**云密码综合服务系统**

**用户操作手册**

**版本：V1.0**

**南京壹证通信息技术有限公司**

**2022年6月**

文档中的全部内容属南京壹证通信息科技有限公司所有，

未经允许，不可全部或部分发表、复制、使用于任何目的。

**目录**

[1. 引言 3](#_Toc3751)

[1.1系统概述 3](#_Toc31220)

[1.2系统功能 4](#_Toc15652)

[1.3编写目的 4](#_Toc6081)

[1.4系统运行环境 4](#_Toc16655)

[2. 系统功能 4](#_Toc26785)

[2.1登录 4](#_Toc23210)

[2.1.1功能介绍 4](#_Toc4291)

[2.1.2操作步骤 5](#_Toc13965)

[2.2首页 6](#_Toc26333)

[2.2.1功能介绍 6](#_Toc17168)

[2.2.2操作步骤 6](#_Toc12414)

[2.3 系统设置 7](#_Toc17877)

[2.3.1服务管理 7](#_Toc477)

[2.3.2用户管理 14](#_Toc23243)

[2.3.3 RA管理 17](#_Toc25955)

[2.3.4系统证书 21](#_Toc4130)

[2.3.5密码机配置 26](#_Toc20544)

[2.4租户管理 27](#_Toc12040)

[2.4.1租户列表 27](#_Toc21693)

[2.4.2租户证书 31](#_Toc32552)

[2.4.3费用统计 32](#_Toc18489)

[2.5订阅管理 34](#_Toc831)

[2.5.1订阅服务 34](#_Toc494)

[2.6 SVS服务 38](#_Toc24393)

[2.6.1在线测试 38](#_Toc16623)

[2.7 TSS服务 43](#_Toc23819)

[2.7.1在线测试 43](#_Toc31484)

[2.8 加解密服务 45](#_Toc27147)

[2.8.1在线测试 45](#_Toc8996)

[2.9日志管理 52](#_Toc569)

[2.9.1服务调用日志 52](#_Toc11853)

[2.9.2操作日志 56](#_Toc21706)

[3. FAQ常见问题 57](#_Toc3349)

# 引言

## 1.1系统概述

云密码综合服务系统是一种全新的密码能力交付模式，是云计算技术与身份认证、数据加密、数字签名、时间戳等密码技术的深度融合。云密码服务按照云计算技术架构的要求整合密码产品、密码使用策略、密码服务接口和服务流程，将密码系统设计、部署、运维、管理、计费等组合成一种服务，来满足用户的密码应用需求。用户不再需要“购买”密码硬件或密码系统 等密码产品，而是以“租用”密码服务的方式使用云密码基础设施中提供的各种密码功能。

## 1.2系统功能

系统功能包含对系统的配置、SVS服务、TSS服务、加解密服务、租户管理、订阅管理、查看服务调用日志和操作日志，从而满足各种业务的数据加密保护(证书加密)、数据身份可信(数字签名)、数据产生和使用时间可信(时间戳)以及数据产生等各种密码应用。服务以SDK或API方式为用户业务系统提供密码服务，只需把“无身份明文数据”输入给SDK，由SDK连接云密码综合服务系统完成相应的密码服务，输出“有身份加密数据”给业务系统。

## 1.3编写目的

编写目的在于帮助用户更好地了解和使用该软件,提高用户与软件的亲和度。统一规范系统业务操作，明确各系统人员操作流程及所涉及模块，提升应用熟练度和工作效率。

## 1.4系统运行环境

（1）本系统建议在Windows操作环境下运行；

（3）系统推荐浏览器是谷歌浏览器，其他浏览器不推荐使用

# 系统功能

## 2.1登录

### 2.1.1功能介绍

目前云密码综合服务系统支持三个角色的登录操作，包含系统管理员、系统操作员和系统审计员，不同角色对应不同的菜单权限。

### 2.1.2操作步骤

1. 点击“账户密码登录”，可选择账号密码方式来登录，如图所示：



输入正确的用户名（必填）、登录密码（必填）和验证码（必填），可登录云密码综合服务系统；

2、点击“证书登录”，可选择已绑定的证书登录，如图所示：



证书登录时，点击证书登陆按钮，然后点击选择证书，会弹出浏览器证书选择已绑定的证书，并输入正确的PIN码，可登录云密码综合服务系统；

## 2.2首页

系统管理员、系统操作员和系统审计员均拥有首页菜单权限。

### 2.2.1功能介绍

首页展示累计SVS服务调用次数、累计TSS服务调用次数、累计加解密服务调用次数、租户量、服务订阅量，以及通过可视化图表的方式展示核心业务指标和变化趋势，供系统用户分析业务情况。

### 2.2.2操作步骤

点击菜单〖首页〗，进入首页信息页面，如下图所示：



>> 页面分别展示累计SVS服务调用次数、累计TSS服务调用次数、累计加解密服务调用次数、租户量、服务订阅量以及SVS服务、TSS服务、加解密服务调用次数的趋势分析图；

>>“**SVS服务调用次数**”展示截至目前SVS服务调用的总次数；

>>“**TSS服务调用次数**”展示截至目前TSS服务调用的总次数；

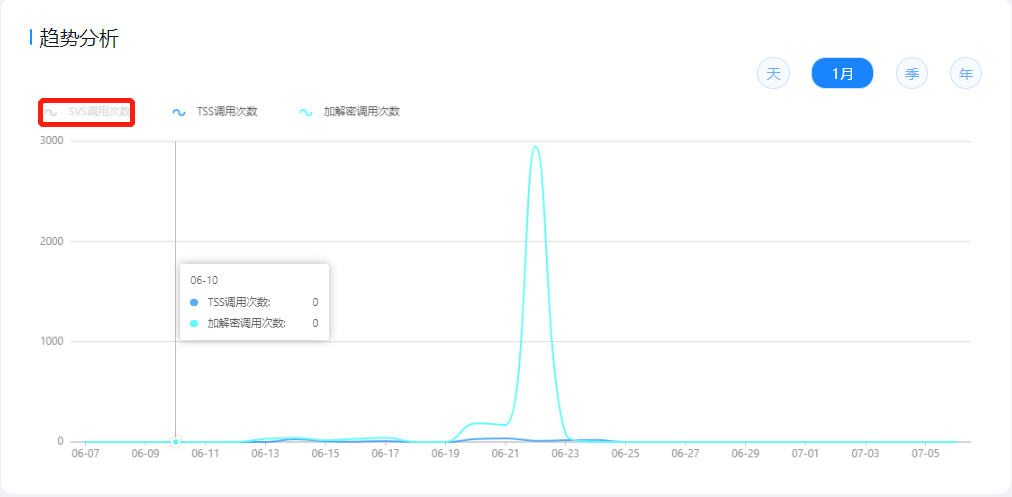
>>“**加解密服务调用次数**”展示截至目前加解密服务调用的总次数；

>>“**租户量**”展示当前租户的总数量；

>>“**服务订阅量**”展示当前租户对服务的订阅总量；

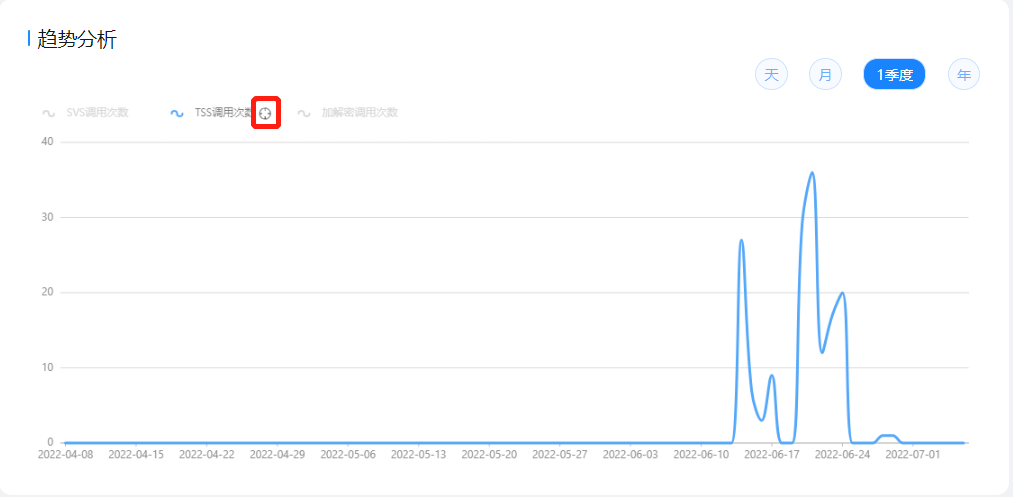
>>“**趋势分析**”展示SVS服务、TSS服务、加解密服务调用次数按周、月、季、年的趋势变化。

1. 点击趋势分析页面的【SVS调用次数/TSS调用次数/加解密调用次数】按钮，可隐藏该服务的趋势图，便于对比分析其他两个服务的趋势变化。如下图所示：



>> 可以结合周、月、季、年来分析服务的趋势变化；

1. 点击趋势分析页面的【SVS调用次数/TSS调用次数/加解密调用次数】后面的按钮，可仅显示该服务的趋势图，便于分析单个服务的趋势变化。如下图所示：



>> 可以结合周、月、季、年来分析服务的趋势变化；

## 2.3 系统设置

系统管理员拥有系统设置菜单权限。

**2.3.1服务管理**

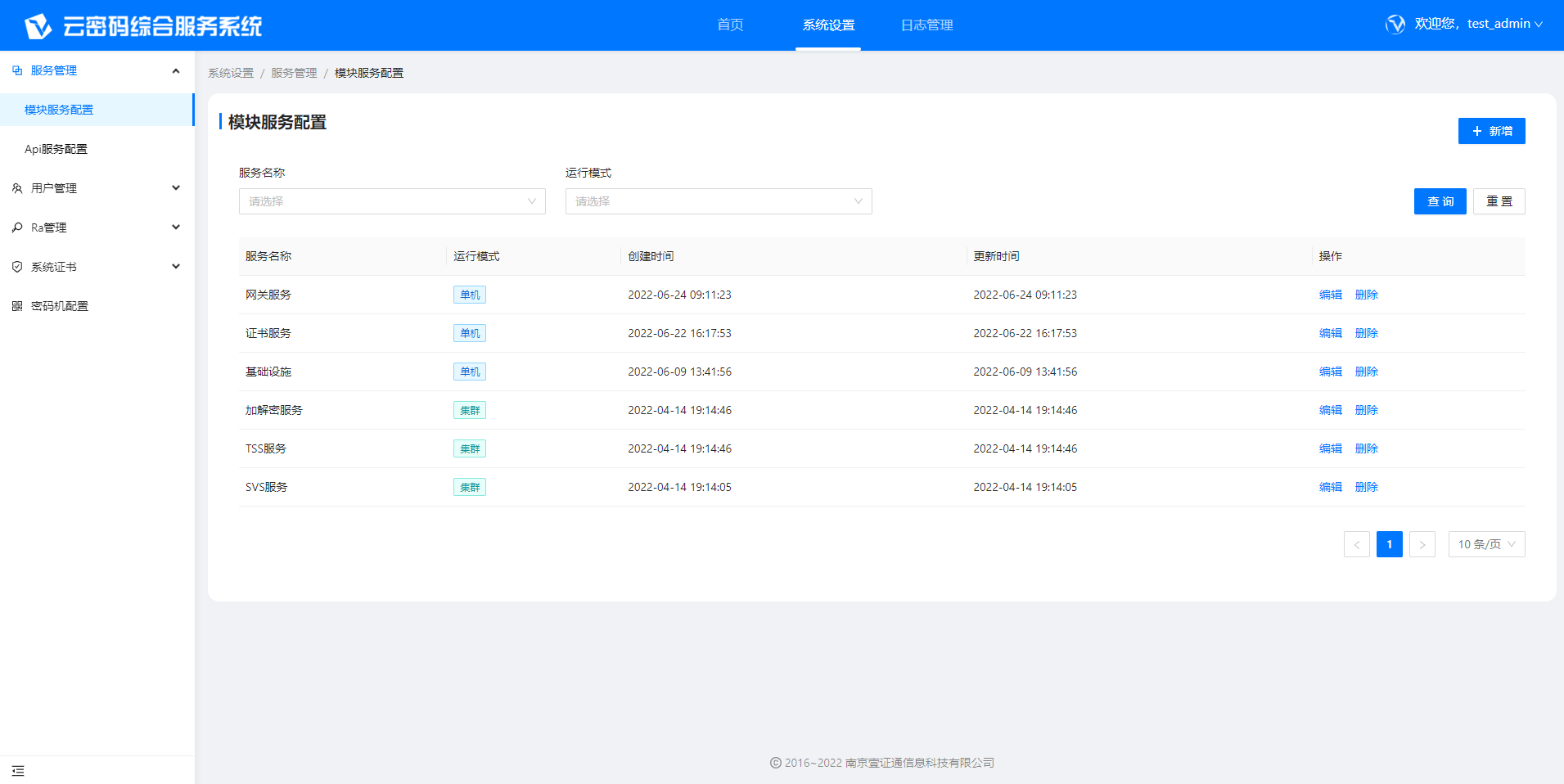
#### **2.3.1.1模块服务配置**

##### 2.3.1.1.1功能介绍

模块服务配置主要对模块服务进行新增和配置，用于证书的发放以及SVS服务、TSS服务和加解密服务的使用。模块服务配置一般在项目部署后，由开发协同系统管理员进行相关配置，一般情况下无需配置。

##### 2.3.1.1.2操作步骤

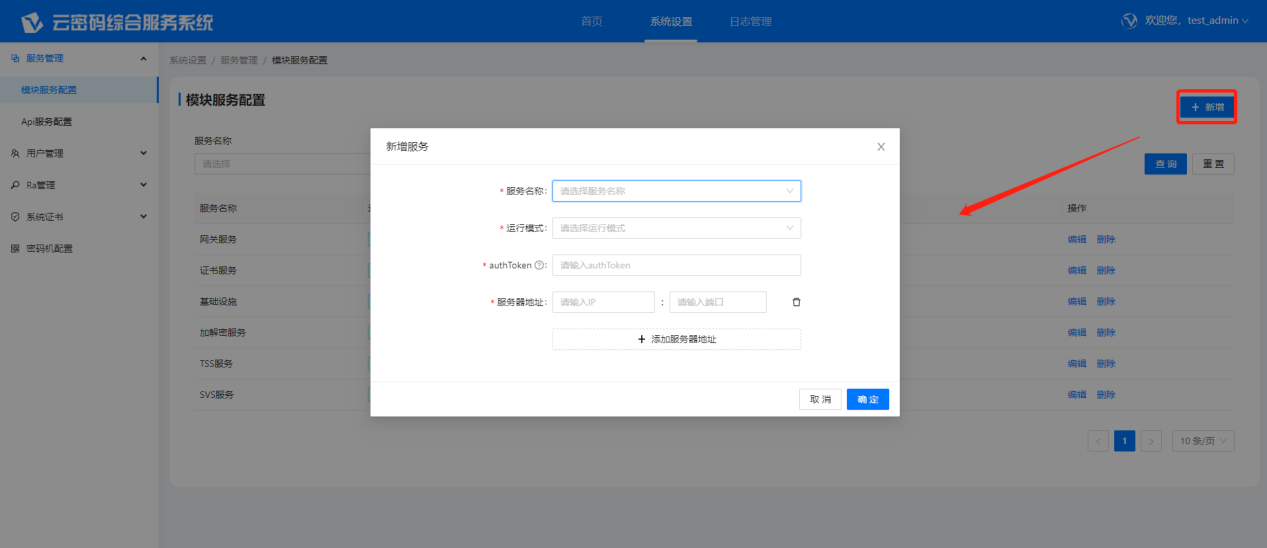
点击菜单〖系统设置〗-〖服务管理〗-〖模块服务配置〗，进入模块服务配置页面，如下图所示：



>> 列表展示所有模块服务配置信息，包含服务名称、运行模式、创建时间、更新时间和操作；

>> 可以根据“服务名称”、“运行模式”查询项来进行查询操作；

1. 点击页面的【新增】按钮，新增模块服务，如下图所示：



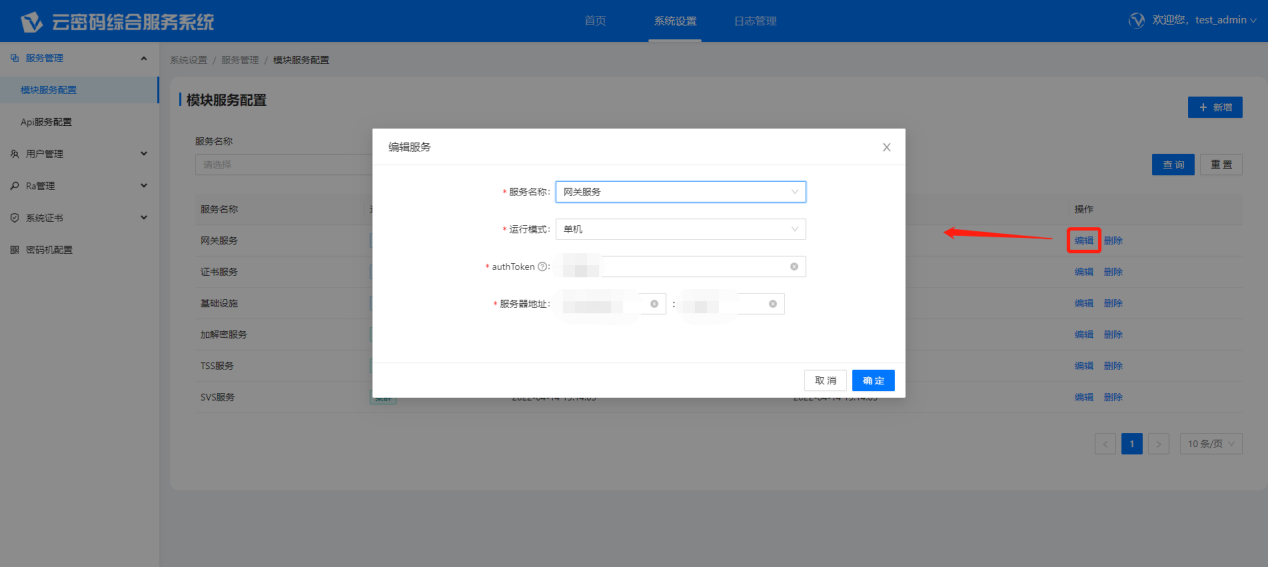
>> “**服务名称**”用于填写服务名称；

>> “**运行模式**”分为单机和集群，可根据需要选择相应的运行模式；

>> “**authToken**”为内部校验的凭证；

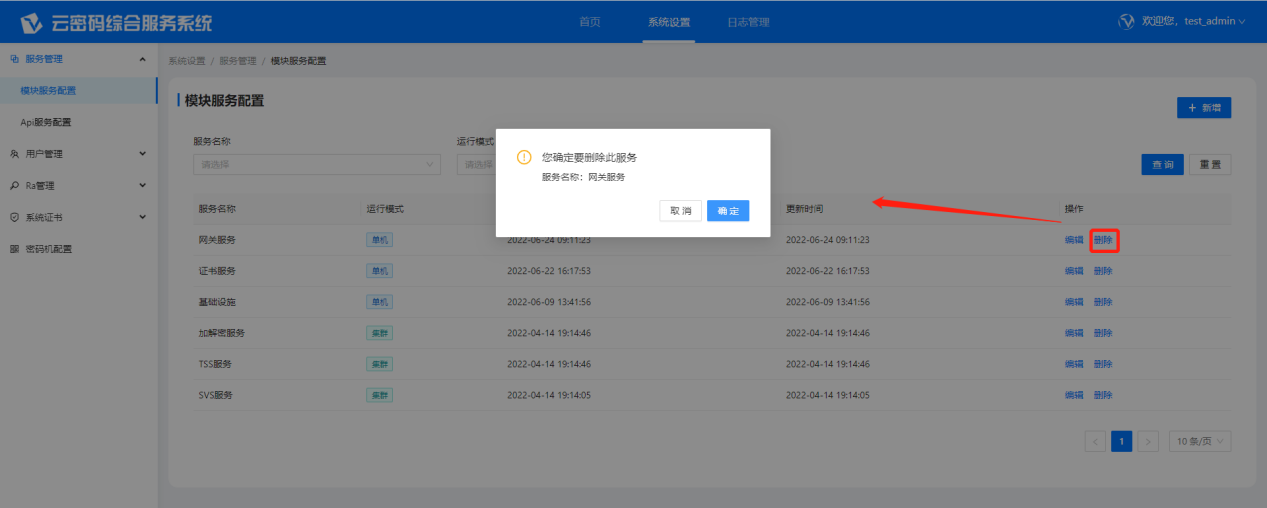
>> “**服务器地址**”用于添加具体的服务器地址

1. 点击操作中的【编辑】按钮，可以对已添加的模块服务进行编辑操作，如下图所示：



>> 编辑操作同“新增”操作，详见描述请见“新增”服务操作步骤和描述；

1. 点击操作中的【删除】按钮，可以删除该模块服务，如下图所示：



>> 点击确定后，服务被删除；

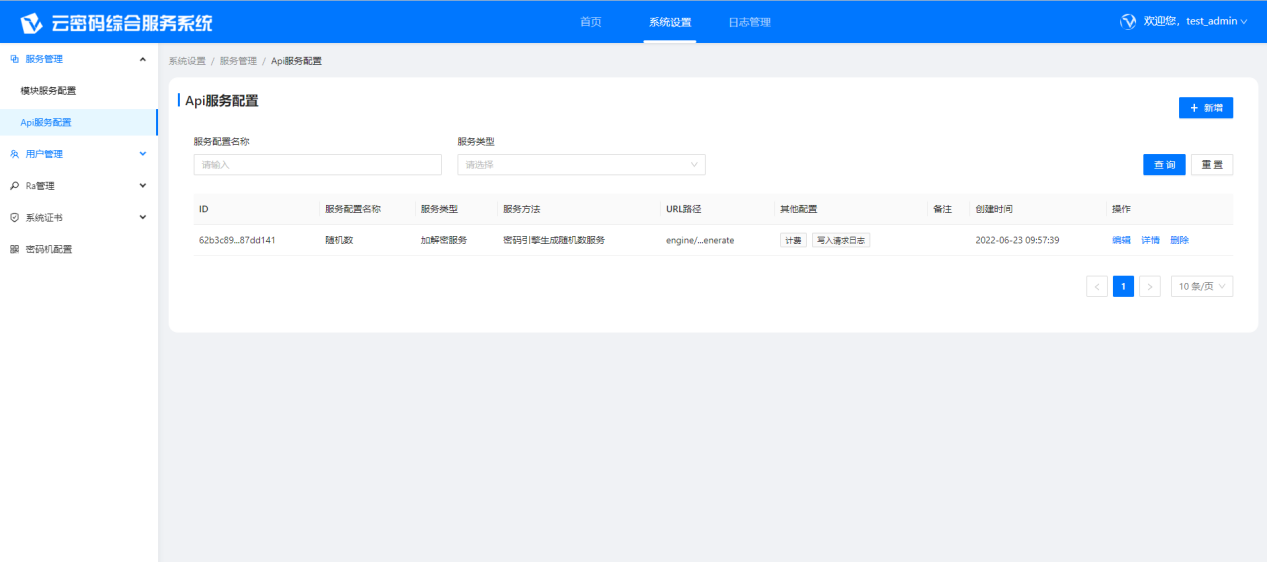
#### 2.3.1.2 Api服务配置

##### 2.3.1.2.1功能介绍

Api服务配置主要对SVS、TSS和加解密的Api服务进行新增和配置。

##### 2.3.1.2.2操作步骤

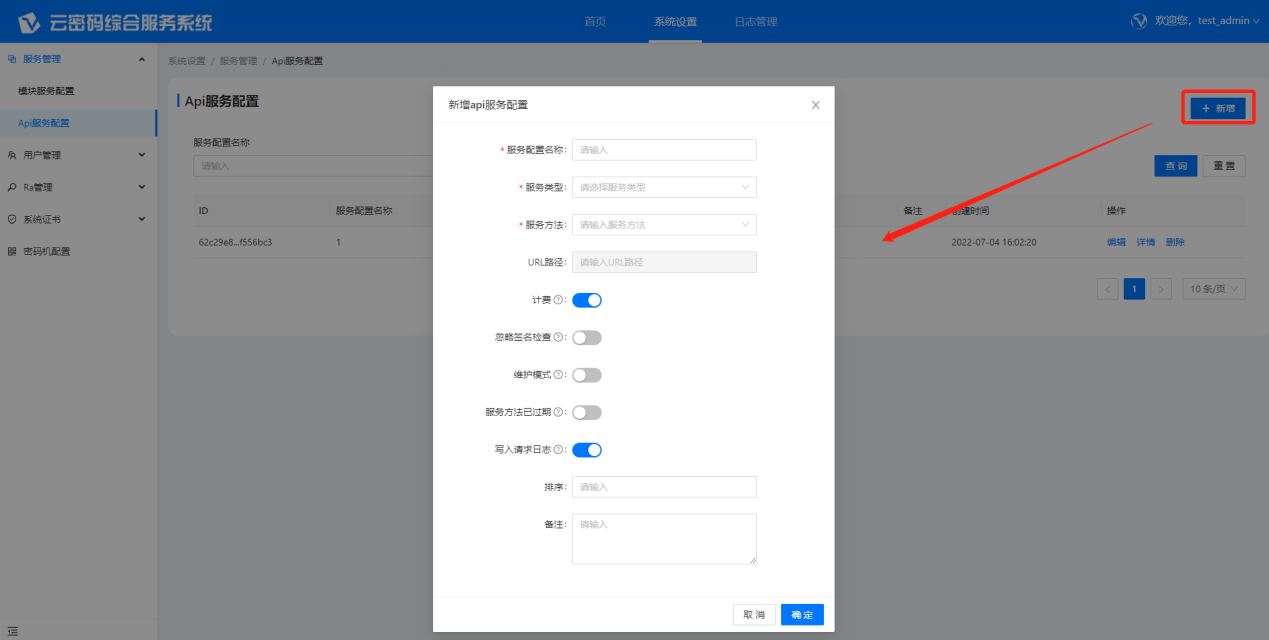
点击菜单〖系统设置〗-〖服务管理〗-〖Api服务配置〗，进入Api服务配置页面，如下图所示：



>> 列表展示所有Api服务配置信息，包含ID、服务配置名称、服务类型、服务方法、URL路径、其他配置、创建时间、备注和操作；

>> 可以根据“服务配置名称”、“服务类型”查询项来进行查询操作；

1. 点击页面的【新增】按钮，新增Api服务配置，如下图所示：



>> “**服务配置名称**”用于填写服务配置名称；

>> “**服务类型**”用于选择服务类型，包含SVS服务、TSS服务、加解密服务；

>> “**服务方法**”用于选择相应服务类型下的服务方法；

>> “**URL路径**”在选择了服务类型和服务方法后，会自动跳出相应的地址；

>> “**计费**”用于选择是否需要计费。当选择计费后，会默认在服务调用成功时写入日志；

>> “**忽略签名检查**”用于选择是否忽略签名检查；

>> “**维护模式**”用于开启后服务方法将出来维护状态，不可使用；

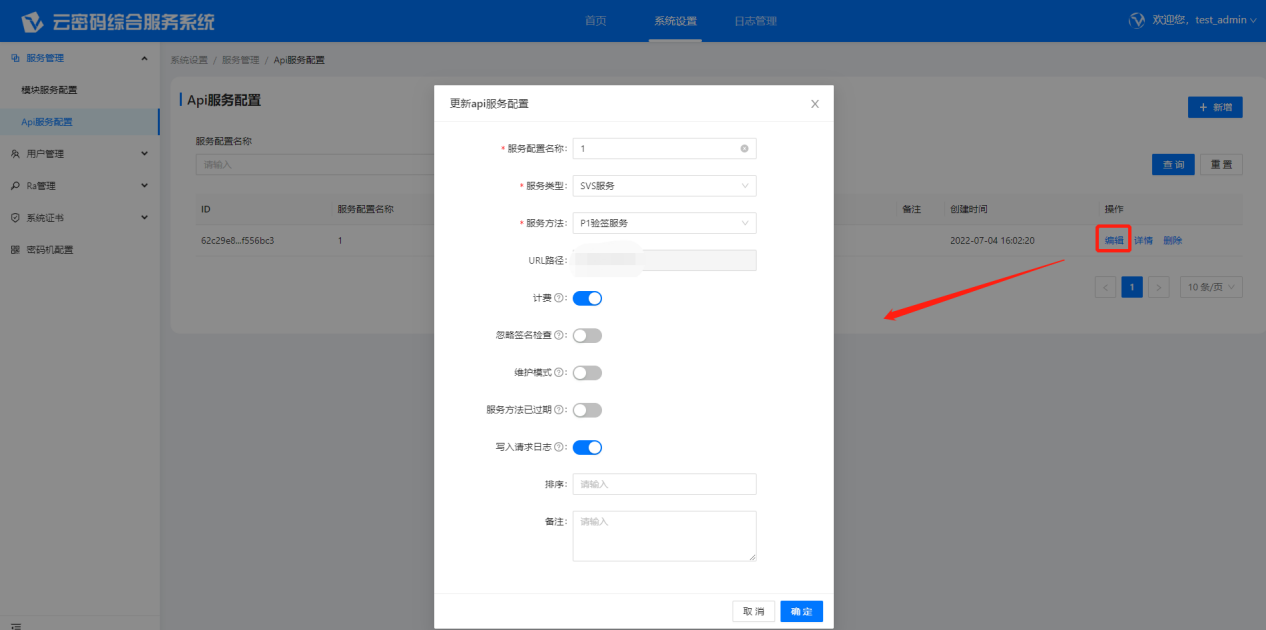
>> “**服务方法已过期**”用于选择服务方法是否已经过期，即调用后无法返回正常响应；

>> “**写入请求日志**”用于选择调用成功时是否需要写入日志；

>> “**排序**”用于服务的排序；

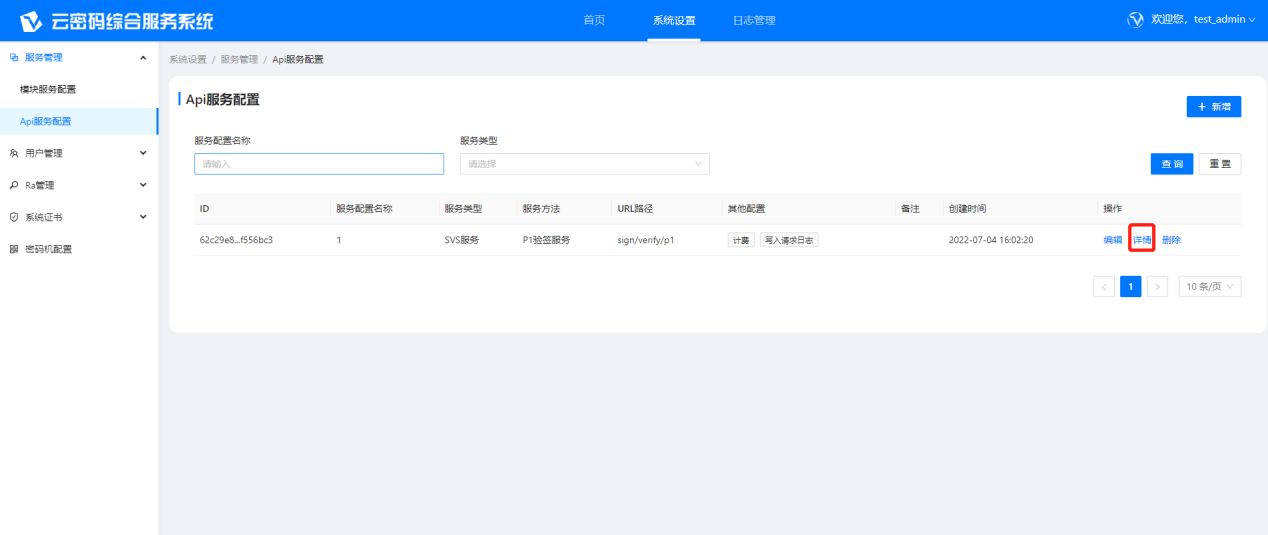
>> “**备注**”用于输入Api服务的备注信息；

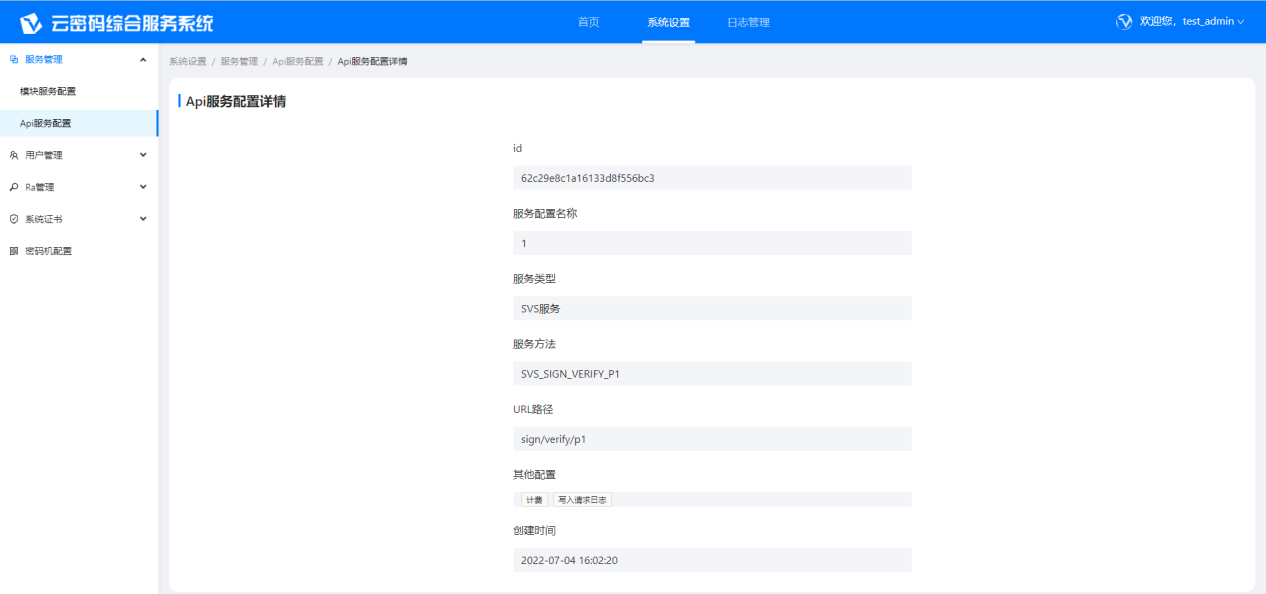
1. 点击操作中的【编辑】按钮，可以对已添加的Api服务进行编辑操作，如下图所示：



>> 编辑操作同“新增”操作，详细描述请见“新增”Api服务操作步骤和描述；

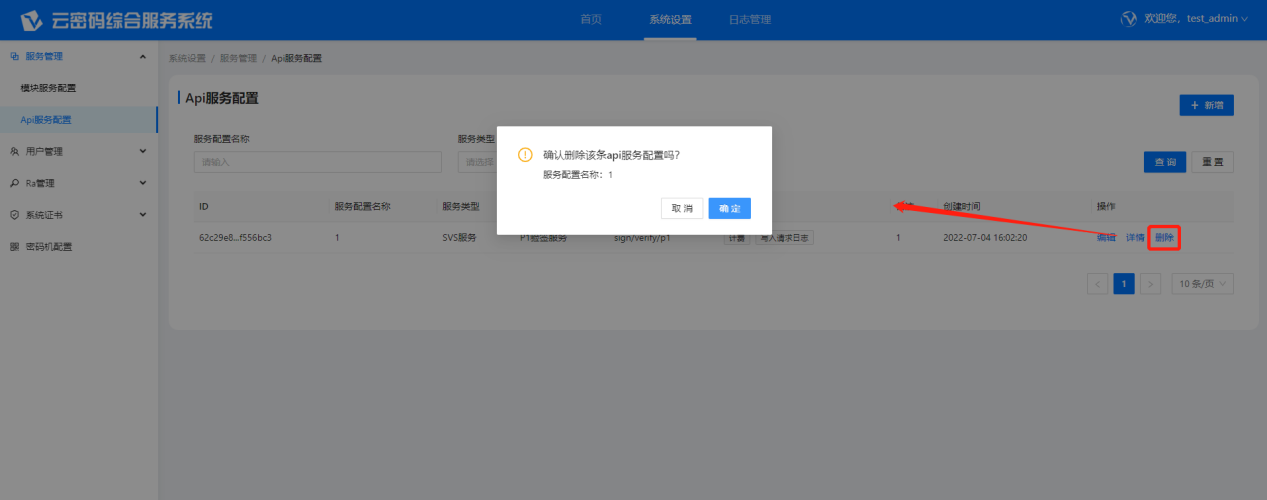
1. 点击操作中的【详情】按钮，可查看Api服务的详细信息，如下图所示：





>>页面展示该Api服务配置详情，主要包括包含ID、服务配置名称、服务类型、服务方法、URL路径、其他配置、创建时间信息；

1. 点击操作中的【删除】按钮，可以删除该Api服务，如下图所示：



>> 点击确定后，该Api服务被删除；

### 2.3.2用户管理

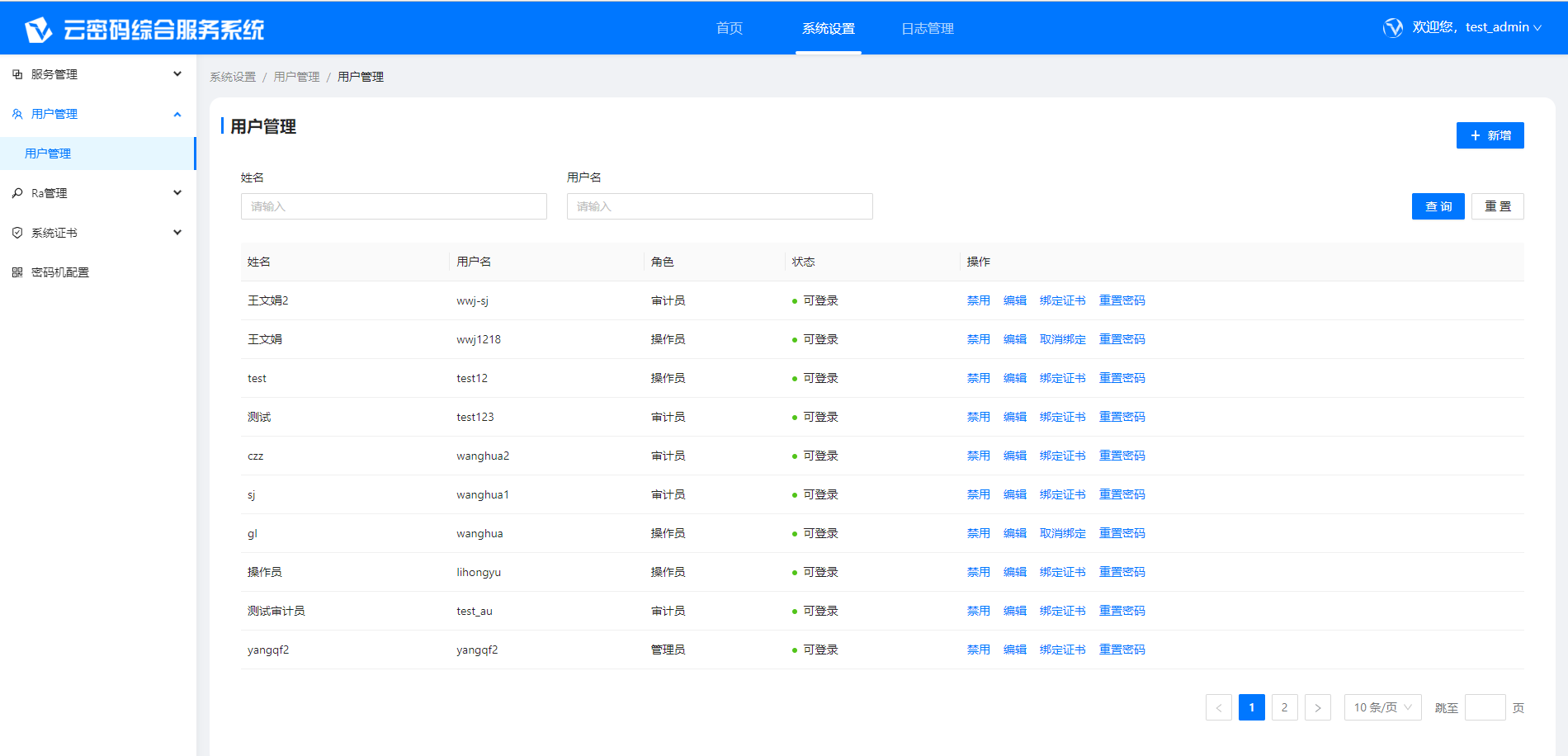
#### 2.3.2.1用户管理

##### 2.3.2.1.1功能介绍

用户管理主要是添加系统人员，并对新增人员进行系统权限的分配以及管理。

##### 2.3.2.2.2操作步骤

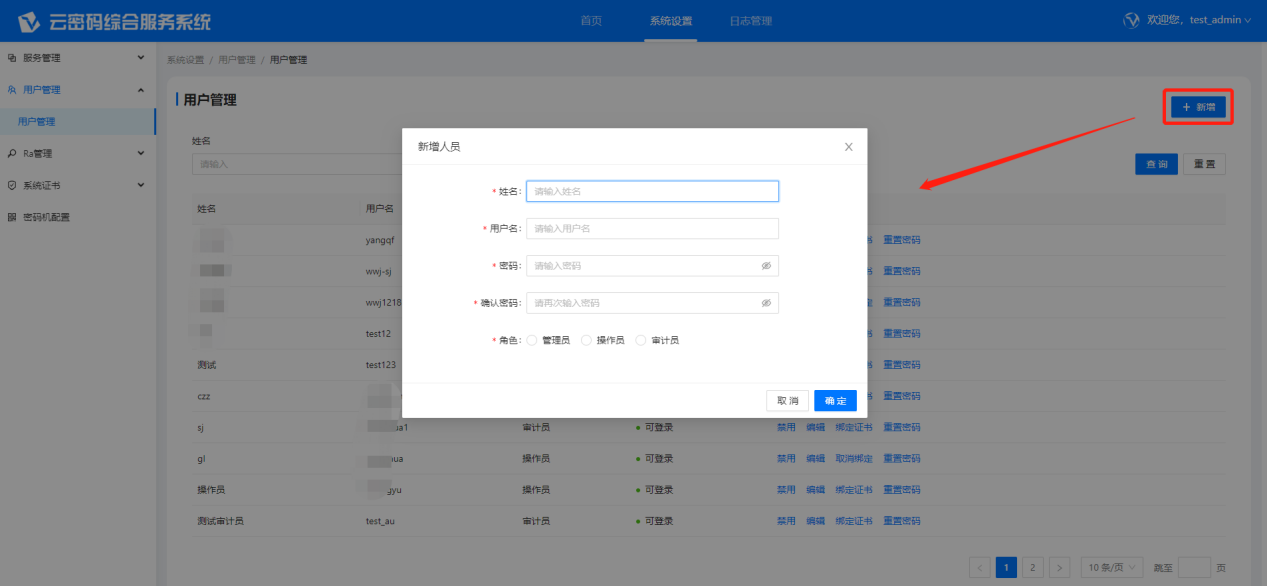
点击菜单〖系统设置〗-〖用户管理〗-〖用户管理〗，进入用户管理页面，如下图所示：



>> 列表展示所有用户信息，列表展示姓名、用户名、角色、状态和操作；

>> 可以根据“姓名”、“用户名”查询项来进行查询操作；

1. 点击页面的【新增】按钮，新增人员，如下图所示：

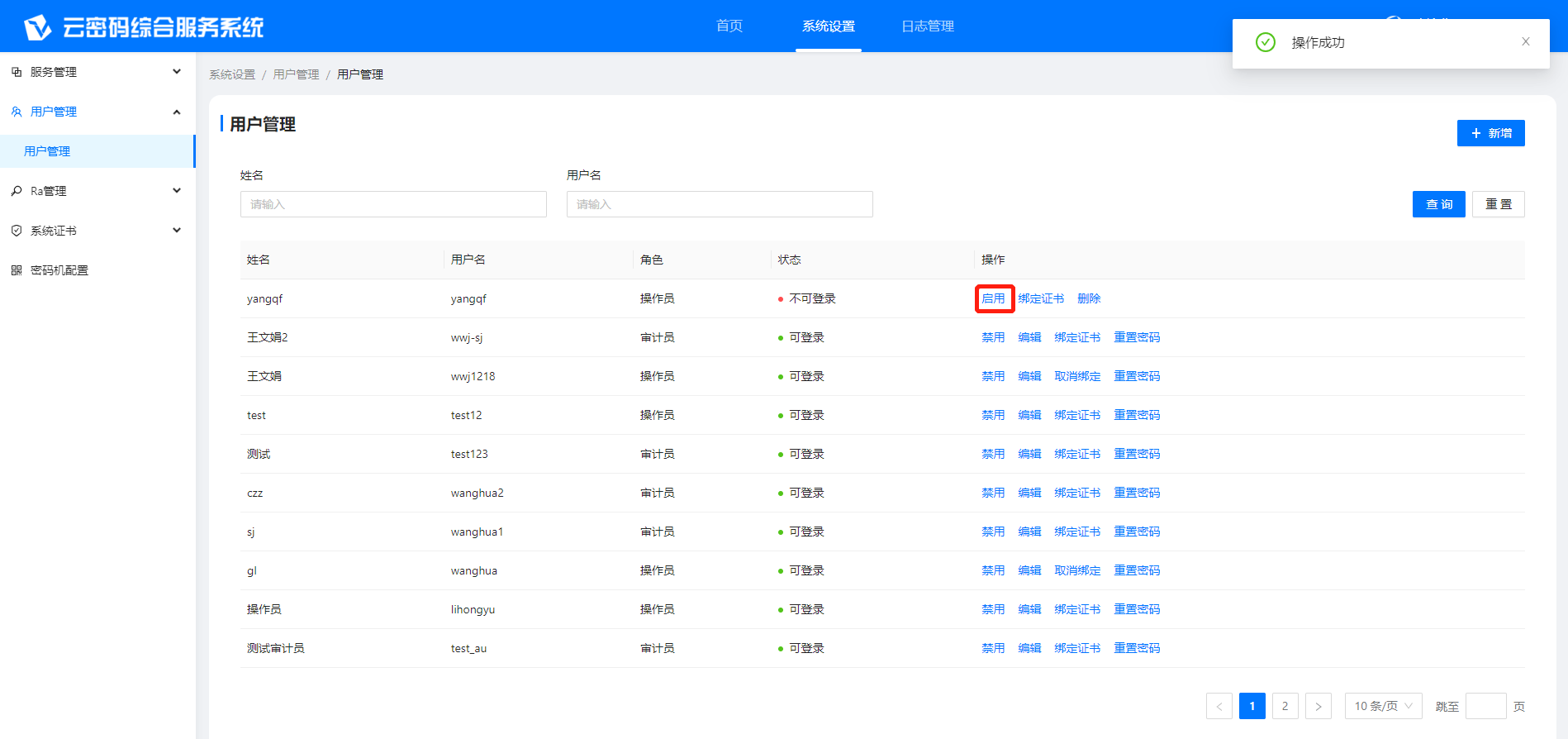


（1）在新增人员窗口输入姓名、用户名、密码、确认密码，选择角色；

（2）点击【确定】，则添加成功，信息栏会增加显示一条新增数据。如果点击【取消】，则添加失败

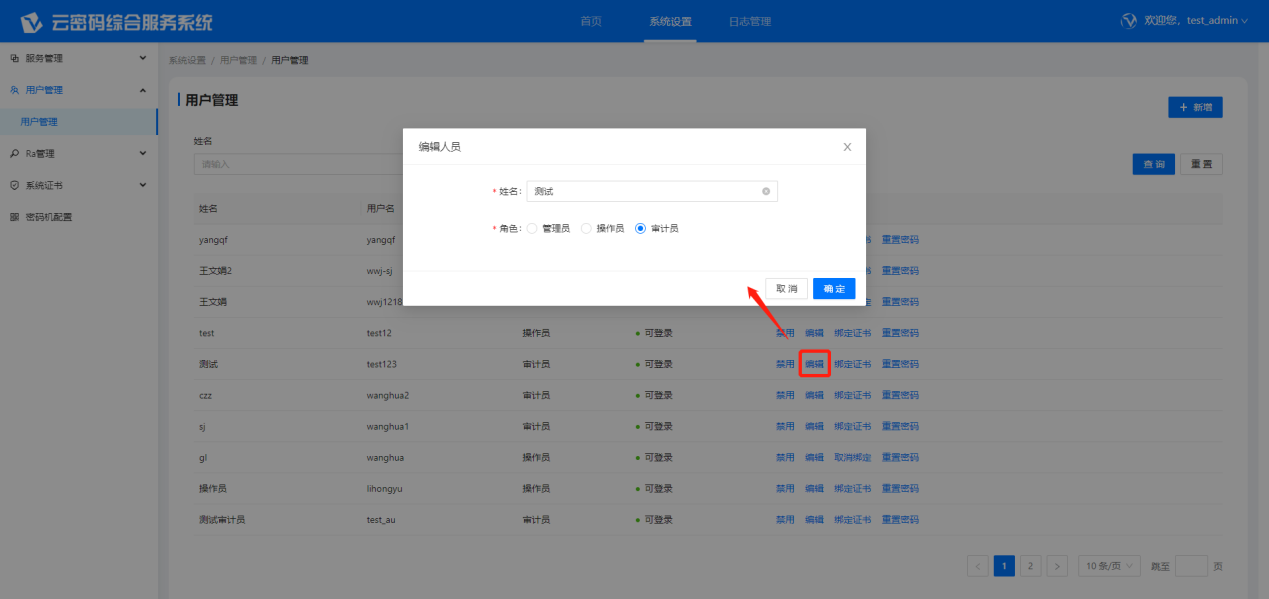
注：管理员角色拥有首页、系统设置、日志管理-服务调用日志的菜单权限；操作员角色拥有首页、SVS服务、TSS服务、加解密服务、租户管理、订阅管理的菜单权限；审计员拥有首页、日志管理-操作日志的菜单权限。

1. 点击操作中的【禁用/启用】按钮，可以启用或禁用该用户账号，如下图所示：



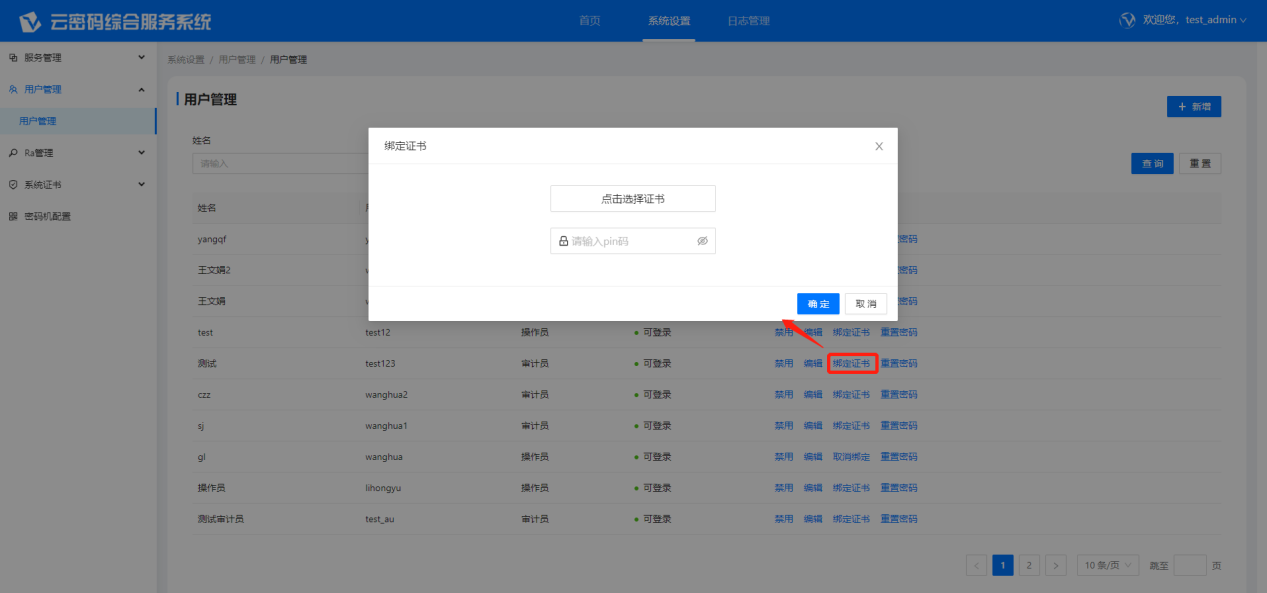
>> 点击禁用后，该用户账号被禁用，无法登录；

1. 点击操作中的【编辑】按钮，可以对已添加的用户进行编辑操作，如下图所示：



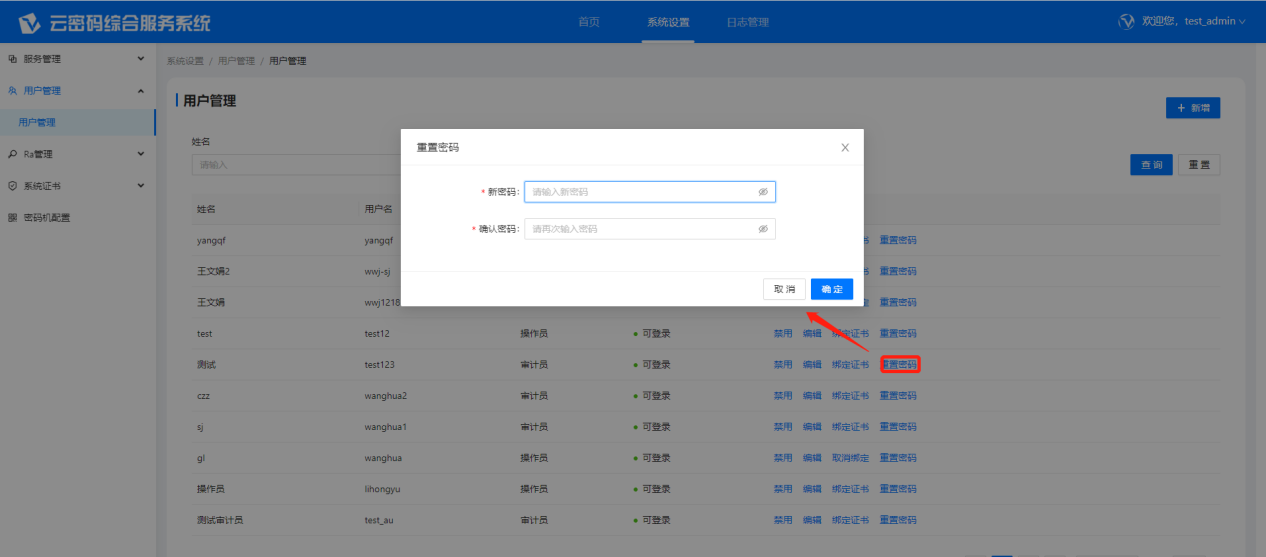
>> 在编辑人员页面可对姓名和角色进行编辑；

1. 点击操作中的【绑定证书】按钮，可以对已添加的用户进行绑定证书操作，如下图所示：



>> 需要提前插入USBkey，选择证书后输入pin码，点击确定后即可为用户绑定证书，绑定成功后即可通过证书登录系统；

1. 点击操作中的【重置密码】按钮，可以对已添加的用户进行重置密码操作，如下图所示：



>> 当用户忘记密码后，可通过重置密码登录账号。输入新密码、确认密码，点击确定，即可重置密码；

### 2.3.3 RA管理

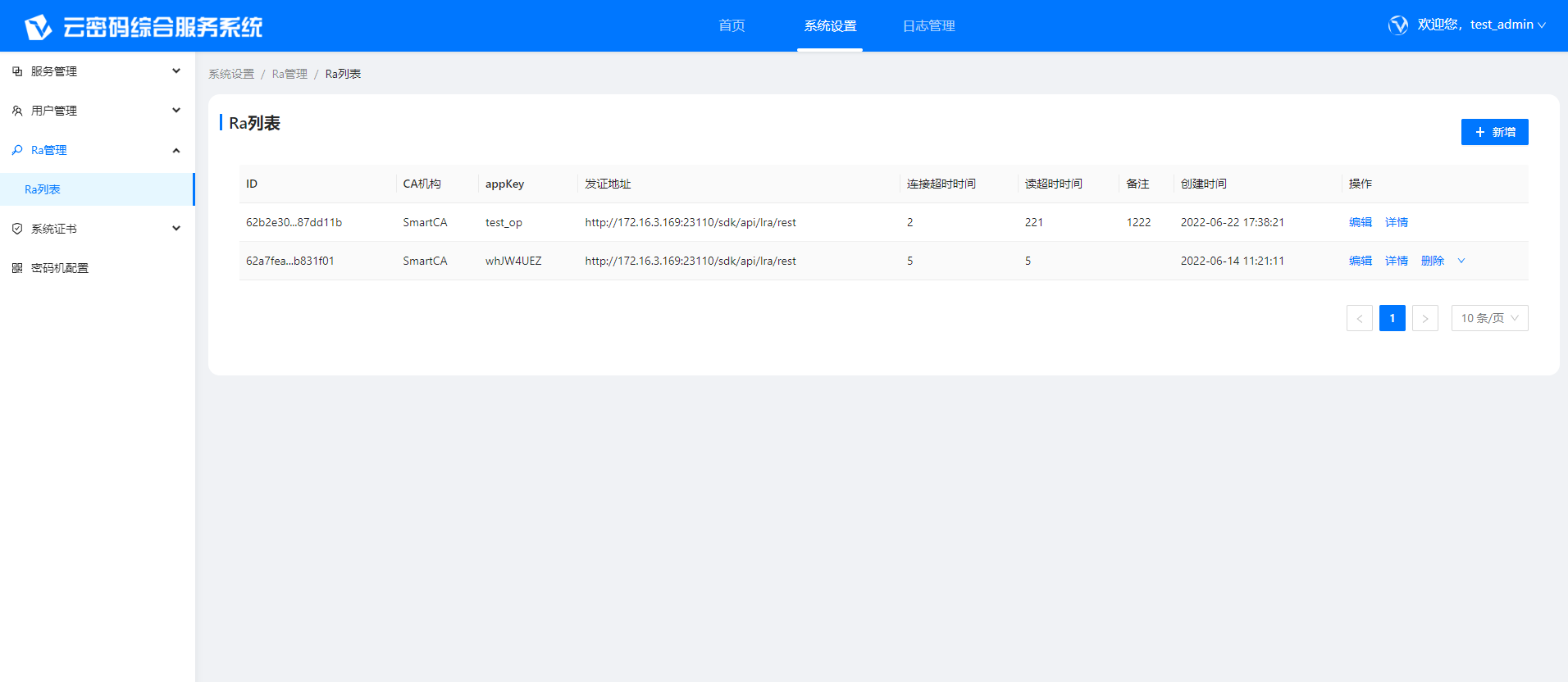
#### 2.3.3.1 RA列表

##### 2.3.3.1.1功能介绍

RA列表主要用来添加和配置可用的RA服务，添加完后可用于证书签发服务。

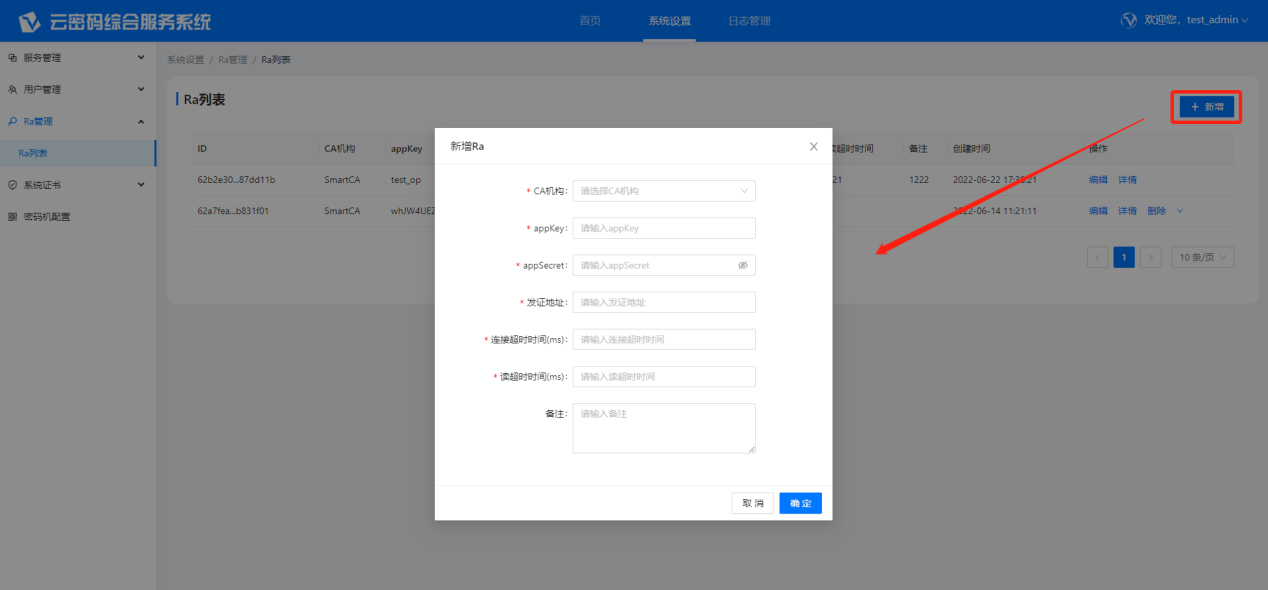
##### 2.3.3.1.2操作步骤

点击菜单〖系统设置〗-〖RA管理〗-〖RA列表〗，进入RA列表页面，如下图所示：



>> 列表展示所有RA信息，列表展示ID、CA机构、appkey、发证地址、连接超时时间、读超时时间、创建时间、备注和操作；

1. 点击页面的【新增】按钮，新增RA，如下图所示：



（1）在新增RA窗口选择CA机构，输入appkey、appSecret、发证地址、连接超时时间、读超时时间和备注；

（2）点击【确定】，则添加成功，信息栏会增加显示一条新增数据。如果点击【取消】，则添加失败

>> “**CA机构**”用于选择RA所属的CA机构；

>> “**appkey**”用于配置LRA应用的appkey；

>> “**appSecret**”用于输入LRA应用的appSecret；

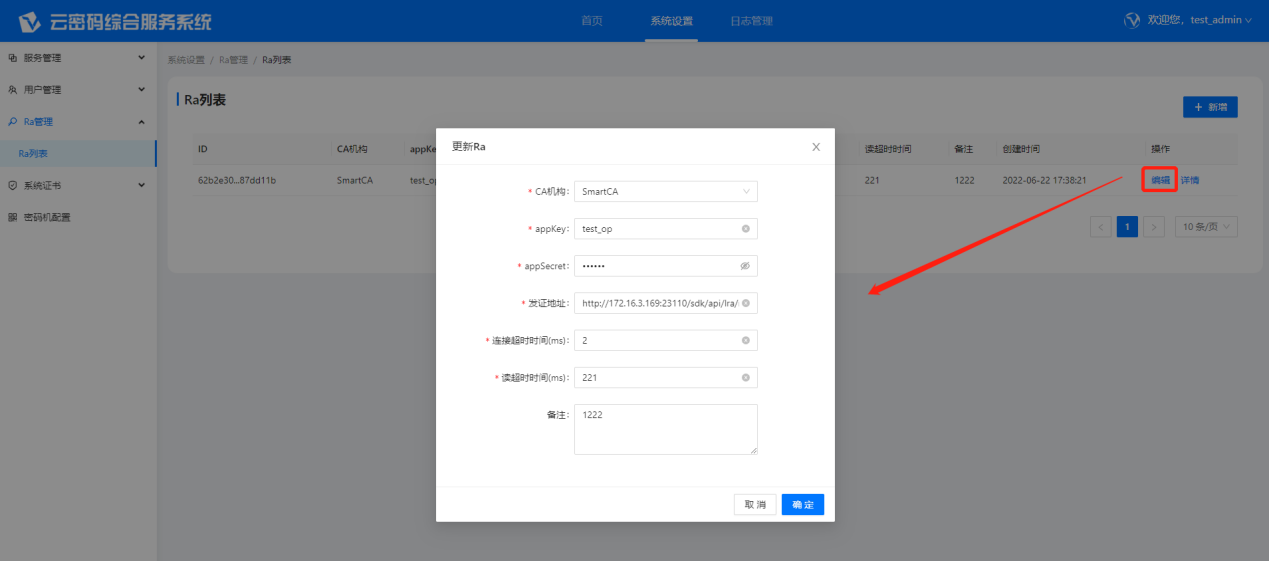
>> “**发证地址**”用于配置LRA的发证地址；

>> “**连接超时时间**”为配置连接LRA应用的超时时间，连接LRA应用时间超过该时间会自动取消连接；

>> “**读超时时间**”为配置读取LRA应用内容数据超时时间，云密码综合服务系统连接LRA应用后，然后进行内容数据的获取，当读取时间超过该时间时，则自动断开；

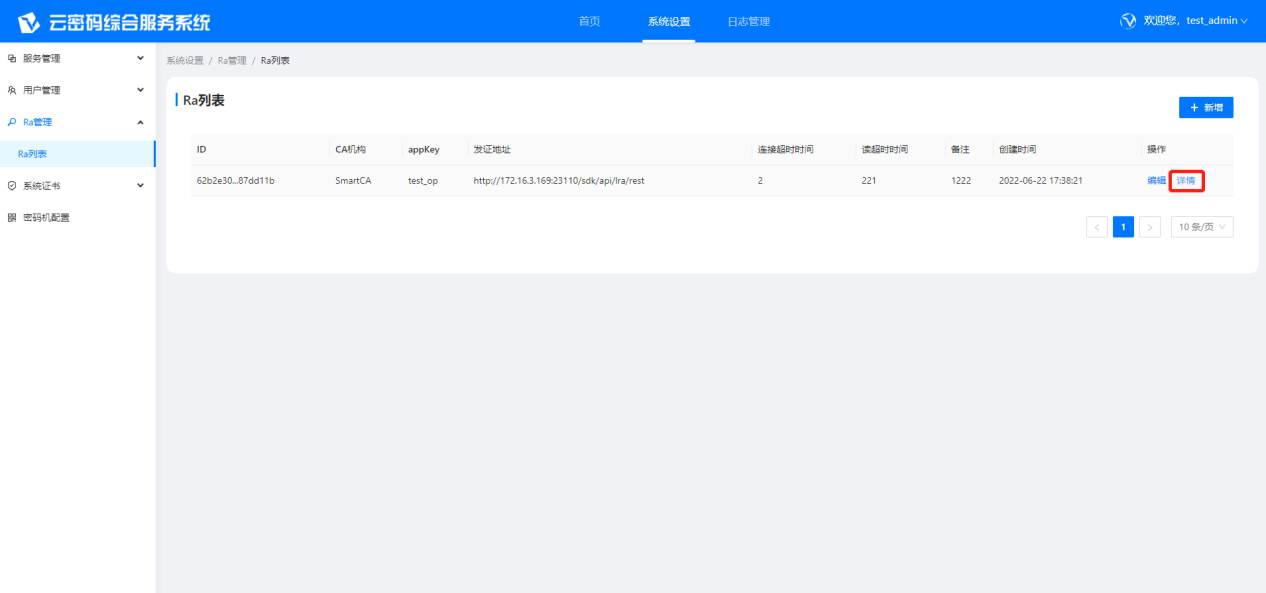
>> “**备注**”用于输入RA的备注信息

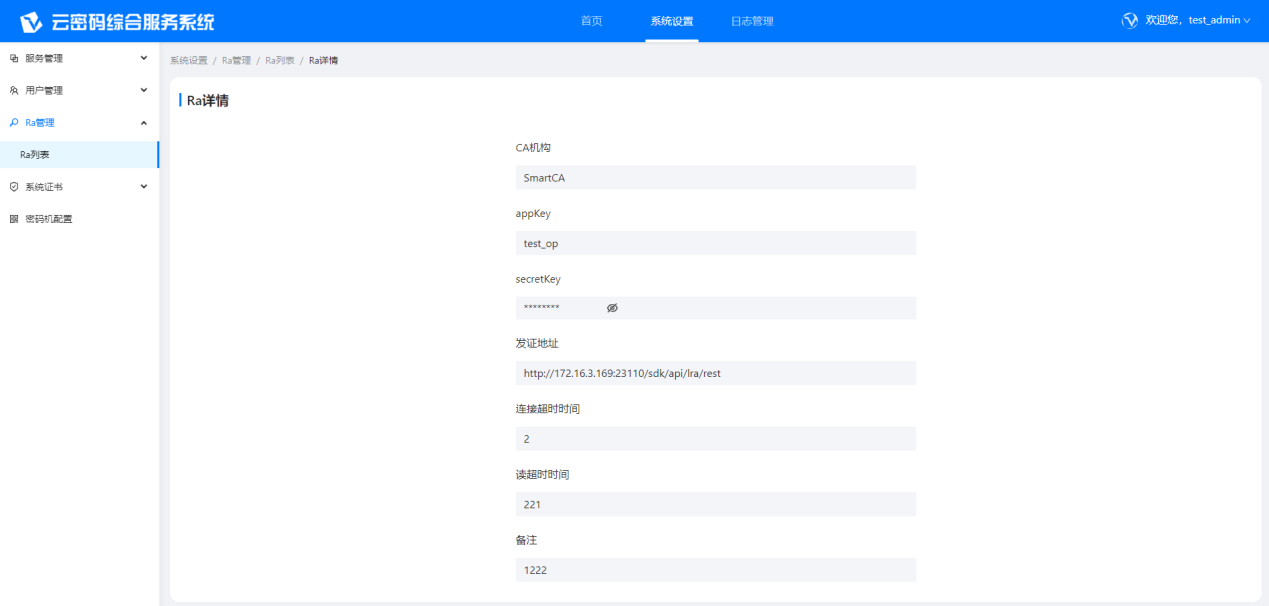
1. 点击页面的【编辑】按钮，可以对已添加的RA进行编辑操作，如下图所示：



>>编辑操作同“新增”操作，详细描述请见“新增”RA操作步骤和描述；

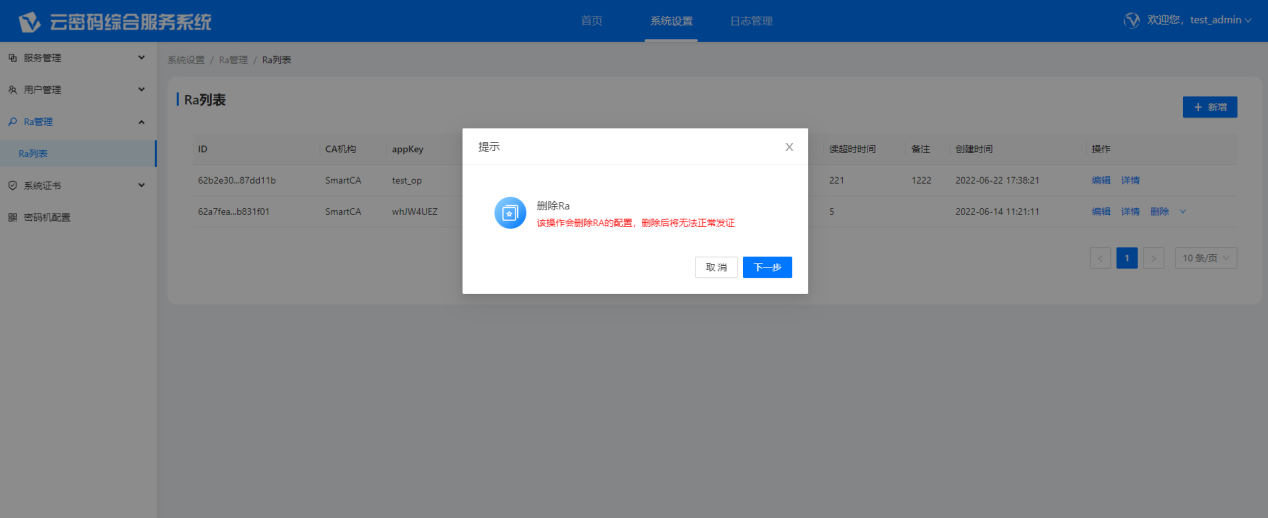
1. 点击页面的【详情】按钮，可以查看RA的详细信息，如下图所示：

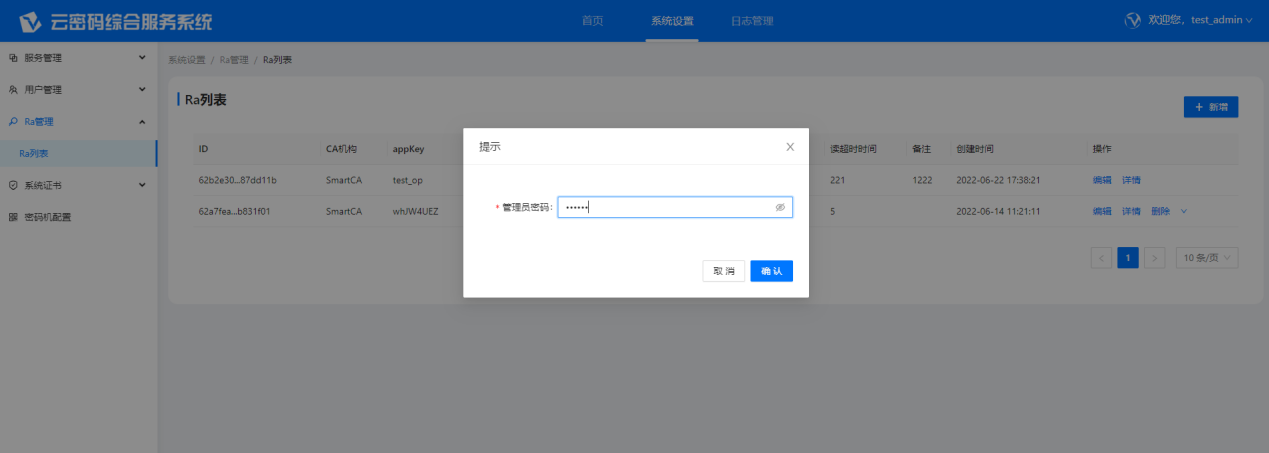




>> RA详情展示所有RA信息，包含CA机构、appkey、SecretKey、发证地址、连接超时时间、读超时时间、备注；

1. 点击页面的【删除】按钮，可以删除该RA，如下图所示：

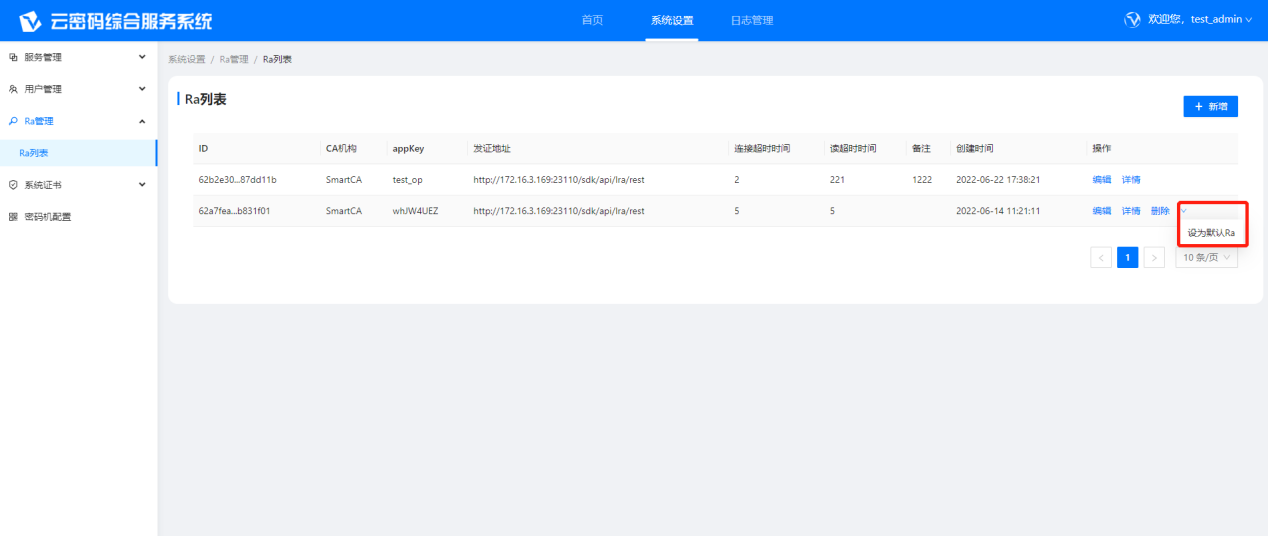




（1）点击删除后会跳出“该操作会删除RA的配置，删除后将无法正常发证”的提示。

（2）点击下一步，输入管理员密码后点击确定，即可删除该RA

1. 点击页面的下拉按钮，可以将该RA设为默认RA，如下图所示：



>> 将RA设为默认RA后，操作栏的删除按钮将会隐藏；

### 2.3.4系统证书

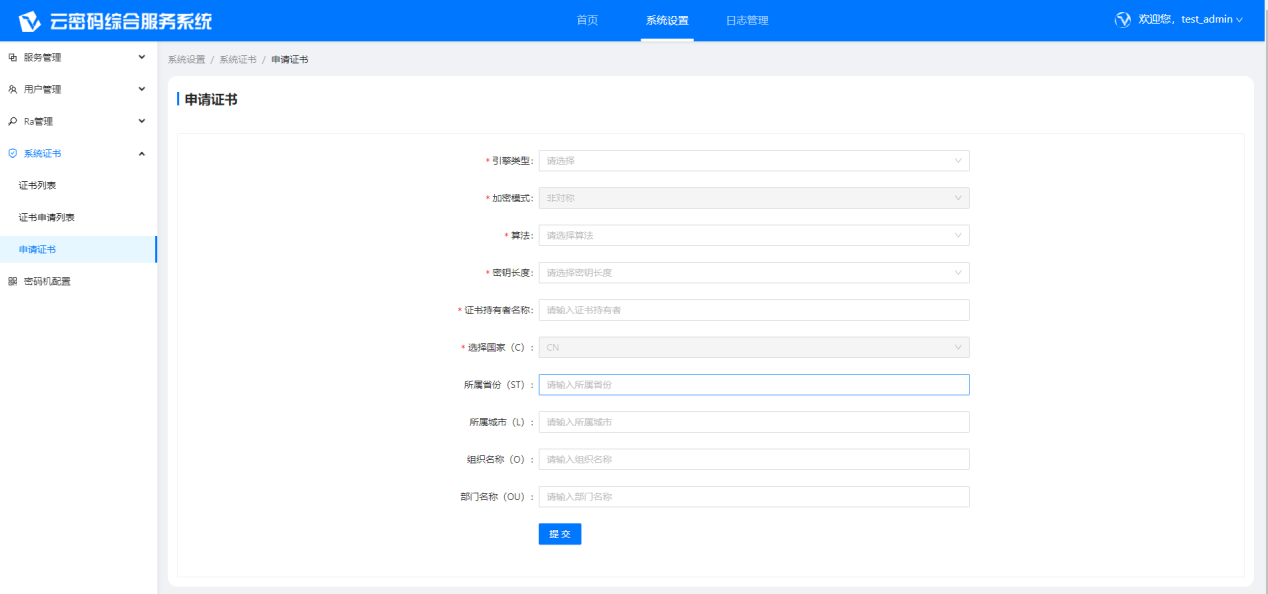
#### 2.3.4.1申请证书

##### 2.3.4.1.1功能介绍

系统证书用于申请时间戳证书，默认签发单证。密码机配置完成后，才能申请证书。证书信息提交后，通过密码机中提供的密钥对来产生P10，用于给CA机构签发时间戳证书。最后将证书导入系统后，方可调用TSS服务。

##### 2.3.4.1.2操作步骤

点击菜单〖系统设置〗-〖系统证书〗-〖申请证书〗，进入申请证书页面，如下图所示：



>> “**引擎类型**”只支持华为云；

>> “**加密模式**”默认为非对称模式，不可修改；

>> “**算法**”只支持SM2算法；

>> “**密钥长度**”只支持256；

>> “**证书持有者名称**”为输入证书持有者的名称；

>> “**选择国家（C）**”默认为CN，不可修改；

>> “**所属省份（ST）**”为输入证书所属的省份，为可选项；

>> “**所属城市（L）**”为输入证书所属的城市，为可选项；

>> “**组织名称（O）**”为输入证书所属组织，为可选项；

>> “**部门名称（OU）**”为输入证书所属部门，为可选项；

证书主题项填写完后，点击【提交】按钮，证书提交成功，申请的证书进入〖证书申请列表〗页面。

\*注：如果申请证书失败，需要检测密码机配置是否配置正确或者密码机服务是否正常。

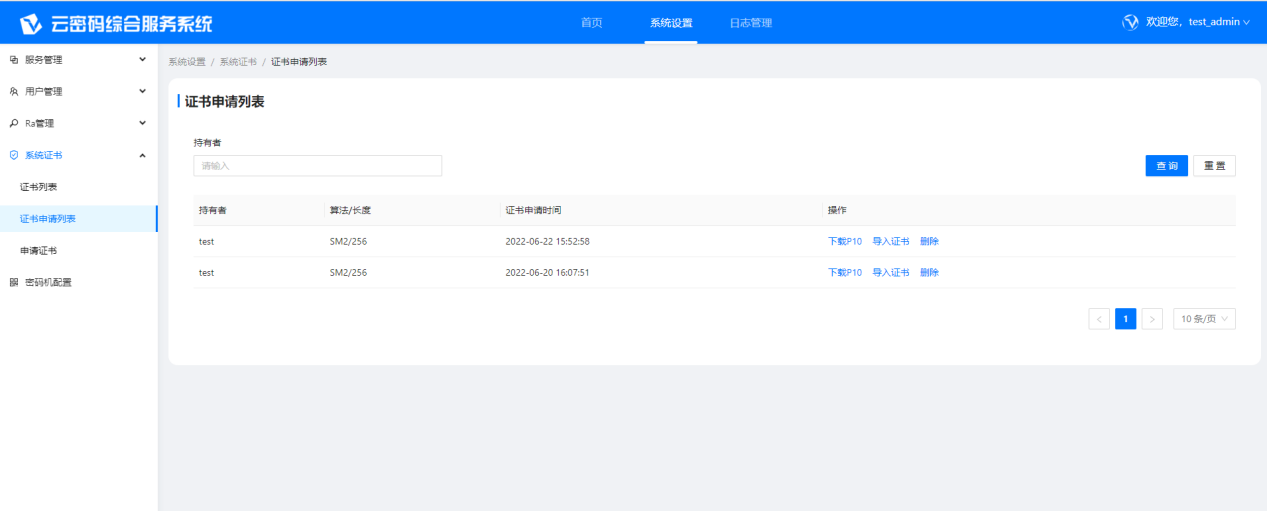
#### 2.3.4.2证书申请列表

##### 2.3.4.2.1功能介绍

证书申请列表页面展示所有已申请且未导入的待申请证书，可下载P10请求给CA机构签发时间戳证书，然后把时间戳证书的签名证书导入进去，最终生成系统证书。

##### 2.3.4.2.2操作步骤

点击菜单〖系统设置〗-〖系统证书〗-〖证书申请列表〗，进入证书申请列表页面，如下图所示：

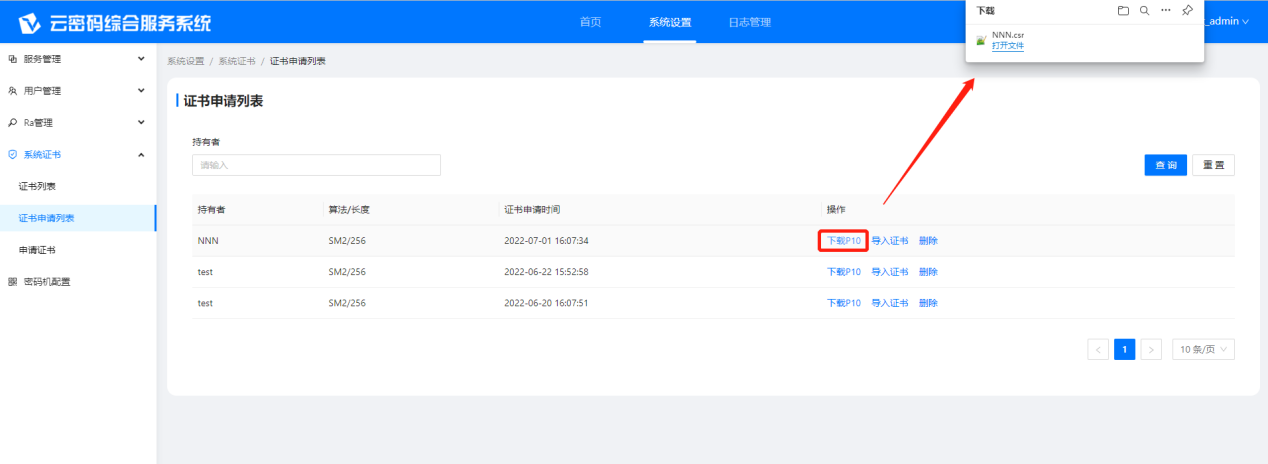


>> 证书申请列表展示所有待申请的证书，展示信息包含持有者、算法/长度、证书申请时间和操作；

>> 可以通过“持有者”查询项来查询对应的待申请证书；

>>证书申请列表支持“下载P10”、“导入证书”和“删除”的操作

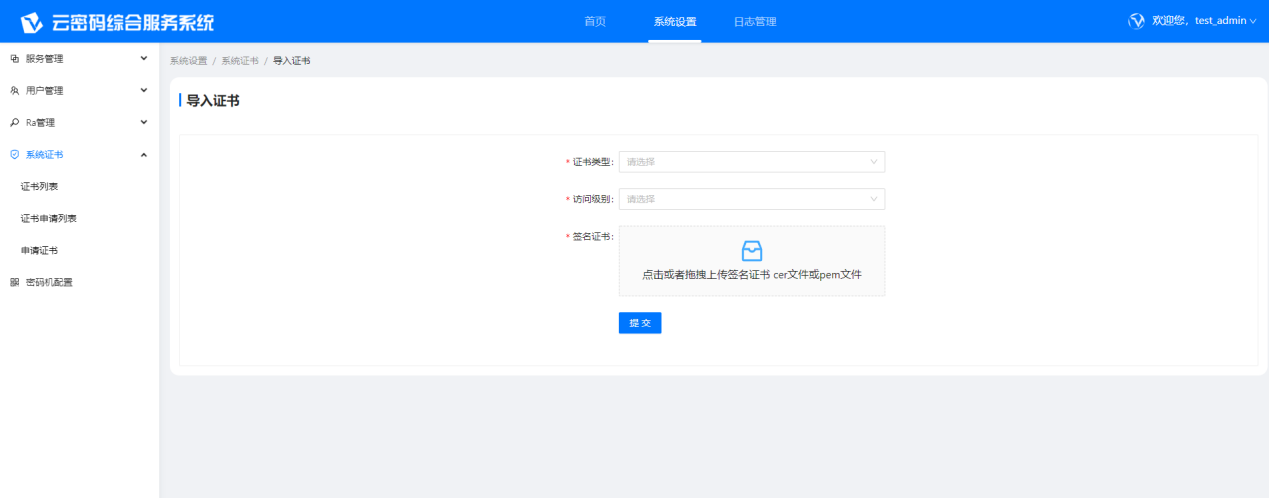
1、生成系统证书前需要先下载P10，管理员选择需要去签发的待申请证书，点击【下载P10】按钮，如下图所示：



>> P10证书里存放的是一段可以向CA申请证书的P10请求；

>> 用文本编辑工具打开下载的P10，里面存放的是一个base64文件；可以把base64数据也可以把.csr的P10文件提交给相关CA机构进行时间戳证书签发；

2、CA机构根据提交的P10证书请求签发完时间戳证书后，会返回对应的签名证书和证书链；然后上传到对应的签名证书区域：

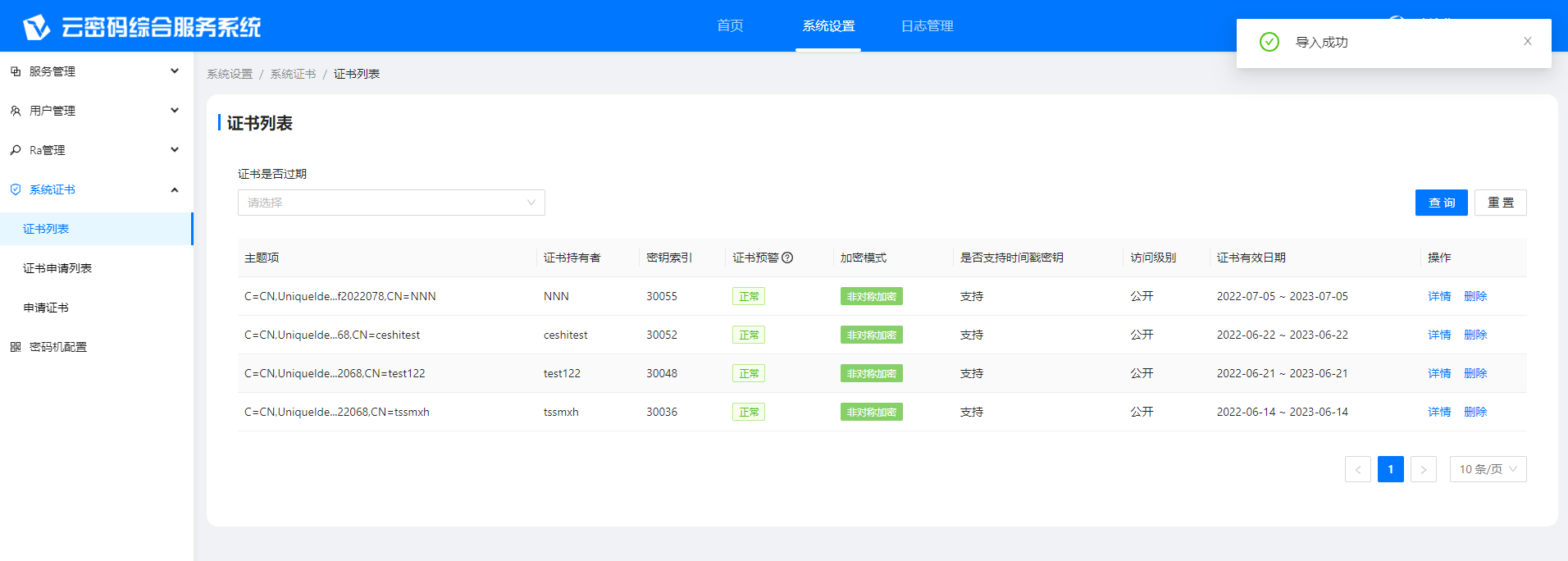


>> 证书类型目前仅支持单证；

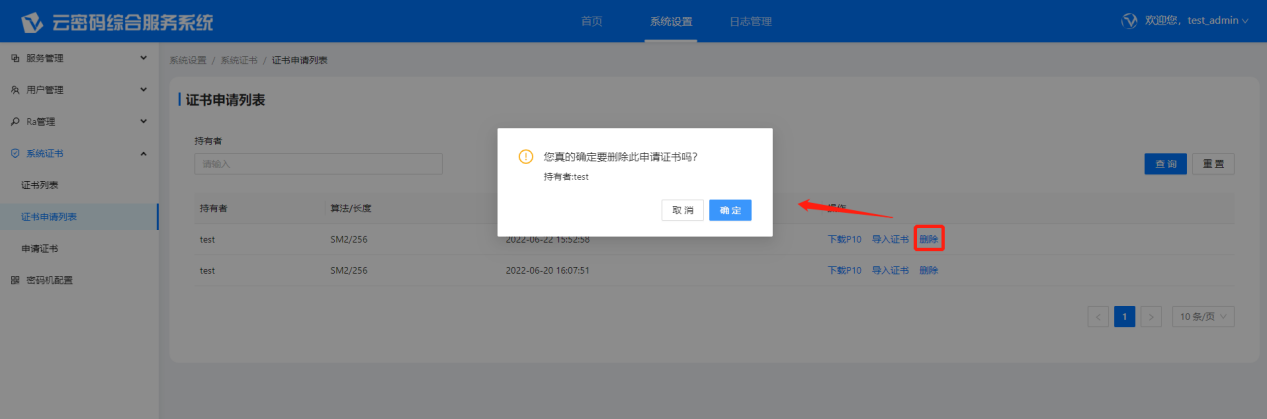
>> 访问级别目前仅支持公开；

>> 签名证书支持pem或cer文件的导入。

3、证书导入后，点击【提交】按钮，提示导入成功，导入的证书显示在〖证书列表〗页面



在证书申请列表页面，如果申请的证书不符合要求，可以进行删除操作，点击【删除】按钮，如下图所示：



在弹出的对话框中“您真的确定要删除此申请证书吗？”。若确定，点击【确定】，即可删除该证书；若要取消操作，则点击【取消】，则返回〖证书申请列表〗，该证书申请记录仍存在。

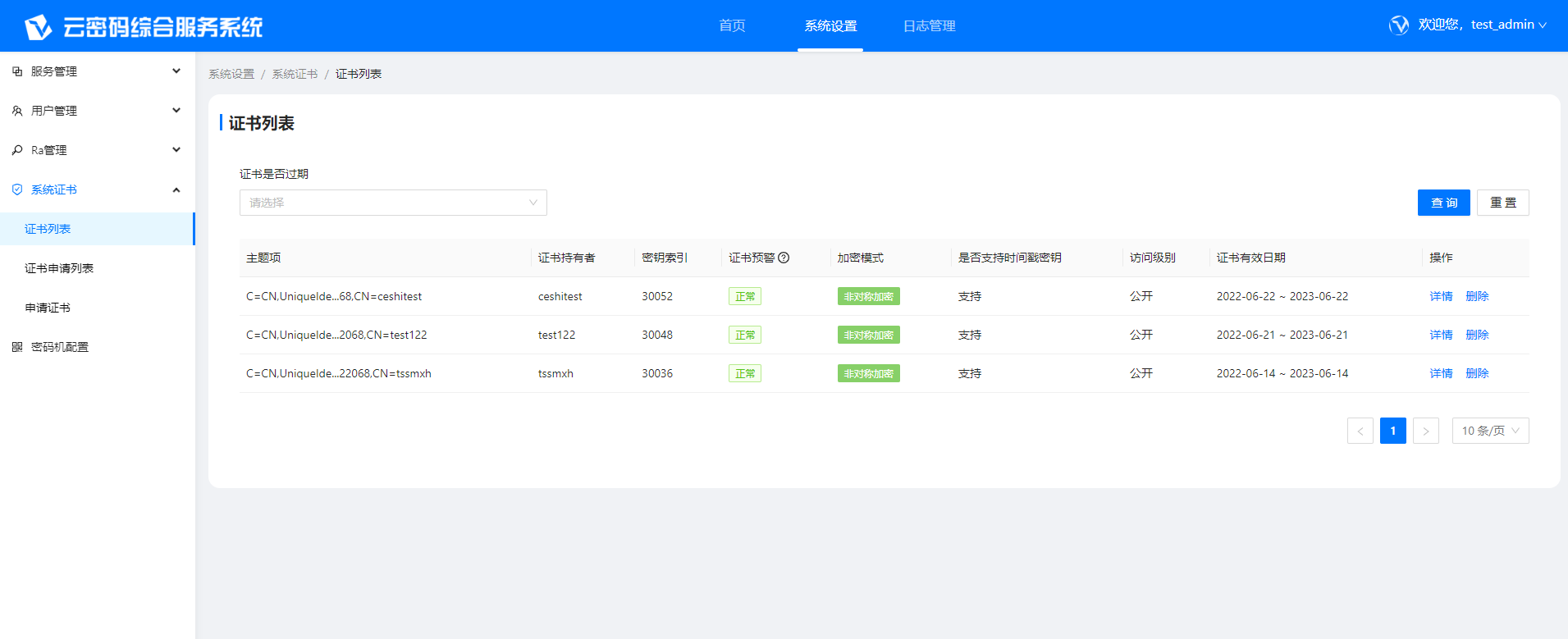
#### 2.3.4.3 证书列表

##### 2.3.4.3.1功能介绍

证书列表展示所有已导入的已签发证书，证书可用于TSS服务调用（签发时间戳和验证时间戳）。

##### 2.3.4.3.2操作步骤

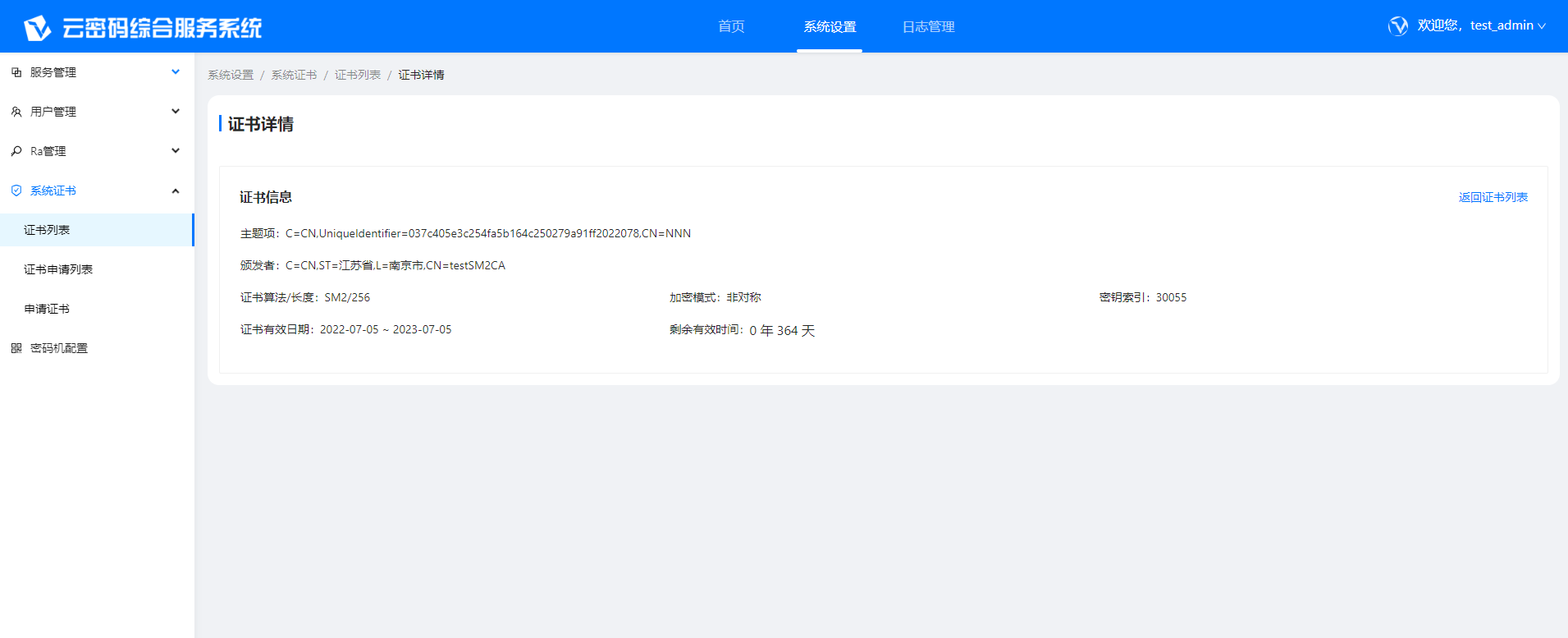
点击菜单〖系统设置〗-〖系统证书〗-〖证书列表〗，进入证书列表页面，如下图所示：



>> 证书列表展示主题项、证书持有者、密钥索引、证书预警、加密模式、是否支持时间戳密钥、访问级别、证书有效日期和操作；

>> 可以根据“证书是否过期”查询项来进行查询。

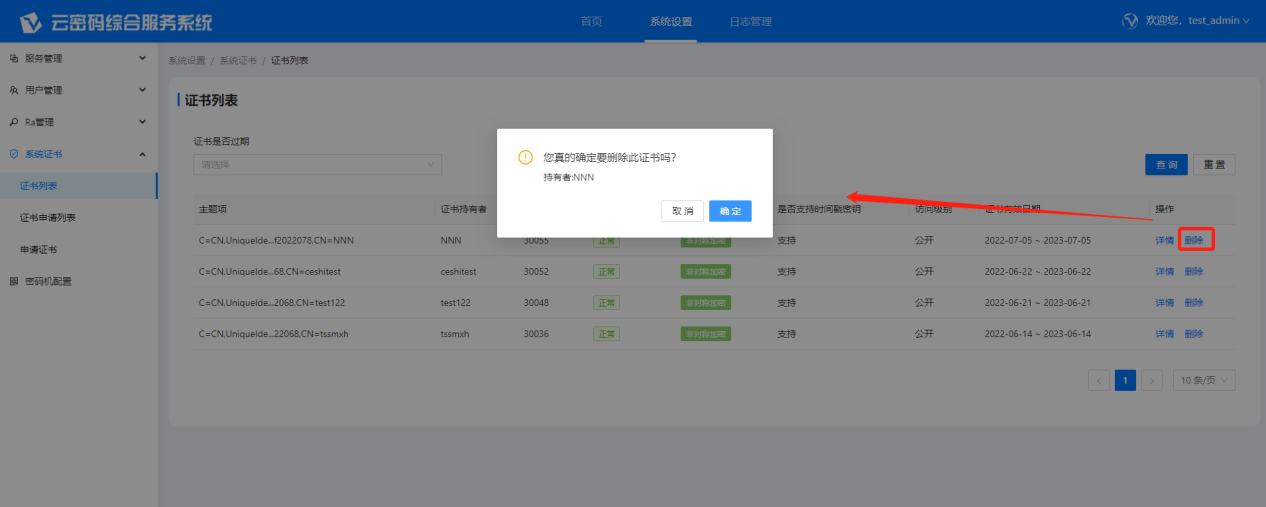
1. 点击操作中的【详情】按钮，可以查看证书的详细信息，如下图所示：



>> 页面展示该证书的主题项、颁发者、证书算法/长度、加密模式、密钥索引、证书有效日期、剩余有效日期；

>> 点击“返回证书列表”，即可返回至证书列表页面

1. 点击操作中的【删除】按钮，可以对证书进行删除操作，如下图所示：



>> 点击确定，即可删除该时间戳证书；

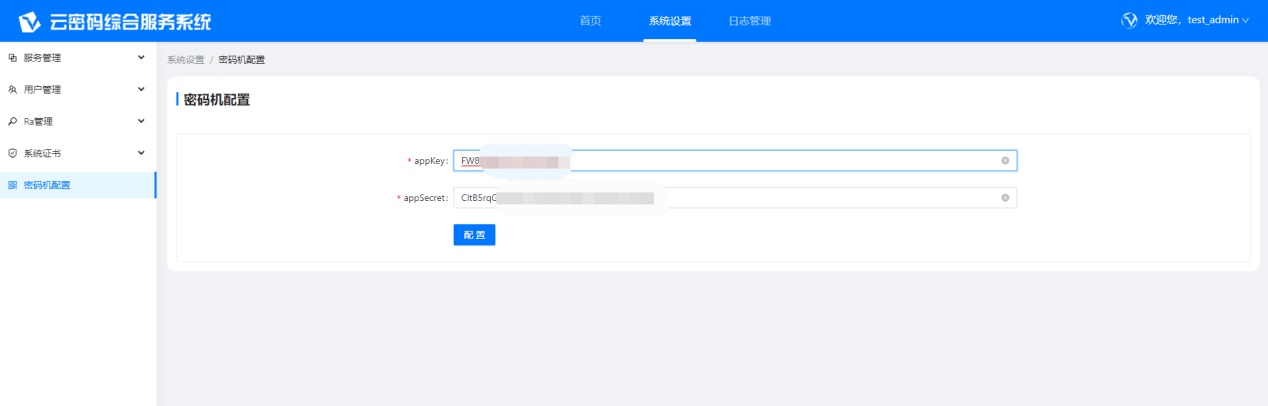
### 2.3.5密码机配置

#### 2.3.5.1功能介绍

密码机配置主要配置连接华为云密码机DEW。

#### 2.3.5.2操作步骤

点击菜单〖系统设置〗-〖密码机配置〗，进入密码机配置页面，如下图所示：



>> 在密码机配置表单配置华为云密码机的appkey和appSecret，点击配置即可配置成功；

## 2.4租户管理

系统操作员拥有租户管理菜单权限。

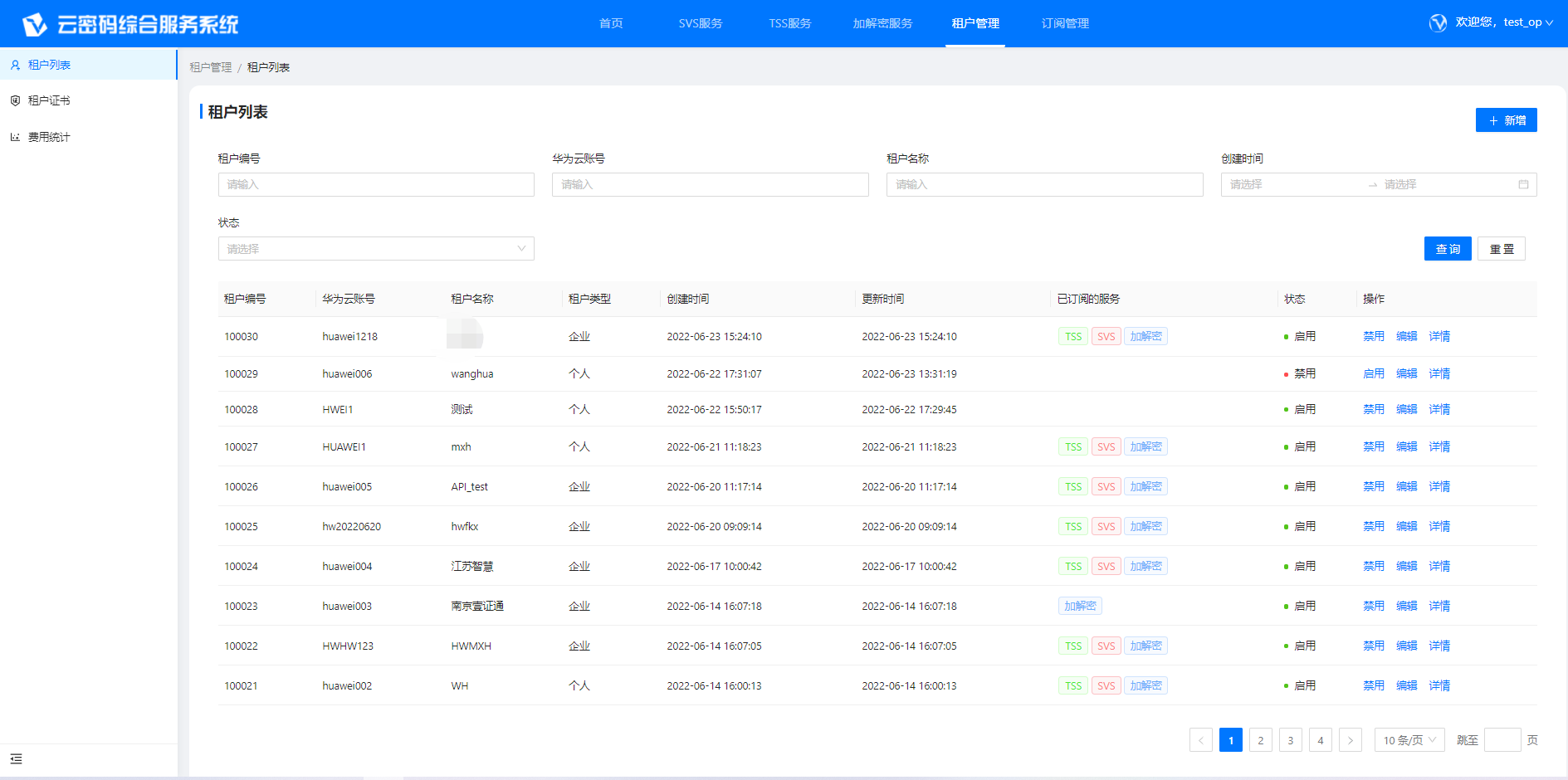
### 2.4.1租户列表

#### 2.4.1.1功能介绍

租户列表主要对系统的租户信息数据进行新增和维护。

#### 2.4.1.2操作步骤

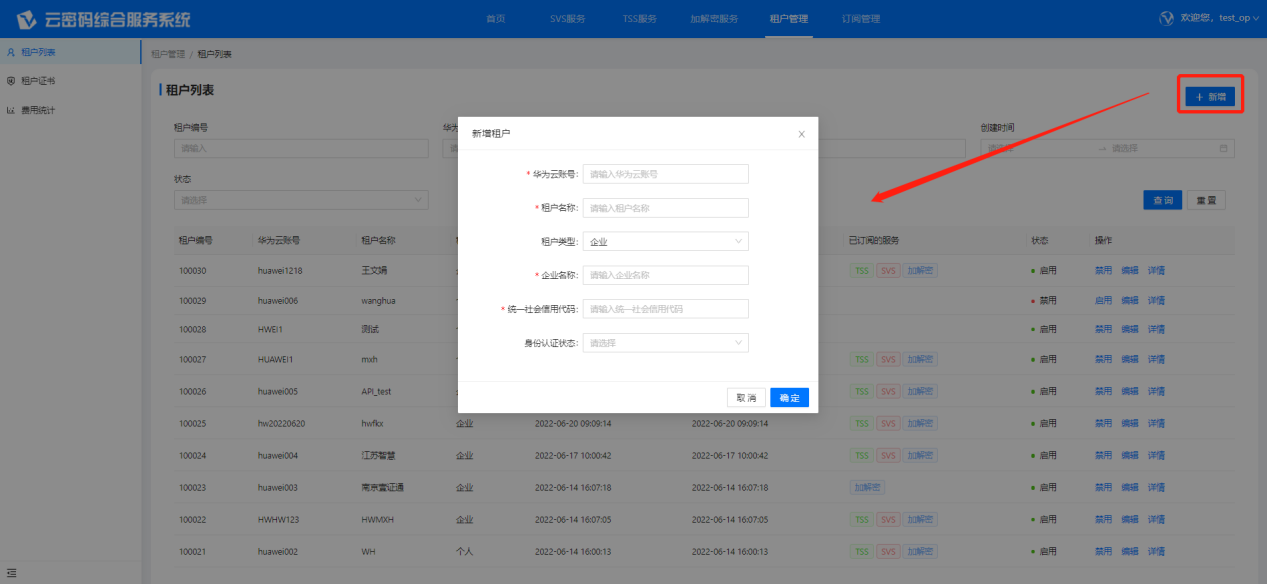
点击菜单〖租户管理〗-〖租户列表〗，进入租户列表页面，如下图所示：

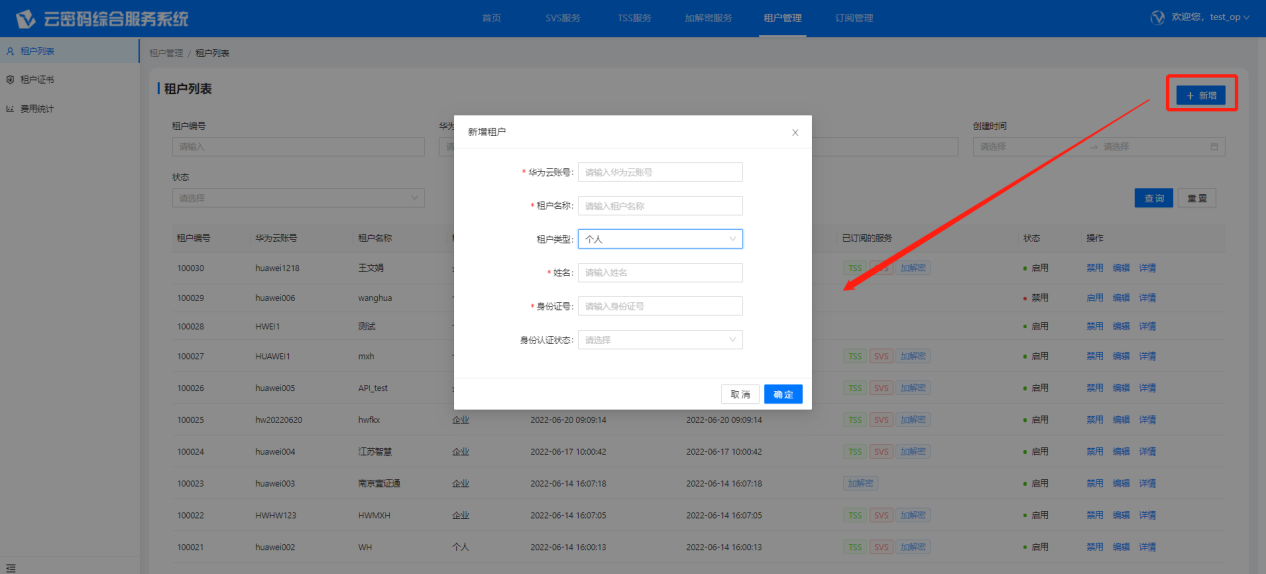


>> 页面展示所有租户信息，包含租户编号、华为云账号、租户名称、租户类型、创建时间、更新时间、已订阅的服务、状态和操作。

>> 可以根据“租户编号”、“华为云账号”、“租户名称”、“创建时间”、“状态”查询项来查询操作日志信息。

1、点击页面的【新增】按钮，新增租户，如下图所示：





>> “**华为云账号**”为输入已有的华为云账号；

>> “**租户名称**”为输入租户的具体名称；

>> “**租户类型**”为可选项，分为企业和个人，根据需要选择相应的类型；

>> “**企业名称**”为输入企业的具体名称；

>> “**统一社会信用代码**”为输入企业的统一社会信用代码；

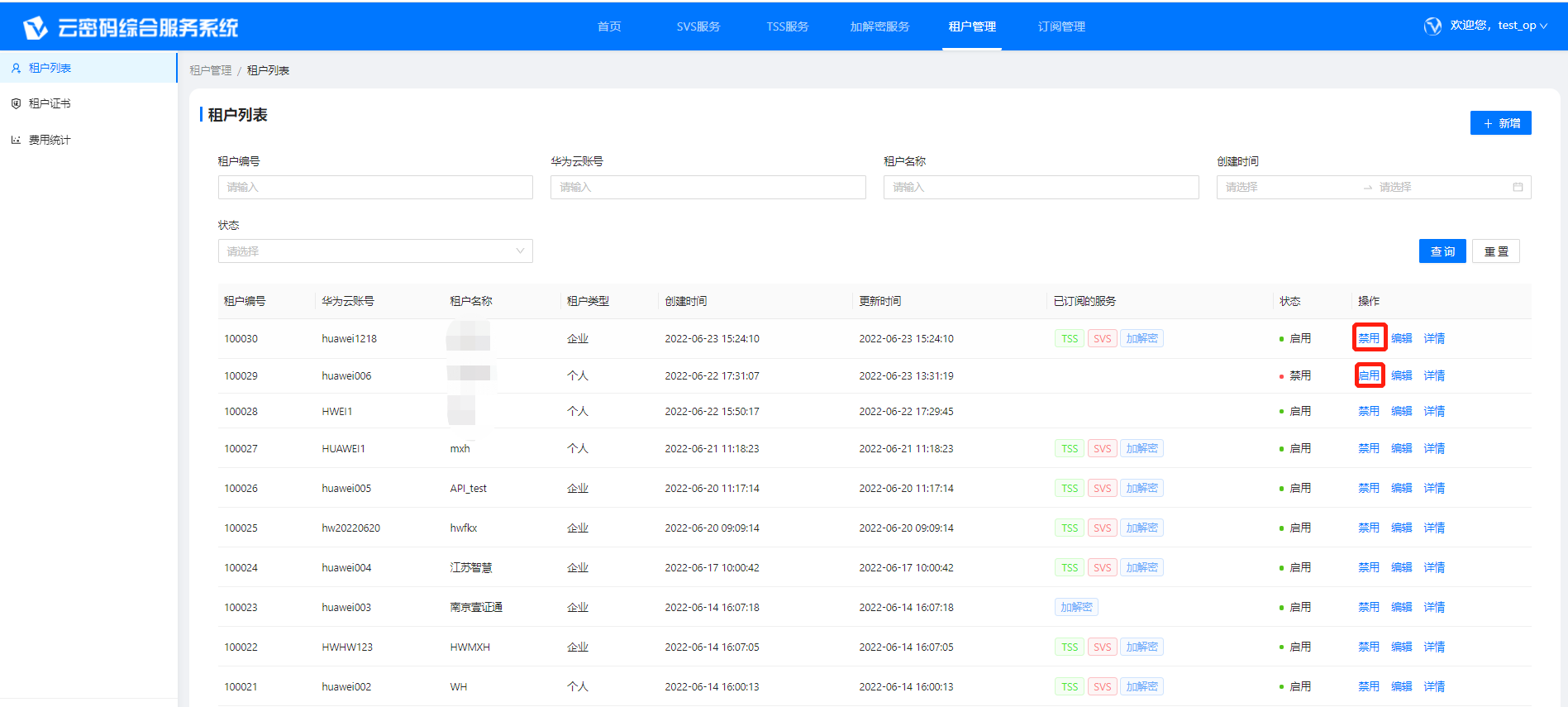
>> “**姓名**”为输入个人的姓名；

>> “**身份证号**”为输入个人的身份证号；

>> “**身份认证状态**”为可选项，分为已认证和待认证，根据需要选择相应的状态；

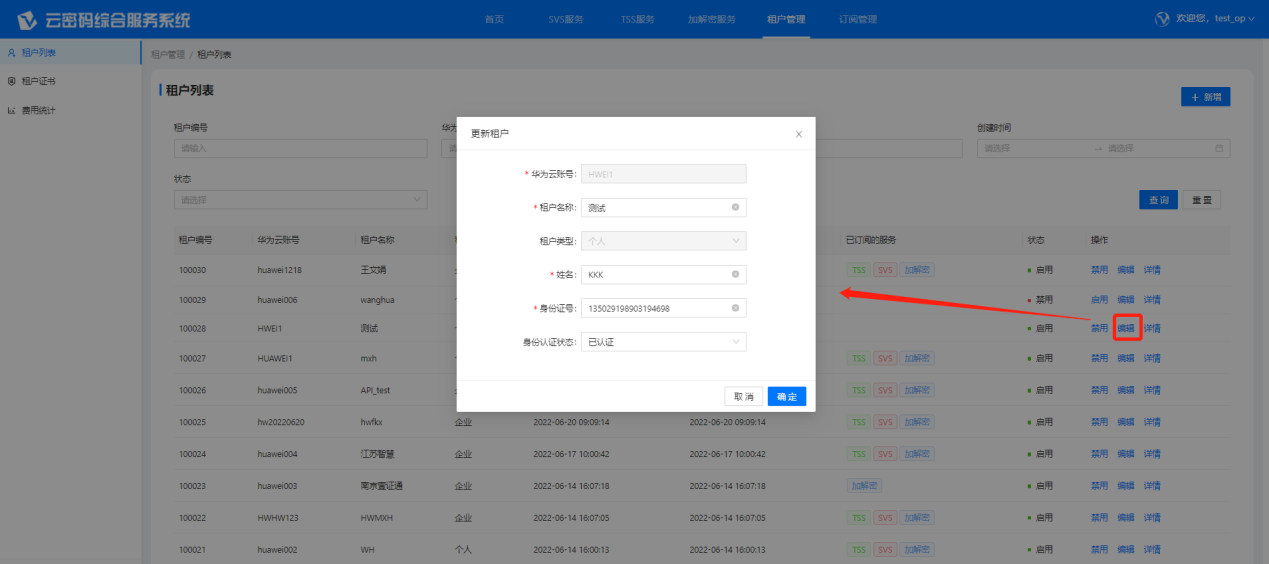
填写好新增租户的表单信息后，点击确定即可新增租户。新增租户成功后，系统会为租户签发一个租户证书，可在租户证书查看。

2、点击操作中的【禁用/启用】按钮，可以启用或禁用该租户，如下图所示：



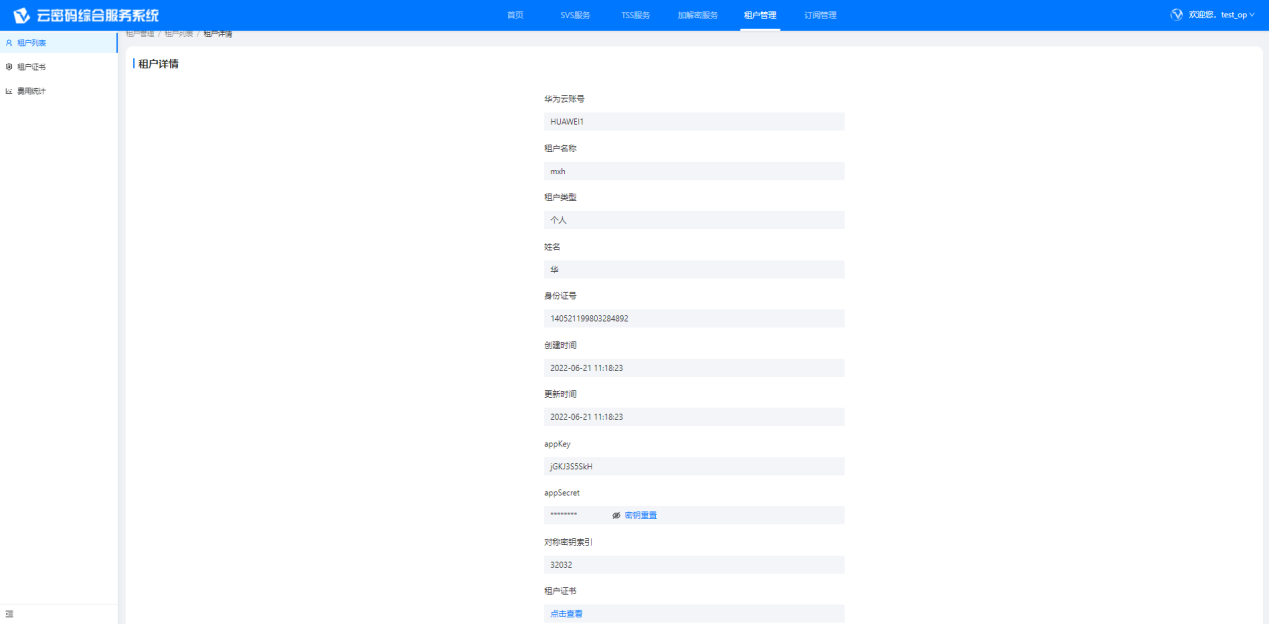
>> 点击禁用后，该租户订阅的所有服务被禁用，不可调用；

1. 点击操作中的【编辑】按钮，可以对已添加的租户进行编辑操作，如下图所示：



>>编辑操作同“新增”操作，详见“新增”租户操作步骤和描述；

1. 点击操作中的【详情】按钮，可查看租户的详细信息，如下图所示：



>> 页面展示该租户详情，主要包括华为云账号、租户名称、租户类型、公司名称/姓名、统一社会信用代码/身份证号、创建时间、更新时间、appkey、appSeret、对称密钥索引、租户证书；

>> 点击详情页面中的【密钥重置】按钮，可重置密钥。重置后将可能导致原有的功能不可用；

>> 点击详情页面中的租户证书下的【点击查看】按钮，可以查看租户证书。

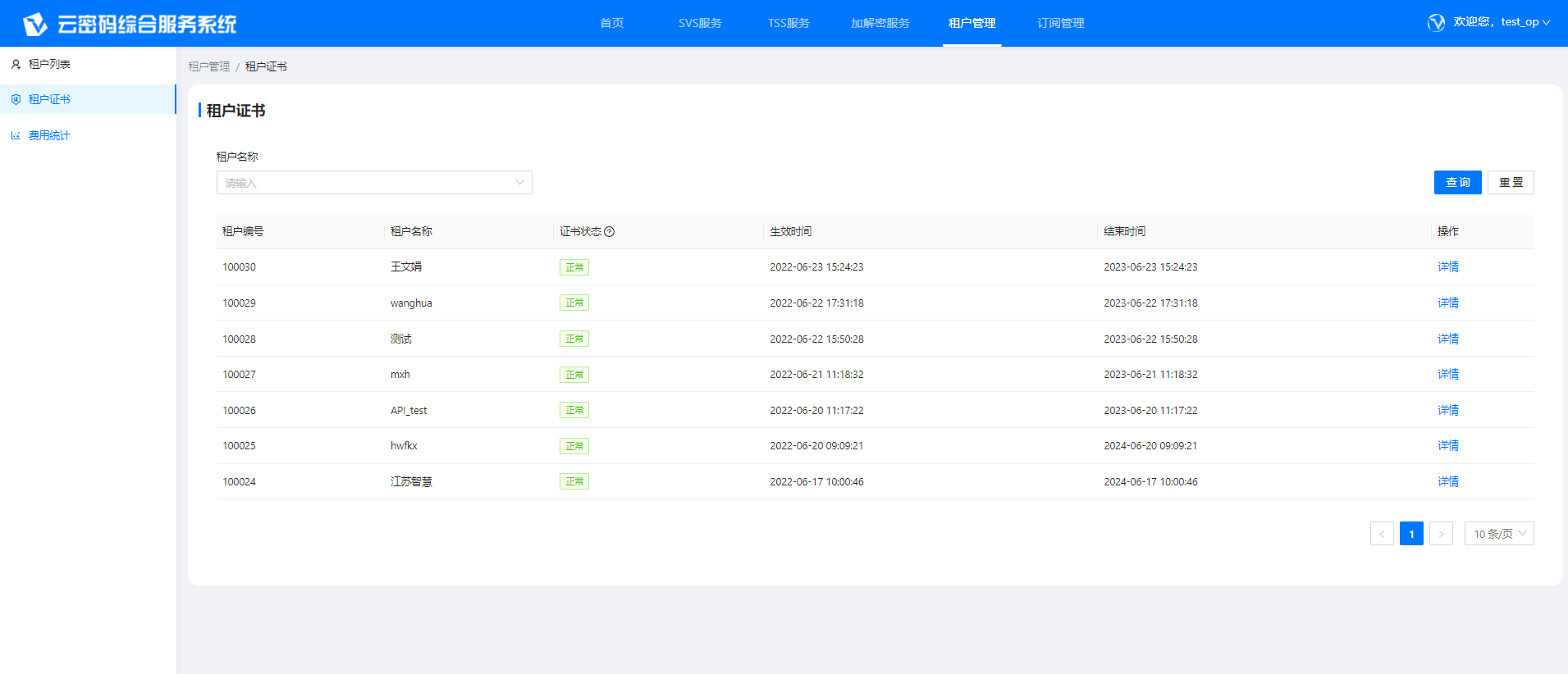
### 2.4.2租户证书

#### 2.4.2.1功能介绍

租户证书主要展示新增租户时默认签发的双证书，即租户证书。

#### 2.4.2.2操作步骤

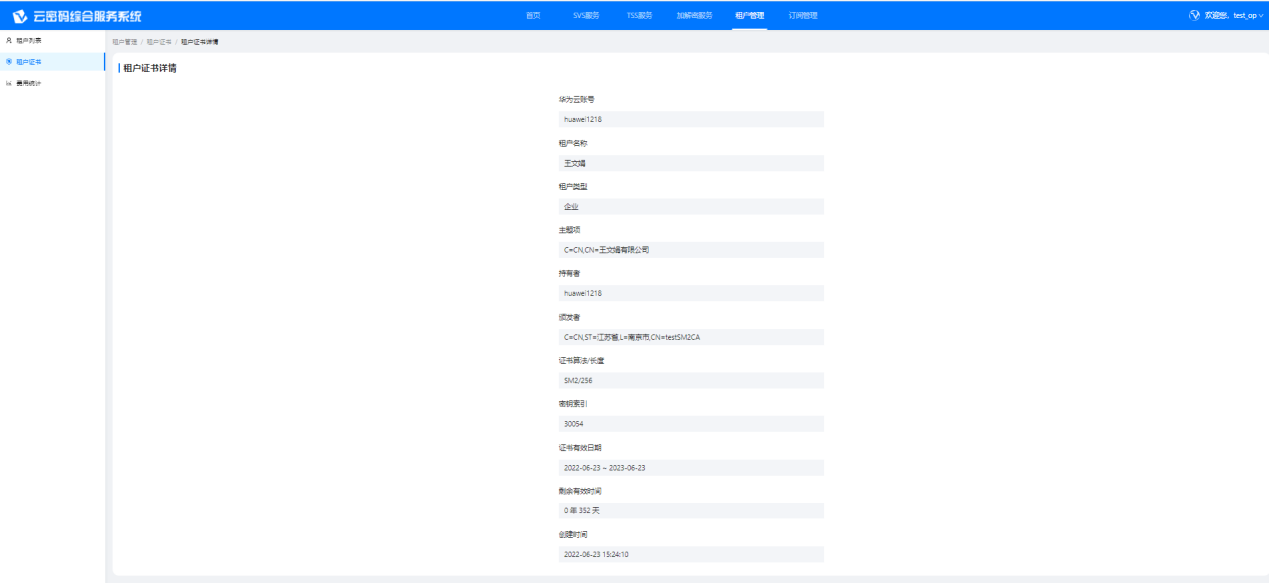
点击菜单〖租户管理〗-〖租户证书〗，进入租户证书页面，如下图所示：



>> 页面展示所有租户证书的信息，包含租户编号、租户名称、证书状态、生效时间、结束时间和操作。

>> 可以根据“租户名称”查询项来查询操作日志信息。

1、点击操作中的【详情】按钮，可查看租户证书的详细信息，如下图所示：



>> 页面展示该租户证书详情，主要包括华为云账号、租户名称、租户类型、主题项、持有者、颁发者、证书算法/长度、密钥索引、证书有效日期、剩余有效时间、创建时间；

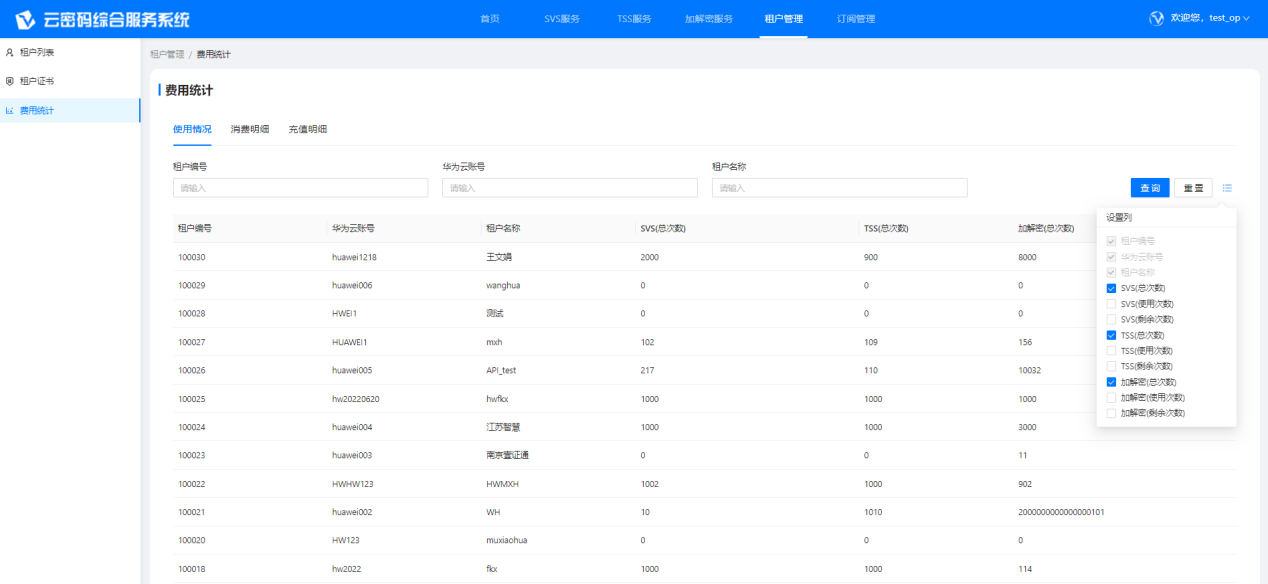
### 2.4.3费用统计

#### 2.4.3.1功能介绍

费用统计主要对使用情况、消费明细和充值明细进行统计查询。

#### 2.4.3.2操作步骤

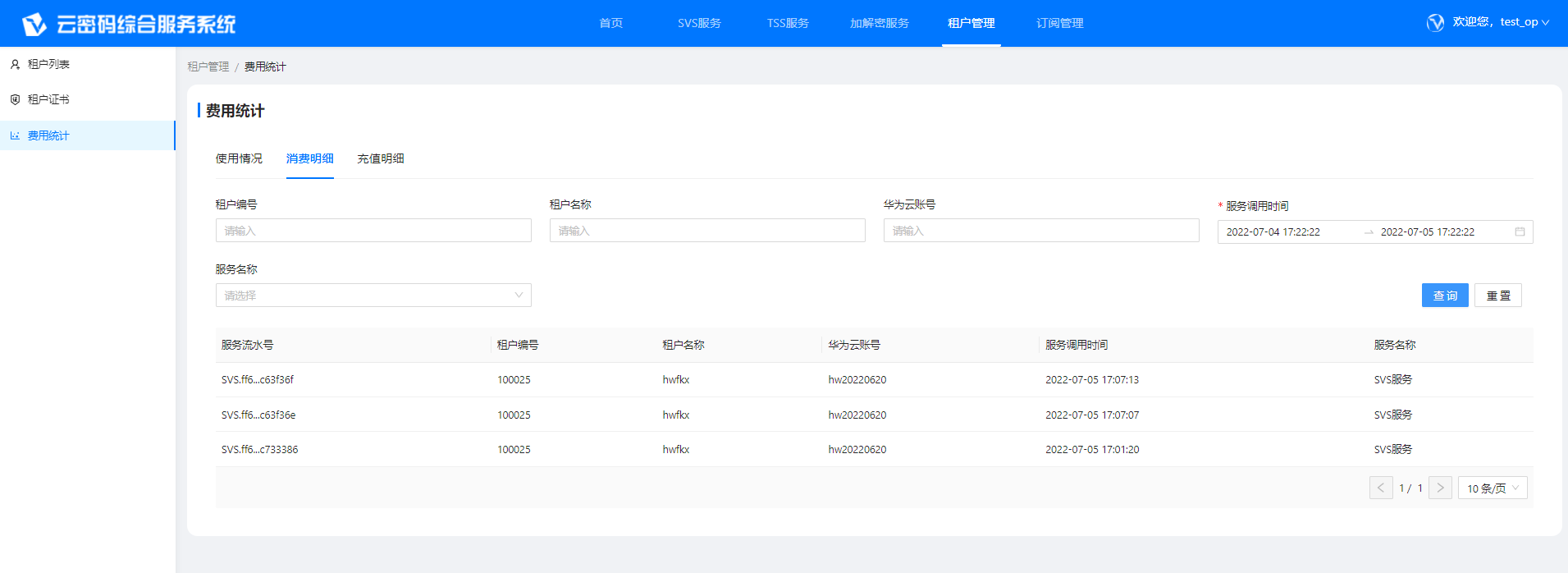
点击菜单〖系统设置〗-〖租户管理〗-〖费用统计〗，进入费用统计页面，如下图所示：



>> 使用情况页面展示所有使用情况统计的信息，包含租户编号、华为云账号、租户名称、SVS（总次数）、TSS（总次数）、加解密（总次数）。可点击重置按钮后面的设置列按钮，增加展示其他项目的统计信息；

>> 可以根据“租户编号”、“华为云账号”、“租户名称”查询项来查询操作日志信息。

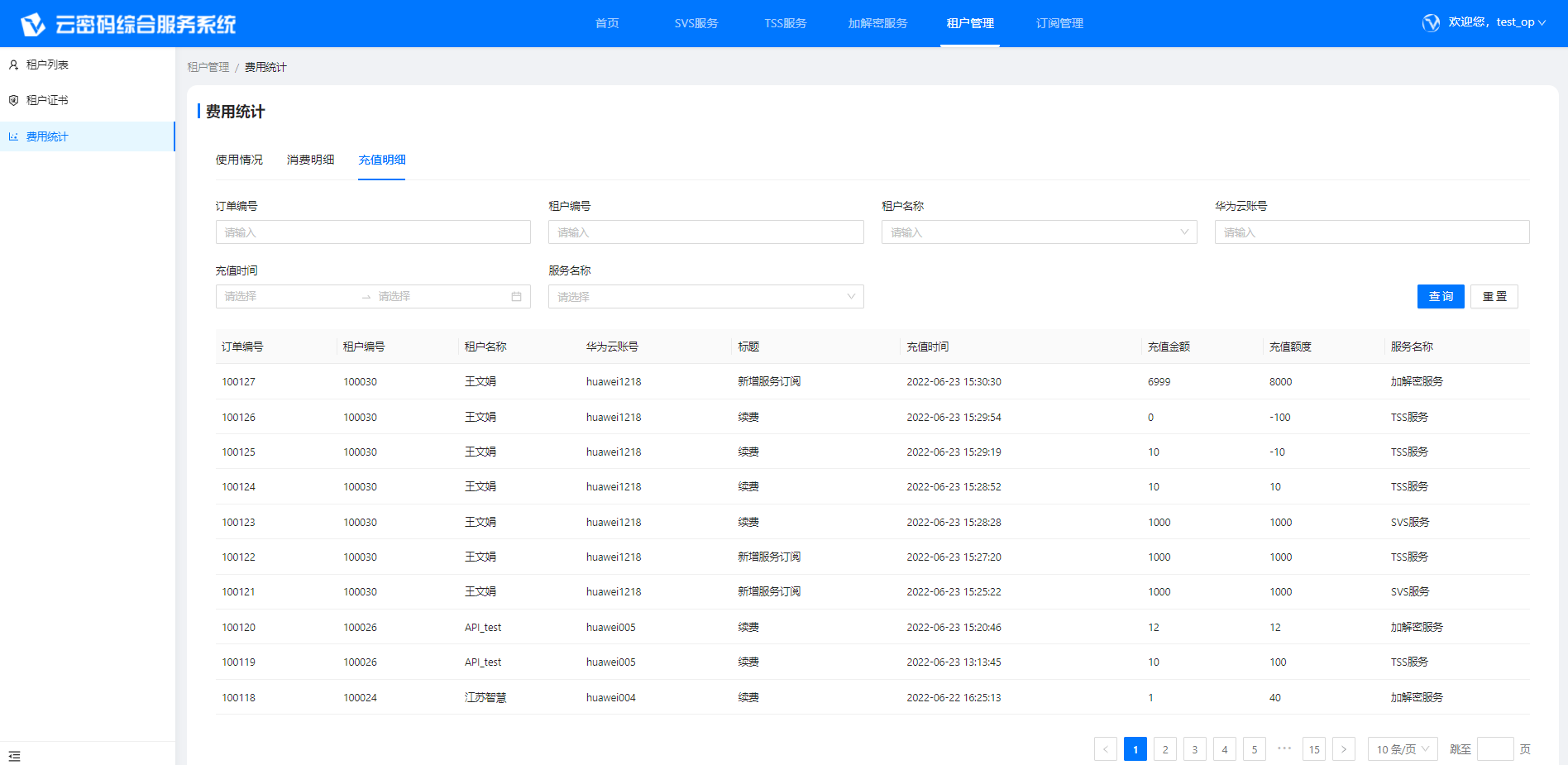
1. 点击页面的【消费明细】按钮，查看消费明细，如下图所示：



>> 消费明细页面展示所有消费明细的信息，包含服务流水号、租户编号、租户名称、华为云账号、服务调用时间、服务名称；

>> 可以根据“租户编号”、“租户名称”、“华为云账号”、“服务调用时间”查询项来查询操作日志信息。

1. 点击页面的【充值明细】按钮，查看消费明细，如下图所示：



>> 充值明细页面展示充值明细的信息，包含订单编号、租户编号、租户名称、华为云账号、标题、充值时间、充值金额、充值额度和服务名称；

>> 可以根据“订单编号”、“租户编号”、“租户名称”、“华为云账号”、“充值时间”、“服务名称”查询项来查询操作日志信息。

## 2.5订阅管理

系统操作员拥有订阅管理菜单权限。

### 2.5.1订阅服务

#### 2.5.1.1功能介绍

订阅服务主要对租户的订阅服务信息数据进行新增和维护，内容服务包括：SVS服务、TSS服务、加解密服务。

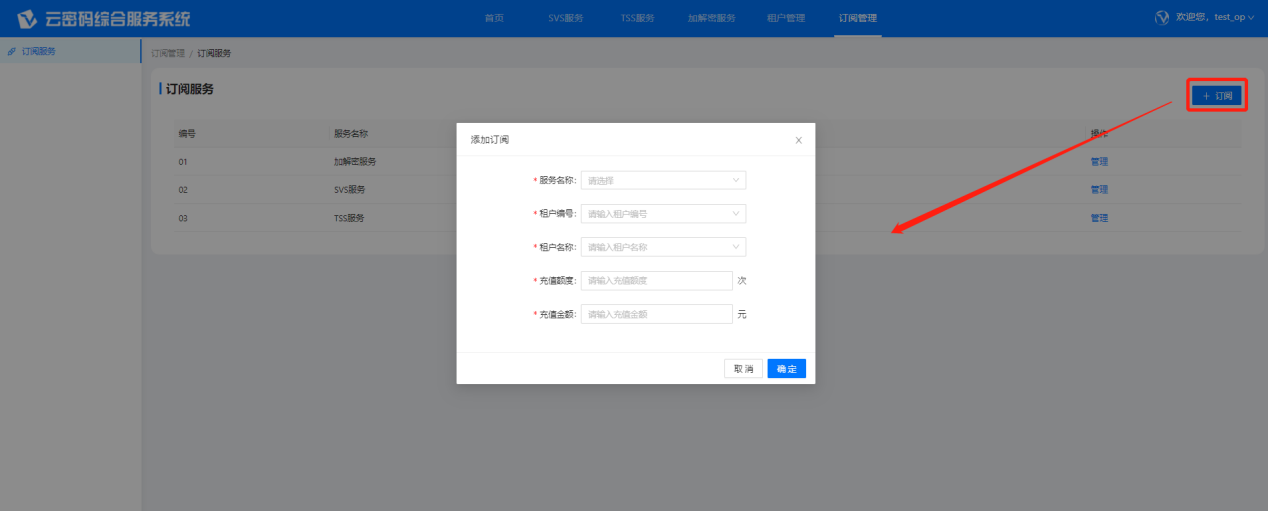
#### 2.5.1.2操作步骤

点击菜单〖订阅管理〗-〖订阅服务〗，进入订阅服务页面，如下图所示：



>> 页面展示订阅服务的信息，包含编号、服务名称、已订阅（用户数）和操作；

1. 点击页面的【订阅】按钮，为租户订阅服务，如下图所示：



>> “**服务名称**”用于选择服务，包含SVS服务、TSS服务、加解密服务；

>> “**租户编号**”用于输入租户编号，输入编号后，系统自动匹配租户名称；

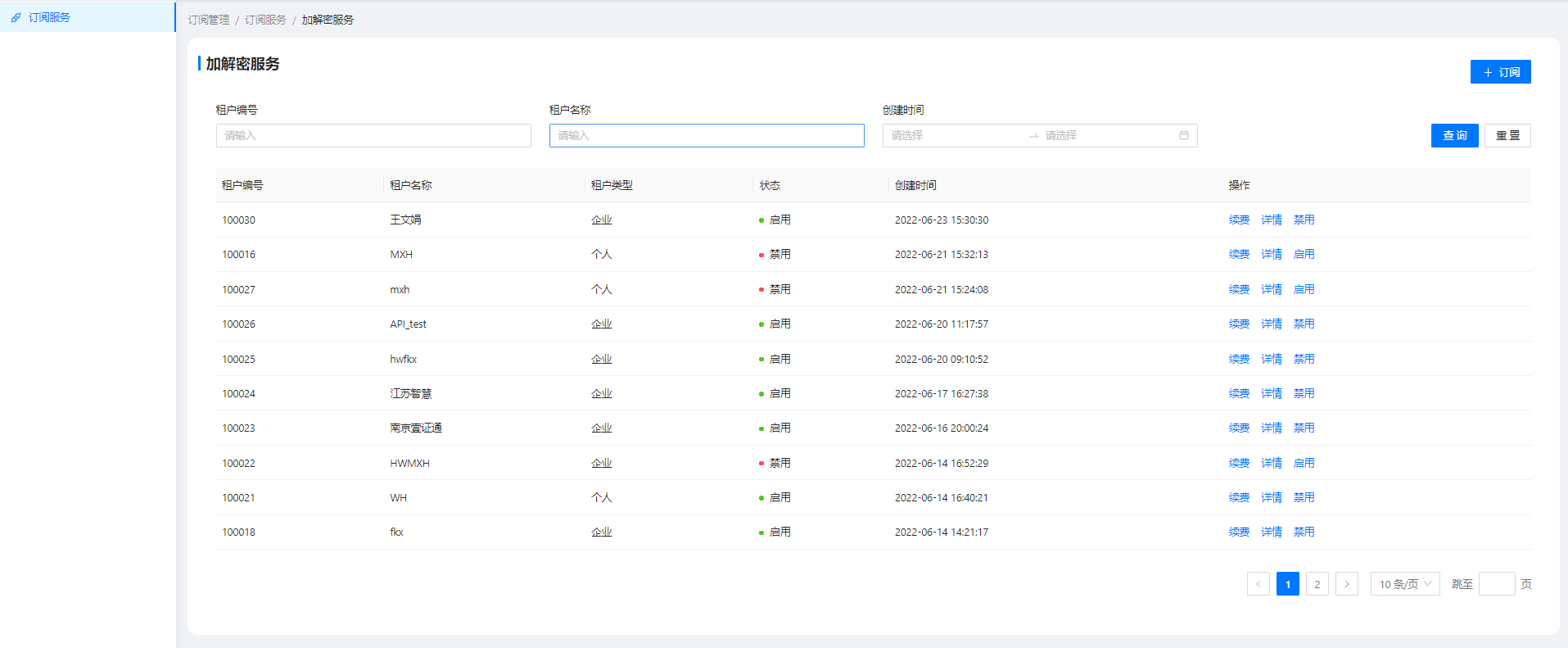
>> “**租户名称**”用于输入租户名称，输入名称后，系统自动匹配租户编号；

>> “**充值额度**”用于输入充值额度，单位：次。充值额度支持正负数（设置负数是为防止操作员操作失误，可逆向修改充值额度）；

>> “**充值金额**”用于输入充值金额，单位：元；

添加订阅表单填写好后，点击确定即可为租户订阅服务。订阅记录可在相应的单个订阅服务页面查看。

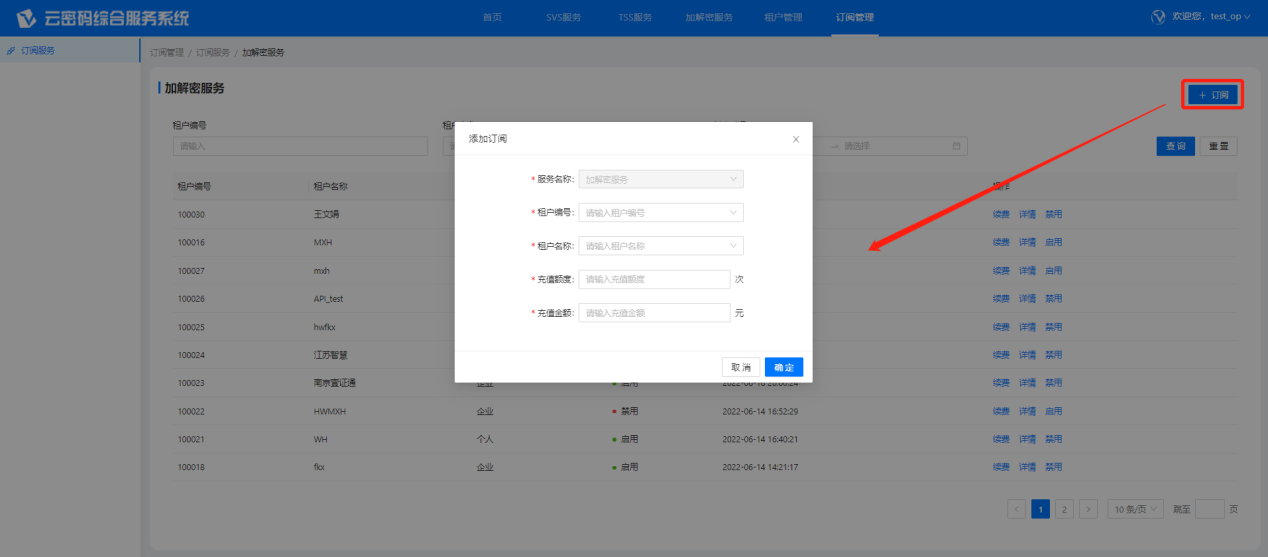
1. 点击页面的【管理】按钮，进入加解密服务页面，如下图所示：



>> 页面展示订阅加解密服务的信息，包含租户编号、租户名称、租户类型、状态、创建时间和操作；

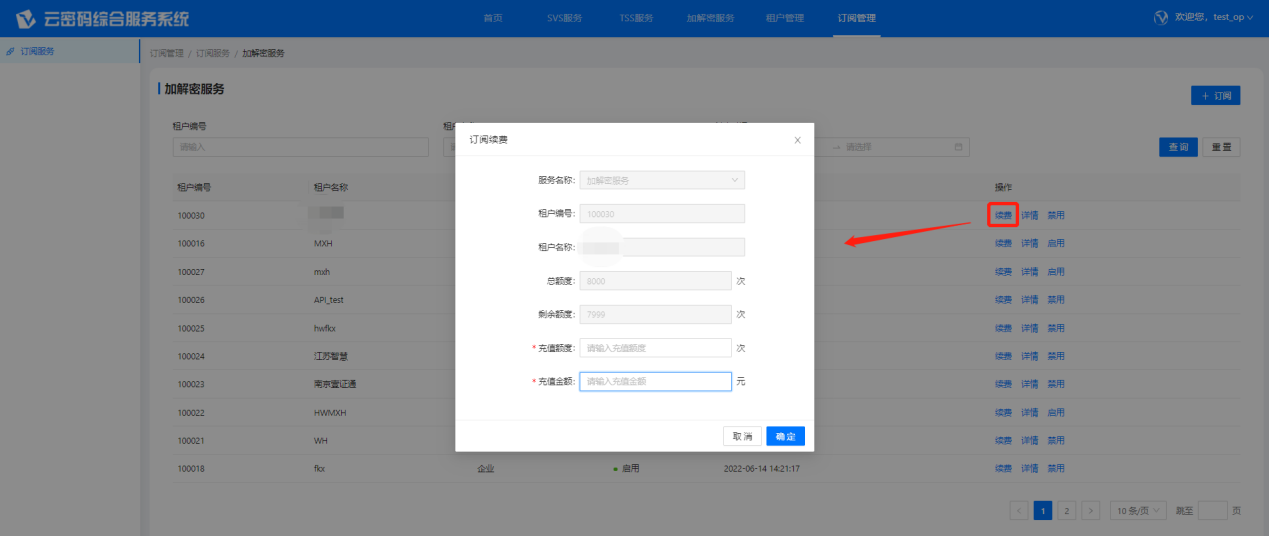
>> 可以根据“租户编号”、“租户名称”、“创建时间”查询项来查询操作。

1. 点击页面的【订阅】按钮，进入添加订阅页面，如下图所示：



>> 订阅操作同订阅服务页面的订阅操作，详细描述请见“订阅服务”操作步骤和描述；

1. 点击页面的【续费】按钮，进入订阅续费页面，如下图所示：



>> 订阅续费页面可对充值额度和充值金额进行修改，点击确定即续费成功；

1. 点击页面的【详情】按钮，进入加解密服务详情页面，如下图所示：



>> 页面展示该加解密服务详情，主要包括服务名称、租户编号、租户名称、租户类型、创建时间、访问限额；

1. 点击页面的【禁用/启用】按钮，可以启用和禁用该租户的加解密服务，如下图所示：



>> 点击禁用后，该租户的加解密服务被禁用，无法调用；

SVS服务和TSS服务页面的操作同加解密服务，详细描述请见“加解密服务”描述和操作

## 2.6 SVS服务

系统操作员拥有SVS服务菜单权限。

### 2.6.1在线测试

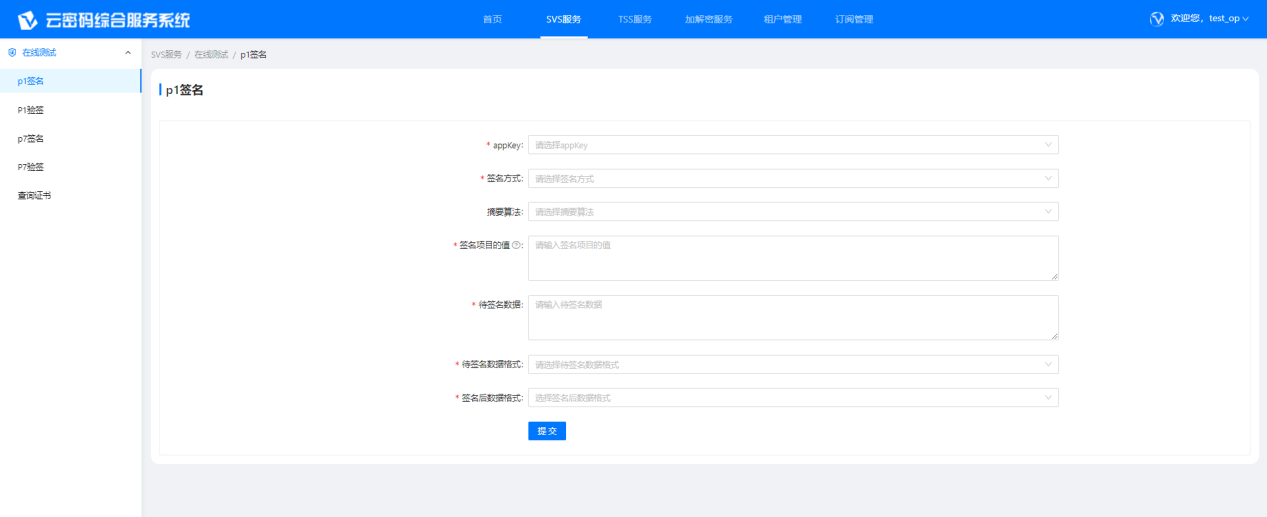
#### 2.6.1.1 P1签名

##### 2.6.1.1.1功能介绍

P1签名用于对某数据进行P1签名操作。

##### 2.6.1.1.2操作步骤

点击菜单〖SVS服务〗-〖在线测试〗-〖P1签名 〗，进入P1签名页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**签名方式**”用于选择具体的签名方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**摘要算法**”仅支持SM3，为可选项；

>> “**签名项目的值**”用于输入选择的签名方式的具体值；

>> “**待签名数据**”用于输入待签名的数据；

>> “**待签名数据格式**”用于选择待签名数据的格式，包含原文、原文BASE64、原文HEX、摘要BASE64、摘要HEX；

>> “**签名后数据格式**”用于选择签名后的签名值的数据格式，包含BASE64、HEX；

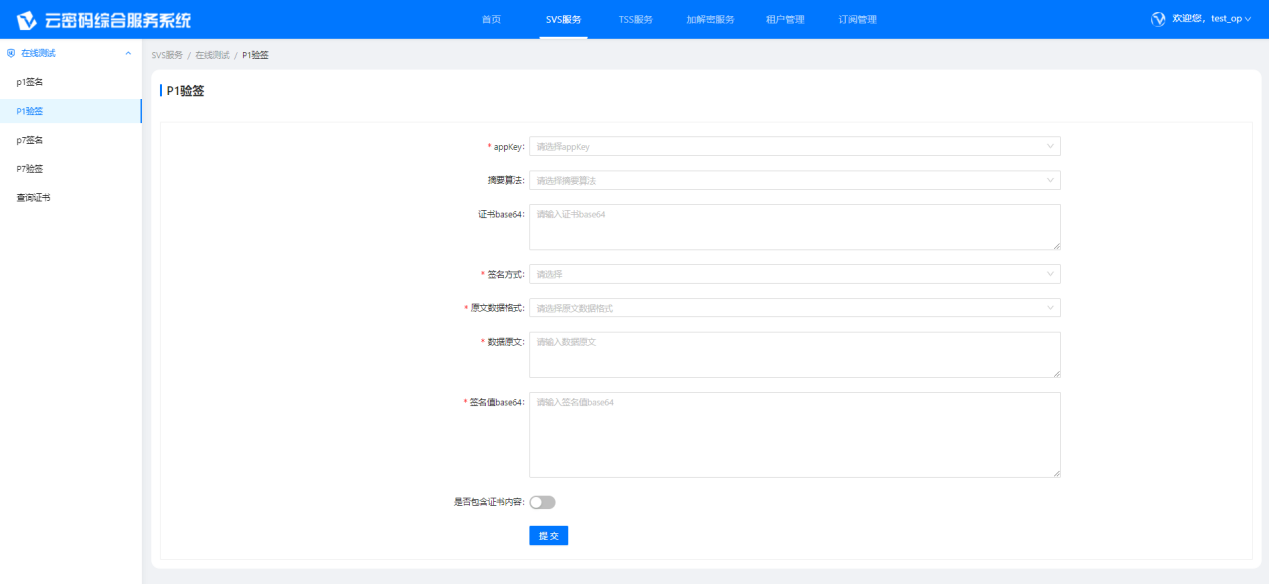
#### 2.6.1.2 P1验签

##### 2.6.1.2.1功能介绍

P1验签用于对P1签名值进行验证。

##### 2.6.1.2.2操作步骤

点击菜单〖SVS服务〗-〖在线测试〗-〖P1验签〗，进入P1验签页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**摘要算法**”仅支持SM3，为可选项；

>> “**证书BASE64**”用于输入租户的签名证书（BASE64格式），为可选项；

>> “**签名方式**”用于选择具体的验证签名方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**原文数据格式**”用于选择原文数据格式，包含原文、原文BASE64、原文HEX；

>> “**数据原文**”用于输入数据原文，即待签名数据；

>> “**签名值BASE64**”用于输入P1签名后的签名值（BASE64格式）；

>> “**是否包含证书内容**”用于选择响应中是否包含证书内容，为可选项；

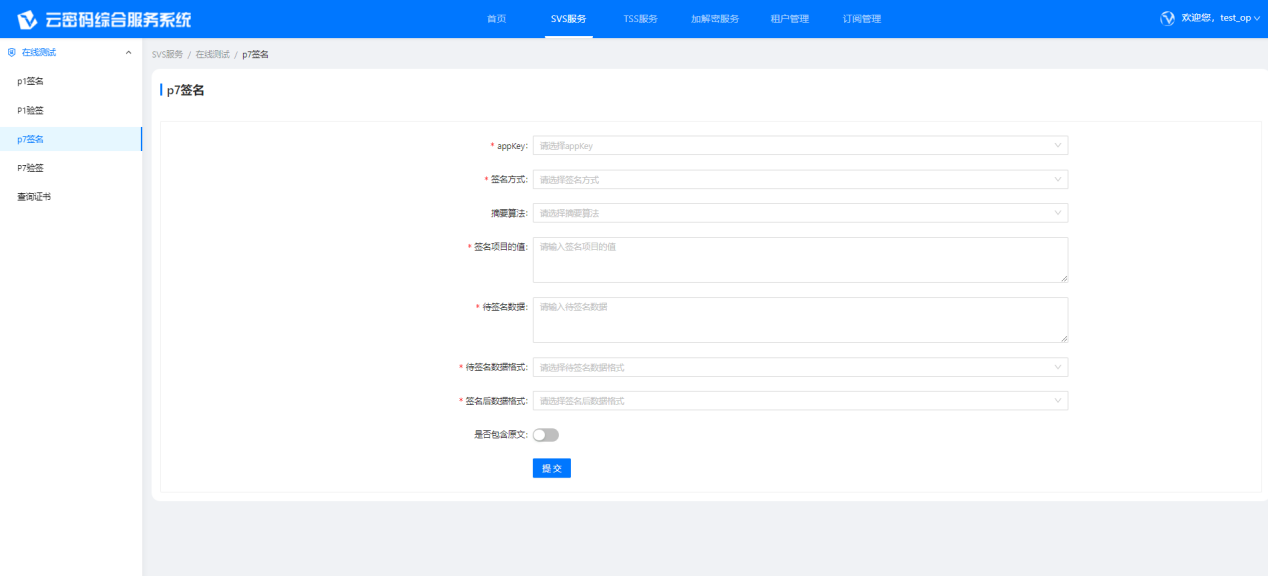
#### 2.6.1.3 P7签名

##### 2.6.1.3.1功能介绍

P7签名用于对某数据进行P7签名操作。

##### 2.6.1.3.2操作步骤

点击菜单〖SVS服务〗-〖在线测试〗-〖P7签名 〗，进入P7签名页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**签名方式**”用于选择具体的签名方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**摘要算法**”仅支持SM3，为可选项；

>> “**签名项目的值**”用于输入选择的签名方式的具体值；

>> “**待签名数据**”用于输入待签名的数据；

>> “**待签名数据格式**”用于选择待签名数据的格式，包含原文、原文BASE64、原文HEX；

>> “**签名后数据格式**”用于选择签名后的签名值的数据格式，包含BASE64、HEX；

>> “**是否包含原文**”用于选择签名中是否包含原文，为可选项；

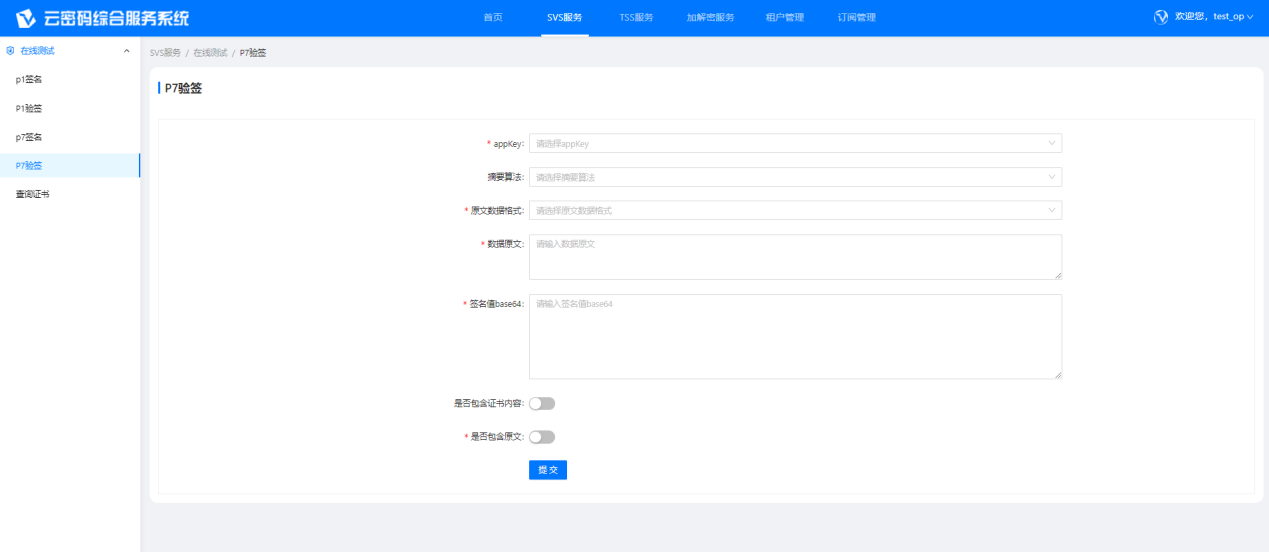
#### 2.6.1.4 P7验签

##### 2.6.1.4.1功能介绍

P7验签用于对P7签名值进行验证。

##### 2.6.1.4.2操作步骤

点击菜单〖SVS服务〗-〖在线测试〗-〖P7验签〗，进入P7验签页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**摘要算法**”仅支持SM3，为可选项；

>> “**原文数据格式**”用于选择原文数据格式，包含原文、原文BASE64、原文HEX；

>> “**数据原文**”用于输入数据原文，即待签名数据；

>> “**签名值BASE64**”用于输入P7签名后的签名值（BASE64格式）；

>> “**是否包含证书内容**”用于选择响应中是否包含证书内容，为可选项；

>> “**是否包含原文**”用于选择签名结果中是否包含原文；

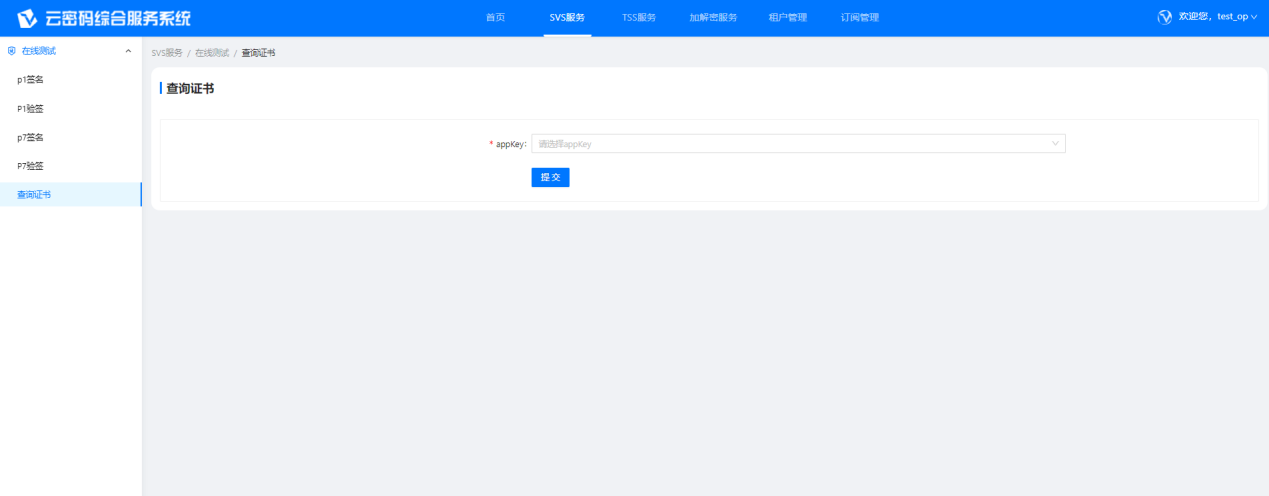
#### 2.6.1.5 查询证书

##### 2.6.1.5.1功能介绍

查询证书用于查询租户证书和时间戳证书，获得具体的证书信息。

##### 2.6.1.5.2操作步骤

点击菜单〖SVS服务〗-〖在线测试〗-〖查询证书〗，进入查询证书页面，如下图所示：



>> 选择租户应用的appkey后，点击提交即可查询到相应的租户证书和时间戳证书；

## 2.7 TSS服务

系统操作员拥有TSS服务菜单权限。

### 2.7.1在线测试

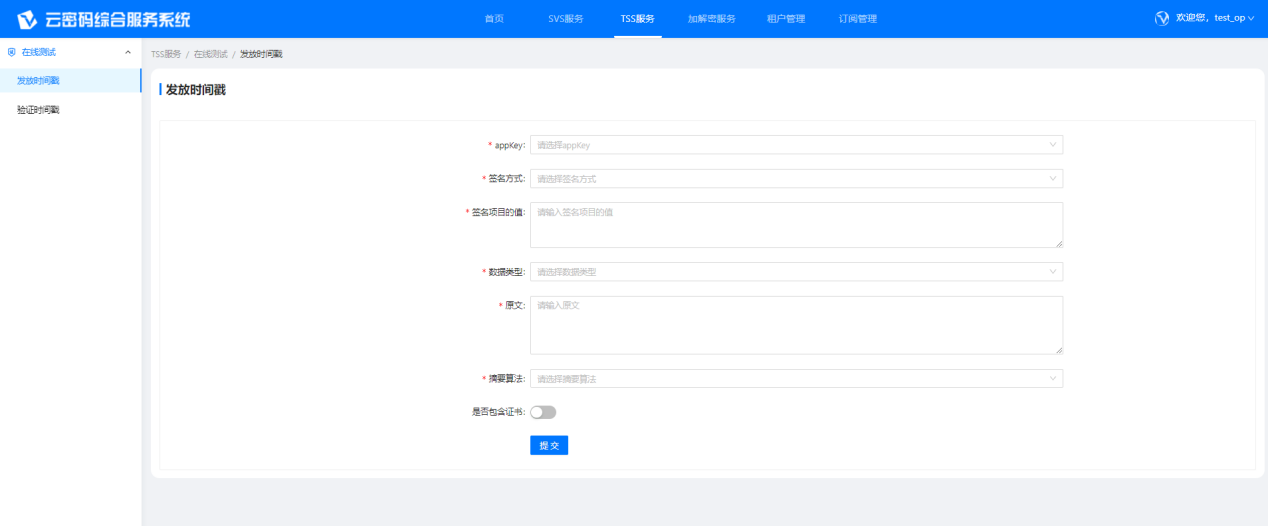
#### 2.7.1.1发放时间戳

##### 2.7.1.1.1功能介绍

发放时间戳用于时间戳的发放。

##### 2.7.1.1.2操作步骤

点击菜单〖TSS服务〗-〖在线测试〗-〖发放时间戳〗，进入发放时间戳页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**签名方式**”用于选择具体的签名方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**签名项目的值**”用于输入选择的签名方式的具体值；

>> “**数据类型**”用于选择原文数据格式，包含原文、原文BASE64、原文HEX、摘要BASE64、摘要HEX；

>> “**原文**”用于输入数据原文，即待签名数据；

>> “**摘要算法**”仅支持SM3；

>> “**是否包含证书**”用于选择时间戳中是否包含证书，为可选项；

#### 2.7.1.2验证时间戳

##### 2.7.1.2.1功能介绍

验证时间戳用于时间戳的验证。

##### 2.7.1.2.2操作步骤

点击菜单〖TSS服务〗-〖在线测试〗-〖验证时间戳〗，进入发放时间戳页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**数据类型**”用于选择原文数据格式，包含原文、原文BASE64、原文HEX、摘要BASE64、摘要HEX；

>> “**原始数据**”用于输入数据原文，即待签名数据；

>> “**时间戳**”用于输入发放的时间戳；

## 2.8 加解密服务

系统操作员拥有加解密服务菜单权限。

### 2.8.1在线测试

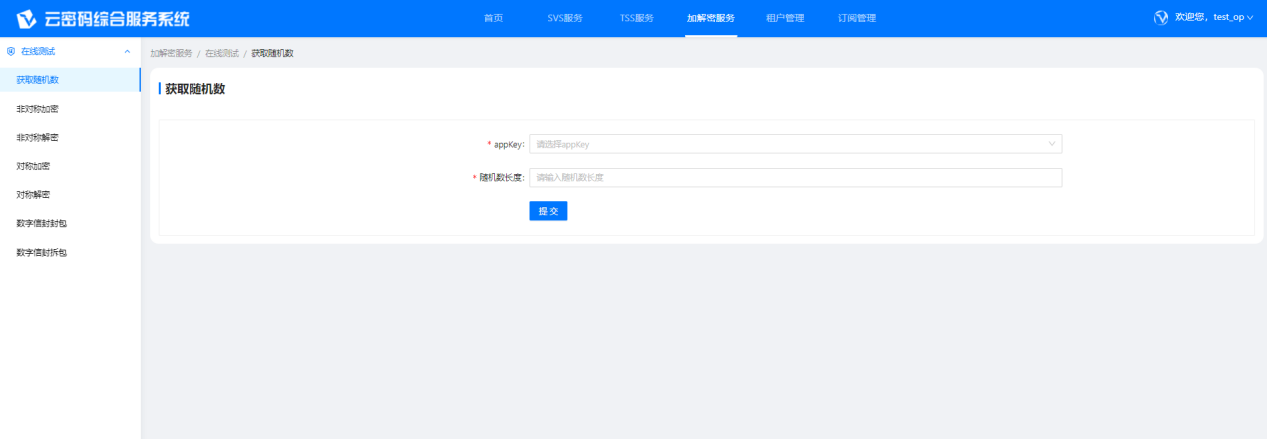
#### 2.8.1.1获取随机数

##### 2.8.1.1.1功能介绍

获取随机数用于获取随机数。

##### 2.8.1.1.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖获取随机数〗，进入获取随机数页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**随机数长度**”用于输入随机数的长度；

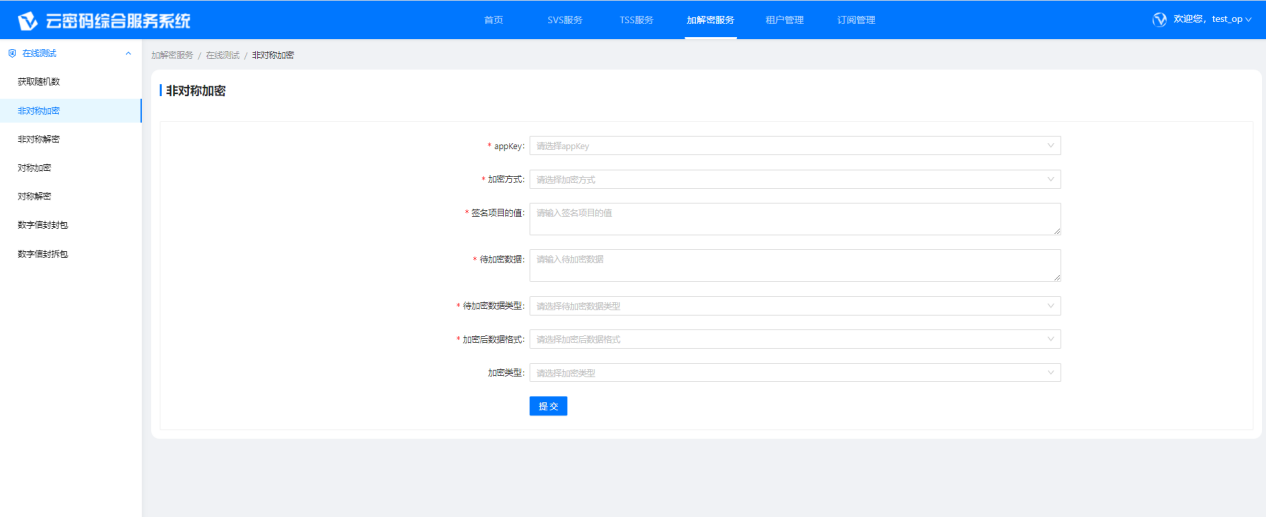
#### 2.8.1.2非对称加密

##### 2.8.1.2.1功能介绍

非对称加密用于对待加密数据进行公钥加密。

##### 2.8.1.2.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖非对称加密〗，进入获非对称加密页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**加密方式**”用于选择具体的加密方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**签名项目的值**”用于输入选择的加密方式的具体值；

>> “**待加密数据**”用于输入待加密的数据；

>> “**待加密数据类型**”用于选择待加密数据的类型，包含原文、原文BASE64、原文HEX；

>> “**加密后数据格式**”用于选择加密后的加密值的数据格式，包含BASE64、HEX；

>> “**加密类型**”只支持加密秘钥，为可选项

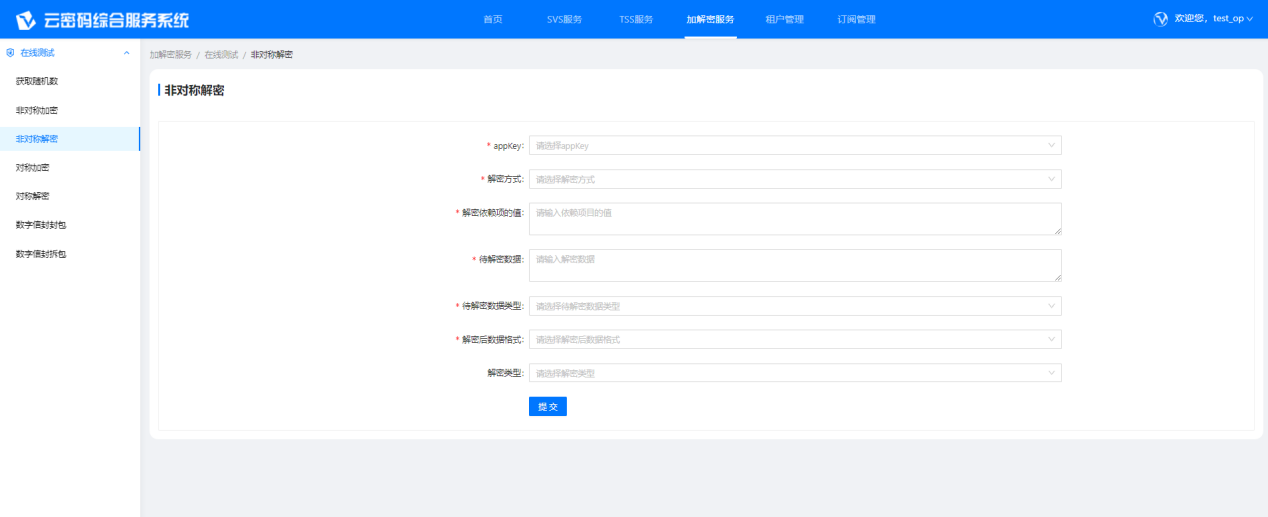
#### 2.8.1.3非对称解密

##### 2.8.1.3.1功能介绍

非对称解密用于对非对称加密数据进行私钥解密。

##### 2.8.1.3.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖非对称解密〗，进入获非对称解密页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**解密方式**”用于选择具体的解密方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**解密依赖项的值**”用于输入选择的解密方式的具体值；

>> “**待解密数据**”用于输入待解密的数据；

>> “**待解密数据类型**”用于选择待解密数据的类型，包含BASE64、HEX；

>> “**解密后数据格式**”用于选择加密后的加密值的数据格式，包含原文、原文BASE64、原文HEX；

>> “**解密类型**”只支持加密秘钥，为可选项

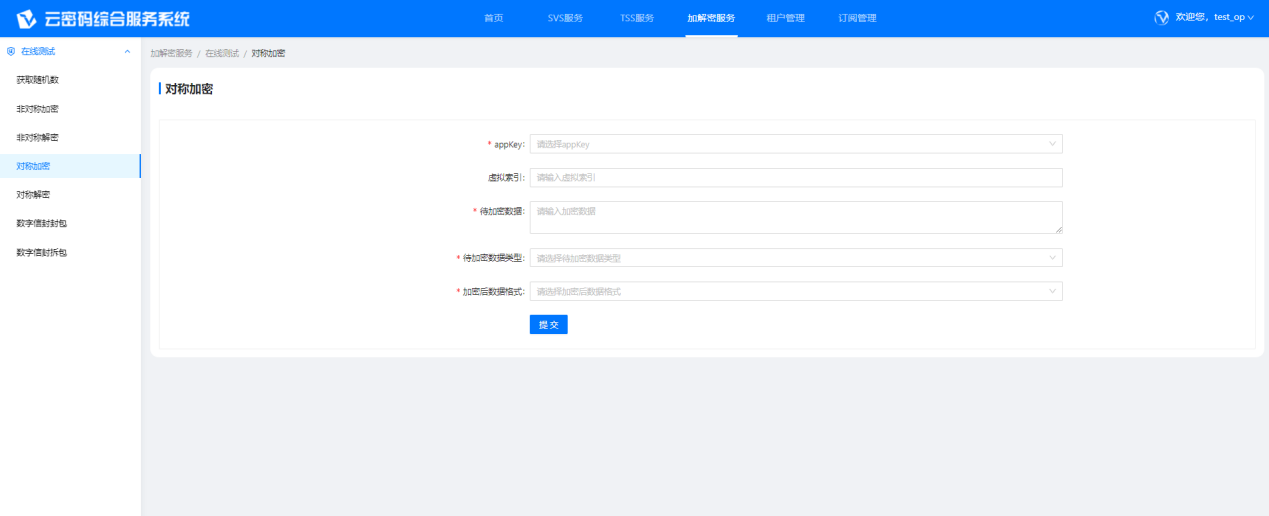
#### 2.8.1.4对称加密

##### 2.8.1.4.1功能介绍

对称加密用于待加密数据进行对称加密。

##### 2.8.1.4.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖对称加密〗，进入获对称加密页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**虚拟索引**”用于输入虚拟索引，为可选项；

>> “**待加密数据**”用于输入待加密的数据；

>> “**待加密数据类型**”用于选择待加密数据的类型，包含原文、原文BASE64、原文HEX；

>> “**加密后数据格式**”用于选择加密后的加密值的数据格式，包含BASE64、HEX；

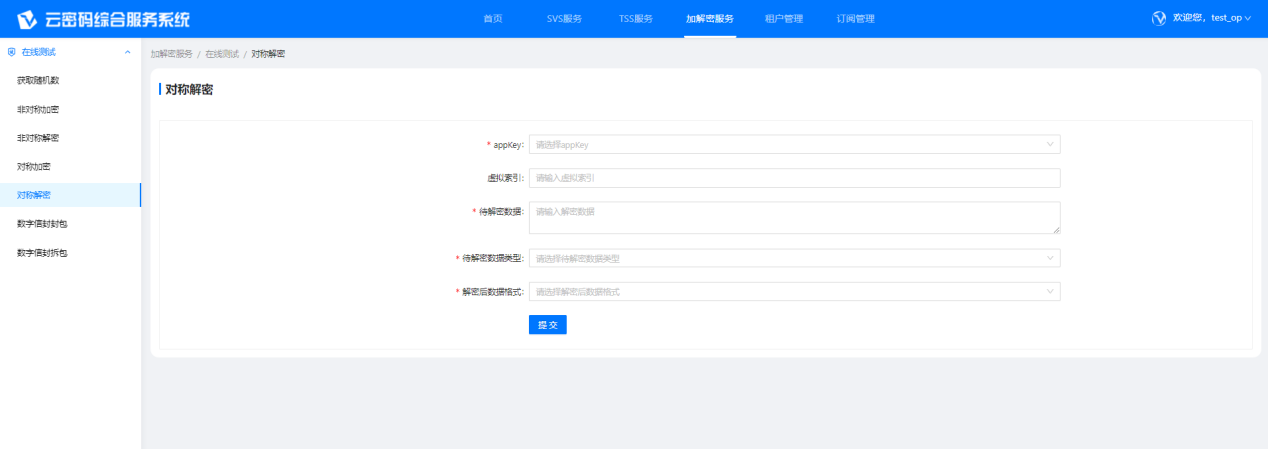
#### 2.8.1.5对称解密

##### 2.8.1.5.1功能介绍

对称解密用于对对称加密数据进行解密。

##### 2.8.1.5.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖对称解密〗，进入获对称解密页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**虚拟索引**”用于输入虚拟索引，为可选项；

>> “**待解密数据**”用于输入待解密的数据；

>> “**待解密数据类型**”用于选择待解密数据的类型，包含BASE64、HEX；

>> “**解密后数据格式**”用于选择解密后的解密值的数据格式，包含原文、原文BASE64、原文HEX；

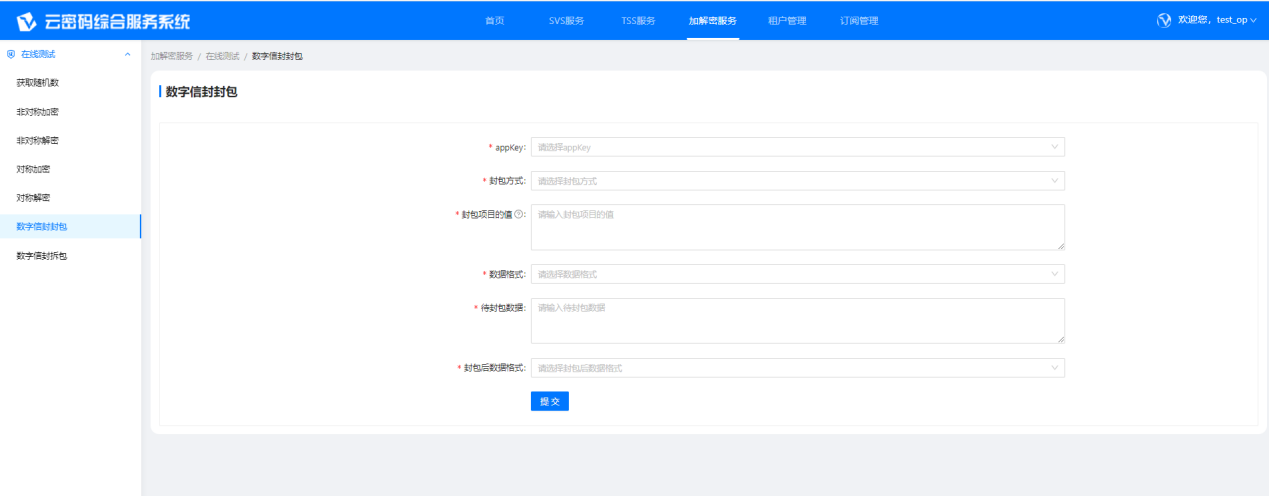
#### 2.8.1.6数字信封封包

##### 2.8.1.6.1功能介绍

数字信封封包用于对数据的数字信封封包。

##### 2.8.1.6.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖数字信封封包〗，进入数字信封封包页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**封包方式**”用于选择具体的封包方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**封包项目的值**”用于输入选择的封包方式的具体值；

>> “**数据格式**”用于选择待封包数据的类型，包含原文、原文BASE64、原文HEX；

>> “**待封包数据**”用于输入待封包的数据；

>> “**封包后数据格式**”用于选择封包后的封包值的数据格式，包含BASE64、HEX；

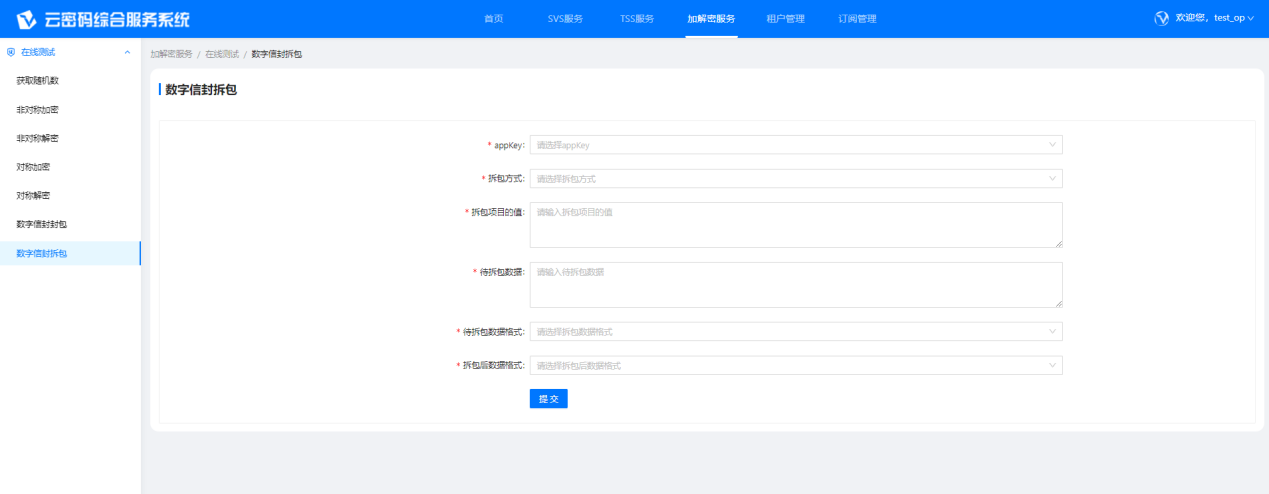
#### 2.8.1.7数字信封拆包

##### 2.8.1.7.1功能介绍

数字信封拆包用于对数字信封封包的数据进行拆包。

##### 2.8.1.7.2操作步骤

点击菜单〖加解密服务〗-〖在线测试〗-〖数字信封拆包〗，进入数字信封拆包页面，如下图所示：



>> “**appkey**”用于选择租户应用的appkey；

>> “**拆包方式**”用于选择具体的拆包方式，包含证书、证书ID、证书CN项、证书主题项、密钥索引、证书序列号（十进制格式）、证书序列号（十六进制格式）、证书指纹；

>> “**拆包项目的值**”用于输入选择的拆包方式的具体值；

>> “**待拆包数据**”用于输入待拆包的数据；

>> “**待拆包数据格式**”用于选择待拆包数据的格式，包含BASE64、HEX；

>> “**拆包后数据格式**”用于选择拆包后的拆包值的数据格式，包含原文、原文BASE64、原文HEX；

## 2.9日志管理

### 2.9.1服务调用日志

系统管理员拥有服务调用日志菜单权限。

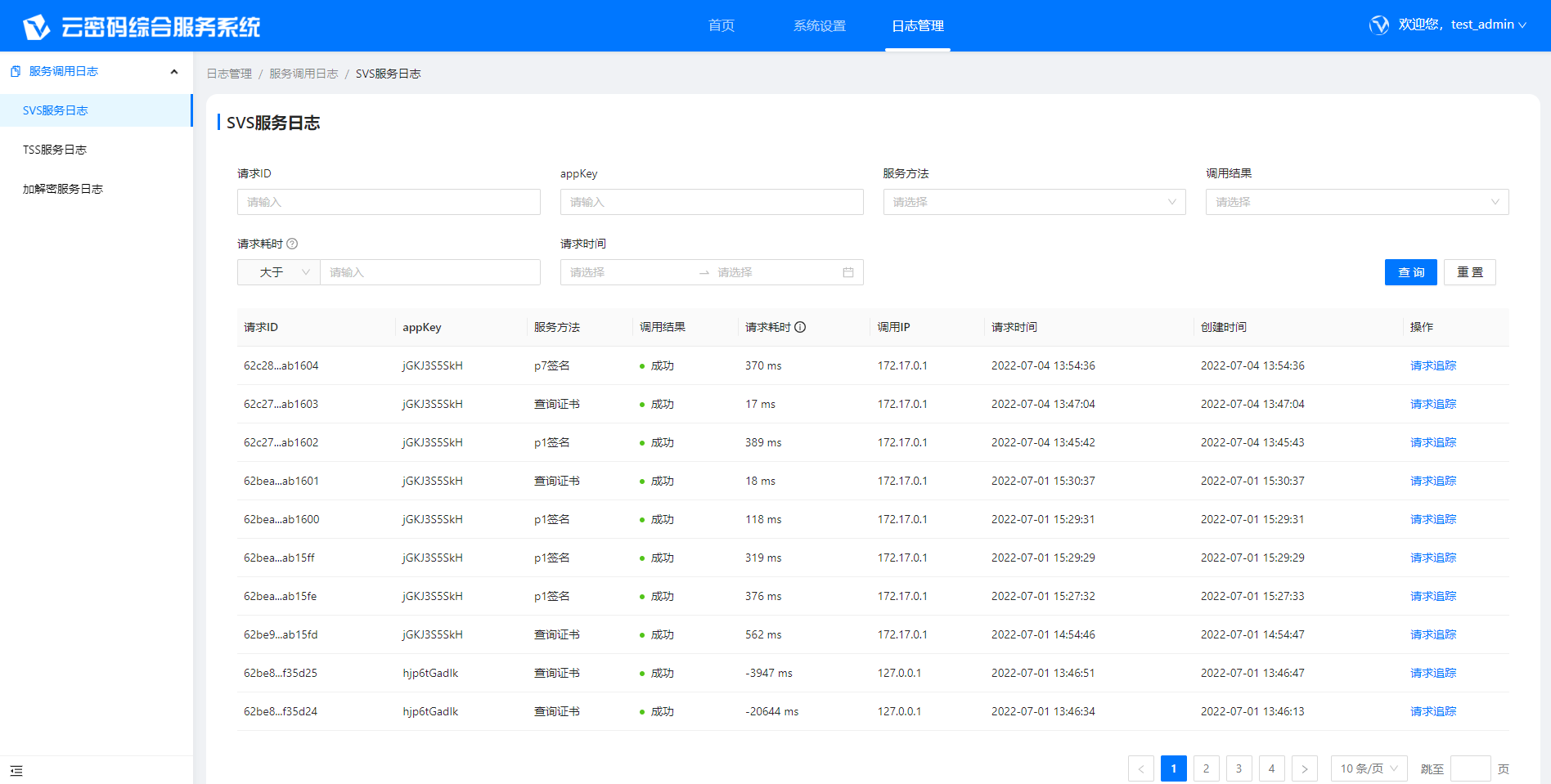
#### 2.9.1.1 SVS服务日志

##### 2.9.1.1.1功能介绍

SVS服务日志主要用于查看SVS服务的调用日志。

##### 2.9.1.1.2操作步骤

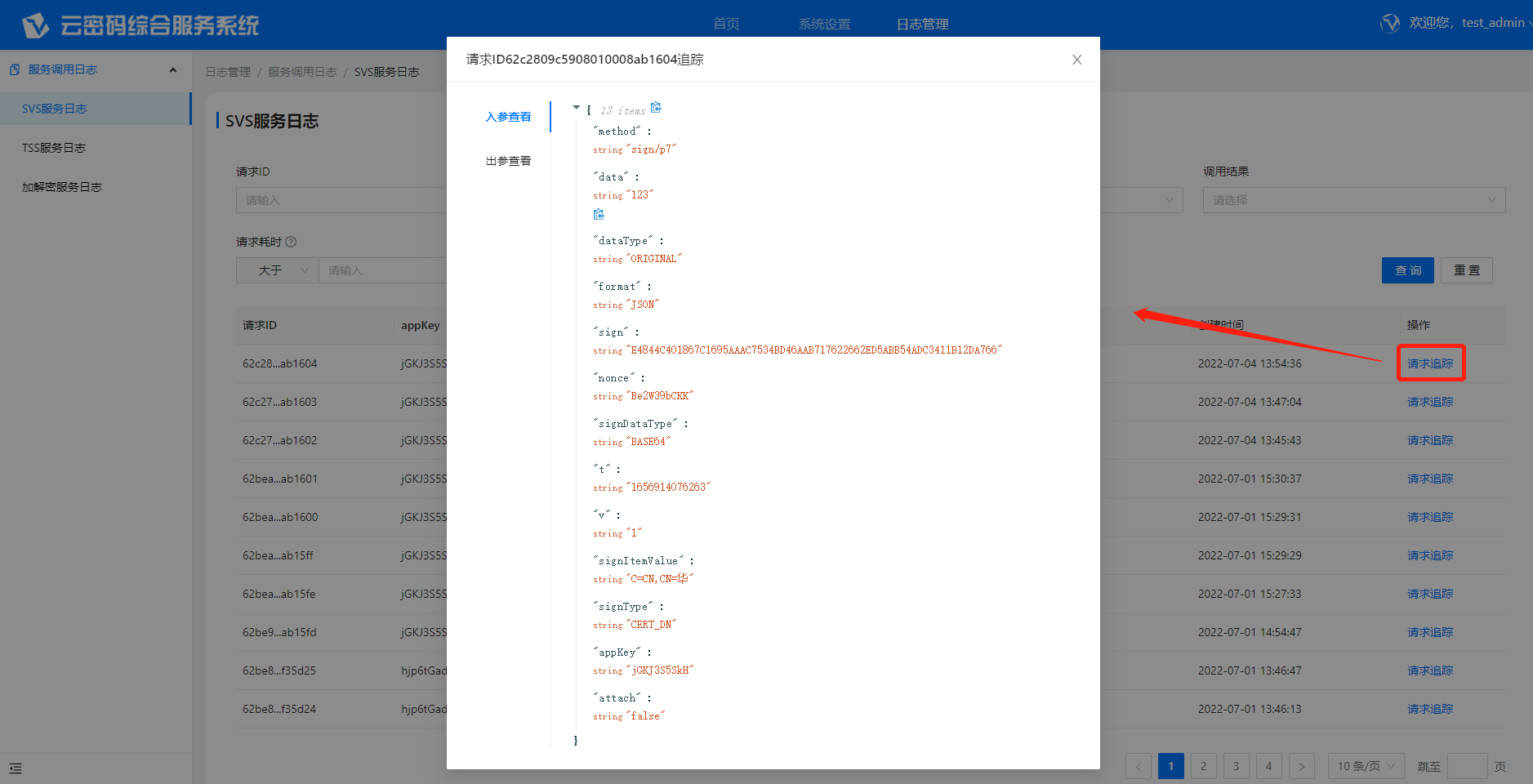
点击菜单〖日志管理〗-〖服务调用日志〗-〖SVS服务日志〗，进入SVS服务日志页面，如下图所示：



>> 页面展示所有SVS服务的调用记录，包含请求ID、appkey、服务方法、调用结果、请求耗时、调用IP、请求时间、创建时间和操作。

>> 管理员可以根据“请求ID”、“appkey”、“服务方法”、“调用结果”“请求耗时”、“请求时间”查询项来查询服务日志信息。

1、点击页面的【请求追踪】按钮，进行入参出参查看，如下图所示：



>> 请求追踪页面详细展示入参和出参的详细信息，可通过查看入参和出参来检查服务调用情况；

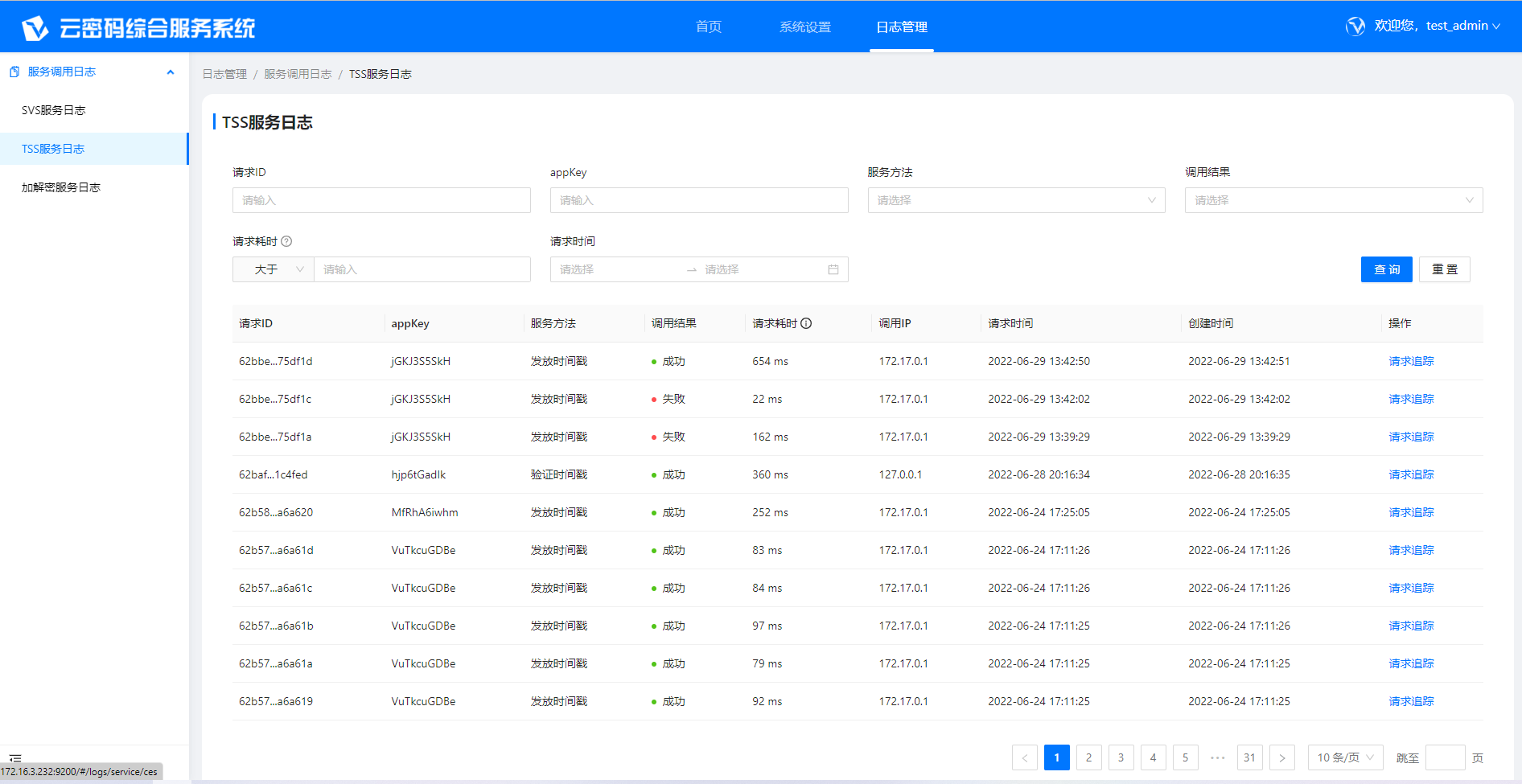
#### 2.9.1.2 TSS服务日志

##### 2.9.1.2.1功能介绍

TSS服务日志主要用于查看TSS服务的调用日志。

##### 2.9.1.2.2操作步骤

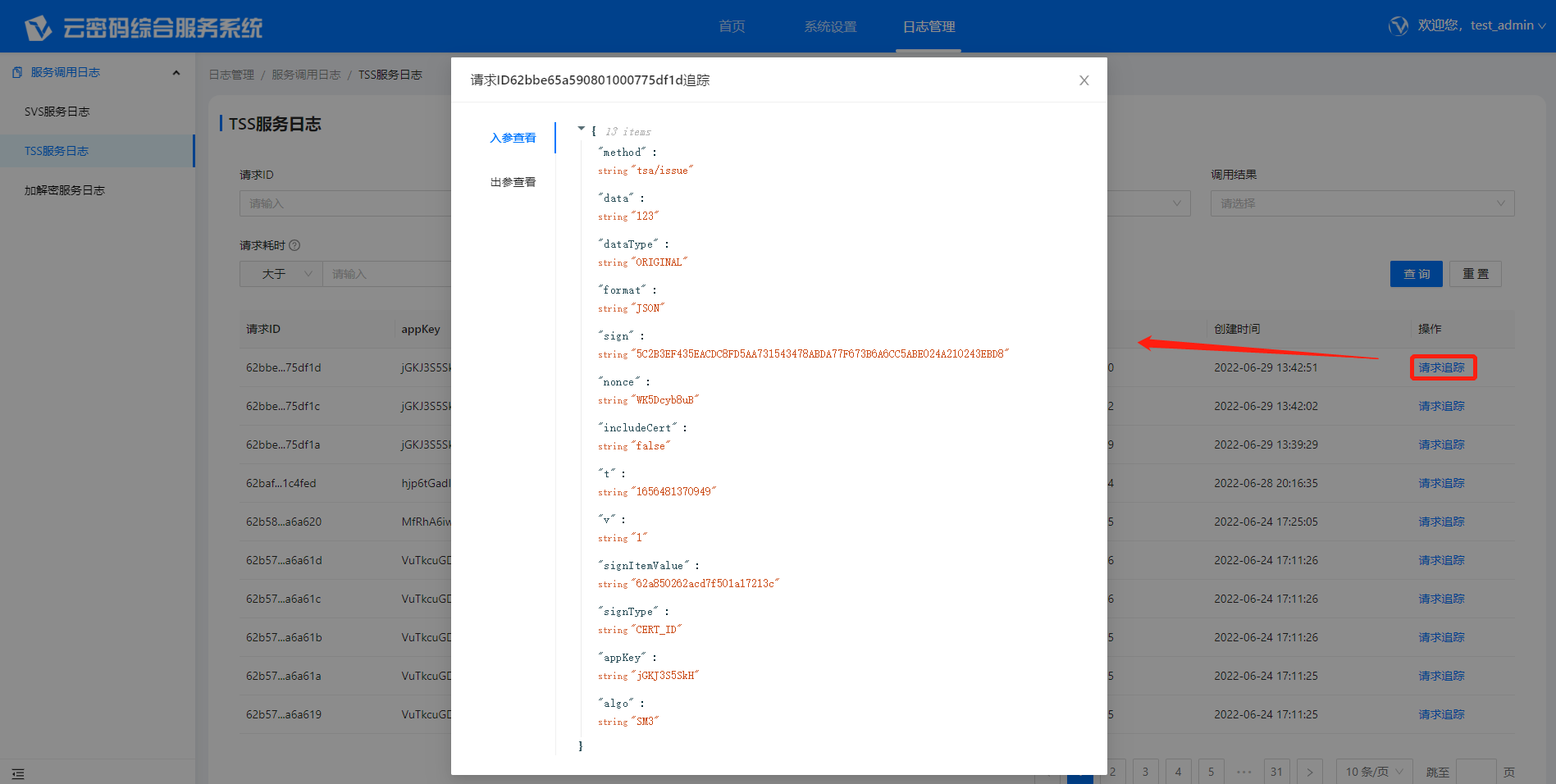
点击菜单〖日志管理〗-〖服务调用日志〗-〖TSS服务日志〗，进入TSS服务日志页面，如下图所示：



>> 页面展示所有TSS服务的调用记录，包含请求ID、appkey、服务方法、调用结果、请求耗时、调用IP、请求时间、创建时间和操作。

>> 管理员可以根据“请求ID”、“appkey”、“服务方法”、“调用结果”“请求耗时”、“请求时间”查询项来查询服务日志信息。

1、点击页面的【请求追踪】按钮，进行入参出参查看，如下图所示：



>> 请求追踪页面详细展示入参和出参的详细信息，可通过查看入参和出参来检查服务调用情况；

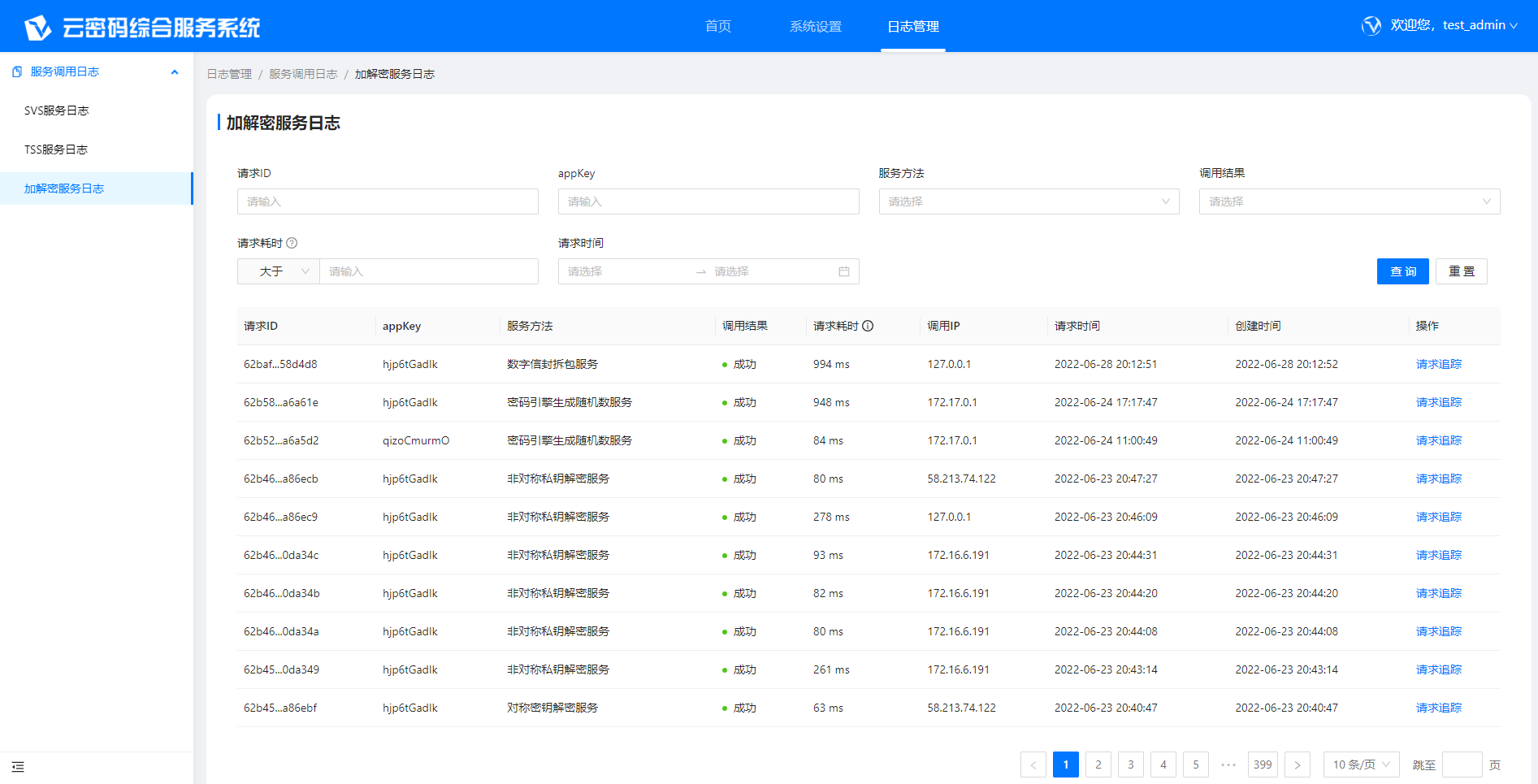
#### 2.9.1.3 加解密服务日志

##### 2.9.1.3.1功能介绍

加解密服务日志主要用于查看加解密服务的调用日志。

##### 2.9.1.3.2操作步骤

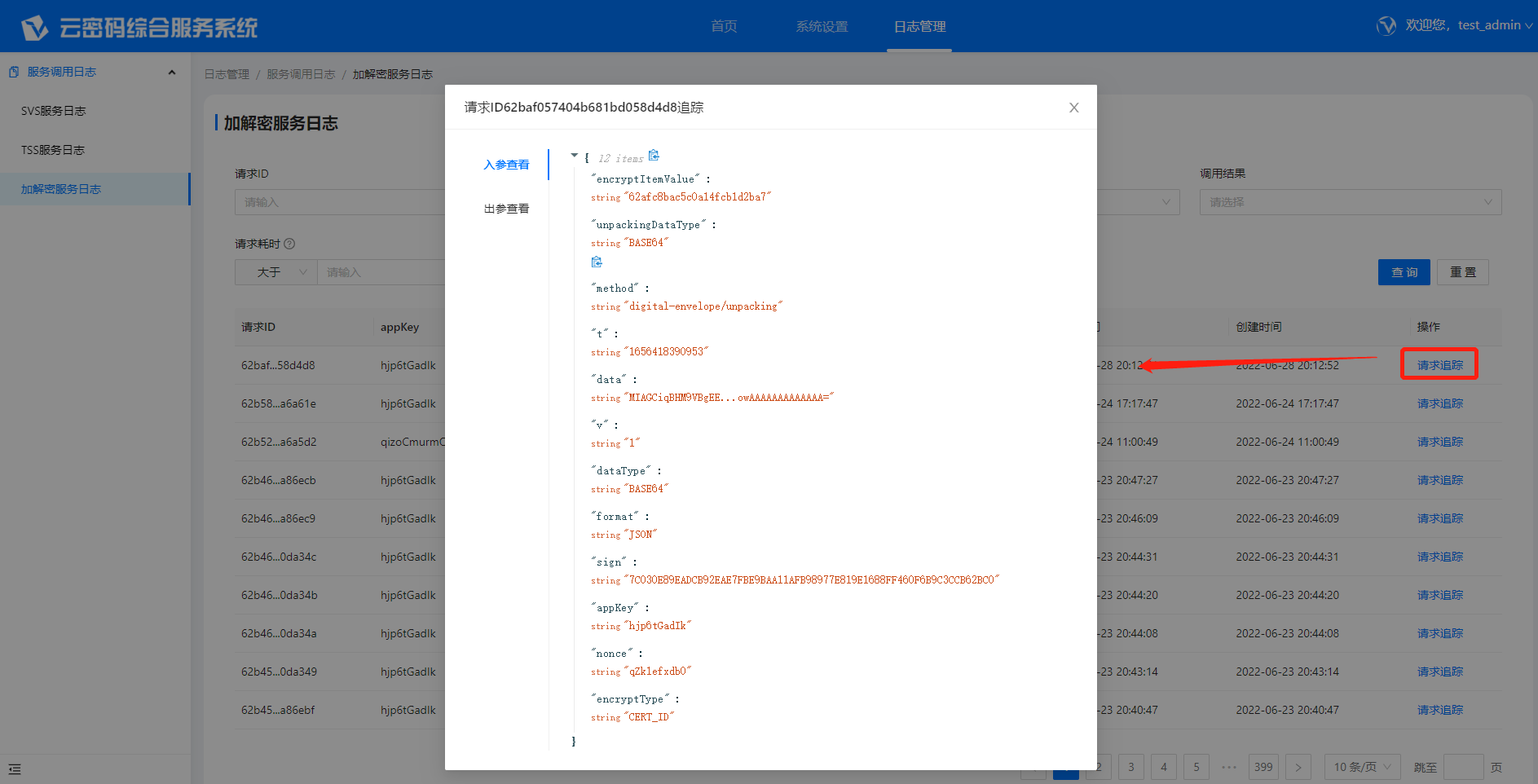
点击菜单〖日志管理〗-〖服务调用日志〗-〖加解密服务日志〗，进入加解密服务日志页面，如下图所示：



>> 页面展示所有加解密服务的调用记录，包含请求ID、appkey、服务方法、调用结果、请求耗时、调用IP、请求时间、创建时间和操作。

>> 管理员可以根据“请求ID”、“appkey”、“服务方法”、“调用结果”“请求耗时”、“请求时间”查询项来查询服务日志信息。

1. 点击页面的【请求追踪】按钮，进行入参出参查看，如下图所示：



>> 请求追踪页面详细展示入参和出参的详细信息，可通过查看入参和出参来检查服务调用情况；

### 2.9.2操作日志

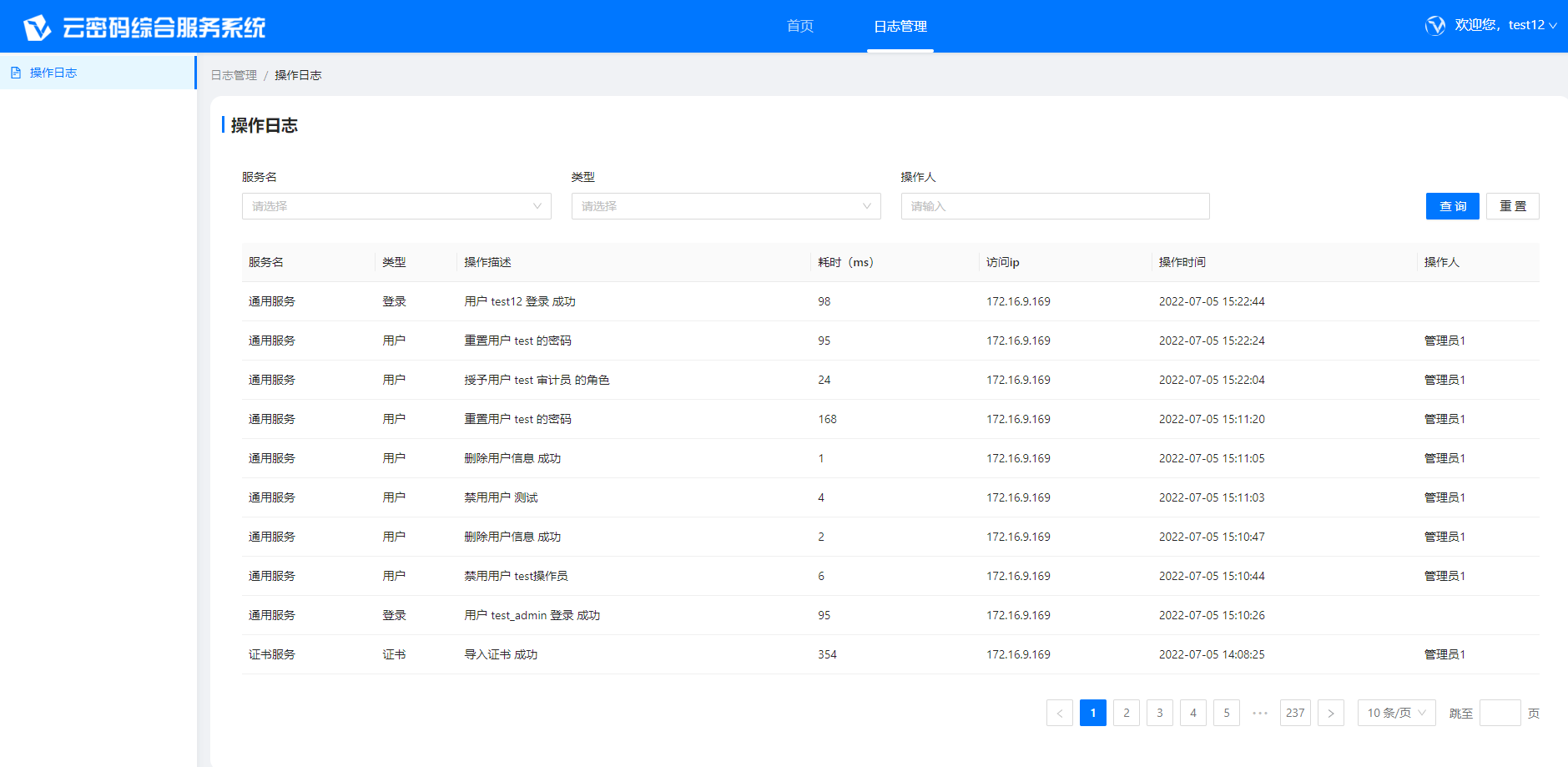
系统审计员拥有操作日志菜单权限。

#### 2.9.2.1功能介绍

操作日志主要用来查看所有操作管理员对云密码综合服务系统的操作记录。

#### 2.9.2.2操作步骤

点击菜单〖日志管理〗-〖操作日志〗，进入操作日志页面，如下图所示：



>> 页面展示所有操作人操作的记录，包含服务名、类型、操作描述、耗时、访问IP、操作时间、操作人。

>> 管理员可以根据“服务名”、“类型”、“操作人”查询项来查询操作日志信息。

# FAQ常见问题