企业通用权限平台

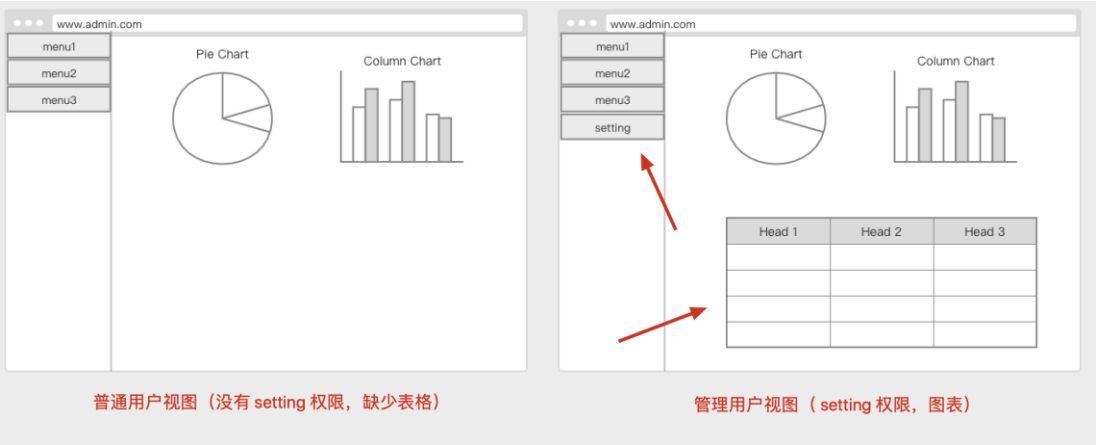
一、 项目基本情况

企业通用权限平台是任何企业发展过程必备的基础系统平台。企业内有很多对内，对外的业务系统，几乎所有的系统都有权限管理需求。

一些系统的权限需求比较简单（某些个人和角色对某些界面有操作权限，某些界面没有操作权限），可以快速在系统中实现；一些权限管理需求比较复杂（例如：权限集合需要可继承，用户可分租，申请和授权要走审批流，权限授予、访问可审计、可回溯等）；

多个系统都进行建设的话，会造成比较严重的人力浪费。所以打造一个通用的，可以同时满足简单和复杂业务权限管理诉求的平台是必然的一步。

图一：普通用户和管理员查看的视图不一样（常规需求举例）



该项目的需求是结合企业实际权限管理应用场景抽象而来。经典的权限管理系统都是 RBAC（Role Based Access Control）模型拓展而来的。

通用的权限系统是易用性，可拓展性的一个平衡。让同学们从最基础的核心功能起步，去体验实际企业级应用场景的建模和工程实践。

二、 基本功能说明

基本功能

实现一个 RBAC 经典模型的通用权限管理系统，可以为多业务系统（客户）提供标准化服务。核心功能如下：

1） **多应用支持。**每一个应用的权限配置（数据）和使用相互隔离。

2） **权限定义有可扩展的建模和实现。**

a. 权限目标可以支持多种类型（例如：URL，菜单，按钮，表格，表格列，数据库表，数据库字段等）；

b. 权限操作可以支持多种类型（例如：访问、增加、删除、编辑、审批、拒绝）。

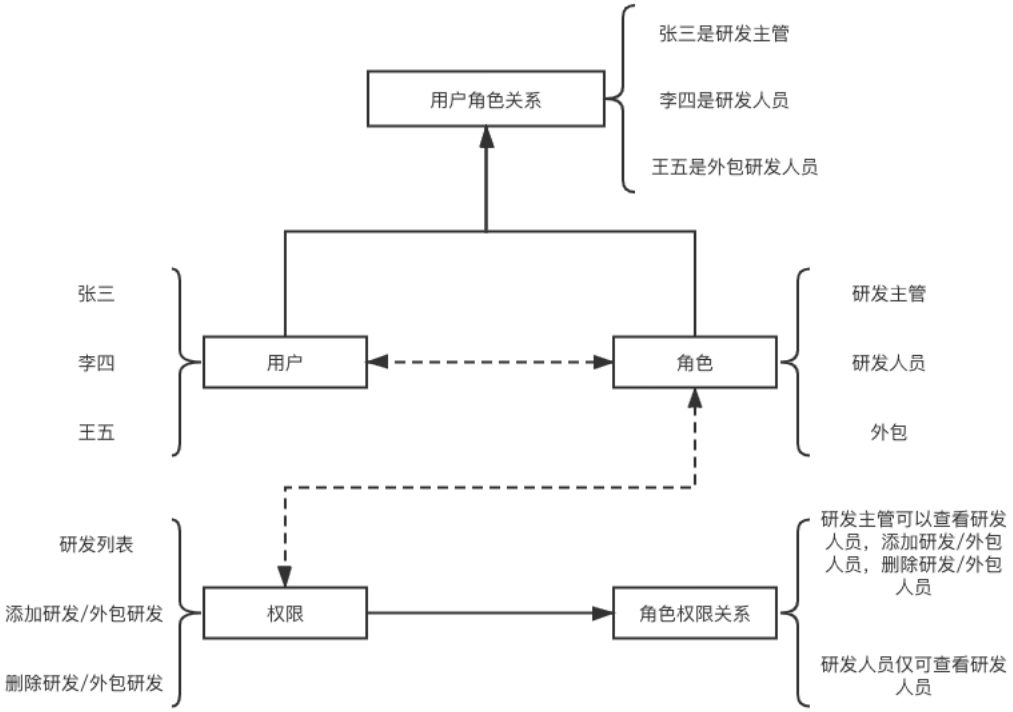
3） **角色定义支持。**一个角色可关联多个权限，一个权限可关联多个角色，可以通过角色查询所有关联权限，可以通过权限查询所有使用角色。

4） **用户定义支持。**一个角色可关联多个用户，一个用户可关联多个角色，可以通过用户查询用户的所有角色和权限，可以通过角色查询所有拥有该角色的用户。

5） **权限查询 API。**在权限管理和定义之后，远程业务系统，可以通过 API，获得特定应用，特定用户，特定类型（可选）的权限。

6） **授权管理支持（待定、可选）。**实现申请授权和权限审批流程定义，支持申请人和审批人两种角色，支持审批状态流转。

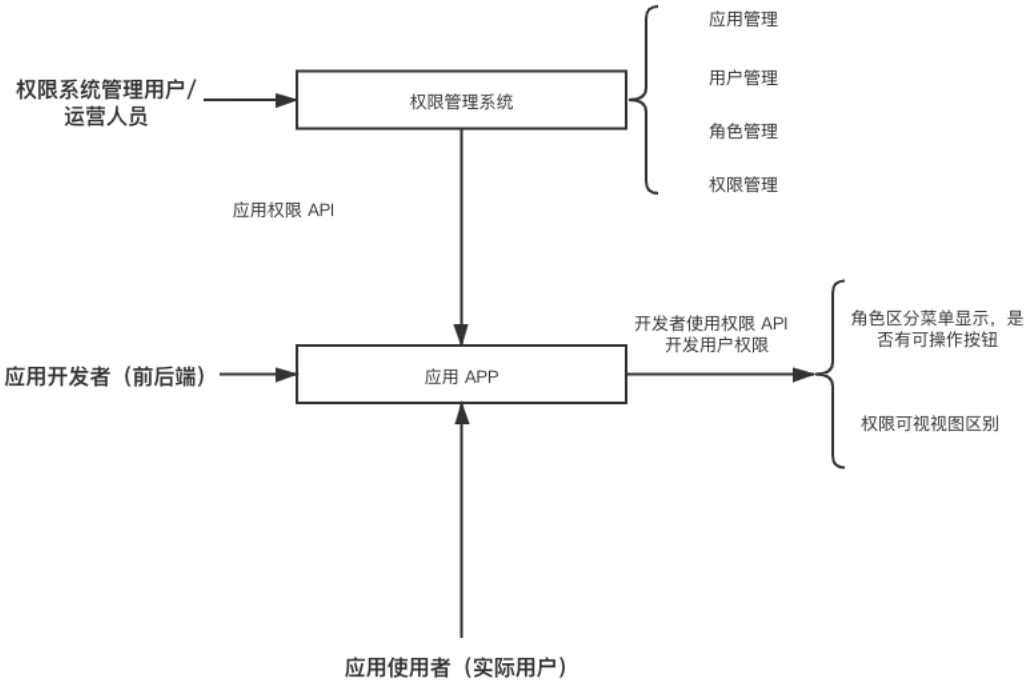
图二：标准 RBAC 系统的核心概念（User，Role，Authorization）



图三：系统间关系和系统用户

关于权限的解释

权限可以理解为目标对象 + 目标对象间的关系+目标对象上的操作。如上图，研发主管（角色）对研发列表（对象）具有查看、添加删除（动作）的权限，而研发人员（角色）则只有对研发列表（对象）查看（动作）的权限。



基本功能的应用场景举例

A．场景视角:

- 站在通用权限系统的用户视角：HR 系统的前端开发人员

B．HR 系统的客户:

- 候选人：查看，并更新自己的个人信息
- HR： 录入多候选人信息，并进行状态流转
- 面试官：查看需要面试的候选人信息，挑选，面试并进行面试结果记录

C．HR 系统需求举例:

- 控制菜单项： 例如，
- 1）候选人，查看「个人信息」菜单；
- 2）HR，查看「所有用户」菜单；
- 3）面试官，查看「所有用户」菜单，查看「我的面试」菜单等
- 控制操作项：例如：
- 1）候选人，查看、修改个人信息；
- 2）HR，录入候选人，查询用户，状态流转；
- 3）面试官，查看候选人，状态流转信息等

D．HR 系统的前端开发来到"通用权限系统"前端界面，配置权限：

- 创建 App（App 名称、描述，App 管理员列表） 不同 App 的权限隔离，获得 AppKey（调用权限 API 使用）
- 创建要控制的权限对象和操作
    - 查看个人申请【菜单项：个人】
    - 申请并录入个人信息【按钮：个人】
    - 修改个人信息【按钮：个人】
    - 查看候选人列表【菜单项：HR，面试官】
    - 查看我的面试【菜单项：HR，面试官】

    - 查看候选人详情【按钮：个人，HR，面试官】
    - 选取候选人为待面试【按钮：面试官】
    - 选取候选人给面试官待面试【按钮：HR】
    - 录入候选人信息【按钮：HR】
    - 编辑候选人信息【按钮：HR】
    - 标记面试结果（通过、失败，待定）【按钮：面试官】
    - 标记面试通过，待入职【按钮：HR】
- 创建角色
    - 候选人
    - HR
    - 面试官
- 关联角色和用户
    - 每一个角色都可以添加，删除多个用户，至少有一个用户关联角色才有意义
    - 拥有角色的用户，拥有该角色的所有的权限
    - 用户预定义（先实现为固定列表（例如：30 人预定义用户），一般的权限系统依赖公司通用的用户系统）
- 关联角色和权限
    - 关联角色和菜单、按钮权限
    - 候选人
        - 1）录入个人信息；
        - 2）修改个人信息；
    - HR
        - 1）查看候选人列表；
        - 2）查看候选人详情；
        - 3）选取候选人给面试官待面试；
        - 4）查看我的面试列表；
        - 5）录入候选人信息；
        - 6）编辑候选人信息；
        - 7） 标记面试通过，待入职；
    - 面试官
        - 1）查看候选人列表；
        - 2）查看候选人详情；
        - 3）选取候选人为待面试；
        - 4）查看我的面试列表；
        - 5）标记面试结果（通过、失败）；
- 配置成功后（配置修改实时生效），查看权限 API 调用示例
    - 查看特定用户权限，通过 userId，appId，appKey
    - 查看特定角色权限，通过 roleId，appId，appKey

E．在 HR 系统中，调用权限 API，并实现系统逻辑

- 根据权限信息，控制 UI 的展示和操作

可选功能

1） 权限授权期限管理（实际业务场景）：任何人和最终的权限绑定关系，都有时间的限制，超出时间范围，会自动把权限和人的关系解除。
2） 用户组管理（RBAC 1 模型）：实现用户组和用户组嵌套功能
3） 角色管理（RBAC 1 模型）：：实现角色继承和重载能力
4） 角色管理（RBAC 2 模型）：实现角色互斥能力，实现角色的总人数显示，实现角色获得的前序角色限制条件
5） 权限与组织架构管理（实际业务场景需求）：组织架构是一颗树形结构，公司的人员是属于不同的组织架构的，不同的组织可以具备不同的权限集合，默认上层组织具备下级组织的所有权限（同时可定制），人员加入或者离开不同的组织架构会自动拥有和调整对应的权限。
6） 通过 API 导入组织架构和权限的映射管理（实际业务场景）。
7） 权限与职称管理（实际业务场景）：不同的职称会拥有不同的系统的不同权限集合，同一个公司人员可能有不同的身份和职称，获得和调整职称会自动获得相应的权限。
8） 通过 API 导入职称和权限映射关系（实际业务场景）。
9） 权限组管理（实际业务场景）：实现权限组和权限组嵌套功能。

非功能需求

1. 权限定义的通用性和可扩展性

在建设平台的时候并不完全清楚其他系统的权限定义和使用场景，为了保证平台的可复用性，权限模型本身的扩展性是其中的一个关键点。

权限模型的扩展性（包括但不限于）：

1） 权限种类可添加（不需要编码）。例如：菜单权限，按钮权限，URL 权限，可以动态扩展出，Service 权限，Block 权限，Tab 权限，数据表格权限，数据列（字段）权限等。
2） 权限对象（资源）有层次拓展（不需要编码）。例如：控制了菜单权限，也能拓展子菜单，子菜单的子菜单权限等。
3） 权限操作（动作）可拓展（不需要编码）。例如：可以控制可视、创建操作权限，也能拓展修改，删除，审批操作权限。

这里“不需要编码”指的是在不需要修改代码的前提下用户可以动态地添加或扩展新的权限种类、对象或类型。

2. 用户权限配置的 UE 设计（可选）

在通用的权限模型设计基础上，为用户的常规需求，提供更容易理解的权限配置界面，从而降低简单权限需求的接入，理解和使用成本，例如：URL 的可访问控制，菜单项的可访问控制，界面按钮的展示控制，界面区块的可展示控制，数据库表的可访问控制，数据库列（字段）的可访问控制等。

3. 查询效率（可选）

通过用户名称查询特定系统的所有权限是公司内最常用的功能，需要保证，在 100 QPS+ 的情况下，100ms 以内的平均查询返回效率。

4. 服务稳定性设计（可选）

任何一个权限系统都是被其他系统顺序依赖的核心系统，如果权限系统服务出现问题会导致所以的"下游"系统因为缺失权限信息而不可用。例如：保证不会被流量击穿，保证水平拓展，保证部分错误自动探测和导流，保证服务更新的灰度能力和滚动更新等等。

实现要求

1． 架构要求，后台服务，前端管理（界面）服务分离。

- 后台服务：
  i. 能够为前端管理（界面），提供数据 CRUD 支持；
  ii. 能够为第三方 App，提供权限查询的对外接口
- 前端服务：
  i. 能够支持新建 App，查看 App 列表，删除 App，获取 App 接口 Token
  ii. 能够支持新建、查看、删除、编辑权限及权限操作
  iii. 能够支持新建、查看、删除、编辑角色
  iv. 能够支持关联角色和权限的关系
  v. 能够支持关联角色和用户的关系
  vi. 能够查看 App 的 2 个权限接口调用示例
  vii. 用户可预定义为固定列表，不需实现增删编辑操作
- 对第三方 App 提供的接口【标准定义】【支持远程调用】
  i. 查询用户权限
    1. 输入：用户的 id (userId)
    2. 输入举例：

```
{
   "userId": "wangleilei",
    "appToken": "XXXXX"
}
```

    3. 输出，数据结构：Array；
       a. 权限类型(authType)、权限 Key(authKey)、权限值(authValue)、权限操作(authOperation)、 子权限(authChildren, Optional)
    4. 输出举例：菜单和子菜单

```
[{
  "authType": "Menu",
  "authKey": "salary",
  "authValue": "工资",
  "authOperation": [
   "read",
   "write"
```

```
      ],
      "authChildren": []
     },
     {
      "authType": "Menu",
      "authKey": "health",
      "authValue": "健康报告",
      "authOperation": [
       "read"
      ],
      "authChildren": [
       {
        "authType": "Menu",
        "authKey": "selfHealth",
        "authValue": "个人健康报告",
        "authOperation": [
         "read",
         "write"
        ],
        "authChildren": []
       },
       {
        "authType": "Menu",
        "authKey": "selfHealth",
        "authValue": "团队健康报告",
        "authOperation": [
         "read",
         "write"
        ],
        "authChildren": []
       }
      ]
     }
    ]"
```


ii. 查询角色权限

1. 输入：用户的 id (roleId)
2. 输入举例：

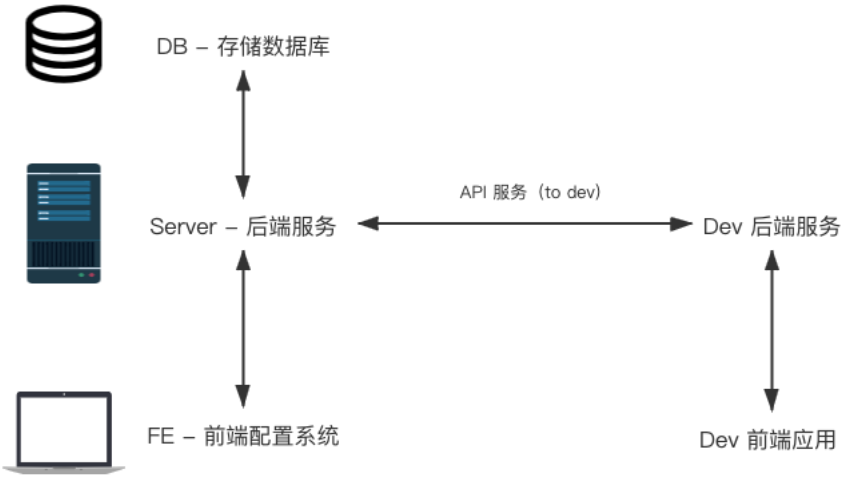

```
{
   "roleId": "departmentAdmin",
    appToken: "XXXXX"
}
```


3. 输出，数据结构：同“查询用户权限”
4. 输出举例：同“查询用户权限”

2． 技术选型，前后端技术选择任意。(推荐：后端服务：Java 或 Node.js，数据库：MySQL，前端服务：Webpack Dev Server 或 Node.js，React。如果课程需要，可提供前后端服务的可启动工程样例。)

- **请注意**：同学们要实现的内容是“图四”中的“权限管理主要实现部分”，不同开发“实际业务开发者应用实现”

图四：系统核心组成部分



检查标准

1. 数据库、数据模型、交互设计文档，用户使用说明
    a. 数据库设计
    b. 数据模型设计
    c. 后端系统和前端界面交互设计
    d. 前端界面的用户使用说明
2. 系统演示和讲解
    a. 系统演示主要步奏，请参考：“基本功能”中的场景描述
    b. 基本要求：
        1）多 App 支持（>=2）；
        2）多权限类型（>=3），多权限定义（>=3），权限操作支持（>=3）；
        3）多角色支持（>=3）；
        4）动态绑定角色和权限关系；
        5）动态绑定角色和用户关系；
3. 使用第三方的系统（非同学实现），连接同学实现的权限系统，检查对外 API 效果
    a. 查询某用户的权限（接口定义，请参考“实现要求”）
    b. 查询某角色的权限（接口定义，请参考“实现要求”）
4. 加分项，拓展功能和可扩展性。
    a. 实际的客户应用场景，来抽验系统权限模型是否可以支持扩展。（参考：非功能需求 1，对于可扩展性的描述）

i. 创建新的权限类型
ii. 添加新的权限，使用新的权限类型
iii. 添加新的权限操作，并使用新的权限操作
iv. 为角色分配新的权限定义

b. 拓展功能的实现（哪些额外功能已实现）

预期用户

企业内的所有系统，前后端开发和业务（包含运营）人员。所有的内部系统，甚至对外系统都有权限管控的需求，企业通用权限平台为这些系统提供了快捷、通用的权限管理入口和拓展能力，不需要其他系统的人员自己建立权限管理的能力，可以快速的接入，配置和使用。

用户代表

联系人：纪伟，张捷
电话：13810641821, 18085766145
邮件：jiwei@kuaishou.com, zhangjie13@kuaishou.com