# 资料、文章备留：

## PM

《如果你是新晋的leader， 你可能需要了解这些》

https://mp.weixin.qq.com/s/xdpmB8ne8NKQluJBNMJVRg

《初次走上技术管理岗位的思考总结》

https://mp.weixin.qq.com/s/WFiYcc0tlMzAdKTWn7f60A

《一个小公司老板的日常管理总结》

https://mp.weixin.qq.com/s/NaoVRgRzOwB0XTuLE4DX4Q

## Redis

《硬核！15张图解Redis为什么这么快 》

https://mp.weixin.qq.com/s/abjEHiMjPC8dnXweN1da-A

源码C语言、纯内存访问、单线程、IO多路复用

《四个大点，搞懂 Redis 到底快在哪里？》

https://mp.weixin.qq.com/s/4kPlBE3C6lTuSvt5mY5hUQ

（I/O复用模型，epoll）：将用户socket对应的fd注册进epoll（实际上服务器和操作系统之间传递的不是socket的fd而是fd\_set的数据结构），然后epoll只告诉哪些需要读/写的socket，只需要处理那些活跃的、有变化的socket fd的就好了。这样，整个过程只在调用epoll的时候才会阻塞，收发客户消息是不会阻塞的。

《为什么 Redis 单线程能支撑高并发？》

https://mp.weixin.qq.com/s/wINh2\_FA6B-B9jrG5V7WnA

《Redis 性能问题分析》

https://www.jianshu.com/p/67093716547b

减少网络延时，减少耗时操作，优化数据结构，OS，硬件，持久化方面，分布式，读写分离

《性能测试 —— Redis 基准测试 》

https://mp.weixin.qq.com/s/wt-qSslcka7KauiweXWwDQ

基于redis-benchmark的性能压力测试。

《Java 中 Redis 五大基本类型的用法》Java 基基

https://mp.weixin.qq.com/s/ZfE5yI7uOlquFzHqyU6Q-w

《Redis 如何保持和 MySQL 数据一致 》

https://mp.weixin.qq.com/s/CCbS61JRPbYaIXXIAamCvg

缓存先删，后查DB库，成功后再写回redis。

高并发情况下，可以将请求放在队列里，已有相同操作的情况下，轮询200ms等待读缓存。

《80% 人不知道的 Redis 分布式锁的正确实现方式（Java 版）》

https://mp.weixin.qq.com/s/7ze2v9HQH07rvYoNpUTmzw

保障锁的设置和过期具有原子性。

操作完需要手动解锁，保证自己的锁自己解，可以将锁的值设置为请求的唯一索引。

可以使用lua脚本，jedis.eval()。

if redis.call('get', KEYS[1]) == ARGV[1] then

return redis.call('del', KEYS[1])

else

return 0

end

《业务性能优化之redis批处理利器 》

https://mp.weixin.qq.com/s/BJ\_TfFTabxKztGfT69mCXA

远程调用redis的get/set会影响性能：

1，改用 pipeline，使用messagepack序列化/反序列化业务实体，以增加网络传输效率。

2，使用mq解耦

《Redis浅入浅出 -- 敖丙在蘑菇街的技术分享 》

https://mp.weixin.qq.com/s/xS2dqi5IG10AF7cHbzguAA

偏实操层面，有具体使用场景。可以参考书籍《Redis深度历险》

《面试被问 Redis 锁，我哭了 qaq 。。。》

https://mp.weixin.qq.com/s/EDR3ooUMQNF-g716Qzl8aA

讲解 Redisson的用法。更擅长分布式、集群场景下的加锁和解锁。

Zookeeper

《架构师必备：Zookeeper集群“脑裂”问题处理大全》

https://mp.weixin.qq.com/s/rtHUZyKCzvJhIEEb1X1LLA

脑裂的情况，多个分布式节点之间协调选取出Leader节点，正常就1个，但是异常情况下，由于各种原因，可能出现多个leader。

要解决Split-Brain脑裂的问题，一般有下面几种种方法：

1，Quorums (法定人数) 方式: 比如3个节点的集群，Quorums = 2, 也就是说集群可以容忍1个节点失效，这时候还能选举出1个lead，集群还可用。比如4个节点的集群，它的Quorums = 3，Quorums要超过3，相当于集群的容忍度还是1，如果2个节点失效，那么整个集群还是无效的。这是Zookeeper防止"脑裂"默认采用的方法；

2， Redundant communications (冗余通信)方式：集群中采用多种通信方式，防止一种通信方式失效导致集群中的节点无法通信。

3，Fencing (共享资源) 方式：比如能看到共享资源就表示在集群中，能够获得共享资源的锁的就是Leader，看不到共享资源的，就不在集群中。

4，仲裁机制方式；

5，启动磁盘锁定方式。

# Redis

## 【安装】

apt install redis-server

【gcc源码编译安装】

wget http://download.redis.io/releases/redis-5.0.8.tar.gz

curl --output redis.tar.gz http://download.redis.io/releases/redis-5.0.8.tar.gz

mv redis-5.0.8 /usr/redis

make

make install

https://www.jb51.net/article/136019.htm

## 【配置】

/etc/redis/redis.conf

更改

bind 127.0.0.1

protected-mode yes

更改为

# bind 127.0.0.1

protected-mode no

设置密码

requirepass dddd123 指定密码dddd123

设置防火墙的6379端口可以进行访问

### 【Redis 主从模式】

从属于某个 master，实时数据同步

1，从属命令

redis> SLAVEOF 127.0.0.1 6379

2，断开从属命令，保存同步的数据，可以作为 master 的备份体

redis> SLAVEOF NO ONE

类似功能的命令

从 5.0.0. 以后的版本

REPLICAOF hostname port

REPLICAOF NO ONE

配置文件里，可以改：

replicaof 192.168.118.131 6379

### 【Redis 哨兵模式】

安装哨兵

apt install redis-sentinel

修改sentinel配置文件

vim /usr/local/redis/6379/26379.conf

# 主要修改这一项：sentinel monitor；最后的数字表示：主掉线后，从变主的最小投票数

sentinel monitor macrog-master 192.168.24.131 6379 2

# 添加守护进程模式

daemonize yes

# 添加指明日志文件名

logfile "/usr/local/redis/6379/sentinel26379.log"

# 修改工作目录

dir "/usr/local/redis/6379"

# 修改启动端口

port 26379

# 添加关闭保护模式

protected-mode no

启动哨兵

redis-sentinel [配置文件]

哨兵工作原理，哨兵的工作流程主要分为以下几个阶段：

状态感知

心跳检测

选举哨兵领导者

选择新的master

故障恢复

客户端感知新master

## 【操作命令】

Redis 命令参考网站 http://doc.redisfans.com/

--启动 Redis

./redis-server [redis.conf]

--启动 Windows客户端连接工具

redis-cli.exe -h 127.0.0.1 -p 6379

-- Linux 下连接

redis-cli

redis-cli -h 127.0.0.1

【重启】

systemctl restart redis-server

--密码认证登录

auth "admin123456"

auth "ffpredis123" //在线版

--远程连接

telnet 172.21.126.164 6379

telnet 172.21.138.36 6379

$redis-cli -h 172.21.126.164 -p 6379 -a "ffpredis123"

--设置不需要安全模式

CONFIG SET protected-mode no

--测试是否正常

ping

--获取属性

config get paramName

config get \* // 获取全部属性

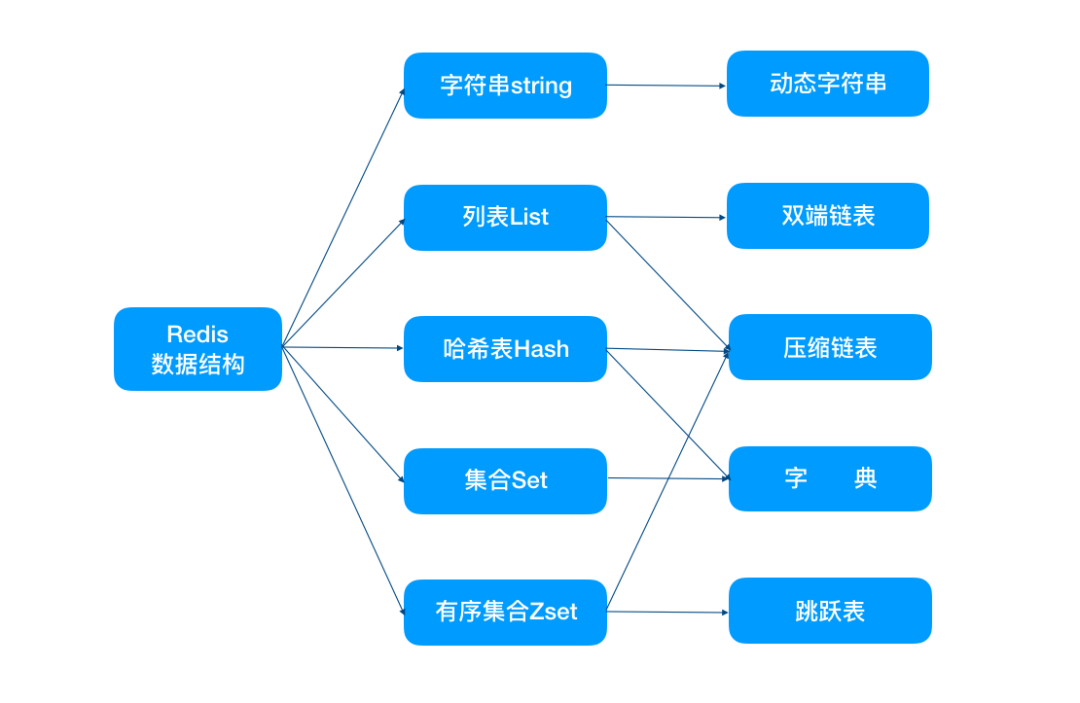
--输出 redis 安装目录

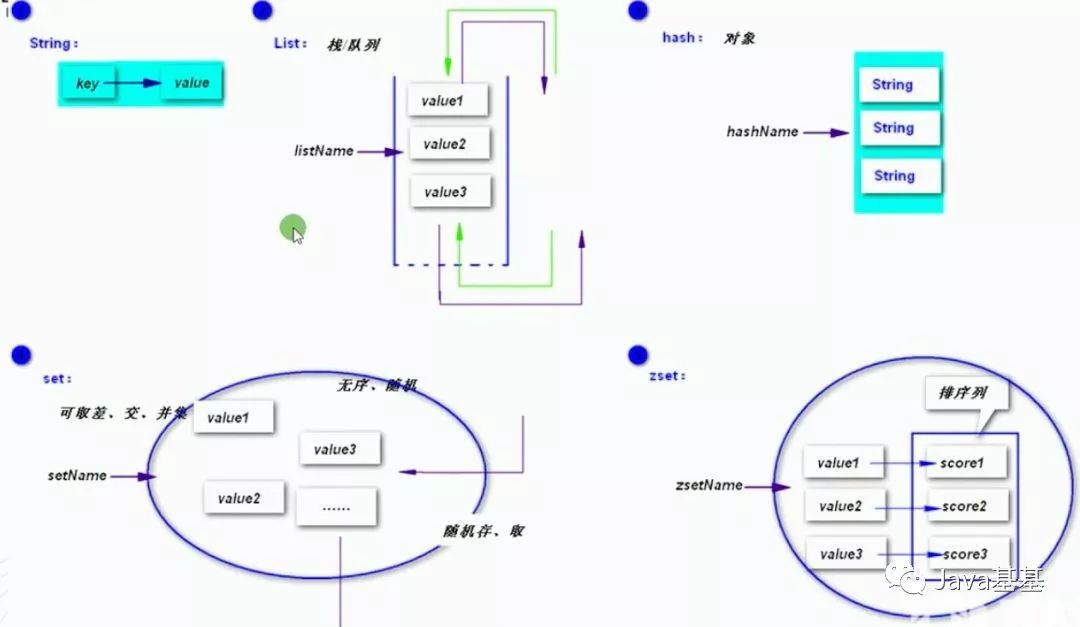
CONFIG GET dir

--设置属性"认证密码"

config set requirepass admin123456

## 【数据结构及操作】





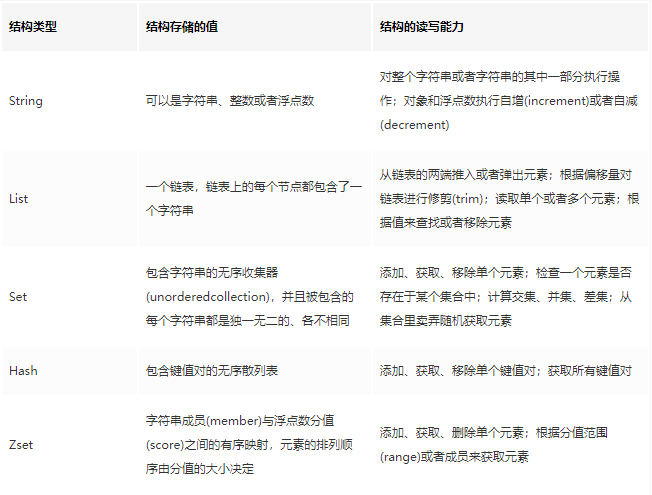
备记：hash类型，操作的是map对象，

//存值 参数第一个变量的名称， map键名(key)， map键值(value)

Long num = jedis.hset("hash1", "username", "caopengfei");

String res = jedis.hmset("hash2", map); // 存取多个key-value

jedis.hgetAll("hash2");



-- 获取全部key

keys \*

-- 设置值

set key value

setNx key value -- set if not exist

-- 不存在值即设置，返回 1；存在不做操作，返回 0

-- 获取值

get key

-- 设置过期时间

expires key 秒数

-- 获取过期剩余时间

TTL key

-- 查看redis服务

ps -ef |grep redis

【查看当前 redis 角色等信息】

info replication

【sortedset】有序集合

127.0.0.1:6379> ZADD b 1 zookeeper

127.0.0.1:6379> zadd b 1 redis

127.0.0.1:6379> zincrby b 2 "zookeeper"

127.0.0.1:6379> add b 2 mongodb

127.0.0.1:6379> zrevrange b 0 1 withscores // 降序前2

1) "zookeeper"

2) "3"

3) "mongodb"

4) "2"

127.0.0.1:6379> zrange b 0 1 withscores // 升序前2

1) "redis"

2) "1"

3) "mongodb"

4) "2"

127.0.0.1:6379> ZRANGE b 0 -1 withscores // 全部

1) "redis"

2) "1"

3) "mongodb"

4) "2"

5) "zookeeper"

6) "3"

### 【持久化】

save

该命令将在 redis 安装目录中创建dump.rdb文件，将 cache 数据保存到文件中

【恢复数据】

如果需要恢复数据，只需将备份文件 (dump.rdb) 移动到 redis 安装目录并启动服务即可。

bgsave

在后台新的子进程进行备份，可以使用lastsave查看最新的进度。

Redis有RDB和AOF的持久化机制。

RDB：基于快照，将某一时刻的所有数据保存到一个RDB文件中，默认方式。

AOF(append-only-file)，当Redis服务器执行写命令的时候，将执行的写命令保存到AOF文件中，默认关闭。

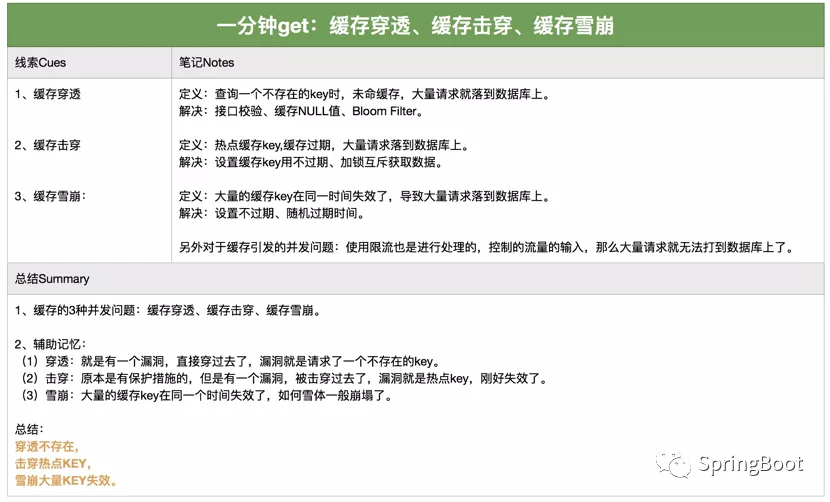
AOF持久化功能的实现可以分为3个步骤：

命令追加：命令写入aof\_buf缓冲区

文件写入：调用flushAppendOnlyFile函数，考虑是否要将aof\_buf缓冲区写入AOF文件中

文件同步：考虑是否将内存缓冲区的数据真正写入到硬盘

## 【实践】



# Zookeeper

ZooKeeper “动物管理员”

ZK是一个树形的目录服务

作用：协调分布式的系统

做 “配置中心”，Eureka 与 ZK 功能类似

## 【安装】

apt install zookeeper

## 【配置】

Connection() 链接

//server：172.21.126.163:2181,172.21.126.164:2181,172.21.126.165:2181

this.zk = new ZooKeeper(server, 6000, this);// 初始化 zk

[SYSTEM]

THREADS=100

COMMANDTIMEOUT=60

[JMS]

#AQ\_URL=tcp://172.21.126.164:61616

AQ\_URL=failover:(tcp://172.21.126.163:61617,tcp://172.21.126.164:61617,tcp://172.21.126.165:61617)?Randomize=false

[REDIS]

#IP=172.21.126.164

IP=172.21.126.165:26380,172.21.126.165:26381

PASSWORD=ffpredis123

【ZK节点类型】

1.持久节点(persistent)

持久节点，创建后一直存在，直到主动删除此节点。

2.持久顺序节点(persistent\_sequential)

持久顺序节点，创建后一直存在，直到主动删除此节点。

在ZK中，每个父节点会为它的第一级子节点维护一份时序，记录每个子节点创建的先后顺序。

3.临时节点(ephemeral)

临时节点在客户端会话失效后节点自动清除。临时节点下面不能创建子节点。

4.顺序临时节点(ephemeral\_sequential)

临时节点在客户端会话失效后节点自动清除。临时节点下面不能创建子节点。

父节点 getChildren 会获得顺序的节点列表。

## 【操作命令】

Create() 创建节点

String zkPath = "/ffp/commands/" + SystemConfig.getAppId();// /ffp/commands/FFPSERVER\_ZHOUMIN\_1

this.zk.create(zkPath, json.getBytes(), Ids.OPEN\_ACL\_UNSAFE, CreateMode.EPHEMERAL);

GetChildren()获取子节点

this.zk.getChildren(name, watch);// name:/ffp/commands，获取子节点

[FFPSERVER\_SYSTEM\_1, FFPSMSEMAIL\_SYSTEM\_1, FFPSERVER\_XUPING\_1]

删除节点

//if (zk.exists("/mcp/commands/"+SystemConfig.getAppId(), true)==) {

zk.delete("/mcp/commands/" + SystemConfig.getAppId(), 0);// 创建节点前不能存在同名节点？

//}

GetData()获取数据

this.zk.getData(name, false, null);// name:/ffp/config/FFPWEB，获取节点（的配置信息？）

监控数据变化

@Override

public void process(WatchedEvent event)

根据 WatchedEvent 的不同枚举类型，进行相应的操作

*// ZkClient client = new ZkClient("192.xxx:2181");*

client.subscribeChildChanges(path, new IZkChildListener() {  
 @Override  
 public void handleChildChange(String s, List<String> list) throws Exception {  
 System.*out*.println("service change:" + s);  
 list.forEach(s1 -> System.*out*.println(s1));  
  
 serviceList = list;  
 }  
});  
client.subscribeDataChanges(path, new IZkDataListener() {  
 @Override  
 public void handleDataChange(String s, Object o) throws Exception {  
 System.*out*.println("data change:" + s + " → " + o);  
 }  
  
 @Override  
 public void handleDataDeleted(String s) throws Exception {  
 System.*out*.println("node deleted:" + s);  
 }  
});

## 【zkcli脚本命令介绍】

zkcli 连接默认zookeeper服务器

zkcli -server ip:port 连接指定的zookeeper服务器

create -s -e path data [acl] 创建节点，-s表示顺序，-e表示临时，默认是持久节点，acl缺省表示不做任何权限限制

ls path [watch] 显示path下的节点，不递归显示，watch注册监听，命令行可忽视

ls2 path 显示当前节点下的节点和当前节点的属性信息

get path [watch] 获取path的属性信息和数据内容

set path data [version] 更新path的数据内容，version是做类似cas的功能的对应dataversion，命令行可忽略

delete path [version] 删除节点，不能递归删除，只能删除叶子节点

setacl path acl 设置节点acl，例子(scheme:id:password=:perm)-(digest:example:sha-1(base64(pwd))=:cdrwa) create delete read write admin

getacl path 获取path节点的acl

stat path 查看path的属性信息

quit 退出zkcli

# Oshi

测试案例：

public class test {  
 public static void main(String[] args) {  
 SystemInfo systemInfo = new SystemInfo();  
 HardwareAbstractionLayer hardware = systemInfo.getHardware();  
 GlobalMemory memory = hardware.getMemory();  
 for (PhysicalMemory m : memory.getPhysicalMemory()) {  
 System.*out*.println(m.getManufacturer() + " " + m.getCapacity());  
 }  
 }  
}

## SystemInfo 总类（门面？）

包含：

PlatformEnum

1，OperatingSystem

不同的OS

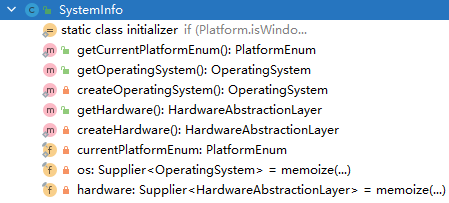
2，HardwareAbstractionLayar

基于不同OS的硬件抽象

Eg. WindowsHardwareAbstractionLayer

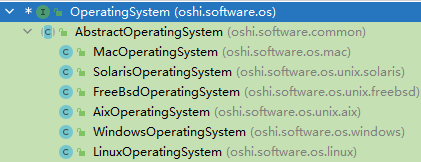
具体不同的硬件

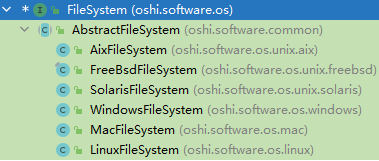
Eg.Processor(CPU), Memory



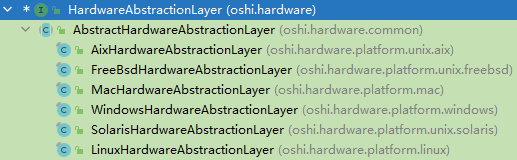
## 重要类的层级关系

### OS





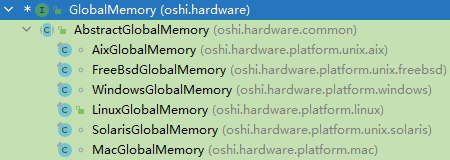
### 硬件 Hardware

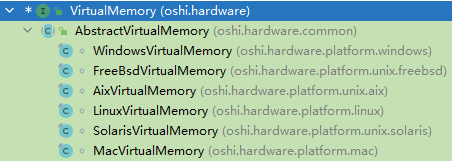


#### ComputerSystem

#### Processor

#### Memory





#### Sensors

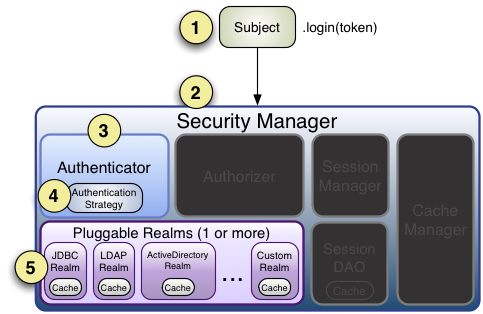
# Shiro，兼ruoyi框架学习

教程： https://www.w3cschool.cn/shiro/

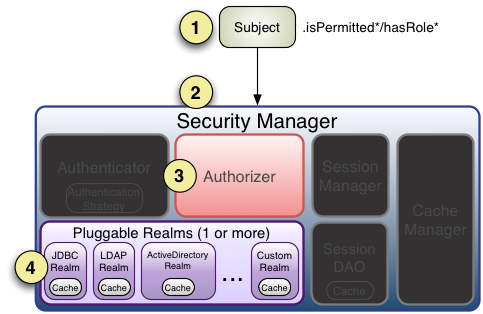
核心类和架构



身份认证流程



鉴权流程（授权？）



## 配置类

**com.ruoyi.framework.config.ShiroConfig**

★ securityManager

- userRealm

- remembermeManager

- enCacheManager

- sessionManager

> loginUrl

> unAuthorizedUrl

· OnlineSessionFilter 根据session\_id 读取 sys\_user\_online 表

- OnlineSessionDAO

· SyncOnlineSessionFIlter 每个请求（60s间隔）都会更新到 sys\_user\_online 表

- OnlineSessionDAO

· CaptchaValidateFilter

· KickoutSessionFilter

· LogoutFilter

-- 免登陆页面

-- 需要校验验证码的页面

▲ShiroDialect：thymeleaf 和 shiro整合的bean

▲AuthorizationAttributeSourceAdvisor：shiro注解通知器？

## 配置文件

classpath:ehcache/ehcache-shiro.xml

## 认证和鉴权类

登录流程：

com.ruoyi.project.system.user.controller.LoginController#ajaxLogin 登录入口类

1，准备登录实体，UsernamePasswordToken和Subject

2，判断重试次数，超过阀值直接返回报错

3，校验username、password（md5 + salt）是否匹配

不匹配的话，就记录错误次数

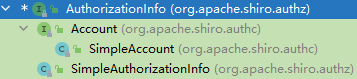
认证成功是由UserRealm处理的，封装生成SimpleAuthenticationInfo 实体

登出流程

在 LogoutFilter里定义，过滤器里logout，SecurityUtils.getSubject().logout()

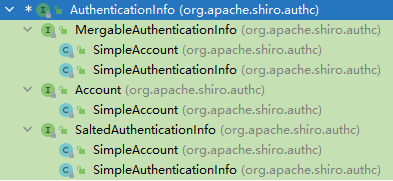
鉴权授权：com.ruoyi.framework.shiro.realm.UserRealm#doGetAuthorizationInfo

返回 SimpleAuthorizationInfo 类型实体，包含roles、permissions

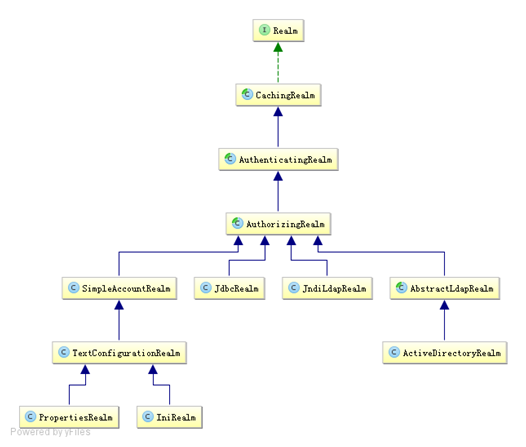


登录认证：com.ruoyi.framework.shiro.realm.UserRealm#doGetAuthenticationInfo

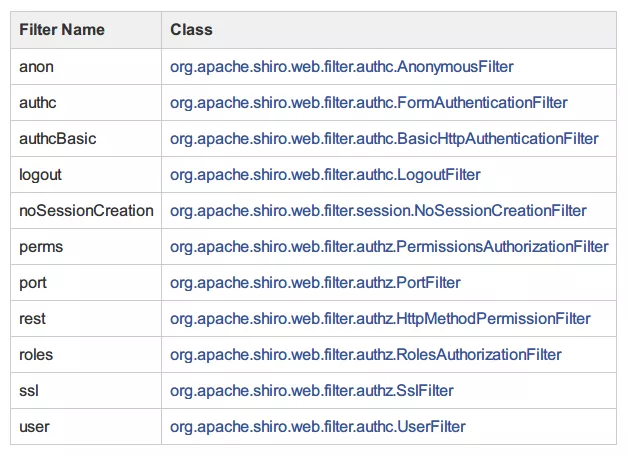
返回 SimpleAuthenticationInfo 类型实体，包含username、password

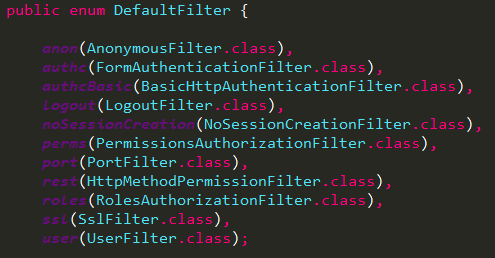


UserRealm 继承了 AuthorizingRealm 类



Shiro的过滤器





### 一、菜单级权限

1，菜单加载

获取当前登录用户

Shiro: SecurityUtils

Ruoyi: ShiroUtils

com.ruoyi.common.utils.security.ShiroUtils#getSysUser

获取菜单，menuService.selectMenusByUser(user)，前台生成菜单

2，菜单鉴权

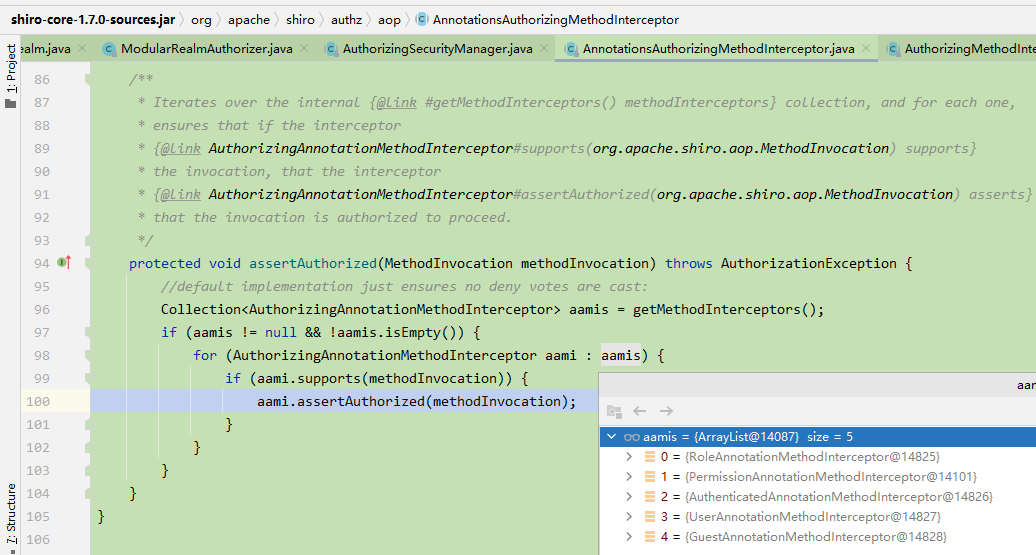
每个菜单都绑定了 [一级模块:二级模块:view] 权限，类似操作级权限的鉴权，具体看下小节。

校验不通过时，报AuthorizationException异常。

public void checkPermission(PrincipalCollection principals, String permission) throws AuthorizationException {  
 assertRealmsConfigured();  
 if (!isPermitted(principals, permission)) {  
 throw new UnauthorizedException("Subject does not have permission [" + permission + "]");  
 }  
}

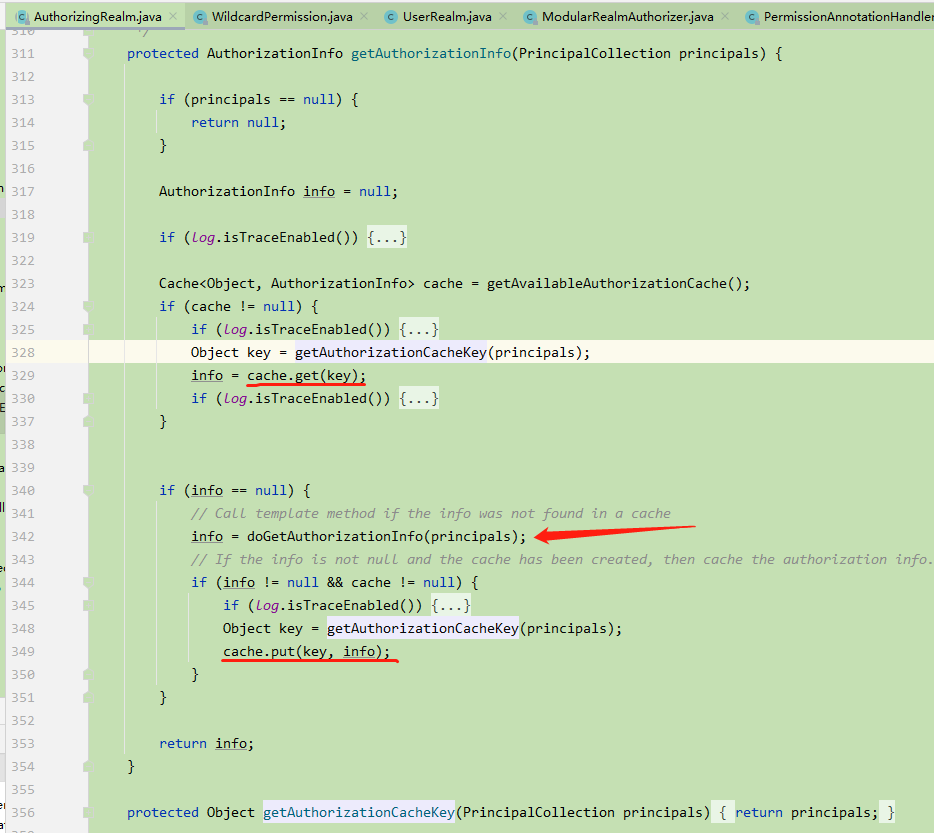
### 二、操作级权限

方法上可以加的注解，@RequiresRoles， @RequiresPermissions(模块:功能:操作，例如：sys:user:edit)，@RequiresAuthentication等



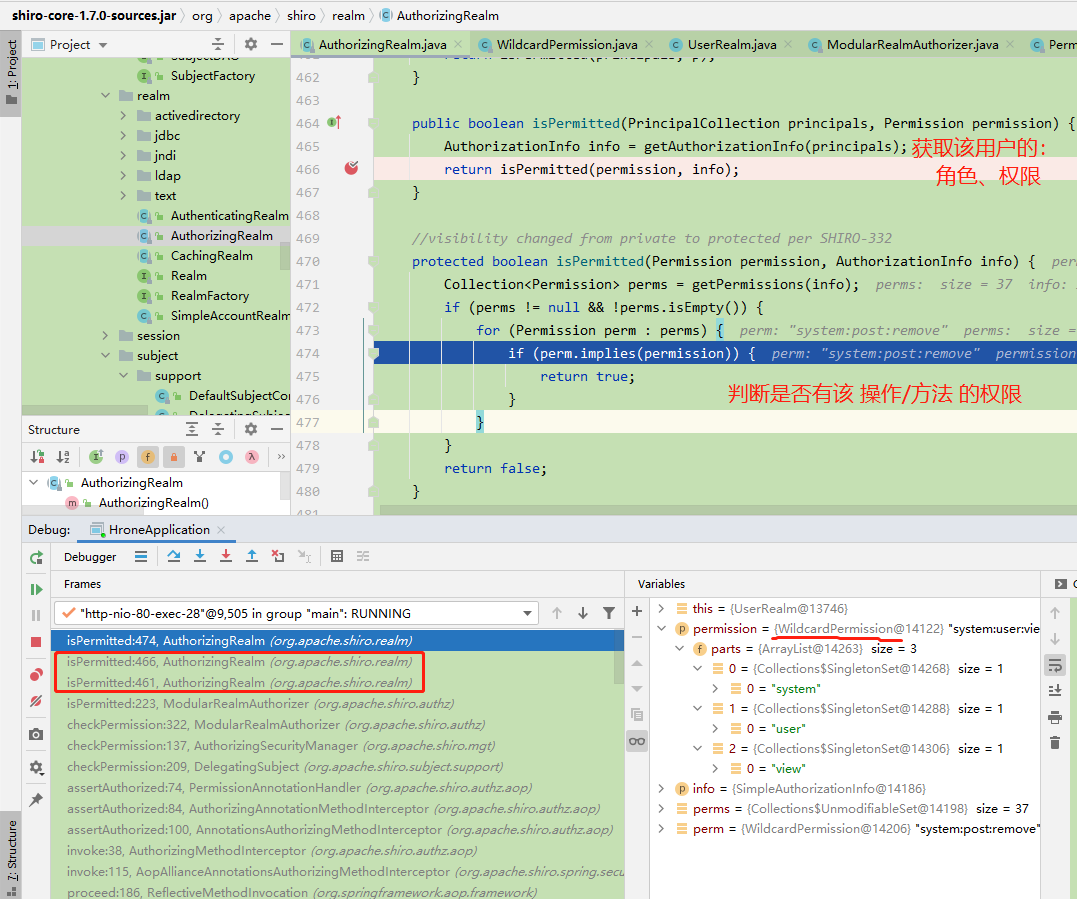
1，该用户、角色全部权限的加载

存在缓存的机制，有缓存直接返回；不存在的话调用子类重新的方法，再cache一下。



2，权限的鉴定

获取权限（上面第1步），和用户需要访问，或操作的权限进行比对



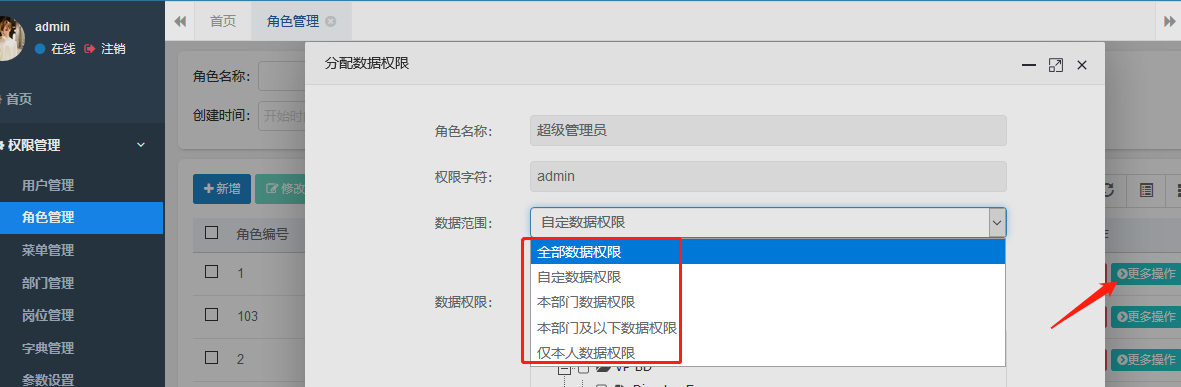
未通过校验时，报AuthorizationException异常。在全局异常处理器里，友好反馈。



### 三、数据级权限

1，定义的位置

1.1 前台页面上，对角色的数据权限进行设置



1.2 对具体的实体操作上，需要在Service类的方法上，加@DataScope注解

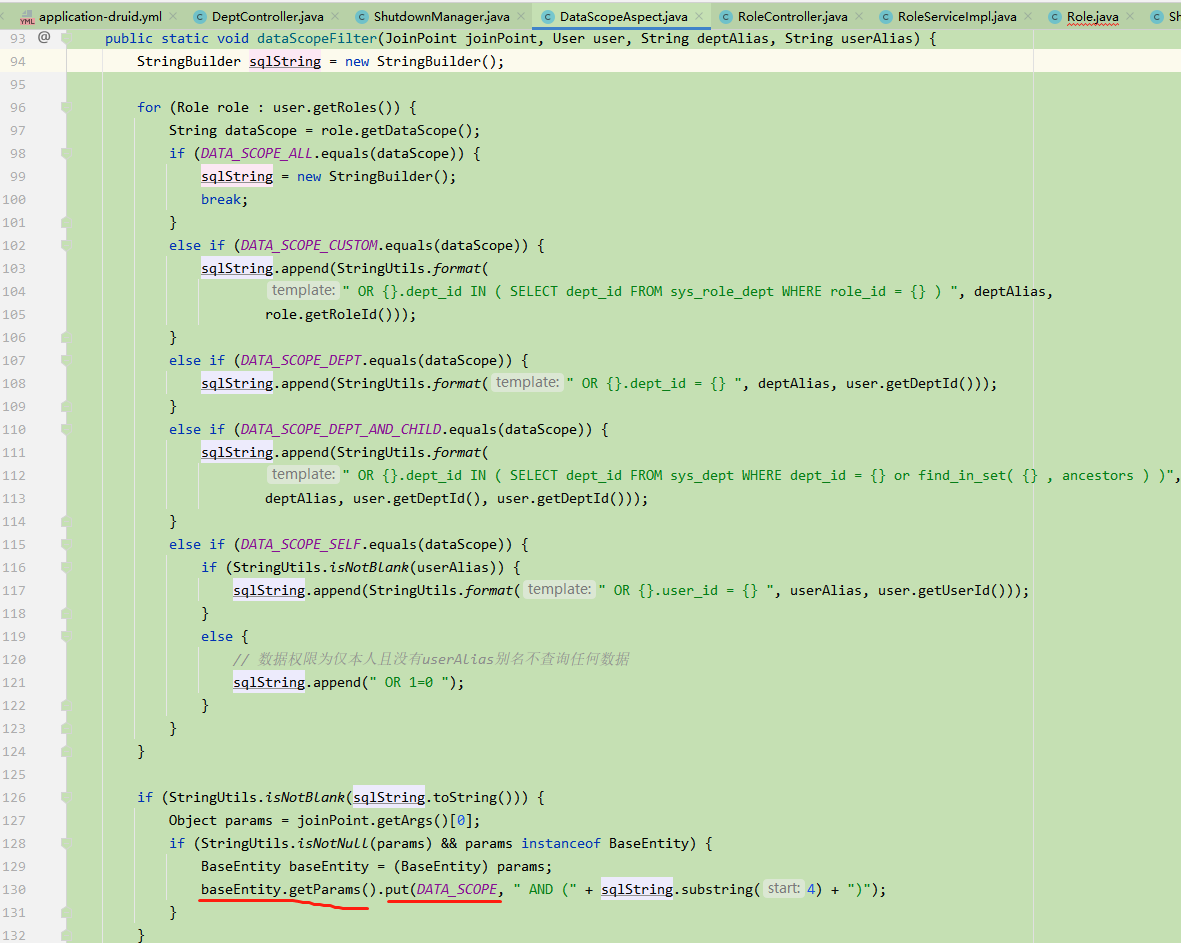
@Override  
@DataScope(deptAlias = "d", userAlias = "u")  
public List<SysUser> selectUserList(SysUser user)  
{  
 return userMapper.selectUserList(user);  
}

2，实现原理

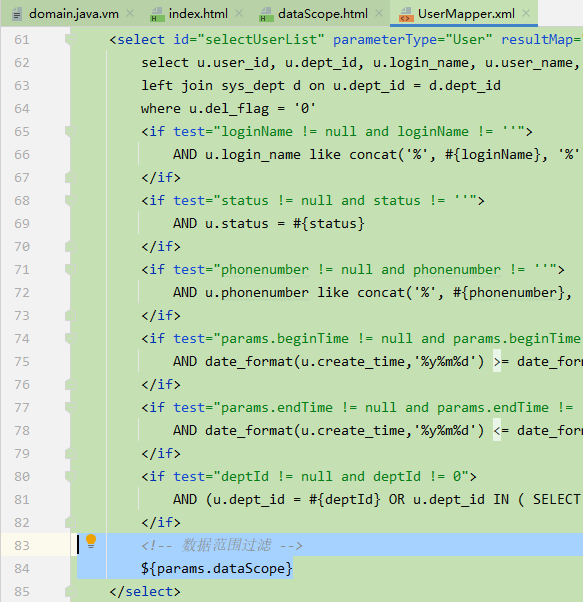
com.ruoyi.framework.aspectj.DataScopeAspect 里面，对@DataScope注解的AOP增强

protected void handleDataScope(final JoinPoint joinPoint) {  
 *// 获得注解* DataScope dataScope = getAnnotationLog(joinPoint);  
 if (dataScope == null) {  
 return;  
 }  
 *// 获取当前的用户* User currentUser = ShiroUtils.*getSysUser*();  
 if (currentUser != null) {  
 *// 如果是超级管理员，则不过滤数据* if (!currentUser.isAdmin()) {  
 *dataScopeFilter*(joinPoint, currentUser, dataScope.deptAlias(), dataScope.userAlias());  
 }  
 }  
}

params变量在BaseEntity里，增加上key为“dataScope” 的sql条件过滤语句。



3，具体执行的地方，sql里加上过滤条件



4，鉴权

目前系统里没有查询单个详情的API，否则前台容易伪造主键id去查询。

漏洞：拥有修改、删除等权限的用户，可能通过伪造主键id修改别的部门数据。

## 工具方法

密码加密模块

默认是 md5 散列值

com.ruoyi.framework.shiro.service.PasswordService#encryptPassword

缓存操作类

com.ruoyi.common.utils.CacheUtils

异步执行管理器

com.ruoyi.framework.manager.AsyncManager

线程池配置

com.ruoyi.common.config.thread.ThreadPoolConfig

装配Bean: ThreadPoolTaskExecutor 线程池类，ScheduledExecutorService 计划执行池类

关闭程序前，关闭后台线程

ShutdownManager

# EhCache

配置

核心类

