ACL 示例图 （对Entity的控制）

**一、后台**

**要求：**

**1、存档前：**

katie 为 Message的管理员，可以管理任何一条 Message 记录。aru 是普通编辑人员，只能修改自己编写的信息，但是能看其他人的信息。Ken是boss。

**2、存档后**

所有人都没有对 Message 操作的权限(除system和root，更改Message 的Group属性和操作权限)。

用户与组的关系（User & Group）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| User  Group | aru  （编辑） | feila (总编) | yinru （人事） | fion (人事主管) | ken  （Boss） | systems  (系统应用) | root  (所有权限) |
| User （用于登入使用） | √ | √ | √ | √ | √ |  |  |
| admin (每个单独应用管理员) |  |  |  |  | √ |  |  |
| system |  |  |  |  |  | √ |  |
| root |  |  |  |  |  |  | √ |
| News.class (实例默认) | √(C权限) | √(C) |  |  |  |  |  |
| News\_Admin.class (默认) |  | √(C) |  |  |  |  |  |
| User.class |  |  | √ | √ |  |  |  |
| User\_Admin.class |  |  |  | √ |  |  |  |

对象属性（Object ）

|  |  |  |
| --- | --- | --- |
| Object  Mod & Own | Mod | Own (通过业务逻辑细分到字段权限) |
| 存档前Message (访问单条数据) | URD, AR, R  URD, R, -  (OWN, GROUP, OTHERS) | aru : cn.ptp. Message  fion : cn.ptp. Message (指派)  (赋予指定用户权限,多用户) |
| 存档前Message List (访问列表) (默认忽略每条记录的单独权限，如有记录设置为不可读而又不想显示在列表,需客户端单独开发) | R, R, R | system : message (OWN : GROUP) |
| 存档后 Message | R, R, R | system : message |
| 存档后 Message List | R, R, R | system : message |
| News | URD, AR, - (只有message组的用户才可以访问) | aru: News |
| News List | R, R, - (只有用户管理组才可以访问) - | system : news |

C: Create (用户授权时既有，业务控制)，U: Update，R: Read，D: Delete，A: Object\_Admin

**API名称：appCode.package.class eg: www.onionh.com.cn.ptp.News**

**一、前台**

**要求：每个人都可以访问 News，注册用户可以访问 Message, 红钻可以进入Book, 绿钻可以进入 Music，蓝钻可以进入 Video，每个人都可以编辑自己的内容。**

用户与组的关系（User & Group）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| User  Group | kevin | zhuzhu | hong | yolanda | general | red | green | blue |
| general | √ | √ | √ | √ | √ |  |  |  |
| red |  | √ | √ | √ |  | √ |  |  |
| green |  |  | √ | √ |  |  | √ |  |
| blue |  |  |  | √ |  |  |  | √ |

对象属性（Object ）

|  |  |  |
| --- | --- | --- |
| Object  Mod & Own | Mod | Own |
| News | URD, AR, R (OWN, GROUP, OTHERS) | aru: news (仅后台) (OWN : GROUP) |
| News List | R, R, R | system : system |
| Message | URD, AR, -  R, R, -  URD, R, -  R, URD, -  URD, -, -  R, URD, - | aru : message (仅后台,前后台独立表)  general: general (后台上传的)  kevin : general (kevin创建的)  system: message (kevin创建的并发)  zhuzhu: general (zhuzhu创建的)  system: message (zhuzhu创建的并发) |
| Message List | R, R, - | general: general (zhuzhu设置了不许组查看则不显示) |
| Book | R, R, - URD, R, - URD, -, - | red : red (后台上传的情况)  zhuzhu : red (前台用户上传的情况)  hong : red (hong创建的) |
| Book List | R, R, - | red: red (hong设置了不许组查看则不显示) |
| Music | URD, R, - | hong : green (前台用户上传的情况) … |
| Music List | R, R, - | green: green …. |
| Video | R, R, - | blue: blue (后台上传的情况) … |
| Video List | R, R, - | blue: blue … |

C: Create (用户授权时既有，业务控制)，U: Update，R: Read，D: Delete，A: Object\_Admin

**API名称：appCode.package.class eg: www.onionh.com.cn.ptp.News**