

ORACLE

数据备份与零数据丢失方案探讨

钟水林

资深首席解决方案工程师，甲骨文中国

6/17/2022



议程

- 1 客户MAA评估中数据备份常见问题
- 2 零数据丢失恢复解决方案探讨

Oracle推荐的8大维度业务连续性健康风险评估

- Oracle 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8个维度：

① 数据备份

- 是否归档模式
- 备份策略
- 日常备份完成情况
- 恢复演练环境及实施情况
- 备份技术/厂家
- 备份保存策略（本地/异地）
- 有效备份校验方法
- 备份是否采用独立网络
- 是否采用零数据丢失备份恢复技术

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

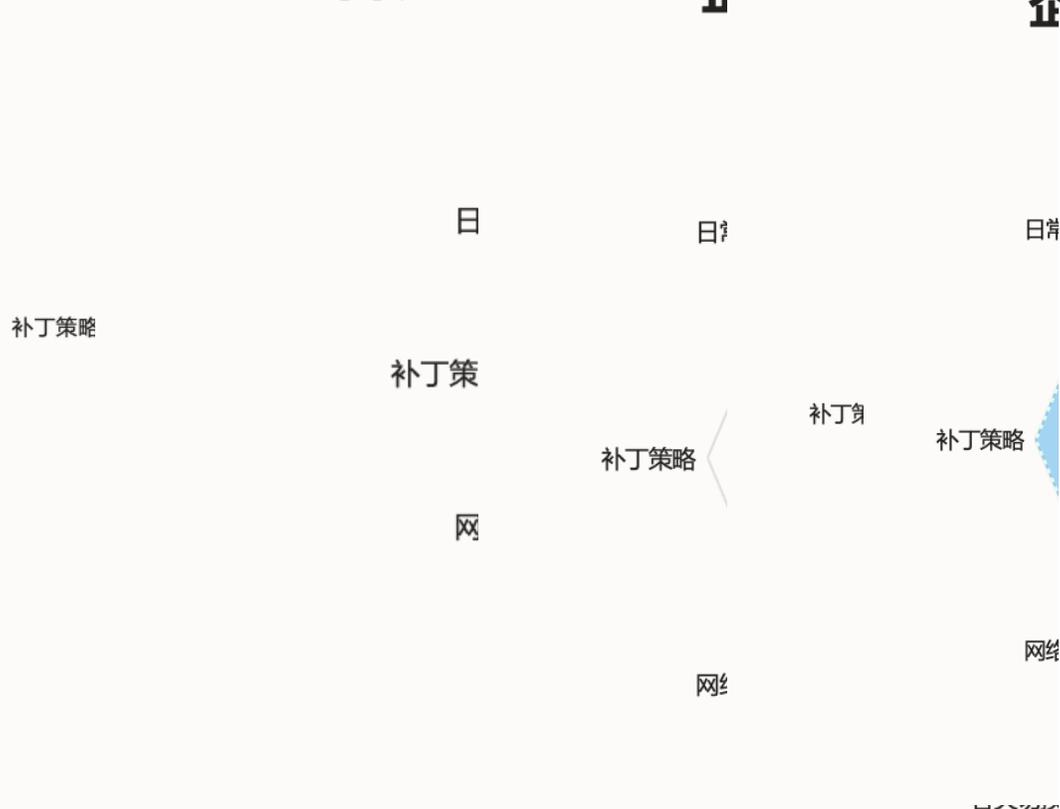
⑦ 补丁策略

⑧ 日常维护

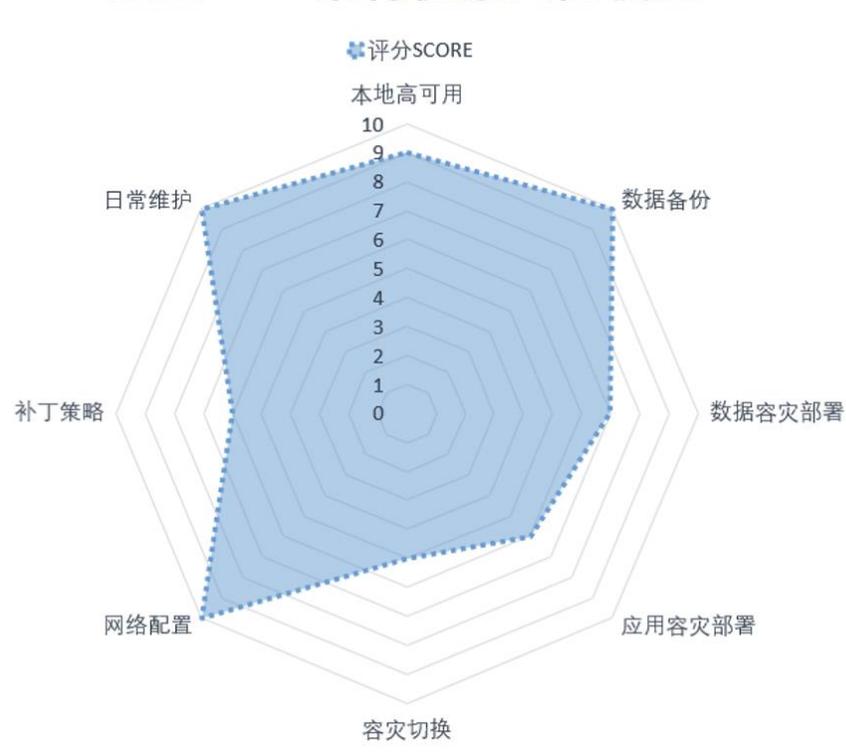
部分实际客户MAA架构健康风险评估结果

企业级客户对核心业务数据库基本配置了数据备份，但改进的空间很大

某客户MAA架构健康风险模型
客户MAA架构健康风险模型



企业MAA架构健康风险模型

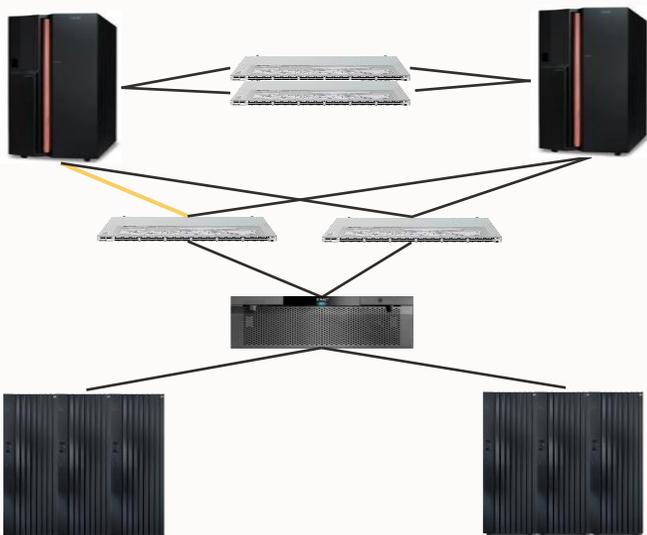


某行业客户MAA评估数据备份的情况

单数据中心，单库数据量巨大，仅传统备份

指标期望与现状

- ① 期望RTO=60分钟，RPO=0
- ② 实际RTO=可能>2天，RPO=可能24小时



核心业务数据库：2节点RAC，67TB
服务器：IBM p870 * 2台
存储：EMC VMAX 100K*2台

评估项	调研结果
备份策略	7天一周期，周末全备，晚8点增量及归档日志备份
日常备份完成情况	其中一业务库目前约67TB，每周六全量备份，时长约26小时；每周一至周五晚8点增量及归档日志备份时长约16-18小时。
恢复演练环境及实施	一年一次，仅一个全量restore需14小时以上
备份技术	传统RMAN备份，NBU，备份一体机
备份保存策略	本地保存，保留2个恢复窗口期，无异地转存保存
有效备份校验方法	依赖备份设备，备份完成后无校验
是否采用实时备份技术	否

企业MAA架构健康风险模型



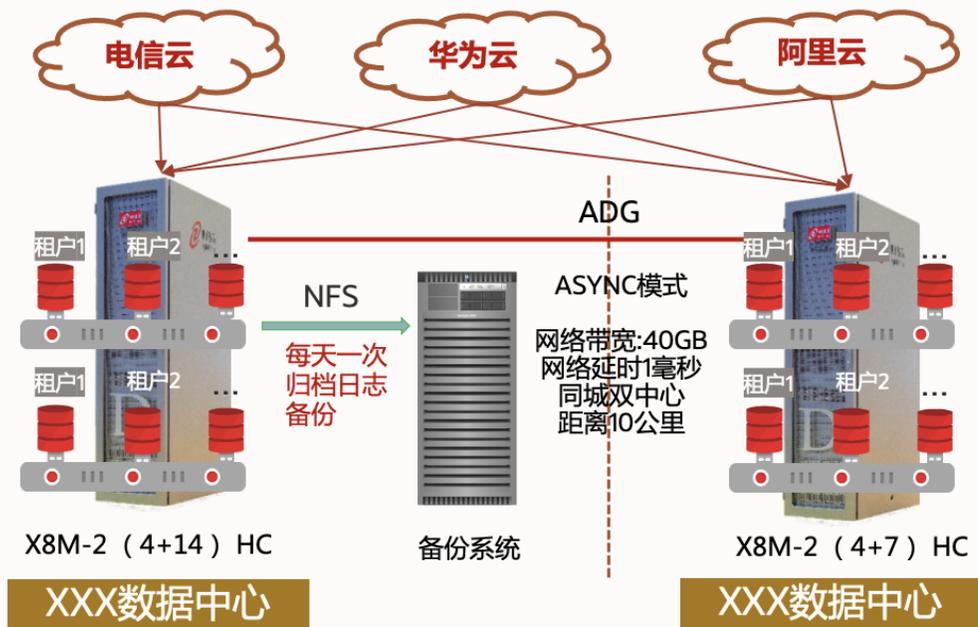
某DBaaS客户MAA评估数据备份的情况

同城双中心，单CDB数据量巨大，备份压力大

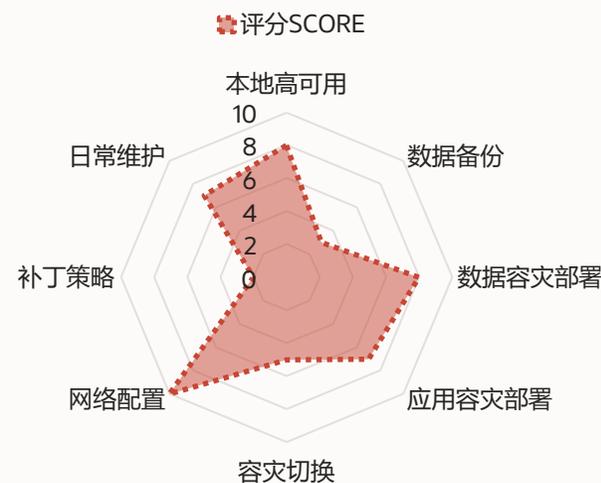
指标期望与现状

- ① 期望RTO=120分钟，RPO=0
- ② 站点切换RTO=60分钟，RPO=0
- ③ 数据恢复RTO可能>24小时，RPO可能>24小时

评估项	调研结果
备份策略	每隔15天全备，每天增量及归档备份
日常备份完成情况	根据服务目录不同，多CDB供应数据库服务，CDB大小15-40TB，每个CDB每半个月全量备份，时长13~31小时不等，备份失败时有发生，增量备份数小时内。
恢复演练环境及实施	缺乏演练
备份技术	传统RMAN备份，备份至NAS存储
备份保存策略	本地保存，保留1个恢复窗口期，无异地转存保存
有效备份校验方法	无
是否采用实时备份技术	否



企业MAA架构健康风险模型

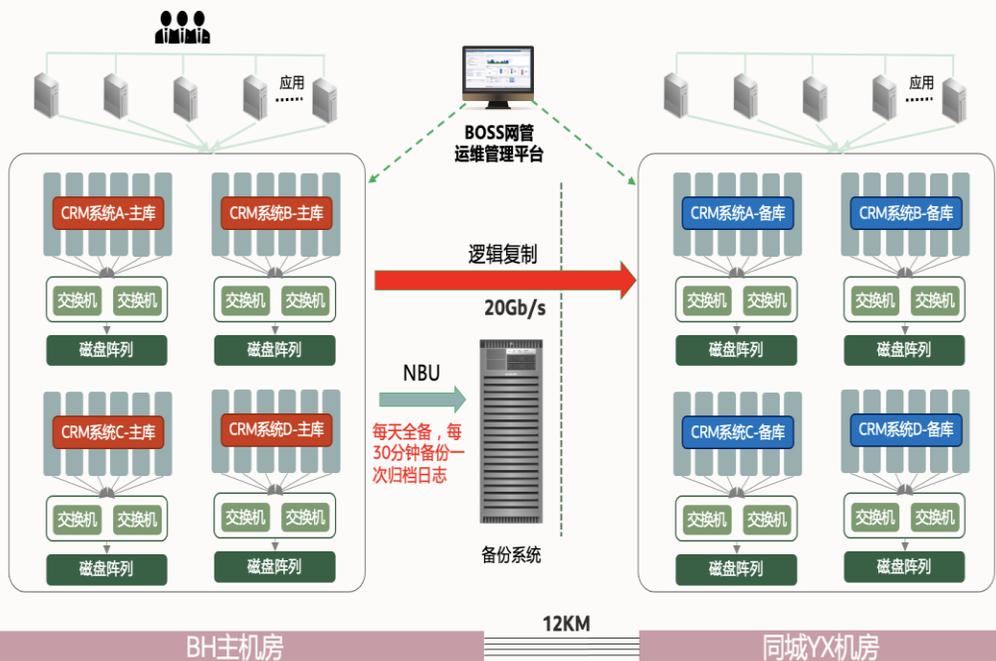


某通信行业客户MAA评估数据备份的情况

每天全备，缺乏实时备份能力

指标期望与现状

- ① 期望RTO=30分钟，RPO=0
- ② 站点切换RTO=10分钟，RPO=5
- ③ 数据恢复RTO>5小时，RPO最大30分钟

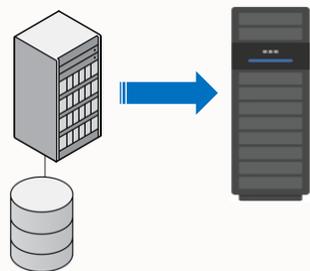


评估项	调研结果
备份策略	每天全备，每30分钟备份归档日志
日常备份完成情况	4个核心业务数据库，每个大小8-12TB，每个备份时长5-6小时。
恢复演练环境及实施	一季度一次，恢复时间5-6小时
备份技术	传统RMAN备份，备份至本地文件系统
备份保存策略	本地保存、异地转存，保留2周恢复窗口期
有效备份校验方法	无
是否采用实时备份技术	否

企业MAA架构健康风险模型



小结：MAA评估发现客户数据备份普遍存在的问题



传统备份方式为主
定期全量+增量+归档



缺乏端到端的可视性和可靠性验证，不能保证数据库级可恢复性



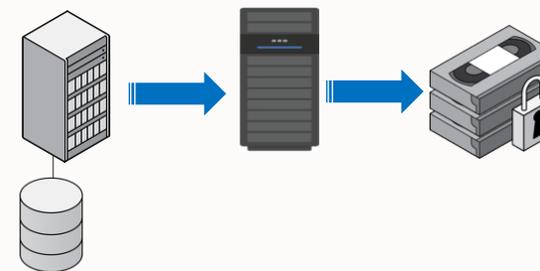
非实时备份技术，只能恢复上次备份以前的数据，数据丢失风险高，RPO通常小时级



业务库数据量越来越大，备份空间紧张且扩展能力有限，备份保留窗口期有限，通常1-2周



备份时间窗口长、IO和网络压力大，甚至备份失败，影响 SLA



较多的客户只有本地备份，无备份卸载、异地介质保存



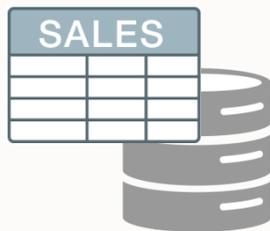
我们真正需要的备份与恢复解决方案

备份对生产系统基本无影响，所有完成的事务都可恢复，保留窗口期内可恢复到任意时间点



影响最小的备份技术

- 日常备份可以快速、分钟级完成，对应用程序没有任何影响，无备份窗口问题
- 备份只消耗最少的资源和存储，只传送变化数据，所有备份处理和磁带复制压力被卸载，无需消耗数据库端CPU和IO资源



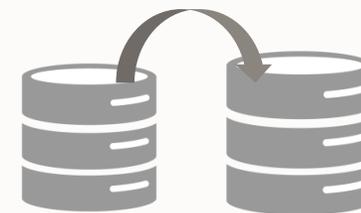
完整，可靠，快速恢复

- 所有完成的事务都是可恢复的(零数据丢失, RPO≤1秒)
- 基于时间点恢复可用(用户错误, 勒索软件...), 保留窗口期内恢复到任意时间点
- 实时验证和监控可恢复性状态



弹性架构

- 数据库-集成的硬件和软件
- 使用线性大规模可扩展服务轻松保护数据中心所有数据库
- 灵活的高可用架构，可级联，可归档备份到磁带或云上



低停机数据库克隆和迁移

- 使用生产库备份快速克隆测试/开发数据库环境
- 使用生产备份创建ADG Standby数据库
- 只需几个步骤轻松完成跨平台数据库迁移



真实的客户事件

误操作删除数据，最终不完全恢复，有数据丢失

IBM Power 服务器集群



多个核心业务数据库，单库数据量10TB以上

RMAN

传统备份



磁带库

存在的问题：

- 承载多个生产库备份、数据量大，某核心库全备份一次需要14小时以上，影响业务
- 定期备份数据T+1，日常备份无校验
- 无冗余备份
- 开发人员误操作，truncate了多张核心表数据，从磁带库恢复耗时20+小时，不完全恢复，有数据丢失，造成跨数据库的一致性问题。



客户对数据库备份进行升级改造

由传统备份升级到零数据丢失备份与恢复



IBM Power 服务器集群



多个核心业务数据库，单库数据量10TB以上

实时备份



零数据丢失恢复技术

备份转存异地



引入零数丢失备份恢复技术，并转存备份数据到原有的带库上，异地保存



ZDLRA帮助客户消除数据丢失的风险

RPO < 1秒、全备性能提升 > 5倍、增量备份 < 30分钟、恢复性能提升 > 3倍、数据去重比为 150:1

被保护的
核心
库

数据保护87天，备份42TB的数据库，只需要不到21TB空间

RPO < 1秒

已开启实时保护

The screenshot displays the Oracle Enterprise Manager Cloud Control 13c interface. The top section shows the 'Recovery Appliance' configuration for 'scswzdlra'. Below this, a table lists '受保护数据库 (7)'. The table columns include '数据库', '目标类型', '版本', '保护策略', '数据库大小 (GB)', '恢复窗口', '所需空间 (GB)', '未受保护数据窗口', '阈值', '当前', '错误和警告', and '重做传输'. A red dashed box highlights the '数据库' column, with a red arrow pointing to the text '被保护的 核心 库'. Another red dashed box highlights the '所需空间 (GB)' column, with a red arrow pointing to the text '数据保护87天，备份42TB的数据库，只需要不到21TB空间'. A third red dashed box highlights the '恢复窗口' column, with a red arrow pointing to the text 'RPO < 1秒'. A fourth red dashed box highlights the '重做传输' column, with a red arrow pointing to the text '已开启实时保护'. The bottom section shows a '备份报告' (Backup Report) for '集群数据库'. The report table has columns for '状态', '命令', '类型', '目标', '开始时间', '所用时间', '输入大小 (GB)', '输出大小 (GB)', and '输出速率 (MB/秒)'. The second row of the report shows a backup of 'DAILY_0613220' with a status of '成功' (Success), a command of 'DB INCR', and a type of 'Recovery Appliance'. The '输出大小 (GB)' column for this row is highlighted with a red dashed box, showing a value of 115.1538 GB.

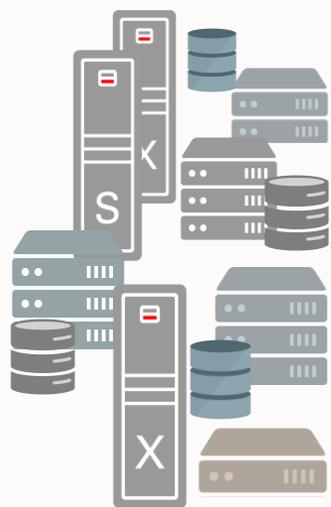
数据库	目标类型	版本	保护策略	数据库大小 (GB)	恢复窗口	所需空间 (GB)	未受保护数据窗口	阈值	当前	错误和警告	重做传输
ARC_DA_0613	Recovery Appliance	vzdlra	ARCHIVELOG	0.7491	00:00:49	0.7491	0.7495	15.6633	六月 13, 2022 11:10:44 ...		
DAILY_0613220	Recovery Appliance	zdlra	DB INCR	414.4056	00:19:20	115.1538	101.6530	六月 13, 2022 09:00:58 ...			

状态	命令	类型	目标	开始时间	所用时间	输入大小 (GB)	输出大小 (GB)	输出速率 (MB/秒)
成功	ARCHIVELOG	Recovery Appliance	vzdlra	六月 13, 2022 11:10:44 ...	00:00:49	0.7491	0.7495	15.6633
成功	DB INCR	Recovery Appliance	zdlra	六月 13, 2022 09:00:58 ...	00:19:20	414.4056	115.1538	101.6530

广泛验证的零数据丢失恢复解决方案

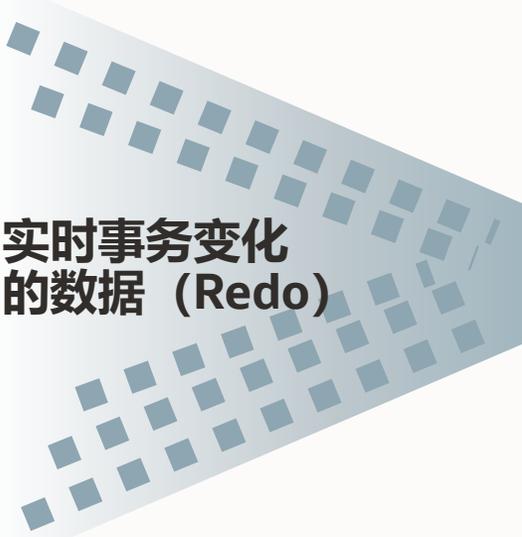
实时数据保护、一次全量、永久增量、端到端的验证、灵活的高可用部署架构

所有Oracle数据库



任何平台上的
Oracle DB 12c-21c

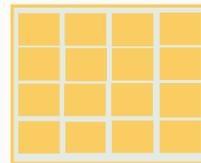
实时事务变化的
数据 (Redo)



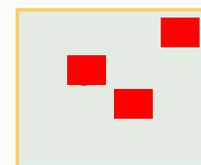
一次全备,
永久增量



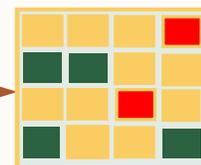
第一天全备



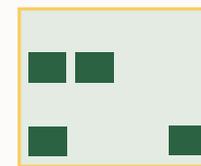
第二天增量



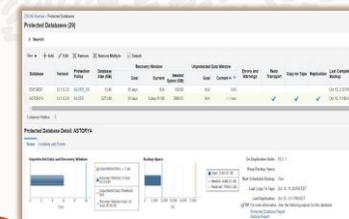
第N天状态



第N天增量



虚拟全备份



EM 备份配置,
实时保护状态
& 空间监控



云存储



远程副本



ZFS



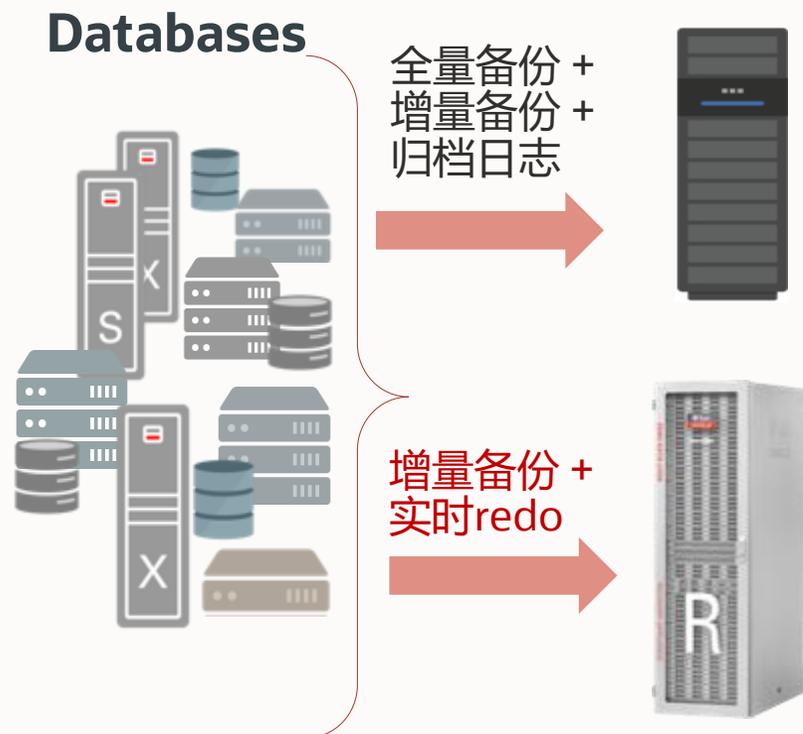
磁带

端到端 Oracle 恢复验证
灾难恢复的近零数据丢失



真正的实时数据保护能力 | RPO<1秒

Redo实时传输，确保所有完成的事务都可恢复



通用 Bit-Copy 备份设备

- 每天备份一次
- 丢失最后一次备份以来所有变化数据的风险

Zero Data Loss Recovery Appliance

- 基于Data Guard技术连续实时传输Redo来保护正在发生的交易数据；
- 从内存缓冲区立即传输每一个提交的事务，不涉及磁盘I/O，对生产系统影响小；
- ZD都会自动创建压缩的归档日志备份，不再需要从生产库备份归档日志；
- 日志采用异步（data guard async）传输模式，减小系统影响。

数据丢失本身就很糟糕，更糟糕的是，它会造成跨数据库的大量一致性问题。



一键式配置实时数据保护

在OEM的备份设置中选定ZDLRA作为备份目的地，选择“启用实时重做传输”即可开启Redo实时传输：

db12c (容器数据库) ⓘ 登录身份 sys | x5gw.cn.osc.oracle.com

Oracle 数据库 ▾ 性能 ▾ 可用性 ▾ 安全性 ▾ 方案 ▾ 管理 ▾

备份设置 还原 应用

设备 备份集 策略

Recovery Appliance 设置
此数据库配置为将备份发送到 Recovery Appliance。
以下列出的虚拟专用目录用户是已授予了备份受保护数据库所需权限的 Recovery Appliance 数据库用户，这些用户的已命名身份证明已设置为可供 Recovery Appliance 管理员访问。
提示 此数据库将配置为使用 HTTP 协议将备份发送到 Recovery Appliance。有关配置 HTTPS 协议的说明，请参阅 Recovery Appliance 文档。

Recovery Appliance ZDLRAX5
虚拟专用目录用户 cdbvpc1

启用实时重做传输

选择有权将备份从此数据库发送到所选 Recovery Appliance 的 Recovery Appliance 虚拟专用目录用户。
为了避免丢失数据，数据库会配置为将内存中重做数据实时传输到 Recovery Appliance。此操作可能需要重新启动数据库。

测试备份 清除配置

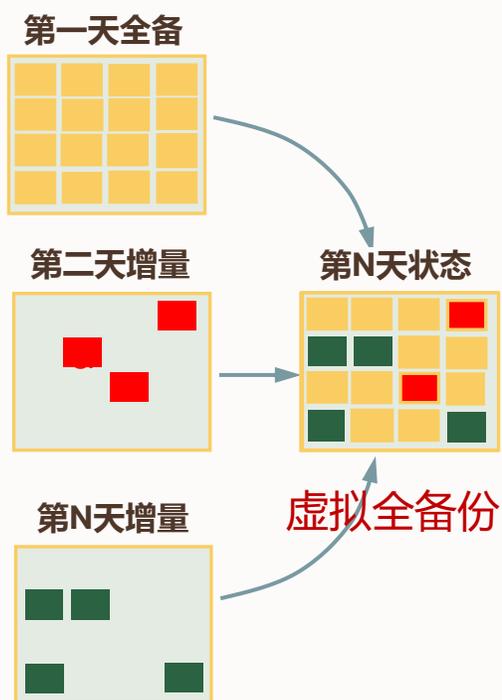
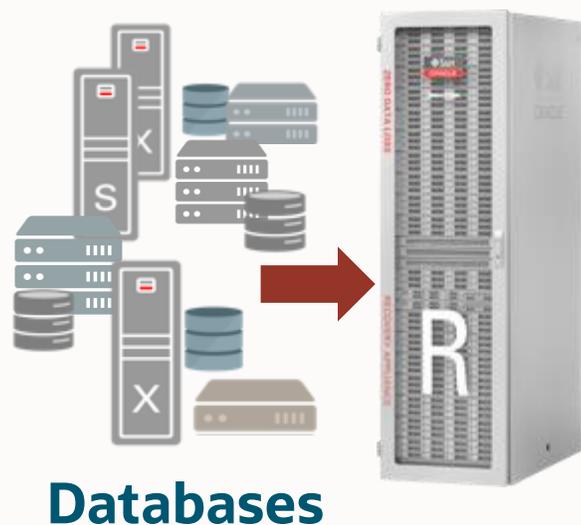
显示高级设置

此过程完全由OEM自动完成，期间需要重启数据库，开启之后数据库参数变化如下例所示：

- `*.log_archive_config='dg_config=(zdlradb,db12c)'`
- `*.log_archive_dest_2='SERVICE="x5zdingest-scan1:1521/zdlradb:dedicated"',
' ASYNC DB_UNIQUE_NAME=zdlradb VALID_FOR=(ALL_LOGFILES, ALL_ROLES)'`
- `*.log_archive_dest_state_2='ENABLE'`
- `*.redo_transport_user='CDBVPC1'`

“虚拟”全备份大幅度提升备份及存储效率

一次全备、永久增量的备份方式，彻底解决备份窗口问题

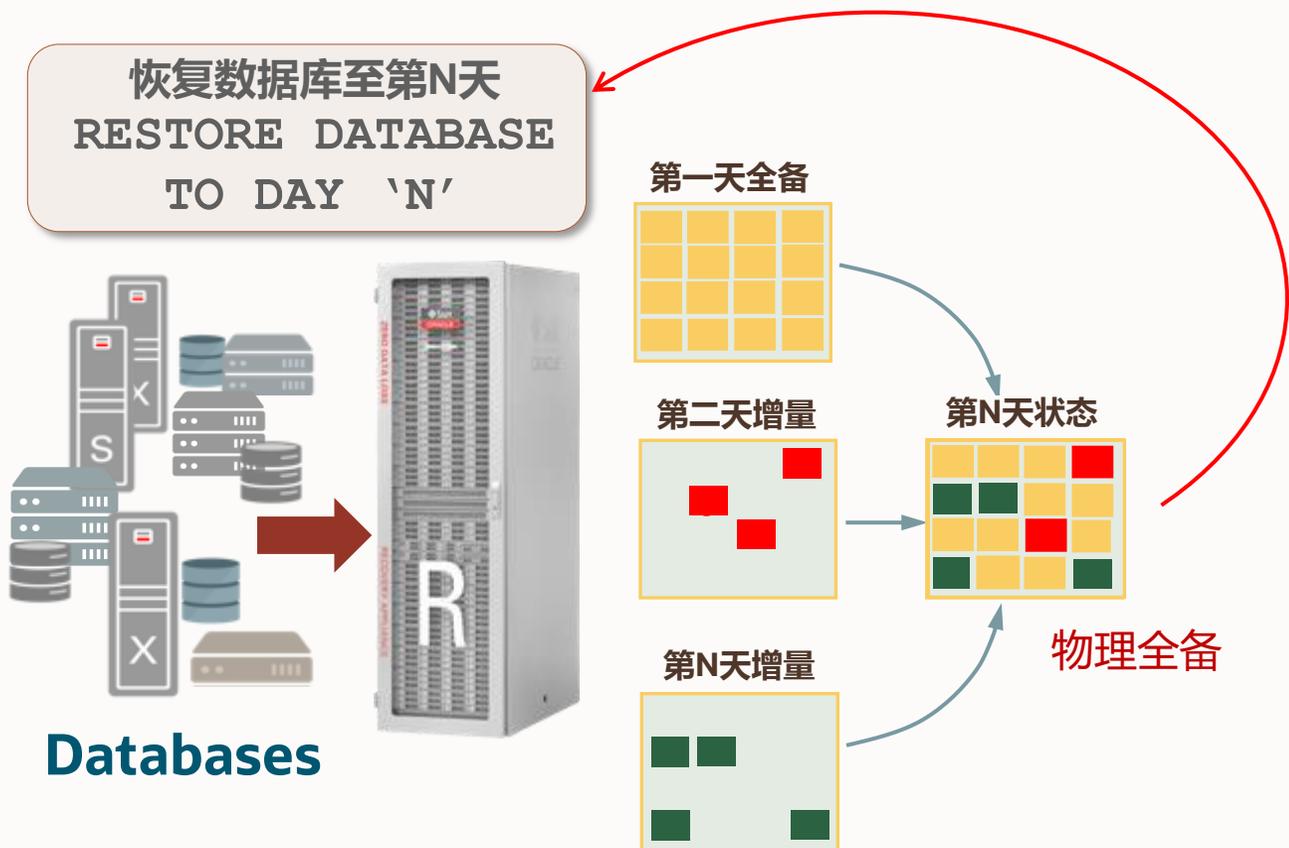


- 当完成初始的全量备份后，后续的每个增量备份自动生成**虚拟**数据库全备份
- 花费增量备份的时间，基于**指针**呈现物理全备份
- 虚拟备份通常节省**10倍**以上存储空间
- 尽可能消耗更少的存储空间保存更长久的备份数据
- 增量推送在源端完成数据去重
 - 快速增量备份(block change tracking)
 - 生产数据库的备份处理减少**10倍**以上
 - 减少备份网络消耗**10倍**以上



快速恢复到任意时间点

无需增量应用 = 减少生产服务器恢复时间



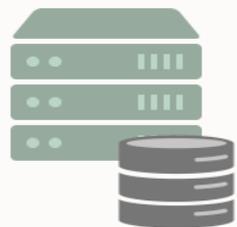
- 直接恢复任一虚拟全备份
 - 虚拟全备提供可预见的恢复效率;
 - 高效检索虚拟全备份需要的所有块;
 - 消除传统恢复依次应用增量备份所带来的开销。
- 采用了Exadata的高性能和高扩展性的硬件架构, 保证数据恢复的效率



端到端的数据损坏保护能力，保证数据的可恢复性

只有Oracle充分理解数据库的数据格式并提供端到端的数据块校验，是永久增量备份技术的基础

RAMN生成备份



- 备份时数据校验
- 已损坏块被发现并告警

生产备份一体机



云/磁带归档



远程复制



Oracle ASM 数据块校验与自动修复



自动用重镜像块中进行修复

坏块发现!



用好块去修复!

ZDLRA 数据校验时刻:

- 备份时数据校验，检测损坏/异常的块格式
- 数据接收和恢复时做校验
- 日常数据自动巡检，读取并校验数据块是否正常（默认每7天，可调整）
- Oracle ASM 数据块校验与自动修复
- ZDLRA至磁带库的读取与写入环节
- ZDLRA至其它ZDLRA的复制环节
- 除了RAMN生成备份时校验在生产上外其他校验在一体机上完成

ZDLRA自带磁盘冗余

- ZD磁盘中数据条带化和镜像
 - catalog 库三倍镜像
 - 数据库备份两倍镜像（默认）
- ZD 服务器组成一个集群(RAC) 提供fail over



实时可见的数据库可恢复状态

OEM集成的监视、告警及报告

所有被保护数据库的实时可恢复状态信息：

版本	数据库	目标类型	数据库大小 (GB)	重做传输	未受保护数据窗口		恢复窗口			复制	复制到云	复制到磁带	上次完全备份
					阈值	当前	目标	当前	所需空间 (GB)				
19.8.0.0.0	CXJB	集群数据库	3058.68	✓	2天 00:00:00	< 1秒	180天	192天 11:45	1721.11			✓	2021-10-17 下午08时28分31秒 CST
19.8.0.0.0	JGBX	集群数据库	1978.17	✓	2天 00:00:00	< 1秒	180天	301天 06:27	2469.89			✓	2021-10-17 下午07时00分24秒 CST
19.8.0.0.0	JGK	集群数据库	4041.02	✓	2天 00:00:00	< 1秒	180天	287天 22:13	2631.95			✓	2021-10-7 上午11时25分11秒 CST

开启redo实时传输

当前未受保护的数据量<1秒，恢复窗口目标180天，实际>180天



如果数据库不满足用户定义的恢复目标或阈值，则发出警报和警告



数据保护即服务：基于策略的管理，以满足整个企业的恢复SLA



可恢复性状态和系统利用率报告

基于策略的数据库保护即服务

简单明了的配置规则与方式

白金级保护策略



磁盘: 45天
磁带: 90天



黄金级保护策略



磁盘: 35天
磁带: 90天



白银级保护策略



磁盘: 10天
磁带: 45天



青铜保护策略



磁盘: 3天
磁带: 30天



Tape



Replica



远程复制目标端
ZDLRA同样基于
策略管理

ZDLRA 保护策略

- DBA熟悉的管理配置图形化界面
- 标准化恢复窗口大小、磁带保留时间、远程复制策略
- 客户可以自定义保护策略
- 远比传统备份软件容易理解和使用
- 让系统管理员和存储管理员从数据库备份中解脱出来

自定义保护策略

可以自定义保护策略来统一管理同一类型的数据库

Protection Policies

A protection policy contains Recovery Appliance properties for multiple protected databases in a single object.

Name	Disk Recovery Window Goal	Unprotected Data Window Threshold	Media Manager Recovery Window Policy	Maximum Disk Backup Retention	Storage Location
BRONZE	3 days		30 days		DELTA
GOLD	35 days		90 days		DELTA
OSC_PP1	1 day		1 day		DELTA
PLATINUM	45 days		90 days		DELTA
SILVER	10 days		45 days		DELTA

Protected Databases Using Protection Policy BRONZE

Database	Target Name
No data to display.	

Edit Protection Policy

Name: PLATINUM
Description: Default Platinum Protected Policy

Storage Location ← 存储池
Select the storage location where backups will be placed for all databases using this protection policy.

Name	Size (GB)	Reserved Space	
		%	GB
DELTA	63926.7	32.0	20480.0

Disk Recovery Window Goal
Specify a recovery window goal that Recovery Appliance should attempt to meet for point-in-time recovery using disk backups.

* Recovery Window: 45 days ← 磁盘保留策略

Unprotected Data Window Threshold
Specify the maximum amount of time in which there is potential data loss exposure for databases associated with this protection policy. If this amount of time is exceeded for a database associated with this policy, a warning will be generated.

Threshold: [] days ← 数据不受保护 最大时间

Media Manager Recovery Window Policy
Specify a longer window within which point-in-time recovery capability from a media manager (e.g., Oracle Secure Backup) will be maintained.

Recovery Window: 90 days ← 磁带保留时间

Maximum Disk Backup Retention
Specify the maximum time that disk backups should be retained. This value must be greater than or equal to the disk recovery window goal. If not specified, backups will be retained beyond the disk recovery window goal as space permits.

Maximum Retention: [] days ← 磁盘上最大保留时间默认有空间就不删除

Advanced Parameters

Backup and Redo Failover
Specify whether protected databases using this protection policy will use this Recovery Appliance as an alternate destination in a backup and redo failover strategy. If enabled, backups and redo for protected databases that use this protection policy will be stored temporarily for later forwarding to a primary Recovery Appliance, after which they will be deleted from this Recovery Appliance.

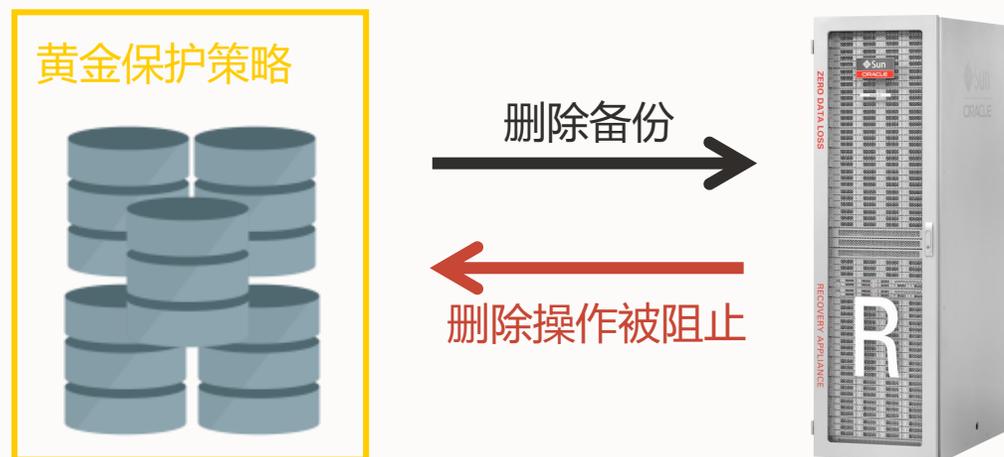
OK Cancel

说明：先按规划自定义保护策略，在通过OEM添加受保护数据库时，要求选择与数据库关联的保护策略。

基于策略的职责分离

职责划分保证数据安全，避免恶意或误删备份

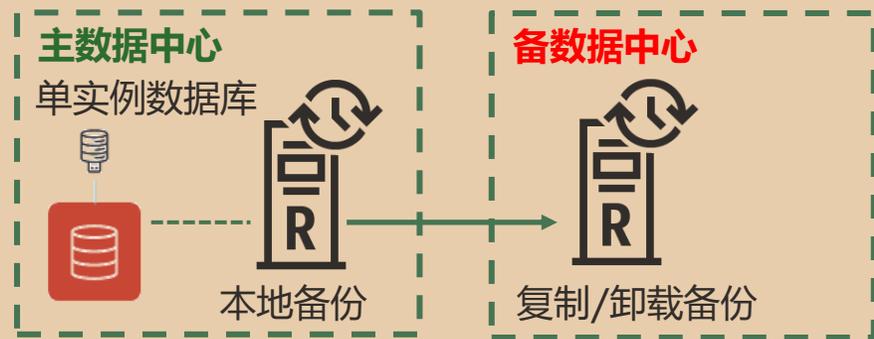
- 在保护策略中可以通过高级参数，来阻止对存储在ZDLRA中的备份执行RMAN DELETE操作；
- 任何管理员（DBA或RA）都不能删除数据库备份；
- 备份空间的重复利用由保留策略决定；
- 存储设备没有意识到错误的删除操作，这可能导致业务SLA受损；
- 集中化、数据库感知的“保护即服务”与常规文件备份的显著区别，传统备份方式无法保证数据不被删除。



双中心数据备份是MAA架构的基础

青铜

开发、测试



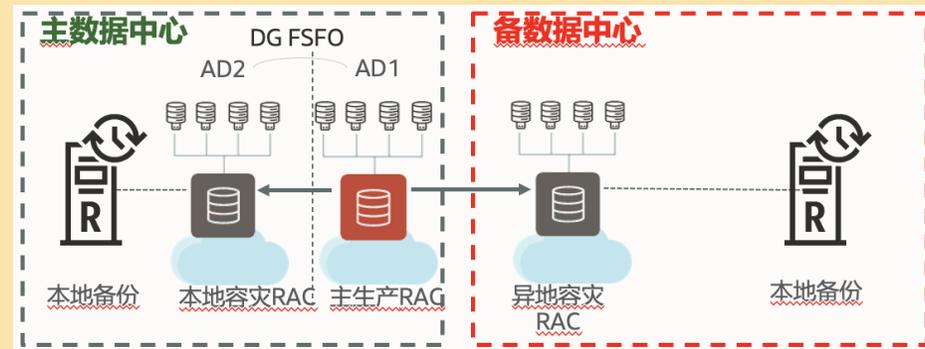
白银

部门级/普通应用



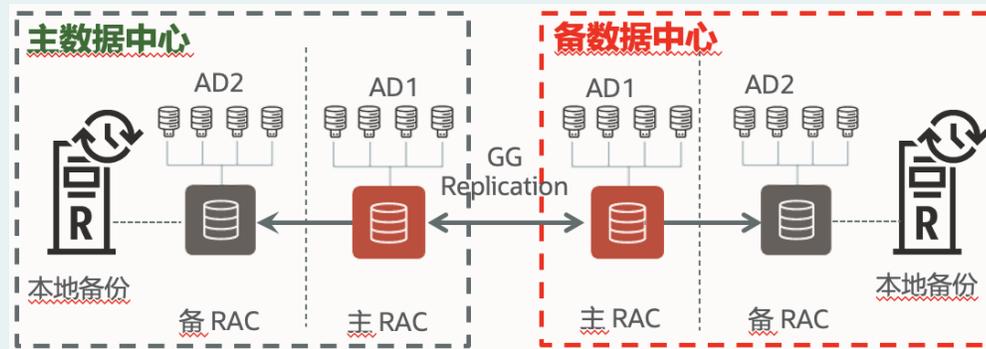
黄金

关键业务



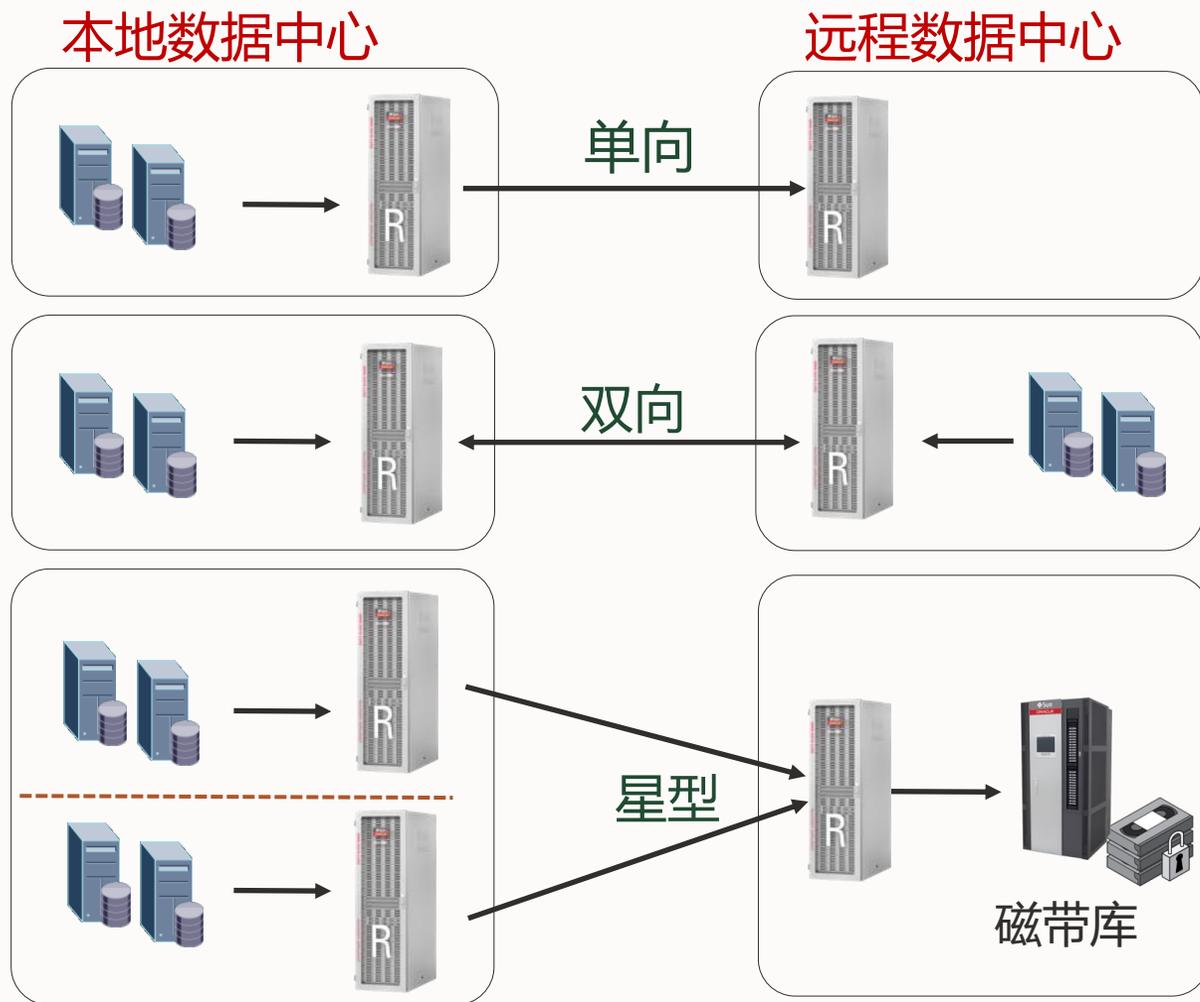
白金

极端关键业务



ZDLRA灵活的高可用架构

备份数据异地保存确保数据万无一失



- ZDLRA基于Exadata的冗余硬件架构
 - 2 RAC节点, 最少3存储节点
 - Catalog库3副本, 备份数据2副本
 - Catalog定期备份到本地, 可配异地备份
- 备份数据复制到远程数据中心容灾
- 定期卸载备份到磁带库, 增强备份生命周期管理
 - 在OEM上配置定时任务自动将全备/增备/归档复制到磁带库
- 自动智能直接从本地或磁带库或远程ZDLRA恢复数据

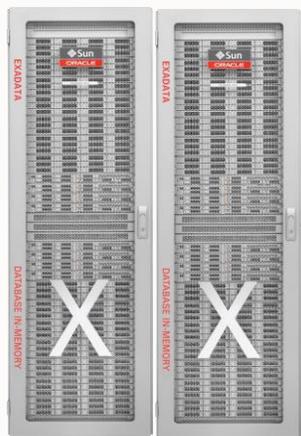


建设方案参考 | 某政府客户核心业务系统零数据丢失高可用架构

同城黄金级别双活中心，ZDLRA实时备份并卸载备份到备中心带库，PBBA从备库定期备份

主生产中心

核心业务多租户部署，
超过20PDBs



核心数据库资源池
登云X8M HC 1/2*2
Oracle 19c

数据交换、回流



X86+存储

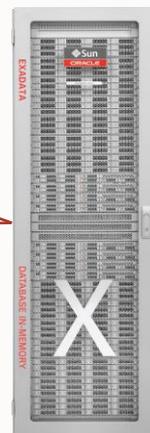
OEM统一管理



ADG

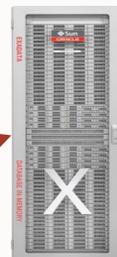
从生产中心

核心业务备库，
读写分离



登云X8M HC 1/2
Oracle 19c

分析、统计
报表等



X8M-2 HC 1/4

实时备份



ZDLRA
Base Rack+扩容存储

卸载备份



昆腾带库

专用备份设备PBBA，定期全量+增量+归档备份



某政府客户核心业务系统零数据丢失高可用架构

实时可见的数据库备份及可恢复状态

ZDLRA备份一体机

Recovery Appliance

ZDI db2 (容器数据库)

集群数据库 性能 可用性 安全性 方案 管理

备份报告

查看 总计 1 (已完成 1)

备份名	状态	命令	目标	开始时间	所用时间	输入大小 (GB)	输出大小 (GB)

ORACLE Enterprise Manager Cloud Control 13c

企业(E) 目标(T) 收藏夹(E) 历史记录(O) 设置(S)

ZDLRA备份一体机

Recovery Appliance

ZDLRA备份一体机 > 复制到介质作业模板

复制到介质作业模板

复制到介质作业模板描述应复制到介质的备份，并指定用于控制复制操作的介质管理器属性集。

查看 创建 编辑 删除 分离

ZDLRA复制备份到带库任务状态

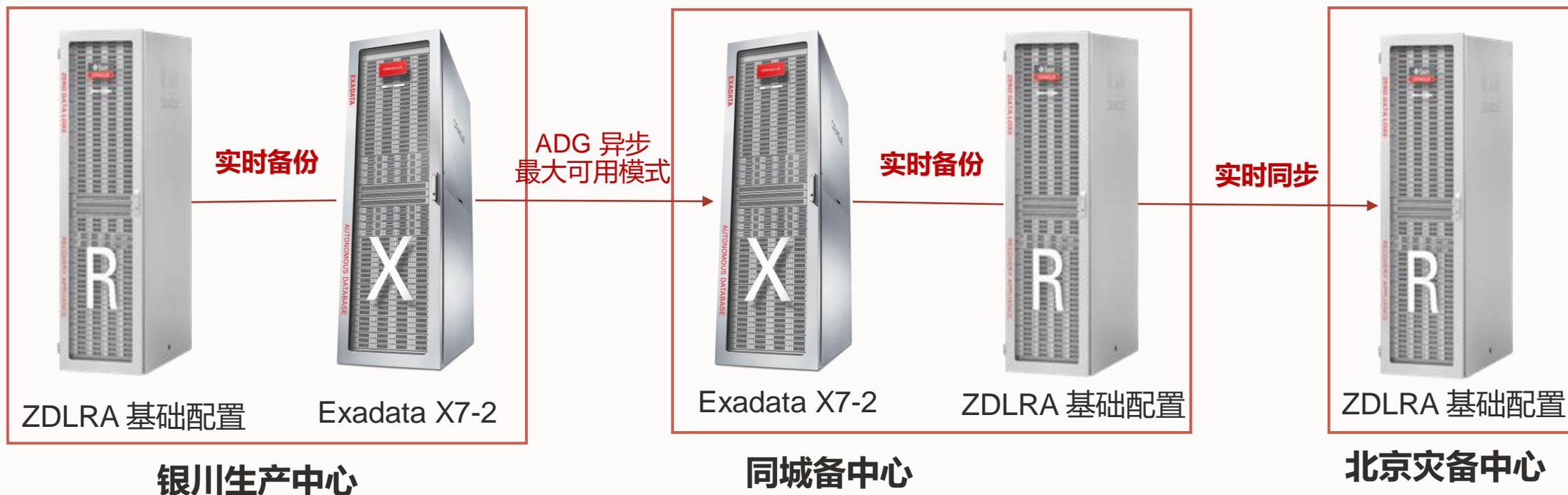
保护策略	介质管理器			数据库	备份类型	优先级	已调度	名称	任务				上次复制活动	排队数据 (GB)	压缩算法
	库	属性集	状态						已排队	正在运行	已完成 (过去 24 小时)	状态			
	ROBOT0	ROBOT0_DRIVE_COUNT_2	●	DB1	FULL		✓	COPY_FULL_DB1	106			⚠		9980.0	LOW
	ROBOT0	ROBOT0_DRIVE_COUNT_2	●	DB2	FULL		✓	COPY_FULL_DB2	1127	1	3	✓		12642.0	LOW
	ROBOT0	ROBOT0_DRIVE_COUNT_2	●	DB2	INCR		✓	COPY_INC_DB2			46	✓			LOW
	ROBOT0	ROBOT0_DRIVE_COUNT_2	●	DB1	INCR		✓	COPY_INC_DB1		1	41	✓			LOW



建设方案参考 | 某银行新一代核心系统零数据丢失三中心高可用架构

多重保护，确保RPO=0

- 两地三中心，ADG最大可用容灾同步，每个中心各一台ZDLRA；
- 同城容灾中心的ZDLRA实时同步备份到北京容灾中心的ZDLRA中；
- 两地三中心的Exadata及ZDLRA通过OEM集中化监控和管理。



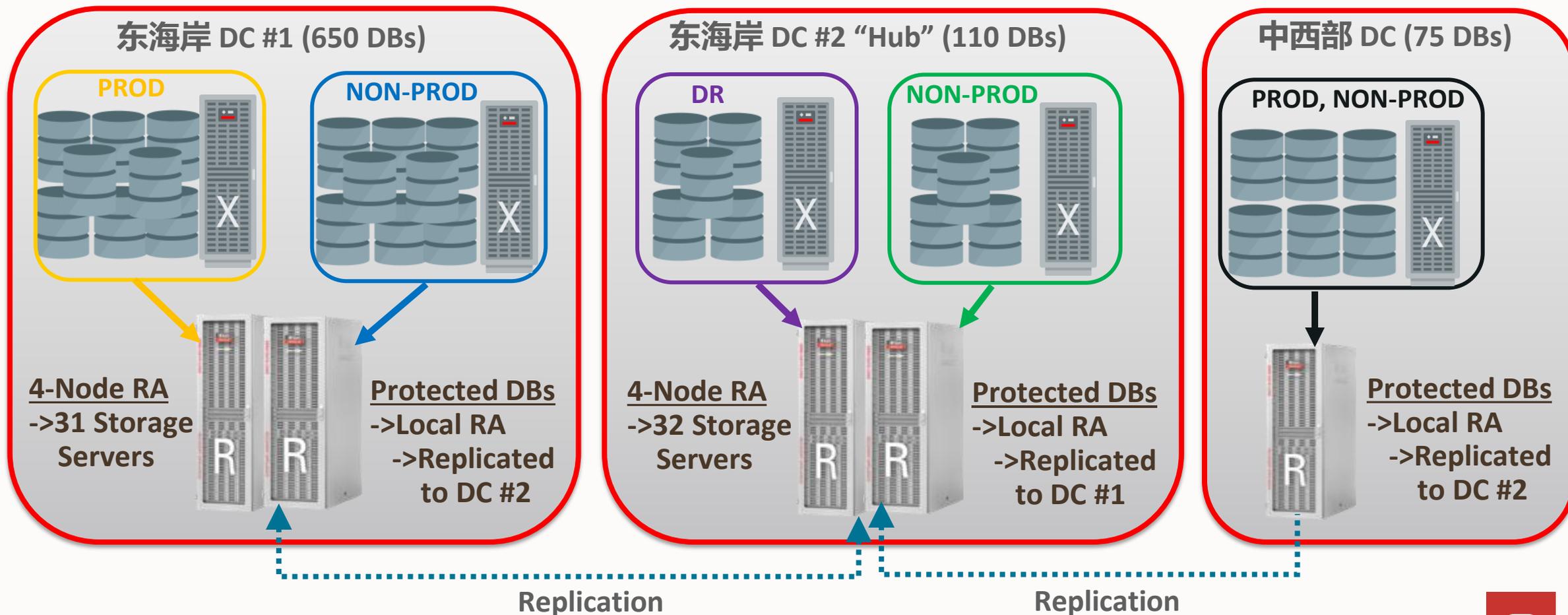
建设方案参考 | 安森保险云级的弹性扩展架构

按需扩展备份恢复能力，灵活组合构建高可用架构



Cloud Scale

- 领先的北美健康福利公司 - 4000万+会员
- 800+受保护的数据库，3个数据中心，双向 + 星型实时复制



总结

1

全球客户实践总结出来的 Oracle 最大可用性架构(MAA)，满足系统严苛的 RTO 和 RPO 要求

2

Oracle 零数据丢失恢复解放方案可有效消除数据丢失的风险

3

今天就开始您的企业 MAA 架构健康风险评估，揭示潜在风险，得到业务连续性优化的方向指引



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

