# 宸析全维度数据监测平台V1.0使用手册

1. 用户登录

浏览器输入地址，打开登录页面， 输入用户名与密码，点击登录按钮登录系统。

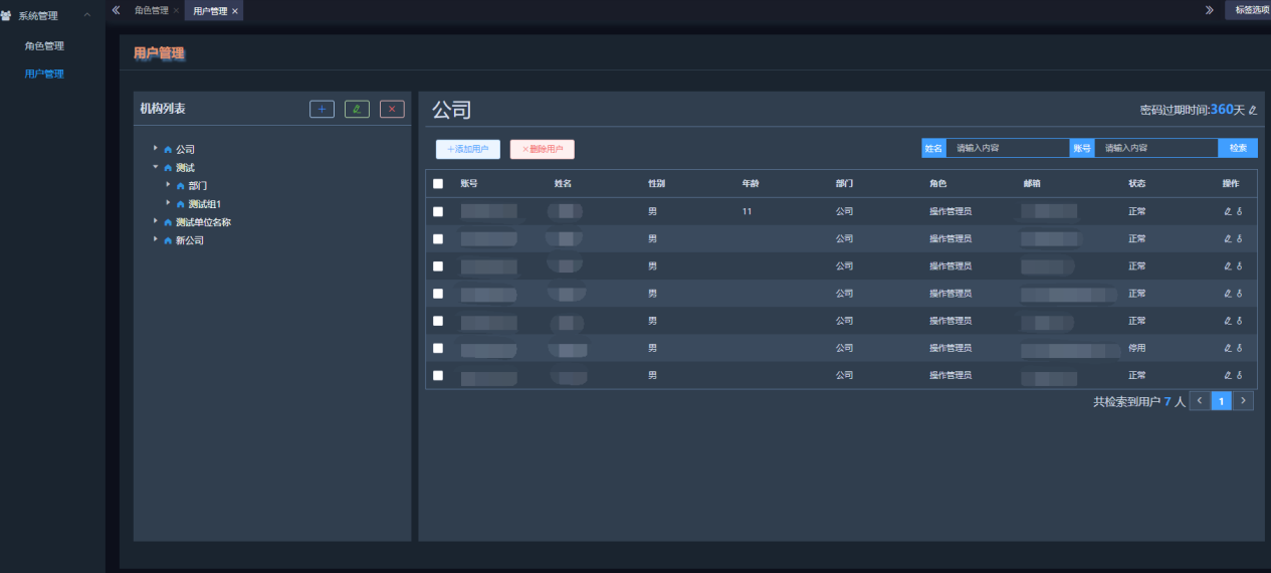


如果是第一次登录需要上传license，点击证书更新，选择证书文件，上传后关闭即可。

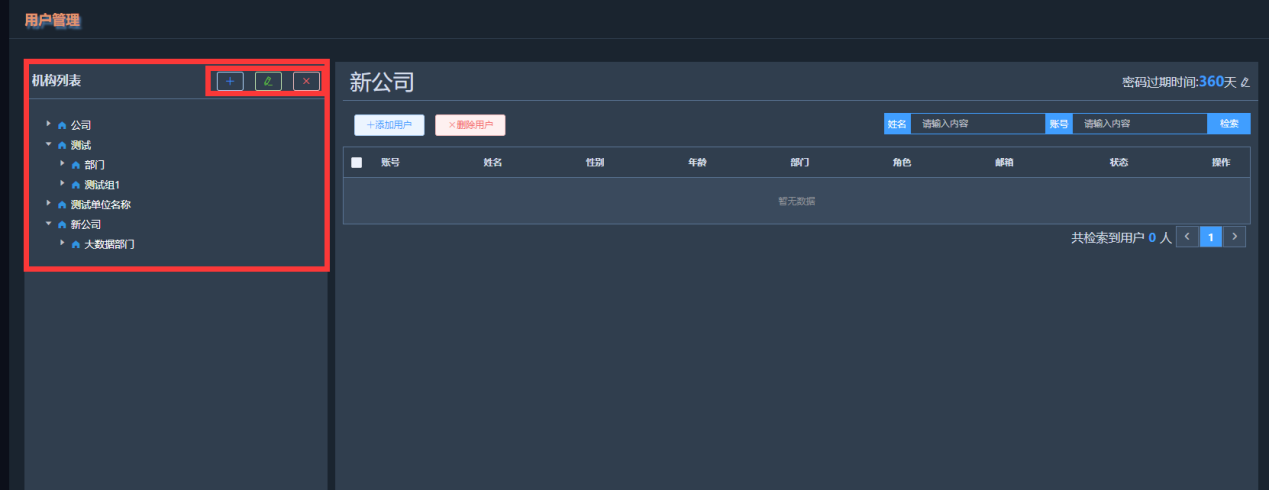


1. 系统管理
2. 用户管理

点击左侧用户管理，进入用户管理页面。



可以在机构列表部分对组织机构进行增、删、改的操作

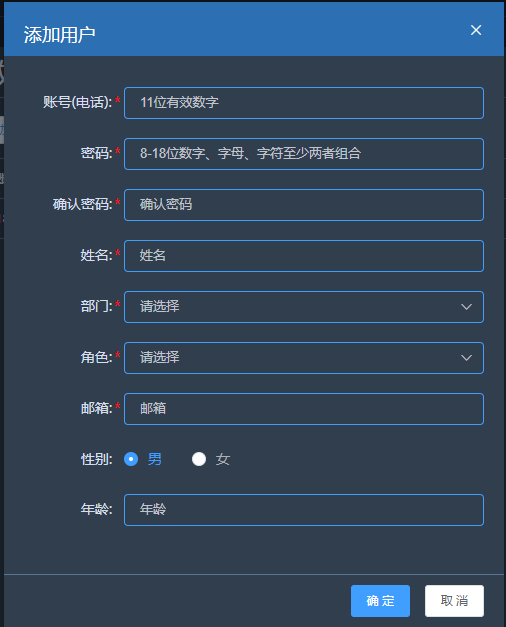




在用户管理页面的右侧可以进行用户的创建、修改、删除、查询、重置密码等功能。



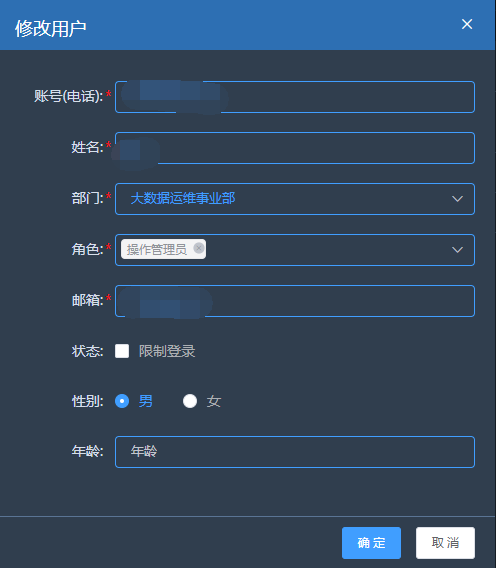
点击【添加用户】按钮，完善用户基本信息，点击“确定”后实现用户添加。



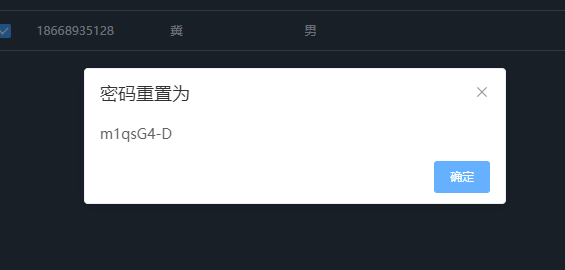
选择一个或多个用户，点击【删除用户】按钮，实现用户删除。



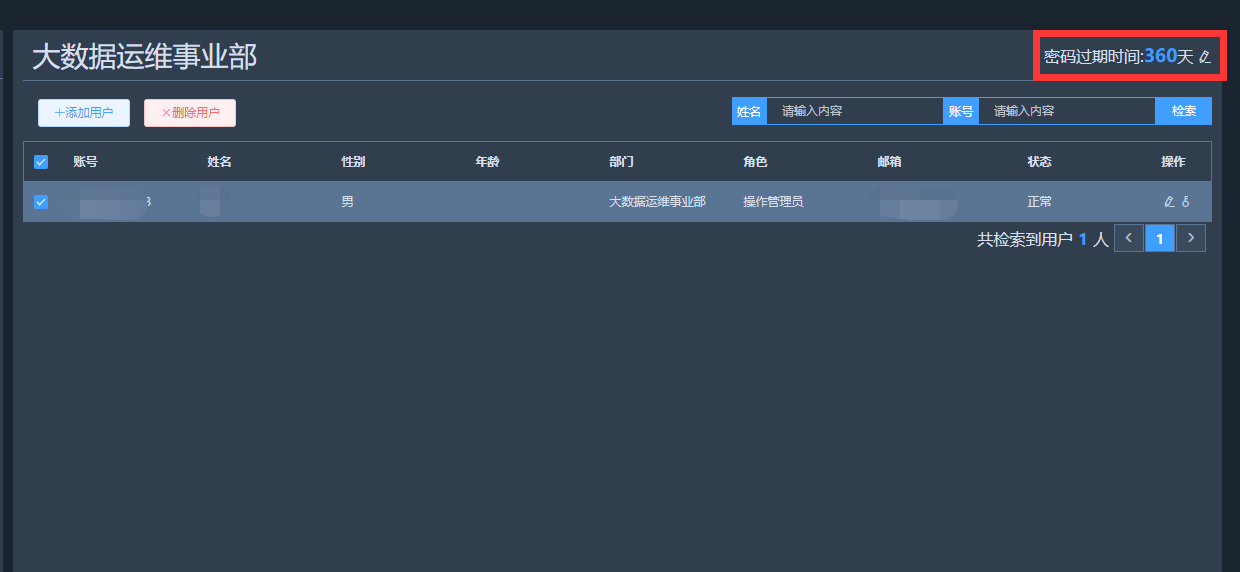
点击用户信息右侧“操作”栏下的按钮可编辑用户信息。



点击用户信息右侧“操作”栏下的按钮可重置用户密码。



为了保证用户密码的安全性，管理员可以设置密码过期时间，超过时间没修改过密码的用户，在登录时会强制修改密码。



1. 角色管理

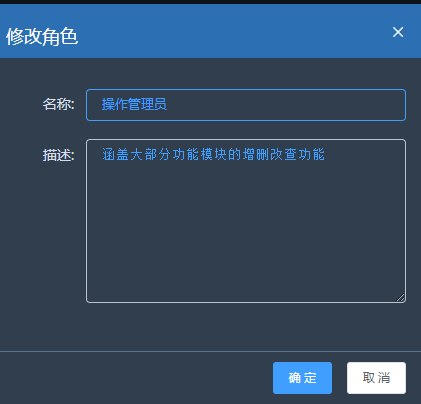
点击左侧用户管理，进入角色管理页面。



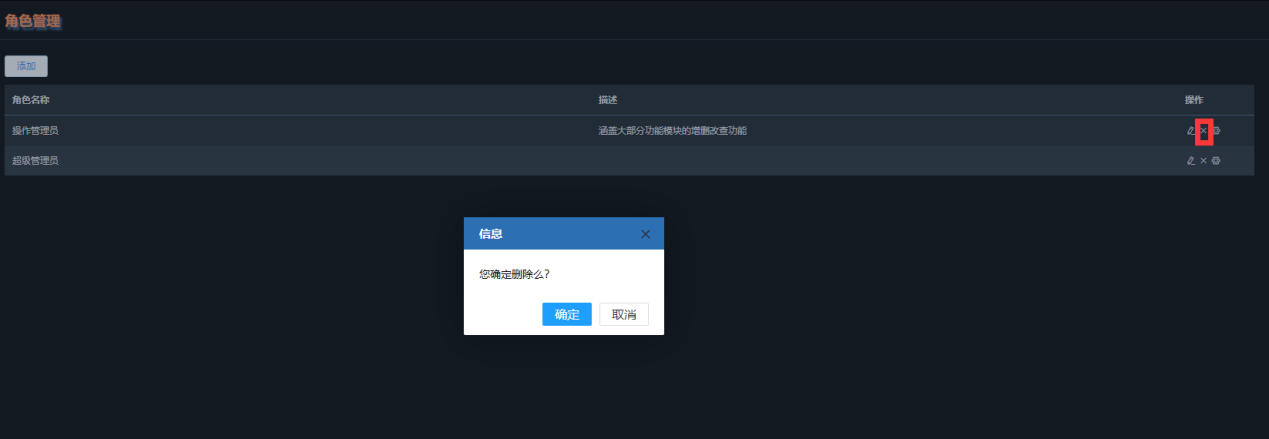
点击【添加】按钮，填写角色名称及描述，完成角色创建。



创建角色后，点击角色右侧“操作”栏下的可以编辑角色信息。



点击角色右侧“操作”栏下的可以删除角色。



点击角色右侧“操作”栏下的可以配置角色菜单。



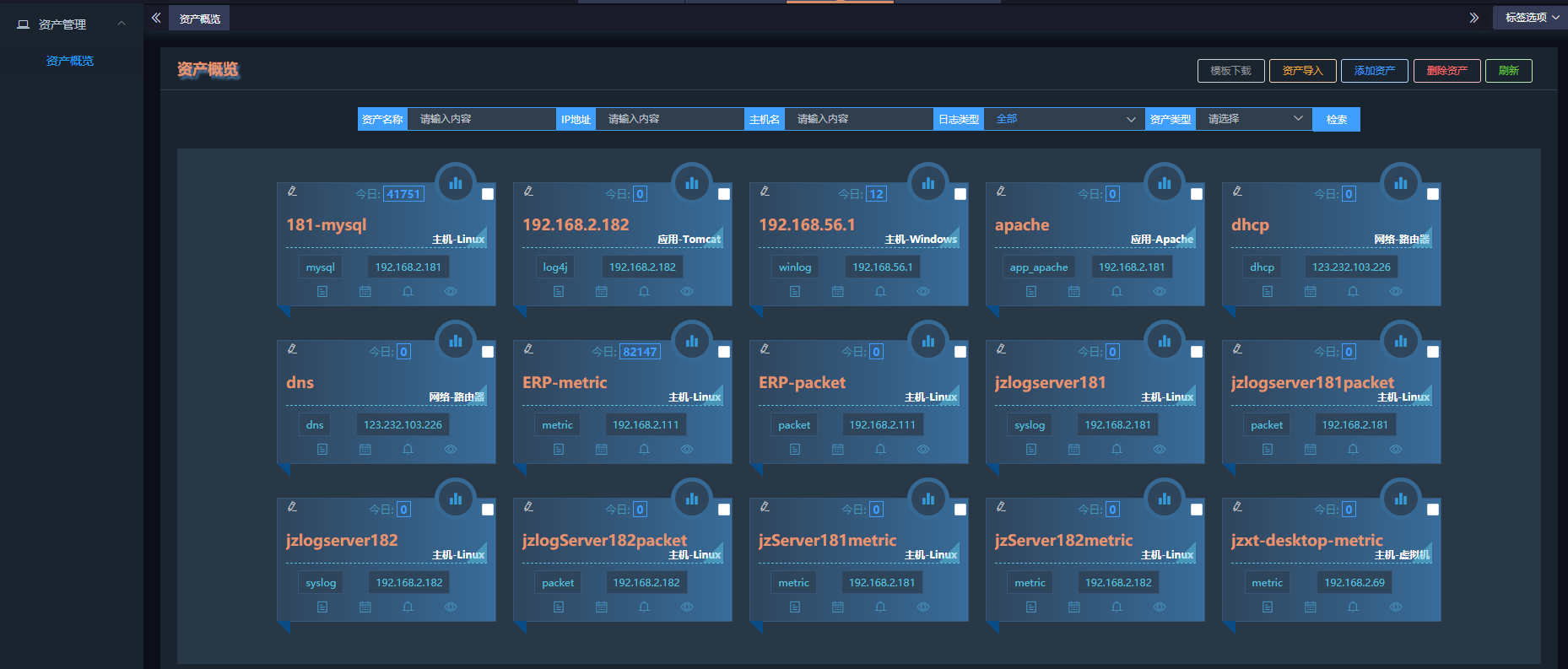
勾选菜单后，还可以设置该角色在响应菜单下的按钮的操作权限。



设置完成后，点击确定即可。当用户设置为相应角色后，登录账户只能看到设置的菜单和按钮。

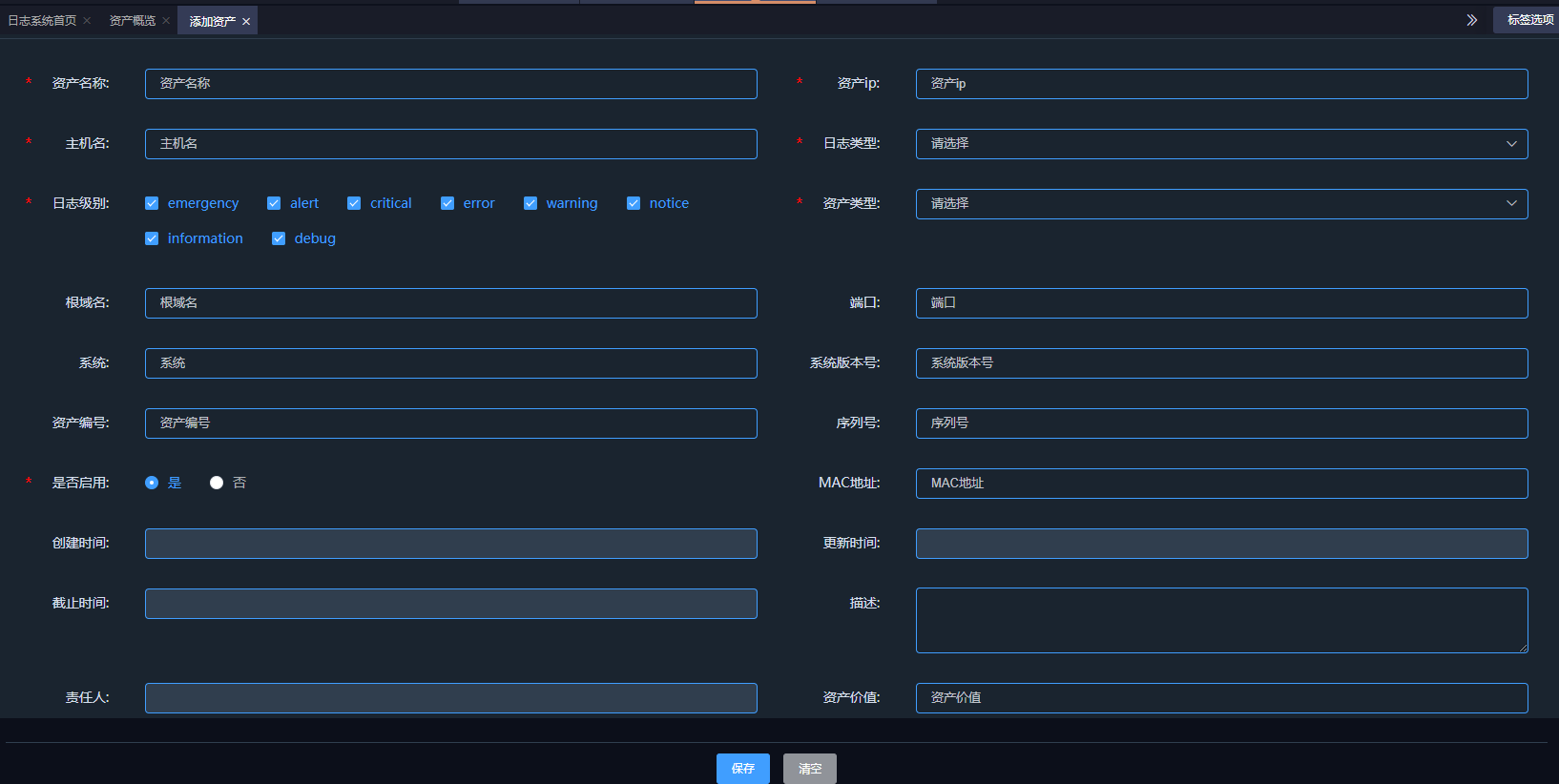
1. 资产管理

点击左侧菜单“资产管理”-“资产概览”，进入资产页面。



1. 添加资产

点击右上角【添加资产】按钮，输入资产的相关信息，即可完成资产添加。



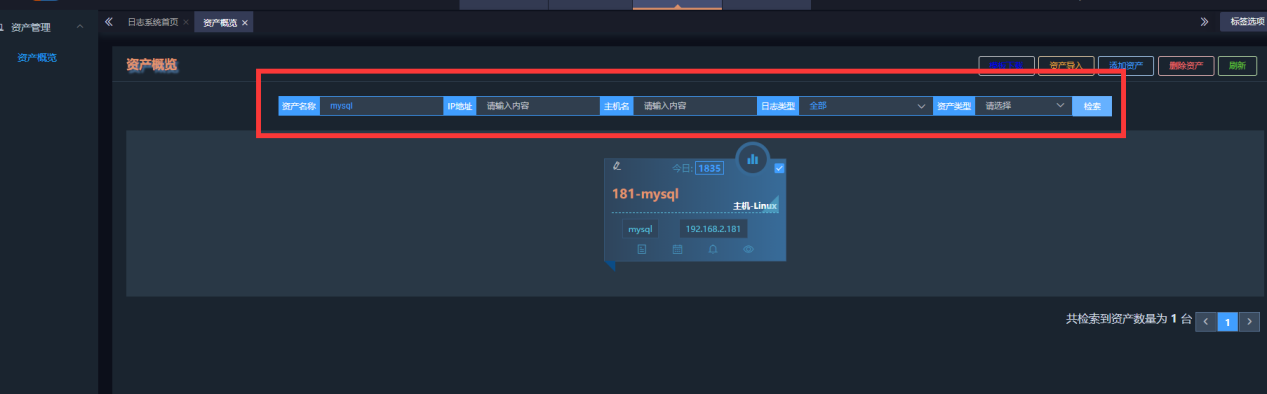
1. 删除资产

勾选资产右上角的选择框，支持多选，然后点击【删除】按钮，可以实现资产的删除。



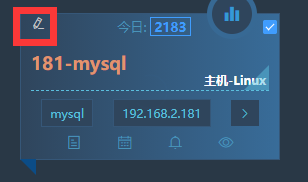
1. 查询资产

资产管理页面上方提供资产查询框，支持资产名称、IP地址、主机名、日志类型、资产类型的查询。



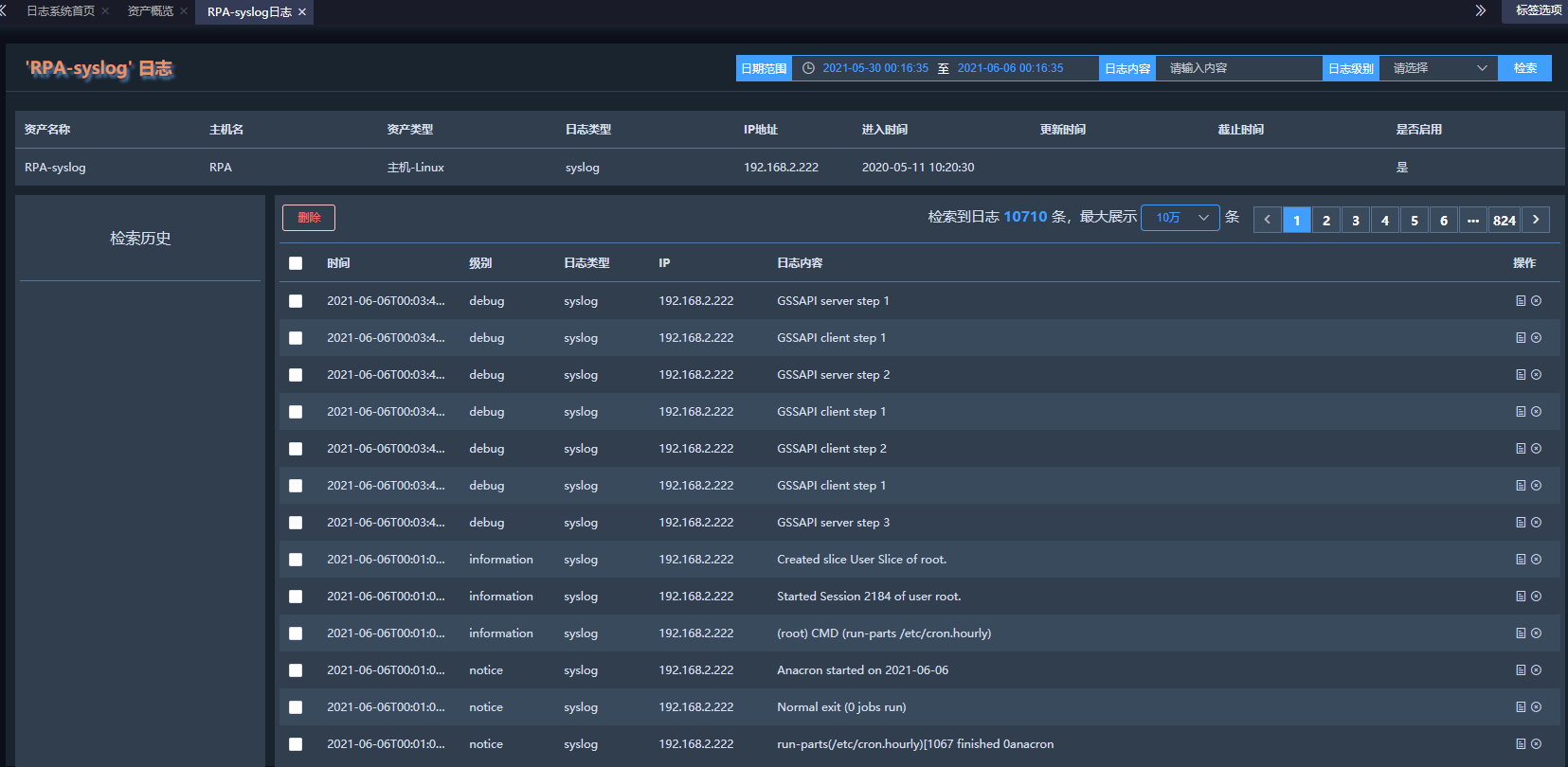
1. 修改资产

点击资产左上角的按钮，可以编辑资产信息，修改信息后，点击【保存】按钮即可。



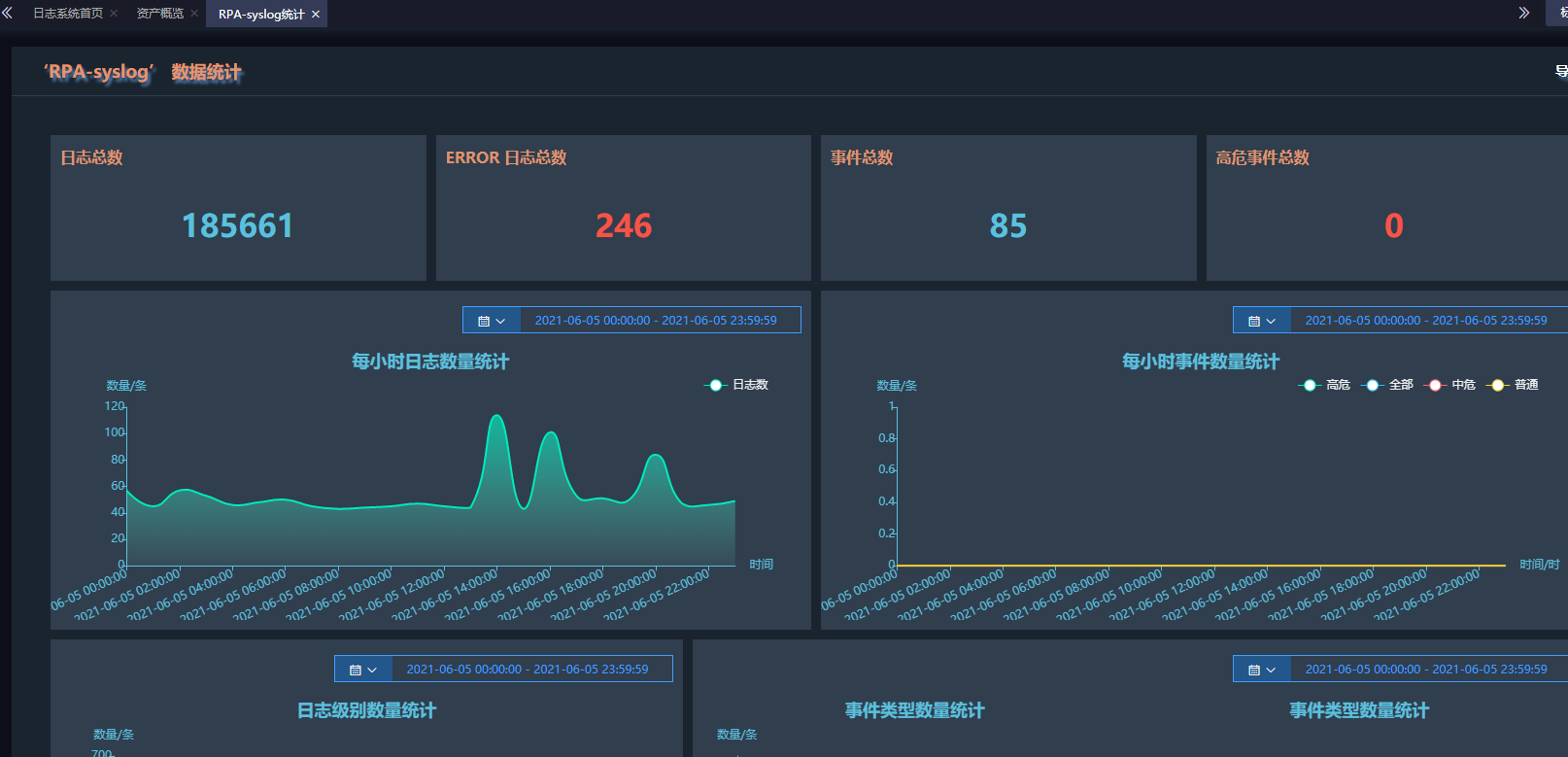
1. 查看资产日志

点击资产左下角的按钮可以查看资产日志信息。



1. 查看资产报表

点击资产右上角的按钮，可以查看资产报表。



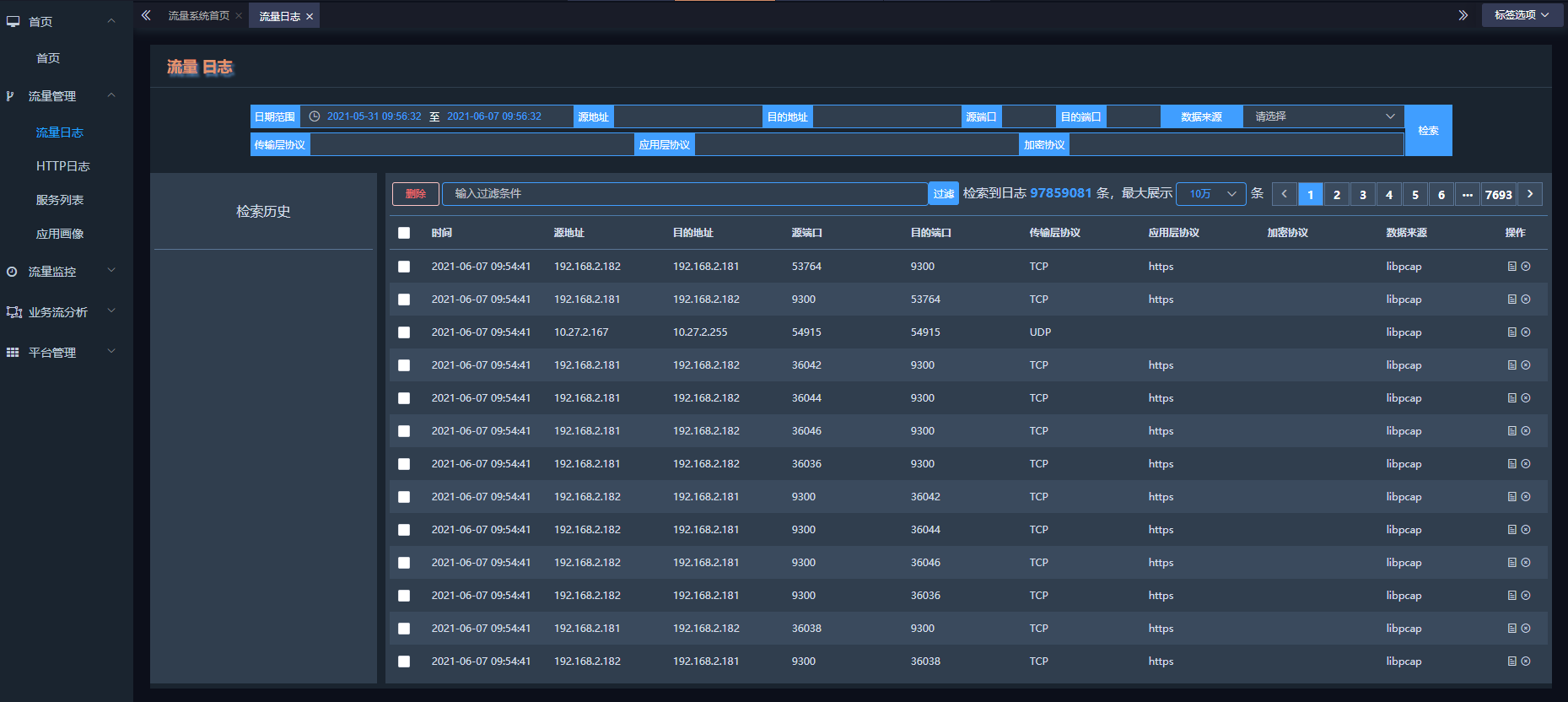
1. 流量管理
2. 首页

点击流量管理系统的“首页”，也可进行流量数据的概览。



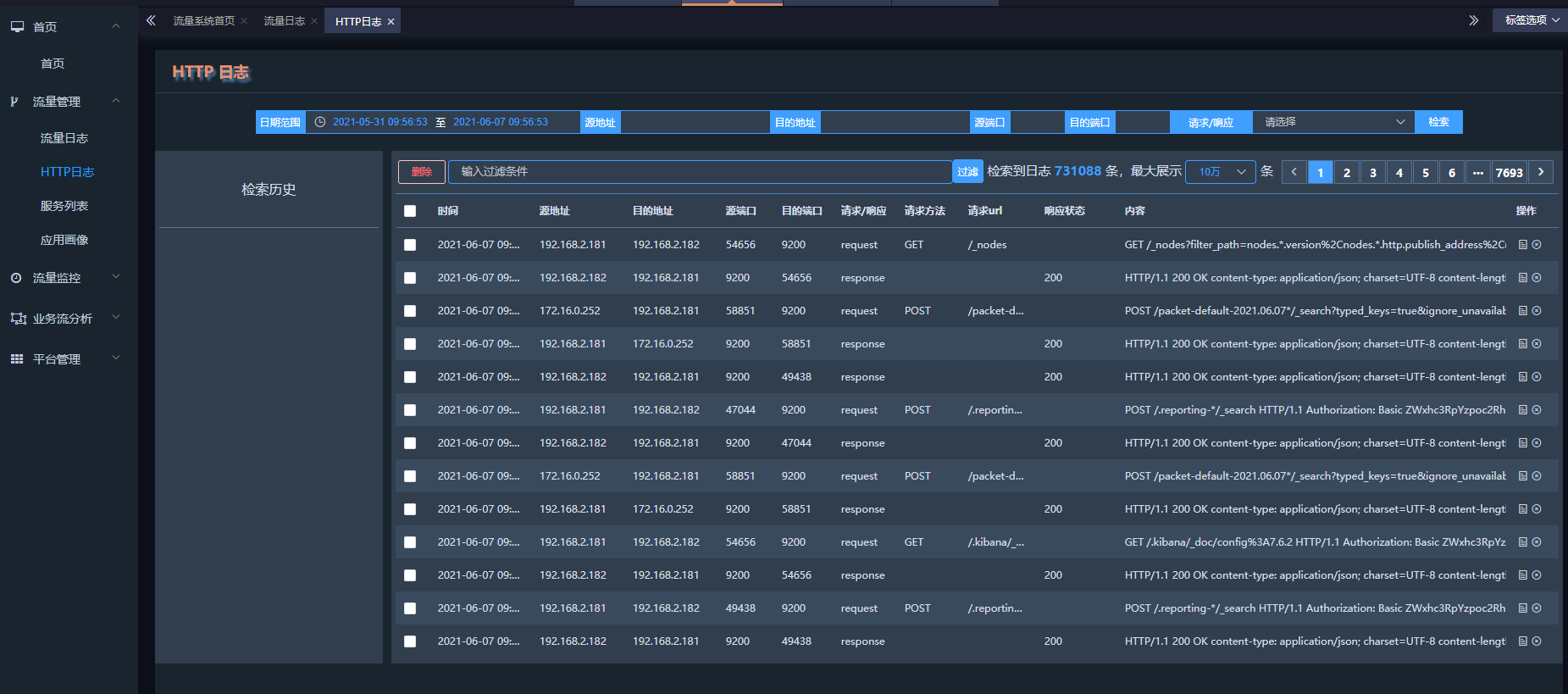
1. 流量管理
2. 流量日志

点击左侧菜单“流量管理”-“流量日志”，可以查看流量日志信息，并可以根据多个条件组合查询。



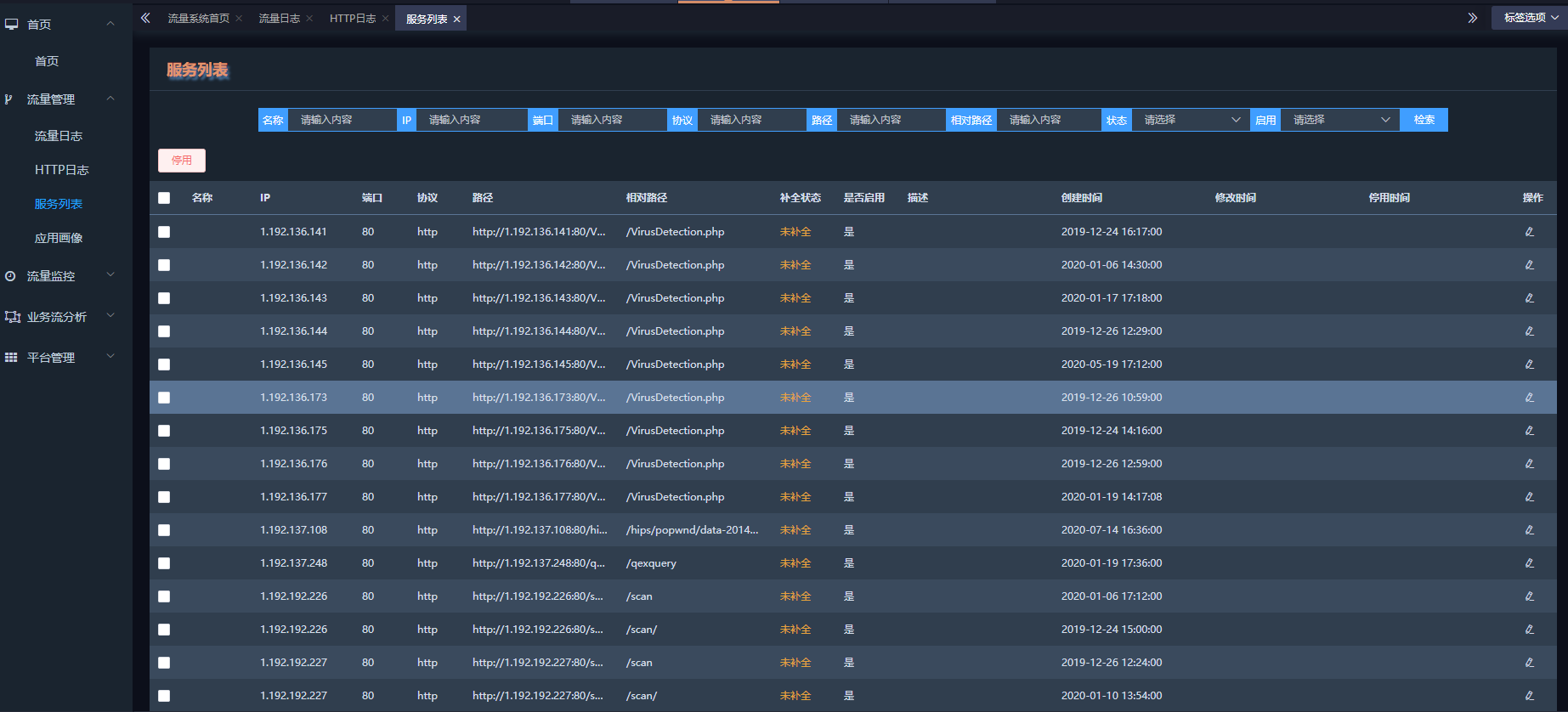
1. HTTP日志

针对流量数据中的http流量日志进行查看和查询。



1. 服务列表

通过对流量数据的分析，将其中与应用服务有关的数据进行解析，形成服务列表。



点击右侧的编辑按钮，，可以对服务信息添加名称标记，在后续的统计报表中可以查看相关的标记信息。



1. 应用画像

针对流量数据中分析出的应用访问信息，统计访问的URL TOP10。并可以对URL进行深钻统计分析。



1. 流量监控

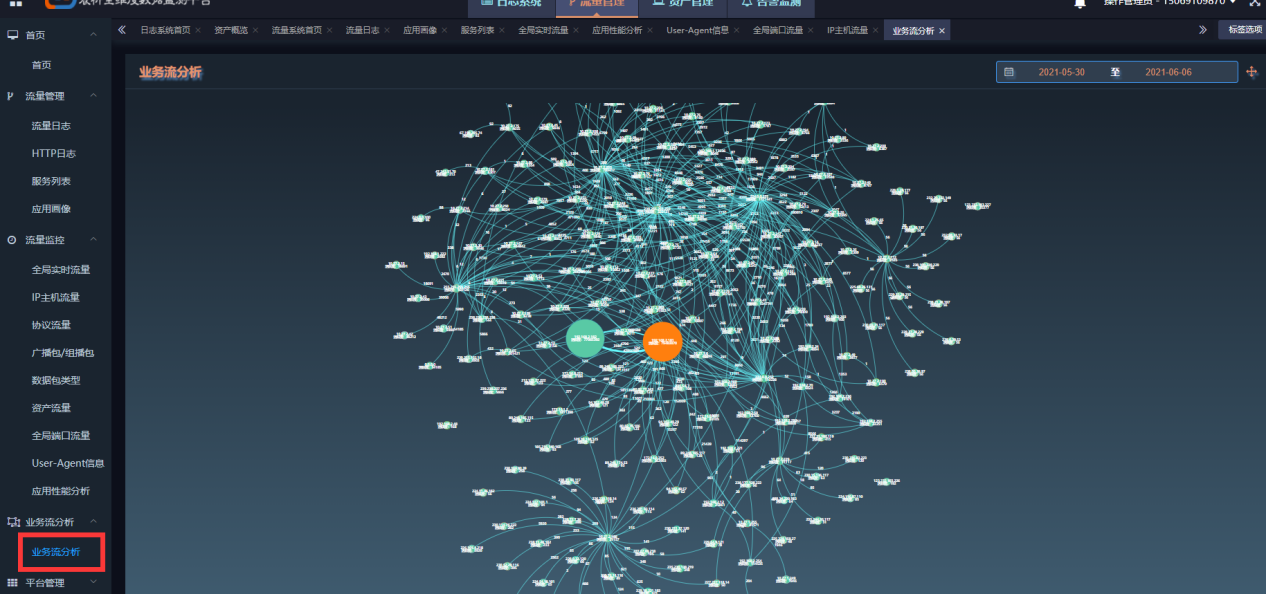
针对流量数据提供各个层面的统计分析报表。

包括：全局实时流量、IP主机流量、协议流量、广播包/组播包、数据包类型统计、资产流量统计、全局端口流量、User-Agent信息、应用性能分析。



1. 业务流分析

针对全局流量信息，对各个IP之间的流量进行统计，并进行展示。同时还可以通过点击IP地址或流量连线深钻到日志查询页面查看相应的流量日志。



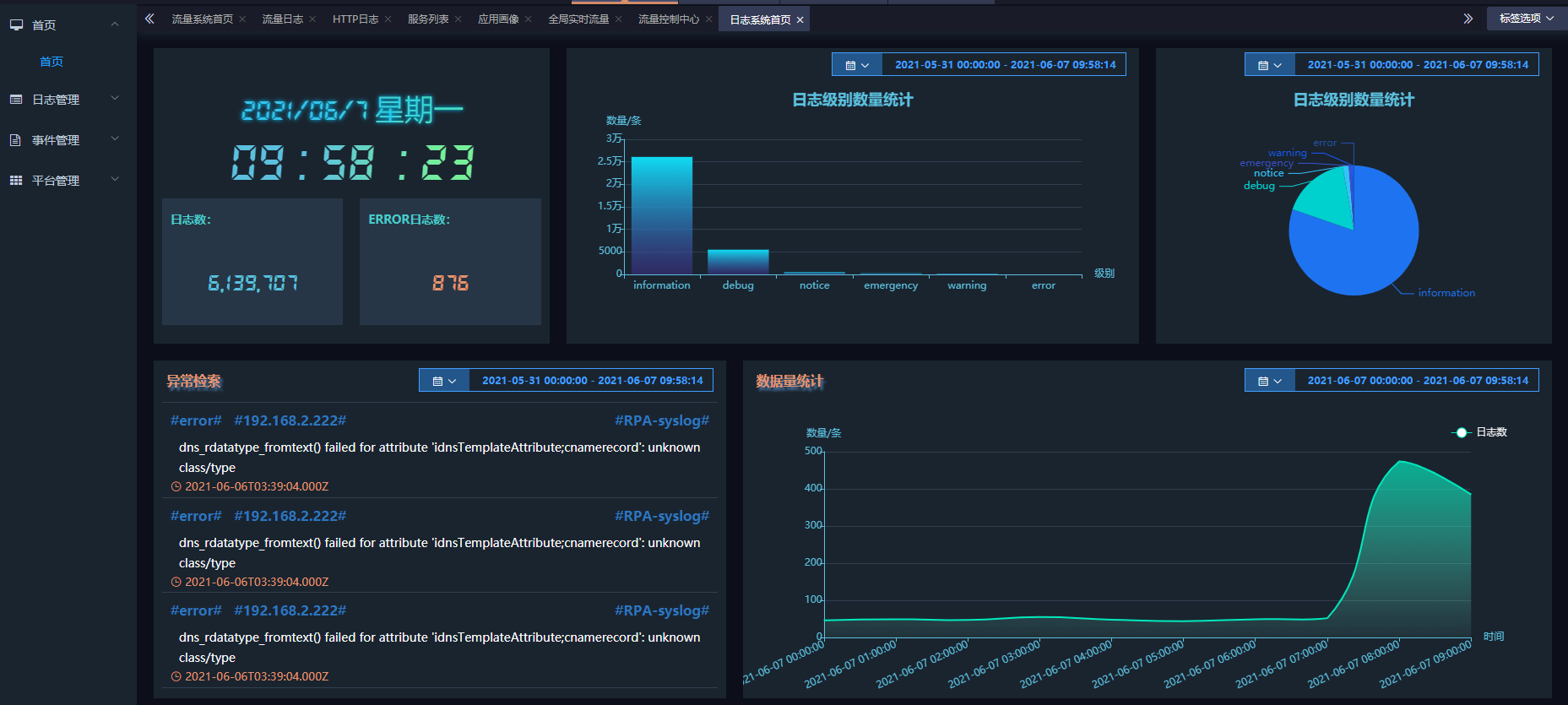
1. 平台管理

点击左侧菜单“平台管理”-“流量控制中心”可以对流量采集进行开启和关闭操作。



1. 日志系统
2. 首页

点击“日志系统”左侧菜单“首页”，可以查看日志系统部分的首页内容。

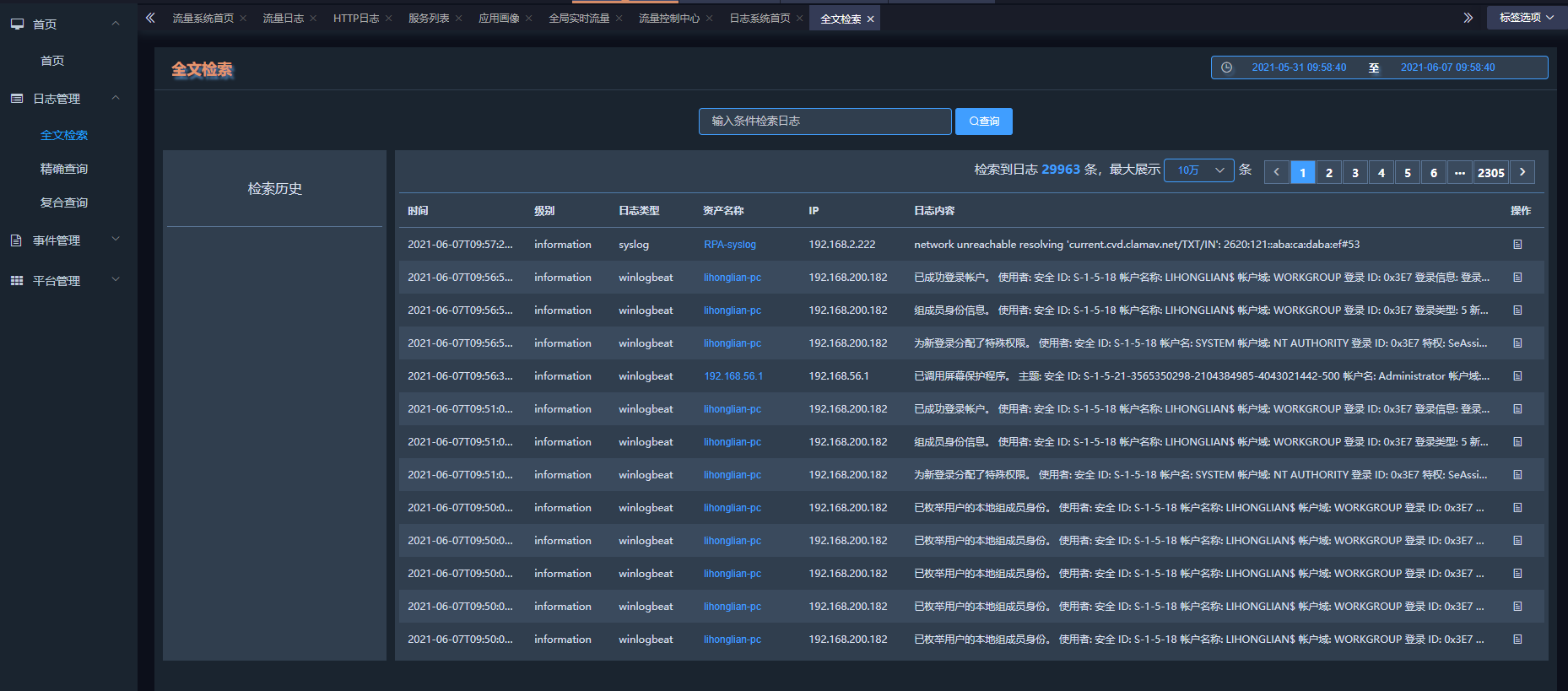


1. 日志管理

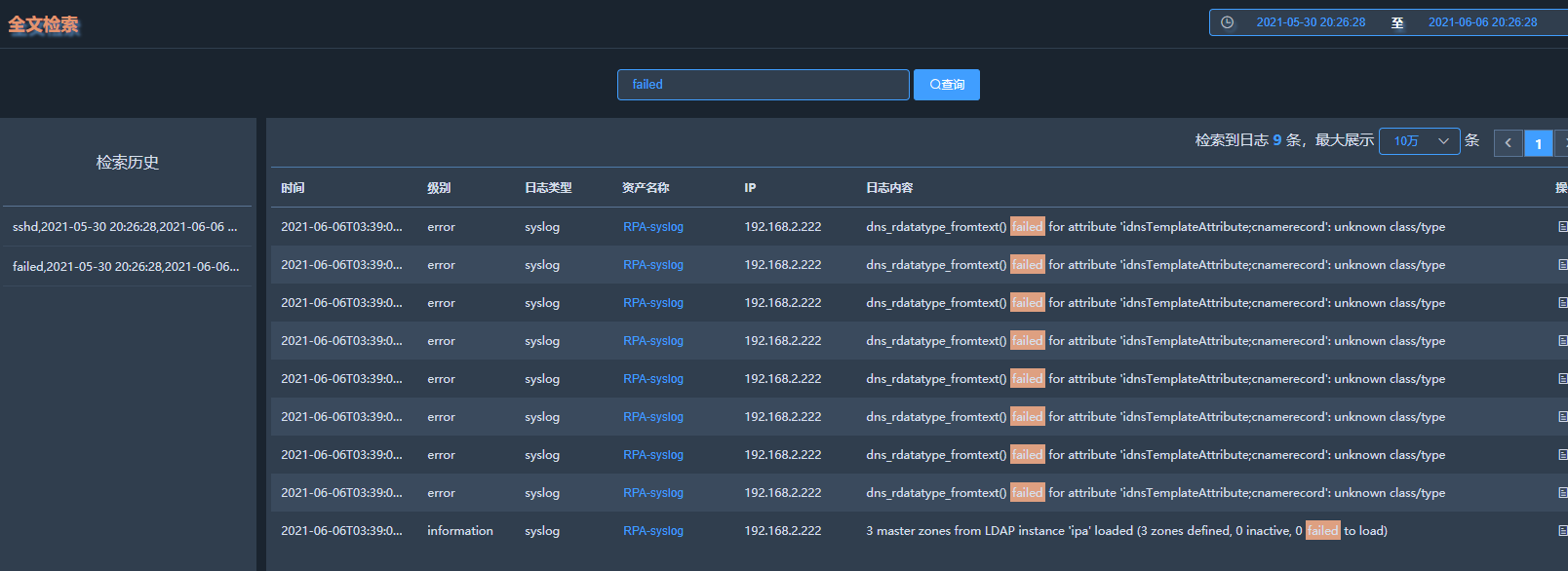
点击左侧菜单的日志管理，有全文检索、精确查询、复合查询三个功能页面。

1. 全文检索

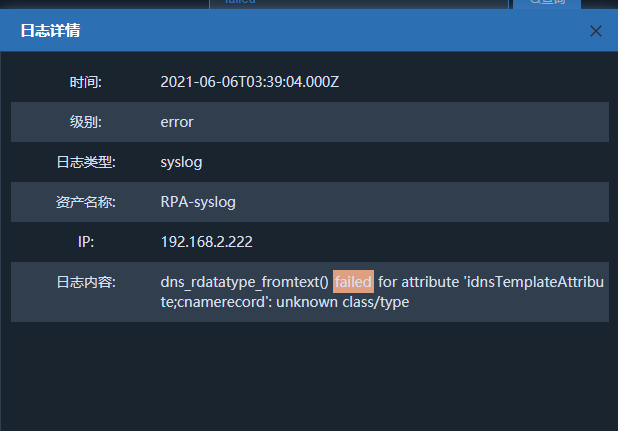
点击左侧菜单“全文检索”，进入检索页面。



可以在输入框中填写查询内容，系统会实现全文内容的快速检索，并对匹配的词语进行标记。

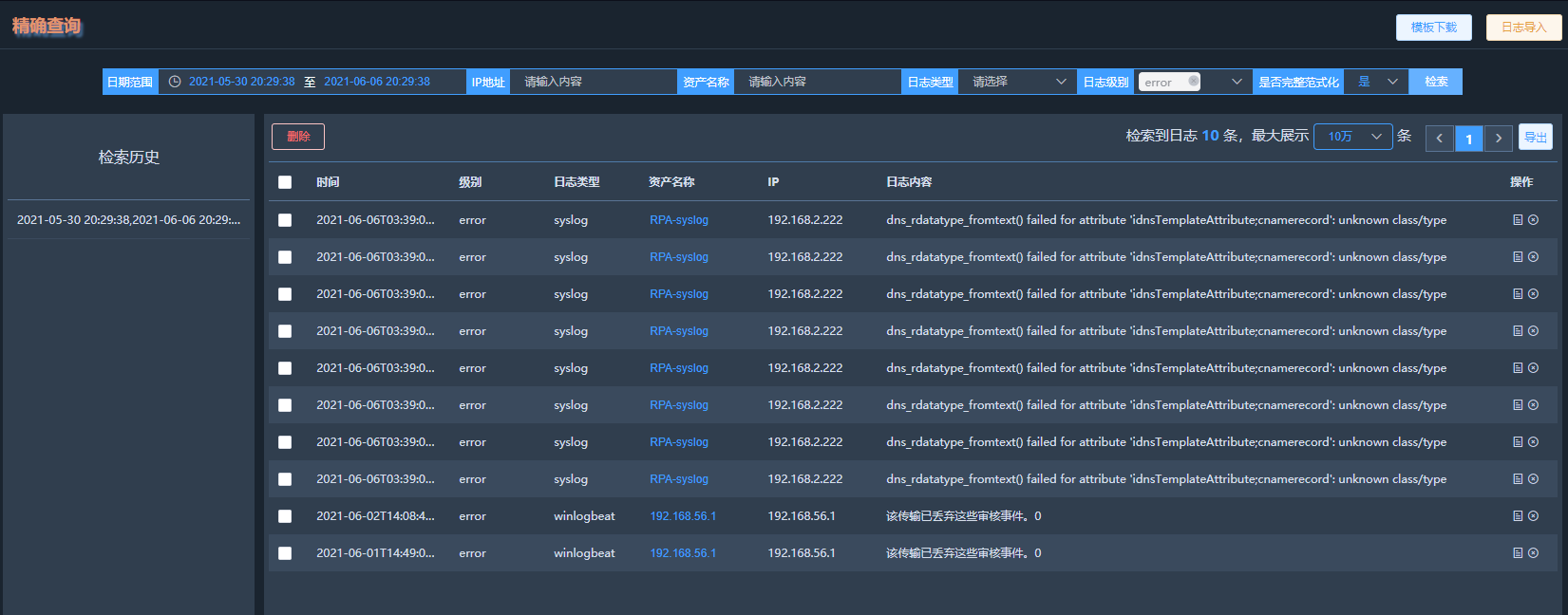


点击日志右侧按钮，可以查看日志详情。



1. 精确查询

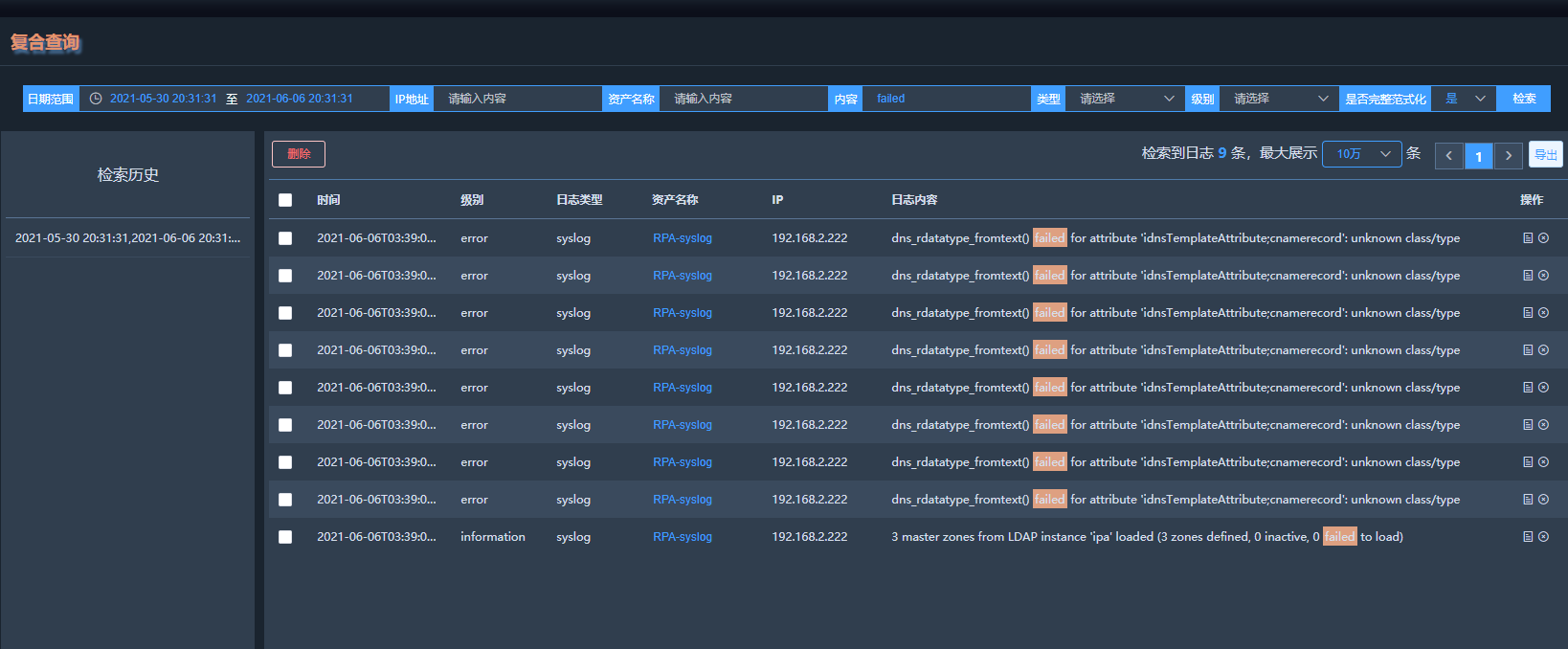
点击左侧菜单“精确查询”，进入精确查询页面。可以针对更具体的字段进行更准确的查询，查询速度更快、内容更准确。



同时可以进行日志的导出功能，由于日志文件较大，导出的日志默认会放到服务器/home/export目录下。

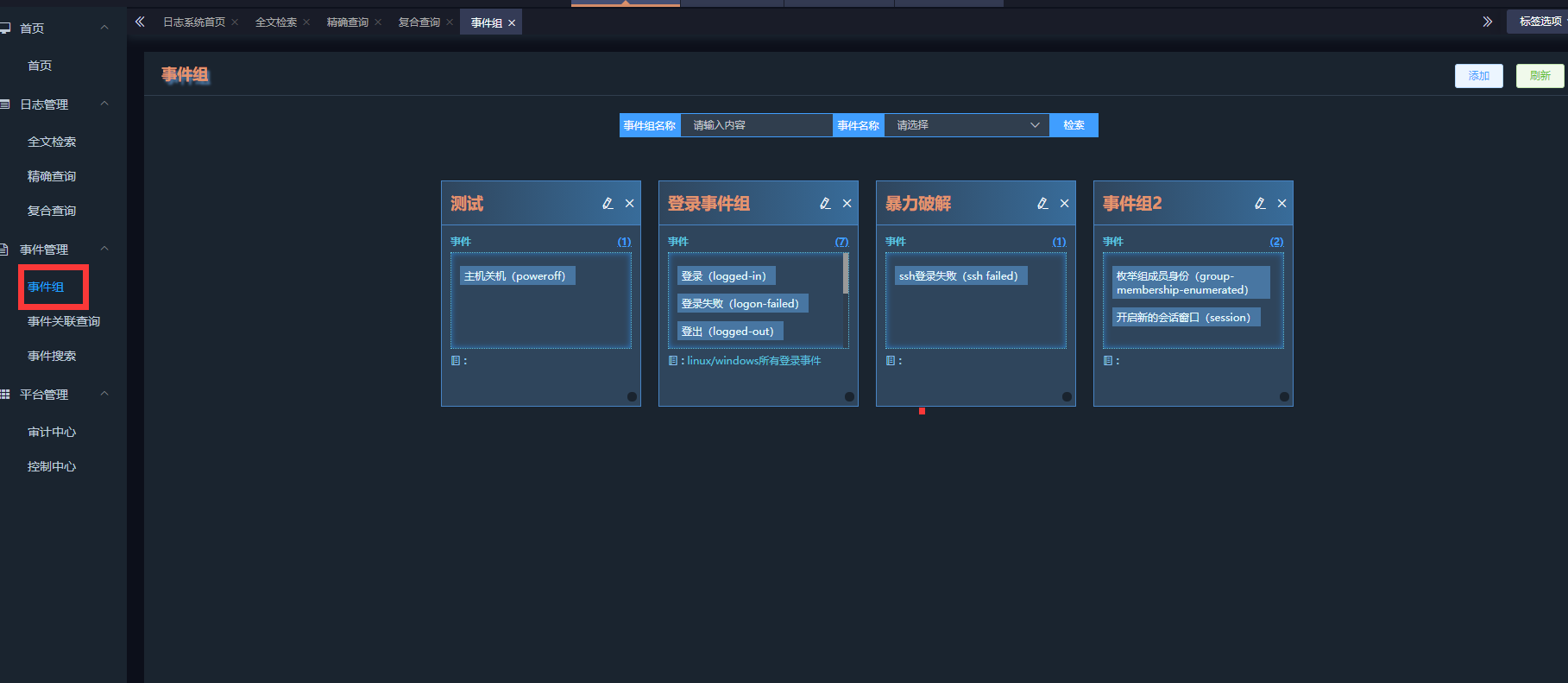
1. 复合查询

复合查询将模糊查询和精确查询进行一定程度的整合。实现日志内容的模糊查询，其他字段数据保持精确查询。



1. 事件管理
2. 事件组

点击左侧菜单“事件管理”-“事件组”，进入事件组管理页面。

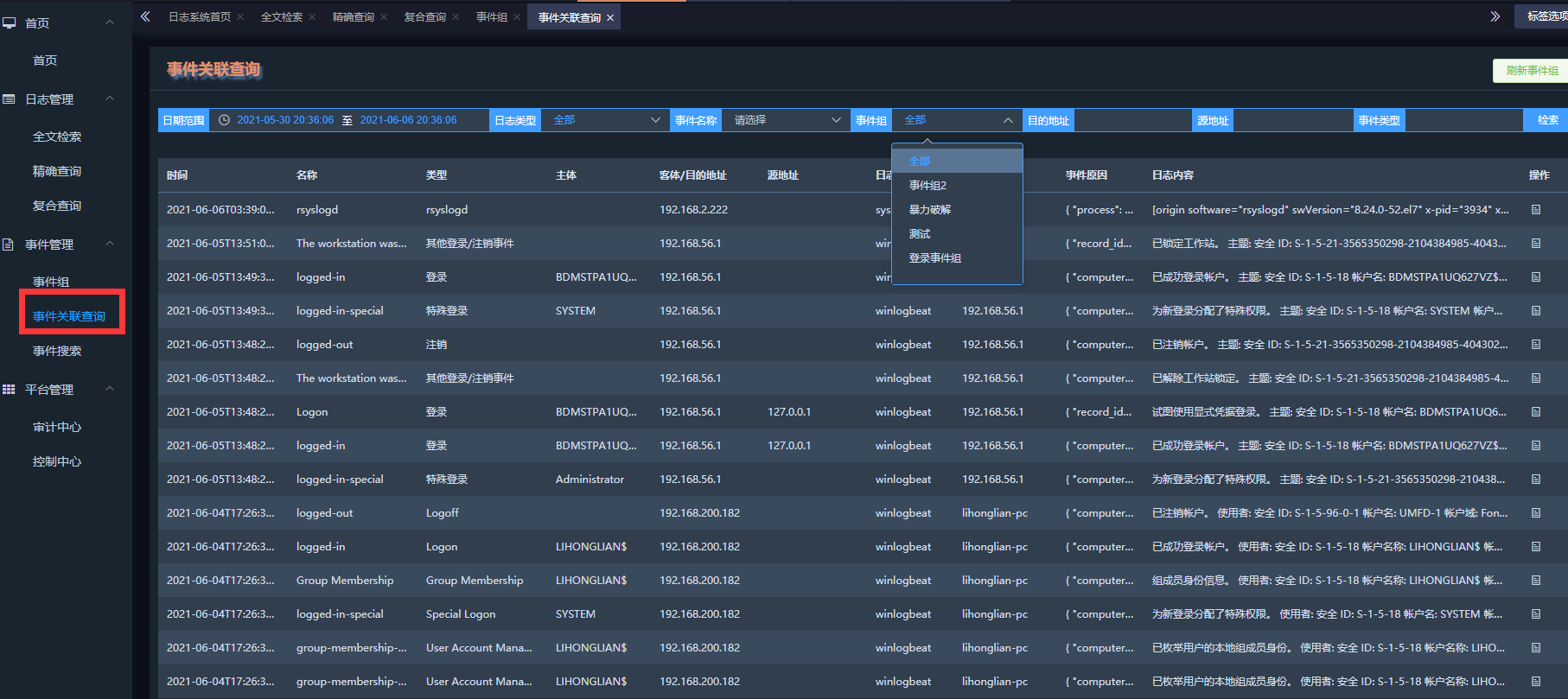


事件组为多个事件的组合，可以手动添加。



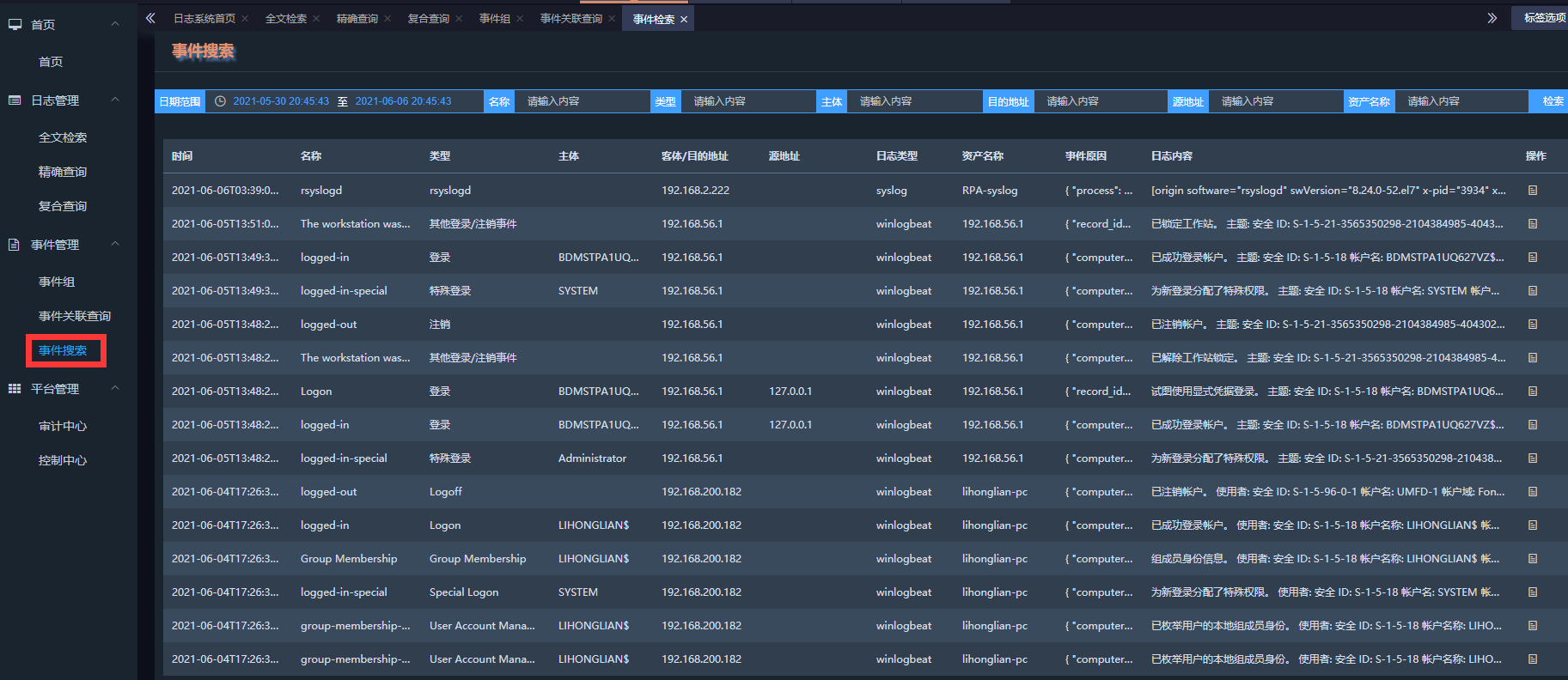
1. 事件关联查询

定义好事件组后，可以点击“事件关联查询”页面，对多个事件的日志数据进行关联查询。



1. 事件搜索

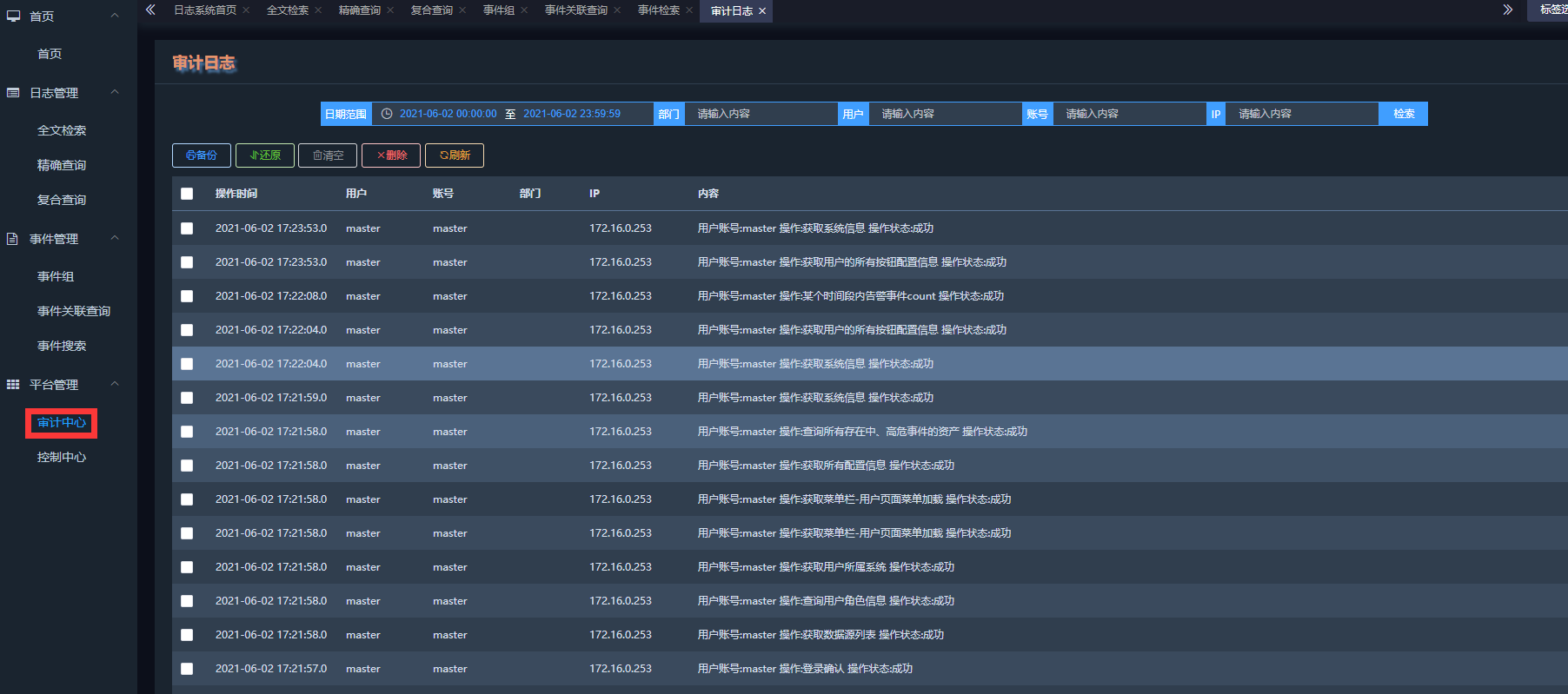
事件搜索页面提供基于事件的基本信息的查询，如主体、客体、日志类型、事件原因等内容。



1. 平台管理
2. 审计中心

点击左侧菜单的“审计中心”，进入系统自身日志的审计页面。提供操作时间、用户、账号、部门、IP、内容等信息。

可以进行审计日志的查询、备份及还原功能。



1. 控制中心

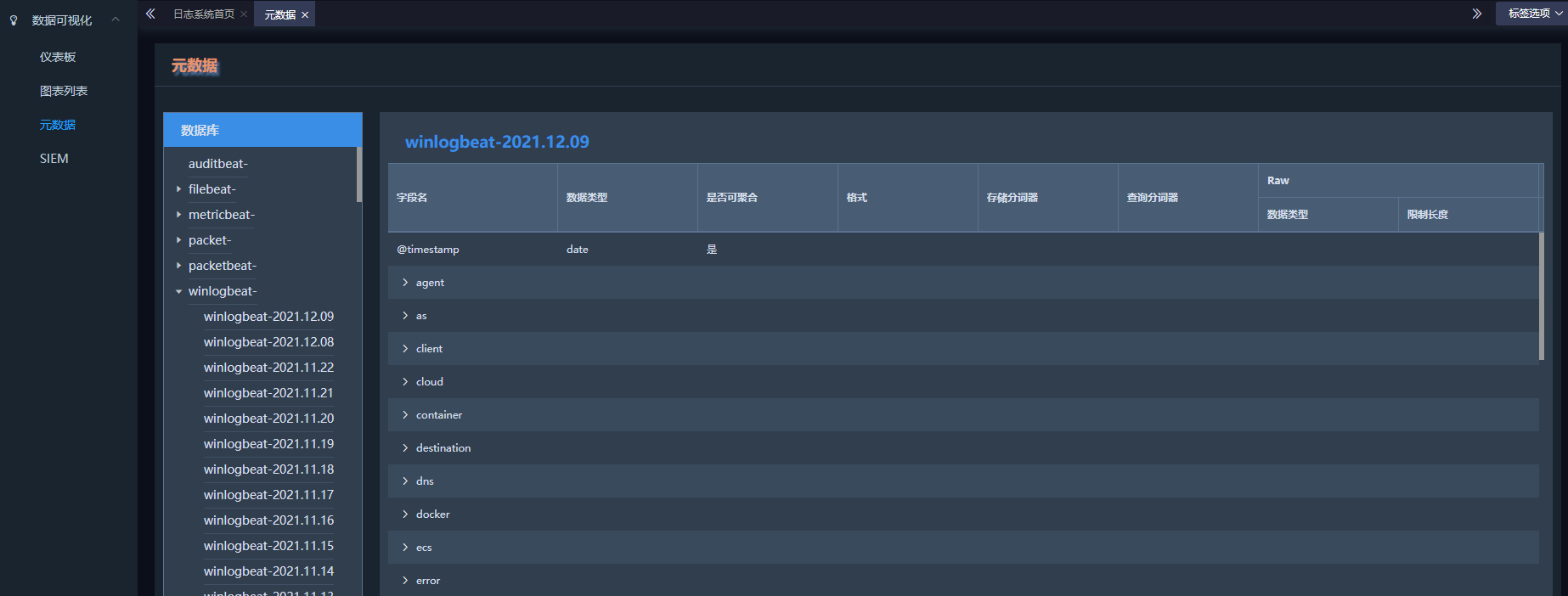
点击左侧菜单的“控制中心”，进入系统控制页面。

可以进行采集器的开启和关闭，进行日志备份及还原功能。并提供系统初始化按钮进行数据初始化操作。



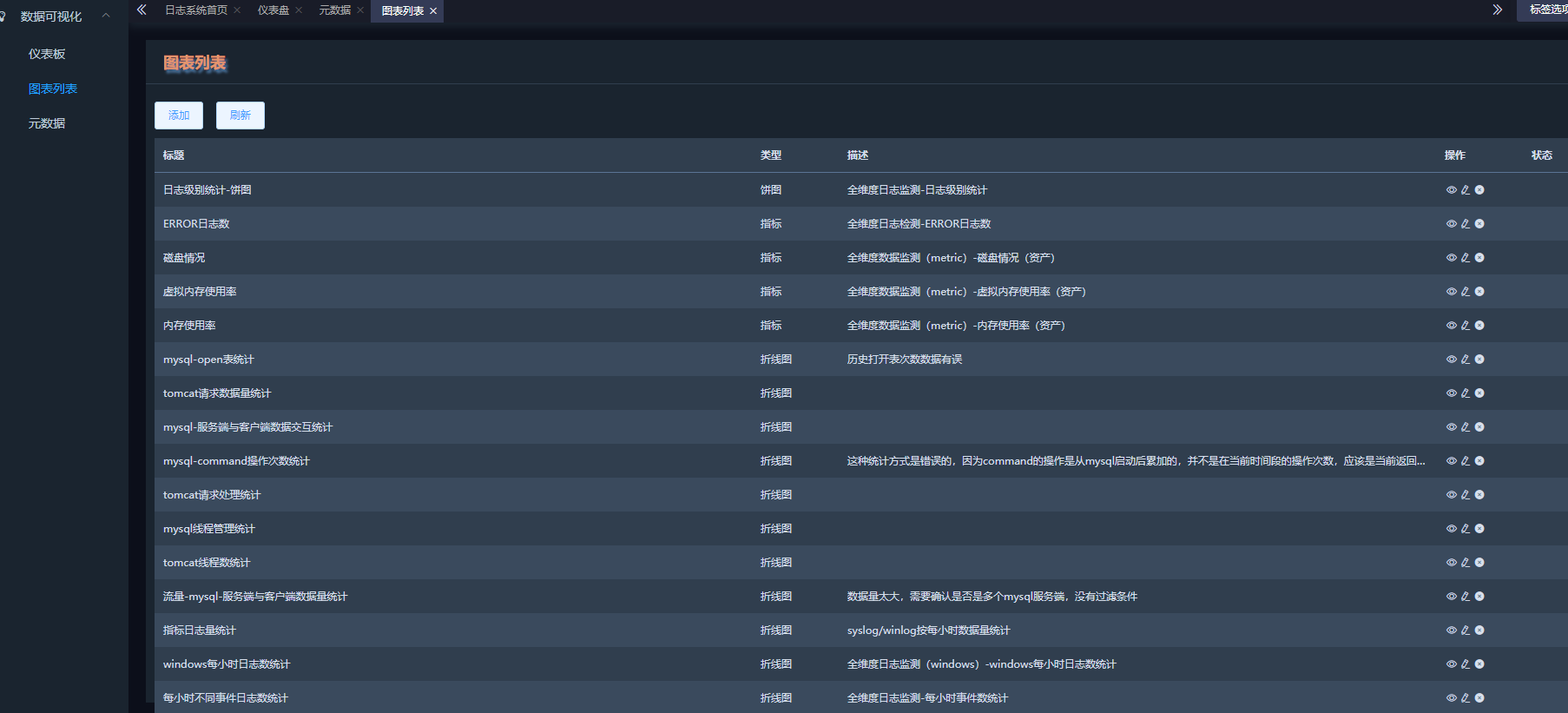
1. 数据可视化
2. 元数据

点击“数据可视化”-“元数据”可以查看存储的数据的数据结构信息。为图表制作提供字段依据。



1. 图标列表

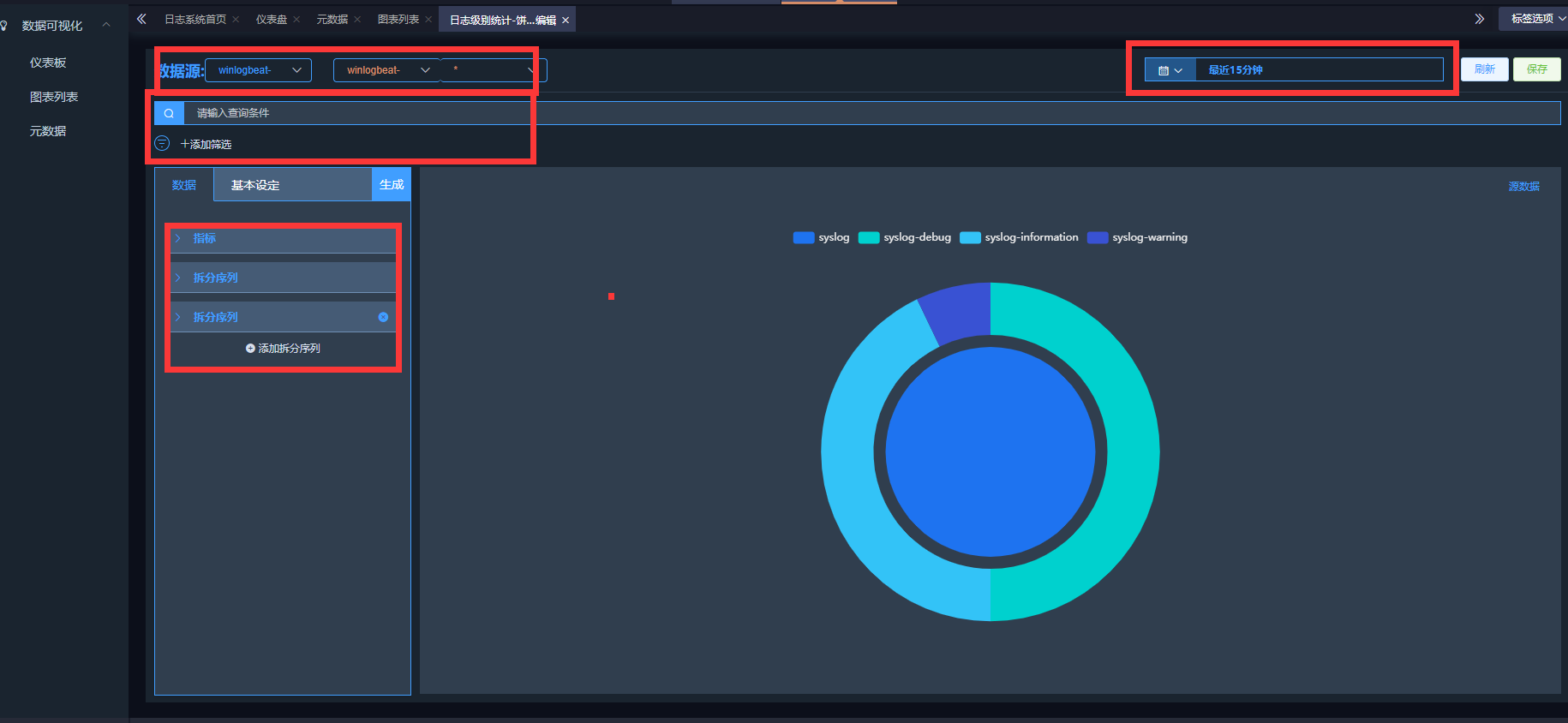
点击左侧菜单“图表列表”，进入图表列表信息页面。



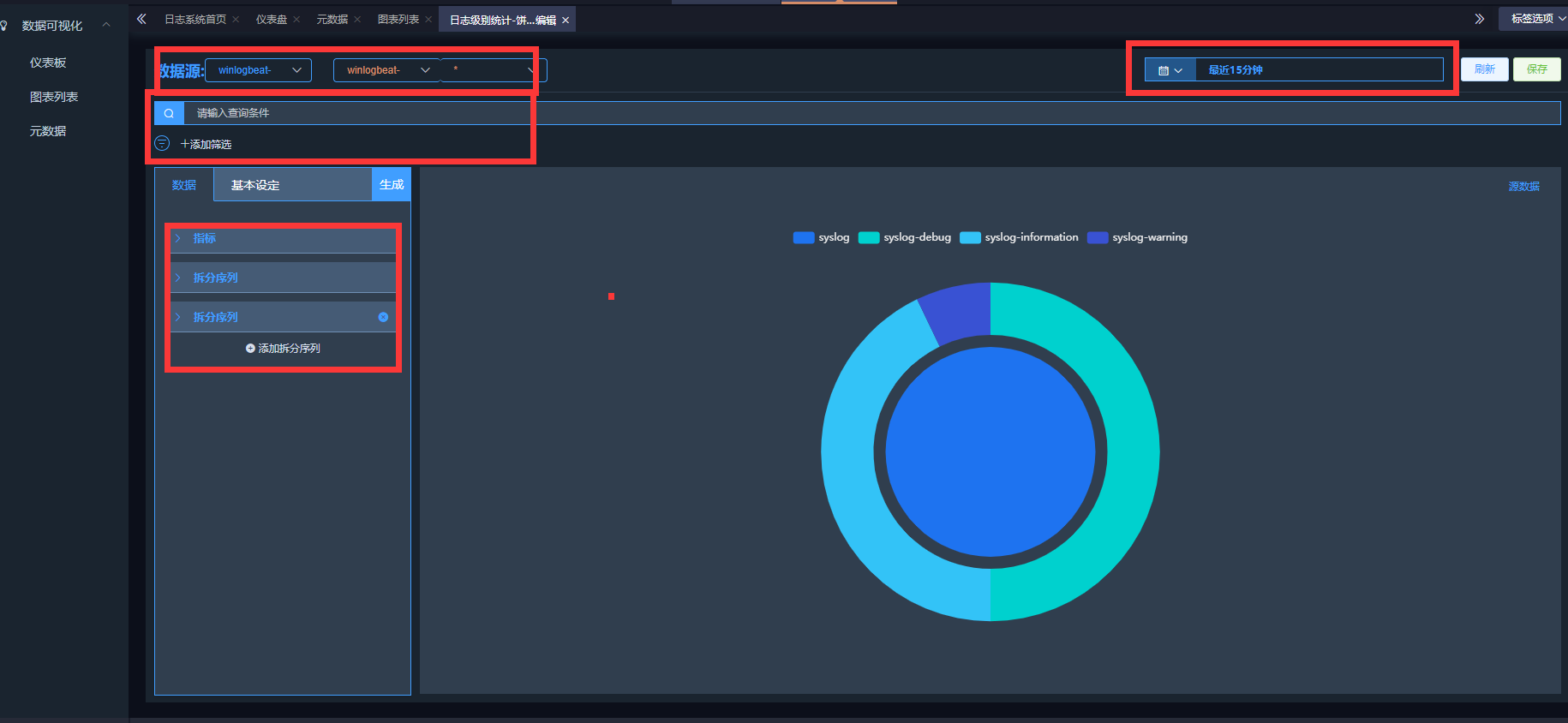
点击【添加】按钮，首先需要选择要制作的图表，支持柱状图、饼图、折线图、指标、表格。



确定要制作的图表后，进入图表操作页面。



图表的生成需要设置4个部分的内容：数据源、筛选条件、数据统计方式、时间周期。

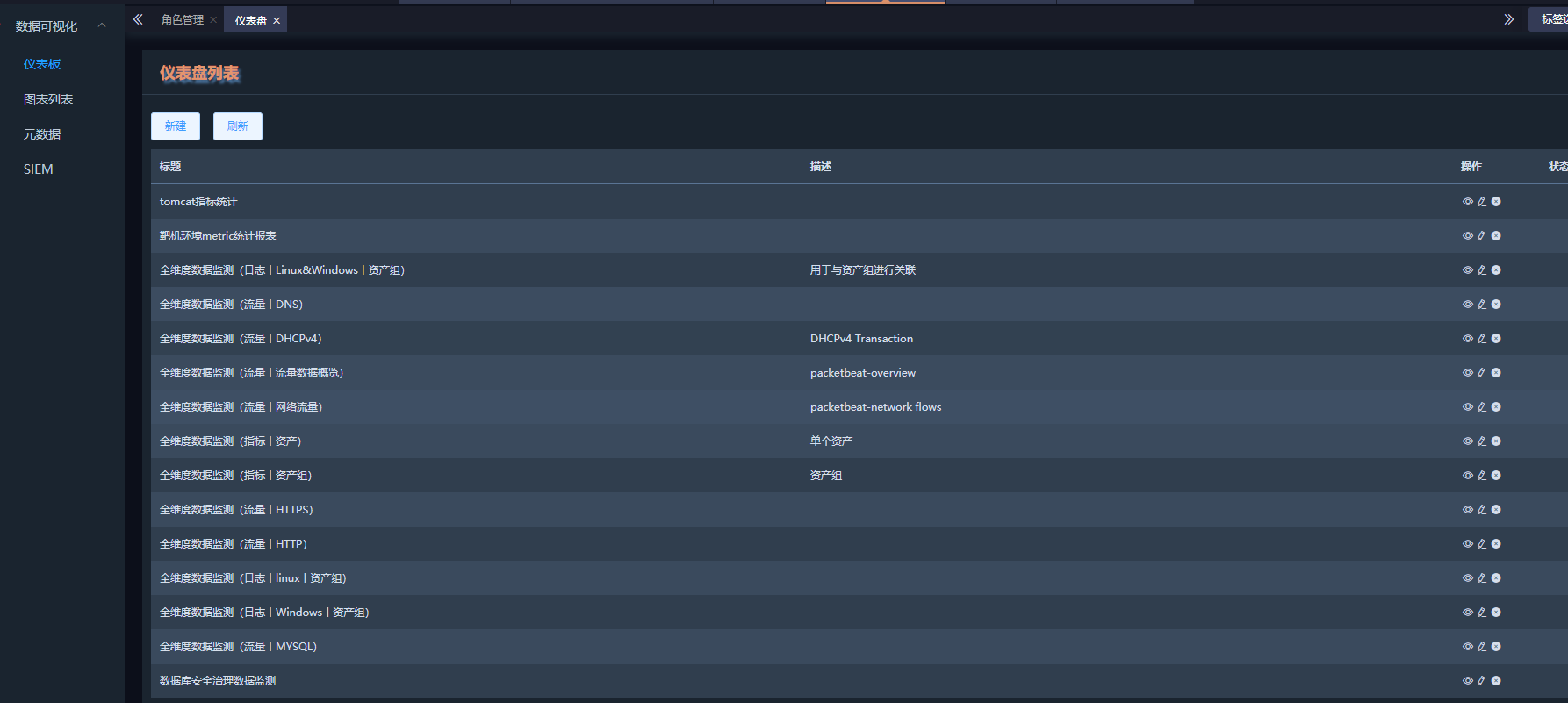


这部分操作锁选择的数据源、字段信息等信息的填写需要参照“元数据”模块。

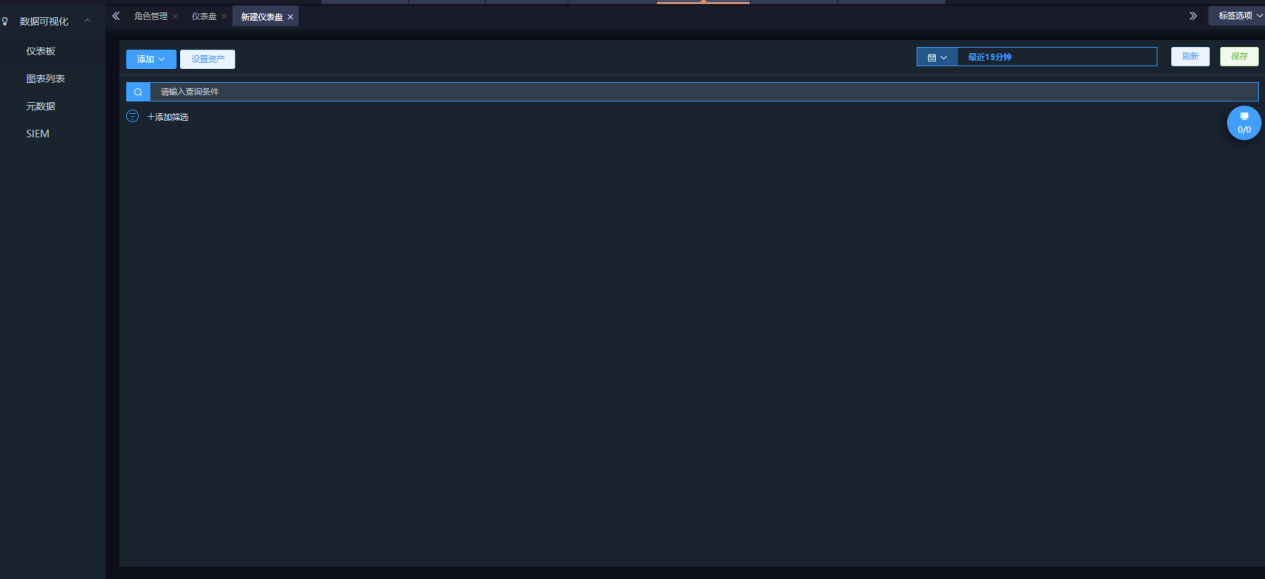
1. 仪表板

制作多个图表之后，需要将多个图表整合成一个大的仪表板（dashboard），方便进行多维度的查看及大屏展示。

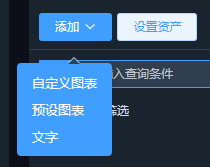
点击左侧菜单“仪表板”，进入仪表板的列表页面。

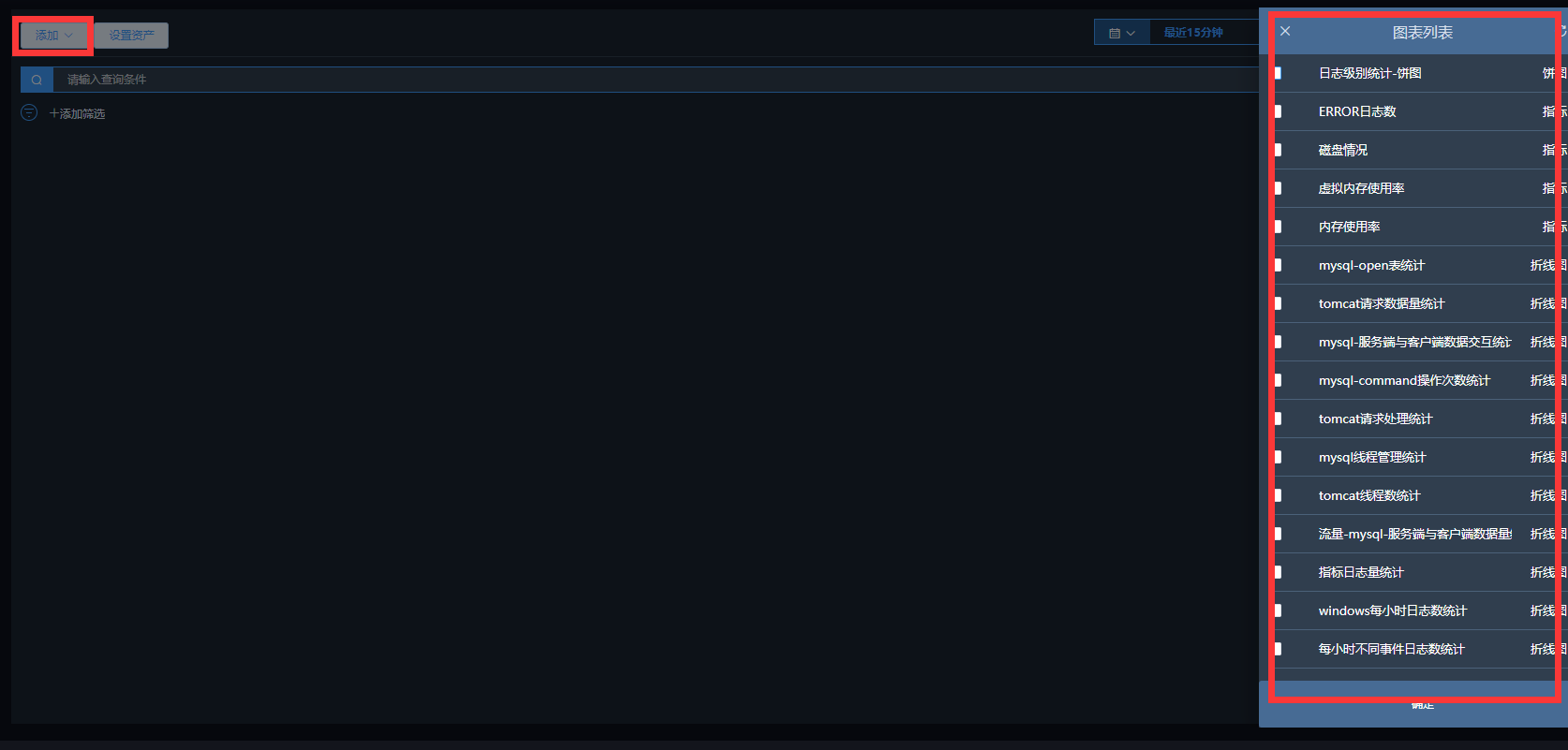


点击【新建】按钮，进入仪表板操作页面。



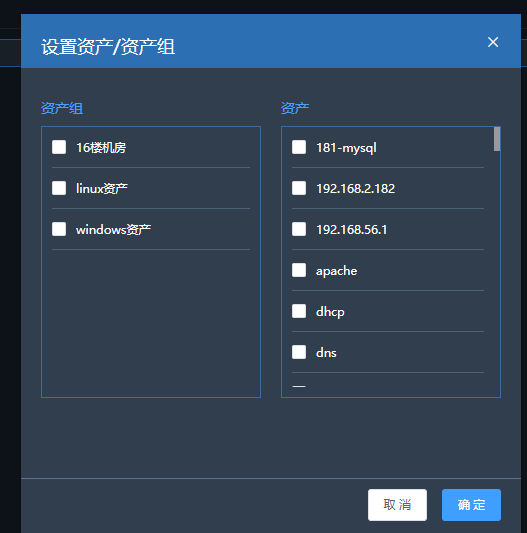
点击【添加】按钮。可以添加在“图表列表”中自定义的图表以及系统内置图表（预设图标）和文字信息。



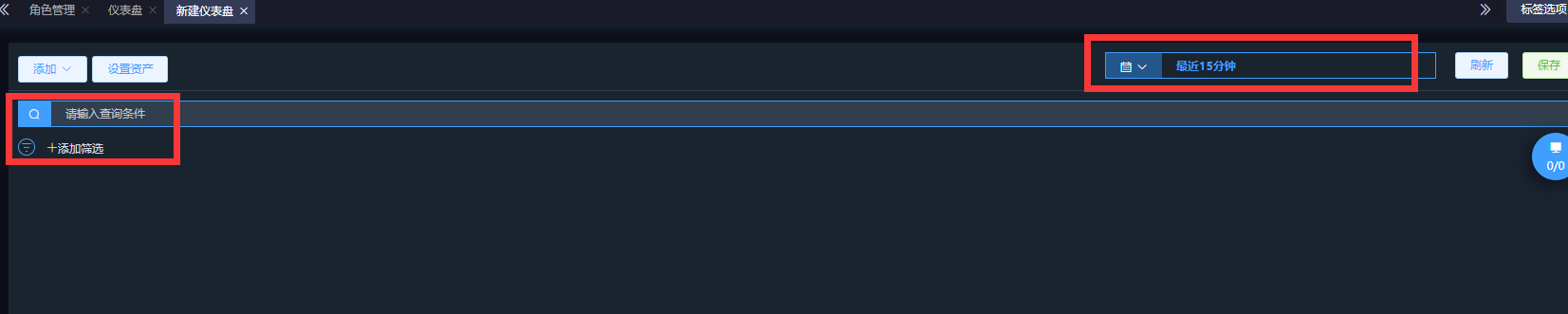




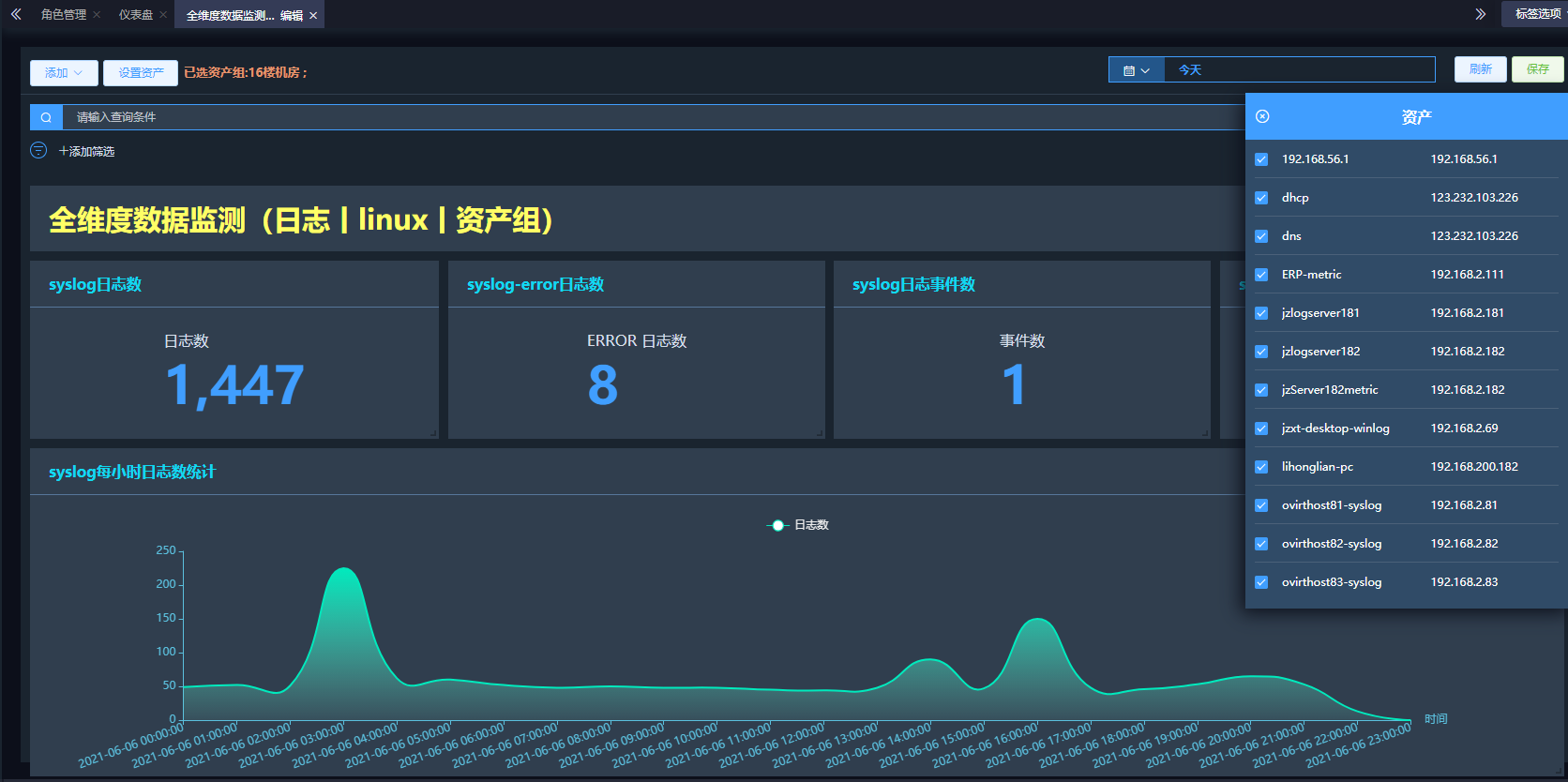
点击【设置资产】可以设置该仪表板服务的资产（单个资产、资产组、全局）。



可以对仪表板的时间及数据的查询条件进行设置。



添加的文字或图表可以通过拖拽的方式移动位置，也可以设置其大小，最终形成一个完整的仪表板。

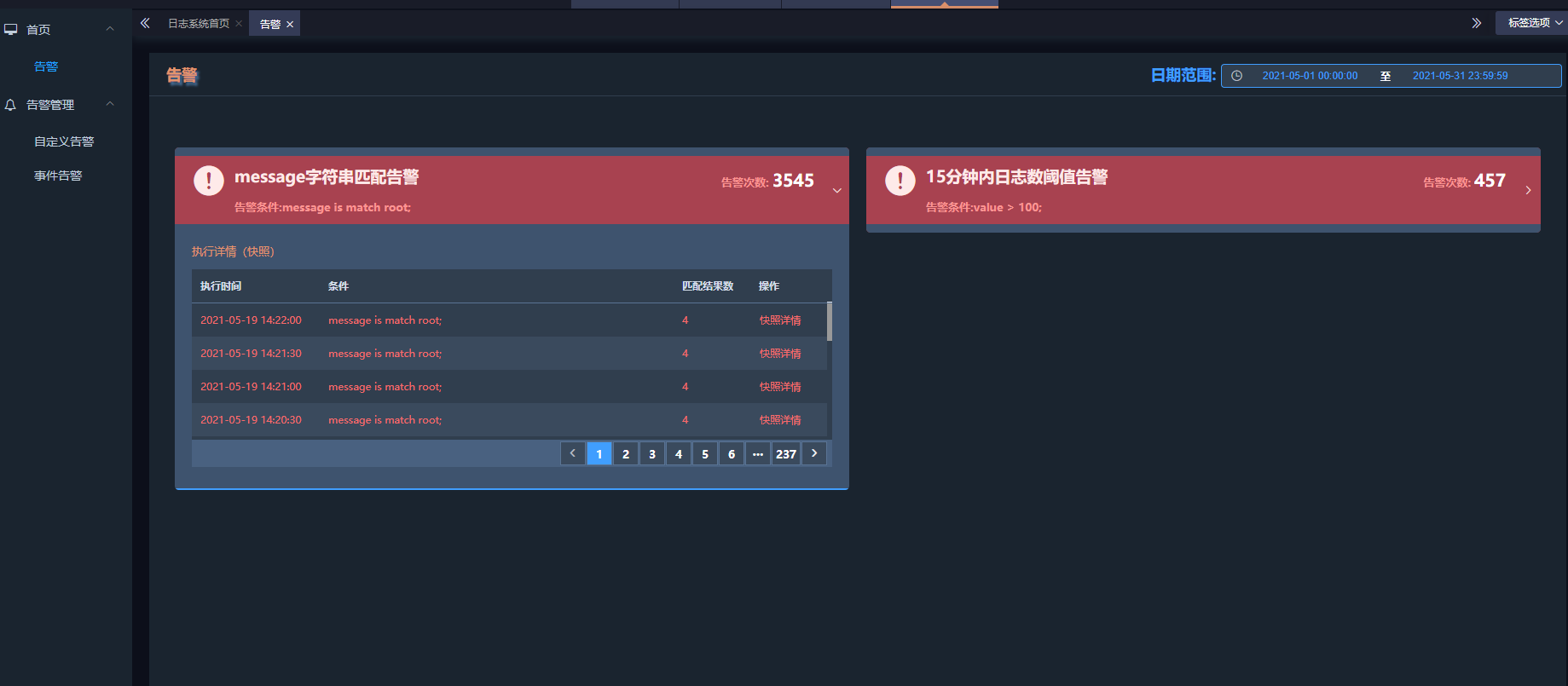


然后点击右上角【保存】按钮。

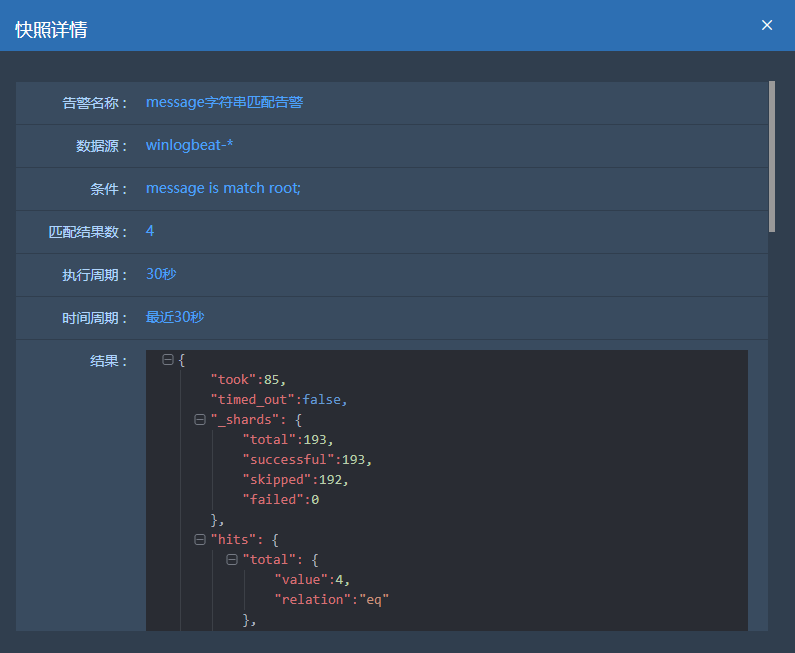


1. 告警监测
2. 首页

点击“告警监测”-“首页”-“告警”菜单，进入告警监测模块首页。

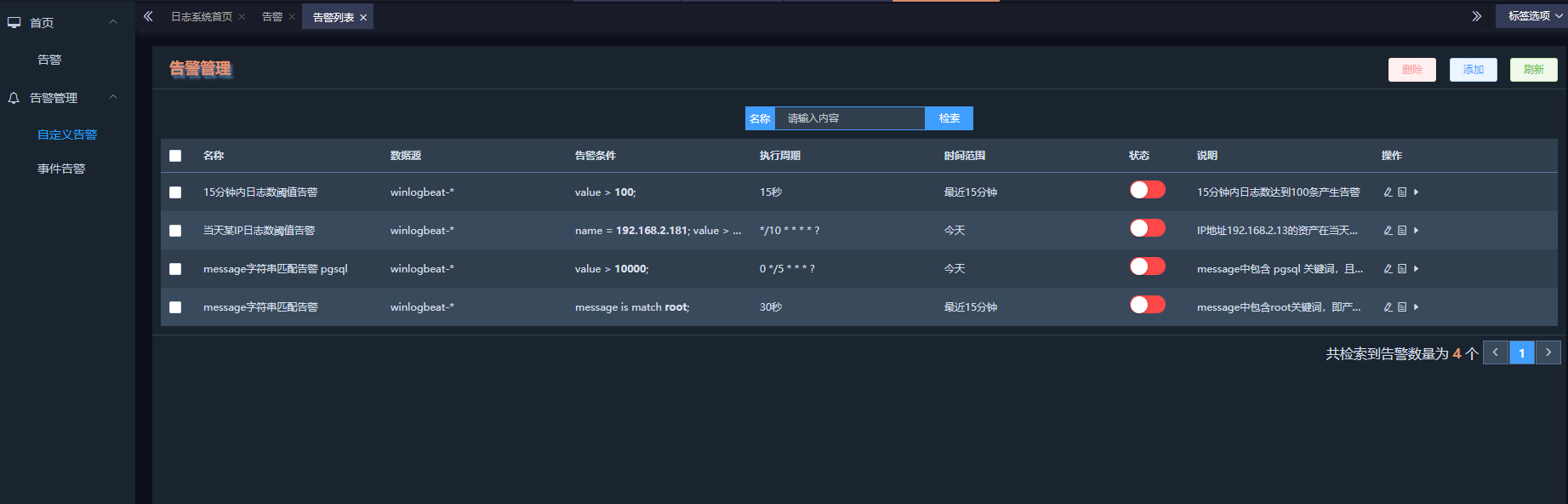


可以查看一定时间范围内产生的告警事件，并可以查看事件详情。



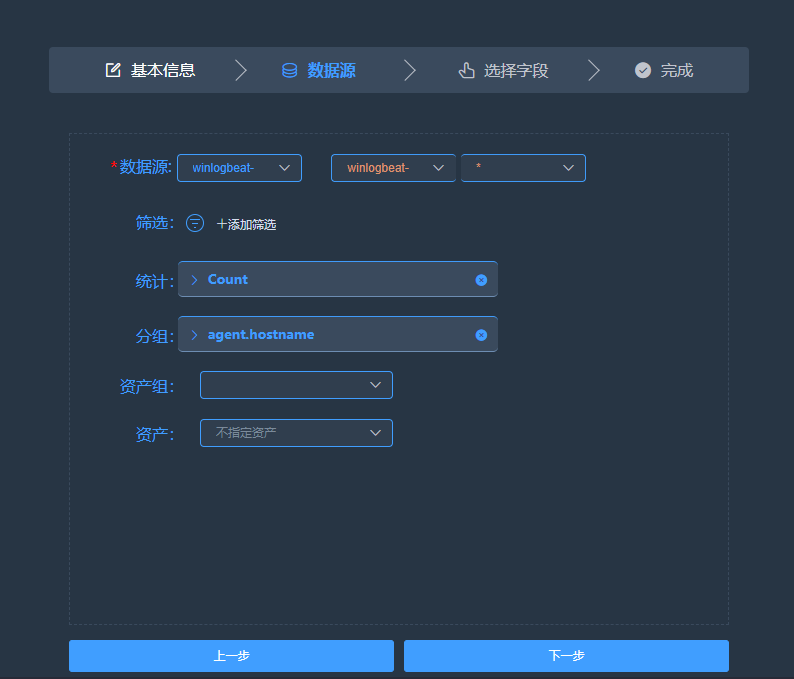
1. 自定义告警

点击“告警管理”-“自定义告警”菜单，进入自定义告警的管理页面。



点击【添加】按钮，添加一个自定义的告警信息。







添加的信息包括告警的名称、周期、说明、数据的统计方式、告警的条件等信息。

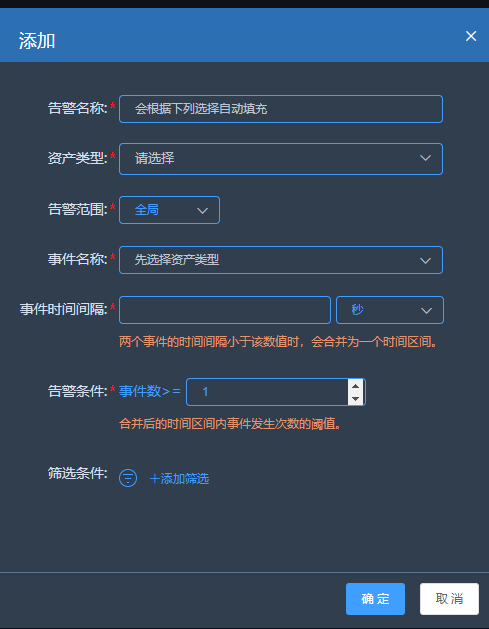
可以在自定义告警管理页面启动告警，如果发现告警信息，可以实时在首页进行查看。  
 同时，自定义告警管理页面，提供告警信息的删除、编辑、查看功能。

1. 事件告警

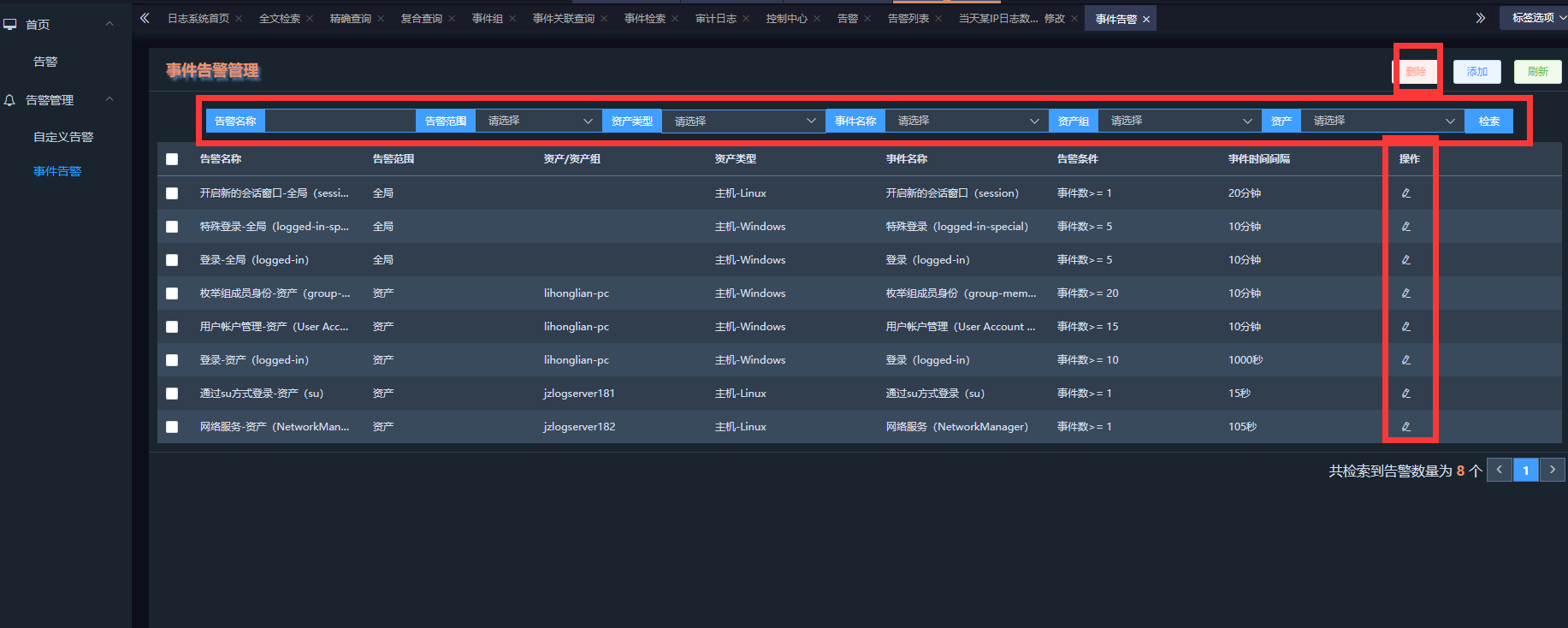
点击左侧菜单的“事件告警”进入事件告警管理页面。



点击【添加】按钮，添加事件告警信息。事件告警信息包括告警名称、资产类型、告警范围、事件名称、事件时间间隔、告警条件以及数据筛选条件。根据设置的告警可以实时对数据进行统计分析，判断是否产生告警。



在事件告警页面可以对告警信息进行查询、编辑、删除操作。



设置完告警后，可以在资产管理页面，查看资产是否产生告警。

