

中信期货有限公司信息技术标准

Q/CITICF 001—2023

信息系统应用高可用性设计规范

Design specification of highly available applications for information
systems of CITIC Futures Co., Ltd.

2023 年 9 月 11 日 发布

2023 年 9 月 11 日 实施

中信期货有限公司金融科技委员会 发 布

目次

目次 I

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 设计要求 2

 4.1 总体设计要求 2

 4.2 应用层高可用性设计要求 2

 4.3 系统层高可用性设计要求 3

附录 A（规范性） 中信期货有限公司信息系统类别/级别 5

 A.1 概述 5

 A.2 参考的法律、行政法规和规章 5

 A.3 信息系统类别/级别 6

附录 B（规范性） 应用高可用性设计要求适用情况参考 7

参考文献 8

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。

本文件由中信期货有限公司 IT 架构审查小组提出并归口。

本文件起草单位：中信期货有限公司金融科技委员会技术规划部。

本文件主要起草人：郑敏俊、杜思捷。

引 言

信息系统是支撑企业业务经营和内部管理的重要平台，维护信息系统安全是企业信息安全的重点，因发生灾难导致业务中断，可能对企业内部管理、公民、法人和其他组织的金融权益甚至金融稳定和行业秩序产生影响。

为规范和引导在信息系统架构设计活动中合理运用高可用技术实现业务承载和灾难恢复，有效防范信息系统风险，保护企业和客户的合法权益，特编制本文件。

信息系统应用高可用性设计规范

1 范围

本文件提出了中信期货有限公司信息系统应遵循的应用高可用性设计规范要求，主要包括总体设计要求、应用层高可用性设计要求、系统层高可用性设计要求等方面的内容。关于信息系统数据高可用性设计（含数据容灾）、数据中心高可用性设计的要求不在本文件中展开讨论。

在信息系统新建及重大改造的架构设计过程中，技术方案和集成方案应遵照本文件要求进行应用高可用性设计，具体产品选型可参照相应的技术标准或配置导引展开具体配置层面的设计。

本文件适用于中信期货有限公司总部、各分公司信息系统的架构设计，各子公司参照执行。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

3.1

可用性 availability

信息系统服务的可用性是指信息系统应用在约定条件下和约定时刻或时间区间内能够提供约定服务的能力。

3.2

可用性指标 availability index

一般指可用率，该指标通过系统的可靠性（reliability）和可维护性（maintainability）来度量。平均无故障时间（MTTF）用来度量系统的可靠性，平均维修时间（MTTR）用来度量系统的可维护性，可用率=平均无故障时间÷（平均无故障时间+平均维修时间）×100%。

3.3

高可用性 high availability

指通过缩短因日常维护操作（计划内）和突发的系统崩溃（计划外）所导致的停机时间，以提高信息系统服务的可用性。高可用技术指为实现高可用性目标所采用的技术手段，负载均衡、高可用集群等是目前常见的高可用技术。应用高可用性设计更关注信息系统在应用层、系统层的技术解决方案和最佳实践。

3.4

有状态应用 stateful applications

指服务器存有用户会话，应用服务器保留用户会话的上下文信息，用户的后续请求依赖前序会话。

3.5

无状态应用 stateless applications

指在响应服务调用方的请求时应用服务器不会保留用户会话中的任何上下文信息，并且要求用户请求本身包含了处理该请求所需的全部信息，此类应用的多个服务器（或实例）间关系对等且无相互依赖，用户请求在不同服务器（或实例）上的处理结果一致。

3.6

短连接 short-lived connections

指通讯双方有数据交互时建立连接，交互完成后连接关闭，即单次连接完成一项业务的发送。

3.7

长连接 persistent connections

指一个连接上可以发送多个数据包，在保持连接期间，如无数据包发送，需要发链路检测包。

3.8

本地域名解析服务（器） local DNS server

指由客户端自身实现域名到 IP 地址的转换，不依赖网络中的域名解析服务（器）。

4 设计要求

信息系统应用高可用性设计应遵循如下要求，下述如与已发布的技术标准存在冲突，须以本文件为准。

4.1 总体设计要求

- a) 针对 C 类信息系统，优先采用单活部署模式，并且至少确保以现有基础环境高可用技术（如 VMware vSphere HA、H3C CAS HA）来保证服务可用性，对于单次停机时间要求较高的系统，可以考虑应用负载均衡和数据库高可用性设计。
- b) 针对 B 类信息系统，优先采用双活部署模式，应用服务器应以负载均衡方式部署多份计算资源，并确保承载相应服务的计算资源已经能构成有效冗余，同时数据库服务器也应采用高可用性设计，以便发生故障时仍能保持服务可用。对数据的完整性、可用性和可恢复性有较高要求的信息系统，优先考虑使用相应的数据库高可用技术。
- c) 针对重要信息系统、A 类信息系统，必须采用双活部署模式，同时还应减少中间件、数据库以及应用的启动恢复时间，应使用相应的高可用技术以支持免重启恢复服务和客户端连接自动切换。
- d) 优先将联机服务和 Web 服务设计成无状态服务。
- e) 应支持在线服务自侦测，并且在服务器或服务的进程重启后实现服务自动加载。

4.2 应用层高可用性设计要求

4.2.1 Web 服务场景

- a) 对 Web 应用服务应采用负载均衡架构并维护健康检查信息，包括使用各类负载均衡服务（优先考虑硬件设备）以及微服务框架提供的负载均衡能力等，避免单点部署。
- b) 应用服务应对等配置和部署，即属同一应用服务的不同服务器（或实例）在部署时使用相同配置和参数。

4.2.2 联机服务场景

- a) 同 Web 服务场景全部要求。
- b) 服务的请求方与提供方通讯时应采用长连接，也应根据实际情况考虑采用连接保活机制（KeepAlive），特别是在跨防火墙通讯等场景下。

4.2.3 批处理场景

- a) 批处理任务应设计配套的调度机制，支持失效转移（如双机切换）后的作业状态识别，并实现作业重做的判断逻辑或断点接续的判断逻辑，且以无需上下游系统随之调整为宜。
- b) 对于大批量数据处理任务，宜采用分布式批量任务调度架构。

4.2.4 数据库重连要求

- a) 对使用数据库（含数据库连接池）长连接的客户端应用，应使用连接保活机制（KeepAlive），应实现中断监控并自动重连，并引入重试机制。

- b) 数据库连接宜配置为浮动/虚拟 IP 地址所对应的域名。

4.2.5 数据缓存

- a) 高并发、无状态改造、大数据量及复杂数据缓存场景下，在应用服务器和数据库服务器间应采用合适的缓存技术。
- b) 应用设计应考虑数据缓存失效时的服务降级机制，尽可能避免服务完全失效，并且应在缓存故障恢复后通过缓存预热等措施，尽快恢复服务水平。
- c) 远大于服务接口调用周期的数据持久化需求宜通过数据库及时入库实现。

4.2.6 消息队列

- a) 为解决应用耦合、异步消息和流量消降等问题，在应用的不同服务间优先考虑使用合适的异步消息队列技术。
- b) 应考虑消息队列崩溃后的服务降级机制，尽可能避免消息丢失和服务完全失效，应在消息队列故障恢复后通过积压消息处理、消息补发等措施，尽快恢复服务水平。
- c) 如需使用数据库持久化方案，应选用异步模式，以控制故障影响面。
- d) 微服务如使用消息队列实现彼此的通信与业务流程的驱动，每个微服务应对应一个队列，并在同一个微服务的不同服务器（或实例）间负载均衡，从而实现不同服务之间的解耦。

4.2.7 定时任务要求

服务节点发生失效转移（如双机切换）时，原节点定时任务应停止，切换后的节点应实现定时任务切换/拉起机制。

4.2.8 服务降级和熔断

- a) 应支持应用和服务负荷的即时侦测并根据压力测试数据合理设置阈值。
- b) 负荷过载时支持停止相关服务的熔断机制。
- c) 压力陡增时支持对承载非核心业务的服务进行限流或停服的降级机制，以保证核心业务的正常运行，降级范围应根据业务重要程度做好分级设计。
- d) 服务降级和熔断触发后，系统应根据最新的侦测数据自动解除限制。

4.3 系统层高可用性设计要求

4.3.1 面向应用服务的系统层设计要求

- a) 采用负载均衡架构并优先选择微服务架构。
- b) 非微服务应用（适用于同一系统内）互相访问应使用域名，且域名和访问端口应为可配置项。
- c) 不应使用本地域名解析服务，信息系统面向用户的客户端访问入口应使用统一的域名解析服务（含全局流量管理服务、智能域名解析系统等）或能与之保持同步的下级域名解析服务。
- d) 启用负载均衡服务或配置操作系统高可用软件的应用服务器，应通过域名（解析到由负载均衡服务或高可用软件管理的虚拟 IP 地址）对外提供访问地址。
- e) 使用操作系统高可用技术时，应优先使用双机热备的故障转移方式。
- f) 针对操作系统节点的自动切换，应有完整的切换条件输入，如心跳、状态位等；针对需要人工切换的场景，应提供包含完整信息的操作界面，以尽可能减少人工判断和处理为宜。
- g) 当使用多份计算资源（含跨同城机房场景）冗余部署时，具体冗余数量应结合信息系统的可用性指标（可用率）和 IT 服务级别协议（SLA）指标来综合考量。
- h) 针对可用性指标（可用率）要求较高的信息系统，应确保在损失单份或同城单一机房内所有资源的情况下，处理能力能满足业务（包括高峰期）的需要。

4.3.2 面向数据服务的系统层设计要求

- a) 部署数据库应用应使用数据库资源池服务，在无法满足需求情况下方可申请服务器自建。
- b) 自建数据库应选用主备、主从或分布式等满足高可用性要求的架构（如 Oracle RAC、MySQL dual-master + Keepalived、MySQL InnoDB Cluster、MySQL NDB Cluster），应使用同一集群内部分节点故障仍不影响数据库整体对外服务的数据库高可用技术保证数据库服务的连续性。
- c) 自建数据缓存应采用集群（如 Redis/Tendis Cluster）或哨兵（如 Redis Sentinel）等满足高可用性要求的架构，并使用缓存数据持久化技术保证缓存数据的一致性和可靠性。
- d) 自建消息队列应采用集群（如 RabbitMQ Cluster）或联邦（如 RabbitMQ Federation）等满足高可用性要求的架构，并使用负载均衡、消息多副本机制、消息持久化等技术保证消息的一致性和可靠性。

附录 A
(规范性)
中信期货有限公司信息系统类别/级别

A.1 概述

信息系统分为重要系统（四级）、A 类系统（三级）、B 类系统（二级）、C 类系统（一级），共四个类别/级别，根据监管机构、中信期货有限公司已发布的相关制度标准综合判定。

A.2 参考的法律、行政法规和规章

《深证证监局关于加强网络安全等级保护工作的通知》（深证局办字〔2022〕204 号）的附件《证券期货业典型网络和信息系統定级表》给出了对信息系统定级的一种依据。

表 A.1 证券期货业典型网络和信息系統定级表

等级级别	标准描述
第三级	1、期货公司及其下属注册交易用户数超 10 万的交易系统； 2、注册的用户数或存储的用户信息数超 1000 万的法人结算系统、客户账户管理系统、呼叫中心系统、风险控制系統、基金销售系统、基金注册登記結算系統、基金清算系統等業務管理、業務支撐系統。
第二级	1、期货公司及其下属机构注册交易用户数超过 100 不足 10 万的交易系统； 2、注册的用户数或存储的用户信息数不足 1000 万的法人结算系统、客户账户管理系统、呼叫中心系统、风险控制系統、基金销售系统、基金注册登記結算系統、基金清算系統等業務管理、業務支撐系統； 3、专业化交易系统、投资交易系统、会计估值核算系统、门户网站、互联网邮件系统。
第一级	不满足上述条件的，定义为一級。

《证券期货业网络安全事件报告与调查处理方法》（证监会公告〔2021〕12 号）的附件《网络和信息系統分类表》给出了对信息系统分类的一种依据。

表 A.2 网络和信息系統分类表

系統类别	标准描述
四类系統	近 20 个交易日日均活跃用户数超过 100 万的实时交易系统及相关行情系統。
三类系統	1、近 20 个交易日日均活跃用户数超过 10 万但不足 100 万的实时交易系统及相关行情系統； 2、近 20 个交易日日均活跃用户数超过 100 万的新股申购、基金销售等非实时交易系统，基金账户数超过 1000 万的基金注册登記、资金清算、会计核算等系統。
二类系統	1、近 20 个交易日日均活跃用户数超过 1000 但不足 10 万的实时交易系统及相关行情系統； 2、近 20 个交易日日均活跃用户数超过 10 万但不足 100 万的新股申购、基金销售等非实时交易系统，基金账户数超过 100 万但不足 1000 万的基金注册登記资金清算、会计核算等系統； 3、近 20 个交易日日均活跃用户数超过 100 万的具有账户开立、银证银期转账信息查看功能等各类非交易业务办理功能的系統。
一类系統	1、近 20 个交易日日均活跃用户数不足 1000 的实时交易系统及相关行情系統；

	2、近 20 个交易日日均活跃用户数不足 10 万的新股申购、基金销售等非实时交易系统，基金账户数不足 100 万的基金注册登记、资金结算、会计核算等系统； 3、近 20 个交易日日均活跃用户数不足 100 万的具有账户开立、银证银期转账信息查看功能等各类非交易业务办理功能的系统； 4、官方网站。
--	--

A.3 信息系统类别/级别

表 A.3 中信期货有限公司信息系统分类定级表

类别/级别	典型系统	网安类别	等级级别
重要（四级）	CTP 综合交易平台、中信期货 APP 系统。	三类系统	第三级
A 类（三级）	1、实时交易系统（次席）及相关的行情系统； 2、非实时交易系统，如风险控制系统、基金销售系统、专业化交易系统、投资交易系统。	二类系统	第二级
B 类（二级）	各类非交易业务办理功能的系统，如法人结算系统、客户账户管理系统、基金注册登记结算系统、基金清算系统、会计估值核算系统、呼叫中心系统。	一类系统	
C 类（一级）	1、运维监控类系统； 2、网络安全类系统； 3、综合办公类系统； 4、不满足上述分类的其他系统。	N/A	第一级

附录 B
(规范性)
应用高可用性设计要求适用情况参考

表 B.1 将不同情况下所适用的应用高可用性设计要求通过表格进行展示，供信息系统开发维护人员在架构设计时参考。

表 B.1 应用高可用性设计要求适用情况

设计要求	适用场景	适用系统类别/级别
总体设计要求		
针对C类系统，可采用单活部署模式，并且至少确保已利用现有基础环境高可用技术（如VMware vSphere HA、H3C CAS HA）来保证服务可用性。对于单次停机时间要求较高的系统，可以考虑采用负载均衡架构和数据库高可用性设计。	生产系统	C类系统
针对B类系统，优先采用双活部署模式。应用服务器应以负载均衡架构部署多份计算资源，并确保承载相应服务的计算资源已经能构成有效冗余；数据库服务器也应采用高可用性设计，以便发生故障时仍能保持服务可用。对数据的完整性、可用性和可恢复性有较高要求的信息系统，优先考虑采用相应的数据库高可用技术。	生产系统	B 类系统
针对重要系统、A类系统，除满足上述第2点要求外，必须采用双活部署模式。同时还应减少中间件、数据库以及应用的启动恢复时间，应使用相应的高可用技术以支持免重启恢复服务和客户端连接自动切换。	生产系统	重要系统、 A 类系统

参 考 文 献

- [1] 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）
 - [2] 证券期货业网络安全事件报告与调查处理方法（证监会公告〔2021〕12 号）
 - [3] 深圳证监局关于加强网络安全等级保护工作的通知（深证局办字〔2022〕204 号）
-