日志监控

产品文档

文档目录

产品简介
产品概述
什么是日志监控?

最近更新时间: 2023-02-13 10:54:18

日志监控（LogMon）（以下简称日志监控或LogMon）是一站式的日志数据管理工具，它配置简单、功能强大、容易使用同时集日志收集、数据分析以及数据视图化功能，帮助用户提升运维、运营效率，快速查找和定位问题，广泛应用于在线业务状态实时监控、 业务异常原因定位、业务日志数据统计分析、及安全与合规审计等场景。

相关概念

最近更新时间: 2023-02-13 10:54:17

了解LogMon时，通常会涉及到以下概念：

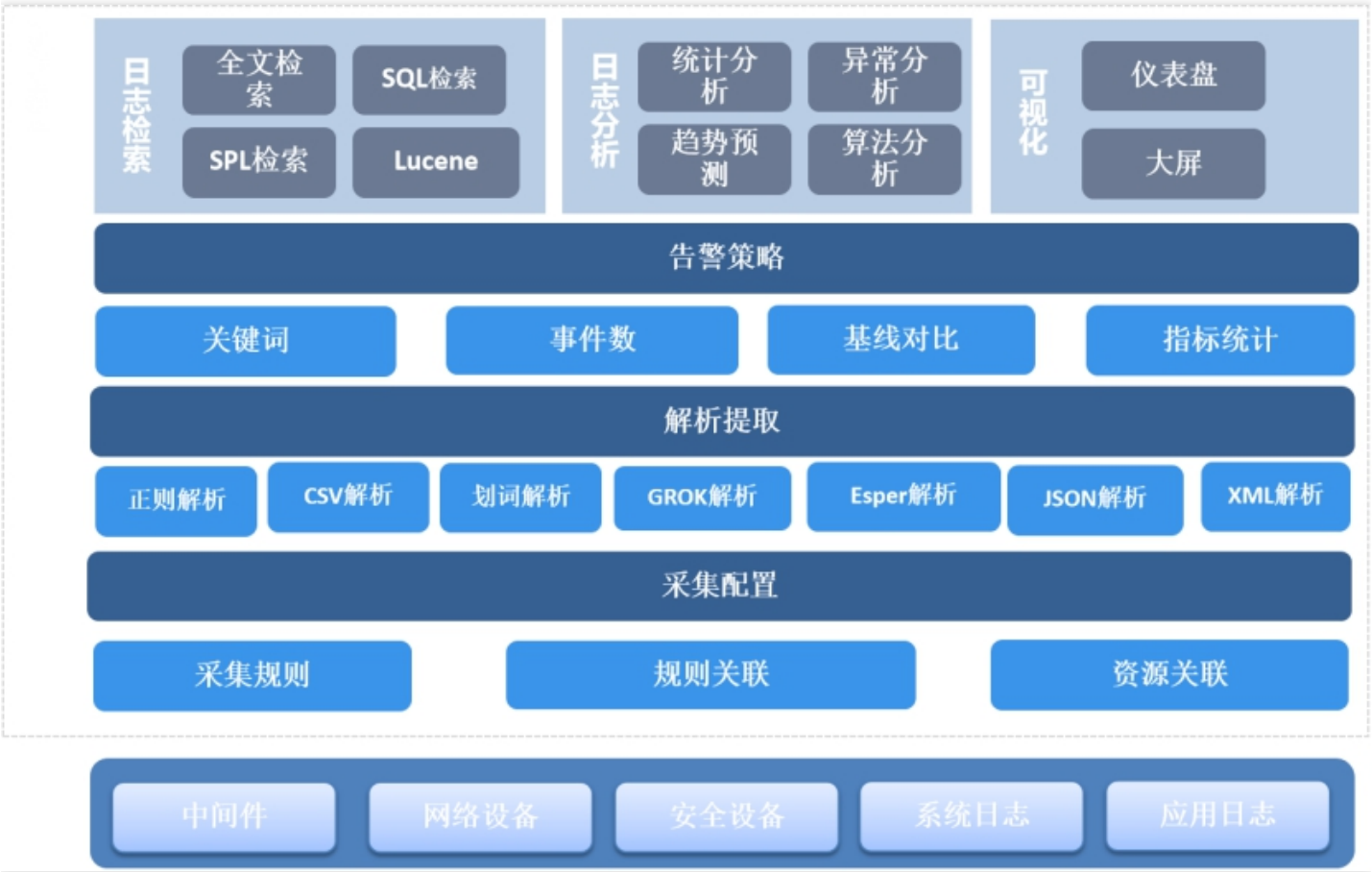
缩略语/术语	说 明
字段	日志索引后会产生公共字段，匹配解析规则后会产生私有字段，可以通过公共字段和私有字段进行逻辑运算查询
业务应用	采集的日志所属的业务应用，例如部署的nginx服务的应用是CMDB，那业务应用即为CMDB
日志采集路径	待采集的日志文件的路径，同一种应用，可能存在多个日志格式日志文件，每个日志格式对应1个采集路径，例如nginx有访问日志，err日志
应用标签	标签是针对每种日志文件的一个扩展说明，通过标签可以将属于同一个资源类型的不同日志分开，例如nginx日志，分别给访问日志LogMon中使用应用标签每个解析规则都需关联一个应用标签（应用标签详见标签管理），应用标签与采集规则中的应用标签相对应。采集到的日志会根据应用标签，自动找到解析规则对日志原文进行结构化解析。
日志格式	单行日志：采集的日志文件中，如果您希望每一行日志在界面中都显示为一条单独的日志数据，则选择单行日志。 多行日志：采集的日志中包含像java异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志则每一行都显示为一条单独的日志数据，则选择多行日志，方便您查看日志并且定位问题。
日志时间	系统时间：表示系统当前时间，默认为日志采集时间 时间格式：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志每条日志的行首显示日志的打印时间。 日志中不含打印时间时，时间解析方式依次顺序：时间格式>默认解析格式>系统时间 如果日志中的时间格式为：2019-01-01 23:59:59，时间格式应该填写为：YYYY-MM-DD hh:mm:ss。 如果日志中的时间格式为：19-1-1 23:59:59，时间格式符应该填写为：YY-M-D hh:mm:ss。
日志格式	日志格式选择多行日志时，需要以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。
过滤	过滤器将会按照您输入的过滤关键词在该日志主题下执行过滤和累加关键词的动作。

关键词	仅支持过滤单个字词，例如Error、Warning或者Fail to root等，不支持过滤组合后的字词，日志服务的过滤方式是精确匹配，且区分大小写，数字及特殊符号需用双引号包含起来。
采集状态	表示依据配置的采集规则，关联主机在此规则下对日志的采集情况。
Base路径	base路径的设计初衷是一般的业务应用，中间件都有专门的日志目录，日志存储在一个目录下，但在不同项目中不同机器上安装路径不一样，这样使用base路径之后，可以通过修改base路径进行统一修改操作。

产品逻辑架构

最近更新时间: 2023-02-13 10:38:45

LogMon提供强大的日志检索和日志分析功能，支持对保存的日志进行全文检索、SQL检索、SPL检索、Lucenue语法检索等多种方式进行检索查询，支持对日志的统计分析、异常分析等功能，帮助用户快速定位问题，多角度分析，及时发现问题进行预防和避免。对于像中间件、网络设备、安全设备、系统与应用产生的日志，通过配置对应的采集规则，实现对设备中对应路径的日志数据采集。采集数据根据用户配置的解析规则进行解析提取，解析规则支持正则、csv解析、划词解析、GROK解析、Esper解析、json解析、XML解析等多种解析方式。同时通过用户自定义配置的告警策略对日志信息进行实时监控。



产品特色

日志采集与分析

最近更新时间: 2023-02-13 10:58:11

主机和云服务的日志数据，不方便查阅并且会定期清空，日志监控采集日志后，日志数据可以在日志监控以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

数据可视化

最近更新时间: 2023-02-13 10:58:11

强大的日志检索功能；提供快速图表、仪表盘、大屏等丰富的多视角日志数据呈现、帮助用户实现运维日志数据可视化。

快速故障定位

最近更新时间: 2023-02-13 10:58:11

支持日志异常事件监测定位告警、监测策略丰富多样，支持应用日志的链路分析、关联分析等；通过日志对故障进行溯源，提升运维效率。

快速入门
日志搜索
搜索栏查询
搜索栏查询

最近更新时间: 2023-02-15 13:46:57

在日志搜索页面，点击上方的搜索栏，输入日志关键字或者字段查询语句（支持lucene语法查询），可以对当前已经采集到系统的日志进行查询。

查询语法

最近更新时间: 2023-02-15 13:46:57

日志分析LogMon支持全文检索和字段查询。全文检索包含：（1）关键字查询。例如：输入 get，匹配所有与get相关的日志，不区分大小写；（2）短语查询。使用双引号包裹需要查询的短语，例如：“Windows NT”；（3）模糊查询。在词的中间或者末尾加上模糊查询关键字，即*(零次多次)和?(零次一次),返回匹配的日志。查询时必须指定前缀，即* 和?不能出现在词的开头。指定的词越精确，查询结果越精确。字段查询中，字段说明：日志索引后会产生公共字段，匹配解析规则后会产生私有字段，可以通过公共字段和私有字段进行逻辑运算查询。运算符，如下所示：

名称	语义
AND	query1 AND query2，查询交集
OR	query1 OR query2，查询并集
NOT	query1 AND NOT query2，表示符合 query1，不符合 query2的结果，如 NOT status:200 不包含 status 值为 200 的数据
( )	把一个或多个query合并成一个query，提升优先级，如 ip:(a OR b) 查询 ip 字段为 a 或者 b 的数据
[ ]	区间查询，包括边界，如 status:[400 TO 500] 查询 status 字段在 400 到 500 区间内的数据
:	用于 key-value 对的查询。term1:term2构成一个 key-value 对。如果 key 或者 value 内有空格（）、冒号（:）等保留字符，需要用双引号””把整个 key 或者 value 包裹起来
\	转义字符，如正则表达式搜索时表达式包含反斜杠的情况，如 request_path:/\/query\/abc\/.*/ 查询 request_path 字段匹配正则表达式 /path/abc/.*的数据
>,=, <,≥,≤	区间查询，如 status:>=500 查询 status 大于 500 的数据

搜索栏自动联想

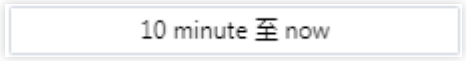
最近更新时间: 2023-02-15 13:46:57

日志分析会根据用户输入的信息自动进行内容联想，如下图所示：

输入信息联想功能，支持中文输入、解析规则字段、公共字段。

快速时间选择

最近更新时间: 2023-02-15 13:46:57



点击 按钮，展开时间选择控件，如下图所示：

在【最近】栏内，输入并选择时间及单位，点击 按钮用选择时间进行查询。

例如：3 分

在【快速选择】栏内，点击已列出的快速查询时间按钮，可以立即进行搜索。

在【精确选择时间】栏内，可以精确选择开始时间及结束时间，点击 按钮用选择时间进行查询。

常用搜索

最近更新时间: 2023-02-15 11:30:10

当您需要重复使用某些搜索条件搜索日志时，可以将其保存为常用搜索语句。

点击 按钮，会出现下拉菜单，选择【保存搜索】选项。

保存的常用搜索语句中搜索条件包括：关键字、字段查询语句、主机名称/IP、日志路径、业务系统、应用标签。

当需要使用已保存的常用搜索语句时，点击 按钮，再点击【我的搜索】，再在【我的常用搜索】选择常用搜索语

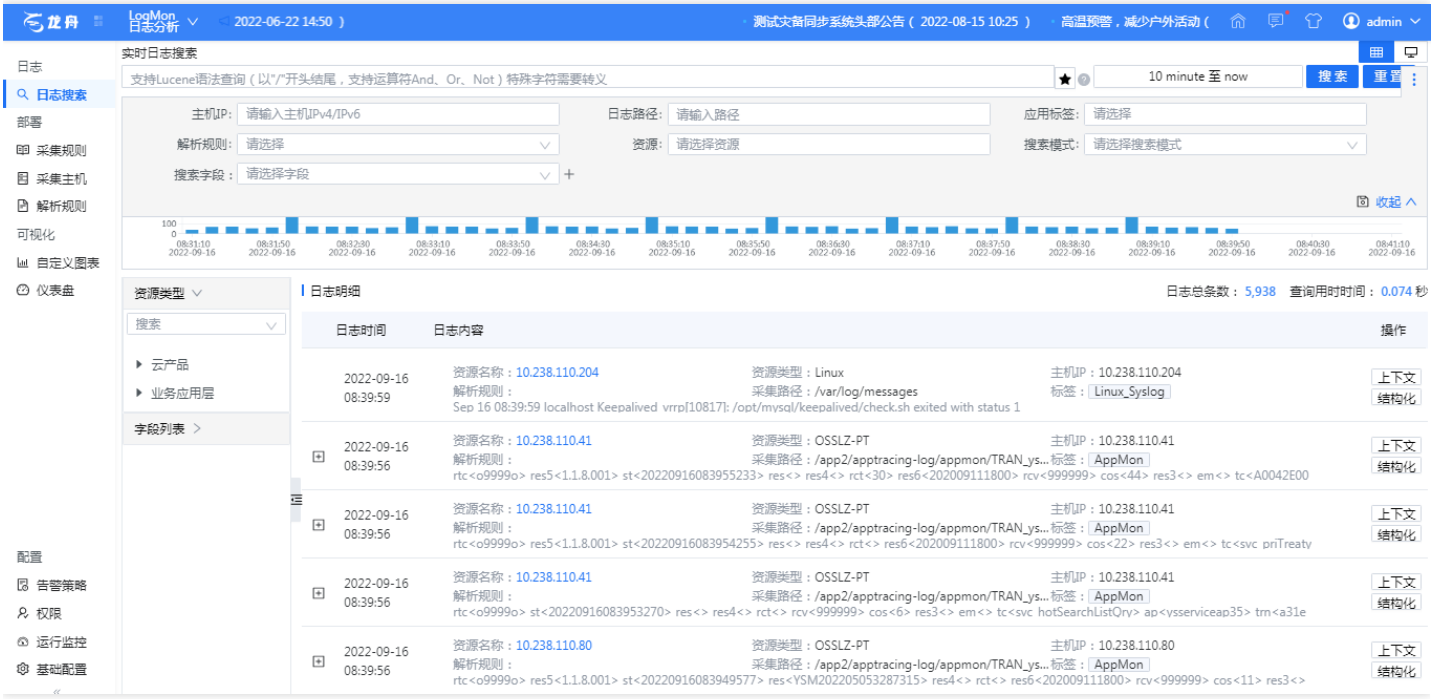
句，可将已保存的常用搜索语句中的条件带入查询栏并进行查询。

在我的常用搜索中，可对已保存的常用搜索进行【编辑名称】和【删除】的操作。

高级搜索

最近更新时间: 2023-02-15 11:30:10

点击 按钮，会出现下拉菜单。在下拉菜单中选择【高级搜索】，展开更多查询条件，配合输入的关键字/搜索语句及时间进行更精确的日志搜索，如下图所示：



保存告警

最近更新时间: 2023-02-15 11:30:10

可将搜索条件保存为告警策略，其中搜索条件包括搜索栏及高级搜索条件。点击 按钮，在下拉菜单中选择【保存告警】选项。可跳转到告警策略配置页面，进行告警策略的配置。

导出

最近更新时间: 2023-02-15 11:30:10

当需要将一定查询条件下所得的结果导出，可以点击 按钮，在下拉菜单中选择【导出】选项。

输入需要导出的日志条数，及导出文件名称，点击 按钮，即可以文件的形式导出。

搜索结果

最近更新时间: 2023-02-15 11:30:09

搜索结果是搜索之后的结果展示。主要包含三个模块：日志分布直方图、日志明细，字段导航栏。如下图所示：

左侧区域字段导航栏，将结构化的字段进行了聚合展示，分为公共字段、解析规则字段。 右侧区域日志明细，展示当前查询结果，也就是当前查询条件命中的日志。

公共字段含义：

字段名称	含义
agentIp	主机IP
agentName	主机名称
agSourceOs	操作系统
agSourceOsArch	操作系统架构
agSourceOsVersion	操作系统版本
spLoglevel	日志级别
agPath	日志路径
spParseRule	解析规则Code

spParseTag	解析规则标签
agCollectType	采集器类型
agSourceTags	采集规则标签

字段列表

字段列表

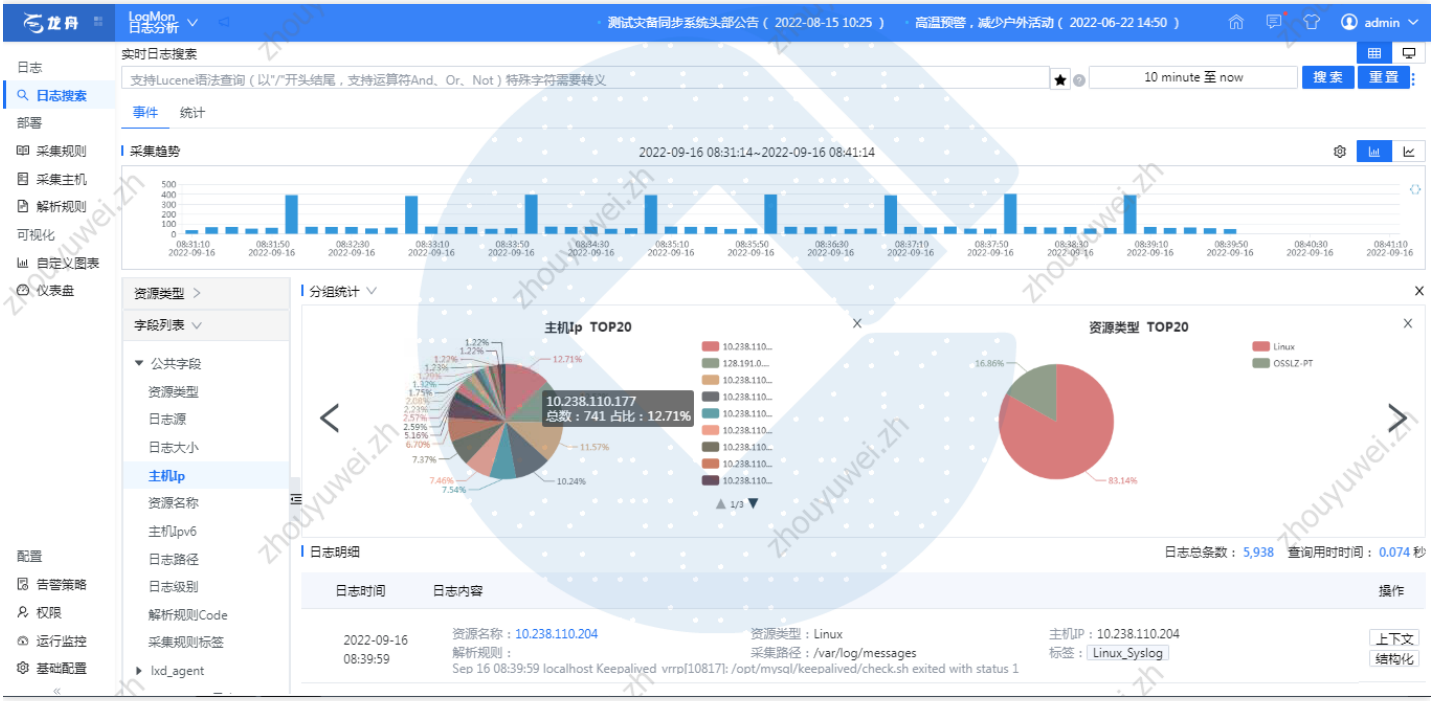
最近更新时间: 2023-02-15 13:46:57

点击字段导航栏中某一字段名称，出现浮动框。如下图所示：

分组统计

最近更新时间: 2023-02-15 13:46:57

点击【分组统计】按钮， 可以查看该字段所有值的分布情况。



趋势分析

最近更新时间: 2023-02-15 13:46:57

点击【趋势分析】按钮， 可以查看该字段所有值在各时间段的分布情况。

加入搜索

最近更新时间: 2023-02-15 13:46:57

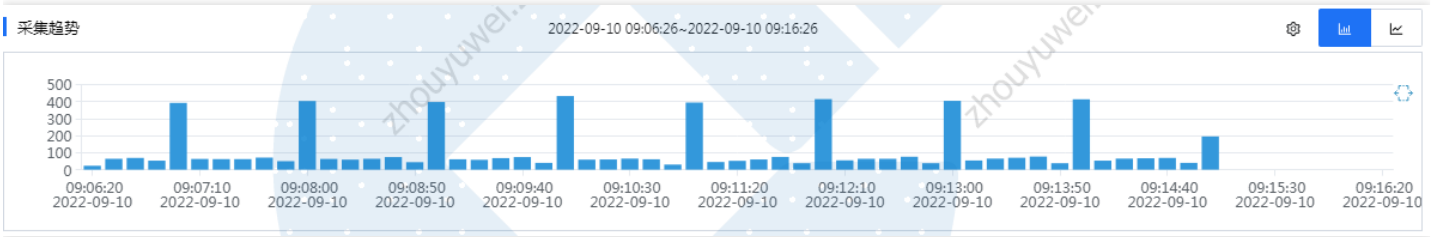
点击【加入搜索】按钮， 可将字段加入到搜索栏的查询语句中。

日志分布直方图

日志分布直方图

最近更新时间: 2023-02-15 13:52:08

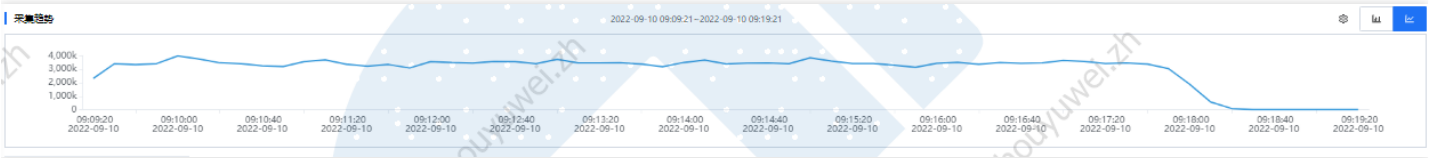
日志分布直方图主要展示查询到的日志在时间上的分布，将鼠标指向数据块，可查看该数据代表的时间范围和日志命中次数。如下图所示：



折线图切换

最近更新时间: 2023-02-15 13:52:08

点击 按钮，可以进行柱状图与折线图的切换，如下图所示：



滑动钻取

最近更新时间: 2023-02-15 13:52:08

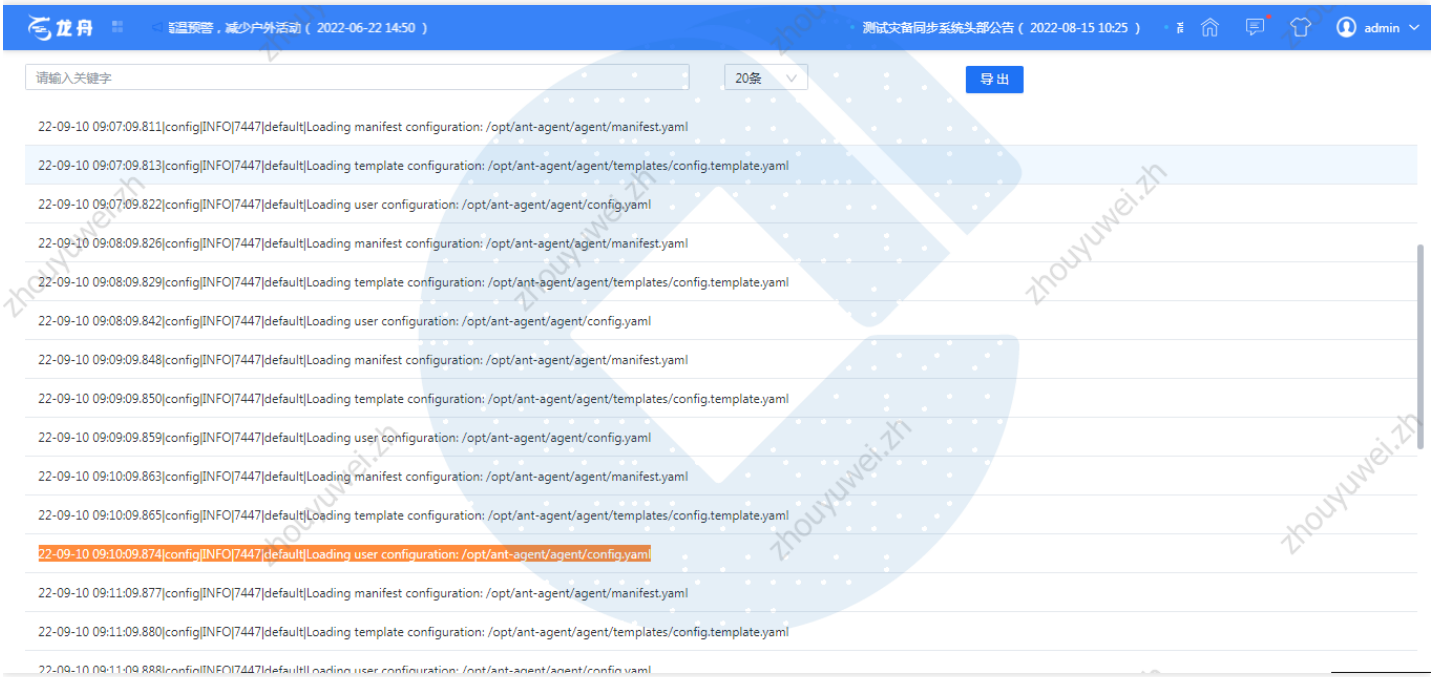
框选数据块，可以查看更细时间粒度的日志分布，同时日志明细列表中也会同步展示下钻后的日志查询结果。查询开始时间、结束时间时间分别取框选区域中第一根柱子和最后一根柱子的时间范围。

上下文

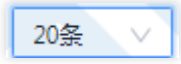
上下文

最近更新时间: 2023-02-15 14:18:13

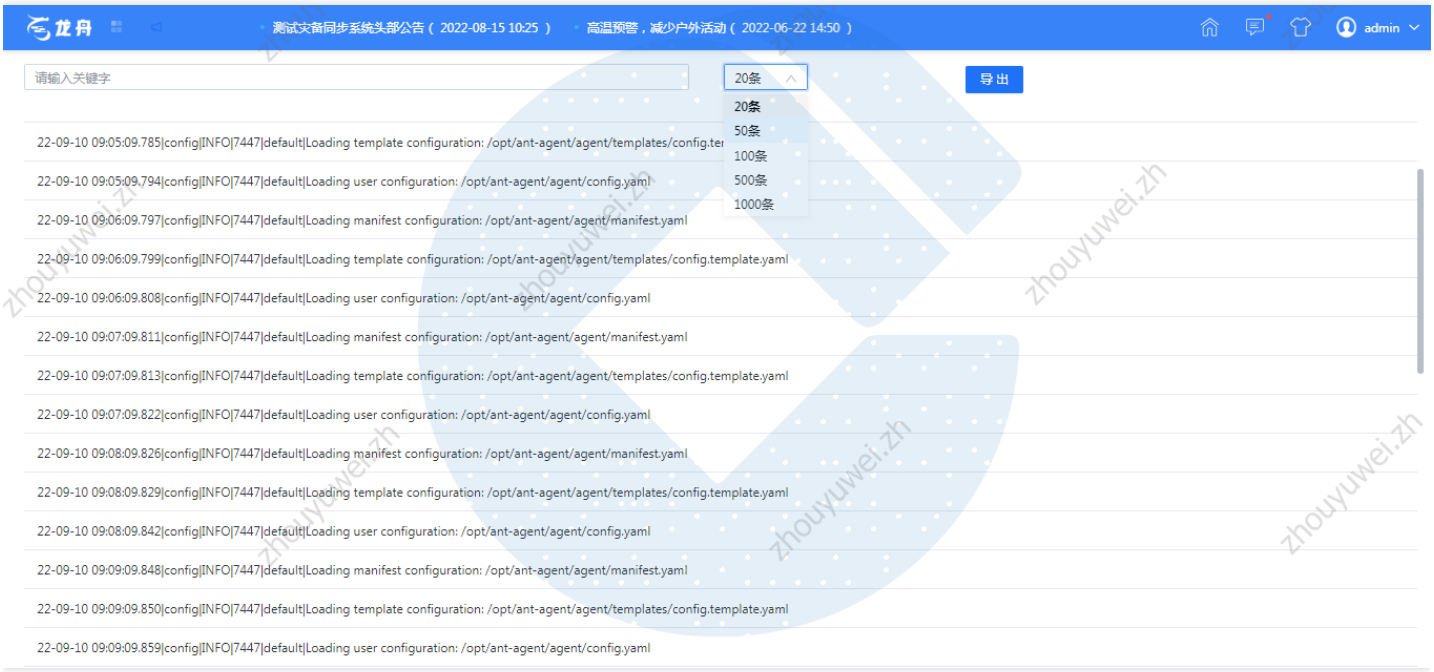
在日志明细列表中，点击操作列下的【上下文】按钮，从新开页面查看指定日志的上下文信息，可通过关键字进行日志上下文检索。



在查看日志上下文中，可通过关键字查询，查询目标日志为基线，含关键字的上下50条（默认）日志内容。



可按需点击 选择需要展示上下文的条数。

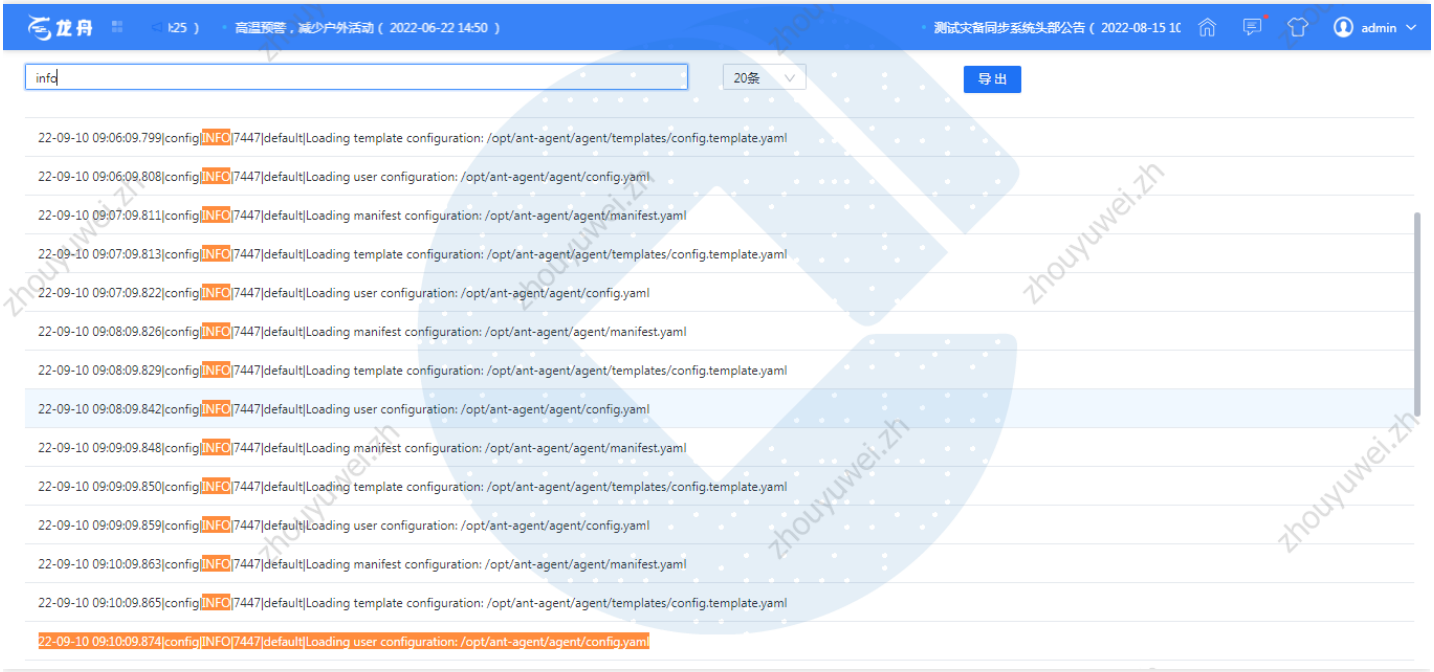


向上滚动至顶部，可向上加载更多；向下滚动至底部，可向下加载更多。

上下文关键字检索

最近更新时间: 2023-02-15 14:18:13

在上下文页面，点击上方的搜索栏，输入关键字，可以对当前所选日志的上下文信息进行查询。



导出

最近更新时间: 2023-02-15 14:18:12

当需要导出该日志的上下文信息时，点击 按钮，即可导出当前页面显示的所有上下文信息。

结构化

最近更新时间: 2023-02-15 14:24:39

在日志明细列表中，点击操作列下的【结构化】按钮，从右侧滑出抽屉查看按字段索引结构化后的日志内容。

公共字段

最近更新时间: 2023-02-15 14:24:39

结构化内默认展示公共字段，可查看当前日志公共字段对应字段名称和字段值。

结构化字段

最近更新时间: 2023-02-15 14:24:39

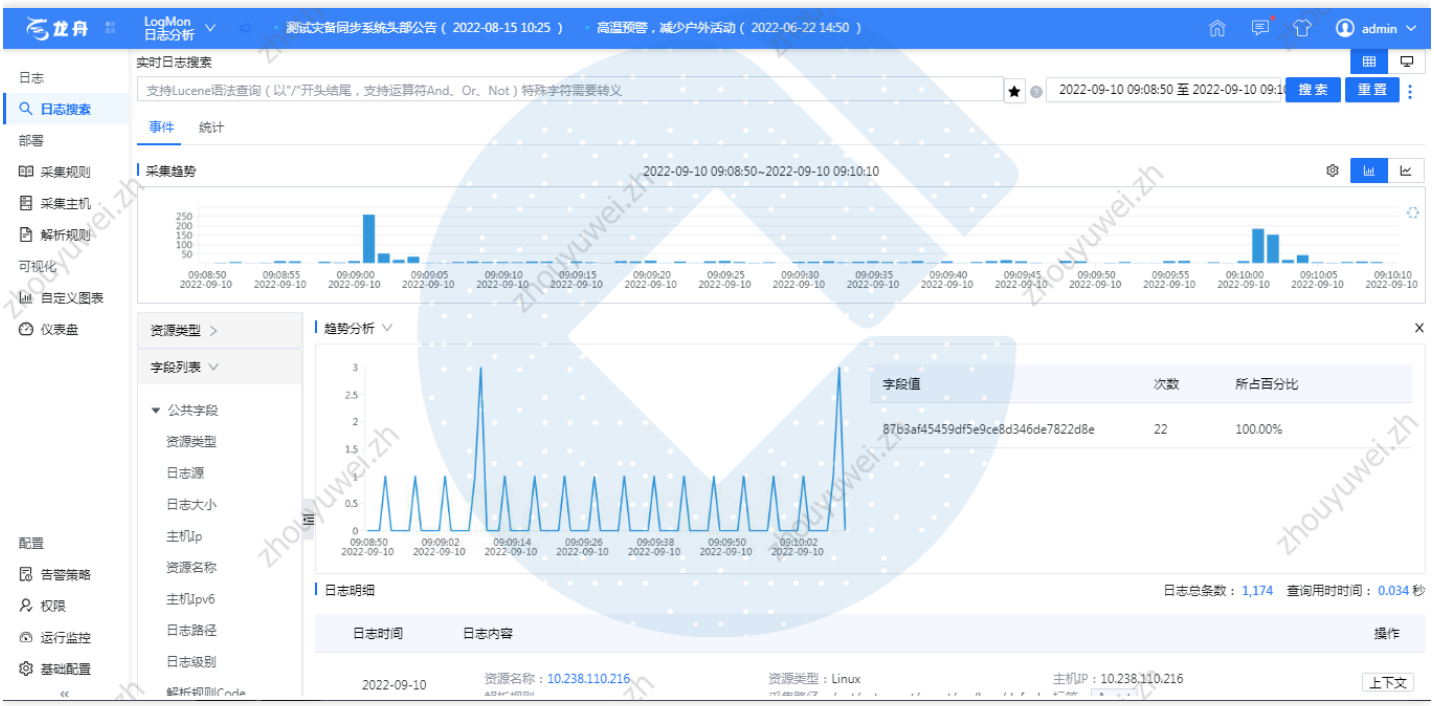
点击【结构化字段】，可查看当前日志被解析规则提取解析结构化后的字段和值。

趋势分析

最近更新时间: 2023-02-15 14:24:39

点击字段对应值，会出现悬浮框，如图所示：

点击【趋势分析】，可以查看该字段所有值在各时间段的分布情况 。



加入搜索

最近更新时间: 2023-02-15 14:24:39

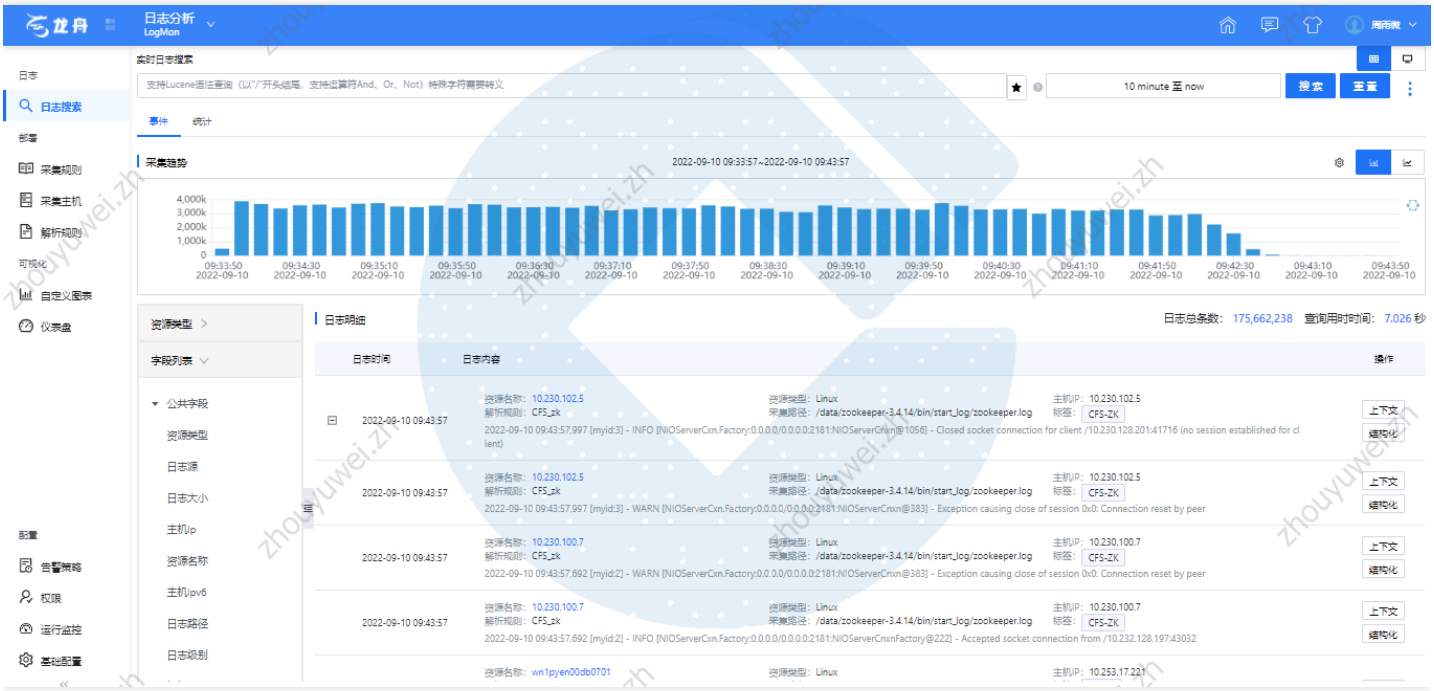
点击【加入搜索】， 可将字段值加入到搜索栏的查询语句中。

日志明细

多行展开

最近更新时间: 2023-02-15 14:07:31

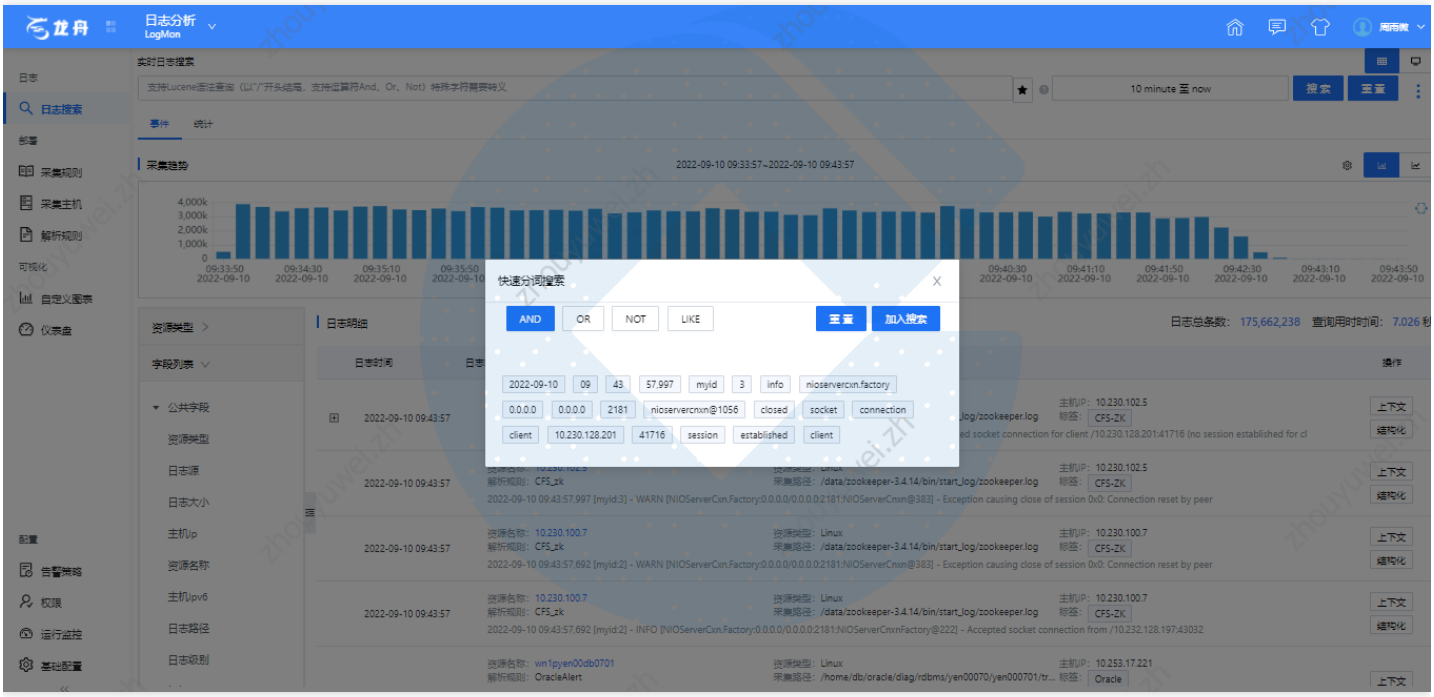
当日志内容多于一行时，为进行折叠，点击 ⊞ 按钮可将其展开查看完整内容，如图：



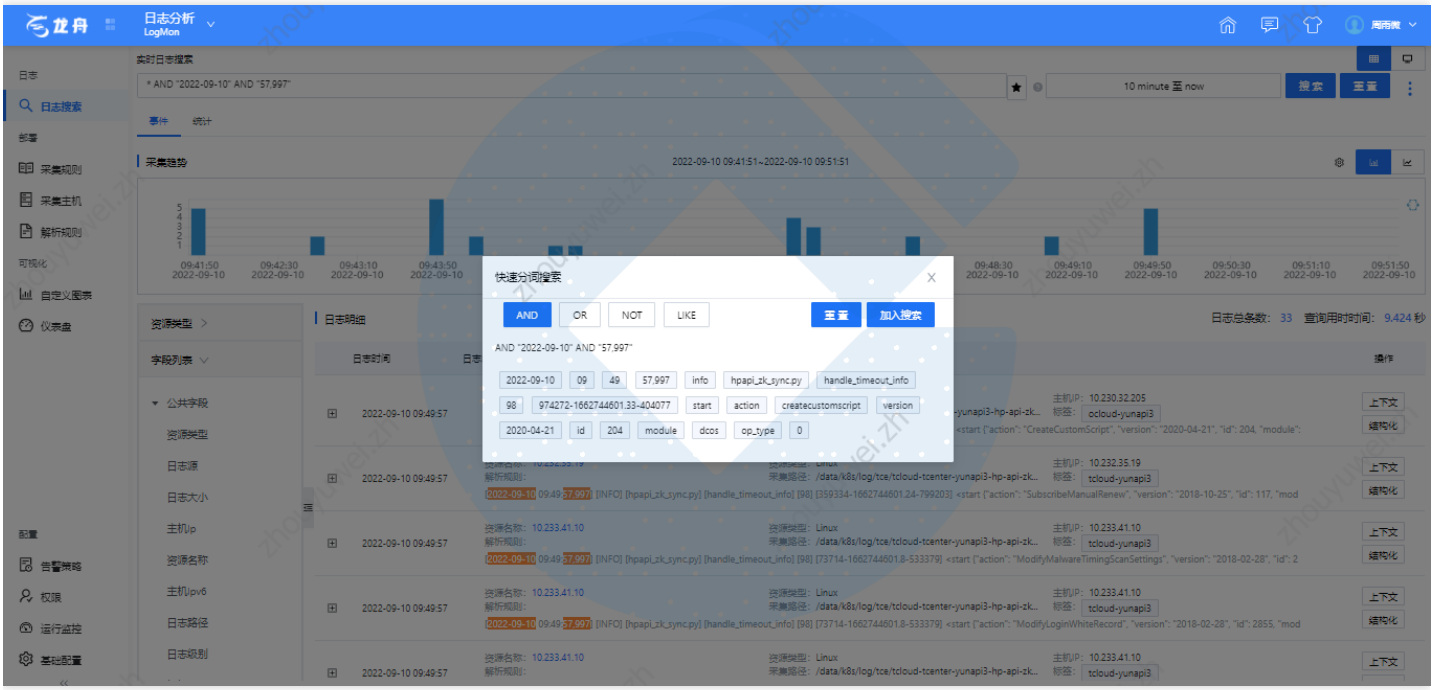
日志原文分词快速检索

最近更新时间: 2023-02-15 14:09:59

在日志内容中，双击某一条日志原文，日志分析会将该日志原文切分为多个分词，并将分词结果进行展示，如下图所示：



可以选中任意一个或者多个分词结果，结合【AND】、【OR】、【NOT】、【LIKE】等条件进行组合全文检索，完成后点击 加入搜索 将语句加入搜索条件。


日志分析
LogMon
实时日志搜索
* AND "2022-09-10" AND "57.997"
10 minute 至 now
搜索
重置
事件
统计
采集趋势
2022-09-10 09:41:51~2022-09-10 09:51:51
日志明细
日志总条数：33
查询用时时间：9.424 秒
快速分词搜索
AND
OR
NOT
LIKE
重置
加入搜索
AND "2022-09-10" AND "57.997"
2022-09-10
09
49
57.997
info
hpapi_zk_sync.py
handle_timeout_info
98
974272-1662744601.33-404077
start
action
createcustomscript
version
2020-04-21
id
204
module
dcos
op_type
0

关键字高亮

最近更新时间: 2023-02-15 14:09:59

输入搜索条件后进行查询，查询语句内对应关键字会高亮显示高亮，如图：

采集规则

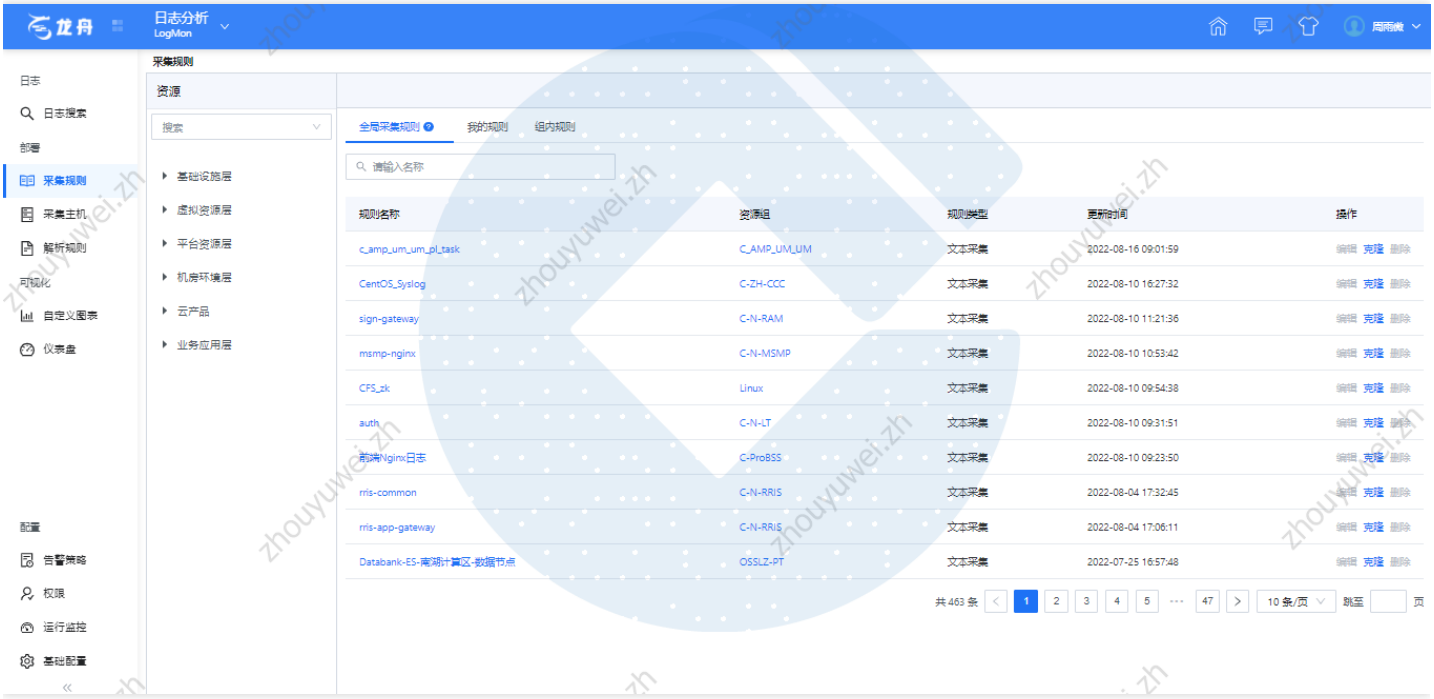
采集规则

最近更新时间: 2023-02-13 13:52:32

采集规则配置界面按照采集规则类型区分，包含全局采集规则、我的规则与组内规则，各条规则均可以被查看。每条采集规则可关联多台采集主机（注:需采集规则和主机类型操作系统一致）。

采集规则类型	含义	查看	编辑	克隆	删除
全局采集规则	历史版本内置采集规则	√		√	
我的规则	用户创建的采集规则	√	√	√	√
组内规则	组内共享规则	√		√	

【采集规则】页面，如下图所示：



搜索规则

最近更新时间: 2023-02-13 13:52:32

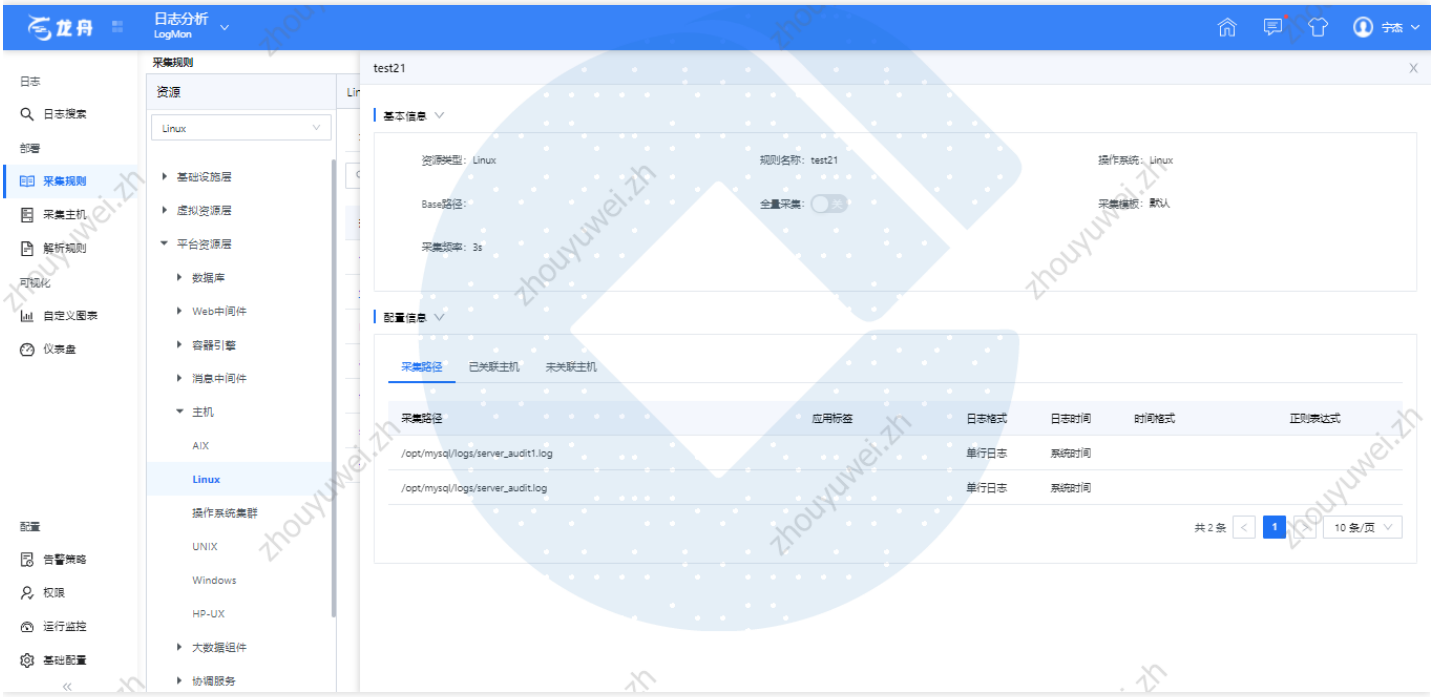
资源类型为默认的搜索条件，选择相应的资源类型，立即执行搜索资源类型下的采集规则，再选择采集规则类型，输入关键词后，进行搜索，如下图所示。

查看规则

最近更新时间: 2023-02-13 13:52:32

在【采集规则】页面，选择查看的规则类型，如【我的规则】，再点击【规则名称】字段值的链接，如test21，如图：

进入采集规则查看页面，如下图所示：


龙舟
日志分析
LogMon
采集规则
日志
日志搜索
部署
采集规则
采集主机
解析规则
可视化
自定义图表
仪表盘
配置
告警策略
权限
运行监控
基础配置
资源
Linux
基础设施层
虚拟资源层
平台资源层
数据库
Web中间件
容器引擎
消息中间件
主机
AIX
Linux
操作系统集群
UNIX
Windows
HP-UX
大数据组件
协调服务
test21
基本信息
资源类型：Linux
规则名称：test21
操作系统：Linux
Base路径：
全量采集：
采集模板：默认
采集频率：3s
配置信息
采集路径
已关联主机
未关联主机
采集路径
应用标签
日志格式
日志时间
时间格式
正则表达式
/opt/mysql/logs/server_audit1.log
单行日志
系统时间
/opt/mysql/logs/server_audit.log
单行日志
系统时间
共 2 条
1
10 条/页

编辑规则

最近更新时间: 2023-02-13 13:52:32

根据实际情况，修改对应的规则名称、Base路径、采集路径信息。确认无误后，点击【保存】钮即可。

克隆规则

最近更新时间: 2023-02-13 13:52:32

点击【克隆】按钮，将进入采集规则克隆页面（只克隆采集规则下采集路径信息），规则名称自动在原来值基础上加_copy,如下图所示：

删除规则

最近更新时间: 2023-02-13 13:52:32

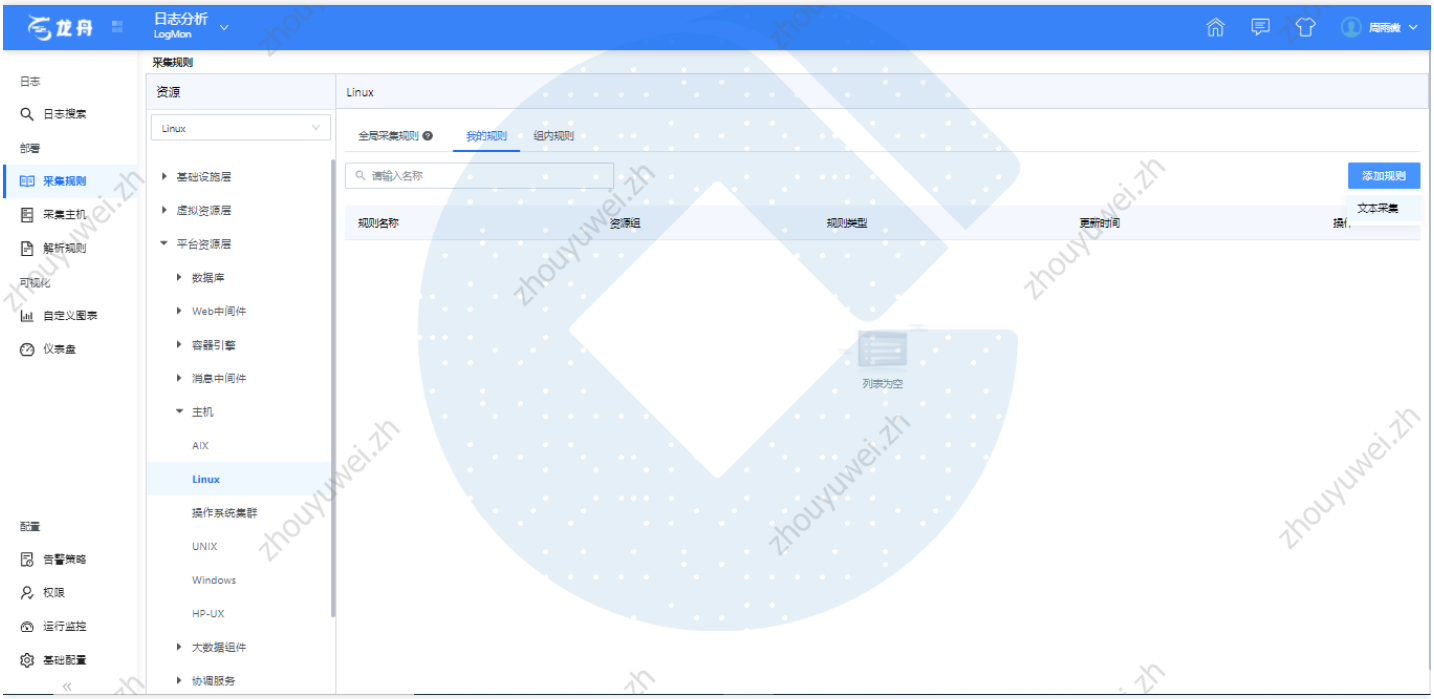
点击【删除】按钮，弹出提示确认是否删除。可根据实际情况变化删除已有的采集规则配置。已关联采集主机的采集规则在进行删除操作前，需先解除关联全部的采集主机。

新增规则

添加规则

最近更新时间: 2023-02-13 15:07:00

在【我的规则】页面下，先选择【资源类型】，如Linux；再点击【添加规则】，再选择【文本采集】可进行采集规则的创建，如下图所示。

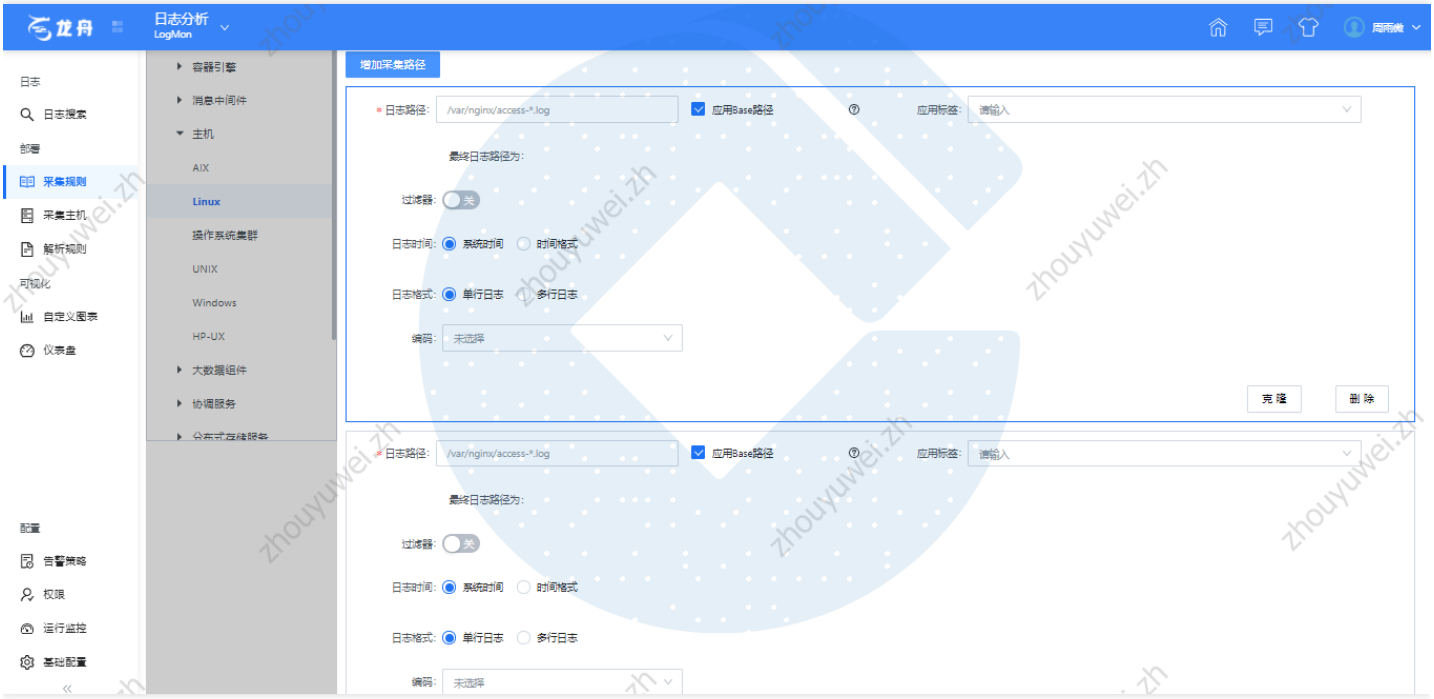


如下图，根据实际情况，填写日志路径、应用标签、过滤器、日志时间、日志格式，确认无误后，进行后续操作。

名称	描述	是否必填
规则名称	定义采集规则名称	是
操作系统	根据采集主机类型选择对应的操作系统	是
Base路径	公共采集路径，多条采集路径可以共用同一个Base路径	否
全量采集开关	是否对历史日志数据进行采集，关闭表示从当前时间开始采集，开启表示会对路径下历史日志进行采集。	否
资源类型	默认为linux，暂不需要修改	是
采集模板	标准的采集批准，暂不需要修改	否
采集频率	采集日志的周期频率	是

日志路径	采集日志的具体路径	是
应用标签	自定义标签，可在基础配置的标签配置中新增标签进行关联	否
过滤器	可以选择【采集】【不采集】根据字符串或者正则过滤掉采集或者不采集的日志信息	否
日志时间	“时间格式”需要选择或者手动输入将要采集日志的时间格式，系统会自动根据此时间格式解析当作日志的原始时间，如选择的是“系统时间”，系统将采集的时间作为日志时间	是
日志格式	可定义单行采集或多行采集	是

当采集路径有多个路径时，需要点击【增加采集路径】按钮，可以新增一条采集路径信息栏，如下图所示：



克隆采集路径

最近更新时间: 2023-02-13 15:07:00

克隆

选择需要克隆的目标采集路径，点击目标采集路径信息块中 按钮，将采集路径信息栏复制新增一条，如下图所示：

根据实际情况，修改日志路径、应用标签、过滤器、日志时间、日志格式，确认无误后，进行后续操作。

配置采集路径最小颗粒为文件（不支持文件夹）。

删除采集路径

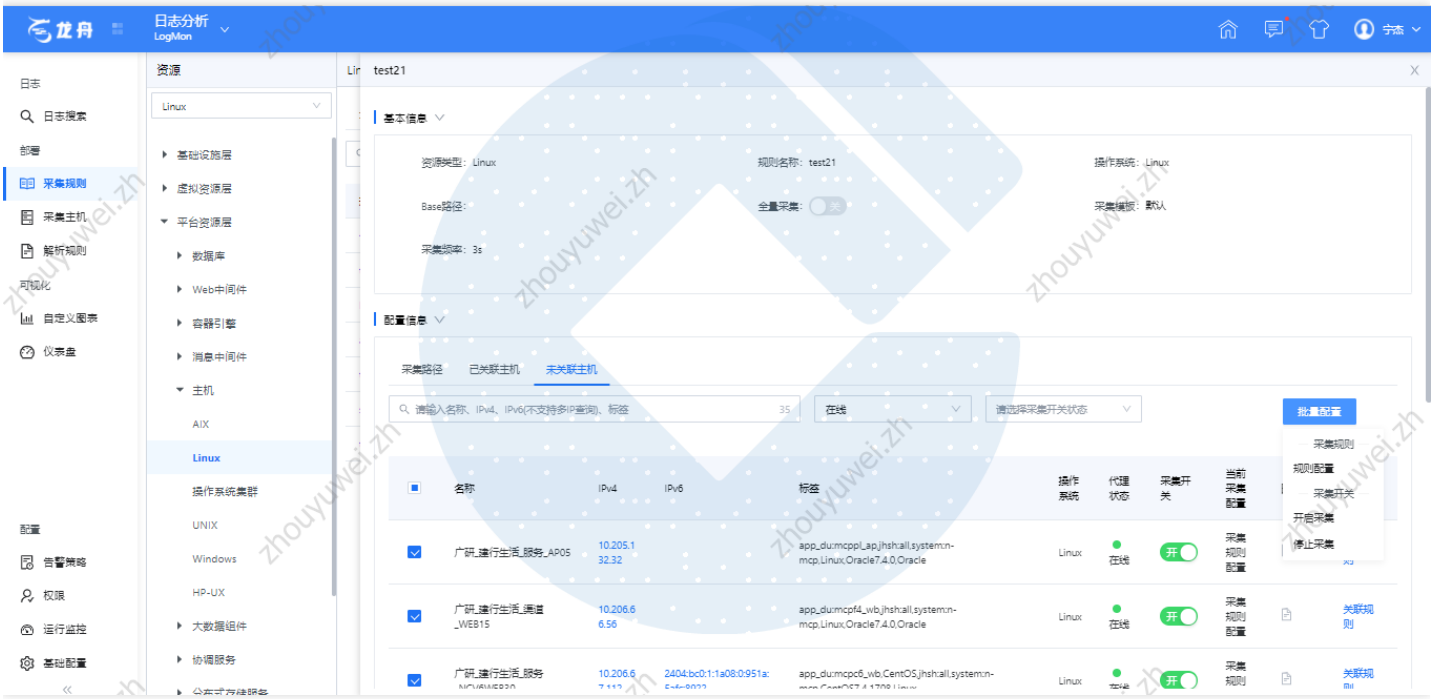
最近更新时间: 2023-02-13 15:07:00

可根据实际情况，点击采集路径信息栏中 按钮，删除已有的采集路径 。

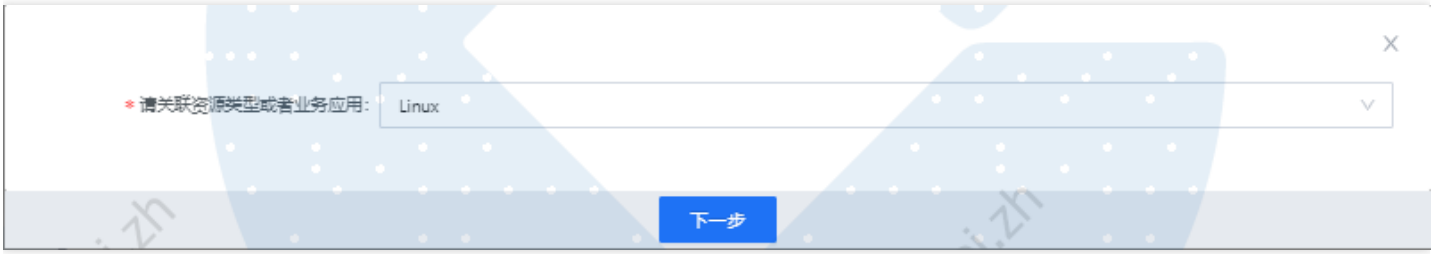
规则关联
批量关联主机

最近更新时间: 2023-02-13 15:07:00

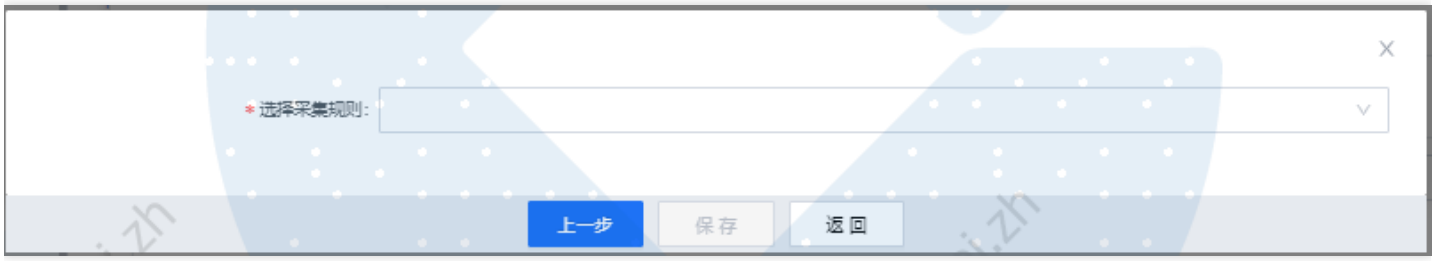
成功添加采集规则后，可为采集规则关联同一类操作系统主机。点击【未关联主机】按钮，进入未关联采集主机界面。如下图所示：



【批量配置】中，可以选择批量开始或关闭采集；还可以点击【规则配置】进行批量关联，将弹出 请关联资源类型或者业务应用 界面，选择好后，点击【下一步】。



之后将弹出 选择采集规则界面，选择对应的采集规则后，点击【保存】。



即可实现采集规则的批量关联，关联成功后采集主机会显示在已关联主机中：点击【已关联主机】关联主机页面，显示该采集规则已关联的采集主机。

单一主机关联

最近更新时间: 2023-02-13 15:07:00

在【未关联主机】页面中，点击一台主机的【关联主机】按钮，点击【确定】。

解除关联单一主机

最近更新时间: 2023-02-13 15:07:00

点击【已关联主机】切换至关联主机页面，显示该采集规则已关联的采集主机。在【已关联主机】页面中，点击一台主机的【解除关联】按钮，会弹出解除关联二次确认框，点击【确定】按钮解除关联。

批量解除关联主机

最近更新时间: 2023-02-13 15:07:00

在【已关联主机】页面中，批量选择一批待关联规则主机，点击【批量配置】按钮，再选择【批量解除】，会弹出解除关联二次确认框，点击【确定】按钮解除关联。

采集状态说明

最近更新时间: 2023-02-13 13:52:32

采集状态为三种，分别是未知、异常、正常。未知代表目前还在检测,尚未采集到数据入库；异常，代表当前规则条目应用异常，可能是采集路径不存在或接收数据端口异常等；正常代表规则条目正常采集到数据并且解析入库。

采集主机

搜索

最近更新时间: 2023-02-13 12:02:43

默认通过“主机主机名称/IP/标签”进行模糊匹配快速搜索，输入搜索条件，按ENTER回车键进行搜索。

规则配置

采集规则信息

最近更新时间: 2023-02-13 12:08:37

在采集主机页面中，点击某一主机后的“操作列的”规则配置 图标，选择对应的采集类别，打开显示已配置的采集规则信息，可展示当前采集规则的具体采集信息，点击【解除关联】将解除主机与当前规则的绑定，【解除关联】按钮变成【操作撤回】；点击【操作撤回】恢复到之前的状态,如图。

主机个性化配置

主机个性化配置

最近更新时间: 2023-02-13 12:08:37

主机个性化配置主要功能是对当前主机的采集规则做参数个性化调整，满足当前主机的采集需求。在采集主机页面

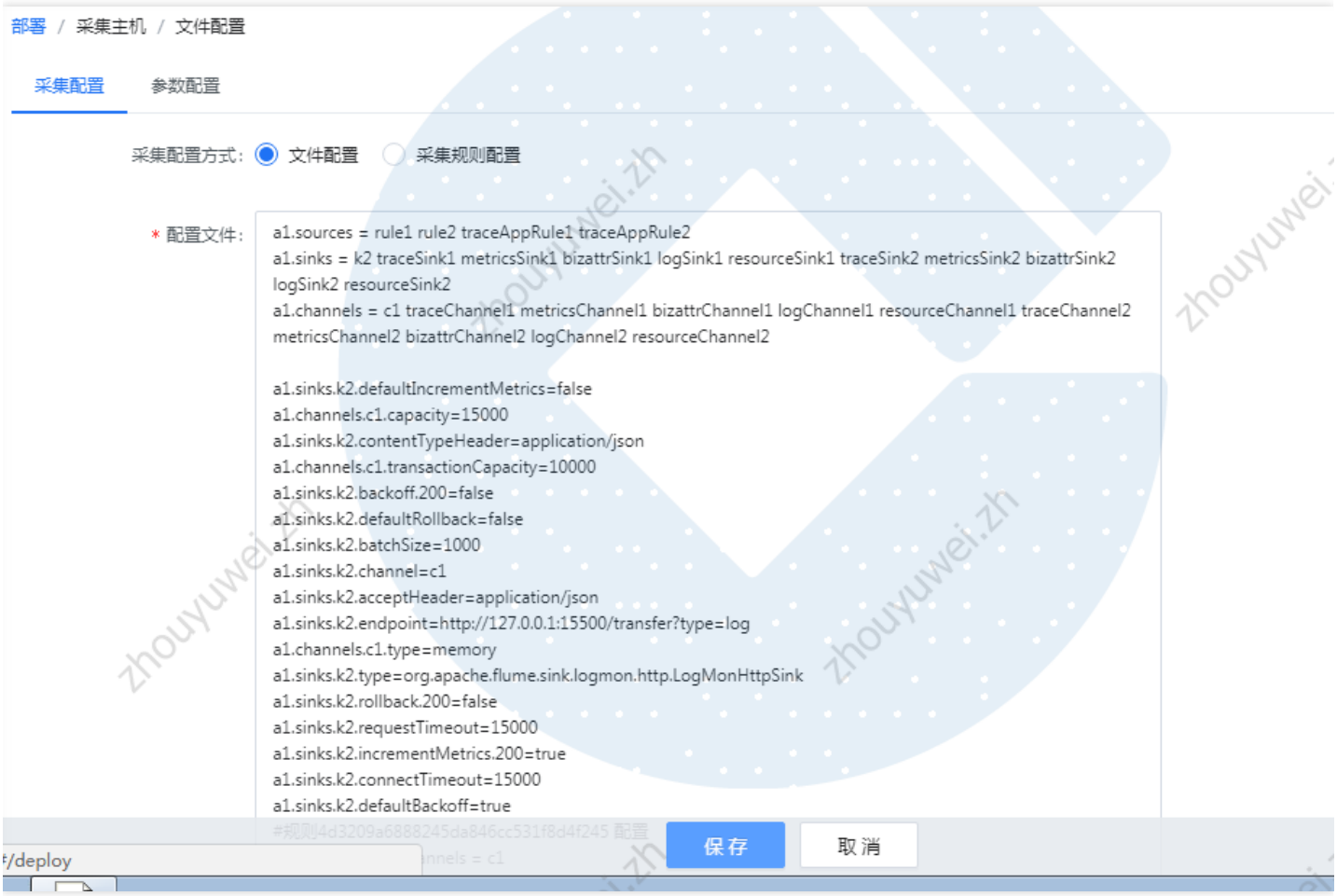
中，点击某一主机后的 配置图标，进入文件配置信息页面。

文件配置

最近更新时间: 2023-02-13 12:12:01

编辑

文件配置中初始数据来源于关联的采集规则配置文件。点击 按钮，可修改配置文件中的参数，根据实际情况修改，确认无误后，点击【保存】即可。

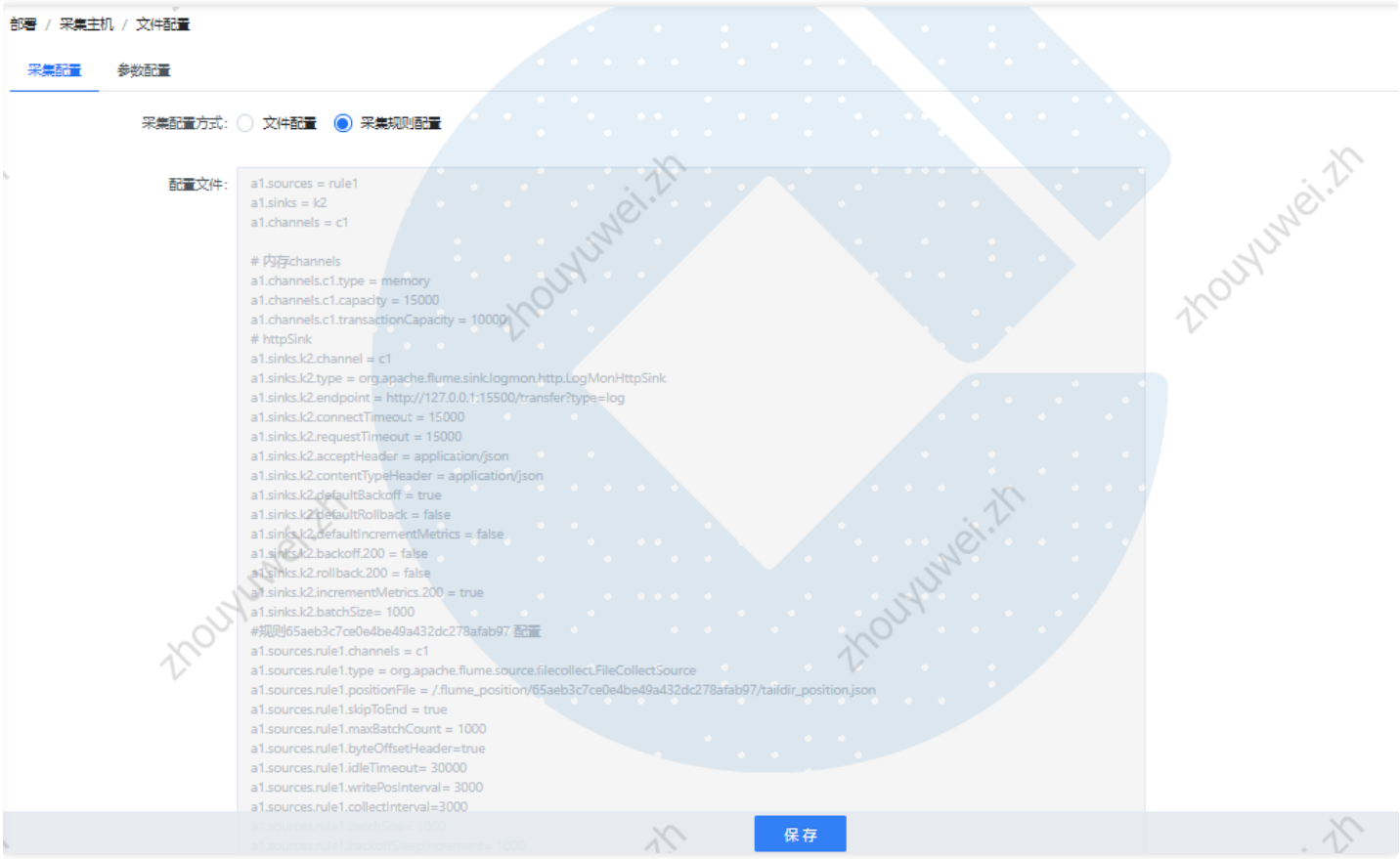


修改保存后的配置文件，默认为该采集主机日志采集的采集规则，调整后采集规则只应用当前主机有效，采集规则再次修改后不会对当前主机起任何作用。可通过修改采集配置优先级调整采集主机的日志采集规则。

采集规则配置

最近更新时间: 2023-02-13 12:12:01

采集规则配置文件只能查看，可通过修改采集配置优先级调整采集主机的日志采集规则，点击【采集规则配置】，点击【保存】，可以将当前主机的采集优先级调整回采集规则配置。



参数配置

最近更新时间: 2023-02-13 12:12:01

参数配置主要针对当前主机的进程JVM信息以及监控信息做调整，作用于文件配置、采集规则配置，点击【编辑】对相应的性能参数和监控参数做调整后，点击【保存】，服务器会重新按照新的参数下发采集代理进程，如下图所示.

解析规则
新增解析规则
新增解析规则

最近更新时间: 2023-02-13 11:46:18

添加规则

点击 按钮，出现下拉列表，选择需要的解析方式：如选择【正则解析】，新增解析规则，如下图所示：

根据实际情况填写解析规则基本信息编写、提取失败不存储开关说明：开关打开情况若提取规则一个都没有提取情况不保存当前日志、识别规则编辑/删除、提取规则编辑/删除，点击【测试】按钮，通过测试后点击【保存】即可。

每个解析规则都需关联一个应用标签（应用标签详见标签管理），应用标签与采集规则中的应用标签相对应。采集到的日志会根据应用标签，自动找到解析规则对日志原文进行结构化解析。

解析规则配置中识别规则、提取规则缺一或未通过测试的解析规则无法保存。

左侧区域上部，展示解析规则基本信息，依据实际情况填写解析规则名称、解析规则Code、应用标签、日志解析开关。

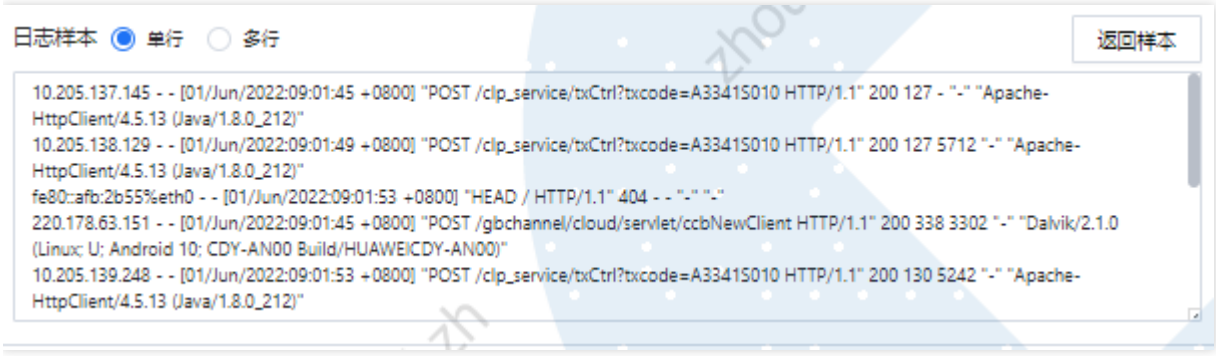
左侧区域下部，展示日志样本。有以下两种日志样本获取方式：

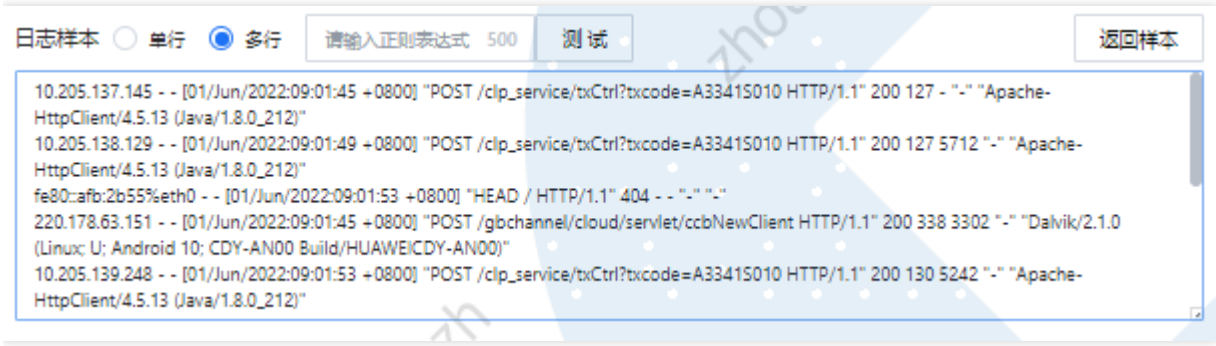
1）获取样本

通过应用标签、日志搜索关键字查询日志，点击【获取日志】按钮，获取查询条件范围内的日志内容。

2） 输入样本

点击【输入样本】按钮，进入文本编辑框，根据实际需求输入日志内容文本，日志分割可选择单行和多行，多行分割需要单独输入分割的正则表达式，确认无误后，点击【返回样本】按钮即可。





识别规则
新增识别规则

最近更新时间: 2023-02-13 12:00:42

在上图中，点击【识别规则】按钮，新增识别规则。

根据实际情况填写识别规则名称等，测试通过后点击保存即可。
主要采用正则表达式和关键字方式进行识别。正则表达式识别：通过输入的正则表达式匹配每一行日志样本，匹配通过的将日志样本目标行背景色标注。

编辑识别规则

最近更新时间: 2023-02-13 12:00:42

在识别规则列表信息区域，点击某一识别规则名称后【编辑】按钮，进入识别规则编辑页面。

根据实际情况，填写识别规则名称、解析表达式，确认无误后，点击【测试】，测试通过后，点击【确实】即可。

删除识别规则

最近更新时间: 2023-02-13 12:00:42

可根据实际情况变化删除解析规则下已有的识别规则。

提取规则

提取规则

最近更新时间: 2023-02-13 12:00:42

在新增解析规则，右侧区域下部，展示提取规则信息，如下图所示：

新增提取规则

最近更新时间: 2023-02-13 12:00:42

点击【提取规则】按钮，新增提取规则。

根据实际情况填写提取字段Code、字段名称、字段类型、提取规则，点击【测试，】测试通过后点击【确定】即可。

主要采用两种种方式进行识别，其中包含正则表达式，特征值。

1)正则表达式识别：用户通过自定义正则表达式，提取日志样本中的值；匹配通过的将日志样本目标行被提取的值深色背景标注

2)特征值识别：用户通过观察日志样本规律，当日志总是出现以XX开始和XXX结束的特征，可配置XXX为字段开始

特征，XXX未结束特征字段，匹配结果是将中间的值提取出来。匹配通过的将日志样本目标行被提取的值深色背景标注

编辑提取规则

最近更新时间: 2023-02-13 12:00:42

在提取规则信息区域，点击某一提取规则名称后【编辑】按钮，进入提取规则编辑页面。

根据实际情况，填写识别规则名称、解析方式，确认无误后，点击【测试】，测试通过后，点击【确定】即可。

删除识别规则

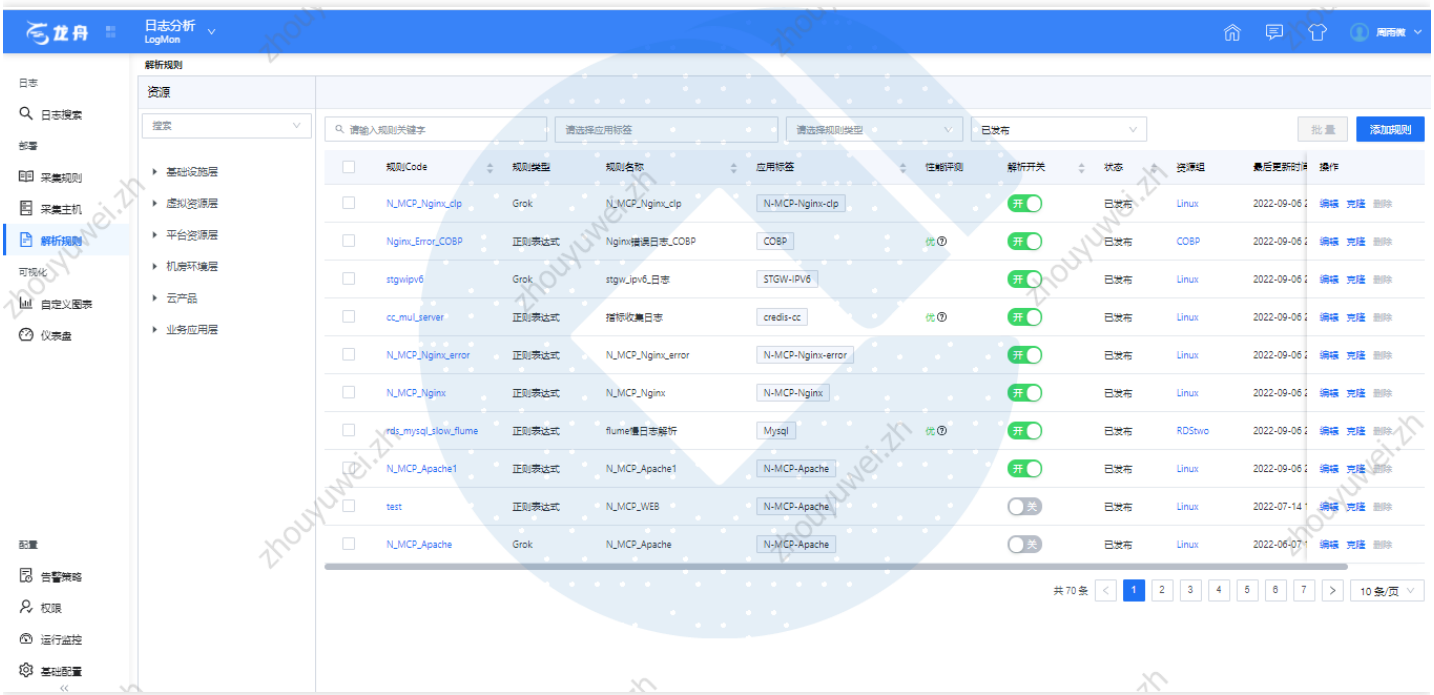
最近更新时间: 2023-02-13 12:00:42

可根据实际情况变化删除解析规则下已有的提取规则。

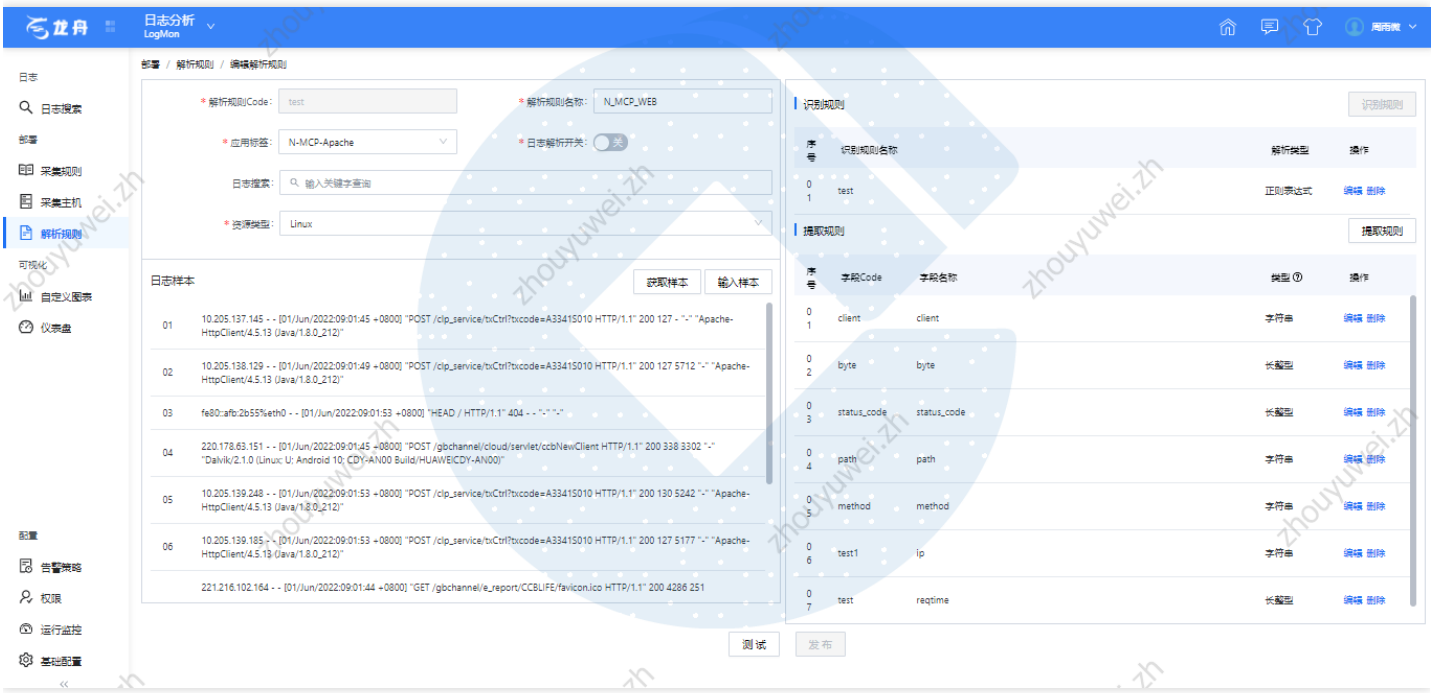
编辑解析规则

最近更新时间: 2023-02-13 11:33:12

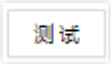
点击【解析规则】，进入解析规则列表页面，如下图所示：



点击【编辑】按钮，进入解析规则编辑页面，如下图所示：



根据实际情况填写解析规则基本信息编写、日志样本可分为单行采集和多行采集，特别说明多行采集需要输入分行

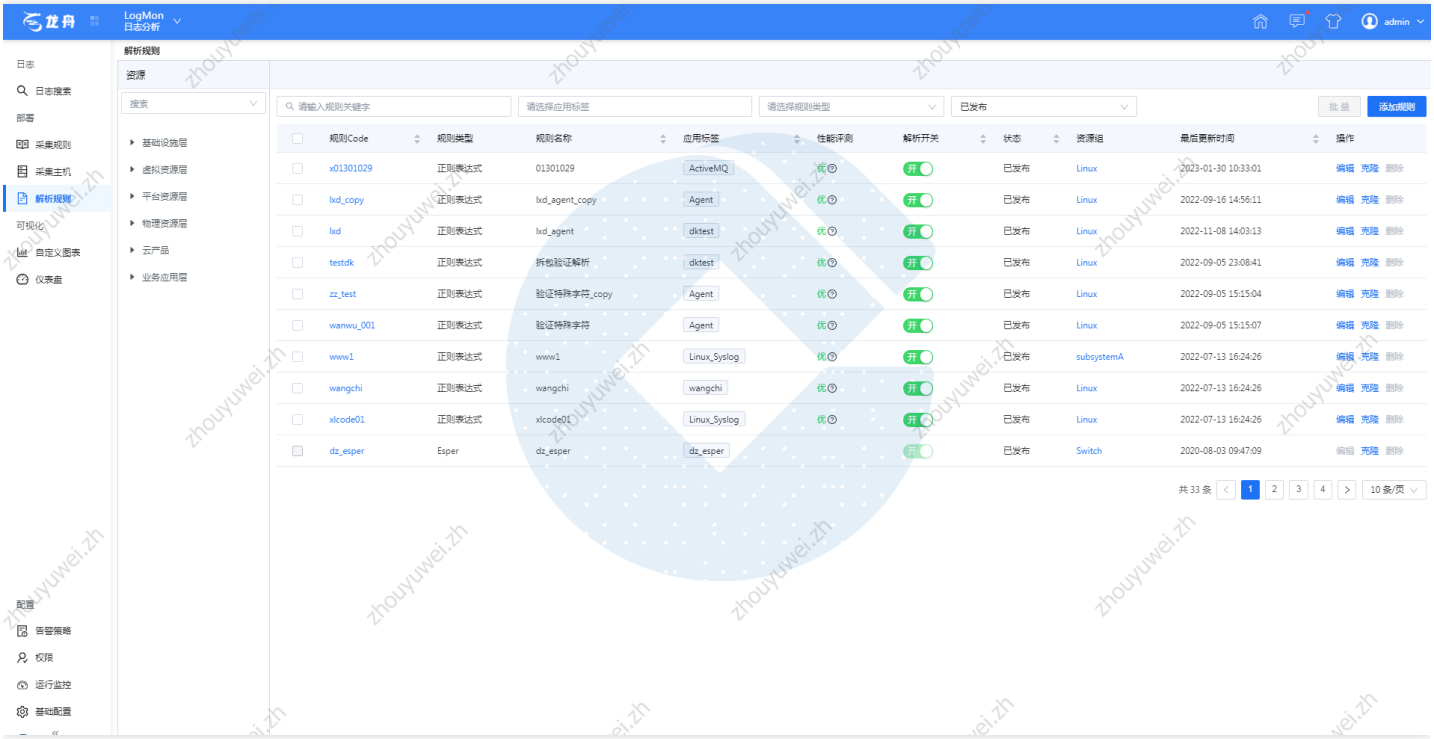
的正则表达式，识别规则创建/修改/删除、提取规则创建/修改/删除，点击 

按钮，通过测试后点击【保存】即可。

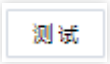
克隆解析规则

最近更新时间: 2023-02-14 16:20:52

点击【解析规则】，进入解析规则列表页面，如图所示：



点击【克隆】按钮，将克隆目标解析规则，如下图所示：



根据实际情况填写解析规则基本信息编写、识别规则编辑/删除、提取规则编辑/删除，点击 按钮，通过测试后点击【保存】即可.

删除解析规则

最近更新时间: 2023-02-13 11:33:12

可根据实际情况变化删除已有的解析规则配置，内置解析规则不可删除。

解析规则草稿

最近更新时间: 2023-02-13 11:33:12

可对未编写完的解析规则进行草稿保存，以便下次能继续编写；点击【存为草稿】按钮。

解析规则搜索

最近更新时间: 2023-02-13 11:33:12

点击【解析规则】，进入解析规则列表页面，如下图所示：

输入规则code和规则名称可以进行解析规则模糊搜索，可以选择标签和解析规则状态进行条件搜索，状态包括已发布和草稿两种。

日志告警
告警策略搜索

最近更新时间: 2023-02-13 11:33:12

在检索条件输入框中输入‘告警策略名称值’按Enter键进行模糊查询，点击【高级查询】即可展开告警查询栏，包含搜索条件告警类型、告警开关、告警等级，可组合查询到符合所有类型的告警策略。

批量配置针对于告警策略列表进行批量处理，若不选择任何告警策略，则【批量配置】按钮为禁用状态，勾选任意项告警策略后，【批量配置】按钮为启用状态，点击【批量配置】按钮弹出三个配置项，包含批量开启、批量关闭、批量删除。点击后进行二次确认即可进行相应操作

1.批量开启：对于选中的告警策略批量开启告警，此后开始可以触发告警；

2.批量关闭：对于选中的告警策略批量关闭告警，此后开始不再触发告警；

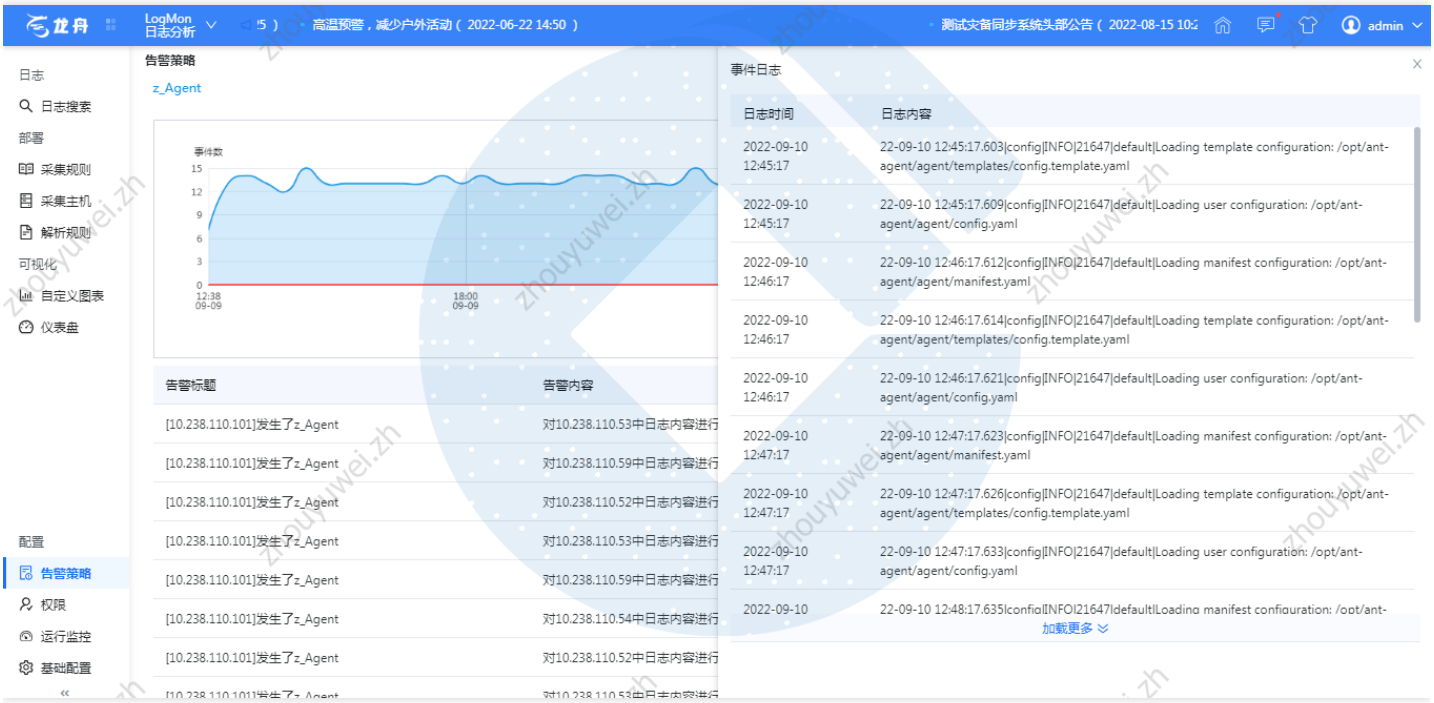
3.批量删除：对于选中的告警策略批量删除。

告警事件查看

最近更新时间: 2023-02-13 11:33:12

告警策略页面中【告警趋势】项展示的是该告警策略的近24h的触发告警情况面积图的缩略图，点击【告警趋势项缩略图】即可进入该项的趋势分析页面，点击某一告警的告警趋势图，即可进入该告警的查看详情页面。

上半部分为告警该告警策略的告警情况展现面积图，x轴为时间，y轴为告警事件数。鼠标放置折线图上可展示当前时间点的各个告警具体条数。下半部分为告警列表部分，包含了告警标题、告警内容、告警级别以及告警时间几项，点击告警时间的头部【告警时间】即可对该列表进行告警时间的升降序排列。点击操作项的【查看事件日志】则弹出日志时间框，展示详细日志内容。


龙舟
LogMon
日志分析
高温预警，减少户外活动（ 2022-06-22 14:50 ）
admin
日志
日志搜索
部署
采集规则
采集主机
解析规则
可视化
自定义图表
仪表盘
配置
告警策略
权限
运行监控
基础配置
告警策略
z_Agent
事件数
15
12
9
6
3
0
12:38
09-09
18:00
09-09
告警标题
告警内容
[10.238.110.101]发生了z_Agent
对10.238.110.53中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.59中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.52中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.53中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.59中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.54中日志内容进行
[10.238.110.101]发生了z_Agent
对10.238.110.52中日志内容进行
事件日志
日志时间
日志内容
2022-09-10 12:45:17
22-09-10 12:45:17.603|config|INFO|21647|default|Loading template configuration: /opt/ant-agent/agent/templates/config.template.yaml
2022-09-10 12:45:17
22-09-10 12:45:17.609|config|INFO|21647|default|Loading user configuration: /opt/ant-agent/agent/config.yaml
2022-09-10 12:46:17
22-09-10 12:46:17.612|config|INFO|21647|default|Loading manifest configuration: /opt/ant-agent/agent/manifest.yaml
2022-09-10 12:46:17
22-09-10 12:46:17.614|config|INFO|21647|default|Loading template configuration: /opt/ant-agent/agent/templates/config.template.yaml
2022-09-10 12:46:17
22-09-10 12:46:17.621|config|INFO|21647|default|Loading user configuration: /opt/ant-agent/agent/config.yaml
2022-09-10 12:47:17
22-09-10 12:47:17.623|config|INFO|21647|default|Loading manifest configuration: /opt/ant-agent/agent/manifest.yaml
2022-09-10 12:47:17
22-09-10 12:47:17.626|config|INFO|21647|default|Loading template configuration: /opt/ant-agent/agent/templates/config.template.yaml
2022-09-10 12:47:17
22-09-10 12:47:17.633|config|INFO|21647|default|Loading user configuration: /opt/ant-agent/agent/config.yaml
2022-09-10
22-09-10 12:48:17.635|config|INFO|21647|default|Loading manifest configuration: /opt/ant-
加载更多

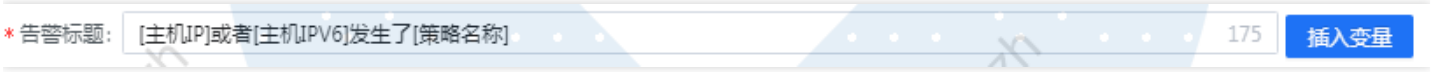
告警策略配置–关键字告警

最近更新时间: 2023-02-13 11:33:12

点击主页面的【新增】按钮即可进入新增告警页面，选择关键字告警：

输入项前有红色 * 则代表该项为必填项，各项会有固定的格式要求，若不符合格式则会有红色文字警示。关键字支持字符串或正则的方式对日志信息中的关键字进行匹配。其中新增页面的‘告警标题’以及‘告警内容’右侧的【插入变量】按钮，点击后展开下拉框展示可插入的变量，点击标题或内容中的某位置，即可点击【插入变量】选择相应的变量插入。变量插入位置为光标所在位置。

例：原告警标题为“[主机IP]发生了[策略名称]”。如要更改，将光标移到插入位置，输入‘或者’文本，点击【插入变量】选择【主机IPV6】，文本生成如下：



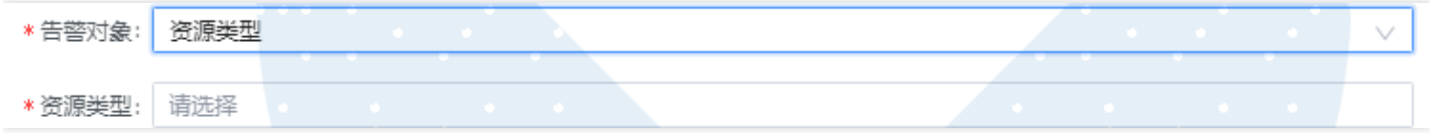
其中告警标题和告警内容变量是在初始时用该变量名代替，当发生告警后该变量会翻译为确定的告警常量值：

例：填写告警标题为：[主机IP]发生了[策略名称]

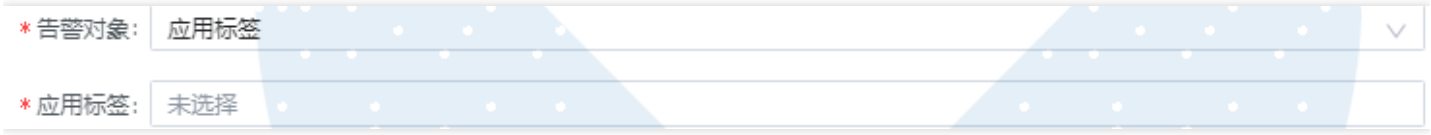
告警发生后告警标题可为：101.37.17.6发生了Nginx日志

当【告警对象】选择为主机IP时，下方会弹出【主机IP】输入框，可输入多个IP，用逗号‘，’分隔：

当【告警对象】选择为资源类型时，下方会弹出【资源类型】选择栏，只可单选：



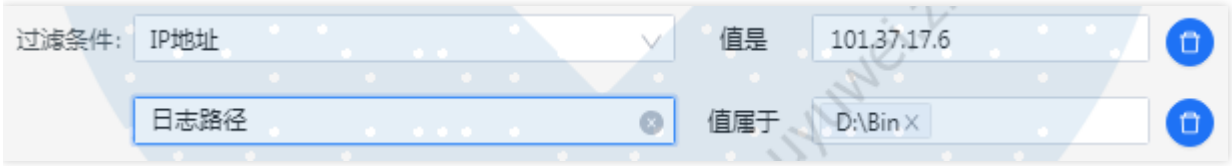
当【告警对象】选择为应用标签时，下方会弹出【应用标签名称】选择栏，可多选：



高级配置中的【解析规则名称】为该租户下的解析规则内容，选择确定的解析规则名称后在过滤条件中会新增该解析规则名称下的字段。若不选择任何解析规则名称则展现默认的‘日志级别’和‘日志路径’该两个默认字段。点击过滤

条件下的【新增】按钮可新增过滤条件，点击过滤条件后的 ，可删除该条过滤条件。

选择某字段后需选择该字段的属性，一共分为‘是、不是、属于、不属于、有值、无值’该6种，可添加多个过滤条件。例：



过滤条件为：Ip地址值是101.37.17.6 AND 日志路径是D:\Bin

输入完所有必填项即可点击下方【保存】按钮进行保存，点击【取消】按钮即返回主页面。

告警策略配置–事件数告警

最近更新时间: 2023-02-13 11:33:12

点击主页面的【新增】按钮即可进入新增告警页面，选择事件数告警：

输入项前有红色‘* ’则代表该项为必填项，各项会有固定的格式要求，若不符合格式则会有红色文字警示。其中新增页面的‘告警标题’以及‘告警内容’右侧的【插入变量】按钮，点击后展开下拉框展示可插入的变量，点击标题或内容中的某位置，即可点击【插入变量】选择相应的变量插入。变量插入位置为光标所在位置。其中告警标题和告警内容变量是在初始时用该变量名代替，当发生告警后该变量会翻译为确定的告警常量值

点击时间范围下方的【新增】按钮即可新增一条时间范围选项，点击时间范围后的 即可删除该条时间范围，只有一条时间范围时不展示。

默认为5分钟出现5次触发告警，级别警告，可选择相应的部分修改，最多一共只能增加为3条时间范围，且告警级别不能有重复。点击【执行频率】选择项选择为定时任务即可展开为Cron表达式页面，右侧会展现具体表达式的值，左侧自定义时间可自定义范围为24h，可选择分度值为‘分钟’和‘小时’。

标签管理

新增标签

最近更新时间: 2023-02-13 11:33:17

新增标签

点击 按钮，打开新增标签窗口，标签名称不可重复，如下图所示：

删除标签

最近更新时间: 2023-02-13 11:33:17

点击【标签管理】进入标签管理页面。在标签列表中，点击某一标签名称后点击【删除】按钮，删除该标签。
已关联采集规则或解析规则的标签无法删除，如需删除该状态标签，先解除标签关联。

常见问题
日志采集准备工作

最近更新时间: 2023-02-13 10:38:45

采集日志前首先确认以下内容

1、在采集日志前确保对应主机已完成采集插件安装，在采集主机页面主机显示在线状态；

2、配置对应的采集规则，确保规则中采集的日志路径准确；

3、采集规则配置完成后，需要将规则关联对应的采集主机。

日志采集的影响

最近更新时间: 2023-02-13 10:38:45

配置日志采集后，采集对应主机的日志时，会启动采集进程消耗对应主机的cpu、内存、磁盘等资源，相关资源消耗情况如下：

代理及插件名称：日志采集；编码：local-log-flume；

磁盘占用：默认生产在/opt目录下，不含日志占360M，日志文件最多7个，每个最大50M====合计710M；

日志是否持续增长：否；

CPU占用平均值：3%

CPU占用峰值：20%

内存平均值：384M；

内存峰值：512M

是否默认安装：否

备注：分配内存默认最小为256M，随着配置采集路径增加，内存会增长，最大不超过512M

请确保采集主机具备充足的资源。

日志采集不到问题检查

最近更新时间: 2023-02-13 10:38:45

主机关联采集规则后，无法搜索到采集日志，可以进入采集主机页面，选择对应的采集主机，点击主机ip，查看关联的采集规则详情，采集状态分为三种，分别是未知、异常、正常。灰色未知代表目前还在检测,可能当前未生成最新的日志，尚未采集到数据入库，请检查采集日志文件是否有最新的日志内容产生；红色异常，代表当前配置规则异常，请检查采集路径是否存在或接收数据端口是否异常等；正常代表规则条目正常采集到数据并且解析入库。