ICS 35.240.40
CCS A 11

团　　体　　标　　准

T/BFIA 041—2024

金融分布式系统　运维能力要求

Requirements for operation and maintenance 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

全国团体标准信息平台

全国团体标准信息平台

版权保护文件

版权所有归属于该标准的发布机构，除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版、影印版，或发布在互联网及内部网络等。使用许可可与发布机构获取。

目　　次

全国团体标准信息平台

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、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、中电金信数字科技集团有限公司、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、周歆、王炳辉、王鑫、张家宇、沈力、巫春梅、施经纬、易辛悦、任政、郑凯、郭相权、沈一帆、杨超、苏小强、方培贻、胡佳、武文斌、张正园、隋宁宁、杨永、唐成山、丁陈飞、杜鹏、王晓华、葛志赟、董婷婷、侯楠楠、张文、胡晓磊、郭智慧、蒋增增、李克鹏、骆君柱、刘昕、范广、邹明、隋成龙、许刚、李培、徐省委。

全国团体标准信息平台

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业IT系统架构的重要架构形式。当前，仍存在较多的金融业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、微服务、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。

全国团体标准信息平台

金融分布式系统　运维能力要求

1　范围

本文件规定了金融分布式系统提供的运维能力的总体要求，涵盖部署、监控、故障定位与分析、运行保护等领域的通用要求。

本文件适用于指导金融业分布式架构转型的运维能力体系建设。

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。

T/BFIA 037-2024　金融分布式系统　术语

3　术语和定义

T/BFIA 037-2024中界定的以及下列术语和定义适用于本文件。

3.1

持续部署　continuous deployment

一种在软件开发流程中以自动化方式，频繁而且持续性的将软件部署到生产环境中，使软件产品能够快速迭代的软件工程方法。

3.2

限流　flow control

一种当服务请求流量达到预定阈值时，对超过阈值的流量进行快速闭环的方法。

3.3

熔断　circuit breaker

一种当连续访问超时、访问报错达到预定阈值时，暂时断开当前服务访问，并在一定时间后，尝试恢复服务访问的方法。

3.4

灰度发布　grayscale release

一种通过新旧版本短期并存，控制新版本只向特定用户发布的方式，达到新版本的问题只影响部分用户，使得应用系统能够在旧版本和新版本之间平滑过渡的发布方式。

4　缩略语

下列符号和缩略语适用于本文件。

CPU：中央处理单元（Central Processing Unit）

JSON：基于JavaScript编程语言的对象表示法（JavaScript Object Notation）

ID：身份标识号（Identity Document）

IP：网际互联协议（Internet Protocol）

TPS：每秒事务处理数（Transaction Per Second）

5 概述

金融分布式系统运维能力体系由部署、监控、故障定位与分析、运行保护四大部分组成，分布式系统运维能力体系示意图见图1。

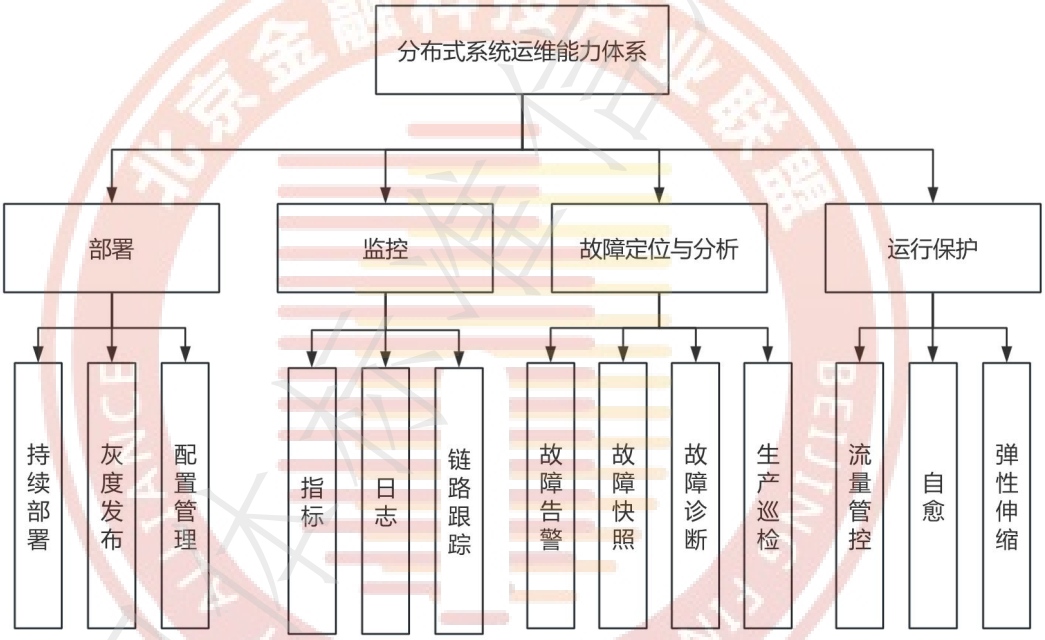

图1 分布式系统运维能力体系示意图

6 分布式系统运维能力体系

6.1 部署

6.1.1 持续部署

6.1.1.1 部署原则

通过对部署软件的产生规则、依赖关系、部署流程进行约束，实现部署过程的标准化和规范化，具体要求如下：

a） 持续部署系统应支持将部署过程涉及的活动纳入统一的部署流程（如持续部署流水线）进行标准化处理；

b） 持续部署系统应把部署软件的流水线和其相关的部署说明文档等建立唯一关联关系；

c） 部署软件应和其承载的应用或应用集群建立明确关联关系，持续部署系统应继承应用架构关系；

d） 部署软件应和需求管理系统中的需求子条目建议明确的包含关系，并支持在部署过程进行按需查阅；

e） 部署软件间的部署依赖应在部署的依赖关系中进行明确标识，持续部署系统应关联并管控相关依赖，按照依赖关系实施部署；

f） 部署软件的具体版本应由持续部署系统实现自动判断和甄选，无需人工干预。

6.1.1.2 部署策略

通过对部署对象在风险管控条件下具备相应的部署策略进行约束，实现安全部署，具体要求如下：

a） 部署软件的部署和发布策略应在系统中进行明确，相关策略应纳入持续部署系统，包括但不限于如下：

——灰度发布策略；

——分批部署策略；

——技术验证策略；

——业务验证策略；

——风险应对策略。

b） 部署软件的部署流程应和其承载的应用或服务集群建立唯一映射关系；

c） 部署软件的灰度发布策略应根据应用属性特征按照灰度发布内容要求实施，由持续部署系统触发灰度策略的实施；

d） 部署过程和策略应包含备份、部署、验证、回退、结果通知步骤内容，持续部署系统应对部署策略实施管控，部署流程中应包含策略并进行刚性控制，纳入部署质量准入门禁；

e） 部署流程策略应经过测试验证，提前发现可能造成中断的因素，未经测试的部署流程应由持续部署系统进行管控和提示，纳入部署质量准入门禁；

f） 部署对象的具体范围应由持续部署系统根据部署环境和节点信息实现自动判断和甄选，无需人工干预。

6.1.1.3 部署风险管控

通过对人工和自动的部署风险措施进行提前约束和落地，实现部署风险的管控和防御，具体要求如下：

a） 应用版本的部署风险防范应在部署前，根据改造内容及所服务的对象范围、业务交易调用链路关系明确潜在影响范围，并确定变更风险级别；

b） 在部署前，运维工程师应协同业务人员、版本人员、测试人员根据部署策略，实施部署推演，发现潜在风险，并制定应对措施；

c） 在部署前，制定应用相应的防御机制和策略，包括灰度模式、流量范围、生效批次、步长、间隔等，持续部署系统应对变更防御机制进行刚性控制，并纳入部署质量准入门禁；

d） 版本部署前应提前完成预处理操作，包括但不限于如下：

——版本提前下载；

——验证策略导入；

——应急方案；

——部署流水线制定。

e） 部署流程应完成流程审批操作，确保部署信息同步对称到相关干系方，持续部署系统开始部署前应完成流程准入判断，纳入部署质量准入门禁；

f） 部署流程应根据服务环境划分实现可复用、可验证、可视化、自适应等特性，并由持续部署系统提供平台能力。

6.1.1.4 部署验证监控

通过部署过程中串联技术和业务验证要求，提升部署过程和业务功能的可靠性水平，具体要求如下：

a） 验证要点应包含技术验证内容，由部署验证平台进行公共验证能力的储存，并纳入质量准入门禁，技术验证内容包括但不限于如下：
——业务的交易量；
——成功率；
——响应时间；
——服务可用性；
——数量。

b） 验证要点应包含本次部署涉及的业务线的重要核心交易场景，以及部署涉及内容的交易验证；

c） 验证要点应由部署验证平台实现分层分级管理，并根据事后部署发布结果，复盘完善验收要点和机制；

d） 部署过程的验证应实现自动化实施能力，具备专门的智能验证平台；

e） 部署过程中持续部署系统验证平台应联动监控平台实时监控业务的运行情况，若异常第一时间启动应急流程；

f） 部署验证平台应结合部署前后的变化，纳入部署流程驱动变更部署过程，验证节点应纳入持续部署系统的部署过程中进行刚性控制，并纳入部署质量准入门禁。

6.1.1.5 部署回退

通过提前定制可一键式执行的回退策略，实现故障场景下的业务快速恢复，具体要求如下：

a） 应在部署前制定完备的应急预案；

b） 回退分为整体回退和部分回退两种类型，整体回退流程实施后应用回到部署前状态，部分回退对应潜在的定制化的回退场景；

c） 部署应具备整体回退流程，部分回退流程可根据部署软件的场景制定，持续部署系统应分类支持，对整体回退纳入部署过程中进行刚性控制，并纳入部署质量准入门禁；

d） 应急回退流程应纳入部署流水线，由持续部署系统进行标识，回退流程与正向部署流程应建立关联关系，回退流程的命名应与对应的部署流程命名相对应；

e） 应支持自动化的回退流程；

f） 对于不能纳入自动化回退流程的回退场景，应提前准备可执行的回退方案；

g） 部署后的回退应由持续部署系统支持，纳入部署失败进行统计度量，根据失败原因进行针对分析和复盘总结。

6.1.1.6 部署后评估

通过对部署过程的全生命周期进行度量分析与智能评估，得出相应指标帮助部署系统在后续迭代过程中参照优化，具体要求如下：

a） 部署过程中的数据应纳入统一管控平台，以便进行事中事后的统计、度量分析、迭代提升；

b） 部署过程的效能、中断、验证、回退等环节应可度量、可视化；

c） 部署时长应纳入部署过程的度量指标，优化压缩部署时长；

d） 部署中断应纳入部署过程的度量指标，优化减少部署中断；

e） 验证有效率和问题未发现次数应纳入部署过程的度量指标，持续分析，提升验证覆盖率和有效性；

f） 部署回退次数应纳入部署过程的度量指标，持续分析，提高回退的有效性和时效性。

6.1.2 灰度发布

灰度发布系统应支持应用系统的物理灰度发布策略，如系统滚动升级、蓝绿发布、灰度发布、逻辑灰度等。具体要求如下：

a） 灰度发布系统应支持业务系统使用独立于正式环境的物理灰度环境，同时支持业务系统使用正式环境下的逻辑灰度环境，应用在版本升级或业务上线前，在物理/逻辑灰度环境上进行版本发布，并根据提前定制的灰度发布策略，引流特定生产流量到灰度环境，经过充分的业务验证和一段时间稳定运行后，再进行正式环境升级。在灰度发布期间，存在正式和灰度两套版本同时对外服务；

b） 灰度发布平台应根据监控系统持续关注灰度环境的性能容量情况，避免灰度环境设备浪费或不足；

c） 业务系统在灰度验证期内，为解决灰度环境版本问题而发布的紧急补丁，应通过灰度平台首先在灰度环境上实施安装，并实施验证、验收工作；

d） 业务系统在灰度验证期内，宜具备自定义兜底策略，在灰度交易出现问题时宜触发兜底策略，不影响该笔交易成功进行。

e） 灰度发布平台通过对持续交付流水线的管控，实现灰度版本投产、渐进式引流、技术验证、应急隔离、灰度转正等自动化变更能力；

f） 在业务系统灰度发布前应准备好版本回退、流量切换等应急策略及预案，遇到交易等问题后通过平台提供的自动或一键式操作实现版本回退、流量切换等，保障业务连续性不因灰度发布受到影响；

g） 灰度发布平台应具备对系统灰度发布的目标、系统灰度发布的内容清单、系统灰度发布结果评价的管理能力。

6.1.3 配置管理

6.1.3.1 配置数据源

配置中心应对应用参数进行统一管理，各应用应从配置中心获取参数，确保参数的单源性管理，避免应用参数多头维护。

6.1.3.2 分类管理

配置中心应按参数类型来管理参数，不同类型的参数具备不同的管理规则。参数分类应包含以下两种类型：

a） 环境参数：应用根据实际环境不同而需配置、调整的环境参数，具体参数值根据各环境情况配置；

b） 版本参数：应用在程序发版时带出的参数，参数值在不同环境保持相同，即参数值在各环境下无需调整。

6.1.3.3 分层管理

配置中心应根据参数实际生效范围的不同对参数进行分层管理，以满足参数集约化管理要求。参数分层应包含以下两种类型：

a） 节点级参数：参数的定义和生效范围面向特定节点（包含多个实例），对其他节点不可见；
b） 应用级参数：参数的定义和生效范围面向整个应用（包含多个节点），不同节点间均可使用该参数。

6.1.3.4 隔离管理

配置中心应按照不同环境、版本对参数进行隔离运维，满足应用多版本并行研发、测试和投产的需要。具体要求如下：

a） 按环境隔离：应对同一应用在研发、测试、生产等不同环境下的参数进行隔离管理，保证参数的生效范围封闭在当前环境中；
b） 按版本隔离：应对应用不同版本中的参数进行隔离管理，满足并行版本研发、生产投产后快速回退的要求。

6.1.3.5 生效管理

配置中心应支持应用在版本投产、生产变更和应急等场景下维护和生效参数，对于生效的方式具体要求如下：

a） 分批生效：参数应支持按灰度、正式、不同环境进行分批生效；
b） 回退生效：参数应支持按版本整体回退和单参数回退；
c） 动态生效：参数维护后，应具备无需安装版本、重启服务的情况下动态生效的能力，满足在线变更需要。

6.1.3.6 可追溯性

配置中心应满足以下可追溯性要求。具体要求如下：

a） 应完整记录参数从定义、修改、生效和退出全生命周期中的变更情况，确保参数的可追溯性；
b） 应支持按参数名、操作时间、操作人等维度进行查询，满足内外部审计需要。

6.1.3.7 配置安全

配置中心在提供参数管理能力时，应满足以下安全保护要求。具体要求如下：

a） 应用安全：应支持按应用进行身份鉴别，避免应用在获取参数时出现跨应用使用的问题；
b） 用户安全：应支持按用户进行权限控制，不同用户权限需自行申请，经审批后方可生效；
c） 存储安全：应支持对敏感类参数存储的机密性和完整性保护，防止敏感参数的泄漏和被篡改。

6.2 监控

6.2.1 指标

6.2.1.1 指标采集能力要求

通过采集不同的监控对象的指标数据，实现不同场景的监控覆盖，具体内容如下：

a） 指标采集应覆盖操作系统、中间件、应用程序、业务等不同维度的指标类型；
b） 系统、中间件指标的监控对象宜包括但不限于如下：
——CPU；
——内存；
——管道；
——队列；
——进程；

——线程；
——磁盘 I/O；
——网络通信带宽；
——网络端口可用性；
——文件系统参数；
——JVM；
——数据库；
——数据库连接池；
——数据库表大小；
——当前会话数；
——新建会话数。

c） 应用程序指标的监控对象宜包括但不限于如下：
——服务接口；
——SQ；
——缓存访问；
——消息队列访问；
——本地方法调用。

d） 业务指标的监控对象宜包括但不限于如下：
——业务交易量；
——业务成功率；
——金额；
——当前直接用户数；
——无交易持续时间；
——连续失败交易笔数；
——平均交易时长；
——累计失败笔数；
——交易量变化率。

e） 指标宜避免重复采集；

f） 指标采集应支持不同类型的框架和组件，并支持组合发送；

g） 指标采集配置宜支持热加载能力，实现对于指标采集发送的动态配置；

h） 指标采集宜携带必要元数据信息：
——园区信息：部署园区的唯一标识，用于描述监控指标来源的物理部署信息；
——单元信息：部署单元的唯一标识，用于描述监控指标来源的物理部署信息；
——IP地址：服务器IP地址，用于标识监控指标来源的服务器；
——应用标识：应用ID或名称，用于标识监控指标来源的应用；
——集群标识：应用集群ID或名称，用于标识监控指标来源的应用集群；
——灰度信息：是否灰度标识，用于描述监控指标来源是否为灰度交易；
——其他自定义元数据。

6.2.1.2 指标性能容量要求

通过对监控指标采集和传输存储各环节提出性能容量要求，实现被监控系统和监控平台本身的安全稳定运行，具体内容如下：

a） 应控制指标采集对业务应用的性能影响，支持无侵入式采集，指标的采集或发送异常不应该影响应用正常服务；
b） 应对指标的采集链路实现自监控能力，针对指标丢失、时延等场景进行监控；
c） 指标采集链路宜具备限流能力，以便在突发流量过大的情况下对指标采集动作实施限流措施。

6.2.1.3 指标聚合能力要求

通过交易、系统运行等指标，结合日志实现对应用运行情况的监控，实现指标定制和聚合分析，具体内容如下：

a） 描述负载情况的指标宜采用百分比形式进行展示；
b） 描述交易服务水平状态的指标应包含：
——吞吐量：单位时间内处理的请求的数量；
——并发数：系统同时处理的请求数量；
——平均响应时间：完成交易处理的平均耗时；
——总数：处理的交易总数量；
——失败数：处理的失败交易数量。
c） 宜通过可视化工具实现指标的多种视图展示，基于指标视图配置实时报警规则；
d） 宜针对指标引入算法实现基于智能运维无阈值报警、波动报警；
e） 应实现基于指标的报警分析，例如基于交易的成功率、耗时等报警，具备智能故障根因分析能力。

6.2.2 日志

6.2.2.1 日志收集能力要求

金融分布式系统通过采集应用、系统、设备日志，并汇聚保存到分布式存储介质，日志收集具体要求如下：

a） 日志采集应支持多种日志格式，包括但不限于纯文本、分隔符、JSON 等；
b） 日志采集应支持不同字符集，包括但不限于 UTF-8、GBK 等，并支持转换；
c） 日志采集应具备配置化的采集文件扫描能力，并实时更新获取信息；
d） 日志采集宜避免重复采集；
e） 日志采集应保证数据传输的连续性，并具备本地缓存能力，当出现异常的时候能进行恢复和重发；
f） 采集的每条日志时间标识应与应用日志记录的时间一致；
g） 日志采集应支持不同类型接收端，包括但不限于分布式消息、时序数据库、分布式文件系统，支持组合发送；
h） 日志采集应独立部署于环境中，通过共享存储、接口等方式获取应用日志，避免与业务系统耦合；
i） 日志采集配置宜支持热加载能力，实现对于日志采集发送的动态配置；
j） 应用日志的发送链路宜具备故障监控能力，出现日志数据采集或传输异常时能及时监控；
k） 应用日志的发送链路宜具备数据加工能力，宜支持对应用个性化添加规则进行日志数据的加工和过滤，处理性能应不低于分钟级；
l） 应用日志的发送链路宜具备限流能力，单一应用突发流量过大应进行应用日志限流；
m） 应用日志的发送链路宜具备动态调整能力，应用日志链路故障、目标集群故障时应具备动态调整到健康的链路和目标集群的能力；

n） 日志采集进程应部署健康检查和重启机制，进程故障、停止后能触发自动重启。

6.2.2.2 日志检索能力要求

在分布式存储介质保存的交易日志，需提供便捷的日志检索功能，具体要求如下：

a） 日志检索能力应由独立平台提供，不应和业务系统产生耦合；
b） 应提供近实时的快速查询应用日志的功能，支持按照日期、应用、节点、关键字等信息进行快速筛选日志的功能；
c） 应提供复合查询功能，支持用户方便查询到成功率等复合计算数据；
d） 应通过可视化工具支持应用个性化定制查询语句进行日志快速搜索、定位；
e） 应提供功能支持应用日志进行下载，实现按照日期时间、应用、节点等信息进行日志差异化下载功能；
f） 应实现调用链与日志数据的关联查询，可直接在调用链中查看抽样的日志数据，也可通过链路唯一标识等关键字关联日志系统进行详细的交易日志分析。

6.2.2.3 日志性能容量要求

分布式系统日志数量庞大，对于日志存储端性能容量要求较高，具体要求如下：

a） 日志集群搭建部署机器应支持虚拟机或物理服务器搭建方式，从数据量读写效率、存储容量等指标评估，宜采用物理服务器；
b） 日志存储端集群搭建和扩容应建立自动化流水线，实现集群的快速自动化搭建和扩容；
c） 日志集群应建立长周期存储机制，包括但不限于由分布式文件系统、时序数据库进行存储；
d） 日志存储端集群节点应具备故障恢复能力，故障状态时，能根据故障指标进行自动隔离、重启、报警；
e） 应具备日志生命周期管理能力，支持自动或手工清理日志搜索集群和分布式文件系统日志。

6.2.3 链路跟踪

6.2.3.1 链路埋点与跟踪能力要求

通过链路埋点实现链路监控数据采集，结合指标、日志等监控数据提供关联分析能力，实现应用和业务视角的监控功能，具体要求如下：

a） 应满足交易全链路的调用跟踪需求，包含链路调用父子关系，客户端发起请求时间、服务端接收请求时间、服务端发起响应时间、客户端接收响应时间的可视化展示；
b） 应提供应用视角的监控分析功能，整合应用的链路、指标、日志等监控数据，支持关联分析；
c） 应提供业务视角的监控分析功能，整合业务的链路拓扑、指标、日志等监控数据，支持从上到下逐层钻取；
d） 链路数据采集宜采用 SDK 或探针等方式实现，减少对业务系统的侵入；
e） 应采用异步队列传输模式对采集到的数据进行异步发送，不阻塞业务线程，应关注异步队列的大小，避免对业务应用产生影响；
f） 不应在采集端进行数据清洗和分析操作，避免对业务应用产生影响。

6.2.3.2 链路性能容量要求

通过对链路监控数据采集和传输存储各环节提出性能容量要求，实现被监控系统和监控平台本身的安全稳定运行，具体要求如下：

a） 链路监控数据的采集应基于百分比采样或者固定速率采样，设置百分比采样时仅对一定比例交易进行链路数据采集，设置固定速率采样时每秒采集的链路数据应低于设定阈值；
b） 应结合业务实际情况限制监控数据采集和传输占用的资源，如将 CPU 和内存消耗限制在 5%以下作为参考阈值；
c） 监控网关应根据监控数据类型将数据分发到相应的消息队列，并能水平扩展；
d） 应使用消息队列作为监控数据采集和存储两个模块之间的缓冲。

6.3 故障定位与分析

6.3.1 故障告警

对于金融分布式系统故障告警，具体要求如下：
a） 应具备告警信息统一上送的渠道，支持各应用软硬件设施依照统一格式上发报警，宜采用 JSON 形式，报警报文格式示例见表 1；

表 1 报警报文格式示例

字段名	说明
_id	技术主键
warnTitle	告警标题
warnType	告警类型
warnSource	告警来源
warnLevel	告警等级
warnDate	告警时间
warnStatus	告警状态（已处理、未处理、已忽略）
createDate	告警开始时间
lastDate	告警最后发生时间
appName	告警应用
warnNo	告警编号
info	告警信息
ext	告警扩展信息

b） 应提供报警信息存储能力，支持存储一段时间内的报警，以便追溯；
c） 应提供报警信息查询服务，应支持多维度的聚合查询能力，如按照应用、报警类型、园区、集群、宿主机等维度；
d） 应提供报警通知配置能力，支持用户提前订阅报警内容，并配置报警渠道，如邮件、短信等；
e） 宜支持基于告警信息生成告警事件，并持久化存储，包括但不限于文本存储或其他数据库；
f） 应具备告警信息反查和对应预警观测视图展示；
g） 应支持固定告警阈值配置，宜支持无阈值告警能力。

6.3.2 故障快照

在金融分布式系统故障分析过程中，需对故障对象下发特定的命令，获取对象的实时状态信息，称之为故障快照。在故障快照运维能力方面，具体要求如下：
a） 故障快照的覆盖范围应包括但不限于 CPU、内存、网络、存储等信息；
b） 快照应支持按秒级执行能力，用于比对分析；

c） 快照执行应屏蔽底层操作系统、中间件差异，宜通过选择或者配置的方式执行快照任务；
d） 快照执行宜避免应用改造，对应用无入侵；
e） 支持多种触发方式，如手工执行、定时触发、报警联动等；
f） 快照执行宜高亮提示存在的风险与隐患，务必二次确认后生效；
g） 快照执行应进行严格的任务并发控制、超时以及其他异常处理，避免影响正常系统运行；
h） 快照配置、执行应有明确的执行记录；
i） 快照持久化存储宜配置定期清理策略。

6.3.3 故障诊断

6.3.3.1 问题诊断

在金融分布式系统运维过程中，问题诊断能力要求如下：
a） 应提供多维度的诊断功能，诊断功能示例见表 2；

表 2 诊断功能示例

诊断类型	诊断说明
日志关键字诊断	查询某一时间范围内日志是否存在预期字段
数据库预期值诊断	验证数据库中某个字段是否符合预期
容器运行情况诊断	验证容器运行状况是否正常
配置文件诊断	验证生产环境配置文件值是否符合预期

b） 各诊断能力宜支持参数配置，诊断内容应进行校验，不应通过诊断功能进行变更操作；
c） 诊断能力宜支持组合、编排，模拟人工执行；
d） 诊断配置、执行应有明确的执行记录；
e） 宜支持多种触发方式，包括但不限于手工执行、定时触发、报警联动；
f） 提供类专家库配置等方式，实现诊断专家经验的固化、更新；
g） 诊断结果宜配置定期清理策略；
h） 提供监控视图多维度展现和下钻分析的能力，支持根据各种维度下钻展现运行情况，分析异常范围，下钻维度包括但不限于：
——园区：提供整个园区的运行状况的监控视图，可定位故障所在的园区；
——应用：提供单个应用的整体运行状况的监控视图，可定位故障所属应用；
——集群：在上云环境中，提供云平台集群的整体运行状况监控视图，可定位故障所在的集群；
——服务器：提供单台服务器的整体运行状况的监控视图，可定位故障所在的服务器。
i） 提供故障原因人工智能辅助分析的能力，基于监控、日志、链路等运维信息辅助定位问题原因；
j） 宜支持根据故障类型配置不同诊断入口，引导用户进行自主故障定位。

6.3.3.2 异常检测

在金融分布式系统运维能力中，针对指标可引入基于智能算法的异常检测，提升故障发现能力。异常检测功能要求如下：
a） 异常检测算法应覆盖不同分布类型的指标数据，包括但不限于：
——周期型：指标波动按同样的顺序重复出现，呈现出周期性，周期型指标示例见图 2；

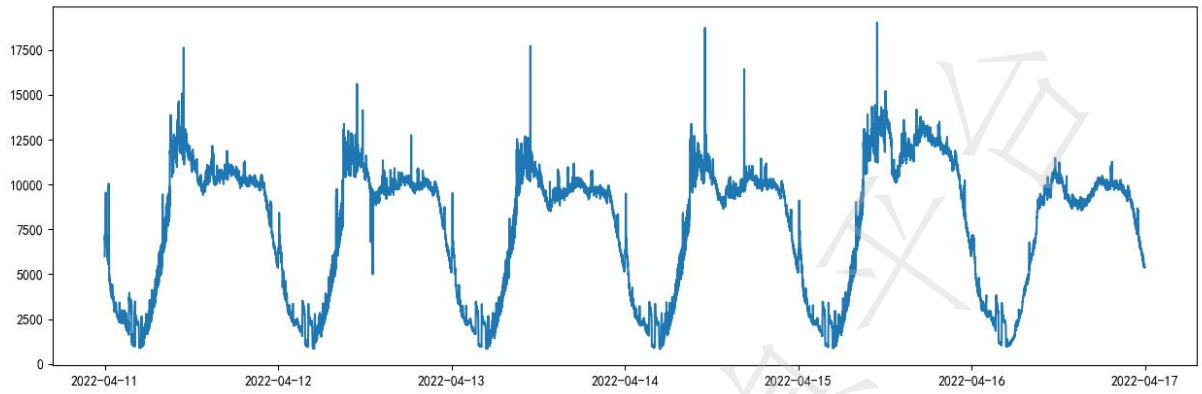

图 2　周期型指标示例

——平稳型：指标均值、方差均无系统的变化，呈现出平稳状态，平稳型指标示例见图 3。

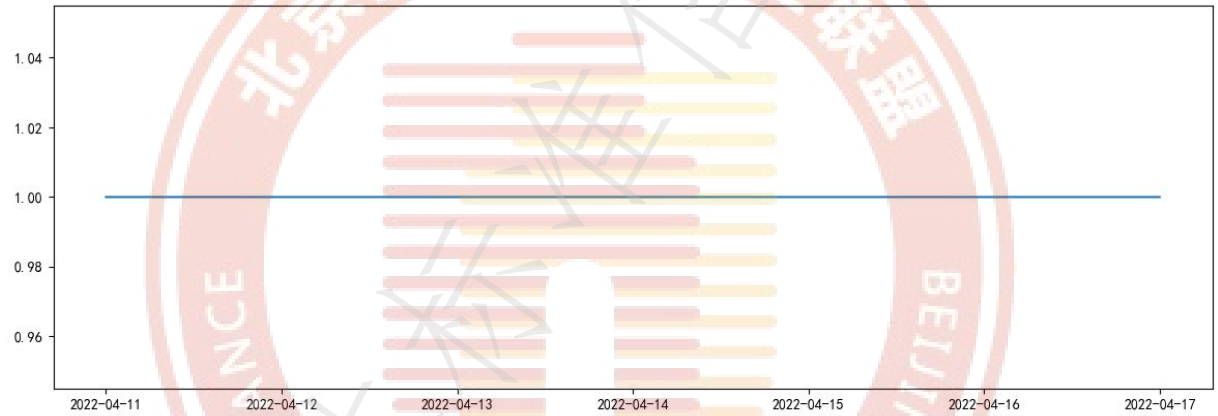

图 3　平稳型指标示例

b）　宜支持根据指标的历史数据自学习和判断指标分布类型，并路由到不同检测算法；

c）　应提供精细化参数调优的能力；

d）　应提供异常检测结果的存储和展示能力。

6.3.3.3　根因定位

在金融分布式系统运维中，根因定位功能具体要求如下：

a）　宜支持对接多种开源监控数据，作为根因分析的源数据输入；

b）　应支持集成故障诊断、异常检测、故障告警等不同的异常来源信息；

c）　应支持根据横向链路调用，定位异常节点的能力；

d）　应支持根据纵向的部署信息，定位出异常层级的能力，包括但不限于：

——容器故障：在上云环境中，通过根因定位，可识别出故障是否集中在具体某个容器；

——宿主机故障：在上云环境中，通过根因定位，可识别出故障是否集中发生在某台宿主机；

——机房故障：通过根因定位，可识别出故障集中在发生在某个机房；

——园区故障：通过根因定位，可识别出故障集中发生在某个园区。

e）　应提供根因定位算法参数调优的能力；

f）　应提供根因定位结果的存储与展示能力；

g） 应支持根据历史数据自学习与自动调优能力，例如根据指标的历史数据可学习形成检测定位模型，随着时间变化，若指标数据出现形态或周期变动时，可自识别，并调整检测定位模型。

6.3.4 生产巡检

生产巡检旨在报警体系外，对应用生产运行开展日常的巡检，发现潜在安全隐患，并对隐患进行分析及改进，具体要求如下：

a） 应提供涵盖分布式系统的生产运行情况，宜涵盖 CPU、内存等性能容量指标和服务失败、批量作业中断、事务悬挂等应用业务指标，及时发现生产安全隐患；

b） 宜提供按部门、应用等多维度的巡检视图，支持用户提前配置并订阅，并通过邮件的形式进行推动；

c） 宜支持个性化巡检配置，包括但不限于自定义巡检指标、自定义巡检指标阈值、自定义巡检频率；

d） 应提供巡检异常汇总视图查询和展示；

e） 宜提供智能化巡检能力，例如依托孤立森林、逻辑回归、时间序列算法等智能算法，实现波动巡检预警、无阈值巡检。

6.4 运行保护

6.4.1 流量管控

6.4.1.1 限流

金融分布式系统应具备限流能力，具体要求如下：

a） 流量管控平台应提供限流能力，包括但不限于 TPS 控制和瞬时并发控制，帮助服务提供方保护自身性能容量，避免在流量突破节点性能容量造成更大的业务损失；

b） 流量管控平台应提供动态配置能力供生产应急使用，提供对节点限流相关参数（如 TPS 或并发数）实时调整的能力；

c） 流量管控平台应提供静态配置能力，在节点网络通信出现异常时，始终有兜底策略运行，平台应具备加载静态配置文件的能力，确保节点与远程配置中心出现网络异常时，限流能力不会消失。

6.4.1.2 熔断

金融分布式系统应具备熔断能力，具体要求如下：

a） 流量管控平台应提供熔断能力，帮助服务调用方自动识别并屏蔽关键场景下的非关键调用，避免因为非关键的服务调用异常导致整体业务成功率下降；

b） 流量管控平台应提供动态配置能力，供生产应急使用，平台应利用远程配置中心等能力提供对节点熔断相关参数（如响应时间或异常比例）实时调整的能力；

c） 流量管控平台应提供静态配置能力，在节点网络通信出现异常时，始终有兜底策略运行，平台应具备加载静态配置文件的能力来确保节点与远程配置中心出现网络异常时，熔断能力不会消失。

6.4.1.3 阻断

流量管控平台应针对节点的入口流量以及出口流量提供截断全部流量的能力，保证在任何场景下，当判断需要截断网络流量时，能够快速闭环相关流量。

6.4.1.4 应急切流

流量管控平台自动应急切流能力要求如下：

a） 当某一个分区故障时，应支持自动切流到其他分区，并且不影响对外服务能力；

b） 当某个节点故障时，应支持自动切流到其他正常节点，并且不影响对外服务能力。

6.4.1.5 故障隔离

流量管控平台自动故障隔离能力要求如下：

a） 当某一个分区故障时，应支持自动隔离故障分区，并且不影响对外服务能力；

b） 当某个节点故障时，应支持自动隔离故障节点，并且不影响对外服务能力。

6.4.2 自愈

自愈的重点在问题检测和故障修复两个方面。问题检测是通过定时执行健康探测，以检查节点内部是否按照预期的状态工作；故障修复是如果探测失败，通过重启等应急策略对节点进行故障修复，保证业务节点的整体稳定性。具体能力要求如下：

a） 应支持自定义多种类型的服务探测的能力，包括但不限于如下：

——命令行式；

——TCP 方式；

——HttpGet 方式。

b） 应具备动态调度的能力，在底层服务器节点正常时，应支持在原服务器上自动重启；在底层服务器异常时，应支持通过人工切换或容器自动漂移等方式，在其他正常的底层服务器上启动节点。

6.4.3 弹性伸缩

弹性伸缩是当业务节点达到目标状态时，对超过阈值的节点自动扩大实例数，以此保障业务节点对外服务稳定，对低于阈值的节点自动缩小实例数，释放资源保障资源合理分配和利用，具体要求如下：

a） 应具备自动化能力，无需投入大量人力来调整容器资源，根据预置的度量指标自动弹性扩张和弹性收缩；

b） 应具备支持多种伸缩模式兼容，可灵活调度应对各种复杂的场景，其模式包括但不限于如下：

——定时；

——自定义；

——动态。

c） 应具备丰富的扩缩指标，包括但不限于 CPU、内存的平均利用率等。

A

参 考 文 献

[1] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范
[2] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[3] GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
[4] JR/T 0166—2020 云计算技术金融应用规范 技术架构
[5] JR/T 0205—2020 分布式数据库技术金融应用规范灾难恢复要求

全国团体标准信息平台