RestCloud-组织权限中心操作手册V4.5

文档编号	V4.5
文档密级	商密 （本文档只授权给谷云公司服务的企业内部传阅， 未经谷云许可不得对外传阅）

RestCloud组织权限中心
操作手册V4.5

谷云科技(广州)有限责任公司
http://www.restcloud.cn

声　明

由于软件版本及功能更新较快所以操作手册有可能有部分功能与软件操作有异
最终以软件版本的功能为准

修订历史记录

版本	日期	AMD	修订者	说明
4.0	2020-10-15	A	RestCloud	修改文档
4.5	2021-03-17	M	RestCloud	修改文档

A-添加，M-修改，D-删除）

组织权限中心

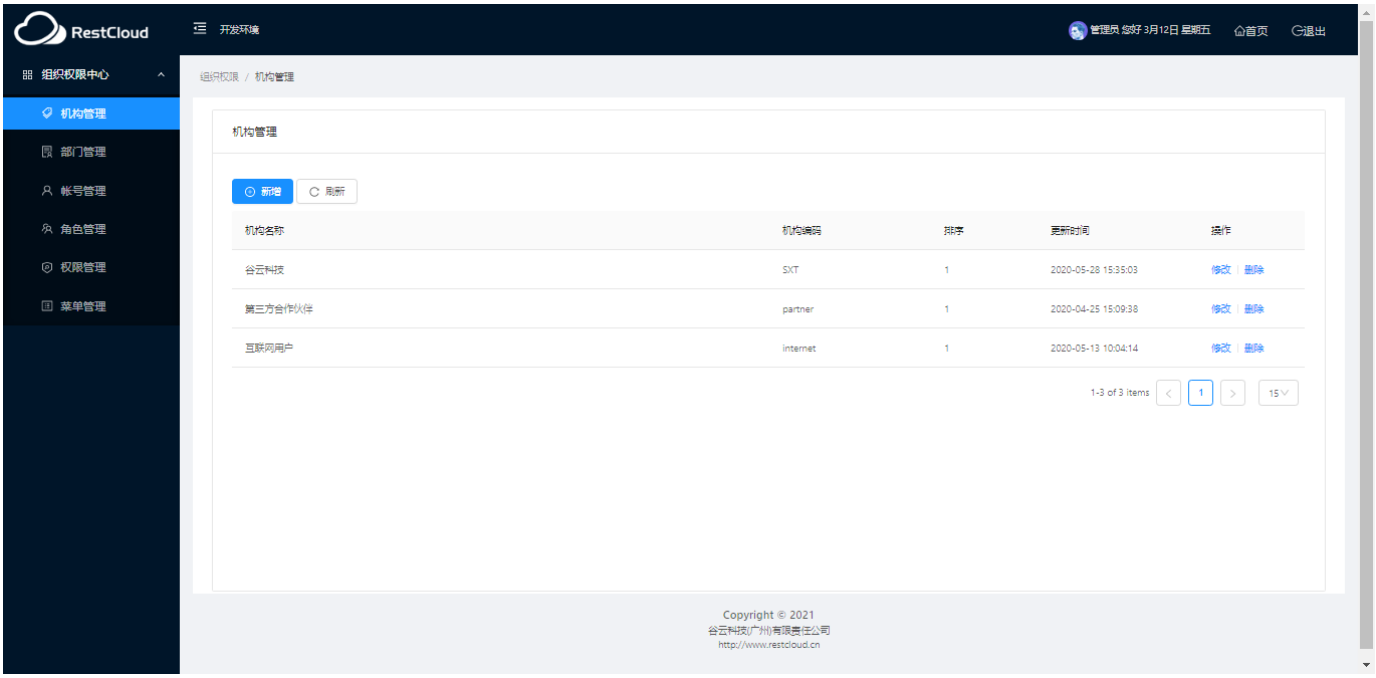
统一对平台的组织、用户、角色、权限进行管理并发布

功能操作说明

机构管理

功能说明：

机构即公司或者子公司是指一个组织的最高层级，如果有多个机构则是并例的关系，如果是子公司则可以作为部门进行注册管理。

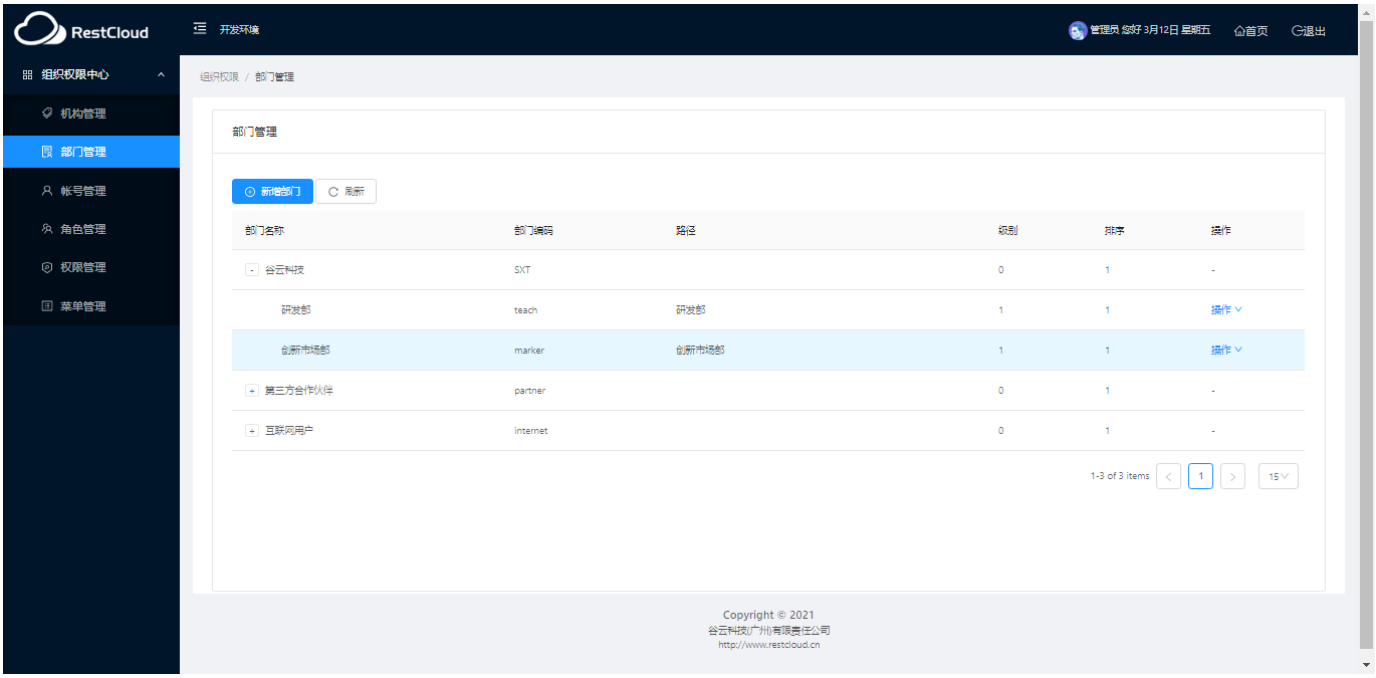


- 新增：新增一个机构
- 修改：修改一个机构的名称
- 删除：删除一个机构（删除后不可恢复）

部门管理

功能说明：

所有机构下的部门及子公司都可以注册为部门进行管理，部门下还可以有子部门

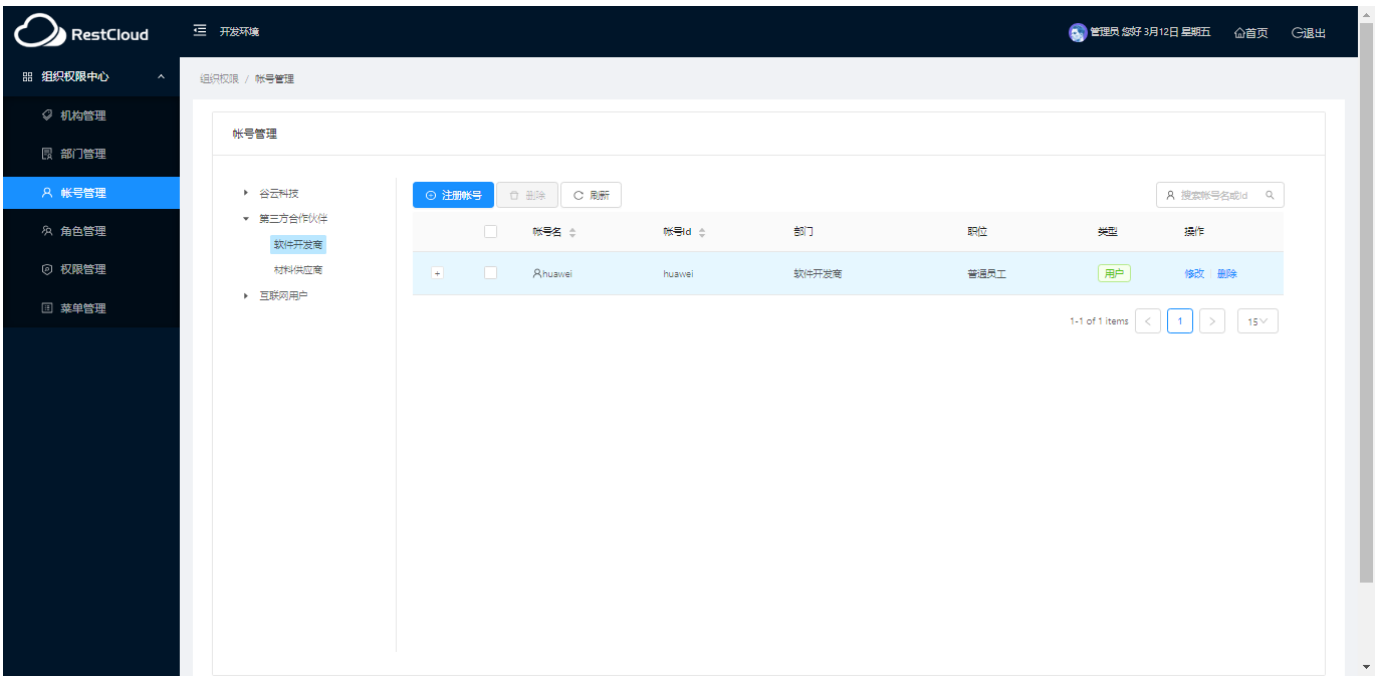


- 新增：选择一个机构或部门，在其下新增一个部门
- 修改：选择一个机构或部门，在其下修改一个部门
- 删除：选择一个机构或部门，在其下修改一个部门

账号管理

功能说明：

对一个机构下所有部门的员工的登录账号进行管理



，

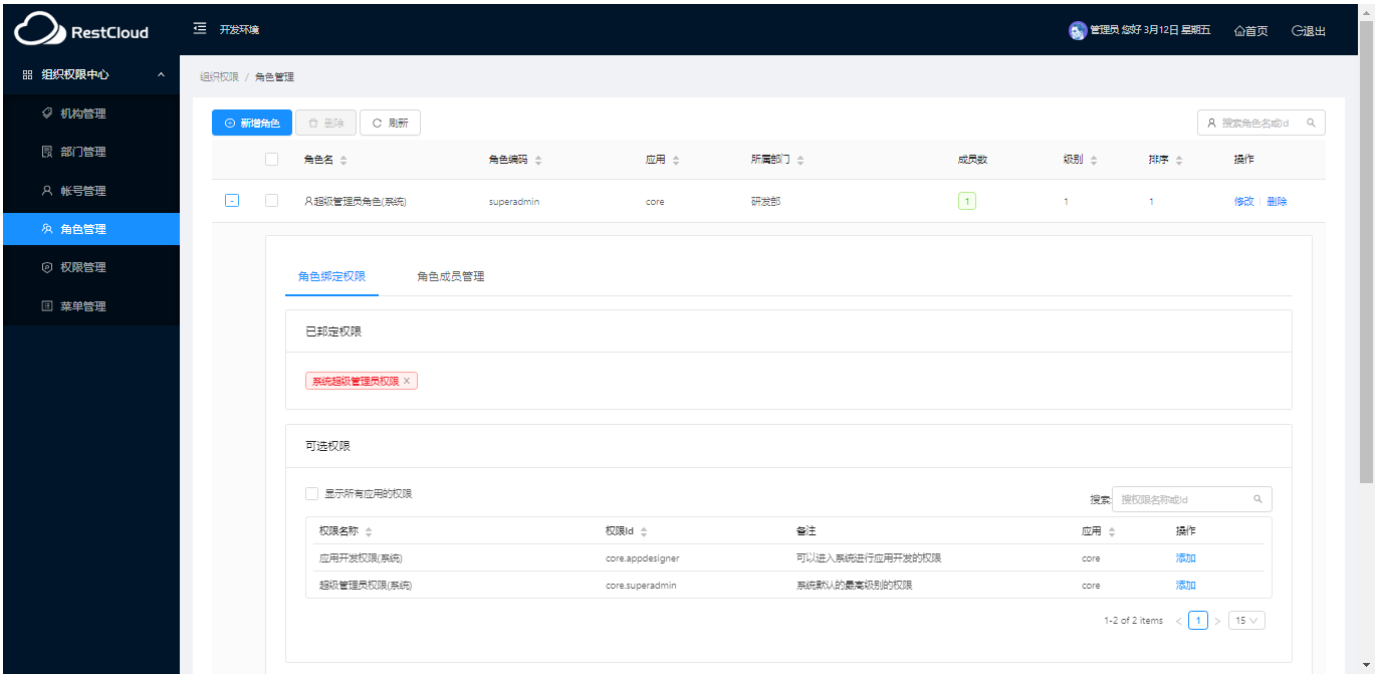
- 注册：选择一个机构下的部门，在该部门下注册一个员工登录账号

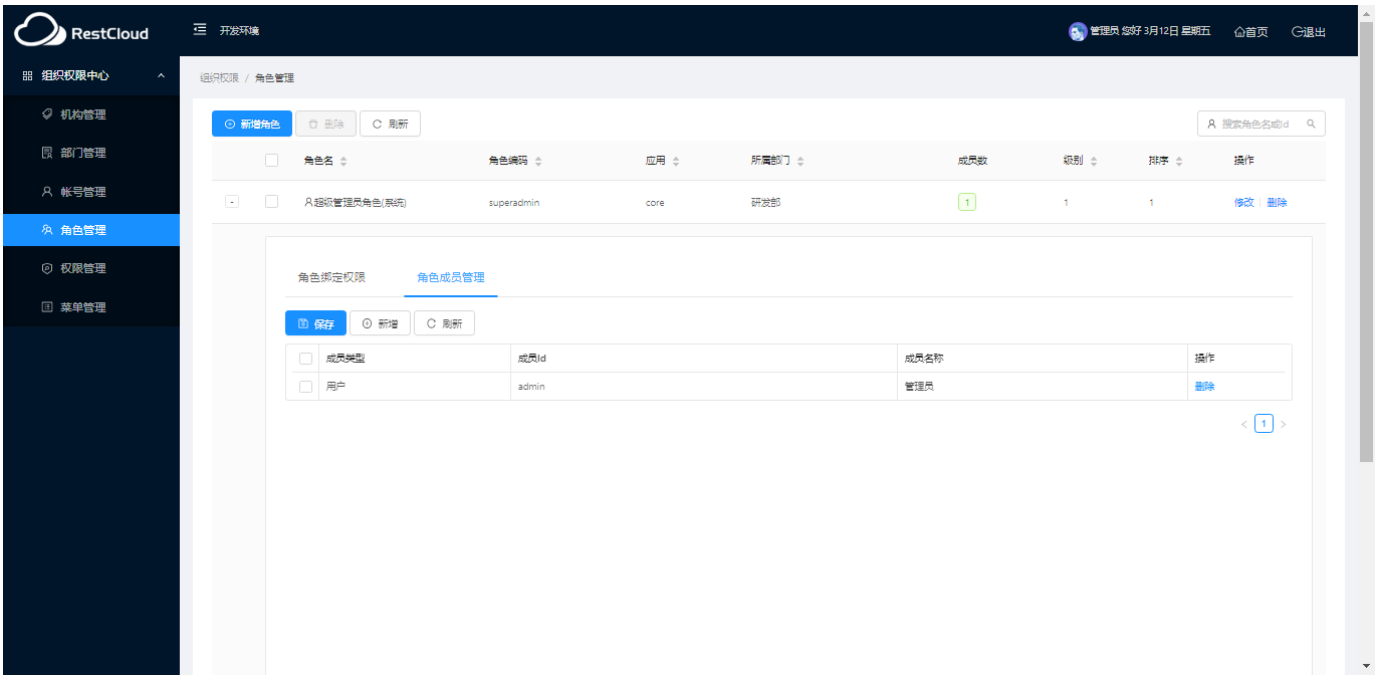
    - 权限设置：设定用户所能放问的功能模块，账号认证密钥，数据加密密钥等账号权限
    - 角色设置：设定用户的角色以明确用户对API的调用权限
- 修改：选择一个机构下的部门，在该部门下修改一个员工的账号信息
- 删除：选择一个机构下的部门，删除一个在该部门下的员工账号

角色管理

功能说明：

这是本平台实现权限管理的核心功能，账号通过配置角色，而角色关联权限来对Rest服务的调用进行控制





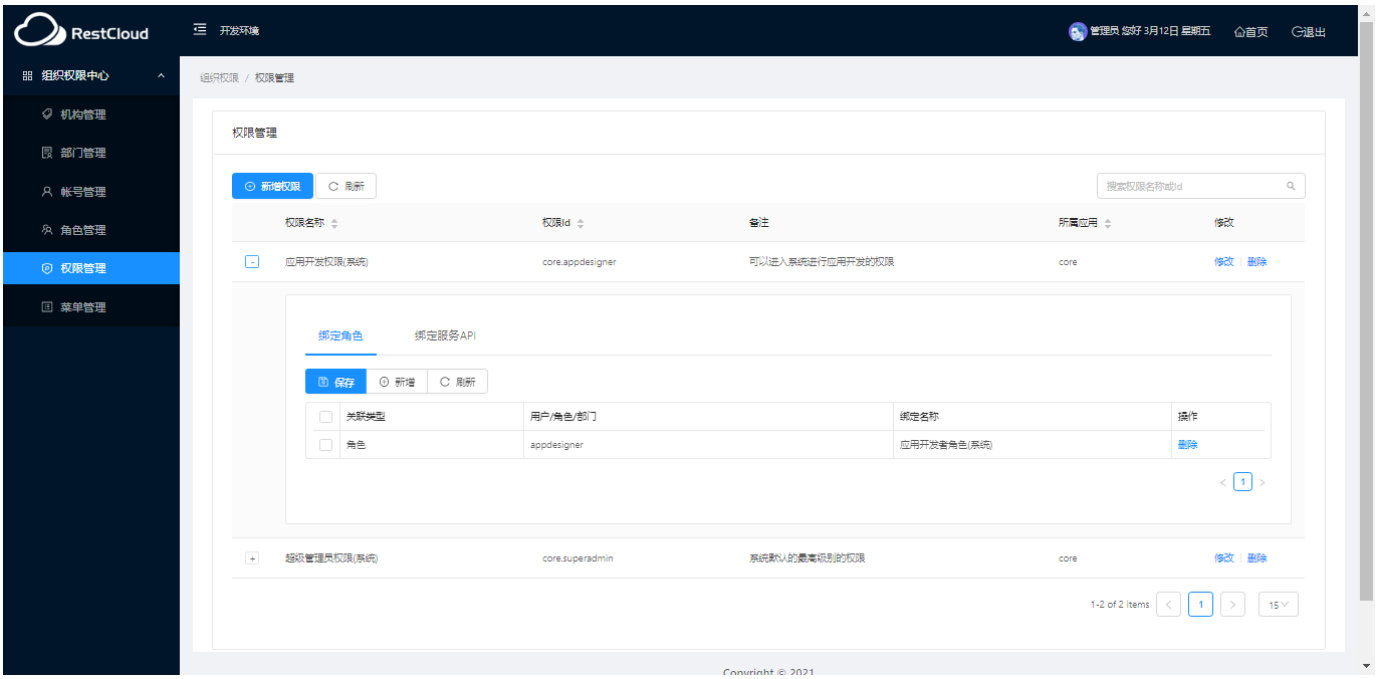
- 新增：新增一个角色

    - 绑定权限：角色通过已绑定权限对API的调用进行控制
    - 成员：添加账号作为称号，让账号获得当前角色的权限
- 修改：修改一个角色
- 删除：删除一个角色

权限管理

功能说明：

本平台的角色与服务的权限进行关联用来控制服务的访问权限，本平台的权限控制思路为，先把需要控制的某一些服务组成一个权限控制点，然后再由权限控制点去关联角色。



- 新增：新增一个权限控制点
    - 绑定角色：在当前权限控制点绑定角色，让角色获得当前权限控制点对某一些服务的控制。
    - 绑定服务：在当前权限控制点绑定某一些服务，让当前权限获得这些服务的调用权限。
- 修改：修改一个权限控制点
- 删除：删除一个权限控制点

场景示例

1、给账户用户配置某应用接口开发权限示例

场景说明：用户获得对某一个应用下的开发权限

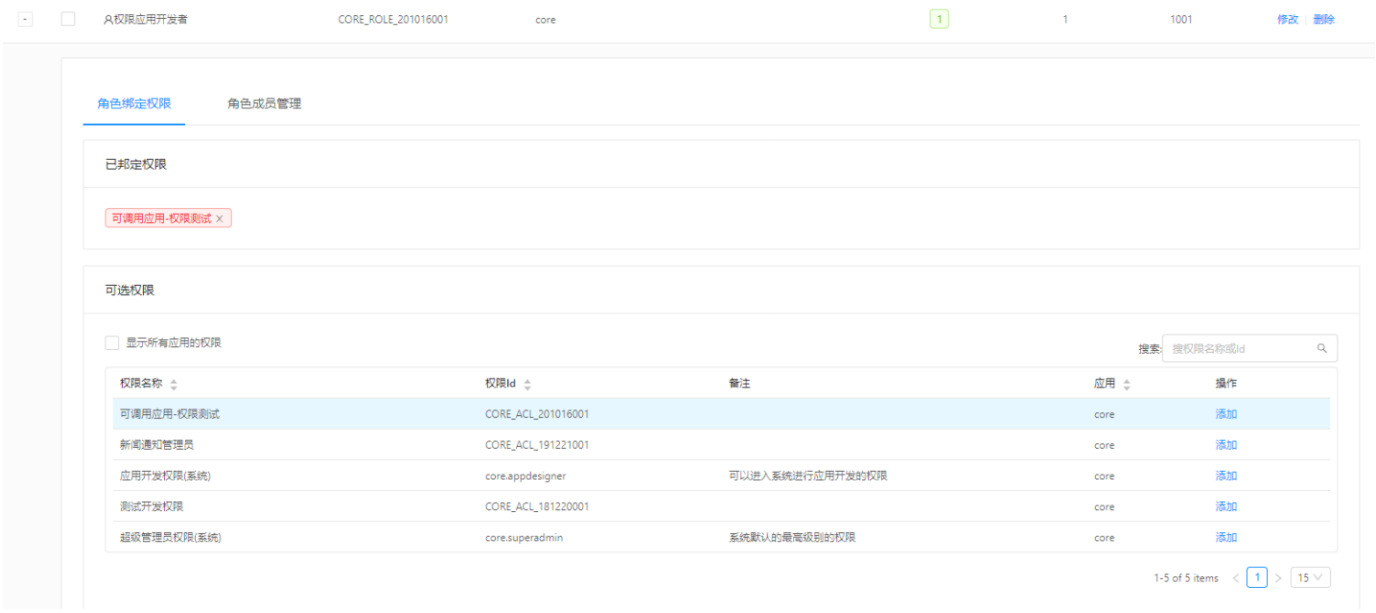
1、新建一个用户

2、新建一个权限

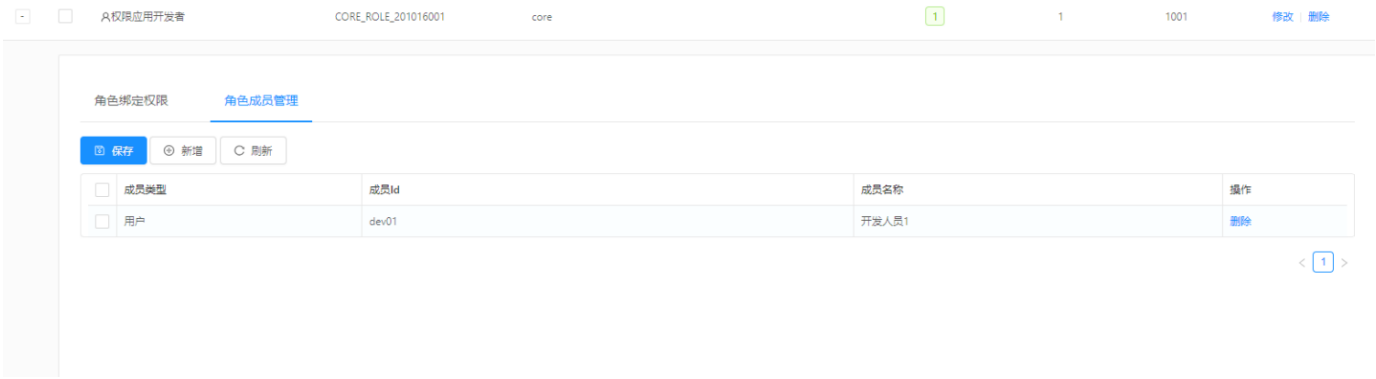
3、新建一个角色，建立权限和账号的关联


角色属性
API控制属性
* 所属应用：
core|核心应用
应用唯一id
* 所属部门：
研发部
* 角色名称：
权限应用开发
* 角色编码：
CORE_ROLE_201016002
保存后如需要修改需要确认没有被引用，如果已经有引用的情况下修改将造成引用对像出错
* 角色级别：
1
用来扩展区分角色的不同级别或分类
* 排序：
1001
备注：
提交
取消

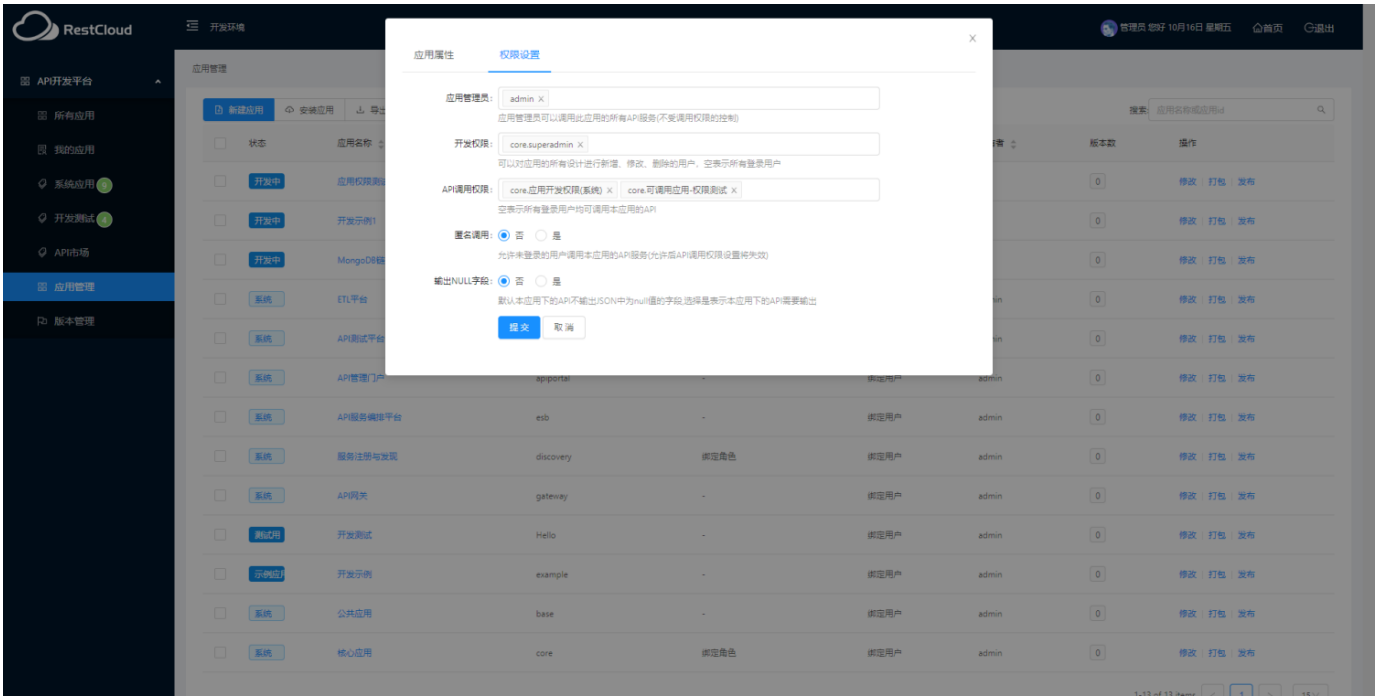
绑定权限



添加账户



4、配置权限具备开发权限



在开发平台的应用管理中，选择核心应用，将权限加入核心应用的API调用权限

5、新建一个应用

权限设定为其他权限

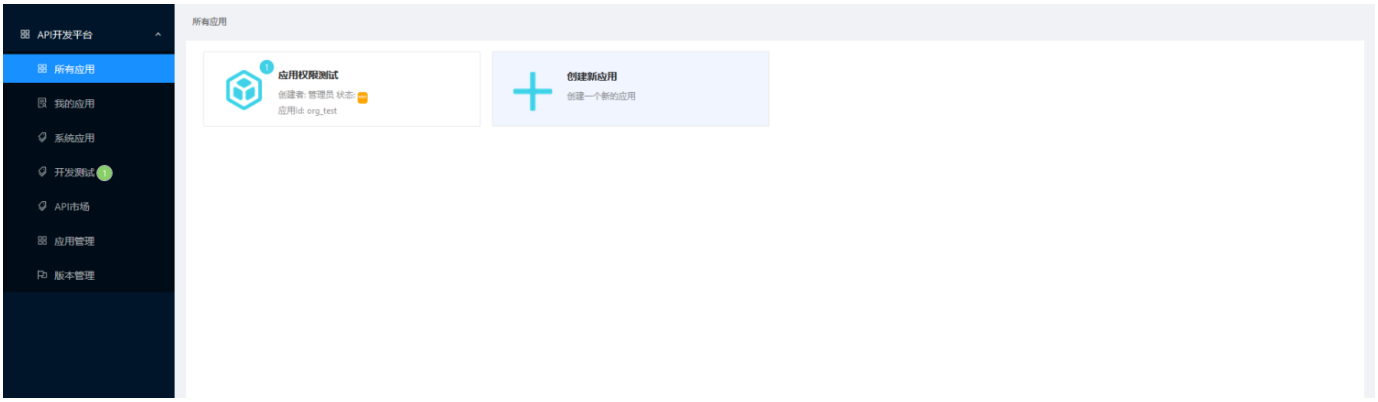
用户“开发人员1”进入

看不到任何应用

6、配置开发人员权限

进入应用管理，修改应用权限，在开发权限中加入“开发人员1”

7、开发人员访问应用开发模块



可以看到配置了开发权限的应用，可以对该应用进行开发

2、给应用账户配置应用接口调用权限示例

场景说明：用户获得对某一个应用下的所有API的调用权限

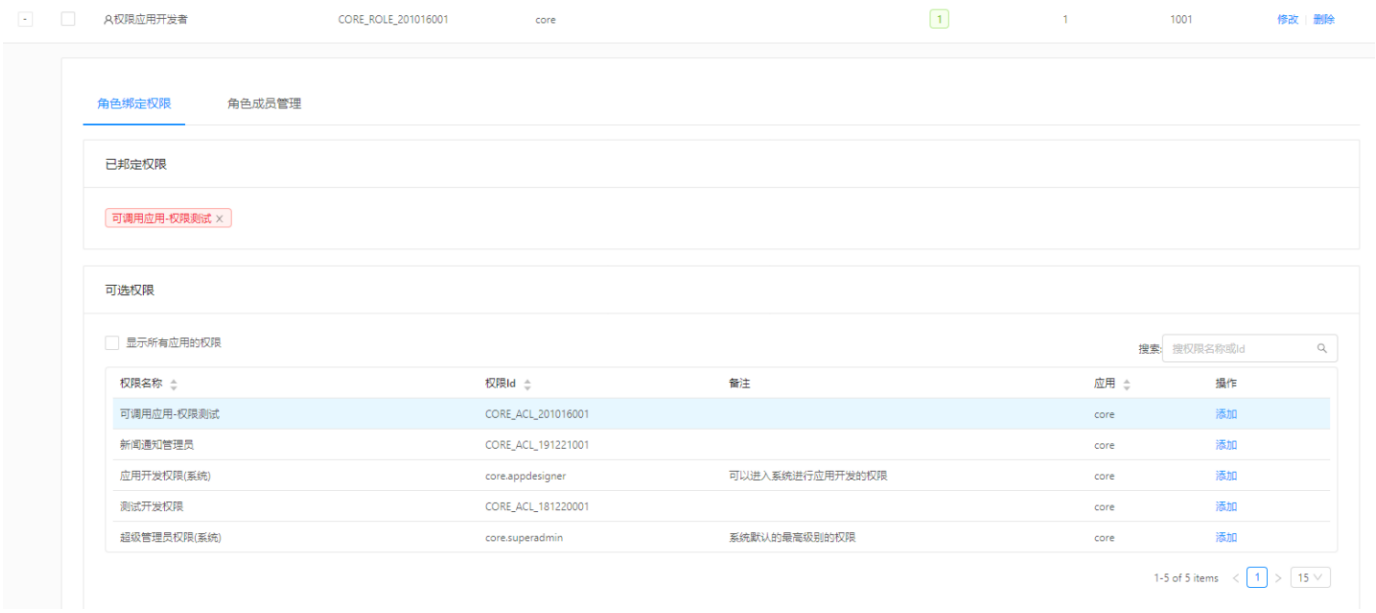
1、新建一个用户

2、新建一个权限

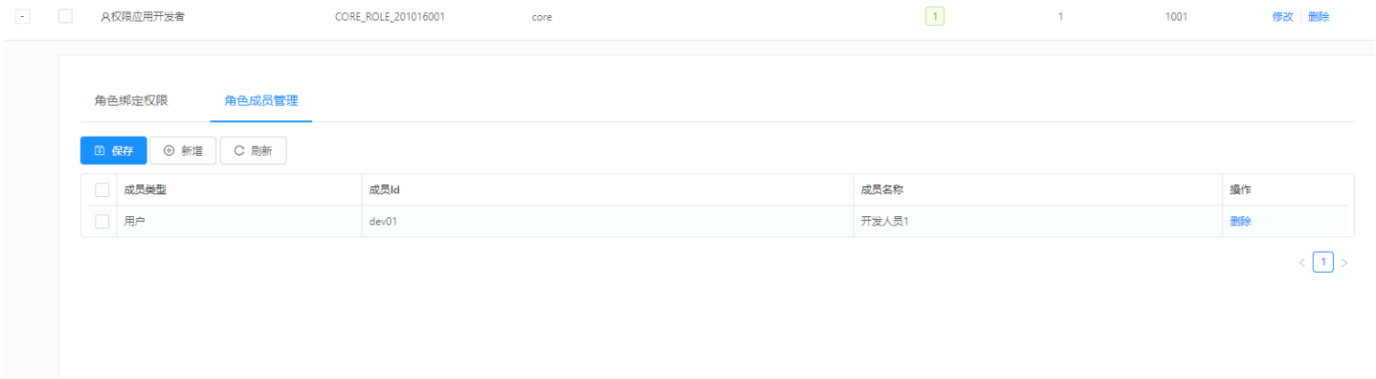
3、新建一个角色，建立权限和账号的关联


角色属性
API控制属性
* 所属应用：
core|核心应用
应用唯一id
* 所属部门：
研发部
* 角色名称：
权限应用开发
* 角色编码：
CORE_ROLE_201016002
保存后如需要修改需要确认没有被引用，如果已经有引用的情况下修改将造成引用对像出错
* 角色级别：
1
用来扩展区分角色的不同级别或分类
* 排序：
1001
备注：
提交
取消

绑定权限



添加账户



4、新建一个应用

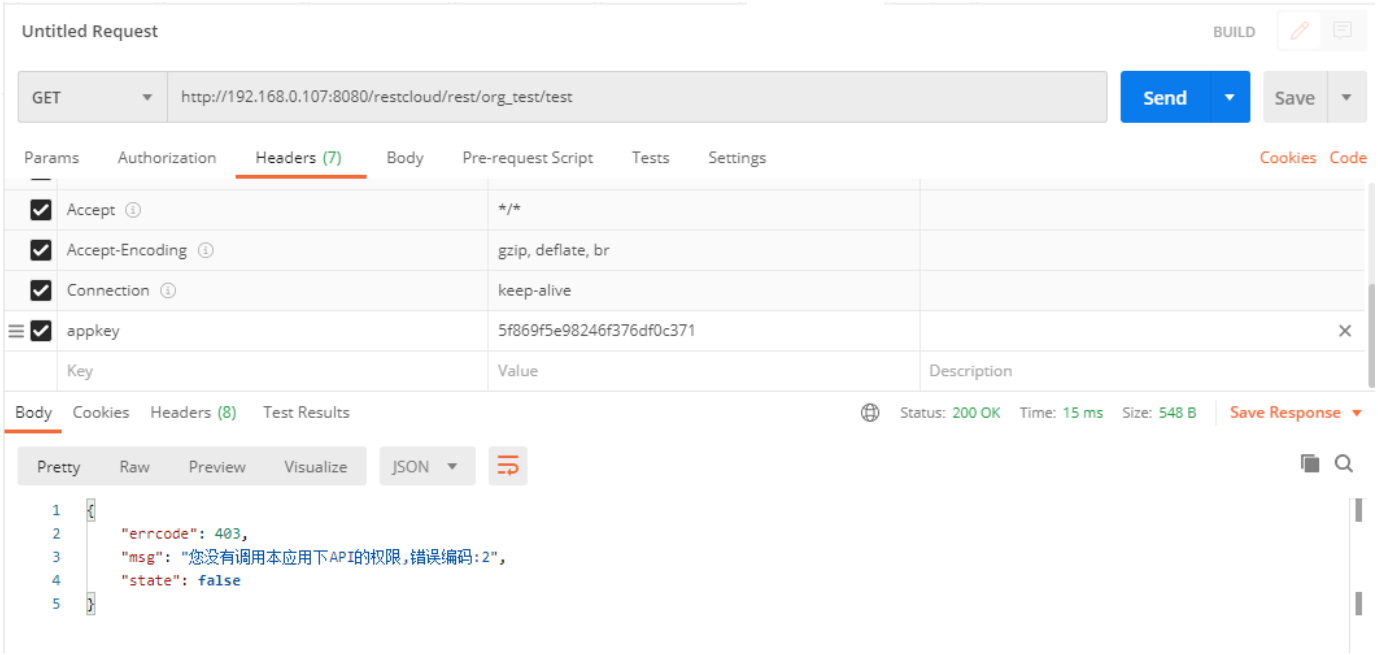
权限设定为其他权限

5、在应用中创建一个接口

接口认证模式设置为appkey认证

6、在postman测试

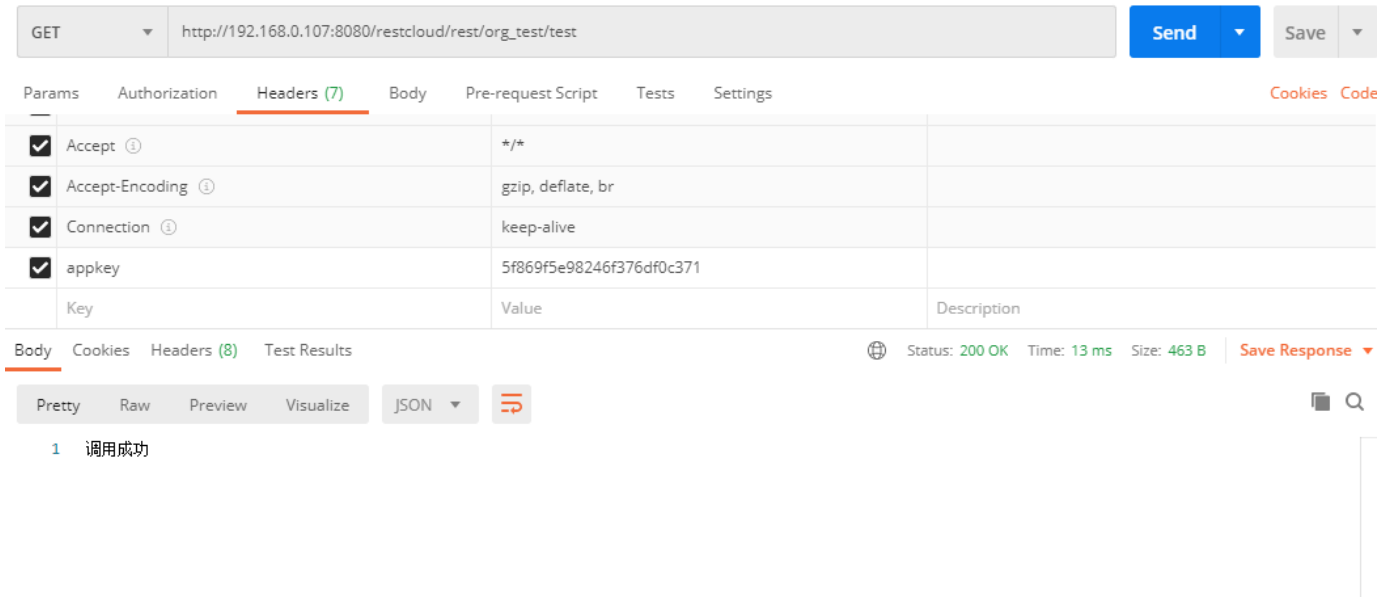
将用户“开发人员1”的appkey放在请求头中



当前用户所拥有的权限没办法对该应用下的API访问

7、修改应用权限

8、postman中测试



3、给用户账户配置应用接口查看权限示例

场景说明：用户只能看到某个应用的已发布API

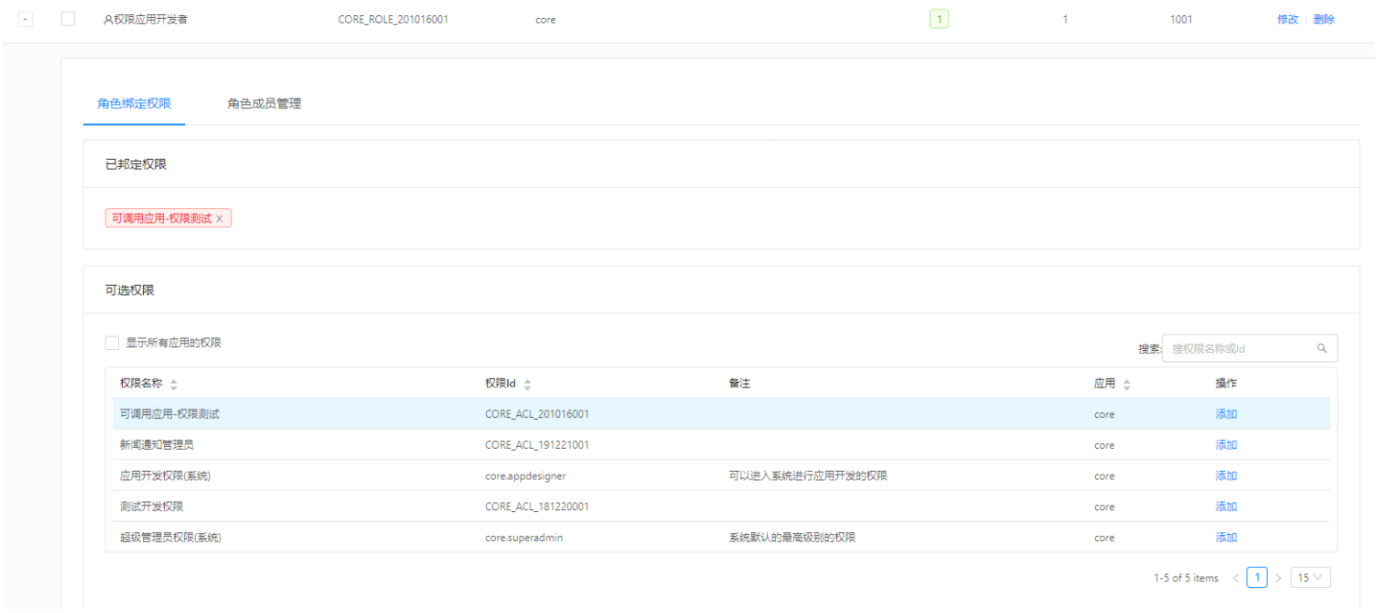
1、新建一个用户

2、新建一个权限

3、新建一个角色，建立权限和账号的关联


角色属性
API控制属性
* 所属应用：
core|核心应用
应用唯一id
* 所属部门：
研发部
* 角色名称：
权限应用开发
* 角色编码：
CORE_ROLE_201016002
保存后如需要修改需要确认没有被引用，如果已经有引用的情况下修改将造成引用对像出错
* 角色级别：
1
用来扩展区分角色的不同级别或分类
* 排序：
1001
备注：
提交
取消

绑定权限



添加账户

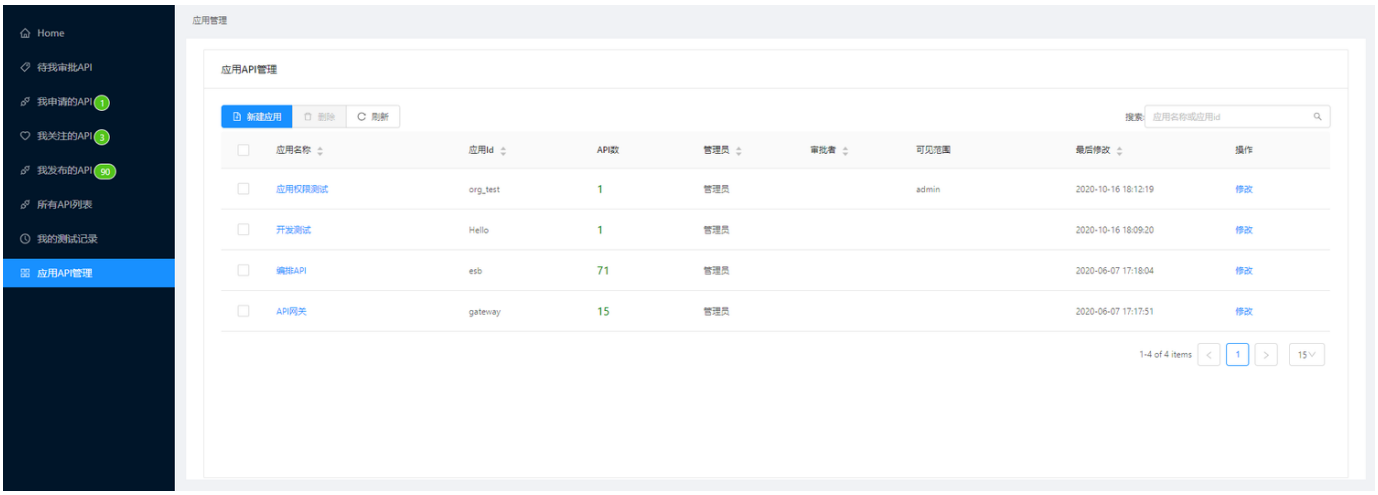
4、新建一个应用

权限设定为其他权限

5、在应用中创建一个接口

接口认证模式设置为appkey认证

6、在API管理门户中创建应用



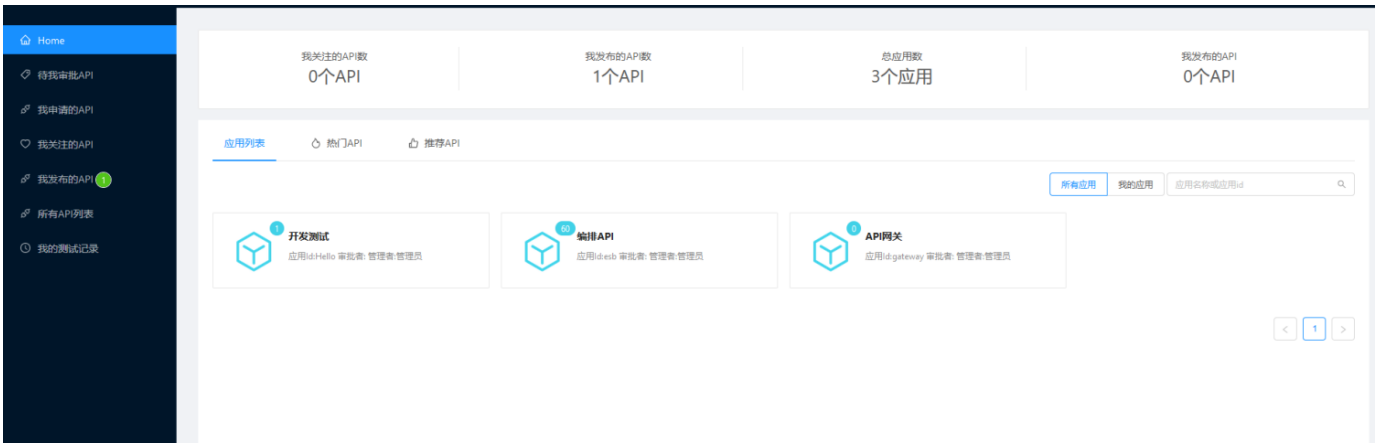
新建一个应用

如果是开发平台应用发布的API，其所属应用ID要跟开发平台中的应用的ID保持一致

7、发布API

进入开发平台，将API发布到管理门户中

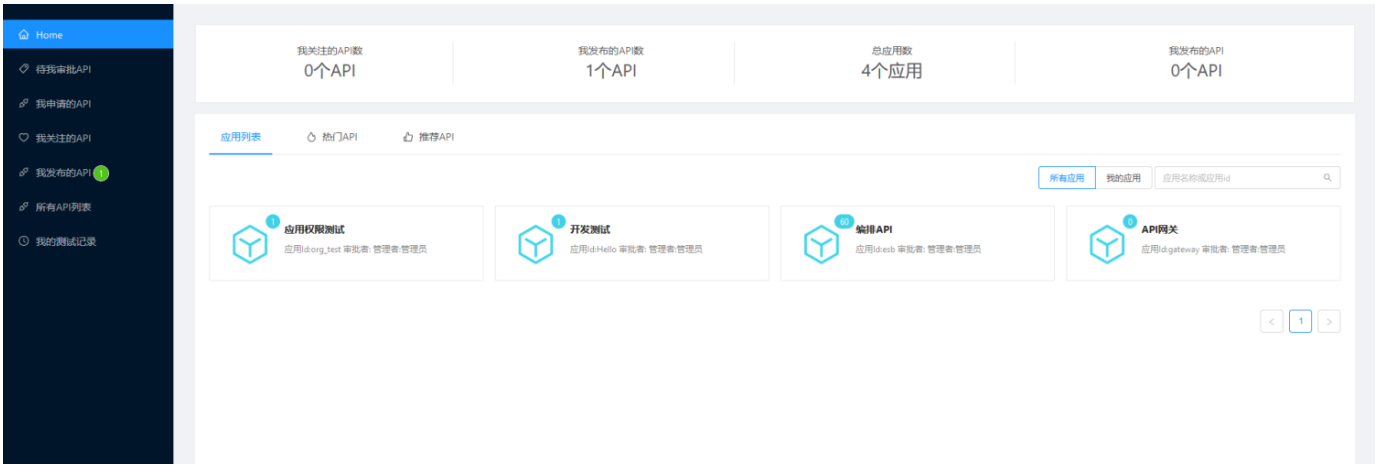
8、第三方应用账户进入管理门户



看不到应用

9、修改应用权限

10、第三方应用账户进入管理门户



可看到应用