OA 权限模块设计

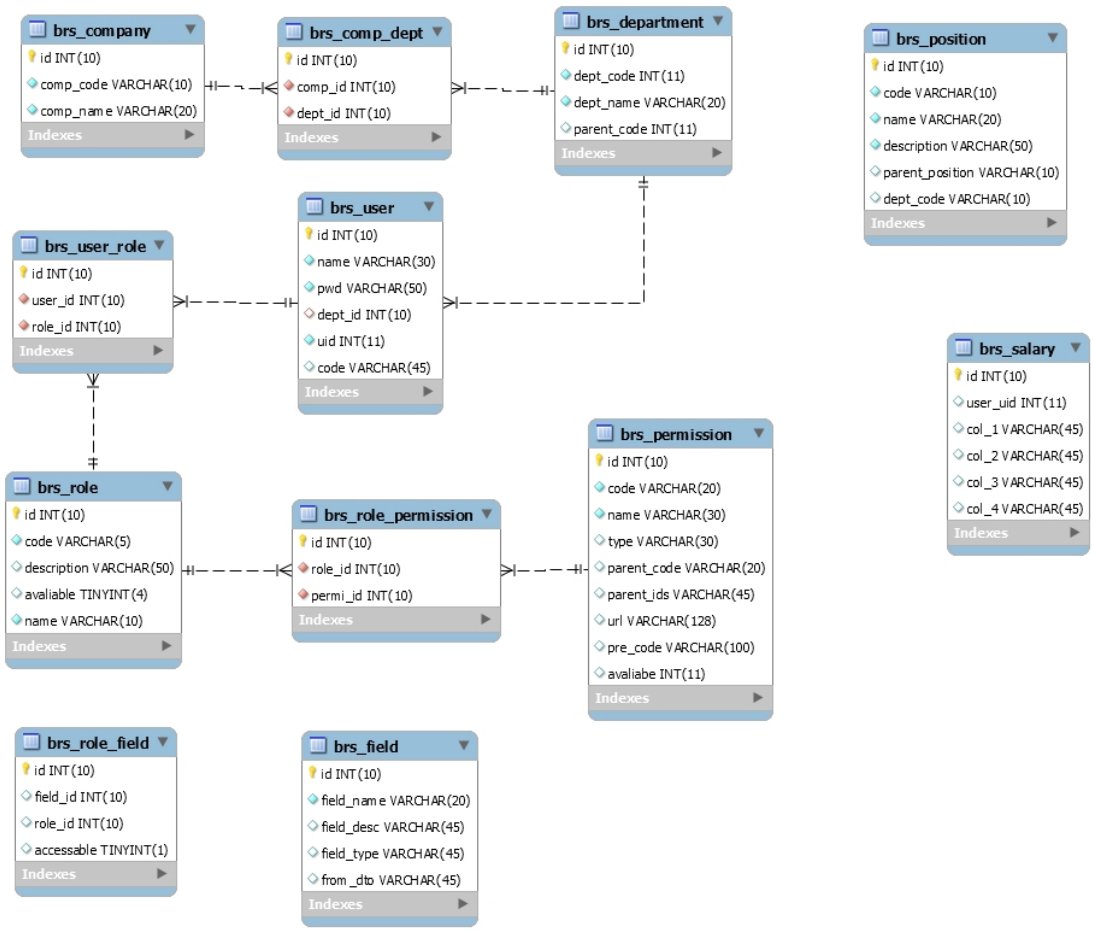
Tiny jjlin

OA 权限系统设计方案

采用基于角色的访问控制模型（Role-Based Access Controll)。即 RBAC 模型。

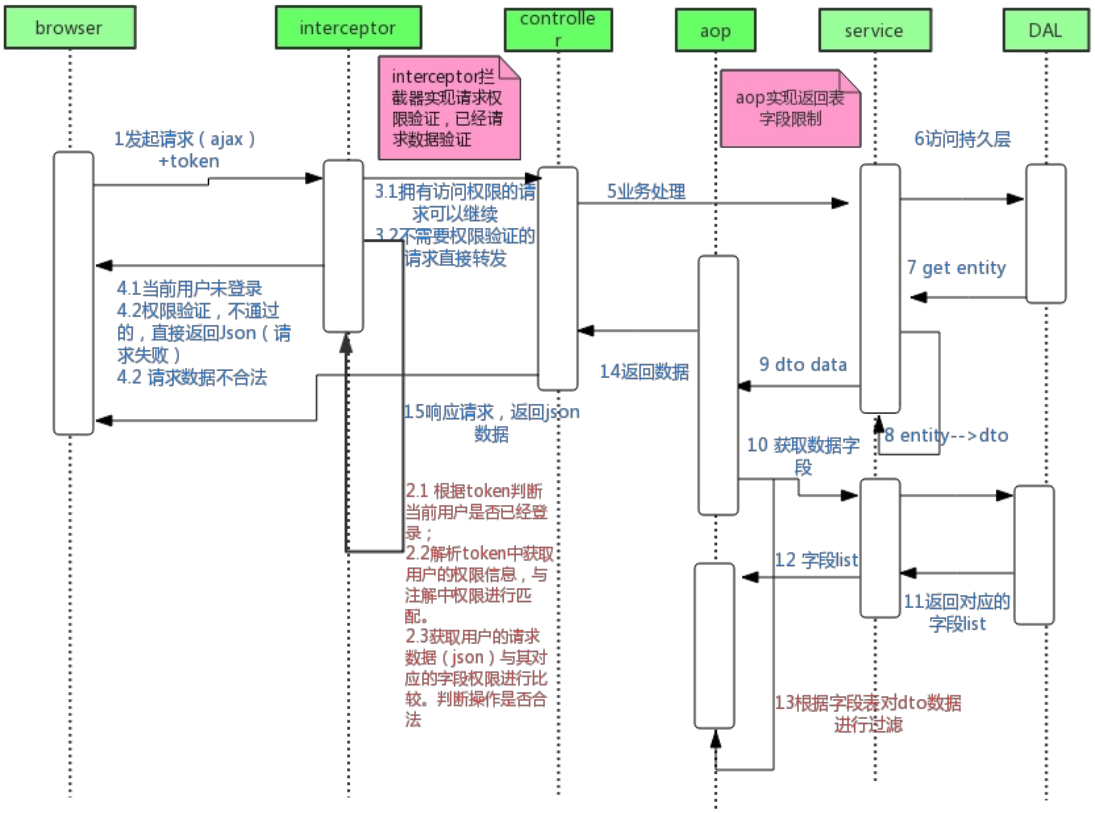
其他模型有：ACL 模型。它们之间的比较，优缺点（为什么采用该方案待补充）

数据库设计（ER 图）



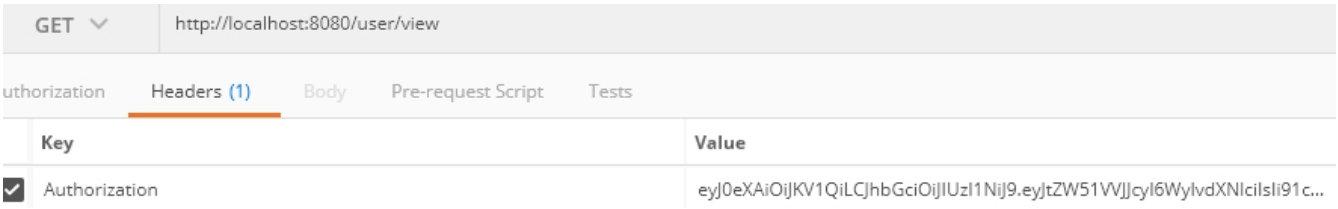
OA 权限详细设计

OA 系统采用前后端分离的设计，后端服务只提供 api 接口。因此后端的权限只是针对 api 接口进行权限设计。具体分为功能权限，和数据权限。
功能权限：判断当前 subject 是否登录，是否有操作，访问的权限。
数据权限：判断当前 subject 对具体数据的读写权限，如根据其所属部门限制其读取数据的范围；以及对访问修改字段值的限制。

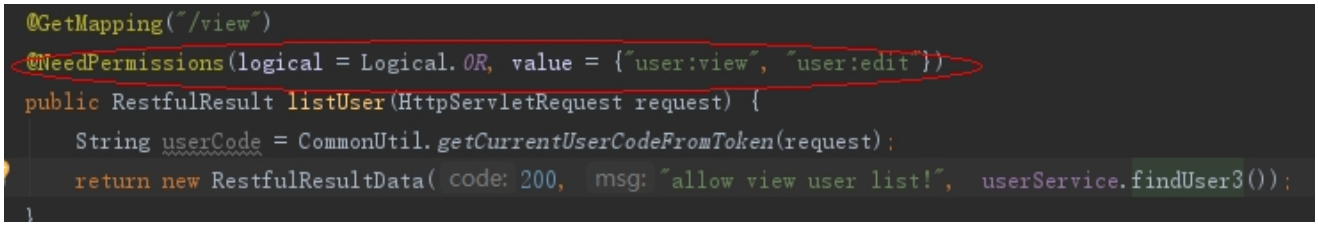


前端如何调用接口

1 前端发起的请求头部必须带有 token。
http://localhost:8080/user/view



2 请求进行权限验证



3 请求用户的权限与服务端接口注解中定义的权限进行比较。如果通过，可以继续访问；否则直接返回。