长亭科技
CHAITIN

洞鉴(X-Ray)安全评估系统
产品使用手册

北京长亭科技有限公司

一、首次访问

部署成功后，首先需要长亭科技签发的官方许可证文件，验证通过后，才可使用洞鉴安全评估系统。

1.1 部署并上传许可证

部署成功后，访问服务器网址，会出现如下界面：

- 复制机器码给相关工作人员，申请绑定机器码的 license；
  - 如果授权的 license 绑定的机器码与当前机器码不符，则无法认证成功，需重新上传。
- 点击或拖拽许可证文件；
- 上传正确的许可证文件后，会显示初始用户名、初始密码、被授权的企业名称和授权使用时间，管理员确认无误后，点击“确认”，即可完成许可证的更新，此时 许可证内容显示新上传的许可证信息。

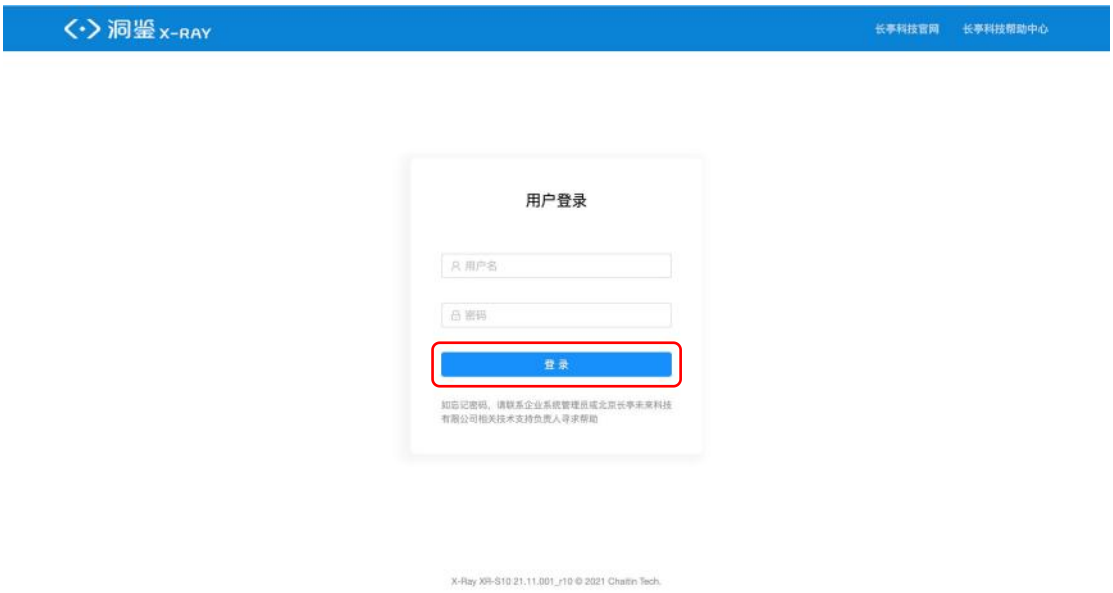
注意：这一步注意要复制好密码，点击“确认”后，需要用此密码登录。

- 此时的初始用户名和初始密码，在许可证信息上传成功后，用于登录系统。

1.2 登录

1.2.1 用户登录

- 输入正确的用户名和密码后进入主页面。



温馨提示：如忘记密码，请联系企业系统管理员或公司相关技术支持负责人寻求帮助。

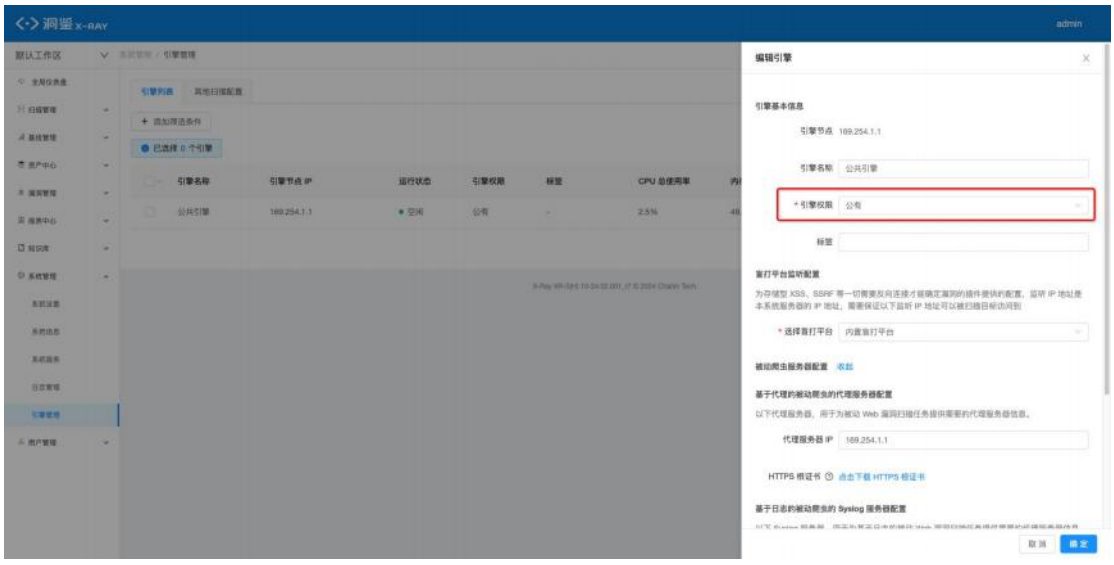
1.2.2 未登录时顶部导航栏

可导航至长亭科技官网和帮助中心

1.3 首次使用注意事项

1.3.1 引擎权限分配

新部署的引擎权限默认未配置，需要手动分配成公有或私有的权限



二、系统界面布局介绍

2.1 菜单导航

洞鉴(X-Ray)安全评估系统菜单栏从全局仪表盘、扫描管理、基线管理、镜像管理、资产中心、漏洞管理、报表中心、知识库、系统管理、用户管理进行分类展示。

- 全局仪表盘：从全局提供一些关注度高的信息统计视图，如漏洞、资产等。
- 扫描管理：存放扫描相关的各项操作和数据展示内容：
  - 任务统计：包括任务概览、结果统计
  - 扫描策略
  - 任务列表
  - 扫描设置
    - 字典管理
    - 端口组管理
    - 全局白名单配置
    - 盲打平台监听配置
- 基线管理：包含基线检查相关的数据和操作
  - 基线检查任务列表：包含在线检查列表、离线检查列表、离线本地列表
  - 基线检查配置
- 镜像管理：包含镜像检查相关的数据和操作
  - 镜像扫描任务列表
- 资产中心：此模块主要用于企业的资产进行管理，系统将企业的资产数据进行综合统计计算并可视化，方便直观的展示给用户，并支持对已知资产与未知资产进行集

中管理，包括对资产的查询、筛选、添加、删除、快速扫描等操作。企业可对资产进行分组和指派责任人、管理员。

- 资产全景
- 资产列表
  - 主机资产列表
  - Web 站点资产列表
  - 资产组列表
- 资产属性管理
  - IP 段管理
  - 业务系统管理
  - 网络区域管理
  - 标签管理

- 漏洞管理：方便用户对系统所有漏洞、有风险的资产进行管理
  - 漏洞全景
  - 漏洞列表
- 报表中心：对已生成的不同类型报告的管理
  - 报表管理
  - 报表模板：包括扫描任务报表、基线检查报表、资产报表、漏洞报表
- 知识库
  - 漏洞库
  - 自定义 POC
  - 自定义指纹
- 系统管理
  - 系统设置：包含基本配置、显示配置、网络配置
  - 系统信息：包含基本信息、状态监控、服务状态
  - 系统服务：包括引擎升级、漏洞库升级、备份还原、引擎网络诊断、网络诊断工具
  - 日志管理
  - 引擎管理：包括引擎列表、其他扫描配置
- 用户管理
  - 系统用户管理
  - 用户角色设置
  - 组织单位管理
- 个人中心
  - 个人中心：包含个人基本信息，修改登录密码
  - Open API
  - 退出

2.2 面包屑

- 面包屑主要作为辅助导航，帮助用户方便定位当前所处的位置，快速进入到上一级或更上一级的页面；

2.3 正文区域

左侧导航栏右方的区域展示正文的详细内容。用户可在此进行查看、扫描和管理等各种操作。详情可以查阅下文三、四、五章中，对各功能模块的详细介绍。

三、功能模块介绍

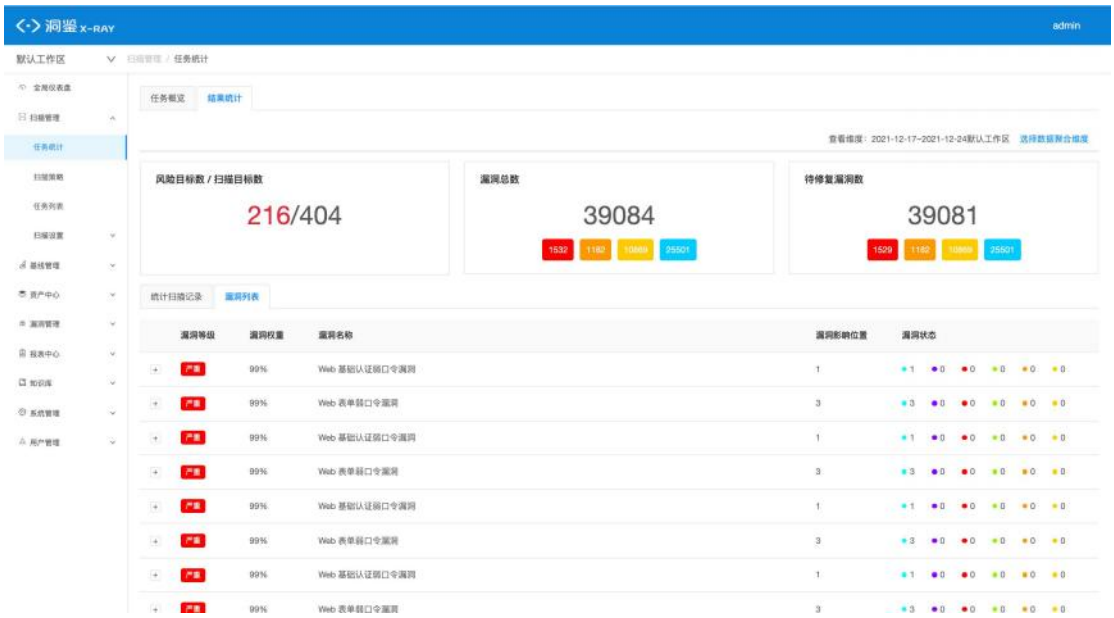
主要功能有：扫描管理、基线管理、镜像管理、资产中心、漏洞管理、报表中心和知识库。

3.1 扫描管理

3.1.1 任务统计

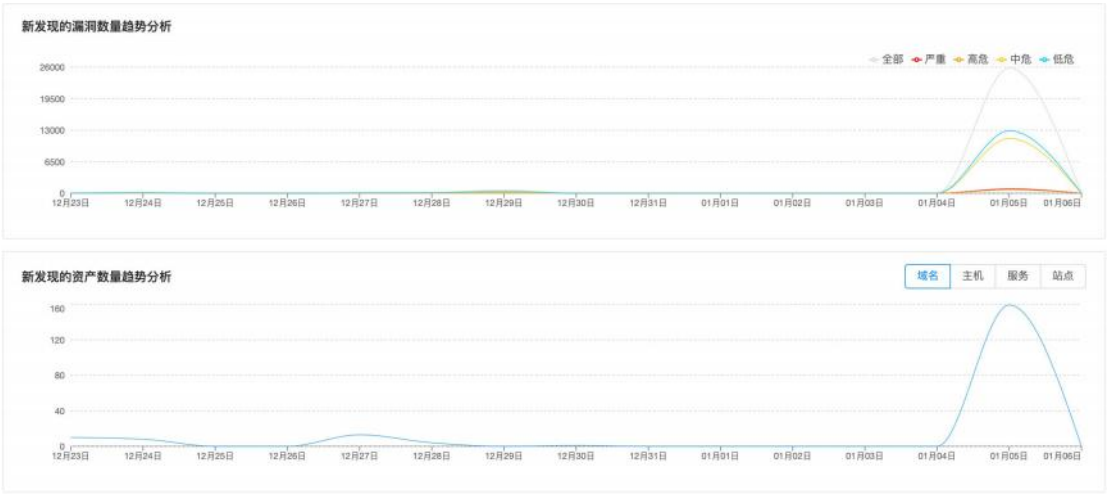
在左侧导航栏中，选择“扫描管理–任务统计”，进入扫描任务列表界面。

任务统计页面展示系统中的任务概览和结果统计。

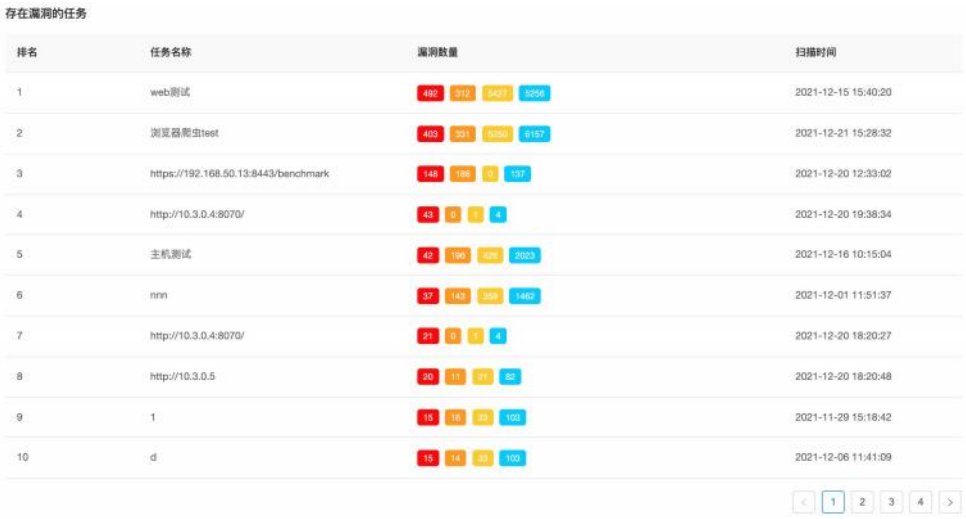


3.1.1.1 任务概览

- 不同扫描策略的任务数量分布：
  - 展示不同扫描策略的任务数量，鼠标悬浮在饼图上方可以看到具体的任务数。
- 最大并行任务数统计：
  - 展示系统当前正在并行的任务数（正在运行的任务总数），以及剩余并行任务数（还能够同时运行的任务数量）；
  - 最大任务并行数由 license 配置决定。



- 新发现的漏洞数量趋势分析：
  - 展示系统最近 15 天内，新发现的漏洞数量趋势；
  - 鼠标悬浮在图形上方，可以看到当天新发现的各个风险等级的漏洞数量。
- 新发现的资产数量趋势分析：
  - 展示系统最近 15 天内，新发现的资产数量趋势 ；
  - 鼠标悬浮在图形上方，可以看到当天新发现的资产数量 ；
  - 点击图形右上角的按钮，可以切换展示不同资产类型的趋势分析 。



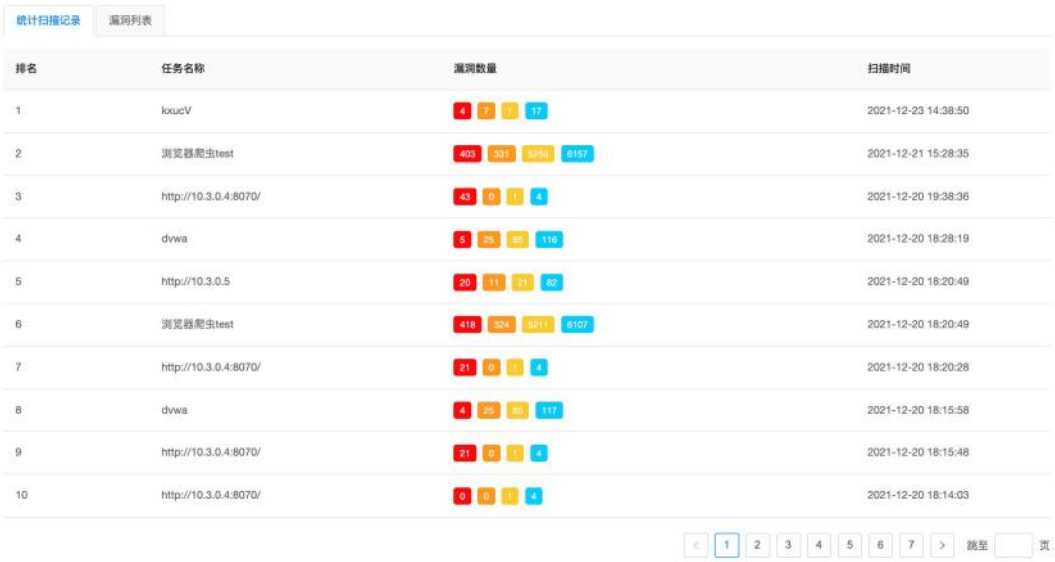
- 存在漏洞的任务：
  - 展示所有存在漏洞的任务，方便用户直观地找到最需要处理与排查的任务；
  - 任务的排名由任务发现漏洞的风险程度决定：严重漏洞越多，排名越高；严重漏洞相同的任务，高危漏洞越多排名越高；以此类推。

3.1.1.2 结果统计

- 选择聚合维度操作：
  - 用户可以选择展示的维度，其中包含扫描任务、扫描时间、创建用户和组织单位；

- 扫描漏洞信息：

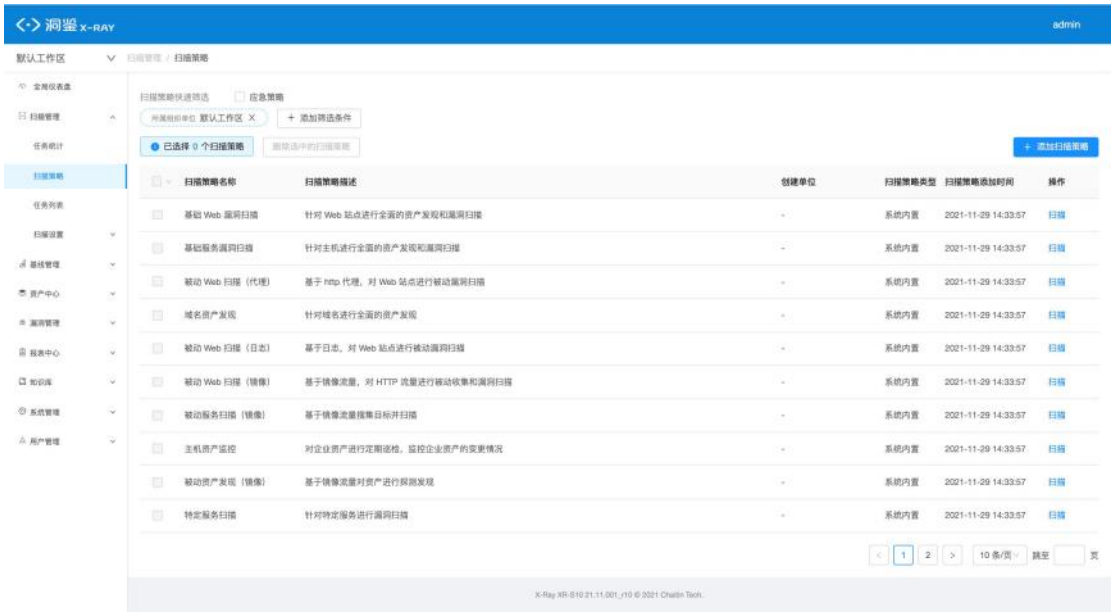
- 统计扫描记录：



- 漏洞列表信息：

3.1.2 扫描策略

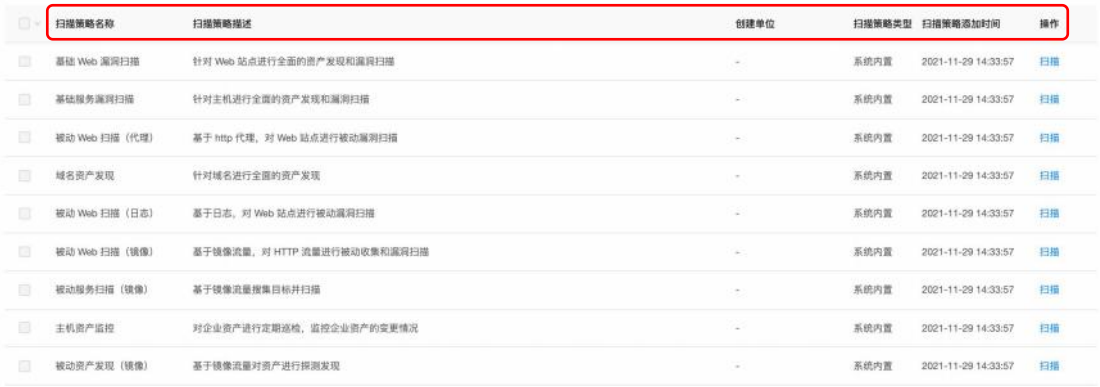
在导航栏中，选择“扫描管理–扫描策略”，进入列表界面。



扫描策略主要用于在创建扫描任务时，提供扫描规则模板，实现一键式便捷快速扫描。扫描策略总体分为以下两类：

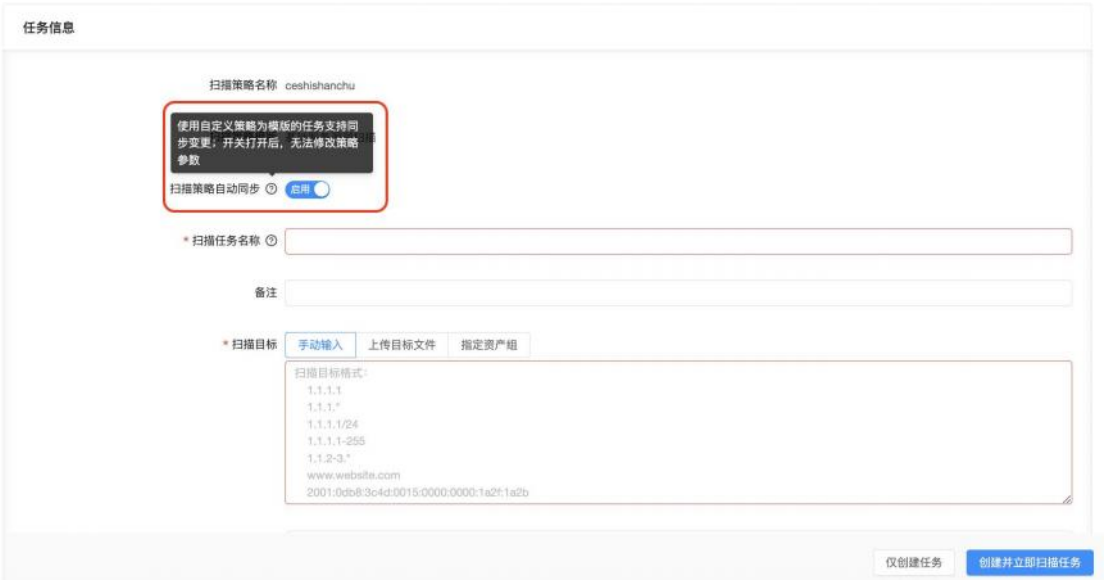
- 系统内置扫描策略：
  - 主机扫描：
    - 主动扫描：基础服务漏洞扫描
    - 被动扫描：被动服务扫描（镜像）
  - Web 扫描：
    - Web 主动扫描：基础 Web 漏洞扫描、逻辑漏洞扫描
    - Web 被动扫描：被动 Web 扫描（代理）、被动 Web 扫描（日志）、被动 Web 扫描（镜像）、 被动 Web 扫描（KafKa）
  - API 扫描：
    - 被动 API 扫描（OpenAPI）
  - 资产发现与监控
    - 域名资产发现
    - 被动资产发现（镜像）
    - 主机资产监控
- 自定义扫描策略
  - 由用户基于系统内置扫描策略，自行配置具体参数而建立

3.1.2.1 内容展示



扫描策略名称	扫描策略描述	创建单位	扫描策略类型	扫描策略添加时间	操作
基础 Web 漏洞扫描	针对 Web 站点进行全面的资产发现和漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
基础服务漏洞扫描	针对主机进行全面的资产发现和漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描（代理）	基于 http 代理，对 Web 站点进行被动漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
域名资产发现	针对域名进行全面的资产发现	-	系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描（日志）	基于日志，对 Web 站点进行被动漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描（镜像）	基于镜像流量，对 HTTP 流量进行被动收集和漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
被动服务扫描（镜像）	基于镜像流量搜集目标并扫描	-	系统内置	2021-11-29 14:33:57	扫描
主机资产监控	对企业资产进行定期巡检，监控企业资产的变更情况	-	系统内置	2021-11-29 14:33:57	扫描
被动资产发现（镜像）	基于镜像流量对资产进行探测发现	-	系统内置	2021-11-29 14:33:57	扫描

当使用自定义扫描策略进行扫描任务时，可开启扫描策略自动同步按钮，开关打开后，无法修改策略参数。



3.1.2.2 快速扫描

- 每个扫描策略后均有“扫描”的操作，可以点击快速创建扫描任务，作为启动任务的快速入口，任务参数配置见 3.1.5 添加扫描任务。

3.1.2.3 筛选操作

通用条件筛选

- 在此页面，可对扫描策略进行筛选操作，可根据扫描策略名称、扫描策略描述、扫描策略类型、扫描策略添加时间，自由添加一个或多个条件进行筛选，筛选条件之间为并集关系。

例如：应急策略筛选

应急策略主要用于新爆发漏洞的检测。对于漏洞爆出后，发布的应急扫描策略一旦在产品上更新，再次直接筛选出来可对应急策略进行编辑，或直接去创建扫描任务。

3.1.2.4 删除操作

- 支持选择一个或多个自定义扫描策略，对已选的自定义扫描策略进行删除操作。系统内置扫描策略不可被删除，用户只能删除自定义扫描策略。

3.1.2.5 添加扫描策略

由扫描策略列表页的“ + 添加扫描策略”进入，可进行自定义扫描策略的添加操作， 具体步骤如下:

- 点击“ + 添加扫描策略”，跳转到添加扫描策略界面；

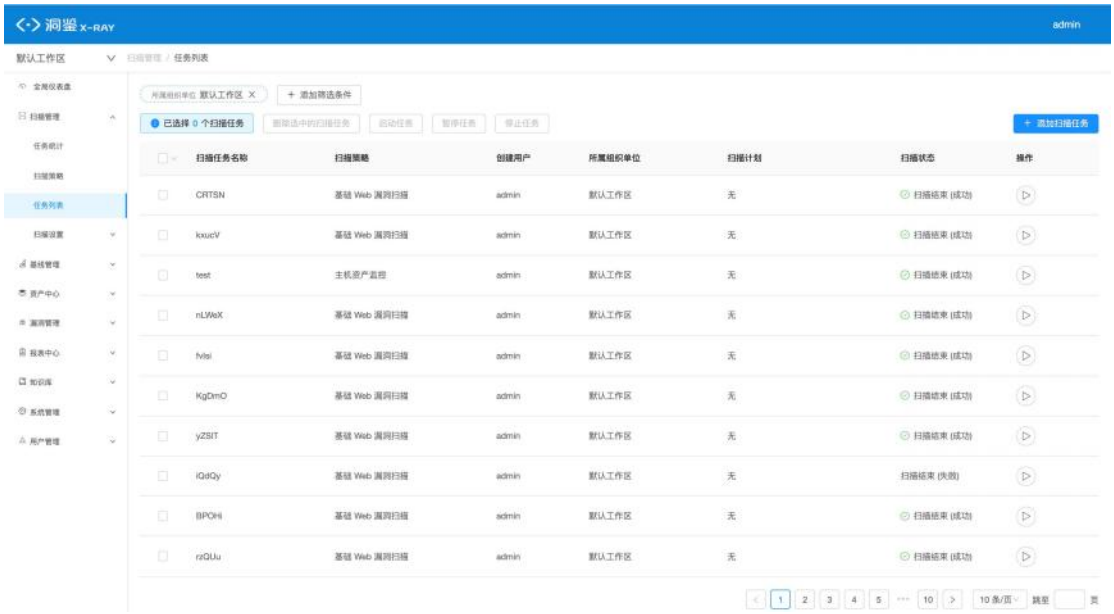
- 配置扫描策略基本信息：
  - 输入扫描策略名称、描述；
  - 选择策略创建单位，默认为当前所在默认工作区；
  - 上传扫描策略图标，默认为洞鉴图标；

- 点击“下一步”，点击选择扫描策略依据的基础策略：
  - 依据的基础策略可以是系统内置扫描策略，也可以是自定义的扫描策略；

- 点击“下一步”，配置扫描策略具体参数
  - 可自行对每一项参数进行设置；
  - 上一步选择不同的基础策略，所需要配置的参数会有所不同，参数配置的详情可以参考 3.1.5 添加扫描任务；
  - 扫描策略默认参数配置完成后，点击“完成”，创建扫描策略成功，可以在扫描策略列表页查看。

3.1.3 任务列表

在左侧导航栏中，选择“扫描管理–任务列表”，进入任务列表界面，展示系统创建的所有扫描任务信息：



3.1.3.1 表头配置

在列表尾部可以对列表表头进行配置操作，可以自定义展示更多信息

3.1.3.2 筛选操作

- 在列表页可对任务进行筛选操作，可根据扫描任务名称、扫描策略、扫描计划、创建时间、下次执行时间、扫描状态、创建用户、所属组织单位，自由添加一个或多个条件进行筛选。

- 若想删除筛选条件，点击已添加条件右侧的“X”按钮，即可删除条件。

3.1.3.3 批量操作

删除操作：

- 在列表页一旦执行删除操作，所有已选任务的记录均将被删除。

启动任务、暂停任务、停止任务

在列表页可以对任务直接进行操作，可进行的操作包括立即扫描与停止扫描。

- 启动任务：对非正在扫描的任务，可以进行立即扫描的操作，具体步骤为：
  - 点击任务右侧操作栏的“启动”按钮，即可进行立即扫描的操作。任务扫描状态变为等待扫描或者正在扫描，操作图标显示“暂停”和“停止”按钮；
  - 进行立即扫描的操作后，任务将按照最新保存的参数配置进行扫描。
  - 注意：系统正在扫描的任务达到了最大并发任务数时，新启动的任务将进入等待扫描状态。

- 暂停任务：对正在扫描的任务，可以进行暂停扫描的操作，具体步骤为:
  - 点击任务右侧操作栏的“暂停”按钮，即可进行暂停扫描的操作。任务扫描状态变为已暂停，操作图标显示“启动”和“停止”按钮；
  - 进行暂停扫描的操作后，任务自动保存当前扫描的进度，以便于后续进行断点续扫。
  - 注意：暂停任务的断点记忆存储没有限制，但需要消耗大量资源。如果是手动暂停的任务，扫描状态显示为“暂停扫描（手动）”，如果是系统因时间设置等原因暂停任务，扫描状态显示为“暂停扫描（系统）”。其中手动操作的优先级高于系统操作。手动暂停后，任务将不会自动启动扫描
- 停止任务：对正在扫描或等待扫描的任务，可以进行停止扫描的操作，具体步骤为:
  - 点击任务右侧操作栏的正方形按钮，显示确认操作的提示弹窗；
  - 点击弹窗中的“确定”，即可完成停止扫描的操作。任务扫描状态变为扫描结束，操作图标显示“启动”按钮。

暂停计划、启用计划

在列表页可以对任务直接进行操作，可进行对选中任务的定时扫描计划的批量暂停和恢复。

- 暂停计划：对任务进行定时扫描计划的暂停，扫描计划暂停后，从下次周期性扫描的时间开始，该任务的计划将不会被执行，处于扫描计划处于已禁用状态

- 启用计划：对任务进行定时计划的再次启用，启用后，扫描计划回复正常

生成报表

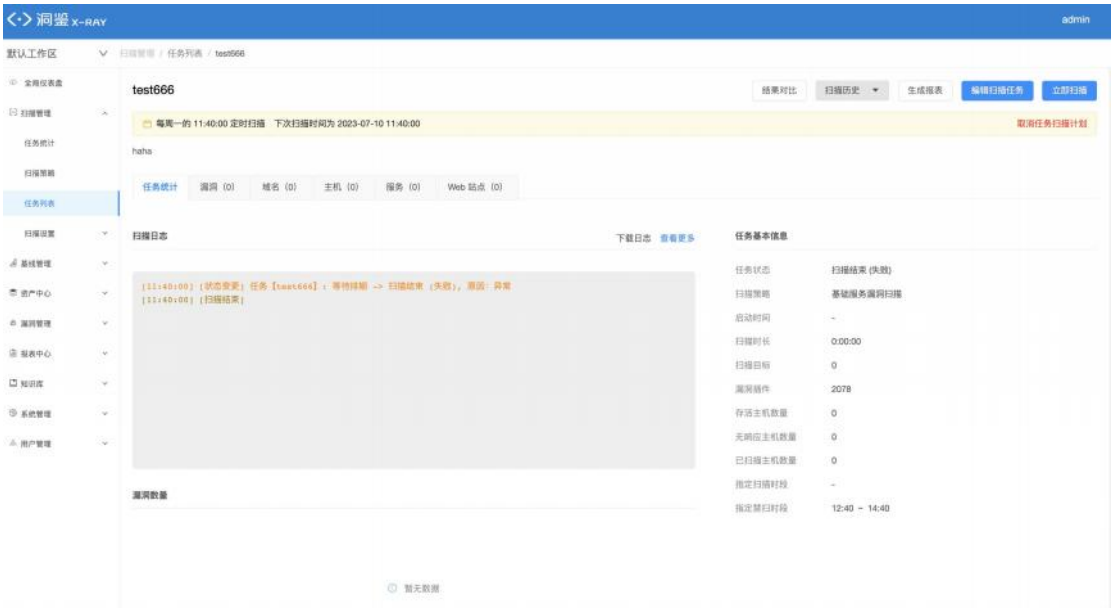
在列表页可以批量选择任务进行生成报表操作。

3.1.3.4 添加扫描任务

点击“添加扫描任务”按钮，选择要使用的扫描策略模板，然后进行任务参数配合，详情见 3.1.5 添加扫描任务 。

3.1.3.5 查看任务详情操作

点击列表上的扫描任务，即打开扫描任务详情页，可看到该任务的详细信息。



在任务详情页可以查看任务执行后的扫描结果，还可对任务进行启动、停止、编辑等操作。

内容展示：

扫描结束的任务详情页面分为任务统计、漏洞列表、资产列表等多个标签页。

1. 扫描进度：

- 任务正在扫描时，页面会展示扫描的进度，任务扫描的阶段根据扫描策略的不同，可能包含信息收集阶段和漏洞探测阶段；
- 界面还将展示最近 30 秒的平均响应时间、最近 30 秒的响应失败率；

- 若扫描进度长时间不增长，且最近 30 秒的平均响应时间较长、响应失败率较高，有可能是系统访问被目标防火墙拦截，建议在任务结束后，检查网络连接、目标防火墙配置是否正常，扫描目标、扫描参数是否填写正确。

2. 任务统计页：

任务统计标签页，展示当次扫描结果的统计信息。

- 扫描日志：任务扫描结束时，页面会展示扫描过程中的日志信息，可供下载和查看，如果出现异常可将日志发送给长亭技术支持获取帮助：

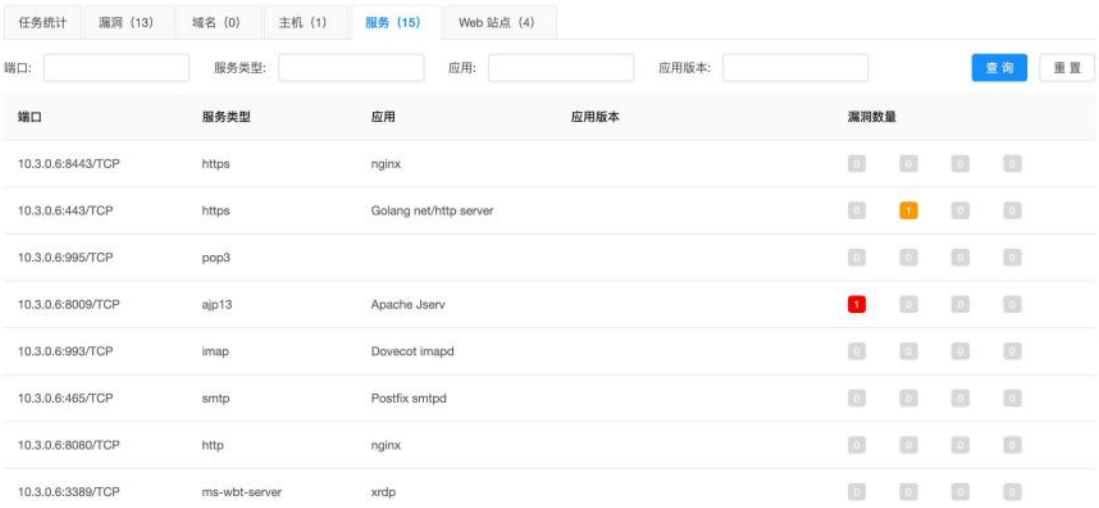
- 漏洞数量
- 漏洞类型分布
- 服务类型分布
- 任务基本信息

3. 漏洞标签页：

4. 域名标签页：

5. 主机标签页:

6. 服务标签页:



7. Web 站点标签页:

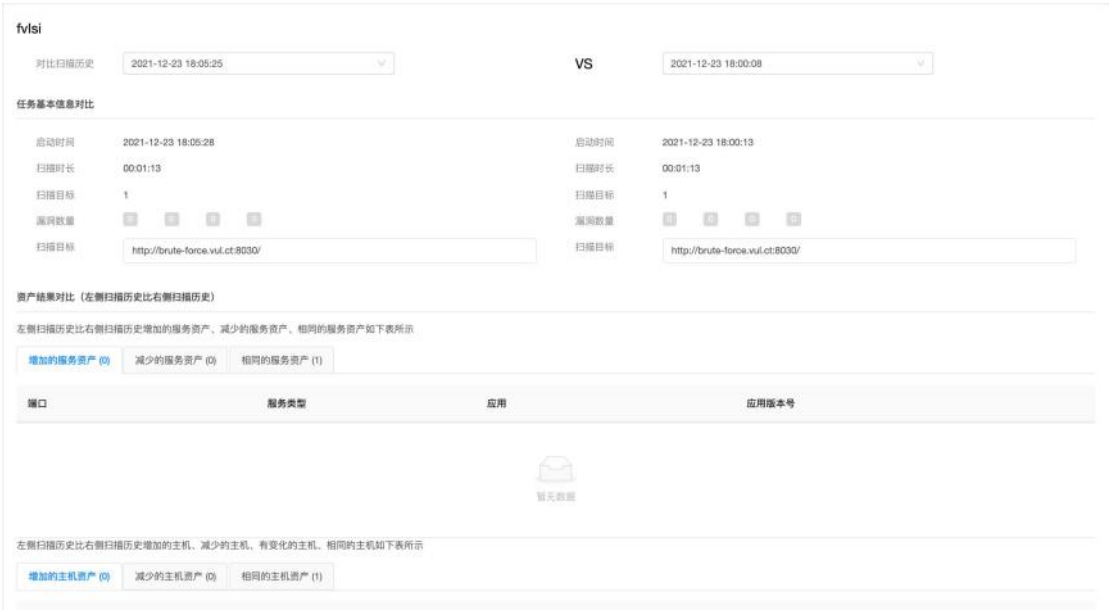
进行操作：

点击任务详情页面顶部的按钮，可以对任务进行一系列的操作。

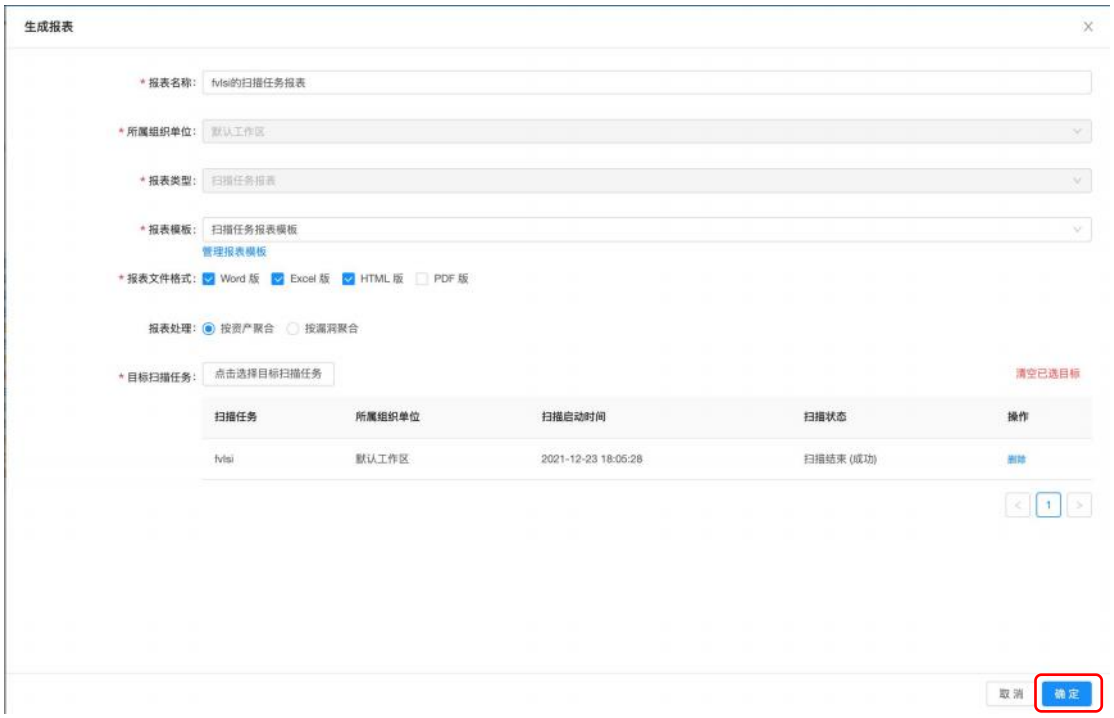
- 若当前任务有定期扫描计划，详情顶部展示，点击可以查看计划详情：

- 查看历史扫描结果：
  - ◆ 从任务列表打开扫描任务详情时，默认展示最近一次扫描的扫描结果

- 结果对比：
  - ■ 点击结果对比按钮，跳转到结果对比页面，默认显示最近两次扫描的对比结果；

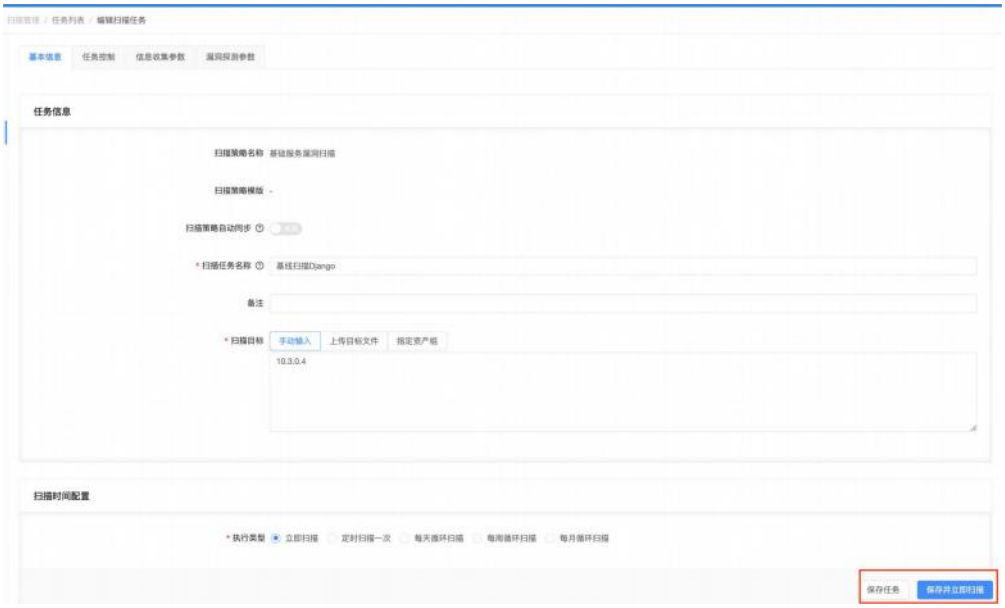


- 生成报表：
  - ◆ 在任务详情页可以直接生成该任务(在当前扫描历史下)的报告；报告中不包含被标记为“误报”的漏洞；正在扫描中的任务无法生成报告。可以选择等待任务结束、停止任务，或是选择任务一个以往的扫描历史生成报告。



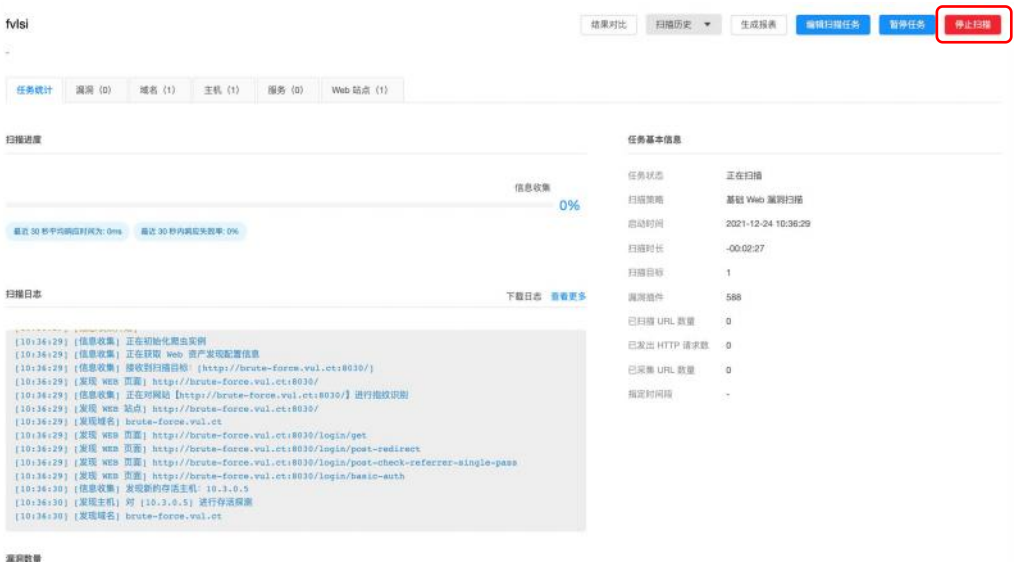
- 快速深度扫描：
  - 用于将任务的扫描结果作为目标进行快读扫描；
  - 点击后选择一种扫描模式，然后可以快速选择扫描策略进行扫描。

- 编辑扫描任务：
  - 在任务详情页可以修改扫描任务的参数配置，编辑扫描任务的方法与添加扫描任务基本相同，除了任务的扫描策略不可编辑，其他的一切都可以编辑。

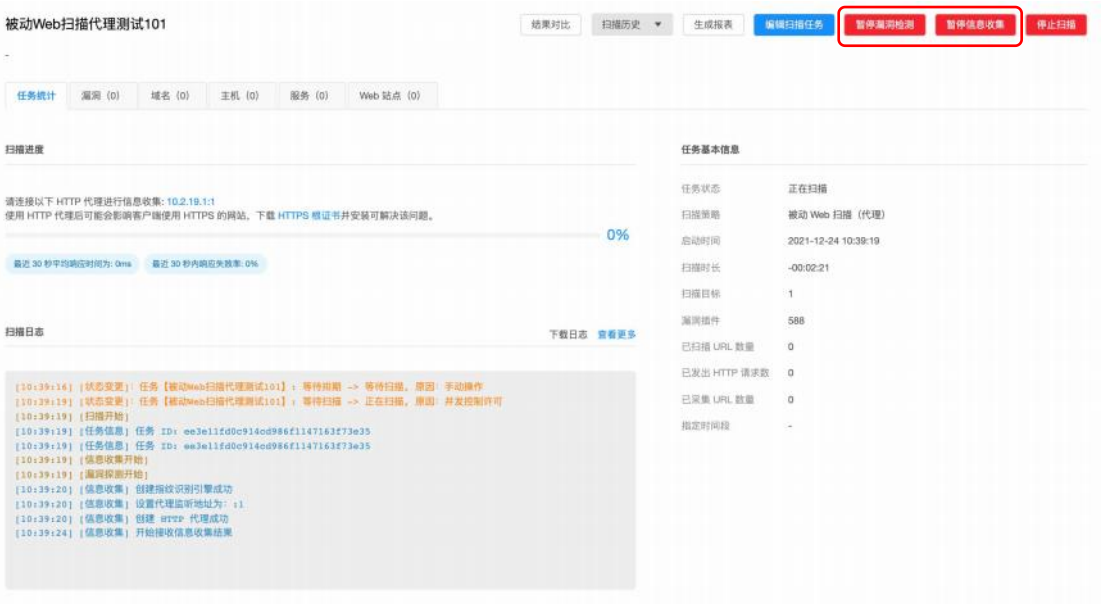


- 立即扫描：
  - 启动后，任务可能立即开始扫描，也可能进入等待扫描。这取决于系统当前正在扫描的任务数量，是否达到了系统的最大任务并发数。

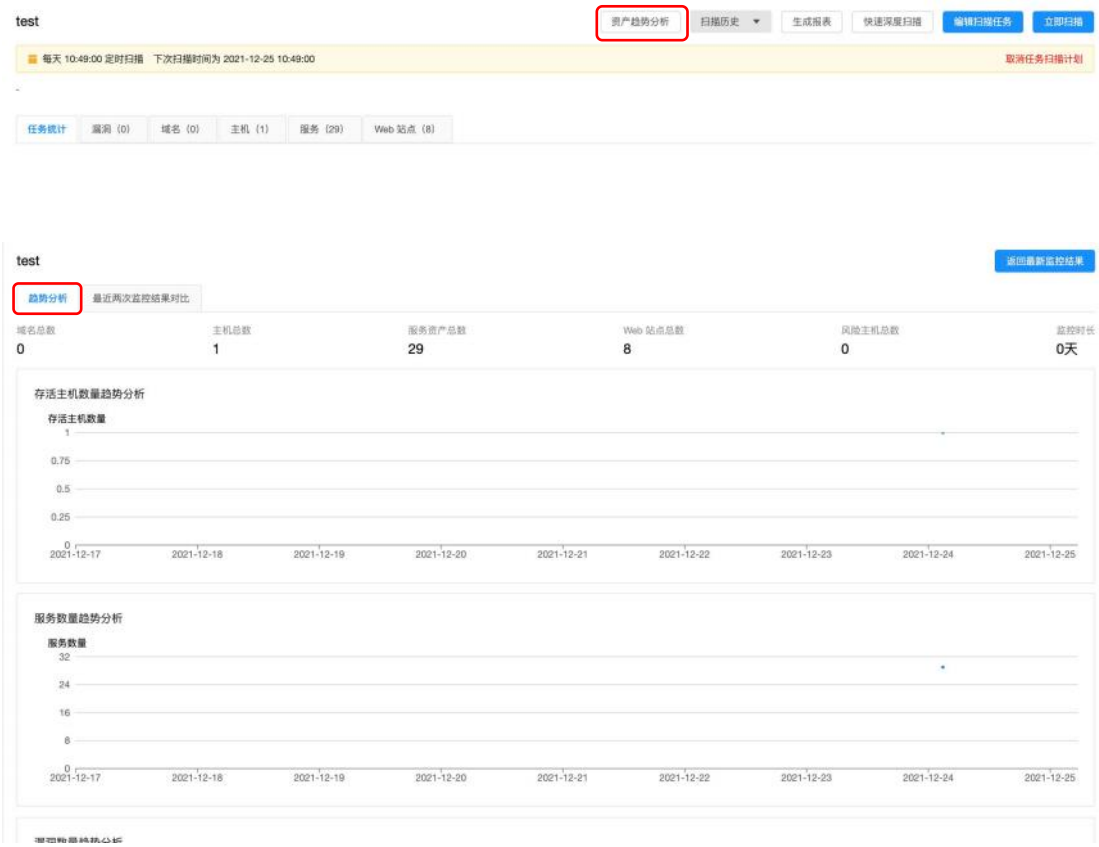
- 停止扫描：

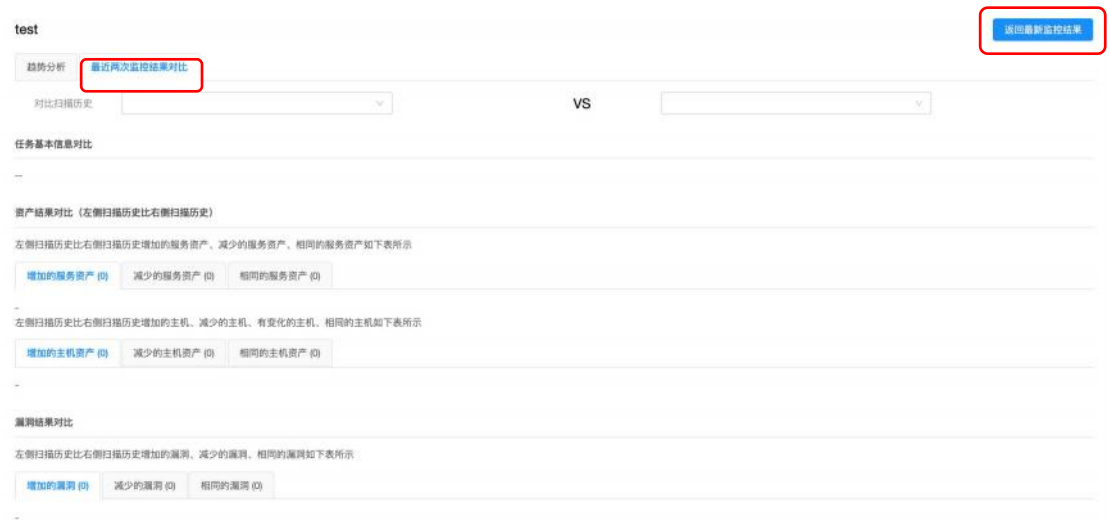


- 暂停漏洞检测【被动 Web 扫描（代理/日志）特有操作】：
  - 暂停漏洞检测，系统只进行信息收集，不进行漏洞检测；
  - 暂停信息收集，系统会继续检测漏洞，但不会进行信息收集；
  - 继续漏洞检测，可恢复漏洞扫描引擎工作。



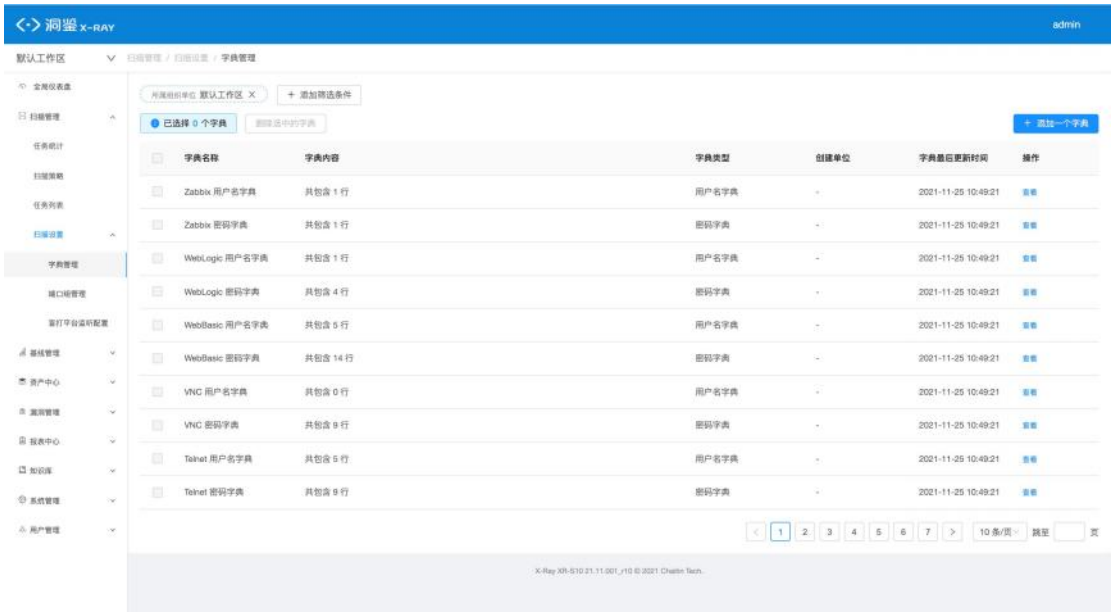
- 资产趋势分析【主机资产监控特有操作】：
  - 正在扫描的任务展示发现资产的趋势分析结果与最近两次监控结果的对比
  - 展示最近 9 天的存活主机数量趋势分析、服务数量趋势分析、不同风险等级的漏洞数量趋势分析
  - 点击右上角的返回最新监控结果跳转到详情页展示内容在扫描结束的任务详情基础上多出扫描进度


test
资产趋势分析
扫描历史
生成报表
快速深度扫描
编辑扫描任务
立即扫描
每天 10:49:00 定时扫描 下次扫描时间为 2021-12-25 10:49:00
取消任务扫描计划
任务统计
漏洞 (0)
域名 (0)
主机 (1)
服务 (29)
Web 站点 (8)
test
返回最新监控结果
趋势分析
最近两次监控结果对比
域名总数
0
主机总数
1
服务资产总数
29
Web 站点总数
8
风险主机总数
0
监控时长
0天
存活主机数量趋势分析
存活主机数量
1
0.75
0.5
0.25
0
2021-12-17
2021-12-18
2021-12-19
2021-12-20
2021-12-21
2021-12-22
2021-12-23
2021-12-24
2021-12-25
服务数量趋势分析
服务数量
32
24
16
8
0
2021-12-17
2021-12-18
2021-12-19
2021-12-20
2021-12-21
2021-12-22
2021-12-23
2021-12-24
2021-12-25


test
返回最新监控结果
趋势分析
最近两次监控结果对比
对比扫描历史
VS
任务基本信息对比
资产结果对比（左侧扫描历史比右侧扫描历史）
左侧扫描历史比右侧扫描历史增加的服务资产，减少的服务资产，相同的服务资产如下表所示
增加的服务资产 (0)
减少的服务资产 (0)
相同的服务资产 (0)
左侧扫描历史比右侧扫描历史增加的主机、减少的主机、有变化的主机、相同的主机如下表所示
增加的主机资产 (0)
减少的主机资产 (0)
相同的主机资产 (0)
漏洞结果对比
左侧扫描历史比右侧扫描历史增加的漏洞，减少的漏洞，相同的漏洞如下表所示
增加的漏洞 (0)
减少的漏洞 (0)
相同的漏洞 (0)

3.1.4 扫描设置

在左侧导航栏中，选择“扫描管理–扫描设置”，选择要设置的方向，进入对应的界面。

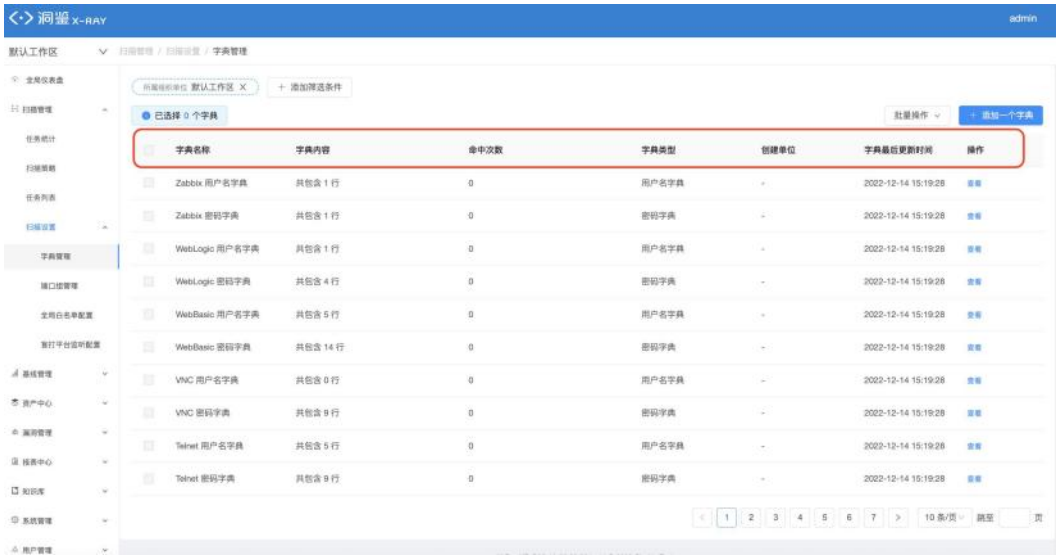


3.1.4.1 字典管理

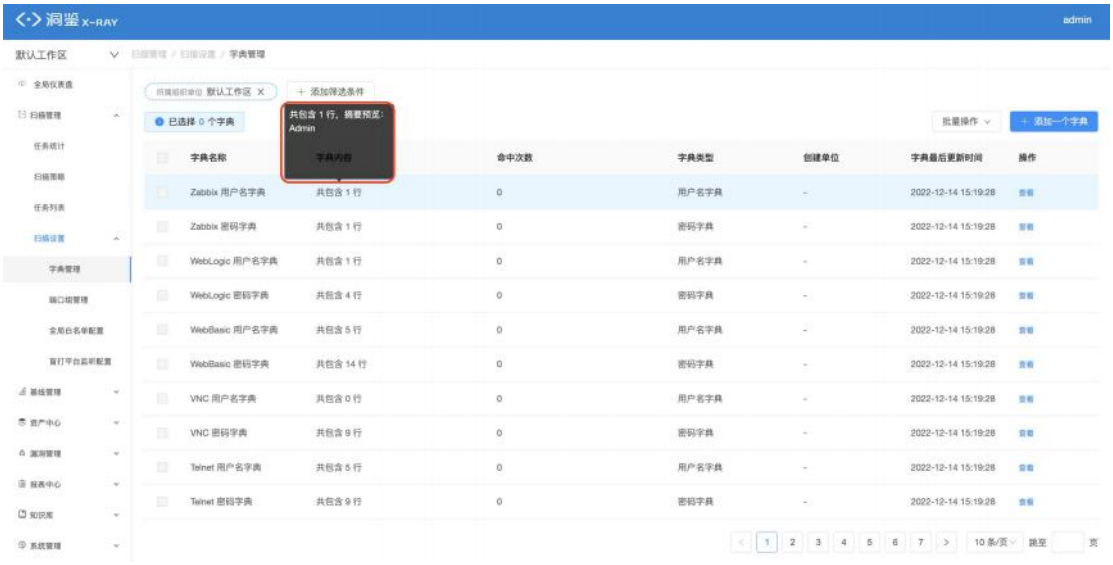
字典可以方便您更好地通过添加自定义字典进行扫描过程的定制。

内容展示：

字典列表为您展示所有字典的基本信息：



- 字典内容，展示字典内容的总行数：



查看字典：

在字典管理页面可点击字典条目查看字典内容；可以一键复制字典内容；对字典的命中次数进行清零操作。

筛选字典：

- 在字典管理页面可顶部可以添加筛选条件并保存，筛选维度为字典名称、所属组织单位、字典类型与字典最后更新时间；可以在页面顶部或者筛选弹窗中删除已经设定的筛选条件

添加字典：

在字典管理页面可以添加字典。

- 填写、选择、上传字典的具体信息如图：字典名称是字典的标识，不能和已有的字典名称重复；上传字典文件大小不能超过 10M；

删除字典：

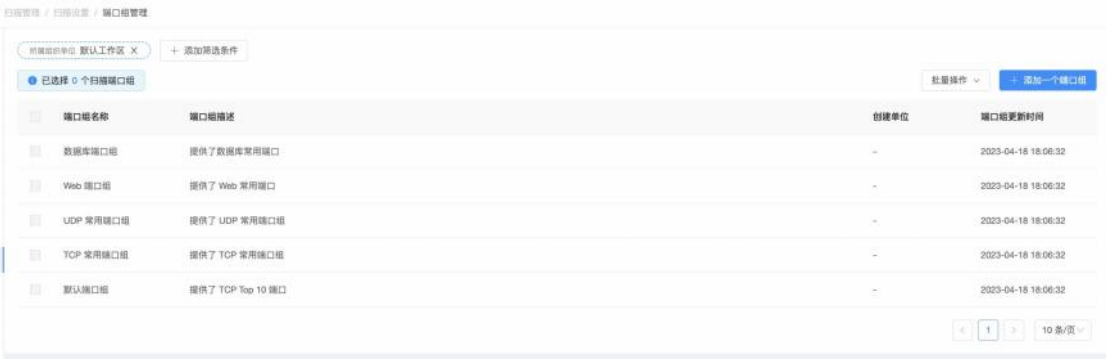
- 在字典管理页面可以批量删除已有的字典。

编辑字典：

- 自定义的字典可以进行编辑操作：字典内容支持空格或空行为空口令，如果输入多个空行，点击确定后只保留第一个空行为空口令。

3.1.4.2 端口组管理

端口组可以方便您更好地进行扫描过程的端口组的定制，您可以在此处进行端口组的预览、添加和删除。



内容展示：

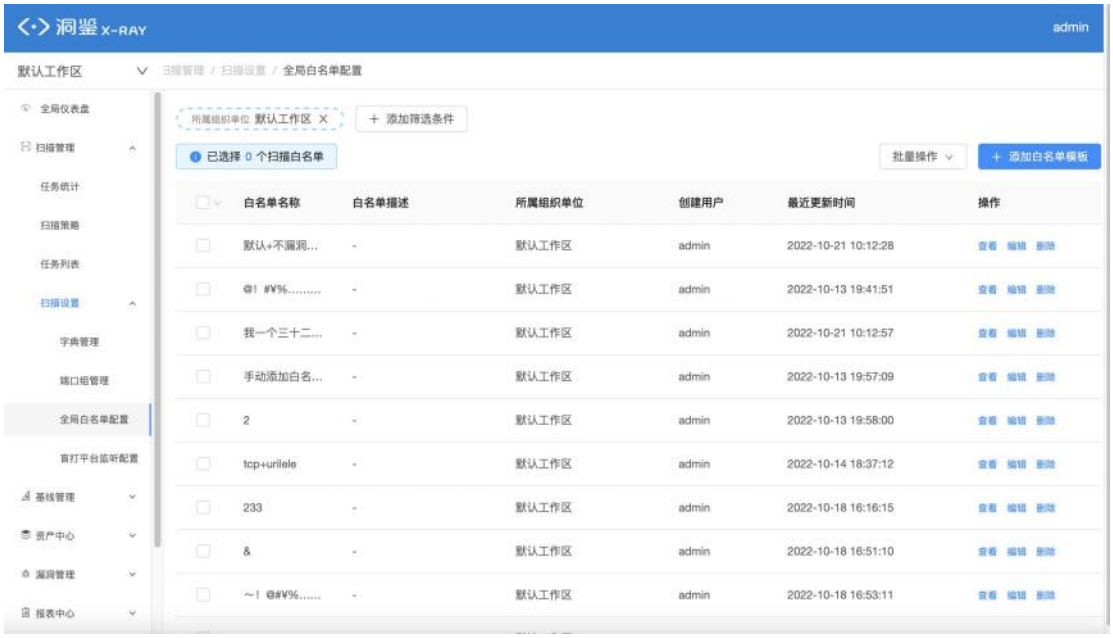
端口组列表为您展示所有端口组的名称，端口组描述、创建单位、端口组更新时间。对端口组列表可进行筛选、删除和编辑操作。注意：内置的端口组不可编辑和删除。

添加端口组：

- 在扫描端口组列表页面，可以添加自定义的端口组。
- 端口组名称，添加或编辑主机扫描任务时，若要从端口组添加需要扫描的端口，端口组名称是用户能够看到的唯一信息，请务必填写一个容易分辨的端口组名称；
- tcp /udp 端口组，端口组中包含的 tcp/udp 端口：
  - 可以输入单个端口或端口段，如:80，10–20；也可同时填写多个端口或端口段，端口或端口段之间换行分隔，如下图中所示：

3.1.4.3 全局白名单配置

全局白名单配置页面可以添加配置和管理可应用于多个不同任务的全局白名单，可对添加的白名单进行查看、编辑、删除操作



添加白名单：

可以添加白名单名称、描述、所属组织单位、信息，导入或者添加想要规避的扫描目标。注意只能导入所属组织单位以及其子单位的主机/Web 资产。同时可以编辑规避扫描的 URL 关键字。保存后可以应用到扫描任务。

全局白名单应用于全局：

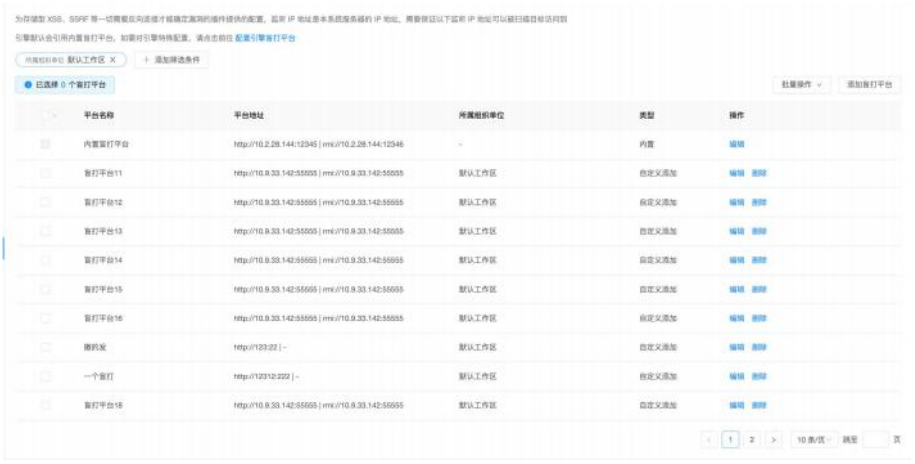
“应用配置”开启后，该工作区的任务会在下一次扫描时应用全局配置，勾选“同步应用到子工作区”可将此全局白名单配置同步应用到子工作区。若当前开启了全局白名单的应用配置，那么该版本后创建的任务首次/再次开启扫描任务时，会应用全局配置。一个工作区可存在多个全局白名单，支持开启多个，支持任务应用多个。

3.1.4.4 盲打平台监听配置

部分插件需要反向连接才能够确定漏洞，如存储型 XSS、文件上传、SSRF 等。此处可以为这类插件提供监听 IP 的配置，分为内置盲打平台和外链盲打平台。

内置盲打平台配置：

如果扫描目标与洞鉴服务器可以互相通信，那么仅需配置内置盲打平台即可。此处监听 IP 地址是洞鉴服务器的 IP 地址。



配置内置盲打平台 IP 地址：

初次配置监听 IP 的步骤如下:

- 确认洞鉴服务器的地址，保证可以被扫描目标访问到，作为内置盲打平台 IP 地址；
- 在盲打平台监听配置处，输入 IP 地址。

修改内置盲打平台 IP 地址：

“编辑”操作可修改内置盲打平台的 IP 地址。

外链盲打平台配置：

如果扫描目标与洞鉴服务器不能互相通信，则需要在与两者都可通信的地方自行部署盲打平台，并在此进行配置。

添加外链盲打平台：

- 点击“添加盲打平台”，填写以下相关信息（token、HTTP 服务、RMI 服务 的配置参数见下文中的“外链盲打平台部署说明”）：
  - 盲打平台名称：用于扫描任务配置的选项；
  - 组织单位：仅该组织单位下的用户可在扫描任务配置中使用该盲打平台；仅该组织单位的负责人能够编辑和删除已添加的外链盲打平台；
  - 通信 token：作为通信认证依据；
  - HTTP 服务:按照提示格式填写 http 服务通信地址；
  - RMI 服务:按照提示格式填写 RMI 服务通信地址。
  - DNS 配置
    - DNS 服务器域名
    - DNS 服务器 IP

修改外链盲打平台：

权限说明：编辑和删除仅限该盲打平台所属工作区的负责人操作。

- 同修改内置盲打平台，点击操作列的“编辑”按钮，即可修改。

外链盲打平台部署说明：

外链盲打平台使用步骤：

- 下载盲打平台客户端(联系技术支持人员获取)，在需要部署的服务器上启动；
- 通过命令行，启动盲打平台的 http、rmi、dns 服务，设置通信 token；
- 在洞鉴系统上，“扫描管理–扫描配置–全局配置”处，添加外链盲打平台，并将 2 中设置的 http、rmi、dns 和 token 按规定格式填写并保存；
- 创建扫描任务时，盲打平台配置处启用上述设置的盲打平台即可。

启动服务使用说明：

```
GLOBAL OPTIONS:
   --http-listen value   start a http reverse service, eg. 127.0.0.1:1111
   --rmi-listen value    start a rmi reverse service, eg. 127.0.0.1:2222
   --server-ip value     IP address of the server, used to configure dns
   --domain value        dns domain, eg. xxxxx.com
   --domain-name-server  Whether to set the server to name server
   --token value         reverse service token
   --dbpath value        set the db path
   --config FILE         load config from FILE
   --version, -v         print the version
```

样例说明：

只启动 http 服务的反连平台

```
./reverse --http-listen 0.0.0.0:1111 --token aabb
```

启动 http 和 rmi 服务

```
./reverse --http-listen 0.0.0.0:1111 --rmi-listen 0.0.0.0:1099 --token
aabb
```

手动设置数据存储位置

```
./reverse --http-listen 0.0.0.0:1111  --token aabb --dbpath ./save.db
```

由于现在添加了 DNS 的配置，所以推荐使用配置文件进行启动，启动样例如下：

```
./reverse --config conf.yaml --dbpath a.db
```

其中 conf.yaml 的内容如下：

```
reverse:
  reverse_token: "aabb"
  http_reverse_port: "1111"
  rmi_reverse_port: "1099"
  dns_reverse_domain: "xxxxx.com"
  is_domain_name_server: true
  server_ip: "0.0.0.0"
```

当然也可以使用如下参数命令行启动：

```
./reverse --http-listen 0.0.0.0:1111 --domain xxxxx.com --domain-name-server true --token aabb
```

其中的 domain 是准备好的反连的配置好的域名，domain-name-server 的参数配置是代表是否修改了域名的 ns 为反连平台，如果是，那 nslookup 等就不需要指定 dns 了，也就是可以直接 ping+域名进行漏洞验证。

dns 反连平台配置准备工作：

云服务器

Ubuntu 20.04

安全策略：开启反连平台对外端口，开启 53 端口（UDP 协议）

也就是修改安全组策略，将 53 端口开放，　　注意，协议类型一定要是 UDP

然后将需要对外开放的，部署反连平台的端口进行开放，比如 8777，　注意，该端口的协议类型是 TCP

解决 53 端口被 systemd-resolve 占用的问题

首先使用以下命令确认端口占用情况

sudo netstat -nultp

在确认被占用后，可以执行如下命令停用 systemd-resolved

sudo systemctl stop systemd-resolved

编辑 resolved.conf

sudo vim /etc/systemd/resolved.conf

将文件中的对应内容改为如下内容

```
[Resolve]
DNS=x.x.x.x              #取消注释，增加 dns，此处的值可以填写你的云服务器公网 IP
#FallbackDNS=
#Domains=
#LLMNR=no
#MulticastDNS=no
#DNSSEC=no
#DNSOverTLS=no
#Cache=no-negative
DNSStubListener=no       #取消注释，把 yes 改为 no
#ReadEtcHosts=yes
```

修改完成后运行如下命令即可解除占用

sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf

域名

以下的 ip 请替换为准备好的云服务器的公网 ip

1. 仅配置如图所示的内容：

主机记录	记录类型	线路类型	记录值	权重	MX	TTL	最后操作时间	操作
ns1	A	默认	8.130.41.223	-	-	600	2022-10-18 11:34:53	SSL
ns2	A	默认	8.130.41.223	-	-	600	2022-10-18 11:34:52	SSL

不做其他任何变动，同时配置文件填写好，在启动后，支持 http/rmi 的反连，dns 仅支持在使用 dig 或者 nslookup 时，指定 IP 解析的情况下，接收到请求。

也就是说，执行 ping/curl 命令时，反连平台并没有办法收到 dns 解析记录。

如果想要让反连平台的 dns 功能也正常工作，应进行如下操作：

腾讯云

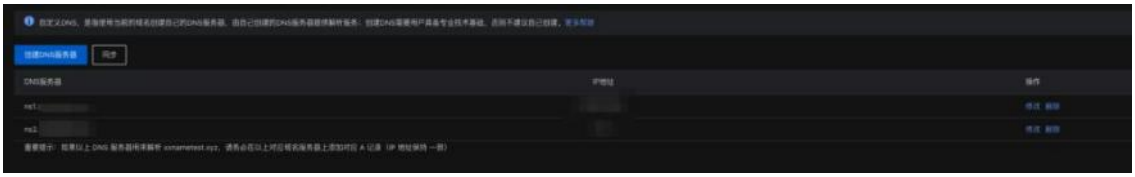
1. 自定义 DNS Host

2. 修改域名的 DNS 解析

3. 修改完成后，需要 10 分钟到几小时不等的时间生效，时间越久，部署效果越好

阿里云

1. 自定义 DNS Host



2. 修改域名的 DNS 解析

准备好后，即可将工具上传上去，将准备好的域名填写上去即可

注意事项：

- http 服务必须启动，由于远程 server 通过 http 服务来做数据交换，不设置会直接报错；
- token 需要保持和服务端一致，这样才能正常通信；
- dbpath 如果没有指定，会将数据存在临时文件内，它是一个简单的 kv 数据库，其作用是用来存储反连数据，可以做数据持久化。

3.1.5 添加扫描任务

添加扫描任务入口：

- 在扫描任务列表页点击 " + 添加扫描任务"，即可添加一个扫描任务。
- 在扫描策略列表，每个扫描策略右侧，点击“扫描”，即可快速创建一个扫描任务。
- 在资产列表中，选中多个主机资产/web 站点/资产组，可针对特定的资产下发扫描任务。
- 在知识库-漏洞库中，选中多个漏洞，可针对特定的漏洞类型下发扫描任务。

扫描参数配置：

详情见对应的以下各个扫描策略模板参数配置说明

Web 漏洞扫描：

- 主动 Web 扫描：
  - 基础 Web 漏洞扫描–模板参数配置
- 被动 Web 扫描：
  - 被动 Web 扫描（代理）–模板参数配置
  - 被动 Web 扫描（日志）–模板参数配置
  - 被动 Web 扫描（镜像）–模板参数配置
  - 被动 Web 扫描（kafka）–模版参数配置
  - 被动 Web 扫描（burp）–模板参数配置

系统漏洞扫描：

- 主动系统漏洞扫描：
  - 基础服务漏洞扫描–模板参数配置
  - 特定服务扫描–模板参数配置
- 被动系统漏洞扫描：
  - 被动服务扫描(镜像)–模板参数配置

资产发现与监控：

- 主机资产监控–模板参数配置
- 域名资产发现–模板参数配置
- 被动资产发现（镜像）–模板参数配置

逻辑漏洞扫描：

- 逻辑漏洞扫描–模版参数配置

参数配置完成添加任务

- 扫描任务参数配置完成后，点击“创建并立即扫描任务”或“仅创建任务”，即 可完成扫描任务的添加：
- 若点击“创建并立即扫描任务”，则创建任务，同时会立即按配置好的参数 扫描任务
- 若点击“仅创建任务”，则仅创建任务，但不做扫描操作

由资产批量添加扫描任务

由资产批量添加扫描任务时，系统会根据资产所在的组织单位，自动分配对应可选的引擎节点，并只提供快速下发入口（无法配置详细参数）。

3.1.5.1 基础 Web 漏洞扫描

可对 Web 站点进行基础主动的漏洞扫描。

- 扫描目标：Web 站点地址。
- 适用场景：需要对特定的 Web 站点资产进行基础的风险检测。

基本信息

- 任务信息
- 扫描时间配置
- 全局白名单选择
- 引擎节点选择

任务控制

- 扫描优先级
- 扫描任务限制
- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知

- 扫描结果处理方式

信息收集参数

- HTTP 请求配置
- HTTPS 客服端证书
- HTTP 基础认证
- Web 表单登录
- 网站可用性验证
- Web 爬虫
- 目标采集文件
- 自定义路径猜解字典
- 启用自定义指纹

漏洞探测参数

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令配置
- 自定义路径猜解字典
- URL 去重设置

3.1.5.2 被动 Web 扫描（代理）–模板参数配置

可对 Web 站点进行漏洞扫描，在收集扫描目标的同时，进行漏洞检测。

- 扫描目标：Web 站点地址。

- 适用场景：需要对特定的 Web 站点资产进行更加精准的风险检测，比如：
  - 需要扫描到不容易自动爬虫到的独立页面、API 接口等信息；
  - 需要扫描到经过复杂交互，如输入特定口令才能获取的页面信息；
  - 需要根据企业业务流程，定制精准的 payload 进行测试。

基本信息

- 任务信息
- 通用数据来源
- 引擎节点选择
- 全局白名单选择

任务控制

- 扫描任务限制
- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- HTTPS 客服端证书
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注：被动 Web 漏洞扫描（代理）任务创建后，使用方法和其他任务也有所不同。更多详情，可参见下文“3.1.7 代理服务器配置方法”。

3.1.5.3 被动 Web 扫描（日志）–模板参数配置

可对 Web 站点进行漏洞扫描，在收集扫描目标的同时，进行漏洞检测。

- 扫描目标：日志文件中的内容。
- 适用场景：对日志文件进行解析扫描。

基本信息

- 任务信息
- 日志信息采集
- 引擎节点选择
- 全局白名单选择

任务控制

- 扫描任务限制
- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注意：要创建被动 Web 扫描（日志）任务，需要先在“系统管理 / 其他扫描配置 / 被动爬虫服务器配置”处，配置好 syslog 服务器地址。

3.1.5.4 被动 Web 扫描（镜像）–模板参数配置

该扫描策略基于 Web 的镜像流量进行扫描

- 扫描目标：交换机上镜像的流量，仅在硬件版上生效
- 使用场景：基于镜像流量，对 HTTP 流量进行被动收集和漏洞扫描

流量采集基础设置

- 任务信息
- 全局白名单选择
- 流量信息采集
- 引擎节点选择

流量采集高级设置

- 采集信息设置
- HTTP 客户端限制
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

流量漏洞扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

3.1.5.5 被动 Web 扫描（流量）-模版参数配置

可对 Web 站点进行漏洞扫描，在收集扫描目标的同时，进行漏洞检测。

- 扫描目标：流量数据中的内容。该策略在软件版上生效。
- 适用场景：对流量数据进行解析扫描。

基本信息

- 任务信息
- 全局白名单选择
- 通用数据来源
- 引擎节点选择

任务控制

- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注：要创建 被动 Web 扫描（流量）任务，需要借助流量被动扫描工具。

3.1.5.6 被动 Web 扫描（kafka）—模版参数配置

可对 Web 站点进行漏洞扫描，在收集扫描目标的同时，进行漏洞检测。

- 扫描目标：kafka 数据中的内容。
- 适用场景：对 kafka 数据进行解析扫描。

基本信息

- 任务信息
- 全局白名单选择
- 通用数据来源
- 引擎节点选择

任务控制

- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注：要创建 被动 Web 扫描（kafka）任务，需要借助 kafka 被动扫描工具。

3.1.5.7 被动 Web 扫描（burp）—模板参数配置

可对 Web 站点进行漏洞扫描，在收集扫描目标的同时，进行漏洞检测。类似被动 Web 扫描（日志）策略。

- 扫描目标：burp 中的内容。
- 适用场景：对 burp 文件进行解析扫描。

基本信息

- 任务信息
- 全局白名单选择
- 目标采集
- 引擎节点选择

任务控制

- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

3.1.5.8 基础服务漏洞扫描-模板参数配置

可对服务进行基础的漏洞扫描。

- 扫描目标：主机 IP 地址、域名。
- 适用场景：需要对特定主机上的服务进行风险检测。

基本信息

- 任务信息
- 全局白名单选择
- 引擎节点选择
- 扫描时间配置

任务控制

- 扫描任务限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

信息收集参数

- HTTP 请求配置
- 主机存活探测
- TCP 协议扫描
- UDP 协议扫描
- 其他检测选项
- 启用自定义指纹

漏洞探测参数

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令配置

3.1.5.9 特定服务扫描–模板参数配置

可对指定的服务资产进行批量漏洞扫描。

- 扫描目标：端口服务。
- 适用场景：需要对特定服务进行风险检测，尤其是针对性的应急漏洞检测。

基本信息

- 任务信息
- 全局白名单选择
- 引擎节点选择
- 扫描时间配置

任务控制

- 扫描任务限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

信息收集参数

- 主机存活探测
- TCP 协议扫描
- UDP 协议扫描
- 其他检测选项
- 启用自定义指纹

漏洞探测参数

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令配置

3.1.5.10 被动服务扫描(镜像)–模板参数配置

基于镜像流量，对企业资产进行全面的收集与发现，进而对资产进行风险评估。

- 扫描目标:交换机上镜像的流量
- 适用场景:不知道自己有什么资产，需要摸清家底，并且进行风险检测，且可以提供镜像口的场景。

流量采集基础信息

- 任务信息
- 流量信息采集
- 引擎节点选择

流量采集高级设置

- 采集信息设置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

漏洞扫描配置

- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典

3.1.5.11 主机资产监控–模板参数配置

主要对系统服务进行扫描并监控动态。

- 扫描目标：主机 IP 地址、域名。
- 适用场景：对企业系统资产进行定期巡检，监控资产的变更和风险情况。

基本信息

- 任务信息
- 全局白名单选择
- 引擎节点选择
- 监控频率及时间设置（与扫描时间设置类似，但无立即扫描）

任务控制

- 扫描任务限制
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

监控信息设置

- 监控端口范围
- 监控白名单配置
- 监控内容设置

漏洞探测参数

- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典

3.1.5.12 域名资产发现-模板参数配置

可针对域名进行全面的资产发现。

- 扫描目标：域名。
- 适用场景：需要对拥有的资产进行大面积的发现，以方便后续的风险评估和资产管理。

基本信息

- 任务信息
- 引擎节点选择

任务控制

- 扫描任务限制
- 单个扫描目标限制
- DNS 解析配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- 自定义域名猜解字典
- 其他检测选项

3.1.5.13 被动资产发现（镜像）—模板参数配置

基于镜像流量，对企业资产进行全面的收集与发现。

- 扫描目标：交换机上镜像的流量。
- 适用场景：不知道自己有什么资产，需要摸清家底，且可以提供镜像口的场景。

流量采集基础设置

- 任务信息
- 流量信息采集

流量采集高级设置

- 采集信息设置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

3.1.5.14 逻辑漏洞扫描-模版参数配置

基本信息

- 任务信息
- 全局白名单选择
- 逻辑漏洞权限配置
- 引擎节点选择

任务控制

- 扫描任务限制
- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

3.1.5.15 被动 API 扫描（Open API）

基于 Swagger，收集 API 信息，对其进行漏洞扫描。

- 扫描目标：Swagger 链接或 json 文件。
- 适用场景：对 Swagger 进行解析扫描。

基本信息

- 任务信息
- 信息收集
- 全局白名单选择
- 引擎节点选择

任务控制

- 扫描优先级
- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

特殊说明：

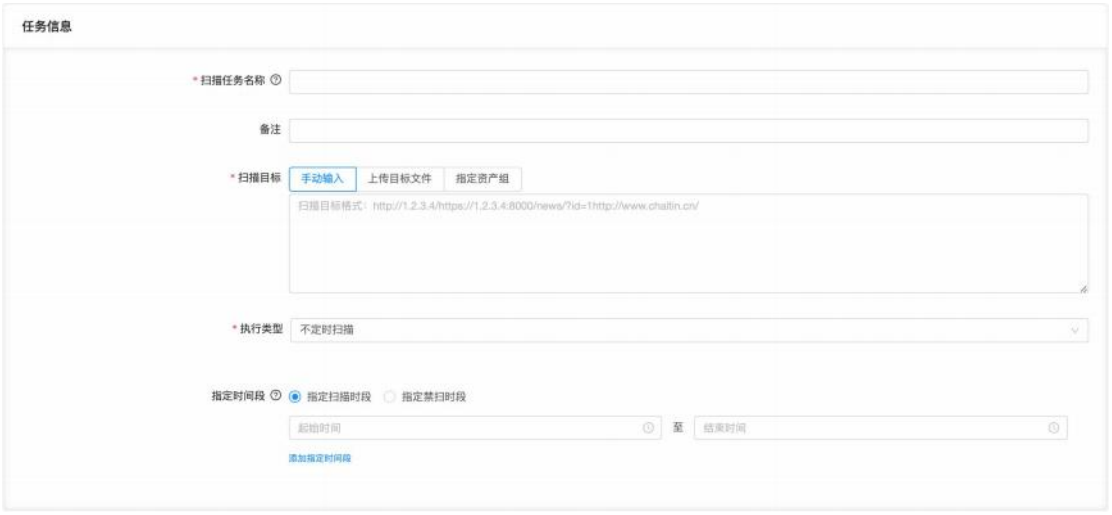
若调用接口中存在认证限制，需要在 HTTP 请求配置中增加自定义 http headers，此时请求中会带着认证进行接口调用测试

部分目标接口若存在修改数据库的情况，需要在扫描白名单配置中过滤对应的请求方式或接口路径，以避免对生产数据造成篡改的风险

优先使用文件上传的方式，以确保扫描目标可通

3.1.6 配置参数模块

3.1.6.1 任务信息



- 扫描任务名称：1–255 个字符
  - 扫描任务名称会显示在任务列表上，也可以用于筛选；
- 备注：
  - 显示在扫描任务详情页
- 注：被动 Web 扫描（镜像），被动服务扫描（镜像），被动资产扫描（镜像）不包含以下参数项。
- 扫描目标：
  - 输入该任务需要扫描的目标
  - 手动输入：
    - 支持输入多个目标，多个目标以换行分隔。
  - 上传目标文件：
    - 支持上传单个目标文件：
      - 目标文件为 .txt 格式，内容和手动输入要求相同：每行包含一个目标，换行分隔多个目标；
      - 目标文件为 .csv 格式，用于配置批量主机登录信息，每行包含一个目标，以及登录方式信息。
    - 目标文件上传后，如果有异常目标，会显示异常结果的提示。包含有误的目标、出现在的上传文件的文件名、目标的行数、错误的原因。如有误，需要修改后重新上传添加。

- 指定资产组：
  - 点击“ + 选择资产组”，打开弹窗，可以选择想要添加的资产组；
  - 可选择多个资产组。
  - 注：被动 Web 扫描（代理），特定服务扫描，主机资产监控，域名资产扫描，逻辑漏洞扫描不可进行指定资产组操作。
- 注：被动 Web 扫描（日志），被动 Web 扫描（流量），被动 Web 扫描（kafka），被动 Web 扫描（burp）不需添加扫描目标。

3.1.6.2 通用数据来源

- 接受地址：
  - 选择代理服务器接受地址：
    - 选择 “4.5.2.1 被动爬虫服务器配置” 配置过的内容。
- 代理服务器可用端口范围：限制任务生成代理服务的端口的范围，不填表示使用全局配置处的默认端口范围，详情请参考 4.5.2.1 被动爬虫服务器配置。
- 用户名、密码：
  - 填写地址的验证用户名和密码。

3.1.6.3 日志信息采集

这里的配置项，仅用于被动 Web 扫描（日志）这个扫描策略，对收集日志信息进行一些配置。

- 接受地址：
  - 选择代理服务器接受地址：
    - 选择“4.5.2.1 被动爬虫服务器配置”配置过的内容。
- Syslog 服务器连接配置：
  - Syslog 服务器 IP ，点击“全局配置”，前往全局页面进行配置；
  - Syslog 服务器端口，填写通信的端口数字，填写完后可以点击右侧的“验证端口可用性”进行验证，给出可用的提示信息，即可正常使用。
- 日志参数匹配规则：
  - 选取解析日志的规则；
  - 点击下拉菜单选择规则。
- 验证日志规则有效性：
  - 输入要解析的日志样例，验证规则是否可以正常解析。
- host 设置：
  - 对于日志文件中没有 host 信息的，可以在此处配置：
    - 选择协议，填写服务器 IP 和端口。

传输日志数据方法说明

下载“日志传输客户端”辅助工具（联系公司内部技术支持人员获取）。当前工具版本：洞鉴（X-Ray）辅助工具-日志传输客户端 v6

- 客户端适用系统说明

工具名称	适用系统
pioneer_darwin_amd64	MAC 64 位
pioneer_darwin_386	MAC 32 位
pioneer_linux_amd64	Linux 64 位
pioneer_linux_386	Linux 32 位
pioneer_windows_386	Windows 32 位
pioneer_windows_amd64	Windows 64 位

- 工具使用说明：
  - 操作指令：[工具名称] send-log-file --log-server-host [洞鉴部署的服务器 IP] --log-server-port [传输日志的端口] --logfile [日志文件名逗号分隔] --log-per-second [数字，建议 10] --disable-filter

    mac 样例：./pioneer_darwin_amd64 send-log-file --log-server-host 192.168.54.17 --log-server-port 1234 --logfile ../users.log --log-per-second 10 --disable-filter

- mac 下使用样例：

3.1.6.4 流量信息采集

此处主要用于采集镜像流量，适用于洞鉴硬件版。软件版流量采集参数配置说明见通用数据来源。

- 接受地址：
  - 选择代理服务器接受地址：
    - 选择“4.5.2.1 被动爬虫服务器配置”配置过的内容。
- 选择流量网卡：
  - 具体网口配置请参考 4.1.3.2 网口配置。

此处主要用于流量或 kafka 被动扫描。

- 接收地址
  - 选择通用数据接收地址 IP，接收地址列表为管理节点可访问的引擎节点地址；
  - 填写通用数据接收地址 IP，根据机器的端口开放情况和自身需要，填写任务占用的端口。

通用数据接收方法说明 ：

- 下载“kafka 被动扫描工具”或“流量被动扫描工具”；
- 根据工具包中的说明文档，启动被动 web 扫描客户端；

- 工具使用注意事项：
  - 先创建任务后，再进行 流量/kafka 被动扫描工具配置，以避免操作客户端工具时，没有数据接收端口。

3.1.6.5 目标采集

这里的配置项，仅用于被动 Web 扫描(burp)这个扫描策略，对上传的 burp 信息进行采集。

支持上传不超过 100M 的文件，文件格式为“.xml”

3.1.6.6 信息收集

这里的配置项，仅用于被动 API 扫描(Open API)这个扫描策略，对目标信息进行采集。

3.1.6.7 逻辑漏洞权限配置

用于配置不同权限的账号 cookie，用于检查越权漏洞。

- 被测账号 Cookie：
  - 代理访问的用户默认为权限最高用户账号，此处填写的账号默认为低权限用户，且等级数字越小，权限越高。
  - 对应填写的信息：
    - Cookie 认证的域:支持输入 IP 或域名；
    - Cookie 值:Cookie 认证的域对应的 Cookie 值；
    - 权限等级:数字越小，权限越大，默认选中 1。
- 添加一条用户认证信息：
  - 支持添加更多权限不同的账户信息。

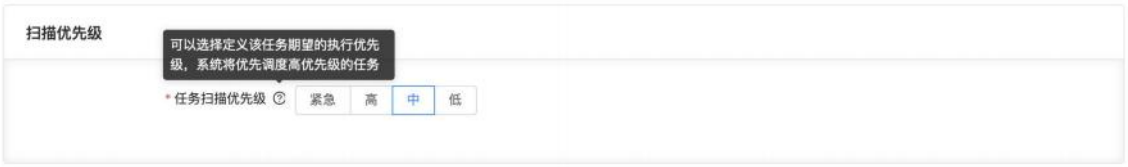
3.1.6.8 引擎节点选择

显示当前系统部署的所有引擎节点，默认选中一个引擎节点，用户可按需选择同时启动的节点。

- 单选：
  - 只能选择一个引擎节点；
  - 仅适用于：基础 Web 漏洞扫描，逻辑漏洞扫描

- 多选：
  - 能选择多个引擎节点，任务目标会被分配到不同节点进行扫描；

3.1.6.9 扫描优先级



- 任务扫描优先级：
  - 可以配置该项目决定在引擎资源饱和后的优先级调度，优先级越高的任务在有引擎资源是释放后越能优先被调度
  - 适用于所有策略

3.1.6.10 扫描任务限制

- 任务最大运行时间：
  - 限制任务执行的最大时间，默认为 3 小时。
  - 当任务总执行时间超过此限制时，将强制结束任务。
- 允许收集的最大链接数：
  - 限制该任务扫描时收集的最大链接数量。
  - 任务收集的链接超过该数量后，不会再继续收集链接。

仅应用于以下参数的扫描策略：基础服务漏洞扫描，特定服务扫描。

- 任务最大运行时间：
  - 限制任务执行的最大时间，默认为 3 小时。
  - 当任务总执行时间超过此限制时，将强制结束任务。
- 最大并发主机：
  - 主机扫描可同时执行的主机数，最大并发主机数越高，扫描速度越快，性能消耗越强。
- 最大带宽限制：
  - 主机扫描任务全局带宽限制，可控制主机扫描的信息收集以及漏洞扫描阶段，引擎消耗的最大带宽。
  - 单位是 KB/s。
  - 智能流量管控：
    - 由引擎智能根据当前请求的返回情况调节扫描速度，以最优的资源占用实现高效扫描

3.1.6.11 HTTP 客户端限制

- 请求失败后的重试次数：
  - 设置对扫描目标发送 HTTP 请求失败后，最大的重试次数；
  - 若重试过该次数后，仍然请求失败，任务就不会再尝试对该目标发送请求；
  - 设置合适的请求重试次数，和下文中的“HTTP 请求连接超时时间”、“HTTP 请求响应超时时间”相配合，可以最大程度地降低网络波动等意外情况对任务扫描过程的影响，同时保证任务扫描的效率。
- 最大重定向次数：
  - 限制一次 HTTP 请求重定向的次数；
  - 任务对目标发送一次 HTTP 请求时，遇到 30X 重定向的次数超过最大重定向次数时，任务就不会再继续跟随；
  - 如果目标重定向次数过多，甚至无限递归，任务无限制地跟随会耗费大量资源；
  - 适当限制最大重定向次数可以减少这个问题造成的影响，同时能够正常收集使用重定向的目标的信息。
- HTTP 请求连接超时时间（单位为毫秒）：
  - 限制任务发送 HTTP 请求进行 TCP 连接的超时时间；
  - 若超过该时间仍未连接，则判断为连接超时，请求失败；
  - HTTP 请求连接时间过长的原因可能是网络未连接、参数错误、缺少证书等，此时任务继续等待也无法连接，只会不断耗费时间；
  - 适当限制连接超时时间有助于避免这种情况。
- HTTP 请求响应超时时间（单位为毫秒）：

- 限制任务发送 HTTP 请求后等待响应的最大时间；
- 若超过该时间未得到目标的响应，则判断为响应超时，请求失败；
- HTTP 请求长时间未响应可能是因为服务器忙碌、防火墙拦截等，尤其是防火墙拦截即使继续等待也不会得到响应；
- 适当限制响应超时时间，有助于避免因为这种情况耗费太多时间。

- 每个站点并发连接数：
  - 限制任务在扫描过程中允许并发连接的最大数量；
  - 任务在扫描过程中同时连接多个目标尝试扫描，可以提高扫描的速度，但也会占用服务器的运行资源；
  - 适当限制并发连接数，能在服务器处理能力内最大程度地低提高扫描的速度。
- 每秒最大请求数：
  - 限制该任务扫描时，每秒能发送的最大请求数；
  - 每秒请求数量太低会对扫描速度产生影响，但太高会占用洞鉴服务器的运行资源，也有可能对扫描目标服务器造成负担；
  - 适当限制每秒请求数量，可以尽可能地在不造成负面影响的情况下提升扫描速度。
- 页面大小限制（单位为 KB）：
  - 限制读取单个页面的 HTTP 响应时的页面大小；
  - 若超过页面大小限制，则不会再继续读取超过限制的部分；
  - 单个页面太大的话，任务不加限制的读取扫描将会耗费很多的资源和时间；
  - 在了解需扫描目标的页面大小的情况下，适当限制读取页面的大小，有时能够很大程度地节约扫描的时间。

3.1.6.12 扫描白名单配置

该模块默认开启。开启后，排除扫描目标中不进行漏洞检测或者不进行资产发现的目标。

主机白名单配置：

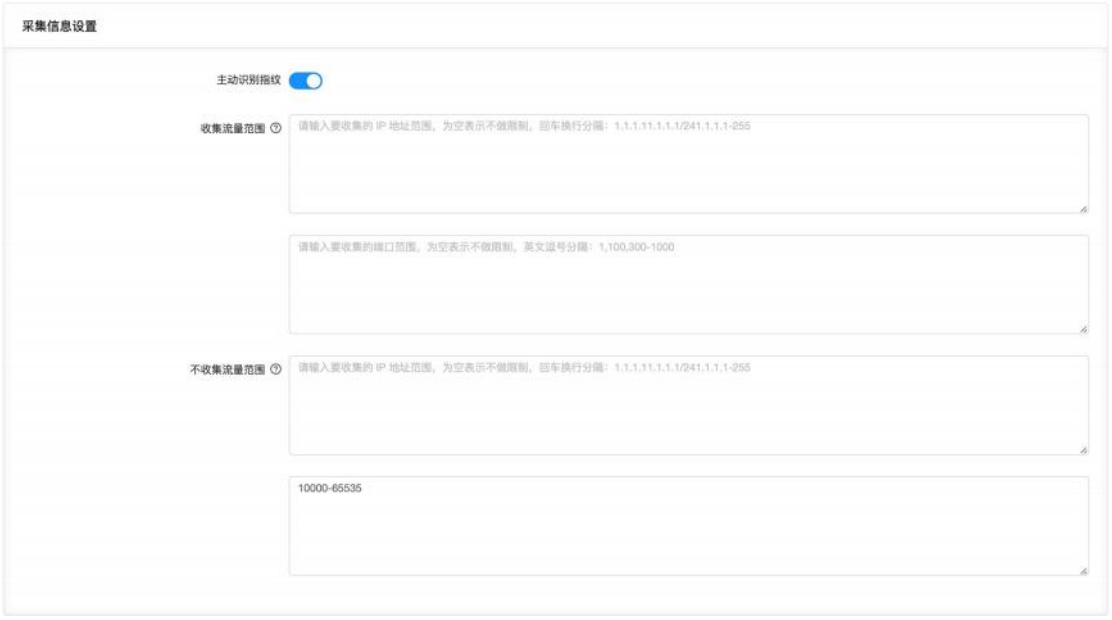
Web 白名单配置：

- 白名单应用：可以选择全局白名单中预置好的白名单模版，进行编辑填充
- 规避扫描的目标：
  - 按照格式要求，手动填写不想进行漏洞检测或不想进行资产发现的目标地址；
    - 主机白名单支持 IP 段、IP 加端口的格式，详细见 placeholder。
- 扫描白名单适用范围可以多选：
  - 不进行资产发现：不进行资产发现与漏洞检测
  - 不进行漏洞探测：进行资产发现，但是不进行漏洞检测
- 不扫描包含以下关键字的 URL（Web 策略）
  - 限制任务爬虫爬取的范围；

- 配置后，任务在爬取链接过程中，若判断出 URL 中包含指定的关键字，就会主动停止该次访问；
- 配置合适的关键字，如 delete、remove、logout 等来排除 URL，有助于减小爬虫对资源破坏的几率、也有利于爬虫信息收集的完整性。
- 具体配置方法为：
  - 输入需要排除的关键字，按回车键添加；
  - 点击关键字右侧的关闭图标，可以删除已添加的关键字。

3.1.6.13 采集信息设置

主要用于对镜像流量的采集和筛选。



- 主动识别指纹：
  - 默认开启，开启后会对采集的流量进行主动探测指纹。
  - 关闭后，不再对指纹进行主动探测，流量中采集到的是什么信息就是什么信息。
- 收集流量范围：
  - 可以对要采集流量的 IP 和端口进行限制；
  - 不设置，表示所有端口都会捕获；
  - 设置后，只收集地址为设置 IP 和端口的流量。
- 不收集流量范围：
  - 可以对不采集流量的 IP 和端口进行限制；
  - 不设置，表示所有端口都会捕获；
  - 设置后，填写的 IP 和端口相关的流量均不会收集。

3.1.6.14 单个扫描目标限制

- 单个目标最大扫描时间：
  - 限制每个目标的最大扫描时间。超过限制时，会直接结束对当前目标的扫描。
  - 如果任务目标较多，限制单个目标最大扫描时间可以有效的控制任务的总时长，避免网络波动、网站防御等情况对任务效率造成过大的影响。不过单个目标最大扫描时间太短，可能还没收集到什么信息，就结束该目标的扫描了。通常情况下，如果任务目标只有几个，则建议把单个目标最大扫描时间设高一些，以避免信息收集和漏洞探测不全
- 最大子域名深度：
  - 限制任务递归猜解的最大子域名深度。超过了此限制后，就不会继续猜解。
  - 任务在进行目标的域名发现时，会自动猜解子域名，猜解成功后默认会继续递归猜解。一般情况下，三、四级子域名就算是比较多的了。但是一些特殊设计的域名结构或 DNS 服务器规则，可能对目标的所有子域名都返回 IP 结果，导致无限制的递归猜解。为了避免这种情况，就需要限制最大子域名深度。设置的时候参考实际的域名级数，不要设得太小以免域名发现不全就可以了。
- 并发 DNS 查询数量：
  - 限制任务同时发送 DNS 请求的线程的最大数量。
  - DNS 查询可以用于发现域名资产，解析域名 IP 等。如果并发 DNS 查询数量太大，容易给 DNS 服务器造成压力;反之，并发 DNS 查询数量太小则 可能影响扫描速度 。

3.1.6.15 DNS 解析配置

此处用以配置全局 DNS 配置无法解析的扫描目标。

- 此配置项默认处于关闭状态。
- 开启后，按要求格式填写 IP 地址，换行分隔：
  - 当前填写的 IP 地址会覆盖全局配置的 DNS 配置。

3.1.6.16 自动生成扫描列表

开启后，任务在每次扫描结束后将自动生成报告，可前往报告管理下载。如果开启了扫描动态通知，选中的不同格式的扫描报表会自动发送至邮箱。

- 如果资产组开启了“任务发送报表通知”，则会将选中格式的报表文件发送至资产组绑定邮箱。

- 报表名称：
  - 默认为自定义的扫描任务报表模版，也可以选择自定义的模板或英文模版。
- 报表文件格式：
  - 系统默认选择 HTML 版
  - 用户可自行选择 Word 版，Excel 版，PDF 版。

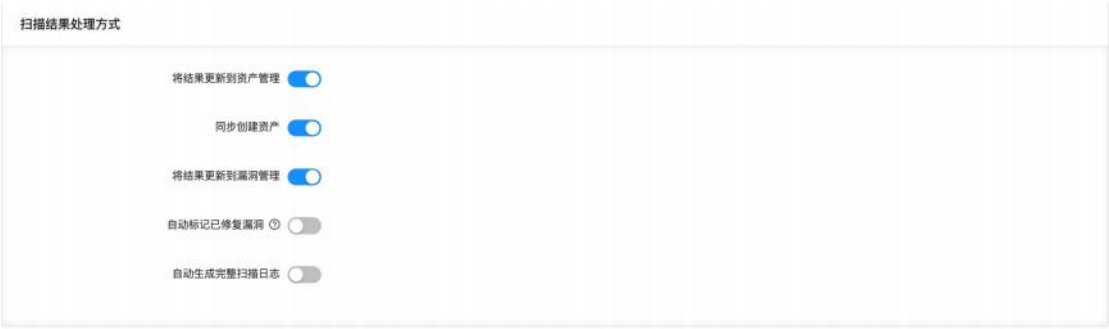
3.1.6.17 扫描动态通知

启用时，每次任务结束后系统都将自动给此处填写的邮箱发送邮件通知。对于扫描耗时较长、或是定时扫描的任务，开启扫描动态通知，可以在收到邮件通知后再查看扫描结果，而不需要频繁查看任务以获得扫描结果。

- 接收通知的邮箱：
  - 在此填写需要接收通知的邮箱；
  - 支持同时输入多个邮箱，多个邮箱以换行分隔。
  - 邮箱格式如下：
    - alarm@example.com
    - report@xxxx.com
  - 注意：只有在系统 SMTP 配置成功的情况下，邮箱才能够接收到通知。关于 SMTP 配置的详细信息可参见 4.1.1.3 SMTP 服务器设置。

3.1.6.18 扫描结果处理方式

对扫描结果的处理方式做自定义的配置



- 将结果更新到资产管理：
  - 默认开启，扫描结果中的资产信息将自动更新到资产中心；
  - 结果更新的前提是创建了该资产，该资产存在才可以将结果更新到资产中，否则什么都不做；
  - 关于资产分配：
    - 服务资产更新到主机资产详情中端口列表；
    - 域名资产更新到 web 资产详情中目录结构信息。
- 同步创建资产：
  - 默认开启，
- 将结果更新到漏洞管理：
  - 默认开启，扫描结果中的漏洞信息将自动更新到漏洞管理；
  - 若漏洞管理中不存在，任务会将其自动添加到漏洞管理中；
  - 若漏洞管理中以存在：
    - 且漏洞状态为“已修复”，任务会以“未分配”状态更新该漏洞；
    - 且漏洞状态不为“已修复”，则漏洞管理中的状态不会被改变。
- 自动标记已修复漏洞：
  - 默认关闭，开启后，某目标下已存在的漏洞，若在本次扫描中未被发现，会自动置为已修复状态。“忽略”以及“误报”状态的漏洞除外。
- 自动生成完整扫描日志：
  - 默认关闭，开启后在扫描日志中会生成 debug 日志，便于定位扫描过程中遇到的问题。

3.1.6.19 HTTP 请求配置

对任务在信息收集阶段或漏洞探测阶段发送的 HTTP 请求做详细配置。

- User-Agent：
  - 配置后，任务将使用这里的 User-Agent 作为请求头发送请求；
  - 某些目标对特定 User-Agent 的请求访问有所限制，配置合适的 User-Agent 可以解决这个问题。
  - 配置的具体方法有两种:
    - 直接输入所需 User-Agent 的值；
    - 点击 User-Agent 输入框，在下拉备选菜单中点击需要配置的值。
- Cookie：
  - 配置后，任务将使用这里的 Cookie 作为请求头发送请求；
  - 配置好正确的 Cookie 后，才可以扫描某些需要 Cookie 认证的目标；
  - 配置时，可以对每个 Cookie 选择是否“允许覆盖”；
    - 若不允许覆盖，任务会始终使用该 Cookie 配置的值；
    - 否则，任务会根据返回信息重新设置 Cookie，更符合真实访问情况。

- 如果服务器对该 Cookie 的访问限制是相对不变的，选择不允许覆盖该 Cookie，可以保证扫描信息与预期一致，也能有效地避免爬虫时自动登出的问题；
- 如果服务器对该 Cookie 的访问限制是动态的、需要实时更新才能保持登陆，又或者是需要扫描的漏洞与 Cookie 覆盖行为本身相关，那么允许覆盖该 Cookie 才能更真实地获取目标信息。

- 配置的具体方法为:
  - 直接输入 Cookie 内容，样例如上图中所示；
  - 展开“高级选项”，可以预览配置的 Cookie 信息，并且可以对每一条 Cookie 选择是否“允许覆盖”。
- 逻辑漏洞扫描不需要配置 Cookie

- 其他自定义 HTTP 请求头：
  - 配置后，任务将使用这里的 HTTP 请求头发送请求；
  - 配置特定的请求头，可以应对扫描目标可能存在的、对访问的特殊限制。
  - 配置的具体方法为:
    - 点击“ + 增加一个 HTTP 请求头”，填写请求头的名称与值；
    - 可以同时添加多条自定义 HTTP 请求头；
    - 点击已添加 HTTP 请求头的删除图标，可以删除该 HTTP 请求头。
- HTTP 代理：
  - 填写后，任务将使用此 HTTP 代理来扫描目标；
  - 如果洞鉴服务器因为某些原因（如和目标不在同一个网络、目标对访问者 IP 有所限制等）无法直接访问需要扫描的目标，配置合适的 HTTP 代理可以解决问题配置的具体方法为:

- ◆ 直接输入 HTTP 代理的 URL；
- ◆ 注意：配置时代理时请确保洞鉴服务器可以访问到该 HTTP 代理，且该 HTTP 代理可以访问到扫描目标

■ 支持配置多个代理，通过换行符分隔

3.1.6.20 HTTPS 客服端证书

默认关闭，HTTPS 客户端证书启用且配置正确后，可以扫描某些需要 HTTPS 客户端证书认证的目标。

3.1.6.21 HTTP 基础认证

默认关闭，HTTP 基础认证启用且配置正确后，才可以扫描某些需要 HTTP 基础认证的目标。

- 用户名：
  - 填写 HTTP 基础认证的用户名；
  - 若启用 HTTP 基础认证但不填写用户名，任务将使用空用户名尝试认证。
- 密码：
  - 填写 HTTP 基础认证的密码；
  - 若启用 HTTP 基础认证但不填写密码，任务将使用空密码尝试认证。

3.1.6.22 Web 表单登录

默认关闭，Web 表单登录启用且配置正确后，才可以扫描某些需要表单登录的目标。

- 表单所在的 URL：
  - 填写进行表单登录的 URL；
- 用户名：
  - 填写表单登录的用户名；
  - 若启用 Web 表单登录但不填写用户名，任务将使用空用户名尝试登录。
- 密码：
  - 填写表单登录的密码；
  - 若启用 Web 表单登录但不填写密码，任务将使用空密码尝试登录。

3.1.6.23 网站可用性验证

默认关闭，启用后任务在扫描 Web 站点之前，会先对网站进行可用性验证，确认网站可用再进行扫描；否则任务将不考虑网站的存活情况，直接尝试扫描。

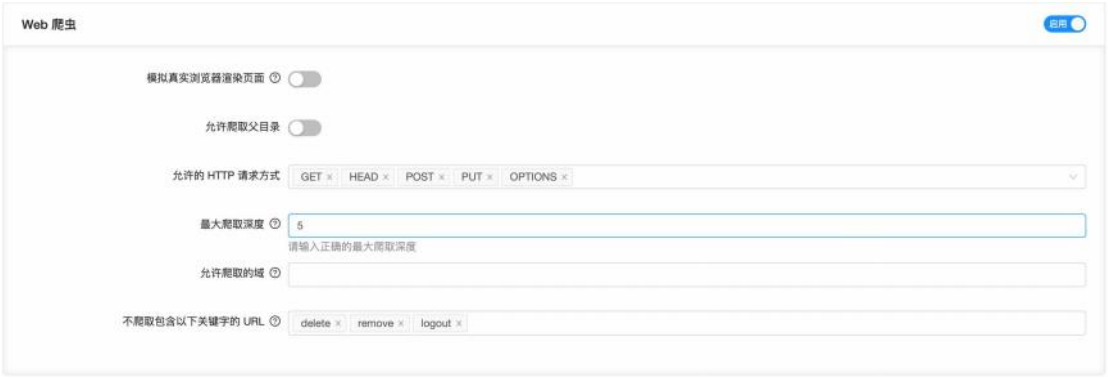
由于直接扫描不存活的网站一般耗时较久，启用并合理配置网站可用性验证，可以提高扫描的速度。

- 验证地址：
  - 填写可以验证网站可用性的地址。
- 特征字符串：
  - 填写网站的 response 字段，点击“一键验证”，验证网站是否可达；
  - 如果失败，说明网站不可达。

3.1.6.24 Web 爬虫

默认开启，任务会使用 Web 爬虫以收集网站的更多信息；若关闭 Web 爬虫，任务将只扫描用户填写的目标网站。

启用并合理配置 Web 爬虫，可以收集更多关于网站的信息，而不仅局限于填写的目标。



- 模拟真实浏览器渲染页面：
  - 默认关闭
  - 开启后爬虫会模拟浏览器的行为来解析 HTML 页面，并执行其中的 JavaScript 脚本；

  - 否则爬虫只会使用普通的 HTML 解析器来解析页面中的表单与链接。

- 若网页的前端代码中使用了大量的 JavaScript 脚本来实现页面，启用该选项可以更加真实地收集页面的信息；
- 但模拟浏览器渲染页面比较耗时，会降低任务的扫描速度。

- 允许爬取父目录
  - 默认关闭，开启后任务会尝试爬取扫描目标的父目录，否则只会爬取目标和目标的子目录；
  - 爬取父目录可以收集到更多的页面信息，但会增加任务的耗时。
- 允许的 HTTP 请求方式：
  - 限制任务扫描时允许使用的 HTTP 请求方式；
  - 任务将只使用此处填写的方式来发送请求。
  - 注意：不当的请求方式有可能造成目标资源的损坏，如 DELETE、PUT、POST，请谨慎使用此类请求方式。
  - 具体配置方法为:
    - 输入允许的 HTTP 请求方式，按回车键添加；
    - 或是点击输入框，在下拉菜单中点击需要的请求方式；
    - 系统可以使用的请求方式有：GET、POST、PUT、HEAD、 OPTIONS、DELETE、TRACE、CONNECT；
    - 点击请求方式右侧的关闭图标，可以删除已添加的请求方式。
- 最大爬取深度：
  - 限制任务爬虫时最大的爬取深度；
  - 当任务将单个目标设为起始页，一层层追踪链接，层数达到最大爬取深度时，就会停止向下追踪；
  - 爬取深度更大时，任务可能收集到更多的信息，但也会增加任务的耗时；
  - 适当限制最大爬取深度，可以让任务在能够接受的耗时内最大程度收集信息。
- 允许爬取的域
  - 限制任务爬虫爬取的范围；
  - 配置后，任务会额外爬取允许爬取的域，否则任务将只爬取和扫描目标中 URL 相同的域；
  - 添加允许爬取的域，可以扩大任务信息收集的广度；
  - 用户可以根据实际所需配置，如允许任务爬取一些子域，这些子域和扫描目标中的 URL 相同。
  - 具体配置方法为：
    - 输入允许爬取的域，按回车键添加；

- 系统支持通配符“*”，如可以使用“* .test.com”、“ *.test.cn”等；
- 点击域右侧的关闭图标，可以删除已添加的域。

3.1.6.25 主机存活探测

启用后，任务执行时，会先执行一次快速预扫描，发现扫描目标中存活的主机。

由于直接扫描不存活的主机，无效且费时，启用并恰当配置主机存活探测，能够大幅提升任务扫描的速度。

- 探测方式：
  - 点击下拉菜单选择方式。
- 探测强度：
  - 选择主机探测的强度；
  - 用户可以根据对扫描速度和精度的需求自行选择。
- 超时等待时长：
  - 固定为 1 秒。
- 最小重试次数：
  - 固定为 3 次。
- 最大重试次数：
  - 固定为 100 次。
- 跳过无响应的主机
  - 启用后，对于主机存活探测中发现不存活的主机，任务不会再尝试扫描；
  - 否则任务会不考虑主机存活状态，直接尝试扫描所有主机。
  - 关闭时可能导致扫描速度大幅下降。

3.1.6.26 TCP 扫描协议

启用后，可以对任务扫描的 TCP 端口进行自定义。关闭时，任务会使用默认的端口组扫描目标。启用并配置后如下图所示:

- 端口列表：
  - 输入需要扫描的 TCP 端口；
  - 具体配置方法：
    - 直接输入端口；
      - 输入端口号，多个端口号之间以英文逗号“,”分隔；
      - 支持输入端口段，如：“10–18”。
    - 导入端口组：
      - 点击“ + 导入端口组”；
      - 在弹窗中选中要导入的端口组，点击“确定”；
      - 端口组中的端口会自动加入当前的端口列表后方。
  - 特定服务扫描不需要输入端口。
- 扫描方式：
  - 选择对 TCP 端口对扫描方式；
  - TCP CONNECT 方式结果准确，但速度较慢；

- TCP SYN 方式速度较快，但有一定误差；
- 用户可根据对扫描速度和精度的需求自行选择。

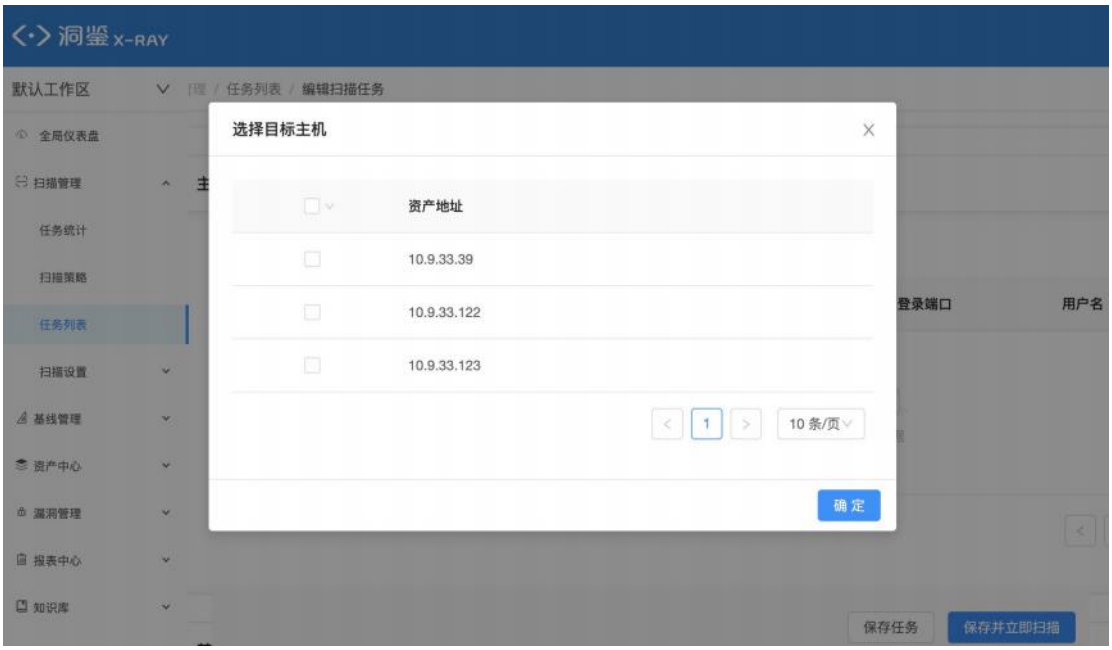
- 扫描前度：
  - 基于不同的扫描强度会加载不同的参数配置；
  - 强度分为快速扫描、常规扫描、精准扫描和自定义扫描：
    - 其中扫描速度快速扫描>常规扫描>精准扫描；
    - 扫描精准度精准扫描>常规扫描>快速扫描；
    - 在以上选项时参数不可配，需要调整参数则要选择自定义选项。

- TCP SYN 可控参数
  - 超时等待时长，控制连接的超时时长限定
  - 最小重试次数，控制连接不成功时重试的最小次数
  - 最大重试次数，控制连接不成功时重试的最大次数
- TCP Connect 可控参数
  - 超时等待时长，控制连接的超时时长限定
  - 最大并发端口连接数，控制同时并发的端口数
  - 最大 QPS，限制每秒最大请求数

- 指纹探测：
  - 启用指纹探测时，任务会尝试探测发现的开放端口上的服务和应用。
  - 启用后，可更改探测精度：
    - 低，中，高

3.1.6.27 主机登录扫描

默认不开启，启用后，可以对扫描目标中输入的主机资产进行主机登录扫描。点击选择目标进行主机选择



选择主机资产后，进行用户名密码的配置。输入主机用户名以及登录所使用的密码或者私钥，点击登录验证。成功后，点击确定即配置该主机成功。

也可对主机进行批量配置用户名密码后登录验证。

3.1.6.28 UDP 端口扫描

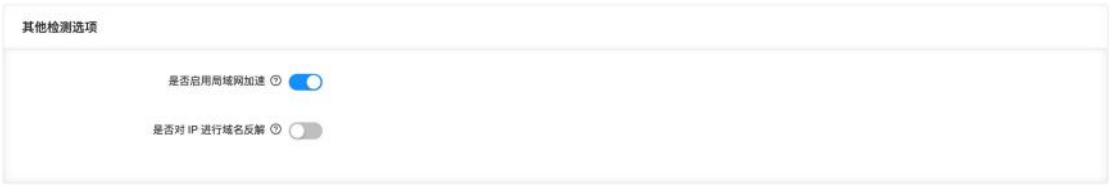
启用后，可以对任务扫描的 UDP 端口进行自定义；关闭时，任务不会扫描 UDP 端口。

注：UDP 端口扫描速度较慢，且结果误差大，在没有强烈需求的情况下建议关闭。

- 端口列表：
  - 输入需要扫描的 UDP 端口；
  - 具体配置方法为：
    - 直接输入端口：
      - 输入端口号，多个端口号之间以英文逗号“,”分隔；
      - 支持输入端口段，如“10-18”。
    - 导入端口组
      - 点击“ + 导入端口组”；
      - 在弹窗中选中要导入的端口组，点击“确定”；
      - 端口组中的端口会自动加入当前的端口列表的后方。
  - 特定服务扫描不需要输入端口。
- 扫描强度：
  - 仅提供常规扫描；

- 超时等待时长：控制连接的超时时长限定；
- 最小重试次数：控制连接不成功时重试的最小次数；
- 最大重试次数：控制连接不成功时重试的最大次数。

3.1.6.29 其他检测选项



- 是否启用局域网加速：
  - 如果扫描目标和扫描器处于同一局域网中，那么使用 APP 来优化扫描请求。
- 是否对 IP 进行域名反解：
  - 通过 DNS 反解查询扫描结果中 IP 对应的域名。

3.1.6.30 启用自定义指纹

启用后，同类指纹以自定义为准。

3.1.6.31 监控端口范围

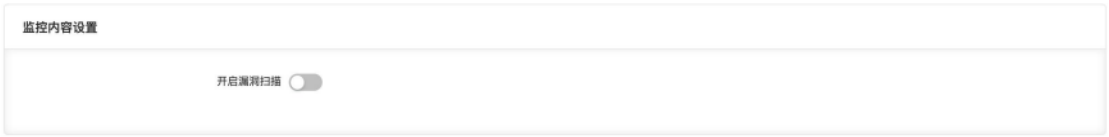
- TCP 端口列表：
  - TCP 端口为 1 至 65535。
  - 具体配置方法：
    - 直接输入端口；
      - 输入端口号，多个端口号之间以英文逗号“,”分隔；
      - 支持输入端口段，如：“10–18”。
    - 导入端口组：
      - 点击“ + 导入端口组”；
      - 在弹窗中选中要导入的端口组，点击“确定”；
- 端口组中的端口会自动加入当前的端口列表后方。UDP 端口列表：
  - UDP 端口为 1 至 65535。
  - 具体配置方法：
    - 同上 TCP
- 跳过不存活的主机：
  - 启用后，对于主机存活探测中发现不存活的主机，任务不会再尝试扫描；
  - 否则任务会不考虑主机存活状态，直接尝试扫描所有主机。
  - 关闭时可能导致扫描速度大幅下降。

3.1.6.32 监控白名单配置

开启后，排除扫描目标中不进行漏洞检测或者不进行资产发现的目标。

- 检测白名单：
  - 按照格式要求，手动填写不想进行漏洞检测或不想进行资产发现的目标地址；
  - 或通过点击“导入主机资产”导入目标地址。

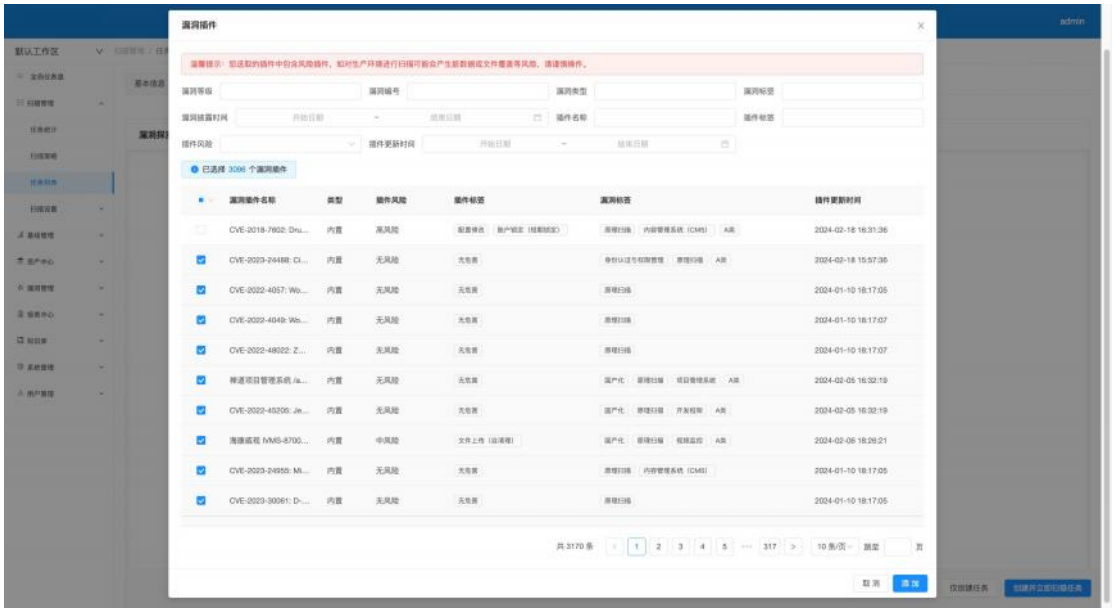
3.1.6.33 检测内容设置



- 开启漏洞扫描

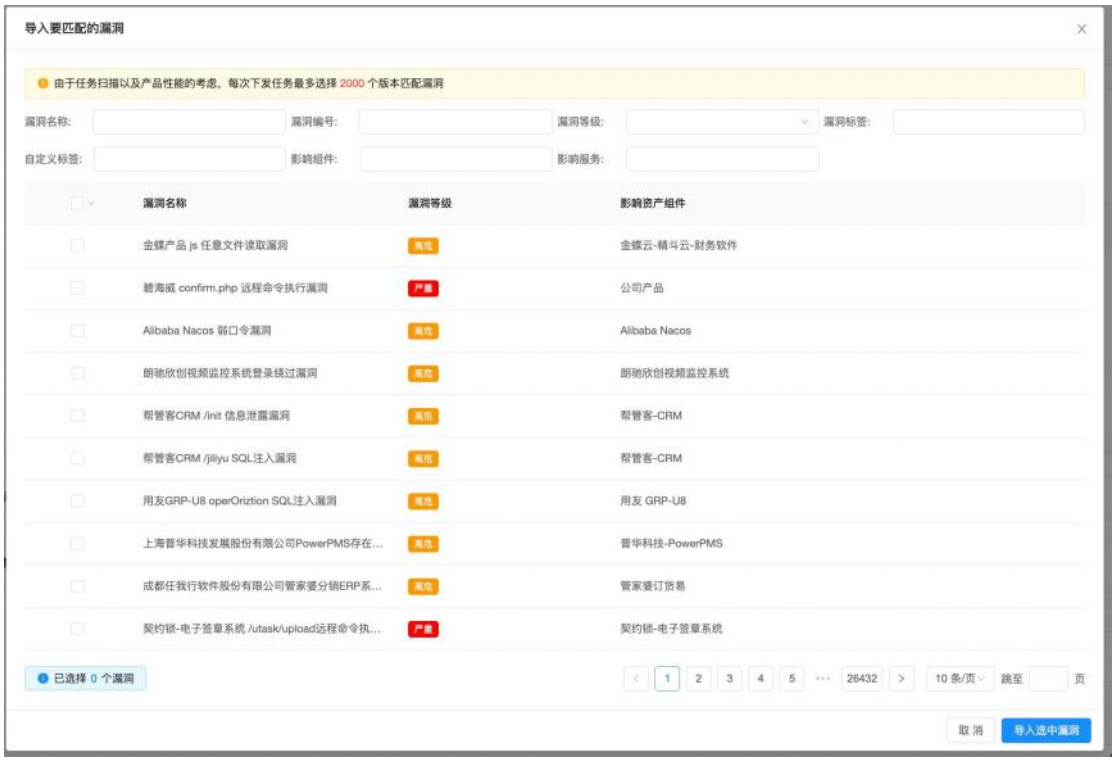
3.1.6.34 漏洞探测插件

可以在此自定义任务启用的插件。



- 不同的插件可以探测不同的漏洞。
- 可以在漏洞等级、漏洞编号、漏洞类型、漏洞标签、漏洞披露时间、插件名称、插件标签、插件风险八个维度进行对插件的筛选
- 根据插件选择情况展示可能扫描到漏洞的总数，对应四种风险等级的数量

- 版本匹配配置
  - 支持对版本匹配的漏洞进行进一步选择
  - 每次扫描最大支持选择 2000 条漏洞
  - 支持筛选


导入要匹配的漏洞
由于任务扫描以及产品性能的考虑，每次下发任务最多选择 2000 个版本匹配漏洞
漏洞名称:
漏洞编号:
漏洞等级:
漏洞标签:
自定义标签:
影响组件:
影响服务:
漏洞名称
漏洞等级
影响资产组件
金蝶产品 js 任意文件读取漏洞
高危
金蝶云-精斗云-财务软件
碧海威 confirm.php 远程命令执行漏洞
严重
公司产品
Alibaba Nacos 弱口令漏洞
高危
Alibaba Nacos
朗驰欣创视频监控系统登录绕过漏洞
高危
朗驰欣创视频监控系统
帮管客CRM /init 信息泄露漏洞
高危
帮管客-CRM
帮管客CRM /jiliyu SQL注入漏洞
高危
帮管客-CRM
用友GRP-U8 operOriztion SQL注入漏洞
高危
用友 GRP-U8
上海普华科技发展股份有限公司PowerPMS存在...
高危
普华科技-PowerPMS
成都任我行软件股份有限公司管家婆分销ERP系...
高危
管家婆订货易
契约锁-电子签章系统 /utask/upload远程命令执...
严重
契约锁-电子签章系统
已选择 0 个漏洞
1
2
3
4
5
26432
10 条/页
跳至
页
取 消
导入选中漏洞

3.1.6.35 自定义弱口令猜解字典

任务扫描 Web 弱口令漏洞时，默认使用智能弱口令字典探测。启用“自定义弱口令猜解字典”后，则可以自定义扫描 Web 页面时的弱口令探测字典。如何配置自定义字典，可以参考 3.1.4.1 字典管理 中的说明。

注：自定义弱口令探测字典，只有在“漏洞探测插件配置”中，启用“Web 表单弱口令漏洞扫描插件”时才能生效。

- 用户名字典：
  - 选择探测弱口令用户名时使用的字典；
  - 字典内容一般选择常见的用户名：
    - 如 admin、root 等；也可以尝试选择企业、组织内部的默认用户名，比如工号、学号、电话号码等。
- 密码字典：
  - 选择探测弱口令密码时使用的字典；
  - 字典内容一般选择常见的弱密码；
    - 比如 123456 等。

3.1.6.36 自定义路径猜解字典

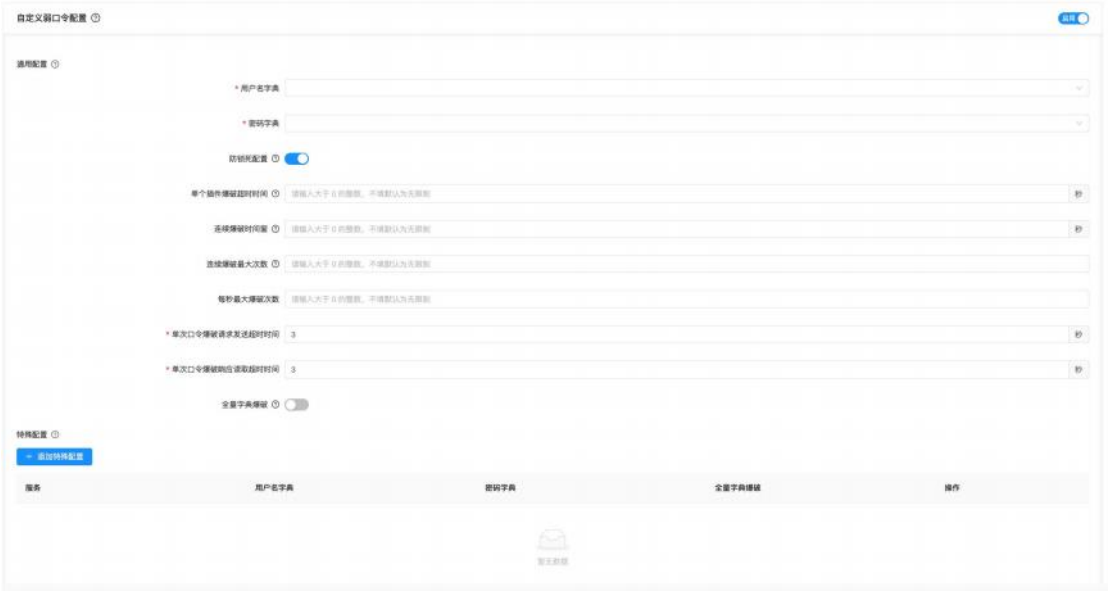
当目标 Web 页面上的链接不多，或者有很多独立页面时，字典猜解可以作为 Web 爬虫 的一个很好的补充，帮助任务收集网页信息。

当“自定义字典猜解”关闭时，任务默认使用智能的字典猜解模式;启用时，则可以自 定义扫描 Web 站点时的路径猜解字典。如何配置自定义字典，可以参考 3.1.4.1 字典管理 中的说明。

注：自定义字典猜解，只有在“漏洞探测插件配置”中，启用“自定义字典信息泄露漏洞检测插件”时才能生效。

- 路径猜解字典：
  - 选择路径猜解时使用的字典；
  - 选择后，任务会尝试用字典中每一行的内容作为目录，猜解扫描目标：
    - 如，扫描目标为 http://www.test.com，路径猜解字典每行分别为 /a /、/b/、/c/ ……。则任务会尝试猜解 http://test.com/a/、http://www.test.com/b/、http://www.test.com/c/ …… 页面

3.1.6.37 自定义弱口令配置



- 用户名字典
- 密码字典
- 单个插件爆破超时时间
  - 填写大于 0 的数字，不填写则代表无限制
- 最大连续爆破次数
  - 填写大于 0 的数字，不填写则代表无限制
- 连续爆破时间窗
  - 填写大于 0 的数字，不填写则代表无限制
- 每秒最大爆破次数
  - 填写大于 0 的数字，不填写则代表无限制
- 单次口令爆破请求发送超时时间
- 单次口令爆破响应读取超时时间
- 全量字典爆破：对字典全匹配进行爆破尝试，会增加扫描时长
- 特殊配置：
  - 为某个扫描对象单独配置参数
  - 具体操作：
    - 点击“ + 添加特殊配置”，跳出弹窗；
    - 在“配置服务”中选择目标对象；
    - 其余参数同上；
    - 点击“保存”， 完成配置。
  - 保存的配置会一直存在，可选操作：

- 编辑
- 删除


特殊配置
* 配置服务
SSH 弱口令漏洞检测插件
* 用户名字典
SSH 用户名字典
* 密码字典
SSH 密码字典
单个插件爆破超时时间
请输入大于 0 的整数，不填默认为无限制
秒
连续爆破最大次数
请输入大于 0 的整数，不填默认为无限制
连续爆破时间窗
请输入大于 0 的整数，不填默认为无限制
秒
每秒最大爆破次数
请输入大于 0 的整数，不填默认为无限制
* 单次口令爆破请求发送超时时间
3
秒
* 单次口令爆破响应读取超时时间
3
秒
全量字典爆破
取消
保存

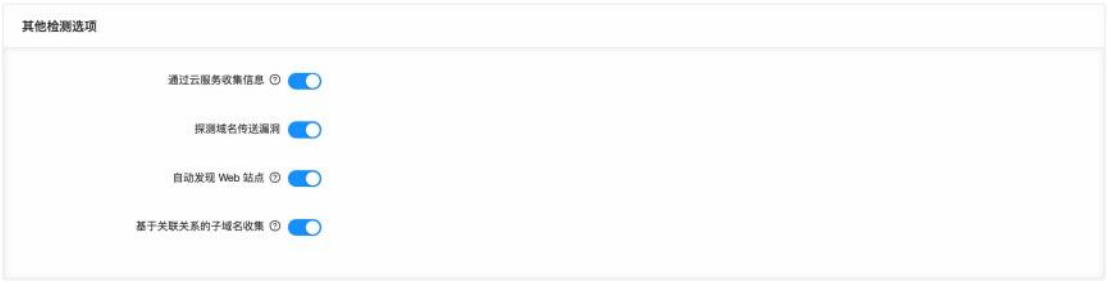
3.1.6.38 自定义域名猜解字典

进行域名发现时，域名猜解是是发现子域名的重要方式。

当“自定义域名猜解字典”关闭时，任务默认使用智能的域名猜解。启用时，则可以自定义子域名的猜解过程。如何配置自定义字典，可以参考 3.1.4.1 字典管理 中的说明。

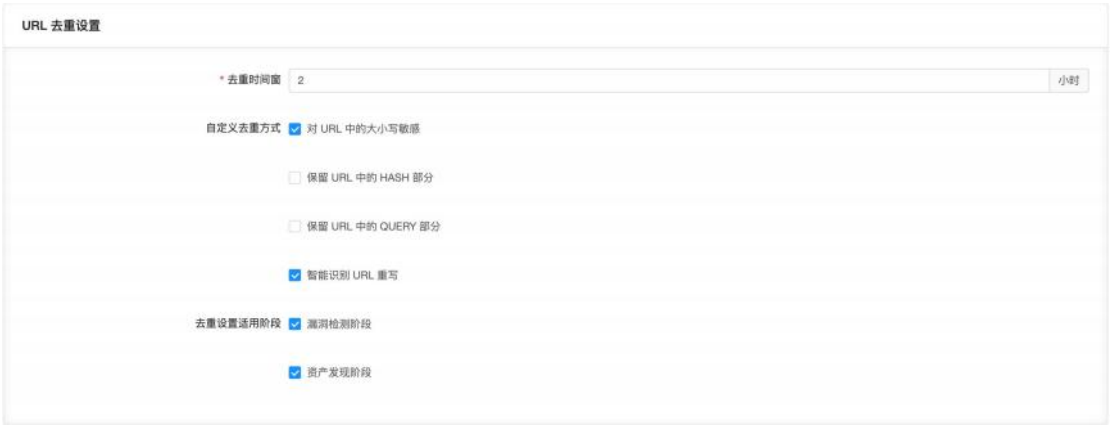
- 域名猜解字典：
  - 选择域名猜解时使用的字典；
  - 选择后，任务会尝试使用字典中每一行的内容作为子域名，去猜解目标域名。
    - 如，域名目标为 news.example.com，字典每行分别为 test1、 test2、test3 ……。则任务会尝试猜解 test1.news.example.com、test2.news.example.com、test3.news.example.com …… 等域名。
- 是否允许递归猜解：
  - 开启时，任务在第一层域名猜解成功后，会对猜解到的域名，继续进行递归猜解。
- 递归猜解字典：
  - 选择开启递归猜解时使用的字典。

3.1.6.39 其他检测选项



- 通过云服务收集信息：
  - 启用时，任务会尝试使用公开、免费而可靠的第三方云服务收集目标的信息；
  - 通过云服务收集是子域名发现重要的补充手段，可以突破域名猜解固定字典的限制，收集到不在字典内的子域名信息。
- 探测域名传送漏洞：
  - 启用时，任务会尝试探测 DNS 服务器是否存在域名传送漏洞，以借此收集域名信息；
  - 域名传送漏洞是指由于 DNS 的配置不当，导致某个域的所有查询记录泄露给匿名用户。域名传送漏洞如果存在，则是一个有效的收集域名的方法。
- 自动发现 Web 站点：
  - 启用后，任务会自动探测发现的每个域名下是否有对应的网站；
  - 很多域名都直接对应一个网站，如果需要收集一整个域下的网络拓扑结构，使用域名资产发现策略，并开启自动发现 Web 站点，是一个简单而全面的方法；
  - 当然，如果并不需要 Web 站点信息，可以关闭“自动发现 Web 站点”，这样能减少任务耗费的时间。

3.1.6.40 URL 去重设置



- 去重时间窗：
  - 用于设置去重的时间间隔
- 自定义去重方式：
  - 对 URL 中的大小写敏感：默认开启
  - 保留 URL 中的 HASH 部分：默认关闭
  - 保留 URL 中的 QUERY 部分：默认关闭
  - 智能识别 URL 重写：默认开启
- 去重设置使用阶段：
  - 漏洞检测阶段：
    - 在漏洞检测阶段使用此处的去重配置信息。
  - 资产发现阶段：
    - 在资产发现阶段使用此处的去重配置信息。
  - 注：基本 Web 漏洞扫描，被动 Web 扫描（镜像） 无该选项组

3.1.6.41 全局白名单选择

- 根据当前工作区可获取到全部的全局白名单（应用配置开启并且该工作区在应用配置范围内）
- 不勾选全局白名单，即禁用，任务循环执行时不再应用该全局白名单。
- 可查看白名单：

3.1.6.42 扫描时间配置

- 执行类型：规定此任务时间窗从什么时候开始。
  - 立即扫描

  - 定时扫描一次

  - 每天循环扫描

  - 每周循环扫描

- 每月循环扫描

- 指定时段：开启后，可以选择指定扫描时段或者禁扫时段实现对任务扫描时段的控制可以选择指定扫描时段或者禁扫时段实现对任务扫描时段的控制。和执行类型的开始扫描时间不冲突。
  - 可添加“每天”/“每周”/“每月”的扫描时间段或设置为“禁扫时段”。

  - 每天：

  - 每周：

- 每月：

可按照“第几个周几”和“每月第几日”选择指定时段。如果月份中不存在选中的天，那么在该月则不会进行扫描任务。

备注 1：参数使用第 5 个周几的发布任务存在扫描风险，因为每个月不会存在涵盖所有的第 5 个周一到周日，所以尽量规避设置在第 5 个周几。

备注 2：参数使用第几个周日的发布任务存在扫描风险，尽量规避设置在第几个周日。

3.1.6.43 其他插件配置

- 启用盲打平台：
  - 主要用于插件对无回显漏洞对验证；
  - 辅助扫描插件输出结果中对无回显漏洞。
  - 正常通信前提需要对盲打平台进行配置，点击“前往配置盲打平台”可前往进行配置，详情配置信息可见 3.1.4.3 盲打平台监听配置。

- 设置 Web 漏洞检测深度
  - “？”提示：设置漏洞插件对 web 目标资产拼接前的路径的深度的限制，默认为 2，设置范围为 1–10。

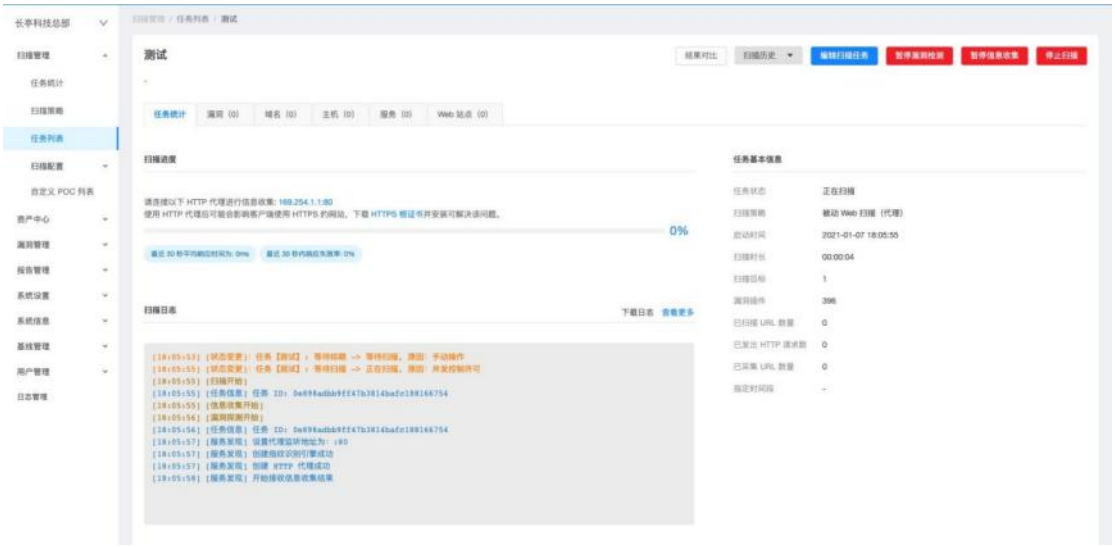
- 最大并发插件数
  - 支持对所选漏洞插件最大并发数量做限制
  - 默认 30
  - 设置范围为 1–100
- 智能插件调用
  - “？”提示：根据资产指纹识别的结果，进行精准的漏洞探测，扫描速度会有所提升；基础服务扫描需要手动开启指纹识别，以提高资产指纹识别准度，web 扫描默认开启指纹识别

3.1.7 代理服务器配置方法

配置好代理服务器后，就可以使用被动 Web 扫描了。

具体步骤为:

- 添加一个被动 Web 扫描任务，填写需要扫描的目标站点。根据所需配置其他参数 ，并保存任务；
- 启动任务，此时任务详情页面将展示 HTTP 代理服务器的 IP 地址和分配的端口号；



- 这时用户需要打开自身客户端系统网络设置，或者浏览器的网络配置，将网页的代理服务器设为任务详情页面显示的代理服务器：
  - Mac OS 系统可在系统偏好设置 / 网络 / 高级 / 代理中设置：

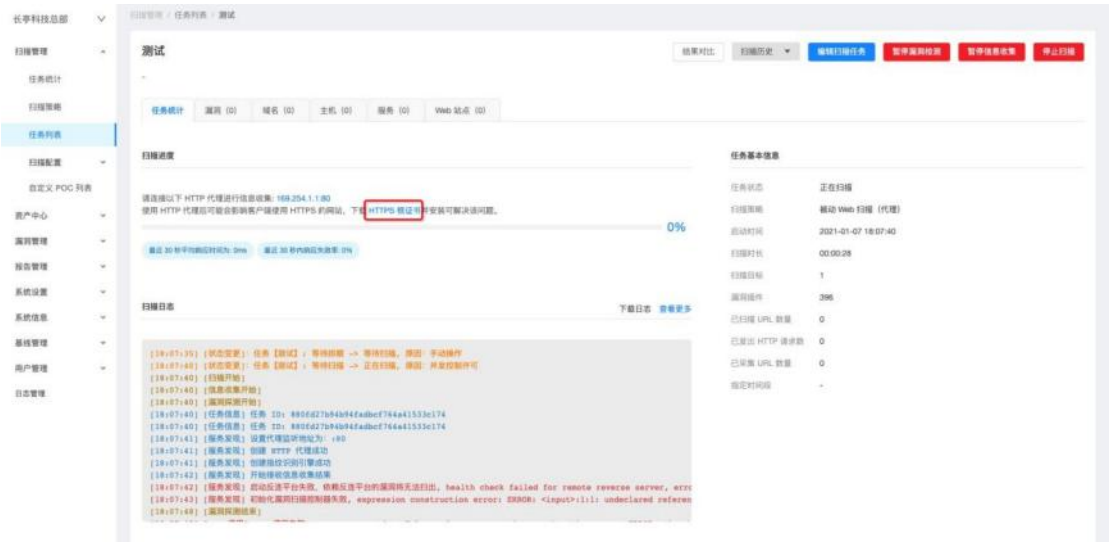
- Windows 可以在控制面板 / 网络和 Internet / Internet 选项 / 链接 / 局域网设置中，选择“为 LAN 使用代理服务器”：

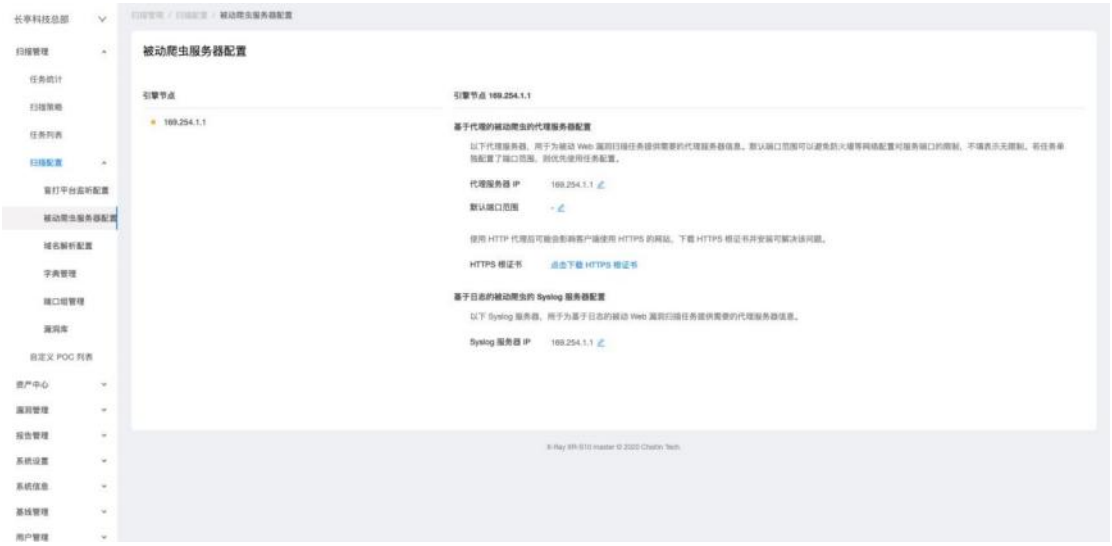
- 用户也可以直接使用支持自定义代理的浏览器，如 Chrome 浏览器的插件 SwitchyOmega：

- 配置好客户端的代理服务器后，就可以用客户端的浏览器打开需要扫描的目标站点，依次访问自己希望扫描的页面；
- 回到之前的扫描任务处，可以看到任务通过代理收集的信息，并且同时进行漏洞探测；

注意：

- 使用 HTTP 代理可能会影响客户端使用 HTTPS 的网站，在扫描详情页或全局配置页可以下载 HTTPS 的根证书，安装并信任后可以解决该问题（如下两图所示）：



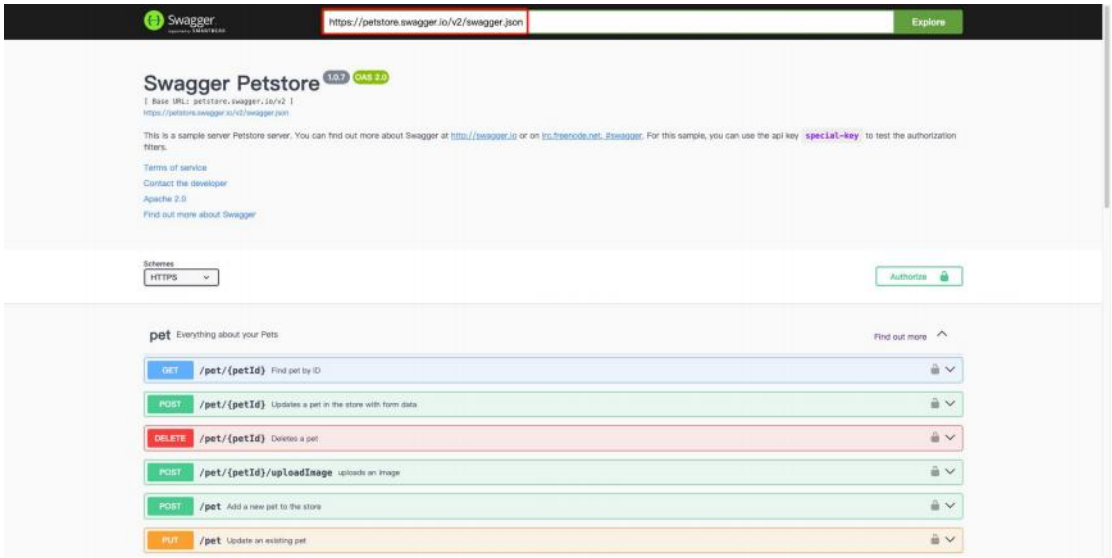


- 代理服务器的端口在被动 Web 漏洞扫描的任务开始时会自动分配。任务结束后，端口将被自动收回。请注意每次开始一个被动 Web 漏洞扫描的任务时，都需要重新配置客户端的代理设置。

3.1.8 API 扫描文件获取方式

3.1.8.1 接收地址 配置说明

访问在线 swagger 文档的链接，可在图中标红的输入框中获取



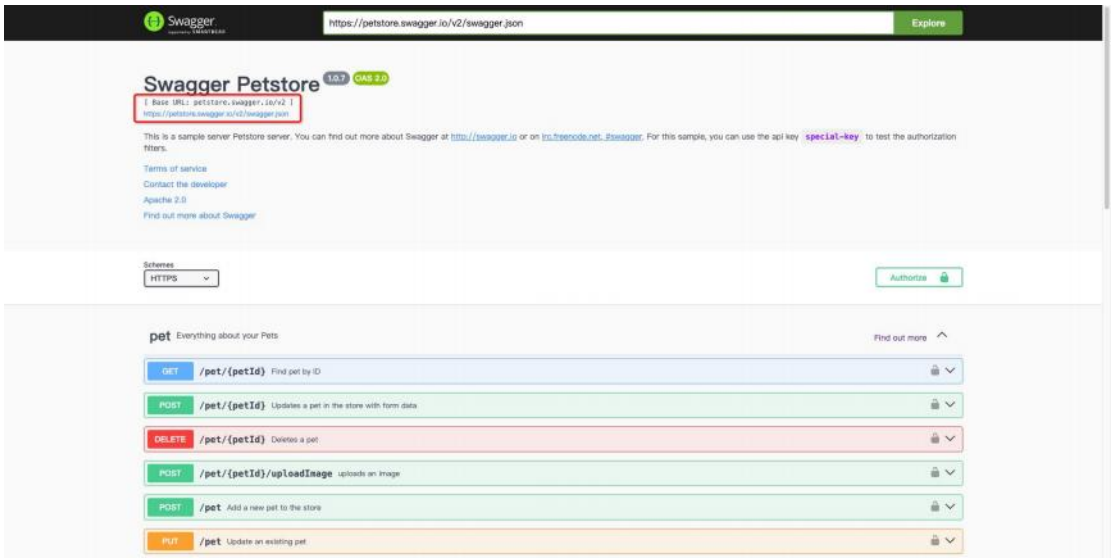
注：仅限于用 swagger 工具进行开发管理接口的情况，其他情况使用“文件上传”的方式

3.1.8.2 文件上传 配置说明

方式一：

通常可以在 swagger UI 界面左上角找到以".json"结尾的 URL

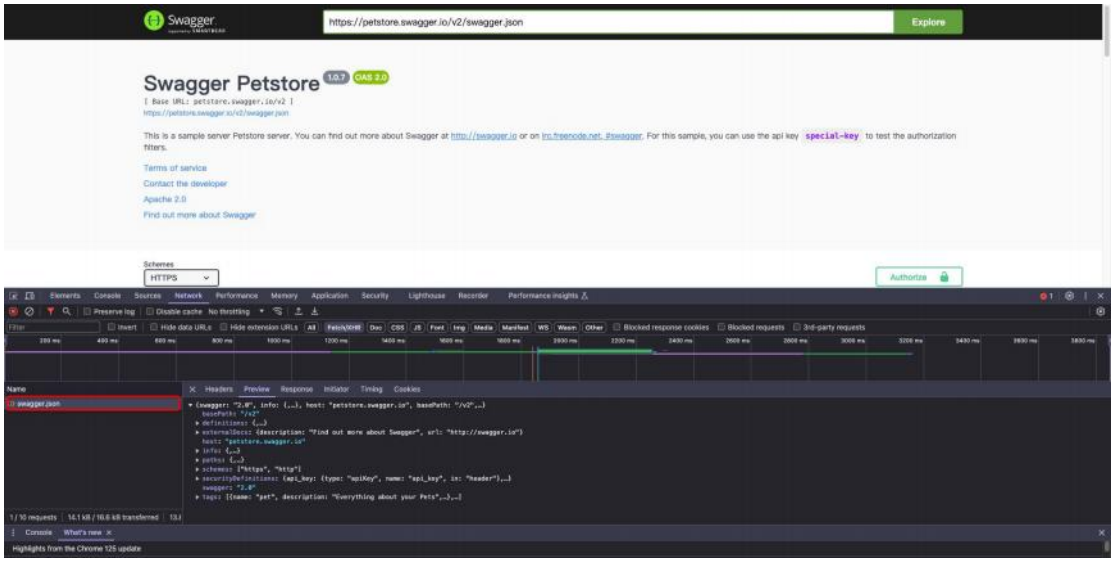
链接处右键，保存为“.json”格式文件



方式二：

当界面没有 URL 链接时，可通过 F12 打开浏览器控制台，然后定位到「Network –> Fetch/XHR」后刷新页面，找到 ".json" 格式的文件

双击访问页面，在空白处右键，保存为“.json”格式文件

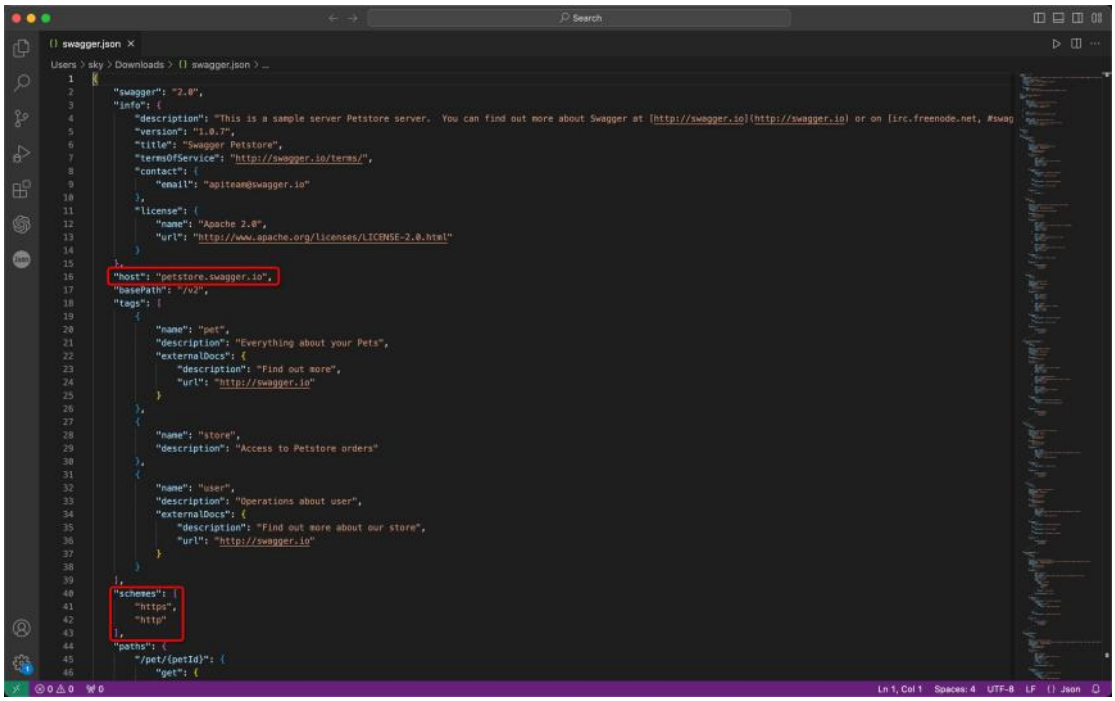


方式三：

若客户未使用 Swagger 工具进行开发和管理，需要导出以 swagger 格式为准的 json 文件，方可使用

3.1.8.3 注意事项

需要确保 json 文件中包含“host”和“schemas”字段，在某些不规范的开发过程下，导出的文件可能并不包含，需要手动补充添加，才可以实际扫描到接口



3.2 基线管理

Xray 目前版本支持 Linux 和 Windows 的基线检测

3.2.1 基线检查任务列表

在左侧导航栏中，选择“基线管理–基线检查任务列表”，进入基线检查任务列表界面。

3.2.1.1 内容展示

基线检查任务列表包括在线检查列表，离线批量列表和离线本地列表，展示系统创建的所有基线检查任务。

在线检查列表

列表包含检查任务名称、检查策略、扫描计划、检查结果、任务状态、操作：

- 任务名称；
- 检查策略：展示实际检查中勾选的检查策略，鼠标悬浮展示全部；
- 扫描计划：展示周期执行时间。鼠标悬浮展示任务执行周期和任务指定执行时间段；
- 检查结果：展示不合格检查项数量/已进行检查项数量/总检查项数量；
- 任务状态：展示任务执行状态；
- 操作：进行检测，编辑，删除操作。

点击任务所在行，可跳转至任务详情页。

离线批量列表

列表包含检查任务名称、检查策略、检查结果、最后检查时间、操作：

- 检查任务名称；
- 检查策略：展示实际检查中勾选的检查策略。鼠标悬浮展示全部；
- 检查结果：展示不合格检查项数量/已进行检查项数量/总检查项数量；
- 最后检查时间；
- 操作：进行编辑和删除操作。

点击任务所在行，可跳转至任务详情页。

离线本地列表

同离线批量列表。

3.2.1.2 筛选操作

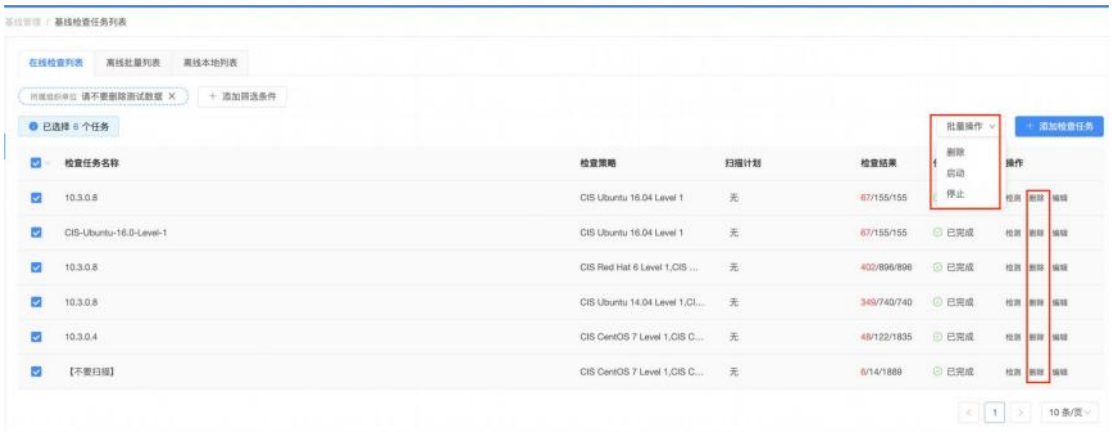
在列表页可对任务进行筛选操作，可根据扫描任务名称、检查策略、创建时间、任务状态（仅在线检查列表）、最近一次运行时间（仅在线检查列表），自由添加一个或多个条件进行筛选，操作说明如下:

- 点击“添加筛选条件”按钮；
- 在弹出的添加筛选条件对话框中配置筛选条件：
  - 选择要增加的筛选条件类型并填写相应的要筛选的内容；
  - 点击“添加筛选条件”，可以增加新的筛选限制条件；
  - 点击“删除”，可以删除掉不需要的筛选限制条件；
  - 筛选条件限制至少要添加一条；
- 设置好条件后，点击“保存”，筛选条件完成；
- 若想删除筛选条件，点击已添加条件右侧的“删除”按钮，即可删除条件。

3.2.1.3 删除操作

在列表页可以对任务进行删除操作，一旦执行删除操作，所有已选任务的删除条目均无法恢复，有以下两种途径：

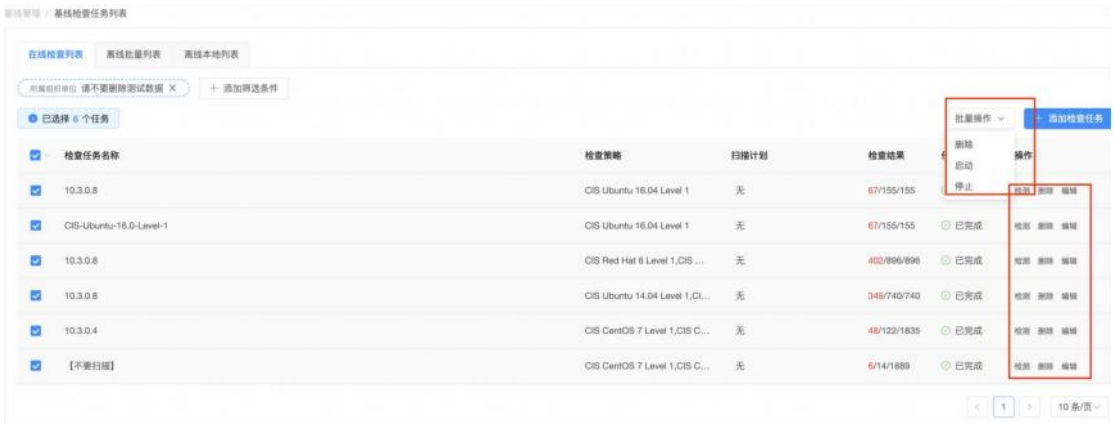
- 单个任务删除，
- 批量删除操作



3.2.1.4 立即扫描（仅在线检查列表）

对非队列中、进行中的任务，可以执行检查的操作，有以下两种途径：

- 单个任务执行检测，具体步骤为：
  - 点击任务右侧操作栏的“检测”，即可进行立即扫描的操作。任务扫描状态变为等待扫描或者正在扫描。
- 在列表页可以对任务进行批量检测操作，具体步骤为：
  - 选中要执行的扫描任务，此时会显示已选择的扫描任务总数；
  - 点击“执行选中的任务”，则任务扫描状态变为等待扫描或者正在扫描，弹窗显示提示；
  - 若选中任务存在“队列中”、“进行中”状态，则跳过该任务。



注意：

- 进行立即扫描的操作后，任务将按照最新保存的参数配置进行扫描；
- 系统正在扫描的任务达到了最大并发任务数时，新启动的任务将进入等待扫描状态。

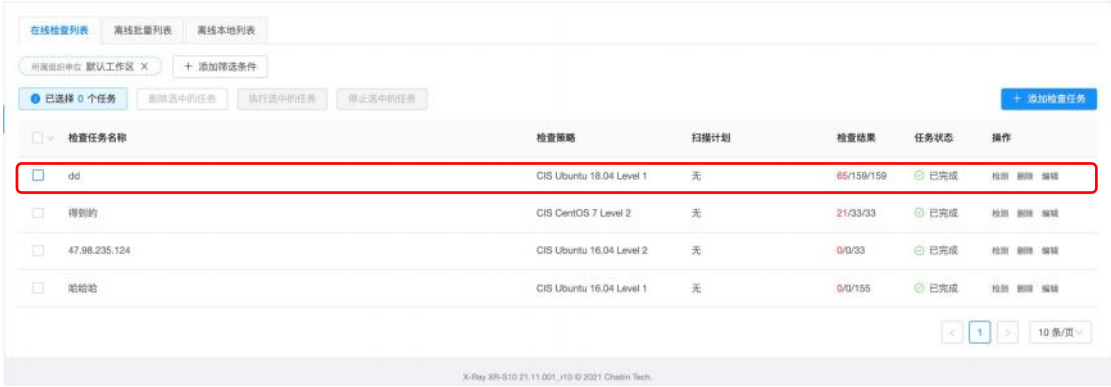
3.2.1.5 停止扫描（仅在线检查列表）

对正在扫描或等待扫描的任务，在列表页可以进行单个或批量停止扫描的操作，具体步骤为:

- 选中要停止的扫描任务，此时会显示已选择的扫描任务总数；
- 点击“停止选中的任务”，则弹窗显示提示“所有选中任务已停止”， 停止的任务状态显示为已完成。

3.2.2 检查任务详情

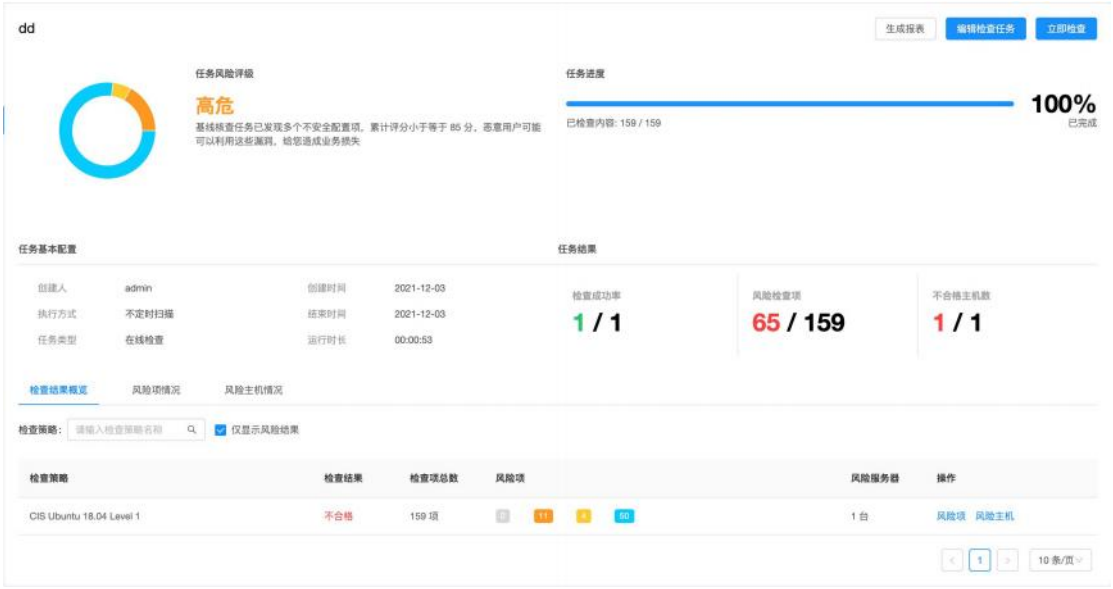
在任务详情页可以查看任务执行进度、任务配置和检查结果，以及离线批量和离线本地检查模式下的相关操作，还可对任务进行启动、停止、编辑等操作。



3.2.2.1 内容展示

页面分为任务时间轴、任务风险评级、任务进度、任务基本配置、任务结果、检查结果概览、风险项情况、风险主机情况、离线检查操作（仅离线检查任务）等模块。

说明：对于离线检查，初始下发任务后，任务统计处无数据显示，需要管理员按照离线检查操作中的内容进行手动操作任务下发后，将 output.json 上传后，才会显示相应数据。



任务时间轴，展示扫描历史：

- 在非展开状态下，时间轴包含标题、时间说明、展开操作；
- 点击展开，在展开状态下，以柱状图形式展示最近扫描记录，横轴为时间，纵轴为个数。
- 单次检查记录数据包括：
  - 风险主机数
  - 安全主机数
  - 未知主机数

任务风险评级：

- 以圆环图显示高、中、低风险的数量排列，数量为检查项的数量；
- 对风险进行评价，评价分为严重、高危、中危、低危、info 五个等级，评级说明、评价标准和计算方式如下：
- 评价标准：
  - 严重：基线核查任务已发现多个不安全配置项，累计评分小于等于 75 分，恶意用户可能可以利用这些漏洞，给您造成业务损失；
  - 高危：基线核查任务已发现多个不安全配置项，累计评分小于等于 85 分，恶意用户可能可以利用这些漏洞，给您造成业务损失；
  - 中危：基线核查任务已发现一些不安全配置项，累计评分小于等于 95 分，恶意用户可能可以利用这些漏洞，给您造成业务损失；

- 低危：基线核查任务已发现少量不安全配置项，累计评分在 95~100 分区间，恶意用户可能可以利用这些漏洞，给您造成业务损失；
- 安全：基线核查任务暂未发现存在不安全配置项，您的系统较为安全，请继续保持；
- 未知：基线核查任务暂未发现存在不安全配置项，但存在未知检查结果，请仔细确认结果。

- 评价标准：
  - 脆弱性元素分值
    - 每有一个严重，分值–5
    - 每有一个高危，分值–1
    - 每有一个中危，分值–0.5
    - 每有一个低危，分值–0.1
    - 每有一个 info，分值– 0.01
  - 资产或任务评分标准
    - 总分为 100 分
    - 安全评级：100
    - 低危评级：95 < x <100
    - 中危评级：85 < x <= 95
    - 高危评级：75 < x <= 85
    - 严重评级：0 < x <=75

- 计算方式：
  - 当任务开始下发时，任务风险显示为未知；
  - 检查结果 = 通过和未知时，不纳入计算；
  - 当所有检查项均完成执行后，若分值仍为 100：
    - 若系统中存在未知，则评价为未知；
    - 若均为安全，则评价为安全。

任务进度：

- 进度条和进度百分比：当前已进行检查的检查项数量与此次检查任务目标对象总数的比值；
- 已检查内容：数值展示当前已进行检查的检查项数量与/此次检查任务目标对象总数。

任务状态：

- 运行中——任务正在运行；
- 队列中——任务正在排队；
- 已完成——任务执行完成；
- 已失败——任务因各类原因导致中断检测，直接返回了失败（如网络不可达，超时等），鼠标悬浮可出现对应失败的 message 信息。

注意：离线检查任务的任务进度显示为 100%，任务状态显示为已完成或已失败。

任务基本配置：

- 创建人
- 执行方式：离线显示“-”
- 基线模式
  - 在线远程基线检查
  - 离线批量基线检查
  - 离线本地基线检查
- 创建时间
- 结束时间
- 运行时长

任务结果：

包含检查成功率，风险检查项，不合格主机数。

- 检查成功率：所有检查项均成功检查的主机数/总检查主机数；
- 风险检查项：风险项/总检查项；
- 不合格主机数：风险主机数/全部主机数。

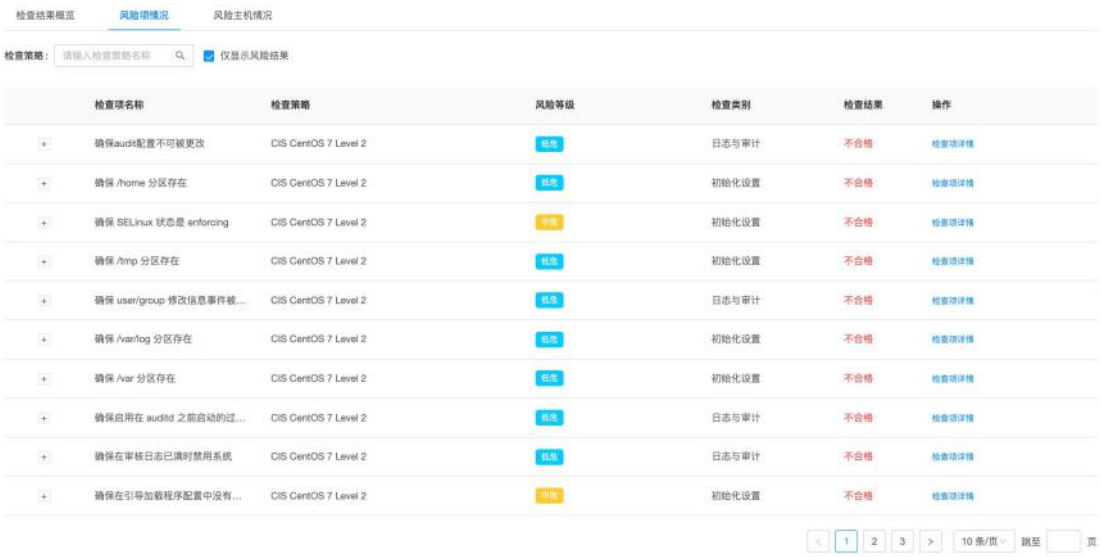
检查结果概览：

- 检查策略名称检索：
  - 可输入检查策略名称进行检索，支持模糊匹配，并允许基于输入在下方联想。
- 仅显示风险结果开关：
  - 若开启，检查结果概览页下，仅显示检查结果为不合格的检查策略；
  - 若关闭，检查结果概览页下，显示全部下发的检查策略。
- 内容展示：
  - 检查策略：
    - 显示检查策略名称，如 CIS_level2_CentOS6/7 安全核查。
  - 核查结果：
    - 合格：该检查策略下的所有检查项，所有检查项均为安全，则为安全；
    - 不合格：该检查策略下的所有检查项，存在不合格检查结果；
    - 未知：该检查策略下的所有检查项，不存在不合格的检查项，且存在未知的检查项包括 error。
  - 启用检查项数：
    - 该策略的检查项数总和数量统计。
  - 风险项：
    - 不合格的检查项，分别展示严重、高危、中危、低危的检查项数量。
  - 风险服务器：
    - 存在风险服务器的主机数。
  - 进行操作：
    - 风险项：可跳转到“风险项情况”页，附带选中的检查策略为筛选条件；
    - 风险主机：跳转到“风险主机情况”页，附带选中的检查策略为筛选条件。

风险项情况：

- 检查策略名称检索
  - 可输入检查策略名称进行检索，支持模糊匹配，并允许基于输入在下方联想。
- 仅显示风险结果开关
  - 若开启，检查结果概览页下，仅显示检查结果为不合格的检查项；
  - 若关闭，检查结果概览页下，显示全部下发的检查项。
- 内容展示
  - 检查项名称：展示具体单个检查项的名称。
  - 检查策略：展示该检查项所属的检查策略。
  - 风险等级：展示具体单个检查项的风险等级，若为原先扫描出来，但当前不存在的风险检查项，风险等级以低危展示。
  - 检查类别：展示检查项的检查类别

- 风险项检查结果
  - 该检查项下，若所有的主机检查结果均为合格，则判定检查项聚合结果为合格；
  - 该检查项下，若存在不合格的检查结果，则判定检查项聚合结果为未通过；
  - 该检查项下，若不存在不合格的检查结果，且存在未知的检查项，则判定检查项聚合结果为未知。
- 进行操作
  - 点击“检查项详情”后出现弹窗，包含：
    - 描述
    - 类型
    - 验证方法
    - 修复建议
- 检查项聚合结果为未通过时，点击对应行显示影响主机。

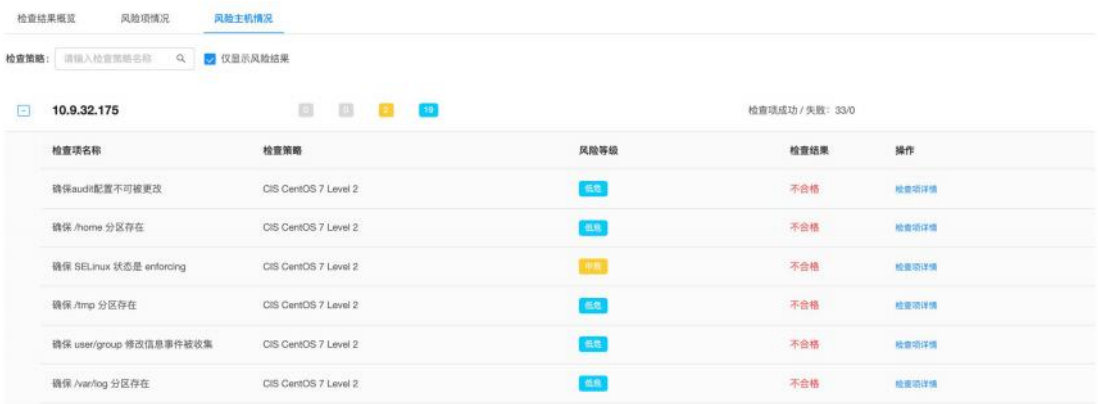


风险主机情况：

- 检查策略名称检索

- 可输入检查策略名称进行检索，支持模糊匹配，并允许基于输入在下方联想。

- 仅显示风险结果开关
  - 若开启，检查结果概览页下，仅显示存在风险检查项的主机列表；
  - 若关闭，检查结果概览页下，显示全部的主机列表。
- 内容展示：
  - 直接展示所有主机列表，不会受筛选而遭受影响。
  - 主机地址：IP 地址
  - 主机风险情况：分别展示严重、高危、中危、低危的风险数量。
  - 检查项成功/失败：主机检查情况，展示成功项数量/失败项数量：
    - 成功项数量 = 通过 + 未通过的检查项数量；
    - 失败项数量 = 未知 + error 的检查项数量。
  - 主机检查项详细列表：
    - 检查项名称
    - 检查策略
    - 风险等级
    - 检查结果
      - 通过：检查项执行成功且判定结果为通过，显示为绿色；
      - 未通过：检查项执行成功且判定结果为未通过，显示为红色；
      - 未知：标识该检查项执行失败，存在以下情况：
        - 该检查项执行失败，返回为 error，鼠标悬浮显示对应 error_message；
        - 该检查项执行失败，鼠标悬浮 message 显示“由于网络或其他未知原因，当前检查返回为空，建议重新检查”。
    - 操作：点击“检查项详情”可查看对应内容。



离线检查操作：

说明：离线检查类型任务启动后，系统会生成对应的配置文件，需要管理员下载配置文件和检查工具在目标主机上手动执行

- 管理员需按照离线检查操作页中提示的步骤进行操作，具体操作步骤如下:
  - 下载下方的离线检查工具和配置文件，其中:
    - baseline_tool_ 开头的工具为离线批量检查工具，Windows 系统选择 basel ine_tool_windows，Linux 系统选择 baseline_tool_linux，macOS 系统选择 baseline_tool_darwin。
    - baseline_checker_ 开头的工具为离线单机检查工具，本次任务不需要关心， 但是必须存在
    - config.json 为在洞鉴网页上下载的配置文件文件名
  - 根据执行检查的机器的操作系统，运行检查命令

    ssh_check --config --json_output

    - 具体到操作系统上，以 output.json 为输出路径的话，示例如下：
    - Windows 系统上，在 cmd.exe 或者 PowerShell 中运行检查工具
    - baseline_tool_windows.exe ssh_check --config config.json --json_output output.json
    - Linux 系统上，在终端中运行检查工具 ：./baseline_tool_linux ssh_check --config config.json -- json_output output.json
    - macOS 系统上，在终端中运行检查工具 ：./baseline_tool_darwin ssh_check --config config.json -- json_output output.json
  - 将检查结果输出文件 output.json，在下方“导入结果”处上传，即可查看 检查结果。


离线检查操作
检查项目
资产列表
检查项 id
cis_windows_server_2012_level_2
检查工具下载
前往基线检查全局配置下载
导入检查结果
支持文件格式：.json 文件或多个 .json 文件的 .zip 包
点击或将文件拖拽到这里上传
文件大小不超过 100 M
操作说明
1. 下载下方的离线检查工具和配置文件，其中：
baseline_checker_ 开头的工具为离线单机检查工具，其他文件本次任务不需要关心
2. 根据被检查的机器的操作系统，运行以下命令
工具文件名 check --set_id 检查项 id --local --host 被检查的机器 IP --json_output 输出文件名
具体到操作系统上，以 output.json 为输出路径，检查项 id 请见上方的检查项 id 项，以 cis_ubuntu_16.04_level_1 为例，示例如下：
Linux 系统上，在终端中运行检查工具
./baseline_checker_linux check --set_id cis_ubuntu_16.04_level_1 --local --host 1.1.1.1 --json_output output.json

3.2.2.2 进行操作

点击任务详情页面右上角的按钮，可以对任务进行一系列的操作。

编辑检查任务

- 在任务详情页可以修改扫描任务的参数配置，具体操作如下：
  - 点击右上角的“编辑扫描任务”
  - 进入编辑任务页面，修改任务的参数配置
    - 编辑扫描任务的方法与添加扫描任务基本相同，除了任务目标，基线模式，检查策略不可编辑
  - 配置完成后，点击“保存任务”后，任务数据会自动刷新，但不会自动进行检查

立即检查

- 在任务详情页，点击详情右上角 "立即扫描" 即可启动任务
- 如果此时任务详情展示的是历史的扫描结果，任务启动时，会按照该扫描历史的参数配置来启动任务
  - 启动后，任务可能立即开始扫描，也可能进入等待扫描。这取决于系统当前正在扫描的任务数量，是否达到了系统的最大任务并发数

停止扫描

- 任务正在检查或着等待检查时，若希望停止扫描或取消等待检查，可以点击右上角的“停止检查”


dd
生成报表
编辑检查任务
立即检查
任务风险评级
高危
基线核查任务已发现多个不安全配置项，累计评分小于等于 85 分，恶意用户可能可以利用这些漏洞，给您造成业务损失
任务进度
已检查内容: 159 / 159
100%
已完成
任务基本配置
创建人 admin
执行方式 不定时扫描
任务类型 在线检查
创建时间 2021-12-03
结束时间 2021-12-03
运行时长 00:00:53
任务结果
检查成功率
1 / 1
风险检查项
65 / 159
不合格主机数
1 / 1
检查结果概览
风险项情况
风险主机情况
检查策略：
仅显示风险结果
检查策略
检查结果
检查项总数
风险项
风险服务器
操作
CIS Ubuntu 18.04 Level 1
不合格
159 项
11
50
1 台
风险项
风险主机
10 条/页


编辑任务
任务基本信息
* 任务名称
dd
* 检查目标
手动输入
上传目标文件
25.25.205.57
优先级
高
中
低
任务速度
慢速模式
快速模式
控制基线任务并发的速度，快速模式支持并发 50 台主机
* 执行类型
不定时扫描
指定时间段
起始时间
至
结束时间
添加指定时间段
基线参数配置
基线模式
在线检查
在线远程基线检查可支持通过远程连接协议，如 ssh，对目标设备的相关文件进行读取，捕获不安全基线配置信息
检查策略
CIS Ubuntu 18.04 Level 1
取消
保存任务

3.2.3 添加基线任务

在基线任务列表界面，点击“ + 添加检查任务”，进入添加基线检查任务的入口：

3.2.3.1 任务配置

点击右上方“添加基线检查任务”按钮，出现基线检查任务配置的抽屉界面：

进入任务配置页面，设置任务的基本信息和基线参数配置

3.2.3.2 任务基本信息参数

任务名称（必填项）：

- 对该任务进行命名标识

任务目标（必填项）：

- 手动输入 – 按照提示的格式输入目标地址
- 文件上传 – 下载文件模板进行填充后上传，可用于批量站点的任务下发
  - 若选择文件上传方式，则无需填写下方基线参数配置的登陆方式等参数：

优先级（必填项）：

- 执行时被引擎扫描的优先级
- 可选择高优先级、中优先级、低优先级三种，默认为中优先级

任务速度（必填项）：

- 快速模式：支持并发 50 台主机；
- 低速模式：支持并发 20 台主机；
- 默认为快速模式；最大并发主机数越高，扫描速度越快，性能消耗越强。

执行方式（必填项）：

- 立即扫描
- 定时扫描一次

- 每天循环扫描
- 每周循环扫描
- 每月循环扫描

指定时间段（必填项）：

- 通过指定相应时间段控制任务的执行时间，当任务在指定时间段内未完成时将进入暂停状态，下次到达后将进行断点续扫。

3.2.3.3 基线参数配置

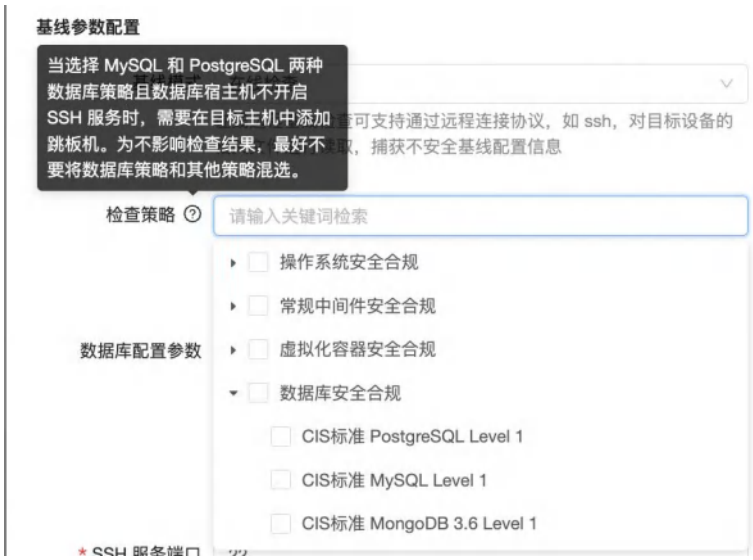
基线模式（必填）

分为”在线远程基线检查“、”离线本地基线检查“、”离线批量基线检查“三种模式

- 在线远程基线检查——在线远程基线检查可支持通过远程连接协议，如 ssh，对目标设备的相关文件进行读取，捕获不安全基线配置信息
- 离线本地基线检查——离线本地基线检查可支持通过本地程序运行的方式，对当前文件所在设备的配置进行读取，捕获不安全基线配置信息
- 离线批量基线检查——离线批量基线检查可支持通过生成配置文件和本地程序的方式，依赖堡垒机等介质设备对目标进行检查

检查策略（必填）

- 可以选择多个基线检查策略执行
- 支持按策略名称、检查对象、所属标准检索
- 支持跨检查对象类，勾选基线检查策略
- 策略受基线模式影响，对应模式将影响策略列表的加载
- 当选择 MySQL 和 PostgreSQL 两种数据库策略且数据库宿主机不开启 SSH 服务时，需要在目标主机中添加跳板机。为不影响检查结果，最好不要将数据库策略和其他策略混选。



数据库配置参数（非必填项）：

- 选择数据库 Mysql 和 PostgreSQL 数据库类策略必填，多种数据库参数可换行分隔，输入参数需要匹配对应的数据库配置格式。

登陆方式：必选，支持 SSH 或 SMB 的方式

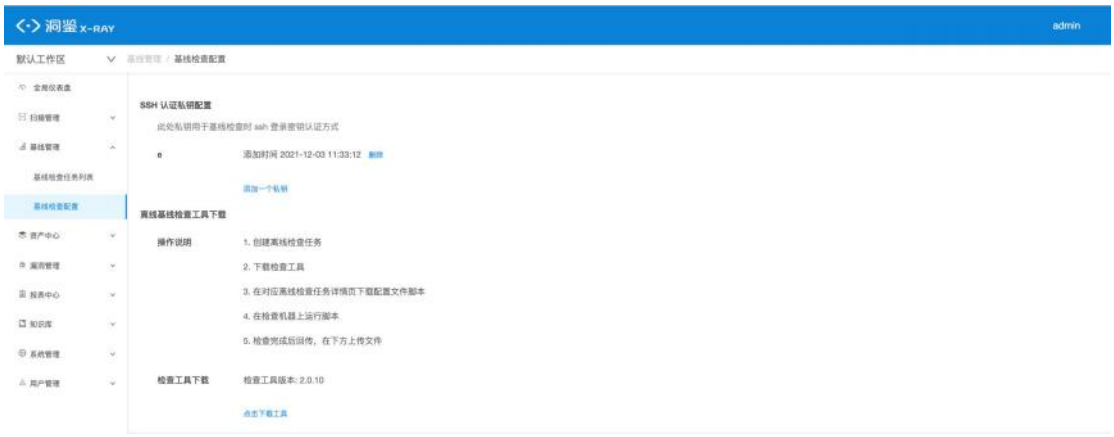
- SSH
  - SSH 端口（必填项）
  - SSH 用户名（必填项）
  - SSH 认证口令（必填项）
  - SSH 服务登录认证口令，分统一密码、SSH 私钥、两种类型
- SMB
  - SMB 端口（必填）
  - SMB 用户名（必填）
  - SMB 密码（必填）

任务执行

检查参数无误后，点击右下角的“仅创建任务”按钮或“创建并立即扫描任务”，即可创建任务。

3.2.4 基线检查配置

在左侧导航栏中，选择“基线管理–基线检查配置”，进入基线检查配置界面。

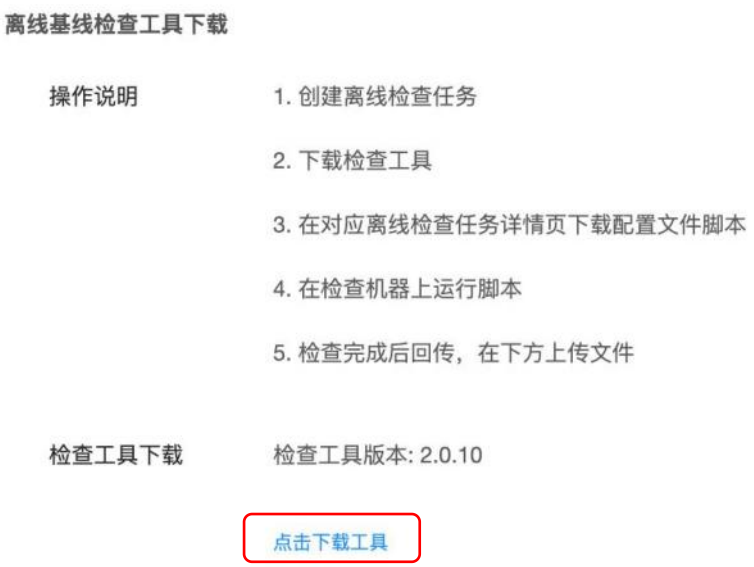


3.2.4.1 SSH 认证私钥配置

此处私钥用于基线检查时 ssh 登录密钥认证方式（如下图），通过添加私钥名称和 SSH 私钥，点击确认添加证明。

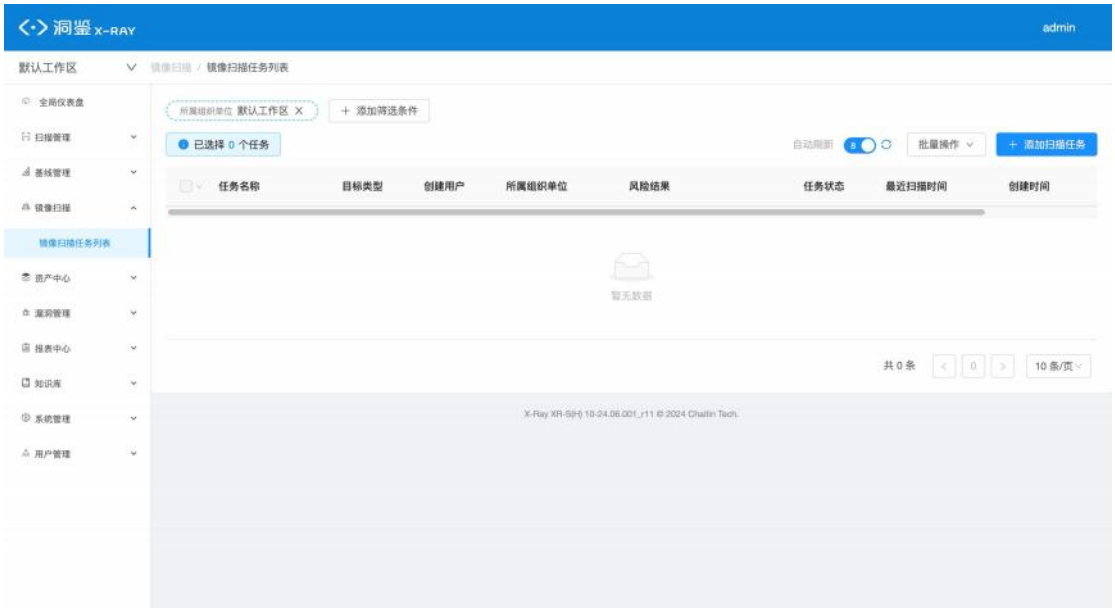
3.2.4.2 离线基线检查工具下载

包含操作说明，以及检查工具的版本信息和下载入口，点击进行下载



3.3 镜像管理

在左侧导航栏中，选择“基线管理–基线检查任务列表”，进入基线检查任务列表界面。



3.3.1 镜像扫描任务列表

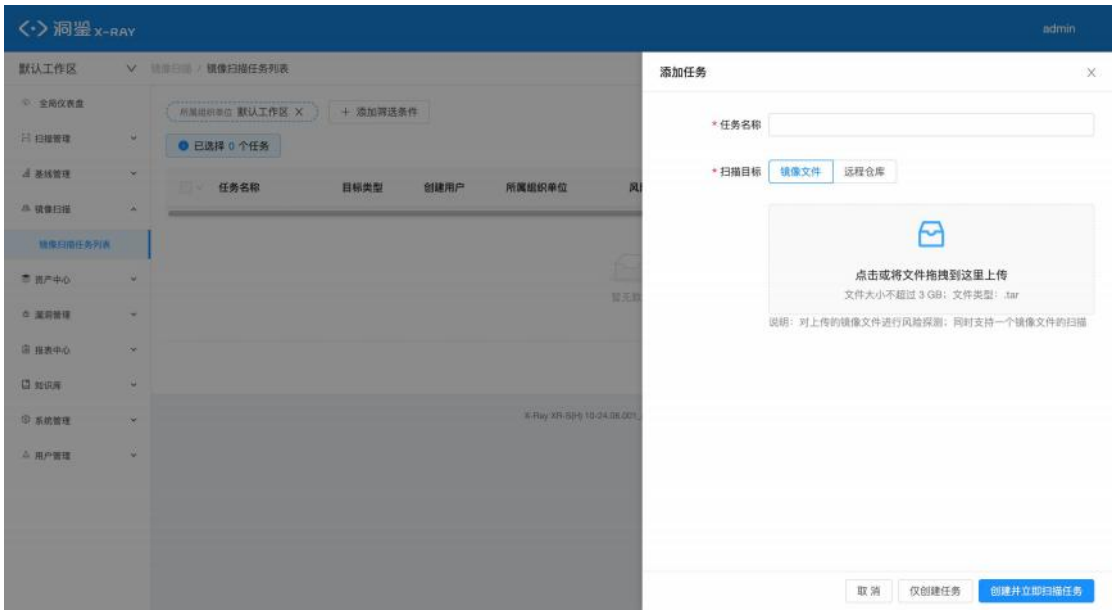
展示创建的镜像扫描列表，包含“任务名称”、“目标类型”、“创建用户”、“所属组织单位”、“风险结果”、“任务状态”、“最近扫描时间”、“创建时间”

支持对“所属组织单位”、“任务名称”、“任务状态”、“创建时间”、“最近扫描时间”进行筛选

支持对镜像扫描任务批量执行“删除”、“启动”、“停止”操作

3.3.2 添加镜像扫描任务

3.3.2.1 镜像文件



支持上传“.tar”格式的镜像文件，作为扫描目标

导出镜像的方式：

1. 找到要导出的镜像全名称(格式 registry/[path/]image[:tag])

   (1) repository：仓库名，通常是一个用户名或者组织名。

   (2) path：路径名，通常用于区分业务

   (3) image：镜像名称

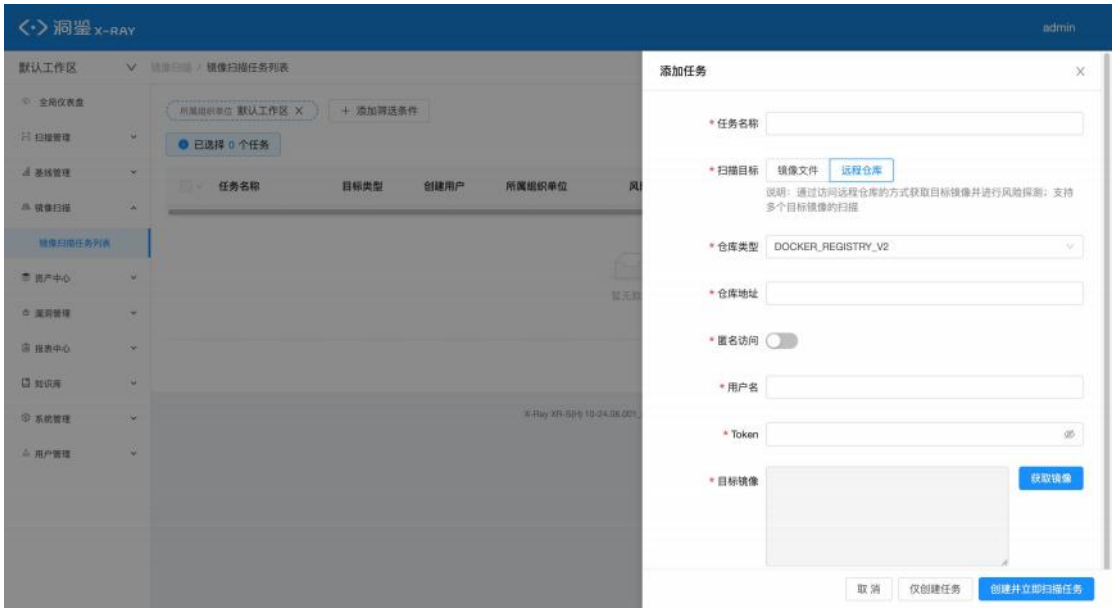
   (4) tag：标签，默认为 latest

2. 执行导出命令：

   (1) docker save –o nginx.tar 10.9.34.84:5000/nginx:latest

注：导出镜像 Tag 时，不能使用 tag 的 ID

3.3.2.2 远程仓库



通过远程登录镜像仓库上，获取镜像目标，进行扫描

注：该版本仅支持 DOCKER_REGISTAR_V2 的仓库类型

需要配置仓库地址、用户名、token，支持匿名访问

正确配置完上述信息后，点击“获取镜像”

在弹窗中选择，需要扫描的镜像文件

注：该版本每个镜像只获取其中一个版本，默认为 latest，当不存在 latest 则获取列表最后一个镜像

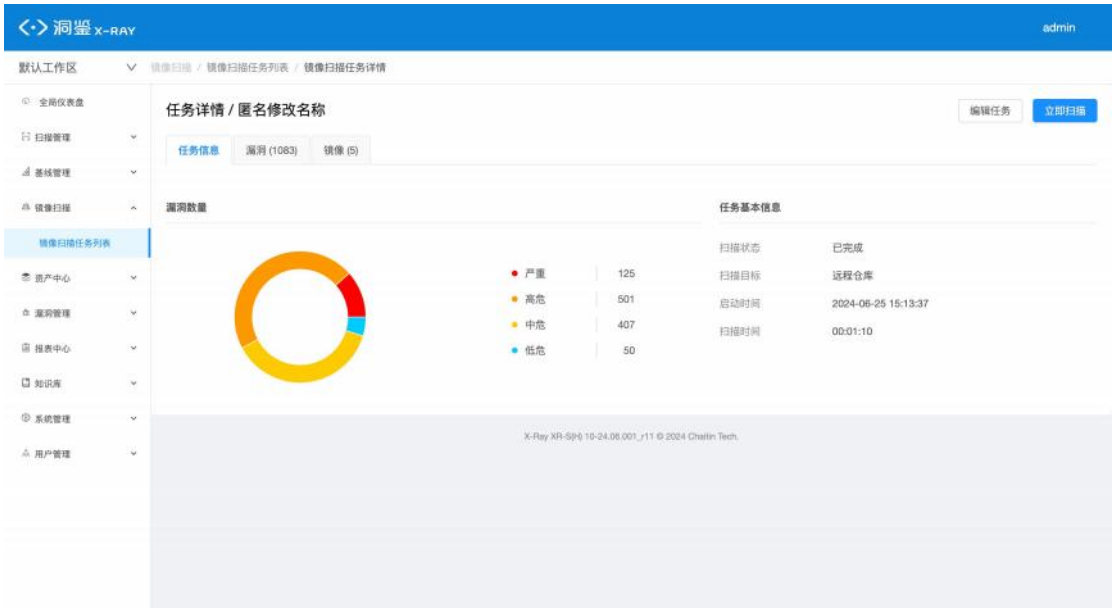
3.3.3 镜像扫描任务详情

3.3.3.1 任务信息

当扫描任务正在扫描中时，展示进度条，当扫描结束后，隐藏展示

展示漏洞数量分布图

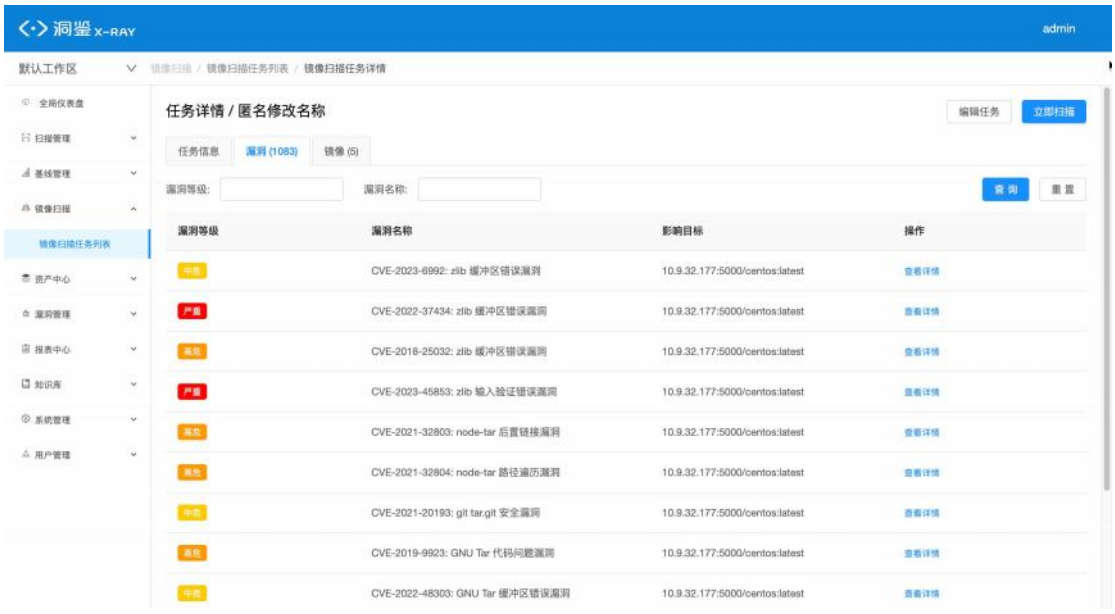
展示任务基本信息：包含扫描状态、扫描目标类型、启动时间、扫描时间



3.3.3.2 漏洞列表

展示镜像扫描版本匹配到的漏洞列表，包含“漏洞等级”、“漏洞名称”、“影响目标”字段

支持根据“漏洞等级”、“漏洞名称”进行筛选

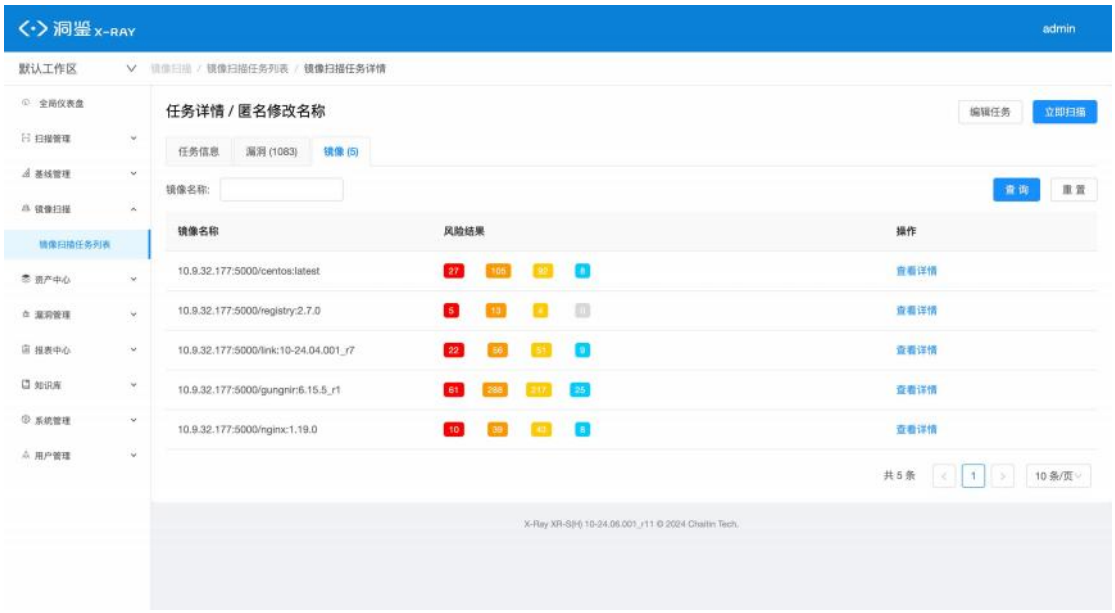


点击“查看详情”，可在弹窗中查看漏洞描述和漏洞修复方案等信息

3.3.3.3 镜像列表

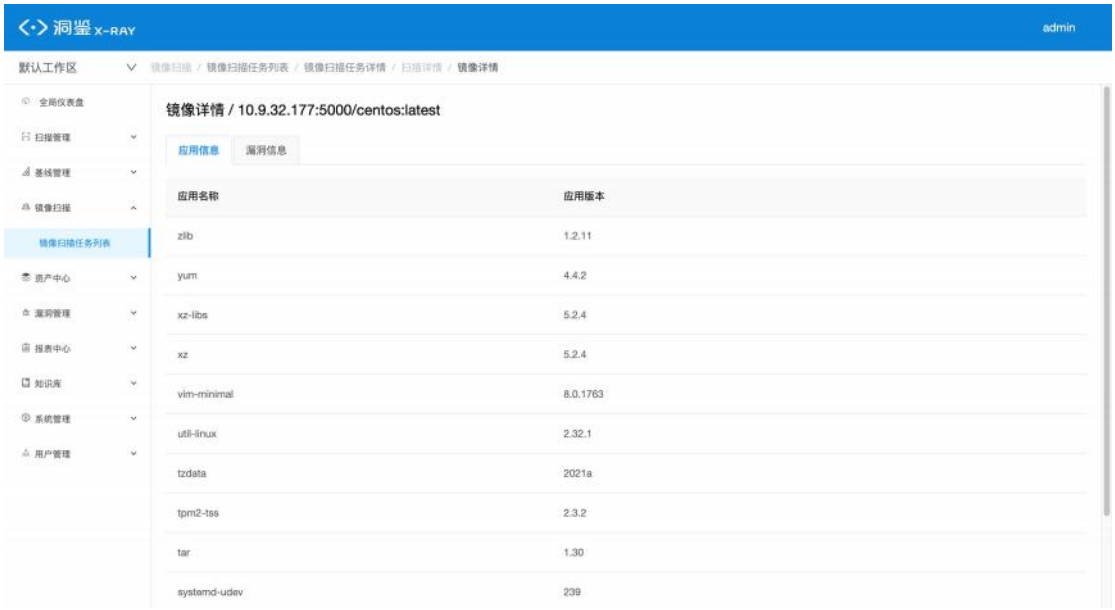
展示镜像扫描识别到的镜像列表，包含“镜像名称”、“风险结果”字段

支持通过镜像名称进行模糊匹配



点击“查看详情”，跳转查看镜像的应用信息和关联的漏洞信息

应用信息展示识别到的应用列表，包含“应用名称”、“应用版本”字段


洞鉴 X-RAY
admin
默认工作区
镜像扫描 / 镜像扫描任务列表 / 镜像扫描任务详情 / 扫描详情 / 镜像详情
全局仪表盘
扫描管理
基线管理
镜像扫描
镜像扫描任务列表
资产中心
漏洞管理
报表中心
知识库
系统管理
用户管理
镜像详情 / 10.9.32.177:5000/centos:latest
应用信息
漏洞信息
应用名称
应用版本
zlib 1.2.11
yum 4.4.2
xz-libs 5.2.4
xz 5.2.4
vim-minimal 8.0.1763
util-linux 2.32.1
tzdata 2021a
tpm2-tss 2.3.2
tar 1.30
systemd-udev 239

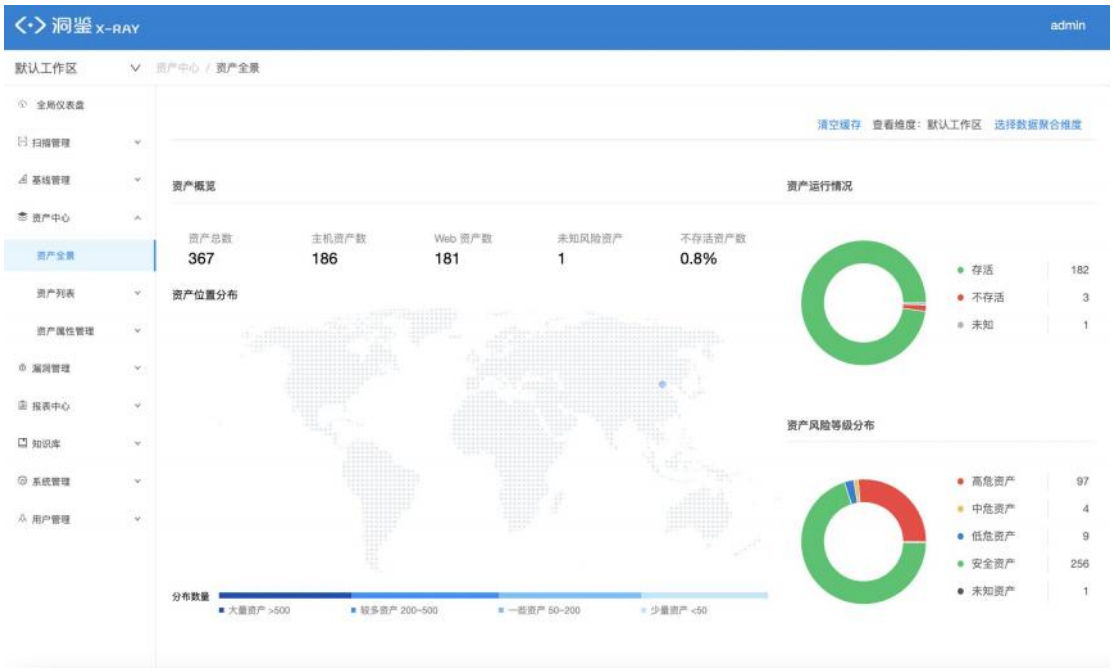
3.4 资产中心

此模块主要用于企业的资产进行管理，系统将企业的资产数据进行综合统计计算并可视化，方便直观的展示给用户，并支持对已知资产与未知资产进行集中管理，包括对资产的查询、筛选、添加、删除、快速扫描等操作。企业可对资产进行分组和指派责任人、管理员。

3.4.1 资产全景

在左侧导航栏中，选择“资产中心–资产全景”，进入基线检查配置界面。

此页面针对资产数据进行综合统计计算，生成可视化数据直观展示用户在资产管理场景下需要的数据，便于清楚当前所管理的资产情况，支持筛选查找和清空缓存。



3.4.1.1 内容展示

资产概览：

- 此处展示当前用户在系统中的资产管理关键指标及资产的地理位置分布；
- 展示的信息包括：
  - 资产总数，主机资产数，Web 资产数，未知风险资产（未做过安全检测的资产），不存活主机资产数（仅针对主机资产）及资产的地理位置分布。

资产运行情况：

- 此处展示当前用户在系统中各个资产的运行情况统计数据；
- 环状图展示主机资产的运行情况占比，鼠标悬浮在环状图上会出现相应的运行状态数量及占比。

资产风险等级分布：

- 此处展示当前用户在系统中资产的风险等级统计数据；
- 环状图展示资产的风险等级，鼠标悬浮在环状图上会出现资产的风险等级数量及占比

资产指纹画像：

- 此处展示当前用户在系统中的资产指纹的相关统计数据；
- 展示的信息包括：
  - 开放端口的资产占比及排名
  - 服务程序的资产占比及排名
  - 应用中间件的资产占比及排名
  - 设备类型的资产占比及排名
  - 操作系统的资产占比及排名
  - CMS 系统的资产占比及排名
  - 使用语言的资产占比及排名
- 点击标签可切换资产指纹；
- 鼠标悬浮在资产占比的表头上时会出现资产占比的计算公式。

业务系统资产分布：

- 此处展示当前用户在系统中资产的各业务系统使用资产的分布及排名情况；
- 展示的信息包括：
  - 左侧条状图展示业务系统资产的排名及占比
  - 右侧的表展示业务系统的排名及资产数量
- 左侧条状图基于右侧表变换数据；
- 鼠标悬浮在业务系统名字上时会出现业务系统的名字。

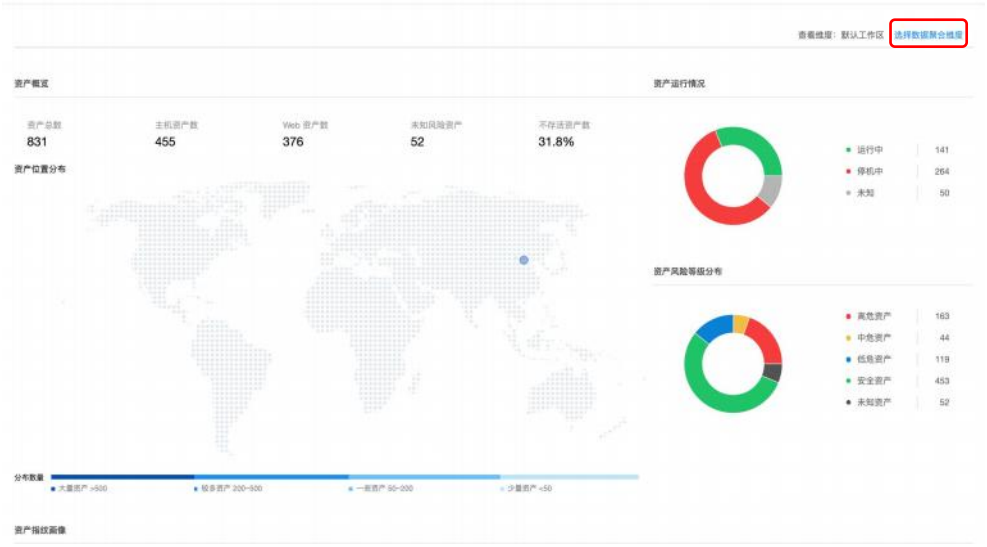
组织单位资产分布：

- 此处展示当前用户在系统中资产的组织单位资产分布及排名情况；
- 展示的信息包括：
  - 左侧柱状图展示组织单位的资产数量情况
  - 右侧表展示组织单位的资产数排名情况
  - 左侧柱状图图基于右侧表变换数据
- 鼠标悬浮在左侧柱状图的某项数据上会出现该组织单位的名字及资产数量；
- 鼠标悬浮在右侧表的组织单位名字上会出现该组织单位的名字。

3.4.1.2 筛选资产

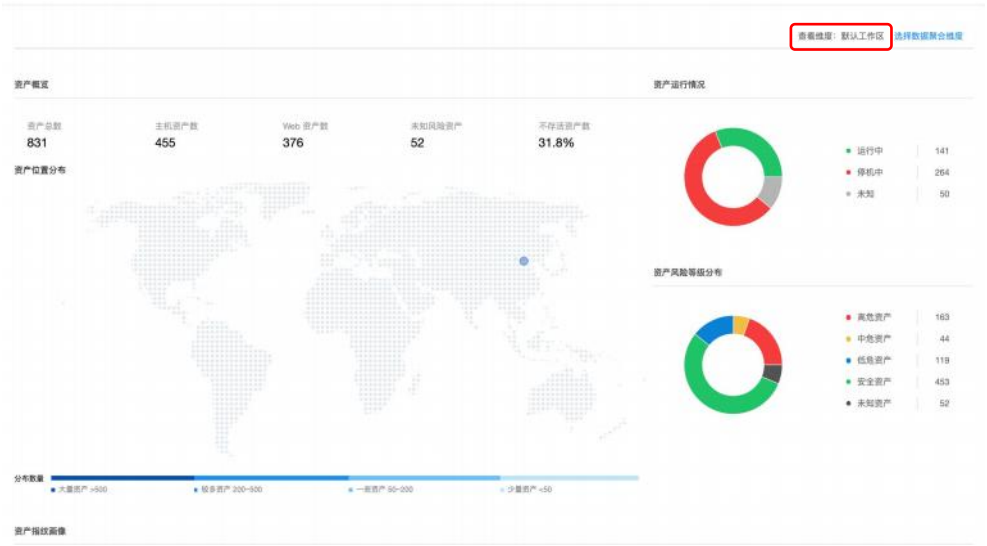
在资产全景页可对资产进行数据筛选操作，以改变资产全景页展示的数据，可根据业务系统，组织单位，所在地址，网络区域，标签进行多维度的筛选操作。具体操作为:

- 点击页面右上角的选择数据聚合维度：



- 弹出筛选条件对话框。由于数据量比较大，多维度的筛选可能会影响页面性能；

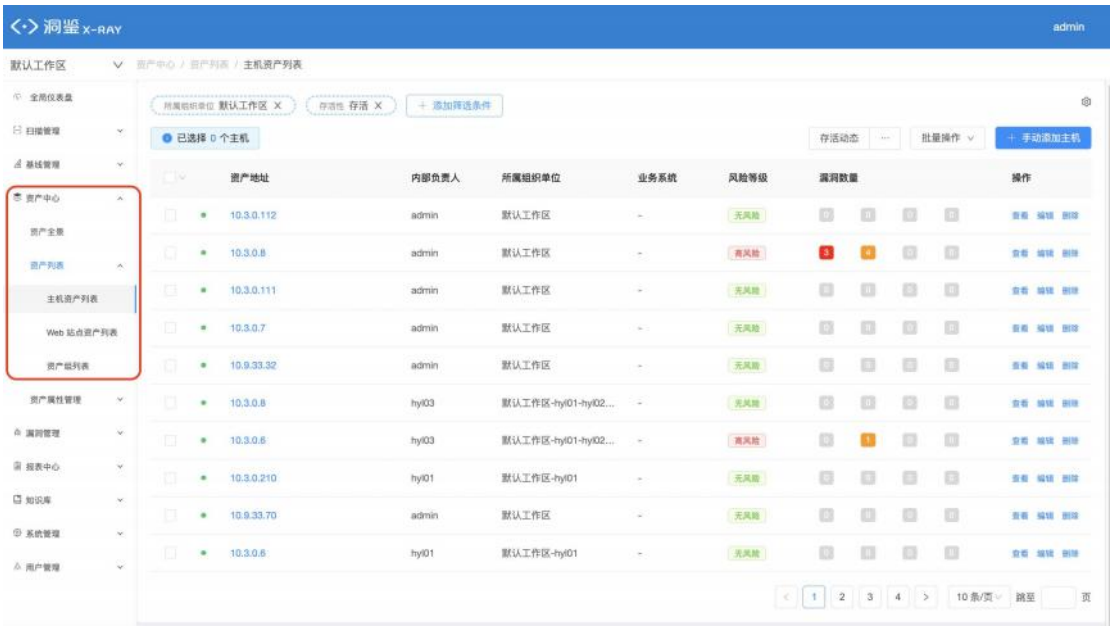
- 筛选的条件会在全景页的右上角“查看维度：xxx”展示，悬浮在维度上会出现所有筛选的维度；



- 填写想要筛选的内容，并按下“聚合维度”按钮进行筛选；
- 想要重置筛选内容，可以点击“重置条件”按钮，清空筛选对话框的内容，再点击“聚合维度”按钮，将筛选的资产复原。

3.4.2 主机资产

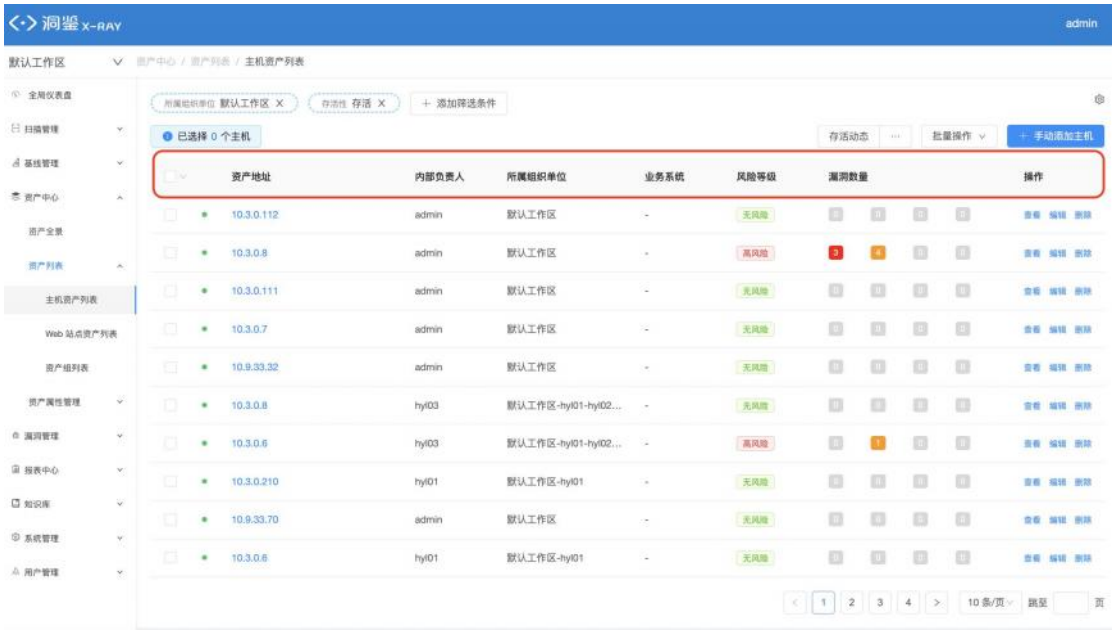
在左侧导航栏中，选择“资产中心–资产列表–主机资产列表”，进入主机资产列表界面。



3.4.2.1 主机资产列表

内容展示：

主要展示所有的主机资产信息，内容包括：资产运行情况（资产地址前的圆点）、主机资产地址、资产负责人、所属组织单位、业务系统、风险等级和各漏洞等级数量：

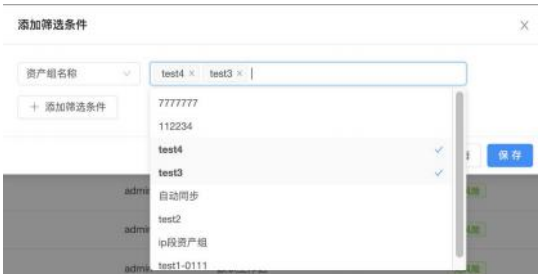


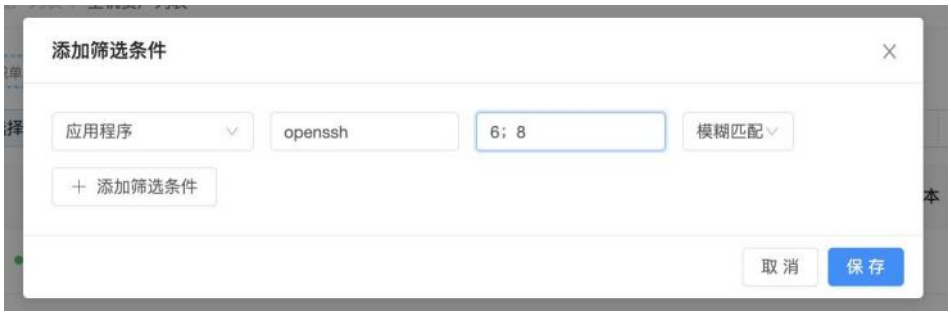
筛选主机：

在主机资产列表页可对主机资产进行筛选，可根据资产地址、风险等级、内部负责人、外部负责人、 组织单位、业务系统、标签、网络区域、操作系统、设备类型、资产名称、所在地址、端口、应用程序、服务类型，自由添加一个或多个条件进行筛选，具体操作说明如下:

- 点击“添加筛选条件”按钮，弹出添加筛选条件对话框；
- 选择要增加的筛选条件类型并填写相应的要筛选的内容；
- 点击“增加一个筛选条件”，可以增加筛选限制条件；
- 点击“删除”，可以删除掉不需要的筛选限制条件；
- 筛选条件限制至少要添加一条；
- 设置好条件后，点击“保存”，即可展示符合筛选条件的列表。
- 筛选条件按照使用优先级进行排序
  - 例：选择“相关扫描任务”和“资产组名称”的筛选条件，允许用户根据扫描任务和所在资产组名称进行多组筛选。
  - 筛选功能优化：

- 选择“应用程序”筛选条件，可进行应用程序版本号的批量搜索，不同版本之间用英文符号“;”分隔。





添加主机：

在资产列表页可以通过手动添加一个或导入 cvs 文件的方式添加资产，方便管理员添加企业资产，具体操作为：

- 在列表页点击 " + 手动添加 XX 资产"，显示填写内容的弹窗：

- 选择添加方式：
  - 手动添加一个资产
  - 上传资产文件（上传资产文件完全后，会提醒资产的上传结果）

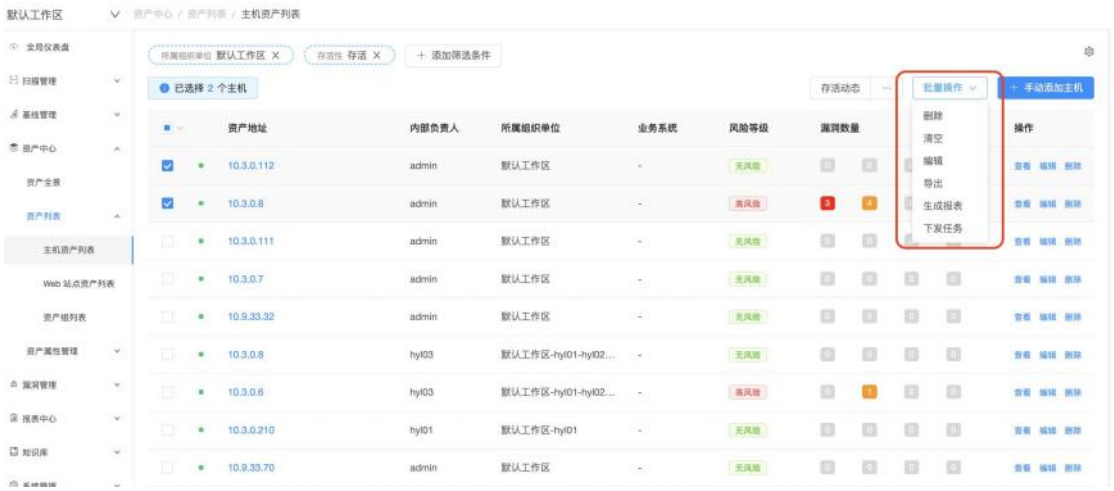
- 

- 按照不同方式的添加要求，填写选择资产相关信息包含（资产地址、资产名称、所在地址、组织单位、内部负责人、外部负责人、资产组、资产权重、业务系统、网络区域、标签）；
- 点击“确定”按钮，完成资产添加。
- 注意：
  - 已经存在的资产不能被重复添加；
  - 上传文件格式必须严格按照模板提供的格式添加，不同资产列表的模板不一样，请下载查看生成主机资产报表。

生成报表：

在主机列表页可以选择多个主机并生成所选主机的报表，具体操作为:

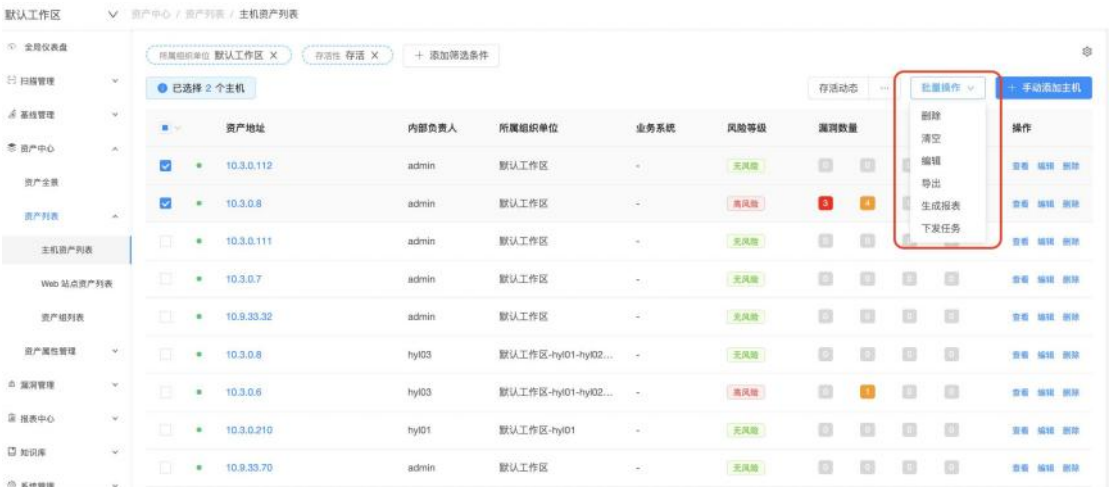
- 选中希望生成报表的主机资产，此时显示已选择的主机资产总数，同时“批量操作”–“生成报表”按钮变为可点击状态；
- 点击“批量操作”–“生成报表”按钮；
- 在弹出的窗口中，输入相应的生成配置；
- 点击“确认”，即可开始生成报表。可以前往报表管理页面查看报表生成的情况，或下载生成好的报表。
- 当选择超过一个主机资产时，可生成“资产对比报表”。



删除主机：

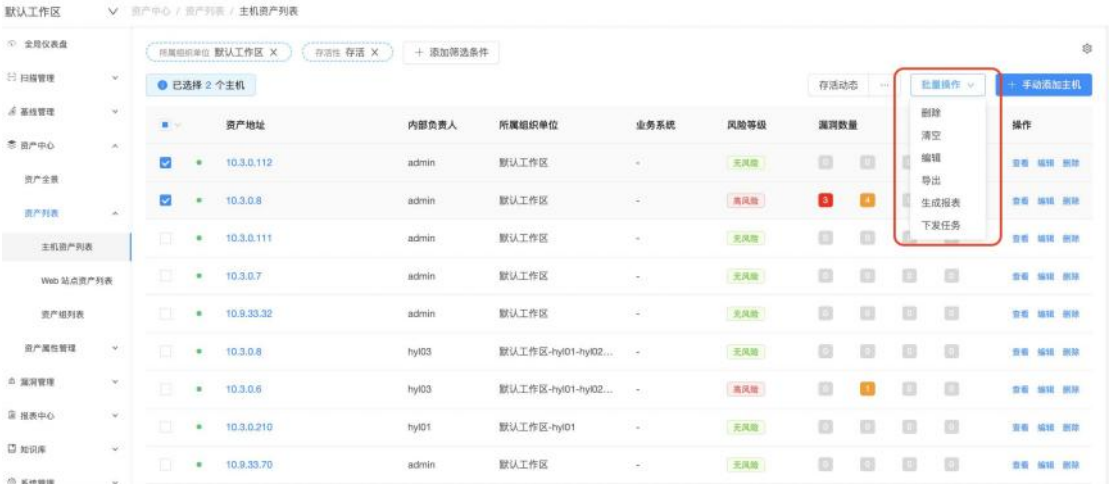
在主机资产列表页可以主机资产进行批量删除，一旦执行了删除操作，所有选中的主机资产信息均将被删除，具体操作为:

- 选中要删除的主机资产，此时显示已选择的主机资产总数；
- 点击“删除选中的主机”按钮，提示框提示确定是否删除，点击“确定”，则删除成功。



编辑选中的主机：

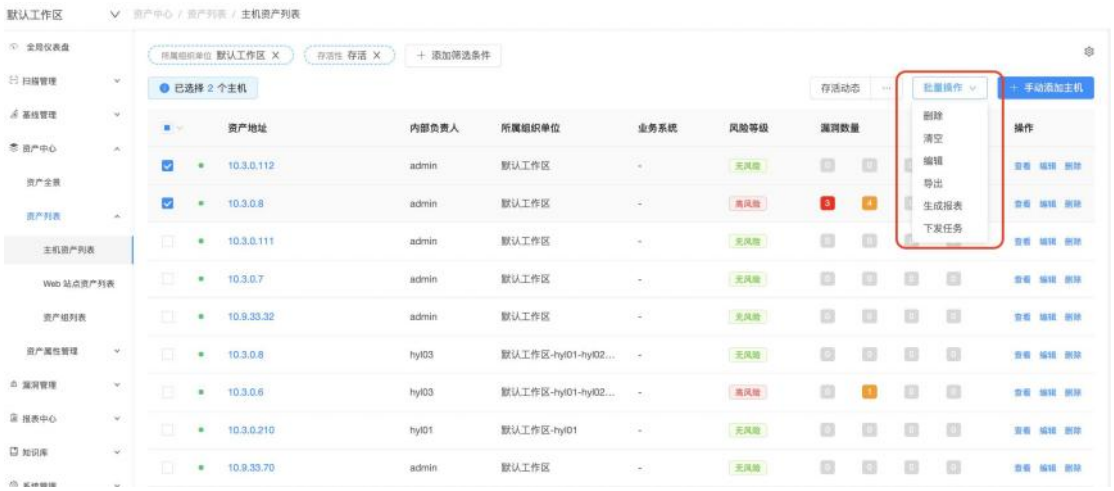
- 选中要编辑的主机资产，填写目标信息
- 点击确定或者取消操作

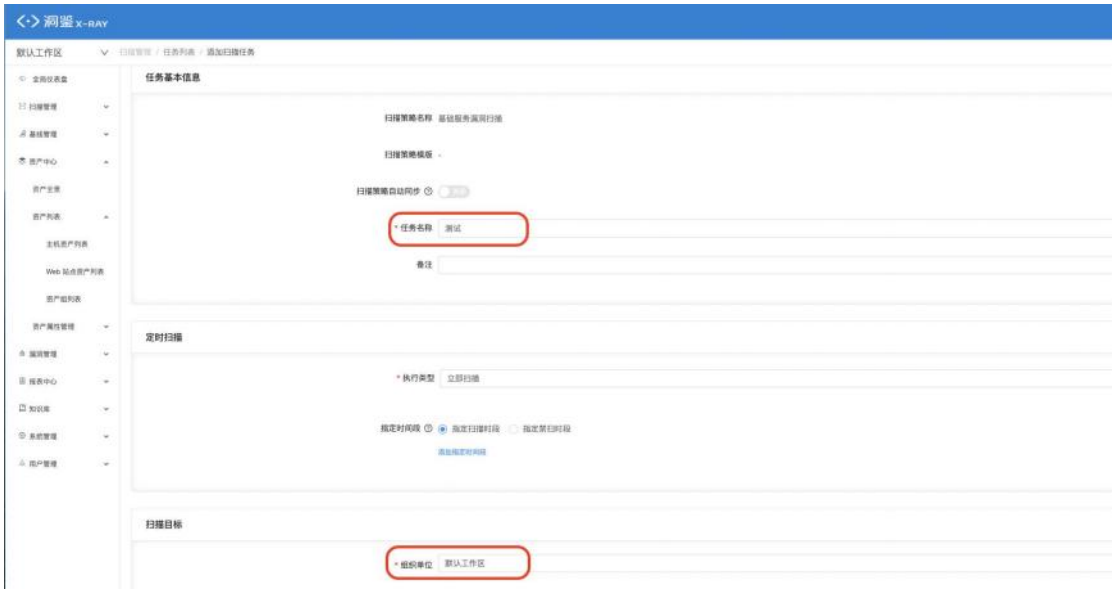


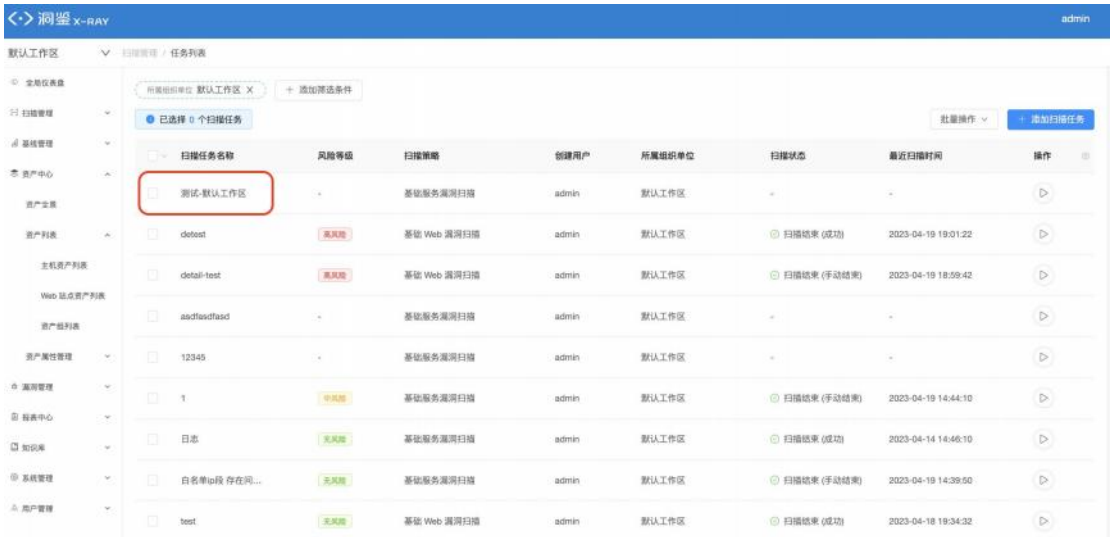
快速扫描主机：

在主机资产列表页可以对选中主机资产进行快速扫描，具体操作为:

- 选中要扫描的主机资产，此时显示已选择的主机资产总数；
- 当以选中主机资产创建扫描任务时，创建的扫描任务名称会自动变为：“任务名称+所在组织单位名称”
- 点击 “批量操作”–“下发任务”按钮，跳转至添加扫描任务界面 添加扫描任务界面，扫描目标处会自动填写进第一步中选中的主机资产，具体参数 配置参考 3.1.5 添加扫描任务。


默认工作区
资产中心 / 资产列表 / 主机资产列表
全局仪表盘
扫描管理
基线管理
资产中心
资产全景
资产列表
主机资产列表
Web 站点资产列表
资产组列表
资产属性管理
漏洞管理
报表中心
知识库
所属组织单位 默认工作区
存活性 存活
添加筛选条件
已选择 2 个主机
存活动态
批量操作
手动添加主机
删除
清空
编辑
导出
生成报表
下发任务
资产地址
内部负责人
所属组织单位
业务系统
风险等级
漏洞数量
操作
10.3.0.112 admin 默认工作区
10.3.0.8 admin 默认工作区
10.3.0.111 admin 默认工作区
10.3.0.7 admin 默认工作区
10.9.33.32 admin 默认工作区
10.3.0.8 hyl03 默认工作区-hyl01-hyl02...
10.3.0.6 hyl03 默认工作区-hyl01-hyl02...
10.3.0.210 hyl01 默认工作区-hyl01
10.9.33.70 admin 默认工作区

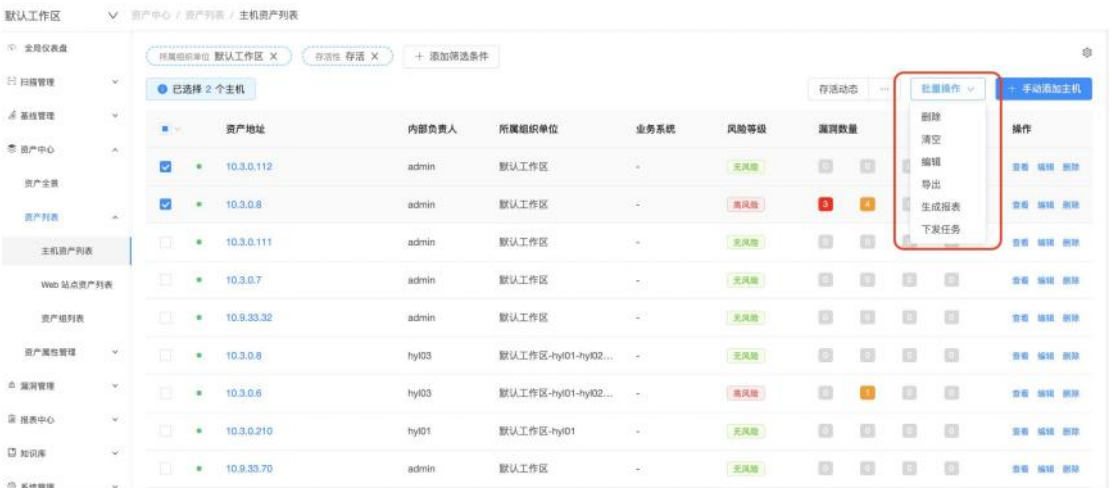

洞鉴 X-RAY
默认工作区
任务基本信息
扫描策略名称 基础服务漏洞扫描
扫描策略模版
扫描策略自动同步
* 任务名称 测试
备注
定时扫描
* 执行类型 立即扫描
指定时间段
扫描目标
* 组织单位 默认工作区


洞鉴 X-RAY
admin
默认工作区
扫描管理 / 任务列表
所属组织单位 默认工作区
添加筛选条件
已选择 0 个扫描任务
批量操作
添加扫描任务
扫描任务名称
风险等级
扫描策略
创建用户
所属组织单位
扫描状态
最近扫描时间
操作
测试-默认工作区 基础服务漏洞扫描 admin 默认工作区
detest 基础 Web 漏洞扫描 admin 默认工作区 扫描结束 (成功) 2023-04-19 19:01:22
detail-test 基础 Web 漏洞扫描 admin 默认工作区 扫描结束 (手动结束) 2023-04-19 18:59:42
asdfasdfasd 基础服务漏洞扫描 admin 默认工作区
12345 基础服务漏洞扫描 admin 默认工作区
1 基础服务漏洞扫描 admin 默认工作区 扫描结束 (手动结束) 2023-04-19 14:44:10
日志 基础服务漏洞扫描 admin 默认工作区 扫描结束 (成功) 2023-04-14 14:46:10
白名单ip段 存在问... 基础服务漏洞扫描 admin 默认工作区 扫描结束 (手动结束) 2023-04-19 14:39:50
test 基础 Web 漏洞扫描 admin 默认工作区 扫描结束 (成功) 2023-04-18 19:34:32

导出选中的主机：

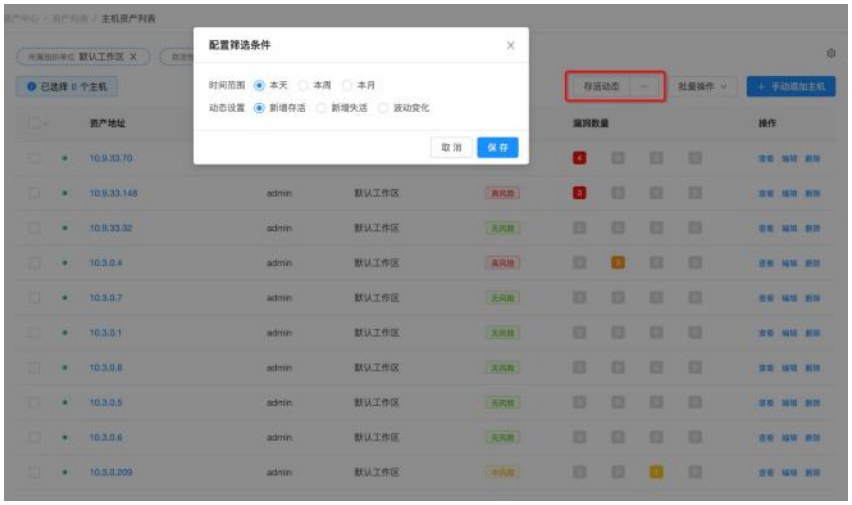
在主机资产列表页可以选择多个主机并导出所选主机的地址，具体操作为:

- 选中希望导出的主机地址，此时显示已选择的主机资产总数，同时"导出"按钮变为可点击状态；
- 点击“导出”，系统将自动把选中的资产地址存为 txt 文件。

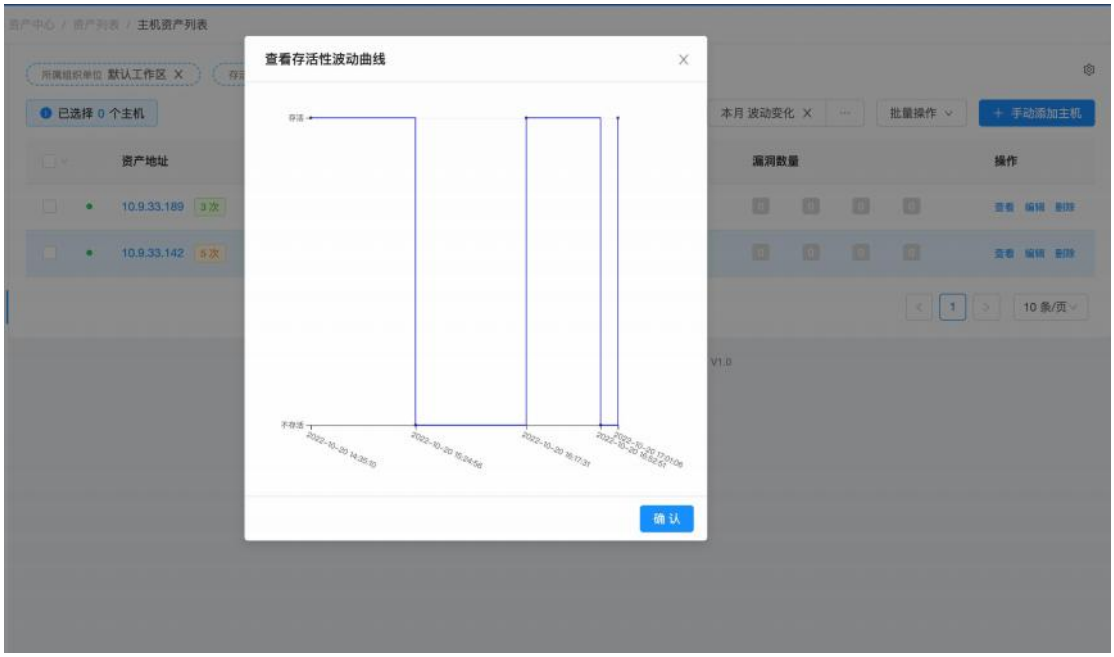


存活动态快速筛选：

在主机资产列表页可以配置时间维度和动态维度，来查看一段时间内资产存活性的动态变化:



对于筛选后的资产，可以在资产地址后面看到“新增存活”、“新增失活”、“波动次数”的标签，点击标签，可以查看资产存活性变化的情况：

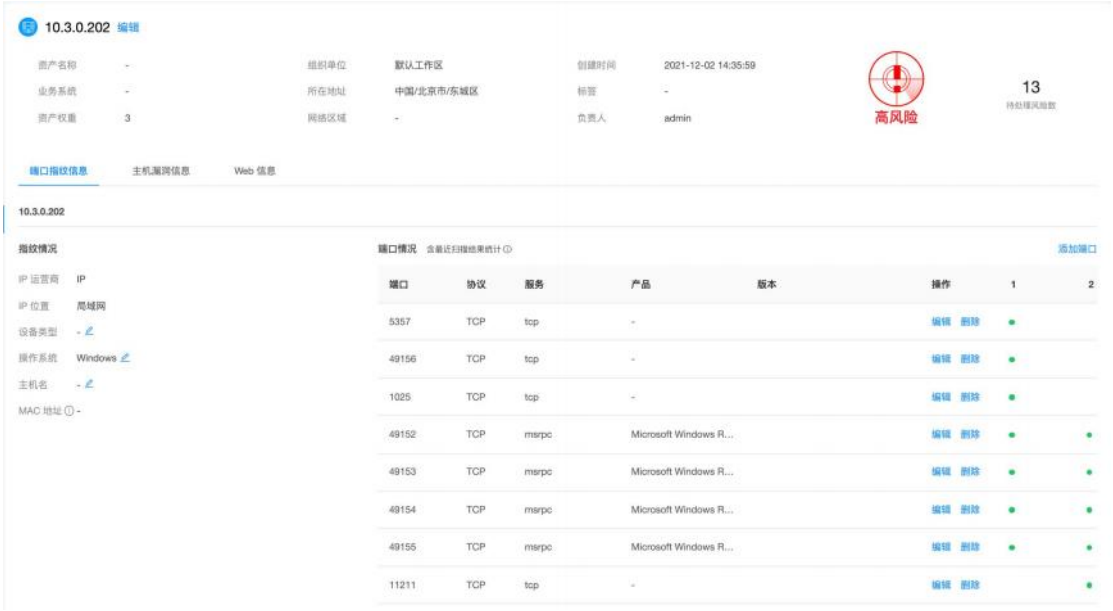


3.4.2.2 主机资产详情

在主机列表处，点击“查看”，即可打开主机详情界面。

内容展示：

主机详情页顶部主要展示主机的资产名称，组织单位，创建时间，业务系统，所在地址，标签，网络区域，负责人及资产风险等级图标：



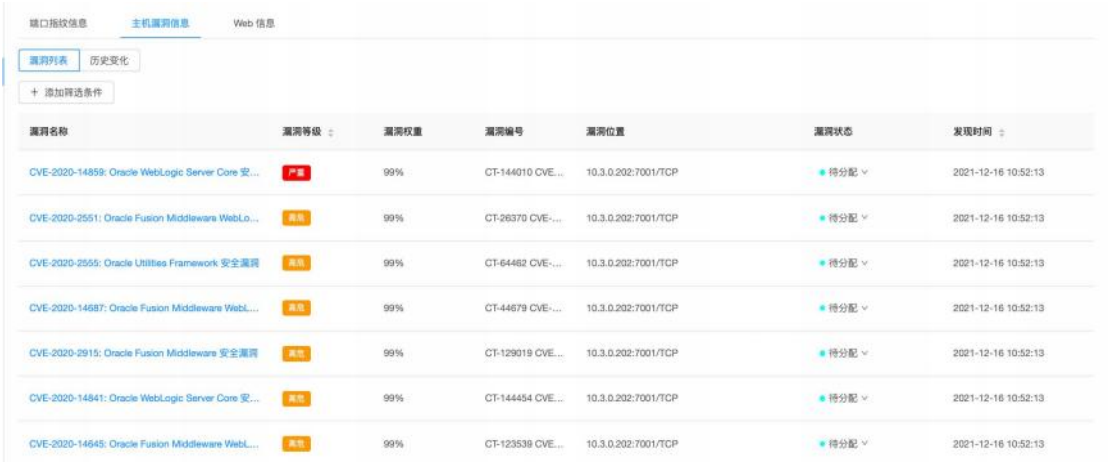
端口指纹信息：

此选项主要展示当前主机资产的指纹情况与端口开发情况，包括 IP 运营商，IP 位置， 设备类型，操作系统，主机名，端口，协议，服务，产品，产品的版本（如上图所示）：

- 设备类型可以在此手动修改，点击设备类型右侧的图标即可编辑；
- 操作系统可以在此手动修改，点击网络区域右侧的图标即可编辑；
- 主机名可以在此手动修改，点击主机名右侧的图标即可编辑。

主机漏洞信息：

此选项卡主要展示与当前主机相关的所有漏洞信息，内容包括漏洞名称、漏洞等级、漏洞权重、存在漏洞的位置、发现时间：



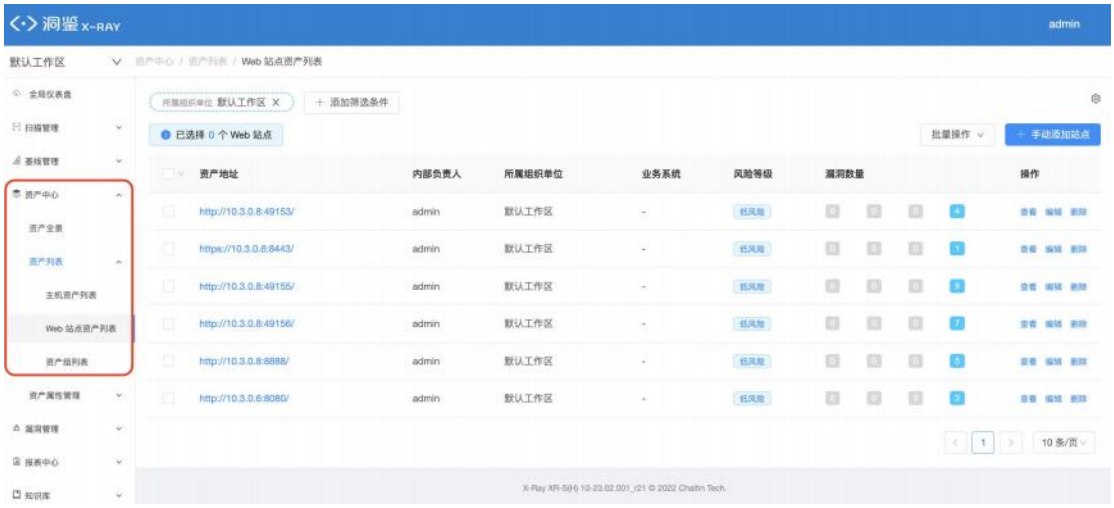
- 点击“风险等级”、“发现时间”右侧的三角图标，可以将列表按风险等级、发现时间升序或者降序排列；
- 点击漏洞名称，可以跳转至漏洞详情页面。

Web 信息：

此选项卡主要展示与当前主机相关 web 站点信息，内容包括 web 站点地址：

3.4.3 Web 站点资产列表

在左侧导航栏中，选择“资产中心–资产列表–Web 站点资产列表”，进入 Web 站点资产界面。



3.4.3.1 Web 站点资产列表

内容展示：

主要展示所有的 Web 资产信息，内容包括资产地址、负责人、所属组织单位、业务系统、风险等级和各等级下漏洞数量：

筛选 Web 站点：

在 Web 资产列表页可对 Web 站点资产进行筛选操作，可根据资产地址、风险等级、负责人、组织单位、业务系统、标签、网络区域、资产名称、所在地址、web 应用、网站 title、开发语言、CMS、WAF、CDN，自由添加一个或多个条件进行筛选，具体操作为：

- 点击“添加筛选条件”按钮，弹出添加筛选条件对话框；
- 选择要增加的筛选条件类型并填写相应的要筛选的内容；
- 点击“增加一个筛选条件”，可以增加筛选限制条件；
- 点击“删除”，可以删除掉不需要的筛选限制条件；
- 筛选条件限制至少要添加一条；
- 设置好条件后，点击“保存”，即可展示符合筛选条件的列表。

添加 Web 站点：

在资产列表页可以通过手动添加一个或导入 cvs 文件的方式添加资产，方便管理员添加企业资产，具体操作为:

- 在列表页点击 " + 手动添加 XX 资产"，显示填写内容的弹窗
- 选择添加方式：
  - 添加一个资产
  - 上传资产文件
- 按照不同方式的添加要求，填写资产相关信息；
- 点击“确定”按钮，完成资产添加。
- 注意：
  - 已经存在的资产不能被重复添加；
  - 上传文件格式必须严格按照模板提供的格式添加，不同资产列表的模板不一样，请下载查看。

生成 Web 站点资产报表：

在 Web 站点列表页可以选择多个 Web 站点并生成所选站点的报表（如下图所示），具体操作为:

- 选中希望生成报表的 Web 站点资产，此时显示已选择的 Web 站点资产总数，同时“批量操作”–“生成报表”按钮变为可点击状态；
- 点击“批量操作”–“生成报表”按钮；
- 在弹出的窗口中，选择相应的生成配置；
- 点击“确认”，即可开始生成报表。可以前往报表管理页面查看报表生成的情况，或下载生成好的报表。

编辑选中的 Web 站点：

- 选中要编辑的主机资产，填写目标信息；
- 点击确定或者取消操作。

删除选中 Web 站点：

在 Web 站点列表页可以对 Web 站点资产进行批量删除，一旦执行了删除操作，所有选中的 Web 站点资产信息均将被删除，具体操作为：

- 选中要删除的 Web 站点资产，此时显示已选择的 Web 站点资产总数，同时“删除选中的 Web 站点”按钮变为可点击状态；
- 点击“删除选中的 Web 站点”按钮，在弹出的是否确定删除的提示框中，点击“确定”，则删除成功。

快速扫描 Web 站点

在 Web 站点列表页可以对选中 Web 站点资产进行快速扫描，具体操作为：

- 选中要扫描的 Web 站点资产，此时显示已选择的 Web 站点资产总数，同时“批量操作”–“下发任务”按钮变为可点击状态；
- 点击“批量操作”–“下发任务”按钮，跳转至添加扫描任务界面；
- 添加扫描任务界面，扫描目标处会自动填写进第一步中选中的 Web 站点资产
- 当以选中 Web 站点资产创建扫描任务时，创建的扫描任务名称会自动变为：“任务名称+所在组织单位名称”，同主机资产。
- 在添加扫描任务界面，具体参数配置参考 3.1.5 添加扫描任务。


所属组织单位 默认工作区 X
+ 添加筛选条件
已选择 2 个 Web 站点
批量操作
+ 手动添加站点
删除
清空
编辑
生成报表
下发任务
资产地址
内部负责人
所属组织单位
业务系统
风险等级
漏洞数量
操作
http://10.3.0.8:49153/ admin 默认工作区 - 低风险
https://10.3.0.6:8443/ admin 默认工作区 - 低风险
http://10.3.0.8:49155/ admin 默认工作区 - 低风险
http://10.3.0.8:49156/ admin 默认工作区 - 低风险
http://10.3.0.8:8888/ admin 默认工作区 - 低风险
http://10.3.0.6:8080/ admin 默认工作区 - 低风险
查看 编辑 删除
1
10 条/页

3.4.3.2 Web 站点资产详情

在 Web 站点资产列表处，点击“查看”，即可打开 Web 站点详情界面。

内容展示：

此页面顶部展示 web 资产的资产名称，组织单位，创建时间，业务系统，所在地址，标签，资产权重，网络区域，负责人，资产风险等级图标以及待处理风险数：

Web 指纹信息：

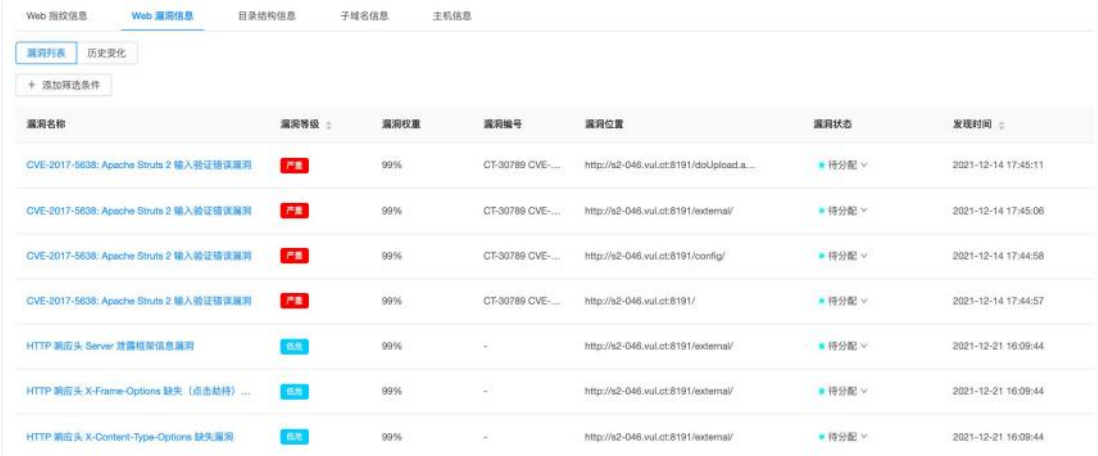
此选项卡内主要展示 Web 资产的指纹情况与 Web 情况，包括网站标题，开发语言，CDN 解析，WAF 识别，CMS 识别，原始 banner 及 Web 应用与应用版本，支持对应用及应用版本进行添加、编辑与删除（如上图所示）：

- 点击查看原始 banner 可查看原始 banner；
- 点击“添加 Web 应用”可以手动添加 web 应用，点击“编辑”可以编辑 web 应用名称与版本号，点击“删除”可以删除 web 应用。

Web 漏洞信息：

此选项卡内主要展示当前 web 资产的漏洞信息，包括漏洞名称，漏洞等级，漏洞权重，漏洞位置，发现时间：

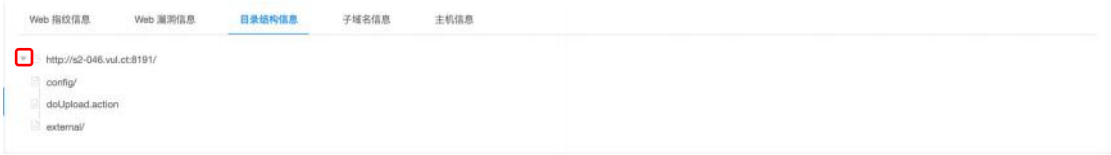
- 点击“风险等级”、“发现时间”右侧的三角图标，可以将列表按风险等级、发 现时间升序或者降序排列
- 点击漏洞名称，可以跳转至漏洞详情页面



目录结构信息：

此选项卡以结构树形式展示了 web 站点的结构：

- 点击目录左侧的图标可以展开或收起。



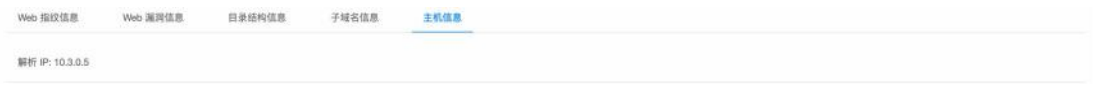
子域名信息：

此选项卡以结构树的形式展示了该 Web 资产下的子域名：

- 点击目录左侧图标可以展开或收起

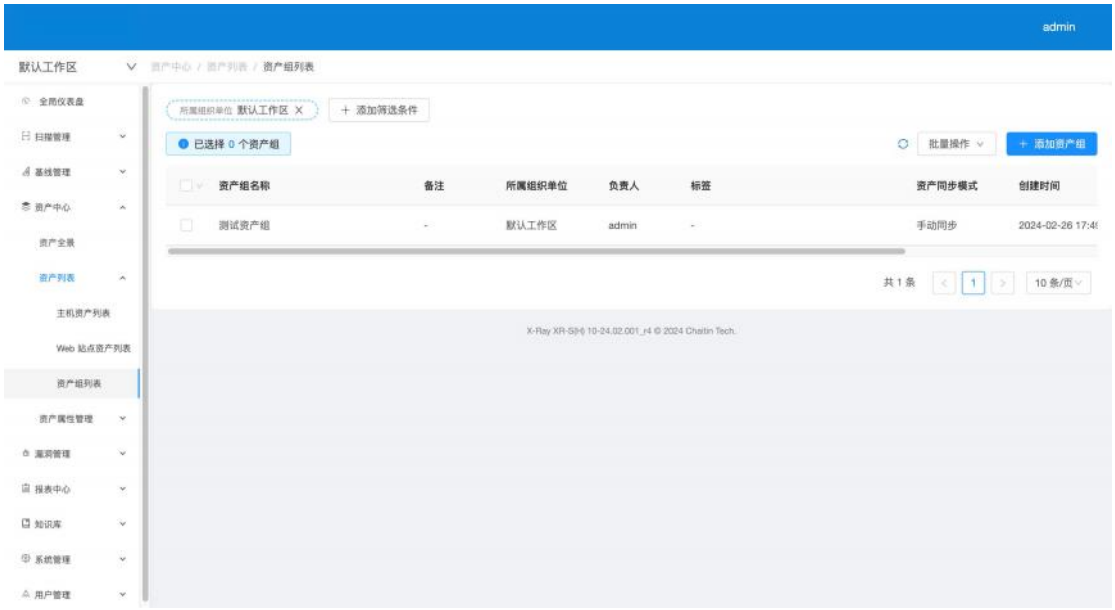
主机信息

此选项卡展示了与该 web 资产相关的主机 ip：



3.4.4 资产组列表

在左侧导航栏中，选择“资产中心–资产列表–Web 站点资产列表”，进入资产组界面。



3.4.4.1 资产组列表

内容展示：

主要展示所有的资产组信息，内容包括资产组名称、备注、所属组织单位：

添加筛选条件：

同 3.4.2.1 主机资产列表。

生成报表：

同 3.4.2.1 主机资产列表。

删除选中的资产组：

同 3.4.2.1 主机资产列表。

快速扫描资产组

同 3.4.2.1 主机资产列表

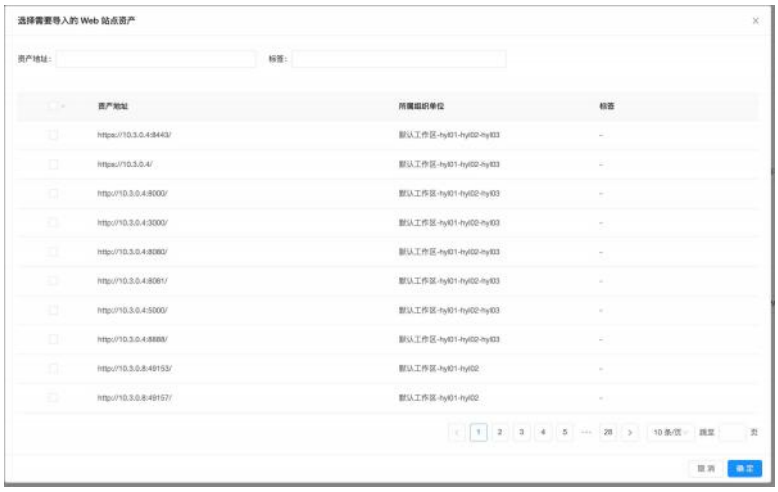
3.4.4.2 添加资产组

在资产组列表处，点击“ + 添加资产组”，即可打开添加资产组界面（如下图所示）：

具体操作如下：

- 输入资产组名称，不能为空；
- 选择性输入备注内容；
- 选择所属组织单位
- 选择负责人
- 联系邮箱
  - 一个资产组可绑定多个联系邮箱，当开启“任务发送报表通知”按钮时，针对该资产组下发的任务所生成的扫描报表（只针对开启“自动生成扫描报表”的任务）会发送至该资产组绑定的联系邮箱。
- 标签
- 选择资产同步模式
  - 手动同步：
    - 点击 “从资产列表导入”，弹出弹窗，选择要添加的主机资产（如下图所示）：

◆ 点击“选择目标 Web 站点”，弹出弹窗，选择要添加的 Web 站点资产：



◆ 点击“完成”成功添加新资产组。

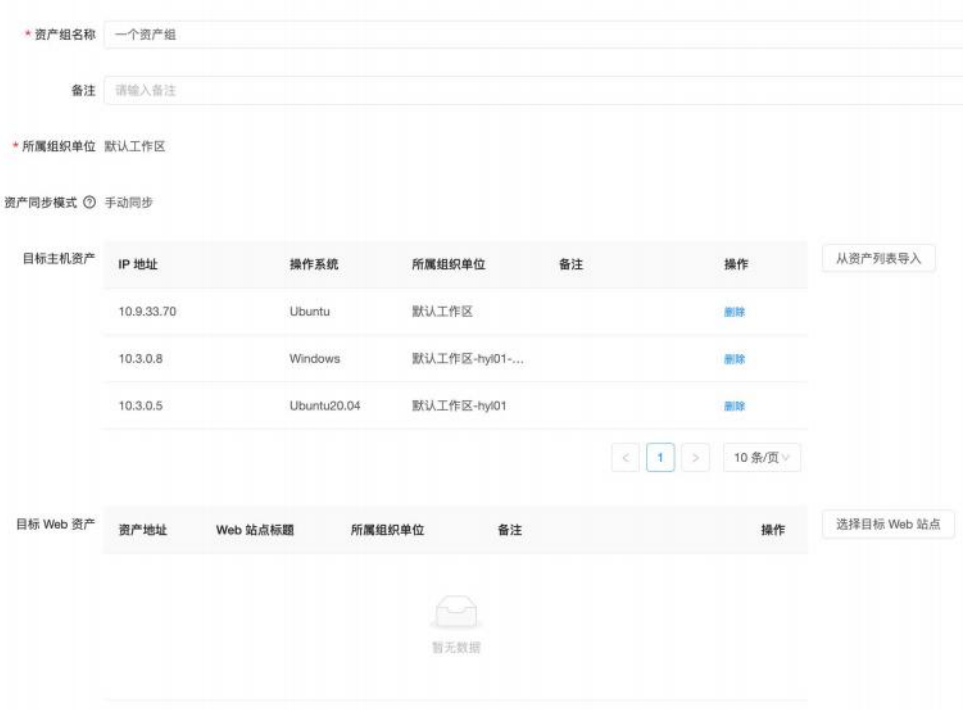
■ 自动同步：

◆ 当前可以以 IP 段为维度，配置自动同步的字段

- 点击“完成”成功添加新资产组。

3.4.4.3 手动类型资产组列表编辑

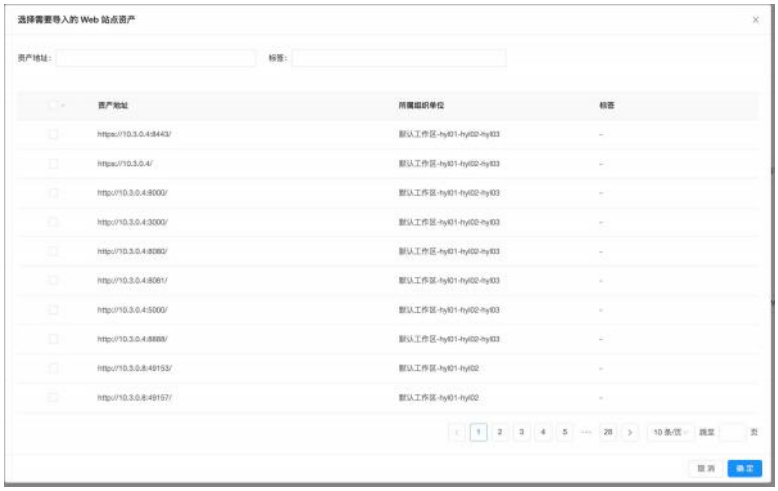
在资产组列表处，点击手动同步类型资产组的“编辑”，即可打开编辑资产组界面（如下入所示）：



具体操作如下：

- 可修改资产组名称，不能为空；
- 可修改备注内容；
- 所属组织单位和资产同步模式不可更改；
- 点击“从资产列表导入”，弹出弹窗，选择要添加的主机资产：

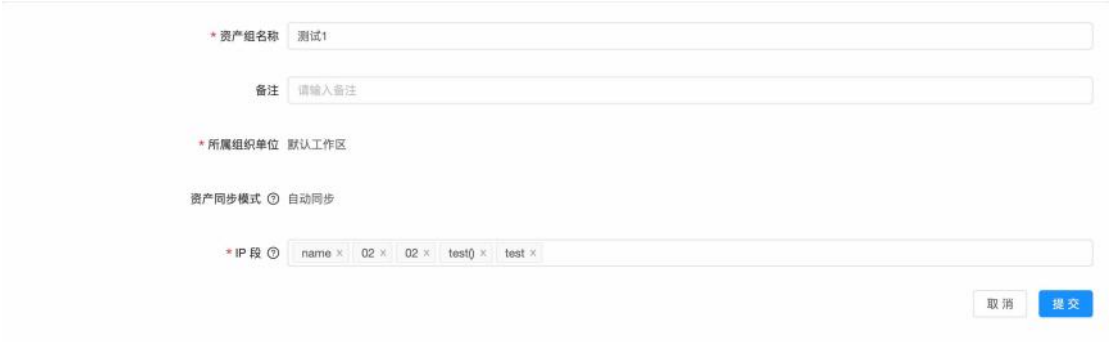
- 点击“选择目标 Web 站点”，弹出弹窗，选择要添加的 Web 站点资产：



- 点击“删除”，可以删除在资产组列表里的目标主机资产和目标 Web 资产；
- 点击“提交”成功修改资产组。

3.4.4.4 自动类型资产组列表编辑

在资产组列表处，点击自动同步类型资产组的“编辑”，即可打开编辑资产组界面（如下入所示）：



具体操作如下：

- 可修改资产组名称，不能为空；
- 可修改备注内容；
- 所属组织单位和资产同步模式不可更改；
- IP 段可编辑，不能为空；
- 点击“提交”成功修改资产组。

3.4.5 资产属性管理–IP 段管理

在左侧导航栏中，选择“资产中心–资产属性管理–IP 段管理”，进入 IP 段管理界面：

此页面可以帮助企业的管理员对 IP 段进行管理，支持对 IP 段的增加，编辑，删除，查询。

3.4.5.1 内容展示

该页面展示 IP 段的名称、具体段内容、负责人、所属组织单位等信息。用户可以根据筛选条件筛选条目，添加、查看、编辑、删除条目

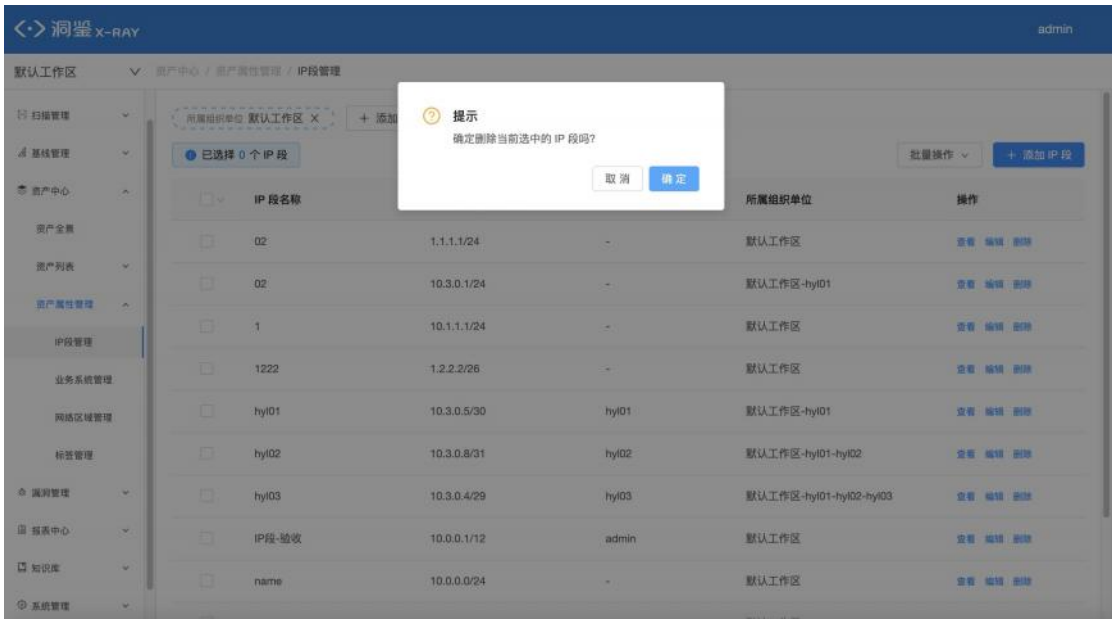
支持批量操作：

3.4.5.2 添加/编辑 IP 段

点击右侧“+添加 IP 段”添加新的 IP 段，输入 IP 段名称，以 10.0.0.1/24 的格式输入 IP 段/IP 段列表，所属组织单位以及负责人信息保存

3.4.5.3 删除 IP 段

点击“删除”条目删除 IP 段，并可以再二次提醒后删除



3.4.5.4 查看 IP 段

点击“查看”条目查看 IP 段信息，包含 IP 段名称、描述、所属组织单位、负责人，IP 段信息等

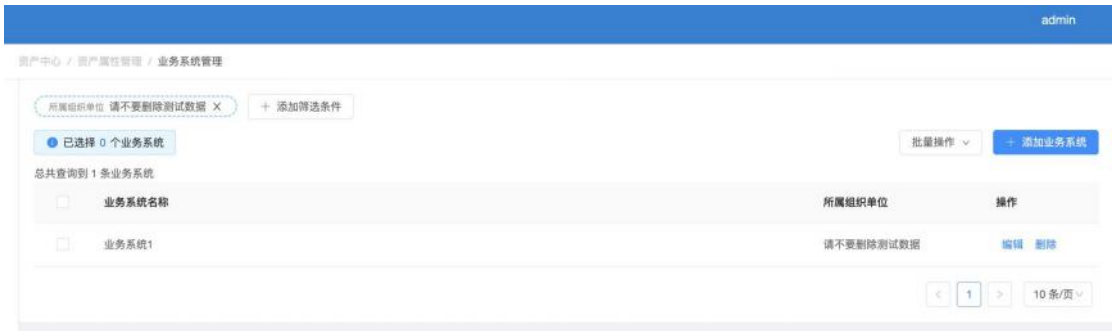
支持查看每个 IP 段的理论 IP 数、实际存活 IP 数

3.4.6 资产属性管理–业务系统管理

在左侧导航栏中，选择“资产中心–资产属性管理–业务系统管理”，进入业务系统管理界面。

3.4.6.1 内容展示

主要展示所有的业务系统名字（如下入所示）：



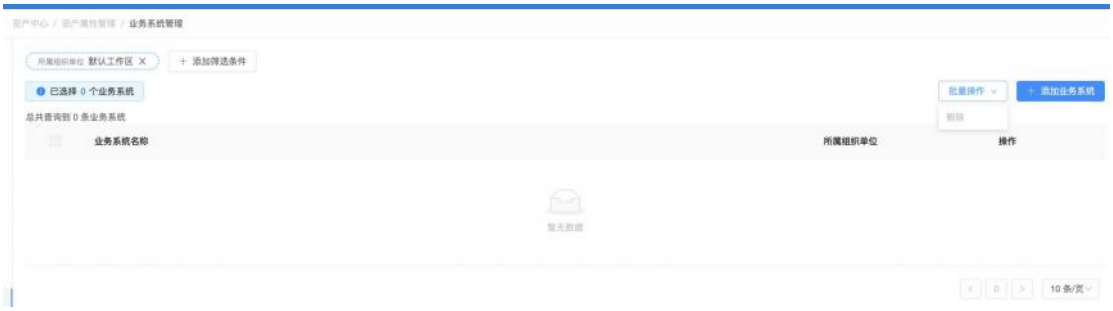
3.4.6.2 业务系统操作

添加业务系统

- 在列表页点击“添加业务系统”按钮，显示填写内容的弹窗
- 注意：业务系统不能被重复添加。

删除业务系统

- 批量/单次删除业务系统
  - 注意：如果业务系统正在被使用，那么该业务系统不允许被删除。



编辑业务系统

- 点击列表页的“编辑”按钮，显示更改内容的弹窗：

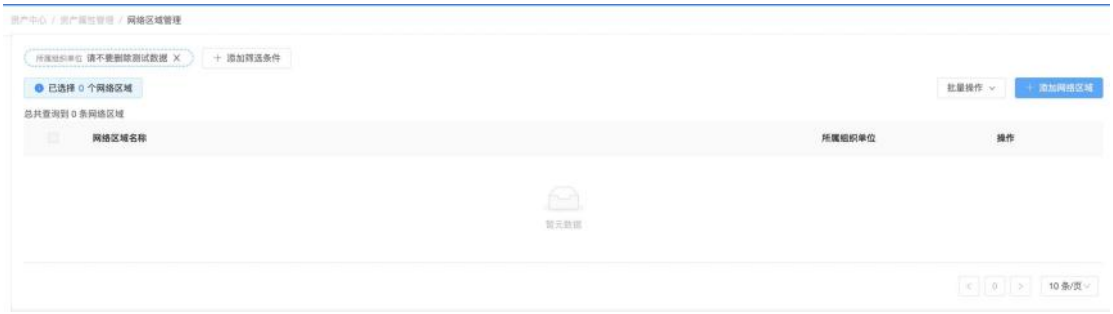

编辑业务系统
* 业务系统名称：
业务系统1
* 组织单位：
请不要删除测试数据
取 消
确 定

3.4.7 资产属性管理–网络区域管理

在左侧导航栏中，选择“资产中心–资产属性管理–网络区域管理”，进入网络区域管理界面。

3.4.7.1 内容展示

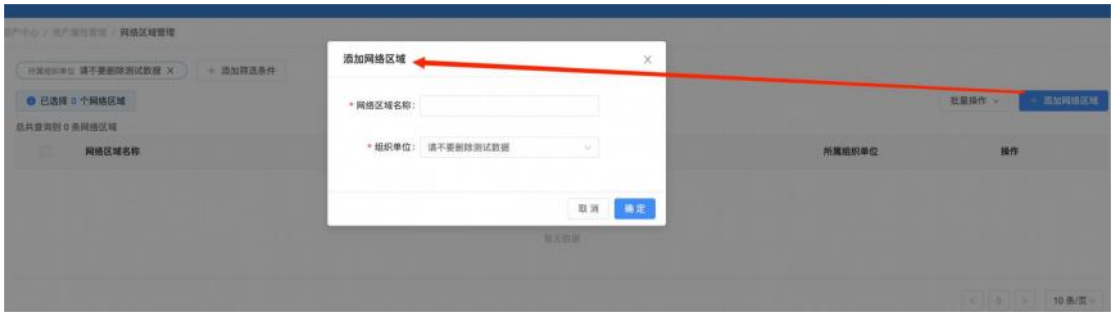
主要展示所有的网络区域名字：



3.4.7.2 网络区域操作

添加网络区域

- 在列表页点击“添加网络区域”按钮，显示填写内容的弹窗：



删除网络区域

- 批量/单次删除网络区域：

- 注意：如果网络区域正在被使用，那么该网络区域不允许被删除。

编辑网络区域

- 点击列表页的“编辑”按钮，显示更改内容的弹窗：

3.4.8 资产属性管理–标签管理

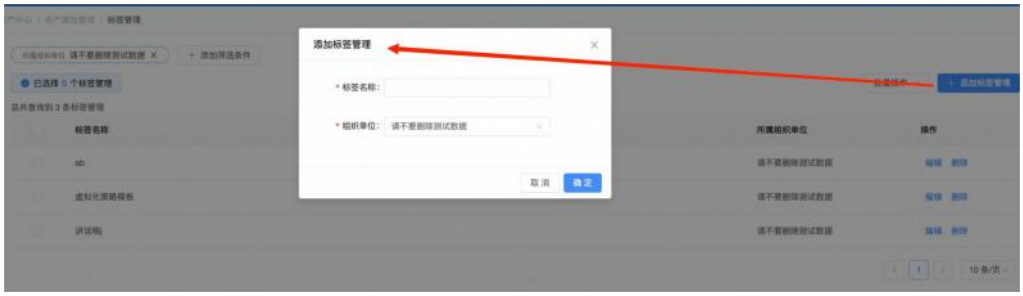
在左侧导航栏中，选择“资产中心–资产属性管理–标签管理”，进入网络区域管理界面：

3.4.8.1 内容展示

3.4.8.2 标签操作

添加标签

- 在列表页点击“添加标签”按钮，显示填写内容的弹窗：
- 注意：标签不能被重复添加。



删除标签

- 批量/单次删除标签
- 注意：如果标签正在被使用，那么该标签不允许被删除。

编辑标签

- 点击列表页的“编辑”按钮，显示更改内容的弹窗：

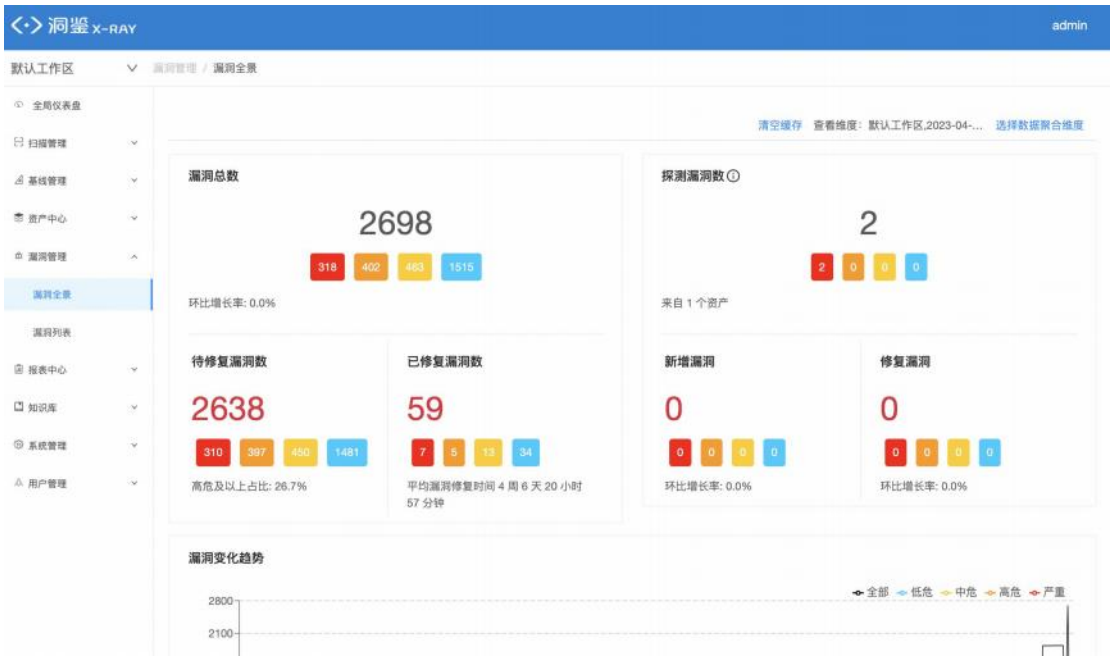
3.5 漏洞管理

此模块主要提供对漏洞管理的功能，包括对漏洞的查询筛选、删除、漏洞状态的跟踪更新等，方便企业对漏洞进行管理。

3.5.1 漏洞全景

在左侧导航栏中，选择“漏洞管理–漏洞全景”，进入基线检查配置界面。

此页面展示系统所有漏洞的统计信息，内容包括：



- 漏洞数量：
  - 漏洞数量：包含漏洞总数、待修复漏洞数量、已修复漏洞数量的数据，展示不同风险程度的漏洞数量（严重、高危、中危、低危）；
  - 显示漏洞总数的环比增长率、高危及以上占比、平均漏洞修复时间；
  - 探测漏洞数量及来自的资产个数、新增漏洞及环比增长率、修复漏洞及环比增长率。

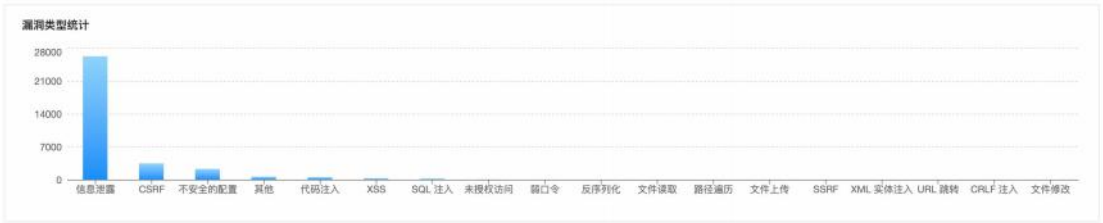
- 漏洞变化趋势：
  - 最近十一次扫描的漏洞数量变化趋势；
  - 鼠标悬浮在图形上，会显示当前状态下的漏洞数量，包含（全部、严重、高危、中危、低危）。

- 漏洞修复状态统计

- 饼状图展示不同类型的漏洞分布情况，鼠标悬浮在饼图上会显示所选部分标识的漏洞类型、漏洞数量占比
- 数据展示不同漏洞类型的漏洞数量
- 修复漏洞耗费时间分布，主要展示修复不同风险程度的漏洞时，所耗费时间的分布情况
- 未修复的漏洞数量，主要展示处于待修复状态下不同风险程度的漏洞数量

- 漏洞类型统计
  - 常见漏洞类型数量统计，鼠标悬浮显示漏洞、名称、数量、占比

- 弱口令统计
  - 显示弱口令名称、占比、排名、影响服务、弱口令数、影响资产数



- 业务系统漏洞分布情况
  - 显示排名、业务系统、漏洞总数、影响资产数

- 组织单位漏洞分布情况
  - 显示排名、组织单位、漏洞总数、影响资产数

3.5.2 漏洞列表

在左侧导航栏中，选择“漏洞管理–漏洞列表”，进入漏洞列表界面。

3.5.2.1 漏洞列表

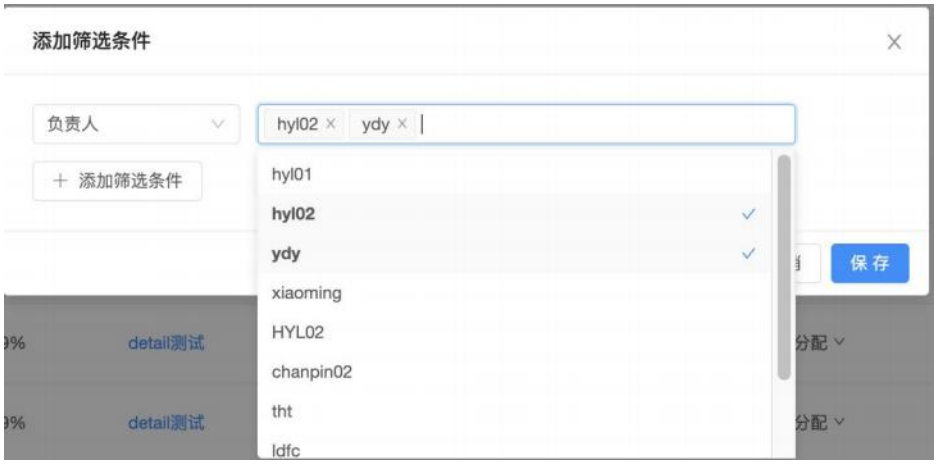
内容展示：

漏洞列表页面展示洞鉴扫描出的所有漏洞信息，展示内容包括漏洞等级、漏洞权重、漏洞名称、存在漏洞的位置、负责人、漏洞状态、建议处理优先级、创建时间、最近发现时间、漏洞的发现次数、操作栏，(如下图所示)：

- 漏洞权重越高，越确信漏洞的存在
- 建议处理优先级从 p0–p4，优先级逐渐降低

筛选漏洞：

- 在列表页可对漏洞进行筛选操作，可根据漏洞名称、漏洞风险等级、漏洞确信程度、相关资产、漏洞状态、发现时间、创建时间、相关扫描任务，自由添加一个或多个条件进行筛选
  - 当选择“负责人”筛选条件时，可根据所选择的负责人进行多组筛选。



删除漏洞：

在列表页可以对漏洞进行批量删除，一旦执行了删除操作，所有选中的漏洞均将被删除，具体操作说明如下：

- 选中要删除的漏洞，此时显示已选择的漏洞总数；
- 同时 "删除" 按钮变 为可点击状态；
- 点击 “删除” 按钮，提示框提示确定是否删除，点击 “确定”，则删除成功。

生成漏洞报表：

在漏洞列表页可以选择多个漏洞并生成漏洞报表，具体操作说明如下：

- 选中希望生成报表的漏洞，此时显示已选择的漏洞总数；
- 同时“生成报表”按钮变为可点击状态；
- 点击“生成报表”按钮；
- 在弹出的窗口中输入相关生成配置；
- 点击“确认”，即可以开始生成所选漏洞的报表。
- 注：可以前往报表管理页面查看报表生成的情况，或下载生成好的报表。

复测选中漏洞：

在列表页可以对漏洞进行批量复测：

- 点击漏洞复测按钮，系统会针对该漏洞进行重放请求，漏洞复测通常用时较短，复测中的漏洞不能停止，超出 1min 中后，将自动结束复测任务；
- 填写对应参数，需要注意，在不填写任何参数时，会直接按原有参数执行具体操作说明如下：
  - 选中希望复测的漏洞，此时显示已选择的漏洞总数，同时“复测漏洞”按钮变为可点击状态；
  - 点击“复测漏洞”按钮
  - 在弹出的漏洞复测对话框中配置相应信息；

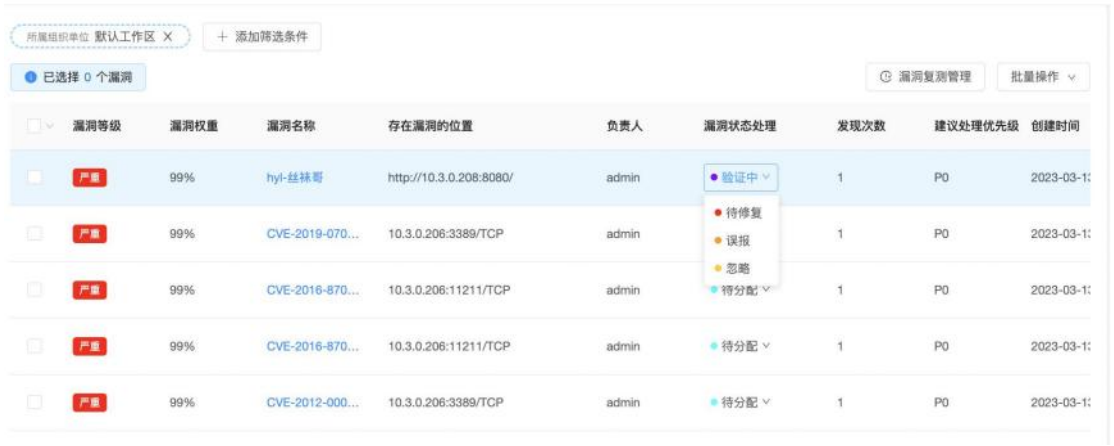
- 点击确定开始复测。

- 说明：漏洞验证仅支持验证漏洞权重大于 75%的漏洞，系统将会默认复测您选中的漏洞中漏洞权重大于 75%的漏洞。

更改漏洞状态：

- 漏洞状态包括待分配，验证中，修复中，误报，忽略，复核中，已修复，漏洞状态会根据洞鉴扫描或管理员修改而变化；
- 洞鉴扫描发现的新漏洞，会默认设置为“待分配”状态；

- 洞鉴扫描发现的已有漏洞，若已经在“待分配”、“验证中”、“修复中”、“复核中”、“误报”、“忽略”，则不会更新状态；
- 洞鉴扫描发现的已有漏洞，若已经设置为“已修复”状态，则重新设置为“待分配”状态；
- 管理员可以对漏洞状态进行跟踪，手动修改漏洞状态（若变为已修复，则不可手动更改）。
- 可以点击列表头批量调整漏洞状态来批量选中漏洞并调整漏洞的状态为任何目标状态



3.5.2.2 漏洞详情

点击漏洞列表中的漏洞，可以打开漏洞详情页面，了解漏洞更多的相关信息和技术细节：

基础信息：

漏洞详情右侧上方展示漏洞的基础信息。

- 漏洞名称：该漏洞名称
- 漏洞类型：该漏洞类型
- 漏洞等级：该漏洞等级，可手动修改
- 漏洞权重：权重越高，漏洞存在的可能性越大
- 漏洞编号：漏洞的 CVE、CNNVD 编号
- 所属资产：点击可跳转到该漏洞所在的资产详情页面（若 license 中不包含资产管理模块或者无权限查看该模块则无此功能）
- 影响资产类别
- 最近扫描任务：点击可跳转到扫出该漏洞最近的一次扫描任务详情页面
- 发现时间：表示此漏洞在目标上扫描出来的时间
- 漏洞状态处理：可在此更改漏洞状态：
  - 点击漏洞状态右侧的“铅笔”图标，漏洞状态变为可操作的下拉菜单；
  - 在下拉菜单中点击新的漏洞状态，即可修改漏洞状态；
  - 若不想改变漏洞状态，点击右侧的“取消”即可退出对漏洞状态的更改。
- 处理过程：显示漏洞状态的发现或状态更新过程

技术细节：

漏洞详情页面左侧展示漏洞的技术细节信息。技术细节提供关于漏洞的详细的技术支持，包含漏洞描述、漏洞危害等等。

- CVSS 风险评分：

- CVSS 是一个通用的漏洞风险评分系统，CVSS 评分可以表示该漏洞的风险情况，评分越高表示风险越高。

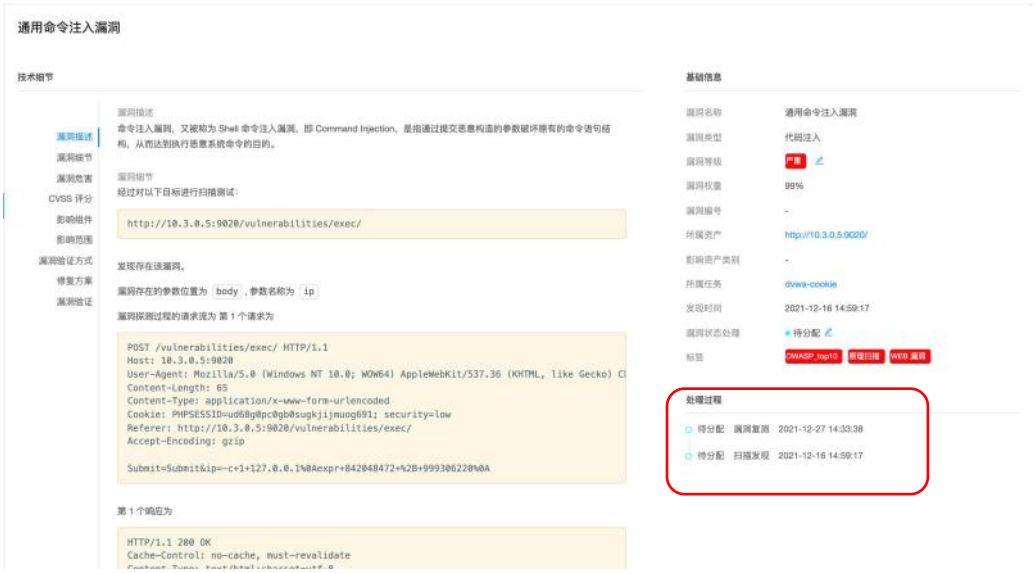
- CVE 类型介绍：
  - CVE 是一个通用的漏洞类型信息库。CVE 信息可以对漏洞形成的原因做一个较好的补充说明；
  - 洞鉴系统仅节选一部分 CVE 类型介绍。如果用户希望获得更多信息，可以访问 CVE 官网（https://cve.mitre.org/），并搜索洞鉴系统提供的 CVE 编号（形如“CVE-119”）获取更多漏洞类型说明。

漏洞复测：

针对 POC 检测的漏洞支持漏洞复测：

- 下发漏洞验证任务：
  - 点击“漏洞复测”按钮，系统会针对该漏洞进行重放请求，漏洞复测通常用时较短，复测中的漏洞不能停止，超出 1min 中后，将自动结束复测任务；
  - 填写对应参数，如图，需要注意，在不填写任何参数时，会直接按原有参数执行。

- 验证结果显示：
  - 验证后的结果会在右侧，出现漏洞复测操作，并显示漏洞状态：



- 漏洞复测管理
  - 点击“漏洞复测管理”按钮可对复测的漏洞管理任务进行查看，支持一键清空全部复测记录。
  - 将漏洞的最近一次复测结果同步显示到漏洞列表中，”已下线“表示对应的服务或端口已被关闭则复测。

3.6 报表中心

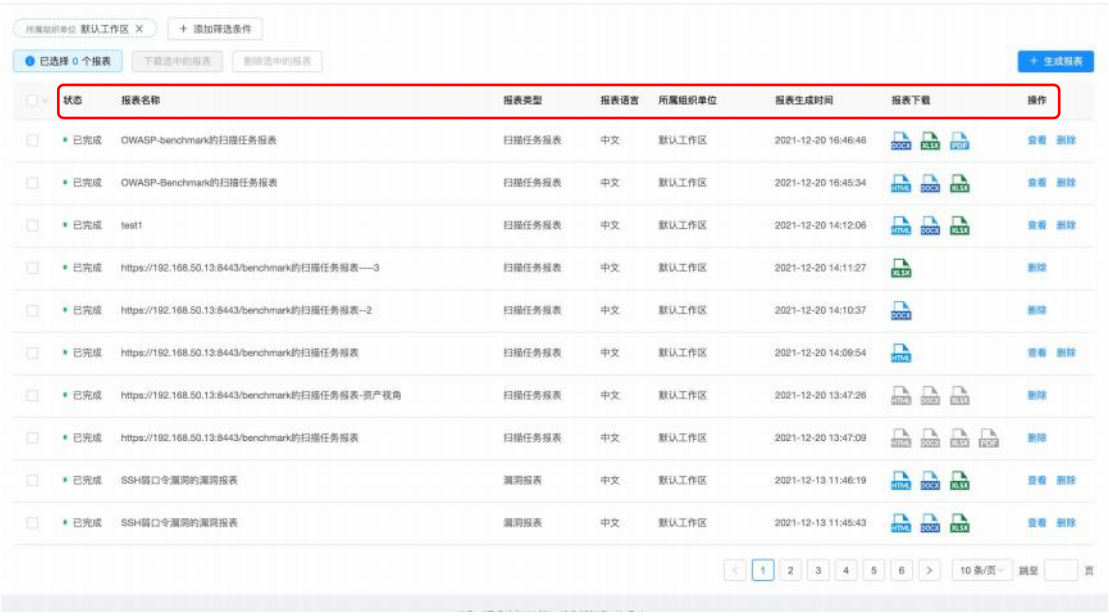
报表中心主要用于对洞鉴生成的报表和报表模版进行管理，包括报表管理和报表模版。

3.6.1 报表管理

在左侧导航栏中，选择“报表中心–报表管理”，进入报表管理界面。

3.6.1.1 内容展示

报告列表页展示生成的所有报告，内容包括生成状态、报告名称、报表类型、报表语言、所属工作区、报告生成时间、可下载的报表文件：



3.6.1.2 筛选操作

- 在报告列表页可对报告进行筛选操作，可根据生成状态、报告名称、报告类型和报告生成时间，自由添加一个或多个条件进行筛选

3.6.1.3 下载操作

在“报表下载”列，会展示生成报表时勾选的文件格式（共有 word、html、Excel、PDF、JSON），若生成的为英文版则显示左上角带有 EN 标识的 icon：

- 图标为较透明的彩色：表明对应格式的文件正在生成；
- 图标为彩色：表明对应格式的文件已生成，点击可下载；
- 图标为灰色：表明对应格式的文件已生成。

在报告列表页可以批量下载报告，具体操作为：

- 选中要下载的报告，此时显示已选择的报告总数，同时“下载选中的报告”按钮变为可点击状态；
- 点击“下载选中的报告”按钮，选择要下载的报告格式，点击确定后以 zip 的形式将所有选择的报告下载到本地，文件包含选择的要下载的文件格式。

3.6.1.4 查看操作

报表生成 html 格式成功后，可点击“查看”按钮在线查看生成的报表：

3.6.1.5 删除操作

在报告列表页可以对报告进行批量删除，一旦执行了删除操作，所有选中的报告信息均将被删除且不能恢复，具体操作为:

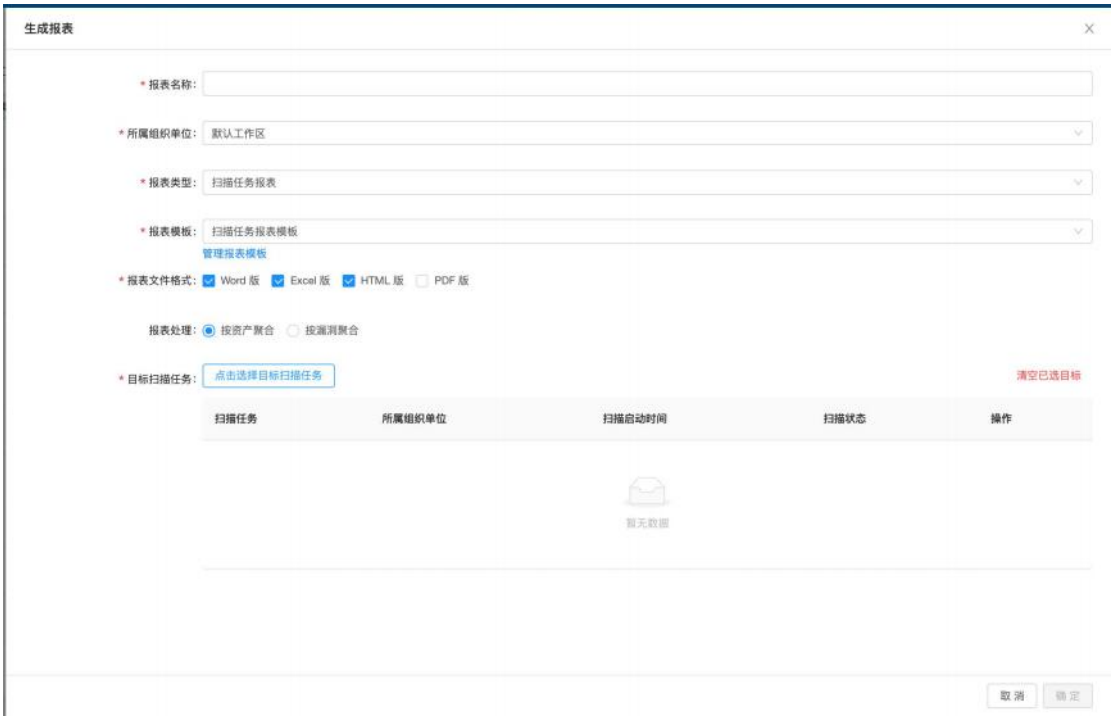
3.6.2 生成报表

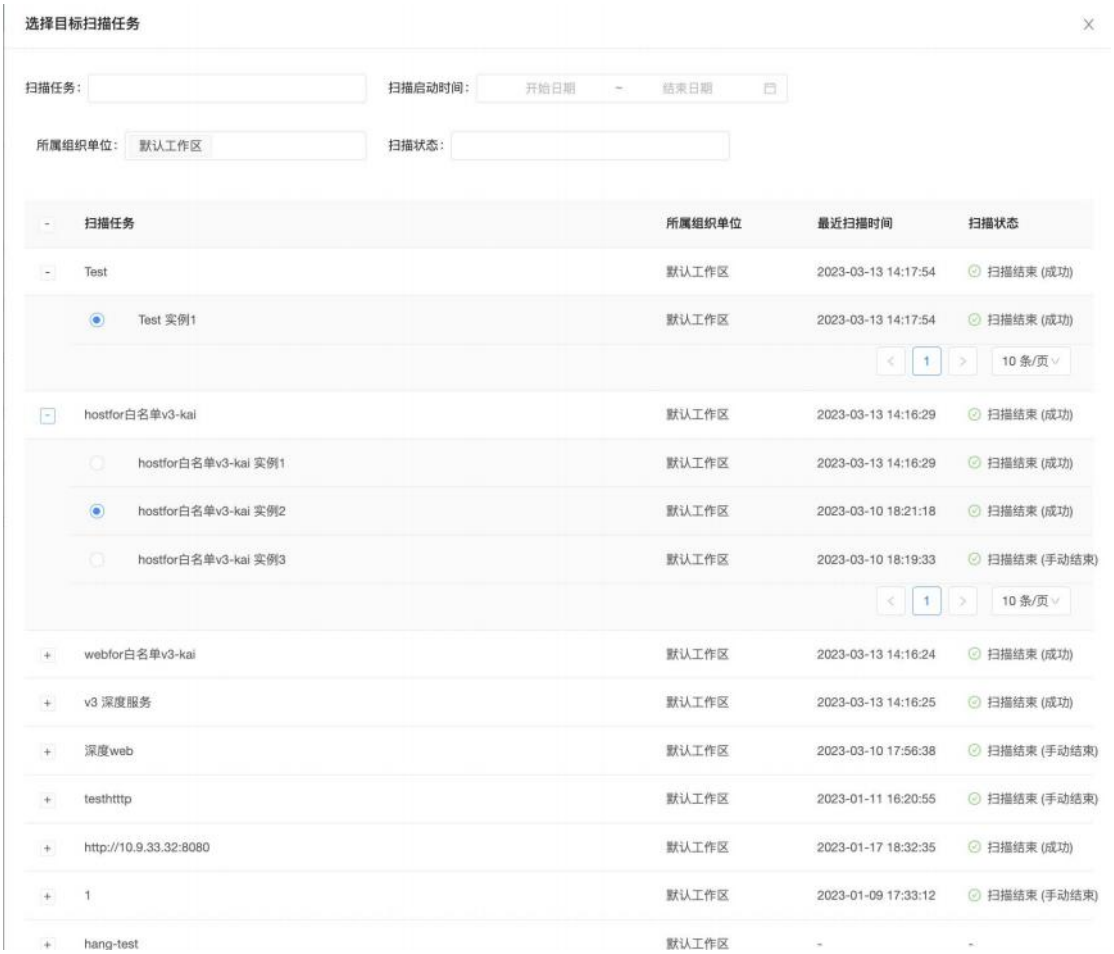
在报告管理可以生成报告，具体操作为:

- 从报告列表页点击“ + 生成报告”按钮，打开弹窗；
- 填写报告名称；
- 选择所属组织单位；
- 选择报告类型，包括扫描任务报表、基线检查报表、资产报表、漏洞报表四种类型
- 根据报告类型的不同，需要设置的内容也不同，每种报告模板对应的设置说明如下：

扫描任务报表：

- 报表模版：可选项为“扫描任务报表”下的模版；系统模板默认只生成漏洞权重大于 50%的漏洞信息，如需更改请使用自定义模版。
  - 点击“管理相关模版”可打开模版管理页面，对相关模版进行管理；
- 报表文件格式：勾选要生成的文件格式；
- 报表处理：
  - 按资产聚合：扫描任务的漏洞将以所属资产的维度呈现；
  - 按漏洞聚合：扫描任务的漏洞将以漏洞种类的维度呈现；
- 拆分子报表：报表目标数量过多时建议选择拆分模式拆分为多个报表，避免单个报表打不开等异常问题
- 报表目标：点击按钮可选择目标扫描任务，支持选择多个扫描任务。
- 全部设置好后，点击“确定”，则成功生成报告，系统自动跳转至报告管理页；
  - “合并生成”：多个任务结果输出 1 份报表
  - “批量生成”：多个任务结果输出多份报表
- 可在报告列表页对刚生成的报告进行查看、下载和删除。


生成报表
* 报表名称:
* 所属组织单位: 默认工作区
* 报表类型: 扫描任务报表
* 报表模板: 扫描任务报表模板
管理报表模板
* 报表文件格式: Word 版 Excel 版 HTML 版 PDF 版
报表处理: 按资产聚合 按漏洞聚合
* 目标扫描任务: 点击选择目标扫描任务
清空已选目标
扫描任务
所属组织单位
扫描启动时间
扫描状态
操作
暂无数据
取 消
确 定


选择目标扫描任务
扫描任务:
扫描启动时间: 开始日期 ~ 结束日期
所属组织单位: 默认工作区
扫描状态:
扫描任务
所属组织单位
最近扫描时间
扫描状态
Test 默认工作区 2023-03-13 14:17:54 扫描结束 (成功)
Test 实例1 默认工作区 2023-03-13 14:17:54 扫描结束 (成功)
10 条/页
hostfor白名单v3-kai 默认工作区 2023-03-13 14:16:29 扫描结束 (成功)
hostfor白名单v3-kai 实例1 默认工作区 2023-03-13 14:16:29 扫描结束 (成功)
hostfor白名单v3-kai 实例2 默认工作区 2023-03-10 18:21:18 扫描结束 (成功)
hostfor白名单v3-kai 实例3 默认工作区 2023-03-10 18:19:33 扫描结束 (手动结束)
10 条/页
webfor白名单v3-kai 默认工作区 2023-03-13 14:16:24 扫描结束 (成功)
v3 深度服务 默认工作区 2023-03-13 14:16:25 扫描结束 (成功)
深度web 默认工作区 2023-03-10 17:56:38 扫描结束 (手动结束)
testhtttp 默认工作区 2023-01-11 16:20:55 扫描结束 (手动结束)
http://10.9.33.32:8080 默认工作区 2023-01-17 18:32:35 扫描结束 (成功)
1 默认工作区 2023-01-09 17:33:12 扫描结束 (手动结束)
hang-test 默认工作区 - -

资产报表：

- 报表模版：可选项为“资产报表”下的模版；系统模板默认只生成漏洞权重大于 50%的漏洞信息，如需更改请使用自定义模版。
  - 点击“管理相关模版”可打开模版管理页面，对相关模版进行管理；
- 报表文件格式：勾选要生成的文件格式；
- 报表目标：点击按钮可选择目标资产：资产组、Web 站点资产和主机资产；
- 全部设置好后，点击 "确定"，则成功生成报告，系统自动跳转至报告管理页；
- 可在报告列表页对刚生成的报告进行查看、下载和删除。

漏洞报表：

- 报表模版：可选项为“漏洞报表”下的模版；系统模板默认只生成漏洞权重大于 50%的漏洞信息，如需更改请使用自定义模版。

- 点击“管理相关模版”可打开模版管理页面，对相关模版进行管理；

- 报表文件格式：勾选要生成的文件格式；
- 报表目标：点击按钮可选择目标漏洞；
- 全部设置好后，点击 "确定"，则成功生成报告，系统自动跳转至报告管理页；
- 可在报告列表页对刚生成的报告进行查看、下载和删除。

基线检查报表：

- 报表模版：可选项为“基线检查报表”下的模版；

- 点击“管理相关模版”可打开模版管理页面，对相关模版进行管理；

- 报表文件格式：勾选要生成的文件格式；
- 报表处理：

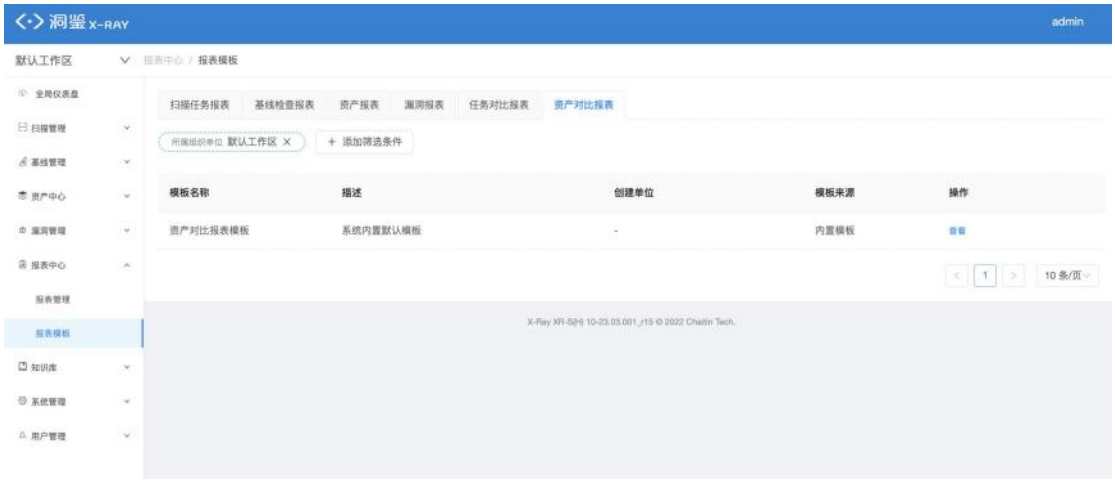
- 按资产聚合：基线检查的结果将检查资产的维度呈现；
- 按检查策略聚合：基线检查的结果将以检查策略的维度呈现；
- 提示：若检查的主机数量较多，可能会导致相同检查项被重复打印多次，导致生成报告内容过多；建议选择“按检查策略聚合”。

- 报表目标：点击按钮可选择目标基线检查；
- 全部设置好后，点击 "确定"，则成功生成报告，系统自动跳转至报告管理页；

- 可在报告列表页对刚生成的报告进行查看、下载和删除。

3.6.3 报表模版

在左侧导航栏中，选择“报表中心–报表模版”，进入报表管理界面。



3.6.3.1 内容展示

扫描任务报表、基线检查报表、资产报表、漏洞报表、任务对比报表、资产对比报表。这 6 种类型的报表对应模版差异较大，可通过顶部 tab 页面切换。

在报表模版中，展示已有模版的模版名称、描述、模版来源：

- 模版来源：系统出产自带的为 “内置模版”，其余均为“自定义模版”；
- 内置模版仅可查看，不可编辑和删除；
- “自定义模版”可以点击操作列的按钮，查看、编辑和删除。

3.6.3.2 筛选操作

- 在报告模版页可对报告进行筛选操作，可所属组织单位、模版名称、模版来源维度筛选，自由添加一个或多个条件进行筛选。

3.6.3.3 添加报表模版

- 选择报表类型：目前只支持扫描任务报表、基线检查报表、资产报表和漏洞报表。不同类型的报表，可勾选的内容、可筛选的标准有所不同；
- 模版名称：同类型的报表模版名称不可有重复；
- 报表语言：支持中文和英文版两种报表语言，默认为中文。选择该模版的报表生成后将会是对应的语言；
- 报表封面标题：最终显示到报表封面的标题，如果不填写则默认显示报表名称；
- 描述；

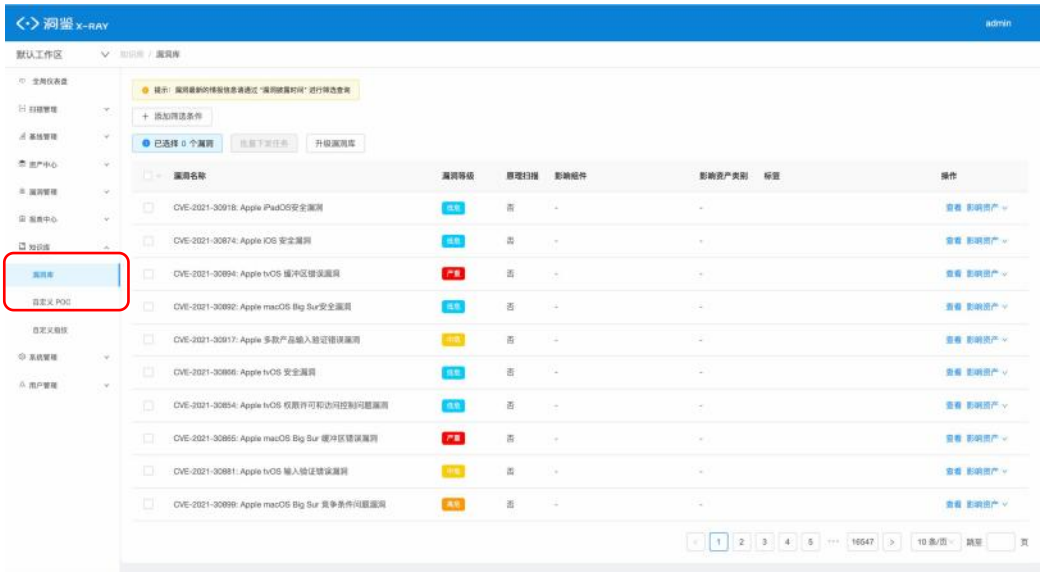
- 模版创建单位：选择工作区；
- 模版内容：勾选组合想要在报表中展示的内容模块；
- 数据筛选：对生成报告的初始数据进行筛选过滤，不同的报表模版类型有不同的数据筛选项。包含资产/漏洞风险等级、漏洞权重、资产类型、资产存活性、漏洞标签等筛选项

3.7 知识库

3.7.1 漏洞库

在左侧导航栏中，选择“知识库–漏洞库”，进入漏洞库界面。

显示当前漏洞库中漏洞相关的信息：



3.7.1.1 列表内容

- 漏洞名称
- 漏洞等级：包括严重、高危、中危、低危
- 原理扫描：包含是/否
- 影响组件
- 影响资产类别
- 标签：为漏洞添加的标签

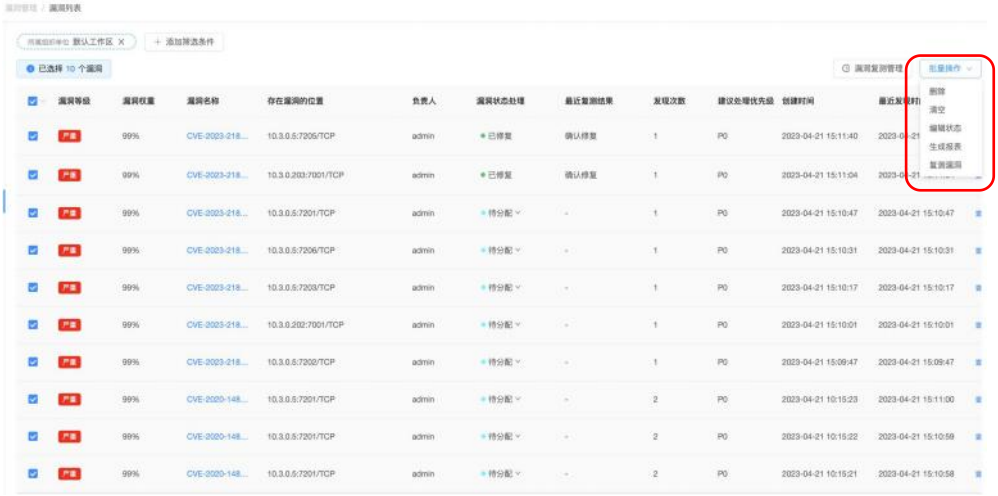
3.7.1.2 添加筛选条件

可以通过添加筛选条件，包含漏洞名称、等级、编号、影响组件、服务类型、操作系统、标签、厂商、是否需要反连、漏洞类型、影响资产类别、是否原理扫描、漏洞披露时间、自定义标签：

- 添加筛选条件可以选择后保存，或者删除；
- 可以在列表上点击删除删除已经设定的筛选条件。

3.7.1.3 批量下发任务

- 点击全选或者单个选中漏洞项目，点击批量下发任务，进行任务的扫描：



- 当以选中漏洞批量创建扫描任务时，创建的扫描任务名称会自动变为：“任务名称+所在组织单位名称”，同主机资产下发扫描任务。

3.7.1.4 升级漏洞库

详情请见 4.3.2 漏洞库升级。

3.7.1.5 自定义标签

支持给漏洞库自定义标签，自定义标签支持在扫描任务/扫描策略中筛选对应的漏洞插件。

3.7.1.6 查看详情

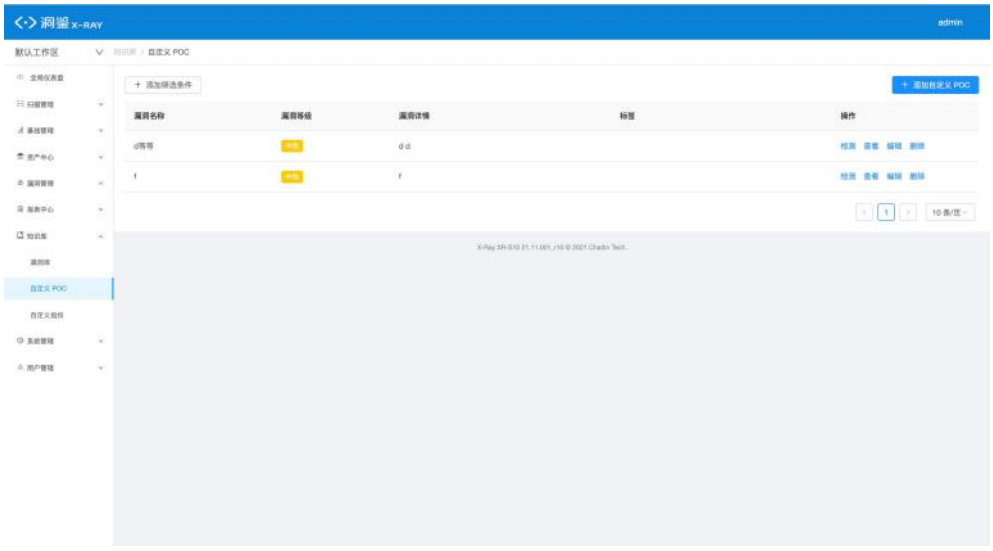
- 点击查看，进入漏洞情况页面：
- 包含漏洞名称、风险等级、标签、影响资产类别、漏洞类型、是否原理扫描、漏洞概述、漏洞编号、漏洞披露时间、漏洞危害、CVSS 评分、影响组件、影响范围、修复方案、影响资产数量以及漏洞近一周、一月、一年的漏洞趋势。

3.7.1.7 其他操作

点击影响资产，选择主机资产或者 Web 资产跳转到对应影响的资产详情页面。

3.7.2 自定义 POC

在左侧导航栏中，选择“知识库–自定义 POC”，进入自定义 POC 界面。



权限说明:

- 该功能需要具备“扫描管理”功能模块的 license，详细请联系长亭工作人员获取；

超级管理员支持编辑和可见权限，系统管理员仅有可见和使用权限。

3.7.2.1 自定义 POC 列表—内容展示

自定义 POC 列表展示系统中所有自定义 POC 列表，列表包含漏洞名称、漏洞等级、 漏洞类型、漏洞编号、标签。

3.7.2.2 筛选操作

- 在列表页可对任务进行筛选操作，可根据扫描漏洞名称、风险等级、漏洞编号、标签。

3.7.2.3 删除操作

在列表页可以对单条 POC 进行删除操作，一旦执行删除操作，对应 POC 均将被删除，会影响启用了该 POC 的任务配置，具体步骤为:

- 找到列表中要删除的扫描任务，点击尾部操作栏中的 “删除”按钮。

3.7.2.4 查看 POC 操作

在列表页可以对单条 POC 进行查看操作，具体步骤为:

- 找到列表中要查看的扫描任务，点击尾部操作栏中的“查看”按钮。

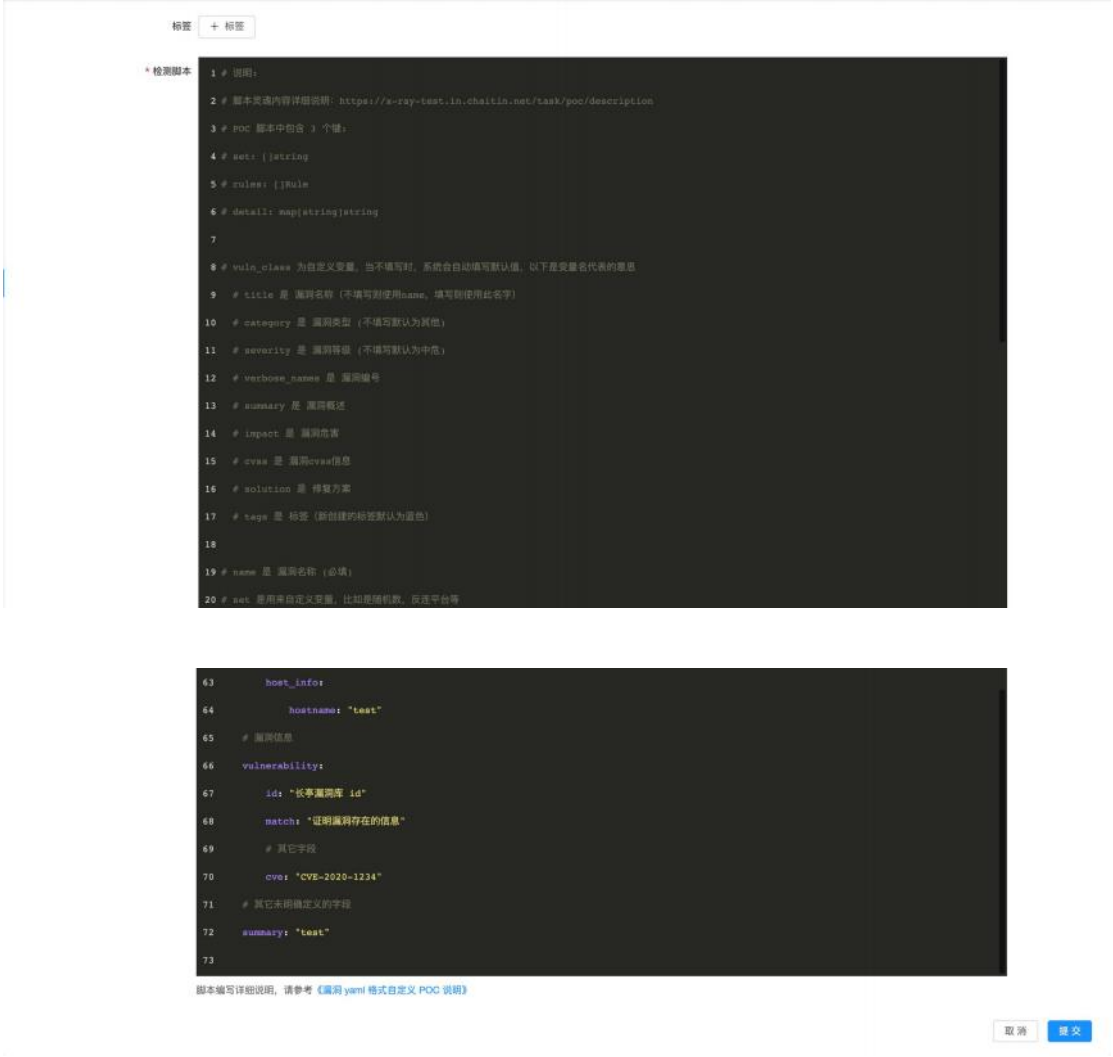
3.7.2.5 添加自定义 POC

添加 POC 可以手动添加或者上传文件。

手动添加：

- 点击“添加自定义 POC”按钮，选择手动添加，填写对应的漏洞模板，然后在下面的代码编辑器中，粘贴对应的检测脚本或按照脚本说明编写相应的检测脚本：
  - 漏洞模板--包含漏洞相关的静态描述字段，包括漏洞名称、漏洞类型、风险 等级、漏洞编号、漏洞概述、漏洞危害、漏洞 CVSS 信息、漏洞修复方式以及标签；
  - 检测脚本--包含漏洞的检测脚本 yaml 格式，用户可以根据提示的编写规则粘贴或编写对应的脚本。在代码编辑器下，可以点击跳转详细的《洞鉴 yaml 格式自定义 POC 说明》。


* 漏洞名称
请输入漏洞名称
* 漏洞类型
请选择漏洞类型
* 漏洞等级
请选择漏洞等级
漏洞编号
请填写对应的漏洞编号，例如 CVE-2019-2315，CNVD-2018-1015，以逗号分隔
* 漏洞概述
请输入漏洞概述
* 漏洞危害
请输入漏洞危害
漏洞 CVSS 信息
请输入漏洞 CVSS 信息
修复方案
请输入修复方案


标签
+ 标签
* 检测脚本
# 说明：
# 脚本灵魂内容详细说明：https://x-ray-test.in.chaitin.net/task/poc/description
# POC 脚本中包含 3 个键：
# set: []string
# rules: []Rule
# detail: map[string]string
# vuln_class 为自定义变量，当不填写时，系统会自动填写默认值，以下是变量名代表的意思
# title 是 漏洞名称（不填写则使用name，填写则使用此名字）
# category 是 漏洞类型（不填写默认为其他）
# severity 是 漏洞等级（不填写默认为中危）
# verbose_name 是 漏洞编号
# summary 是 漏洞概述
# impact 是 漏洞危害
# cvss 是 漏洞cvss信息
# solution 是 修复方案
# tags 是 标签（新创建的标签默认为蓝色）
# name 是 漏洞名称（必填）
# set 是用来自定义变量，比如是随机数，反连平台等
host_info:
hostname: "test"
漏洞信息
vulnerability:
id: "长亭漏洞库 id"
match: "证明漏洞存在的信息"
其它字段
cve: "CVE-2020-1234"
其它未明确定义的字段
summary: "test"
脚本编写详细说明，请参考《漏洞 yaml 格式自定义 POC 说明》
取消
提交

上传文件

- 点击自定义 POC，选择从文件夹上传；
- 导入根据文件模版写成的.yml 格式的文件，点击确定添加。

3.7.2.7 编辑自定义 POC

在列表页可以对单条 POC 进行编辑操作，具体步骤为:

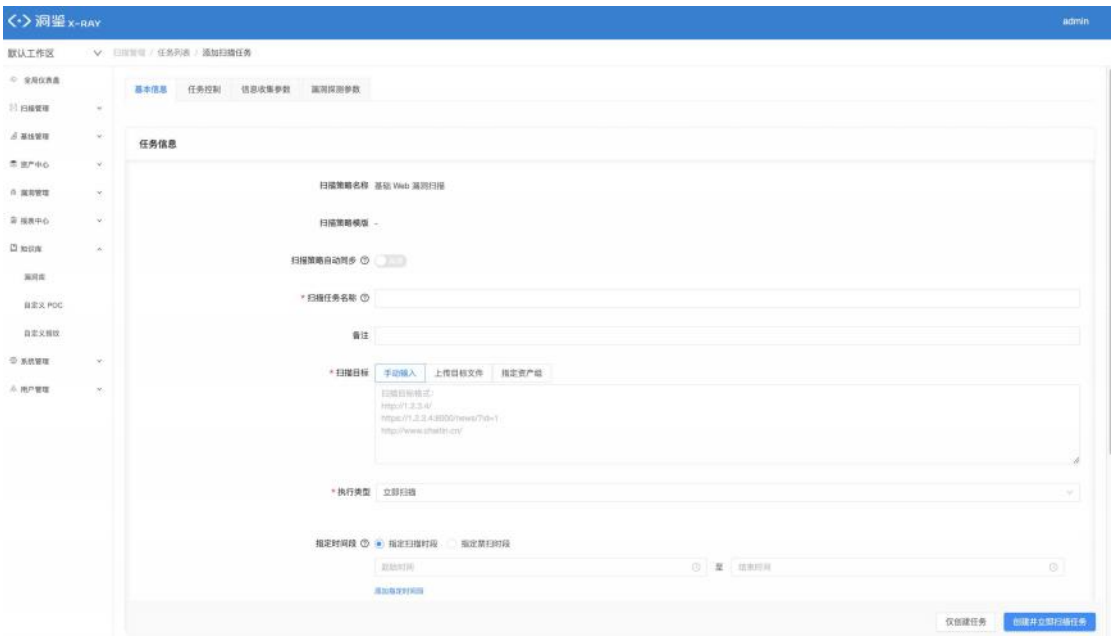
- 找到列表中要查看的扫描任务，点击尾部操作栏中的编辑按钮，进入漏洞编辑页面；
- 填写对应的漏洞模板，然后在下面的代码编辑器中，粘贴对应的检测脚本或按照脚本说明编写相应的检测脚本：
  - 漏洞模板--包含漏洞相关的静态描述字段，包括漏洞名称、漏洞类型、风险等级、漏洞编号、漏洞概述、漏洞危害、漏洞 CVSS 信息、漏洞修复方式以及标签；
  - 检测脚本一包含漏洞的检测脚本 yaml 格式，用户可以根据提示的编写规则粘贴或编写对应的脚本。在代码编辑器下，可以点击跳转详细的《洞鉴 yaml 格式自定义 POC 说明》。

- 说明：编辑后的漏洞模板在进行新的任务检测后，新的字段会批量覆盖到之前与该漏洞模板关联的漏洞。

3.7.2.8 自定义 POC 快速检测

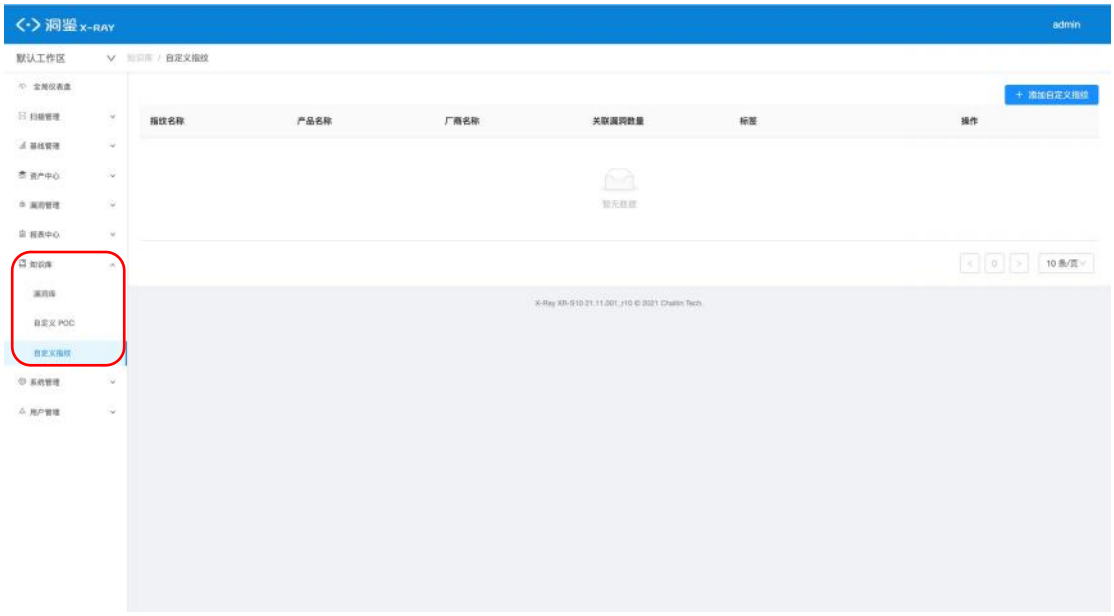
在列表页可以对单条 POC 进行检测操作，具体步骤为:

- 找到列表中要查看的扫描任务，点击尾部操作栏中的检测按钮，进入 web 漏洞检测任务下发流程；
- 默认插件选择仅有自定义 POC 对应的插件。



3.7.3 自定义指纹

在左侧导航栏中，选择“知识库–自定义指纹”，进入自定义指纹界面。

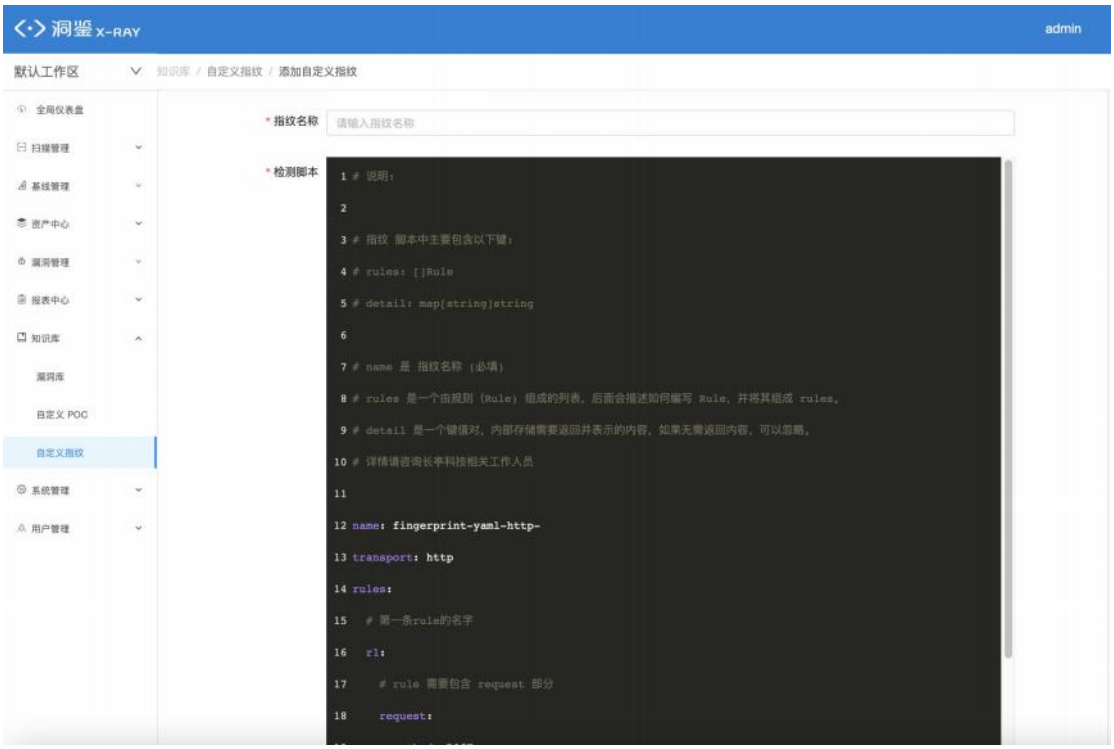


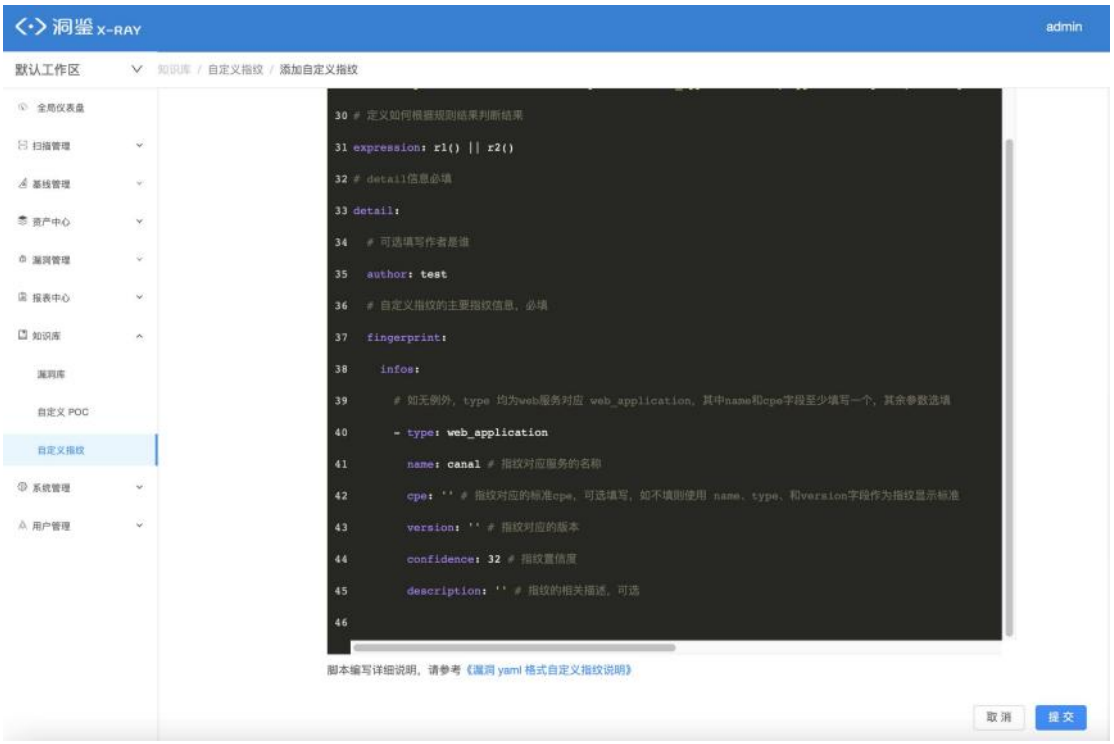
3.7.3.1 自定义指纹列表

- 显示指纹信息，包含指纹名称、产品名称、厂商名称、标签（如下图）：
- 可以查看、删除、编辑自定义指纹。
- 可以通过指纹名称、厂商名称、产品名称筛选自定义指纹

3.7.3.2 添加自定义指纹

- 点击添加自定义指纹，进入模版添加指纹名称、产品名称、检测 yaml 脚本
- 填写指纹名称、脚本中可输入指纹的 cpe，版本，描述等信息，点击提交保存


洞鉴 X-RAY
admin
默认工作区
知识库 / 自定义指纹 / 添加自定义指纹
全局仪表盘
扫描管理
基线管理
资产中心
漏洞管理
报表中心
知识库
漏洞库
自定义 POC
自定义指纹
系统管理
用户管理
* 指纹名称
请输入指纹名称
* 检测脚本
1 # 说明：
2
3 # 指纹 脚本中主要包含以下键：
4 # rules: []Rule
5 # detail: map[string]string
6
7 # name 是 指纹名称 (必填)
8 # rules 是一个由规则 (Rule) 组成的列表，后面会描述如何编写 Rule，并将其组成 rules。
9 # detail 是一个键值对，内部存储需要返回并表示的内容，如果无需返回内容，可以忽略。
10 # 详情请咨询长亭科技相关工作人员
11
12 name: fingerprint-yaml-http-
13 transport: http
14 rules:
15 # 第一条rule的名字
16 r1:
17 # rule 需要包含 request 部分
18 request:

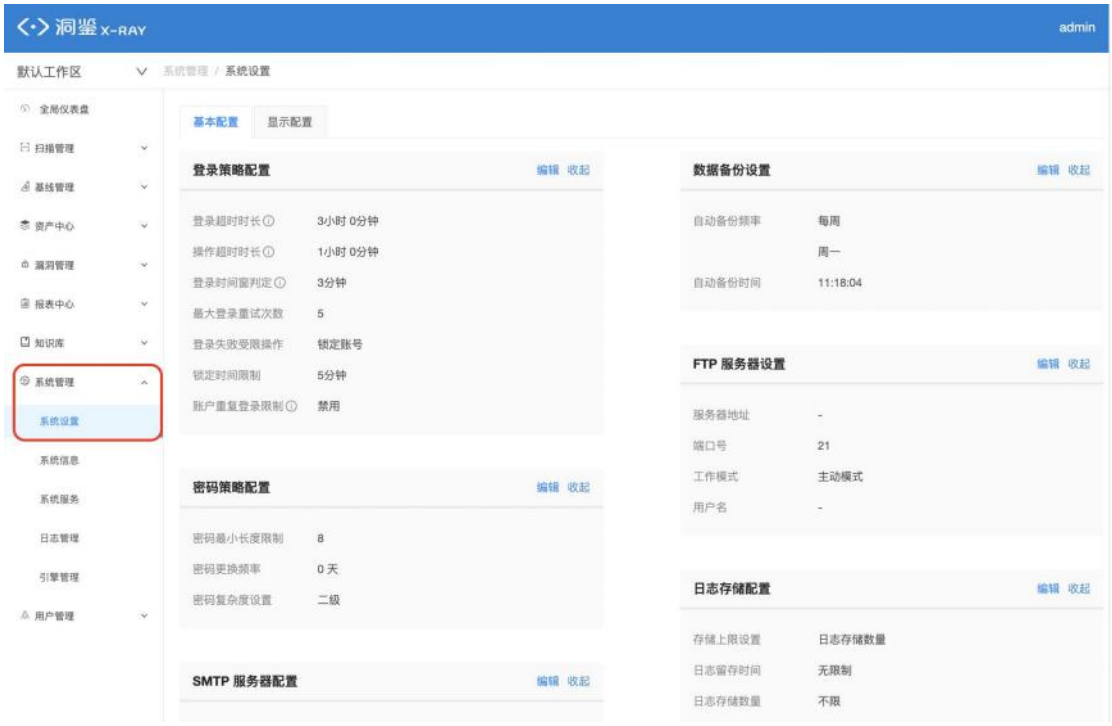

洞鉴 X-RAY
admin
默认工作区
知识库 / 自定义指纹 / 添加自定义指纹
全局仪表盘
扫描管理
基线管理
资产中心
漏洞管理
报表中心
知识库
漏洞库
自定义 POC
自定义指纹
系统管理
用户管理
30 # 定义如何根据规则结果判断结果
31 expression: r1() || r2()
32 # detail信息必填
33 detail:
34 # 可选填写作者是谁
35 author: test
36 # 自定义指纹的主要指纹信息，必填
37 fingerprint:
38 infos:
39 # 如无例外，type 均为web服务对应 web_application，其中name和cpe字段至少填写一个，其余参数选填
40 - type: web_application
41 name: canal # 指纹对应服务的名称
42 cpe: '' # 指纹对应的标准cpe，可选填写，如不填则使用 name、type、和version字段作为指纹显示标准
43 version: '' # 指纹对应的版本
44 confidence: 32 # 指纹置信度
45 description: '' # 指纹的相关描述，可选
46
脚本编写详细说明，请参考《漏洞 yaml 格式自定义指纹说明》
取消
提交

四、系统管理介绍

4.1 系统设置

4.1.1 基本配置

在左侧导航栏中，选择“系统管理–系统配置”，默认进入基本配置界面。



基本配置包含登陆策略配置、密码策略配置、日志相关配置数据备份设置、FTP 服务器设置、日志存储配置、访问 IP 限制等，每个模块的配置点击右上角“编辑”可进行修改。

4.1.1.1 登录策略配置

对登录机制进行设置:

- 登录超时时长：登录超时设置，用户单次登录时长超过设置的时间，账号会自动登出，需要重新登录，默认 3 个小时，系统保留超时日志。
- 操作超时时长：操作超时设置，用户单次登录中超过设置时间未进行点击操作后，账号自动登出，需要重新登录，默认 1 个小时，不可设置 0 数值，系统保留超时日志。

- 登陆时间窗判定：设定一段时长，在此时间内达到了最大登录重试次数，将触发受限，默认 3 分钟；
- 最大登录重试次数：登录系统时，账号和密码的连续尝试次数，默认 5 次；
- 登录失败受限操作：设置当连续登陆失败达到最大重试次数时，触发的受限，默认锁定账号，可选项为：
  - 不限制；
  - 锁定账号，一段时间后自动解锁：该用户账户状态变更为“锁定”，期间可由管理员手动解锁，或到期自动解锁；锁定时长可在下方“锁定时间限制”中设置。
  - 锁定 IP，一段时间后自动解锁：该登陆 IP 地址进入【访问 IP 限制】–【被锁定 IP】，期间可由管理员手动解锁，或到期自动解锁；锁定时长可在下方“锁定时间限制”中设置。
- 锁定时间限制：因登陆失败达到最大重试次数而触发的锁定账户或 IP 的锁定时长，默认 5 分钟；
- 账户重复登录限制：默认为关闭。若开启，则在同一时刻，一个帐户仅能在一个 IP 地址登陆，若在第二个 IP 地址登陆，会强制退出前一个 IP 的登陆。

- 登录验证码限制：默认为关闭。若开启，在登录界面会要求输入验证码。

4.1.1.2 密码策略配置

- 密码最小长度限制：设置用户账户密码长度的最小值，默认 8 位；在添加或编辑用户时，账户密码长度需大于等于最小长度；
- 密码更换频率：如果当前密码的使用时长达到设置的时间上限，没有做任何更改，那么再次登录时，必须按照向导先进行修改密码操作，才可查看并使用系统功能；默认无限制；
- 密码复杂度设置：选择密码复杂度级别，默认二级，各级别对应以下要求：
  - 一级：至少包含大写字母、小写字母、数字、特殊字符中的任意 1 种字符；
  - 二级：至少包含大写字母、小写字母、数字、特殊字符中的任意 2 种字符；
  - 三级：至少包含大写字母、小写字母、数字、特殊字符中的任意 3 种字符；
  - 四级：同时包含大写字母、小写字母、数字、特殊字符。

4.1.1.3 SMTP 服务器设置

简单邮件传输协议（SMTP）是一种发送、接收邮件的标准协议。SMTP 配置页面可以帮助用户配置 SMTP 服务器。成功配置 SMTP 后，用户可以使用扫描结束后接收邮件通知的功能。

配置 SMTP

若用户还没有配置过 SMTP 服务器，在此处可以进行 SMTP 的配置，具体操作如下:

- 点击右上角“编辑”，显示 SMTP 配置的弹窗；
- 在弹窗中根据文案提示，配置相应信息；
  - SMTP 服务器:用户决定用来发送邮件的服务器地址 如:smtp.gmail.com；
  - 端口：该服务器提供 SMTP 服务的端口；
    - 如：465

- 发件邮箱账号：认证 SMTP 服务器所需的用户名；
  - 如：xiaoming.li@gmail.com
- 发件人名称：将显示在用户收到的通知邮件“发件人”中，用户可以自行定义；若此处为空，则系统默认以【显示配置】中的“产品名称”字段值作为发件人名称；
- 连接授权码：认证 SMTP 服务器所需的密码；
- 加密方式：该服务器端口所使用的加密方式，默认不加密；
- 邮件签名：邮件签名将显示在用户收到的通知邮件中，用户可以自行定义；

- 点击“保存”，即可保存填写的 SMTP 配置。

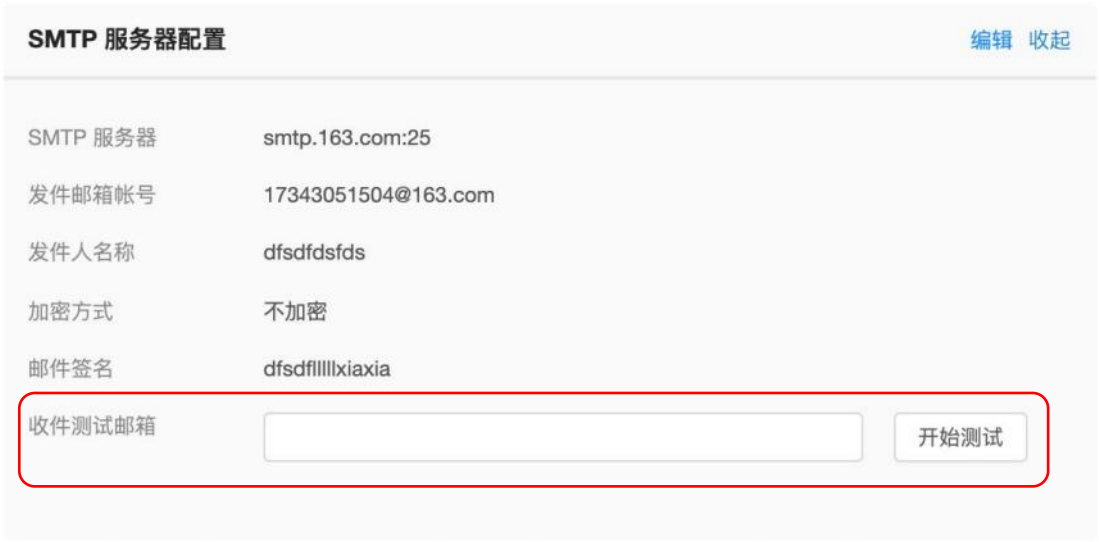
内容展示

配置完成后，页面展示 SMTP 配置信息，包括服务器和端口、发件邮箱账号、发件人名称、邮箱签名。

测试 SMTP 发件配置

用户可在此处测试 SMTP 是否成功配置:

- 在“测试 SMTP 发件配置”处，填写收件测试邮箱的地址；
- 点击“开始测试”



- 打开上文填写的收件测试邮箱，若能收到来自发件邮箱的通知邮件，则证明 SMTP 配置成功

4.1.1.4 日志输出配置

可配置 syslog 服务器，配置成功后，本系统操作日志将自动传输至 syslog 服务器。

- 日志输出内容：当前仅支持输出全部内容；
- SYSLOG 服务器：输入服务器和端口；
- RFC：选择数据格式规范协议，支持 RFC3164 或 RFC5424；
- 协议：支持 TCP 或 UDP。

4.1.1.5 数据备份配置

可开启自动备份并设置自动备份的周期和时间。

- 自动备份频率：可选择备份频率，每周、每月或自定义天数；默认不开启自动备份；
- 自动备份时间：开启自动备份后，设置具体的备份时间点。

4.1.1.6 FTP 服务器设置

此处仅配置 FTP，后续将可将报告上传至配置的 FTP 服务器。

- 服务器地址；
- 端口号，默认 21；
- 工作模式：可选主动模式或被动模式；
- 用户名：用户名为空则表示以匿名方式登陆；
- 密码：以匿名方式登陆无需输入密码。

4.1.1.7 日志存储配置

- 存储上限设置：可选择按时间或者按数量对存储的日志进行限制；
- 日志留存时间：若选择按时间对日志存储进行限制，则选择日志的保留时间；超过留存时间的日志将自动从数据库中移除；
- 日志存储数量：若选择按数量对日志存储进行限制，则设置系统最大存储的日志条数，默认不限；
- 达到上限告警通知:填写告警邮箱，当快达到设置的存储上限时，会给出邮件告警通知：

- 该功能使用的前提：必须已成功配置 SMTP（详情见 3.1.1 基本配置–SMTP 服务器设置）。

4.1.1.8 访问 IP 限制

对访问洞鉴系统的 IP 地址以黑名单或白名单进行限制。

- 限制方式：选择开启黑名单或白名单，对可访问系统的 IP 进行限制；
- 访问黑名单：在黑名单内的 IP 不可访问系统；输入支持 CIDR 和单个 IP 地址；各 IP 间之间用换行隔开；支持 ipv6 和 ipv4；
- 访问白名单：仅在白名单内的 IP 可访问系统；输入支持 CIDR 和单个 IP 地址；各 IP 间之间用换行隔开；支持 ipv6 和 ipv4；
- 被锁定 IP：展示因登陆失败达最大次数触发的被锁定 IP 列表；可手动对该 IP 进行解锁，或等待锁定时间结束后，IP 自动解锁。

4.1.1.9 报表设置

- 报表生成超时时长：生成报表时若超过该设定值，报表生成将被判定为失败；默认两小时。

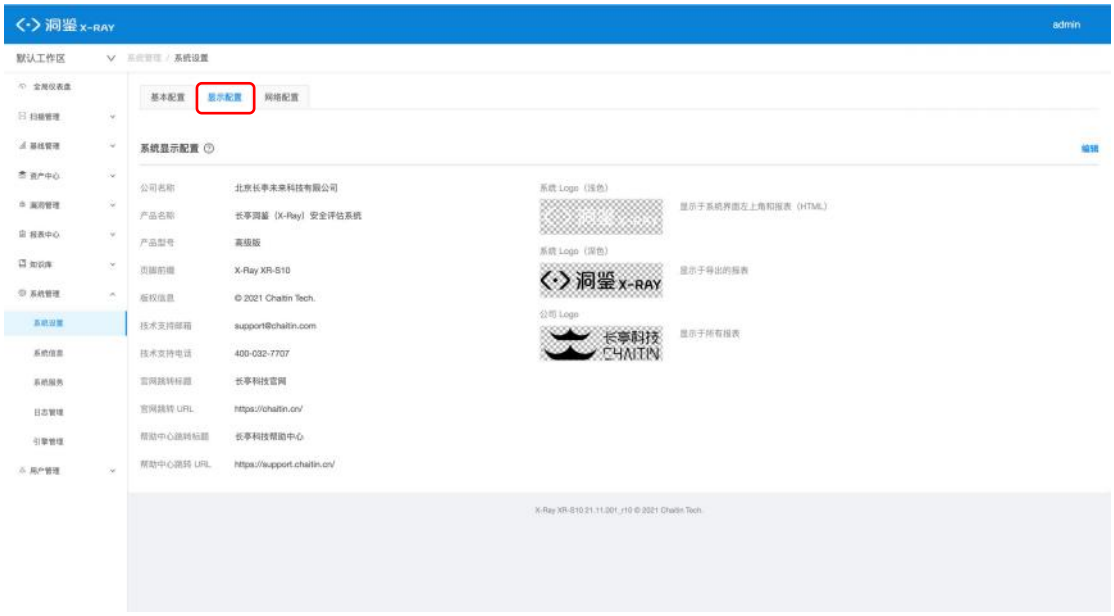
4.1.1.10 时间服务配置

- 系统时间：设置系统时间
- 是否同步：
  - 启用则每 30 秒通过 ntp 服务器同步一次时间；
  - 关闭则不同步时间，且不需要设置 ntp 服务器。
- ntp 服务器：当同步开启时，输入 ntp 服务器地址。

注：NTP 服务器时间配置能力仅支持硬件版。

4.1.2 显示配置

在上方分栏中，选择“显示配置”，进入显示配置界面。



支持企业对系统界面进行 OEM 配置，包含公司名称、产品名称、系统 Logo 等字段。

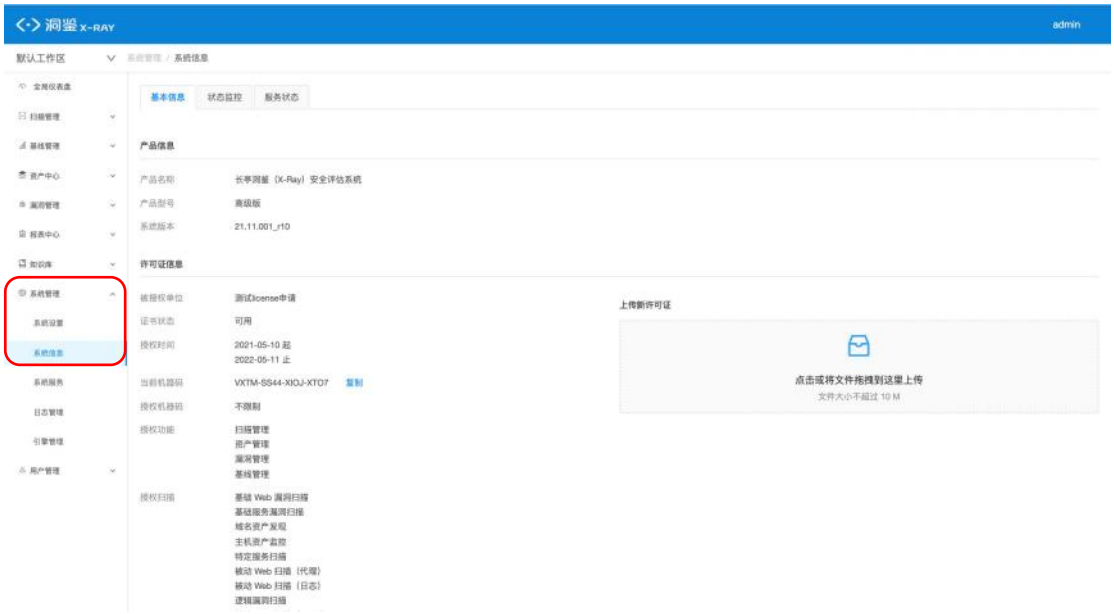
- 点击“系统显示配置”后的“问号”图标，可展开各配置项的影响位置说明。

- 点击右上角的“编辑”按钮，可对显示配置的各项进行编辑

4.2 系统信息

4.2.1 基本信息

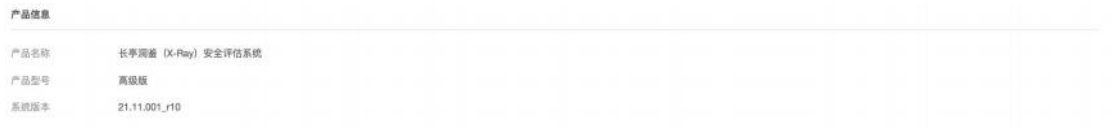
在左侧导航栏中，选择“系统管理–系统信息”，默认进入基本信息界面。



包含产品信息、许可证信息和技术支持信息

4.2.1.1 产品信息

展示洞鉴的产品全称、当前产品型号、当前系统版本



4.2.1.2 许可证信息

展示信息：

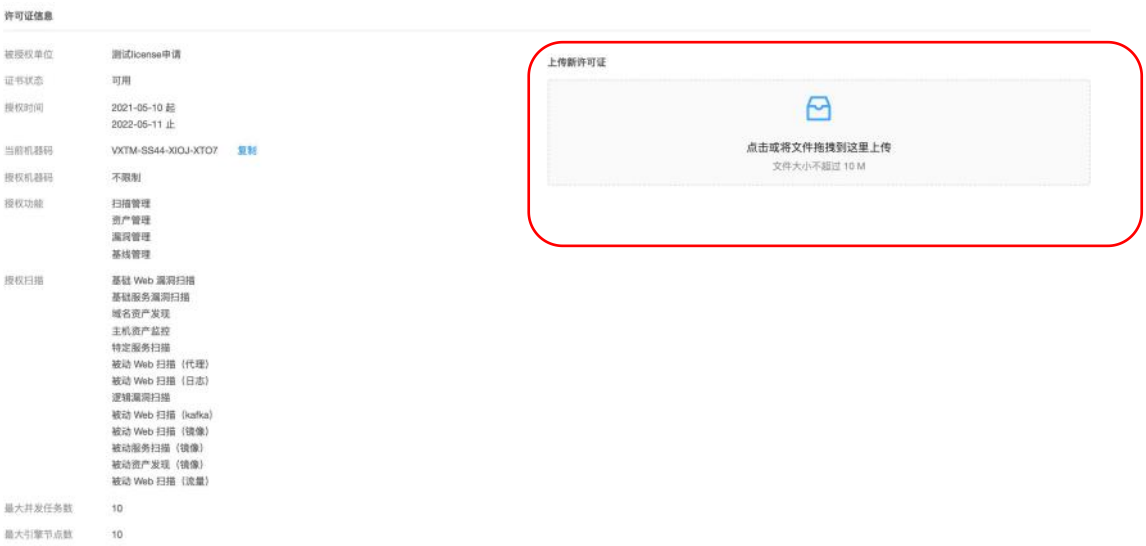
许可证信息页面展示企业的许可证信息，内容包括以下字段：

- 被授权的企业名称
- 证书状态：证书到期前 30 天，会开始倒数提示证书还有多少天到期
- 授权时间
- 当前机器码
- 授权机器码
- 授权功能
  - 不同 license 版本具有不同的产品功能，详情可以联系对接您的长亭技术支持同事
- 授权扫描
  - 授权扫描包括各类扫描策略
- 最大并发任务数
  - 决定了该产品最大可同时并发执行的任务数量上限(不限任务类型)
- 最大引擎节点数
  - 决定管理平台可连接的引擎数量上限

上传/更新许可证

在许可证信息页面，可对即将过期的许可证进行更换，具体操作如下：

- 在上传新许可证的地方，点击或将许可证文件拖拽到此处上传：
  - 点击红色区域，弹出文件框，选择许可证文件并点击确认，完成许可证的上传；
  - 直接将许可证文件拖到红色框选区域，也可完成许可证的上传。



- 上传正确的许可证文件后，会显示被授权企业名称与授权使用时间。管理员确认无误后，点击“确认”，即可完成许可证的更新，此时许可证内容显示新上传的许可证信息。

4.2.1.3 技术支持

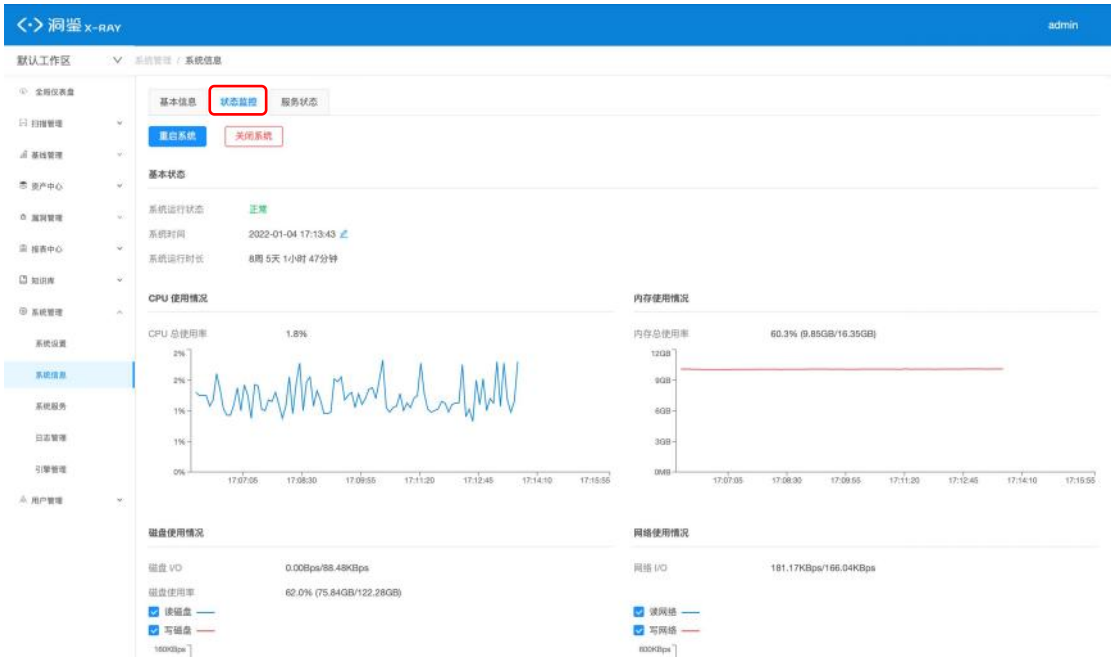
展示技术支持邮箱和技术支持电话

- 若用户遇到了产品使用手册上无法解决的问题，可以通过技术支持邮箱和技术支持电话，向长亭科技的技术支持人员求助。

4.2.2 状态监控

在上方分栏中，选择“状态监控”，进入状态监控界面。

展示系统的整体运行状态，如下图所示：



4.2.2.1 系统操作

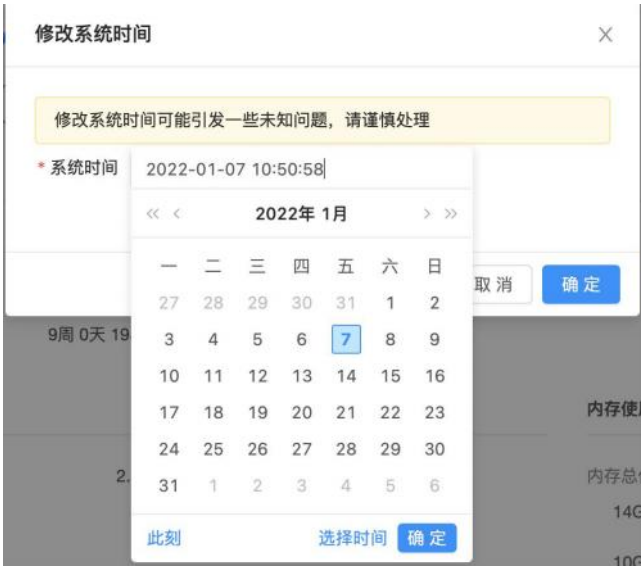
【硬件设备特有功能】– 系统操作，可对系统进行操作：

- 重启系统：重启硬件设备
- 关闭系统：关闭硬件设备

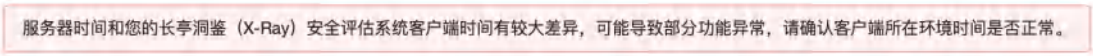
4.2.2.2 基本状态

展示系统的整体运行状态和系统运行时长

- 系统运行状态：显示状态正常或者异常或者停止；
- 系统时间：显示系统时间；可以点击更改客户端时间（不建议无端更改，可能会引发未知问题，请谨慎处理）



- 若客户端显示的与服务器时间的不符：

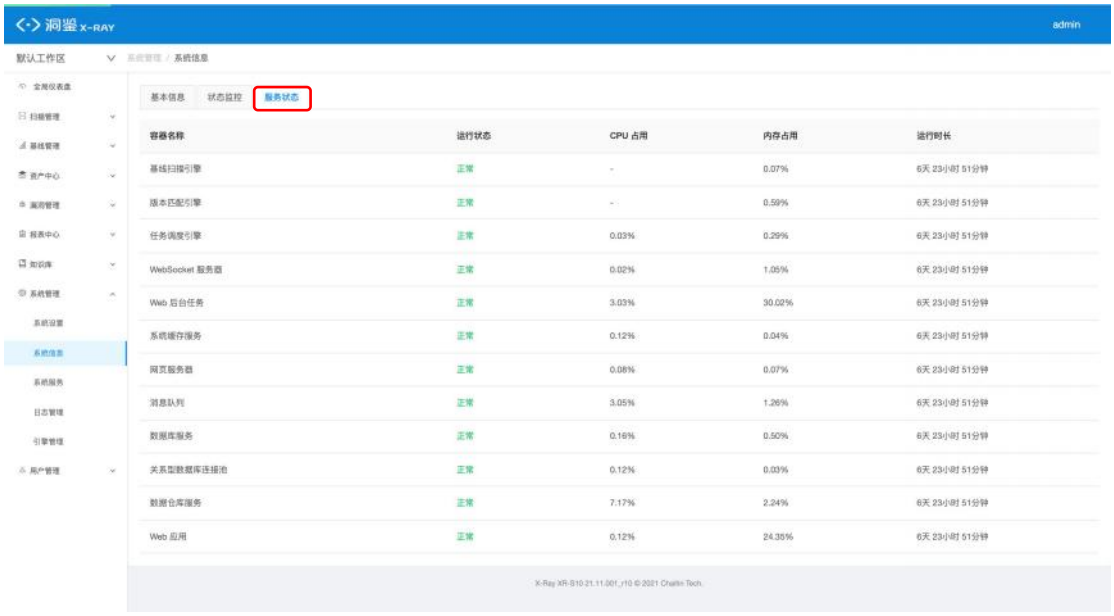


- 系统运行时长：显示系统运行时长；
- CPU 使用情况：展示最近 10 分钟的 CPU 总使用率；
- 内存使用情况：展示最近 10 分钟的内存总使用率、内存总使用量和内存总量；
- 磁盘使用情况：展示最近 10 分钟的磁盘读写情况、磁盘总使用率、磁盘总使用量和磁盘总量。

4.2.3 服务状态

在上方分栏中，选择“服务状态”，进入服务状态界面。

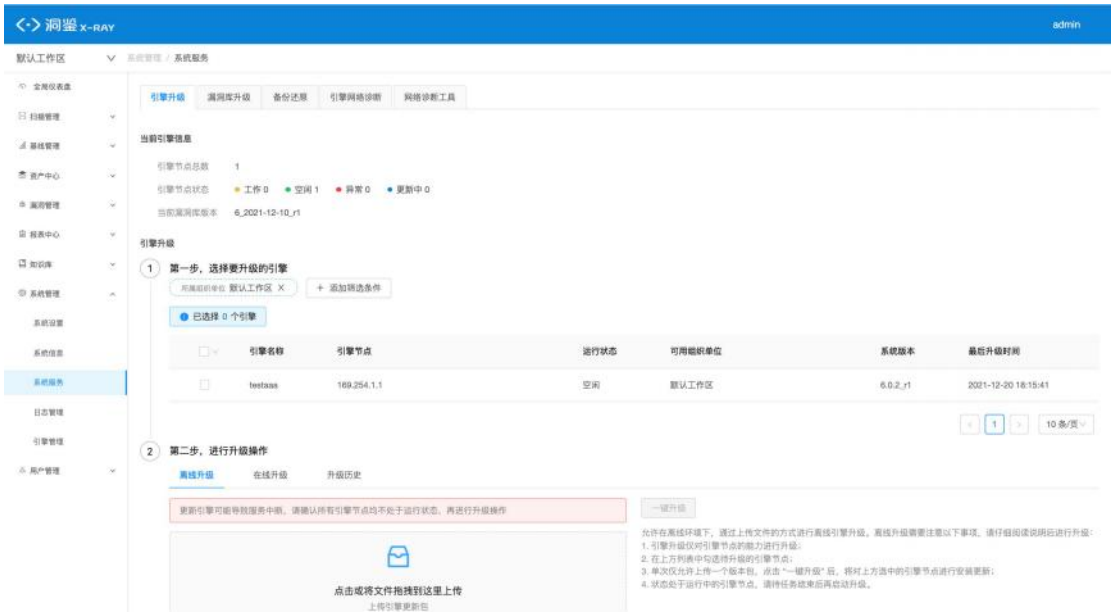
展示各容器的运行状态，包含容器名称、运行状态、CPU 占用率、内存占用率、运行时长：



4.3 系统服务

4.3.1 引擎升级

在左侧导航栏中，选择“系统管理–系统服务”，默认进入引擎升级界面。



4.3.1.1 内容展示

注：想要查看所有有权限查看的引擎节点请删掉默认的当前组织单位的筛选条件。

版本信息页面展示当前系统的版本信息，具体包括:

- 引擎节点数
- 引擎节点状态（工作、空闲、异常、更新中的个数）
- 当前漏洞库版本
- 每个引擎节点的版本等相关信息：
  - 引擎名称
  - 引擎节点
  - 运行状态
  - 可用组织单位
  - 系统版本
  - 最后升级时间

- 系统版本：
  - 系统版本表示洞鉴扫描算法与策略的版本；
  - 系统版本与系统预置的扫描策略、扫描插件等密切相关，更高的引擎版本会有更优秀的扫描效果；
  - 系统版本可以在版本信息页面上直接更新，详情见下文“引擎节点升级”。

- 引擎状态：
  - 引擎状态表示当前洞鉴的扫描引擎运行状态；
  - 状态有 4 中类型：
    - 工作：正在执行扫描任务的节点；
    - 空闲：状态正常且没有执行扫描任务的节点；
    - 异常：状态不正常的节点，这种状态的节点，一般无法正常运行扫描任务，异常状态可能存在的问题可以参考当前洞鉴版本的部署文档“常见问题四”中的解决方法；
    - 更新中：引擎节点正在进行升级操作时的状态，该状态下不能启动扫描任务。

4.3.1.2 引擎节点升级

在版本升级页面可以直接更新引擎版本。当前支持离线升级和在线升级。

注意：更新引擎可能导致服务中断。若系统有正在运行的任务，则不能更新引擎版本。请停止所有正在运行的任务，再尝试更新引擎版本。

内容展示：显示引擎名称、引擎节点 IP、运行状态、可用组织单位、最后升级时间

操作步骤：更新引擎版本的具体操作步骤如下：

- 确定系统当前的引擎版本、需要的引擎版本，准备对应的引擎更新包；
- 升级模式支持“一键升级全部引擎节点”和“单节点升级”；
- 确保系统没有任务处于正在扫描状态。

离线升级：

- 上传框上传引擎更新包，或将引擎升级包拖拽到此处上传，上传过程显示上传进度

- 更新包上传完成后，确认引擎版本是否正确:

- 点击“一键升级”；
- 确认引擎版本正确后，点击“确认更新”；
- 返回版本信息页面，引擎状态变为“更新中”；

■ 引擎更新大概需要十几分钟，期间扫描任务无法正常启动。请耐心等待更新完成。

- 引擎更新完后，版本信息页面的“引擎版本”相应变化，引擎状态显示“运行正常”，则表示引擎版本更新成功

在线升级：

前提：需要注册在线升级平台后方可使用在线升级功能

1. 访问升级服务平台

2. 使用许可证进行注册

3. 点击“更新升级服务平台地址”，输入“https://product-support.chaitin.cn/”，点击“确定”即可

- 在第二步选择“在线升级”Tab 后，若有新的可下载的在线升级包，会显示红色气泡及对应的数量；
- 点击最新引擎版本旁的下载新版本开始下载；
- 下载后可以开始升级。

4.3.2 漏洞库升级

在上方分栏中，选择“漏洞库升级”，进入漏洞库升级界面。

- 点击进入系统服务的漏洞库升级中，显示当前漏洞库信息（版本、漏洞总数、上次更新时间），可通过一键升级或者上传升级包来操作离线升级漏洞库；
- 可以查看升级历史，包含漏洞库版本、漏洞更新描述、开始升级时间、完成升级时间、更新状态。

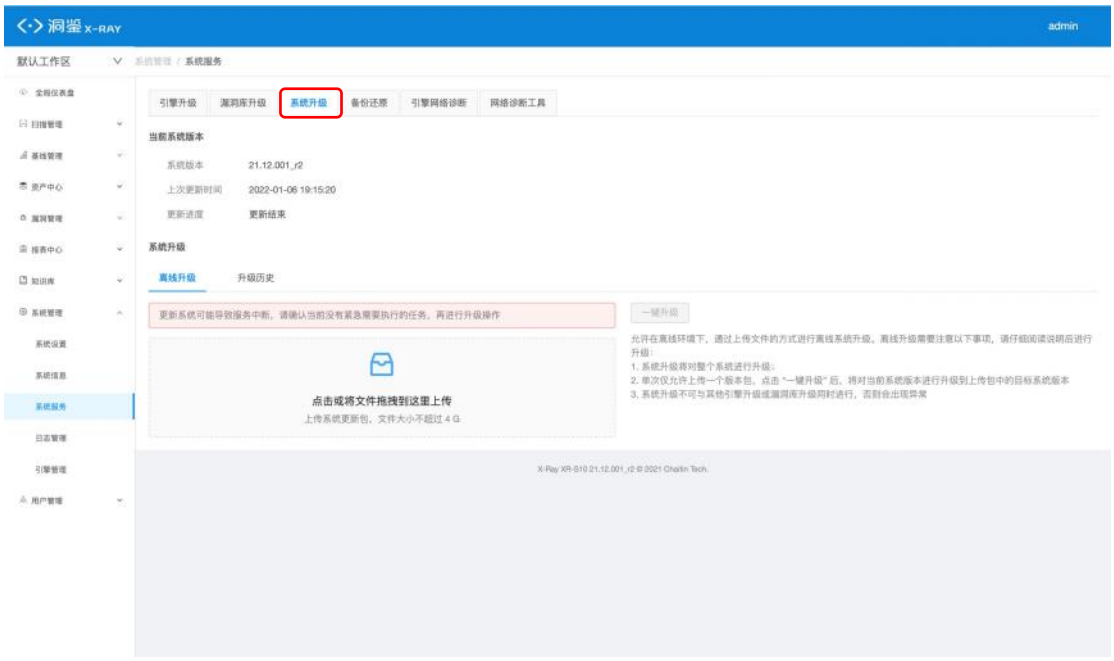
漏洞库升级：

同“引擎升级”中的离线升级和在线升级，且能查看升级历史。

4.3.3 系统升级

展示内容：

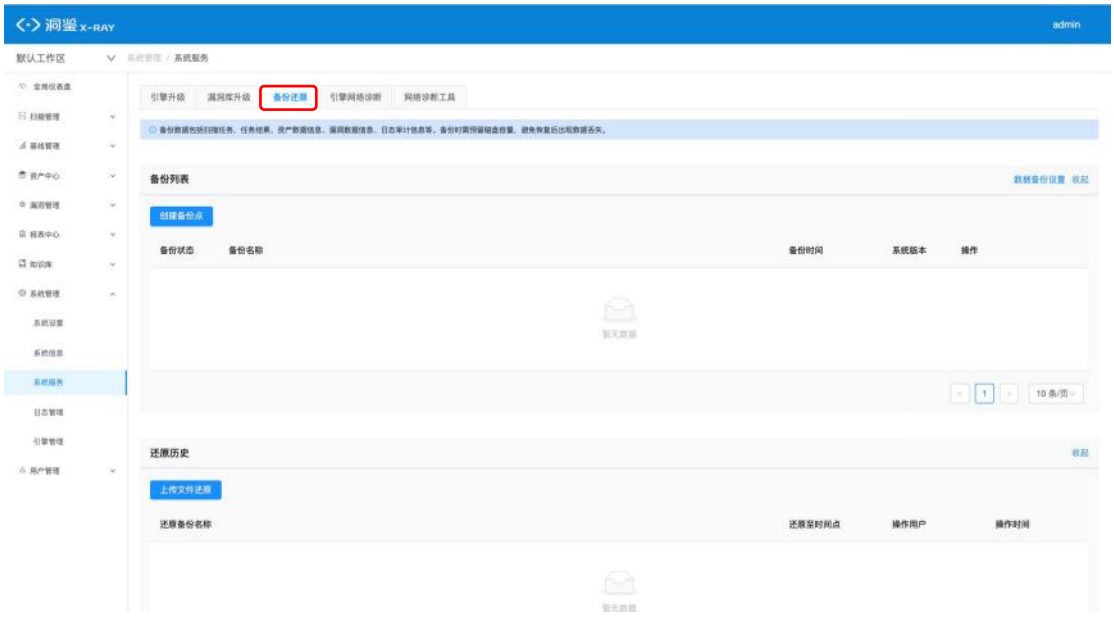
- 当前系统版本：
  - 系统版本：显示版本号
  - 上次更新时间：
  - 更新进度：



系统升级：

- 离线升级：可以通过上传升级包（小于 4GB）后一键升级。升级过程中任务会中断，且不能与引擎同时升级。
- 升级历史：可以查看历史升级的相关情况。

4.3.4 备份还原



备份还原提供备份系统数据库、还原系统数据的功能。

4.3.3.1 系统备份

备份数据包括扫描任务，任务结果、资产数据信息、漏洞数据信息、日志审计信息等。备份时需预留磁盘容量，避免恢复后出现数据丢失。

此处以备份列表展示备份记录。

- 点击列表上方“创建备份点“，可编辑备份名称，点击确定后开始备份；备份期间请勿离开当前页面，否则会取消当前备份任务；
- 可在【系统设置】–【基本配置】中开启自动备份功能，详见 4.1.1.5 数据备份配置；
- 开始创建备份点后，备份列表会出现一条新记录，展示备份状态、备份名称、备份时间、系统版本和可进行的操作；
- 待备份完成后，可对备份点进行备份文件下载至本地、在线还原、删除操作：
  - 点击在线还原，可将系统还原至该备份点，当前系统数据被覆盖。

4.3.3.2 系统还原

可通过备份列表，对某备份点在线还原，或者上传备份文件手动还原；可还原历史版本和当前版本的备份文件。系统还原列表记录还原操作历史。

- 点击列表上方的“上传文件还原”，选择本地的备份文件，上传结束后，会解析出备份文件相关信息；点击“确认恢复”，将对备份数据进行还原

4.3.5 引擎网络诊断

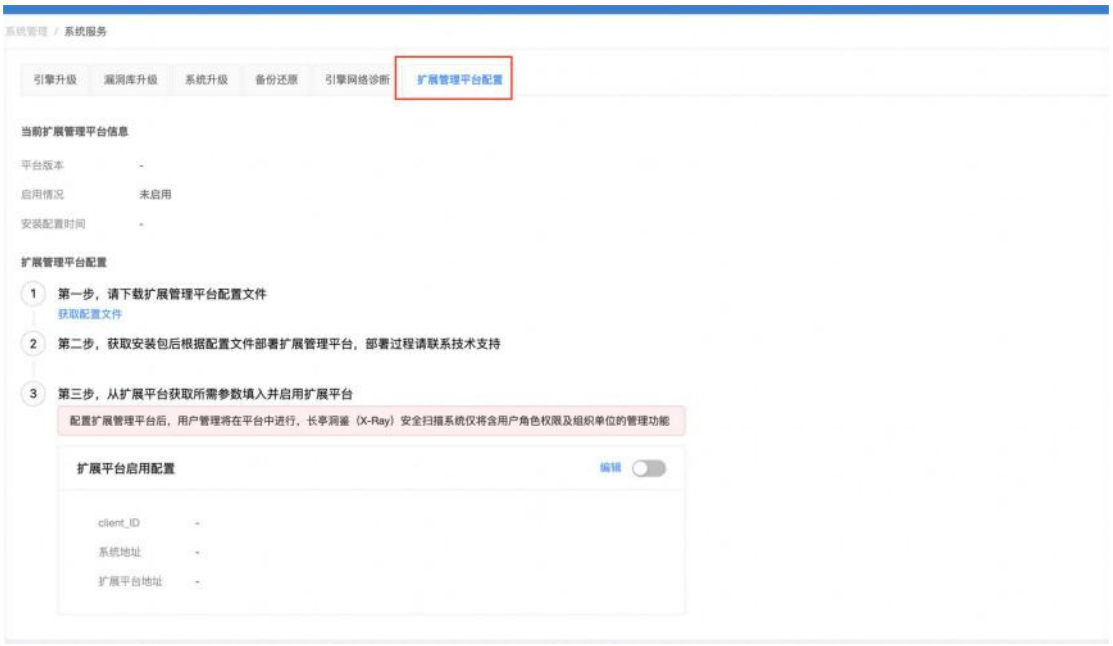
在上方分栏中，选择“引擎网络诊断”，进入引擎网络诊断界面。

用于诊断每个扫描与扫描目标的连通性，用于测试引擎节点与目标 IP 之间的连通性，具备 ping、traceroute 和 nmap 命令进行网络诊断：

- 选择命令：ping、traceroute 或 nmap；

- 填入目标 IPv4 或者 IPv6 地址，点击按钮进行连通性测试，后查看结果。

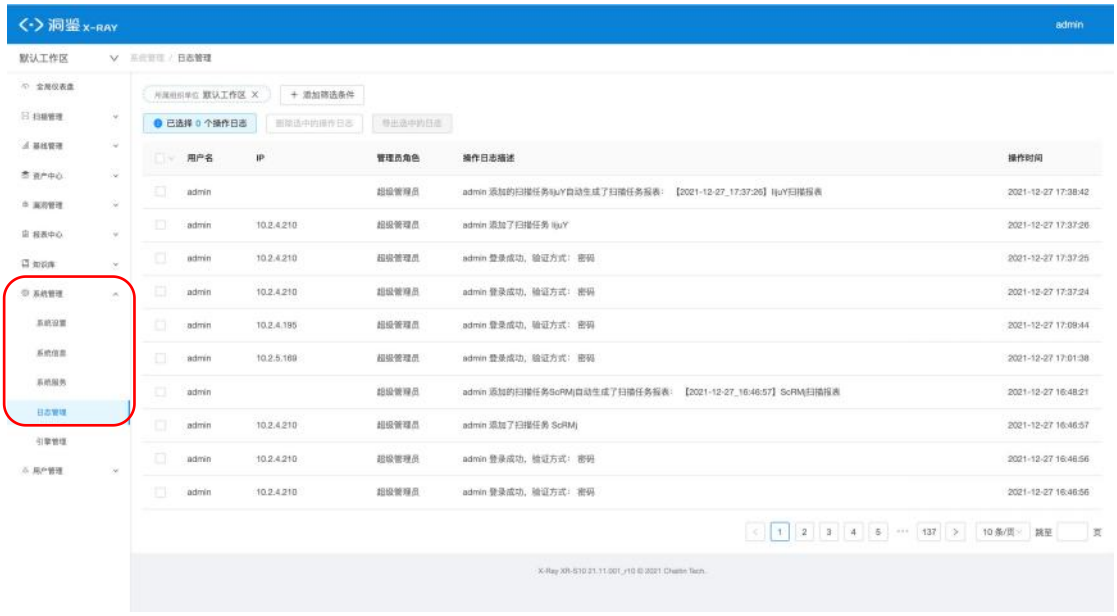
4.3.6 扩展管理平台配置



可查看当前扩展管理平台的配置信息，还可以通过三步完成对扩展平台的配置。

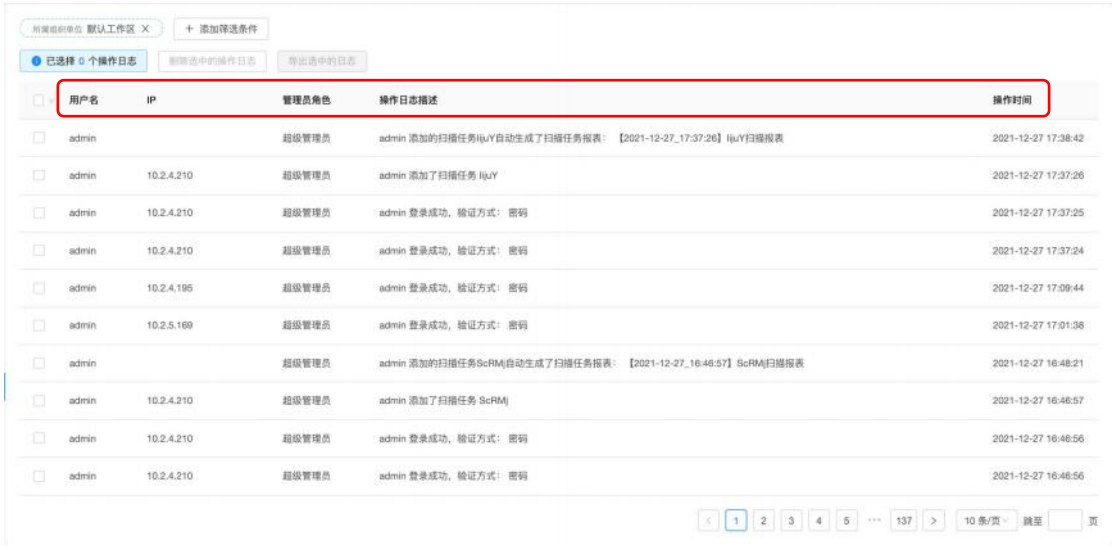
4.4 日志管理

4.4.1 操作日志列表



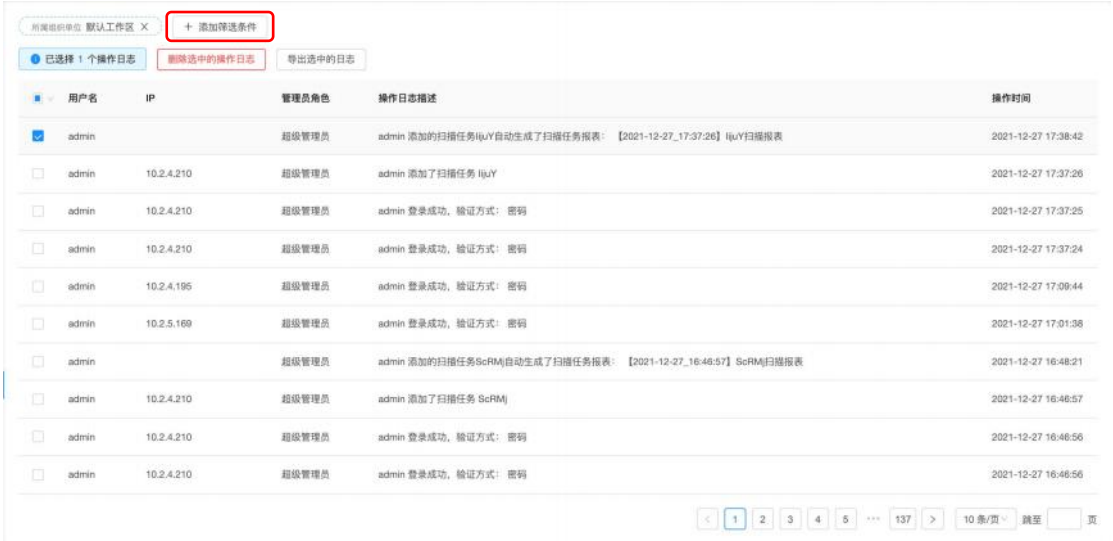
4.4.1.1 内容展示

主要展示使用洞鉴的所有用户的操作日志，内容包括用户名、IP、管理员角色、操作描述、操作时间：



4.4.1.2 添加筛选条件

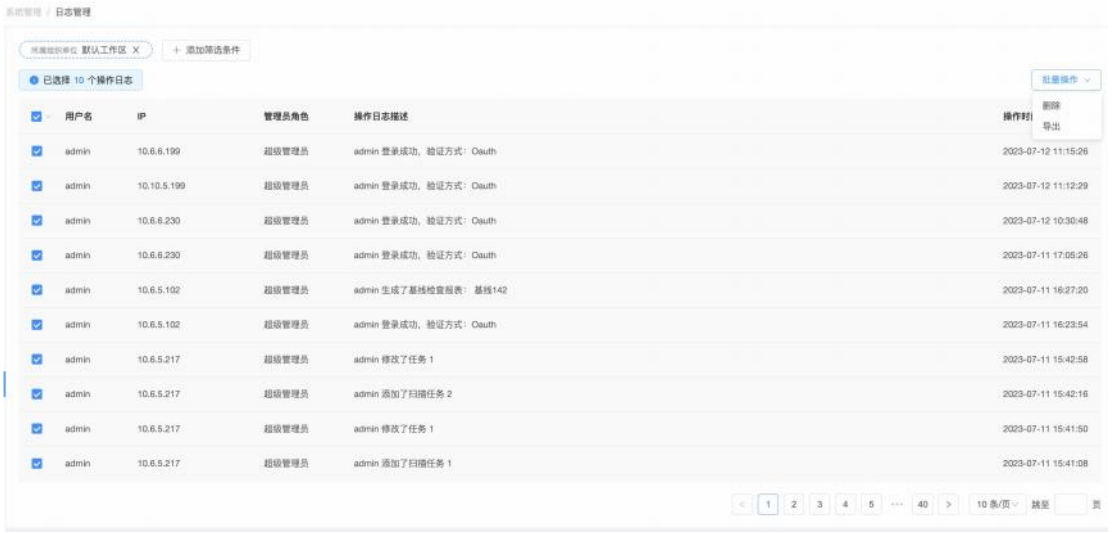
- 点击添加筛选条件，从用户名、管理员角色、操作关键词、操作时间、所属组织单位；
- 可以采用精确匹配或者模糊匹配的方式；
- 点击保存生效；
- 可以在弹窗或者列表中删除已经设定的筛选条件。



4.4.1.2 批量操作日志

只有有日志管理权限的人才可以批量导出和删除日志。

- 选择要导出/删除的日志，然后点击“导出/删除”，即可自定导出并下载 json 文件或删除日志。

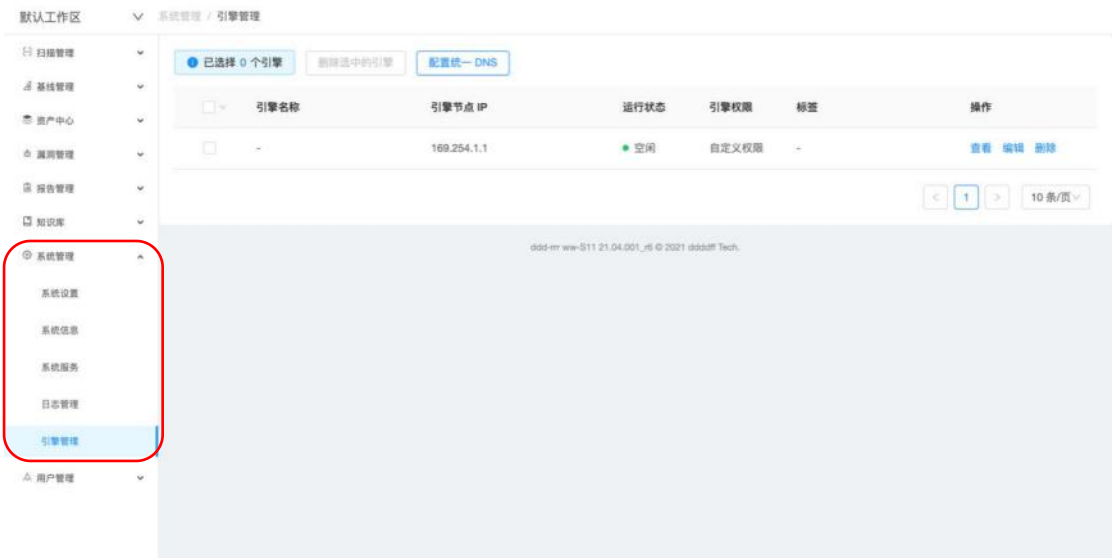


4.5 引擎管理

注：洞鉴在第一次使用时，引擎列表内无引擎节点，需要将筛选项“默认工作区”删除后，方可看到所有引擎，然后点击编辑，将之分配到“默认工作区”或目标工作区后继续使用。

4.5.1 引擎列表

在左侧导航栏中，选择“系统管理–引擎管理”，默认进入引擎列表界面。



4.5.1.1 内容展示

在引擎管理页面中，以列表方式展示所有引擎节点的相关信息，包括引擎名称、引擎节点 IP、运行状态、引擎权限、标签、CPU 总使用率和内存总使用率、以及对应操作选项。

4.5.1.2 筛选操作

点击列表上方“添加筛选条件”，可根据引擎名称、引擎节点 IP、运行状态、所属组织单位对列表中的引擎进行筛选。

4.5.1.3 批量操作

删除引擎

勾选选择一个或多个引擎后，可点击“批量操作”–“删除”，对引擎进行删除：

- 若选中删除的引擎包含内置引擎，则无法删除；

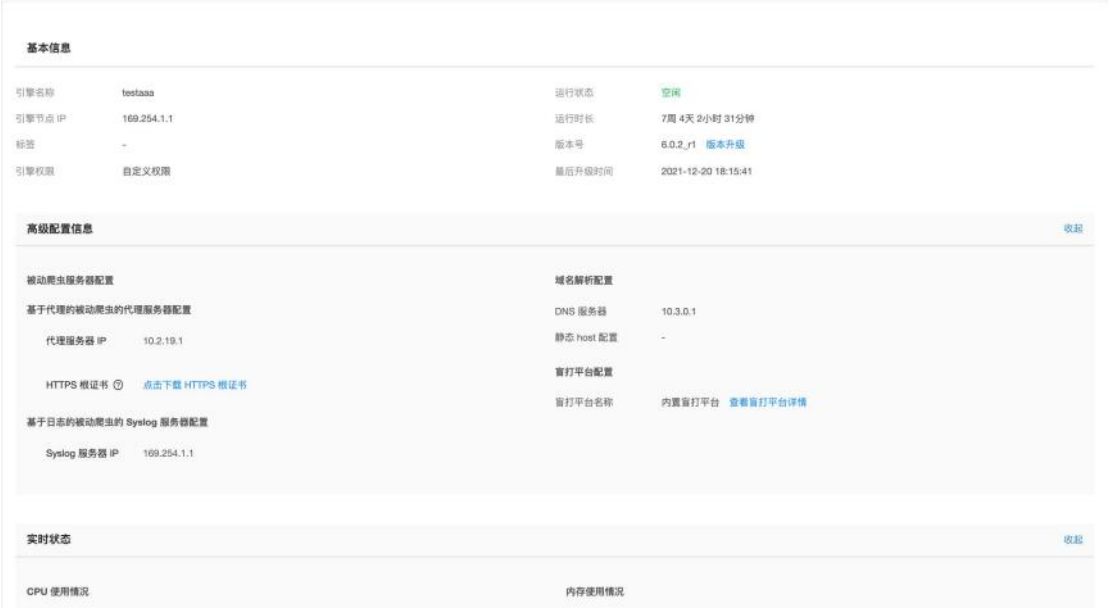
- 若删除的引擎有关联的扫描任务，则系统会返回相关任务列表；需在扫描任务的配置中修改引擎选择后，重试删除操作，才可成功删除。

配置统一 DNS

- 点击列表“批量操作–配置 DNS”，参考 4.5.2.2 域名解析配置

4.5.1.4 查看引擎详情

点击操作列的 “查看”，可以查看节点详情：



基本信息

展示引擎节点名称、引擎节点 IP、标签、引擎权限、引擎运行状态、运行时长、引擎版本号、最后升级时间

- 点击版本号右侧的“版本升级”按钮，可跳转至【系统服务】–【引擎升级】页面进一步操作；

高级配置信息

展示该引擎节点的被动爬虫服务器配置、域名解析配置信息；

实时状态

该引擎节点的 CPU 状态、内存状态、网络状态、磁盘状态，与上文介绍的【系统信息】-【状态监控】数据指标一样

4.5.1.5 编辑引擎

点击操作列的“编辑”，可以编辑引擎节点的信息：

引擎基本信息

可编辑引擎名称、权限、组织单位等属性，组织单位针对工作区全程支持模糊匹配功能。

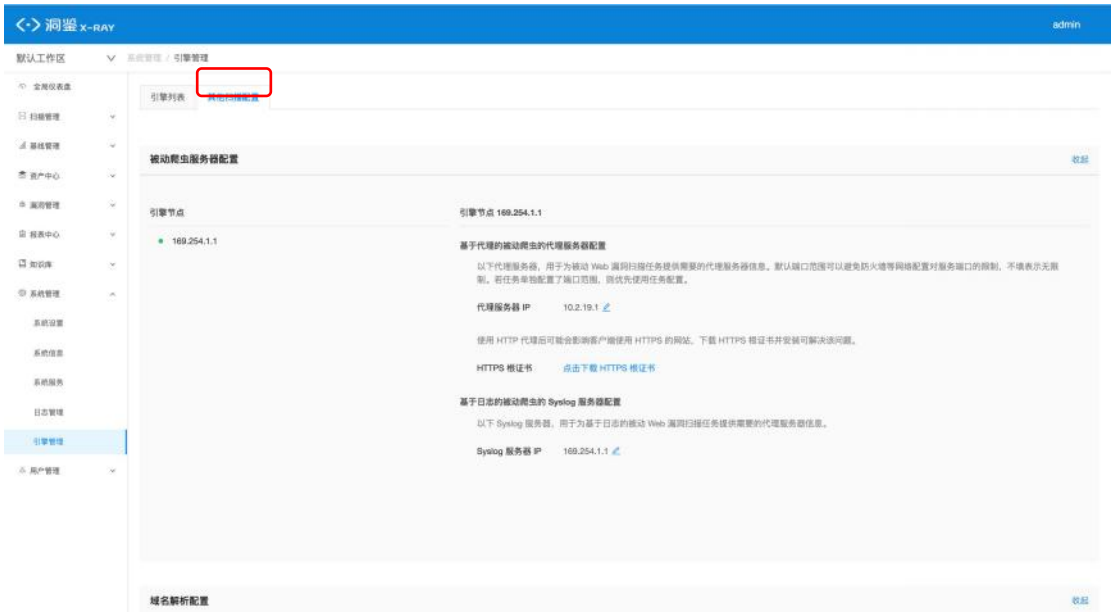
被动爬虫服务器配置

配置该引擎节点的被动爬虫服务器，与 4.5.2.1 被动爬虫服务器配置实现相同功能。

域名解析配置

与 4.5.2.2 域名解析配置实现相同功能。

4.5.2 其他扫描配置



4.5.2.1 被动爬虫服务器配置

在使用被动 Web 扫描（代理）和被动 Web 扫描（日志）这两个被动扫描策略时，需要在此处进行配置操作。

代理服务器 IP 和 Syslog 服务器 IP 默认为各节点的服务器 IP，用户可以在这里查看、配置、修改代理服务器的 IP 和端口范围。

每个节点单独配置，不支持统一配置。

基于代理的被动爬虫代理服务器配置

此处配置用于该引擎节点可运行被动 Web 扫描(代理)任务。

- 代理服务器 IP：默认为引擎节点 IP，点击“编辑”图标可手动修改；
- HTTPS 根证书：使用 HTTP 代理后可能会影响客户端使用 HTTPS 的网站，下载 HTTPS 根证书并安装可解决该问题。

基于日志的被动爬虫的 Syslog 服务器配置

此配置用于被动 Web 漏洞扫描（日志）这个扫描策略，用于为该扫描策略提供需要的代理服务器信息，收集日志中的相关信息。

- Syslog 服务器 IP：默认为引擎节点 IP，点击“编辑”图标可手动修改。

4.5.2.2 域名解析配置

如果用户希望在扫描主机资产时，使用自定义的 DNS 服务器、或自定义的静态 host 配置来解析域名，可以在此处配置相应信息。

所有节点可以统一配置 DNS 服务器或每个节点单独配置服务器：

统一配置 DNS 服务器：

- 点击“统一配置 DNS 服务器”，弹框如下图所示:

- 填写 DNS 服务器信息：
  - 如果配置了 DNS 服务器，当洞鉴的一个主机扫描任务尝试解析域名目标时，将依次向已配置的 DNS 服务器发送 DNS 请求。
  - 在输入框内输入 DNS 服务器的 IP 地址，可同时输入多个 IP，以换行分隔。
- 填写静态 host 配置信息：
  - 如果配置了静态 host，当洞鉴的一个主机扫描任务尝试解析域名目标时，将首先尝试用此处配置的静态 host 来解析；
  - 在输入框内配置静态 host，可同时输入多个静态 host 配置，以换行分隔。
- 选择引擎节点：
  - 默认选中全部引擎节点，可自由定义要应用的引擎节点。
- 点击“确定”，即完成配置。

单节点配置 DNS 服务器：

在每个节点右侧显示的 DNS 服务器和静态 host 配置处，修改相应信息即可。配置方案如下：

- DNS 服务器：
  - 在输入框内输入 DNS 服务器的 IP 地址，可同时输入多个 IP，以换行分隔；
  - 点击“保存”，即完成配置。
- 静态 host 配置：
  - 在输入框内配置静态 host，可同时输入多个静态 host 配置，以换行分隔；
    - 静态 host 的格式为：主机 IP 地址 + 域名，IP 和域名间至少要有一个空格。
  - 点击“保存”，即完成配置。

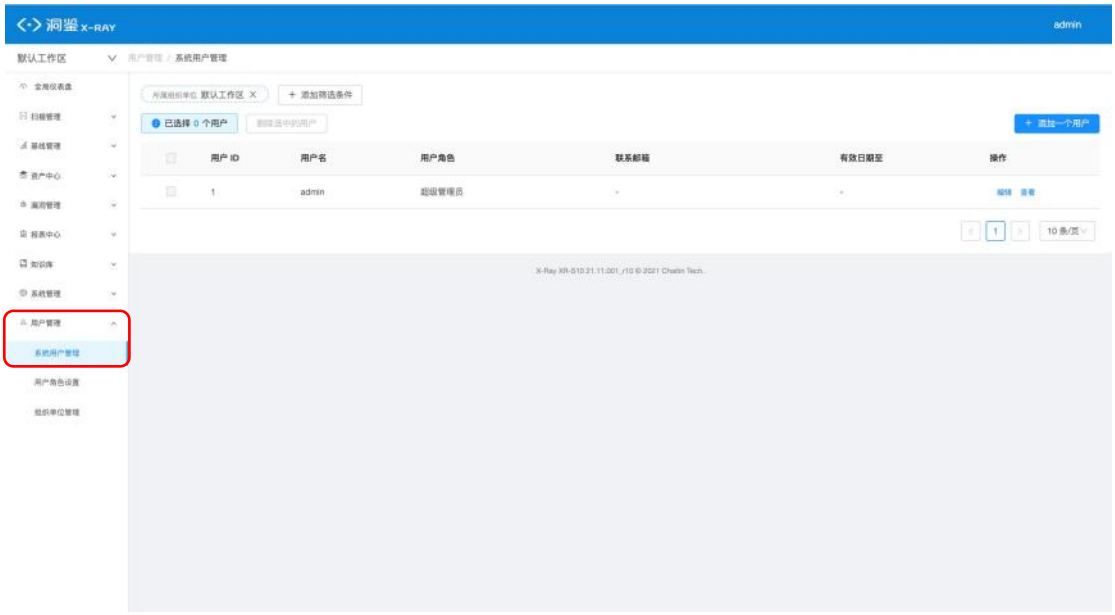
五、用户管理

此模块主要用于企业对使用洞鉴的用户的管理，包括添加用户、删除用户、修改用户信息，查看操作日志等。

5.1 系统用户管理

5.1.1 系统用户管理

在左侧导航栏中，选择“用户管理–系统用户管理”，进入系统用户管理界面。



5.1.1.1 内容展示

系统用户管理页主要展示使用洞鉴的所有用户的信息，内容包括用户 ID、用户名、用户角、联系邮箱和有效日期等：

- admin 为洞鉴部署时的默认用户，用户 ID 为 1 ，用户角色为系统管理员；

5.1.1.2 筛选操作

可以通过用户名称、用户角色及所属组织单位对列表中的用户进行筛选。

5.1.1.3 添加用户信息

- 在系统用户管理页面可以添加用户，

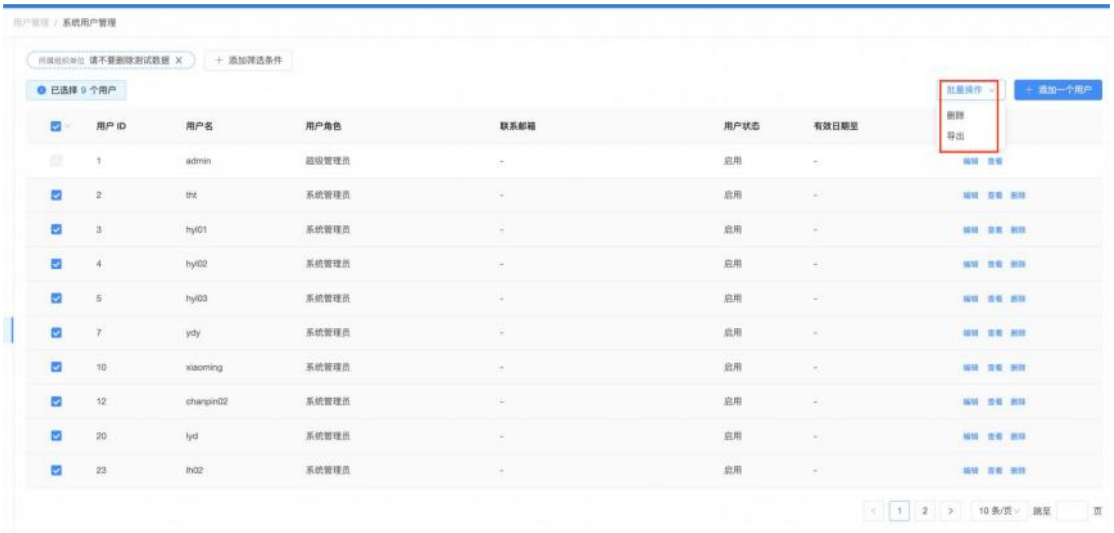
5.1.1.4 修改用户信息

- 在系统用户管理页面可以编辑现有的用户

- 在弹窗中根据文案提示，填写修改后的密码、确认密码：
  - 若不填写密码，则表示不修改旧密码。

5.1.1.5 批量操作

在系统用户管理页面可以批量删除和导出用户信息。

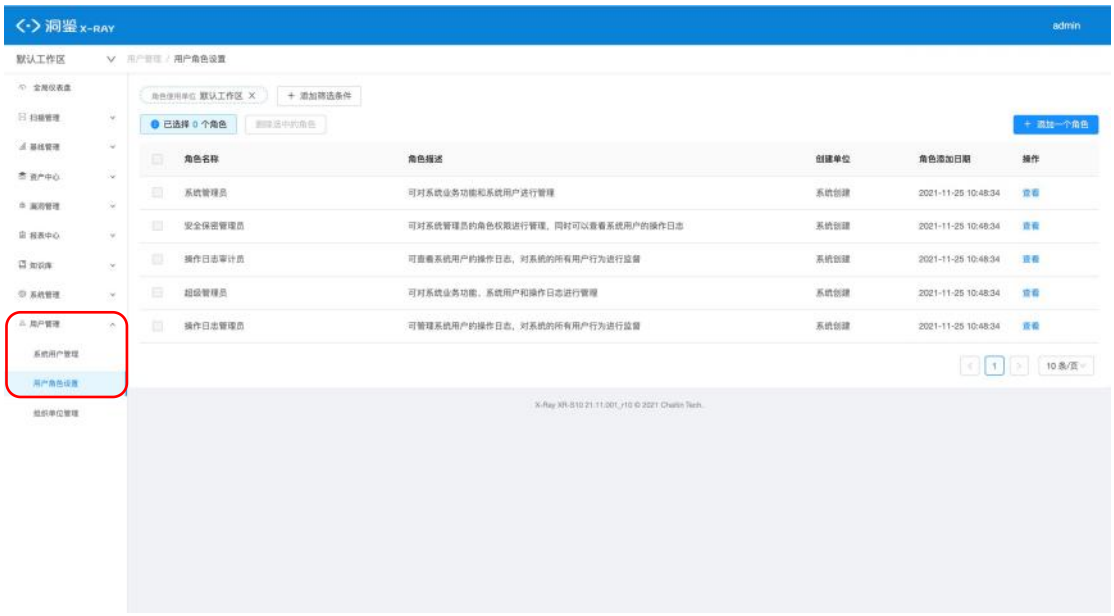


5.2 用户角色设置

主要定义登录系统的管理员角色，不同的角色可以设置不同的管理权限，只有安全保密管理员才可以对系统角色进行管理。

5.2.1 用户角色列表

在左侧导航栏中，选择“用户管理–用户角色设置”，进入用户角色设置界面。



5.2.1.1 内容展示

显示角色名称、角色描述、创建单位、角色添加日期：

- 其中系统管理员、安全保密管理员、操作日志审计员、超级管理员、操作日志管理员系统管理员、安全审计员是系统内置的管理员角色，不可被更改或删除：

  - 超级管理员：只包含一个 admin 账户，不可设置其他账户，不允许被删除，该账号只对其自己可见。可以增删改查系统用户和角色，可以查看导出删除日志，查看修改系统信息；
  - 系统管理员：管理操作系统业务功能，对系统用户进行管理。可以查看系统用户和角色，可以查看系统信息；
  - 安全保密管理员：对管理员角色进行管理，增删查改系统角色，对系统操作日志进行审查；
  - 操作日志审计员：查看系统用户操作日志；
  - 操作日志管理员：查看、导出、删除系统用户操作日志。

5.2.1.2 筛选用户角色

点击列表上方“添加筛选条件”，可根据角色名称，角色使用单位进行筛选。

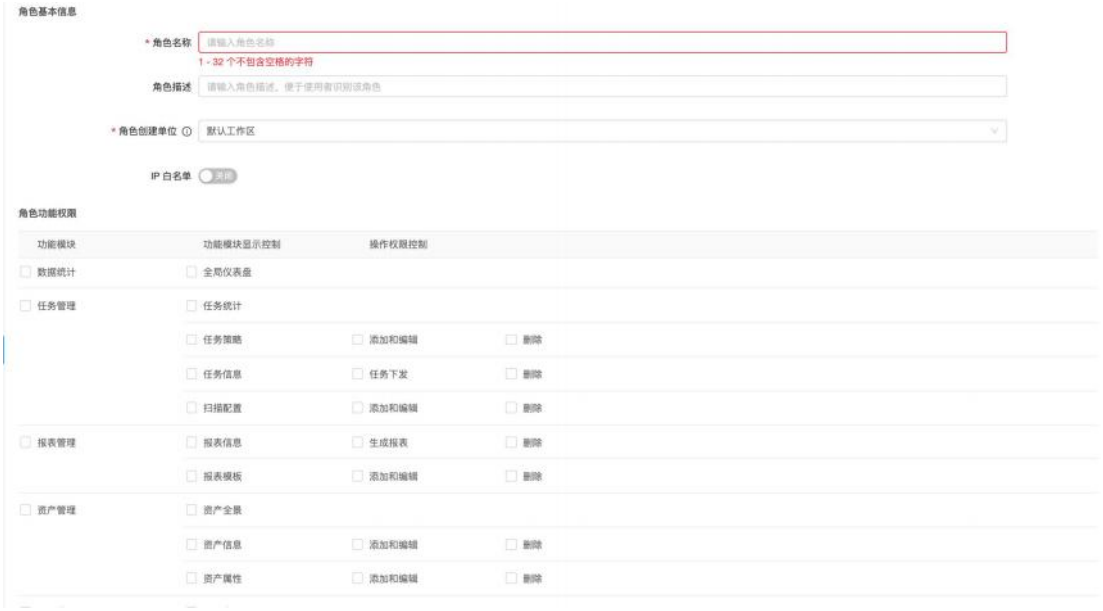
5.2.1.3 添加自定义管理员角色

安全保密管理员可以按需增加系统管理员角色，并赋予管理员角色权限

- 点击“添加一个角色”按钮，按照弹框提示一步步操作即可，分别填写相应内容
- 基本信息：
  - 角色名称：定义角色的名字，供管理员创建用户时选择；
  - 角色描述：对定义的管理员角色，进行简要说明。
- 操作权限设置：
  - 业务功能管理：可对系统的所有业务功能进行查看、操作、管理；
  - 用户管理：可对登录系统的用户进行管理。
- 访问权限设置（IP 白名单）：

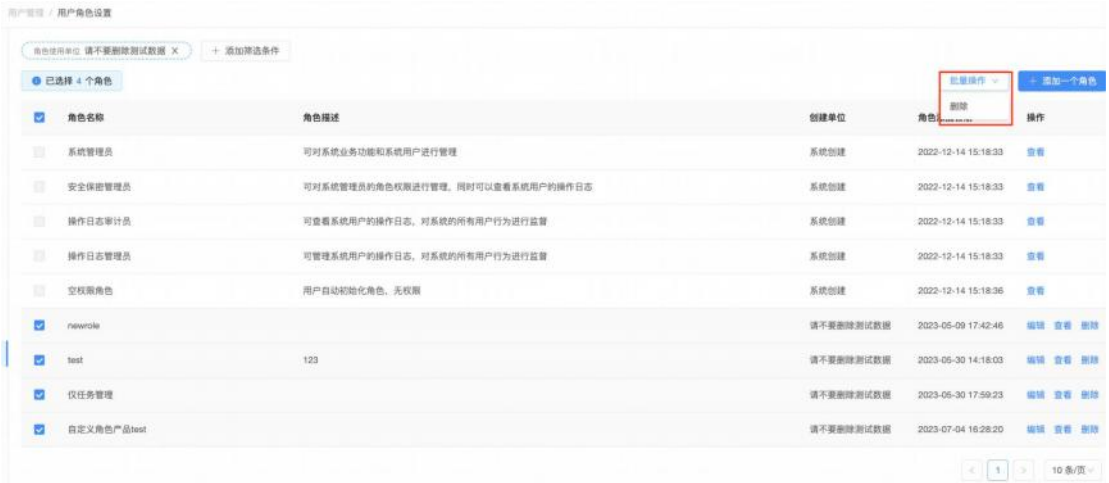
- 这里可以对允许角色登录的 IP 进行设置；
- 不设置默认不做任何限制；
- 填写了 IP 后，该角色只能在设置的 IP 下可以登录。

- 信息确认：
  - 查看前面填写的角色相关信息，确认无误时，点击“完成”即可成功创建角色。



5.2.1.4 删除管理员角色

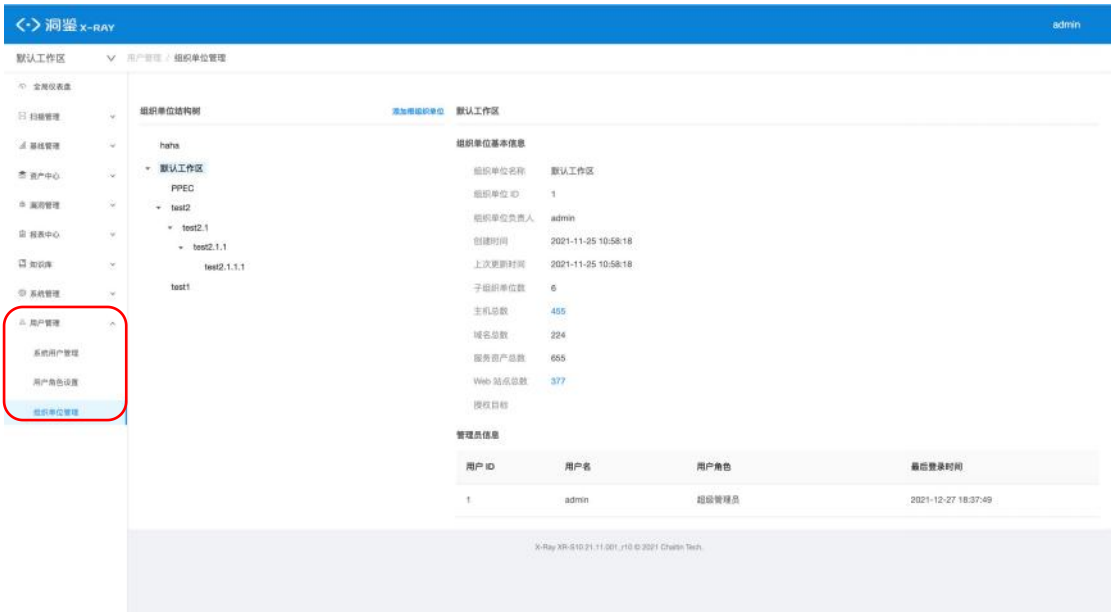
可以对自定义的管理员角色进行删除。



5.3 组织单位管理

此模块主要用于对系统中的资产或用户进行分区域的权限划分，用户可根据自身组织结构、办公区域等维度自由分配组织单位和各级账号间的权限关系

5.3.1 组织单位树



5.3.1.1 内容展示

组织单位管理页主要分为两个区，分别是左侧的组织单位结构树和右侧组织单位相关信息展示：

- 组织单位结构树：

- 包含用户可见的所有组织单位展示以及对应层级关系树
- 组织单位层级向下无上限，用户可根据实际情况自由创建

- 组织单位相关信息展示：

  - 展示组织单位的基本信息，包括以下字段：

    - 名称
    - ID
    - 负责人
    - 创建时间
    - 更新时间
    - 子组织单位统计
    - 主机总数
    - 域名总数
    - 服务资产总数
    - web 站点总数
    - 授权目标

  - 展示具备组织单位使用权限的用户列表，包括以下字段：

    - 用户 ID
    - 用户名
    - 用户角色
    - 最后登录时间

5.3.1.2 组织单位添加

添加根组织单位，点击“添加根组织单位”文字按钮，填写组织单位的相应参数：

- 组织单位名称
- 组织单位负责人
  - 默认为创建人，具备组织单位的编辑、删除等管理权限
- 组织单位管理员
  - 默认为负责人的所有上级管理，具备组织单位的查看权限
- 授权目标限制
  - 授权目标可控制用户可扫描的目标权限，为空时表示不限制
- 备注

5.3.1.3 添加子组织单位

对根组织单位或其他已存在组织单位可创建其子组织单位。通过组织单位结构树选中需要创建子组织单位的父级组织单位，点击“添加”按钮，填写相应参数即可创建子组织单位：

添加流程同 5.3.1.2 组织单位添加。

5.3.1.4 组织单位编辑

通过组织单位结构树，选中要编辑的组织单位，点击“编辑”按钮，变更相应参数即可：修改完毕后，点击“确认”，改动参数即生效 若点击取消或右上方的“×”，则改动不会生效。

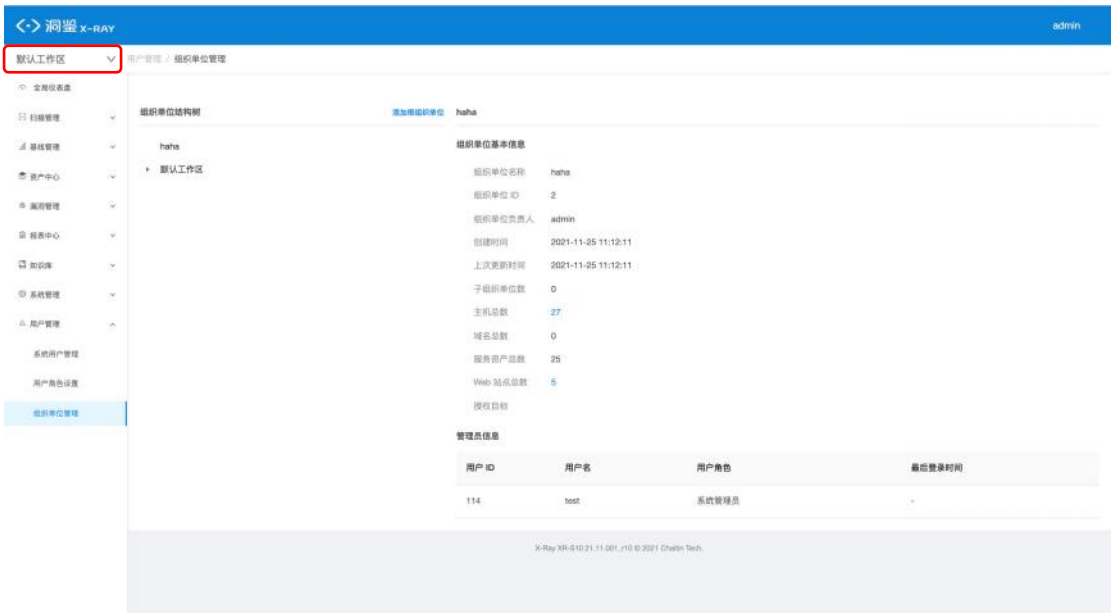
5.3.1.5 组织单位删除

说明：

删除正在被使用的组织单位会影响组织单位下的用户查看、操作对应资产、引擎等的权限，建议删除前仔细检查是否有绑定的用户和引擎，修改后再进行删除。

5.3.1.6 组织单位切换

在左侧的二级导航栏上会显示用户当前所处的组织单位维度，点击“下拉”按钮可选择用户可见的所有组织单位并切换视角：



说明：用户在不同组织单位下具备不同资产和引擎的查看或管理权限

5.3.1.7 组织单位视角数据查看

在组织单位基本信息中，点击主机总数、web 站点总数可切换至目标组织单位后，展示 对应资产列表：

六、个人中心模块

6.1 个人中心

点击界面的右上角用户名，出现下拉菜单，点击“个人中心”，即可进入个人中心页面。

个人中心页面主要展示当前用户的个人信息，包括个人基本信息、和登陆选项的设置。

6.1.1 个人基本信息

个人基本信息展示当前登陆用户的用户名、用户 ID 和创建时间。

- 用户名：创建当前用户时设置的用户名称
  - admin 用户为系统预设用户
- ID：创建当前用户时产生的唯一 ID
- 创建时间：创建当前用户的时间

6.1.2 登录选项

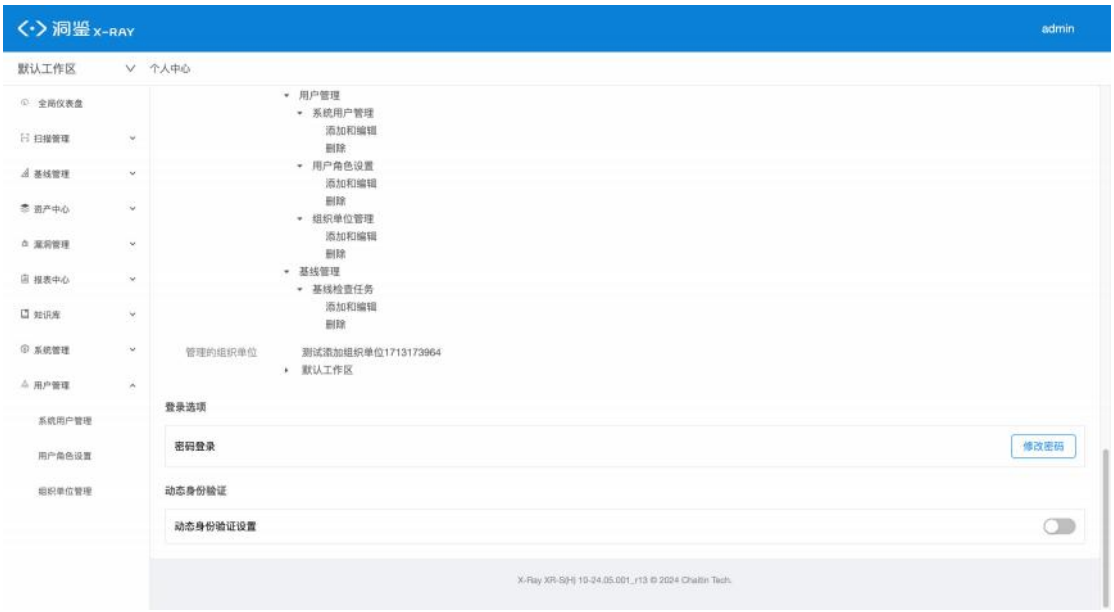
登陆选项展示当前用户的登陆设置。

若用户为密码登陆，在此处可以修改密码，具体操作为:

- 点击密码登陆右侧的 "修改密码" 按钮
- 弹出密码修改页面。用户输入当前密码、新密码和确认新密码
- 点击确认，系统提示 "密码修改成功"，跳转到登陆页面

6.1.3 动态身份验证

可以选择开启默认关闭的动态身份验证。



初次使用时候通过输入登录密码进入设置界面。可以使用手机APP（手机APP store或应用商城搜索“Auth”或者“动态身份验证”，如 Authy、OTP Auth、Google Authenticator）扫二维码添加私钥到手机认证应用。后每次通过密码登录后还需要查看认证 APP 并填写六位数动态验证码才能继续访问系统。

如想关闭动态身份验证设置，点击关闭并填写系统登录密码校验通过后关闭。

6.2 Open API

点击界面的右上角用户名，出现下拉菜单，点击“Open API”，即可进入 Open API 页面。

Open API 页面主要展示当前用户配置的 API。用户可以在此处查看、添加、编辑、删除自定义的 Open API。

6.2.1 Token 展示

汇总了用户的全部 Token，并且提供可以查看 Open API 文档的接口。

6.2.1.1 内容展示

展示当前用户添加的所有 Open API，次序从新到旧排列，如下图所示：

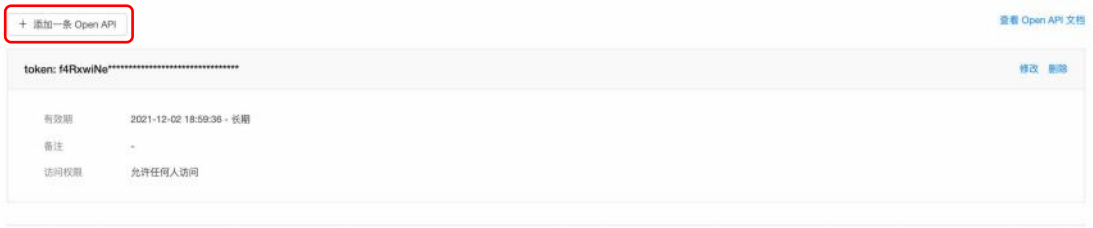
- 单个 Open API 展示信息包括：
  - token：Open API 的 token。Open API 添加后，将只展示 token 的前八位，其他位数加密处理
  - 有效：Open API 的有效期限。一个 Open API 的 toekn 只能在其有效期内才能使用。token 过期后即失效，界面上将高亮提示过期

- 备注：用户为 Open API 添加的备注。因 token 加密展示，添加合适的备注可以方便地使用户区分各个 Open API
- 访问权限：可访问该 Open API 的主机 IP 白名单。如果不设置访问权限，Open API 将允许任何人访问
- 可进行操作：用户可对 Open API 进行修改或删除的操作。详情可见下文修改和删除的说明

6.2.1.2 添加 Open API

可以在此界面添加多个 Open API，具体步骤为：

- 点击“ + 添加一条 Open API”按钮，显示配置相应信息的弹窗；



- 配置基本信息：
  - 过期时间，配置 Open API 的过期时间，有填写、选择两种设置方法：
    - 填写过期时间，时间格式为 yyyy-MM-dd HH:mm，例如:2018- 10-17 10:28；
    - 选择过期时间：
      - 点击输入框，在出现的下拉菜单中选择日期；
      - 点击“选择时间”，在出现的下拉菜单中选择时间。
  - 备注，可在此为 Open API 添加自定义的备注：
    - Open API 添加后，token 将加密展示，添加合适的备注可以方便用户区分各个 Open API。

- 点击“下一步”，配置访问权限：
  - 选择是否启用 IP 白名单：
    - 若禁用 IP 白名单，Open API 将没有访问限制，允许任何人访问；
    - 若启用 IP 白名单，需填写 IP 白名单：
      - 只有 IP 白名单上的 IP 方可访问该 Open API；
      - 多个 IP 间以换行分隔。

- 点击“下一步”，确认信息：
  - 在生成 token 前最后确认配置的过期时间、备注和访问权限是否无误。

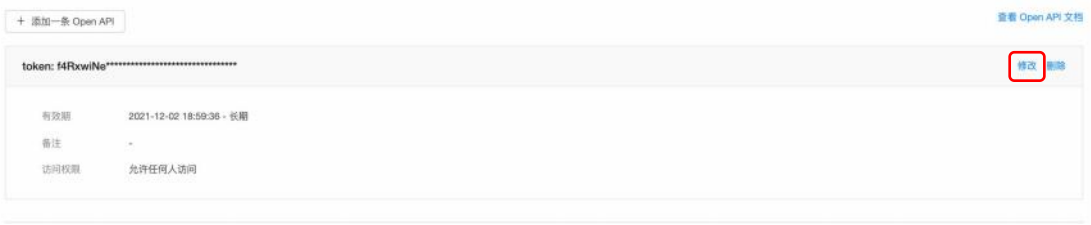
- 点击“完成”，Open API 生成成功，界面将展示 token 和配置信息：
  - 点击 token 旁的“复制”按钮可以一键复制 token；
  - 注意:token 只在此界面显示一次，界面关闭后，软件将再也不会显示 token。请务必在此页面复制好 token，并妥善保存。

- 点击“已完成复制保存，关闭当前页面”或弹窗右上角的关闭，关闭界面；
- 回到 Open API 界面，显示该 Open API 已添加，并展示在所有 Open API 的最上方。

6.2.1.3 修改 Open API

可在此界面修改已添加的 Open API，具体步骤为：

- 找到需要修改的 Open API，点击 Open API 右侧的“修改”：



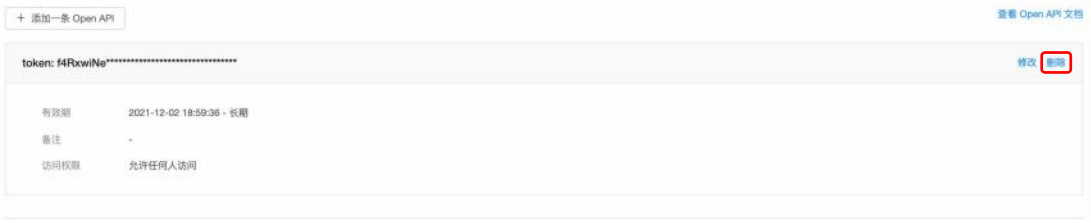
- 编辑需要修改的配置，编辑配置的方式与添加 API 时类似：
  - 过期时间，可编辑 Open API 的过期时间，有填写、选择两种编辑方法
    - 填写过期时间，时间格式为 yyyy-MM-dd HH:mm，例如:2018- 10-17 10:28
    - 选择过期时间
      - 点击输入框，在出现的下拉菜单中选择日期
      - 点击“选择时间”，在出现的下拉菜单中选择时间
  - 备注，可编辑 Open API 的备注
  - IP 白名单，可编辑访问权限配置
    - 若禁用 IP 白名单，Open API 将没有访问限制，允许任何人访问
    - 若启用 IP 白名单，填写或编辑已添加的 IP 白名单
      - 只有 IP 白名单上的 IP 方可访问该 Open API
      - 多个 IP 间以换行分隔

- 配置完所有信息后，点击“保存”
- Open API 修改成功，界面显示已修改的 Open API 信息

6.2.1.4 删除 Open API

可在此界面删除已添加的 Open API，具体步骤为：

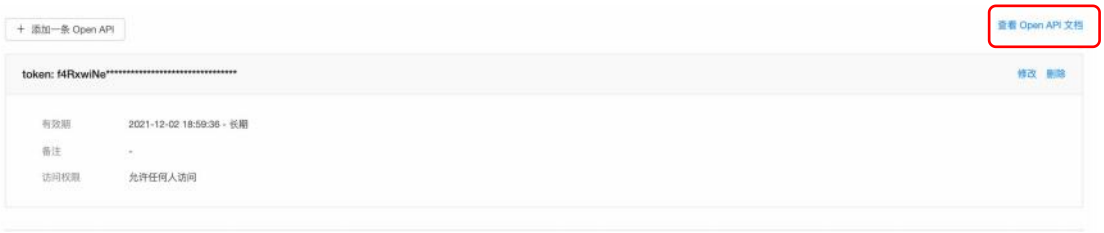
- 找到需要删除的 Open API，点击 Open API 右侧的“删除”：



- 在提示确认是否删除的弹窗中，点击“确认”；
- 成功删除 Open API 。

6.2.2 查看 Open API 文档

点击“查看 Open API 文档”按钮，可以跳转到 Open API 文档页面：



Open API 文档到具体使用方法请参考 Open API 文档。

6.3 登出系统

点击界面的右上角用户名，出现下拉菜单，点击“退出”，即可退出系统，跳转至登录界面。