信息技术应用创新系统  
集中运维管理平台建设技术规范

（草稿）

2025年6月

版本控制

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **时间** | **人员** | **变动** | **内容** | **备注** |
|  | 0531 | 谭可久 | 初 | 编制框架 |  |
|  | 0613 | 谭可久 | 更 | 添加基础条款、格式处理 |  |
|  | 0614 | 谭可久 | 添 | 添加用户管理、知识库管理  删除性能要求 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

目 录

[前 言 III](#_Toc21799)

[1 范围 1](#_Toc29498)

[2 规范性引用文件 1](#_Toc26846)

[3 术语、定义 1](#_Toc21576)

[4 缩略语 2](#_Toc14649)

[5 概述 3](#_Toc12358)

[6 平台总体要求 3](#_Toc18223)

[6.1 平台定位与目标 3](#_Toc1330)

[6.2 总体架构要求 3](#_Toc7713)

[6.3 遵循标准与规范要求 3](#_Toc2266)

[6.4 信创生态兼容性要求 3](#_Toc23760)

[6.5 平台安全总体要求 3](#_Toc18047)

[7 平台技术架构要求 3](#_Toc13038)

[7.1 分层架构模型 4](#_Toc8857)

[7.2 网络架构要求 4](#_Toc24674)

[7.3 高可用与高可靠要求 4](#_Toc15769)

[7.4 可扩展性要求 4](#_Toc27506)

[7.5 开放性与集成性要求 4](#_Toc13788)

[8 平台功能要求 4](#_Toc11630)

[8.1 终端管理 4](#_Toc2614)

[8.2 工单管理 5](#_Toc4503)

[8.3 用户管理 5](#_Toc10674)

[8.4 知识管理 5](#_Toc86)

[8.5 远程运维管理 6](#_Toc25215)

[8.6 自动化运维管理 6](#_Toc247)

[8.7 报表与可视化分析 6](#_Toc12582)

[9 平台安全要求 7](#_Toc11915)

[9.1 身份认证 7](#_Toc14962)

[9.2 网络安全 7](#_Toc16550)

[9.3 数据安全 7](#_Toc19904)

[9.4 行为审计 7](#_Toc12033)

[9.5 自身安全防护 8](#_Toc31365)

[9.6 特权账号管理 8](#_Toc28498)

[10 平台接口要求 8](#_Toc23374)

[10.1 数据采集接口 8](#_Toc1760)

[10.2 单点登录（SSO） 8](#_Toc2444)

[10.3 管理控制接口 8](#_Toc13711)

[10.4 数据共享接口 8](#_Toc2275)

[10.5 接口安全规范 9](#_Toc28285)

[11 平台部署与实施要求 9](#_Toc11740)

[11.1 部署架构 9](#_Toc12908)

[11.2 用户培训要求 9](#_Toc25377)

[12 平台测试与验收要求 9](#_Toc17032)

[12.1 功能性测试 9](#_Toc2481)

[12.2 性能测试 9](#_Toc5706)

[12.3 安全性测试 9](#_Toc21428)

[12.4 可靠性测试 10](#_Toc5511)

[12.5 信创环境兼容性测试 10](#_Toc14029)

[12.6 验收流程与标准 10](#_Toc24558)

[13 附录 10](#_Toc14879)

前 言

本文件按照GB/T 1.1一2020《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这些专利的责任。

本文件由广西电子学会提出并归口。

本文件起草单位：南宁市迈越软件有限责任公司、广西数广信创信息技术有限公司、河池学院。

本文件主要起草人：×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××、×××。

信息技术应用创新系统 集中运维管理平台建设技术规范

1. 范围

本技术规范规定了集中运维管理平台的术语定义、总体要求、技术架构、功能、性能、安全、接口、部署实施及测试验收等内容，适用于平台的设计、开发、部署、运维及验收等环节，为平台的全生命周期管理提供技术依据。

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规范必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本规范；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB/T 18336.1-2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 18336.3-2015信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069-2022信息安全技术 术语

GB/T 35273-2020信息安全技术 个人信息安全规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 2887-2011 计算机场地通用规范

GB/T 9387.2-1995 信息处理系统 开放系统互连 安全体系结构

GB/T 25068.1-2020 信息安全技术 网络安全技术 网络安全管理数据格式

1. 术语、定义

GB/T 18336.1一2015、GB/T 18336.3一2015和GB/T 25069一2022界定的以及下列术语和定义适用于本文件。

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源：GB/T25069一2022,3.616]

集中运维管理平台 Centralized Operations and Maintenance Management Platform

通过统一的技术架构与管理界面，对组织中的硬件设备、软件系统、云资源、应用程序等各类IT资产集中监控、远程管理和远程运维的系统。

终端Terminal

是运行国产操作系统、具备命令行或图形交互能力的设备，用于访问系统、运行程序和进行用户操作。

远程运维 Remote Operations and Maintenance

通过网络技术，客服工程师对终端用户的设备进行远程操作，以解决故障或进行维护的过程。

工单管理 Ticket Management

对终端用户提交的故障申报进行全流程管理，包括工单的创建、分配、处理、跟踪和关闭等环节。

日志管理 Log Management

对平台内所有操作和登录事件进行记录、存储和分析，以便事后审计和故障排查。

高可用性 High Availability (HA)

通过技术手段确保平台在主服务器发生故障时，能够快速切换到备份服务器，保证服务的连续性和数据的安全性。

1. 缩略语

下列缩略语适用于本文件。

B/S：浏览器 / 服务器架构(Browser/Server)

UEFI：统一可扩展固件接口(Unified Extensible Firmware Interface)

IP：互联网协议地址(Internet Protocol Address)

DNS:域名系统(Domain Name System)

SSO：单点登录(Single Sign-On)

信创系统：信息技术应用创新系统(Information Technology Application Innovation / ITA 系统)

1. 概述

本标准旨在规范信创系统中集中运维管理平台的建设与实施过程，为信创系统的高效、安全、协同运行提供统一、标准化的运维支撑。本规范围绕平台的架构设计、功能模块、接口规范、安全要求、运维流程管理等方面展开，提出了一套适用于信创环境下的集中运维管理平台的建设原则和技术标准。

通过本规范的实施，能够有效提升信创系统的运维效率，增强系统稳定性与安全性，实现对多源异构系统的统一监控、故障预警、资源调度和日志分析，为政府、企业及各类组织在推进国产化替代和信息化建设过程中提供技术依据和实施指导。

1. 平台总体要求
   1. 平台定位与目标

平台定位为云终端集中运维管理解决方案，目标是提高运维效率，降低人力成本，缩短故障处理时间，保障业务连续性，确保系统稳定可靠运行。

* 1. 总体架构要求

采用 B/S 架构，平台由集中管理端和客户端组成，集中管理商安装在服务器上，客户端安装在云终端上。通过管理端的 Web 界面实现集中式的运维管理模式，支持多终端接入和多用户协作。

* 1. 遵循标准与规范要求

遵循国家相关法律法规和信息安全标准，确保平台的合规性和安全性。

* 1. 信创生态兼容性要求

应与国产操作系统、国产芯片及国产数据库等信创产品兼容，满足信创环境下的运维需求。

* 1. 平台安全总体要求

建立完善的安全体系，包括身份认证、权限控制、数据加密、安全审计等，保障平台及数据的安全性，防止未授权访问和数据泄露。

1. 平台技术架构要求
   1. 分层架构模型

平台可分为基础资源层、数据层、平台层、应用层和展示层。

1. 展示层：为用户提供友好的 Web 界面，实现用户与平台的交互，包括登录、操作、数据展示等功能。
2. 应用层：集成客服管理、工单管理、远程协助、日志管理、系统设置等核心应用功能，处理业务逻辑。
3. 平台层：提供基础服务支撑，如权限管理、消息通知、任务调度等，保障应用层的稳定运行。
4. 数据层：负责数据的存储和管理，包括用户数据、工单数据、日志数据等，采用安全可靠的数据库技术，确保数据的完整性和一致性。
5. 基础资源层：包括服务器、存储设备、网络设备等基础设施，为平台提供计算、存储和网络资源支持。
   1. 网络架构要求

采用稳定可靠的网络架构，支持局域网和广域网接入，确保远程协助和数据传输的稳定性和高效性。配置合理的网络安全设备，如防火墙、入侵检测系统等，保障网络安全。

* 1. 高可用与高可靠要求

实现主服务器数据的实时同步与备份，当主服务器发生故障时，能够无缝切换到备份服务器，切换时间应小于 [5] 分钟，确保服务中断时间最短，数据不丢失。

* 1. 可扩展性要求

平台架构应具备良好的可扩展性，能够根据业务需求灵活扩展功能模块和硬件资源，支持新设备、新系统的接入和集成。

* 1. 开放性与集成性要求

提供开放的接口和标准，支持与第三方系统（如监控系统、资产管理系统等）进行集成，实现数据共享和协同工作。

1. 平台功能要求
   1. 终端管理
2. 系统应支持对信创环境中各类终端设备进行集中管理，包括但不限于台式机、笔记本、移动终端、虚拟终端等。
3. 终端管理功能应包括终端设备的注册、识别、信息采集、运行状态监控、资产动态管理及操作日志记录。
4. 系统应支持远程策略下发及终端配置管理，确保终端设备符合统一的管理规范。
5. 系统应具备终端行为分析能力，以便及时发现异常使用行为。
6. 终端管理功能应支持终端的远程操作和软件安装，便于统一运维与维护。
7. 系统应可对终端设备进行安全合规检测，包括系统版本控制、补丁状态、安全策略执行情况等。
8. 系统应提供包括在线状态、故障状态、硬件信息和其他信息的可视化展示功能，能实时监控终端设备的状态。
   1. 工单管理
9. 系统应支持对运维工作中产生的服务请求、故障事件、变更申请等进行工单管理。
10. 工单管理应包括创建、分配、处理、跟踪、关闭和归档等全生命周期管理流程。
11. 系统应支持对工单设置优先级，以保证紧急或重要事件的高效处理。
12. 系统应对工单状态的变更进行记录，确保事件处理过程的可追溯性和可审计性。
13. 系统应提供工单处理时效提醒功能，确保运维任务按时完成。
14. 工单可由系统自动触发、人工提交或由第三方系统集成导入。
15. 工单管理应具备与知识库、服务目录、资产管理系统等进行数据交互的能力，实现运维服务的标准化与智能化。
    1. 用户管理
16. 系统应支持对平台用户的集中管理，包括用户身份的创建、修改、删除、禁用等操作。
17. 系统应实现用户角色的分级管理，明确管理员、运维人员、审计人员和普通用户等不同角色的权限范围。
18. 系统应对用户进行访问控制，确保用户仅能访问其权限范围内的资源和功能模块。
19. 系统应具备用户账号与权限的生命周期管理能力，支持用户状态变更的记录与审计。
20. 用户管理功能应保障用户操作行为的可追溯性，确保运维平台符合国家信息安全相关标准要求。
    1. 知识管理
21. 系统应提供统一的知识库管理功能，支持运维知识的采集、存储、检索、更新与共享，提升运维知识资产的复用效率。
22. 知识库应支持知识的版本管理和变更记录，以确保知识的追溯性与安全性。
23. 系统应支持知识的生命周期管理，包括发布、生效、作废、归档等状态管理功能。
24. 系统应支持知识内容与运维流程、工单、事件等系统的关联映射，增强知识与业务的联动能力。
25. 系统应提供高效的全文检索功能，支持模糊匹配、关键词检索、高级搜索（如分类、标签、发布人、时间等）等搜索方式。
26. 系统应建立知识访问的权限控制机制，支持基于用户角色、组织、访问权限的多级控制。
27. 平台应支持与 AI 系统的集成，例如知识图谱构建、问答引擎训练、智能搜索优化等，提升知识自动服务水平。
28. 平台应具备良好的工具扩展能力，支持常见运维工具的集成与联调，提升统一运维管理能力。
    1. 故障申报
29. 故障申报程序应以窗口化形式展示当前用户申报信息的整体概览，便于用户实时确认申报内容。
30. 故障申报程序在启动时应默认加载运维平台地址，普通用户无需手动配置基础地址信息。
31. 运维平台地址仅在断开平台连接后允许手动编辑或更新，变更后应具备连接状态检测与重新连接机制。
32. 系统应对运维平台地址变动进行本地记录，并在管理后台提供查看日志功能，以保障平台端与终端一致性和可追溯性。
33. 故障申报界面应提供运维工程师的选择列表，列表应包含工程师姓名、工号及在线状态。
34. 在线状态应由运维平台通过心跳机制自动同步，确保用户选择时能确认工程师是否在线。
35. 故障申报程序应提供故障原因选择，包含常见问题类型。
36. 故障申报的数据需在平台中完整归档，包括选择的运维人员、联系电话、申报时间、故障描述、故障分类等信息。
37. 所有申报记录应具备可追溯性，系统应记录用户IP、系统时间戳及操作记录，用于后续安全审计与问题复盘。
38. 系统应支持对历史申报记录的导出与查询功能，便于统计分析与改进运维决策。
    1. 远程运维管理
39. 平台应支持远程操作过程中的会话录制与回放，记录全过程的命令、响应、图形界面等操作内容。
40. 远程访问应具备动态授权机制，如根据风险评估结果调整访问权限或要求多因子认证。
41. 平台应提供远程接入会话的强制断开、超时断开、多端切换控制等管理功能，防止未授权操作与资源滥用。
42. 平台应支持对违规操作、越权行为、异常操作等进行告警与自动阻断，确保远程操作合规可审。
    1. 自动化运维管理
43. 系统应支持自动化运维任务的定义、调度与执行功能，包括但不限于定时任务、批量操作、任务链编排和业务流程自动化处理。
44. 系统应支持自动化任务的执行控制，包括任务启停、暂停、恢复以及异常终止等操作，并应提供操作日志与审计追踪。
45. 系统应提供自动化运维任务的运行状态监控功能，包括任务进度、执行耗时、成功率、失败原因等内容的实时展示与记录。
46. 系统应具备接口化能力，提供标准化的 API 或集成接口，支持用户或第三方系统调用、触发与扩展自动化运维流程。
47. 系统应支持自动化运维操作的版本管理和回滚功能，确保任务操作具有可维护性和可逆性。
    1. 报表与可视化分析
48. 系统应支持运维相关数据的汇总、统计与报表生成功能，满足运维管理人员对系统运行状态和事件处理情况的分析需求。
49. 系统应对关键运维指标（如问题响应时间、解决率、终端使用状态、用户行为模式）进行自动化分析与展示。
50. 系统应提供多种格式的报表导出能力，包括但不限于 PDF、Excel、Word 和 CSV 格式。
51. 平台安全要求
    1. 身份认证
52. 系统应支持按照国家网络安全等级保护制度及相关法律、法规和标准要求，实施必要的安全管控措施和审计机制。
53. 系统应支持多因子认证机制，确保身份验证的强安全性，防止非法访问与操作行为的发生。
54. 平台应支持运维设备访问前的身份验证与设备指纹识别，用于防范非法接入与设备仿冒。
    1. 网络安全
55. 平台应支持使用通用安全通信协议，如 Transport Layer Security（TLS）等，保障数据在传输过程中的完整性与保密性。
56. 平台应支持国密通信协议 TLCP（Transport Layer Cryptographic Protocol），满足国产密码算法在安全通信上的合规性要求。
57. 平台应支持双向认证机制，确保通信双方身份的真实性和合法性，如客户端与服务端均使用证书认证。
58. 平台应支持自动检测加密协议与算法的兼容性，并提示潜在安全风险，如使用已知不安全的密码套件。
    1. 数据安全
59. 对敏感数据进行加密存储，如用户密码、终端隐私数据等。
60. 采用可靠的存储设备和存储技术，确保数据的存储安全，防止数据丢失和损坏。
61. 平台应具备数据自动备份功能，支持全量与增量备份，并可在多个存储节点之间灵活迁移。
62. 平台应提供备份数据的完整性校验机制，确保数据在备份、传输和恢复过程中不受篡改。
    1. 行为审计
63. 系统应对用户登录过程中的异常行为进行识别和记录，包括不合规的登录时间、登录设备变动、频繁失败登录等，应具备自动告警与响应能力。
64. 系统应对用户操作行为进行完整、实时的审计记录，审计内容应包括但不限于操作时间、操作用户、操作对象、操作内容、操作结果及会话过程。保存审计日志，以便于事后审计和故障追溯。
    1. 自身安全防护

定期对平台进行安全加固，修复系统漏洞和安全隐患。

* 1. 特权账号管理

对特权账号（如系统管理员账号）进行严格管理，采用专人专责制度，定期更换密码，记录特权账号的操作行为，确保特权操作的安全性和可追溯性。

1. 平台接口要求
   1. 数据采集接口
2. 系统应支持与各类运维对象（如操作系统、数据库、中间件、网络设备、虚拟化平台、云平台等）之间的数据采集接口接入功能。
3. 系统应支持定时采集、实时采集、事件触发采集等多种采集方式，以满足多类运维数据的采集需求。
4. 系统应支持国产化协议与接口的接入能力，确保符合国家信息技术应用创新相关技术规范。
5. 系统应具备采集数据的格式转换和标准化处理能力，自动识别并解析源数据，确保数据结构统一、格式一致。
6. 采集接口与平台之间的数据传输应遵循加密与安全机制，确保数据在传输过程中不被篡改或泄露。
   1. 单点登录（SSO）

系统应提供与现有企业身份认证系统的集成能力，包括但不限于 LDAP、Active Directory（AD）、OAuth 2.0、SAML 等协议，实现统一身份管理。

* 1. 管理控制接口

提供管理控制接口，支持对终端设备进行远程控制和管理，如远程重启、关机、配置下发等。

* 1. 数据共享接口

1. 平台应提供标准、稳定、安全的数据开放与共享接口，支持与其他信息系统、管理平台、分析工具等实现数据互通与共享。
2. 平台应具备接口注册与管理功能，支持第三方接口资源的注册、授权、状态监控和生命周期管理。
3. 数据开放应支持结构化数据格式，包括但不限于 JSON、XML、CSV、TSV、YAML、Protobuf 等，确保接口的通用性与可读性。
4. 平台应支持接口性能的预警与告警机制，在接口响应超时、调用异常、负载过高时进行通知和提示。
5. 平台应对数据开放接口的调用情况进行日志记录，包括调用者信息、调用时间、调用内容和调用响应结果。
   1. 接口安全规范

接口应遵循安全规范，采用身份认证、数据加密、签名验证等安全措施，确保接口的安全性和可靠性。

1. 平台部署与实施要求
   1. 部署架构

平台应支持集中式/分布式部署架构

* 1. 用户培训要求

为用户提供全面的培训服务，包括平台的操作培训、维护培训和安全培训等，确保用户能够熟练使用平台的各项功能，保障平台的正常运行。

1. 平台测试与验收要求
   1. 功能性测试

对平台的各项功能进行测试，确保功能的完整性和正确性，如客服管理、工单管理、远程协助、日志管理等功能是否正常运行。

* 1. 性能测试

测试平台的性能指标，如并发处理能力、响应时间、吞吐量等，确保平台能够满足业务需求，在高负载情况下稳定运行。

* 1. 安全性测试

测试平台的安全性能，包括身份认证、权限控制、数据加密、安全审计等，确保平台的安全性符合相关标准和规范。

* 1. 可靠性测试

测试平台的可靠性，如高可用切换、数据备份与恢复等功能，确保平台在发生故障时能够快速恢复，数据不丢失。

* 1. 信创环境兼容性测试

在信创环境下对平台进行兼容性测试，确保平台与国产操作系统、芯片、数据库等信创产品兼容，满足信创要求。

* 1. 验收流程与标准

制定详细的验收流程和标准，包括功能验收、性能验收、安全验收等环节，验收合格后签署验收报告。验收标准应符合国家相关法律法规和技术规范的要求，以及用户的实际需求。

1. 附录

附录A（资料性附录） 基础远程运维流程示例

附录B（规范性附录） 典型应用场景

附录C（资料性附录） ××××××××××××