# B简历：

# -------------------------------------------

### 基本信息

|  |  |  |  |
| --- | --- | --- | --- |
| 基本情况 | | | |
| **姓名** | **王少鹏** | 性别 | 男 |
| **出生日期** | 1993-02-23 | 属相 | 猴 |
| **现住地** | 丰台区 东营里 2号院 |  |  |
| 大学情况 | | | |
| **学校** | 南昌理工学院 | 专业 | 计算机应用技术 |
| **入学时间** | 2011-9 | 毕业时间 | 2015-7 |
| **专业课** | **C语言、数据结构课程设计、数据库原理课程设 计、操作系统实训、Java程序设计** | | |
| **学历** | **本科** | 学位 | **学士学位** |
| **学校地址** | 江西省南昌市昌北经济开发区英雄大道901号 | 校长 | **学校领导都没见过，所以也不知道校长的名字** |
| **去学校的方式：** | **在火车站乘232路公交车到枫林大道下车** | | |
| **上小学日期：** | **1999年9月 6岁六年** | | |
| **上初中日期：** | **2005年9月 12岁三年** | | |
| **上高中日期：** | **2008年9月 15岁三年** | | |
| **上大学日期：** | **2011年9月 18岁四年** | | |
| **毕业时间：** | **2015年 7月 22岁** | | |
| **在校学生：** | **5000左右** | | |
| **有教师：** | **不太清楚** | | |

|  |  |
| --- | --- |
| 第一家公司 ： | 北京艾雷朗特软件开发有限公司 |
| **地址：** | 北京市北清路68号用友软件园（只说大厦名称） |
| **入职时间：** | **2015年8月初** |
| **离职时间：** | **2017年1月** |
| **公司性质：** | **民营** |
| **职位：** | **Java工程师** |
| **项目经理名字：** | **张惠涛** |
| **薪资方面：** | **刚刚毕业转正以后工资是6K左右，过完年大概三月份涨到7K左右** |
| **路线：** | 步行90米龙跃苑一区西门站上车 昌25路,13站 佰嘉城北门站下车步行300米二拨子站 上车543路 11站, 永澄路口西站 下车,步行 500米 |

|  |  |
| --- | --- |
| **第二家公司情况：** | 北京华城兴业软件开发有限公司(只说公司简称) |
| **公司地址**： | **北京市丰台区丰台镇 东货场路38号11栋116A室** |
| **公司规模：** | **80人左右，我们项目组8人，一个项目经理，4名开发人员，1名前端，1个测试，1个运维** |
| **公司性质：** | **民营** |
| **公司行业：** | **互联网和虚拟现实的软件产品的开发。** |
| **去公司路线：** | 460路 → 地铁13号线 → 地铁10号线 → 地铁9号线 |
| **入职时间：** | **2017年2月** |
| **离职时间：** | **2019年11月初** |
| **职位：** | **Java工程师** |
| **项目经理名字：** | **于笑** |
| **税前：** | **15K** |
| **税后：** | **14K** |
| **缴税：** | **1K左右(具体原因不清楚当时公司就是这样扣的税)** |
| **期望薪资：** | **16K** |
| **薪资的构成:** | **岗位工资(5K)+绩效工资(10K)** |

|  |
| --- |
| 四年涨薪： **2015年工作的时候是5.5K，税后大概5.4K左右，**  **转正6K左右**  **2016上半年涨了1K左右 ，总7K左右。**  **2017年2月跳槽涨了3K左右 总10K**  **2017年12月涨1K总 11K左右**  **2018年9月工作一年涨了2K左右**  **2019年7月工作一年涨了2K左右**  **2019年11月初离职时工资为15K** |

**面试常见问题：**

|  |
| --- |
| **你为什么从上家公司离职？** |
| **想换个工作环境，不断的提高充实自己** |
| **你交社保了吗？为啥没交？** |
| **没交**  **在上家公司的时候，人事说咱们公司的五险一金如果要上的话都是从自己工资里面扣的，当时感觉没啥必要也就没上。** |
| |  | | --- | | **三个词形容自己**： 交流表达能力强，团队协作能力强，抗压自学能力强 (**可以综合自己自学的知识表达**) | | **你的优缺点是啥？** |   **优点:**  **抗压能力强（有一次项目就要上线了，连着加班了一周，每天都到夜里很晚，但我最后也是成功完成任务。），**  **乐于分享，**  **团队协作能力强**  **缺点: 我这个人说话比较直，你像在和团队成员探讨问题的时候，容易得罪人，**  **不过现在已经改进的差不多了** |
| **你知道五险一金都是啥吗？** |
| **养老保险、医疗保险、失业保险、工伤保险、生育保险，和住房公积金。** |
| **你能接受加班吗** |
| **能** |
| **你能接受出差吗** |
| **能** |
| 你期望薪资多少？你上家工资多少？税后拿到手的有多少？扣了多少钱的税？ |
| 期望薪资 16K 上家工资15K 税后14K左右 扣了1K左右的税 |
| 你的五年规划是啥？ |
| **前2,3年 继续加强自己的技术功底，**  **然后朝着项目经理(技术经理,产品经理)方面发展** |
| 是统招吗 是是本科吗 是能在学信网查到吗 我当时上的是民办大学，能在民教网查到！ |
| 你们公司还有什么福利？多少薪： 13薪  **车补**  220左右  **项目奖金**  8k-10k，做完项目，收完尾款的时候发。  **年终奖**  就是1个月的工资，  最后一个月和工资一块儿发/年后发  **电话补助**  260  **饭/餐补**  **15、**30/天  **电脑补**  310 |

**公司内其他部门：**

**技术部，人事部，销售部，财务部**

**---------------------------------------------------------------------**

**其他问题：**

**笔试问题：我工作这么多长的时间了，理论上的知识忘得差不多了，你和你们经理联系一下直接面试吧，不行的话那么我就去直接去下一家！**

**-----------------------------------------------------------------------------------------------------------------**

# **业务功能模块:**

-->日志管理-->负载均衡加redis分布式session-->基于Token的用户登录【jwt】--> 基于redis的购物车-->订单

-->项目的重构【从ssmp框架升级为springboot+springcloud组成的微服务】

-->sql优化-->通过线程池提高程序的性能

**核心概念：**

**咱们也知道这几年这个微服务springboot和springcloud用的非常多，而我在上一个项目中使用的也是这个springboot+springcloud进行的开发，那我就先说一下这个我对这个微服务框架的理解吧：**

当时在做的时候用的是

Eureka建立注册中心项目，在pom文件中引入Eureka的依赖，之后在启动类中加入 @EnableEurekaServer的注解证明该项目的作用是作为注册中心使用，并且在对应的application.properties中指明Eureka注册中心服务器的地址，方便提供者和消费者对其进行访问，为了增强注册中心的高可用性，我们做了Eureka集群，防止因为单台Eureka导致的单点故障问题。通过注册中心可以让服务端注册到注册中心上去，并且可以进行负载均衡；这样就可以达到高可用以及提高并发的 目的。客户端 也不需要 直接 调用服务端，而是通过注册中心获取地址列表，从地址列表中选一个服务端接口进行调用，后续的维护各方面也会比较方便。

具体开发一个微服务的时候使用的是SpringBoot，首先在项目的pom文件中同样需要引入Eureka的依赖，并且在application.properties文件中通过spring.application.name指明自身的服务名以及注册中心的地址，这样才能将其注册到注册中心中被其他消费者访问。

在项目中还使用到了 @SpringBootApplication，之所以可以省略那么多的配置文件，靠的就是这个注解。这个注解的本质是包含了 @Configuration， @EnableAutoConfiguration， @ComponentScan这三个注解，通过这些注解就起到了扫描类以及自动加载配置信息的作用。

还在biz/service业务层上通过 @Transactional(rollbackFor = Exception.class)指明了事务的控制，使其在抛出Exception异常时能够回滚。默认情况下事务只对运行时异常进行回滚所以才会通过rollbackFor = Exception.class将其改为对所有的异常都进行回滚。想要在service层注入 Mapper 层的接口，还需要在启动类上加入 @MapperScan这个注解对其Mapper层的接口进行扫描。

如果没有注册中心，客户端通过ip地址访问服务端，如果服务越来越多，调用也会越来越复杂，一旦ip地址发生变动，则所有用到的地方都需要发生改变，维护起来会特别麻烦；如果服务端宕机了，所有访问的客户端也都会受到影响。

总体来说在项目中我们使用SpringBoot开发微服务并结合SpringCloud的注册中心Eureka和支持负载均衡的客户端Feign来完成整个项目的开发,使用Zuul充当网关；其中Feign是为了在微服务之间进行调用的时候使用，而Zuul发挥了反向代理和负载均衡的作用，前端发送的所有请求经过Zuul，进行安全验证，通过后再转发到具体的微服务上。

**在这个微服务的搭建过程中也有可能发生微服务雪崩的问题**

，说白了就是A->B->C,如果C这个微服务出现问题，就会影响到B,同样B出现问题，就会导致A也出问题，最后导致所有的微服务都不可用。就像咱们现实生活中，一个路口堵车，就会导致整条街慢慢拥堵，再后来影响的范围就会越来越大。为了解决这个问题同时也是为了保证我们微服务的高可用性我们当时使用到了Hystrix。

咱们都知道Hystrix可以进行熔断，降级和资源隔离。熔断其实就可以理解成咱们家里面的保险丝。保险丝是为了保证在高负载情况下电路的安全，如果某个电路出现了负载过大情况，保险丝就会熔断，从而保证其他电路不受影响。Hystrix的熔断功能比较强大，它还可以进行自动检测并修复。

具体的原理是这样的，默认情况下在10s内，每当20个请求中，有50%失败时，就会触发熔断，导致hystrix从闭合状态切换到打开状态，这样就不需要每次都去调用远程微服务而是直接走调用者本地的降级方法。5秒后hystrix会进入到半打开状态，这时如果有新的请求再过来hystrix就会尝试再次进行远程微服务调用，如果调用成功就会进入到闭合状态，如果不成功就会再次进入到打开状态，继续进行熔断。这个就是hystrix的自动检测并修复的能力。

降级说白了就是进行熔断后需要执行本地的方法。也是为了保证微服务的高可用。

[说白了就像咱们看的打仗时候的急行军，为了保证按时到达作战地点，我就把身上其他的干粮，背包全部丢掉，只带上最基本作战的武器，快速前进保证最终的结果。**可以省略**]

在Hystrix中, 有两种资源隔离方式，信号量隔离和线程池隔离，我们主要用的是线程池隔离. 通常在使用的时候我们会根据调用的远程服务划分出多个线程池. 比如调用产品服务的Command放入A线程池, 调用会员服务的Command放入B线程池. 这样就可以将运行环境隔离开。就算调用服务的代码存在bug或者由于其他原因导致自己所在线程池被耗尽, 也不会对系统的其他服务造成影响。

**接下来我来说下这个Feign的使用吧**

我们当时在项目中有很多的模块需要互相调用，比如说这个购物车需要调用商品进行 查询，我们当时为了解决这个问题使用的是Feign来进行微服务之间的调用

又因为Feign集成了Hystrix,所以我们当时通过在配置文件中开启hystrix,并且在具体使用Feign的接口上通过 @FeignClient 中的 Fallback指定降级时候需要执行的类即可。这样在熔断后就会自动调用Fallback类中对应的降级方法，降级方法中，可以记录下日志并且返回null。这样使用Feign的客户端在调用 远程微服务 的方法后，判断返回值是否为null,如果是null则证明走了降级方法，进行特殊处理就行。

Feign还拥有负载均衡的特性，说白了它是靠Ribbon进行的负载均衡。在 @FeignClient的注解上指明要调用的微服务的名字，这样就可以通过该服务名从注册中心Eureka中获取对应的地址列表，方便进行负载均衡的调用。

其次我们会创建对应的服务端，服务端项目中要保证 请求的方式，请求的地址以及方法名，返回值，参数都要和feign中定义的保持一致。

**--》Zuul**

接口安全这方面的话我们是用zuul来里面的过滤器进行处理的

因为这个外部客户端的请求都是通过Zuul网关路由到具体的微服务，所以为了保证微服务的安全，我们就在Zuul中自定义了过滤器，对所有微服务的安全进行统一的处理，还有，因为涉及到前后端分离，前端项目访问后端微服务涉及到跨域问题，所以我们在Zuul中 也自定义了关于跨域的过滤器，进行统一处理。

具体是这么做的，首先你得先定义一个继承于ZuulFilter的类，重写里面的filterType()方法filterOrder()方法，shouldFilter()方法，还有一个最核心的用来写具体业务逻辑的run()方法。其中filterType方法的作用是用来返回一个字符串，指明该过滤器的类型，经常用到的有pre类型，说白了就是在请求被发送到微服务之前调用；我们的微服务安全认证以及跨域这块都是用的pre类型的过滤器，这样对非法请求，就可以在发送到具体的微服务之前拒绝它；

还有post类型，说白了就是微服务执行完后再执行该过滤器，filterOrder()方法返回一个int类型的值，用来指明该过滤器的执行顺序，数字越小表示优先级越高，就越先执行，shouldFilter()方法返回一个boolean值，用来指明该过滤器是否执行，true表示执行,false表示不执行。

run方法中就是之前说的，用来放具体的处理逻辑。

在run方法中，首先获取一个RequestContext对象，之后就可以通过调用它的getRequest()方法来获取request对象；这样就可以获取头信息，按照之前基于token的方式进行接口的安全验证，至于这个基于token的登录说白了就是自己写的一个类似于jwt的登录，这个我在后面在做介绍。

过程中特别需要注意的就是当验证不通过的时候，需要通过fastjson将要响应的数据转换为json格式的字符串，之后设置响应的内容类型为application/json并且指定utf-8的编码方式，用来处理中文乱码问题；通过setResponseBody将Json格式的字符串设置为响应的内容，最后通过setSendZuulResponse为false，禁止路由转发。如果想要将zuul过滤器中的数据传递给后端微服务中使用，则需要通过addZuulRequestHeader方法来进行，而后端微服务中就可以通过request.getHeader来获取值。这里面需要特别注意的就是，如果传递的数据中含有中文则需要通过URLEncoder进行utf-8的编码，同样在获取数据后也需要通过URLDecoder进行解码。

最后想要使自定义的过滤器生效，得进行相关的配置。我通过创建一个配置类，

并且在类上通过 @Configuration 和 方法上的 @Bean 结合起来，完成自定义filter的配置。

这就是我们当时搭建这个微服务框架的一个过程

**至于这个springboot的运行原理的话 我也做过一些了解**

在我看来他的运行原理就是最核心的两行代码

@springbootapplication 和 springappliction.run方法

在 @SpringBootApplication 的内部包含了3个注解

@Configuration

@EnableAutoConfiguration

@ComponentScan

@Configuration是基于JavaConfig形式的Spring Ioc容器的配置类，可以把它看成xml配置文件中的beans标签。 @Configuration写到类上面，在类中的方法上如果写了 @Bean注解，那么它的返回值将作为一个bean注册到Spring的IoC容器，方法名默认作为bean的id。

@ComponentScan这个注解对应XML配置中的context:component-scan元素， 说白了它的作用就是自动扫描并加载符合条件的组件,比如 @Component和 @Service等或者bean定义，最终将这些bean定义加载到IoC容器中。

我们可以通过basePackages来指定 @ComponentScan 自动扫描的范围,如果不指定，则默认Spring框架实现会从声明 @ComponentScan所在类的package进行扫描。这也是SpringBoot的启动类最好是放在root package下的原因。

@EnableAutoConfiguration 这个注解是借助 @Import的帮助，将所有符合自动配置条件的bean定义加载到IoC容器中。

**功能模块这部分的话当时**

我负责的功能模块的有这个类似jwt的基于token的登录，购物车，订单，以及支付这些模块

那我就先来介绍下这个

基于Token的用户登录吧

这个token登录啊，我刚才也说了是类似于jwt的登录，说白了就是自己写的一个jwt，咱们也知道网上有开源的jwt jar包，但是我感觉这个东西不太好用而且这个毕竟不是自己写的可控性不好，所以就决定自己写一个类似的登录方式，想改什么自己也能直接改，用起来也更灵活。

业务实现这方面 他大概的流程是这样的：用户在前台输入用户名密码通过ajax发送请求到后台接口，后台接口在进行层层验证后，如果验证成功就把响应信息传给前台，前台会在ajax的成功回调函数里面接受到数据，把他暂时存到会话cookie中，在后续发送请求的时候，再从cookie中取出数据把他放到header中通过自定义header的方式传到后台接口的拦截器中进行各种验证，通过验证后才能访问登录后的资源。至于这个自定义的header，我当时起的名字叫x-auth。

具体在做的时候我遇到了这么几个问题：

首先是ajax跨域请求的问题，因为当时采用了分布式的开发方式，所以前台页面和后台接口在两个不同的微服务中，因为端口号和ip地址不同所以就涉及到了跨域问题，咱们都知道ajax默认是不允许跨域的，解决这个跨域问题的方式有多种，可以通过jsonp,也可以通过spring给咱们提供的一个叫 @CrossOrigin的注解来实现，或者自己写一个CorsFilter来实现，但是我们当时的项目中所有的请求都会先经过zuul网关的过滤器进行安全验证，所以我就将跨域处理的相关代码写到了过滤器里面。

实现的时候是首先获取一个RequestContext对象，之后就可以通过调用它的getResponse()方法来获取response对象

然后调用response的setHeader方法添加几个头信息来允许ajax的跨域请求，具体记得不是太清楚了，好像叫allow\_methods,allow\_headers还有allow\_origin;其中allow\_methods指明能够接受的跨域的请求类型，比如 put,get,post,delete,options这些，allow\_headers指的是允许接受的自定义的头信息，allow\_origin表示允许 跨域的远程ip地址和端口号。

再者ajax跨域的时候要传递头信息，我们为了让每个ajax发送请求时候都能自动加上这个自定义头信息进行传递，我就写一个公共的js文件，并且在这个js文件中通过了$.ajaxSetup来定义全局的ajax设置，并且通过beforeSend 函数来在所有ajax发送请求前，通过xhr.setRequestHeader传递自定义的头。这样在每个前台页面中引入这个公共的js文件就可以了。

然后就是这个后台登录接口的处理逻辑，先进行各种非空判断以及用户名和密码的验证，如果都成功则将会员id,会员名，以及一个uuid组成json格式的字符串，并通过base64进行编码；之后将base64编码后的用户信息结合服务端定义的秘钥用md5生成签名，目的是为了保证数据不被篡改，因为秘钥在服务端；之后再将会员名和uuid组合起来作为key,设置指定的过期时间，将其存入到redis中，这样做是为了后期在拦截器中进行过期判断。最后将前面用户信息的base64编码的内容和签名信息的base64编码内容通过.作为分隔符连接起来，响应给 前台，前台就可以在登录的回调函数中将这个信息暂时存入cookie中，方便后期取出cookie中的数据放到ajax的请求头中。

最后最重要的就是zuul网关过滤器中的处理逻辑。首先要处理一下options请求。之所以会发送options请求，是因为我们前台客户端在发送ajax请求的时候传递了自定义的头信息，这就会导致发送真实的请求前先发送一个options请求，但这个options的请求不会传递 任何实质的数据，所以在后台拦截器处理的时候我们可以通过request.getMethod来判断下请求方式是否是options,如果是就不放行，直接通过setSendZuulResponse为false，禁止路由转发然后return null进行拦截,处理完后前台就会自动发送真实的请求过来。

处理完这个options请求后又考虑到在项目中有些请求是不需要登录就能访问的，有些请求是登录后才能访问的，为了对处理这类请求，我在zuul的配置文件中写了一个自定义属性，

这个自定义参数里面放的就是登录之后才能访问的资源，通过@Value取出这个自定义属性

，然后在过滤器中，使用这个request.getRequestURI()获取当前请求的路径，遍历这个自定义属性 判断当前的请求是否需要登录之后才能访问，如果需要继续往后判断，不需要直接放行。

接下来我会判断前端传过来的请求中是否包含自定的头信息，如果没有则通过之前在zuul网关中说的方法，使用这个response.body返回提示信息给前台，在通过setSendZuulResponse设置为false，禁止路由转发。

告诉前端头信息不完整。

如果有头信息就到了最关键的验签过程，目的 就是防止内容被篡改，具体的逻辑是这样处理的，首先将传过来的头信息根据.进行切割，切割后就取到了经过base64编码的用户信息和经过base64编码的签名，之后用经过base64编码的用户信息和服务端的秘钥经过md5得到签名，再对base64编码的签名进行解码，然后两个签名进行对比如果一致，则证明数据没被篡改，否则同样给前台一个提示信息然后禁止路由。

验签后就要判断存储在redis中的key是否过期，这个比较简单，就是将base64编码的用户信息进行解码得到 json格式的字符串，并通过阿里巴巴提供的fastjson这个第三方jar包，将json格式的字符串转换为对应的 会员对象，这样就能从中获取到会员的相关信息包含会员名，会员id，以及uuid这个标识，紧接着根据 会员名和uuid组合key，调用redis工具类判断该key是否还存在，如果不存在则抛出异常提示数据过期了。

如果存在就会给对应的key进行续命，其实也特别简单就是调用redis工具类中的expire方法就行了。这个续命说白了有点类似于session的过期时间处理，比如session的过期时间是30分钟，如果到最后一分钟了 又有客户端请求发送过来则会重置为30分钟。

经过这些层层判断后就可以将会员信息通过addZuulRequestHeader方法传递给后端微服务中使用

，这样做是为了方便在其他微服务控制层的方法中通过这个request.getHeader方法来获取会员的相关数据，最后return null放行即可。

之所以我们做这个前台项目的时候 使用这个token的登录方式是因为

之前基于session的登录方式，是在用户登录成功后将用户信息存入到session中，这样不利于程序的横向扩展，并且随着登录用户的增加，会不断的占用服务端的内存资源；而现在这种基于token的登录方式，是在登录成功后将用户信息存入到客户端的中，不会额外占用服务端的内存资源，并且通过签名和验签可以保证数据不被篡改。

以上就是我当时做的一个类似于jwt的登录

**接下来我给您介绍下我做的这个购物车模块吧**

考虑到用户操作购物车的性能问题，我当时做的是基于redis的购物车，将购物车的所有数据都存储到redis中。

当时用了redis中的hash结构来存储所有用户购物车的数据，咱们都知道在使用hash的时候，涉及到key,field,value这三个方面的参数信息，key这块我用了CartMap这个静态的常量来表示，在field这块因为每个用户都有一个购物车，为了保证唯一性，我用了member:会员id来表示，在value这块我是把会员对应的整个购物车的信息都转换为Json格式进行了存储。整个购物车对应的数据结构是这个样子的。

购物车中包含 商品总件数，总价格，以及 购物车的商品项列表，在商品项中包含 商品id,商品名，商品单价，商品件数，商品图片，商品小计 等，这里面特别要注意的就是关于价格这块在java中要用bigDecimal这个数据类型，这样可以防止精度丢失。

我们当时的购物车是会员登录后才能操作的，比如添加商品，删除商品等。关于登录这块，就是我刚才说的这个基于token的用户登录

用起来更加的灵活方便，我们在zuul过滤器中的通过经过层层验证之后通过addZuulRequestHeader方法 把用户信息数据传递给后端微服务中使用 ，而后端微服务中就可以通过request.getHeader来获取值，后来为了方便在控制层的方法中获取这个用户信息我使用了spring提供的这个自定义参数解析器，这样就不用在每个方法上都通过这个request.getHeader来获取会员信息，省去了一定的代码重复

具体我是这样做的，自定义了一个实现HandlerMethodArgumentResolver接口的参数解析器 类，这里面最主要有两个方法，supportsParameter和resolveArgument，在supportsParameter中我通过methodParameter获取参数的类型和我自定义的会员类进行对比如果相等则返回true,证明找到了会员类型的参数，当返回true时就会走resolveArgument方法，在该方法中，通过request.getAttribute()获取拦截器中存入的会员信息，并将其强转为指定的会员类，进行返回。最后要想使自定义的参数解析器生效，还需要在配置类中通过配置让他生效

这个配置类的话具体是这样做的

创建一个类 在类上面添加一个注解@Configuration 实现一个WebMvcConfigurer接口

重写里面的方法，然后通过@Autowired 注入这个自定义参数解析器

最后在addArgumentResolvers方法中通过add方法添加让他生效

那么具体在做添加商品到购物车的业务逻辑是这样的。这个接口方法接受3个参数，其中商品id和商品个数是直接从前台传过来的，而会员类则是通过自定义的参数解析器来完成赋值的。首先我会根据商品id判断该商品是否存在，如果不存在则提示商品不存在的信息，如果存在则需要判断该商品的状态是否正常，比如是否是上架状态，如果状态是下架则提示该商品已经下架。

经过这些验证后，我会判断该会员在redis中是否有对应的购物车信息，是通过封装的工具类redisUtil中的hget来获取的，如果该会员对应的购物车信息为空，则首先要创建购物车，并且将当前商品添加到购物车中，最后还要计算购物车中的总件数和总价格，通过阿里巴巴的fastjson将其转换为json格式，并通过我封装的redisUtil的工具类hset方法，将其存入到redis中的hash结构里。

如果会员对应的购物车信息不为空，则分情况进行处理。首先看看该商品是否已经在购物车中了，如果是，则找到该商品并更改商品的数量为商品原有的数量加上前台传过来的商品的数量，还要重新计算该商品的小计，以及重新计算整个购物车中商品的件数以及总价格，最后更新redis中的数据。

如果该商品不存在购物车中，则将该商品加入会员的购物车，并重新计算整个购物车中商品的件数以及总价格，最后更新redis中的数据。

这就是整个往购物车中添加商品的逻辑，至于减少商品的个数，完全可以使用和添加商品一样的方法，只不过传过来的商品的个数为负数就行了。

而且还有一些小细节，就是如果不断的减少商品个数，当商品个数减少到零的时候，就将该商品一并从购物车中删除掉。当购物车中所有的商品都被删除的时候，也同时删除整个购物车。最后都得更新redis。

购物车这个模块我是这样做的。

**至于订单这个模块就比较复杂了**

需要我们考虑的事情也比较多。

像 表设计，重复下单问题， 商品的超卖问题，包括订单也都是用户登录后才能

进行的操作等等。我之前也说过我是通过自定义注解来区分公共资源和私有资源的

那么我就先来说下这个重复下单的问题吧，这个重复下单说白了就是要考虑接口的幂等性

至于这个幂等性我是这样理解的

就是对接口调用一次和调用多次，产生的结果都是一样的。像查询方法，就天生具有幂等性的特点。

而我们的订单属于添加操作，对于添加操作本身是不具备幂等性的特点，所以需要我们特别处理下，如果不处理就会出现因为网络抖动或者服务器重发请求，造成虽然用户只操作了一次，但是可能最终发送了多次添加订单的请求，这样就会让用户感觉到很奇怪，明明我就下了一个订单，怎么会出现两个一模一样的订单呢。

对于接口的幂等性我是基于redis+token的方式解决的。具体的思路是这样的。

首先我会写一个创建token的接口，这个接口的代码也特别简单，就是生成一个uuid作为token，然后响应给客户端，并且将该token存储到redis中，而且设置它的过期时间为10分钟，这样在客户端中就可以调用这个接口生成一个唯一的token标识,并且在后续的请求中将该token作为header中的信息传入到接口的服务端进行相关验证。

接着我就在zuul网关的配置文件中写了一个自定义参数，这个自定义参数里面放的就是我需要拦截的这个请求，通过@Value取出这个自定义属性的值然后使用这个request.getRequestURI()获取当前请求的路径 判断当前的请求是否需要解决这个幂等性问题，如果包含继续判断，不包含直接放行。

幂等性过滤器中的判断是最核心的。首先我会判断请求中是否包含token头信息，如果没有就响应给客户端一个提示，头信息丢失。如果存在则获取该token的内容，调用redis中的exist方法来判断在redis中是否存在该token，如果不存在则提示token不存在。最后就是调用redis的delete方法，将该token作为key进行删除操作，如果返回的值等于0,则证明已经有其他请求发送过来了，该请求就不在是第一个发送过来的请求，就提示请求重复，否则证明是第一个请求，放行即可。

然后就是这个超卖的问题 既然要说这个超卖的问题那么我肯定要先说下我这个下订单的业务逻辑了

首先我们从redis中取出用户的购物车数据，如果为空，则响应给客户端一个用户购物车为空的提示信息，如果不为空则取出用户对应的购物车的json数据，将其转换为java对象。

首先通过年月日时分的时间戳加上雪花算法生成一个订单的唯一标识，然后从购物车对应的java对象中取出购物车中的商品列表，这个商品列表其实对应的就是订单明细，循环遍历商品列表，减库存，如果减库存成功，则将该商品插入订单明细表，如果不成功就不需要插入订单明细表了，而且还需要从购物车中剔除该商品，更新购物车的总价格和总件数，并将该库存不足的商品加入一个列表，用于响应给前端进行提示。

将更新后的购物车信息中的总价格和商品总件数插入到订单表中，并设置创建时间为当前时间，当前订单状态为 未支付。

最后插入支付日志表，这个表记录的是支付时候的相关信息在插入的时候，

将支付日志表中的订单id设置为刚才插入的订单id,将支付状态设置为 未支付，并将该支付日志插入到redis缓存中，方便后续在支付的时候直接从缓存中取出来进行使用。紧接着就清空该用户对应的redis中的购物车数据。因为当时购物车数据是以hash的方式存储的，所以通过hdel进行删除就行了。

在这个过程中要注意，

如果整个购物车中的商品都库存不足，则直接提示前端，下单失败，库存不足；也就不需要再插入订单表和支付日志表了。这样可以解决一个单线程的情况下超卖的问题

具体操作的时候使用的是基于数据库乐观锁的方式进行订单超卖的处理。核心思路就是在update语句中加入库存量是否大于或等于购买量的where条件。比如原来更新数据库中的商品库存我这样写，先查询下该商品对应的库存量，然后和需要购买的商品数量来进行对比如果库存量大于等于购买量则执行update 商品表 set 库存=库存-购买量 where 商品id=购物中的商品id;否则提示库存不足。

表面看上去没有任何问题，但在遇到多线程高并发的时候，就会出现多个线程同时查询商品对应的库存量，都符合条件，所以多个线程都会依次进行update语句，最后就造成商品可能为负数，出现商品超卖的情况。

我是通过将update语句改造为 update 商品表 set 库存=库存-购买量 where 商品id=购物中的商品id and 库存量>=购买量，然后根据update的返回值，如果返回值为0，则证明没有执行该sql语句，证明库存已经不足了。这样即便在多线程的时候也不会出现超卖问题。

至于这个订单的表设计的话

订单这个模块中包括 订单表和订单明细表，像订单表我当时设计

的有这些字段：

订单id 他的生成方式就是我刚才说的通过年月日时分加上雪花算法生成的

这样既能从一个订单id中看到这个订单是啥时候生成的也能通过雪花算法保证整个订单编号的唯 一性。

用户id 就是当前登录的会员id，是为了指明这个订单是哪个会员的订单。

订单支付方式 我们当时系统中有多种支付方式，比如1 微信支付 2 支付宝支付

订单的总金额 总件数 这个没啥要特别说的，这个就是当时购物车中添加的商品总价格及其 总件数

订单的创建时间 这个字段比较重要，因为在用户下单后可能不及时支付订单 我们当时在系统中 设定的是15分钟后自动关闭订单，所以就可以用当前时间减去订单创建时间如果大于15分钟就 关闭订单 当然 这时候就需要用到订单状态字段 设置订单状态为 交易关闭 当然 他还有很多的 状态，有

未支付 已支付 已发货 交易成功 已完成评价

当然还有一个订单的状态描述

比如咱们的关闭订单 有手动关闭订单、自动关闭订单

还有用户支付后，如果要退款也会进入到交易关闭状态。

所以需要记录一个具体的描述

除此之外还有订单的支付时间，交易关闭的时间，交易成功的时间，发货时间，完成评价的时间。

当用户收到货物后点击确认收货，会进入到交易成功状态，如果用户没有点击确认收货，那么是在发货时间15天后自动将订单变为交易成功状态，只有交易成功后才能对商品发表评论。

当然还有一些收件人的信息 包括手机号，地址，邮编，名字等等，这样做是通过这些个冗余字段，避 免为了获取这些信息还要进行多表联查，因为多表联查会降低性能而通过冗余字段就可以避免多表联 查，无形中也就提升了性能。

那么这就是我做这个订单模块的一个业务逻辑

最后就是这个支付模块了

在进行支付的时候，我们是这样处理的，整体上来说调用微信的统一下单接口，根据返回的code\_url,生成二维码，扫描该二维码，进行支付后，通过调用查询订单状态的接口，来判断订单是否支付成功，如果成功则跳转到支付成功页面。

默认情况下code\_url的有效时间是2个小时，也就是说如果2个小时内没有进行扫码支付，过期后扫码将不能再次发起支付。我们可以通过传递接口文档中指定的参数，将这个有效时间设置为了30分钟。

在调用统一下单接口的时候需要传递一些必要的参数信息，比如

应用ID，微信平台提供的

商户号，微信平台提供的

商户订单号，我们是通过时间戳加上雪花算法生成唯一的订单标识

总金额，单位是分，这点要特别注意，我们数据库中存储的单位是元，所以得进行转换

生成签名时候的秘钥，为了避免攻击者生成假的签名，因为key这个秘钥在服务端存储

是一个随机数，为了保证签名的不可预测，通过nonce\_str来保证签名只能用一次，防止重放攻击

notify\_url：回调的url地址

trade\_type： 交易类型，我用的是Native，也就是生成二维码进行扫码支付的方式

body：商品描述

sign：签名，是为了防止数据被篡改。

生成签名的规则就是将要传递的数据按照字典排序，使用URL键值对的格式（即key1=value1&key2=value2…） 拼接成字符串，将该字符串拼接上秘钥key,并对拼接后的数据进行md5，得到的值转换为大写，这样就生成了签名。

调用统一下单接口后，获取return\_code和result\_code，只有两者都正常才证明调用接口成功，这样就可以从响应中获取code\_url信息，生成二维码。

为了将生成的二维码的有效期设置为30分钟，我通过time\_expire参数，设置这个参数的值为当前时间加上30分钟，最后还要将它转换为接口文档中指定的年月日时分秒的字符串格式。

查询订单状态这块我是这样做的，同样需要传递应用ID，商户号，随机字符串，签名，最主要的还有一个商户订单号， 这样就可以查询指定的订单信息，如果返回的result\_code和result\_code都为SUCCESS，则证明调用接口成功，这时候 就可以从响应中获取trade\_state这个交易状态，如果状态为SUCCESS则代表支付成功，在这个时候我就可以更新支付日志的状态，更新订单状态，并且删除redis缓存中存储的支付日志信息。

在这个过程中还有个特殊的处理，当生成二维码，展示到前台页面后，用户可能不会马上进行扫码支付，这个时候如果发送了查询订单状态的请求，肯定会出现订单的状态是未支付，所以在后台代码中我是这样处理的，每隔5秒钟发送一次请求，总共发送60次，如果在这个过程中订单状态为支付成功则跳转到支付成功页面，如果这整个过程都没有进行支付，则提示二维码过期，需要用户重新刷新页面生成新的二维码进行支付！！！

**这就是我当时在前台项目中负责的一些功能**

**我在之前还负责过后台管理项目中的日志管理模块以及项目的负载均衡，我们当时部署项目使用的是nginx加多个tomcat进行的负载均衡**

**这个技术，这是为了提高我们项目的一个高可用性，当然 负载均衡还可以承受更多并发量，不过在我们后端项目这块主要起到的就是一个备份的作用，保证服务的不间断。**

**咱们都知道nginx有不同的负载均衡策略，默认是轮询策略，说白了就是将请求均匀的分发到不同的tomcat上，比如我们有两台tomcat，分别是t1和t2,当4个请求到来的时候，第一个请求被nginx发送到t1上，第二个请求被nginx发送到t2上，第三个请求又被发送到t1上，第四个请求又被发送到t2上，这就是nginx默认的轮询策略，当其中一台tomcat宕机时，会被自动剔除掉。**

**第二种使用的是一个加权轮询的策略，我们都知道在企业中不同tomcat所在机器的配置和性能都不一样，这个时候如果用默认的轮询策略就显的比较浪费资源，我们可以通过weight这个关键字配置加权轮询，比如将性能高的那台tomcat的权重设置为4，将普通配置的那台tomcat设置为1，这样就能达到让性能高的那台tomcat处理更多的请求。**

**除此之外还有一个IP\_Hash的负载均衡策略，这个策略说白了就是根据访问的客户端的ip地址，对其进行hash化，然后如果该客户端第一次请求被发送到t1上了，那么它就会和t1进行绑定，以后的每次请求也会被发送到t1上，只有t1宕机了，请求才会被发送到其他tomcat上。**

**当时在项目部署完之后，遇到这么个问题，用户登录输入验证码的时候，明明验证码输入的正确，但总是提醒说验证码不正确从而不能正常登录，经过分析后发现有可能第一次请求被发送到t1上，那么放在session中的验证码就被放到了t1上，当用户输入验证码点击登录时，新发送的请求有可能被发送到t2上面，而t2的session中不存在该验证码，这样在进行对比时就肯定会不一致从而提示验证码输入错误。**

**为了解决这个问题我们使用了ip\_hash这种负载均衡策略来代替默认的轮询策略。但这里面还有一个问题，如果被客户端绑定的这台tomcat宕机了，那么请求就会被发送到其他tomcat上，这个时候在用户进行操作时，请求会被拦截器拦截，拦截器中的代码会验证session中是否有当前登录的用户信息，如果没有则跳转到登录页面，因为这台tomcat上的session中不存在用户登录的信息所以就会跳转到登录页面，这就会导致用户的体验度非常不好，感觉也会很怪异。**

**为了最终解决这个问题，我通过上网查资料，就决定通过采用基于redis的分布式session来解决session共享的问题。**

**要想完成分布式session的编码工作，就必须需要搞清楚单机版的session是如何工作的，这样我们就可以模拟它工作的流程和机制，并且把相关的信息存储到redis这个缓存服务器中。**

**单机版session的工作原理是这样的，当访问页面时如果遇到getSession()这个方法，那么就会在服务端的内存中开辟一块空间用来存储以后要放到session中的数据，并且会生成一个唯一的 sessionId 作为和这块空间关联的依据，写入到客户端浏览器的会话Cookie中。说的通俗一点可以这样理解，就相当于我们去超市购物的时候一个个的存储柜，其中sessionId就是这个存储柜上的钥匙，而存储在session中的数据就是存储到这一个个存储柜中的物品。一把钥匙只能开一个柜子们，这样就保证了不同人拿着他们唯一的那把钥匙去开各自的柜子们，取到属于自己的物品。**

**当知道了这些以后，我们就清楚，这里面最主要涉及到会话cookie的操作以及将数据存储到redis中并且还得让会话cookie和redis中的key产生关联，这样每次发送请求时，会将本地存储cookie的域名和当前访问的域名进行对比，如果匹配则会将cookie自动提交到服务器端，这样就可以根据cookie中存储那个自定义的sessionId在redis中找到对应的数据，**

**首先我封装了一个cookie的工具类，然后在里面写了常见的 写cookie,读cookie,删cookie的常见操作。这里面要注意的是，cookie被分为会话cookie和持久化cookie，他们的区别就是会话cookie的生命周期和浏览器保持一致，一旦浏览器关闭了，就会消失；而持久化cookie是存储在硬盘上，他的生命周期取决于在编程的时候设置的maxAge的值；在具体编码的时候会话cookie不需要设置maxAge属性，而持久化cookie要根据项目的要求设置maxAge；再者在设置cookie时候还需要设置 域名以及Path,通常将域名设置为当前域名，将path设置为 / ；代表网站的根目录。写cookie通过的是response的addCookie方法，而读cookie用的是request的getCookies方法，返回一个cookie数组，然后根据cookie的name进行对比找到需要的cookie信息，删除cookie比较简单，说白了就是将指定name的cookie的maxAge设置为0,然后重新通过response的addCookie方法写入到客户端浏览器中，这样就完成了对指定cookie的删除工作。**

**在项目中我是通过jedis来作为中间的桥梁操作redis服务器的，并且考虑到性能问题配置了jedis连接池，这样就可以在大并发访问时候提高性能；并且把对redis的常规操作也都封装成了工具类，方便后续的使用。**

**我将项目中单机版session的地方都改为了通过redis的进行信息的存储。首先在生成验证码的地方，我首先通过CookieUtil读取指定name的cookie，如果没有读取到则通过uuid生成一个唯一的标识作为cookie的值，用指定的LoginId作为cookie的name将其通过CookieUtil的writeCookie方法写入到客户端浏览器中，这样就保证了最开始没有LoginId的时候会生成新的,如果LoginId存在则无论怎么刷新会使用现存的LoginId而不会刷新一次就创建一个新的。并且会将Cookie的值作为redis中的key,将生成的随机数验证码作为值，调用redisUtil工具类存储到redis中，并设置过期时间为5分钟，因为验证码没必要一直存在占用内存空间。**

**在登录方法中首先通过CookieUtil的readCookie方法根据LoginId作为key，读取指定的cookie，获取cookie中的值，将该值作为redis中key,读取对应的验证码信息，和用户输入的验证码进行对比，如果一致则验证码正确进行后面的验证，否则验证码输入错误。在各项验证都成功后将获取的用户信息通过Gson转换为json格式的字符串作为值，用“user:”+LoginId作为key，将用户信息存入到redis中，并设置过期时间为30分钟，同时删除redis中的验证码，释放空间。**

**最后就是在拦截器中通过CookieUtil的readCookie方法读取到会话cookie中存储的LoginId的值，用“user:”+LoginId作为redis中的key读取用户信息,如果为null则证明用户没有成功登录跳转到登录页面，否则证明用户成功登录，调用redisUtil中的expire方法给redis中的用户信息续命，重新设置为30分钟，这也是参考本地session的工作机制。这样就完成将整个项目中的本地session切换为基于自定义cookie+redis的分布式session。**

**就解决了在进行负载均衡配置后，如果一台tomcat宕机，用户也无需重新登录的问题。**

**那么这就是我当时部署项目的使用遇到的问题**

**至于我当时做的这个日志管理模块的话，**

**在之前的做其他的项目的时候**

我是使用AOP做的统一日志的处理，这样就可以让我们程序员在工作的时候把精力花在核心业务代码的处理上。

具体在做的时候我是这样写的。首先写一个日志切面类，这个切面类说白了就是一个普通的java类，后面会通过配置文件的配置让他具备切面类的功能。在这个普通的java类中我会自定义一个横切逻辑，说白了就是一个普通的方法，但这个方法中需要特别注意几点，因为当时在项目中我使用的是环绕通知，所以就会让这个方法返回一个Object类型值，再者就是在方法中有一个ProceedingJoinPoint类型的参数。

具体在写方法的时候是这样写的，首先要获取当前登录的用户，用户的信息是存储在Redis中的， 我当时采用的使用了自己写的一个工具类，从redis缓存服务器中拿出登录后的用户信息

获取了用户信息之后就要记录用户做了什么事情，在这块我们当时的项目是这么规定格式的，就是要记录用户执行了哪个类的哪个方法，并且要把执行这个方法时候对应的参数信息也给获取到，比如用户添加了一个商品，那 记录的信息就应该是调用了ProductController类的addProduct方法，并且也要获取到添加的商品信息参数，这样才能看的更明白。

获取类名和方法名这块是通过反射机制，调用ProceedingJoinPoint的相关方法获取的，获取参数信息是通过 request.getParameterMap()之后对其进行循环遍历，这样就获取到了提交时候的参数详情.

在这整个切面类中还有一个特别重要的方法就是ProceedingJoinPoint.proceed();它代表的就是实际要执行的 核心业务逻辑，它的返回值就是实际执行方法的返回值，比如刚才说的ProductController类中的addProduct方法， 这个proceed()代表的就是addProduct方法，而他的返回值就是控制层中addProduct方法的返回值。之所以 它的返回值类型为Object就是因为不同方法的返回值不一样，但它们都属于Object对象。

接着我会把proceed方法进行try...catch...捕获，然后在这个方法执行完后记录操作成功的日志并且把日志信息插入数据库，在catch捕获异常的时候记录错误日志，同时会把异常信息记录数据库。

最后需要在spring的配置文件中配置aop:config以及配置切点表达式来对控制层中的增，删，改方法进行拦截，这里就用到了切点表达式中特殊符号的双竖杠||。

在上交完任务后，我们经理给我说这个东西，做的整体上还不错，但是有个问题，就是日志虽然记录了操作哪个 类的哪个方法，程序员可以读懂，但业务员根本就看不明白，不够人性化，让我的日志记录再改进下。

我通过和我们团队的人讨论，最终决定通过自定义注解来完成这个改进。

在写自定义日志注解时候，通过 @Target 设置为Method指明该注解只能用在方法上面，通过将 @Retention设置为RunTime指明将注解保留至运行时。这样就可以通过反射去获取注解信息。

在注解中声明了一个String类型的value来让程序员手工设置日志的信息，之所以采用value，是因为value这个字段有特殊的含义，它可以在使用自定义注解给日志信息赋值的时候省略不写，用起来更加方便。之后就可以在Controller中的方法上加入自定义注解并且对value进行日志信息的赋值，如 @Log("增加商品")。

最后在AOP的日志切面类中通过获取方法签名得到Method，通过Method的isAnnotationPresent判断该方法上面是否加入了自定义日志注解，如果 是 则再通过Method的getAnnotation来获取自定义的日志注解，最后再通过.value()方法获取自定义注解中日志信息的值，这样在记录日志的时候就可以显示更加人性化的信息。

这是我当时在后台项目负责的模块

’

当然我还负责过一些小的功能比如这个导出excel，我当时在做这个导出excel的时候呢使用的是这个反射来完成的

java反射机制 说白了 就是在运行过程中，对于类来说，咱们可以获取它的属性和方法，对于对象来说，可以动态调用它的任意方法和属性。

动态获取信息 以及 动态调用对象的方法 就是反射机制！！！

我在项目中做导出excel功能的时候就是用的反射机制，这样就能达到导出excel的通用性，只用这么一个工具类，就可以导出不同的业务数据，比如商品，会员，品牌，分类，而且用起来也特别方便。

想要用反射首先得获取类，获取类的方式我知道的有这几种，可以通过对象的getClass()方法获取类，可以通过Class.forName("类的全称")来获取类，可以通过 类名.class 获取类。

·

之后可以通过 getDeclared【的科泪尔德】Fields()获取类的所有属性，getDeclaredField(属性名)获取类中指定 名字的 属性,getDeclaredMethods()获取类的所有方法，获取属性后还可以通过getType()获取属性的类型，通过getName()获取属性名。

动态调用方法这块如果是get方法可以使用 属性.get(对象) 来调用get方法，如果是set方法可以通过 属性.set(对象，值)来调用，但因为get,set方法一般都是私有的，所以得先通过 属性.setAccessible(true) 来开启访问权限。如果是普通的方法可以通过 方法.invoke(对象，参数) 来调用。

以上就是我之前在项目中做过的功能和用到的技术。

**最后我来说一下我们当时对项目的一些优化方案吧**

**我们当时使用的是这个索引来优化提高我们sql的查询速度，它就相当于是书的目录，我们通过目录可以快速锁定想要查看的内容，如果没有这个索引的话**

**我们想要查询一个东西的时候就需要一页一页的找**

但是这个索引也不是越多越好，因为它会占用额外的空间，并且在进行增删改的时候还需要额 外维护索引。

索引的类型得从两方面来说

一方面是特性，它分为

唯一索引和普通索引

但是从这个字段的个数来说他又分为

单一索引和复合索引【字段的个数，如果对多个字段同时加索引则称之为复合索引】

这个唯一索引所在字段中的值必须是唯一的。

我们的主键会自动创建唯一索引

这个创建索引的语法的话 他是这样的

-- 普通索引

create index index\_status on t\_log(status);

-- 创建唯一索引

create unique index index\_username on t\_user(userName);

https://www.cnblogs.com/summer0space/p/7247778.html

-- 创建复合索引

create index index\_status\_logincount on t\_user(status, loginCount);

索引里面又有这个聚集索引和非聚集索引：

聚集索引：主键就属于聚集索引。在一张表上聚集索引只能有一个。

非聚集索引: 除了主键以外的唯一索引，普通索引。在一张表上非聚集索引可以有多 个。

至于这个创建索引的原则的话我们一般：

给频繁查询的字段上创建索引

根据当前字段的业务含义，来区分是创建唯一索引还是创建普通索引

考虑到索引不是越多越好，也可以根据业务情况创建复合索引，

想要使其复合索引起作用，在查询的时候需要按照当时创建

复合索引的字段的顺序来,也就是最左匹配原则。

但是创建完这个索引，不一定就能使用上索引；

要是想要索引生效必须满足

两个条件，第一，该字段上有索引；第二，所写的sql语句必须支持索引。

那么什么时候索引不起作用?

1.如果在有索引的字段上进行运算，那么索引失效，会进行全表扫描。

2.在使用like的时候如果%在前面则索引失效

全文检索技术

java:[开源的搜索引擎技术]

Lucene：

Solr【是对lucene的封装】：企业级的搜索引擎技术

ES【是对lucene的封装】：互联网级的搜索引擎技术

3.避免在查询条件中使用is null,可以采用默认值的方法来解决

当然还有一些sql的优化方案

1. 比如说我们的SELECT语句中会避免使用'\*’，只查询需要返回的字段，这样可以

减 少 解析sql语句的时间，以及减少 带宽，cpu,内存，io等 各方面的消耗。

2. 然后我们对于这个大数据量的分页就不在使用常规的 limit 开始位置，每页条数查询了；这样越靠后查询时间越长，效率越低，当时是使用的id>=的方法来替代，比如

select 字段名 From 表名

where id >= (select id from 表名 limit 开始位置，1)

Limit 每页条数

这样只需要和数据库交互两次，不需要多次交互数据库 大大的提高了查询的效率

3. 外键必须加索引，这样可以提升多表联查的性能

4. 通过冗余字段避免多表连查，从而提高性能。比如在商品表中可以不仅有分类的id， 还可以加上分类的名字，这样就不用为了显示分类名字而去进行多表联查了。又 比如在会员表中不仅有地区的id，还可以有地区的名字这样也可以避免为了显示地 区名而进行多表联查。

5. 在 where，order by 以及GROPU BY 涉及的列上建立索引，为了避免全表扫描。

6. In和exists的区别：

主要是就是驱动顺序的改变，这是性能变化的关键，

* 1. 如果是exists，那么以外层表为驱动表，先被访问，如果是IN，那么先执行子查询，以内层表为驱动表。
  2. 所以IN适合于外表大而内表小的情况；EXISTS适合于外表小而内表大的情况。

7. 通常要用小表去驱动大表，这样可以提高性能，在left join 中 左边的表为驱动表，所以应该让左边的表尽可能的为小表，在right join 中 右边的表为驱动表，所以应该让右边的表尽可能的小，在 inner join 中 mysql会自动选择较小的表为驱动表。

那么这就是我当时对于sql优化方面的心得

**执行计划:**

如果我们想要查看当前sql使用了那些索引可以

通过explain查看sql语句的执行计划，通过执行计划可以查看

在这个执行计划里面

key:代表mysql实际使用 的索引。

type:这个字段比较重要，它表示MySQL在表中找到所需行的方式：

Const：主键在where条件中

Range：扫描部分索引，常见于between、<、>等的查询

Index：代表扫描全部 索引树

ALL：代表扫描全 表/全表扫描/不走索引。

**在提高程序性能方面我们使用的了线程池**

首先线程池可以避免频繁的创建和销毁线程所造成的性能损耗，原理就和数据库连接池差不多，说白了就是项目启动的时候在线程池中就已经创建好了指定数量的线程，需要的时候直接去用，用完后再放回线程池供其他程序进行使用。

再者用线程池中的多线程可以处理大批量的数据，比如我要将数据库中的图片加水印或者在硬盘上批量生成文件，这时候都可以用线程池。

就像要洗100个碗，你可以让一个人去干，这一个人就像是一个线程，你也可以让10个人一块去干，这就是线程池中的多线程。相比而言多线程执行的时间更短，效率更高。

在项目中我们是用ThreadPoolExecutor来创建线程池的，它里面有几个核心

的参数信息，线程池的核心大小，队列以及线程池的最大值。线程池的工作原理是这样的，默认情况下，创建线程池之后，线程池中是没有线程的，需要提交任务之后才会创建线程。如果当前线程池中的线程数目小于核心线程数，则每来一个任务，就会创建一个线程去执行这个任务；如果当前线程池中的线程数目>=核心线程数，则每来一个任务，会尝试将其添加到队列中，若添加成功，则该任务会等待空闲线程将其取出去执行；当队列已满，添加失败，就会尝试创建新的线程去执行这个任务；这时候创建新的线程是根据线程池时的最大线程数为依据的，如果当前线程池中的线程数目达到最大线程数，则会采取任务拒绝策略进行处理；说的简单点就是先把核心线程数给占满了，不够用就开始往队列里面放，如果队列也占满了，就往创建的最大线程池里面放，如果也占满了就可以根据策略进行拒绝处理。

如果线程池中的线程数量大于 corePoolSize【核心线程】时，某线程的空闲时间超过keepAliveTime【存活时间】，线程将被终止，直至线程池中的线程数目不大于corePoolSize【核心线程】。

打个比方我的核心线程为5，队列是20，最大线程数是10 对应着 快递公司的五个正式员工，

20个快递柜，如果这时候来了五个快递，正式员工就去派送了，然后又来了20个快递就放到了快递柜等待派送，后来又来了第26个快递，我的快递柜和员工都被占用了，只能选择聘请一些临时员工，但是又因为经济有限，所以最多聘请5个，在后续多的快递我就不送了，

那么为什么叫临时员工呢，意思是说 过了一段时间后 我们的快递基本都配送完了，临时员工已经有很久没工作了，我就会选择把辞退，不然还需要给他发工资，很浪费资源。

被动说：

一般需要根据我们会根据任务的类型来配置线程池大小，如果是CPU密集型任务，就需要尽量压榨CPU，可以设为 CPU个数\*CPU核数+1，如果是IO密集型任务，参考值可以设置为2\*CPU个数\*CPU核数。

**基础概念:**

HashMap和ConcurrentHashMap底层原理

**HashMap的底层原理**

HashMap底层就是一个数组结构，数组中的每一项又是一个链表。

当新建一个HashMap的时候，就会初始化一个数组。

Entry就是数组中的元素，每个 Entry 其实就是一个key-value对，

它持有一个指向下一个元素的引用，这就构成了链表。

HashMap 在底层将 key-value 当成一个整体进行处理，这个整体就是一个 Entry 对象。 HashMap 底层采用一个 Entry[] 数组来保存所有的 key-value 对，

当需要存储一个 Entry 对象时，会根据hash算法来决定其在数组中的存储位置，

再根据equals方法决定其在该数组位置上的链表中的存储位置；当需要取出一个Entry时，

也会根据hash算法找到其在数组中的存储位置，

再根据equals方法从该位置上的链表中取出该Entry。

默认是构建一个初始容量为 16，负载因子为 0.75 的 HashMap。

也就是说，默认情况下，数组大小为16，那么当HashMap中元素个数超过16\*0.75=12的时候，就 把数组的大小扩展为 2\*16=32，即扩大一倍，然后重新计算每个元素在数组中的位置，而这是一 个非常消耗性能的操作，所以如果我们已经预知HashMap中元素的个数，

那么预设元素的个数能够有效的提高HashMap的性能。

Jdk1.8中引入了红黑树，目的是避免单条链表过长而影响查询效率。

**ConcurrentHashMap原理**

在java并发包里面，ConcurrentHashMap是线程安全的hashMap，通过

引入分段锁的概念将一个大的Map拆分成多个小的HashTable.在存值

和取值得时候通过key.hashCode()来计算key及其对应的值应该放到

哪个HashTable中。默认情况下ConcurrentHashMap会创建16个分段数组集合。

这样在进行操作的时候如果有3个线程A B C，这时候A B两个线程根据key.hashCode()

可能被分配到同一个hashtable中，这样A在进行操作的时候B就会阻塞。但C这个

线程可能被分配到了另外一个hashtable中，这样C就可以直接执行而不会阻塞。

**所以效率就得到了极大的提升。默认情况下可以提高16倍。**

## Hashtable与HashMap的区别

**1.Map是一个以键值对存储的接口。Map下有两个具体的实现，分别是HashMap 和HashTable.**

**2.HashMap是线程非安全的，HashTable是线程安全的，所以HashMap的效率 高于HashTable.**

**3.HashMap允许键或值为空，而HashTable不允许键或值为空**

**4.HashTable之所以是线程安全的是因为在它的方法上加上了synchronized 锁。**

**5.LinkedHashMap是有序的**

## Set,List,Collection(可来可神),Collections的区别？

**List和Set都是接口，他们都继承于接口Collection,List是一个有序的可 重复的集合，而Set的无序的不可重复的集合。 Collection是集合的顶 层接口，Collections是一个封装了众多关于集合操作的静态方法的工具类, 因为构造方法是私有的，所以不能实例化。**

**List接口实现类有ArrayList,LinkedList,Vector。ArrayList和Vector(v 可特)是基于数组实现的,所以查询的时候速度快，而在进行增加和删除的时 候速度较慢LinkedList是基于链式存储结构，所以在进行查询的时候速度较 慢但在进行增加和删除的时候速度较快。又因为Vector是线程安全的，所以 他和ArrayList相比而言，查询效率要低。**

## String,StringBuffer,StringBuilder的区别

**String是一个常量，是不可变的，所以对于每一次+=赋值都会创建一个新的对象，StringBuffer和StringBuilder都是可变的，当进行字符串拼接时采用append方法，在原来的基础上进行追加，所以性能比String要高，又因为StringBuffer是线程安全的而StringBuilder是线程非安全的，所以StringBuilder的效率高于StringBuffer.对于大数据量的字符串的拼接，采用StringBuffer,StringBuilder.**

**单例：**

饿汉式

public class Sing {  
  
 private volatile static Sing *sing* = new Sing();  
  
 private Sing (){}  
  
 public static Sing getSing(){  
 return *sing*;  
 }  
}

懒汉式

public class Sing2 {  
  
 private volatile static Sing2 *sing2* = null;  
  
 private Sing2 (){}  
  
 public static Sing2 getSing2(){  
 if(*sing2*==null){  
 *sing2* = new Sing2();  
 }  
 return *sing2*;  
 }  
}

双重判断锁

public class Sing3 {  
  
 private volatile static Sing3 *sing3* = null;  
  
 private Sing3 (){}  
  
 public static Sing3 getSing3(){  
 if(*sing3*==null){  
 synchronized (Sing3.class){  
 if(*sing3*==null){  
 *sing3* = new Sing3();  
 }  
 }  
 }  
 return *sing3*;  
 }  
}

**大批量数据的插入/更新?**

1.一条条插入

1. 分段 批量 提交【推荐】【减少和数据库的交互次数】
2. 批量插入和数据库交互一次

### Jvm虚拟机调优

我们的linux服务器,安装centos6.5, 64位的操作系统和64位的软件，

配置了4个cpu,64G内存。

我们在jvm优化的时候是这样做的

首先JVM将内存划分为：

年轻代

年老代

永久代（方法区）

其中年轻代和年老代属于堆内存，永久代不属于堆内存，有虚拟机直接分配。

年轻代：年轻代用来存放JVM刚分配的Java对象

年老代：年轻代中经过垃圾回收没有回收掉的对象将被放到年老代

永久代：永久代存放Class类、Method方法元信息，其大小跟项目的规模、类、方法的量有关，一般设置为128M就足够，预留30%的空间。通过

-XX:PermSize=128M -XX:MaxPermSize=128M 来设置永久代（方法区）的大小。

jvm的垃圾回收算法有[GC]

串行算法（单线程）

并行算法

并发算法

**吞吐量优先的并行收集器**

**响应时间优先的并发收集器**

我们的项目设置的是响应时间优先的并发收集器，

将堆大小通过 -Xms -Xmx设置为3G,将年轻代通过 -Xmn 设置为2g,

设置年老代为并发收集，当时设置的是运行7次GC以后对 内存空间进行压缩、 整理。打开对年老代的压缩，可以消除碎片。

### **tomcat调优**

1.启用线程池，默认的tomcat没有启用线程池，

在tomcat中每一个用户请求都是一个线程，所以可以使用线程池提高性能。

我们在项目中将maxThreads[最大线程数]设置为1000，将排队数acceptCount和maxThreads设置相等。

当tomcat的线程数达到maxThreads后，新的请求就会排队等待，超过排队数的请求会被拒绝。

2.使用64位的tomcat和jdk，禁用AJP协议。

3.开启APR通讯模式，支持高并发。因为默认tomcat采用的是性能最低的BIO【阻塞IO】模式。

4.tomcat中设置JVM参数 通过-server开启server模式 通过-Xms4000m和-Xmx4000m设置初始堆大小和最大堆大小，

通常将两个值设置为一样，避免堆空间不断增大和缩小所带来的性能损耗。

被动说：

jvm的内存结构：

方法区【持久代】

堆【java对象】

栈【基本数据类型，对象引用（指针/对象名）】

本地方法栈

计数器

**springmvc的运行原理**  
 整个处理过程从一个HTTP请求开始：  
 1.Tomcat在启动时加载解析web.xml,找到spring mvc的前端总控制器 DispatcherServlet,并且通过DispatcherServlet来加载相关的配置文件信息。  
 2.DispatcherServlet接收到客户端请求，找到对应HandlerMapping，根据映射规则，找 到对应的处理器（Handler）。  
 3.调用相应处理器中的处理方法，处理该请求后，会返回一个ModelAndView。  
 4.DispatcherServlet根据得到的ModelAndView中的视图对象，找到一个合适的 ViewResolver（视图解析器），根据视图解析器的配置，DispatcherServlet将要显示的 数据传给对应的视图，最后显示给用户。

**spring中的ioc我是这样理解的**

·就是说原来咱们想要创建一个类的对象，得自己通过new的方式进行，  
·而现在可以通过在spring的配置文件中写上一段<bean id="" class=""/>的配置，  
·从而让创建对象实例的过程交给spring容器来完成，而我们在程序中可以直接获取  
·创建好的对象实例进行使用。这就是IOC的控制反转。

AOP的切面在项目中用的还是比较多的，咱们都知道spring中的事务管理就是通过AOP 切面的方式来实现的。切面的好处就是把分散在代码中的重复代码提取出来进行统一的维 护和控制。我们在项目中就使用aop完成日志的统一处理。原来是把日志记录的相关代码 分散到各个控制层的相关方法中，但这就会导致程序员在开发时候不能将精力集中到业务 逻辑的处理上，还得考虑记录日志，工作效率就大打折扣，我在项目中通过....[将aop 中日志的统一处理融进去]

jdk1.8新特性:  
 在项目中/在工作中 我用lambda表达式还有stream

**数据库持久层相关知识点**

1.视图：

视图里面并没有存放真正的数据，存放的是sql语句，真正的数据还是存放在表里。可以通过 create view 视图名 as select语句 的方式来创建视图，这样可以将比较复杂的查询语句作为一个视图，后续再需要执行这个复杂的sql，就不用重新再写一遍了，而是直接 select \* from 视图名 就行了。

2.存储过程：

这个东西我们项目中基本不用，之前有了解过，说白了，存储过程里封装了sql语句，也支持传参和返回值，有点类似于java中的方法，这样你就可以直接在java端调用存储过程执行复杂的逻辑，而不需要发送多条 sql语句，一定程度上降低了和数据库的交互次数，提高了性能，但存储过程的可移植性比较差， mysql和oracle支持的语法结构和关键字也都不一样。

1. mysql的存储引擎有哪些，它们的区别是什么：

有MyISAM和InnoDB两种存储引擎。

它们的区别是：

MyISAM用的是表锁，InnoDB用的是行锁。

MyISAM不支持事务处理,不支持外键而InnoDB支持。

# mybatis 俩种取参数方式的区别：

.mybatis中的#和$的区别

1. #将传入的数据根据类型进行相应的转换，如果类型不匹配则报错。如果传入的是字符串类型则会自动加上双引号。

2. $将传入的数据直接显示在sql中。

3. #方式能够很大程度上防止sql注入，$方式无法防止Sql注入，所以一般能用#的就别用$。

**spring cloud的版本:**spring cloud的版本:  
1.5  
你咋没用2.0呢，1.5都淘汰了?  
我们当时项目用的就是1.5的  
你知道gateway吗?【网关】  
springCloud 2.0里面的gateway就是1.5里面的zuul  
你知道consul?【注册中心】  
springCloud 2.0里面的consul就是1.5里面的eureka  
你们的springCloud的配置中心用的是啥？  
1.SpringCloud Config  
2.用的是携程的 Apollo 配置中心。  
具体咋用的？  
  
这个当时是其他人配置的，我在项目中看到过，  
自己具体还没配过，不过，应该也不难啥，  
要是咱们公司需要，我也可以搭建。  
你们的链路追踪用的是啥？  
我知道的有Spring Cloud Sleuth和Zipkin，但项目中我们还没用到。

冒泡排序：

for (int i = 0; i < arr.length; i++) {  
 for (int j = 0; j < arr.length-1-i; j++) {  
 if(arr[j]>arr[j+1]){  
 int temp = arr[j];  
 arr[j] = arr[j+1];  
 arr[j+1] = temp;  
 }  
 }  
}

**session和cookie的区别**

session是存储在服务器端，cookie是存储在客户端的，所以安全来讲session的安全性要比cookie高，然后我们获取session里的信息是通过存放在会话cookie里的sessionid获取的。又由于session是存放在服务器的内存中，所以session里的东西不断增加会造成服务器的负担，所以会把很重要的信息存储在session中，而把一些次要东西存储在客户端的cookie里，然后cookie确切的说分为两大类分为会话cookie和持久化cookie，会话cookie确切的说是存放在客户端浏览器的内存中，所以说他的生命周期和浏览器是一致的，浏览器关了会话cookie也就消失了，然而持久化cookie是存放在客户端硬盘中，而持久化cookie的生命周期就是我们在设置cookie时候设置的那个保存时间，然后我们考虑一问题当浏览器关闭时session会不会丢失，从上面叙述分析session的信息是通过sessionid获取的，而sessionid是存放在会话cookie当中的，当浏览器关闭的时候会话cookie消失所以我们的sessionid也就消失了，但是session的信息还存在服务器端，这时我们只是查不到所谓的session但它并不是不存在。那么，session在什么情况下丢失，就是在服务器关闭的时候，或者是sessio过期，再或者调用了invalidate()的或者是我们想要session中的某一条数据消失调用session.removeAttribute()方法，然后session在什么时候被创建呢，确切的说是通过调用getsession()来创建，这就是session与cookie的区别

**linux的常用命令**

1 ifconfig；

查看ip地址

2 mkdir

创建文件夹

3 rpm -ivh

安装软件

4 rpm -qa | grep 软件名

查看是否安装

5 rpm -e 软件名

卸载软件

6 echo $PATH :查看环境变量

7 pwd

查看完整路径

8 vi/vim

编辑

ESC 命令模式

/ 输入关键字 查找

n 下一个

shift + n 上一个

9

source /etc/profile

让配置文件立即生效

10

ps -ef | grep 查看服务是否启动

11

在bin目录下通过 tail -f ../logs/catalina.out 查看启动日志

. 代表目录

根据当前目录判断是否需要加 .

tar -zxvf 解压文件

tar -zcvf 压缩文件

mv 原文件名 新文件名 ; 重命名

删除文件的时候 文件夹名称 / \* 是删除这个文件夹下的所有东西

不加 是删除这个文件夹

make 编译

mysql数据库 默认情况下 不允许远程连接【只要是通过ip地址访问 就不行 只能通

localhost访问】

如果想要远程连接 需要 授权

命令： all是权限 root是用户名

grand all on \*.\* to ‘root’@‘%’ identified by ‘密码’（123456）

flush privileges; 立即生效

默认 linux系统的防火墙是开启的 需要放过 tomcat 服务器的端口

vi /etc/sysconfig/ip

关闭tomcat

kill -9 进程号：强制杀死进程

ps - ef grep java

查看查看进程号

linux安装软件的方式

1. rpm

2. 解压缩/绿色版

3. 在线安装 yum 需要联网 推荐

在linux中安装一些软件的时候，有时候需要先配置很多相关的环境，下载一些相关的插

件，但是使用yum的话，这些事情都不用我来负责了，yum会自动安装这些软件所需要

的软件，而且这些软件版本号都是匹配的，不会出现版本冲突的或者版本过高、过低的

问题

wget 在线下载

locate 全局搜索

nginx 启动命令

/usr/local/webserver/nginx/sbin/nginx

/usr/local/webserver/nginx/sbin/nginx -s reload # 重新载入配置文件 /usr/local/webserver/nginx/sbin/nginx -s reopen # 重启 Nginx /usr/local/webserver/nginx/sbin/nginx -s stop # 停止 Nginx

nginx -t 验证配置文件是否正确

main 调用 网易云短信 发短信

tailf /opt/tomcat/logs/catalina.out

unzip apache-tomcat-7.0.67.zip 解压 zip文件

查看日志

**jenkins:**

它是做持续化集成用的，说白了以前 部署项目的流程是 获取源代码，编译打成war包，上传到linux服务器中的tomcat下，再重新启动tomcat。

整个过程都需要人为的一步步操作，特别麻烦，特别是当项目多了以后，部署起来更是麻烦。现在使用jenkins后，整个打包，编译，部署，启动 的过程就完全自动化，只需要登录jenkins的后台管理，配置git,目的是为了从指定的git服务器上下载源代码；配置maven,目的是为了对源代码进行编译，打包；配置tomcat，目的为了指明项目部署的位置，还要编写一个简单的shell脚本，目的是为了杀死对应的tomcat进程，再重新启动。这样就配置了一个完全自动化的

任务，后续 再部署项目 只需要运行该任务，就可以自动完成项目部署的工作。

Docker[容器化部署]:

基于Docker的容器化部署，整体来说就是让配置整套环境更加方便， 可以达到一键部署的效果。

说白了不用Docker我们也能搭建环境，部署项目，但是比较费劲，步骤比较繁琐，而且如果要把项目迁移到另外一台机器上，还将相关的软件重头到尾安装一遍，而且有时候机器的操作系统版本不一样，即便按照同样的配置步骤也有可能出现软件的不兼容，而且在改配置文件的时候可能会因为手误导致配置出错，多个逗号，少个分号啥的，这些都比较耗费时间，也降低了工作效率。

**锁：**

在这个多线程的情况下如果有多个线程操作同一个资源会引发一个线程安全的问题说白了就是执行的最终结果和预期的结果不一致，遇到这个多线程并发访问的线程安全问题，通常可以采用锁的方式进行解决。

最经常用的就是synchronized同步锁，我在写单例设计模式的时候就会用到。

通过这个双重判定锁可以在保证线程安全的情况下，提高程序的性能，通过这个同步代码块

可以减小这个锁定的范围，调高性能，而锁内部的判断是为了保证这个多线程的情况下的单例

比如A,B两个线程过来后同时进入方法，都满足最外层的判断，这时候两个线程抢占锁资源，然后A获取了锁，则B只能在外面等待，A在最里层的if判断中，因为最开始对象为null,所以会给对象赋值。当A线程离开了同步代码块后，会自动释放锁；这时候B线程获得锁资源，同样进行最里层判断，因为对象已经不为null,则可以直接返回该对象不需要再次创建，这就保证了单例。如果后续又有新的线程过来，则在最外层的判断中已经不为null,就可以直接返回对象，无需再次锁定。这样也就提高了性能！！!

但是这种双重判定锁本身也有一个缺陷就是可能会出现一个重排序的问题，就是说实例化一个对象其实是分为三步 1 开辟一个空间 2 初始化对象 3 将引用指向这个对象，但是由于指令重排的问题，可能他的顺序就不再是这三步了 可能会先执行 1 3 步 那么这个时候 这个对象已经不为空了就跳过了if判断 那么在后续调用这个不完整的对象的时候就会报错，为了解决这个问题，我们使用了volatile这个关键字来避免这个重排序的问题

像java里面的hashtable和vector都是用的synchronized来保证线程安全。

除此之外，还有读写锁。读写锁表示有两个锁，一个是读操作相关的锁，也称为共享锁；另一个是写操作相关的锁，也叫排它锁。

多个读锁之间不互斥，读锁与写锁互斥，写锁与写锁互斥。

通过分离读锁和写锁，使得并发性相比一般的排它锁有了很大的提升。也就是说多个Thread可以同时进行读取操作，但是同一时刻只允许一个Thread进行写入操作。通过lock()方法加锁，通过unlock()方法解锁。

除此之外还有分布式锁，普通的锁[synchronized]是为了解决多线程访问产生的安全问题，分布式锁是为了解决多进程【多个tomcat】多线程访问产生的安全问题。我们在项目中使用Redisson来完成分布式锁。

除此之外从数据库层面来说有悲观锁，乐观锁。包括有表锁和行锁。

悲观锁,

每次去查询数据的时候都认为别人会修改，

所以每次在查询数据的时候都会上锁，

这样别人想拿这个数据就会阻塞直到它拿到锁。

传统的关系型数据库里边就用到了这种锁机制，

比如通过select ....for update进行数据锁定。

乐观锁,

每次去查询数据的时候都认为别人不会修改，

所以不会上锁，但是在更新的时候会判断一下在此期间别人有没有

去更新这个数据，可以使用版本号，时间戳等机制。

乐观锁适用于多读的应用类型，这样可以提高吞吐量。

**缓存【redis】穿透：**

缓存穿透是指查询一个一定不存在的数据，比如商品最多只有1000个，我查询1001,1002这些一定不存在的id,这个时候因为查询的信息在缓存中不存在，大量的并发请求就会直接到数据库上，而数据库中也不存在这样的数据，所以缓存就形同虚设，这个id一定不存在的请求以后都会到数据库上，增加数据库的压力。

为了解决这个问题，可以缓存空值,也就是说即便在数据库中 查询的数据不存在，也会在缓存中缓存个空值，这样下一次就可以走缓存而不是数据库了，但太多的空值也会占用内存空间，导致内存的浪费，可以通过设置过期时间比如3-5分钟，这样当到期后，空值对应的key就会消失；释放空间；但导致的另外一个问题就是如果在这3-5分钟内后台增加数据，这个时候就有id为1001的数据了，而缓存中还是空，所以就会导致数据库和缓存中数据的不一致，为了解决这个问题可以在后台增加数据的同时主动更新缓存中的数据。

**缓存【redis】雪崩：**

如果缓存在一段时间内同时失效，发生大量的缓存穿透，所有的查询都落在数据库上，造成了缓存雪崩。

解决这个问题可以

1.为不同的key，设置不同的过期时间，让缓存失效的时间点尽量均匀

2.做双缓存策略。

A1为原始缓存，A2为拷贝缓存，A1失效时，可以访问A2，

A1缓存失效时间设置为短期，A2设置为长期。

**redis持久化：**

有AOF和RDB两种方式,我们一般使用默认的RDB方式。因为它的效率会更高，

RDB持久化是在指定的时间间隔内将内存中的 数据 写入到硬盘的rdb文件中，实际操作过程是fork[分]一个子进程，先将数据集写入临时文件，写入成功后，再替换之前的文件，用 二进制 压缩存储。

具体是在redis.conf中配置的，找到save关键字， 指定每隔多长时间有多少个key发生变化，就将其持久化。

AOF：是将每个 写操作对应的指令 保存到后缀名为aof的 文本 文件中。

rdb的性能要高于aof：

因为rdb中直接存储的是数据，所以在redis服务器启动的时候，直接加载rdb文件中的数据到内存中就行了。

而aof中存储的是写指令，所以在redis服务器启动的时候，需要先加载aof

文件中的指令，之后还需要再次执行这些指令。

aof的 实时性、可靠性 要高于rdb：

因为每个写操作指令都会及时写入aof文件中，所以aof这种持久策略不容易丢失数据，而rdb是在指定的时间间隔后才会写入数据到文件中，所以有可能会丢失一部分数据。

**我们当时使用的是restful风格的接口**

**这个restful风格的接口**是ROA面向资源编程的一种设计风格，restful不是一项新技术,就是新瓶装旧酒,其实就是符合restful风格的url,都被称之为restful类型的接口,,像这个restful在使用的时候就要注意，路径中不能出现动词，最好是名词并且要以复数的形式出现，restful是基于http协议现有的Get动作进行查询，Post动作进行增加，Put动作进行修改，Delete动作进行删除，当然这是标准的restful接口的定义，具体在使用的时候可以灵活变通

分布式事务：

分布式事务:跨了多个数据库事务管理,在微 服 wu 架构每个服 wu 都有自己数据库,在微服 wu 架构中必然要用到分布式事务.  
分布式事务这块，在项目中我没有具体做过，但我之前看过这方面文章，要么可以通过LCN实现，要么可以通过 最终消息一致性 实现。

这个lcn框架

主要是为微服务框架提供分布式事务的支持，在微服务框架上做了进一步的事务机制优化，在一些负载场景上LCN事务机制要比本地事务机制的性能更好，4.0以后框架开方了插件机制可以让更多的第三方框架支持进来。  
特点：  
   ①支持各种基于spring的db框架  
   ②兼容SpringCloud、Dubbo、motan  
   ③使用简单，低依赖，代码完全开源  
   ④基于切面的强一致性事务框架  
   ⑤高可用，模块可以依赖RPC模块做集群化，TxManager也可以做集群化  
   ⑥支持本地事务和分布式事务共存  
   ⑦支持事务补偿机制，增加事务补偿决策提醒  
   ⑧添加插件拓展机制  
如果问到说项目中是否用过，就说暂且还没用到或者说自己没有负责这块。  
【咱们现在的事务只能解决单个数据库的问题，如果出现了跨数据库的操作，则需要分布式事务才能解决】  
  
分库分表：  
当一张表数据越来越大，这时候就需要分表。  
按地区分  
按时间分  
地区+时间  
   当分表已经不能解决问题的时候，就需要分库了。  
业务功能分

关于这方面的技术的话我知道有这个**MyCat**

**这个Mycat可以简单概括为may**  
-  一个彻底开源的，面向企业应用开发的大数据库集群  
-  支持事务、ACID、可以替代MySQL的加强版数据库  
-  一个可以视为MySQL集群的企业级数据库，用来替代昂贵的Oracle集群  
-  一个融合内存缓存技术、NoSQL技术、HDFS大数据的新型SQL Server  
-  结合传统数据库和新型分布式数据仓库的新一代企业级数据库产品  
-  一个新颖的数据库中间件产品

没用过  
  
SSO单点登录:  
我之前看到过用CAS[开源的框架]可以做单点登录，就是有A,B两个项目，在其中任意一个项目上登录后，再访问另外一个项目就可以直接访问而不需要再次登录，这里面可以用CAS做为中央认证服务器， A项目和B项目的登录全部都跳转到CAS这个中央认证服务器上面统一进行。

在项目中自己没有负责这块  
  
工作流都用过哪些:  
我知道有Jbpm,Activiti工作流引擎。

项目中暂且还没用到

Redis Cluster:  
为了避免redis服务器产生单点故障，也为了提高redis服务器的存储数据的容量；我们将redis配置为集群模式，为了提高集群的高可用性，我们使用了3台redis作为master【主】;  
并且为每台master都配置了对应的slave【从】；这样就可以达到数据扩容同时提高集群的可用性。  
  
整个集群是由不同的node【节点】组成的，而每个node【节点】上面被分配了slot也就是槽，数据是被放到了对应的slot【槽】中。  
  
redis集群中共有16384个槽，集群会把这16384个槽平均分配到不同的节点上；当向集群中存数据的时候，会根据key采用CRC16算法，算出来一个值，让这个值和16384求余数，这样就把数据分片的存储到不同的槽中，也就落到了不同的节点上，实现了数据的分片，同时也起到了扩容的目的。  
  
如果没有配置对应的slave服务器，则一台master宕机就会导致整个集群不可用，这就大大削弱了集群的功能，所以我们可以为每台master配置一个slave，这样当master宕机时，对应的slave就会充当master，使集群继续提供服务。如果宕掉的那台master又被重启了，则该master会变为slave。  
  
在我们构建的redis集群中，有3个主，3个从，当存活的 主 节点的数量小于总节点的一半时，集群不可用。即当存活的主节点数量为2时，集群不可用。