数据容灾顶层规划

公益讲座11：00分准时开始，请大家先浏览云技术微信公众号技术文章资料会在各群同步发布，已入群客户请勿重复入群!

20-17

数据库和云讲座群

甲骨文云技术公众号

ORACLE

数据容灾顶层规划

保证业务连续性项目成功实施

沈国坤

Master Principal Solution Engineer, Oracle China

July. 2022

议题

- 从业务需求出发，规划设计数据容灾体系
- 绕开数据容灾陷阱，实现容灾目标

保证业务连续性的重要性

财务风险

- 业务中断意味着**收入损失**
- 计划外**恢复成本**
- **声誉/品牌损害会降低市场价值**

客户风险

- **体验不佳的客户可能流失**
- 广泛流传的停机事件会使**吸引新客户变得更加困难**

监管风险

- **受监管企业可能因意外业务中断而面临处罚**
- 也可能受到额外的持续审查

灾备建设国家标准

2003年8月，中央办公厅、国务院办公厅联合下发了《国家信息化领导小组关于加强信息安全保障工作的意见》。 ***--- 第一次提到了重要信息系统需要具备灾难恢复能力。***

2004年9月，国务院信息化办公室下发了《关于加强国家重要信息系统灾难备份工作的意见》

2005年4月，国务院信息化办公室联合银行、电力、民航、铁路、证券、税务、海关、保险等国内八大重点行业，制定发布了《重要信息系统灾难恢复指南》。

2007年7月，《重要信息系统灾难恢复指南》经过修改完善后正式升级成为国家标准GB/T 20988-2007 ***《信息系统灾难恢复规范》。 --- 中国灾难备份与恢复行业的第一个国家标准***

2008年2月，中国人民银行发布JR/T 0044—2008 《银行业信息系统灾难恢复管理规范》。

2018年12月，国家市场监督管理总局、中国国家标准化管理委员会发布《信息安全技术灾难恢复服务要求（GB/T 36957-2018）》

《信息系统灾难恢复规范》主要内容

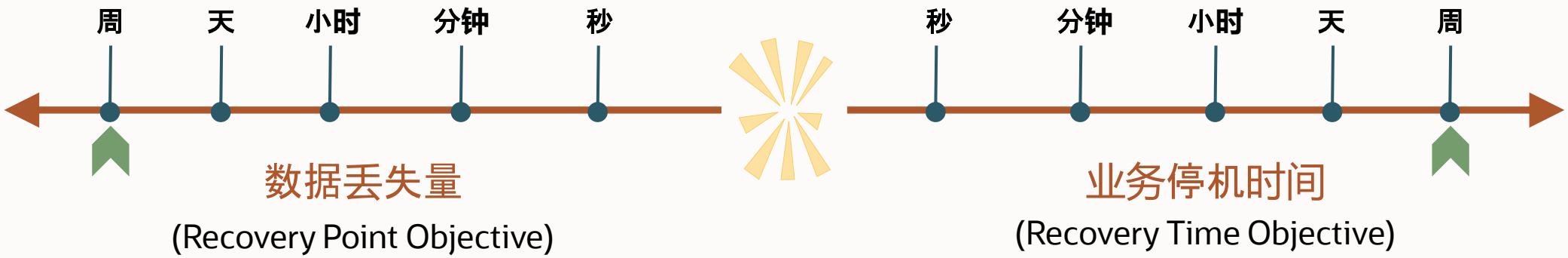
对灾备系统建设具有重要的指导意义

- **灾难恢复行业相应的术语和定义**
  - 灾难备份中心 、灾难备份 、灾难备份系统、业务连续管理、业务影响分析、关键业务功能、数据备份策略、灾难、灾难恢复、灾难恢复预案、灾难恢复规划、灾难恢复能力、演练、场外存放、主中心、主系统、区域性灾难、恢复时间目标 RTO、恢复点目标 RPO、重续、回退
- **灾难恢复概述**
  - 包括灾难恢复的工作范围、灾难恢复的组织机构、灾难恢复规划的管理、灾难恢复的外部协作、灾难恢复的审计和备案
- **灾难恢复需求的确定**
  - 包括风险分析、业务影响分析、确定灾难恢复目标
- **灾难恢复策略的制定**
  - 包括灾难恢复策略制定的要素、灾难恢复资源的获取方式、灾难恢复资源的要求
- **灾难恢复策略的实现**
  - 包括灾难备份系统技术方案的实现、灾难备份中心的选择和建设、专业技术支持能力的实现、运行维护管理能力的实现、灾难恢复预案的实现

灾备系统建设的两个关键指标：RTO与RPO

灾备系统建设目标

在灾难发生时，能够保证**数据尽量少的丢失**，系统能够**不间断地运行**，或者**尽量快的恢复**正常运行。



RPO: 恢复点目标

- 灾难发生后，系统和数据必须恢复到的时间点要求。
- 早上6点故障；早上8点恢复，但是数据最近的备份是还是昨天晚上12点做的，则RPO=6小时

RTO: 恢复时间目标

- 灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。
- 早上6点故障；早上8点恢复，则RTO=2小时

《信息系统灾难恢复规范》灾难恢复能力等级划分

国际标准SHARE78		《信息系统灾难恢复规范》GB/T 20988－2007	
Tier-0	无异地备份数据	第1级	基本级，备份介质场外存，安全保管、定期验证。
Tier-1	有数据备份，无备用系统 用卡车运送备份数据		
Tier-2	有数据备份，有备用系统。 用卡车运送备份数据。	第2级	备份场地支持，网络和业务处理系统可在预定时间内调配到备份中心。
Tier-3	电子链接，消除运送工具的需要，提高了灾难恢复速度	第3级	电子传输和部分设备支持。灾备中心配备部分业务处理和网络设备，具备部分通讯链路。
Tier-4	灾难恢复具有两个中心彼此备份数据，允许备份行动在任何一个方向发生。两个中心之间，彼此的关键数据的拷贝不停地相互传送着。在灾难发生时，需要的关键数据通过网络可迅速恢复，通过网络的切换，关键应用的恢复也可降低到小时级或分钟级。	第4级	电子传输和完整设备支持。数据定时批量传送，网络/系统始终就绪。温备中心模式。
Tier-5	保证交易的完整性，为关键应用使用了双重在线存储，在灾难发生时，仅传送中的数据被丢失，恢复时间被降低到分钟级。	第5级	实时数据传输及完整设备支持。采用远程复制技术，实现数据实时复制，网络具备自动或集中切换能力，业务处理系统就绪或运行中。
Tier-6/7	无数据丢失，同时保证数据立即自动地被传输到恢复中心。Tier6被认为是灾难恢复的最高的级别，在本地和远程的所有数据被更新的同时，利用了双重在线存储和完全的网络切换能力。第7层实现能够提供一定程度的跨站点动态负载平衡和自动系统故障切换功能。	第6级	数据零丢失和远程集群支持。数据实时备份，零丢失，系统/应用远程集群，可自动切换，用户同时接入主备中心

《信息系统灾难恢复规范》中提出的灾备级别的行业参考标准举例

灾难恢复能力等级	RTO	RPO
1	2天以上	1天至7天
2	24小时以上	1天至7天
3	12小时以上	数小时至1天
4	数小时至2天	数小时至1天
5	数分钟至2天	0至30分钟
6	数分钟	0

- 灾难恢复能力**等级越高**，对于信息系统的**保护效果越好**，但同时**成本也会急剧上升。**
- 需要根据**成本风险平衡原则**，确定业务系统的合理的**灾难恢复能力等级。**
- 每个业务单位中的**不同业务系统**，可采用**不同的灾难恢复策略。**

《信息系统灾难恢复规范》中灾难恢复资源要素

序号	要素	要素的考虑要点
1	备用基础设施	灾难备份中心选址与建设； 备用的机房及工作辅助设施和生活设施；
2	数据备份系统	数据备份范围与RPO； 数据备份技术； 数据备份线路；
3	备用数据处理系统	数据处理能力； 与生产系统的兼容性要求； 平时的状态（处于就绪还是运行）；
4	备用网络系统	备用网络通信设备系统与备用通信线路的选择； 备用通信线路的使用状况；
5	灾难恢复预案	明确灾难恢复预案的： A）整体要求 B）制订过程的要求 C）教育、培训和演练要求 D）管理要求
6	运行维护管理能力	运行维护管理组织架构； 人员的数量和素质； 运行维护管理制度； 其他要求；
7	技术支持能力	软件、硬件和网络等方面的技术支持要求； 技术支持的组织架构； 各类技术支持人员的数量和素质等；

1. 灾备中心基础设施建设
2. 灾备技术架构选择及应用
3. 日常运维和管理

业务连续性项目成功实施的重要举措

从业务需求出发，选择合适技术，规划设计数据容灾体系

举措一：业务连续性需求评估

- 评估关键系统的业务连续性需求等级，及相应的RTO/RPO指标要求

举措二：建立完整的保障体系

- 四位一体保障体系：生产系统高可用、同城容灾、异地容灾、数据备份

举措三：选择合适的业务连续性技术

- 在网络、应用、虚拟化、操作系统、数据库、主机、存储等不同层面选择最适合的业务连续性技术，并打通技术堆栈

举措四：定期演练，熟能生巧

- 完善运维管理工作，定期演练，检验能力，优化流程，提升效率

举措一：业务系统评估，确定业务所需的连续性指标等级

业务连续性指标分级，业务系统重要程度分级

- **业务连续性指标分级**

结合**业务**需求，考虑目前企业当前**技术**手段可实现的业务连续性水平，细化RTO、RPO分级。

指标级别	业务恢复时间目标（RTO）
1级	1分钟内恢复
2级	10分钟内恢复
3级	1小时内恢复
4级	8小时内恢复
5级	1天恢复
6级	可恢复，但不保证时间要求

RTO指标分级示例

指标级别	可容忍丢失的数据（RPO）
1级	无数据损失
2级	10秒内的数据损失
3级	1分钟内的数据损失
4级	1小时内的数据损失
5级	一天之内的数据损失
6级	一周之内的数据损失

RPO指标分级示例

- **业务系统重要程度分级**

按照业务系统重要程度进行分级。

业务线条	系统名称	一级功能	二级功能	三级功能	四级功能	业务级别
市场	CRM	渠道管理	渠道运营支撑	渠道控制	接入管理	关键
大数据	大数据平台	数据仓库	数据集市	ODS	数据展现	常用
IT	运维管理	设备管理	软件版本管理	排班系统	知识管理	部门
……						

业务系统分级示例

举措一：业务系统评估，确定应对不同风险的业务连续性指标等级

对业务系统进行业务影响分析、风险分析、确定灾难恢复目标

业务线条	系统名称	业务分级	系统说明	机房	数据丢失导致的后果	业务出现中断导致的影响
BSS	CRM	关健业务	面向前台客户的核心业务支撑系统	主机房、同城机房、远程机房	承载客户业务相关的重要数据，此类数据的丢失将会极大降低客户的满意度，对信誉以及收益造成巨大的影响	承载客户敏感的关键业务，此类业务的中断将会极大降低客户的满 意度，对企业形象造成重大负面影响； 集团公司考核99.9%可用性，业务中断10分钟为故障
……						

业务连续性指标需求示例

业务中断类型	中断原因	常见问题	RTO目标	RPO目标
计划外业务中断	计算故障	服务器故障	1级	1级
		站点级故障/灾难	站点故障：1级 区域性灾难：2级	站点故障：1级 区域性灾难：2级
	数据故障	应用/人为错误	1级	1级
		存储故障	1级	1级
		逻辑数据损坏	1级	1级
计划内业务中断	系统变化	平台软件小版本/补丁升级	1级，缩小停机影响范围	/
	数据变化	存储硬件变更/数据迁移	1级	/
	应用变更	应用软件版本升级	缩小停机影响范围	/

举措一：业务系统评估，确定应对不同风险的业务连续性指标等级

对业务系统进行业务影响分析、风险分析、确定灾难恢复目标

业务线条	系统名称	业务分级	系统说明	机房节点	数据丢失导致的后果	业务出现中断导致的影响
大数据	大数据平台	常用业务	信令、日志、语音文本等大数据存储和分析处理	生产机房	信令、日志、语音文本等数据丢失会导致无法及时输出分析结果。数据需要从其他系统重新抽取。	信令、日志、语音文本等大数据分析业务 相关分析业务中断，无法及时输出分析结果

业务连续性指标需求示例

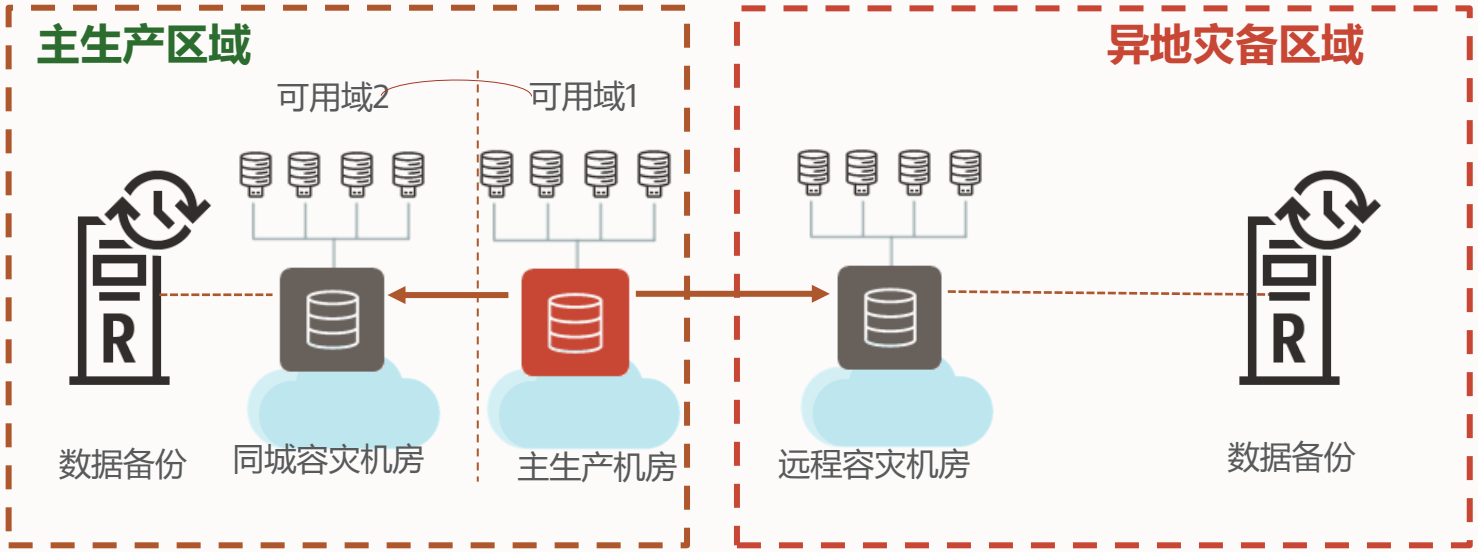
业务中断类型	中断原因	常见问题	RTO目标	RPO目标
非计划业务中断	计算故障	服务器故障	2级~3级	1级
		站点级故障/灾难	站点故障：3级 区域性灾难：6级	站点故障：3级 区域性灾难：6级
	数据故障	应用/人为错误	6级	4级~5级
		存储故障	1级	1级
		逻辑数据损坏	6级	4级~5级
计划内业务中断	系统变化	平台软件版本/补丁升级	2级~3级	/
	数据变化	存储硬件变更/数据迁移	2级~3级	/
	应用变更	应用软件版本升级	4级	/

举措二：建立完整的业务连续性保障体系

建立“四位一体”的业务连续性保障体系架构

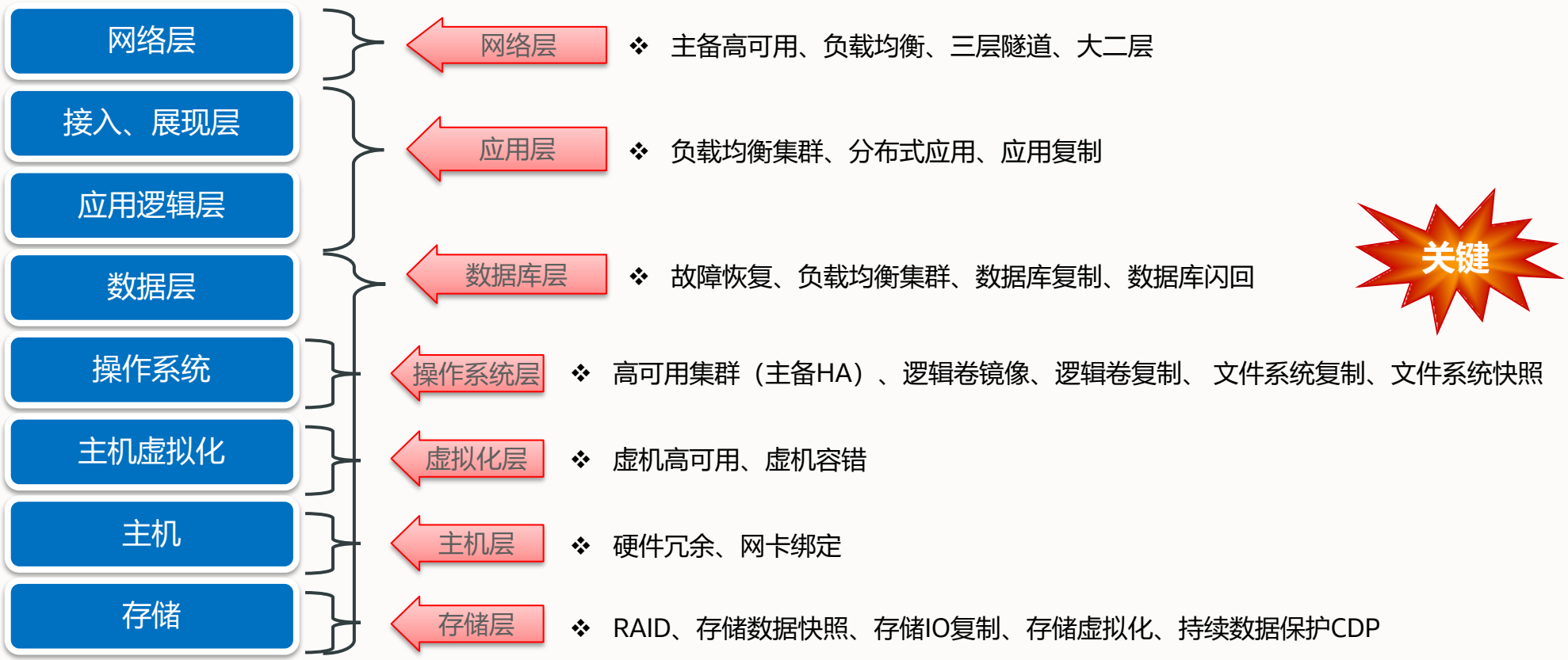
建立**“四位一体”**的业务连续性保障体系架构，包含：**生产系统本地高可用、同城灾备系统、异地灾备系统，**以及**数据备份系统**组成，相互配合共同保证IT支撑系统整体的业务连续性

- 生产系统**本地高可用**性是业务连续性保障的**基础**
- **同城灾备**系统是**业务快速恢复**的手段，在本地高可用失效的情况下，通过同城灾备系统快速接管，保证业务连续性
- **异地灾备**系统是建立在异地灾备中心的一套整体生产系统恢复体系，**重大灾难故障时**，通过启动灾备系统接管生产系统
- **数据备份**系统在线将生产系统各种数据（包括数据库和文件系统中的数据）备份到备份设备上，是**数据的最后保障。**



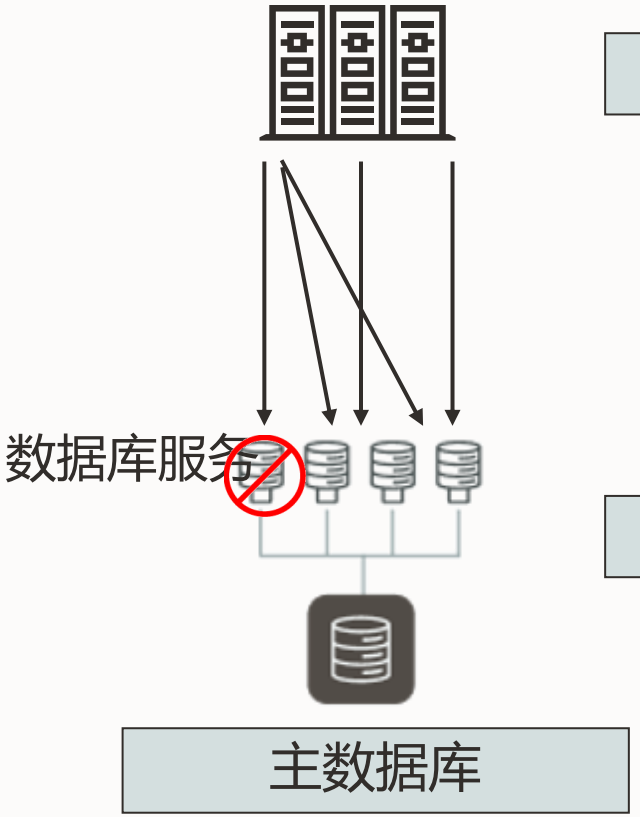
举措三：选择最合适技术，打通技术堆栈进行有机集成

选择数据层灾备技术架构是关键



数据层本地高可用技术—— Oracle RAC

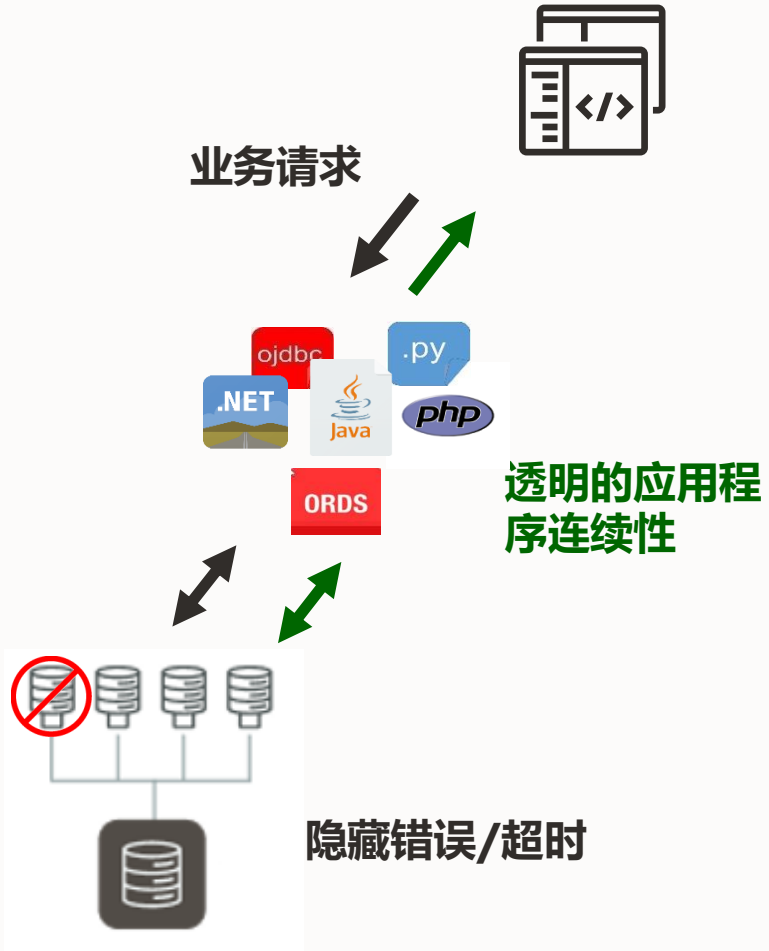
服务器节点故障、数据库实例故障、滚动升级维护



- 同时利用 Oracle 数据库的两个或多个实例
- 非常容易扩展
  - 所有实例都处于活动状态;在线添加处理能力;数据库整合的理想选择
- 高可用性
  - 将服务自动故障转移到活动实例
  - 中断对用户透明，正在进行的事务不会中断
  - 零停机滚动维护

数据层本地高可用技术—— 透明的应用程序连续性（TAC)

应用程序在RAC数据库实例中断期间不会报错



- 结合Oracle RAC群集使用TAC功能
- 透明地跟踪和记录会话信息，以防出现故障
- 内置于数据库内部，因此无需任何应用程序更改即可工作
- 重建会话状态，在发生突发故障时重放正在进行的事务
- TAC 也可以处理计划内的节点维护，以从一个或多个节点中释放会话
- 适应应用的变化：为可能发生的变化提供应用连续性保护

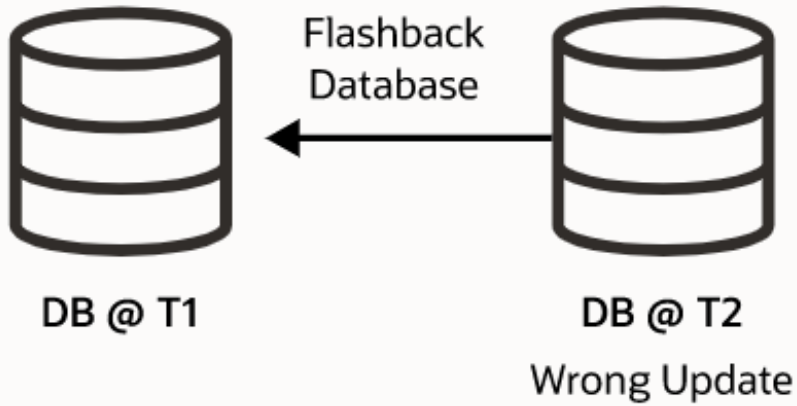
数据层本地高可用技术—— Flashback 闪回技术

Oracle 数据库的倒带按钮

- 快速时间点恢复(PITR)
  无需复杂的数据库恢复操作
- 错误回溯检查
  - 查看截至上一个时间点的数据
- 纠错
  - 回退交易
  - 表更新不正确
  - 倒带整个数据库

@T1	Col-1	Col-..	Col-n
Row-1	Abby	1234	officer
Row-2	Ben	8834	mgr
Row-3	Charlie	9837	officer
Row-n	Tom	8793	vp

@T2	Col-1	Col-..	Col-n
Row-1	Tom	1234	vp
Row-2	Ben	8834	vp
Row-3	Charlie	9837	vp
Row-n	Tom	8793	vp

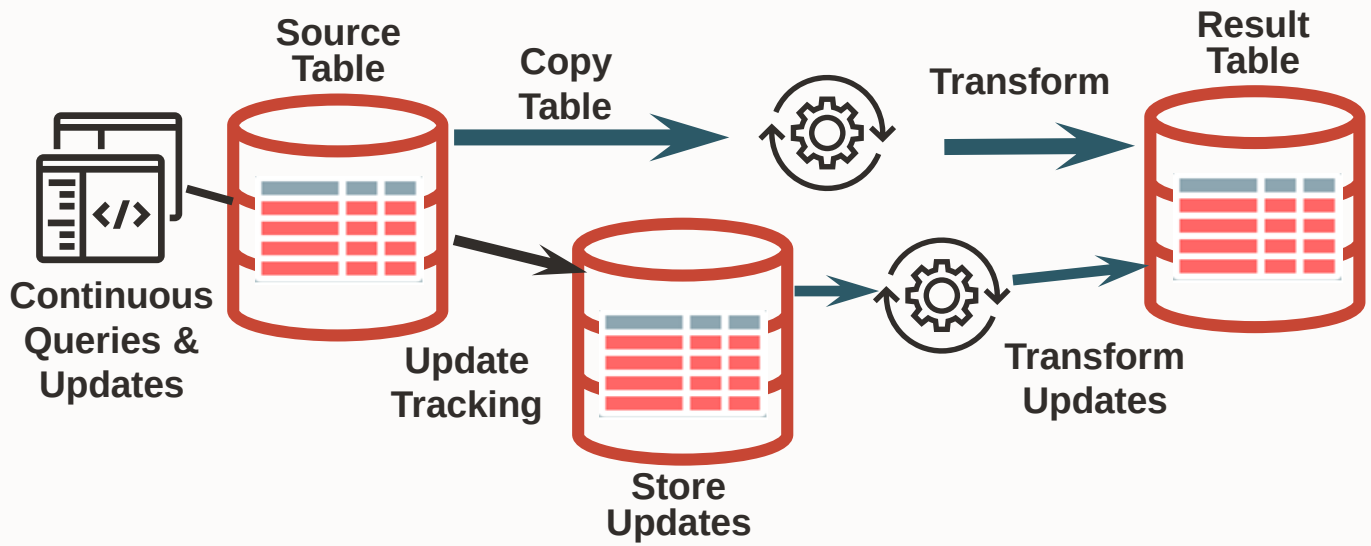


数据层本地高可用技术 —— 在线重定义

Oracle数据库在线重新定义

DBMS_REDEFINITION允许您在线重新组织和重新定义表

- Add/drop/rename/reorder 列
- 修改物理存储结构
- 在线重新组织和转换数据



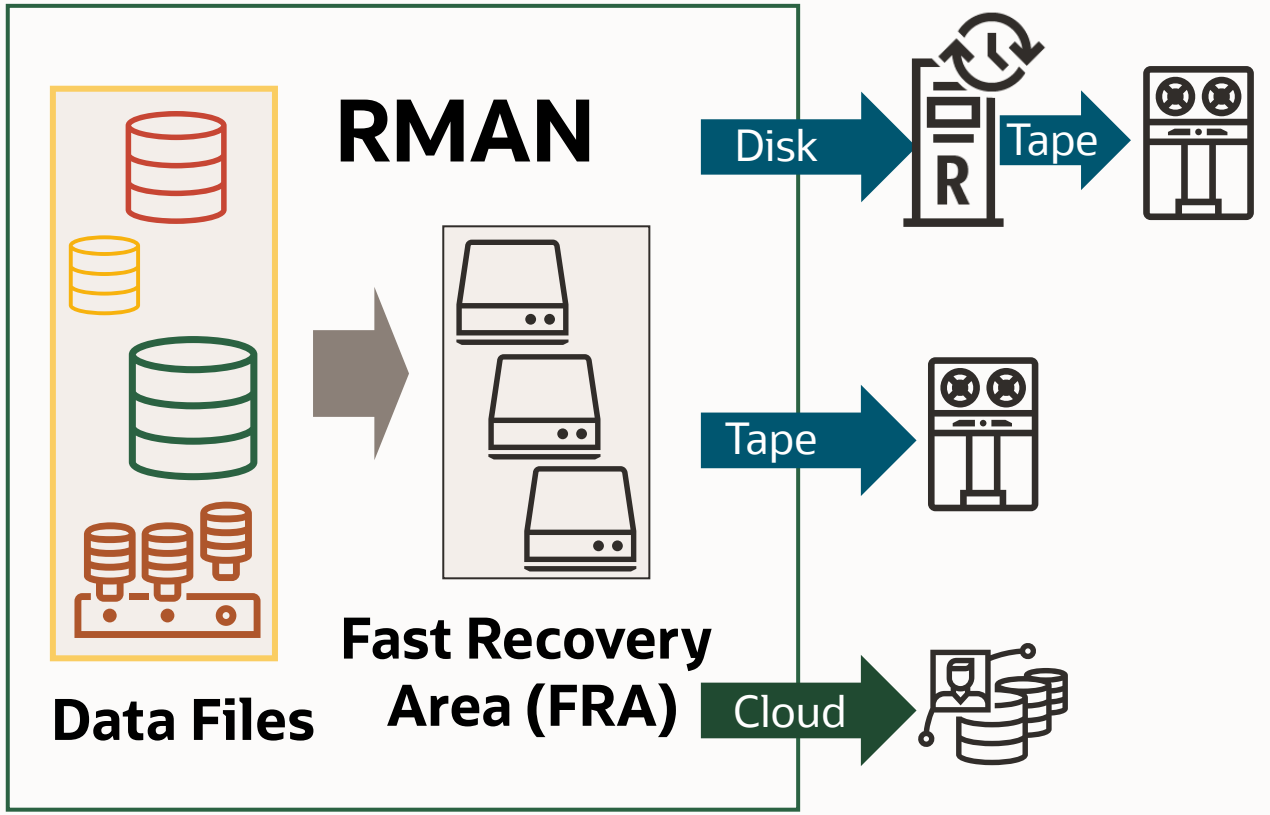
使用DBMS_REDEFINITION的其他好处

- 容错（在故障点恢复）和跟踪更改，以实现快速回滚到先前的定义
- 整个重新定义过程无需获取独占 DDL 锁即可运行
- 使用 V$online_redef 监控重组

数据库备份技术—— Oracle RMAN

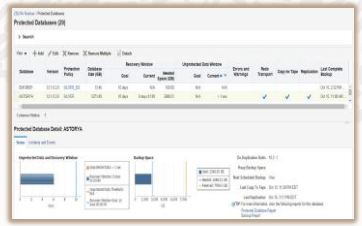
数据库预集成的备份和恢复工具

- 数据库备份和恢复过程的独特能力
  - 数据块验证
  - 在线块级恢复
  - 本机加密、压缩
  - 表/分区级恢复
  - 多租户支持
- 磁带和云备份
- 统一管理



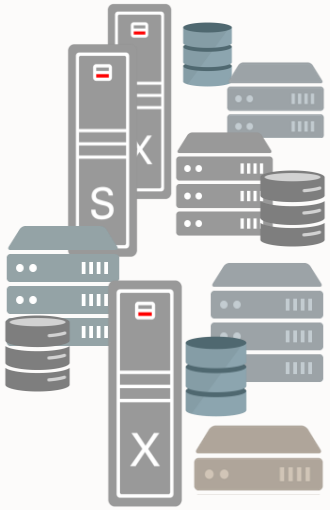
数据库备份技术—— 备份恢复一体机 ZDLRA

显著提高Oracle数据库备份、恢复可靠性及效率

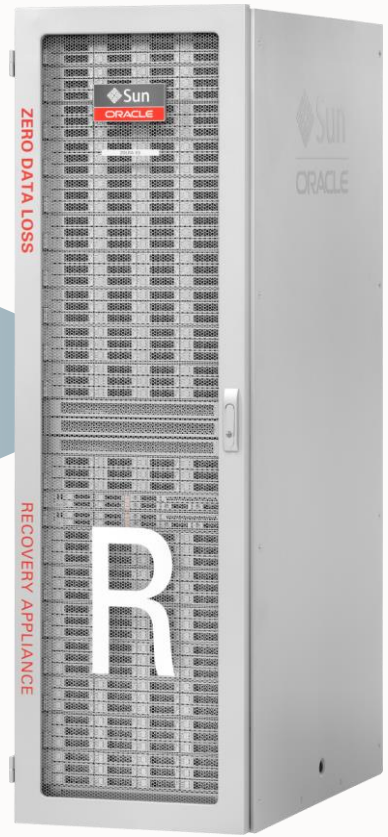


EM实时
保护状态和空间监控

Oracle 数据库



事务块更改



Day 1 Full

Day 2 Changes

Day N State

Day N Changes

虚拟全库备份

公有云存储

远程副本

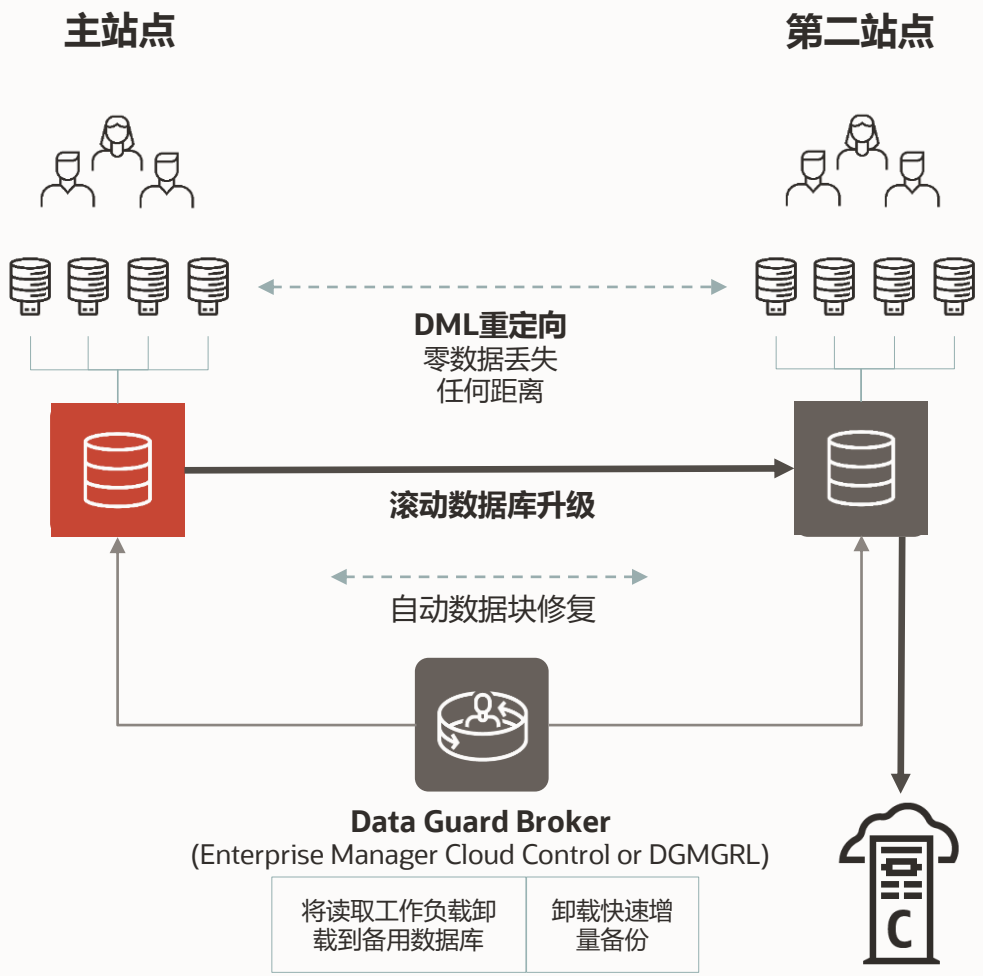
磁带

任何平台上的 Oracle DB 12c-21c

只需一次全库备份，永远增量

端到端 Oracle 恢复验证
数据丢失几乎为零

数据库容灾复制技术——Oracle *Active* Data Guard (ADG)



- **灾难恢复**
- **Active-active***
  - 在容灾库运行查询、报表、备份
  - 在容灾库进行少量更新(19c)
  - 确保知道容灾系统正常运行
- **自动数据块修复**
- **应用程序连续性**
- **任何距离的零数据丢失**
- **许多其他功能**

https://www.oracle.com/database/technologies/high-availability/dataguard-activedataguard-demos.html

数据库容灾复制技术—— ADG，支持在容灾端更新数据

DML on ADG

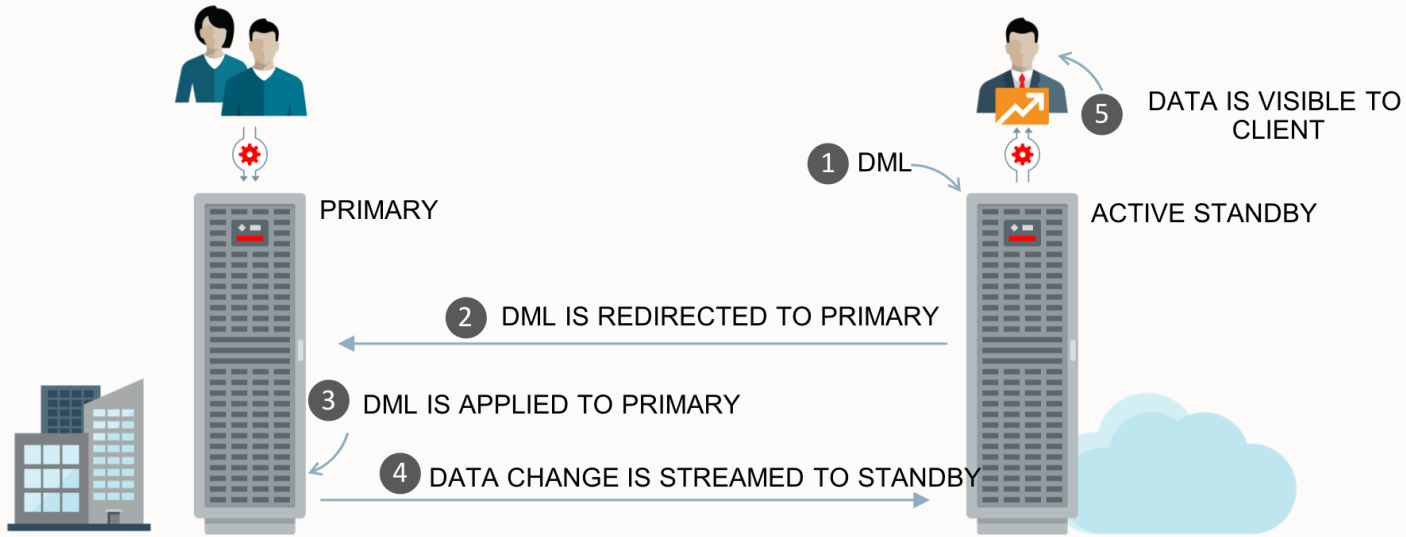
从ADG备用数据库执行DML，自动重定向到主数据库，不会影响 ACID

- 新的参数ADG_REDIRECT_DML控制 DML 重定向
- 新 `alter session ADG_REDIRECT_DML` 会话级别设置DML重定向
- 新 `ADG_REDIRECT_PLSQL`命令

Oracle Database **19c** 支持

- 适用于“读取为主，偶尔更新”应用程序

https://www.oracle.com/technetwork/database/availability/adg-redirect-5305796.gif



数据库容灾复制技术—— ADG Far Sync 远距离同步传输

任何长距离的零数据丢失保护技术

主数据库

- Production copy

Far Sync实例

- 数据库控制文件和日志文件
- 无需数据库文件
- 无需介质恢复
- 可卸载传输压缩和/或加密

活动备用数据库

- 零数据丢失故障转移目标
- 数据库以只读方式打开
- 持续的数据库验证
- 手动或自动故障转移

数据库容灾复制技术—— Oracle GoldenGate

异构数据库双向复制

Capture:通过读取事务日志，捕获（并可以筛选）已提交的事务.

Trail:用于路由分发的暂存和队列数据.

Distribution Server/Receiver:分发数据并传输到目标(s).

Route:数据被压缩，加密传输到目标(s).

Delivery:应用具有事务完整性的数据.

数据库容灾复制技术—— 存储远程镜像技术

将生产数据库对存储的所有I/O进行复制，同步/异步模式传送到远端，写入容灾存储

....包括损坏的块或错误的数据

数据层高可用最佳实践—— Exadata数据库一体机

内置高可用性，开箱即用

冗余数据库服务器

Active-Active 高可用群集服务器
热插拔电源和风扇
冗余配电单元
集成的 HA 软件/固件堆栈

冗余网络

冗余 100Gb/s ROCE 连接和交换机
使用高可用绑定网络进行客户端访问
集成的高可用软件/固件堆栈

冗余存储网格

跨存储服务器镜像的数据
冗余、非阻塞 I/O 路径
集成的高可用软件/固件堆栈

IDC

Exadata 提供三种部署模式

用户可选择合适的部署模型

私有云

Exadata

用户数据中心
购买
用户管理

公有云本地化（专有云）

Exadata Cloud at Customer

用户数据中心
订阅
Oracle 管理

公有云

Exadata Cloud Service

Oracle 公有云
订阅
Oracle 管理

ExaCC 专有云数据库一体机特点

与Exadata相同技术架构，同时获得公有云特性及私有化优点

数据无忧

部署在用户数据中心

Oracle 负责运营

省时省力

快速部署

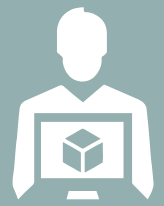
Exadata性能优势

分期付费

公有云订阅式服务

按使用量付费

应用广泛



支持Oracle应用

支持第三方应用

合规遵从

遵从法规

数据主权

ExaCC 专有云数据库一体机的优势

提高灾备中心设备资源利用率，降低灾备中心运营成本

公有云本地化
（专有云）

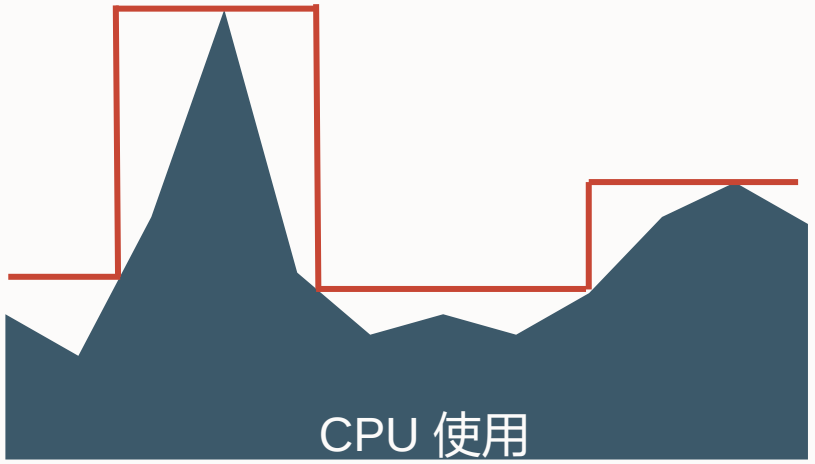
Exadata Cloud at Customer

灾备数据中心

订阅

Oracle 管理

按需增加或减少 CPU 激活数量



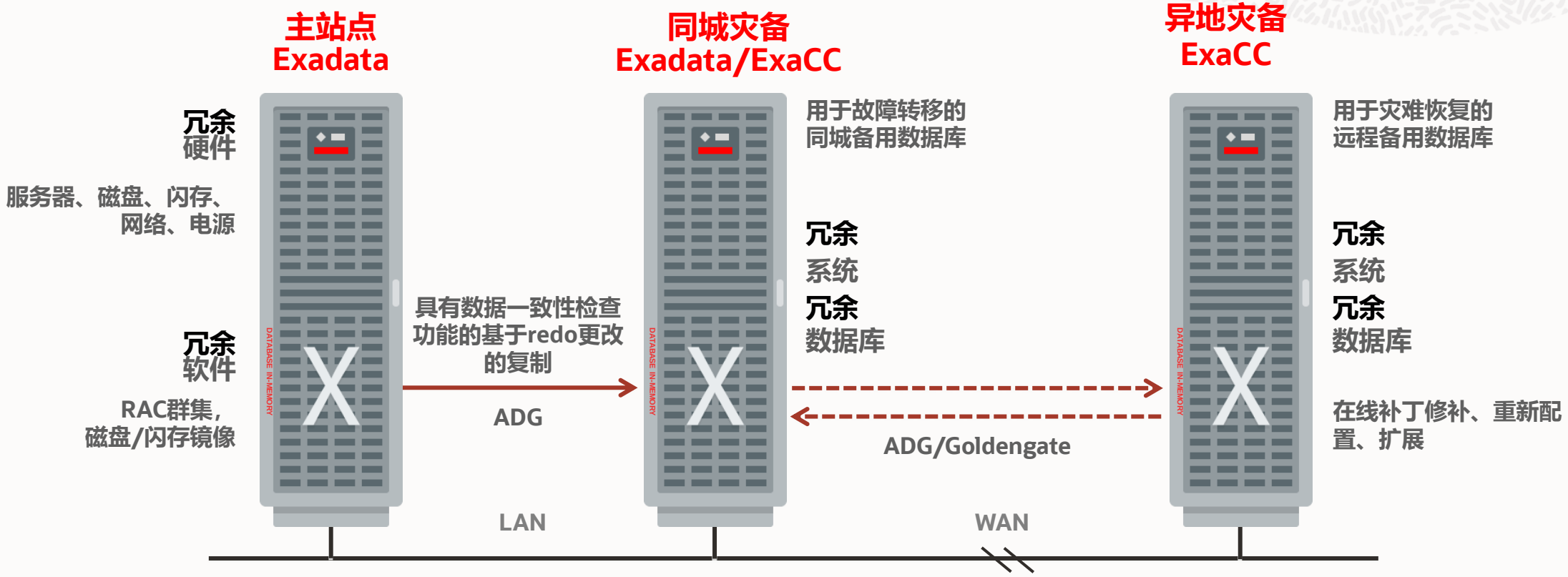
ExaCC – 弹性伸缩能力

少量CPU满足**日常容灾**需求

容灾切换时，快速扩容CPU资源

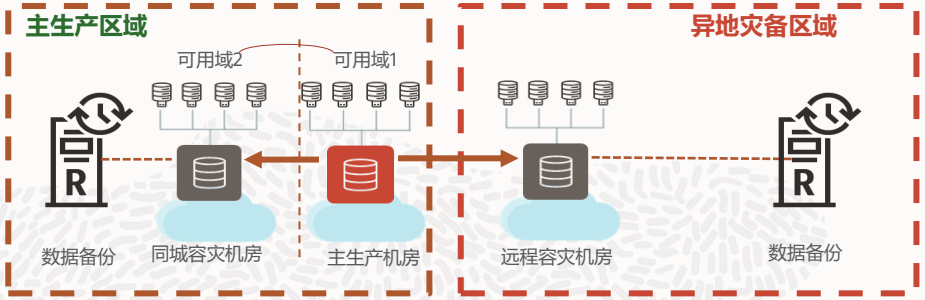
基于Exadata 的数据容灾最高可用架构

经过专门设计和测试验证的架构，可处理所有故障场景



最佳的最大可用架构数据库平台|最快的 RAC 实例和节点故障恢复|最快的备份速度 — RMAN 备份卸载到存储
深度 ASM 镜像集成| 最快的 Data Guard Redo Apply | 以最快的时间完成故障节点检测
经常更新的运行状况检查工具ExaChk

举措三：选择合适技术，匹配业务连续性需求

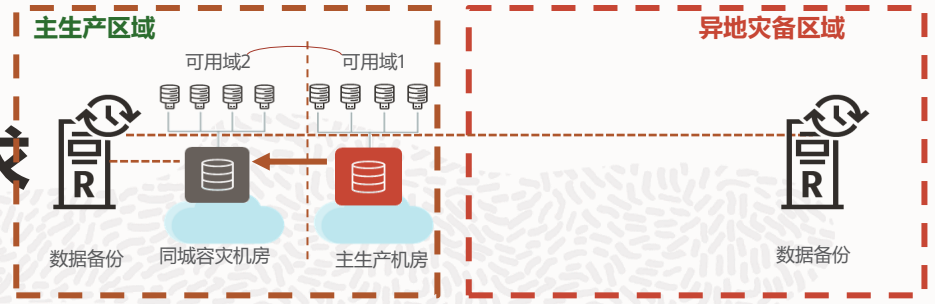


关键业务

非常重要的业务系统，业务中断、数据丢失会造成非常严重社会影响或经济损失

业务中断类型	中断原因	常见问题	RTO目标	RPO目标	本高可用	同城容灾	异地容灾	备份
计划外业务中断	计算故障	服务器故障	< 1分钟	0	RAC集群 TAC应用连续性			
		站点级故障/灾难	站点故障： <1分钟	站点故障： 0	TAC应用连续性	ADG同步复制		同城备份 ZDLRA(可选)
	数据故障		区域性灾难： <10分钟	区域性灾难： <10秒	TAC应用连续性		ADG Far Sync复制 Goldengate（可选）	异地备份
		应用/人为错误	< 1分钟	0	Flash back 闪回			同城备份
		存储故障	< 1分钟	0	ASM（存储冗余）	ADG同步复制		同城备份 ZDLRA(可选)
		逻辑数据损坏	< 1分钟	0		ADG数据块检查		备份检查验证 ZDLRA(可选)
计划内业务中断	系统变化	平台软件小版本/补丁升级	< 1分钟	0	RAC滚动升级 TAC应用连续性	ADG滚动升级		
	数据变化	存储硬件变更/数据迁移	< 1分钟	0	ADG/Goldengate			
	应用变更	应用软件版本升级	< 1分钟	0	在线重定义			

举措三：选择合适技术，匹配业务连续性需求

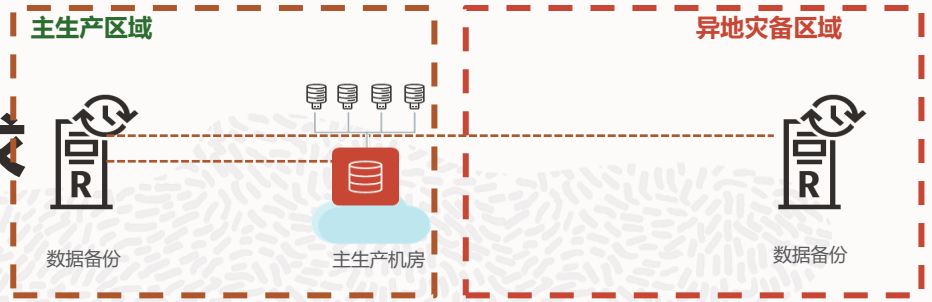


常用业务

要求完善的高可用保护，当面临站点灾难时，系统业务允许暂时中断，但要尽量减少数据丢失。

业务中断类型	中断原因	常见问题	RTO目标	RPO目标	本高可用	同城容灾	异地容灾	备份
计划外业务中断	计算故障	服务器故障	< 1分钟	0	RAC集群 TAC应用连续性			
		站点级故障/灾难	站点故障： 1小时内恢复	站点故障： <1分钟		ADG复制		同城备份
	数据故障		区域性灾难： 1天恢复	区域性灾难：、 <1小时				异地备份
		应用/人为错误	< 1分钟	0	Flashback 闪回			同城备份
		存储故障	< 1分钟	0	ASM（存储冗余）	ADG复制		同城备份
		逻辑数据损坏	< 1分钟	0		ADG数据块检查		备份检查验证
计划内业务中断	系统变化	平台软件小版本/补丁升级	< 1分钟	0	RAC滚动升级 TAC应用连续性			
	数据变化	存储硬件变更/数据迁移	< 1分钟	0	ADG/Goldengate			
	应用变更	应用软件版本升级	< 1分钟	0	在线重定义			

举措三：选择合适技术，匹配业务连续性需求



部门业务

只要求基本的系统高可用性和数据保护。

业务中断类型	中断原因	常见问题	RTO目标	RPO目标	本高可用	同城容灾	异地容灾	备份
计划外业务中断	计算故障	服务器故障	< 1分钟	0	RAC集群 TAC应用连续性			
		站点级故障/灾难	站点故障: 1天恢复	站点故障: <1小时				同城备份
	数据故障		区域性灾难: 1天恢复	区域性灾难: <1小时				异地备份
		应用/人为错误	< 1分钟	0	Flashback 闪回			同城备份
		存储故障	< 1分钟	0	ASM（存储冗余）			同城备份
		逻辑数据损坏	< 小时	0				备份检查验证
计划内业务中断	系统变化	平台软件小版本/补丁升级	< 1分钟	0	RAC滚动升级 TAC应用连续性			
	数据变化	存储硬件变更/数据迁移	< 1分钟	0	ADG/Goldengate			
	应用变更	应用软件版本升级	< 1分钟	0	在线重定义			

举措四：制定灾难恢复计划并定期演练，确保切换能力

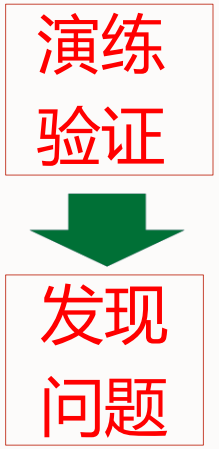
制定灾难恢复计划

- **灾难恢复目标及范围**
  - 定义灾难恢复的范围、恢复的方式、RTO、RPO
  - 确定恢复业务品种范围、需要有限恢复的网点和渠道
- **灾难宣告流程**
  - **灾难告警**，由生产运行负责人向灾备中心**预警**，主备切换；
  - **灾难评估**，负责人召集专家团进行评估，确定**是否做灾难切换**；
  - **灾难宣告**，负责人向上级、灾备中心、各业务部门宣告灾难切换，**启动灾难恢复计划。**
- **灾难恢复团队及人员构成**
  - 责任人通常是主管信息科技的**企业领导**；还包括：技术方案团队、业务方案团队、对外联络团队等 。
- **联络清单**
  - 提供灾难发生情况下的紧急联系信息，包括信息科技部、业务部、后勤支持保障等各部门，以及供应商、维保公司、客户、政府部门等。
- **灾难切换流程**
  - 灾难恢复技术团队**按预先制定的规程恢复系统**，技术解决方案团队与业务解决方案团队人员针对恢复的业务完整性、数据及时完整性、网点和服务渠道范围进行**审核和案例验证。**

举措四：制定灾难恢复计划并定期演练，确保切换能力

定期演练

小演练	• **定期（较频繁）**随机选择数据库进行**本地高可用切换**、备份数据验证，检验业务和数据的可用性；
中演练	• **每季度**对所建设的容灾数据库进行**单独切换演练**，检验切换时间RTO是否达标；
真实演练	• 确保所有最核心系统，**每年**组织真实的容灾系统的**整体全面切换演练**，检验端到端业务恢复能力。



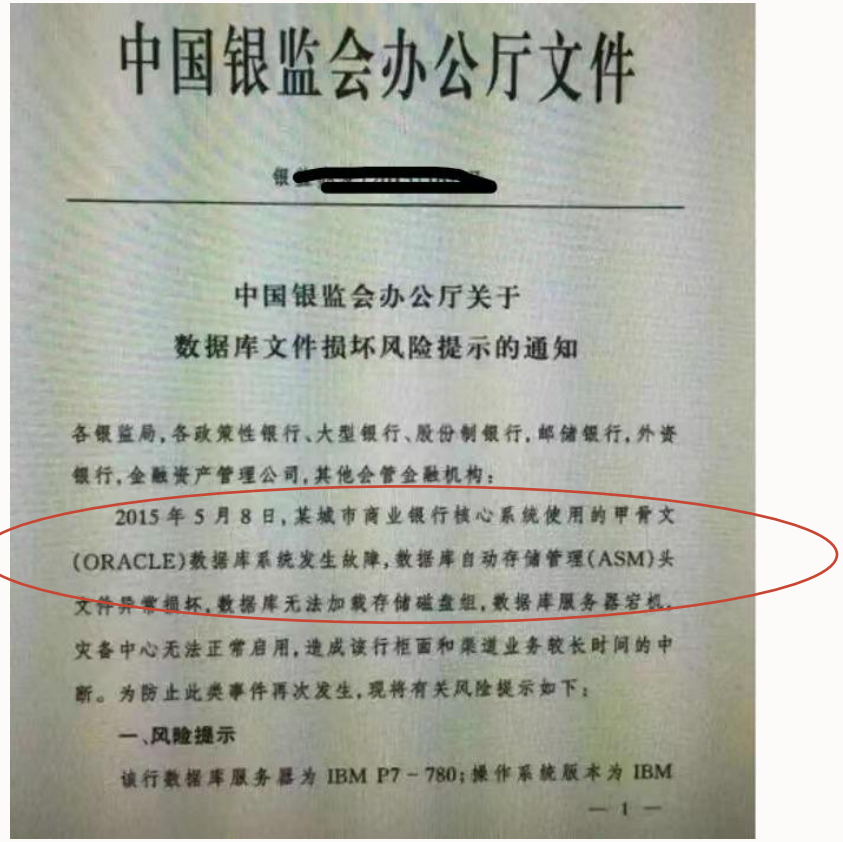
演练原则	确保所有业务连续性能力随时可用，增强操作人员对切换操作的熟练度，保证切换高效的完成。
演练内容	按照操作手册，要求被各相关人员在具体操作中做到正确、熟练的执行相关步骤。
演练要求	切换演练操作时，做到操作人员和复核人员分离。

议题

- 从业务需求出发，规划设计数据容灾体系
- 绕开数据容灾陷阱，实现容灾目标

数据容灾陷阱一：存储镜像数据块复制

存储镜像，生产端错误传递到容灾端，导致容灾功能失效



中国银监会办公厅文件

[redacted]

中国银监会办公厅关于

数据库文件损坏风险提示的通知

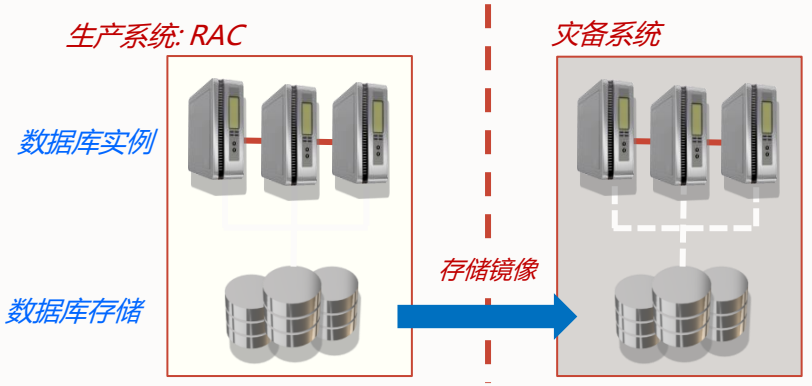
各银监局，各政策性银行、大型银行、股份制银行，邮储银行，外资银行，金融资产管理公司，其他会管金融机构：

2015年5月8日，某城市商业银行核心系统使用的甲骨文（ORACLE）数据库系统发生故障，数据库自动存储管理（ASM）头文件异常损坏，数据库无法加载存储磁盘组，数据库服务器宕机，灾备中心无法正常启用，造成该行柜面和渠道业务较长时间的中断。为防止此类事件再次发生，现将有关风险提示如下：

一、风险提示

该行数据库服务器为IBM P7－780；操作系统版本为IBM

— 1 —

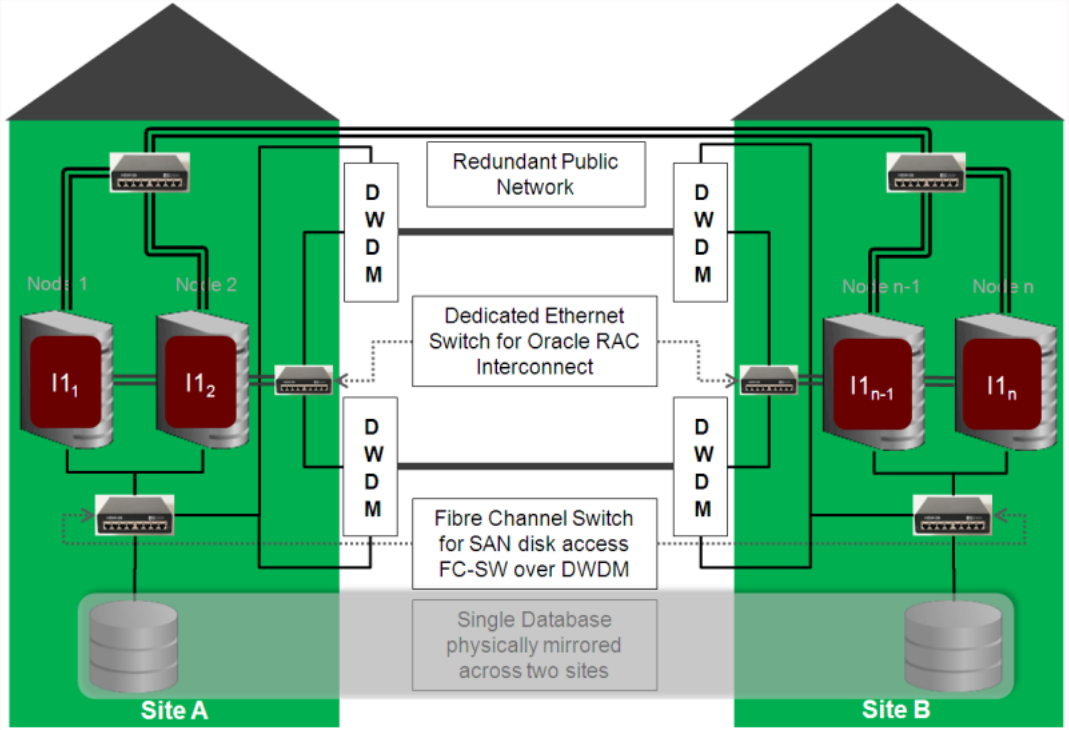


ASM 磁盘头被误操作清空，错误的数据块被存储镜像“无误”地传递到容灾端存储！

绕开陷阱： 实施ADG数据库复制容灾，同时在容灾端启用Flashback

数据容灾陷阱二：Extended RAC 双活架构

网络性能问题严重影响Extended RAC群集正常运行，影响日常生产业务运行



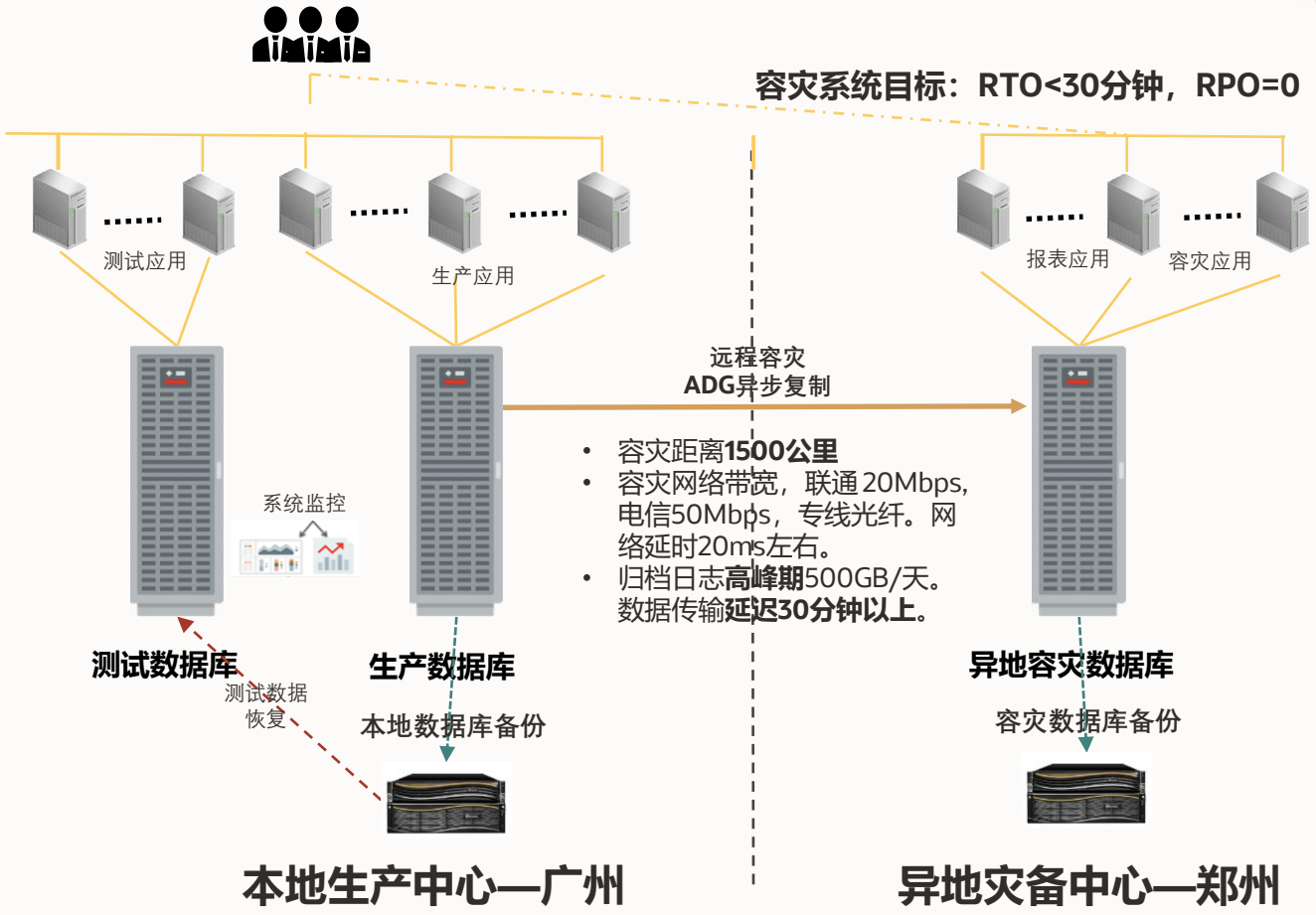
远距离Oracle RAC群集

- Extended RAC 逻辑上是一个数据库，不能防止误操作或数据块损坏传播。
- 远距离网络的性能及稳定性问题，容易导致RAC集群性能严重下降、甚至集群数据库down。

绕开陷阱：严格控制站点距离，设置第三方仲裁盘！只有一个站点处在活动状态！

数据容灾陷阱三：只注重远程异地灾备中心

远程异地灾备RTO/RPO指标难保障，真实切换失败风险较高。



- 远程容灾网络成本高昂，往往远程网络带宽不足、时延长，经常导致高峰期数据传输延迟严重。**实际RPO很难达到业务需求。**
- 业务大部分在本地，远程灾备中心资源闲置明显，**资源利用率低。**
- 关联业务系统多，切换复杂，**很难组织容灾切换演练。**

绕开陷阱：同城灾备中心能应对80%以上常见风险。在成本控制情况下，优先建设同城灾备中心，异地灾备中心以数据保护为主，条件成熟时升级到应用级保护。

数据容灾陷阱四：只关注灾备环境建设，运维管理跟不上

灾难发生时，不敢切！切不成！切的慢！

切换操作不熟练	• 导致出现故障后不敢切容灾，切换带来的二次故障风险高，依赖个别专业人才能操作
切换决策流程长	• 由于缺乏决策制度或决策流程长，当灾难发生后，无法快速决策
业务连续性技术运维不足	• 完成业务连续性高可用、应急、容灾、数据备份初始建设后，如果没有在生产系统发生变更时同步进行维护，可能导致业务连续性能力失效
缺乏真实切换演练	• 日常维护管理工作中，**主导维稳，不愿意进行真实切换演练**，对技术缺乏实践操作和验证（特别是系统发生变更后）

绕开陷阱：制定灾难恢复计划 + 切换工具软件 + 定期演练 = 敢于切！切得成！切得快！

总结

1. 国家及行业标准对灾备系统建设具有重要的指导意义

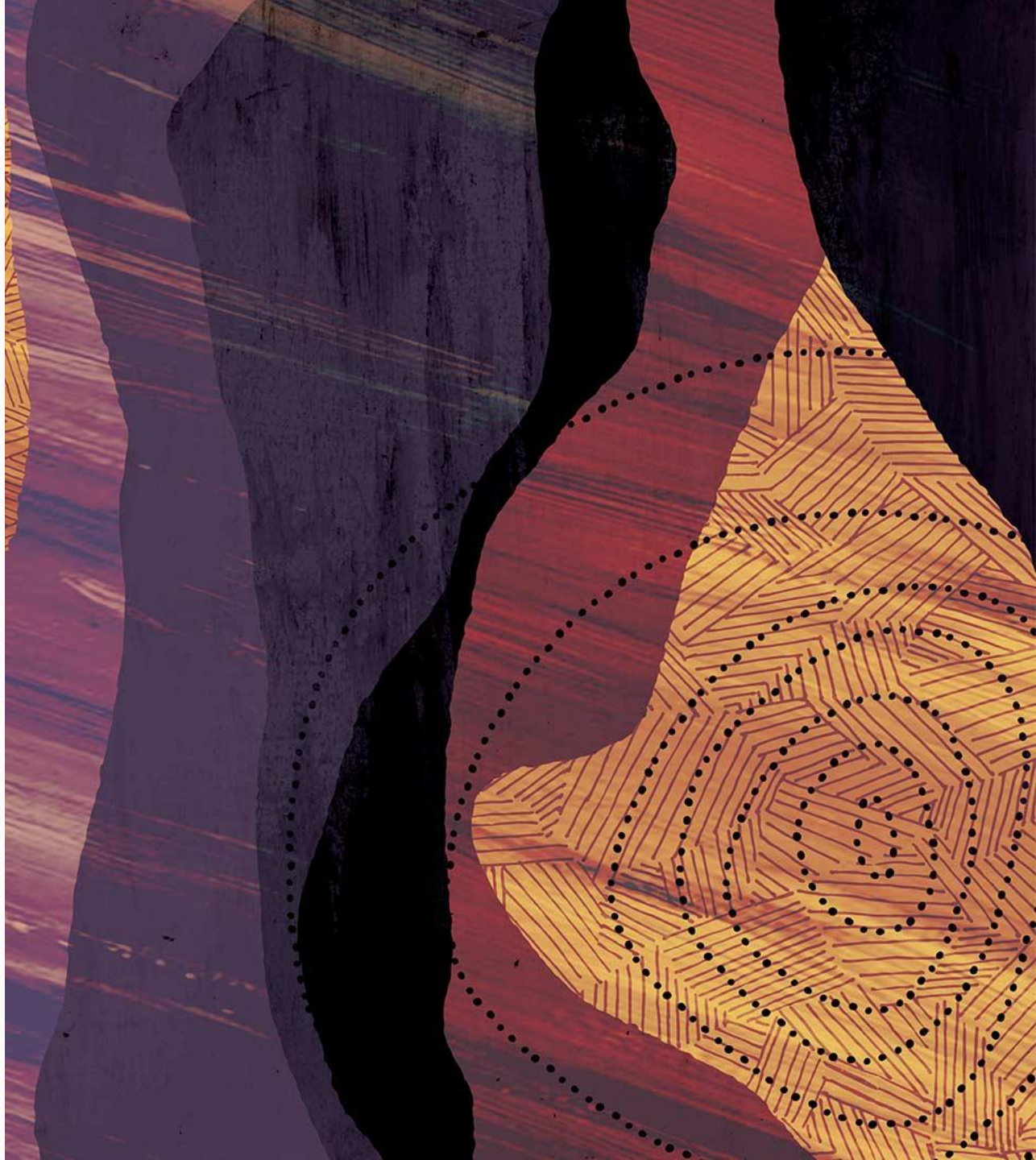
2. 灾备级别与成本成正比，需要根据成本风险平衡原则，确定业务系统的合理的灾难恢复能力等级。

3. 选择正确的灾备技术，避开灾备陷阱，保证灾备项目成功

谢谢

沈国坤
首席解决方案工程师

甲骨文中国



应用连续性规划与实战

数据库和云系列(七十三)

张羿

- 资深解决方案工程师
- 专注Oracle技术十余载，在电信行业拥有丰富的业务连续性架构实践经验

内容简介

- 某电信客户业务连续性建设实践分析
- 业务连续性建设路径

直播时间：7月8日 11:00 - 12:00

扫描二维码注册并安装手机Zoom进入直播

Zoom ID: 976 6962 5763 密码: 98039717

数据库和云讲座群

20-17

甲骨文云技术公众号

技术专家1V1深入交流