ICS 35.240.01
CCS L 70

SJ

中华人民共和国电子行业标准

SJ/T 11938—2024

安全可靠 分布式事务型数据库技术要求

Safety and reliability—Technical requirement for distributed transactional database

2024-07-19 发布　　2024-10-01 实施

中华人民共和国工业和信息化部　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。

本文件由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、华为云计算技术有限公司、武汉达梦数据库有限公司、北京人大金仓信息技术股份有限公司、阿里云计算有限公司、腾讯云计算有限责任公司、华为技术有限公司、星环信息科技（上海）股份有限公司、天津南大通用数据技术股份有限公司、成都虚谷伟业科技有限公司、平凯星辰（北京）科技有限公司、北京奥星贝斯科技有限公司、中兴通讯股份有限公司、北京万里开源软件有限公司、北京科蓝软件系统股份有限公司、北京偶数科技有限公司、北京柏睿数据技术股份有限公司、湖南亚信安慧科技有限公司、国家工业信息安全发展研究中心、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、工业和信息化部电子第五研究所、中国信息通信研究院。

本文件主要起草人：付平、董建、杨磊、张群、杨锐、石建军、冷建全、樊文凯、陈琢、冯柯、刘汪根、赵伟、明玉琢、余梦杰、王栩、吕伟初、娄帅、殷正栋、苏景志、刘睿民、张桦、张士宗、王剑、梁佳男、王寒冰、李峙、张杰、王秀娟、陈伟红、程静、董文、廖涵、耿航、张浩、谢玉波、吴明远、苏德财、曹金龙、隗华、秦延涛、郑贵德、姚佳丽、赵菁华、洪建辉。

安全可靠　分布式事务型数据库技术要求

1　范围

本文件规定了在安全性和可靠性方面具有更高要求的分布式事务型数据库（以下简称“分布式数据库”）的功能、性能、可靠性、安全性、兼容性和售后服务要求。

本文件适用于分布式数据库产品的设计、开发和应用。

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 18030　信息技术　中文编码字符集

GB/T 20273—2019　信息安全技术　数据库管理系统安全技术要求

GM/T 0028　密码模块安全技术要求

SJ/T 11936—2024　安全可靠　服务器操作系统技术要求

SJ/T 11941—2024　安全可靠　服务器技术要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

关系数据库　relational database

采用关系数据模型的数据库。

[来源：GB/T 28821—2012，3.2]

3.2

数据库管理系统　database management system

基于硬件与软件，用于定义、监理、操纵、控制、管理和使用数据库的系统。

[来源：GB/T 5271.17—2010，17.01.03]

3.3

事务　transaction

一组以原子性、一致性、隔离性、持久性为特征的相关操作。

3.4

节点　node

在网络中，将其连接到一个或多个其他实体的实体。

3.5

分布式事务型数据库　distributed transactional database

具有分布式事务处理机制的关系数据库。

注：用计算机网络将物理上分散的多个数据库节点连接起来组成的一个逻辑上统一的单一数据库实例。

3.6

可用区 availability zone

一个或多个通过网络连接的物理数据中心的集合。

注：通常可用区内数据中心位于同一城市，相互距离一般不超过50km。

3.7

角色 role

具有相同数据库权限的用户集合。

3.8

恢复点目标 recovery point objective

灾难发生后，系统和数据恢复到的时间点要求。

[来源：JR/T 0044—2008，3.17]

3.9

恢复时间目标 recovery time objective

灾难发生后，信息系统或业务功能从停顿到恢复的时间要求。

[来源：JR/T 0044—2008，3.18]

4 缩略语

下列缩略语适用于本文件。

ACID：原子性、一致性、隔离性、持久性（atomicity、consistency、isolation、durability）

API：应用编程接口（application programming interface）

CLOB：字符大对象（character large object）

CPU：中央处理器（central processing unit）

DBMS：数据库管理系统（database management system）

EAL：评估保障级（evaluation assurance level）

GIS：地理信息系统（geographic information system）

I/O：输入/输出（input/output）

IP：互联网协议（internet protocol）

IPv6：互联网协议第6版（internet protocol version 6）

JDBC：Java数据库互联（Java database connectivity）

JSON：JavaScript对象表示（JavaScript object notation）

NUMA：非统一内存访问（non uniform memory access）

ODBC：开放数据库互联（open database connectivity）

RPO：恢复点目标（recovery point objective）

RTO：恢复时间目标（recovery time objective）

SMP：对称多处理结构（symmetric multi-processing）

SQL：结构化查询语言（structured query language）

SSL：安全套接层（secure sockets layer）

TLCP：传输层密码协议（transport layer cryptography protocol）

TLS：传输层安全（transport layer security）

TPC：事务处理性能委员会（transaction processing performance council）

TPS：每秒事务处理量（transaction per second）

XML：可扩展置标语言（extensible markup language）

5 功能

5.1 安装与升级

5.1.1 数据库安装与启停

5.1.1.1 数据库的安装与卸载

分布式数据库的安装与卸载应符合下列要求：

a） 支持可配置安装能力；

b） 依据安装环境提供相应的初始化参数配置值，包括内存配置等；

c） 提供组件安装向导，如工具或驱动等；

d） 安装完成后，支持各节点的状态查询；

e） 支持数据库的卸载。

5.1.1.2 数据库的启动与关闭

分布式数据库应支持关闭服务后，再启动服务，服务正常。

5.1.2 安装配置日志

分布式数据库的安装配置日志应符合下列要求：

a） 记录软件安装信息和配置信息；

b） 提供安装配置操作的日志记录功能，包括安装路径和数据目录等。

5.1.3 升级维护

分布式数据库的升级维护应符合下列要求：

a） 支持数据库版本滚动升级；

b） 厂商提供保证版本升级功能和数据的兼容性文档；

c） 厂商提供当前版本与历史版本的差异说明文档，包含新版本对软件和硬件的支持情况。

5.1.4 节点部署

分布式数据库宜支持通过单一节点发起部署，将数据库部署在多个节点上。

5.2 系统配置

5.2.1 配置生效

分布式数据库的参数配置应符合下列要求：

a） 依据工作负载和运行环境，提供配置参数建议值及修改的能力；

b） 修改数据库配置参数后，配置参数立即生效或数据库重新启动生效，立即生效的配置参数和需要数据库重新启动方可生效的配置参数应在相关文档中明确。

5.2.2 存储配置

分布式数据库的存储配置宜符合下列要求：

a） 提供数据文件、日志文件和归档文件的物理存储位置和逻辑存储参数配置功能；

b） 提供数据库存储对象空间使用参数的配置功能；

c） 提供索引数据存储参数管理功能。

5.2.3 内存配置

分布式数据库的内存配置宜符合下列要求：

a) 提供数据库内存规划和配置建议；
b) 依据物理内存规划数据库可用内存。

5.2.4 网络配置

分布式数据库的网络配置应符合下列要求：

a) 支持对连接参数、主机、端口和协议等网络参数进行配置；
b) 支持 IPv6 访问。

5.2.5 其他配置

分布式数据库应支持对字符集、大小写等参数进行配置。

5.3 SQL 功能

5.3.1 基础数据类型

分布式数据库应支持下列基础数据类型：

a) 数值类型，
b) 字符类型，
c) 二进制类型，
d) 日期和时间类型，
e) 布尔类型，
f) 文本类型，如 CLOB 或 TEXT，
g) 大对象类型，
h) 间隔、数组、XML 和 JSON 等数据类型。

5.3.2 扩展数据类型

分布式数据库宜支持 GIS、时序或向量等扩展数据类型。

5.3.3 自定义数据类型

分布式数据库宜具备用户自定义数据类型的能力。

5.3.4 数据存储

分布式数据库的数据存储符合下列要求：

a) 应支持基础数据类型；
b) 宜支持扩展数据类型；
c) 宜支持自定义数据类型。

5.3.5 数据检索

分布式数据库的数据检索符合下列要求：

a) 应支持基础数据类型；
b) 宜支持扩展数据类型；
c) 宜支持自定义数据类型；
d) 宜支持中文检索功能，如使用中国纪年历法进行检索。

5.3.6 核心 SQL 能力

分布式数据库应提供下列核心 SQL 能力：

a) 左外连接，
b) 右外连接，
c) 内连接，
d) 全连接。

5.3.7 字符集

分布式数据库中文字符集应符合 GB 18030 的要求。

5.3.8 常用操作符

分布式数据库应支持下列常用操作符：

a) 逻辑操作符及相关运算，
b) 比较操作符及相关运算，
c) 算术运算符及相关运算。

5.3.9 条件表达式

分布式数据库应支持下列条件表达式：

a) 对比条件表达式，
b) 逻辑条件表达式，
c) 空值条件表达式，
d) 等于条件表达式，
e) 模式匹配条件表达式，
f) 区间条件表达式，
g) IN 条件表达式，
h) 存在条件表达式，
i) 以上条件表达式的复合表达式。

5.3.10 SQL 执行计划

分布式数据库的 SQL 执行计划应符合下列要求：

a) 支持查看 SQL 语句执行计划与统计信息；
b) 支持对 SQL 执行计划的优化，如用户指定（Hint）等。

5.4 数据库对象

5.4.1 基础对象类型

5.4.1.1 数据库

分布式数据库应支持数据库的创建、删除和修改。

5.4.1.2 用户

分布式数据库应支持用户的创建、删除和修改。

5.4.1.3 角色

分布式数据库应支持角色的创建、删除和修改。

5.4.1.4 存储过程

分布式数据库应支持存储过程的创建、删除和修改。

5.4.1.5 表

分布式数据库应支持表的创建、删除和修改。

5.4.1.6 序列

分布式数据库的序列符合下列要求：

a) 应支持序列的创建、删除和修改；
b) 宜支持全局唯一的自增序列。

5.4.1.7 索引

分布式数据库的索引符合下列要求：

a) 应支持索引的创建、删除和修改；
b) 宜支持函数索引；
c) 宜支持分区索引。

5.4.1.8 约束

分布式数据库应支持主键约束（包括单列主键约束和联合主键约束）、唯一性约束、检查约束和非空约束。

5.4.1.9 游标

分布式数据库应支持游标的声明、打开、拨动和关闭。

5.4.1.10 视图

分布式数据库应支持视图的创建、删除和修改。

5.4.1.11 函数

分布式数据库的函数符合下列要求：

a) 应支持数值计算函数、字符处理函数、日期时间值函数、类型转换函数、位运算函数、聚合函数、格式化和系统信息等函数；
b) 应支持自定义函数；
c) 宜支持文本检索函数、XML 函数或 JSON 函数。

5.4.2 扩展对象类型

5.4.2.1 包

分布式数据库宜支持包的创建、删除和修改。

5.4.2.2 触发器

分布式数据库宜支持触发器的创建、删除和修改。

5.4.2.3 外部连接

分布式数据库宜支持外部连接的创建、删除。

注：分布式数据库通过外部连接进行外部访问。

5.4.2.4 作业

分布式数据库宜支持作业的创建、删除和修改。

5.4.2.5 同义词

分布式数据库宜支持对表、视图、序列、函数或存储过程等对象创建同义词，并支持同义词的查看和删除。

5.4.2.6 伪列

分布式数据库宜支持对伪列进行查询。

示例：rowid 或 rownum。

5.4.2.7 临时表

分布式数据库宜支持创建临时表。

5.4.3 基础表分区管理

分布式数据库应提供以下基础表分区方式：

a) 哈希分区，
b) 范围分区，
c) 列表分区。

5.4.4 扩展表分区管理

分布式数据库宜提供以下扩展表分区方式：

a) 二级分区，
b) 间隔分区。

5.4.5 查看信息

5.4.5.1 查看数据库对象

分布式数据库宜支持查看下列数据库对象信息：

a) 数据库，
b) 表，
c) 索引，
d) 字段，
e) 约束，
f) 实例，
g) 表空间。

5.4.5.2 查看日志

分布式数据库应提供查看日志文件的能力。

5.4.5.3 查看系统信息

分布式数据库宜支持查看下列系统信息：

a) 实例数据缓存，
b) 日志缓存，
c) 数据字典。

5.4.6 查看系统表或视图

分布式数据库宜支持查看下列系统表或视图：

a) 会话标识，
b) 进程/线程标识，
c) 用户标识，
d) 最近的用户请求命令，
e) 缺省模式，
f) 登录时间，
g) 会话状态，
h) 等待会话的锁信息，
i) 等待时间统计信息，
j) 使用时间统计信息。

5.4.7 异构数据库联机访问

分布式数据库宜提供异构数据库数据联机访问功能。

5.5 事务能力

5.5.1 事务基础特性

分布式数据库的事务基础特性应符合下列要求：

a) 支持分布式事务的 ACID；
b) 支持多种隔离级别，支持读未提交、读已提交、可串行化和可重复读中两种及以上隔离级别。

5.5.2 死锁检测与处理

分布式数据库的死锁检测与处理应符合下列要求：

a) 在并发执行过程中，检测到死锁并记录；
b) 提供解决全局死锁的机制。

5.5.3 自治事务

分布式数据库宜提供包、存储过程或触发器的自治事务能力，支持自治事务内的语句级回滚。

注：语句级回滚仅回滚发生错误的语句。

5.6 运维和监控

5.6.1 运行时统计信息

5.6.1.1 慢 SQL 统计

分布式数据库应支持统计慢SQL的用户名、数据库名和执行时长。

5.6.1.2 性能状态

分布式数据库的性能状态统计符合下列要求：

a) 应支持统计每秒事务数和查询数；
b) 应支持统计 SQL 平均响应时间；
c) 应支持统计高频 SQL；
d) 宜支持统计集群节点 CPU 使用情况；

e) 宜支持统计集群节点内存使用情况；
f) 宜支持统计集群节点磁盘使用情况；
g) 宜支持统计集群节点网络使用情况。

5.6.2 日志

分布式数据库的日志统计应符合下列要求：
a) 具备对各类事件（如数据库实例、网络通信或数据库对象）进行日志记录的功能。通过日志查看操作内容、执行过程和结果；
b) 具备提示和警告功能，提示和警告数据库结构修改和数据库运行配置修改等重要操作；
c) 日志完整正确，并且提供可读文本的形式；
d) 支持中文日志，如安装状态信息。

5.6.3 远程运维

分布式数据库应具备远程维护功能。

5.6.4 报警

分布式数据库的报警应符合下列要求：
a) 提供通知管理员的方法或工具；
b) 支持设置报警基线，数据库运行中遇到重要事件、异常事件（如资源不足）和状态超过报警阈值等情况时，通知管理员；
c) 提供报警 API；
d) 报警发生时，支持报警信息的实时展示。

5.6.5 SQL 监测与优化建议

分布式数据库宜提供SQL监测与优化建议功能，符合下列要求：
a) 实时监测 SQL 执行过程中资源使用情况；
b) 提供查询计划的缓存管理功能；
c) 提供 SQL 改写的优化建议；
d) 根据系统统计信息，生成新的执行计划。

5.6.6 物理空间

分布式数据库应支持查看数据库的核心文件（如数据文件、临时文件或日志文件等）的空间使用情况（如空间使用率），并提供配置数据库的核心文件的回收策略能力。

5.6.7 数据监控

分布式数据库的数据监控符合下列要求：
a) 应支持特定事件或事务发生时收集监控数据；
b) 应支持跟踪数据库等待事件；
c) 监控数据采集粒度宜达到分钟级或秒级。

5.6.8 归档管理

分布式数据库应支持对归档模式、归档文件位置和归档启用停用进行管理。

5.7 数据迁移

5.7.1 迁移

数据迁移应符合下列要求：

a) 提供元数据、数据库、数据库对象和表数据迁移的功能；
b) 支持数据迁移工具实现同构或多源异构数据库之间的数据迁移；
c) 在数据迁移过程中应具备应对传输异常的能力，保障数据迁移的稳定性、连续性和一致性；
d) 支持存量数据的一次性迁移和增量数据库的持续同步；
e) 迁移前提供迁移评估报告，包括迁移对象等信息；
f) 支持并行数据迁移。

5.7.2 比对

数据比对符合下列要求：

a) 对源数据库和目标数据库之间的数据进行比对，应支持数据一致性，并提供一致性比对报告；
b) 数据比对规模应是可配置的，进行库级和表级等级别的比对；
c) 宜提供数据修复功能；
d) 宜支持增量迁移过程中进行阶段性（如时间粒度等）的数据校验。

5.8 备份恢复

5.8.1 数据备份

数据备份应符合下列要求：

a) 运行状态下支持对数据库进行全库备份；
b) 运行状态下支持对数据库进行部分（如表级）备份；
c) 运行状态下支持对数据库进行增量备份。

5.8.2 备份数据管理

分布式数据库的备份数据管理宜符合下列要求：

a) 支持备份数据的加密，密码要求见 8.1.2；
b) 支持备份数据的压缩；
c) 支持备份数据的存储。

5.8.3 用户或模式备份恢复

分布式数据库用户或模式的备份恢复宜符合下列要求：

a) 支持对数据库的所有或指定用户或模式下的数据进行备份；
b) 支持对数据库的所有或指定用户或模式下的数据备份进行恢复。

5.8.4 多种存储媒体备份和还原

分布式数据库应支持多种备份存储媒体，支持多种存储媒体的部分和完整数据库数据还原处理能力。

5.8.5 备份还原的一致性校验

分布式数据库应提供数据库备份数据一致性校验的命令或工具。

5.8.6 备份转储和恢复

分布式数据库宜支持将备份文件转储，并在另外一个集群进行数据库还原操作。

5.8.7 备份限速

分布式数据库宜提供备份限速功能，通过设置备份最大速率，减少备份过程网络资源占用。

5.9 集群管理

5.9.1 集群构建与管理

分布式数据库的集群构建与管理符合下列要求：

a) 应支持集群的运行环境；
b) 应支持创建并配置数据库集群；
c) 配置信息应包括日常运维管理、容灾管理、日志管理、备份管理和监控等；
d) 在读写操作负载差距较大时，宜提供读写分离能力；
e) 宜支持同一集群在不同 CPU 架构上混合部署。

5.9.2 数据分布

分布式数据库应按照指定规则设置数据分布。

5.9.3 分布式计算

分布式数据库应支持在分布式节点上的并行计算。

5.9.4 集群扩展

分布式数据库的集群扩展应符合下列要求：

a) 支持在线扩容和缩容；
b) 集群扩容和缩容过程中支持分布式事务 ACID 特性。

5.9.5 数据重分布

分布式数据库应支持按照数据库集群的节点、状态和负载的变化，进行重分布。

5.9.6 对应用透明

分布式数据库应支持对应用透明，当数据分布、分布计算、集群扩展和数据重分布等变化时，不需要修改应用代码。

5.9.7 负载均衡

分布式数据库应支持集群环境下的事务并行执行，且各分布式节点上的负载保持均衡。

5.10 工具

5.10.1 数据库开发调试工具

分布式数据库的开发调试工具符合下列要求：

a) 应提供图形化的开发调试工具；
b) 应具备导入、编辑、保存、执行 SQL 语句和 SQL 脚本功能；
c) 应具备关键词显示标记和动态语法提示的 SQL 编辑器功能；
d) 宜提供预编译工具，支持嵌入式 SQL 编程。

5.10.2 运维和监控工具

分布式数据库应提供图形化的运维和监控工具。

5.10.3 数据迁移工具

分布式数据库的数据迁移工具应符合下列要求：

a） 支持不同格式（如 csv 或 txt 等）数据的导入和导出功能；

b） 支持不同级别（如表级、库级或用户级）和不同数据库对象的导入/导出功能。

5.10.4 图形化管理

分布式数据库的图形化管理宜符合下列要求：

a） 使用图形化方式实现数据库的安装与升级，见 5.1；

b） 使用图形化方式实现数据库的数据配置，见 5.2；

c） 使用图形化方式实现数据库的数据库对象，见 5.4；

d） 使用图形化方式实现数据库的备份恢复，见 5.8；

e） 使用图形化方式实现数据库的集群管理，见 5.9。

6 性能

基础软硬件环境符合 SJ/T 11941—2024 和 SJ/T 11936—2024 的要求，TPC 中的 C 类（TPC-C）模型下，生产厂商应给出分布式多节点情况下具体性能值。

7 可靠性

7.1 稳定运行

分布式数据库应支持7×24 h 稳定运行。

7.2 故障切换

在主节点出现故障时，分布式数据库应形成新的主节点，保障业务正常运行。

7.3 容灾能力

7.3.1 多副本策略

分布式数据库应提供多副本策略，支持主副本与从副本之间的数据同步，最低时延由生产厂商提供。

7.3.2 实例容灾

分布式数据库的实例容灾应符合下列要求：

a） 在任意数据库实例出现故障时，集群内服务正常运行，数据不丢失，集群整体业务可用；

b） 在实例故障或节点故障等单数据库实例故障时，RPO 时间等于 0，RTO 时间小于 30 s。

7.3.3 容灾部署

分布式数据库的容灾部署应符合下列要求：

a） 提供远程容灾部署与管理功能；

b） 提供生产中心与备份中心之间的容灾部署与管理功能。

7.3.4 同城容灾

分布式数据库的同城容灾应符合下列要求：

a） 支持同城双中心部署，当主中心故障时，业务切换到备中心；

b) 由于网络或供电等原因造成的可用区级故障，触发集群计划外停机，在同城多可用区场景下，RPO 时间等于 0，RTO 时间小于 1 min。

7.3.5 异地容灾

分布式数据库的异地容灾宜符合下列要求：

a) 城市级故障，比如地震，业务切换到异地；

b) 异地灾备场景支持两地三中心部署架构，在本地建立同城灾备中心，在异地建立异地灾备中心，RPO 时间小于 1 min，RTO 时间小于 10 min。

7.4 容错性

7.4.1 服务端编程稳定性

当用户自定义的存储过程和函数运行异常时，分布式数据库应稳定运行。

7.4.2 网络容错

网络中断时，应保障事务一致性。

7.4.3 检测报警

分布式数据库的检测报警应符合下列要求：

a) 支持数据库实例启动时错误检测能力；

b) 支持加载不同文件格式和大小数据出现错误时的故障检测和处理能力；

c) 支持数据库备份执行过程中发生故障时报错或者报警能力；

d) 支持数据库恢复发生故障时报错或者报警能力。

7.4.4 故障恢复

分布式数据库应支持不同级别（包括事务故障、系统故障和存储媒体故障）的故障可恢复，应符合下列要求：

a) 系统故障重启后能正常运行且支持数据一致性；

b) 提供基于时间点故障恢复功能。

8 安全性

8.1 基本安全

8.1.1 基本要求

分布式数据库应通过安全可靠测评。

8.1.2 密码要求

分布式数据库的密码应符合 GM/T 0028 的相关规定。

8.2 基础安全

8.2.1 安全架构

分布式数据库应将系统管理员分为数据库管理员、数据库安全员和数据库审计员三种类型。

8.2.2 漏洞管理

分布式数据库厂商应建立漏洞管理机制，及时通过邮件或网站等方式将安全漏洞告知用户，并提供

安全补丁对漏洞进行修复。

8.2.3 身份鉴别及访问控制

分布式数据库应支持身份鉴别及访问控制，要求如下：

a) 提供外部鉴别方式；
b) 支持配置访问黑白名单；
c) 支持 SSL 和 TLS。

8.2.4 加解密

分布式数据库的加解密符合下列要求：

a) 应具有加解密能力；
b) 宜支持表级和列级加解密能力。

8.2.5 EAL 要求

在安全审计、用户数据保护、标识和鉴别、安全管理、安全功能保护、资源利用、数据库访问和密码支持等方面应符合 GB/T 20273—2019 中 7.2 的 EAL2 级别的安全要求。

8.3 增强安全

8.3.1 防篡改

分布式数据库的防篡改宜符合下列要求：

a) 支持对指定的表开启防篡改能力，开启后，对重要数据的创建、删除和修改操作，记录篡改校验信息，并提供篡改校验接口；
b) 支持对指定的表开启追溯能力，开启后，对数据的变更具有全向追溯能力，记录数据变更的历史信息以及相应的操作记录。

8.3.2 全密态

分布式数据库的全密态宜符合下列要求：

a) 支持从客户端内存到服务端内存，再到服务端存储媒体全生存周期加密保护；
b) 支持全密态的等值查询能力。

8.3.3 动态脱敏

分布式数据库宜支持数据的动态脱敏。

8.3.4 透明加密

分布式数据库宜支持存储媒体上的数据文件（如库、表或表空间）自动加密，并且对应用透明。

8.3.5 闪回查询

分布式数据库宜支持闪回查询。

8.3.6 闪回恢复

分布式数据库的闪回恢复宜符合下列要求：

a) 支持闪回查询实时恢复数据；
b) 支持不同级别（如库级或表级等）的闪回恢复。

8.3.7 资源限制

分布式数据库的资源限制宜符合下列要求：

a) 支持用户资源限额，设置用户资源（包括 CPU、内存、I/O 和连接数等）使用；

b) 支持 SQL 资源限制。

8.3.8 强制访问控制

分布式数据库宜支持强制访问控制。

9 兼容性

9.1 软件兼容

9.1.1 云化部署

分布式数据库应支持虚拟化部署或容器化部署等云化部署方式。

9.2 硬件兼容

9.2.1 硬件平台兼容

分布式数据库的硬件平台应兼容以下至少三种通过安全可靠测评的 CPU 平台架构：

a) ARM，

b) LoongArch，

c) MIPS，

d) SW64，

e) x86。

9.3 接口兼容

分布式数据库的接口兼容符合下列要求：

a) 应支持 ODBC 和 JDBC 等接口；

b) 宜支持 python 或 GO 等应用开发接口。

10 售后服务

10.1 交付方式

厂商应以光盘、便携式移动设备、镜像文件、在线下载等交付方式提供产品交付物。

10.2 服务周期

分布式数据库的服务周期应符合下列要求：

a) 产品自发布之日起至产品停止功能升级（包含新特性、新硬件支持）之日止不少于 5 年；

b) 产品停止功能升级之日起至产品停止功能维护（主要包括问题修复）之日止不少于 4 年；

c) 产品功能维护停止之日起至产品停止安全维护（包括中高风险漏洞修复）之日止不少于 2 年；

d) 自销售之日起，产品售后服务周期不少于 6 年；

e) 产品说明书中应明确产品发布日期、计划停止升级日期、计划停止服务日期。

10.3 服务保障

分布式数据库的服务保障符合下列要求：

a) 应提供多种形式支持服务，包含电话、电子邮件、远程连接等；
b) 应提供技术支持服务，支持同城 4h、异地 12h 响应要求，两个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案；
c) 应提供培训材料、产品手册、培训视频等培训相关内容；
d) 应建立全国技术服务体系和服务团队，符合专业服务体系标准要求，提供原厂中文服务；
e) 服务周期内应支持版本免费升级；
f) 应提供数据库参数、慢 SQL 语句的性能优化指南，包含性能优化的具体措施、技巧、案例及建议等；
g) 针对关键客户宜提供代码级定制优化服务；
h) 宜提供原厂团队驻场服务；
i) 宜支持在线问题反馈。

参 考 文 献

[1] GB/T 5271.17—2010 信息技术 词汇 第17部分：数据库
[2] GB/T 28821—2012 关系数据管理系统技术要求
[3] JR/T 0044—2008 银行业信息系统灾难恢复管理规范
[4] JR/T 0205—2020 分布式数据库技术金融应用规范 灾难恢复要求

中华人民共和国
电子行业标准

安全可靠　分布式事务型数据库技术要求

SJ/T 11938—2024

*

中国电子技术标准化研究院　编制
中国电子技术标准化研究院　发行

电话：（010）64102612　传真：（010）64102617
地址：北京市安定门东大街1号
邮编：100007
网址：www.cesi.cn

*

开本：880×1230　1/16　印张：1 1/2　字数：9千字

2024年7月第一版　2024年7月第一次印刷
印数：200册　定价：60.00元