ICS 35.240.40
CCS A 11

团　　体　　标　　准

T/BFIA 040—2024

金融分布式系统　技术平台能力要求

Requirements for technical platform capabilities of financial distributed system

2024－11－29 发布　　2024－11－29 实施

北京金融科技产业联盟　　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。

本文件由北京金融科技产业联盟归口。

本文件起草单位：中国金融电子化集团有限公司、北京金安信息技术有限责任公司、中国工商银行股份有限公司、建信金融科技有限责任公司、中国农业银行股份有限公司、中国银行股份有限公司、中银金融科技有限公司、上海浦东发展银行股份有限公司、华为技术有限公司、蚂蚁科技集团股份有限公司、腾讯云计算（北京）有限责任公司、中电金信软件有限公司、安超云软件有限公司、新华三技术有限公司。

本文件主要起草人：姜云兵、班廷伦、马国照、韩竺吾、李晨晓、王鑫、张家宇、沈力、巫春梅、夏龙飞、施经纬、滕达、徐克宝、吴纯波、武文斌、钟小威、林镇熙、郝春雨、王海萌、肖飞军、张正园、隋宁宁、杨永、唐成山、丁陈飞、陈军、郭维、胡晓磊、郭智慧、蒋增增、李克鹏、骆君柱、王鹏飞、隋成龙、许刚、李培、徐省委。

引　言

近年来随着科技与金融加速融合，金融业务模式逐步朝着线上化和多样化的方向发展，分布式架构具备高效弹性、开放灵活等特性，可有效适应业务的快速调整和市场的快速变化，为金融信息系统的发展筑牢基石。

金融业IT系统分布式架构转型提升了应用系统海量交易高并发和海量数据处理的整体性能，保证了金融应用系统的可用性，分布式架构是未来金融行业IT系统架构的重要架构形式。当前，仍存在较多的金融IT系统运行于集中式架构之上，IT系统整体进行分布式架构转型还面临着业务连续性要求高、海量遗留系统改造难、海量应用管理难、缺少行业级架构设计标准指导以及潜在技术安全风险等共性问题，随着金融行业数字化转型的深入，这些问题将影响金融机构数字化转型质量与进程。

为帮助和引导金融机构快速构建自身的分布式架构支撑体系，推动金融行业应用系统的整体分布式架构转型，提升各金融机构分布式架构转型的质量和效率，降低实施成本，特编制金融分布式系统系列标准。

本文件是金融分布式系统系列标准之一，金融分布式系统系列标准包括：

——《金融分布式系统　术语》。目的在于给出本标准系列中所使用的专业名词，是其余各部分阅读和应用的基础。

——《金融分布式系统　IT治理指引》。目的在于给出金融机构分布式架构转型后IT治理能力建设原则、流程管理、技术要求、技术支撑体系等方面的要求，以指导金融业分布式架构转型的IT治理能力建设，形成贯穿研发、运维、管理各领域的立体式的深度治理体系。

——《金融分布式系统　参考架构》。目的在于给出金融机构IT系统分布式架构设计参考，确立金融业IT系统分布式架构的核心模块、组件以及整体结构，阐明分布式系统架构下各模块和组件的主要功能以及相互间关系。

——《金融分布式系统　应用设计原则》。目的在于给出金融应用微服务改造设计的总体要求，阐明微服务设计、单元化设计、一致性方案设计、并行验证设计以及正确性验证等通用要求。

——《金融分布式系统　技术平台能力要求》。目的在于给出金融应用运行时所需关键技术平台能力的总体要求，阐明软负载均衡、分布式服务、分布式事务、分布式消息、分布式数据库、分布式缓存以及批量调度等领域的通用要求和安全扩展要求。

——《金融分布式系统　应用开发测试原则》。目的在于给出分布式架构下金融应用开发与测试相关要求，阐明分布式应用软件开发规范、工具方法与测试要求、内容、方法、过程、环境、文档、工具以及管理的通用要求，保障金融分布式应用的研发质量，更好满足用户需求。

——《金融分布式系统　运维能力要求》。目的在于给出金融应用运维时所需关键支撑能力的总体要求，阐明金融应用部署、监控、故障定位与分析、运行保护等领域的通用要求。

金融分布式系统　技术平台能力要求

1　范围

本文件规定了金融分布式系统技术平台能力的总体要求，涵盖软负载均衡、分布式服务、分布式事务、分布式消息、分布式数据库、分布式缓存以及批量调度处理等领域的通用要求和安全扩展要求。

本文件适用于金融业分布式架构技术平台建设。

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 40473.7—2021　银行业应用系统　非功能需求　第7部分：安全性

JR/T 0203—2020　分布式数据库技术金融应用规范　技术架构要求

JR/T 0205—2020　分布式数据库技术金融应用规范　灾难恢复要求

T/BFIA 037-2024　金融分布式系统　术语

3　术语和定义

T/BFIA 037-2024中界定的术语和定义适用于本文件。

4　缩略语

下列符号和缩略语适用于本文件。

ACID：原子性(Atomicity)、一致性(Consistency)、隔离性(Isolation)和持久性（Durability）

CPU：中央处理单元（Central Processing Unit）

ECMP：等价多路径路由（Equal-Cost Multi-Path）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

IPv6：互联网协议第 6 版（Internet Protocol Version 6）

IPv4：互联网协议第 4 版（Internet Protocol Version 4）

JVM：虚拟机（java Virtual Machine）RPO：恢复点目标（Recovery Point Objective）

RTO：恢复时间目标（Recovery Time Objective）

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

TCP：传输控制协议（Transmission Control Protocol）

UDP：用户数据报协议（User DatagramProtocol）

5　概述

分布式系统技术平台主体由三层七个平台组成，按照交易处理流程自上而下分为统一接入层、服务集成层和数据处理层。

统一接入层为解决传统硬件负载均衡扩展能力弱的问题，主要涵盖软负载均衡技术平台，支持服务器加软件的方式，实现高度可定制化的流量分发调度和故障隔离能力，提高接入效率。

服务集成层为传统单体应用拆分提供了方法论和底层基础支撑框架，主要涵盖分布式服务、分布式事务、分布式消息三大技术平台，支持业务系统按照分布式服务架构部署和运行，具备跨系统间事务一致性，高峰缓冲解耦场景下消息通信模式。

数据处理层为分布式架构下数据处理和存储访问提供平台支撑，主要涵盖分布式数据库、分布式缓存、分布式批量三个技术平台，支持数据可靠存储，高效访问及分布式数据的批量调度等分布式架构下配套的数据处理能力。

分布式系统技术平台架构组成图见图1。

图 1　分布式系统技术平台架构组成图

6　技术平台能力要求

6.1　软负载均衡平台

6.1.1　总体要求

软负载均衡满足以下总体要求：

a）应支持基于OSI网络模型第四层协议网络传输层的负载均衡，支持TCP、UDP协议负载均衡；

b）应支持基于OSI网络模型第七层协议应用层的负载均衡，支持HTTP、HTTPS协议负载均衡；

c）应支持最少连接数、轮询、随机、权重等负载均衡策略；

d）应支持自助服务、健康告警、性能分析、应急操作等运维管理能力。

6.1.2　部署架构要求

软负载均衡分为四层软负载和七层软负载。软负载均衡架构宜采用四七层软负载的双层负载均衡的部署架构。四层软负载集群宜通过 ECMP 多活模式或虚拟路由冗余协议（VRRP）主备模式来实现集群内节点的高可用性和可扩展性。七层软负载集群宜通过七层软负载集群的负载均衡能力来实现高可用性和

可扩展性。ECMP 多活模式示意图见图 2。

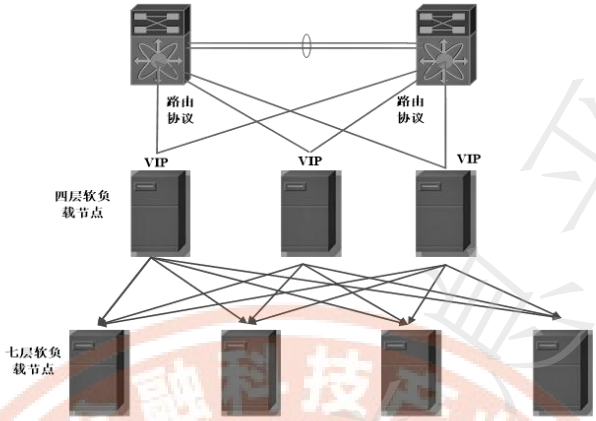

图 2　ECMP 多活模式示意图

VRRP主备模式示意图见图3。

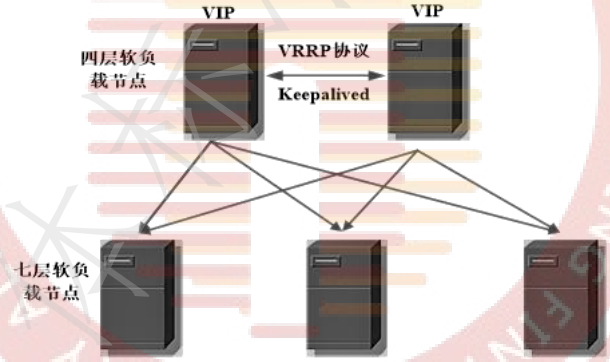

图 3　VRRP 主备模式示意图

6.1.3　核心能力要求

软负载均衡平台核心能力要求如下：

a）应提供多元化的负载均衡算法，包括但不限于如下配置能力：

——最少连接数；

——权重；

——轮询；

——随机；

——一致性 hash。

b）应提供包括传输层到应用层的负载均衡与调度服务；

c）应支持基于TCP、UDP协议的传输层负载均衡；

d）应支持基于HTTP、HTTPS协议的应用层负载均衡；

e）应提供多维度的检查真实服务节点健康状态的检查策略；

f）应支持基于TCP连接和基于HTTP请求的健康检查；
g）应支持可定制健康检查方案，包括但不限于如下配置能力：
——健康检查策略；
——频率；
——周期。
h）应提供主要使用基于IP和基于Cookie会话保持策略的会话保持服务；
i）应提供IPv4与IPv6兼容的双栈负载均衡与调度服务；
j）应提供明确的服务异常错误码和错误信息，如返回HTTP错误码；
k）应具备并发限流能力，支持针对并发连接数、新建连接数等进行限流；
l）应具备访问超时控制能力，并根据业务特征合理配置超时时间；
m）宜支持通过插件方式对统一接入层的功能进行动态配置扩展。

6.1.4 管理面板要求

软负载均衡管理面板要求如下：
a）软负载均衡管理面板应具备独立性，管理平台任何服务器异常，不应影响负载均衡流量调度核心功能的可用性；
b）软负载均衡管理面板应满足可靠性要求，管理面板不应因应用节点异常导致不可用；
c）软负载均衡的运维管理能力应包括以下管理能力：
——配置管理能力，应支持用户通过前端页面或者接口调用的方式，方便快捷的实现配置管理；
——灵活发布能力，应支持对接入服务进行灵活发布，如版本号灰度、百分比灰度、分组发布等；
——监控管理能力，应支持统一监控采集，快速上报监控报警信息，保证处理的时效性和准确性；
——应急管理能力，应支持运维人员通过管控平台实现快速应急管理操作；
——统计分析能力，应支持以视图或者报表的形式展示运行指标统计结果。

6.2 分布式服务平台

6.2.1 总体要求

分布式系统应支持业务通过微服务的形式通信和交互。抽象业务领域的边界，业务能力应具备内聚和解耦，实现业务服务的高度复用，研发效率和产品组合能力的极大提升。微服务架构在部署上相较于传统集中式架构，应具备独立部署和按需扩缩容的特性，具体包括如下：
a） 注册中心；
b） 服务注册；
c） 服务订阅；
d） 服务调用；
e） 服务下线。

6.2.2 核心能力要求

6.2.2.1 注册中心

注册中心功能要求如下：
a） 应支持服务注册与服务注销，动态获取服务实例地址及上下线等服务信息；
b） 应支持服务订阅，服务调用方能从注册中心获取到所有订阅服务的服务信息；

c) 应支持服务通知，当服务注册和服务反注册引起注册中心信息变更，注册中心主动通知到服务订阅方；
d) 应支持服务健康检查，定时检测服务提供方的健康状态；
e) 应支持集群内故障容错，半数以内宕机不影响集群可用性；
f) 应具备故障不影响服务正常调用；
g) 宜具备对冲击性负载的自我保护能力，不因过载负荷导致集群运行故障；
h) 宜具备故障快速恢复，恢复过程不影响应用服务正常调用；
i) 宜支持服务信息动态续租；
j) 宜支持注册中心多租户隔离；
k) 宜支持多集群故障容错，单个集群故障不影响注册订阅服务能力；
l) 宜支持多集群数据之间的动态同步。

6.2.2.2 服务网关

服务网关功能要求如下：
a) 应支持全链路灰度功能，可通过设置灰度标签路由到灰度提供方；
b) 应支持限流功能，针对应用级及服务级限流防止某个应用出问题影响其他应用调用；
c) 应支持泛化调用，提供方发生变化无需重启网关便可进行调用；
d) 应支持告警功能，当遇到问题时能及时通知；
e) 应支持服务网关的生命周期管理；
f) 应支持 API 安全管理，支持 SSL/TSL 加密；
g) 宜在服务网关开展身份鉴权和白名单管理，网关后路由的微服务可不进行黑白名单管理。

6.2.2.3 服务注册

服务注册功能要求如下：
a) 宜具备注册状态校验，宜具备对外提供服务能力时再向注册中心注册；
b) 宜针对服务身份进行验证，防止服务未经授权注册。

6.2.2.4 服务订阅

服务订阅要求如下：
a) 应包含订阅服务的名称；
b) 应只订阅有实际调用关系的服务；
c) 宜对服务订阅者的身份进行认证，防止未经授权订阅。

6.2.2.5 服务调用

服务调用要求如下：
a) 消费方应具备直连提供方的能力，在进行服务调用时，不用经过注册中心等第三方节点，应与提供方点对点调用，服务调用关系示意图见图 4；

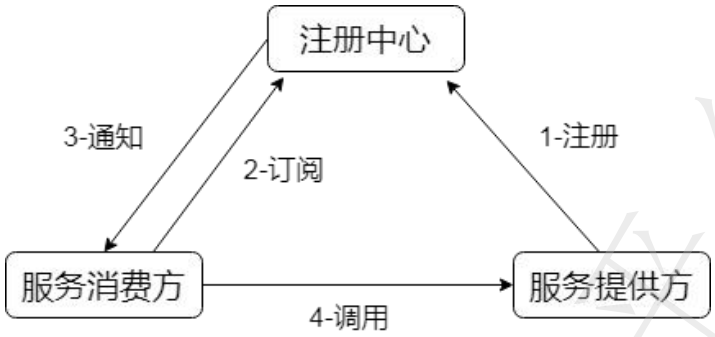

图 4　服务调用关系示意图

b) 服务调用应具备负载均衡的能力，消费方在服务调用时应根据服务提供方的技术特性，合理使用负载策略，包括但不限于如下负载策略：
——随机；
——最小连接数；
——轮循；
——一致性 hash。
c) 服务调用应具备失败容错的能力，在服务调用时应根据业务特性，包括但不限于如下容错策略：
——合理使用超时重试；
——并发限流；
——快速失败。
d) 服务调用应支持服务降级（如自动开关降级），服务提供方和消费方在服务调用时应根据业务特性，合理使用降级策略；
e) 服务调用宜支持智能化园区优先能力，优先选择同园区的服务方，当同园区服务提供方数量与同城其他园区对比少于特定阈值，智能切换到同城优先模式，不再执行同园区优先策略；
f) 服务调用宜提供熔断机制，当服务调用失败率超过特定阈值，不再对服务进行真实调用；
g) 服务调用时应具备超时控制能力，并根据业务特征合理配置超时时间；
h) 消费方在服务调用时应根据业务特性，合理提供多种流控能力，包括但不限于如下流控能力：
——延迟处理；
——部分拒绝处理或拒绝处理。
i) 服务方应具备业务功能预热启动能力，提供方在业务功能预热完成后再对外暴露服务，本地业务规则信息未预热完成前不允许交易流量接入；
j) 服务方应具备运行时故障自隔离、自恢复能力，隔离延时在秒级，降低单一节点故障对系统的业务连续性影响；
k) 服务调用宜满足 GB/T 40473.7—2021 中 3.1 规定的要求，拒绝非法服务调用，以使用户、其他产品或系统具有其授权类型和授权级别一致的数据访问度。

6.2.2.6 服务注销

服务注销过程要求如下：
a) 服务提供方应主动通知注册中心注销服务；
b) 注册中心应删除服务注册相关信息；
c) 应用侧应具备优雅停机能力，保证在途交易执行完成。

6.2.3　服务治理

服务治理方面，在业务系统微服务拆分后，系统规模和服务数量增多，应具备对服务进行场景化治理的功能，服务治理通常包括熔断、限流、容错、路由等，相关的治理项要求如下：

a) 应支持微服务自动注册发现；
b) 应支持微服务负载均衡策略配置；
c) 应支持微服务限流策略配置；
d) 应支持微服务降级策略配置；
e) 应支持微服务熔断策略配置；
f) 应支持微服务容错策略配置；
g) 应支持微服务错误注入策略配置；
h) 应支持微服务黑白名单策略的访问控制配置；
i) 应支持微服务系统路由策略管理；
j) 宜支持微服务系统接口级访问管控策略管理；
k) 宜支持微服务系统接口报文 Schema 配置及校验开关。

6.3 分布式事务平台

6.3.1 事务模型概述

根据 CAP 定理，分布式事务没有完美的解决方案，应根据不同业务场景需求，采用不同的分布式事务模型。分布式事务平台应提供 XA 模型、Saga 模型、Tcc 模型 3 种分布式事务典型场景的技术支撑。

6.3.2 事务接入能力

分布式事务应具备统一的接入规则，具体要求如下：

a) 应提供统一的分布式事务中间件，内置各类事务处理能力，满足各类事务模型的接入需求；
b) 分布式事务处理应支持分布式微服务通信协议，如 HTTP、Dubbo、gRPC 等。

6.3.3 事务异常处理能力

分布式事务平台应对处理异常机制如下：

a) 异常自动化处理机制，应满足包括但不限于如下要求：
——通讯异常、处理超时等异常场景下的自动重试机制；
——幂等、空回滚、防悬挂等保障机制。
b) 异常预警能力，若异常的自动化处理机制失效，或无法完全覆盖异常场景时（即无法通过自动化处理机制确保异常场景下事务最终处理成功），应建立兜底机制及时告警预警；
c) 异常排查能力，应具备事务状态监控和统计，以及链路回查能力，应提供异常场景下快速排查机制；
d) 异常手工介入能力，在自动化机制失效，无法有效处理事务时，应具备异常场景下手工运维能力，提供手工快速应急机制，通过可视化的管理前台进行手工运维。

6.4 分布式消息平台

6.4.1 概述

分布式消息是一种分布式系统或组件之间相互协作的通信机制，是分布式系统中的重要组件，广泛应用于异步解耦、消息通知、流量削峰、数据共享、事务最终一致性等场景。消息服务应具备高安全、高可靠、高性能、可伸缩等企业级特性。

消息服务主要涉及消息发布者（Publisher）、消息代理（Message Broker）、消息订阅者

（Subscriber）、管理控制台（Console）以及监控（Monitor）等核心组件，具体如下：

a) 消息发布者：送消息的应用系统，消息发布者将消息发送到消息代理组件，支持发送一种或者多种类型的消息；
b) 消息代理组件：负责接收消息的系统，消息代理可根据消息类型和消息订阅元数据将消息分发投递到一个或多个消息订阅者，分发投递过程涉及消息类型校验、消息持久化存储、消息订阅关系匹配、消息投递、消息恢复等核心功能；
c) 消息订阅者：阅消息的应用系统，消息订阅者可订阅一种或者多种类型消息，消息订阅者的消息来自消息代理组件；
d) 管理控制台：集成消息查询、节点启停、扩缩容等常用运维操作，图形化展示集群运行状态的组件；
e) 监控组件：采集集群、节点性能、可用性数据，分析性能、可用性数据组件。

6.4.2 核心能力要求

6.4.2.1 消息发布、订阅要求

消息发布、订阅具体要求如下：

a) 消息发布、订阅应通过用户名、用户标识接入消息服务；
b) 消息发布、订阅应具备超时控制能力，可根据业务特性合理配置超时时间，超时可自动进行重试；
c) 消息交付语义应为至少一次（At-least-once，消息不会丢失，但可能被处理多次）；
d) 消息订阅者应支持消息处理幂等性；
e) 消息发布应支持消息主题分区或全局有序；
f) 消息订阅者应支持按集群模式部署，消费组内部分订阅者实例宕机，其余订阅者可接管其订阅分区，不影响业务连续性。

6.4.2.2 消息代理要求

消息代理具备高可用、可扩展等企业级特性，具体要求如下；

a) 消息代理应支持集群方式部署，消息主题（或分区）应支持多副本模式，可通过消息节点多园区部署，消息主题（或分区）副本跨节点分布，支持多中心多活架构，部分节点下宕不影响整个集群的对外服务能力；
b) 消息集群同城多园区应具备热切换能力，支持园区故障秒级切换园区，切换过程对业务无影响；
c) 消息主题应支持多分区部署，可通过横向扩展分区提高系统整体吞吐量；
d) 消息代理应支持消息服务的安全认证，对使用消息服务的用户进行身份鉴别，并控制其访问不同消息主题的权限；
e) 消息代理应支持用户、节点级的限流能力，防止流量突增导致服务不可用；
f) 消息代理应支持按时间、空间维度制定消息清理策略，数据清理前应进行告警提示，避免数据在订阅者成功消费前被清理；
g) 消息代理应具备消息确认机制，消息订阅者在消费异常时能自动进行消费重试；
h) 消息代理应具备死信队列机制，对于多次消费仍无法确认的消息，可按照一定的策略自动清理；
i) 消息代理应具备数据镜像复制能力，可在灾备场景保障秒级故障恢复能力。

6.4.3 管理能力要求

消息服务在管控层面应具备完备的管控能力，具体要求如下：

a） 台账管理：应支持实时查看或管理消息主题、分区、消息发布、订阅者等信息；
b） 消息查询：应支持根据消息偏移量或时间查询消息；
c） 消息订阅查询：应支持实时查询在线消费组订阅状态；
d） 消息轨迹查询：宜支持消息轨迹查询能力；
e） 运维操作：应支持节点启停、动态扩分区等常用运维操作；
f） 权限管理：应支持按照用户角色来分配用户权限，应支持不同角色的自助化服务；
g） 消息服务监控：对于交易量、发送/订阅延迟、订阅者消费进度等系列指标应进行有效监控；
h） 监控告警：对于运行过程中的异常事件应支持进行实时检测和报警；
i） 系统资源监控：对于节点 CPU、内存、存储、连接数等系统状态应支持进行监控；
j） 进程状态监控：对于服务进程的可用性、JVM 性能、线程数等跟进程相关的参数应支持进行有效监控。

6.5 分布式数据库平台

6.5.1 技术架构能力要求

分布式数据库技术架构，具体要求如下：
a) 应具备灵活的部署的能力，本地部署和云部署方式应至少支持一种；
b) 应具备基础 SQL 语法的能力，应支持分布式事务，满足 ACID 特性，至少支持已提交读、可重复读、串行化中的一种隔离级别；
c) 应具备读写分离的能力，应支持业务在架构层面进行读写分离优化，数据库集群内宜支持一主多从，即主节点提供读写服务，多个从节点提供读服务；
d) 应采用存储和计算分离的技术架构，应支持根据需求可独立扩展存储和计算资源；
e) 应具备并发处理的能力，充分利用节点计算资源，应支持各种数据库并发操作；
f) 应具备基本软硬件的适配的能力，兼容主流的 Linux 操作系统、开发语言、开源数据库协议和硬件平台；
g) 应具备服务高可用的能力，全链路的组件均要求应支持高可用部署，当数据库系统发生节点级故障时，RTO 要求在秒级，RPO 要求为 0，应支持自动化方式切换；
h) 应具备数据冗余的能力，结合分布式数据库一致性协议算法等数据冗余相关技术，实现数据副本间的一致性；
i) 应具备数据分片的能力，应支持多种常用分片策略；
j) 应具备弹性扩展能力，应支持水平扩展和垂直扩展的功能；
k) 应具备多租户能力，应支持租户间的资源和数据隔离；
l) 应具备智能运维的能力，应支持自动化安装部署、监控告警、性能容量、系统配置、升级维护、数据迁移、数据备份恢复、日志分析等。

6.5.2 灾难恢复能力要求

分布式数据库灾难恢复能力，具体要求如下：
a) 应具备灾难恢复的能力，根据 JR/T 0205—2020 中划分的容灾等级，满足金融领域容灾能力 6 级中 RTO 和 RPO 的指标要求；
b) 应具备灾环境建设的能力，应支持同城和异地灾备的环境搭建要求，满足从数据备份、数据处理、网络能力和运维能力 4 个要素给出的容灾能力等级相关技术要求。
c) 应具备跨集群数据同步功能，并满足 JR/T 0203—2020 中 8.11 规定的数据同步要求。

6.5.3 数据库接口能力要求

分布式数据库接口能力，具体要求如下：

a) 应具备基础的数据库功能接口的能力，支持部署管理接口、节点管理接口、数据库管理接口、多租户功能接口等接口，支持数据分布、读写分离、并发处理的设置，支持分布式事务、跨库的联合查询、分布式全局唯一且有序递增的数字序列的能力等；
b) 应具备运维管理接口的能力，支持服务高可用接口、数据高可靠接口、运维审计接口、节点扩缩容接口、备份恢复接口、导入导出接口、监控告警接口、日志采集接口，支持数据库滚动升级、补丁管理能力等，导入导出接口应满足 JR/T 0203—2020 中 8.10 规定的导入导出要求；
c) 产品接口参数应支持共用参数和共用错误信息。

6.6 分布式缓存平台

6.6.1 基本功能

分布式缓存平台提供以key-value形式存储数据服务，应满足数据的存取需求，具体要求如下：

a) 应支持 key 的批量写入和读取操作；
b) 应支持在单个 key 上增删查改；
c) 应支持各种 key 和 value 的数据宽度；
d) 应支持 value 自增/自减运算；
e) 应具备命令行交互的能力；
f) 应支持数据的导出和导入能力；
g) 应支持数据淘汰能力，在内存到达阈值时通过逐出算法保证新数据可正常写入；
h) 应支持数据的磁盘持久化的能力；
i) 应支持数据过期时间设置，自动或手动地对历史数据进行清理；
j) 应支持单机模式、主备模式、集群模式，应支持主从数据同步；
k) 应支持主备数据复制，可在灾备场景保障秒级故障恢复能力。

6.6.2 兼容能力

分布式缓存平台在部署上应兼容多种部署场景，提供多语言场景的接入，具体要求如下：

a) 应兼容主流 X86 硬件，ARM 或 MIPS 等异构硬件，不同 CPU 型号和不同 Linux 操作系统；
b) 应支持多种部署方式，可通过虚拟机（KVM/XEN）、容器或其他工具安装部署；
c) 客户端/服务端存在不同版本的数据时，应保证数据读取正确（向下兼容）；
d) 应支持 C/C++、Java、Python 等多语言接入能力。

6.6.3 管理能力

分布式缓存平台在运维层面应提供完备的管控能力，具体要求如下：

a) 应支持自动化部署方式；
b) 应具备全局范围内的数据库配置在线管理能力；
c) 应对缓存服务运行状态进行实时监控，并应具备告警能力，应支持用户自定义监控阈值和告警策略；
d) 应支持用户管理能力，包括用户创建、删除、修改；
e) 应支持权限管理能力，可按照用户角色来分配用户权限。
f) 应支持观测数据库 key 分布分析能力（数据类型、长度、占用空间），应支持离线分析及在线抓取热点 key 的能力；

g） 应具备完整的原地重启能力，重启后重新将存储数据装载后上线服务；
h） 应具备清理掉所有数据和其中部分数据的能力；
i） 不应将缓存当做可靠的持久化存储使用。

6.6.4 高可用特性

分布式缓存平台支持多维度的高可用，具体要求如下：
a） 应具备在电源、硬盘、网线、交换机故障时的故障监测、自动切换能力；
b） 应保障节点故障时的服务能力；
c） 应保障出现超过系统承载压力时的可用性。

6.7 分布式批量平台

6.7.1 调度能力要求

分布式批量平台主要用于分布式体系下的批量作业调度，应具备调度多个执行器协同完成批量作业运行，以及相应的管理与监控的能力，具体要求如下：
a） 应支持多种作业类型，包括定时作业、依赖作业、轮询作业，支持编排负责的任务流程；
b） 应支持任务分片能力，支持按一定的规则将任务分片给多个执行器并行处理；
c） 分配任务时应具备多样的负载均衡策略：随机策略、最小负载策略、第一个执行器等；
d） 应支持失败重试，任务失败时，根据配置的重试策略，按策略要求重跑；
e） 应支持异常自动恢复，发现异常执行器，并把在上面运行的批量作业分配给正常的执行器重新执行；
f） 应具备批量运行监控能力，包括开始时间监控、结束时间监控、运行时长监控、运行结果监控能力及其异常报警能力；
g） 应支持各应用执行器自动注册和动态上下线，上线后即可承担批量作业运行；
h） 应支持对执行器进行资源（如 CPU、内存等）实时收集，并以此作为作业分发过程中的执行器选择依据；
i） 应支持对接入应用按一定逻辑划分租户并支持“多租户调度”能力，以使不同租户之间的作业实现安全隔离。

6.7.2 作业运行要求

分布式批量应具备作业的运行可靠性要求，具体要求如下：
a） 应支持重跑，异常后重新运行最终处理数据正确；
b） 应支持断点续跑，支持按一定的规则将任对于执行时间长的批量（大于 30 分钟），执行过程中记录执行进度信息。批量异常应重新执行时，可从上次处理的数据继续处理。

6.7.3 管理能力要求

分布式批量应具备作业的多种管理能力要求，具体要求如下：
a） 应支持查看各执行器的基本信息及其上面作业运行情况；
b） 应支持查看作业的定义信息及其作业间的依赖关系；
c） 应支持查看各作业的运行情况，包括基本信息及其运行状态、运行进度；
d） 应支持作业应急处理，包括启动、停止、跳过等，并提供可视化运维操作前台。