**IUAP平台使用指南**

**数据权限组件**

用友网络科技股份有限公司

二○一八年五月

**此文档为保密文档，未经用友软件股份有限公司书面同意，不得向任何单位或个人提供、转让本文档中的任何内容，用友软件股份有限公司将保留对泄漏文档内容的起诉权利。**

**IUAP平台使用指南**

|  |  |  |
| --- | --- | --- |
| 文件状态：  [ ] 草稿  [**√**]正在修改  [] 正式发布 | 文件标识： |  |
| 当前版本： |  |
| 作者： |  |
| 完成日期： |  |

版本历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 作者 | 参与者 | 起止日期 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

审核记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 姓名 | 职位 | 审阅日期 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[第一章业务场景 1](#_Toc515435251)

[1.1系统内置参照权限使用方案 1](#_Toc515435252)

[1.2自定义参照数据权限开发方案 4](#_Toc515435253)

[第二章环境准备 5](#_Toc515435254)

[1.1 开发环境配置 5](#_Toc515435255)

[2.1数据库脚本配置 5](#_Toc515435256)

[2.1.1预置数据 5](#_Toc515435257)

[2.1.2后台代码实现 6](#_Toc515435258)

[2.1.2.1业务表调整 6](#_Toc515435259)

[2.1.2.2数据转换url的实现 6](#_Toc515435260)

[2.1.2.3参照模型配置权限 7](#_Toc515435261)

[2.1.2.4根据数据权限过滤数据 10](#_Toc515435262)

[1.2 前台配置 13](#_Toc515435263)

# 业务场景

## 系统内置参照权限使用方案

此处使用组织和部门作为参照数据权限控制的示例

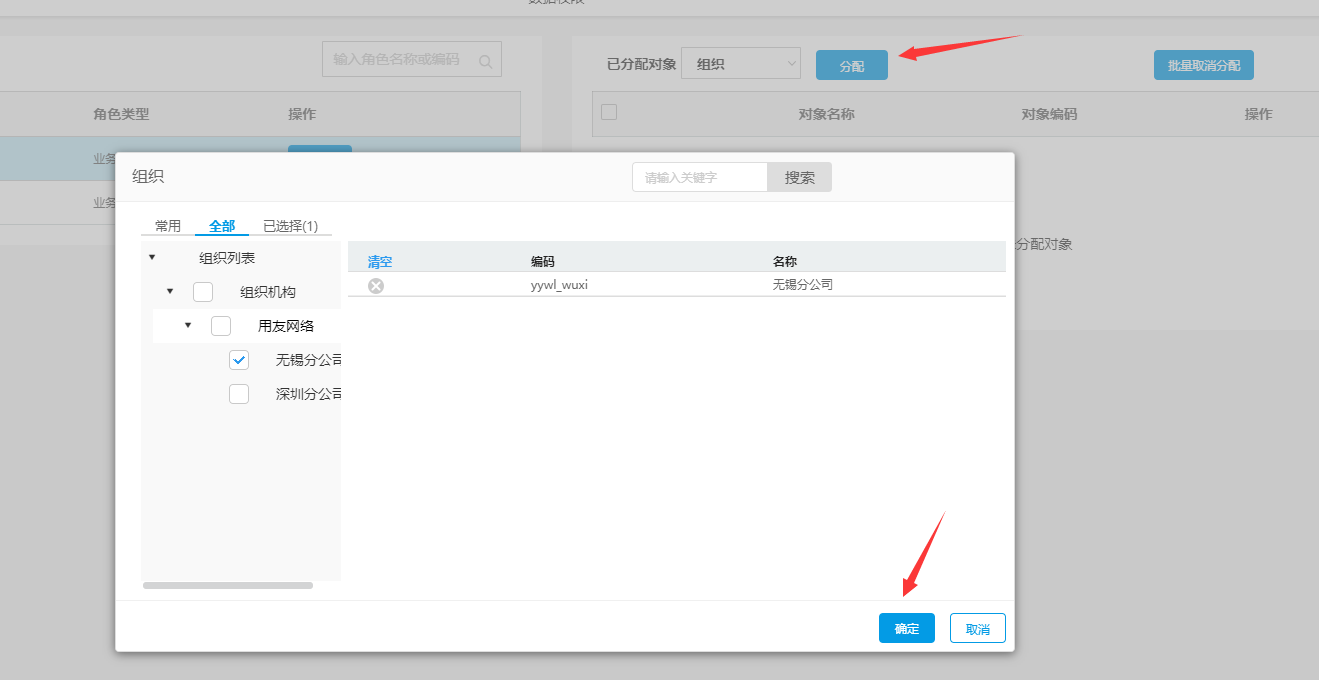
1. 使用系统管理admin登录系统，进入管理中心-数据权限，如下图所示



1. 点击分配对象，会弹出如下弹出框，选择组织，点击确定按钮



1. 在界面中点击分配功能，可以给对应角色分配有权限的组织，分配好组织权限后，点击确定保存。



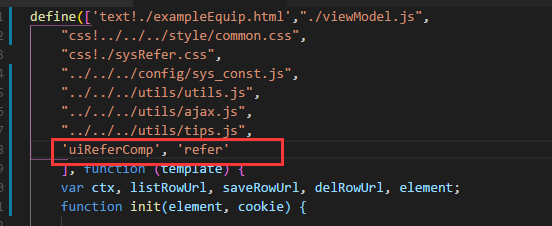


1. 在管理中心 部门中在相应的组织下新建相应的部门。

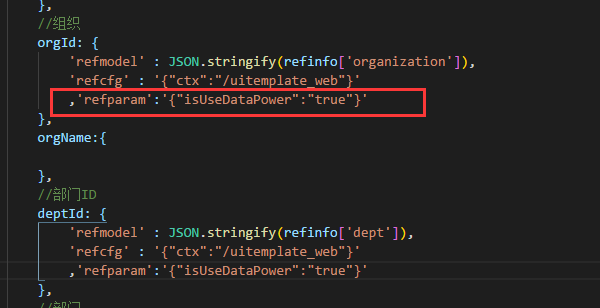




1. 在业务的js代码中要引用参照对应的js



1. 前台配置完毕，还需要在对应的功能节点的viewModel.js中添加启用数据权限的代码，必须加入红色标注的代码，否则权限控制不起作用。



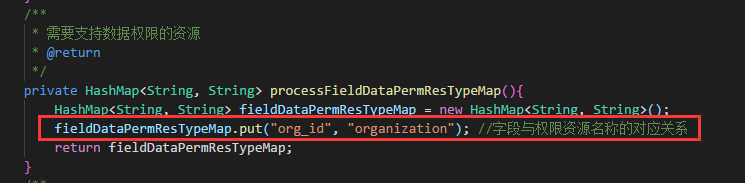
1. 在html页面中要引用的参照应引用如下图所示的uiRefer;切记不要用uiNewRefer，这样配置的数据权限不会生效。

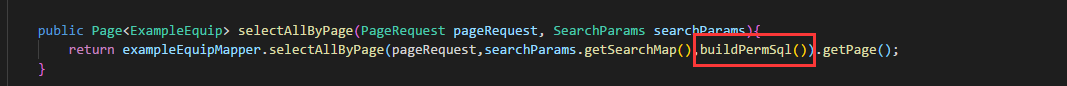


1. 后台页面配置

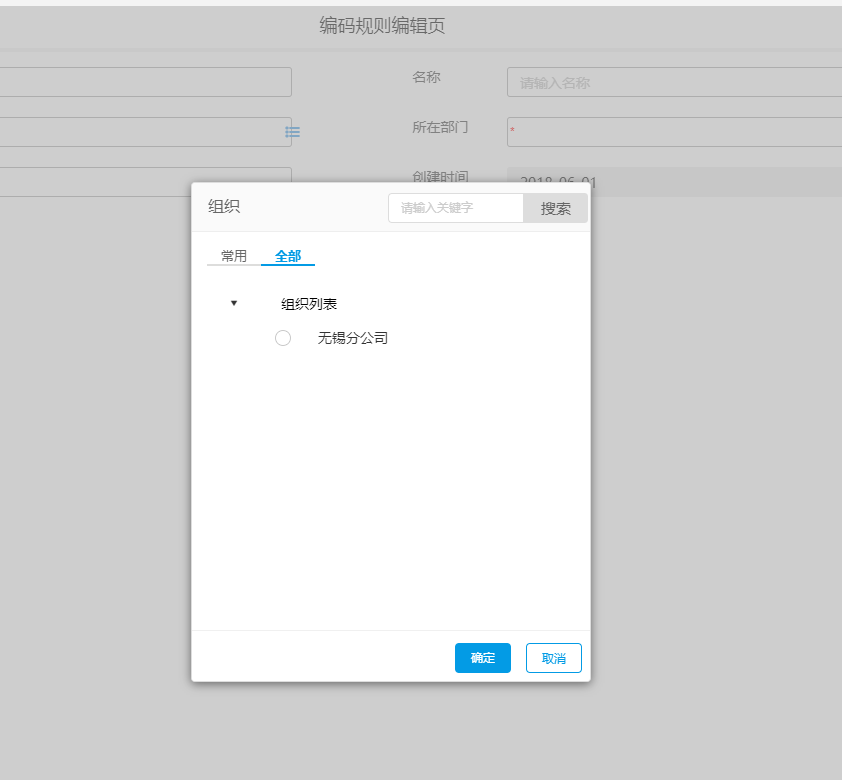
前台配置完毕后,还需要在对应的后台业务代码中增加关于数据权限过滤的功能.这块可以参考后面自定义配置中的1.2.2.4.2中API方法调用的代码。

这里面的fieldDataPermResTypeMap赋值的时候 key 为需要过滤的业务表字段,value为对应的系统内参照的名称。代码详见 com.yonyou.iuap.example.sysRefer.service.ExampleEquipService





8. 前后台配置完毕后，当以业务角色role01的用户user01登录后，在节点上打开功能，加载数据时，按照数据权限过滤，仅能查看有权限访问的数据；点击参照时，只能看到有权限访问的数据

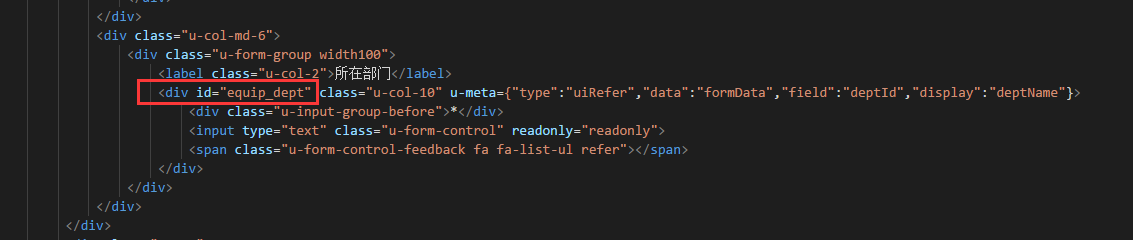


注意：

组织数据权限这块在前台html的u-meta配置中的type 要用uiRefer，否则配置不会生效。

## 1.2系统参照联动

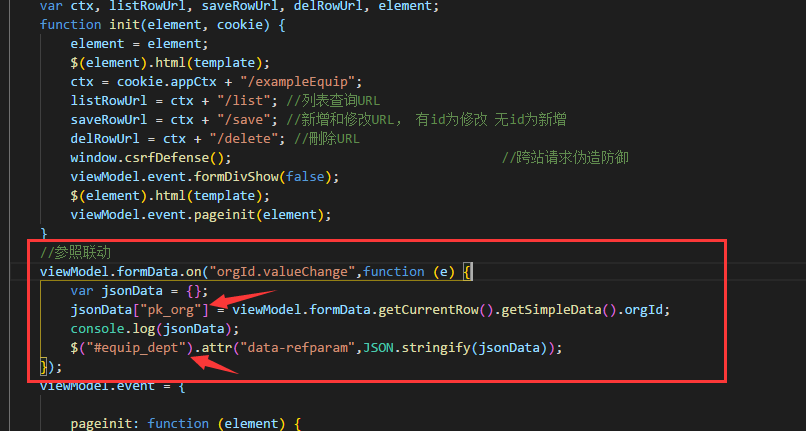
1. 在html页面需要被联动的节点即本例中的部门节点上设置一个id,如下图所示。



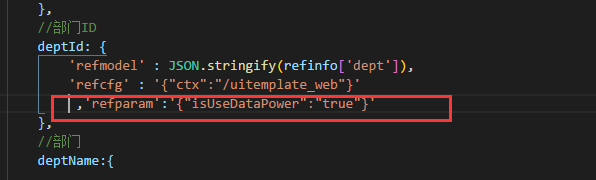
2.在js页面中添加如下代码

其中pk\_org 是 获取组织机构的固定写法;

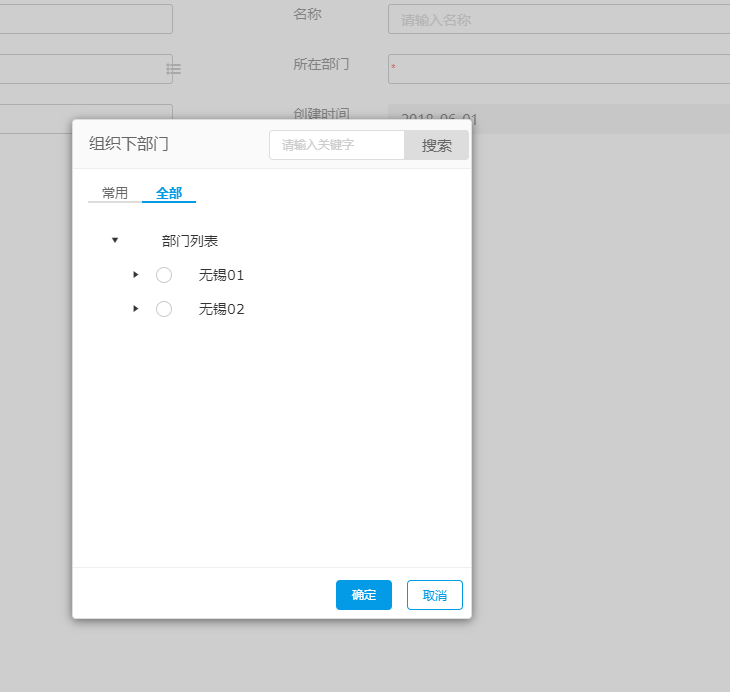
Equip\_dept 为在html中定义的id



3.如果需要对部门也进行数据权限的过滤,则需要在viewModel.js中添加如下内容



4.打开页面选择完组织后,点击部门可以看到如下内容.



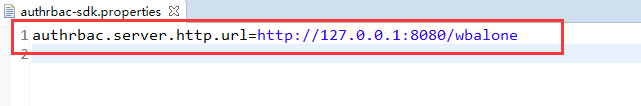
## 1.3自定义参照数据权限开发方案

# 环境准备

## 开发环境配置

**注意事项:**

1.修改项目内 src/resources目录下的authrbac-sdk.properties中的authrbac.server.http.url路径，修改为应用服务器部署的IP，如下图所示



2. 数据权限会用到wbalone项目中的dataConvertCallback.http.url的配置(在wbalone/WEB-INF/classes/application.properties),当开发环境在本地且应用平台和本机不在一起部署的时候,建议在sysconfig.bat或者sysconfig.sh执行的时候将http服务器IP和http服务器端口修改为nginx的地址和端口,这样在分配数据权限的时候才能回调到数据.



3. 需要在业务表中增加 tenant\_id字段，且值必须设置为 “tenant”，具体实现方式可以通过数据库默认值或者在service层保存时设置均可。

## 数据库脚本配置

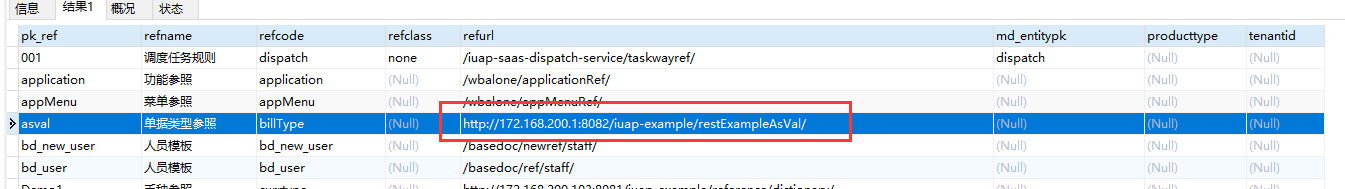
### 预置数据

1. 参照注册ref\_refinfo

注意:因为参照是在本地开发环境中,且应用中心不在本地,所以在要在refurl中加入<http://nginxIP:nginx>端口号或者http://本地开发环境IP:中间件端口号,否则会回调不成功,如果将项目放到应用中心包下,则不需要配置该IP,同时建议这个地方使用IP,不要使用localhost,同时访问的时候尽量使用IP访问.

SQL：

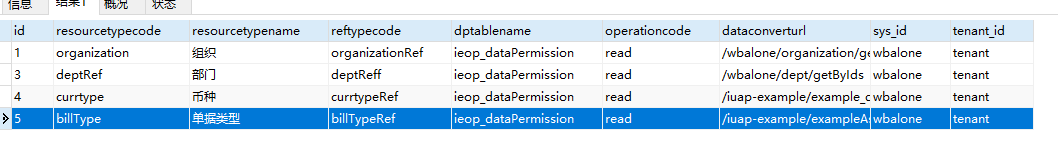
|  |
| --- |
| INSERT INTO `iuap\_test`.`ref\_refinfo` (`pk\_ref`, `refname`, `refcode`, `refclass`, `refurl`, `md\_entitypk`, `producttype`, `tenantid`) VALUES ('asval', '单据类型参照', 'billType', NULL, 'http://172.168.200.1:8082/iuap-example/restExampleAsVal/', NULL, NULL, NULL); |



b. ieop\_dpprofile\_reg权限资源注册表，在表中可以参考已有资源，注册案例中的单据类型资源，如下图所示.

SQL

|  |
| --- |
| INSERT INTO `iuap\_test`.`ieop\_dpprofile\_reg` (`id`, `resourcetypecode`, `resourcetypename`, `reftypecode`, `dptablename`, `operationcode`, `dataconverturl`, `sys\_id`, `tenant\_id`) VALUES ('5', 'billType', '单据类型', 'billTypeRef', 'ieop\_dataPermission', 'read', '/iuap-example/exampleAsVal/getByIds', 'wbalone', 'tenant'); |



resourcetypecode：为用户分配权限后，实现代码的时候要依据此字段来查询权限。

dataconverturl：负责将币种转成应用平台可接受的格式以供应用平台展现数据。在代码部分会有详细介绍。

### 后台代码实现

本例中只会着重介绍关于数据权限相关的代码配置，关于参照的设计文档请先查阅对应的文档。

#### 业务表调整

注意：需要在业务表中增加一个 tenant\_id的字段,在业务表中要增加一个 tenant\_id的字段，因为数据权限过滤的时候会用到；可以通过在数据库层面设置默认值实现或者在service层通过save方法赋值实现。

#### 数据转换url的实现

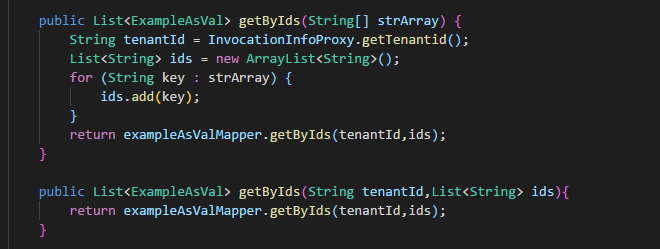
在ExampleAsValController中添加如下方法，即刚才在ieop\_dpprofile\_reg表中配置的dataconverturl方法（具体代码在com.yonyou.iuap.example.asval.web.controller.ExampleAsValController）。

这块代码除了红框中标注的实体类型、属性和getByIds方法需要自己实现外,其他的代码均是固定写法.

1.controller层代码



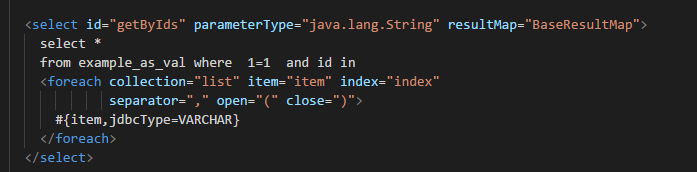
2.service方法



3.dao层



4.mapper.xml文件



#### 参照模型配置权限

参照模型com.yonyou.iuap.example.asval.web.controller.ExampleAsValRefController,在加载数据时判断是否需要支持权限，如果支持则拼接对应权限SQL

1. 在前台viewModel.js中配置启用数据权限（pages/authRefer/userDefRef/viewModel.js）



1. 判断前端传入的参数，是否需要启用数据权限，这段代码复制即可，不需要修改其中的内容。

/\*\*

\* 是否需要启用数据权限,通过当前人角色和前端配置共同判断

\* @param refViewModelVO

\* @return

\*/

private boolean isUserDataPower(RefViewModelVO refViewModelVO){

if(isAdmin()){

return false;

}

boolean isUserDataPower = false;

String clientParam = refViewModelVO.getClientParam();

if(clientParam != null && clientParam.trim().length()>0){

net.sf.json.JSONObject json = net.sf.json.JSONObject.fromObject(clientParam);

if(json.containsKey("isUseDataPower")){

isUserDataPower = json.getBoolean("isUseDataPower");

}

}

return isUserDataPower;

}

/\*\*

\* 判断当前登录人是否为管理员用户

\*/

private boolean isAdmin(){

String userId = InvocationInfoProxy.getUserid();

if("U001".equals(userId)){

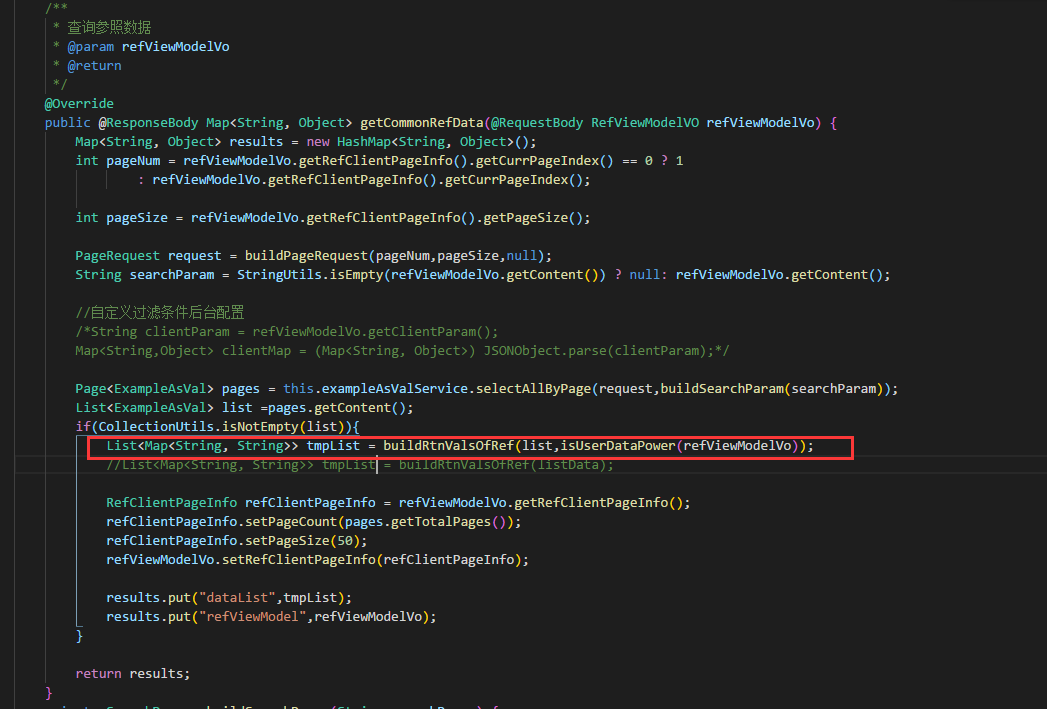
return true;

}

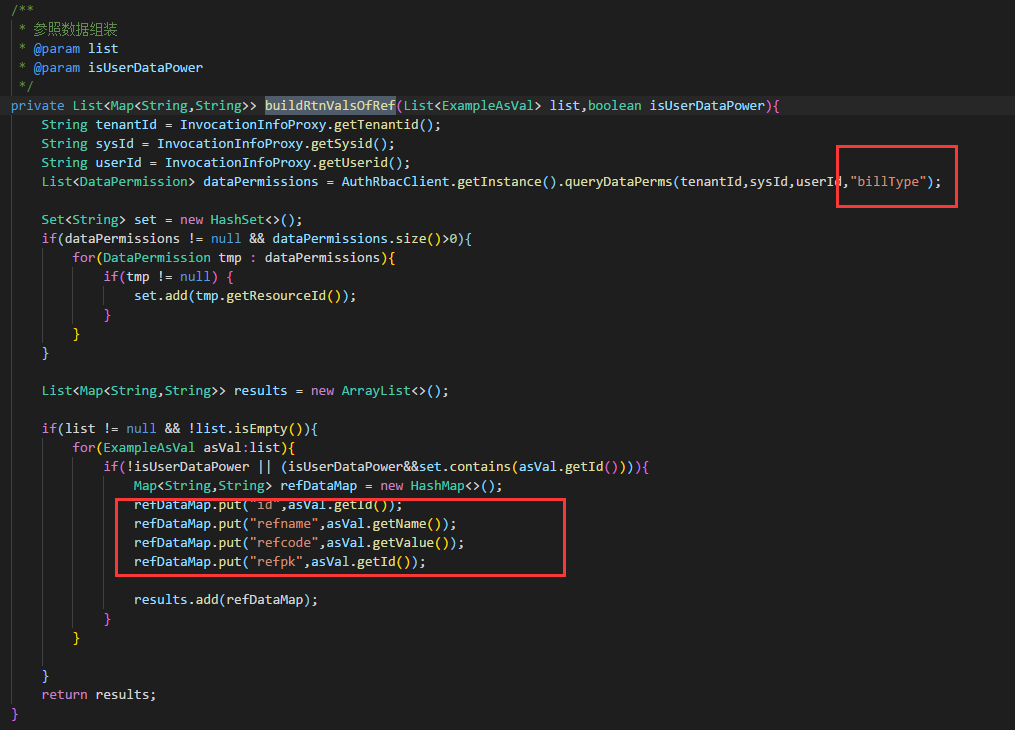
return false;

}

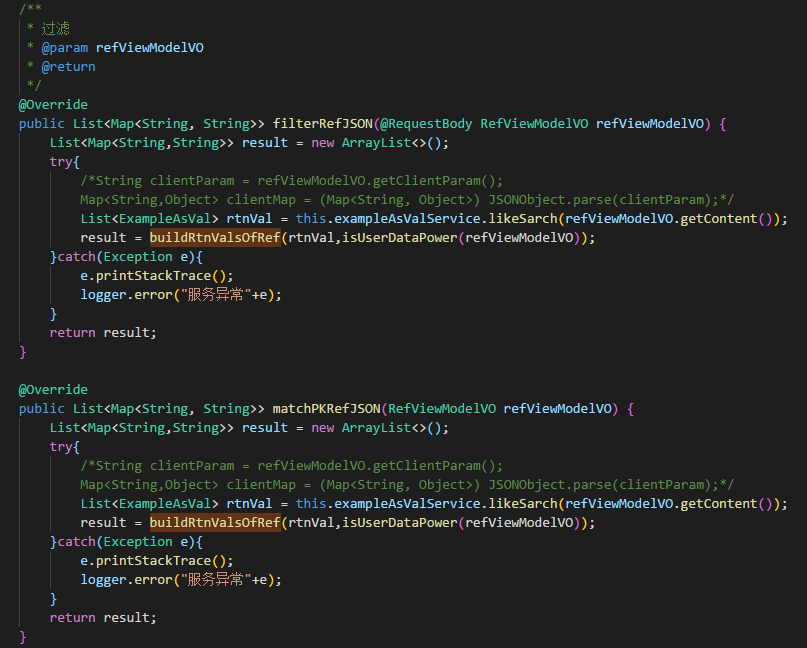
1. 查询或者搜索时加载权限SQL，getCommonRefData方法在原有方法的基础上修改下红色标记处的代码；buildRtnValsOfRef方法中的billType为在1.2.1预置数据中ieop\_dpprofile\_reg.resourcetypecode字段；refDataMap中的数据根据业务表中的实际字段录入,详情可以参考com.yonyou.iuap.example.asval.web.controller.ExampleAsValRefController中的代码内容.

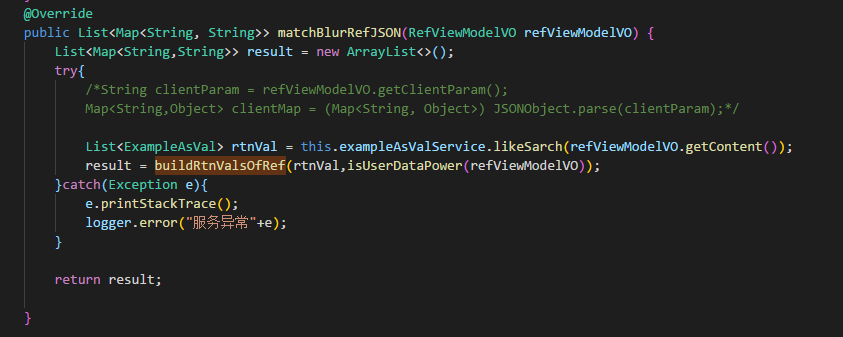


调用权限API查询用户权限，并过滤数据集。



此处的查询方法需要自己根据业务情况重写





#### 根据数据权限过滤数据

业务单据查询时，根据数据权限过滤业务数据

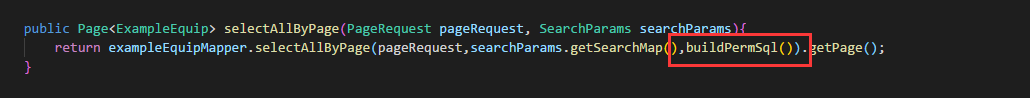
##### 获取数据权限过滤数据API

List<DataPermission> com.yonyou.uap.ieop.security.sdk.AuthRbacClient.queryDataPerms(String tenantId, String sysId, String userId, String resourceTypeCode)

|  |
| --- |
| 查询参数： |
| tenantId租户ID  sysId 系统ID  userId 当前用户ID  resourceTypeCode数据权限资源编码 |
| 返回结果 |
| 返回结果集为有权限的数据权限数组，从如下方法可以获取资源ID  com.yonyou.uap.ieop.security.entity.DataPermission.getResourceId() |

##### API方法调用

1．在分页查询方法中，拼接并传入参数SQL，返回结果集。在service方法中添加如下方法.具体代码详见 com.yonyou.iuap.example.userDefRef.service.ExampleBillService.



2. 拼接SQL代码，这块是固定写法，不需要修改

/\*\*

\* 构造数据权限SQL

\* @return

\*/

public String buildPermSql() {

StringBuilder sqlBuilder = new StringBuilder();

sqlBuilder.append(String.format(" and %s='%s'", CommonConstants.TENANT\_FiELEDNAME, InvocationInfoProxy.getTenantid()));

HashMap<String, String> fieldDataPermResTypeMap = processFieldDataPermResTypeMap();

Set<String> keySet = fieldDataPermResTypeMap.keySet();

Map<String, Set<String>> resTypeDataPermMap = new HashMap<String, Set<String>>();

for (String columnname : keySet) {

String resourceTypeCode = fieldDataPermResTypeMap.get(columnname);

Set<String> set = resTypeDataPermMap.get(resourceTypeCode);

if(set == null){

set = getAuthData(resourceTypeCode);

resTypeDataPermMap.put(resourceTypeCode, set);

}

if(!set.isEmpty()){

sqlBuilder.append(" and ").append(columnname).append(" in (");

for (String param : set) {

sqlBuilder.append(String.format("'%s',", param));

}

sqlBuilder.deleteCharAt(sqlBuilder.length() - 1);

sqlBuilder.append(")");

}

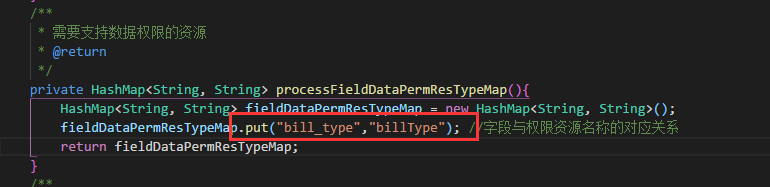
}

String querySql = sqlBuilder.toString();

return querySql;

}

3．返回需要支持数据权限的资源，可以配置多个，配置多个时，在上面方法中需要对多个资源处理，bill\_type为业务表中的字段，配置在该处即为对对该字段进行数据权限的认证，billType为ieop\_dpprofile\_reg表中的resourcetypecode。



1. 调用API获取权限数据,这块直接复制即可,无需修改.

/\*\*

\* 调用API获取有权限的数据

\* @param resourceTypeCode

\* @return

\*/

private Set<String> getAuthData(String resourceTypeCode) {

String tenantId = InvocationInfoProxy.getTenantid();

String sysId = InvocationInfoProxy.getSysid();

String userId = InvocationInfoProxy.getUserid();

List<DataPermission> dataPerms = AuthRbacClient.getInstance().queryDataPerms(tenantId, sysId, userId, resourceTypeCode);

Set<String> set = new HashSet<String>();

for (Iterator<DataPermission> iterator = dataPerms.iterator(); iterator.hasNext();) {

DataPermission dataPermission = (DataPermission) iterator.next();

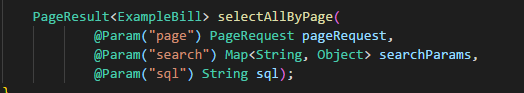
set.add(dataPermission.getResourceId());

}

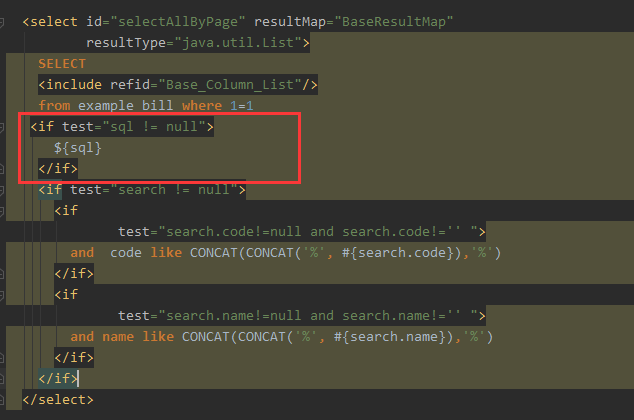
return set;

}

1. Dao层的代码



1. Mapper.xml文件的代码



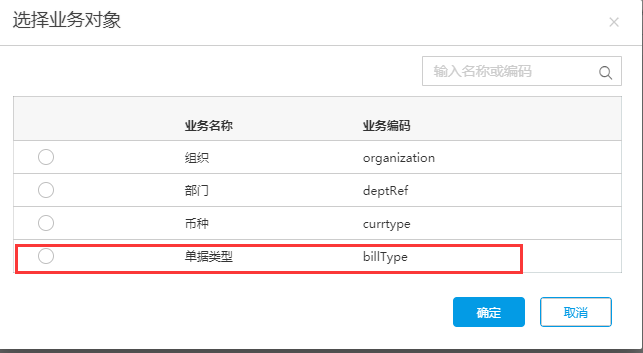
## 前台配置

单据类型中的数据是来自example\_as\_val表中,如果该表中没有数据,可以通过如下SQL语句导入,或者通过前台页面新增保存操作（前台新增需要先配置编码规则）。

SQL语句：

|  |
| --- |
| INSERT INTO `iuap\_test`.`example\_as\_val` (`id`, `pid`, `code`, `name`, `value`, `ord\_index`, `lstdate`, `is\_system`) VALUES ('36455629-8ee5-4ce0-81e0-410ba41f4eb8', 'BILL\_TYPE', null, '财政补助', 'CZSB', '2', '2018-05-31 13:58:34', '1');  INSERT INTO `iuap\_test`.`example\_as\_val` (`id`, `pid`, `code`, `name`, `value`, `ord\_index`, `lstdate`, `is\_system`) VALUES ('b615bb54-fb60-426e-a43d-aedebbbdc1d4', 'BILL\_TYPE', null, '地税', 'DS', '1', '2018-05-31 13:32:51', '0'); |

用系统管理员admin登录，进入管理中心-数据权限；分配权限，选择币种，点击确定，如下图所示



若分配了多个权限，可以在已分配对象处的下拉框中选择



选择单据类型，点击分配，选择需要进行过滤的数据，点击确定；



数据权限分配完后的界面如下图所示



用角色01的用户user01登录，查看票据管理界面

点击新增，查看单据类型，会发现数据权限已经起作用了

