97 | 项目实战三：设计实现一个支持自定义规则的灰度发布组件（设计）

王争 · 设计模式之美

上一节课，我们介绍了灰度组件的一个需求场景，将公共服务平台的 RPC 接口，灰度替换为新的 RESTful 接口，通过灰度逐步放量，支持快速回滚等手段，来规避代码质量问题带来的不确定性风险。

跟前面两个框架类似，灰度组件的功能性需求也比较简单。上一节课我们做了简单分析，今天我们再介绍一下，这个组件的非功能性需求，以及如何通过合理的设计来满足这些非功能性需求。

话不多说，让我们正式开始今天的学习吧！

非功能性需求

上一节课中，我给你留了一个作业，参照限流框架，分析一下灰度组件的非功能性需求。对于限流框架，我们主要从易用性、扩展性、灵活性、性能、容错性这几个方面，来分析它的非功

能性需求。对于灰度组件，我们同样也从这几个方面来分析。

易用性

在前面讲到限流框架和幂等框架的时候，我们都提到了“低侵入松耦合”的设计思想。因为框架需要集成到业务系统中使用，我们希望它尽可能低侵入，与业务代码松耦合，替换、移除起来更容易些。因为接口的限流和幂等跟具体的业务是无关的，我们可以把限流和幂等相关的逻辑，跟业务代码解耦，统一放到公共的地方来处理（比如 Spring AOP 切面中）。

但是，对于灰度来说，我们实现的灰度功能是代码级别的细粒度的灰度，而替代掉原来的 if-else 逻辑，是针对一个业务一个业务来做的，跟业务强相关，要做到跟业务代码完全解耦，是不现实的。所以，在侵入性这一点上，灰度组件只能做妥协，容忍一定程度的侵入。

除此之外，在灰度的过程中，我们要不停地修改灰度规则，在测试没有出现问题的情况下，逐渐放量。从运维的角度来说，如果每次修改灰度规则都要重启系统，显然是比较麻烦的。所以，我们希望支持灰度规则的热更新，也就是说，当我们在配置文件中，修改了灰度规则之后，系统在不重启的情况下会自动加载、更新灰度规则。

扩展性、灵活性

跟限流框架一样，我们希望支持不同格式（JSON、YAML、XML 等）、不同存储方式（本地配置文件、Redis、Zookeeper、或者自研配置中心等）的灰度规则配置方式。这一点在限流框架中已经详细讲过了，在灰度组件中我们就不重复讲解了。

除此之外，对于灰度规则本身，在上一节课的示例中，我们定义了三种灰度规则语法格式：具体值（比如 893）、区间值（比如 1020-1120）、比例值（比如 %30）。不过，这只能处理比较简单的灰度规则。如果我们要支持更加复杂的灰度规则，比如只对 30 天内购买过某某商品并且退货次数少于 10 次的用户进行灰度，现在的灰度规则语法就无法支持了。所以，如何支持更加灵活的、复杂的灰度规则，也是我们设计实现的重点和难点。

性能

在性能方面，灰度组件的处理难度，并不像限流框架那么高。在限流框架中，对于分布式限流模式，接口请求访问计数存储在中心存储器中，比如 Redis。而 Redis 本身的读写性能以及限

流框架与 Redis 的通信延迟，都会很大地影响到限流本身的性能，进而影响到接口响应时间。所以，对于分布式限流来说，低延迟高性能是设计实现的难点和重点。

但是，对于灰度组件来说，灰度的判断逻辑非常简单，而且不涉及访问外部存储，所以性能一般不会有太大问题。不过，我们仍然需要把灰度规则组织成快速查找的数据结构，能够支持快速判定某个灰度对象（darkTarget，比如用户 ID）是否落在灰度规则设定的区间内。

容错性

在限流框架中，我们要求高度容错，不能因为框架本身的异常，导致接口响应异常。从业务上来讲，我们一般能容忍限流框架的暂时、小规模的失效，所以，限流框架对于异常的处理原则是，尽可能捕获所有异常，并且内部“消化”掉，不要往上层业务代码中抛出。

对于幂等框架来说，我们不能容忍框架暂时、小规模的失效，因为这种失效会导致业务有可能多次被执行，发生业务数据的错误。所以，幂等框架对于异常的处理原则是，按照 fail-fast 原则，如果异常导致幂等逻辑无法正常执行，让业务代码也中止。因为业务执行失败，比业务执行出错，修复的成本更低。

对于灰度组件来说，上面的两种对异常的处理思路都是可以接受的。在灰度组件出现异常时，我们既可以选择中止业务，也可以选择让业务继续执行。如果让业务继续执行，本不应该被灰度到的业务对象，就有可能被执行。这是否能接受，还是要看具体的业务。不过，我个人倾向于采用类似幂等框架的处理思路，在出现异常时中止业务。

框架设计思路

根据刚刚对灰度组件的非功能性需求分析，以及跟限流框架、幂等框架非功能性需求的对比，我们可以看出，在性能和容错性方面，灰度组件并没有需要特别要处理的地方，重点需要关注的是易用性、扩展性、灵活性。详细来说，主要包括这样两点：支持更灵活、更复杂的灰度规则和支持灰度规则热更新。接下来，我们就重点讲一下，针对这两个重点问题的设计思路。

首先，我们来看，如何支持更灵活、更复杂的灰度规则。

灰度规则的配置也是跟业务强相关的。业务方需要根据要灰度的业务特点，找到灰度对象（上节课中的 darkTarget，比如用户 ID），然后按照给出的灰度规则语法格式，配置相应的灰度规则。

对于像刚刚提到的那种复杂的灰度规则（只对 30 天内购买过某某商品并且退货次数少于 10 次的用户进行灰度），通过定义语法规则来支持，是很难实现的。所以，针对复杂灰度规则，我们换个思路来实现。

我暂时想到了两种解决方法。其中一种是使用规则引擎，比如 Drools，可以在配置文件中调用 Java 代码。另一种是支持编程实现灰度规则，这样做灵活性更高。不过，缺点是更新灰度规则需要更新代码，重新部署。

对于大部分业务的灰度，我们使用前面定义的最基本的语法规则（具体值、区间值、比例值）就能满足了。对于极个别复杂的灰度规则，我们借鉴 Spring 的编程式配置，由业务方编程实现，具体如何来做，我们放到下一节课的代码实现中讲解。这样既兼顾了易用性，又兼顾了灵活性。

之所以选择第二种实现方式，而不是使用 Drools 规则引擎，主要是出于不想为了不常用的功能，引入复杂的第三方框架，提高开发成本和灰度框架本身的学习成本。

其次，我们来看，如何实现灰度规则热更新。

规则热更新这样一个功能，并非灰度组件特有的，很多场景下都有类似的需求。在第 25、26 讲中，讲到性能计数器项目的时候，我们也提到过这个需求。

灰度规则的热更新实现起来并不难。我们创建一个定时器，每隔固定时间（比如 1 分钟），从配置文件中，读取灰度规则配置信息，并且解析加载到内存中，替换掉老的灰度规则。需要特别强调的是，更新灰度规则，涉及读取配置、解析、构建等一系列操作，会花费比较长的时间，我们不能因为更新规则，就暂停了灰度服务。所以，在设计和实现灰度规则更新的时候，我们要支持更新和查询并发执行。具体如何来做，我们留在下一节课的实现中详细讲解。

重点回顾

好了，今天的内容到此就讲完了。我们一块来总结回顾一下，你需要重点掌握的内容。

今天，我们对比限流框架、幂等框架，讲解了灰度组件的非功能性需求，主要包含易用性、扩展性、灵活性、性能、容错性这样几个方面，并且针对性地解释了对应的设计思路。

在易用性方面，我们重点讲解了“低侵入、松耦合”的设计思想。限流、幂等因为其跟业务无关，可以做到最大程度跟业务解耦，做到低侵入。但是，我们这里实现的代码层面的灰度，因为跟业务强相关，所以，跟业务代码耦合的比较紧密，比较难做到低侵入。

在扩展性、灵活性方面，除了像限流框架那样，支持各种格式、存储方式的配置方式之外，灰度组件还希望能支持复杂的灰度规则。对于大部分业务的灰度，我们使用最基本的语法规则（具体值、区间值、比例值）就能满足了。对于极个别复杂的灰度规则，我们借鉴 Spring 的编程式配置，由业务方编程实现。

在性能方面，灰度组件没有需要特殊处理的地方。我们只需要把灰度规则组织成快速查找的数据结构，能够支持快速判定某个灰度对象（darkTarget，比如用户 ID），是否落在灰度规则设定的区间内。

在容错性方面，限流框架要高度容错，容忍短暂、小规模的限流失效，但不容忍框架异常导致的接口响应异常。幂等框架正好相反，不容忍幂等功能的失效，一旦出现异常，幂等功能失效，我们的处理原则是让业务也失败。这两种处理思路都可以用在灰度组件对异常的处理中。我个人倾向于采用幂等框架的处理思路。

课堂讨论

在项目实战这部分中，我们多次讲到“低侵入、松耦合”的设计思路，我们平时使用 Logger 框架，在业务代码中打印日志，算不算是对业务代码的侵入、耦合？

欢迎留言和我分享你的想法。如果有收获，也欢迎你把这篇文章分享给你的朋友。

灰度规则的设计思路，包括使用规则引擎或支持编程实现灰度规则。总的来说，本文为读者提供了灰度发布组件设计和实现的思路和方法，对于需要实现灰度发布组件的开发人员具有一定的参考价值。文章还讲解了灰度组件的非功能性需求，主要包含易用性、扩展性、灵活性、性能、容错性这样几个方面，并且针对性地解释了对应的设计思路。在易用性方面，重点讲解了“低侵入、松耦合”的设计思想。在扩展性、灵活性方面，除了像限流框架那样，支持各种格式、存储方式的配置方式之外，灰度组件还希望能支持复杂的灰度规则。在性能方面，灰度组件没有需要特殊处理的地方。在容错性方面，限流框架要高度容错，容忍短暂、小规模的限流失效，但不容忍框架异常导致的接口响应异常。幂等框架正好相反，不容忍幂等功能的失效，一旦出现异常，幂等功能失效，我们的处理原则是让业务也失败。

全部留言 (11)

最新　精选

汝林外史
2020-07-10

发布之前进行充分的测试不就行了吗？灰度测试是针对什么场景呢？

作者回复: 即便是充分测试，也很难保证一点都不出问题呢

共 4 条评论>　5

Jxin
2020-06-15

1.这要看系统运行日志属不属于业务逻辑的一部分。我认为是属于的。毕竟我要的是可追溯的业务代码，而不是只有功能的业务代码。可追溯我认为是业务的一部分。同理还包括主动告警。

2.所以我认为算不上侵入。至于耦合，log的实现层是可以替换的，所以也没有耦合。

29

，
2020-06-15

我在工作的过程中,遇到的常规业务方法大概是这样的:
1.权限校验,权限合法才能继续往下走,不合法就抛异常
2.参数校验,参数合法才能继续往下走,不合法就抛异常

3.业务处理,处理成功才能继续往下走,不成功就抛异常
4.业务附加处理(例如短信通知,记录业务日志),处理完成返回,失败则在第三方打印异常,这个部分一般不会出现异常

如果再加上课里面讲到的幂等框架,限流框架等,想要做到零侵入,低耦合,个人感觉并不现实,应该看项目的具体安排,如果时间紧任务重,以服务调用的方式也未尝不可,也就一行代码的事,侵入性并没有想象中的那么夸张,如果时间宽裕,做一个漂亮的切面,也是不错的

课后题:

打印日志算不算对业务代码的侵入,个人认为完全看对"业务代码"范围的定义。比如一次保存稿件的功能,有的人认为只有 save(docuemnt) 这一步才算业务,其他都属于附加功能,但有的人认为权限校验,参数校验,业务处理,业务附加处理全部加起来才算一个完整的业务流程,这时,关键性的业务日志打印/存储其实也属于业务范围内的事情了,权限校验和参数校验也一样。我还是倾向于认为第二种更接近"业务代码"范围的定义。

简而言之,我的观点是 日志打印/存储如果是为了debug,那么则不属于业务范围内,对代码有一定侵入性,如果是为了留档,方便以后的核对等工作,那么则属于业务范围内的事情,对代码没有侵入性。

20

不惑ing
2020-07-17

低侵入松耦合，不是不侵入不耦合，所以Logger符合

4

test
2020-06-15

Logger需要用户控制打什么日志，在哪里打，算是牺牲了一定耦合度

4

守拙
2020-07-14

Logger框架是否符合"低侵入, 松耦合"要根据Logger框架的提供的功能来判定.

例如Logger框架提供全局配置的开关功能, 就体现了一定程度的低侵入. 因为不需要Log时全局关闭对业务没有丝毫影响.

Logger框架是否做了足够的封装, 适用于多种场景: 本地log, log上传至Server, log写入db/文件系统;

是否支持多种格式的log: 纯文本, json格式, xml格式等是衡量Log易用性, 灵活性, 可扩展性的量化指标.

总结: 项目只要使用Log框架, 就无法避免耦合的情况. 既然Log对于项目是必须的, 我们就应该综合参考Log框架是否低侵入松耦合, 易用性, 扩展性, 性能, 可复用性等指标, 以量化的方式做框架的选型.

3

Heaven
2020-06-15

从耦合的角度来看,是在业务代码之中打印的,这是和业务代码耦合在了一起,但是和业务无关,需要删去的时候,不需要修改业务代码,只移除非业务代码,我的角度来看,是不属于对于业务代码的侵入耦合的

3

小晏子
2020-06-15

如果使用的是log4j，logback等这种基于实现类编程的框架，那么是有侵入，有耦合性的。
如果使用的是slf4j这种日志接口框架，那么多业务代码是无侵入的，低耦合的，因为底层具体实现的log框架可以无缝替换为另外一个。

2

只为更好
2021-09-23

老师，业务逻辑的灰度如何去做？如果业务代码写很多开关，也会降低代码的可维护性、可读性等，另外数据模型的调整，比如字段修改、删除如何做灰度呢

1

否极泰来
2021-04-10

不算，因为我们需要查看日志定位问题，我觉得是属于业务的一部分。

1