ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0204—2020

分布式数据库技术金融应用规范 安全技术要求

Financial application specification of distributed database technology—Security requirements

2020-11-26 发布　　2020-11-26 实施

中国人民银行　发布

目　　次

引　言

随着金融领域分布式架构的转型升级，分布式数据库技术在金融领域应用逐步深入。为规范分布式数据库技术在金融领域应用，强化分布式数据库技术对金融服务的技术支撑，提升分布式数据库技术对业务连续性和信息安全的保障能力，特编制本文件。

本文件是分布式数据库技术金融应用系列标准之一，分布式数据库技术金融应用系列标准包括：

——《分布式数据库技术金融应用规范　技术架构》；

——《分布式数据库技术金融应用规范　安全技术要求》；

——《分布式数据库技术金融应用规范　灾难恢复要求》。

分布式数据库技术金融应用规范 安全技术要求

1 范围

本文件规定了在金融领域分布式事务数据库技术的安全要求，涵盖基础支撑保障、用户管理、访问控制、数据安全、监控预警、密钥管理、安全管理和安全审计等内容。

本文件适用于金融领域分布式事务数据库的研发、测试、评估和应用。

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/T 32633 分布式关系数据库服务接口规范

JR/T 0203 分布式数据库技术金融应用规范 技术架构

3 术语和定义

JR/T 0203界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

DCL：数据控制语言（Data Control Language）

DDL：数据定义语言（Data Definition Language）

DML：数据操纵语言（Data Manipulation Language）

DQL：数据查询语言（Data Query Language）

IO：输入和输出（Input Output）

QPS：查询/秒（Queries Per Second）

SQL：结构化查询语言（Structured Query Language）

TPS：事务数/秒（Transactions Per Second）

5 概述

分布式事务数据库与传统集中式数据库相比，具有服务器横向扩展、计算存储分离、数据分片、多副本技术实现大容量存储、高并发处理、数据高可靠和服务高可用等优势。本文件主要从基础支撑保障、用户管理、访问控制、数据安全、监控预警、密钥管理、安全管理和安全审计等方面提出分布式事务数据库金融应用的安全要求。

本文件将具体条款分为基本要求和增强要求。基本要求是通用、基础的安全要求，分布式事务数据库应全部支持；增强要求是从安全技术的发展趋势和金融用户的前瞻性需求提出的推荐性要求。

分布式事务数据库的安全体系详见图1。

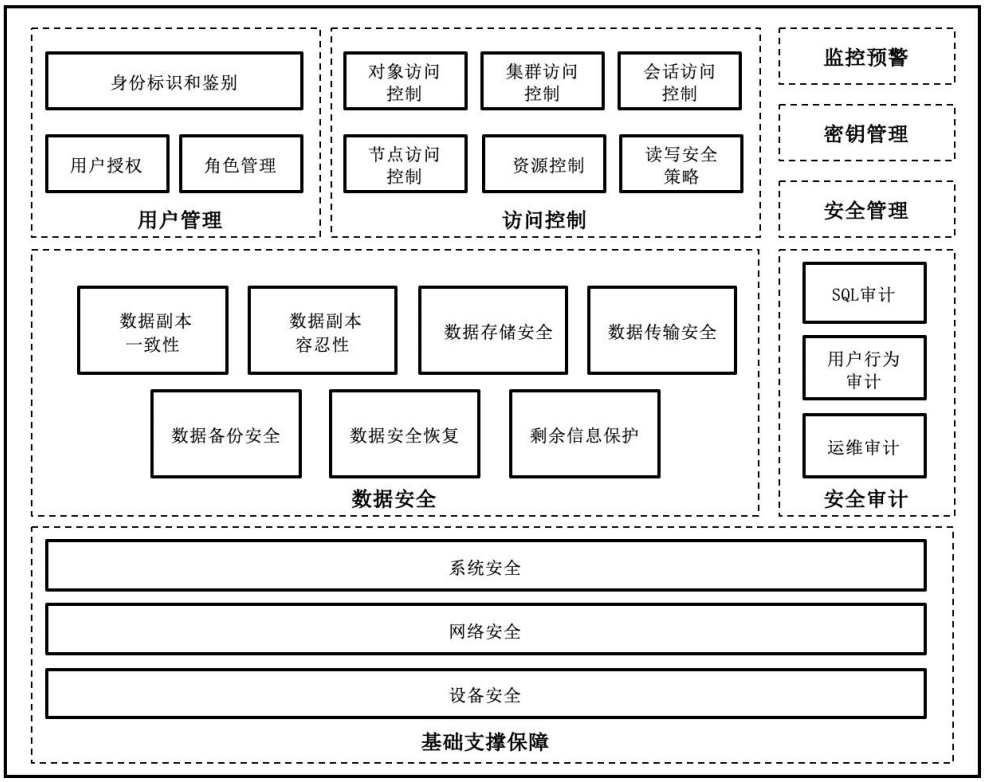

图 1 分布式事务数据库安全体系

6 基础支撑保障

6.1 网络安全要求

基本要求：

a） 应划分不同的网络安全区域，并设置安全隔离级别，分布式事务数据库集群应部署于高安全级别的区域内。

b） 应定期对分布式事务数据库集群所部署的网络域进行安全渗透测试，并修复网络安全漏洞。

增强要求：

a） 宜确保部署的不同数据库集群网络的物理隔离。

b） 宜确保对外提供服务的网络与数据库管理网络间的物理隔离。

6.2 系统安全要求

基本要求：

a） 应根据业务需求和系统安全分析确定系统的访问控制策略。

b） 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。

c） 应定期对分布式事务数据库集群所依赖的底层软件环境进行恶意代码静态检测和行为检测，并及时进行安全补丁包的更新，如：操作系统、虚拟化软件。

d） 应定期对分布式事务数据库集群所依赖的开源组件进行恶意代码静态检测和行为检测，并及时进行安全补丁包的更新。

增强要求：

无。

6.3 设备安全要求

基本要求：

a） 应对关键设备根据高可用需求进行冗余部署。

b） 应对数据存储设备在重用、更换、报废时进行数据的安全清除。

c） 应对密码设备在重用、更换、报废时进行密钥的安全清除。

d） 应对关键的网络设备在重用、更换、报废时进行敏感配置信息的安全清除。

增强要求：

宜确保部署的关键设备的物理专用性。

7 用户管理

7.1 身份标识和鉴别

基本要求：

a） 应支持身份标识（如用户名）具备唯一性，支持通过用户口令进行身份鉴别的功能。

b） 应支持对用户口令复杂度设置、检测及限制使用弱口令的功能。

c） 应支持对用户身份鉴别失败处理的设置、检测及限制登陆的功能。

d） 应支持用户身份鉴别信息（如用户口令）的加密存储。

增强要求：

宜采用 2 种或 2 种以上组合的鉴别技术对管理用户进行身份鉴别。

7.2 用户授权

基本要求：

a） 应支持基于用户的授权方法。

b） 应支持用户的创建、注销及限制登陆功能。

c） 应支持用户的权限添加和撤销功能。

增强要求：

a） 宜支持基于用户组的授权方法。

b） 宜支持用户组的创建、注销及限制登陆功能。

c） 宜支持用户组的权限添加和撤销功能。

d） 宜支持对用户权限的级联传递和回收功能。

7.3 角色管理

基本要求：

a） 应提供不同的数据库管理员角色，以提供职责分离、角色约束等管理功能。

b） 应设立系统管理员、审计管理员、安全管理员等角色，并定义各个角色的职责。

c） 应支持对普通用户权限的限制，其权限不应超过对自身业务数据及数据库对象的管理范围。

增强要求：

a） 系统管理员的权限宜包括对数据库集群的创建、变更、配置和维护等重要操作。

b） 审计管理员的权限宜包括含对各类日志及审记记录的查看、审计记录的导入和导出等操作。

c） 安全管理员的权限宜限于制定、修改、检查安全规则等操作。

d） 宜在系统管理员、审计管理员、安全管理员三个角色基础上提供更细颗粒度的权限，以满足数据库应用方自定义最小化职责分离的需求。

8 访问控制

8.1 对象访问控制

基本要求：

a） 应支持对各类数据库对象（如库表）配置不同的访问权限的功能。

b） 应支持独立的数据库用户管理数据库对象权限，如对象访问权限的授予与回收等。

c） 应支持对库表结构维护权限的控制，如创建、删除、更改库表结构等，库表结构的维护应由其所属用户或相关授权用户来完成。

d） 应支持对库表数据访问权限的控制，库表数据访问权限应包括对某个库表或视图数据的插入、更新、删除、查询的权限，库表数据的访问应由其所属用户或相关授权用户来完成。

增强要求：

a） 宜将库表结构维护的权限仅授予系统管理员。

b） 宜支持限制系统管理员、安全管理员对库表数据的访问功能。

c） 宜支持基于标签的访问控制策略。

8.2 集群访问控制

基本要求：

多个应用共享数据库集群时，应支持多个应用间自有数据库对象的逻辑隔离。

增强要求：

无。

8.3 会话访问控制

基本要求：

应支持基于 IP 地址、端口、数据库、用户和密码的连接认证功能，会话应进行安全隔离。

增强要求：

无。

8.4 节点访问控制

基本要求：

应支持白名单功能，只有白名单列表上的地址才能连接访问。

增强要求：

宜支持用户加源地址白名单功能。

8.5 资源控制

基本要求：

a） 应支持并发控制策略，防止高并发连接影响数据库整体服务质量。

b） 应支持流量分散负载策略，控制流量能够均衡分布到不同的计算节点，避免流量过于集中。

增强要求：

a） 宜支持基于逻辑域划分数据库集群资源的功能。

b） 宜支持资源保护机制，避免因单个连接或会话消耗过高资源而影响可用性。

8.6 读写安全策略

基本要求：

a） 应具备保护措施避免数据在从节点被SQL请求直接更新。

b） 应统一读写入口，避免直接访问数据存储节点。

增强要求：

宜提供读负载权重的控制策略或动态调整读负载的能力。

9 数据安全

9.1 数据副本一致性

基本要求：

应支持指定数量副本的数据在任意情况下都是一致的，其他副本最终完成数据同步。

增强要求：

宜支持所有副本的数据在任意情况下都是一致的。

9.2 数据副本容忍性

基本要求：

a） 应支持当少于总数据副本数量的50%的数据副本故障时，仍能正常对外提供服务。

b） 应支持当大于等于总数据副本数量的50%的数据副本故障时，通过人工干预或其他技术手段，仍能对外提供服务。

c） 应支持副本故障容忍数阈值告警，且告警阈值可设置。

d） 应支持设定副本故障容忍数阈值，并在副本故障容忍数阈值范围内，发生网络异常或部分节点故障情况时，保证数据不丢失。

e） 应支持当故障副本数量恢复到可靠性水平后，分布式事务数据库能自动恢复读写服务。

增强要求：

无。

9.3 数据存储安全

基本要求：

a） 应采用加密技术或其他保护措施实现鉴别信息保密性。

b） 应根据国家与行业主管部门相关规定加密存储敏感数据。

c） 应支持采用密码算法技术对数据表进行加密。

d） 应支持采用密码算法的方式对字段进行加密。

e） 应支持采用密码算法技术对数据库进行整库加密。

增强要求：

无。

9.4 数据传输安全

基本要求：

a) 应采用技术措施保证敏感数据和个人信息传输的保密性。

b) 应能够检测到数据在传输过程中完整性是否受到破坏。

增强要求：

无。

9.5 数据备份安全

基本要求：

a） 应支持数据备份的存储位置可选，包括但不限于本地备份、同城容灾中心、异地容灾中心等。

b） 应支持采用密码算法技术，保证备份文件、导出文件的数据完整性与保密性。

增强要求：

a） 宜支持多重层级数据备份，包括但不限于库级、表级、集群级、用户级等。

b） 运维接口宜与外部业务接口、内部集群数据接口进行隔离。

9.6 数据安全恢复

基本要求：

a） 在数据恢复时，应保证恢复到备份时刻状态。

b） 在数据恢复时，应保证恢复到数据全局一致状态。

c） 应支持将数据恢复到具备恢复条件时间段内任意时刻的能力。

增强要求：

a） 宜支持表级别数据快速恢复的能力。

b） 宜支持库级别数据快速恢复的能力。

9.7 剩余信息保护

基本要求：

a） 应支持在集群扩缩容和重分布过程中因物理存储介质变更产生的剩余信息进行自动清理。

b） 应支持在数据迁移、数据导入导出过程中，对产生的中间数据进行检查和清理。

增强要求：

无。

10 监控预警

基本要求：

a） 应具备对数据库进程的健康状态进行监控的功能，保证及时发现异常状态并进行告警。

b） 应具备对数据库集群整体、各物理服务器节点的健康状态进行集中监控的功能，关键指标包括但不限于：

——CPU 使用率；

——内存使用率；

——磁盘空间使用率；

——IO 统计；

——网络带宽使用率；
——数据库集群状态；
——TPS 和 QPS 统计；
——SQL 平均响应时间统计；
——慢 SQL 统计；
——锁，等待事件；
——数据库会话连接监控。

c） 应提供告警API接口功能。

增强要求：

a） 宜支持集中的图形化管理界面，具体要求如下：
——能够从系统层、数据库层、用户层对集群状态、节点状态、数据库运行状态、多副本数据同步状态等关键信息进行监控告警；
——能够按照重要程度、触发阈值、接受对象等进行分类设置，出现异常时自动显示告警。

b） 宜支持集中监控并识别异常数据库访问，并能及时预警。

c） 宜支持集中的日志查询接口及集中的异常告警接口。

11 密钥管理

基本要求：

a） 应保证密钥的安全存储和管理。

b） 应使用经国家密码管理部门认可的商用密码产品。

c） 应保证密钥长度符合国家密码管理部门及行业主管部门要求。

d） 应支持数据加解密和密钥管理，数据加解密、数字签名等技术应符合国家密码管理部门及行业主管部门要求。

增强要求：

a） 宜支持安全硬件对数据库管理员的鉴别信息进行加密存储。

b） 宜提供密钥功能接口以供应用实现密钥全生命周期的统一管理。

c） 宜提供适配方案以支持多种硬件加密模块。

12 安全管理

12.1 岗位配置

基本要求：

a） 应设立安全管理的职能部门，设立安全主管、安全分管负责人岗位，定义部门及负责人职责。

b） 应设立数据库管理员、数据库安全管理员、数据库审计员等工作岗位。

c） 应成立信息安全工作指导委员会或领导小组，最高领导由单位主管领导委任或授权。

增强要求：

a） 数据库管理员、数据库安全管理员、数据库审计员不宜兼任。

b） 关键事务岗位宜配备多人共同管理。

c） 宜审查管理员资质。

12.2 风险管理

基本要求：

a） 应采取必要的措施识别安全风险，对发现的安全风险进行评估，并及时修补。

b） 应定期开展安全测评，形成安全测评报告，并对发现的安全问题采取应对措施。

c） 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份情况等。

d） 应在发生重大变更时开展全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

增强要求：

a） 宜定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

b） 宜制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，并将安全检查结果告知相关方。

12.3 应急响应

基本要求：

a） 应按照国家和行业主管部门要求制定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。

b） 应制定重要安全事件的应急预案，包括应急处理流程、恢复流程等内容。

c） 应定期对系统相关的人员进行安全事件的应急预案培训，并进行应急预案的演练。

d） 应根据业务系统重要程度开展安全事件的应急演练。

增强要求：

宜定期评估相关安全事件的应急预案并进行修订完善。

12.4 变更管理

基本要求：

a） 应在变更前明确变更需求、制定变更方案，并经过审批后方可实施。

b） 应在变更前制定回退方案并充分评估。

c） 应建立变更申请和审批流程，记录变更实施过程。

d） 应明确审批人、实施者的职责和变更流程。

增强要求：

a） 宜根据业务系统重要程度对变更过程进行演练。

b） 宜建立变更的中止、暂停、恢复环节。

13 安全审计

13.1 SQL 审计

基本要求：

a） 应支持对DDL、DML、DQL、DCL操作进行审计，并至少支持对象审计和语句审计2种模式。

b） 审计记录应至少包括以下要素：

——事件的日期和时间；

——事件类型；

——主体身份；

——操作的 SQL 语句；

——事件结果（成功或失败）等。

增强要求：

无。

13.2 用户行为审计

13.2.1 用户创建删除操作审计

基本要求：

a） 应支持对用户创建删除操作进行审计。

b） 审计记录应至少包括以下要素：

——事件的日期；

——事件描述；

——事件类型（如用户权限变更、密码变更）；

——主体（如安全管理用户名）；

——客体（被创建的用户）；

——事件结果。

c） 审计日志中应记录完成该操作的用户名信息，但不应记录密码的明文信息。

增强要求：

无。

13.2.2 用户授权审计

基本要求：

a） 应支持对用户授权操作进行审计。

b） 审计记录应至少包括以下要素：

——授权用户；

——被授权用户；

——授予权限信息；

——操作时间；

——操作命令等。

增强要求：

无。

13.2.3 登入登出审计

基本要求：

a） 应支持对用户在数据库的登入登出操作进行审计。

b） 审计记录应至少包括以下要素：

——登录用户标识；

——会话标识；

——请求地址；

——登入登出时间戳等。

增强要求：

无。

13.3 运维审计

13.3.1 服务启停审计

基本要求：

a） 应支持对服务启停操作进行审计。

b） 审计记录应至少包括以下要素：

——操作人信息；

——操作时间；

——执行命令等。

增强要求：

无。

13.3.2 扩缩容审计

基本要求：

a） 应支持对数据库集群扩容、缩容操作进行审计。

b） 审计记录应至少包括以下要素：

——操作人信息；

——操作时间；

——操作命令等。

增强要求：

无。

13.3.3 备份恢复审计

基本要求：

a） 应支持对备份恢复操作进行审计。

b） 审计记录应至少包括以下要素：

——操作人信息；

——操作时间；

——备份或恢复的库、表、备份文件信息等。

增强要求：

无。

13.4 审计记录安全

基本要求：

a） 应保证审计记录的存储安全，对存储的审计记录进行保护和定期备份，避免受到未预期的删除、修改或覆盖等。

b） 应保证审计记录的留存时间符合相关法律法规要求。

增强要求：

宜支持审计报告的自动生成和导出，用于审查和风险管理。

参 考 文 献

[1] GB/T 20273—2016 《信息安全技术 数据库管理系统安全技术要求》