业务访问行为

# 一、需求分析

针对API访问行为提取用户行为信息，目的是通过对API访问行为的分析，分析用户的操作使用

## API访问日志存储

获取API访问日志信息；

## 数据存储和处理

将API日志存储在CKH当中，进行快速查询及人工分析；

## 行为分析

通过分析API日志，标注出账户信息及操作行为动作；

## 数据可视化

通过标注API日志的行为信息，将识别分析结果存储到业务访问行为模块中，帮助运营人员和开发人员理解用户行为；

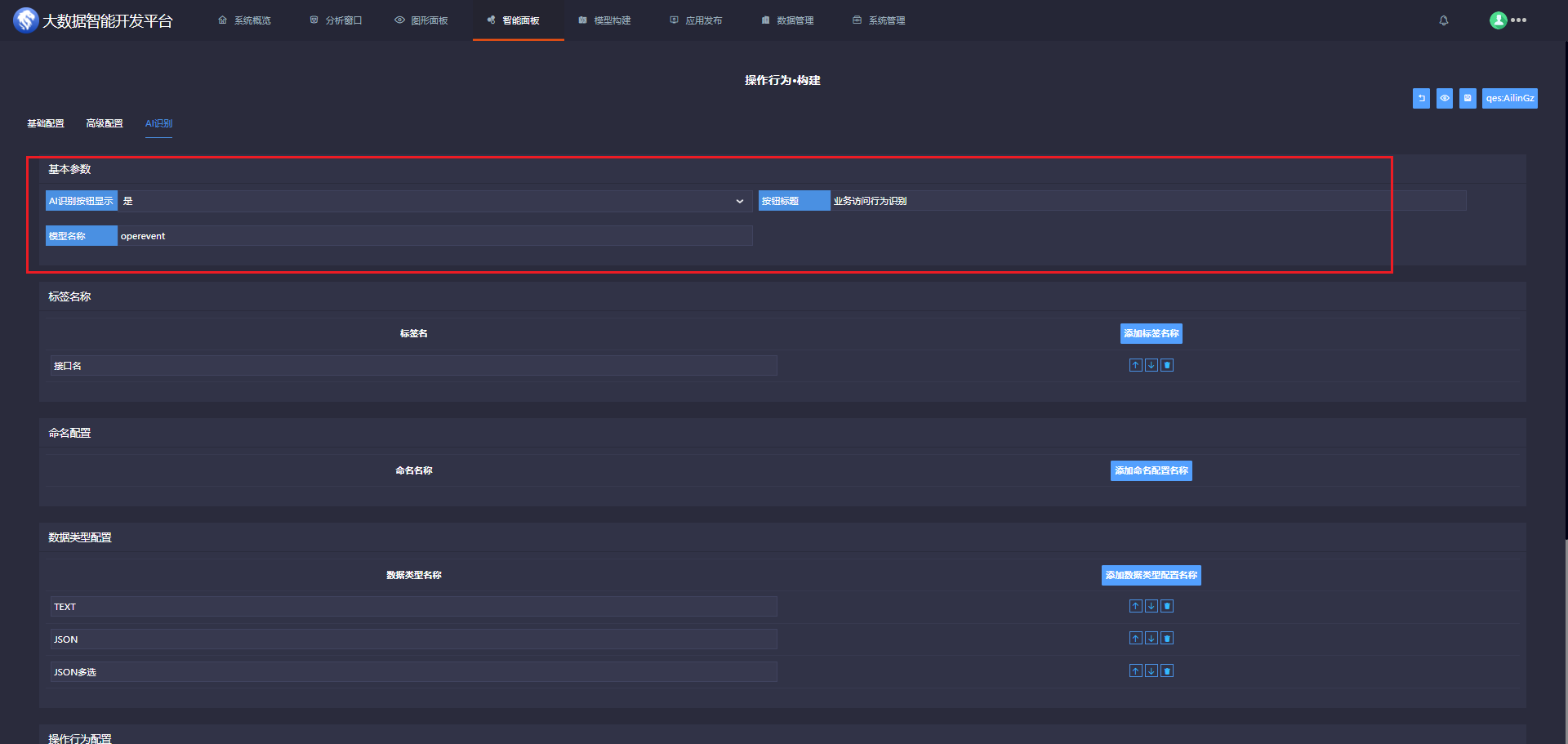
提供过滤和查询的功能，支持对特定用户，时间段和行为的分析和查看；

# 设计过程

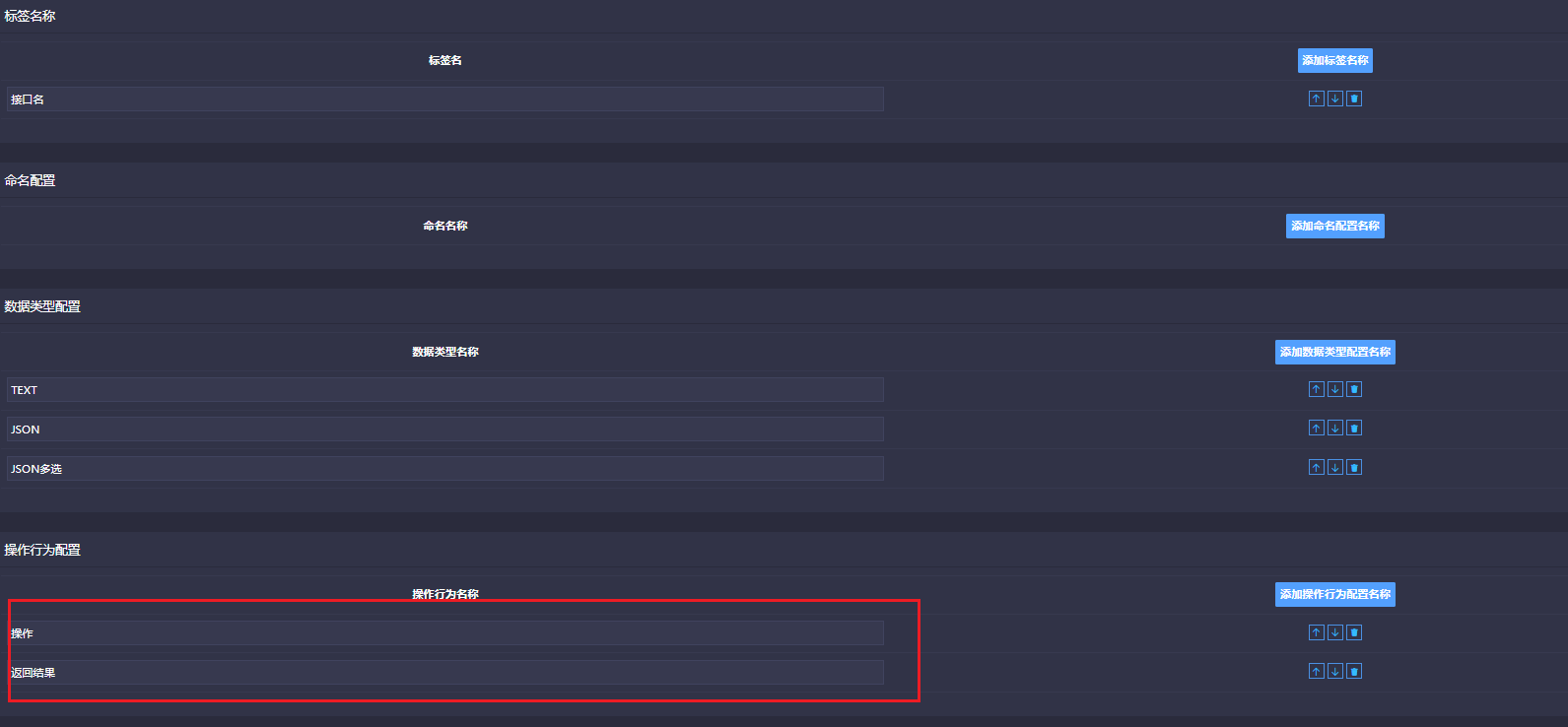
## 配置信息

针对API访问行为的查询分析模块，进行AI识别配置

①第一步：开启识别模块，修改按钮标题，模块名称填写



②第二步：自定义标签名称、命名配置、 操作行为配置；目前操作行为配置为 操作、返回结果。操作行为配置尽量跟想要输出的结果相匹配；



## 2.数据表的创建

用于业务行为数据的存储，以下是表结构信息：

CREATE TABLE default.analy\_model(

time DateTime64(6),

url String,

app String,

parameter String,

account String,

response\_body String,

request\_body String,

id String,

oper\_dic String,

res\_dic String

)ENGINE = MergeTree　ORDER BY time　PARTITION by toYYYYMMDD(time);

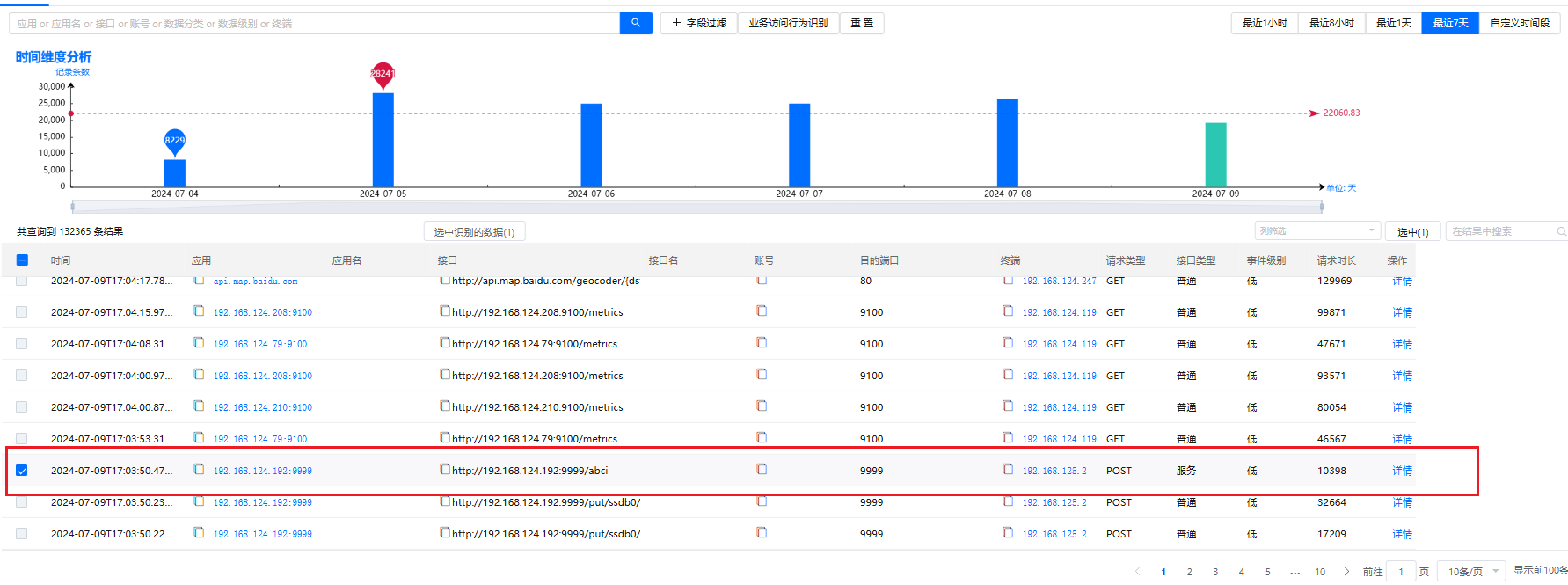
这里的 oper\_dic 对应了 操作行为配置中的 操作；

这里的 res\_dic 对应了 操作行为配置中的返回结果；

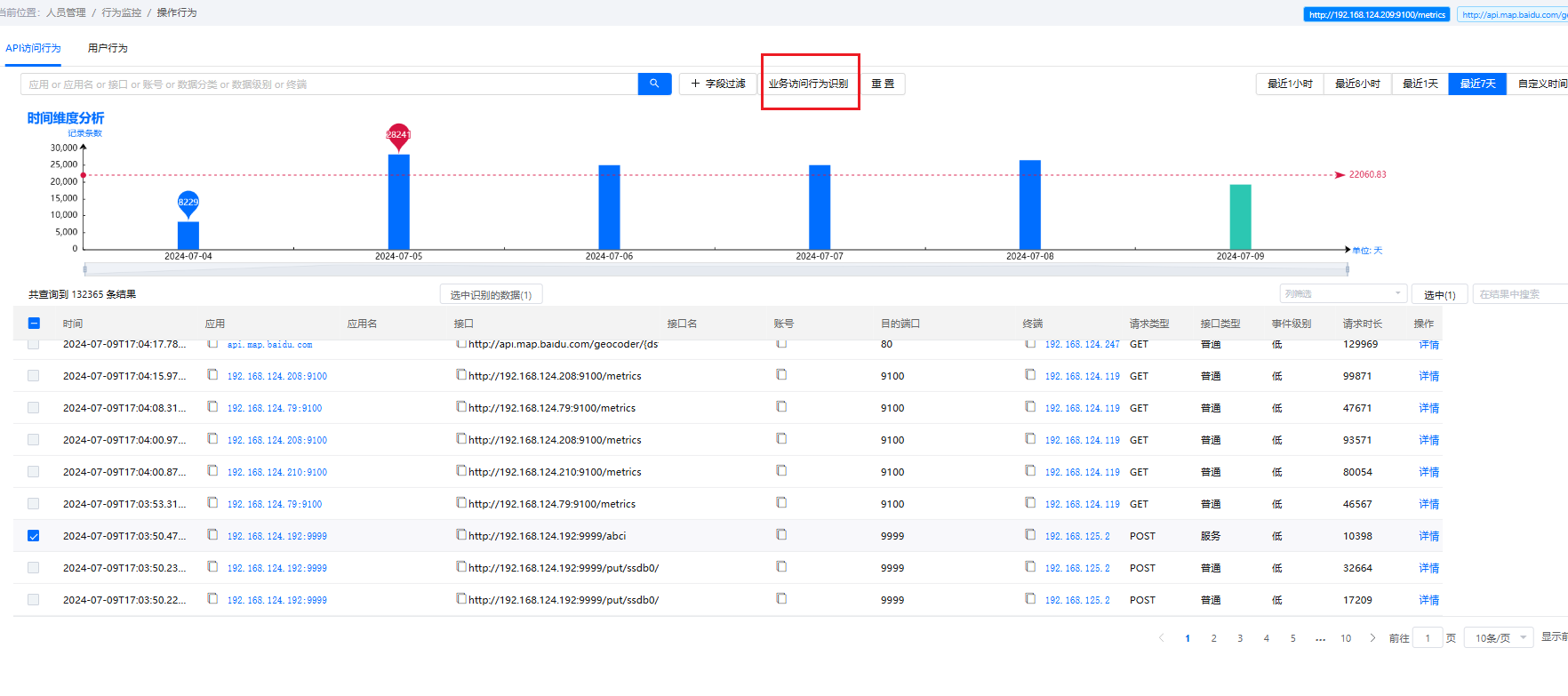
## 3.日志分析及标注

通过观察API访问行为日志信息，获取到API当前账户信息及行为分析，例如：在91环境上监控其他环境用户的操作，通过观察分析，可以对其进行标注

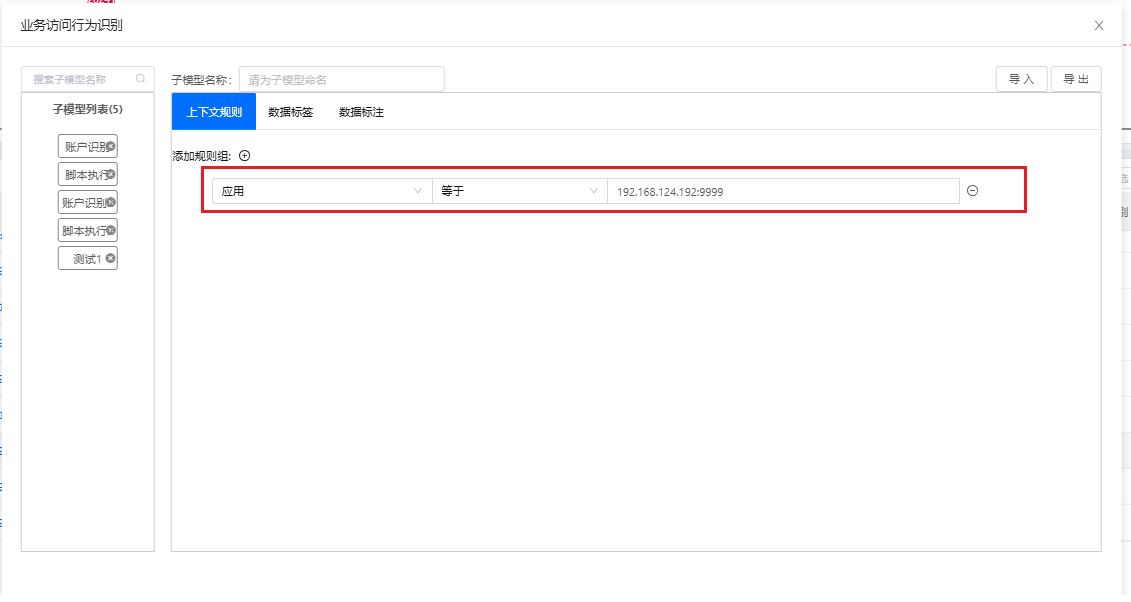
①第一步:选择需要标注的信息数据



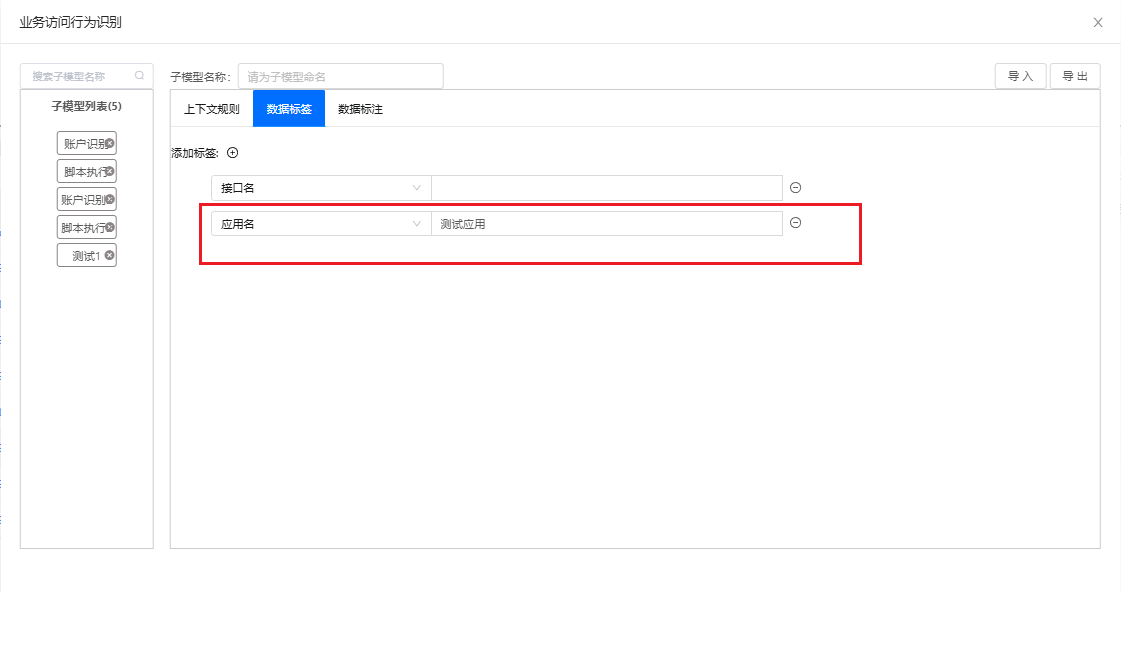
②第二步：点击业务访问行为识别



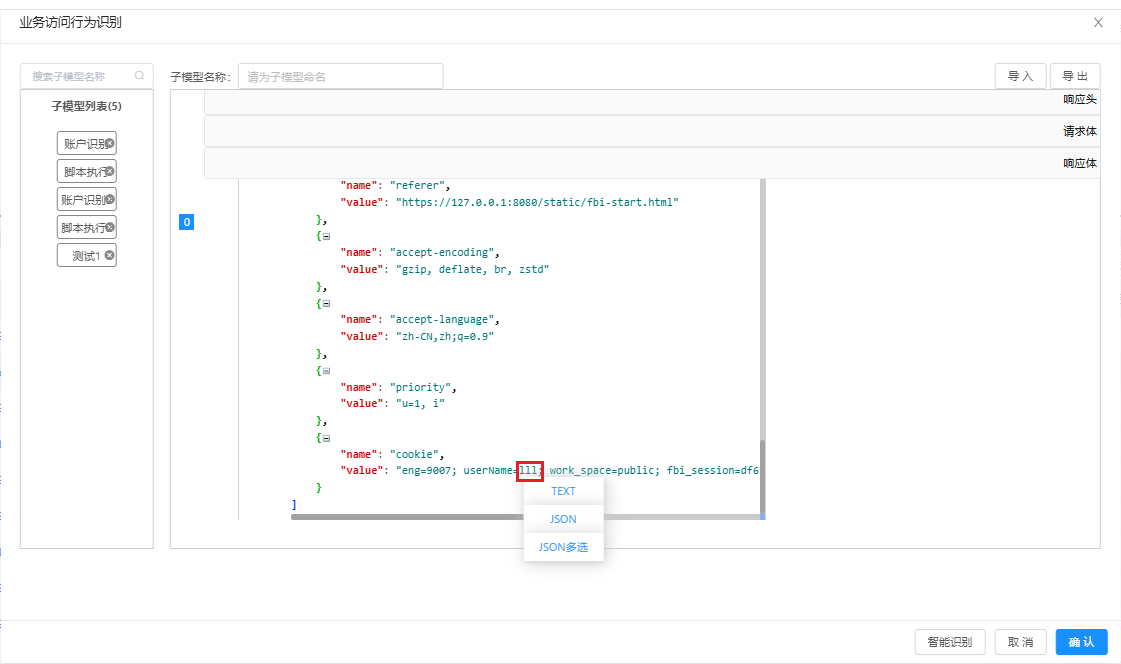
③第三步：筛选上下文规则，通过分析观察，发现针对当前应用 192.168.124.192:9999用户认证都为同一种方法，上下文规则就可以筛选成当前应用即可



④第四步：填写数据标签，如果需要对当前应用命名可以添加应用名的标签信息，接口名为默认配置项，也可以进行删除



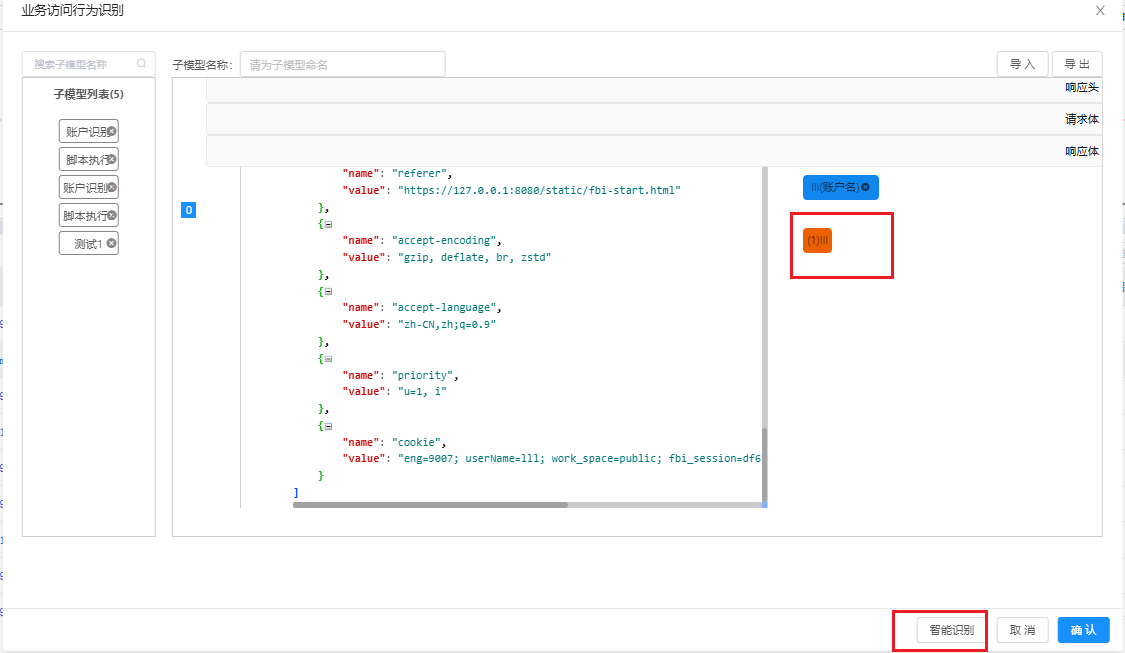
⑤第五步：进行数据标注信息，针对当前API日志信息，获取到请求头中存在账户信息，进行标识；选择TEXT数据类型；



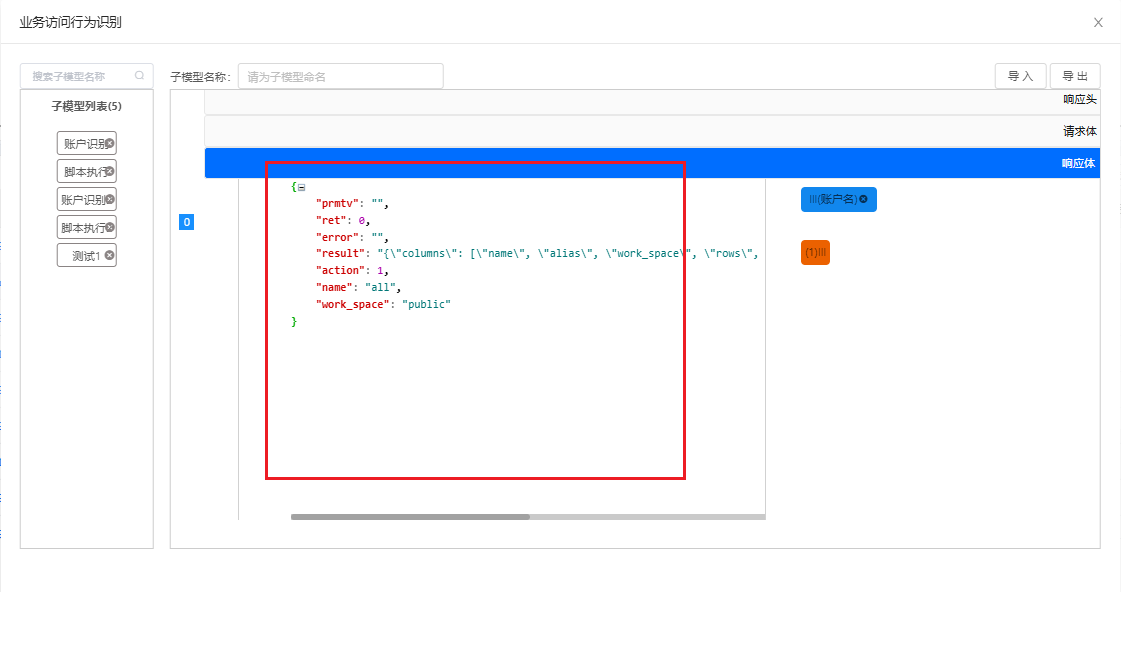
命名名称：账户名 命名标签名称： （可以为空）；（如果想要将账户名单独作为一列值存储，当前的中文命名，开发人员需要知道，根据当前的命名信息进行存储账户名列值）



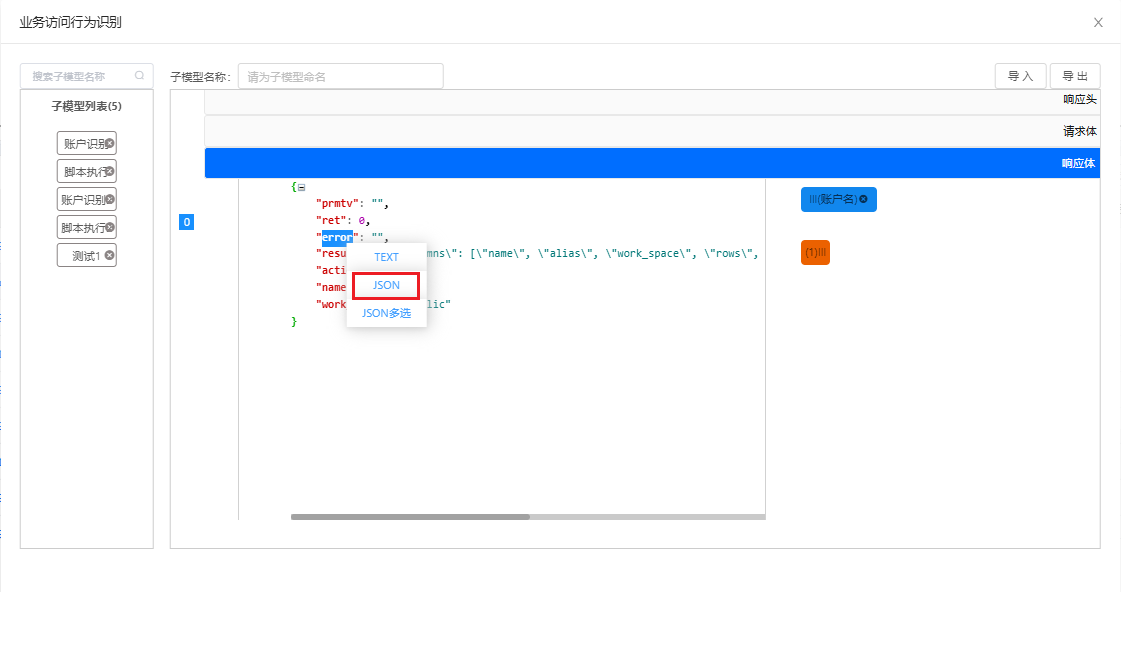
⑥第六步：信息配置完成后确定，点击智能识别，会获取到当前我们标注的结果信息



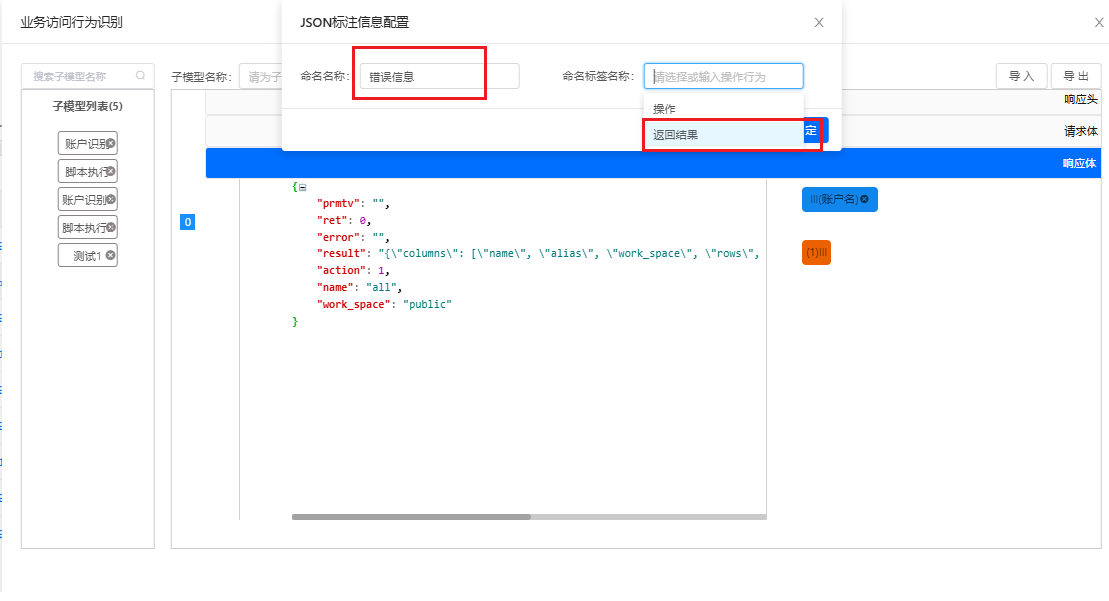
同样的我们也可以获取到当前应用下面的返回结果中的信息，例如：响应体中存在消息体，就可以获取的错误信息；



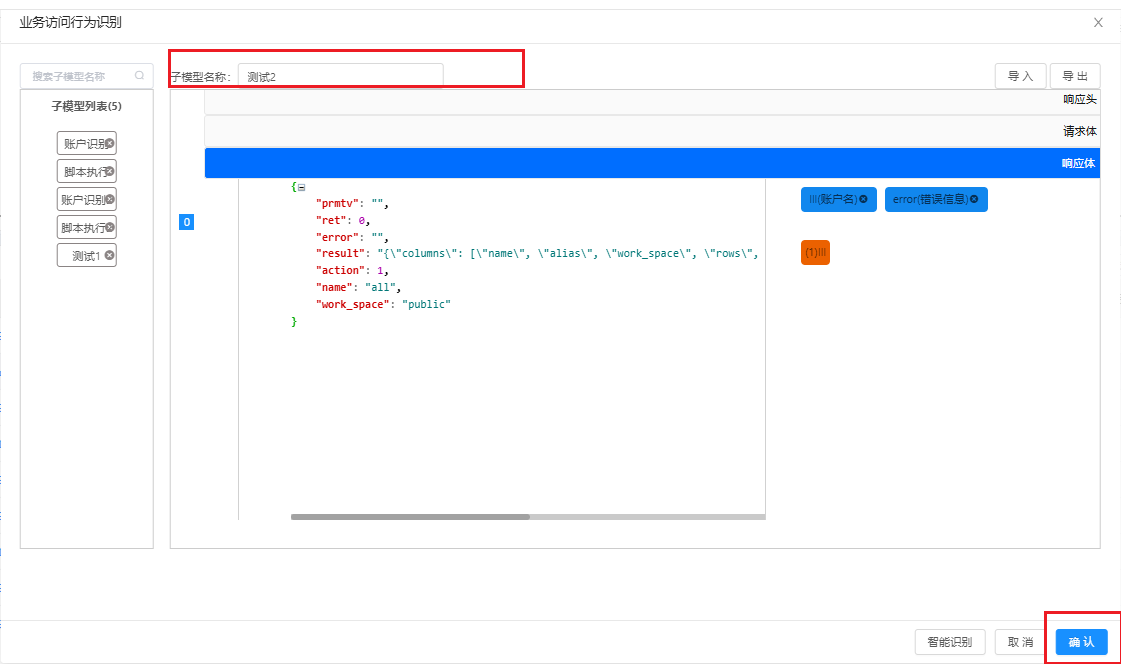
选择JSON识别，标注 “error”



标签配置，命名名称为：错误信息、 命名标签名称为：返回结果



⑦第7步：输入子模型名称，点击保存当前模型



## 4.数据模型获取及识别

①第一步：创建analy\_model.xlk文件，针对当前API行为分析出业务行为



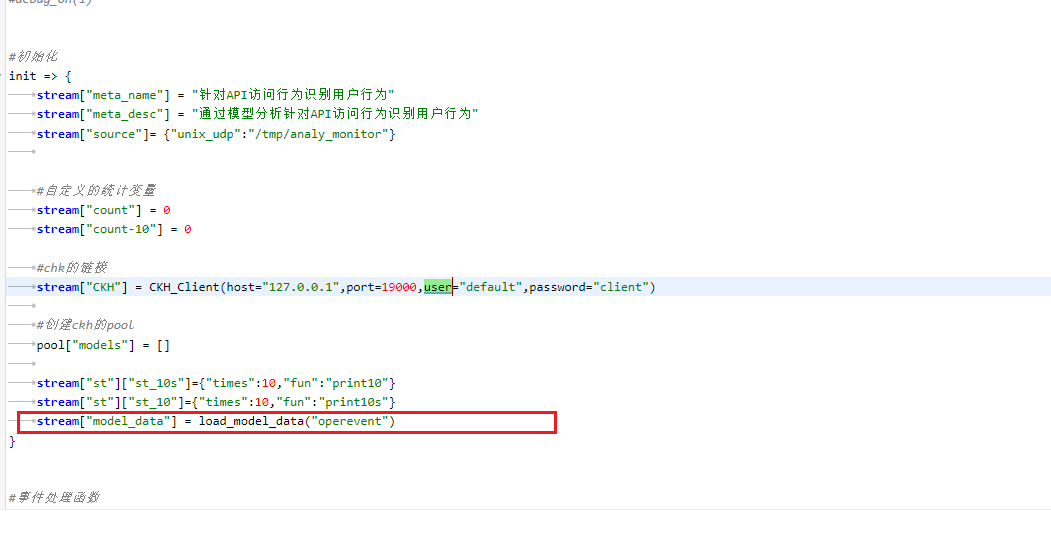
②第二步：获取Event事件信息，获取到存储API访问行为的日志流信息，API访问行为是通过 api\_monitor\_ckh.xlk 文件存储，上一级是api\_merge.xlk,因此从api\_merge.xlk分发出第二份数据到新xlink文件 analy\_model.xlk中



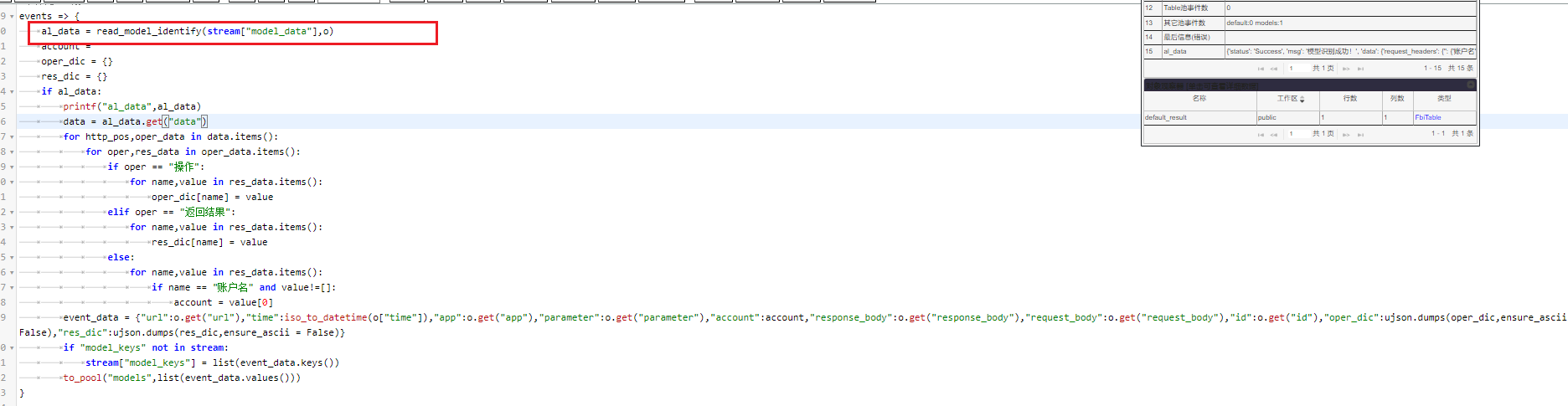
③第三步：导入包



④第四步：导入模型文件，模型文件名是基于配置信息中的基本参数：模型名称



⑤第五步：使用模型函数进行识别当前信息



⑥第6步：处理识别出的信息，识别结果为DICT信息，

‘data’:即标注识别的结果；

‘label\_info’:表示标签信息;

data中键的描述：

‘request\_headers’:表示识别的位置信息；

‘返回结果’：即我们标注时的命名标签配置；

‘’：这个空值就是在标注账户时，命名标签配置为空的值，以便于后续在Xlink判断时单独将账户名列出来进行存储；

⑦第7步：存储处理信息

## 数据展示

识别结果处理之后存储信息到业务访问行为模块；（具体业务还需根据具体场景选择不同的方式）

