动机：为什么要有基础账户

这个你懂的，我就不废话了。

计划应用场景

- 用`Walnut`账户登录`Walnut`
- 用`Domain`账户登录`域站点`
- 用`Domain`账户登录`Walnut`
- **!!!不支持**`Walnut`账户登录`域站点`

这里的重点是用`Domain`账户登录`Walnut`：

- `Walnut`无所谓业务角色
- 登录后，用户的主组为当前域，组角色为`0:非组员`

设计思路与边界

- 如果指定了账户表，则使用
- 否则用一个默认账户表

数据结构描述

文件结构树

```
#-------------------------------------
# Walnut 系统用户账户存放方式
/auth/
  |-- usr/index/         # 存放所有的系统账户信息
  |   |-- root           # 根用户为默认存在
  |   |-- xiaobai        # 每个用户一个文件
  |   |-- xiaohei        # 元数据记录了用户的信息
  |-- grp/               # 存放所有的系统账户分组
      |-- ID(root)/          # 根组
      |   |-- ID(root){1}    # 账户在组内的角色
      |-- ID(xiaobai)/       # 每个用户都有一个自己的主组
      |   |-- ID(xiaobai){1}    # 自己在主组内通常为管理员
#------------------------------
# 会话的存放地址
/var    # 系统运行时数据存放区
  |-- session/           # 会话存放目录
  |   |-- ${TICKET}      # 每个会话存放一个文件
  |-- captcha/           # 验证码存放目录
      |-- login/         # 一个场景一个目录
          |-- 13910110055    # 一码一文件
```

```
#-------------------------------------
# 用户域
/home/${YOUR DOMAIN}/
  |-- www/      # 存放站点的文件夹
  |   |-- ${OneSite}  # 某一个站点，这里关联了账户库
  #-----------------------------
  # 用户库
  |-- accounts/
  |   |-- xiaobai       # 每个用户一个文件
  |   |-- xiaohei       # 元数据记录了用户的信息
  #-----------------------------
  # 业务角色库
  |-- roles/
  |   |-- admin         # 这里的角色名，不是系统的角色名
  |   |-- member        # 为了区分，这里的角色名用字符串
  |   |-- operator      # 还可以指定其他角色名
  |   |-- service       # 作为
  #-----------------------------
  # 域的 web 服务临时数据存放区
  |-- .www
  |   |-- session/     # 存放会话信息
  |       |-- ${SITE ID}      # 站点的ID
  |           |-- ${TICKET}   # 每个会话存放一个文件
  |-- captcha/          # 验证码存放目录
  |       |-- ${SITE ID}    # 站点的ID
              |-- login/    # 一个场景一个目录
                  |-- 13910110055   # 一码一文件
```

站点元数据

```
id : ID,       # 站点的 ID

# 本站的映射域名，可以是  www.youdomain.com 之类的域名
# 只要在 `/domain` 里做了映射，则会转到这个目录下
# 默认 "ROOT" 的话要用 /www/your-domain/ 来直接指明
www : "ROOT"

# 当访问站点，但是没有指明入口页时，默认跳转到哪个页面，
# 默认是 index.wnml | index.html
www_entry : "enter.html",

# 声明虚拟页，给定的路径匹配的话，则采用指定虚拟页
www_pages : ["index.wnml:abc/page/*,xyz/page/*"]

# 这里是站点关联的集合（ThingSet）
accounts : "~/accounts"   # 账户库
roles    : "~/roles"      # 角色库
orders   : "~/orders"     # 订单库
products : "~/products"   # 商品库
coupons  : "~/coupons"    # 优惠券库

# 商户映射表：根据支付类型前缀来决定
sellers : {
  # 微信配置目录名称，该目录位于 ~/.weixin/ 目录下
  # 微信登录，公众号消息推送，微信支付等功能均在这个目录下配置
  # 当支付类型为 `wx.` 时需要这个配置项目
```

```
  wx : "theName"

  # 支付宝配置目录名称，该目录位于 ~/.alipay/ 目录下
  # 支付宝支付等功能均在这个目录下配置
  # 当支付类型为 `zfb.` 时需要这个配置项目
  zfb : "theName"
}

# 默认会话时长（秒）
se_du : 86400
```

会话元数据

```
{
  id   : "45..8a",    // 会话唯一ID
  nm   : "54..8m",    // 会话的票据，会定期变化
  expi : 159..,       // 过期时间点 AMS
  uid  : "u6..8r",    // 会话的用户ID
  unm  : "xxx",       // 用户的名称（冗余）
  // 会话的创建场景
  //  - web_vcode  : 网页动态验证码登录， scence_value 为手机号或邮箱
  //  - web_passwd : 网页账号密码登录，scence_value 为用户登录名
  //  - wx_xxxxxxx : 某微信公众号code自动登录，scene_value 为用户 OpenId
  //  - microapp : 微信小程序，scene_value 为用户 OpenId
  by_tp  : "web_passwd",
  by_val : "xxx"
}
```

用户的元数据

> 无论是系统用户还是域用户，下面的元数据通用

```
id : ID            # 【唯一】唯一的用户 ID
#---------------------------------------------------
# 登录信息
nm    : "xxx"      # 【唯一】用户的登录名，默认为 ID
phone : "139.."    # 【唯一】绑定手机
email : "x@y.z"    # 【唯一】绑定邮箱
#---------------------------------------------------
# 密码/盐
passwd : "xxx"     # 加盐后密码
salt   : "xxx"     # 盐值（随机数）
#---------------------------------------------------
# 基本信息
role  : "user"     # 用户业务角色名，角色库的 'nm' 段值
thumb : "id:xxx"   # 用户的头像文件
sex : 1,           # 性别：0=未知，1=男，2=女
th_nm : "xxx"      # 用户昵称
#.............................
# OAuth2 认证
oauth_github  : "xxxxxxx",
oauth_wxlogin : "oSQW..cYq"
#---------------------------------------------------
# 微信公号 OpenID
wx_gh_site0 : "OpenId"     # 某微信公号下的 OpenId
```

```
#------------------------------------------------
# 时间戳
ct    : AMS      # 创建/注册时间
lm    : AMS      # 最后修改时间
login : AMS      # 最后登录时间
#------------------------------------------------
# 用户更多信息
country  : "xxx"    # 国家
province : "xxx"    # 省/直辖市
city     : "xxx"    # 市/市辖区
#------------------------------------------------
# 系统用户特殊元数据
home : "/home/xiaobai"       # 用户的登录主目录
open : "wn.console"          # 登录后打开的应用
theme     : "light"           # 管理界面主题
app_path  : "/app"            # 应用路径, 多路径`:`分隔
view_path : "/rs/ti/view"     # 视图组件路径, 多路径`:`分隔
sidebar_path : "~/.ti/sidebar.json"  # 侧边栏路径, 多路径`:`分隔
```

系统组角色

映射关系存放在 `/auth/grp/ID($domain-user)/ID($user)` 文件元数据中

```
nm   : ID($user)     # 文件名为系统账户ID
role : 1             # 角色值
```

Role	说明
0	非组员，不在组内（默认）
1	管理员
10	组员
100	预备组员，等待管理员审批，期间，和非组员权限一样
-1	黑名单，完全阻止任何访问，也不可以自我申请为预备组员

域用户角色

```
nm       : "admin"           # 角色名
th_nm    : "Peter Zhang"     # 角色显示名
isdft    : false,            # 是否为默认角色，只能有一个有效
ismember : false,            # 【选】系统账户登录是否作为组员
mainpage : "index.wnml",     # 【选】着陆页
```

使用方式

相关知识点

- 基础权限模型