

ORACLE
甲骨文

MAA 方法论

数据库和云系列(七十九)



范宏伟

- 资深解决方案工程师
- 专注数据库技术领域十余载，对Oracle MAA领域有深入了解和电信行业业务连续性架构实践经验

2022年6月10日

内容简介

- Oracle 最大可用性架构介绍
- 8大维度业务连续性评估模型



直播时间：5月13日 11:00 - 12:00
扫描二维码注册并安装手机Zoom进入直播
Zoom ID: 919 7151 8106 密码: 58317986
https://oracle.zoom.us/webinar/register/WN_-EKAb7hwSH-XLBtmb773Mg



每周五上午 11:00 ~ 12:00
扫描二维码安装手机Zoom进入直播
https://oracle.zoom.us/webinar/register/WN_-EKAb7hWSH-XLBtmb773Mg
Zoom ID: 919 7151 8106 密码: 58317986



行业大咖、技术大拿专业直播分享



甲骨文数据库与云系列公益讲座

甲骨文数据库、一体机、云服务最新前沿技术、优秀案例及解决方案分享。
加入19c 公益课微信群，获取更多技术资讯



甲骨文云技术
官方微信公众号

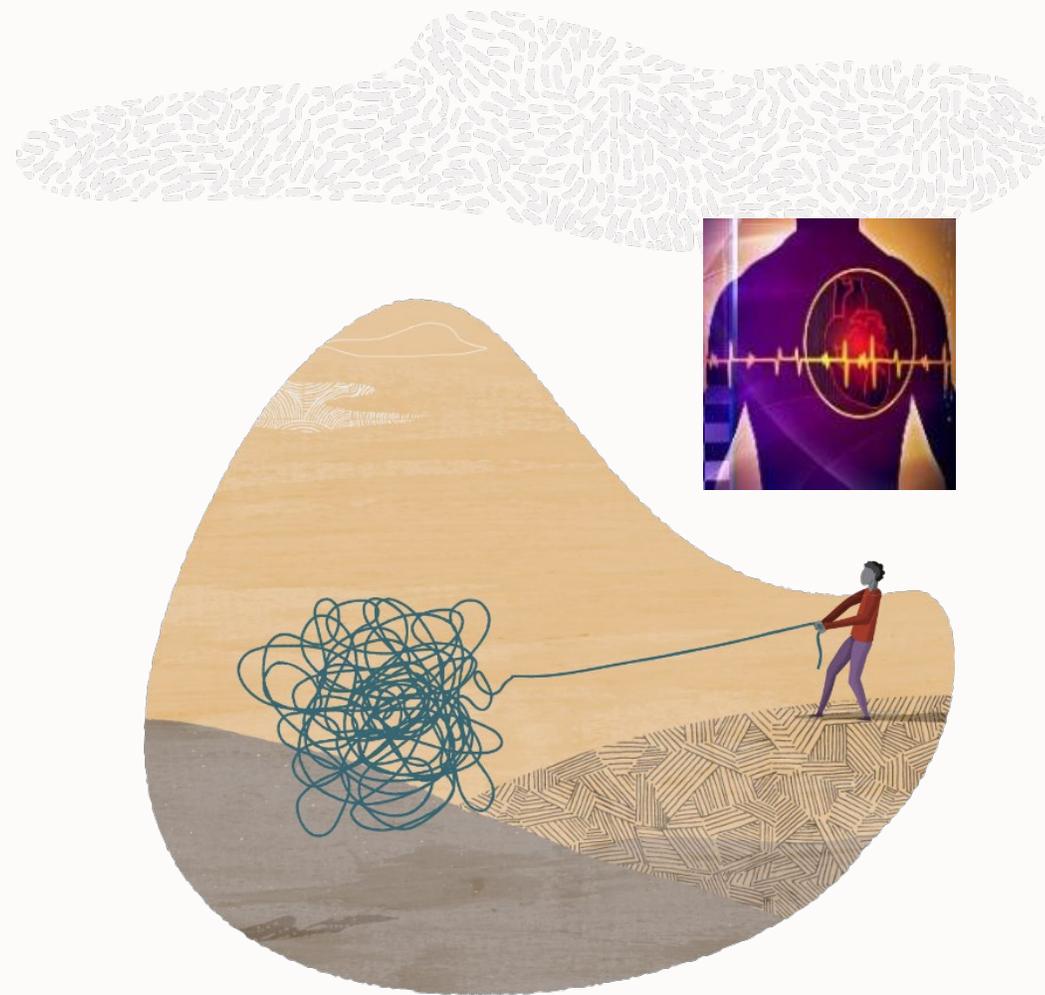


ORACLE

Oracle MAA方法论

范宏伟

2022年6月10日

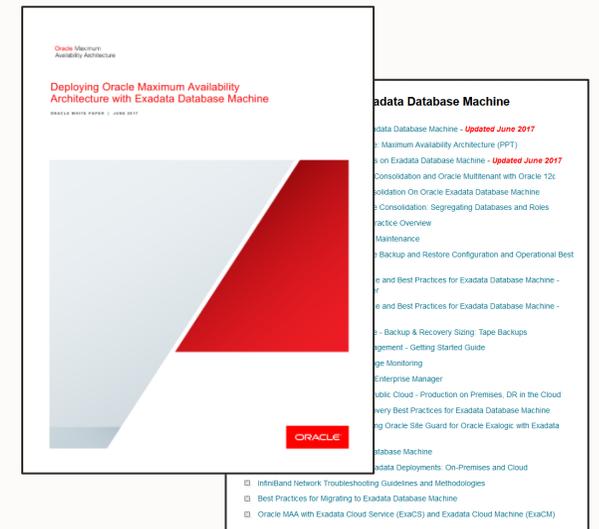
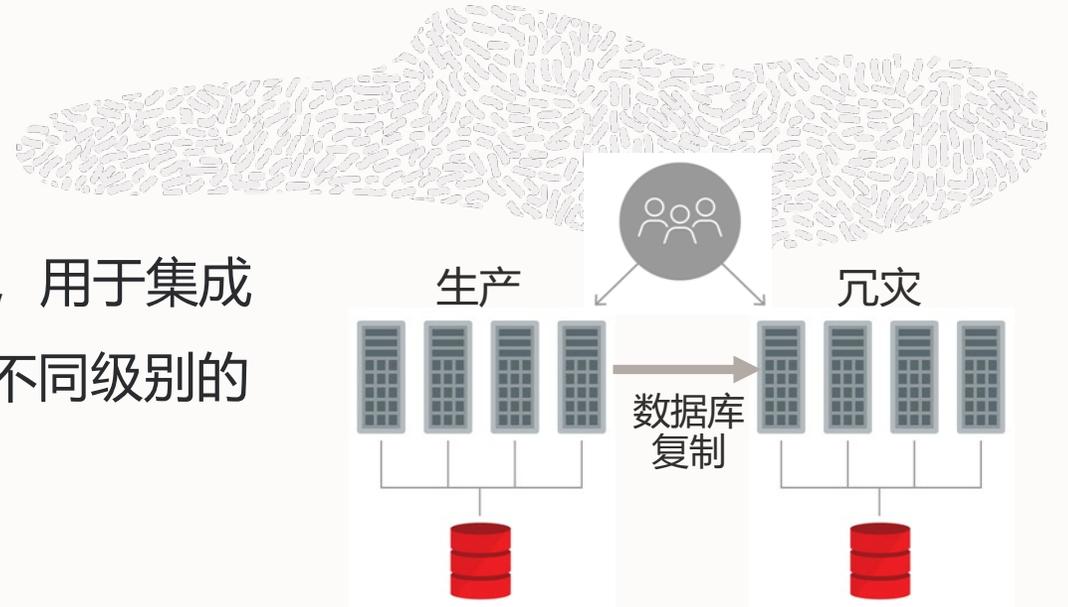


Oracle数据库最大可用性架构 (Maximum Availability Architecture)

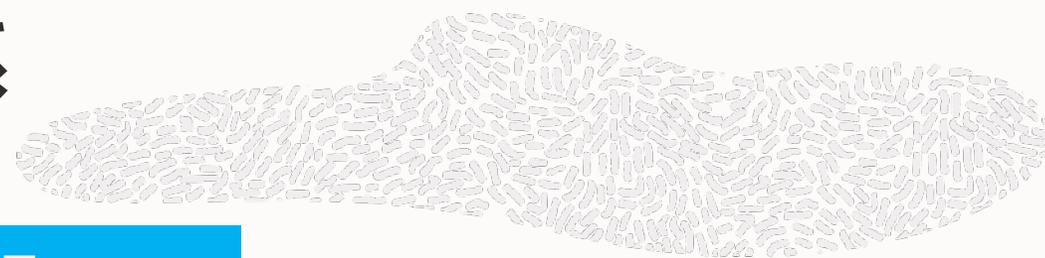
高可用性, 灾难恢复和数据保护

Oracle最大可用性架构(MAA)由一套最佳实践蓝图组成, 用于集成使用Oracle的高可用性(HA)和灾难恢复(DR)技术, 支持不同级别的高可用性。

- **MAA Home:**
 - <http://oracle.com/goto/maa>
- **On-Premise MAA:**
 - <https://www.oracle.com/database/technologies/high-availability/oracle-database-maa-best-practices.html>
- **Exadata MAA:**
 - <https://www.oracle.com/database/technologies/high-availability/exadata-maa-best-practices.html>
- **Cloud MAA:**
 - <https://www.oracle.com/database/technologies/high-availability/oracle-cloud-maa.html>



Oracle MAA与业务连续性的关系



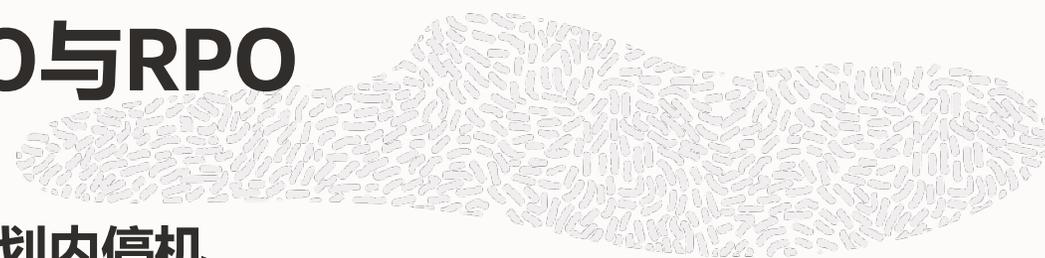
应用系统	柜面系统、核心交易、报表分析、用户认证.....
平台系统	服务器、操作系统、集群与数据库、中间件.....
数据系统	结构化数据、非结构化数据、存储系统.....
网络系统	交换机、负载均衡、防火墙、防病毒.....



- 数据库及业务数据是整个IT系统的核心, 业务正常运转离不开数据库系统的健壮运行
- 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
- 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



业务连续性的两个关键指标：RTO与RPO



RTO: 恢复时间目标

- 从某个故障中需要多长时间才能恢复
- 早上6点故障；早上8点恢复，则RTO=2小时

RPO: 恢复点目标

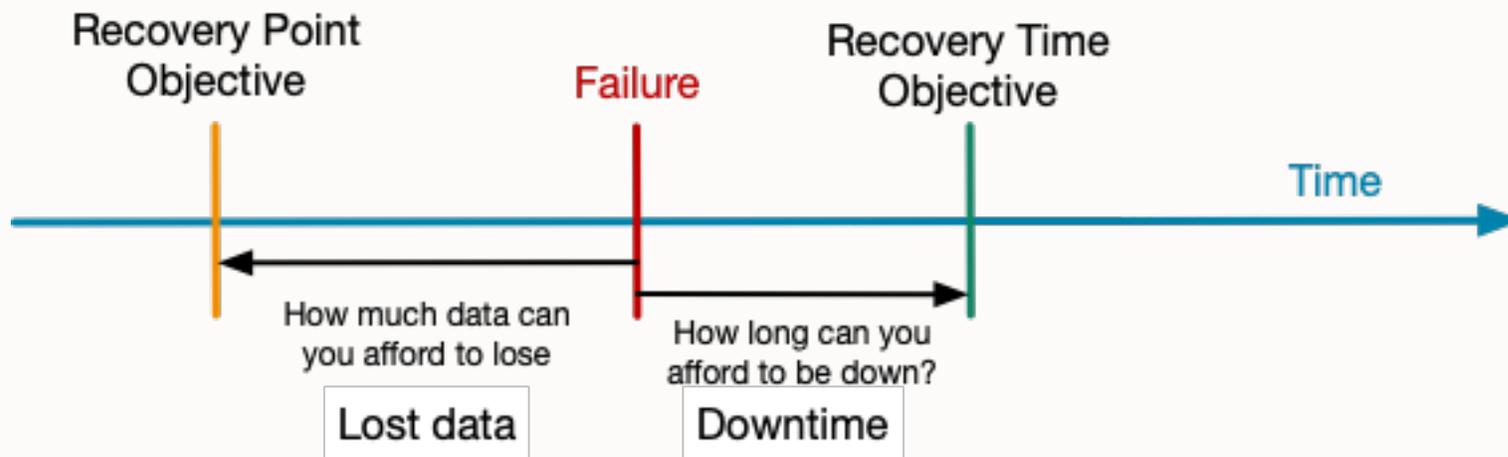
- 当某个故障发生时可能有多少数据会丢失
- 早上6点故障；早上8点恢复，但是数据最近的备份是还是昨天晚上12点做的，则RPO=6小时

计划内停机

- 软硬件计划中停机，例如变更、改造、升级、补丁、迁移、替换等

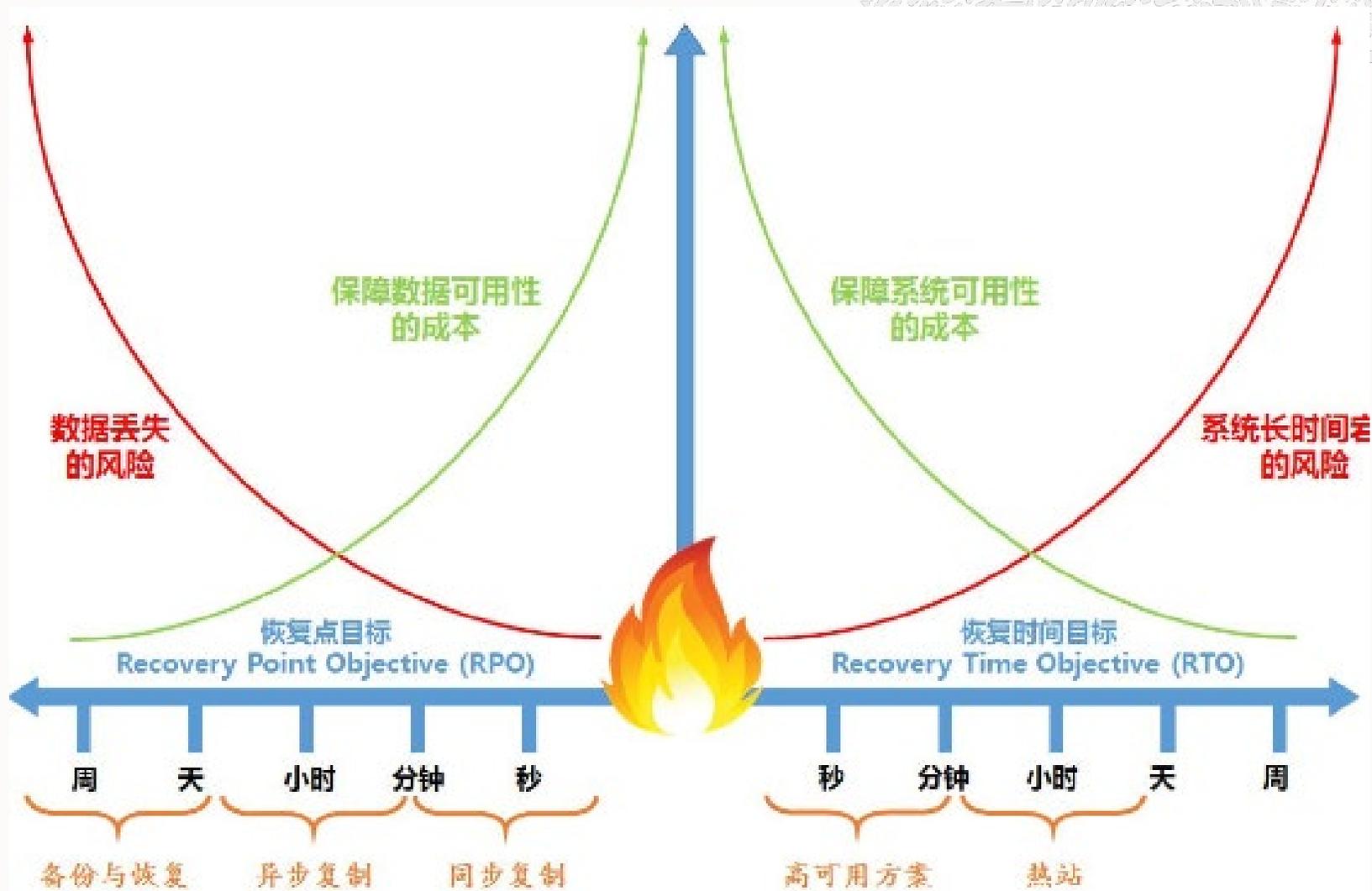
计划外停机

- 软硬件非预期的故障或停机，例如网络故障/主机故障/存储故障/病毒/bug/电源故障/自然灾害/人为错误/数据损坏等



理想状态：RTO=0；RPO=0

要求越高，成本越高



MAA 和混沌工程 (Chaos Engineering)

混沌工程是混沌一门在系统上进行实验的学科，目的是建立对系统在生产中承受动荡条件的能力的信心。

***Chaos Engineering** is the art form of experimenting (i.e. proactively breaking things) on a system in order to build confidence in a system's resilience to withstand turbulent events in production*

在当今的数字时代，包括但不限于：

- 网络、服务器和存储故障
- 人为错误
- 数据损坏
- 电源故障或站点故障
- 应用、数据库、服务器软件更新
- 数据重组或变更
- 应用程序更改和优化

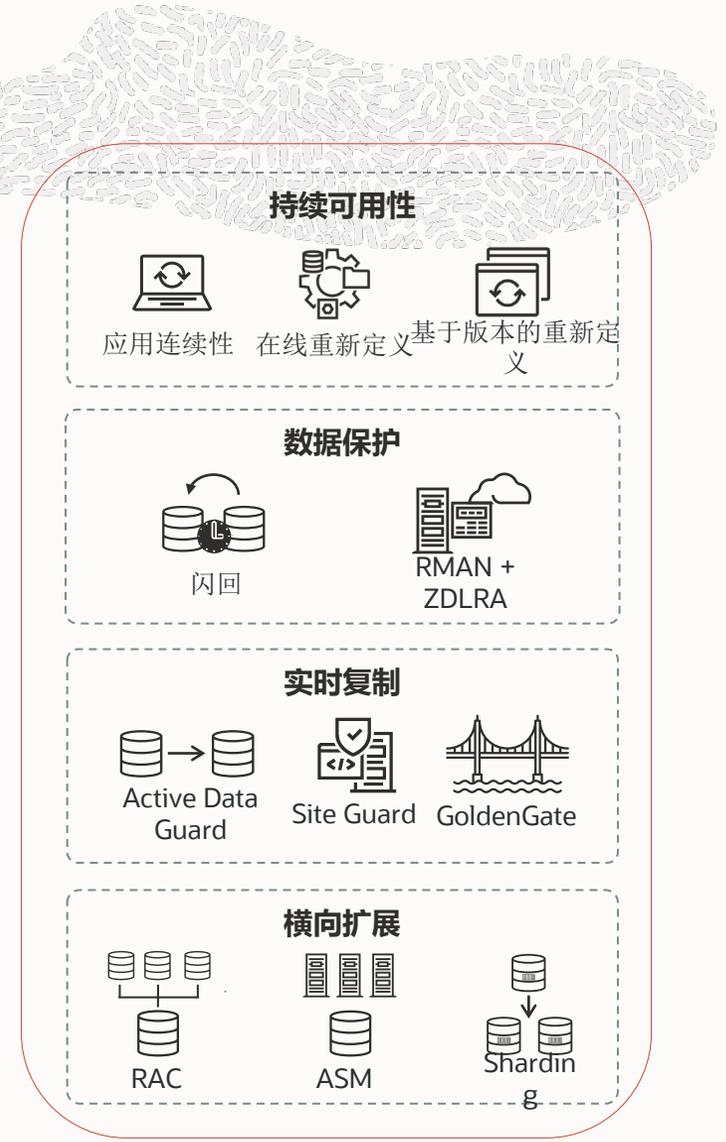
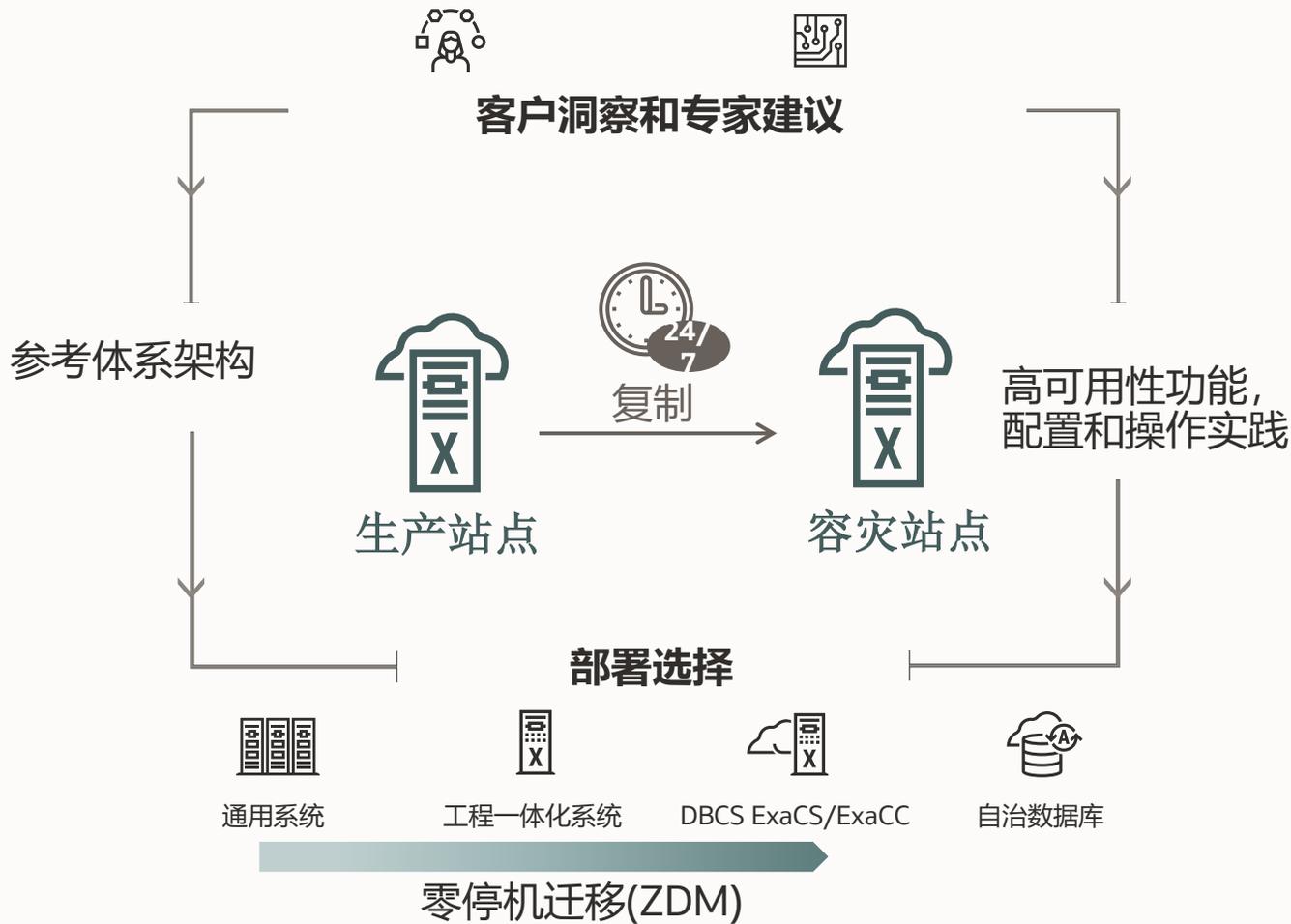


数据库高可用性有哪些影响因素？



Oracle 最大可用性架构(MAA)

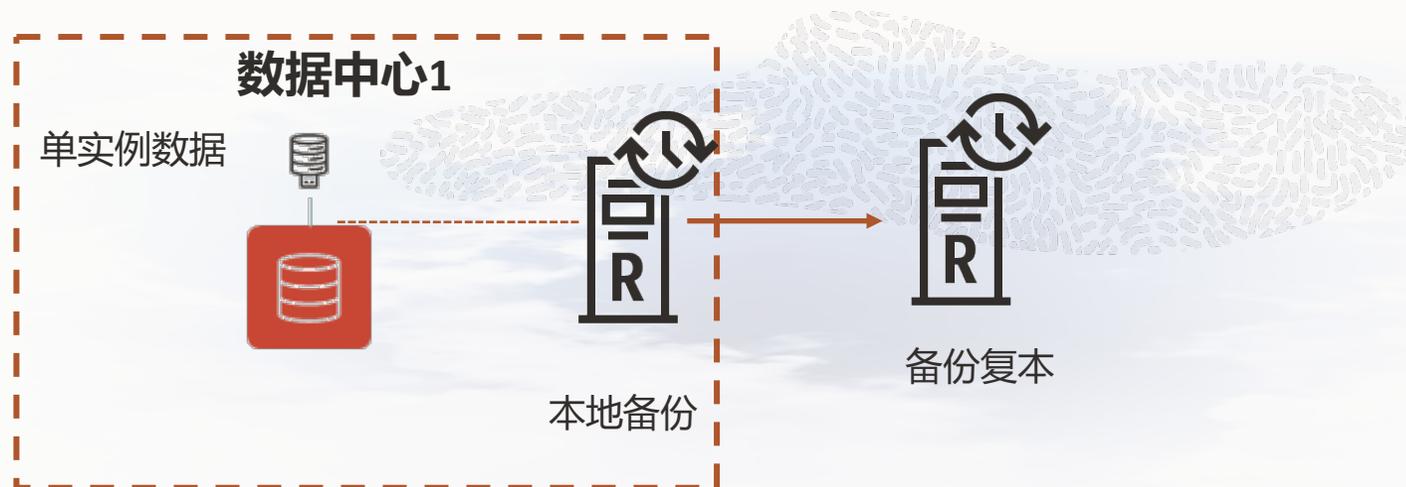
白金
黄金
白银
青铜



青铜

开发/测试/小型生产 -带备份的单实例或多租户数据库

- 单实例 (with clusterware restart)
- RMAN高级备份/恢复
 - 可选: ZDLRA, 具有永久增量和接近于零的 RPO, 自动定期校验可恢复性
- 使用 ASM 进行存储冗余和验证
- 多租户数据库
- 在线重定义
- 预防数据块损坏
- 闪回恢复



非计划停机

RTO/RPO*

可恢复故障

分钟到小时

站点故障损毁

小时到天级别 (RPO上一次备份)

计划维护

软件/硬件升级

分钟到小时级别

数据库大版本升级

分钟到小时级别

* RPO=0 除非明确指定

数据备份系统

数据备份是数据保护的最后一道防线，在本地高可用、全业务容灾系统的数据保护都失效导致数据丢失的情况下，企业还可以从数据备份系统恢复数据。

数据备份重点考虑的能力包括：



**最大程度降低
数据丢失风险：**
连续、实时的备份
减少数据丢失RPO



**缩短备份/恢复
时间窗口：**
缩短备份窗口减少生产
性能影响
快速恢复缩短RTO



**减少备份数据的空
间占用：**
提升备份空间利用率



**提供端到端可视性，
有备份校验机制**
备份的数据库数据保
护可验证



**云化可扩展的备份
架构：**
备份系统具备高科扩
展性，跨数据中心备
份部署

白银

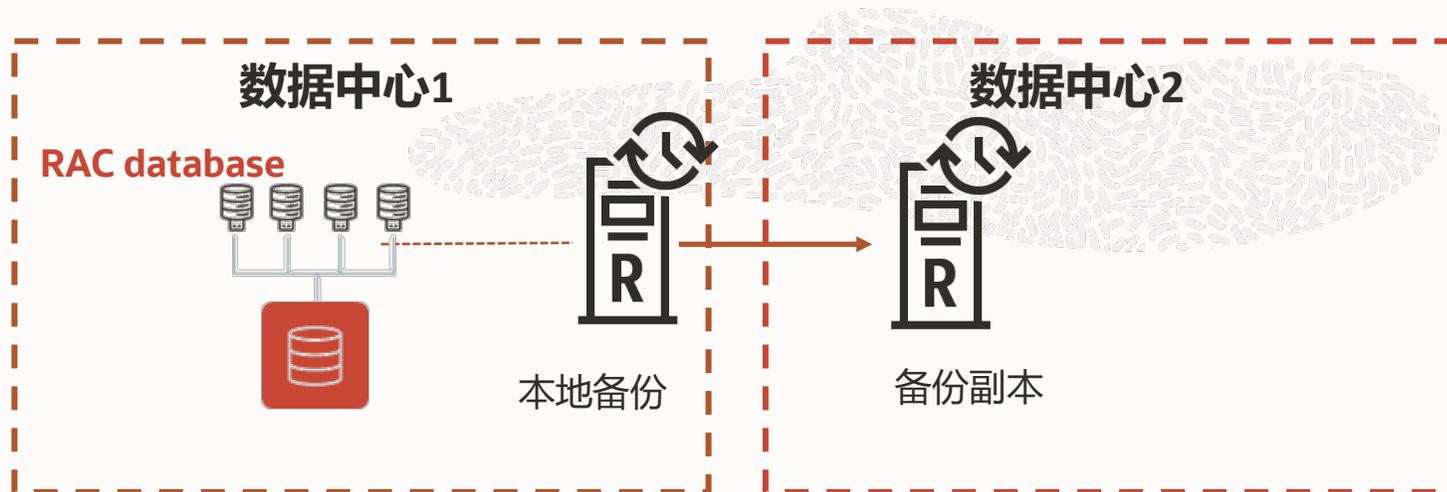
部门级/生产

青铜 +

- Real Application Clustering (RAC)
- 应用连续性 (AC/TAC)
- Sharding (可选)
 - 提供故障隔离、可扩展性和地理分布

MAA OTN

<https://www.oracle.com/a/tech/docs/application-checklist-for-continuous-availability-for-maa.pdf>



非计划停机	RTO/RPO*
可恢复故障	秒级
站点故障损毁	小时到天级别 (RPO上一次备份)
计划维护	
软件/硬件升级	0
数据库大版本升级	分钟到小时

* RPO=0 除非明确指定



透明应用连续性Transparent Application Continuity (TAC)

保护程序不受故障干扰



- 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
- 在计划外故障时重建会话状态并重播正在进行的事务计划维护可由TAC处理，以从一个或多个节点中耗尽会话
- 适应应用程序的变化：为未来提供保护

黄金级架构

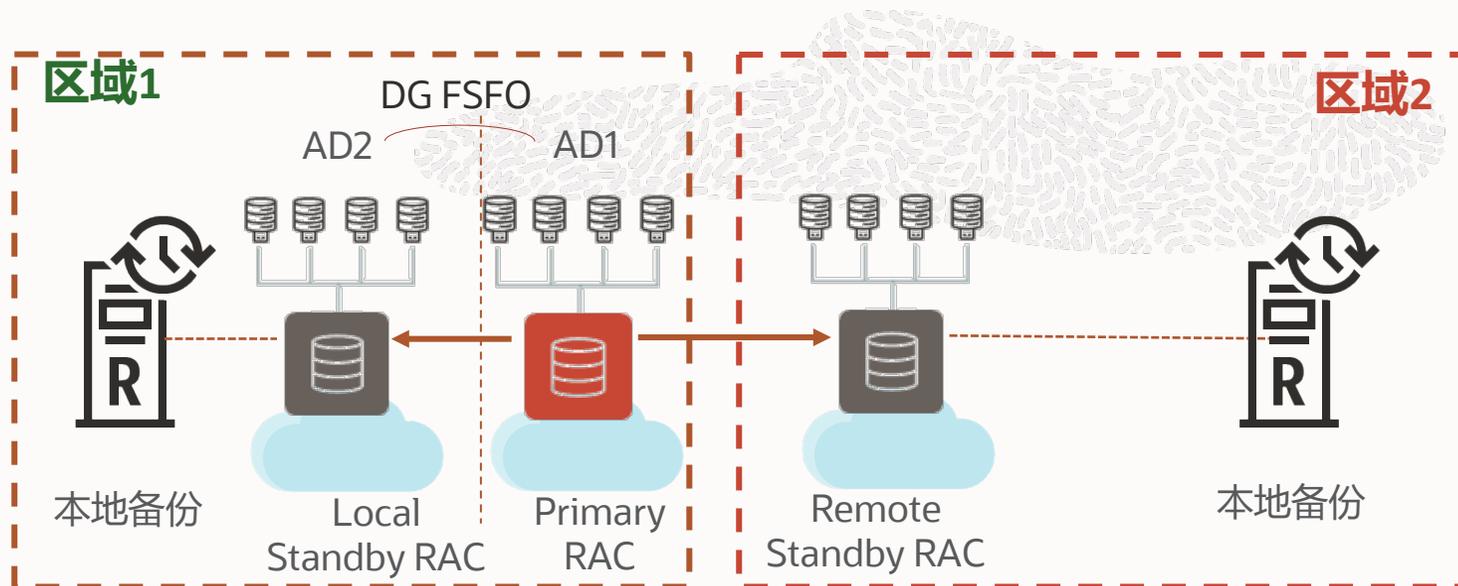
重要业务

白银 +

- Active Data Guard
 - 数据保护

MAA 架构增加:

- 至少有一个本地 & 异地备点数据库服务
- 主节点数据复制到备节点
- Active Data Guard 快速启动故障转移(FSFO)
- 双中心均有本地备份



非计划停机

RTO/RPO*

可恢复故障

秒级

站点故障损毁

秒级到2分钟, RPO为0或秒级

计划维护

软件/硬件升级

0

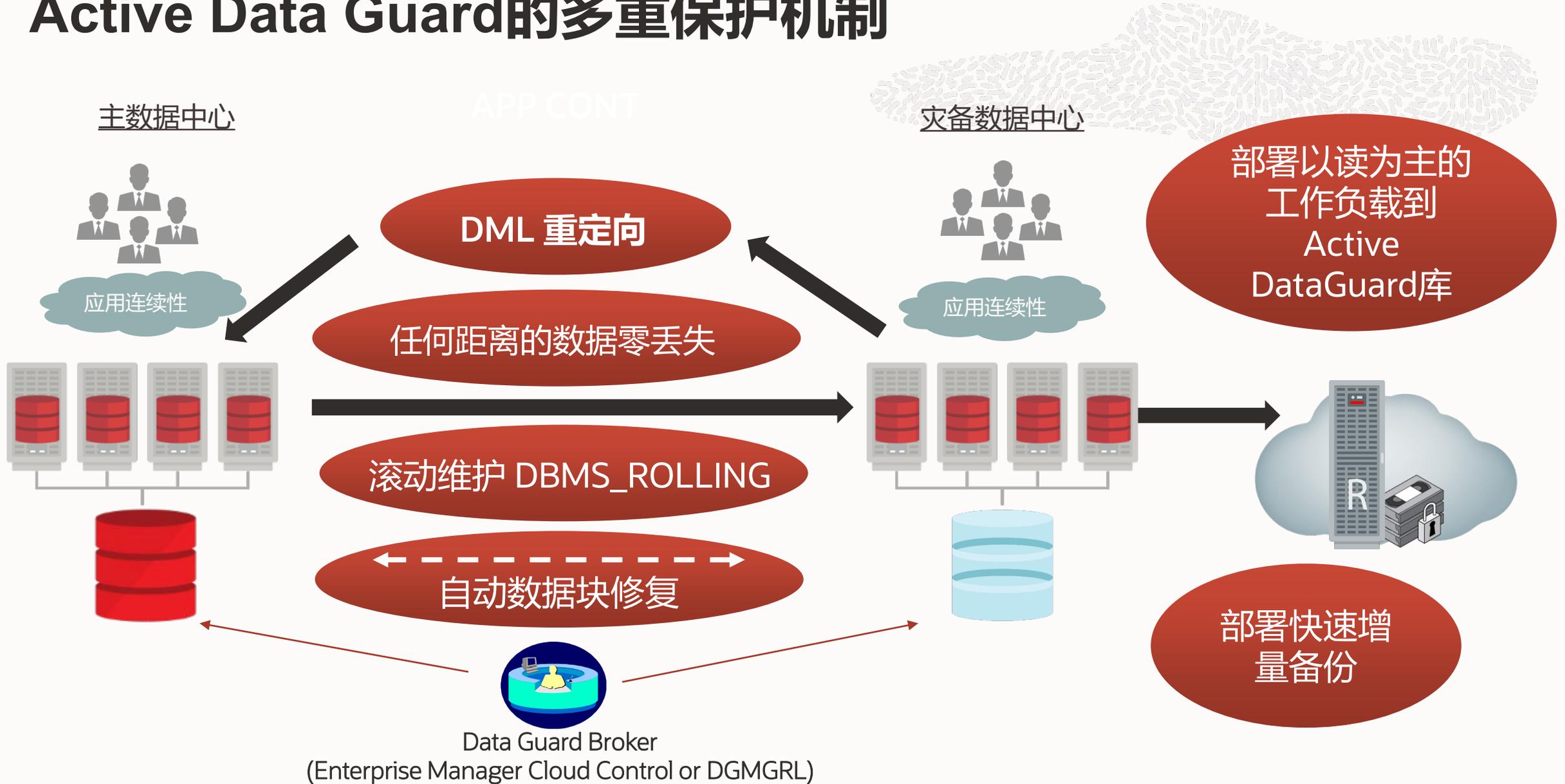
数据库大版本升级

<30秒

* RPO=0 除非明确指定



Active Data Guard的多重保护机制



白金级架构

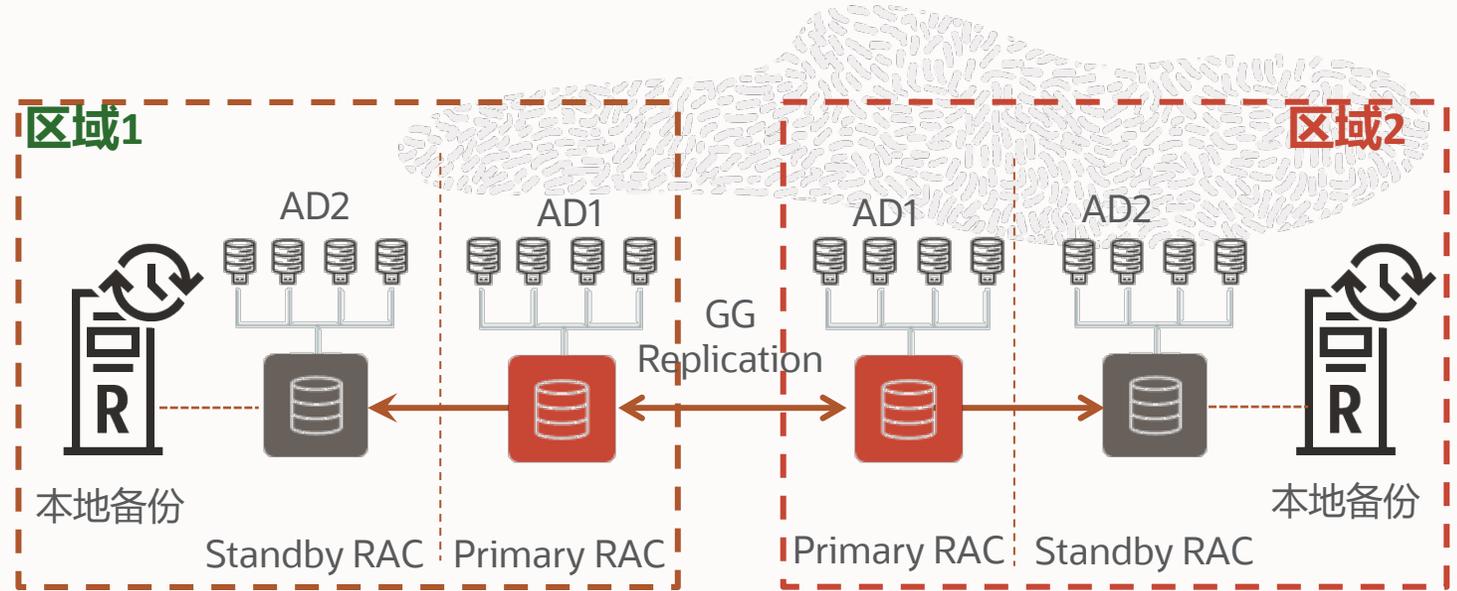
核心关键业务

黄金+

- GoldenGate Active/Active 复制
- Sharding和基于版本的重定义 (EBR) -- 可选

MAA 架构:

- 每个 GoldenGate主点都有 Exadata, RAC 和 Active Data Guard 保护
- 一个数据中心 (或 AD) 中的主节点复制到远程数据中心 (或 AD) 中的另一个主节点
- 基于 OGG 和版本重新定义实现零停机应用程序升级
- 用于可扩展性和故障隔离的分片
- 两个站点上的本地备份
- 通过自定义故障转移到 GG 副本实现零停机



非计划停机

RTO/RPO*

可恢复故障

0或几秒

站点故障损毁

0

计划维护

软件/硬件升级

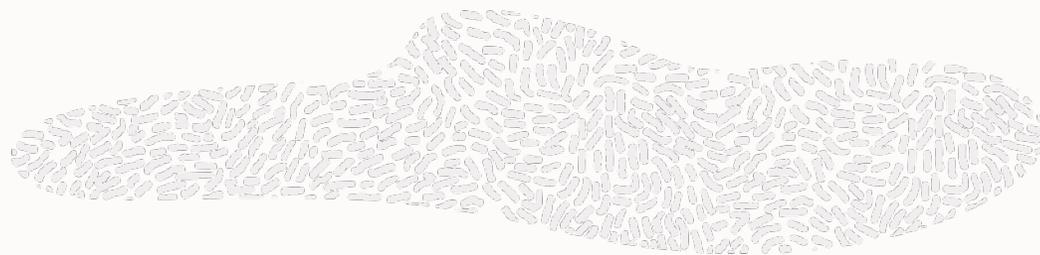
0

数据库大版本升级

0

MAA 参考体系架构

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

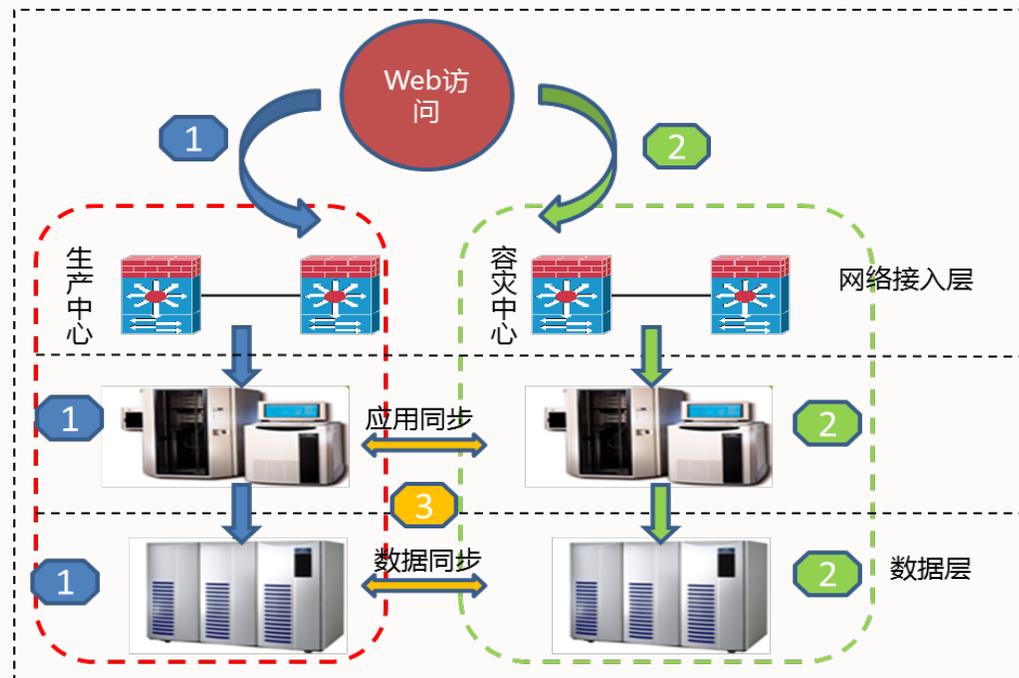
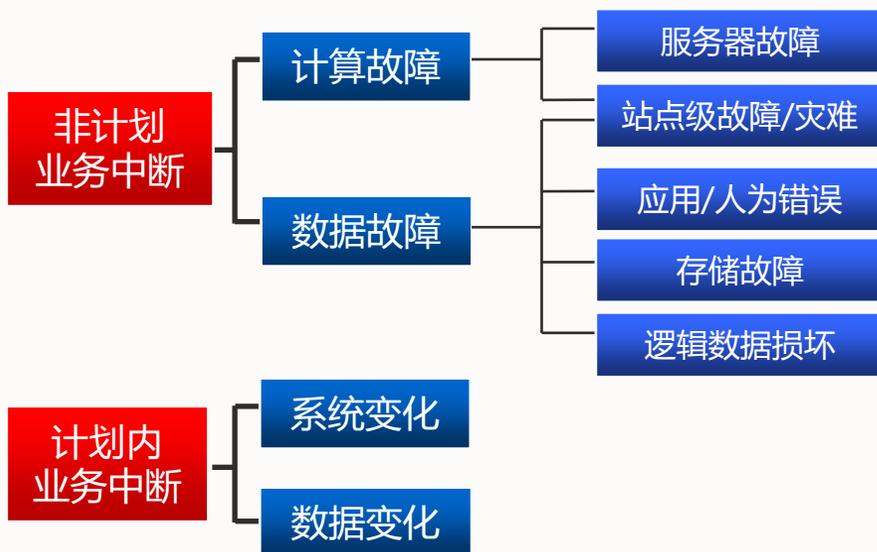


所有层都可在于私有云和公有云中实现

业务连续性能力的主要关注点

业务连续性：IT系统应对灾难和故障等风险，可以自动调整和快速反应，保障用户在使用过程中的连续性体验，以及在系统内部维护及产品上线时的保障业务不间断运转的能力。

业务中断风险



全面应
对各类
风险

快速切
换无感
知

业务数
据无损
失

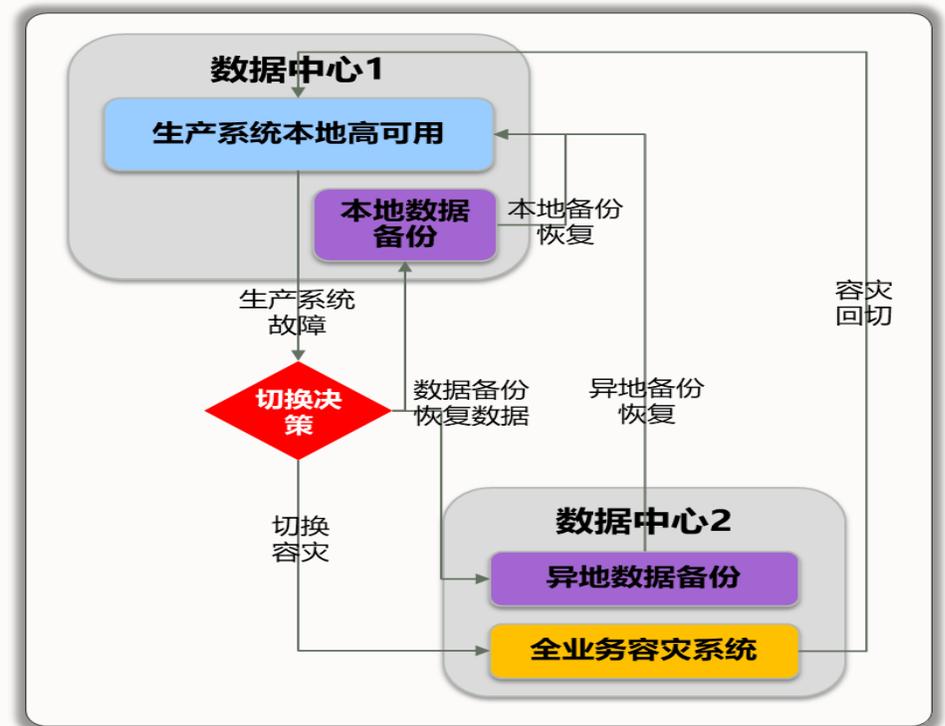
完善的业务连续性保障体系范例

“**多位一体**”的业务连续性保障体系架构，在**数据中心基础架构**之上，包含：**生产系统本地高可用**、**容灾系统**，以及**数据备份系统**组成，相互配合共同保证整体的业务连续性：

- **生产系统本地高可用性**是业务连续性保障的**基础**
- **容灾系统**是建立在异地容灾中心的一套整体生产系统恢复体系，重大灾难故障时，通过启动容灾系统可以**全面接管生产系统**
- **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）备份到磁带等备份设备上，在生产数据发生意外时进行恢复，是**数据的最后保障**。

良好的**运营实践**，充分发挥业务连续性保障架构的能力。

- **故障处理流程固化**
- **故障切换自动化**
- **故障切换演练**
- **对变更充分地测试验证**

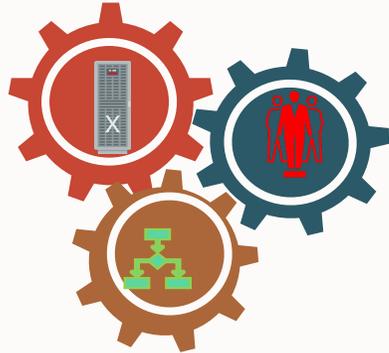


Oracle 业务连续性健康风险评估

- MAA架构健康风险评估，全面评估业务连续性保障体系，发现短板，展现企业业务连续性健康状况，提出业务连续优化的方向

- 全面的企业级MAA架构健康风险评估包括以下维度：

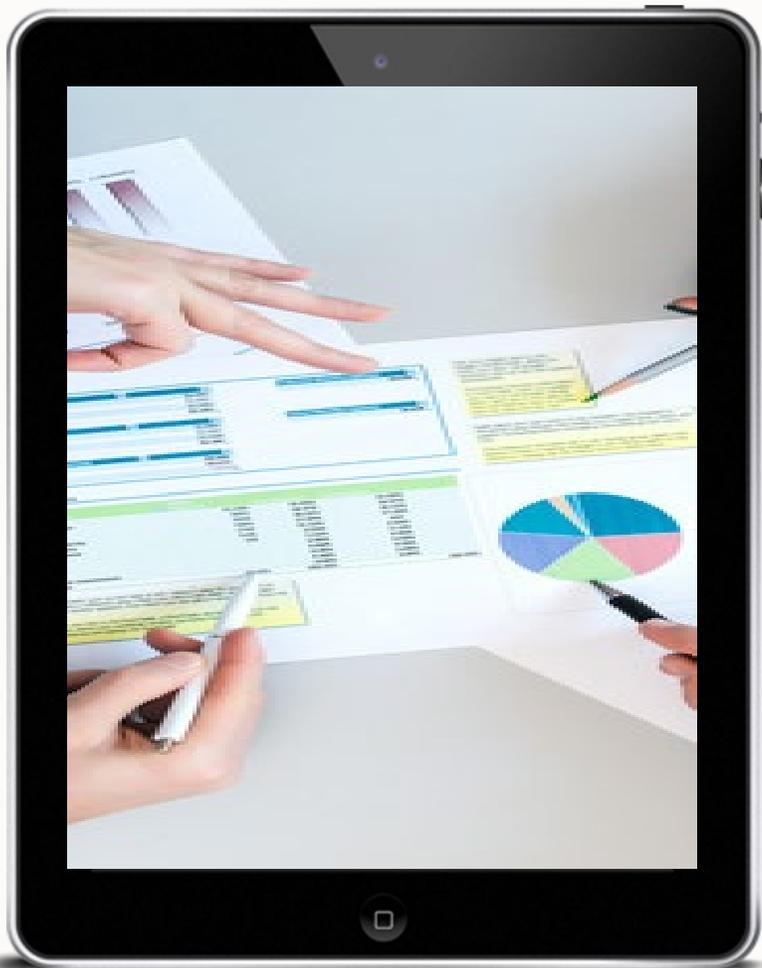
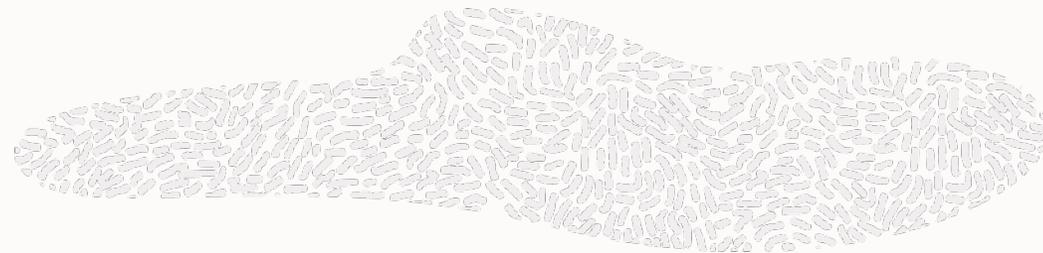
- ① 数据备份
- ② 本地高可用
- ③ 数据容灾
- ④ 应用容灾
- ⑤ 容灾切换
- ⑥ 网络配置
- ⑦ 补丁策略
- ⑧ 日常维护



Category	Item	Description	Value
客户基础信息	Customer Name	客户名称	XX Customs
	Expected RTO(Mins)	该客户期望达到的RTO	<30 分钟
	Expected RPO(Mins)	该客户期望达到的RPO	
	DataCenter Location	该客户部署的数据中心： 单中心/同城双中心/两地三中心	两地三中心，深圳/上海
	DR Mode	备	灾难应
	Database DR Capacity	例	生产：本地容灾，异地容灾=1:1
所评估的应用基础信息	DataCenter Distance	同城/异地数据中心距离	同城30公里，异地1000公里
	DataCenter Network Latency	同城/异地数据中心间网络延迟	同城3毫秒，异地10毫秒
	Business system	业务系统名称	信用卡系统
	App Vendor	应用开发商	自研
	App priority	系统等级（核心/重要/一般）	核心
	Apps Deployment Model	该应用部署模式：本地高可用+同城双中心	
	Database Server Hardware & Model	数据库服务器型号	IBM Power 980
	OS version	操作系统及版本	AIX 7.2
	Storage Model	存储型号	EMC XC
	Exadata Model	Exadata 型号	
备份方式	Exadata Image	XD Image 版本	
	GI Version	GI 版本	
	DB version	DB 版本	19.11
	DB Redo log	每天产生的日志量	
	Data Volume	数据库大小	20TB
	Yearly Data increase rate	数据库年增量	30%
	Archive Mode	是否归档模式	Yes
	Backup Strategy	备份策略	每天增量，每20分钟备份一次日志
	Backup Technology	备份技术/厂家	NBU
	Backup Lifecycle	备份保存策略（本地/异地）	本地+异地
本地高可用	Verify tools for Backup Validation	有效备份验证方法	ASA
	Dedicated Backup Network	备份是否采用独立网络	Yes
	ZDRBA	是否使用ZDRBA	No
	Cluster Deployment	是否使用RAC	Yes
	Local Current RTO	该应用本地当前RTO	60
	Local Current RPO	该应用本地当前RPO	20分钟
	RAC Deployment Model	RAC的节点数量	
	RAC Deployment Model	RAC提供服务或 HA 方式	HA 方式
	RAC Compute Node Capacity	RAC单节点能否承担整个集群的业务压力	Yes
	Private Network for RAC	RAC节点间互联是否专用冗余网络及交换机	虚拟网络
容灾与切换	CD/PDB	是否为多租户，如果是部署了多少PDB	是，1 CDB /1 PDB
	DB Storage Mode	数据库存储方式（ASM or ?）	ASM
	ASM Redundancy	ASM 冗余模式	3 倍冗余
	Local ADG in same DC	有无本地ADG数据库应急部署	Yes
	Local ADG with Apps Deployment	本地ADG有无应用部署	No
	Local ADG Hardware	本地ADG的硬件配置	IBM Power980 分区
	Local ADG Capacity	本地ADG的计算能力与生产系统能力比例	1:1
	ADG Sync/Async	本地 ADG 保护模式部署	Sync
	Application Continuity	是否使用AC/TAC	Yes
	Error Block detection & Repair	数据环状检测和修复	Enable
容灾与切换	Flashback Enabled	是否启用闪回（主/备）	Yes
	DR Mode - Same City/Remote	同城容灾/异地容灾	同城+异地
	Application Deployment	应用是否部署在每个容灾中心	Yes
	Same City/Remote Current RTO	该应用同城/异地当前RTO	同城RTO 30分钟，异地RTO 60分钟
	Same City/Remote Current RPO	该应用同城/异地当前RPO	同城RPO 5分钟，异地RPO 5分钟
	DR Workload Capacity	灾备能力比例	生产：同城容灾：异地容灾=1:1:0
	DR support Ops Capacity	容灾中心是否有生产同等运维能力	Yes
	DR Mode - ADG	容灾手段：ADG容灾？	ADG
	Switchover/Failover practise	是否有切换演练	Yes
	Switchover Time	切换演练周期与时长	每年一次切换演练，每次一天左右
Time to Database Switchover	数据库ADG切换耗时	切换1分钟，异地数据库切换3分钟	
Total Time to DR(DB+APP)	应用切换总耗时(DB+APP)	异地切换60分钟	
日常维护	Workload Switchover	是否主备切换后，灾备端承担一段时间的业 务运行？运行时间？	Yes, 3 Day
	ADG Sync/Async	同城/异地 ADG 保护模式部署	同城ASync, 异地ASyn
	ADG FarSync	是否启用FarSync	No
	ADG DML ReDirection	是否启用ADG DML重定向	No
	DG Management	DG管理方法（DGBroker/脚本切换？）	DGBroker
	Application Development	应用开发语言与应用开发框架	Java, SpringCloud



数据库本地高可用架构



数据库是否运行集群系统

是否至少2台机器同时读写，
是否能够快速切换

是否具备本地数据库容灾系统

数据坏块检测和修复

应用是否有高可用配置

应用是否有集群配置，会话
是否能透明切换

数据库能否快速从误操作中恢复

是否有闪回

容灾架构

数据库容灾部署

- 数据库是否具有容灾部署
- 数据灾备系统技术选型
- 数据库是否能保证数据零丢失
- 企业是否部署多中心灾备系统架构

应用容灾部署

- 企业是否具备本地应用容灾系统
- 企业是否具备异地应用容灾系统
- 应用是否支持实时应用故障切换

容灾切换

- 企业是否制定容灾切换流程
- 企业是否定期进行容灾演练
- 灾备切换方式

数据备份和补丁策略

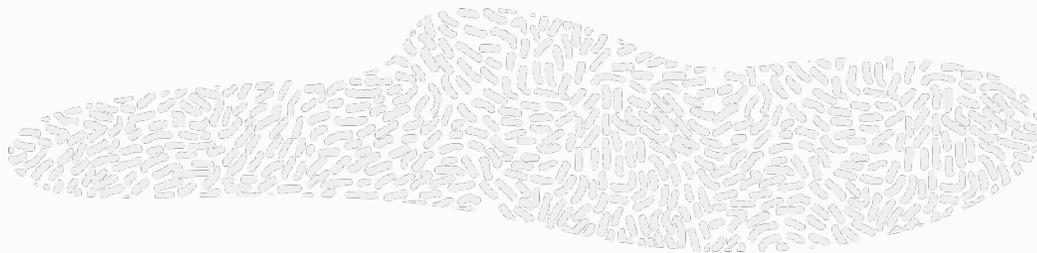
数据备份

- 企业是否有备份校验机制
- 数据库备份恢复时长需求
- 数据备份方式评估

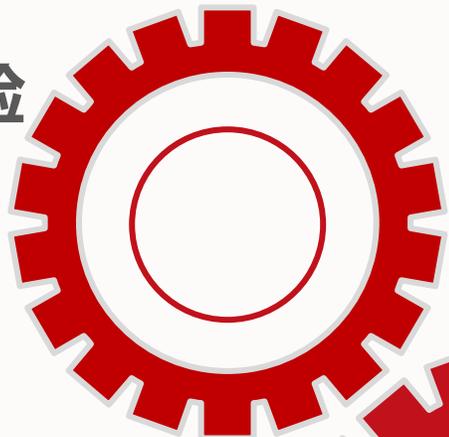
补丁策略

- 是否有测试环境
- 企业的安全补丁策略
- 企业的数据库补丁策略
- 数据库补丁上线前是否有充分测试和冲突分析
- 数据库补丁是否支持在线升级和回退

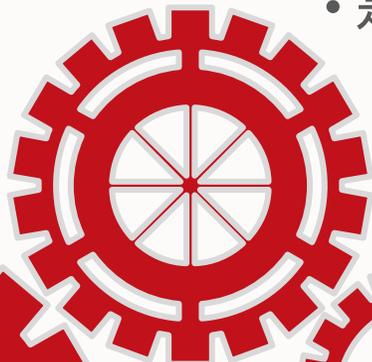
日常运维



是否进行健康巡检



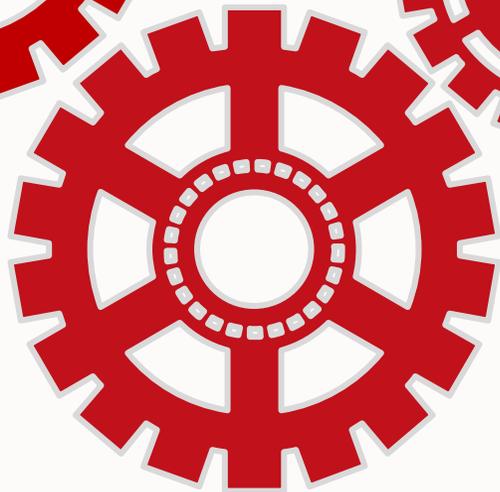
是否进行日常维护



- 否有稳定的数据库日常维护团
- 是否有完善的日常维护手册



是否具备紧急处理流程



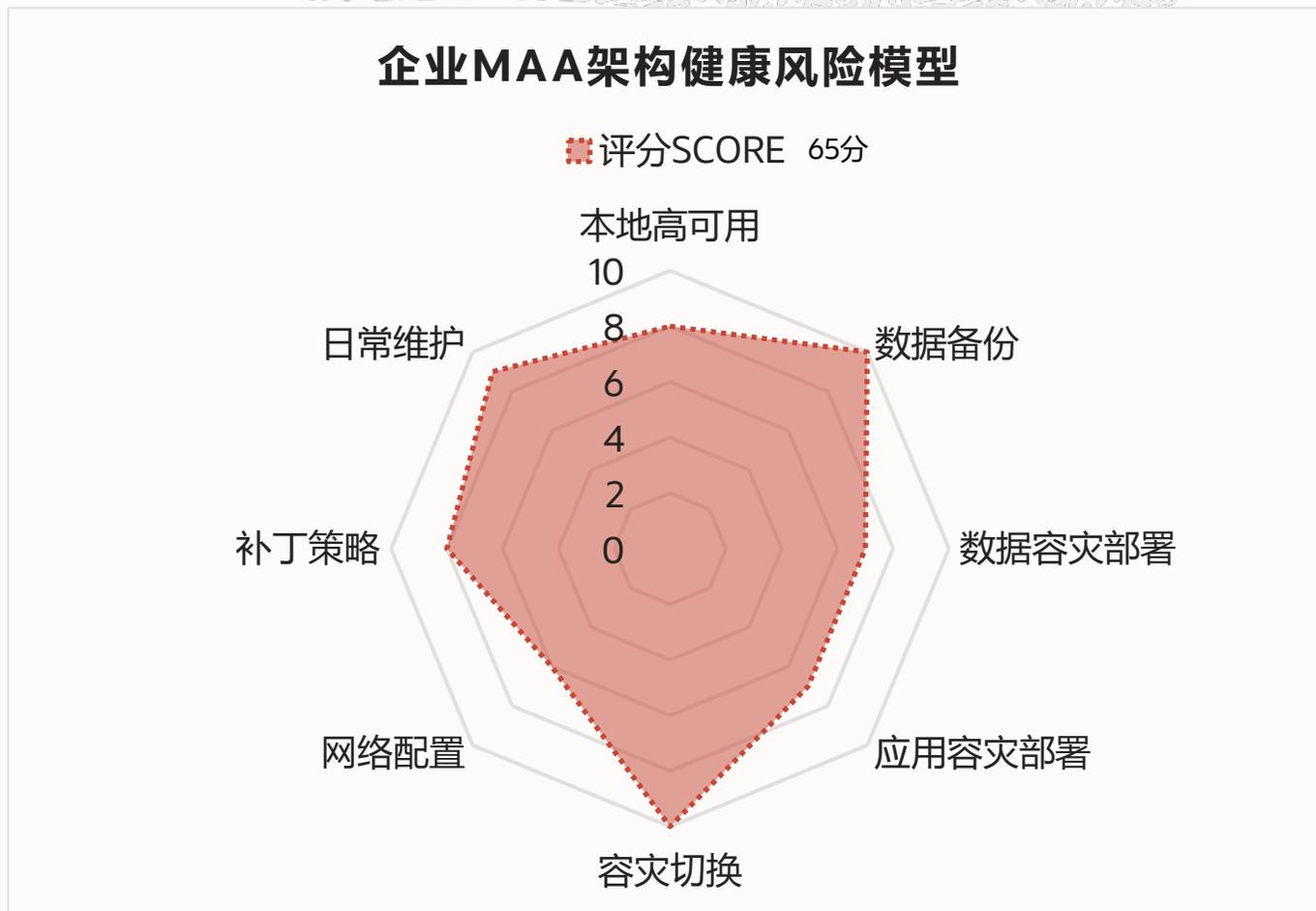
是否具备日常监控告警处理

- 是否监控硬件、系统、网络、数据库和存储
- 是否处理日常监控告警

业务连续性8大维度评分雷达图 (示例65分/满分80分)

Items	评分SCORE
本地高可用	8
数据备份	10
数据容灾部署	7
应用容灾部署	7
容灾切换	10
网络配置	6
补丁策略	8
日常维护	9

应用容灾部署	企业是否具备本地应用容灾系统	评估应用是否部署本地应用容灾系统	2	7
		评估应用是否正常演练切换至本地应用容灾系统	1	
		评估本地容灾中心是否具备与生产端同等配置	1	
	企业是否具备异地应用容灾系统	评估应用是否部署异地应用容灾系统	1	
		评估应用是否正常演练切换至异地应用容灾系统	1	
		评估异地容灾中心是否具备与生产端同等配置	0	
	应用是否支持实时应用故障切换	评估应用故障切换时长	1	
评估应用系统是否部署TAC配置		0		





ORACLE
甲骨文

>>>>>>>> Oracle 

免费业务连续性评估

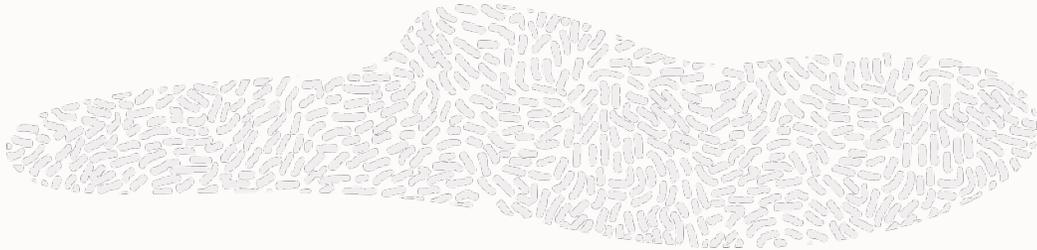
如何满足 RTO / RPO 严苛要求?

快来给你的系统做个 CT 吧!



· 即刻扫码报名免费评估 ·

*活动最终解释权归甲骨文公司所有



即刻扫码报名免费评估

您将体验到

- 八大维度高可用性架构评估
- 专业的数据库团队服务
- 高质量业务连续性改进建议

