1 背景

- 每次增加需要认证授权的系统时，都需要独自实现一套认证登录流程
- 只支持admin用户登录
- 不支持三方系统认证授权

2 特性:

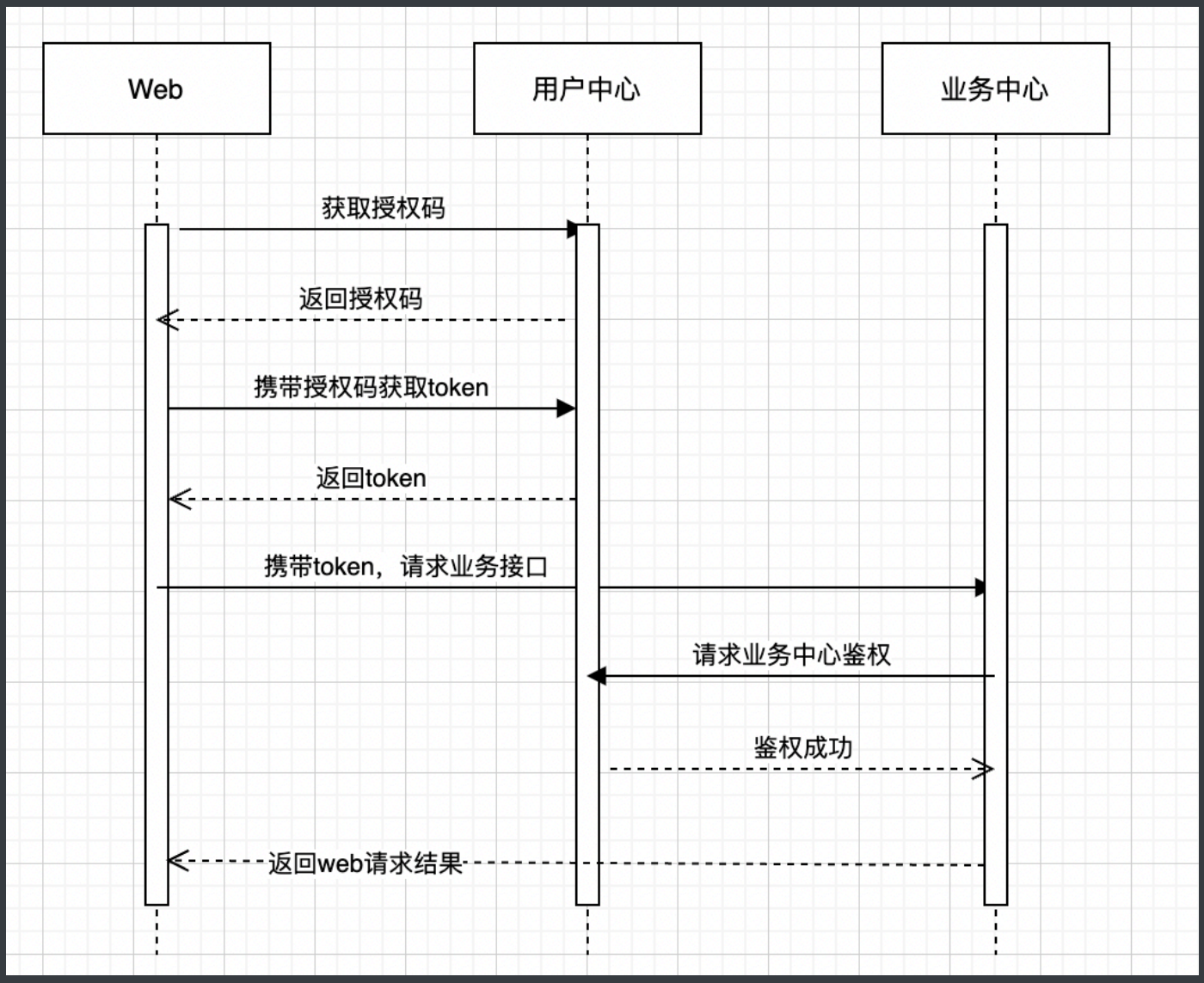
- 支持多用户多角色多权限
- 一套认证授权，处处使用
- 支持三方系统接入
- 支持多种授权模式
- 遵循业内标准的认证授权协议oauth2

3 架构

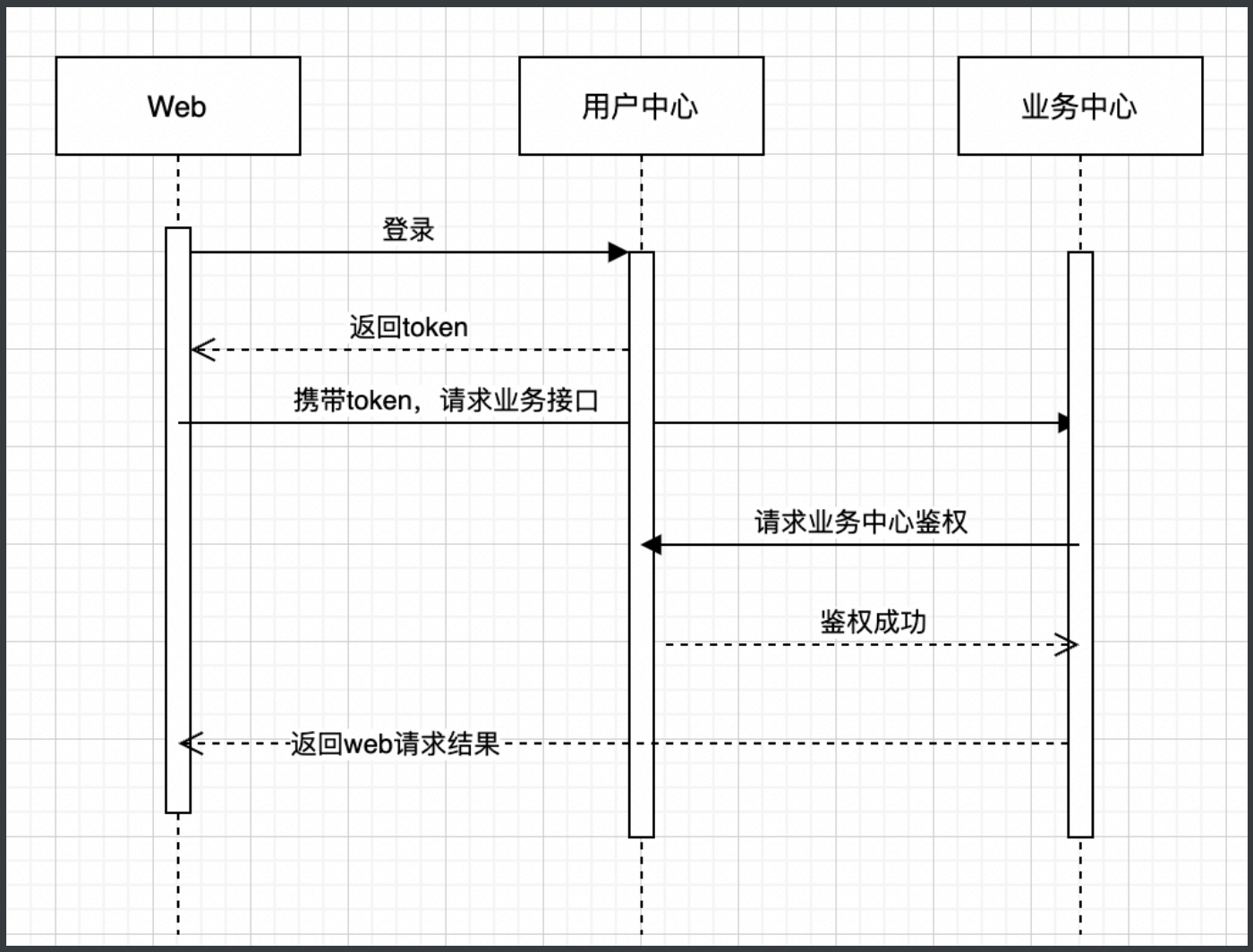
```
SpringSecurityOauth2+Jwt+Mysql
```

4 时序图

1 授权码模式


Web
用户中心
业务中心
获取授权码
返回授权码
携带授权码获取token
返回token
携带token，请求业务接口
请求业务中心鉴权
鉴权成功
返回web请求结果

2 密码模式



5 协议

协议详细用例和说明

获取授权码

```
http://127.0.0.1:8080/processing/user/oauth/authorize?
response_type=code&client_id=client&redirect_uri=https://www.baidu.com
GET
Params
response_type:code 授权类型，填code
client_id:client   客户端id，用来唯一标识客户端
redirect_uri:https://www.baidu.com 重定向地址

注意：弹出http://127.0.0.1:8080/processing/user/login页面，手动输入用户名和密码后，授权码拼接在redirect_uri中
```

获取token（授权码模式）

```
http://127.0.0.1:8080/oauth/token
POST
Headers
Content-Type:application/x-www-form-urlencoded
Authorization:Basic YWRtaW46YWRtaW4=
Body
grant_type:authorization_code
code:Oy1EBQ
redirect_uri:https://www.baidu.com
Response
{
    "access_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3BlIjpbImFsbCJdLCJleHAiOjE2NTE2ODAxMTcsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2Nlc3NpbmcvdXNlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iXSwianRpIjoiMTljNDcwYmEtNTQ2Ni00OTk1LWFjNjMtOGU1ZGI0MzA2Njc5IiwiY2xpZW50X2lkIjoiY2xpZW50IiwiZW5oYW5jZSI6IuWinuW8uueahOS_oeaBryJ9.jMlzt46oj5ey8XjrbVF5AYDBRJjg02dVmPbFuv5e46M",
    "token_type": "bearer",
```

```
    "refresh_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3
BlIjpbImFsbCJdLCJhdGkiOiIxOWM0NzBiYS01NDY2LTQ5OTUtYWM2My04ZTVkYjQzMDY2Nz
kiLCJleHAiOjE2NjE2NzI5MTcsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2Nlc3NpbmcvdX
Nlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iXSwianRpIjoiNTU2ZTY0ZG
YtOGU0MS00MzFlLWFkNGUtZWZkYzNhM2MzNzAwIiwiY2xpZW50X2lkIjoiY2xpZW50IiwiZW
5oYW5jZSI6IuWinuW8uueahOS_oeaBryJ9.ljDSeYM6vV5L7ZMFFrA-
iISaSt8z06i_JuhXDPmdHh8",
    "expires_in": 6007,
    "scope": "all",
    "enhance": "增强的信息",
    "jti": "19c470ba-5466-4995-ac63-8e5db4306679"
}
```


获取token（密码模式）


```
http://127.0.0.1:8080/processing/user/oauth/token
POST
Headers
Content-Type:application/x-www-form-urlencoded
Authorization:Basic YWRtaW46YWRtaW4=
Body
grant_type:password
username:admin
password:admin
scope:all
Response
{
    "access_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3
BlIjpbImFsbCJdLCJleHAiOjE2NTE2ODAxMTcsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2
Nlc3NpbmcvdXNlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iXSwianRpIj
oiMTljNDcwYmEtNTQ2Ni00OTk1LWFjNjMtOGU1ZGI0MzA2Njc5IiwiY2xpZW50X2lkIjoiY2
xpZW50IiwiZW5oYW5jZSI6IuWinuW8uueahOS_oeaBryJ9.jMlzt46oj5ey8XjrbVF5AYDBR
Jjg02dVmPbFuv5e46M",
    "token_type": "bearer",
```

```
    "refresh_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3
BlIjpbImFsbCJdLCJhdGkiOiIxOWM0NzBiYS01NDY2LTQ5OTUtYWM2My04ZTVkYjQzMDY2Nz
kiLCJleHAiOjE2NjE2NzI5MTcsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2Nlc3NpbmcvdX
Nlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iXSwianRpIjoiNTU2ZTY0ZG
YtOGU0MS00MzFlLWFkNGUtZWZkYzNhM2MzNzAwIiwiY2xpZW50X2lkIjoiY2xpZW50IiwiZW
5oYW5jZSI6IuWinuW8ueahOS_oeaBryJ9.ljDSeYM6vV5L7ZMFFrA-
iISaSt8z06i_JuhXDPmdHh8",
    "expires_in": 6035,
    "scope": "all",
    "enhance": "增强的信息",
    "jti": "19c470ba-5466-4995-ac63-8e5db4306679"
}
```

刷新token

```
http://127.0.0.1:8080/processing/user/oauth/token
POST
Headers
Content-Type:application/x-www-form-urlencoded
Authorization:Basic YWRtaW46YWRtaW4=
Body
grant_type:refresh_token
refresh_token:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZ
G1pbiIsInNjb3BlIjpbImFsbCJdLCJhdGkiOiIxOWM0NzBiYS01NDY2LTQ5OTUtYWM2My04Z
TVkYjQzMDY2NzkiLCJleHAiOjE2NjE2NzI5MTcsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb
2Nlc3NpbmcvdXNlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iXSwianRpI
joiNTU2ZTY0ZGYtOGU0MS00MzFlLWFkNGUtZWZkYzNhM2MzNzAwIiwiY2xpZW50X2lkIjoiY
2xpZW50IiwiZW5oYW5jZSI6IuWinuW8ueahOS_oeaBryJ9.ljDSeYM6vV5L7ZMFFrA-
iISaSt8z06i_JuhXDPmdHh8
Response
{
```

```
    "access_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3
BlIjpbImFsbCJdLCJleHAiOjE2NTE2ODE2NTMsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2
Nlc3NpbmcvdXNlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iLCJHRVQ7L3
Byb2Nlc3NpbmcvdXNlci91c2VyL2dldEN1cnJlbnRVc2VyIl0sImp0aSI6IjY5YWNhYmYyLT
RkYzctNDcxZi1hZjk1LWNiNGI3ZTFjMjYxNSIsImNsaWVudF9pZCI6ImNsaWVudCIsImVuaG
FuY2UiOiLlop7lvLrnmoTkv6Hmga8ifQ.7njMesWU26O99EFjQ4slfSgIIJHqZqVH0zD3QA9
nCiA",
    "token_type": "bearer",
    "refresh_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3
BlIjpbImFsbCJdLCJhdGkiOiI2OWFjYWJmMi00ZGM3LTQ3MWYtYWY5NS1jYjRiN2UxYzI2MT
UiLCJleHAiOjE2NjE2NzQ0NTMsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2Nlc3NpbmcvdX
Nlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iLCJHRVQ7L3Byb2Nlc3Npbm
cvdXNlci91c2VyL2dldEN1cnJlbnRVc2VyIl0sImp0aSI6IjNmOGFhYTJmLWQyZWEtNGQ5MS
05Y2Y4LTE1ZTQ5YjU1OTliNyIsImNsaWVudF9pZCI6ImNsaWVudCIsImVuaGFuY2UiOiLlop
7lvLrnmoTkv6Hmga8ifQ.pp22G6C5ezPWe9-5i46Qz1VnPICbqrioH0arPDlMFmc",
    "expires_in": 7199,
    "scope": "all",
    "enhance": "增强的信息",
    "jti": "69acabf2-4dc7-471f-af95-cb4b7e1c2615"
}
```


校验token

```
http://127.0.0.1:8080/processing/user/oauth/verify_token?
method=POST&uri=/hello
GET
Headers
Authorization:Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3B
lIjpbImFsbCJdLCJleHAiOjE2NTE2NzgxMTgsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3VzZXI
vY2hhbmdlUGFzc3dvcmQiLCJQT1NUOy9oZWxsbyJdLCJqdGkiOiIwNGIyYjBlYS01YmY0LTR
hMTktODBmYy0yOWI1YmNjZGE1N2MiLCJjbGllbnRfaWQiOiJjbGllbnQiLCJlbmhhbmNlIjo
i5aKe5by655qE5L-h5oGvIn0.bnbyutAWEe30K2vF-pWvidZebVFNf5M-6s3yZoC1KjQ
Params
method:POST
uri:/hello
Response
true/false
```

删除token

```
http://127.0.0.1:8080/processing/user/oauth/remove_token
DELETE
Headers
Authorization:Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3B
lIjpbImFsbCJdLCJleHAiOjE2NTE2NzgxMTgsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3VzZXI
vY2hhbmdlUGFzc3dvcmQiLCJQT1NUOy9oZWxsbyJdLCJqdGkiOiIwNGIyYjBlYS01YmY0LTR
hMTktODBmYy0yOWI1YmNjZGE1N2MiLCJjbGllbnRfaWQiOiJjbGllbnQiLCJlbmhhbmNlIjo
i5aKe5by655qE5L-h5oGvIn0.bnbyutAWEe30K2vF-pWvidZebVFNf5M-6s3yZoC1KjQ
```

修改用户密码

```
http://127.0.0.1:8080/processing/user/user/changePassword
POST
Headers
Content-Type:application/json
Authorization:Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiJhZG1pbiIsInNjb3Bl
IjpbImFsbCJdLCJleHAiOjE2NTE2ODE4NTYsImF1dGhvcml0aWVzIjpbIlBPU1Q7L3Byb2N
lc3NpbmcvdXNlci91c2VyL2NoYW5nZVBhc3N3b3JkIiwiUE9TVDsvaGVsbG8iLCJHRVQ7L3B
yb2Nlc3NpbmcvdXNlci91c2VyL2dldEN1cnJlbnRVc2VyIl0sImp0aSI6IjYzNzQ1MjVhLWV
mNDEtNGJjNy04YWQ0LTk1YmEwOTFkMTA0NyIsImNsaWVudF9pZCI6ImNsaWVudCIsImVuaGF
uY2UiOiLlop7lvLrnmoTkv6Hmga8ifQ.5mNylhtK4kefpRYEe4T0F9Ijvk7biAPgcRLtnacK
ypM
Body
{
    "username":"admin",
    "password":"admin"
}
Response
true/false
```

6 数据库表结构

sql文件

Spring Cloud Oauth2框架默认需要的表

```
-- ----------------------start Spring Cloud Oauth2框架默认需要的表
CREATE TABLE `oauth_access_token` (
  `token_id` varchar(256) DEFAULT NULL,
  `token` blob,
  `authentication_id` varchar(256) NOT NULL,
  `user_name` varchar(256) DEFAULT NULL,
  `client_id` varchar(256) DEFAULT NULL,
  `authentication` blob,
  `refresh_token` varchar(256) DEFAULT NULL,
```

```
  PRIMARY KEY (`authentication_id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

CREATE TABLE `oauth_client_details` (
  `client_id` varchar(256) NOT NULL,
  `resource_ids` varchar(256) DEFAULT NULL,
  `client_secret` varchar(256) DEFAULT NULL,
  `scope` varchar(256) DEFAULT NULL,
  `authorized_grant_types` varchar(256) DEFAULT NULL,
  `web_server_redirect_uri` varchar(256) DEFAULT NULL,
  `authorities` varchar(256) DEFAULT NULL,
  `access_token_validity` int DEFAULT NULL,
  `refresh_token_validity` int DEFAULT NULL,
  `additional_information` varchar(4096) DEFAULT NULL,
  `autoapprove` varchar(256) DEFAULT NULL,
  PRIMARY KEY (`client_id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

CREATE TABLE `oauth_refresh_token` (
  `token_id` varchar(255) DEFAULT NULL,
  `token` blob,
  `authentication` blob
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 ;
-- ----------------------end Spring Cloud Oauth2框架默认需要的表
```

rbac权限管理需要的表

```
-- ----------------------start rbac权限管理需要的表
CREATE TABLE `rbac_user` (
  `id` bigint NOT NULL AUTO_INCREMENT COMMENT '用户 ID',
  `username` varchar(255) NOT NULL COMMENT '用户名',
  `password` varchar(255) NOT NULL COMMENT '密码，加密存储，admin/1234',
  `is_enabled` int DEFAULT '1' COMMENT '帐户是否可用(1 可用，0 删除用户)',
  `memo` varchar(255) CHARACTER SET utf8 COLLATE utf8_general_ci DEFAULT
NULL COMMENT '备注',
```

```
  `create_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `update_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=utf8mb4 COMMENT='用户表';

CREATE TABLE `rbac_role` (
  `id` bigint NOT NULL AUTO_INCREMENT COMMENT '角色 ID',
  `name` varchar(64) NOT NULL COMMENT '角色名称',
  `memo` varchar(255) DEFAULT NULL COMMENT '备注',
  `create_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `update_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COMMENT='角色表';

CREATE TABLE `rbac_user_role` (
  `id` bigint NOT NULL AUTO_INCREMENT COMMENT '主键 ID',
  `user_id` bigint NOT NULL COMMENT '用户 ID',
  `role_id` bigint NOT NULL COMMENT '角色 ID',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COMMENT='用户角色表';

CREATE TABLE `rbac_permission` (
  `id` bigint NOT NULL AUTO_INCREMENT COMMENT '权限 ID',
  `name` varchar(255) NOT NULL COMMENT '权限名称',
  `url` varchar(255) DEFAULT NULL COMMENT '授权路径',
  `method` varchar(10) CHARACTER SET utf8 COLLATE utf8_general_ci
DEFAULT NULL,
  `memo` varchar(255) DEFAULT NULL COMMENT '备注',
  `create_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `update_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COMMENT='权限表';

CREATE TABLE `rbac_role_permission` (
  `id` bigint NOT NULL AUTO_INCREMENT COMMENT '主键 ID',
  `role_id` bigint NOT NULL COMMENT '角色 ID',
```

```
  `permission_id` bigint NOT NULL COMMENT '权限 ID',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COMMENT='角色权限表';
-- ----------------------end rbac权限管理需要的表
```