ICS 03.060
CCS A11

团　　体　　标　　准

T/SZSSA 0006-2023

证券公司重要信息系统数据库管理标准

Standard for Database Management of Important Information Systems in Securities Companies

2023-12-18 发布　　2023-12-18 实施

深圳市证券业协会　　发　布

目　次

前　言

本文件按照 GB/T1.1-2020 《标准化工作导则 第一部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件中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。

本标准主要起草单位：深圳市证券业协会、深圳资本市场金融科技委员会、中信证券股份有限公司、中国中金财富证券有限公司、长城证券股份有限公司、五矿证券有限公司、第一创业证券股份有限公司、东亚前海证券有限责任公司、世纪证券有限责任公司、中山证券有限责任公司、华鑫证券有限责任公司。

本标准主要起草人：张植斌、林国峰、谷明泽、方兴、骆毅、刘殿兴、郭旭瑞、陈辉华、谢碧松、戴先宇、蔡坤、刘伟、郭臣义、李翔、徐楠、肖志武、叶龙贤、张欣磊、刘耀东、薛海波、张俊跃、甘照、胡超、黄华艺、姚刚、赵茂军、高丽峰，关为、黄俊、张林方。

1 范围

本文件给出了证券公司重要信息系统数据库管理的程序和措施，以加强重要信息系统数据库相关的计划、实施、监控等管理活动，保障数据库系统稳定高效运行。

本文件所指重要信息系统参考《证券基金经营机构信息技术管理办法》重要信息系统定义。

本文件适用于证券公司重要信息系统数据库的管理。

2 引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

《证券基金经营机构信息技术管理办法》（中国证券监督管理委员会令 第179号 附件一）

《证券期货业网络和信息安全管理办法》（中国证券监督管理委员会令 第218号）

JR/T 0059—2010 证券期货经营机构信息系统备份能力标准

JR/T 0099—2012 证券期货业信息系统运维管理规范

如相关办法进行了修订或废止，应以其最新版本为准。

3 术语和定义

3.1 重要信息系统 important information system

支持证券基金经营机构和证券基金专项业务服务机构关键业务功能、如出现异常将对证券期货市场和投资者产生重大影响的信息系统。包括集中交易系统、投资交易系统、金融产品销售系统、估值核算系统、投资监督系统、份额登记系统、第三方存管系统、融资融券业务系统、网上交易系统、电话委托系统、移动终端交易系统、法人清算系统、具备开户交易或者客户资料修改功能的门户网站、承载投资咨询业务的系统、存放承销保荐业务工作底稿相关数据的系统、专业即时通信软件以及与上述信息系统具备类似功能的信息系统。

3.2 实时信息系统 real-time information system

对业务连续运行要求很高的信息系统。这类系统短暂停顿或性能指标严重下降，将对证券期货市场造成较大的影响或者损害到投资者及市场其他参与方的合法权益，如交易类、行情类和通信类信息系统（《JRT 0059-2010 证券期货经营机构信息系统备份能力标准》术语和定义）。典型的实时信息系统包括：集中交易系统、投资交易系统、金融产品销售系统、第三方存管系统、融资融券业务系统、网上交易系统、电话委托系统、移动终端交易系统等交易类系统等。

3.3 非实时信息系统 non-real-time information system

对业务连续运行要求不高的信息系统。这类系统短暂停顿或性能指标严重下降，不会对证券期货市场造成较大的影响或者损害到投资者及市场其他参与方的合法权益，如结算类、业务类、风控类、网站类信息系统（《JRT 0059-2010 证券期货经营机构信息系统备份能力标准》术语和定义）。典型的非实时信息系统包括：估值核算系统、投资监督系统、份额登记系统、法人清算系统、具备开户交易或者客户资料修改功能的门户网站、承载投资咨询业务的系统、存放承销保荐业务工作底稿相关数据的系统、专业即时通信软件等估值、清算和即时通信系统以及与上述信息系统具备类似功能的信息系统。

3.4 恢复时间目标 recovery time objective (RTO)

从故障系统切换到备份系统所需的时间。（《JRT 0059-2010 证券期货经营机构信息系统备份能力标准》术语和定义）

3.5 恢复点目标 recovery point objective (RPO)

信息系统和数据必须恢复到的时间点要求。（《JRT 0059-2010 证券期货经营机构信息系统备份能力标准》术语和定义）。

4 故障应对能力与高可用架构

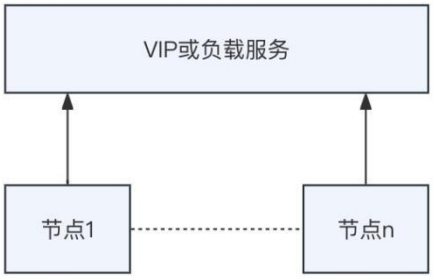
4.1 故障应对能力要求

在不同类型的故障场景下，具体需要达到的故障应对能力要求见表格。对于重要信息系统而言，必须采用高可用架构管理。比较常见的高可用架构和对应的容灾保障能力，可参考 4.2 章节，各证券公司可以根据自身需求选择适合自己的技术方案。

	软硬件单点故障		数据库集群故障		单机房故障		城市级机房故障（可选）	
故障应对能力	RTO	RPO	RTO	RPO	RTO	RPO	RTO	RPO
实时信息系统	<1 分钟	<30 秒	<10 分钟	<30 秒	<20 分钟	<1 分钟	<30 分钟	<2 分钟
非实时信息系统	<5 分钟	<1 分钟	<20 分钟	<5 分钟	<30 分钟	<10 分钟	<1 小时	<20 分钟

4.2 主流高可用架构及能力要求

4.2.1 多活集群架构



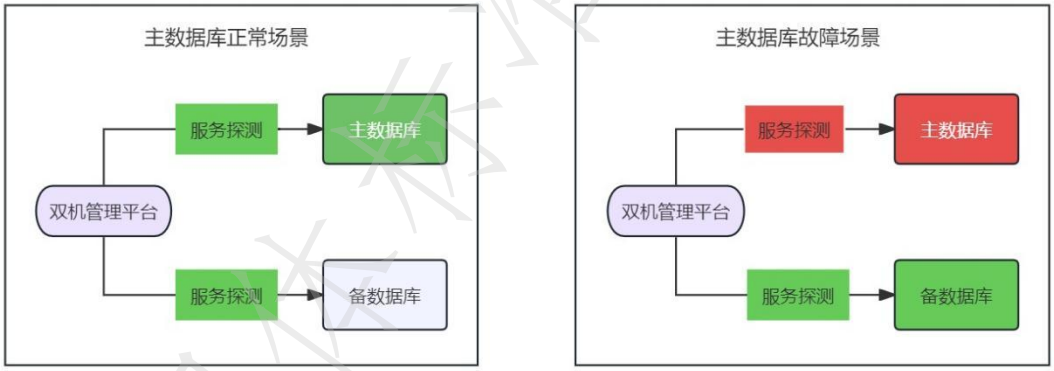
4.2.1.1 不同数据库多活架构不同，ORACLE 的 RAC 集群、MySQL 的 MySQL Group Replication 集群架构等。

4.2.1.2 通过 VIP 或负载方式提供服务，当某个数据库节点故障后，服务 IP 不变，master 节点能实现快速切换。

4.2.1.3 多活集群架构需要达到的故障应对能力为：实时信息系统、非实时信息系统 RTO 小于 1 分钟，RPO 为 0，但多数情况下仅限于在同一机房内实现该能力。为实现机房级的高可用，往往还需搭配存储或主备数据库复制技术，RTO 通常小于 10 分钟，RPO 通常小于 5 分钟。

4.2.1.4 近年来涌现出一系列基于 Paxos/Raft 等共识协议实现的多副本强一致的数据库产品，特别适合于金融行业对于 RTO & RPO 方面比较高的要求，且已经有相应的同城容灾甚至三地五中心异地容灾的实际案例。这些数据库产品往往能达到 RPO=0，RTO<1 分钟的能力，证券公司可以酌情选择。

4.2.2 双机冷备架构



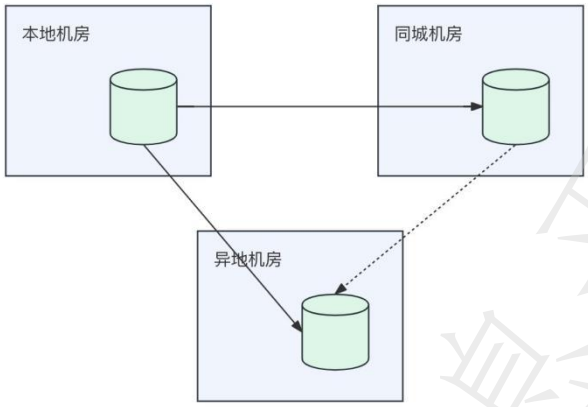
4.2.2.1 双机冷备架构需要有可靠的双机管理软件或平台，主备数据库分别部署在两个服务器上，当主数据库无法提供服务时，双机管理平台将备用数据库的服务拉起。

4.2.2.2 主备数据库的数据文件是共用的，需存放在共享文件系统（如 NFS）上，或共用外置存储磁盘。

4.2.2.3 数据库的配置文件如果存放在服务器本地磁盘，需要用实时同步工具进行同步，以保证备用数据库能正常启动并提供服务。

4.2.2.4 双机冷备架构需要达到的故障应对能力为：实时信息系统 RTO 小于 15 分钟，RPO 小于 1 分钟；非实时信息系统 RTO 小于 1 小时，RPO 小于 5 分钟。

4.2.3 容灾架构



4.2.3.1 容灾能力包括同城容灾和异地容灾，对于实时信息系统，通常需要部署两地三中心架构（既有同城容灾，也有异地容灾）。同城主中心、容灾中心之间物理距离建议大于 10 公里，小于 100 公里，异地容灾中心建议跨城市或省份。

4.2.3.2 同城容灾架构的数据库，通常需要实现主备数据库实时同步。每套系统在主中心需要部署 2 个及以上数据库实例，同城容灾中心需要部署 1 个及以上数据库实例。主备同步需采用多数副本落盘算法，确保每笔数据至少落盘 2 个副本。

4.2.3.3 异地容灾架构由于网络带宽的限制，恢复时长较久，建议应先建立同城容灾架构，在具备同城容灾架构的前提下再建立异地容灾。

4.3 数据库高可用切换演练

大规模分布式系统往往包含复杂的交互和依赖，潜在可能存在风险以及级联风险的地方很多，任何一个内部异常处理机制存在缺陷就有可能导致出现严重业务异常，或者其他种种无法预料的异常行为。当下不能完全避免这些故障的发生，所以需要能够尽早地识别出系统中脆弱的、易出故障的环节，同时有针对性地进行加固、防范，数据库自然是其中很重要的一环。

4.3.1 数据库高可用切换演练主要是为了验证其高可用架构的有效性，以及高可用灾难恢复预案的完整性和有效性，提高预案的执行能力和效率，确保各参与方在灾难发生时的有效协同，以及业务系统的快速恢复，应至少每年进行 1 次相关预案的切换演练。

4.3.2 对于切换演练，需要形成容灾演练报告，并总结演练中发现的问题，同时针对发现的问题进行分析，形成改进方案，并在生产环境中进行修复。最终通过再一次的切换演练，验证并确认问题修复，形成闭环。演练报告应至少保存 5 年。

4.3.3 切换演练需要覆盖 4.1 章节提到的软硬件单点故障、数据库集群故障、单机房网络故障等场景。

4.3.4 建议与鼓励各证券公司以数据库服务质量目标为基础，建设数据库可用性度量体系，结合混沌工程故障注入能力，通过更高的演练频次、更细致的演练场景、更加常态化与随机性的演练机制，打造更完善的数据库高可用能力回归体系。

5 运维管理

5.1 监控分析

5.1.1 证券公司应采取监控措施，配备监控和报警工具，对数据库系统进行 7×24 小时监控。报警方式可包括声光、电话、短信、邮件、企业微信等。

5.1.2 主要监控指标有：

a) 主机设备运行状态、中央处理器使用率、内存利用率、磁盘空间利用率、通信端口状态等；

b) 数据库日志信息、表空间使用率、连接数、锁等待、数据同步状态、备份状态等；

c) 数据库、表、索引、存储过程状态；

d) 监控性能瓶颈 SQL 语句

指标类型	监控指标	指标说明
主机	主机设备运行状态	数据库主机设备可用性
	处理器使用率	采集主机 CPU 利用率，应当包含 sys、wait 等
	内存利用率	内存利用率应当包含 buffer、swap 等
	空间利用率	各挂载点磁盘空间利用率
	通信端口状态	主机网络、SAN 端口状态速率等信息
数据库可用性	数据库日志信息	包括数据库和集群的告警日志采集
	表空间使用率	数据库逻辑空间使用率（如不存在逻辑空间可不做监控）
	数据库同步状态	数据库备库的同步状态、同步延时等信息

指标类型	监控指标	指标说明
	备份状态	数据库当日各类备份完成情况
	无效对象	数据库、表、索引、存储过程等可用状态
	安全性	数据库访问控制、漏洞、稳定性等状态
数据库性能监控	性能瓶颈 SQL 语句	TOP SQL、慢 SQL 等性能瓶颈 SQL 监控，应当包括执行 SQL 的主机信息、执行时间、耗时和次数、执行时扫描行数或逻辑读数、锁或等待耗时、执行计划及变动信息
	连接数	会话、进程、连接数等数量和活动状态信息
	数据库内存信息	包括各类数据库内存区域当前使用状态
	数据库活动时间	DB TIME、CPU TIME、等待时间等数据库活动时间统计
	阻塞会话和锁状态	阻塞和被阻塞会话、锁持有和锁等待会话信息

5.1.3 正确设置自动化监控工具的预警阈值，并定期进行检查和评估。

5.1.4 除自动化监控工具以外，对核心交易业务系统数据库应辅以人工巡检制度，巡检结果应及时记录，如遇异常应及时处理，并按规定要求进行报告。

5.1.5 应每日分析监控日志和巡检记录，跟踪处理日志分析中发现的异常事件。对监控机制执行效果进行定期检查评估并持续优化。

5.1.6 重要系统上线前通过压力测试等手段，对数据库进行调优，建立基准参数配置，记录性能基线。

5.1.7 上线后应加强性能监控，并定期进行数据库运行分析，根据实际运行状况，进行动态优化调整，编制调优文档并保持更新。

5.1.8 监控日志保存周期与对应系统的数据备份保留周期一致。

5.2 升级变更

5.2.1 应采用经应用系统测试验证通过的安全稳定的数据库版本。

5.2.2 版本控制满足安全需求，定期跟踪数据库厂商发布的安全预警和缺陷修正，确认是否受到同样问题的影响，数据库重大缺陷必须及时修复、更新软件，以保持数据库的可用性。

5.2.3 数据库升级操作参照变更管理标准执行，做好备份与测试，提交变更流程并审批通过后方可实施，并且须双人复核。针对不同风险的操作划分低/中/高风险级别，并匹配不同的审批流程，越高的风险级别，根据其可能带来的影响程度，匹配越严格的审批流程，并对变更内容与审批过程进行留痕，保留时间≥3 年。

5.2.4 在变更之前应检查确认连接的环境正确，如正确的主机、正确的实例、正确的路径，等等。禁止层层跳转的服务器登录方式，避免打开过多的窗口导致操作错误，并且完成变更或运维操作后应退出登录。

5.2.5 在业务繁忙时段禁止进行 DDL 操作、慎重进行统计信息收集和创建索引操作。

5.2.6 建议构建仿真测试环境，与生产环境的平台架构保持一致，升级变更操作先在仿真环境做 1 轮以上的数据库全要素验证。构建仿真测试环境时，要充分考虑数据的敏感性，通过工具或平台保证敏感数据的安全，避免敏感信息泄漏。

5.2.7 变更过程应实时观察业务监控指标或者通过业务全流程回归验证，确保变更不造成预期外的系统/业务异常；如出现预期外异常，需要对变更操作快速回滚。

5.3 数据归档

5.3.1 根据数据归档的适用范围，数据库按时间划分成：当前库、历史库、归档库。需要考虑到实际业务需求和数据特点，以确保数据库的性能和可靠性。同时，还需要根据实际情况进行优化和调整，以达到最佳的性能和效率。

5.3.2 建立数据归档机制，对当前库数据应根据数据访问需求定期归档，以减小当前库数据量大小，提升访问性能和减小数据备份压力。

a) 编写脚本：根据实际需求，编写数据归档脚本，包括归档和备份脚本。脚本需要考虑到分区表的分区类型、分区键、分区数等因素，以确保脚本的正确性和可靠性。

b) 执行脚本：按照计划，定期执行脚本，进行数据归档和备份。在执行脚本之前，需要进行必要的备份和测试，以确保操作的安全性和正确性。

c) 监控和优化：定期监控数据库的运行情况和脚本执行情况，根据实际情况进行优化和调整，以提高数据库性能和保证数据安全。

需要注意的是，数据归档需要根据实际情况进行定期操作，以保证数据库的正常运行和数据的安全性。同时，还需要考虑到数据的性能和可靠性，以确保操作的正确性和有效性。

5.4 数据存储

5.4.1 数据和日志以及应用分开存储，单独规划分盘，数据盘应保证扩展性，使用存储设备划盘，或可扩展磁盘槽位能够满足数据库 3 年的数据增长量。

5.4.2 定期对数据库存储容量进行检查和评估，形成评估报告。

5.4.3 分析数据增长趋势，确保可用存储空间至少可满足数据库 120 天的数据增长量，为存储扩容预留充足的时间窗口。

6 安全管理

6.1 权限控制

6.1.1 账户分类

a) 应用用户，又分为业务系统用户和采集查询用户。

b) 审计用户，不应当包括修改权限。

c) 业务运维用户，实名制。

d) 数据库管理员，实名制。

e) 数据库各类用户应进行隔离，操作员访问数据库应使用不同于应用用户的用户，不同操作员应设置专有的用户。

6.1.2 最小化权限原则

a) 用户权限应在满足需求的基础上按照最小化权限原则进行设置，只赋予用户完成任务所需的最小权限，避免分配不必要的权限。

b) 数据库管理员权限不应分配给除了数据库管理员以外的其他人员，禁止使用系统管理员帐号和操作员用户帐号进行业务操作。

6.1.3 在数据库系统上线前，应修改数据库系统默认密码，并对不需要的账户进行删除或锁定。

6.1.4 定期检查数据库的用户、口令及权限设置的正确性。应在用户账户变化时，同时变更或撤销其权限。对于不再使用的账户，应及时注销。注销账号之前建议先做好数据备份，锁定用户一个业务周期后（建议不少于 7 天）再注销删除。

6.1.5 不同的数据库系统应使用不同的密码，并且测试环境和生产环境不得使用相同的密码。

6.2 审计

6.2.1 重要信息系统数据库应当通过旁路审计方式的数据库审计系统进行审计。

6.2.2 数据库审计日志建议保留 5 年。

6.2.3 审计要素应当包括时间、客户端 IP、客户端端口、服务端 IP、服务端端口、数据库账号、资产信息、数据库实例、客户端工具、数据库类型、主机名、执行时长、操作类型等。

6.2.4 应当纳入审计的风险场景包括安全规则、SQL 注入、黑名单语句、违反授权策略等 SQL 行为。对风险事件应当及时通过多种渠道告警。