链滴

RBAC 权限管理系统设计思路

作者：alex18595752445

原文链接：https://ld246.com/article/1584865461083

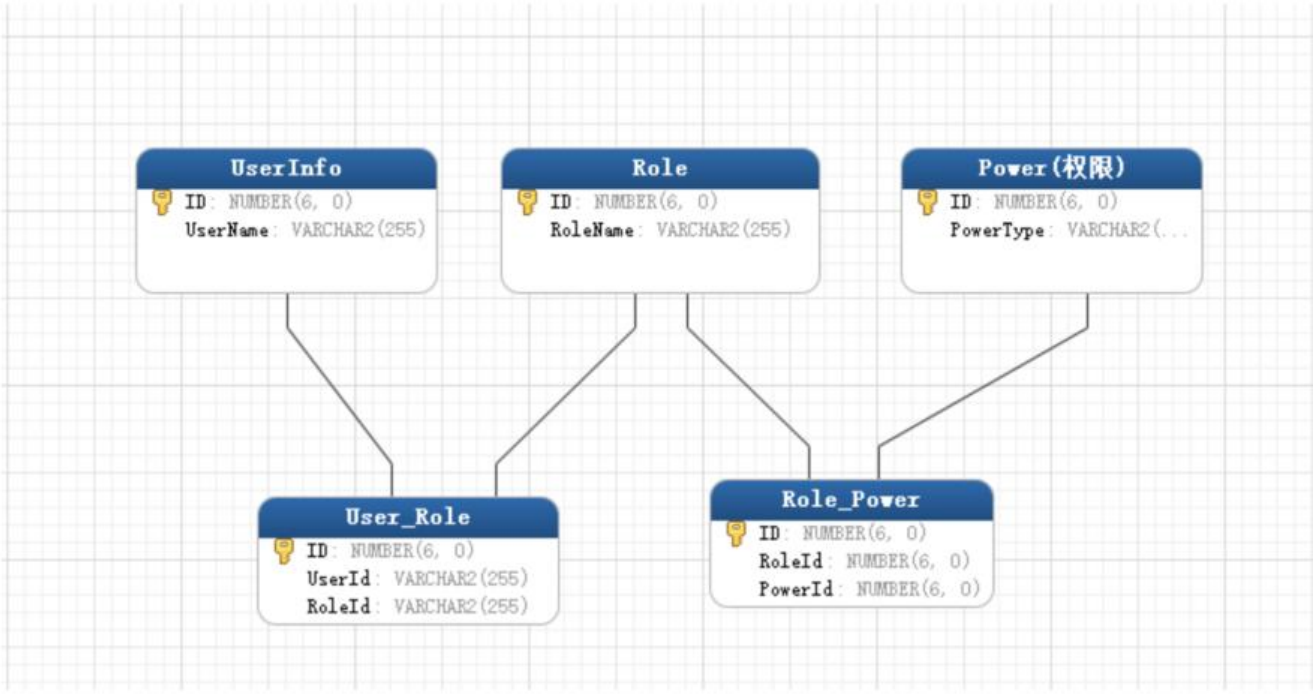
来源网站：链滴

RBAC 权限管理系统设计思路

作者：不哼不哈

博客园：cnblogs.com/myindex/p/9116177.html

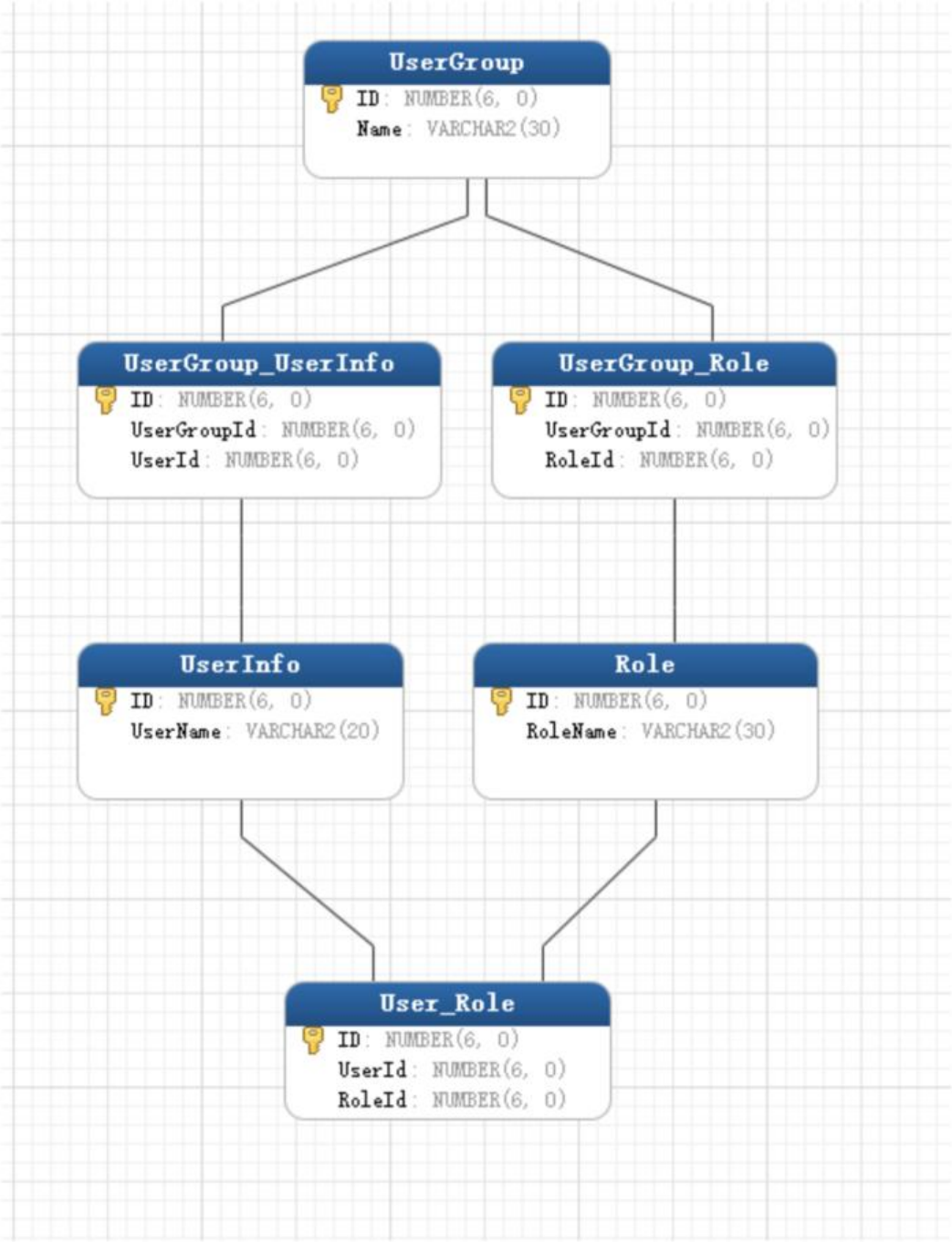
我们比较常见的就是基于角色的访问控制，用户通过角色与权限进行关联。简单地说，一个用户拥有个角色，一个角色拥有多个权限。这样，就构造成“用户-角色-权限”的授权模型。在这种模型中，户与角色之间、角色与权限之间，通常都是多对多的关系。如下图：



基于这个，得先了解角色到底是什么？我们可以理解它为一定数量的权限的集合，是一个权限的载体

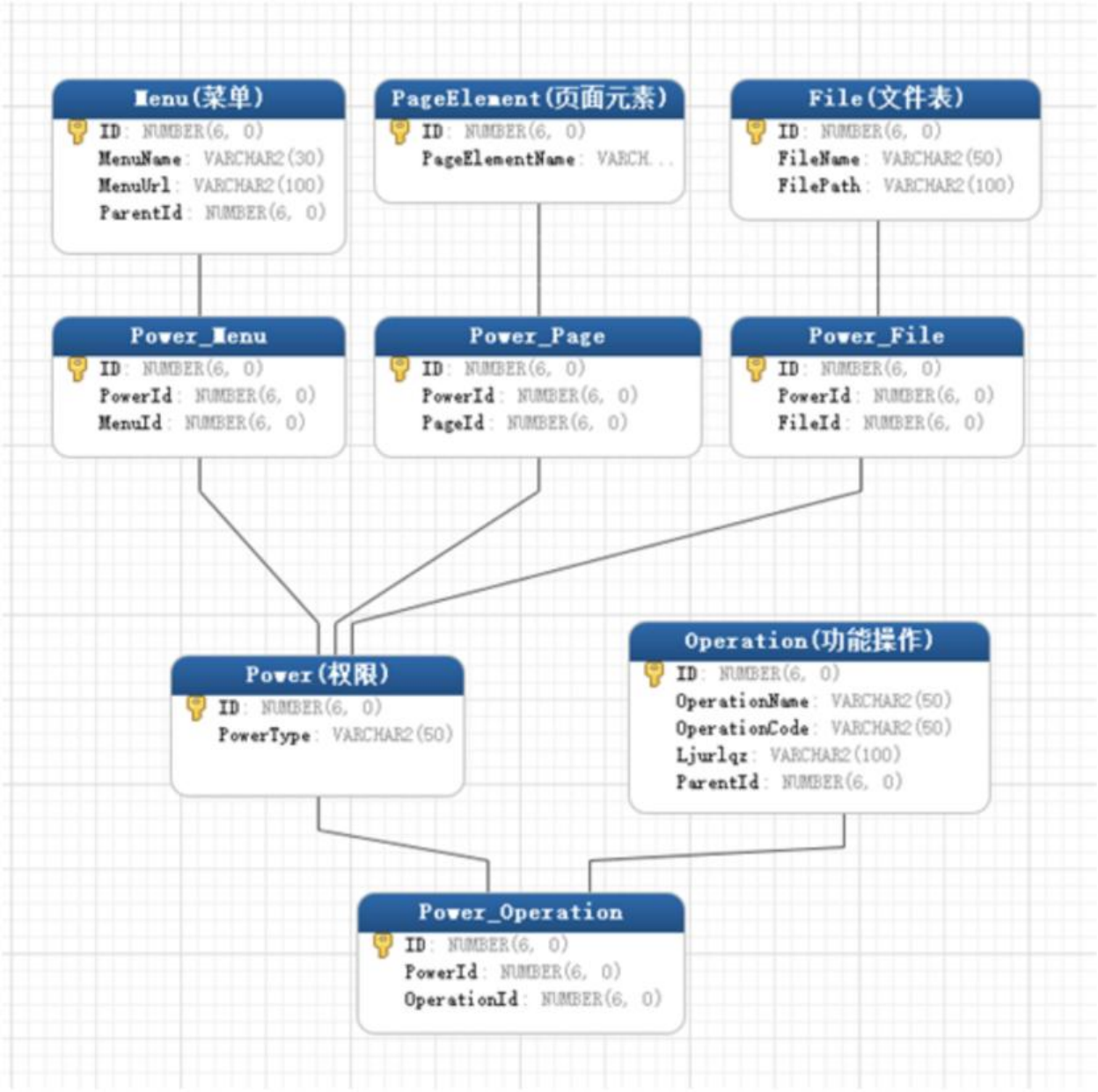
例如：一个论坛的“管理员”、“版主”，它们都是角色。但是所能做的事情是不完全一样的，版主能管理版内的贴子，用户等，而这些都是属于权限，如果想要给某个用户授予这些权限，不用直接将限授予用户，只需将“版主”这个角色赋予该用户即可。

但是通过上面我们也发现问题了，如果用户的数量非常大的时候，就需要给系统的每一个用户逐一授权分配角色)，这是件非常繁琐的事情，这时就可以增加一个用户组，每个用户组内有多个用户，除了给个用户授权外，还可以给用户组授权，这样一来，通过一次授权，就可以同时给多个用户授予相同的限，而这时用户的所有权限就是用户个人拥有的权限与该用户所在组所拥有的权限之和。用户组、用与角色三者的关联关系如下图：



通常在应用系统里面的权限我们把它表现为菜单的访问(页面级)、功能模块的操作(功能级)、文件上传删改，甚至页面上某个按钮、图片是否可见等等都属于权限的范畴。有些权限设计，会把功能操作作一类，而把文件、菜单、页面元素等作为另一类，这样构成“用户-角色-权限-资源”的授权模型。而

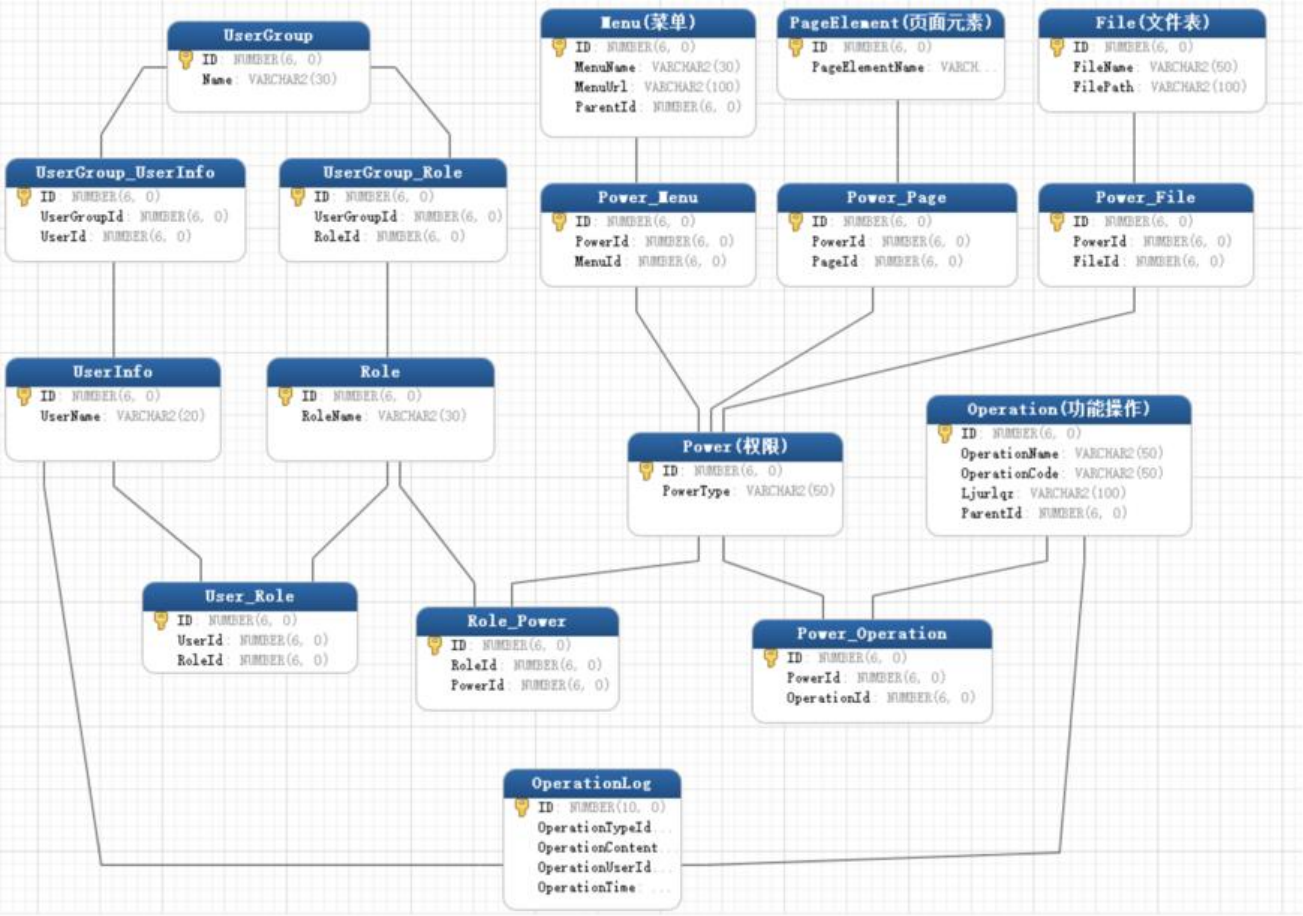
做数据表建模时，可把功能操作和资源统一管理，也就是都直接与权限表进行关联，这样可能更具便性和易扩展性。如下图：



这里特别需要注意以下权限表中有一列“PowerType(权限类型)”，我们根据它的取值来区分是哪一权限，可以把它理解为一个枚举，如“MENU”表示菜单的访问权限、“OPERATION”表示功能模的操作权限、“FILE”表示文件的修改权限、“ELEMENT”表示页面元素的可见性控制等。

这样设计的好处有两个。一、不需要区分哪些是权限操作，哪些是资源，（实际上，有时候也不好区，如菜单，把它理解为资源呢还是功能模块权限呢？）；二、方便扩展，当系统要对新的东西进行权控制时，我只需要建立一个新的关联表“权限 XX 关联表”，并确定这类权限的权限类型字符串即可。

需要注意的是，权限表与权限菜单关联表、权限菜单关联表与菜单表都是一对一的关系。（文件、页权限点、功能操作等同理）。也就是每添加一个菜单，就得同时往这三个表中各插入一条记录。这样可以不需要权限菜单关联表，让权限表与菜单表直接关联，此时，须在权限表中新增一列用来保存菜的 ID，权限表通过“权限类型”和这个 ID 来区分是种类型下的哪条记录。最后扩展出来的模型完整计如下图：



注意上面我额外增加了一个操作日志表；

随着系统的日益庞大，为了方便管理，如果有需要可引入角色组对角色进行分类管理，跟用户组不同角色组不参与授权。例如：当遇到有多个子公司，每个子公司下有多个部门，这是我们就可以把部门解为角色，子公司理解为角色组，角色组不参于权限分配。另外，为方便上面各主表自身的管理与查，可采用树型结构，如菜单树、功能树等，当然这些可不需要参于权限分配。

数据字典

1. 用户表：

用户信息表(UserInfo)			
字段名称	字段	类型	备注
用户ID	ID	Int	PK not null
用户名	UserName	Varchar(20)	not null

2. 角色表：

角色表(Role)			
字段名称	字段	类型	备注
角色ID	ID	Int	PK not null
角色名	RoleName	Varchar(30)	not null

3. 用户与角色关联表

用户与角色关联表(User_Role)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
用户ID	UserId	Int	FK not null
角色ID	RoleId	Int	FK not null

4. 用户组表

用户组表(UserGroup)			
字段名称	字段	类型	备注
用户组ID	ID	Int	PK not null
用户组名	UserGroupName	Varchar(30)	not null

5. 用户组与用户信息关联表

用户组与用户信息关联表(UserGroup_UserInfo)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
用户组ID	UserGroupId	Int	FK not null
用户ID	UserId	Int	FK not null

6. 用户组与角色关联表

用户组与角色关联表(UserGroup_Role)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
用户组ID	UserGroupId	Int	FK not null
角色ID	RoleId	Int	FK not null

7．菜单表

菜单表(Menu)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
菜单名称	MenuName	Varchar(30)	not null
菜单URL	MenuUrl	Varchar(100)	
菜单父ID	ParentId	Int	

8. 页面元素表

页面元素表(PageElement)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
页面元素名称	PageElementName	Varchar(100)	not null

9. 文件表

文件表(File)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
文件名称	FileName	Varchar(50)	not null
文件路径	FilePath	Varchar(100)	

10. 权限表

权限表(Power)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
权限类型	PowerType	Varchar(50)	not null

11. 权限与菜单关联表

权限与菜单关联表(Power_Menu)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
权限ID	PowerId	Int	FK not null
菜单ID	MenuId	Int	FK not null

12. 权限与页面元素关联表

权限与页面元素关联表(Power_Page)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
权限ID	PowerId	Int	FK not null
页面元素ID	PageId	Int	FK not null

13. 权限与文件关联表

权限与文件关联表(Power_File)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
权限ID	PowerId	Int	FK not null
文件ID	FileId	Int	FK not null

14. 功能操作表

功能操作表(Operation)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
操作名称	OperationName	Varchar(50)	not null
操作编码	OperationCode	Varchar(50)	
拦截URL前缀	Ljurlqz	Varchar(100)	
操作父ID	ParentId	Int	

15. 权限与功能操作关联表

权限与功能操作关联表(Power_Operation)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
权限ID	PowerId	Int	FK not null
操作ID	OperationId	Int	FK not null

16. 角色与权限关联表

角色与权限关联表(Role_Power)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
角色ID	RoleId	Int	FK not null
权限ID	PowerId	Int	FK not null

17. 操作日志表

操作日志表(OperationLog)			
字段名称	字段	类型	备注
ID	ID	Int	PK not null
操作类型Id	OperationTypeId	Int	FK not null
操作内容	OperationContent	Varchar(500)	
操作用户ID	OperationUserId	Int	FK not null
操作时间	OperationTime	Date	