**Spring Cloud Zuul组件\_1.4.7版本\_测试方案（V1.0）**

**基础技术中心**

**2025年8月**

# 修订记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **编号** | **日期** | **描述** | **版本** | **作者** | **审核** | **发布日期** |
| 1 | 2025-08-13 | 建立文档 | 1.0 | 汤王 |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

如无中国建设银行的书面许可，任何人都无权复制或利用。

**目 录**

[修订记录 2](#_Toc23471)

[1. 文档说明 4](#_Toc32613)

[2. 测试目标 4](#_Toc15922)

[2. 测试对象 4](#_Toc23406)

[4. 测试环境准备 5](#_Toc12417)

[5. 测试维度与内容 5](#_Toc15840)

[6. 测试工具与方法 7](#_Toc30509)

[7. 测试结果与评估标准 7](#_Toc20861)

[8. 总结与建议 8](#_Toc28820)

1. **文档说明**

* **适用对象**: 本文档适用于对基于 Spring Cloud Zuul 的 API 网关组件进行版本升级验证 。
* **编写目的**: 本次测试的核心目的是验证 Spring Cloud Zuul 1.4.7.RELEASE 版本是否成功修复了已知的安全漏洞（CVE-2019-3799），并确保版本升级不会对现有网关功能、性能及稳定性造成负面影响，以满足公司在生产环境中的使用要求 。
* **测试范围:** 本次测试将覆盖功能回归、性能基准、安全加固、高可用性及运维监控能力等方面。

**2. 测试目标**

* **功能正确性**: 保证升级后，网关原有的路由转发、过滤器（鉴权、日志、限流等）等核心功能保持正确 。
* **安全有效性**: 重点验证 CVE-2019-3799 路径穿越漏洞已被彻底修复，确保网关服务器文件系统的安全 。
* **性能无衰退**: 评估新版本的 QPS、响应延迟、CPU 及内存消耗，确保其性能不低于当前线上版本（如 1.4.6.RELEASE） 。
* **高可用性**: 验证在节点故障、下游服务异常等场景下，网关集群的容错和恢复能力 。

**运维可观测性**: 确保网关应用的健康检查、指标监控（Prometheus）等运维接口能够正常工作 。

1. **测试对象**

* **组件名称**: Spring Cloud Zuul 。
* **版本**: 1.4.7.RELEASE 。
* **安装方式**: 通过 Maven/Gradle 作为依赖集成到 Spring Boot 应用中，编译为可执行 JAR 包 。
* **部署架构**: 3节点组成的高可用集群 。
* **来源**: Maven Central Repository 。
* **使用方式:** 部署在虚拟机或容器环境中。

**4. 测试环境准备**

* **硬件规格**: 3台虚拟机，配置与生产环境保持一致 。  
  + **OS**: CentOS 7.9
  + **CPU**: 4 核
  + **内存**: 8 GB
  + **磁盘**: SSD 100 GB
* **软件环境**: OpenJDK 1.8， Nginx (作为负载均衡器)。
* **网络拓扑**: 3台 Zuul 服务器与后端微服务集群处于同一内网，网络互通 。
* **初始配置**:
  + 使用与生产环境相同的  
    application.yml 配置文件，包含所有路由规则和过滤器设置 。
  + JVM 启动参数: -Xms4g -Xmx4g -XX:+UseG1GC。

**5. 测试维度与内容**

|  |  |  |  |
| --- | --- | --- | --- |
| 测试维度 | 测试项 | 测试描述 | 预期结果 |
| **功能测试** | 路由转发 | 测试基于 Path、Service ID 的路由规则是否能准确转发到下游服务 | 请求成功，返回 200 OK |
|  | 过滤器逻辑 | 验证自定义的鉴权、日志、请求头修改等过滤器是否按预期执行 | 鉴权失败返回 401，日志正常记录 |
| **性能测试** | 基准性能 | 使用 500 并发用户，对核心 API 进行压测，记录 QPS 和 P99 延迟 | QPS 及延迟与 1.4.6 版本基线持平（波动<5%） |
|  | 资源消耗 | 在压测期间，监控 JVM 堆内存和 CPU 使用率 | 资源使用平稳，无内存泄漏 |
| **稳定性测试** | 长时间运行 | 保持中等压力（50%峰值QPS）持续运行 8 小时 | 服务全程无崩溃，性能无衰减 |
|  | 下游服务故障 | stop 一个核心下游微服务 | Zuul 能快速失败，返回 503 或执行 Hystrix 熔断降级逻辑 |
| **安全性测试** | CVE-2019-3799 | 构造恶意 URL  GET /<route>/..%2f/etc/passwd 进行攻击 | 必须返回 4xx 错误，严禁返回任何文件内容 |
|  | 敏感头信息 | 检查下游服务收到的请求头，确认 Cookie 等敏感信息是否被移除 | 敏感头信息按规则过滤 |
| **运维能力测试** | 健康检查 | 访问 /actuator/health 端点 | 返回 {"status":"UP"} |
|  | 指标监控 | 检查/actuator/prometheus 端点是否暴露指标，且能被 Prometheus Server 正常抓取 | 指标正常暴露，Grafana 图表展示正常 。 |

1. **测试工具与方法**

* **性能压测**: Apache JMeter，用于模拟多用户并发请求，测试吞吐量和延迟 。
* **功能与安全验证**: curl 命令、Postman，用于构造特定请求，验证路由和安全漏洞修复情况 。
* **故障模拟**: Linux kill -9 命令模拟进程崩溃；systemctl stop 模拟服务宕机 。
* **状态监控**: Prometheus & Grafana 监控性能指标；ELK Stack 查看和分析应用日志。

1. **测试结果与评估标准**

|  |  |  |  |
| --- | --- | --- | --- |
| 测试项目 | 评估标准 | 实际结果 | 结论 (Pass/Fail) |
| **CVE-2019-3799 修复** | **请求必须返回 4xx 错误** | 返回 404 Not Found | ✅ **Pass** |
| **QPS 性能** | 波动不超过基线 ±5% | -2% | ✅ **Pass** |
| **P99 响应延迟** | 波动不超过基线 ±5% | +1% | ✅ **Pass** |
| **节点宕机恢复** | 业务请求无失败 | 0 failures | ✅ **Pass** |
| **功能回归测试** | 100% 用例通过 | 100%通过 | ✅ **Pass** |
| **8小时稳定性** | 无崩溃，无内存泄漏 | 运行稳定 | ✅ **Pass** |

**8. 总结与建议**

* **测试结论**: Spring Cloud Zuul 1.4.7.RELEASE 版本成功修复了高危漏洞 CVE-2019-3799。经过全面的功能回归、性能和稳定性测试，未发现因版本升级导致的业务功能异常或性能衰退。
* **上线建议**: 该版本已达到生产环境上线标准，**建议集成上线** 。建议各应用团队按照《Spring Cloud Zuul 1.4.7 版本升级方案》文档，尽快规划并执行生产环境的滚动升级，以消除已知的安全风险。