|  |  |
| --- | --- |
| ICS | 35.080 |
| CCS | L 73 |

|  |
| --- |
| 4102 |

开封市地方标准

DB4102/T XXXX—XXXX

软件系统运维技术规范

征求意见稿

2024 - XX - XX发布

2024 - XX - XX实施

开封市市场监督管理局  发布

目次

[前言 II](#_Toc165989795)

[1 范围 1](#_Toc165989796)

[2 规范性引用文件 1](#_Toc165989797)

[3 术语和定义 1](#_Toc165989798)

[4 运维人员要求 2](#_Toc165989799)

[4.1 资格证书和专业认证 2](#_Toc165989800)

[4.2 技能和经验要求 2](#_Toc165989801)

[4.3 沟通和团队协作 2](#_Toc165989802)

[4.4 培训和合法性意识 2](#_Toc165989803)

[5 准备工作 3](#_Toc165989804)

[5.1 运维目标和计划 3](#_Toc165989805)

[5.2 风险评估和措施 3](#_Toc165989806)

[5.3 环境检查和工具准备 3](#_Toc165989807)

[5.4 人员培训和分配 3](#_Toc165989808)

[5.5 文档准备和变更记录 3](#_Toc165989809)

[5.6 通信和协作机制 4](#_Toc165989810)

[5.7 应急预案 4](#_Toc165989811)

[6 现场运维操作 4](#_Toc165989812)

[6.1 系统监控 4](#_Toc165989813)

[6.2 故障诊断与响应 4](#_Toc165989814)

[6.3 数据备份与恢复 4](#_Toc165989815)

[6.4 安全检查和权限审核 5](#_Toc165989816)

[7 数据后处理 5](#_Toc165989817)

[7.1 数据收集与整理 5](#_Toc165989818)

[7.2 性能数据分析 5](#_Toc165989819)

[7.3 安全事件分析 5](#_Toc165989820)

[7.4 故障分析与预防 5](#_Toc165989821)

[7.5 报告生成 6](#_Toc165989822)

[7.6 性能优化 6](#_Toc165989823)

[8 软件系统管理及维护 6](#_Toc165989824)

[8.1 软件系统管理 6](#_Toc165989825)

[8.2 软件系统维护 6](#_Toc165989826)

1. 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。

本文件由河南大学软件学院提出。

本文件由河南大学信息化管理办公室归口。

本文件起草单位：河南大学软件学院、河南省智能数据处理工程研究中心、河南省智能网络理论与关键技术国际联合实验室。

本文件主要起草人：张济仕、于俊洋、韩志杰、甘志华、丁爽、渠慎明、王光辉、程普、王春华、申展。

软件系统运维技术规范

* 1. 范围

本文件规定了软件系统运维技术的术语和定义、运维人员要求、准备工作、现场运维操作、数据后处理、软件系统管理及维护。

本文件适用于软件系统运维工作。

* 1. 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 5271 信息技术 词汇

GB∕T 11457-1995 软件工程术语

GB/T 8567 计算机软件文档编制规范

* 1. 术语和定义

GB/T 5271、GB∕T 11457-1995界定的以及下列术语和定义适用于本文件。

运维人员

对软件系统进行软硬件维护的工作人员。

软件更新

对原有软件进行问题修复、功能优化、界面修改、性能提升等方面的操作形成对原有版本的小范围的升级，不涉及架构的变更，会保留上一个版本的大部分功能和使用习惯等。

系统配置

通过在软件生命周期的不同的时间点上对软件配置进行标志并对这些被标志的软件配置项的更改进行系统控制，从而达到保证软件产品的完整性和可溯性的过程。

系统监控

运用软件工具实时跟踪和分析IT基础设施的性能和健康状况的过程，包括对硬件、软件、网络和服务的监控。

性能优化

通过技术手段改善系统性能的过程，这可能包括调整配置、升级硬件、优化代码等策略。

* 1. 运维人员要求
     1. 资格证书和专业认证
        1. 基础资格

所有运维人员应至少拥有计算机科学或相关领域的大专及以上学历，或相等的技术培训证书。

* + - 1. 专业认证

要求运维人员获得专业认证，如Microsoft Certified Solutions Expert (MCSE)、Cisco Certified Network Associate (CCNA)、Certified Information Systems Security Professional (CISSP)、ITIL Foundation等，证明他们在具体技术领域的专业知识和技能水平。

* + 1. 技能和经验要求
       1. 技术技能

运维人员必须熟悉操作系统（如Windows、Linux）、数据库管理、网络、云平台服务（如AWS、Azure）等关键技术。

* + - 1. 故障排除技能

运维人员应该具有能够快速有效地识别和解决软件、硬件和网络问题的能力。

* + - 1. 自动化和脚本编写技能

运维人员应该具备使用自动化工具（如Ansible、Puppet）、脚本语言（如Python、Shell）和最新的安全防护技术的能力，以提高工作效率。

* + - 1. 经验要求

运维人员至少有三年的网络管理经验或五年的数据库维护经验，确保他们能够处理复杂的软件系统运维问题。

* + 1. 沟通和团队协作
       1. 沟通技巧

运维人员能够清晰有效地与团队其他成员、管理层和非技术人员沟通技术问题和解决方案。

* + - 1. 团队协作

运维人员应具备良好的团队合作精神，能够在跨部门项目中进行有效协作。

* + 1. 培训和合法性意识
       1. 定期培训

运维人员应根据自身的现有技能和未来岗位需求，定期接受最新技术和实践操作的相关培训，以增强实战经验和适应不同岗位的能力。

* + - 1. 合法性意识

运维人员必须遵守和了解相关的法律、法规和组织政策，特别是涉及数据保护和隐私的领域。

* 1. 准备工作
     1. 运维目标和计划
        1. 运维目标设置

明确运维活动的目标和预期成果，如提升系统稳定性、减少故障响应时间等。

* + - 1. 运维计划制定

基于运维目标，制定具体的运维计划，包括定期维护、监控策略、安全审计、备份和恢复等。

* + 1. 风险评估和措施
       1. 风险评估

识别和评估潜在的运维风险，如硬件故障、软件漏洞、安全威胁等。

* + - 1. 风险应对措施

针对每一种风险，制定详细的应对措施和备份计划。例如，确保数据备份和恢复流程的有效性，以及在网络故障时启用备用通信通道。

* + 1. 环境检查和工具准备
       1. 环境检查

运维活动开始前，对所有系统组件进行详细检查，包括软件版本、网络配置、硬件状态、存储空间等，确保所有系统参数符合预设标准、所有组件都能正常工作。

* + - 1. 工具准备

确保所有必要的运维工具和软件都已安装、配置并处于最佳状态，包括监控软件、自动化工具、安全工具等。

* + 1. 人员培训和分配
       1. 人员培训

确保所有运维人员都接受了必要的培训，包括新工具的使用、最新的运维实践和安全政策。

* + - 1. 角色和责任

明确每个运维团队成员的角色和责任，确保在运维活动中每个任务都有明确的负责人，确保每个角色的职责与个人的技能和经验相匹配。

* + 1. 文档准备和变更记录
       1. 文档准备

准备和软件更新运维相关文档，包括系统架构、配置管理文档、运维手册等，按照GB/T 8567的规定执行，确保文档的准确性和完整性。

* + - 1. 变更记录

建立和维护变更管理记录，记录所有系统和配置的变更历史，以便于追踪和审计。

* + 1. 通信和协作机制
       1. 沟通计划

制定运维期间的沟通计划，包括团队内部沟通、与其他部门的协作、以及如何向管理层报告运维状态。

* + - 1. 协作工具

确定并准备协作工具，如即时通讯软件、项目管理工具等，以支持团队协作和信息共享。

* + 1. 应急预案

准备应对可能发生的各种紧急情况的预案，包括数据丢失、系统故障、安全事件等，确保能够迅速恢复正常操作。

* 1. 现场运维操作
     1. 系统监控
        1. 实时监控

利用监控工具（如 Prometheus 和 Grafana等）实时跟踪系统性能指标，包括CPU使用率、内存使用、磁盘空间和网络流量等。

* + - 1. 告警响应

对于系统生成的告警，可以通过 Grafana进行性能趋势分析并立即进行评估，确定是否需要采取行动，如需要，按照预定的故障响应流程进行处理。

* + 1. 故障诊断与响应
       1. 故障诊断

当监控系统报告问题或用户报告故障时，首先进行快速诊断，可以使用 Wireshark 进行网络诊断和数据包分析，使用 Sysinternals Suite 分析Windows系统问题，确定问题范围和严重性。

* + - 1. 快速响应

基于故障的性质和严重程度，快速采取行动，可能包括重启服务、回滚变更或应用补丁等，例如，在数据丢失或系统崩溃情况下，可以通过 Veeam 或 Acronis 进行系统和数据的快速恢复。

* + 1. 数据备份与恢复
       1. 定期备份

执行定期的数据备份计划，包括关键数据库、应用数据和系统配置的备份。

* + - 1. 恢复测试

定期进行备份恢复测试，确保在需要时能够快速、准确地恢复数据。

* + 1. 安全检查和权限审核
       1. 安全检查

定期执行系统安全扫描，可以使用 Bitdefender 或 Norton 进行病毒防护和系统安全检查，包括漏洞扫描和病毒检查，识别和修复安全漏洞。

* + - 1. 权限审核

审核系统访问权限，确保只有授权用户才能访问敏感资源和数据。

* 1. 数据后处理
     1. 数据收集与整理
        1. 日志聚合

将来自不同来源的日志数据（如应用程序日志、系统日志、安全日志）汇集到一个中央日志管理系统中，如 ELK Stack（Elasticsearch, Logstash, Kibana）或 Splunk，便于分析、存储、索引和搜索。

* + - 1. 数据清洗

对收集到的数据进行清洗，去除无关数据，纠正错误信息，以保证数据的准确性和完整性。

* + 1. 性能数据分析
       1. 性能趋势分析

分析系统性能指标（如响应时间、吞吐量、资源利用率）的变化趋势，可以通过数据分析工具如 Apache Spark 或 Hadoop，对收集的大数据进行处理和分析，识别系统性能瓶颈或潜在的性能问题。

* + - 1. 基准比较

将当前性能数据与历史性能数据或预设的性能基准进行比较，评估系统性能是否符合预期。

* + 1. 安全事件分析
       1. 安全日志分析

分析安全日志，识别异常行为或潜在的安全威胁，如未授权访问、恶意软件活动、数据泄露等。

* + - 1. 漏洞评估

根据安全扫描结果，评估系统中存在的安全漏洞的严重程度和风险，制定相应的补救措施。

* + 1. 故障分析与预防
       1. 故障分析

对系统故障事件进行深入分析，确定故障的根本原因，以防止未来的重复发生。

* + - 1. 预防措施

基于故障分析结果，提出具体的预防措施和改进建议，提高系统的可靠性和稳定性。

* + 1. 报告生成

根据数据分析结果生成详细的报告，也可以利用报表工具如 Tableau 或 Power BI生成可视化的报告，包括性能评估报告、安全分析报告、故障分析报告等，为管理层提供决策支持。

* + 1. 性能优化

定期对系统进行性能评估和优化，分析性能数据，识别瓶颈，实施必要的硬件或软件升级；通过使用高效的负载均衡和资源管理策略，优化数据库查询、服务器配置和应用程序代码，以提高系统的效率。

* 1. 软件系统管理及维护
     1. 软件系统管理
        1. 资产管理

维护软件系统资产清单，包括软件应用、服务器、网络设备及其配置信息，确保所有资产信息准确、更新及时。

* + - 1. 配置管理

通过配置管理数据库跟踪和管理软件系统的配置项及其变更，确保系统配置的一致性和完整性。

* + - 1. 许可证管理

管理和审计软件许可证，确保软件使用合法且符合许可协议要求。

* + - 1. 性能监控

实时监控系统性能指标，及时发现并解决可能影响系统性能的问题。

* + - 1. 安全管理

实施安全策略和控制措施，定期进行安全审计，确保系统免受安全威胁和攻击。

* + 1. 软件系统维护
       1. 定期审查

定期审查系统性能、安全和功能，识别需要改进或软件更新的地方。

* + - 1. 补丁管理

定期检查并应用软件和操作系统的安全补丁和软件更新，以修复已知漏洞。

* + - 1. 故障恢复

对于发现的系统问题，快速响应并进行故障修复，最小化对业务的影响。

* + - 1. 数据备份和恢复

执行定期的数据备份计划，并确保在数据丢失或系统故障时可以快速恢复。

* + - 1. 技术支持

为系统用户提供技术支持服务，解决用户在使用过程中遇到的问题。

