ICS 35. xxx
CCS Lxx

团 体 标 准

T/ISC XXX—XXXX

安全可信中间件能力要求 第 3 部分 分布式数据缓存中间件

Requirements for Secure and Trustworthy Middleware Capability Requirements
Part 3:Distributed Data Caching Middleware

xxxx－xx－xx 发布 xxxx－xx－xx 实施

中 国 互 联 网 协 会 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。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

——

引　言

随着信息技术的快速发展和数字化转型的深入推进，中间件技术作为软件基础设施的重要组成部分，正被广泛应用于互联网、金融、通信、交通、医疗等多个关键领域，显著提升系统间通信效率，降低系统耦合度，增强数据处理能力，有效提升信息系统的整体性能与稳定性。

安全可信中间件往往基于自主研发的软硬件基础设施，具备高度的自主性与良好的兼容性，能够在复杂的系统环境中平稳运行。尤其针对党政、医疗、金融等对数据安全和系统可靠性要求严苛的行业，安全可信中间件提供了有效的数据安全保障机制，能够防范外部恶意攻击，保障数据的机密性、完整性和可用性，对推动重点行业的数字化转型和保障关键领域信息安全具有重要意义。

本系列标准针对中间件产品研发和行业用户应用过程中所面临的安全风险与挑战，依据现行法律法规和行业特定需求，明确安全可信中间件的技术要求和可信验证机制，建立涵盖基础环境适配、软硬件设施建设、平台功能开发的统一标准体系，规范产品研发、应用部署和服务保障等全生命周期管理活动。通过构建科学合理的安全可信体系指引和产品能力量化评估标准，为产业发展提供有力的技术支撑，促进市场可持续健康发展。本文件针对安全可信分布式数据缓存中间件能力要求进行规范。

对本文件中的具体事项，法律法规另有规定的，需遵照其规定执行。

安全可信中间件能力要求 第3部分 分布式数据缓存中间件

1 范围

本文件规定了分布式数据缓存中间件的功能要求、性能要求、可靠性要求、安全性要求、可维护性要求、可扩展性要求和兼容性要求。

本文件适用于从事安全可信分布式数据缓存中间件研发、应用及评价的各类机构。

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 33847—2017 信息技术 中间件术语

GB/T 28168—2011 信息技术 中间件 消息中间件技术规范

3 术语和定义

GB/T 33847—2017、GB/T 28168—2011界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 33847—2017、GB/T 28168—2011中的某些术语和定义。

3.1

中间件 middleware

位于系统软件之上，用于支持分布式应用软件，连接不同软件实体的支撑软件（2.1）。

[来源：GB/T 33847—2017，2.1]

3.2

应用 application

应用程序

通过调用开发接口，在运行过程中使用中间件系统提供功能和服务的各种程序（3.1.1）。

[来源：GB/T 28168—2011，3.1.1]

3.3

集群 cluster

若干消息中间件系统组建为一个群组，对外提供消息的发送、接收和处理功能，宜具备负载均衡和防止单点失效的功能。

[来源：GB/T 28168-2011，3.1.15]

4 符号和缩略语

下列符号和缩略语适用于本文件。

API： 应用编程接日(Application Programming Interface)
TCP/IP：传输控制协议/因特网协议(Transfer Control Protocol/Internet Protocol)
HTTP： 超文本传输协议(Hypertext Transfer Protocol)
JDK： Java开发工具包(Java Development Kit)

5 安全可信要求

安全可信要求须符合《安全可信中间件能力要求 第1部分 总体要求》中5的规定。

6 分布式数据缓存中间件能力要求

6.1 功能要求

6.1.1 安装部署

a) 分布式数据缓存中间件应提供命令行方式启动和停止,宜提供图形化启动和停止操作。
b) 分布式数据缓存中间件应具有单机部署功能。
c) 分布式数据缓存中间件应具有集群部署功能,须实现数据分片和副本同步机制。
d) 分布式数据缓存中间件宜具有虚拟化或容器化等云化部署方式。
e) 分布式数据缓存中间件宜提供图形化的安装和卸载程序,引导用户安装和卸载的全过程。

6.1.2 缓存一致性与数据持久化

a）应提供数据持久化方式，包括RDB快照和AOF日志。
b）应支持外部数据导入，提供工具保证数据的一致性。
c）应支持集群部署模式，提供数据的分片和负载均衡，将数据分布到多个实例上，每个实例存储部分数据。

6.1.3 缓存失效与容错性

a） 应支持缓存失效机制，提供过期策略。
b） 宜支持缓存预热策略自定义（如定时预热、按需预热）。
c） 宜支持缓存穿透保护机制（如布隆过滤器、空值缓存。

6.1.4 性能优化与扩展性

a） 应支持读写分离，提高效率满足高并发需求。
b） 应支持分片变更，支持计算层扩容。
c） 应支持集群在线缩扩容，新增节点时数据应自动重平衡。

6.1.5 集群管理与运维

a） 应支持向导式创建，支持一键式创建集群的配置向导。
b） 应支持支持生命周期管理过程中实例的批量运维能力，包括创建、启动、停止和卸载、升级多个实例。
c） 应支持集群操作，支持增减分片和节点。
d） 宜支持慢请求分析、Key分析及诊断报告。
e） 宜支持数据迁移可视化监控，实时展示节点和分片状态。

6.1.6 灵活性与数据结构支持

a） 应支持包括String、List、Hash、Set、SortedSet以及Stream等多种数据类型。
b） 宜支持 Bitmaps、HyperLogLog、Geo 以支持高级查询功能。
c） 应支持Lua脚本以及LRU驱动。

6.1.7 配置可视化

a） 宜支持配置可视化，提供更加简洁的操作，提供对常用操作可视化的管理能力，包括日志，主从复制，集群同步，持久化等配置项。

6.1.8 日志

a） 应支持日志文件按照时间、文件大小进行轮转，避免日志过大导致占用过多的存储空间。

6.2 性能要求

6.2.1 数据缓存处理能力

a） 应测试中间件处理读取请求能力，读取延迟应符合产品性能指标清单。
b） 应测试中间件处理写入请求能力，写入延迟应符合产品性能指标清单。
c） 应测试中间件的吞吐量，吞吐量应符合产品性能指标清单。
d） 应测试中间件的命中率，即命中缓存的比例，缓存利用率。
e） 应测试高负载下中间件性能。

6.3 可靠性要求

a） 应能保证业务容错性，对错误操作进行执行询问，恢复操作不影响正常运行。
b） 应具备业务稳定性，保证在一定负载运行情况下仍能正常提供服务。应保证在多种误操作下仍能稳定运行。
c） 应具备故障切换与恢复能力，单个节点出故障不影响业务平台的功能性。
d） 应能保证数据的一致性,确保数据在缓存中与存储系统的一致性,在故障发生后能被正确恢复。
e） 应支持数据备份和复制功能，当某节点数据丢失可从备份进行恢复。
f） 宜支持集群大于半数主节点同时宕机时集群状态可用，适用异地容灾实时热备场景。

6.4 安全性要求

a） 应提供对国密算法的支持，以国密算法对客户端和实例的通道进行加密。
b） 应支持屏蔽一些高危命令，避免误操作导致的严重事故。
c） 应支持敏感信息加密，对实例通讯密码进行加密处理，确保实例被安全访问。
d） 应进行访问控制与身份鉴别，应支持自定义用户操作权限，严格管控不同用户的使用权限。
e） 应支持TLS数据加密（支持配置TLS的最低版本），保证数据链路安全。
f） 应支持白屏方式管理账号和权限配置。
g） 应支持网络白名单配置，避免外部攻击。
h） 应隔离业务功能和管理功能，防止不当业务操作（如客户端执行了错误的config set等）影响系统正常运行。

6.5 可维护性要求

5.5.1 日志管理

a) 应提供数据缓存中间件系统的日志功能，记录消息处理过程中的错误信息，日志级别可以按需进行调整。

5.5.2 版本升级

a) 应支持系统增量升级功能，对系统部件、安全补丁等升级。
b) 应支持在线升级和离线升级，且升级不得修改破坏用户数据，不得影响原有软硬件兼容性。
c) 应支持升级回退机制，能卸载已升级的软件包，恢复系统原有状态；如升级为不可回退，则系统升级前以显式的提示告知用户。

5.5.3 监控告警

a) 应提供用于监控和管理消息中间件的API接口，供外部监控管理运维系统调用。
b) 应提供必要的命令行工具、图形化的监控管理工具。

5.5.4 容灾备份

a) 应提供合理的容灾备份技术来满足客户对可用性的要求，容灾包括但不限于数据、应用、业务层面，备份包括但不限于备援中心、本地磁带备份，异地保存、热备份站点备份等。
b) 应提供备份恢复能力，通过灾备快速恢复经营生产。
c) 专用模式应提供多副本数据设计，单份数据损坏应提供快速恢复。

6.6 可扩展性要求

a) 应支持使用第三方语言扩展现有的产品能力。
b) 应支持Redis标准协议（RESP）以兼容现有客户端。
c) 应支持插件化架构，允许通过模块扩展新功能。
d) 宜提供SDK多语言支持，降低接入成本。

6.7 兼容性要求

a) 应基于安全可信CPU、操作系统、数据库等。
b) 应在所有应用平台上提供一致的应用开发接口，以实现应用程序在不同平台上的迁移。
c) 应支持一键式迁移Redis数据至产品中，使用RDB文件，或者PSync、Scan命令进行数据迁移。