**针对Linux平台的工业软件运行行为监控模块验收报告**

# 项目概述

## 项目背景

项目组通过**公开询价**的方式，从广州道本信息科技有限公司购置针对Linux平台的工业软件运行行为监控模块，于2020年12月签订采购合同。项目组依照《工业和信息化部电子第五研究所工业软件运行行为监控模块采购项目合同》和《工业和信息化部电子第五研究所工业软件运行行为监控模块采购项目询价文件》指标对工具进行验收。

## 针对Linux平台的工业软件运行行为监控模块简介

针对Linux平台的工业软件运行行为监控模块支持对Linux内核版本3.10以上的操作系统进行系统软件的运行行文监控。其中支持的监控行为包括文件读写、进程调用、设备控制、网络访问、文件对象权限修改等。

针对不同软件运行行为的监控结果，支持通过运行用户、行为时间等基础条件进行搜索汇总，并且支持搜索结果导出xlsx文件，同时支持全量监控结果导出xlsx文件。

支持记录软件行为的历史监听记录，支持通过HTTP接口上报监控结果和下发监控任务。

## 参考资料

项目组验收是依据《工业和信息化部电子第五研究所工业软件运行行为监控模块采购项目合同》和《工业和信息化部电子第五研究所工业软件运行行为监控模块采购项目询价文件》中的合同指标进行验收。

# 验收定义

## 验收方式

针对Linux平台的工业软件运行行为监控模块的验收工作是由工具厂商和课题组成员共同参与，课题组提供测试环境，工具厂商指引课题组成员对工具进行操作。项目组主要是通过操作截图、测试验证等方式进行验收。

## 验收范围

针对Linux平台的工业软件运行行为监控模块验收范围和指标如下所示：

2.2.1 支持Linux 64位操作系统（内核版本3.10以上）中运行的软件行为监听功能。

2.2.2 可以选定软件，实现对软件的行为监听功能。

2.2.3 至少支持但不限于以下种类的行为监听：

2.2.3.1 网络监听：能够记录网络连接发起地址记录、发送及接收的数据包内容。

2.2.3.2 进程监听：能够记录受监听进程内创建子进程的调用，以及对其他进程的调用和交互行为，能够对进程的自启动行为进行监听。

2.2.3.3文件监听：能够监听文件访问和修改，在修改发生前备份文件数据，能够记录文件写操作的内容，能够对文件权限的修改进行监听。

2.2.3.4 操作系统关键系统调用监听：能够监听并记录软件进行系统重要调用的行为及内容。

2.2.3.5 设备监听：能够记录设备及驱动的访问记录与访问内容。

2.2.4 具有简单的UI管理界面，具备待监听软件的管理功能，具有对指定软件行为数据查看、筛选、标记等分析功能。

2.2.5 能够记录软件行为的用户身份归属，记录行为所属的用户身份，并能够在管理界面中根据用户身份进行条件筛选。

2.2.6 具有对外交互数据接口，能和统一的门户平台进行数据交互、任务下发管理等。

2.2.7 提供产品的全部源代码，并可以正常编译。

2.2.8 提供产品操作手册与安装部署手册。

## 验收标准

对验收范围内的指标进行一一确认，在确认过程中，根据结论应满足以下条件，则测试结果为通过，否则，测试结果为不通过：

（1）所有测试项的测试结果均为通过；

（2）测试结果存在不通过的项，厂商应对不通过项进行整改，然后进行再次验收，确保发现的错误已全部修复。

# 验收过程

## 测试流程及介绍

### 产品形态验证

对工具的产品形态（软件版）的形式进行验证。

### 工具能力验证

本软件主要包含软件行为监控、行为结果查询、行为结果导出等功能：

（1）软件行为监控的主要功能：可添加Linux软件运行命令，添加的运行命令可列在软件列表中。针对添加的运行命令可以使用启动并监听和已启动进程监听功能。启动的软件进程可在界面中显示具体的进行信息。

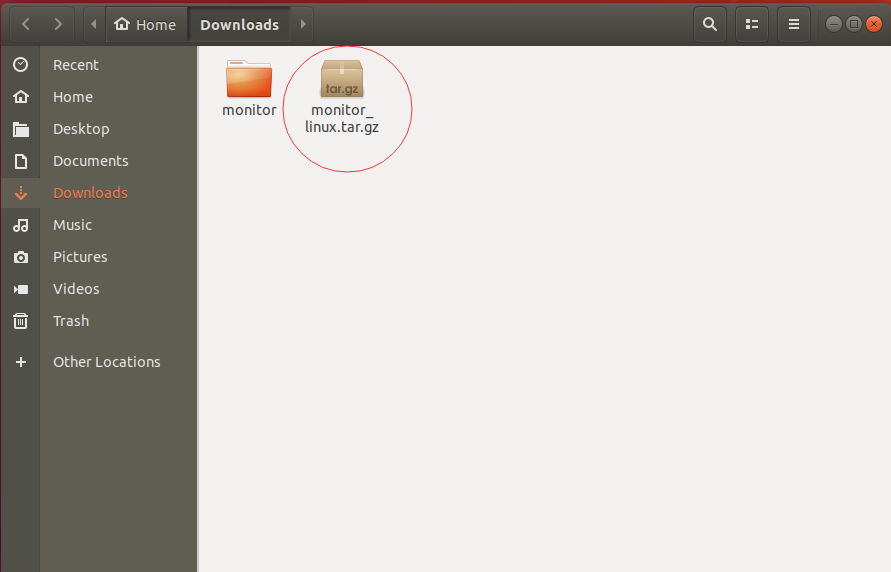
（2）行为结果查询的主要功能：可以根据文件读写、进程调用、设备控制、网络访问、文件对象权限等不同类别行为进行分类查询。

（3）行为结果导出的主要功能：可以根据软件监控行为的结果进行文件导出，支持xlsx格式文件导出。

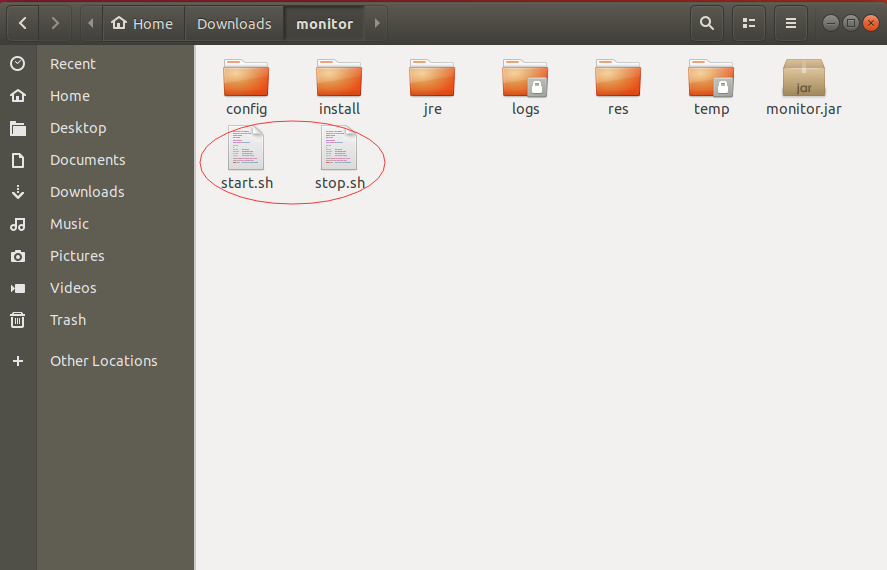
## 测试操作及控制信息

### 产品形态验证

产品形态如下图所示：



产品采用软件的形式，其中软件为tar.gz的压缩包文件，解压后可直接通过命令行启动使用运行，如下图。

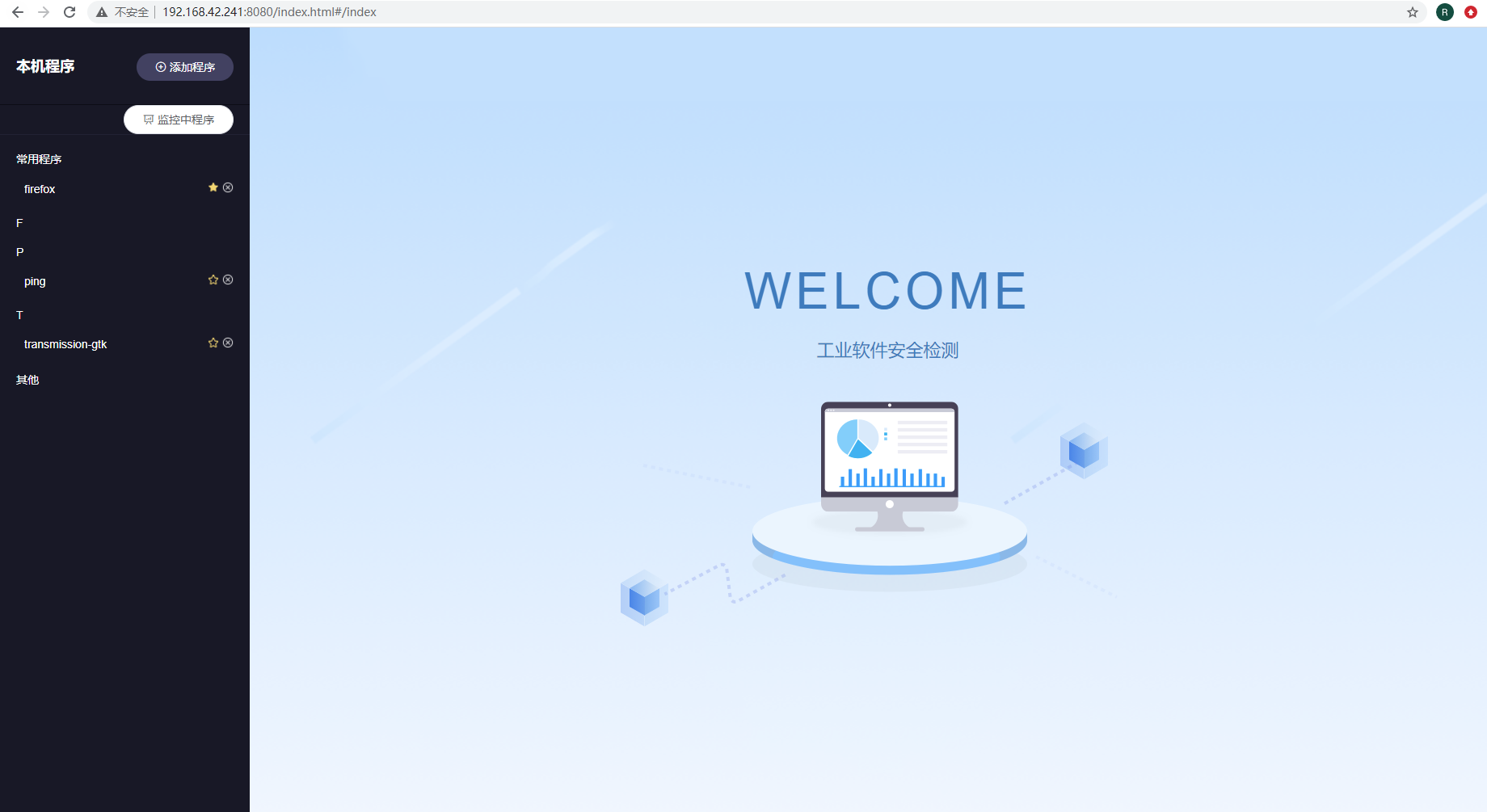


产品满足合同中对于软件形态的相关要求。

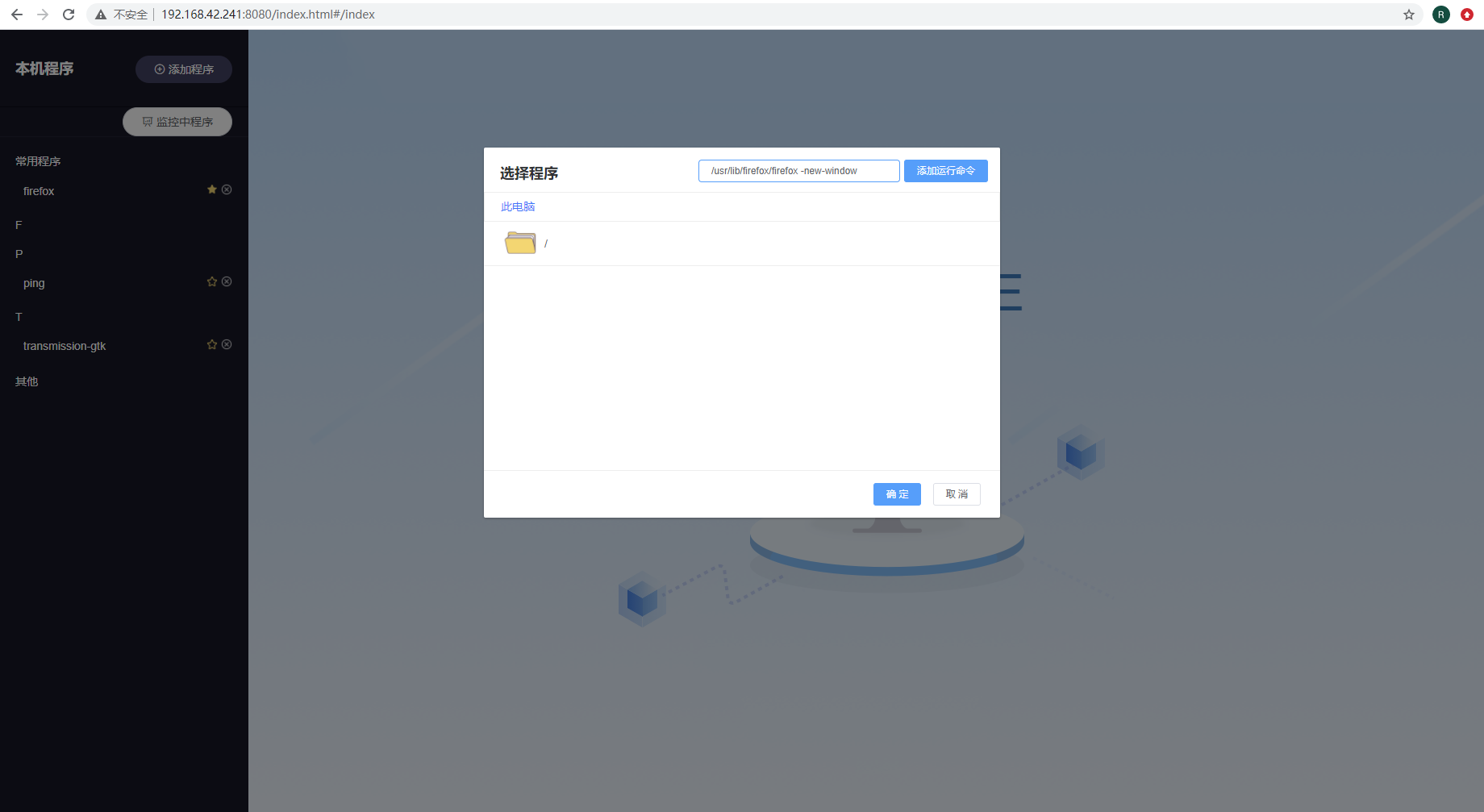
### 软件行为监控能力测试

监控软件管理：用户可以自行添加可执行程序或自行添加可执行命令，并对添加的运行软件进行监控。测试步骤如下：

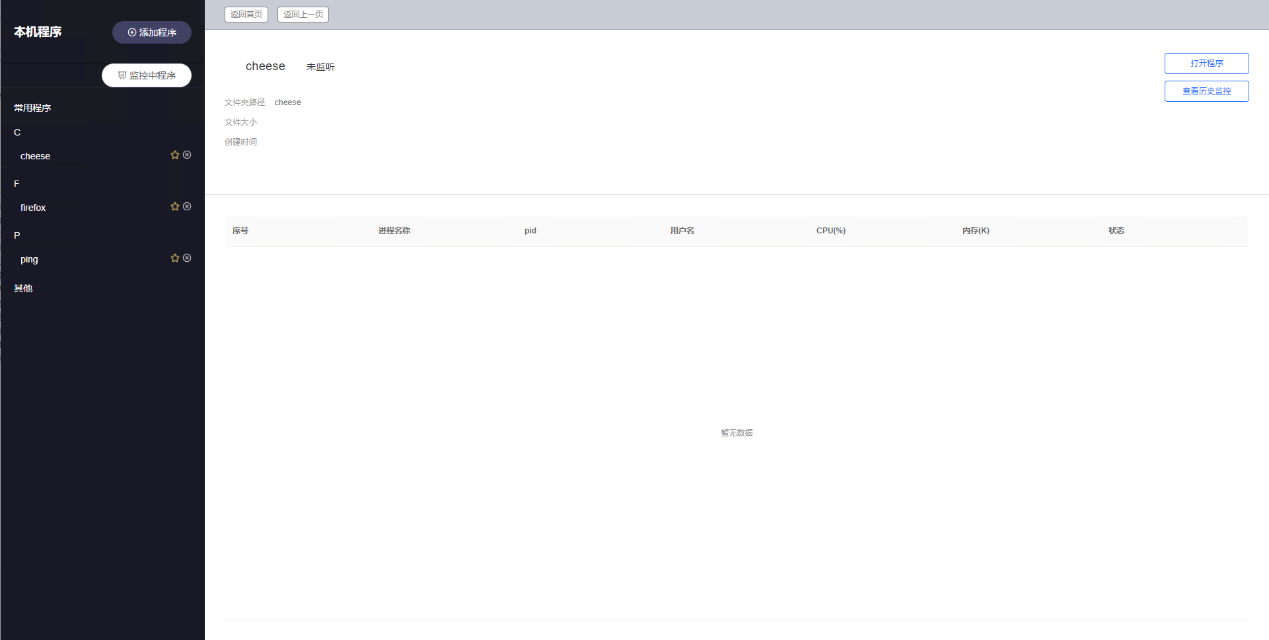
通过web登陆监控模块系统。



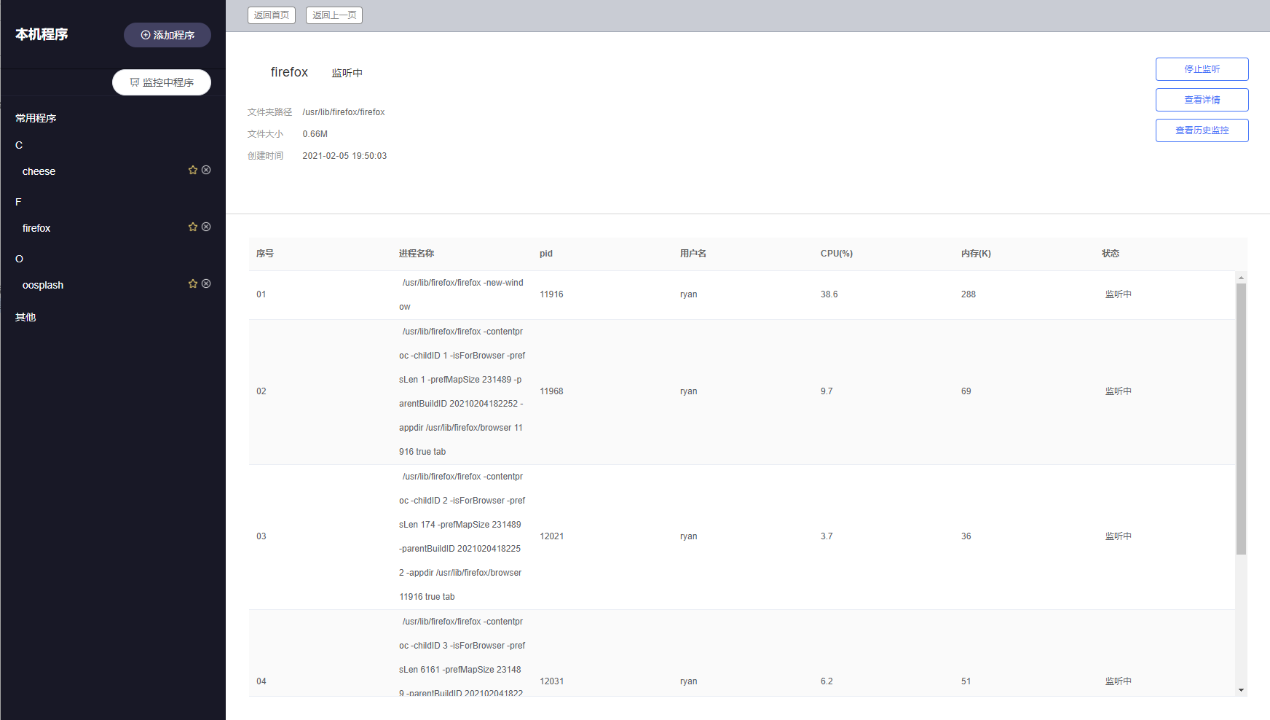
点击左上角添加程序，在弹出输入框的右上角输入要添加的命令行，点击添加运行命令添加到软件列表种。 如firefox的启动命令：/usr/lib/firefox/firefox -new-window



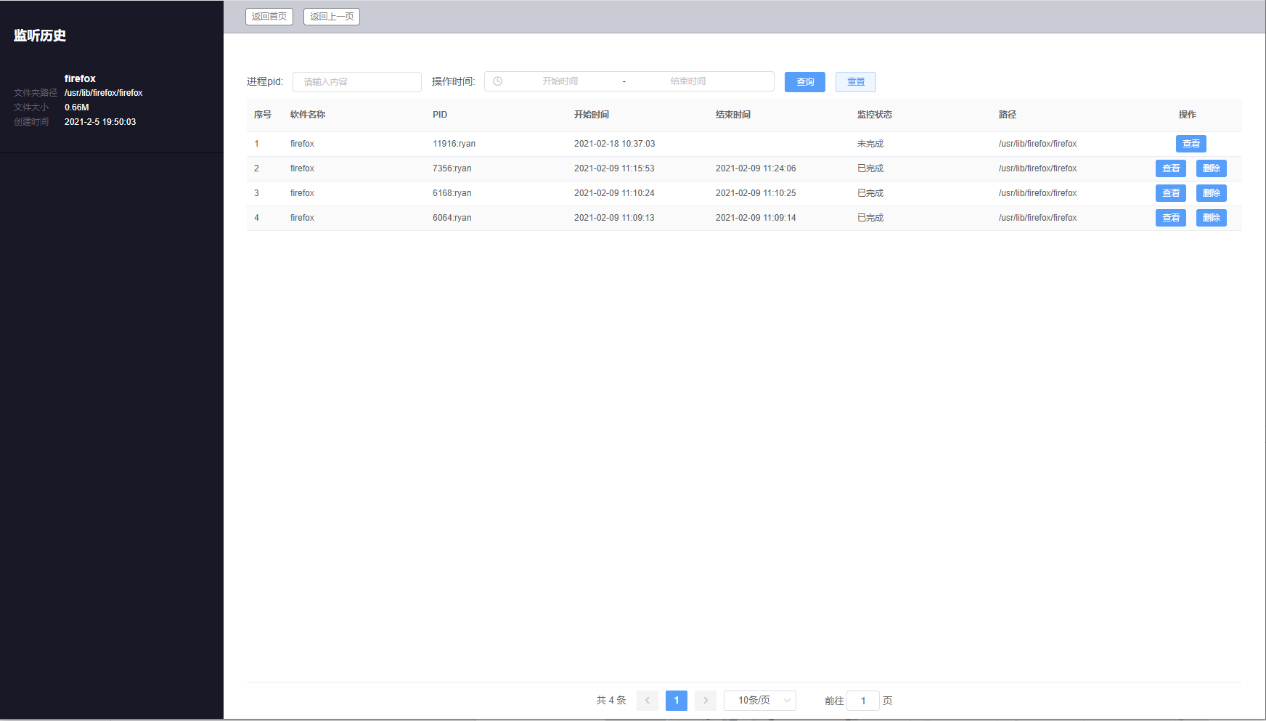
点击左侧软件名称打开软件详情。



详情页中将会显示软件的详细信息和监控状态，正在运行的软件会显示对应的进程列表。



点击打开程序可以启动程序并进行监听，监听中的软件点击查看详情可以进入监听行为查询界面。点击监控历史可以查询历史监控记录。

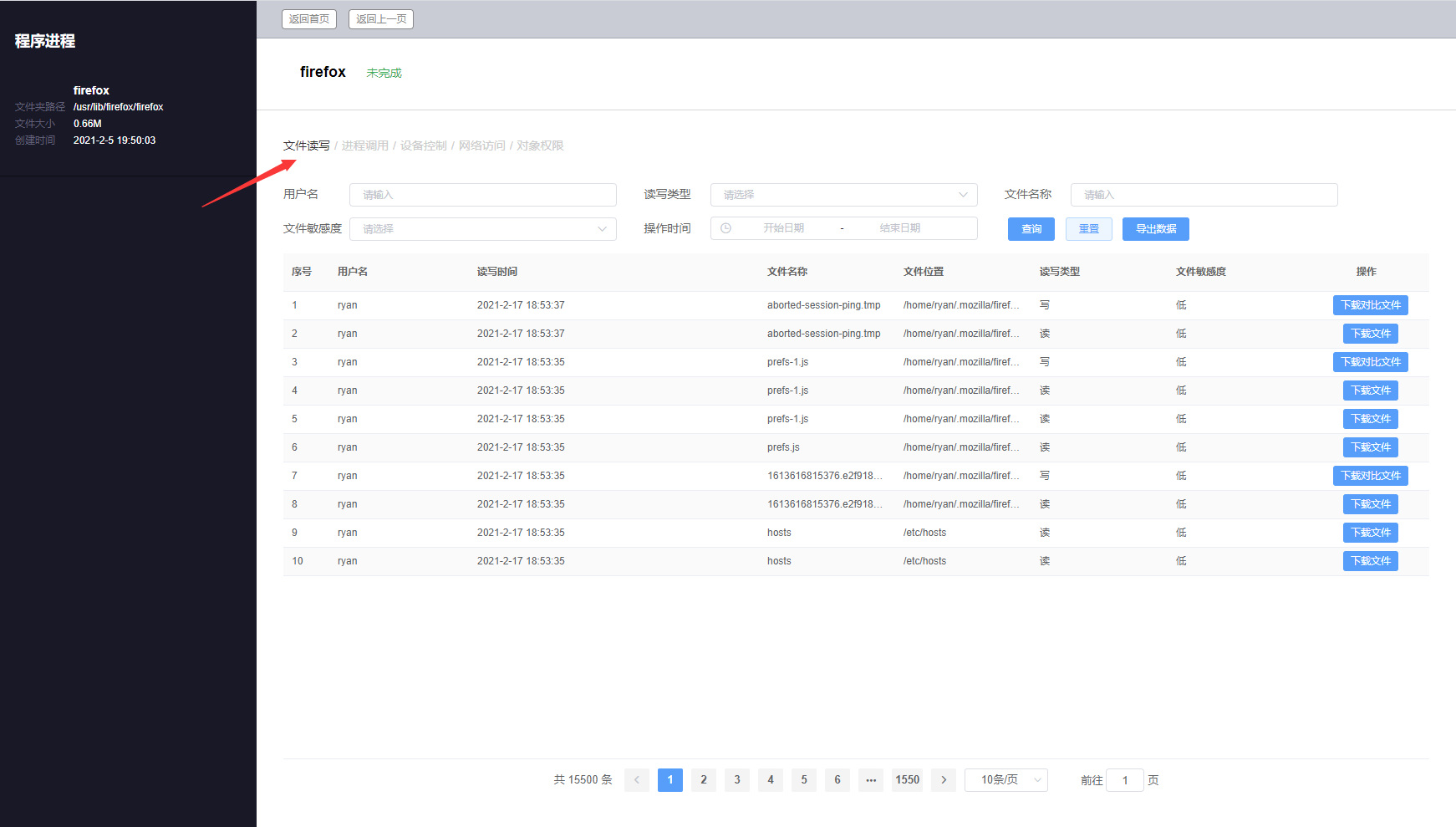


### 软件行为结果查询测试

监控模块支持文件读写、进程调用、设备控制、网络访问、对象权限等行为进行查询。

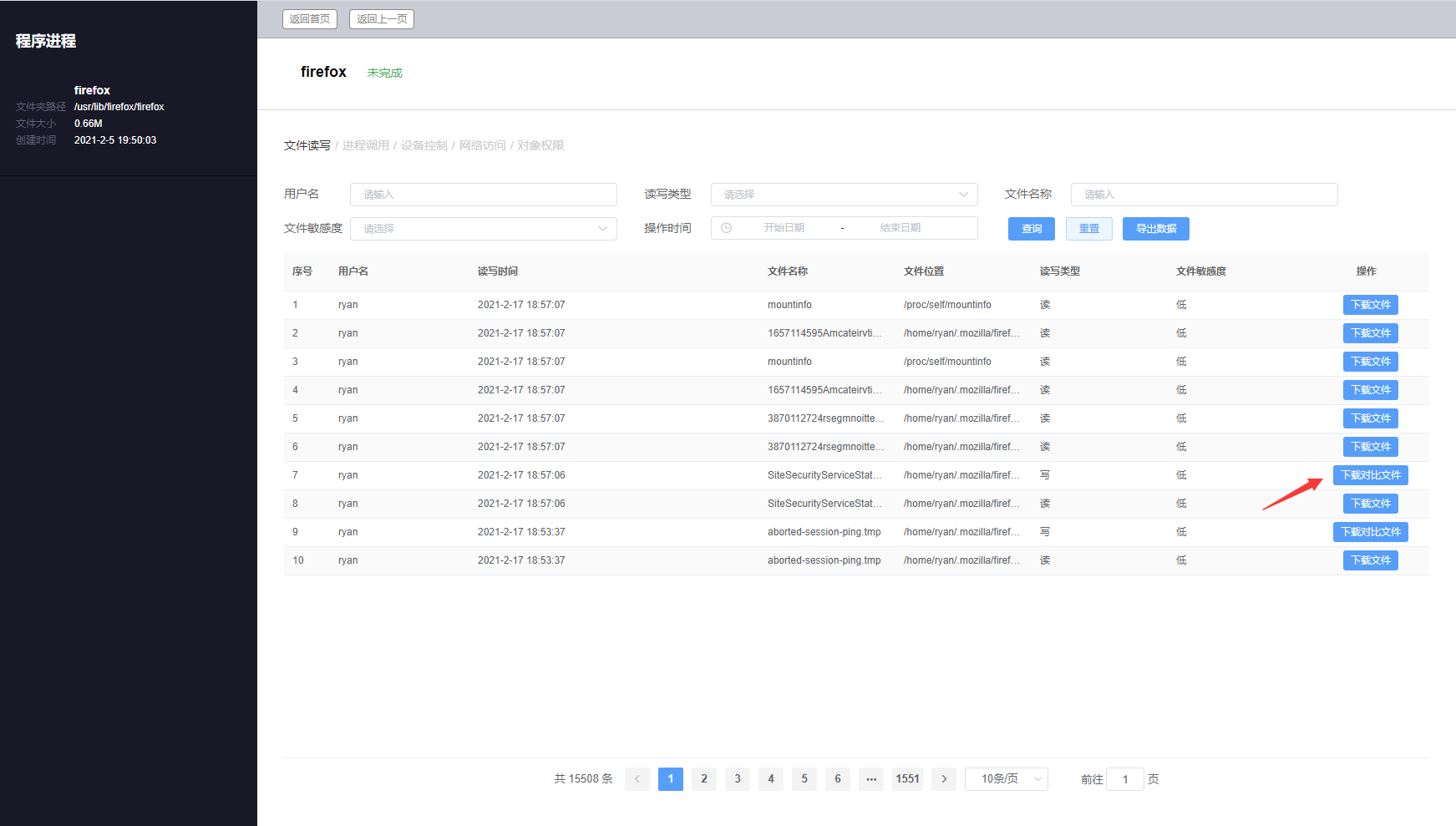
文件读写监听

1.进入监控详情，切换到文件读写监听栏目

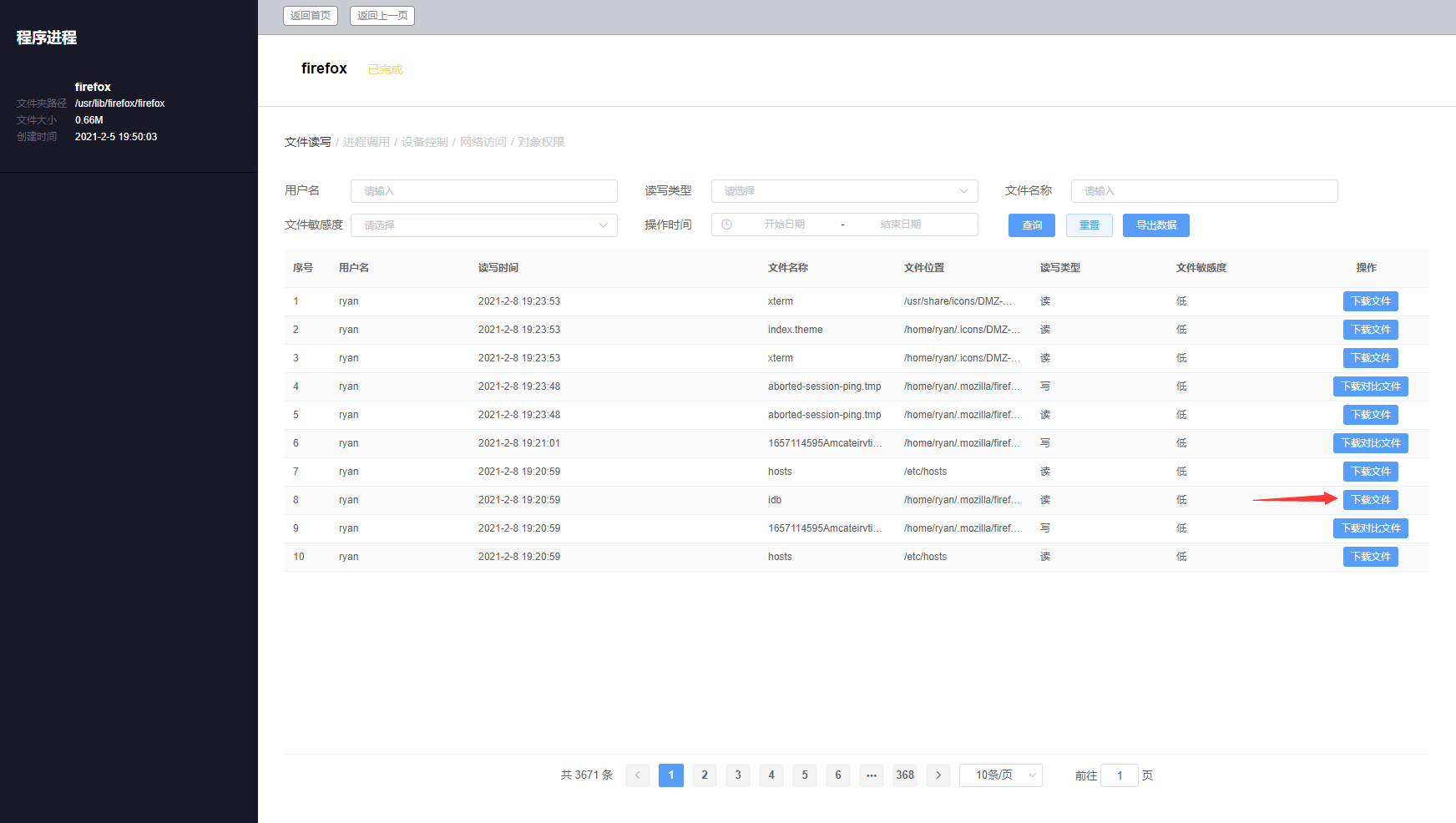


1. 针对写文件记录，可以进行“下载对比文件”操作，下载回来的是zip包，包含old和new 2个文件，分别为写入前和写入后对比文件。 用户可以使用其他文件对比工具进行文件变更细节对比。

如果写入的文件为新文件，则下载回来的zip包中不含有old文件记录。

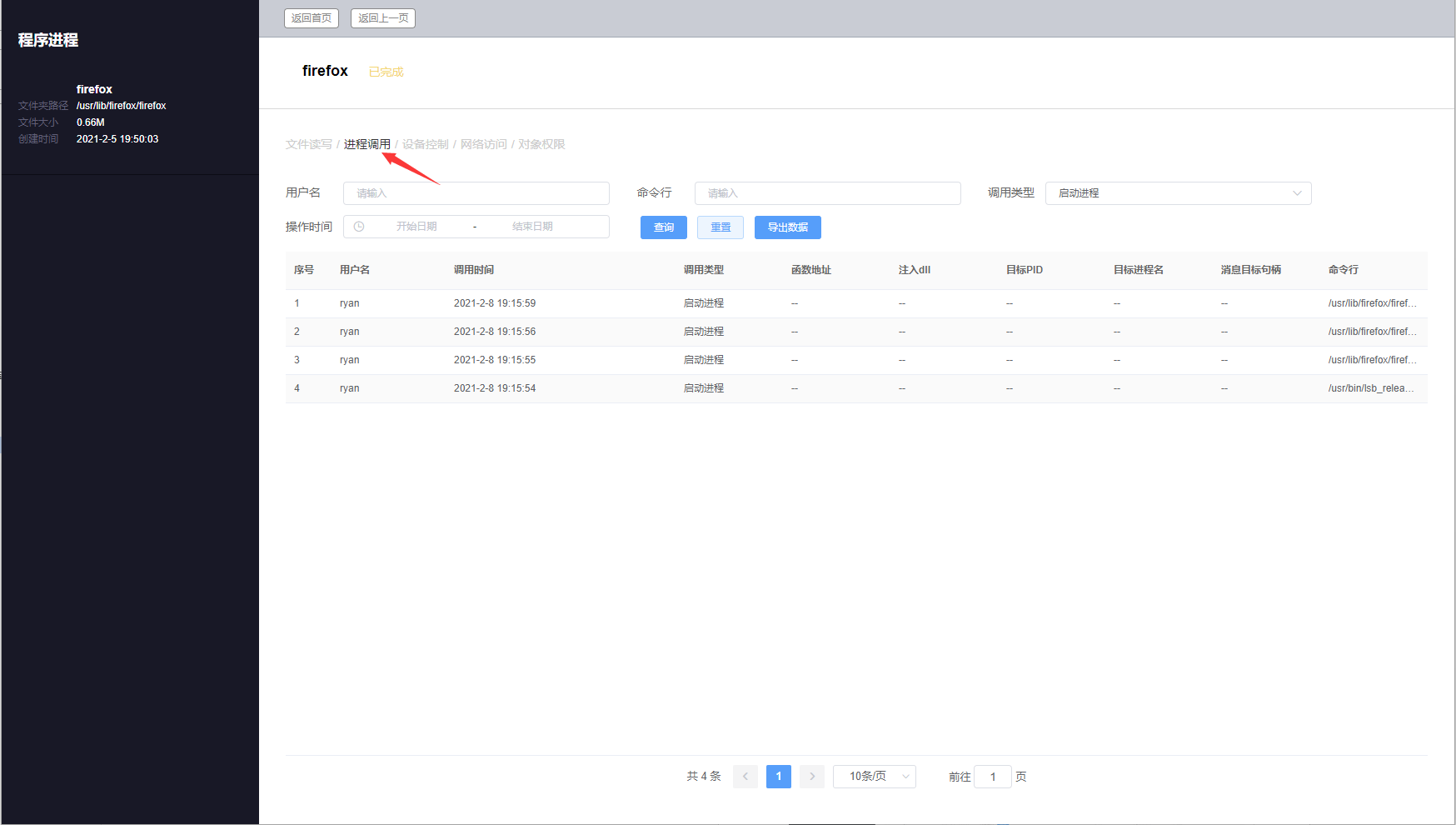


1. 针对读和删除类型的文件操作，可以进行“下载文件”操作，会下载系统备份的文件。



进程调用

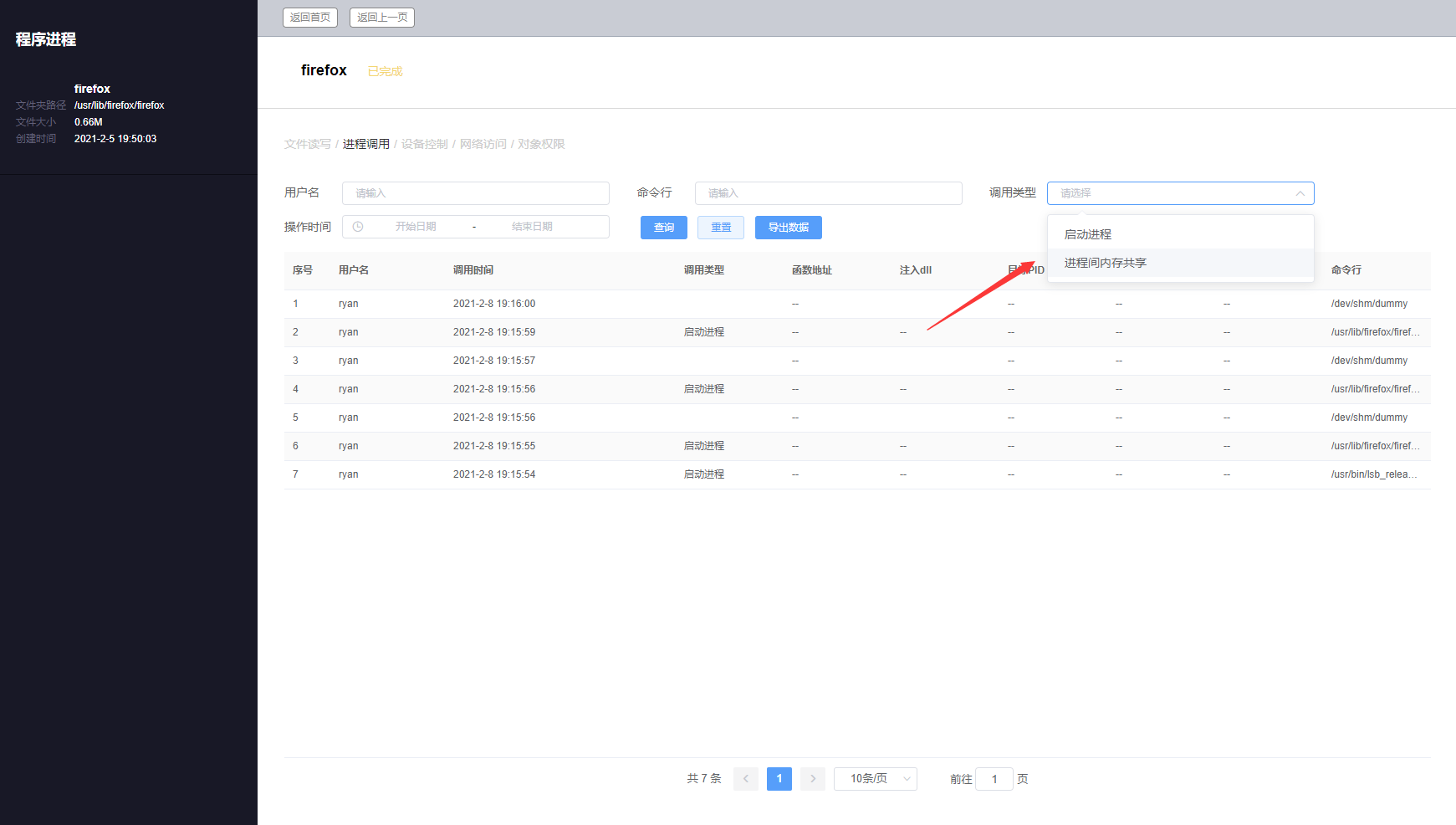
1.进入监控详情，切换到进程调用栏目



2.系统监听了3大类常用进程调用，包括启动进程、进程注入和消息通讯。

启动进程: 表示软件启动了其他进程

进程间内存共享：表示软件进行内存共享的常用的进程间调用方法。

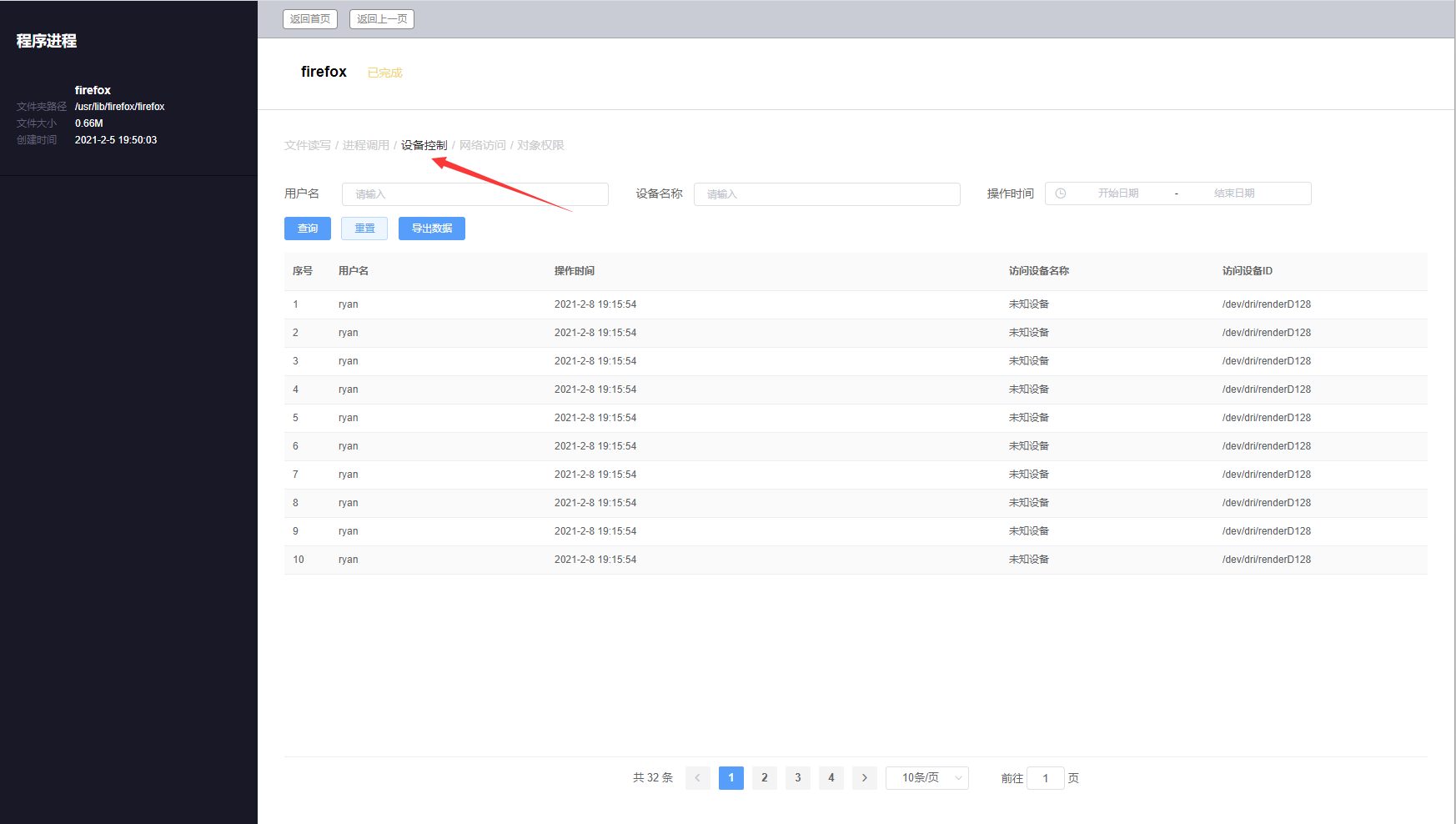


3.启动进程： 界面会显示具体的启动进程命令

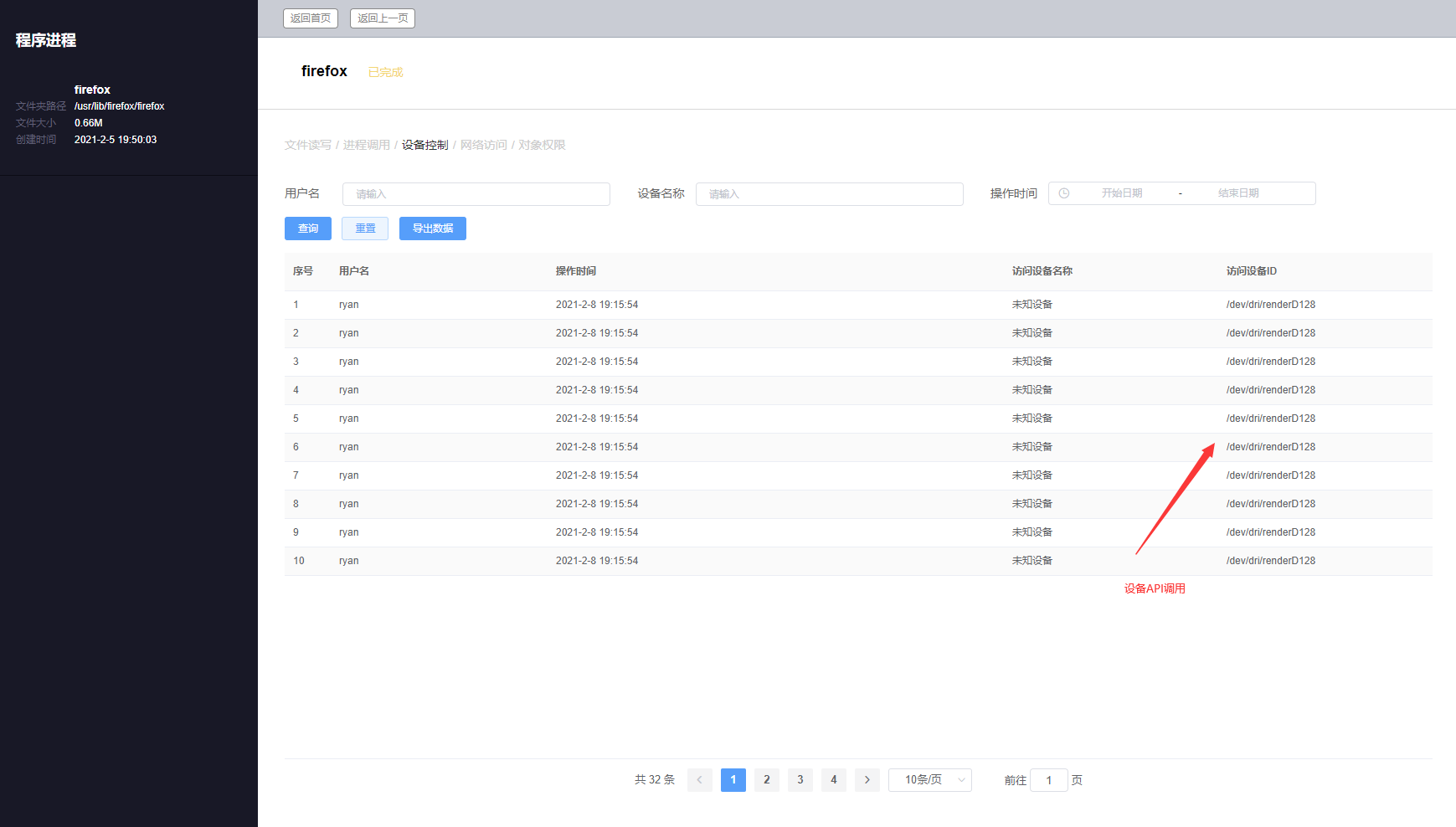
进程间内存共享： 界面会显示对应的共享进程命令行

设备控制

1.进入监控详情，切换到设备控制监听栏目

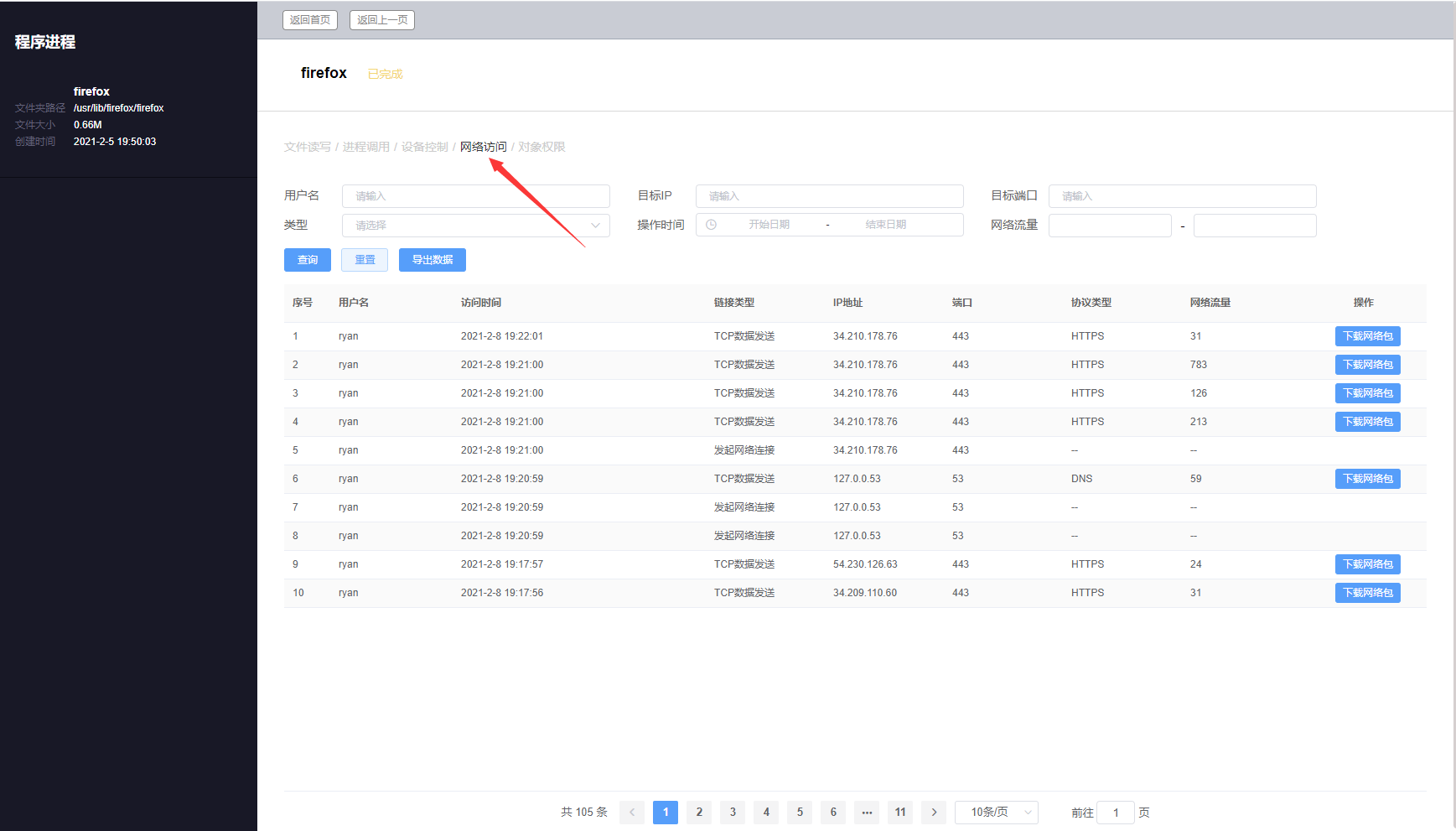


2.设备控制会监控软件所有的设备相关调用行为，注意设备除了摄像头，打印机等物理设备外，还监控记录了软件的虚拟设备行为，包括设备搜索、设备相关API调用、设备管道调用等。

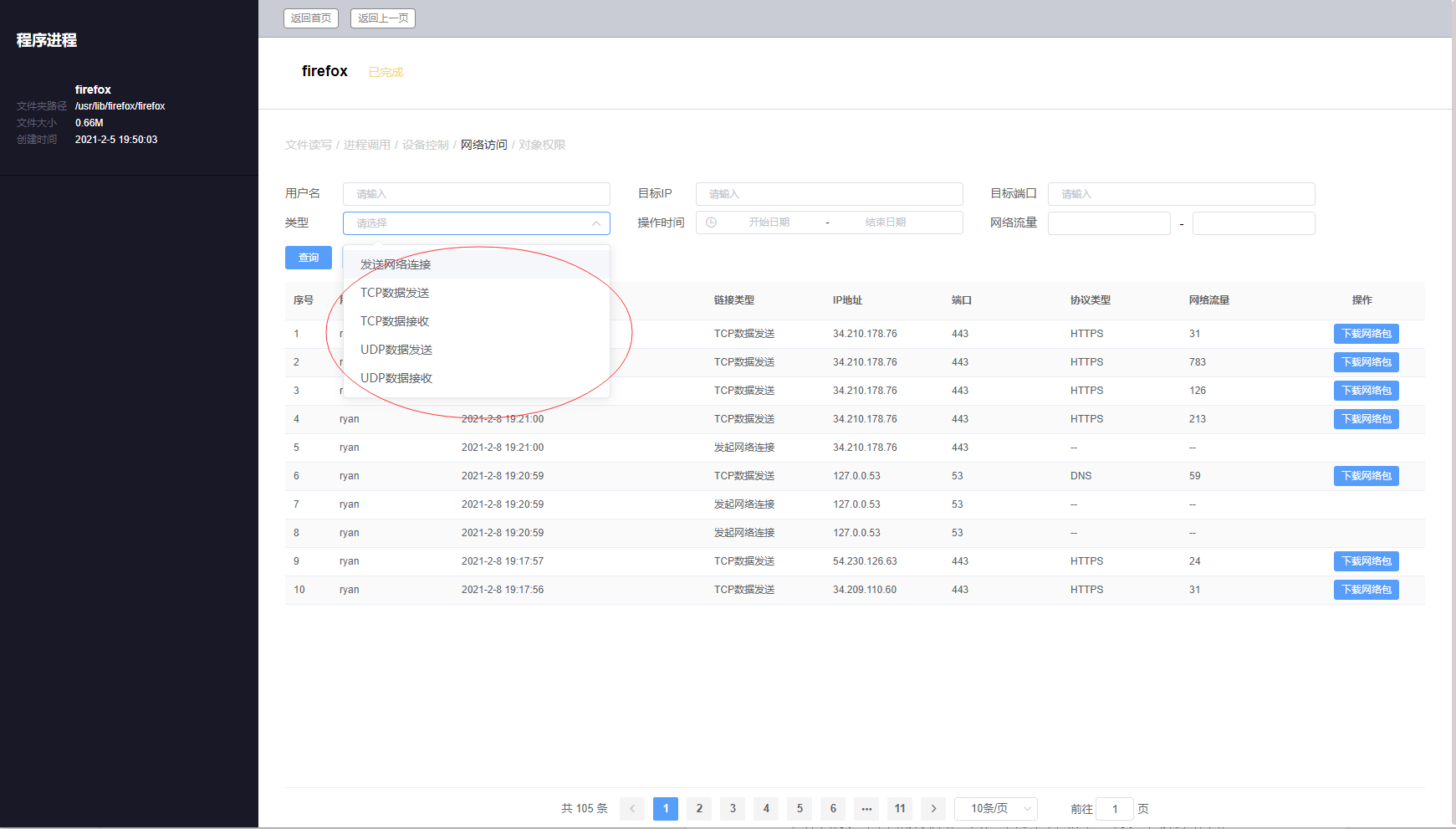


网络访问监听

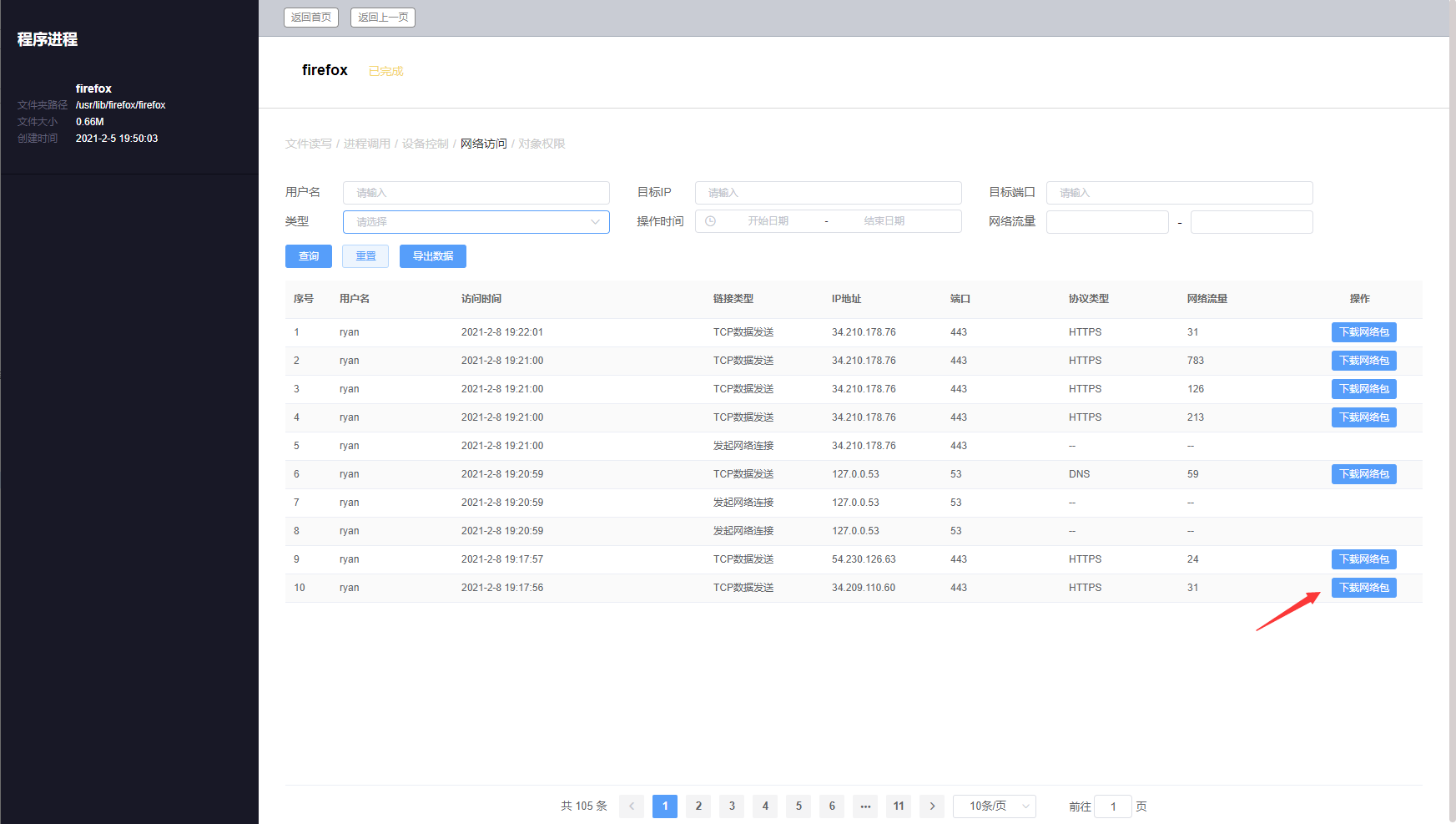
1.进入监控详情，切换到网络访问监听栏目



2. 软件监听了5大类型的网络访问，包括发起网络链接、TCP数据发送、TCP数据接收、UDP数据发送、UDP数据接收

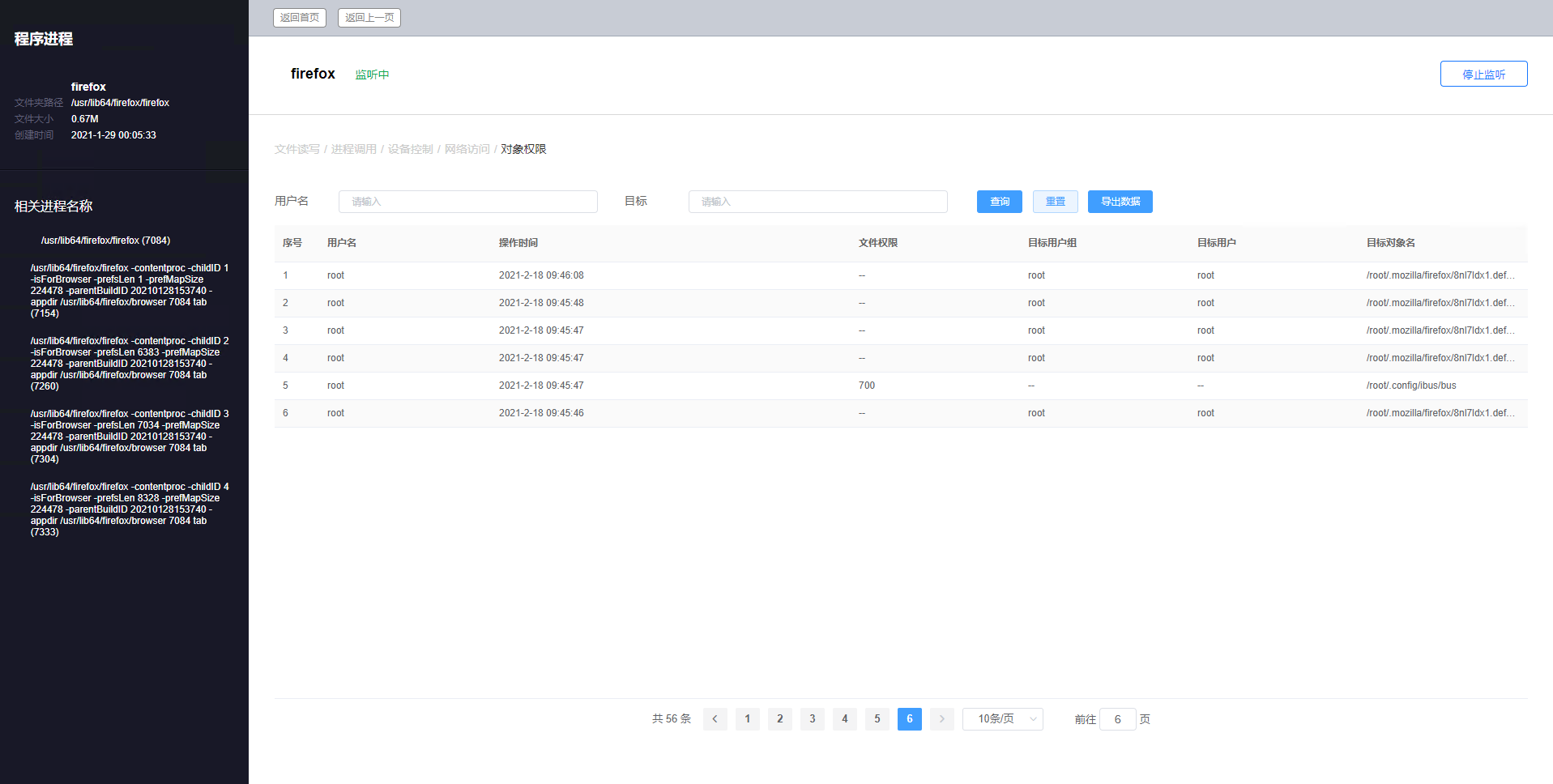


3. 针对网络发送和网络接收操作，用户可以点击下载对应的发送和接收的网络包。



文件对象权限监听

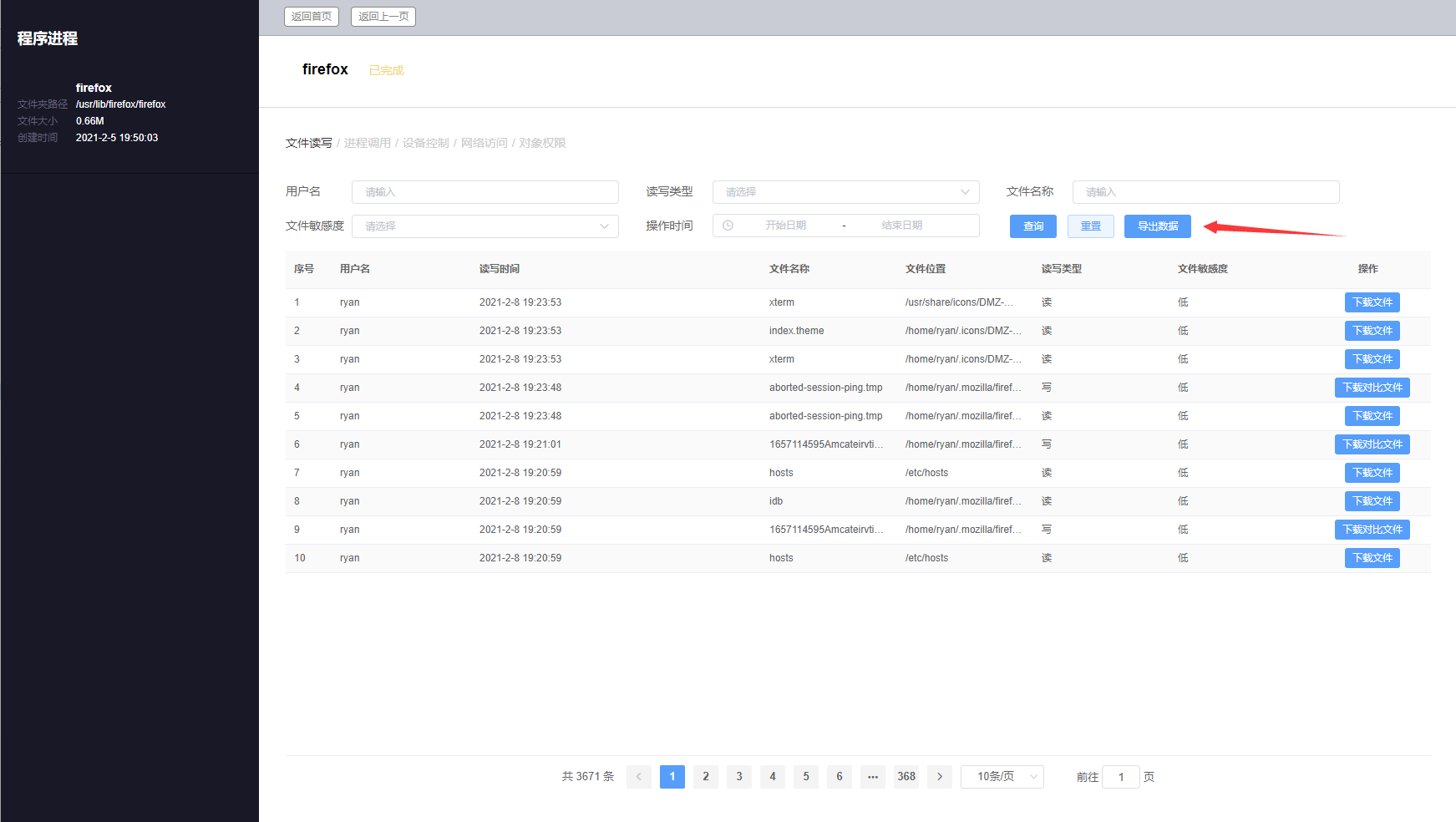
1.进入监控详情，切换到文件对象权限监听栏目

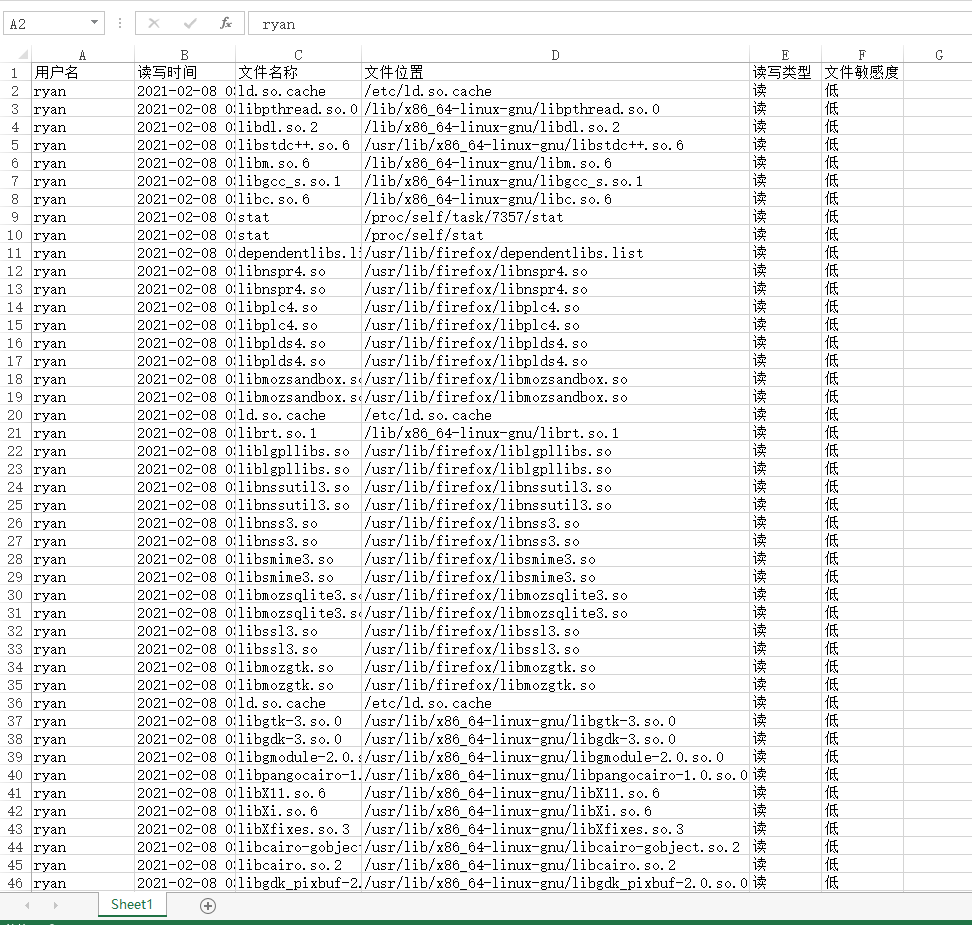


2. 文件对象权限监听主要是监听软件调用了Linux下的文件所属用户变更(chown)和文件权限变更(chmod)等相关api。

### 软件行为结果导出测试

监控模块支持根据软件监控行为的结果进行文件导出，支持xlsx格式文件导出。

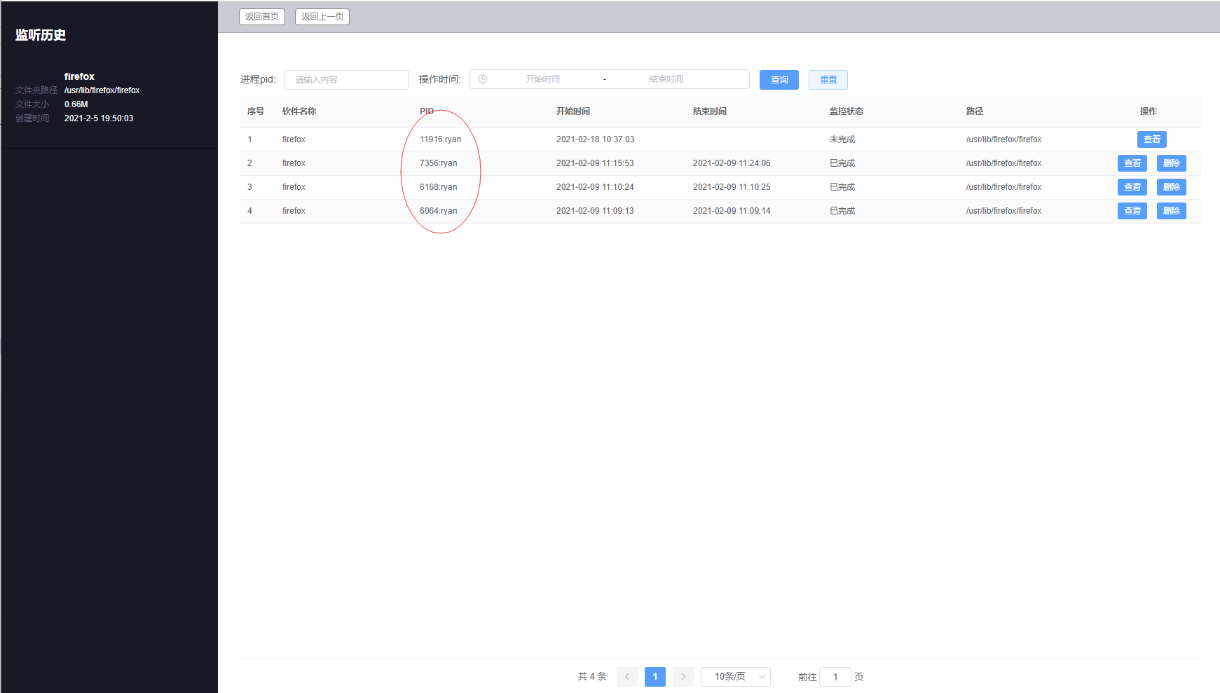


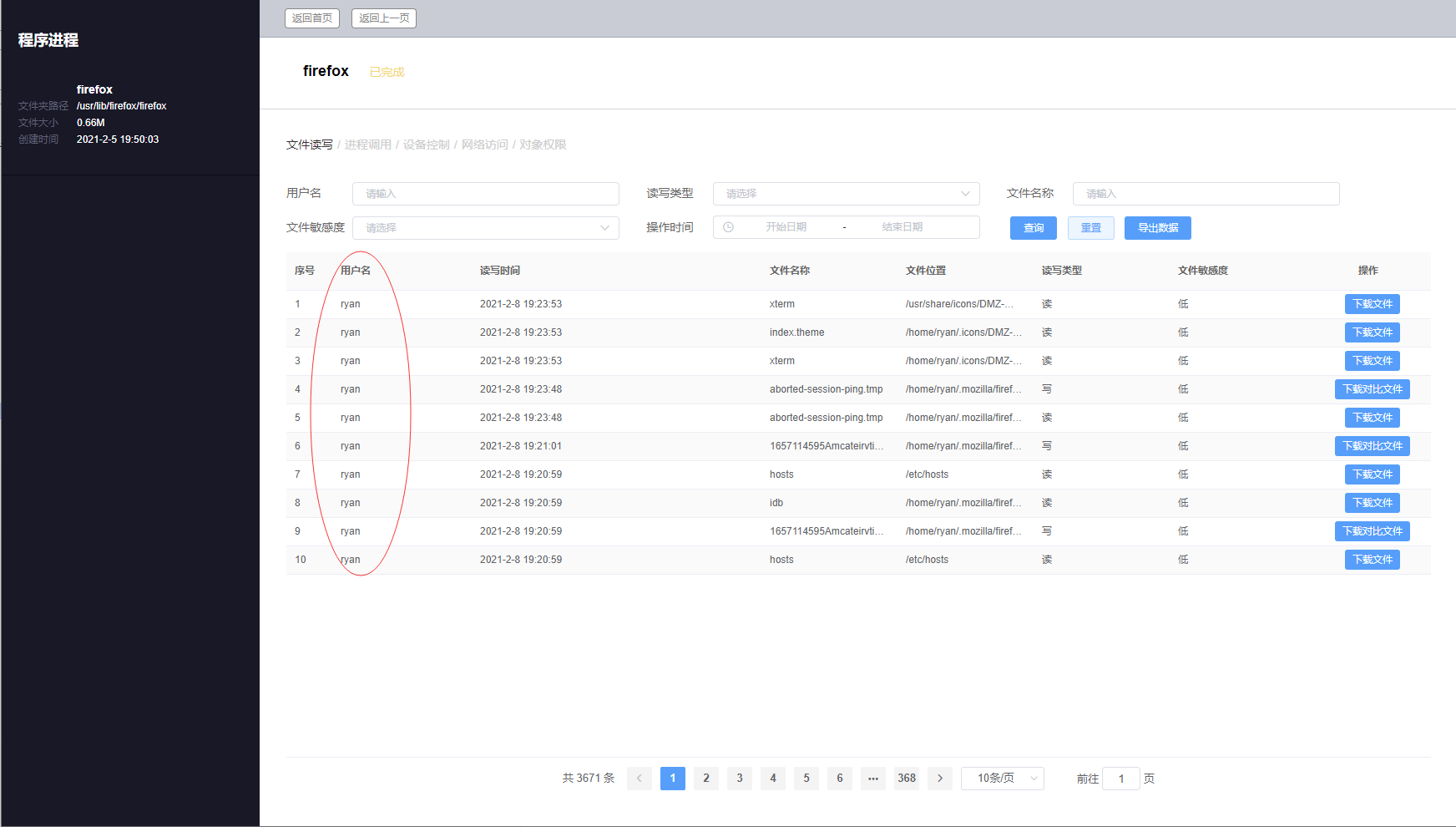


### 软件行为用户身份记录测试

监控模块支持记录进程的启动系统用户和行为的操作系统用户。

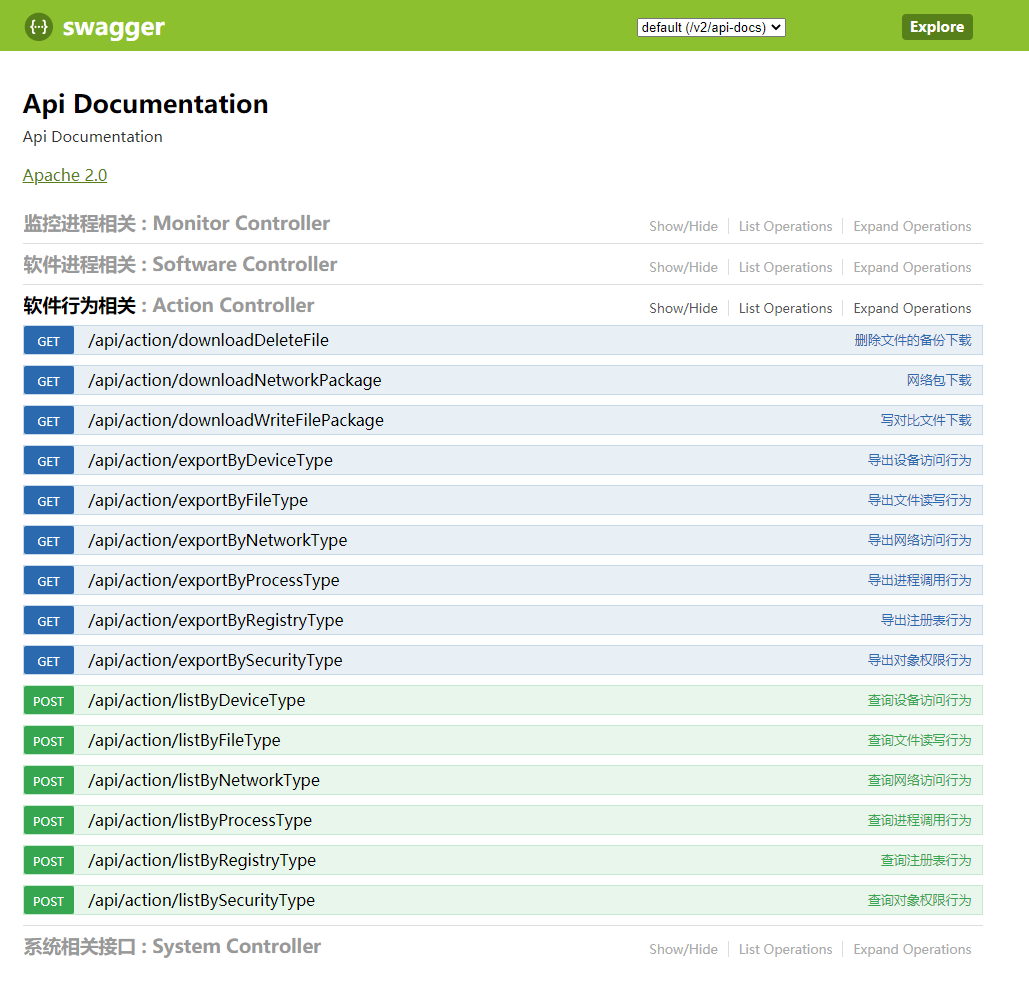
从监控历史记录的列表中可以查看每次启动的用户，进入行为详情也可以查询行为的操作用户。



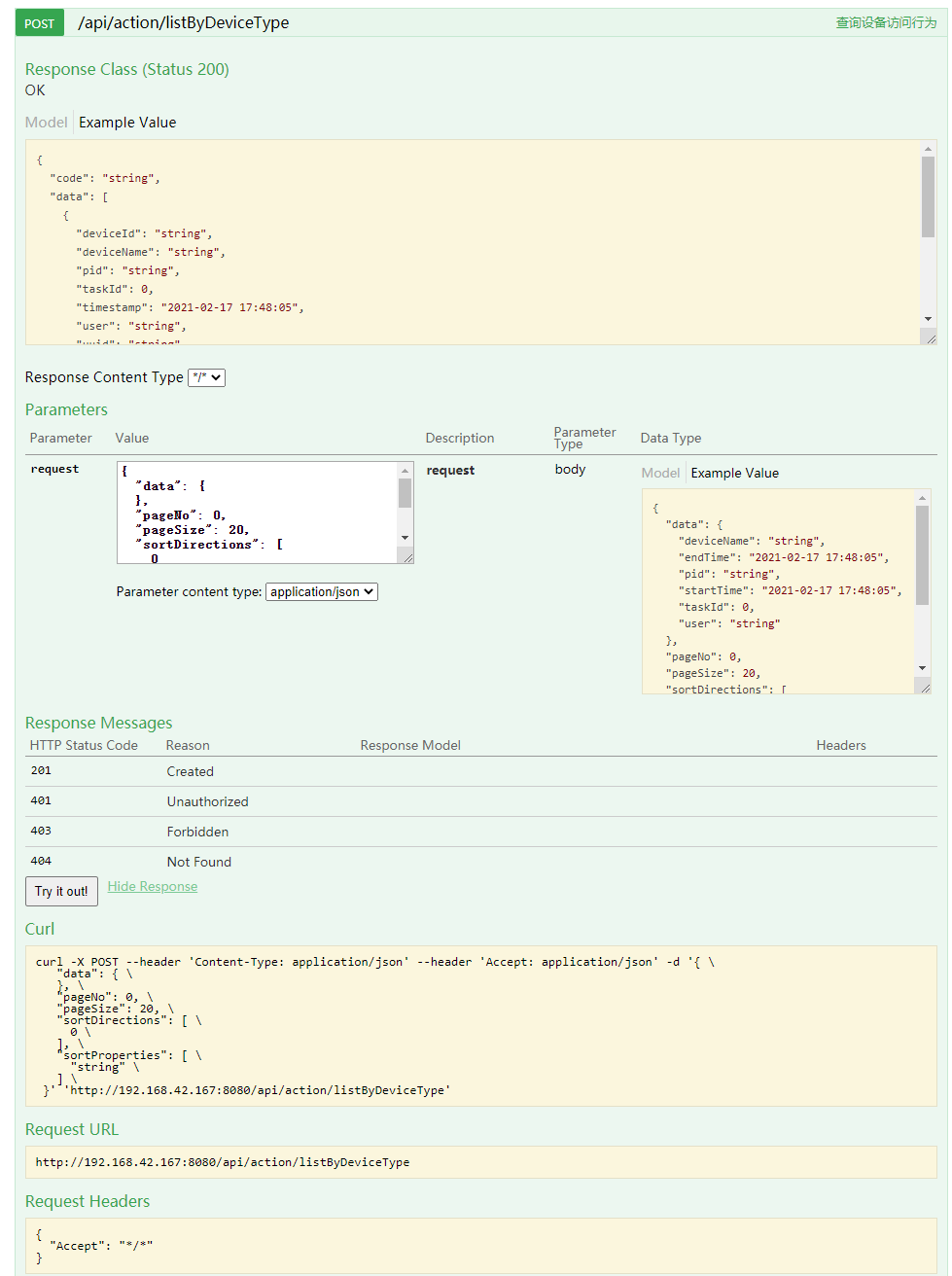


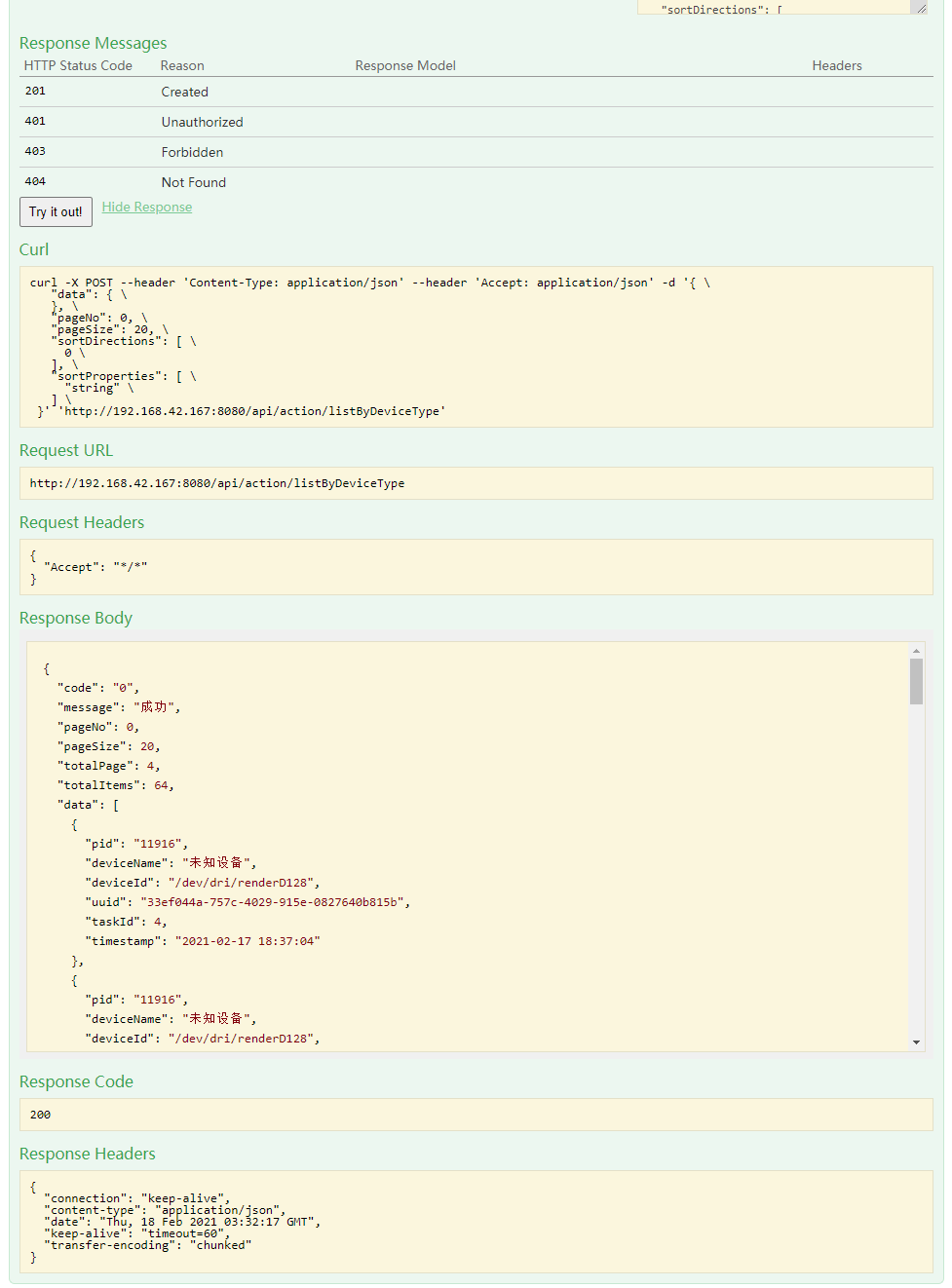
### 软件行为对外数据接口测试

监控模块提供对外接口测试模块，可以通过访问<http://127.0.0.1:8080/swagger-ui.html> 启动接口测试界面。



测试界面支持输入接口参数进行接口模拟调用测试并返回结果





# 验收结论

经过项目组的测试评估，一致认为“针对Linux平台的工业软件运行行为监控模块”验收通过。

项目组成员签字：

部门领导签字：