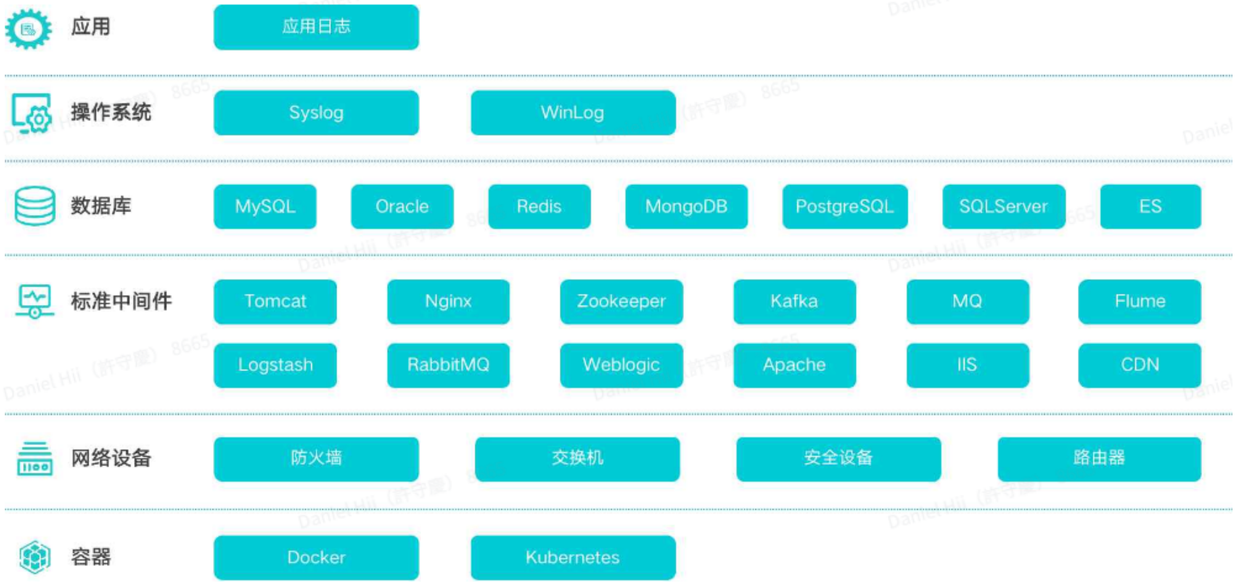
Hera Product White Paper

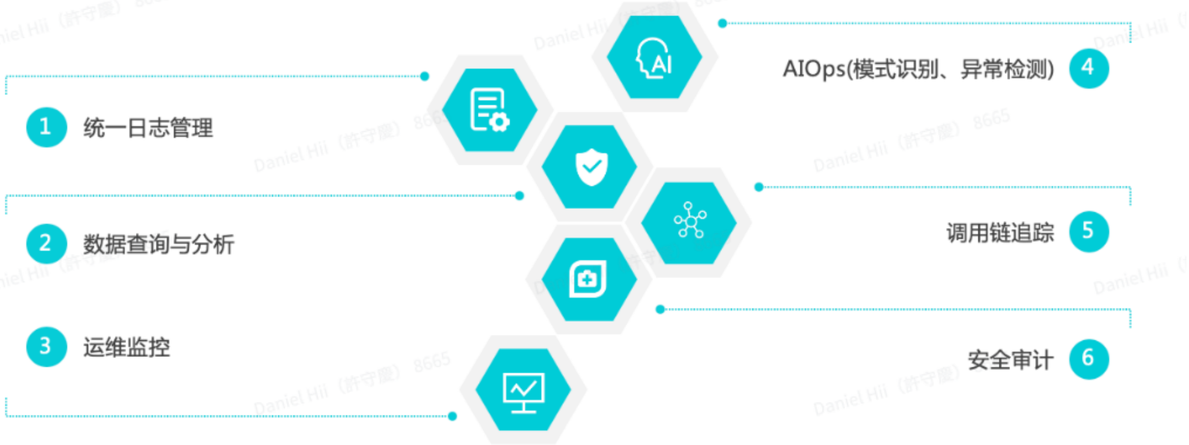
Product Background

What is a log? A log is a time-ordered collection of some operations performed on specified objects by the system and the outcomes of those operations. Each log file consists of log records, each of which describes a separate system event. Logs contain necessary and valuable information about activities related to IT resources such as servers, workstations, firewalls, and application software. Logs are categorized into application logs, security logs, system logs, Scheduler service logs, FTP logs, DNS server logs, etc.



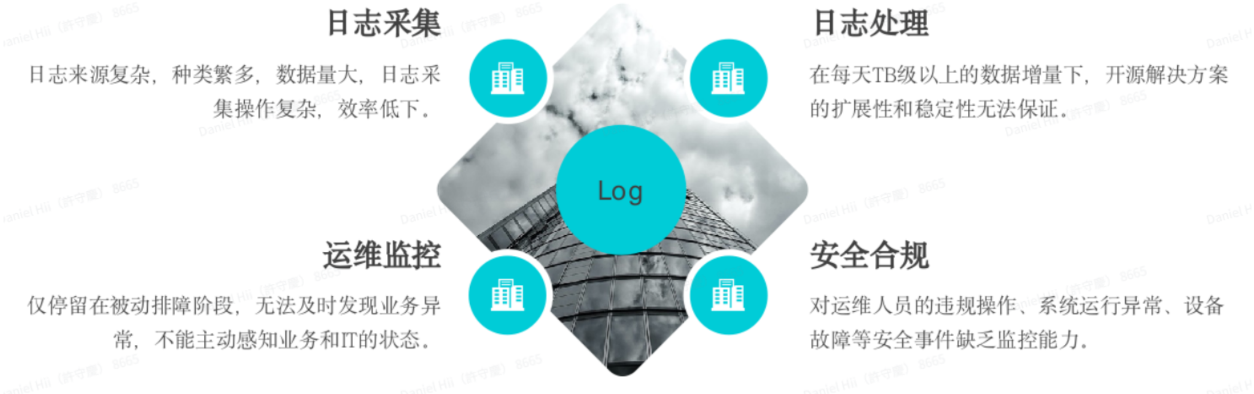
应用	应用日志
操作系统	Syslog WinLog
数据库	MySQL Oracle Redis MongoDB PostgreSQL SQLServer ES
标准中间件	Tomcat Nginx Zookeeper Kafka MQ Flume Logstash RabbitMQ Weblogic Apache IIS CDN
网络设备	防火墙 交换机 安全设备 路由器
容器	Docker Kubernetes

The Role of Logs in Operations and Maintenance



Logs, which contain rich data information, provide detailed data for problem localization and fault prediction, playing an important role in operations and maintenance. Log operation and maintenance is a crucial aspect of O&M, enabling operators to understand detailed information about servers, hardware and software, and user behaviour. This allows for the quick discovery of faults and timely alerting or preemptive warning of yet-to-occur faults, thus improving the efficiency of operations.

Challenges Faced by Enterprises in Log Application



日志采集

日志来源复杂，种类繁多，数据量大，日志采集操作复杂，效率低下。

日志处理

在每天TB级以上的数据增量下，开源解决方案的扩展性和稳定性无法保证。

运维监控

仅停留在被动排障阶段，无法及时发现业务异常，不能主动感知业务和IT的状态。

安全合规

对运维人员的违规操作、系统运行异常、设备故障等安全事件缺乏监控能力。

Enterprises currently face several challenges in log application, including how to efficiently manage and analyze large volumes of log data, ensure the security and privacy of log data, and leverage the full potential of log data to support decision-making and business optimization.

Hera's Solutions

Log Monitoring: Hera provides log anomaly detection capabilities based on thresholds and intelligent algorithms, along with exceptional analysis capabilities to ensure business continuity.
No Need for Format Parsing: Hera can directly interface with raw log content, completing data analysis to detect faults. This reduces dependency on experts and allows for quick delivery of business value.
Strong Discovery and Troubleshooting Capabilities: Hera has high accuracy in fault discovery and provides clear presentations during faults, offering directions for troubleshooting and speeding up the localization process.
Complementary to Existing Monitoring: Hera is compatible with existing monitoring rules and often discovers faults not covered by existing rules, bringing significant business value.

Product Features

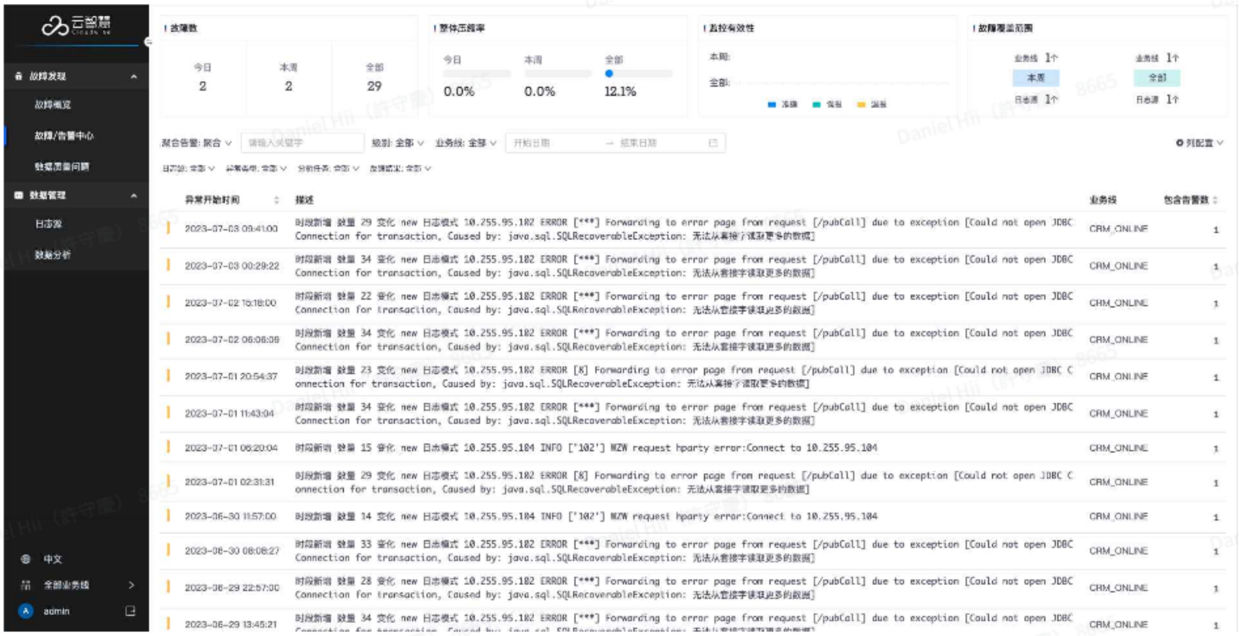
Hera uses advanced data processing and analysis technologies to efficiently handle large volumes of log data. Its capabilities include powerful fault discovery functions, visual presentations of data and analysis results, flexible log source management functions, and highly customizable data analysis tasks to meet diverse user requirements.

Product Value

Hera provides value in basic operations and maintenance by improving the efficiency of fault localization and enabling timely discovery and handling of abnormalities. In business analysis, it aids in quickly analyzing system performance issues and understanding key business information. Hera's anomaly detection and data analysis capabilities ensure business continuity and support operations and maintenance activities.

Core Functions

Fault Center: A core module providing a list of faults and key information to help users understand the fault situation in the system.
Fault Details Display: Offers detailed descriptions of faults and possible solutions.
Data Quality Issue Monitoring: Focuses on log data quality issues to help users discover potential data anomalies.
Log Source Management: Provides convenient functions for log data integration and management.
Data Analysis: Assists in pattern recognition and anomaly detection based on log data, offering key analysis results.



故障数: 今日 2, 本周 2, 全部 29

整体压缩率: 今日 0.0%, 本周 0.0%, 全部 12.1%

聚合告警: 聚合 | 请输入关键字 | 级别: 全部 | 业务线: 全部 | 开始日期 → 结束日期

日志源: 全部 | 异常类型: 全部 | 分析任务: 全部 | 故障状态: 全部

异常开始时间	描述	业务线	包含告警数
2023-07-03 09:41:00	时段新增 数量 29 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-03 00:29:22	时段新增 数量 34 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-02 15:18:00	时段新增 数量 22 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-02 06:06:09	时段新增 数量 34 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-01 20:54:37	时段新增 数量 23 变化 new 日志模式 10.255.95.182 ERROR [8] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-01 11:43:04	时段新增 数量 34 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-07-01 06:20:04	时段新增 数量 15 变化 new 日志模式 10.255.95.184 INFO ['102'] MZW request hparty error:Connect to 10.255.95.184	CRM_ONLINE	1
2023-07-01 02:31:31	时段新增 数量 29 变化 new 日志模式 10.255.95.182 ERROR [8] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-06-30 11:57:00	时段新增 数量 14 变化 new 日志模式 10.255.95.184 INFO ['102'] MZW request hparty error:Connect to 10.255.95.184	CRM_ONLINE	1
2023-06-30 08:08:27	时段新增 数量 33 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-06-29 22:57:00	时段新增 数量 28 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC Connection for transaction, Caused by: java.sql.SQLRecoverableException: 无法从套接字读取更多的数据]	CRM_ONLINE	1
2023-06-29 13:45:21	时段新增 数量 34 变化 new 日志模式 10.255.95.182 ERROR [***] Forwarding to error page from request [/pubCall] due to exception [Could not open JDBC	CRM_ONLINE	1

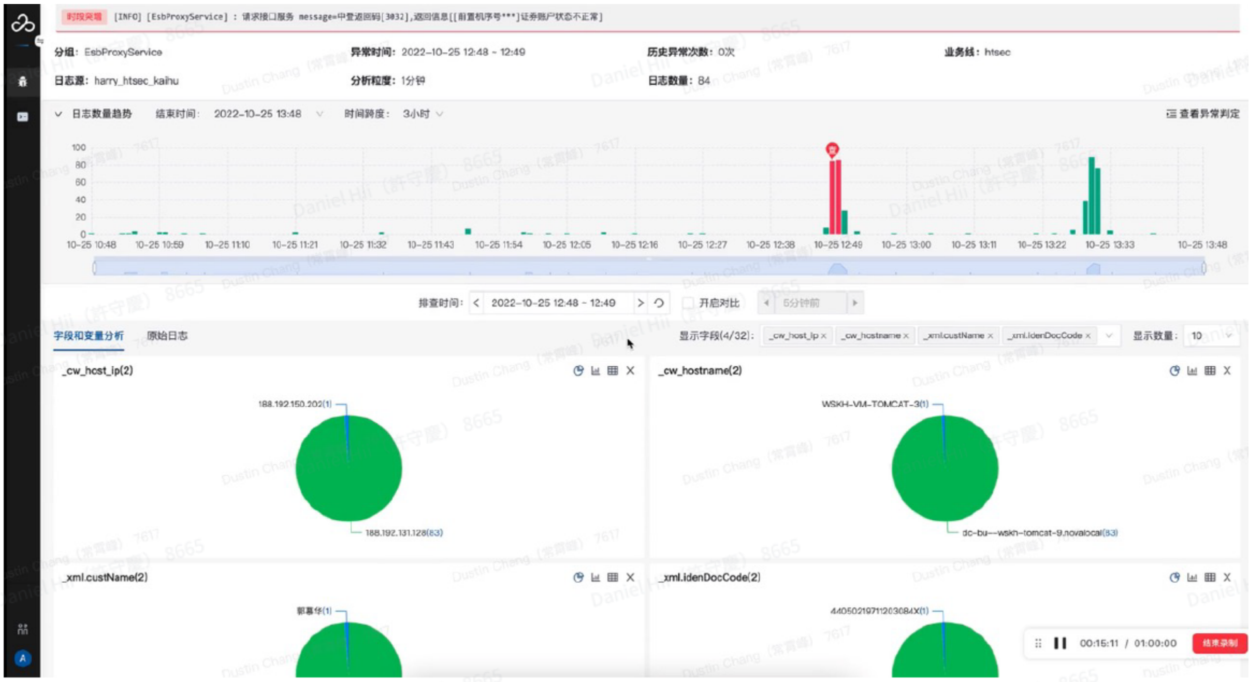
Applicable Range of the Product

Hera is suited for various types of logs, with certain types being more effectively managed and analyzed than others. It is particularly effective with business logs from sectors like banking and brokerage, and also performs well with database, middleware, and operating system logs.

Fault Details Display

The Fault Details module provides detailed information about faults, helping users to deeply understand the background and impact of the fault. The main functions include:

Fault Level Assessment: Conducts a level assessment based on the severity of the fault, helping users to prioritize key faults.
Exception Start Time Record: Records the start time of the fault, helping users to determine the period when the fault occurred.
Problem Description and Solution: Provides a detailed description of the fault and possible solutions, helping users to quickly resolve the issue.
Business Line and Log Source Information: Identifies the business line and log source to which the fault belongs, helping users locate the source of the fault.



时段突增 [INFO] [EsbProxyService] : 请求接口服务 message=中登返回码[3032],返回信息[[前置机序号***]证券账户状态不正常]

分组: EsbProxyService 异常时间: 2022-10-25 12:48 - 12:49 历史异常次数: 0次 业务线: htsec
日志源: harry_htsec_kaihu 分析粒度: 1分钟 日志数量: 84

日志数量趋势 结束时间: 2022-10-25 13:48 时间跨度: 3小时

排查时间: 2022-10-25 12:48 - 12:49 开启对比 5分钟前

显示字段(4/32): _cw_host_ip _cw_hostname _xml.custName _xml.idenDocCode 显示数量: 10

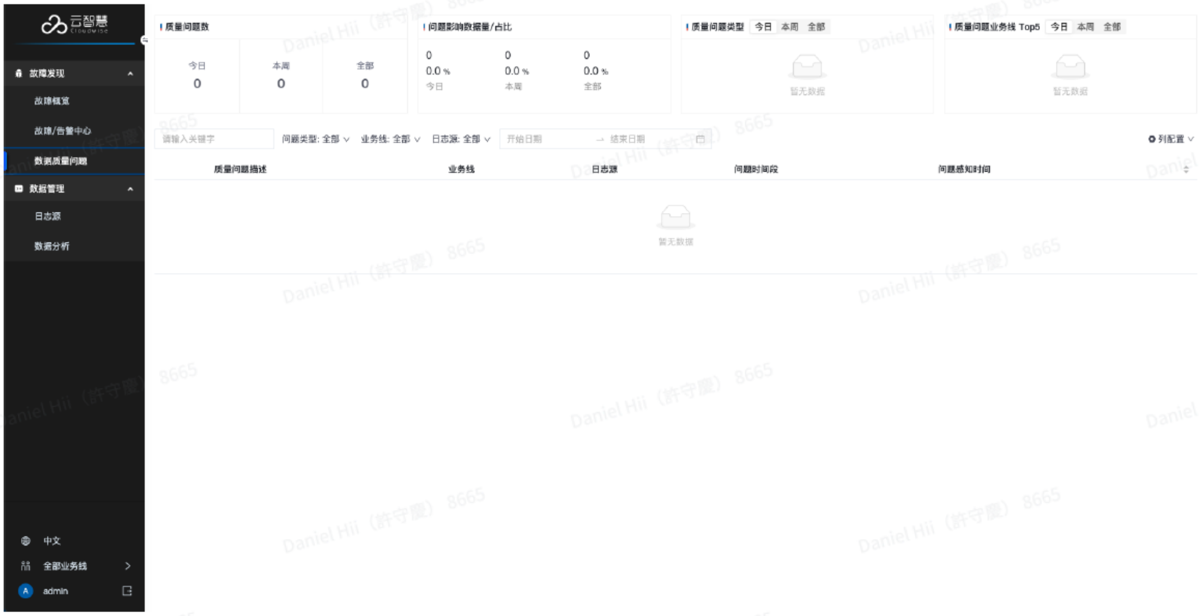
Data Quality Issue Monitoring

The Data Quality Issue Monitoring module mainly focuses on the quality issues of log data, helping users discover potential data anomalies.

The main functions include:

Data Loss Detection: Detects missing situations in log data, helping users promptly identify issues with data loss.

Data Duplication Detection: Identifies duplicate log data to avoid interference with analysis results.
Data Latency Analysis: Analyzes the latency of log data, assisting users in assessing the system's real-time performance.



质量问题数

今日	本周	全部
0	0	0

问题影响数据量/占比

0	0	0
0.0 %	0.0 %	0.0 %
今日	本周	全部

质量问题类型 今日 本周 全部

质量问题业务线 Top5 今日 本周 全部

请输入关键字　问题类型: 全部　业务线: 全部　日志源: 全部　开始日期 → 结束日期

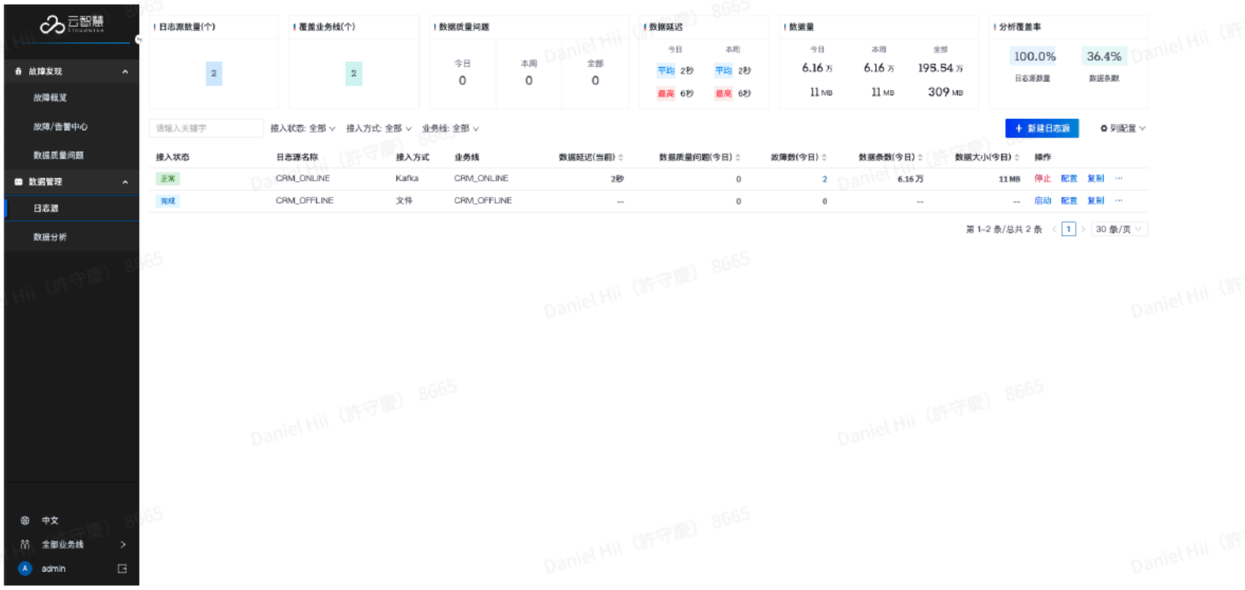
质量问题描述	业务线	日志源	问题时间段	问题感知时间

Log Source Management

The Log Source Management module is responsible for the integration of log data, offering convenient management features. Main functionalities include:

Creating New Kafka Log Sources: Supports users in creating Kafka log sources for easy data access and management.
Creating New Offline Log Sources: Supports users in creating offline log sources for handling offline data analysis tasks.

Log Source Management: Provides management capabilities for log sources, including editing, deleting, and viewing log source information.



日志源数量(个)
2

覆盖业务线(个)
2

数据质量问题
今日 0 | 本周 0 | 全部 0

数据延迟
今日: 平均 2秒, 最高 6秒
本周: 平均 2秒, 最高 6秒

数据量
今日: 6.16 万, 11 MB
本周: 6.16 万, 11 MB
全部: 195.54 万, 309 MB

分析覆盖率
100.0% 日志源数量
36.4% 数据条数

请输入关键字 接入状态: 全部 接入方式: 全部 业务线: 全部

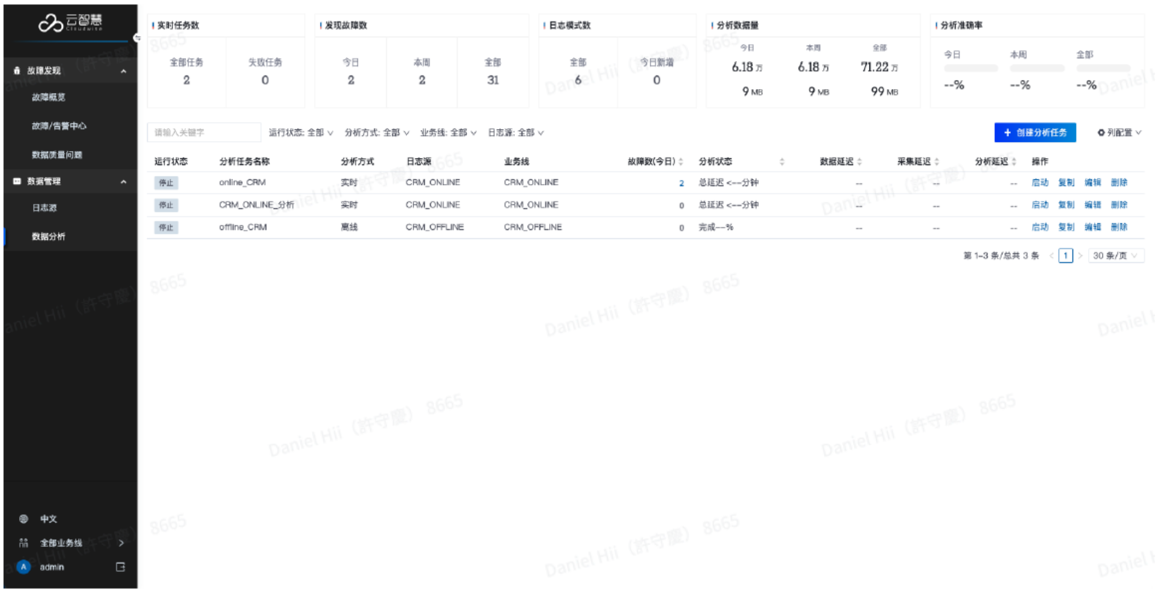
接入状态	日志源名称	接入方式	业务线	数据延迟(当前)	数据质量问题(今日)	故障数(今日)	数据条数(今日)	数据大小(今日)	操作
正常	CRM_ONLINE	Kafka	CRM_ONLINE	2秒	0	2	6.16万	11 MB	停止 配置 复制 ···
完成	CRM_OFFLINE	文件	CRM_OFFLINE	--	0	0	--	--	启动 配置 复制 ···

第 1-2 条/总共 2 条 1 30 条/页

Data Analysis

The Data Analysis module assists users in pattern recognition and anomaly detection based on log data, delivering key analysis outcomes. Main functionalities include:

Data Analysis Task Creation: Supports users in creating data analysis tasks, defining analysis rules and objectives.
Fault Quantity Statistics: Counts the number of faults discovered by each task, helping users assess the effectiveness of the analysis.
Log Pattern Recognition: Identifies patterns within logs, aiding users in understanding the structure and characteristics of log data.
Analysis Data Quantity Record: Records the amount of data analyzed by each task, helping users comprehend the scope of the analysis.
Analysis Accuracy Assessment: Evaluates the accuracy of data analysis, helping users determine the reliability of the analysis results.



实时任务数: 全部任务 2 | 失败任务 0

发现故障数: 今日 2 | 本周 2 | 全部 31

日志模式数: 全部 6 | 今日新增 0

分析数据量: 今日 6.18 万 9 MB | 本周 6.18 万 9 MB | 全部 71.22 万 99 MB

分析准确率: 今日 --% | 本周 --% | 全部 --%

运行状态	分析任务名称	分析方式	日志源	业务线	故障数(今日)	分析状态	数据延迟	采集延迟	分析延迟	操作
停止	online_CRM	实时	CRM_ONLINE	CRM_ONLINE	2	总延迟 <--分钟	--	--	--	启动 复制 编辑 删除
停止	CRM_ONLINE_分析	实时	CRM_ONLINE	CRM_ONLINE	0	总延迟 <--分钟	--	--	--	启动 复制 编辑 删除
停止	offline_CRM	离线	CRM_OFFLINE	CRM_OFFLINE	0	完成--%	--	--	--	启动 复制 编辑 删除

第 1-3 条/总共 3 条 1 30 条/页

Our log analysis product aims to address common issues within the current industry and provide efficient, stable, and user-friendly solutions. By facilitating fault discovery and aiding in troubleshooting and localization, it helps enterprises enhance system stability and performance. We believe that with our product, users can identify and resolve faults more quickly and accurately, thereby improving business efficiency and customer satisfaction.

Product Applicability Range

Logs not suitable:

Logs where every entry contains identical fields, nginx/apache logs, binary logs, logs with JSON/dictionary content with unordered fields.
Logs that may affect the effectiveness:

Logs containing binary content, logs with more than 400 characters per line, logs with JSON/dictionary content.
Logs with good effectiveness:

Business logs (such as those from mobile banking, online banking, collection systems, brokerages' counters, core trading, mobile apps, various platforms, customer centers, comprehensive wealth management, phone trading, financial malls, etc.), especially logs with a variety of error messages.

Logs with relatively good effectiveness:

Database, middleware, operating system logs.