

Pi Engine 权限系统设计 原理及用例简介

Permission Design for Pi Engine

姜太文 taiwen@me.com

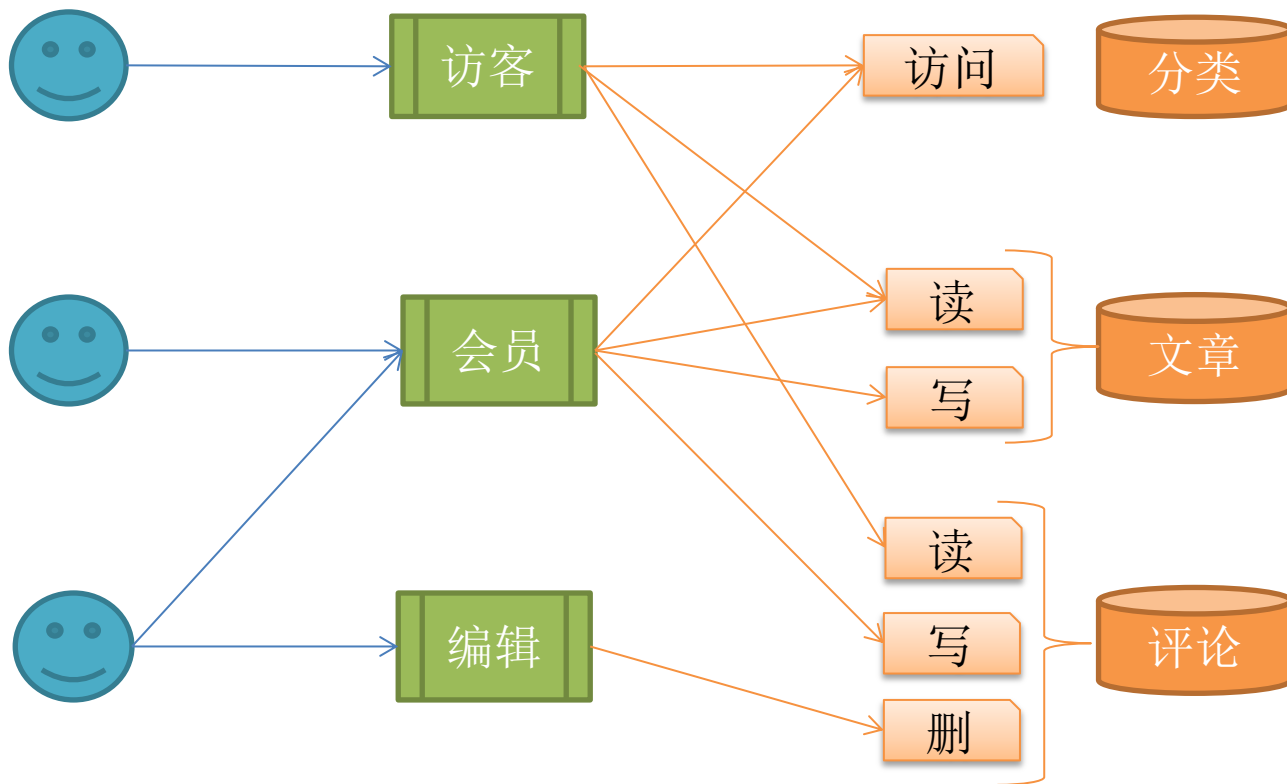
<http://pialog.org>

2014.04

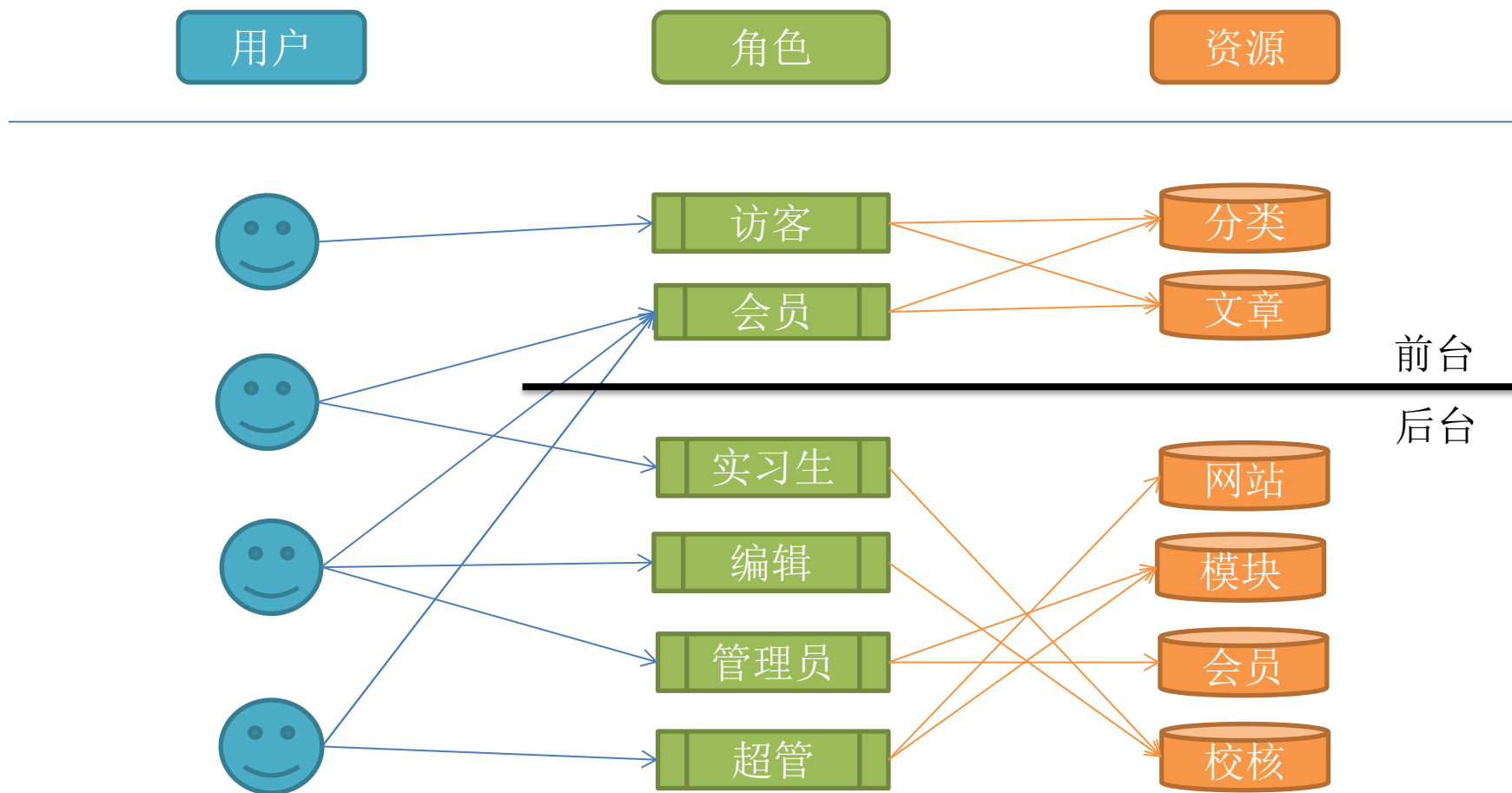
权限控制策略

- **ACL模型：Access Control List**
 - 用户与资源直接直接关联
- **RBAC模型：基于角色的权限控制**
 - 通过角色分配控制资源权限
 - 各种变体
 - 角色分级与继承
 - 角色分组与用户分组
 - 权限约束

RBAC基本原理



RBAC变体及扩展用例：子系统隔离



操作：角色管理(Role)

子系统	名称（编辑）	唯一标识	类型	删除	成员列表
前台	访客（E）	guest	系统		
	会员（E）	member	系统		查看 →
	编辑（E）	editor	定制	删除	查看 →
	版主（E）	moderator	定制	删除	查看 →
	添加角色（A）				
后台	员工（E）	staff	系统		查看 →
	超管（E）	admin	系统		查看 →
	管理员（E）	manager	定制	删除	查看 →
	添加角色（A）				

操作：用户角色分配（UA）

用户 王小明 角色分配：

子系统	角色	操作
前台	会员	
	编辑	取消 x
	版主	赋值 +
	...	
后台	员工	取消 x
	超管	取消 x
	管理员	赋值 +
	...	

操作：权限分配（PA）- 前台

前台

后台

	会员	测试	游客	版主	
模块全局权限					
模块操作	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
模块管理	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
模块权限资源					
全局公开资源	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
仅游客可见	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
仅会员可见	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
区块					
基本信息	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
用户管理	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
用户账号	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>
登录	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div><div></div></div>

操作：权限分配（PA）- 后台

前台

后台

员工

管理员

超管

模块全局权限

模块操作



模块管理



模块权限资源

总体权限



操作：模块



操作：主题



操作：导航



操作：角色



操作：维护



管理：配置



管理：区块



操作：资源定义

- Meta 预定义方式
 - 名称
 - 唯一标识
 - 适用于已知或可遍历的资源
- 动态Callback方式
 - 类型名
 - 类型标识
 - Callback定义
 - 适用于动态变化资源，如文章按分类控制