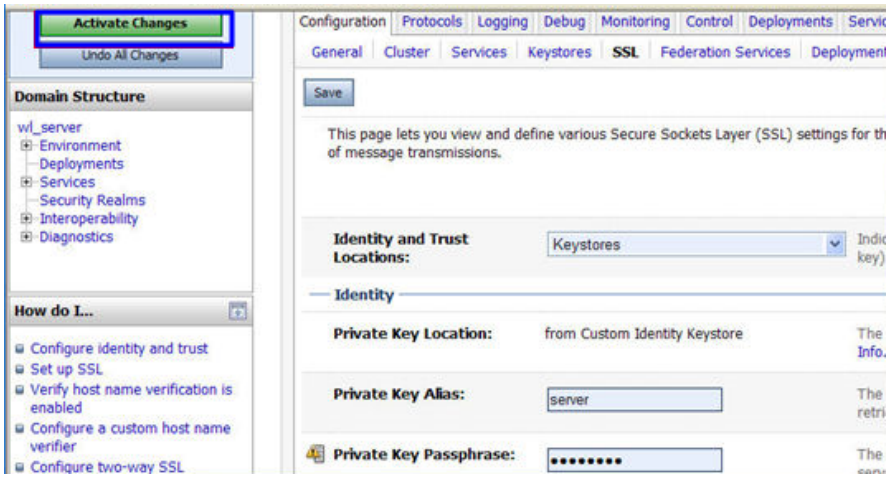
图 4-19 私钥



- **Identity and Trust Locations**：请选择为“Keystores”。
- **Private KeyAlias**：配置私钥库中的私钥别名信息。私钥别名可以使用**keystool -list**命令查看。
- **Private Key Passphrase**：输入私钥保护密码。通常私钥保护密码和keystore文件保护密码相同。
- **Confirm Private Key Passphrase**：再次输入私钥保护密码。

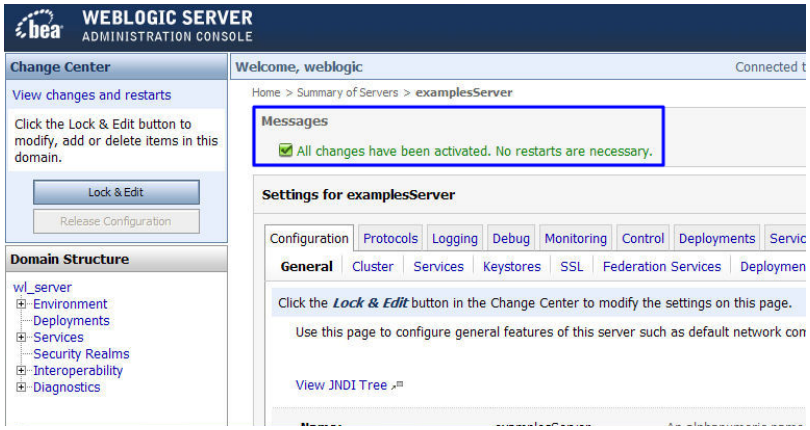
8. 设置完成后，单击“Active Changes”，保存所有修改。

图 4-20 保存配置



9. （可选）如果系统提示需要重启Weblogic，则需要重启后才能使配置生效。如图4-21所示，则无需重启。

图 4-21 提示信息



步骤三：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.1.8 在 Resin 服务器上安装 SSL 证书

本章节介绍将国际标准证书安装到Resin服务器，您在安装国际标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载证书**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国际标准证书。

操作步骤

在Resin服务器上安装SSL证书的流程如下所示：

①获取文件 → **②配置Resin** → **③效果验证**

步骤一：获取文件

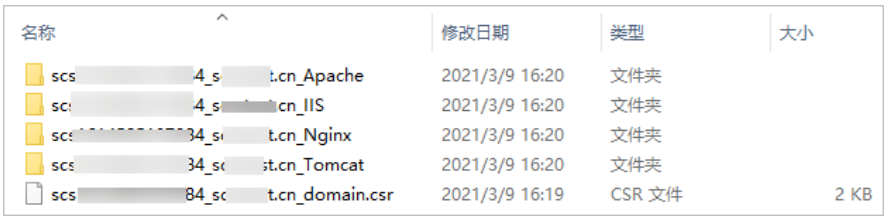
安装证书前，需要获取证书文件和密码文件，请根据申请证书时选择的“证书请求文件”生成方式来选择操作步骤：

- 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**。

具体操作如下：

- **系统生成CSR**
  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4-22**所示。

图 4-22 本地解压 SSL 证书



b. 从“*证书ID_证书绑定的域名*_Tomcat”文件夹内获得证书文件“*证书ID_证书绑定的域名*_server.jks”和密码文件“*证书ID_证书绑定的域名*_keystorePass.txt”。

- **自己生成CSR**

a. 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。

b. 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。

i. “pem”文件和生成CSR时的私钥“server.key”放在OpenSSL工具安装目录的bin目录下。

ii. 在OpenSSL工具安装目录的bin目录下，执行以下命令将pem格式证书转换为PFX格式证书，按“Enter”。

openssl pkcs12 -export -out server.pfx -inkey server.key -in *证书ID_证书绑定的域名*_**server.pem**

回显信息如下：

```
Enter Export Password:
```

iii. 输入PFX证书密码，按“Enter”。

此处输入的密码为用户自定义密码，请根据自己的需求进行设置并输入密码。

回显信息如下：

```
Verifying - Enter Export Password:
```

说明

请牢记此处输入的PFX证书密码。后续设置JKS密码需要与此处设置的PFX密码保持一致，否则可能会导致Resin启动失败。

为提高用户密码安全性，建议按以下复杂度要求设置密码：

- 密码长度为8～32个字符。
- 至少需要包含大写字母、小写字母、数字、空格、特殊字符~`!@#$%^&*()_+|{}:"<>?-=\[];',./中的3种类型字符。

iv. 再次输入PFX证书密码，按“Enter”。

当系统没有回显任何错误信息，表示已在OpenSSL工具安装目录下成功生成“server.pfx”文件。

c. 使用Keytool工具，将PFX格式证书文件转换成JKS格式，得到“server.jks”文件。

i. 将**b**中生成的“server.pfx”文件复制到“%JAVA_HOME%/jdk/bin”目录下。

ii. 在“%JAVA_HOME%/jdk/bin”目录下，执行以下命令，按“Enter”。

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

回显信息如下：

```
输入目标密钥库口令:
```

iii. 输入JKS证书密码，按“Enter”。

须知

请将JKS密码设置为与PFX证书密码相同的密码，否则可能会导致Resin启动失败。

回显信息如下：

```
再次输入新口令:
```

iv. 再次输入JKS证书密码，按“Enter”。

回显信息如下：

```
输入源密钥库口令:
```

v. 输入**2.c**中设置PFX证书密码，按“Enter”。

回显类似如下信息时，则表示转换成功，已在OpenSSL工具安装目录下成功生成“server.jks”文件。

```
已成功导入别名 1的条目。
已完成导入命令：1个条目成功导入，0个条目失败或取消
```

vi. 在“%JAVA_HOME%/jdk/bin”目录下新建一个“keystorePass.txt”文件，将JKS的密码保存在该文件中。

d. 将转换后的证书文件“server.jks”和新建的密码文件“keystorePass.txt”放在同一目录下。

步骤二：配置 Resin

须知

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

1. （可选）安装Resin。

   如果已安装，则请跳过该步骤。

   a. 登录**Resin官网**并根据您的系统下载不同的应用程序包。

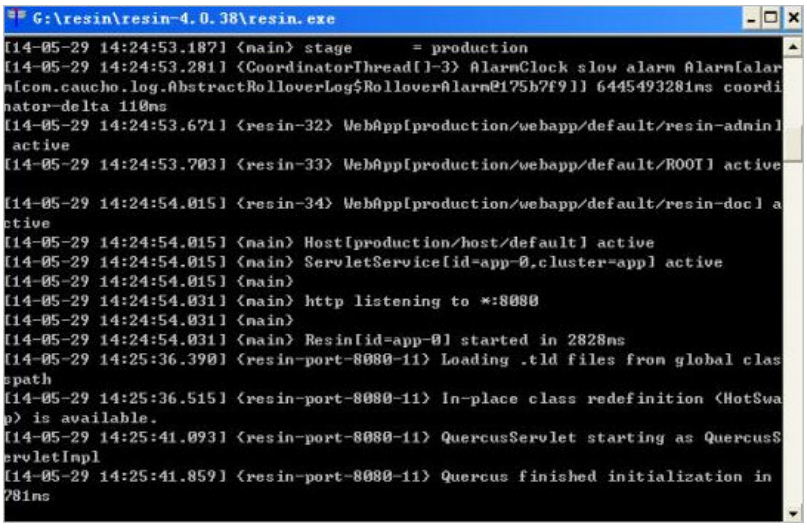
      本步骤以下载**Windows**版本的**Resin-4.0.38**版本为例进行说明。

   b. 解压下载的Resin包。

   c. 进入Resin-4.0.38根目录并找到resin.exe文件。

   d. 运行resin.exe文件，运行期间将出现如**图4-23**所示的命令提示符窗口。

图 4-23 提示窗口



e. 运行完成后，启动浏览器，在Web地址栏中输入Resin默认地址“http://127.0.0.1:8080”，并按“Enter”。

当界面显示如图4-24所示时，则表示安装成功。

图 4-24 登录 Resin

2. 修改配置文件。

a. 在Resin安装目录下的“Resin.properties”配置文件（由于Resin版本的不同，配置文件也可能为“resin.xml”文件）中，找到如下参数：

```
# specifies the --server in the config file
# home_server : app-0

# Set HTTP and HTTPS bind address
# http_address : *

# Set HTTP and HTTPS ports.
# Use overrides for individual server control, for example: app-0.http : 8081
app.http        : 8080
# app.https       : 8443

web.http        : 8080
# web.https       : 8443
```

b. 将“app.https”和“web.https”前的注释符“#”去掉，并将“8443端”口修改为“443”。修改后，如下所示：

“app.https”、“web.https”：指定服务器要使用的端口号，建议配置为“443”。

```
# specifies the --server in the config file
# home_server : app-0

# Set HTTP and HTTPS bind address
# http_address : *

# Set HTTP and HTTPS ports.
# Use overrides for individual server control, for example: app-0.http : 8081
app.http          : 8080
app.https          : 443

web.http          : 8080
web.https          : 443
```

c. 找到如下参数，并将“jsse_keystore_tye”、“jsse_keystore_file”和“jsse_keystore_password”三行前的注释符“#”去掉。

```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_tye : jks
jsse_keystore_file : cert/server.jks
jsse_keystore_password : 证书密码
```

d. 修改证书相关配置参数，具体配置请参见**表4-4**。

```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_tye : jks
jsse_keystore_file : cert/server.jks
jsse_keystore_password : 证书密码
```

表 4-4 参数说明

参数	参数说明
jsse_keystore_tye	设定Keystore文件的类型，一般都设为**jks**
jsse_keystore_file	“server.jks”文件存放路径，绝对路径和相对路径均可。示例：cert/server.jks
jsse_keystore_password	“server.jks”的密码。填写“keystorePass.txt”文件内的密码。 **须知** 如果密码中包含**“&”**，请将其替换成**“&”**，以免配置不成功。 示例： 如果keystorePass="Ix6**&**APWgcHf72DMu"，则修改为keystorePass="Ix6**&**APWgcHf72DMu"。

e. 修改完成后保存配置文件。

3. 重启Resin。

步骤三：效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。

- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.2 安装国密标准（SM2）SSL 证书到 Web 服务器

4.2.1 下载 SSL 证书

SSL证书签发后，需要将SSL证书下载到本地。下载后，还需要将已下载的证书上传到Web服务器并修改服务器的相关配置，才能使SSL证书生效。

该任务介绍如何在SSL证书管理平台下载证书。

前提条件

“证书状态”为“已签发”或“托管中”。

约束条件

- 仅支持在证书有效期内，不限次数的下载证书，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。
- “证书请求文件”选择的是“系统生成CSR”，下载的文件包含了“Apache”、“Nginx”、2个文件夹和1个“domain.csr”文件。
- “证书请求文件”选择的是“自己生成CSR”，下载的证书包含了“server.pem”、“encrypt.pem”、“encrypt.key.pem”文件。“server.pem”文件中已经包含两段签名证书代码，分别是服务器证书和CA中间证书。签名证书私钥为用户自行保存的，华为云SSL证书管理不提供。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要下载的证书所在行的“操作”列，单击“下载”，如图**下载证书**所示。

图 4-25 下载证书

步骤5 在证书详情页面，确认证书信息无误后，单击“下载证书”。

步骤6 证书下载后，需要安装到对应的服务器上，才能使SSL证书生效。

不同Web服务器安装SSL证书的具体操作不同，以下介绍了两种在主流Web服务器上安装国密标准SSL证书的方法，请根据您的需要进行选择：

- **在Nginx服务器上安装国密标准SSL证书**

- 在Apache服务器上安装国密标准SSL证书

----结束

下载的证书文件说明

下载文件说明：根据申请证书时，选择的“证书请求文件”方式的不同，下载文件也有所不同。

- 申请证书时，如果“证书请求文件”选择的是“系统生成CSR”，则下载文件说明如下：

  下载的文件包含了“Apache”、“Nginx”、2个文件夹和1个“domain.csr”文件，如图**解压SSL证书**所示，具体文件说明如表**下载文件说明**所示。

  图 4-26 解压 SSL 证书

表 4-5 下载文件说明

文件夹/文件名称	文件夹内容
Nginx	server.crt：签名证书文件，包含两段证书代码，分别为服务器证书和CA中间证书。 server.key：签名证书私钥文件，包含一段签名证书私钥代码。 encrypt.crt：加密证书文件，包含一段加密证书代码。 encrypt.key：加密证书私钥文件，包含一段加密证书私钥代码。
Apache	ca.crt：证书链文件，包含一段中级CA代码。 server.crt：签名证书文件，包含一段服务器证书代码。 server.key：签名证书私钥文件，包含一段证书私钥代码。 encrypt.crt：加密证书文件，包含一段加密证书代码。 encrypt.key：加密证书私钥文件，包含一段加密证书私钥代码。
domain.csr	证书请求文件。

- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，则下载文件说明如下：

下载的证书下载的证书包含了“server.pem”、“encrypt.pem”、“encrypt.key.pem”文件。“server.pem”文件中已经包含两段签名证书代码，分别是服务器证书和CA中间证书。

签名证书私钥为用户自行保存的，华为云SSL证书管理不提供。在各个服务器上安装证书时，需要填写对应私钥的位置。

4.2.2 在 Nginx 服务器上安装国密标准 SSL 证书

本文以CentOS 7操作系统中的Nginx 1.8.0服务器为例介绍国密标准（SM2）SSL证书的安装步骤，您在安装国密标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“**证书状态**”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载SSL证书**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国密标准证书。

操作步骤

在CentOS 7操作系统中的Nginx 1.8.0服务器上安装SSL证书的流程如下所示：

①环境配置 → **②获取文件** → **③修改配置文件** → **④验证配置是否正确** → **⑤重启Nginx** → **⑥效果验证**

步骤一：环境配置

1. 准备gmssl_openssl

   下载页面**https://www.gmssl.cn/gmssl/index.jsp**中的openssl国密版

   拷贝到/root/目录并解压

   tar xzfm gmssl_openssl_1.1_b2024_x64_1.tar.gz -C /usr/local

   则/usr/local/gmssl为国密版openssl目录
2. 准备nginx
3. 下载nginx-1.18.0

4. tar zxfm nginx-1.18.0.tar.gz
5. cd httpd-2.4.46
6. vi auto/lib/openssl/conf
7. 将全部$OPENSSL/.openssl/修改为$OPENSSL/并保存
8. ./configure \
9. --without-http_gzip_module \
10. --with-http_ssl_module \
11. --with-http_stub_status_module \
12. --with-http_v2_module \
13. --with-file-aio \
14. --with-openssl="/usr/local/gmssl" \
15. --with-cc-opt="-I/usr/local/gmssl/include" \
16. --with-ld-opt="-lm"
17. 然后make install
18. 则/usr/local/nginx为生成的国密版nginx目录
19. 注：可能需要安装pcre-devel包。

步骤二：获取文件

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**。

具体操作如下：

- **系统生成CSR**
  a. 在本地解压已下载的证书文件。
  下载的文件包含了“Apache”、“Nginx” 2个文件夹和1个“domain.csr”文件，如图**本地解压SSL证书**所示。

  图 4-27 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”、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*_encrypt.crt”和私钥文件“*证书ID_证书绑定的域名*_ encrypt.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 EC PRIVATE KEY-----”和“-----END EC PRIVATE KEY-----”。
- “*证书ID_证书绑定的域名*_ encrypt.crt”文件包括一段加密证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
- “*证书ID_证书绑定的域名*_ encrypt.key”文件包括一段私钥代码“-----BEGIN EC PRIVATE KEY-----”和“-----END EC PRIVATE KEY-----”。

- **自己生成CSR**

  a. 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。

  b. 将“*证书ID_证书绑定的域名*_server.pem”的后缀名修改为“crt”，即“server.crt”。

  c. 将“*证书ID_证书绑定的域名*_encrypt.pem”的后缀名修改为“crt”，即“encrypt.crt”。

  d. 将“server.crt”，“encrypt.crt”，“encrypt.key”和生成CSR时的私钥“server.key”放在任意文件夹内。

在/usr/local/nginx/conf目录下创建“cert”目录，并且将“server.key”、“server.crt”、“encrypt.key”和“encrypt.crt”复制到“cert”目录下。

步骤三：修改配置文件

说明

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

配置/usr/local/nginx/conf目录下的“nginx.conf”文件。

1. 找到如下配置内容，并取消注释

```
#server {
#    listen       443 ssl;
#    server_name  localhost;
#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;
#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;
#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;
#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
```

2. 修改如下参数，具体参数修改说明如表**参数说明**所示。

```
ssl_certificate cert/server.crt;
ssl_certificate_key      cert/server.key;
```

完整的配置如下，其余参数根据实际情况修改：

```
server {
    listen       443 ssl; #配置HTTPS的默认访问端口为443。如果在此处未配置HTTPS的默认访问端口，可能会导致Nginx无
    server_name  test
```

```
.com; #修改为您证书绑定的域名。
        ssl_certificate      /usr/local/nginx/conf/
cert/server.crt; #替换成您的签名证书文件的路径。
        ssl_certificate_key  /usr/local/nginx/conf/
cert/server.key; #替换成您的签名证书私钥文件的路径。
        ssl_certificate      /usr/local/nginx/conf/
cert/encrypt.crt; #替换成您的加密证书文件的路径。
        ssl_certificate_key  /usr/local/nginx/conf/
cert/encrypt.key; #替换成您的加密证书私钥文件的路径。
        ssl_session_cache    shared:SSL:1m;
        ssl_session_timeout  5m;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_ciphers  ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #加密套件。
        ssl_prefer_server_ciphers  on;
        location / {
            root   html; #站点目录。
            index  index.html index.htm; #添加属性。
                }
}
```

说明

不要直接复制所有配置，参数中“ssl”开头的属性与证书配置有直接关系，其它参数请根据自己的实际情况修改。

表 4-6 参数说明

参数	参数说明
listen	SSL访问端口号，设置为“443”。 配置HTTPS的默认访问端口为443。如果未配置HTTPS的默认访问端口，可能会导致Nginx无法启动。
server_name	证书绑定的域名。示例：www.domain.com
ssl_certificate	证书文件“server.crt”。 设置为“server.crt”文件的路径，且路径中不能包含中文字符，例如“/usr/local/nginx/conf/cert/server.crt”。
ssl_certificate_key	私钥文件“server.key”。 设置为“server.key”的路径，且路径中不能包含中文字符，例如“/usr/local/nginx/conf/cert/server.key”。

1. 修改完成后保存配置文件。

步骤四：验证配置是否正确

进入Nginx执行目录下，执行以下命令：

sbin/nginx -t

当回显信息如下所示时，则表示配置正确：

```
nginx.conf syntax is ok
nginx.conf test is successful
```


步骤五：重启 Nginx

执行以下命令，重启Nginx，使配置生效。

cd /usr/local/nginx/sbin

./nginx -s reload

效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.2.3 在 Apache 服务器上安装国密标准 SSL 证书

本文以CentOS 7操作系统中的Apache 2.4.46服务器为例介绍国密标准（SM2）SSL证书的安装步骤，您在安装国密标准证书时可以进行参考。证书安装好后，您的Web服务器才能支持SSL通信，实现通信安全。

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。

如参考文档安装证书后，HTTPS仍然不生效或遇到其他问题，请单击**一对一咨询**购买SSL证书配置优化服务，联系专业工程师为您排查具体问题。

前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载SSL证书，具体操作请参见**下载SSL证书**。

约束条件

- 证书安装前，务必在安装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。
- 如果一个域名有多个服务器，则每一个服务器上都要部署。
- 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。
- 待安装证书为国密标准证书。

操作步骤

在CentOS 7操作系统中的Apache 2.4.46服务器上安装SSL证书的流程如下所示：

①环境配置 → ②获取文件 → ③修改配置文件 → ④重启Apache → ⑤效果验证

步骤一： 环境配置

1. 准备gmssl_openssl
   下载页面https://www.gmssl.cn/gmssl/index.jsp中的openssl国密版
   拷贝到/root/目录并解压
   tar xzfm gmssl_openssl_1.1_b2024_x64_1.tar.gz -C /usr/local
   则/usr/local/gmssl为国密版openssl目录
2. 准备Apache httpd
   安装必要开发包：pcre-devel，expat-devel，apr，apr-util，bison，bison-devel，flex，flex-devel
   下载Apache httpd 2.4.46
   tar zxfm httpd-2.4.46.tar.gz
   cd httpd-2.4.46
   ./configure --prefix=/usr/local/httpd --enable-so --enable-ssl --enable-cgi --enable-rewrite --enable-modules=most --enable-mpms-shared=all --with-mpm=prefork --with-zlib --with-apr=/usr/local/apr/apr --with-apr-util=/usr/local/apr/util --with-ssl=/usr/local/gmssl LDFLAGS=-lm
   vi build/config_vars.mk
   找到ab_LIBS = -L/usr/local/gmssl/lib -lssl -lcrypto -lrt -lcrypt -lpthread -ldl
   将-L/usr/local/gmssl/lib -lssl -lcrypto替换为/usr/local/gmssl/lib/libssl.a /usr/local/gmssl/lib/libcrypto.a
   然后make install
   则/usr/local/httpd为生成的国密版Apache httpd目录

步骤二：获取文件

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**。

具体操作如下：

- **系统生成CSR**
  a. 在本地解压已下载的证书文件。
     下载的文件包含了“Apache”、“Nginx”、2个文件夹和1个“domain.csr”文件，如图**本地解压SSL证书**所示。

     图 4-28 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”，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*_encrypt.crt”和私钥文件“*证书ID_证书绑定的域名*_ encrypt.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 EC PRIVATE KEY-----”和“-----END EC PRIVATE KEY-----”。
- “*证书ID_证书绑定的域名*_ encrypt.crt”文件包括一段加密证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
- “*证书ID_证书绑定的域名*_ encrypt.key”文件包括一段私钥代码“-----BEGIN EC PRIVATE KEY-----”和“-----END EC PRIVATE KEY-----”。

- **自己生成CSR**

a. 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。

b. 复制“*证书ID_证书绑定的域名*_server.pem”文件的第一段证书代码（服务器证书），并另存为“server.crt”文件。

c. 复制“*证书ID_证书绑定的域名*_server.pem”文件的第二段证书代码（中级CA），并另存为“ca.crt”文件。

d. 复制“*证书ID_证书绑定的域名*_encrypt.pem”文件的证书代码（加密证书），并另存为“encrypt.crt”文件。

e. 将“ca.crt”、“server.crt”、“encrypt.crt”、“encrypt.key”和生成CSR时的私钥“server.key”放在任意文件夹内。

在/usr/local/httpd/conf目录下创建“cert”目录，并且将“server.key”、“server.crt”、“ca.crt”、“encrypt.key”和encrypt.crt”复制到“cert”目录下。

步骤三：修改配置文件

说明

修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

1. 打开Apache安装目录下“httpd.conf”文件
2. vi /usr/local/httpd/conf/httpd.conf
3. 找到以下两行配置，取消注释
4. #LoadModule ssl_module modules/mod_ssl.so
5. #Include conf/extra/httpd-ssl.conf
6. 打开“httpd-ssl.conf”文件
7. vi /usr/local/httpd/conf/extra/httpd-ssl.conf

8. 注释掉所有带SSLSessionCache的配置行
9. 配置算法SSLCipherSuite HIGH:ECC-SM4-SM3:ECDHE-SM4-SM3
10. 注释掉默认证书和key
11. #SSLCertificateFile "/usr/local/httpd/conf/server.crt"
12. #SSLCertificateKeyFile "/usr/local/httpd/conf/server.key"
13. 配置国密双证书/私钥
14. SSLCertificateChainFile "/usr/local/httpd/conf/cert/scsxxxxxx_test.com_ca.crt"
15. SSLCertificateFile "/usr/local/httpd/conf/cert/scsxxxxxx_test.com_server.crt"
16. SSLCertificateKeyFile "/usr/local/httpd/conf/cert/ scsxxxxxx _test.com_server.key"
17. SSLCertificateFile "/usr/local/httpd/conf/cert/ scsxxxxxx _test.com_encrypt.crt"
18. SSLCertificateKeyFile "/usr/local/httpd/conf/cert/ scsxxxxxx _test.com_encrypt.key"

说明

以上配置仅供参考，证书文件名，证书所在目录等配置请以您的实际情况为准。

1. 验证配置文件
2. /usr/local/httpd/bin/httpd -t
3. 当回显信息如下所示时，则表示配置正确：
4. Syntax OK

步骤四：重启 Apache

执行以下操作重启Apache，使配置生效。

1. /usr/local/httpd/bin/httpd -k restart

效果验证

部署成功后，可在浏览器的地址栏中输入“https://域名”，按“Enter”。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

- 如果网站仍然出现不安全提示，请参见**为什么部署了SSL证书后，网站仍然出现不安全提示？**进行处理。
- 如果通过域名访问网站时，无法打开网站，请参见**为什么部署了SSL证书后，通过域名访问网站时，无法打开网站？**进行处理。
- 如果仍未解决或出现其他问题，华为云市场提供SSL证书配置优化服务，专业工程师一对一服务，请直接单击**一对一咨询**进行购买，购买服务后，联系工程师进行处理。

4.3 部署国际标准 SSL 证书到华为云产品

4.3.1 部署 SSL 证书到 WAF

SSL证书签发后，您可以将国际标准SSL证书一键部署到华为云产品Web应用防火墙（Web Application Firewall，WAF）。部署后，可以帮助您提升云产品WAF访问数据的安全性。

前提条件

- 已开通Web应用防火墙（Web Application Firewall，WAF），且已在WAF中配置了与SSL证书匹配的网站域名。
- 如果没有购买WAF，或数字证书所绑定的域名没有在WAF中开通服务，请不要将数字证书部署到WAF中，如部署将可能导致部署失败。
- 已在云证书管理服务中申请SSL证书且状态为“已签发”，或者已将在其他平台签发的SSL证书上传至云证书管理服务中且状态为“托管中”。

约束条件

- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，由于云上没有该证书的私钥，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及私钥并进行部署。
- 国密证书暂不支持一键部署到华为云其他云产品。

说明

已上传的第三方证书和有效期为三个月的测试证书部署到华为云产品需要收费，每一张证书部署到华为云产品的一个域名计为一次部署，证书部署费用为30元/次。具体收费详情请参见**关于调整证书部署功能的通知**。

部署证书

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“部署证书”，系统从右面弹出证书部署详细页面，如**图4-29**所示。

图 4-29 部署证书

步骤5 在部署证书页面的“部署详情”下，选择“WAF”页签。

图 4-30 选择 WAF

步骤6 单击企业项目或区域名称右侧的 ▼ ，选择部署的企业项目或区域。

步骤7 选择当前证书中需要部署的域名，并单击“操作”列的“重新部署”。

如需部署多个域名，则从域名列表中勾选所有待部署的域名，并单击列表左上角的“批量更新”。

步骤8 （可选）如果当前域名已经部署过该证书，单击“重新部署”后，界面会弹出重复部署仍会收费的提示框，确认无误后，单击“确定”。

步骤9 在弹出的确认框中，确认无误后，勾选“我已知悉本次部署将产生如上费用，部署成功后按需扣费，不支持退款”，单击“确认”。

图 4-31 部署证书提示信息

部署成功后，对应域名的“部署模式”刷新为“已部署”。

----结束

4.3.2 部署 SSL 证书到 ELB

SSL证书签发后，您可以将国际标准SSL证书一键部署到华为云产品弹性负载均衡（Elastic Load Balance，ELB）中。部署后，可以帮助您提升云产品ELB访问数据的安全性。

前提条件

- 已开通以下弹性负载均衡（Elastic Load Balance，ELB），且已在ELB中配置了与SSL证书匹配的网站域名。

  如果没有购买ELB，或数字证书所绑定的域名没有在ELB中开通服务，请不要将数字证书部署到ELB中，如果部署将可能导致部署失败。
- 已在云证书管理服务中申请SSL证书且状态为“已签发”，或者已将在其他平台签发的SSL证书上传至云证书管理服务中且状态为“托管中”。

约束条件

- 您需要在ELB中创建监听器并完成其**HTTPS配置**，才能通过CCM服务一键部署SSL证书。
- 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CCM证书的域名与其是否完全匹配。如果不完全匹配，则在CCM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CCM中证书的域名。
- 申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，由于云上没有该证书的私钥，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及私钥并进行部署。
- 国密证书暂不支持一键部署到华为云其他云产品。

说明

- 已上传的第三方证书和有效期为三个月的测试证书部署到华为云产品需要收费，每一张证书部署到华为云产品的一个域名计为一次部署，证书部署费用为30元/次。具体收费详情请参见**关于调整证书部署功能的通知**。
- 通过CCM更新ELB中的证书，可以更新部署在ELB监听器下的证书，即在CCM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。

部署证书

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“部署证书”，系统从右面弹出证书部署详细页面，如**图4-32**所示。

图 4-32 部署证书

步骤5 在部署证书页面的“部署详情”下，选择“ELB”页签。

图 4-33 选择 ELB

步骤6 单击区域名称右侧的 ▼ ，选择部署的区域。

步骤7 选择当前证书中需要部署的域名，并单击“操作”列的“更新证书”。

如需更新多个域名，则从域名列表中勾选所有待更新的域名，并单击列表左上角的“批量更新”。

步骤8 （可选）如果当前域名已经部署过该证书，单击“更新证书”后，界面会弹出重复部署仍会收费的提示框，确认无误后，单击“确定”。

步骤9 在弹出的确认框中，确认无误后，勾选“我已知悉本次部署将产生如上费用，部署成功后按需扣费，不支持退款”，单击“确认”。

图 4-34 更新证书提示信息

页面出现证书更新成功提示，表示SSL证书更新至ELB服务成功。

----结束

相关操作

因在CCM侧更新证书，会同时更新部署在ELB监听器下的证书，您可以在CCM侧查看已绑定的ELB监听器信息。

图 4-35 查看监听器信息

4.3.3 部署 SSL 证书到 CDN

SSL证书签发后，您可以将国际标准SSL证书一键部署到华为云产品CDN（Content Delivery Network，内容分发网络）中。部署后，可以帮助您提升云产品CDN访问数据的安全性。

前提条件

- 已开通CDN（Content Delivery Network，内容分发网络），且已在CDN中配置了与SSL证书匹配的网站域名。

  如果没有购买CDN，或数字证书所绑定的域名没有在CDN中开通服务，请不要将数字证书部署到CDN中，如果部署将可能导致部署失败。
- 已在云证书管理服务中申请SSL证书且状态为“已签发”，或者已将在其他平台签发的SSL证书上传至云证书管理服务中且状态为“托管中”。
- 证书为国际标准证书。

约束条件

申请证书时，如果“证书请求文件”选择的是“自己生成CSR”，由于云上没有该证书的私钥，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及私钥并进行部署。

说明

已上传的第三方证书和有效期为三个月的测试证书部署到华为云产品需要收费，每一张证书部署到华为云产品的一个域名计为一次部署，证书部署费用为30元/次。具体收费详情请参见**关于调整证书部署功能的通知**。

部署证书

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“部署证书”，系统从右面弹出证书部署详细页面，如**图4-36**所示。

图 4-36 部署证书

步骤5 在部署证书页面的“部署详情”下，选择“CDN”页签。

图 4-37 选择 CDN

步骤6 选择当前证书中需要部署的域名，并单击“操作”列的“部署”或“重新部署”。

如需部署多个域名，则从域名列表中勾选所有待部署的域名，并单击列表左上角的“批量更新”。

步骤7 （可选）如果当前域名已经部署过该证书，单击“重新部署”后，界面会弹出重复部署仍会收费的提示框，确认无误后，单击“确定”。

步骤8 在弹出的确认框中，确认无误后，勾选“我已知悉本次部署将产生如上费用，部署成功后按需扣费，不支持退款”，单击“确认”。

图 4-38 部署证书提示信息

部署成功后，界面将提示部署成功，请前往部署记录查看。

----结束

4.3.4 查看已关联云资源

您将SSL证书部署到华为云产品后，如需查看SSL证书已关联云产品的详细信息，请参照本章节处理。

前提条件

证书已部署到华为云产品。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

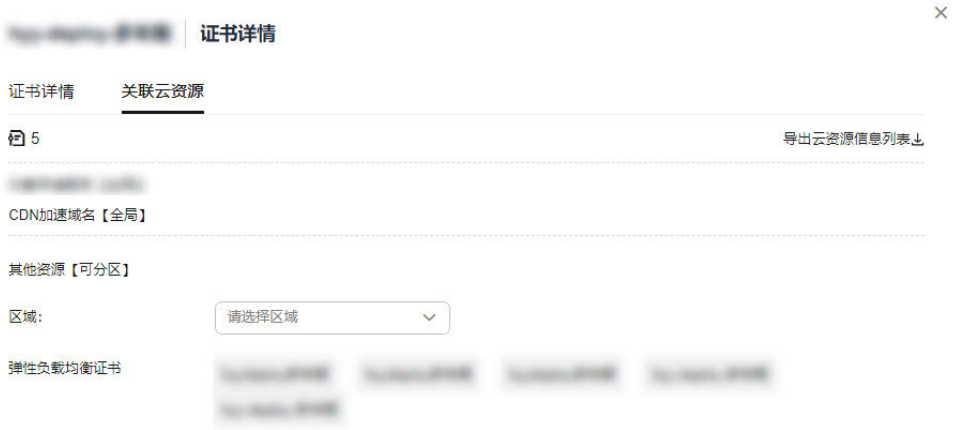
步骤3 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入SSL证书列表页面。

步骤4 选中已完成部署的SSL证书，鼠标悬浮至“关联资源”列，单击“查看详情”，系统从右侧弹出证书详情页面。

步骤5 选择“关联云资源”页签，查看证书已关联云资源，如图 关联云资源详情所示，关联云资源参数说明如表 关联云资源参数说明所示。

如需查看更详细的信息，可以单击页面右上角“导出云资源信息列表”，导出关联云资源信息列表，保存到本地查看。

图 4-39 关联云资源详情



说明

对于已过期证书，可单击“更多”查看该证书在其他云产品的部署记录。

表 4-7 关联云资源参数说明

参数名称		参数说明
全局服务	CDN加速域名	该证书已关联内容分发网络（CDN）服务中的加速域名。
可分区服务	区域	选择ELB或WAF已部署该证书的区域。
	弹性负载均衡证书	该证书已关联某区域弹性负载均衡（ELB）服务中的证书。
	Web应用防火墙防护域名	该证书已关联某区域Web应用防火墙（WAF）服务中“default”企业项目下的防护域名。 **说明** 云证书管理服务中的证书只支持部署到WAF的“default”企业项目下，因此此处仅显示证书关联WAF“default”企业项目下的云资源。

----结束

4.3.5 开启 SSL 证书到期自动替换

对于部署到华为云产品的SSL证书，如果为多年有效期或已开启自动续费的SSL证书，支持开启证书到期自动替换。

开启证书到期自动替换后，在旧证书到期前，多年期后续证书或自动续费的证书签发后24小时内将自动更新到已部署的华为云产品替换旧证书。

⚠ 注意

为了避免多年期证书自动申请失败，**请勿取消隐私授权**。

前提条件

- SSL证书已部署到华为云产品。
- 证书为多年有效期SSL证书（剩余证书张数大于0）或已为SSL证书开启自动续费。

约束条件

开启到期自动替换后，在旧证书过期前，新签发的多年期后续证书或续费证书将由云证书管理服务自动更新到已部署的华为云产品替换旧证书，为了保证证书自动替换成功，您必须在旧证书过期前配合CA机构完成新证书签发。否则，在旧证书过期后，到期自动替换功能失效，新签发的多年期后续证书或续费证书您需要手动部署到华为云产品中。

特殊场景

因CA机构每5-10年会更换一次根证书，当您在已预埋根证书的情况下使用证书自动替换功能，如果根证书已经变化，证书自动替换功能会执行失败。此时需要您手动完成证书替换。

操作步骤

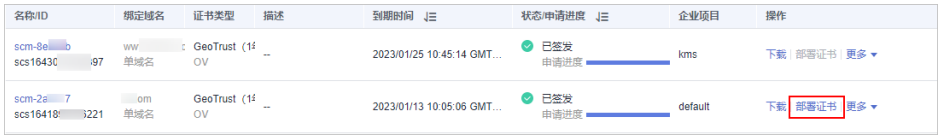
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“部署证书”，系统从右面弹出证书部署详细页面，如图4-40所示。

图 4-40 部署证书



步骤5 在证书部署详情页面中的“部署详情”栏中，选择已部署的云产品。

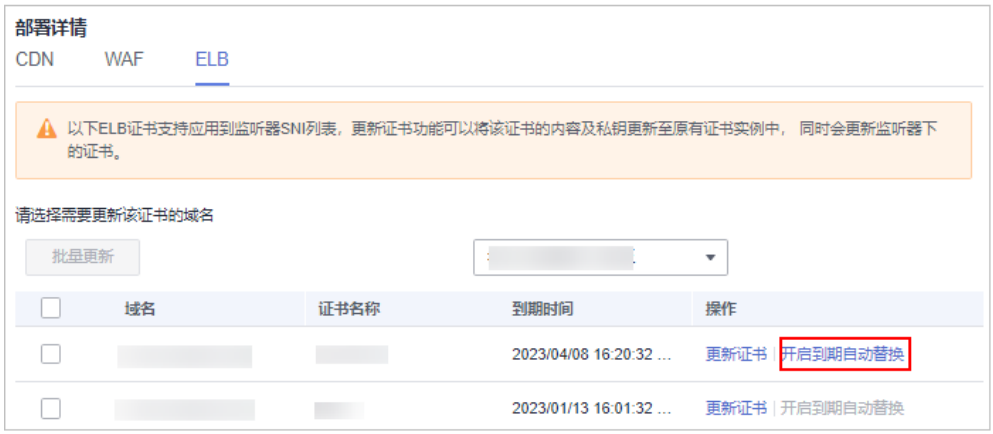
图 4-41 选择云产品

步骤6 （可选）当部署的云产品为WAF或ELB时需要执行此步骤。

单击区域名称右侧的 ▼ ，选择部署的区域。

步骤7 选择需要开启到期自动替换的域名，并单击“操作”列的“开启到期自动替换”。

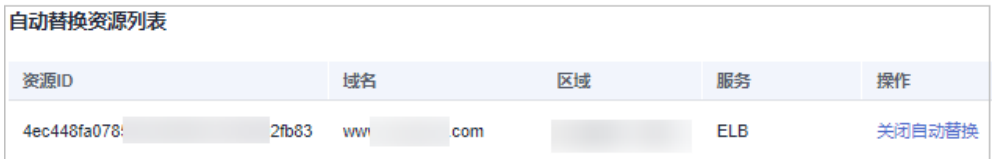
图 4-42 开启到期自动替换



步骤8 在弹出的确认框中确认信息，确认无误后单击“确认”。

步骤9 自动替换资源列表中出现该域名资源，表示开启到期自动替换成功。

图 4-43 开启到期自动替换成功



----结束

4.3.6 关闭 SSL 证书到期自动替换

部署到华为云产品的SSL证书不再需要到期自动替换，请参见本章节进行处理。

前提条件

部署到华为云产品的SSL证书已开启到期自动替换。

操作步骤

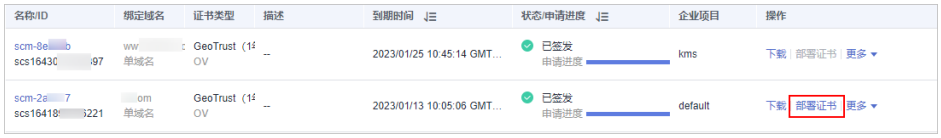
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“部署证书”，系统从右面弹出证书部署详细页面，如图4-44所示。

图 4-44 部署证书



步骤5 在自动替换资源列表中，选择需要关闭自动替换的域名，并单击“操作”列的“关闭自动替换”。

图 4-45 关闭自动替换

步骤6 自动替换资源列表中不再含有该域名资源，表示关闭自动替换成功。

----结束

5 管理 SSL 证书

5.1 重新签发

SSL证书重新签发，是指在SSL证书仍然有效时由于某些特殊原因，用户需要获取一张新的证书，而原有证书将被替换的过程。通常在下述场景下，需要重新签发SSL证书：

- 密钥泄露或丢失：如果网站的密钥泄露或丢失，为了网站的安全，建议重新签发一张新的SSL证书。
- 更改域名：如果网站更改了域名，则原有的SSL证书将不再适用，需要重新签发SSL证书以匹配新的域名。
- 证书配置错误：如果SSL证书在申请时，配置信息错误（例如，域名有误或组织信息错误），则需要重新签发SSL证书。

前提条件

- 证书状态为“已签发”。
- 证书为“单域名”、“泛域名”证书。

约束条件

- 免费证书、多域名类型证书、已吊销证书不支持重新签发。
- 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：
  - GlobalSign品牌：5天。
  - DigiCert品牌和GeoTrust品牌：25天。
  - CFCA品牌、TrustAsia品牌和vTrus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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“更多 > 重新签发”，进入“重新签发”页面，如**图 重新签发**。

图 5-1 重新签发

说明

如您遇到无法重签或找不到“重新签发”按钮的情况，请确认以下几项内容：

- 证书状态是否为“已签发”，未签发证书不可重签。
- 证书类型是否为“单域名”或“泛域名”，免费证书和多域名证书不支持重签。
- 如您的证书品牌为GlobalSign，请确认是否在证书签发后5天内，超过5天后不可重签。
- 如您的证书品牌为DigiCert、GeoTrust、CFCA 、TrustAsia或vTrus品牌，请确认是否在证书签发后25天内，超过25天后不可重签。

步骤5 如果您需要重新绑定域名，可参照**表 域名信息参数说明**进行操作，同时您也可以修改公司联系人/授权人信息。

图 5-2 重新签发页面

表 5-1 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?** 。 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。两种证书请求文件的区别请参见**系统生成的CSR和自己生成CSR的区别?** 。	系统生成CSR
绑定域名	当购买的是“单域名”、“泛域名”类型的SSL证书时，显示该参数。 ● 当“证书请求文件”选择“自己生成CSR”时，域名将根据CSR文件自动解析出来，不需要手动输入域名。 ● 当“证书请求文件”选择“系统生成CSR”时，需要手动输入证书需要绑定的域名或泛域名。 “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 “泛域名”填写示例：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，则在“绑定域名”中填写*.huaweicloud.com	www.domain.com

参数名称	参数说明	取值样例
域名验证方式	按照CA中心的规范，如果您申请了数字证书，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。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。 选择域名验证方式： ● 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：系统自动添加DNS记录验证，无需您进行任何操作。 如果您购买的是DV（域名型）证书、在华为云上申请的域名，且域名已使用华为云云解析服务，可选择此验证方式。 – 手动DNS验证：您需要前往域名的DNS解析服务商进行操作。 ● 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。 ● 邮箱验证：指登录域名管理员邮箱，接收域名确认邮件并根据提示进行操作来验证域名所有权。 **说明** ● DV域名型和DV基础版证书（GeoTrust入门级SSL证书和DigiCert免费SSL证书）默认通过“DNS验证”方式进行验证，无需进行配置。 ● 纯IP（公网IP）的证书仅支持通过“文件验证”方式进行验证，且仅纯IP证书支持“文件验证”方式验证。	手动DNS验证

步骤6 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。

当证书不在审核中，可取消隐私信息授权。取消隐私信息授权后，华为云将不再保存并删除您的相关信息（包括联系人姓名、电话、邮箱、企业信息）。具体操作请参见**取消隐私信息授权**。

步骤7 单击“提交申请”。

1. 证书重签申请提交后，证书状态将变为“CA审核中（重签）”。
2. CA机构将在1-2个工作日内通过您预留的邮箱向您发送确认取消已签发证书的邮件，确认取消并邮件回复后，CA机构会将已签发证书取消，该证书将进入重签流程。

   如果您修改了域名或者公司联系人/授权人信息，原证书取消后，证书状态为“待完成域名验证”，您需要完成**域名验证**和**组织验证（OV、EV）**(OV、OV Pro、EV和EV Pro类型证书)，才可以重新签发新的证书。

----结束

5.2 退订 SSL 证书

如果您通过华为云SSL证书管理控制台购买了SSL证书，在符合退款条件的情况下，可在SCM控制台申请退款。

本章节介绍符合退订的条件以及如何退订SSL证书。

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。
- 多年期证书，第一张证书已签发，并在下单后7个自然日内完成了证书吊销流程，支持全额退订。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要退订的证书所在行的“操作”列中，单击“退订”，如图5-3所示。

图 5-3 退订

步骤5 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6 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

5.3 续费 SSL 证书

5.3.1 手动续费

CA机构签发的SSL证书默认有效期为1年，证书过期后服务器将无法进行HTTPS加密通信，为避免证书过期影响您的业务，您可以在证书到期前手动续费证书。

手动续费限制说明

- 续费证书不支持修改公司名称。
- 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。
- 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。

前提条件

- 付费证书处于即将到期状态。
- 证书未开通自动续费。

操作步骤

1. 登录**管理控制台**。
2. 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。
3. 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。
4. 在需要续费的证书所在行的“操作”列中，单击“续费”，如**图 续费**所示。

图 5-4 续费

5. 在续费证书页面确认待续费证书信息，确认信息无误后，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。
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”。
7. 在购买页面，请选择付款方式进行付款。

   成功付款后，在SSL证书管理界面，可以查看证书列表中购买的证书。

   此时，续费购买证书的状态为待申请，您必须提交证书申请。CA中心审核通过您的续费证书申请后，才会为您签发续费证书。

后续操作

1. 提交证书申请。

   详细操作请参见**提交SSL证书申请**。

须知

填写证书申请信息时，公司名称请保持与旧证书一致，续费证书不支持修改公司名称。

2. 域名验证。
   详细操作请参见**域名验证**。
3. （OV、EV型）组织验证。
   详细操作请参见**组织验证**。
4. 签发证书。
   以上操作完成后，请您耐心等待，CA机构将还需要一段时间进行处理。CA机构审核通过后，将会签发证书。
5. 安装证书。
   将已签发的续费证书安装到您的Web服务器，替换即将过期的旧证书。如果您没有在Web服务器中安装续费证书，则在旧证书过期后，您的服务器将无法正常使用HTTPS服务。
   不同Web服务器安装SSL证书的具体操作不同，以下介绍了几种在主流Web服务器上安装SSL证书的方法，请根据您的需要进行选择：
   - **在Tomcat服务器上安装SSL证书**
   - **在Nginx服务器上安装SSL证书**
   - **在Apache服务器上安装SSL证书**
   - **在IIS服务器上安装SSL证书**
   - **在Weblogic服务器上安装SSL证书**
   - **在Resin服务器上安装SSL证书**
6. 查看续费证书是否安装成功。
   续费证书安装到Web服务器后，可通过浏览器查看证书是否已更新。
   a. 通过Web浏览器访问您的网站。
   b. 单击浏览器地址栏的  ，查看证书的有效期是否已更新。
      如果证书有效期已显示为新证书的有效期，表示您的续费证书已完成更新。

图 5-5 有效期

5.3.2 自动续费

为避免证书到期未及时续费，您可以设置开通自动续费。开通自动续费后，系统将在证书即将到期前30天内自动续费购买证书。

⚠ 注意

为了避免证书自动申请失败，**请勿取消隐私授权**。

自动续费限制说明

- 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。
- 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) 泛域名证书自动续费在证书到期前**15个自然日内**触发。
- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要续费的证书所在行的“自动续费”列中，单击  ，开启自动续费。

----结束

后续操作

1. 域名验证。
   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，详细操作请参见域名验证。

2. （OV、EV）组织验证。

   验证您是否发起了证书申请，详细操作请参见**组织验证**。

3. 签发证书。

   以上操作完成后，请您耐心等待，CA机构将还需要一段时间进行处理。CA机构审核通过后，将会签发证书。

4. 安装证书。

   将已签发的续费证书安装到您的Web服务器或部署到华为云产品，替换即将过期的旧证书，详细操作请参见**安装SSL证书**。

5. 查看续费证书是否安装成功。

   续费证书安装到Web服务器后，可通过浏览器查看证书是否已更新。

   a. 通过Web浏览器访问您的网站。

   b. 单击浏览器地址栏的  ，查看证书的有效期是否已更新。

      如果证书有效期已显示为新证书的有效期，表示您的续费证书已完成更新。

图 5-6 有效期

5.4 吊销 SSL 证书

吊销证书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。

如果您不再需要某张已签发的SSL证书或某张SSL证书密钥丢失或出于其他安全因素考虑，可以在SSL证书管理控制台申请吊销证书。

吊销证书后，将清除该证书所有的记录，包括CA机构的记录，且无法恢复，请谨慎操作。

证书被吊销后，不支持**重新签发**，但满足一定条件下，支持**重新申请**。

前提条件

证书的状态为“已签发”。

约束条件

- 仅支持吊销已签发的证书。
- 上传的证书无法吊销。
- 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。
- 吊销证书申请提交后，将无法取消，但是证书吊销不影响再次购买新证书。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要吊销的证书所在行的“操作”列中，单击“吊销”或单击“更多 > 吊销”，如**图5-7**所示。

图 5-7 吊销证书按钮

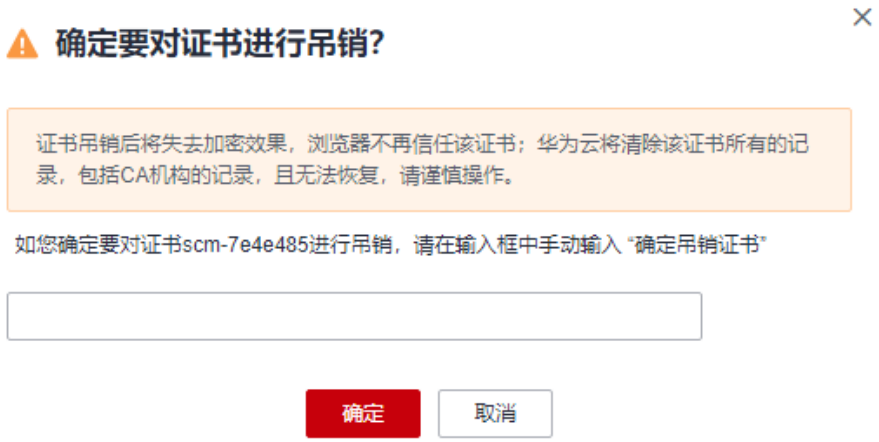
步骤5 在弹出的对话框中，输入“确定吊销证书”，单击“确定”。

在页面的右上角弹出“吊销证书成功”，表示吊销证书申请已成功提交审核，等待CA机构审核通过后即吊销成功。

须知

吊销证书申请提交后，将无法取消，请谨慎操作。

图 5-8 吊销证书提示



步骤6 （可选）如果您要吊销的是OV、EV证书，您需要完成邮件确认。

提交证书吊销申请后，CA中心会向您的联系人邮箱（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。

----结束

5.5 重新申请已吊销的 SSL 证书

SSL证书吊销后，满足一定条件下，CCM会返回您未使用的证书额度，支持重新申请SSL证书，可节约证书的使用成本。

前提条件

证书的状态为“已吊销”。

约束条件

- 免费证书吊销后，不支持重新申请。
- 不同品牌的证书被吊销后，重新申请时需满足如下限制：
  - GlobalSign证书签发后，在6天之内吊销，支持重新申请。
  - 其余品牌证书签发后，在28天之内吊销，支持重新申请。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“重新申请”。

图 5-9 选择重新申请

步骤5 在重新申请页面，填写申请信息。

- 您可以基于上次申请证书时填写的信息进行重新申请，也可以修改已有信息。
- 各参数详情，请参见**提交SSL证书申请**。

图 5-10 填写重新申请信息

步骤6 确认填写信息无误后，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勾选框，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**。

----结束

5.6 删除 SSL 证书

删除证书是指将SSL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。

本章节介绍如何删除不需要的证书。

前提条件

- 付费证书状态为“已签发”、“已吊销”或“已到期”。
- 免费证书状态为“待申请”、“已吊销”或“已到期”。

- 上传的证书状态为“托管中”。

约束条件

- 暂不支持在云证书管理控制台上对处于“已签发”状态的免费证书执行删除操作，如果您想要删除处于“已签发”状态的免费证书，您可以使用API接口进行删除，详情请参见**删除证书**。
- 证书删除后，华为云平台将不再保管您的证书，证书文件与私钥需要您自行保管，因此建议您只删除不需要的证书。
- 证书删除后，无法恢复，请谨慎操作。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要删除的证书所在行的“操作”列，单击“删除”或单击“更多 > 删除”。

说明

如需批量删除证书，请勾选需要删除的证书后，单击左上角“删除”。

步骤5 在弹出的对话框中，单击“确定”，页面右上角弹出“删除证书成功”，完成证书删除。

----结束

5.7 上传已有 SSL 证书

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。证书上传后，均支持证书下载、证书到期提醒设置，另外国际标准证书支持部署到华为云其他云产品。

该任务指导您如何在本地将外部SSL证书上传到云证书管理平台。

前提条件

已准备好需要上传证书的相关文件，具体如下：

- PEM编码格式的证书文件（文件后缀是PEM或者CRT）。
- PEM编码格式的证书私钥文件（文件后缀是KEY）。

说明

- 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?**。

  更多关于证书链的相关配置请参见**证书链配置说明**。
- 证书私钥需要是无密码保护的，更多详细介绍请参见**为什么要使用无密码保护的私钥?**。
- 上传的证书，SCM会在证书到期前30天提醒您证书即将到期，同时还支持配置消息提醒，设置后SSL证书管理系统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，具体配置操作请参见**如何配置SSL证书到期提醒?**。

约束与限制

- 不支持上传已过期的证书。
- 不支持上传证书链长度为1的证书，即待上传的证书必须包含证书链，不能是单张证书。
- 待上传的证书的CN必须是域名DNS格式或者IP格式。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击“上传证书”页签，进入上传证书管理界面，在上传证书列表左上角，单击“上传证书”，进入“上传证书界面”。

图 5-11 上传证书

步骤5 在“上传证书”对话框中，输入证书信息，如**图5-12**所示，上传国际标准证书参数说明如**表 上传国际标准证书参数说明**所示，上传国密（SM）证书参数说明如**表 上传国密（SM）证书参数说明**所示。

图 5-12 上传原有证书

表 5-2 上传国际标准证书参数说明

参数	说明
证书标准	选择国际标准证书。
证书名称	用户自定义。
企业项目	将上传的SSL证书分配至对应的企业项目中。
证书文件	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”），将证书内容复制到此处。 按照“服务器证书-证书链”的顺序依次排列上传。具体方法请参见**如何上传证书文件?** 。
证书私钥	以文本方式打开待上传证书里的KEY格式的文件（后缀名为“.key”），将私钥内容复制到此处。

表 5-3 上传国密（SM）证书参数说明

参数	说明
证书标准	选择国密（SM）证书。
证书名称	用户自定义。
企业项目	将上传的SSL证书分配至对应的企业项目中。
签名证书	以文本方式打开待上传证书里的签名证书PEM格式的文件（后缀名为“.pem”），将证书内容复制到此处。 按照“服务器证书-证书链”的顺序依次排列上传。具体方法请参见**如何上传证书文件？**。
签名私钥	以文本方式打开待上传证书里的签名私钥KEY格式的文件（后缀名为“.key”），将私钥复制到此处。
加密证书	以文本方式打开待上传证书里的加密证书PEM格式的文件（后缀名为“.pem”），将证书内容复制到此处。 此处无需上传证书链。
加密私钥	以文本方式打开待上传证书里的加密私钥KEY格式的文件（后缀名为“.key”），将私钥内容复制到此处。

说明

- 上传的原有证书和密钥必须是一一对应的。
- 保证私钥无密码保护，更多详细介绍请参见**为什么要使用无密码保护的私钥？**。
- 如您在上传证书时遇到报错提示，请参见**上传SSL证书时可能有哪些报错，如何解决？**。

步骤6 单击“确定”，完成上传证书。

证书上传成功，证书列表中新增一条状态为“托管中”的证书。

上传的国际标准证书可以部署到云产品中。

----结束

相关操作

上传国际标准证书可部署到华为云其他云产品中，具体操作请参见**部署国际标准SSL证书到华为云产品**。

5.8 新增附加域名

如果您购买的是多域名类型的SSL证书，且该证书有可追加附加域名的额度，您可以在证书签发后，增加附加域名。

本章节介绍如何新增附加域名。

前提条件

- 证书状态为“已签发”。
- 待新增附加域名的证书有可追加附加域名的额度。

约束条件

- 证书有效期以第一次签发日开始计算。
- 新增附加域名提交审核后，当前证书仍然可以下载（下载的证书不适用于审核中的附加域名）。
- 待新增的附加域名审核完成，证书签发后，即可下载新的证书。原有证书将不再提供下载，用户需自行保存原有证书。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“更多 > 新增附加域名”，弹出“新增附加域名”对话框。

步骤5 在对话框中，补全新增附加域名的信息，如**图5-13**所示，参数说明如**表5-4**所示。

图 5-13 新增附加域名

表 5-4 参数说明

参数名称	参数说明	取值样例
新增附加域名	输入此次需要添加的附加域名。	domain03.com domain04.com

参数名称	参数说明	取值样例
联系人邮箱	请填写正确的邮箱地址。证书提交审核后华为云将会向您的邮箱发送通知邮件（证书签发通知），请注意及时查收。 **须知** CA中心发来的认证邮件将发送到域名管理员的邮箱，请您提交审核后务必第一时间登录域名管理员的邮箱进行查收和认证。	-

步骤6 单击“确定”。

新增附加域名完成，页面进入到SSL证书管理界面，状态更新为“CA审核中（追加域名）”。

----结束

后续处理

提交审核后，证书颁发机构将向您填写的邮箱发送一封域名验证邮件，您需要按照需求进行域名验证。如果您不进行域名验证，您的证书将一直处于“CA审核中（追加域名）”状态，且您的证书将无法通过审核。验证时间根据不同CA中心的要求而不同，请您关注您的邮箱和电话，及时回馈能有效缩短您的数字证书的验证时间。

新增附加域名仅需进行域名验证，待域名验证完成，CA系统中心审核通过后，即可签发证书。

域名验证详细操作请参见**域名验证**。

相关操作

新增域名审核提交后，如需更改新增加的域名或修改联系人邮箱，则可以撤回申请。操作步骤如下：

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“撤回申请”，弹出“取消申请流程”提示框。

步骤5 在弹出的“取消申请流程”提示框中，单击“确定”。

页面右上角弹出“取消申请流程成功”，则说明取消申请流程提交成功。

此时，证书的状态仍然为“CA审核中（追加域名）”，待服务审核取消申请流程通过后，取消申请成功，证书的状态切换为“已签发”。

----结束

5.9 撤回 SSL 证书申请

该任务指导用户撤回申请。

当用户已提交审核，域名注册平台DNS或者用户信息正在审核中，此时用户可以撤回申请。

撤回后，CA将终止审核，请谨慎操作。需要注意，由于处理流程的原因，可能您选择撤回时CA已经审核通过，那么您的撤回申请将会失败。因此，是否撤回成功以华为云SCM证书列表呈现最终状态为准。

前提条件

证书状态为“待完成域名验证”、“待完成组织验证”或“CA审核中（追加域名）”。

约束条件

- 证书未签发前，可通过撤回证书申请，修改域名或相关信息；证书签发后，如果需要更改绑定的域名，“单域名”和“泛域名”证书可以在规定的时间内重新签发证书，详细操作请参见**重新签发**。
- 删除和吊销证书的申请提交后，无法撤回。
- 撤回证书成功后，证书状态处于“待申请”，您需要重新完成“提交证书申请 > 域名验证 > 组织验证”，才可以签发证书。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标证书所在行的“操作”列，单击“撤回申请”，如**图5-14**所示。

图 5-14 撤回申请

步骤5 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”。

须知

撤回后，CA将终止审核，请谨慎操作。需要注意，由于处理流程的原因，可能您选择撤回时CA已经审核通过，那么您的撤回申请将会失败。因此，是否撤回成功以华为云SCM证书列表呈现最终状态为准。

----结束

相关操作

证书申请撤回成功后，证书的状态切换为“待申请”，可再次申请证书，具体操作请参见**提交SSL证书申请**。

5.10 取消隐私信息授权

该任务指导用户取消隐私信息授权。

当用户申请证书后，除了证书的状态处于审核中（即“待完成域名验证”、“待完成组织验证”、“即将签发”和“CA审核中（追加域名）”）之外，其他的状态中用户可以取消隐私信息授权。

取消隐私信息授权后，华为云将不再保存并删除您的相关信息（包括联系人姓名、电话、邮箱、企业信息）。

前提条件

- 已完成申请证书操作。
- 证书状态不在审核中（即“待完成域名验证”、“待完成组织验证”、“即将签发”和“CA审核中（追加域名）”）。

约束条件

- 当证书的状态处于审核中（即“待完成域名验证”、“待完成组织验证”、“即将签发”和“CA审核中（追加域名）”）时，不可以取消隐私信息授权。
- 取消隐私信息授权后，该证书所属的所有隐私信息将无法恢复，请谨慎操作。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击需要取消授权信息的证书名称，系统从右面弹出证书详情页面。

步骤5 在证书详情的页面最下方，找到“隐私授权”配置项。

图 5-15 隐私授权

步骤6 关闭隐私授权。

步骤7 在弹出的“取消隐私信息授权”对话框中，单击“确定”。

页面右上角弹出“您已成功取消隐私信息授权”，则说明取消隐私信息授权成功。

证书详情页面的申请人/组织信息详情页面将不会显示您的相关信息。

----结束

5.11 推送 SSL 证书到云产品

SSL证书签发后，您可以将SSL证书一键推送到弹性负载均衡（Elastic Load Balance，简称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。推送后，可以帮助您提升云产品访问数据的安全性。

前提条件

证书的状态为“已签发”或者“托管中”。

约束条件

- 推送WAF的场景下，可选择推送证书至不同企业项目下。
- 推送到CDN中，**不能**与CDN中已有SSL证书名称重复，否则将会推送失败。
- 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**推送到云产品。
- 如果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，请不要将数字证书推送到对应的云产品中，如果推送将可能导致推送失败。
- 如果您已将证书推送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平台推送时，将会推送失败。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在需要推送的证书所在行的“操作”列，单击“更多 > 推送”，系统从右面弹出证书推送详细页面。

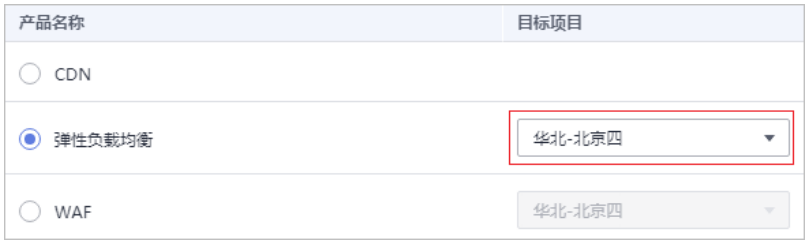
步骤5 选中需要推送的云产品。

图 5-16 选择云产品

步骤6 （可选）设置推送区域，当推送到ELB、WAF时，需要执行该步骤。

单击目标项目右侧的 ▼ ，选择推送的区域，您可以同时勾选多个区域（最多可勾选10个区域），实现多区域的证书推送。

图 5-17 选择推送区域



步骤7 在页面右下角单击“推送”。

页面出现推送证书成功提示，表示SSL证书推送给目标服务成功。

此时，您还需要在目标服务中进行证书配置操作才能在目标服务中正确启用HTTPS服务。

步骤8 确认是否需要立即前往目标服务进行证书配置操作。

- 是，单击“立即前往配置”，系统将进入目标服务管理页面，请进行证书配置操作。
- 否，单击“继续推送”或单击页面右上角的 ✕ ，系统将返回到证书推送页面或SSL证书管理界面。

  您可以后续自行前往目标服务页面进行证书管理配置操作。

您可在证书推送界面，查看最近10条推送记录。

----结束

后续操作

证书推送成功后，需要前往目标服务页面进行证书管理配置操作。

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。

- ELB：如果需要支持HTTPS数据传输加密认证，在创建HTTPS协议监听的时候需绑定证书。此时，如果选择一键推送证书到ELB，则可以在ELB中选择已推送的证书。否则，需要手动上传证书。具体操作请参见**ELB证书管理**文档。

另外，一般的HTTPS业务场景只对服务器做认证，因此只需要配置服务器的证书即可，某些关键业务（如银行支付），需要对通信双方的身份都要做认证，即双向认证，以确保业务的安全性。双向认证具体操作请参见**HTTPS双向认证**。

- CDN：如果需要实现HTTPS安全加速，则需要通过配置加速域名的HTTPS证书，并将其部署在全网CDN节点。此时，如果选择一键推送证书到CDN，则可以在CDN中选择已推送的证书。否则，需要手动上传证书。具体操作请参见**CDN证书配置**文档。

  说明

  - 如需部署证书到CDN，请参见**部署SSL证书到CDN**章节。
  - 已上传的第三方证书和有效期为三个月的测试证书部署到华为云产品需要收费，每一张证书部署到华为云产品的一个域名计为一次部署，证书部署费用为30元/次。具体收费详情请参见**关于调整证书部署功能的通知**。

- WAF：当接入防护域名至WAF时，如果客户端与WAF之间的通信采用HTTPS协议，则需要配置证书。此时，如果选择一键推送证书到WAF，则可以在WAF中选择已推送的证书。否则，需要手动上传证书。具体操作请参见**WAF证书配置**文档。

  如果已配置证书到WAF中，仅需要更新证书，具体操作请参见**更新证书**。

5.12 分配 SSL 证书至企业项目

企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。更多关于企业项目的信息，请参见**《企业管理用户指南》**。

该任务指导用户如何将SSL证书分配至对应的企业项目中。

前提条件

- 已创建企业项目。如需使用该功能，请**开通企业管理功能**。
- 购买证书的账号拥有“EPSFullAccess”权限。

  说明

  EPSFullAccess：企业项目管理服务所有权限，具体操作请参见**权限管理**。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在目标SSL证书所在行的“操作”列，单击“分配至项目”。

步骤5 在弹出的对话框中，选择迁入的企业项目。

图 5-18 分配至项目

步骤6 单击“确定”。

----结束

5.13 查看 SSL 证书详情

该任务指导用户查看已购买证书的详细信息，包括已购买的付费证书和测试证书以及上传的第三方证书。

您还可以参考本章节进行查看证书审核进度、修改证书名称和描述的操作，以及证书是否即将到期的提醒。托管中和已签发的证书到期前30天，云证书管理控制台在SSL证书列表的“状态/申请进度”栏会提示您有即将到期的证书。

前提条件

已购买证书或者已上传原有证书。

操作步骤

步骤1 登录**管理控制台**。

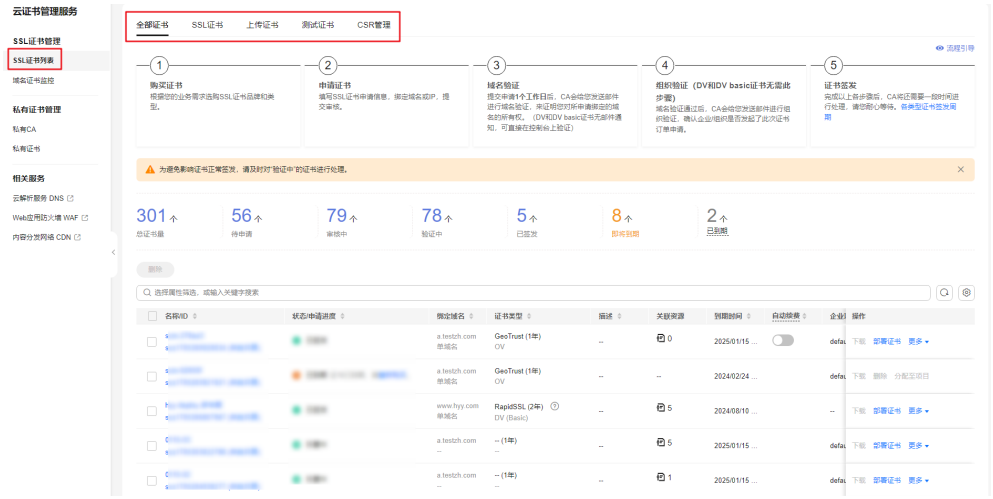
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 查看证书信息，如**图 证书列表**，证书参数说明如**表 证书参数说明**所示。

- 查看全部证书信息，请单击“全部证书”页签
- 查看付费证书信息，请单击“SSL证书”页签。
- 查看上传证书信息，请单击“上传证书”页签。
- 查看测试证书信息，请单击“测试证书”页签。

图 5-19 证书列表



说明

- 在搜索栏选择证书筛选条件，并输入相应内容，单击或按“Enter”，可以搜索指定的证书。
- 单击证书名称，可以查看证书的详细信息。
- 托管中和已签发的证书到期前30天，云证书管理控制台在SSL证书列表的“状态/申请进度”栏会提示您有即将到期的证书。
- 如果您的某张证书已经到期超过30天，SSL证书列表会自动折叠该证书，不会在证书列表显示，如需查看该证书详情，需要您在SSL证书列表进行手动筛选。
- 在云证书管理服务中，SSL证书管理仅支持保存过期3年以内的证书。

表 5-5 证书参数说明

参数名称	说明
名称/ID	成功购买证书后，证书名称由系统自动生成，用户可以修改证书名称。具体操作请参见**修改证书名称和描述**。

参数名称	说明
状态/申请进度	证书状态/申请进度说明如下： • 待申请 购买的证书需要提交域名和用户信息。具体操作请参见**提交SSL证书申请**。 申请进度为0%。 • 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**。 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（OV、EV）**。 申请进度为70%。 • 即将签发 购买的证书已完成申请证书、域名验证和组织验证，正在等待CA机构签发证书。 申请进度为90%。 • 已签发 域名验证、组织验证成功以及用户信息验证通过。 申请进度为100%。 • 审核失败 用户信息验证失败。 • CA审核中（重签） 已签发的证书执行了重新签发操作，正在等待CA机构审核。具体操作请参见**重新签发**。 • CA审核中（追加域名） 多域名证书已提交追加域名的申请，CA机构正在对新增的附加域名进行审核。具体操作请参见**新增附加域名**。 • CA审核中（撤回申请） 购买的证书已提交撤回申请，正在等待CA机构审核。具体操作请参见**撤回证书申请**。 • CA审核中（吊销） 购买的证书已提交吊销申请，正在等待CA机构审核。 • 已吊销 证书已吊销。 • 托管中 上传的证书的状态为托管中。 • 已到期 证书已到期。证书到期后无法续费，只能重新购买并申请新证书。 • 吊销审核中（待域名验证） 已提交吊销证书的请求，需要按照CA机构的要求完成域名授权验证。

参数名称	说明
绑定域名	证书绑定的域名信息。
证书类型	购买证书时选择的证书类型。
描述	证书的补充信息，用户可以修改描述内容。具体操作请参见**修改证书名称和描述**。
关联资源	显示当前证书已关联的所有云服务资源，如需查看关联资源详情，请参见**查看已关联云资源**。
到期时间	证书到期的日期。 **说明** 已签发的证书，系统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。
自动续费	可选择开启 或关闭 自动续费。关于自动续费详情请参见**自动续费**。
企业项目	显示当前证书所属企业项目名称。
操作	用户可以在操作栏中，执行申请证书、域名验证、组织验证、撤销申请等操作。

----结束

修改证书名称和描述

说明

共享证书不支持修改名称和描述。

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击需要修改的证书名称，系统从右面弹出证书的详情页面。

步骤5 修改证书名称和描述。

单击“证书名称”（或“描述”）栏后的 展开编辑框，在编辑框中输入证书名称（或描述信息）后，单击 保存修改的信息，页面右上角弹出“修改成功”，则说明修改证书名称（或描述信息）成功，如**图5-20**所示。

注意

修改证书名称会造成账单实际出账名称和证书修改后名称不一致，请谨慎修改。

图 5-20 修改证书名称和描述

----结束

5.14 查看申请进度

该任务指导用户查看已提交申请的证书的审核进度。

用户可根据申请进度中的提示执行对应操作，以便尽快获取证书。

前提条件

- 已购买证书。
- 已提交证书申请。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 在待查看审核进度的证书所在行的“状态/申请进度”列，查看证书的申请进度，如**图5-21**所示。

图 5-21 查看申请进度

查看后，请根据证书状态进行对应操作。以下为几个重要操作的示例：

- 待申请：此时代表您购买的证书还未提交证书申请，您需要手动提交，具体操作请参见**提交SSL证书申请**。
- 待完成域名验证：此时代表您已提交申请证书的请求，但还未完成域名验证，您需要按照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**。
- 待完成组织验证：当您购买和申请了OV或EV类型证书时，除了需要完成域名验证以外，CA机构还会进行一次组织验证，以确认您的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（OV、EV）**。
- 即将签发：此时代表您已完成域名验证、组织验证等操作，等待CA机构审核中，请您耐心等待。

待所有信息验证通过后，证书“状态”更新为“已签发”。

----结束

5.15 CSR 管理

如您需要生成基于RSA、ECC、SM2（国密）密钥算法的CSR和私钥或上传已有的CSR，并对其进行统一管理，可参考本章节。

5.15.1 创建 CSR

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击“创建CSR”。

步骤5 在弹出页面完成参数配置，如**图 创建CSR**。

图 5-22 创建 CSR

参数说明如**表 参数说明**。

表 5-6 参数说明

参数名称	参数说明
CSR名称	为创建的CSR自定义一个名称。 支持使用英文大小写字母（a~z和A~Z）、阿拉伯数字（0~9）、下划线（_）、短划线（-）。长度不超过50个字符。
绑定域名/IP	填写要申请证书的域名。 如果您想在提交证书申请时使用该CSR，必须确保证书绑定域名包含此处设置的域名。 示例：假设您在此处设置域名为huaweiyun.com，则证书申请中的证书绑定域名必须包含huaweiyun.com，才可以匹配到该CSR。
绑定附加域名	填写与已设置的域名共用一张证书的其他域名。支持填写多个域名，多域名之间使用半角逗号（,）分隔。

参数名称	参数说明
密钥算法	选择密钥算法的类型。可选项： • RSA_2048 • RSA_3072 • RSA_4096 • EC_P256 • EC_P384 • SM2
CSR用途	选择您生成的CSR用途。可选项： • 个人证书 • 企业证书 当选择CSR用途为企业证书时，需填写您的“公司名称”和所在“国家/地区”。

步骤6 单击“确定”生成CSR。

----结束

后续操作

- 完成创建CSR后，您可以在CSR列表 查看已创建的CSR详情。
- 后续您在提交证书申请时，可以将**CSR生成方式**设置为**选择已有的CSR**并从匹配到的CSR中选择目标CSR。

  说明

  您还可以在CSR列表的操作栏对现有CSR进行“编辑”和“删除”操作。
  - 编辑操作仅支持修改CSR名称。
  - 删除CSR后无法恢复，请谨慎操作。

5.15.2 上传 CSR

如您在申请证书时需要使用未在云证书管理服务控制台创建的CSR，可参考本章节上传已有的CSR，并对其进行统一管理。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击“上传CSR”。

步骤5 在弹出页面单击上传，分别上传证书文件和证书私钥，如图 上传CSR。

图 5-23 上传 CSR

表 5-7 参数说明

参数名称	参数说明
CSR名称	为创建的CSR自定义一个名称。 支持使用英文大小写字母（a~z和A~Z）、阿拉伯数字（0~9）、下划线（_）、短划线（-）。长度不超过50个字符。
证书文件	上传目标CSR文件 单击文本框下的“上传”并选择存储在本地计算机的CSR文件，将文件内容上传到文本框。
证书私钥	上传证书私钥文件 单击文本框下的“上传”并选择存储在本地计算机的证书私钥文件，将文件内容上传到文本框。

步骤6 单击“确定”完成CSR上传。

----结束

后续操作

- 完成上传CSR后，您可以在CSR列表 查看已上传的CSR详情。
- 后续您在提交证书申请时，可以将**CSR生成方式**设置为**选择已有的CSR**并从匹配到的CSR中选择目标CSR。

  说明

  您还可以在CSR列表的操作栏对现有CSR进行“编辑”和“删除”操作。
  - 编辑操作仅支持修改CSR名称。
  - 删除CSR后无法恢复，请谨慎操作。

6 共享

6.1 共享概述

共享简介

云证书管理服务提供共享功能，用户可以将账号A的SSL证书同时共享给同一组织单元内的所有成员账号，这些账号可以将这些共享证书部署到ELB、WAF和CDN等服务，以启用HTTPS协议，比如账号B、账号C等。

- 账号A是SSL证书所有者，以下简称为所有者。
- 账号B、账号C均属于SSL证书接受者，以下简称为接受者。

SSL 证书所有者和接受者权限说明

所有者可以对SSL证书执行任何操作，接受者仅可以执行部分操作，接受者支持的操作说明如**表 SSL证书接受者支持的操作列表**所示。

表 6-1 SSL 证书接受者支持的操作列表

角色	支持的操作	操作说明
接受者	scm:cert:get	通过控制台或API进行访问
	scm:cert:getApplicationInfo	通过控制台或API进行访问
	scm:cert:getDomainValidation	通过控制台或API进行访问
	scm:cert:listDeployedResources	通过控制台或API进行访问
	scm:cert:listCertificatesByTag	通过控制台或API进行访问
	scm:cert:listTagsByCertificate	通过控制台或API进行访问

角色	支持的操作	操作说明
	scm:cert:listAllTags	通过控制台或API进行访问
	scm:cert:push	通过控制台或API进行访问
	scm:cert:listPushHistory	通过控制台或API进行访问
	scm:cert:enableAutoDeploy	通过控制台或API进行访问
	scm:cert:listAutoDeployedResources	通过控制台或API进行访问
	scm:cert:deployResources	通过控制台或API进行访问
	scm:cert:listDeployResourcesHistory	通过控制台或API进行访问
	scm:cert:getDeployQuota	通过控制台或API进行访问

支持共享的资源类型和区域

当前SCM服务支持共享的资源类型和区域如**表 SCM服务支持共享的资源类型和区域**所示。

表 6-2 SCM 服务支持共享的资源类型和区域

云服务	资源类型	支持共享的区域
SCM	cert：SSL证书	ALL

计费说明

关于SCM的计费可参见**计费项**。

共享证书的计费，由证书拥有者支付证书购买等费用。即所有共享资源产生费用均由资源拥有者账号产生。

6.2 创建共享

操作场景

要共享您拥有的资源给其他账号使用时，请创建共享。创建共享的流程分为指定共享资源、权限配置、指定使用者以及配置确认。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 单击页面右上角的“创建共享”，进入“创建共享”页面。

步骤5 选择资源类型为“scm:cert”，选择对应区域，勾选需进行共享的SSL证书。单击“下一步：权限配置”。

步骤6 进入“权限配置”页面，选择指定资源类型支持的共享权限，配置完成后，单击页面右下角的“下一步：指定使用者”。

步骤7 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

表 6-3 参数说明

参数名称	参数说明
使用者类型	• 组织 关于组织创建相关操作可参见**创建组织**。 **说明** 如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”。具体操作可参见**启用与组织共享资源**。 • 华为云账号ID

步骤8 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成资源共享实例的创建。

说明

共享创建完成后，RAM会向指定的使用者发送共享邀请，如果指定的使用者类型为“华为云账号ID”时，使用者需接受共享邀请后，才可以访问和使用被共享的资源；如果指定的使用者类型为“组织”时，组织中的账号无需接受邀请即可访问和使用被共享的资源。

----结束

6.3 更新共享

用户可以随时更新资源共享实例，支持更新共享实例的名称、描述、标签、共享的资源、共享权限以及共享使用者。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 在共享管理列表中选择需要更新的共享，单击“操作”列的“编辑”。

步骤5 进入“指定共享资源”页面，您可根据需要更新共享的名称、描述、标签以及增加或删除共享的资源。

步骤6 更新完成后，单击页面右下角的“下一步：权限配置”。

步骤7 进入“权限配置”页面，您可根据需要增加或删除“scm:cert”支持的共享权限，更新完成后，单击页面右下角的“下一步：指定使用者”。

步骤8 进入“指定使用者”页面，您可根据需要增加或删除共享密钥的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

步骤9 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成共享的更新。

----结束

6.4 查看共享

用户可以通过共享管理列表查看所有已创建共享的详情，并支持在列表中进行搜索、编辑和删除共享的操作，便于管理共享。同时用户可以查看已被共享的资源以及资源使用者。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 在列表中单击需要查看的共享实例名称，进入共享详情页，查看该共享的详细配置。

说明

支持用户查询已被共享的SSL证书资源以及资源使用者，具体操作请参见**查看您共享的资源**、**查看资源使用者**。

----结束

6.5 接受/拒绝共享邀请

用户可以通过共享管理列表查看共享邀请，并确认是否接受邀请。

约束条件

- 如果资源所有者与您属于同一组织，且启用“启用与组织共享资源”功能，将自动获得共享资源的访问权限，无需接受邀请。
- 如果资源所有者与您不属于同一组织，或者属于同一组织但未启用“启用与组织共享资源”功能，将收到加入资源共享实例的邀请。
- 资源共享实例的邀请默认保留7天，如果在到期前未接受邀请，系统会自动拒绝邀请，如还需使用共享资源，请再次创建共享实例以生成新的邀请。

说明

若需要启用“启用与组织共享资源”功能，具体操作请参见**启用与组织共享资源**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“共享给我 > 共享管理”，进入共享管理页面。

步骤4 单击“待接收共享”，在列表中选择需要接受或拒绝的共享，在操作列单击“接受”或“拒绝”。

步骤5 在弹出的对话框中，单击“确认”。

步骤6 接受共享邀请后，在“已接受共享”页面中可以查看所有已接受的共享。

说明

接受邀请后，可以查看使用的共享资源以及资源所有者，具体操作请参见**查看您共享的资源**、**查看资源使用者**。

----结束

6.6 退出共享

若用户不再需要访问共享的SSL证书资源，可以随时退出共享。退出共享后，用户将失去对SSL证书的访问权限。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“共享给我 > 共享管理”，进入共享管理页面。

步骤4 单击“已接收共享”，在列表选择需要退出的共享实例，单击“退出”。

步骤5 在弹出的对话框中，单击“退出”，即可完成退出共享实例。

----结束

7 标签管理

7.1 标签概述

操作场景

标签可以对SSL证书进行标识，当您拥有多张证书需要统一管理时，可以使用标签按各种维度（例如用途、所有者或环境等）对其进行分类。

您可以在购买证书时添加标签，也可以在证书购买完成后，在证书资源的详情页添加标签。

标签命名规则

- 每个标签由一对键值对（Key-Value）组成。
- 每个SSL证书最多可以添加20个标签。
- 对于每个证书资源，每个标签键（Key）都必须是唯一的，每个标签键（Key）只能有一个值（Value）。
- 标签共由两部分组成：“标签键”和“标签值”，其中，“标签键”和“标签值”的命名规则如**表 标签参数说明**所示。

  说明

  如您的组织已经设定云证书管理服务的相关标签策略，则需按照标签策略规则为SSL证书添加标签。标签如果不符合标签策略的规则，则可能会导致SSL证书标签添加失败，请联系组织管理员了解标签策略详情。

表 7-1 标签参数说明

参数	规则	样例
标签键	• 必填。 • 对于同一个SSL证书，标签键唯一。 • 长度不超过128个字符。 • 首尾不能包含空格。 • 不能以_sys_开头。 • 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符“_”、“.”、“:”、“=”、“+”、“-”、“@”	cost
标签值	• 可以为空。 • 长度不超过255个字符。 • 首尾不能包含空格。 • 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符“_”、“.”、“:”、“=”、“+”、“-”、“@”	100

7.2 创建标签策略

标签策略简介

标签策略是策略的一种类型，可帮助您在组织账号中对资源添加的标签进行标准化管理。标签策略对未添加标签的资源或未在标签策略中定义的标签不会生效。

例如：标签策略规定为某资源添加的标签A，需要遵循标签策略中定义的大小写规则和标签值。如果标签A使用的大小写、标签值不符合标签策略，则资源将会被标记为不合规。

标签策略有如下两种应用方式：

1. 事后检查 —— 资源标签如果违反标签策略，则在资源在合规性结果中显示为不合规。

2. 事前拦截 —— 标签策略开启强制执行后，则会阻止在指定的资源类型上完成不合规的标记操作。

约束条件

只有组织管理员才可以创建标签策略，委托管理员无法执行此操作。

说明

在创建标签策略并将其附加到组织单元和账号之前，必须先启用标签策略，且只能使用组织的管理账号启用标签策略。

操作步骤

步骤1 以组织管理员或管理账号的身份登录华为云。

步骤2 单击页面左侧 ☰，选择“管理与监管 > 组织”，默认进入“组织管理”界面。

步骤3 单击左侧“策略管理”，进入策略管理页，单击“标签策略”，进入标签策略页面。

图 7-1 进入标签策略

步骤4 单击“创建”，进入标签策略创建页面。

图 7-2 创建策略

步骤5 输入策略名称。注意，创建的策略名称不能与已有策略名称重复。

步骤6 根据**标签策略语法**，标签策略内容。填写时，系统会自动校验语法。如不正确，请根据提示进行修正。

图 7-3 填写标签策略

步骤7 （可选）为策略添加标签。在标签栏目下，输入标签键和标签值，单击添加。

步骤8 单击右下角“保存”后，如跳转到标签策略列表，则标签策略创建成功。

说明

如果需对标签策略进行修改、删除，可参见**修改、删除标签策略**。

具体绑定与解绑操作，参见**绑定和解绑标签策略**。

----结束

7.3 创建标签

本章节指导用户为已有SSL证书添加标签。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击目标SSL证书名称，进入SSL证书详情页面。

步骤5 单击“标签”进入标签管理页面。

步骤6 单击“添加标签”，弹出添加标签对话框，如**图 添加标签**所示，在弹出的“添加标签”对话框中输入“标签键”和“标签值”。

图 7-4 添加标签

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤7 单击“确定”，完成标签的添加。

----结束

7.4 通过标签搜索 SSL 证书

该任务指导用户在SSL证书管理界面，通过标签搜索当前项目下满足标签搜索条件的SSL证书。

前提条件

已添加标签。

约束条件

可添加多个标签进行组合搜索，最多支持20个不同标签的组合搜索，如果进行多个标签组合搜索，则搜索结果的每个SSL证书均满足标签组合搜索条件。

操作步骤

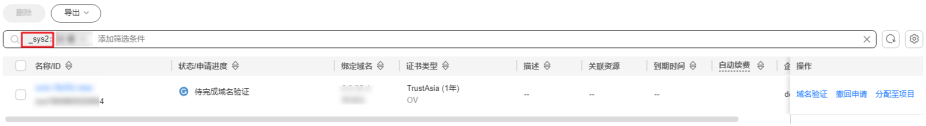
步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击搜索框，选择资源标签中的“标签键”和“标签值”后，显示满足搜索条件的SSL证书列表，如**图 搜索结果**所示。

图 7-5 搜索结果



说明

- 可添加多个标签进行组合搜索，最多支持20个不同标签的组合搜索，如果进行多个标签组合搜索，则搜索结果的每个SSL证书均满足标签组合搜索条件。
- 如果需要在搜索条件中删除添加的标签，可在搜索条件中单击指定标签后的，删除添加的标签。

----结束

7.5 修改标签值

本章节指导用户对已创建SSL证书标签进行修改。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击目标SSL证书名称，进入SSL证书详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

步骤6 单击“编辑”，弹出“编辑标签”对话框。修改标签值后单击“确定”，完成标签值修改。

----结束

7.6 删除标签

本章节指导用户对已创建SSL证书标签进行删除。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 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4 单击目标SSL证书名称，进入SSL证书详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

步骤6 单击“编辑标签”，在右侧弹框中目标标签所在行单击“删除”，再单击“确定”，完成标签的删除。

----结束

8 SCM 权限管理

8.1 创建用户并授权使用 SCM

如果您需要对您所拥有的SCM进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用SCM资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将SCM资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用SCM服务的其它功能。

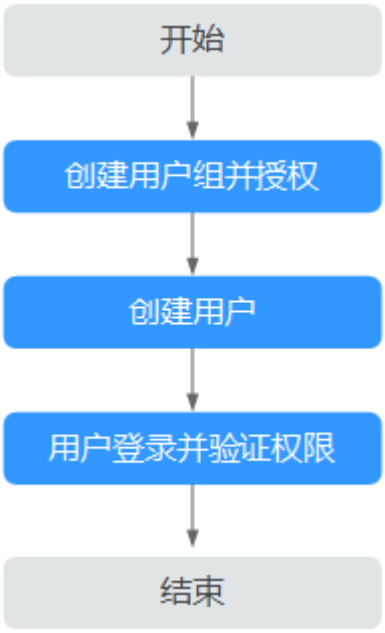
本章节为您介绍对用户授权的方法，操作流程如**图8-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的SCM权限，并结合实际需求进行选择，SCM支持的系统权限，请参见**CCM系统权限**。如果您需要对除CCM之外的其它服务授权，IAM支持服务的所有策略请参见**系统权限**。

示例流程

图 8-1 给用户授权 SCM 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予SSL证书管理服务的管理员权限“SCM Administrator”。
2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在“服务列表”中选择云证书管理服务，如果未提示权限不足，表示“SCM Administrator”已生效。

8.2 SCM 自定义策略

如果系统预置的CCM权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的SCM自定义策略样例。

SCM 自定义策略样例

- 示例1：授权用户下载证书

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "scm:cert:download"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- 示例2：拒绝用户删除证书

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先原则。

  如果您给用户授予“SCM Administrator”的系统策略，但不希望用户拥有“SCM Administrator”中定义的删除证书权限，您可以创建一条拒绝删除证书的自定义策略，然后同时将“SCM Administrator”和拒绝策略授予用户，根据Deny优先原则，则用户可以对证书执行除了删除证书外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "scm:cert:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "scm:cert:complete",
                "scm:cert:push",
                "cdn:configuration:queryHttpsConf"
            ],
            "Effect": "Allow"
        }
    ]
}
```


9 SCM 关键操作审计管理

9.1 SCM 支持云审计的操作列表

云审计服务记录SSL证书管理相关的操作事件，如表9-1所示。

表 9-1 云审计服务支持的 SCM 操作列表

操作名称	资源类型	事件名称
修改证书	scm	modifyScmCert
新建证书订单	scm	createScmNewCert
购买证书	scm	purchaseScmCert
上传用户认证信息	scm	uploadScmUserMessage
补全证书信息	scm	completeScmCert
下载证书	scm	downloadScmCert
删除证书	scm	deleteScmCert
取消证书审核	scm	cancelScmCert
吊销证书	scm	revokeScmCert
上传证书	scm	uploadScmCert
推送证书到ELB	scm	pushScmCertToELB

9.2 查看 SCM 审计日志

开启了云审计服务后，系统开始记录云证书管理服务相关的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 SCM 的云审计日志

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。

  在下拉框中选择查询条件：
  - “事件类型”选择“管理事件”。
  - “事件来源”选择“SC”。
  - “筛选类型”选择“事件名称”时，还需选择某个具体的事件名称；选择“资源ID”时，还需选择或者手动输入某个具体的资源ID；选择“资源名称”时，还需选择或手动输入某个具体的资源名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- “事件级别”：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- “时间范围”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

步骤5 单击“查询”，查看对应的操作事件。

步骤6 在需要查看的记录左侧，单击 ⌄ 展开该记录的详细信息，展开记录如图9-1所示。

图 9-1 展开记录

步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，显示了该操作事件结构的详细信息。

----结束

10 域名证书监控

10.1 域名证书监控简介

应用场景

域名证书监控功能用于为您统一监控所有站点的HTTPS状态并简化证书维护的复杂度，开启后可帮助您监测多个站点的HTTPS业务状态并及时发现站点上的SSL证书安全问题（例如：未配置SSL证书、证书已过期等），方便您统一维护多站点HTTPS，降低因人为疏忽导致HTTPS业务中断的风险。

说明

- 初次使用域名证书监控功能，系统会为您发放一个有效期为**7天**的免费实例，您可以试用该实例体验域名证书监控功能。有效期截止后实例自动失效。
- 如需继续使用，您可以单击右上角“购买域名证书监控”购买更多域名证书监控实例。

功能优势

- 提供简单、易操作的配置，无需花费大量时间和精力维护已有证书。
- 支持证书到期提醒，不用担心证书到期无人知晓从而影响业务。

监控指标

表 10-1 域名监控指标说明

监控指标	说明
域名安全等级分布·	域名安全等级由高至低依次分为： ● A级 安全 ● B级 低风险 ● C级 中风险 ● D级 高风险 ● 未知

监控指标	说明
SSL证书到期预警	统计证书到期时间分别为 • 已到期 • 到期时间<=30天 • 到期时间>30天 • 证书未知 **说明** 证书未知类目显示未绑定证书的域名或绑定了证书 但是端口号输入错误的域名，如您需要对已有证书进行监控，建议您添加已绑定证书的域名并输入正确的端口号。
SSL漏洞扫描	SSL漏洞扫描分为： • 低风险漏洞 • 中风险漏洞 • 高风险漏洞
合规检测	• ATS：应用程序安全传输（App Transport Security，简称ATS），是苹果在iOS 9 中首次推出的隐私安全保护功能。从2017年1月1日起，所有提交到App Store 的App必须强制开启ATS。启用ATS后，它会屏蔽明文HTTP资源加载，强制App通过HTTPS连接网络服务，对传输数据进行加密，保障用户数据安全。 • PCI DSS：支付卡协会数据安全标准（Payment Card Industry Data Security Standard, 简称 PCI DSS）是目前广受国际认可的数据安全标准。PCI DSS要求在开放的公共网络上传输持卡人数据，需使用高强度加密算法对数据进行保护。

10.2 购买并添加域名证书监控

本章节指导用户购买并添加域名证书监控，通过对多个站点不同域名检测，实现统一维护多站点HTTPS，降低因人为疏忽导致HTTPS业务中断的风险。

购买域名证书监控服务

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名证书监控”，进入域名证书监控界面。

步骤4 单击右上角“购买域名证书监控”进入域名证书监控购买页。

- **服务类型**：域名证书监控
- **规格**：支持购买5个域名、20个域名、100个域名和1000个域名
- **区域**：全区域可用
- **购买时长**：可选1年、2年和3年

步骤5 确定服务类型、规格和购买时长后单击“立即购买”。

步骤6 进入订单确认界面，勾选我已阅读并同意《云证书管理服务（CCM）免责声明》并单击“去支付”。

步骤7 完成支付后，域名证书监控服务即购买成功。

----结束

须知

- 购买域名证书监控服务后，在其有效期内仅支持升级域名证书监控规格，无法重复购买。如您当前购买的域名证书监控实例无法满足业务需求，您可以单击右上角“升级规格”，获取更多监控实例。
- 域名证书监控服务当前仅支持**包年/包月**计费模式，实际费用以页面显示为准，更多计费规则请参见**计费说明**。

添加域名证书监控

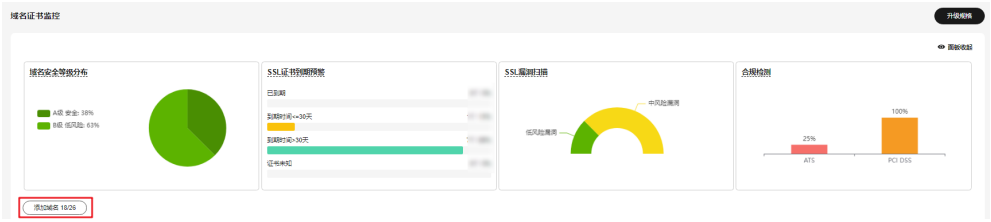
步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名证书监控”，进入域名证书监控界面。

步骤4 单击“添加域名”，如**图 添加域名**。

图 10-1 添加域名



步骤5 在弹出的“添加域名”对话框中根据提示配置参数，如**图 添加域名并配置参数**所示，参数说明如**表 配置参数**所示。

图 10-2 添加域名并配置参数

表 10-2 配置参数

参数名称	参数说明
当前可监控	显示当前剩余监控实例数量，如需购买更多实例，请单击“前往扩容”
域名/IP	需要进行监控的域名地址或IP地址
端口	端口号，默认为443
开启监控	• 单击开启“监控按钮” 开启监控后，将对该域名所使用证书的状态和有效期进行持续的监控服务。 • 单击关闭开启“监控按钮” 关闭监控后，该域名的状态和有效期将不会被监控。

步骤6 配置完成后，单击“确定”完成添加域名监控。

----结束

10.3 查看域名证书监控数据

本章节指导用户如何查看域名的监控数据，从域名安全等级分布、SSL证书到期预警、SSL漏洞扫描结果和合规检测结果等方面来展示域名和证书的安全状况。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名监控”，进入域名监控界面。

步骤4 查看已经添加的域名监控列表，显示的参数详情如**表 参数说明**。

表 10-3 参数说明

参数名称	参数说明
绑定域名/IP	已添加至域名监控列表的域名或IP地址
证书品牌	已添加至域名监控列表的域名绑定的证书品牌
证书类型	已添加至域名监控列表的域名绑定的证书类型
状态	域名监控状态： • 正常：域名监控状态正常。 • 失败：域名监控失败，可能原因为网络波动和域名填写有误。 • 未开启：未开启域名监控，可重新配置。 • 扫描中：已成功添加域名监控，正在对添加的域名进行扫描。
证书到期时间	已添加域名绑定的证书到期时间
安全等级	安全等级由高至低依次分为A、B、C、D四个等级
监控剩余天数	每个域名监控的剩余天数
监控频率	已添加域名的监控频率，默认为30分钟
监控	 ：开启监控  ：关闭监控
操作	• 监控为开启状态时，操作栏可单击“监控报告”查看监控详情。 • 监控状态为关闭时，操作栏可单击“监控配置”重新配置域名监控参数。

步骤5 单击“监控报告”如**图 查看监控报告**查看详细监控数据。

图 10-3 查看监控报告

步骤6 监控报告显示的信息详情如**表 监控数据详情**

表 10-4 监控数据详情

参数	参数说明
概览	域名安全评级概览
监控状态	• 失败 • 正常 • 扫描中
ATS	• 满足 • 不满足 **说明** 当监控报告中显示ATS不满足时，可单击“查看详情”查看各检查项的扫描结果是否通过并进行逐一排查。
PCI DSS	• 满足 • 不满足 **说明** 禁止使用TLS 1.1或更早的不安全传输加密协议，如此项不满足，则PCI DSS扫描结果为不满足。
优化建议	针对当前域名的安全评级等信息给出相应的优化建议
SSL证书信息	• 通用名称：当前SSL证书的通用名称 • 颁发者：当前SSL证书的颁发机构名称 • 加密算法：当前SSL证书使用的加密算法 • 签名算法：当前SSL证书使用的签名算法 • 证书透明（CT）：当前证书签发行为是否透明公开 • 证书品牌：当前SSL证书的品牌名称 • 证书类型：当前SSL证书的类型 • 开始时间：当前SSL证书签发时间 • 结束时间：当前SSL证书到期时间 • 组织机构：组织名称 • 备用名称：当前SSL证书的备用名称

参数	参数说明
证书链信息	• 颁发给：需要颁发证书的域名 • 颁发者：SSL证书的颁发机构名称 • 有效期：证书有效期
协议	显示对于以下6种协议类型是否支持 TLS 1.3 TLS 1.2 TLS 1.1 TLS 1.0 SSL 3 SSL 2
SSL漏洞检测	SSL漏洞检测信息
套件	支持的加密套件详情

----结束

10.4 管理域名证书监控

当业务变化或当前添加的域名监控不符合您的业务需求时，您可以参考本章节关闭、开启、修改或删除已配置的域名监控。

关闭域名监控

前提条件

- 已添加域名监控。
- 域名监控功能为开启状态。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名监控”，进入域名监控界面。

步骤4 在域名监控列表找到需要关闭域名监控功能的域名，单击  ，如**图 关闭域名监控**。

图 10-4 关闭域名监控

步骤5 在弹出框单击“确定”关闭当前域名的监控功能。

----结束

须知

域名监控成功添加后，监控剩余天数立即开始计时，关闭域名监控功能后计时不会停止。

开启域名监控

前提条件

- 已添加域名监控。
- 域名监控功能为关闭状态。

操作步骤

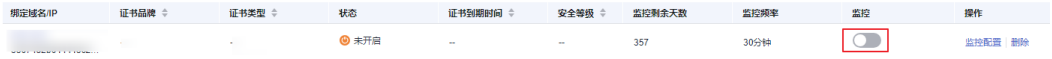
步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名监控”，进入域名监控界面。

步骤4 在域名监控列表找到需要开启域名监控功能的域名，单击  ，如图 开启域名监控。

图 10-5 开启域名监控



步骤5 在弹出框单击“确定”开启当前域名的监控功能。

----结束

修改域名监控配置

前提条件

- 已添加域名监控。
- 域名监控功能为关闭状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名监控”，进入域名监控界面。

步骤4 在域名监控列表找到需要修改配置的域名，在操作栏单击“监控配置”如**图 修改监控配置**。

图 10-6 修改监控配置

步骤5 在弹出框重新配置参数并单击“确定”完成配置修改。

----结束

删除域名证书监控

前提条件

已添加域名证书监控。

须知

域名证书监控开启或关闭状态都可以对其进行删除操作，请谨慎操作。

操作步骤

步骤1 登录**管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 云证书管理服务”，进入云证书管理界面。

步骤3 在左侧导航栏选择“SSL证书管理 >域名监控”，进入域名监控界面。

步骤4 在域名监控列表找到需要删除的域名，在操作栏单击“删除”，如**图 删除域名监控**

图 10-7 删除域名证书监控

步骤5 在弹出框单击“确定”，完成域名证书监控删除操作。

----结束