

RestCloud-组织权限中心操作手册V4.5

组织权限中心

功能操作说明

机构管理

部门管理

账号管理

角色管理

权限管理

场景示例

- 1、给账户用户配置某应用接口开发权限示例
- 2、给应用账户配置应用接口调用权限示例
- 3、给用户账户配置应用接口查看权限示例

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

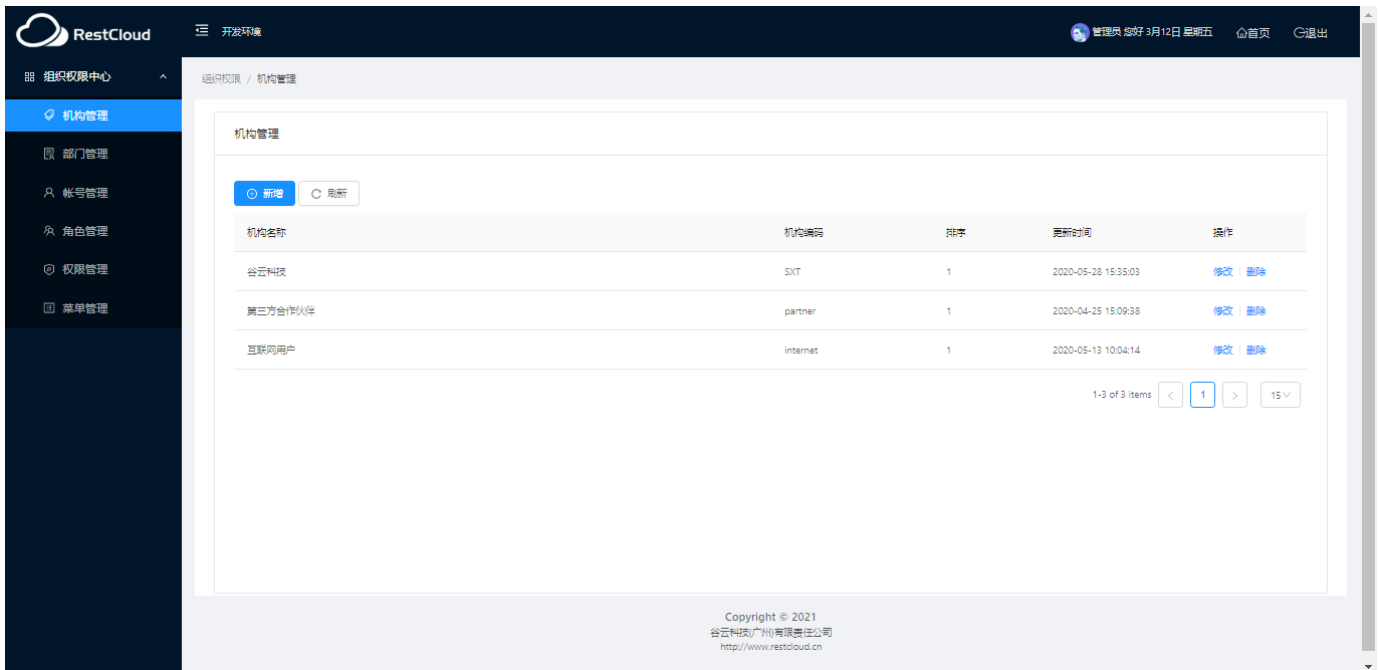
统一对平台的组织、用户、角色、权限进行管理并发布

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列的关系，如果是子公司则可以作为部门进行注册管理。

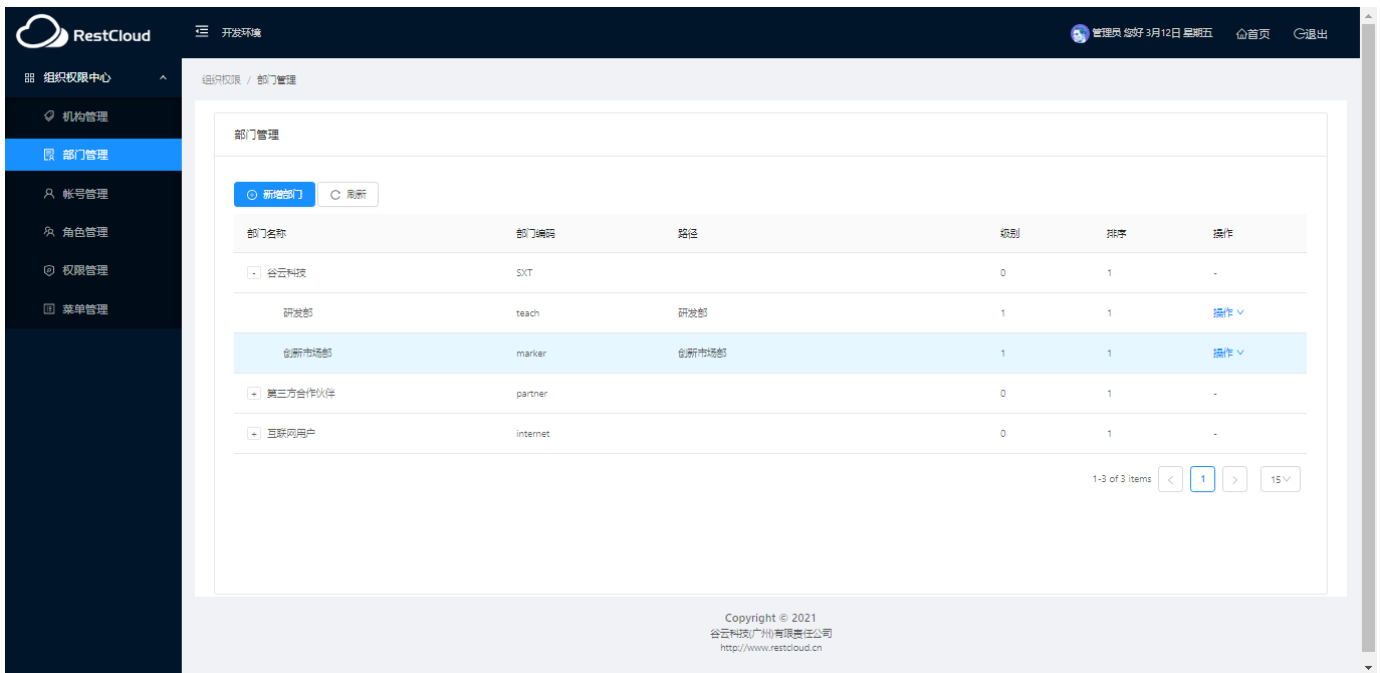


- 新增：新增一个机构
- 修改：修改一个机构的名称
- 删除：删除一个机构（删除后不可恢复）

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

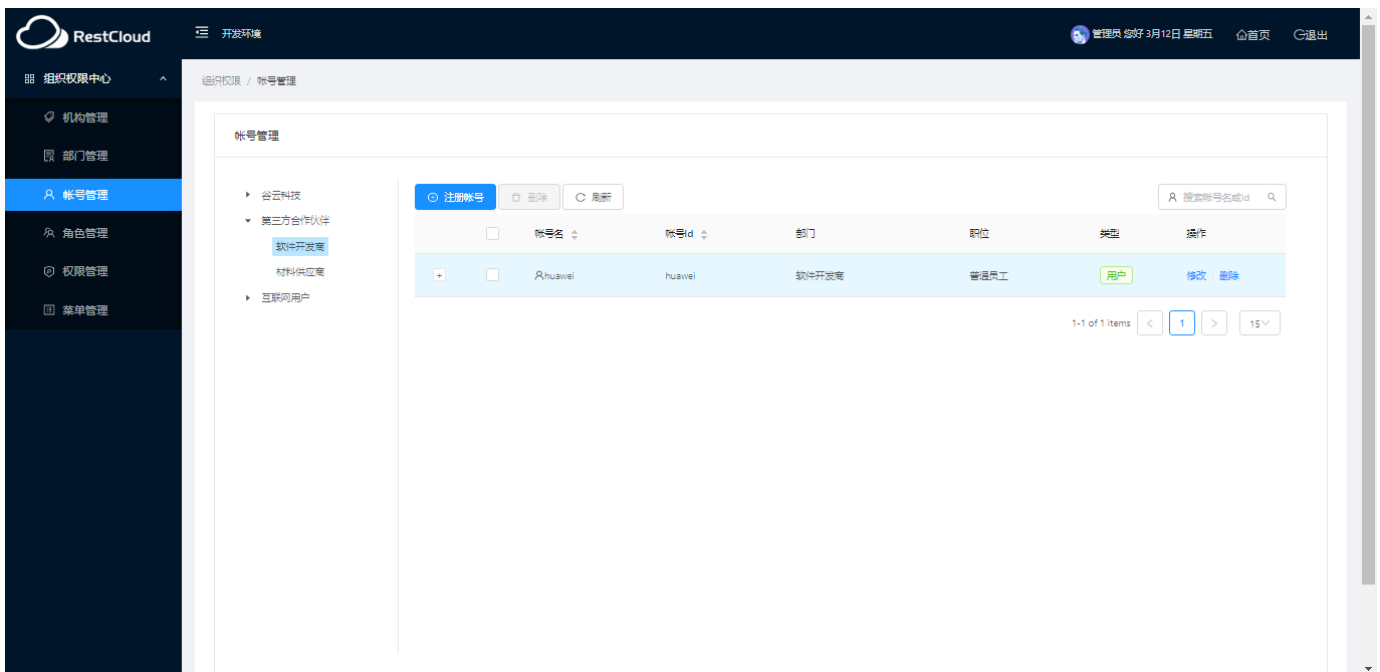


- 新增：选择一个机构或部门，在其下新增一个部门
- 修改：选择一个机构或部门，在其下修改一个部门
- 删除：选择一个机构或部门，在其下修改一个部门

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



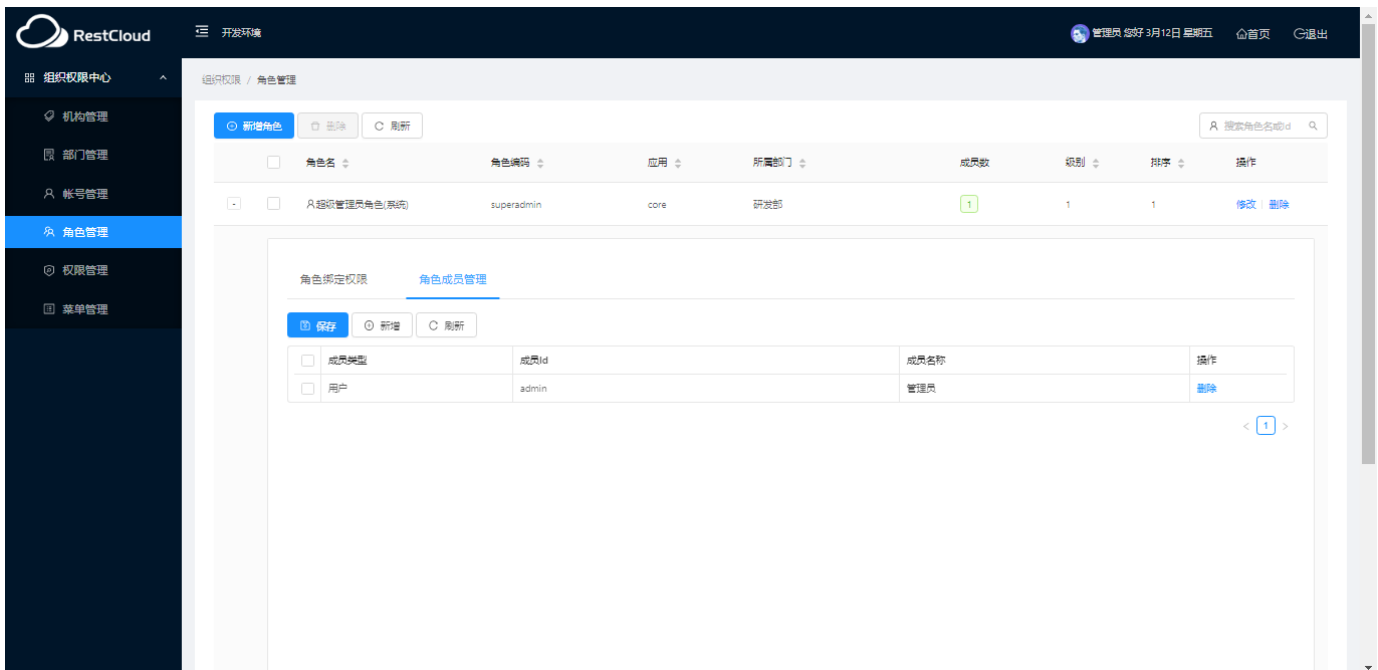
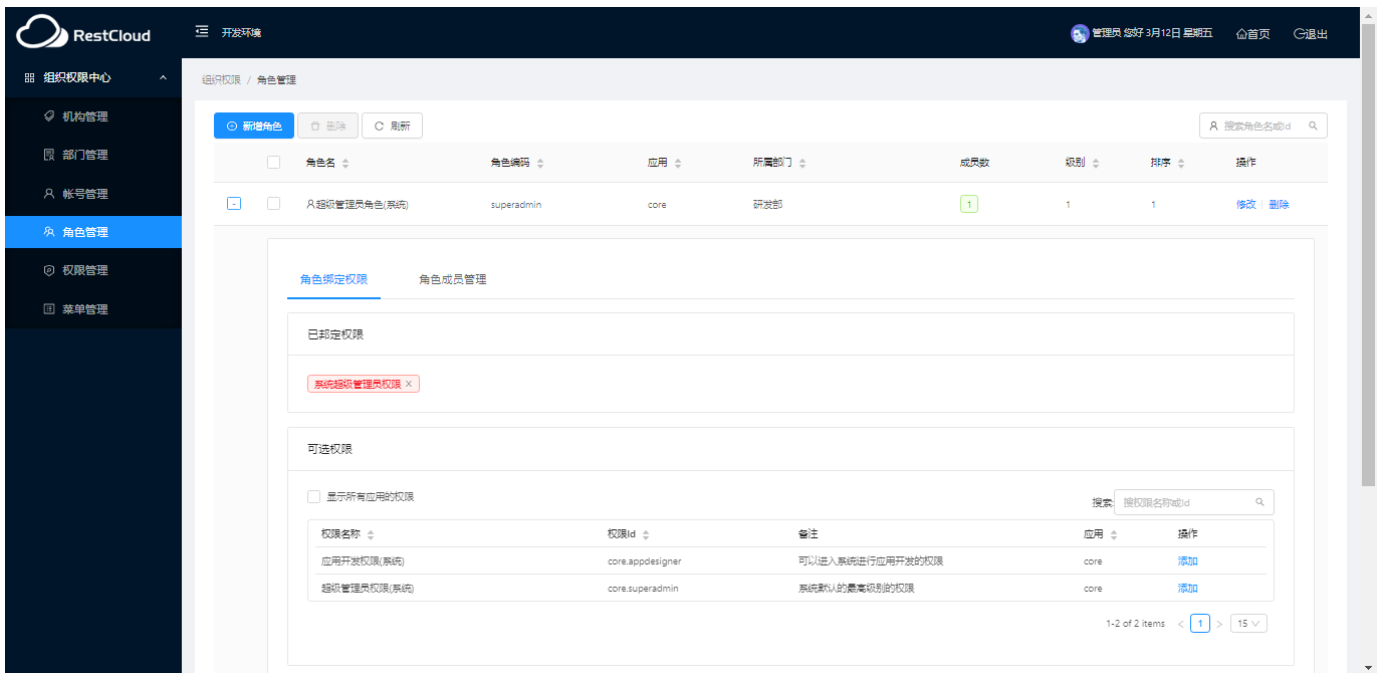
- 注册：选择一个机构下的部门，在该部门下注册一个员工登录账号

- 权限设置：设定用户所能访问的功能模块，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



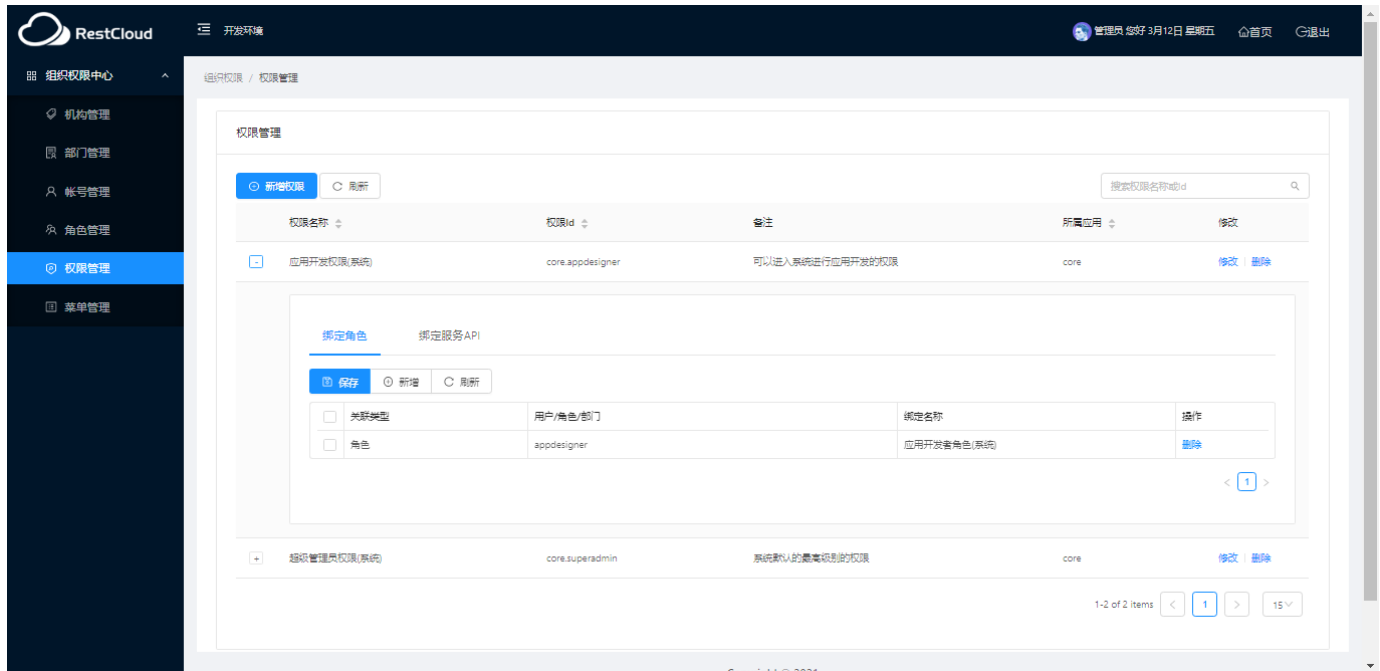
- 新增：新增一个角色

- 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

用户属性

权限设置

更多设置

头像

* 所属部门: 研发部 ✓

* 用户名: 开发人员1
用户中文名称

* 用户登录Id: dev01 ✓
必须唯一且注册后不可修改(所有用户建议使用固定长度的字符串作为Id如6位工号等)

帐号类型: 普通用户帐号 ✓
普通用户表示进入本系统进行开发运维的帐号,应用系统帐号表示仅供外部应用查询和调用API使用的帐号

职位: 普通员工 ✓

* 登录密码:
密码建议由大写字母、小写字母、数字、特殊字符组成, 最多30个字符(具体验证规则可在平台参数中配置)

密码有效日期: Select date 
空表示永久有效

提交 取消

2、新建一个权限

权限属性

* 所属应用: core|核心应用 ✓
应用唯一id

* 权限唯一Id: CORE_ACL_201016002 ✓
注意:保存后如果要修改请确认权限没有被引用, 否则引用的对象将会出错

* 权限名称: 可调用应用-权限测试 ✓
指定任何有意义且能描述本权限的名称

备注:

保存并关闭 关闭

3、新建一个角色, 建立权限和账号的关联

*

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

权限应用开发者

CORE_ROLE_201016001

core

1

1

1001

修改 | 删除

角色绑定权限

角色成员管理

已绑定权限

可用应用-权限测试

可选权限

显示所有应用的权限

搜索: 搜权限名称或id

权限名称	权限Id	备注	应用	操作
可用应用-权限测试	CORE_ACL_201016001		core	添加
新闻通知管理员	CORE_ACL_191221001		core	添加
应用开发权限(系统)	core.appdesigner	可以进入系统进行应用开发的权限	core	添加
测试开发权限	CORE_ACL_181220001		core	添加
超级管理员权限(系统)	core.superadmin	系统默认的最高级别的权限	core	添加

1-5 of 5 items < 1 > 15

添加账户

权限应用开发者

CORE_ROLE_201016001

core

1

1

1001

修改 | 删除

角色绑定权限

角色成员管理

保存

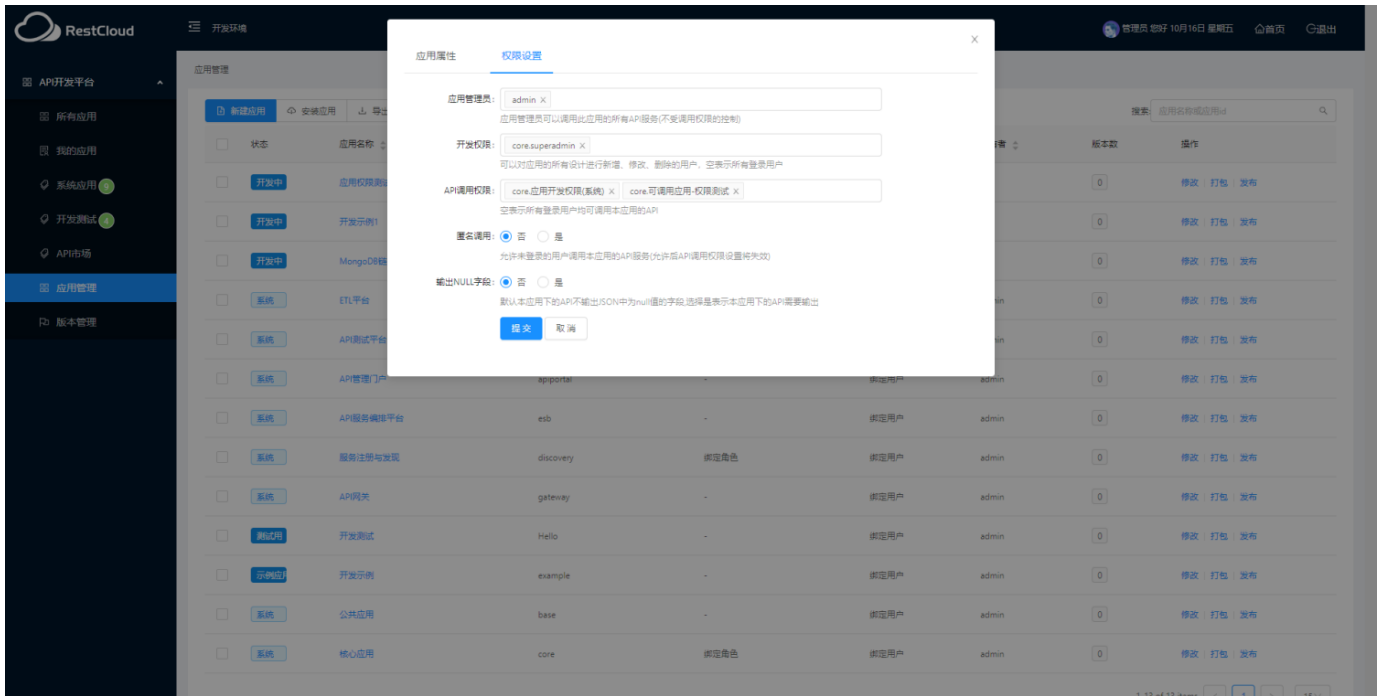
新增

刷新

成员类型	成员Id	成员名称	操作
用户	dev01	开发人员1	删除

< 1 >

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

应用属性

权限设置

* 所属分类：

开发测试

请选择应用的所属分类

* 应用名称：

应用权限测试

任意可描述本应用功能或模块的名称

* 应用Id：

org_test

应用Id必须唯一,任意小写英文字母或数字组成，如果应用已经有设计元素修改应用Id会丢失设计元素

状态：

开发中

指定应用当前的开发进度或状态

版本：

1.0

备注：

提交

取消

权限设定为其他权限

应用属性

权限设置

应用管理员:

admin X

应用管理员可以调用此应用的所有API服务(不受调用权限的控制)

开发权限:

admin X

可以对应用的所有设计进行新增、修改、删除的用户, 空表示所有登录用户

API调用权限:

core.应用开发权限(系统) X

空表示所有登录用户均可调用本应用的API

匿名调用:



否



是

允许未登录的用户调用本应用的API服务(允许后API调用权限设置将失效)

输出NULL字段:



否



是

默认本应用下的API不输出JSON中为null值的字段,选择是表示本应用下的API需要输出

提交

取消

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”

X

应用属性

权限设置

应用管理员:

admin X

应用管理员可以调用此应用的所有API服务(不受调用权限的控制)

开发权限:

管理员 X 开发人员1 X

可以对应用的所有设计进行新增、修改、删除的用户, 空表示所有登录用户

API调用权限:

core,应用开发权限(系统) X

空表示所有登录用户均可调用本应用的API

匿名调用:

☒ 否 ☐ 是

允许未登录的用户调用本应用的API服务(允许后API调用权限设置将失效)

输出NULL字段:

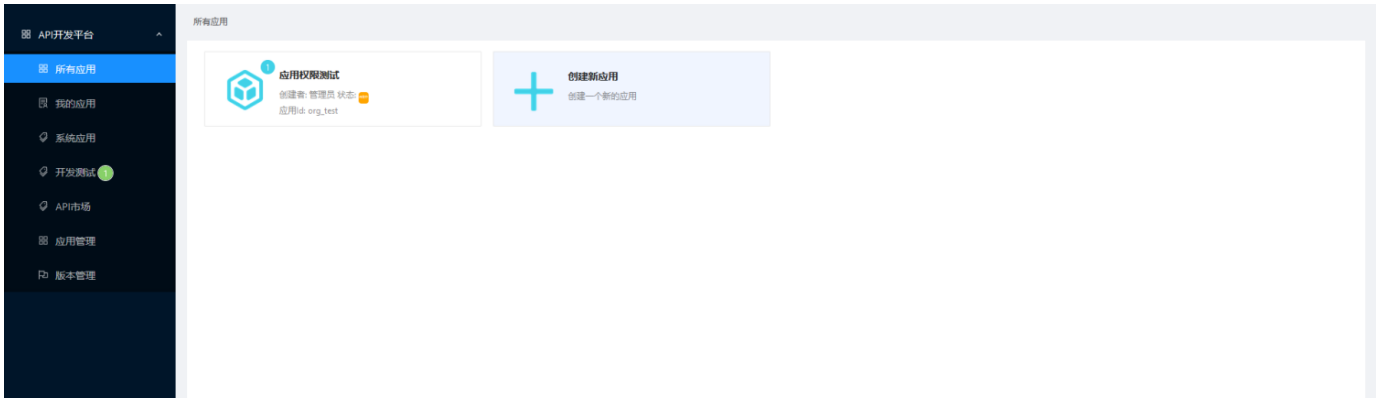
☒ 否 ☐ 是

默认本应用下的API不输出JSON中为null值的字段,选择是表示本应用下的API需要输出

提交

取消

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

用户属性

权限设置

更多设置

头像

* 所属部门: 研发部 ✓

* 用户名: 开发人员1
用户中文名称

* 用户登录Id: dev01 ✓
必须唯一且注册后不可修改(所有用户建议使用固定长度的字符串作为Id如6位工号等)

帐号类型: 普通用户帐号 ✓
普通用户表示进入本系统进行开发运维的帐号,应用系统帐号表示仅供外部应用查询和调用API使用的帐号

职位: 普通员工 ✓

* 登录密码:
密码建议由大写字母、小写字母、数字、特殊字符组成, 最多30个字符(具体验证规则可在平台参数中配置)

密码有效日期: Select date 
空表示永久有效

提交 取消

2、新建一个权限

权限属性

* 所属应用: core|核心应用 ✓
应用唯一id

* 权限唯一Id: CORE_ACL_201016002 ✓
注意:保存后如果要修改请确认权限没有被引用, 否则引用的对象将会出错

* 权限名称: 可调用应用-权限测试 ✓
指定任何有意义且能描述本权限的名称

备注:

保存并关闭 关闭

3、新建一个角色, 建立权限和账号的关联

*

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

权限应用开发者

CORE_ROLE_201016001

core

1

1001

修改 | 删除

角色绑定权限

角色成员管理

已绑定权限

可用应用-权限测试

可选权限

显示所有应用的权限

搜索: 搜权限名称或id

权限名称	权限Id	备注	应用	操作
可用应用-权限测试	CORE_ACL_201016001		core	添加
新闻通知管理员	CORE_ACL_191221001		core	添加
应用开发权限(系统)	core.appdesigner	可以进入系统进行应用开发的权限	core	添加
测试开发权限	CORE_ACL_181220001		core	添加
超级管理员权限(系统)	core.superadmin	系统默认的最高级别的权限	core	添加

1-5 of 5 items < 1 > 15

添加账户

权限应用开发者

CORE_ROLE_201016001

core

1

1001

修改 | 删除

角色绑定权限

角色成员管理

保存

新增

刷新

成员类型	成员Id	成员名称	操作
用户	dev01	开发人员1	删除

< 1 >

4、新建一个应用

应用属性

权限设置

* 所属分类: 开发测试 ▼
请选择应用的所属分类

* 应用名称: 应用权限测试
任意可描述本应用功能或模块的名称

* 应用Id: org_test
应用Id必须唯一,任意小写英文字母或数字组成, 如果应用已经有设计元素修改应用Id会丢失设计元素

状态: 开发中
指定应用当前的开发进度或状态

版本: 1.0

备注:

提交 取消

权限设定为其他权限

应用属性

权限设置

应用管理员: admin X
应用管理员可以调用此应用的所有API服务(不受调用权限的控制)

开发权限: admin X dev01 X
可以对应用的所有设计进行新增、修改、删除的用户, 空表示所有登录用户

API调用权限: core.应用开发权限(系统) X
空表示所有登录用户均可调用本应用的API

匿名调用: ☒ 否 ☐ 是
允许未登录的用户调用本应用的API服务(允许后API调用权限设置将失效)

输出NULL字段: ☒ 否 ☐ 是
默认本应用下的API不输出JSON中为null值的字段,选择是表示本应用下的API需要输出

提交 取消

5、在应用中创建一个接口



接口认证模式设置为appkey认证

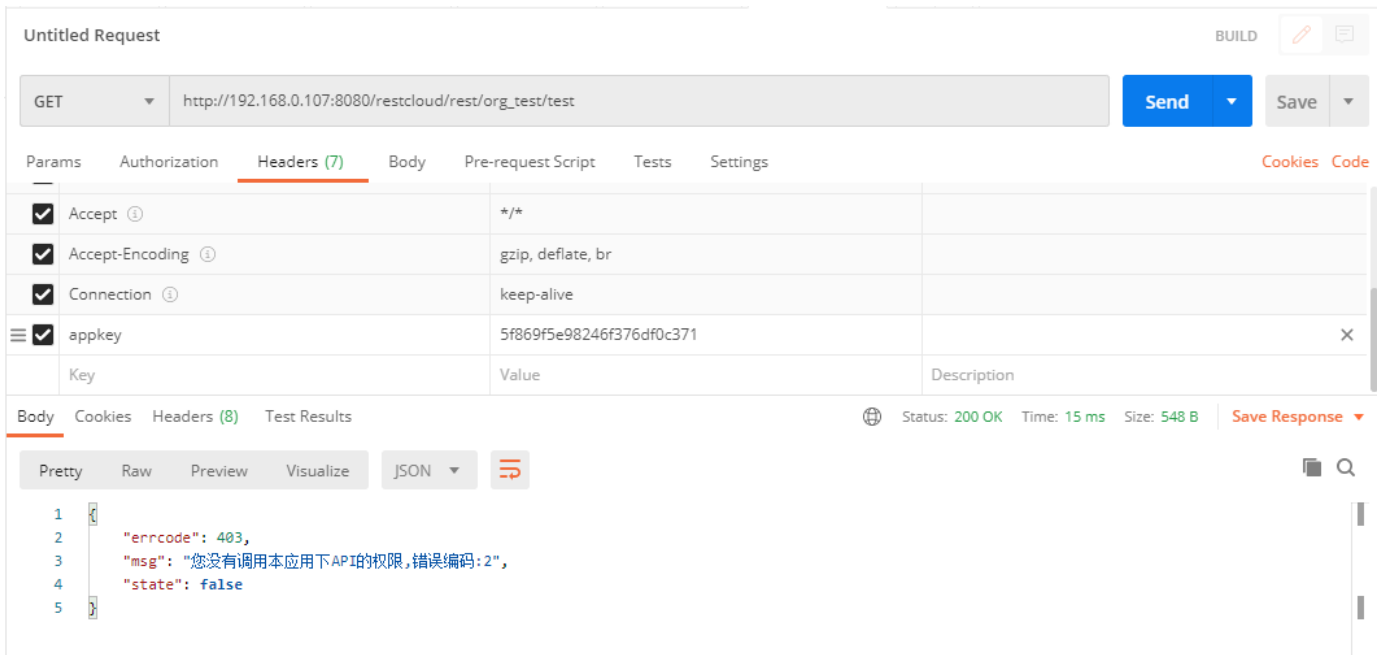
只有关系数据库才支持事务功能

认证方式: ☐ 需要认证(token) ☒ 需要认证(appkey) ☐ 需要审批 ☐ 匿名调用

需要认证表示用户登录后如果有权限则可调用,需要审批表示用户必须申请了API的调用权限才可以,匿名调用表示无需登录直接调用

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

应用管理员:

应用管理员可以调用此应用的所有API服务(不受调用权限的控制)

开发权限:

可以对应用的所有设计进行新增、修改、删除的用户, 空表示所有登录用户

API调用权限:

空表示所有登录用户均可调用本应用的API

匿名调用: ☒ 否 ☐ 是

允许未登录的用户调用本应用的API服务(允许后API调用权限设置将失效)

输出NULL字段: ☒ 否 ☐ 是

默认本应用下的API不输出JSON中为null值的字段,选择是表示本应用下的API需要输出

8、postman中测试

GET

http://192.168.0.107:8080/restcloud/rest/org_test/test

Send

Save

Params

Authorization

Headers (7)

Body

Pre-request Script

Tests

Settings

Cookies

Code

<input checked="" type="checkbox"/>	Accept	*/*	
<input checked="" type="checkbox"/>	Accept-Encoding	gzip, deflate, br	
<input checked="" type="checkbox"/>	Connection	keep-alive	
<input checked="" type="checkbox"/>	appkey	5f869f5e98246f376df0c371	
	Key	Value	Description

Body

Cookies

Headers (8)

Test Results

Status: 200 OK

Time: 13 ms

Size: 463 B

Save Response

Pretty

Raw

Preview

Visualize

JSON

1

调用成功

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

用户属性

权限设置

更多设置

头像

* 所属部门: 研发部 ✓

* 用户名: 开发人员1
用户中文名称

* 用户登录Id: dev01 ✓
必须唯一且注册后不可修改(所有用户建议使用固定长度的字符串作为Id如6位工号等)

帐号类型: 普通用户帐号 ✓
普通用户表示进入本系统进行开发运维的帐号,应用系统帐号表示仅供外部应用查询和调用API使用的帐号

职位: 普通员工 ✓

* 登录密码:
密码建议由大写字母、小写字母、数字、特殊字符组成, 最多30个字符(具体验证规则可在平台参数中配置)

密码有效日期: Select date 
空表示永久有效

提交 取消

2、新建一个权限

权限属性

* 所属应用: core|核心应用 ✓
应用唯一id

* 权限唯一Id: CORE_ACL_201016002 ✓
注意:保存后如果要修改请确认权限没有被引用, 否则引用的对象将会出错

* 权限名称: 可调用应用-权限测试 ✓
指定任何有意义且能描述本权限的名称

备注:

保存并关闭 关闭

3、新建一个角色, 建立权限和账号的关联

*

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

权限应用开发者

CORE_ROLE_201016001

core

1

1001

修改 | 删除

角色绑定权限

角色成员管理

已绑定权限

可用应用-权限测试

可选权限

☐ 显示所有应用的权限

搜索: 搜权限名称或id

权限名称	权限Id	备注	应用	操作
可用应用-权限测试	CORE_ACL_201016001		core	添加
新闻通知管理员	CORE_ACL_191221001		core	添加
应用开发权限(系统)	core.appdesigner	可以进入系统进行应用开发的权限	core	添加
测试开发权限	CORE_ACL_181220001		core	添加
超级管理员权限(系统)	core.superadmin	系统默认的最高级别的权限	core	添加

1-5 of 5 items < 1 > 15

添加账户

权限应用开发者

CORE_ROLE_201016001

core

1

1001

修改 | 删除

角色绑定权限

角色成员管理

保存 | 新增 | 刷新

成员类型	成员Id	成员名称	操作
用户	dev01	开发人员1	删除

< 1 >

4、新建一个应用

应用属性

权限设置

* 所属分类: 开发测试 ▼
请选择应用的所属分类

* 应用名称: 应用权限测试
任意可描述本应用功能或模块的名称

* 应用Id: org_test
应用Id必须唯一,任意小写英文字母或数字组成, 如果应用已经有设计元素修改应用Id会丢失设计元素

状态: 开发中
指定应用当前的开发进度或状态

版本: 1.0

备注:

提交 取消

权限设定为其他权限

应用属性

权限设置

应用管理员: admin X
应用管理员可以调用此应用的所有API服务(不受调用权限的控制)

开发权限: admin X dev01 X
可以对应用的所有设计进行新增、修改、删除的用户, 空表示所有登录用户

API调用权限: core.应用开发权限(系统) X
空表示所有登录用户均可调用本应用的API

匿名调用: ☒ 否 ☐ 是
允许未登录的用户调用本应用的API服务(允许后API调用权限设置将失效)

输出NULL字段: ☒ 否 ☐ 是
默认本应用下的API不输出JSON中为null值的字段,选择是表示本应用下的API需要输出

提交 取消

5、在应用中创建一个接口



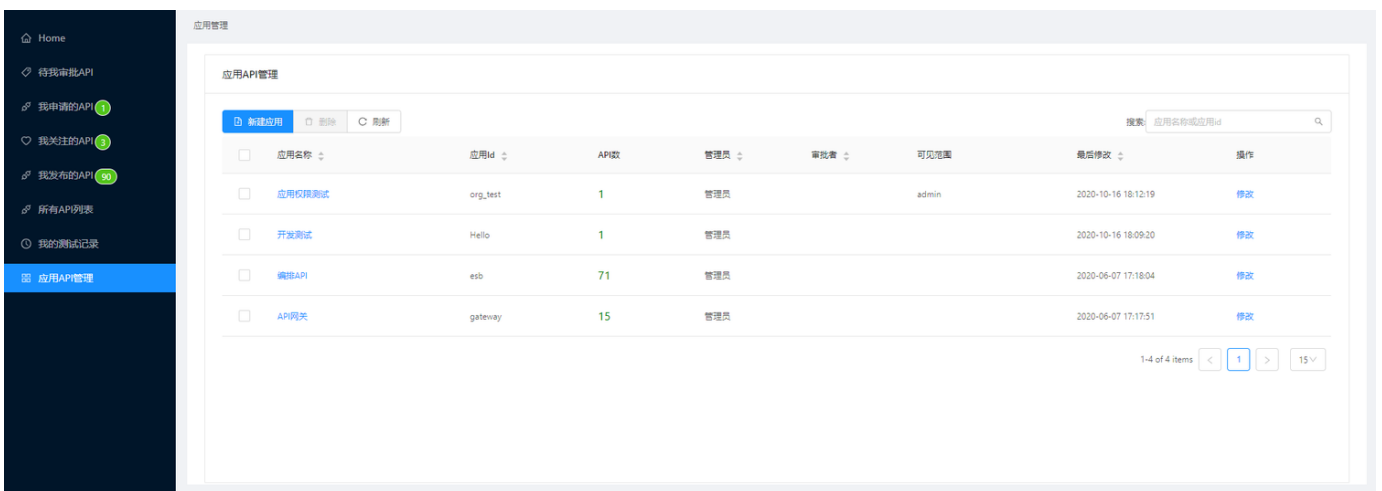
接口认证模式设置为appkey认证

只有关系数据库才支持事务功能

认证方式: ☐ 需要认证(token) ☒ 需要认证(appkey) ☐ 需要审批 ☐ 匿名调用

需要认证表示用户登录后如果有权限则可调用,需要审批表示用户必须申请了API的调用权限才可以,匿名调用表示无需登录直接调用

6、在API管理门户中创建应用



新建一个应用

* 应用名称: 应用权限测试 ✓
建议与API开发平台中的应用名称保持一致

* 应用唯一Id: org_test
如果要与API开发平台的API进行同步则必须与API开发平台中的应用Id保持一致

后端服务器URL:
指定本应用注册的API的后端服务器的基础路径或服务实例多个用逗号分隔(不指定则在注册API时填写全路径)如:http://localhost:8080/api

* 应用管理员: admin X
指定本应用的管理者,管理者可以修改应用属性可以注册API

应用可见范围: admin X
指定本应用的可见范围的用户,空表示所有用户均可浏览本应用中的API

API调用审批: Please select ▼
指定本应用中API调用申请的审批者,如果不指定则由API的发布者进行审批

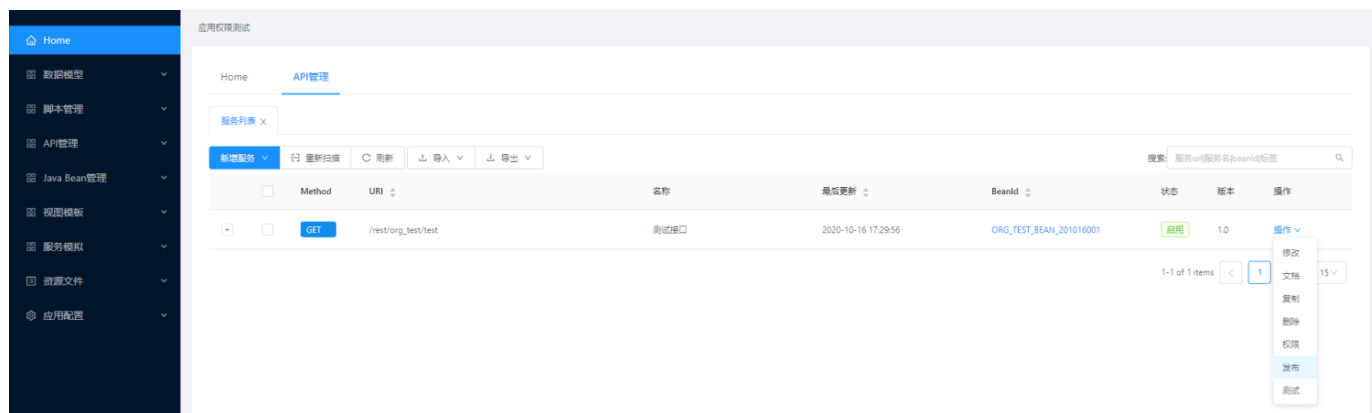
API默认可见范围: Please select
指定本应用下发布的API的默认可见用户

备注:

提交 取消

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

远程服务器:

发布API到其他远程服务器中(如:http://192.168.1.1/restcloud),空表示发布到本机服务器

* API名称:

任意能描述本API的说明

* URL:

注意:如果URI路径已经存在,系统不会重复发布相同URI的API

* 发布应用:

org_test

选择发布到API门户中的应用

发布范围: ☐ 发布本应用下的所有API

同步本应用的下的所有API到API管理平台中

更新选项: ☐ 强制更新

是否强制更新API门户中的API信息?默认会自动检测API是否有变化再决定更新!

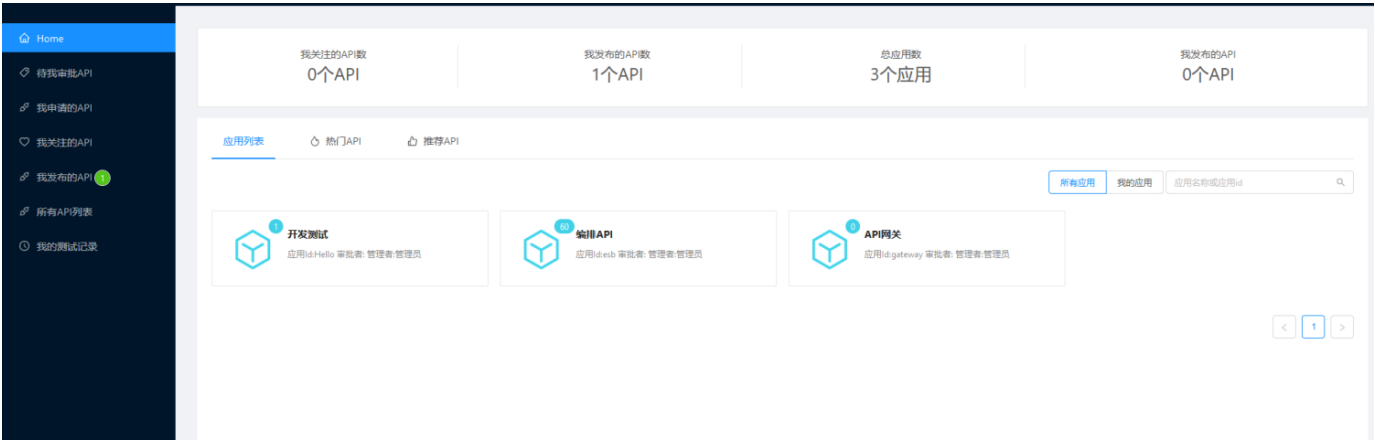
发布说明:

说明本次发布API修改的地方或功能

提交

关闭

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

* 应用名称: ✓
建议与API开发平台中的应用名称保持一致

* 应用唯一Id:
如果要与API开发平台的API进行同步则必须与API开发平台中的应用Id保持一致

后端服务器URL:
指定本应用注册的API的后端服务器的基础路径或服务实例多个用逗号分隔(不指定则在注册API时填写全路径)如:http://localhost:8080/api

* 应用管理员: X
指定本应用的管理者,管理者可以修改应用属性可以注册API

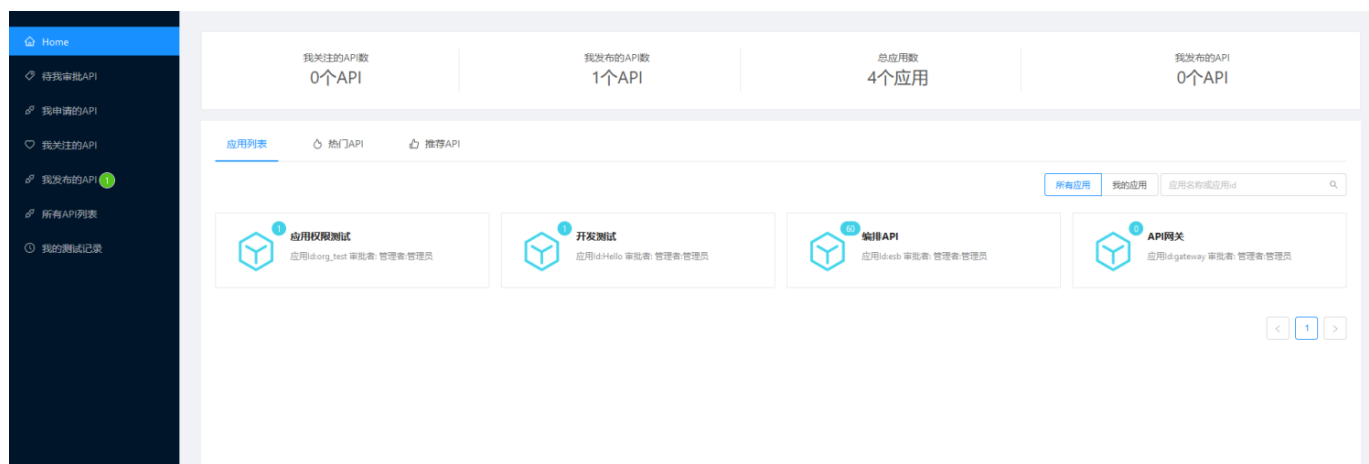
应用可见范围: X X
指定本应用的可见范围的用户,空表示所有用户均可浏览本应用中的API

API调用审批: ▼
指定本应用中API调用申请的审批者,如果不指定则由API的发布者进行审批

API默认可见范围:
指定本应用下发布的API的默认可见用户

备注:

10、第三方应用账户进入管理门户



可看到应用

