公开阅读

华顺信安
HuaShun XinAn

网络资产测绘及分析分析系统
FOSEE-V1.0
用户使用手册

FOSEE/田鹏

版本号：V1.0

流通范围	**完全公开（仅供北京华顺信安科技有限公司相关人员对外开展业务合作使用）**
	限制公开（仅供北京华顺信安科技有限公司内部交流使用，如需对外发布，请联系原作者进行授权）
	内部交流（仅供北京华顺信安科技有限公司内部交流使用，严禁外泄）

北京华顺信安科技有限公司
2023年1月28日

文档更新说明			
系统版本	文档版本	文档更新时间	修改人
V1.0	V1.0	2023-01-28	吴曦

目录

1．简介

随着企业的发展和 IT 信息化建设的快速开展，承载企业业务的资产越来越多，接入互联网的设备也是五花八门，除了个人 PC 机和服务器，还包括交换机、路由器、打印机、视频监控、移动设备、物联网设备、工控设备等等。这些设备有的部署在内网，有的部署在外网，内外网的联网设备共同组成了企业所处的网络空间。网络空间测绘是一个针对政府、企事业单位开发的网络空间资产检索系统，能够自动获取企业存活的资产和开启的服务，然后进行协议识别，根据协议的信息对资产进行产品识别；特有的 PoC 漏洞专扫模块，刻意快速发现资产上存在的安全风险。刻意出具各种可视化资产及漏洞统计报表等信息。

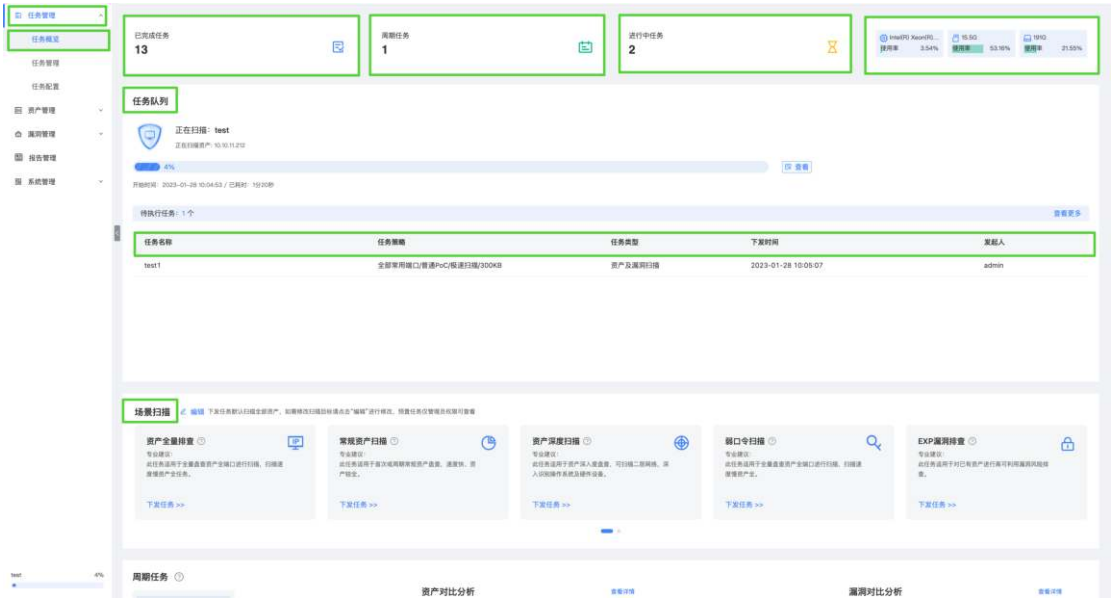
2. 产品功能使用

在《配置手册》中已经介绍了硬件的拆包、部署、IP 配置过程，本文档以产品使用为主介绍使用过程

2.1 任务管理

2.1.1 任务概览

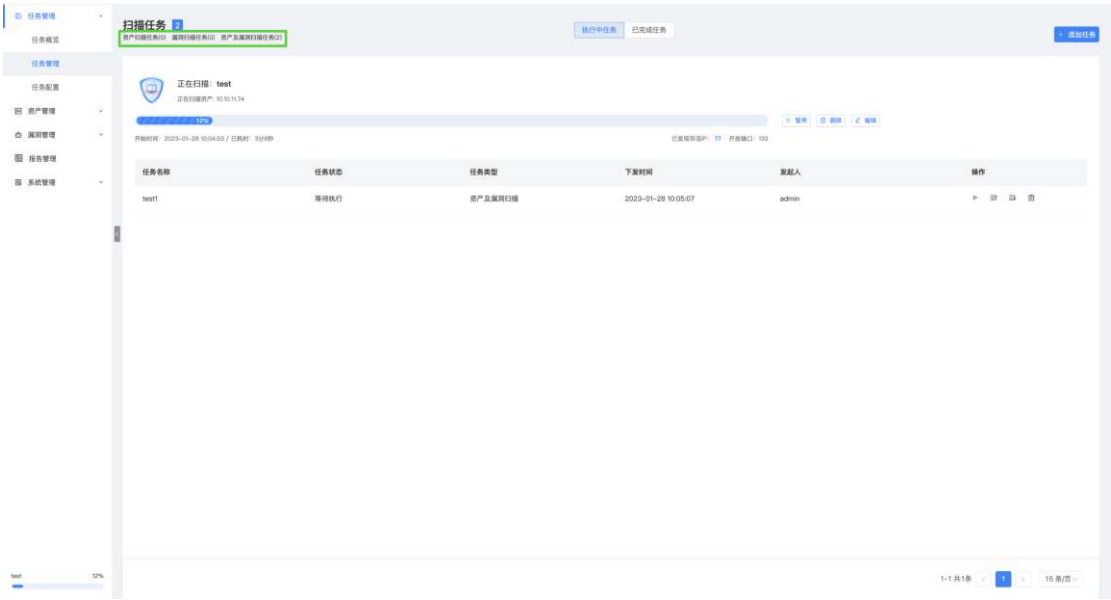
【任务管理】-【任务概览】页展示“已完成任务”、“周期任务”、“进行中的任务”、“CPU、内存、磁盘使用情况”、“任务队列”、“待执行任务”、“场景扫描”、“周期任务”等信息概览。



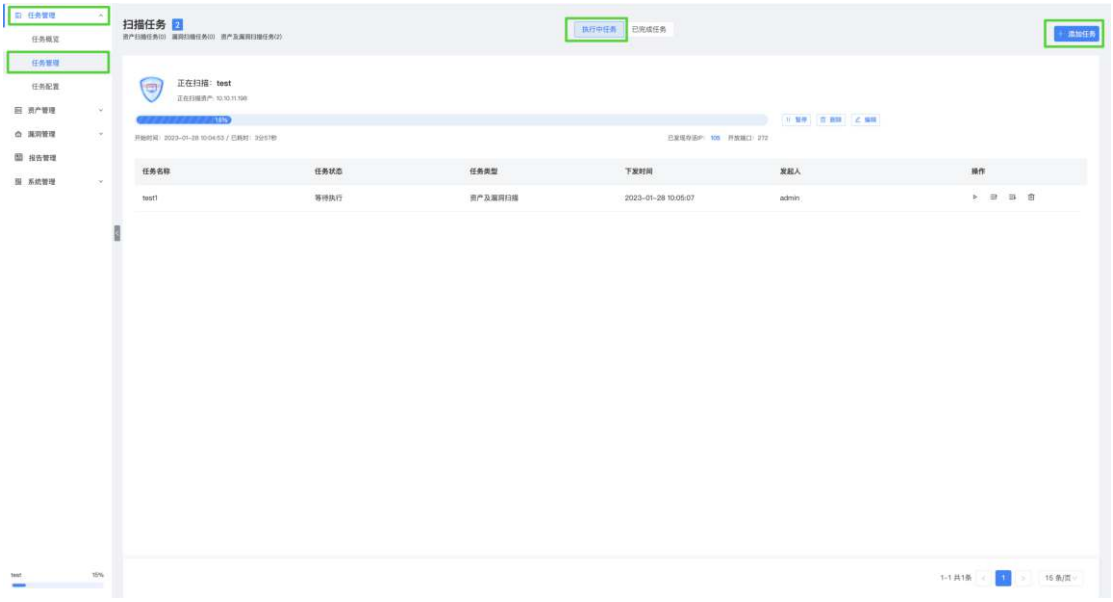
2.1.2 任务管理

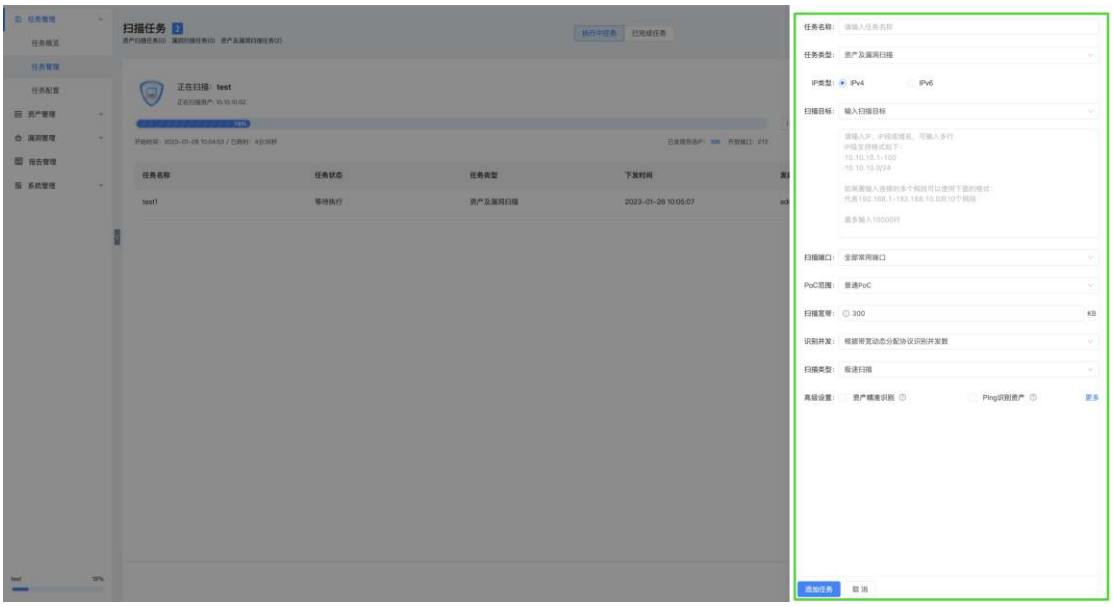
2.1.2.1 执行中任务

1.【任务管理】-【任务管理】页，默认展示“执行中的任务”，标题栏显示执行中的任务数量，具体分为：“资产扫描任务数量”、“漏洞扫描任务数量”、“资产及漏洞扫描任务数量”。



2. 添加任务：【任务管理】-【任务管理】-“执行中的任务”点击“添加任务”按钮，即可新建扫描任务。





a.“任务名称”：为自定义输入设置添加扫描任务名

b.“任务类型”：有资产扫描任务、漏洞扫描任务、资产及漏洞扫描任务，三种任务类型选择，初次使用系统建议选择使用资产及漏洞扫描任务。

c.“IP 类型”：可选择 IPV4、IPV6 两种类型。

d.“扫描目标”：可选择“输入 IP 信息”、“上传 IP 信息文件”、“现有全部 IP”、“根据 IP 段筛选”、“负责人”、“业务系统”、“资产等级”、“机房信息”、“管理单元”以及“自定义标签”等多种选择。

(i)“上传 IP 信息文件”：只能上传 xlsx 文件，且不能超过 1M。

(ii) 格式标准：必须从 A1 单元格开始，最多 10 列数据，超过 10 列的数据不做处理。前 7 列为固定字段，可以为空但必须存在，分别为：IP、备注信息、地理位置、管理单元、业务系统、负责人、机房信息，后 3 列为用户自定义的管理标签，自定义的管理标签的导入条件是用户已经在标签管理中创建了相同名称的标签分类，在导入时如果在标签管理中没有找到相同名称的标签分类，将不做处理。负责人列必须包含姓名、电话和邮箱，缺少信息将不做处理，使用英文逗号隔开，以上内容可在扫描目标选择为“上传 IP 信息文件”后在页面点击“模板下载 ”获取。

IP	备注信息	地理位置	管理单元	业务系统	负责人	机房信息	A标签分类	B标签分类	C标签分类
10.10.10.1-50		河北省,石家庄	石家庄总公司	支付系统	小左，18518325564，18518325564@163.com	石家庄资产中心	A1标签	B1标签	C1标签
10.10.10.51-100		北京市	北京总公司	客服系统	张三，18518325564，1661361970@qq.com	北京资产中心	A2标签	B2标签	C2标签

(iii) “输入 IP 信息” ：如填入了域名，系统将自动解析是 IP 下发扫描。

e. “扫描端口” ：有全部常用端口、知名端口、常用端口 TOP50、数据库端口、企业端口、工控端口、网络精简端口、视频网专用端口组、公安网专用端口组、运维端口、0-65535、现有端口组、全部预置端口组、非标端口组等可选择，初次使用建议选择“全部常用端口”。

f. “PoC 范围” ：有普通 PoC、弱口令、全部 PoC、指定 PoC、ASUTOR 等可选择。

g. “扫描宽带” ：带宽设置高可以提高扫描速度，但是过高可能还会影响到网络正常使用，最大值为 20000，系统默认设置为 300。

h. “识别并发” ：可选择识别并发的数量，建议选择根据带宽动态分配协议识别并发数。

i. “扫描类型” ：支持极速扫描、深度扫描两种类型，极速扫描相对扫描速度更快一些；深度扫描支持二层网络扫描及 IPV6 扫描，扫描资产更全面相对扫描时间更长。

j. “高级设置” ：为多选项，可选择资产精准识别、Ping 识别资产、Treck 协议栈指纹检测、全协议识别、版本号识别、深度识别操作系统及设备、域名解析、开启爬虫可多重沟通选，高级设置只有任务类型为“资产扫描”或“资产及漏洞扫描”才可以勾选设置。

(i) “资产精准识别” ：选择此模式可以获取更全面的资产数据，但是扫描时间会增加。

(ii) “Ping 识别资产” ：Ping 存活资产，也可入库，无论是否开放端口及协议。

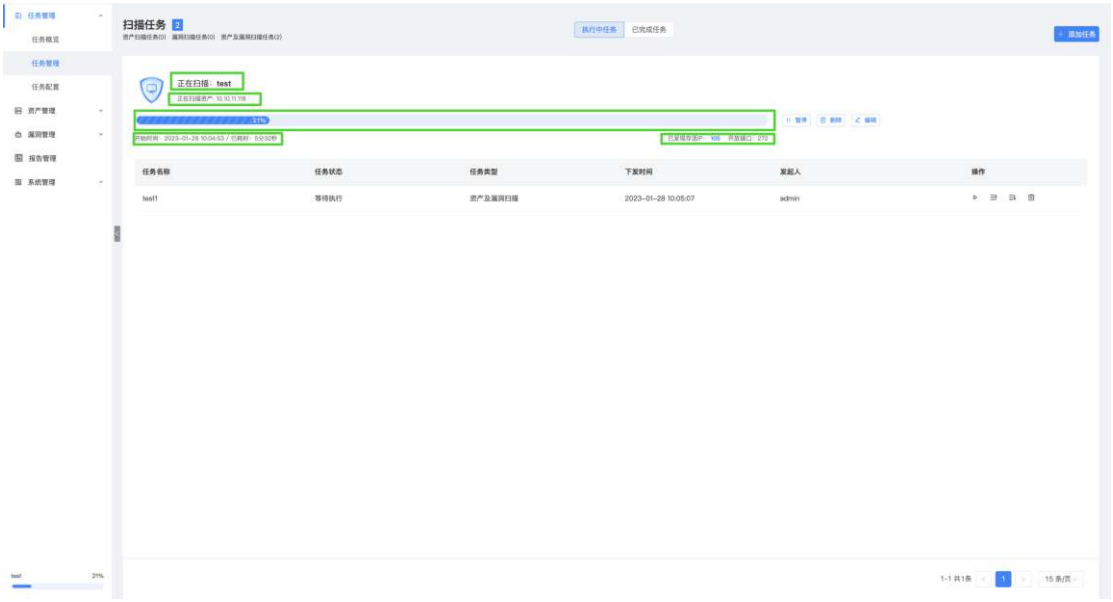
(iv)“版本号识别”：选择此模式可以识别版本号信息，但是扫描时间会增加。

(v)“深度识别操作系统及设备”：选择此模式，可深度识别操作系统及设备相关信息，扫描时间相应增长。

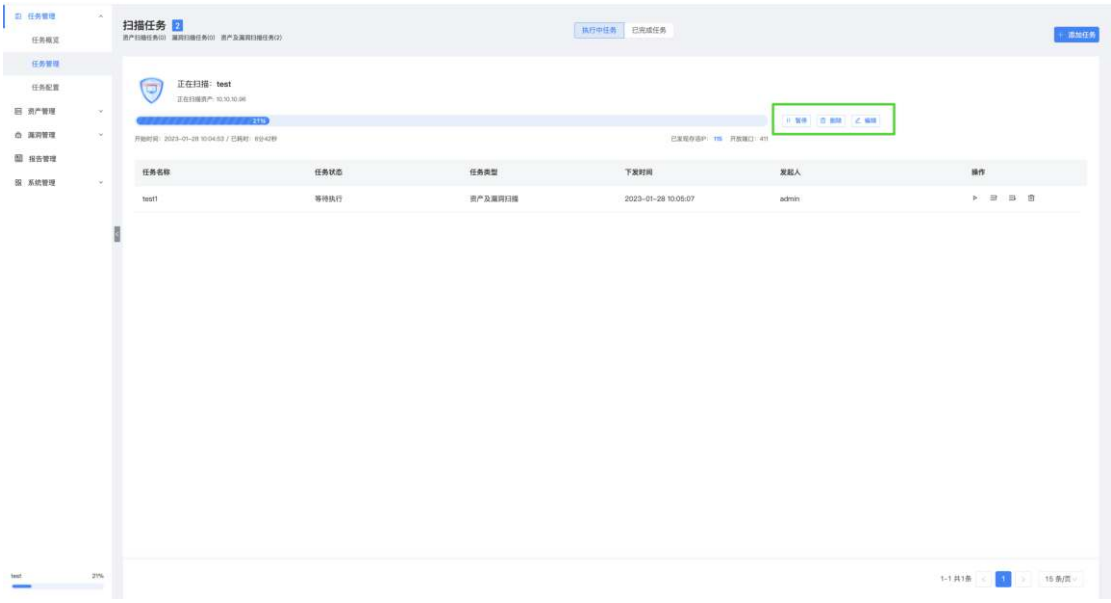
(vii)“开启爬虫”：开启爬虫后，需要爬取的资产越多，扫描时间越长。

3. 扫描任务状态

a. 在下发扫描任务后，显示扫描任务的相关信息，包括内容：任务名称、正在扫描资产、开始时间、任务耗时、任务进度等。

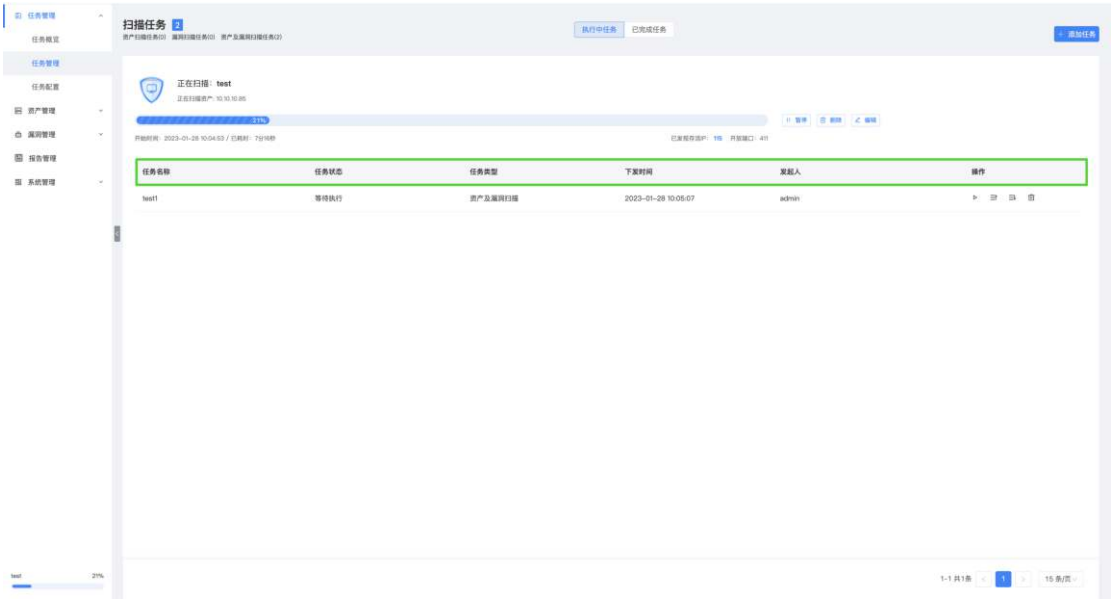


b. 如果有特殊情况需要停止或者暂停扫描点击“删除”按钮或者“暂停”按钮即可；若等待任务列表存在扫描任务，当前任务扫描完成或被删除后，会自动开始执行任务队列中的第一个任务；若不存在扫描任务，进入空数据页面。

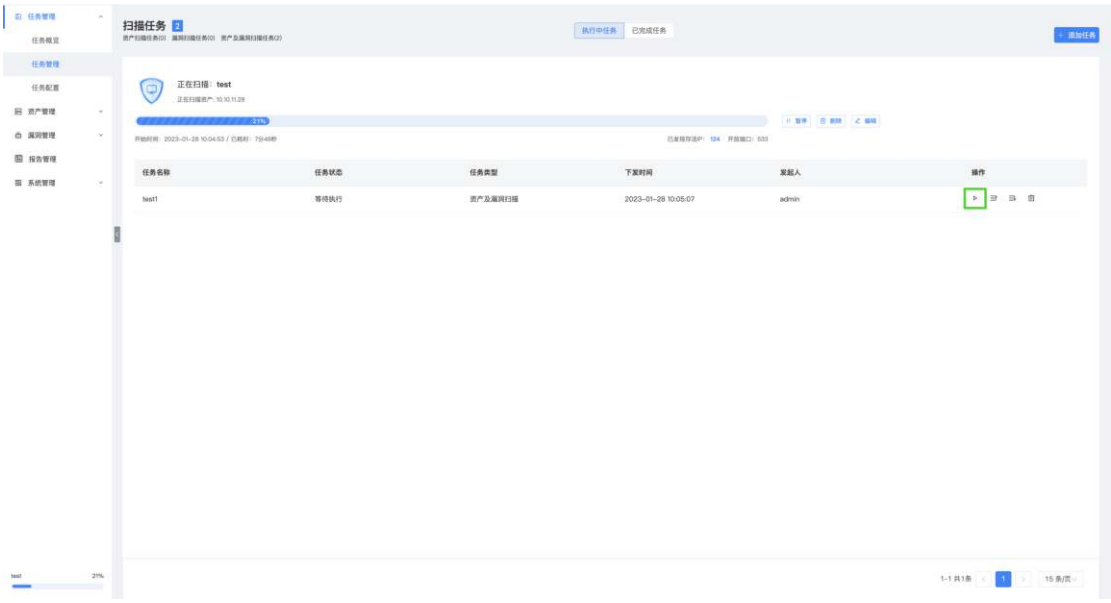


4. 等待扫描任务列表

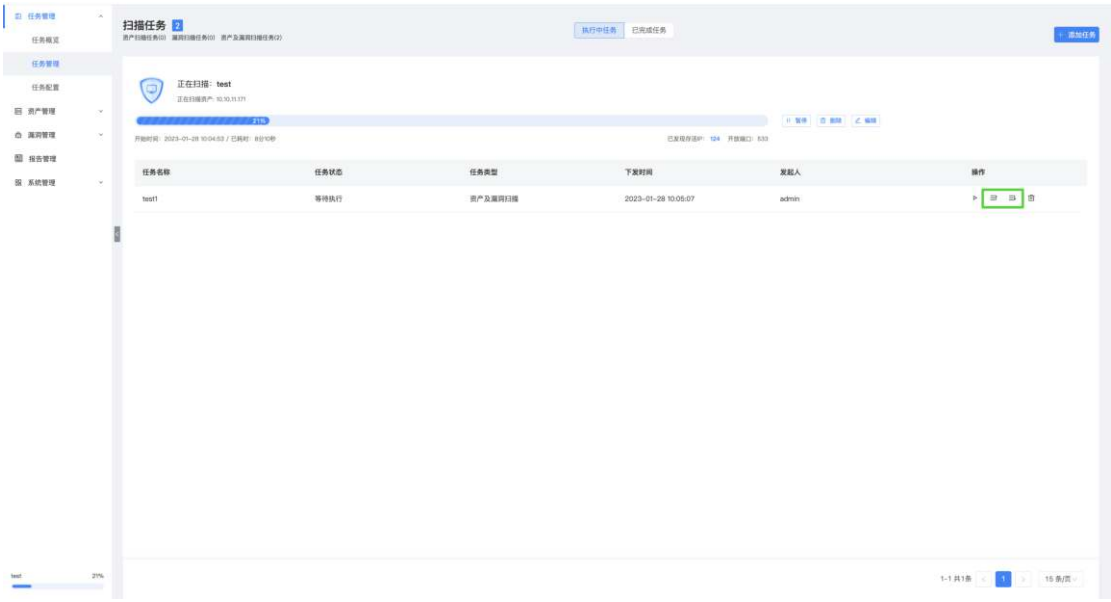
a. 等待扫描任务列表显示待扫描的任务，包含内容：任务名称、任务状态、任务类型、下发时间、发起人等信息。



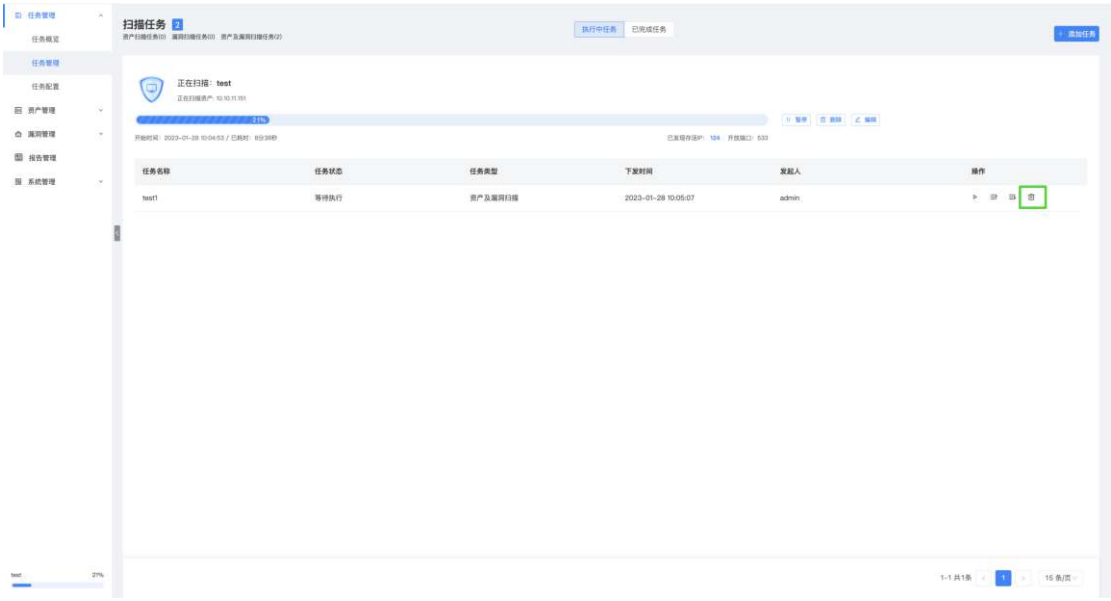
b. 等待任务列表，选中某个任务，点击开始图标，即可暂停正在执行的任务，立即执行该任务，被暂停的任务将显示在队列的第一个，并显示进度信息。



c. 等待扫描任务列表，选中某个任务，点击降低排位或者提升排位图标，可以更换执行扫描任务的先后顺序。

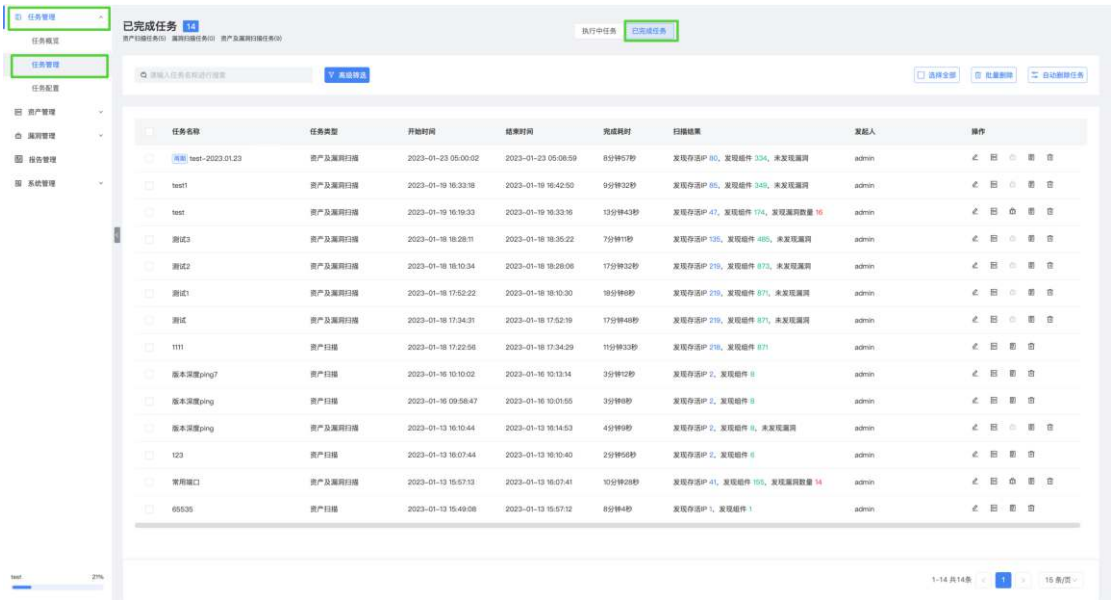


d. 等待扫描任务列表，选中某个任务，点击删除图标，可以删除该扫描任务，不在执行扫描。

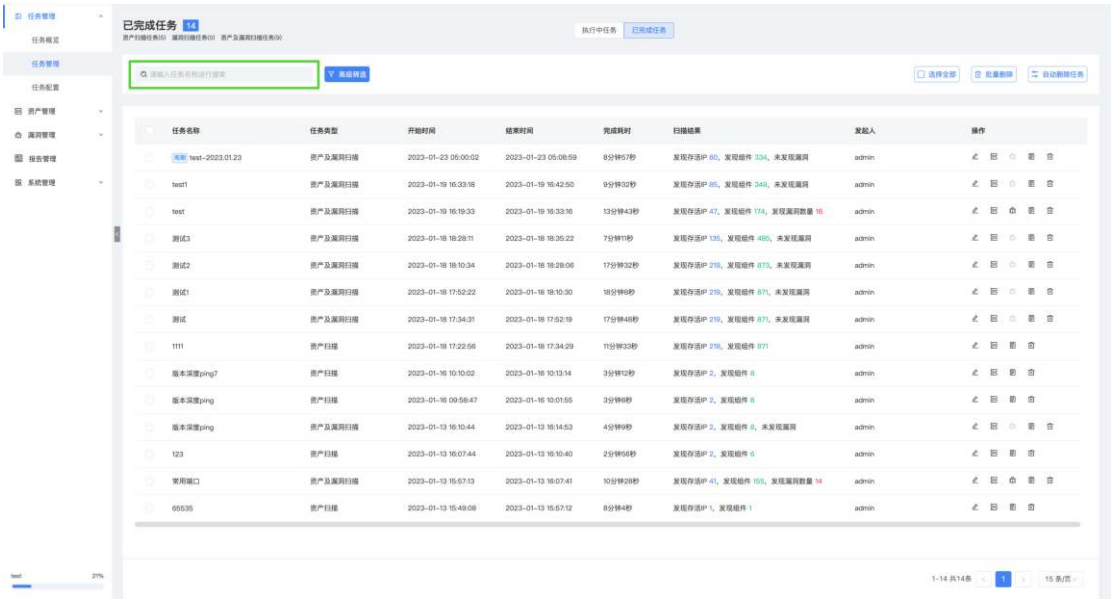


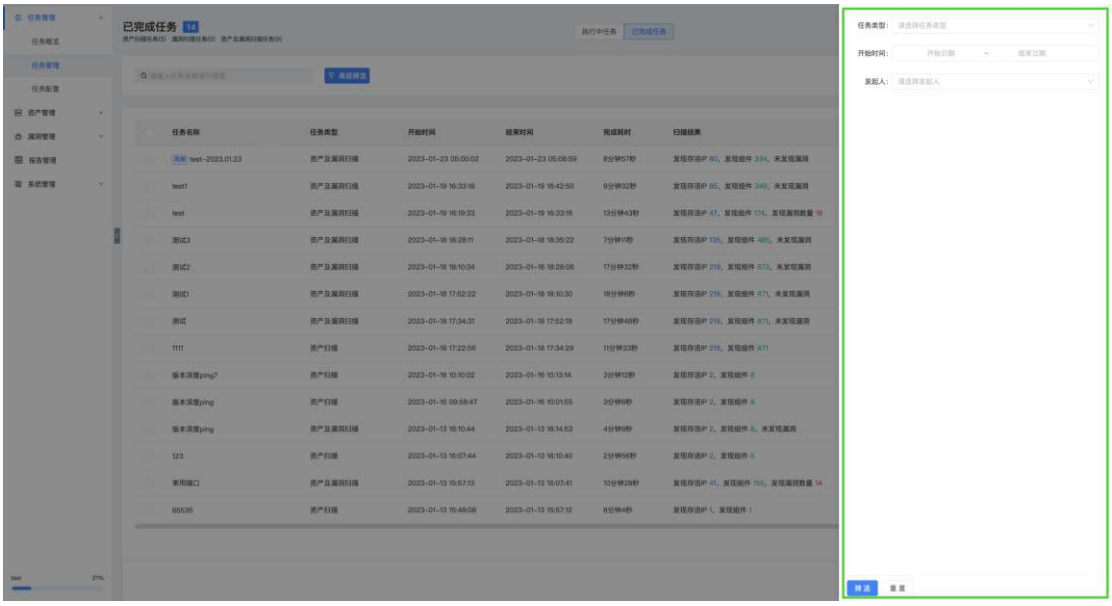
2.1.2.2 已完成任务

1.【任务管理】-【任务管理】页，点击“已完成任务”，标题栏显示已完成任务数量，具体分为：“资产扫描任务数量”、“漏洞扫描任务数量”、“资产及漏洞扫描任务数量”。

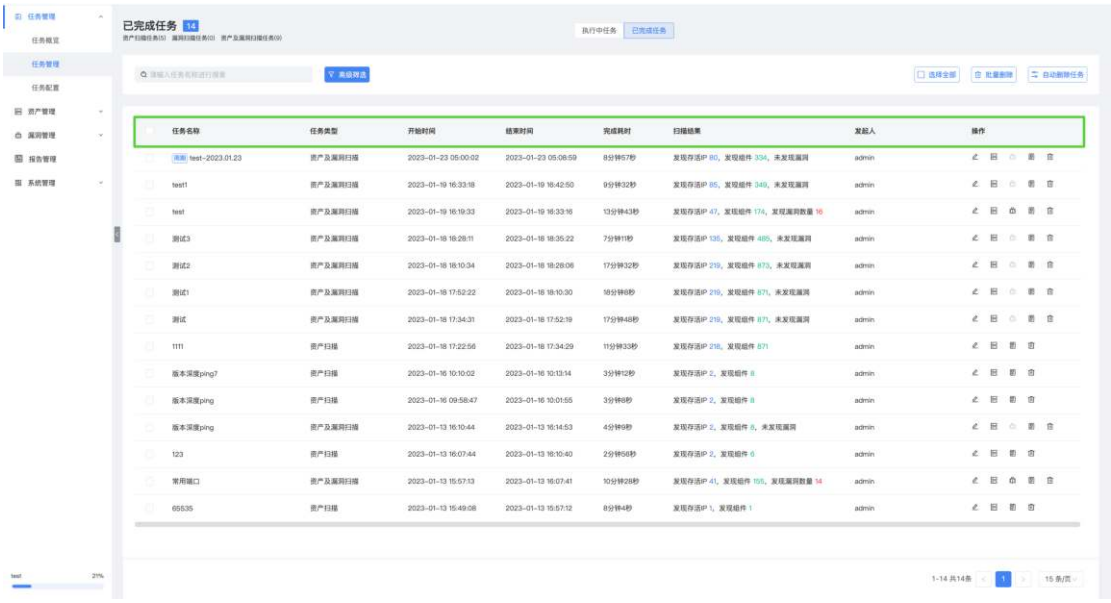


2. 支持任务名称的模糊搜索查询，支持高级筛选，包含内容：任务类型、开始时间、发起人。

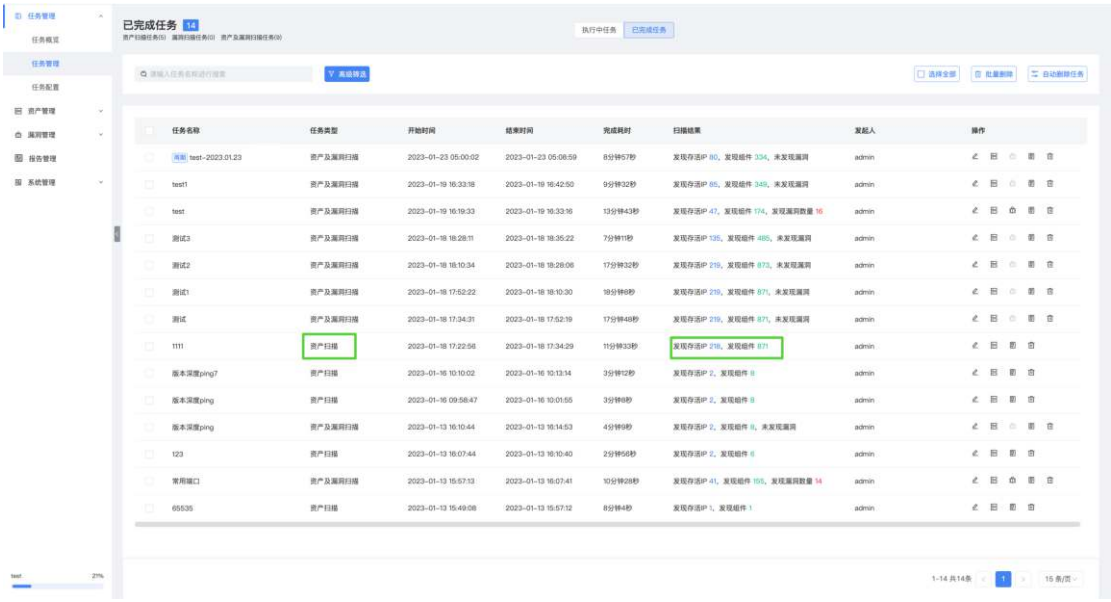




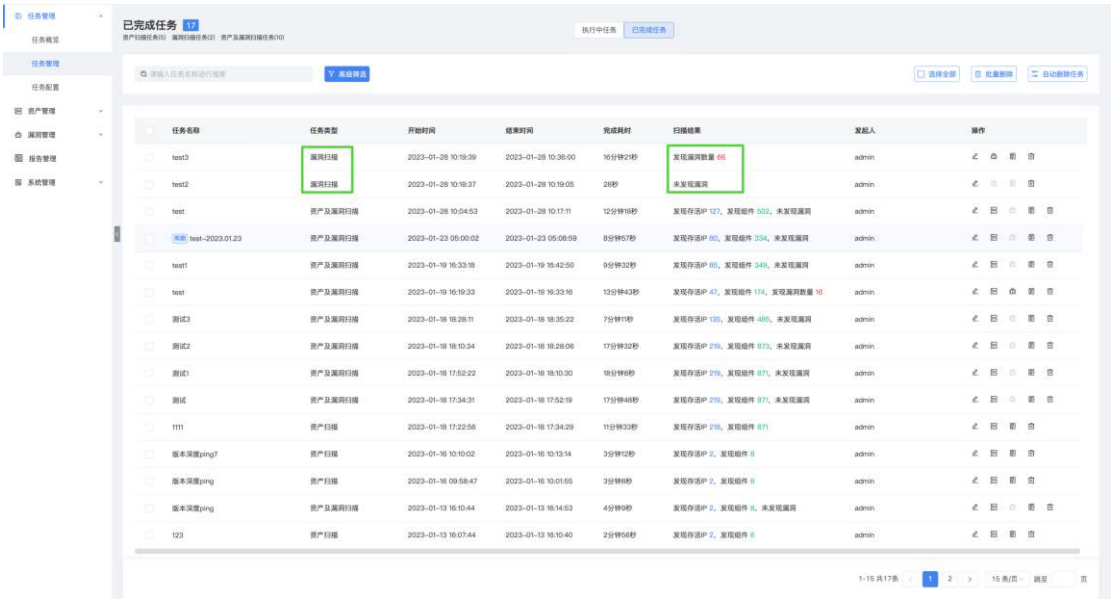
3. 显示已完成任务列表，包含内容：任务名称、任务类型、开始时间、结束时间、完成耗时、扫描结果、发起人等信息。



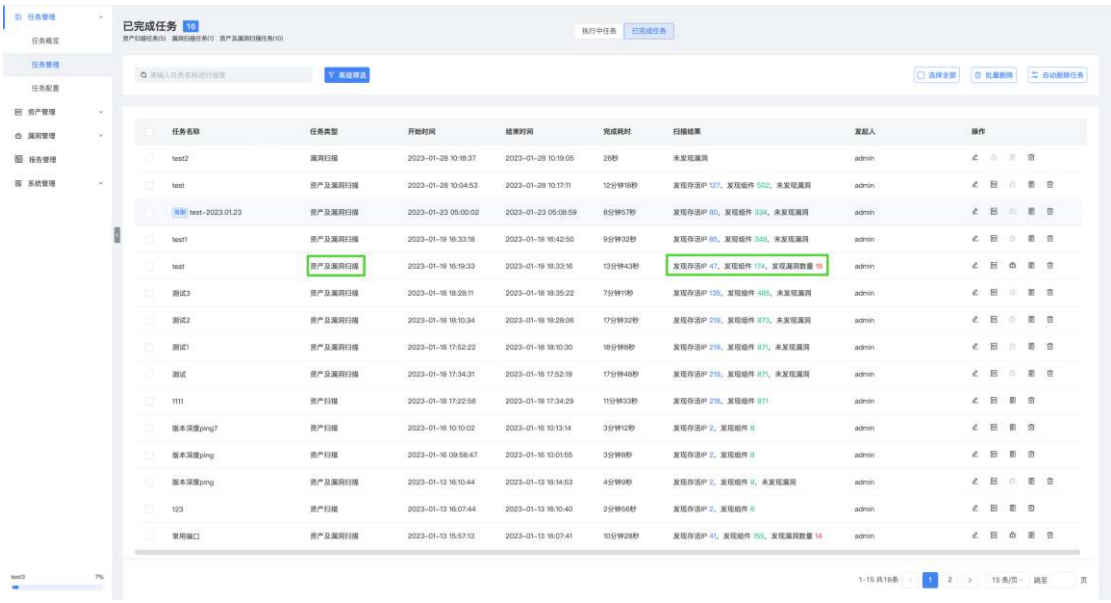
a. 资产扫描结果有两种情况：未发现网络资产；发现存货 IP XXX，发现资产组件 XXX。



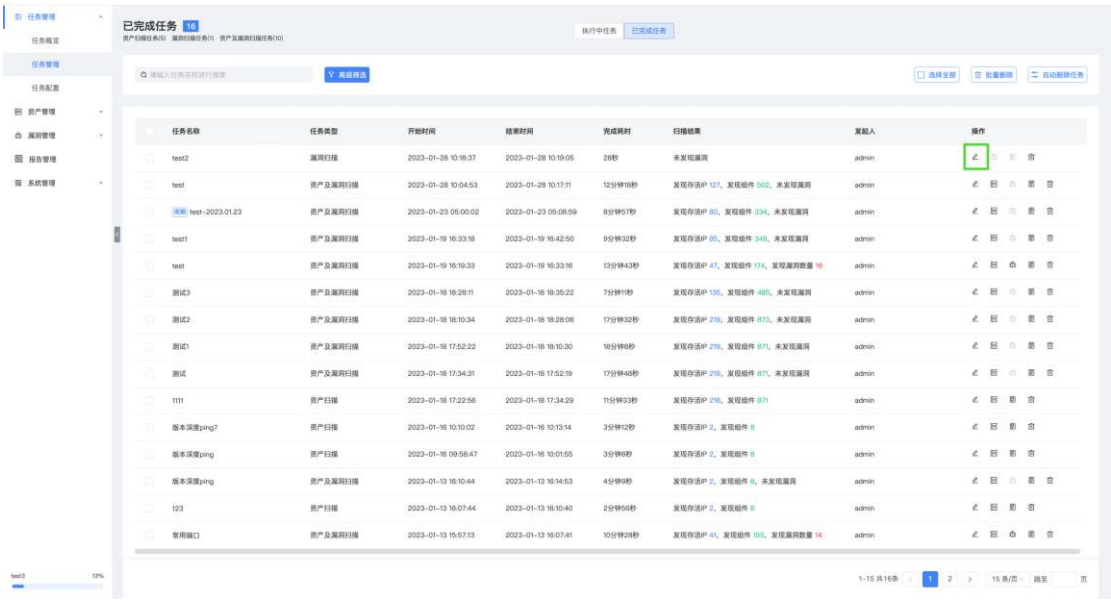
b. 漏洞扫描结果有两种情况：未发现漏洞；发现漏洞 XXX。



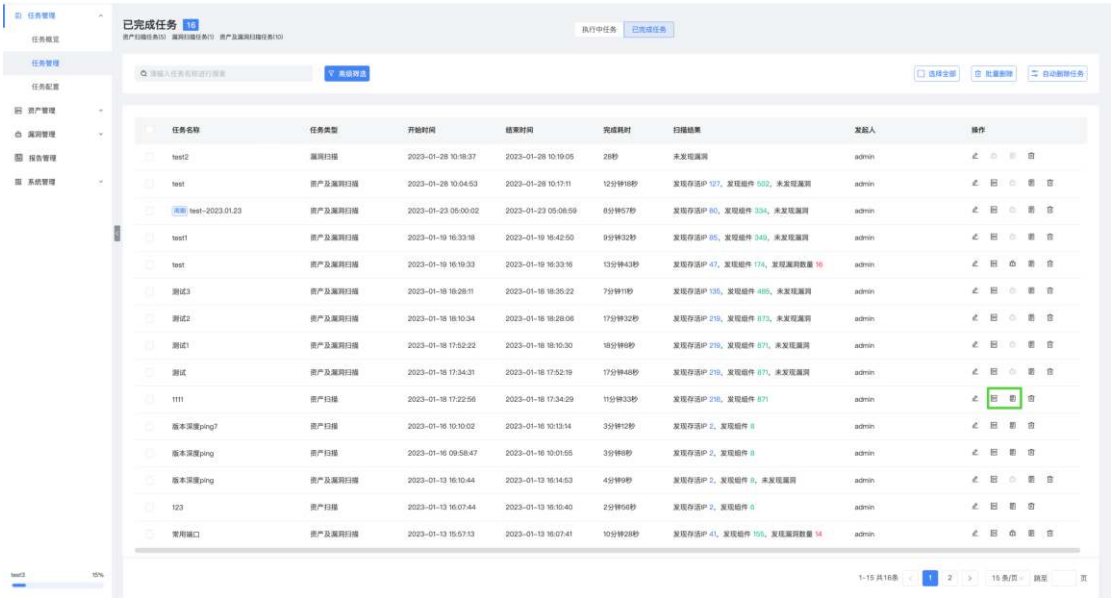
c. 资产及漏洞扫描结果



d. 已完成任务操作：选中某个任务，点击再次编辑图标，可二次编辑任务下发相关扫描策略，或重新下发该任务，下发扫描任务到执行中任务列表。



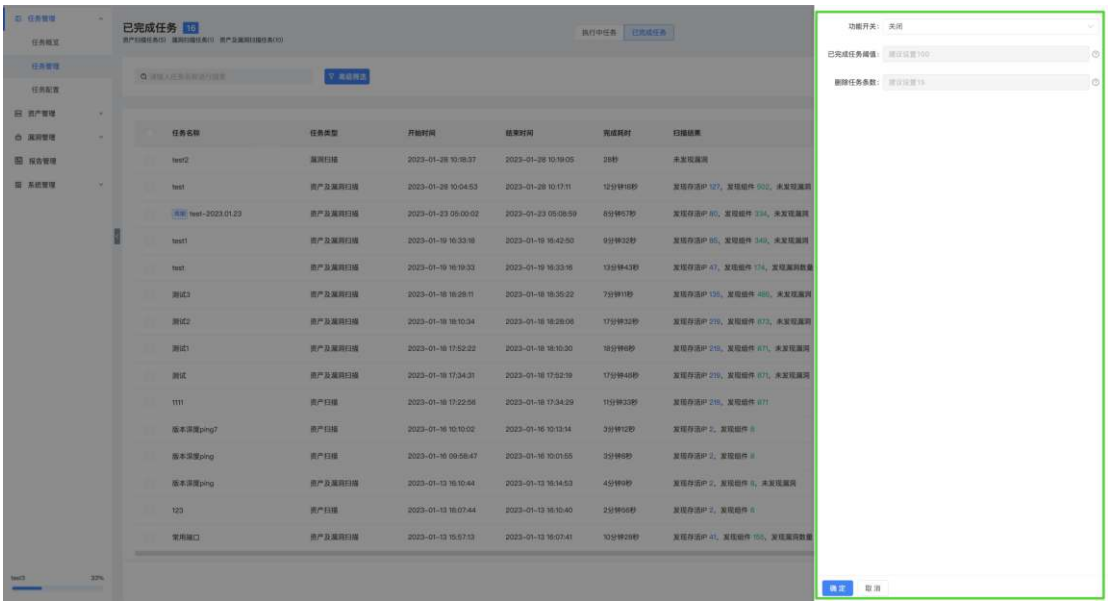
e. 选中某个任务，点击查看列表图标，查看该扫描任务的数据。资产扫描任务查看资产列表；漏洞扫描查看漏洞列表；资产及漏洞扫描查看资产列表和漏洞列表，仅限该任务扫描出来的数据范围，没有数据的时候该按钮为不可点击状态，打开列表后不可对数据进行修改或删除。



f. 选中某个任务，点击查看报告图标，查看该扫描任务的报告分析。

g. 已完成任务列表，选中某个任务，点击删除（右上角“批量删除”）图标，删除该扫描任务。

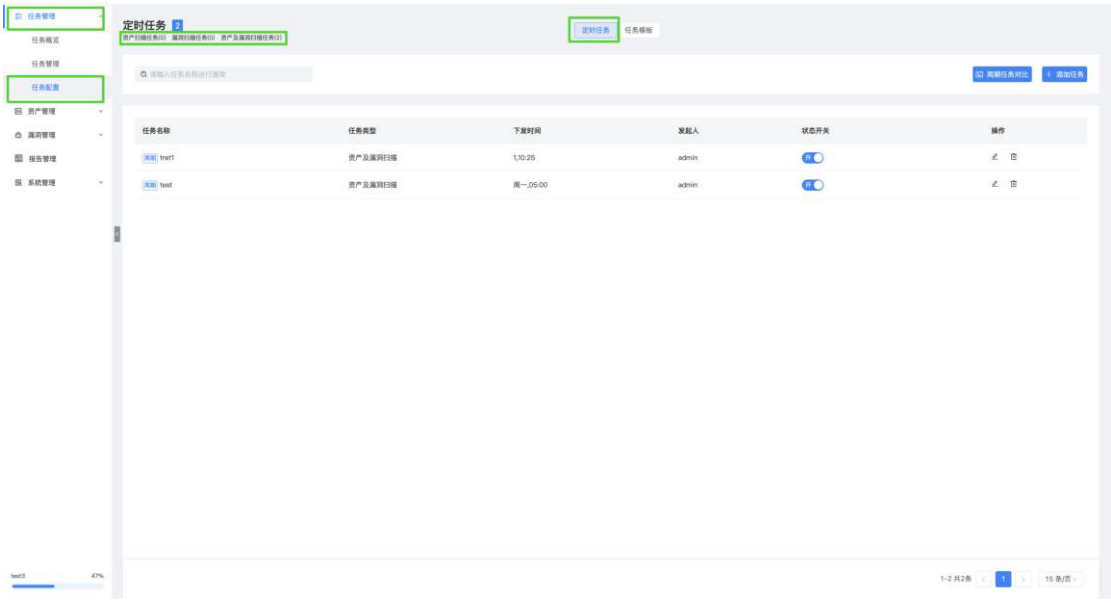
h. 已完成任务列表上，点击“自动删除”，开启后，支持根据设置的已完成任务条数阈值与删除已完成任务条数自定义删除任务。



2.1.3 任务配置

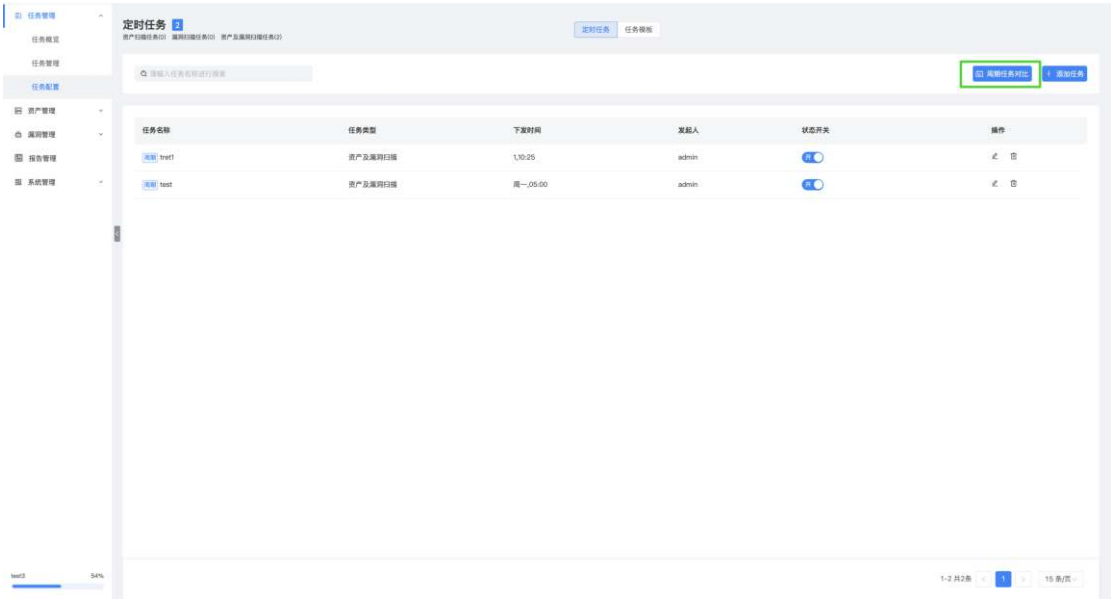
2.1.3.1 定时任务

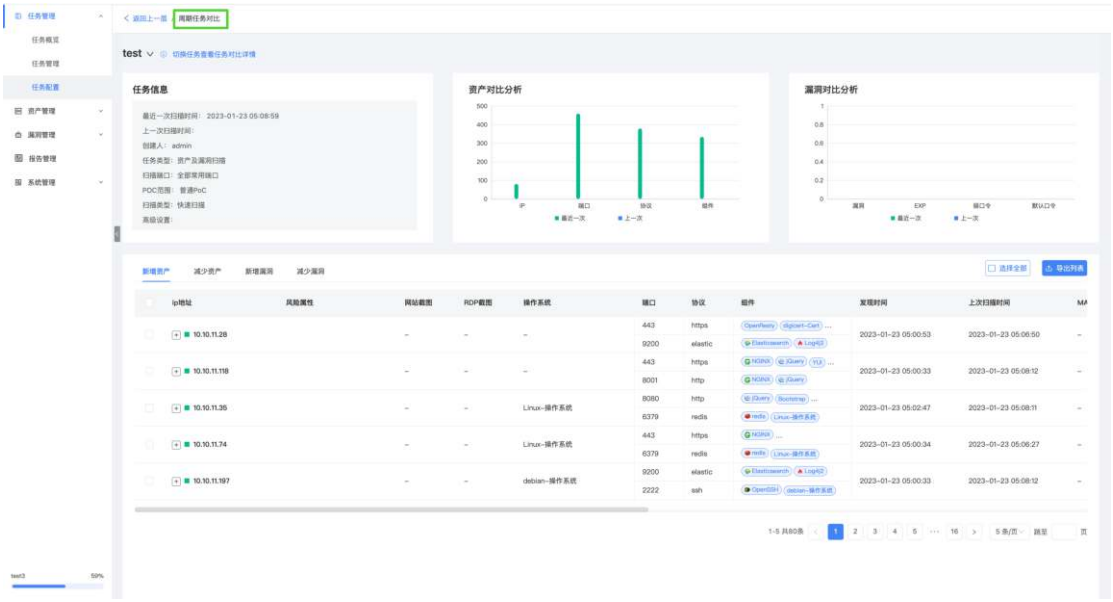
1.【任务管理】-【任务配置】页，默认显示“定时任务”，标题栏显示定时任务数量，具体分为：“资产扫描任务数量”、“漏洞扫描任务数量”、“资产及漏洞扫描任务数量”。



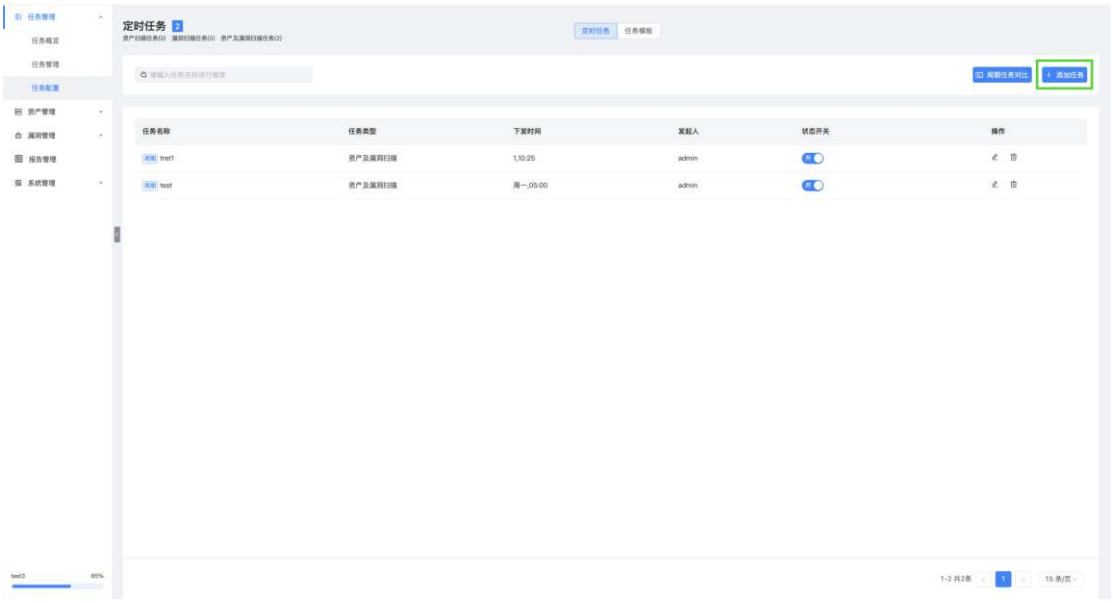
2. 支持根据任务名称对定时任务进行搜索查询，查询结果中的匹配字段高亮显示。

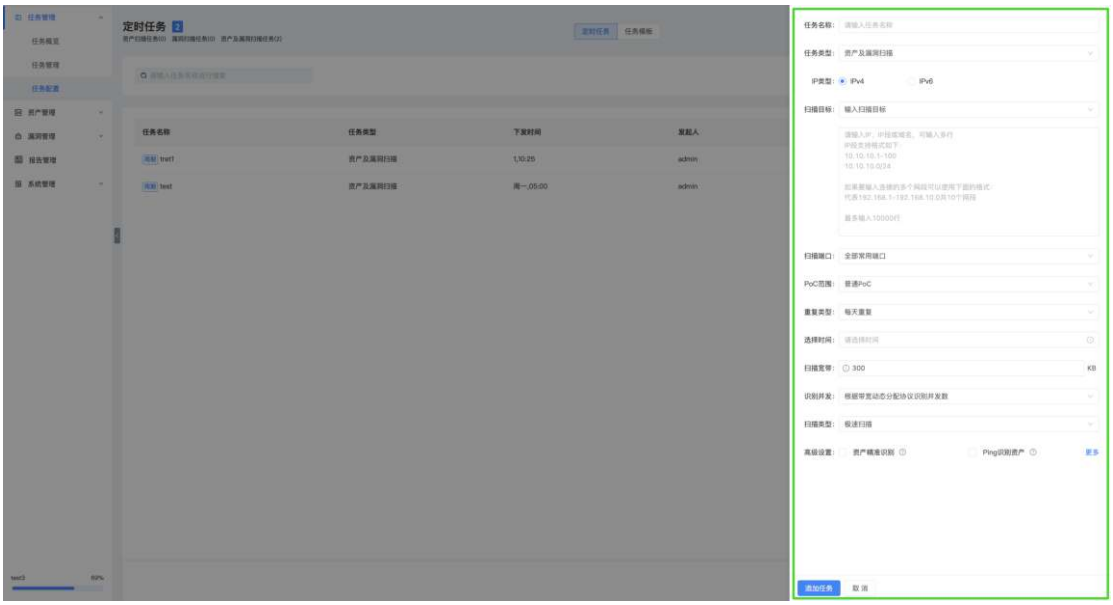
3. 支持周期任务对比，点击“周期任务对比”按钮，跳转周期任务对比详情页。



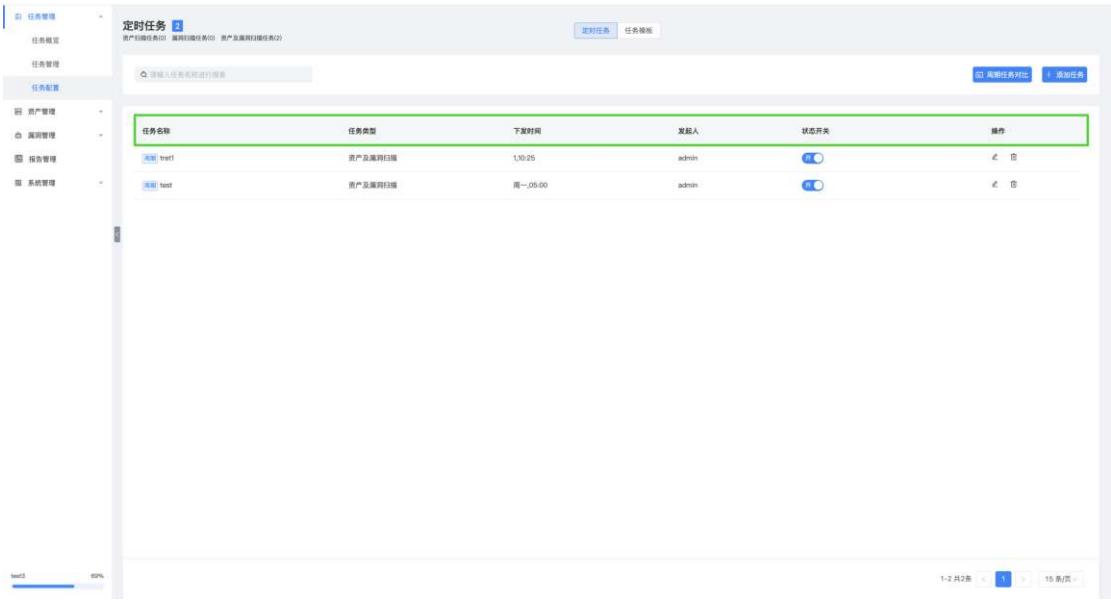


4. 支持添加任务，点击“添加任务”按钮，进行定时任务添加设置。添加定时任务“重复类型”：每天重复定时任务：每天重复 HH:MM；每周重复定时任务：每周重复 星期 X HH:MM；每月重复定时任务：每月重复 日期 HH:MM；仅执行一次定时任务：YYYY,MM.DD HH:MM。定时任务到达约定时间后会自动下发扫描任务到执行中任务列表，仅执行一次的定时任务成功下发任务后将自动从定时任务列表中删除。





5. 定时任务列表：展示已添加的定时任务列表，包括：任务名称、任务类型、下发时间、发起人、任务开关等信息。

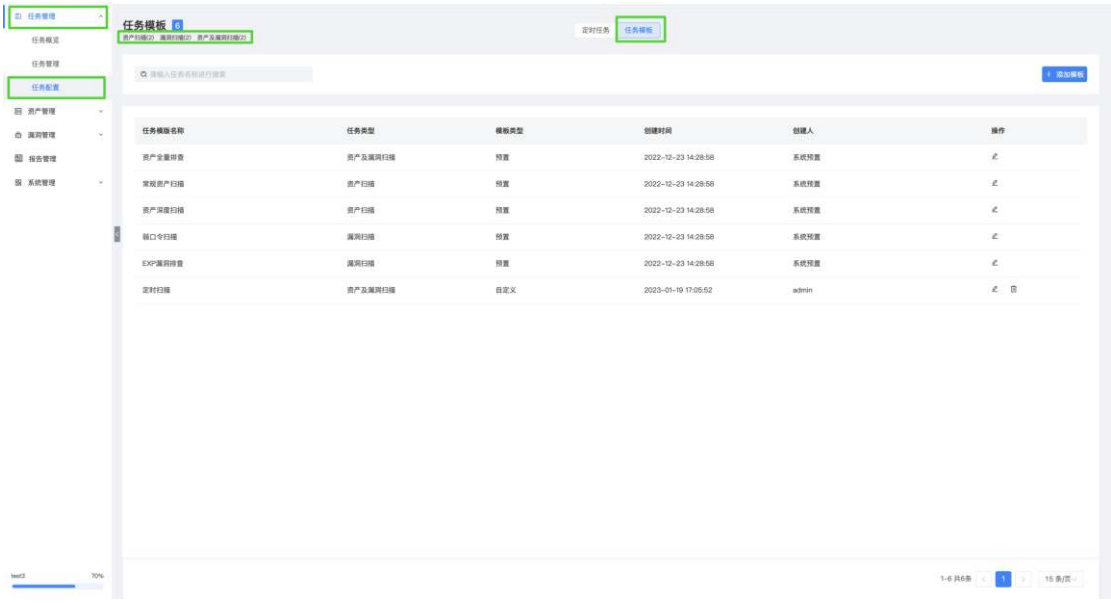


a. 选中定时任务列表中的某个定时任务，点击关闭/开启按钮，可以关闭或开启周期性定时任务，关闭后不再执行；普通定时任务不存在任务开关。

b. 选中定时任务列表中的某个定时任务，点击编辑/删除按钮，可以对定时任务编辑、删除。

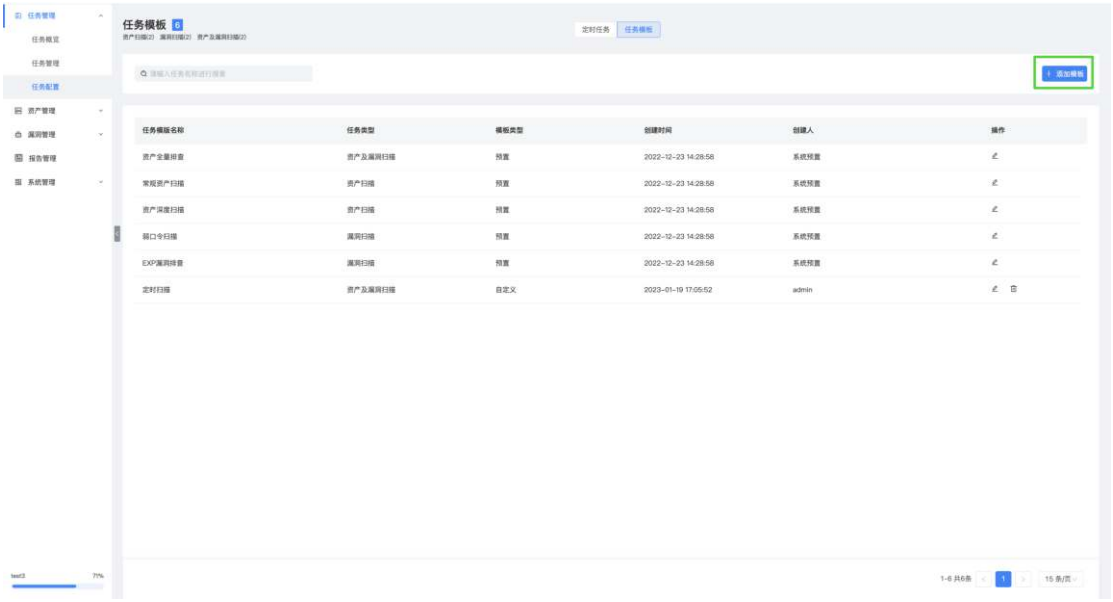
2.1.3.2 任务模板

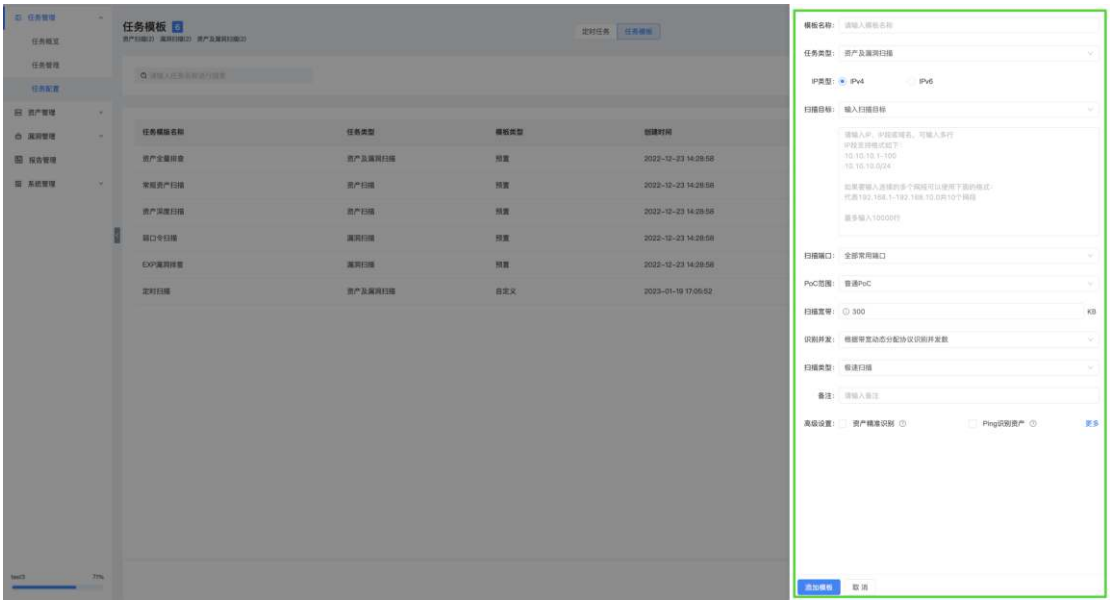
1.【任务管理】-【任务配置】页，点击“任务模板”，标题栏显示任务模板数量，具体分为：“资产扫扫描任务数量”、“漏洞扫描任务数量”、“资产及漏洞扫描任务数量”。



2. 支持根据模板名称进行搜索查询

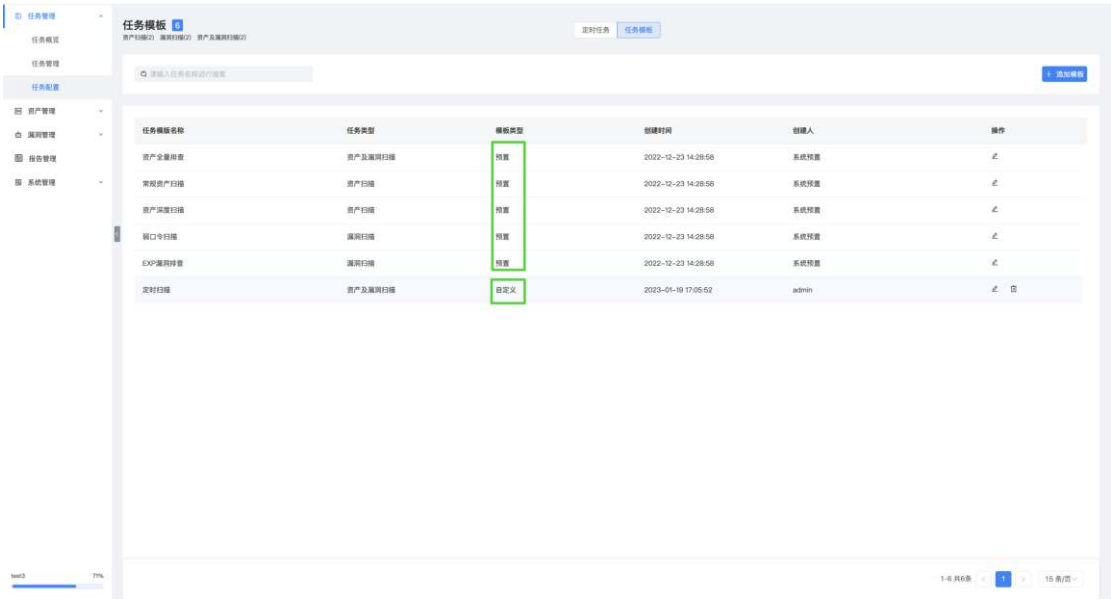
3. 点击“添加模板”按钮，自定义添加任务模板。





4. 任务模板列表：展示任务模板列表，包括：任务模板名称、任务类型、模板类型、创建时间、创建人等信息。

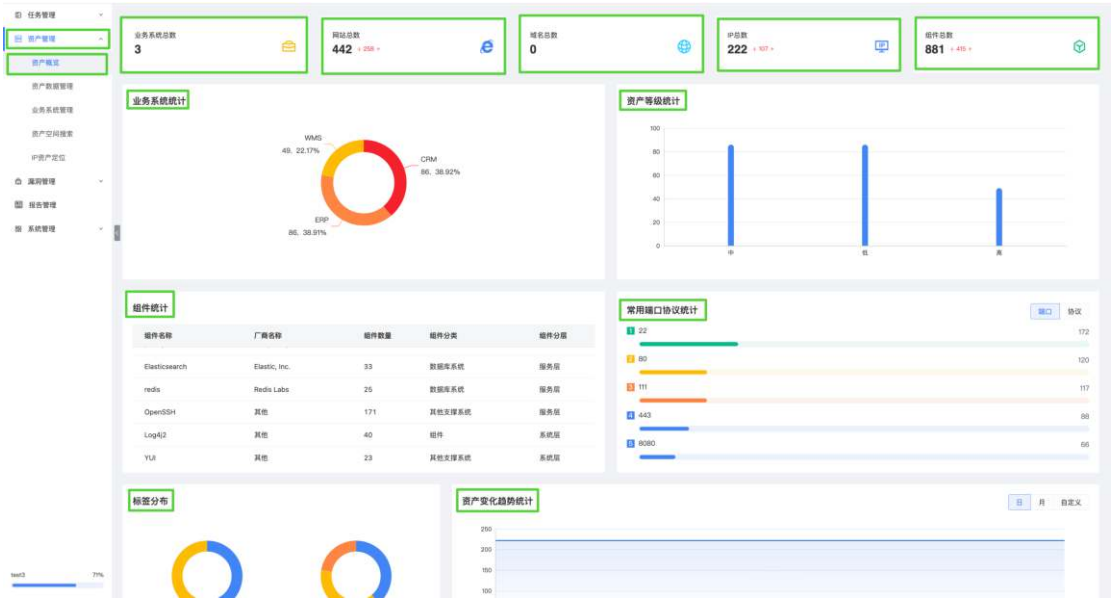
5. 模板类型包括系统预置、自定义两种，其中系统预置模板可编辑系统预置模板的扫描目标与扫描宽带，不可删除；自定义模板可随便编辑/删除。



2.2 资产管理

2.2.1 资产概览

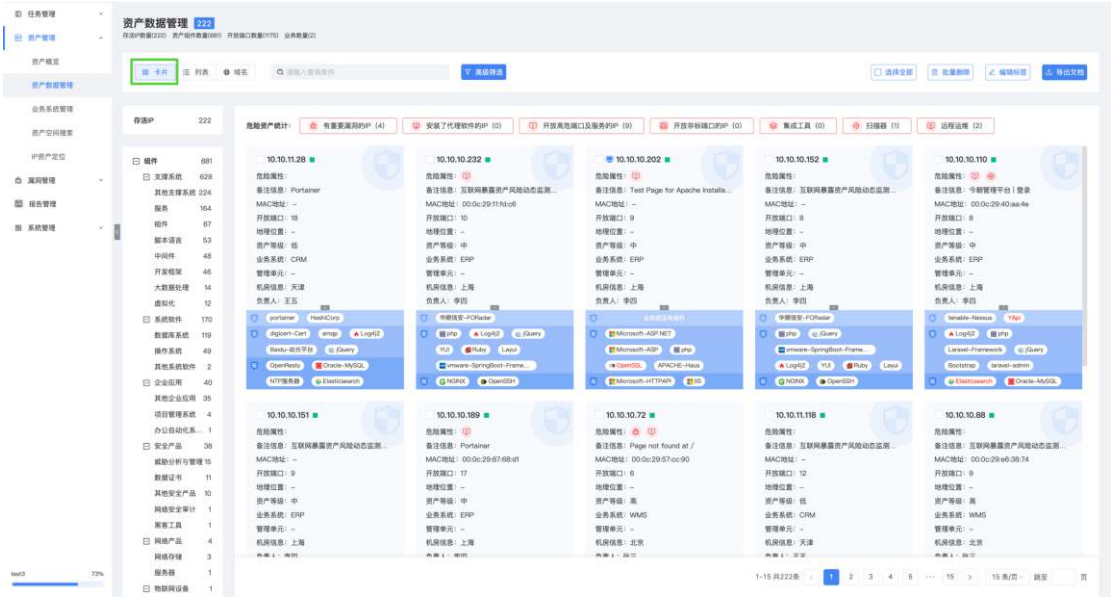
【资产管理】-【资产概览】页，展示了“业务系统总数”、“网站总数”、“域名总数”、“IP 总数”、“组件总数”以及“组件统计”、“常用端口协议统计”、“标签分布”、“资产变化趋势统计”等信息概览。

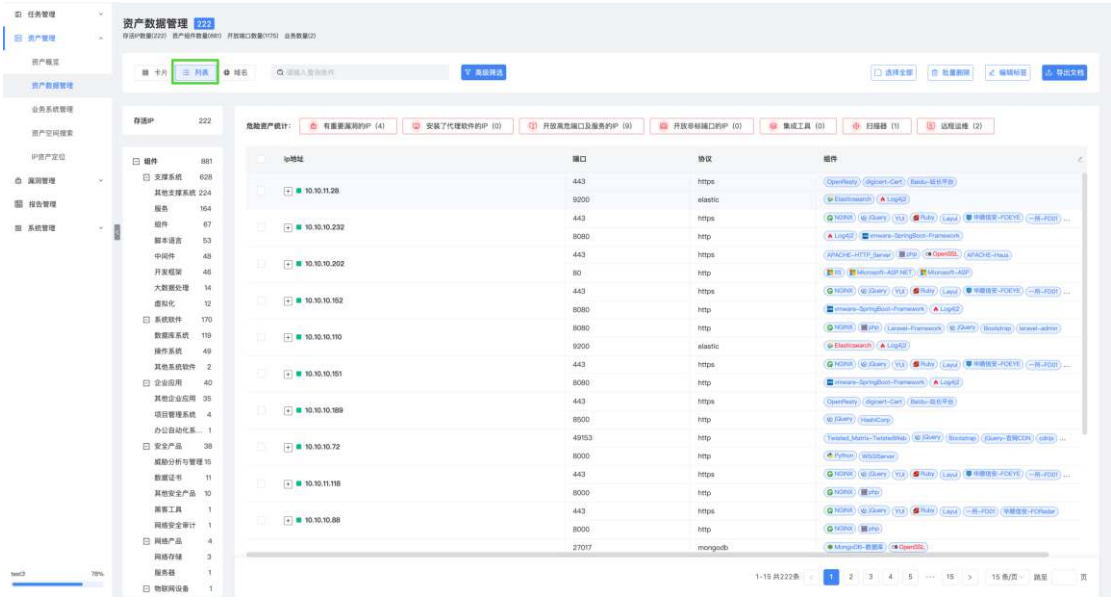


2.2.2 资产数据管理

1.【资产管理】-【资产数据管理】页，标题栏显示全量资产的数据信息，具体分为：“存活 IP 数量”、“资产组件数量”、“开放端口数量”、“业务数量”。基本单元为 IP，因此添加的对象大部分是与 IP 相关的。

2. 该页包括卡片、列表、域名视角。卡片视角可直接查看各层组件信息；列表视角支持查看更多 IP 详细信息；域名视角支持查看域名下相关的 IP 信息。





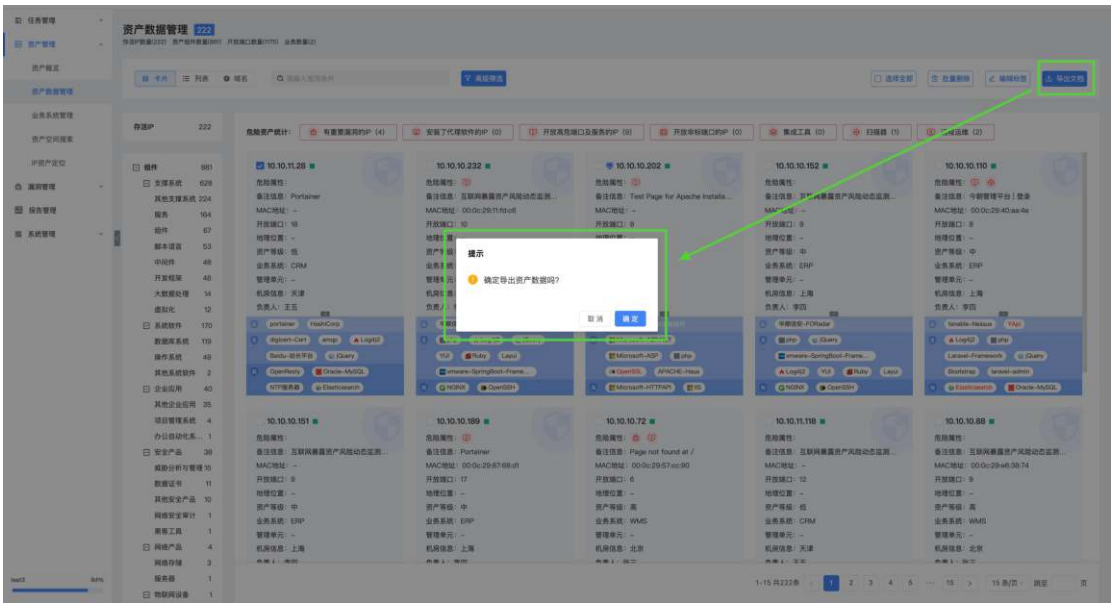
3. 支持对资产进行模糊查询，查询字段包括：IP、备注信息、MAC 地址、开放端口、开放服务、组件标签等，查询结果中的匹配字段高亮显示

a. 支持高级搜索，筛选项包括：组件类型（包含以及和二级分类）、组件名称、IP 类型、资产状态、发现方式、开放端口、开放服务、厂商品牌、负责人信息、业务系统、管理单元、资产等级、机房信息、地理位置、发现时间、自定义标签等。

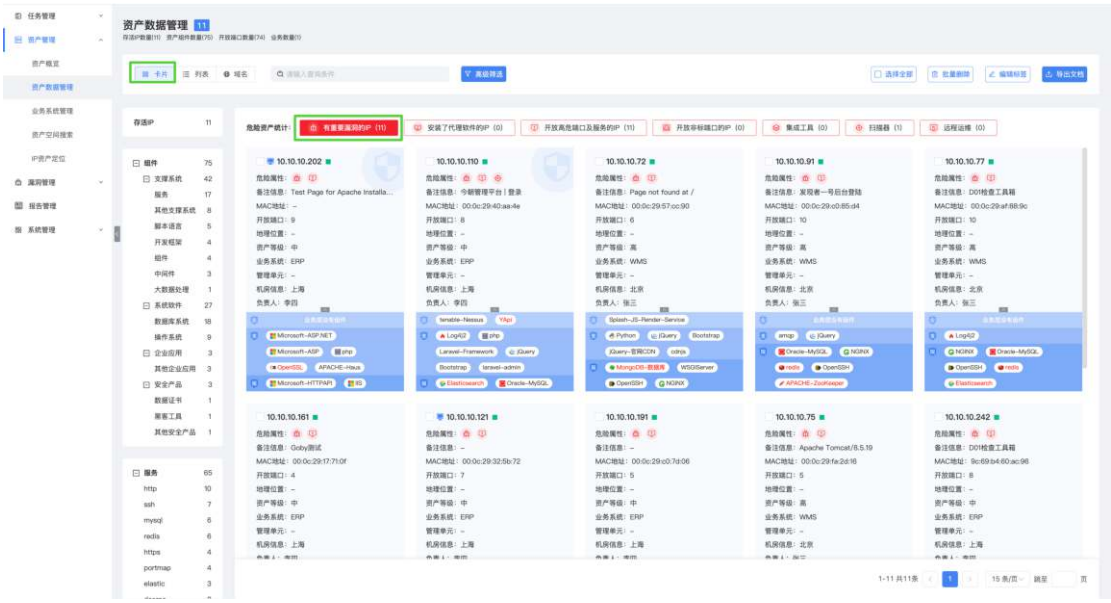
4. 支持全选功能，对当前列表中的全部数据进行全选，选择后可以进行删除资产，也可以对资产进行标签修改。

5. 支持查看网络拓扑信息，点击“网络拓扑”按钮即可跳转查看相关信息。

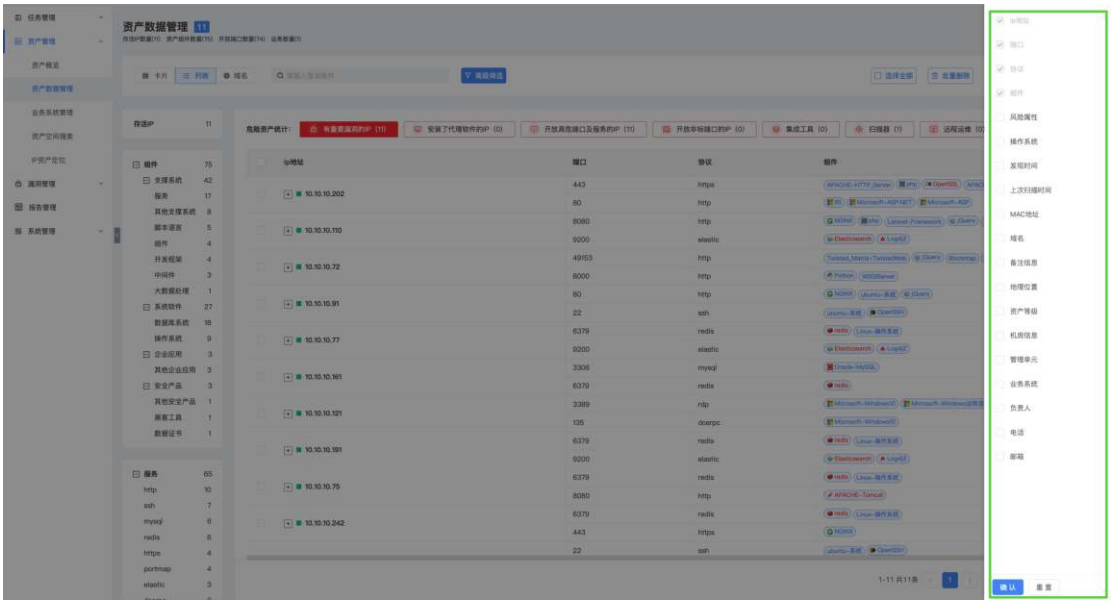
6. 支持资产信息导出功能，选择资产后点击“导出文档”按钮，导出的文档可选择普通列表或 IP+端口两种类型，导出的文档为 Excel，文件名称为：“资产列表_YYYYMMDD_HHMMSS”



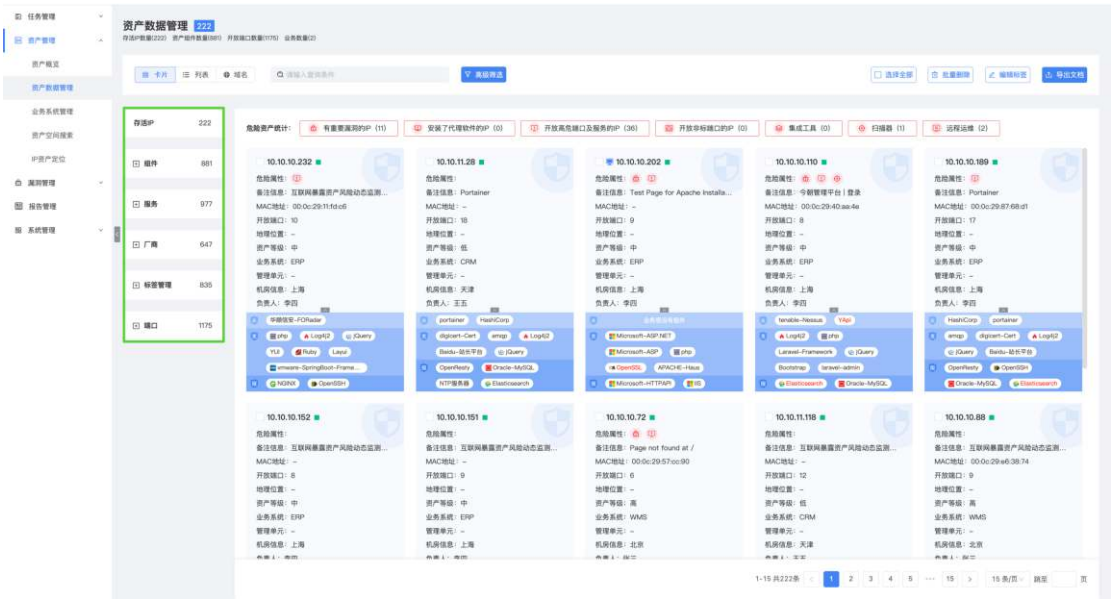
7. 卡片、列表维度支持危险资产标签筛选功能。



8. 列表维度支持自定义显示字段

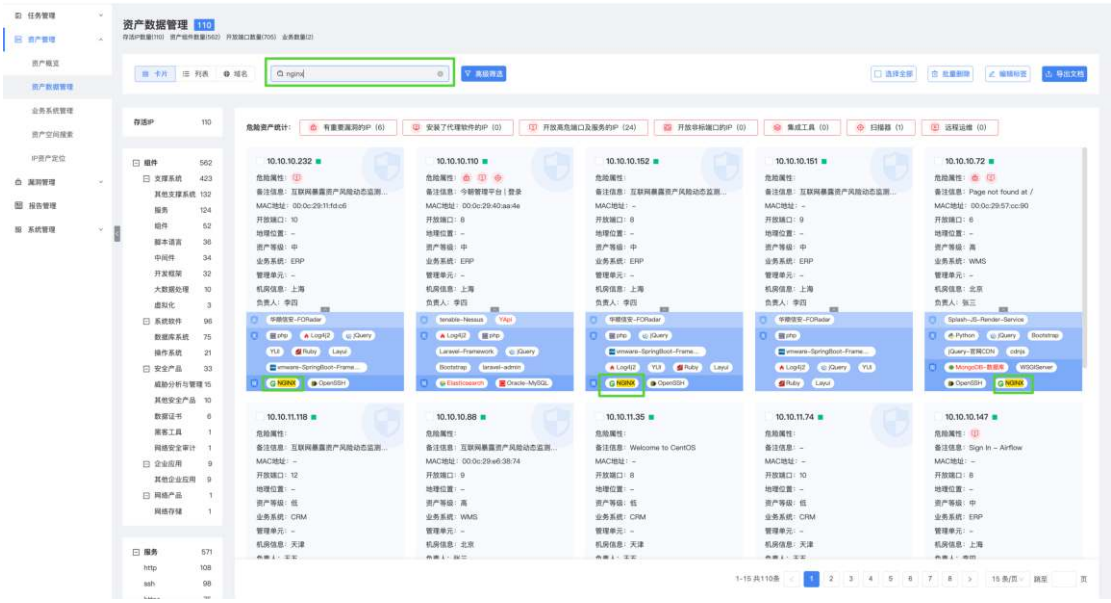


9. 资产数据统计栏：资产数据统计栏显示当前资产范围的数据统计信息，可以对含有子类的数据项展开或收起，默认全部展开，一级分类包含：存活 IP、组件、服务、厂商、标签管理、端口。



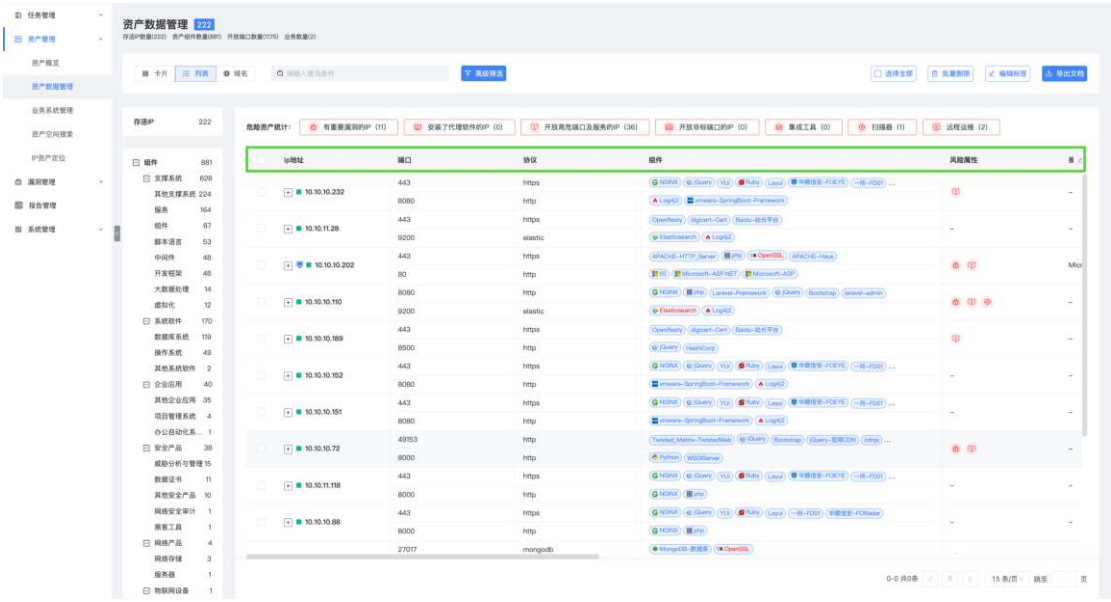
10. 资产数据展示

a. 资产以卡片的形式展示，包含数据如下：IP 地址、危险属性、备注信息、MAC 地址、开放端口、地理位置、资产等级、业务系统、管理单元、机房信息、负责人、组件标签：分层显示组件信息、层级结构为：应用层、支撑层、服务层、系统层、硬件层。当层级没有组件信息时显示“层级名称未发现组件”等信息。组件标签刻意点击执行查询，会在搜索框中显示查询的组件信息。

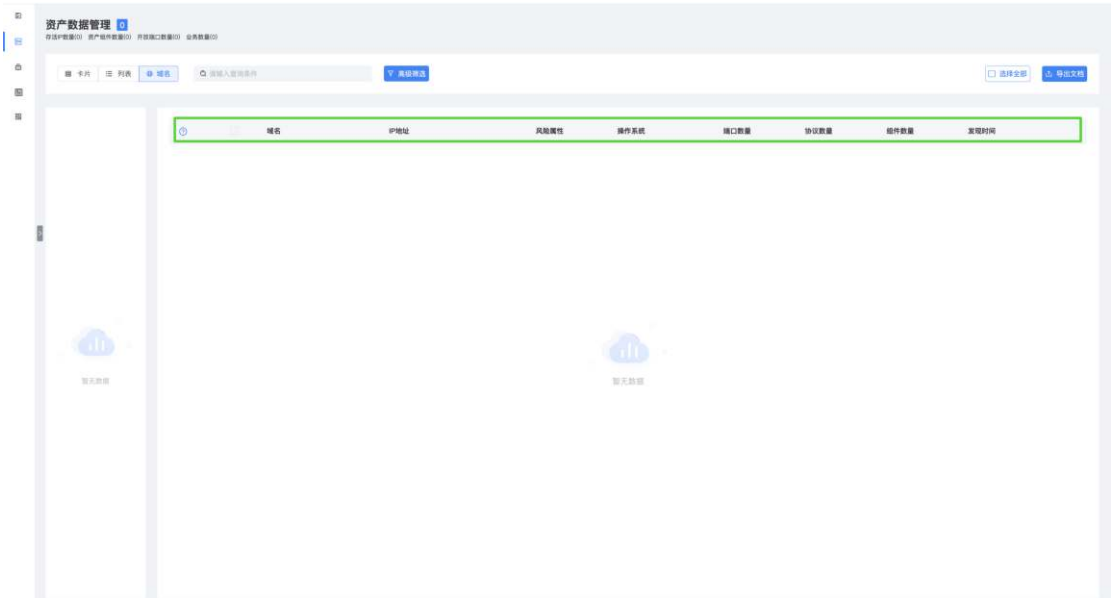


b. 资产以列表的形式展示，包含字段：IP 地址、端口、协议、组件、风险属性、操作系统、发现时间、上次扫描时间、MAC 地址、域名、地理位

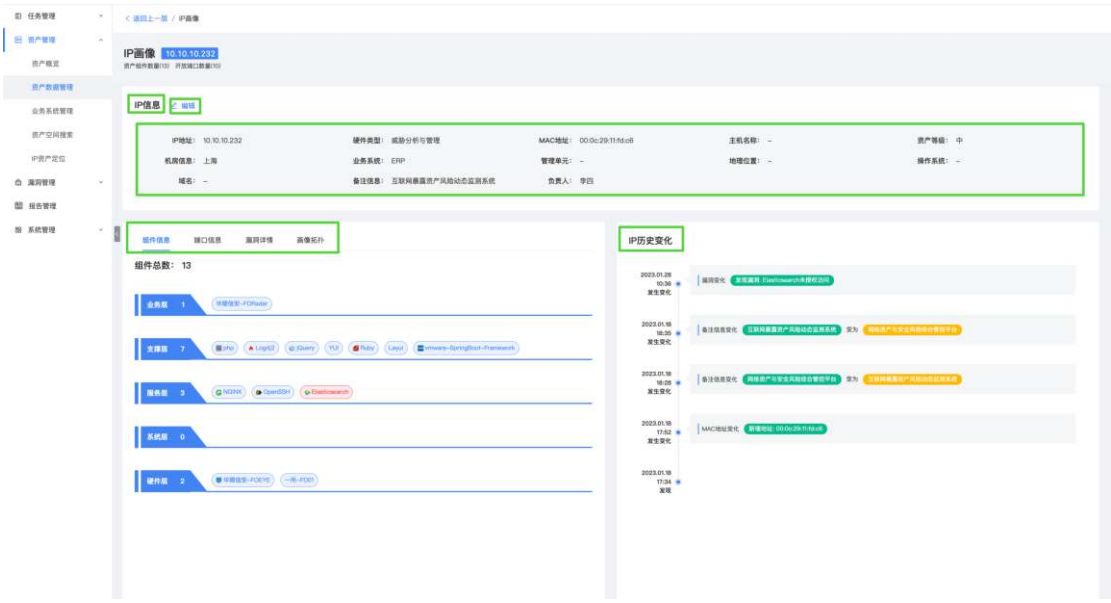
置、资产等级、机房信息、管理单元、业务系统、负责人、电话、邮箱、标签等



c. 展示域名资产，包含字段：域名、IP 地址、风险属性、操作系统、端口数量、协议数量、组件数量、发现时间。

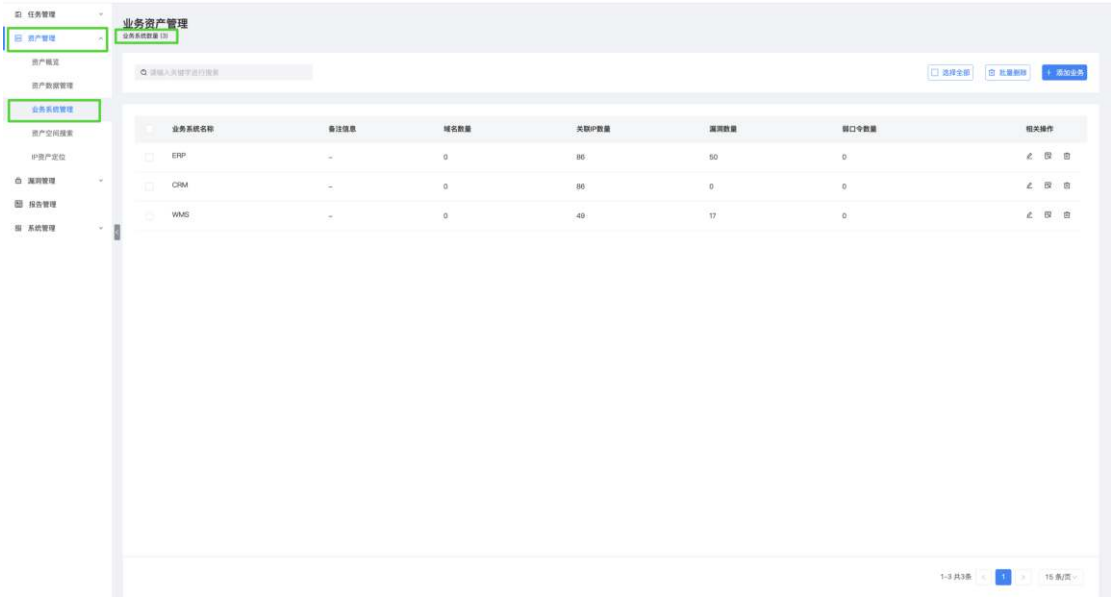


11. IP 画像：【资产管理】-【资产数据管理】点击单个 IP 查看资产详情，包含：IP 信息、组件信息、端口信息、漏洞详情、画像拓扑、IP 历史变化。其中 IP 信息包含：IP 地址、硬件类型、MAC 地址、资产等级、机房信息、业务系统、管理单元、地理位置、操作系统、域名、备注信息、负责人。支持 IP“备注信息”、MAC 地址的编辑修改。端口信息可查看相关链接和网页代码；漏洞详情点击漏洞名称可查看漏洞详情内容。



2.2.3 业务系统管理

1.【资产管理】-【业务系统管理】页，标题显示业务系统数量。

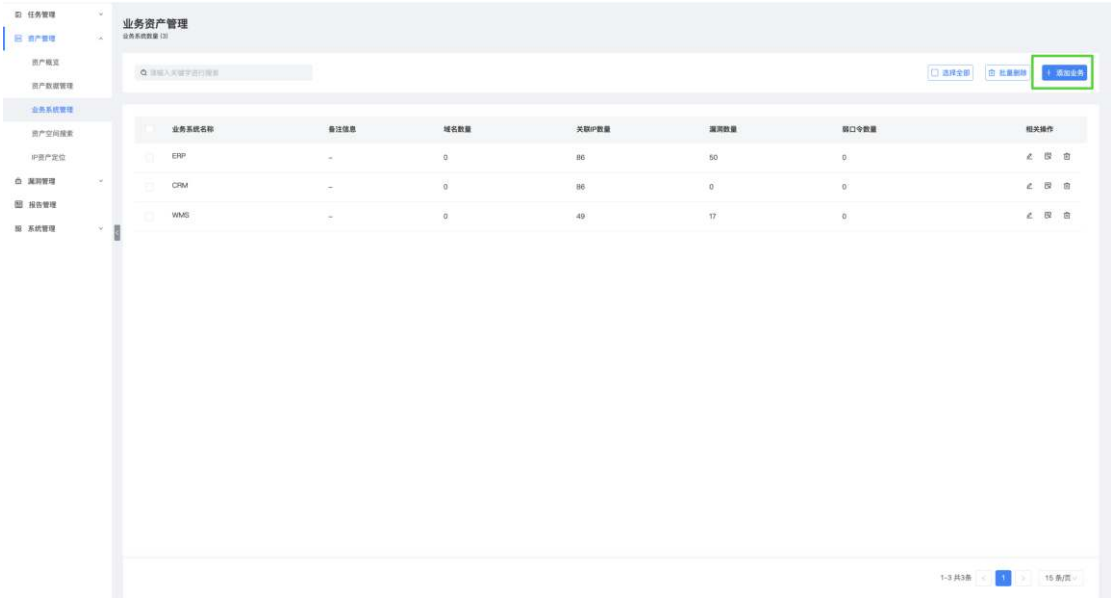


2. 支持模糊搜索 支持根据业务系统名称进行模糊搜索查询，查询结果中的匹配字段高亮显示。

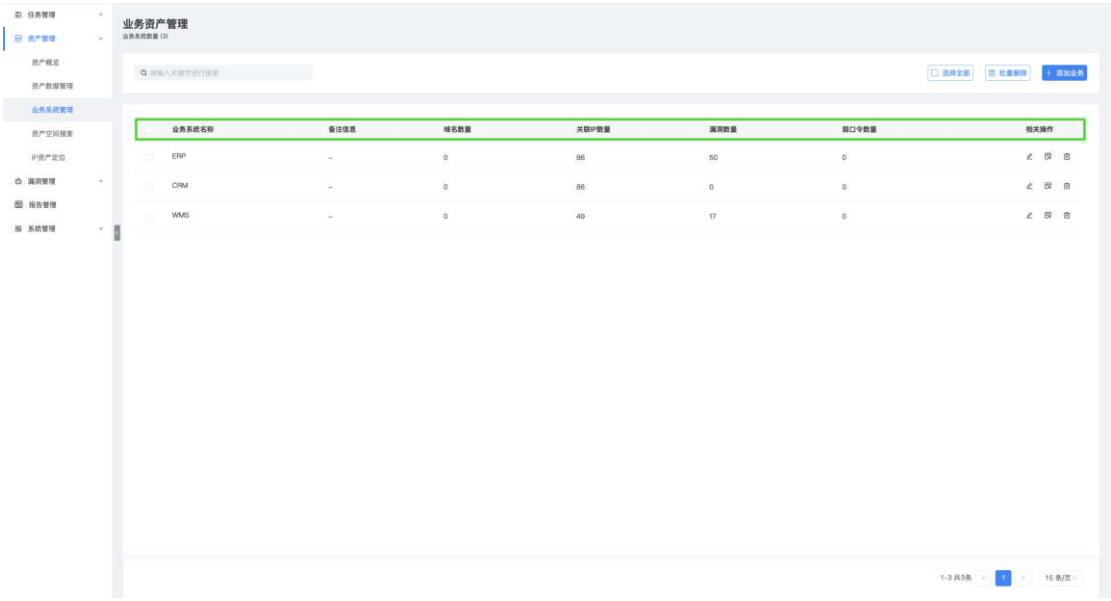
3. 支持全选功能，对当前列表中的全部数据进行全选，选择后可以进行

批量删除。

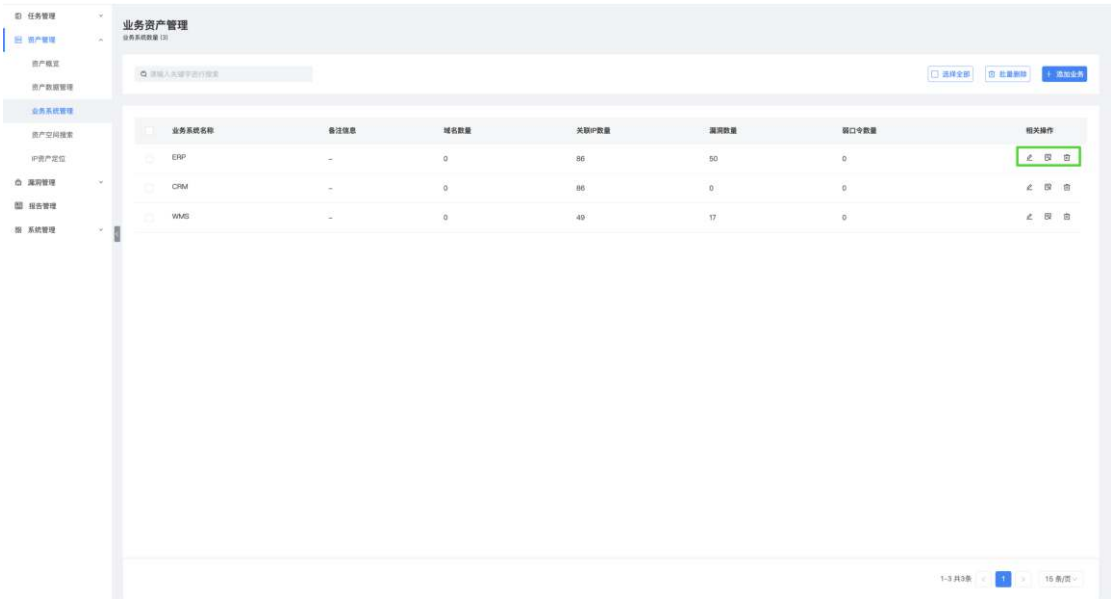
4. 添加业务：点击“添加业务”按钮，即可添加新的业务系统，需要的添加的内容包括：选择业务系统或手动输入业务系统名称、备注信息、关联IP。



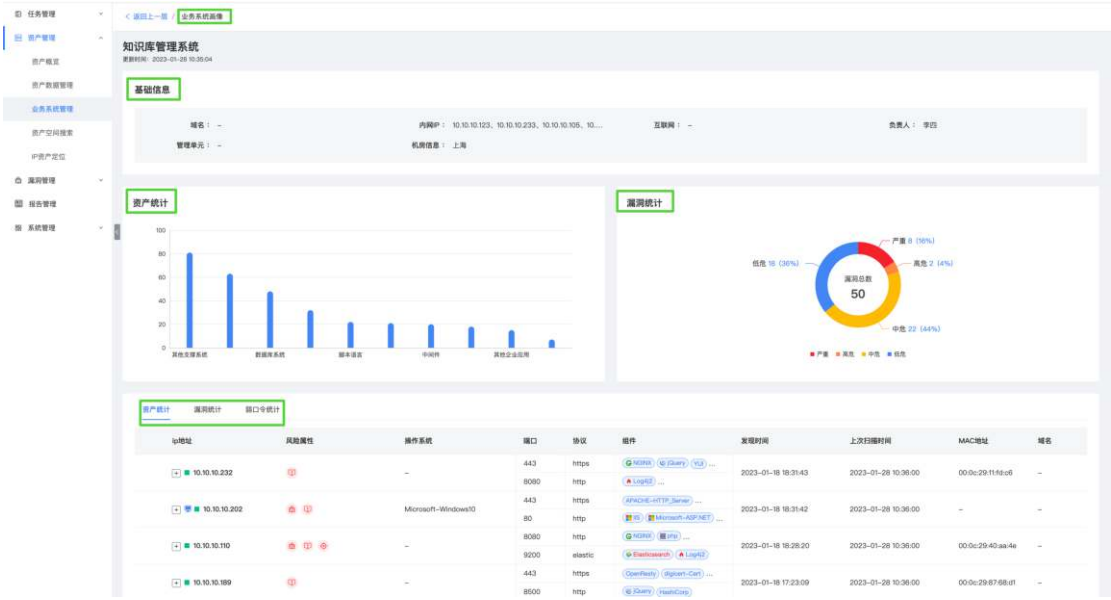
5. 业务系统列表：显示业务系统列表，包含字段为：业务系统名称、备注信息、域名数量、关联 IP 数量、漏洞数量、弱口令数量等信息。



a. 业务系统列表操作：选中某个业务系统可点击编辑、查看、删除按钮进行相关操作。编辑与添加业务操作方式相同；查看可跳转业务系统画像页；删除即删除选中的业务系统。

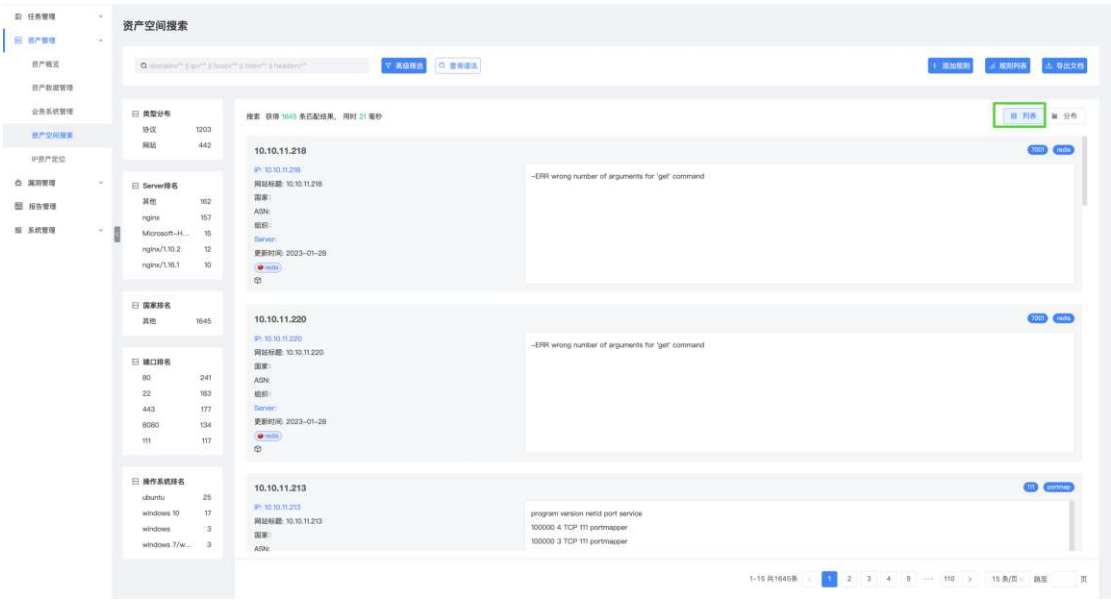


b. 业务系统画像：展示内容为基础信息、资产统计、漏洞统计、弱口令统计等相关信息。



2.2.4 资产空间搜索

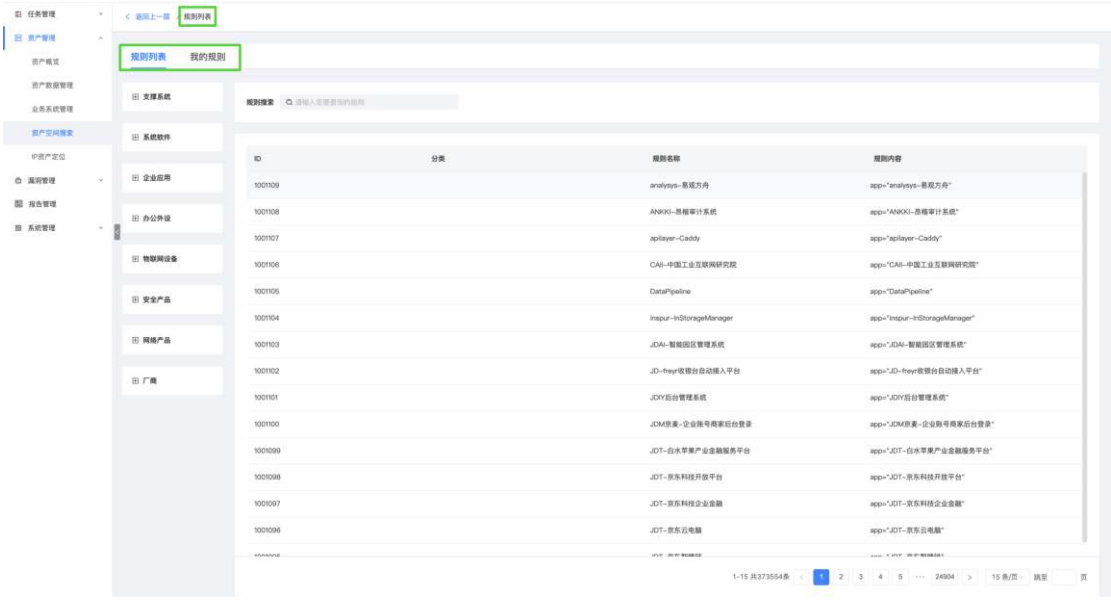
1.【资产管理】-【资产空间搜索】页，分为搜索结果列表视角与搜索结果分布图视角。列表视角如下展示资产（网站+协议）数据，包括 IP、网站标题、国家、ASN、组织、Server、扫描时间、端口、网站信息等；搜索结果分布图视角，以图形化更直观展示不同的分布情况。



2. 支持搜索，高级筛选，包括 IP 地址、端口、服务、操作系统、域名等。

3. 支持查看查询语法

4. 规则列表：点击“规则列表”按钮，跳转规则列表页，页面包含规则列表、我的规则，可分别点击查看。



a. 规则列表：默认展示系统预置的规则，列表字段包括：ID、分类、规则名称、规则内容。 ；支持输入搜索，支持筛选。

b. 我的规则：为用户添加的规则，支持输入搜索；支持添加规则；展示添加的规则列表，列表字段为；ID、分类、分层、规则名称、规则内容等信

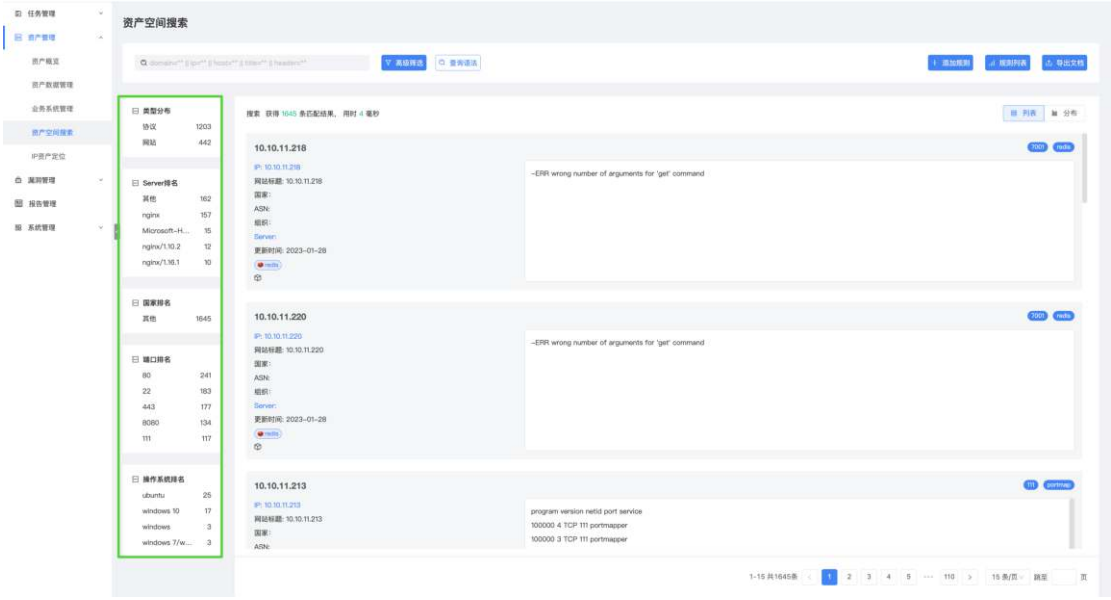
息；支持对添加的规则进行编辑、删除等操作。

5. 添加规则：点击“添加规则”按钮，所需选写信息为：分类、规则内容、厂商名称、规则名称、应用网站、分层，点击“保存”按钮。

6. 规则列表：点击查看系统预置规则。

7. 支持导出文档，导出 json 格式文档。

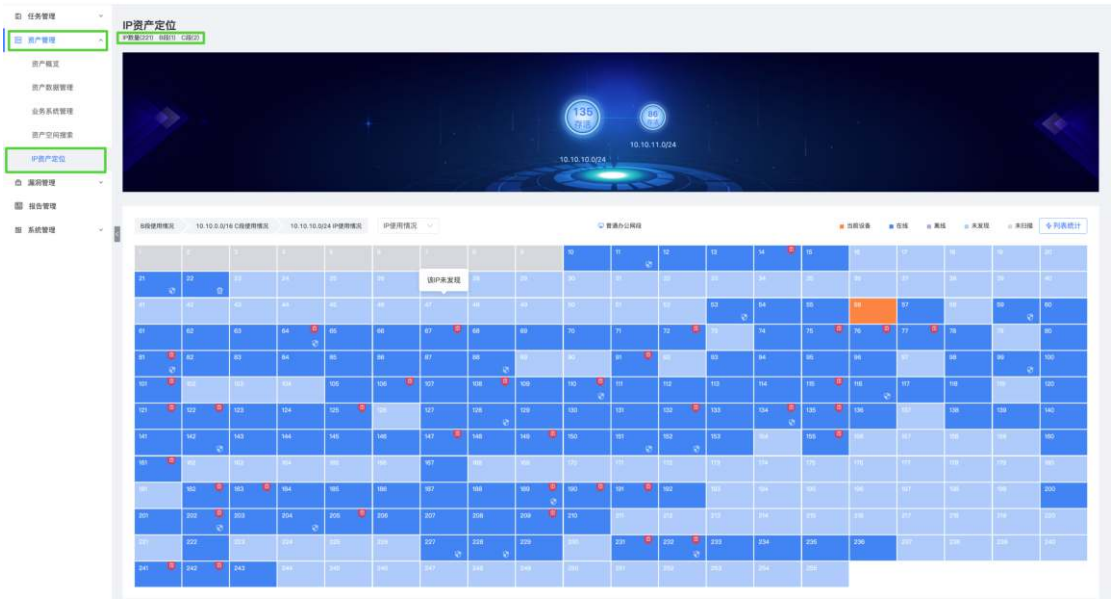
8. 资产空间统计栏：信息统计栏显示当前资产范围的数据统计信息，可以对含有子类的数据项展开或收起，默认展开一级子类。包含数据内容如下：特征资产聚类、类型分布、Server 排名、国家排名、端口排名、操作系统排名。组件分类列表：包含以及和二级分类。所有列表均按照数量进行排序，数量多的排在上面，用户在资产列表进行查询或高级筛选后信息统计栏中的数据会进行更新。



9. 资产详情：点击单个 IP，支持跳转到网站详情页面，查看网站信息。

2.2.5 IP 资产定位

1.【资产管理】-【IP 资产定位】页，展示 IP 定位信息，标题栏显示“IP 数量”、“B 段数量”、“C 段数量”。

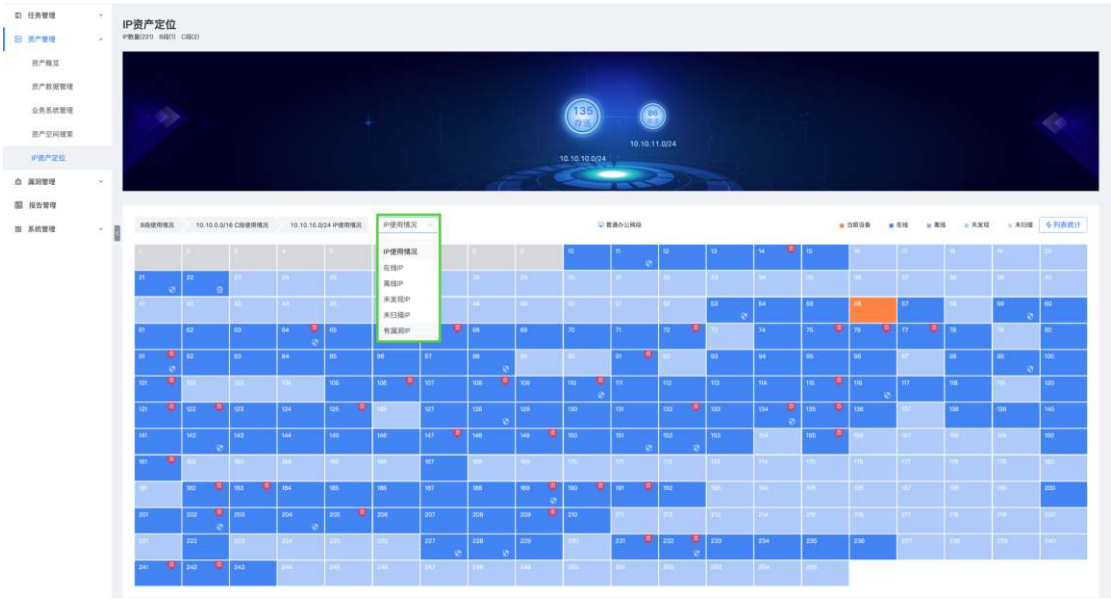


2. IP 资产定位有 IP 矩阵图统计视角和列表统计视角，如下图为 IP 矩阵图视角，点击 IP 段示意图标，可查看该 IP 段的全部信息。

a. 导航栏查看，点击“B 段使用情况”，可查看所有 B 段 IP 详情

b. 导航栏查看，点击“XXXIPC 段使用情况”，可查看所有 C 段 IP 详情

c. 筛选不同 IP 状态：包含 IP 使用情况、在线 IP、离线 IP、未发现 IP、未扫描 IP、有漏洞 IP

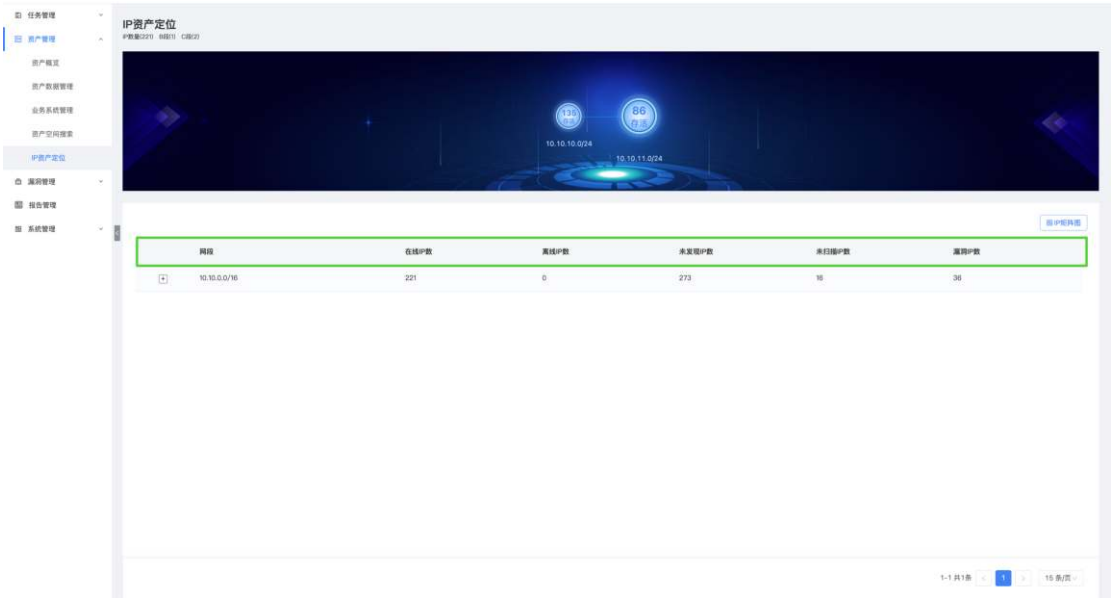


d. IP 状态示意图标，包括当前设备、在线、离线、未发现、未扫描。IP 矩阵图中每个 IP 矩形颜色与示意图标颜色相对应。

e. 查看 IP 矩形详情，点击 IP 矩形跳转到 IP 画像页，查看 IP 详情。

3. 列表统计视角，列表字段包含：网段、在线 IP 数、离线 IP 数、未发

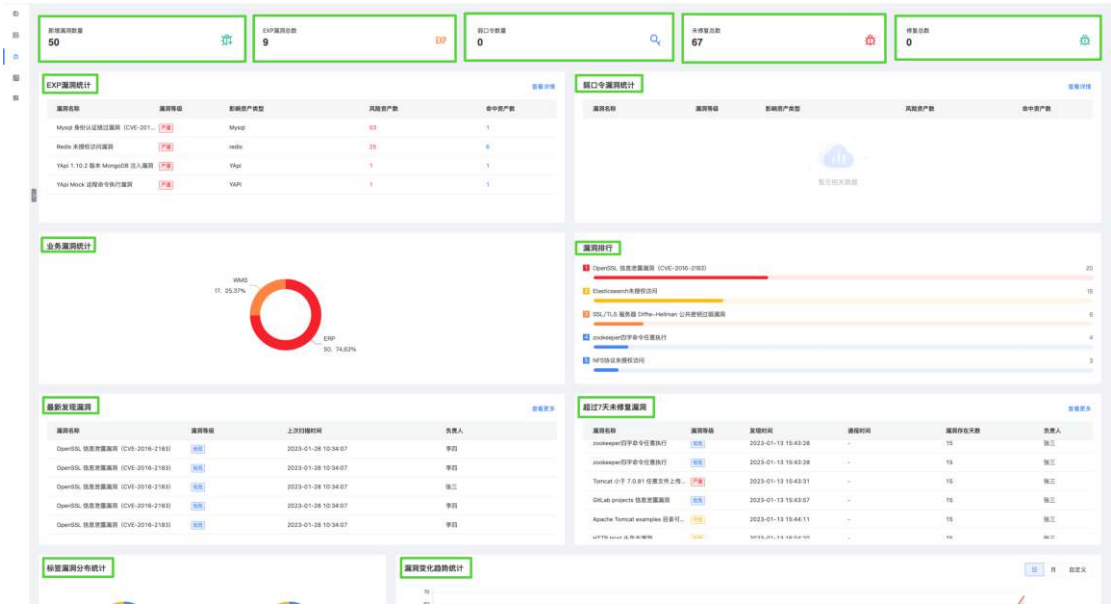
现 IP 数、未扫描 IP 数、漏洞 IP 数。网段信息可展开查看详细 IP 地址



2.3 漏洞管理

2.3.1 漏洞概览

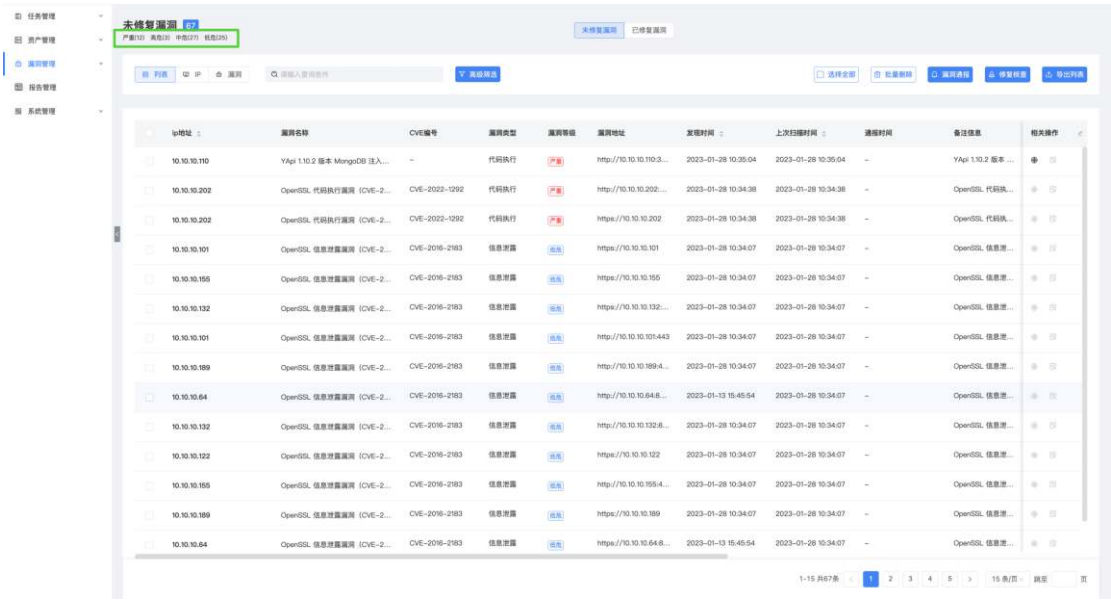
1.【漏洞管理】-【漏洞概览】页，展示“新增漏洞数量”、“EXP 漏洞数量”、“弱口令数量”、“未修复总数”、“修复总数”以及“EXP 漏洞统计”、“弱口令漏洞统计”、“业务漏洞统计”、“漏洞排行”、“新发现漏洞”、“超过 7 天未修复漏洞”、“标签漏洞分布统计”、“漏洞变化趋势统计”等信息概览。



2.3.2 漏洞管理

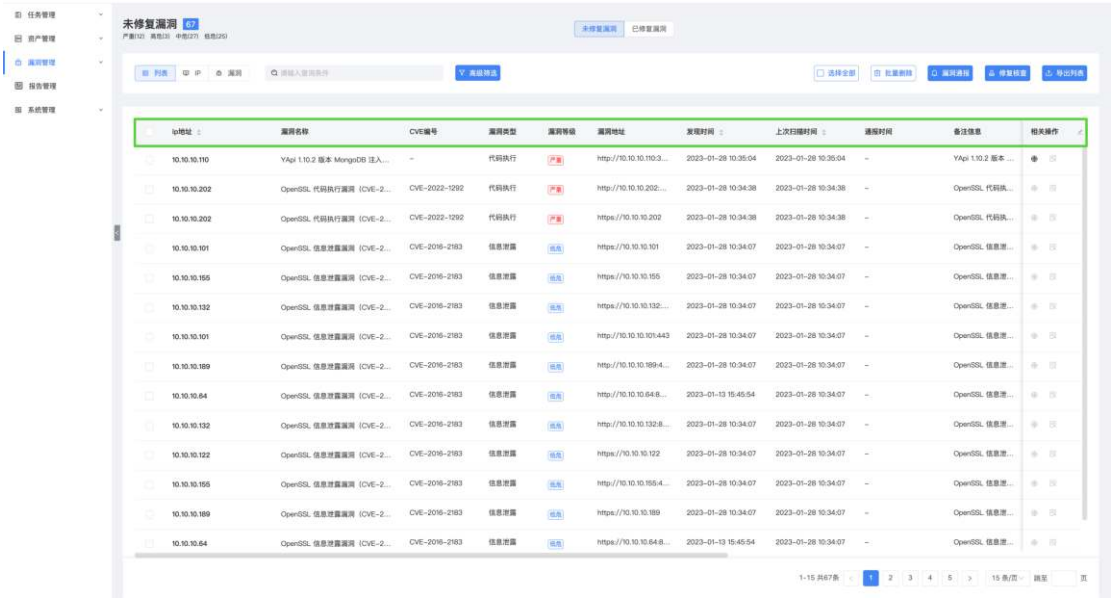
2.3.2.1 未修复漏洞

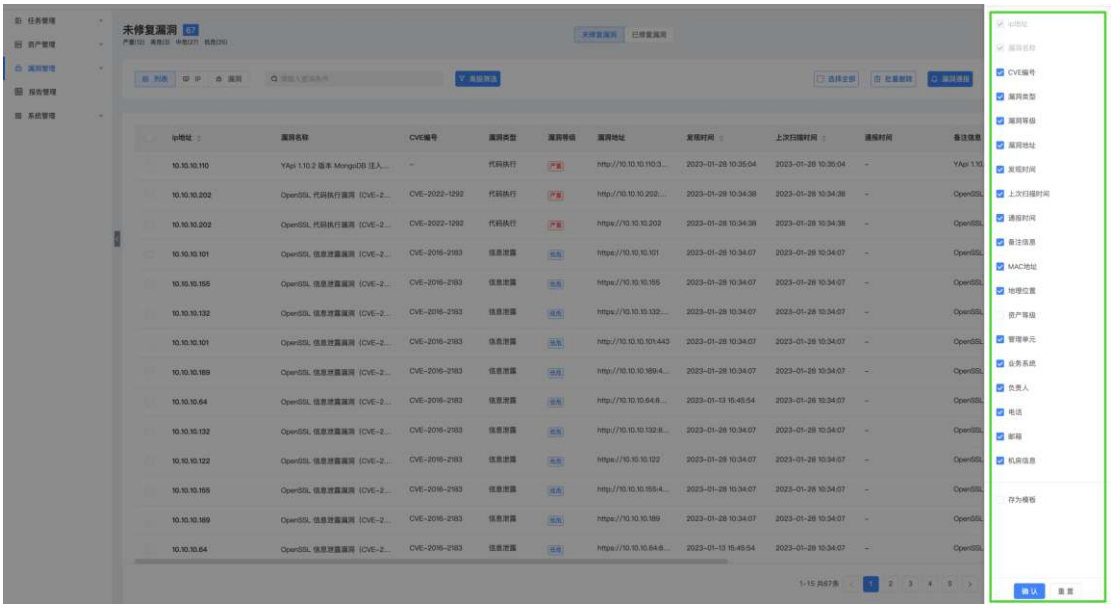
1.【漏洞管理】-【未修复漏洞】页，展示未修复漏洞信息，标题栏显示未修复漏洞分类及数量，具体分为“严重漏洞数量”、“高危漏洞数量”、“中危漏洞数量”、“低危漏洞数量”。



2.【漏洞管理】-【漏洞管理】-【未修复漏洞】页，包括列表维度、IP 维度、漏洞维度 3 个视角；列表维度展示了已扫描到结果的 IP 地址、漏洞名

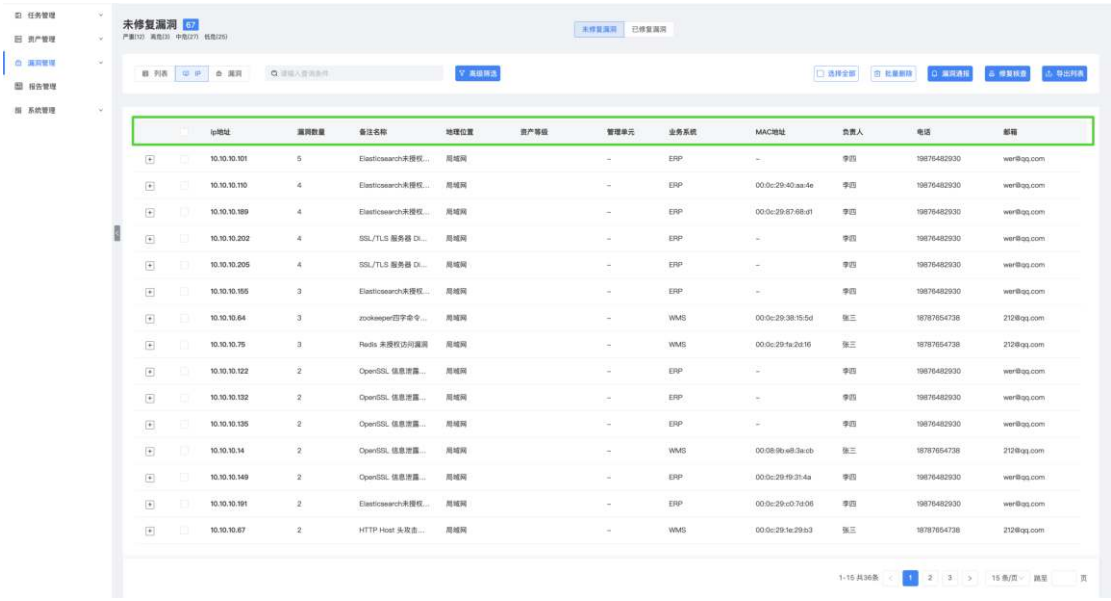
称、CVE 编号、漏洞类型、漏洞等级、漏洞地址、发现时间、上次扫描时间、通报时间、备注信息、MAC 地址、地理位置、资产等级、管理单元、业务系统、负责人、电话、邮箱、机房信息、标签信息等内容，列表字段可自定义配置。



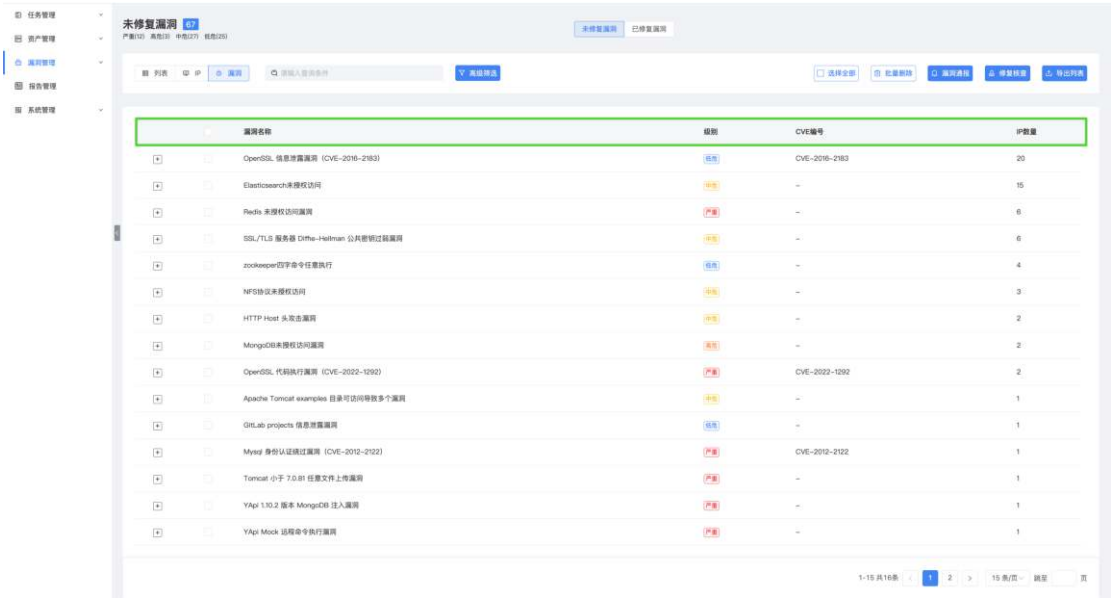


列表相关操作：在列表选中一条漏洞可查看漏洞响应结果。

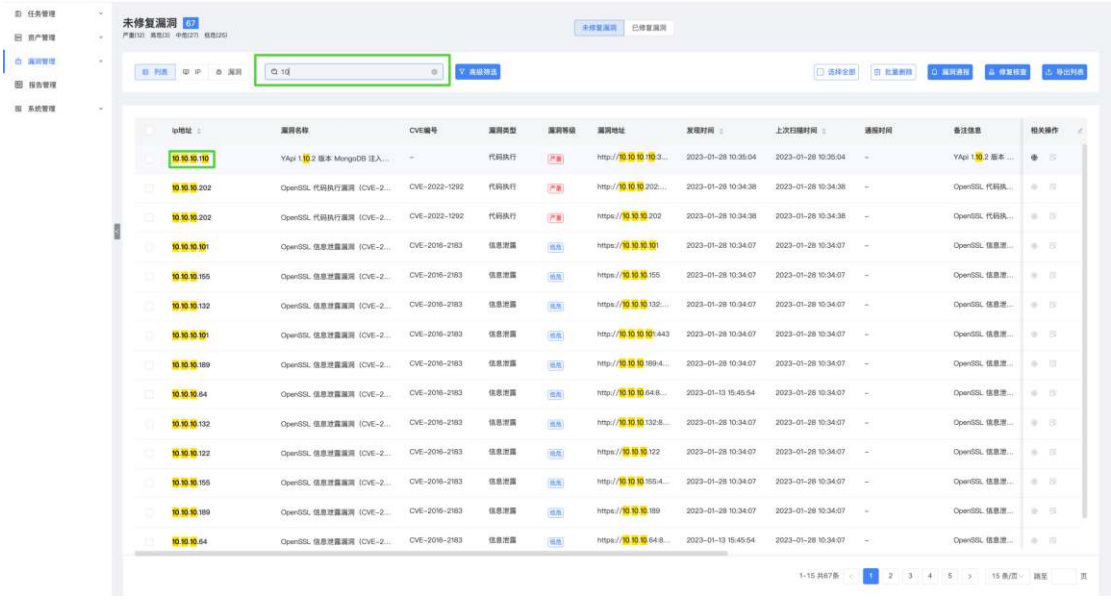
3. IP 维度以 IP 为视角展示了该 IP 下检测的所有漏洞信息，列表字段包括 IP 地址、漏洞数量、备注名称、地理位置、资产等级、管理单元、业务系统、MAC 地址、负责人、电话、邮箱。

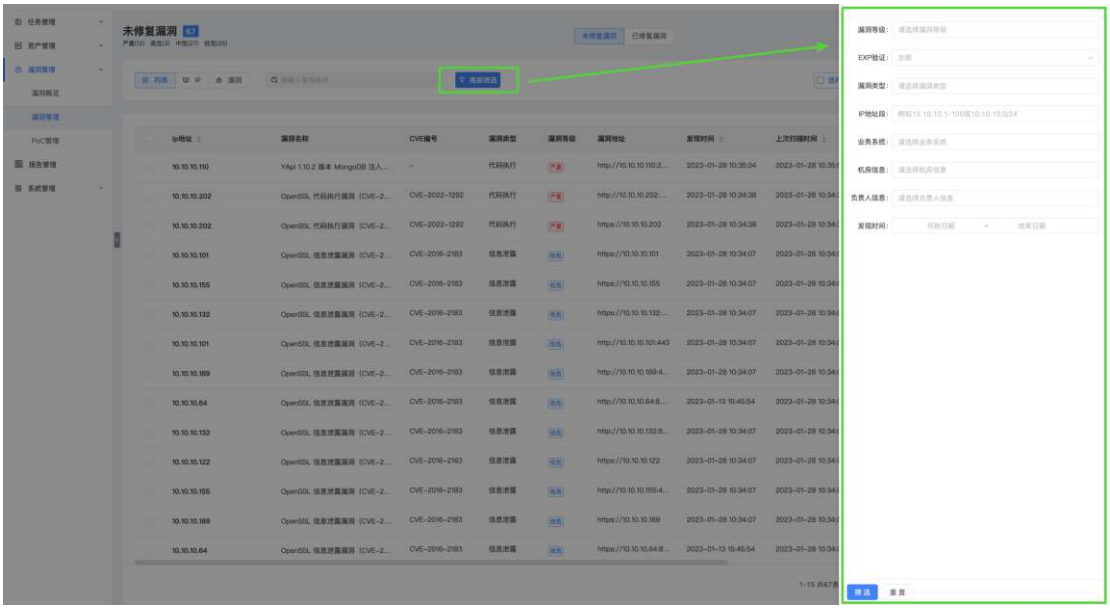


4. 漏洞维度以漏洞为视角，展示了漏洞名称、漏洞级别、CVE 编号、IP 数量；支持点击漏洞名称展开查看漏洞下的所属 IP 信息，包括 IP 地址、漏洞地址、发现时间、备注名称、地理位置、资产等级、管理单元、业务系统、MAC 地址、负责人、电话、邮箱等信息。

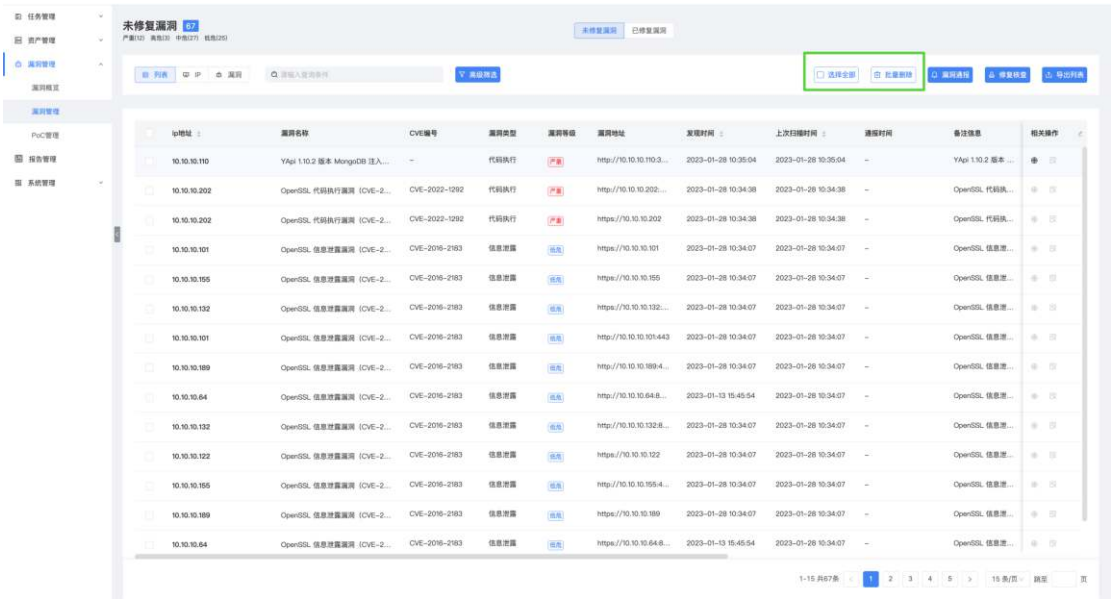


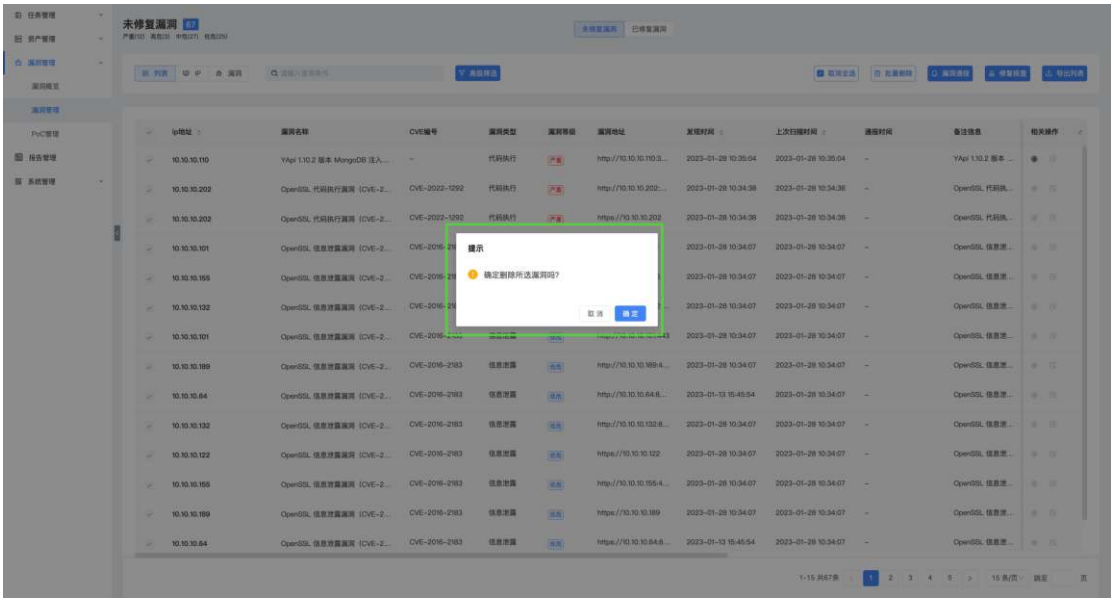
5. 支持未修复漏洞关键字搜索以及“高级筛选”内容为：漏洞等级、EXP 验证、漏洞类型、IP 地址段、资产等级、管理单元、业务系统、机房信息、负责人信息、标签信息、时间段等。





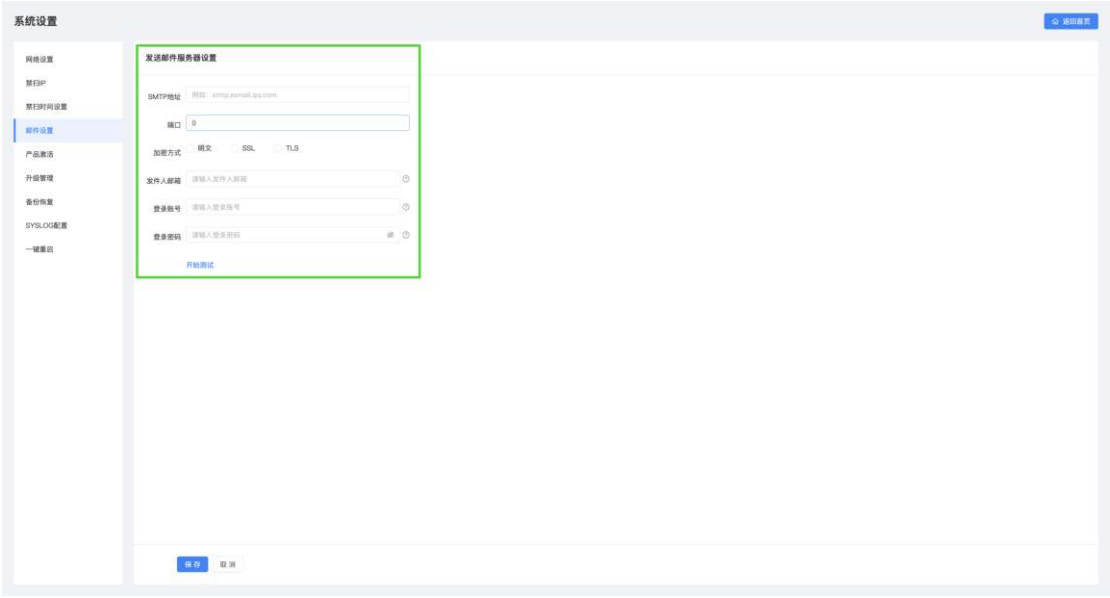
6. 支持全选功能，对当前列表中的全部数据进行全选，选择后可以进行删除。

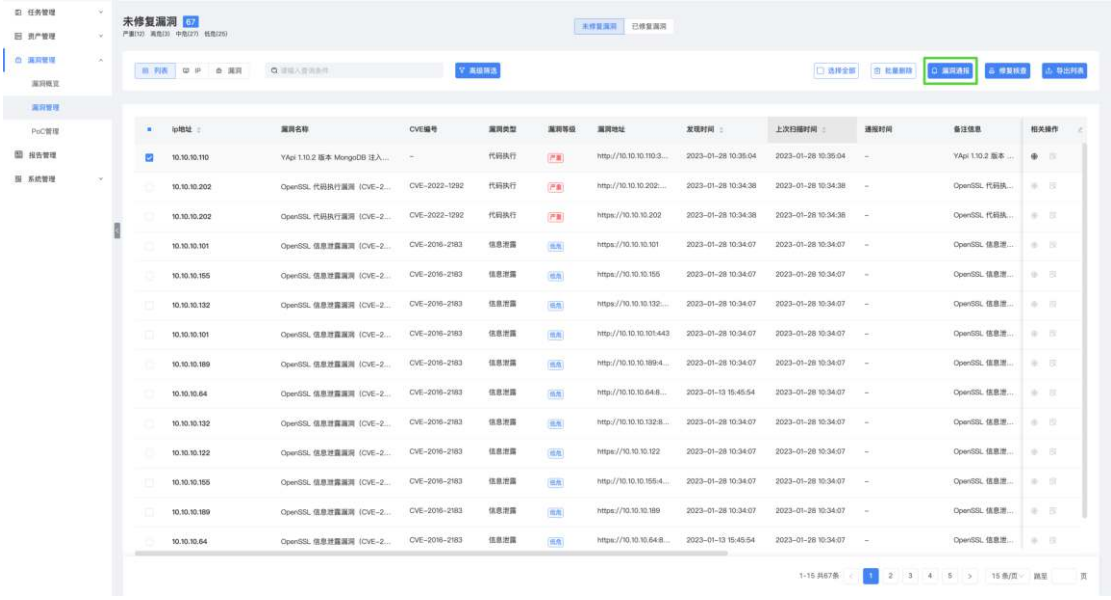


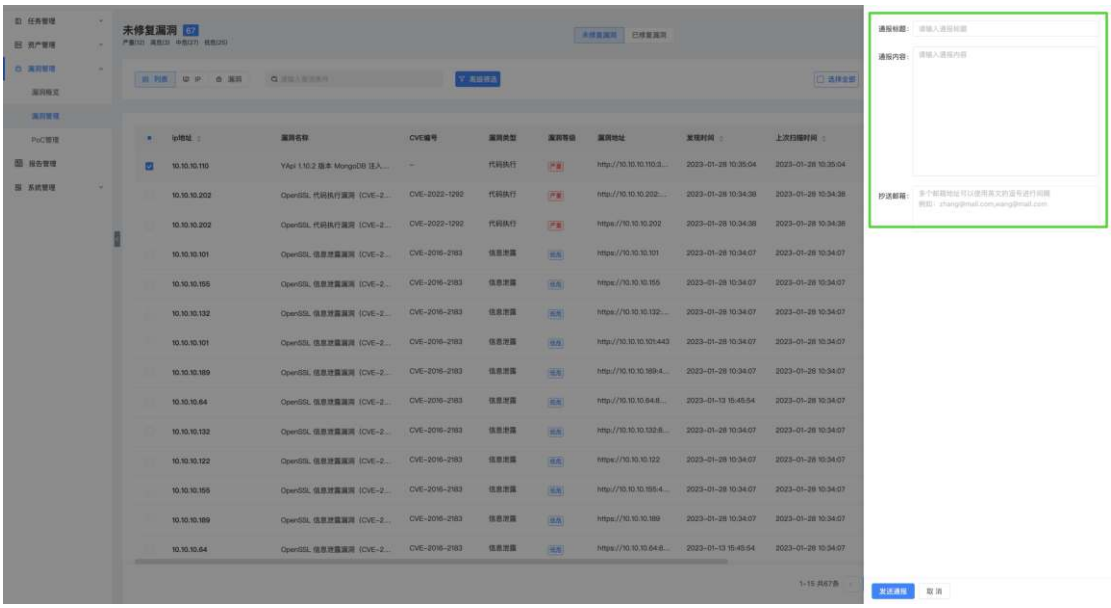


7. 支持未修复漏洞“漏洞通报”功能，可将结果通过邮件发送至负责人邮箱。系统右上角【邮件设置】填入接收方邮件的“SMTP 地址”、“端口”、“发送邮箱”、“登录密码”信息后点击【开始测试】按钮，如接收到邮件，则证明功能可用。

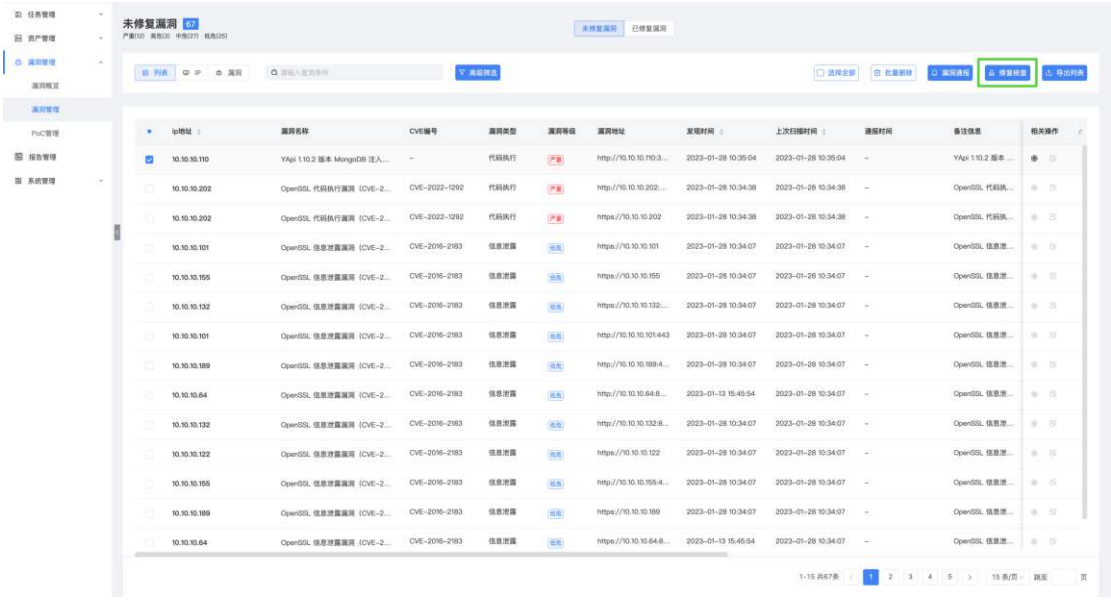
【漏洞管理】-【未修复漏洞】-选择要通报的内容-【漏洞通报】填入“通报标题”、“通报内容”、“抄送邮箱”后，点击【发送通报】按钮。

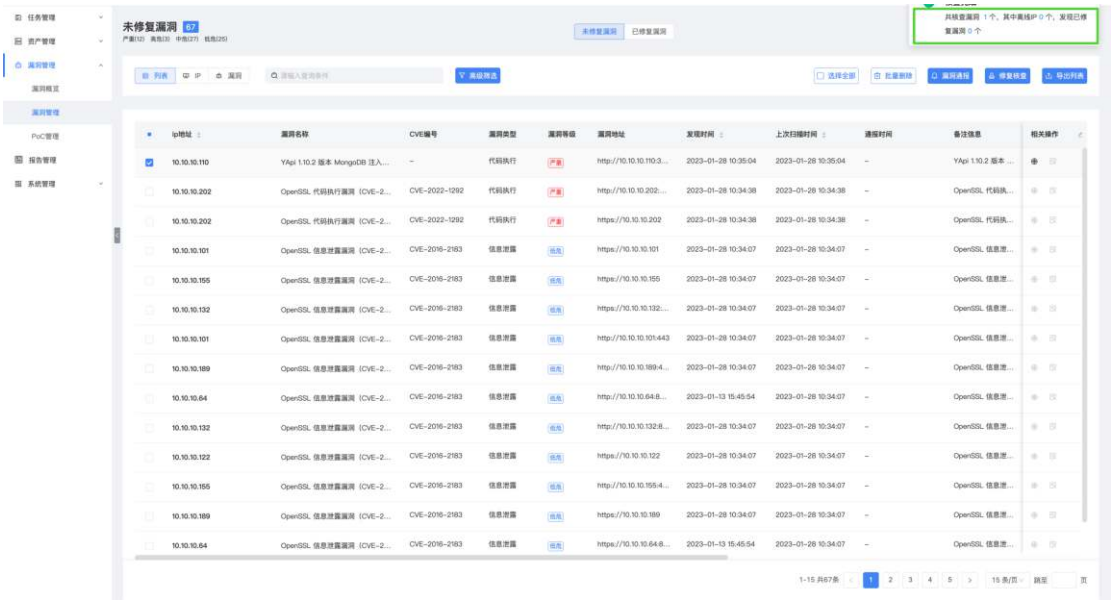

系统设置
发送邮件服务器设置
SMTP地址
端口
加密方式
发件人邮箱
登录账号
登录密码
开始测试
保存


未修复漏洞
已修复漏洞
漏洞通报
修复核查
导出列表



8. 修复核查：点击“修复核查”按钮，系统开始对未修复漏洞进行核查，检查是否有修复，核查完成后有弹窗提示核查的结果。

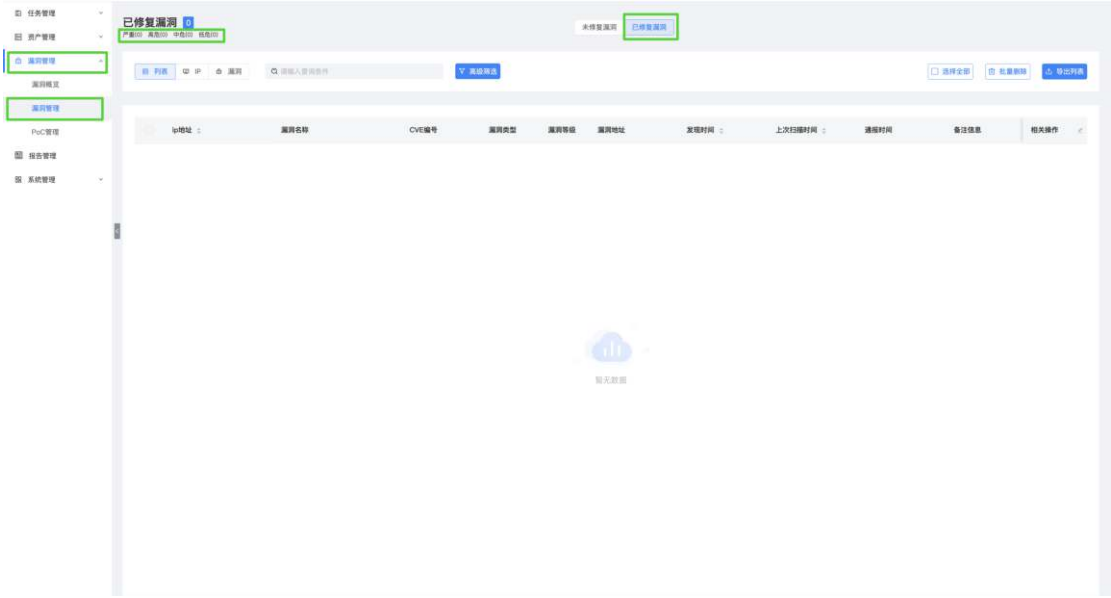




9. 导出列表：支持将未修复的漏洞导出为 Excel 文件

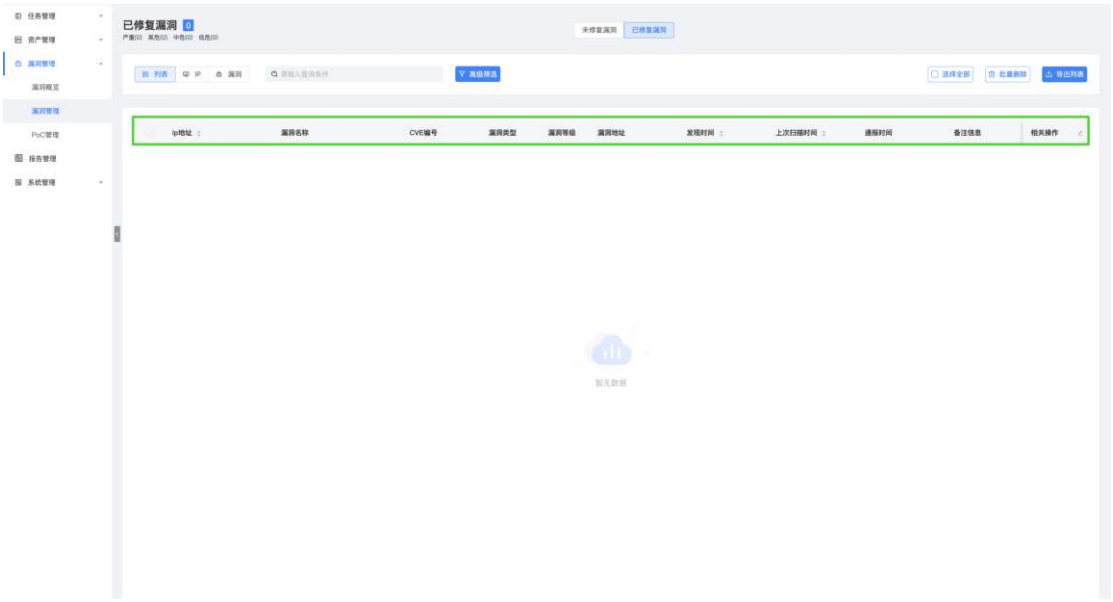
2.3.2.2 已复漏洞

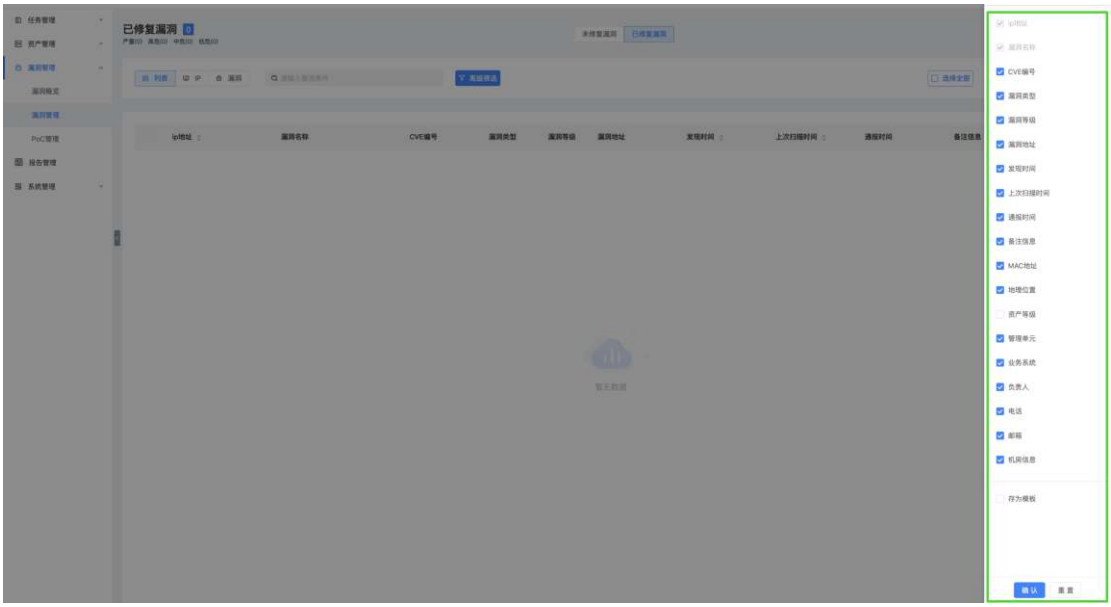
1.【漏洞管理】-【漏洞管理】-【已修复漏洞】页，展示已修复漏洞信息，标题栏显示已修复漏洞分类及数量，具体分为“严重漏洞数量”、“高危漏洞数量”、“中危漏洞数量”、“低危漏洞数量”。



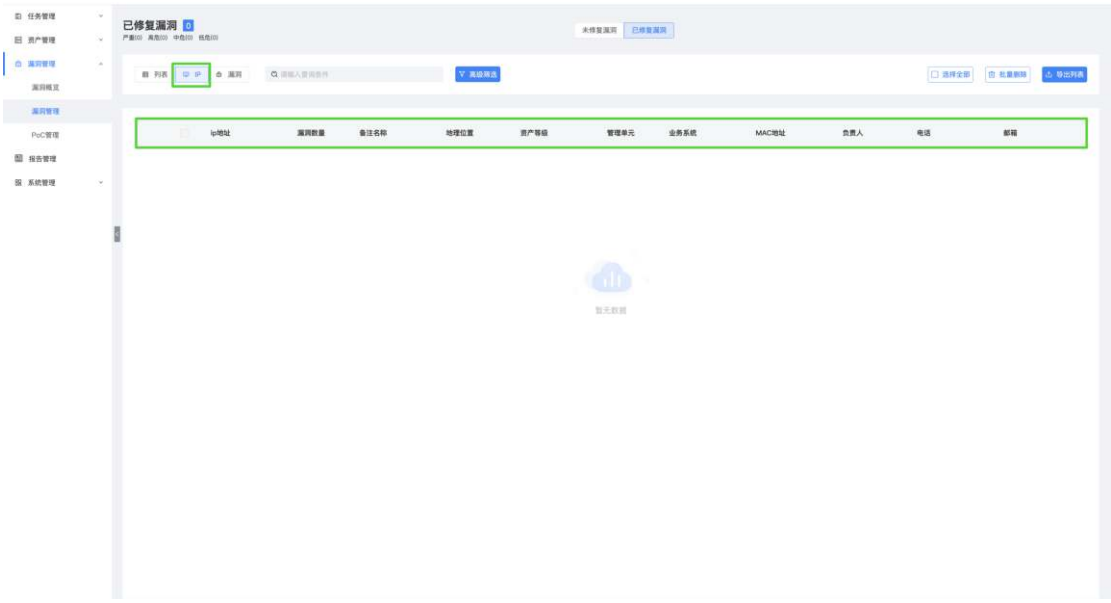
2. 已修复漏洞是再次扫描后修复了的漏洞，包括列表维度、IP 维度、漏洞维度 3 个视角；列表维度展示了 IP 地址、漏洞名称、CVE 编号、漏洞类型、漏洞等级、漏洞地址、发现时间、上次扫描时间、通报时间、备注信

息、MAC 地址、地理位置、资产等级、管理单元、业务系统、负责人、电话、邮箱、机房信息、标签信息等内容，列表字段可自定义配置。

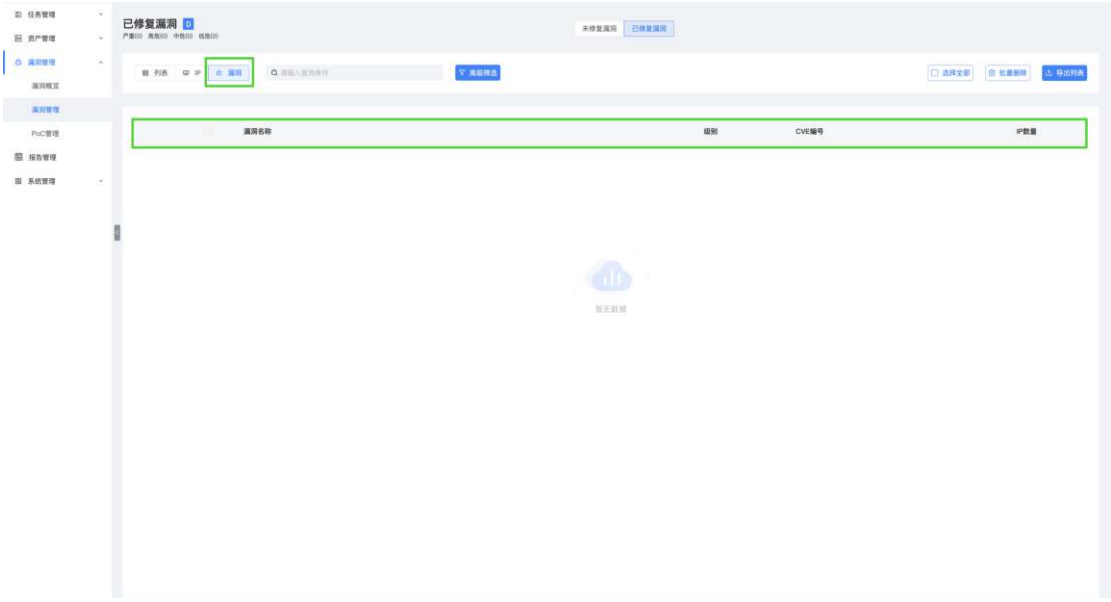




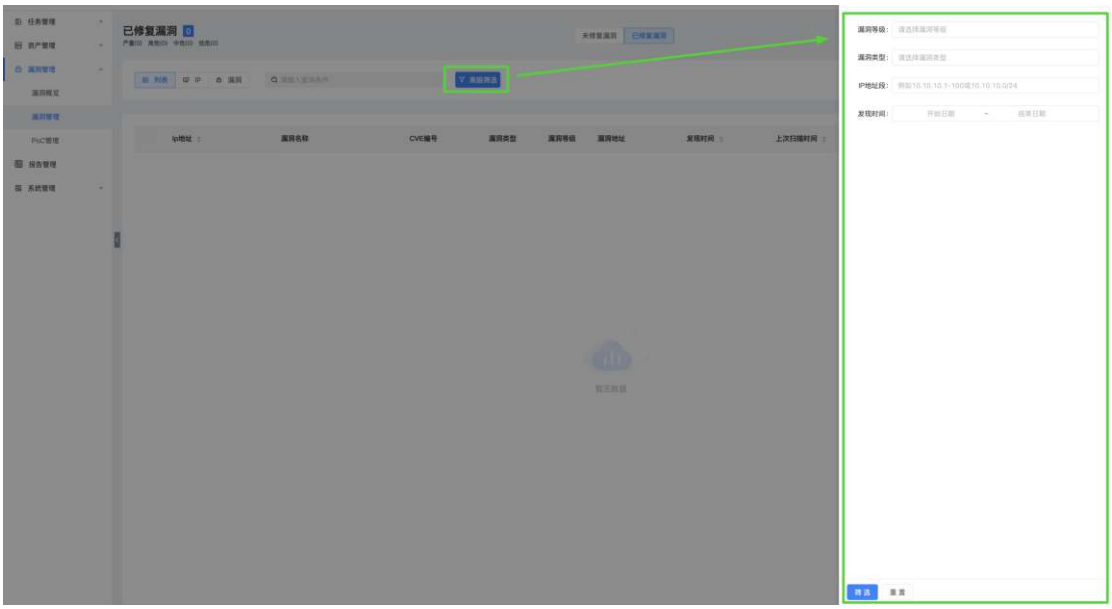
a. IP 维度以 IP 为视角展示了该 IP 下所有已修复漏洞信息，列表字段包括 IP 地址，漏洞数量、备注名称、地理位置、管理单元、业务系统、MAC 地址、负责人、电话、邮箱等信息；支持点击 IP 左侧展开查看 IP 下的所有已修复漏洞信息，包括漏洞名称、漏洞编号、漏洞等级、漏洞地址、时间等信息。



b. 漏洞维度以漏洞为视角展示了漏洞名称、漏洞级别、CVE 编号、IP 数量；支持点击漏洞名称左侧展开查看该漏洞下的所属 IP 信息，包括 IP 名称、地址、发现时间、MAC 地址等信息。



3. 支持已修复漏洞关键字搜索以及“高级筛选”，点击“高级筛选按钮”选择漏洞等级（严重、高危、中危、低危）、漏洞类型，输入 IP 地址段、发现时间等。

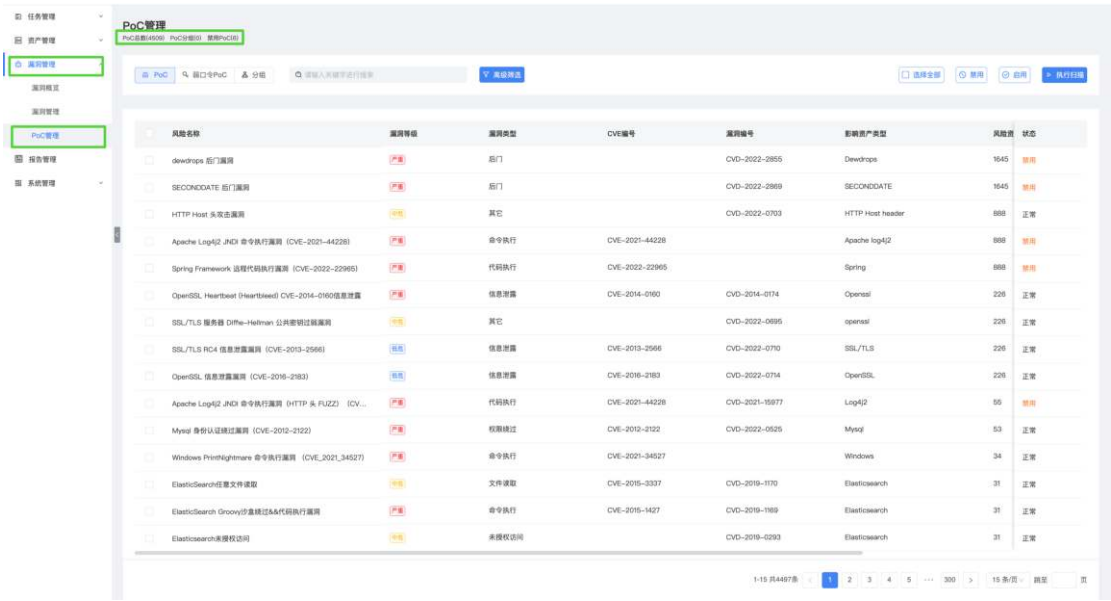


4. 支持全选功能，对当前列表中的全部数据进行全选，选择后可以进行已修复漏洞删除。

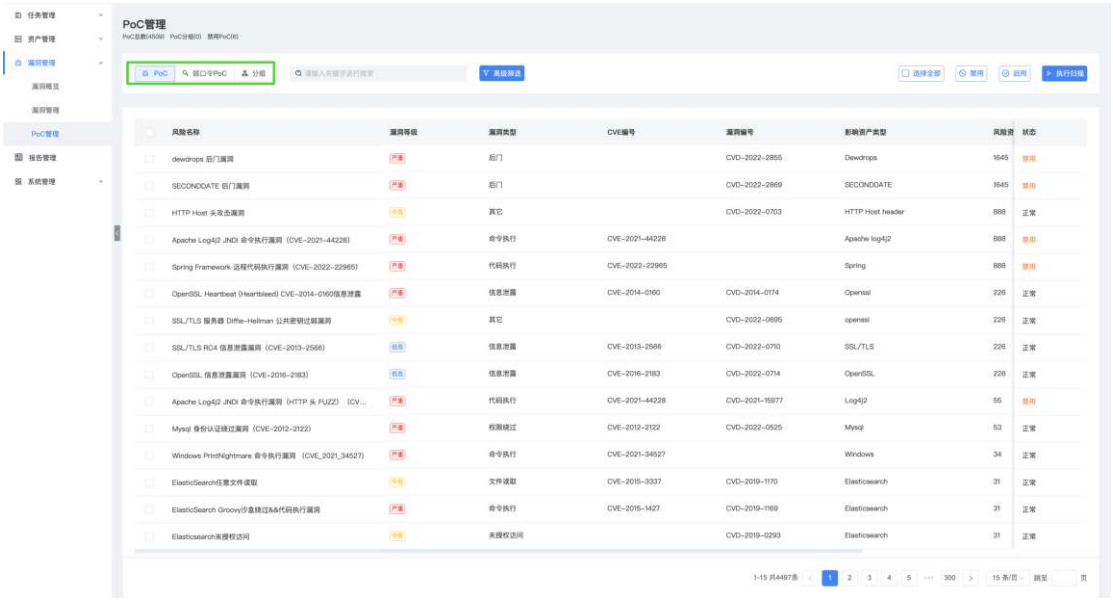
5. 支持已修复漏洞“导出列表”功能。

2.3.3 PoC 管理

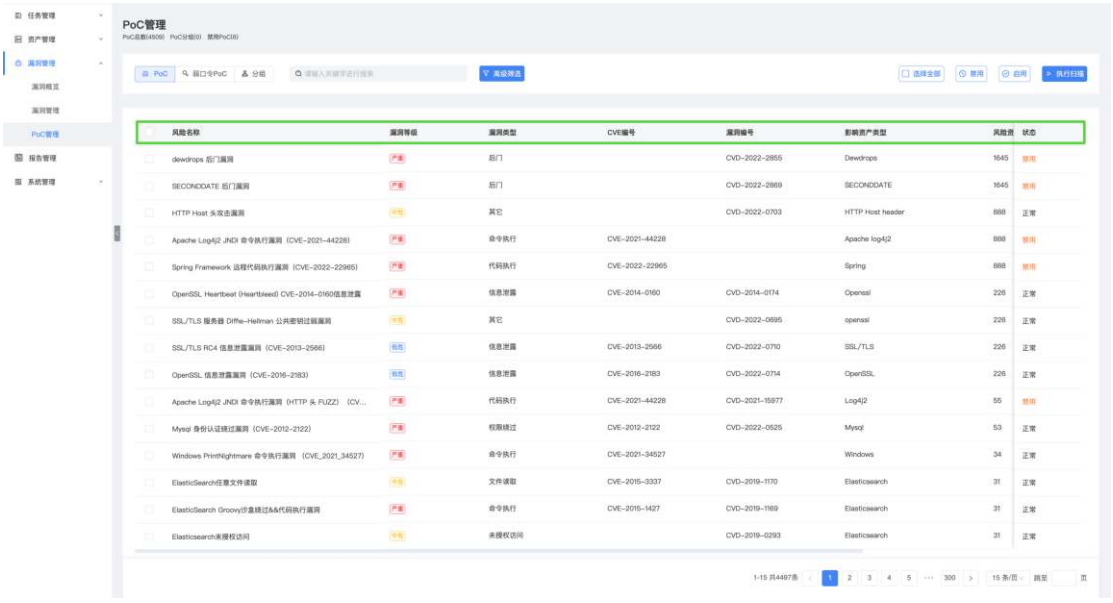
1.【漏洞管理】-【PoC 管理】页，展示 PoC 信息，标题栏显示 PoC 分类详情，具体分为“PoC 总数数量”、“PoC 分组数量”、“禁用 PoC 数量”。



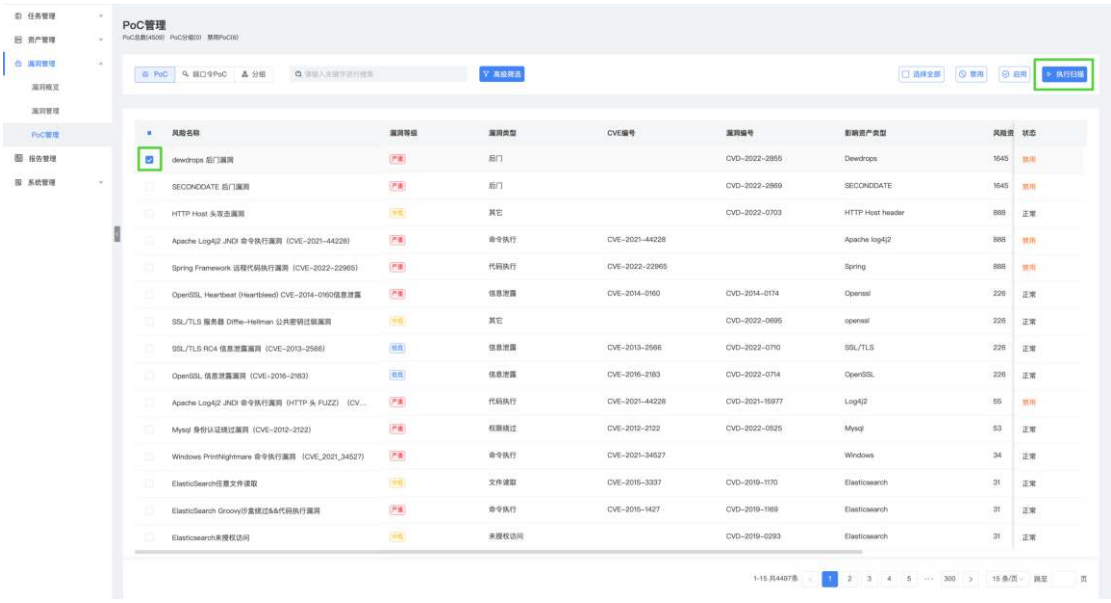
2. PoC 管理分为 PoC 视角、弱口令视角、自定义视角、分组视角。



a. PoC 视角：PoC 视角中，在 PoC 列表展示了“风险名称”、“漏洞等级”、“漏洞类型”、“CVE 编号”、“漏洞编号”、“影响资产类型”、“风险资产数”、“分组”、“更新时间”、“状态”“等信息。

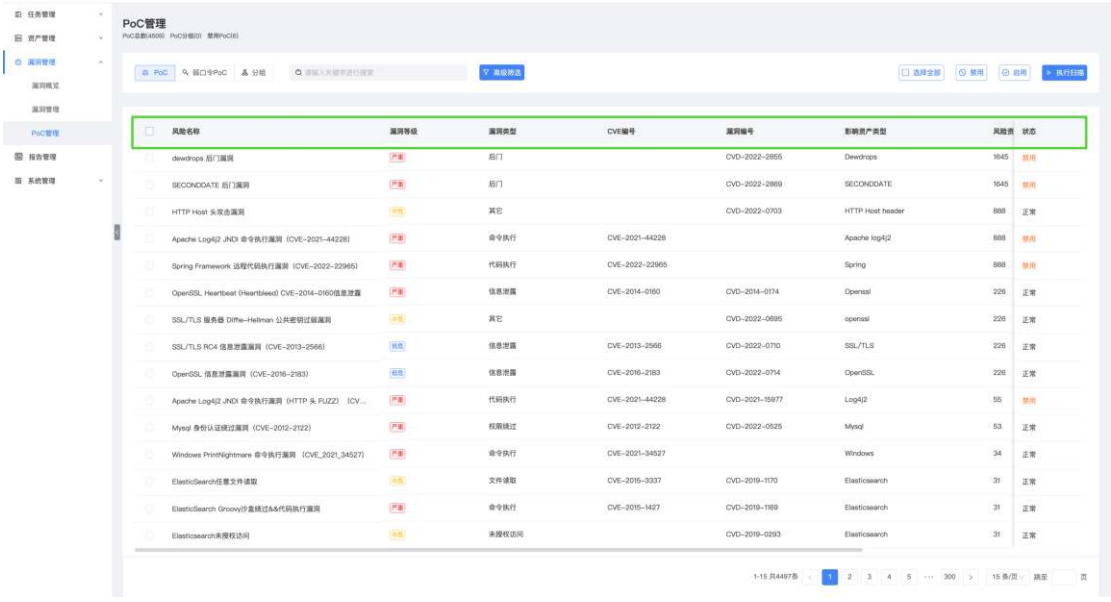


(i) 支持 PoC 视角中，选择想要扫描的漏洞 PoC，点击“执行扫描”按钮，即可启动扫描下发扫描任务；通过 PoC 规则对所有存在对应组件的资产进行扫描，快速识别资产中是否存在某个漏洞。

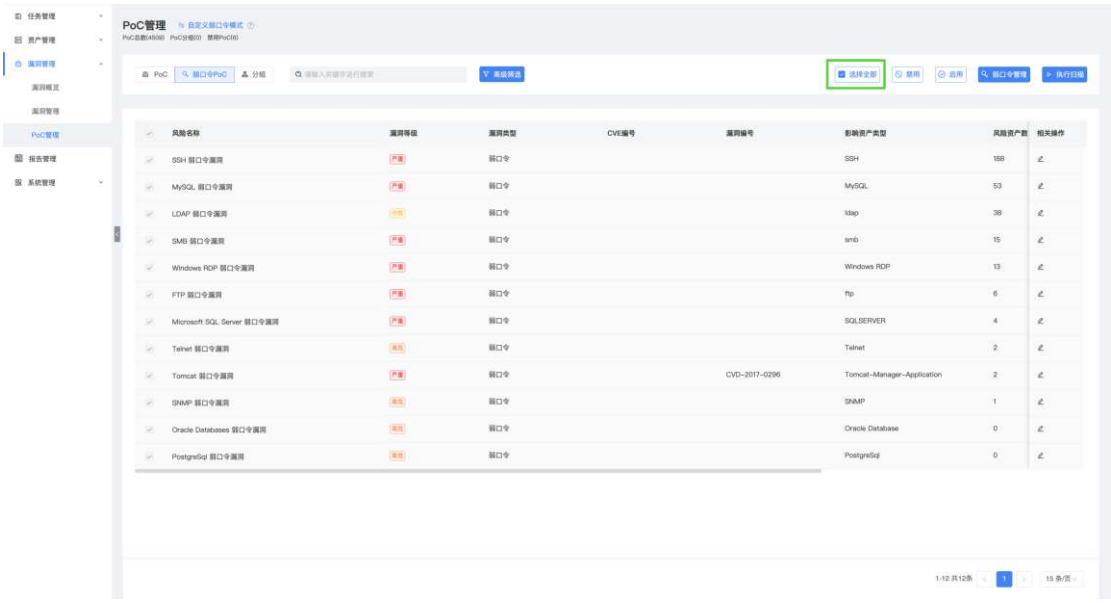


(ii) PoC 视角中，支持禁用/启用（批量禁用/批量启用）PoC，筛选需要禁用/启用的 PoC，并点击“禁用”/“启用”按钮，禁用后下发此扫描任务时，不会扫描该禁用 PoC；启用后下发此扫描任务时候，会扫描该 PoC。

b. 弱口令视角中，列表展示、风险名称、漏洞等级、漏洞类型、CVE 编号、漏洞编号、影响资产类型、风险资产数、分组、更新时间、状态等信息。

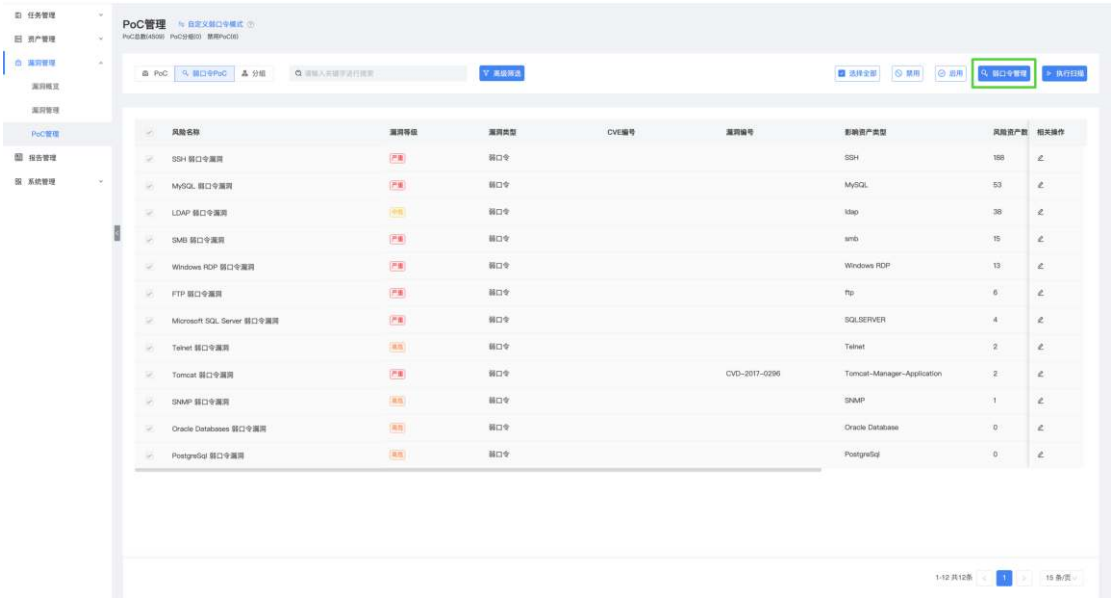


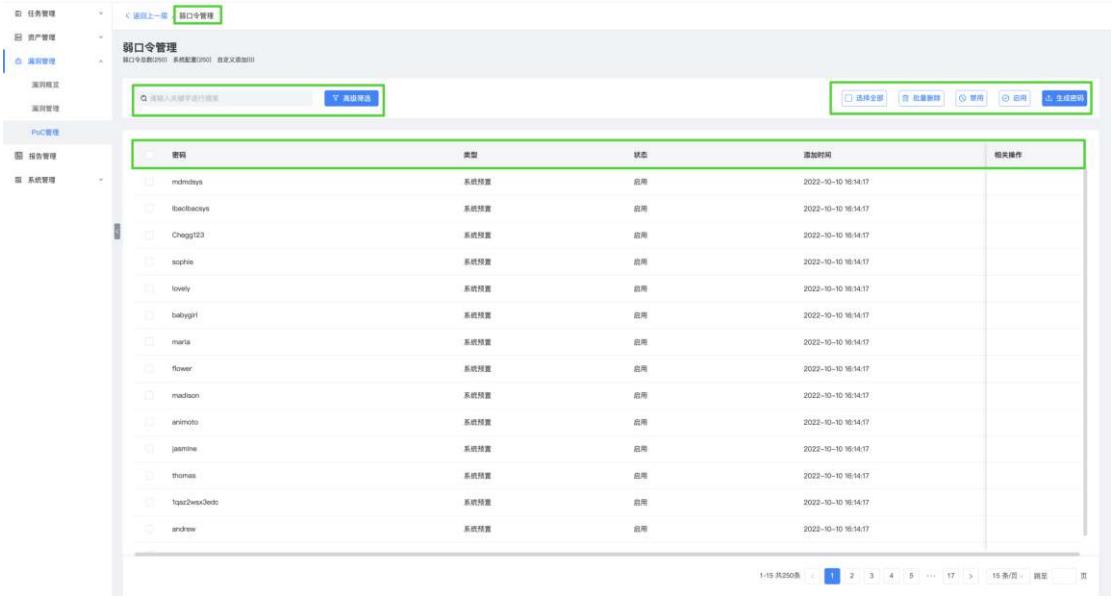
(i) 弱口令视角列表支持全选功能

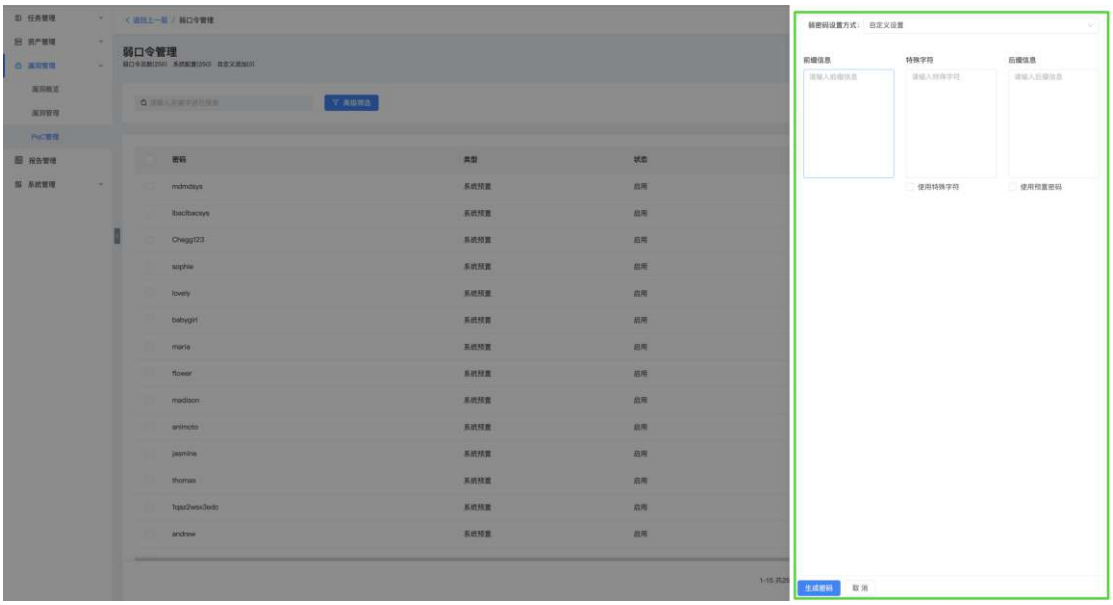


(ii) 弱口令视角列表选中后支持禁用/启用（批量禁用/批量启用），禁用后下发扫描任务时，不会扫描该禁用弱口令；启用后下发扫描任务时，会扫描该弱口令。

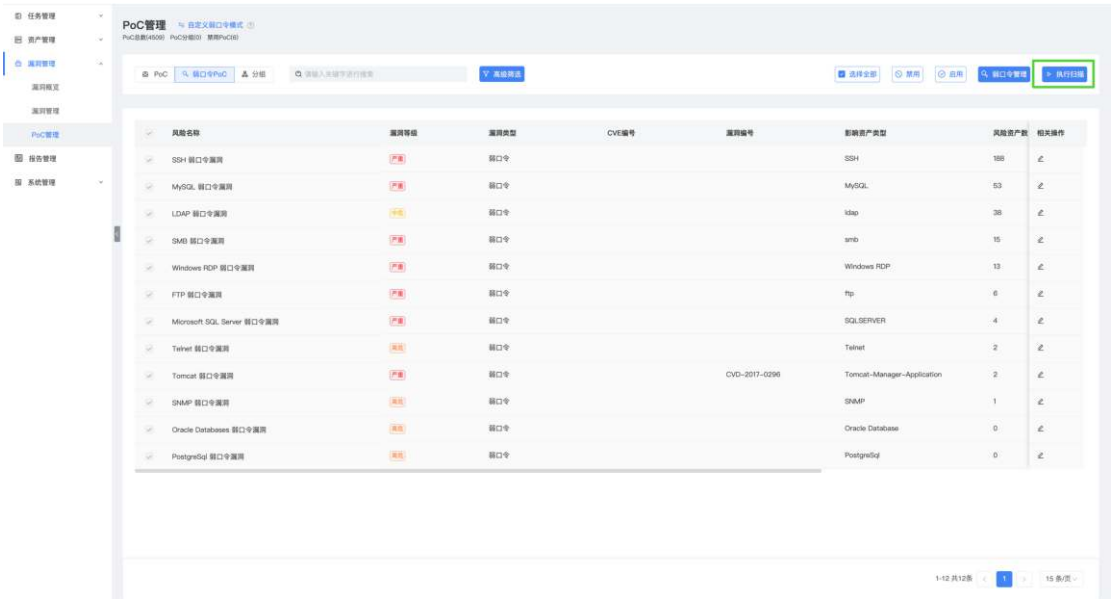
(iii) 弱口令管理：点击“弱口令管理”按钮，进入弱口令管理页；支持搜索，以及根据添加方式、状态进行高级筛选；支撑全选；支撑批量删除（系统预置不可删除）；支持批量禁用；支撑批量启用；支持生成密码，选择弱密码设置方式，填写前缀信息、特殊字符、后缀信息，后点击生成密码。



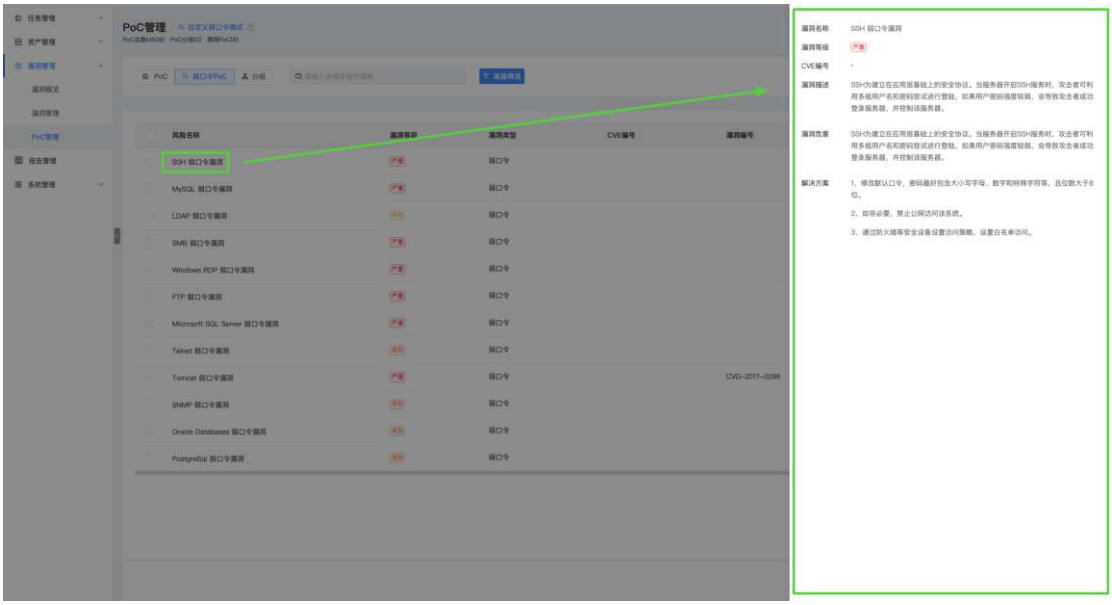




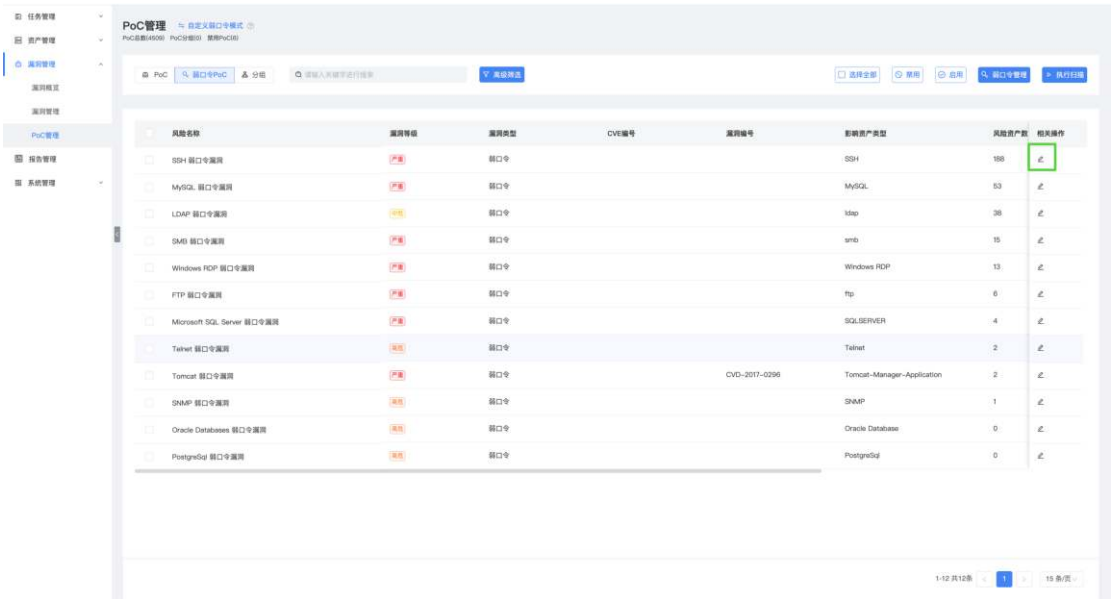
(iv) 弱口令视角中，选择想要扫描的漏洞 PoC，点击“执行扫描”按钮，即可启动扫描下发扫描任务；通过 PoC 规则对所有存在对应组件的资产进行扫描，快速识别资产中是否存在某个漏洞。



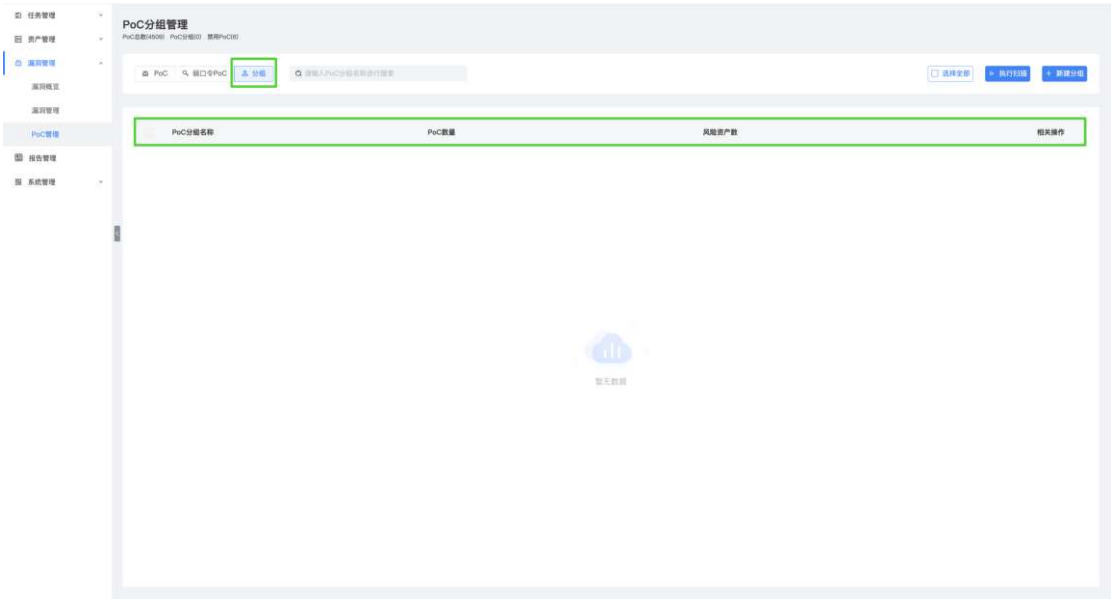
(v) 弱口令视角列表，点击风险名称可查看漏洞详情。



(vi) 弱口令视角列表，可针对部分弱口令进行字典编辑。（例如：SSH 弱口令）



c. PoC 分组视角中，列表展示 PoC 分组名称、PoC 数量、风险资产数等信息。



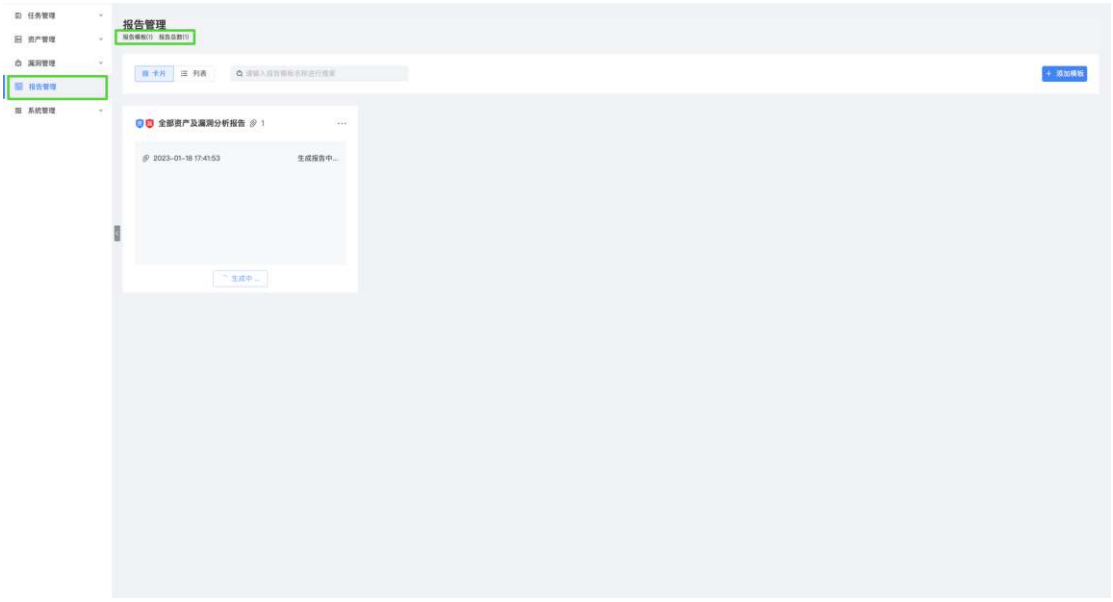
(i) 支持搜索、全选、执行扫描功能

(ii) 支持新建/编辑/删除 PoC 分组，新建/编辑需要填写分组名称、选择 PoC 信息。

2.4 报告管理

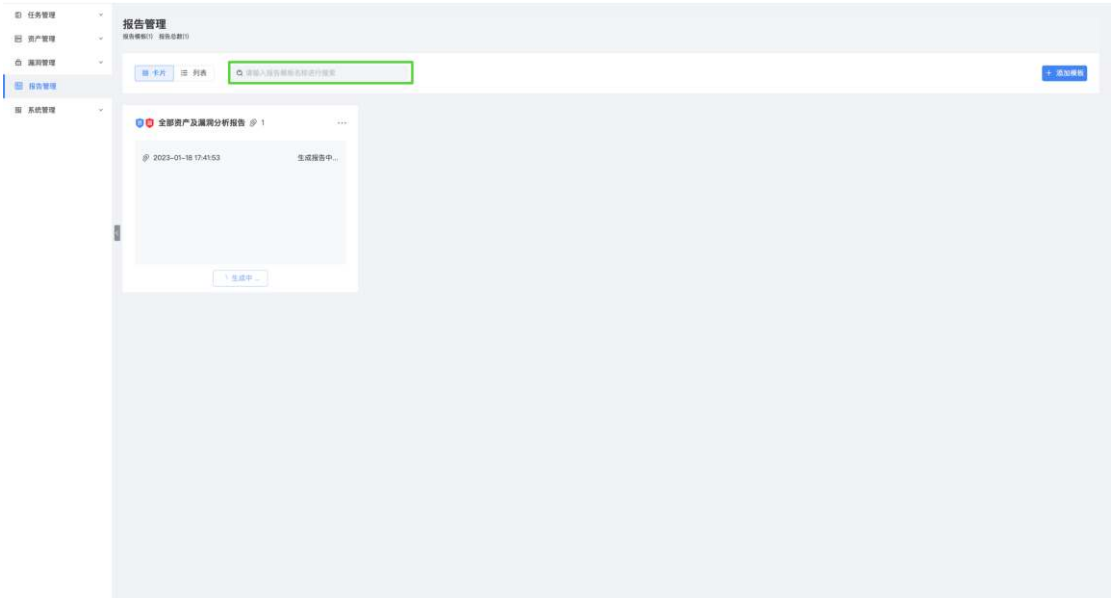
1.【报告管理】页，对识别出来的资产进行多维度统计分析，生成综合报表，提供给管理者查看，可生成 PDF 报告下载，标题栏统计展示“报告模板

数量”、“报告总数”。

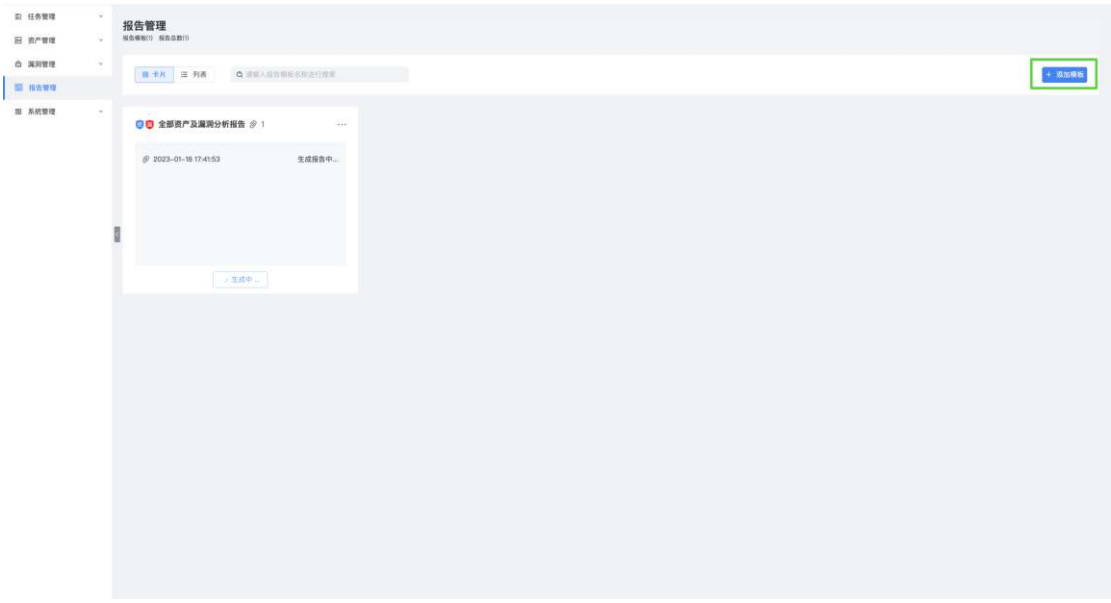


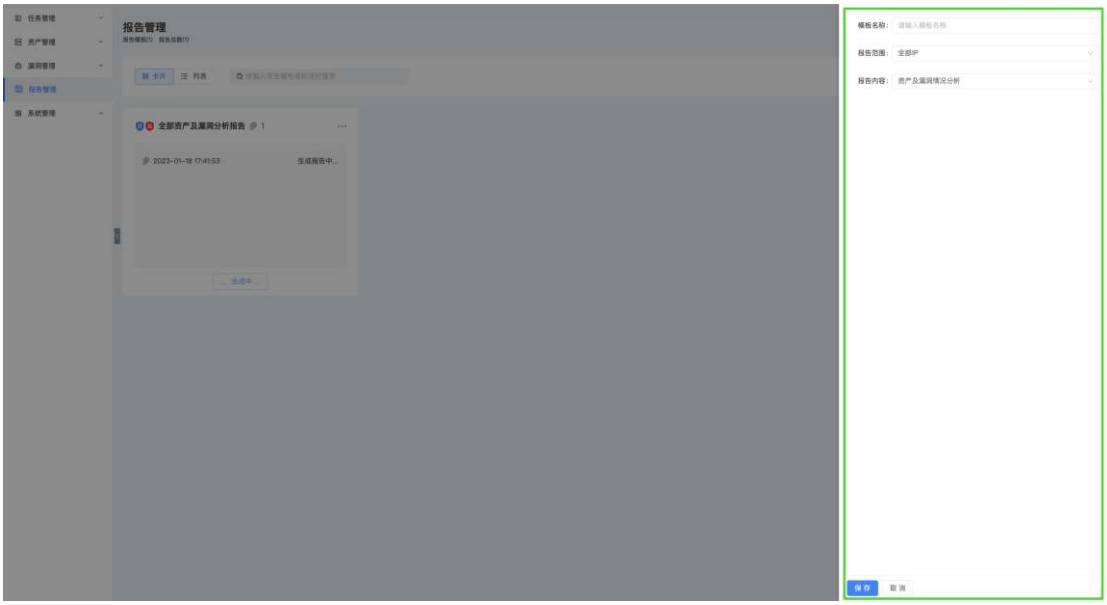
2. 报告管理操作

a. 根据关键字对已新增的报告模板搜索



b. 点击“添加模板”按钮，支撑添加模板功能。

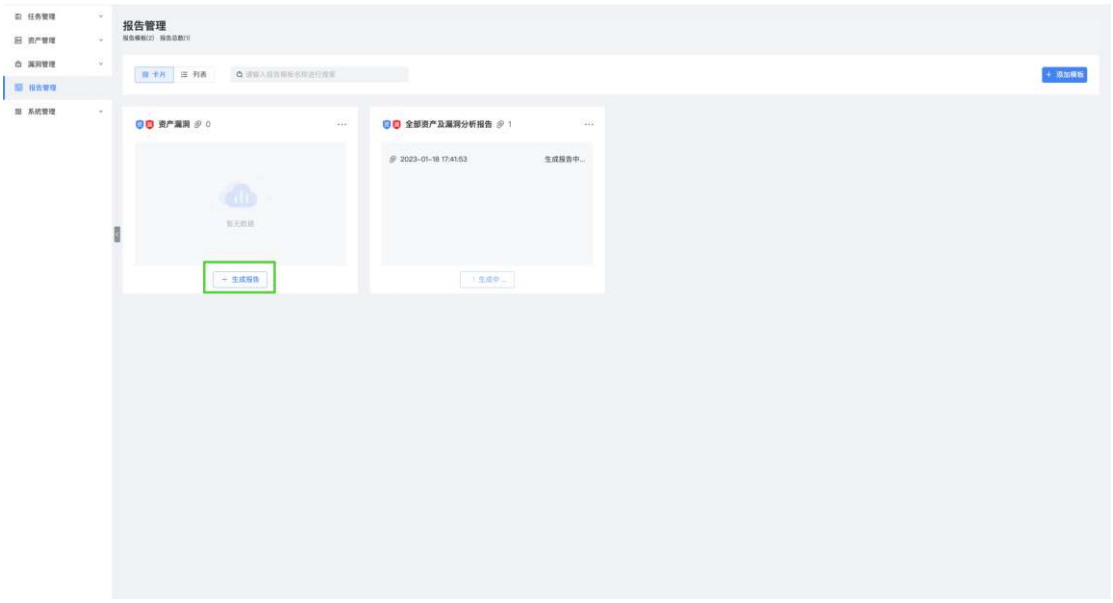




c. 报告模板编辑，点击如图编辑按钮，支持编辑报告名称。

d. 报告模板删除，点击如图删除按钮，支持删除报告模板。

e. 生成报告，点击如图生成按钮，支持根据该模板生成报告。



f. 查看报表，点击如图查看按钮，支持查看该报告。

g. 下载报告，点击如图下载按钮，支持下载该报告，包括 PDF、HTML 两种格式。

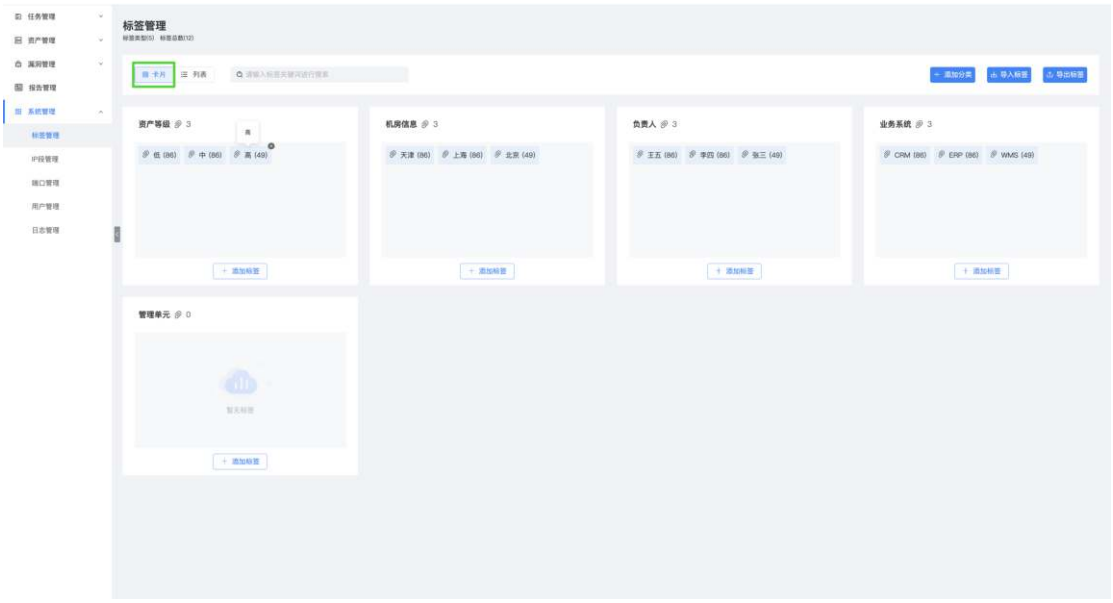
h. 删除报告，点击如图删除按钮，支持删除该报告。

2.5 系统管理

2.5.1 标签管理

2.5.1.1 标签管理列表

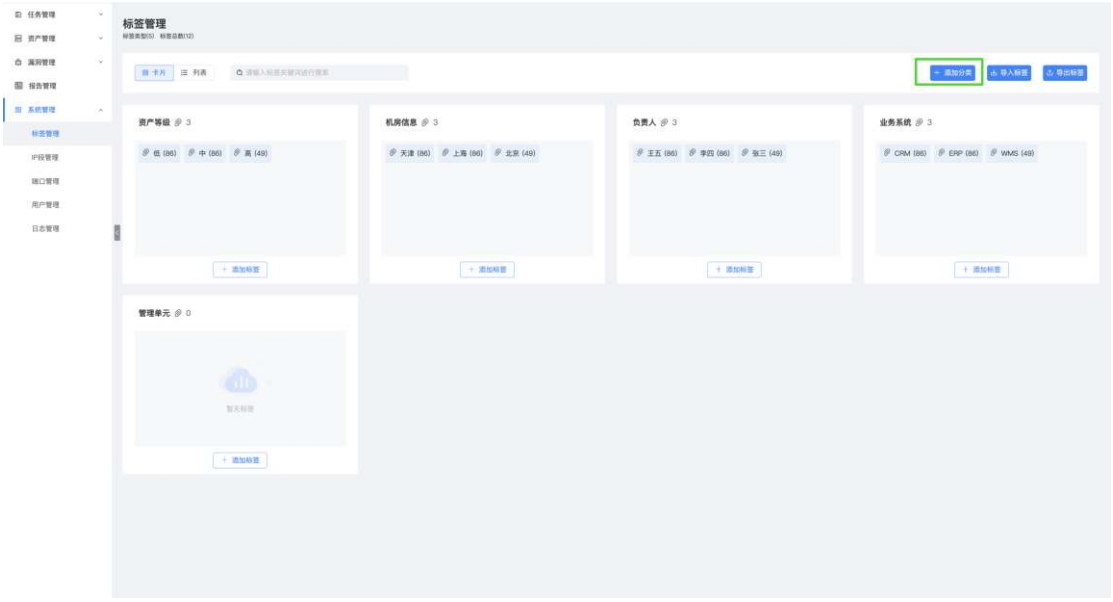
资产所属的标签管理，用来更好的分类管理资产。分为卡片视角与列表视角 2 个视角。卡片视角以卡片形式展示了标签信息，包括标签分类、标签名称等信息等。

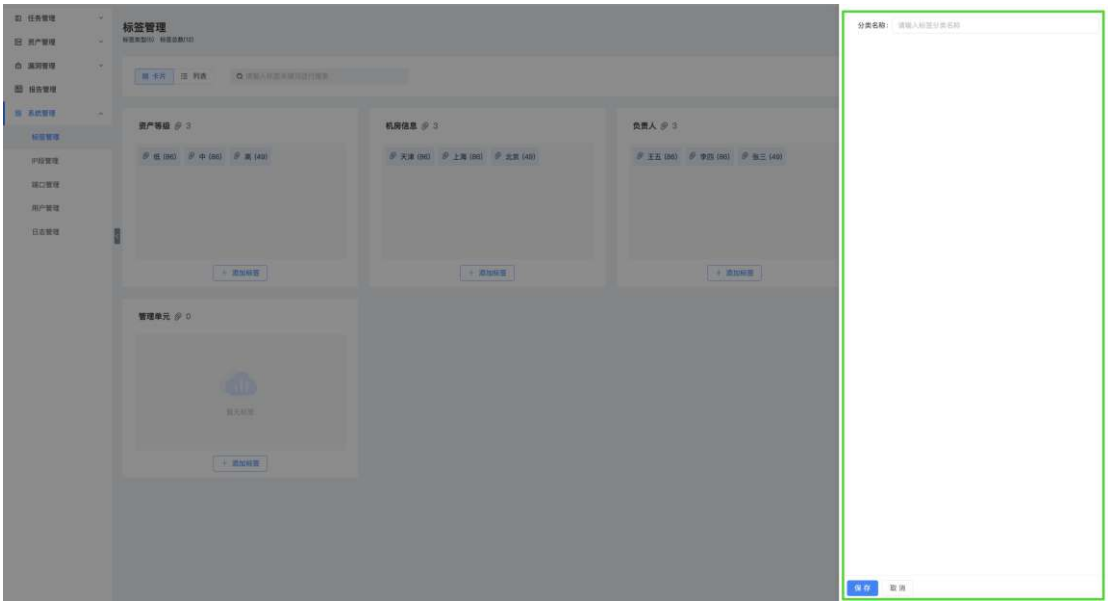


列表维度以列表形式展示了标签信息，包括分类名称、标签类型、标签数量、创建时间、以及相关操作等。

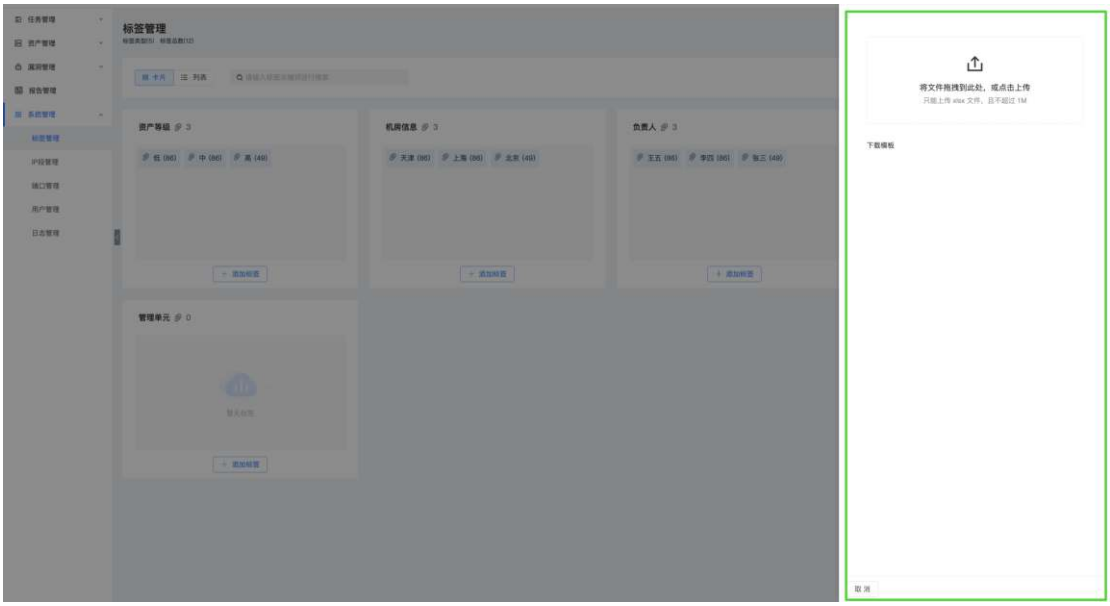
2.5.1.2 标签管理操作

【系统管理】-【标签管理】，点击【添加分类】，支持添加标签分类，最多支持自定义 3 个标签分类，每个分类下最多支持添加 300 个标签。

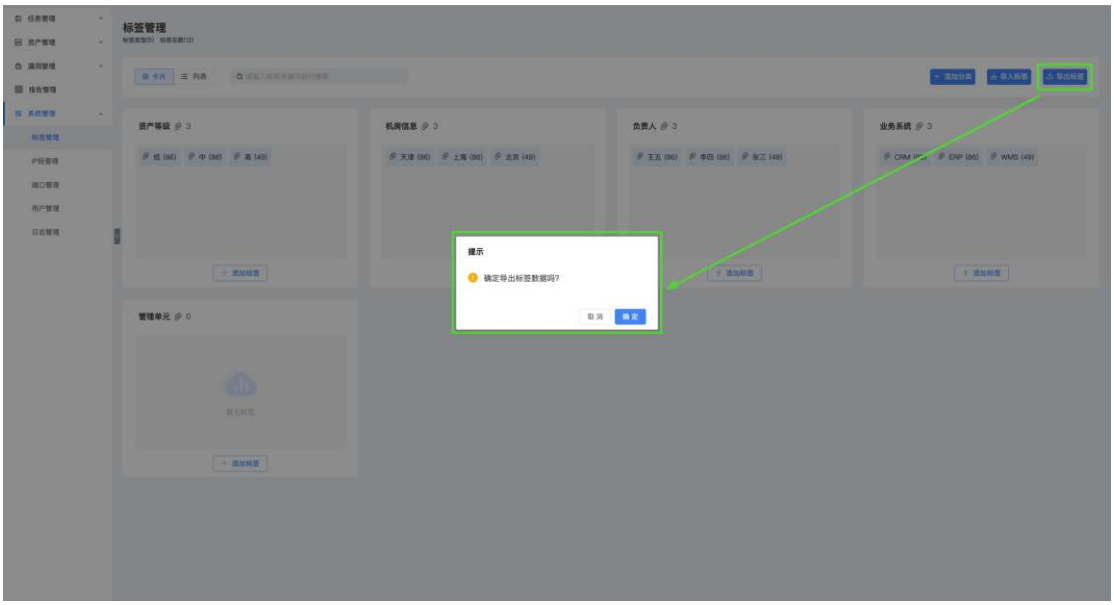




【系统管理】-【标签管理】，支持【导入标签】功能。



【系统管理】-【标签管理】，支持【导出标签】功能。



【系统管理】-【标签管理】，点击【添加标签】，支持新增标签。

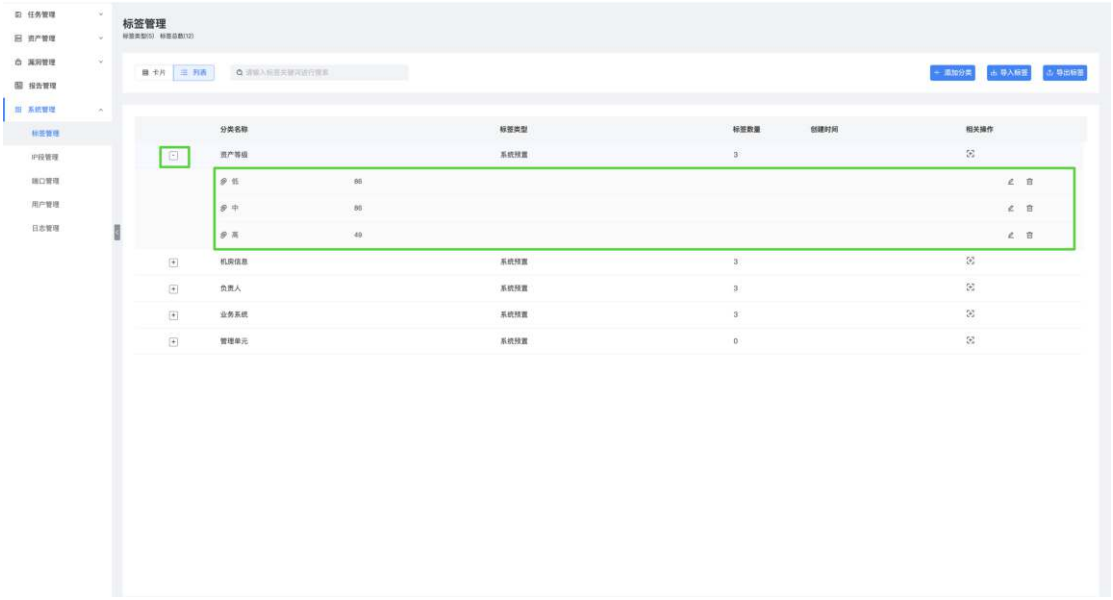
【系统管理】-【标签管理】，支持根据关键字搜索标签。

【系统管理】-【标签管理】，点击自定义标签分类模块“...”，支持编辑、删除该标签分类信息。

【系统管理】-【标签管理】，点击“标签”，支持编辑该标签。

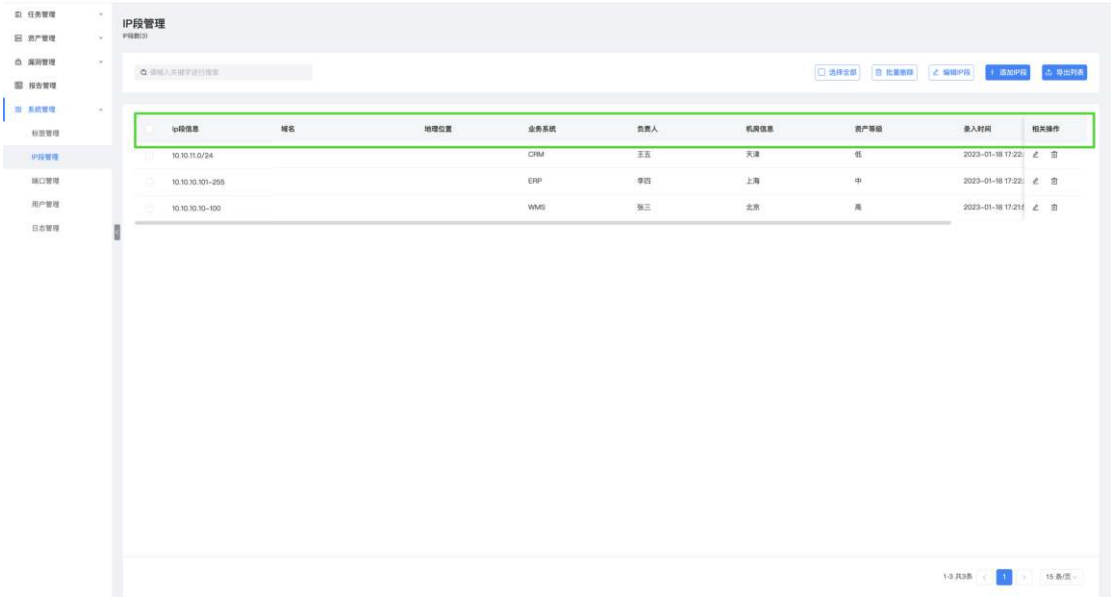
【系统管理】-【标签管理】，点击“标签”上的 X 号，支持删除该标签。

【系统管理】-【标签管理】，列表视角下，支持点击标签分类查看该分类下的标签信息。

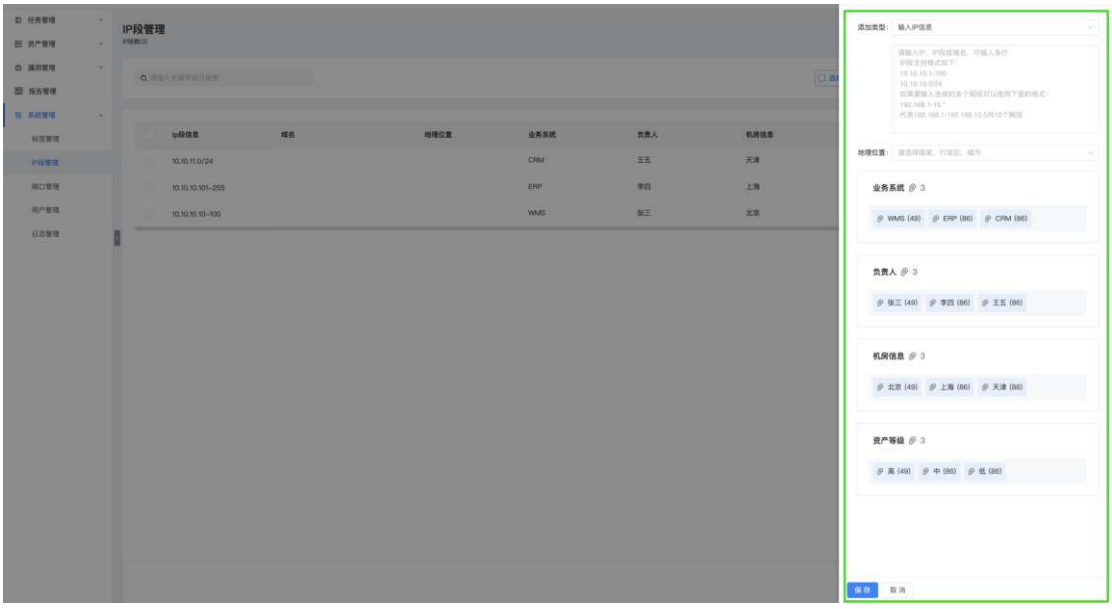


2.5.2 IP 段管理

【系统管理】-【IP 段管理】显示所有管理的 IP 段（每次下发任务时，填入的 IP、IP 段，都会默认保存到“IP 段管理”列表中）。

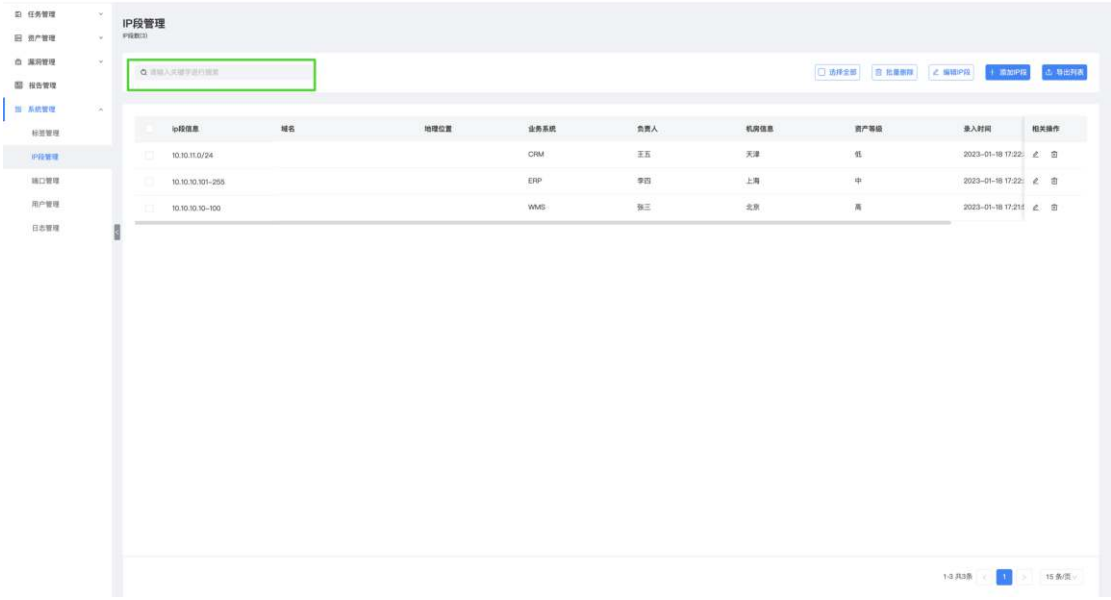


【系统管理】-【IP 段管理】，点击【添加 IP 段】，为 IP 段打上标签等信息。



【系统管理】-【IP 段管理】，支持编辑、批量编辑 IP 段内资产的“IP 段信息”、“地理位置”、“管理单元”、“业务系统”、“负责人”、“机房信息”等信息。

【系统管理】-【IP 段管理】，支持搜索 IP 段信息。

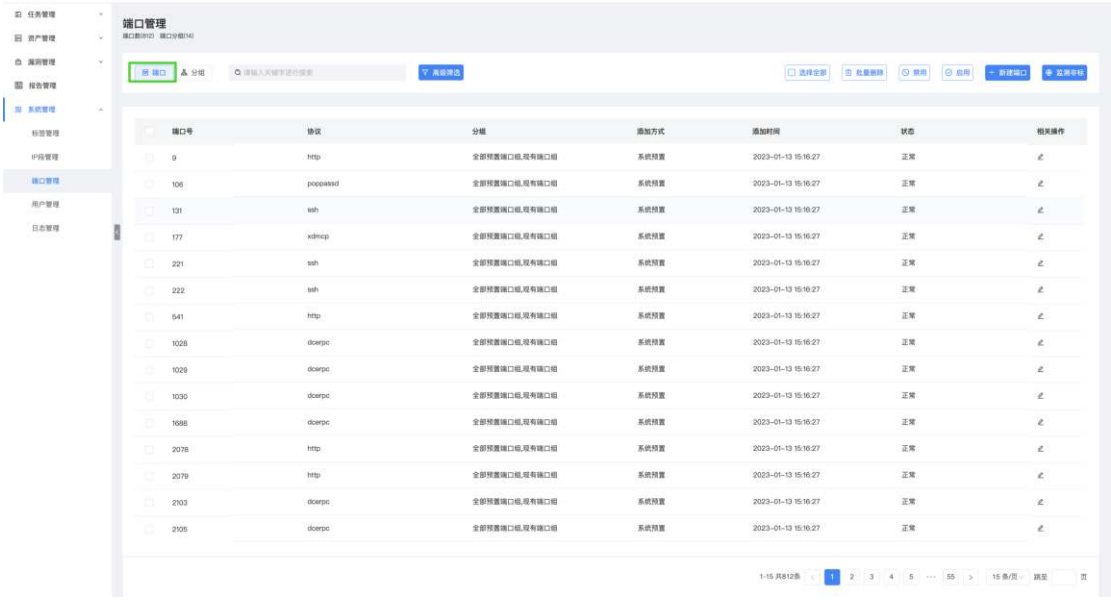


【系统管理】-【IP 段管理】，支持删除 IP 段信息。

【系统管理】-【IP 段管理】，点击【导出列表】按钮，支持导出功能。

2.5.3 端口管理

【系统管理】-【端口管理】分为端口视角与分组视角，默认分为 10 个分组，端口视角如图：



【系统设置】-【端口管理】端口视角中，支持自定义添加端口，选择协议。 点击【新建端口】，选择要添加的端口号，并指定协议、端口组。

【系统设置】-【端口管理】端口视角中，支持编辑端口信息，点击编辑

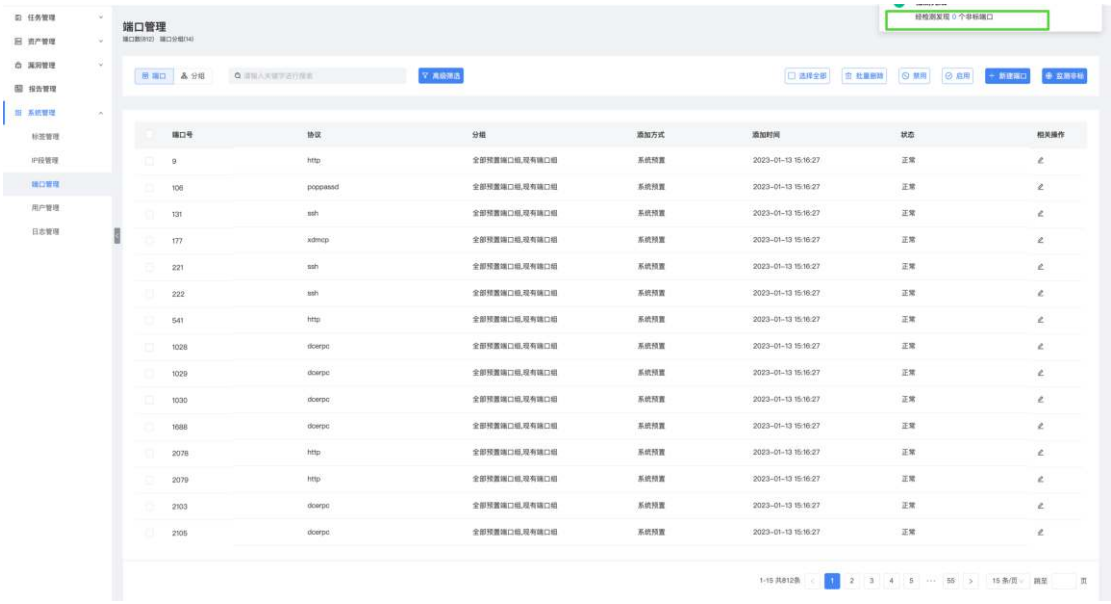
按钮。

【系统设置】-【端口管理】端口视角中，支持禁止某些端口扫描。 筛选需要禁用的端口，并点击【禁用】按钮，禁用后下发此端口的端口组时，不会扫描该禁用端口。

【系统设置】-【端口管理】端口视角中，也可点击【启用】解除该端口的禁用扫描功能。

【系统设置】-【端口管理】端口视角中，支持搜索以及高级筛选，高级筛选包含内容如下：添加方式（扫描添加、系统预置）、协议名称、状态（启用、禁用）、端口分组。

【系统设置】-【端口管理】端口视角中，点击【检测非标】，支持检测非标端口，检测完毕后弹出检测结果。



【系统设置】-【端口管理】端口视角中，点击【删除】，支持删除（批量删除）端口，弹出确认删除按钮，点击确认后即可删除该端口。

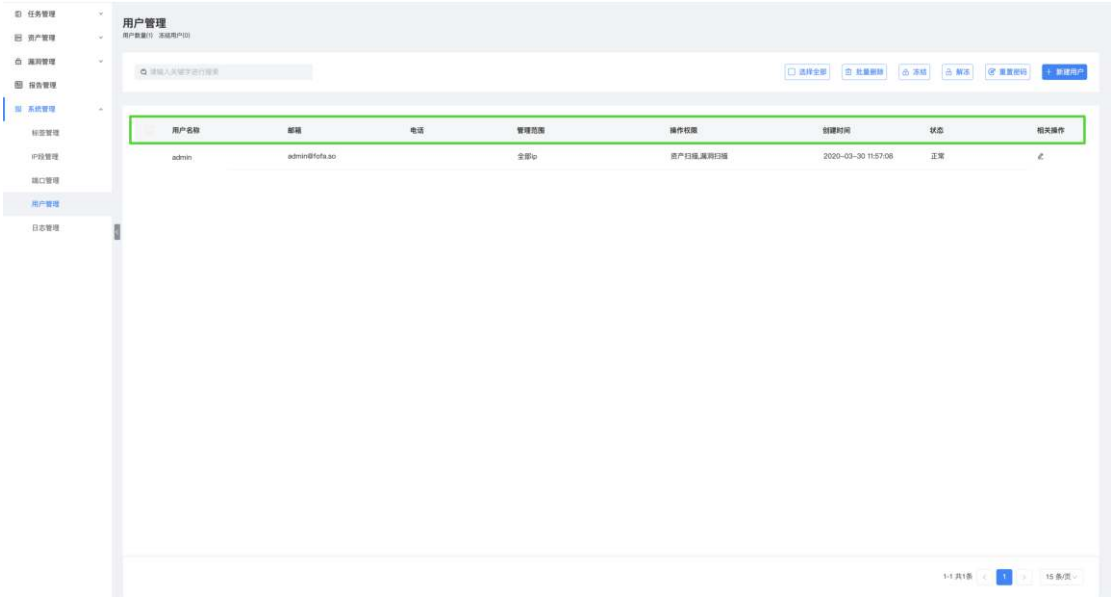
【系统设置】-【端口管理】分组视角中，支持新建分组，点击【新建分组】，输入分组名称，选择端口，点击【保存】。

【系统设置】-【端口管理】分组视角中，支持根据关键字搜索端口分组。

【系统设置】-【端口管理】分组视角中，支持对端口分组编辑、，针对自定义新增端口支持删除操作。

2.5.4 用户管理

【系统管理】-【用户管理】模块展示了所有用户的“用户数量”、“冻结用户”数量。



【系统管理】-【用户管理】页面，展示“用户名称”、“邮箱”、“电话”、“管理范围”、“操作权限”、“创建时间”、“状态”等信息。

【系统管理】-【用户管理】，支持新建用户，系统用户分为两种类型，超级管理员、普通管理员。只有超级管理员用户登录才能看到用户管理的主导航菜单。只有超级管理员可以创建用户，创建的用户均为普通用户，普通用户无法使用用户管理和日志管理。

添加用户可以为用户设置操作权限，资产扫描、漏洞扫描、合规监测三种权限。并且可以设定普通管理员的管理范围，全部 IP、根据 IP 段筛选、管理单元、业务系统、负责人、机房信息、自定义标签。

操作权限：

资产扫描和漏洞扫描将影响用户下发扫描任务和定时任务可以选择的任务类型，也会影响用户制定报告模板时可以选择的报告内容。如果用户两种任务类型都不选择，将无法下发扫描任务以及看不到任务管理相关的菜单和页面。如三种操作全都不勾选，那普通用户仅可进行数据查看，不可下发扫描任务等操作。

管理范围：

全部资产：用户可以查看和操作全部资产，默认选项。

根据 IP 段进行筛选：用户可以选择跟此用户绑定的 IP 段，下发扫描任务和定时任务只能根据 IP 段进行下发，其他扫描范围的选项均不在出现。

根据【标签类型】进行筛选：用户可以选择跟此用户绑定的管理标签，下发扫描任务和定时任务只能根据标签进行下发，其他扫描范围的选项均不在出现。

一般用户仅可操作、查看自己数据范围内的数据。

必须为用户绑定资产数据，否则无法创建用户。

支持添加用户；【系统管理】-【用户管理】-【新建用户】，输入用户的“用户名称”、“登录密码”、“邮箱地址”、“电话号码”、“操作权限”、“管理范围”后点击【保存】。

支持根据关键字进行查询。

支持用户“冻结”、“解冻”功能；【系统管理】-【用户管理】-【冻结】、【解冻】。

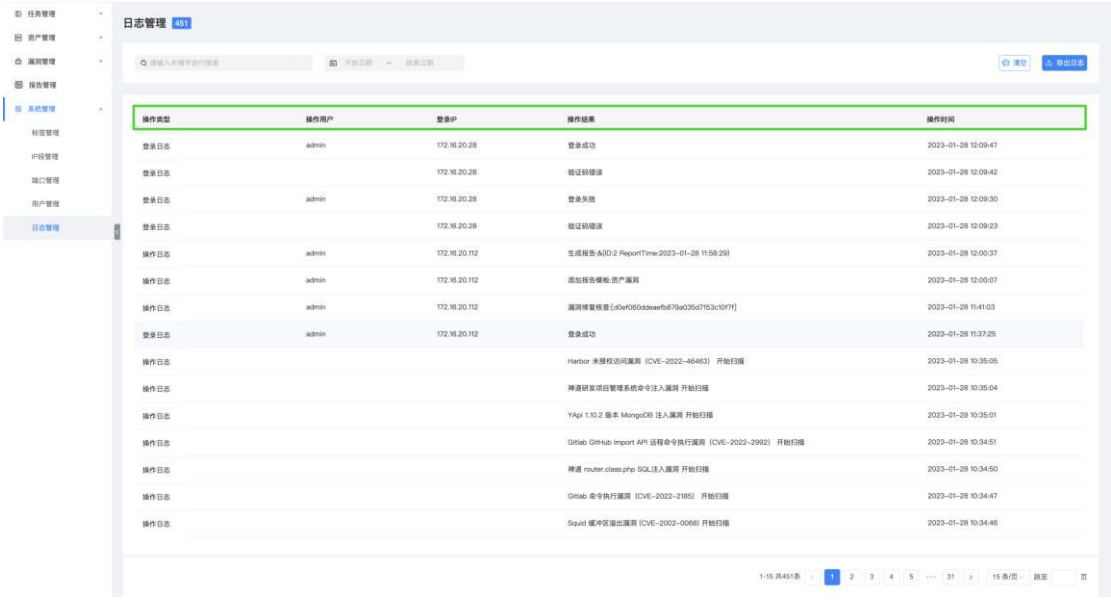
支持用户“重置密码”。【系统管理】-【用户管理】-【重置密码】。

支持用户信息“编辑”。【系统管理】-【用户管理】-【编辑】。

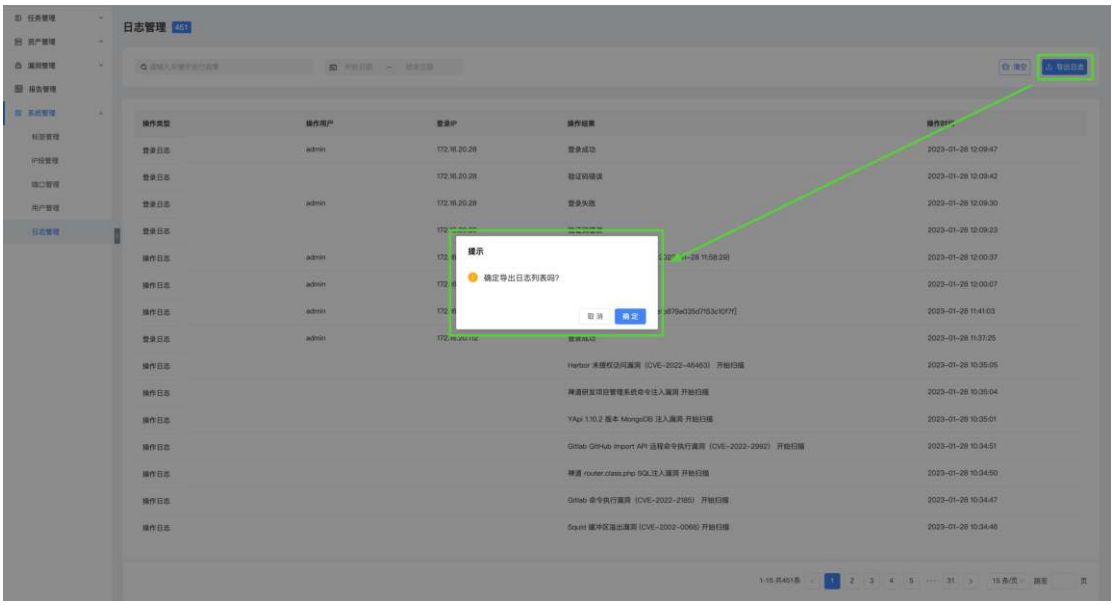
支持用户“删除（批量删除）”。【系统管理】-【用户管理】-【删除】。

2.5.5 日志管理

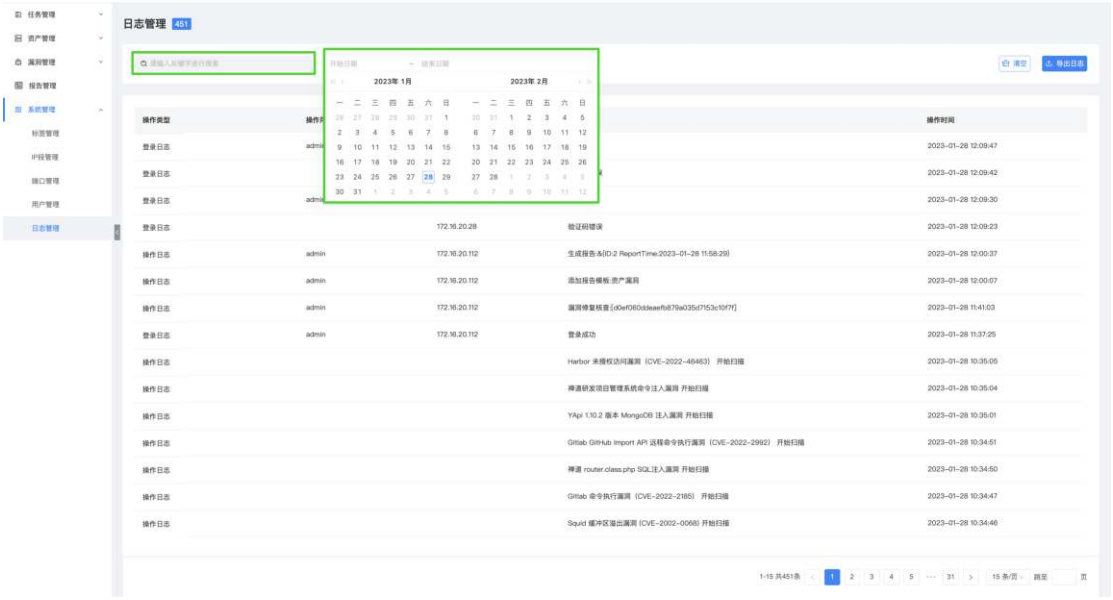
【系统管理】-【日志管理】记录了用户日常的操作，展示了“操作类型”、“操作用户”、“登录 IP”、“操作结果”、“操作时间”等信息。



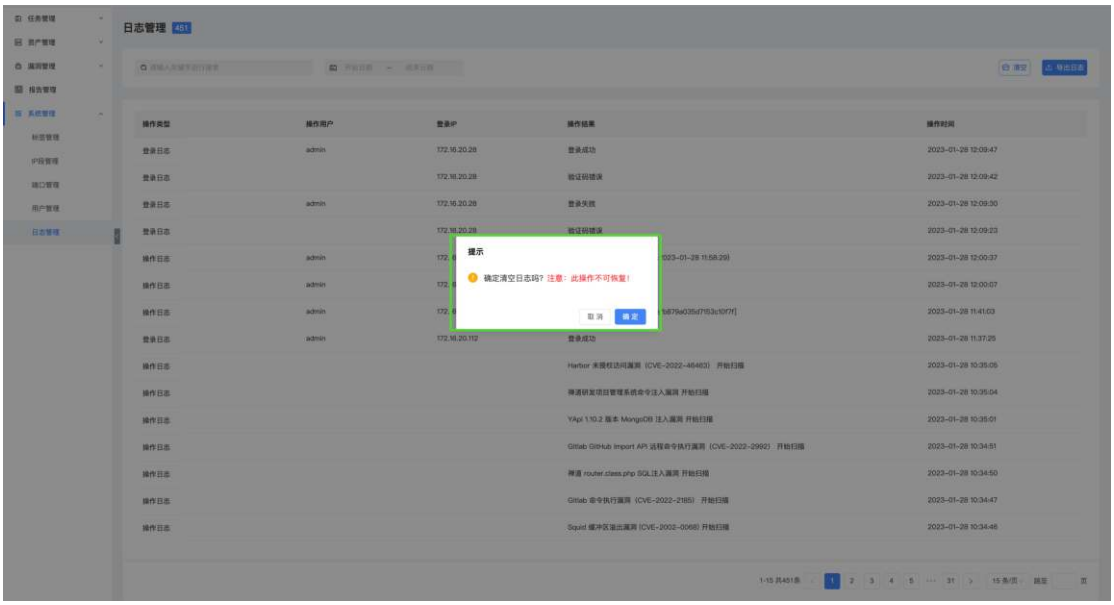
支持日志导出功能,【系统管理】-【日志管理】-【导出日志】



支持日志筛选功能，可对日志的关键词、日期范围进行筛选。



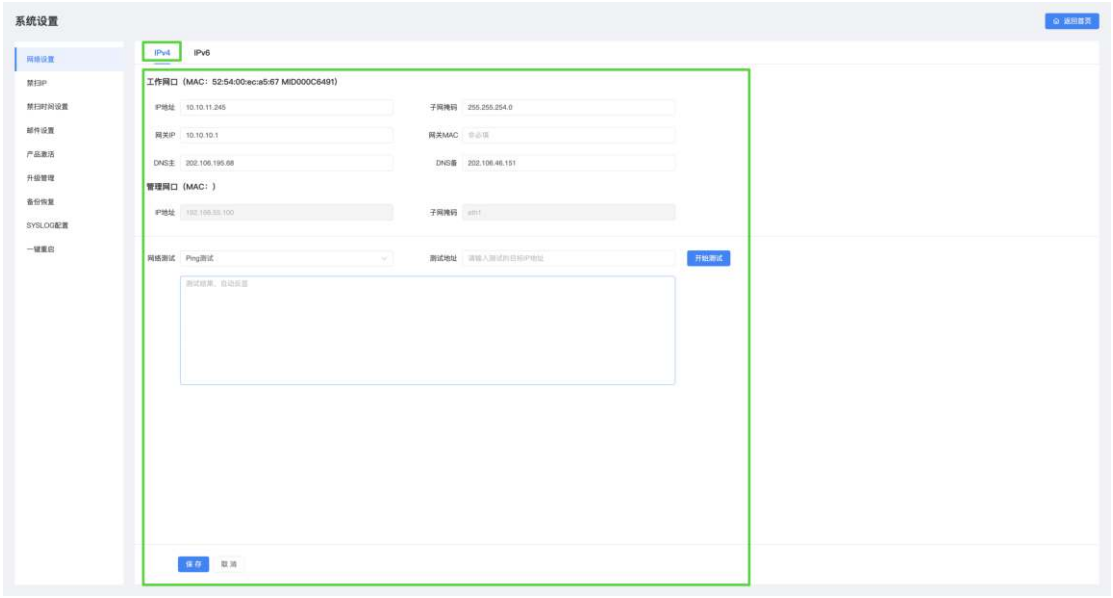
支持清空日志功能，点击【清空】。



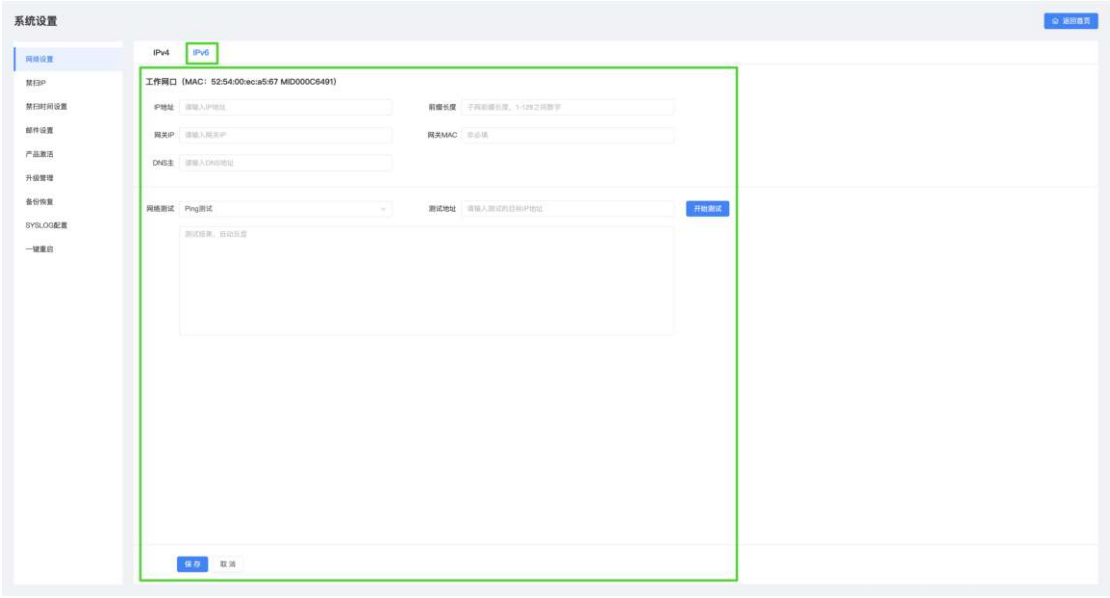
2.6 系统设置

2.6.1 网络设置

【系统设置】-【网络设置】支持设置该系统网络信息，包括 IPV4 与 IPV6 的设置。IPV 如图：

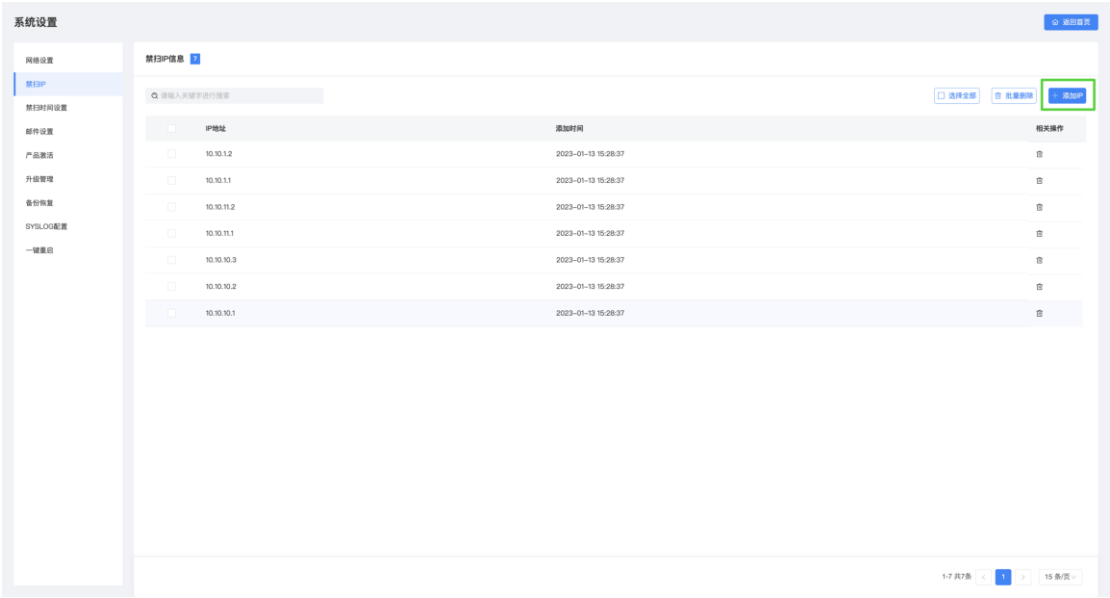


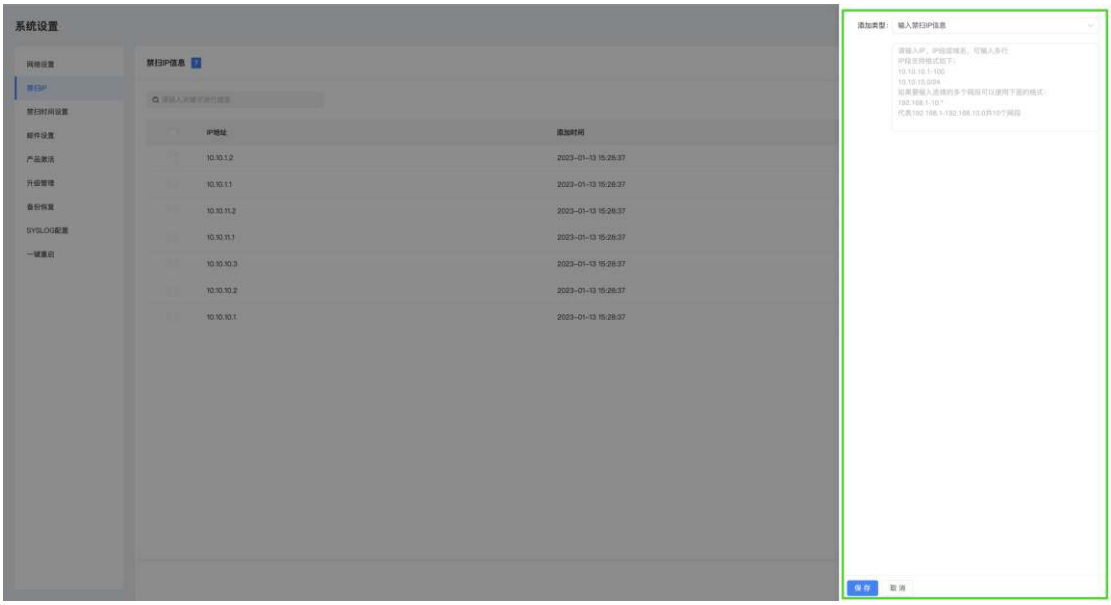
【系统设置】-【网络设置】，IPV6 如图：



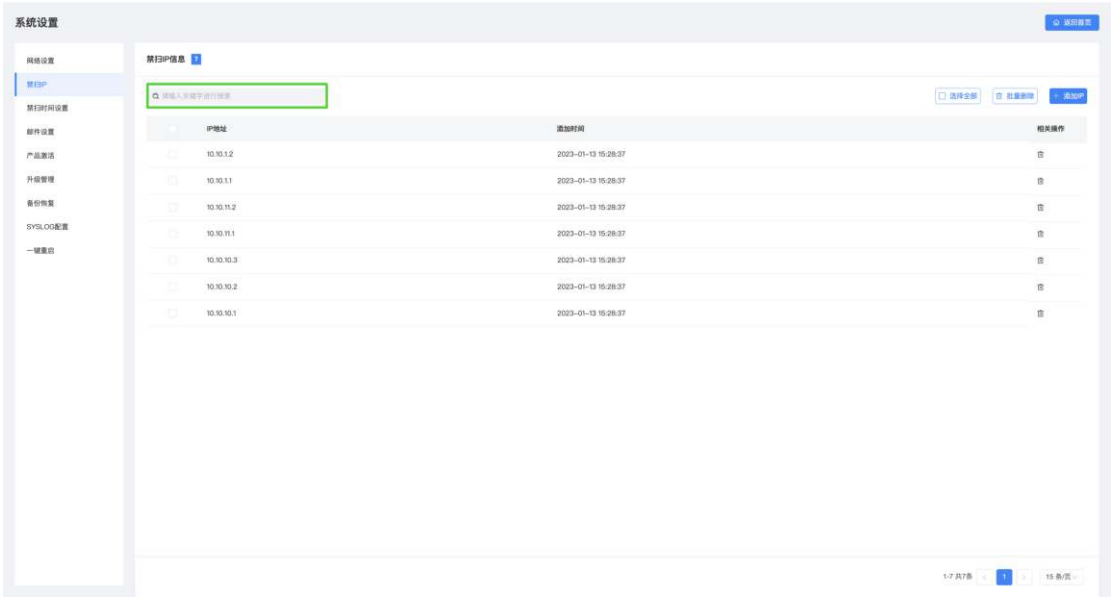
2.6.2 禁扫 IP

【系统设置】-【禁扫 IP】支持添加禁扫 IP 信息，支持手动添加或上传文件添加，添加后的 IP，下发扫描任务时将不进行扫描。

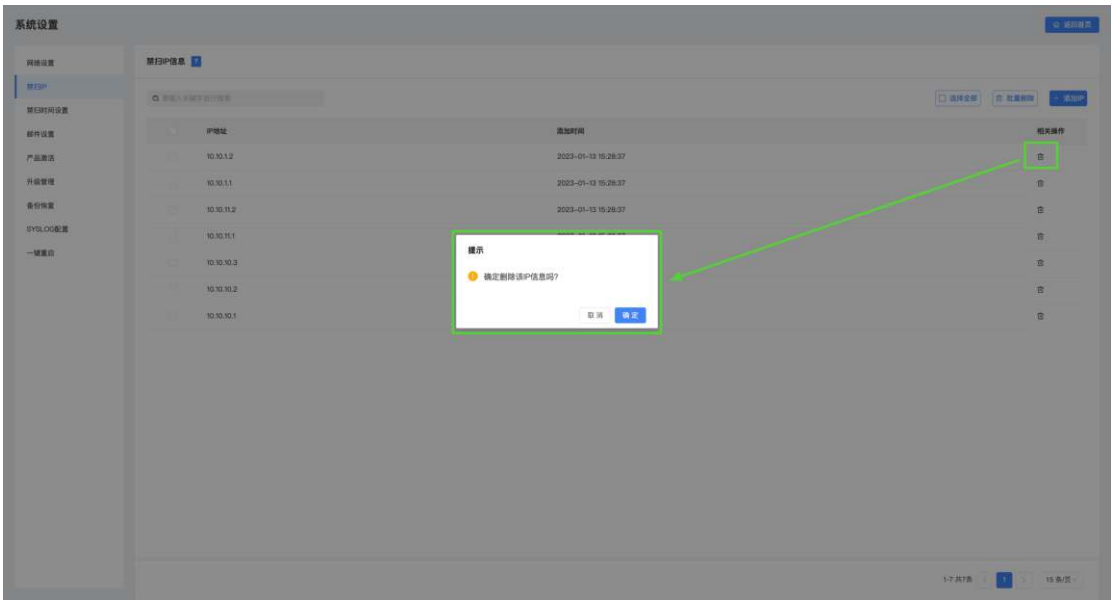




【系统设置】-【禁扫 IP】，支持已添加禁扫 IP 信息的搜索。

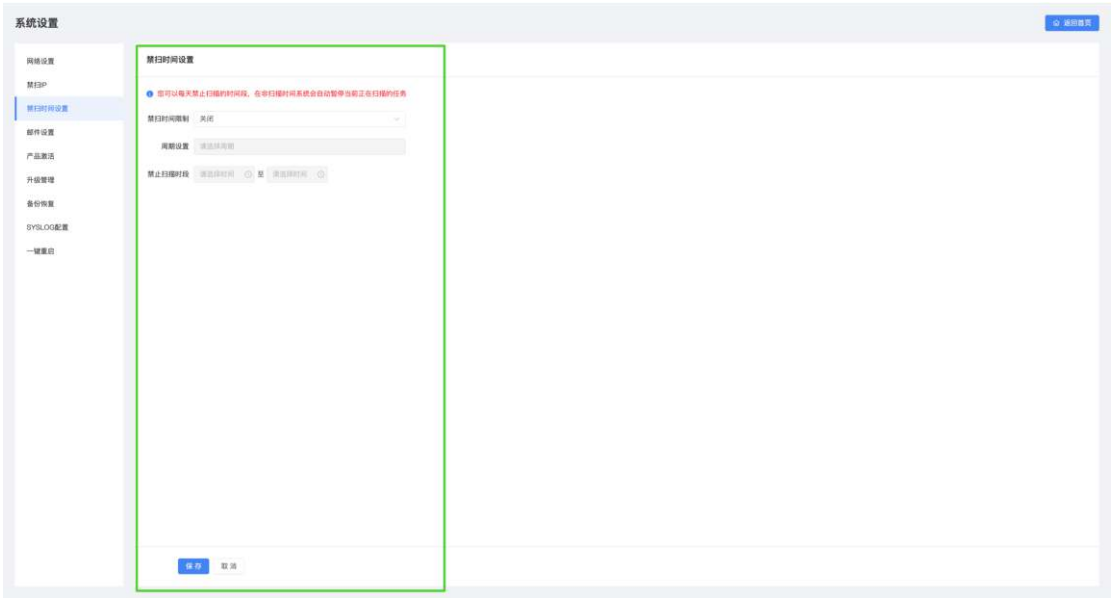


【系统设置】-【禁扫 IP】，支持已添加禁扫 IP 信息的删除（批量删除）。



2.6.3 禁扫时间设置

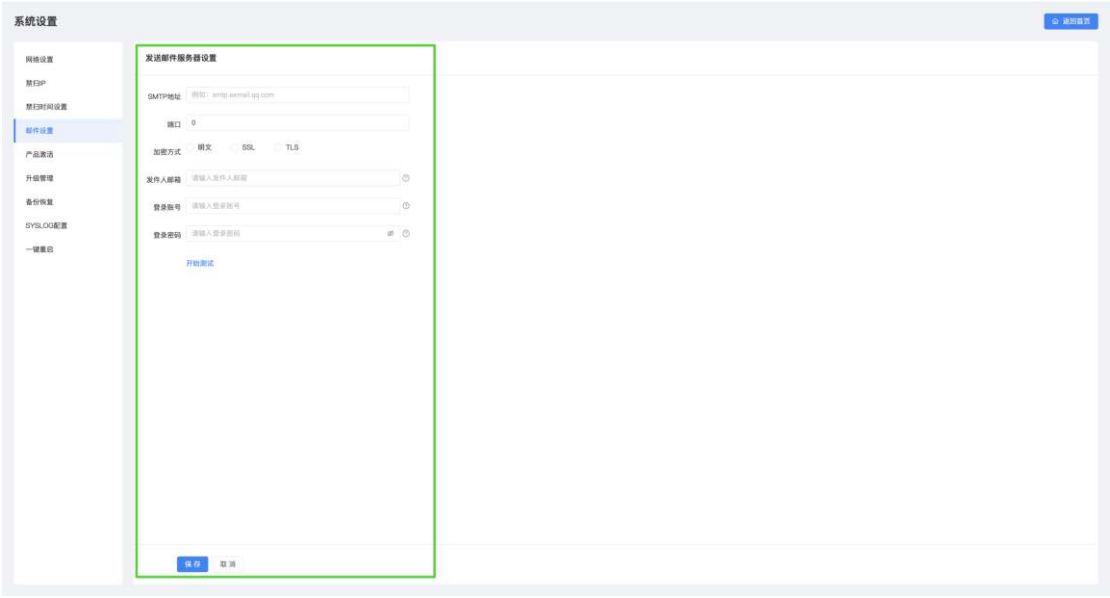
【系统设置】-【禁扫时间设置】选择开启以及设置禁扫时间段，在设置的时间段内将不可进行扫描任务，正在执行的扫描任务也会自动暂停扫描，过了禁扫时间将自动恢复扫描。



2.6.4 邮件设置

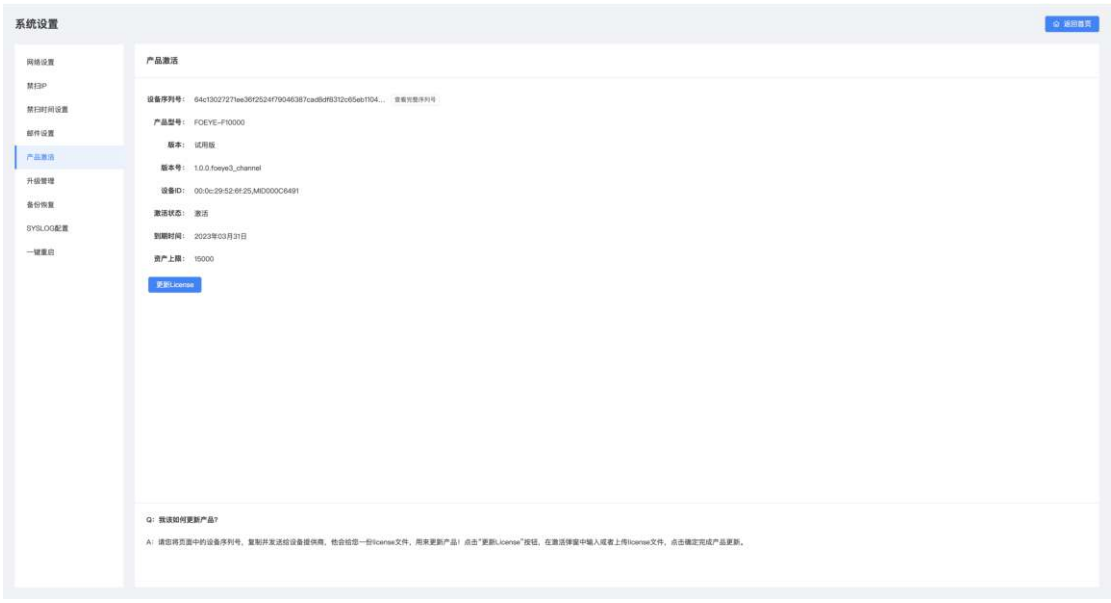
【系统设置】-【邮件设置】可在每次漏洞扫描完后的结果发送至指定用

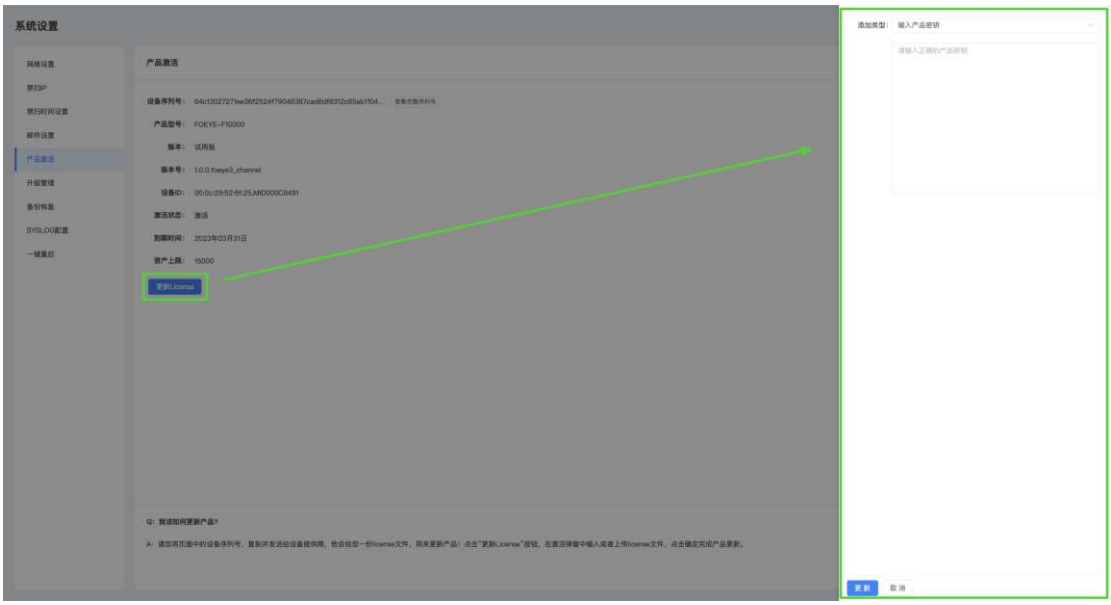
户邮箱；填入“STMP 地址”、“端口”、“发件人邮箱”、“登录账号”、“登录密码”后，选择“加密方式”，包括明文、SSL、TLS 三种方式，点击【保存】按钮即可；也可支持发送测试邮件。



2.6.5 产品激活

【系统设置】-【产品激活】通过 license 激活产品、产品延期、产品增加资产上限，将设备序列号复制全，发送给设备提供商，设备提供商会提供相应 license，点击“更新 license”输入 license 点击保存即可激活。

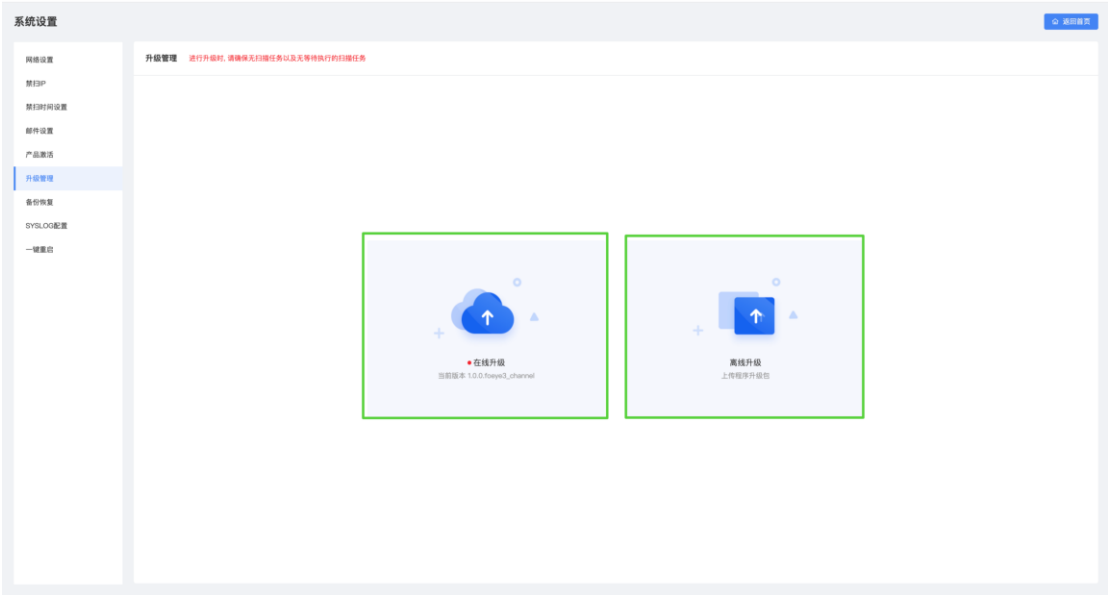




2.6.6 升级管理

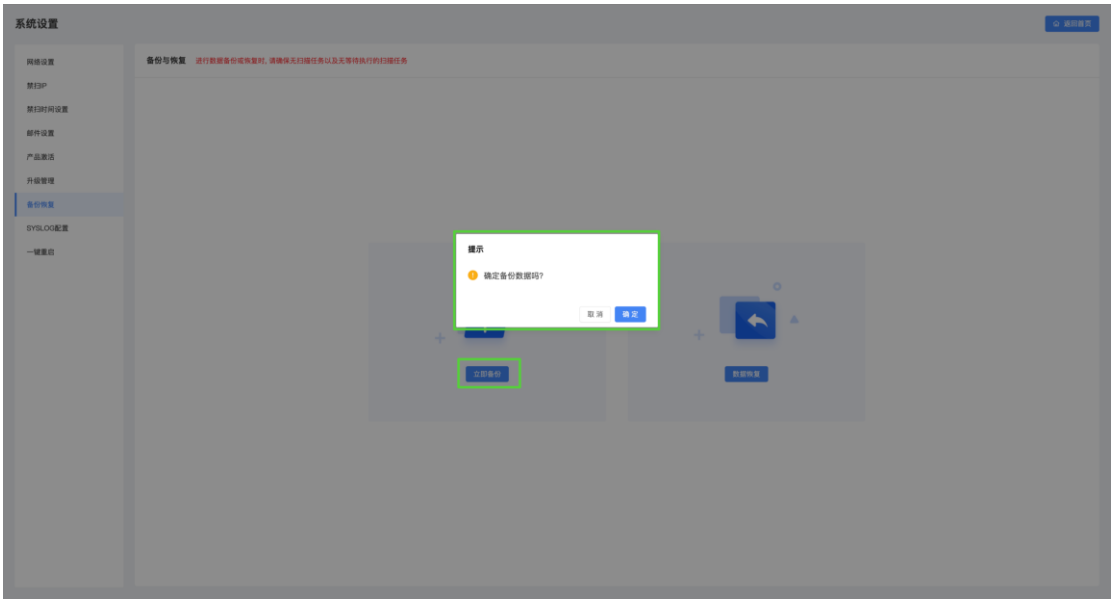
系统升级分为代码升级和漏洞库升级，上传升级的程序包，系统会自动的升级，升级期间请不要关闭当前页面，也不要执行任何操作，等待升级完成提醒即可。

支持“在线升级”（需要能够连接到升级服务器）与“离线升级”2 种方式。

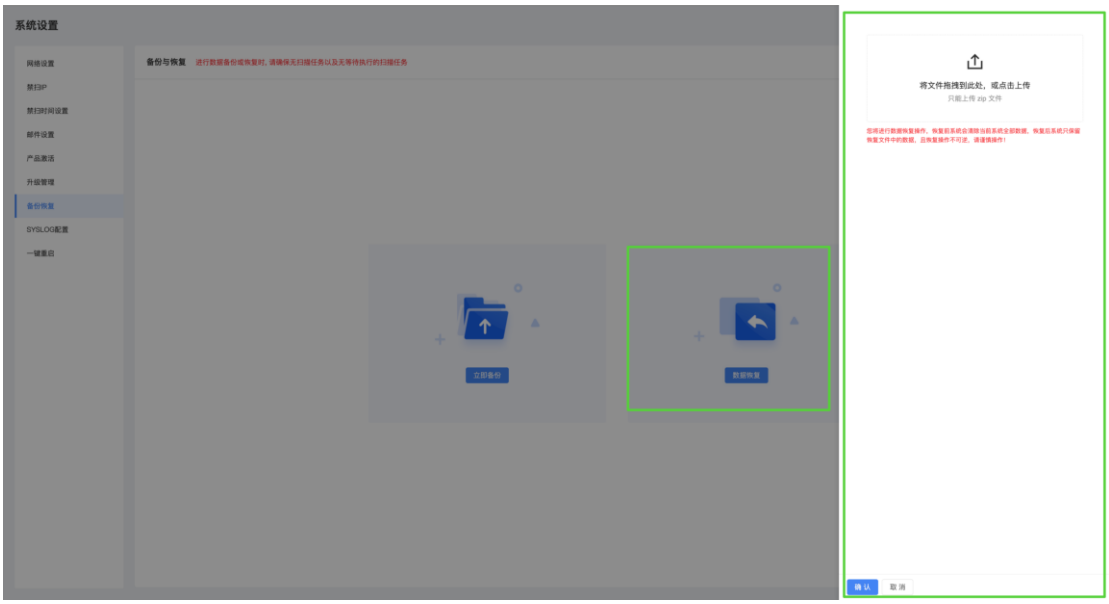


2.6.7 备份恢复

【系统设置】-【备份恢复】，数据备份模块，点击【立即备份】可备份数据。

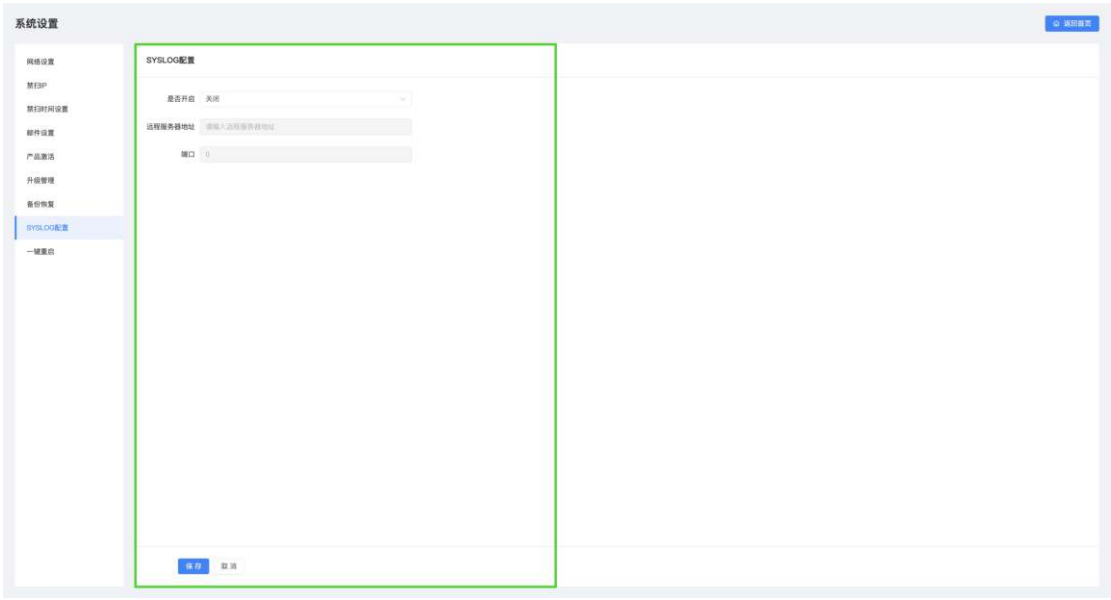


【系统设置】-【备份恢复】，数据恢复模块，点击【数据恢复】上传文件后可恢复数据。

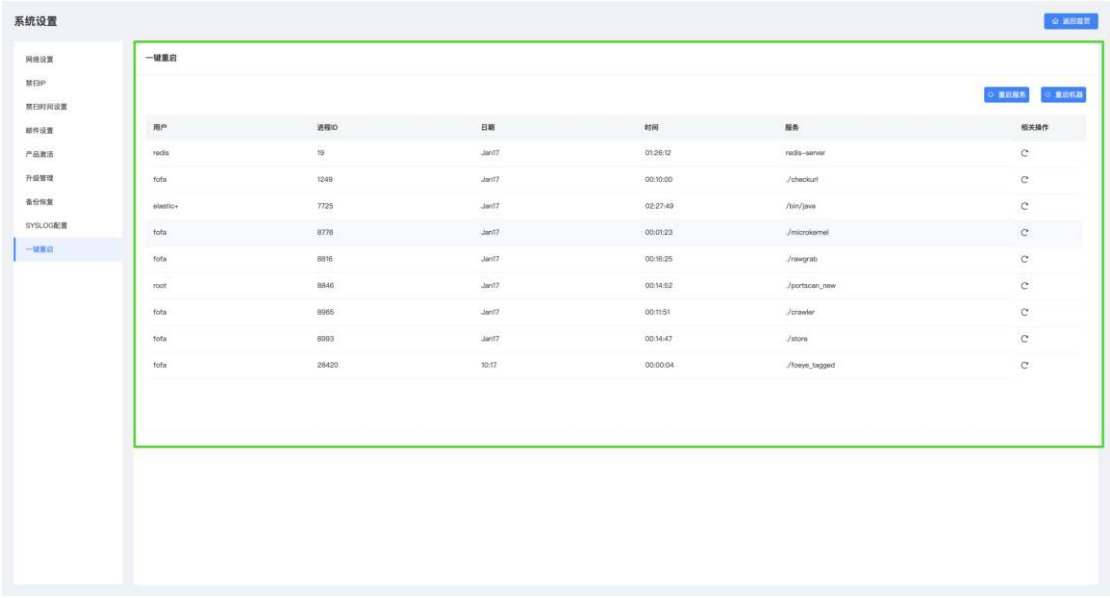


2.6.8 SYSLOG 配置

【系统设置】-【SYSLOG 配置】选择开启后填入“远程服务器地址”、“端口信息”点击【保存】。



2.6.9 一键重启

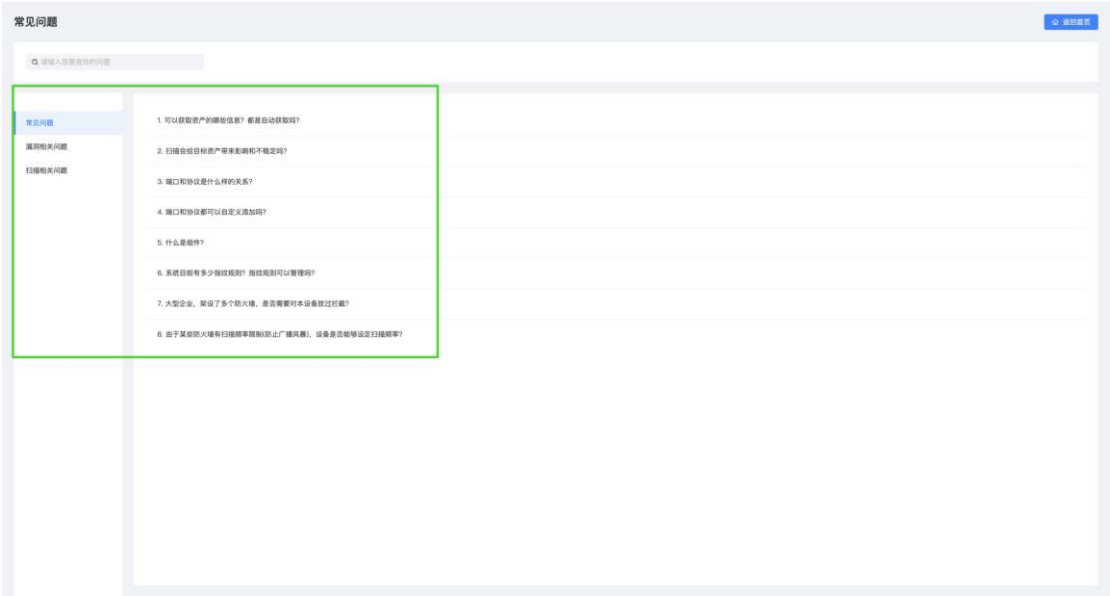


2.6.10 使用指南

页面右上角如图，点击【使用指南】，跳转到使用指南页面，用户可参考该指南使用系统。

2.6.11 常见问题

页面右上角如图，点击【常见问题】，跳转到常见问题页面。支持查看常见问题、漏洞相关问题、扫描相关问题、环境配置问题等。



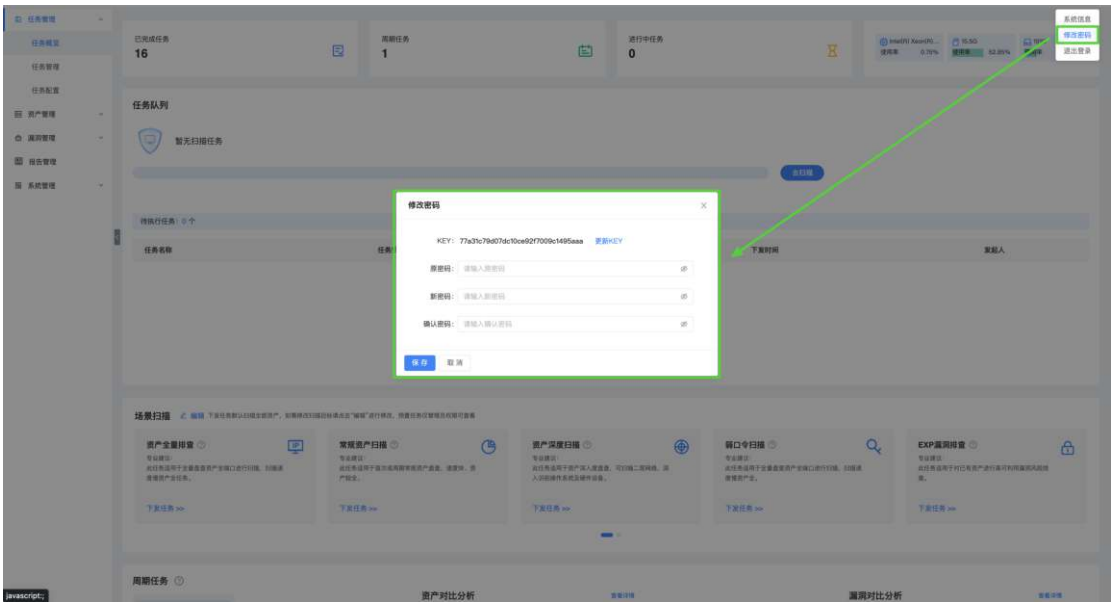
2.6.12 系统信息

页面右上角【系统信息】展示了设备的“产品型号”、“系统版本”、“PoC 版本”、“管理上限”、“厂商信息”、“服务电话”、“服务邮箱” “服务到期”，CPU 型号、内存容量、硬盘容量及使用率等信息。

支持重启、关机服务器。

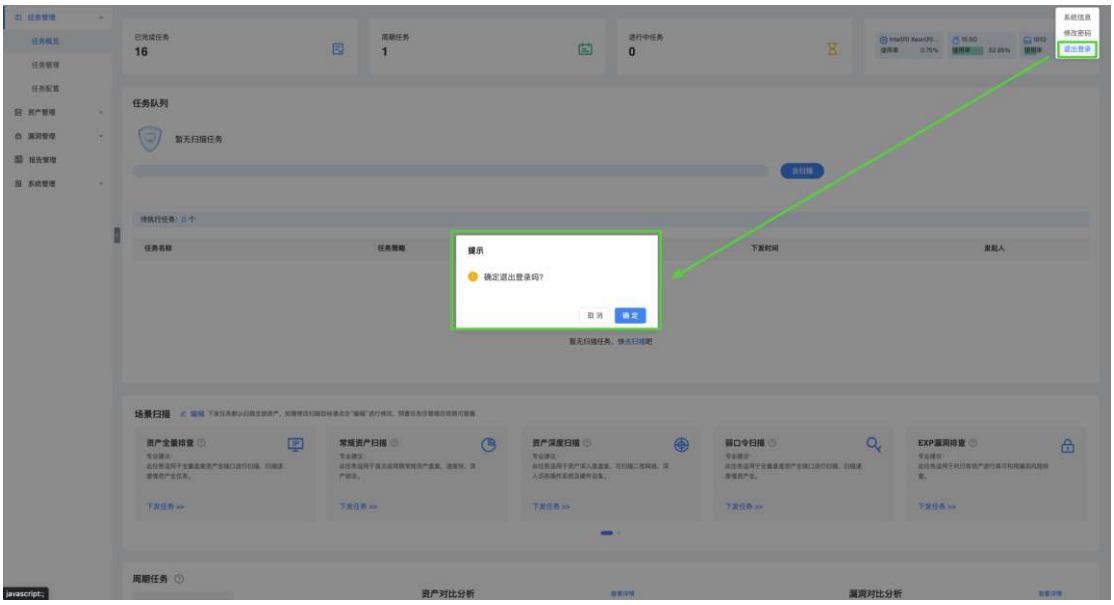
2.6.13 修改密码

页面右上角【修改密码】支持当前用户密码修改功能；页面右上角【修改密码】，输入“原密码”、“密码”、“确认密码”后，点击【保存】按钮即可修改当前用户密码。



2.6.14 退出登录

页面右上角【退出登录】支持退出当前用户登录；页面右上角点击【退出登录】按钮即可退出当前用户登录系统。



2.7 资产全景图

通过可视化大屏展示系统中的资产信息以及风险信息，快速掌握网络资产详情。