



云证书管理服务

# 用户指南

发布日期 2023-03-30

# 目录

<b>1 产品介绍</b>	<b>1</b>
1.1 什么是云证书管理服务	1
1.2 功能特性	1
1.3 产品优势	2
1.4 应用场景	2
1.5 基本概念	3
1.6 计费说明	6
1.7 CCM 权限管理	7
1.8 与其他云服务的关系	9
1.9 个人数据保护机制	10
<b>2 用户指南</b>	<b>11</b>
2.1 私有证书申请概述	11
2.2 管理私有 CA	12
2.2.1 创建私有 CA	12
2.2.2 激活私有 CA	15
2.2.3 查看私有 CA 详情	18
2.2.4 导出私有 CA 证书	20
2.2.5 禁用私有 CA	21
2.2.6 启用私有 CA	22
2.2.7 计划删除私有 CA	22
2.2.8 取消删除私有 CA	24
2.3 管理私有证书	25
2.3.1 申请私有证书	25
2.3.2 下载私有证书	30
2.3.3 安装私有证书	32
2.3.3.1 信任根 CA	32
2.3.3.2 在客户端安装私有证书	36
2.3.3.3 在服务器安装私有证书	38
2.3.3.3.1 在 Tomcat 服务器上安装私有证书	38
2.3.3.3.2 在 Nginx 服务器上安装私有证书	40
2.3.3.3.3 在 Apache 服务器上安装私有证书	43
2.3.3.3.4 在 IIS 服务器上安装私有证书	45
2.3.3.3.5 在 Weblogic 服务器上安装私有证书	48

2.3.3.3.6 在 Resin 服务器上安装私有证书.....	54
2.3.4 吊销私有证书.....	57
2.3.5 查看私有证书详情.....	59
2.3.6 删除私有证书.....	60
2.4 权限管理.....	61
2.4.1 创建用户并授权使用 CCM.....	61
2.4.2 CCM 自定义策略.....	62
<b>3 常见问题.....</b>	<b>64</b>
3.1 什么是公钥和私钥? .....	64
3.2 为什么要使用无密码保护的私钥? .....	65
3.3 主流数字证书有哪些格式? .....	66
3.4 如何制作 CSR 文件? .....	68
3.5 如何解决“审核失败 - 主域名不能为空”的问题? .....	72
3.6 私有证书有效期相关问题.....	72
3.7 私有证书管理服务是如何收费的? .....	73
3.8 私有证书签发后, 能否停用私有 CA? .....	74
<b>A 修订记录.....</b>	<b>75</b>

# 1 产品介绍

## 1.1 什么是云证书管理服务

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

私有CA颁发的证书仅在您的组织内受信任，在Internet上不受信任。

## 1.2 功能特性

云证书管理服务提供以下功能，帮助您实现组织内部的应用身份认证和数据加解密。

功能名称	功能描述
托管的证书颁发机构	私有证书管理服务提供证书颁发机构（Certificate Authority，CA），支持多种密钥算法，其中包括：RSA_2048、RSA_4096、EC_P256、EC_P384等。支持X.509 v3的证书格式，支持CA多级扩展和多级认证，采用国际通用的对称和非对称算法，符合PKI/CA国际标准。
私有证书生命周期管理	私有证书管理服务提供对私有证书的申请、下载、吊销，具备千万级以上的证书管理能力。
密钥生命周期管理	私有证书管理服务使用密钥管理服务（Key Management Service，KMS）、硬件安全模块HSM（Hardware Security Module）来保护CA密钥的安全，支持软件和硬件产生密钥对，完成密钥的产生、更新、删除、恢复等功能。
私有证书撤销列表（Certificate Revocation List，CRL）管理	私有证书管理服务能定期自动向您的OBS桶发布和更新证书撤销列表，供您或应用下载。应用程序、服务以及设备可以定期使用CRL评估证书状态。
API自动化集成	私有证书管理服务提供API，可以帮助您在开发环境高效集成，快速进行产品部署。

## 1.3 产品优势

### 私有 CA 托管能力

用户无需构建和维护复杂的CA基础设施，可轻松获得CA管理能力。

### 完整私有 CA 层次结构

支持创建灵活的CA层次结构，包括根CA和从属CA，同时支持外部CA，满足更多应用部署。

### 私有证书生命周期管理

提供证书、密钥统一管理，具备千万级以上的证书服务管理能力，支持证书撤销列表及时提醒租户证书状态，避免证书过期。

### 私有证书支持多种密钥算法

支持RSA\_2048、RSA\_4096、EC\_P256、EC\_P384等多种密钥算法，支持X.509 v3证书格式，符合PKI/CA国际标准。

### 私有证书密钥存储安全可靠

通过密钥管理服务（KMS）和硬件安全模块（HSM）提供安全保护，可以安全可靠保存密钥。

### 私有证书 API 灵活集成

提供丰富的API接口，可以帮助您在开发环境高效集成，快速进行产品部署，为企业租户提供了巨大的灵活性。

## 1.4 应用场景

### 企业对内实行应用数据安全管控

您可以通过私有证书管理建立企业内部的证书管理体系，在企业内部签发和管理自签名私有证书，实现企业内部的身份认证、数据加解密、数据安全传输。

### 车联网应用

车企TSP使用私有证书管理服务，为每台车辆终端颁发证书，提供车-车、车-云、车-路多场景交互时鉴权、认证、加密等安全能力。

### 物联网应用

IoT平台使用私有证书管理服务，为每台IoT设备颁发证书，并通过IoT平台联动PCA，实现IoT设备的身份校验与认证，保障IoT场景下设备接入安全。

## 1.5 基本概念

### 根 CA

颁发机构（CA）的公钥证书，是公钥基础设施（PKI）体系中的信任锚。可签发从属CA、私有证书与证书吊销列表。当被导入客户端信任列表后，可对其签发的证书进行校验。

### 从属 CA

也称中间CA或子CA，用于隔绝根CA与私有证书，是划分CA层次结构的关键，在证书链校验过程中对下一层证书进行校验。当路径深度大于0时，从属CA可向下签发从属CA。

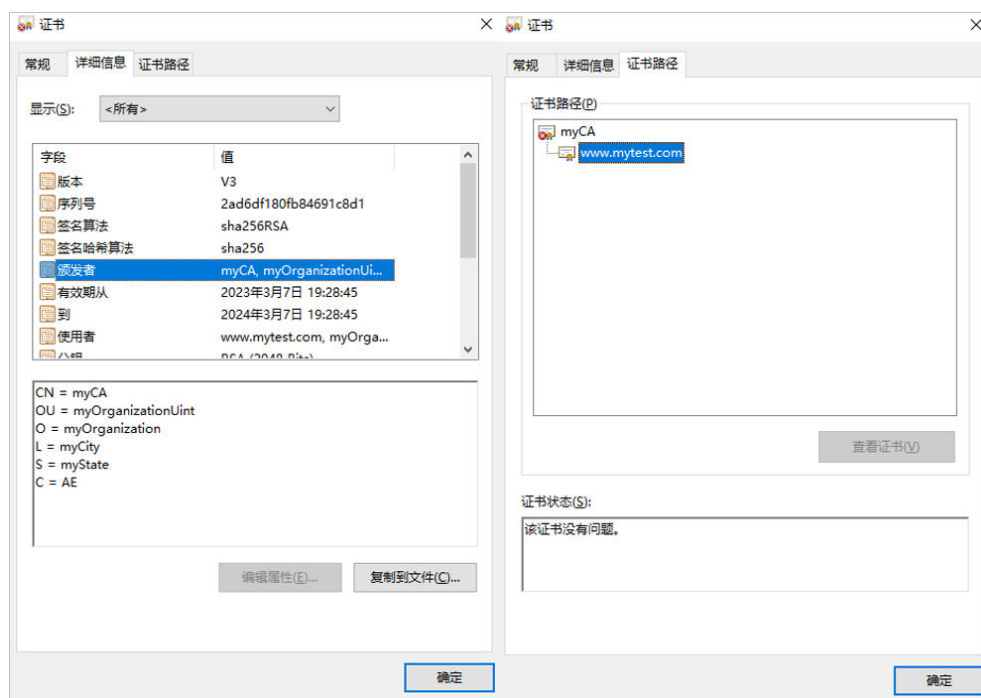
#### 📖 说明

从属CA的路径深度，即当前CA可以签发下级从属CA的层次数量，用于控制证书链深度（证书链最后一层为私有证书）。

### 私有证书

私有证书又称终端实体证书，安装在终端实体上的证书，含客户端证书（应用于客户端）、服务器证书（应用于服务器）等。承担实体的身份验证的作用，不可用于签发证书，属于证书链中的最后一层，是拥有该证书的实体与其它实体进行HTTPS通信的凭证。私有证书内容，如图 [私有证书](#) 所示。

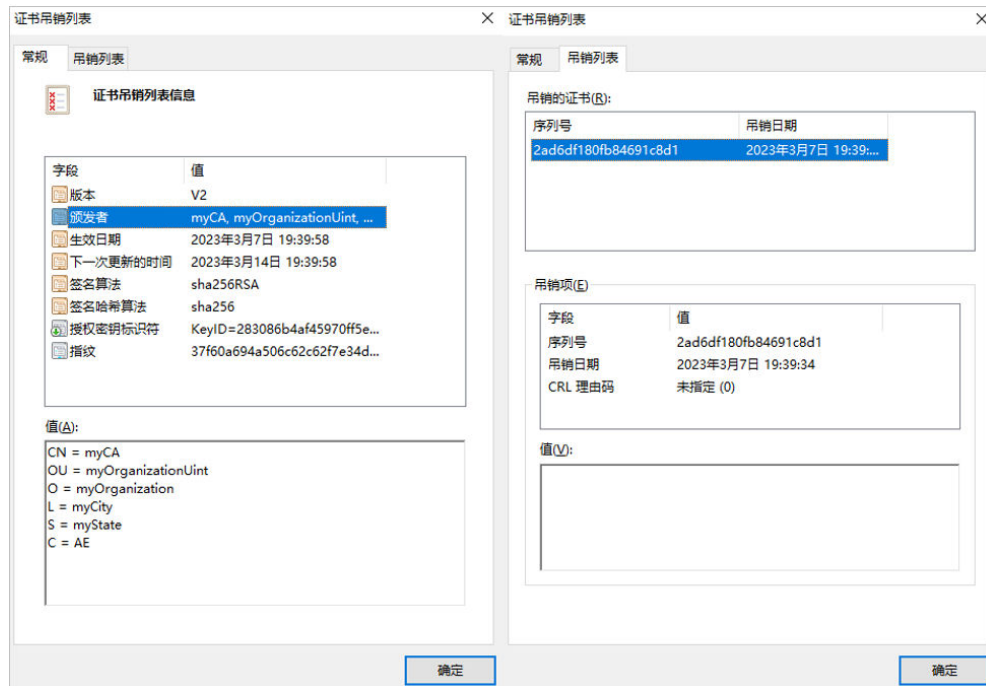
图 1-1 私有证书



## 证书吊销列表

证书吊销列表（Certificate Revocation List, CRL）是指在有效期内就被其父CA吊销的证书的名单，其中被吊销的证书类型，包含从属CA与私有证书。证书吊销列表是一种有固定格式的结构化数据文件，其中包含颁发者信息、吊销列表的生效时间、列表下一次更新时间、签发算法、指纹以及已被吊销证书的序列号与对应的吊销时间和吊销理由码。证书吊销列表具体内容，如图 [证书吊销列表](#) 所示。

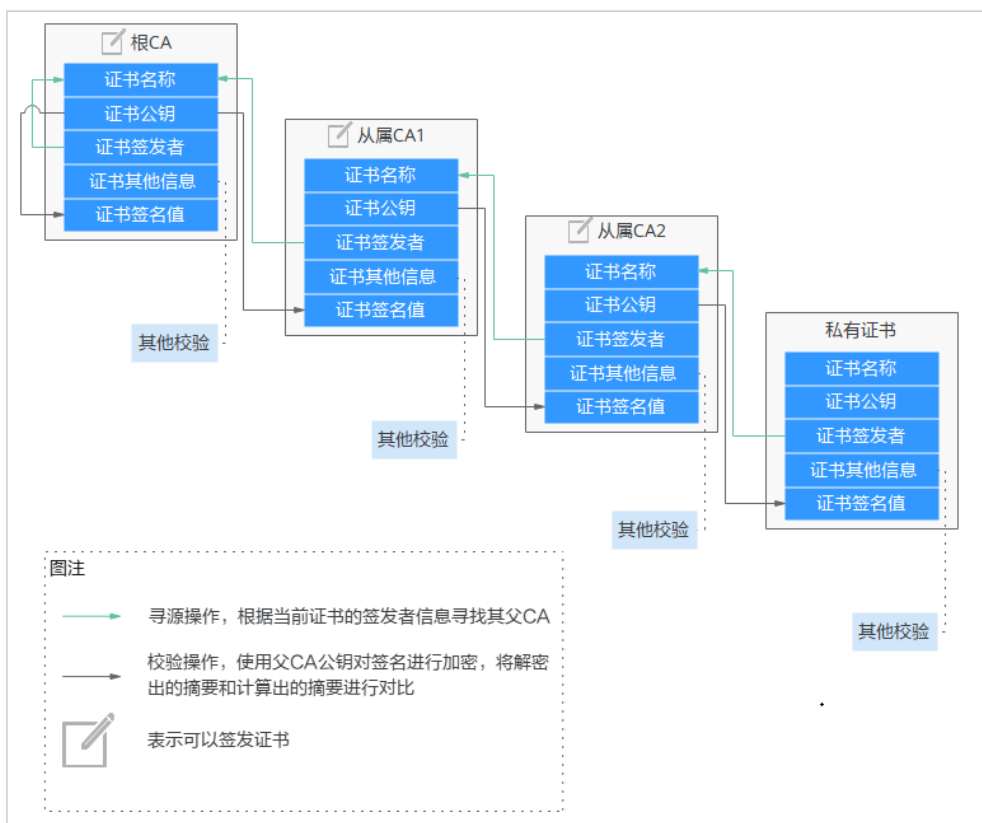
图 1-2 证书吊销列表



## 证书链

从根CA到私有证书之间的完整的证书链路，即各个层级证书按序链在一起的文件，用于进行身份的逐层校验。各级证书的链接关系，如图 [证书链](#) 所示。

图 1-3 证书链



证书校验主要体现在两方面：

- 证书链的完整性校验，逐层校验证书的有效性。
- 证书链中的根CA是否被校验方所信任（提前预置到信任列表中）。

证书校验过程中主要包含的校验项：

- 实体所宣称的主体信息（如服务端的域名）是否在证书可选名称的范围内。
- 证书是否过期。
- 密钥用法是否符合当前操作（如密钥协商、数字签名等）。
- 数字签名验证。
- 是否已被吊销。

### 📖 说明

此处未列举出所有校验项，X509证书允许用户增加多种自定义扩展项，详情请参考相关国际标准。

## PCA 证书有效期

在证书链中，根CA是整条链的信任起点，一旦根CA过期，其与其从属CA签发的所有证书将不再被信任，因此根CA的有效期是其下层所有证书的有效期上限。即使签发下层证书时，可以将有效期填写超过根CA的有效期（不做强制要求下），但在校验证书链时，只要链中根CA过期，校验就会失败。



在PCA服务中，强制要求新签发的证书的到期时间不可超过其父CA的到期时间，确保从根CA到私有证书之间的链路上，有效期逐层递减。PCA服务对各类证书有效期的约束见[表 证书有效期约束](#)。

不同类型证书的有效期是根据其扮演的角色而定的。使用越频繁的证书，其密钥材料泄露风险更高，有效期应尽量设置更小。例如，根CA通常只用于签发从属CA，使用频率最少，且使用最高的安全保护措施（PCA中使用KMS进行CA密钥管理），有效期一般设置为10~30年左右。从属CA根据其所在的层级，越往下有效期逐级减少，最下层的证书用于签发大量的私有证书，有效期通常设置为2~5年左右。私有证书，频繁用于通信，通常根据使用场景的安全要求，将有效期设置为几个小时、几个月以及一两年不等。

表 1-1 证书有效期约束

证书类型	最小有效期	最大有效期	是否支持延长	有效期其它约束
根CA	1小时	30年	否	无
从属CA	1小时	20年	否	在父CA有效期内
私有证书	1小时	20年	否	在父CA有效期内

## 1.6 计费说明

### 计费项

云证书管理服务根据您的**私有CA数量**、**私有证书数量**进行收费。

### 计费模式

私有CA和私有证书都是按需计费。其中，根CA创建后即开始计费；从属CA创建后不收费，激活后才开始计费。私有CA创建后各状态的收费情况，请参见[表 私有CA计费说明](#)

按需计费模式，即按实际使用的时长收费，以小时为单位，每小时整点结算，不设最低消费标准。

表 1-2 私有 CA 计费说明

私有CA状态	是否收费	备注信息
待激活	否	需激活方可正常使用
已激活	是	可签发证书、吊销证书和签发证书吊销列表 <b>须知</b> 此功能受密钥用途限制

私有CA状态	是否收费	备注信息
已禁用	是	只禁用了签发证书的功能，仍可吊销证书和发布证书吊销列表 <b>须知</b> 此功能受密钥用途限制
计划删除	<ul style="list-style-type: none"><li>“计划删除”状态，删除时间到时，私有CA将会被删除，此期间不收费</li><li>当私有CA被“取消删除”时，将对私有CA处于“计划删除”期间进行补充收费</li></ul> 例如：您在2022年01月01日00:00执行了删除私有CA的操作，且设置的私有CA计划删除推迟时间为7天，7天后私有CA被删除，那么，PCA服务将不收取这7天的费用；如果您在2022年01月04日00:00取消了计划删除，私有CA未被删除，那么，PCA服务将补齐2022年01月01日00:00至2022年01月04日00:00期间的费用。 <b>须知</b> 只有“已禁用”或“已过期”状态的私有CA被删除后才会转为“计划删除”状态，不会立即删除。计划删除最快7天生效（根据您设置的推迟时间为准）	仅提供取消删除操作
已过期	是	此状态下，私有CA将不再可信，不提供签发证书、吊销证书和签发证书吊销列表功能，但占用CA配额，可导出 <b>注意</b> 如您不再使用，请尽快删除，避免被收费。
已吊销	否	只有从属CA可被吊销，如其父CA开启了证书吊销列表，则其吊销信息将会被发布到证书吊销列表中，被吊销的私有CA将不再可信

## 变更配置

私有CA和证书申请为按需计费。

如需停止计费，请删除申请的私有CA和私有证书。

## 1.7 CCM 权限管理

如果您需要对云上的云证书管理服务（CCM）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and

Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制他们对云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有云证书管理服务（CCM）的使用权限，但是不希望他们拥有删除CCM等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CCM，但是不允许删除CCM的权限策略，控制他们对CCM资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CCM服务的其它功能。

## CCM 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CCM部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置权限，访问CCM时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CCM服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表1-3所示，包括了CCM所有系统角色。

表 1-3 CCM 系统角色

角色名称/策略名称	描述	类别	依赖关系
PCA FullAccess	私有证书管理服务所有权限。	系统策略	创建私有CA或私有证书需要依赖BSS Administrator角色。 EPS FullAccess: 系统策略，企业项目管理服务所有权限。 OBS Administrator: 系统策略，对象存储服务管理员。

### 须知

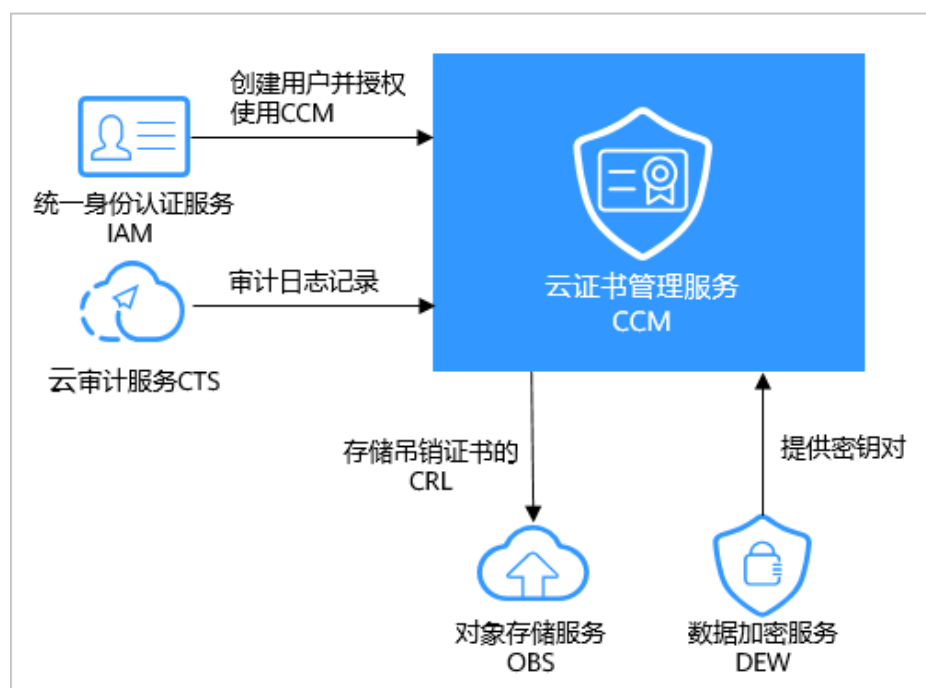
如需购买证书，账号除了必须拥有“SCM Administrator”或“SCM FullAccess”之外，还需要拥有“BSS Administrator”权限。

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。

## 1.8 与其他云服务的关系

云证书管理服务与周边服务的依赖关系如图1-4所示。

图 1-4 与其他云服务的关系



### 与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。私有证书管理服务中执行吊销证书操作时，吊销证书的CRL会存储在用户的OBS桶里，供客户查询。

### 与数据加密服务的关系

数据加密服务（Data Encryption Workshop，DEW）为云证书管理服务提供密钥对生成及保护的功能。

### 与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录云证书管理服务的相关的操作事件，方便用户日后的查询、审计和回溯。

## 与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为云证书管理服务提供了权限管理的功能。

需要拥有PCA FullAccess的用户才能使用CCM。

如需开通该权限，请联系拥有Security Administrator权限的用户。

## 1.9 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，CCM通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

### 收集范围

CCM收集及产生的个人数据如表1-4所示：

表 1-4 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
租户ID	<ul style="list-style-type: none"><li>在控制台进行任何操作时Token中的租户ID</li><li>在调用API接口时Token中的租户ID</li></ul>	否	是，租户ID是证书资源身份标识
邮箱	在申请私有证书时填写的邮箱	否	否

### 存储方式

CCM通过加密算法对您个人敏感数据加密后进行存储。

- 租户ID：不属于敏感数据，明文存储
- 邮箱：加密存储

### 访问权限控制

您的个人数据通过加密后存储在CCM数据库中，访问个人数据需要通过Token认证。

### 日志记录

您的个人数据的所有操作，包括修改、查询和删除等，CCM都会记录审计日志并上传至云审计服务（CTS），您可以并且仅可以查看自己的审计日志。

# 2 用户指南

## 2.1 私有证书申请概述

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

私有CA颁发的证书仅在您的组织内受信任，在Internet上不受信任。

私有证书申请流程如[图 私有证书申请流程](#)所示，流程相关说明如[表 私有证书申请流程说明](#)所示。

图 2-1 私有证书申请流程

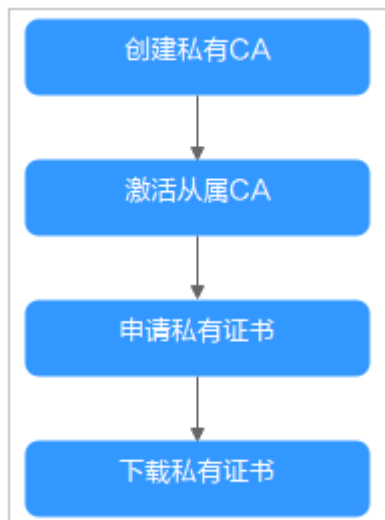


表 2-1 私有证书申请流程说明

步骤	申请操作	说明
1	创建私有CA	根据需要创建私有CA。 首次创建私有CA时，须先创建根CA。后续可以在已有根CA下创建多个从属CA。
2	激活私有CA	私有根CA创建后，即可用于签发私有证书。 私有从属CA创建后需要激活，激活后才能使私有CA正式生效，并且用于签发私有证书。
3	申请私有证书	通过已激活的私有CA，申请私有证书。
4	下载私有证书	申请完成后，即可下载私有证书并在服务器上安装使用。

## 2.2 管理私有 CA

### 2.2.1 创建私有 CA

云证书管理服务可以帮助您通过简单的可视化操作，以低投入的方式创建企业内部CA并使用它签发证书。

本章节帮助您通过云证书管理控制台创建私有CA（支持创建根CA和从属CA）。

#### 背景信息


- 私有CA分为根CA和从属CA（即中间CA或子CA），从属CA隶属于根CA，根CA下可以包含多个从属CA。
- 首次创建私有CA时，须先创建根CA。
- 每个用户可以创建100个CA，已计划删除的私有CA也将计入CA限制值内，直到计划删除CA执行删除为止。

#### 前提条件

创建私有CA的账号拥有“PCA FullAccess”权限。

#### 操作步骤

**步骤1** 登录管理控制台。

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

**步骤3** 在私有CA列表右上角，单击“创建CA”，进入创建CA界面。

**步骤4** 配置私有CA信息。

您需要配置“基本信息”、“证书唯一标识名称（DN）”和“证书吊销配置”信息。

- 配置基本信息，如#ccm\_01\_0016/zh-cn\_topic\_0000001124217631\_fig19641142713913所示，参数说明如表2-2所示。

**基本信息**

\* CA类型  根CA 创建根CA，用于建立新的CA层次结构。  
 从属CA 创建从属CA，用于在现有的CA层次结构中增加新的层次。

\* 密钥算法

\* 签名哈希算法

\* 有效期

到期时间: 2023/11/10 15:52:33 GMT+08:00

表 2-2 基本信息参数说明

参数名称	参数说明	取值样例
CA类型	选择待创建的私有证书颁发机构的类型。 CA类型： - 根CA：如果要建立新的CA层次结构，则选择此项。 <b>说明</b> 首次创建私有CA，则须创建根CA。 - 从属CA：用于在现有的CA层次结构中增加新的层次。	根CA
密钥算法	选择密钥算法和密钥的位大小。 - RSA2048 - RSA4096 - EC256 - EC384	RSA2048
签名哈希算法	“CA类型”选择“根CA”时，显示该参数。 可选择签名哈希算法： - SHA256 - SHA384 - SHA512	SHA256



参数名称	参数说明	取值样例
有效期	“CA类型”选择“根CA”时，显示该参数。 选择私有证书颁发机构有效期，可选择最长有效期为30年。	3年

- 配置证书唯一标识名称（Distinguished Name, DN）信息，如图2-2所示，参数说明如表2-3所示。

图 2-2 DN 信息

表 2-3 DN 信息参数说明

参数名称	参数说明	取值样例
CA名称 (CN)	自定义私有CA名称。	-
国家/地区	申请单位所属国家或地区，只能是两个字母的国家或地区代码。	AE
省/市	申请单位所在省名或市名。	Abu Dhabi
城市	申请单位所在城市名。	Abu Dhabi
公司名称 (O)	申请单位法定名称。	-
部门名称 (OU)	申请单位的所在部门。	Cloud Dept.

- （可选）配置证书吊销信息。  
如果需要为私有CA吊销的证书发布证书吊销列表（Certificate Revocation List, CRL），则可配置证书吊销信息。  
如果无需配置，请直接跳过该步骤。  
配置证书吊销信息，如图2-3所示，参数说明如表2-4所示。

图 2-3 证书吊销

表 2-4 证书吊销参数说明

参数名称	参数说明
OBS授权	确认是否授权CCM服务访问您的OBS桶并上传CRL文件。 如果确认授权，则单击“立即授权”，并根据提示完成授权。 授权成功后，取消授权需要到统一身份认证服务控制台委托服务列表中删除委托。 如果已授权，则无需再次授权。
启用CRL发布	确认是否启用CRL发布。
OBS桶	选择已有的OBS桶，或单击“创建新的OBS桶”来创建新的OBS桶。
CRL更新周期	CRL更新的周期。私有证书管理服务将在指定时间内重新生成CRL。 可设置为7~30的整数更新天数，如果未设置则默认为7天。

**步骤5** 单击“下一步”，进入确认信息页面。

**步骤6** 确认信息以及价格无误后，单击“确认并创建”，完成创建私有CA操作。

如果创建的是**根CA**，则创建后便已激活；如果创建的为从属CA，则需要进行激活操作。

私有**从属CA**创建后，如需立即安装CA证书并激活CA，则单击“立即激活”；如需后续再激活，单击“稍后再激活”。

----结束

## 后续处理

私有**根CA**创建成功后，即可用于签发私有证书，申请私有证书详细操作请参见[申请私有证书](#)。

私有**从属CA**创建成功后，需要安装证书并激活CA，具体操作请参见[激活私有CA](#)。

### 2.2.2 激活私有 CA

如果您创建的私有CA为**从属CA**，则需要创建后进行激活。激活后，才能使私有CA正式生效，并且才能可以用于签发私有证书。

本章节指导用户如何激活**从属CA**，系统提供通过内部私有CA和外部私有CA来激活私有CA两种不同的激活方式，请根据您的需要进行操作。


- 内部私有CA：使用云证书管理平台已有的私有CA来激活从属CA。
- 外部私有CA：使用外部私有CA（非云证书管理平台已有的私有CA）来激活从属CA。

## 前提条件

- 已创建私有从属CA，详细操作请参见[创建私有CA](#)。
- 私有从属CA处于“待激活”状态。

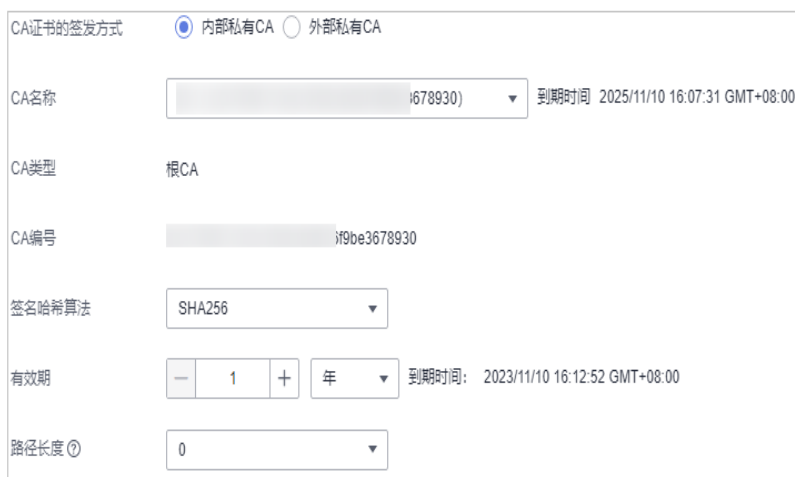
## 使用内部私有 CA 激活从属 CA

**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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在待激活的私有CA所在行的“操作”列，单击“激活”，系统从右面弹出激活CA详细页面，如[图2-4](#)所示，请填写激活CA相关信息。

图 2-4 内部私有 CA



1. 选择“CA证书的签发方式”。  
此处请勾选“内部私有CA”。
2. 配置私有CA相关参数。

表 2-5 内部私有 CA 激活配置参数说明

参数名称	参数说明
CA名称	选择根CA或从属CA的名称。 选中后，系统将自动显示该CA的类型和编号。
签名哈希算法	选择签名哈希算法： - SHA256 - SHA384 - SHA512
有效期	选择私有CA有效期，可选择的最长有效期为20年。


参数名称	参数说明
路径长度	<p>该从属CA的路径长度，即当前CA可以签发下级从属CA的层次数量，用于控制证书链深度。</p> <p><b>说明</b> 证书链是指根CA、从属CA、私有证书三者之间通过层层信任关系链接而成的序列。</p>

**步骤4** 确认填写的信息无误后，单击“确定”。

----结束

## 使用外部私有 CA 激活从属 CA

**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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在待激活的私有CA所在行的“操作”列，单击“激活”，系统从右面弹出激活CA详细页面，请填写激活CA相关信息。



CA证书的签发方式  内部私有CA  外部私有CA

1 导出CSR      2 外部CA签发证书      3 导入证书

**当前CA信息**

类型: 从属CA  
CA名称(CN): te...  
CA编号: C...

**CA的CSR**

导出CSR为文件 您可以将pem编码的CSR导出到文件中，并使用您拥有的外部CA对其签名生成证书。

**导入外部CA签发的证书**

\* 证书: 将用pem编码的证书粘贴到此处

证书链: 将用pem编码的证书链粘贴到此处

1. 选择“CA证书的签发方式”：此处请勾选“外部私有CA”。
2. 导出CSR。  
在“CA的CSR”中，单击“导出CSR为文件”。  
用pem编码的CSR导出到文件中，并让一个父CA对其进行签名。
3. 外部CA签发证书。

使用您的私有CA签发待激活从属CA证书。

#### 4. 导入证书。

在“导入外部CA签发的证书”中，将导入证书和证书链。

表 2-6 导入证书参数说明

参数	说明
证书	导入证书体，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”），将证书体复制到此处。
证书链	导入证书链，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”），将证书链复制到此处。

**步骤4** 确认填写的信息无误后，单击“确定”。

当私有CA的状态更新为“已激活”，则表示激活私有CA成功。

----结束

## 后续处理

私有CA激活后，即可用于签发私有证书，申请私有证书详细操作请参见[申请私有证书](#)。

## 2.2.3 查看私有 CA 详情


本章节指导用户查看已创建私有CA的信息，包括私有CA名称、部门名称、类型和状态等。

## 前提条件

已创建私有CA，详细操作请参见[创建私有CA](#)。

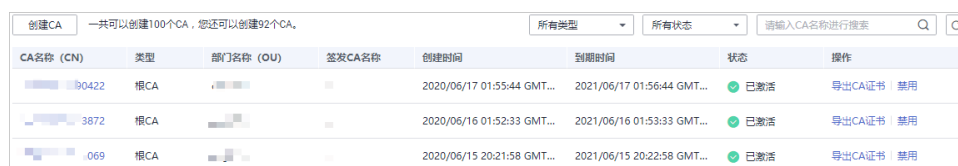
## 操作步骤

**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 > 云证书管理服务”，进入云证书管理服务界面。


**步骤3** 在私有CA列表中，查看私有CA信息，如[图2-5](#)所示，证书参数说明如[表2-7](#)所示。

图 2-5 私有 CA 列表



CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
90422	根CA			2020/06/17 01:55:44 GMT...	2021/06/17 01:56:44 GMT...	已激活	导出CA证书   禁用
3872	根CA			2020/06/16 01:52:33 GMT...	2021/06/16 01:53:33 GMT...	已激活	导出CA证书   禁用
069	根CA			2020/06/15 20:21:58 GMT...	2021/06/15 20:22:58 GMT...	已激活	导出CA证书   禁用

**说明**

- 在“所有类型”（或“所有状态”）搜索栏选择CA类型（或状态），私有CA列表界面将只显示对应类型（或状态）的CA。
- 在私有CA列表右上角的搜索框中输入CA名称，单击  或按“Enter”，可以搜索指定的CA。

**表 2-7 CA 参数说明**

参数名称	说明
CA名称（CN）	用户自定义的CA名称。
类型	私有CA的类型，说明如下： <ul style="list-style-type: none"><li>根CA：私有CA属于根CA，可用于签发其他从属CA。</li><li>从属CA：私有CA属于从属CA。</li></ul>
部门名称（OU）	私有CA所属的部门名称。
签发CA名称	签发该私有CA对应CA的名称。
创建时间	私有CA创建的时间。
到期时间	私有CA到期的时间。
状态	私有CA的状态，说明如下： <ul style="list-style-type: none"><li>待激活：私有CA处于待激活状态。</li><li>已激活：私有CA处于已激活状态。</li><li>已禁用：私有CA处于已禁用状态。</li><li>计划删除：私有CA处于计划删除状态。</li><li>已过期：私有CA处于已过期状态。</li></ul>
操作	用户可以在操作栏中，执行激活、启用、禁用CA等操作。

**步骤4** 用户可单击私有CA名称，查看私有CA的详细信息，如[图2-6](#)所示。

您可在CA详情页单击“添加标签”标识CA。如果您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，建议在TMS中创建预定义标签。

图 2-6 私有 CA 详细信息

CA名称 (CN)		状态	已激活
类型	根CA		
详细信息		CA证书	CRL配置
CA编号	3f9be3678930	类型	根CA
密钥算法	RSA2048	路径长度	7
创建时间	2022/11/10 16:07:32 GMT+08:00	到期时间	2025/11/10 16:07:31 GMT+08:00
CA名称 (CN)		国家/地区	
省/市		城市	
公司名称 (O)		部门名称 (OU)	
证书来源	系统创建		
标签			
添加标签	刷新	您还可以创建20个标签。	

----结束

## 2.2.4 导出私有 CA 证书

私有CA创建并激活后，您可以导出私有CA证书。

如果您的业务用户通过浏览器访问您的Web业务，您需要将根证书加入您的浏览器信任列表中，并且在您的Web服务器安装经该根CA签发的私有证书，即可实现客户端与服务端的HTTPS通信。

如果您的业务用户通过Java等客户端访问您的Web业务，您需要在对应客户端手动安装根证书，保证客户端能够校验服务端的加密信息。


本章节为您详细介绍导出私有CA证书的操作流程。

### 前提条件

待导出私有CA证书的私有CA需处于“已激活”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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在待导出的私有CA所在行的“操作”列，单击“导出CA证书”。

CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
0422	根CA			2020/06/17 01:55:44 GMT...	2021/06/17 01:56:44 GMT...	已激活	导出CA证书 禁用
3872	根CA			2020/06/16 01:52:33 GMT...	2021/06/16 01:53:33 GMT...	已激活	导出CA证书 禁用

**步骤4** 在弹出的提示框中，单击“确定”。

执行操作后，云证书管理服务将使用浏览器自带的下载工具，将私有CA证书文件下载至本地指定的位置。

获得“根CA名称\_certificate.pem”的私有CA证书文件。

----结束

## 2.2.5 禁用私有 CA

如果您不再需要使用某个私有CA来签发证书，可以禁用该私有CA。

私有CA被禁用后，您将不能使用该私有CA签发任何私有证书。如果要使用该私有CA进行签发私有证书操作，您需将该私有CA重新启用，具体操作请参见

本章节将介绍如何对指定的私有CA进行禁用。

### ⚠ 注意


私有CA禁用期间也将保持收费。

## 前提条件

待禁用的私有CA需处于“已激活”或“已过期”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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在需要禁用的私有CA所在行的“操作”列，单击“禁用”。

CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
90422	根CA			2020/06/17 01:55:44 GMT...	2021/06/17 01:56:44 GMT...	已激活	导出CA证书   禁用
3872	根CA			2020/06/16 01:52:33 GMT...	2021/06/16 01:53:33 GMT...	已激活	导出CA证书   禁用

**步骤4** 在弹出的对话框中输入“DISABLE”，并单击“确定”，完成禁用私有CA操作。

图 2-7 禁用 CA 提示信息





当页面右上角弹出“禁用CA xxx 成功！”，且私有CA状态更新为“已禁用”，则说明禁用私有CA操作成功。

----结束

## 2.2.6 启用私有 CA

如果您需要使用某个已禁用的私有CA来签发证书，可以将该证书恢复到已激活状态。


本章节介绍启用私有CA，使被禁用的私有CA恢复到已激活或已过期状态。

### 前提条件

待启用的私有CA需处于“已禁用”状态。禁用私有CA详细操作请参见[禁用私有CA](#)。

### 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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在需要启用的私有CA所在行的“操作”列，单击“启用”。

图 2-8 启用私有 CA

CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
...	根CA	...	...	2020/06/03 01:59:40 GMT+08:00	2021/06/03 02:00:40 GMT+08:00	● 已禁用	<a href="#">启用</a> <a href="#">删除</a>
...	根CA	...	...	2020/02/28 22:16:41 GMT+08:00	2021/02/28 22:17:41 GMT+08:00	● 已禁用	<a href="#">启用</a> <a href="#">删除</a>

当页面右上角弹出“启用CA xxx 成功！”，且私有CA状态更新为“已激活”，则说明启用私有CA操作成功。

----结束

## 2.2.7 计划删除私有 CA

在删除私有CA前，您需要确保该私有CA没有被使用且将来也不会被使用。

用户执行删除私有CA操作后，私有CA不会立即删除（待激活的私有CA将立即删除），私有证书管理服务会将该操作按用户指定时间推迟执行，推迟时间范围为7天~30天。在推迟删除时间未到时，如果需要重新使用该私有CA，可以执行取消删除私有CA操作。如果超过推迟时间，私有CA将被彻底删除，请谨慎操作。

**注意**

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


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

## 前提条件

待删除的私有CA需处于“已禁用”或“待激活”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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在需要删除的私有CA所在行的“操作”列，单击“删除”。

图 2-9 删除私有 CA

CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
...	根CA	...	...	2020/06/03 01:59:40 GMT+08:00	2021/06/03 02:00:40 GMT+08:00	● 已禁用	启用 删除
...	根CA	...	...	2020/02/28 22:16:41 GMT+08:00	2021/02/28 22:17:41 GMT+08:00	● 已禁用	启用 删除

**步骤4** 不同状态私有CA操作不同：

- 待激活状态私有CA  
在弹出的对话框中，输入“DELETE”。

图 2-10 删除私有 CA（待激活状态私有 CA）



- 已禁用、已过期状态私有CA  
在弹出的对话框中，输入“DELETE”，并填写“推迟删除”的时间。

图 2-11 计划删除时间（已禁用、已过期状态私有 CA）



**步骤5** 单击“确定”，完成删除私有CA操作。

- 待激活状态私有CA：当页面右上角弹出“删除CA xxx 成功！”，则说明删除私有CA操作成功。
- 已禁用、已过期状态私有CA：当私有CA状态更新为“计划删除”，则说明计划删除私有CA操作成功。

----结束

## 2.2.8 取消删除私有 CA


本章节介绍在未超出删除私有CA的推迟时间，对私有CA进行取消删除操作，取消删除后私有CA处于“已禁用”状态。

### 前提条件

待取消删除的私有CA需处于“计划删除”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 > 云证书管理服务”，进入云证书管理服务界面。

**步骤3** 在需要取消删除的私有CA所在行的“操作”列，单击“取消删除”。

图 2-12 取消删除私有 CA

CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作
9680	根CA			2020/06/15 16:36:25 GMT+08:00	2021/06/15 16:37:25 GMT+08:00	计划删除	取消删除
618	根CA			2020/06/11 17:53:59 GMT+08:00	2021/06/11 17:54:59 GMT+08:00	计划删除	取消删除

**步骤4** 在弹出的对话框中，单击“确定”，完成取消删除私有CA操作。

当页面右上角弹出“取消删除CA xxx 成功！”，且私有CA状态为“已禁用”，则说明取消删除私有CA操作成功。

取消删除后，如需使用该私有CA签发证书，还需要将其启用，详细操作请参见[启用私有CA](#)。

----结束

## 2.3 管理私有证书

### 2.3.1 申请私有证书

通过云证书管理控制台创建并激活私有CA后，您就可以通过私有CA申请私有证书，用于组织内部应用的身份认证和数据加解密。


本章节介绍如何申请私有证书。每个用户可以申请100,000个证书。

#### 前提条件

已创建并激活私有CA，详细操作请参见[创建私有CA](#)、[激活私有CA](#)。

#### 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 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。

**步骤3** 在私有证书列表的右上角，单击“申请证书”，进入申请证书界面，请填写申请证书的相关信息。

图 2-13 申请证书-系统生成文件

证书请求文件    **系统生成文件**    自己生成文件

---

### 证书配置

\* 证书名称 (CN)

---

### 高级配置

密码算法    签名哈希算法    密钥用法    增强型密钥用法    自定义扩展字段    配置证书AltName信息

密码算法

签名哈希算法

密钥用法

增强型密钥用法

自定义扩展字段

---

### 配置证书AltName信息

类型	值
1 IP address	<input type="text"/>

[+](#) 添加 你还可以添加4项AltName信息

---

### 选择签发CA

CA名称 (CN)

到期时间: 2023/11/10 11:10:46 GMT+08:00

类型: 根CA

CA编号: eb4b6711-3db2-408c-8707-17b238cde073

有效期:

预计到期时间 (不超过签发CA到期时间): 2023/11/10 11:10:46 GMT+08:00

图 2-14 申请证书-自己生成文件

证书请求文件
系统生成文件
自己生成文件

**i** 1. 我们需要您线下制作好CSR证书请求文件并上传。如何制作CSR证书请求文件?  
 2. 请保存好您的私钥, 私钥丢失将导致数字证书无法使用, 原有加密的数据不能解密。什么是公钥和私钥?  
 3. 在云产品中使用数字证书, 需要保证您的私钥无密码保护。为什么要使用无密码保护的私钥?

\* CSR证书请求文件

请将证书请求文件内容粘贴在此处

解析

**选择签发CA**

CA名称 (CN) rr (eb4b6711-3db2-406c-8707-17b236cde073)

到期时间: 2023/11/10 11:10:46 GMT+08:00

类型 根CA

CA编号 eb4b6711-3db2-406c-8707-17b236cde073

有效期 - 1 + 年

预计到期时间 (不超过签发CA到期时间) : 2023/11/10 11:10:46 GMT+08:00

1. 选择证书请求文件生成方式。

表 2-8 证书请求文件

参数名称	参数说明
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	使用已有的CSR。需执行以下操作: 1. 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。 2. 单击“解析”。

参数名称	参数说明
说明	<ul style="list-style-type: none"> <li>- 证书请求文件（Certificate Signing Request, CSR）即证书签名申请，获取证书，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。</li> <li>- 建议选择“系统生成CSR”，避免出现内容不正确而导致的审核失败。</li> <li>- 手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥文件。私钥和数字证书一一对应，一旦丢失了私钥您的数字证书也将不可使用。</li> <li>- 证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。</li> </ul>

2. 配置证书主题信息。

仅当“证书请求文件”选择“系统生成文件”时，需要配置该参数。

“证书名称（CN）”：您可以自定义申请的私有证书的名称。

3. 单击“高级配置”右侧的<sup>^</sup>，进行高级配置。

仅当“证书请求文件”选择“系统生成文件”时，需要配置该参数。

表 2-9 高级配置

参数名称	参数说明	示例
密钥算法	选择待申请私有证书的密钥算法和密钥的位大小。 可选择“RSA2048”、“RSA4096”、“EC256”、“EC384”。	RSA2048
签名哈希算法	选择待申请私有证书的签名哈希算法： 可选择“SHA256”、“SHA384”、“SHA512”。	SHA256
密钥用法	选择待申请证书的密钥用法，支持选择（可多选）： <ul style="list-style-type: none"> <li>- digitalSignature（数字签名）</li> <li>- nonRepudiation（防抵赖）</li> <li>- keyEncipherment（密钥加密）</li> <li>- dataEncipherment（数据加密）</li> <li>- keyAgreement（密钥协议）</li> <li>- keyCertSign（证书签发）</li> <li>- cRLSign（黑名单签名）</li> <li>- encipherOnly（仅加密）</li> <li>- decipherOnly（仅解密）</li> </ul>	digitalSignature

参数名称	参数说明	示例
增强型密钥用法	选择待申请证书的增强型密钥用法，支持选择（可多选）： <ul style="list-style-type: none"><li>- 服务器身份验证</li><li>- 客户端身份验证</li><li>- 代码签名</li><li>- 安全电子邮件</li><li>- 时间戳</li></ul>	服务器身份验证
自定义扩展字段	填写待申请是的自定义信息。	-
（可选）配置证书AltName信息	如果该私有证书需要应用到多个主体，可以通过证书AltName添加其他主体的信息。 支持配置“IP address”、“DNS”、“Email”和“URI”四种类型的AltName信息。配置不同的类型AltName信息时，需要填写对应类型的值： <ul style="list-style-type: none"><li>- IP address: 填写IP地址</li><li>- DNS: 填写域名</li><li>- Email: 填写邮箱</li><li>- URI: 填写网络地址</li></ul> 最多可配置5条AltName信息。	-

#### 4. 选择签发CA。

表 2-10 签发 CA

参数名称	参数说明
CA名称（CN）	选择已创建的私有CA的名称。
类型	选择“CA名称（CN）”后，系统将自动显示该CA的类型。
CA编号	选择“CA名称（CN）”后，系统将自动显示该CA的编号。
有效期	设置私有证书的有效期。 <b>说明</b> <ul style="list-style-type: none"><li>- 您可以自定义私有证书有效期，该有效期不得超过当前已激活私有CA的有效期。</li><li>- 私有CA有效期最长为30年。</li></ul>

**步骤4** 确认信息以及价格无误后，单击“确定”。



申请成功后，系统将返回到私有证书页面，在页面右上角弹出“申请证书xxx成功！”，则说明私有证书申请成功。

----结束

## 后续处理

私有证书签发后，就可以下载到本地，并分发给证书主体进行安装使用，详细操作请参见[下载私有证书](#)。

## 2.3.2 下载私有证书

私有证书申请后，您可以将私有证书下载到本地。证书下载后，才可以分配给对应的证书主体进行安装使用。


本章节介绍如何下载私有证书，只有证书状态为“已签发”时，才可以下载。

## 前提条件

已申请私有证书并私有证书的状态为“已签发”，详细操作请参见[申请私有证书](#)。

## 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 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。

**步骤3** 在需要下载的私有证书所在行的“操作”列，单击下载。

图 2-15 下载私有证书

证书名称 (CN)	签发CA名称	创建时间	到期时间	状态	操作
887		2020/06/04 17:51:...	2021/06/04 17:49:...	已签发	<a href="#">下载</a>   <a href="#">吊销</a>   <a href="#">删除</a>
747		2020/06/04 16:10:...	2021/06/04 16:08:...	已签发	<a href="#">下载</a>   <a href="#">吊销</a>   <a href="#">删除</a>

**步骤4** 请根据您需要的服务器类型，在对应的“页面”单击“下载证书”，进行私有证书下载操作。

执行操作后，云证书管理服务将使用浏览器自带的下载工具，将私有证书文件下载至本地指定的位置。

----结束

## 私有证书安装说明

私有证书下载后需要安装到客户端/服务器上进行处理：

- 在客户端安装证书，您可以参考[在客户端安装私有证书](#)
- 在服务器安装证书，您可以参考[表2-11](#)

表 2-11 安装私有证书操作示例

服务器类型	操作示例
Tomcat	<a href="#">在Tomcat服务器上安装私有证书</a>
Nginx	<a href="#">在Nginx服务器上安装私有证书</a>
Apache	<a href="#">在Apache服务器上安装私有证书</a>
IIS	<a href="#">在IIS服务器上安装私有证书</a>
Weblogic	<a href="#">在Weblogic服务器上安装私有证书</a>
Resin	<a href="#">在Resin服务器上安装私有证书</a>

## 下载的证书文件说明

根据申请私有证书时，选择的“证书请求文件”方式（“系统生成文件”和“自己生成文件”）的不同，下载文件也有所不同。

- 系统生成文件

申请私有证书时，如果“证书请求文件”选择的是“系统生成文件”，则下载文件说明如[表 下载文件说明（一）](#)所示。

表 2-12 下载文件说明（一）

服务器类型	zip压缩包中包含的文件
Tomcat	keystorePass.txt：证书密码。 server.jks：证书文件。
Nginx	server.crt：证书文件，分别为服务器证书和证书链。 server.key：证书私钥文件。
Apache	chain.crt：证书链文件。 server.crt：证书文件。 server.key：证书私钥文件。
IIS	keystorePass.txt：证书密码。 server.pfx：证书文件。
其他	chain.pem：证书链文件。 server.key：证书私钥文件。 server.pem：证书文件。

- 自己生成文件

申请私有证书时，如果“证书请求文件”选择的是“自己生成文件”，则下载文件说明如[表 下载文件说明（二）](#)所示。

表 2-13 下载文件说明（二）

服务器类型	zip压缩包中包含的文件
Tomcat	server.crt: 证书文件。 chain.crt: 证书链文件。
Nginx	server.crt: 证书文件
Apache	server.crt: 证书文件。 chain.crt: 证书链文件。
IIS	server.crt: 证书文件。 chain.crt: 证书链文件。
其他	cert.pem: 证书文件。 chain.pem: 证书链文件。

## 2.3.3 安装私有证书

### 2.3.3.1 信任根 CA

在安装私有证书之前，需要根据实际验证需求将根CA加入客户端或服务器受信任的根证书颁发机构中。

#### 前提条件

已创建根CA并已导出私有根CA证书，导出私有CA证书的详细操作请参见[导出私有CA证书](#)。

#### 约束与限制

- 单向验证  
当服务端无需校验客户端的证书身份时（互联网上大部分公开的网站不校验客户端证书），为了使得客户端信任服务端证书，需要将服务端证书的根CA加入到客户端受信任的根证书颁发机构中。
- 双向验证  
当服务端与客户端皆需校验对方的证书时，需要双方将对方的根CA加入到自己的受信任的根证书颁发机构中。

#### 操作步骤

根据不同的操作系统选择以下方式，将根CA加入受信任的根证书颁发机构中：

##### 说明

以信任根CA“PCA TEST ROOT G0”为例。

- **Windows系统**
  - a. 将根CA证书文件后缀由“.pem”改为“.crt”，双击证书文件，根CA证书信息显示该根证书不受信任。

图 2-16 根 CA 不受信任



- b. 单击“安装证书”，根据使用场景选择证书存储位置，单击“下一步”。
- c. 选择“将所有证书都放入下列存储（P）”，单击“浏览”，选择“受信任的根证书颁发机构”，单击“确定”，如[图 存储根证书](#)所示。

图 2-17 存储根证书



- d. 单击“下一步”，再单击“确定”，会有弹窗提示“Windows将信任该私有根CA证书颁发的所有证书”，单击“是”。
- e. 双击根CA证书文件，此时根CA证书信息显示系统已信任该根CA证书，表示根CA加入受信任的根证书颁发机构成功。

图 2-18 信任根 CA



- **Linux系统**

不同版本的Linux操作系统中，根CA证书存放路径以及操作方法不一致，需要您根据实际情况进行操作。以下操作以Centos6版本的Linux系统为例：

- 将根CA证书文件复制到“/home/”路径下。
- 当服务器未安装“ca-certificates”时，使用如下命令安装“ca-certificates”。  
**yum install ca-certificates**
- 使用如下命令将根CA证书复制到“/etc/pki/ca-trust/source/anchors/”路径下。  
**cp /home/root.crt /etc/pki/ca-trust/source/anchors/**
- 使用如下命令将根CA证书添加到根证书信任文件中。  
**update-ca-trust extract**
- 使用如下命令查看根CA证书是否添加成功信息，查看到新添加的根CA证书信息表示根CA加入受信任的根证书颁发机构成功，如[图 新添加的根CA证书](#)所示。

### view /etc/pki/tls/certs/ca-bundle.crt

图 2-19 新添加的根 CA 证书



#### 说明

当openssl版本过低时，可能导致配置无法生效，可尝试使用yum update openssl -y 命令更新openssl版本。

- macOS系统
  - 打开mac的启动台，选择“钥匙串”。
  - 输入密码登录到“钥匙串”。
  - 将需要信任的根CA证书文件拖入钥匙串中，此时拖入的根CA证书会显示不被系统信任。
  - 选中根CA证书文件，单击鼠标右键选择“显示简介”。
  - 选择“信任>使用此证书时”，选择“始终信任”，单击“关闭”。
  - 输入密码使信任根CA证书配置生效。
  - 在“钥匙串”主页查看根CA证书，证书显示被信任表示根CA加入受信任的根证书颁发机构成功。

### 2.3.3.2 在客户端安装私有证书

本文介绍如何在客户端安装私有证书。

#### 前提条件

私有证书已签发，且已下载私有证书。下载证书操作请参见[下载私有证书](#)。

#### 约束条件

当服务器需要校验客户端证书时，需要在服务器将客户端证书的根CA加入到服务器受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。

## 操作步骤

以下操作以Windows系统为例。



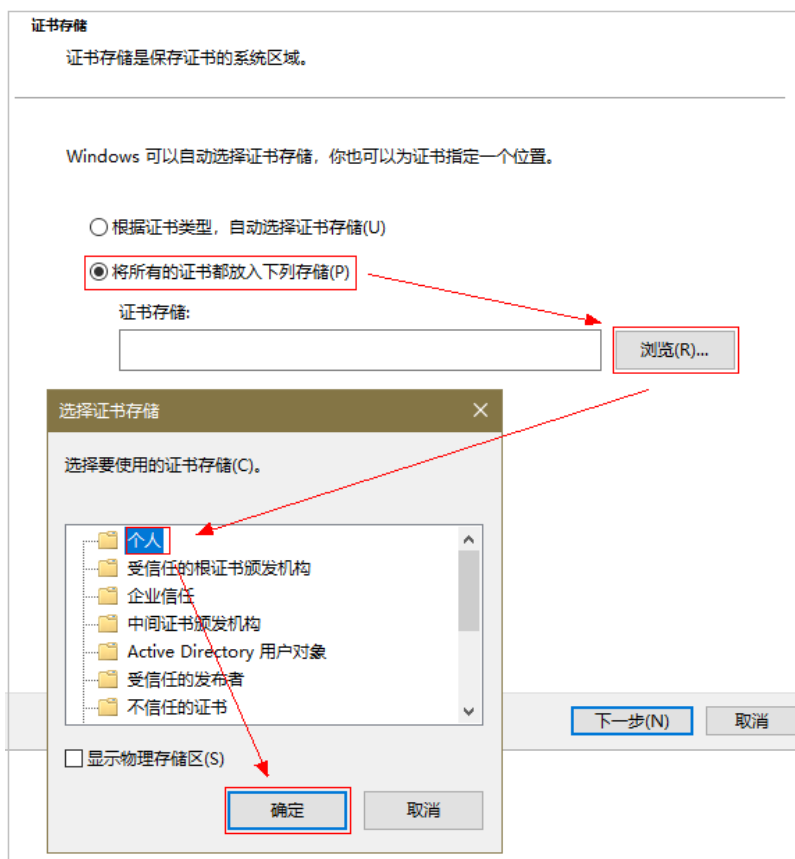
- 步骤1** 登录管理控制台。
- 步骤2** 单击页面左上方的 ，选择“安全与合规 > 云证书管理服务”，并在左侧导航栏选择“私有证书管理 > 私有证书”进入私有证书管理界面。
- 步骤3** 单击页面上方的“服务列表”，选择“安全 > 云证书管理服务”，进入云证书管理服务界面。
- 步骤4** 单击页面左上方的 ，选择“安全 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。
- 步骤5** 在目标证书所在行的“操作”列，单击“下载”，进入下载证书页面。
- 步骤6** 选择证书下载格式为“IIS”，单击“下载证书”。
- 步骤7** 解压下载的证书文件压缩包“client\_iis.zip”，解压后，获得证书文件“server.pfx”和私钥密码文件“keystorePass.txt”。
- 步骤8** 双击证书文件“server.pfx”，根据使用场景选择证书存储位置，单击“下一步”。
- 步骤9** 确认要导入的证书文件名，单击“下一步”。
- 步骤10** 输入从私钥密码文件“keystorePass.txt”中获取的密码，单击“下一步”。
- 步骤11** 选择“将所有的证书放入下列存储（P）”，单击“浏览”，选择“个人”，单击“确定”如图 [存储私有证书](#)所示。



图 2-20 存储私有证书



步骤12 单击“下一步”，单击“完成”，出现弹窗提示证书“导入成功”，证书安装成功。  
----结束

### 2.3.3.3 在服务器安装私有证书

#### 2.3.3.3.1 在 Tomcat 服务器上安装私有证书

本文以Linux操作系统中的Tomcat7服务器为例介绍私有证书的安装步骤。

##### 📖 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

##### 前提条件

- 证书已签发。
- 已下载Tomcat格式的私有证书，具体操作请参见[下载证书](#)。
- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。

##### 约束条件

- 证书安装前，务必在安装私有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。

- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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服务器上安装私有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

在本地解压已下载的Tomcat格式证书文件并获得证书文件“server.jks”和密码文件“keystorePass.txt”。

### 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2-14](#)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 2-14 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。 <b>须知</b> 如果密码中包含“&”，请将其替换成“&amp;”，以免配置不成功。 示例： 如果keystorePass="Ix6&APWgcHf72DMu"，则修改为keystorePass="Ix6&amp;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。

- 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">
```

- 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">
```

- 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。

## 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。

### 2.3.3.3.2 在 Nginx 服务器上安装私有证书

本文以CentOS 7操作系统中的Nginx 1.7.8服务器为例介绍私有证书的安装步骤。

## 📖 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

## 前提条件

- 证书已签发。
- 已下载Nginx格式的私有证书，具体操作请参见[下载证书](#)。
- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。

## 约束条件

- 证书安装前，务必在安装私有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。
- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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CentOS 7操作系统中的Nginx 1.7.8服务器上安装私有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验证配置是否正确 → ⑤重启Nginx → ⑥效果验证

### 步骤一：获取文件

在本地解压已下载的证书文件。

获得证书文件“server.crt”和私钥文件“server.key”。

- “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。
- “server.key”文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

### 步骤二：创建目录

在Nginx的安装目录下创建“cert”目录，并且将“server.key”和“server.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。

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2-15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 2-15 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，例如“cert/server.crt”。
ssl_certificate_key	私钥文件“server.key”。 设置为“server.key”的路径，例如“cert/server.key”。

4. 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。

#### 2.3.3.3.3 在 Apache 服务器上安装私有证书

本文以CentOS 7操作系统中的Apache 2.4.6服务器为例介绍私有证书的安装步骤。

##### 📖 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

#### 前提条件

- 证书已签发。

- 已下载Apache格式的私有证书，具体操作请参见[下载证书](#)。
- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。

## 约束条件

- 证书安装前，务必在安装私有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。
- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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CentOS 7操作系统中的Apache 2.4.6服务器上安装私有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

在本地解压已下载的证书文件。

获得证书文件“ca.crt”、“server.crt”和私钥文件“server.key”。

- “ca.crt”文件包括一段中级CA证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
- “server.crt”文件包括一段服务器证书代码“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”。
- “server.key”文件包括一段私钥代码“-----BEGIN RSA PRIVATE KEY-----”和“-----END RSA PRIVATE KEY-----”。

### 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
```
- 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，例如“cert/server.crt”。  
完整配置如下：  
SSLCertificateFile "cert/server.crt"
  - 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，例如“cert/server.key”。  
完整配置如下：  
SSLCertificateKeyFile "cert/server.key"
  - 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，例如“cert/ca.crt”。  
完整配置如下：  
SSLCertificateChainFile "cert/ca.crt"
  - 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。

- 执行**service httpd stop**命令停止Apache服务。
- 执行**service httpd start**命令启动Apache服务。

## 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。

### 2.3.3.3.4 在 IIS 服务器上安装私有证书

本章节介绍如何将私有证书安装到IIS服务器。

#### 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

## 前提条件

- 证书已签发。
- 已下载IIS格式的私有证书，具体操作请参见[下载证书](#)。



- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。

## 约束条件

- 证书安装前，务必在安装私有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。
- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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IIS服务器上安装私有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

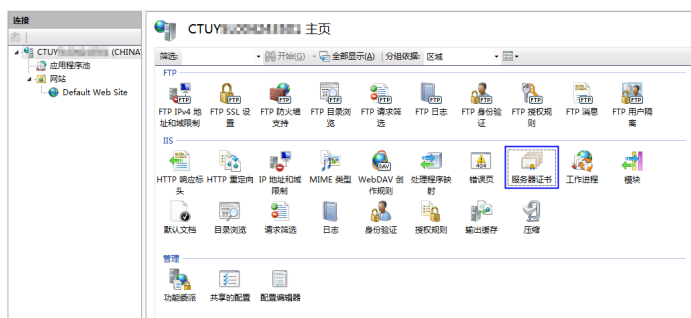
在本地解压已下载的证书文件。

获得证书文件“server.pfx”和密码文件“keystorePass.txt”。

### 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2-21](#)所示。

图 2-21 服务器证书



3. 在弹出的窗口中，单击“导入”，如[图2-22](#)所示。

图 2-22 导入



4. 导入“server.pfx”证书文件，单击“确定”。

**说明**

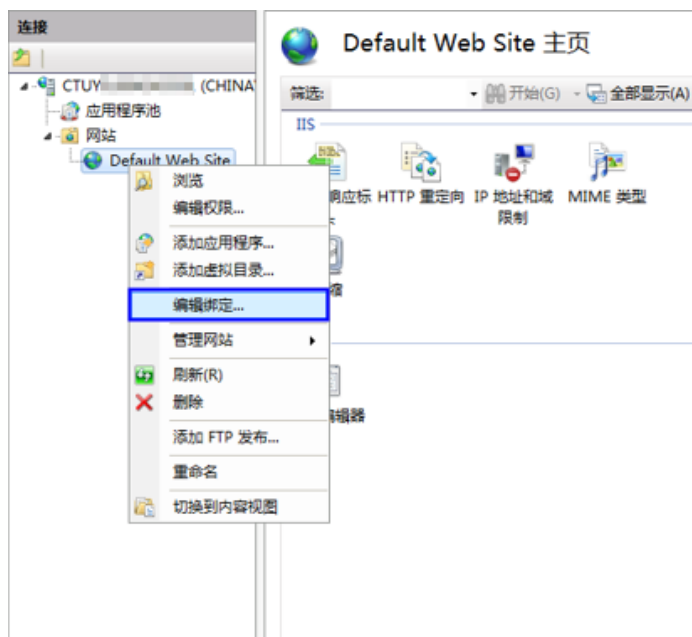
“密码”配置框内需要输入“keystorePass.txt”文件内的密码。

图 2-23 导入 pfx 证书文件



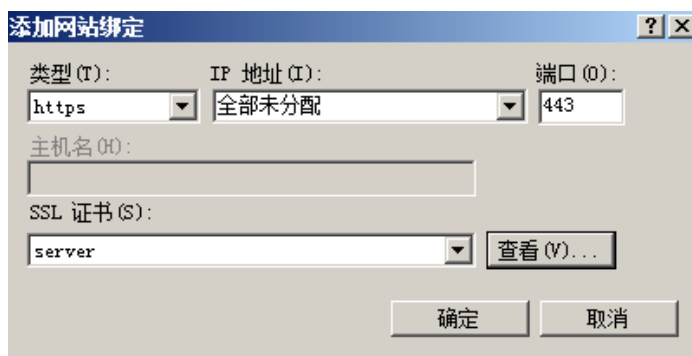
5. 鼠标右键单击目标站点（这里以默认站点为例），选择“编辑绑定”，如图2-24所示。

图 2-24 编辑绑定



6. 在弹出的窗口中，单击“添加”，并填写以下信息。

图 2-25 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”。

## 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。

### 2.3.3.3.5 在 Weblogic 服务器上安装私有证书

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。

本章节介绍如何将私有证书安装到Weblogic服务器。

### 📖 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

## 前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载Tomcat格式的私有证书，具体操作请参见[下载证书](#)。
- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。
- 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，务必在安装私有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。
- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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Weblogic服务器上安装私有证书的流程如下所示：

①[获取文件](#) → ②[配置Weblogic](#) → ③[效果验证](#)

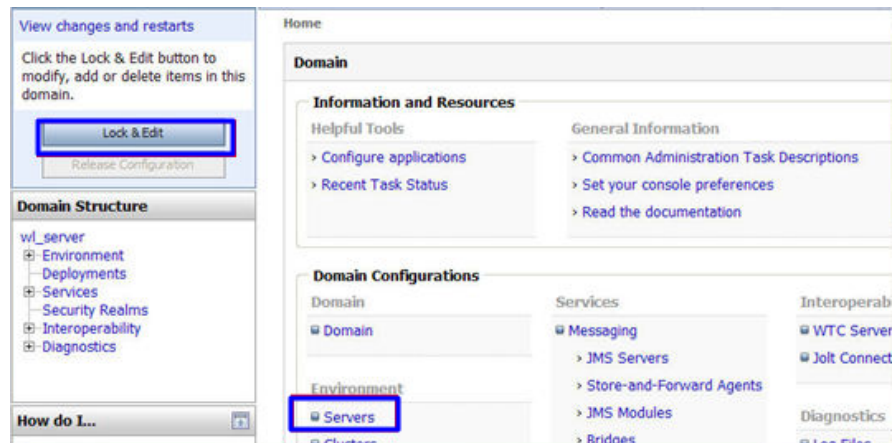
### 步骤一：获取文件

在本地解压已下载的Tomcat格式证书文件并获得证书文件“server.jks”和密码文件“keystorePass.txt”。

### 步骤二：配置 Weblogic

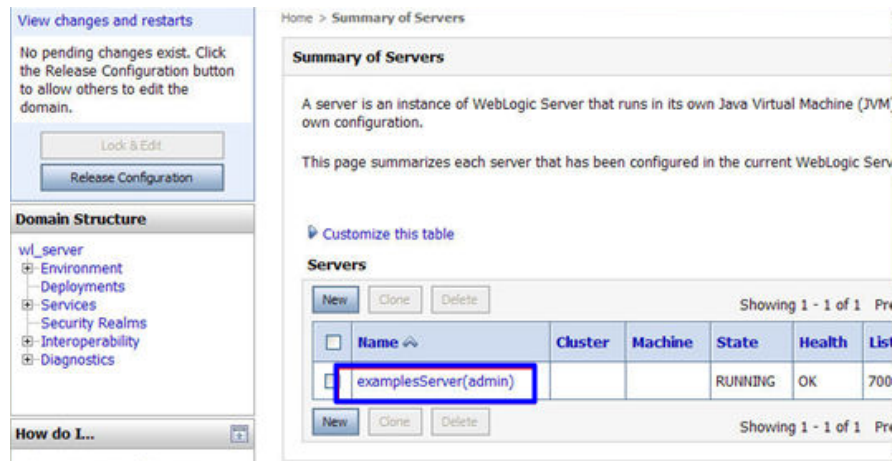
1. 登录Weblogic服务器管理控制台。
2. 单击页面左上方“Lock & Edit”，解锁配置。
3. 在“Domain Configurations”中，单击“Servers”。

图 2-26 服务器



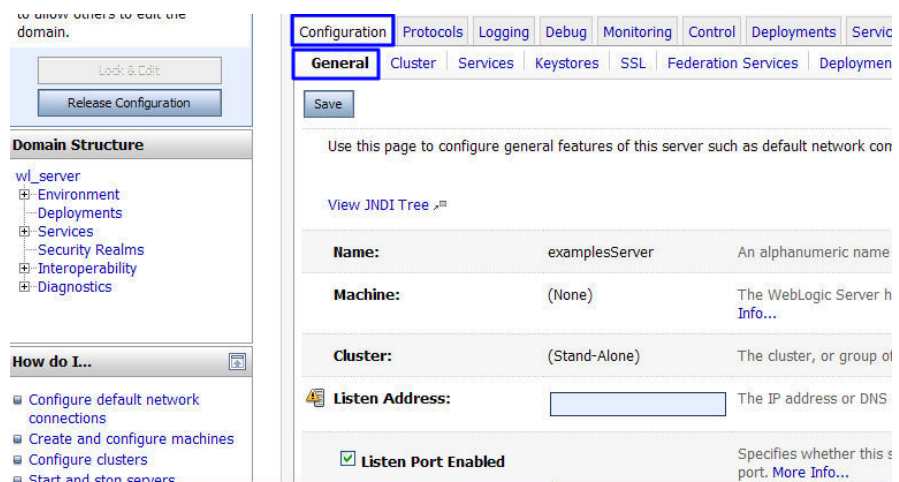
4. 在服务器列表中，选择您需要配置服务器证书的Server，进入服务器的设置页面。

图 2-27 目标服务器



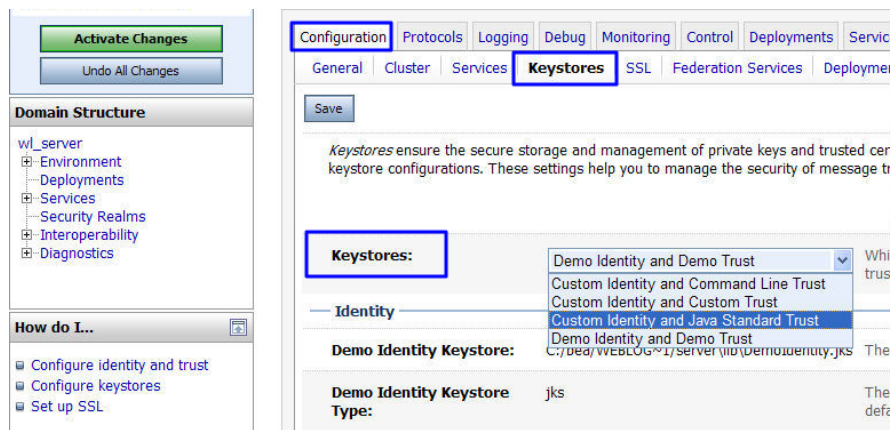
5. 修改HTTPS端口。  
在服务器的配置页面，选择“General”页签，配置是否启用HTTP和HTTPS，以及访问端口号。  
请勾选“Listen SSL Port Enabled”，并修改端口号为“443”。

图 2-28 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。

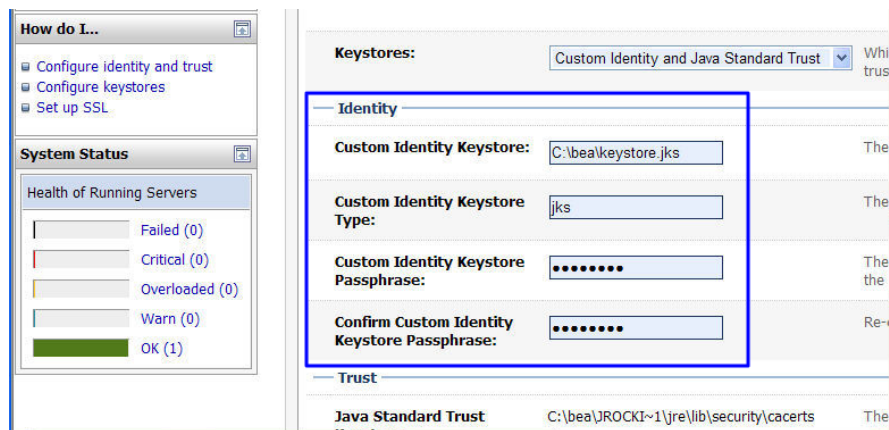
图 2-29 认证方式



- 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。

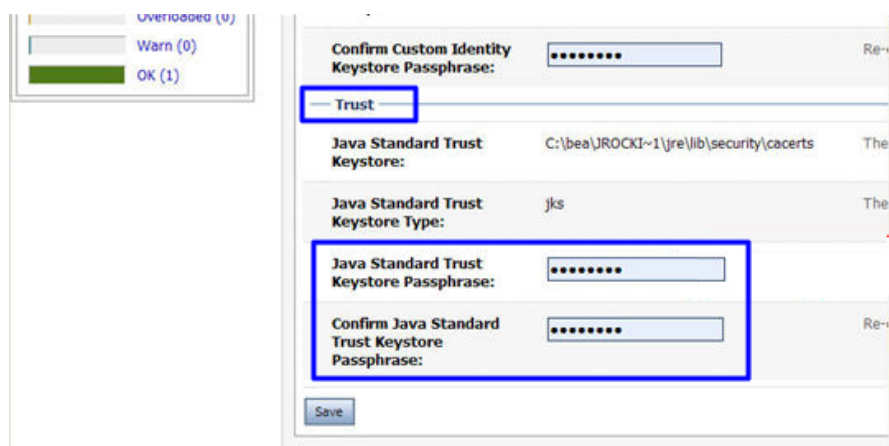
配置密钥库文件server.jks所保存的服务器上的路径，并填写密钥库文件密码。

图 2-30 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。

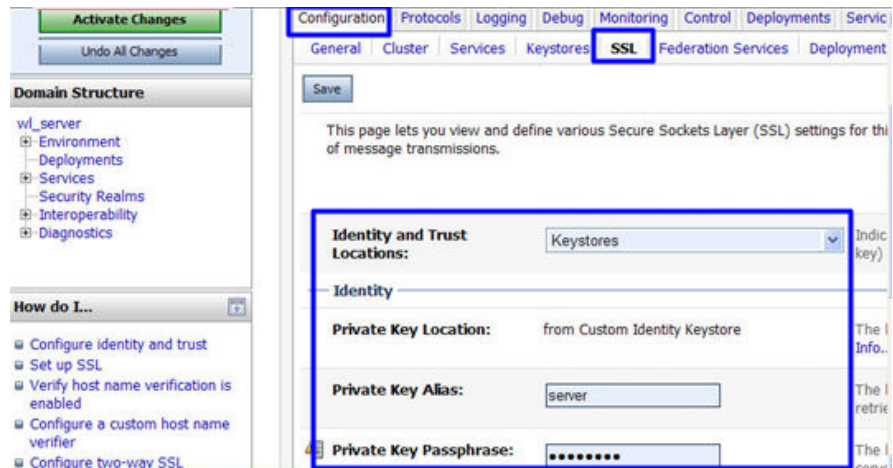
图 2-31 信任库文件



- **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:

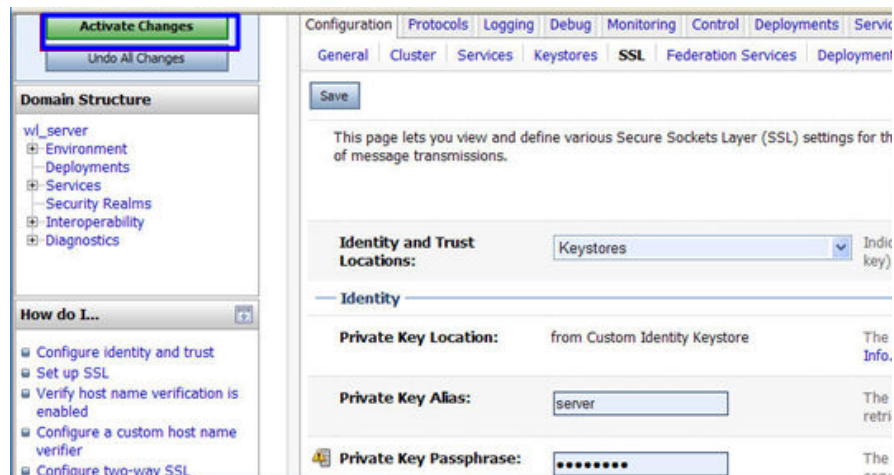


图 2-32 私钥



- **Identity and Trust Locations:** 请选择为“Keystores”。
  - **Private Key Alias:** 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。

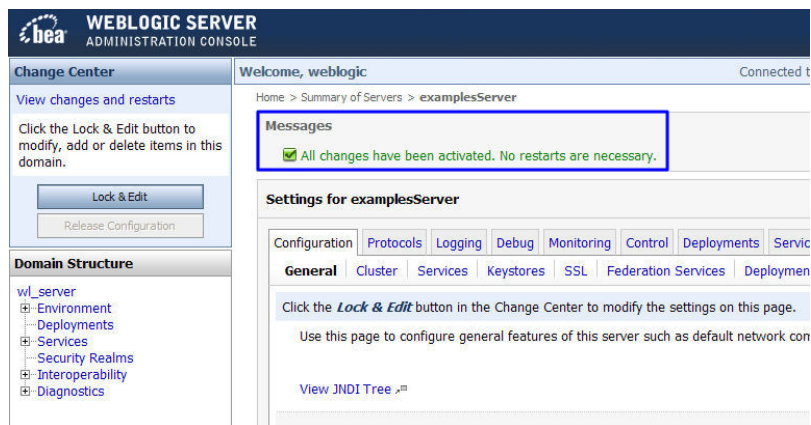
图 2-33 保存配置



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 2-34 所示，则无需重启。



图 2-34 提示信息



## 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。

### 2.3.3.3.6 在 Resin 服务器上安装私有证书

本章节介绍如何将私有证书安装到Resin服务器。

#### 📖 说明

由于服务器系统版本或服务器环境配置不同，在安装私有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。

## 前提条件

- 证书已签发且“证书状态”为“已签发”。
- 已下载Tomcat格式的私有证书，具体操作请参见[下载证书](#)。
- 申请证书时选择的“证书请求文件”生成方式为“系统生成文件”。

## 约束条件

- 证书安装前，务必在安装私有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。
- 为了使客户端信任服务器证书，需要将服务器证书的根CA加入到客户端受信任的根证书颁发机构中，详细操作请参见[信任根CA](#)。
- 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，即申请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Resin服务器上安装私有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

在本地解压已下载的Tomcat格式证书文件并获得证书文件“server.jks”和密码文件“keystorePass.txt”。

## 步骤二：配置 Resin

### 须知

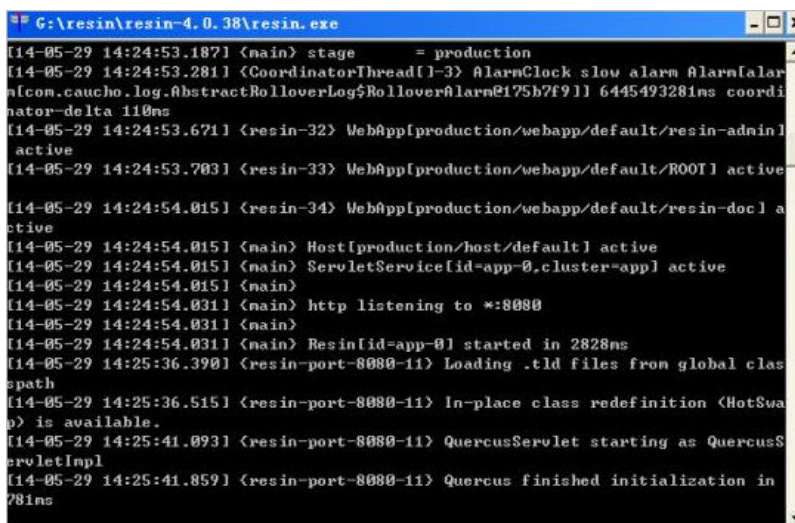
修改配置文件前，请将配置文件进行备份，并建议先在测试环境中进行部署，配置无误后，再在现网环境进行配置，避免出现配置错误导致服务不能正常启动等问题，影响您的业务。

#### 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2-35所示的命令提示符窗口。

图 2-35 提示窗口



```
G:\resin\resin-4.0.38\resin.exe
[14-05-29 14:24:53.187] <main> stage = production
[14-05-29 14:24:53.281] <CoordinatorThread[1-3] AlarmClock slow alarm Alarm[alar
alcom.caucho.log.AbstractRolloverLog$RolloverAlarm@175b7f9] 6445493281ms coordi
nator-delta 110ms
[14-05-29 14:24:53.671] <resin-32> WebApp[production/webapp/default/resin-admin]
active
[14-05-29 14:24:53.703] <resin-33> WebApp[production/webapp/default/ROOT] active
[14-05-29 14:24:54.015] <resin-34> WebApp[production/webapp/default/resin-doc] a
ctive
[14-05-29 14:24:54.015] <main> Host[production/host/default] active
[14-05-29 14:24:54.015] <main> ServletService[id=app-0,cluster=app] active
[14-05-29 14:24:54.015] <main>
[14-05-29 14:24:54.031] <main> http listening to *:8080
[14-05-29 14:24:54.031] <main>
[14-05-29 14:24:54.031] <main> Resin[id=app-0] started in 2828ms
[14-05-29 14:25:36.390] <resin-port-8080-11> Loading .tld files from global clas
spath
[14-05-29 14:25:36.515] <resin-port-8080-11> In-place class redefinition (HotSwa
p) is available.
[14-05-29 14:25:41.093] <resin-port-8080-11> QuercusServlet starting as QuercusS
ervletImpl
[14-05-29 14:25:41.859] <resin-port-8080-11> Quercus finished initialization in
781ms
```

- 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2-36所示时，则表示安装成功。

图 2-36 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。

```
# JSE 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2-16。

```
# JSE 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 2-16 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。<br><b>须知</b><br>如果密码中包含“&”，请将其替换成“&amp;”，以免配置不成功。<br>示例：<br>如果keystorePass="lx6&APWgcHf72DMu"，则修改为keystorePass="lx6&amp;APWgcHf72DMu"。 |

- e. 修改完成后保存配置文件。
3. 重启Resin。

## 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。

## 2.3.4 吊销私有证书

私有证书到期前，如果您不再需要使用该证书或者该私有证书私钥丢失，可以通过云证书管理控制台吊销该证书。私有证书吊销后，将不再被组织内部环境所信任。

私有证书吊销后，将不再继续计费。

本章节介绍吊销私有证书的操作步骤。

## 前提条件


私有证书的状态为“已签发”。

## 约束条件

- 吊销私有证书申请提交后，将无法取消，请谨慎操作。
- 吊销证书后，将清除该证书所有的记录，包括私有CA的记录，且无法恢复，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 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。

**步骤3** 在需要吊销的私有证书所在行的“操作”列，单击“吊销”。

图 2-37 吊销私有证书

| 证书名称 (CN) | 签发CA名称 | 创建时间                 | 到期时间                 | 状态  | 操作           |
|-----------|--------|----------------------|----------------------|-----|--------------|
| 887       |        | 2020/06/04 17:51:... | 2021/06/04 17:49:... | 已签发 | 下载   吊销   删除 |
| 747       |        | 2020/06/04 16:10:... | 2021/06/04 16:08:... | 已签发 | 下载   吊销   删除 |

**步骤4** 在弹出的对话框中，输入“REVOKE”，并选择吊销原因，以确认吊销证书信息。默认的吊销原因为“UNSPECIFIED”，吊销原因可选值及其含义如表 吊销理由及含义所示。

图 2-38 吊销私有证书提示信息

**你确定要吊销以下证书吗?**

吊销证书后，该证书将不可用，吊销操作无法恢复，请谨慎操作。  
请在下方输入框输入REVOKE确认吊销以下证书。

请输入REVOKE确认吊销

| 证书名称 (CN) | 状态  |
|-----------|-----|
| te        | 已签发 |

吊销原因: UNSPECIFIED

确定 取消

表 2-17 吊销原因及含义

| 吊销理由                             | 对应RFC 5280标准中的吊销理由码 | 含义               |
|----------------------------------|---------------------|------------------|
| UNSPECIFIED                      | 0                   | 吊销时未指定吊销原因，为默认值  |
| KEY_COMPROMISE                   | 1                   | 证书密钥材料泄露         |
| CERTIFICATE_AUTHORITY_COMPROMISE | 2                   | 签发路径上，存在CA密钥材料泄露 |
| AFFILIATION_CHANGED              | 3                   | 证书中的主体或其他信息已经被改变 |
| SUPERSEDED                       | 4                   | 证书已被取代           |

| 吊销理由                           | 对应RFC 5280标准中的吊销理由码 | 含义                  |
|--------------------------------|---------------------|---------------------|
| CESSATION_OF_OPERATION         | 5                   | 证书或签发路径中的实体已停止运营    |
| CERTIFICATE_HOLD               | 6                   | 证书当前不应被视为有效，将来可能会生效 |
| PRIVILEGE_WITHDRAWN            | 9                   | 证书不再有权声明其列出的属性      |
| ATTRIBUTE_AUTHORITY_COMPROMISE | 10                  | 担保证书属性的机构可能已受到损害    |

**步骤5** 单击“确定”。

当页面右上角弹出“吊销证书xxx成功！”，且私有证书状态将更新为“已吊销”，则说明吊销成功。

----结束

## 2.3.5 查看私有证书详情


该任务指导用户查看已申请私有证书的详细信息，包括私有证书名称、到期时间和状态等。

### 前提条件

已申请私有证书，详细操作请参见[申请私有证书](#)。


### 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 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。

**步骤3** 查看私有证书信息，证书参数说明如[表2-18](#)所示。

#### 说明

- 在“所有状态”搜索栏选择证书状态，证书列表界面将只显示对应状态的证书。
- 在私有证书列表右上角的搜索框中输入证书名称，单击 或按“Enter”，可以搜索指定的证书。

**表 2-18** 证书参数说明

| 参数名称      | 说明              |
|-----------|-----------------|
| 证书名称 (CN) | 申请证书时设置的私有证书名称。 |

| 参数名称   | 说明                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 签发CA名称 | 签发私有证书对应私有CA的名称。                                                                                                                                 |
| 创建时间   | 私有证书创建的时间。                                                                                                                                       |
| 到期时间   | 私有证书到期的时间。                                                                                                                                       |
| 状态     | 私有证书的状态，说明如下： <ul style="list-style-type: none"> <li>已签发<br/>私有证书处于已签发状态。</li> <li>已过期<br/>私有证书处于已过期状态。</li> <li>已吊销<br/>私有证书处于已吊销状态。</li> </ul> |
| 操作     | 用户可以在操作栏中，执行下载、吊销和删除证书等操作。                                                                                                                       |

**步骤4** 用户可单击私有证书名称，查看私有证书的详细信息，如图2-39所示。

您可在私有证书详情页单击“添加标签”标识私有证书。如果您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，建议在TMS中创建预定义标签。

图 2-39 私有证书详细信息



----结束

## 2.3.6 删除私有证书

删除证书是指将证书资源从系统中删除。证书仍然有效，浏览器仍然信任该证书。

如果您要删除不再需要的证书，请参照本章节进行处理。

### 前提条件


证书状态为“已到期”、“已签发”或“已吊销”。

## 约束条件

- 证书删除后将无法恢复，请谨慎操作。
- 删除证书申请提交后，将无法取消，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 > 云证书管理服务”，并在左侧导航栏选择“私有证书”进入私有证书管理界面。

**步骤3** 在需要删除的私有证书所在行的“操作”列，单击“删除”。

图 2-40 删除私有证书

| 证书名称 (CN) | 签发CA名称 | 创建时间                 | 到期时间                 | 状态  | 操作                  |
|-----------|--------|----------------------|----------------------|-----|---------------------|
| 887       |        | 2020/06/04 17:51:... | 2021/06/04 17:49:... | 已签发 | 下载   吊销   <b>删除</b> |
| 747       |        | 2020/06/04 16:10:... | 2021/06/04 16:08:... | 已签发 | 下载   吊销   删除        |

**步骤4** 在弹出的对话框中输入“DELETE”，以确认删除证书信息。

图 2-41 删除私有证书提示信息



**步骤5** 单击“确定”，页面右上角弹出“删除证书xxx成功！”，则说明删除成功。

----结束

## 2.4 权限管理

### 2.4.1 创建用户并授权使用 CCM

如果您需要对您所拥有的CCM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CCM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CCM资源委托给更专业、高效的其他账号或者云服务，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CCM服务的其它功能。

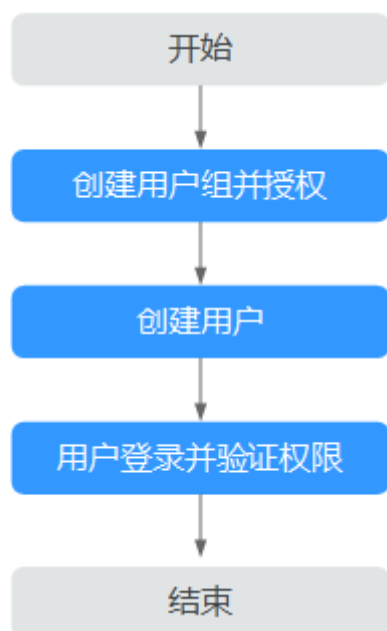
本章节为您介绍对用户授权的方法，操作流程如图 [给用户授权CCM权限流程](#)所示。

## 前提条件

给用户组授权之前，请您了解用户组可以添加的CCM权限，并结合实际需求进行选择，CCM支持的系统权限，请参见[CCM系统权限](#)。

## 示例流程

图 2-42 给用户授权 CCM 权限流程



1. 创建用户组并授权  
在IAM控制台创建用户组，并授予私有证书管理服务管理员权限“PCA FullAccess”。
2. 在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 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“PCA FullAccess”已生效。

### 2.4.2 CCM 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。

目前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。

本章为您介绍常用的CCM自定义策略样例。

## CCM 自定义策略样例

- 示例1：授权用户创建CA

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "pca:ca:create"
      ],
      "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“PCA FullAccess”的系统策略，但不希望用户拥有“PCA FullAccess”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“PCA FullAccess”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": [
        "pca:ca:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

# 3 常见问题

## 3.1 什么是公钥和私钥？

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

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

### 说明

由于私钥的非公开属性，建议在证书申请过程中，由客户自己生成私钥，并妥善保管。一旦发生证书私钥丢失的事件，请立刻吊销已有证书并对相关域名重新申购SSL证书。以避免因私钥丢失导致网站信息泄露等恶性事件的发生。

## 数字证书的原理

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

由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。

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

## 创建私钥

云证书管理对您的私有密钥的加密算法和长度有如下要求：

- 加密算法使用RSA算法
- 加密长度至少2048位

### 📖 说明

建议您使用2048位加密长度的SHA256摘要算法。

您可以通过以下两种方式创建您的私钥：

- 使用OpenSSL工具生成私钥

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

### 📖 说明

要求OpenSSL版本必须是1.0.1g或以上版本。

安装OpenSSL工具后，在命令行模式下运行**openssl genrsa -out myprivate.pem 2048**即可生成您的私钥文件。

- “myprivate.pem” 即为您的私钥文件。
- “2048” 指定加密长度。

- 使用Keytool工具导出私钥

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

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

在导出的文件中，以下部分的内容即是您的私钥：

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

或者

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

### 须知

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

## 3.2 为什么要使用无密码保护的私钥？

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

在您生成私钥时，请去掉密码保护后再进行上传。

### 如何去除私钥密码保护

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

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

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

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

## 什么样的私钥是有密码保护的

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

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

### 说明

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

## 3.3 主流数字证书有哪些格式？

主流的Web服务软件，通常都基于OpenSSL和Java两种基础密码库。

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

### 查看证书文件的格式

- 您可以使用以下方法简单区分带有后缀扩展名的证书文件：
  - \*.DER或\*.CER文件：这样的证书文件是二进制格式，只含有证书信息，不包含私钥。
  - \*.CRT文件：这样的证书文件可以是二进制格式，也可以是文本格式，一般均为文本格式，功能与\*.DER及\*.CER证书文件相同。
  - \*.PEM文件：这样的证书文件一般是文本格式，可以存放证书或私钥，或者两者都包含。\*.PEM文件如果只包含私钥，一般用\*.KEY文件代替。

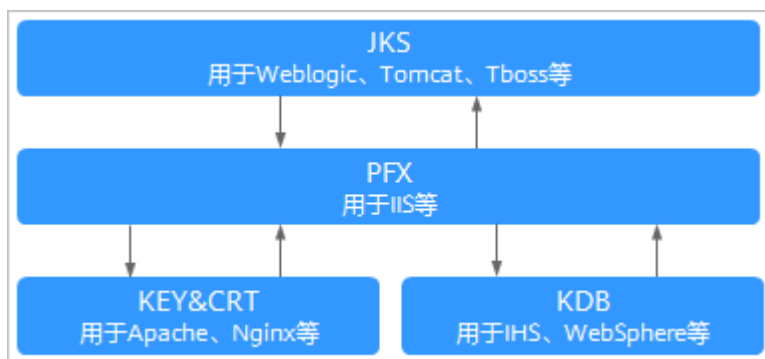
- \*.PFX或\*.P12文件：这样的证书文件是二进制格式，同时包含证书和私钥，且一般有密码保护。
- 您也可以使用记事本直接打开证书文件。如果显示的是规则的数字和字母，则表示该证书文件是文本格式。  
举例：

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

## 证书格式转换

证书格式之间是可以互相转换的，如图3-1所示。

图 3-1 证书格式转换



您可使用以下方式实现证书格式之间的转换：

- 将JKS格式证书转换为PFX格式  
您可以使用JDK中自带的Keytool工具，将JKS格式证书文件转换成PFX格式。  
例如，您可以执行以下命令将“server.jks”证书文件转换成“server.pfx”证书文件：  
**keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -srcstoretype JKS -deststoretype PKCS12**
- 将PFX格式证书转换为JKS格式  
您可以使用JDK中自带的Keytool工具，将PFX格式证书文件转换成JKS格式。  
例如，您可以执行以下命令将“server.pfx”证书文件转换成“server.jks”证书文件：  
**keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks -srcstoretype PKCS12 -deststoretype JKS**
- 将PEM/KEY/CRT格式证书转换为PFX格式  
您可以使用OpenSSL工具，将KEY格式密钥文件和CRT格式公钥文件转换成PFX格式证书文件。  
例如，将您的KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）复制至OpenSSL工具安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pfx”证书文件：  
**openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt**

- 将PFX格式证书转换为PEM/KEY/CRT格式  
您可以使用[OpenSSL](#)工具，将PFX格式证书文件转化为PEM格式证书文件、KEY格式密钥文件和CRT格式公钥文件。  
例如，将您的PFX格式证书文件复制至OpenSSL安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pem”证书文件、KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）：  

```
openssl pkcs12 -in server.pfx -nodes -out server.pem  
openssl rsa -in server.pem -out server.key  
openssl x509 -in server.pem -out server.crt
```

#### 须知

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

## 3.4 如何制作 CSR 文件？

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

#### 说明

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

手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥。

此处提供2种制作方法，请根据您的需要进行选择：

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

#### 说明

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

## 使用 OpenSSL 工具生成 CSR 文件

**步骤1** 安装[OpenSSL](#)工具。

**步骤2** 执行以下命令生成CSR文件。

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

- -new：指定生成一个新的CSR。

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

**步骤3** 生成CSR文件“mydomain.csr”。

**图 3-2** 生成 CSR 文件

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

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

需要输入的信息说明如下:

| 字段                       | 说明                                 | 示例                              |
|--------------------------|------------------------------------|---------------------------------|
| Country Name             | 申请单位所属国家, 只能是两个字母的国家码。例如, 中国只能是CN。 | CN                              |
| State or Province Name   | 申请单位所在省名或州名, 可以是中文或英文。             | ZheJiang                        |
| Locality Name            | 申请单位所在城市名, 可以是中文或英文。               | HangZhou                        |
| Organization Name        | 申请单位名称法定名称, 可以是中文或英文。              | HangZhou xxx Technologies, Inc. |
| Organizational Unit Name | 申请单位的所在部门, 可以是中文或英文。               | IT Dept.                        |



| 字段                   | 说明                                                                                                                                          | 示例              |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Common Name          | 申请SSL证书的具体网站域名。<br><b>说明</b> <ul style="list-style-type: none"><li>多域名类型的证书，请填写需要绑定的主域名。</li><li>泛域名类型的证书，请填写泛域名。示例：*.example.com</li></ul> | www.example.com |
| Email Address        | 申请单位的邮箱。<br>无需输入，请直接按“Enter”。                                                                                                               | -               |
| A challenge password | 设置CSR文件密码。<br>无需输入，请直接按“Enter”。                                                                                                             | -               |

#### 说明

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

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

----结束

## 使用 Keytool 工具生成 CSR 文件

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

**步骤2** 使用Keytool工具生成keystore证书文件。

#### 说明

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

1. 执行以下命令生成keystore证书文件。

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

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

图 3-3 生成 keystore 证书文件

```

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

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

```

2. 输入证书保护密码，然后根据下表依次输入所需信息：

| 问题                                                 | 说明                                                                                         | 示例                            |
|----------------------------------------------------|--------------------------------------------------------------------------------------------|-------------------------------|
| What is your first and last name?                  | 申请证书的域名。<br><b>说明</b><br>- 多域名类型的证书，请填写需要绑定的主域名。<br>- 泛域名类型的证书，请填写泛域名。示例：<br>*.example.com | www.example.com               |
| What is the name of your organizational unit?      | 申请单位的所在部门名称。                                                                               | IT Dept                       |
| What is the name of your organization?             | 申请单位的所在公司名称。                                                                               | HangZhou xxx Technologies,Ltd |
| What is the name of your City or Locality?         | 申请单位的所在城市。                                                                                 | HangZhou                      |
| What is the name of your State or Province?        | 申请单位的所在省份。                                                                                 | ZheJiang                      |
| What is the two-letter country code for this unit? | 申请单位所属国家，ISO 国家代码（两位字符）。                                                                   | CN                            |

输入完成后，确认输入内容是否正确，输入Y表示正确。

3. 根据提示输入密钥密码。可以与证书密码一致，如果一致直接按回车键即可。

### 步骤3 通过证书文件生成证书请求。

1. 执行以下命令生成CSR文件。

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

- -sigalg: 指定摘要算法, 使用SHA256withRSA。
  - -alias: 指定别名, 必须与--alias中keystore文件中的证书别名一致。
  - -keystore: 指定证书文件。
  - -file: 指定证书请求文件 (CSR), 名称可自定义。
2. 根据提示输入证书密码即可以生成“mydomain.csr”。

----结束

## 3.5 如何解决“审核失败 - 主域名不能为空”的问题?

### 问题描述

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

### 问题原因

在创建CSR文件时, 未正确填写Common Name字段。

### 解决方法

重新制作并上传CSR文件, 确保正确填写Common Name字段。

#### 须知

Common Name字段必须是证书绑定的主域名。

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

## 3.6 私有证书有效期相关问题

### 私有证书的有效期是多久?

私有证书的有效期是您根据申请证书时设置的有效期而定的。

#### 📖 说明

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

图 3-4 设置有效期

The screenshot shows a web interface for certificate configuration. At the top, there are two tabs: '证书请求文件' and '系统生成文件' (selected). Below the tabs is the '证书配置' section, which includes a text input for '证书名称 (CN)'. Underneath is the '高级配置' section with sub-tabs for '密钥算法', '签名哈希算法', '密钥用法', '自定义扩展字段', and '配置证书AltName信息'. The '选择签发CA' section contains a dropdown for 'CA名称 (CN)', a '到期时间' field showing '2021/09/26 14:51:41 GMT+08:00', and fields for '类型' and 'CA编号'. At the bottom, the '有效期' is set to '1' year, with a '到期时间' field also showing '2021/09/26 14:51:41 GMT+08:00'. A red box highlights the '有效期' dropdown and its corresponding '到期时间' field.

私有证书由处于激活状态的CA进行签发

证书申请成功后，可在私有证书列表页面查看证书到期时间，如图3-5所示。私有证书到期后，需重新申请。

图 3-5 到期时间

The screenshot shows a table of private certificates. The table has columns for '证书名称 (CN)', '签发CA名称', '创建时间', '到期时间', '状态', and '操作'. The '到期时间' column is highlighted with a red box. The table contains three rows of certificate data.

| 证书名称 (CN)              | 签发CA名称               | 创建时间                          | 到期时间                          | 状态  | 操作       |
|------------------------|----------------------|-------------------------------|-------------------------------|-----|----------|
| create_cert_123        | create_ca_162400693  | 2021/07/27 15:51:18 GMT+08:00 | 2026/06/18 15:19:26 GMT+08:00 | 已吊销 | 删除       |
| create_cert_1626330346 | create_ca_1624003511 | 2021/07/15 14:25:49 GMT+08:00 | 2022/07/15 14:26:49 GMT+08:00 | 已签发 | 下载 吊销 删除 |
| create_cert_1626330019 | create_ca_1624003511 | 2021/07/15 14:20:20 GMT+08:00 | 2022/07/15 14:21:20 GMT+08:00 | 已签发 | 下载 吊销 删除 |

## 私有证书的有效期快到了，怎么避免业务中断？

为了避免证书过期，导致业务中断，您需要提前轮换证书。在旧证书过期前，用新签发的证书进行替换。

## 3.7 私有证书管理服务是如何收费的？

私有CA和私有证书都是按需计费，将根据您的私有CA数量、私有证书数量进行收费。具体收费情况以购买页面显示为准。

### 如何停止私有 CA 或私有证书的计费？

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

如需停止计费，删除申请的私有CA和私有证书即可。

 **注意**

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

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

### 3.8 私有证书签发后，能否停用私有 CA？

您可以根据实际情况选择以下方法停用私有CA的部分功能或者停用私有CA：

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

 **注意**

私有CA禁用期间也将持续计费。

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

# A 修订记录

| 发布日期       | 修改说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2023-03-30 | <p>第二次正式发布。</p> <p>更新如下章节，刷新图片：</p> <ul style="list-style-type: none"><li>● <a href="#">基本概念</a></li><li>● <a href="#">禁用私有CA</a></li><li>● <a href="#">启用私有CA</a></li><li>● <a href="#">取消删除私有CA</a></li></ul> <p>更新如下章节，新增内容：</p> <ul style="list-style-type: none"><li>● <a href="#">创建私有CA</a></li><li>● <a href="#">下载私有证书</a></li><li>● <a href="#">CCM自定义策略</a></li></ul> <p>新增如下章节：</p> <ul style="list-style-type: none"><li>● <a href="#">个人数据保护机制</a></li><li>● <a href="#">在Weblogic服务器上安装私有证书</a></li><li>● <a href="#">在Resin服务器上安装私有证书</a></li><li>● <a href="#">创建用户并授权使用CCM</a></li><li>● <a href="#">私有证书管理服务是如何收费的？</a></li></ul> |
| 2022-12-15 | 第一次正式发布。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |