云证书管理服务

用户指南（私有证书管理）

文档版本 12

发布日期 2024-01-16

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

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

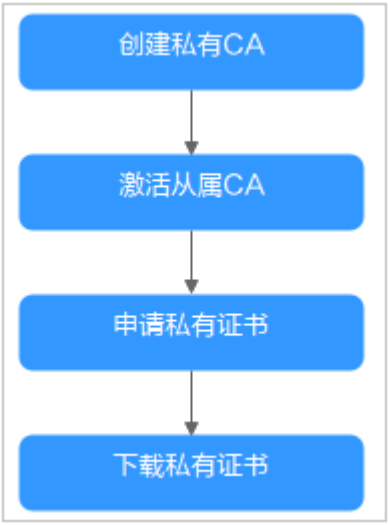


表 1-1 私有证书申请流程说明

步骤	申请操作	说明
1	**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。

步骤	申请操作	说明
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 管理私有 CA

2.1 创建私有 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“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）”、“企业项目”和“证书吊销配置”信息。

1. 配置基本信息，如**图 基本信息**所示，参数说明如**表2-1**所示。

表 2-1 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。 **说明** 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 – SM2	RSA2048
签名哈希算法	“CA类型”选择“根CA”时，显示该参数。 当“密钥算法”选择“SM2”时，签名哈希算法默认为“SM3”无需进行选择。 当密钥算法选择非SM2时，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

2. 配置证书唯一标识名称（Distinguished Name，DN）信息，如图2-1所示，参数说明如表2-2所示。

图 2-1 DN 信息

表 2-2 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。	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.

3. （可选）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。

4. （可选）配置证书吊销信息。

   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），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2-2所示，参数说明如表2-3所示。

图 2-2 证书吊销

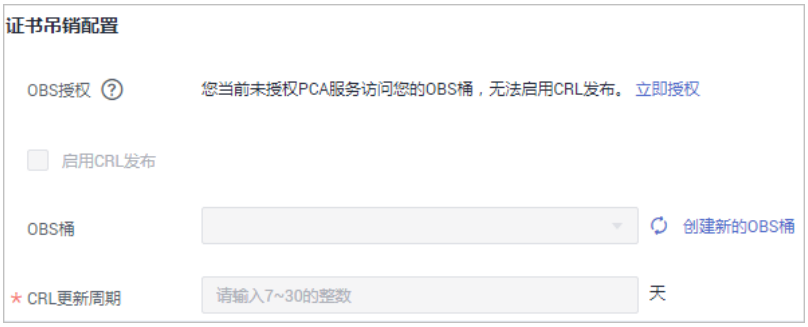


表 2-3 证书吊销参数说明

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“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 激活私有 CA

如果您创建的私有CA为**从属CA**，则需要在创建后进行激活。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：使用华为云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（非华为云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”，系统从右面弹出激活CA详细页面，如**图2-3**所示，请填写激活CA相关信息。

图 2-3 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 2-4 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。
路径长度	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。 **说明** 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。

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”，系统从右面弹出激活CA详细页面，请填写激活CA相关信息。

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 2-5 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**。

2.3 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**。

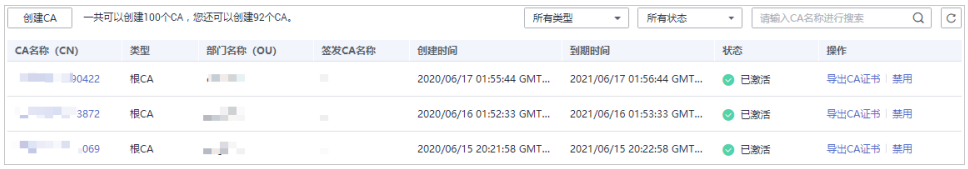
操作步骤

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**图2-4**所示，证书参数说明如**表2-6**所示。

图 2-4 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 2-6 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，可用于签发其他从属CA。 • 从属CA：私有CA属于从属CA。
部门名称（OU）	私有CA所属的部门名称。

参数名称	说明
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2-5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 2-5 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 2-6 CRL 配置

表 2-7 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。

参数名称	参数说明
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

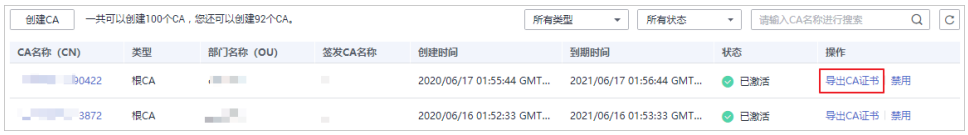
待导出私有CA证书的私有CA需处于“已激活”状态。

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”。



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

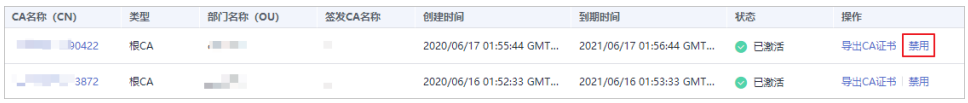
待禁用的私有CA需处于“已激活”或“已过期”状态。

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”。



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

2.7 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转态。

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**。

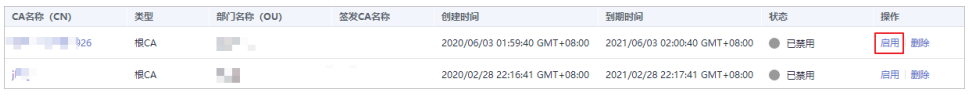
操作步骤

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 2-8 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 2-9 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 2-10 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

2.9 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。

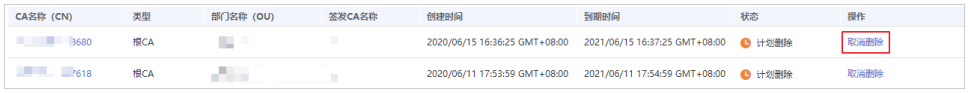
操作步骤

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 2-12 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”。

参数名称	参数说明
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

参数名称	参数说明	示例
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： – 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。

参数名称	参数说明
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. （可选）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 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。
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。

证书类型	服务器类型	zip压缩包中包含的文件
	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。
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 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 3-4 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 3-5 吊销私有证书提示信息

表 3-7 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

吊销理由	对应RFC 5280标准中的吊销理由码	含义
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

3.4 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3-6**所示，证书参数说明如**表3-8**所示。

图 3-6 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 3-8 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3-7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 3-7 私有证书详细信息

----结束

3.5 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 3-8 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 3-9 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。

- 帐号A是私有CA所有者，以下简称为所有者。
- 帐号B、帐号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。即所有共享资源发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帐号使用时，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**。 • 华为云帐号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“华为云帐号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，组织中的帐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 设置标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。云证书管理服务支持为已购买的私有CA和私有证书配置标签，方便管理。

5.1 设置私有 CA 标签

操作步骤

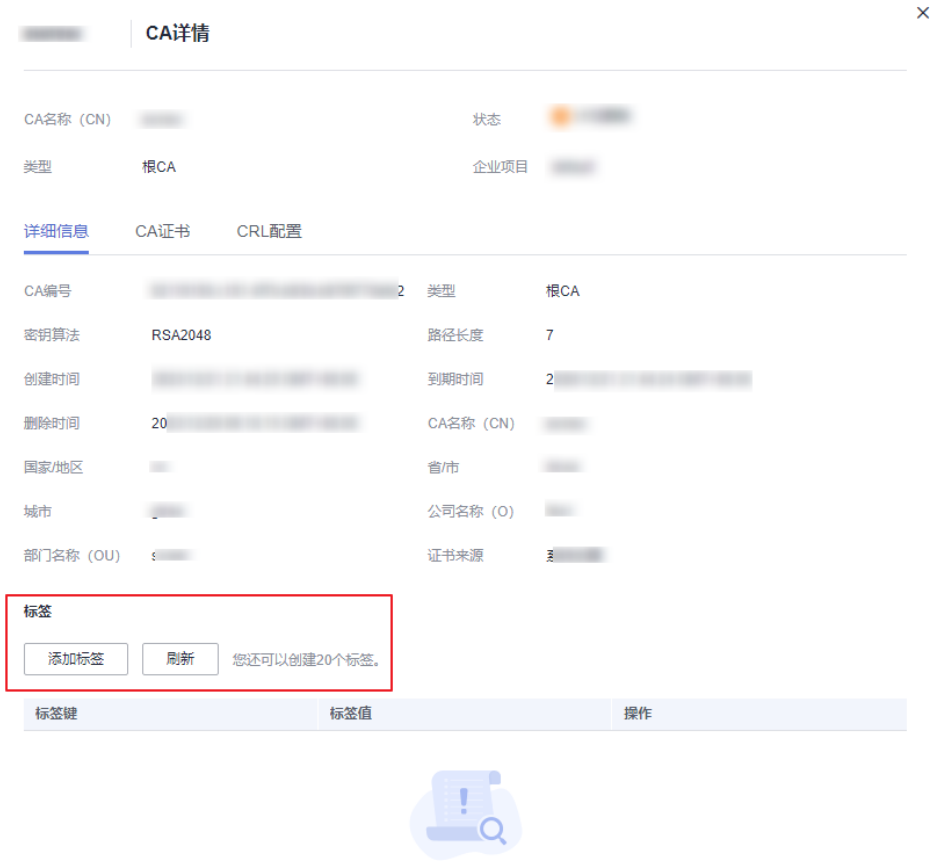
步骤1 登录管理控制台。

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

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

步骤4 在需要设置标签的私有CA所在行，单击私有CA名称，在右侧弹框证书详情页单击“添加标签”。

图 5-1 添加标签



步骤5 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 5-2 设置标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。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。

步骤6 单击“确定”。

----结束

5.2 设置私有证书标签

操作步骤

步骤1 登录管理控制台。

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

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

步骤4 在需要设置标签的私有证书所在行，单击私有证书名称，在右侧弹框证书详情页单击“添加标签”。

图 5-3 添加标签

步骤5 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 5-4 设置标签

步骤6 单击“确定”。

----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。

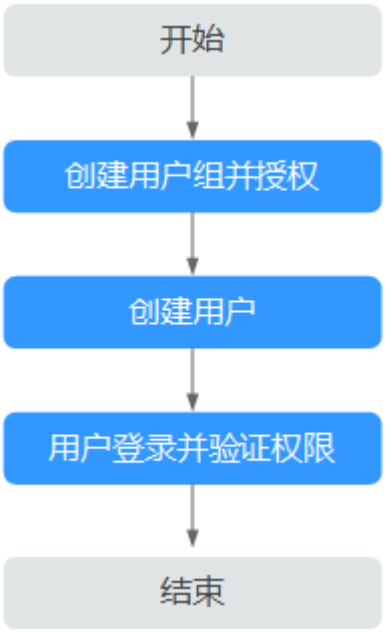
本章节为您介绍对用户授权的方法，操作流程如**图 给用户授权PCA权限流程**所示。

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

A 修订记录

发布日期	修改说明
2024-01-16	第十二次正式发布。 新增**设置标签**章节，增加了对私有证书、私有CA设置标签的描述。
2023-1-11	第十一次正式发布。 ● 刷新**创建私有CA**、**申请私有证书**章节，支持SM2算法。 ● 刷新**下载私有证书**章节，增加国密证书文件下载说明。 ● 新增**配置证书吊销列表**章节。
2022-11-16	第十次正式发布。 新增**PCA自定义策略**。 优化 ● **创建私有CA** ● **申请私有证书**
2022-10-31	第九次正式发布。 ● 优化文档架构。用户指南拆分为SSL证书管理和私有证书管理两本手册。 ● 优化**PCA权限管理**、**PCA关键操作审计管理**章节内容。
2021-11-01	第八次正式发布。 ● 根据界面控制台显示修改刷新资料。 ● 调整文档架构。
2021-08-16	第七次正式发布。 私有证书管理服务商用版本发布，刷新相关章节内容。

发布日期	修改说明
2020-08-31	第六次正式发布。 ● 优化**创建私有CA**，增加根CA最长有效期的说明。 ● 优化**激活私有CA**，增加从属CA最长有效期的说明。
2020-06-19	第五次正式发布。 优化**管理私有CA**、**管理私有证书**章节，根据控制台显示参数调整而刷新资料相关描述。
2020-04-29	第四次正式发布。 优化**管理私有证书**章节，支持配置申请证书的密钥长度、证书用途等参数信息。
2020-03-31	第三次正式发布。 ● 新增章节**下载私有证书**。 ● 删除“导出私有证书”、“导出私钥”章节。
2020-02-28	第二次正式发布。 ● **申请私有证书**章节中，新增支持选择证书请求文件的内容和描述。 ● 私有证书管理服务的服务级别改为全局级别，刷新用户指南相关内容。 ● 根据界面风格改动，刷新资料截图。
2020-01-17	第一次正式发布。