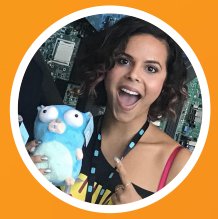
云原生时代下全场景服务流量治理

×



iyacontrol

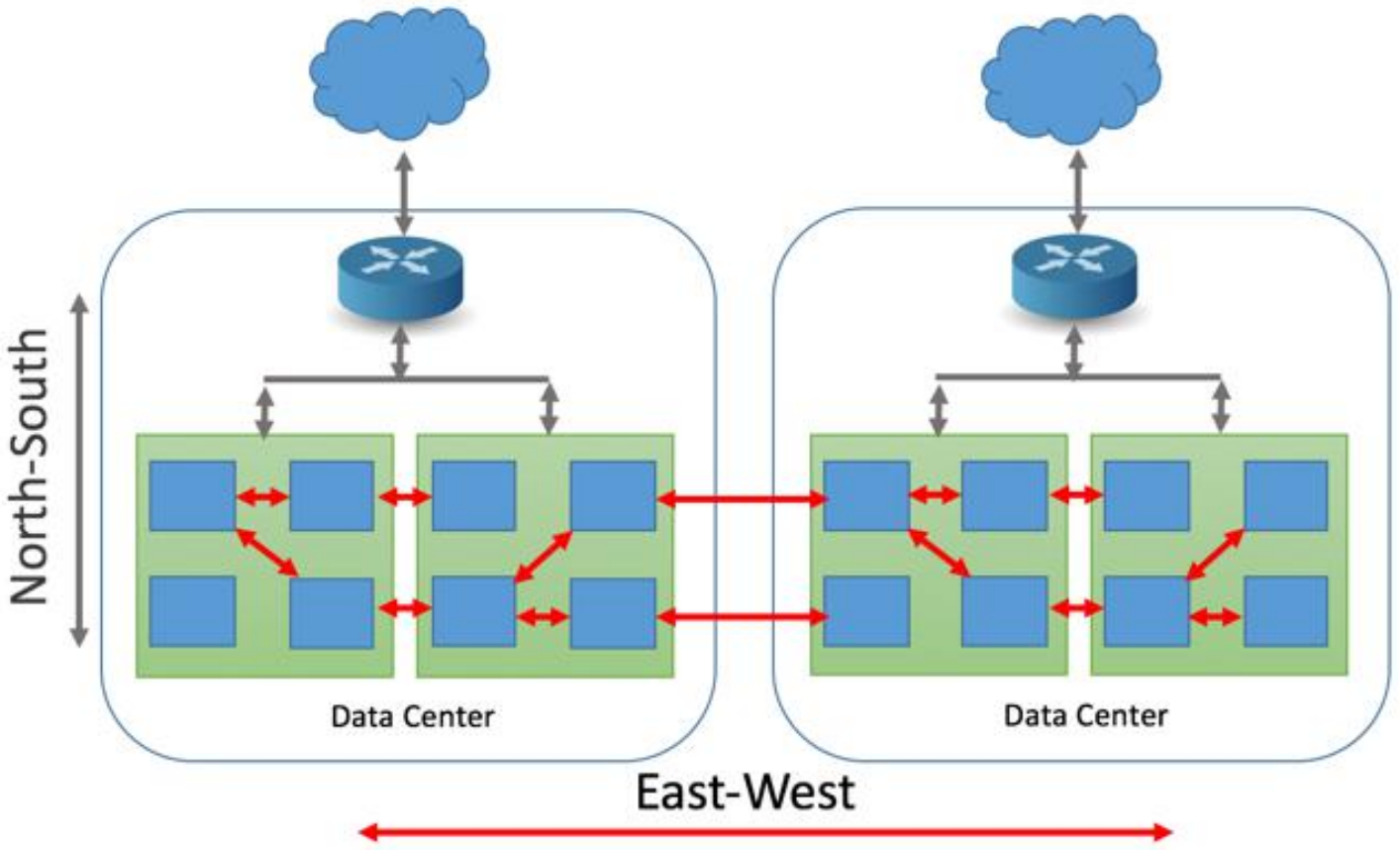
SHAREit 云原生负责人

目录

第一部分

南北向服务流量治理

南北向和东西向流量的定义



统一流量网格解决了哪些问题？

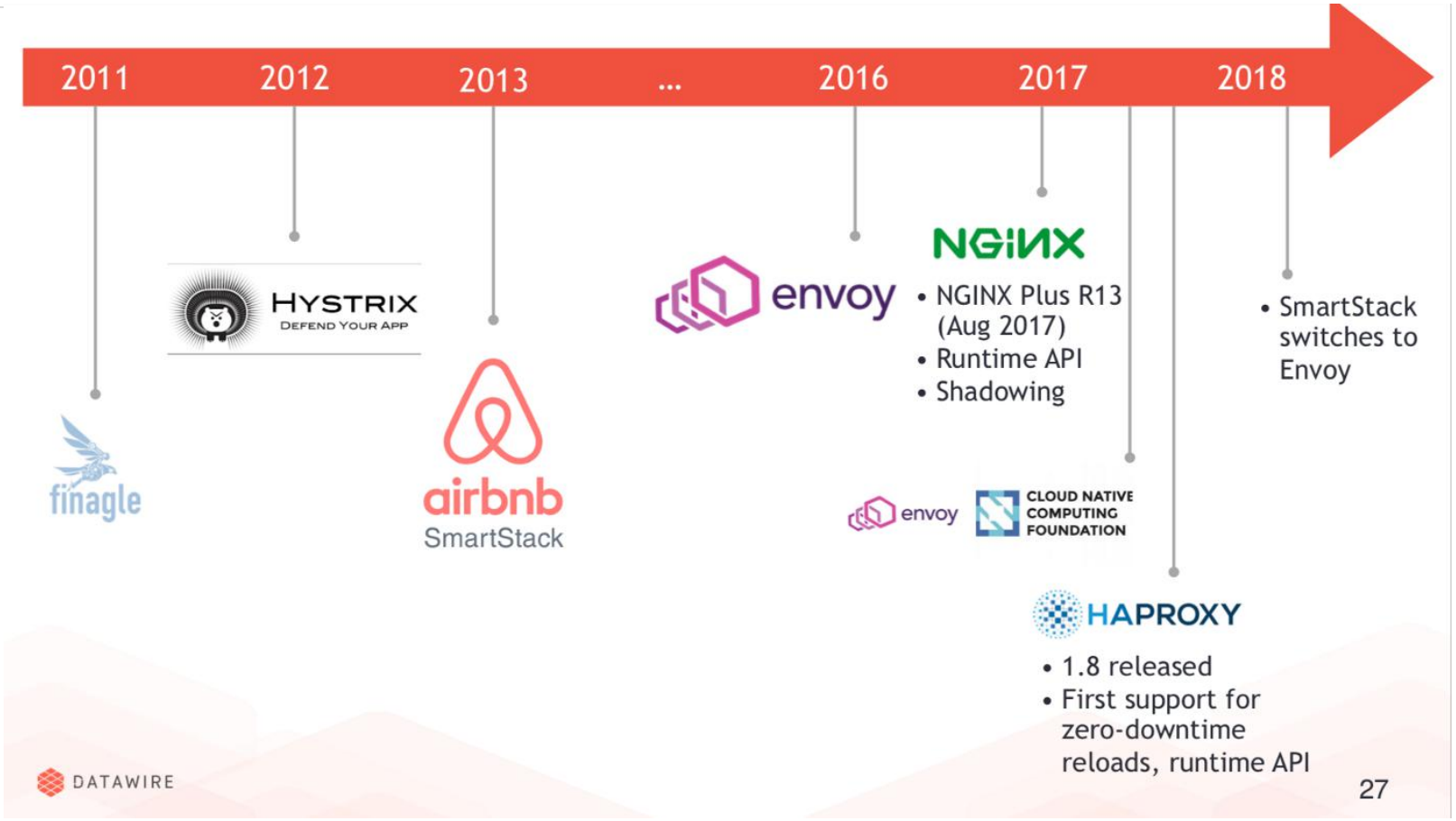
一：公有云7层LB存在的痛点

1．多云场景下，各家LB差异性增加了迁移的难度
2．不支持gRPC协议
3．无法定制开发一些特殊功能，比如部分历史遗留接口需要返回固定返回值，由网关返回无需后端实现，区域感知路由，慢启动

二：Kubernetes Ingress 存在的痛点

1．Ingress 属于命名空间的资源，无法做到跨命名空间，跨集群转发流量
2．不同集群、命名空间对于同一个域名证书需要多次配置，影响效率。而且在证书到期的时候，替换新的证书复杂且容易遗漏
3．Ingress支持功能有限，不支持熔断和限流等功能

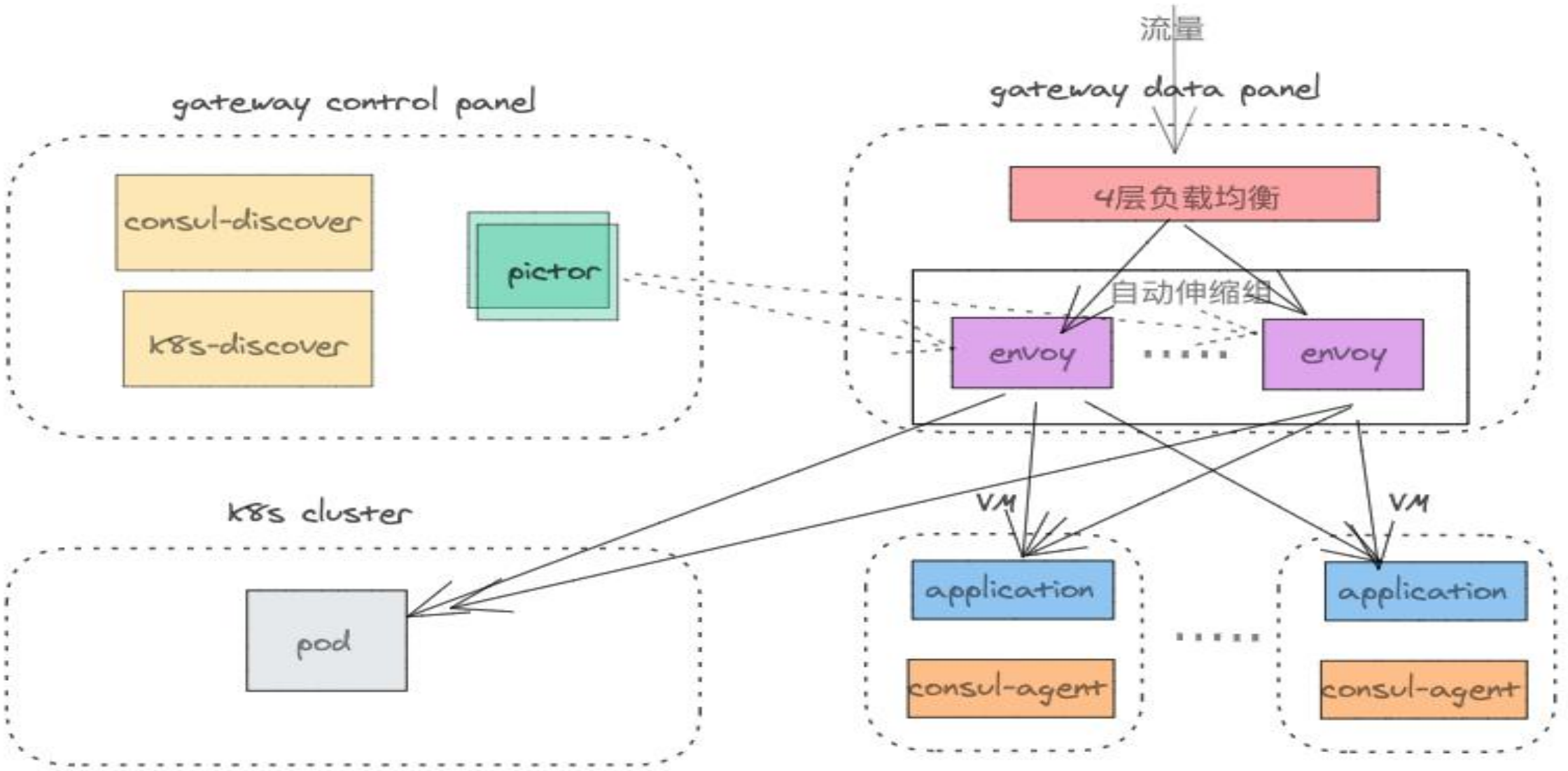
为什么选择Envoy作为数据面？



一：Envoy 技术特征：1）接口化与API 2）动态性 3）扩展性 4）可观测性 5）现代性

二：Envoy 已经成为Service Mesh解决方案数据面事实上的标准。选择同一个数据面可以带来诸多好处：1）网关上积累的经验可以无缝切换到Service Mesh 2）一套可观察性方案可以同时满足网关和Service Mesh。

架构


流量
gateway control panel
gateway data panel
consul-discover
k8s-discover
pictor
4层负载均衡
自动伸缩组
envoy
envoy
k8s cluster
pod
VM
VM
application
application
consul-agent
consul-agent

第二部分

东西向服务流量治理

服务治理框架选型--SDK or Sidecar?

背景：

1．多语言：Java，c++，golang，python等
2．容器化程度比较高，除部分中间件外，其余业务均已容器化
3．随着业务急速发展，急需一个服务治理框架

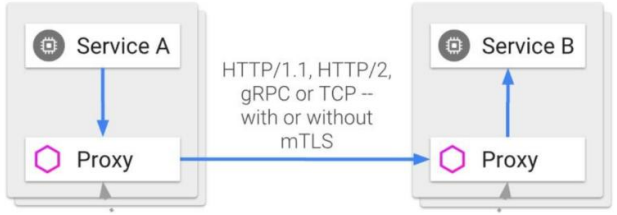
Spring Cloud

优势：

1：提供了完善的服务治理功能
2：生产环境被大量应用

劣势：

1：与Java平台紧密耦合
2：侵入式



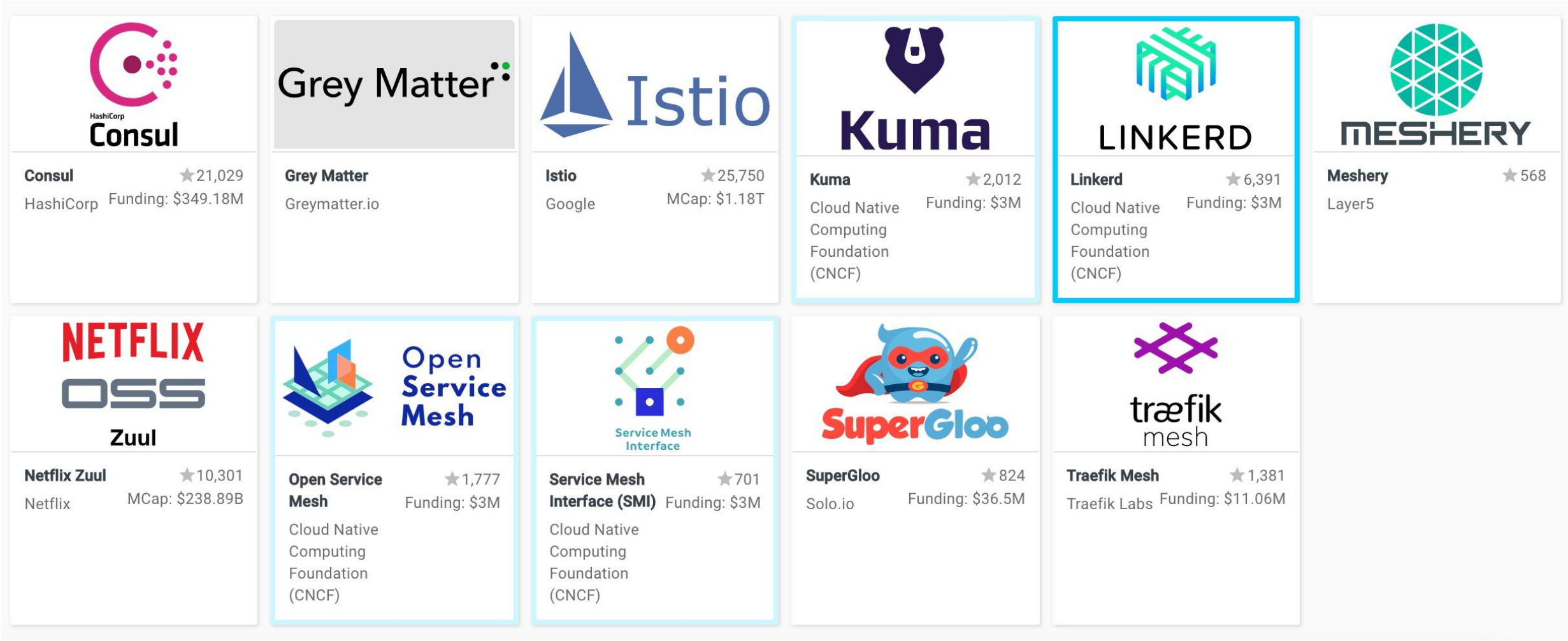
优势：

1：社区活跃，更加云原生
2：松耦合，非侵入式

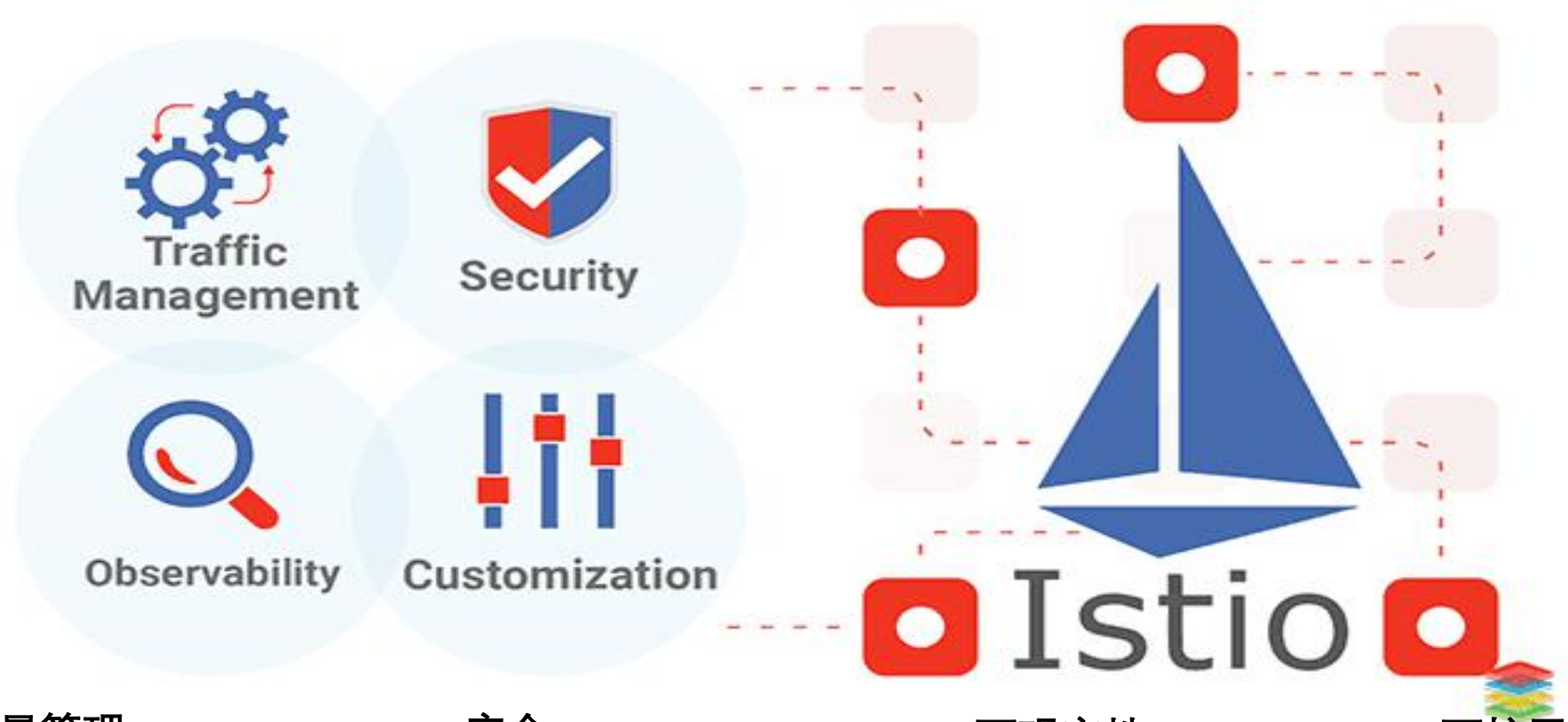
劣势：

1：新技术，生产环境应用相对较少
2：Sidecar 引入带来的延迟增加

百家争鸣的Service Mesh



Istio--服务网格解决方案事实上的标准



流量管理

1. 请求路由
2. 故障注入
3. 超时和重试
4. 熔断
5. 流量镜像

安全

1. 认证
2. 鉴权
3. mTLS

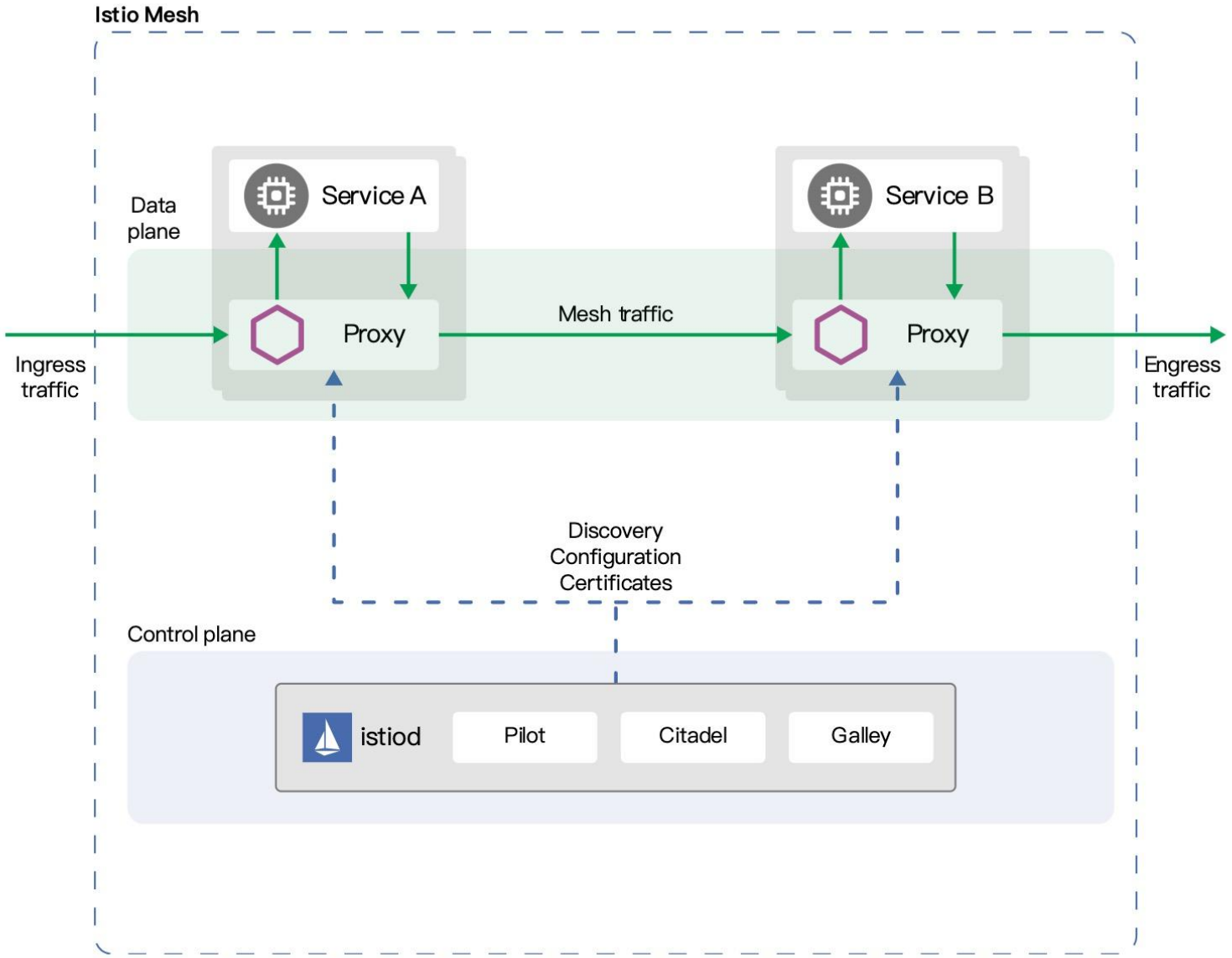
可观察性

1. 日志
2. metrcis
3. trace

可扩展性

1. wasm

选择哪个版本的Istio？



Istio 架构

Istio V1.15+变化：

1：控制面回归单体，降低安装复杂度、增加控制面可运维性
2：正视性能问题，摒弃Mixer

落地Istio的思考

1: 没有能搞定一切的银弹

2: 专注于实际场景，做减法

3: 小版本升级

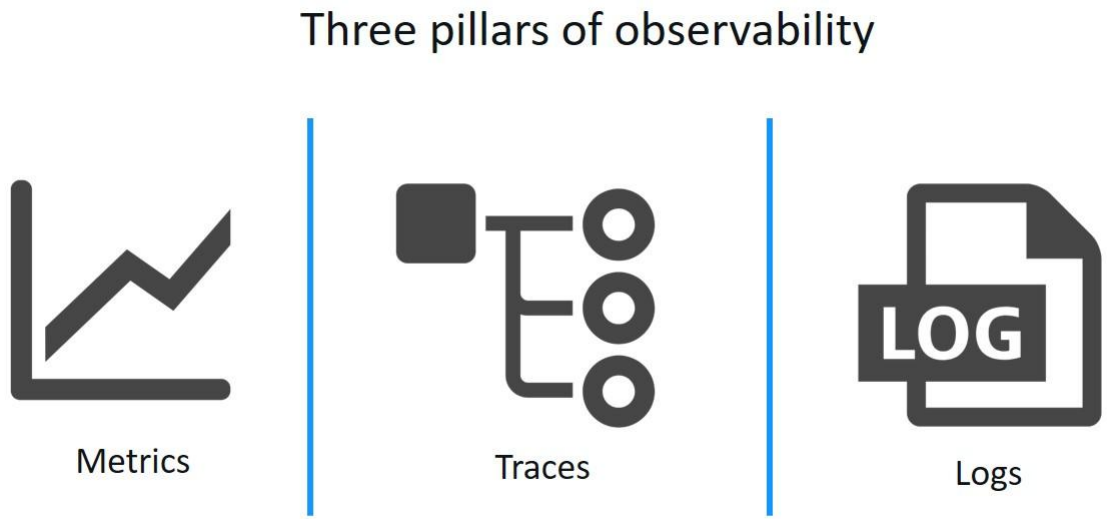
4: 数据面和控制面全面优化

5: 二次抽象，产品化

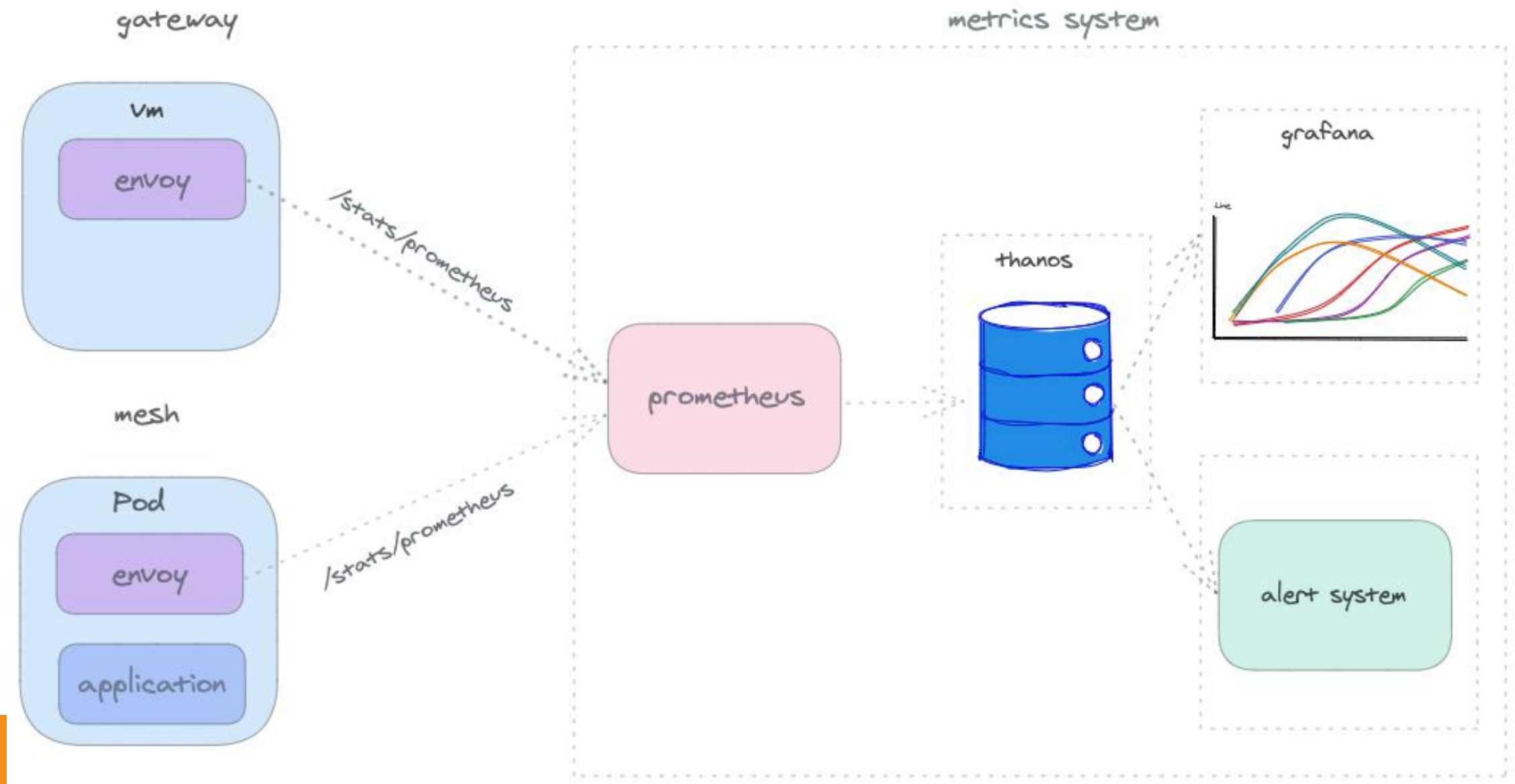
第三部分

如何实现服务流量的可观察性

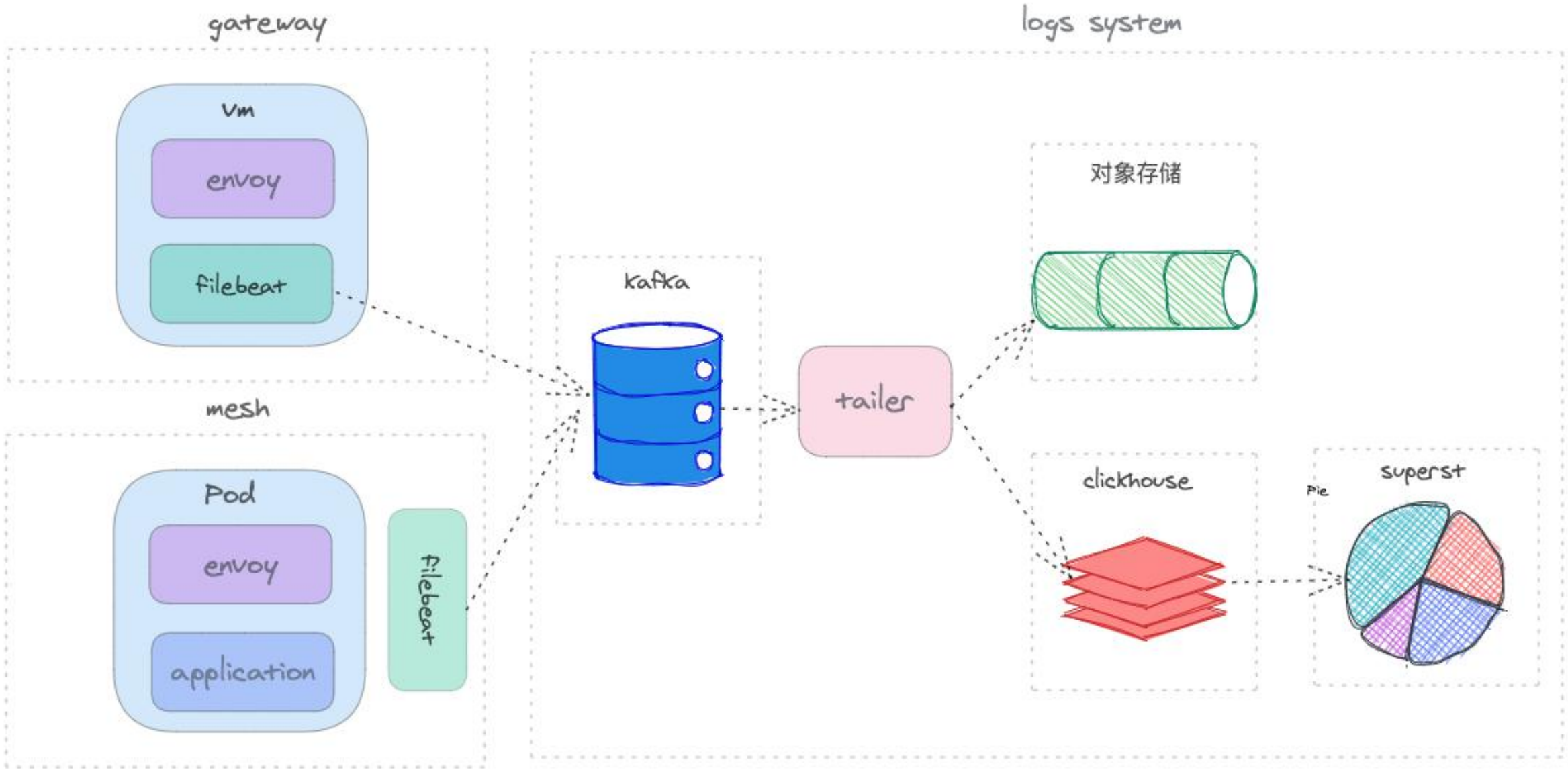
为什么可观察性很重要？



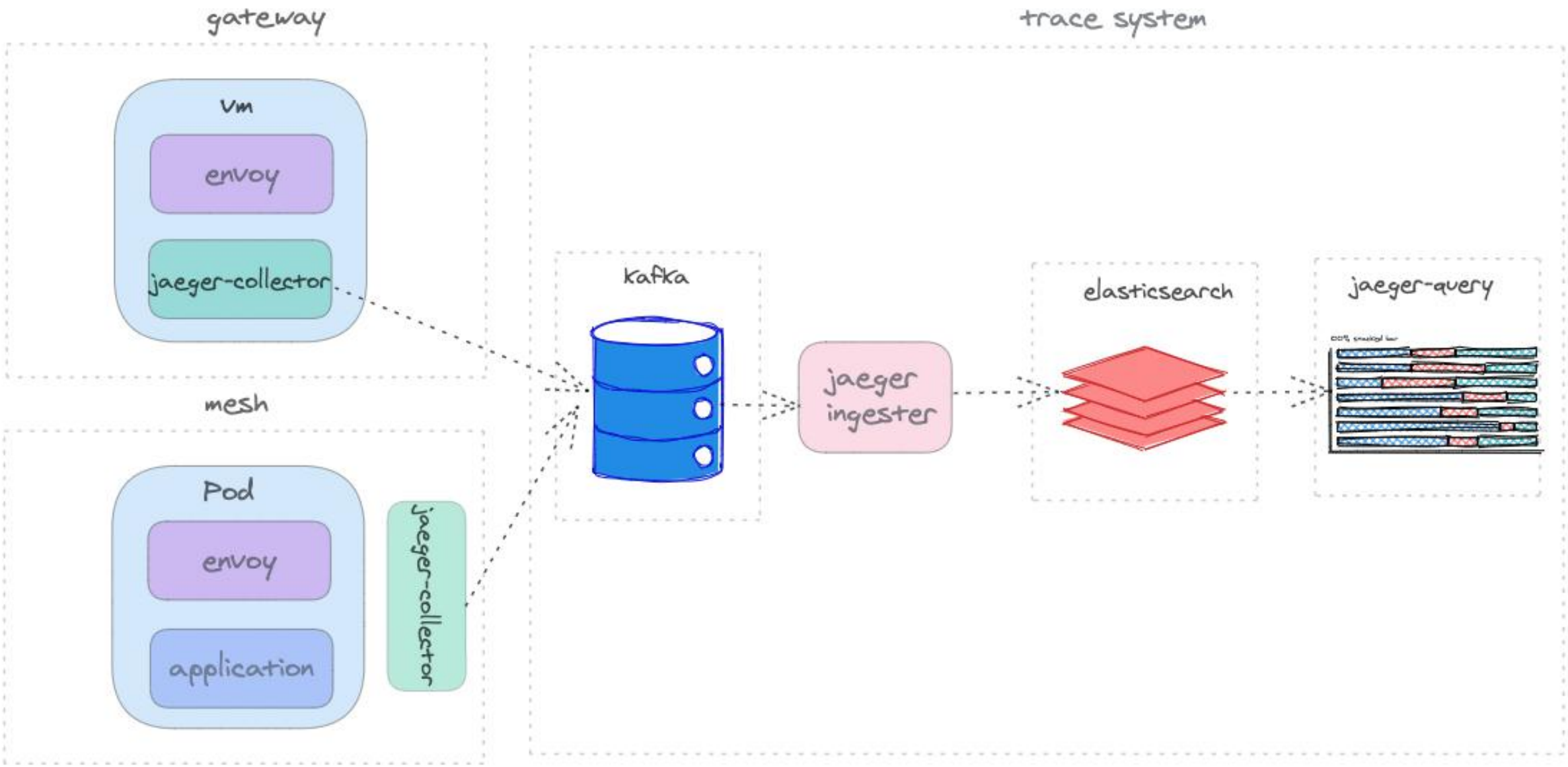
Metrcis


gateway
metrics system
vm
envoy
/stats/prometheus
grafana
thanos
prometheus
mesh
Pod
envoy
application
/stats/prometheus
alert system

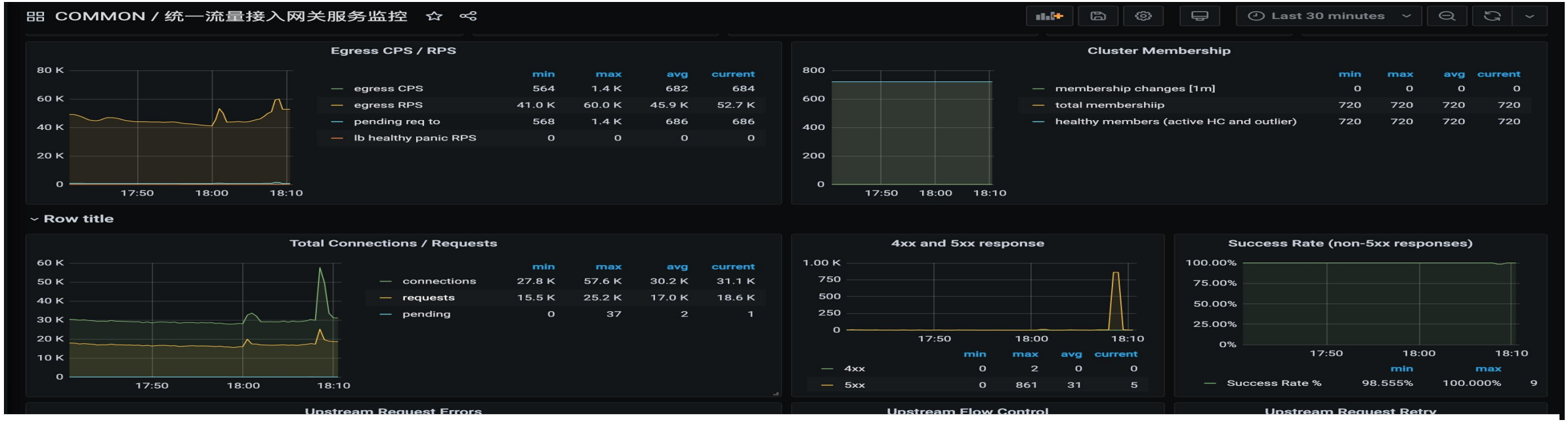
Log

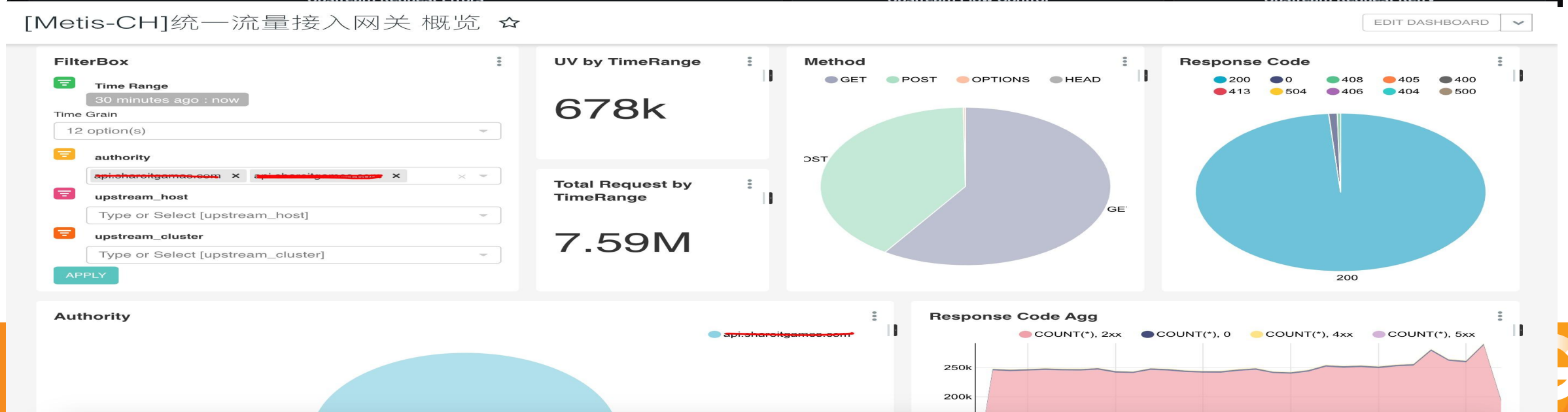

gateway
logs system
vm
envoy
filebeat
mesh
Pod
envoy
application
filebeat
kafka
tailer
对象存储
clickhouse
superst
Pie

Tracing


gateway
trace system
vm
envoy
jaeger-collector
kafka
elasticsearch
jaeger-query
jaeger
ingester
mesh
Pod
envoy
application
jaeger-collector

实际效果


COMMON / 统一流量接入网关服务监控
Last 30 minutes
Egress CPS / RPS
egress CPS 564 1.4 K 682 684
egress RPS 41.0 K 60.0 K 45.9 K 52.7 K
pending req to 568 1.4 K 686 686
lb healthy panic RPS 0 0 0 0
Cluster Membership
membership changes [1m] 0 0 0 0
total membershiip 720 720 720 720
healthy members (active HC and outlier) 720 720 720 720
Row title
Total Connections / Requests
connections 27.8 K 57.6 K 30.2 K 31.1 K
requests 15.5 K 25.2 K 17.0 K 18.6 K
pending 0 37 2 1
4xx and 5xx response
4xx 0 2 0 0
5xx 0 861 31 5
Success Rate (non-5xx responses)
Success Rate % 98.555% 100.000% 9
Upstream Request Errors
Upstream Flow Control
Upstream Request Retry


[Metis-CH]统一流量接入网关 概览
EDIT DASHBOARD
FilterBox
Time Range
30 minutes ago : now
Time Grain
12 option(s)
authority
upstream_host
Type or Select [upstream_host]
upstream_cluster
Type or Select [upstream_cluster]
APPLY
UV by TimeRange
678k
Total Request by TimeRange
7.59M
Method
GET POST OPTIONS HEAD
Response Code
200 0 408 405 400
413 504 406 404 500
Authority
Response Code Agg
COUNT(*), 2xx COUNT(*), 0 COUNT(*), 4xx COUNT(*), 5xx
250k
200k

感谢！