**基于IPv6的网络服务质量监控及多权限消息预警系统**

**用**

**户**

**手**

**册**

基于IPv6的网络服务质量监控及多权限消息预警系统

## 1.1系统介绍

21世纪，信息技术飞速发展，基于Internet的网络应用已经遍布社会发展的各个领域，在人们欣然享受互联网带来的便利的同时，网络的信息安全问题也日益突出。

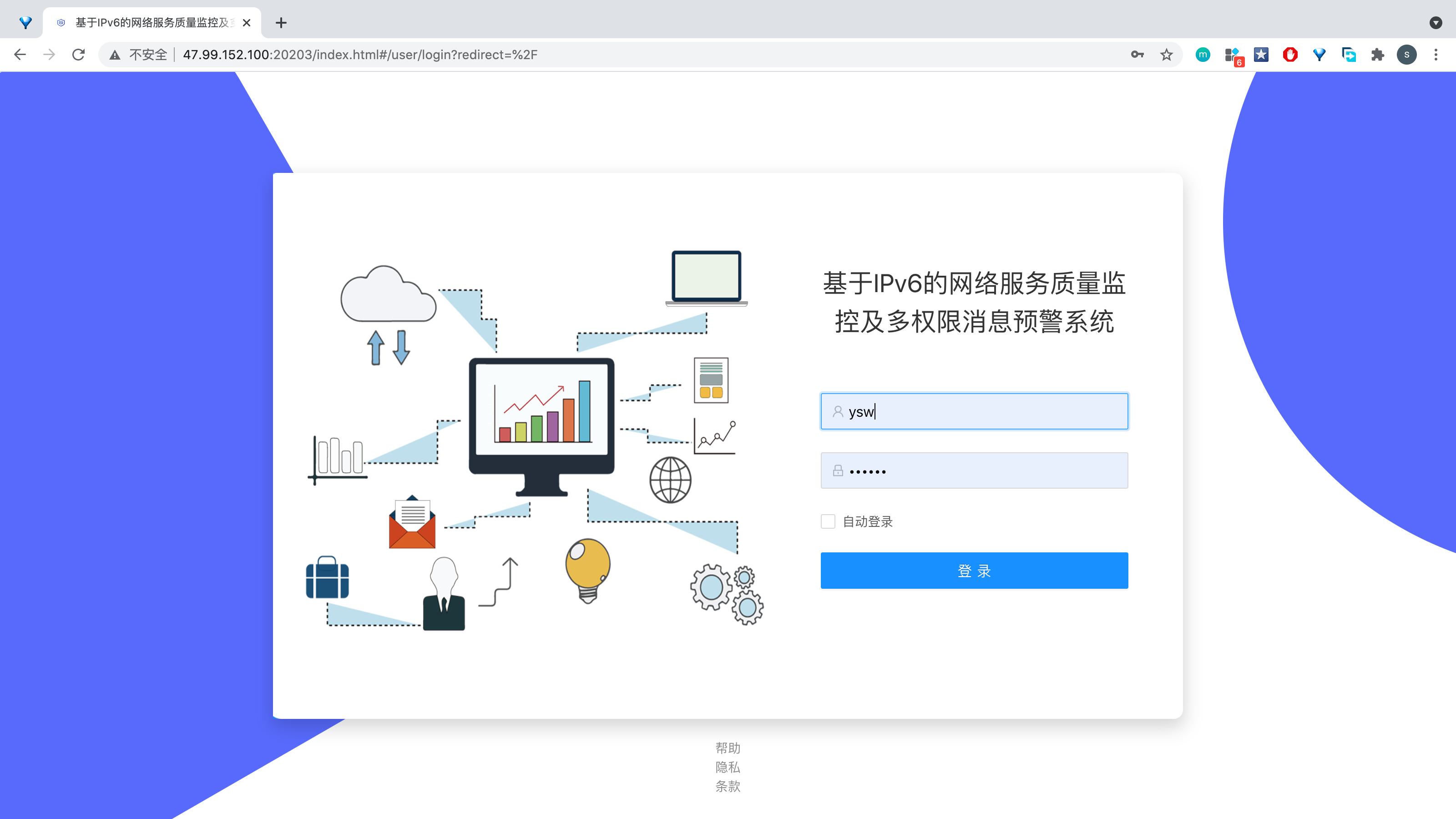
目前，互联网Web应用面临的主要威胁有XSS（跨站脚本攻击）、SQL注入、CSRF（跨站请求伪造）、传输劫持、账密泄露、暴力破解和身份token被窃取等，当企业由于网站漏洞、维护问题面临这些威胁时，将很可能面临客户数据丢失、业务中断的影响，企业的经济和声誉都会因此受到损失。

如今，面对这些威胁，市场上出现了一些网络安全态势感知平台，这些平台，在大规模环境中，对能够引起网络态势发生变化的所有安全要素进行获取、理解、显示以及预测未来的发展趋势，并将信息实时反馈给监控者，监控者通过使用其他平台更改防火墙或路由器的命令对恶意数据包进行拦截，从而保证网络的安全性。但由于监控者监控网络使用的态势感知平台和更改防火墙或路由器命令的平台往往由不同公司搭建，大大降低了监管者的网络安全监管效率。为提升监管效率，本网络安全联动防御系统将为监管者提供态势感知和防范管理的一体化平台，平台为监管者提供实时网络态势的同时，可针对恶意攻击联动路由器或防火墙等网络安全设备进行拦截，并保存相应日志供监管者查看，满足监管者全方位，全天候的控管需求。监管者可事先保存好针对不同品牌安全设备的命令，并勾选相应的格式，平台在观测到恶意攻击时，直接调用对应命令联动安全设备进行防护。本系统有很强的实时性和可扩展性，提升了监管者的监管效率。

## 1.2系统功能描述

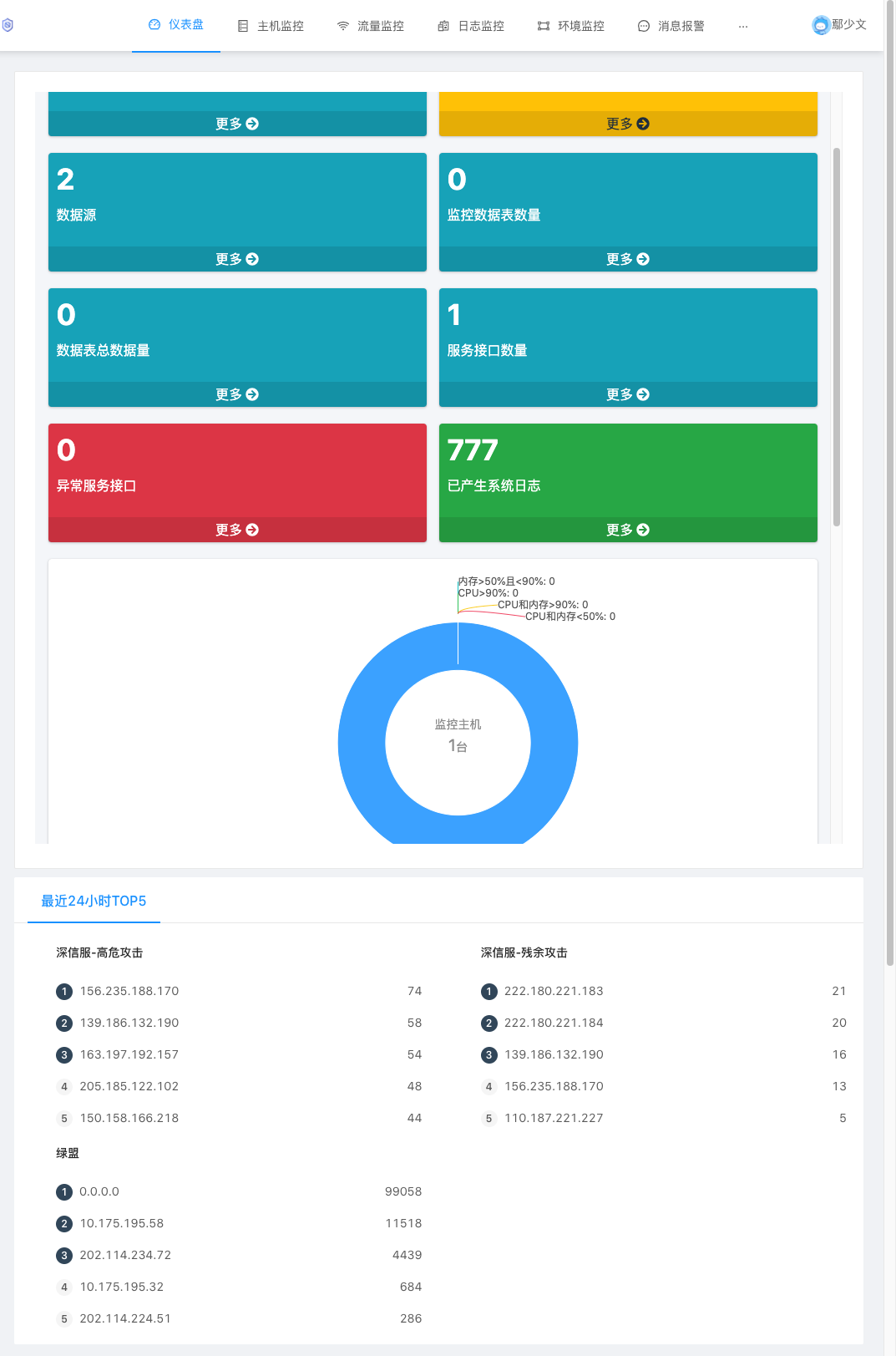
1. 管理员登录

系统管理员可以通过事先配置好的用户名和密码进行登录，密码的储存和网络传输过程中均已加密。



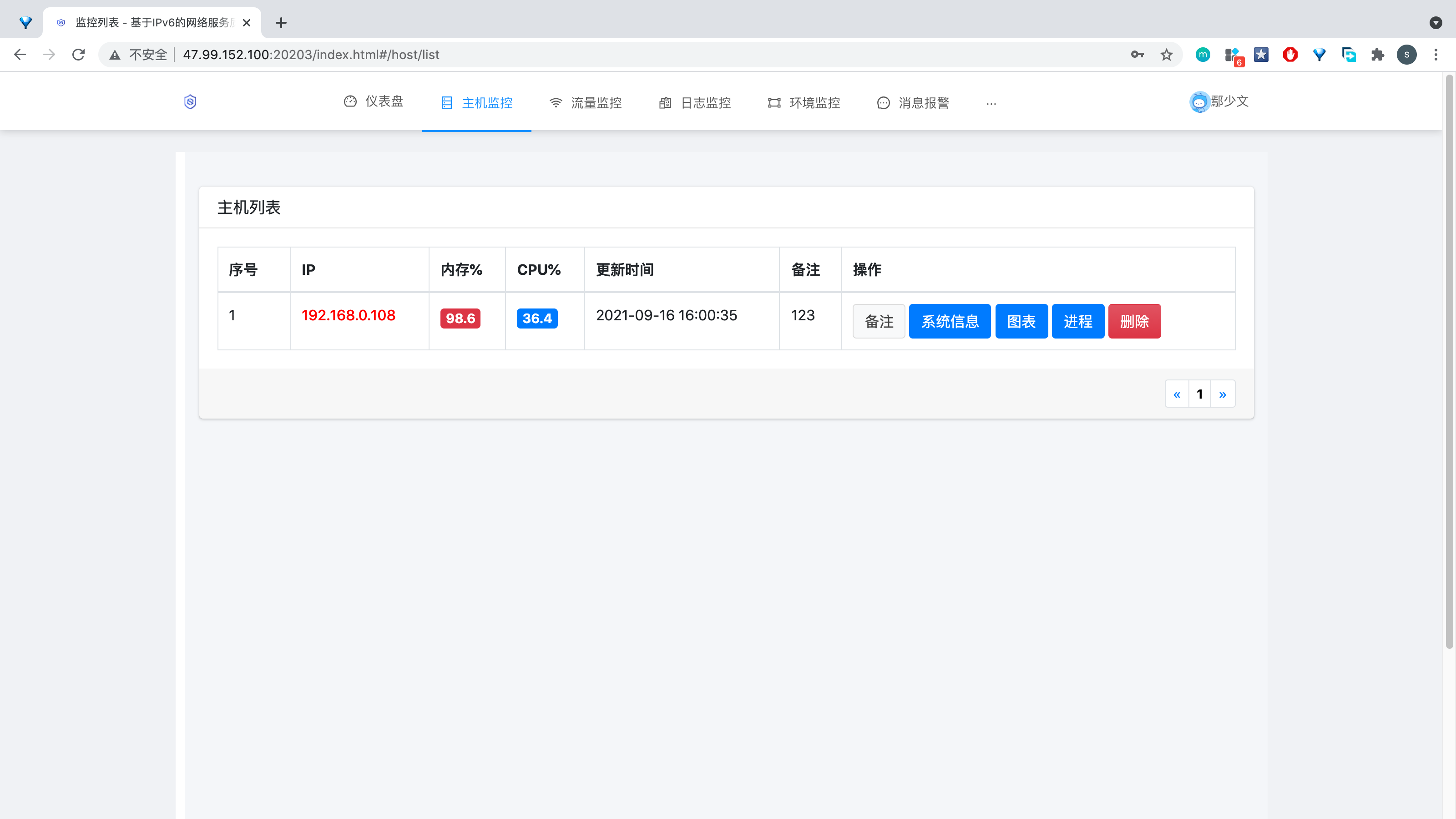
1. 实时同步各监控主机的概览信息以及主流安全态势感知平台的信息

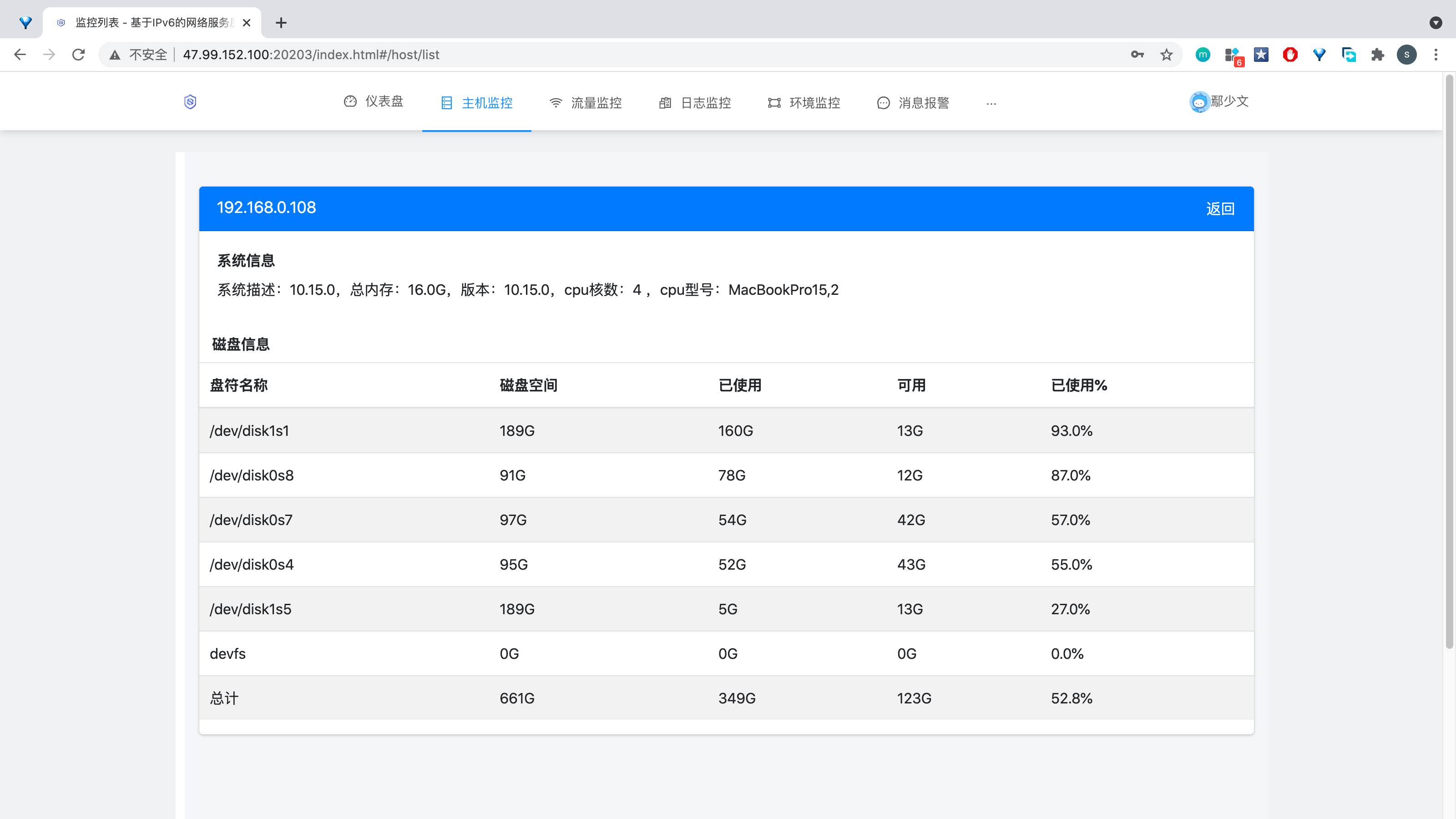
本系统的数据源端具有很强的兼容性，可对多个主流安全态势感知平台的数据信息进行同步，获取平台中各类攻击列表的外部IP参数，将恶意IP的Top5显示在主页上。

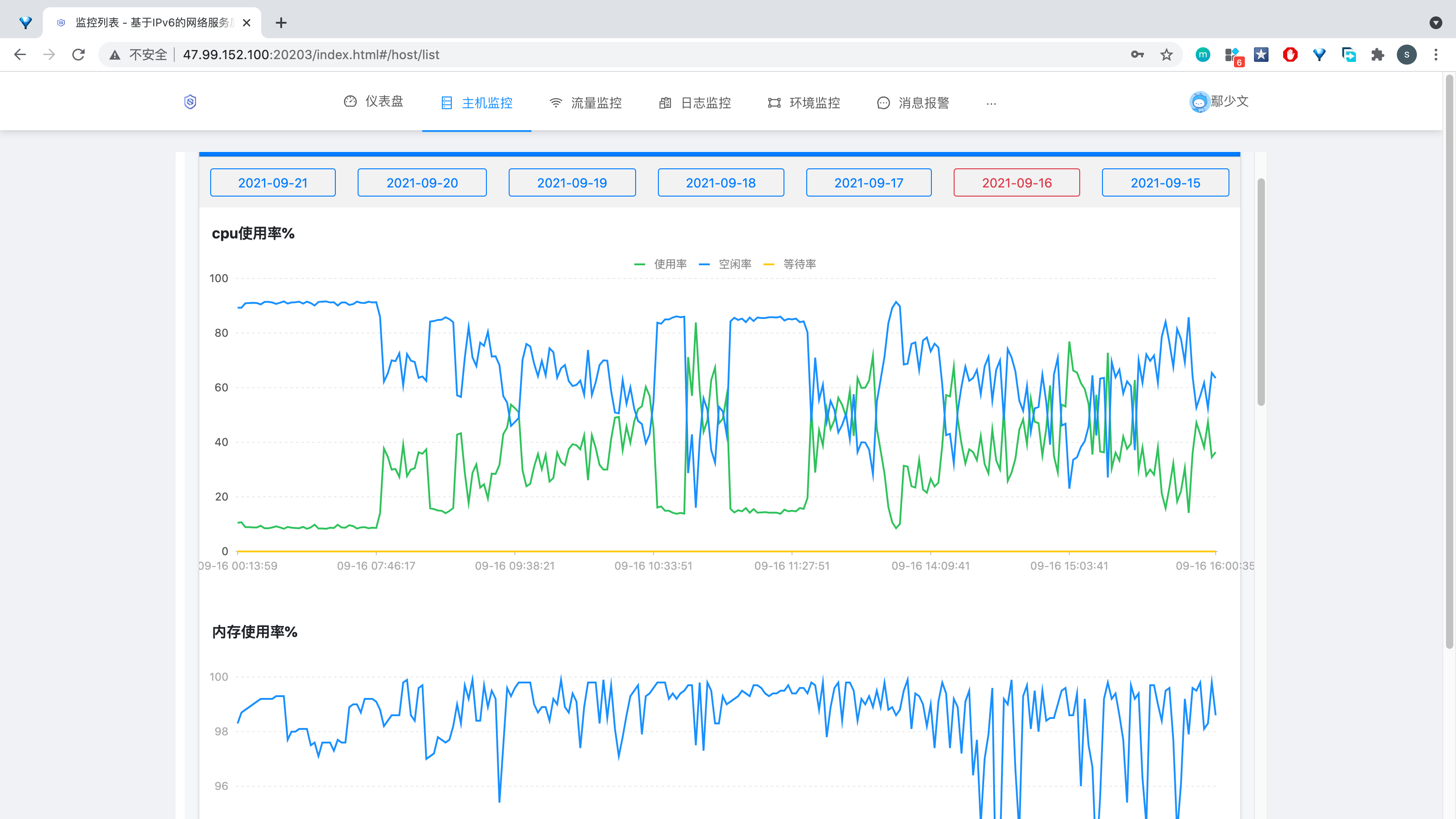




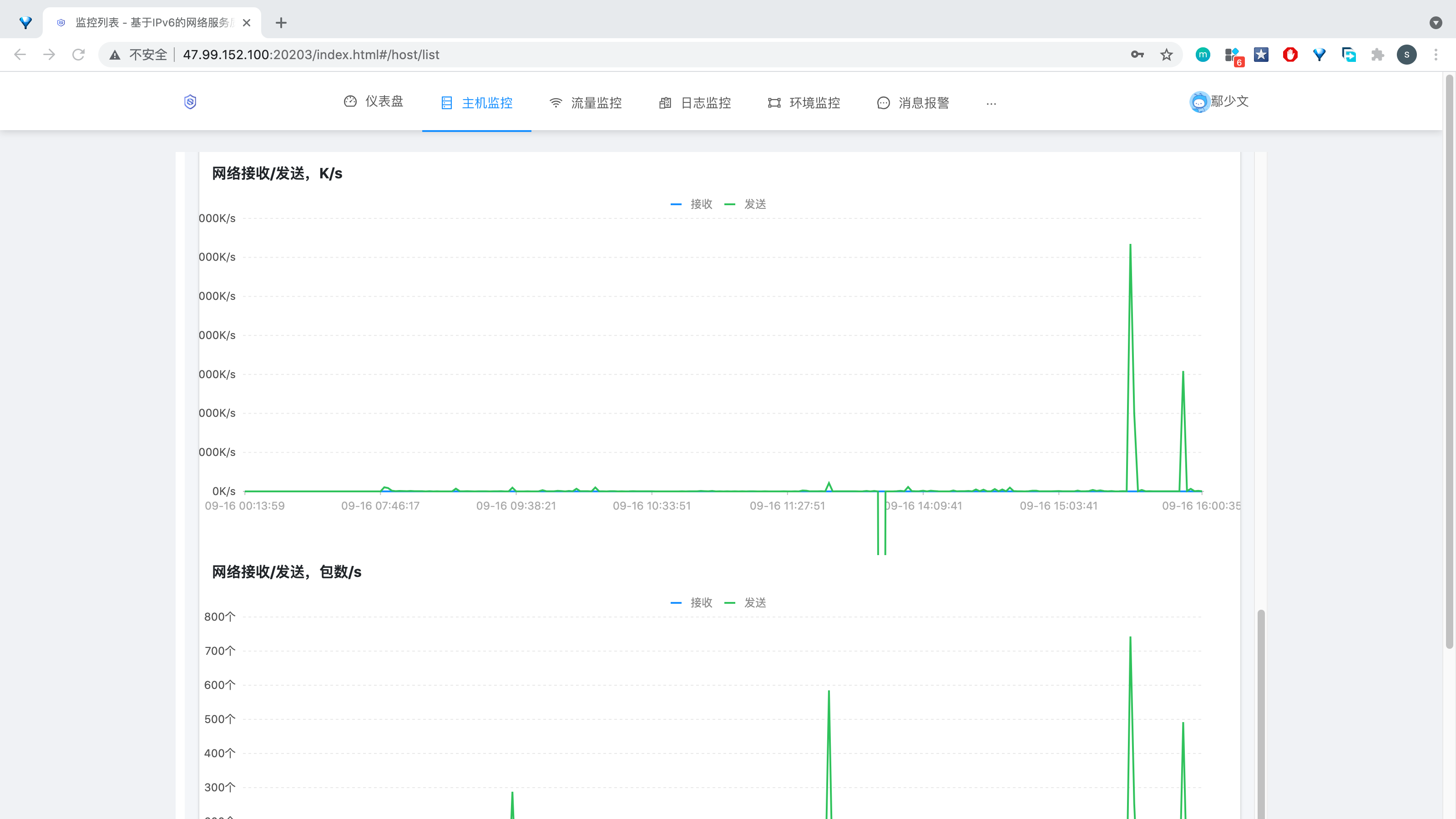
1. 管理监控的主机并查看各主机的磁盘空间，CPU，内存信息，网络流量，系统负载





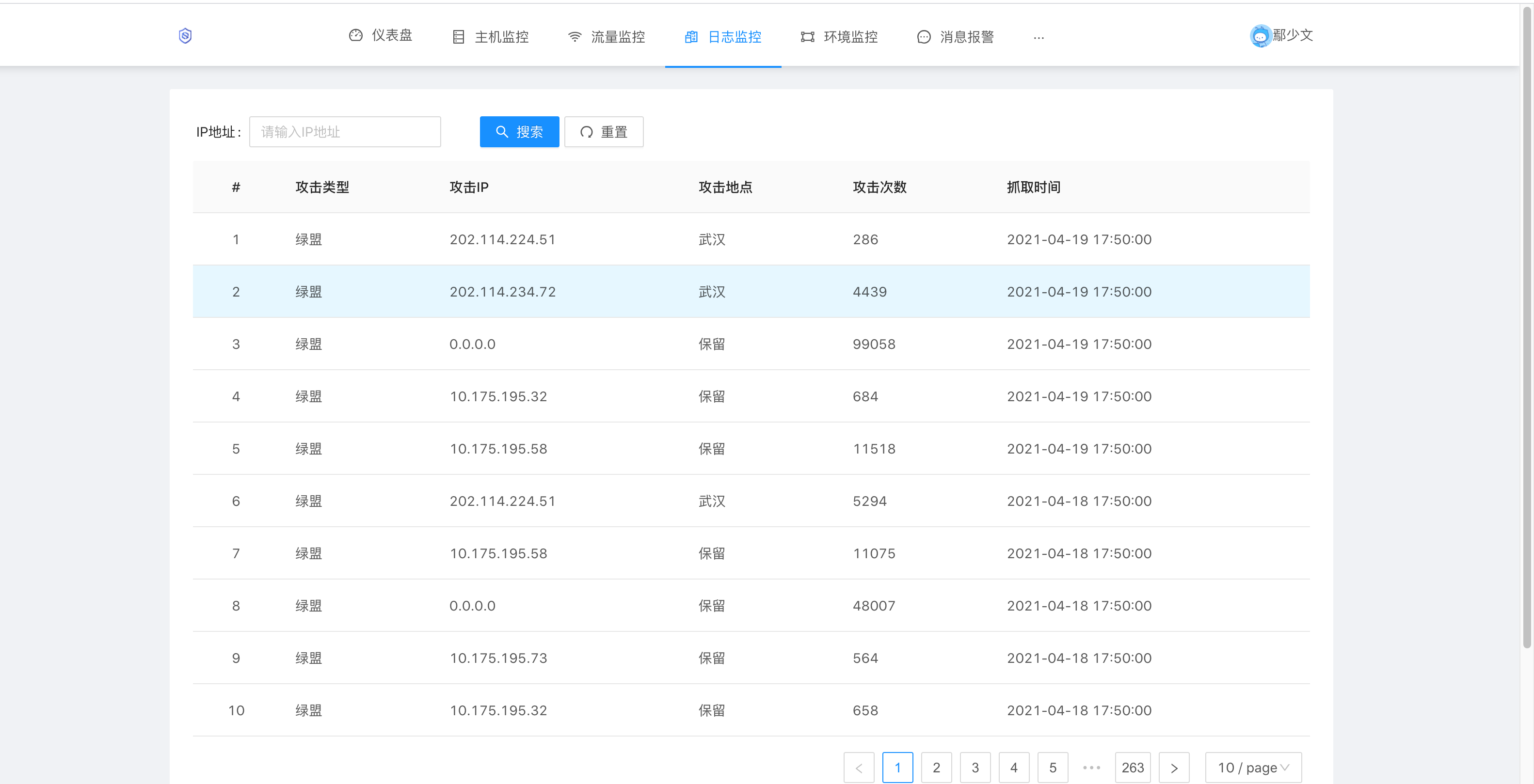


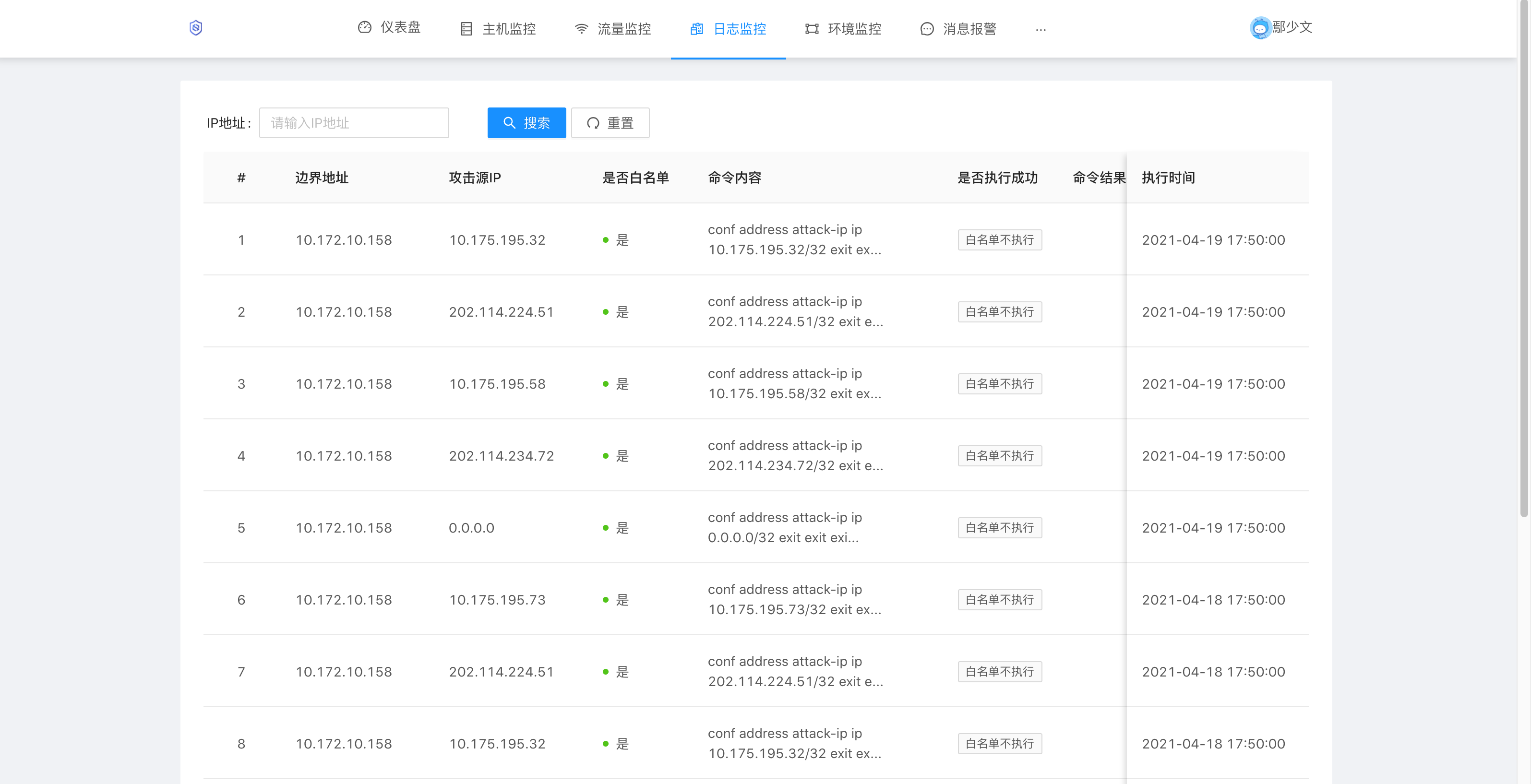


****

1. 支持系统日志和防御日志功能

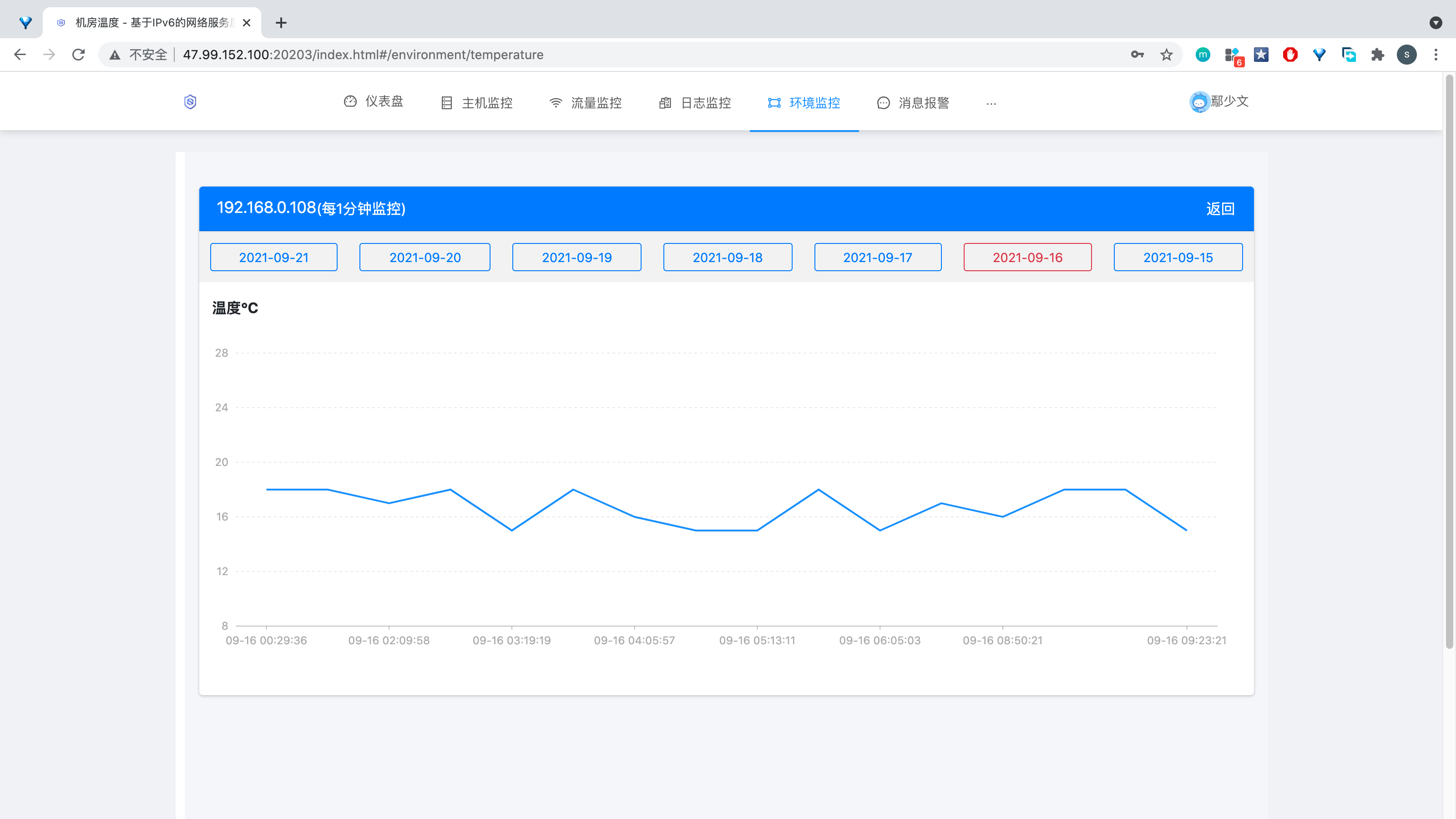
本系统可将系统运行记录、用户操作记录等生成日志，供用户查看，增强系统的可维护性，当系统报错或出现警告时，用户可通过查看系统日志快速查找原因并进行恢复。本系统还支持上万条防御日志记录功能，用户可从时间、类型等多角度搜索防御日志，查看系统防御记录。

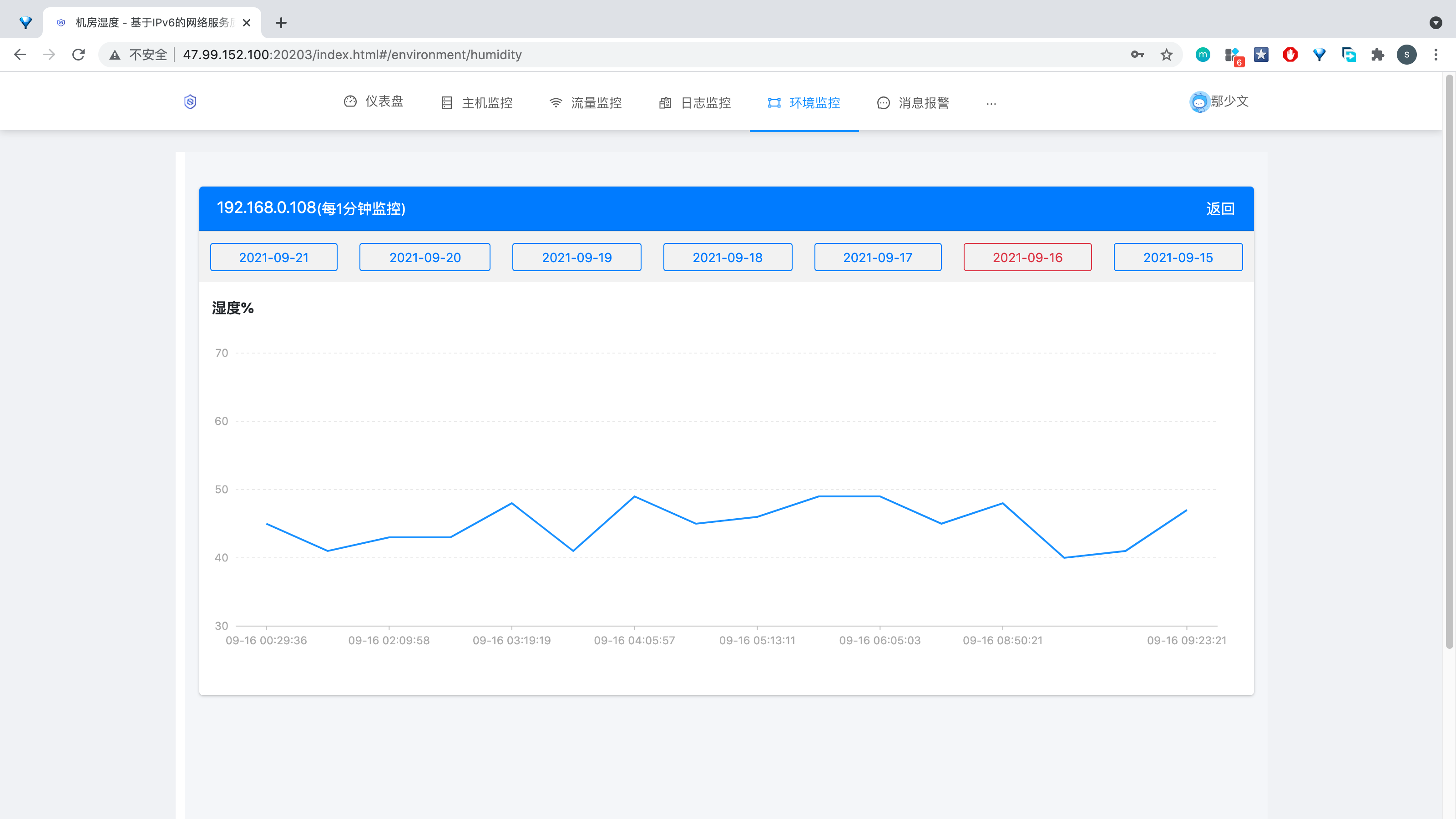




1. 机房温湿度监控

监控主机所在机房的温度和湿度。



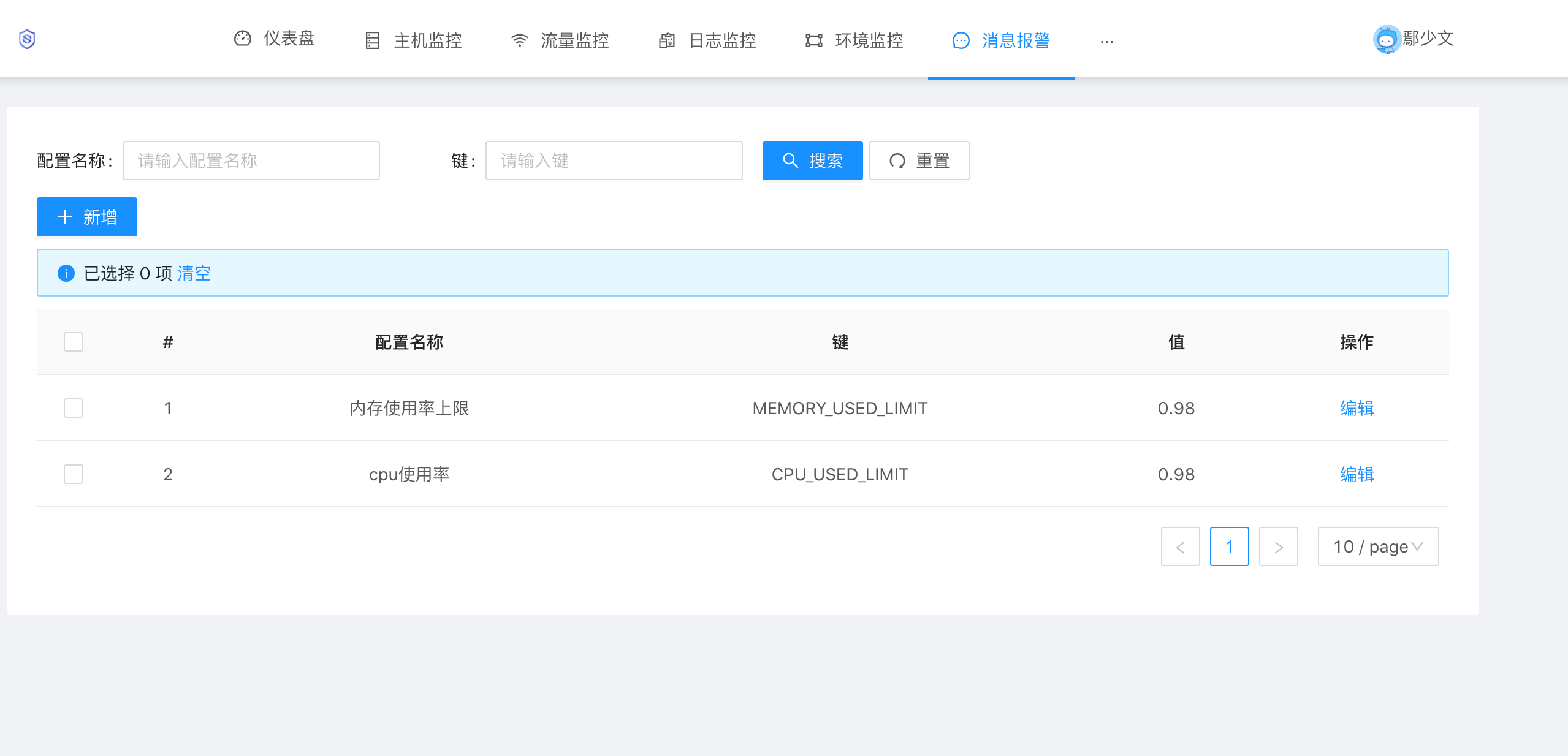


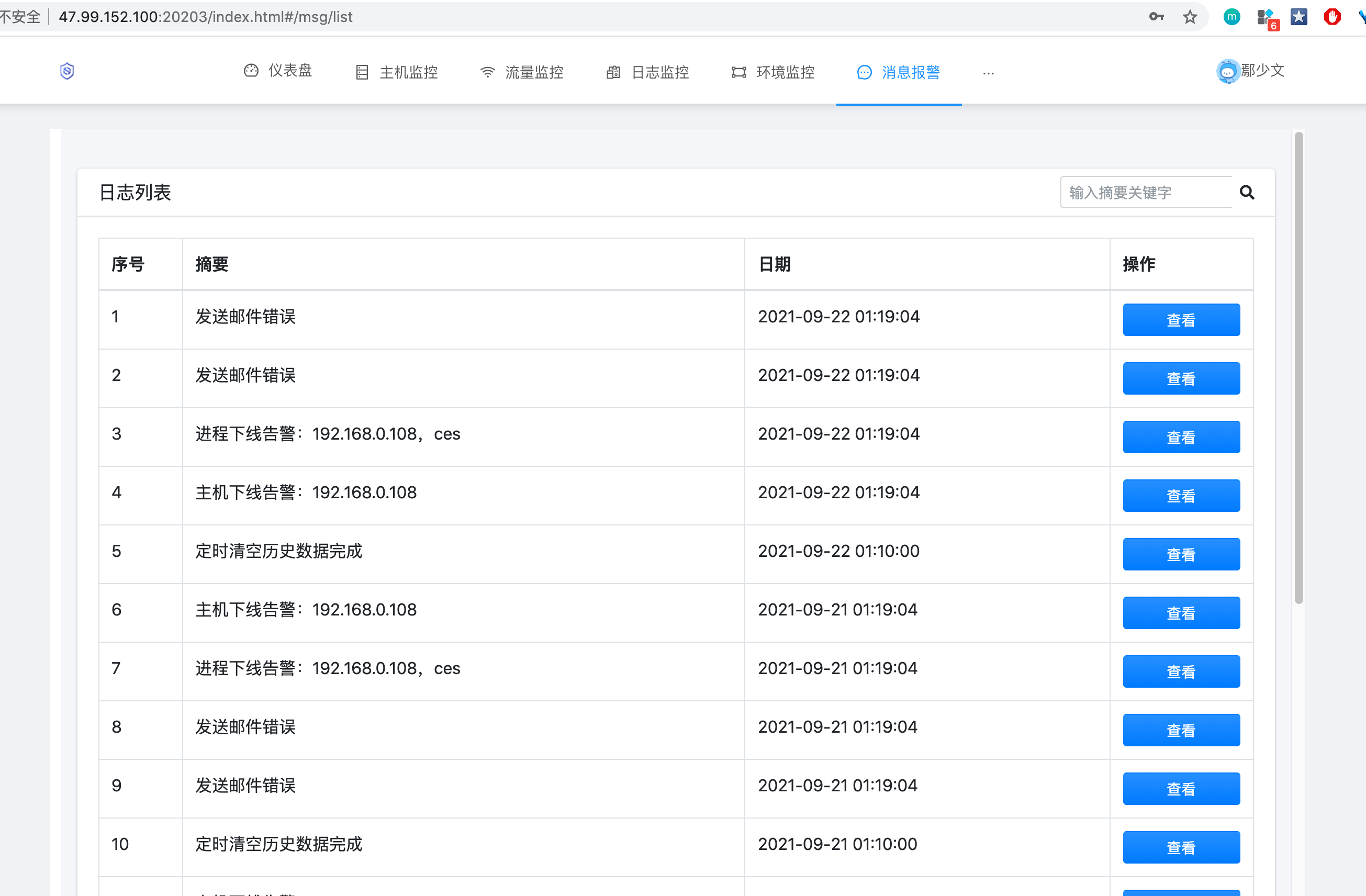
1. 针对主机的CPU，内存使用率，上下线进行报警提示

支持采用邮件和短信对指定管理人员发送报警提醒，且能够配置主机的CPU，内存使用率报警上限，同时能够回溯每一次的报警记录及报警原因。



****

****

****

1. 管理能够登录系统的人员以及这些人员对应的角色

****

1. 联动主流防火墙、网闸、路由器等安全网关设备对目标进行防御

本系统兼容主流防火墙、网闸、路由器等安全网关设备，用户可对不同安全网关设备设置命令并保存，当需要系统监测到恶意IP，需要对其进行拦截时，便调用事先写好的命令联动相应安全网关设备，进行防御。



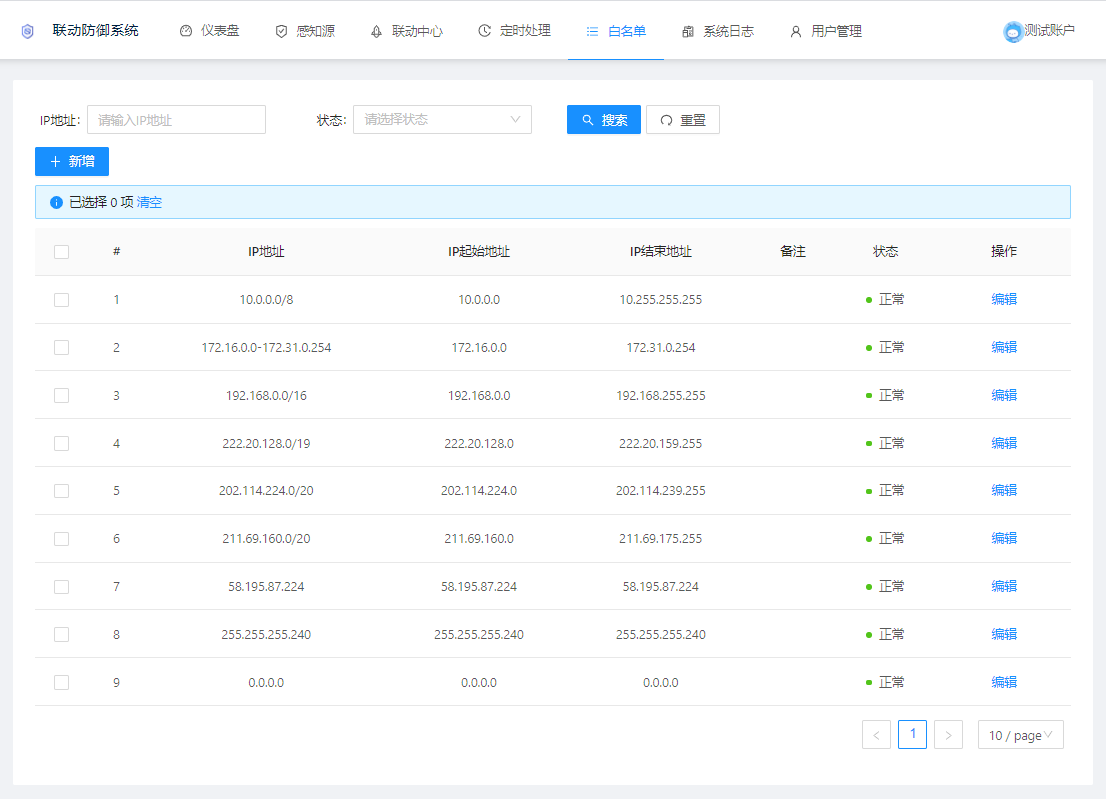
1. 用户自定义溯源时间和执行时间功能

本系统支持任意时段定时溯源和定时执行功能，用户可自定义系统溯源和执行联动操作的时间段，从而将更多的时间和精力投入到其他的工作中，提高用户工作效率，增加时间和操作的灵活性。



1. 支持白名单功能

用户在使用本系统时，可设置白名单规则，系统在执行网络联动防御功能时，生成内部白名单数据库，当位于白名单中的IP地址再次请求所监控的网站时，系统会允许其优先通过，大大提高了系统的安全性和快捷性。



1. 系统旁路运作。
2. 兼容性强。目前安全策略执行侧支持主流防火墙、路由器等高端网关型设备。

## 1.3系统优势

目前，市场上的网络安全产品可分为六大类别，四大场景。六大类别是指：网络安全、终端安全、应用安全、数据安全、身份与访问管理及安全管理。四大场景包括云安全、大数据安全、物联网安全和移动安全。从大数据场景来看，人们通过搭建态势感知平台对网络环境中能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，并根据结果进行决策，利用路由器、防火墙等网络安全设备有选择地抵御恶意攻击。这种方式虽然减少了一部分人力，但由于态势感知平台和网络安全设备通常不是同一个厂家，在决策阶段往往还需要人工操作，运行效率没有达到最优，实时性也相对不足。基于此类网络维护方式的不足，我们提出了网络联动防御系统这一“中间人”的设计，弥补该方式的不足，提高生产效率。本系统主要有以下几点优势：

1. 联通性

本系统为态势感知平台和安全设备之间搭起了一座桥梁，监管者在进行网络维护时不再需要“两边跑”，在一个平台即可完成网络维护。

1. 兼容性

本系统提供针对防火墙、路由器等不同类型、不同厂家的网络安全设备进行自定义命令设置，监管者可自行选择安全设备进行维护。

1. 实时性

传统的网络维护方式需要人工耗费大量的时间和精力对态势感知平台的数据进行分析决策，运行效率不高，实时性不强，经常会导致由于没能及时处理恶意攻击，导致网络安全遭到威胁的情况发生。本系统为监管者提供提前保存防护命令的服务，系统在同步态势感知平台数据时，便可及时针对top5威胁进行处理，大大提高了网络维护的效力与实时性。

1. 可扩展性

目前本系统已经实现了对绿盟和深信服两家态势感知平台的数据进行实时同步，未来，我们可以与更多主流平台的数据进行同步，为用户提供更多选择。

1. 便捷性

本系统支持白名单功能，当位于白名单中的IP地址再次请求所监控的网站时，系统会允许其优先通过，减少二次监测， 更加方便快捷。

1. 专业性

网络联动防御系统专家团队具有多年的安全服务经验，可为用户提供更专业的数据分析和命令提示，帮助用户及时、准确地完成网络安全的维护。