ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0205—2020

分布式数据库技术金融应用规范 灾难恢复要求

Financial application specification of distributed database technology—Disaster recovery 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　灾难恢复要求

1　范围

本文件规定了金融领域分布式事务数据库的灾难恢复要求，涵盖容灾能力分级、灾备技术要求和灾备管理流程。

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、应用、运维和管理。

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 20988—2007　信息安全技术　信息系统灾难恢复规范

GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南

GB/T 30146—2013　公共安全　业务连续性管理体系要求

JR/T 0044—2008　银行业信息系统灾难恢复管理规范

JR/T 0203—2020　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—2020界定的以及下列的术语和定义适用于本文件。

3.1

灾难　disaster

由于人为或自然的原因，造成信息系统严重故障、瘫痪或其数据严重受损，使信息系统支持的业务功能停顿或服务水平达到不可接受的程度，并持续特定时间的突发性事件。

[来源：JR/T 0044—2008，3.2]

3.2

灾难恢复　disaster recovery

为了将信息系统从灾难造成的不可运行状态或不可接受状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受的状态而设计的活动和流程。

[来源：JR/T 0044—2008，3.3]

3.3

灾难恢复能力　disaster recovery capability

在灾难发生后利用灾难恢复资源和灾难恢复预案及时恢复和继续运作的能力。

3.4

灾难恢复预案 disaster recovery plan

定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。

注：用于指导相关人员在预定的灾难恢复目标内恢复信息系统支撑的关键业务功能。

[来源：JR/T 0044—2008，3.14]

3.5

风险分析 risk analysis

确定影响信息系统正常运行的风险，评估对单位业务运营至关重要的功能，定义降低潜在危险控制手段的流程。

注：风险分析经常涉及对特殊事件发生可能性的评估。

[来源：JR/T 0044—2008，3.6]

3.6

业务影响分析 business impact analysis

分析业务功能及其相关信息系统资源，评估特定灾难对各业务功能的影响，确定信息系统可接受的RTO和RPO目标。

[来源：JR/T 0044—2008，3.7]

3.7

业务连续性 business continuity

在中断事件发生后，组织在预先确定的可接受的水平上连续交付产品或提供服务的能力。

[来源：GB/T 30146—2013，3.3]

3.8

恢复时间目标 recovery time objective；RTO

灾难发生后，信息系统从停顿到必须恢复的时间要求。

[来源：JR/T 0044—2008，3.17]

3.9

恢复点目标 recovery point objective；RPO

灾难发生后，数据必须恢复到的时间点要求。

[来源：JR/T 0044—2008，3.18]

3.10

系统可用性 system availability

在要求的外部资源得到保证的前提下，分布式事务数据库在规定的条件下和规定的时刻或时间区间内（不包括计划内服务中断时间）处于可执行规定功能状态的能力。

注：一般按允许计划外年服务中断时间、可用程度至少达到“n个九”来衡量。

3.11

生产系统 production system

正常情况下支持单位生产运行的信息系统。包括主数据、主数据处理系统和主网络。
[来源：JR/T 0044—2008，3.9]

3.12

生产中心 production center

生产系统所在的数据中心。
[来源：JR/T 0044—2008，3.10]

3.13

同城数据中心 data center in the same city

能够抵御因供电供水中断、水淹、火灾、网络故障、硬件损毁、交通中断等灾难同时影响的数据中心。

注：一般情况下与生产中心距离为数十公里以内。

3.14

异地数据中心 data center in the different city

能够抵御因战争、洪水、海啸、台风、地震等大范围区域性灾害同时影响的数据中心。

注：一般情况下与生产中心距离为数百公里以上。

3.15

演练 exercise

基于灾难恢复预案进行的演习。

注：形式包括桌面演练、模拟演练、实战演练等。

4 缩略语

下列符号和缩略语适用于本文件。

RPO：恢复点目标（Recovery Point Objective）

RTO：恢复时间目标（Recovery Time Objective）

5 概述

近年来，分布式事务数据库技术在金融领域应用不断深入，深刻影响和变革了金融机构的技术架构、服务模式和业务流程，也给灾难恢复带来了新的挑战。分布式事务数据库在灾难恢复的影响评估、关键指标、技术要求和组织管理等方面与传统架构存在诸多差异，应重点关注并妥善应对。为了保障应用业务连续性，确保数据的可靠性达到管理规范要求，应评估具体业务在故障或灾难发生时可能造成的影响。根据不同灾难恢复等级，确定灾难恢复目标，设计和实施对应的检测机制和恢复手段。

6 容灾能力分级

6.1 风险与业务影响分析

金融机构应根据业务连续性目标和业务发展规划，对分布式事务数据库进行详细的风险分析。在风险分析过程中，应根据不同的业务场景，重点界定风险分析的目标和范围，使用恰当的分析方法，对所面临的威胁进行深入剖析，评估各类风险发生的概率和可能导致的损失。

在金融领域分布式事务数据库应用场景中，风险分析应重点关注使用分布式事务数据库技术可能引发的新风险、威胁、脆弱性和损害，包括但不限于以下方面：

a) 无法预知的区域局部性灾难，如生产中心所在的楼宇发生火灾、爆炸、全部楼宇停电、通信瘫痪等。
b) 严重的台风、地震、洪水等自然灾害。
c) 访问控制不当可能导致的信息泄露。
d) 系统人员误操作造成意外宕机或关键数据丢失。
e) 硬件设备、网络等性能瓶颈可能导致的系统中断。
f) 手段频多的黑客攻击、病毒入侵、垃圾邮件、网络与系统的漏洞而造成安全隐患。
g) 系统故障、升级等可能导致的问题群发。
h) 适应金融行业与政府的标准法规不断变化。

经过严谨的风险分析之后，应对风险可能造成的业务影响进行研判。在金融领域分布式事务数据库使用场景下，对业务影响进行分析时，首先需要根据监管要求、业务性质、业务服务范围、数据集中程度、业务时间敏感性、功能关联性等要素进行业务功能分析，并在此基础上评估业务中断可能造成的影响，确定灾难恢复目标及恢复优先级。

在金融领域分布式事务数据库应用场景中，业务影响分析应关注的内容包括但不限于以下方面：

a) 以量化的方法，评估业务功能中断可能造成的直接经济损失或间接经济损失，主要包括：
   ——直接经济损失：
   - 资产损失；
   - 收入损失；
   - 额外费用增加；
   - 财务处罚。

   ——间接经济损失：
   - 预期收益损失；
   - 商业机会损失；
   - 市场份额影响。

b) 以非量化的方法，评估业务功能中断可能造成的影响，主要包括：
   ——社会影响。
   ——法律影响。
   ——信用影响。
   ——品牌影响。

6.2 容灾能力级别划分

根据GB/T 20988—2007、 GB/T 22240—2008、 JR/T 0044—2008的相关要求，按照所承载的业务系统发生故障或瘫痪的影响范围、危害程度等对分布式事务数据库容灾能力要求进行划分。

结合金融领域特性，将分布式事务数据库发生故障或瘫痪的影响范围分为4个层级：

a） 内部辅助管理：未对金融机构经济效益、社会声誉产生直接影响的内部管理事项。
b） 内部运营管理：对金融机构经济效益、社会声誉产生直接影响的内部管理事项。
c） 公民、法人和其他组织的金融权益，包括：
——公民、法人和其他组织的财产安全权、知情权、公平交易权、依法求偿权、信息安全权。
——其他影响公民、法人和其他组织的金融权益的事项。
d） 国家金融稳定、金融秩序，包括：
——国家对外活动中的经济金融利益。
——国家金融政策的制定与执行。
——国家金融风险的防范。
——国家金融管理活动。
——多数关键金融机构、金融市场及其基础设施的稳定运行。
——其他影响国家金融稳定、金融秩序的事项。

将分布式事务数据库发生故障或瘫痪的危害程度划分为3类：

a） 较小影响：指的是工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题、较低的财产损失等。
b） 一般影响：指的是工作职能受到一般影响，业务能力显著下降且影响主要功能的执行，引发一般的法律问题、较高的财产损失等。
c） 严重影响：指的是工作职能受到严重影响或丧失行使能力，业务能力严重下降或功能无法执行，出现严重的法律问题等。

根据应用于金融领域的分布式事务数据库的业务系统的重要程度和发生故障或瘫痪的影响范围、危害程度，将其容灾能力等级划分为6级，具体见表1。

表 1　应用于金融领域分布式事务数据库容灾能力等级要求划分

影响范围	危害程度		
	较小影响	一般影响	严重影响
内部辅助管理	第1级	第2级	第3级
内部运营管理	第2级	第3级	第4级
公民、法人和其他组织的金融权益	第3级	第4级	第5级
国家金融稳定、金融秩序	第4级	第5级	第6级

6.3　关键指标

应用于金融领域的分布式事务数据库灾难恢复能力应至少达到4级及以上能力要求，具体对应的RTO、RPO、灾备部署等关键指标要求见表2。

表2　应用于金融领域的分布式事务数据库容灾能力等级划分

容灾等级	RTO（恢复时间目标）	RPO（恢复点目标）	灾备部署
4级	≤30分钟	0	同城灾备或异地灾备
5级	≤15分钟	0	异地灾备
6级	≤1分钟	0	异地灾备

7　灾备技术要求

7.1　灾备建设模式

应用于金融领域的分布式事务数据库应具备自动或手动灾难恢复能力，满足不同等级灾难恢复要求。在单个机房发生灾难的情况下（如机房进水导致机房整体受损），提供不同等级的容灾能力。在受灾机房恢复之前，应保证受灾机房中所对应的数据库数据和应用服务能通过技术手段全部恢复或者部分恢复，即对数据可靠性和服务可靠性的影响控制在可预期范围内，数据恢复点目标和恢复时间目标根据应用容灾等级进行约束。

分布式事务数据库的灾备建设模式选择，应结合风险分析、业务功能分析和业务中断影响分析，根据成本风险平衡原则以及运行管理要求，选取相应的灾备建设模式。

灾备建设模式具体要求如下：

基本要求：

同城灾备场景：应支持同城两中心或同城多中心部署架构，具体为在生产中心所在城市建设同城数据中心，以应对火灾、电力中断等生产中心可能发生的灾难。

增强要求：

异地灾备场景：宜支持两地三中心或多地多中心等部署架构，具体为在生产中心所在城市建立同城数据中心，同时在与生产中心处于不同地理区域的城市建立异地数据中心，以应对可能发生的同城范围的灾难。

7.2 技术要求

金融领域分布式事务数据库应至少达到4级容灾能力要求，容灾能力相关技术要求应符合GB/T 20988—2007中的规定。本章节从数据备份、数据处理、网络能力和运维能力4个要素给出不同容灾能力等级的具体要求，详见表3至表5。

表3 第6级技术要求

要素	分布式事务数据库相关要求
数据备份	a) 数据应在生产、同城和异地数据中心至少各有2个数据副本。 b) 确保每个同城数据中心至少有1个副本是同步复制，保障数据一致性。 c) 完全数据备份至少每2天1次。 d) 增量数据备份至少每天1次。
数据处理	a) 备用数据处理系统的主机、操作系统等资源与生产数据处理系统完全兼容。 b) 异地和同城数据中心均具备与生产数据处理系统相一致的备用数据处理能力，并处于运行状态。 c) 应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a) 提供充足的网络带宽，保证备份数据传输带宽大于业务峰值所需的带宽需求。 b) 异地和同城数据中心的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同。
运维能力	a) 应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量自动或集中切换。 b) 灾难事件发生后，备份数据中心的数据库资源管理仍可完成对备份数据中心的资源管理和调度。 c) 对生产系统关键运行状态进行实时监控和告警。 d) 分布式事务数据库需要为关键的运营数据提供数据备份。

表4 第5级技术要求

要素	分布式事务数据库相关要求

数据备份	a）数据应在生产和同城数据中心至少各有2个数据副本，在满足RPO、RTO的要求下，异地至少有1个数据副本。 b）确保每个同城数据中心至少有1个副本是同步复制，保障数据一致性。 c）完全数据备份至少每周1次。 d）增量数据备份至少每天1次。
数据处理	a）备用数据处理系统的主机、操作系统等资源与生产数据处理系统完全兼容。 b）异地和同城数据中心均具备与生产数据处理系统相一致的数据处理能力，至少有1个备份处于运行状态。 c）应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a）提供充足的网络带宽，保证备份数据传输带宽满足业务峰值所需的带宽需求。 b）异地和同城数据中心的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同。
运维能力	a）应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量自动或集中切换。 b）灾难事件发生后，备份数据中心的分布式事务数据库资源管理仍可完成对备份数据中心的资源管理和调度。 c）对生产系统关键运行状态进行实时监控和告警。 d）分布式事务数据库需要为关键的运营数据提供数据备份。

表5　第4级技术要求

要素	分布式事务数据库相关要求
数据备份	a）至少有1个数据副本处于同城或异地数据中心。 b）至少存在1个数据副本是同步复制，保障数据一致性。 c）完全数据备份至少每周1次。 d）增量数据备份至少每天1次。
数据处理	a）同城数据中心备用数据处理系统的主机、操作系统等资源与生产数据处理系统完全兼容。 b）同城数据中心具备与生产数据处理系统相一致的数据处理能力，至少有1个备份处于运行状态。 c）应确保备用数据处理系统具备与生产数据处理系统相同的高可用特性。
网络能力	a）提供充足的网络带宽，保证备份数据传输带宽满足业务峰值所需的带宽需求。 b）同城数据中心的虚拟网络、物理网络、出口网络带宽及链路配置与生产系统的网络能力相同。
运维能力	a）应能够对灾备能力进行集成管理，支持通过可定制的标准化流程完成流量集中切换。 b）灾难事件发生后，备份数据中心的分布式事务数据库资源管理仍可完成对备份数据中心的资源管理和调度。 c）对生产系统关键运行状态进行实时监控和告警。 d）分布式事务数据库需要为关键的运营数据提供数据备份。

8　灾备管理流程

8.1 灾难预防

灾难预防应支持对数据中心灾备环境与主生产环境一体化管理，将数据中心的变更、容量、配置、监控、事件、应急、安全等管理流程延伸到同城数据中心和异地数据中心，尤其当主生产环境发生变更时，应定期对灾备环境进行同步变更。

灾难预防应建立和完善的机制包括如下内容：

a) 应支持数据库灾备环境系统可用性检测。

b) 应支持自动或手动切换服务的功能。

c) 数据中心应定期制定灾备切换演练计划，定期进行灾备切换演练，验证灾备系统的有效性。

d) 数据中心应建立完善的应急处理体系，灾难恢复预案和流程应经过切换演练的验证，能确保在紧急情况下发挥作用。

8.1.1 灾难预案管理

灾难预案管理通常包含如下内容：

a) 可用性检测管理：

——应具备灾难检测预案和灾难检测机制，判断资源的可用性。

——应支持对资源的状态进行实时检测，当检测到生产中心异常时及时触发灾备切换。

b) 数据备份管理：

——应具备数据备份方案，定期对生产数据中心和灾备数据中心的数据进行备份。

——应具备数据一致性检测方案，定期对备份数据进行一致性检测。

——应具备备份数据的恢复校验功能，避免因为异常导致备份数据不可用。

——备份数据宜存储在 2 个以上机房。

c) 灾备切换策略管理：

——应具备完善的灾难切换策略。

——应具备完善的恢复回切管理。

——宜在有对应安全机制的前提下，模拟灾难场景，验证灾备系统是否具备完善的灾备切换和恢复回切管理，并以最小化影响业务为原则，满足不同等级的容灾要求。

8.1.2 灾难切换演练

灾难切换演练主要是为了验证灾难恢复预案的完整性和有效性，提高预案的执行能力，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，具体实施方案包括：

a) 同城机房故障切换方案：

——生产中心切换同城数据中心。

——生产中心恢复。

——同城数据中心回切。

b) 异地机房故障切换方案：

——生产中心切换到异地数据中心。

——异地数据中心差异数据修复。

——生产中心恢复。

——异地数据中心回切。

8.2 应急处理

应急处理主要是当数据库系统发生事故停止工作时，整个数据库系统能切换到灾备系统运行，使得数据库系统功能可以继续正常工作。

应急处理流程应包括：数据备份、切换灾备系统运行、业务数据验证、事故检查与验证、恢复和切回生产系统、回溯总结等步骤。相关要求如下：

a) 数据备份，内容如下：
——应在启动事故处置操作前，对数据进行备份，避免在恢复过程中造成数据丢失或损坏。
——当本地已部署有数据库及存储设备，可通过远程存储做本地数据库的数据备份。
——当本地数据库发生故障时可通过远程存储将数据恢复到本地。
——如果发生城市级故障，则应把原有数据备份传输到异地。

b) 切换灾备系统运行，内容如下：
——对生产端和灾备端的数据进行验证，包括一致性验证、完整性验证和可用性验证，确保灾备数据与生产数据一致且可用。
——将发生事件的生产系统切换到灾备系统运行，灾备系统应提前经过运行测试，确保灾备系统可接替生产系统运行。

c) 业务数据验证，内容如下：
——业务数据验证是指当数据库系统切换到灾备系统后，验证系统自身所产生的业务数据，或与其他相关应用系统的交互数据是否正确。
——业务数据验证包括交易数据验证和汇总数据验证，内容如下：
- 交易数据是指数据库系统在工作时段所产生的数据；
- 汇总数据是指数据库系统在工作时段结束后产生报表时所产生的数据。

——交易数据和汇总数据均经验证与生产一致，才能通过业务数据验证，针对发出提交指令但是未收到确认回复的存疑事务进行校验和处置。

d) 事故检查与验证，内容如下：
——对事故发生的原因，受影响的机房、服务器、数据库的范围等进行检查和验证。
——制定事故处置的实施方案，事故处置的实施方案应经过详细的测试与验证，且应包含系统回退方案，确保实施过程中发生意外事件时，系统能回退到实施前的状态。

e) 恢复和切回生产系统内容包括：对生产系统进行恢复，并在生产系统正常运行后，应切回生产系统。

f) 回溯总结内容包括：应对事故处置过程进行全程日志记录，针对事故处置过程中存在的问题进行回溯总结，制定灾难预防措施，并对相关事故处置的预案文档进行修订、发布和宣讲，提升对事故的响应和处置能力。

8.3 管理保障

8.3.1 监控管理

监控管理包括对监控能力和监控职责的管理，具体要求如下：

a） 监控能力：分布式事务数据库环境的灾难恢复应具备的监控能力，包括但不限于：
——应实时监控生产中心和灾备中心的业务应用系统可用性和性能状态。
——应能够有效监控灾备切换过程。
——应能够监控灾备同步状态。
——应具备告警功能。

b） 监控职责：分布式事务数据库应对灾难恢复系统的日常生产维护工作进行监控，包括但不限于：

——应监控分布式事务数据库资源的运行状态并进行优化。
——应执行分布式事务数据库的日常操作、维护工作和升级工作。
——应解决分布式事务数据库资源的基础架构的故障和问题。

8.3.2 监督管理

监督管理包括审计管理和通知报告管理，具体要求如下：

a） 审计：审计包括内部审计和外部审计。内部审计由金融机构内部相关审计部门承担，外部审计由具有国家相应监管部门认定资质的中介机构组织实施。在金融领域分布式事务数据库应用场景中，除了 GB/T 20988—2007 所要求的相关内容，还应重点关注如下问题：

——加大对如下问题的审计力度：

- 灾难恢复过程中应用与数据库运维之间协同是否顺畅，是否能满足不同灾难恢复需求；
- 灾难恢复过程中是否具备系统全流程和全环境的监控预警体系；
- 灾难恢复过程中是否在机制和技术架构上存在缺陷；
- 灾难恢复流程是否存在数据泄露的风险。

——审计的要求：

- 分布式事务数据库运维人员应至少每年提供 1 次更新的预案、演练记录和报告给相关审计部门进行备案和审计；
- 金融机构的相关审计部门应至少每 3 年组织 1 次审计，审计可以由内部审计部门负责也可以由具备国家相应监管部门认定资质的第三方独立审计机构组织，容灾审计工作应形成审计报告；
- 分布式事务数据库运维人员在审计报告出具后应及时对审计报告提出的改进意见给出书面答复，答复的内容至少应包括改进计划、改进措施和历次改进计划的执行情况；
- 审计报告和书面答复应作为风险内控措施的成果进行存档，留存时间不得少于 10 年。

b） 通知报告：分布式事务数据库金融应用中，需要通知相关方和报告相关金融监管部门的具体情况如下：

——应通知分布式事务数据库相关方参与的情况，包括但不限于：

- 需要共同协作的演练；
- 发生重大事件或面临重大风险；
- 需要相关方共同调整方法、流程和协作渠道。

——应报告相关金融监管部门的情况，包括但不限于：

- 可能影响多个金融机构的重大风险；
- 涉及多个金融机构的重大事故处置情况；
- 灾难性事件的处置情况报告。