共享文件审计系统

V2.4

**使用手册**

# 背景

目前使用文件服务器和私有云的企业越来越多，这大大提高了工作效率，但由于缺乏专业的共享文件管理工具，使得某些重要文件，尤其是商业机密文件被破坏和泄露，而且无法追责，这无疑是一个重大的安全隐患，稍有不慎，企业将损失惨重。

服务器共享文件被随意读取、下载、复制、另存、修改、新建、剪切，或者通过QQ、微信、邮件、云盘等途径发送出去，导致重要商业机密外泄。

服务器共享文件被局域网用户或新接入的外来电脑，有意、无意删除破坏后，无法进行备份和恢复，导致企业重要数据丢失和损坏，给企业带来不可估量的损失。

有时为了工作需要，必须开通共享文件的更改权限，导致用户可以随意修改共享文件，如果操作失误，会导致原始数据无法恢复，从而失去文件真正的使用价值。

服务器操作系统本身没有日志记录功能，以及没有专业服务器共享文件监控软件管理，导致用户的操作行为不受监管，一旦出现问题，无从查证，无法追究责任。

商业机密外泄

文件随意修改

文件删除破坏

责任追究困难

**安全**

**问题**

应对目前存在的问题，睿信数盾推出了业内技术领先的共享文件管理审计系统。

## 优势

相对于其他审计软件厂商，睿信数盾共享文件审计系统有多重优势：

* 性能卓越
* 支持日志、流量等多种数据源
* 兼容多种设备协议（Windows、第三方NAS等）
* 支持文件防泄密/打印等高级功能
* 支持鲲鹏/x86/Cavium等多类系统平台

# 设计原理

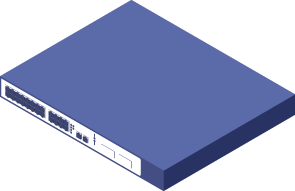
睿信数盾共享文件审计系统使用存储设备自带的日志（非消息队列版本），并进行日志提取、报警处理、统计分析、审计报表等逻辑。

架构图如下：

业务网络以太网交换机



华为OceanStor 9000



睿信数盾共享文件审计系统

笔记本电脑

台式机电脑

Pad

工作流程大体如下：

1. 存储设备对外提供CIFS/NFS/FTP服务，并手动对目录、用户、用户组等进行分配（也可以在审计系统中分配）
2. 存储设备开启日志服务
3. 对日志目录进行权限配置，以便审计系统能够访问该目录
4. 审计系统挂载日志目录（CIFS/NFS协议）
5. 审计系统对日志进行扫描、增量更新、解析、入库
6. 审计系统对入库日志数据进行各类分析处理
7. 审计系统进行各类展示、控制逻辑

# 使用步骤

## 登录

默认账号密码均为admin，登录后请及时修改密码



## 实例管理

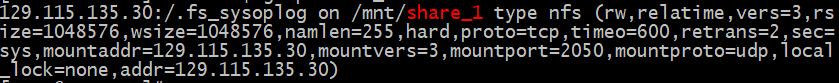


增加9000实例(CIFS挂载)：



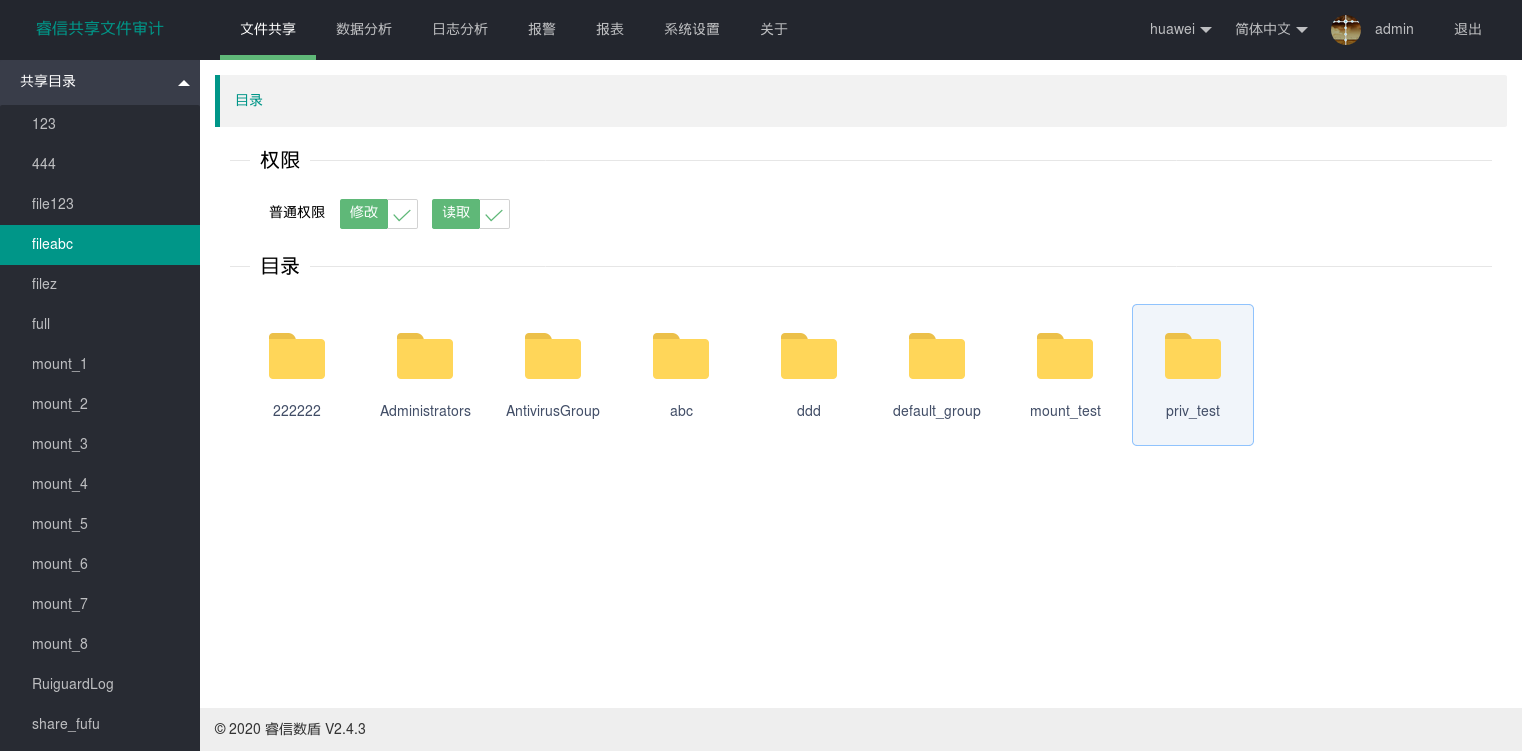
增加9000实例(NFS挂载)：



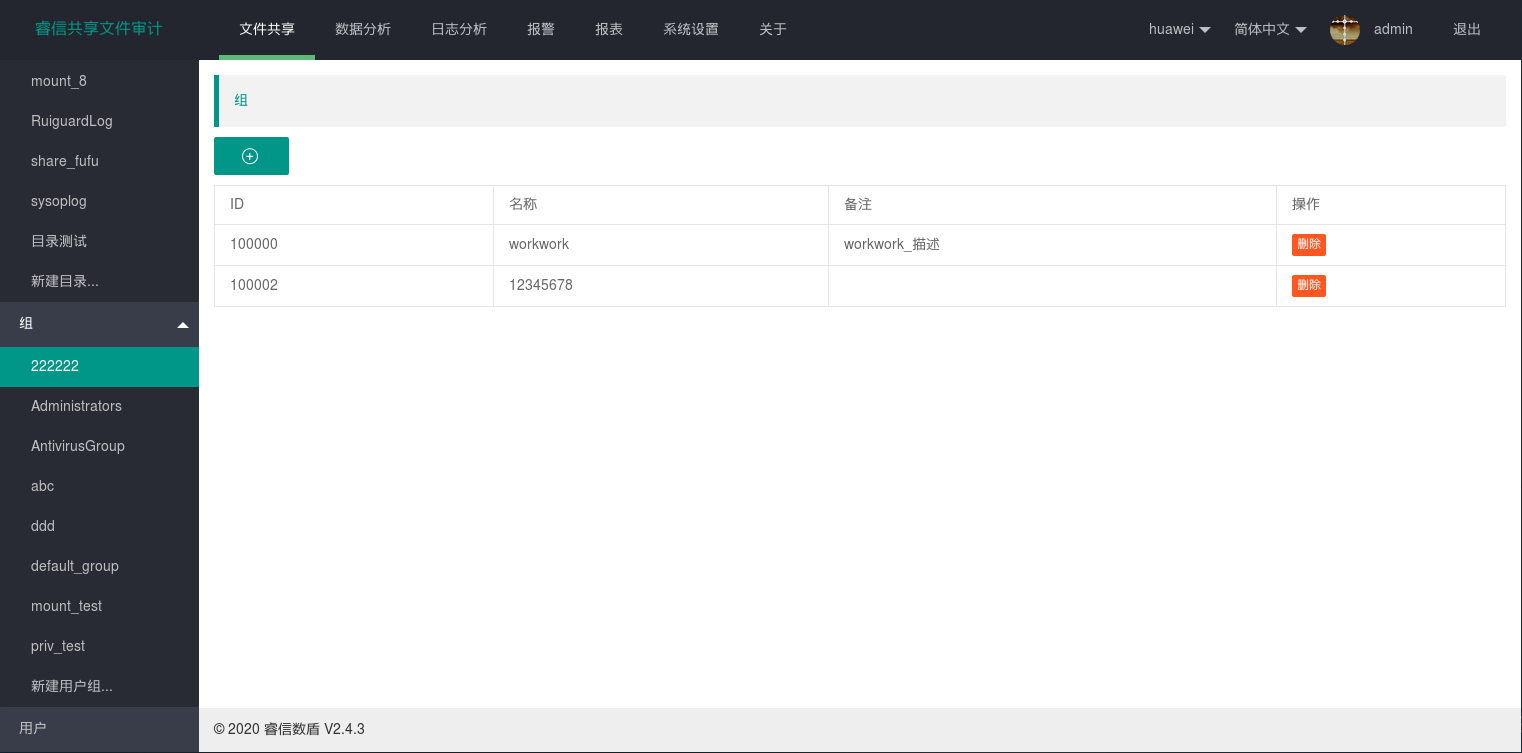


## 文件权限管理

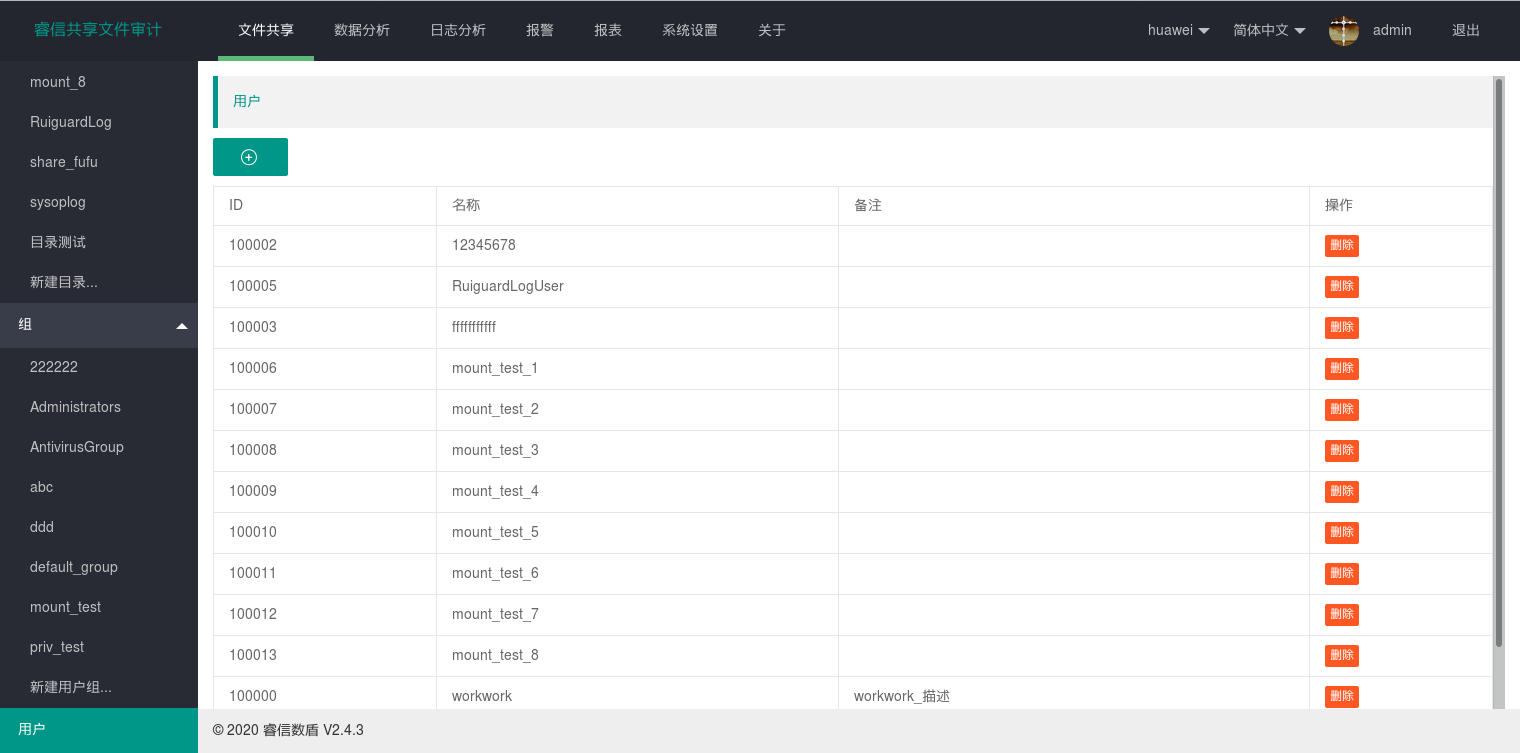
点击权限即可设置权限（下一版本通过客户端实现高级功能，如禁止文件泄密、禁止文件打印、禁止文件另存等功能）



可以增加组、对组内用户进行增加、删除操作

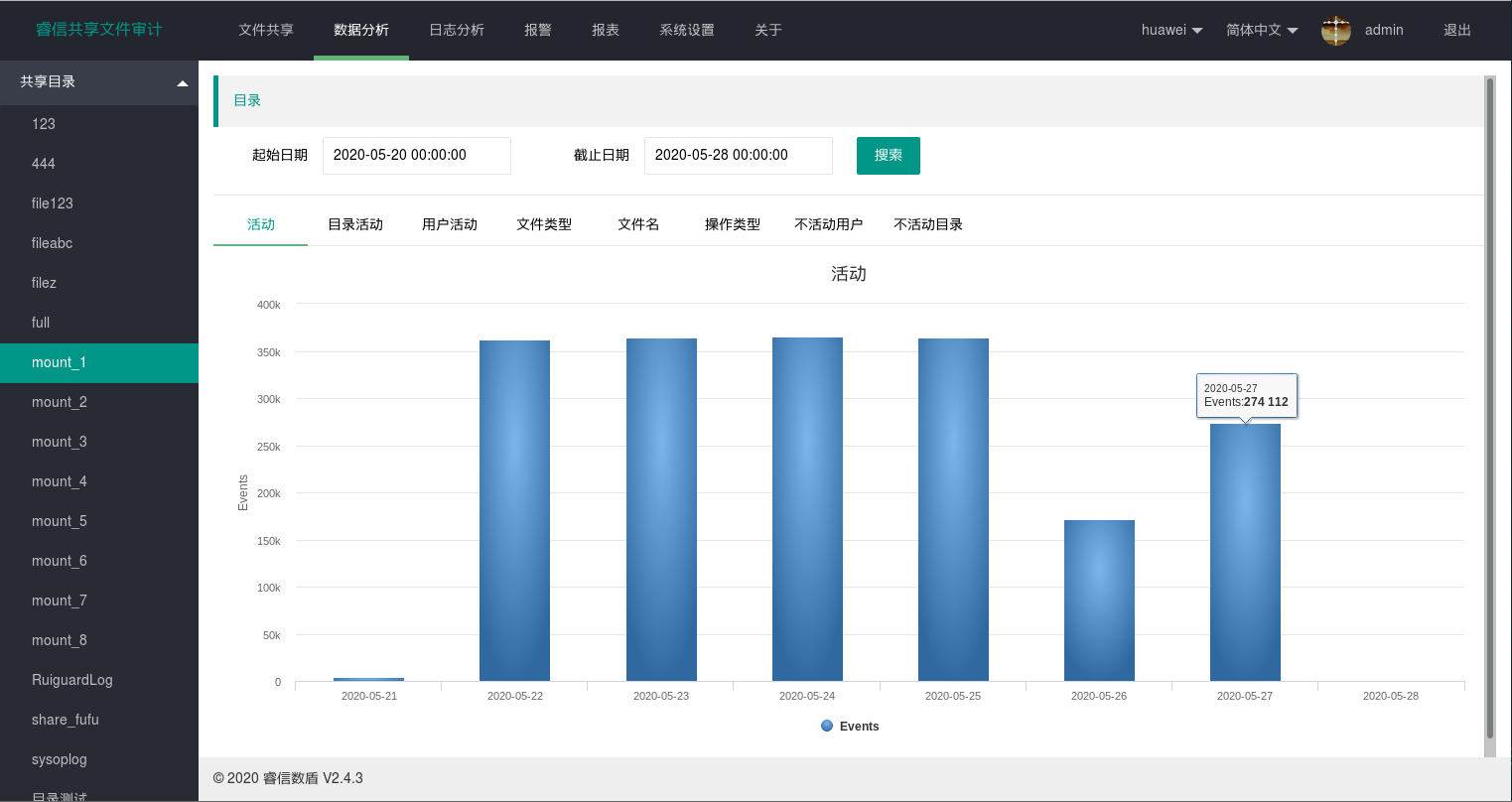


可以对本地用户进行增加、删除操作

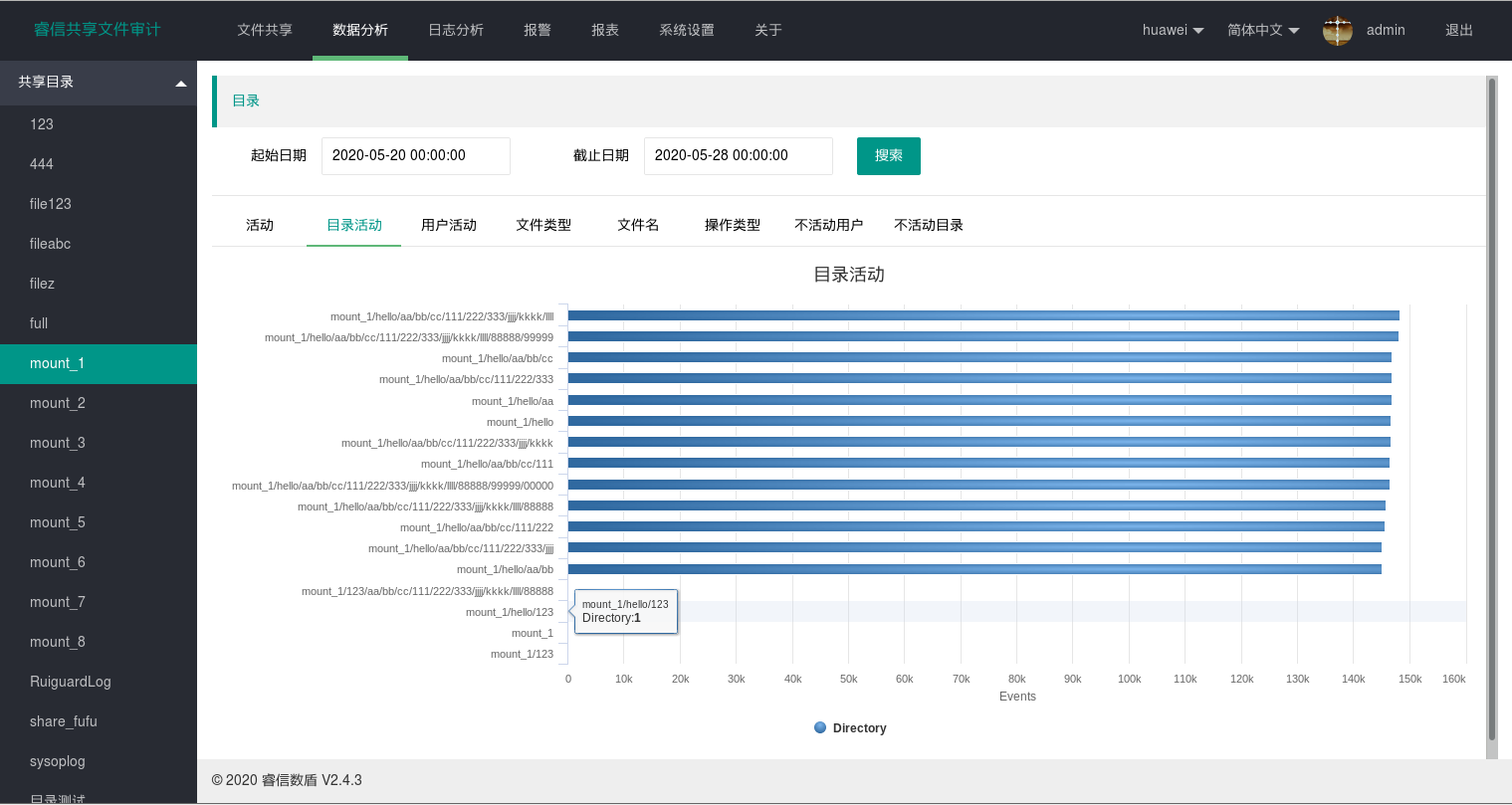


## 数据分析

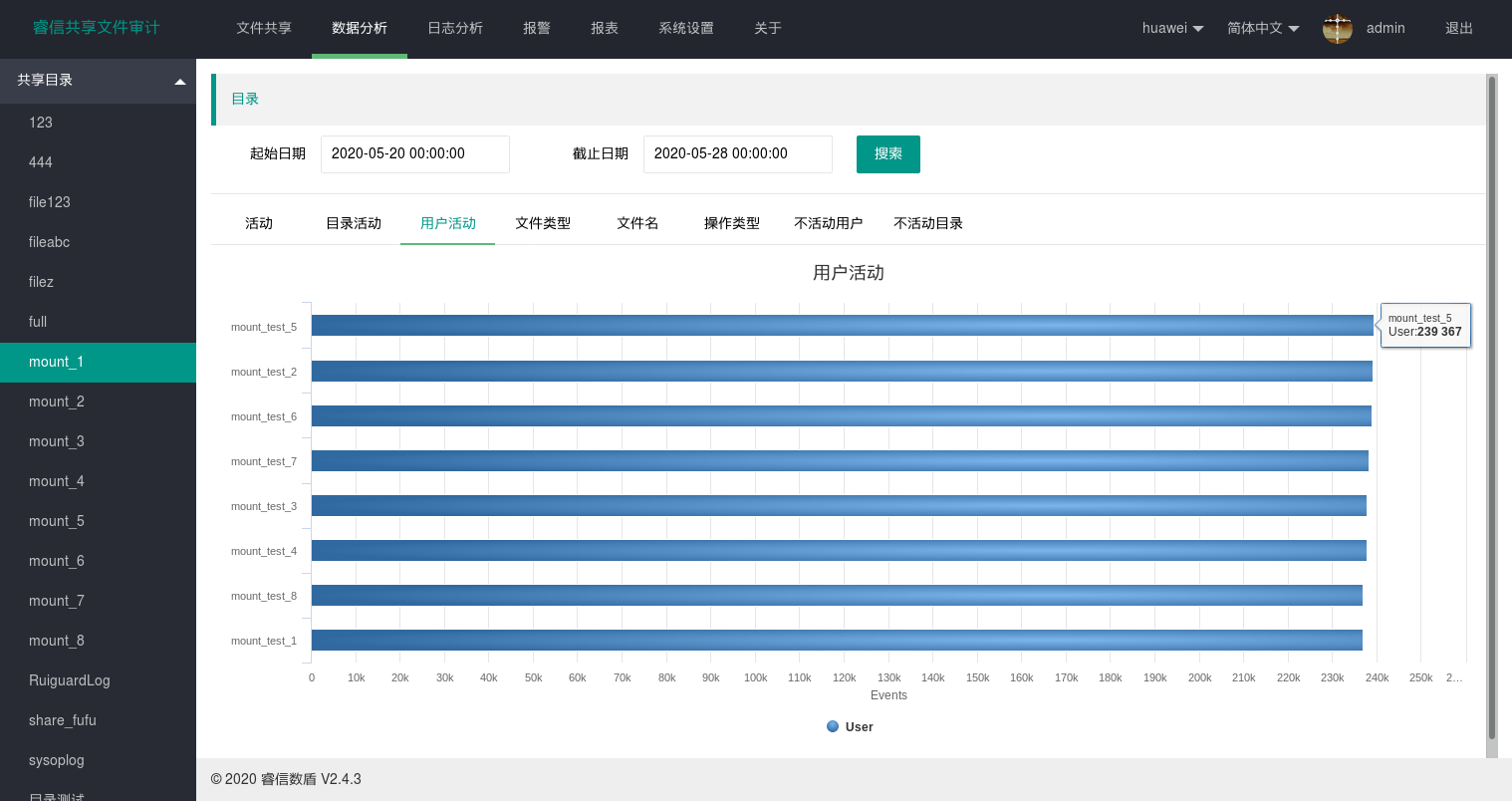
活动：



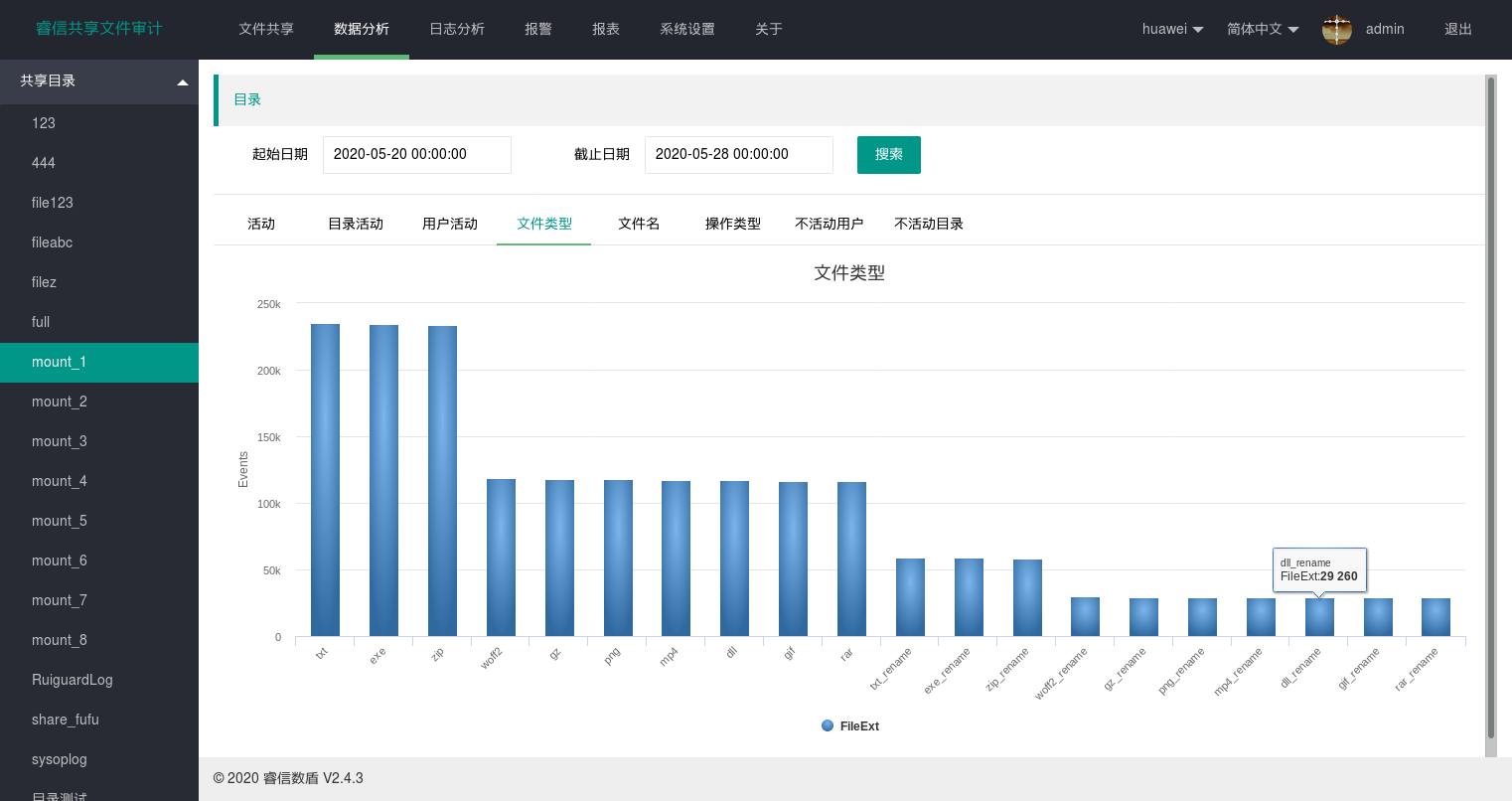
目录活动：



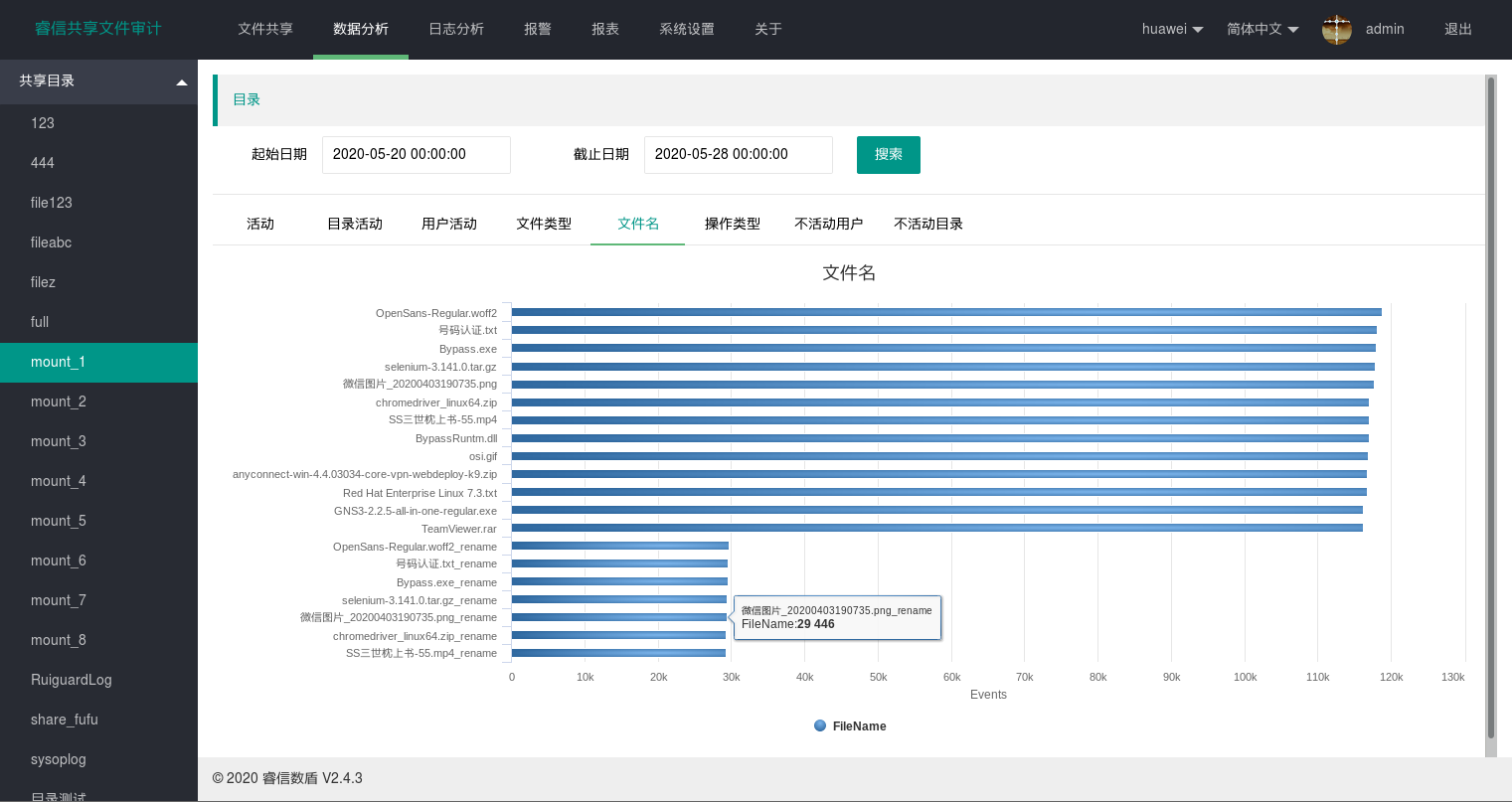
用户活动：



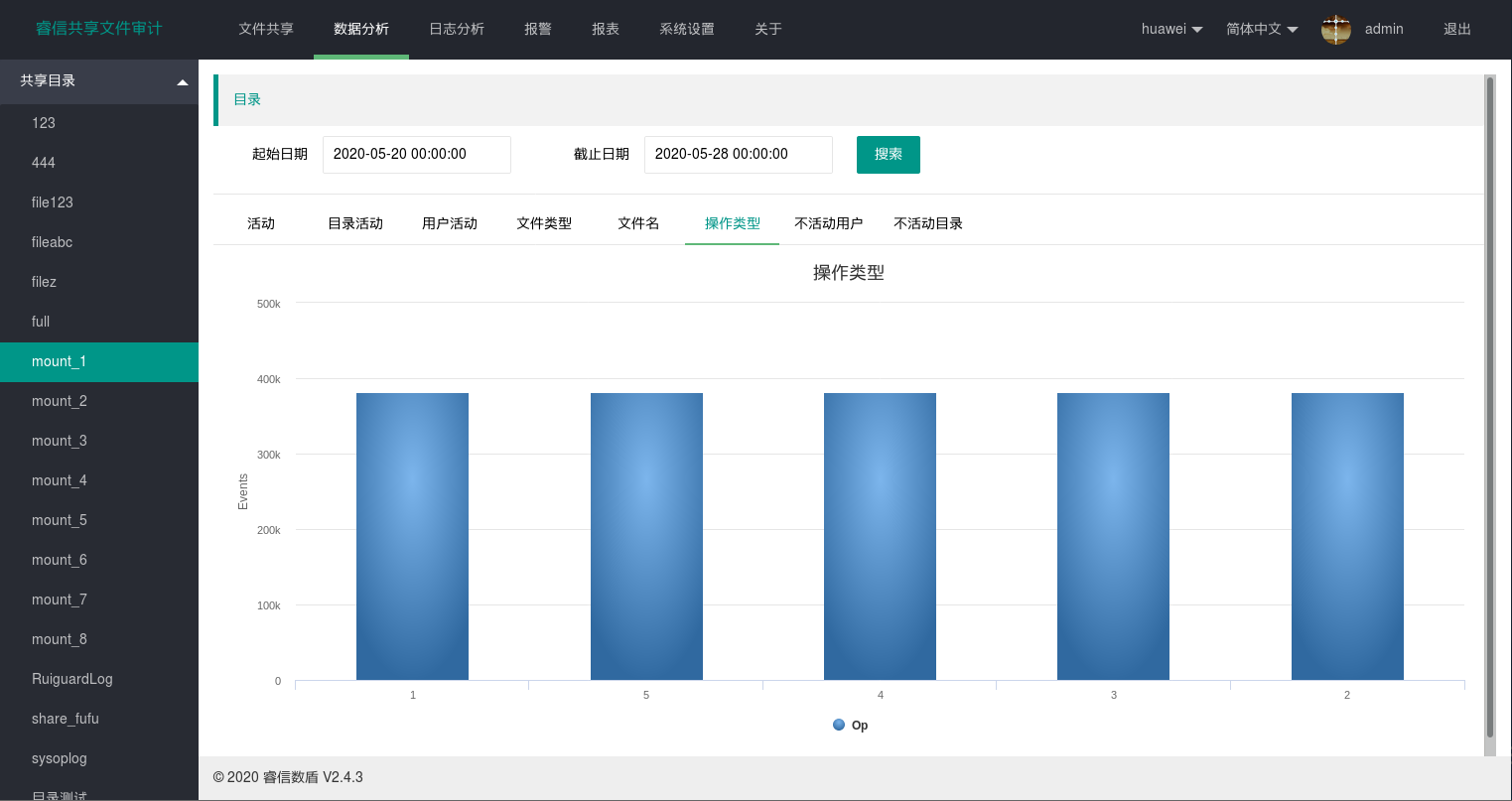
文件类型：



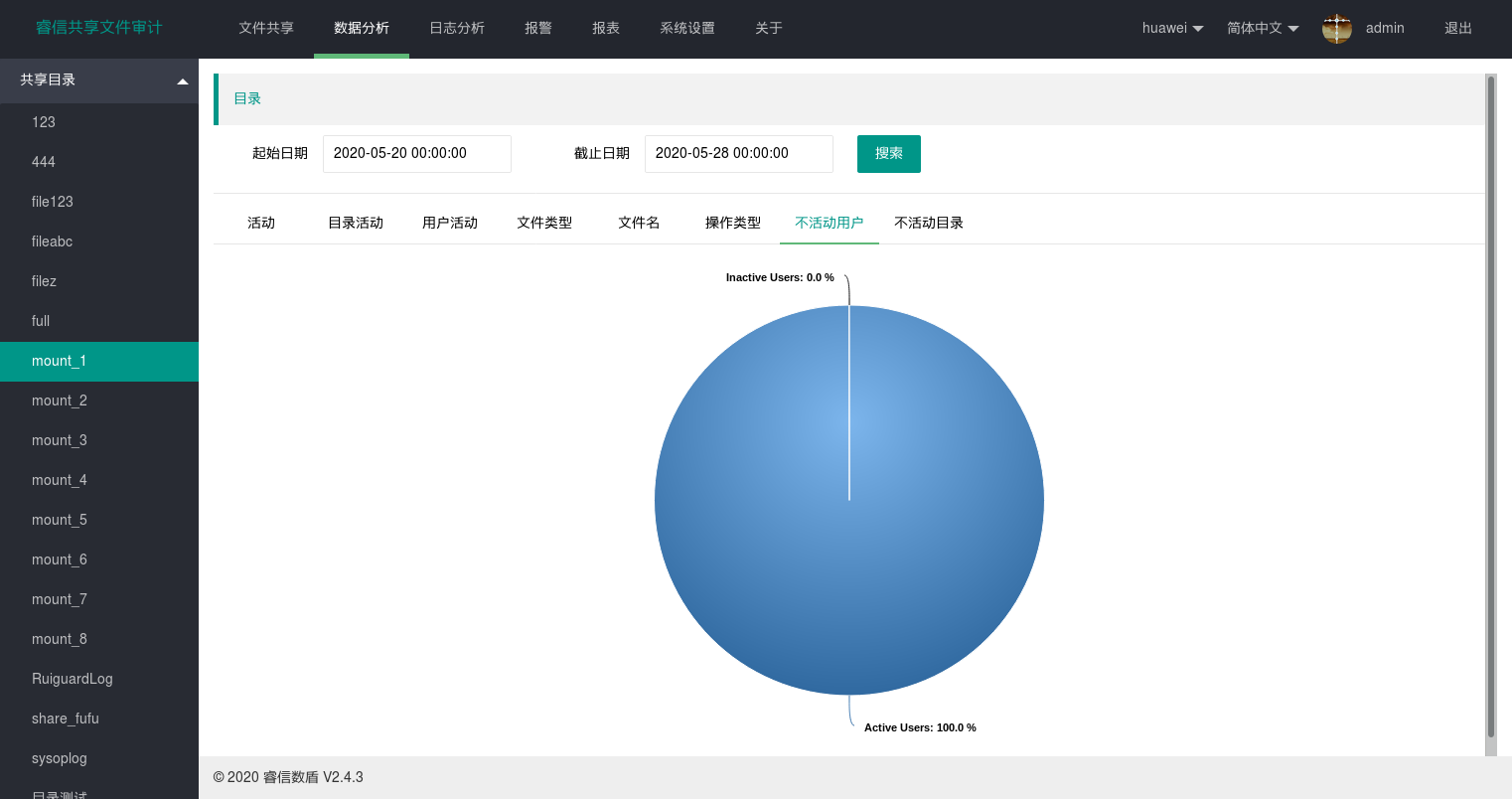
文件名：



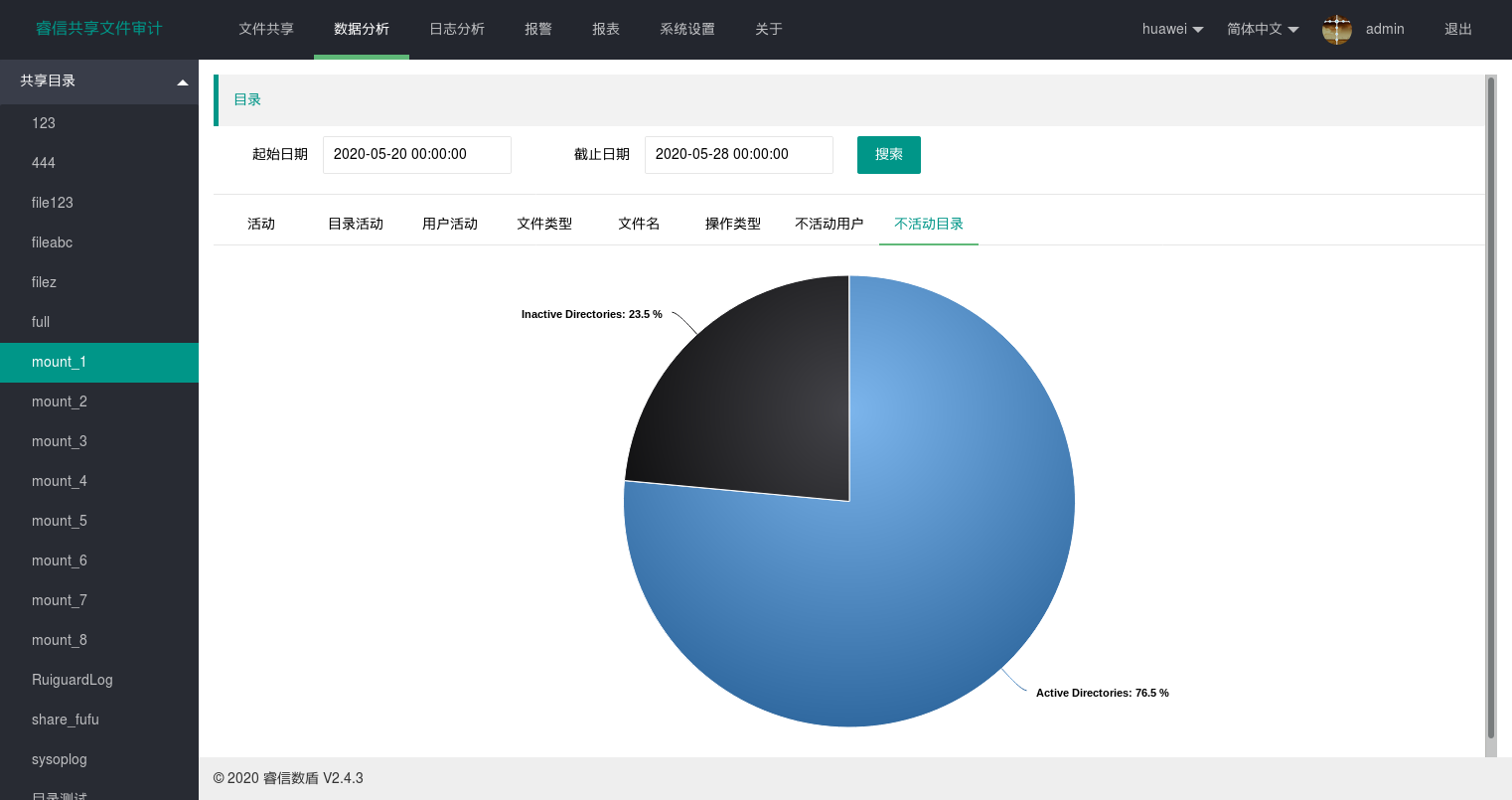
操作类型：



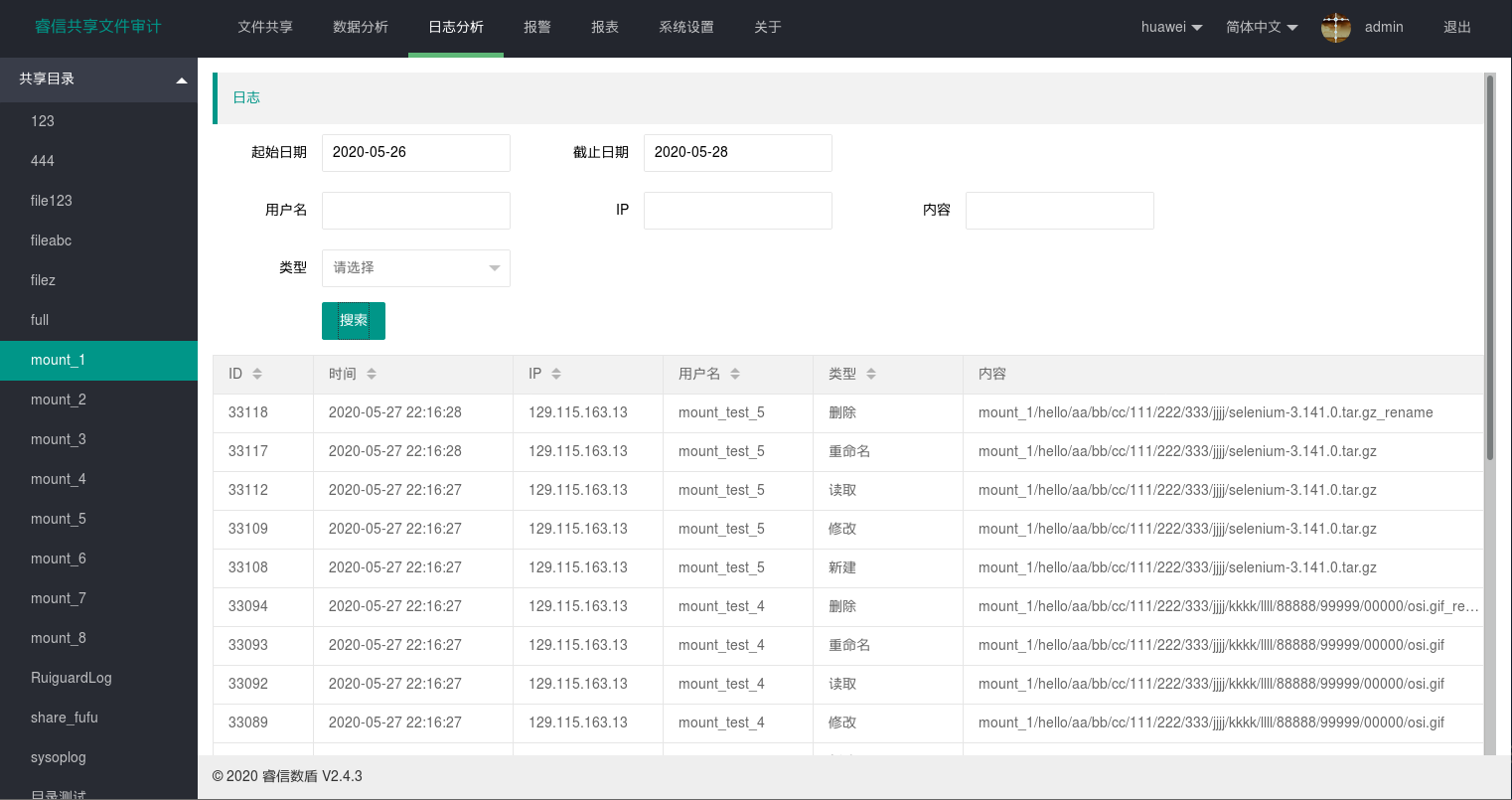
不活动用户：



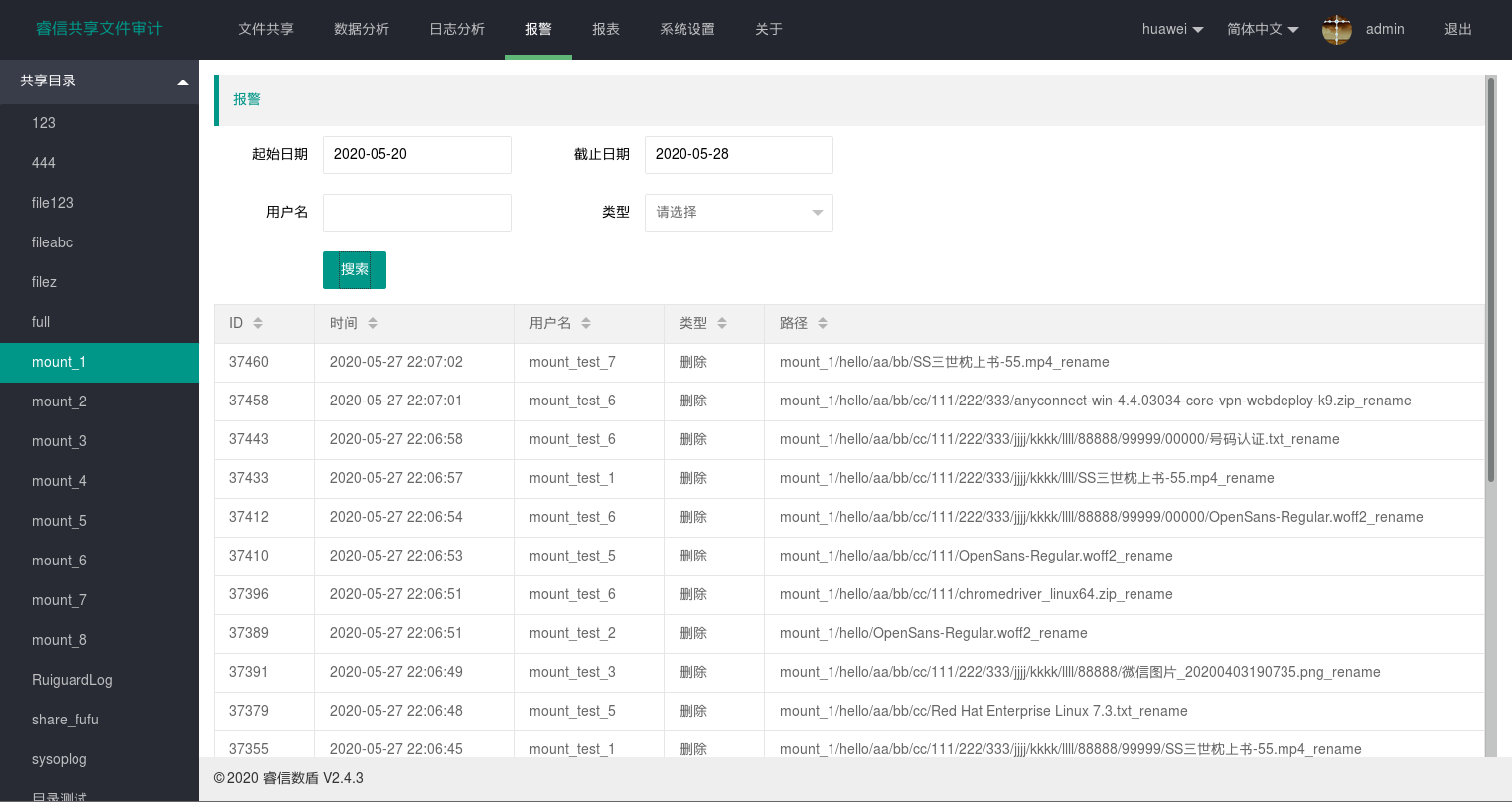
不活动目录：



## 日志分析

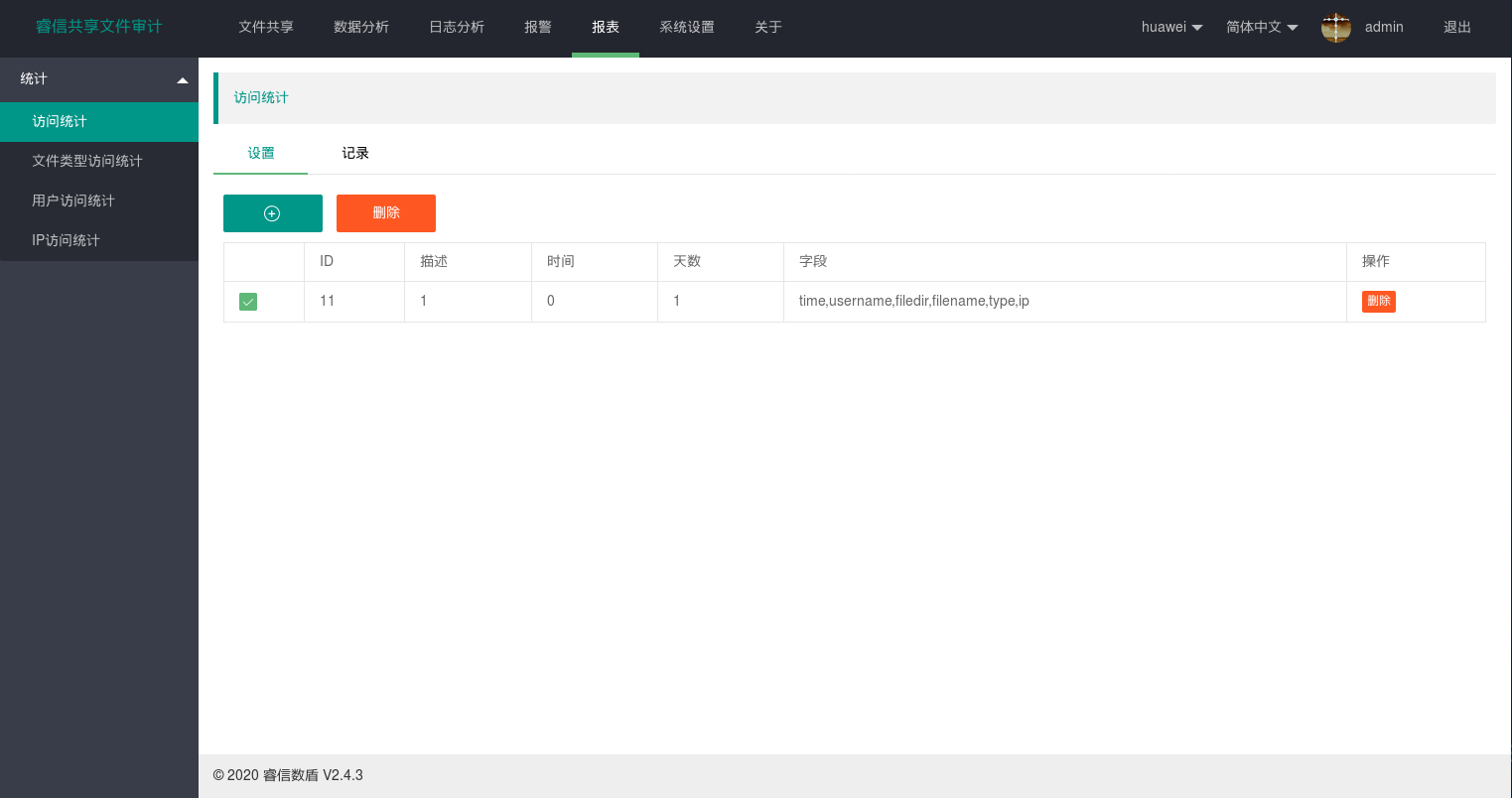


## 报警



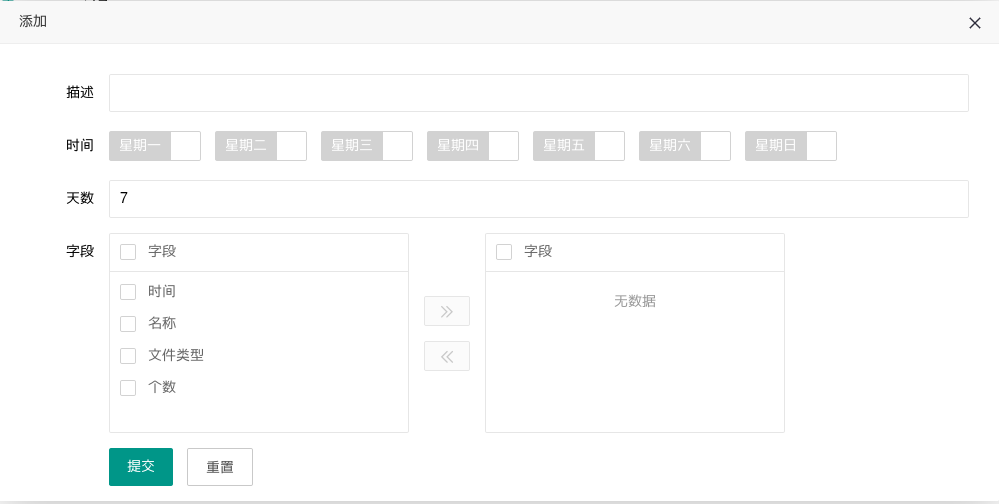
## 报表

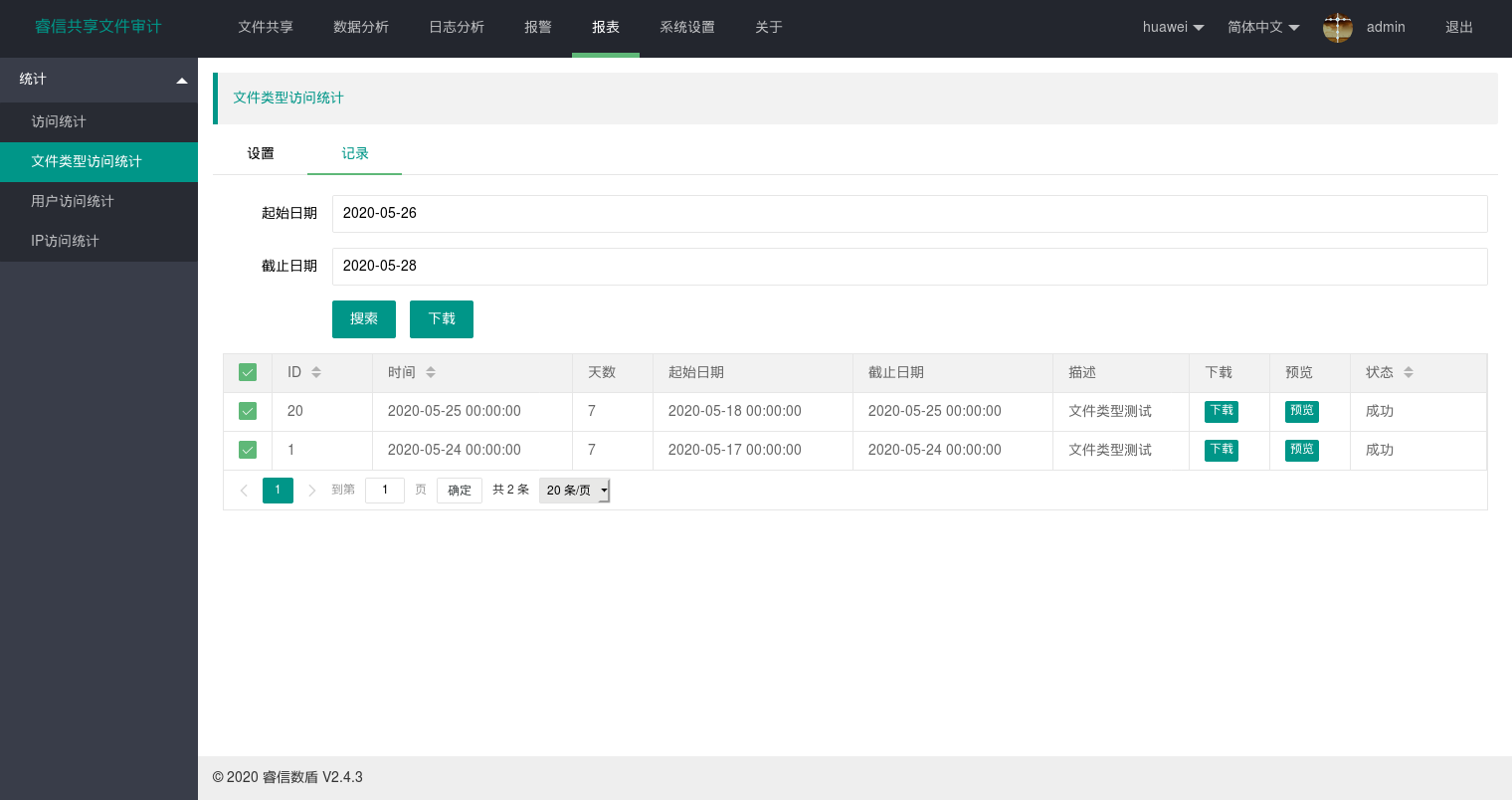
访问统计：



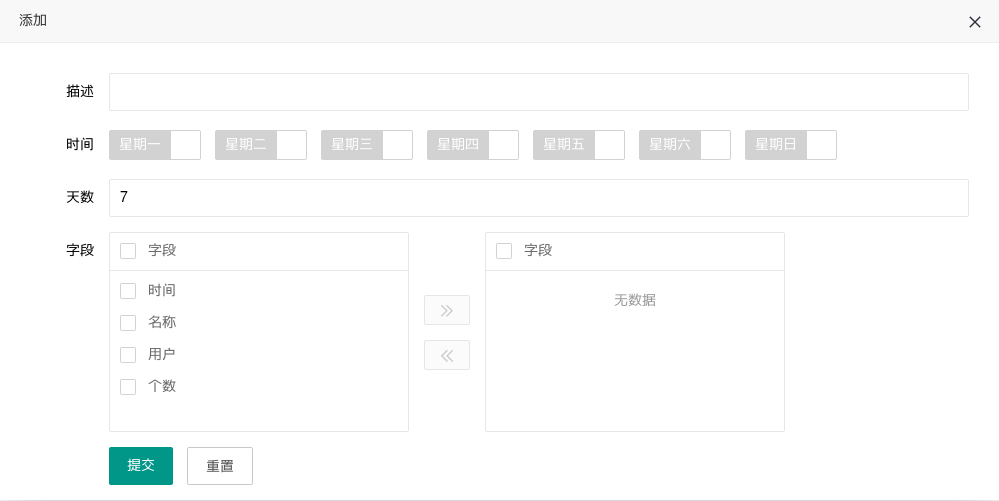


文件类型：

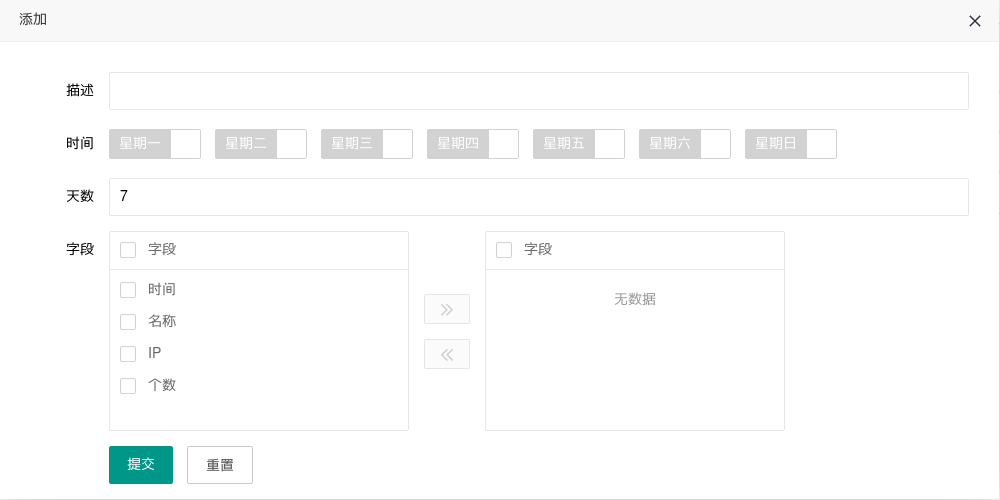




用户：

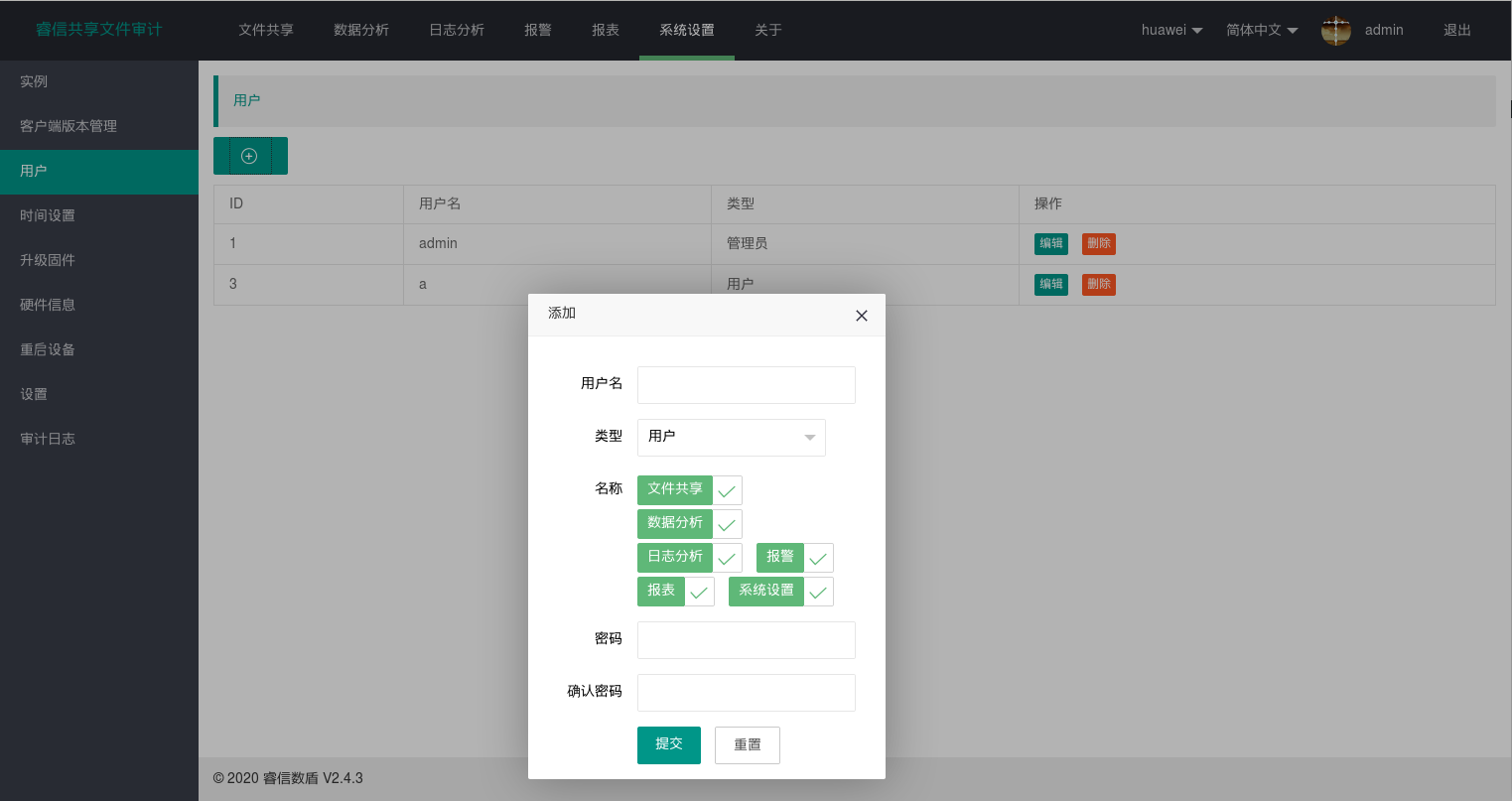


IP：

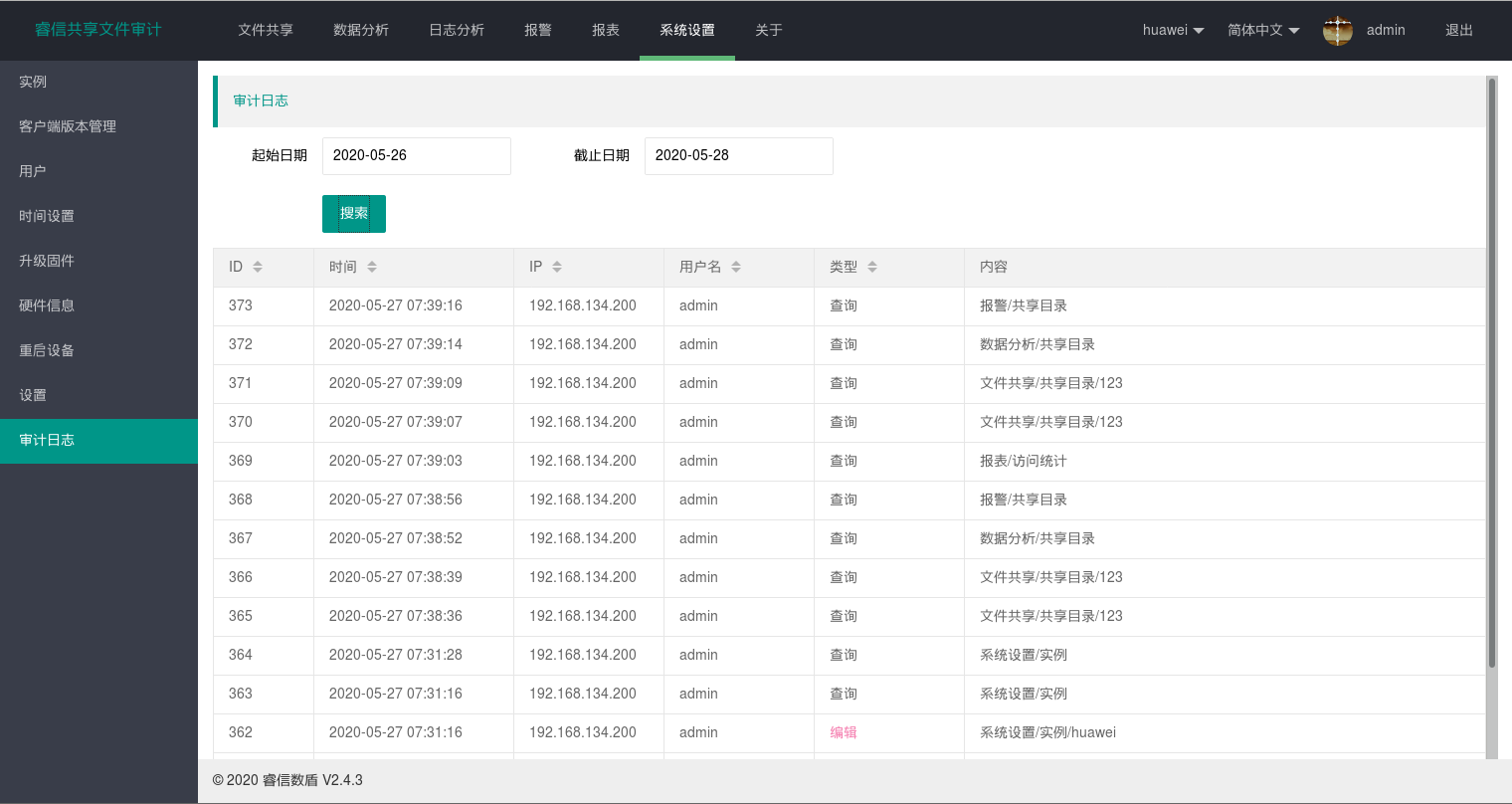


## 系统配置

用户管理：



用户操作日志审计：



**有任何使用问题、定制开发需求，请致电：010-80870460**