

DTCC

数 / 造 / 未 / 来

第十二届中国数据库技术大会

DATABASE TECHNOLOGY CONFERENCE CHINA 2021

2021 年 10 月 18 日 - 20 日 | 北京国际会议中心



阿里云RDS安全体系和自治服务

王颜培

阿里云数据库技术专家



数 / 造 / 未 / 来





CONTENT

● 01 阿里云RDS简介

● 02 RDS的安全可信体系

● 03 DAS自治服务在阿里集团的实践





阿里云RDS简介



国内规模最大最稳定的云数据库



云原生技术演进

IaaS+PaaS垂直整合优化
全面CPU/内存/存储池化
On ESSD云盘百万IOPS



三节点企业版

十年双十一锻炼
自研MySQL内核
保证RPO=0
阿里集团能力输出



MySQL



PostgreSQL



MariaDB



SQL Server

DAS智能化加持
SQL自动限流、诊断优化、自动扩缩容

K8S云原生多租户
CPU和内存资源池化

计算与存储分离
存储资源池化

高性能云服务器ECS
(神龙架构)

云存储
(ESSD 云盘)



智能化加持

DAS加持，迈入自治时代
智能算法、自诊断、自优化



丰富的企业级能力

4个9高可用，稳如泰山
全链路安全
(TDE/BYOK/SSL/落盘加密)
差异化内核能力，超越自建性能

能力持续进化

RDS MySQL三节点企业版
RDS MySQL 8.0发布
RDS 支持ESSD云盘，百万IOPS
RDS 支持32TB存储
RDS 支持跨域备份&容灾恢复
RDS 云盘秒级快照&秒级恢复
RDS 支持库表级备份恢复
RDS 支持全链路安全
RDS MySQL支持企业级线程池
RDS MySQL支持独享代理
RDS MySQL Statement Outline
RDS MySQL Recycle Bin





RDS的安全可信体系



数据安全大事件

□ 事件一: 超5万台MongoDB数据库实例被勒索

2017年1月、9月, 黑客通过在互联网上扫描开放外部连接的MongoDB数据库, 入侵了超5万台服务器, 删除数据并留下勒索信息。

□ 事件二: Gitlab误删库事件

2017年1月, “Gitlab误删库事件” 导致300GB数据被误删, 差不多6小时的数据丢失, 影响约5000个项目, 5000个评论和700个新用户账户。

□ 事件三: 2.4亿条酒店开房记录 (疑似) 被转卖

2018年, 国内某知名连锁酒店数据以8个比特币在暗网转卖, 其中包含了1.3亿条个人信息、2.4亿条酒店入住登记信息。

□ 事件四: 删库跑路事件

2020年2月, 因公司内部员工恶意破坏线上生产环境数据, 导致服务不可用超过120小时, 股价暴跌22%, 市值缩水超30亿港元。

.....



RDS安全体系 - 功能大图

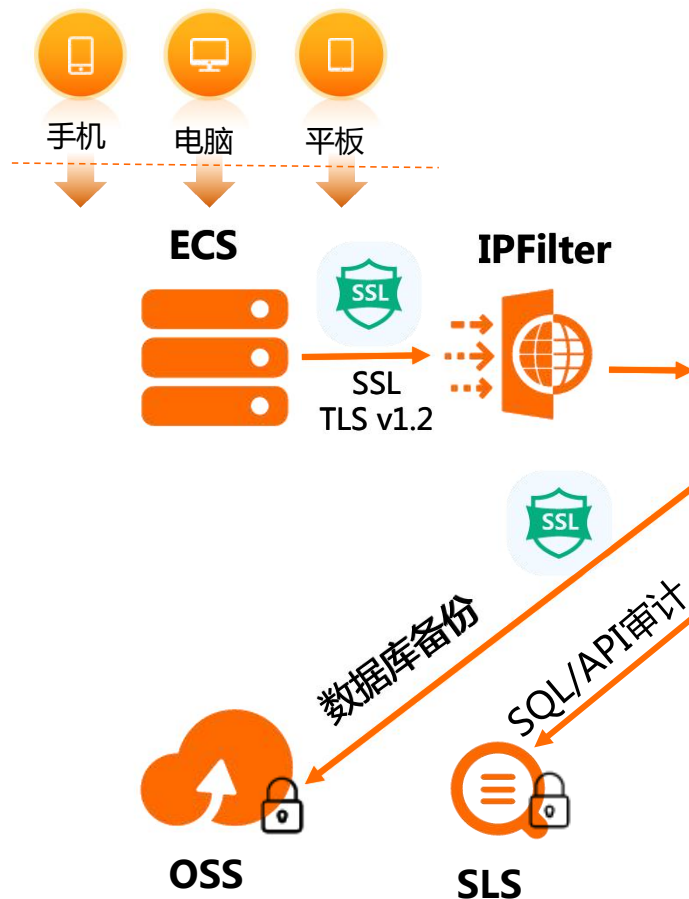


RDS安全体系 - 全链路生命周期



RDS安全体系 - 最严格的安全合规

Computer & Mobile Apps



事前防范

权限管控: 用户权限管控

用户名密码: 用户名和密码完全匹配

ACL: 访问控制

白名单: 允许的客户端IP才能访问

VPC/SG: 应用ECS与RDS相同VPC/SG,网络隔离

事中保护

SSL: SSL证书防中间人欺骗

TDE: 透明数据加密, 防拖库

BYOK: 用户自带密钥

云盘加密: 基于KMS Key的落盘加密

备份加密: 数据库备份文件加密

事后审计

SQL审计: 全量SQL审计日志

API审计: 全量API调用审计日志





DAS自治服务在阿里集团下的实践



阿里集团数据库的业务特性

Digital Media & Entertainment



Core E-Commerce



Local Services



Financial Service



Logistics



Marketing



Cloud Computing

超大规模实例集群
超大研发用户群体

任何故障会导致
业务的巨大损失

双十一零点高峰热点



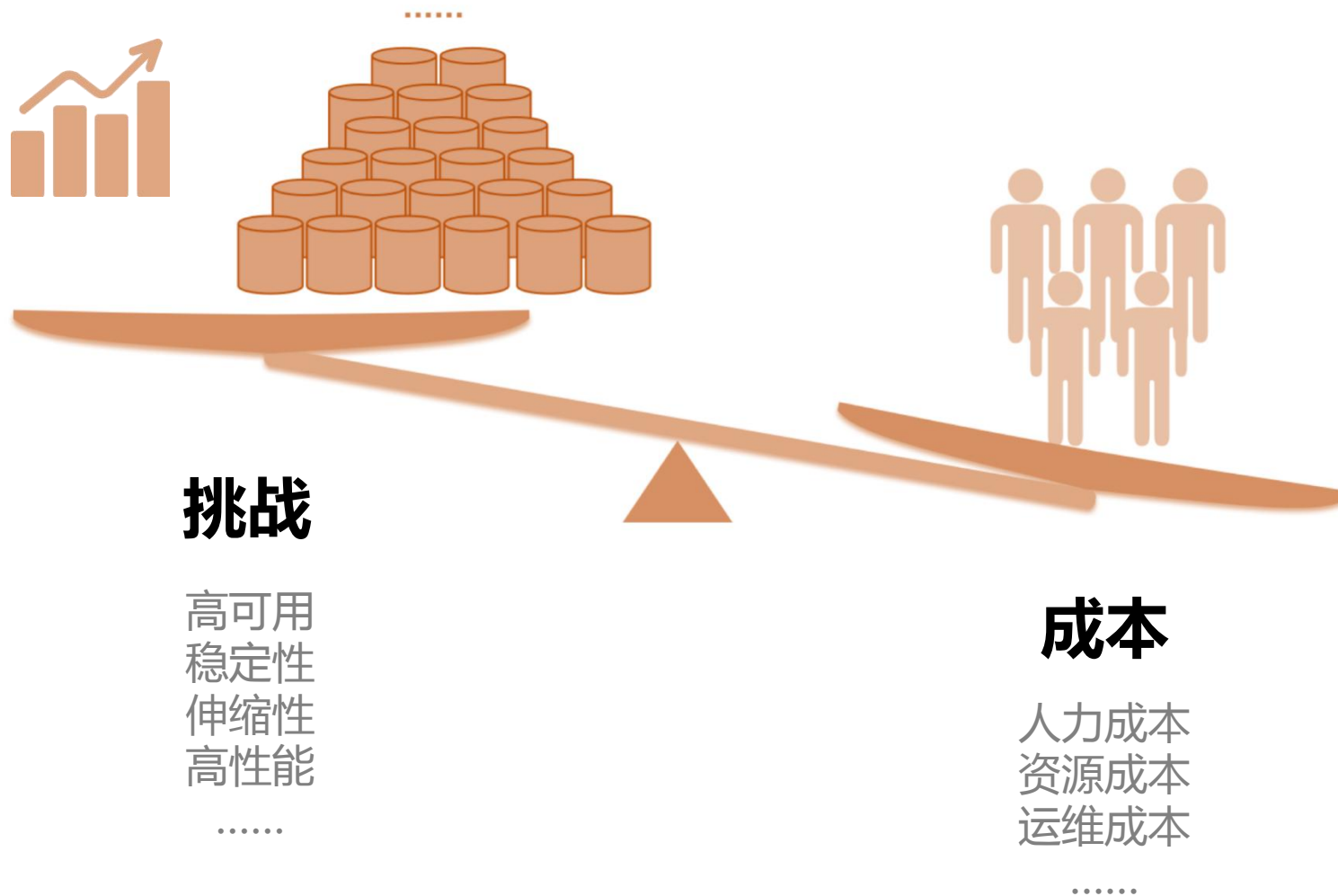
数 / 造 / 未 / 来



阿里集团的数据库挑战



DTCC 2021
第十二届中国数据库技术大会
DATABASE TECHNOLOGY CONFERENCE CHINA 2021



数，造，未，来



云原生+智能化数据库管控平台



阿里巴巴实践：

- 90% 人力成本下降
- 4.6PB 存储优化
- 12% 内存优化
- 4900万 全网慢SQL优化

数据库云服务平台，数据库自治服务DAS

自动优化

SQL优化

全链路优化

自动异常修复

异常定位

异常修复

自动安全保护

安全诊断

安全修复

容量自动管理

资源预测

容量弹性

基于K8S+容器的资源管理与编排调度



数，造，未，来



自动SQL限流&优化

□ 7x24小时异常检测

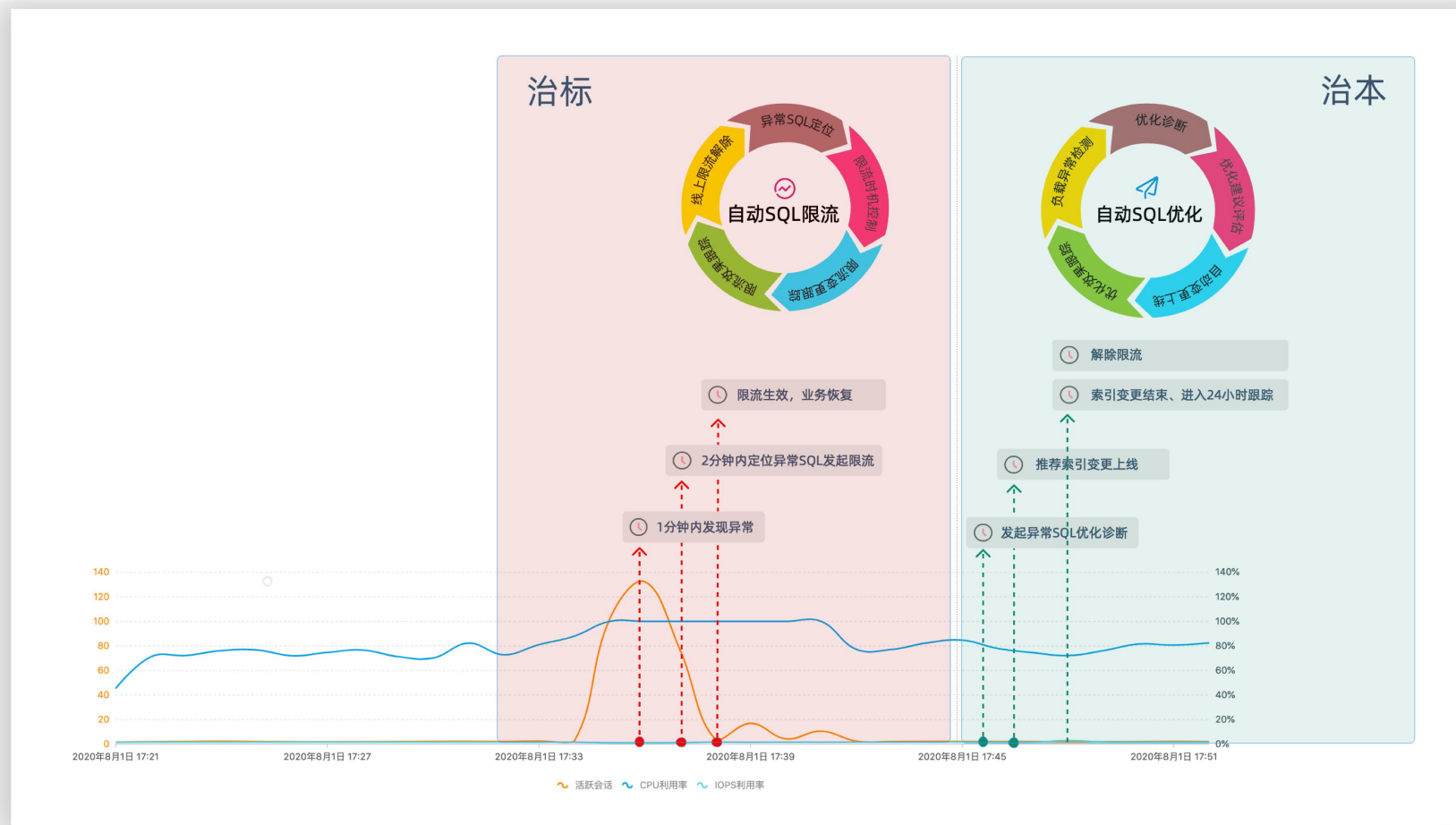
- ✓ 检测范围更广
- ✓ 准实时的检测
- ✓ 具备周期性识别能力

□ 故障自愈

- ✓ 自动执行相关止损操作
- ✓ 满足“1-5-10”异常自愈能力

□ SQL自动优化

- ✓ 索引，语句改写推荐
- ✓ 自动SQL优化闭环
- ✓ 24小时的优化效果跟踪评估



□ 支持基于策略的自动弹性能力

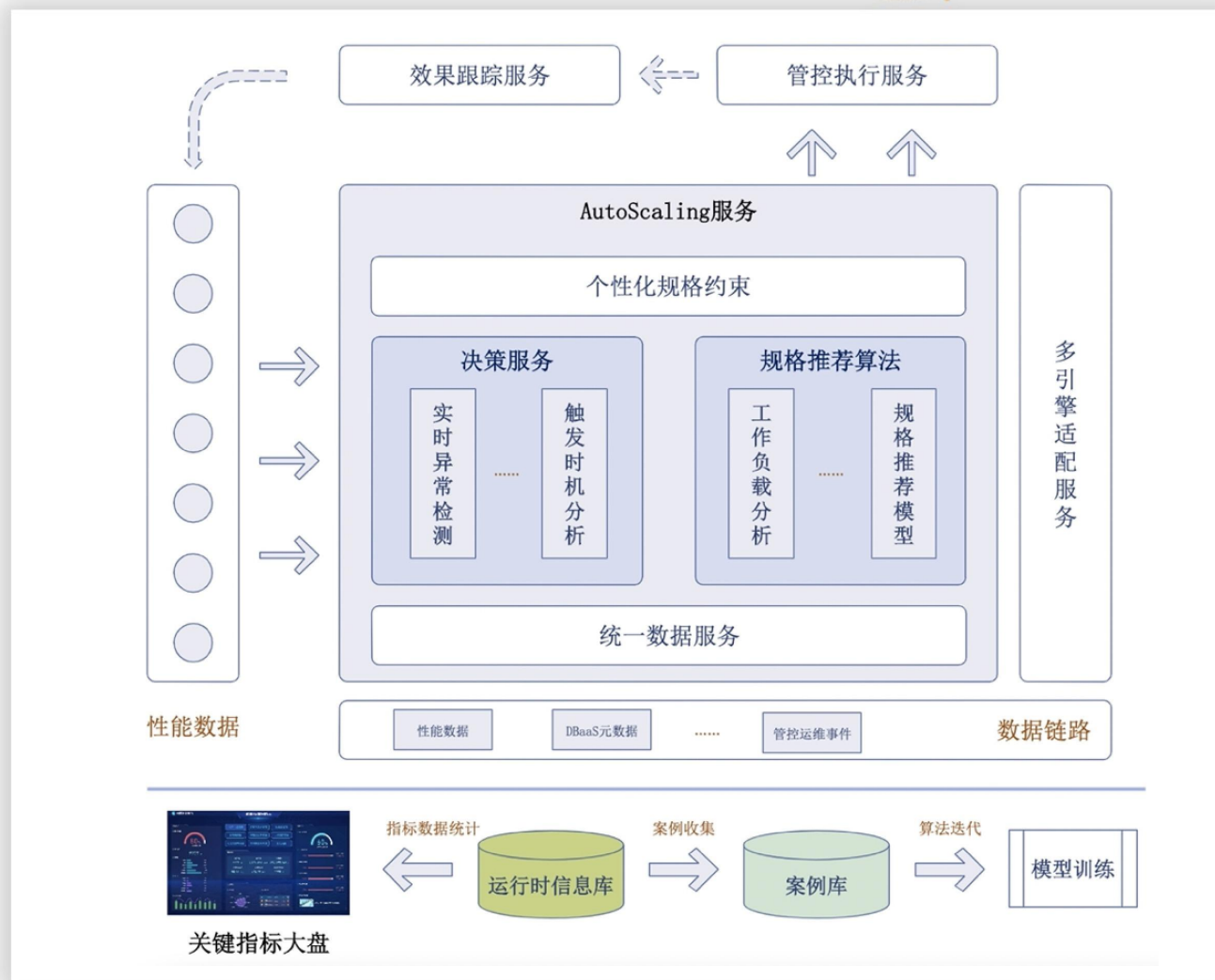
- ✓ 规格弹性
- ✓ 存储扩容

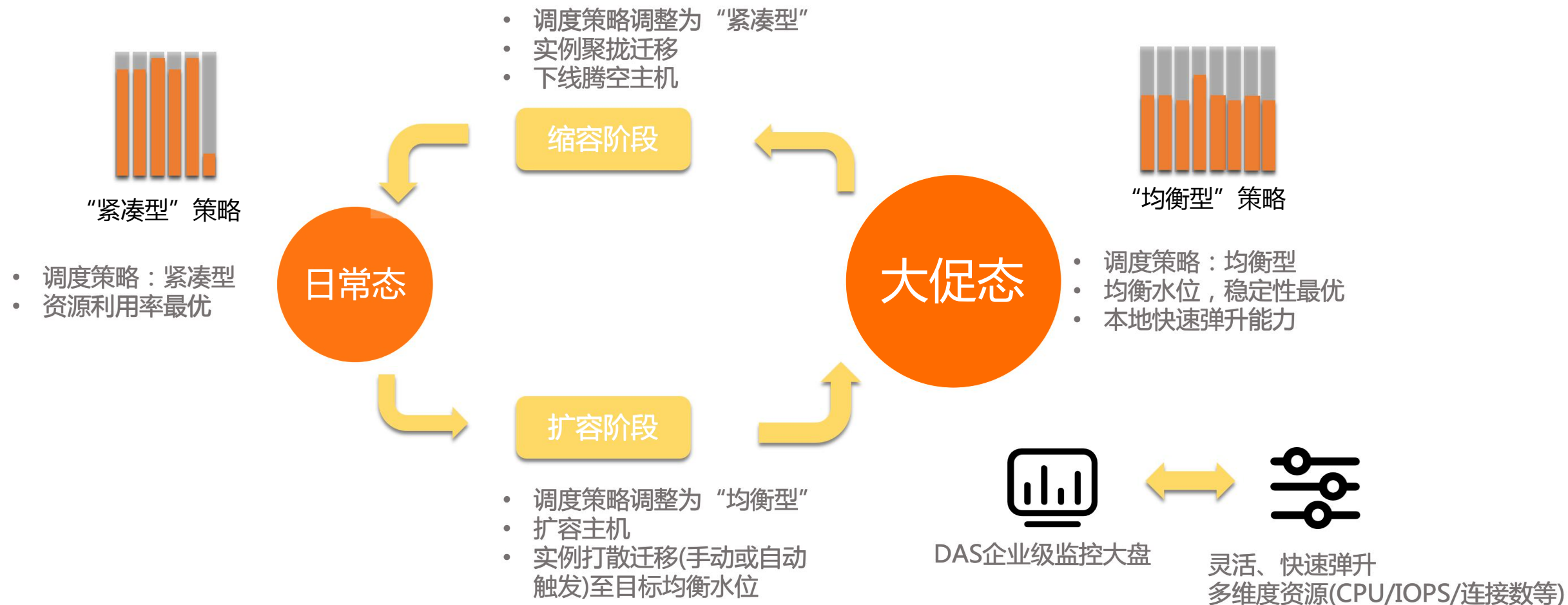
□ 应对突发流量

- ✓ 高低峰业务
- ✓ 突发流量
- ✓ 周期性但周期性短业务

□ 降低成本

- ✓ 规格灵活
- ✓ 低成本自动扩容







THANKS