团　　体　　标　　准

银行业智能化运维(AIOps）可观测性技术能力要求

The technical capability requirements of Observabilityfor Banking artificial intelligence operations

（征求意见稿）

[××××]-[××]-[××]发布　　[××××]-[××]-[××]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这些专利的责任。

本文件由中国互联网协会归口。

本文件起草单位为：

本文件主要起草人：

引　言

当前智能运维应用前景广泛，适用多种场景，企业需要一个广泛达成共识的智能运维能力成熟度模型，以指导企业稳步提升工作效率和服务质量，提高企业的核心竞争力。因此，开展智能化运维能力成熟度模型标准编写工作，规范并促进国内智能运维的发展和应用，让国内众多企业可以共享、复用智能运维技术和能力，指导国内各行业在智能运维方向的相关实践落地。本文件旨在指导企业从初级到高级逐步构建智能运维体系，以数据层和核心能力层作为能力支撑，从常态运维、故障应急、变更管控、性能容量四大运维场景描述了智能化运维可观测性技术能力要求。

本标准目的在于提出构建智能化运维领域的可观测性能力需要具备的系统和工具能力以及相应的观测场景，明确了建设可观测性能力需要具备的功能及能力要求，以及相应的分级评估方法。

银行业智能化运维(AIOps)可观测性技术能力要求

1. 范围

本文件规定了银行业智能运维领域的可观测性能力要求。

本文件面向银行业智能运维可观测性整体能力建设，适用于指导基于可观测性的智能运维平台的规划、设计与实现，为相关企业选择可观测性系统工具提供选型依据，也可供企业建设基于可观测性的智能运维平台能力提供标准依据。

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 43208.1-2023 信息技术服务 智能运维 第 1 部分：通用要求

GB/T 17143.6-1997 信息技术 开放系统互连 系统管理 第 6 部分：日志控制功能

GB/T 44886.3-2025 网络安全技术 网络安全产品互联互通 第 3 部分：告警信息格式

GB/T 8566-2007 信息技术 软件生存周期过程

3. 术语和定义

下列术语和定义适用于本文件。

3.1.

智能化运维 artificial intelligence for IT operations (AIOps)

是人工智能技术（如机器学习（3.3）等）和数据科学在IT运营问题上的应用，用于增强和部分替代主要的IT运营功能。

［来源：GB/T 43208.1-2023］

3.2.

可观测性 observability

通过采集和分析系统的外部输出（如指标、日志、链路追踪等数据），推断系统内部状态的能力，用于监控、故障排查和性能优化。

3.3.

指标 metric

对系统或业务运行状态进行量化测量的数据点，通常包含时间戳、名称、数值和维度标签，如CPU使用率、交易成功率、响应时间等。

3.4.

日志 log

系统、应用或设备在运行过程中产生的带有时间戳的结构化或非结构化事件记录，用于故障追溯、审计分析和行为洞察。

［来源：GB/T 17143.6-1997］

3.5.

链路追踪 trace

记录一个请求或事务在分布式系统中经过的完整调用路径，包含各节点（服务、中间件、数据库等）的耗时、状态和关联标识，用于性能分析和故障定位。

3.6.

告警 alert

当监控指标或事件满足预设规则时，主动发出的通知，用于提醒运维人员关注异常情况，并触发相应处置流程。

［来源：GB/T 44886.3-2025］

3.7.

拓扑 topology

系统中各组件（基础设施、服务、网络等）之间的静态或动态连接关系与层级结构，用于展示架构依赖和故障传播路径。

3.8.

基线 baseline

基于历史正常运行数据建立的参考值或范围，用于对比当前观测数据，识别异常波动或性能退化。

［来源：GB/T 8566-2007］

4. 缩略语

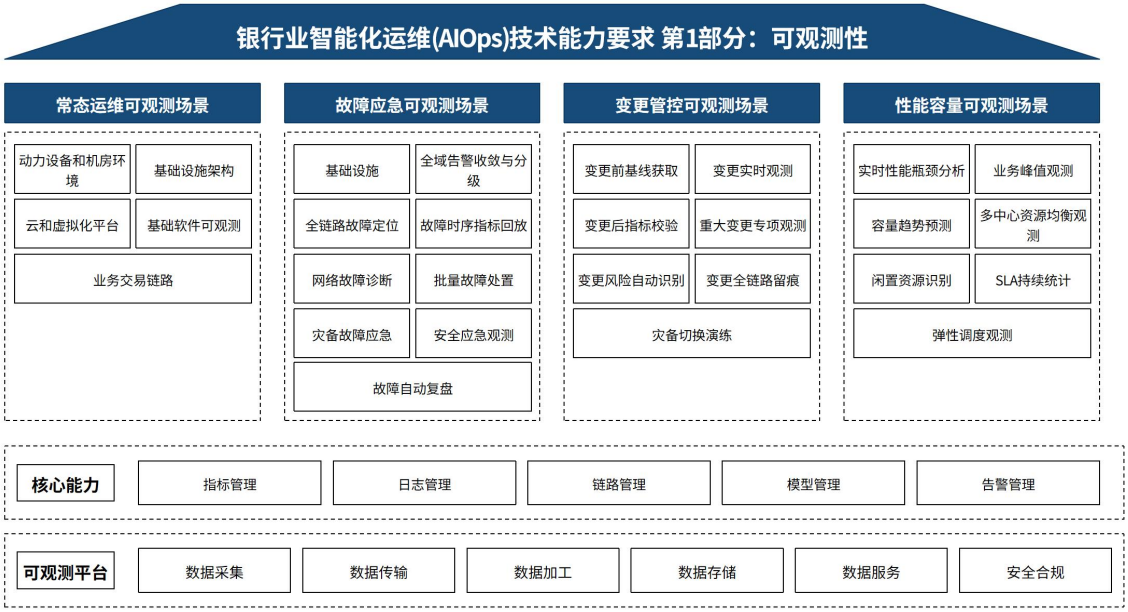
下列缩略语适用于本文件。

AI	人工智能	Artificial Intelligence
AIOps	智能化运维	Artificial Intelligence for IT Operations
API	应用程序编程接口	Application Programming Interface
APM	应用性能管理	Application Performance Management
CMDB	配置管理数据库	Configuration Management Database
MTBF	平均故障间隔时间	Mean Time Between Failures
MTTR	平均修复时间	Mean Time To Repair
RUM	真实用户监测	Real User Monitoring
SLA	服务等级协议	Service Level Agreement
SLO	服务等级目标	Service Level Objective
TraceID	链路追踪唯一标识	Trace Identifier

5. 智能化运维可观测性能力框架

智能化运维（AIOps）可观测性能力要求提供将来自不同系统的运维数据通过采用数据分析、人工智能技术等方法进行分析并与智能运维场景结合，以增强及拓展智能运维及传统运维场景能力，达到提高整体运维效率的目的，其中包括：常态运维可观测场景、故障应急可观测场景、变更管控可观测场景、性能容量可观测场景、核心能力和可观测平台，如图 1 所示。

图 1 智能化运维可观测性能力框架



6. 可观测性能力分级要求

智能化运维可观测性能力可以划分为三个级别，每个级别中按照基础能力和高级能力的实现程度，呈现递进的方式，分别是：

——初始级观测性能力，已经建立较为完善的监控体系，能够实时收集、存储、分析和报告系统的运行状态数据，实现全面的基础设施和应用程序监控，具备初步的问题诊断和根因分析能力，并能够快速定位并解决一般性问题；

——全面级可观测性能力，能够对各观测场景进行端到端的监控，形成了全面的监控体系，实现监控数据的整合和可视化，开始引入人工智能和机器学习技术辅助分析和决策，能够深入挖掘系统性能瓶颈和潜在问题；

——卓越级可观测性能力，具备快速响应和解决复杂问题的能力，形成一套完善的可观测性指标体系和最佳实践流程，将可观测性作为推动业务创新和发展的重要驱动力，并且在行业中具有极高的影响力和示范效应。

7. 银行业智能运维可观测性场景

7.1. 常态运维可观测场景

7.1.1. 动力设备和机房环境

7.1.1.1. 机房环境观测

机房环境观测指对机房内外部环境参数、安防设备状态、能耗水平开展实时监测、多维度统计与趋势分析的能力，保障机房运行环境符合IT设备温湿度、压差等运行标准，规避环境故障引发业务中断风险。

基本能力：

——应支持机房环境与安防感知采集监测，覆盖机柜进/出风口、冷热通道等点位温湿度，以及门禁、漏水、烟感等安防参数，支持多级阈值配置，异常即时触发告警；

——应支持机房能效与能耗统计分析，实现机柜级、机房级 PUE 指标实时计算与多维度展示；完成动力、制冷、IT 设备的能耗分项计量，提供日、月、年度能耗趋势视图，支撑机房能效评估；

——应支持机房视频监控联动能力，环境告警触发时可自动关联对应区域监控画面，辅助故障快速核实；

——应支持机房负载趋势统计分析，可按机柜、机房维度展示 IT 负载的变化趋势，支撑机房容量规划；

——应支持碳排放指标统计与展示，可基于能耗数据核算机房碳排放量，满足绿色数据中心监管要求；

高级能力：

——宜支持机房环境异常预测能力，基于历史温湿度、能耗数据识别异常波动趋势，提前预警环境风险；

——宜支持机房能耗优化分析能力，结合 IT 负载与制冷效率给出能耗优化建议，辅助提升机房能效水平；

——宜支持机房环境数字孪生可视化能力，可直观展示机房布局、设备位置、环境参数分布与告警位置；

——宜支持机房安防事件智能识别能力，可通过视频分析识别人员违规进入、异常操作等安防事件。

7.1.1.2. 动力供配电观测

动力供配电观测指对数据中心 UPS 系统、蓄电池组、精密配电柜、柴油发电机组等供配电设施的运行状态、电气参数、健康水平进行监测与分析的能力，用于保障银行数据中心供电连续性，防范供电系统故障引发的业务中断。

基本能力：

——应支持 UPS 设备运行状态实时监测，覆盖输入输出电压、电流、频率、负载率、旁路状态等核心参数，支持异常阈值告警；

——应支持蓄电池组运行状态监测，覆盖单体电压、内阻、温度、组端电压、充放电电流等参数，支持蓄电池劣化告警；

——应支持精密配电柜支路监测能力，可采集每路输出的电压、电流、功率、电能等参数，支持支路过载告警；

——应支持柴油发电机组运行状态监测，覆盖启动状态、运行时长、油温、油压、燃油液位、输出参数等，支持启动失败、设备故障告警；

——应支持供配电系统切换事件全量记录，包含市电中断、UPS 转旁路、柴油发电机启动等事件的时间、状态、持续时长；

——应支持蓄电池放电时长估算能力，基于蓄电池容量与当前负载计算后备供电时长，支撑供电风险评估；

——应支持双路供电冗余校验能力，可监测双路供电的运行状态，识别单路断电、负载失衡等冗余失效风险；

高级能力：

——宜支持蓄电池健康状态评估与寿命预测能力，基于内阻、温度、充放电历史数据评估电池劣化程度，预测剩余使用寿命；

——宜支持供配电系统负载智能调度分析，结合 IT 负载变化给出供配电回路负载优化建议，提升供电系统利用率；

——宜支持供配电系统应急演练仿真能力，可模拟市电中断、设备故障等场景，验证供配电系统的冗余能力与处置流程。

7.1.1.3. 制冷暖通观测

制冷暖通观测指对数据中心精密空调、冷水机组、冷却塔、冷通道封闭系统等制冷设施的运行状态、性能参数、制冷效率进行监测与分析的能力，用于保障机房制冷系统稳定运行，满足 IT 设备散热需求，提升制冷能效。

基本能力：

——应支持精密空调运行状态实时监测，覆盖送风温度、回风温度、湿度、风机转速、压缩机运行状态、滤网状态等参数，支持温度异常、设备故障告警；

——应支持冷水机组运行状态监测，覆盖出水温度、回水温度、流量、负载率、压缩机运行参数、冷媒压力等，支持机组故障告警；

——应支持冷却塔运行状态监测，覆盖进出水温度、风机运行状态、水位、补水状态等，支持异常告警；

——应支持冷通道封闭系统状态监测，覆盖通道门状态、压差、温湿度分布等，支持通道异常开启、温湿度超标告警；

——应支持制冷系统流量、压差监测，覆盖供回水管路的流量、压差参数，支持管路堵塞、流量异常告警；

——应支持风机故障、水泵故障等制冷设备部件异常的实时监测与告警，记录故障发生时间与持续时长；

——应支持制冷系统能耗统计与能效分析，可计算制冷系统 COP（能效比），支持按日、月维度统计制冷能耗；

高级能力：

——宜支持制冷系统智能调优能力，结合机房 IT 负载与温湿度分布，动态调节空调、冷水机组运行参数，提升制冷能效；

——宜支持制冷设备故障预测能力，基于设备运行历史数据识别劣化趋势，提前预警部件故障风险；

——宜支持机房热点智能识别能力，结合机柜负载与温湿度分布数据，定位局部热点区域，给出制冷优化建议；

——宜支持制冷系统应急故障联动能力，单台制冷设备故障时可自动调节周边设备运行参数，保障机房制冷冗余。

7.1.2. 基础设施架构可观测

7.1.2.1. 服务器硬件观测

服务器硬件观测指对物理服务器的计算、存储、散热、供电等核心硬件组件的运行状态、性能参数与健康水平进行实时采集、监测与故障预警的能力，用于及时发现服务器硬件异常，防范硬件故障引发的业务系统中断，支撑服务器硬件全生命周期运维管理。

基本能力：

——应支持服务器硬件全组件状态监测，覆盖 CPU 温度 / 内存硬件错误、磁盘硬件状态与 IO 性能、风扇散热、电源模块、RAID 卡及 BBU 电池等硬件参数，支持多级阈值告警；

——应支持服务器硬件故障统一告警管理，识别硬件宕机、组件失效、硬件报错日志等事件，按故障等级分级推送至对应运维责任人；

——应支持服务器硬件资产信息关联管理，展示服务器型号、序列号、保修期限、硬件配置等资产数据，支撑硬件资产全生命周期台账管理；

——应支持服务器硬件状态多维度统计展示，可按机房、机柜、业务归属维度统计硬件健康度、故障分布与故障率，支撑运维分析决策。

高级能力：

——宜支持服务器硬件寿命预测与健康度评分能力，基于硬件运行历史数据、损耗指标评估硬件劣化程度，预测核心部件剩余使用寿命；

——宜支持硬件故障预测性维护能力，可提前识别硬件潜在故障风险，生成分级维护建议，辅助运维人员提前处置，降低非计划停机概率；

——宜支持硬件备件管理联动能力，可结合硬件故障告警与寿命预测数据，自动匹配备件库存信息，生成备件申领与更换计划建议。

7. 1. 2. 2. 存储设备观测

存储设备观测指对银行集中式存储、NAS 存储等各类存储设备的容量水位、性能表现、硬件健康、数据保护状态进行持续监测与分析的能力，用于保障银行业务数据存储的可靠性、访问性能与安全性，满足数据安全合规与业务连续性要求。

基本能力：

——应支持存储硬件、池容量与 RAID 组状态监测，覆盖存储池容量水位、磁盘硬件健康、RAID 组状态及重构进度，支持容量越限、磁盘故障、RAID 降级/失效告警；

——应支持存储性能指标监测，覆盖块存储 IOPS、时延、吞吐量、队列深度，以及 NAS 文件读写时延、吞吐量、并发连接数，支持性能异常突增、时延超标告警；

——应支持数据保护与文件系统状态监测，覆盖快照、备份任务执行状态与成功率，文件目录容量分布及增长趋势，识别备份失效、目录异常膨胀风险；

——应支持存储安全访问监测，识别越权访问、异常批量文件操作、非授权 IP 访问行为，触发安全告警并留存审计日志，满足合规要求；

高级能力：

——宜支持存储容量趋势预测能力，基于历史容量增长数据与业务发展规律，预测存储池、核心

目录的容量耗尽时间，辅助容量规划与扩容决策；

——宜支持存储性能瓶颈智能分析能力，可结合业务负载特征与存储性能指标，定位性能瓶颈节点，输出存储性能优化与资源调优建议；

——宜支持存储数据风险智能预警能力，可识别备份长期失效、RAID 冗余不足、磁盘批量劣化等数据丢失风险，提前预警并给出分级处置方案；

——宜支持存储资源智能优化分析能力，可自动识别闲置存储资源、冷热数据分布，给出数据分层存储、闲置资源回收的优化建议，提升存储资源利用率。

7.1.2.3. 物理网络硬件观测

物理网络硬件观测指对银行数据中心交换机、路由器、防火墙等网络硬件设备的运行状态、性能指标、链路连通性与冗余架构进行持续监测、分析与故障定位的能力，用于保障银行网络基础设施稳定运行，防范网络故障引发的业务中断与数据传输风险，支撑网络架构高可用运维。

基本能力：

——应支持交换机、路由器、防火墙等网络设备的运行状态与负载监测，覆盖设备 CPU 使用率、内存使用率、并发会话数、设备运行时长等核心指标，支持负载超标告警；

——应支持网络端口状态与错误统计监测，覆盖端口上下线状态、端口入/出流量、错包率、丢包率、CRC 校验错误等参数，支持端口异常闪断、错误率超标告警；

——应支持光模块运行状态与损耗监测，覆盖光模块发送功率、接收功率、光衰值、工作温度、工作电压等参数，支持光模块劣化、光功率异常告警；

——应支持堆叠与虚拟化链路状态监测，覆盖堆叠成员设备状态、堆叠链路连通性、虚拟化集群成员状态、集群链路健康度等，支持集群分裂、链路中断告警；

——应支持机房布线链路连通性监测，可关联物理链路两端端口状态，识别链路中断、链路闪断等异常，支撑物理链路故障的快速定位；

——应支持链路带宽占用实时监测与趋势统计，可按链路、时间段展示带宽利用率、流量走势，识别带宽拥塞、流量突增等异常场景；

——应支持光纤链路状态监测，可识别光纤中断、光纤衰耗过大等故障，结合光路资源台账快速定位故障点位，支持光纤故障即时告警；

——应支持冗余链路失效监测，可识别双活链路、备份链路的单链路失效状态，告警提示网络冗余能力下降，防范单点故障引发的业务中断；

高级能力：

——宜支持网络硬件故障预测能力，基于端口错误统计、光模块损耗趋势、设备负载规律等历史数据，预测设备与链路的故障风险，提前发布预警；

——宜支持网络流量智能分析能力，可自动识别异常流量、攻击流量、业务流量突增场景，关联业务交易特征，辅助网络容量规划与安全防护决策；

——宜支持网络冗余架构健康度评估能力，可综合评估链路冗余、设备冗余、机房跨区冗余的健康水平，识别架构单点故障风险点并输出优化建议；

7.1.2.4. 操作系统观测

操作系统观测指对物理服务器操作系统层面的系统资源、进程线程、文件系统、网络协议栈、内核事件、系统安全基线、系统日志开展持续采集、监测、告警与统计分析的能力，承接硬件与上层业务应用，及时发现操作系统层面资源耗尽、内核异常、安全基线偏离等风险，规避因操作系统异常引发业务中断，满足金融运维审计、安全合规要求。

基本能力：

——应支持操作系统资源与业务进程监测，覆盖 CPU、内存、Swap、句柄、线程等系统资源，关键业务进程/守护进程运行状态，识别资源耗尽、进程僵死、泄漏、异常重启等风险并配置阈值告警；

——应支持文件系统与网络协议栈监测，覆盖文件系统挂载状态、使用率、inode 占用，TCP 连接、套接字、端口监听状态，识别挂载丢失、inode 耗尽、连接耗尽等异常；

——应支持内核事件、系统日志与安全基线监测，捕获 OOM、panic 等内核高危事件，监控操作系统版本、补丁、账号登录、关键配置变更，识别补丁缺失、非法登录、配置篡改，留存审计日志；

——应支持操作系统资产关联，对接硬件资产台账，记录操作系统版本、内核版本、补丁清单，支撑系统版本全生命周期管理；

高级能力：

——宜支持操作系统风险趋势预测，基于历史资源使用趋势，预测 CPU、内存、文件系统、句柄等资源耗尽时间，支撑容量提前规划；

——宜支持操作系统基线合规校验分析，周期性比对系统配置、账号、补丁基线，自动输出基线偏离清单与整改建议；

——宜支持操作系统故障仿真与影响评估，可模拟 OOM、文件系统只读、网络栈异常等典型 OS 故障，辅助验证应急预案有效性。

7.1.3. 云和虚拟化平台可观测场景

7.1.3.1. 云平台管控与虚拟化观测

云平台管控与虚拟化观测，是对云平台虚拟化层、平台管控层的计算、存储、网络资源以及管控运维运营服务开展监控、分析和评估的过程。目的是及时发现性能、容量、功能、权限、操作等各类潜在异常，保障虚拟化基础设施与云平台管控能力稳定可靠运行，支撑上层业务应用正常运转。

基本能力：

—— 应实现虚拟化宿主机、虚拟机、网络、存储统一基础观测，并实现运行状态可监控、可追

溯；

—— 应实现虚拟化资源池与云平台管控节点容量观测，按日、周、月输出统计报表，并对容量占用设置告警阈值；

—— 应集中采集并留存虚拟化与云平台管控日志，包括宿主机系统日志、虚拟化管理平台日志、虚拟机系统操作日志，以及管控端账号登录、资源创建、配置修改、权限变更、资源删除、调度调整等全量操作日志，满足金融运维合规审计要求；

—— 应实现虚拟化与云平台管控基础故障告警，覆盖宿主机资源过载、虚拟机宕机、磁盘故障、网络中断、虚拟化服务异常，支持阈值触发和常态化告警；

—— 应持续监测云平台管控核心服务与链路可用性，覆盖控制台访问、API 调度、资源管控、数据同步等核心服务，以及管控节点、网络连通和资源调度链路，保障管控能力稳定可用；

—— 应实现多租户管控权限与配置基线观测，查看租户资源访问权限、操作权限、权限有效期，建立管控配置、资源参数、调度规则基线，监测变更并标记偏离基线的非法变更；

—— 应搭建虚拟化与云平台管控基础可视化看板，整合宿主机、虚拟机、资源池、网络、存储、故障告警等核心观测数据，展示平台整体运行状态、资源负载和故障告警信息。

高级能力：

—— 宜实现虚拟化与云平台资源负载、容量智能预测，基于历史性能、容量、业务流量等数据，推演未来一周、一月资源占用趋势，识别资源瓶颈；

—— 宜实现业务关联与多链路关联观测，将虚拟化节点运行数据与上层金融业务系统绑定，评估节点异常对承载业务的影响范围和程度；

—— 宜实现故障智能根因分析，结合日志、指标、链路数据开展多维度关联分析，自动区分硬件故障、配置故障、网络故障、人为操作故障等类别，定位管控异常、调度故障、资源报错根因；

—— 宜实现变更、备份恢复与自动化合规分析，汇总运维操作、故障处置、权限管控、变更记录，输出适配金融监管要求的运维合规报表；

—— 宜建立运维观测数据分析复盘体系，依托历史观测数据自动生成月度、季度、年度虚拟化与云平台运维分析报告，支撑持续优化；

—— 宜建立云平台管控操作行为观测基线，依据操作习惯、权限范围、操作时段，识别批量删资源、异地登录、高危操作、越权尝试等异常行为；

—— 宜搭建云平台综合观测大屏，整合资源状态、故障告警、操作风险、容量趋势、合规情况，实现运维与风险态势全景可视。

7.1.3.2. 容器与微服务基础设施观测

容器与微服务基础设施可观测体系，面向金融云原生架构，覆盖容器集群、网关、服务网格、注册中心全栈底座，通过指标、日志、链路、事件一体化采集分析，实现基础设施可视、故障可溯、风险可控、容量可判，全面保障分布式业务稳定运行。

基本功能：

——应实现全栈资源指标可视。统一采集集群节点、容器Pod、网关及微服务的CPU、内存、网络、吞吐量、时延、成功率、QPS等核心指标，支持多维度聚合展示，实时呈现集群资源水位与业务运行态势。
——应实现容器全生命周期监控。完整覆盖容器调度、拉起、运行、退出全流程，精准识别镜像拉取失败、调度异常、Pod重启、OOM退出等常见故障，实现问题早发现、早预警。
——应实现服务注册状态观测。持续监测注册中心健康状态与服务实例心跳、上下线变更，及时识别实例批量离线等异常，保障微服务治理稳定性。
——应实现全量日志归集检索。统一采集容器、网关、服务网格运行日志，支持多条件快速检索，还原故障现场上下文，满足金融运维追溯与合规要求。
——应实现分布式链路追踪。贯通网关、网格、业务应用的全链路调用，实现指标、日志、链路数据联动关联，快速定位跨服务调用异常与卡顿问题。
——应实现标准化告警管控。针对资源过载、流量突变、服务报错、实例离线等风险场景，配置分级告警规则，实现异常实时通知、问题快速处置。

高级功能：

——宜依托业务潮汐特征构建动态告警基线，区分业务正常峰谷波动与真实异常隐患，有效过滤无效告警，大幅提升告警研判精准度。
——宜自动绘制全局服务调用拓扑，动态识别上下游依赖关系，针对时延突增、频繁重启、成功率下跌等故障，开展多层级根因辅助推理。
——宜精细化分层拆解调用耗时，区分网关路由、网格转发、网络传输、业务执行耗时差异，精准定位性能瓶颈所在层级。
——宜具备资源容量趋势预判能力，基于历史资源消耗与业务增长规律，预测资源饱和时点，输出扩容等容量优化建议。

7.1.4. 基础软件可观测场景

7.1.4.1. 消息中间件观测

消息中间件观测指对银行系统中用于异步解耦、流量削峰、数据同步的消息中间件集群的运行状态、消息流转性能、数据可靠性进行持续监测与分析的能力，保障支付清算、账务通知、数据同步等业务场景的消息传输稳定可靠。

基本能力：

——应支持消息流转全维度监测，按主题/队列/分区监测堆积水位、生产消费 TPS，识别堆积、速率异常波动；监测消费失败、消息丢失、死信队列、重试机制、事务消息状态，对堆积超限、消费失败、重试耗尽、事务异常配置告警；

——应支持 Broker 节点运行状态与资源负载监测，覆盖 Broker 磁盘占用率、内存使用率、CPU 使用率、节点存活状态等，支持节点故障与资源过载告警；

——应支持分区同步延迟监测，可统计主从分区、副本间的消息同步延迟量与延迟时长，支持同步延迟超标告警，保障消息数据冗余可靠性；

——应支持事务消息状态监测，可跟踪事务消息的提交、回滚、悬挂状态，统计事务消息回滚率，支持事务消息异常告警。

——应支持安全与操作审计，留存消息中间件管理账号登录、权限变更、配置修改操作日志，识别异常账号访问、高危配置变更，满足金融审计追溯；

——应支持备份任务监测与校验，跟踪集群元数据、主题配置备份任务执行状态、备份完整性，识别备份失败、备份文件损坏，留存备份操作审计记录。

高级能力：

——宜支持消息堆积智能预测能力，基于业务流量规律与历史堆积数据，预测业务峰值下的消息堆积风险，提前给出扩容与削峰建议；

——宜支持消息中间件容量智能评估能力，结合业务增长趋势评估集群容量水位，给出集群节点扩容、分区扩缩容的优化建议；

——宜支持消息链路端到端追踪能力，可关联业务交易与消息流转全路径，实现业务交易→消息生产→消息消费→业务落地的全链路可观测。

7.1.4.2. 应用中间件观测

应用中间件观测指对承载银行业务应用的 Web 容器、应用服务器等中间件的运行状态、资源使用、请求处理性能进行持续监测与分析的能力，保障渠道接入、业务服务等应用系统的稳定运行与服务性能。

基本能力：

——应支持 JVM 与线程资源监测，采集堆/分代内存、GC、FullGC、线程、死锁、线程池指标，识别内存溢出、频繁 FullGC、线程死锁、线程池耗尽并告警；

——应支持连接池运行状态监测，覆盖数据库连接池、服务连接池的活跃连接数、空闲连接数、等待连接数、连接超时次数，支持连接池耗尽告警；

——应支持请求处理性能监测，可统计请求吞吐量、平均响应时间、请求排队时长、请求错误率，支持请求时延突增、错误率上升告警；

——应支持 Servlet 请求处理全量监测，可统计各接口的请求量、耗时、报错分布，支持慢接口识别与告警；

——应支持会话状态监测，覆盖在线会话数、会话超时率、会话异常断开数，支持会话数突增、异常断开率超标告警；

——应支持实例生命周期与节点资源监测，识别应用启动失败、超时、端口冲突，采集节点 CPU/内存/磁盘 IO，对启动异常、节点资源过载告警；

——应支持安全审计与配置备份观测，留存中间件账号登录、权限变更、配置修改审计日志；监测配置备份任务执行状态，识别备份失败，满足运维合规追溯。

高级能力：

——宜支持 JVM 内存泄漏智能识别能力，基于长期内存运行趋势分析内存泄漏风险，给出泄漏可疑点与优化建议；

——宜支持应用性能瓶颈智能诊断能力，可自动关联请求、线程、JVM、连接池等多维度指标，

定位应用性能瓶颈根因，输出优化方案；

——宜支持应用容量弹性评估能力，结合业务流量增长预测应用中间件的容量水位，给出节点扩缩容、资源配置调优建议；

——宜支持应用异常自动溯源能力，应用报错、请求失败时可自动关联对应日志、线程栈、链路追踪数据，辅助快速定位问题代码与依赖组件。

7.1.4.3. 交易中间件观测

交易中间件观测指对支撑银行核心账务、支付清算等联机交易的交易中间件的运行状态、交易负载、服务可用性进行持续监测与分析的能力，保障核心交易的高并发处理能力与交易一致性，满足核心业务连续性要求。

基本能力：

——应支持交易服务与会话资源监测，采集服务组吞吐量、并发、响应时延、服务阻塞排队、会话占用状态，识别服务过载、阻塞、会话耗尽 / 泄漏并告警；

——应支持跨节点交易调用状态监测，可统计跨节点调用的成功率、响应时延、调用失败分布，支持跨节点调用失败率上升告警；

——应支持分布式事务状态监测，可跟踪事务提交、回滚、悬挂状态，统计事务回滚率、事务超时率，支持事务异常告警，保障交易一致性；

——应支持交易中间件节点健康状态监测，覆盖节点存活状态、资源负载、服务进程状态，支持节点故障、进程异常退出告警；

——应支持交易路由与流量分布监测，可展示交易请求在各服务组、各节点间的路由分布与流量占比，支持流量不均告警；

——应支持交易异常事件全量记录，包含交易超时、交易失败、事务回滚等事件的交易编号、时间、节点、报错信息，支撑交易故障追溯；

——应支持安全审计与备份观测，留存运维账号登录、权限变更、交易规则 / 路由配置变更操作日志；监测集群配置备份任务状态，识别备份失败，满足交易运维审计合规。

高级能力：

——宜支持核心交易异常智能根因定位能力，交易失败、超时异常发生时，可自动关联交易链路、服务状态、资源负载、数据库性能等多维度数据，定位异常根因与影响交易范围；

——宜支持交易容量压力预测能力，基于历史交易峰值数据与业务增长趋势，预测交易中间件的容量瓶颈，给出服务组扩容、资源调优建议；

——宜支持交易流量智能调度分析能力，结合各节点负载与服务健康状态，给出流量路由优化、服务组动态调整的调度建议，提升交易处理整体性能；

——宜支持交易一致性风险预警能力，可识别悬挂事务、分布式事务不一致等风险场景，提前预警并给出处置指引，保障核心账务数据一致性。

7.1.4.4. 缓存中间件观测

缓存中间件观测指对银行系统中用于数据加速、热点数据访问的缓存中间件集群的运行状态、性能表现、数据可靠性进行持续监测与分析的能力，保障热点业务数据的高效访问，防范缓存失效引发的后端系统压力过载风险。

基本能力：

——应支持缓存业务指标监测，统计读写命中率，识别大 Key、热 Key；监测缓存穿透、击穿、雪崩风险场景，对命中率骤降、大/热 Key 异常进行告警；

——应支持缓存内存资源状态监测，覆盖已用内存、内存使用率、内存淘汰次数、淘汰 Key 数量，支持内存使用率超标、频繁内存淘汰告警；

——应支持主从同步状态监测，可统计主从同步延迟、同步数据量、副本存活状态，支持同步中断、延迟超标告警，保障缓存数据冗余可靠性；

——应支持缓存节点运行状态监测，覆盖节点存活状态、CPU 使用率、连接数、QPS，支持节点宕机、连接数耗尽、QPS 突增异常告警；

——应支持缓存持久化状态监测，可跟踪 RDB/AOF 持久化执行状态、持久化耗时、持久化文件大小，支持持久化失败告警；

——应支持安全审计与备份观测，留存缓存账号登录、权限变更、配置修改审计日志；监控元数据与实例配置备份任务状态，识别备份损坏、备份失败，满足合规追溯。

高级能力：

——宜支持缓存性能智能优化能力，结合大 Key、热 Key 分布与业务访问特征，给出缓存 Key 拆分、热点数据多级缓存、过期时间优化的调优建议；

——宜支持缓存雪崩风险智能预警能力，基于 Key 过期时间分布、业务流量预测，识别批量 Key 同时过期的雪崩风险，提前给出平滑过期、兜底保护建议；

——宜支持缓存容量智能规划能力，结合业务数据增长与访问趋势，预测缓存集群容量需求，给出节点扩容、内存配置优化的规划建议。

7.1.4.5. 集中式数据库观测

集中式数据库观测指对承载银行核心账务、客户信息等关键数据的集中式数据库的运行状态、性能表现、资源负载、数据可靠性进行全维度持续监测与分析的能力，保障核心数据的安全可靠与数据库高效运行，满足银行业务连续性与数据安全监管要求。

基本能力：

——应支持会话、锁与事务监测，采集连接数、活跃 / 空闲 / 等待会话；监测行锁表锁等待、死锁；跟踪长事务、事务回滚，对连接耗尽、锁阻塞、长事务、事务异常告警；

——应支持 SQL、日志与表空间监测，采集慢 SQL 执行信息；监控 Redo/Undo、回滚段、归档日志运行状态；监测表空间使用率，识别归档失败、表空间容量越限告警；

——应支持索引与主备副本监测，识别失效、冗余索引，监控索引命中率；监测主备同步延迟、备库存活，对索引异常、同步中断、延迟超标告警；

——应支持数据库安全审计观测，监测特权账号登录、高危 DDL/DML 操作、权限变更、敏感数据访问行为，留存全量访问与操作审计日志，对高危操作、异常访问告警；

——应支持备份恢复全流程观测，跟踪全量 / 增量备份任务进度、耗时、完整性校验；监控备份存储容量、备份链路状态；支持备份恢复验证，记录恢复演练结果，识别备份失败、备份文件损坏，留存备份恢复操作审计日志。

高级能力：

——宜支持数据库性能瓶颈智能诊断能力，可自动关联慢 SQL、锁等待、资源负载、索引状态等多维度数据，定位性能瓶颈根因，输出 SQL 优化、索引优化、参数调优等建议；

——宜支持数据库容量趋势预测能力，基于历史表空间增长、数据量变化趋势，预测表空间耗尽时间，给出容量扩容、数据归档的规划建议；

——宜支持数据库健康度综合评估能力，基于性能、容量、可靠性、安全等多维度指标，综合评估数据库健康水平，识别潜在风险点并给出分级处置建议。

7. 1. 4. 6. 分布式数据库观测

分布式数据库观测指对银行分布式架构场景下的分布式数据库集群的运行状态、分片负载、数据同步、事务一致性进行持续监测与分析的能力，保障分布式架构下银行业务数据的可靠存储与高效访问，支撑分布式核心系统的稳定运行。

基本能力：

——应支持分片、迁移与扩缩容监测，监控各分片流量、资源负载，识别分片负载倾斜；跟踪分区迁移、集群扩缩容进度，对负载不均、迁移/扩缩容失败超时告警；

——应支持分布式事务与 SQL 性能监测，统计两阶段提交成功率、耗时、回滚、悬挂事务；识别跨分片慢 SQL、低效查询，对事务异常、慢 SQL 性能劣化告警；

——应支持集群节点与副本同步监测，采集计算、存储节点存活状态与资源负载；监控副本同步延迟、同步量，识别副本同步中断、延迟超标告警；

——应支持全局数据一致性校验，定期校验分片间数据一致性，识别数据不一致并告警；

——应支持安全审计观测，监测特权账号登录、高危数据操作、权限变更行为，留存全量访问、DDL/DML 操作审计日志，识别异常访问、高危操作告警；

——应支持备份恢复观测，跟踪集群全量/增量备份任务、备份链路、备份文件校验，支持备份恢复验证，识别备份失败、备份损坏，留存备份恢复操作审计记录。

高级能力：

——宜支持分布式数据库负载智能调优能力，结合分片负载分布与业务访问特征，给出分片拆分、数据迁移、负载均衡策略优化的调优建议，提升集群整体性能；

——宜支持分布式事务异常智能诊断能力，事务回滚、悬挂、一致性异常发生时，可自动关联事务链路、节点状态、网络时延等数据，定位异常根因与影响数据范围；

——宜支持分布式数据库容量智能规划能力，基于业务数据增长趋势与分片容量分布，预测集群容量瓶颈，给出节点扩容、分片拆分的规划建议；

——宜支持分布式集群故障自愈分析能力，节点故障、网络分区等异常发生时，可自动评估集群冗余能力与故障影响范围，给出故障切换、流量调度的自愈处置建议。

7.1.4.7. 数据仓库观测

数据仓库观测指对银行用于数据分析、报表加工、批量数据处理的数据仓库的任务运行状态、数据处理性能、数据质量进行持续监测与分析的能力，保障监管报表、经营分析、数据加工等业务的按时完成与数据准确。

基本能力：

——应支持 ETL 及批量任务全流程监测，跟踪 ETL 任务进度、运行时长；监测数据源加载延迟、批量任务依赖拓扑、资源抢占、临时磁盘占用，识别任务失败、超时、阻塞、资源冲突、磁盘溢出并告警；

——应支持批量作业统计与数据质量校验，统计任务成功率、失败率；监测脏数据、重复、丢失等数据质量异常，对数据质量问题告警；

——应支持数据分区状态监测，可识别分区缺失、分区异常、分区数据倾斜场景，支持分区异常告警，保障查询与加工性能；

——应支持数据加工质量校验监测，可统计数据加工过程中的脏数据、数据丢失、数据重复情况，支持数据质量异常告警。

——应支持安全审计观测，监测批量作业账号、仓库管理账号登录、权限变更、表 / 视图高危操作，留存操作审计日志，识别异常访问、高危变更告警；

——应支持备份恢复观测，跟踪仓库模型、数据表备份任务执行状态、备份校验，支持备份有效性验证，识别备份失败，留存备份恢复操作审计记录。

高级能力：

——宜支持批量任务智能调度优化能力，结合任务依赖关系、资源占用、运行时长，给出任务调度时序、资源分配的优化建议，提升批量作业整体执行效率；

——宜支持批量任务运行时长预测能力，基于历史任务运行数据与数据量变化，预测本次任务运行时长，评估批量作业能否按时完成，提前预警延期风险；

——宜支持离线数据处理瓶颈智能诊断能力，批量任务变慢、执行失败时，可自动关联数据量、资源负载、SQL 性能、依赖任务等维度数据，定位瓶颈根因与优化方向；

——宜支持批量作业风险智能预警能力，可识别任务依赖风险、资源冲突风险、数据质量风险，提前发布预警并给出处置建议，保障批量作业稳定运行。

7.1.5. 业务交易链路端到端可观测场景

7.1.5.1. 前端渠道交易链路观测场景

银行前端渠道交易链路观测，是针对手机银行、小程序、网上银行、柜面、ATM、POS、远程银行等全渠道前端触点，基于端侧监控、链路追踪、设备感知、会话监测、主动拨测等技术手段，对交易全流程、用户体验、设备状态、会话质量、异常故障进行全方位监测、分析与告警的能力，构建“端—渠道—中台—核心”全链路观测闭环，实现前端交易问题早发现、早定位、早处置，保障全渠道交易稳定运行、用户体验合规可控，满足银行业务连续性与服务质量管控要求。

基本能力：

——应支持全渠道前后端链路贯通与黄金指标可观测，通过 TraceID 协议注入与网关透传，打通 RUM 与 APM，围绕可用率、响应时延、交易吞吐量建立监测能力，串联全层级调用，还原故障现场，杜绝链路断点。

——应支持多端 RUM 全量监测，覆盖网银、手机银行等，采集性能指标、报错、崩溃、卡顿，适配鸿蒙等边缘场景，全方位感知用户体验。

——应支持前端接口多维监控与下钻，统计 API 成功率、耗时及异常，按地域、网络、机型等维度拆解，精准识别慢接口，联动 TraceID 定位后端瓶颈。

——应支持物理终端设备健康与外设监测，覆盖 ATM/POS 等，实时采集在线率、硬件工况，分级识别异常，记录操作日志与时长，保障设备合规与业务高效。

——应支持远程银行会话质量监测，监控音视频延迟、丢包、接通率，统计坐席状态与效率，实现全程留痕可追溯。

——应支持全渠道主动拨测，模拟核心交易链路，常态化监测，联动 RUM 区分网络/CDN/后端故障，提前感知服务不可用与性能退化。

——应支持前端异常分级告警与聚合，基于环比同比阈值触发多级告警，适配复合条件与版本关联，规避误报，精准捕捉性能与报错风险。

高级能力：

——宜支持跨渠道统一用户旅程还原，生成跨渠道会话 ID，串联操作片段，可视化展示路径耗时与异常，识别断点，支撑体验优化。

——宜支持灰度发布与 AB 实验观测，监控版本覆盖率与回滚，对比新旧版本体验指标，智能告警劣化，支持流量染色与 AB 对比，保障迭代安全。

——宜支持端侧性能劣化智能预测，基于历史数据构建动态基线，识别首屏耗时、崩溃率等趋势，按机型网络分桶预判，规避大规模体验问题。

——宜支持全维度网络质量画像与故障定界，分析网络耗时与异常率，区分客户端、CDN、后端故障，监控 CDN 命中率，识别区域与运营商异常。

——宜支持前端异常智能聚类与根因分析，聚类慢请求与报错，关联堆栈日志及版本事件，精准定位根因，形成感知-定位-处置闭环。

——宜支持多渠道统一体验治理，搭建统一体验指标与 SLA 体系，统一统计口径，对比多渠道体验，实现标准化与常态化治理。

——宜支持物理终端预测性运维，基于运行参数趋势预判部件故障，结合远程与静默运维，缩短处置时长，降低巡检成本与业务影响。

7.1.5.2. 核心账务联机交易观测场景

核心账务联机交易观测，是针对银行转账、存款等核心联机交易，依托全局流水号链路追踪、交易指标监控、事务状态感知、日志联动告警等能力，对交易全流程风险场景开展全方位监测、定位与预警，覆盖渠道、网关、中间件、数据库、外联清算全链路，实现交易故障可视、可查、可报。

基本能力：

——应支持核心账务交易全链路监控，并依托全局唯一流水号与 TraceID 贯穿渠道、网关、中间件、核心账务、数据库、外联清算全节点链路的可观测，支持设置及可视化黄金三指标以及与账户关联性较高的运行指标包括流量、时延、成功率与业务错误码等，支持多关键字精准检索单笔交易全量信息；

——应支持分交易码成功率实时监控能力，可按转账、存取款、开户、挂失、理财、基金申赎等各类交易码独立统计交易成功率，剔除用户侧无效交易数据，支持多维度下钻分析，配置分级 SLO 阈值告警，实时感知核心交易运行态势；

——应支持交易超时与慢交易精准定位能力，可统计多档位响应时间分位数，自动梳理慢交易、超时交易清单，精准区分客户端、网关、应用、数据库、外联接口等不同超时根因；

——应支持重复交易与幂等性监测能力，可统计系统重复请求率、幂等键命中频次，对账号、金额、凭证等关键要素一致的重复交易行为实时识别预警；

——应支持分布式事务全流程监控能力，可可视化监测 TCC、Saga、AT 等分布式事务各执行阶段成功率，统计事务补偿失败率，精准识别空回滚、事务悬挂等异常状态；

——应支持核心交易关键节点耗时拆解能力，可对余额校验、资金冻结扣减、流水生成、凭证登记、总账入账等账务核心环节进行耗时拆解，快速定位交易链路性能瓶颈；

——应支持观测数据联动与智能告警能力，实现指标、日志、链路追踪数据全关联，支持一键穿透查询异常详情。

高级能力：

——宜支持交易异常智能根因分析能力，基于日志聚类、指标因果关联、链路请求聚类多维度研判，自动区分根因节点与连带异常节点，数字化定位交易故障根源，大幅降低人工排查成本；

——宜支持交易异常聚类与动态基线识别能力，可对慢交易、错误交易进行智能归类，依托历史业务数据训练动态监测基线，精准识别交易流量、耗时、成功率的突增突降异常，同时可识别异常交易行为与高风险账户；

——宜支持单笔交易全链路回放与回溯能力，支持多业务关键字检索任意交易，全量解码还原微服务交易现场，长期留存链路数据，满足故障复盘、问题追溯与合规审计要求；

——宜支持账务资损风险主动预警能力，可实时识别单边账、长期挂账、交易掉单等高危场景，

监控日间及日终对账差异率，对大额异常交易精准预警，实现从被动对账向主动风险防控升级；

——宜支持交易冲正补偿全流程监控能力，可实时统计冲正触发率、冲正成功率，严控冲正滥用风险，完整记录分布式事务补偿链路状态，对补偿失败场景实时告警，筑牢账务数据安全底线；

——宜支持智能运维与故障自愈能力，支持异常节点自动隔离、参数自适应调整，结合混沌工程持续验证观测体系有效性。

7.1.5.3. 批处理观测场景

批处理观测是面向金融账务批量、定时任务调度、批量依赖作业构建的批量作业全生命周期可观测体系。覆盖批量任务执行进度、资源占用、调度时序、依赖链路、异常特征，重点针对定时任务未调起、执行失败、运行超时、重复调起四类典型调度风险建立标准化观测能力，实现批量作业运行透明、异常可控、风险可防、优化可量化，保障金融夜间账务批量、日终结算、数据归档等核心批量作业稳定按期完成。

基本功能：

——应具备批量任务全量指标采集能力，基于批量调度拓扑采集任务启动时间、执行进度、运行时长、重试次数、依赖状态；

——应具备批量资源占用监测能力，持续观测批量作业对服务器算力、数据库连接、中间件队列、磁盘 IO、网络资源的占用情况，识别批量任务资源挤占特征，关联任务异常与资源瓶颈；

——应具备批量异常标准化告警能力，针对任务超时未完成、前置依赖失败、任务停滞阻塞、资源过度占用、定时任务漏调、失败、超时、重跑等场景，实现分级告警、精准触达；

——宜具备批量完工时间智能预测能力，基于平日、月末、季末、年末账务周期的历史运行数据，构建批量耗时基线，动态预判本批次预计结束时间，提前预警超时风险，避免挤占日间运维与交易窗口；

——应具备批量运维可视化能力，搭建专属批量任务监控大盘，可视化展示调度计划、依赖拓扑、实时执行进度，对异常、卡顿、漏调度、重调度任务醒目标记，支持历史批次报表与异常明细审计导出。

高级功能：

——宜具备批量逐级溯源根因能力，对四类定时任务异常自动归类根因，区分配置错误、调度中心异常、资源不足、网络异常等诱因；

——宜具备批量与联机资源隔离观测能力，可实时识别批量任务挤占联机交易数据库、算力、队列资源的行为，以联动调度策略实现资源配额管控，保障日间联机交易资源优先级；

——宜具备批量分片策略动态优化能力，根据每日账务数据量波动自适应调整并行分片度，平衡批量执行效率与数据库负载，规避分片不合理导致的任务堆积、超时、重复执行问题；

——宜具备跨周期批量运行对比分析能力，自动对标历史同期批次的耗时曲线、资源负载、调度成功率，精准识别版本迭代、业务规则变更、数据量增长带来的性能退化与调度异常，形成常态化优化依据；

——宜具备定时任务全局幂等观测与隐性风险巡检能力，基于全局调度唯一标识识别跨节点重

复调起行为，实现实时预警拦截；

7.1.5.4. 第三方外联交易观测场景

第三方外联交易观测，是针对银行与银联、网联、人行清算、第三方理财、银证等外部机构的各类外联交易，适配多类异构协议、异步交互、跨机构对账、限时清算的业务特征，覆盖交易组包、签名、传输、应答、对账、清算全生命周期，实现全流程可视化监测、异常精准预警、风险闭环管控。

基本功能：

——应支持端到端报文全链路监控、追踪与可视化，基于全局流水号贯通行内、前置及第三方全节点，适配 ISO8583 等异构协议，留存原始报文快照，支持多维关键字检索。

——应支持分第三方外联交易收发黄金三指标的可观测及账务可观测，包含成功率、时延、吞吐率、重传次数、疑似单边账笔数，按银联、网联等各类通道及报文类型统计成功率与丢失率，支持多维度下钻分析，实时掌握通道运行态势。

——应支持报文格式错误精准捕获，识别编码异常、字段缺失、校验失败等，按通道/机构统计异常率，自动生成协议合规评分与告警。

——应支持全维度对账差异监控，覆盖日间滚动与日终批量，监测对账任务执行状态，精准统计差异笔数与差异率，及时发现账务偏差。

——应支持外联专线与链路全栈质量监控，实时监测连通率、丢包、时延、TCP 重传、连接池等指标，区分网络层与应用层异常，确保链路稳定。

——应支持交易状态一致性核对，监测全流程状态流转，识别悬挂、未结、重复等异常，主动触发查询核验，保障行内外交易状态最终一致。

——应支持清算窗口时效全流程监控，实时感知清算系统状态与截止时限，监控交易积压、排队、备付金水位，及时预警清算超时与资金滞留。

高级功能：

——宜支持多通道智能择优与故障自愈，基于成功率、时延、费率等特征自动遴选最优通道，主通道异常时毫秒级无感切换备用通道，保障高可用。

——宜支持报文异常智能聚类与字段级归因，自动归类格式异常，精准定位异常字段与机构，关联版本变更，量化合规水平，支撑整改与对接。

——宜支持跨境跨时区清算智能预测排程，适配多时区窗口差异，预判清算完成时效，对临近截止大额交易预警，智能匹配最优窗口与通道。

——宜支持监管报送数据自动穿透校验，自动比对原始报文、账务与报送数据的一致性，校验完整性、准确性，降低违规风险，满足动态监管。

——宜支持第三方 SLA 智能管控与自动取证，自动采集各机构 SLA 指标，对违约留存完整证据链，精准界定责任，支撑考核与商务维权。

——宜支持异常报文自动重发与账务补偿闭环，基于幂等安全重传，识别单边账风险，自动触发

冲正补偿，对失败场景告警，形成处置闭环。

——宜支持智能对账与差异自动核销，实现高频滚动实时对账，智能分类差异成因，自动核销常规差异，依托 AI 提升准确率，降低人工成本。

————宜支持通道灰度验证与流量安全管控，支持测试流量染色隔离、影子通道校验，上线前灰度放量及混沌测试，提前暴露风险，保障生产稳定。

7.2. 故障应急可观测场景

7.2.1. 基础设施

基础设施故障应急可观测是银行智能运维故障应急体系的核心基础场景，覆盖服务器、存储、网络、动环等基础设施层故障发现、告警收敛、分级处置与应急响应全流程。基础设施单点故障极易经调用链传导至核心交易系统，引发交易中断、服务失效、监管报送延误等重大业务风险。本标准通过构建统一告警接入与智能分级体系，依托多源可观测数据实现故障精准识别、告警降噪与快速处置，保障应急过程全程可控、可追溯、合规，最大限度降低基础设施故障对业务连续性的冲击。

基本要求：

——应全面采集服务器、存储、网络设备及机房动环等硬件与环境指标，确保采集频率不低于分钟级，关键传感器支持秒级轮询；

——应建立硬件级故障特征库，针对磁盘 SMART 预警、内存 ECC 纠错计数、电源电压漂移、CPU 过热、存储控制器超时等典型故障模式，配置差异化告警阈值与判定规则，区分故障等级，减少误报漏报；

——应具备硬件故障快速定位能力，故障触发时自动关联设备型号、部件位置、序列号、固件版本及历史维修记录，输出明确故障部件，并提供现场更换或维护指引；

——应自动分析基础设施故障对上层业务的影响范围，快速映射出受影响的应用服务、交易渠道及客户群体，生成影响评估摘要供应急决策；

——应针对高频硬件故障预设标准化处置脚本或操作流程，支持一键执行故障隔离、触发主备切换、自动调用备件库通知等，缩短人为响应时间；

——应全量记录基础设施故障从传感器告警、自动诊断、人工确认、备件更换、恢复验证的全过程操作日志，留存部件序列号、更换时间、操作人、系统日志截图，确保故障处置可追溯、可审计；

——应基于历史故障数据统计设备类型故障率、平均修复时间（MTTR）、平均无故障时间（MTBF）、备件消耗周期，按月度/季度输出可靠性分析报告，定位高故障率机型、批次缺陷或老化趋势；

——应支持基础设施故障应急演练，通过模拟电源中断、磁盘离线、空调失效等场景，验证监控覆盖率、诊断准确性及处置流程有效性，定期优化预案并更新知识库。

高级要求：

——宜基于设备传感器时序数据训练机器学习异常检测模型，提前识别硬件亚健康状态，实现故障预测，触发主动更换，减少突发宕机；

——宜构建基础设施数字孪生模型，实时映射机房内设备布局、电力负载、热力分布，当发生环境异常时，自动模拟通风、电力切换等干预效果，辅助精准决策；

——宜将基础设施监控数据与 CMDB、变更管理联动，当硬件故障发生时，自动查询近期该设备是否有固件升级、配置修改或扩容操作，辅助判断是否因变更引发，并推荐回滚或补偿措施；

——宜利用根因分析算法，综合服务器、存储、网络、环境等多源数据，区分“硬件自身故障”“外部供电波动”等不同源头，并给出因果链路；

——宜自动生成基础设施健康度评分，涵盖设备剩余寿命、部件冗余度、散热效率、供电稳定性等维度，并定期推送巡检报告，为基础设施容量规划、绿色节能优化提供决策支持；

——宜搭建统一的基础设施应急态势看板，实时展示各机房设备运行状态、故障部件高亮、备件库存及维保人员到岗情况，支持应急指挥中心远程查看现场传感器数据，协同多地团队快速响应。

7.2.2. 全域告警收敛与分级

基础设施故障应急可观测是银行智能运维故障应急体系核心基础场景，覆盖服务器、存储、网络、动环等基础设施故障发现、告警收敛、分级处置、应急响应全流程。基础设施单点故障易经调用链传导至核心交易，引发交易中断、服务失效、监管报送延误等重大风险。本标准通过统一告警收敛与智能分级体系，依托可观测数据实现故障精准识别、降噪与快速处置，保障应急全程可控、可追溯、合规，最大限度降低基础设施故障对业务连续性的冲击。

基本要求：

——应统一接入服务器、存储、网络、动环多源异构告警，标准化建模并完成去重、压缩、富化，保障告警全采集、格式统一、时间戳准确，夯实告警收敛数据基础；

——应具备告警智能降噪收敛能力，依托拓扑、时间窗口、依赖关系算法处理风暴、级联、重复、闪断类告警，聚合输出根因事件，减少噪声、避免关键故障漏判；

——应依据银行业务连续性规范，按故障对核心交易影响自动划分告警等级，配套差异化响应流程、处置时效与升级机制，实现分级标准化管控；

——应依托 CMDB 资源与设施依赖图谱自动生成故障关联拓扑，关联映射故障设备承载应用、数据库、中间件及上游交易链路，精准定位受影响业务、模块与用户；支持拓扑下钻查询指标、告警、变更记录，缩短故障排查与影响评估时长；

——应完整记录告警触发、研判、处置、恢复、验证全流程操作数据，留存处置时间、人员、操作指令、结果、回滚等信息，满足监管、审计的全程可追溯、可复盘要求；

——应按故障等级与业务重要程度，通过短信、电话、邮件、运维平台、企业 IM 多通道分级推送通知，精准触达值班、业务、管理负责人；支持未响应逐级升级，杜绝重大故障通知漏发、延迟；

——应自动统计故障频次、影响时长、设备类型、业务范围、处置耗时等指标，按日/周/月/季输出报表与趋势分析，支持多维度下钻，定位薄弱设备与短板，支撑容量规划、设备更新、架构优化决策；

——应针对服务器宕机、存储/网络/电源切换等高频故障预设自动化处置预案与脚本，人工确认

后一键执行故障隔离、流量切换、备份激活，同步反馈执行进度，缩短恢复时长、降低人工操作风险。

高级要求：

——宜基于 CPU、内存、磁盘 IO、网络、温度等时序指标训练机器学习模型，构建设备健康度与故障预测模型，在指标劣化未达告警阈值时提前预警，预判故障概率与劣化周期，实现运维由被动应急向主动预防转型；

——宜整合告警、日志、指标、变更、环境数据，通过因果推理与知识图谱自动定位硬件老化、固件缺陷、配置漂移、容量不足、环境异常等深层根因，配套指标基线、历史案例等举证信息，输出定位与处置建议；

——宜自动量化故障影响服务器、存储、带宽、交易链路规模，核算交易失败量、中断时长、客户覆盖范围等业务指标，自动生成影响评估报告，支撑定级、监管上报、业务协同；

——宜针对进程异常、IO 超时、端口抖动等可自愈故障，按预设安全策略自动执行重启、路由切换、流量调度等自愈操作，自愈后校验健康状态；自愈失败自动升级人工处置，在安全前提下压缩故障恢复窗口；

——宜基于历次应急全量数据识别预案耗时瓶颈、冗余步骤、依赖缺失问题，持续优化脚本、参数、回滚策略，横向比对同类故障处置效能，迭代提升应急处置能力；

——宜搭建融合物理拓扑、逻辑架构、业务部署的应急态势可视化大屏，实时展示故障分布、告警等级、业务影响、人员就位、处置进度，支持多屏联动，为应急指挥提供全局决策视图。

7.2.3. 全链路故障定位

全链路故障定位是银行智能运维故障应急体系实现交易级故障精准定界、快速定位的核心场景，依托分布式调用链追踪，对手机银行、网银、柜面、ATM、POS 等前端渠道至应用、中间件、数据库、核心系统的全链路交易调用做端到端追踪可视化。银行业单笔交易跨大量服务节点与多层技术栈，超时、失败、异常故障存在链路长、依赖复杂、异构系统多等定位难点。本标准搭建银行全链路故障定位体系，依靠标准化调用链采集、智能故障节点定位、自动根因推断，实现交易级故障一键追踪精准定位，支撑业务故障快速定界、高效处置与持续优化。

基本要求：

——应支持银行全渠道交易调用链标准化采集接入，覆盖多类渠道与协议，遵循 OpenTelemetry 生成标准 TraceID、SpanID 及层级关联，完整记录全层级调用路径、节点耗时、状态码、异常堆栈，保障采集完整无偏差，提供故障定位完整数据底座；

——应自动生成并实时更新交易调用链拓扑图谱，端到端展示渠道、网关、服务、中间件、数据库、核心系统调用关系，节点标注健康状态、耗时、错误率，支持按交易、渠道、时间筛选，直观呈现链路全局健康态势；

——应支持由交易告警、异常指标关联流水号、用户标识、渠道编号一键调取完整 Trace 详情，分层展示各 Span 耗时、参数、SQL、缓存记录、返回码、异常堆栈，自动标红慢节点、故障断点，按耗时排序快速锁定性能瓶颈；

——应跨技术栈自动判定故障层级与对应服务实例，跨系统故障提取双方请求、响应、参数、返回数据，明确故障责任，消除跨系统排查盲区与推诿问题；

——应实现调用链 Span 与同期应用/系统/慢查询日志、JVM、接口指标、变更事件自动关联，统一视图聚合多源故障线索，打破信息孤岛，缩短定位与根因分析时长；

——应定位故障节点后自动统计窗口期受影响交易、渠道、用户分布及失败率，量化故障业务影响范围与严重程度，支持多维度拆分排序，为应急决策提供量化依据；

——应将故障时段链路耗时、成功率、延迟等指标与历史基线自动比对，识别异常 Span、新增/消失异常路径，锁定故障引入时点与关联变更，支撑变更回滚决策；

——应支持采样策略动态调节，日常按交易、渠道、用户分级自适应采样控成本，检测错误率、延时突增时自动切换全量采集，完整留存异常交易链路数据用于故障取证。

高级要求：

——宜基于机器学习训练链路画像与性能基线模型，实时识别异常路径、节点性能跳变、流量模式偏移，依托异常 Span 因果图自动推导根因节点与故障传播路径，自主从海量链路数据识别异常定位根源；

——宜时序关联故障链路与同期发布、配置、数据库、网络、基础设施变更，做因果分析并输出变更相关可信度与证据链，辅助判断是否执行变更回滚；

——宜针对支付、账务、理财、贷款、信用卡、监管报送等银行典型业务搭建差异化诊断模型与策略模板，匹配场景 SLA、链路特征、故障模式设定判定规则，实现场景化精准诊断；

——宜结合链路根因、历史故障经验与运维知识库自动推送处置方案，联动应急平台一键执行对应预案，压缩故障定位至处置的耗时；

——宜分层存储链路冷热温数据，支持跨周期性能趋势分析，识别长期性能退化、周期性瓶颈、架构调用复杂度上涨趋势，为架构优化与容量规划提供长期数据支撑。

7. 2. 4. 故障时段指标回放

故障时序指标回放是银行智能运维故障应急体系实现故障全流程复盘、深度根因分析的关键能力，依托故障前后全维度可观测数据时序回放与交叉分析，完整还原故障发生、扩散、恢复全流程并构建完整证据链。银行业故障常叠加基础设施、应用、数据库、网络、中间件多维度异常，单一快照无法还原真实演变过程。本标准搭建银行故障时序指标回放体系，依靠多源数据时间对齐、时序同步回放、智能异常识别，可视化还原故障全过程并精准取证，支撑根因深挖、责任界定与优化措施制定。

基本要求：

——应自动采集业务、应用、中间件、数据库、基础设施全维度指标，统一毫秒级时间戳对齐多源数据精度，保障同时间轴数据完整准确，夯实时序回放数据底座；

——应围绕故障时间点划定完整回放窗口，统一界面同步展示多层指标趋势，支持调速、拖拽定位、时点标注，直观呈现指标时序因果与异常传导链路；

——应依托突变算法自动识别故障起始、扩散、峰值、处置生效、业务恢复关键节点，时间轴绑定指标快照与告警，生成完整故障时间线；

——应基于基线与统计算法识别突增、突降、趋势漂移、周期紊乱、剧烈波动五类指标异常并高亮，联动同期关联指标，快速锁定异常信号与传导影响；

——应回放指标时同步关联时段日志、变更、伸缩、人工操作事件，统一时间轴串联指标、日志、事件，形成完整交叉印证证据链；

——应支持保存任意时点全维度指标快照，可横向对比正常 / 故障、处置前后、新旧同类故障快照，自动输出差异报告，提供量化比对依据；

——应全程记录回放操作人员、时段、速率、标注、快照、对比等操作，支持导出分享，复盘过程可审计可追溯，符合银行内控与监管合规要求；

——应导出回放窗口全部指标、关键节点、异常分析、日志快照数据，自动生成标准化复盘报告，覆盖时间线、指标趋势、根因、影响、处置及优化建议，满足归档与报送规范。

高级要求：

——宜采用格兰杰检验、贝叶斯网络、传递熵等因果算法分析指标异常因果强弱，自动生成故障传播链路，定位源头指标与根因层级，区分相关性与真实因果；

——宜构建银行故障模式知识库，对历次故障时序特征向量化标注，新故障自动匹配历史相似案例，推送对应根因与处置经验，缩短研判周期；

——宜回放指标时关联时段交易明细，绑定每笔失败交易完整调用链与故障节点，实现宏观指标至微观交易逐层下钻对账，精准统计故障影响、核对客诉；

——宜基于故障关键时间节点自动测算感知、响应、处置、恢复时效指标，量化评估应急全流程，定位处置瓶颈，输出效能报告与预案优化建议，迭代应急能力；

——宜支持专家在复盘时标注指标异常、因果逻辑、处置方案，系统沉淀结构化案例入库，结合后续处置效果持续迭代知识库，实现运维经验沉淀传承。

7.2.5. 网络故障诊断

网络故障诊断是银行智能运维故障应急体系保障交易网络连通与服务质量的核心场景，覆盖多中心互联链路监控与故障定位。银行网络承载渠道接入、服务通信、数据库复制、灾备同步、清算、监管及外联机构交互核心业务，设备故障、链路抖动、配置错误、带宽拥塞易引发大规模交易失败、清算延迟、灾备中断等重大风险。本标准搭建银行网络故障诊断体系，依托标准化网络观测数据采集、端到端路径可视化、智能故障定位与影响评估，实现网络故障快速发现、精准定位、高效恢复，保障业务网络稳定与交易安全。

基本要求：

——应通过多类协议自动发现生成覆盖数据中心多层、广域网、外联区完整网络拓扑，涵盖路由器、交换机、防火墙等设备，展示物理 / 逻辑链路与带宽，实时标注设备运行指标与告警，支持按机房、层级、业务分区筛选拓扑；

——应全域部署探测节点执行多层级端到端探测，实时监测链路连通、延迟、丢包、抖动，链路异常时逐跳定位故障网段与设备，区分内网、跨中心、外联、运营商故障，将故障定界压缩至分钟级；

——应实时感知防火墙全量策略变更，流量异常时关联近期修改记录，对比规则差异并标注流量阻断条目，一键输出回滚建议，缩短策略变更类故障处置时长；

——应采集负载均衡全量运行指标，检测服务池异常、流量分配失衡、会话中断、SSL 握手失败等问题，联动后端应用与服务器状态综合判定故障层级，避免无效排查；

——应通过流协议采集全网流量，建立业务网段正常流量基线，实时识别 DDoS、端口扫描、流量突增突降、非法横向访问等异常，输出完整流量溯源信息，支撑网络与业务故障联合排查；

——应全量留存网络设备配置变更记录，故障发生时检索同期修改项，识别路由、ACL、VLAN、QoS 等风险变更，校验变更流程合规性，兼顾根因定位与内控审计；

——应依托拓扑与 CMDB 业务模型，定位故障设备 / 链路后自动关联受影响网段、应用、数据库、外联通道，映射对应交易、渠道、用户与资金链路，输出业务影响清单与拓扑视图支撑应急分级处置；

——应针对交换机切换、防火墙主备、负载均衡调度、ACL 管控等常见网络故障预设自动化处置脚本，授权后一键执行流量切换、策略调整，操作完成自动校验业务与网络指标恢复状态，保障处置高效可靠。

高级要求：

——宜构建网络设备与链路健康度 AI 评估模型，学习设备资源、光模块、链路质量时序规律，提前识别性能退化、容量瓶颈等潜在风险并分级预警，支撑设备更换、带宽扩容等预防性运维；

——宜针对两地三中心、多活冗余网络做多路径关联分析，整合连通性、延迟、路由、SDN 策略数据，区分链路、协议、控制器、硬件类根因，评估冗余链路容灾承载能力；

——宜联动网络性能指标与安全事件日志联合研判，区分 DDoS、扫描等攻击引发的资源耗尽故障与独立设备网络故障，消除安全、网络问题交叉干扰造成的误处置；

——宜采集历次故障全流程时效与处置效果数据，识别预案冗余步骤、执行瓶颈、次生风险点，输出优化建议并跟踪同类故障处置效能改善，闭环迭代应急处置能力；

——宜搭建融合多中心拓扑、交易链路、实时网络状态的应急态势一张图，全域展示故障机房、层级、业务影响、人员值守、流量切换进度，支持在线协同研判、指令下发与执行跟踪，统一支撑应急指挥决策。

7. 2. 6. 批量故障处置

批量故障处置是金融运维高频高危场景，多由集群、链路、配置共性问题引发，易造成多系统、多交易批量异常，直接影响业务连续性与资金交易安全。通过标准化基础处置能力筑牢风险底线，依托智能化高级能力实现故障预判、自愈与迭代优化，全面提升金融批量故障处置的合规性、高效性与主动性。

基本能力：

——应具备批量故障全域感知能力，依托日志、指标、链路、资源多维度可观测数据，覆盖全栈运维对象，可快速识别批量告警，杜绝单点告警遗漏、批量故障盲区问题；

——应具备批量告警降噪与收敛能力，自动聚合冗余告警，过滤无效抖动告警，精准提炼真实批

量故障事件；

——应具备批量故障分级分类能力，严格贴合金融运维故障定级规范，自动对批量故障划分 P0-P4 故障等级，同步匹配对应处置流程、响应时效与责任人，实现批量故障标准化分级管控；

——应具备批量故障基础定位与关联分析能力，依托系统拓扑、业务调用链路、资源依赖关系，自动关联批量故障关联节点与故障传播路径；

——应具备批量故障处置全程留痕能力，对批量故障的全流程数据进行实时记录留存，满足金融监管合规留存时限要求；

——应具备批量故障应急通知与分级触达能力，根据批量故障等级、影响业务重要度，自动匹配邮件、运维平台、企业微信等多渠道通知方式，精准触达相关人员；

——应具备批量故障基础复盘统计能力，可自动统计批量故障发生次数、影响时长、覆盖设备及业务数量、处置耗时等基础指标，生成简易故障统计报表；

高级能力：

——宜具备批量故障智能根因精准定位能力，自动识别硬件故障、版本迭代、参数异常、网络波动、流量突增等批量故障深层根因；

——宜具备批量故障前置预警与趋势预判能力，提前识别系统资源耗尽、链路拥堵、交易异常攀升等潜在批量故障隐患，在故障大规模爆发、影响金融业务交易前发出预警；

——宜具备低风险批量故障智能自愈能力，针对标准化、低风险批量故障场景预设合规自愈策略；

——宜具备批量故障影响量化评估能力，自动生成故障影响评估报告；

——宜具备批量故障传播阻断与风险隔离能力，针对已发生的批量故障，自动识别故障扩散路径，快速完成故障节点、异常链路的隔离熔断；

——宜具备批量故障策略自适应迭代能力，可基于新增批量故障场景、处置结果、误判漏判案例，自动优化告警收敛规则、根因分析模型、自愈策略参数，持续适配业务迭代、系统升级、架构调整后的运维场景。

7.2.7. 灾备故障应急

灾备故障应急是金融容灾体系核心风险场景，涵盖主备集群同步异常、灾备切换失效、数据一致性异常、灾备资源故障等问题，极易引发业务中断、数据丢失、交易异常等重大风险。本规范依托可观测体系，以基础能力筑牢灾备故障处置底线，以高级智能能力提升灾备自愈与风控水平，保障金融业务灾备切换可靠、风险可控、处置合规。

基本能力：

——应支持灾备全环境运行状态实时监测能力，全覆盖主备机房、异地灾备节点、灾备服务器、等核心资源，实时采集链路时延等关键指标并及时识别基础故障；

——应支持主备业务故障联动感知与告警能力，针对生产系统交易中断等核心故障，可自动联动监测对应灾备系统就绪状态，并实时发出分级告警，支撑应急人员快速研判；

——应支持灾备数据同步异常精准识别能力，实时监测金融核心交易数据、台账数据、配置数据的主备同步一致性，自动识别同步中断、数据滞后、同步失败、数据丢包、增量同步异常等问题；

——应支持灾备故障基础信息自动归集梳理能力，针对各类灾备故障与异常事件，自动汇总故障发生时间、故障节点、同步异常类型等核心信息，生成标准化故障台账；

——应支持手动灾备切换流程观测与记录能力，可全程监测人工发起的主备切换、灾备接管、故障回切等操作流程，完整留存切换全过程数据；

——应支持灾备基础合规校验与状态统计能力，按照金融行业灾备建设规范，定期自动校验灾备节点在线率、数据同步成功率、灾备资源可用性等核心指标，统计各类灾备故障发生频次；

——应支持灾备故障基础隔离与防护能力，针对单节点灾备设备故障、局部链路异常等基础问题，可通过预设规则自动隔离故障节点，阻断异常扩散；

——应具备灾备切换全过程自动化闭环执行能力，在生产系统发生重大故障场景下，可依据预设应急策略自动完成主备切换、业务流量迁移、数据补同步、服务校验、状态确认全流程操作；

——应具备灾备应急场景监管合规自动适配能力，自动汇总灾备故障、切换记录、校验报告、运维台账，生成合规审计报表与专项报送数据。

高级能力：

——宜具备多节点灾备故障关联溯源分析能力，针对异地多活、多备节点的复杂架构，可对跨机房、跨链路、跨集群的联动异常进行关联分析；

——宜具备基于业务优先级的智能灾备切换能力，可根据金融业务重要等级、故障影响范围、数据损失风险，智能判定最优切换策略，支持分级、分业务精准灾备接管；

——宜具备灾备切换效果智能校验与自愈能力，切换完成后自动校验灾备业务交易成功率、数据一致性、服务稳定性、链路通畅性，自动触发自愈操作；

——宜具备灾备故障智能复盘与架构优化能力，针对每一次灾备故障、切换事件、回切操作进行智能复盘，自动输出优化建议，迭代灾备切换预案；

——宜具备灾备应急态势可视化与趋势分析能力，多维展示主备机房运行态势、数据同步质量、故障高发节点、切换成功率等核心数据，动态分析灾备故障时序趋势与风险分布。

7.2.8. 安全应急观测

安全应急观测是金融运维抵御网络攻击、违规访问、数据泄露、病毒入侵等安全风险的核心支撑场景，贯穿安全事件发现、研判、处置、溯源全流程。本规范依托全栈可观测体系，通过标准化基础能力夯实安全应急观测底线，借助智能化高级能力提升风险预判与溯源处置能力，全面保障金融系统安全稳定、合规运行、风险闭环可控。

基本能力：

——应支持金融安全应急全量基础监测数据实时采集能力，全面汇聚各类观测数据，覆盖生产、测试、运维全环境，保障数据实时同步、完整留存；

——应支持常规安全风险与应急异常实时告警能力，针对暴力破解、越权访问、违规操作等金融

常见安全风险，通过固定规则实时识别异常并触发告警，明确告警级别、告警对象；

——应支持安全应急事件基础信息自动梳理能力，针对触发的各类安全应急告警，自动归集事件发生时间、影响范围等基础信息，形成标准化事件台账；

——应支持安全应急观测权限分级管控与数据合规能力，对安全观测日志、风险数据、应急事件记录进行分级权限管理，区分运维、安全、审计、管理人员访问权限；

——应支持安全应急处置过程全程记录留存能力，自动采集安全应急事件触发后的全流程操作数据，完整记录处置步骤、操作人、处置时长、执行结果；

——应支持常规安全应急事件分类统计与基础复盘能力，自动对各类安全应急事件进行分类打标、频次统计，定期汇总基础风险态势，输出简易观测分析结果；

——应支持安全应急观测基础联动响应能力，针对低危、常规安全应急事件，可联动基础安全防护策略，自动完成基础防护动作，缩短基础安全事件处置时长。

高级能力：

——宜具备安全应急事件智能定级与分级处置能力，结合金融业务重要等级、事件危害程度等多维度因子，通过智能算法自动划分安全应急事件等级，匹配差异化应急处置流程与处置标准；

——宜具备重大安全应急场景全自动协同响应能力，针对高危入侵、数据泄露、批量异常交易等重大安全事件，可联动安全设备自动执行隔离、阻断等协同操作，实现秒级应急止损；

——宜具备安全应急态势可视化与趋势预判能力，支持全量安全观测数据的多维可视化展示，同时基于历史数据模型预判高发安全风险时段与薄弱环节；

——宜具备安全应急观测监管适配与专项报送能力，自动萃取合规观测数据，生成安全应急专项审计报表、监管报送材料。

7.2.9. 故障自动复盘

故障自动复盘是金融可观测运维体系故障闭环治理核心环节，依托全量观测数据自动完成故障还原、问题汇总、根因梳理与整改沉淀。标准化基础能力保障复盘完整合规，智能化高级能力深挖运维短板，持续优化金融运维架构与应急处置体系。

基本能力：

——应自动归集交易、应用、服务器、网络、数据库、中间件全栈故障数据，涵盖时序指标、日志、交易报文、调用记录，保障数据完整、未篡改、时序对齐，满足故障溯源基础要求；

——应依托归集数据自动梳理故障完整时间轴，识别异常萌芽、故障触发、扩散、恢复关键节点并标注事件，生成标准化时序链路，消除人工梳理时序偏差，适配金融时效追溯要求；

——应基于规则引擎识别资源过载、接口超时、数据库异常、配置错误、网络波动等常见故障，自动判定故障层级、所属模块与初步根因，为运维研判提供基础支撑；

——应自动识别故障覆盖业务、渠道、用户与服务节点，量化失败交易笔数、异常金额、服务中断时长、受影响终端用户，客观统计业务损失，保证复盘数据真实可控；

——应整合数据归集、时序、根因、影响分析结果，自动生成标准化复盘报告，包含故障概况、

时间线、异常清单、影响范围、初步根因、处置记录，符合金融归档规范，支持一键导出；

——应按金融数据合规要求归档复盘原始、分析数据与报告，设置分级访问权限，仅授权人员可查阅，防范数据泄露、篡改、丢失，满足监管审计追溯要求；

——应自动对历史故障分类打标，区分交易、资源、网络、程序故障，归集同类重复故障并统计复发频次，快速识别常态化隐患，支撑运维整改优化；

——应完整记录故障处置人工、自愈、变更操作，留存操作时间、执行人、操作内容与执行结果，核验处置动作匹配度，排查无效、违规操作，规范故障处置流程；

——应按日/周/月/季度汇总复盘数据，输出故障类型趋势、高频故障排行、系统薄弱点、运维风险可视化报表，直观展示运维故障全貌，支撑体系迭代与管理决策。

高级能力：

——宜依托机器学习与故障知识库深度溯源复杂、隐性、连锁故障，分层区分表层异常、中层诱因、底层根源，划分偶发故障、架构缺陷、运维漏洞、版本问题，实现精准深层定位；

——宜结合业务、调用、资源依赖拓扑自动分析故障传播链路，区分源头节点与被动异常节点，还原跨模块、跨系统、跨机房连锁故障传导逻辑；

——宜智能聚类全量历史故障复盘数据，提炼同类故障共性特征、高发时段、薄弱模块与触发条件，主动挖掘隐性隐患并输出分析结论，支撑架构与运维策略优化；

——宜结合故障根因、风险等级、历史处置经验联动故障、预案知识库，自动匹配整改方案、防控策略，明确整改责任人、时限与核验标准，形成复盘整改优化闭环；

——宜自动跟踪故障整改落地成效，对比整改前后异常率、交易成功率、故障复发率，智能评估整改有效性，定位整改不彻底问题，搭建复盘闭环校验机制；

——宜适配金融监管、内部审计核查标准，自动提取合规数据生成专项审计报表，匹配监管报送要求，同步将复盘风险录入运维台账，打通复盘与合规风控流程；

——宜基于历次复盘根因、处置短板、整改经验，识别应急预案、运维规范缺陷，推送预案、流程、策略优化建议，持续迭代故障应急处置与风险防控体系。

7.3. 变更管控可观测场景

7.3.1. 变更前可观测

为规范信息系统变更实施流程，识别变更实施后非预期改动，保障生产环境稳定性，实现变更前后环境可比对、可核验、可回滚，所有生产环境变更实施前须完成当前运行基线快照采集、归档，变更完成后以基线为基准完成一致性比对校验，基线内容的设定，应匹配系统类别和业务连续性等级，保证基线内容的完整性和准确性。变更前基线是指变更实施前，目标系统/设备当前真实运行状态的完整快照信息，作为变更完成后环境比对、差异核查、异常判定、回滚校验的唯一基准依据，基线信息须同步归档至 CMDB 配置管理平台及 ITSM 变更工单附件。

基本能力：

——应具备变更前基础设施和系统层基线，包括物理/虚拟服务器基础信息、硬件及虚拟化配置

信息、网络和存储设备信息，系统用户权限、环境变量、应用部署信息、应用配置信息、代码版本信息、接口信息和日志信息；
——应具备变更前中间件和数据库层基线，包括容器、应用、中间件和缓存中间件配置信息，对象结构信息、权限信息、核心配置表参数类数据信息和集群信息；
——应具备变更前备份灾备基线，包括数据库备份集、应用配置备份、系统快照编号、备份存放位置等变更前全量备份记录，主备节点同步状态、灾备切换参数等灾备集群信息；
——应具备变更前准入风险自动识别能力，变更前增加自动化准入校验，校验变更审批流程进度状态，变更实施人的角色权限风险，变更时间是否符合变更要求，变更内容测试缺陷情况，变更版本和测试版本的一致性，制品来源等内容。

高级能力：
——宜具备变更前安全基线，包括网络信息、镜像和容器安全信息、源代码漏洞扫描信息、和密钥证书信息；
——宜具备变更前身份权限基线，包括运维账号、超级管理员账号等应用/系统账号信息，登录白名单、操作权限、高危命令黑名单等堡垒机/访问策略信息；
——宜具备变更前业务交易基线，包括产品参数信息、机构渠道配置信息和调度任务信息；
——重大变更宜具备变更前风险评估，对变更可能带来的风险进行全面评估，包括变更方案、业务影响等，并制定相应的风险应对措施，所有变更必须经过严格的审批流程，确保变更必要性和合理性。

7.3.2. 变更中可观测

变更中实时可观测，用于在变更过程中，实时感知异常，保障变更按计划进行，应具备基础设施、操作系统和数据库运行状态可观测，变更操作和变更行为可观测，变更过程风险识别以及变更前后一致性比对等基本能力，除此之外，宜具备变更中应用全链路追踪、业务交易和安全可观测，以及业务告警触发变更回退能力等高级能力。

基本能力：
——应具备基础设施、操作系统和数据库运行状态可观测，包括计算资源瞬时指标、负载均衡、消息中间件和缓存可观测，DDL 执行过程观测、事务与锁动态观测和性能动态异常可观测；
——应具备变更操作和变更行为可观测，包括堡垒机变更操作录屏、命令实时回显、高危命令实时拦截和即时告警等远程操作行为信息，程序/配置下发行为、启停重载和脚本执行可观测，变更方式、变更开始和结束时间、变更结果状态、变更执行人、变更复核人、变更耗时等内容；
——应具备变更过程风险识别能力可观测，包括变更容量预估、变更过程状态监控、变更异常风险监控告警、变更超时告警和变更验证超时告警等内容；
——应具备变更前后一致性比对能力可观测，包括变更前基线信息、变更后比对的指标信息和一致性比对结论，以及一致性比对结果的处理情况。

高级能力：
——宜具备变更中应用全链路追踪可观测，包括服务拓扑观测、调用指标实时观测、异常堆栈可观测和内部 RPC 调用观测；
——宜具备业务交易可观测，包括渠道交易指标可观测、核心账务类交易可观测、外联通道可观测，以及定时批处理任务可观测；

——宜具备安全可观测，包括证书加密组件观测、敏感操作审计可观测和入侵异常可观测；
——宜具备业务告警触发变更回退能力，针对影响业务正常运行的情况，包括平台级性能问题、基本功能使用异常、大范围交易失败、整体性响应率低等，设置不同级别业务告警指标，配置告警自动回退策略，由高级别告警自动触发变更版本回退。

7.3.3. 变更后可观测

变更后指标校验，作为投产验证的一部分，是防控变更风险的最后一道防线。根据业务系统类型以及业务连续性级别，设置相匹配的变更后校验指标，通过与变更前基线数据比对，获取变更后异常信息，及时发现系统组件类、数据类以及业务类运行风险，通过比对变更前后版本差异，确认变更是否符合预期，通过分析变更操作指标，提高变更效率，降低操作风险，保障安全运营。

基本能力：
——应具备变更后系统组件类指标校验能力，包括基础设施容量指标，应用服务指标，数据库指标，中间件指标，以及批量任务运行成功率指标等；
——应具备变更后数据类指标校验能力，校验数据完整性和数据准确性，包括但不限于数据库表结构、数据库表容量、数据库对象个数等，防范变更后数据异常风险；
——应具备变更后业务指标校验能力，重点校验新增业务和核心业务，包括但不限于交易响应率、交易成功率、交易响应时间、交易量、交易金额、业务成功率、首比交易成功率、新增交易响应率、差错账、交易性能等指标，防苑整体业务风险；
——应具备变更后版本指标校验能力，包括但不限于投产包版本、镜像版本、操作系统中间件版本等指标，主备一致性校验等。

高级能力：
——宜具备变更操作及日志指标校验能力，包括但不限于变更失败率、变更回退率、变更异常率、变更自动化率、变更超时、验证超时、任务运行成功率指标，系统、中间件、数据库及变更模块、参数配置等应用日志；
——宜具各变更后技术指标自动化校验能力，覆盖系统组件类、数据类和版本类指标，自动获取并自动比对基线数据，提高变更后技术类指标校验效率；
——宜具备变更后业务指标自动化校验能力，覆盖新增业务和核心业务，提高业务验证效率；
——宜具备变更后指标校验闭环能力，校验结果存档分析，横向对比同类系统变更后运行指标，纵向对比同一系统多次变更后的运行指标，总结经验教训，提高变更后指标校验能力。

7.4. 性能容量可观测场景

7.4.1. 实时性能瓶颈分析

实时性能瓶颈分析是银行业智能运维故障应急体系保障高并发交易低延迟稳定运行的核心支撑场景，覆盖数据库、应用 JVM、磁盘 IO、网络链路、分布式缓存全技术栈资源性能指标实时监控、异常识别与瓶颈定位全流程。

基本能力：

——应实时采集数据库 SQL 执行耗时、扫描行数、返回行数等核心指标，精准识别超阈值慢 SQL，记录 SQL 原文、执行时间、访问节点等基础信息，实现异常实时告警；

——应实时监控 JVM 堆内存、元空间使用量及 FullGC 次数、耗时指标，触发阈值时及时告警，记录 GC 发生时间、进程信息、内存占用快照基础数据；

——应实时采集磁盘读写速率、IO 使用率、等待耗时、磁盘繁忙度指标，识别 IO 打满异常状态，记录异常时段、服务节点、IO 负载基础信息并告警；

——应实时监测网络带宽使用率、丢包率、延迟、重传率核心指标，及时发现网络拥堵、链路波动问题，记录网络节点、异常时段基础数据；

——应实时监控缓存命中率、过期量、淘汰量、连接数指标，识别缓存大面积失效、击穿、穿透异常，触发阈值及时推送告警信息。

高级能力：

——宜关联业务链路、交易场景分析慢 SQL 根因，定位索引失效、锁等待等问题，依托智能体自动解析 SQL 语句、识别劣化特征，批量输出标准化优化方案与风险预判；

——宜联动线程状态、内存泄漏特征分析 GC 根源，区分 GC 触发类型，通过智能体自动分析内存快照、线程堆栈，精准定位泄漏对象，预判集群 GC 拥堵故障趋势；

——宜关联进程、日志、数据库场景定位 IO 过载源头，分析业务影响范围，依托智能体复盘 IO 异常时序数据，识别高频无效读写，智能输出资源调度与配置优化策略；

——宜溯源拥堵链路、异常访问 IP、高频传输服务，分析网络波动对金融交易链路的影响，预判链路瓶颈，支持流量调度优化分析；

——宜分析缓存失效诱因，区分过期失效、主动清空、集群故障等场景，关联业务交易卡顿情况，智能给出缓存参数调优及架构优化建议。

7.4.2. 业务峰值观测

业务峰值观测是银行业智能运维故障应急体系应对大促、节假日、清算窗口等高负载场景的核心观测场景，聚焦业务交易并发规模、全链路交易时延两大核心维度，覆盖渠道交易、应用服务、中间件、数据库、基础设施全栈负载监控与异常处置全流程。应构建面向银行业的业务峰值观测体系，实现峰值风险事前预警、事中快速处置、事后容量复盘，保障高并发时段金融交易稳定可控、观测数据完整合规。

基本能力：

——应覆盖峰值时段核心交易业务、中间件、数据库等全维度指标采集，保障高流量场景数据不丢失、不中断；

——应支持业务峰值 TPS、并发量、交易成功率等核心业务指标实时监控，精准捕捉流量突增、业务波动情况；

——应配置峰值场景专属告警阈值，规避流量激增引发的告警风暴，实现异常交易、系统卡顿及

时告警通知；

——应留存业务峰值时段全量日志、指标数据，满足金融合规溯源、峰值故障事后核查复盘需求；

——应支持峰值场景指标分级采集，对核心交易链路高频采集、非核心资源合理降频，平衡观测精度与系统负载；

——应具备峰值数据校验能力，自动识别高并发下数据缺失、重复、异常值，保障观测数据真实有效；

——应实现峰值异常事件秒级感知，缩短高并发故障发现时延，为快速应急处置争取时间窗口；

——应支持多节点峰值数据汇聚汇总，统一展示全平台业务流量、资源负载整体运行态势；

——应适配金融节假日、大促等超大峰值场景，观测规则可快速复用、一键切换部署。

高级能力：

——宜支持多维度峰值数据联动钻取，可从业务指标下钻至链路、主机、日志等底层细节数据；

——宜基于历史峰值数据构建智能预测模型，提前预判流量峰值拐点、资源瓶颈，实现峰值风险事前预警；

——宜支持峰值场景全链路追踪，精准定位高并发下交易超时、链路阻塞、接口异常等问题根因；

——宜具备峰值告警智能降噪、聚合能力，自动合并同源告警，过滤无效告警，提升峰值排障效率；

——宜联动运维管控体系，根据峰值观测数据自动触发限流、扩容、流量调度等自适应运维动作；

——宜支持峰值场景压测数据与生产观测数据联动分析，精准评估系统极限承载阈值与容错能力；

——宜构建峰值容量基线体系，持续迭代优化，精准预判未来业务峰值扩容、资源调配需求。

7.4.3. 容量趋势预测

容量趋势预测是银行业智能运维体系实现资源前置规划、规避容量耗尽故障的核心管控场景，聚焦磁盘存储占用、数据库表空间扩容、服务连接池上限、跨机构专线带宽四类资源中长期增长趋势监测与推演分析，覆盖服务器存储、数据库、中间件、广域网专线全层级资源容量全生命周期管理。

基本能力：

——应持续采集服务器、存储、网络等基础设施容量资源数据，稳定留存时序数据，支撑长期容量趋势统计分析；

——应监控数据库、中间件等业务组件容量使用率、剩余容量，实时掌握各类资源占用变化趋势；

——应基于日、周、月周期统计资源容量消耗规律，输出基础趋势数据，支撑人工初步容量评估；

——应设置容量使用率阈值告警，资源临近饱和时及时触发通知，规避容量不足引发的业务故障；

——应区分日常、业务促销、节假日等不同场景，分类统计容量消耗数据，保障趋势分析贴合业务场景；

——应支持容量数据精准溯源，可查询任意时段资源占用明细，排查容量突增、异常消耗问题；

——应保障容量观测数据完整可靠，杜绝数据断点、缺失问题，为趋势预测提供坚实数据基础；

——应输出基础容量统计报表，直观展示资源消耗增速、剩余可用周期，满足日常运维核查需求。

高级能力：

——宜基于时序算法构建容量预测模型，依托历史数据预判未来资源消耗趋势，提前识别容量瓶颈；

——宜结合业务增量、新系统上线等因素，智能修正容量预测结果，提升中长期容量评估精准度；

——宜支持多维度容量关联分析，联动业务交易量、用户量数据，拆解容量增长核心驱动因素；

——宜具备容量风险预判能力，提前预判资源耗尽时间节点，输出分级容量扩容风险提示；

——宜联动运维资源调度体系，依据容量预测结果，智能推荐扩容、缩容及资源优化方案；

——宜自动生成容量趋势专项分析报告，量化资源利用率及冗余情况，支撑架构和资源规划决策；

——宜持续迭代预测模型，通过实际容量数据反向校验，不断优化预测精度，适配业务迭代变化。

7.4.4. 多中心资源均衡观测

多中心资源均衡观测是银行业两地三中心、双活/多活架构运维体系实现全域资源合理调配、规避单中心过载风险的核心观测场景，核心聚焦多站点算力、存储、网络、数据库、中间件负载差异识别与均衡管控，覆盖多数据中心、多可用区、业务集群全层级资源实时监控、失衡识别、调度管控与事后复盘全流程。

基本能力：

——应全面采集多数据中心、中间件、数据库等全量资源运行指标，实时同步各中心资源负载、使用率、在线状态数据，保障多中心资源观测数据全域覆盖、实时同步；

——应建立多中心资源统一观测口径，统一各站点资源指标采集频率、统计规则、数据维度，实

现全域资源数据标准化、可对比、可统计；

——应实时监测多中心资源负载差异情况，精准识别单中心资源过载、局部资源闲置、跨区域负载失衡等异常状态，持续跟踪各中心资源配比变化，及时发现多中心资源分配不均的基础运维问题；

——应针对多中心资源调度、流量切换、资源迁移、负载分流等操作实现全流程观测记录，完整留存跨中心调度事件、执行状态、操作耗时与结果数据，满足金融运维溯源核查与故障复盘合规要求；

——应联动多中心自动化调度平台，依托实时均衡观测数据，智能触发跨中心流量分流、资源迁移、负载调剂等自适应操作，实现全域资源动态均衡，提升整体资源利用效率；

——应配置多中心资源均衡专属告警规则，针对资源负载差值超标、单中心资源瓶颈、跨中心同步异常、资源调度失效等风险场景及时触发告警，助力运维人员快速处置多中心资源失衡隐患；

——应实现多中心资源态势可视化汇总展示，集中呈现各数据中心资源利用率、负载分布、业务承载量、资源冗余情况，直观展示全域资源均衡状态，支撑运维人员直观把控整体资源运行态势；

——应按日、周、月维度统计多中心资源均衡度、负载偏差率、资源闲置率等核心数据，形成基础统计台账，持续记录各中心资源运行变化规律，为常态化资源均衡运维与基线优化提供数据支撑；

——应联动业务交易指标校验多中心资源均衡效果，结合各中心交易承载量、响应时延、交易成功率等业务数据，验证资源均衡分配后的业务运行稳定性，规避资源失衡引发的业务波动。

高级能力：

——宜基于多中心历史资源数据、业务流量波动规律、节假日峰值特征构建智能分析模型，深度分析跨中心资源负载失衡诱因，辅助优化资源均衡策略；

——宜具备多中心资源均衡动态研判能力，可根据实时业务流量、资源负载、网络时延变化，动态计算各中心最优资源承载配比，精准预判资源失衡趋势，提前给出跨中心资源调优建议；

——宜支持多中心资源均衡仿真推演观测，可模拟突发流量、单中心故障、区域网络波动等极端场景，推演不同资源分流、调度策略下的全域负载均衡效果，为应急预案优化提供支撑；

——宜具备跨中心资源异常根因智能分析能力，针对多中心负载骤变、资源均衡失效、跨区域调度卡顿等异常，自动关联网络、算力、业务流量多维度数据，快速定位故障根源；

——宜构建多中心资源均衡基线体系，结合长期观测数据迭代优化负载均衡阈值、资源配比标准、调度触发条件，适配业务迭代扩容、架构升级等场景，持续优化多中心资源均衡能力；

——宜具备多中心容灾场景均衡观测能力，针对单中心降级、故障隔离、容灾切换场景，实时观测备用中心资源承载压力与负载均衡状态，保障容灾场景下资源合理分配、业务平稳运行。

7.4.5. 闲置资源识别

闲置资源识别是银行业智能运维体系实现算力存储网络资产精细化管控、降本增效的核心观测场景，重点针对长期低负载虚拟机、空闲存储卷、未充分利用专线开展自动识别与全生命周期管控，覆盖虚机、容器、存储、专线、中间件、数据库全品类基础设施负载监测、闲置判定、

台账管理、处置优化全流程。

基本能力：

——应建立金融场景专属闲置资源判定标准，结合行业运维基线定义资源低负载、零访问、长期待机等闲置判定规则，统一闲置资源识别口径；

——应对计算、存储、网络、容器、中间件、数据库等各类基础设施资源的运行指标常态化采集，完整留存资源使用率、活跃度、负载耗时等时序数据；

——应持续监测各类资源的实时负载与历史运行状态，精准甄别长期低负载、业务下线后未回收、测试临时遗留等各类闲置资源，同时区分正常备用、容灾资源与无效闲置资源；

——应针对识别出的闲置资源进行台账化管理，完整记录资源归属机房、业务系统、资源规格、闲置时长、闲置率等关键信息，形成可追溯、可统计的闲置资源明细台账；

——应支持闲置资源生命周期全流程观测，动态跟踪闲置资源从识别、登记、评估、处置到复用下线的完整流程，实时监控处置进度；

——应配置闲置资源超标告警能力，针对资源长期闲置、冗余资源堆积、下线资源未释放等异常场景设置分级告警；

——应支持按业务线、机房集群、资源类型、使用部门多维度筛选统计闲置资源，清晰梳理各维度闲置资源占比与分布情况，精准定位资源冗余集中区域；

——应保障闲置资源观测数据的完整性与准确性，规避采集中断、数据缺失、指标失真等问题，确保闲置资源的判定结果有据可依，支持历史闲置数据溯源查询；

——应联动业务运行数据校验资源闲置状态，结合业务交易量、接口调用频次、服务在线状态等数据，核验资源闲置的真实性，排除业务低峰期正常低负载场景；

——应支持自动生成闲置资源专项分析报告，量化全域闲置资源占比、闲置趋势、成本损耗、复用潜力等核心指标，输出资源清理、规整、复用的优化建议。

高级能力：

——宜构建闲置资源观测基线体系，持续迭代优化闲置判定阈值与识别规则，适配金融业务迭代、系统升级、架构改造等场景变化，动态优化识别模型；

——宜具备闲置资源成因智能分析能力，自动结合业务下线、架构迭代、资源超配、规划冗余等多维度因素，溯源资源闲置核心原因，分类标记闲置资源类型；

——宜基于长期资源运行时序数据与业务运行规律，构建闲置资源智能识别模型，精准区分业务周期性低负载、临时性闲置、长期闲置资源；

——宜具备闲置资源成本精细化分析能力，结合金融资源计费规则、资源规格与闲置时长，精准核算闲置资源产生的资源空置成本、运维成本，量化资源浪费损失；

——宜支持闲置资源复用可行性智能研判，结合剩余资源性能、适配业务场景、安全合规要求，自动评估闲置资源的复用价值，精准筛选可复用、可扩容、可迁移的闲置资源；

——宜联动自动化运维平台实现闲置资源智能处置，对无复用价值的闲置资源自动触发缩容、回收、下线操作，对可复用资源智能推荐调度方案，实现闲置资源闭环智能化管控。

7.4.6. SLA 持续统计

SLA 持续统计是银行业智能运维体系保障业务服务承诺落地、量化服务质量、支撑考核与监管报送的核心观测场景，核心围绕全渠道交易时延、系统月度可用率两大核心指标开展长期采集、持续统计与质量评估，覆盖线上交易系统、中间件、数据库、多活集群全业务域服务指标全周期管控。

基本能力：

——应支持自动收集、统计 IT 基础设施的运行状态数据，包括性能、容量、可用性等指标对业务的满足状态，平均故障恢复时间(MTTR)等信息，并可以显示指定时间段内的指标变化情况；

——应支持自动收集、统计业务系统的运行状态数据，包括交易时延、成功率等指标，并可以显示指定时间段内的指标变化情况；

——应支持性能、容量、可用性等指标超出阈值的频率和时长统计；

——应支持按日/周/月/季度/年度统计和生成 SLA 数据的能力。

高级能力：

——宜具备智能化、自动化生成 SLA 服务报告的能力，对运行状态进行自动分析，并给出服务总结和改进建议；

——宜具备智能化进行 IT 基础设施运行指标与业务 SLA 承诺的关联度分析，并具备针对业务高峰期、业务促销等场景进行特定分析的能力。

7.4.7. 弹性调度观测

弹性调度观测是银行业云原生智能运维体系校验自动化扩缩容执行成效、核查扩容时延是否匹配业务 SLA 的专项观测场景。覆盖云主机、容器、算力、带宽等弹性资源全生命周期调度监控、执行时效校验、负载效果评估，兼顾业务稳定与资源成本管控。

基本能力：

——应全面采集云主机、容器、算力、带宽等可弹性调度资源的运行指标，实时监控资源负载、空闲率及调度状态，精准掌握各类弹性资源的实时运行情况，为基础调度决策提供有效数据支撑；

——应针对扩容、缩容、资源迁移、负载切换等各类弹性调度动作，实现全流程事件记录与状态监控，完整留存调度执行日志，便于后续运维核查、问题追溯与流程复盘；

——应设置弹性调度场景专属资源阈值告警，针对资源过载、调度失败、资源抢占、扩容超时等异常场景及时触发告警，快速发现弹性调度过程中的各类运行故障；

——应区分日常平稳、业务峰值、突发流量、节假日大促等不同业务场景，分类统计弹性资源调度频次、资源使用情况，保障调度观测数据贴合金融业务运行特征；

——应实现弹性资源调度结果可视化展示，直观呈现资源分布、调度执行进度、资源利用率等核心信息，帮助运维人员实时掌控全域弹性资源调度运行态势；

——应保障弹性调度观测数据的完整性与连续性，杜绝调度过程中数据断点、采集缺失、数据错乱等问题，确保每一次弹性调度行为均可精准观测、有效溯源；

——应支持弹性调度基础数据统计分析，可按日、周、月统计资源调度次数、成功率、资源闲置时长等数据，满足金融日常运维统计与合规核查需求；

——应监控弹性调度后的业务运行状态，联动交易成功率、接口响应时延等业务指标，校验资源调度完成后业务运行的稳定性与可用性。

高级能力：

——宜基于历史调度数据与业务流量趋势，构建弹性调度智能预测模型，提前预判未来资源负载变化，预先评估资源调度需求，实现弹性资源调度的事前预判与主动规划；

——宜具备弹性调度异常智能分析能力，针对调度失败、调度滞后、资源浪费、调度冲突等问题，自动关联系统、业务、资源多维度数据，精准定位问题根本原因；

——宜支持多集群、多节点、多区域弹性资源联动观测，统筹分析全域资源调度配比、负载均衡状态，精准识别资源分配不均、局部负载过高的调度短板问题；

——宜实现弹性调度规则自适应优化，依托长期观测数据迭代调整调度触发阈值、扩容缩容梯度、调度时效参数，提升弹性资源调度的精准性与合理性；

——宜联动自动化运维平台，基于实时观测的资源负载与业务态势，支撑无人值守智能弹性调度，实现资源按需自动扩缩容、动态负载均衡调度，并能实现弹性扩缩容后监控、日志、NAS 存储、备份等策略的自动调整；

——宜自动生成弹性调度专项分析报告，量化调度效率、资源利用率、调度故障率、资源冗余率等核心指标，为金融资源架构优化、调度策略迭代提供决策依据；

——宜具备调度成本精细化观测能力，结合资源调度量、使用时长、区域资源单价等维度，统计弹性调度资源消耗成本，助力金融运维降本增效管控。

8. 可观测性核心能力

8.1. 指标管理

指标管理是全链路可观测体系的核心数据治理能力，面向基础设施、中间件、业务应用、微服务、网络链路等全场景数据源，实现观测指标的统一定义、采集接入、存储治理、聚合计算、生命周期管控与合规管理。

基本能力：

——应建立指标全生命周期管理机制，包含指标定义、指标评估、指标上线、指标运营；

——应建立指标设计原则，指标设计要遵循可度量、可采集、可理解、可消费的原则，有明确监控目标和消费场景，支持有关运算；

——应优先定义代表服务可用性的关键指标，明确指标指标适用范围；

——应按照指标的重要程度区分定义指标分级规范，如分为：核心指标（生死指标）、关键指标（告警指标）和常规指标（分析指标、参考）等；

——应建立指标的命名规范，核心是可视可读，定义统一的指标命名规则，至少包含编号的长度限制、编码的构成、各组成部分的具体含义等。例如命名示例：组件名_指标获取方式_指标分类_指标描述；

——应对指标进行分层，以全面覆盖并优化 IT 架构，覆盖基础设施层、硬件设备层、操作系统层、组件服务层、应用性能层、业务运营层等层级。

高级能力：

——宜支持同比、环比、波动率、百分位、速率计算、分桶聚合等高阶统计分析能力，支持自定义聚合规则与计算脚本，满足复杂性能分析、业务趋势研判需求；

——宜支持指标与拓扑节点、告警规则、日志、链路追踪数据的关联绑定，实现单一指标联动多维度观测数据，支撑故障根因快速定位；

——宜提供标准化指标模板库，支持按业务场景、系统类型批量导入、导出、复用指标模板，实现规模化、标准化指标快速部署，提升运维效率。

8.2. 日志管理

日志管理是银行业智能运维体系实现故障追溯、行为审计、问题定位、合规留存的核心基础能力，覆盖系统日志、应用日志、中间件日志、数据库日志、网络设备日志、安全操作日志等全维度运维日志的统一采集、规整、存储、检索与闭环管理，是故障根因分析、运维审计核查、监管合规报送的重要数据支撑。

基本能力：

——应支持机房基础设施、网络设备、应用服务、中间件、数据库、安全操作全场景日志统一采集，覆盖运行日志、异常日志、访问日志、操作日志、审计日志等全量日志类型；

——应具备日志标准化清洗、格式归一、字段解析能力，统一各类异构日志输出口径，完成日志去重、过滤、富化处理，保障日志数据规范可信；

——应支持全域日志实时集中存储与时序归档，按照金融合规要求设定日志留存周期，保障日志数据不丢失、不篡改、可追溯；

——应具备日志多条件精准检索能力，支持按时间、节点、服务、关键字、异常类型、交易流水号多维度快速查询，支撑故障快速定位；

——应支持日志实时监控与异常日志告警，对报错日志、服务异常日志、非法操作日志实时识别并触发通知，提前预警运维风险；

——应实现日志访问、检索、导出、操作全程权限管控与操作留痕，满足金融运维审计、安全管控、监管合规要求；

——应支持日志数据基础统计展示，可按时段、节点、服务、异常类型统计日志分布规律，直观呈现系统运行异常态势。

高级能力：

——宜具备日志智能聚类与降噪能力，自动聚合同源、同类、重复日志，过滤无效冗余日志，精准提炼核心异常信息，提升故障分析效率；

——宜具备日志与指标、链路、告警数据自动关联能力，实现指标异常、链路报错、日志报错多维联动，辅助深度根因溯源；

——宜具备日志异常智能识别与趋势研判能力，依托历史日志基线自动识别新增异常日志、日志报错量突增等隐性风险；

——宜支持日志场景化智能分析，针对交易失败、服务卡顿、数据库异常、网络抖动等场景自动提取关键日志并生成分析结论；

——宜具备日志数据脱敏、安全分级管控能力，自动屏蔽日志中的敏感交易信息、用户隐私数据，保障日志安全合规使用；

——宜支持日志分析报告自动生成，汇总周期内异常日志、高频报错、问题节点，输出运维优化建议，支撑运维持续迭代优化。

8.3. 链路管理

链路管理指对银行 IT 系统全链路的调用关系、交易路径、性能指标、异常事件进行统一采集、建模、存储、分析与可视化的能力，覆盖前端渠道、接入网关、应用服务、中间件、数据库、外联系统等全链路节点，用于支撑交易全流程可观测、故障快速定位、性能瓶颈分析，保障银行业务交易的稳定运行。

基本能力：

——应支持分布式链路追踪能力，可实现跨服务、跨节点的交易全链路追踪，记录每笔交易经过的所有节点的调用信息、耗时与状态；

——应支持链路数据标准化采集，兼容主流的链路追踪协议与探针，可覆盖 HTTP、RPC、消息队列、数据库调用等多种调用类型；

——应支持链路拓扑自动发现与构建，可基于链路调用数据自动生成服务间、系统间的调用关系拓扑，支持拓扑动态更新；

——应支持链路性能指标统计分析，可按服务、接口、链路维度统计调用量、平均响应时延、错误率、吞吐量等核心指标；

——应支持链路异常标记与查询，可识别调用失败、超时、报错等异常链路，支持按交易 ID、时间范围、服务名称等维度检索异常链路详情；

——应支持链路数据与指标、日志数据的关联查询，可通过链路 ID 关联对应节点的指标数据与日志信息，支撑故障深度排查；

——应支持链路数据的分级存储与生命周期管理，可按链路重要程度、时间维度设置不同的存储策略与保留周期；

——应支持银行核心交易链路专项管理，可针对账务类、支付类等核心交易配置专属链路观测策略，保障核心交易可观测性。

高级能力：

——宜支持链路异常智能诊断能力，可基于 AI 算法自动识别链路性能劣化、调用异常等问题，输出异常根因与影响范围分析；

——宜支持自定义业务链路追踪能力，可针对特定业务场景配置专属追踪规则，实现重点业务链路的精细化观测；

——宜支持链路容量评估与压力预测能力，基于历史链路调用数据评估服务容量水位，预测业务峰值下的链路性能表现；

——宜支持全链路压测联动能力，可在压测场景下实时观测全链路性能变化，定位压测过程中的性能瓶颈与异常节点。

8.4. 模型管理

模型管理（拓扑管理）是全链路可观测体系的场景化建模核心能力，基于全域 IT 资源与业务架构，构建物理资源、逻辑服务、业务链路的层级拓扑模型与关联关系模型。通过标准化建模、自动发现、关系梳理、动态更新，直观呈现基础设施、中间件、应用服务、业务接口、网络链路的层级架构与调用关联，实现“资源-服务-业务”的全景可视化。该能力是故障全域定位、链路溯源、架构观测、资源管控的核心载体，为全链路可观测提供场景化、结构化的架构支撑。

基本能力：

——应支持物理资源（服务器、交换机、存储设备）、虚拟资源（虚拟机、容器、集群）、软件资源（中间件、数据库、应用服务）、业务资源（接口、交易链路、业务模块）的标准化建模，定义各类资源的基础属性与建模规范；

——应支持梳理并存储节点间的依赖关系、调用关系、挂载关系，包含上下游调用、主备关联、集群关联、网络挂载等核心关联逻辑，构建完整的业务与资源链路图谱；

——应支持人工辅助编辑模型视图，可手动新增、删除、移动节点，修正自动发现的错误关联关系，支持节点名称、属性、标签的手动维护；

——应支持拓扑节点运行状态实时展示，通过颜色、图标区分正常、异常、离线、维护中节点，直观呈现全域资源运行态势；

——应基于 CMDB 和应用调用关系数据构建面向应用的模型数据；

——应面向应用系统部署情况构建从上到下（应用、微服务、实例、系统与虚拟化、硬件）的纵向的分层对象模型关系；

——基于 APM 或相关工具提供的调用关系构建横向的服务间调用和实例调用关系。

高级能力：

——宜使用使用企业统一的 CMDB 进行存储模型数据；

——宜支持架构变更实时感知，针对服务扩容缩容、节点上下线、链路变更、集群重组等场景，自动更新拓扑模型与关联关系，实现拓扑视图无感知动态迭代；

——宜支持基于业务场景自定义核心交易链路、关键服务链路模型，可人工编排跨系统、跨模块的复杂业务拓扑，适配个性化业务观测需求；

——宜支持按业务维度、运维维度、资源维度、故障维度切换拓扑视图，支持聚焦单业务、单集群、单故障域的精细化拓扑展示，实现全景与局部观测结合；

——宜支持拓扑节点联动指标、告警、日志、链路追踪数据，点击拓扑节点可一键查看对应资源的运行指标、历史告警、异常日志、调用链路，实现架构与数据深度融合；

——宜支持拓扑模型变更全流程记录，自动存储节点新增、删除、关系变更、属性修改的历史记录，支持变更溯源、版本回溯、对比查看，保障架构变更可管控；

——宜支持自动校验拓扑模型的完整性、合理性，识别孤立节点、错误关联、缺失链路等异常拓扑问题，自动规整杂乱拓扑视图，输出拓扑健康度报告。

8.5. 告警管理

告警管理提供告警生成、告警自动处理等灵活的策略控制功能，以及 IT 基础设施、应用软件及业务运行状态告警数据的统一处理和告警操作功能。告警管理主要包括告警策略管理、告警生命周期管理、告警查询统计、告警操作等功能。

基本能力：

——应支持告警策略全生命周期管理（定义、配置、展现、查询、验证），确保快速部署与准确性；

——应提供标准化告警规则模板库，支持按基础设施、应用业务、网络链路、安全运维等场景批量复用告警策略，支持自定义告警处置流程与审批规则，适配规模化运维场景；

——应建立告警发现、分派、处理、核验、关闭全闭环流程，所有告警必须完成闭环处置，全程记录处置时间、处置人员、处置方案；

——应支持对告警数据的系统后台处理，包括告警数据的预处理、告警级别定义、告警关联、告警压缩、告警过滤、告警归并等。对故障类告警信息、性能数据进行统一的、可配置的规则化处理；

——应支持不同等级告警设置 SLA 处理时效超时预警督办，一键创建故障工单，告警与工单双向关联同步状态等操作；

——应支持基础故障定位关联能力，依托资源拓扑，展示告警上下游关联设备；

——应支持基础统计与报表能力，支持总量、误报率、MTTR、MTBF 等指标统计并按业务/机房/月份/类型输出周报/月报，提供趋势折线与故障 Top 看板；

——应支持告警操作面向监控人员提供告警操作管理功能，包括告警故障定位、告警确认、告警清除、告警升降级、告警派单、告警推送、告警显示过滤、告警查询；

——应支持基于运维团队、ECC 值班排班、业务权责配置告警认领权限，实现告警自动分派、轮值承接、超时督办，适配 7×24 小时运维值守场景；

——应支持按时段、业务线、系统模块、告警等级、故障类型多维度生成告警复盘报表，自动统计故障次数、平均处置时长等核心运维指标。

高级能力：

——宜支持基于链路拓扑与指标关联实现智能降噪、聚合与根因自动研判，区分根因与衍生告警，推送核心信号，屏蔽无效告警；

——宜支持告警与运维预案、自动化自愈联动，对常规故障自动触发自愈，重大告警关联应急处置预案，缩短止损时间；

——宜支持基于银行 SLO 配置告警策略，结合可用率、成功率、故障时长等指标，预判服务质量衰减，实现预警前置；

——宜提供自然语言交互入口，运维人员通过文本/语音提问，大模型关联实时告警、历史案例及知识库，输出排查路径与合规处置方案；

——宜支持大模型学习长期告警与工单数据，识别阈值不合理、规则冗余、误报场景，输出优化建议，持续降低误报率与漏报率。

9. 可观测平台能力

9.1. 安全合规

安全合规是全链路可观测体系的安全治理核心能力，覆盖运维数据全生命周期的安全防护与合规管控要求。通过统一的身份认证、权限管控、数据加密、审计追踪与合规校验机制，保障基础设施、应用服务、运维数据及操作行为的保密性、完整性与可用性，确保可观测体系建设符合国家法律法规、行业监管要求及企业内部安全规范，为全链路运维活动提供合规、可信、可审计的安全底座。

基本能力：

——应支持统一身份认证与访问控制，对接企业统一身份管理体系，提供账号管理、角色划分、权限分级能力，确保运维平台及数据访问具备合法身份校验与最小权限管控；

——应支持运维数据全链路加密传输与存储，对敏感指标、告警信息、日志数据、链路追踪数据采用加密技术手段，防止数据在采集、传输、存储、展示各环节泄露；

——应支持操作行为审计与日志留存，完整记录用户登录、配置变更、数据查询、模型修改等关键操作行为，保留操作人、操作时间、操作内容、操作结果等审计要素，满足安全溯源要求。

——应支持敏感数据识别与分级分类管理，对运维数据中的业务敏感信息、个人信息、配置密钥等进行标识与分级，按数据敏感等级实施差异化的访问与展示管控；

——应支持安全基线与合规规则配置，内置等保、行业监管及企业内部安全规范对应的合规检查项，覆盖账号安全、数据安全、网络安全、运维操作等关键维度；

——应支持漏洞与风险告警能力，对可观测平台自身组件、采集探针、数据通道的安全漏洞及异常访问行为进行监测，及时输出安全风险告警信息；

——应支持各能力模块的权限隔离，按业务域、组织架构、角色岗位划分数据与功能的可见范围，避免越权访问。

高级能力：

——宜支持自动化合规巡检与合规报告生成，按周期自动执行合规规则校验，自动识别不合规项并输出整改建议，形成结构化合规评估报告，满足监管审计与内部自查需求；

——宜支持零信任访问架构，基于动态身份、环境上下文与风险评分实施细粒度访问控制，对运维数据查询、配置变更、系统管理等操作实行持续验证与动态授权；

——宜支持数据动态脱敏与隐私保护，在数据查询、展示、导出环节对敏感字段进行实时脱敏处理，兼顾运维分析效率与数据隐私保护要求；

——宜支持安全态势感知与威胁分析，结合访问日志、操作审计、异常告警等多源安全数据，识别异常登录、越权访问、数据批量导出等潜在威胁行为，构建安全威胁全景视图；

——宜支持安全事件应急响应与联动处置，当检测到安全事件时可联动权限系统、告警系统、工单系统自动执行账号冻结、权限回收、告警升级、工单派发等处置动作，缩短安全响应周期；

——宜支持合规变更全流程追溯，对安全策略调整、权限变更、脱敏规则修改等安全配置变更实行审批留痕与版本管理，支持变更前后对比与历史回溯，确保安全变更可管控、可审计；

——宜支持跨系统合规一致性管理，与企业 CMDB、IAM、安全运营平台等系统联动同步安全策略与合规状态，保障可观测体系安全策略与企业整体安全体系对齐统一。

9. 2. 数据采集

数据采集是可观测性平台的基础环节，负责从各类数据源获取日志、指标、链路追踪、剖析等遥测数据。数据采集能力是指通过技术手段获取对机房环境、硬件、计算、存储、网络、业务、应用、中间件、风险安全等目标领域、场景的特定原始数据进行获取的能力。

基本能力：

——应支持从各类数据源采集数据，包括应用程序、基础设施、云服务、中间件、数据库等。Grafana 用户平均配置 16 个数据源，大型企业（5000 人以上）平均配置 24 个数据源；

——应支持对指标、日志、链路追踪三大支柱数据的统一采集。同时应支持持续性能剖析数据的采集，其正成为可观测性的第四大支柱；

——应提供轻量级、高性能的数据采集代理，能够在资源受限环境（如边缘设备、容器和 Kubernetes）中运行，不对系统本身性能造成显著影响；

——应支持结构化日志规范与日志级别设计，使不同语言和技术栈的服务都能以一致的方式输出可观测性数据；

——应支持灵活的采样策略配置，包括头部采样与尾部采样相结合的方式。

高级能力：

——宜支持基于 eBPF 的零侵入数据采集能力。eBPF 允许在 Linux 内核中安全地运行沙箱化程序，以零侵入的方式获取系统级别的深度可观测数据——包括系统调用频率、网络数据包详情、CPU

调度延迟和内存分配热点；

——宜具备 AI 驱动的智能采集能力，能够根据系统状态动态调整采集策略。在正常运行时采用低采样率以降低成本，在检测到异常时自动提升采样粒度以获取更详细的诊断数据；

——宜支持用户自定义指标的采集与上报，兼容开源采集协议对接用户的自定义指标，支持自动化拓扑能力，涵盖微服务、数据库、中间件等调用。

——宜支持在分布式环境中自动传递统一的 Trace ID 和 Span ID，实现跨服务的数据关联。定义统一的数据模型和采集协议，使不同语言和技术栈的服务都能以一致的方式输出可观测性数据。

9.3. 数据传输

数据传输能力是在前端数据采集完成后，依托标准化传输架构、加密通信、链路冗余等技术手段，统筹兼顾整条观测链路传输吞吐效率、数据传输完整性、链路运行可靠性与全流程通信安全的综合支撑能力。数据传输能力是可观测性平台数据管道的关键纽带。

基本能力：

——应针对网络监控设备、运维智能终端等固定算力设备，优先采用有线通信方式完成网络接入，保障传输稳定与带宽充足；

——应针对固定传感设备、移动式采集传感器优先选用无线通信方案接入，支持 WIFI、蓝牙、RFID、ZigBee、4G/5G 等多种无线通信实现方式；

——应要求所有传输网关设备配置主备实例与多链路冗余备份等可靠性保障机制，包括数据重传、断点续传、消息确认等能力，确保在网络波动或目标端暂时不可用时不丢失数据；

——应保障全域数据传输网络的可用带宽、端到端传输时延匹配各类运维观测数据的实时传输、批量同步业务需求；

——应支持在传输过程中对遥测数据进行压缩，减少网络带宽占用，降低传输成本。Elastic 等平台通过优化压缩实现更小的存储占用和传输开销；

——应具备对数据传输链路本身的监控能力，包括传输延迟、吞吐量、丢包率、队列积压等指标的实时观测，确保数据传输管道的健康运行。

高级能力：

——宜支持接收上层分析平台下发的策略编排配置，依据既定规则完成观测数据精细化分发、流量管控与传输限流控制；

——宜具备数据多路分发能力，可将同一份原始观测数据并行分发至数据分析、持久化存储等多个下游功能模块；

——宜提供多类自定义配置交互途径，包含 API 接口、本地配置文件、可视化 GUI 操作界面等，灵活完成传输分发策略调整。

——宜支持从数据采集端到存储端的端到端数据完整性校验，确保数据在传输过程中未被篡改或损坏；

——宜具备自适应传输优化能力，能够根据网络状况、目标端负载、数据量等动态因素自动调整传输参数（如批量大小、压缩级别、超时时间），在保证可靠性的前提下最大化传输效率；

——宜支持跨云、跨地域、跨数据中心的分布式数据传输，满足多云和混合云架构下的可观测性数据汇聚需求。标准化遥测管道可以跨多个云提供商和可观测性工具工作。

9.4. 数据加工

数据加工能力是对业务应用、安全告警等全类运维原始观测数据开展统一清洗、格式转换、指标聚合、逻辑计算、标准化处理的核心处理能力。原始采集数据存在格式杂乱、重复脏数据、维度不统一、指标口径不一致等问题，需通过标准化加工完成数据规整，为上层故障诊断、容量预测、SLA 统计、风险研判提供标准可信数据集。

基本能力：

——应支持将不同来源、不同格式的遥测数据转换为统一的数据模型。统一数据模型打破了可观测性信号的界限——无论是 RUM、APM、Infra 还是日志与事件，都应统一建模为核心模型（指标、调用链、用户体验、日志、事件、剖析等），并通过实体建立信号之间的联系；

——应支持海量运维观测数据全流程抽取、包括无效数据过滤、异常值剔除、重复数据去重、格式转换、指标聚合计算与标准化加载处理；

——应支持数据富化能力，为原始数据补充上下文信息，包括维表数据关联、地理位置信息、服务元数据、业务标签等；

——应配套轻量化、低延迟计算技术方案，控制数据加工耗时，支持实时流式的数据加工能力，使处理时延适配实时告警、故障观测等时效类运维场景；

——应支持对原始数据进行预聚合处理，生成不同时间粒度（分钟级、小时级、天级）的汇总数据，以支持高效的趋势分析和报表查询；

——应完整规范落地全流程数据加工管控流程，覆盖加工任务识别、加工规则定义、任务执行、运行监控、效果复盘全环节管理。

高级能力：

——宜具备 AI 驱动的智能数据加工能力，包括自动化的异常模式识别、智能日志聚类、自动字段提取与类型推断等。OpenTelemetry Collector 可以大规模接收、处理和导出数据，并添加功能以消除无用或重复的数据，推荐更有效地使用遥测数据的方法；

——宜提供可编程的数据加工管道能力，允许用户通过领域特定语言（DSL）或低代码方式自定义数据加工逻辑；

——宜同时提供流式实时处理、批量离线处理、关系图谱计算、高性能指标计算多类计算引擎能力，覆盖不同时效、不同分析场景；

——宜具备全局加工策略统一管控、任务统一调度能力，实现多加工任务有序排队、资源分配、启停管控与周期调度。

9.5. 数据存储

数据存储能力是依据统一存储规范，依托本地存储设备与外置存储介质承载海量实时、离线运维观测数据高效写入、持久化留存和快速查询的基础能力，是金融智能运维全链路数据底座核心支撑。当前，大型可观测性平台每天生成数 PB 级 Trace 数据和数万亿条 Span 记录，要求平台具备高效的实时处理能力和低成本的数据存储解决方案。

基本能力：

——应支持对指标、日志、链路追踪、剖析等多类型数据的统一存储。日志、链路追踪、指标三类数据应有针对性的存储方案；

——应完整配套运维数据清理、定期备份与故障恢复全流程功能；

——应依托分层存储技术实现冷热温数据分级差异化存储，平衡访问时效与存储成本；

——应部署容灾、校验、防误删等技术机制，规避系统故障、人工误操作引发的数据丢失与数据失真问题；

——应支撑海量运维数据长期存储，结合指标、日志、拓扑、调用链路等不同数据特征混合适配多类存储组件，涵盖关系库、时序库、文档库、向量库、图数据库；

——应保障读写吞吐、查询响应性能，满足金融运维实时查询、批量回溯等高并发存储访问需求。

高级能力：

——宜采用分布式架构搭建横向弹性扩展存储集群，可按需扩容存储节点与资源容量；

——宜按需组合适配多类存储技术方案，统筹满足运维存储高可用、高性能、高吞吐、超大容量、低成本多维度综合诉求；

——宜支持智能采样与按需存储策略，控制成本的同时保证分析深度。

9.6. 数据服务

数据服务及可视化能力是指提供运维数据消费接口及自服务的能力，同时提供统一的可视化界面，将运维对象及关联关系、运维流程、运维活动、运维管理信息转换成数字化的图形或图像进行展示，实现数字仿真、可视交互、可视运维、可视管理等功能，帮助运维人员快速做出正确的运维决策。

基本能力：

——应提供丰富的数据可视化能力，包括仪表盘、趋势图、拓扑图、火焰图等多种展示形式；

——应提供统一的查询语言和交互式探索界面，支持对指标、日志、链路追踪等所有数据类型进行跨模型联合查询；

——应提供灵活的告警规则配置和多渠道通知能力。支持静态阈值告警、环比告警、同比告警等多种告警策略，并通过邮件、短信、即时通讯等多种方式及时通知相关人员；

——应支持指标、日志、链路追踪三者之间的关联分析，实现快速根因分析；

——应自动生成微服务之间的调用关系和依赖图谱，帮助运维团队理解系统架构和调用链路；

——应支持多种数据源，包括但不限于：MySQL、Oracle 等常用数据库、电子表格、静态数据、API 等方式。

高级能力：

——宜具备 AI 驱动的智能运维能力；

——宜具备自动化的根因分析能力，提供对数据新鲜度、数据量等维度的实时可见性；

——宜支持通过自然语言生成查询语句的能力，用户可以用日常语言描述问题，平台自动转换为查询语句并返回分析结果；

——宜提供开放的 API 和可编程接口，并支持轻应用/低代码可观测性，通过最小化编写查询或脚本的需求，实现监控和分析工具的轻松快速配置。