权限系统基于apache shiro改造

实施方案

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 修订人 | 修订日期 | 修订内容 |
| v1.0 | 吴文军 | 2017-06-25 | 初稿 |

1. **背景**

云金融服务平台当前认证、授权管理是通过将用户、权限、资源加载在session会话，登录时检查session会话、授权时根据前端Url地址中后6位参数判断用户是否具有权限或者某些权限。当前基于应用强安全性考虑，拟采用apache shiro安全管理框架对权限系统做认证（登录）、授权（权限控制）、会话管理（session）、缓存、并发、密码加密等功能改造。

1. **目标**

权限系统改造后，由shiro框架统一管理用户登录、权限、资源分配情况，并采用缓存提升访问性能、借助框架能力保证高并发访问正常、有效、采用框架提供的标签控制前端菜单、按钮的安全访问、并结合框架注解对前端访问在服务端作方法双端验证。

1. **方案概要**
   1. 所有涉及登录、会话管理、菜单、按钮操作的系统都在此次改造范围内。
   2. 前端页面按钮、菜单需要调用shiro标签配合框架改造，标签用法及示例参照《Shiro教程.pdf》第九章JSP标签。
   3. 后端方法验证用户参照《Shiro教程.pdf》第十二章与Spring集成 Shiro权限注解。
   4. 权限系统将结合当前系统及客户系统增加系统用户表、角色表、资源表、机构表（如平台运营方、收单方）。
   5. 系统详细配置步骤参见spring-shiro-demo。
2. **业务处理流程图**
3. **数据库表设计**
   1. **系统用户表(t\_system\_user)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 类型 | 关键字 | 允许为空 | 说明 |
| id | bigint | PK | N | 主键 |
| organization\_id | bigint(20) |  | N | 机构ID |
| username | varchar(32) |  | N | 用户名 |
| password | varchar(128) |  | N | 密码 |
| salt | varchar(64) |  | N | 盐 |
| role\_ids | varchar(128) |  | N | 角色ID字符串 |
| locked | tinyint(1) |  | N | 是否锁定 |
| cust\_id | varchar(32) |  | N | 客户编号 |
| create\_time | datetime |  | N | 创建时间 |
| update\_time | datetime |  | Y | 更新时间 |

* 1. **系统角色表(t\_system\_role)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 类型 | 关键字 | 允许为空 | 说明 |
| id | bigint | pk | N | 主键 |
| role | varchar(32) |  | N | 角色名称 |
| description | varchar(64) |  | N | 角色描述 |
| resource\_ids | varchar(128) |  | N | 资源ID字符串 |
| available | tinyint(1) |  | N | 是否有效 |
| create\_time | datetime |  | N | 创建时间 |
| update\_time | datetime |  | Y | 更新时间 |

* 1. **系统资源表 (t\_system\_resource)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 类型 | 关键字 | 允许为空 | 说明 |
| id | bigint | PK | N | 主键 |
| name | varchar(32) |  | N | 资源名称 |
| type | varchar(32) |  | N | 资源类型 |
| url | varchar(256) |  | Y | 访问路径 |
| parent\_id | varchar(32) |  | N | 父节点 |
| parent\_ids | varchar(128) |  | N | 所有父节点 |
| permission | varchar(128) |  | N | 权限 |
| available | tinyint(1) |  | N | 是否可用 |
| create\_time | datetime |  | N | 创建时间 |
| update\_time | datetime |  | Y | 更新时间 |

* 1. **系统机构表(t\_system\_organization)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 类型 | 关键字 | 允许为空 | 说明 |
| id | bigint | pk | N | 主键 |
| name | varchar(32) |  | N | 机构名称 |
| parent\_id | varchar(32) |  | N | 父机构ID |
| parent\_ids | varchar(128) |  | N | 所有父机构ID |
| available | tinyint |  | N | 是否可用 |
| create\_time | datetime |  | N | 创建时间 |
| update\_time | datetime |  | Y | 更新时间 |