

QCon 全球软件开发大会 【北京站】2016

蚂蚁金服 金融级异地多活架构

刘浩(庄辛)
技术风险部

背景

容量和容灾等问题在各个微观层面上都影响着蚂蚁金服各项业务的飞速发展。

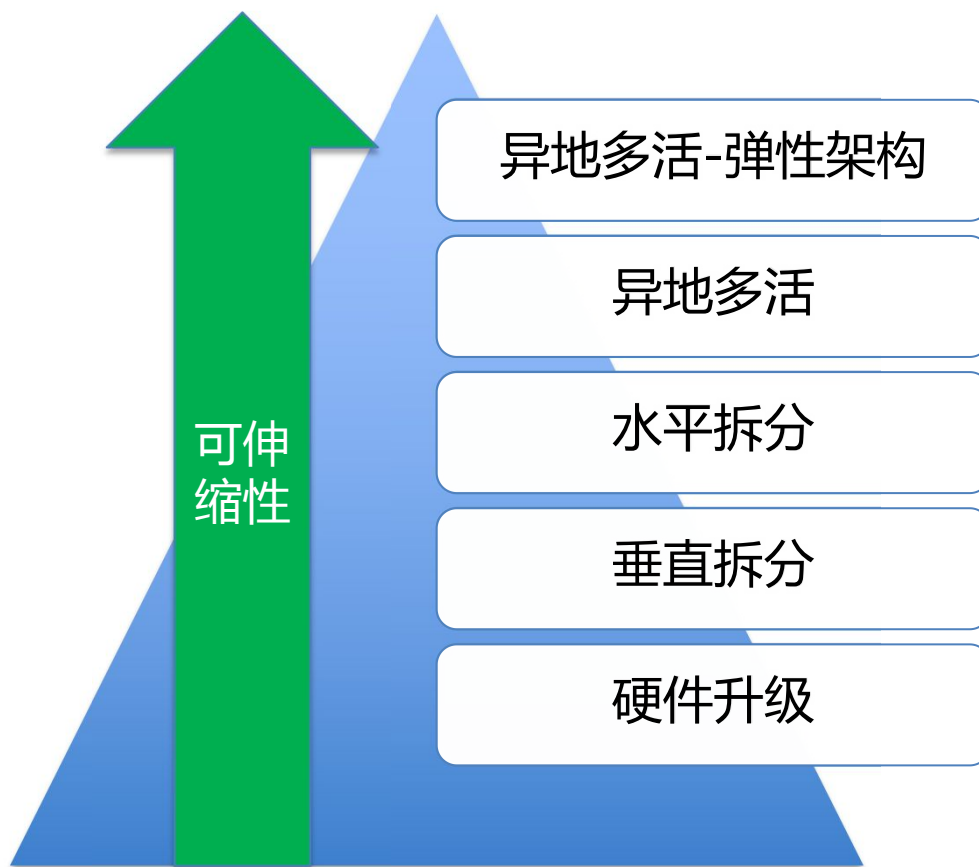
通过“异地多活”架构，将蚂蚁金服各业务的核心应用链条封装在一个IDC单元、在不同地域部署多个这样的单元。

这一方面能够保障在未来3~5年的业务峰值处理能力，另一方面实现异地的容灾能力全面降低**核心业务**的技术风险。

异地多活 vs 两地三中心

方案	容量	容灾	成本
异地多活	<p>[优]基于逻辑机房，容量可伸缩的运维架构</p> <p>[优]容量可异地伸缩</p>	<p>[优]日常运行，容灾时可用性高。</p> <p>[劣]受城际网络故障影响，影响度取决于横向依赖程度</p>	<p>[优]IDC、应用等成本在日常得到有效利用。</p>
两地三中心	<p>[劣]仅可部署在一个城市，容量伸缩有城市级瓶颈</p>	<p>[劣]灾备设施冷备等待，容灾时可用性低</p>	<p>[劣]容灾设施等成本仅在容灾时才使用，且受制于可用性</p>

异地多活@容量 | 能力模型



异地多活 | 核心挑战

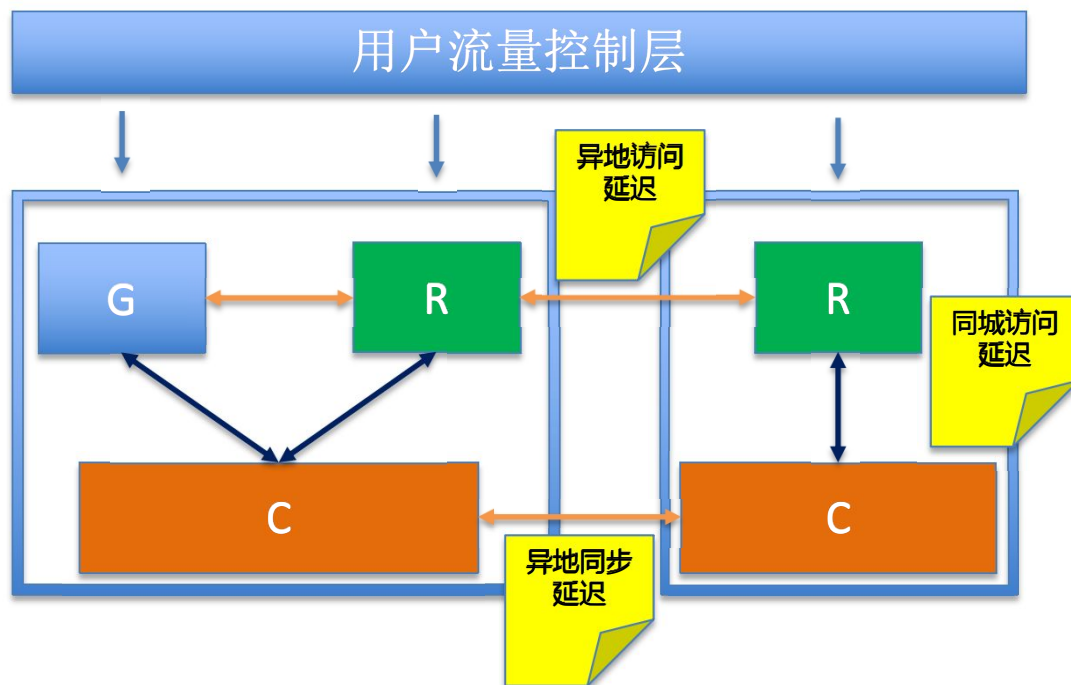
- 异地物理距离带来的延迟：
 - 物理距离在1000公里以上的异地部署，基本能实现全国部署的能力。整个链路上如果有多次异地访问的话，支付耗时将明显增加从而影响用户体验。
- 有状态数据的分区和流量调拨：
 - 将核心应用依赖的有状态数据分区到IDC单元中，才能实现核心应用链条封装在一个IDC单元。选择粒度合理、分布均匀的数据分区维度，将决定整个链路的流量调拨，如网络接入、应用间调用和数据路由。并且在复杂的金融业务背景下，**不是所有数据都适合按一个维度分区**。

蚂蚁金服异地多活(LDC)架构

在蚂蚁金服内部，“异地多活”技术的落地是通过LDC(Logical Data Center)架构来实现的。

在LDC架构中，一个单元被称为一个zone，共有3种不同单元种类的zone。

- **用户单元 (R) :**
按用户维度，水平sharding
- **数据单元 (C) :**
数据全量的在各个城市间复制
- **全局单元 (G) :**
部署了非核心的数据和应用。



LDC架构如何解决异地核心挑战

•流量调拨：

- 无用户ID流量，路由到随机用户单元，待业务应用做用户鉴权后按有用户ID流量处理；有用户ID流量，可以在访问开始点上做方案直接路由对应用户ID的用户单元，或者在业务应用中做流量转发。

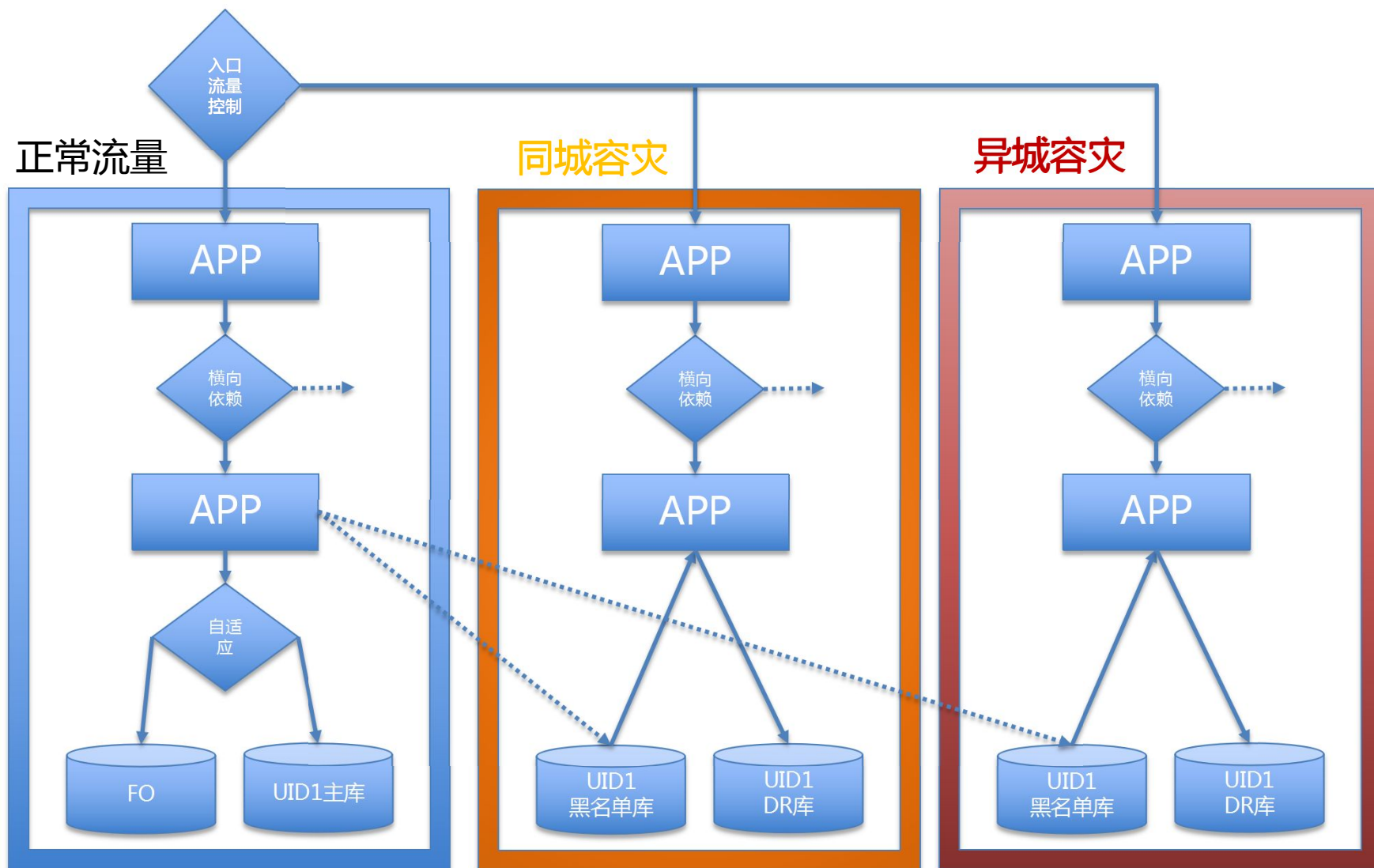
•有状态数据的分区：

- 用户ID相关的事务型数据库部署在各个用户单元的IDC中。全局数据部署在数据单元中，采用数据复制方案或者多点写方案保证多城市数据最终一致性。

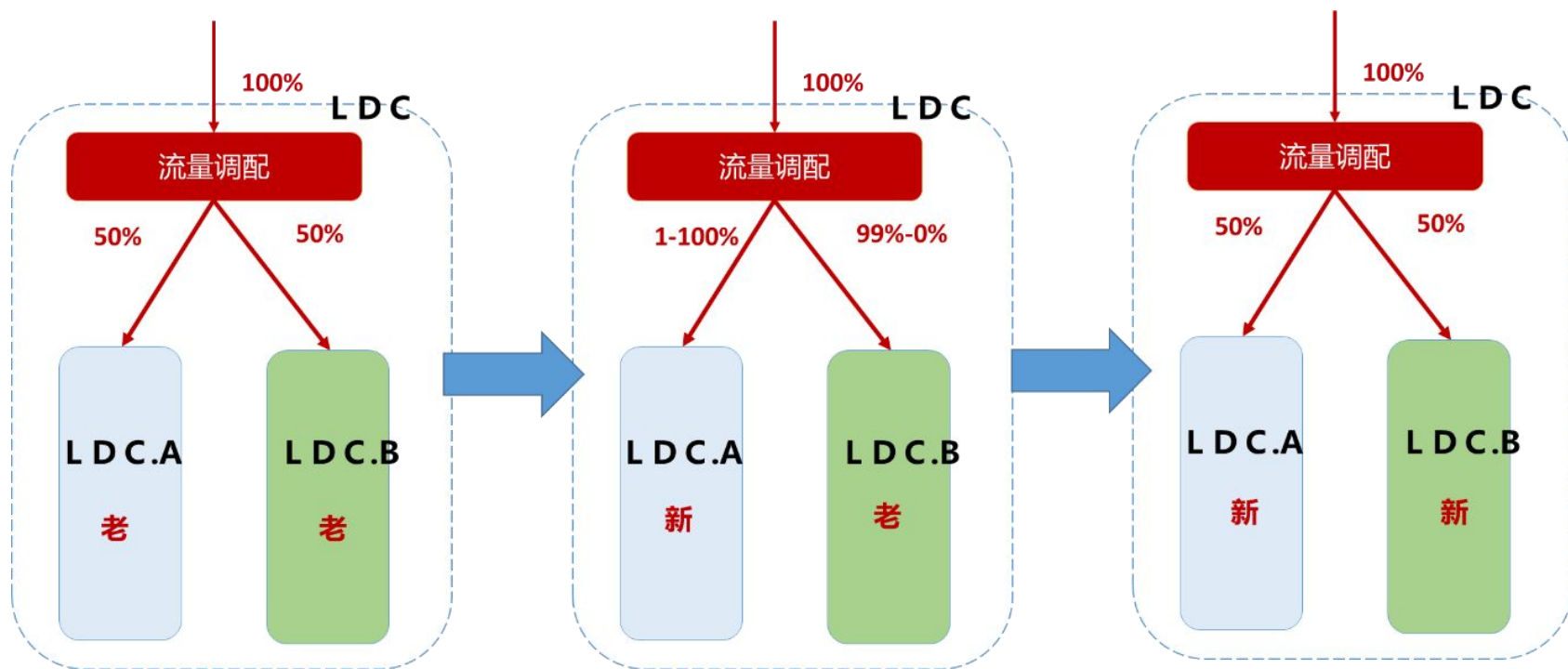
•异地物理距离带来的延迟：

- 业务上尽量地减少和聚集用户单元之间的访问，而基础的数据单元，通过数据时效性延时换来数据访问延时的优化。

异地多活@容灾 | 异地容灾



异地多活@容错 | 蓝绿发布



- Step1.发布前，将“蓝”流量调至0%，对“蓝”的所有应用整体无序分2组发布。
- Step2.“蓝”引流1%观察，如无异常，逐步上调分流比例至100%。
- Step3.“绿”流量为0%，对“绿”所有应用整体无序分2组发布
- Step4.恢复日常运行状态，蓝、绿单元各承担线上50%的业务流量

总结

- **能够保障蚂蚁金服业务的业务峰值处理能力：**

- 2015年“双十一”活动，蚂蚁金服旗下的支付宝平稳支撑起了8.59万笔/秒的交易峰值，这一数值也让支付宝超越Visa，成为**全球处理能力最强的支付平台**。

- **金融级的容灾能力：**

- 在LDC架构框架下配合保障核心业务持续可用性的Failover技术，异地多活技术的容灾能力达到了国家标准的第五级(GB/T20988)。

Q&A

联系方式:

庄辛(刘浩)

蚂蚁金服-平台产品技术部-技术风险部-高可用架构组

Email: hao.lh@alipay.com

欢迎交流:

专注于高可用、高性能、成本优化的金融级架构设计与实施。



THANKS!