基于RAINBOND实现服务熔断和全局限流

好雨交付工程师–郭逊

大纲

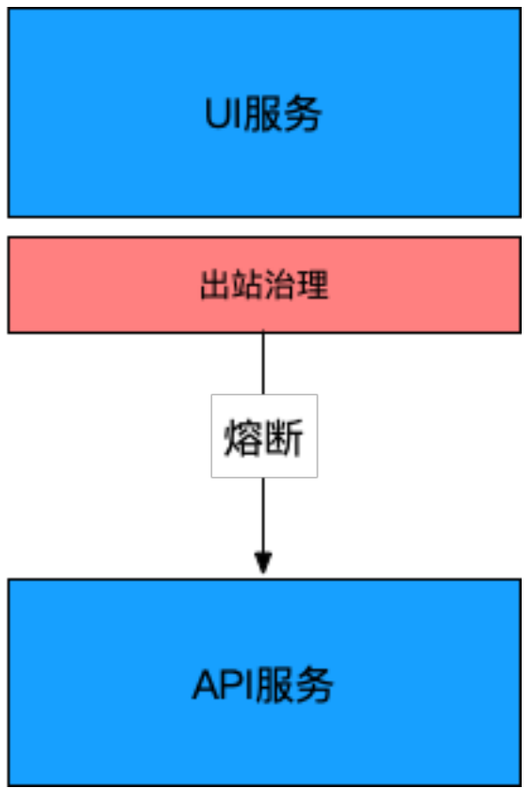
1.网络治理插件

2.实现服务熔断

3.实现全局限流

1.网络治理插件

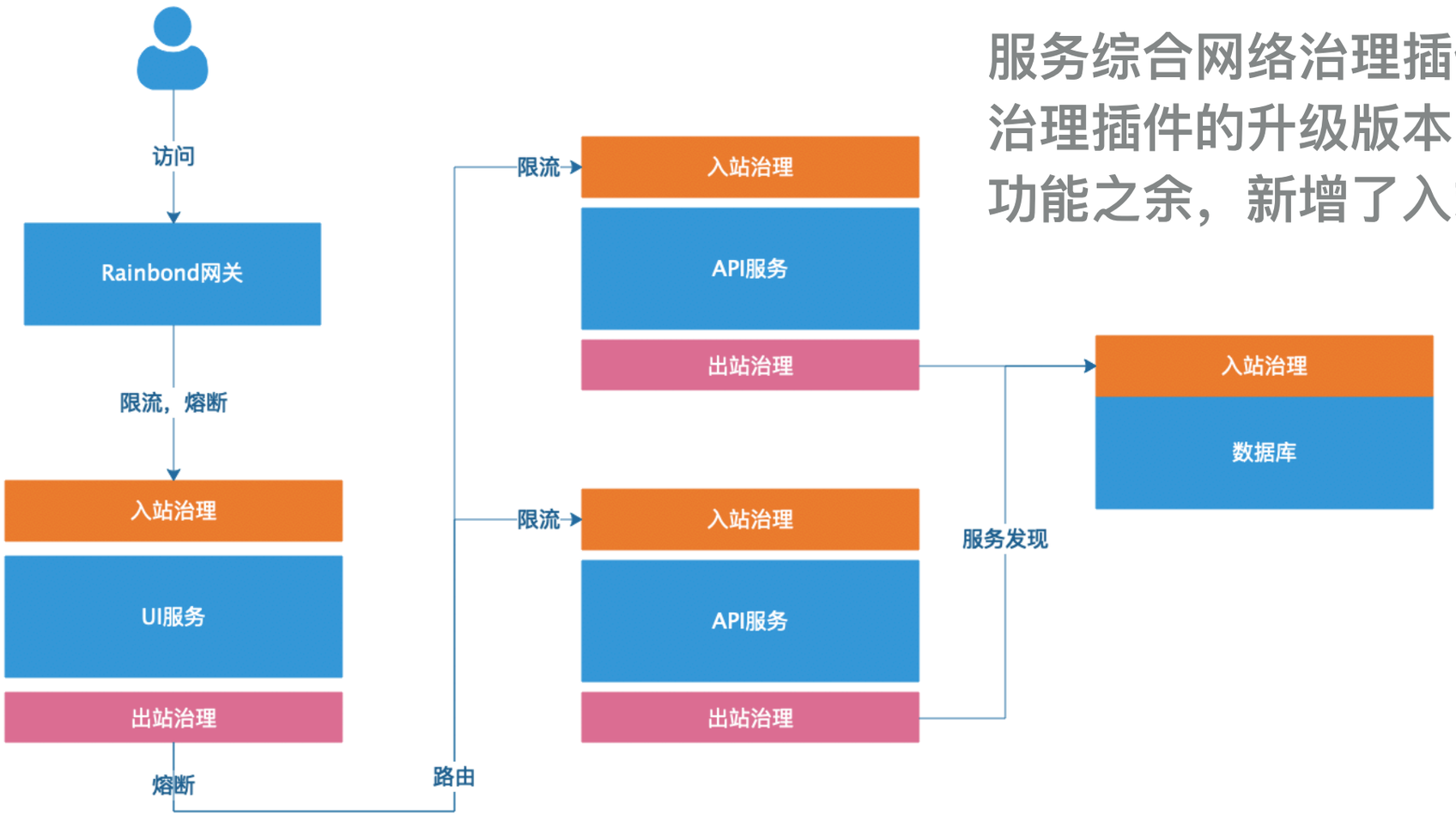
1.1 服务网络治理插件——出站治理



UI服务安装了服务网络治理插件，该插件作用于流量的出口，即通向API服务的一端。出站治理插件会接手管理流向API服务的流量，并可以配置条件，实现熔断。

1.网络治理插件

1.2 服务综合网络治理插件——出入站共治



服务综合网络治理插件，是出站治理插件的升级版本。兼容原有功能之余，新增了入站治理功能。

2.实现服务熔断

服务熔断，是一种保护下游服务（UI服务）的机制。

当来自UI的请求堆积于上游服务（API服务），超越了API服务的处理能力的时候。熔断机制会发生作用，让UI服务去请求其他可用的API服务。总之不要在已经被熔断的API服务这里等待回应。

这样做，可以避免UI服务中其他进程，因为请求API服务没有响应，而发生堆积，最终撑爆UI服务本身。

服务熔断只作用于指定的下游服务。

关键参数：

- MaxConnections 最大连接数，Http协议时仅适用于http1.1，TCP协议时设置最大TCP连接数。
- MaxRequests 并发请求数，适用于HTTP协议
- MaxPendingRequests 最大等待请求数，适用于HTTP协议
- MaxActiveRetries 最大重试次数，适用于HTTP协议
- MaxRequestsPerConnection 单连接最大请求数，适用于HTTP协议，支持http1.1 和http2

2.实现服务熔断

实例演示

3.实现全局限流

全局限流，是一种保护上游服务（API服务）的机制。

当来自UI服务的请求，超越API服务的处理能力。

限流机制会发生作用，全局限流可以对访问到API服务的所有流量进行限制。

这样做，可以保证进入到API服务的流量始终保持一个合适的值，防止了API服务因为请求过量而被撑爆。

限流时可以用IP作为限流条件，从而实现黑/白名单功能。

需要借助第三方服务实现。

关键参数：

- OPEN_LIMIT 开启全局限流功能，全局限流功能依赖于第三方的限流服务，比如ratelimit, 当前服务需要依赖ratelimit服务，并设置RATE_LIMIT_SERVER_HOST和RATE_LIMIT_SERVER_PORT环境变量。
- LIMIT_DOMAIN 限流链路的domain key,与全局限流服务的配置对应

3.实现全局限流

实例演示

我是郭逊，
好雨交付工程师，
我为交付质量代言😄

好雨交付工程师–郭逊