第二届 eBPF开发者大会
www.ebpftravel.com

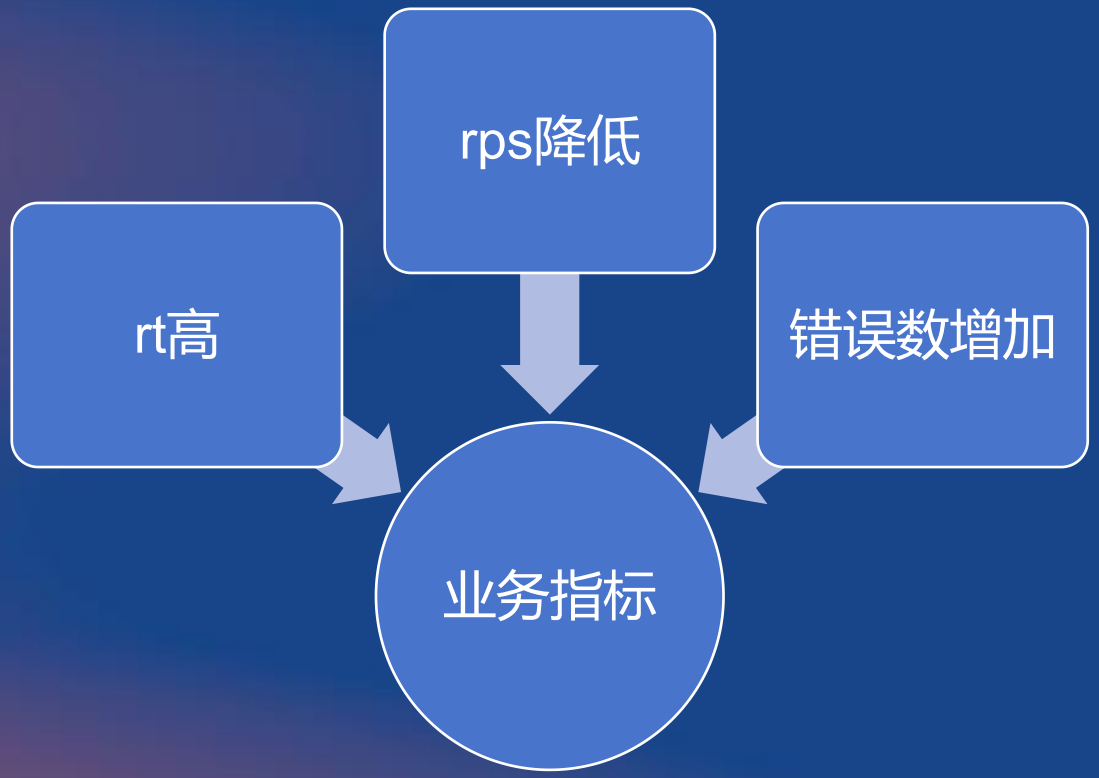
sysom:基于eBPF的网络抖动诊断

程书意
龙蜥社区eBPF技术探索sig maintainer

中国·西安

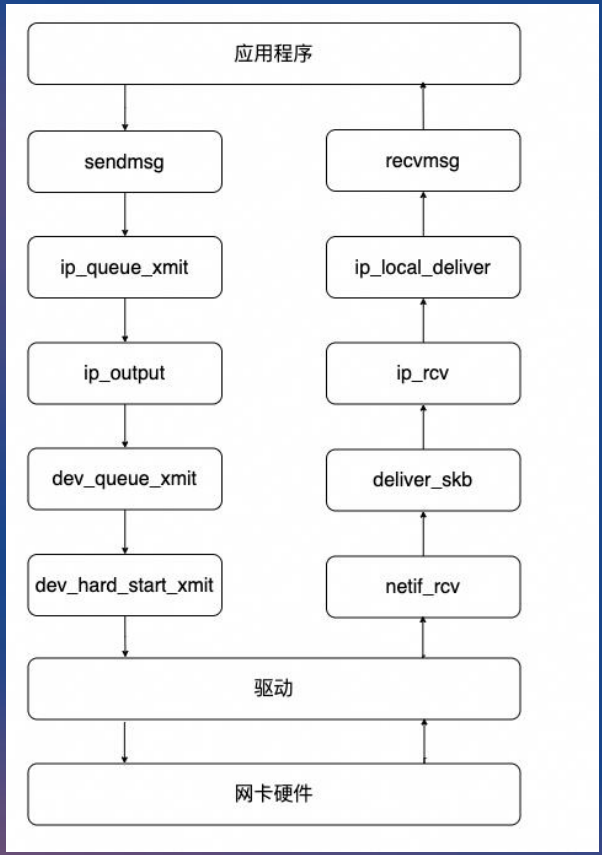
1. 什么是网络抖动?

1.1 业务视角看网络抖动



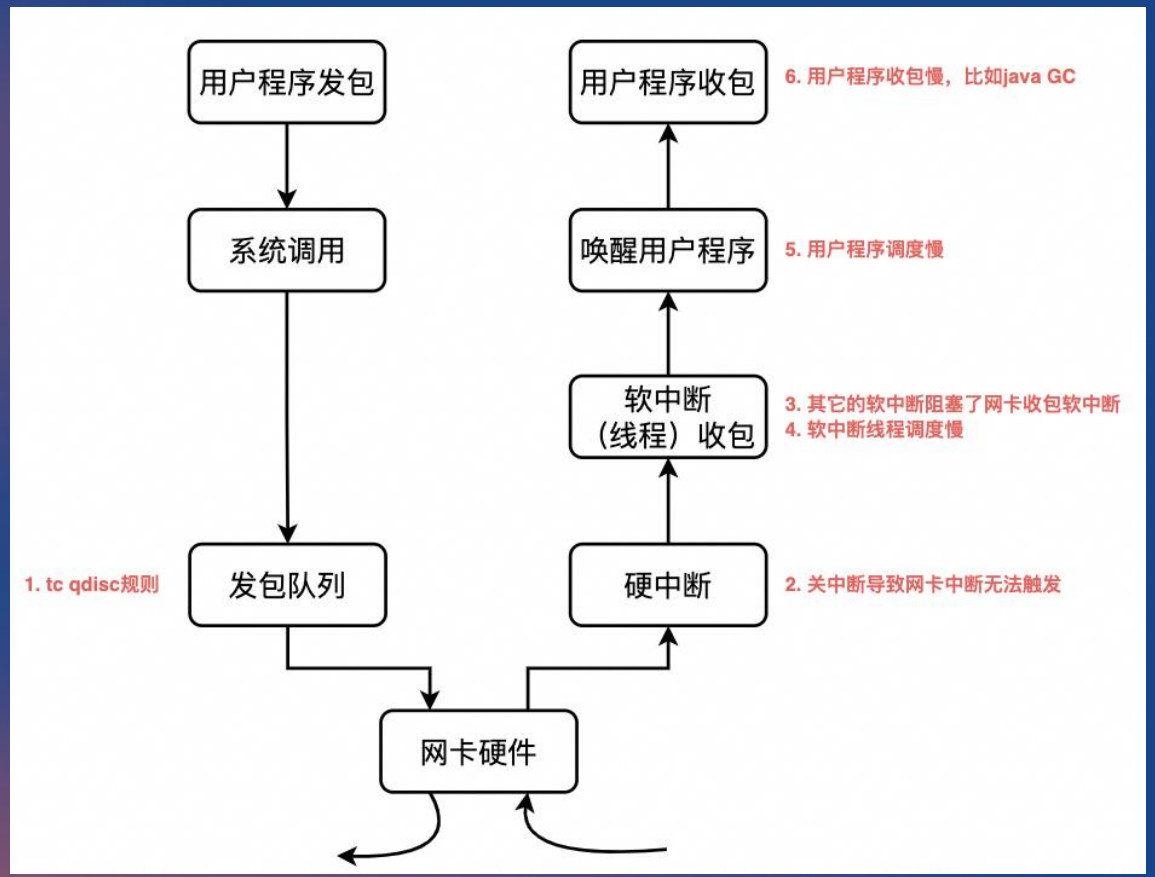
为什么抖动呢?

1.2 内核视角看网络抖动



能够知道抖在哪，仍不知道为什么抖?

1.2 内核视角看网络抖动



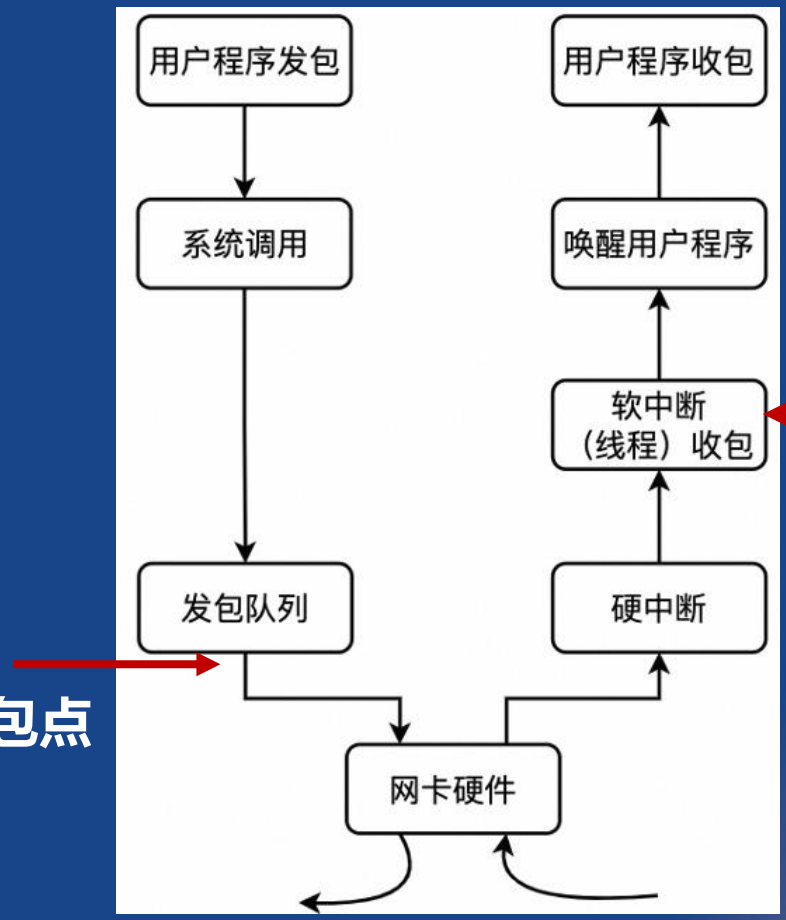
网络抖动根因

- 队列慢
- 关中断
- 软中断慢
- 调度慢
- 用户程序收包慢

2. 网络抖动常见定位手段

2.1 tcpdump & wireshark

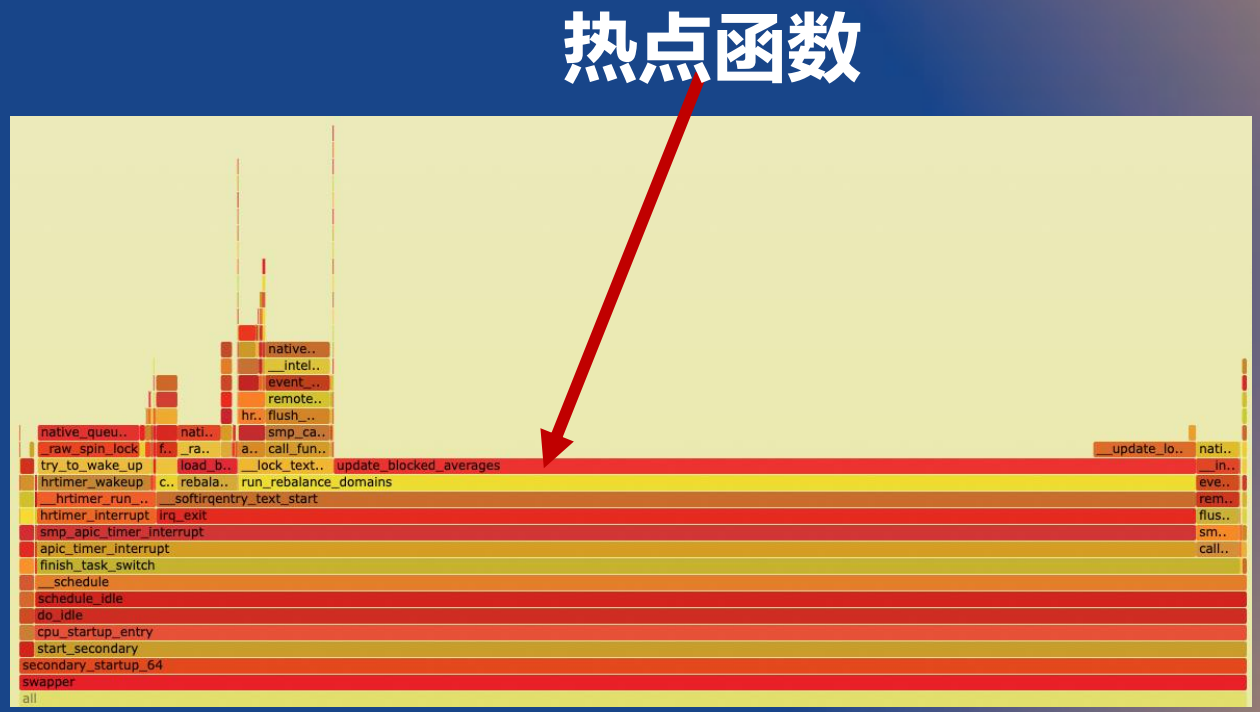
1. 分析丢包、重传
2. 分析链路时延，会存在偏差



2.2 perf分析

关中断、软中断慢会引起热点，
可以通过perf进行热点分析

缺陷：网络抖动到热点分析跨度比较大，过于依赖问题的排查人员的专业程度



2.3 ftrace

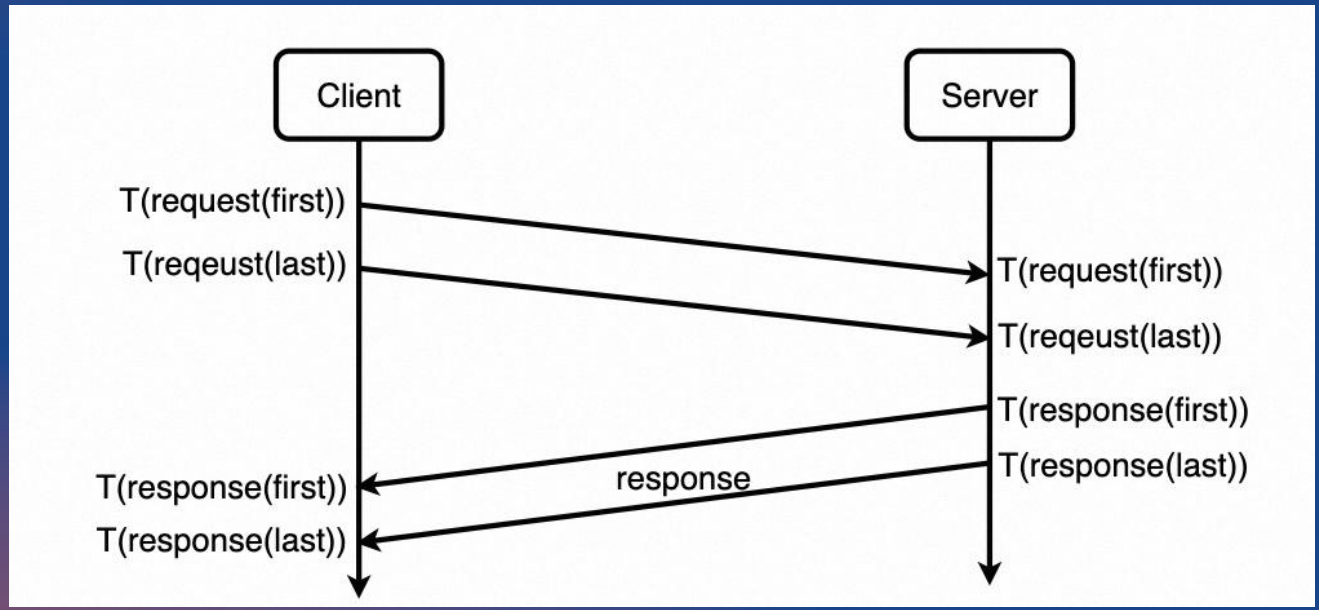
1. 软中断慢：tracepoint:irq:softirq_raise和tracepoint:irq:softirq_entry
2. 用户收包慢：tracepoint:tcp:tcp_probe和tracepoint:tcp:tcp_rcv_space_adjust

缺陷：会吐出大量的数据到trace_pipe，性能差

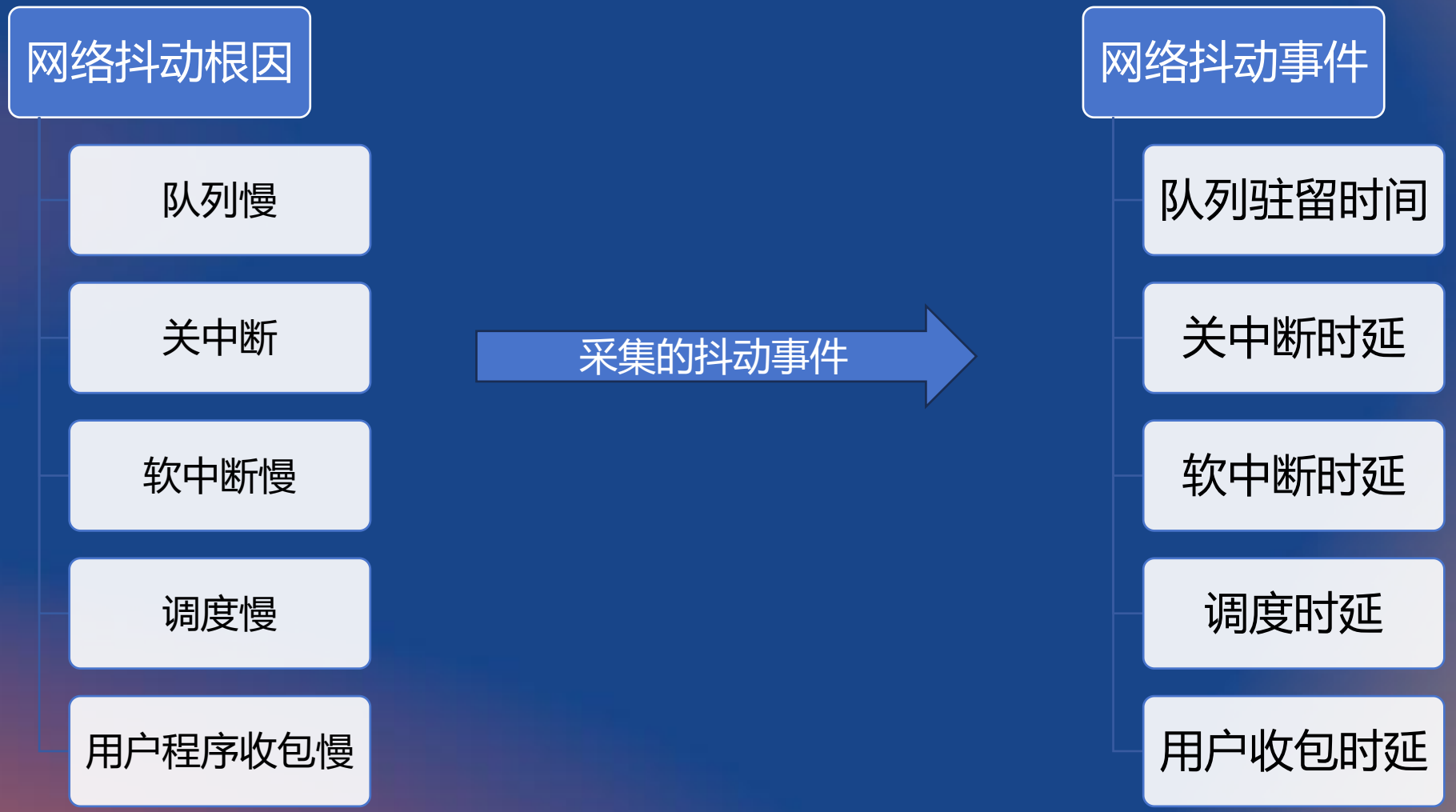
3. 基于eBPF的网络抖动诊断方法

3.1 定位抖动连接及时间点

1. eBPF打点：tcp_sendmsg和tcp_recvmsg
2. 计算时延：T(response(last)) – T(request(first))
3. 时延超过阈值时，输出时间戳和五元组信息

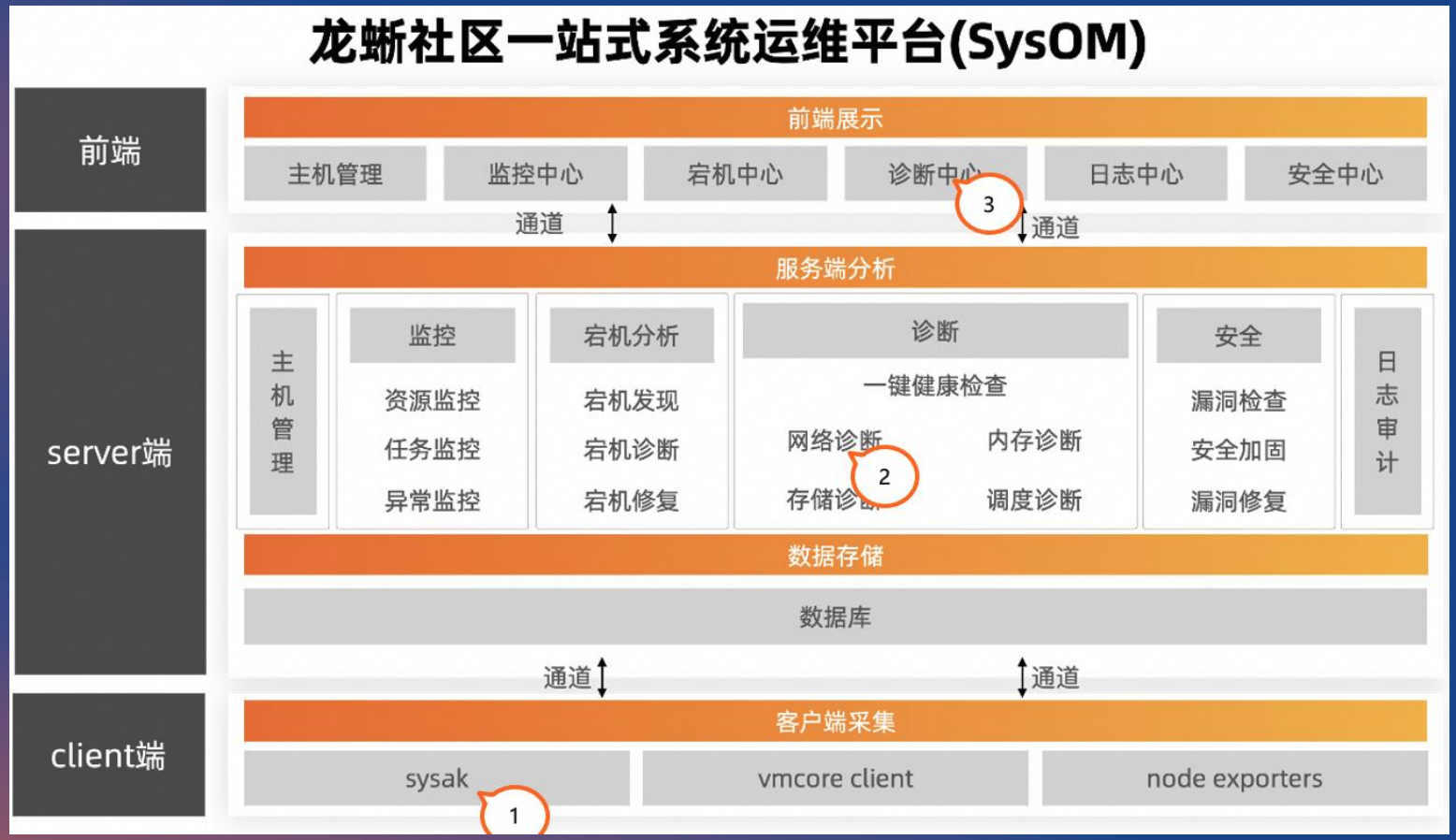


3.2 抖动事件采集


网络抖动根因
队列慢
关中断
软中断慢
调度慢
用户程序收包慢
采集的抖动事件
网络抖动事件
队列驻留时间
关中断时延
软中断时延
调度时延
用户收包时延

3.3 抖动检测与分析

3.4 sysom整体方案



1. sysak: 诊断工具集
2. 服务端分析：网络诊断
3. 前端展示

欢迎关注“酷玩BPF”公众号
一起来探索eBPF技术