Apusic 金蝶天燕

生成时间：2026-05-19

用户手册

金蝶Apusic智能日志平台v2.0

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

Apusic是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

- 12 停止卸载K8s日志采集组件

1 前言

1.1 产品简介

金蝶Apusic智能日志平台(简称：AILP)是一个通用的日志大数据平台，可以使用各种开源的日志收集工具将日志统一上传，并根据预先定义的解析规则将日志数据结构化存储，提供准实时的搜索和仪表盘对日志进行后续的分析处理。

典型的日志数据包括：

- Linux系统日志
- Apache Web服务器日志
- Nginx Web服务器日志
- 中间件日志
- 数据库日志
- JSON日志
- 其他任意文件型日志

1.2 范围和读者

本手册介绍AILP V2.0使用详细说明，适用于该产品的使用用户，产品技术顾问，产品维护人员，以及希望学习了解AILP平台的相关人员。

1.3 文档导航

章节	内容概述
1. 前言	产品简介、文档范围、约定内容
2. 概述	AILP产品概要介绍
3. 快速开始	产品快速使用说明
4. 使用说明	产品详细说明
5. K8s日志采集说明	K8s类型日志采集详细说明

1.4 约定与术语

一些约定的缩略词诠释：

- AILP

Apusic智能日志平台（Apusic Intelligent Log Platform）

2 概述

2.1 概述

金蝶Apusic智能日志平台是日志大数据平台，提供日志数据的采集、管理、分析、开放共享，建立起日志基础平台。支持指标、日志、事件等多种类型数据的统一存储和分析；实现日志数据实时监控、综合分析IT环境各个资源及设备运行情况，提升现有IT运维管理水平。

2.2 工作原理

平台使用Filebeat采集日志数据，将Kafka作为Filebeat的输出端。Kafka实时接收到Filebeat采集的数据后，以Logstash作为输出端输出。输出到Logstash中的数据在格式或内容上可能不能满足您的需求，此时可以通过Logstash的filter插件过滤数据。最后将满足需求的数据输出到ES中进行分布式检索，并通过云日志服务进行数据分析与展示。

2.3 产品特性

- 基于日志模式对异常进行识别，帮助运维人员快速找出自己关心的日志类型，或者发现异常模式日志的告警，缩短问题发现的时间。
- 通过建立各业务系统之间的关联模型来实现业务流程下各业务系统之间关联日志的查询，帮助运维人员在故障发生时全面分析问题，大大缩短了故障定位的时间。
- 提供一站式的日志管理服务，支持离散日志的统一采集、处理、存储以及检索，让用户远离日志管理中的各种烦恼，专注挖掘日志数据的价值。

3 概要

智能日志概要数字展示接入主机、接入应用，接入日志类型数量，图表展示主机日志事件和应用事件记录数。（如图所示）

图4- 1概要

4 仪表盘

1. 仪表盘通过可视化配置的方式，让用户能够根据不同场景的需求自定义日志分析。天燕智能日志平台支持图形面 板、数字面板以及表格面板。其中图形面板包括区域图、柱状图、折线图以及饼图。通过组合不同的面板来完成复杂得报表呈现，支持根据设定的时间范围查询统计数据，可以通过设置自动更新动态更新面板数据，同时面板还支持拖拽缩放等功能。

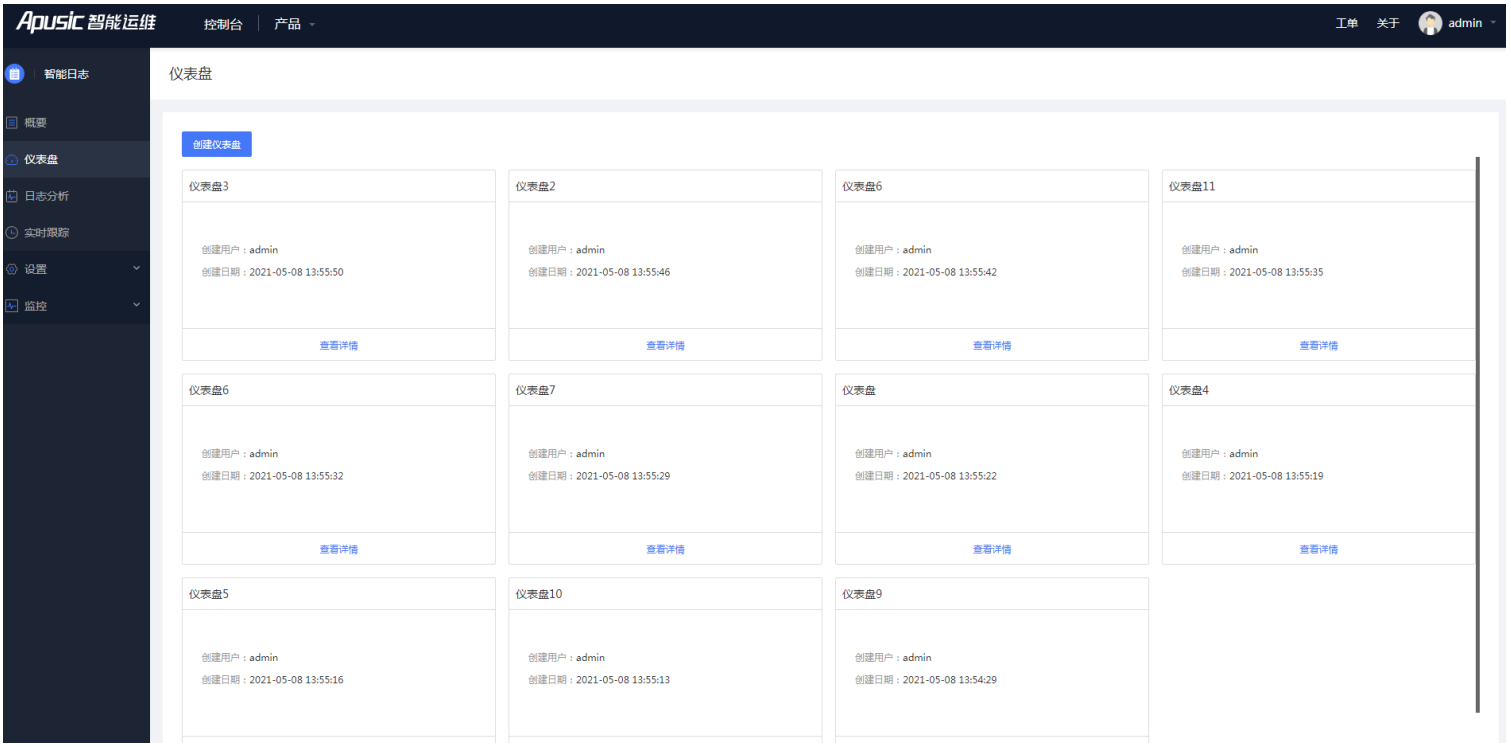


图4- 2仪表盘

2. 该页为仪表盘列表页，用户可以在该页面通过点击最右侧空白仪表盘创建新仪表盘。当鼠标悬停在仪表盘上时，出现编辑和删除操作的按钮，用户可以通过点击编辑按钮对仪表盘名称进行修改，修改窗口如下图，或者对仪表盘进行删除操作。

图4- 3仪表盘

新增面板

1. 点击进入仪表盘详情页，此处展示用户自定义的面板。左上角显示仪表盘名称，右上角第一个下拉选择框可选择面板数据的统计时间，第二个下拉选择框可以设置自动更新的周期时长，默认为关闭自动更新，返回按钮返回仪表盘列表。右下角点击按钮展开新增面板，依次为区域图、柱状图、折线图、饼图、表格面板以及数字面板。

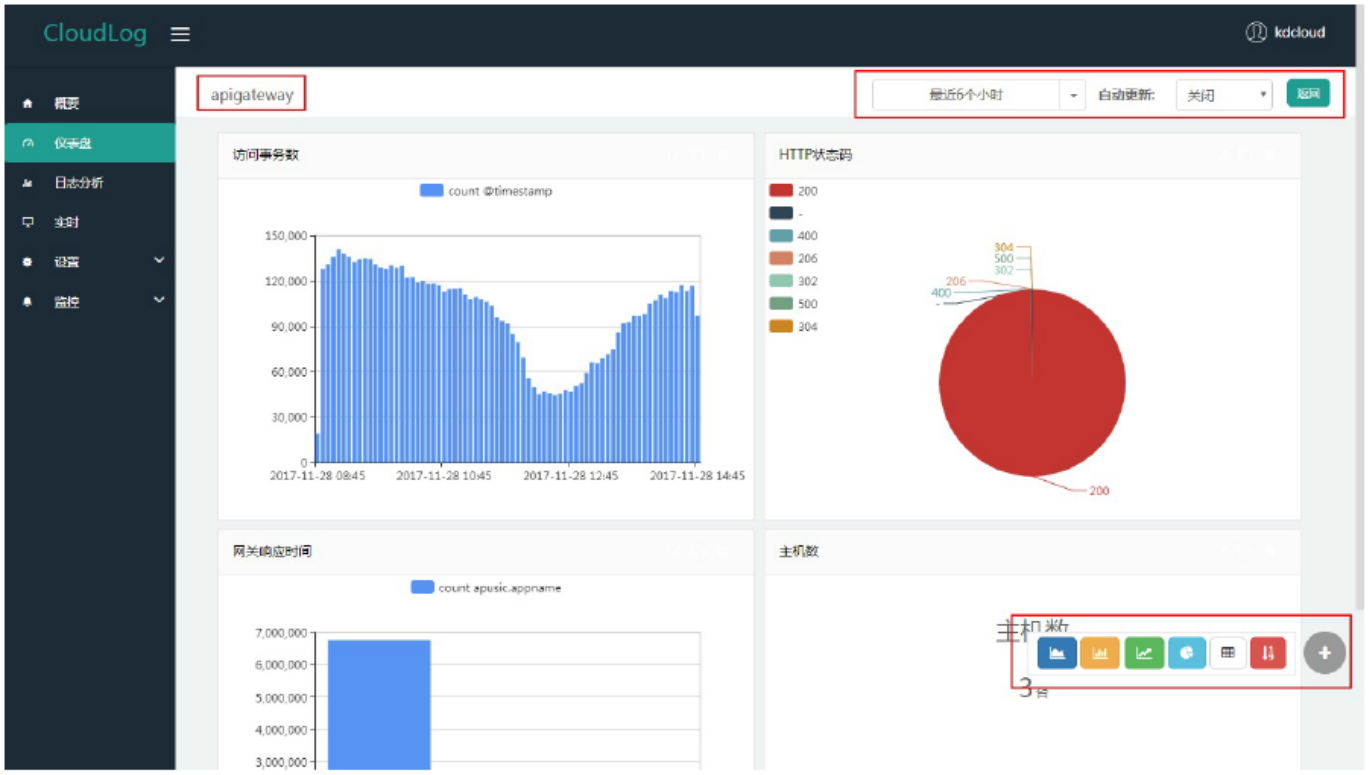


图4- 4图表

2. 选择一种面板类型，进入面板设置页面。

3. 上方为图形预览部分，中间为面板配置项。

- 区域图、柱状图、折线图、饼图

如：选择数据源kdcloud-apigwsuccess-kdcloud_nginx-* 作为索引，Y轴配置中，过滤条件为空，度量维度选择统计@timestamp的总数。通过Y轴配置右侧的按钮动态增删度量维度。X轴配置中，选择Data Histogram分组方式，统计字段为@timestamp，X轴统计间隔为5分钟。

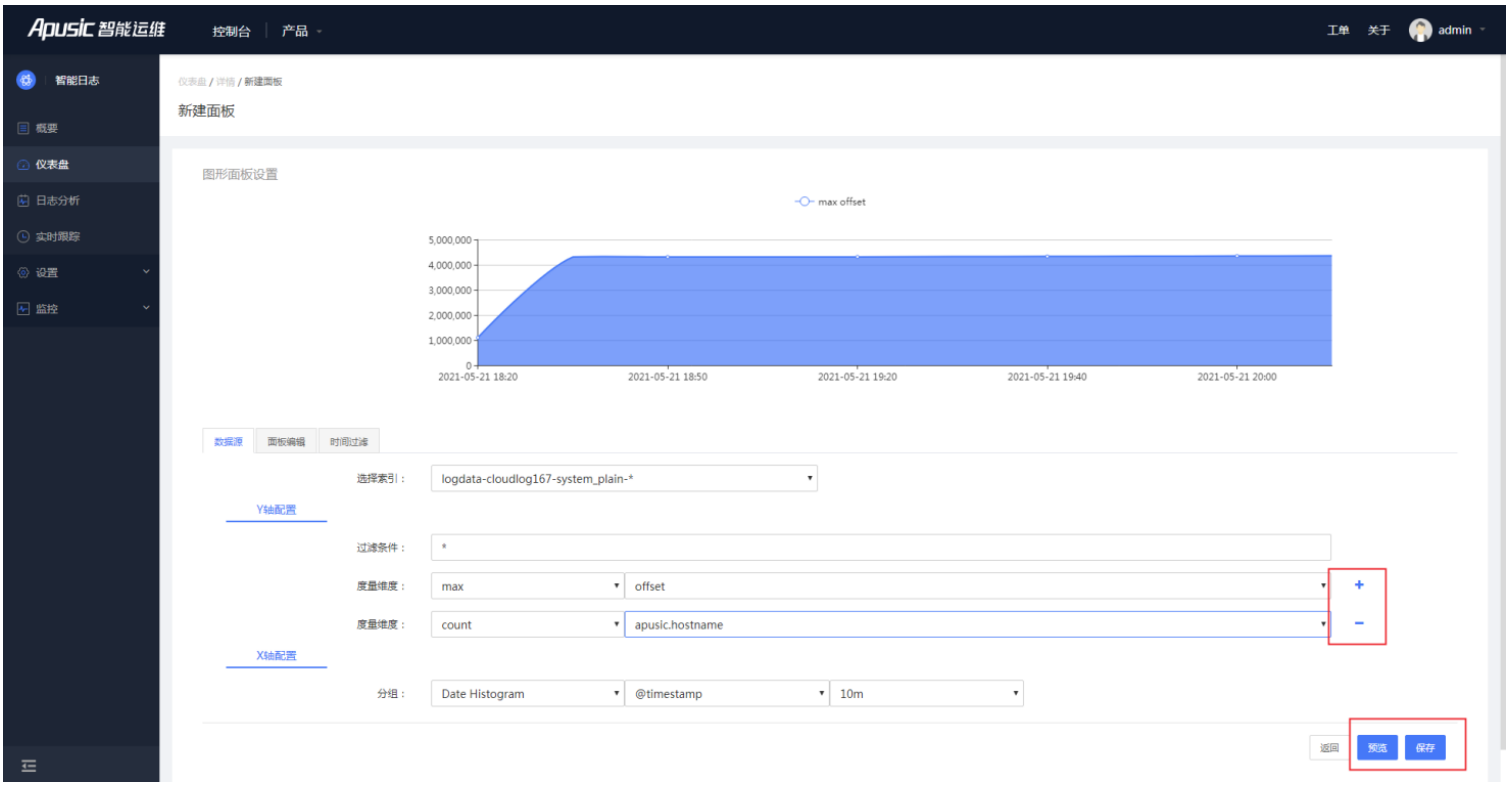


图4- 5数据源

面板编辑页签中选择柱状图为该图表图表展现形式，设置面板标题为访问事务数。

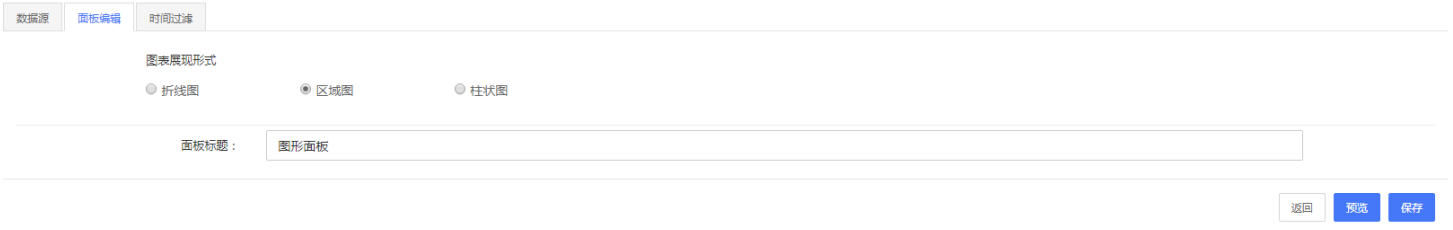


图4- 6面板编辑

时间过滤页签选择今天作为统计的范围。

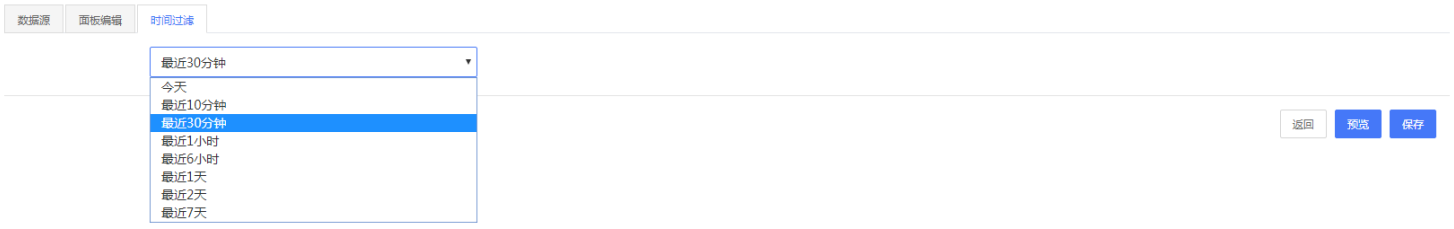


图4- 7时间过滤

- 表格面板

表格面板中对用户自定义的字段进行统计，用户通过多选下拉列表选择数据。并可通过点击右侧 删除图标删除已选字段。

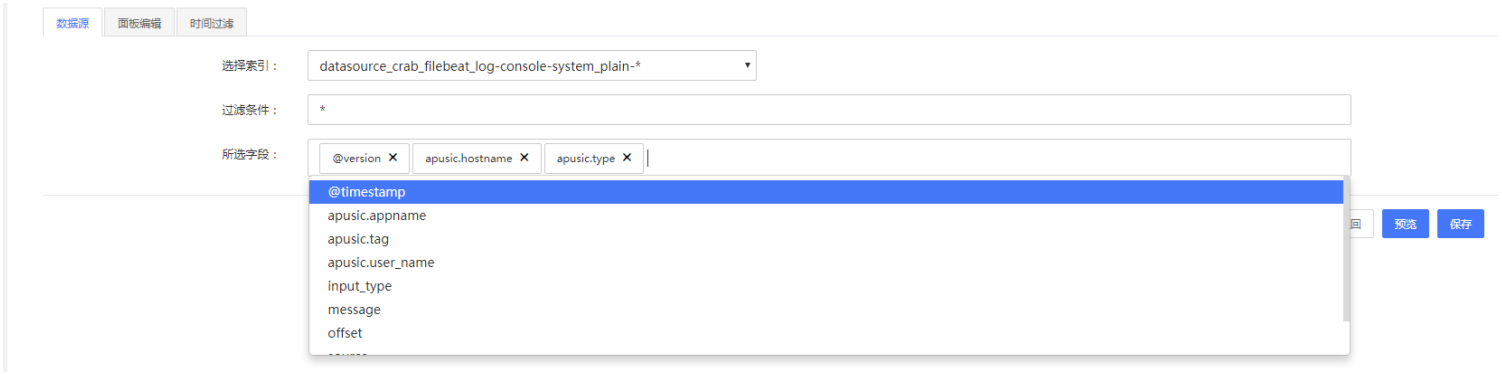


图4- 8表格面板1

根据所选字段统计数据，支持翻页功能。

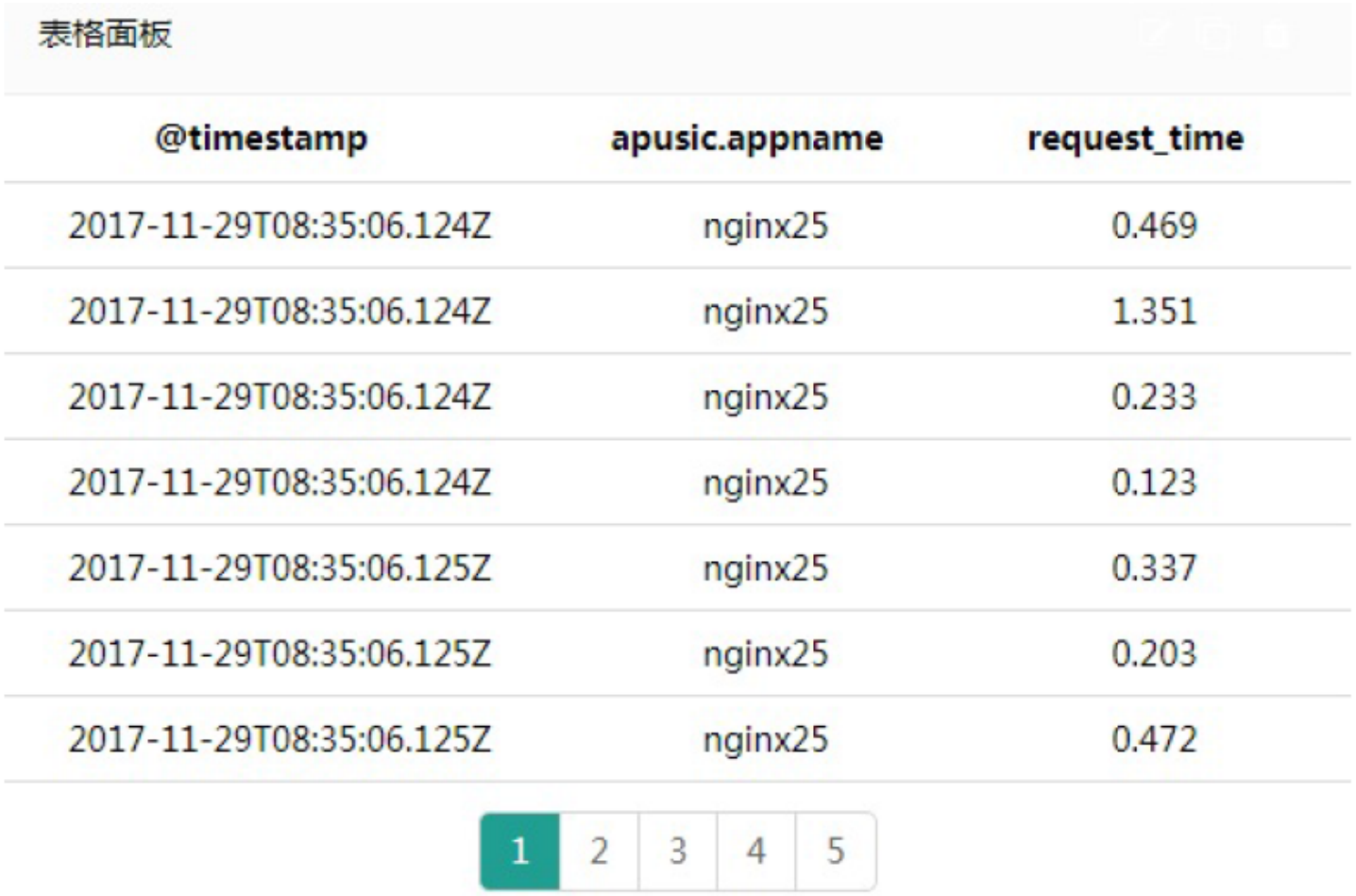
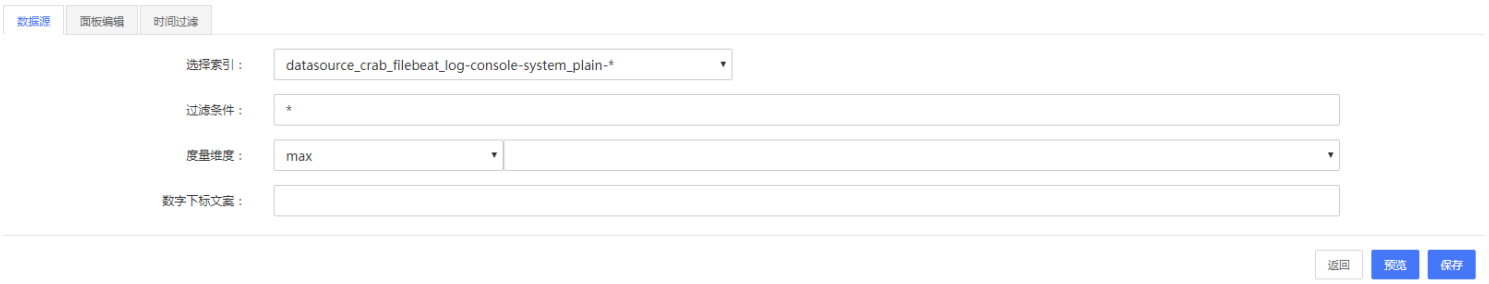


图4- 9表格面板2

- 数字面板

选择索引，过滤条件为空，统计字段为apusic.hostname，数字下标文案为台。



如下图：主机数为面板标题，3为统计所得数据，台为用户填入的数字下标文案。

3、点击页面右下方进行预览或者保存调整到面板列表页。

面板操作

用户能够根据自己的需要移动缩放面板，单个面板具备编辑、复制以及删除的操作。拖住面板任意位置进行移动可以改变面板位置，拖住右下角可以对面板进行缩放，面板中图例会根据面板大小自适应。图形面板可以动态增删图例、表格面板可以进行翻页操作。

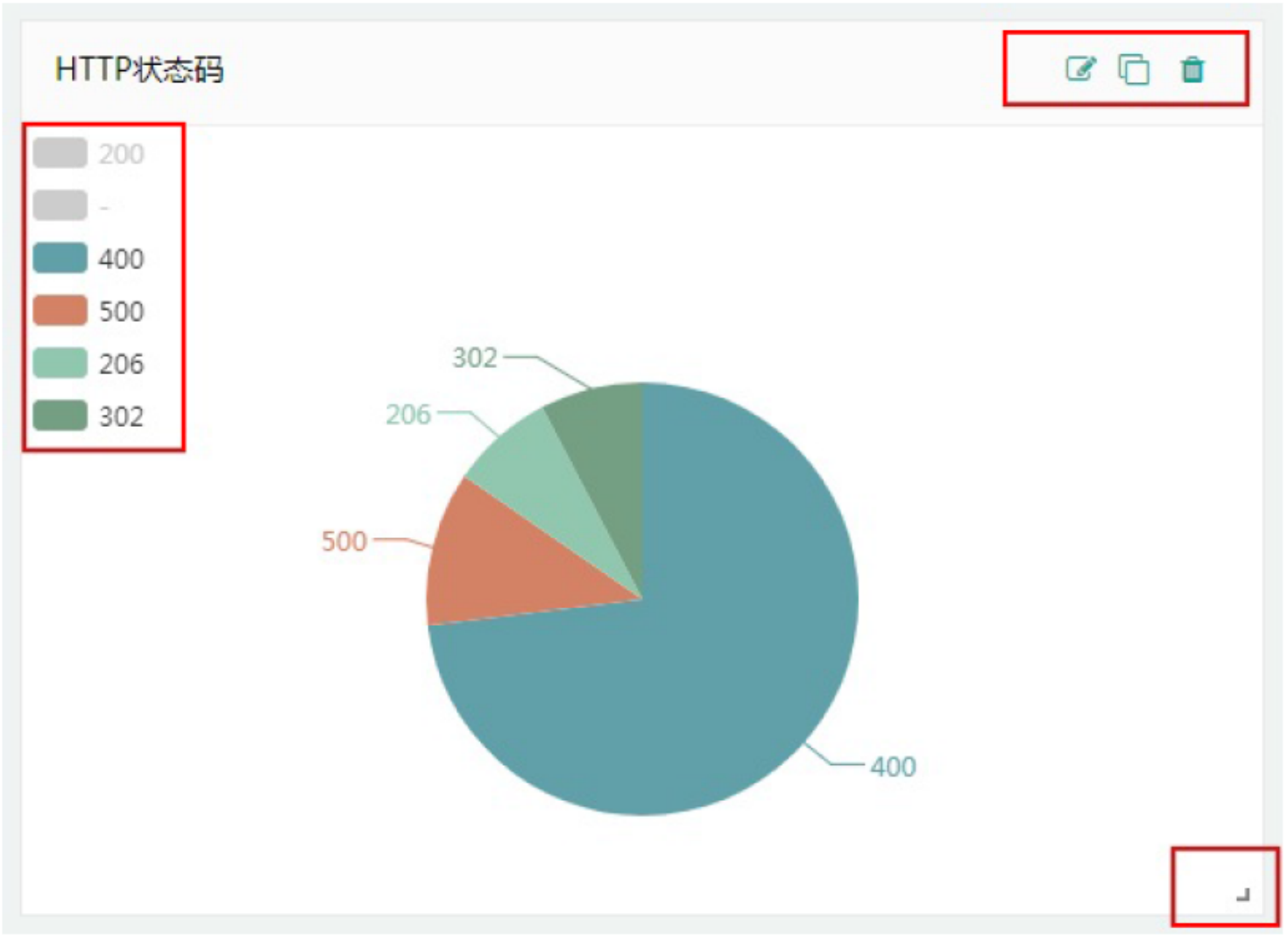


图4- 10面板操作1

点击复制面板，如下图所示。

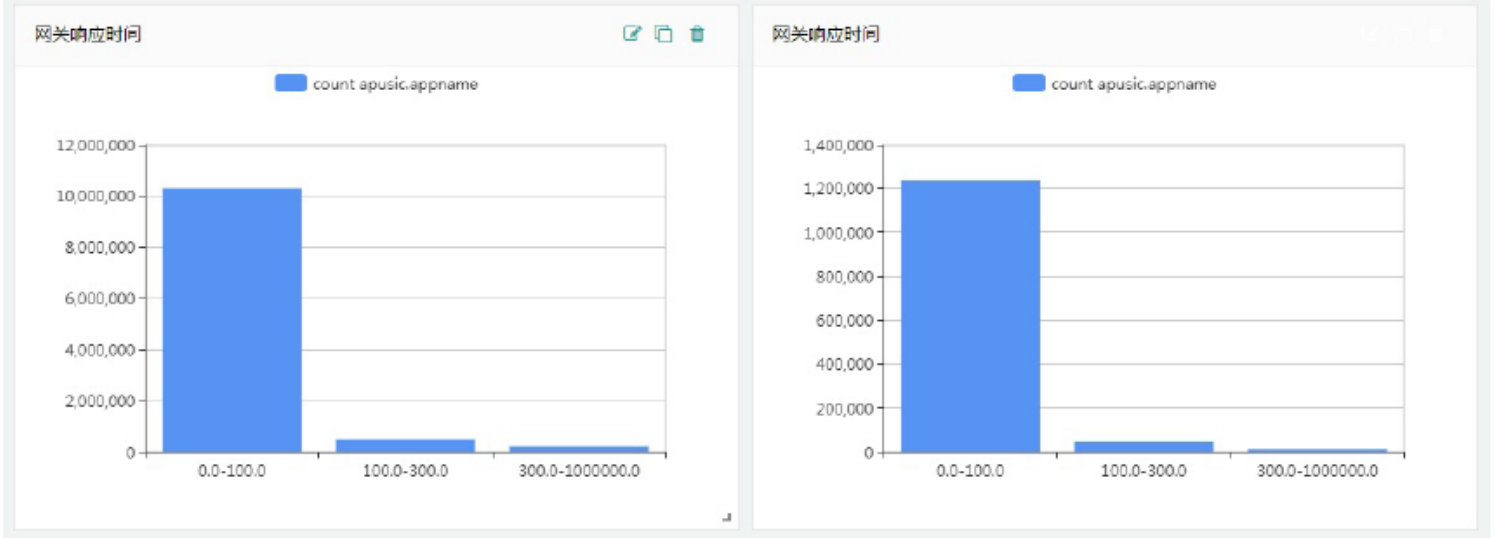


图4- 11面板操作2

5 配置

5.1 日志配置

日志配置是使用Apusic智能日志平台的第一步。在"设置"菜单中点击"日志配置"，即可进入日志配置的引导页面。

- **服务器操作系统**

首先选择需要上传日志的服务器操作系统，目前支持ubuntu和redhat等Linux系统。（如图所示）

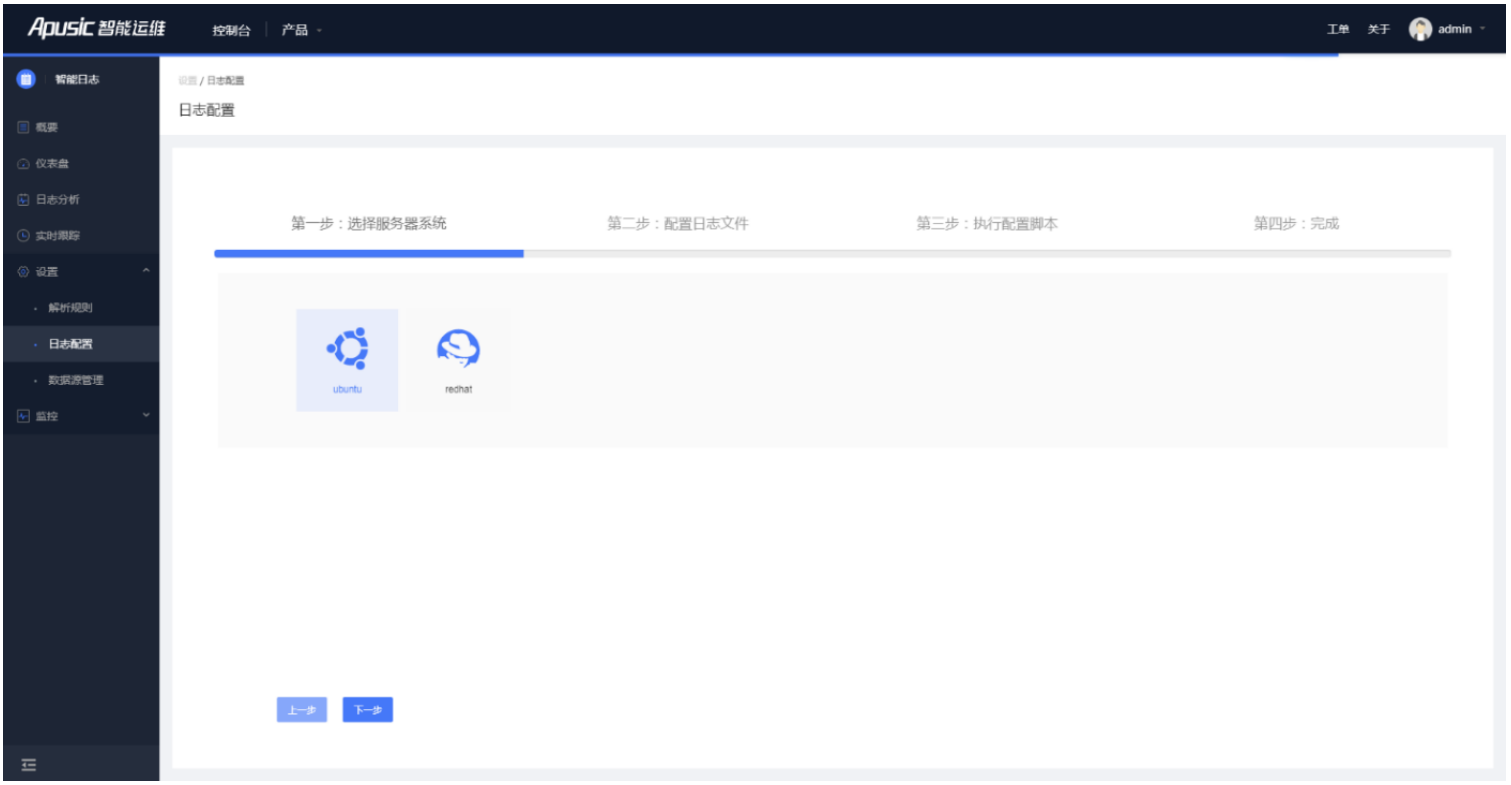


图4- 12选择服务器系统

- **配置日志文件**

配置日志文件需要输入：日志文件绝对路径、应用名和应用标签，同时需要指定日志的解析规则。天燕智能日志平台内置了Mysql Log、Zookeeper Log等常见日志文件的解析规则。如果用户日志比较特殊，则可以使 用自定义的解析规则。如何自定义解析规则，用户可参看下一章节内容。（如图所示）

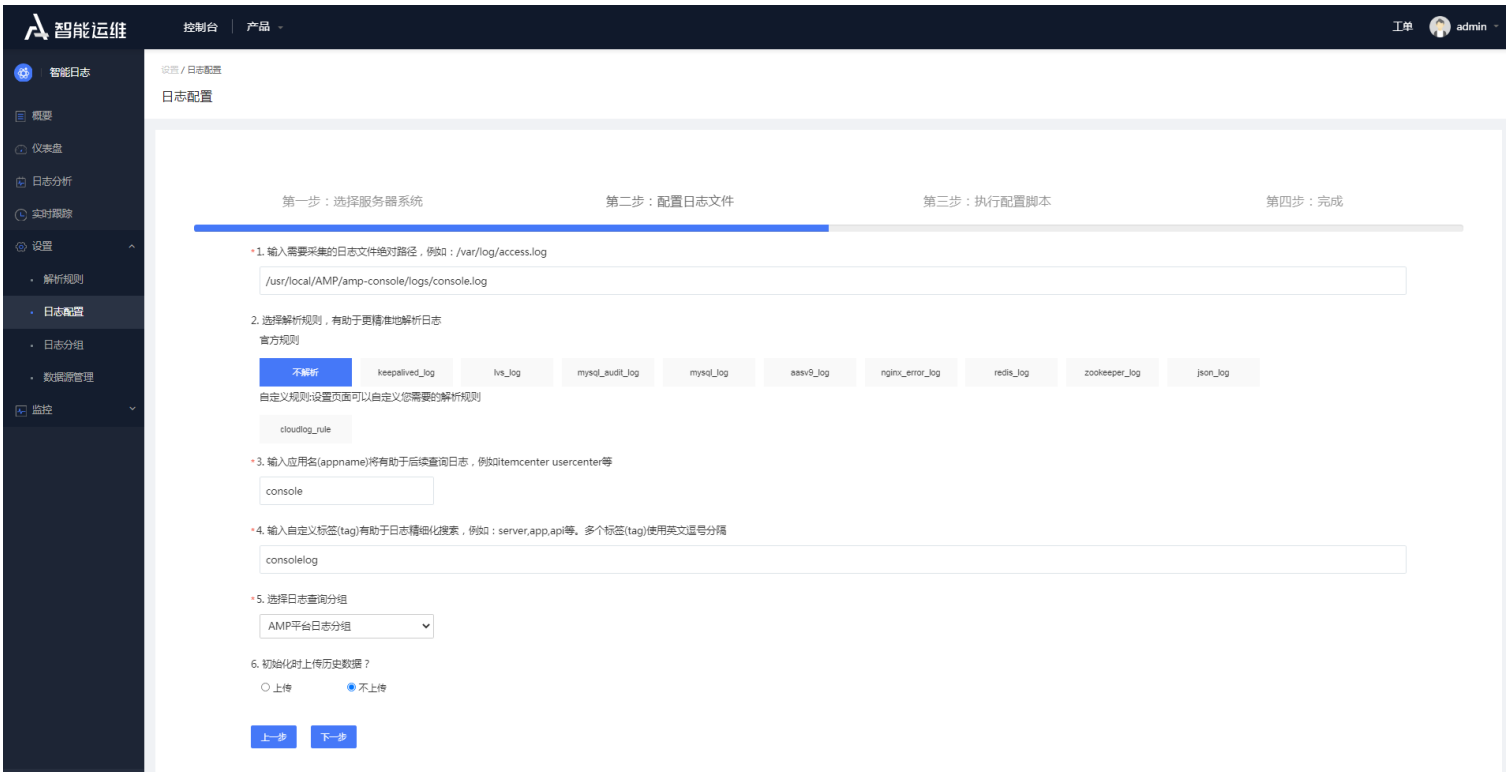


图4- 13配置日志文件

- **执行配置脚本**

配置日志文件完成以后，只需要在目标服务器执行相应shell脚本，即可完成整个日志采集配置过程。

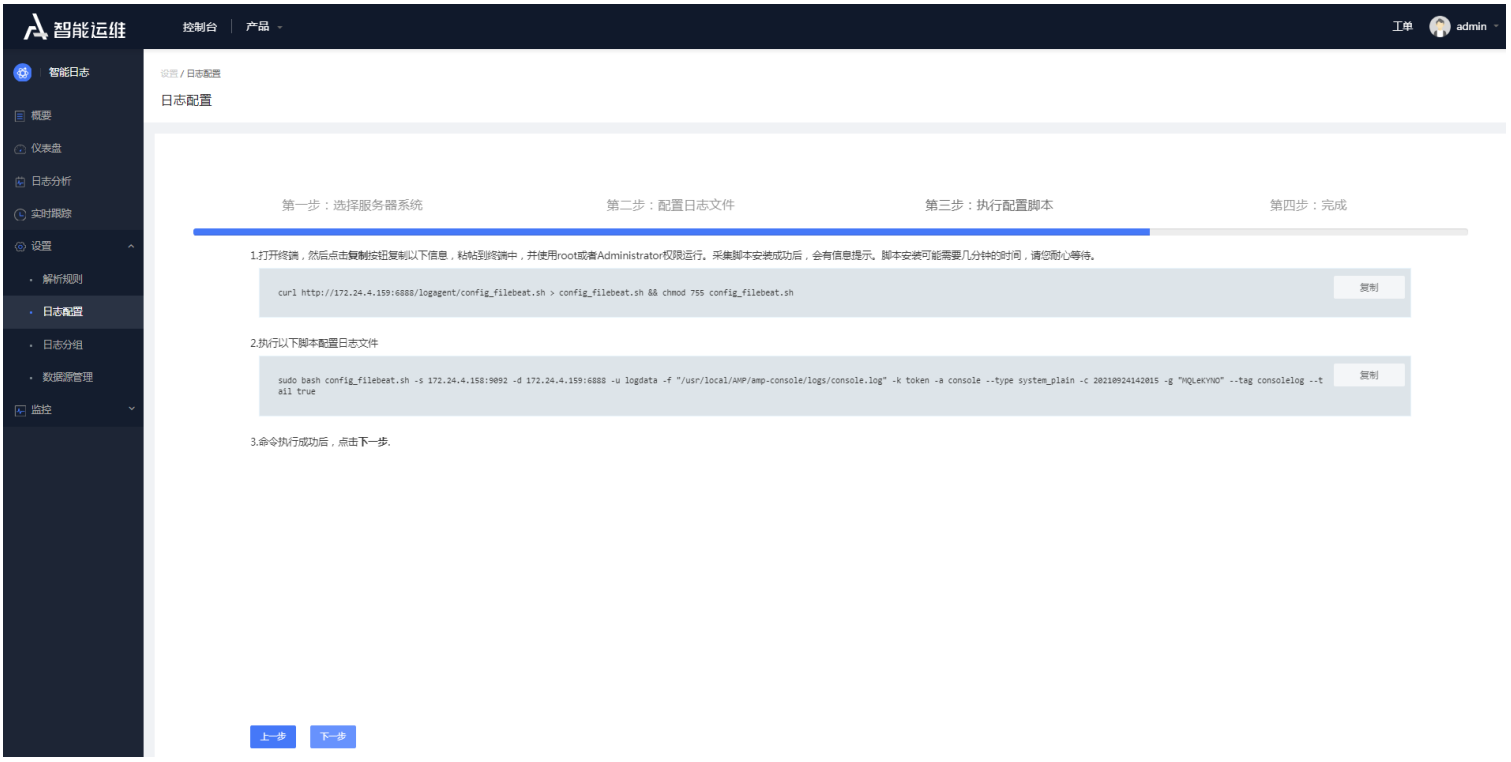


图4- 14执行配置脚本

5.2 解析规则

用户上传的原生日志是一种半结构化数据，一般按行分为不同的记录，每条记录则根据日志类型的不同， 可以拆分成不同的字段。解析日志就是按照预先定义的解析规则将非结构化的日志数据变成结构化的数据。

- **官方解析规则**

AILP智能日志平台提供了常用的**官方**日志解析规则，例如Zookeeper_log、mysql_log、redis-log、keepalived_log、lvs_log、mysql_audit_log、nginx_error_log、json_log。

- **自定义解析规则**

AILP智能日志平台提供了常用的日志解析规则，能够识别和解析常见的日志格式。对于不支持的日志格式，用户可以自定义解析规则。

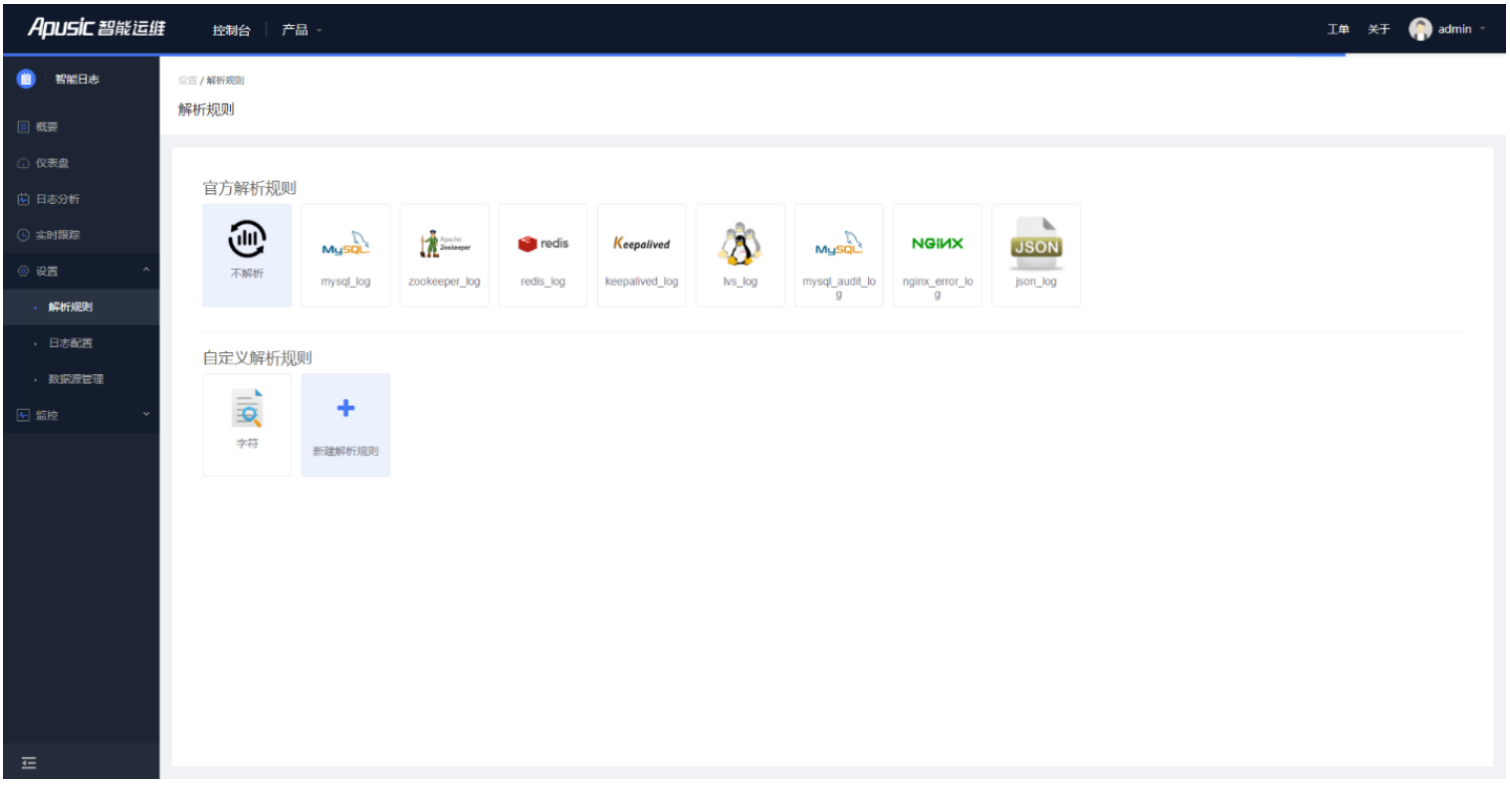


图4- 15解析规则

自定义解析规则首先需要填写一段日志样例，再选择一种解析器，智能日志提供多种解析器，用户选择一项 解析后，填写相应规则，再根据字段进行细粒度地拆分。创建过程如下：

1、添加一段日志样例，并选一种解析器。目前智能日志提供的解析器有四种：

- 正则解析
- JSON解析

- 数值型字段转换
- 时间戳识别等

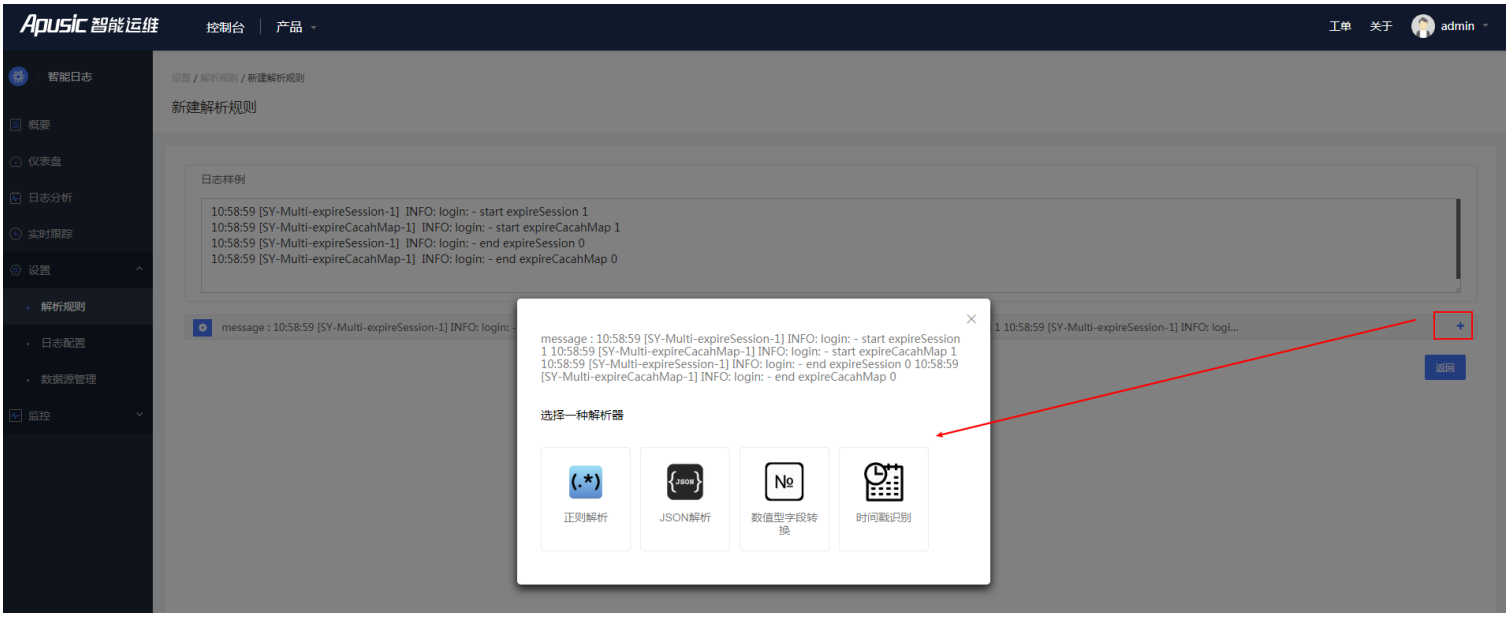


图4- 16正则解析

2、示例中选择正则解析，填写解析规则。

图4- 17填写解析规则

3、在上面窗口中点击"确定"，日志样例将进行日志解析，解析为结构化的数据。

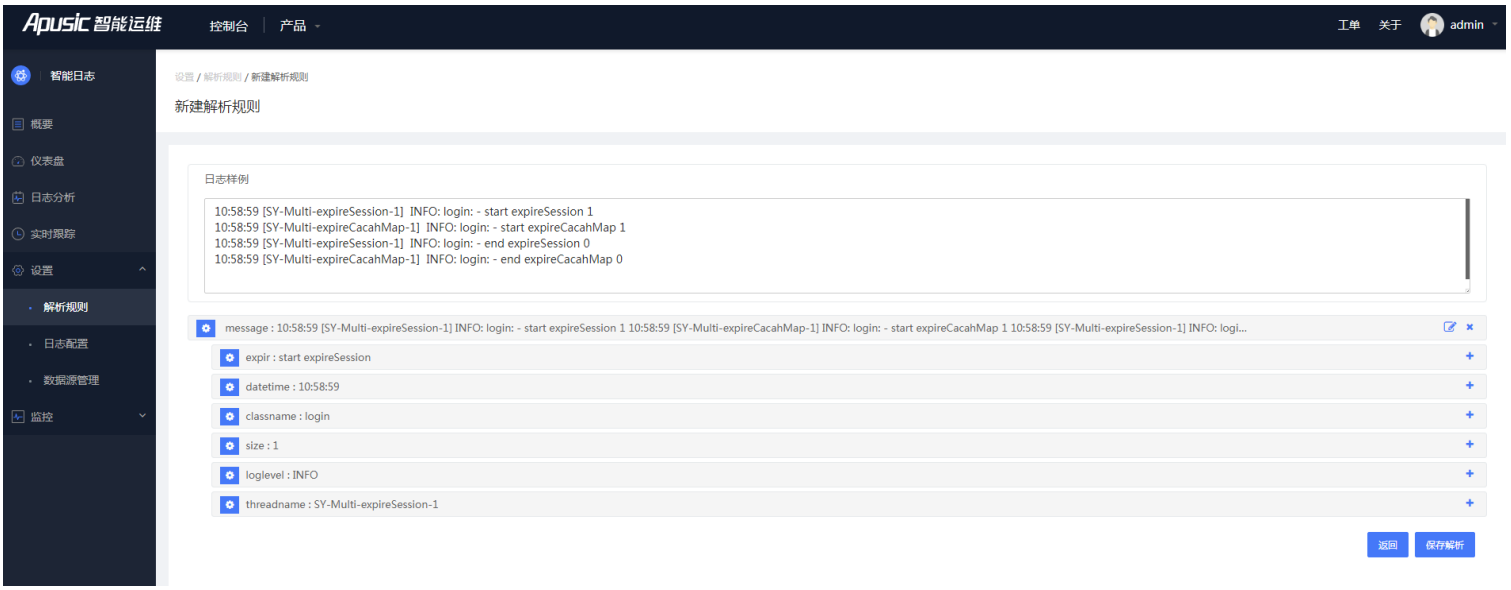


图4- 18编辑解析1

4、默认正则解析的字段类型为字符型，所以可以更细粒度的定义字段类型。

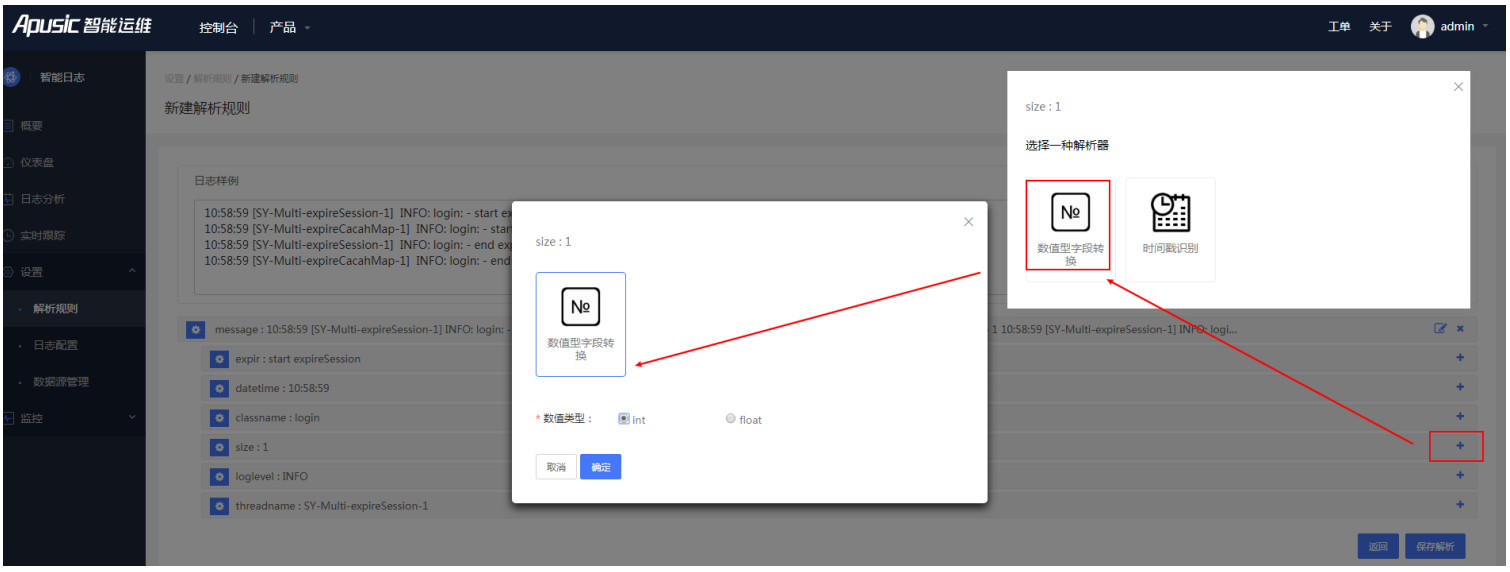


图4- 19编辑解析2

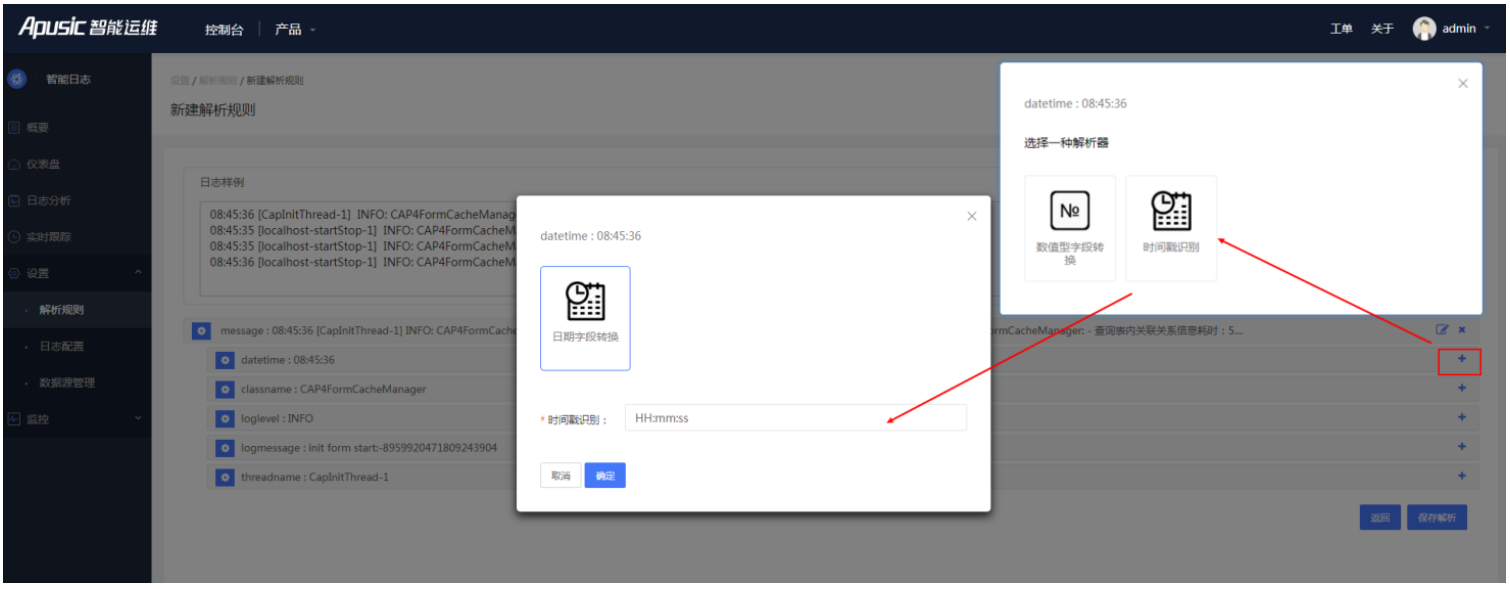


图4- 20编辑解析3

5、最后保存规则。

图4- 21保存规则

5.3 数据源管理

数据源是按照ElasticSearch中的索引来划分的，每个索引对应一个数据源。显示的信息包括：索引名，来源，分组，接入主机，日志文件名，解析规则，应用名，上传日志总数，最后上传时间。

数据源管理并且提供了数据源的删除、暂停和启动操作。

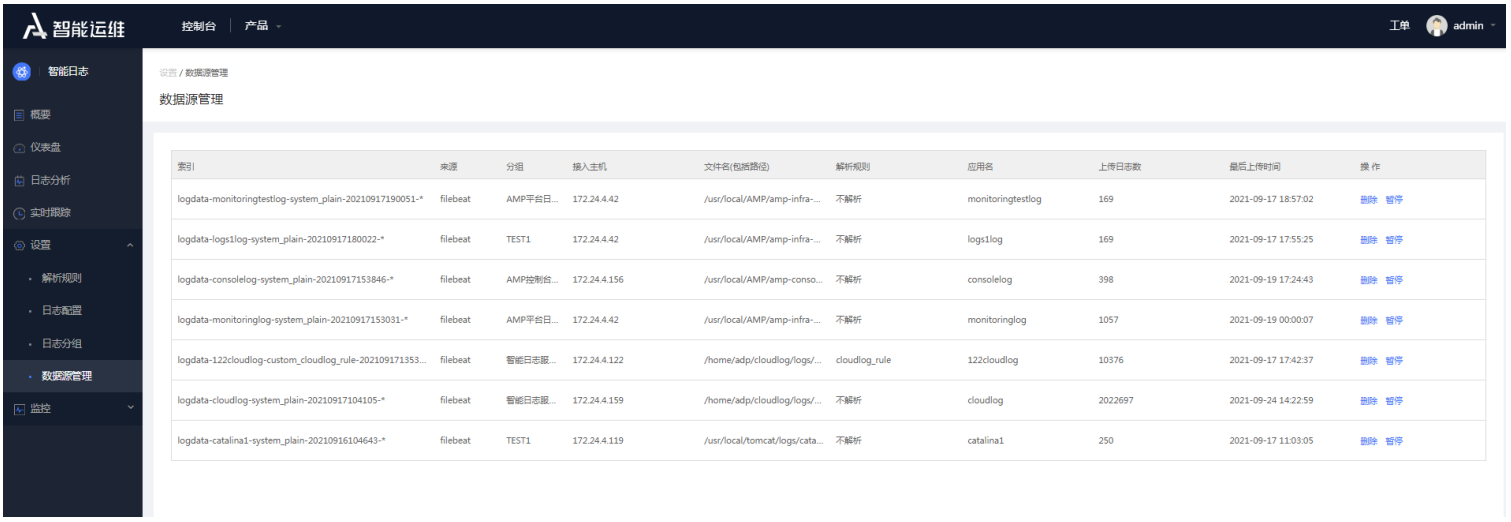


图4- 22数据源列表

6 日志分析

日志分析功能分为两部分，包括你日志搜索，以及根据搜索结果进行统计分析。

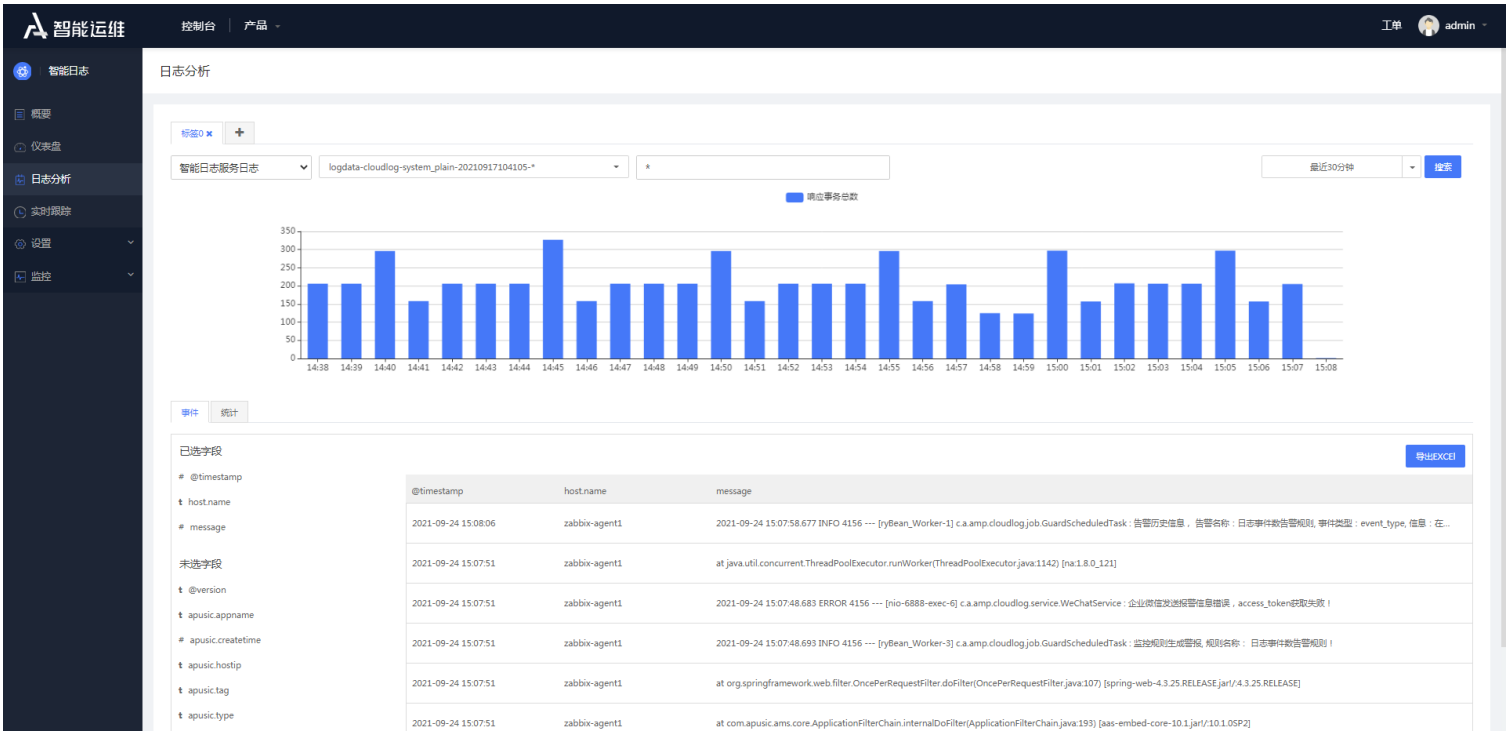


图4- 23日志分析

- **日志搜索**

日志搜索提供了功能强大、简单易用的方式来检索日志，可以快速过滤并找到相关的结果。

搜索条件包括：

1、日志分组：选择日志分组，进行筛选日志数据源

2、数据源：选择数据源对应的索引名称。

3、搜索条件：在搜索框中输入搜索语句。搜索语句支持Lucene语法对日志进行实时搜索。

4、时间范围：快速选择时间或者自定义时间区间。

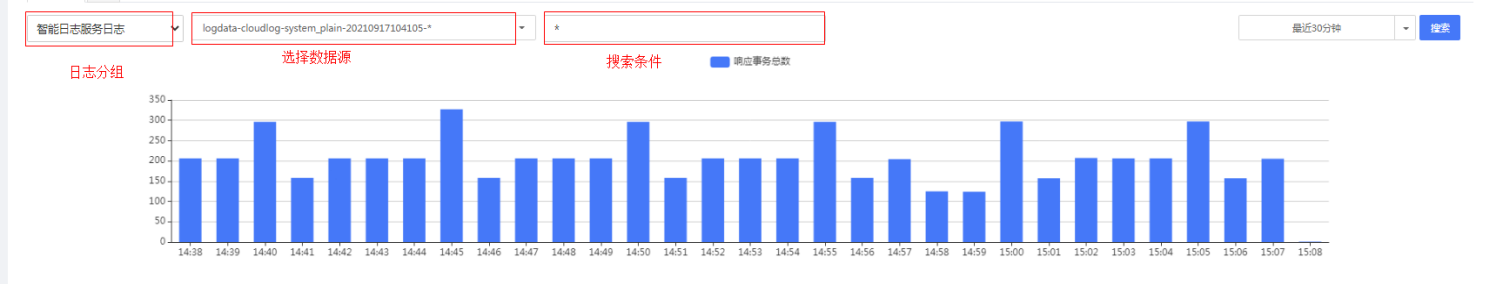


图4- 23统计图

点击"搜索"后，会展示根据搜索条件过滤后事件统计图。如下：

表格字段过滤：在页面左侧的字段列表中，可以过滤表格中显示的字段值。默认显示@timestamp、host.name、message这三个字段值。

需要选择其他字段在未选字段列表中点击"+"进行添加字段，同样，在已选字段列表中也可以点击"-"进行删除字段：

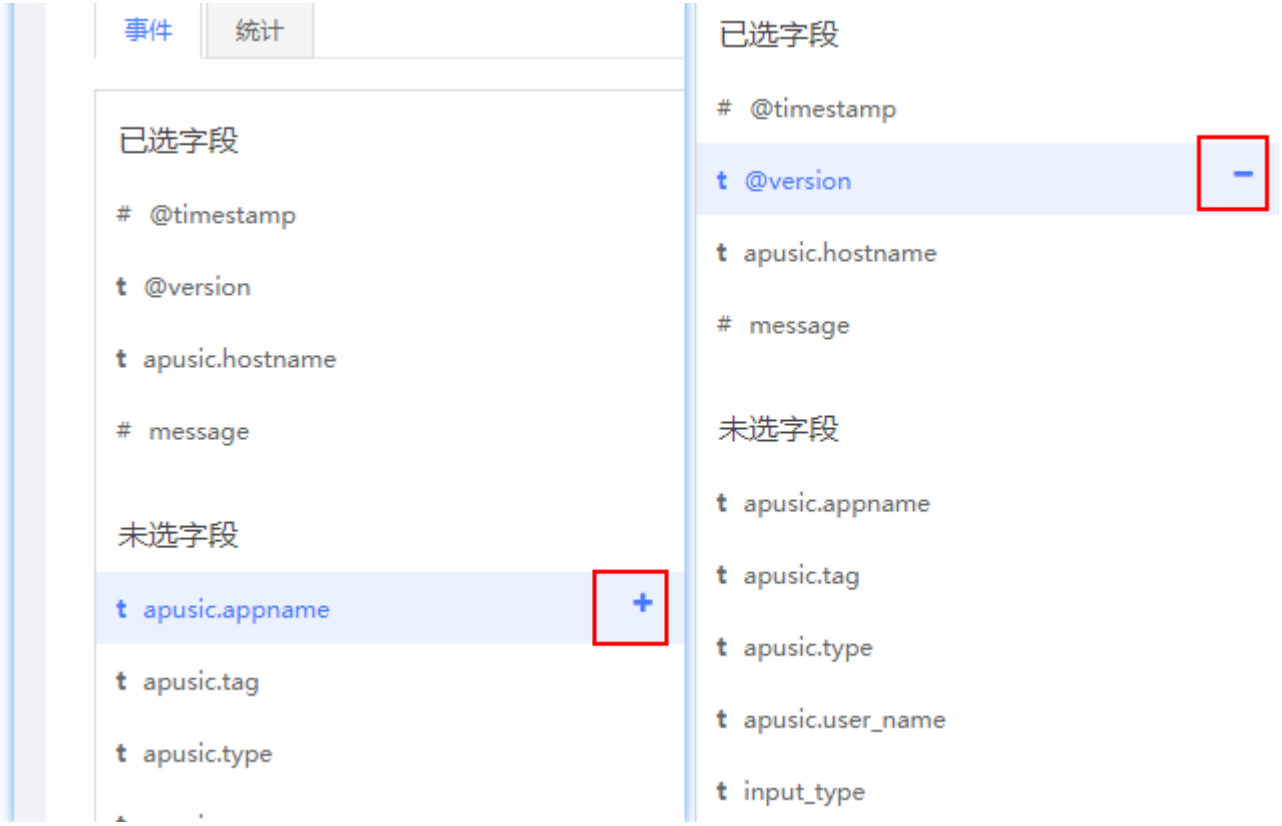


图4- 24过滤字段

- **统计分析**

统计分析是针对搜索结果创建不同展示方式的统计图表，目前支持的统计图有：事件统计，时间分段，数值分段，字段值分类等。

- **事件计数**

事件计数是在当前搜索结果中针对不同的字段值进行事件数量的统计，包括总数量（相当于SQL语句中的 count），和独立值数量（相当于SQL语句中的count distinct）。通过事件计数的统计分析，可以探索不同字段的事件数的分布情况。

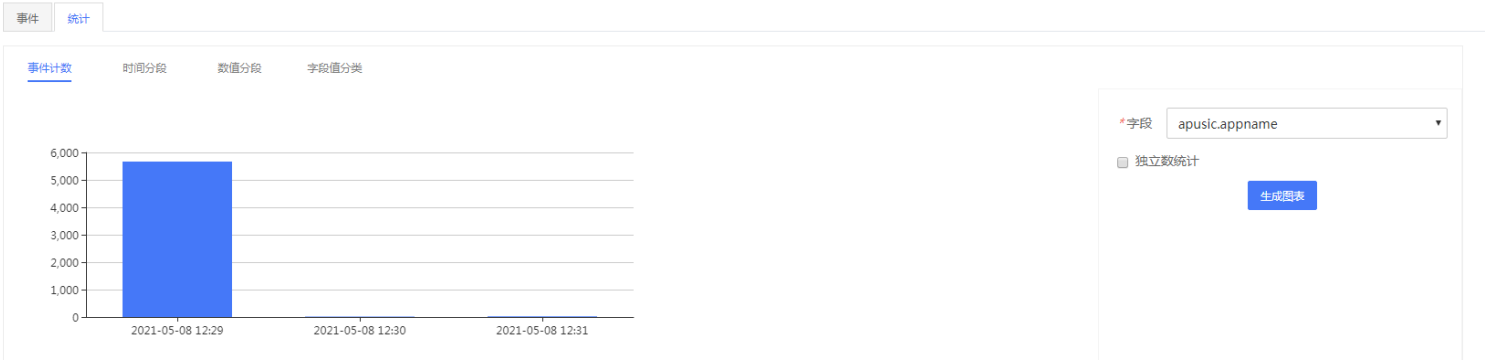


图4- 25事件计数

- **时间分段**

时间分段是自定义不同的区间对事件进行统计分析，并且支持总计（sum），最大值(max)，最小值(min) 和平均值(avg)统计。时间区间维度可以任意指定，统计字段则只支持数值型，不支持字符型。

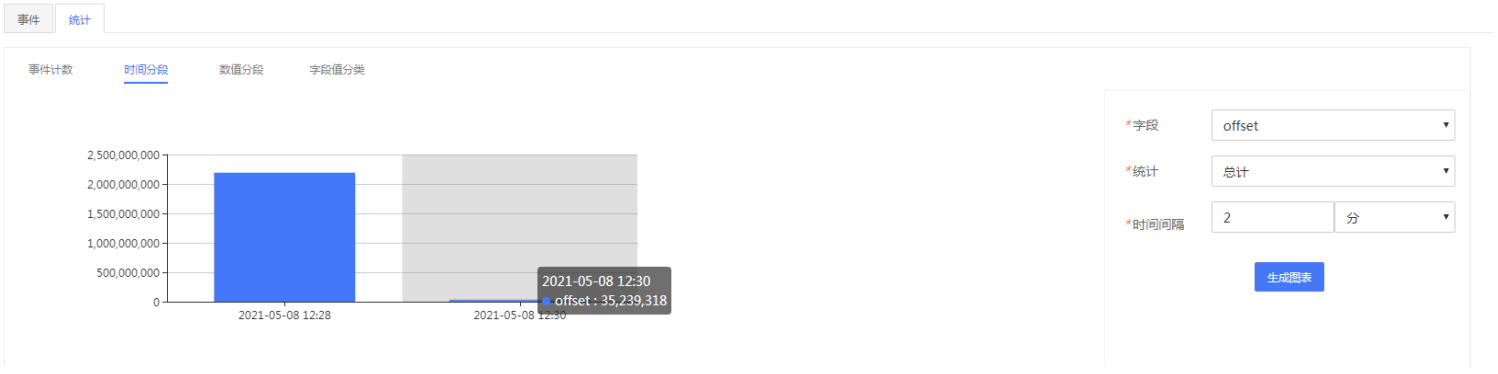


图4- 26时间分段

- **数值分段**

数值分段和时间分段类似，不同的是分段维度。前者是根据数值来分段，后者是根据时间来分段。

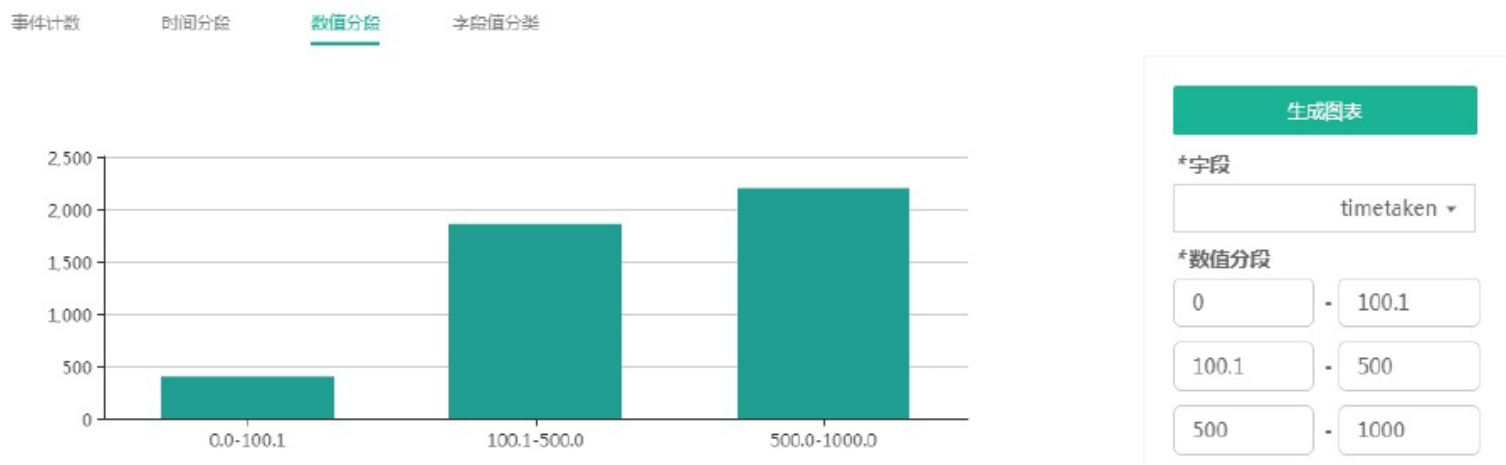


图4- 27数值分段

- **字段值分类**

字段值分类对于分析字段的具体值分布的情况非常有用。可以指定任意字段，将TOP N的值得数量以直方图的形式展示出来。

图4- 28字段值分类

7 实时跟踪

实时跟踪是用户可以根据数据源、主机名进行筛选查看实时日志。功能类似于在服务器上对日志执行tail -f filename.log，现在通过浏览器也可以达到同样的效果。

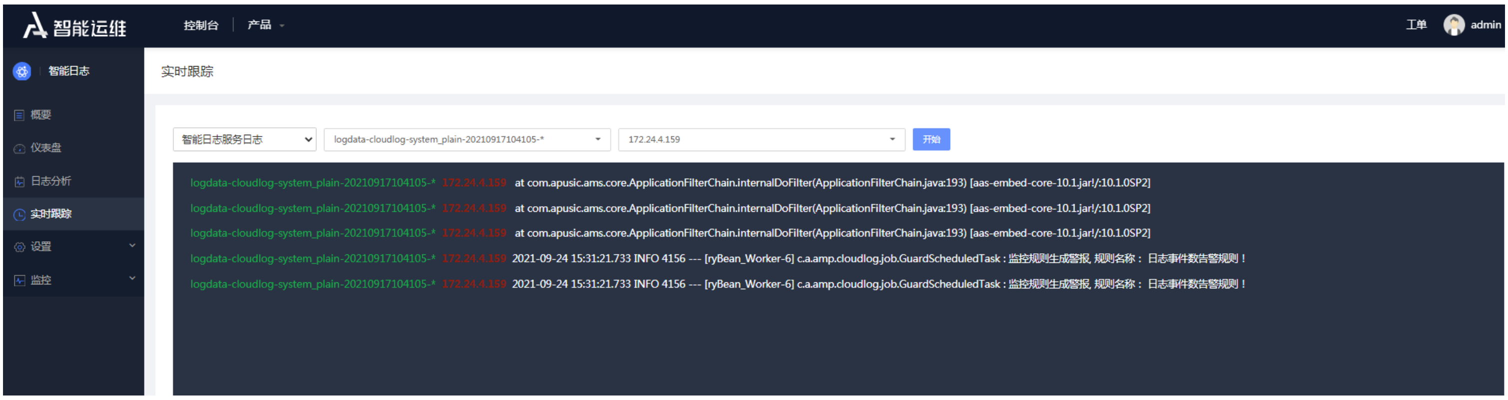


图4- 29实时跟踪

8 监控

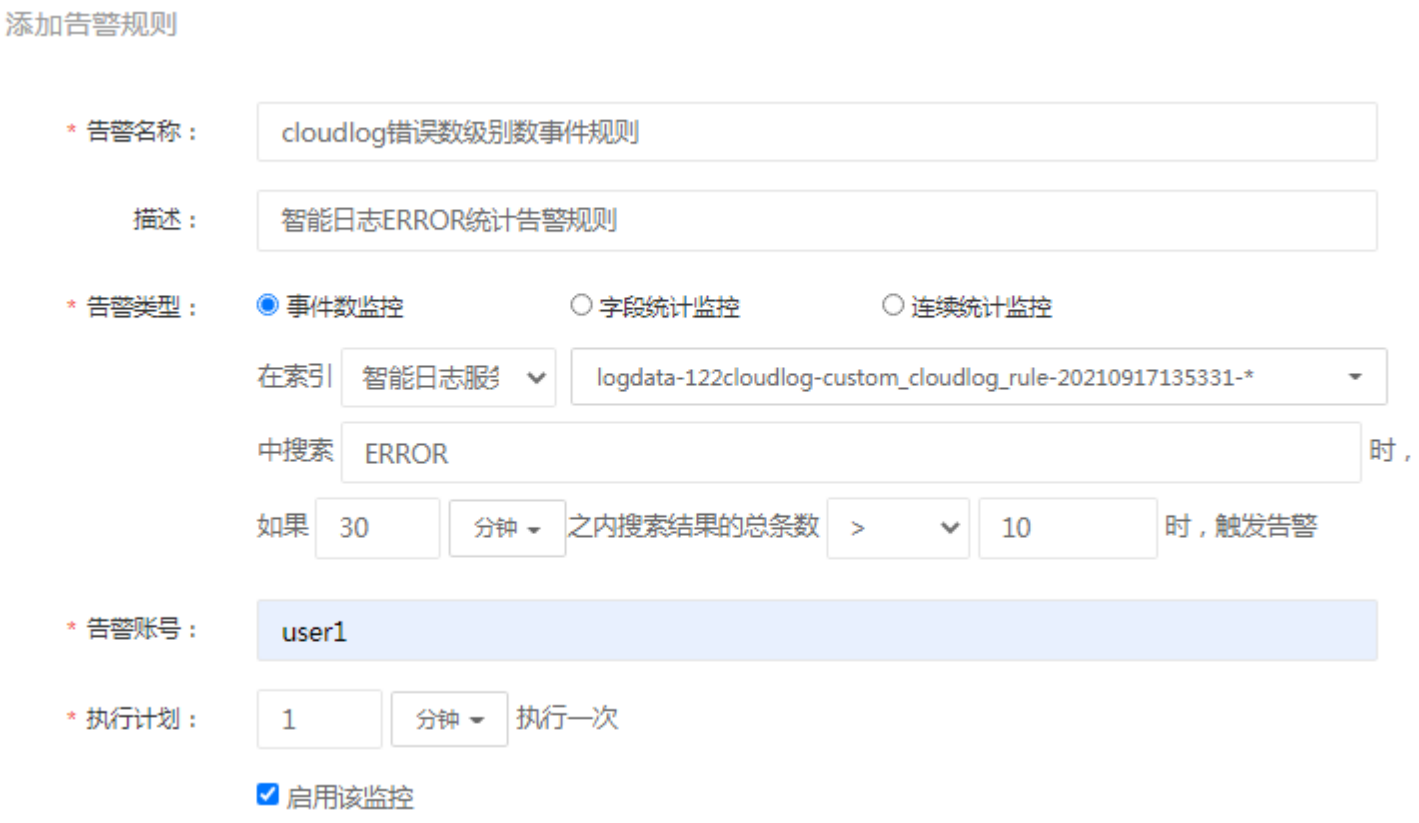
8.1 告警规则

目前智能日志的告警规则类型分为事件数监控、字段统计监控和连续统计监控三种。

- 添加监控

1. 事件数监控：在给定的时间范围内搜索结果的总数达到阈值，则触发告警。如：在2分钟内，搜索条件为"ERROR"的日志出现次数超过10次，触发告警。

搜索条件遵循lucense语法，搜索条件条件为"ERROR"的意思是判断采集到的日志出现ERROR的日志信息。搜索条件也可以为"loglevel:ERROR",其中loglevel是采集到的日志信息根据解析规则解析出的日志级别字段，搜索该字段出现"ERROR"的次数。这种搜索条件依赖日志的解析规则，需要根据根据具体的解析字段进行设置。



2、字段统计监控：在触发条件中填写你需要监测的字段，当该字段在一段时间出现的次数达到阈值，则出发告警。如：在5分钟内，字段timetaken（响应时间）的平均值超过200时，触发告警。

3、连续统计监控：当触发条件中需要监测的字段，在某个时间内连续出现次数达到阈值，则触发告警。

如：在5分钟内，字段timetaken（响应时间）的值超过200的次数超过5次时，触发告警。

智能日志平台支持针对搜索条件触发式的监控告警，告警条件触发以后，可以通过企业微信发送给预先设置的告警接收人。

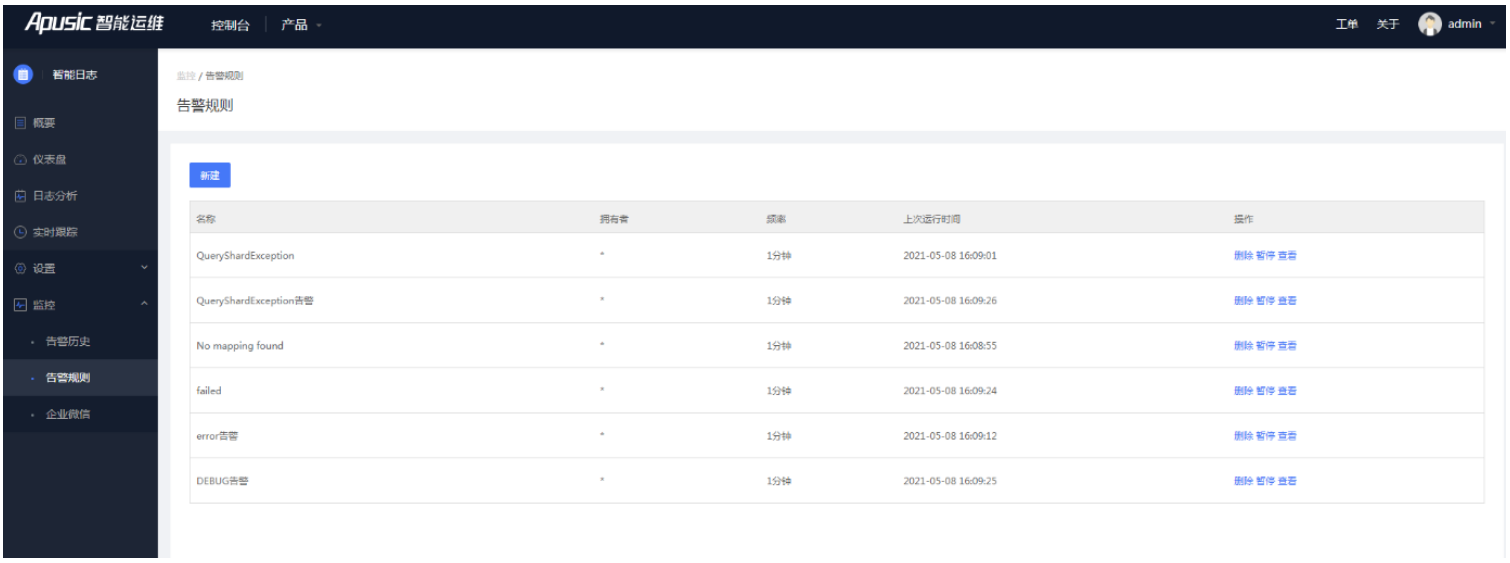


图4- 30告警规则

8.2 告警历史

告警历史展示告警趋势图及系统触发告警的列表。

图4- 31告警历史

告警趋势图可以查当天，本周，本月的告警情况。

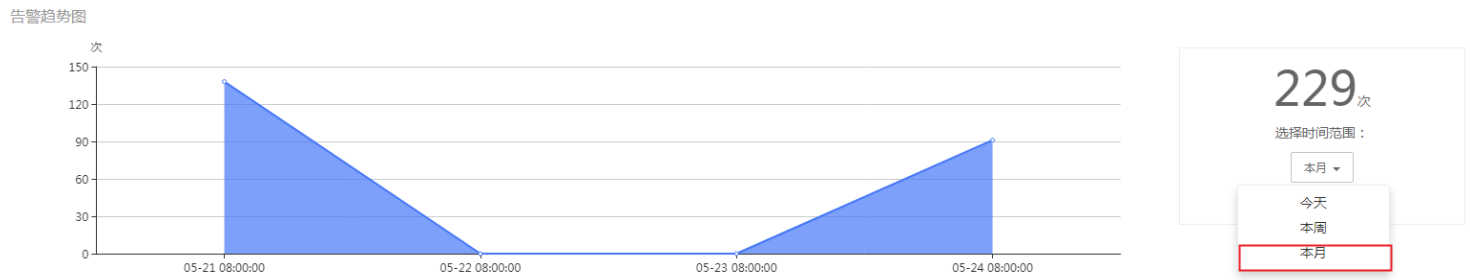


图4- 32告警趋势

具体的告警详情可以查看列表。

8.3 企业微信

智能日志支持使用企业微信发送告警信息。用户需要先前往企业微信注册账号：

注册完成后，用户需要使用 AgentId 、 Corpid 等信息在智能日志中完成企业微信的配置。点击"编译"按钮。

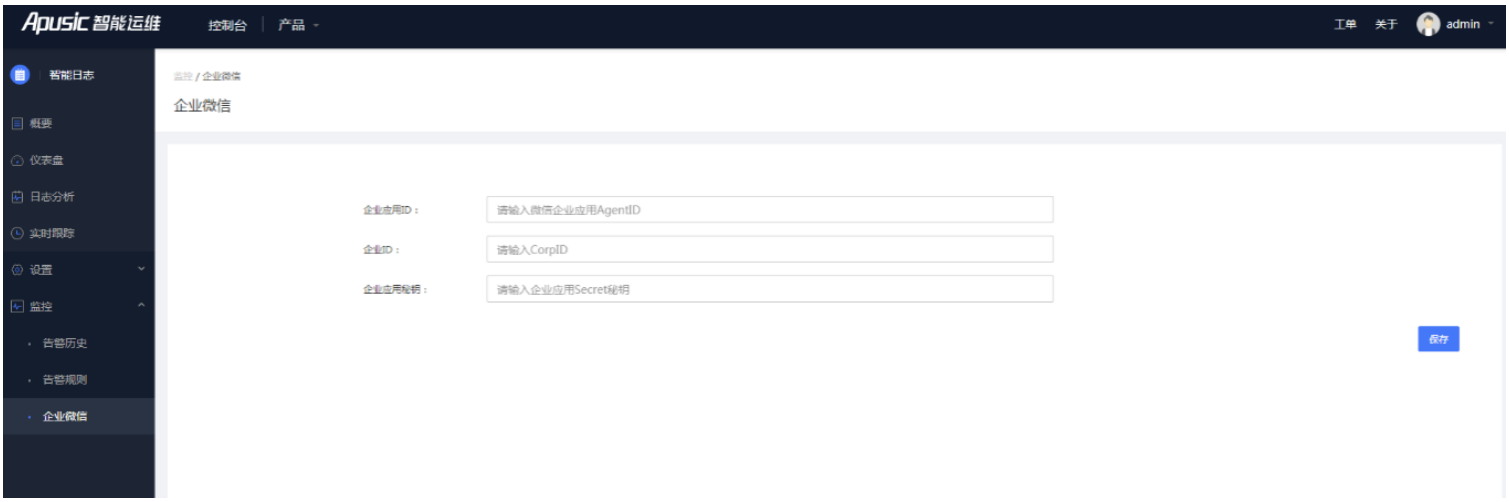


图4- 33企业微信

填写对应信息，点击"保存"，企业微信配置成功。

用户可以在企业微信中维护成员信息。企业微信的使用请参考腾讯的帮助文档。

8.3.1 K8s日志采集说明

9 K8s日志说明

智能日志支持k8s（Kubernetes）环境下日志数据的采集，分析，展现。对于k8s环境中应用日志的采集说明如下。

使用filebeat采集k8s环境下应用日志，通过daemonset的方式，在集群中的每个节点上运行一个采集节点，采集位于/var/log/containers/*.log下k8s的日志，最后将k8s环境下的日志信息采集到日志系统中。

采集k8s环境下采集日志前置条件：

- 需要用户先安装k8s集群环境，docker工具等。
- K8s环境下pod日志需要标准输出容器终端。

10 产品介质说明

1.k8日志采集相关安装介质。

解压安装完成日志服务后，从 cloudlog/public/k8sfilebeatimages路径下如下获取安装包，路径中cloudlog即是日志服务安装包解压后的目录。

- amp-cloudlog-k8s-filebeat.tar.gz

安装k8s应用日志采集的产品介质包

2.amp-cloudlog-k8s-filebeat.tar.gz产品安装包解压后，可以看到下面几个具体的安装包文件：

文件名 | **说明** apusic-filebeat-amd64.tar | Filebeat的amd64（x86_64）产品镜像包 apusic-filebeat-arm64.tar | Filebeat的arm64（aarch64）产品镜像包 K8s-daemonset-filebeat.yml | Filebeat镜像的启动配置文件 addK8sDataSource.sh | 添加注册k8s数据源的脚本文件

11 安装K8s日志采集组件

11.1 加载filebeat镜像

1.上传k8s日志采集组件安装包到服务器，进行解压安装包

解压产品安装包后，得到amd64和arm64版本的filebeat的安装镜像，安装配置文件，添加注册数据源脚本文件。

2.加载镜像

根据具体的环境加载对应的镜像，这里使用arm64环境下镜像进行说明。

成功加载镜像后，查看镜像，可以看到该镜像的具体内容如下。

如果用户的k8s环境存在dockerhub镜像仓库,可以将该镜像上传到镜像仓库，方便k8s集群中其他node节点直接使用。否则需要手动将该镜像上传到其他节点，再进行加载该镜像。

11.2 安装运行filebeat

11.2.0.1 修改filebeat配置文件

获取产品包解压后的amp-cloudlog-k8s-filebeat.tar.gz的配置文件K8s-daemonset-filebeat.yml，修改相应的内容。

1)修改日志数据索引名称apusic.type,如果只存有一个集群可以使用默认值不进行修改，如果多次添加时，需要进行修改。

apusic.type的组成由用户名（logdata），应用名apusic.appname（k8slog），解析规则（system_json_log）,创建时间apusic.createtime(创建时间可以根据添加时的年月日时分秒时间手动替换),使用连接符拼（-）接而成，如果进行修改需要保持一致。

如果进行多次添加时，需要同时进行修改apusic.appname，及apusic.type中的appname，保证应用名不重复。

2)修改kafka服务器的访问地址。

此处kafka的地址即是cloudlog配置文件application.properties中的kafka地址。

修改kafka服务的实际访问地址output.kafka下的hosts,如果是一个kafka节点，格式如下

hosts: ["172.20.140.93:9092"]。

如果是kafka集群多个节点，修改格式如下。

hosts: ["172.20.140.93:9092","172.20.140.94:9092","172.20.140.95:9092"]。

1.修改镜像文件版本。

默认使用arm64(aarch64)版本的镜像，如果服务器是该种环境，则不需要修改，可以跳过该步骤。

如果用户服务器是amd64(x86_64)环境，需要修改镜像的版本。

修改spec.containers.image的值为：apusic.net/filebeat-amd64:5.5.0

11.2.0.2 运行filebeat

进入k8s集群环境中，在服务器执行下列操作，运行filebeat容器服务。

执行上面命令后，filebeat会以daemonset的方式在k8s集群中的每个节点运行一个pod服务，每个pod运行一个filebeat容器，从而进行采集日志到日志系统。

此时执行命令kubectl get pods， 进行查看filebeat的pod节点，此时该节点可能处于ContainerCreating状态，这是正常情况，因为资源需要进行调度，需要花费时间，几分钟后进行查看，可以看到运行filebeat容器的pod节点正常运行。

11.3 注册添加k8s日志数据源

添加注册数据源到智能日志服务系统中，智能日志系统进行日志的查询，分析操作。

获取产品包解压后的amp-cloudlog-k8s-filebeat.tar.gz的脚本文件addK8sDataSource.sh，修改相应的内容。

11.3.0.1 修改注册数据源脚本

1.修改日志服务地址CLOUDLOG_SERVER为实际的服务地址

2.如果5.3.2.1下的apusic.type如果没有进行修改，则跳过。

否则，需要根据上一步进行修改下面配置文件中的APP_NAME等。

此处的创建时间CREATE_TIME需要与上一步配置文件中的保持一致。

11.3.0.2 执行脚本文件

执行脚本文件，进行注册添加数据源到智能日志系统。

如果文件没有可执行权限，执行下面命令，给该文件赋予可执行权限。

如果注册数据源成功，结果如下所示。

如果注册数据源失败，需要根据出错信息进行修改。

判断上一步5.3.2.1中配置信息是否与脚本中的参数对应一致。

执行成功后，可以看到日志服务的数据源管理界面已经存在k8s日志的数据源记录。

后续可以进行日志的查看，分析操作。

12 停止卸载K8s日志采集组件

停止k8s中filebeat日志采集组件采集日志信息

进入到启动filebeat容器的配置文件K8s-daemonset-filebeat.yml的所在目录。

执行下列命令

此时执行命令kubectl get pods， 进行查看filebeat的pod节点，此时该节点可能处于Terminating状态，这是正常情况，因为删除该节点需要对资源做一些处理，需要花费时间，几分钟后进行查看，可以看到运行filebeat的pod节点成功删除。

删除数据源

进入到日志服务的数据源管理界面，找到采集k8s应用日志的记录，点击该条记录后的"删除"按钮进行删除该数据源。

全国统一服务热线

4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。

Apusic 金蝶天燕

云计算国家标准制定企业

金蝶集团旗下基础软件企业

信息技术应用创新核心企业

官网：www.apusic.com