

日志大数据实时采集与异常监测平台系统（使用指南）

版本号: [FCKGCPT3.0-241019]

发布时间: [2025年9月1日]

1 产品概述

日志大数据实时采集与异常监测平台是一个集海量日志实时采集、集中存储、智能分析、可视化监控与智能告警于一体的企业级运维与安全核心工具。它旨在帮助企业从纷繁复杂的IT系统日志中快速提取价值，发现潜在故障与安全威胁，保障业务稳定、安全、高效运行。

同时日志大数据实时采集与异常监测平台在以下几个方面表现出色：

- 性能领先：单集群日采 PB 级数据，3 节点 ES 集群秒索引 5 万 + 日志，流量波动 10 倍仍稳定，可用性 99.99%；
- 效率提升：故障排查从 4.2 小时缩至 17 分钟，异常识别准确率超 95%，某企业年减停机损失 300 万；
- 扩展性强：K8s 环境一键部署，兼容 AWS/Azure 云服务及 VMware，支持二次开发；
- 合规高效：满足 PCI DSS/HIPAA 等要求，某银行合规审计从 15 天缩至 2 天，且在金融（欺诈拦截率 98%）、制造（故障预警延至 8 小时）、互联网（降用户流失 22%）领域价值显著。

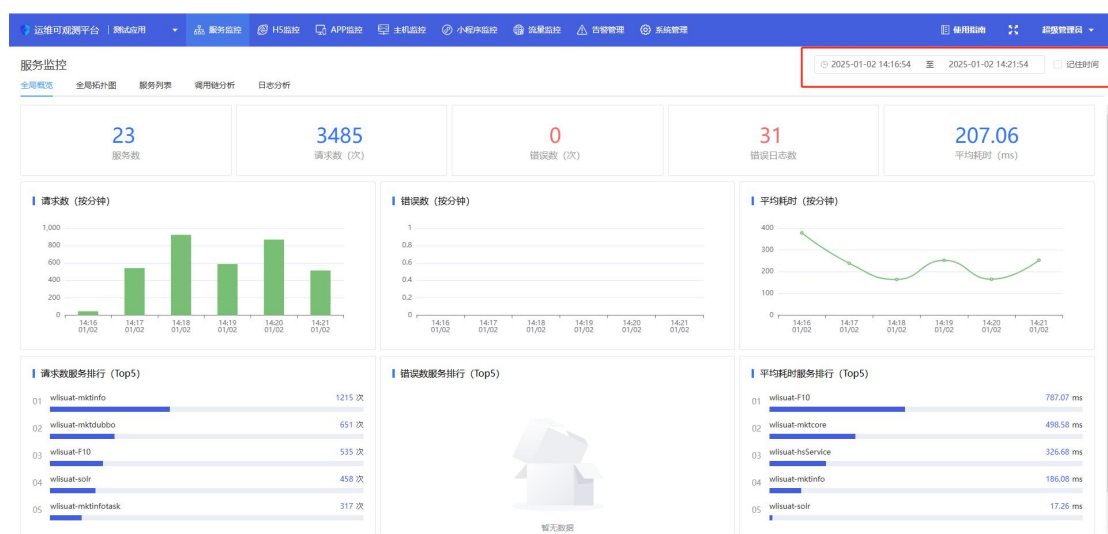
日志大数据实时采集与异常监测平台是一款功能强大、易于使用、高度灵活的应用性能平台。该平台通过技术创新重构了日志分析范式，从被动式问题排查转变为主动式异常预防，从孤立的日志查看升级为全局关联分析，为企业数字化转型提供了坚实的观测性支撑。

2 操作指引

2.1 时间日期选择器使用指南

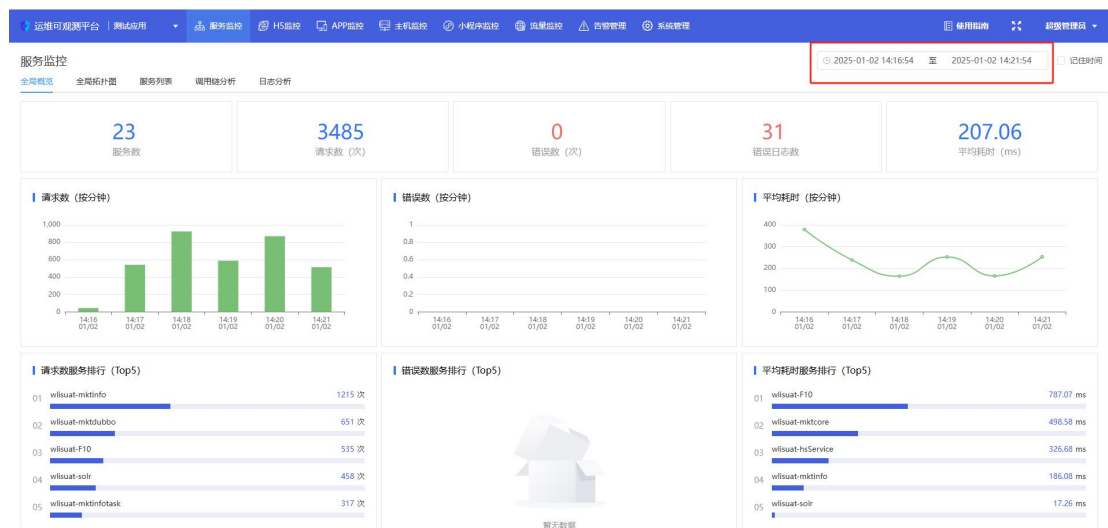
2.1.1 定位时间日期选择器

在系统界面的右上角，您可以找到一个时间日期选择器组件。这个组件用于全局设置您希望查看数据的时间范围。



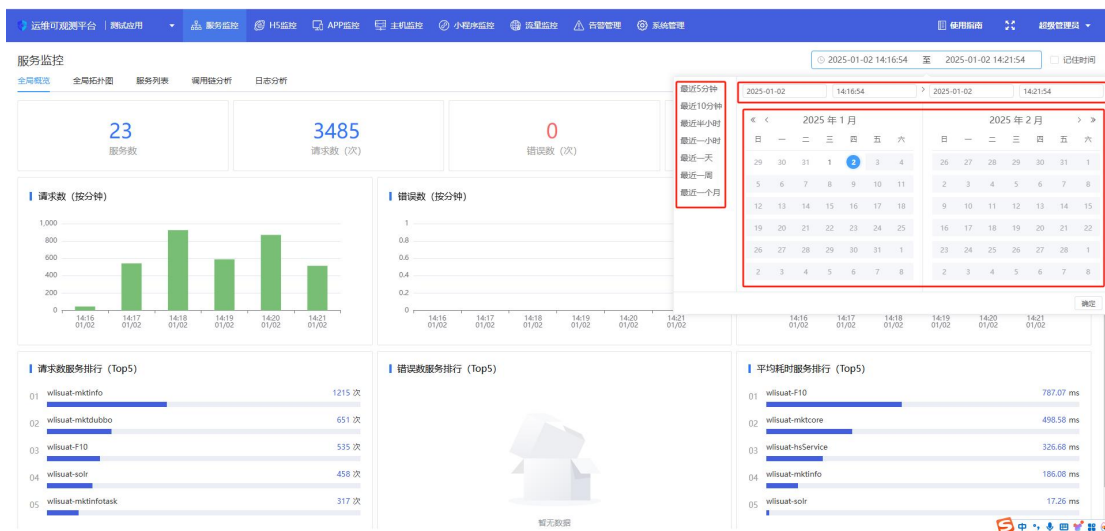
2.1.2 设置默认时间

默认情况下，时间日期选择器会设置为“最近五分钟”。这意味着，如果您不进行任何操作，系统将自动显示最近五分钟内的数据。



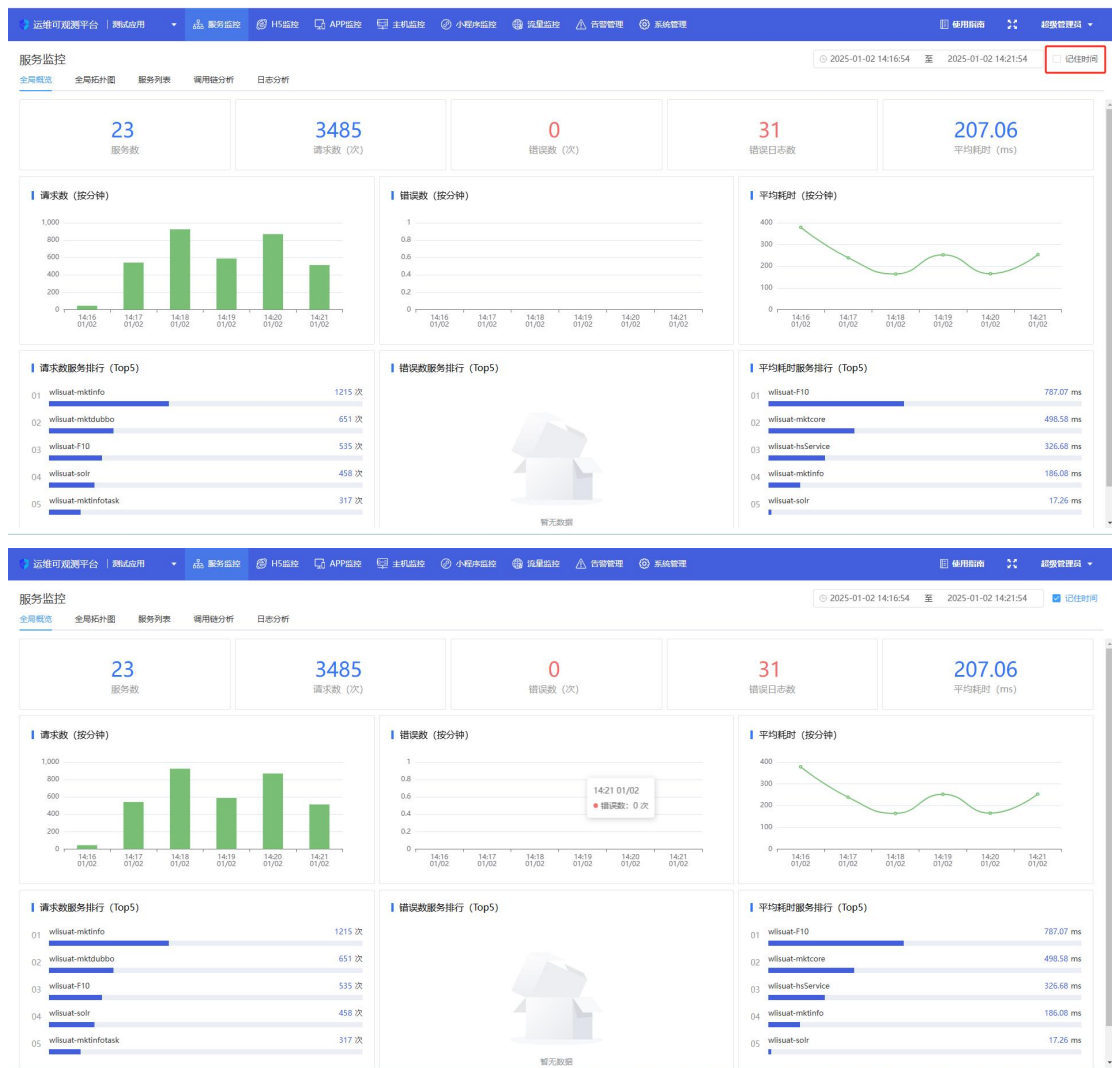
2.1.3 调整时间范围

如果您需要查看其他时间段的数据，可以点击时间日期选择器，并根据需要选择或输入您想要查看的时间范围。



2.1.4 使用“记住时间”功能

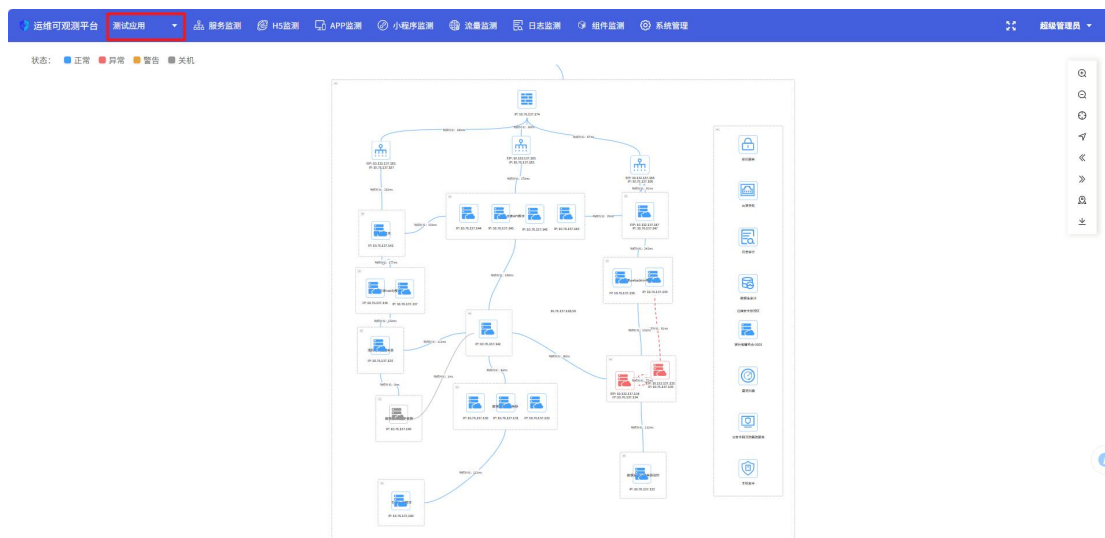
在时间日期选择器的右侧，有一个“记住时间”的选择框。当您选中这个选择框后，当前选择的时间范围将被系统记住。一旦您选中了“记住时间”选择框，并设置了您想要的时间范围，无论您如何刷新页面，系统都会保持您所选择的时间范围，而不会自动恢复到“最近五分钟”。如果您想要取消“记住时间”功能，只需再次点击选择框，将其取消选中即可。此时，系统将在您下次访问时恢复为默认的“最近五分钟”时间范围。



2.2 应用选择使用指南

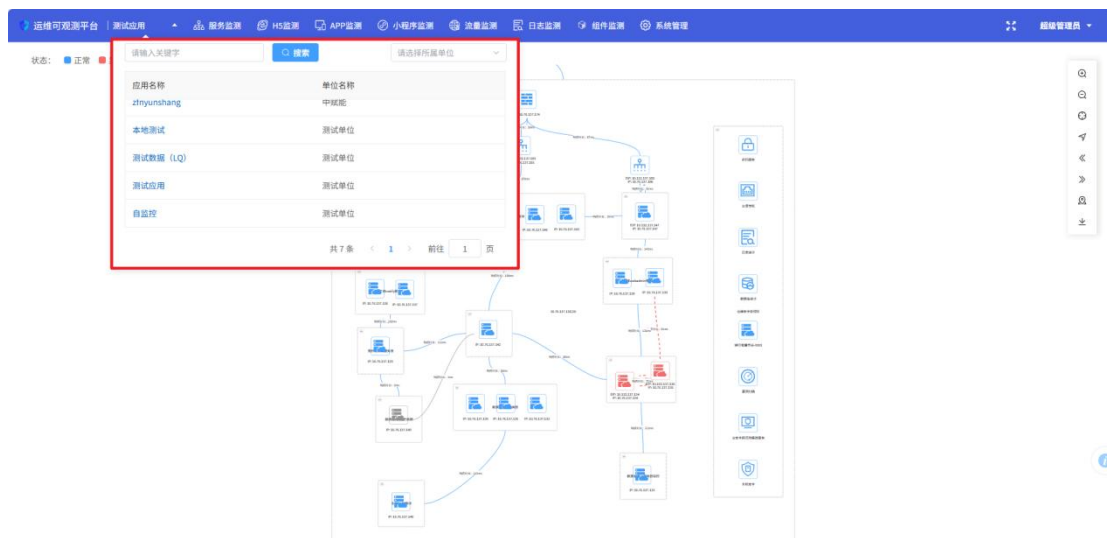
2.2.1 定位当前应用

在系统界面的左上角，您会看到一个当前正在运行的应用名称。



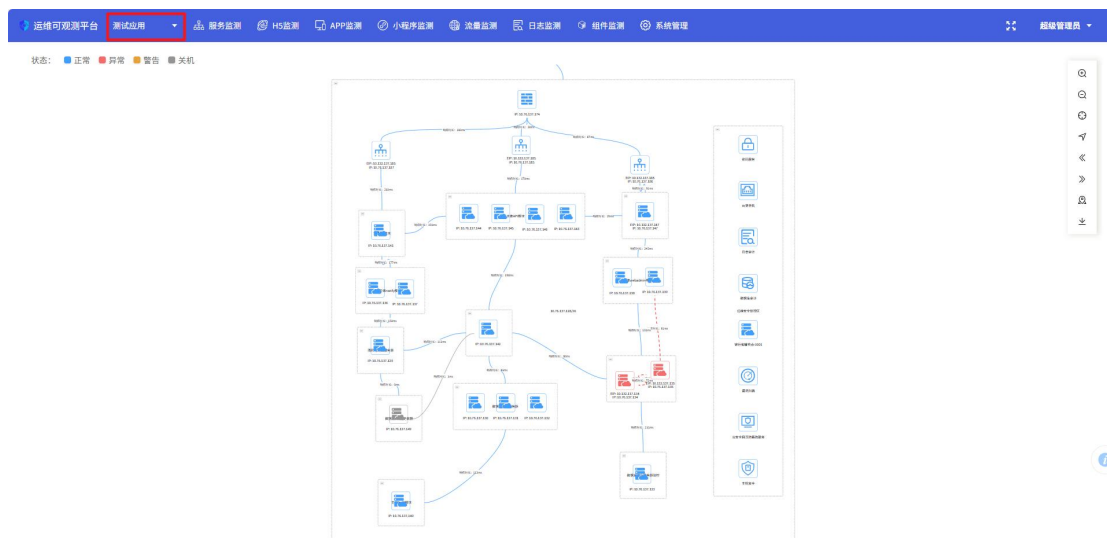
2.2.2 打开应用列表

点击该当前应用名称，系统将会弹出一个包含所有可用应用的列表。



2.2.3 切换应用以及数据切换

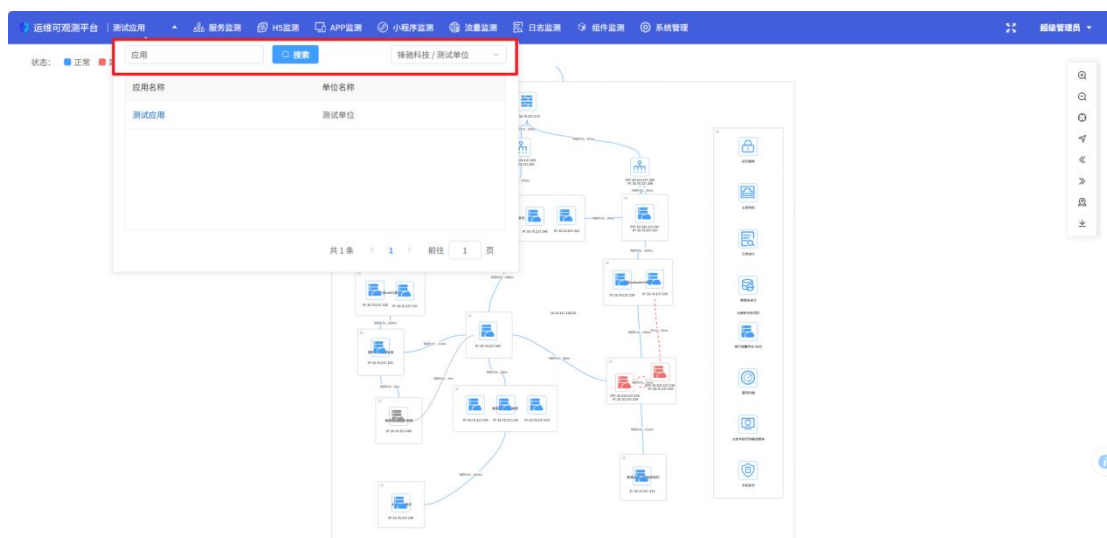
在弹出的应用列表中，您可以浏览并选择您想要切换到的应用。只需点击您想查看的应用即可，在这个时候监控的就是您当前选择应用的数据。



2.2.4 筛选应用

如果您想要快速找到特定的应用，您可以使用两种方式：

1. **使用搜索框：** 在应用列表顶部的搜索框中，根据“应用名称”或“单位名称”进行关键词搜索。输入相关信息后，点击“搜索”按钮，系统将自动筛选出符合条件的应用。
2. **使用单位筛选器：** 通过点击“单位筛选”下拉菜单（或类似控件），直接选择您要查看的单位。系统将立即显示**仅属于该单位**的所有应用列表。



您也可以结合使用这两种方式，例如先选择一个单位进行筛选，然后在结果中再输入应用名称进行更精确的搜索。

2.3 操作指南

点击位于界面右下角的图标，实时感知您所在页面位置。点击后显示当前页面的操作指南，可进行图标拖拽操作。

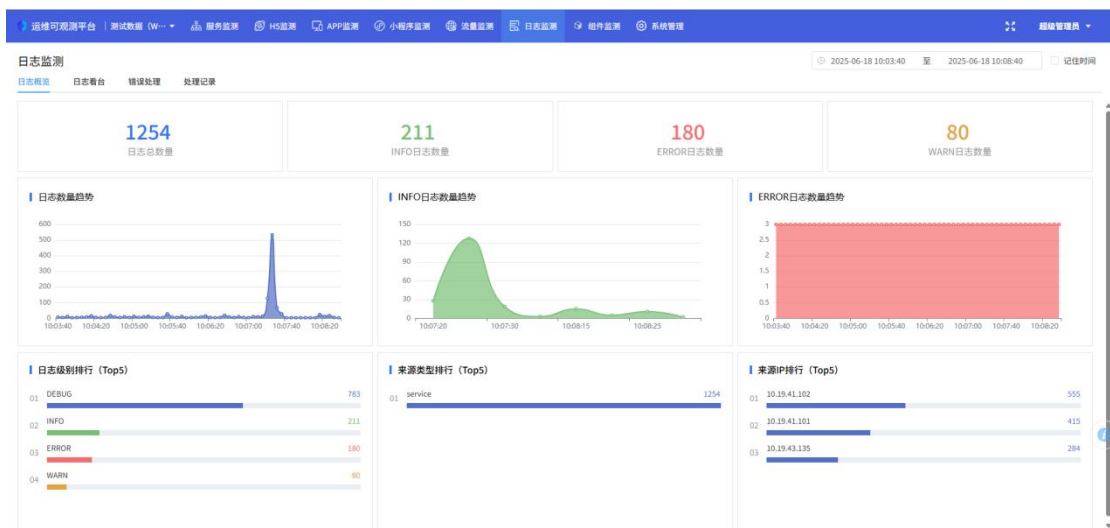


3 功能介绍

3.1 日志监测

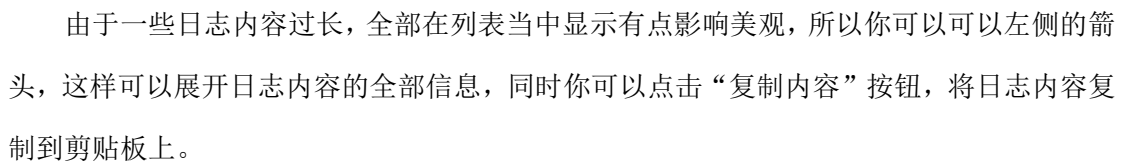
3.1.1 日志概览

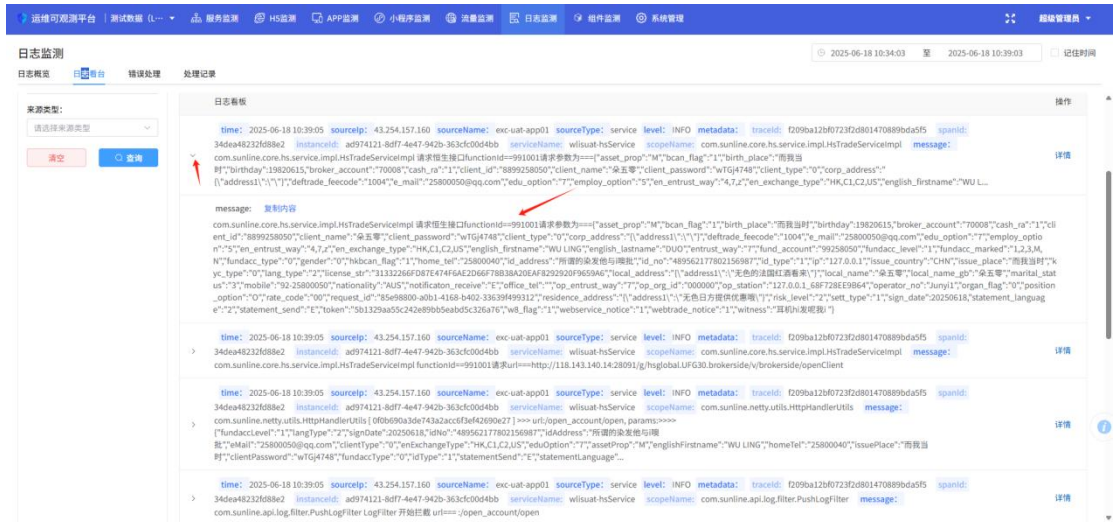
展示当前所选应用所选时间段日志概览（日志总数量、INFO日志数量、ERROR日志数量、WARN日志数量、日志数量趋势折线图、INFO日志数量趋势折线图、ERROR日志数量趋势折线图、日志级别排行（TOP5）、来源类型排行（TOP5）、来源IP排行（TOP5）），其中点击排行点击组件可以跳转到日志看台并且自动完成搜索。



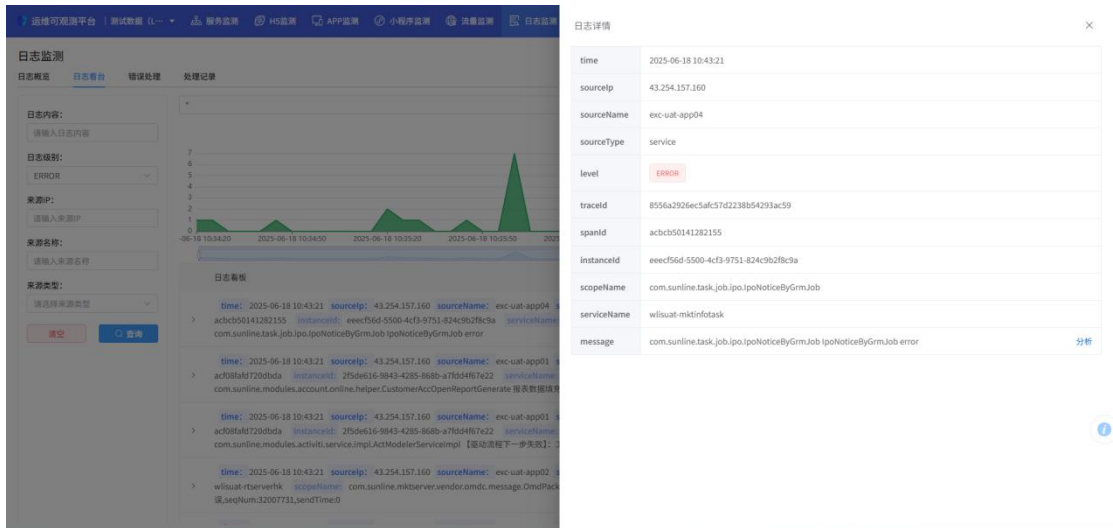
3.1.2 日志看台

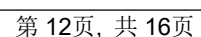
展示当前所选应用所选时间段日志详情信息，包括日志数量折线图以及日志看板信息（时间、来源IP、来源名称、来源类型、日志级别、日志内容等信息），除了目前页面上的搜索内容之外，还支持列表每个字段的搜索，操作就是点击字段，会将这个字段作为搜索条件插入到搜索区域。





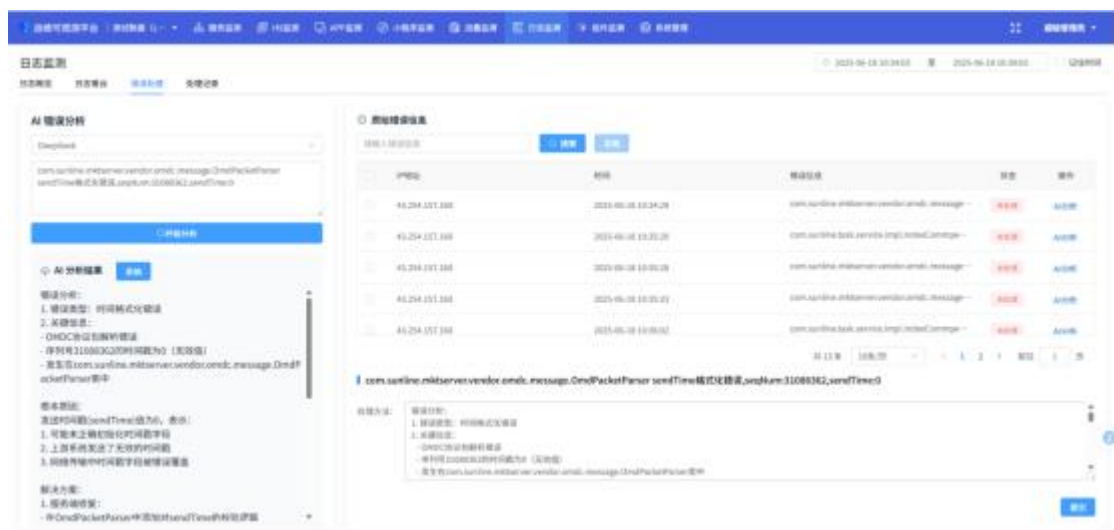
点击操作栏的“详情”按钮可以查看当前日志的详情信息（时间、来源IP、来源名称、来源类型、日志级别等内容），点击日志内容右侧的“分析”按钮，会使用AI工具通过不同的日志级别分析当前日志的信息。



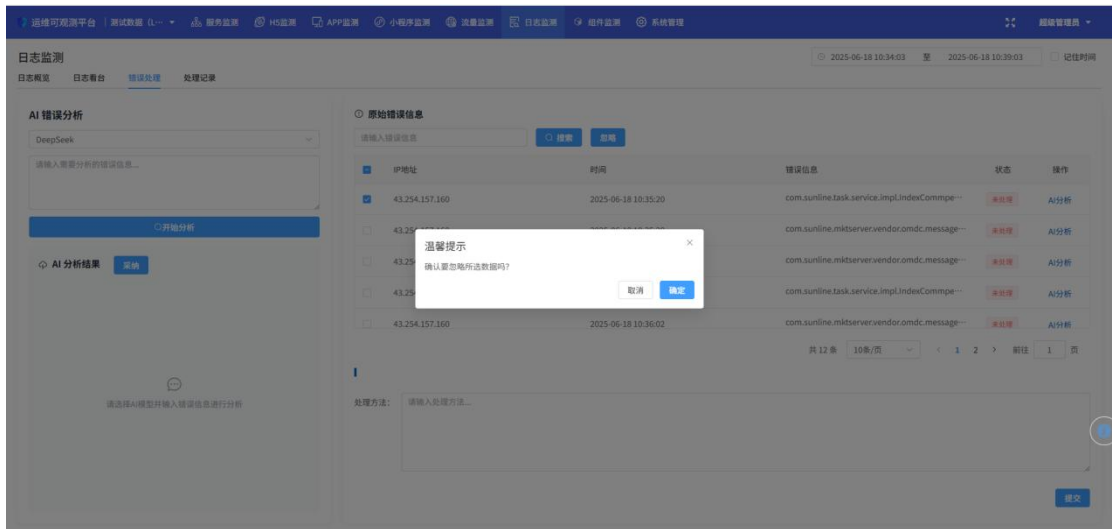


3.1.3 错误处理

该页面主要是使用AI工具分析错误日志，主要是分析当前日志的错误原因以及解决的方案，主要操作步骤就是点击“原始错误信息”列表操作栏的“AI分析”按钮，点击之后会将当前行的错误信息插入到“AI错误分析”的输入框，你只需要点击“开始分析”按钮，这个时候AI就开始分析当前日志的错误原因以及解决方案，分析完成之后你可以点击“AI分析结果”旁边的“采纳”按钮或者双击AI分析出的结果，这个时候AI分析的结果就会插入到处理方法当中，你可以适当对AI给出的结果进行删减，删减完成之后你可以“提交”按钮，代表你已经对该条错误信息处理完成。

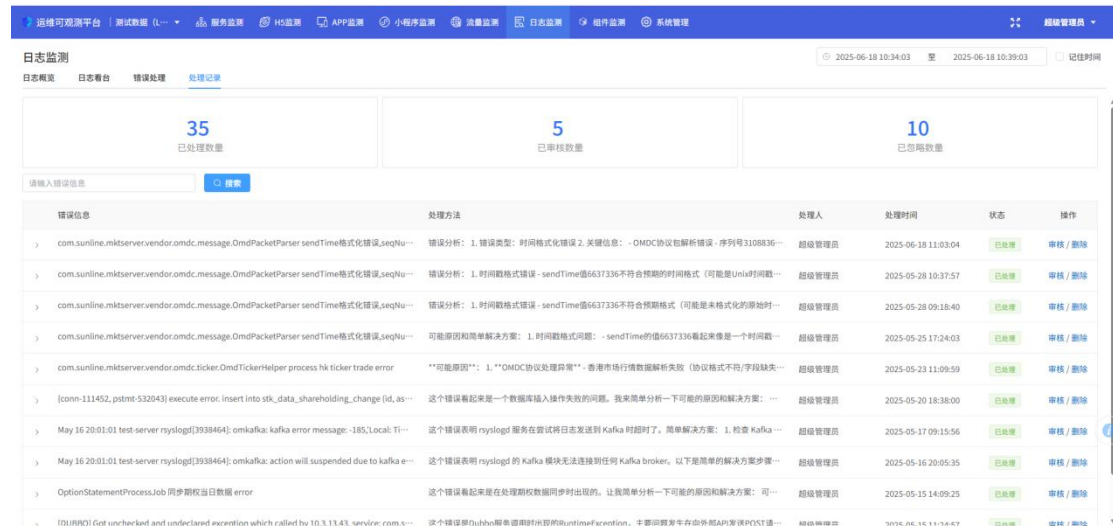


由于一些日志的特殊性，你也可以忽略这条错误日志，不去处理这条错误日志，主要操作步骤就是选择你要选择的日志信息，然后点击“忽略”按钮，即可完成这个操作。



3.1.4 处理记录

当前页面是已经处理过的错误信息（错误信息、处理方法、处理人、处理时间、状态（已处理、已审核、已忽略）），以及各个状态的数量，点击列表上方的各个状态数量可以对列表完成搜索，也可以通过搜索错误信息的关键字也可以对列表完成搜索。



远维可观测平台 | 测试数据 (100) | 服务监控 | HS监控 | APP监控 | 小程序监控 | 流量监控 | 日志监控 | 组件监控 | 系统管理

日志监控

日志概览 | 日志看板 | 错误处理 | 处理记录

35

已处理数量

5

已审核数量

10

已忽略数量

请输入错误信息

搜索

错误信息	处理方法	处理人	处理时间	状态	操作
[DUBBO] Got unchecked and undeclared exception which called by 10.3.13.43, service: com.su...	这个错误是Dubbo服务调用时出现的异常，主要问题在于调用外部API时失败了。以下是简单的解决...	超级管理员	2025-05-08 15:25:27	已审核	审核 / 删除
120.229.31.92 -- [08/Apr/2025:15:36:02 +0800] "GET /api/netflow/flow-mirror/rules/stats/strea...	已忽略	超级管理员	2025-05-08 11:17:36	已审核	审核 / 删除
群数子节点列表异常	已忽略	超级管理员	2025-05-08 11:14:41	已审核	审核 / 删除
开户结果回调异常2024030510000004	111	超级管理员	2025-05-08 11:01:10	已审核	审核 / 删除
[DUBBO] Got unchecked and undeclared exception which called by 10.3.13.43, service: com.su...	这个错误是Dubbo服务调用时发生的RuntimeException，主要问题出现在调用外部API接口时，以...	超级管理员	2025-05-06 16:51:56	已审核	审核 / 删除

共 5 条

10条/页

< 1 >

前往 1 页

由于错误信息以及处理方法过长，全部在列表当中显示有点影响美观，所以你可以可以左侧的箭头，这样可以展开全部的详细信息。

远维可观测平台

测试数据 (100)

服务监控

HS监控

APP监控

小程序监控

流量监控

日志监控

组件监控

系统管理

日志监控

日志概览

日志看板

错误处理

处理记录

35

已处理数量

5

已审核数量

10

已忽略数量

请输入错误信息

搜索

错误信息	处理方法	处理人	处理时间	状态	操作
com.sunline.mktserver.vendor.omdc.message.OmdPacketParser sendTime格式化错误,seqNum...	错误分析: 1. 错误类型: 时间格式化错误 2. 关键信息: - OMDC协议包解析错误 - 序列号3108836...	超级管理员	2025-06-18 11:03:04	已处理	审核 / 删除
错误信息: com.sunline.mktserver.vendor.omdc.message.OmdPacketParser sendTime格式化错误,seqNum:31088362,sendTime:0 已处理 处理时间: 2025-06-18 11:03:04 处理人: 超级管理员					
处理方法: 错误分析: 1. 错误类型: 时间格式化错误 2. 关键信息: - OMDC协议包解析错误 - 序列号31088362的时间戳为0 (无效值) - 发生在com.sunline.mktserver.vendor.omdc.message.OmdPacketParser类中 根本原因: 发送时间戳(sendTime)值为0, 表示: 1. 可能未正确初始化时间戳字段 2. 上游系统发送了无效的时间戳 3. 网络传输中时间戳字段被错误篡改 解决方案: 1. 服务端修复: - 在OmdPacketParser中添加对sendTime的校验逻辑 - 对0值时间戳使用当前系统时间替代或抛出明确异常 2. 客户端检查: - 验证上游系统是否按正常生成时间戳 - 检查网络传输是否可能篡改报文内容 建议同时检查网络设备和协议版本兼容性, 确保时间戳字段传输完整。					
com.sunline.mktserver.vendor.omdc.message.OmdPacketParser sendTime格式化错误,seqNu...	错误分析: 1. 时间戳格式错误 - sendTime值6537336不符合预期的时间格式 (可能是Unix时间戳...	超级管理员	2025-05-28 10:37:57	已处理	审核 / 删除

同时你也可以在操作栏对当前的处理信息进行审核以及删除，审核就是你对AI给出的处理方法有更好的处理方法。

运维综合管理平台 | 测试数据 (100%) | 服务监控 | MS监控 | APP监控 | 小程序监控 | 流量监测 | 日志监测 | 告警配置 | 系统管理

日志监测

日志概览 | 日志看板 | 错误处理 | 处理记录

35
已处理数量

请输入错误信息 搜索

错误信息

com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime错误
com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime错误
com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime错误
com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime错误
com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime错误
[conn=111452, psId=520243] execute error: Insert into xfx_data_sharinghold
May 16 20:01:01 test-server rsyslogd[339464]: omkafka: kafka error message: '185', local: Ti-
May 16 20:01:01 test-server rsyslogd[339464]: omkafka: action will suspended due to kafka e-
OptionStatementProcessJob 用周期日志数据 error
TDI0003 Get unchecked and unhandled exception which called by 10.3.13.41 service.com.s-

5

审核处理记录

错误信息:

com.sunline.mktserver.vendor.omic.message.OmdPacketParser sendTime格式化错误 seqNum:31088362, sendTime:0

处理方法:

错误分析:
1. 错误类型: 时间格式化错误
2. 关键信息:
- OMD 协议包解析错误
- 序列号 31088362 的时间值为 0 (无效值)
- 发生在 com.sunline.mktserver.vendor.omic.message.OmdPacketParser 类中
根本原因:
发送时间 (sendTime) 值为 0, 表示;
3. 可避免正确初始化时间数据字段

审核建议:

取消 确定

10
已忽略数量

处理人	处理时间	状态	操作
超级管理员	2025-06-18 11:03:04	已处理	审核 / 忽略
超级管理员	2025-06-18 10:37:57	已处理	审核 / 忽略
超级管理员	2025-06-28 09:18:40	已处理	审核 / 忽略
超级管理员	2025-05-25 17:24:03	已处理	审核 / 忽略
超级管理员	2025-05-23 11:09:59	已处理	审核 / 忽略
超级管理员	2025-05-20 18:38:00	已处理	审核 / 忽略
超级管理员	2025-05-17 09:15:56	已处理	审核 / 忽略
超级管理员	2025-05-16 20:05:35	已处理	审核 / 忽略
超级管理员	2025-05-15 14:09:25	已处理	审核 / 忽略
超级管理员	2025-05-16 11:24:67	已处理	审核 / 忽略