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5部分 负载均衡中间件

Requirements for Secure and Trustworthy Middleware Capability Requirements
Part 5:Load Balancing 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负载均衡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5部分 负载均衡中间件

1 范围

本文件规定了负载均衡中间件的功能要求、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负载均衡中间件研发、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

3 术语和定义

GB/T 33847—2017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

安全可信 secure and trustworthy

是对基于自主可控技术构建的信息技术产品或解决方案的描述，指其符合安全可靠要求。

注：本文中意义同“安全可靠”。

3.3 **上游节点 Upstream Node**

提供消息发送、接收或处理能力的中间件实例，是负载均衡系统请求分发的目标。

3.4

负载均衡策略 Load Balancing Strategy

用于将消息或请求分发至多个节点的算法，例如轮询、IP哈西、最少连接、哈希等。

3.5

主动健康检查 Active Health Check

以预设频率主动向后端节点发起探测请求，用于判定其是否可用，确保请求不会被转发至故障节点。

3.6

故障转移 Failover

当某个节点因故障不可用时，系统自动将请求转发到其他可用节点，避免服务中断。

3.7

会话保持 Session Persistence

保证来自同一客户端的请求在一段时间内始终路由到同一个后端节点,用于状态相关的消息处理场景。

3.8

反向代理 Reverse Proxy

负载均衡中间件作为客户端与服务节点之间的中介，统一接收外部请求并转发到后端节点。

4 符号和缩略语

下列符号和缩略语适用于本文件。

API： 应用编程接口(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)
HTTPS： 安全超文本传输协议(Hypertext Transfer Protocol Secure)
URL： 统一资源定位器（Uniform Resource Locator）
UDP： 用户数据报协议（User Datagram Protocol）
IP： 互联网协议地址(Internet Protocol Address)
DNS： 域名系统(Domain Name System)

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 负载均衡中间件能力要求

6.1 功能要求

6.1.1 安装部署

a) 应在测试环境下具备安装运行与卸载功能。
b) 应对安装过程中关联的组件自动安装或者具有安装指导，无需用户单独配置。
c) 宜支持覆盖安装，无需卸载后再安装。
d) 宜支持卸载误操作确认，卸载后支持一键安装运行。
e) 宜支持云原生，提高系统的灵活性、可维护性和容错能力。

6.1.2 负载均衡

a） 应提供带权轮询负载均衡算法，根据服务器的不同处理能力，给每个服务器分配不同的权值进行选择，将请求分发到后端应用服务器节点。

b） 应提供IP哈希负载均衡算法，根据客户端 IP 地址的前三个八位字节进行请求分配，将请求分发到后端应用服务器节点。
c） 应提供URL哈希负载均衡算法，按照访问的URL的哈希结果分配请求，将请求分发到后端应用服务器节点。
d） 应提供最小连接负载均衡算法，向活跃连接数最少的服务器转发请求，将请求分发到后端应用服务器节点。
e） 应提供哈希负载均衡算法，根据特定的键值分发请求，将请求分发到后端应用服务器节点。
f） 宜提供随机负载均衡算法，随机选择服务器并将请求转发到活动连接数较少的服务器。
g） 宜支持一致性哈希负载均衡算法，根据特定的键值做一致性哈希计算后，将请求分发到相应的后端服务器节点。

6.1.3 静态资源缓存

a） 宜支持主动回源，在缓存内容过期后立即返回旧缓存，并异步拉取新内容更新缓存。
b） 应支持静态资源压缩，减少网络传输流量。
c） 宜支持缓存策略设置，如按文件类型、URL 规则、热点资源进行缓存。

6.1.4 配置与管理

a） 应支持对用户进行管理，包括用户添加、编辑、删除。
b） 应支持提供操作审计。
c） 应支持添加Nginx第三方模块，增强核心能力。
d） 应支持动态加载或卸载产品负载中间件模块，实现可插拔管理。
e） 应支持对配置参数的查看和修改。
f） 应支持服务发现集成，实现动态扩展与缩减，简化配置管理，提高系统灵活性。
g） 宜支持多租户能力，能支持多租户配置以及基于租户的访问控制和配额控制。

6.1.5 会话管理与路由策略

a） 宜支持会话保持特性，同一用户会话的先后请求分配到相同的后端服务器节点。
b） 宜支持基于地理位置的路由策略，优先分配用户至就近节点。

6.1.6 协议支持与负载均衡模式

a） 应支持四层（TCP、UDP）或七层（HTTP等）协议的负载均衡。

6.2 性能要求

6.2.1 容量特性要求

a） 产品正常运行情况下CPU利用率不超过85%。
b） 产品正常运行情况下内存利用率不超过80%。
c） 使用压测工具进行性能压测，使CPU、内存其中之一系统资源达到100%，然后查看当前并发请求数。

6.3 可靠性要求

a） 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。

6.3.1 基础能力

a) 应支持实例的高可用，实现故障转移，避免单点故障。
b) 应支持处理大量的并发连接。

6.3.2 自适应

a) 同一端口同时支持国内https、国际https。

6.3.3 备份还原

a) 应支持支持系统的备份和还原。
b) 应支持还原到指定备份点。

6.3.4 容错能力

a) 应支持在部分节点服务出现故障的情况下仍保证产品的服务能力，能够进行故障监测，并具备自动切换和重连机制。
b) 应支持请求重试，通过适当的重试机制，解决短暂故障、临时故障等问题。
c) 应支持熔断降级，避免系统过载并使得故障不蔓延，提供降级服务或备用方案以保证系统可用性。
d) 应支持多活数据中心流量调度，实现跨地域容灾。

6.3.5 健康检查能力

a) 应支持主动健康检查，定期通过实际请求进行活检，以确保后端服务的正常运行。
b) 宜支持被动健康检查，在代理请求过程中会自动的监测每个后端服务器对请求的响应状态。

6.3.6 智能 DNS 解析

a) 宜支持智能DNS解析，结合负载均衡状态动态调整域名解析结果。

6.4 安全性要求

6.4.1 系统安全性要求

a) 应支持隐藏版本。
b) 应支持日志记录和监控系统。
c) 应支持全量记录操作日志。
d) 宜支持操作审计功能。

6.4.2 数据安全性要求

a) 应支持传输加密，支持客户端与服务器、服务器与服务器之间的加密通信。
b) 应支持对常见的安全攻击进行拦截。

6.4.3 反向代理

a) 应支持将请求反向代理到不同应用服务器或不同的应用服务器集群。

6.5 可维护性要求

5.5.1 日志管理

a) 应提供负载均衡中间件的日志功能，记录运行过程中的错误信息，日志级别可以按需进行调整。
b) 应支持访问日志功能，记录客户端请求的关键信息，如请求时间、请求方法、请求 URL、响应状态码、响应时间、客户端 IP 等，便于流量分析和故障排查。
c) 应支持访问日志的按需开启和关闭，允许用户灵活控制日志功能，避免对性能造成不必要的影响。
d) 应支持访问日志的格式自定义，允许用户根据业务需求定义日志字段及输出格式。

5.5.2 版本升级

a) 应支持流量镜像，验证新版本的处理效果，发现潜在问题而不影响用户体验。
b) 宜支持灰度发布，保证版本间平滑过渡和快速回滚。

5.5.3 监控告警

a) 应提供用于监控和管理负载均衡中间件的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。

6.6 可扩展性要求

a) 应支持用户扩展和自定义API服务，满足用户需求。
b) 应支持自定义健康检查脚本，适配复杂业务场景。
c) 宜提供插件市场，允许用户按需安装第三方扩展模块。
d) 宜支持自定义负载均衡算法，根据算法实现，将请求分发到后端应用服务器节点。

6.7 兼容性要求

a) 应基于安全可信CPU、操作系统等。