

阿里云云原生多活容灾解决方案

多活容灾架构与最佳实践

远跖

阿里云-高可用架构

2020/02/03

目录

01 为什么做多活

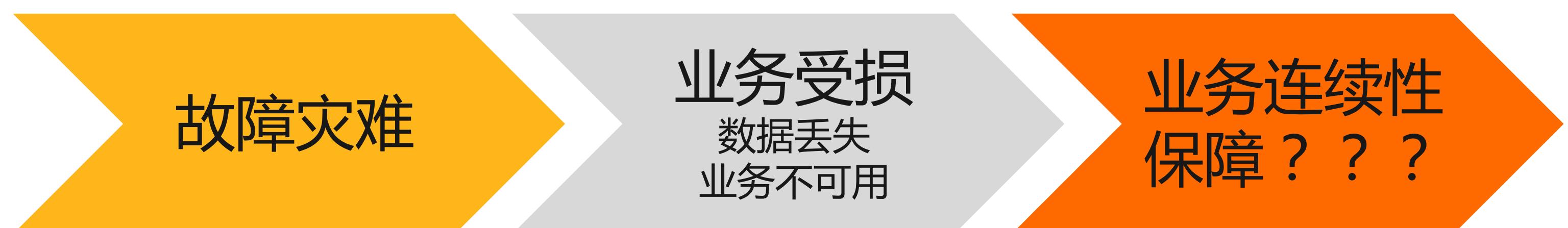
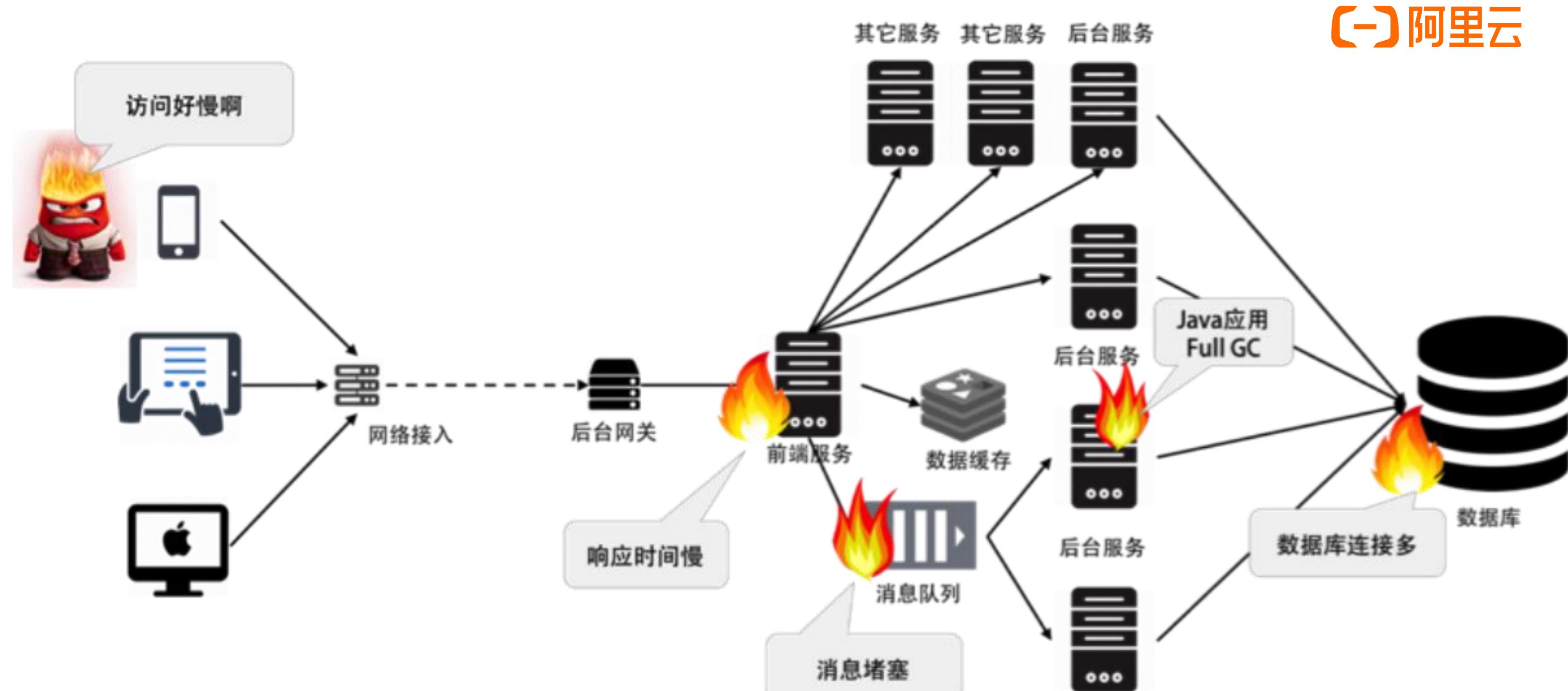
02 多活解决方案介绍

03 客户案例

04 功能演示

故障和灾难不可避免

- 变更操作失误**
配置错误、应用发布失败等等
- 硬件故障**
网络设备出故障，机房/集群影响
- 网络攻击**
DDOS等网络攻击
- 断电/断网**
光纤被挖断
- 自然灾害**
地震、台风、雷击

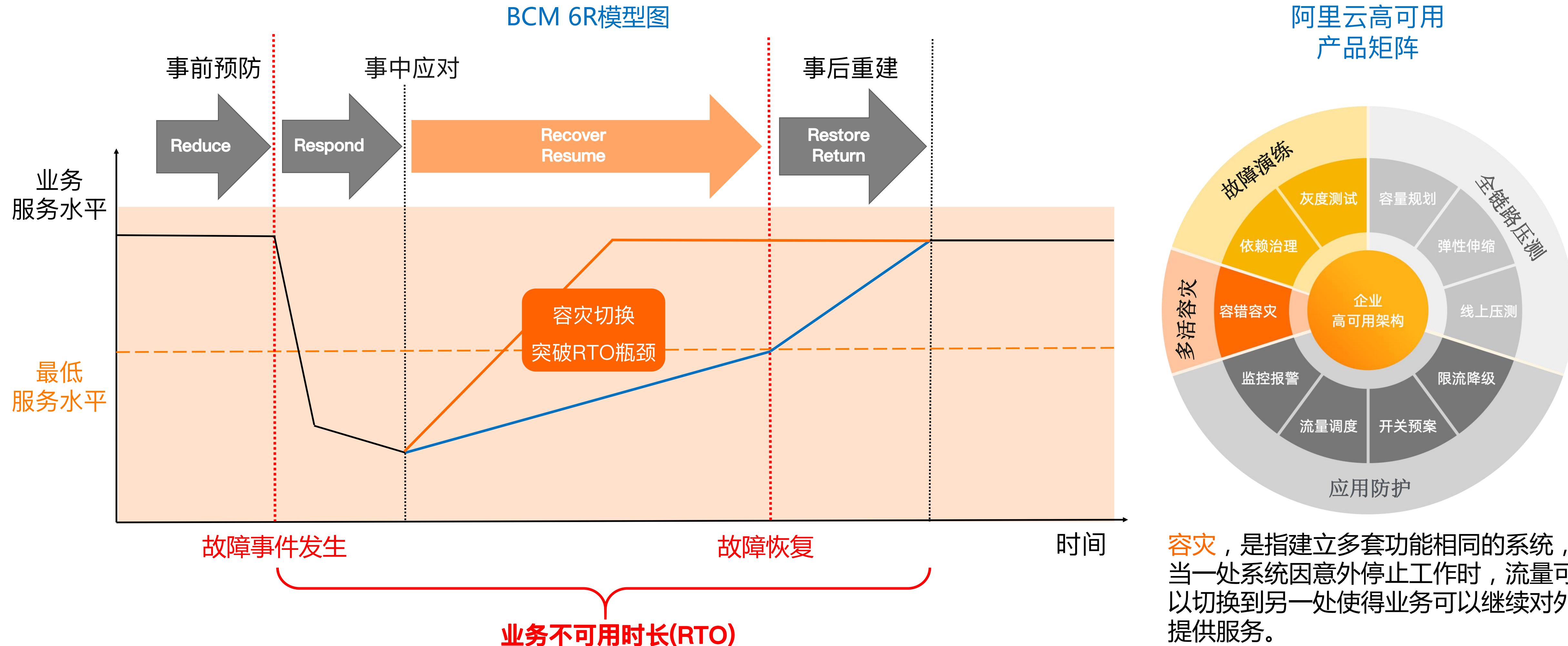


What does **not kill** me, makes me stronger
凡是不能消灭我的，必将会是我更强大--尼采

业务连续性管理BCM

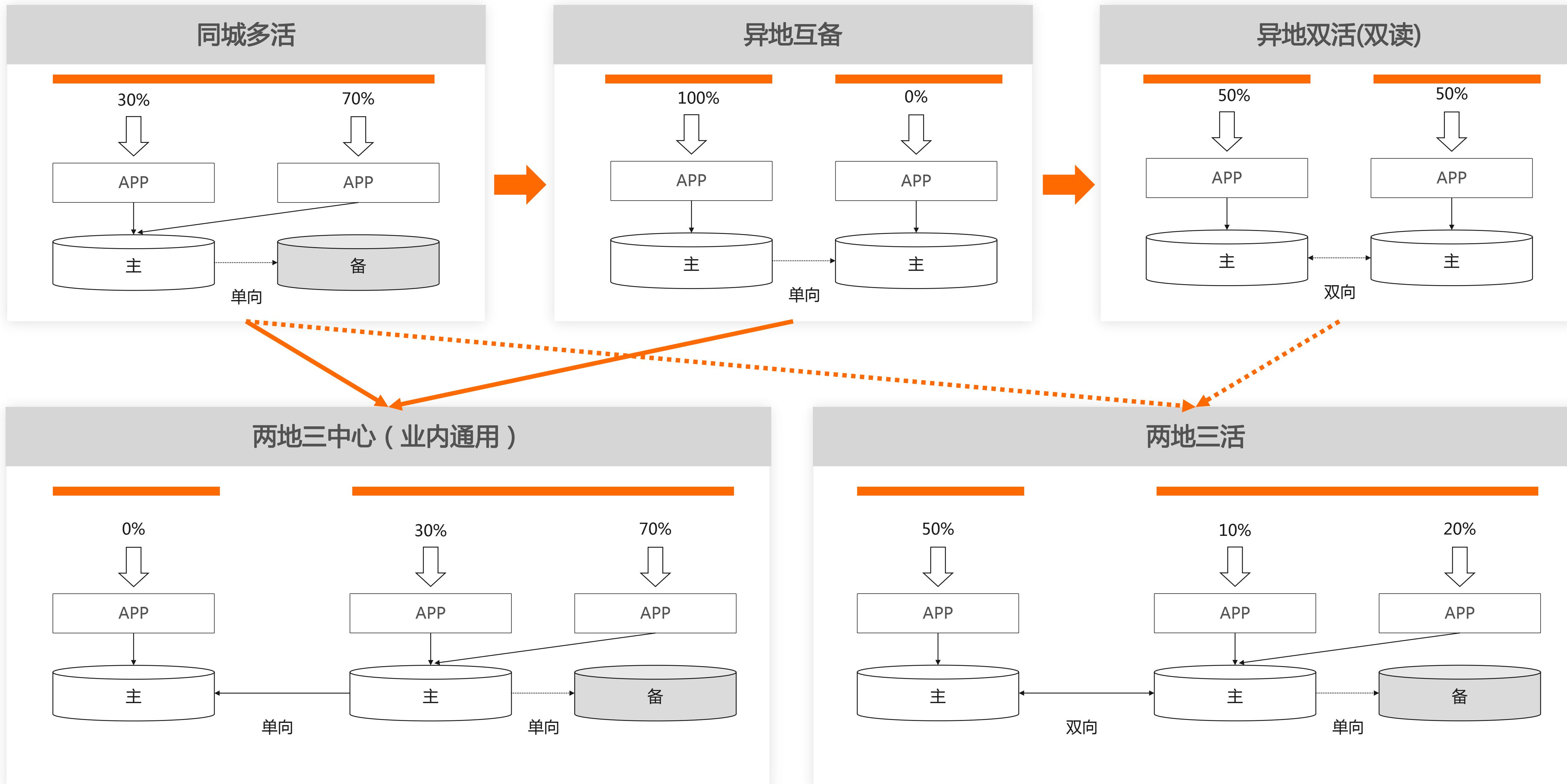
阿里云

BCM (Business Continuity Management) , 研究的是**保障业务连续性的方法** : 发生故障或灾难时 , 以合理的成本和资源保护重要的业务活动 , 确保在规定的时间内恢复业务 , 最大程度的减少灾害带来的冲击和将中断影响降至最低。



递进式多活容灾架构

[-] 阿里云



双活容灾架构解决方案

[-] 阿里云

传统灾备方案



主要特征

- 仅主数据中心对外提供服务

问题

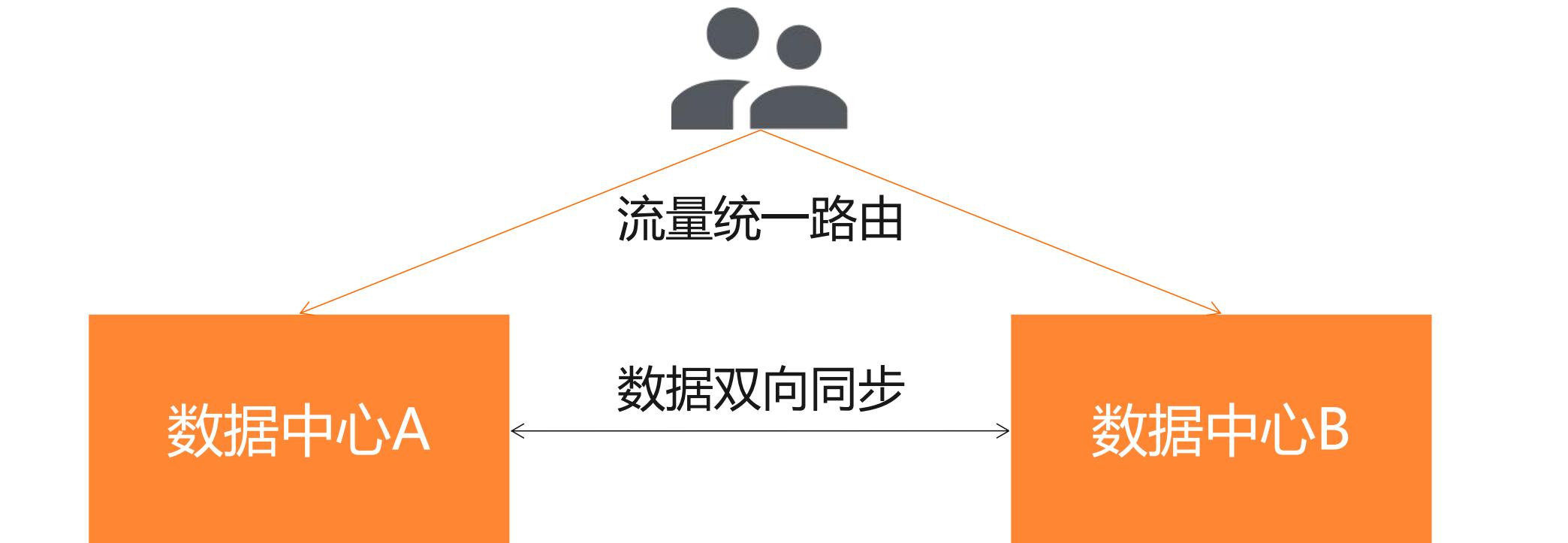
- 备数据中心平时不对外服务
 - 主中心资源单点，备中心资源浪费
 - 关键时刻不敢切换
 - 主数据中心存在容量瓶颈
- RTO：不可控，依赖故障的恢复

RTO(Recovery Time Objective)

恢复时间目标，表示故障场景下业务能够容忍的服务不可用最大时长。

eg : RTO=30s 表示业务仅容忍服务不可用持续30s

双活方案



主要特征

- 隔离的冗余。流量按照一定规则进行路由，流量在单元内封闭。

优势

- 双数据中心同时对外服务，解决了传统灾备方案的资源浪费、不敢切、以及容量瓶颈问题
- RTO：分钟级。故障情况下，可使用切流功能进行快速的业务恢复，将业务恢复和故障恢复解耦，保障业务连续性
- 为技术创新提供实验田

目录

01 为什么做多活

02 多活解决方案介绍

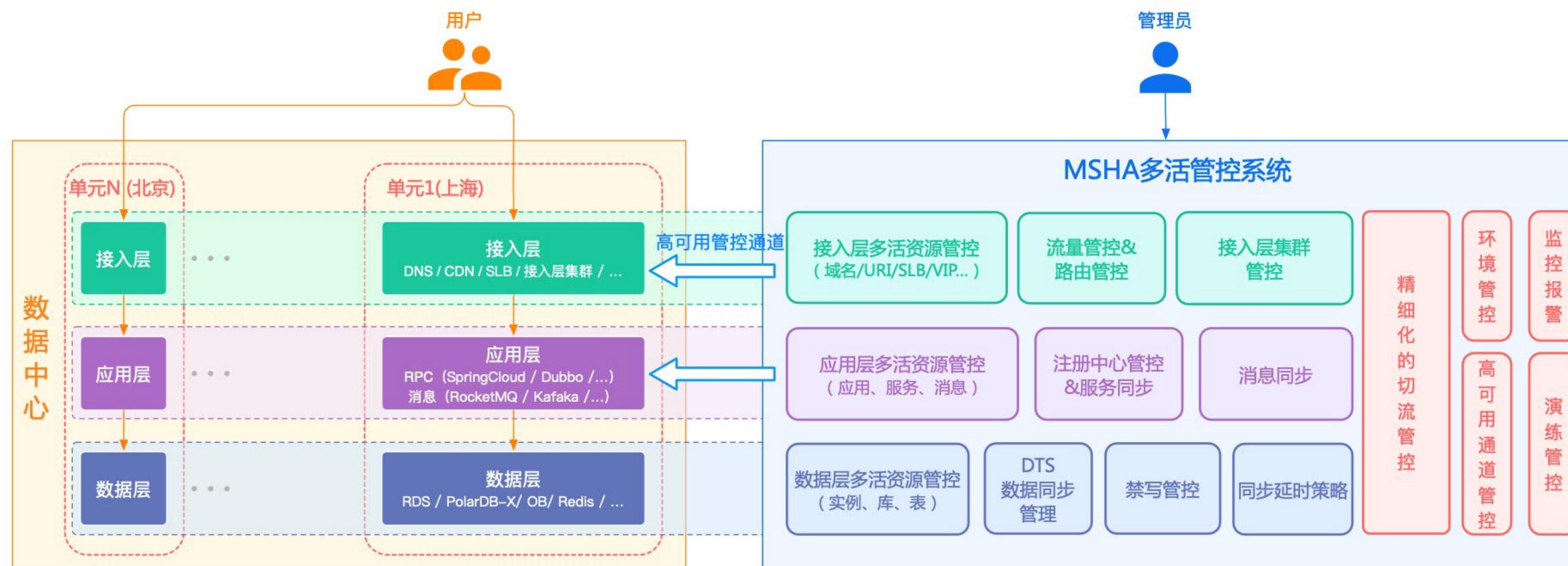
03 客户案例

04 功能演示

MSHA产品架构

(-) 阿里云

MSHA (Multi-Site High Availability)，是在阿里巴巴电商业务环境演进出来的多活容灾架构解决方案。提供基于单元的多活架构管理功能，支持自上到下的各层（接入层、应用层、数据层等）多活资源管控，以及应对故障发生时的容灾切换能力。

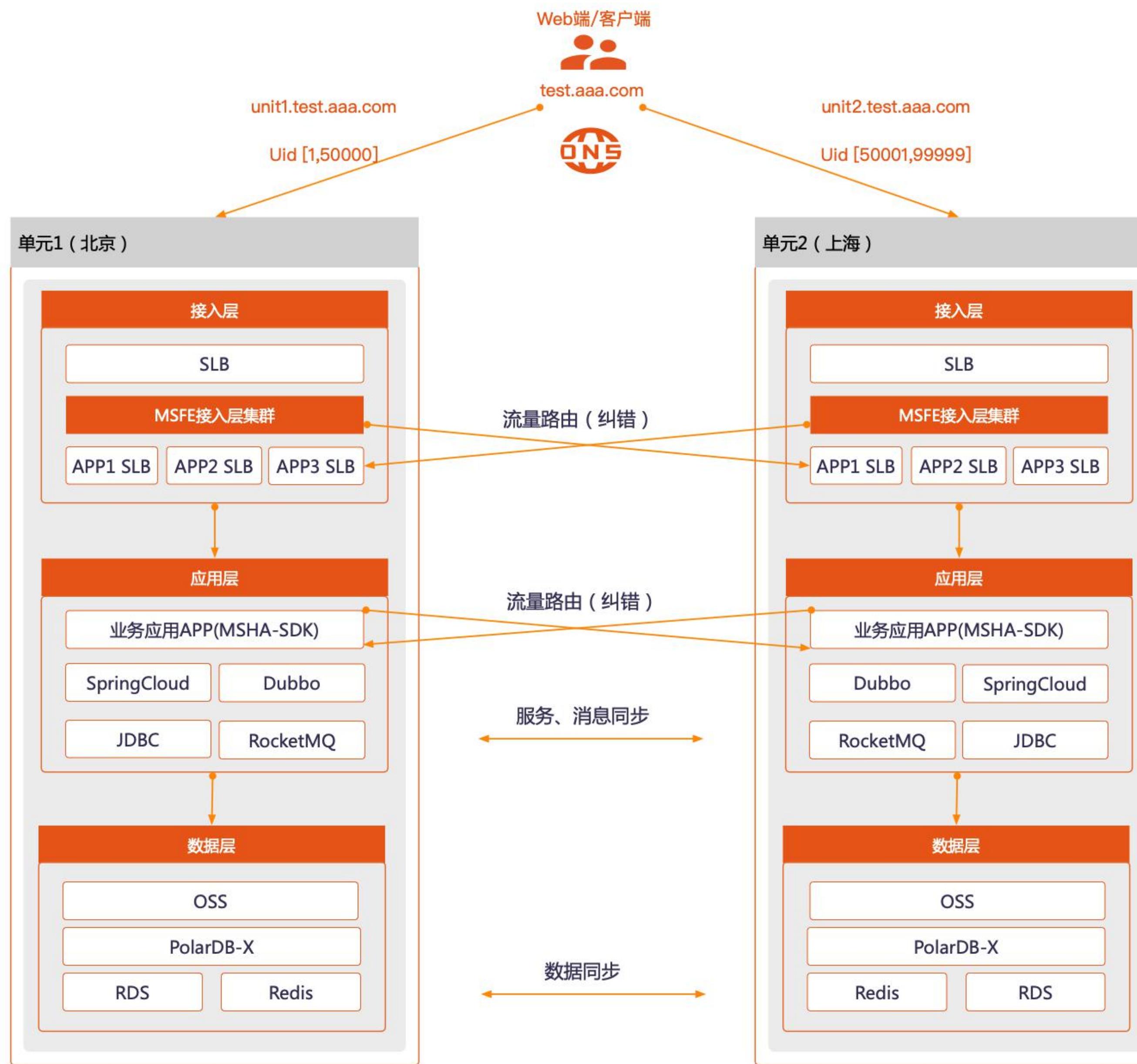


多活接入层组件 + 应用层插件 + 数据层插件 + 数据同步 + 多活控制台
Tengine集群 RPC/MQ/DB数据面插件(SDK/Agent) DTS 管控面Console

多活解决方案 = 技术产品 + 咨询服务 + 定制业务改造方案

异地双活架构

[-] 阿里云



日常态--层层流量管理和数据质量保护的能力：

■ 接入层

• 特性：

- ✓ 自定义分流规则，接入层集群实现入口流量路由和纠错
- ✓ 支持协议：HTTP/HTTPS、WebSocket
- 支持云产品：DNS、SLB、CDN、GTM、HttpDNS...

■ 应用层

• 特性：

- ✓ RPC跨单元调用：RPC路由和纠错，服务双向同步
- ✓ MQ跨单元消费：MQ过滤，消息双向同步
- 支持云产品：EDAS-HSF、RocketMQ...
- 支持开源产品：SpringCloud、Dubbo、Kafka...

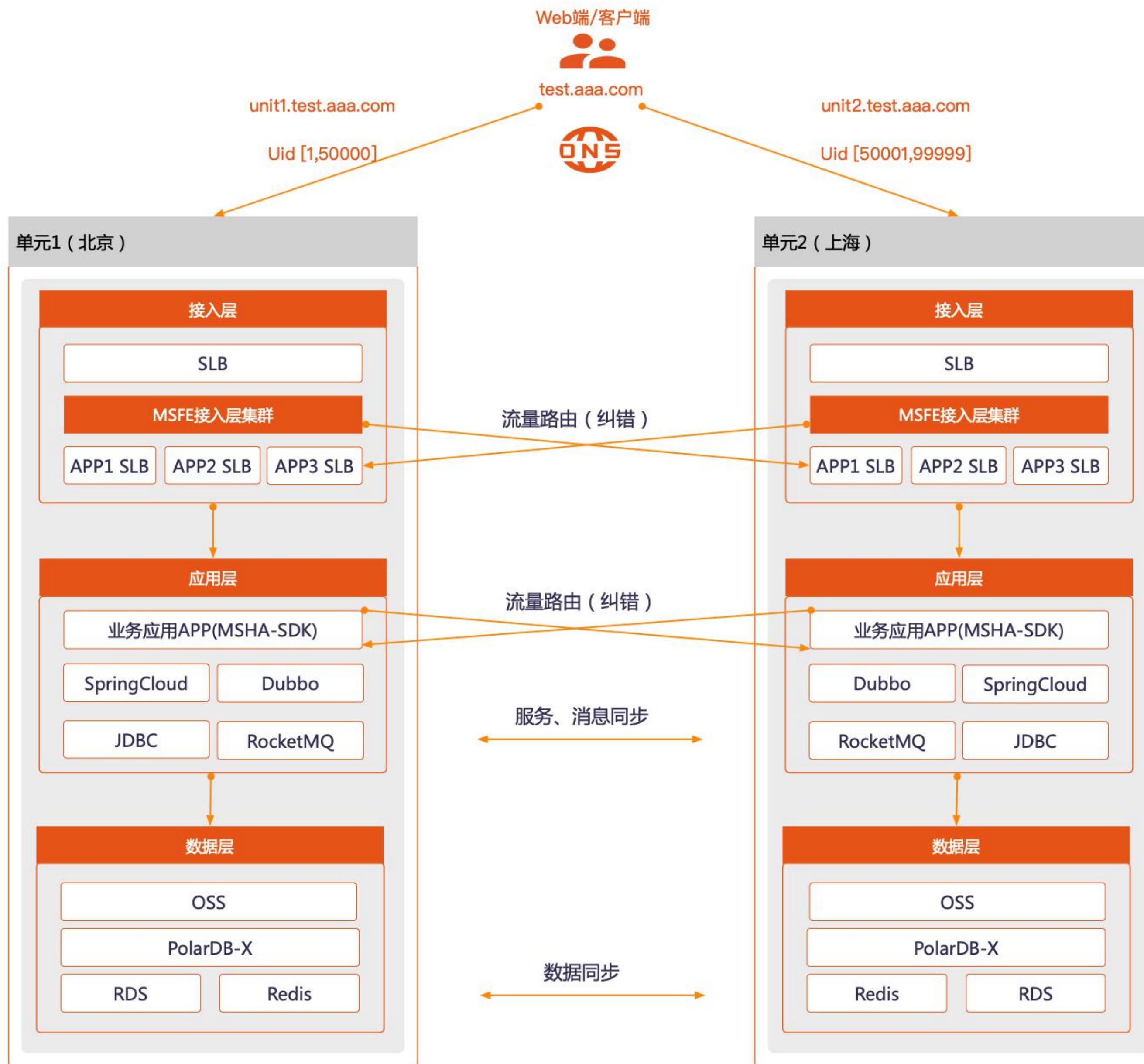
■ 数据层

• 特性：

- ✓ 数据双向同步，防环形复制
- ✓ 数据质量保护，错误流量禁写
- 支持云产品：RDS、PolarDB-X、PolarDB、OB、Tair...
- 支持开源产品：MySQL...

切流引入的问题和风险

[-] 阿里云



I 路由规则下发及时性和高可用

- 新规则推送到MSFE集群和业务应用(MSHA-Agent)--
高可用TCP推送通道 (Pull+Push)

| 流量相关问题

- 纳管DNS，切流时变更DNS流量比例
- 纳管WebSocket，切流时断长连接

| 消息丢失问题

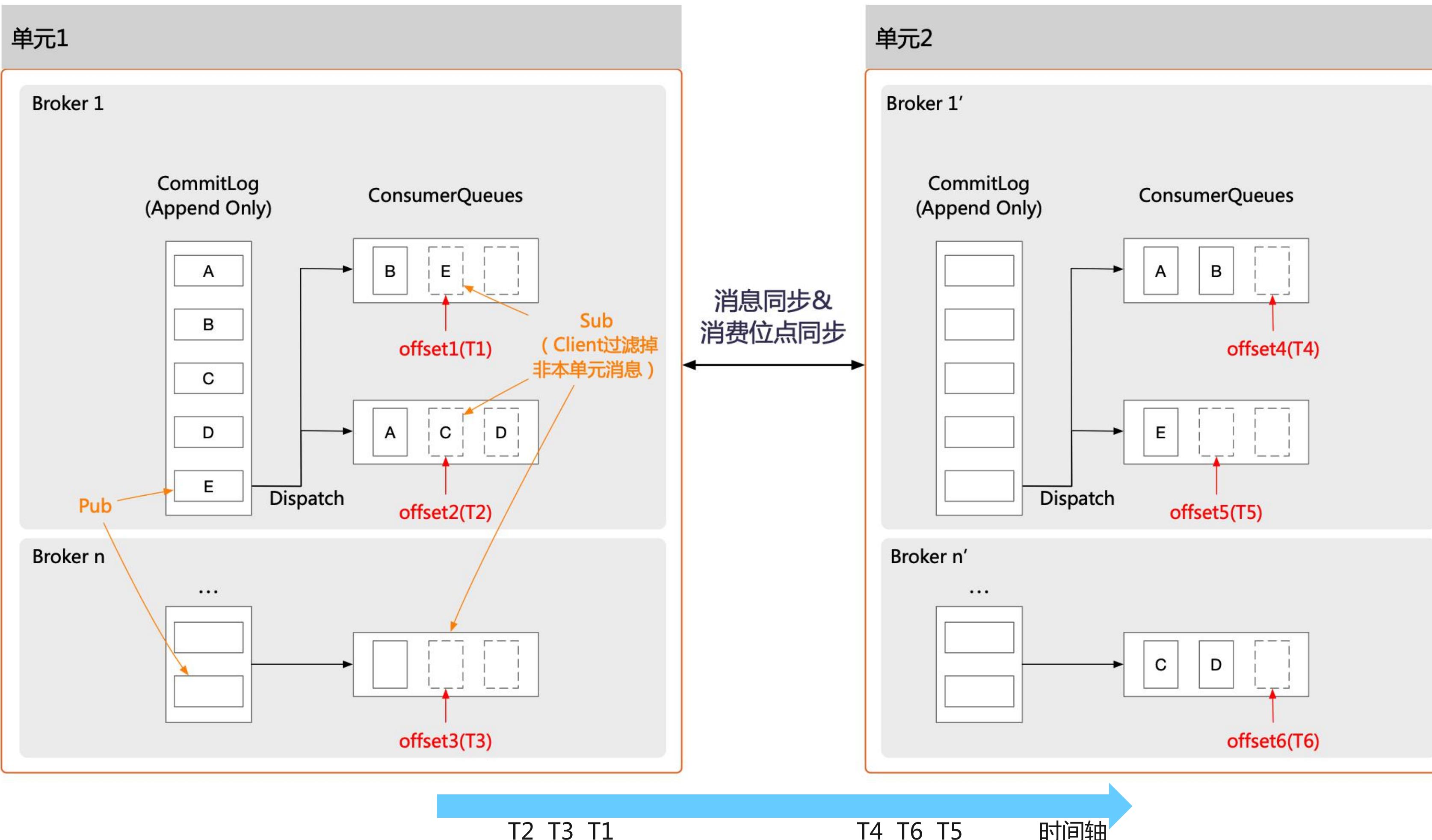
- 源单元未消费的消息，切流后源单元识别为非本单元消息后丢弃

| 数据质量问题

- 切流时，机器路由规则不一致、数据同步未追平都可能导致两单元业务同时写数据，容易造成数据质量问题

切流如何保证消息不丢失？

[-] 阿里云



- 重置时间 = min(源单元位点, 目的单元位点, 切流时间) - 防NTP抖动时间
- eg: 上图重置时间 = min(T1, T2, T3, T4, T5, T6) - 5s

问题

- 切流时, 如何保证在源单元堆积未消费的消息Message C、D、E, 切流后不丢失, 能够在目的单元被消费?

方案--纳管MQ云产品

日常态

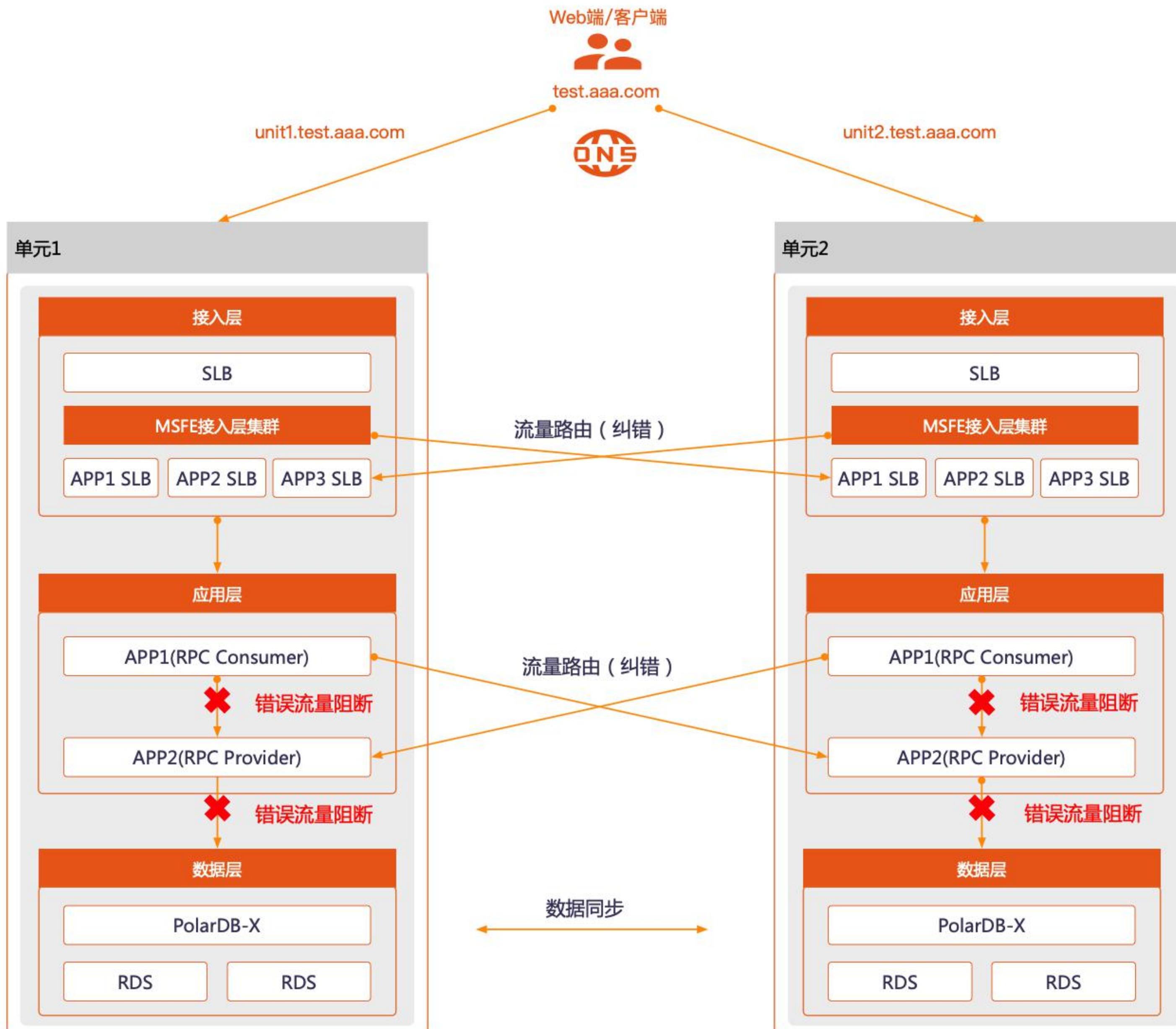
- 消息&消费位点同步
- Client消费时根据routeId路由结果过滤掉非本单元消息

切流态

针对切流目的单元, 进行消费位点重置

切流如何保证数据质量--不脏写？

[-] 阿里云



问题

- ❖ 数据质量问题的核心原因：**数据双写**。切流时，规则下发过程机器规则可能不一致，NTP可能不一致，存在双写的可能
- ❖ 数据同步未完成，目的单元可能读写到旧数据
- ❖ 紧急情况切流，同步延迟严重业务决定放开禁写，目的单元数据更新后可能又因为数据同步造成覆盖

方案--纳管数据库云产品

日常态

- 1) 接入层、RPC Consumer错误流量纠错
- 2) RPC Provider错误流量阻断（单元保护）
- 3) 写数据拦截错误流量阻断（禁写）

切流态

- 1) 绝对禁写。两单元均开启禁写，防止切流规则下发过程机器规则不一致以及NTP抖动造成脏写问题
- 2) 延迟禁写/禁更新。目的单元开启禁写，防止数据未同步完全时出现的脏写问题
- 3) 数据同步开启前镜像匹配。数据未追平时，特殊情况下解除了目的单元的禁写，防止数据同步覆盖目的单元数据



■ 流量管理难度高

- 需要对接入层、应用层、数据层的流量进行统一管理
- 路由规则下发，需要保证众多节点规则的一致性
- 需要具备多维的分流能力，和动态调配能力



■ 数据同步策略复杂

- 需具备服务、消息、数据库、缓存等多种数据的同步能力
- 双向数据同步需解决防环形复制问题
- 远距离数据同步，对同步性能、同步带宽有很高要求



■ 容灾切换数据质量保障难

- 为了保障RPO要求，容灾切换过程中需具备对业务架构的各层进行状态检查的能力
- 对规则分发的收敛情况以及跨数据中心的同步情况进行准确评估，难度较大



■ 多数据中心统一管控难度大

- 需要具备多单元统一管理的能力
- 需要对接众多基础设施、云产品和中间件

阿里云云原生方案优势

(-) 阿里云



■ 阿里多年沉淀

- 阿里13年落地异地多活，阿里云多年的积累和沉淀，在云原生方案上具有诸多优势。



■ 流量精细化管理

- 支持多业务的不同维度的分流策略，满足灵活性
- 流量管理与底层存储解耦，流量按需灵活切换



■ 一体化的解决方案

- 统一管理和路由规则分发
- 从多活建设到容灾演练实现容灾完整闭环



■ 数据质量保障

- 提供多种数据质量保障手段
- 有效控制切流态的数据质量问题



■ 分钟级切换

- 通过“一键切换”能力对各层规则统一管理，可以达到切换RTO分钟级



■ 多活生态

- 深度和阿里云基础设施、云产品、中间件合作
- 未来开放接口，支持生态工具对多活场景的适配

目录

01 为什么做多活

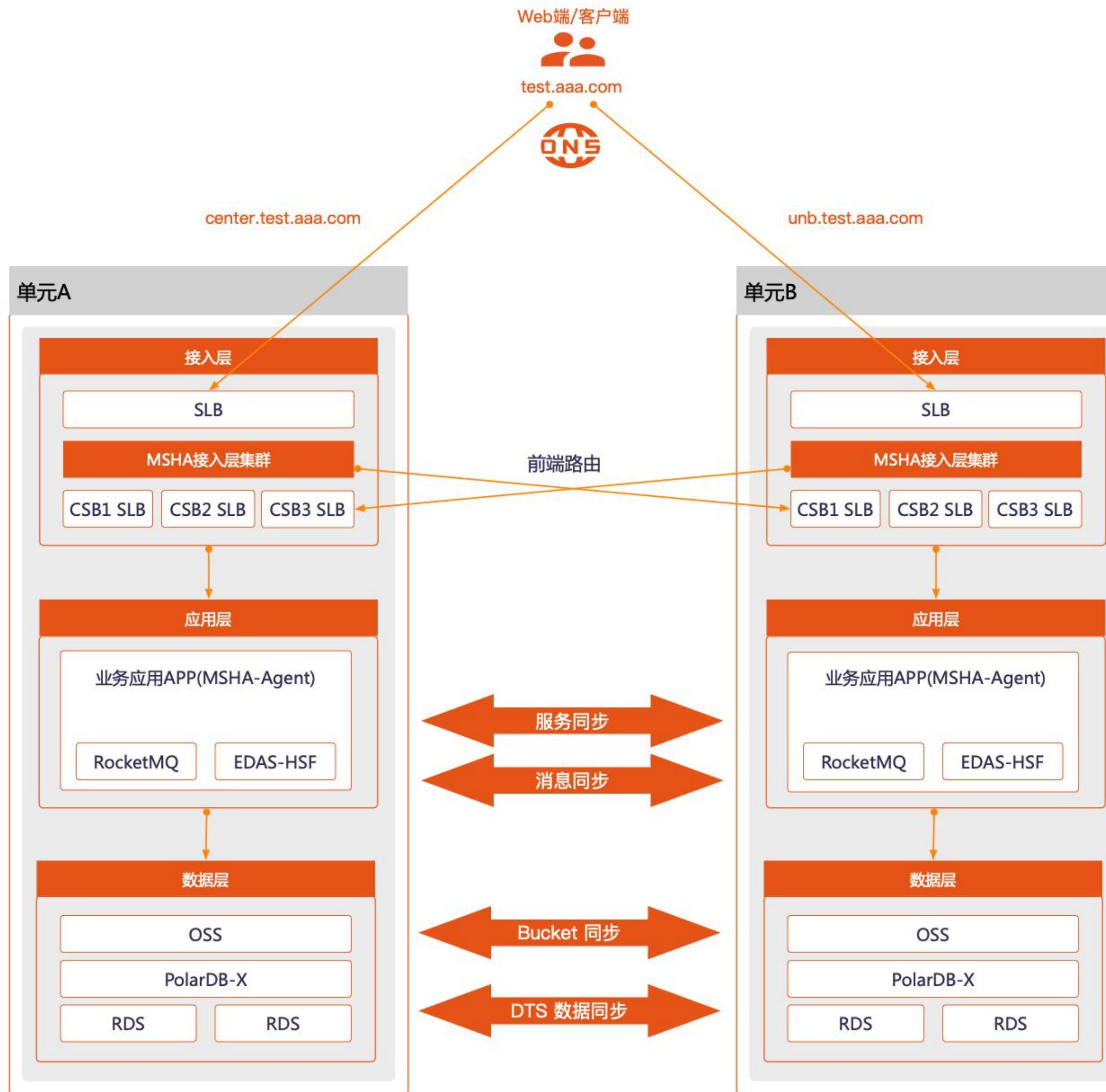
02 多活解决方案介绍

03 客户案例

04 功能演示

异地双活客户案例--某税务核心系统

[-] 阿里云



背景

- 技术栈：EDAS-HSF、企业版MQ、PolarDB-X、RDS
- 容灾能力：项目前单地域部署，RPO、RTO不可控

多活建设方案

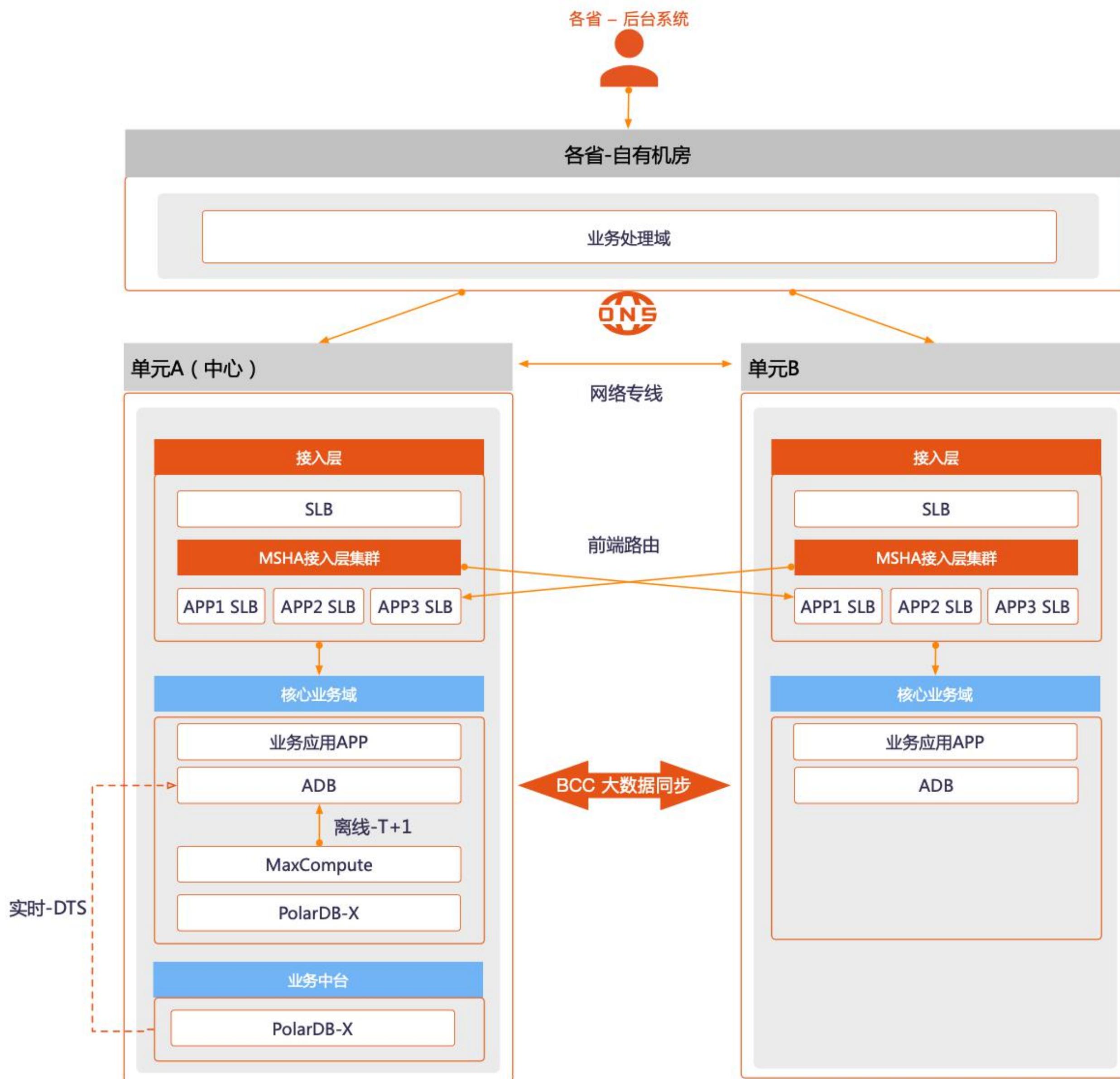
- 接入层：流量按终端用户路由
- 应用层：
 - ✓ 服务、消息双向同步
 - ✓ MSHA-Agent支持错误流量服务调用纠错、消息消费过滤、数据库禁写
- 数据层：数据双向同步

多活实施效果

- 业务核心系统双活，RPO、RTO达到分钟级
- 解决了单地域资源容量问题，解决了数据库单点问题
- 具备灰度放量能力，为技术创新提供了实验田

异地双读客户案例--大数据分析业务

[-] 阿里云



I 背景

- 技术栈：PolarDB-X、MaxCompute、ADB
- 容灾能力：项目前异地灾备部署，RTO不可控，关键时刻不敢切

I 多活建设方案

- 接入层：流量按省份路由
- 数据层：数据双向同步

I 多活实施效果

- 大数据分析业务具备了地域级容灾能力，RTO达到分钟级
- 解决了主数据中心资源瓶颈问题，双活充分利用两单元资源
- 避免了备中心机器闲置资源浪费问题

目录

01 为什么做多活

02 多活解决方案介绍

03 客户案例

04 功能演示

读多写少型业务双读容灾案例

(-) 阿里云

业务背景：电商导购业务

客户容灾现状

- 单地域部署，不具备地域级的容灾能力

客户容灾诉求

- RPO<5min
- RTO<5min (读服务)

客户技术栈

- SpringCloud+ MySQL + Redis

异地双读容灾建设

接入层改造

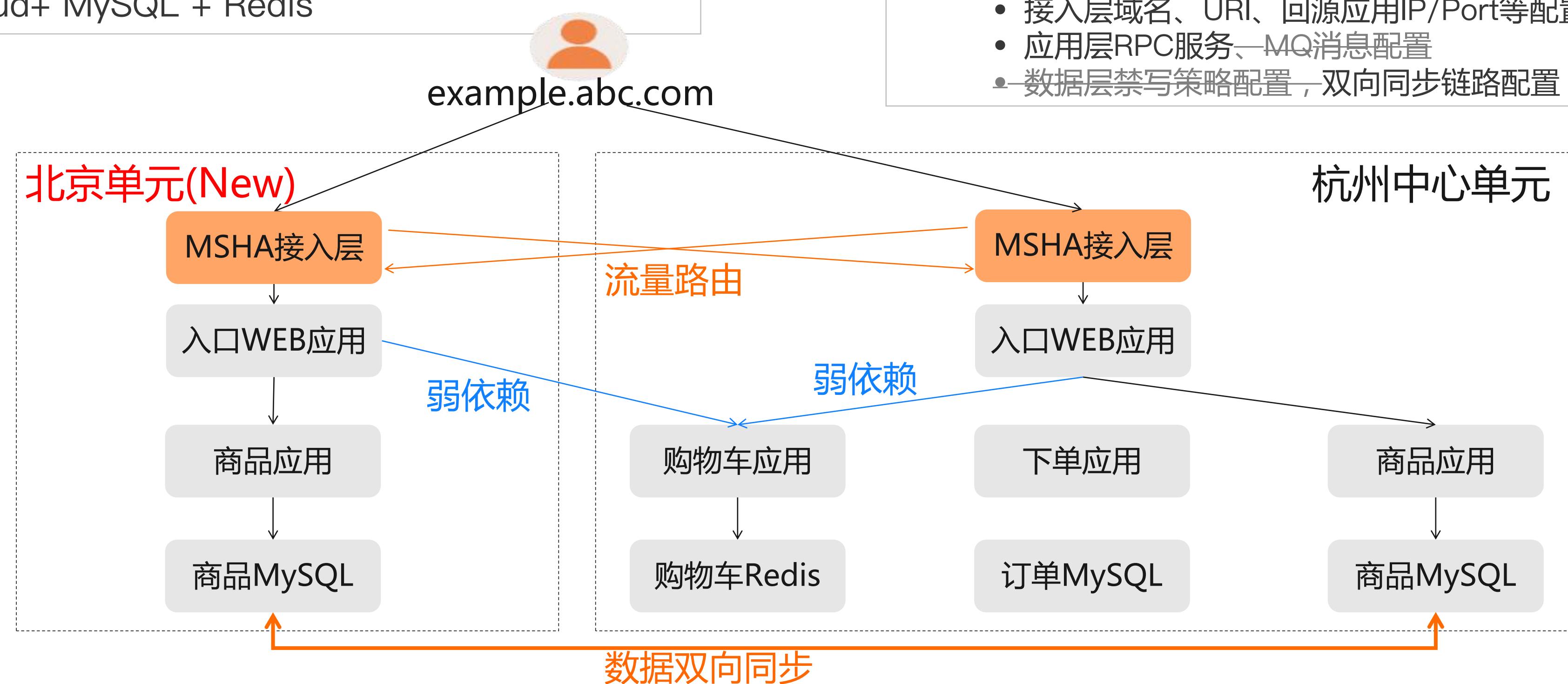
- 入口流量染色，HTTP Header/Cookie 带上路由标识

应用层改造—业务应用安装Agent

- 引入RPC插件，跨单元寻址、调用纠错
- 引入MQ插件，跨单元消费、调用纠错
- 引入DB插件，防脏写保护功能

管控平台进行各层资源配置

- 接入层域名、URI、回源应用IP/Port等配置
- 应用层RPC服务、MQ消息配置
- 数据层禁写策略配置，双向同步链路配置



演示内容：

- ◆ 业务接入MSHA双活解决方案需要进行的配置
- ◆ 接入层流量路由功能
- ◆ 容灾恢复功能—切流快速恢复业务 (RTO: 分钟级)

交流探讨FAQ

□ 交流探讨：

- 你的业务怎么做容灾的，目前容灾能力达到什么水平？
- 你的业务开始做多活了吗，遇到了哪些困难？

□ 延伸阅读

- MSHA x Chaos 容灾高可用实践 <https://developer.aliyun.com/article/780311>
- 读多写少型业务场景多活实践 https://help.aliyun.com/document_detail/196866.html
- 流水单据型业务场景多活实践 https://help.aliyun.com/document_detail/196873.html

□ 咨询和试用

公有云MSHA正在公测中，可进钉群咨询和申请试用

多活容灾交流钉钉群
群号：31623894





阿里云