云证书管理服务

私有证书用户指南

文档版本 13

发布日期 2024-05-30

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 私有证书申请概述

私有证书管理（Private Certificate Authority，PCA）是一个私有CA和私有证书管理平台。它让用户可以通过简单的可视化操作，建立用户自己完整的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。如需使用在Internet上受信任的证书，请购买SSL证书，具体操作请参见**购买SSL证书**。

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 1-1 私有证书申请流程

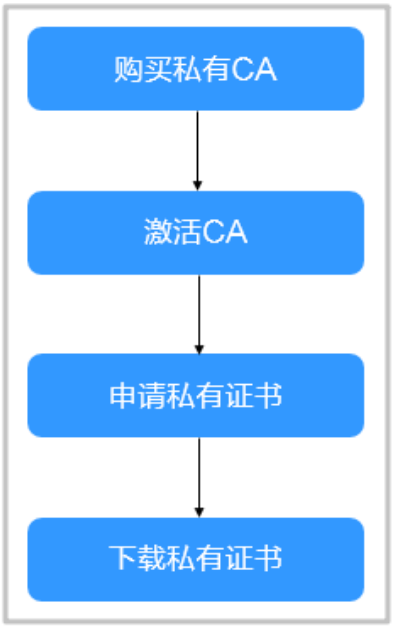


表 1-1 私有证书申请流程说明

步骤	申请操作	说明
1	**购买私有CA**	根据需要购买私有CA。

步骤	申请操作	说明
2	**激活私有CA**	购买私有CA实例后，需要激活才能用于签发证书。 您可以选择激活已购买的私有CA实例为**根CA**或**子CA**。激活后私有CA正式生效，并且可用于签发私有证书。
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 管理私有 CA

2.1 购买私有 CA

华为云云证书管理服务提供有PCA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购买私有CA。

背景信息

- 每个用户可以创建1000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CA”进入私有CA管理界面。

步骤3 在私有CA列表右上角，单击“购买私有CA”，进入购买CA界面。

步骤4 在私有CA购买界面，选择购买规格，参数说明如**表 购买私有CA参数说明**所示。

表 2-1 购买私有 CA 参数说明

参数名称	参数说明
计费模式	私有CA当前仅支持选择“包年/包月”计费模式。
服务类型	购买私有CA，服务类型请选择“私有CA”
区域	PCA为全区域可用服务，无需选择可用区域

参数名称	参数说明
密钥算法	支持选择以下两种密钥算法，请根据您的业务需求选择： ● 国际算法 RSA/ECC ● 国密算法 SM2
购买时长	根据您的业务需求选择时长，为避免因服务到期未及时续费影响您的业务，建议勾选“自动续费。
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。 从下拉列表中选择所在的企业项目。
购买量	根据您的实际情况，输入需要购买的私有CA数量。
标签（可选）	为您当前购买的私有CA添加标签，具体操作请参见**创建标签**。

步骤5 配置好购买参数后，单击右下角“立即购买”。

步骤6 在购买确认界面检查您当前购买的私有CA规格参数，确认无误后，请阅读《云证书管理服务（CCM）免责声明》并勾选“我已阅读并同意《云证书管理服务（CCM）免责声明》”。

步骤7 单击“去支付”进入付款页面，单击“确认付款”，完成支付，购买成功。

须知

付款后将开始计算服务时长，请您付款后尽快前往控制台激活CA。

----结束

后续操作

私有CA购买完成后，需要激活CA方可使用。激活私有CA操作请参见**激活私有CA**。

2.2 激活私有 CA

当您购买私有CA实例后，需要在购买后进行激活。激活后，才能使私有CA正式生效，用于签发私有证书。

本章节指导用户如何激活CA，您可以选择激活当前CA实例为根CA或子CA，**首次激活**CA实例需要选择激活为根CA，请根据您的业务实际需求进行选择。

前提条件

- 已购买私有CA实例，详细操作请参见**购买私有CA**。
- 私有CA处于“待激活”状态。

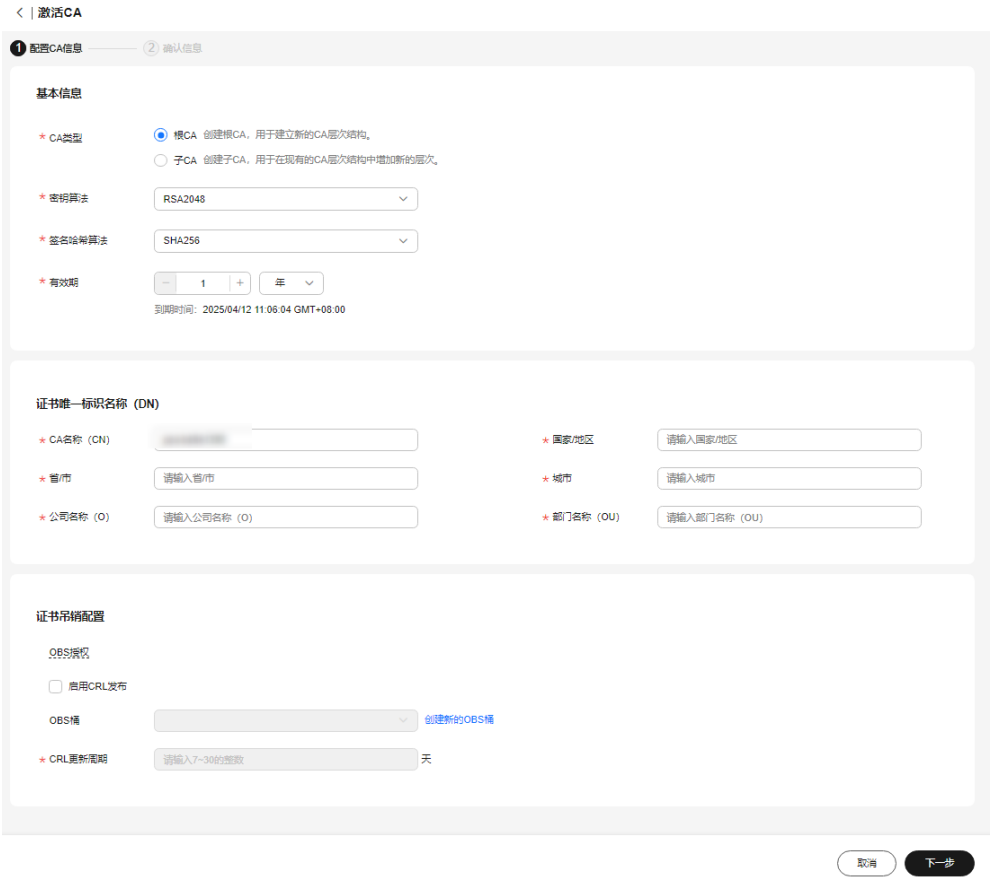
激活为根 CA

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CA”进入私有CA管理界面。

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

图 2-1 配置 CA 信息



1. 激活为根CA需要选择“CA类型”为“根CA”
   根CA：用于建立新的CA层次结构。
2. 配置以下参数。

表 2-2 根 CA 参数配置

参数名称		参数说明
基本信息	密钥算法	选择密钥算法： – RSA2048 – RSA3072 – RSA4096 – EC256 – EC384
	签名哈希算法	选择签名哈希算法： – SHA256 – SHA384 – SHA512 – SHA256_PSS – SHA384_PSS – SHA512_PSS
	有效期	选择私有CA有效期，可选择的最长有效期为30年。
证书唯一标识名称（DN）	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。 CN
	省/市	申请单位所在省名或市名，可以是中文或英文。 ShenZhen
	城市	申请单位所在城市名，可以是中文或英文。 GuangZhou
	公司名称（O）	申请单位法定名称，可以是中文或英文。 -
	部门名称（OU）	申请单位的所在部门，可以是中文或英文。 Cloud Dept.
证书吊销配置（可选）	OBS授权	确认是否授权PCA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。

参数名称		参数说明
	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4 确认填写的信息无误后，单击“下一步”。

步骤5 在信息确认页面对您已填写的参数进行二次确认，确认无误后单击“确认并激活”完成根CA激活。

----结束

使用已有 CA 激活子 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CA”进入私有CA管理界面。

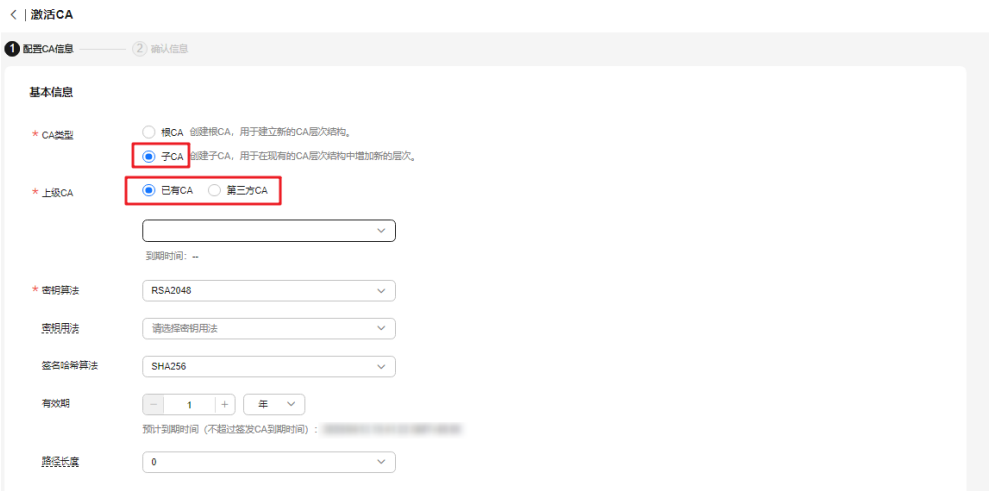
步骤3 在待激活的私有CA所在行的“操作”列，单击“激活”，系统从弹出激活CA详细页面，请填写激活CA相关信息。

1. 激活为子CA需要选择“CA类型”为“子CA”

   子CA：用于在现有的CA层次结构中增加新的层次。

2. 激活为子CA需要先选择上级CA，如图 选择上级CA。

图 2-2 选择上级 CA



- 选择“已有CA”，在下拉列表选择已创建的CA，并配置以下参数

参数名称		参数说明
基本信息	密钥算法	选择密钥算法： ■ RSA2048 ■ RSA3072 ■ RSA4096 ■ EC256 ■ EC384
	密钥用法（可选）	选择密钥用法： ■ digitalSignature ■ nonRepudiation ■ keyEncipherment ■ dataEncipherment ■ keyAgreement ■ keyCertSign ■ cRLSign ■ encipherOnly ■ decipherOnly
	签名哈希算法	选择签名哈希算法： ■ SHA256 ■ SHA384 ■ SHA512 ■ SHA256_PSS ■ SHA384_PSS ■ SHA512_PSS
	有效期	选择私有CA有效期，可选择的最长有效期为20年。
	路径长度	该子CA的路径长度，即当前CA可以签发下级子CA的层次数量，用于控制证书链深度。 **说明** 证书链是指根CA、子CA、私有证书三者之间通过层层信任关系链接而成的序列。

参数名称		参数说明
证书唯一标识名称（DN）	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。 CN
	省/市	申请单位所在省名或市名，可以是中文或英文。 ShenZhen
	城市	申请单位所在城市名，可以是中文或英文。 GuangZhou
	公司名称（O）	申请单位法定名称，可以是中文或英文。 -
	部门名称（OU）	申请单位的所在部门，可以是中文或英文。 Cloud Dept.
证书吊销配置（可选）	OBS授权	确认是否授权PCA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4 确认填写的信息无误后，单击“下一步”。

步骤5 在信息确认页面对您已填写的参数进行二次确认，确认无误后单击“确认并激活”完成子CA激活。

----结束

使用第三方 CA 激活子 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CA”进入私有CA管理界面。

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

1. 激活为子CA需要选择“CA类型”为“子CA”

   子CA：用于在现有的CA层次结构中增加新的层次。

2. 激活为子CA需要先选择上级CA，如图 选择上级CA。

图 2-3 选择上级 CA

- 选择“第三方CA”，并配置以下参数

参数名称		参数说明
基本信息	密钥算法	选择密钥算法： ■ RSA2048 ■ RSA3072 ■ RSA4096 ■ EC256 ■ EC384

参数名称		参数说明
	密钥用法（可选）	选择密钥用法： ■ digitalSignature ■ nonRepudiation ■ keyEncipherment ■ dataEncipherment ■ keyAgreement ■ keyCertSign ■ cRLSign ■ encipherOnly ■ decipherOnly
	签名哈希算法	选择签名哈希算法： ■ SHA256 ■ SHA384 ■ SHA512 ■ SHA256_PSS ■ SHA384_PSS ■ SHA512_PSS
	有效期	选择私有CA有效期，可选择的最长有效期为20年。
	路径长度	该子CA的路径长度，即当前CA可以签发下级子CA的层次数量，用于控制证书链深度。 **说明** 证书链是指根CA、子CA、私有证书三者之间通过层层信任关系链接而成的序列。
证书唯一标识名称（DN）	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。 CN
	省/市	申请单位所在省名或市名，可以是中文或英文。 ShenZhen

参数名称		参数说明
	城市	申请单位所在城市名，可以是中文或英文。 GuangZhou
	公司名称（O）	申请单位法定名称，可以是中文或英文。 -
	部门名称（OU）	申请单位的所在部门，可以是中文或英文。 Cloud Dept.
证书吊销配置（可选）	OBS授权	确认是否授权PCA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4 确认填写的信息无误后，单击“保存，下一步”。

步骤5 在信息确认页面对您已填写的参数进行二次确认，并填写相关信息，如图 第三方CA。

图 2-4 第三方 CA

1. 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。

2. 外部CA签发证书。
   使用您的私有CA签发待激活子CA证书。
3. 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 2-3 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6 确认信息无误后，单击“确认并激活”。完成子CA激活。

----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**。

2.3 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

已购买私有CA，详细操作请参见**购买私有CA**。

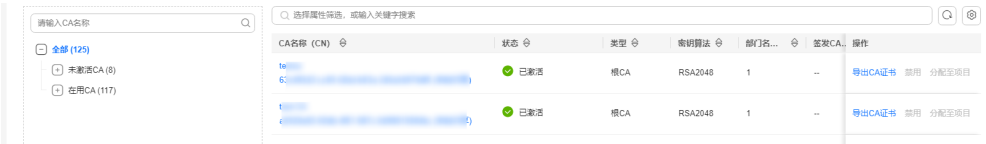
操作步骤

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CA”进入私有CA管理界面。

步骤3 在私有CA列表中，查看私有CA信息，如**私有CA列表**所示，证书参数说明如**表2-4**所示。

图 2-5 私有 CA 列表



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。

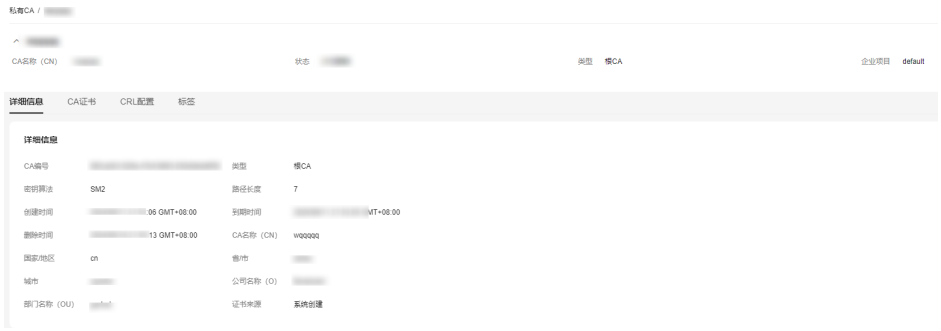
表 2-4 CA 参数说明

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： ● 根CA：私有CA属于根CA，可用于签发其他子CA。 ● 子CA：私有CA属于子CA。
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： ● 待激活：私有CA处于待激活状态。 ● 已激活：私有CA处于已激活状态。 ● 已禁用：私有CA处于已禁用状态。 ● 计划删除：私有CA处于计划删除状态。 ● 已过期：私有CA处于已过期状态。
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



----结束

2.4 配置证书吊销列表

如果需要PCA为私有CA吊销的证书发布证书吊销列表（Certificate Revocation List，CRL），可以启用证书吊销列表。

本章节为您详细介绍启用或停用证书吊销列表的操作流程。

前提条件

待配置CRL的私有CA需处于“已激活”或“已禁用”状态

启用证书吊销列表

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CA”进入私有CA管理界面。

步骤3 单击私有CA名称，系统从右面弹出私有CA详情页面。

步骤4 在私有CA详情页面，选择“CRL配置”页签，配置证书吊销信息，如**图 CRL配置**所示，参数说明如**表 证书吊销参数说明**所示。

图 2-7 CRL 配置

表 2-5 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PCA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“启用”，启用证书吊销列表，系统提示“已启用”，表示启用CRL成功。

----结束

停用证书吊销列表

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CA”进入私有CA管理界面。

步骤3 单击私有CA名称，系统从右面弹出私有CA详情页面。

步骤4 在私有CA详情页面，选择“CRL配置”页签，单击“停用”，系统提示“已停用”，表示停用CRL成功。

----结束

2.5 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。

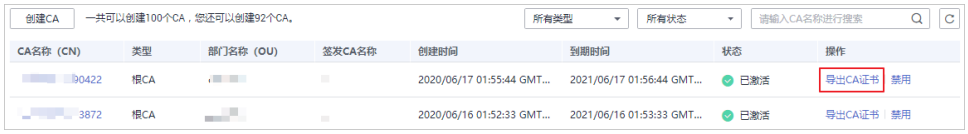
操作步骤

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CA”进入私有CA管理界面。

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”。

图 2-8 导出 CA 证书



步骤4 在弹出的提示框中，单击“确定”。

执行操作后，私有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

2.6 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**启用私有CA**。

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。

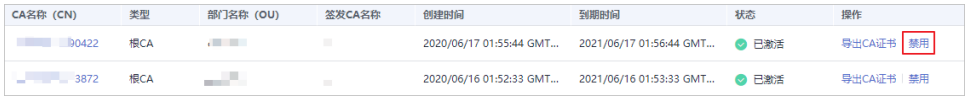
操作步骤

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CA”进入私有CA管理界面。

步骤3 在需要禁用的私有CA所在行的“操作”列，单击“禁用”。

图 2-9 禁用私有 CA



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 2-10 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

2.7 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**。

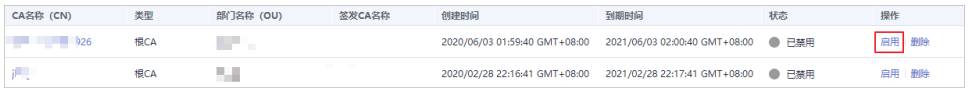
操作步骤

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CA”进入私有CA管理界面。

步骤3 在需要启用的私有CA所在行的“操作”列，单击“启用”。

图 2-11 启用私有 CA



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

2.8 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。

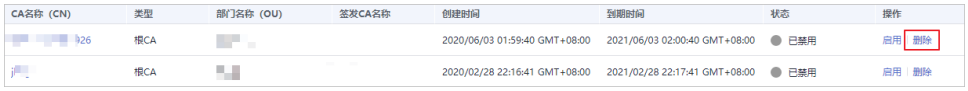
操作步骤

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CA”进入私有CA管理界面。

步骤3 在需要删除的私有CA所在行的“操作”列，单击“删除”。

图 2-12 删除私有 CA



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 2-13 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 2-14 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

2.9 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。

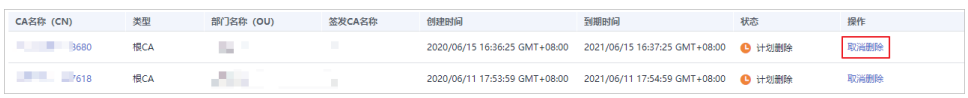
操作步骤

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CA”进入私有CA管理界面。

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 2-15 取消删除私有 CA



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

3 管理私有证书

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

已购买并激活私有CA，详细操作请参见**购买私有CA**、**激活私有CA**。

操作步骤

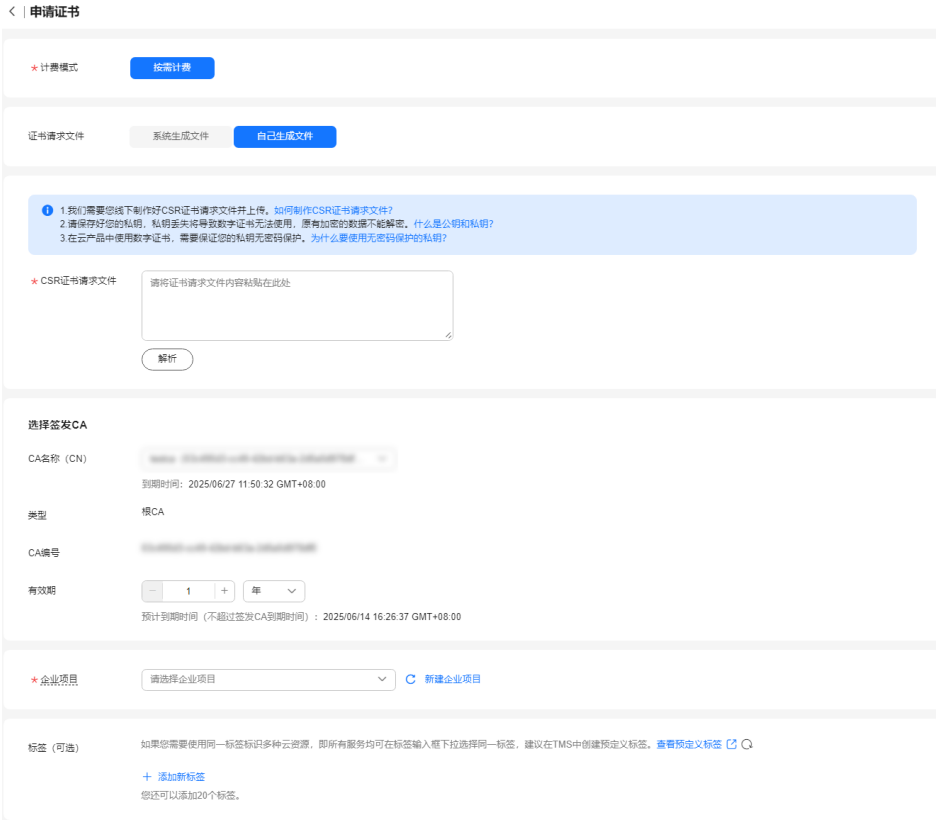
步骤1 登录**管理控制台**。

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 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 3-1 申请证书-系统生成文件

图 3-2 申请证书-自己生成文件



1. 选择证书请求文件生成方式。

表 3-1 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”。
说明 – 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。 – 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。 – 手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥文件。私钥和数字证书一一对应，一旦丢失了私钥您的数字证书也将不可使用。华为云系统不负责保管您的私钥，如果您的私钥丢失，您需要重新购买并替换您的数字证书。 – 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。	

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^，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 3-2 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”、“SM2”。	RSA2048
签名哈希算法	当“密钥算法”选择“SM2”时，，待申请私有证书签名哈希算法默认为“SM3”，无需进行选择。 当密钥算法选择为非SM2时，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）： – digitalSignature（数字签名） – nonRepudiation（防抵赖） – keyEncipherment（密钥加密） – dataEncipherment（数据加密） – keyAgreement（密钥协议） – keyCertSign（证书签发） – cRLSign（黑名单签名） – encipherOnly（仅加密） – decipherOnly（仅解密）	digitalSignature
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）： – 服务器身份验证 – 客户端身份验证 – 代码签名 – 安全电子邮件 – 时间戳	服务器身份验证
自定义扩展字段	填写待申请证书的自定义信息。	-

参数名称	参数说明	示例
（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： – IP address：填写IP地址 – DNS：填写域名 – Email：填写邮箱 – URI：填写网络地址 最多可配置5条AltName信息。	-

4. 选择签发CA。

表 3-3 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。 **说明** – 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。 – 私有CA有效期最长为30年。

5. 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。

步骤4 （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**。

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 在需要下载的私有证书所在行的“操作”列，单击下载。

图 3-3 下载私有证书

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，私有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服务器上进行使用，非国密证书的安装操作与国际标准SSL证书安装操作相同，您可以参考**表 安装SSL证书操作示例**。

表 3-4 安装 SSL 证书操作示例

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

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3-5所示。

  表 3-5 下载文件说明（一）

证书类型	服务器类型	zip压缩包中包含的文件
国际证书	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。

证书类型	服务器类型	zip压缩包中包含的文件
国密SM2证书	其他	是否导出国密GMT 0009-2012标准规范的SM2数字信封： • 是，zip压缩包中包含的文件为： chain.pem ： 证书链文件 encSm2EnvelopedKey.key ： 国密SM2数字信封 encCert.pem：加密证书文件 signCert.key：签名证书私钥文件 signCert.pem：签名证书文件 • 否，zip压缩包中包含的文件为： chain.pem ： 证书链文件 encCert.key ： 加密证书私钥 encCert.pem：加密证书文件 signCert.key：签名证书私钥文件 signCert.pem：签名证书文件

- 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3-6**所示。

  表 3-6 下载文件说明（二）

证书类型	服务器类型	zip压缩包中包含的文件
国际证书	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。

证书类型	服务器类型	zip压缩包中包含的文件
国密SM2证书	其他	是否导出国密GMT 0009-2012标准规范的SM2数字信封： • 是，zip压缩包中包含的文件为： chain.pem ： 证书链文件 encSm2EnvelopedKey.key ： 国密SM2数字信封 encCert.pem：加密证书文件 signCert.pem：签名证书文件 • 否，zip压缩包中包含的文件为： chain.pem ： 证书链文件 encCert.key ： 加密证书私钥文件 encCert.pem：加密证书文件 signCert.pem：签名证书文件

3.3 安装私有证书

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**

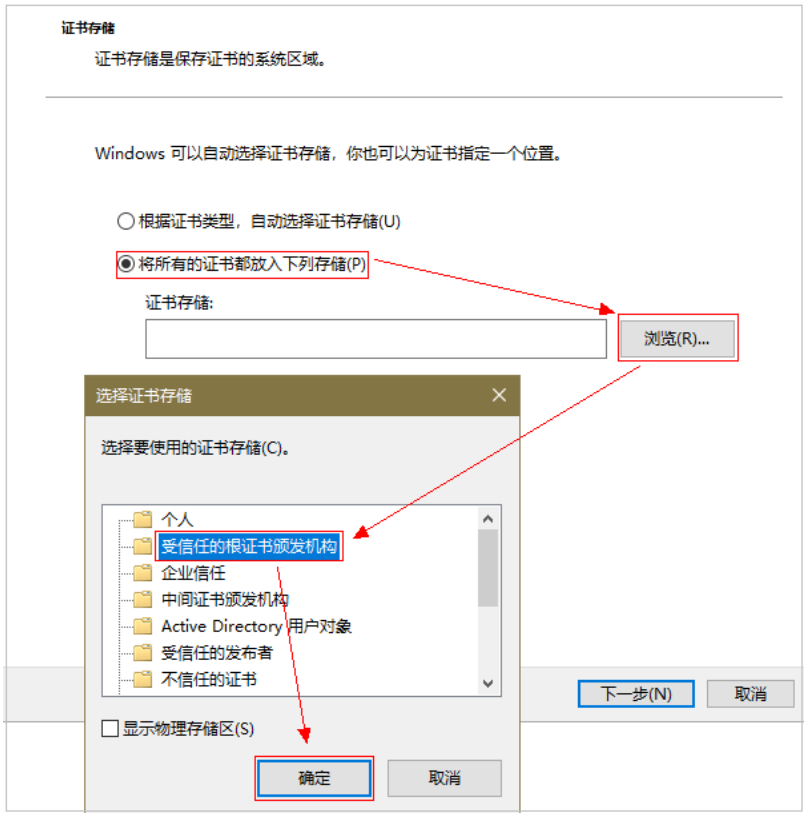
a. 将根CA证书文件后缀由“.pem”改为“.crt”.，双击证书文件，根CA证书信息显示该根证书不受信任。

图 3-4 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“将所有证书都存放入下列存储（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 3-5 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 3-6 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：

  a. 将根CA证书文件复制到“/home/”路径下。

  b. 当服务器未安装“ca-certificates”时，使用如下命令安装“ca-certificates”。

  yum install ca-certificates

  c. 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/

  d. 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

  e. 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 3-7 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**
  a. 打开mac的启动台，选择“钥匙串”。
  b. 输入密码登录到“钥匙串”。
  c. 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。
  d. 选中根CA证书文件，单击鼠标右键选择“显示简介”。
  e. 选择“信任>使用此证书时”，选择“始终信任”，单击“关闭”。
  f. 输入密码使信任根CA证书配置生效。
  g. 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。

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 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4 选择证书下载格式为“IIS”，单击“下载证书”。

步骤5 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”。

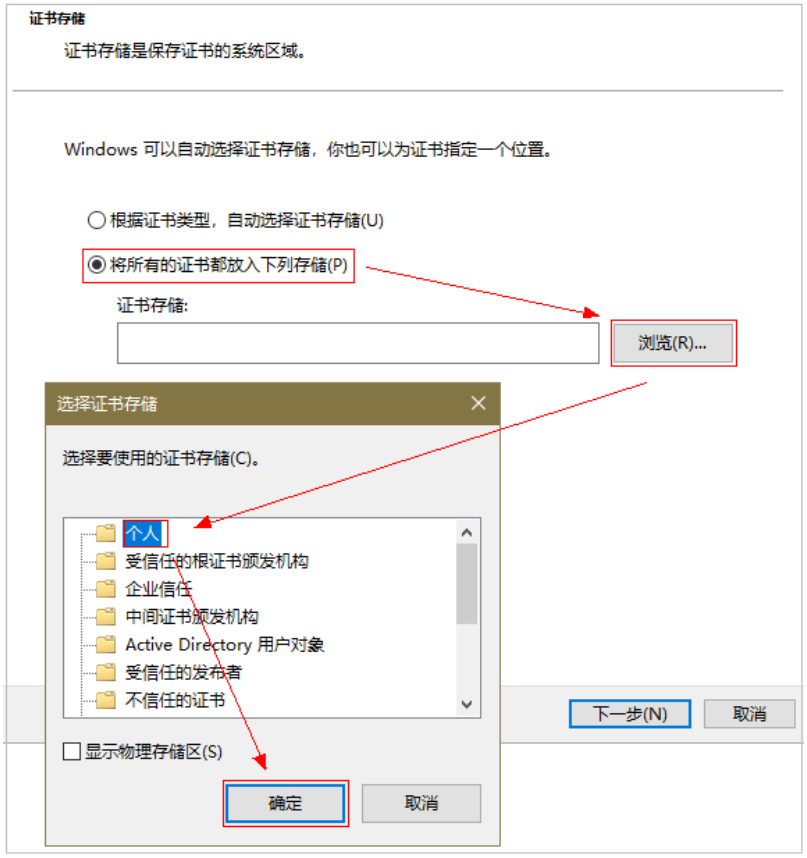
步骤6 双击证书文件“server.pfx”，根据使用场景选择证书存储位置，单击“下一步”。

步骤7 确认要导入的证书文件名，单击“下一步”。

步骤8 输入从私钥密码文件“keystorePass.txt”中获取的密码，单击“下一步”。

步骤9 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 3-8 存储私有证书



步骤10 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

3.3.3 在服务器安装私有证书

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。

如果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。
- 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3-7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 3-7 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="lx6&APWgcHf72DMu"，则修改为keystorePass="lx6&APWgcHf72DMu"。

参数	参数说明
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。

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？**。
- 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。

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。

如果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。
- 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3-8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 3-8 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”。

参数	参数说明
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？**。
- 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。

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。

如果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。
- 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
   ```

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。

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？**。
- 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。

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。

如果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。
- 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

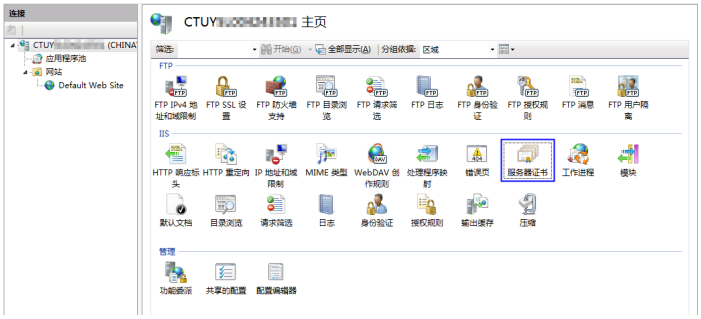
在本地解压已下载的证书文件。

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3-9**所示。

图 3-9 服务器证书



3. 在弹出的窗口中，单击“导入”，如图3-10所示。

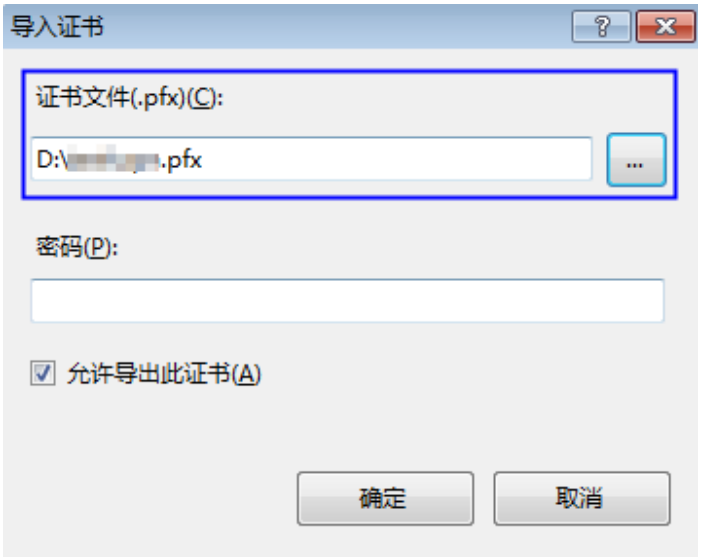
图 3-10 导入

4. 导入“server.pfx”证书文件，单击“确定”。

说明

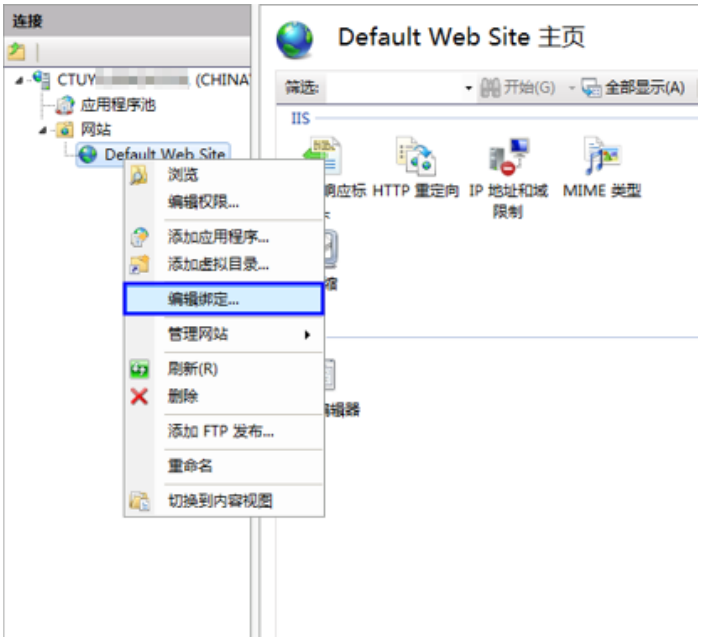
“密码”配置框内需要输入“keystorePass.txt”文件内的密码。

图 3-11 导入 pfx 证书文件



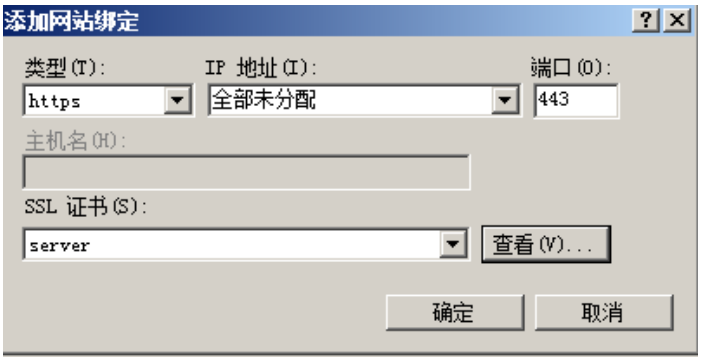
5. 鼠标右键单击目标站点（这里以默认站点为例），选择“编辑绑定”，如图3-12所示。

图 3-12 编辑绑定



6. 在弹出的窗口中，单击“添加”，并填写以下信息。

图 3-13 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。

- 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?**。
- 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。

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。

如果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**

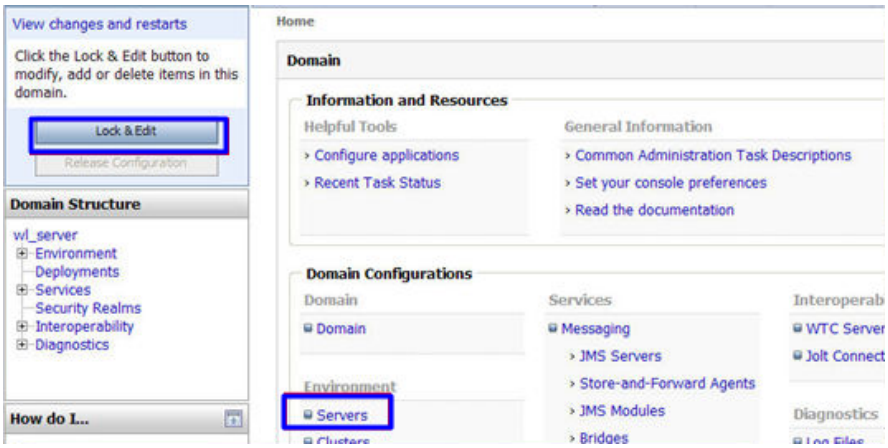
步骤一：获取文件

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

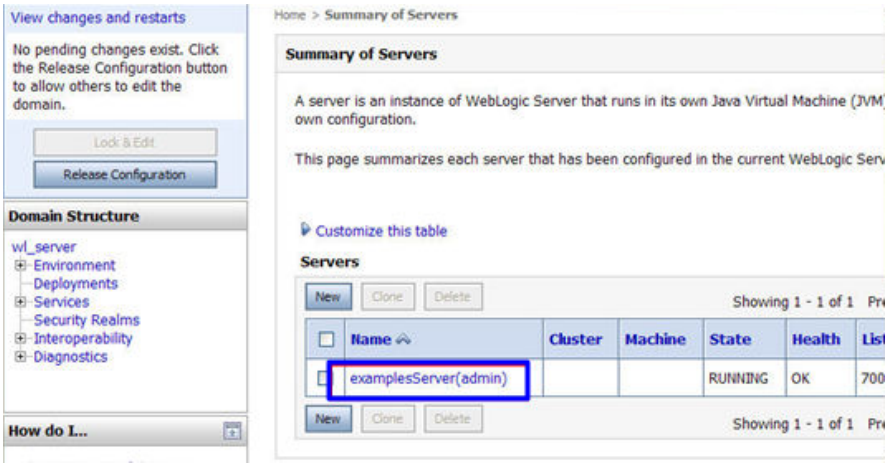
1. 登录Weblogic服务器管理控制台。
2. 单击页面左上方“Lock & Edit”，解锁配置。
3. 在“Domain Configurations”中，单击“Servers”。

图 3-14 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 3-15 目标服务器

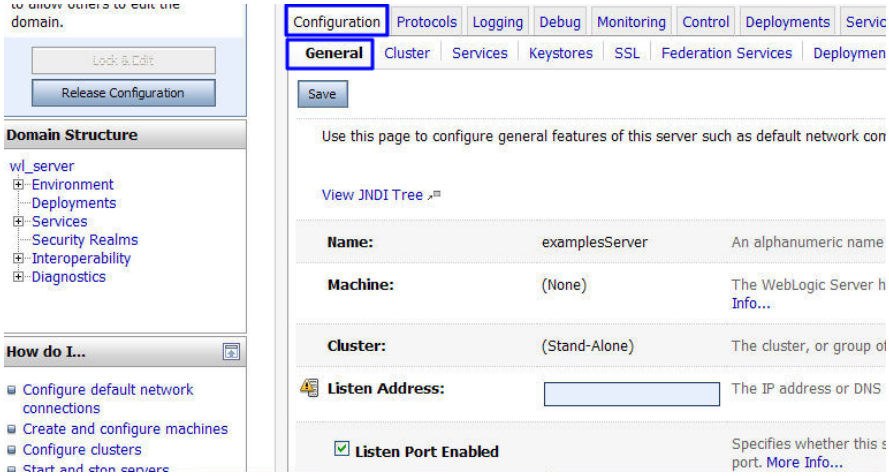


5. 修改HTTPS端口。

   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”。

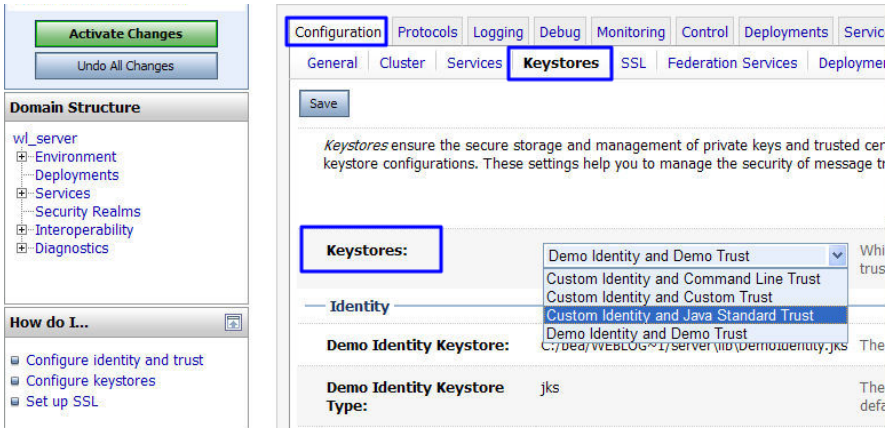
图 3-16 端口



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 3-17 认证方式

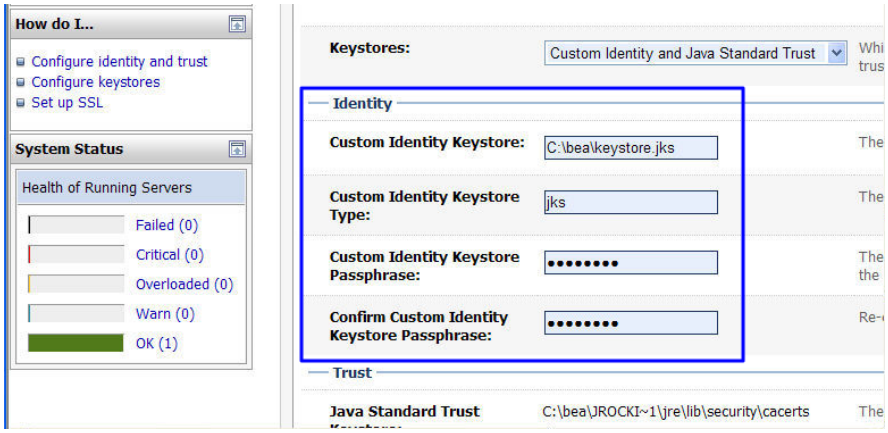


   - 服务器身份认证请选择“Custom identity and Java Standard Trust”。
   - 双向认证请选择“Custom Identity and Custom Trust”。

   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 3-18 密钥

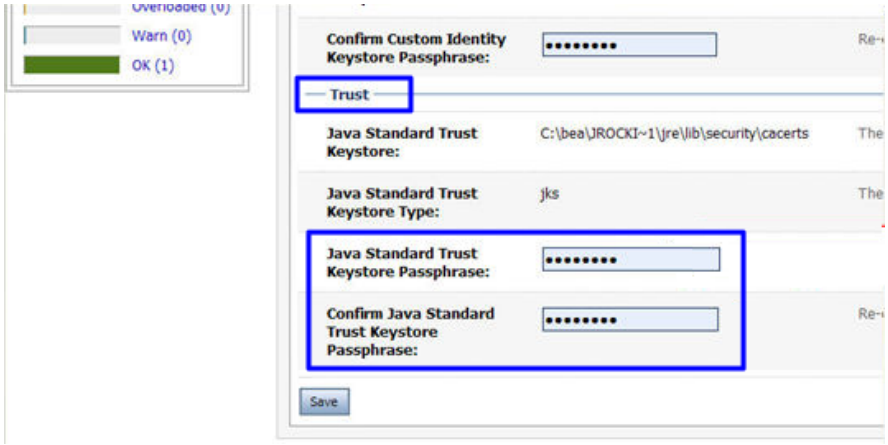


- **Custom Identity Keystore**：请填写jks文件保存路径。示例：C:\bea\server.jks
- **Custom Identity Keystore Type**：文件格式请填写“jks”。
- **Custom Identity Keystore Passphrase**：请填在证书密码，即“keystorePass.txt”中的密码。
- **Confirm Custom Identity Keystore Passphrase**：请再次填写证书密码。

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 3-19 信任库文件

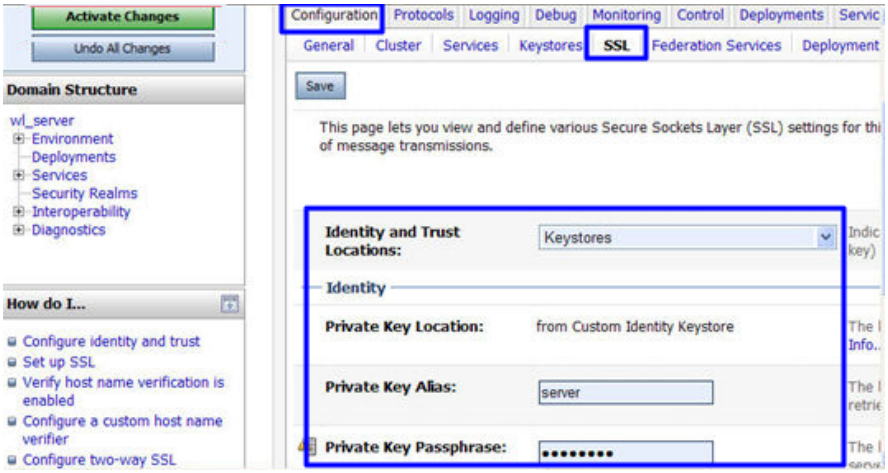


- **Java Standard Trust Keystore Passphrase**：输入默认密码changeit。
- **Confirm Java Standard Trust Keystore Passphrase**：再次输入默认密码。

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：

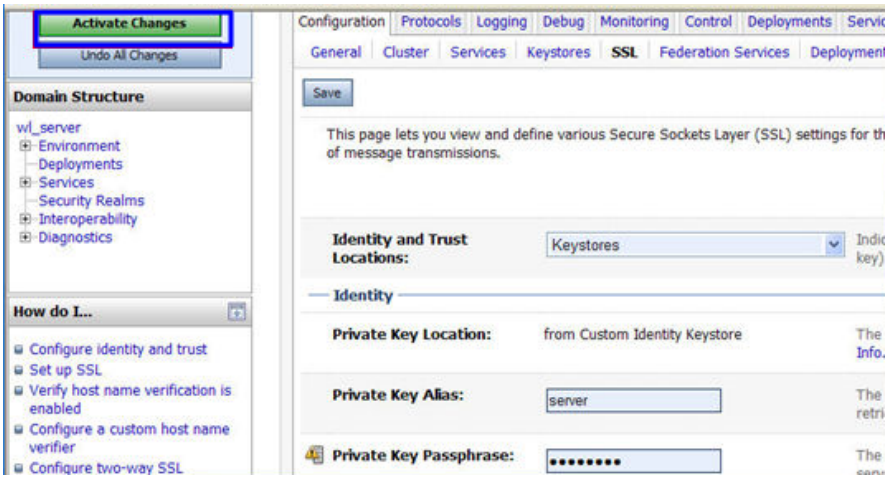
图 3-20 私钥



- **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。

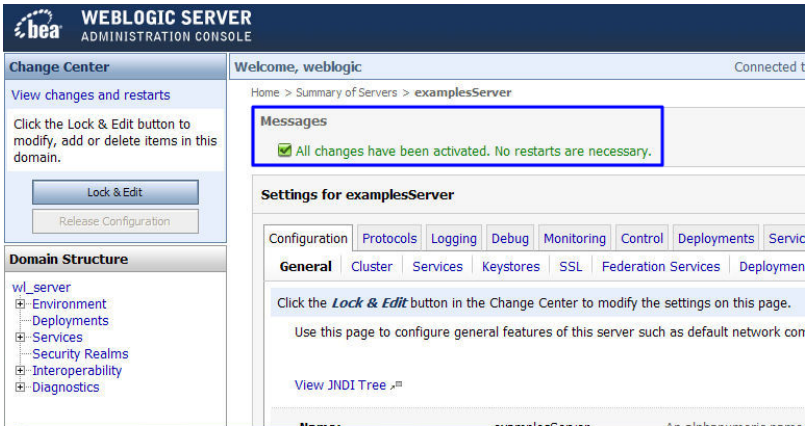
8. 设置完成后，单击“Active Changes”，保存所有修改。

图 3-21 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3-22所示，则无需重启。

图 3-22 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。

- 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？**。
- 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。

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。

如果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。

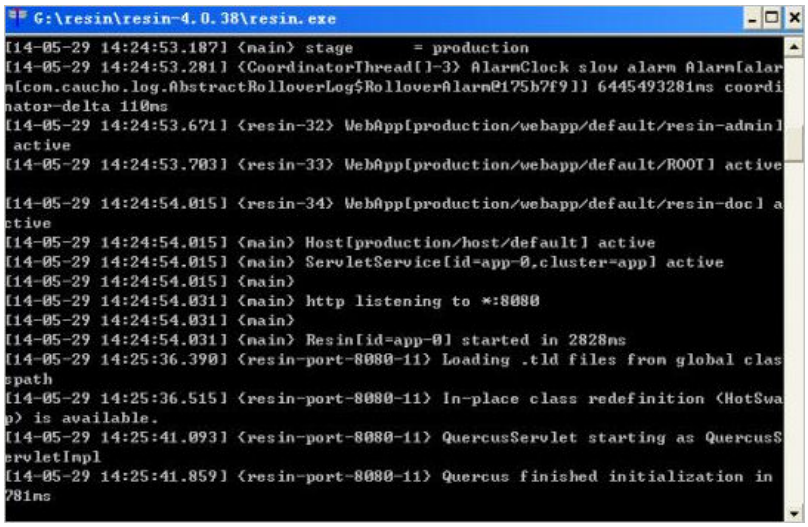
      本步骤以下载**Windows**版本的**Resin-4.0.38**版本为例进行说明。

   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3-23**所示的命令提示符窗口。

图 3-23 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3-24所示时，则表示安装成功。

图 3-24 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3-9**。

```
# 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 3-9 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="lx6**&**APWgcHf72DMu"，则修改为keystorePass="lx6**&**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。

- 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？**。
- 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。

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 在需要吊销的私有证书所在行的“操作”列，单击“吊销”。

图 3-25 吊销私有证书

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 3-26 吊销私有证书提示信息

表 3-10 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
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

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 查看私有证书信息，如**图3-27**所示，证书参数说明如**表3-11**所示。

图 3-27 私有证书列表

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 3-11 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。
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： • 已签发 私有证书处于已签发状态。 • 已过期 私有证书处于已过期状态。 • 已吊销 私有证书处于已吊销状态。
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3-28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 3-28 私有证书详细信息

----结束

3.6 删除私有证书

删除证书是指将证书资源从华为云系统中删除。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 在需要删除的私有证书所在行的“操作”列，单击“删除”。

图 3-29 删除私有证书

步骤4 在弹出的对话框中输入“DELETE”，以确认删除证书信息。

图 3-30 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

4 共享

4.1 共享概述

共享简介

云证书管理服务私有证书管理提供共享功能，用户可以将账号A的私有CA同时共享给同一组织单元内的所有成员账号，这些账号可以使用这些共享CA来签发证书，比如账号B、账号C等。

- 账号A是私有CA所有者，以下简称为所有者。
- 账号B、账号C均属于私有CA接受者，以下简称为接受者。

私有 CA 所有者和接受者权限说明

所有者可以对私有CA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 私有CA接受者支持的操作列表**所示。

表 4-1 私有 CA 接受者支持的操作列表

角色	支持的操作	操作说明
接受者	pca:ca:export	通过控制台或API进行访问
	pca:ca:get	通过控制台或API进行访问
	pca:ca:listTags	通过控制台或API进行访问
	pca:ca:issueCert	通过控制台或API进行访问
	pca:ca:issueCertByCsr	通过控制台或API进行访问
	pca:ca:revokeCert	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PCA服务支持共享的资源类型和区域如**表 PCA服务支持共享的资源类型和区域**所示。

表 4-2 PCA 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
PCA	ca：私有CA	ALL

计费说明

关于PCA的计费可参见**计费项**。

共享私有CA的计费，由私有CA拥有者支付CA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。

4.2 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“pca:ca”，选择对应区域，勾选需进行共享的私有CA。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 4-3 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

4.3 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“pca:ca”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

4.4 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私有CA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

4.5 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

4.6 退出共享

若用户不再需要访问共享的私有CA资源，可以随时退出共享。退出共享后，用户将失去对私有CA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

5 标签管理

5.1 标签概述

操作场景

标签可以对私有CA和私有证书进行标识，当您拥有多个CA或多张私有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CA或私有证书时添加标签，也可以在购买完成后，在CA资源或私有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。
- 每个私有CA或私有证书最多可以添加20个标签。
- 对于每个资源，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私有CA或私有证书添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

表 5-1 标签参数说明

参数	规则	样例
标签键	• 必填。 • 对于同一个私有CA或私有证书，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

5.2 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。具体操作请参见**启用和禁用标签策略**。

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 5-1 进入标签策略

步骤4 单击“创建”，进入标签策略创建页面。

图 5-2 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 5-3 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

5.3 创建标签

本章节指导用户为已购买私有CA和私有证书添加标签。

为私有 CA 创建标签

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。

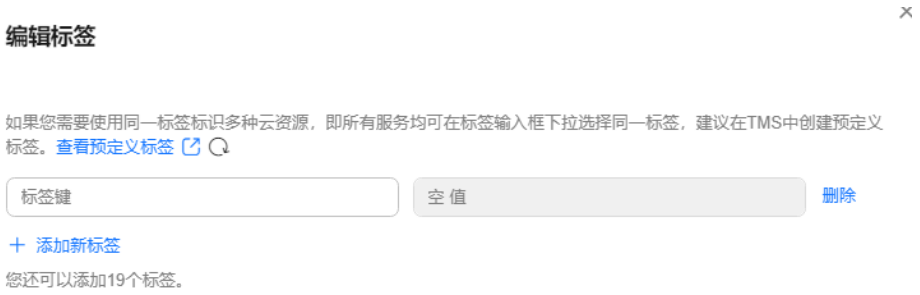
步骤3 在左侧导航栏选择“私有证书管理 > 私有CA”，进入私有CA列表页面。

步骤4 单击目标私有CA名称，进入私有CA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”，弹出编辑标签对话框，单击“添加新标签”在输入框中输入“标签键”和“标签值”。

图 5-4 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

为私有证书创建标签

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。

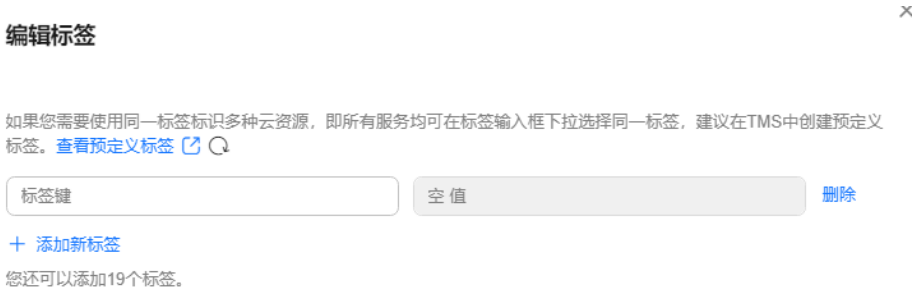
步骤3 在左侧导航栏选择“私有证书管理 > 私有证书”，进入私有证书列表页面。

步骤4 单击目标私有证书名称，进入私有证书详细信息页面。

步骤5 单击“标签”进入标签管理页面。

步骤6 单击“编辑标签”，弹出编辑标签对话框，单击“添加新标签”在输入框中输入“标签键”和“标签值”。

图 5-5 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

5.4 通过标签搜索私有 CA 或私有证书

该任务指导用户通过标签搜索当前项目下满足标签搜索条件的私有CA或私有证书。

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，则搜索结果的每个私有CA或私有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。

通过标签搜索私有 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“私有证书管理 > 私有CA”，进入私有CA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私有CA列表，如**图 搜索结果**所示。

图 5-6 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，则搜索结果的每个私有CA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

通过标签搜索私有证书

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“私有证书管理 > 私有证书”，进入私有证书列表页面。

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私有证书列表，如图 搜索结果所示。

图 5-7 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，则搜索结果的每个私有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

5.5 修改标签值

本章节指导用户对已创建私有CA或私有证书标签进行修改。

修改私有 CA 标签值

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“私有证书管理 > 私有CA”，进入私有CA列表页面。

步骤4 单击目标私有CA名称，进入私有CA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”，弹出编辑标签对话框，在输入框中修改标签值后单击“确定”。完成标签值修改。

----结束

修改私有证书标签值

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“私有证书管理 > 私有证书”，进入私有证书列表页面。

步骤4 单击目标私有证书名称，进入私有证书详细信息页面。

步骤5 单击“标签”进入标签管理页面。

步骤6 单击“编辑标签”，弹出编辑标签对话框，在输入框中修改标签值后单击“确定”。完成标签值修改。

----结束

5.6 删除标签

本章节指导用户对已创建私有CA标签或私有证书标签进行删除。

删除私有 CA 标签

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“私有证书管理 > 私有CA”，进入私有CA列表页面。

步骤4 单击目标私有CA名称，进入私有CA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

删除私有证书标签

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“私有证书管理 > 私有证书”，进入私有证书列表页面。

步骤4 单击目标私有证书名称，进入私有证书详细信息页面。

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

6 PCA 权限管理

6.1 创建用户并授权使用 PCA

如果您需要对您所拥有的PCA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PCA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PCA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PCA服务的其它功能。

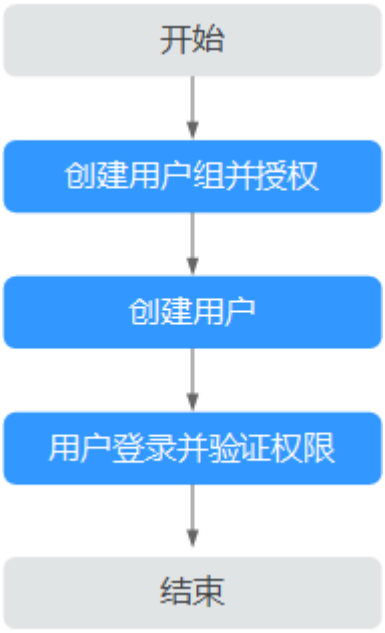
本章节为您介绍对用户授权的方法，操作流程如**图 给用户授权PCA权限流程**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的PCA权限，并结合实际需求进行选择，PCA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 6-1 给用户授权 PCA 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. **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“PCA FullAccess”已生效。

6.2 PCA 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PCA自定义策略样例。

PCA 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"
          }
      ]
  }
  ```


7 PCA 关键操作审计管理

7.1 PCA 支持云审计的操作列表

云审计服务记录私有证书管理相关的操作事件，如表7-1所示。

表 7-1 云审计服务支持的 PCA 操作列表

操作名称	资源类型	事件名称
创建CA	CA	createCertificateAuthority
激活CA	CA	generateCertificateAuthority
导出CA	CA	exportCertificateAuthority
恢复CA	CA	restoreCertificateAuthority
启用CA	CA	enableCertificateAuthority
禁用CA	CA	disableCertificateAuthority
删除CA	CA	deleteCertificateAuthority
申请证书	endEntityCert	createCertificate
删除证书	endEntityCert	deleteCertificate
吊销证书	endEntityCert	revokeCertificate

7.2 查看 PCA 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 PCA 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“PCA”。
  - “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7-1所示。

图 7-1 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

