# B简历：

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

基本信息 **面试常见问题：**

|  |  |  |  |
| --- | --- | --- | --- |
| 基本情况 | | | |
| **姓名** | 刘帅萌 | 性别 | 男 |
| **出生日期** | 1993-06-15 | 属相 | 鸡 |
| **现住地** | 通州区 通州北苑 杨庄北街4号院 |  |  |
| 大学情况 | | | |
| **学校** | 郑州工业应用技术学院 | 专业 | 计算机应用技术 |
| **入学时间** | 2011-09 | 毕业时间 | 2015-07 |
| **专业课** | **计算机硬件实训、C语言、数据库原理、操作系统、Java程序设计** | | |
| **学历** | **本科** | 学位 | **学士学位** |
| **学校地址** | 河南省新郑市 | 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：** | 坐地铁城郊线 华南城站下（5元左右） 打小黑车（15元） | | |

|  |  |
| --- | --- |
| 第一家公司 ： | 北京网拓时代科技有限公司 |
| **地址：** | 北京海淀区西三旗上奥世纪B座2107 |
| **入职时间：** | **2015年9月** |
| **离职时间：** | **2018年12月** |
| **公司性质：** | **民营** |
| **职位：** | **Java工程师** |
| **项目经理名字：** | **甘洋** |
| **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：** | 新龙城东站上车公交（636路/681路） 西三旗桥西站下车 |
|  |  |

|  |  |
| --- | --- |
| **第二家公司情况：** | 北京数字云邦科技有限公司 |
| **公司地址**： | 北京市朝阳区远洋国际中心A座7层 |
| **公司规模：** | **80人左右，我们项目组8人，一个项目经理，1名前端，1个测试，1个运维，其他都是Java工程师** |
| **公司性质：** | **民营** |
| **公司行业：** | 技术开发、技术咨询、技术转让、技术服务；软件开发；计算机系统集成；企业管理咨询；企业策划；设计、制作、代理、发布广告 |
| **去公司路线：** | 通州北苑上地铁（八通线） 四惠站下车（D出口出） 骑小车到远洋国际 |
| **入职时间：** | **2019-01** |
| **离职时间：** | **2019-11** |
| **职位：** | **Java工程师** |
| **项目经理名字：** | **于辉** |
| **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:** | **基本工资(6K)+绩效工资(9K)** |

|  |
| --- |
| 四年涨薪： **2014年工作的时候是5.5K，税后大概5.4K左右，**  **转正6K左右**  **2015上半年涨了1K左右 ，总7K左右。**  **2016年4月跳槽涨了3K左右 总10K**  **2016年12月涨1K总 11K左右**  **2017年9月工作一年涨了2K左右**  **2018年7月工作一年涨了2K左右**  **2018年9月离职时工资为15K** |

|  |  |
| --- | --- |
| **你 为什么从上家公司离职？** |  |
| **上上家公司的福利待遇也算不错，和同事相处的也蛮开心的，但是在技术提升方面不太符合自己发展的预期。就出来历练一下** |  |
| **你交社保了吗？为啥没交？** |  |
| **交了** |  |
| |  | | --- | | **三个词形容自己**： 交流表达能力强，团队协作能力强，责任心强 | | **你的优缺点是啥？** |   **优点:**  **善于倾听，团队协作能力强，责任心强。**  **缺点: 这几年做程序，因为要不断的对代码进行验证确认，所有感觉自己现在有点强迫症。** |  |
| **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？ |  |
| **近期的话我会先让自己的技术能力得到提高，当然，尽快的掌握公司的业务，投入到工作中，然后朝着项目经理发展** |  |
| 是统招吗 是是本科吗 是能在学信网查到吗 这个因为我当时上的是民办大学，所以在民教网查的到！ |  |
| 你们公司还有什么福利？多少薪： 13薪  **车补**  300左右  **项目奖金**  7k-10k，做完项目，收完尾款的时候。  **年终奖**  这个就是1个月的工资，  过年的时候和当月工资一块发  **电话补助**  300  **饭/餐补**  **15、**30/天  **电脑补**  300 |  |

**公司内其他部门：**

**技术部（开发部/研发部），行政部，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！**

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

坐稳再开口！！ 主动性！！ 开门见山！！大白话！！三秒钟原则！！学会反问！！

**Hr人事，leader领导，tean团队，pm项目/产品经理，cto首席技术执行官，coo首席运营官，CEO董事长、**

**介绍流程：**

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

## 主动说：

**你好！**今天来应聘咱们公司 java 开发工程师！

我最近做的一个项目是使用 **Spring Boot+springCloud 来做的微服务项目的开发**

首先先来说一下，这个springboot项目具体是怎么做的吧！

springBoot-->Eureka注册中心-->zull网关-->微服务雪崩问题{Hystrix}-->feigin微服务之间的调用

当时我们项目使用的是SpringBoot框架，首先在项目的pom文件中引入spring-boot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。

在项目中我们用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。

如果没有注册中心，客户端也是可以通过ip地址访问服务端的，只不过随着服务越来越多，调用也会越来越复杂，一旦ip地址发生了变动，则所有用到的地方都需要发生改变，维护起来会特别的麻烦；而且呀如果服务端宕机了，所有访问的客户端也都会受到影响。那么我们就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。而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。

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都会经过Zuul，进行安全验证，通过后再转发到具体的微服务上。

既然所有的请求都要先经过zuul，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，首先我先定义一个继承于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，按照基于jwt机制的token登陆方式进行接口的安全验证。

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设置为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。

在整个微服务搭建的过程中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。就像我们所看的一部电影，丧尸围城，刚开始只有一个，但是被他传染了一个，就会有两个，这两个越传染越多，最后就会导致整座城，乃至整个世界都会被传染。可以用SpringCloud中的Hystrix来解决这个问题。

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

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. 比如调用商品服务的controler放入A线程池, 调用会员服务的controler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。

我们在项目中是用Feigin进行微服务之间的调用的，首先，我先写了一个接口，在这个接口上加上@FeignClient注解，这个注解里加上name这个属性，对应的是我们的客户端在注册中心上的唯一标识。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,如果出现熔断这个问题，我们则需要进行降级的处理，首先要在接口上的@FeignClient这个注解里加上fallback这个属性，指向我们的降级类，这样在进行熔断的时候就会执行我们的降级类中的降级方法，这时候还需要定义一个降级类，这个类其实就实现了我这个接口，在这个类里边并不需要做什么具体的处理，不过可以进行日志的记录，也可以直接返回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。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。

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。

综上所述，这就是我在做这个微服务项目的时候的一些逻辑。

--------------------------------------\*\*----------------------------------------------\*\*--------------------------------------\*\*-------------------

二、上边我也说了是基于类似于jwt的token做的一些安全登陆的验证。在这里我就说下token登陆

这个基于Token的登录方式。说白了就是用户在前台输入用户名密码后通过ajax发送请求到后台接口，后台接口在进行层层验证后，如果验证成功则直接响应相关的信息给前台，前台在ajax的成功回调函数里面接受到数据，将其暂时存入cookie中，之后在后续发送请求时，再从cookie中取出数据将其写到自定义的header中，我当时自定义的header叫x-auth，之后数据就通过header传递给后台接口，在zull网关定义的过滤器中进行各种验证，通过验证后才能访问登录后的资源。

为什么使用这个token做登陆呢，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中的，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。

具体在做的时候我是这样做的：

我们也都知道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格式的字符串存入到我自己构建的一个memberVo里，这个memberVo其实就是存放我这些数据的，之后我会先把我的memberVo转换成json格式的字符串，在将字符串通过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，不会被客户端的所知道，这样就保证了签名的安全性；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过滤器中进行过期判断。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。在发送请求至后台接口时：

就需要解决一系列问题，首当其冲的就是ajax跨域问题。

1. 跨域处理：

我之前也说过，我是在zuul网关里，定义了两个过滤器，其中一个就用来解决我们的跨域问题，将解决跨域问题的过滤器的执行顺序设置为0，最先执行。并将类型设置为pre，让其在发送请求到微服务之情进行处理。

2.options特殊请求的处理

3.对于不需要拦截的请求直接放行

4.判断头信息是否完整

5.验签

6.判断是否过期

7.将会员信息存入我们的zull中，方便在其他控制层获取会员信息

接着就是我们的安全验证的过滤器：

关于options特殊请求是这个样子的。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zull网关的过滤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,就禁止路由转发，处理完后前台就会自动发送真实的请求过来。

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，为了处理这类请求，我就在我们的网关中使用自定义属性的方式解决这个问题，就是把需要我们登陆才能够访问的方法加到我们的属性文件中的自定义属性里，在我们的登陆安全验证过滤器中，通过@value这个注解获取到我们自定义属性的信息，通过Request.getRequestURI()获取到客户端发送请求的路径与我们需要登陆后才能访问的方法做个对比，如果包含在内就证明是需要登陆以后才能访问的信息

接下来我会判断前端传过来的请求中是否包含自定义的头信息，通过request.getHeader()获取头信息，如果没有，则响应给前端一个提示信息，告诉前端头信息丢失，这里响应我们是通过currentContext.setResponseBody()来设置的响应信息;

有头信息的话还需要验证头信息是否完整，这时候我会根据.来进行分割，因为当时返回的时候就是用.拼接成的一个字符串，所以分割的话就会得到一个长度为2的数组，这时候我会判断这个数组的长度是否为2 不为2证明头信息丢失，就响应给前台头信息丢失

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，否则响应给前端一个提示信息提示数据被篡改。

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，如果不存在则提示前端数据过期了。

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。

全部通过则将登陆的会员信息放入zull网关中，放入zull网关的时候需要通过URLEncoder.encode进行加码，防止因为有中文而出现乱码问题，同样在需要用到会员信息的地方，需要用过URLDecoder.decoder进行解码

在之前的项目中我也做过购物车的功能，具体我在做的时候是这个样子的：

当时从表设计到最后用postman进行接口的测试，都是我负责做的。

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 CartInfo 这个固定的字符串来表示，在field这块为了能够表示不同用户的购物车，我用来 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。

只有会员登录后才能操作购物车，比如添加商品，删除商品等。关于登录这块，我采用的是基于jwt机制的token的用户登录，类似于自己写了一个jwt【java web token】因为这个JWT有缺陷，所以我就模仿jwt的机制自己写了一个。

这样用起来更加的灵活方便，因为我们的所有请求都是通过zull网关来进行请求的，当通过了层层关卡的验证后，将会员信息存入到zull中，这样在其他的控制层方法中就可以通过获取头信息的方式来获取当前登录的用户信息。为了方便在每个控制层方法中获取会员信息，我采用了 spring中自定义的参数解析器，这样就避免了在每个控制层方法中都使用来request.getHeandr获取会员信息，而是在自定义的参数解析器中写一遍即可。

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，则需要在spring-mvc的配置文件中配置mvc:annotation-driven，并在其中配置mvc:argument-resolvers，通过bean class指定自定义的参数解析器类，这样就可以在控制层的各个方法中，直接写上会员类参数，就可以通过会员类获取其中的会员id等信息。

这里面涉及到 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。

对于上边所说的，都是一些业务逻辑，但是在项目中，我们考虑到性能方面的问题，做出了许多的优化：

比如说我们的sql优化：

1.在我们进行SELECT语句中避免使用'\*’，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。

1. 外键必须加索引，这样可以提升多表联查的性能

3.对于大数据量的分页不要用常规的 limit 开始位置，每页条数；这样越靠后查询时间越长，效率

越低，可以使用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

4.通过冗余字段避免多表连查，从而提高性能。比如在部门表表中可以不仅有员工的id，还可以加 上员工的名字，这样就不用为了显示员工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。

通过上述所说，我是通过索引来对这个查询做的sql上的优化，因为通过索引可以提高查询的速度，

它就相当于书的目录；

打个比方来说：就像我们正在看三国演义这本书，这本书的目录就相当于我们的索引，而这本书当中的内容就相当于我们数据库的数据，这时候我们如果想找到这本书的第600页，比如说是七擒孟获这个章节，我们就可以通过目录直接定位到这一页，这样就大大节省了时间，提高了效率，换到我们数据库来说，我们就可以根据索引直接找到这条数据所在，直接查询出来，这样就减少了与数据库的交汇，就大大的提高了我们的性能。

当然这个索引也并不是越多越好，因为索引会占用额外的空间，并且在进行增删改的时候还需要额外

维护索引。还拿刚才书的例子来说，我们如果突然把刚才的600页的标题给修改了，那么是不是就要

修改对应的目录。所以，换到数据库来说，这个时候如果我们进行修改的操作，不单单要修改这条数

据，还需要修改这条数据对应的索引。

那么既然这个索引不是越多越好，所以我们创建索引的时候就要遵守创建索引的原则：

1. 给频繁查询的字段上创建索引

2. 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

3. 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。

打个比方，我们都知道我们地区的三级联动，这个时候就可以使用我们的复合索引，这样就可以加快我们的查询速度，而且我们也不可能直接跳过省分去查市

从索引的特性上来说索引可以分为普通索引和唯一索引：

普通索引字段的值可以重复,而唯一索引字段的值则不能重复，必须保证唯一，而且我们的主键会自动生成唯一索引。

创建索引的具体语法是这样的：

唯一索引：create unique index 索引名 on 表名(字段名);

普通索引只是少了我们这个unique这个唯一的关键字，而创建复合索引则只是比创建普通索引多了字段名，也是说字段名可以设置多个

普通索引：create index 索引名 on 表名(字段名);

复合索引：：create unique index 索引名 on 表名(字段名1，字段名2);

但是我们这个索引也不是说我们只要创建就一定能使用上索引，想要使索引生效，还要满足两个条件，

第一，该字段上有索引；第二，所写的sql语句必须支持索引。

那么什么时候索引会失效?

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。

这个当时的解决方案就是不在我们的索引字段上进行运算

2.在使用like的时候如果%在前面则索引失效，当时是这样解决的

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where字句中对字段进行null值判断，这样会导致即便字段上有索引也会进行全表扫描，好的 处理方式就是给字段设置默认值。

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。

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，

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。

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。

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。以上为我所了解的sql优化，

接下来咱说说这个线程池吧，我们也都知道如果没有线程池，则就会频繁的去创建以及销毁线程，这就造成了我们的性能大量的损耗，所以我们在项目中也会通过线程池的方式提高程序的性能。首先我们也都知道了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】。

线程池中的队列，一般常用的有ArrayBlockingQueue【有界阻塞队列】：基于数组的队列，创建时必须指定大小；还有LinkedBlockingQueue【无界阻塞队列】：基于链表的先进先出队列，如果创建时没有指定此队列大小，则默认为Integer.MAX\_VALUE；

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-Xms3000m和-Xmx3000m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。

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

### 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8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256M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

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5G,将年轻代通过 -Xmn 设置为3g,

设置年老代为并发收集，当时设置的是运行8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。

被动说：

在linux服务器上部署项目的时候，通常会使用的一些命令

1. 通过netstat -anp | grep 端口号 可以查看端口对应的进程号，通过netstat -anp | grep 进程号 可以查看进程对应的端口号，之后可以结合ps -ef | grep 进程号， 来查看进程信息。

2.通过wget下载相关的文件

3.通过yum在线安装软件，比如我在linux上

安装mysql时

4.通过ps -ef | grep 进程名来查看进程，

比如我通过 ps -ef | grep java来查看

tomcat是否启动,通过 ps -ef | grep mysql

来查看mysql是否启动。

5.通过service 服务名 start来启动服务，如

通过service mysqld start来启动mysql

6.通过vi /etc/sysconfig/iptables来编辑文件

开启防火墙的端口号，最后通过service iptables restart

来重启防火墙使其配置生效

7.通过 kill -9 进程号来强制杀死进程

8.通过 cat /proc/cpuinfo查看cpu

9.通过 cat /proc/meminfo查看内存

10.通过 df -h 查看硬盘信息

1. 通过 top命令,可以查看正在运行的进程和系统负载信息

SpringBoot

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？  
用的是携程的  Apollo 配置中心。

因为我们现在都是微服务开发的，每个项目里都会有一个配置文件，而且这个配置里都会有一些重复的代码，为了方便管理我们这些配置文件，所以使用我们这个配置中心来统一管理

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。

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。

日志管理模块:【ioc的理解】

IOC我的理解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，我在项目中通过后台管理系统的日志管理模块实现了aop，日志管理模块的作用说白了就是记录用户的操作，这样就知道谁在什么时候干了什么事情。

之前做其他项目的时候，日志处理模块通常都是在控制层结合log4j进行日志的 控制台打印以及日志文件的存储，除此之外还会把日志信息插入到mysql数据库中存储起来，方便查看。

但这样做会有个问题，就是需要在每个Controller类的每个方法中都写上相关的日志记录代码，这样就会出现大量的代码重复，以后维护起来也特别麻烦。

所以说后面在做日志管理模块的时候，我就考虑到可以使用AOP做统一日志的处理，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有几个特别关键的地方，首先因为要获取当前登录的用户，用户的信息是存储在session中的， 我当时采用的解决方案是使用ThreadLocal+Filter来完成在一个普通的java类中获取当前请求的request对象，进而获取存储在session中的用户信息。ThreadLocal可以把它理解成一个Map，但它特殊的地方就是它用当前线程充当key，所以在使用的时候，存储信息用set(value)就行了，之所以没有写key，就是因为当前访问的线程就是默认的key,同理取数据用get();当时我封装了一个工具类，工具类中有个setRequest方法，就是将request对象存储到ThreadLocal中，同样还有个getRequest方法，就是获取当前线程对应的reqeust对象。

之后我会在自定义的Filter中的doFilter方法中，调用工具类的setRequest方法，将当前请求存储到ThreadLocal中，当然还得在web.xml中配置Filter使其生效。接下来我会在日志切面类中通过调用工具类的getRequest方法来获取request,进而通过getSession来获取session，这样就可以取到存在session中的相关用户信息了。

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。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。

**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，

。

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。**

锁：

**再者在多线程的程序中如果涉及到共享资源的访问，就会引发线程安全问题，说白了就是执行的结果和预期的结果不一致。遇到多线程并发访问的线程安全问题，我们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。**

**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。**

【**【通过双重判定锁可以保证在线程安全的情况下，极大的提升程序的性能。通过synchronized代码块，减小锁定的范围从而比将其加到方法上提高了性能，通过最外层的if判断可以使其后面的线程直接返回所需要的单例，而无需再次进行锁定。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，比如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C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！！!**

**但是这种双重判断锁方式自身会有一个缺陷，会出现指令重排序的问题。比如 Product p1 = new Product(),这个过程被分为3步。第一步在堆里面开辟空间，第二部初始化对象，第三步将p1指向初始化后的对象。但是由于指令重排的问题，可能它的执行顺序就不再是1,2,3而变为了1,3,2。在这个时候会出现p1指向堆空间中的对象还没有被完全创建。如果这个时候另一个线程过来了，那么最外层的if判断中，等于null的条件就不成立，那么就会直接返回一个还 不完全 的对象，程序在后续调用这个不完全对象的时候肯定会报错。**

**为了解决这个指令重排序的问题，我们可以通过volatile这个关键字，来避免指令重排！！！】 这段可以根据个人情况，进行省略！！**】

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。**

**save 900 1**

**#在900秒(15分钟)之后，如果至少有1个key发生变化，就会持久化。**

**save 300 10**

**#在300秒(5分钟)之后，如果至少有10个key发生变化，就会持久化。**

**save 60 10000**

**rdbcompression yes**

**rdbchecksum yes**

**dbfilename dump.rdb**

**save 900 1**

**save 300 10**

**save 60 10000**

**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。**

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。

通过docker就可以解决刚刚说的这些个问题。【至少记忆到这个地方】

==============================================

我觉的docker中最重要的就是镜像和容器这两个东西。镜像可以理解成

以前的光盘，这个光盘上包含了我们所有需要的软件及其相关环境；通过docker run 启动镜像后就有了容器。在执行docker run时候可以通过 -d 设置为以后台程序的方式运行，通过-p指定容器端口号到宿主 主机端口号的映射，在最后跟上要启动的镜像的名字。

之后可以通过docer ps 查看启动的容器对应的进程信息，通过docker stop 容器id 来停止容器，通过docker start 容器id来启动已经停止的容器。

在项目中还可以通过 docker-Compose 进行服务编排，说的简单点一个项目想要跑起来需要数据库，需要redis,需要nginx等等，我们可以通过这种服务编排将整个项目所需要的所有软件对应的镜像及其相关信息都写到一个YAML格式的文件中，这样在部署项目的时候直接通过docker-compose up启动服务，通过docker-compose ps查看启动的进程信息，通过docker-compose down来停止服务。就可以达到一键部署的效果。

Java反射：

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 getDeclaredFields()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。

负载均衡：

我们项目在最后上线部署的时候，采用的是nginx+3个tomcat进行负载均衡，在我们不进行负载均衡之前，所有的请求都由一台tomcat进行处理，这样会使我们的tomcat所承受的压力增大，而我们进行负载均衡之后，同样数量的请求经过nginx将其分发到多台tomcat进行处理，从而降低每台tomcat所承受的压力,而且当其中一台机器宕机时，其他机器还可以继续提供服务，保证服务不间断。

    项目在部署完成后，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。

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。

再者在企业中不同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nginx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。

所以我们就用ip\_hash这种负载均衡策略来代替默认的轮询策略，这样就解决了验证码错误问题。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进行信息的存储。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都会使用现存的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中的key,读取对应的验证码信息，和用户输入的验证码进行对比，如果验证码正确则进行后面的验证，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。

## 

## HashMap与Hashtable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是线程不安全的，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是一个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.**

**Restful接口开发：**

我在之前工作的过程中，我们的经理给我说，我们项目需要给前台提供restful接口,当时对这个restful只是了解并没有真正的在项目中使用过,所以下去我也查阅了许多关于restful接口开发的文档,通过文档得知,restful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,因为在互联网中可以通过url去访问任意的资源,比如：文章、图片、视频等,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。

经过了解之后，我就开始了基于SpringMVC进行restful接口项目的开发。开发时用到的注解有 @RestController @PathVariable @RequestBody @ReponseBody @Value @RestControllerAdvice这些，其中 @RestController就相当于 @Controller 和 @ResponseBody的组合体，这样就可以避免在各个方法上加入 @ResponseBody注解了，@ResponseBody的作用是将java对象转换为对应的json格式，默认使用的是Jackson这个第三方的工具包，这个注解的本质说白了就是通过Jackson将java对象转换为对应的json格式的字符串并且通过response获取输出流将json格式的字符串响应给客户端，想要使@ResponseBody起作用除了要在maven的pom文件中导入jackson的依赖外还需要在spring的配置文件中加入<mvc:annotation-driven/>，@PathVariable是为了从路径中获取参数信息比如在删除操作的时候就需要从路径中获取id信息， @RequestBody起到的作用和@ResponseBody看好相反，就是将前端提交过来的json格式的数据，自动转换为对应的java对象；@Value可以从属性文件中根据key获取对应的信息，比如我们可以把调用第三方接口时需要的信息以键值对的形式写到自定义的属性文件中，然后通过context:property-placeholder加载属性文件并且通过@Value根据key找到指定的值，这样可以避免程序中出现硬编码，提高程序代码的可维护性。对于@RestControllerAdvice来说它的作用就是异常的统一处理，就相当于@ResponseBody和@ControllerAdvice的结合体,我们项目中异常的统一处理就是用它来完成的。

我们采用JSON格式的数据作为restful的响应结果，其中用code表示状态码，用message表示提示信息，用data表示返回的数据。为了方便返回的指定格式的JSON数据，我们自己封装了一个ServerResponse对象，该实体对象中就包含code,message,data三项属性，这样我们在Controller层的各个方法中，统一返回的都是我们自定义的Response对象，并且我们也通过自定义的枚举对象ResponseEnum来方便进行code和message的统一赋值。

对于客户端前台调用restful接口，如果涉及到跨域则可以通过多种方案解决。首先我们可以通过ajax的jsonp来解决ajax跨域问题，如果采用这种方案则客户端在发送ajax请求时候需要将datatype设置为jsonp,在服务端需要接受callback参数，结合spring提供的MappingJacksonValue来将要响应的信息作为构造参数进行传递，并调用对应的setJsonpFunction设置为参数callback对应的值；但是这种方案只能发送get请求，如果服务端接口接受的是其他类型的请求如post,put,delete则jsonp就没办法。这个时候我们可以采用spring给我们提供的@CrossOrigin注解来解决，使用这个注解的时候要特别注意一点它需要和jdk1.8及其以上配套使用，否则会报错。通过@C

rossOrign的value属性指定客户端所在的域名这样客户端前台就可以使用普通的ajax进行跨域访问了而且可以发送任意类型的请求，这样就解决了上面所说的ajax jsonp只能发送get请求的问题。

写完接口之后我们通常会通过PostMan去测试接口的正确性，并且会自己编写接口文档，**在编写接口文档时通常需要写清楚接口的业务描述，接口的请求地址，请求方式，请求参数的类型，是否含有头信息，请求参数的含义以及接口的响应格式【json/xml】，响应内容，响应内容的各个字段含义**。

当时我是将商品信息，文章信息，分类信息，品牌信息,评论信息发布出去。

**Springboot运行原理**

SpringBoot运行原理:

我们从springboot项目的的启动类中可以看到最核心的两行代码， @SpringBootApplication和SpringApplication.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。

**支付：**

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

AppID：应用ID，微信平台提供的

MchID：商户号，微信平台提供的

outTradeNo：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

total\_fee：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

Key：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

nonce\_str：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retuen\_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！！！

订单这个模块我在之前的项目中也做过，这个模块相对比较复杂，考虑的事情也比较多。

像 表设计，订单接口幂等性问题， 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。

项目中很多接口是用户登录后才能进行操作的，所以我们采用的是基于token的用户登录，

并且自定义了一个注解，这样在需要登录的控制层的方法上直接加上这个自定义注解配合

自定义的拦截器，就可以达到先登录才能访问接口的目的，使用起来非常方便！！！

先说下订单表的设计吧，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

用户id

订单支付方式

订单的总金额

订单中商品的总件数

订单的创建时间

订单的支付时间

订单交易关闭的时间

订单发货时间

订单交易成功的时间

订单完成评价的时间

订单的状态 【未支付10 已支付20 已发货30 交易成功40 交易关闭50 已完成评价60】

订单状态描述

收件人手机号

收件人地址

邮编

收件人名字

邮费

是否需要发票

在这里面 订单id 作为主键，它的生成方法是年月日时分加上雪花算法生成的标识，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。

订单的支付方式，是考虑到我们的系统要支持好几种支付途径，比如1代表微信支付，2代表支付宝支付。

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，但如果添加到购物车的商品在提交订单进行购买时发现库存不足，我当时的做法就是找到库存不足的商品，弹出提示框告诉用户，并在订单的总金额和总件数中要减去这些库存不足的商品，当然这些库存不足的商品也就不再插入订单明细表了。

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，那我们的系统就是在1个小时后会自动取消订单。所以就可以用当前时间减去订单创建时间，如果大于1小时就将订单状态设置为交易关闭，并在订单状态描述中记录“订单支付超时取消订单”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。

订单的状态我当时设置的有

未支付 已支付 已发货 交易成功 交易关闭 已完成评价

取消订单的时候会进入交易关闭状态，可以是人工取消订单也可以是系统在1个小时后自动取消订单。

当用户支付后，如果要退款也会进入到交易关闭状态。

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。

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。

订单明细表:

订单id:

商品id:

用户id:

商品名:

商品价格:

商品个数：

商品小计:

商品图片:

我当时采用 订单id和商品id 作为联合主键，说白了也就是用多个字段来保证一条数据唯一性。

除此之外还融入了用户id这个字段，目的也是为了通过该冗余字段就能知道某个用户购买的商品明细，而不需要再连接订单表，避免多表联查。

表设计完之后就是正常的写接口，订单接口要考虑重复下单的问题，超卖的问题，以及把redis中存储的购物车数据取出来，插入订单明细表，订单表以及支付日志表。

关于重复下单这块，说白了就是要考虑接口的幂等性。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。

但下订单属于添加操作，对于添加操作本身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。

接着我写了一个自定义的注解，这个注解没有什么实质性的内容，说白了就是一个标识，只要是加上了这个注解的方法，都会在我自定义的拦截器中进行幂等性的处理。

幂等性拦截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。

之后我会在下订单的方法上加入自定义的幂等性注解，就解决了重复下单的问题。

接下来解决的是订单超卖的问题。

下订单的业务逻辑是这样处理的，首先从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，比如outTradeNo,payMoney等，

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。

我当时采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，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。

了解的高大上概念：

分布式锁：   
可以通过redission实现分布式锁，主要是为了解决 多进程 下的线程安全问题。接口的幂等性问题，就可以通过分布式锁的方式来解决，像重复下单或者重复充值。  
  
  
  
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。   
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】

自己网上了解的分布式事务【基于消息一致性了解的】：

****远程调用，结果最终可能为成功、失败、超时；而对于超时的情况，处理方最终的结果可能是成功，也可能是失败，调用方是无法知晓的****

### 事务消息

由于传统的处理方式无法解决消息生成者本地事务处理成功与消息发送成功两者的一致性问题，因此事务消息就诞生了，**它实现了消息生成者本地事务与消息发送的原子性，保证了消息生成者本地事务处理成功与消息发送成功的**最终一致性**问题。**

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  
  
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。

从结构上看，CAS 包含两个部分： CAS Server 和 CAS Client。CAS Server 需要独立部署，主要负责对用户的认证工作；CAS Client 负责处理对客户端受保护资源的访问请求，需要登录时，重定向到 CAS Server

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。  
  
**工作流都用过哪些:**我知道有Jbpm,Activiti工作流引擎。  
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。

**你在哪些地方用过redis???**

**用redis缓存电商分类**

**购物车是基于redis 如果购物车没有和面试官说，可以选择主动去说购物车**

**基于token的登录，用redis**

**基于redis的分布式session**

**防止重复下单中用redis**

**分布式项目中，主键是怎么处理的?【分布式id的解决方案】**

**雪花算法 可以生成分布式id**

**Redis支持哪些数据类型？【持久化缓存数据库 分布式缓存】**

String

Hash

List 有序可重复的

Set 无序不可重复的

Zset 有序不可重复的

### Nosql[Not Only SQL]是啥？

关系型数据库:oracle,mysql,sqlserver

支持事务

不能很好的应对高并发

多表联查

存储比较重要的数据，因为支持事务，不容易丢失

非关系型数据库[NOSQL]:redis, mongodb：

应对高并发

不支持事务

不支持多表联查

存储是大量的廉价的数据，允许出现丢失

事务概述

在项目中我们是通过spring的AOP来进行事务的统一管理的，通常是对service层的增删改这些写操作进行事务管理，对读操作设置为只读事务，提高性能；事务默认情况下只对运行时异常进行回滚，我们通过设置rollbackFor=Exception.class来对所有异常都进行回滚。判断事务是否配置成功的关键是当出现异常的时候，会不会回滚。

咱们都知道事务有原子性，一致性，隔离性，持久性 这四大特性，原子性是说把事务中的操作都当成一个不可分割的整体要么都成功，要么都失败；一致性是说事务得保证数据库中的数据从一个一致性状态变换到另一个一致性状态，数据不被损坏；隔离性是指一个事务的执行不能被其他事务干扰；持久性是指一个事务一旦被提交，它对数据库中数据的改变就是永久的。【至少说到这个地方】

**如果问到分布式事务可以这样说：**

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，要么可以借助消息中间件通过 最终消息一致性实现。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。

**下面的这些当问到传播特性和隔离级别的时候再说：**

Spring中事务的传播特性好像有5个左右，我做项目的时候使用最多的就是

PROPAGATION\_REQUIRED，它所代表的意思支持当前事务，如果当前没有事务，就新建一个事务。  
Spring中事务的隔离级别有5个，默认使用的是ISOLATION\_DEFAULT，（i色类申）  
它代表使用数据库默认的事务隔离级别，也是我们项目中最常使用的。

除此之外还有  
读未提交：  
它充许另外一个事务可以看到这个事务未提交的数据，这种隔离级别会产生脏读，不可重复读和幻像读。  
读提交：  
保证一个事务修改的数据提交后才能被另外一个事务读取，也是大多数数据库的默认值。可以避免脏读，但会产生不可重复读和幻像读。  
不可重复读：  
在一个事务内两次读到的数据是不一样的，因此称为是不可重复读。  
串行化：  
顺序执行事务。除了防止脏读，不可重复读外，还避免了幻像读。  
并发性也最低，但最安全。

不可重复读的重点是修改 :   
同样的条件 , 你读取过的数据 , 再次读取出来发现值不一样了 。

幻读的重点在于新增或者删除 ：  
同样的条件 , 第 1 次和第 2 次读出来的记录数不一样。

在并发状态下出现的问题是这个：不可重复读，脏读，幻读

## 如何客户端禁用cookie怎么办？

Cookie 默认存储数据是4K

LocalStorage的定义和使用：

localStorage 和 sessionStorage 属性允许在浏览器中存储 key/value 对的数据。

localStorage 用于长久保存整个网站的数据，保存的数据没有过期时间，直到手动去删除。

sessionStorage 用于临时保存同一窗口(或标签页)的数据，在关闭窗口或标签页之后将会删除这些数据。

localStorage 属性是只读的。

H5:

LocalStorage 替代 持久化cookie

保存数据语法：localStorage.setItem("key", "value");

读取数据语法：var lastname =localStorage.getItem("key");

删除数据语法：localStorage.removeItem("key");

SessionStorage 替代回话cookie

### Nginx？

反向代理服务器

负载均衡

### 单点故障:【f5】

Lvs:软件，免费，开源的，用起来难

F5:硬件，用起来简单，贵

### 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。

### 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。

### 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 AOP你是怎么用的?

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]

### Spring IOC你是怎么理解的？

IOC我的理解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。

### Application.yml：

**这个文件天然的形成了树形结构，看上去更加一目了然，而且使用起来比较方便，这个文件把公共的一些名字提取了出来，可以减少代码量。**

**并且可以和Application.propties共存**

分布式锁：

可以通过redission实现分布式锁，主要是为了解决 多进程 下的线程安全问题。接口的幂等性问题，就可以通过分布式锁的方式来解决，像重复下单或者重复充值。

### Redis集群

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。

这里我给举个例子说明一下，比如说我们要存储一个key为name的，那么就会通过crc16这个算法将这个key算出对应的节点，具体是通过%的算出来的，然后存到对应的槽中。取值也会根据这个取出来。

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。

**双重判定锁：**

Public Class SingLeton{

Private volatile static SingLeton singLeton = null;

Private SingLeton(){};

Public static SingLeton getSingLeton(){

If(null == singLeton){

Synchronized(SingLeton.class){

If(null == singLeton){

singLeton = new SingLeton();

}

}

}

Return singLeton;

}

}