

灾备交付能力经验及实践培训

宁夏工业和信息化研究院有限公司

1

灾备交付方法论与流程

2

标杆案例解析及经验总结

为何需要建设灾备体系?



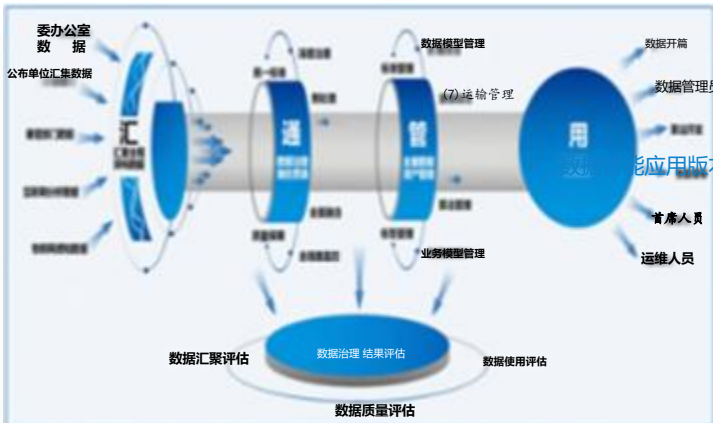
政策法规合规底线

遵循《网络安全法》与《数据安全法》要求，落实等保2.0标准，确保重要系统和数据库具备合规的容灾备份与恢复能力。



业务持续运营保障

数字化时代，系统中断将直接导致收入损失与品牌声誉受损。灾备体系是防止业务停摆、保障企业连续运营的关键防线。



核心数据资产保护

数据已成为企业最核心的数字资产。通过建立完善的灾备体系，可有效防范各类灾难导致的数据丢失风险，确保资产安全。

灾备建设总体流程与思路 (4W4H)



Why to do (为何做)

明确法规遵从、业务发展及战略规划等建设动因，确立项目目标。



What to do (做什么)

确定灾备建设范围、阶段目标和任务分解，明确实施路径。



With what (凭什么)

开展现状调研，摸清组织架构、资产清单及核心业务功能现状。



How to do (怎么做)

制定服务模式和灾备策略，设计整体技术架构与实施方案。



How much (投入多少)

进行可行性研究，申请项目预算，完成立项审批流程。



How/When to use (何时用)

执行集成实施、预案开发、人员培训和首次灾备演练。



How to manage (如何管)

建立长期的系统运维机制，定期进行灾备演练和预案更新，实现持续改进与优化。



01 售前支撑

- ✓ 发现商机：需求初步沟通
- ✓ 确认商机：明确合作意向
- ✓ 方案制定：输出技术方案



02 售中交付

- ✓ 项目立项：组建交付团队
- ✓ 招投标：完成商务签约
- ✓ 系统实施：环境部署与配置
- ✓ 预案开发：定制化灾备策略
- ✓ 演练验收：验证系统有效性



03 售后保障

- ✓ 持续运营：日常运维监控
- ✓ 定期演练：持续验证、优化能力

1

灾备交付方法论与流程

2

标杆案例解析及经验总结



项目背景：全球化能源巨头的IT基石

业务覆盖全球，核心系统（ERP、勘探数据管理等）支撑全链条生产运营，对数据安全和业务连续性提出极高要求。

核心挑战：四大维度的严峻考验

管理分散

多独立系统构成，缺乏统一监控，运维复杂度高。

能力不足

老旧系统灾备手段落后，RTO/RPO指标无法满足需求。

合规压力

需满足等保2.0及行业监管要求，合规性亟待加强。

全球化要求

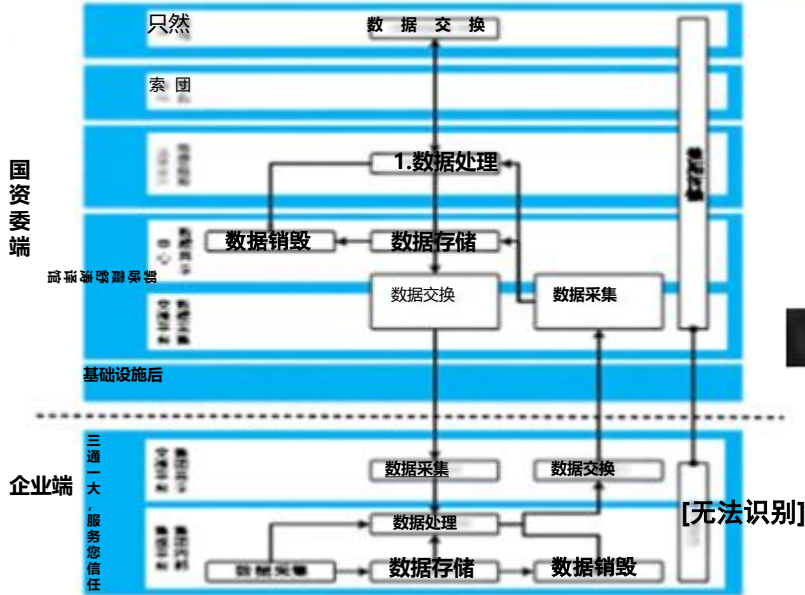
业务全球化布局，对跨地域协同和恢复时效性挑战巨大。

案例一：中国海油 - 核心需求深度剖析

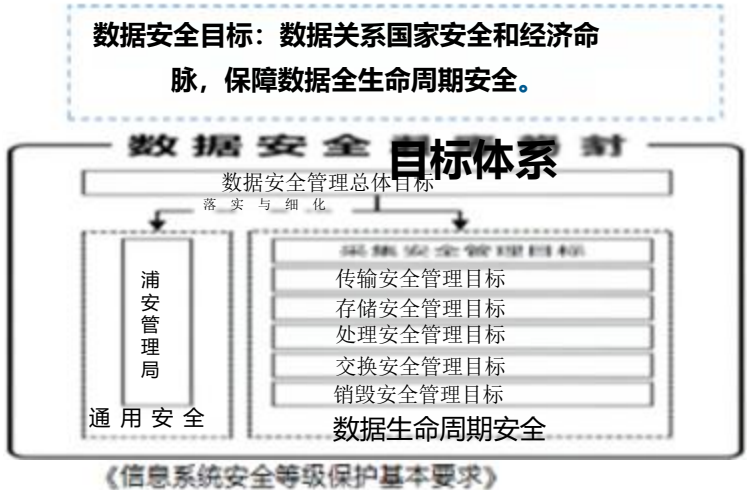


国家发展改革委关于印发
《“十四五”推进国家政务信息化规划》的通知

战略目标：构建“横向道边，纵向到底”的统一信息平台，统一监管全部国资数据资源，统一存储决策支撑型数据。



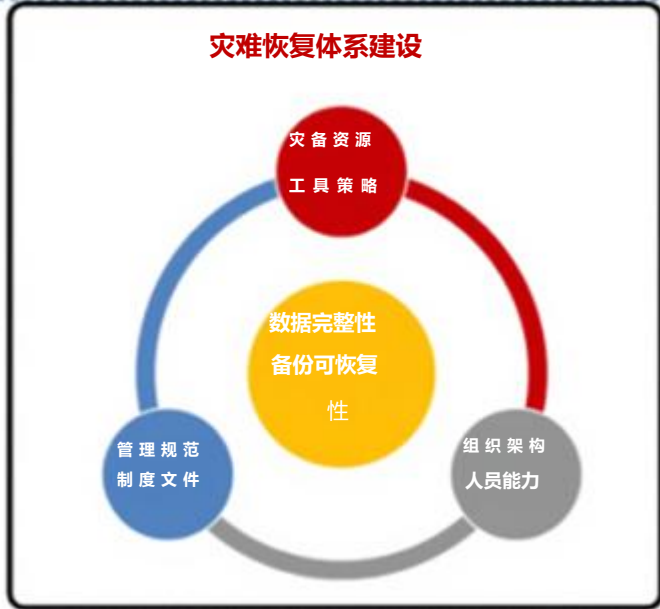
到2025年，政务信息化建设总体迈入以数据赋能、协同治理、智慧决策、优质服务为主要特征的融慧治理新阶段--安全保障达到新水平。**全面落实信息安全和信息系统等级分级保护制度**，基本实现政务信息化安全可靠应用，确保政务信息化建设和应用全流程安全可靠，**实现政务数据资源全生命周期安全保护。**



第二级要求 7.1.4.8 数据备份恢复
应提供异地数据备份功能,利用通信网络将重要数据定时批量传送至备用场地。

第三级要求 8.1.4.9 数据备份恢复
应提供重要数据的本地数据备份与恢复功能; 应提供异地实时备份功能, 备份至备份场地; 应提供重要数据处理系统的热冗余。

当前灾备措施：已不能满足合规性、业务持续发展的诉求，无法有效防范灾难风险导致的数据丢失，业务长时间中断，**亟待加强重要信息系统的灾难恢复体系建设工作，保障信息化建设成果。**



案例一：中国海油 - 分阶段实施路径



根据《中国海油灾难恢复与备份指南》内容和中国海油实际情况，归纳“**五阶段八要点**”用于指导中国海油集团规模化和标准化推进灾难恢复体系建设，确保一致可复用满足集团多元灾备需求。



案例一：中国海油 - 一体化灾备解决方案



坚持中国海油“四个统一”工作原则，即统一规划、统一标准、统一建设和统一管理，统筹制定集团灾难恢复体系建设指南，遵循统一技术标准和技术路线，**构建基于海油云的统一云灾备服务能力**，满足中国海油业务连续性和数据安全保障核心需求，为建设中国特色国际一流能源公司贡献信息化价值。





管理效率提升

- 自动化减少重复工作，管理效率提升50%



恢复能力增强

- 核心业务RTO从小时级缩短至分钟级
- 数据恢复点目标(RPO)达到秒级，保障业务连续性



合规性满足

2.0

- 完全满足行业监管对数据安全和灾备能力的合规要求



成本效益显著

- 资源整合与自动化运维，灾备总体拥有成本(TCO)降低30%
- 实现了良好的投入产出比，降本增效成果显著



项目背景：国家级金融数据安全防线

负责跨境资金流动监测与国际收支统计，核心业务系统处理高度敏感数据，需满足国家级的安全性、稳定性及业务连续性标准。

核心挑战：四大关键技术难点

异构集成适配

深度集成多厂商存储、数据库及安全设备，兼容性要求极高。

顶级安全合规

满足等保三级、涉密分级保护及国密规范，确保敏感数据绝对安全。

两地三中心架构

构建生产、同城灾备、异地灾备协同体系，支持快速切换与容灾。

实时联动同步

保持灾备与生产系统的数据实时一致性，确保灾备数据随时可用。



集成需求：多厂商统一管理

实现自研平台与EMC、IBM、华为、Oracle等主流厂商设备的无缝对接，屏蔽底层架构的复杂性，实现统一纳管。



架构需求：两地三中心标准

构建符合“两地三中心”标准的灾备架构，确保在极端故障下，异地灾备中心能够快速接管业务，保障核心功能不中断。



安全需求：国密算法全周期加密

灾备数据在传输、存储、使用全生命周期采用国密局认可的SM系列算法高强度加密保护，并通过相关安全合规认证。



功能需求：高级运维与应急

提供数据同步状态监控、多中心策略统一配置、一键式灾备切换演练及可视化应急指挥等高级功能，支撑日常运维。

案例二：国家外汇管理局 - 风险分析(RA)与业务影响分析(BIA)



通过严格的风险分析（RA）和业务影响分析（BIA），我们识别了关键风险并量化了业务中断影响，明确了不同业务系统的恢复优先级及RTO/RPO指标。



RTO (恢复时间目标)

指业务功能可容忍的最大中断时间，直接决定了灾备系统的恢复速度要求。



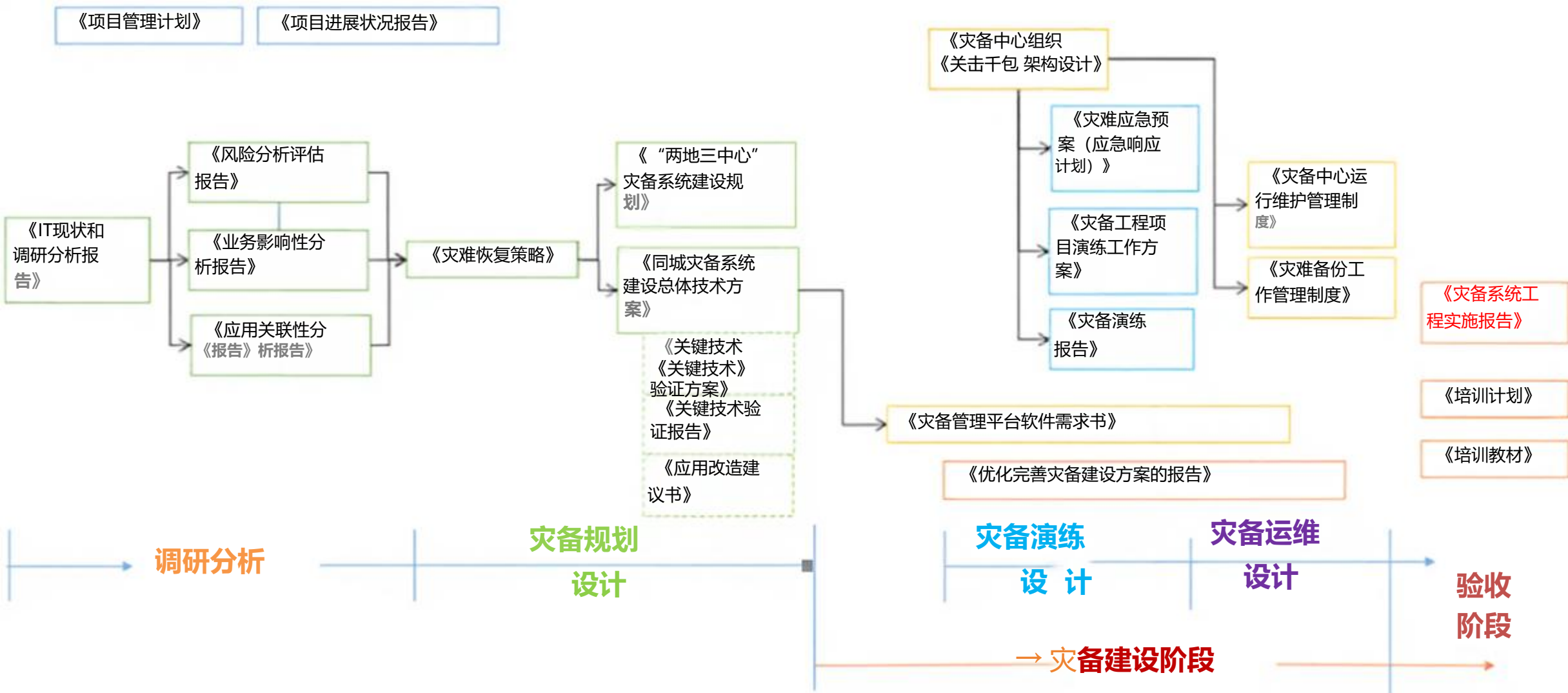
RPO (恢复点目标)

指业务系统可容忍的最大数据丢失量，决定了数据备份的频率和策略。

BIA 分析核心产出：业务系统分级与指标定义表

业务关键级别	业务系统名称	RTO 业务恢复时间目标	RPO 数据最大丢失量
第一级	应用服务平台（ASONE）、个人结售汇系统、标准代码系统，消息传输系统（MTS）等	<2H	0M - <15M
第二级	货物贸易外汇监测系统、银行数据统一采集系统	<4H	<15M 、<24H
第三级	对外金融资产负债及交易统计系统；电子表单系统、跨境资金流动监测与分析系统、国际收支系统等。	<24H	<15M、<24H
第四级	资本项目管理信息系统、门户网站、邮件系统	<48H	<15M 、<24H
第五级	问卷调查系统、内控系统、案件系统、其他网站	<1W	<24H

案例二：国家外汇管理局 - 项目实施成果（咨询设计）



案例二：国家外汇管理局 - 两地三中心解决方案

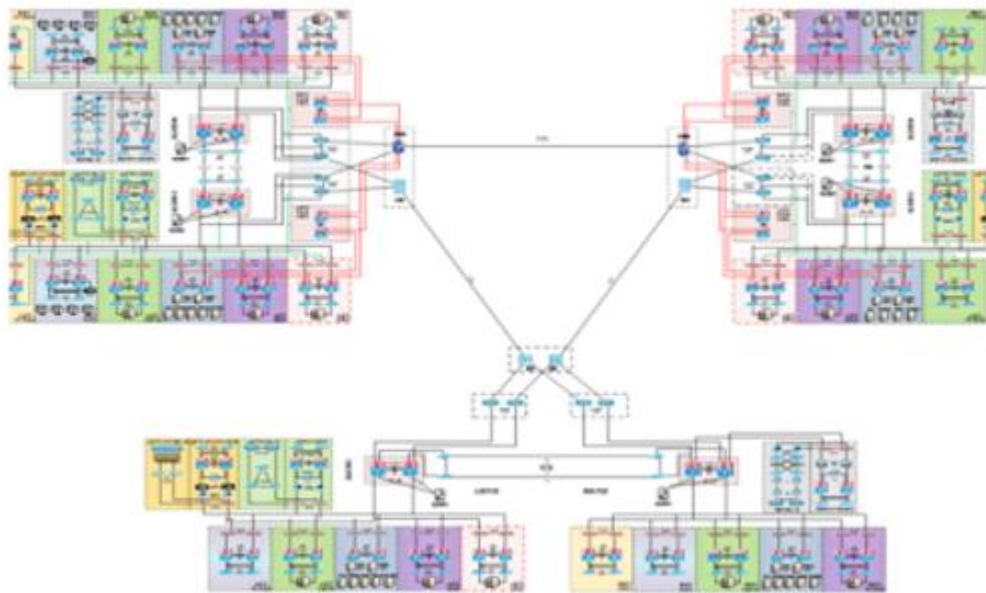


核心业务处理节点，承载日常高并发交易，确保业务连续性与低延迟响应。

采用同步复制技术，实现分钟级RTO，应对生产中心重大故障或区域性灾难。

北京生产中心 (Active)

北京同城灾备中心 (Standby)



上海异地灾备中心 (DR)

利用高速专线进行异步数据复制，作为最后一道防线，确保极端灾难下的数据安全。



异构环境统一纳管

开发标准化API与适配插件，实现多厂商、多类型设备的统一监控与配置管理。



端到端数据加密

内置国密算法模块，保障灾备数据从生产端到灾备端的全链路加密。



跨地域协同管控

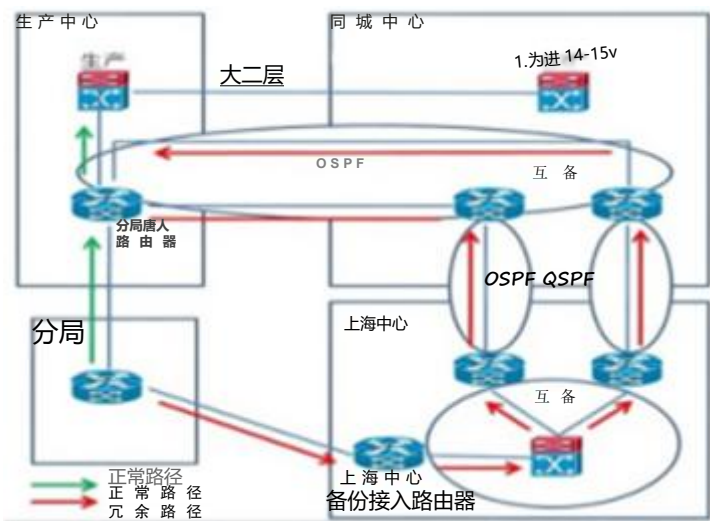
支持生产、同城、异地三中心策略统一配置与状态集中监控，确保高效协同。



智能应急指挥面板

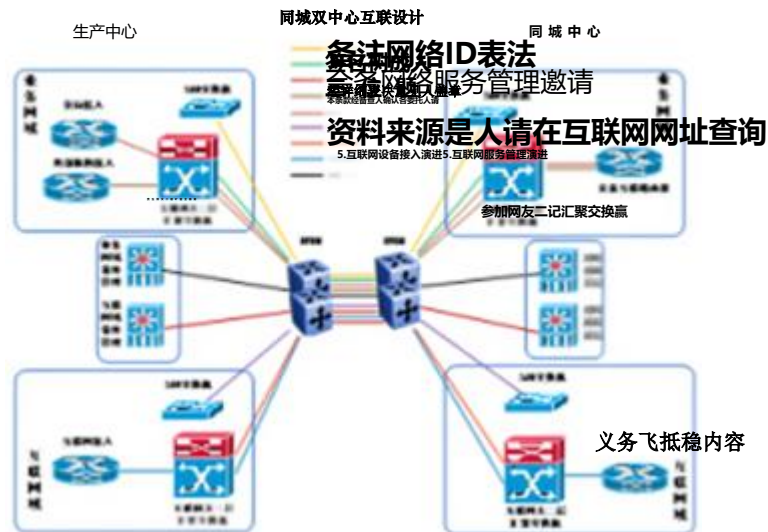
可视化展示系统状态，支持一键式灾备切换与恢复，实时监控操作进度。

网络架构：两地三中心连通及路由设计



- 实现生产中心与同城中心网络无缝迁移，打破物理地域限制。
- 部署OSPF动态路由协议，确保链路故障时实现毫秒级自动切换，保障业务连续性。

网络架构：同城大二层网络设计



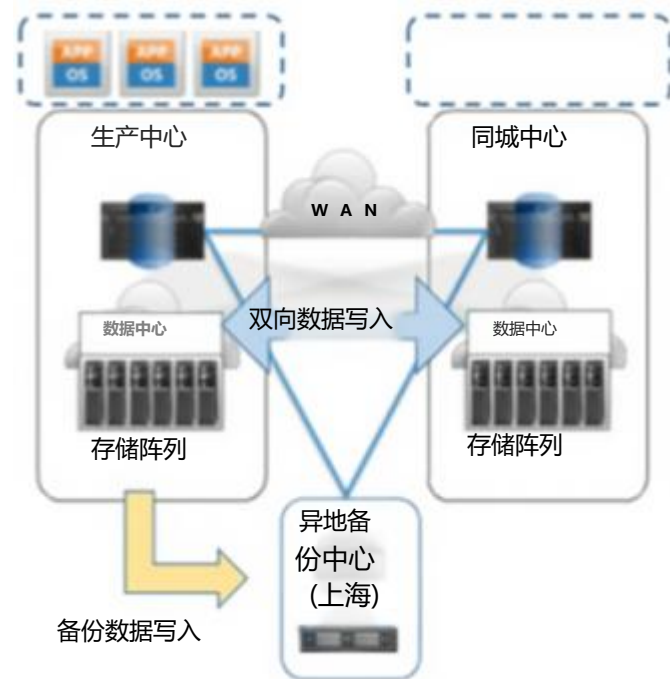
- 构建无阻塞、低时延的二层交换网络，支持虚拟机的大范围动态迁移。
- 采用EVPN/VXLAN技术，实现网络的弹性扩展和多租户隔离，提升资源利用率。

案例二：国家外汇管理局 - 核心技术实现（存储架构）

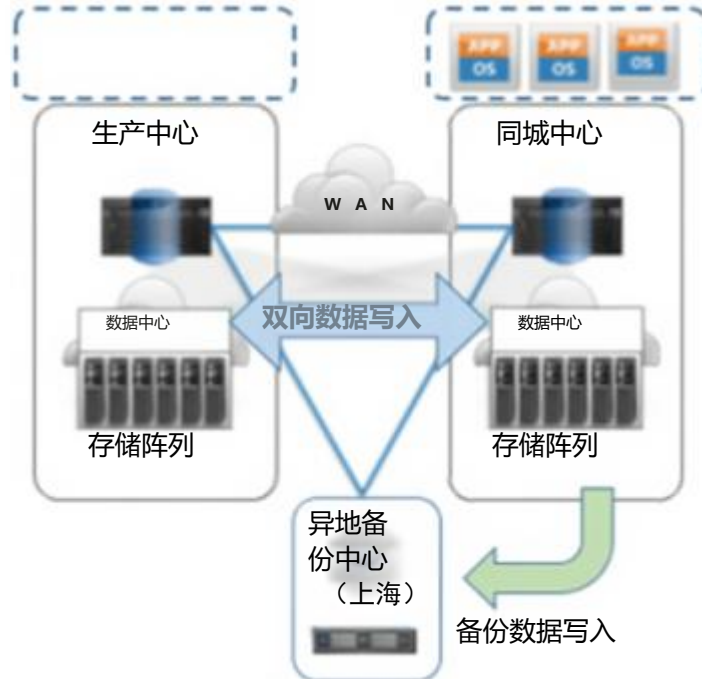


完成北京同城存储双活，上海异地异步复制建设。

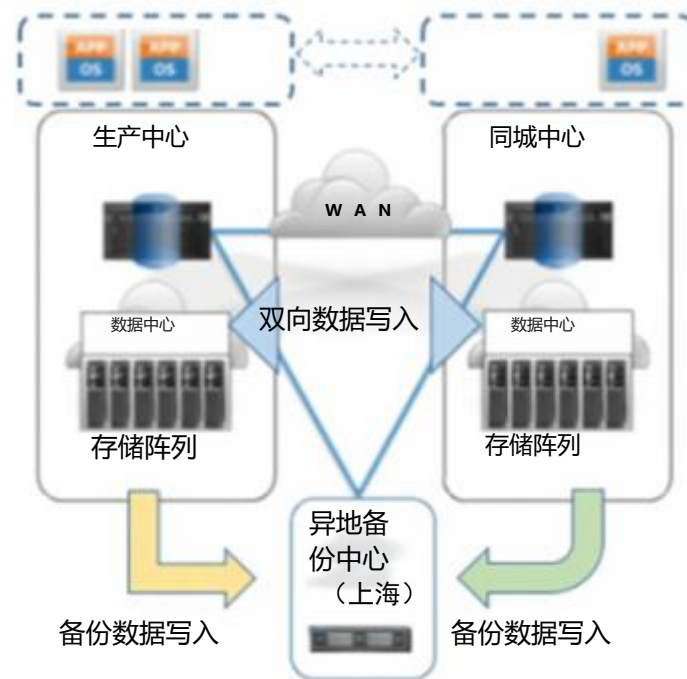
运行模式1：生产中心活动状态下，数据从生产中心向上海灾备中心备份数据。



运行模式2：同城中心活动状态下，数据从同城中心向上海灾备中心备份数据。



运行模式3：双中心活动状态下，数据从生产和同城中心分别向上海灾备中心备份数据。

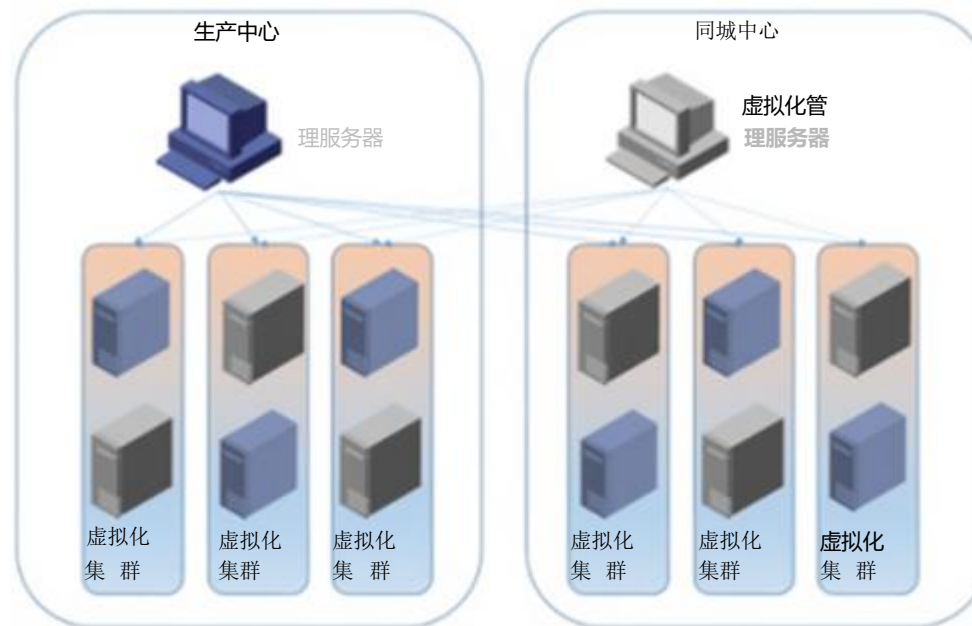
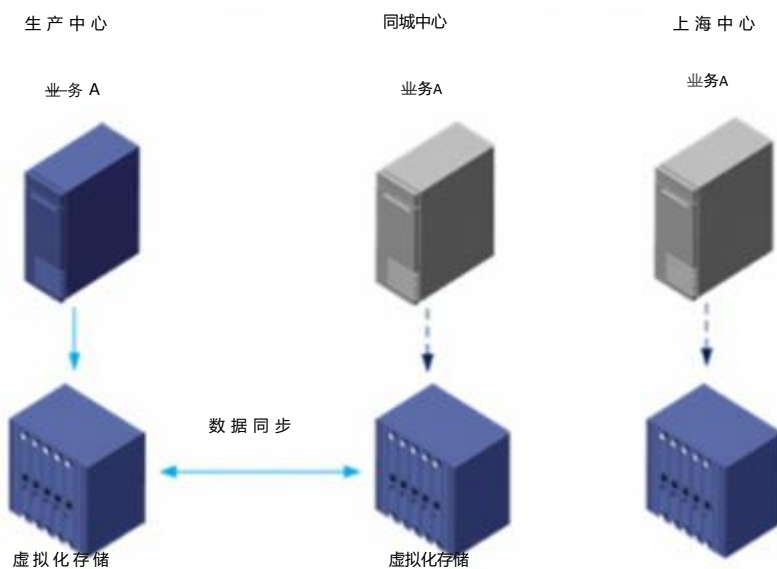


案例二：国家外汇管理局 - 核心技术实现（计算架构）



小型机资源配置：生产、同城中心、上海中心【1:1:0.6配置】，为保证高可用性，我们设计每台小型机上分别部署不同的业务系统，避免物理单机故障造成系统瘫痪。

X86虚拟化资源配置：虚拟机系统采用VMware组建，使用生产中心VC进行统一管理，同城设置备份VC，站点级切换时使用。



案例二：国家外汇管理局 - 项目实施成果（集成实施）



核心设计原则

- ❖ 架构：坚持“三个中心同构”，单中心可承载100%业务量
- ❖ 合规：严格执行三级等保与涉密分级保护标准
- ❖ 平台：定制化智能灾备切换平台，实现自动化运维

全生命周期工作内容 (21项)

- 系统现状调研评估、整体建设方案设计、基础设施集成
- 网络与安全体系搭建、数据迁移与同步策略实施
- 应用系统适配改造、灾备切换演练与流程优化
- 运维体系建立与人员培训、项目验收与交付



集成效率大幅提升

接入时间从数周缩短至数天，整体效率提升70%，运维工作量减少40%。



安全合规达到最高标准

顺利通过等保三级测评及涉密分级保护测评，满足核心政务系统合规要求。



分钟级恢复能力验证

完成跨地域实战切换演练，实现 RTO < 30分钟，RPO < 5分钟的高标准目标。



7x24小时业务连续性保障

数据7x24小时不间断同步，确保有效性与一致性，有力支撑跨境资金监测业务。

案例二：国家外汇管理局 - 项目实施关键节点



2014 商机洞察

敏锐捕捉市场需求，启动前期调研与方案设计，为后续项目奠定坚实基础。



2015 咨询设计

凭借专业的技术方案与服务能力，顺利中标项目，确立项目建设的主导地位。



2017-2018核心建设

完成核心系统同城切换测试与双中心启用，构建起“两地三中心”的灾备架构。



2019 项目终验

重构异地灾备中心实现一键切换，建立完善运维体系，项目成功通过终验。



深刻理解业务需求是前提

所有技术方案都必须服务于业务目标，通过RA/BIA等方法量化需求，确保灾备建设有的放矢。



科学的方法论是保障

遵循灾备方法论或成熟框架，标准化项目流程，确保项目每个环节都得到有效管理和风险控制。



平台化与自动化是趋势

利用统一平台整合资源，通过自动化编排实现快速、可靠的恢复，大幅提升运维效率。



持续的演练与优化是核心

灾备体系不是建成即结束，而是需要通过常态化演练来验证、发现问题并持续优化，确保实战有效。

感谢聆听!