面向信息化建设的服务器运维智能化技术研究与实践

戴丽莉
海军青岛特勤疗养中心　山东青岛　266071

摘　要：信息化建设依托服务器运维质量支撑业务系统的稳定运行，智能化能力成为提升整体效能的重要方向。本文分析了信息化建设中的运维需求，研究了服务器性能预测、故障根因分析、配置漂移检测校正与服务器安全智能运维等关键技术，提出了面向服务器的智能化运维体系框架，旨在通过自动化监测、智能诊断与安全治理提升运维效率与系统可靠性；并通过实践案例构建实验环境、开展运维过程验证与结果分析，验证所提出技术体系在真实场景中的可行性与运维价值。

关键词：信息化建设；服务器运维；智能化技术

引言

信息化建设加速推进使服务器成为数字化系统的性能核心，其运维复杂度随规模增长持续提升[1]。当前服务器运维仍以人工巡检和被动响应为主，在性能预测不精准、故障根因定位困难、配置管理易漂移及安全防护滞后等方面存在明显不足，难以支撑信息化场景中高并发、大规模、动态化的资源管理需求。基于此，本文提出了面向信息化建设的服务器运维智能化技术体系，以数据驱动实现性能预测、故障诊断、配置校正与安全治理的协同优化，该思路突破了传统运维碎片化、经验化的局限，为服务器集群的高效、稳定与安全运行提供具有学术价值的系统化技术路径。

一、需求分析

信息化建设推动服务器规模持续增长，运维场景呈现高并发、高波动、高耦合属性。服务器运维围绕性能稳定、故障定位、配置一致、风险管控四项核心需求展开[2]。业务负载在高峰时段出现快速攀升，CPU、内存、磁盘与网络流量处于剧烈变动状态，传统方式难以预测性能趋势，资源调度出现偏差，引发系统压力积聚。服务器结构由硬件层、系统层、中间件层与应用层组成，关联链路复杂，异常事件交织，人工排查难以梳理异常序列，故障定位过程耗时，整体修复周期偏长。长期运行阶段受补丁更新、系统升级与参数变更影响，服务器配置状态产生偏移，形成漂移风险，性能稳定性下降，安全隐患增大[3]。服务器承载大量敏感数据，安全威胁呈现多样化趋势，合规要求趋严，运维体系需覆盖风险评估、行为分析、日志审计与应急响应等全流程要素，形成贯穿全周期的安全防护框架。

二、面向信息化建设的服务器运维智能化技术研究

（一）服务器性能预测

服务器性能预测依托历史运行数据构建模型，预判未来性能走势，为资源调度与负载分配形成依据。整体流程由数据采集、特征处理、模型训练构成。采集范围覆盖硬件层、系统层、应用层三类指标，硬件层含CPU占用、内存占用、磁盘I/O吞吐、磁盘空闲、带宽利用、网络时延，系统层含进程数量、线程数量、系统负荷、文件句柄数量、日志警告与错误记录，应用层含响应时长、成功率、连接数量、查询时长、中间件吞吐。

采集模块采用Agent模式与无Agent模式，前者采集频率为一秒一次，后者依靠SSH与SNMP完成五秒一次采集，数据落库于时序系统供后续分析使用。采集数据存在噪声与量级差异，需经清洗、标准化处理，缺失值以插值补齐，异常值以统计规则剔除，数值统一映射至0~1区间[4]。经时间序列处理可形成趋势特征、周期特征、突变特征，经特征筛选生成关键输入序列。预测模型由LSTM与XGBoost构成，前者处理长期依赖信息与周期关系，后者处理局部波动与非线性结构。两类输出以加权形式融合，权重依据验证集误差动态更新。

（二）故障根因分析

故障根因分析基于异常序列、运行链路与资源依赖构建智能分析流程。如图1所示，运行状态输入、异常序列输入、链路图输入与特征学习模块之间的信息流动。

作者简介：戴丽莉（1993.02-），女，汉族，山东安丘，本科，初级技师，研究方向：疗养院信息化建设。

运行状态覆盖CPU占用、内存占用、磁盘I/O活动、网络流量、系统日志、进程活动。采集器记录事件时间、事件类型、关联单元、事件文本，经标准化生成结构化特征向量，形成学习输入[5]。特征学习模块依托自注意力结构提取时序关联、因果关联，模型以特征向量为输入并输出根因类别，为后续链路验证环节提供依据。

资源依赖模型以图结构呈现节点关系，将服务器节点、硬件设备、软件系统、应用单元以节点表达，依赖关系以边表达，形成运行链路图。依赖追踪把异常事件所在节点与链路关联，沿链路方向推演影响范围，再反向推回关键单元。根因定位阶段将特征学习输出与依赖链路输出结合，形成根源单元识别结果。分析过程可在界面呈现事件时序、链路图、根因置信度数值，便于理解异常演化过程与资源关联结构，形成从状态采集、事件序列建模、依赖追踪到根源确认的连续分析链条。

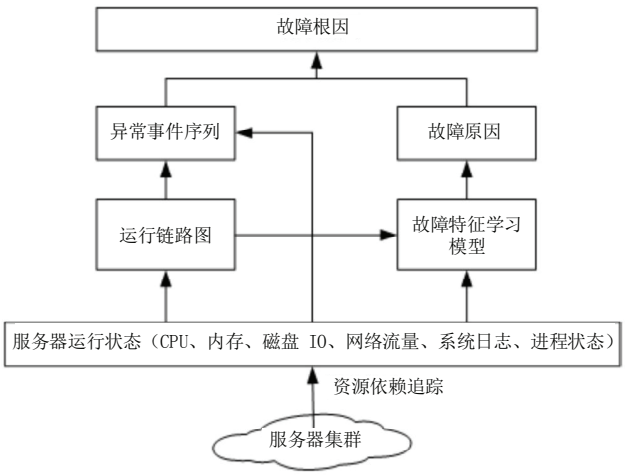

图1　智能化服务器故障根因分析结构图

（三）配置漂移检测校正

配置漂移检测校正面向服务器集群配置一致性场景，依托基线构建、实时采集、智能识别、校正执行形成闭环。标准配置基线囊括硬件层、系统层、中间件层、应用层关键参数，结构化格式存储，具备版本记录与权限约束，适应配置演变需求。实时采集器记录参数内容，采集周期依稳定性设定，核心节点周期短，普通节点周期长。采集过程依靠文件读取、命令执行、数据查询实现参数抓取，采集后与基线进行字段级比对，数值型参数比对数值，字符型参数比对文本，布尔型参数比对状态，构成漂移识别入口。

漂移识别采用分级策略，将偏差区分为轻微级、一般级、严重级。模型基于训练集分析参数偏离对运行态势影响，智能判断漂移级别。轻微级进入记录流程，一般级触发预警，严重级推送紧急告警并进入校正准备阶段。校正机制支持自动模式与人工模式。自动模式适用于参数偏差明确、操作链路固定的漂移场景，生成校正方案后进入前置检查，再执行校正步骤并记录过程，校正完成后采集参数并与基线比对作为验证环节。人工模式适用于结构复杂场景，界面呈现漂移内容与校正建议，辅助运维人员执行校正任务，形成配置稳定性维护路径。

（四）服务器安全智能运维

服务器安全智能运维面向全生命周期安全场景，依托采集、监测、管理、评估构建安全运维体系。如图2所示，由智能采集器、安全监测分析系统、安全管理平台、评估系统构成，形成从数据获取到风险辨识再到管理控制的闭环。智能采集器记录日志数据、网络流量数据、漏洞数据、行为数据。日志数据覆盖系统层、应用层、安全设备层，网络数据记录数据包特征与连接状态，漏洞数据记录编号与风险等级，行为数据记录登录行为、进程行为、文件行为。安全数据经标准化后进入数据湖，形成监测与评估基础。

安全监测分析系统以规则引擎与模型构成分析链路。规则引擎识别常见威胁，模型学习正常行为模式，判定异常登录、异常进程、异常文件操作等行为特征。无监督模型处理无标签数据，提升对新型威胁的识别能力。评估系统依据配置状态、访问控制状态、漏洞修复状态构建风险矩阵，对服务器安全等级开展量化评估，并结合合规要求执行规则校验。管理平台整合监测结果与评估结果，呈现安全态势。当高风险事件出现时，应急机

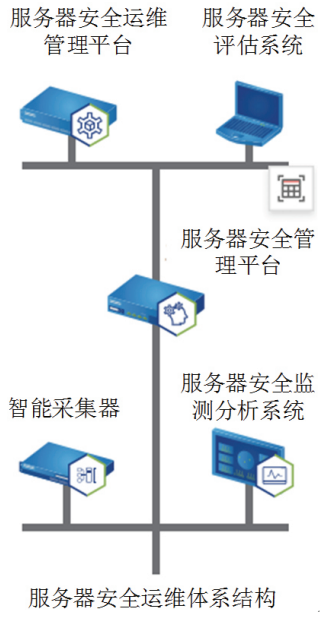

图2　服务器安全智能运维体系结构示意图

制启动处置动作，调整访问规则、隔离节点、清理恶意程序或推送修复补丁，记录处置链路，为后续分析提供依据。

三、实践案例

（一）实践案例

实践对象选取某信息化管理平台的服务器集群，规模约120节点，支撑业务类型覆盖政务服务、内部办公平台、数据交换服务等场景。服务器部署在混合云环境，计算集群由虚拟化节点与物理节点构成，运行负载呈波动态势，早晚高峰时段压力明显集中。运维压力主要表现在性能波动难以提前判断、故障链路追踪复杂、配置偏差积累快、安全事件数量大且来源分散。基于实际运行情况，选取性能预测模块、根因分析模块、配置漂移检测模块、安全智能运维模块作为实践对象，构建自动化运维体系，形成从监测到诊断再到处置的智能链路。

（二）实践过程

系统部署阶段接入全量运行数据，采集指标包含性能序列、配置参数、日志内容、网络流量与安全行为数据。采集后进入预处理模块，数据清洗、结构化转换与特征构建按预设流程执行。性能预测模型基于混合结构训练，特征序列进入模型后输出服务负载趋势，为资源管理平台提供调度依据。根因分析模块结合事件序列、链路结构与特征模型，构建异常定位路径，在异常触发后输出根因类别与关联组件。

配置漂移检测模块围绕基线进行字段比对，偏差内容进入漂移模型，由模型判断影响等级并推送校正建议。安全智能运维模块整合安全监测分析系统与管理平台，监测到的异常行为进入风险评分流程，分级后触发相应处置动作。模型运行阶段各模块按独立调度策略执行，性能预测每日训练增量数据，根因模型在事件积累充足后执行周期优化，安全模块实时分析流量与行为特征。全链路在管理平台统一编排，异常检测、校正任务与安全处置任务以自动化流程运转，人工操作仅在复杂事件中介入。

（三）实践结果分析

基于表1中数据得知，智能化运维体系投入运行后，关键指标呈现显著改善。性能预测准确率由83.20%提升至92.60%，负载趋势判断更稳定。故障定位平均时长由46.3分钟下降至12.7分钟，异常链路收敛速度加快。配置漂移检测命中率与自动校正成功率分别提升至97.20%与94.80%，配置一致性维持效果更稳。安全事件告警准确率提升至93.50%，误报率下降，威胁识别更集中于高风险行为。高危事件响应时间由32.4分钟缩短至6.8分钟，应急链路执行效率显著增强，整体运维能力呈系统性提升。

表1　智能化服务器运维体系优化前后关键指标对比表

指标项	优化前	优化后
性能预测准确率	83.20%	92.60%
故障定位平均时长（分钟）	46.3	12.7
配置漂移检测命中率	78.40%	97.20%
配置自动校正成功率	65.10%	94.80%
安全事件告警准确率	71.60%	93.50%
高危事件响应时间（分钟）	32.4	6.8

结论

本文围绕信息化建设背景下的服务器运维需求，构建了涵盖性能预测、故障根因分析、配置漂移检测校正与安全智能运维的智能化技术体系，并以实践案例验证模型在性能预判、故障定位、配置治理与安全管控方面的成效，形成可复用的智能运维路径，为大规模服务器集群的稳定运行提供技术依据。未来，服务器运维智能化将向自学习、自适应与全局自治方向演进，跨平台协同、时序知识建模、智能安全联动等能力将进一步强化，为信息化基础设施的高质量发展奠定更具弹性与智能化的运维支撑体系。

参考文献

[1]张观东.基于云计算的轨道交通信息智能运维[J].中国科技信息，2025，(21)：125-127.

[2]王静雅，靳志成，赵聪旭.基于Linux系统的服务器自动化运维策略与实践[J].电脑知识与技术，2025，21(29)：85-87.

[3]钟业荣，阮国恒.基于端云协同的大数据信息化云测试系统设计[J].自动化与仪器仪表，2025，(09)：299-302+307.

[4]陈晓燕，吕轩民.电子商务平台信息化建设中的网络安全问题研究[J].数字通信世界，2025，(07)：18-20.

[5]唐文张.三区网络设备智能运维系统研究与应用[J].网络安全和信息化，2025，(07)：59-61.