# 微服务

## 什么是微服务？

微服务架构是一种架构模式，将单一的应用程序划分成一组小的服务，每个服务运行在其独立的自己的进程内，当用户发出请求，服务之间相互协调，相互配合，共同完成整个功能。

## 为什么要用微服务？

### 单一架构模式：

#### 优势：

* 开发效率高
* 易于部署
* 易于测试

#### 劣势：

* 部署成本高（无论是修改1行代码，还是10行代码，都要全量替换）
* 可伸缩性差，系统的扩容只能只对这个应用进行扩容，不能做到对某个功能点进行扩容
* 复杂度高，随着业务的不断迭代，项目的代码量会急剧的增多，项目模块也会随着而增加，模块与模块之间的关系就会变成的很复杂，整个项目就会变成的非常复杂

### 微服务架构

#### 优势

* 微服务是松耦合的，可以对某一修改的模块单独部署
* 可伸缩性比较好，能做到对某个功能点进行扩容
* 不同服务之间可以使用不同的技术

#### 劣势

* 服务间通信成本问题；
* 系统部署比较复杂
* 故障诊断比较难，不容易定位错误节点；

# SpringCloud Netflix

## Eureka（服务治理）

Eureka的服务治理体系有三个核心角色：服务注册中心、服务提供者，，服务消费者。

#### 服务注册中心：

指的是Eureka提供的服务端，主要负责提供服务注册与发现功能。

#### 服务提供者：

指的是可以提供服务的应用。

#### 服务消费者：

指的是消费者从服务注册中心获取服务列表。

服务提供者启动时，会通过发送rest请求的方式向server注册自己，并且携带自身的元数据信息（ip,端口，微服务名称等），保存在server的注册表中，然后服务提供者每隔30s会向server发送心跳，告诉server自己还存活，如果sever在默认的时间（90s）内没有收到来自客户端的心跳，那么server就会注销该服务实例。

sever中保存客户端数据的注册表是基于内存进行存储的，在内存里维护了一个CocurrentHashMap<String ,Map<String,Leasse<InstanceInfo>>>的数据结构。该结构是以双层map的形式来进行存储的数据的，最外层的key是客户端微服务的名称，value也是一个map结构，这个map的key是服务实例的id(host+ serviceId + port),value就是client实例信息（ip、端口号、等信息）。

服务消费者在启动的时候，向注册中心发送REST请求给服务注册中心，从服务注册中心获取服务列表清单。并将其缓存在本地，客户端会使用该信息查找其他服务，从而进行远程调用，同时也会每隔30s也会向server发送心跳，完成服务续约，server中的注册表信息定期（每30秒钟）更新一次。

实际上当客户端在拉取服务注册表的时候，其实客户端不是直接从 Eureka 中的服务注册表中获取数据的，因为Eureka 做了二级缓存，第一级叫做 ReadOnly（ReadOnlyCacheMap） 缓存，二级叫做 ReadWrite（ReadWriteCacheMap） 缓存。首先客户端会直接从ReadOnly 缓存中读取注册表信息。若没有，就找ReadWrite里缓存的注册表。如果还没有，就从内存中获取实际的注册表数据。

当服务在进行注册的时候，先向服务注册表中写入注册信息，服务注册表更新了，立马会同步一份数据到 ReadWrite 缓存中去，此时会有一个定时任务（每隔30s）会定时去检查 ReadWrite缓存是否跟  ReadOnly缓存不一致, 不一致就把数据同步到 ReadOnly缓存中去,如果注册表发生变更的时候，会在内存中更新变更的注册表数据，同时过期掉ReadWrite缓存。此过程不会影响ReadOnly缓存提供人家查询注册表。在一段时间内（默认是30s）,各服务拉取注册表会直接读ReadOnly缓存, 30s过后，后台线程发现ReadWrite缓存已经清空了，也会清空ReadOnly缓存中的缓存, 等到下次有服务拉取注册表，又会从内存中获取最新的数据了，同时填充各个缓存。

#### 多级缓存机制的优点是什么？

尽可能保证了内存注册表数据不会出现频繁的读写冲突问题。并且进一步保证对Eureka Server的大量请求，都是快速从纯内存走，性能极高。

#### 服务同步

当服务提供者发送请求到一个注册中心时，注册中心会将注册的信息转发给其它集群相连的注册中心，完成注册中心之间的服务同步。通过注册中心之间的服务同步，集群注册中心服务信息保持一致。

#### 服务下线：

当服务实例进行正常关闭操作时，它会触发一个服务下线的REST请求Eureka Server，注册中心收到请求时，服务端将该服务状态置为下线(DOWN)，同时把该下线事件传播下去。

#### 失效剔除：

服务有时候并不一定会正常下线，可能由于异常故障使服务运行不正常，但是，服务注册中心并未收到"服务下线"请求。注册中心为了将这些无法提供服务的实例剔除，Eureka Server在启动的时候会创建一个定时任务，默认每隔一段时间(默认为60秒)将当前清单中超时(默认为90秒)没有续约的服务从注册中心剔除。

#### 自我保护：

默认情况下，如果Eureka Server在一定时间内（默认90秒）没有接收到某个微服务实例的心跳，Eureka Server将会移除该实例。

但是当网络分区故障发生时，微服务与Eureka Server之间无法正常通信，而微服务本身是正常运行的，此时不应该移除这个微服务，所以引入了自我保护机制。

自我保护机制的工作机制是如果在15分钟内超过85%的客户端节点都没有正常的心跳，那么Eureka就认为客户端与注册中心出现了网络故障，Eureka Server自动进入自我保护机制，

此时会出现以下几种情况：

1）Eureka Server不再从注册列表中移除因为长时间没收到心跳而应该过期的服务。

2）Eureka Server仍然能够接受新服务的注册和查询请求，但是不会被同步到其它节点上，保证当前节点依然可用。

3）当网络稳定时，当前Eureka Server新的注册信息会被同步到其它节点中。

#### 注解：

@EnableEurekaServer：

@EnableDiscoveryClient

## ribbon（负载均衡）

#### 概要

是一个客户端的负载均衡工具，主要功能是提供客户端的软件负载均衡算法和服务调用，可以和RestTemplate搭配使用，使用@LoadBalanced注解完成服务间的负载均衡调用功能，并携带重试机制。

#### Ribbon 负载均衡策略：

RoundRobinRule: 轮询策略，Ribbon以轮询的方式选择服务器，这个是默认值。所以示例中所启动的两个服务会被循环访问;

WeightedResponseTimeRule: 带有加权的轮询策略，对各个服务器响应时间进行加权处理，响应速度越快的实例选择权重越大，越容易被选择。然后在采用轮询的方式来获取相应的服务器;

RandomRule: 随机选择，也就是说Ribbon会随机从服务器列表中选择一个进行访问;

RetryRule：重试规则，先按照RoundRobinRule的策略获取服务，如果获取服务失败则在指定时间内会进行重试，获取可用的服务。

BestAvailableRule: 最大可用策略，会先过滤掉由于多次访问故障而处于断路器跳闸状态的服务，然后选择一个并发量最小的服务;

AvailabilityFilteringRule: 先过滤掉故障实例，再选择并发较小的实例。

ZoneAvoidanceRule: 区域权衡策略，先使用主过滤条件（区域负载器，选择最优区域）对所有实例过滤并返回过滤后的实例清单，依次使用过滤条件列表中的过滤条件对主过滤条件的结果进行过滤，判断最小过滤数（默认1）和最小过滤百分比（默认0），最后对满足条件的服务器则使用RoundRobinRule(轮询方式)选择一个服务器实例。

#### 自定义负责均衡策略

还可以自定义负责均衡策略，

官方文档明确给出了警告：这个自定义配置类不能放在@ComponentScan所扫描的当前包下以及子包下，否则我们自定义的这个配置类就会被所有的Ribbon客户端所共享，达不到特殊化定制的目的了。

实现这个IRule接口，就能自定义负载均衡策略,在启动类配置@RibbonClient(name= "CLOUD-PAYMENT-SERVICE",configuration=MySelfRule.class)（MySelfRule是自定义策略配置类的名称）

#### 轮训负载均衡算法原理：

负载均衡算法：rest接口第几次请求数 % 服务器集群总数量 = 实际调用服务器位置下标  ，每次服务重启动后rest接口计数从1开始。

List<ServiceInstance> instances = discoveryClient.getInstances("CLOUD-PAYMENT-SERVICE");

如：   List [0] instances = 127.0.0.1:8002

　　　List [1] instances = 127.0.0.1:8001

8001+ 8002 组合成为集群，它们共计2台机器，集群总数为2， 按照轮询算法原理：

当总请求数为1时： 1 % 2 =1 对应下标位置为1 ，则获得服务地址为127.0.0.1:8001

当总请求数位2时： 2 % 2 =0 对应下标位置为0 ，则获得服务地址为127.0.0.1:8002

当总请求数位3时： 3 % 2 =1 对应下标位置为1 ，则获得服务地址为127.0.0.1:8001

当总请求数位4时： 4 % 2 =0 对应下标位置为0 ，则获得服务地址为127.0.0.1:8002

#### Nginx 和 Ribbon 的对比

##### 集中式负载均衡器

将所有请求都集中起来，然后再进行负载均衡（nginx就是属于集中式的负载均衡器）。

##### 进程内负载均衡器

负载均衡器集成到消费方，请求到达消费方，消费方再从服务注册中心获知有哪些地址可用，然后自己再从这些地址中选择出一个合适的服务器。

#### 注解

@LoadBalanced

## Feign（服务调用）

#### 概要:

Feign是一种声明式、模板化的HTTP客户端 ，再RestTemplate的基础上更进一步的封装了，以创建Java接口并使用注解配置的方式来完成对服务提供方的参数绑定，并且在Feign的内部集成了Ribbon负载均衡器，实现了客户端的负载均衡调用。

#### Feign的底层实现

Feign是基于面向接口动态代理的方式生成实现类，然后将请求调用委托到动态代理实现类中，根据默认的contract协议解析接口上的方法和注解，转换成内部的MethodHandler处理方式，根据传入的bean对象和注解信息，从中提取出数据，生成request对象，Feign最终会将请求转化成Http消息发送出去，传入的请求对象，会被解析成消息体。在请求转换的过程，可以自定义拦截器，对请求和响应进行装饰处理，并且在发送请求和响应请求的时候，定义了统一的日志门面来输出日志消息，Feign 真正发送HTTP请求是委托给 Feign.Client 来做的。Feign内部设置一个重试器，当http请求发生io异常时，会有一个最大重试次数。重新发出请求。

#### Feign的源码实现的过程：

* 首先通过@EnableFeignClients注解开启FeignClient
* 根据Feign的规则实现接口，并加@FeignClient注解
* 程序启动后，会进行包扫描，扫描所有的@FeignClient的注解的类，并将这些信息注入到ioc容器中。
* 当接口的方法被调用，通过jdk的代理，将Bean对象和注解信息生成具体的RequesTemplate，构造相对应的Request对象
* Request对象交给Client去处理，其中Client可以是HttpUrlConnection、HttpClient也可以是Okhttp
* 最后Client被封装到LoadBalanceClient类，这个类结合Ribbon做到了负载均衡。
* Feign 内置了一个重试器，当HTTP请求出现IO异常时，Feign会有一个最大尝试次数发送请求

#### Feig和Ribbion的区别：

##### 相同点

Ribbon 和 Feign 都是用于调用其他服务的，都实现了负载均衡和重试机制。

##### 不同点

* 启动类使用的注解不同，Ribbon 用的是@RibbonClient，Feign 用的是@EnableFeignClients。
* 服务的指定位置不同，Ribbon 是在启动类上使用@RibbonClient 注解上声明，Feign则是在定义抽象方法的接口中使用@FeignClient 声明。
* 调用方式不同，Ribbon 需要自己构建 http 请求，模拟 http 请求然后使用 RestTemplate 发送给其他服务，Feign 则是在 Ribbon 的基础上进行了一次改进，采用接口的方式，将需要调用的其他服务的方法定义成抽象方法即可，不需要自己构建 http 请求。不过要注意的是抽象方法的注解、方法签名要和提供服务的方法完全一致。

#### Feign和OpenFeign的区别：

* Feign本身不支持Spring MVC的注解，它有一套自己的注解。
* OpenFeign是Spring Cloud 在Feign的基础上支持了Spring MVC的注解，如@RequesMapping等等

#### 注解

@EnableFeignClients

@FeignClient

## Hystrix（断路器）

#### 概要

Hystrix是一个用于处理分布式系统的延迟和容错的开源库，分布式系统里，为了防止依赖服务之间调用失败，而导致的服务雪崩问题，对依赖服务调用之间出现的调用延迟和调用失败进行控制和容错保护。

#### 服务雪崩：

当微服务A,调用微服务B的接口时，由于微服务B发生异常，产生请求阻塞，用户无法响应，线程得不到释放，就会造成越来越多的请求阻塞，因为服务器的支持的并发数和线程有限，请求一直阻塞，服务器的资源耗尽，会导致其他的服务也不可用，造成雪崩现象的产生。

#### 解决方案：

服务限流、服务熔断、服务降级、超时监控、请求缓存（生产不建议使用）、请求合并（生产不建议使用）

#### 服务降级

服务降级是指，当请求超时、资源不足等情况发生时进行服务降级处理，不调用真实服务逻辑，而是使用快速失败（fallback）方式直接返回一个托底数据，保证服务链条的完整，避免服务雪崩。

##### 哪些情况会出发降级？

* 程序运行异常
* 超时
* 服务熔断触发服务降级
* 线程池/信号量打满也会导致服务降级

#### 服务熔断

当一定时间内，异常请求比例（请求超时、网络故障、服务异常等）达到阀值时，启动熔断器，熔断器一旦启动，则会停止调用具体服务逻辑，通过fallback快速返回托底数据，保证服务链的完整。

##### 熔断机制状态：

对于熔断机制的实现，Hystrix设计了三种状态，熔断关闭、熔断开启、半熔断状态。

###### 熔断关闭状态（Closed）

服务没有故障时，熔断器所处的状态，对调用方的调用不做任何限制。

###### 熔断开启状态（Open）

在时间滑动窗口中内（Hystrix默认是10秒），接口调用次数大于或等于20次，接口调用出错比率达到一个阈值（Hystrix默认为50%），会进入熔断开启状态。进入熔断状态后，后续对该服务接口的调用不再经过远程调用，直接执行本地的fallback方法。

###### 半熔断状态（Half-Open）

在进入熔断开启状态一段时间之后（Hystrix默认是5秒），熔断器会进入半熔断状态。会尝试让一条请求经过断路器，看能不能正常调用。如果调用成功了，那么就自动恢复，断路器转为 Close 状态。如果重试失败，熔断持续开启，并返回fallback数据。等待下一次休眠时间过后重新尝试。

#### 服务限流

服务端的请求承载量是有限的，当客户端请求时，Hystrix 通过判断线程池或者信号量是否已满，限制请求的并发数，当请求数量过大对服务端产生压力超出容量的请求，直接拒绝走降级，从而达到限流的作用。

##### 线程隔离

Hystrix会为每一个依赖服务分配一个小的线程池，用户的请求是通过线程池的空闲线程来调用服务，如果线程池已满或者请求超时，用户的请求将不再直接访问服务，调用将会被拒绝，通过fallback返回托底数据。

###### 优点：

当线程池出现问题时，线程池是完全隔离状态的，是独立的，不会影响到其他服务的正常执行，独立的线程池也提供了限制并发处理能力, 并且支持异步处理，支持超时处理，当请求超时，会自动中断，是默认的隔离机制。

###### 缺点：

线程池隔离机制，请求处理线程和服务调用线程，不是同一个线程，需要上下文切换，会导致服务硬件计算开销加大。

##### 信号量隔离

信号量隔离就是hystrix的限流功能之一。实际上它是通过信号量来实现的限流功能，而信号量说白了就是个计数器，设置一个并发处理的最大极值，计数器计算达到设定的阈值，多余的请求再来请求线程资源，就被拒绝了，直接就做异常处理，通过fallback返回托底数据，保证服务完整性。

###### 优点：

信号量隔离机制，也提供了限制并发处理能力，请求处理线程和服务调用线程，是同一个线程，无线程切换，开销比较小。

###### 缺点：

不支持超时处理，必须等待远程调用结束，才能判断是否超时。

##### 适用场景：

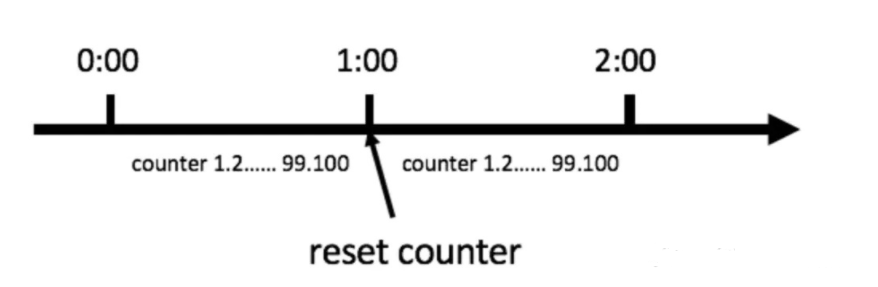
* 线程池技术，适合绝大多数场景，比如说我们对依赖服务的网络请求的调用和访问、需要对调用的 timeout 进行控制（捕捉 timeout 超时异常）。
* 信号量技术，适合说你的访问不是对外部依赖的访问，而是对内部的一些比较复杂的业务逻辑的访问，并且系统内部的代码，其实不涉及任何的网络请求，那么只要做信号量的普通限流就可以了，因为不需要去捕获 timeout 类似的问题。

##### 限流的算法

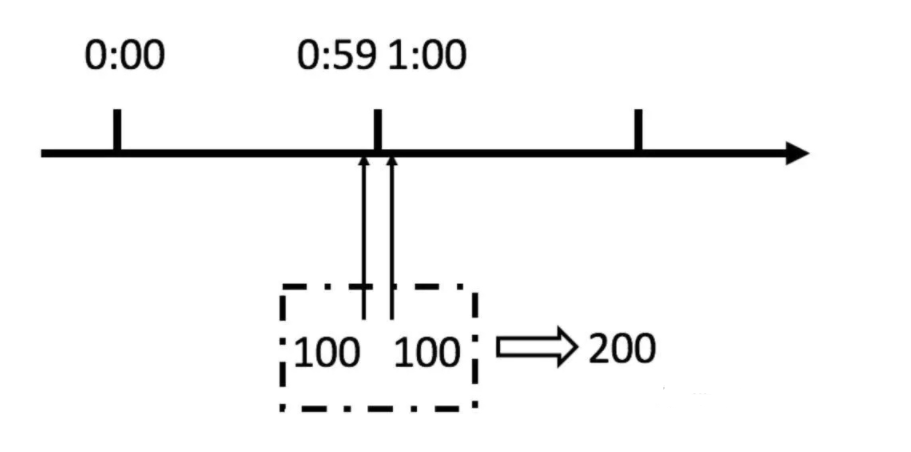
###### 固定窗口计数器算法

**规定我们单位时间处理的请求数量。**

比如我们规定我们的一个接口一分钟只能访问100次的话。使用固定窗口计数器算法的话可以这样实现：给定一个变量counter来记录处理的请求数量，当1分钟之内处理一个请求之后，counter+1，1分钟之内的如果counter=100的话，后续的请求就会被全部拒绝。等到 1分钟结束后，将counter回归成0，重新开始计数（ps：只要过了一个周期就讲counter回归成0）。



这个算法虽然简单，但是有一个十分致命的问题，那就是临界问题。

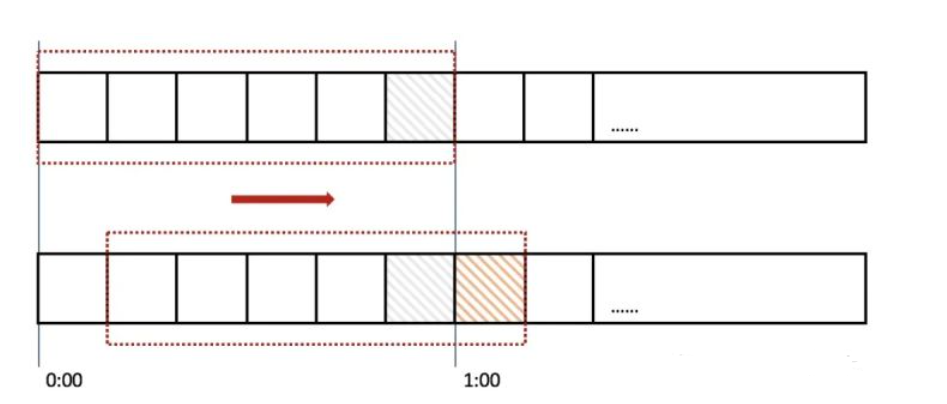


假设有一个恶意用户，他在0:59时，瞬间发送了100个请求，并且1:00又瞬间发送了100个请求，那么其实这个用户在 1秒里面，瞬间发送了200个请求。用户通过在时间窗口的重置节点处突发请求，可以瞬间超过我们的速率限制。用户有可能通过算法的这个漏洞，瞬间压垮我们的系统。

###### 滑动窗口计数器算法

算的上是固定窗口计数器算法的升级版。滑动窗口计数器算法相比于固定窗口计数器算法的优化在于：**它把时间以一定比例分片。**

例如我们的借口限流每分钟处理60个请求，我们可以把 1 分钟分为60个窗口。每隔1秒移动一次，每个窗口一秒只能处理 不大于 60(请求数)/60（窗口数） 的请求， 如果当前窗口的请求计数总和超过了限制的数量的话就不再处理其他请求。



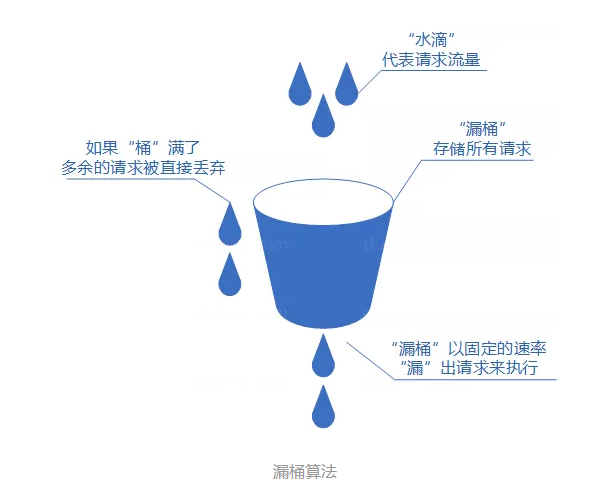
在上图中，整个红色的矩形框表示一个时间窗口，在我们的例子中，一个时间窗口就是一分钟。然后我们将时间窗口进行划分，比如图中，我们就将滑动窗口划成了6格，所以每格代表的是10秒钟。每过10秒钟，我们的时间窗口就会往右滑动一格。每一个格子都有自己独立的计数器counter，比如当一个请求 在0:35秒的时候到达，那么0:30~0:39对应的counter就会加1。

那么滑动窗口怎么解决之前的临界问题的呢？我们可以看上图，0:59到达的100个请求会落在灰色的格子中，而1:00到达的请求会落在橘黄色的格子中。当时间到达1:00时，我们的窗口会往右移动一格，那么此时时间窗口内的总请求数量一共是200个，超过了限定的100个，所以此时能够检测出来触发了限流。

很显然：当滑动窗口的格子划分的越多，滑动窗口的滚动就越平滑，限流的统计就会越精确。

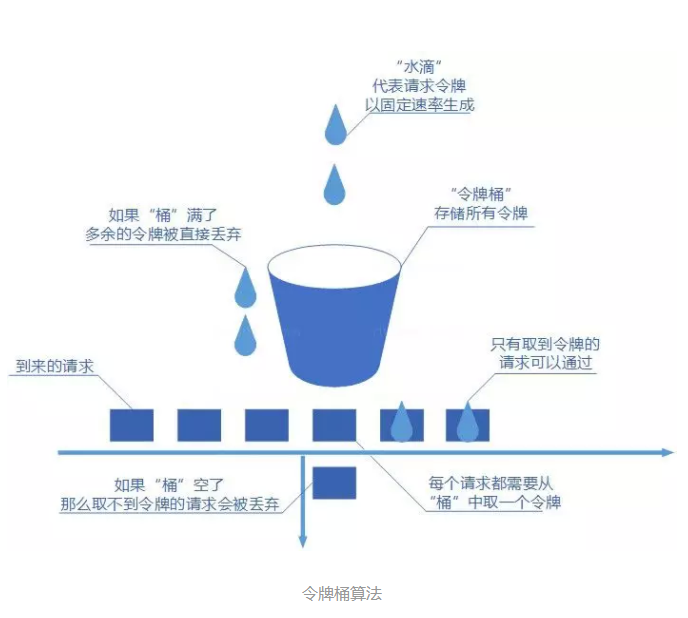
###### 漏桶算法

我们可以把发请求的动作比作成注水到桶中，我们处理请求的过程可以比喻为漏桶漏水。我们往桶中以任意速率流入水，以一定速率流出水。当水超过桶流量则丢弃，因为桶容量是不变的，保证了整体的速率。如果想要实现这个算法的话也很简单，准备一个队列用来保存请求，然后我们定期从队列中拿请求来执行就好了。



###### 令牌桶算法

令牌桶算法和漏桶算法一样,大小固定的令牌桶可自行以恒定的速率源源不断地产生令牌。如果令牌不被消耗，或者被消耗的速度小于产生的速度，令牌就会不断地增多，直到把桶填满，后面再产生的令牌就会从桶中溢出，请求在被处理之前需要拿到一个令牌，请求处理完毕之后将这个令牌丢弃（删除），最后桶中可以保存的最大令牌数永远不会超过桶的大小，所以可以通过控制往桶里添加令牌的速率，可以控制流量峰值的大小。



#### 请求缓存

请求缓存保证在一次请求中多次调用同一个服务提供者接口，在cacheKey不变的情况下，后续调用结果都是第一次的缓存结果，而不是多次请求服务提供者，从而降低服务提供者处理重复请求的压力。

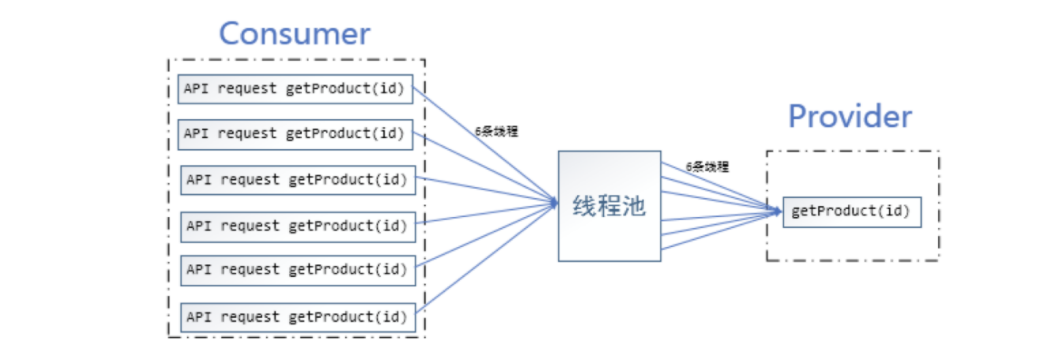
请求缓存不是只写入一次结果就不再变化的，而是每次请求到达Controller的时候，我们都需要为HystrixRequestContext进行初始化，之前的缓存也就是不存在了，我们是在同一个请求中保证结果相同，同一次请求中的第一次访问后对结果进行缓存，缓存的生命周期只有一次请求！

但是使用请求缓存会导致很多的隐患，如：缓存管理不当导致的数据不同步、问题排查困难等，索引解决服务雪崩效应不推荐使用请求缓存。

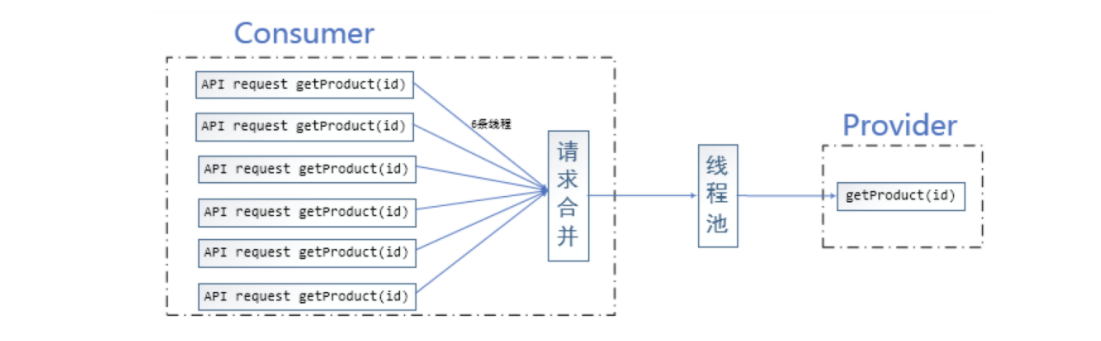
#### 请求合并

在一定时间内，收集一定量的同类型请求，合并请求需求后，一次性访问服务提供者，得到批量结果。这种方式可以减少服务消费者和服务提供者之间的通讯次数，提升应用执行效率。

未使用请求合并



使用请求合并后



##### 优点

当同类型请求的并发数很高，通过设置请求合并器的延迟时间，在一定时间内，收集同类型请求，合并请求需求后，一次性访问服务提供者，可以得到批量结果。减少服务消费者和服务提供者之间的通讯次数，提升应用执行效率。

##### 缺点

通过请求合并器设置延迟时间，这样在并发不高的接口上使用请求合并，会降低响应速度。

#### 注解

@EnableCircuitBreaker

@HystrixCommand

## Zuul（网关）

#### 概要

Zuul是一个微服务网关，会在Eureka注册中心中进行服务的注册和发现。Zuul网关的核心功能是过滤和路由，不管是来自于客户端（PC或移动端）的请求，还是服务内部调用，一切对服务的请求都会经过Zuul这个网关，然后再由网关来实现鉴权、动态路由等操作。

在Zuul的底层使用的是Hystrix+ribbon来实现请求路由，具有负载均衡和服务容错能力，但是Zuul的fallback容错处理逻辑，只针对timeout异常处理，当请求被Zuul路由后，只要服务有返回（包括异常），都不会触发Zuul的fallback容错逻辑。

Zuul中使用Hystrix的配置来设置路由转发时的执行超时时间，其默认的超时时长为1000毫秒。使用Ribbon的配置来设置路由转发时请求连接及处理的超时时间，ribbon底层默认超时时长为5000毫秒。如果Hystrix超时，直接返回超时异常。如果ribbon超时，同时Hystrix未超时，ribbon会自动进行服务集群轮询重试，直到Hystrix超时为止。如果Hystrix超时时长小于ribbon超时时长，ribbon不会进行服务集群轮询重试。并且Zuul网关组件也提供了限流保护。当请求并发达到阀值，自动触发限流保护，返回错误结果。

#### 路由

路由功能负责将外部请求转发到具体的服务实例上去，是实现统一访问入口的基础。

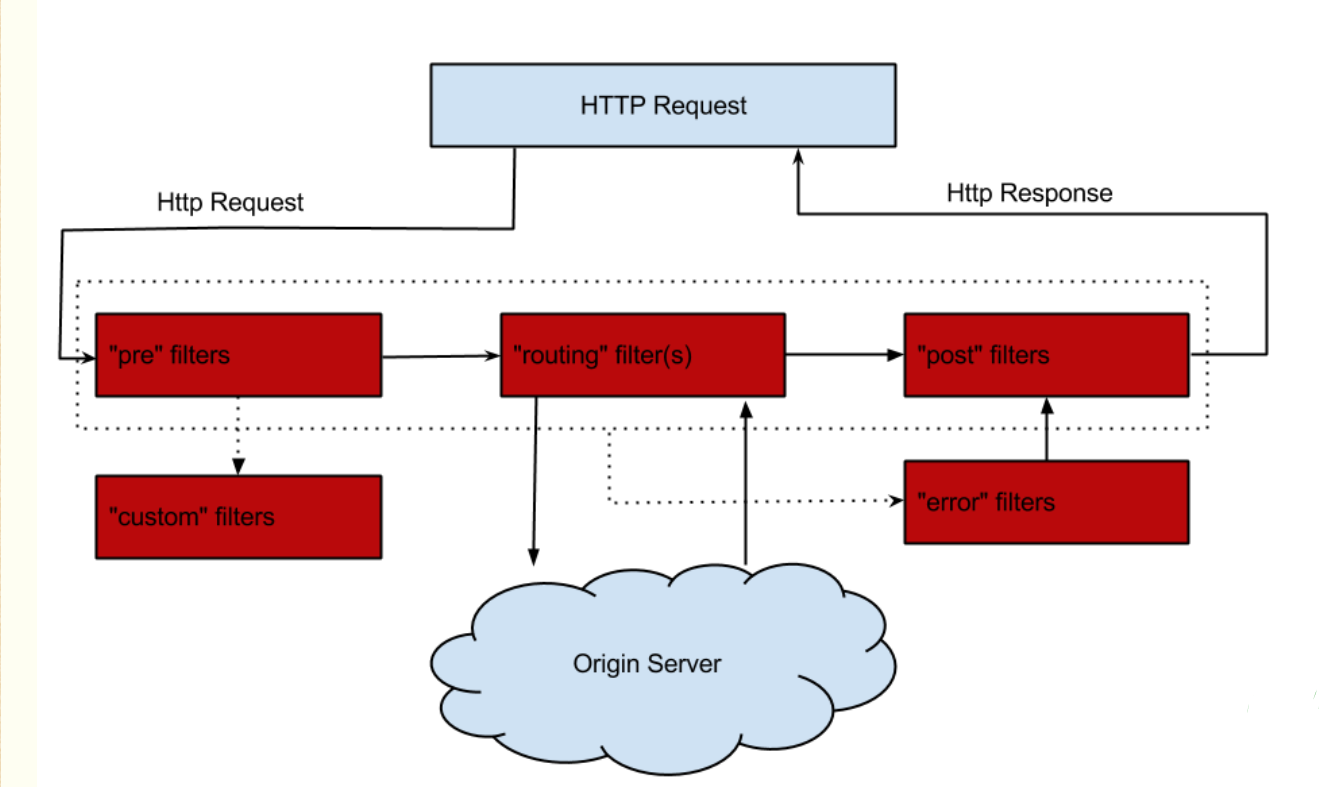
#### 过滤

过滤功能负责对请求过程进行额外的处理，是请求校验过滤及服务聚合的基础。

#### 过滤器类型：

* pre：在请求被路由到目标服务前执行，比如权限校验、打印日志等功能；
* routing：在请求被路由到目标服务时执行，这是使用HttpClient或Ribbon构建和发送原始HTTP请求的地方；
* post：在请求被路由到目标服务后执行，比如给目标服务的响应添加头信息，收集统计数据等功能；
* error：请求在其他阶段发生错误时执行。

#### 请求到过滤的执行流程



首先HTTP请求到达Zuul之后，最先来到pre过滤器（在请求到达路由前被调用），在这里会根据映射Url 找到目标地址，然后将请求与找到的地址交给route类型的过滤器进行求转发，请求服务实例获取响应，通过post类型过滤器对处理结果进行加工与转换等操作返回，在这整个请求过程中只要有异常才会触发，将异常结果交post类型过滤器加工返回。

#### 注解

@EnableZuulProxy

## Config（配置中心）以及Bus（消息总线）

#### 概要

SpringCloud Config一个基于http协议的远程配置实现方式, 通过统一的配置管理服务器进行配置管理，有两个重要的角色，服务端和客户端。

服务端也称为分布式配置中心，它是一个独立的微服务应用，用来连接配置配置仓库（服务器）并为客户端提供获取配置信息。

客户端是通过指定的配置中心来管理应用资源以及业务相关的配置内容，并启动时从配置中心获取和加载配置信息。配置服务器默认采用git来存储配置信息。

#### 注解

@EnableConfigServer

## 1.7、

# Spring Cloud Alibaba

## 2.1、Nacos

## 2.2、Gateway

## 2.3、OpenFeign

## 2.4、Sleuth

## 2.5、Sentinel