ORACLE

应用连续性规划与实践

张羿

Copyright © 2022, Oracle and/or its affiliates

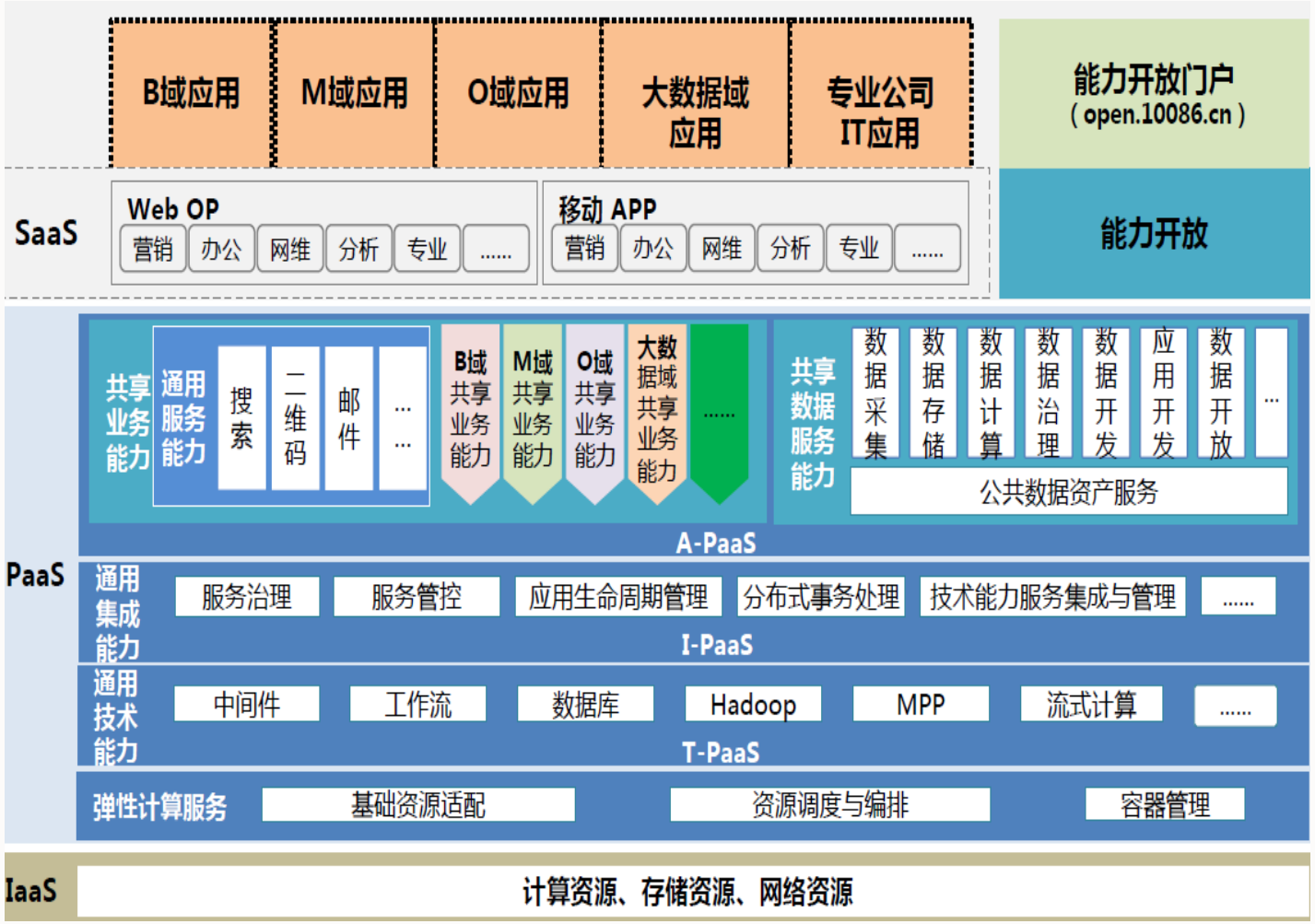
Agenda

- 某电信客户业务连续性建设实践分析
- 业务连续性建设要素分析

Copyright © 2022, Oracle and/or its affiliates

电信运营商客户超大规模的IT系统

电信运营商拥有复杂的IT系统，庞大的在线业务数据，并且用户和业务量仍然在持续增长



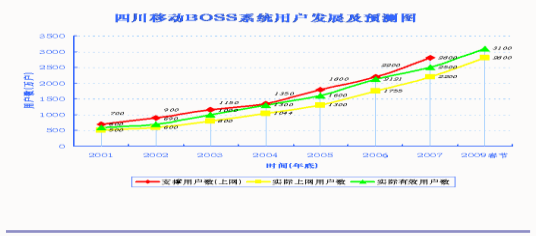
- 运营商按数据域分类（B域，O域，M域等）
- IT总体架构按照IaaS、PaaS、SaaS分层
- 统一的资源池、通用技术能力、通用集成能力、共享业务能力等面向各域的的应用系统。
- 结合统一开发管理、统一运营管理、统一安全管理，实现全网IT系统的统一管控

Copyright © 2022, Oracle and/or its affiliates

按照重要程度分级保障 – 核心，重要，一般

- 两大核心系统BOSS、CRM支撑运营商核心业务。
- 系统按层次主要分为数据采集层、中间层、数据层、接入层/展现层等
- 核心数据库使用Oracle（实时性高、处理逻辑复杂、并发量高、高稳定性、高I/O）

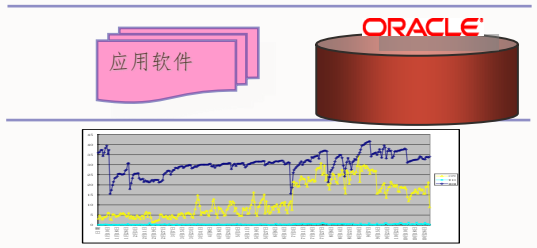
业务能力



- 有效用户数规模6000万以上
- 数据库单库容量超过20TB，单表数据量亿条
- 系统话单
- 缴费量超

电信运营商核心业务系统
具有庞大的系统规模，承载海量的关键业务，业务的连续性至关重要

系统硬件



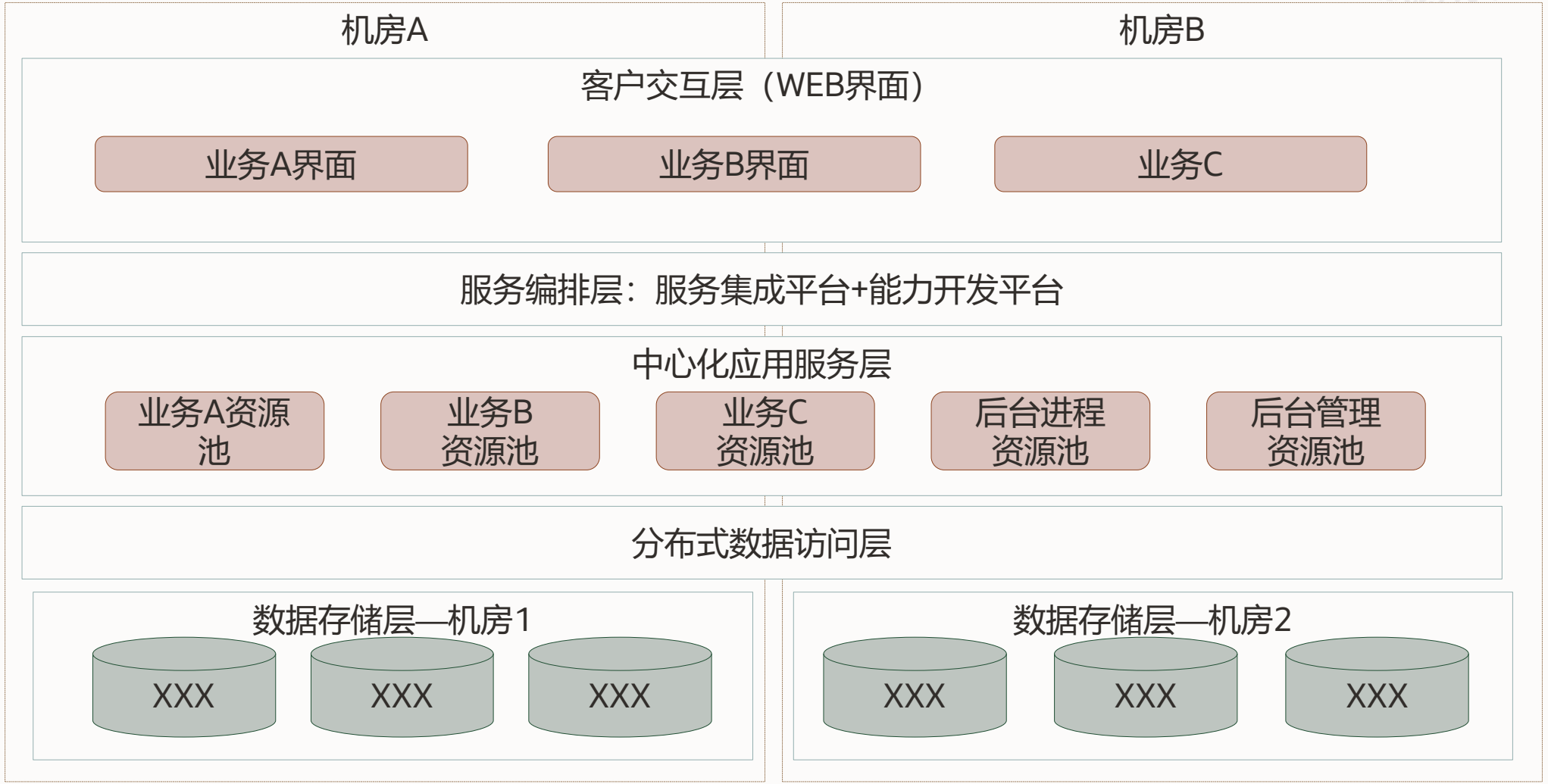
- Exadata一体机/小型机

业务中断的代价　　XXX万/小时

Copyright © 2022, Oracle and/or its affiliates

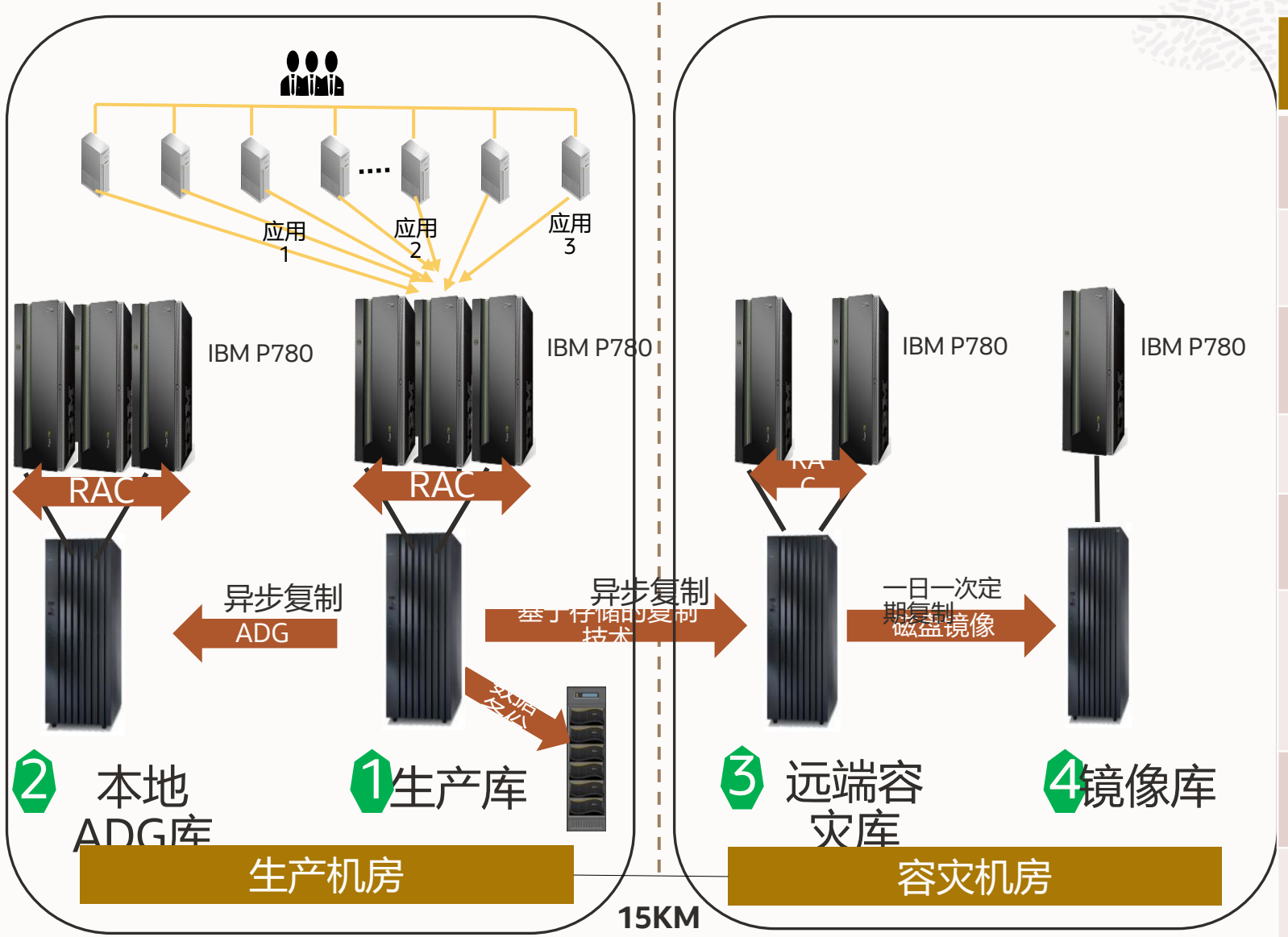
某运营商客户CRM系统架构

- ✓ 双机房部署：分A和B两个机房部署。两个机房互为备份。
- ✓ 应用层：采用**双机房应用双活模式**，可以互为应急，当一个机房应用出现故障后，另一个机房可立即接管，确保业务平稳运行。应用采用**集群化部署**，集群内高可用。**支持按渠道应用集群部署**，渠道之间物理隔离，降低相互影响。
- ✓ 数据层：采用容灾模式，两个机房互为备份；**核心数据双机房分区**部署，提升数据访问效率。



Copyright © 2022, Oracle and/or its affiliates

某运营商CRM核心系统数据库高可用部署架构



数据保护项目	指标及描述
本地ADG恢复级别	未启用far sync，RPO=1分钟；RTO<15分钟
本地ADG物理位置	同一机房的不同楼层，物理位置距离小于100米，传输延迟小于1ms。
本地应用集群切换方法	本地ADG切换后，互换Primary/Standby的IP地址，应用服务器可自动连接到主库，RTO<15分钟。
远程容灾数据库	两机房距离15公里，使用万兆带宽，延迟低于1ms；通过HDS底层复制。
切换演练频率	每年一次，演练完成后恢复到原本状态，本地ADG和远程容灾不能接管业务。
数据备份	部署Veritas NBU5230一体机，和生产库同机房。通过netbackup软件备份生产库；每周四做全备，备份时间6-8小时；每2小时备份一次归档日志。备份保存一个月，超过一个月的自动删除。
备份验证	平时无法验证备份可用性；每半年在测试环境进行恢复验证。
存储高可用配置	使用raid 6做磁盘高可用，数据文件使用裸设备。

Copyright © 2022, Oracle and/or its affiliates

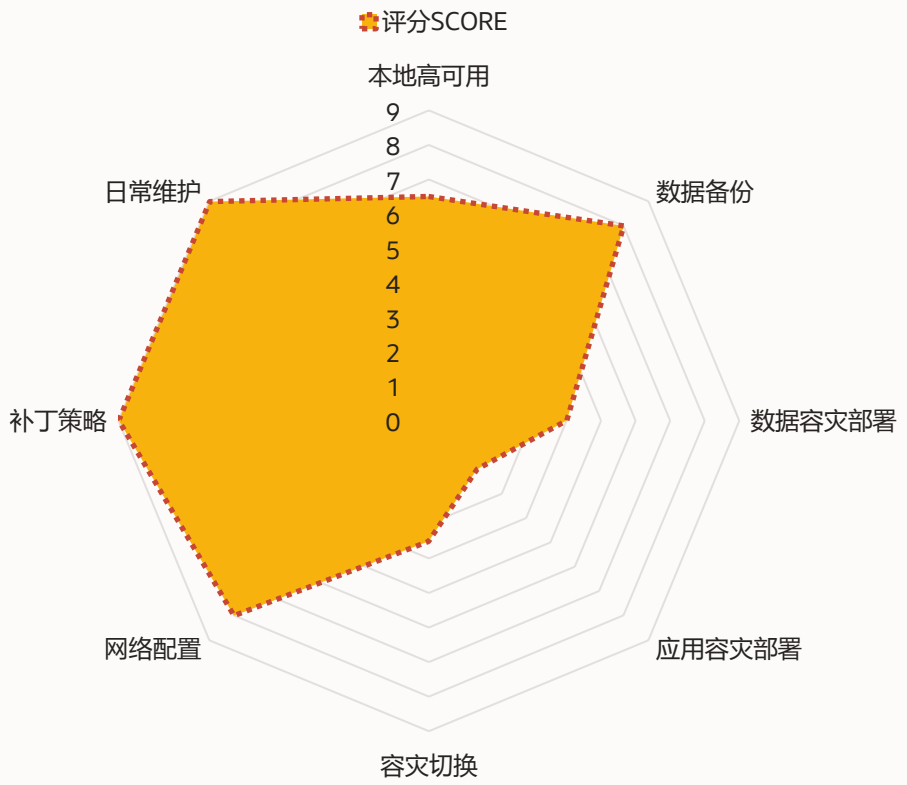
对这个运营商客户MAA高可用架构评估过程

维度	简要描述	覆盖情况
本地高可用	双冗余硬件架构，Active-active 实例，实例间快速故障切换等	
数据保护	数据备份、保存、恢复，数据坏块预防，误操作删除恢复等	
数据容灾	两地三中心架构，跨站点副本，数据同步技术等	
应用容灾	应用多中心部署，应用架构，应用故障自动切换，自动重连数据库服务等	
容灾切换	灾备切换方式，应急，切换流程，演练，灾备站点支持生产运营等	
网络	灾备站点间的网络高可用和性能等	
版本管理	软件版本策略，应用发布,上线前测试等	
日常维护	日常的监控、故障处理、健康检查等流程	

Copyright © 2022, Oracle and/or its affiliates

某运营商客户MAA架构健康风险评估（XX分，满分100）

企业MAA架构健康风险模型



1. 不能满足企业RTO以及RPO目标
   - ✓ 期望RTO=15分钟 RPO=0
   - ✓ 实际RTO=15分钟 RPO=1

2. 缺少应用容灾部署，发生站点级意外时业务将完全中断；

3. Oracle 11g版本过期，存在bug和安全风险；

4. 本地高可用方面，没有开启闪回，导致不能快速恢复逻辑错误；没有使用ASM，不能动态平衡数据库IO热点分布；

5. 数据备份还需要异地备份存放，确保数据不丢失。

6. 数据容灾方面需要启用far sync，实现RPO=0的目标。

…

Copyright © 2022, Oracle and/or its affiliates

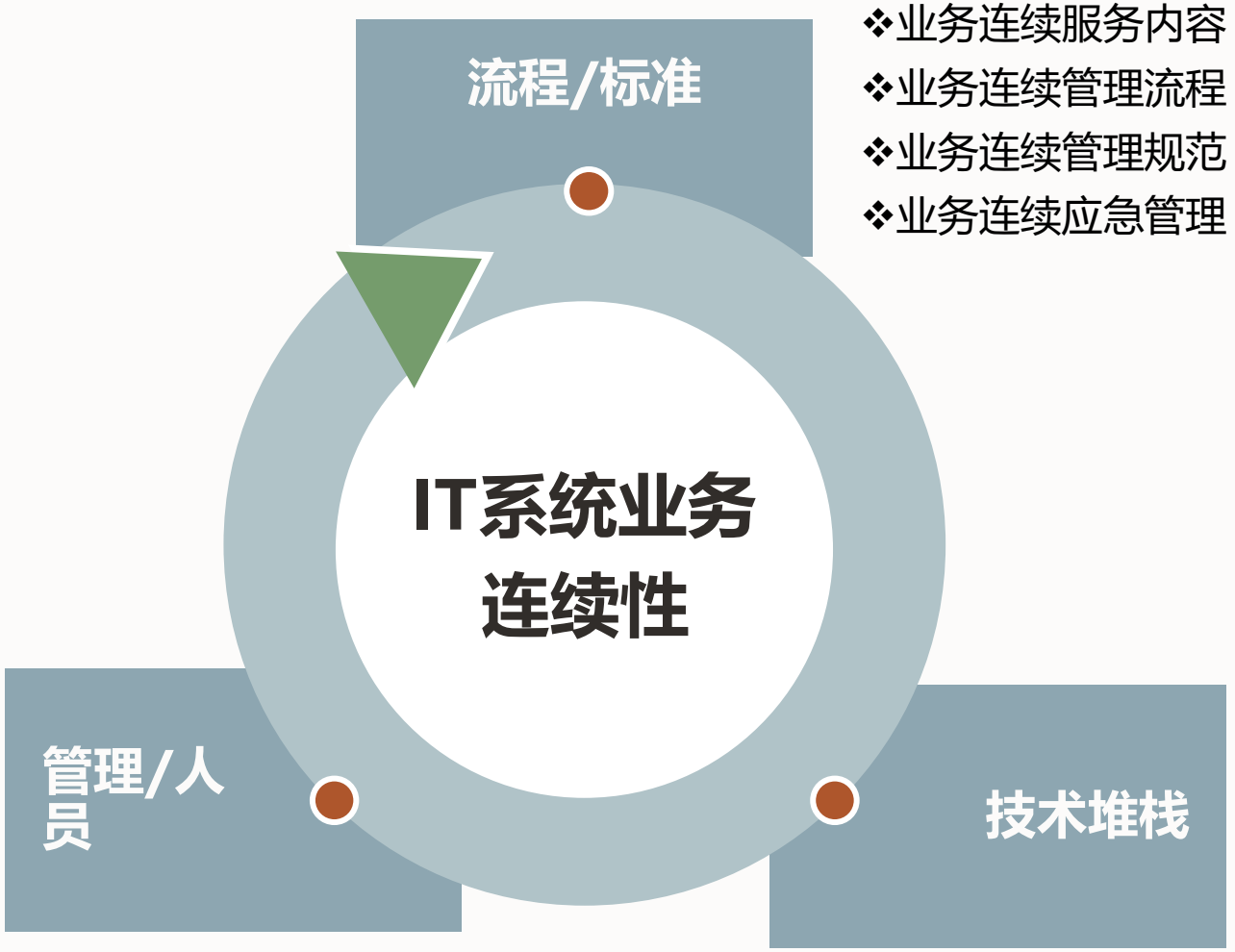
Agenda

- 某电信运营商客户业务连续性实践分析
- 业务连续性建设要素分析

Copyright © 2022, Oracle and/or its affiliates

建设业务连续性体系——三要素

❖业务连续服务目标
❖业务连续服务内容
❖业务连续管理流程
❖业务连续管理规范
❖业务连续应急管理

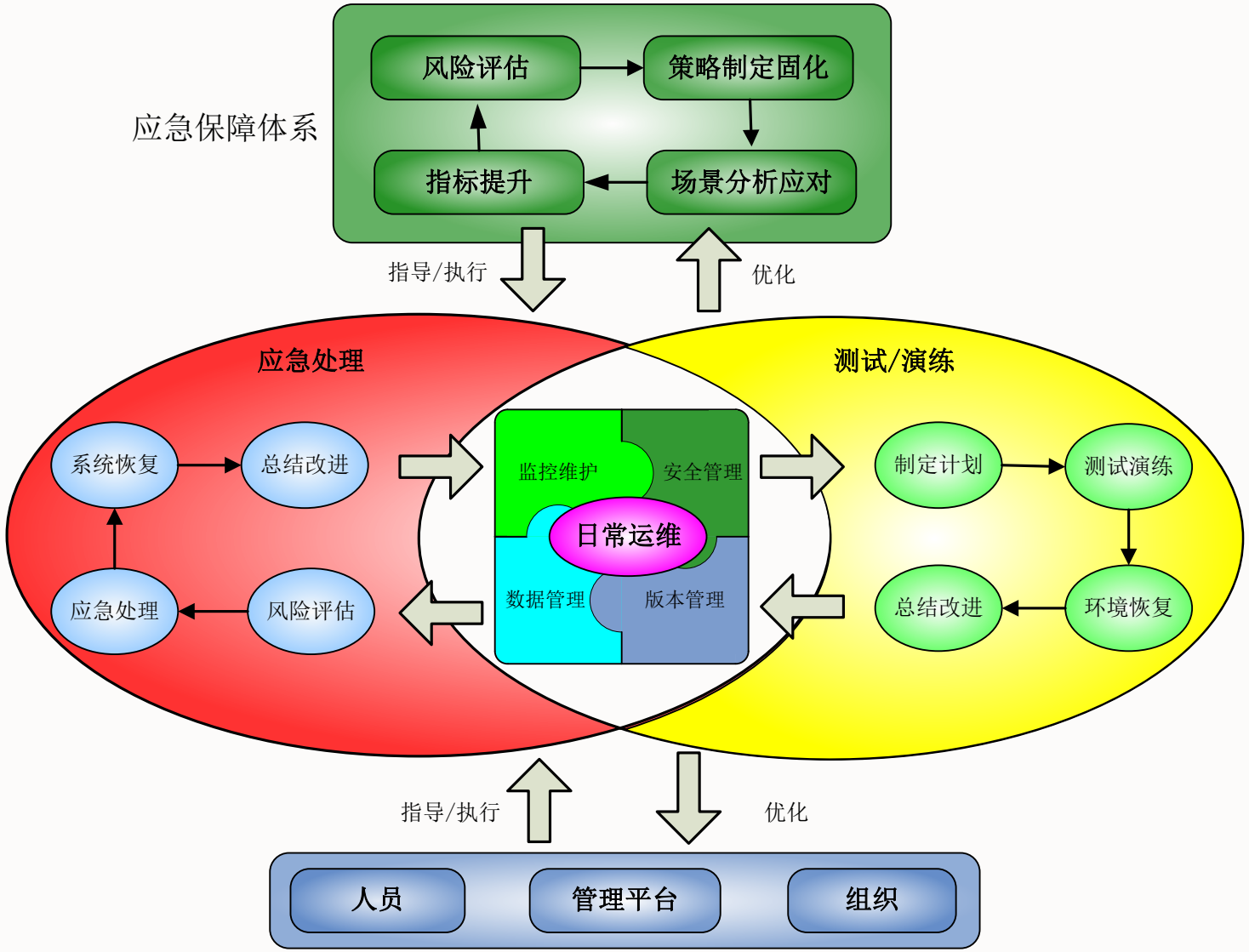


❖人员定岗
❖职责管理
❖技能
❖考核

❖在基础设施，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

Copyright © 2022, Oracle and/or its affiliates

某运营商客户应急保障体系建设



- 风险防范
- 应急保障
- 应急响应

Copyright © 2022, Oracle and/or its affiliates

系统业务评估确定业务连续性等级标准

确定业务连续性目标等级：

RTO和RPO是衡量IT系统业务连续性能力等级的重要指标

级别	恢复时间要求（RTO）	可容忍丢失的数据（RPO）
1级	2小时内恢复	数据损失
2级	4小时内恢复	分钟内的数据损失
3级	8小时内恢复	小时内的数据损失
4级	1天恢复	8小时内的数据损失
5级	可恢复，但无时间要求	一天之内的数据损失

业务连续性指标分级示例

不同关键程度的IT系统在不同风险场景下对业务连续性能力等级的具有不同目标，这是选择业务连续性技术的主要依据之一

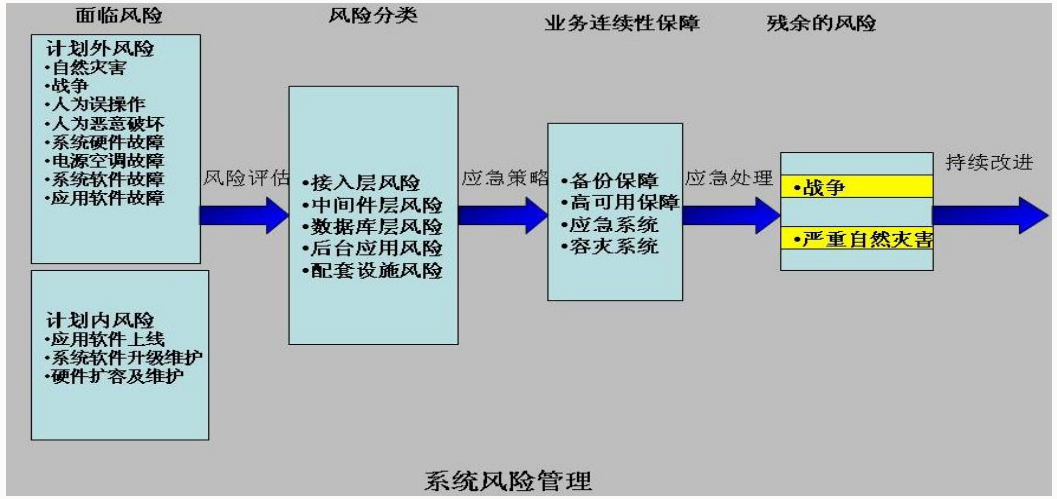
系统	一级功能	二级功能	三级功能	四级功能	业务级别	RPO	RTO
CRM	XX管理						
		XX运营支撑	XX控制	接入管理	关键	2	1
				交互控制	关键	2	1
			XX协同	请求接收与分发	关键	2	2
				业务请求处理	关键	2	2
			XX信息管理		关键	3	3
		XX运营管理	XX运营管理	渠道规划管理	非关键	5	3
				渠道信息管理	非关键	5	3

业务连续性指标级别要求示例

《业务支撑网应急保障管理办法》

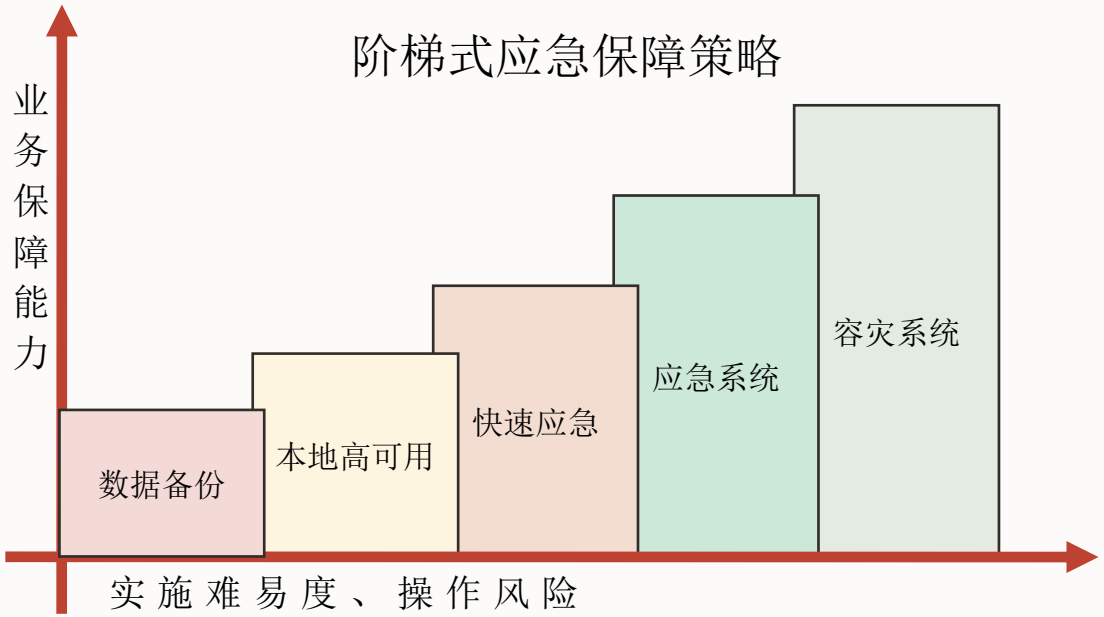
Copyright © 2022, Oracle and/or its affiliates

某电信客户业务连续性标准制定



计划外停机	严重性	频度	应对方案	时间长度
数据错误、数据丢失	中	中	数据备份	只备份关键数据，无法实现应用接管
业务逻辑错误，系统资源锁	低	高	快速应急	RTO=15分钟
软硬件多点故障、系统升级	低	高	应急系统	RTO=15分钟
人力破坏、自然灾害	高	低	容灾系统	RTO=30分钟

计划外停机



计划内维护	频率	时间长度
应用升级	每周三晚上针对部分应用程序做升级	2-4个小时
数据库或者系统升级	每年打一次PSU补丁	4个小时

计划内停机

“多位一体”的业务连续性架构

Copyright © 2022, Oracle and/or its affiliates

国信办业务连续性标准

国务院信息办发布的《重要信息系统灾难恢复指南》

Copyright © 2022, Oracle and/or its affiliates

Oracle的数据库高可用标准MAA

可用性服务级别

青铜

开发、测试

单实例数据库

本地或者云端备份/恢复，低成本但是高的RTO（恢复时间长）

白银

部门级/普通应用

青铜 +

RAC 数据库

本地灾备数据库保障应用连续性

分片（可选）

黄金

关键业务

白银 +

使用 Active Data Guard 进行远端数据库复制，实现灾备目的

白金

极端关键业务

黄金 +

ADG+GoldenGate多数据中心多可用区域AD保护

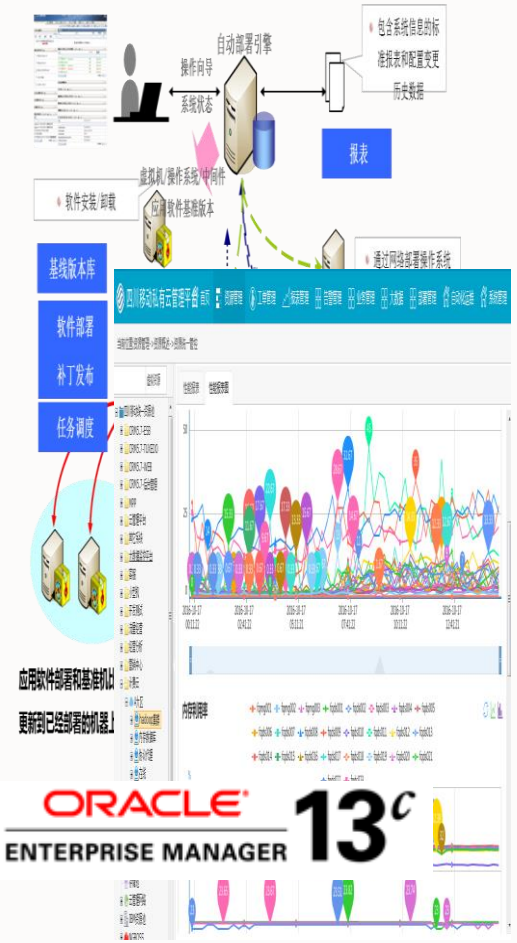
基于版本的重新定义 Edition based redefinition

所有层都可在于私有云和公有云中实现

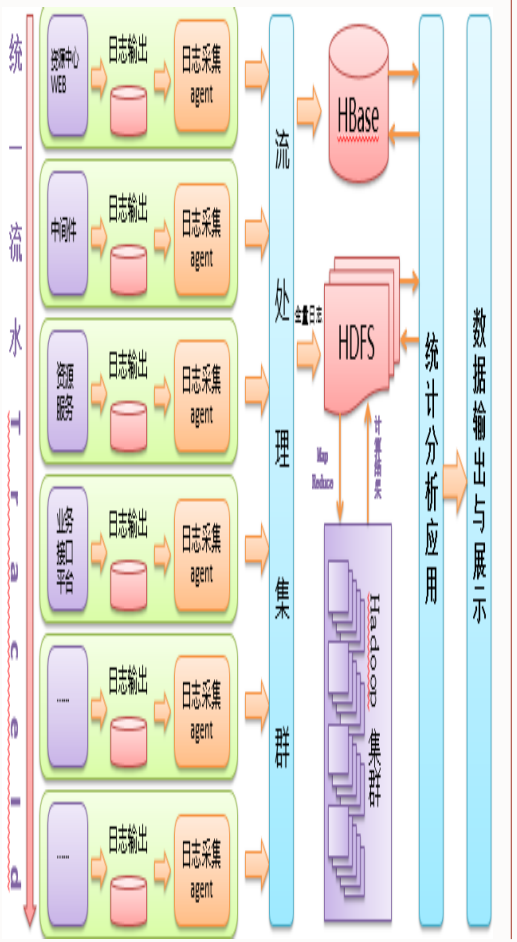
Copyright © 2022, Oracle and/or its affiliates

某电信客户业务连续性保障管理平台

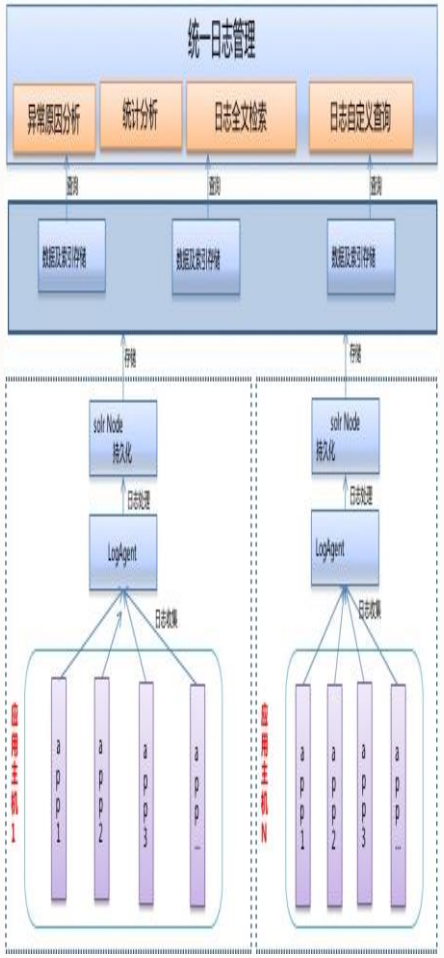
云管理平台能力



端到端监控



统一日志平台

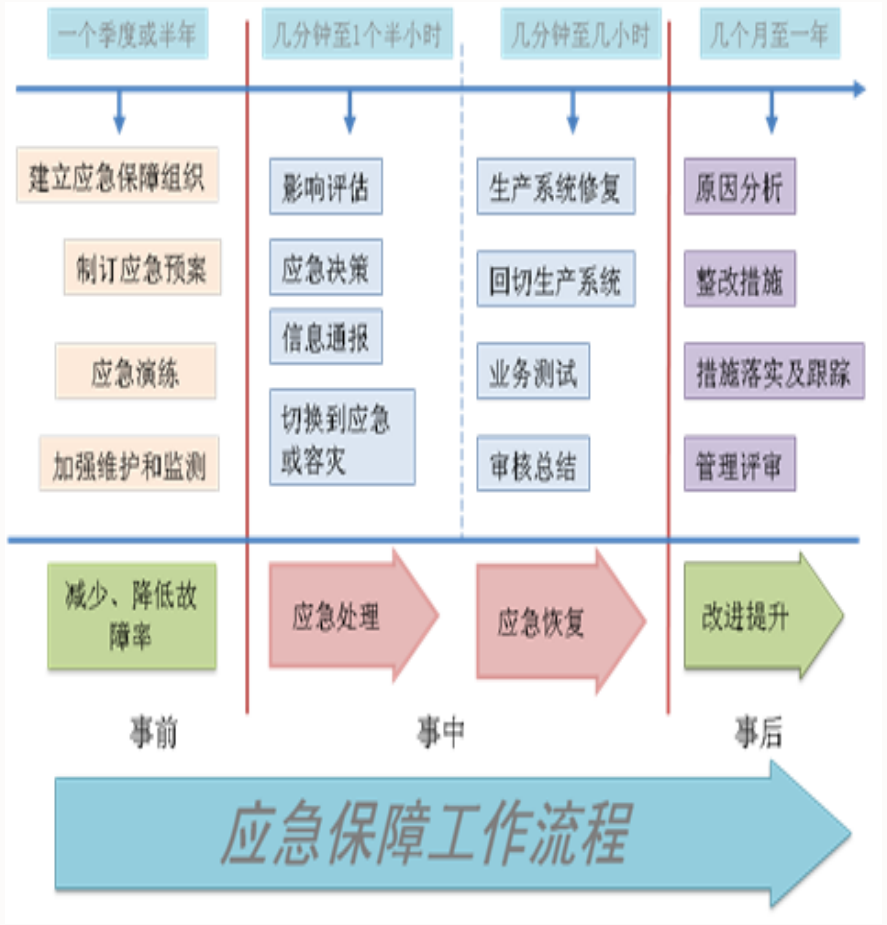


1. 界面化
2. 流程化
3. 自动化

完善运维管理并定期演练，确保切换能力

为什么有些企业花费巨资建设的应急、容灾系统在关键时刻没有发挥作用?

为什么即使应急、容灾系统应用了快速切换、业务快速恢复的技术，平时仍然不敢切换应急、容灾?



业务场景	数据库主机	中间件主机	应用主机	网络
前台无法使用	参照4.1、4.3、4.5、4.7等章节	参照5.1、6.1章节	参照11章节	参照12章节
业务受理缓慢	参照4.1、4.3、4.5、4.7等章节	参照5.1、6.1章节	参照11章节	参照12章节
缴费无法开机	参照4.1、4.5等章节	参照5.2章节	参照11章节	参照12章节
一级BOSS业务办理失败	参照4.1、4.3等章节	参照5.2章节	参照11章节	参照12章节
用户数据上传失败或延迟	参照4.1、4.3等章节	参照5.2章节	参照11章节	参照12章节
数据误删除和逻辑错误	参照3.6等章节			

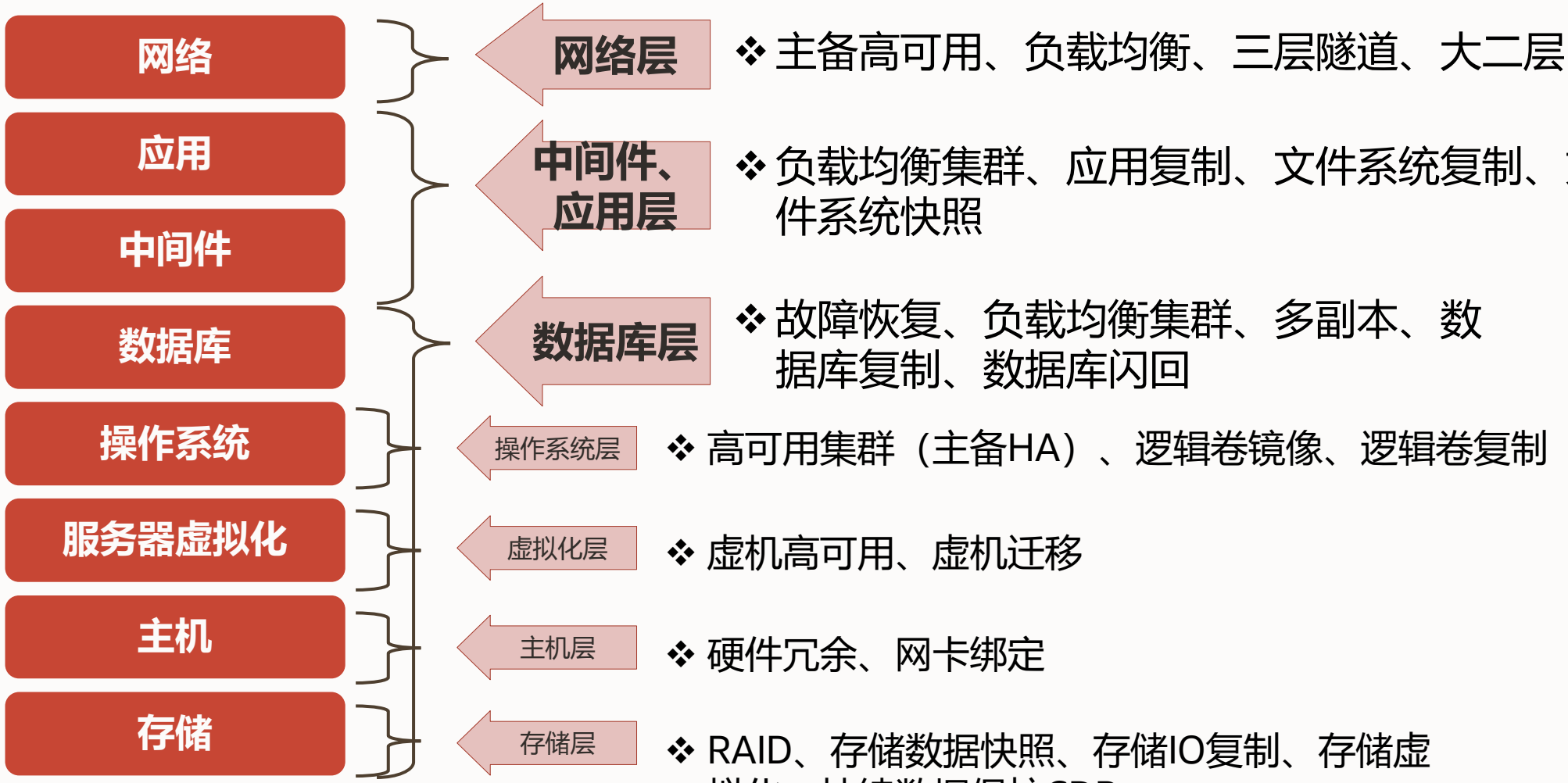
不敢切→敢于切!

切不成→切的成!

切的慢→切的快!

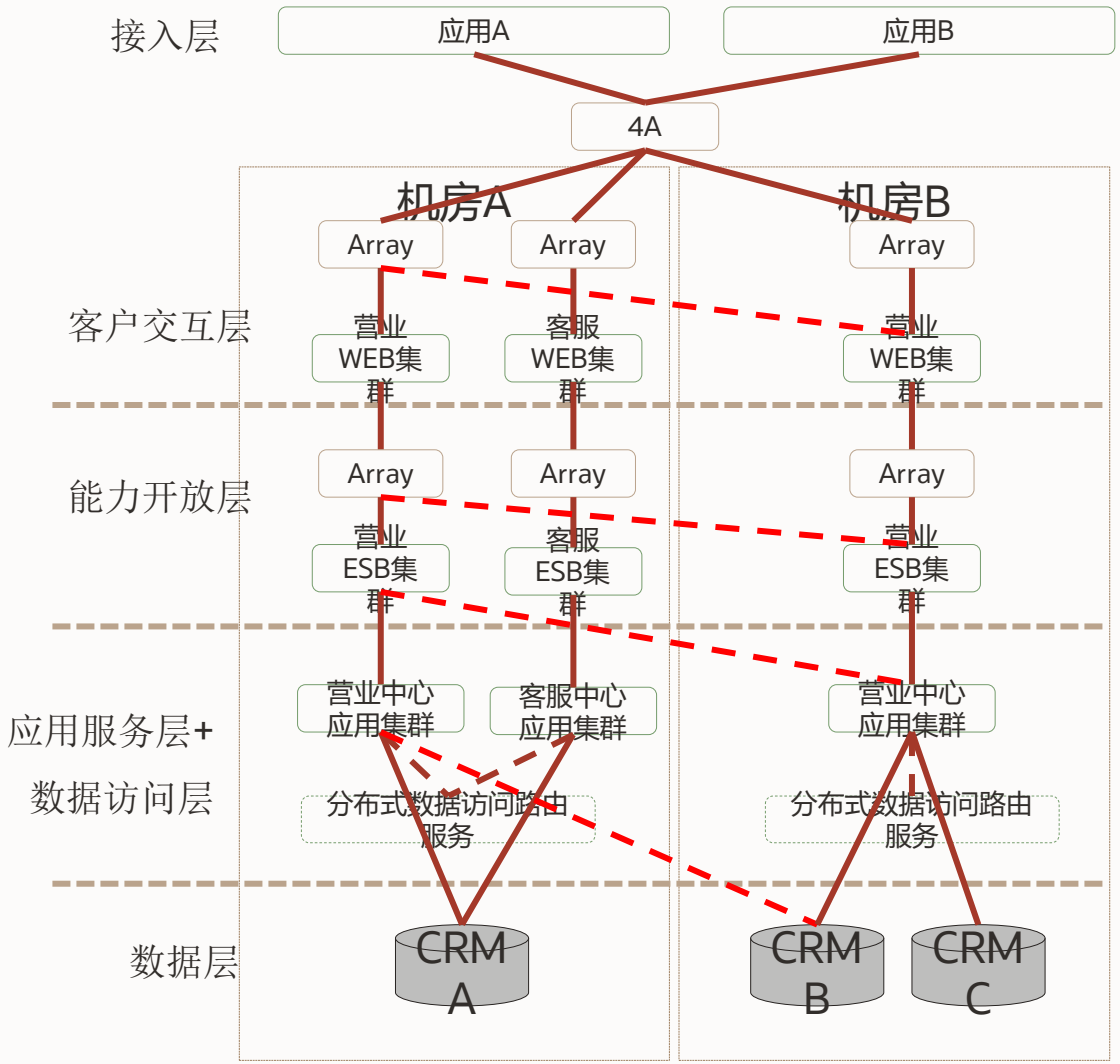
Copyright © 2022, Oracle and/or its affiliates

选择最合适技术，打通技术堆栈进行有机集成



Copyright © 2022, Oracle and/or its affiliates

某电信运营商客户系统高可用技术堆栈



用户交互层	✓ 四层交换接入：营业和客服渠道根据IP路由；路由到不同的机房；由四层交换实现WEB层的高可用。 ✓ 会话保持：WEB会话进行缓存。
服务编排层	✓ 四层交换接入：ESB采用集群部署，外部使用四层交换机访问ESB，由四层交换实现ESB的高可用。 ✓ HSF路由：在ESB中集成HSF客户端，由HSF客户端选择最佳中心服务。
应用服务层	✓ 集群部署：采用虚拟机部署；每台虚拟机可同时部署联系比较紧密的中心，避免跨网络访问，提高访问效率。 ✓ 应用无状态：可以动态增加或减少中间件主机。
分布式数据访问层	✓ 分布式数据库代理：mysql集群部署，对外使用分布式数据库代理访问，功能上实现数据切片、读写分离、Failover。 ✓ 数据路由：对ORACLE的数据访问，提供独立的路由服务，提高数据访问效率
数据存储层	✓ Oracle数据库：采用双机房分区部署；做数据容灾； ✓ Mysql：采用master/slaver的部署模式； ✓ 缓存：分布式部署，提高业务访问效率； ✓ Hadoop（HBASE、HDFS）：内部多备份存储。
分布式后台进程	✓ 后台进程集群：使用分布式后台调度平台（Fortress）做集群部署，内部实现负载均衡和Failover。 ✓ 跨机房：支持跨机房部署；可在机房之间Failover。

Copyright © 2022, Oracle and/or its affiliates

数据层：Oracle MAA与业务连续性的关系

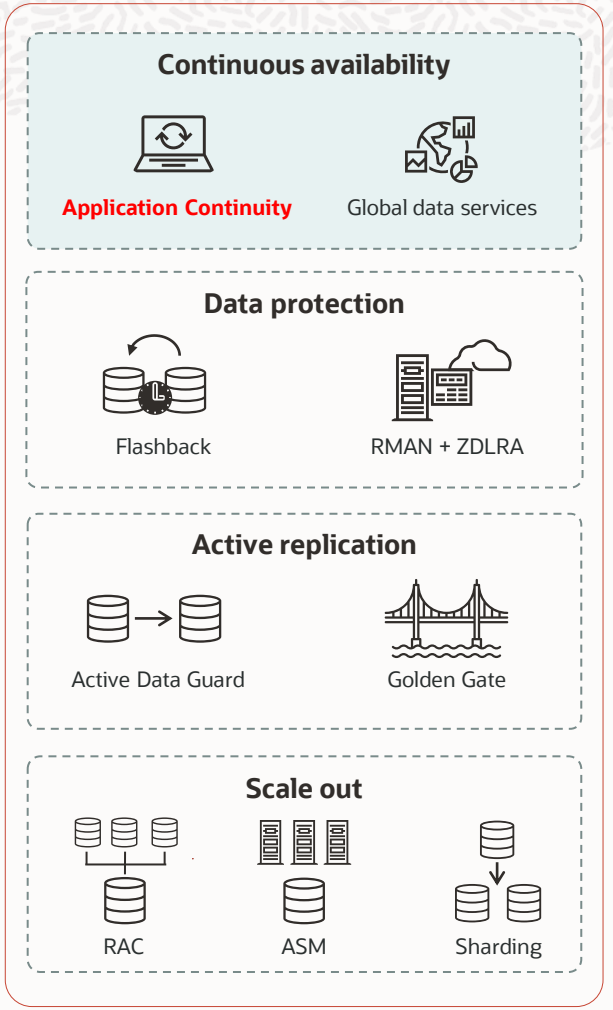
应用系统	柜面系统、核心交易、报表分析、用户认证……
平台系统	服务器、操作系统、集群与数据库、中间件……
数据系统	结构化数据、非结构化数据、存储系统……
网络系统	交换机、负载均衡、防火墙、防病毒……

1. 数据库及业务数据是整个IT系统的心脏，业务正常运转离不开数据库系统的健壮运行
2. 数据库系统不能像硬件一样简单冗余设计即可，坏一个设备不至于影响整体，在数据库体系中，坏一个数据块也可能影响业务连续性
3. 数据库层面的容灾部署MAA架构是高可用基础
4. 应用与数据库的MAA高可用深度集成，实现业务的连续性
5. 数据的保护是业务连续性的最后防线
6. 高可用的运维平滑实现业务连续性
   - 故障/灾难发生的预案、流程，运维团队的切换演练、定期的生产切换

Copyright © 2022, Oracle and/or its affiliates

透明应用程序连续性(TAC)

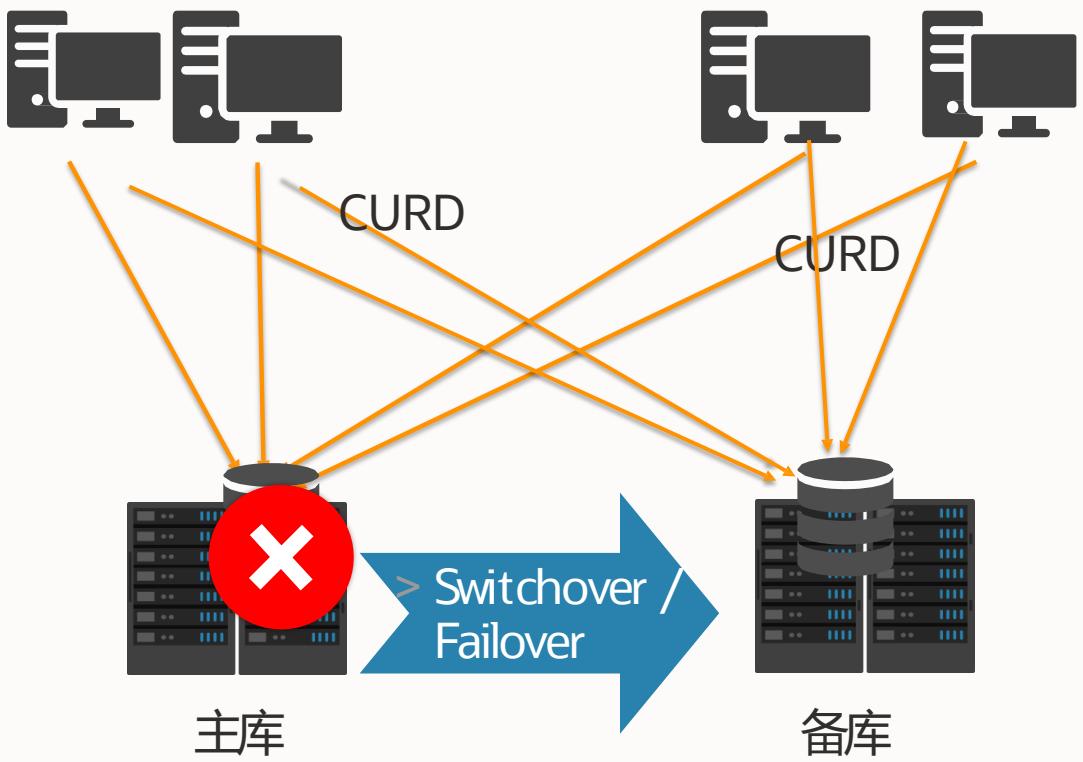
青铜	白银	黄金	铂金
开发, 测试, 生产	**生产**	**Business critical**	**Mission critical**
单实例数据库 可重启 备份/还原	**青铜 +** Database HA with RAC **Application continuity**	**白银 +** DB replication with active data guard	**黄金 +** Golden Gate Edition based redefinition



Copyright © 2022, Oracle and/or its affiliates

透明应用程序连续性(TAC)

应用高可用性到透明应用连续性



- 使用应用程序连续性和 Oracle Real Application Clusters
- 在出现故障时透明地跟踪和记录会话信息
- 内置于数据库内部，因此无需任何应用程序更改即可工作
- 重建会话状态并在计划外失败时重放进行中的事务
- TAC 可以处理计划内维护，以从一个或多个节点排出会话
- 适应应用程序的变化：为未来而保护

Copyright © 2022, Oracle and/or its affiliates

Application continuity
故障转移解决方案

	TAC	AC	TAF	Draining
I don't know how the application is implemented	Yes	No	No	Yes
My application does transactions	Yes	Yes	No for unplanned Transactional disconnect only	Yes
My application uses Oracle state (temp lobs, PL/SQL, temp tables.)	Yes	Yes No for static mode	No	Yes
My application does not use connection pools	Yes	No	Yes	Yes
My application has side effects (such as file transfers)	Yes Side effects are not replayed	Customizable	No	Yes
My app needs Initial State Restored	Yes and custom	Yes and custom	Yes and custom	Yes
Future proofed for application changes	Yes	No	No	Yes

会话故障转移的标准解决方案是Transparent Application Continuity（TAC）。19c New

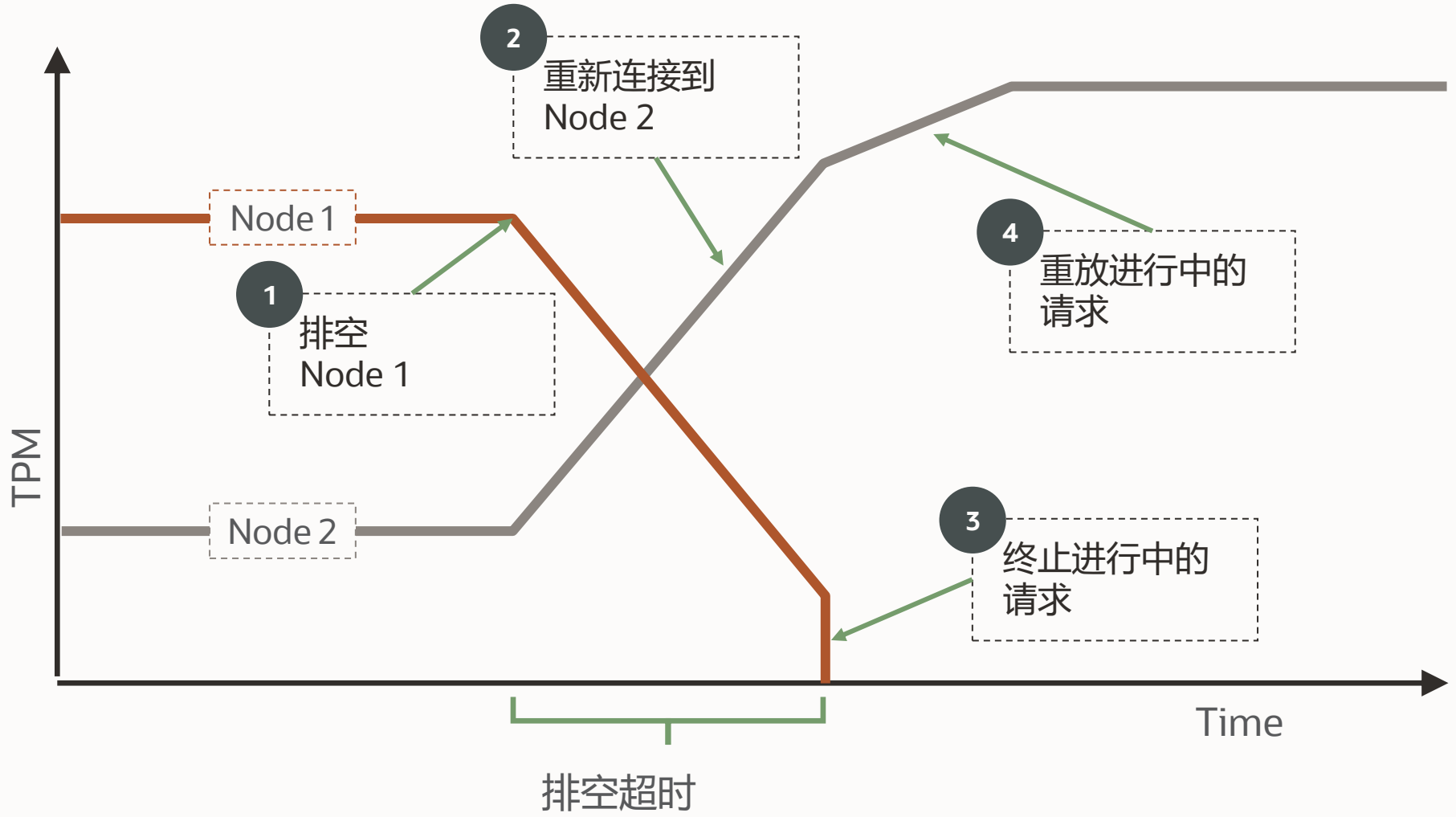
如果您使用的是Oracle Database 12c第2版，或者要在事务中使用回调进行自定义，需要使用Application Continuity（AC）。

如果您的应用程序是只读的，并且在初始设置后未更改会话中的Oracle会话状态，请使用Transparent Application Failover （TAF）。

Copyright © 2022, Oracle and/or its affiliates

TAC如何在计划内停机情况下实现故障转移

排空… 重新连接… 故障转移



Copyright © 2022, Oracle and/or its affiliates

关于TAC的相关资源

Application Continuity product page -> https://www.oracle.com/goto/ac

Technical briefs (how to/explanations/details) ->

Deployment Checklist (for developers, dba's and application owners)

- https://www.oracle.com/technetwork/database/clustering/checklist-ac-6676160.pdf

Fast Application Notification (FAN) – everything anyone would want to know about FAN

- https://www.oracle.com/technetwork/database/options/clustering/applicationcontinuity/learnmore/fastapplicationnotification12c-2538999.pdf

Copyright © 2022, Oracle and/or its affiliates

如何看待数据库“双活”

Extended RAC不是Oracle数据库双活容灾解决方案

比较项	Oracle ADG	Oracle OGG	Oracle数据库RAC远程集群
技术特点	为Oracle数据库容灾最佳解决方案，备用系统可以处于只读状态称为报表或者查询库分担主库的要求	是数据库的CDC工具，主要应用场景为数据分发汇总等；也可以用于容灾	是把RAC集群置于同城异地的一种“双活”解决方案，其特点为物理容灾逻辑单一数据库，本质不是双活
双活	主机生产，备机为只读查询	备用机的数据库处于工作状态，可以读写，可以和生产系统互为备份，主备机的处理压力相互传递，需要解决数据冲突问题	处于异地的RAC双节点或者多节点都处于工作状态
生产性能影响	同步模式，生产性能对距离和延迟敏感 异步模式，对生产性能无影响	Ogg如果安装到生产系统通常占用CPU小于5%	生产性能对距离和延迟敏感，恶劣情况下导致脑裂和生产不稳定
站点距离限制（延迟限制）	同步模式，低于5ms（通常小于20公里） 异步模式，无距离限制	无距离限制	低于5ms（理论要求电缆距离小于100公里，通常小于20公里）
切换时间RTO	<5分钟	备机处于工作状态，数据库切换时间理论上为零，但是数据同步为异步方式，考虑尽可能少丢失数据需要等待备机追平日志	非故障实例需要做实例恢复需要分钟级时间
数据丢失RPO	活支持同步、异步模式，同步工作模式下数据零丢失，另外Fast Sync模式提供了两地三中心的数据库容灾解决方案	工作模式为异步模式，可能丢失数据	处于异地的存储是由ASM或者第三方工具提供的数据同步模式，对于单点数据损坏有保护作用，但无法防止数据库逻辑故障
网络带宽需求	低，每秒生成日志量/70%	通常为每秒生成日志的1/3到一半	高，全量IO复制

Copyright © 2022, Oracle and/or its affiliates

总结：三要素结合共同保障IT支撑系统业务连续性

评估业务连续性需求

建立完整的保障体系

选择合适技术，打通技术堆栈

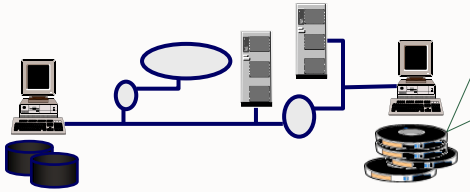
和业务应用软件融合，形成端到端能力

定期演练，熟能生巧

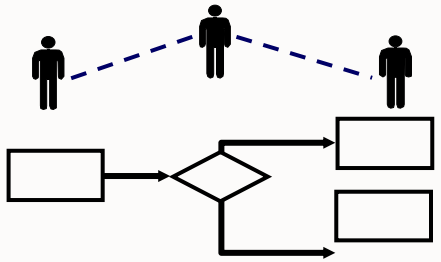
业务需求

系统	一级功能	二级功能	三级功能	四级功能	业务级别	RPO	RTO
CRM	渠道管理						
		渠道运营支撑	渠道控制	接入管理	关键	2	1
				交互控制	关键	2	1
			渠道协同	请求接收与分发	关键	2	2
				业务请求处理	关键	2	2
			接触信息管理		关键	3	3
		渠道运营管理	基础运营管理	渠道规划管理	非关键	5	3
				渠道信息管理	非关键	5	3

技术体系保障



管理/人员和流程保障



完善的**技术体系**是保障IT支撑系统业务连续性的关键基础和前提，才能实现保护核心数据安全，让企业生产应用不间断运行、为客户持续提供服务的目标。

Copyright © 2022, Oracle and/or its affiliates

Copyright © 2022, Oracle and/or its affiliates