

基于信创云的双活建设

王辉 | 太保科技数智研究院

演讲议程

- 01 项目背景与挑战
- 02 核心方法论
- 03 解决方案架构
- 04 技术实现详解
- 05 两地三中心部署模式与灾难应对
- 06 实施效果与经验

01 项目背景与监管挑战

监管合规压力

- **2019年银保监发29号文**：重要业务中断30分钟需作为突发事件上报
- **2024年金融监管局11号文**：重要系统须具备同城和异地灾备能力大型机构应具备完全接管并可长期运行主要业务的能力

业务挑战

- 保险业务7×24小时连续运行要求
- 传统架构灾备切换时间长(RTO>2h)
- 数据丢失风险高(RPO>15min)
- 信创转型过程中的兼容性挑战

关键技术指标

RPO

0

数据零丢失

RTO

<20分钟

快速恢复业务

可用性

数据中心级

机房级双活

架构

两地三中心

同城双活+异地灾备

02 核心方法论："8横4纵"高可用能力层次体系

横向：8个关键路径层次

① 互联网入口/核心网络层

② 负载均衡层/GSL

③ 安全防护层

④ WEB接入层

⑤ APP处理层

⑥ 分布式中间件层

⑦ 数据库处理层

⑧ 数据存储层

纵向：4个高可用级别



数据中心级

太保目标等级 ★



机柜级

机柜故障可切换



节点级

节点故障可切换



部件级

部件故障可切换

02 规划先行、渐进实施

01 规划先行

核心逻辑：锚定价值，分级施策

引入业务连续性分级模型，从财务影响、客户体验及合规风险维度对系统进行价值定级，优先保障核心业务链路，避免资源错配。

关键产出：形成可落地的实施路线图，配套全流程风险预案，为架构建设提供清晰的顶层设计与优先级指引。

02 渐进实施

实施策略：试点先行，稳步推广

拒绝“一刀切”，优先选择业务价值高、依赖关系简单的非核心系统作为试点，验证技术方案与操作流程，沉淀标准化实施经验。（如车险移动理赔、寿险银保通、集团资金平台等）

实施优势：低成本试错，逐步建立团队技术与运维能力，确保核心系统迁移时的平稳过渡，最大程度降低业务中断风险。

03 运维保障

全链路监控体系

覆盖双活架构的网络、存储、数据库同步延迟及应用状态，实现故障秒级发现与告警。

常态化切换演练

定期开展无预告故障演练，模拟真实灾备场景，验证切换流程的可靠性与团队应急能力。

动态化预案迭代

基于演练反馈持续优化应急预案，明确故障分级与处置流程，确保极端场景下有章可循。

03 解决方案架构："一个中心、四个支撑"

核心理念：为"8横4纵"各关键路径的双活实现提供平台级解决方案

一个中心

应用系统双活建设

实现重要业务及其强依赖业务系统的数据中心级双活

信创双活云

计算/存储/网络/数据库/中间件/安全

混合云管平台

统一纳管双活能力发放、演练、应急等

配套基础设施

CMDB/监控/自动化运维

业务连续性平台

容灾演练/切换编排

03 整体解决方案架构

双活数据中心

同城双活部署
双中心同时对外服务
故障自动切换

分布式架构

微服务容器化
弹性伸缩能力

智能流量调度

全局负载均衡
健康检查机制
智能路由算法

数据同步机制

实时数据复制
一致性保障

04 信创双活云：同城双活+第三数据中心仲裁

数据中心1 AZ

生产中心A

- 业务双活部署
- 同城容灾
- 计算/存储/网络
- 数据库/中间件

双向延时 $\leq 1.5\text{ms}$

数据中心2 AZ

生产中心B

- 业务双活部署
- 同城容灾
- 计算/存储/网络
- 数据库/中间件

双向延时 $\leq 1.5\text{ms}$

第三数据中心AZ

灾备+仲裁

- 仲裁服务
- 部分云产品副本
- 异地数据备份
- 应用异地容灾

绕行延迟 $\leq 3\text{ms}$

网络架构要求

- 三机房两两光纤传输双向延时 $\leq 1.5\text{ms}$ ，绕行延迟 $\leq 3\text{ms}$
- 单AZ网络故障时，流量可通过另一AZ绕行
- 结合成都灾备云实现"两地三中心"完整架构

04 网络GSLB整体技术方案



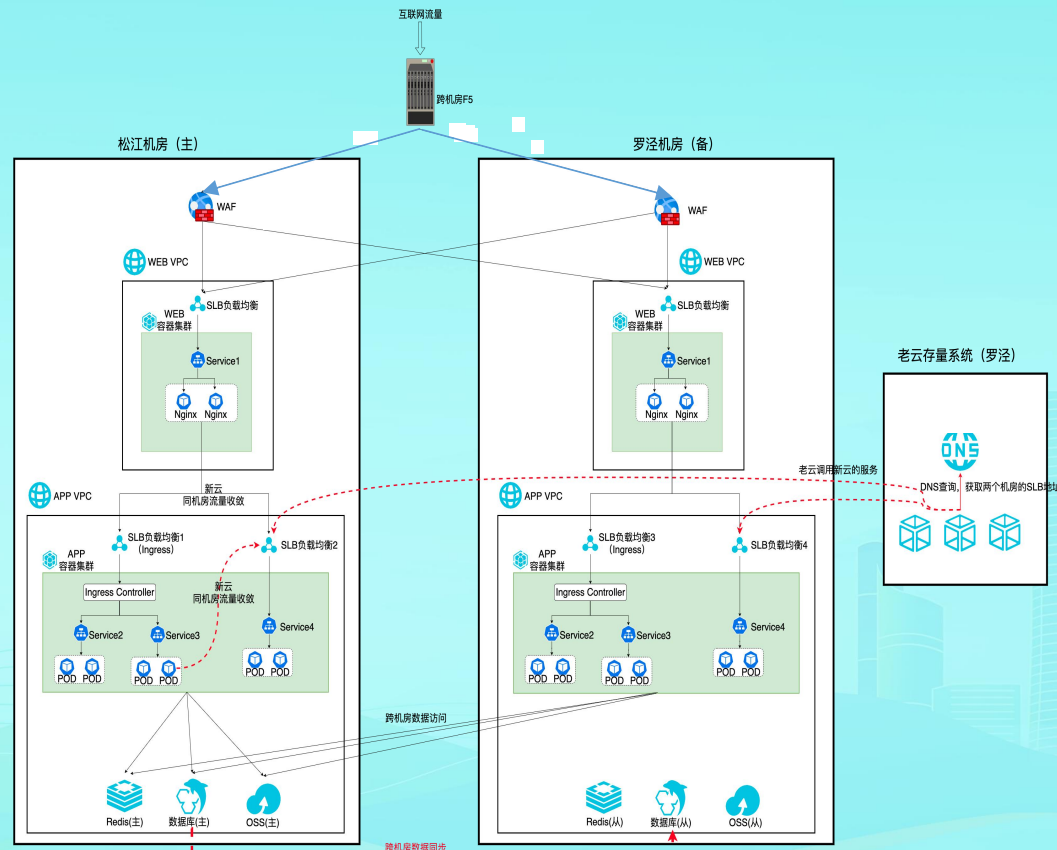
互联网GSLB

- 多AZ NS委派 (轮询)
- GSLB同步组实时同步wideip业务配置
- 多层GSLB调度算法:
 - 一级策略: 地域+运营商 (Topo)
 - 二级策略: GA优先级



内网智能DNS

- 分布式DNS部署、就近DNS解析 (Anycast发布)
- 动态健康状态联动检查及切换
- 基于Ratio比率算法, 按需流量分发模型



04 技术实现详解：数据库中间件层双活方案

数据库类型	产品	双活架构方案
关系型数据库	OceanBase	5副本或3副本部署同城三AZ，单AZ故障后剩余两AZ满足多数派
关系型数据库	达梦	一机房主备数据守护集群+另一机房两异步备机，确认监视器集群管理
关系型数据库	TD-SQL	两地三中心5副本，任意2台故障不影响服务
非关系型数据库	MongoDB	主备机房3节点副本部署，故障后Hidden节点提升为Primary
缓存	Redis	双机房各1套集群组成逻辑集群，HA服务巡检触发切换

技术亮点：多数据库适配能力，同时支持OceanBase、达梦、TD-SQL等信创数据库的双活方案，满足不同业务场景需求

04 应用系统双活技术方案对比

传统双活方案

当前主推

- 应用跨数据中心部署
- 数据库/中间件/网络跨中心组成双活/分布式/主备集群
- 两中心应用访问同一集群
- 改造量较小、快速落地

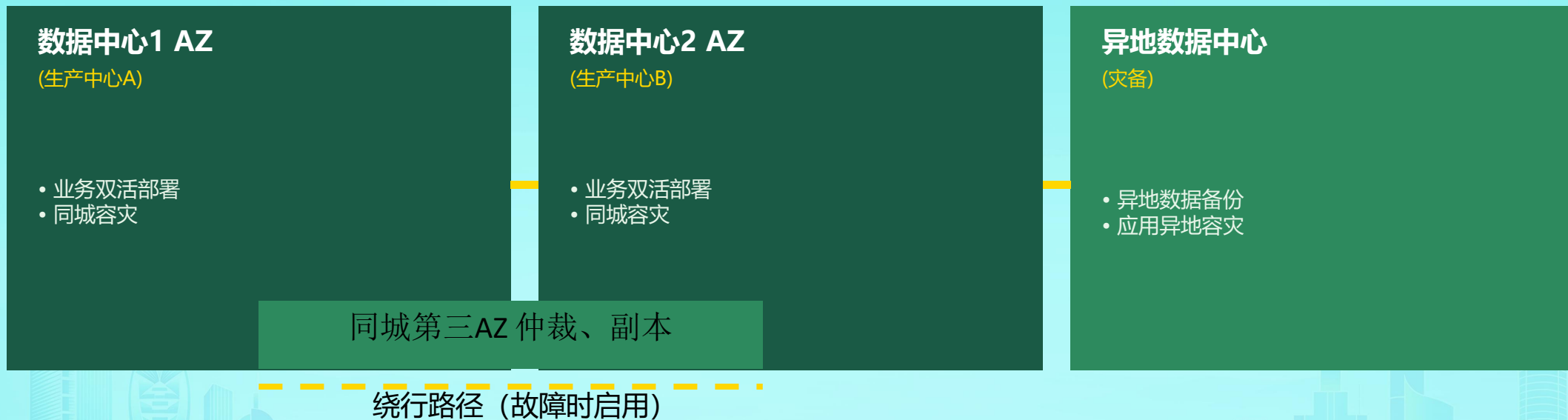
单元化双活方案

后续推进

- 业务分库分表，单元化部署
- 异构集群，每中心为独立业务处理单元
- 扩展能力强、故障影响局部
- 易演进多活

双活方案	业务连续性能力	恢复速度	改造复杂度	硬件成本
单元化双活	都可支持单中心故障的快速恢复	快 最快可以到分钟内	非常高	双活情况下基本相当 多活单元化会有优势 (但实际多活还需要多投入底座资源，未规模化情况下，实际硬件资源并未减少)；
传统双活		较快 20分钟内	比较低	

05 两地三中心部署模式与灾难应对



灾难应对场景矩阵

单应用故障

应用主备切换接管生产流量
RTO: <5分钟

单数据中心灾难

流量切换快速接管双活业务
RTO: <20分钟

城市级灾难

跨地域接管至异地容灾中心
RTO: 2小时

06 实施效果与建设成果

核心指标达成

RPO
0
已达成

RTO
<20分钟
已达成

关键业务可用性
数据中心级双活
已达成

应用系统双活上线
34个
集团及各子公司

平台建设成果

- ✓ 信创双活云：完成机房级、网络级、云产品级、管控面级全系列双活容灾演练验证
- ✓ 混合云管：实现多平台多数据中心资源统一纳管
- ✓ 配套基础设施：CMDB、监控、自动化运维全面升级
- ✓ 业务连续性平台：容灾演练和切换编排能力落地

核心价值

自主可控

从芯片、操作系统、数据库到中间件、应用系统全面自主可控-信创化

业务连续性

同城数据中心级，RPO=0、RTO<20分钟，业务中断时间大幅压缩

监管合规

满足金融监管局对大型金融机构重要业务系统连续性的严格要求

项目建设经验

01 全链路思维

"8横4纵"体系确保从部件到数据中心、从存储到网络的全层级覆盖，避免单点短板

02 应用与平台并重

不能过度聚焦基础设施而忽视应用架构改造，必须同步推进

03 演练常态化

通过常态化演练持续提升切换效率与安全性

推广应用经验

01 分阶段推进

优先选择交易链路清晰、依赖可控、业务价值高的系统试点，验证后再横向复制

02 信创与双活融合

将信创改造与双活改造合并为同一项目周期，避免重复申请资源、重复测试、多次割接

谢谢观看