ICS 35. 220
CCS L 64

# T/CASME

中 国 中 小 商 业 企 业 协 会 团 体 标 准

T/CASME XXXX—2023

# 数据库灾备管理系统体系架构与功能要求

Database disaster manage system architecture and functional requirements

（征求意见稿）

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

发 布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：××××

本文件主要起草人：××××

# 数据库灾备管理系统体系架构与功能要求

## 1 范围

本文件规定了数据库灾备管理系统的术语和定义、体系架构、参数指标、功能要求、接口要求、安全要求、监控流程管理及系统测试内容。

本文件适用于数据库灾备管理系统的设计、开发和集成应用。本文件所涉及的数据库灾备管理系统是指适用于大中型企事业客户单位数据中心Oracle数据库容灾环境，包括在同机房、同城、两地三中心等建设的数据库灾备环境的监控及管理。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**容灾** disaster recovery

一种降低灾难损失的系统部署方案。部署一套和生产系统相当的灾备系统作为生产系统的一个备用，以便在生产系统故障时能够保存生产数据，在生产系统恢复前将应用切换到灾备系统中运行，生产系统恢复后将应用重新切换到原生产系统中运行。

3.2

**灾备中心** disaster recovery center

灾备中心是信息化建设的重要组成部分，是信息化时代防范灾难、降低损失的重要手段。灾备中心的选址失误将导致灾备中心本身面临灾难，最终导致灾难备份措施的失效。

## 4 体系架构

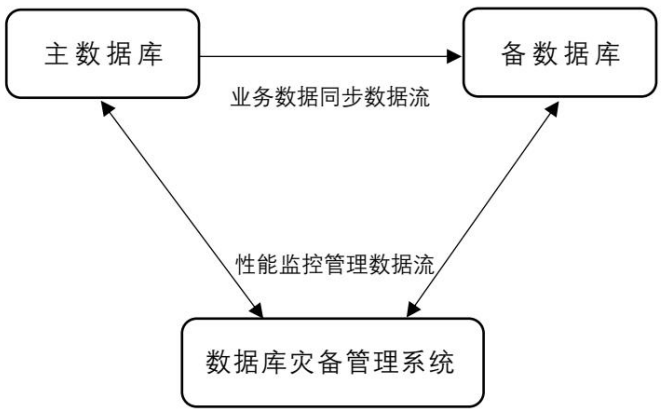


图 1 数据库灾备管理系统体系架构

4.1 应通过数据库内置连接驱动配置各个数据源的连接。
4.2 应大量采集数据库内性能数据及合理阀值设定，简化、准确的反映系统状态。

## 5 参数指标

数据库灾备管理系统的参数指标见表1。

**表 1 参数指标**

| 分类 | 项目 | 参数 |
|---|---|---|
| 兼容性 | 数据库版本 | Oracle Database Standard/Enterprise Edition 9i |
| | | Oracle Database Standard/Enterprise Edition 9i |
| | | Oracle Database Standard/Enterprise Edition 11gR1 |
| | | Oracle Database Standard/Enterprise Edition 11gR2 |
| | | Oracle Database Standard/Enterprise Edition 12c |
| | | Oracle Database Standard/Enterprise Edition 18c |
| | 操作系统版本 | CentOS 7 或以上 |
| | | RedHat Linux 7 或以上 |

## 6 功能要求

### 6.1 可视化状态监控平台

6.1.1 应通过图形直观、简单的显示系统监控的重要指标，如灾备架构拓朴、延迟告警、流量告警及可用性告警等。
6.1.2 应直观地在大屏展示主、备库之间的数据流向、状态、数据差异等、追齐差异估算的时间等信息，最大程度降低运维成本和提升系统运行的连续性。
6.1.3 应针对客户数据库中心的容灾数据库环境有效性进行监控，及时发现容灾数据库运行异常，数据同步中断、数据同步延迟时等状况，并进行预警展现，确保数据库始终处于容灾保护状态下。

### 6.2 综合管理平台

应通过图形向导的方式完成所有监控管理、配置等工作。

### 6.3 独立系统管理

应对每套监控对象可实现单独管理，准确、直观的展示具体监控对象当前状态。包括网络使用、数据同、异步情况等。

### 6.4 同步管理

应能根据管理需要暂停、恢复同步，展现同步差异。

### 6.5 容灾数据库状态可用性监控

应针对客户数据库中心的容灾数据库环境有效性进行监控，及时发现容灾数据库运行异常，数据同步中断、数据同步延迟时等状况，并进行预警展现，确保数据库始终处于容灾保护状态下。

### 6.6 主、备数据库环境数据一致性校验

应实现数据一致性快速校验且不用停机窗口，主要从物理和逻辑两个方面快速校验主、备数据库数据的一致性。

### 6.7 主、备库正常切换可视化导航平台

6.7.1 可通过“一键式”和“分阶段”在 web 界面快速透明实现主备切换，在后台由系统封装了结合 Oracle 最佳实践及客户实际生产环境的切换检查程序，自动进行切换准备，切换条件许可检查及主备切换操作，大幅简化的前台界面用户的操作。
6.7.2 通过可视化切换导航平台，可执行正常例行切换（SWITCH OVER 主备正常切换，切换后不破

换容灾环境），也可在生产端故障时进行紧急故障切换(FALIED OVER) 极大减少故障影响时间，避免人为切换出错。

### 6.8 监控、校验灵活配置

6.8.1 应对图形细颗粒化的监控配置调整，应对各种场景下合理的调整。

6.8.2 应具有短信、邮件告警平台接口，当系统发现异常时用户可以通过短信或邮件进行通知,发送告警数据（需客户配置）。

### 6.9 权限及审计

系统根应据功能权限划分不同角色，通过授予用户不同的角色实现权限管理，并对用户操作进行详细记录及审计。

## 7 接口要求

### 7.1 接口类型及功能

#### 7.1.1 数据存储接口

数据存储接口是访问层与应用平台层之间的接口，该接口应支持：

a) 灾备数据的在线接入和离线接入，并验证源数据完整性；
b) 对灾备数据进行基于不同数据判重模式的数据判重功能；
c) 对灾备数据进行存储前的完整性校验；
d) 灾备数据分布式存储以及索引文件存储。

#### 7.1.2 数据访问接口

访问接口是访问层与应用平台层之间的接口，该接口应支持：

a) 依据索引文件获取当前所需文件数据存储位置信息；
b) 获取数据文件或数据块，进行数据完整拼接；
c) 灾备数据的完整性校验能力；
d) 实现数据的导出及展现能力。

#### 7.1.3 安全审计接口

安全审计接口是访问层与应用平台层之间的接口，该接口应支持：

a) 实现日志审计等功能，审计记录中应至少包括事件的日期和时间、类型、主体身份及结果。
b) 实现日志数据的基本操作管理，包括查询、导出等。

## 8 安全要求

### 8.1 安全审计

#### 8.1.1 日志审计

应能对各类日志进行审计。

#### 8.1.2 审计内容

审计记录中应至少包括事件的日期和时间、类型、主体身份、结果。

#### 8.1.3 日志授权访问

只有授权用户才能访问相应的系统日志。

#### 8.1.4 日志格式

日志格式应规范化，含义应便于理解。

### 8.2 数据安全

#### 8.2.1 数据完整性监视

应能对数据库灾备管理系统中是否出现完整性错误进行监控。

#### 8.2.2 安全传输

数据应以安全的格式传输。

#### 8.2.3 安全存储

数据应以安全的格式存储于备份介质上。

### 8.3 访问控制

#### 8.3.1 身份认证

应该能够在网络中验证操作者身份。

#### 8.3.2 鉴别失败处理

当用户的失败登录次数超过允许的尝试鉴别次数时，应阻止该用户的进一步登录尝试，直至授权管理员恢复对该用户的鉴别能力。

#### 8.3.3 安全相关操作访问控制

应能对系统安全相关操作设置访问控制策略。

### 8.4 风险控制

应按GB/T 22239的规定执行。

### 8.5 系统监控

应能监控系统的运行状态，并以适当方式反馈给管理员，例如电子邮件、手机短信等方式。

## 9 监控流程管理

### 9.1 数据库切换

9.1.1 应能查看地理视图与系统视图。应能查看数据库状态。
9.1.2 应能启动、暂停、刷新对数据库的监控状态。
9.1.3 应能停止主备数据库之间的监控状态。
9.1.4 应能进行主备数据库之间的切换，切换模式应根据系统配置及切换配置里配置的模式进行。
9.1.5 切换类型应分为一键切换模式和分阶段切换模式。
9.1.6 分阶段切换模式下，一次完整的切换一共有 7 个阶段，每个阶段里执行的步骤应是系统固定的，每个阶段只有在改阶段的所有步骤执行完成时才能执行下一阶段；只有在完成或者出错时才能重新执行。
9.1.7 可对容灾数据库进行维护管理，包含参数设置，动静态检测间隔及警告异常延迟阈值设置等功能。

### 9.2 数据校验

数据校验应包括系统校验和切换校验。

### 9.3 数据源配置

9.3.1 数据源配置应能管理同步组与站点，应具备新增需监控的数据库与节点及同步组。
9.3.2 选择某一个站点，应能进行配置站点。
9.3.3 应具备删除某一个同步组或站点的功能。

### 9.4 系统配置

系统配置应能对容灾数据库进行维护管理，可配置整个系统的动态、静态检测间隔、静态检测时间段、警告延迟阈值、邮件通知及切换配置等参数。

### 9.5 权限管理

9.5.1 权限管理应能查看角色管理与用户管理。
9.5.2 应能新增新的角色并进行菜单权限的分配，应能新增新的用户并分配已建好的角色。

### 9.6 系统审计

9.6.1 系统审计应能查看对应时间内所有用户在对应模块所做的操作，应能选择需要的信息。
9.6.2 应具备查看对应时间段内的系统审计情况的功能。

## 10 系统测试

### 10.1 一般规定

#### 10.1.1 测试类别

测试类别为主备切换。

#### 10.1.2 测试内容

测试内容为：
c） 生产中心与同城灾备中心切换；
d） 新生产中心（原同城灾备）与新同城中心（原生产）切换。

#### 10.1.3 测试方法

测试方法为部署 RAC 到单实例数据库的 Oracle Active DG 测试环境，部署灾备监控管理平台，在灾备监控管理平台上进行 RAC 与单实例数据库之间主备互相切换测试。

### 10.2 测试环境

#### 10.2.1 主库信息

主库信息具体要求见表2。

表 2 主库信息

| 项目 | 参数 |
|---|---|
| 操作系统 | RedHat 7.5 |
| IP | 192.168.1.240 |
| 数据库类型 | Single Instance Database |
| ORACLE_SID | dmssadg |
| ORACLE_HOME | /u01/app/oracle/product/12.2.0/dbhome_1 |
| 数据库版本 | 12.2.0.1 |
| 数据库监听端口 | 1521 |

#### 10.2.2 备库信息

备库信息具体要求见表3。

表 3 备库信息

| 项目 | 参数 |
|---|---|
| 操作系统 | RedHat 7.5 |
| IP | 192.168.1.222 |
| 数据库类型 | Real Application Clusters |
| ORACLE_SID | dmss |
| ORACLE_HOME | /u01/app/oracle/product/11.2.0/dbhome_1 |

| 项目 | 参数 |
| --- | --- |
| 数据库版本 | 12.2.0.1 |
| 数据库监听端口 | 1521 |

### 10.3 功能配置

#### 10.3.1 数据源同步组管理

应先添加同步组，并将一组主备库挂靠到同一个同步组下。

#### 10.3.2 数据源配置

10.3.2.1 应在“数据源配置”界面添加测试模拟生产数据源。
10.3.2.2 应添加模拟灾备节点数据源。
10.3.2.3 添加数据源后，应手工拖动数据源到相应的同步组和站点下。

#### 10.3.3 地理视图监控

地理视图监控应显示包括生产机房、同城灾备中心、异地灾备中心等内容。

#### 10.3.4 系统视图监控

系统视图监控应显示包括生产机房、同城灾备中心、归档传输时间、流量等内容。

#### 10.3.5 系统配置

系统配置处可对监控、告警进行设置，也可设定切换模式包括一键切换及分阶段切换。

#### 10.3.6 系统校验功能

应能对主备库归档日志同步情况进行校验。

#### 10.3.7 切换校验功能

应能在主备切换前，对主备库状态进行校验，校验通过时方可进行主备切换。

### 10.4 切换测试

#### 10.4.1 模拟生产到模拟灾备测试数据库切换

10.4.1.1 应在数据库切换界面选中需要切换的同步组。
10.4.1.2 应点击切换按钮打开切换界面，选择切换方式。
10.4.1.3 切换方式分为一键切换与分阶段切换，分属例行维护切换和故障紧急快速切换。两者对数据库执行的操作相同，但后者需要人工干预，将切换任务拆分成多个阶段，上一个阶段执行完毕后，需手工启动下一阶段。

#### 10.4.2 模拟灾备到模拟生产测试数据库切换

10.4.2.1 应将模拟生产测试数据库切换至模拟灾备库后，再次将主库切回。
10.4.2.2 应验证切换后的数据同步，创建表及插入数据。
10.4.2.3 应查询备库中 test 表，数据已同步。