一、权限管理服务

1、整体方案思路

基于成熟的RBAC权限管理模型去做

账号：其实就是电商公司里所有员工都需要具有的一个账号

角色：通常是根据部门里的职位来划分，一个部门里的一个职位对应一个角色，比如会员运营、产品经理、售前客服、采购专员，等等

权限：每个角色都分配对应的权限，权限实际上是3个东西（菜单、按钮、页面链接）

我这里给大家说一个case，例子，就知道权限管理是干嘛的了

就比如说采购部的采购专员，这是一个职位

电商公司里肯定会招聘对应的采购专员

（1）他应该是根据公司里预定的采购规划和流程，每隔一定时间，就会去采购一些商品。每个季度需要采购一批衣服，或者是什么鞋子，之类的东西

（2）采购专员可能就会去创建采购单，使用采购中心里面的采购管理服务提供的对应的功能

（3）采购单出来之后，他会打印出来那个采购单，然后跟对应的供应商去走线下的采购流程，说我要采购这些东西，你给我发货到什么仓库里面，每个商品采购多少件，采购价格是多少

（4）采购专员会负责维护供应商的关系和数据

他需要使用电商系统里的哪些功能？

可以想到的一点是，他肯定不是说所有的功能都需要使用，同时有权限使用的。比如说订单中心，采购专员，公司里有哪些订单，跟他是没有关系的

所以他是不能去搞这个订单的，查询公司里所有的订单，订单也是属于机密性的数据

采购中心-供应商管理

采购中心-采购管理

所以对于我们来说，权限管理，就是说，对公司里不同部门的员工，你给他一个账号

比如说有个员工叫张三，分配一个账号，用户名一般是英文的，zhangsan。如果公司里有多个叫在张三的人，那么就按照先来后到的顺序，叫zhangsan01，zhangsan02，zhangsan45

给他分配一个角色，叫做，采购专员，一般来说，对这种后台系统而言，角色都是跟部门的岗位相关联的

采购专员，这个角色，我们给分配哪些权限呢？可以访问采购中心-供应商管理，这个菜单，对这个菜单出来的界面中，会有一些按钮，创建供应商，删除供应商，审核供应商，上传采购合同。对这个界面中的一些按钮，也可以分配权限，有没有权限去看到这个按钮。

如果说按照最简单的理解，权限就是菜单和按钮，如果他没权限访问比如说订单中心-订单查询这个功能模块，那么这个菜单他直接就看不到。

如果他没有权限在供应商管理界面中，执行删除供应商的操作，那么他就看不到删除供应商的那个按钮

一个系统，他左侧的菜单栏+界面中的按钮，菜单和按钮，就是电商系统里所有的权限

不同的岗位给分配不同的角色，不同的角色就有不同的权限，可以访问不同的菜单栏和不同的按钮

注意点1：给某个账号分配了一个角色之后，可以在此之外，再额外选择授予该角色没有的权限

权限没什么好说的，可能有的同学会觉得权限会比较复杂，根据一个具体的大型的集团公司里，设计一个复杂的权限系统

一个通用的权限系统，就这样吧，我觉得这块，就是很多j2ee就业培训里，都会去讲解这个权限管理，CRUD和授权，认证

我们的需求分析包括什么

正儿八经，如果你干过码农，你应该知道一个角色，叫做产品经理，简称为PM，product manager

一般来说，都是产品经理会设计好一整套的系统的产品设计文档，不是我们来写的，产品经理来写的，对于我们而言，最主要的是去深刻理解产品经理写好的产品设计文档（PRD，Product Requirement Document）

针对PRD做一个事情，叫做需求评审，这个需求评审，一般是怎么玩儿的呢？就是一个PM写好一份文档，然后在会议室里做一整天，给RD（Resource Developer），大型互联网公司里，常用的一些口头语。去讲解业务需求，PM在公司里会扮演我这个课程的一个角色。我现在就是在给大家去讲解这个具体的业务需求。这个事情实际上在公司里应该不是架构师、或者技术经理，是PM去干的。

我在这里扮演了PM的角色

PRD，有很多种形式，没有固定形式的，很多同学如果看了以后，不要去计较一些细节

实际上根据公司的规范不同，行业不同，PM的经验和风格不同，PM的喜好不同，出来的产品设计文档，都是不一样的

PRD，是没有固定格式的，随PM的情况和公司规范、行业不同去写

但是一般来说，PRD主要就是定义清楚，这个产品的一个架构，包括了哪些功能模块，这个功能模块图，类似于我上上一讲，讲解的那个大图，就是一个电商系统架构图

实际上那个图，一般在PRD里是第一个图，给人一个全景式的一个概览，包含了哪些功能模块

然后一般PRD需要有另外一个图，完整的业务流程图，类似于我上一讲讲解的那个图，就是各个功能模块随着这个产品实际的用户使用场景，具体的一个流程是怎么样的，看了这个图，就知道这个系统的调用是如何流转的，具体是干嘛的

对每个子系统，每个功能模块，都做具体的阐述和说明：

（1）原型图，一般是PM用Axure去画的，原型图，就是那个后台系统的前端页面

（2）功能流程图，这个功能模块，整体的一个工作流程是什么，跟其他模块的交互关系是什么

（3）对功能流程图中的每个环节做详细的文字说明，流程中的每个环节，什么时候触发，具体要干什么，数据流转有哪些字段

但是我这里做一点说明，我不画原型图，其实之前我们有学员给我反馈过，原型图画出来

我规划了多少个模块，服务

如果要我手画所有的原型图，类似一个PM那样，就这点儿工作量，估计得耗费我一个月

原型图画起来很慢的，画图，是个慢工出细活儿，不是开玩笑的

对每个功能模块：功能流程图，需求说明（要求是给出清晰的功能使用说明，还有每个环节的详细说明，还有每个数据的字段）

那么我角色就足够了，我们是讲解的是java架构师，实际上来说，在真正的大公司里，前后端分离的，我们后端架构师，关注的主要是后端架构和技术，不是这个前端

我们在这里，对前端页面，我们不做任何开发，纯粹凭借自己的想象，主要关注的功能执行的流程，数据的流转，业务的一些细节.

2、需求分析

2.1 权限管理

需要去对权限进行增删改查，这是一个树形结构，比如：采购中心-供应商管理-添加供应商

每个权限包含的字段都有：权限ID，权限编号（比如说PURCHASE，SUPPLIER\_MGR，ADD\_SUPPLIER），权限的名称（采购中心），父权限ID，URL（每个权限点击菜单，还是点击按钮，都会向一个URL发起请求），备注（COMMENT）

用脑海去想象一下，对权限进行增删改查的时候，是要维护一个树形的东西的，比如添加一个子节点，编辑一个子节点，删除一个子节点，每个子节点就是一个权限

如果要控制有些人登录之后，根据权限去显示左侧的菜单栏，树形的菜单，大家可以想象一下，怎么实现：

（1）一个账号登录之后，根据这个账号分配到的角色以及对应的权限，查出来一个权限的集合。看一下里面根权限（父权限ID是NULL），那么就是左侧菜单栏的一级菜单（采购中心）。然后对每个一级菜单，去查询下面的 二级菜单（供应商管理、采购管理）

（2）如果点击了一个菜单之后，会进入一个界面，对界面上的每个按钮，都需要根据是否有这个按钮的权限（添加供应商，ADD\_SUPPLIER）去决定是否显示，查到这个账号是否对这个权限（ADD\_SUPPLIER）的授权

（3）也许你可以控制不显示出来一些菜单和按钮，但是有些为非作歹的人，也许会直接通过浏览器访问一个URL，来尝试进入某个界面，所以说对所有URL的访问请求，需要做权限控制，看一下他对那个URL是否有权限

每次如果电商后台系统开发好了一个新的功能模块之后，都需要在这个权限管理中进行新增和配置，同时将权限分配给对应的角色

根据实际的使用梳理出来对应的一些操作

（1）左侧可以有一个菜单：权限中心-权限管理-权限管理

（2）点击权限管理进入一个界面，看到的是一棵树，此时需要将整颗权限树给查询出来，显示在界面上

（3）支持这个权限树的一个ajax异步加载，就是刚开始就是查询出来所有的根节点

（4）在前端页面上，点击一个节点，会将这个这个节点下面的直接子节点给查询出来

（5）可以直接在前端界面上，对这颗权限树进行编辑，包括节点的增删改，就是可以对已有的节点，添加根节点，编辑一个节点的信息（点击那个节点，在右侧会出来一个表单，显示出来这个节点的具体信息），删除一个节点；还可以添加子节点；这个全部在前端做，跟我们没有关系

（6）编辑完权限树之后，可以保存权限树，这个时候，我们需要对权限树进行保存，传递过来一个树形结构一个数据结构。我们需要对这个数据结构去进行遍历，看哪些是新增的节点，要插入；哪些节点被编辑过了，要修改；跟数据库中现在的权限树做一下对比，如果有节点被删除了，我们需要删除那些节点

2.2 角色管理

角色增删改查/状态的启用和停用

角色包含的一些字段：角色ID，角色编号（PURCHASE\_STAFF），角色名称（采购专员），备注，是否启用（启用，停用）

每个角色，可以分配一些权限

所以需要一个中间表，角色跟权限是多对多的

角色-权限的中间表：ID，角色ID，权限ID

（1）有一个菜单，权限中心-权限管理-角色管理

（2）点击角色管理，进入一个角色列表页面，这个页面里，展示出来角色所有的字段，是支持对角色列表分页查询，支持条件筛选（角色编号，角色名称，是否启用）

（3）角色列表上面有一个按钮，叫做添加角色，点击，会进入一个添加角色的界面，一个表单，在里面可以去填写角色的一个信息；添加角色的界面上，还会出来一颗权限树，在这个树上可以去勾选，要分配给这个角色的权限

（4）点击保存，可以执行一个添加角色的操作，包括角色自己的信息插入表中，然后角色跟各个权限的关联关系，插入那个中间表中

（5）在这个角色列表中，最右侧一栏，是操作栏，有编辑按钮，点击之后，会进入一个表单，此时会回显出来角色的信息，以及权限树种会回显已经给角色分配的权限，会打钩。在这里可以进行编辑

（6）保存编辑之后，我们要提供一个编辑角色的操作，将角色的基本信息更新到数据库中，同时更新中间表中的角色跟权限的关联关系

（7）在角色列表中，有一个删除按钮，可以删除这个角色，就直接将角色和角色的授权数据都删除

（8）在角色列表中，有启动/停用的按钮，启用或者停用，就是更新角色的一个是否启用的一个字段

（9）为账号列表的筛选，提供一个查询全部角色的一个功能

2.3 账号管理

（1）账号列表

包含字段：ID、用户名、姓名、电话、创建人、创建时间、备注、启用状态

（2）账号列表

有一个菜单，权限中心-权限管理-账号管理

支持账号列表的分页查询

用户名、姓名、电话、角色（下拉框）、创建时间（时间范围）、启用状态（下拉框）

（3）添加账号

在账号列表的上面有一个按钮

基本信息：用户名、密码、姓名、电话、启用状态

分配角色：会出现一个角色列表，可以分页查询，可以按条件筛选，支持复选，选择多个角色

额外分配权限：权限树，随着你勾选不同的角色，会支持将那个角色拥有的权限，在下面的权限树种显示出来。可以额外的去勾选更多的权限

在后台，需要保存账号的基本信息，保存账号-角色的关系（中间表），保存账号-权限的关系（中间表）

（3）编辑账号

基本信息与权限信息，在每一个账号最右侧的操作栏

进入一个编辑页面，可以回显所有的数据，显示账号的基本信息，显示账号的分配的角色，在列表中的复选框会自动勾选，显示账号关联的权限，权限树里的复选框会自动勾选

然后可以编辑

保存，编辑账号，更新账号数据，更新账号和角色的关联关系，更新账号和权限的关联关系

（4）启用/停用账号

修改账号的启用状态

（5）修改密码

修改账号的登录密码，在每一个账号最右侧的操作栏

2.4 权限控制

（1）在左侧菜单栏，先查出来一个账号关联的所有权限中的顶级权限（父权限ID为NULL），再查出来每个顶级权限下面，这个账号有权限的二级权限，两级的左侧菜单就可以显示出来了

（2）点击一个菜单，跟着URL进入一个界面之后，显示按钮的时候，需要根据按钮对应的权限的编号，去后台查一下，那个账号是否拥有某个权限，是这个编号的

（3）所有的URL请求，全部看一下，这个账号授权的权限中，是否某个权限的URL是这个URL，账号是否有权限访问这个URL

子系统-服务-模块-功能，这样的一个结构

二、系统安全服务

菜单：权限中心-系统安全-操作日志

1、业务知识

每个账号在执行各种操作的时候，都会访问后台系统的URL，账号对这些URL的访问，就是操作日志，可以存储下来，以后如果对一些非法的员工，可以去审计他的行为，看他都在干什么

2、操作日志的数据字段

ID、账号ID、IP地址、URL、权限ID、操作时间、是否授权（是/否）

3、添加操作日志

就是说账号在访问所有的URL的时候，都会去添加一条这个操作日志，插入一个表中

4、查看操作日志

显示的列表字段：ID、账号ID、用户名、姓名、IP地址、权限名称、权限编号、权限URL、操作时间、是否授权

可以筛选，账号ID、用户名、姓名、IP地址、权限名称、权限编号、权限URL、操作时间范围、是否授权（下拉框）

菜单：权限中心-系统安全-黑名单

1、业务知识

可能会受到一个攻击，或者不明的ip在访问我们的URL

2、查看黑名单列表

ip地址、备注

3、对黑名单进行增删改

4、黑名单的控制

黑名单中的ip地址，所有的访问一律封禁

15972284201