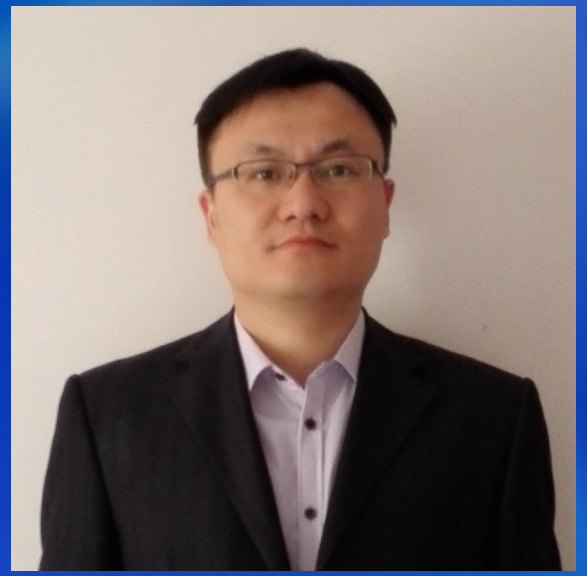
KUBERNETES
COMMUNITY DAYS DALIAN

阿里云服务网格在多集群企业应用中的实践经验分享

王夕宁@阿里云

云原生服务网格负责人

KUBERNETES
COMMUNITY DAYS DALIAN



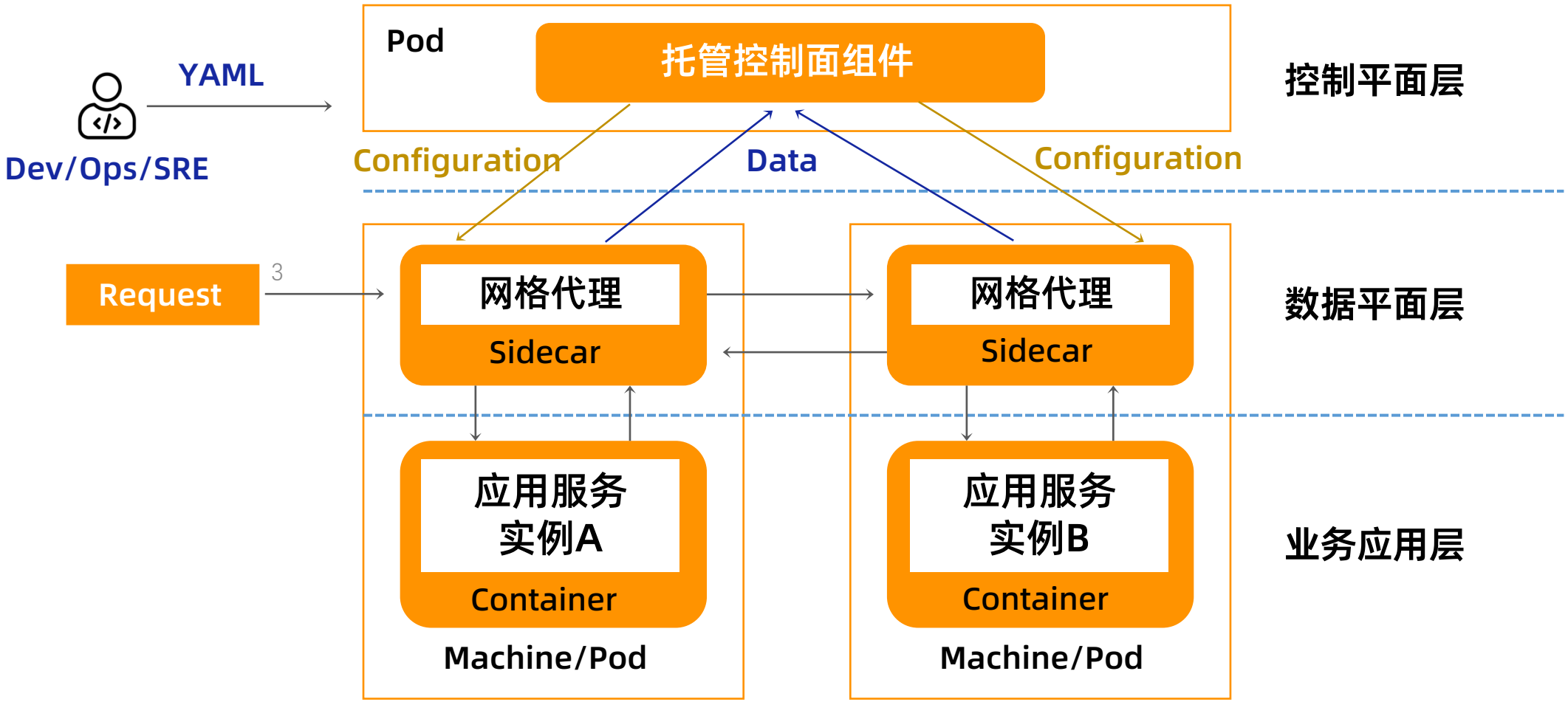
自我介绍
Personal Basic Information

阿里云服务网格技术负责人, 专注Kubernetes/云原生/服务网格等领域；曾在IBM中国开发中心工作, 作为架构师和主要开发人员负责或参与了一系列在SOA中间件、云计算等领域的工作,；曾担任中国研发中心专利技术评审主席, 并拥有70多项相关领域的国际技术专利。

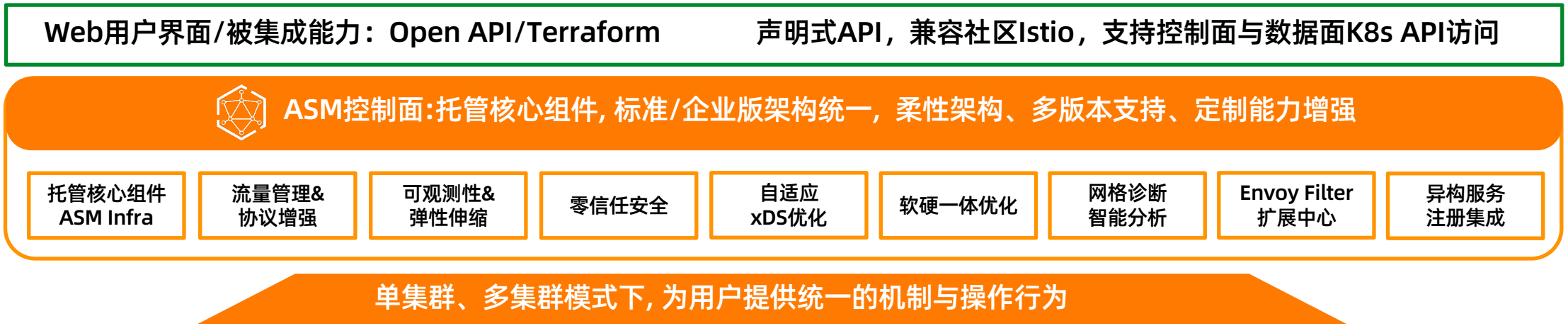
传统的Service Mesh单集群模式

阿里云 | 奥运会全球指定云服务商

控制面与数据面的组件都运行于一个K8s集群中

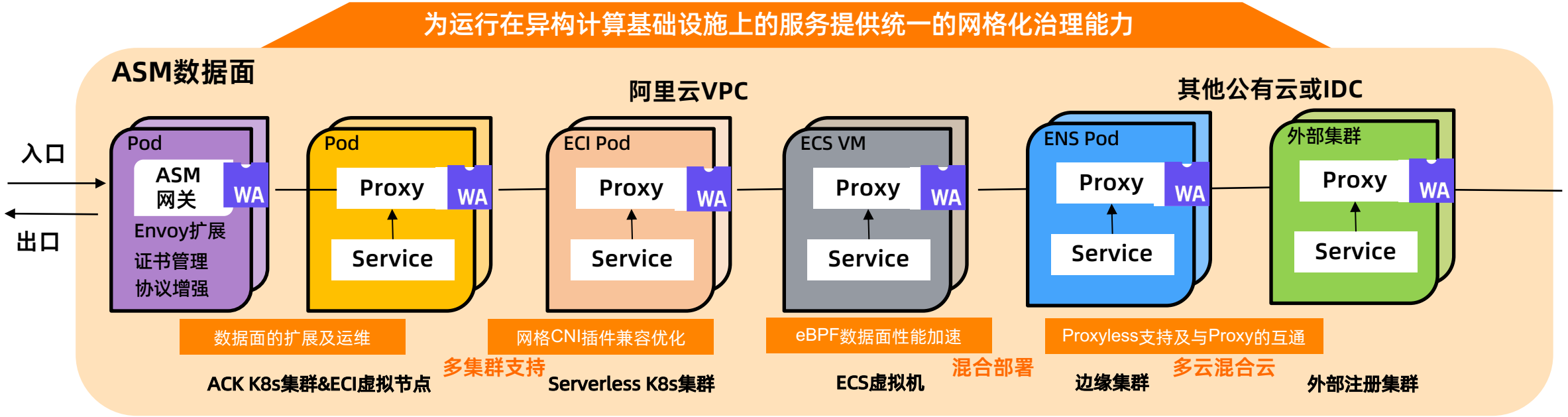


托管的Service Mesh控制面



- 与社区Istio支持的external Istiod模式保持一致
- 以托管方式运行于云账户的资源侧, 不占用用户侧的资源
- 独立解耦运行, 升级管理可以在控制台上一键操作

多样且统一的数据面


为运行在异构计算基础设施上的服务提供统一的网格化治理能力
ASM数据面
阿里云VPC
其他公有云或IDC
入口
出口
Pod
ASM
网关
WA
Envoy扩展
证书管理
协议增强
Pod
Proxy
WA
Service
ECI Pod
Proxy
WA
Service
ECS VM
Proxy
WA
Service
ENS Pod
Proxy
WA
Service
外部集群
Proxy
WA
Service
数据面的扩展及运维
网格CNI插件兼容优化
eBPF数据面性能加速
Proxyless支持及与Proxy的互通
多集群支持
混合部署
多云混合云
ACK K8s集群&ECI虚拟节点
Serverless K8s集群
ECS虚拟机
边缘集群
外部注册集群

ASM下一键添加移除K8s集群

阿里云 | 奥运会全球指定云服务商

- 支持多种不同形态的K8s集群
- 简单易用，一键添加或移除
- 预检查，避免潜在冲突
  - 网络段CIDR冲突
  - Istio API资源定义冲突
  - K8s域名定义冲突
  - ….

阿里云服务网格ASM的技术架构

阿里云 | 奥运会全球指定云服务商

https://www.aliyun.com/product/servicemesh

异构服务统一治理（流量管理、可观测、安全）

跨集群的应用网络管理

与CI/CD工具融合的应用灰度发布与部署

应用上云架构平滑演进

基于KServe的AI弹性服务管理

Web用户界面/被集成能力：Open API/Terraform　　声明式API，兼容社区Istio，支持控制面与数据面K8s API访问

ASM控制面:托管核心组件, 标准/企业版架构统一，柔性架构、多版本支持、定制能力增强

托管核心组件 ASM Infra

流量管理& 协议增强

可观测性& 弹性伸缩

零信任安全

自适应 xDS优化

软硬一体优化

网格诊断 智能分析

Envoy Filter 扩展中心

异构服务 注册集成

为运行在异构计算基础设施上的服务提供统一的网格化治理能力

ASM数据面

阿里云VPC

其他公有云或IDC

入口

出口

Pod
ASM 网关
WA
Envoy扩展
证书管理
协议增强

Pod
Proxy
WA
Service

ECI Pod
Proxy
WA
Service

ECS VM
Proxy
WA
Service

ENS Pod
Proxy
WA
Service

外部集群
Proxy
WA
Service

数据面的扩展及运维

网格CNI插件兼容优化

eBPF数据面性能加速

Proxyless支持及与Proxy的互通

多集群支持

混合部署

多云混合云

ACK K8s集群&ECI虚拟节点

Serverless K8s集群

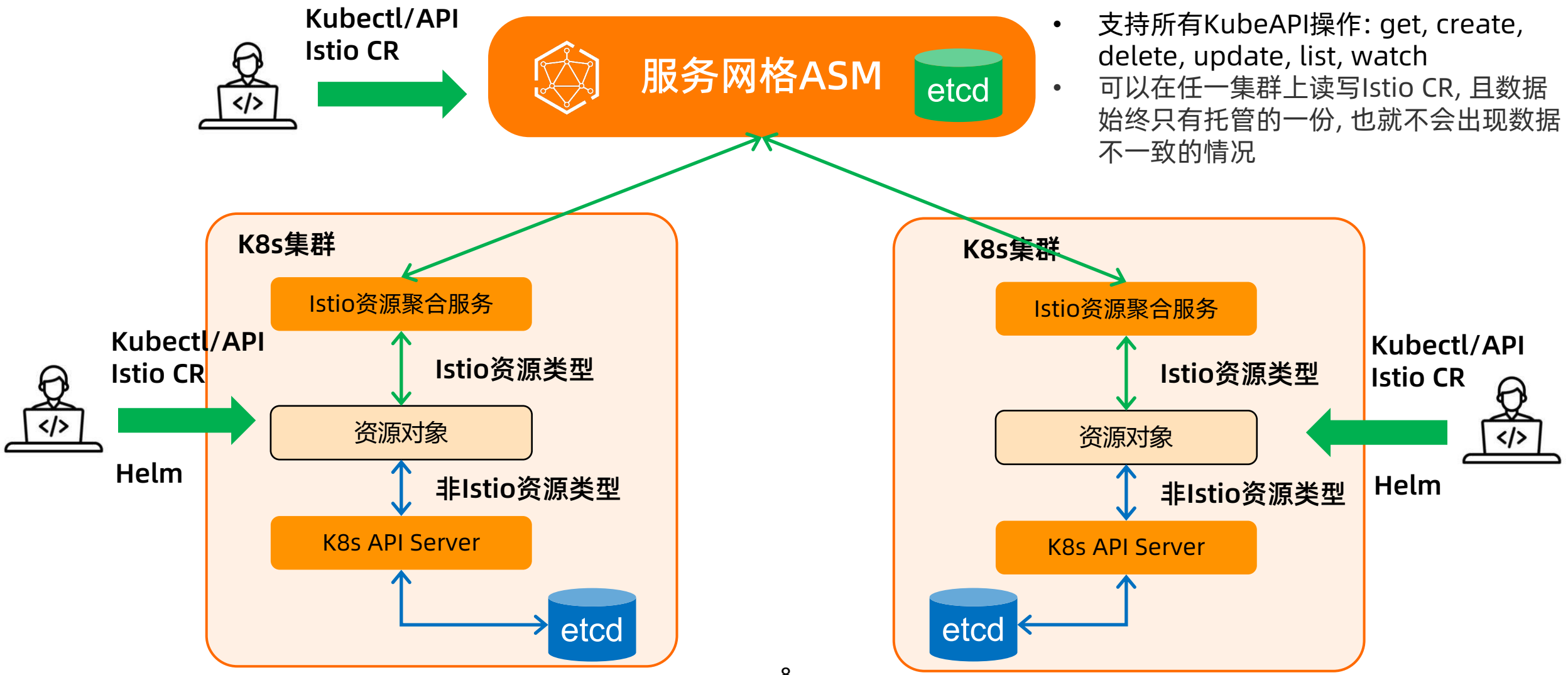
ECS虚拟机

边缘集群

外部注册集群

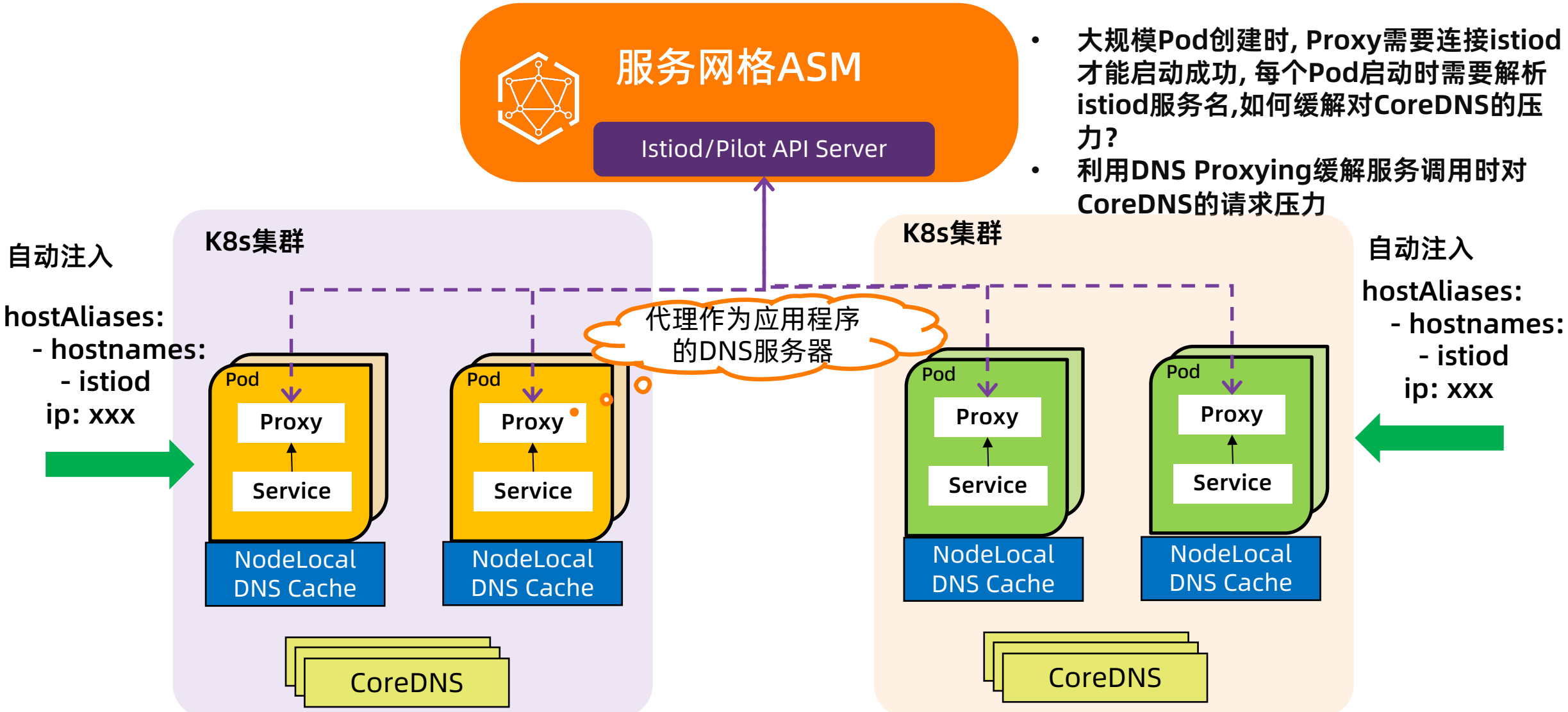
多集群模式下的Istio资源对象的存储与访问

阿里云 | 奥运会全球指定云服务商



- 支持所有KubeAPI操作: get, create, delete, update, list, watch
- 可以在任一集群上读写Istio CR, 且数据始终只有托管的一份, 也就不会出现数据不一致的情况

多集群模式下利用Service Mesh提升DNS解析服务可靠性



- 大规模Pod创建时，Proxy需要连接istiod才能启动成功，每个Pod启动时需要解析istiod服务名,如何缓解对CoreDNS的压力?
- 利用DNS Proxying缓解服务调用时对CoreDNS的请求压力

Service Mesh的定位：应用感知的云原生基础设施

云原生应用治理

- 全链路灰度

云原生应用生态引擎

- AI Serving on ASM

云原生应用网络

- 基于地域、可用区信息的优先路由

云原生零信任安全

- 应用零信任安全中心

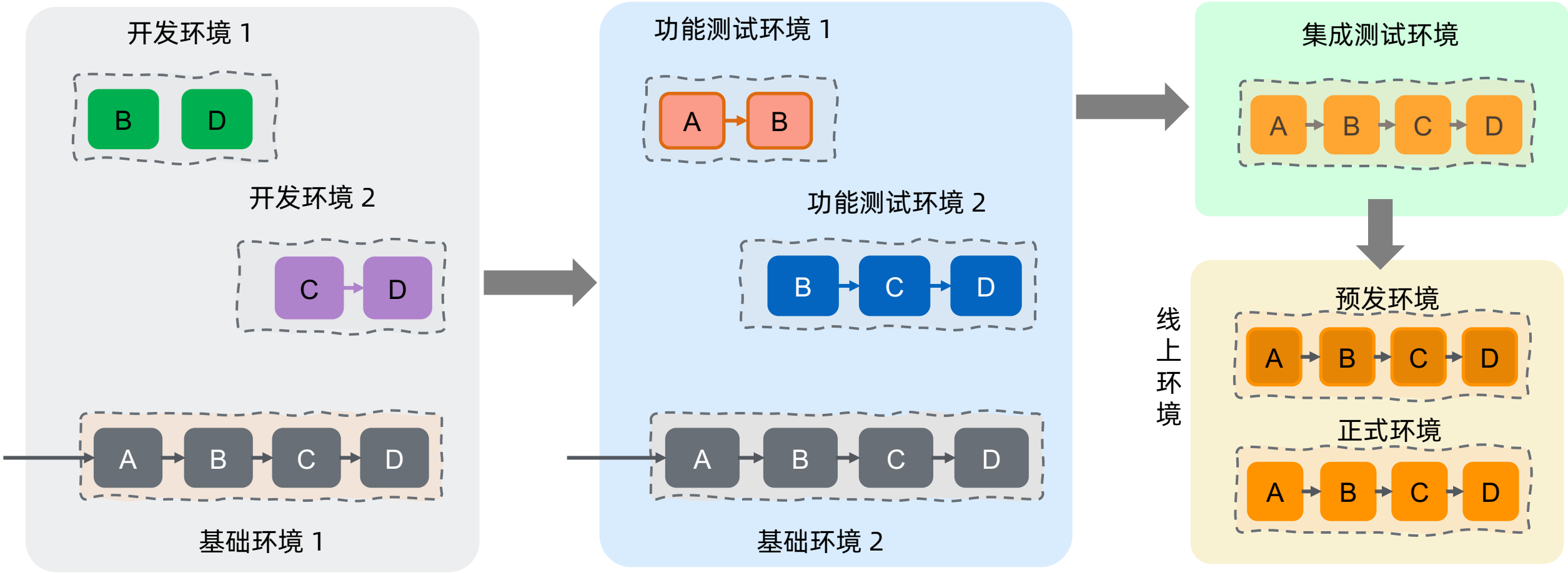
云原生可观测

- 应用可观测中心

案例：某客户研发体系所需要的多套应用环境(多集群)

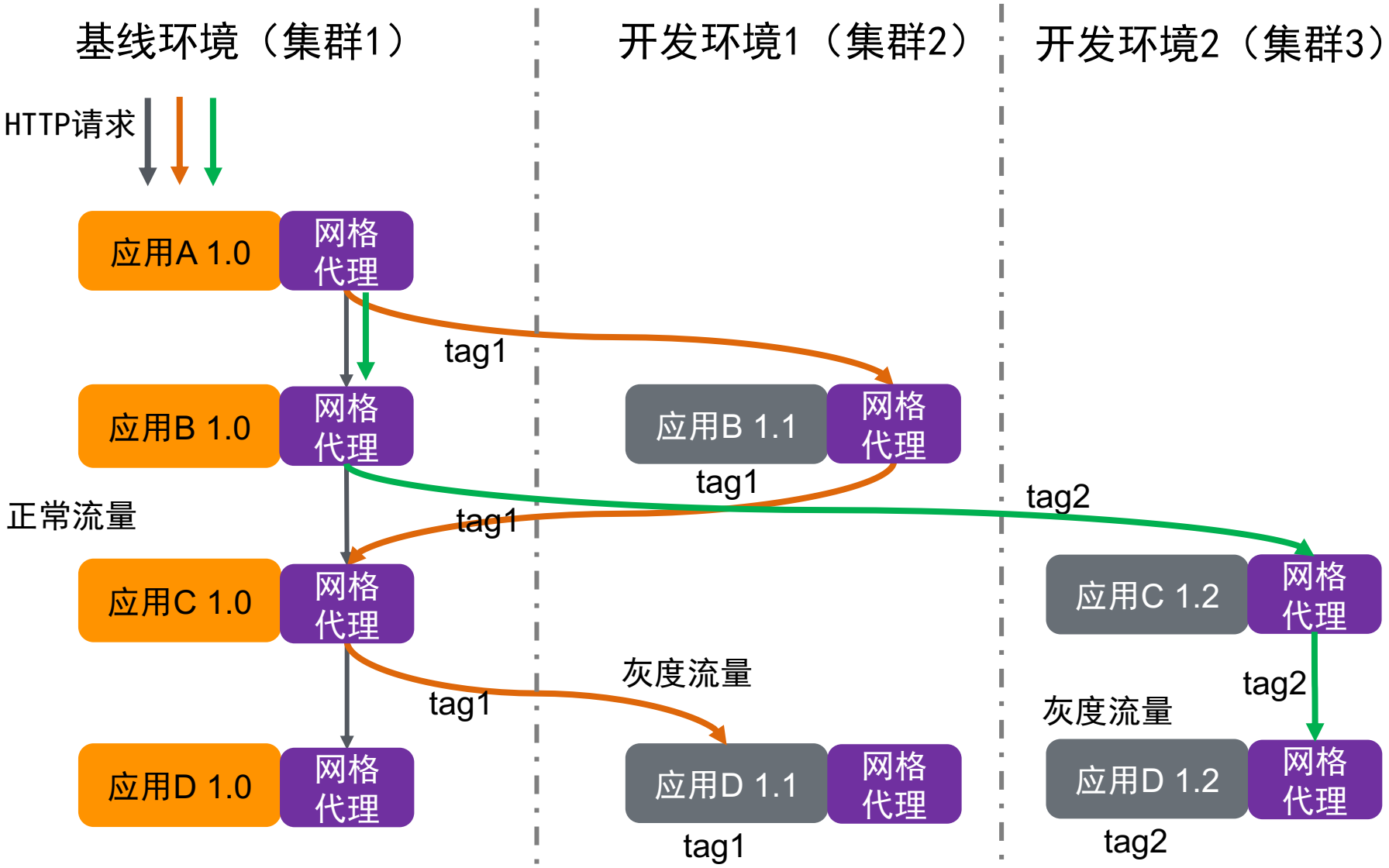
- 多套的开发环境（含基础环境）
- 多套功能测试环境（含基础环境）
- 集成测试环境

- 预发环境
- 支持灰度的生产环境



全链路流量管理：逻辑隔离的动态多环境

阿里云 | 奥运会全球指定云服务商



流量打标：

- 流量标签CR/Controller
- 支持不同粒度，按工作负载或命名空间

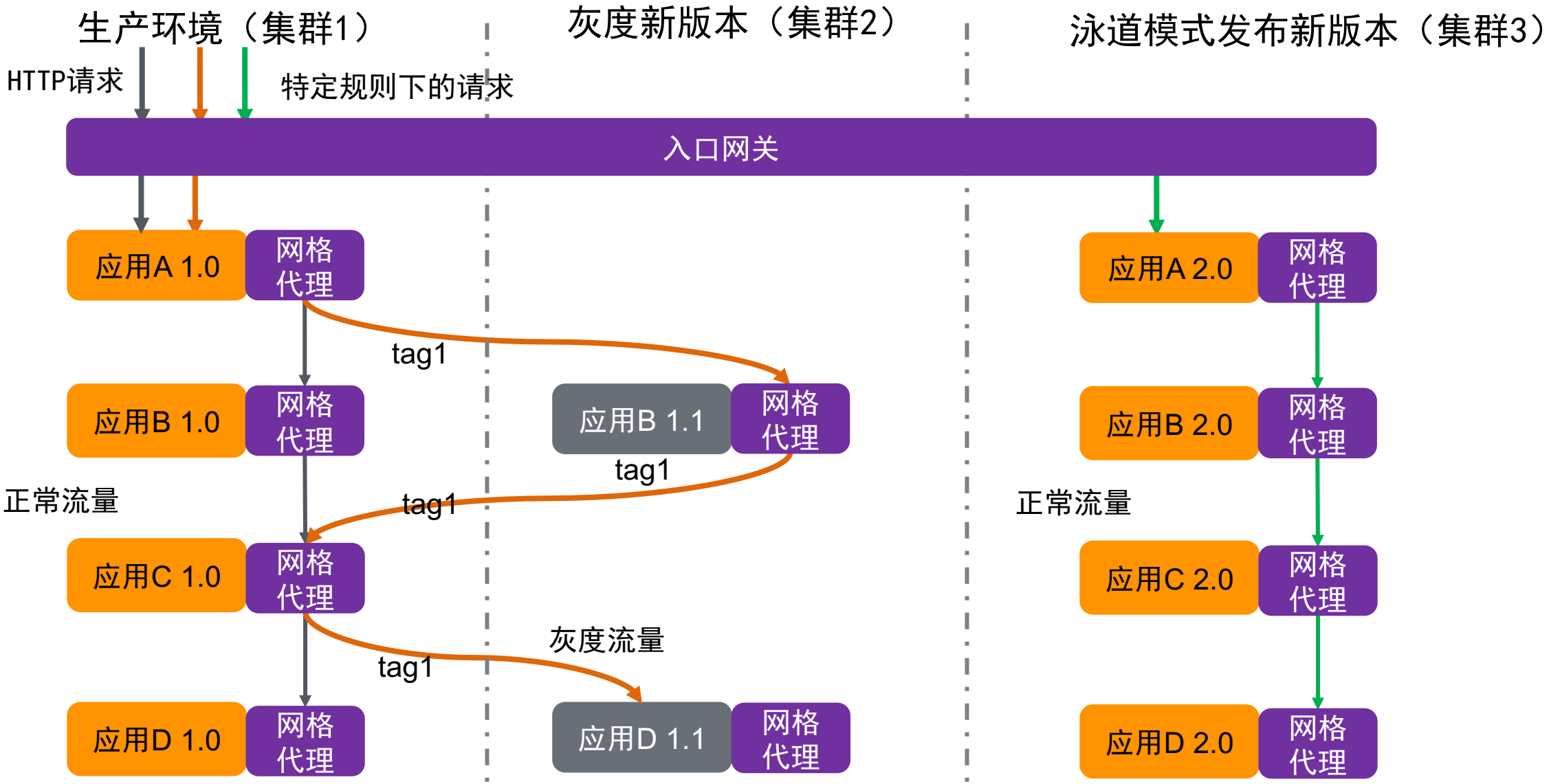
标签路由

- 按标签定义流量路由规则
- 支持回退机制

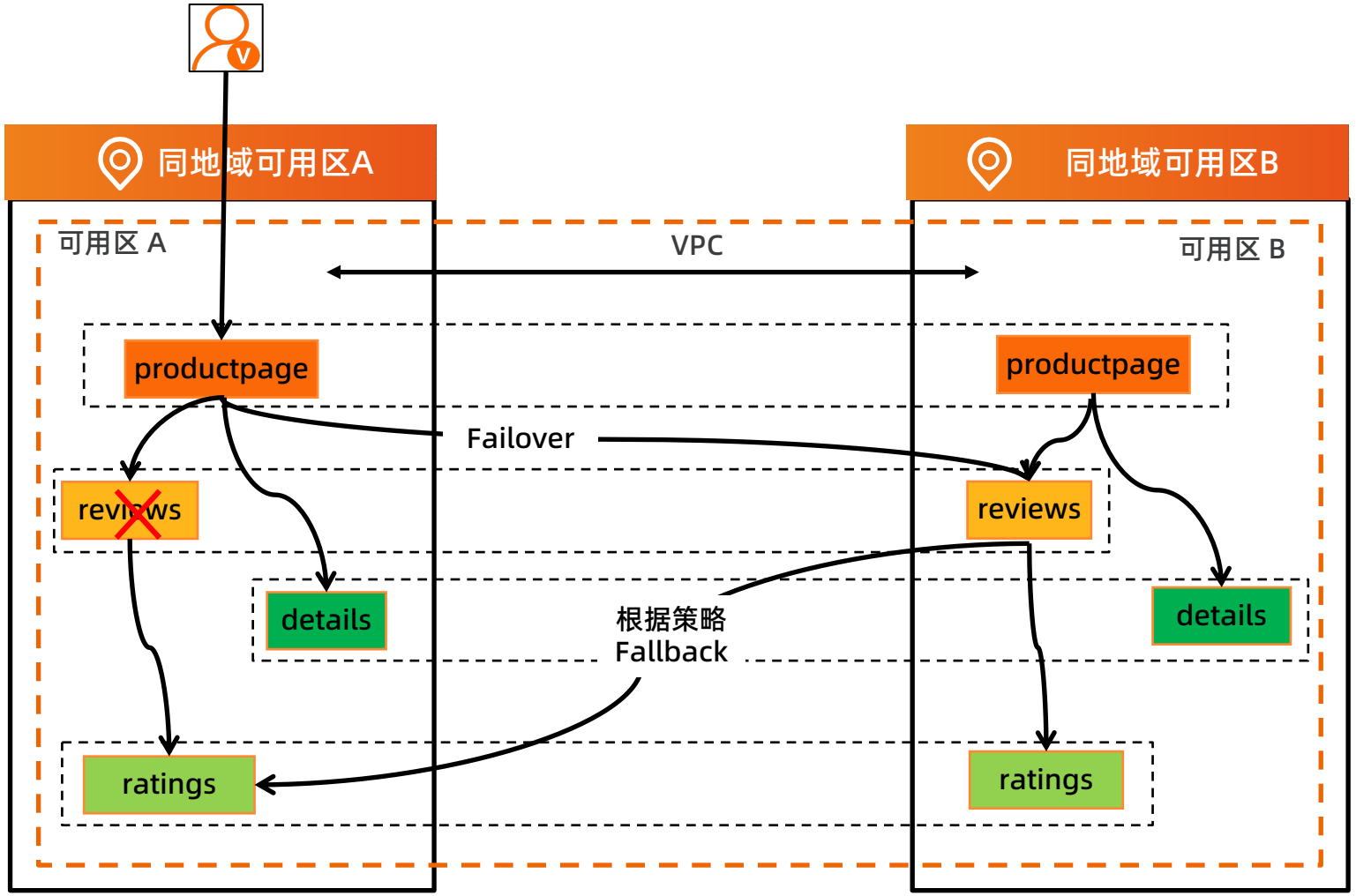
流量染色/自动染色：

- 将流量带上特定标识
- 支持标识在调用链路中传递

全链路流量管理：全链路灰度的生产环境



基于地域可用区信息的流量路由优先及容灾模式

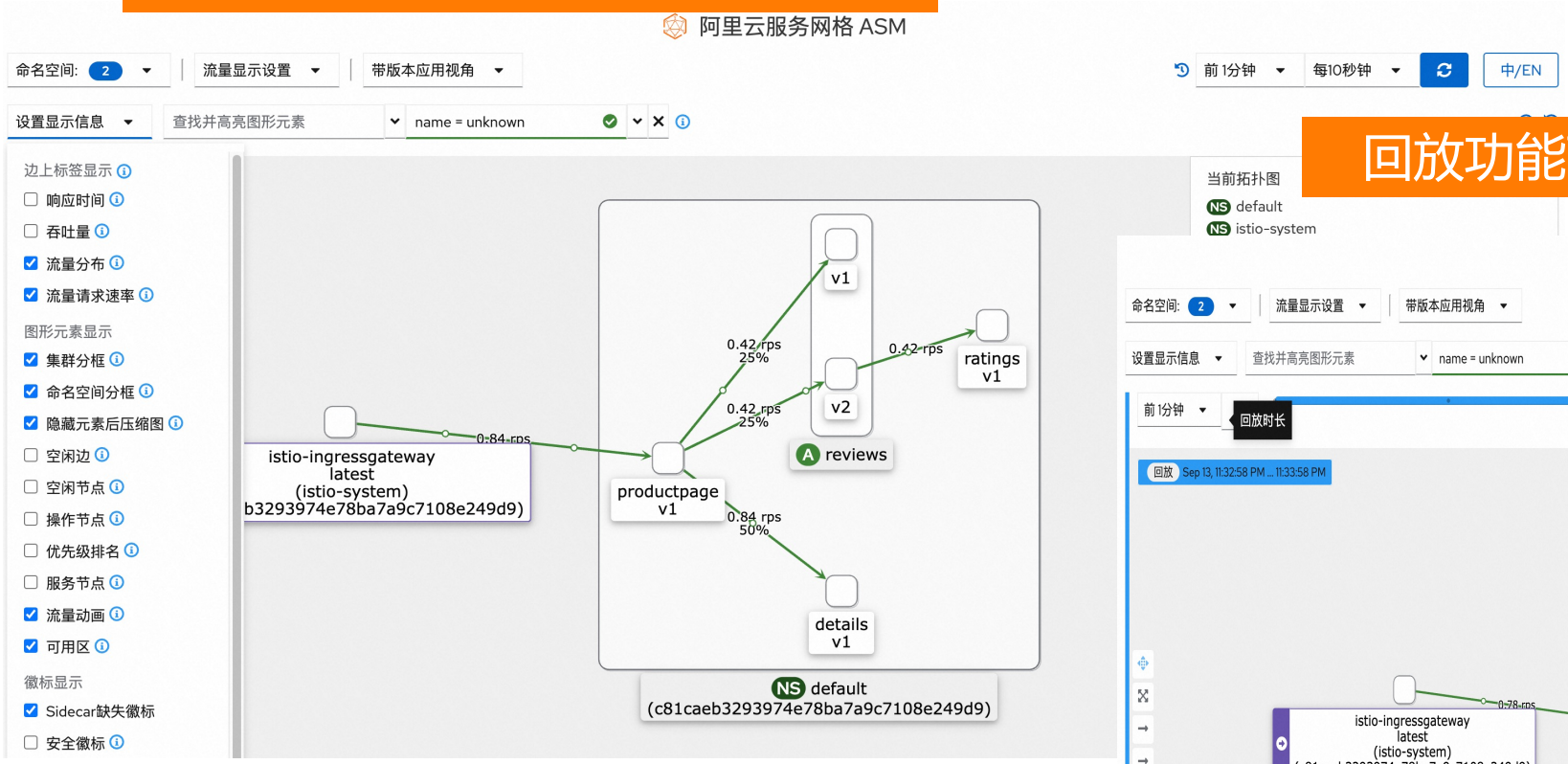


同 Region 切换

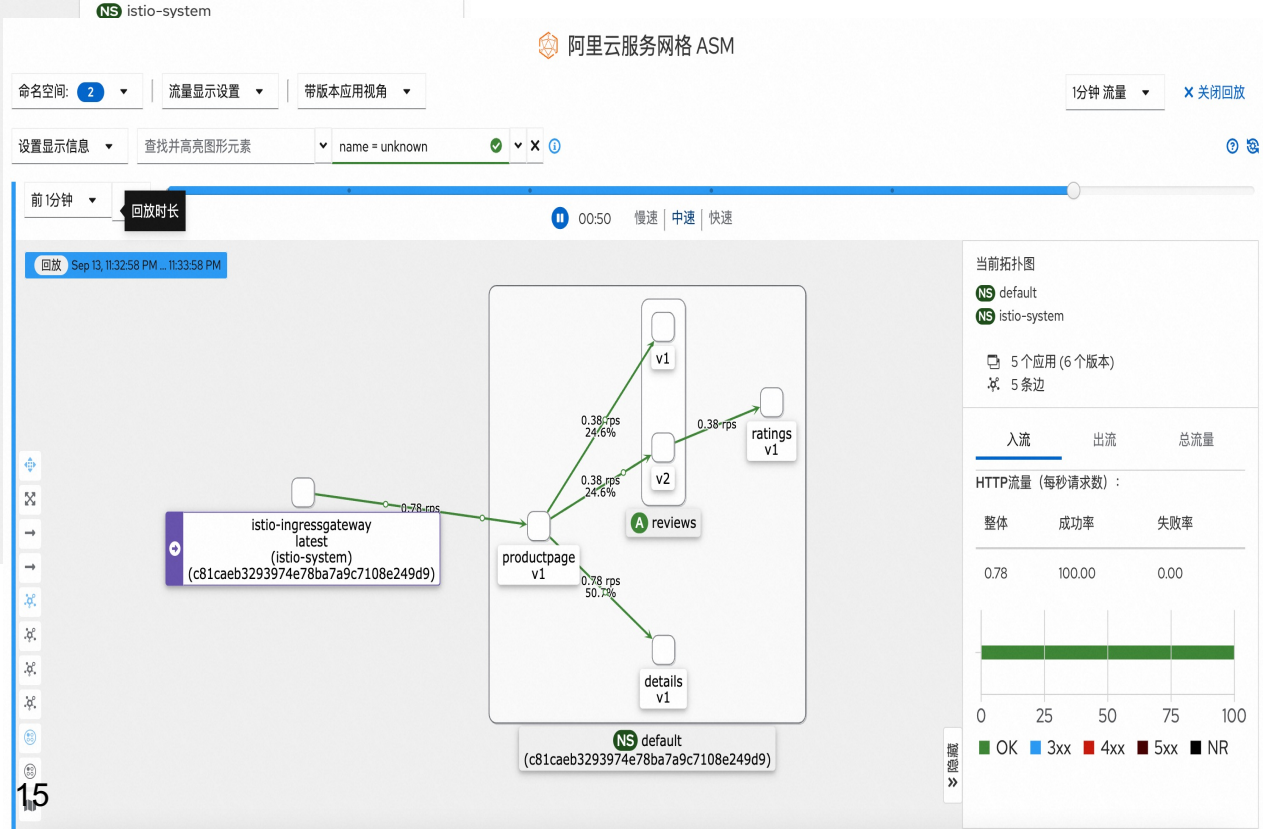
网格拓扑：提供对服务网格行为的即时洞察

阿里云 | 奥运会全球指定云服务商

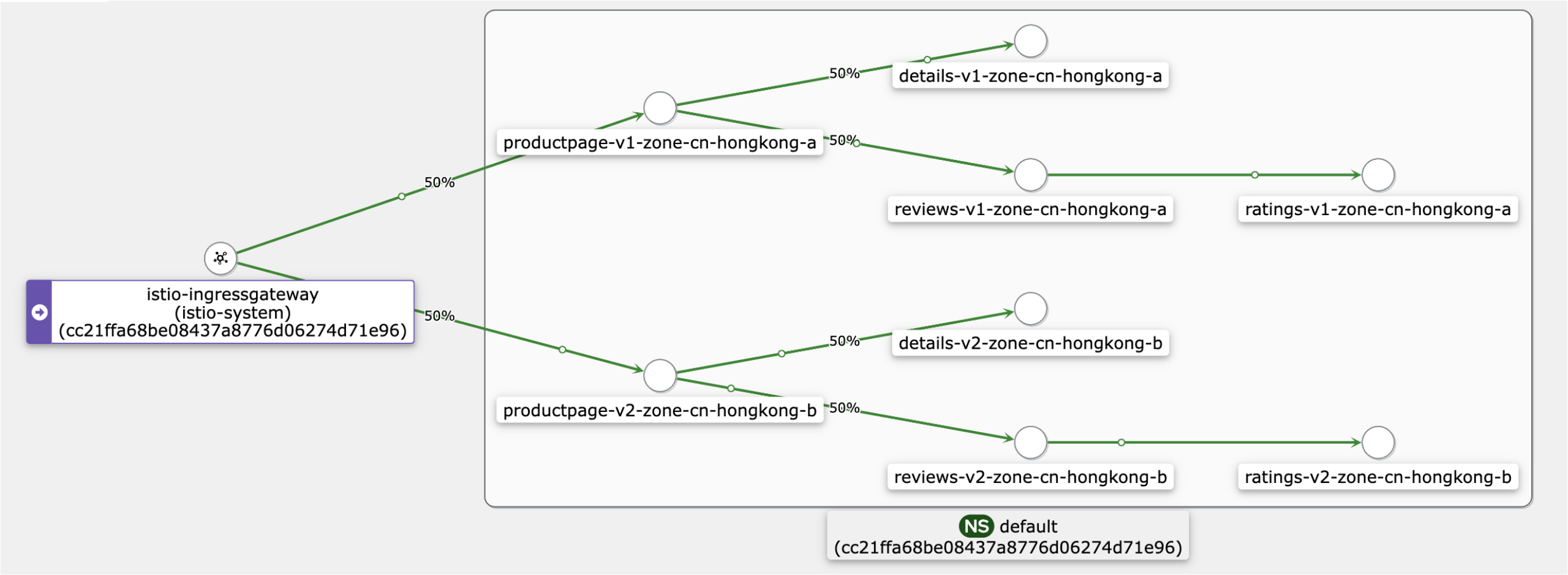
强大的网格流量拓扑可视化



回放功能可以选定过去时间段的流量

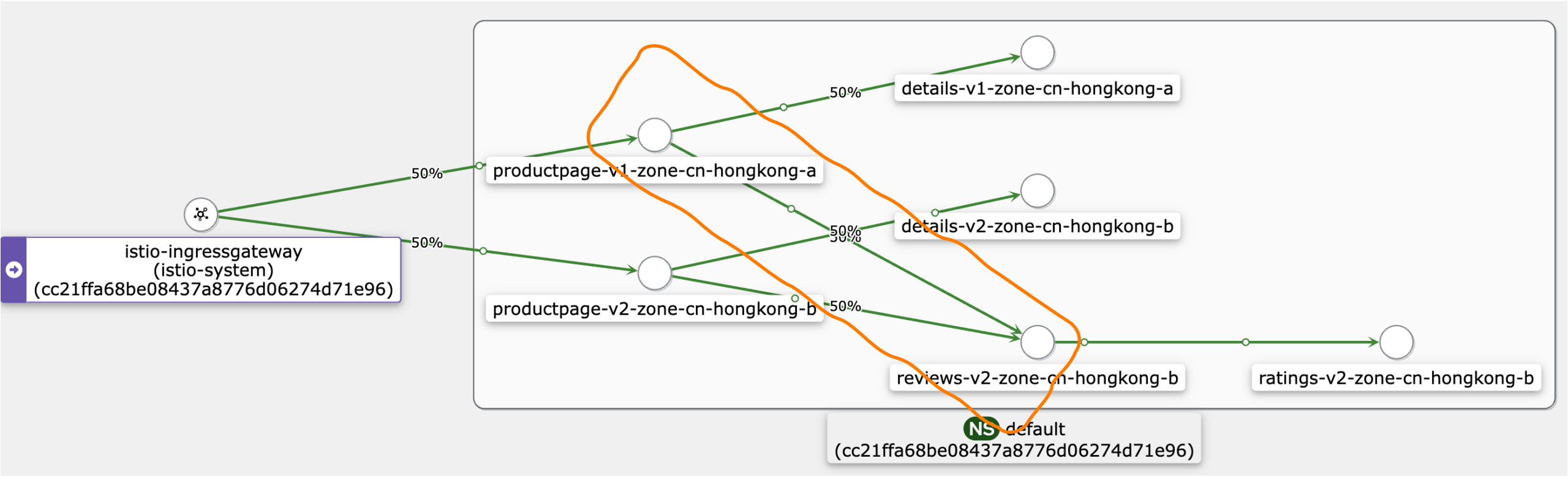


在不需要修改应用代码的情况下可以实现同AZ路由



自动实现故障转移以保证高可用

阿里云 | 奥运会全球指定云服务商

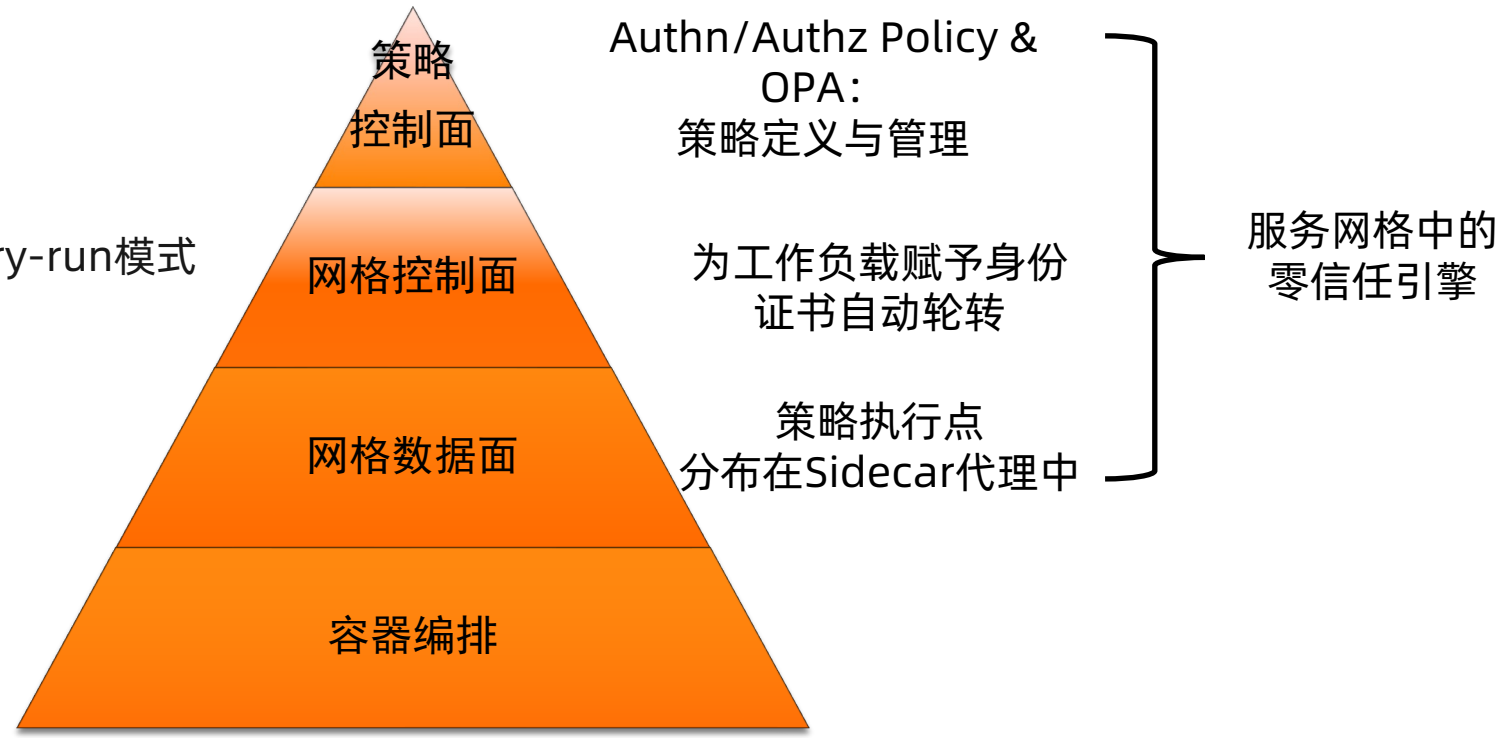


服务网格中的零信任安全体系

阿里云 | 奥运会全球指定云服务商

零信任安全能力体系：

- 零信任的基础 - 工作负载身份 - SPIFFE标准
- 零信任的载体 - 安全证书 - X509 TLS 证书
- 零信任的引擎 - 策略执行 - RBAC/OPA、dry-run模式
- 零信任的洞察 - 可视化与分析 - 监视与审计



使用服务网格实现零信任的优势：

- Sidecar代理生命周期独立
- 动态配置、无需重启
- 服务网格集中控制，降低开发心智负担
- 加强身份认证授权系统本身安全保障
- 集中管理并下发OPA授权策略
- 简化接入第三方授权服务、OIDC身份认证

如何缩小安全漏洞爆炸半径，实现服务间零信任安全？

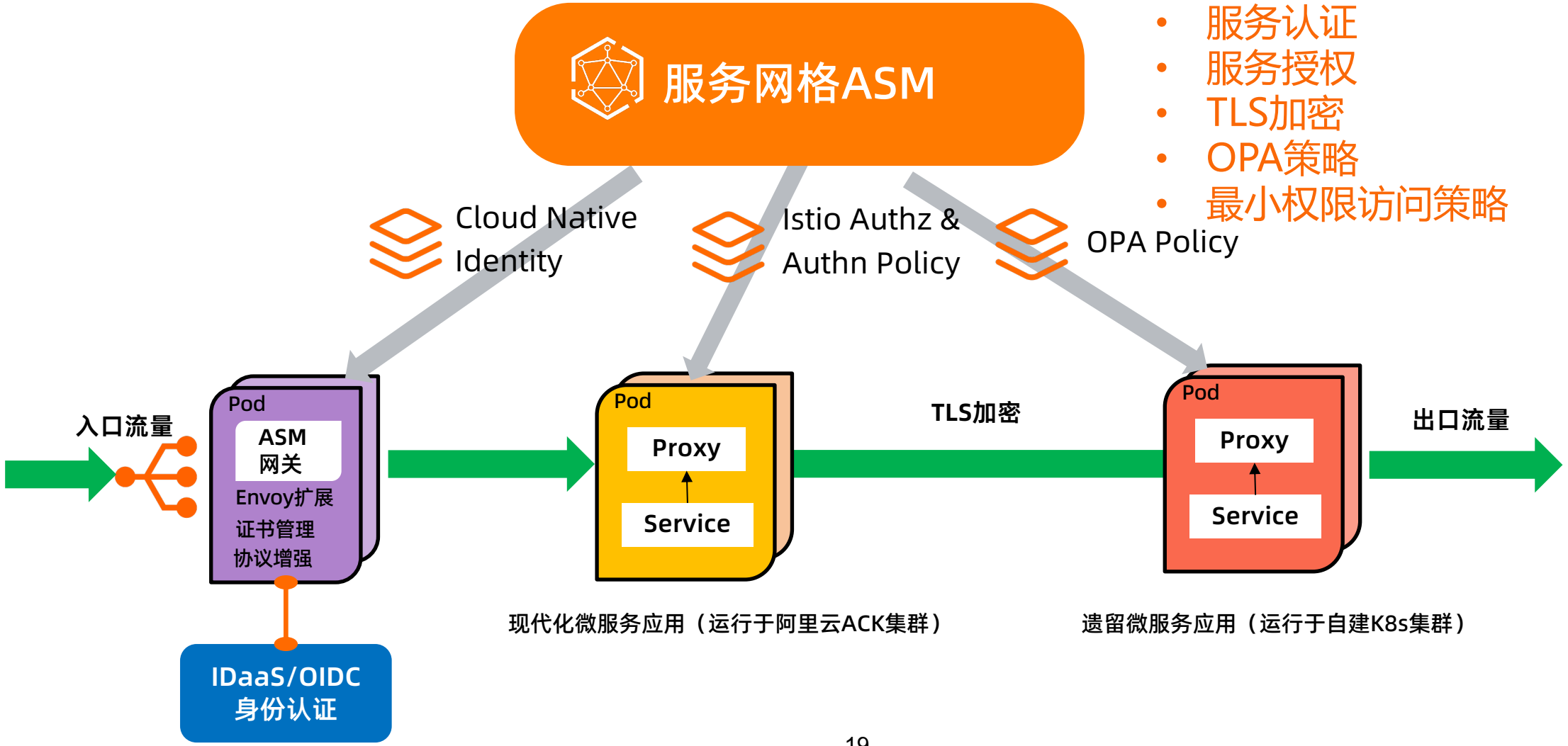
https://developer.aliyun.com/article/844611

客户案例：某平台使用网格零信任安全技术的场景

阿里云 | 奥运会全球指定云服务商

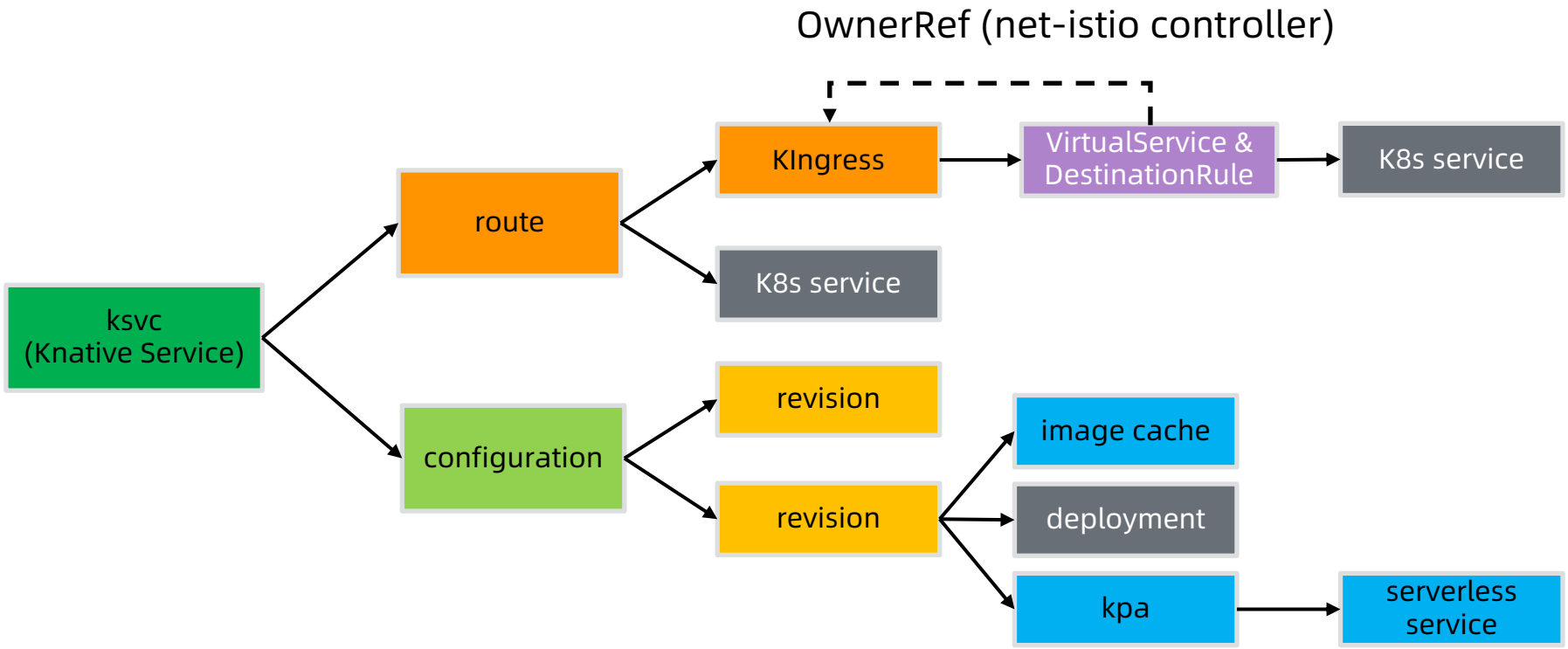
零信任安全架构

- 工作负载身份标识
- 服务认证
- 服务授权
- TLS加密
- OPA策略
- 最小权限访问策略



单集群模式下的Knative Serverless服务

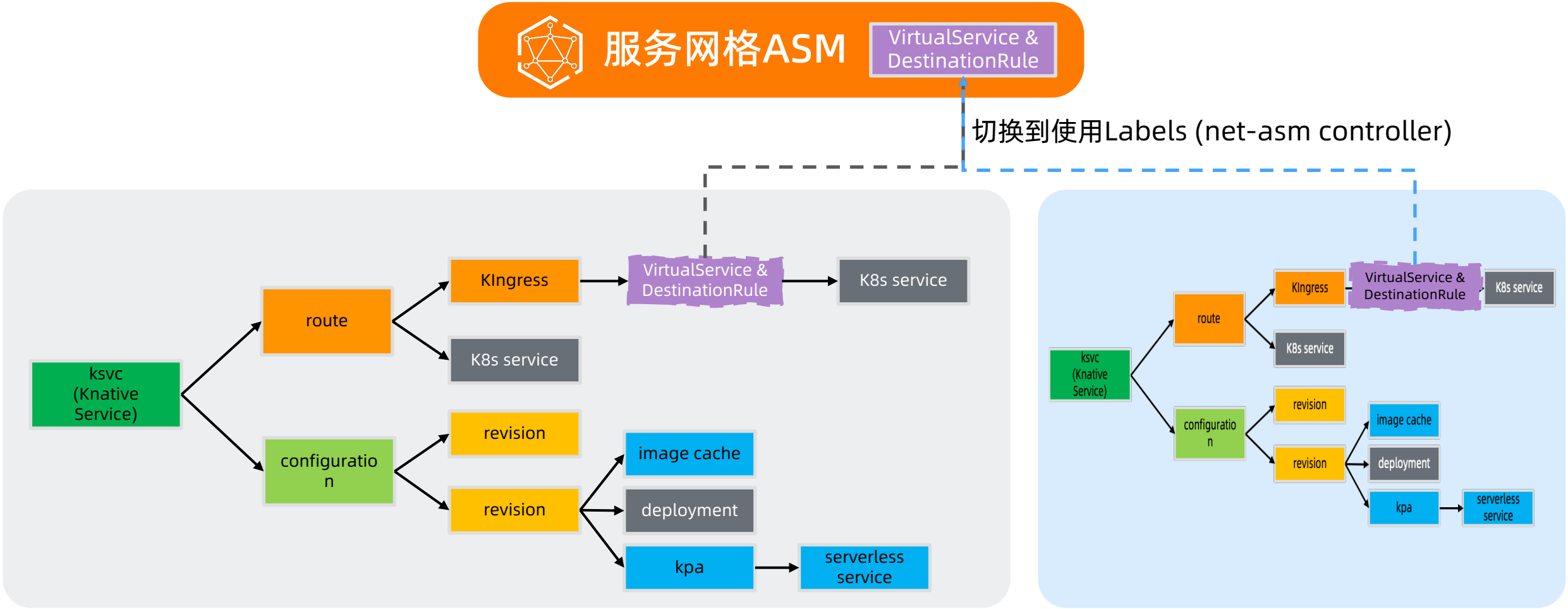
单集群模式下, Knative与Istio运行在同一个K8s集群中



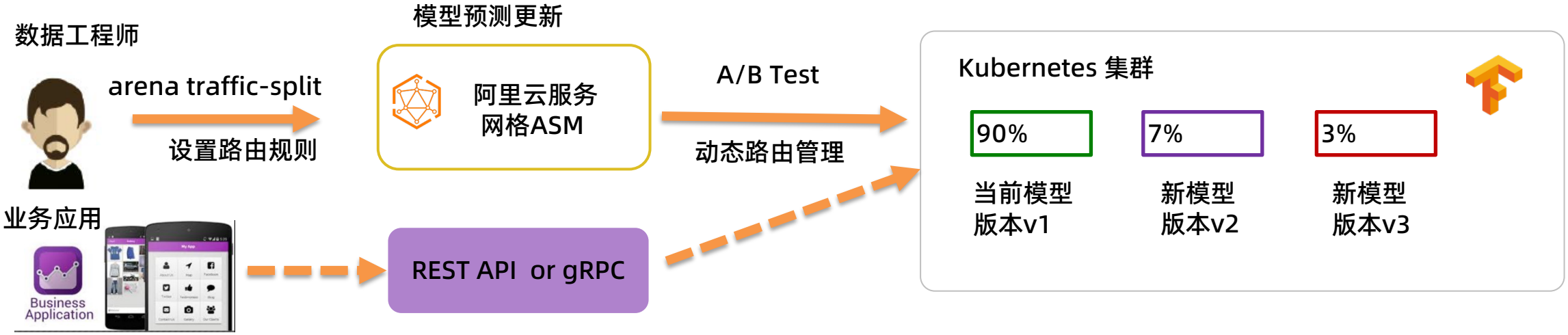
Knative on ASM: 多集群模式下的Serverless服务

阿里云 | 奥运会全球指定云服务商

多集群模式下, Knative与Istio运行在不同的K8s集群中

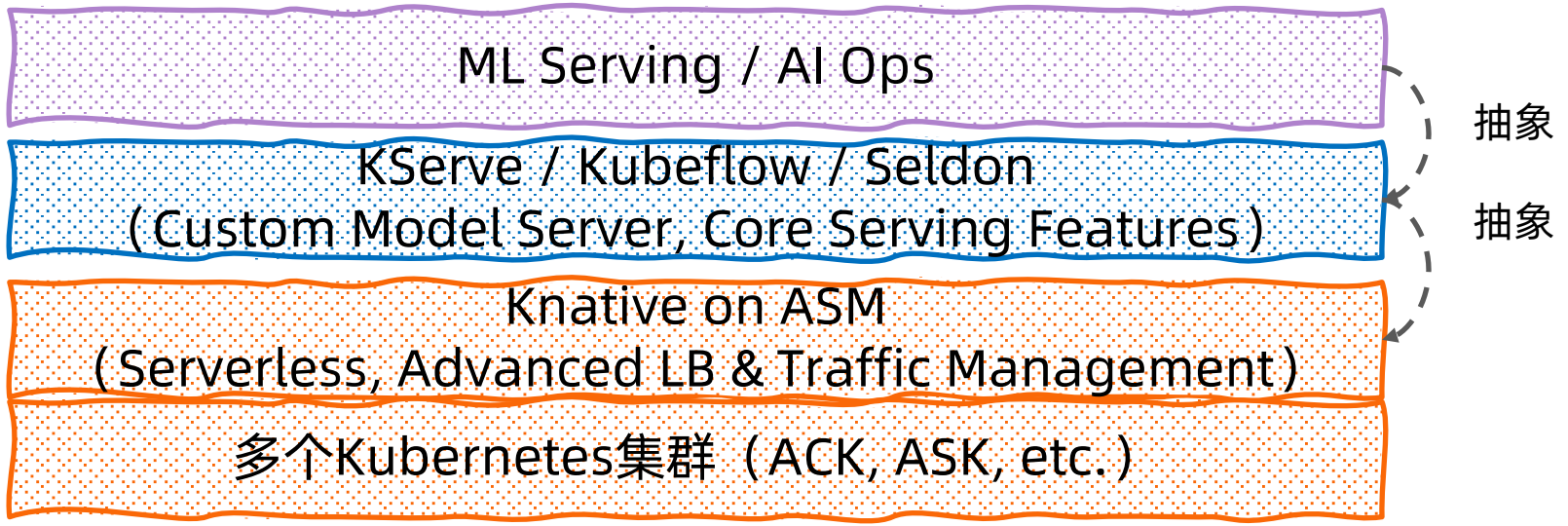


AI Serving on ASM: 多集群模式下的AIOps能力



模型迭代发布效率提升 2~5 倍

服务网格ASM
容器服务ACK




KUBERNETES
COMMUNITY DAYS DALIAN
Thank YOU