

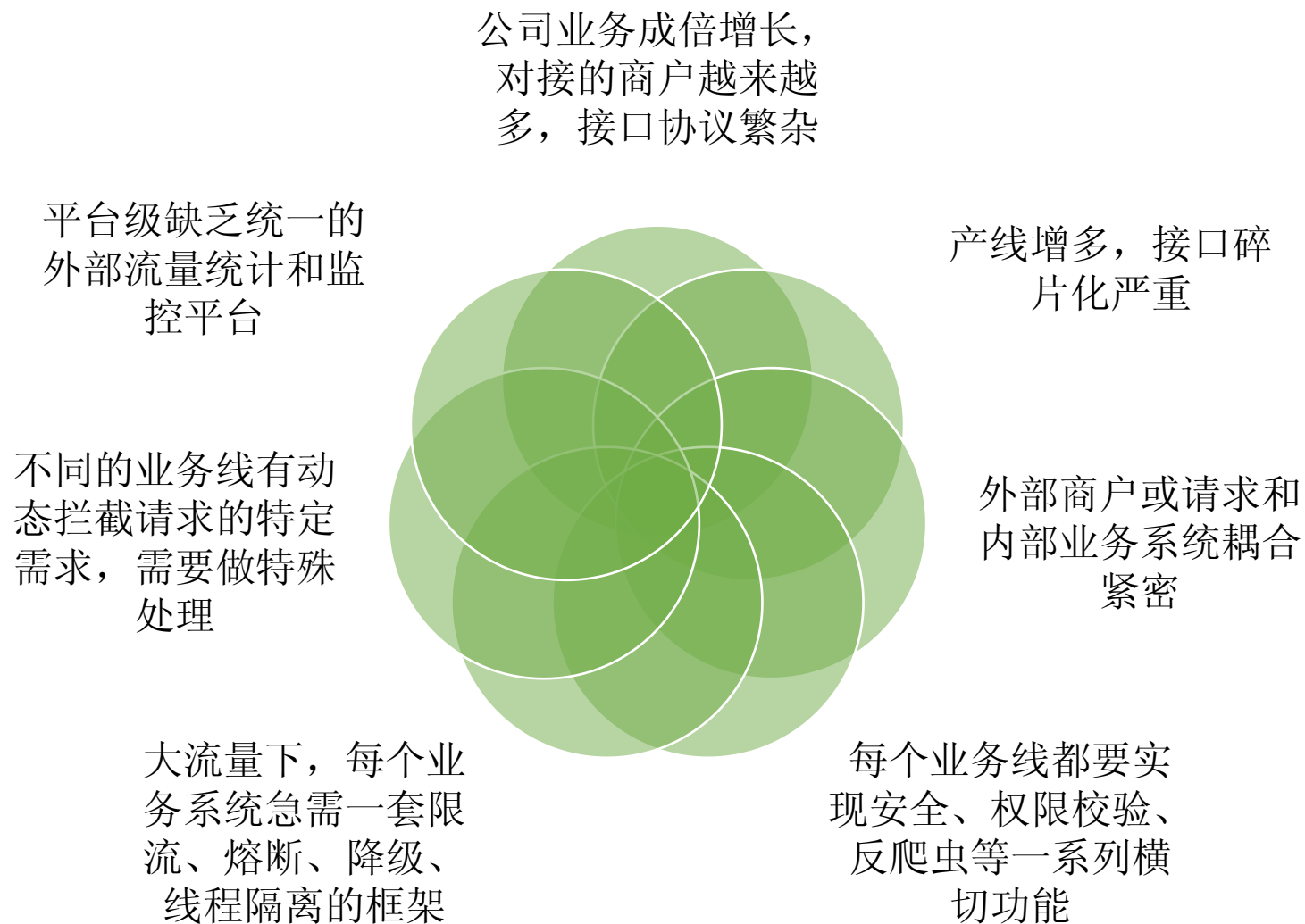
微服务架构下的高可用网关

前隆科技 上海框架部 何雷
2018-03



CONTENTS

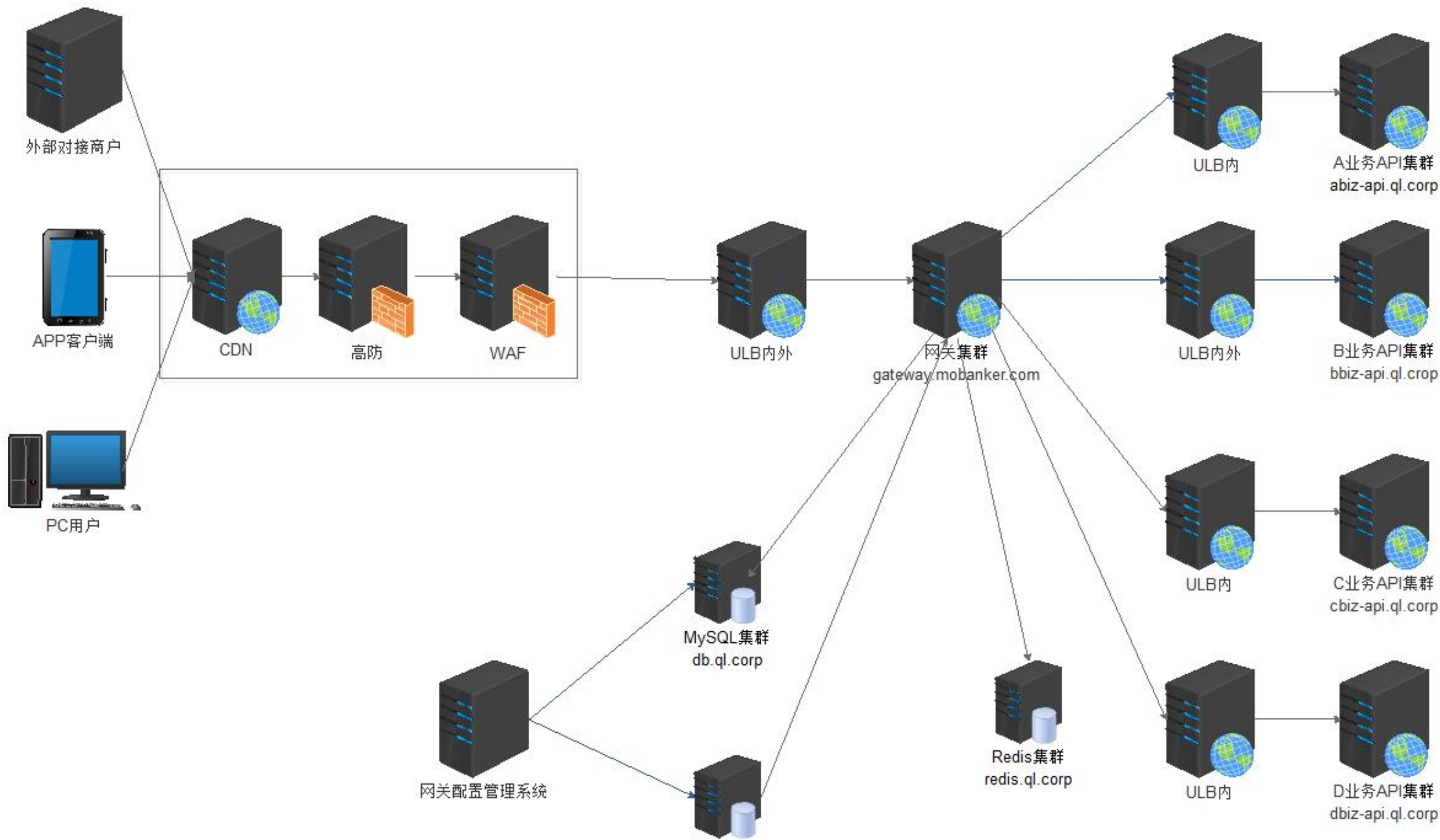
- 前隆网关的背景
- 前隆网关的架构
- 前隆网关高可用措施
 - 监控告警
 - 多维度的认证授权、安全策略
 - 平台级和服务级限流、熔断、降级、线程隔离
 - 实时生成公私钥影响性能的优化
 - 反爬机制措施
 - 动态过滤器



• 技术选型

	Zuul	Kong	Tyk
开发语言/基于平台	Java/Spring Cloud	Nginx	Go
优点	动态过滤 动态路由 验证与安全保障 监控与统计 限流熔断 线程隔离	授权 日志 ip限制 限流 api 统计分析 其他功能通过: lua编写插件实现	不符合当前技术体系
我们的选择	Zuul+ 自研		

前隆网关的架构：物理部署图（部分业务）





网关系统



商户管理



商户列表

路由管理



商户路由管理



路由列表

商户路由管理



流量监控管理



绑定列表

流量监控管理



商户路由管理



流量监控管理



规则列表

控制面板 / 商户管理 / 商户列表

商户列表 - 新增



商户名称:

请输入

商户名称:

InfoQ测试

☒ 是否可用

☒ 是否加密

加密方式:

RSA

签名方式

操作

[查询](#) [编辑](#) [删除](#)

#	ID
1	48

#	ID	服务名	版本号	路径	目标地址	数据传输类型	操作	
1	59	/openapi/1.0.0/**	v1.0	/	/openapi/1.0.0/**/v1.0	http:// :8080	json	查询 编辑 删除
2	45	liftTempLimit	v1.0	/liftTempLimit/v1.0	http:// :8088/business_call_api/api/1.0.0/hycc/	form-data	查询 编辑 删除	

#	ID	商户名称	服务名	版本号	路径	目标地址	操作
1	86	应	yhfq-ajapi/ajapi/**	v1.0	/yhfq-ajapi/ajapi/**/v1.0	http://10.15. 23:8080	查询 编辑 删除
2	85		/openapi/1.0.0/**	v1.0	/ /openapi/1.0.0/**/v1.0	http:// :8080	查询 编辑 删除
3	75	应	yhfq-ajapi/ajapi/**	v1.0	/yhfq-ajapi/ajapi/**/v1.0	http://10.15. 23:8080	查询 编辑 删除
4	73	IVR	selectLimit	v1.0	/selectLimit/v1.0	http:// :8088/business_call_api/api/1.0.0/hycc/	查询 编辑 删除

服务限流开关:



关

网关限流开关:



关

网关监控总阈值:

100000

[更新阈值](#)



[规则说明](#)

服务名:

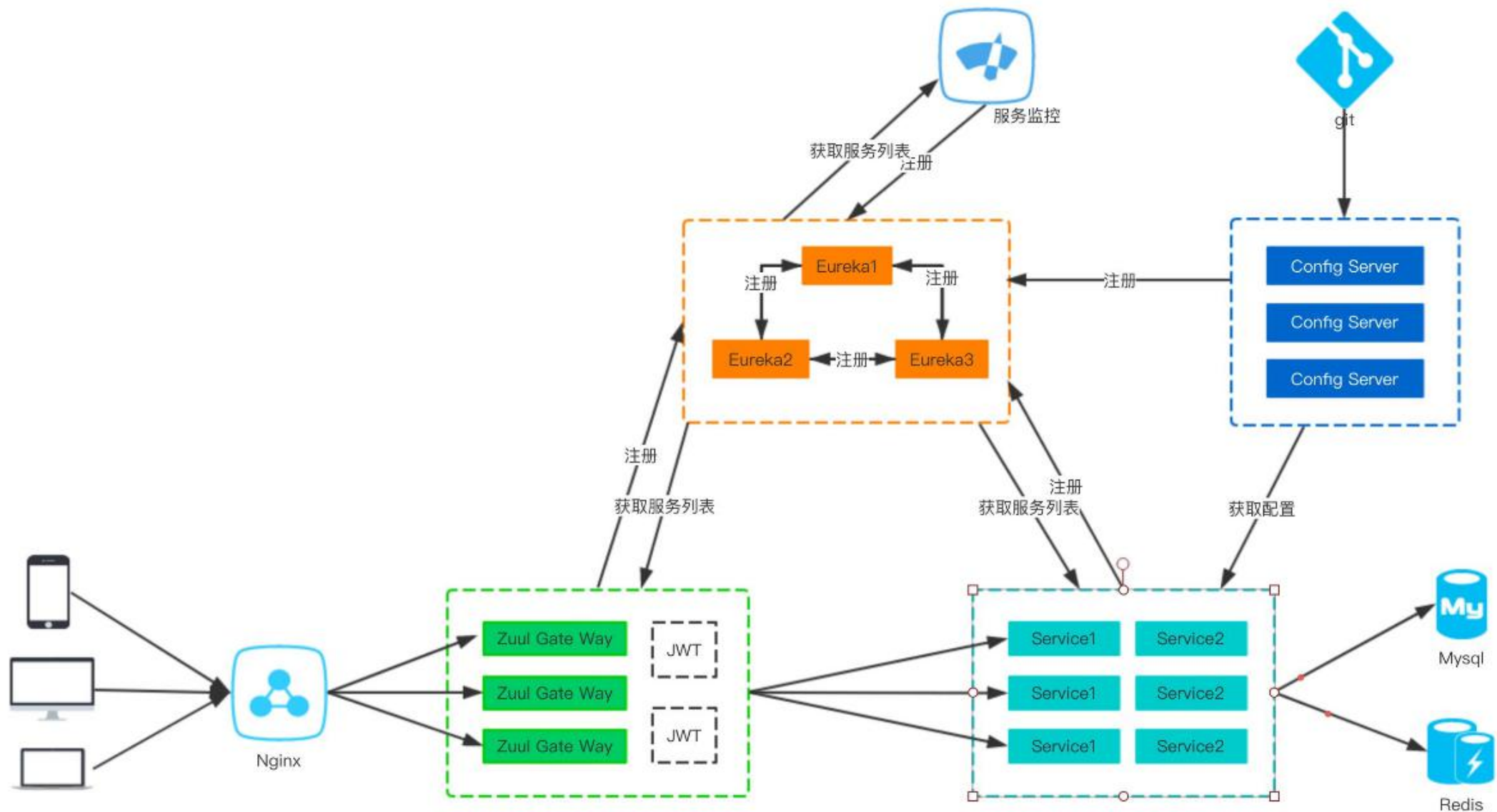
请输入服务名

[查询](#)

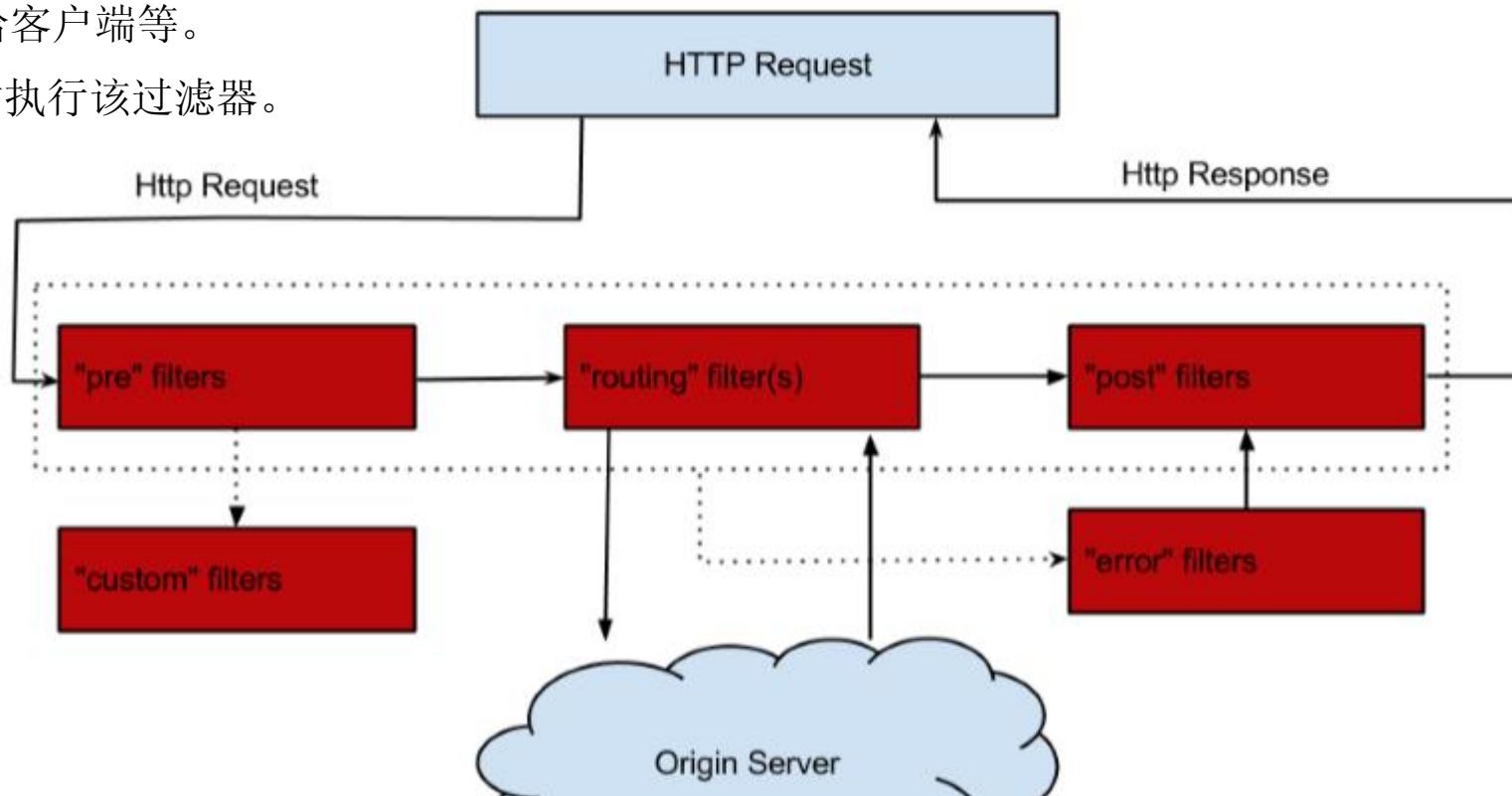
[新增](#)

#	服务名	版本号	时间范围 (秒)	类型	每秒流量	错误码	错误信息	操作
1	/openapi/1.0.0/**	v1.0	1	总流量	10000	err002	后台报错, 请联系管理员	查询 编辑 删除
2	api/user/login	v1.0	1	总流量	10000	err001	卡宜货错误	查询 编辑 删除

前隆网关的架构：Spring Cloud原生态的Zuul



- Zuul大部分功能都是通过过滤器来实现的。Zuul中定义了四种标准过滤器类型，这些过滤器类型对应于请求的典型生命周期。
- (1) **PRE**：这种过滤器在请求被路由之前调用。我们可利用这种过滤器实现身份验证、在集群中选择请求的微服务、记录调试信息等。
- (2) **ROUTING**：这种过滤器将请求路由到微服务。这种过滤器用于构建发送给微服务的请求，并使用Apache HttpClient或Netflix Ribbon请求微服务。
- (3) **POST**：这种过滤器在路由到微服务以后执行。这种过滤器可用于为响应添加标准的HTTP Header、收集统计信息和指标、将响应从微服务发送给客户端等。
- (4) **ERROR**：在其他阶段发生错误时执行该过滤器。



网关与外部交互示例



POST

https://gateway.mobanker.com/openapi/

Params

Send

Save

Authorization

Headers (1)

Body

Pre-request Script

Tests

Code

form-data

x-www-form-urlencoded

raw

binary

JSON (application/json)

```
1 { "merchantsNo": "893146", "service": "SmsCode", "sign": "b3bf714a1c d2f3c1d6", "signType": "md5", "bizRequest": "1q67qBRDODvgjB1mGEeIIV+829Hm8vycz4aDwYv  
++iwd! BAMEZF9JLz33WwSRNGw6ADJDw1I35AX615Ubndmr7rOvNn39SGXuXBQ8XVPzaoMu/POe1rGuhwVXiE BNZTQER6cY3cC2zzG  
+HLZ8t 851+I1kQOI=", "secret": "iSn2m+FZn+oagof4gkU0+3SD2f+9y6FHJ54DdfV7Ba2KzSREtds1w8t pJE0m1AHAtA=" ,  
"version": "v1.0", "uuid": "c218fe92-cd43-4697-b17f-e fa", "timestamp": "2018-03-17 18:26:46"} }
```

Body

Cookies

Headers (4)

Test Results

Status: 200 OK

Time: 513 ms

Pretty

Raw

Preview

JSON

```
1 {  
2   "msg": "成功",  
3   "code": "00000000",  
4   "sign": "f02c45a9b35e aa47955",  
5   "secret": "FJd3+z4Nnn fztVdsPXUWoRiobYJZuY/DiPhBnaw tZEtYoGbSpW3fqRuj7e351TUVe8FWW9RauexZmrxDyKVRyKkq+e8yCKSBEQxKfxZh8+0u9ePhdkAQWVONIUA=",  
6   "bizResponse": "vFq/+ 3jzmpaVGz/LfLXI5Xb11AyZZsSbif oAQQF6hpe3GQ8NY"  
7 }
```

网关

度量平台

指标规则的注册、数据采集、聚合查询

示例：通过三种策略：埋点、接口、sql收集数据

预警平台

构建预警任务、通知预警结果、实时监控仪表盘

示例：错误率达到阈值，短信、邮件、RTX通知负责人

前隆网关高可用措施：度量平台与预警平台



预警平台

仪表盘

预警任务

通知组

时序列

通知记录

预警记录

图表分析

预警平台 / 通知记录

产线: 请选择 应用: 请选择 预警名称: 请选择预警名称 被通知组: 请选择通知组 通知方式: 请选择通知方式 通知状态: 请选择通知状态 查询

被通知组	产线	应用	预警名称	通知状态	内容
rcd	rcd	business_call_api	rcd.call.audio.down.alem	成功	您好，产线：rcd F1(下载量)=0]并
cwc	cwd	financial-web	cwd.repay.fail.rate.warn.task	成功	您好，产线：cwn 2(每日还款总笔
pro	fx	fx-metric	prod.app.count.alem	成功	您好，产线：fx 5 9.000]预警规则
pro	fx	fx-metric	prod.app.count.alem	成功	您好，产线：fx 5 9.000]预警规则
vip3	yhfq	vip3	vip3.success.rate	失败	您好，产线：yhf 数)=38.000 F2(唯
rcd	rcd	business_call_api	rcd.call.audio.down.alem	成功	您好，产线：rcd F1(下载量)=0]并
rcd	rcd	business_call_api	rcd.call.audio.down.alem	成功	您好，产线：rcd F1(下载量)=0]并
cwc	cwd	financial-web	cwd.repay.fail.rate.warn.task	成功	您好，产线：cwn 2(每日还款总笔
rcd	rcd	business_call_api	rcd.call.audio.down.alem	成功	您好，产线：rcd F1(下载量)=0]并
rcd	rcd	business_call_api	rcd.call.audio.down.alem	成功	您好，产线：rcd F1(下载量)=0]并

共 182 条 1 2 3 4 5 6 ... 19 >

共 18 条 1 2 >



支持HTTP和HTTPS协议

只有授权的商户才能访问绑定过的API

针对商户对接：IP、商户的白名单、黑名单机制

公私钥算法保护API接口调用和数据传输安全

请求时，客户端动态生成DES3密钥，对业务数据加密，公钥对DES3密钥加密，服务端反之操作；返回时亦反之操作。

双向MD5加盐对业务数据验签防篡改

H5请求基于动态生成的Token认证，有效期为24小时

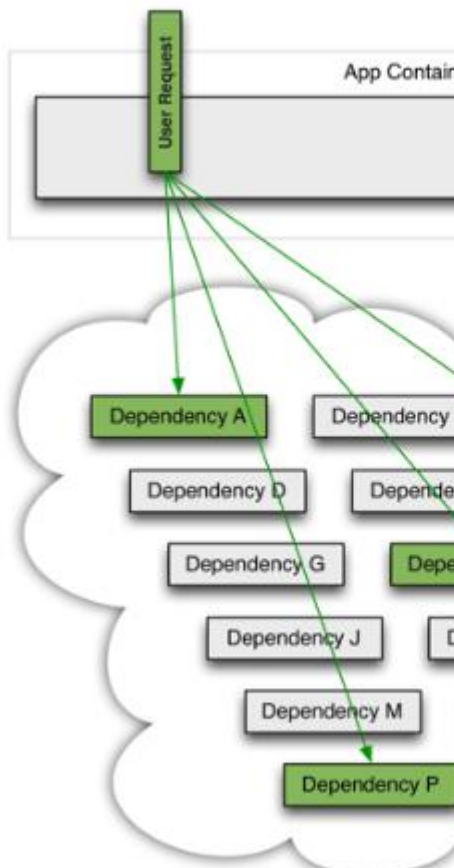
平台级限流：RateLimit，每台网关服务器控制所有业务线的流量请求。实现一个PreFilter，filterOrder为最先顺序执行，以拦截所有请求。请求拿到令牌才能后续执行，未拿到令牌直接返回网络繁忙提示，以保证现有的服务器在请求超过最大峰值时不被冲垮。

服务级限流：Hystrix，使用命令模式(继承HystrixCommand类)来实现具体的服务调用逻辑(run方法)，并在命令模式中添加了服务调用失败后的降级逻辑(getFallback)。

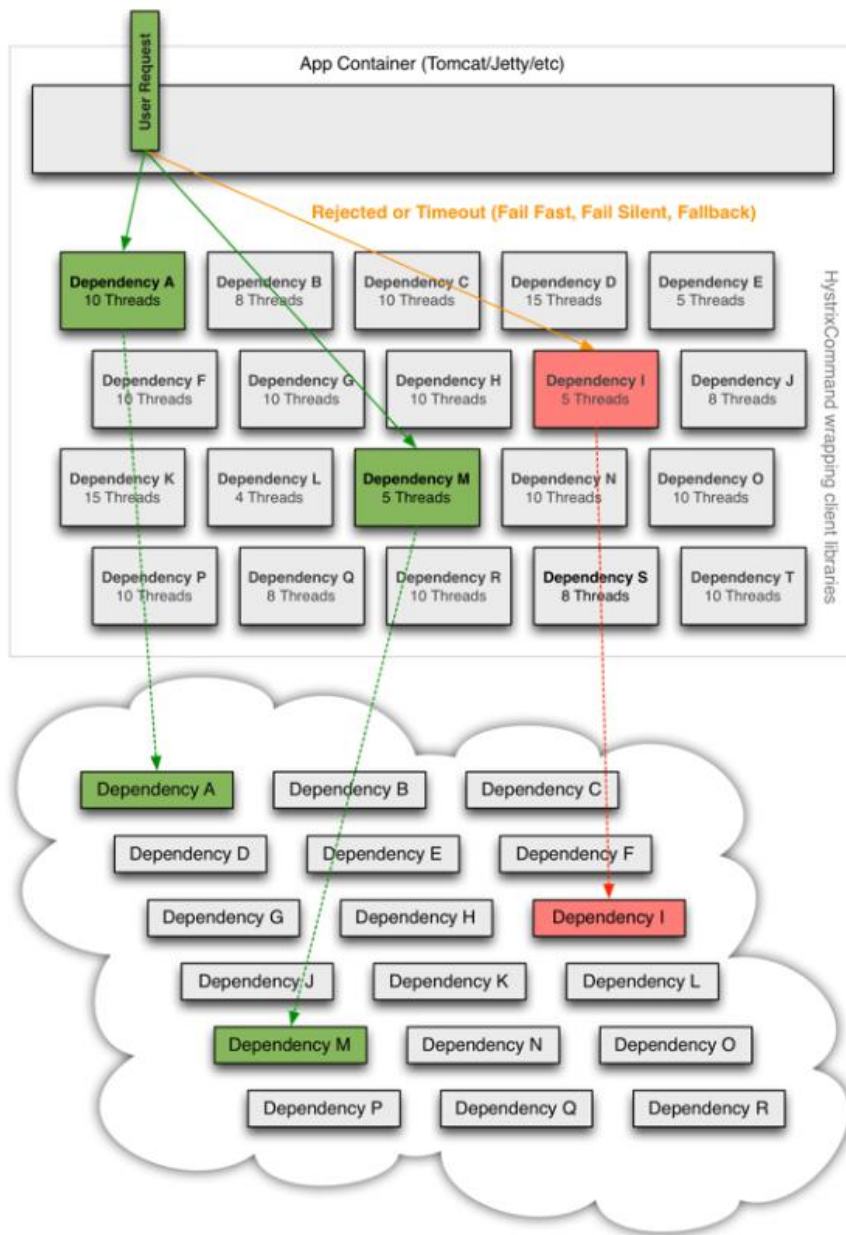
- 为什么需要Hystrix?
- 熔断器模式
- HystrixCircuitBreaker内部逻辑

为什么需要Hystrix?

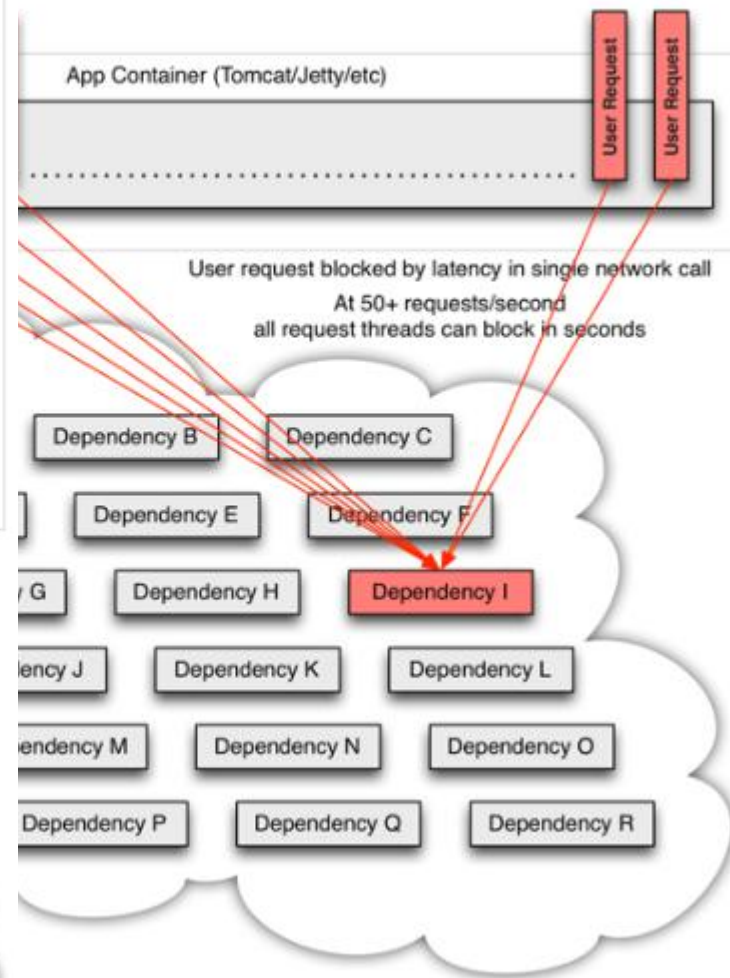
在高并发场景下，系统可能会出现资源耗尽，暂时无法处理新的请求。在大中型分布式系统中，通常系统很多依赖于下游服务，如下图所示：



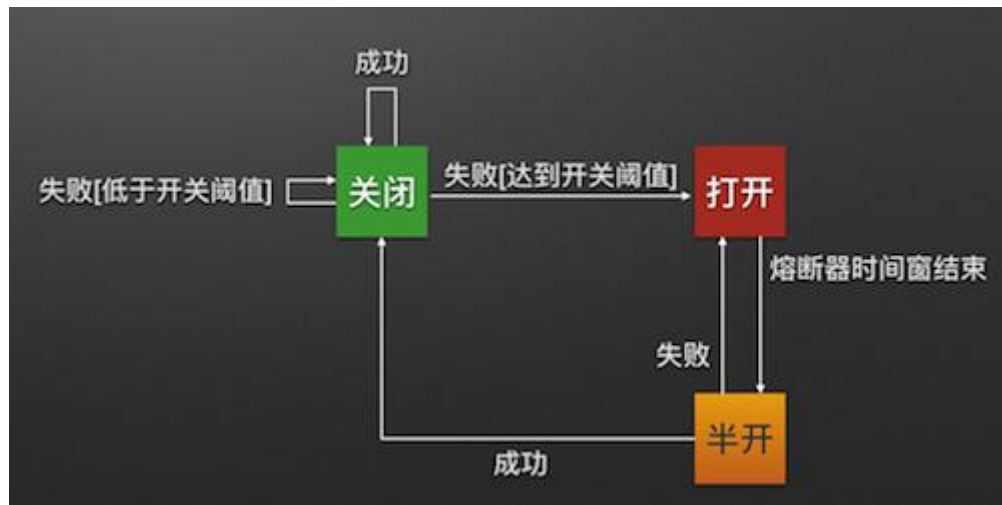
在高并发场景下，系统可能会出现资源耗尽，暂时无法处理新的请求。在大中型分布式系统中，通常系统很多依赖于下游服务，如下图所示：



当线程池出现阻塞(BLOCK)时，会影响整个线上服务的稳定性。如下图所示：



熔断器模式定义了熔断器开关相互转换的逻辑:



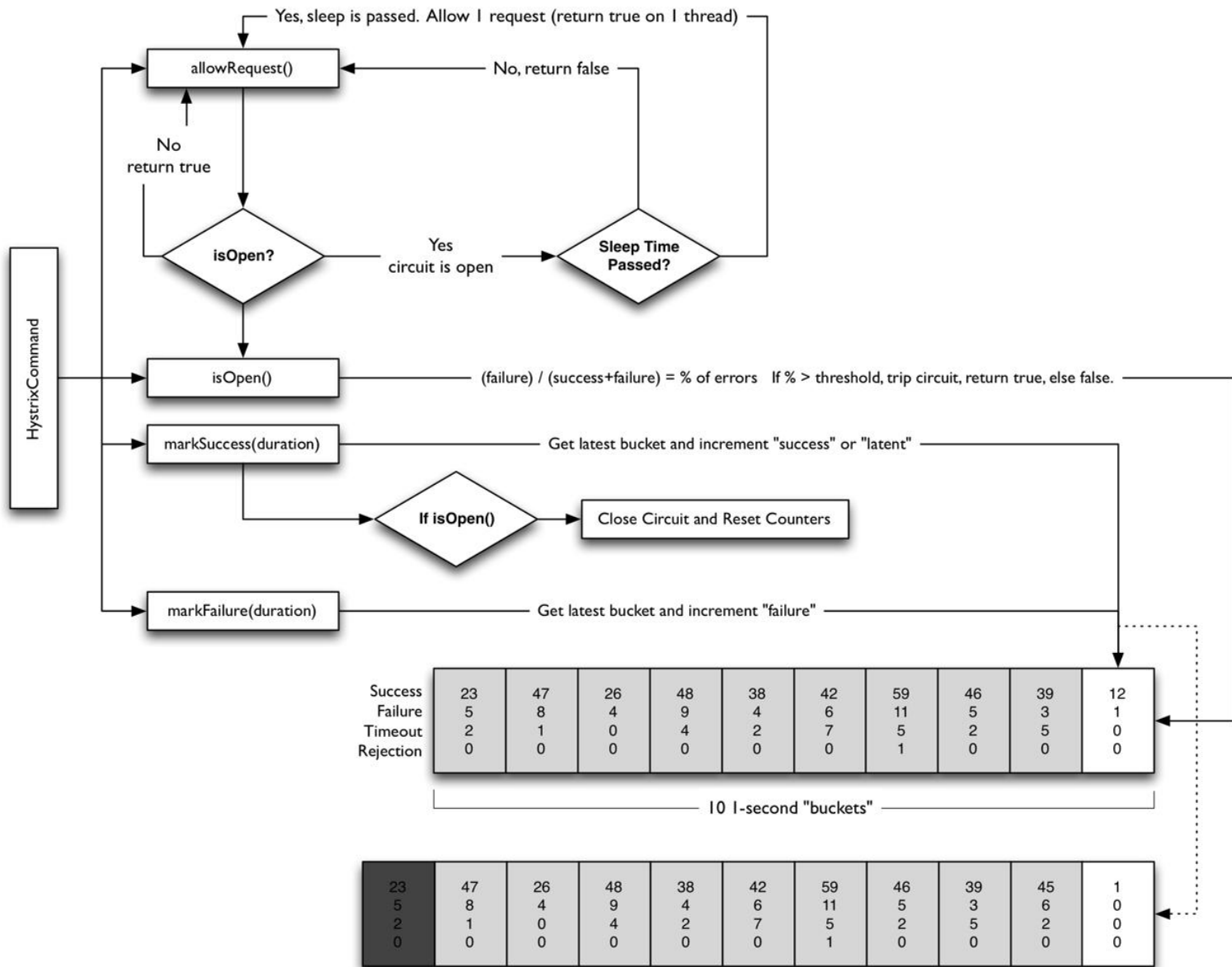
服务的健康状况 = 请求失败数 / 请求总数.

熔断器开关由关闭到打开的状态转换是通过当前服务健康状况和设定阈值比较决定的.

- ✓ 当熔断器开关关闭时, 请求被允许通过熔断器. 如果当前健康状况高于设定阈值, 开关继续保持关闭. 如果当前健康状况低于设定阈值, 开关则切换为打开状态.
- ✓ 当熔断器开关打开时, 请求被禁止通过.
- ✓ 当熔断器开关处于打开状态, 经过一段时间后, 熔断器会自动进入半开状态, 这时熔断器只允许一个请求通过. 当该请求调用成功时, 熔断器恢复到关闭状态. 若该请求失败, 熔断器继续保持打开状态, 接下来的请求被禁止通过.

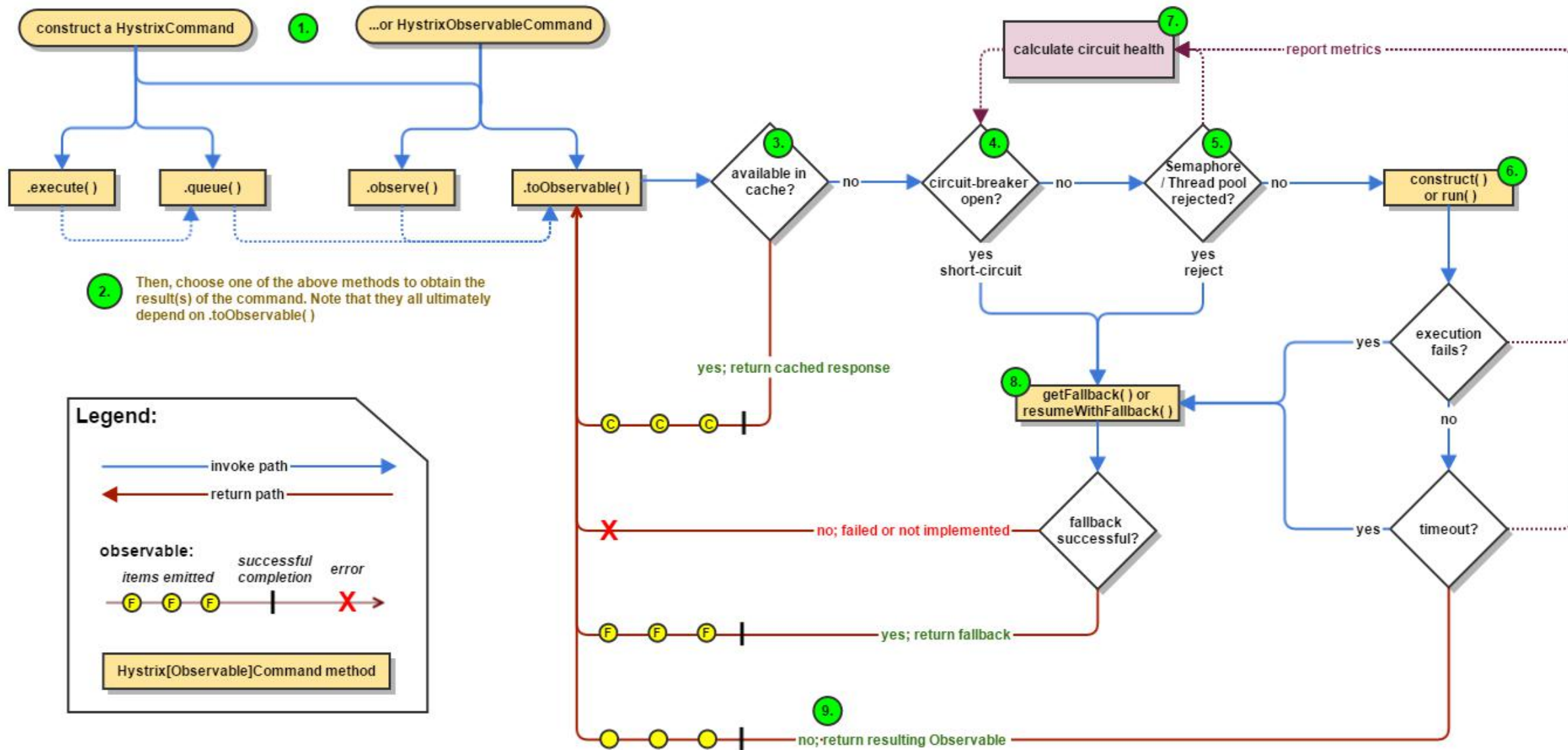
熔断器的开关能保证服务调用者在调用异常服务时, 快速返回结果, 避免大量的同步等待. 并且熔断器能在一段时间后继续侦测请求执行结果, 提供恢复服务调用的可能.

HystrixCircuitBreaker内部逻辑

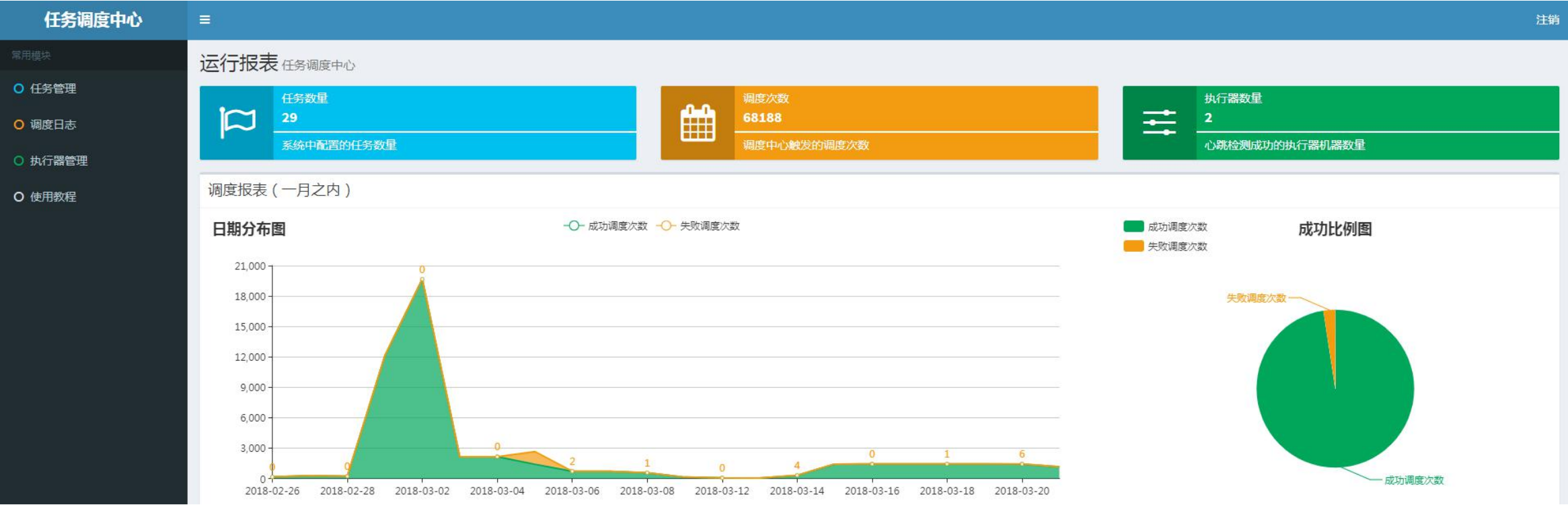


On "getLatestBucket" if the 1-second window is passed a new bucket is created, the rest slid over and the oldest one dropped.

Hystrix工作流程



实时生成RSA密钥影响性能，通过任务调度中心在凌晨时预先批量生成公私钥放在缓冲中，请求来了直接取用。



检测Headers

通过校验Headers携带的User-Agent、Referer、Host、Cookie等信息识别爬虫

统计IP或账号

每次收到请求时记录下IP、访问时间、访问次数，通过判断访问时间、访问次数和阈值大小，识别是否爬虫。
同时，判定IP与上次请求IP是否在同一区域，不在则增加验证码、人工交互等手段拦截请求。

关键数据转成图片

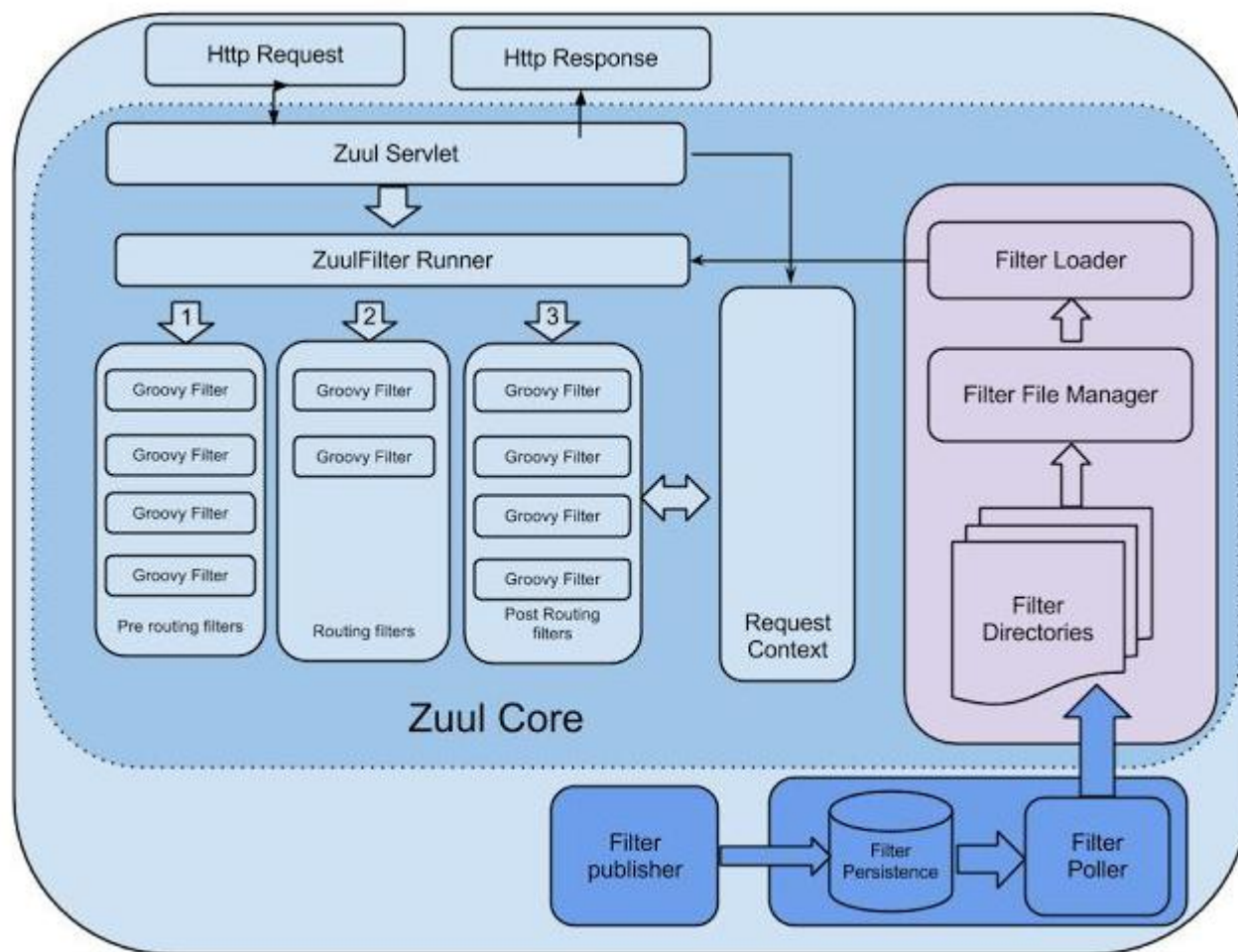
爬

反

前端JS加密混淆



Zuul的过滤器是由Groovy脚本写的，这些过滤器文件被放在Zuul Server上的特定目录下面，Zuul会定期轮询这些目录，修改过的过滤器会动态的加载到Zuul Server中以便过滤请求使用。





谢谢聆听