瑞和云图
Safe in Cloud

云翼-脆弱性扫描与管理系统
用户手册

北京瑞和云图科技有限公司

www.rivercloud.com.cn

2020 年

目 录

版权申明

1 前言

瑞和云图-脆弱性扫描与管理系统（主机漏洞扫描），为客户提供对内网资产持续性的风险评估和检查手段。主要提供以下功能：

- 通过自动发现或录入资产，并为资产分组，系统化的管理资产。
- 为资产的不同分组执行主机漏洞扫描任务，涵盖主机操作系统、网络/安全设备、无线设备、虚拟化平台、应用系统、中间件、数据库等。
- 扫描任务可周期性的执行，定期扫描后，可得出资产漏洞风险的变化趋势。
- 将扫描结果生成报告并导出，以指导安全管理人员对系统脆弱性进行修补和加固。

本手册将按照操作执行顺序，逐一介绍各个功能的操作办法。

2 导入授权

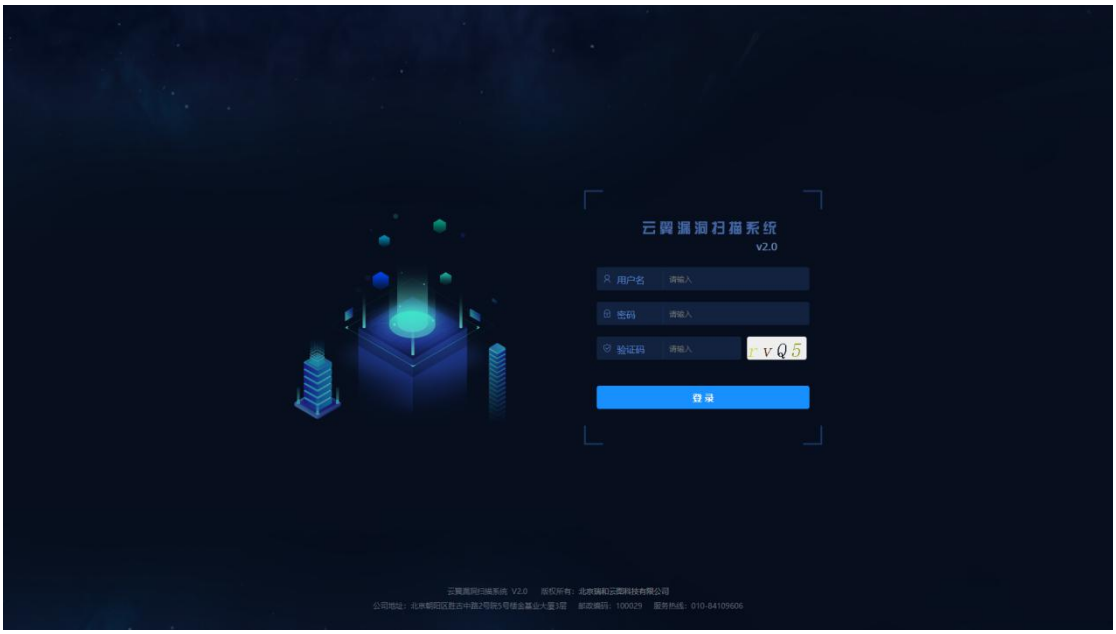
将本系统接入网络后，打开浏览器（建议使用 chrome、firefox 或 ie8 及以上版本），输入地址：https://ip（分配给漏洞扫描的管理 IP）即可访问系统。

第一次进入系统会提示缺少许可文件。

可将“授权号”或“二维码授权号”交给我方人员，通过授权号和项目需求，我方将生成许可文件。可通过点击“导入许可”按钮，选择许可文件导入，激活产品。

3 操作入门

3.1 用户登录



系统预置四个初始账号，对应四种角色。初始账号的用户名、密码、角色和权限如下表所示：

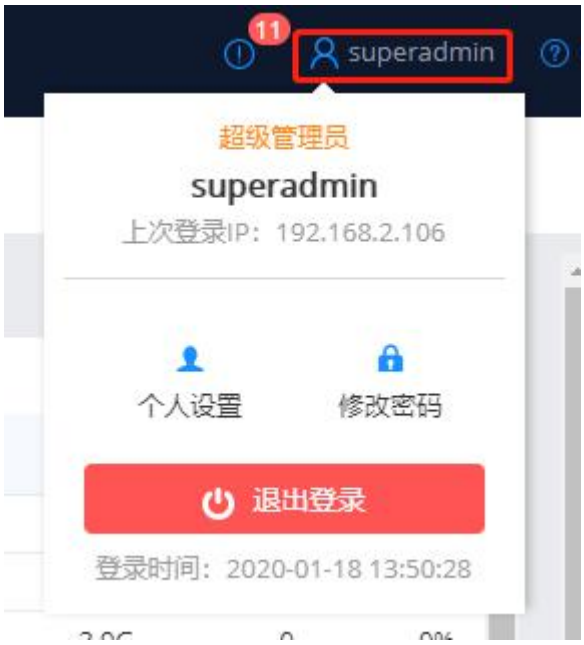
用户名	角色	权限描述	初始密码
admin	系统管理员	“系统管理”相关功能	admin123456
audit	审计管理员	“操作日志”、“系统日志”、“诊断工具”相关功能	audit123456
secret	安全保密管理员	除“系统管理”相关功能外，具备其他功能权限	secret123456
scan	操作员	是安全保密管理员的权限子集，不具备账号、角色管理功能	scan123456

3.2 预警提示

预警提示，显示所有未读的弱点。点击后可进入告警列表查看具体信息。

3.3 账号操作

鼠标悬浮在“账号”上方时，会弹出“账号信息”悬浮框。显示您的角色、账户名以及上次登录该账号的终端 IP 地址。以及三个可操作的功能按钮：“个人设置”、“修改密码”和“退出登录”。



- **个人设置**：点击个人设置后，弹出个人设置界面，可以补充/修改个人信息。修改好后，点击“保存”即可保存修改信息；点击“取消”则不保存修改记录。

- **修改密码**：点击修改密码后，可修改目前登录账号的密码。输入原密码和新密码（需要二次确认），点击“确定”，即可修改登录密码；点击“取消”则放弃此次操作。

- **退出登录**：点击退出登录，弹出确认框体。点击“确定”，则注销该账号的登录，回到登录界面；点击“取消”则放弃此次操作。

3.4 帮助信息

鼠标悬浮在“帮助信息”上方时，会弹出下拉框，包括两个可操作的功能按钮：“帮助文档”和“产品信息”。

- **帮助文档**：点击“帮助文档”按钮，弹出下载框，可下载用户手册。
- **产品信息**：点击“产品信息”按钮，弹出框显示目前产品的授权许可信息。

- 点击“更新许可”，可选择新的授权文件，导入至产品。
- 点击“关闭”或右上角“×”，可关闭该弹出框。

4 主要功能菜单

一级菜单包括：首页、资产管理、任务管理、等保合规、报表管理、模板管理、日志管理和系统管理。

4.1 首页

首页中主要展示系统自身的资源、可用性等统计信息，以及对漏洞扫描结果的统计性可视化信息。

4.1.1 系统信息

展示 CPU、内存的实时使用率，以及硬盘各分区的大小、已用和使用率信息。

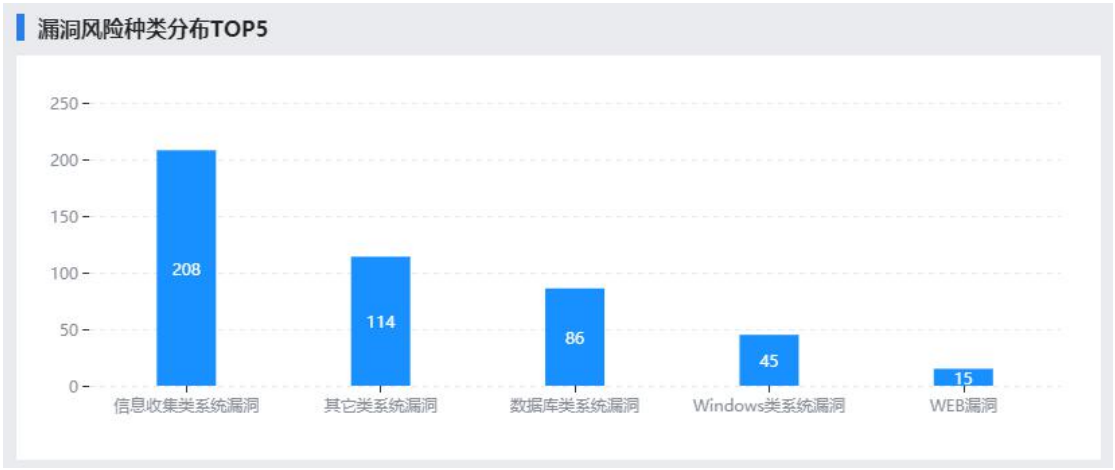
4.1.2 网卡信息

展示本系统的网口信息，如果挂接了多个扫描引擎，可以查看多个引擎的网卡信息。

- 点击“网卡管理”，可进一步查看网卡图例，双击图例，则进一步展示网卡的详细信息。

4.1.3 漏洞风险种类分布 Top5

将漏洞扫描任务中发现的漏洞类别，按发现数量进行排序，进行展示。



4.1.4 漏洞风险等级分布

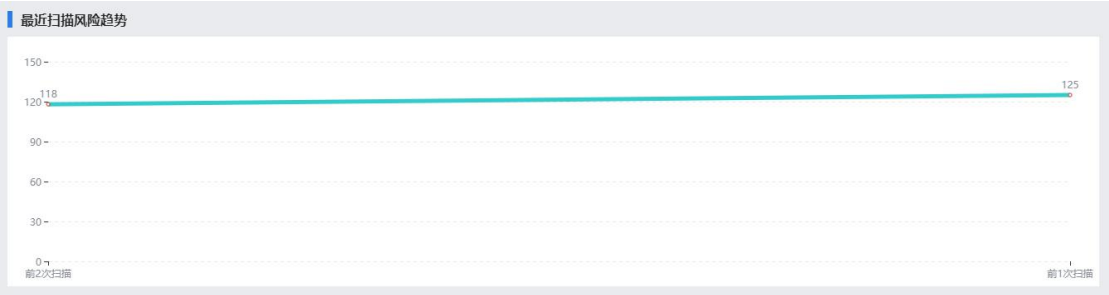
将所有扫描的漏洞，按照主机、网站以及高危、中危、低危、信息分为四个等级，并将其分布进行展示。

4.1.5 资产整体安全评分

对每个已扫描的资产都会有资产评分，将所有资产的评分进行加权平均（可为资产设定价值），得出整体安全评分。

4.1.6 最近扫描风险趋势

将最近 6 次扫描的结果按风险水平得出数值，并通过折线图展示出扫描风险趋势。



4.2 资产管理

在执行漏洞扫描工作之前，首先需要导入被扫描环境的资产。录入资产后，可以为资产定义价值，并持续的通过其他功能管理资产的脆弱性趋势。

资产管理包括的功能：资产分组管理和资产管理。

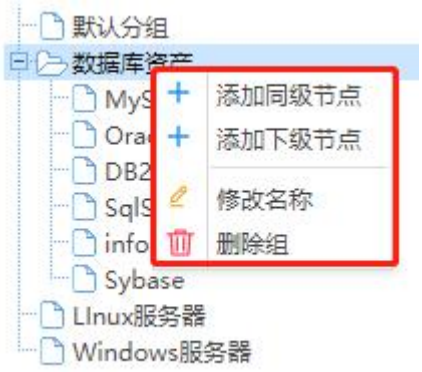
4.2.1 资产分组管理

本功能主要用于管理系统的所有资产组，以资产树的形式管理资产组，支持无限级的管理资产组。

用户可依据自身的资产管理习惯对资产进行分组，例如：

- ✓ 按照资产所属部门进行分组
- ✓ 按照资产的业务属性分组（如数据库、网站、办公终端等）
- ✓ 按照资产的技术属性分组（如 Linux 服务器、Windows 服务器等）
- ✓ 按照安全域分组（依据安全域和业务系统的划分，对资产分组）

- **资产分组操作说明：**右键点击分组，弹出菜单，包含“添加同级节点”、“添加下级节点”、“修改名称”和“删除组”功能。



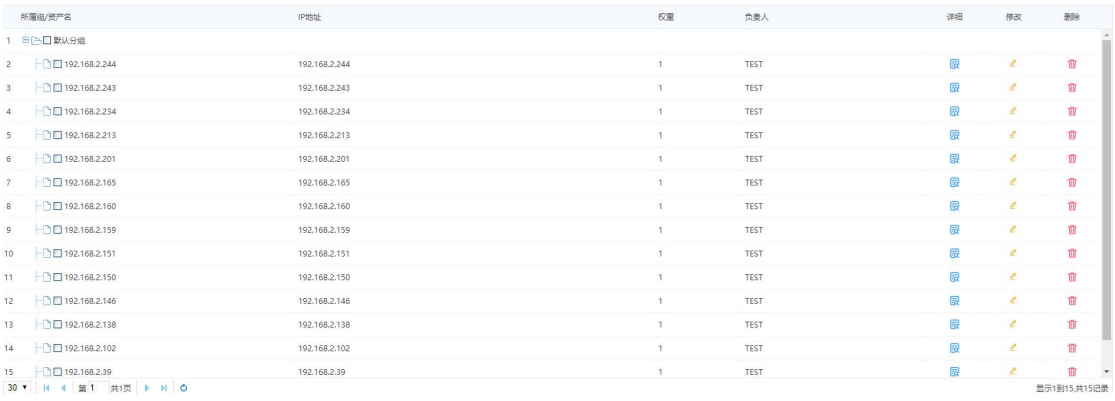
  - **添加同级节点：**可添加平行的分组。
  - **添加下级节点：**可添加归属于目前分组的子分组。
  - **修改名称：**修改当前所选分组的名称。注意：默认分组不可修改名称。
  - **删除组：**删除当前所选分组。注意：默认分组不可删除。

4.2.2 资产管理

本功能主要用于对资产的增删改查等操作，同时也提供快速入口，对资产/

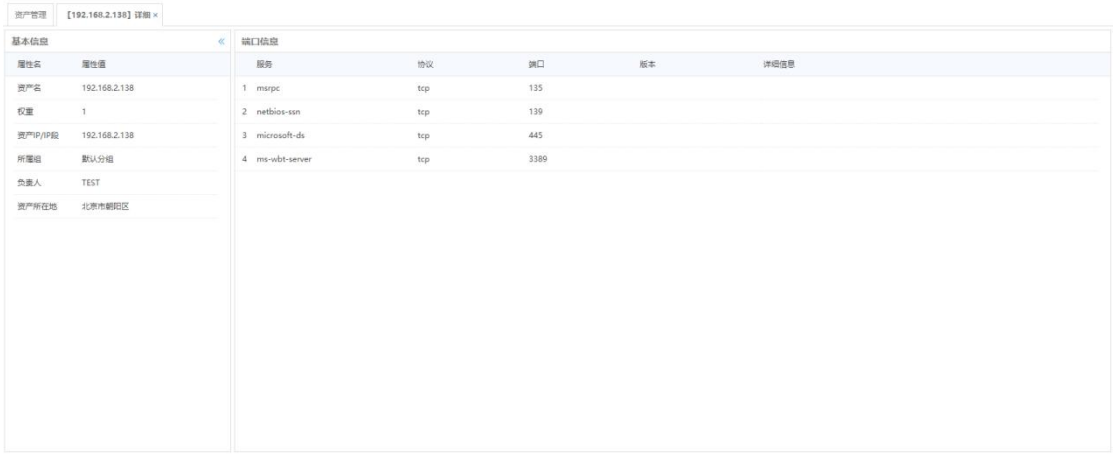
资产组执行漏洞扫描任务。

4.2.2.1 资产列表



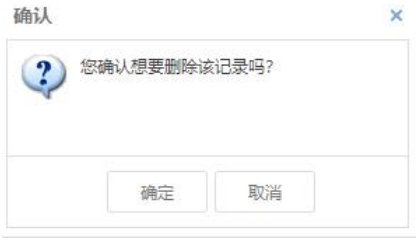
以列表形式，按照资产分组树状形式，展示当前索引条件匹配的所有资产。

- **勾选资产**：点击资产/资产分组左侧的勾选框，可以选中资产。可对勾选的资产执行批量操作（导出资产/风险扫描）。
- **查看详情**：点击，新建一个资产详情页签，可在页签中查看资产的详情。



- **修改资产信息**：点击，弹出资产的详细字段，并可对资产的全字段进行修改。修改后，点击“确定”则保存修改记录；点击“取消”则放弃本次操作。

- **删除资产**：点击🗑，弹出确认框。点击“确认”，可删除该资产（不可恢复，只能重新添加）；点击“取消”，则取消删除操作。



4.2.2.2 资产查询

可通过多条件组合进行资产的查询，页面会根据查询条件显示对应的资产。

- 可通过以下条件检索资产：
  - 资产 IP
  - 资产负责人
  - 资产分组
- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.2.2.3 资产添加

可手动添加资产，通过 Excel 表导入资产，或将资产导出为 Excel 表。

- 点击“添加”按钮，可手动添加资产。弹出添加资产的文本框，填写必要字段，点击“确定”可添加资产；点击“取消”可取消本流程。

- **资产名（必填）**：为资产命名；
- **权重（选填）**：对重要资产，可通过权重描述资产的价值，权重为 1-10（正整数），默认为 1。
- **资产 IP/IP 段（必填）**：支持 IPv4/IPv6 格式，支持添加单个 IP，也支持添加 IP 段。
- **所属组（必填）**：可选择需要添加的资产所属的资产分组。
- **负责人（选填）**：可填写资产的负责人（一般为资产的所属部门的领导）。
- **资产所在地（必填）**：通过下拉框，选择资产的所在地。

- 点击“导出资产”按钮，可将所选的资产以 Excel 表的形式导出并下载。
- 鼠标悬浮于“导入资产”按钮时，弹出下拉框，可选择“从 XLSX 导入”和“下载模板”。
  - **下载模板：**在导入资产之前，需要先下载资产模板，通过在模板 Excel 文件中录入资产后，再执行导入。
  - **从 XLSX 导入：**可将录入好资产的 XLSX 文件拖入弹出框进行上传，或点击弹出框显示文件浏览器选择文件进行上传。

4.2.2.4 执行风险扫描

可以从资产管理页面直接勾选资产，执行漏洞扫描任务。

- 勾选需要进行漏洞扫描的资产后，点击 风险扫描 按钮，继续选择“主机扫描”，即可弹出建立扫描任务的文本框。在选择好扫描各个参数后，即可开始扫描过程。

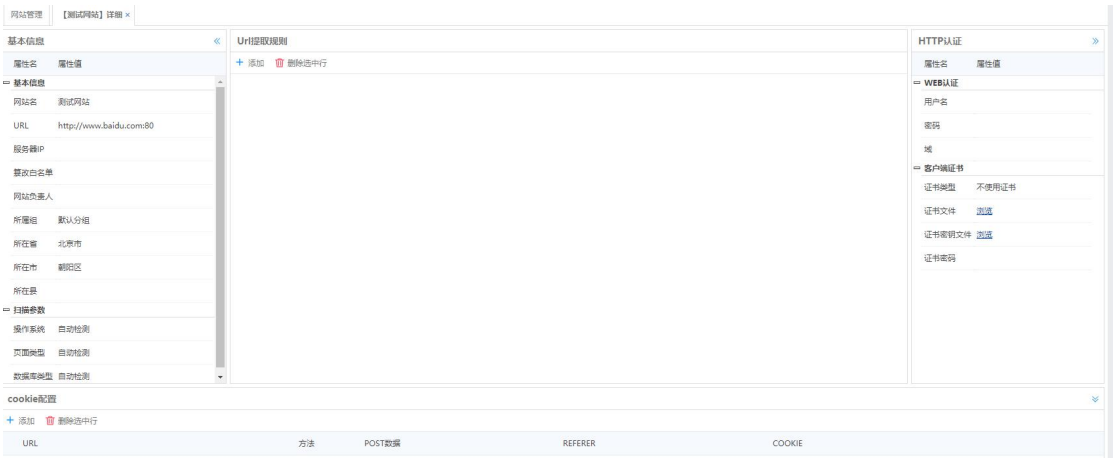
4.2.3 网站管理

对于一些周期性需要执行网站扫描的网站资产，我们可以在此处添加，在扫描的时候就可以直接从资产里面选择这些网站。

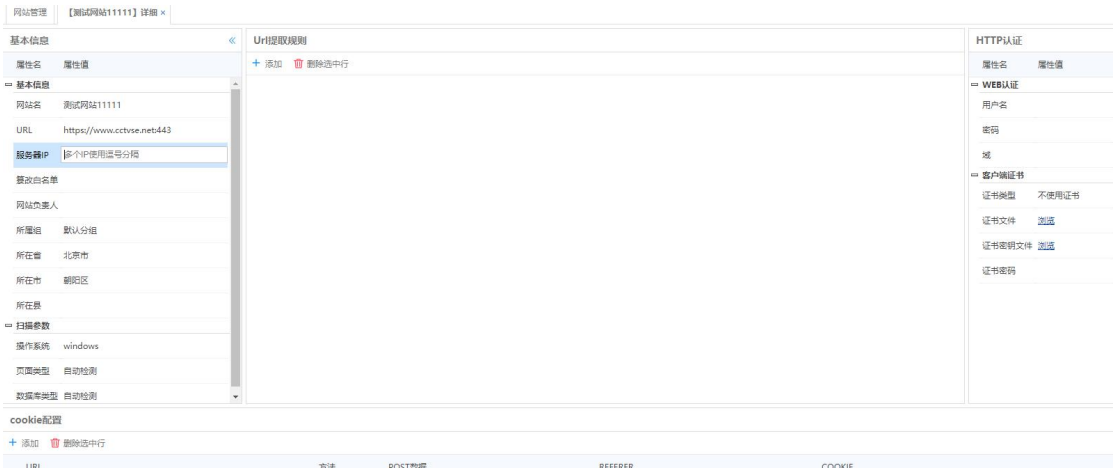
4.2.3.1 资产列表

以列表形式，按照资产分组树状形式，展示当前索引条件匹配的所有资产。

- **勾选资产**：点击资产/资产分组左侧的勾选框，可以选中资产。可对勾选的资产执行批量操作（导出资产/风险扫描）。
- **查看详情**：点击 ，新建一个资产详情页签，可在页签中查看资产的详情。



- **修改资产信息**：点击 ，弹出资产的详细页，这里可对资产的全字段进行修改。修改后，刷新页面变更生效。



- **删除资产**：点击🗑，弹出确认框。点击“确认”，可删除该资产（不可恢复，只能重新添加）；点击“取消”，则取消删除操作。

4.2.3.2 资产查询

可通过多条件组合进行资产的查询，页面会根据查询条件显示对应的资产。

- 可通过以下条件检索资产：
  - 网站名
  - 资产负责人
- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.2.3.3 资产添加

可手动添加资产，通过 Excel 表导入资产，或将资产导出为 Excel 表。

- 点击“添加”按钮，可手动添加资产。弹出添加资产的文本框，填写必要字段，点击“确定”可添加资产；点击“取消”可取消本流程。

  - **网站名（必填）**：为网站资产命名；
  - **URL（必填）**：填写网站资产的 URL。
  - **所属组（必填）**：可选择需要添加的资产所属的资产分组。
  - **负责人（选填）**：可填写资产的负责人（一般为资产的所属部门的领导）。
  - **资产所在地（必填）**：通过下拉框，选择资产的所在地。

- 点击“导出资产网站”按钮，可将所选的资产以 Excel 表的形式导出并

下载。

- 鼠标悬浮于“导入网站”按钮时，弹出下拉框，可选择“从 XLSX 导入”和“下载模板”。
  - **下载模板：**在导入资产之前，需要先下载资产模板，通过在模板 Excel 文件中录入资产后，再执行导入。
  - **从 XLSX 导入：**可将录入好资产的 XLSX 文件拖入弹出框进行上传，或点击弹出框显示文件浏览器选择文件进行上传。

4.2.3.4 执行风险扫描

可以从资产管理页面直接勾选资产，执行漏洞扫描任务。

- 勾选需要进行漏洞扫描的资产后，点击 风险扫描 按钮，继续选择“网站扫描”，即可弹出建立扫描任务的文本框。在选择好扫描各个参数后，即可开始扫描过程。

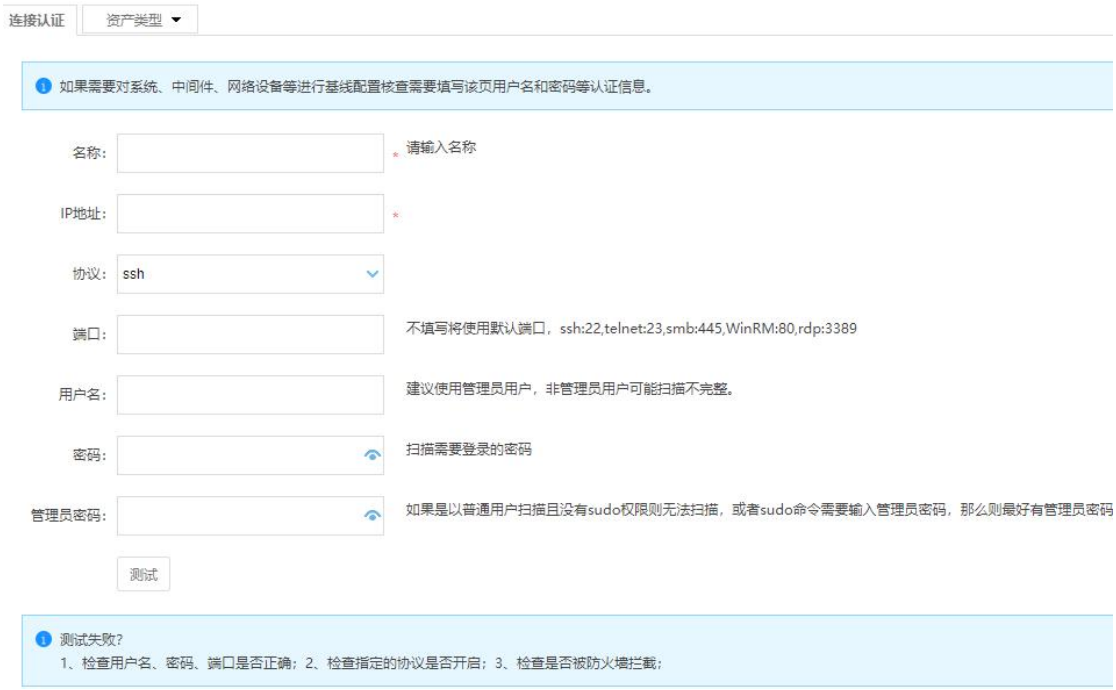
4.2.4 认证信息

在进行基线核查时，需要登录目标设备进行检查。这时需要用到目标设备的用户登录信息，这些信息需要预先存储于认证信息。

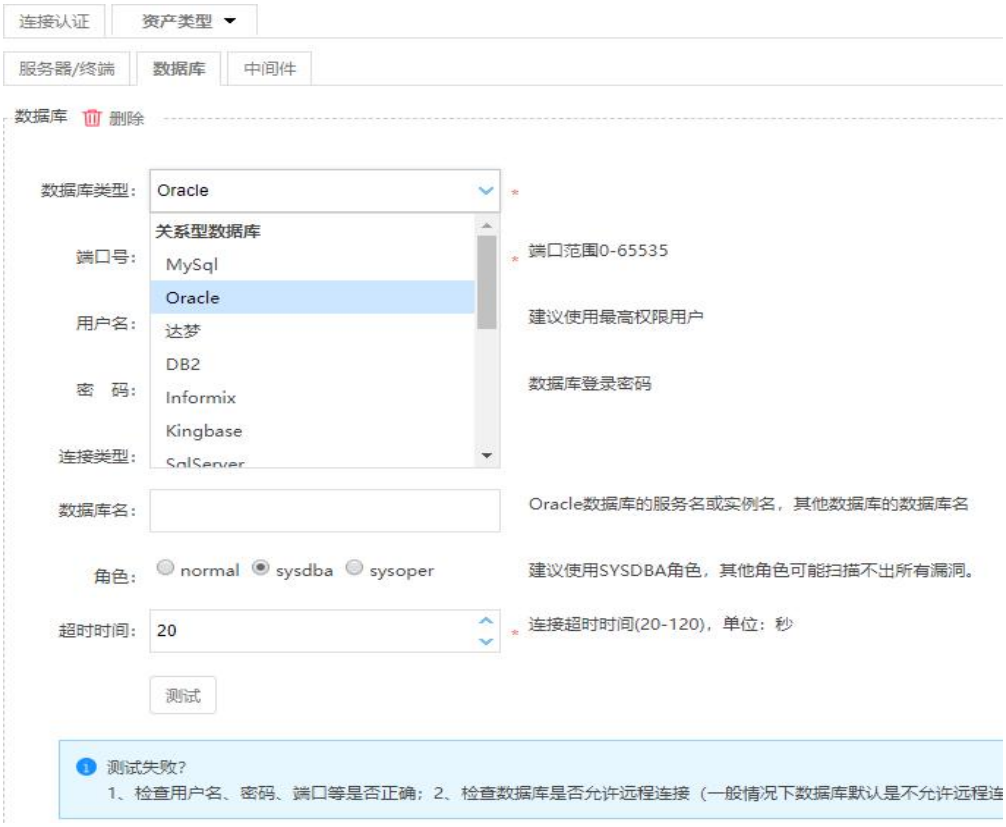
4.2.4.1 添加认证信息

在认证信息页面，点击“添加”按钮。

在弹出的页面中填写准确的认证信息。

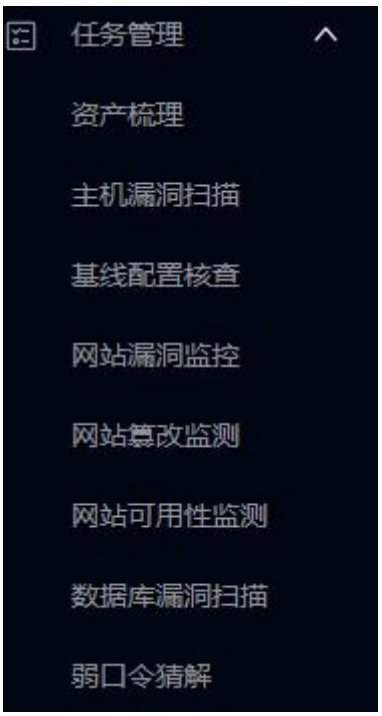


如果只进行系统基线核查，那么配置好上图即可。如果要使用数据库漏洞扫描或者中间件的基线扫描，那么还需配置资产类型。



4.3 任务管理

任务管理提供资产梳理功能（即资产自动发现和探测功能）、主机漏洞、基线核查、弱口令猜解和网站漏洞扫描功能。



4.3.1 资产梳理

资产梳理功能提供资产的自动发现和探测功能，可通过资产梳理功能对内网资产进行自动化的探测，并导入资产列表中，再通过人工修正的方式将资产信息补全。

4.3.1.1 添加资产梳理任务

点击 + 添加 可新建资产梳理任务，输入相应的扫描参数后，即可开始资产发现过程。

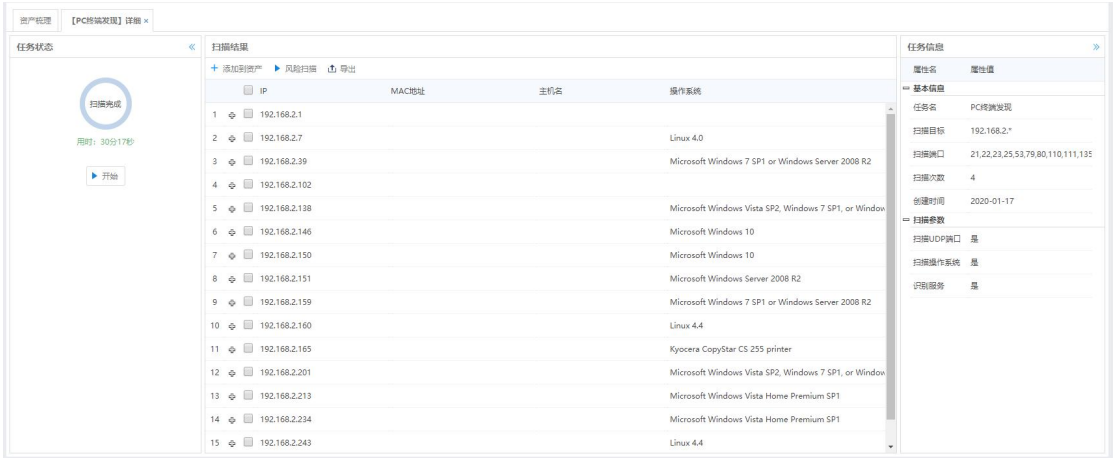
- **任务名（必填）**：输入并命名资产梳理任务；
- **目标引擎（选填）**：可选择自动分配，或选择具体引擎（如存在分布式多引擎部署方式）。建议选择自动即可。
- **探测目标（必填）**：输入需要扫描的网络分段（支持添加 C 段地址）。
- **探测端口（必填）**：可选择多种端口组合方式（建议选择第一项）。
- **扫描参数（选填）**：可选择扫描 UDP、扫描操作系统、识别服务。

点击确定后，即生成一个资产梳理任务记录，可继续选择启动任务执行资产的自动发现和探测。

4.3.1.2 资产梳理任务列表

以列表形式展示所有的资产梳理任务。可对每个资产梳理任务执行：

- **导出结果**：可将资产梳理任务的结果进行导出，以 Excel 形式导出并下载。
- **启/停**：可通过点击▶/■，来开启资产梳理任务或停止任务。
- **详细**：在表格的“详细”列中点击查看资产梳理任务的详情，可在此页面查看扫描结果，并将发现的资产导入至资产管理/导出为 Excel 表/执行主机扫描任务。



- **勾选任务**：点击每个任务左侧的勾选框，可以选中任务。可对勾选的任务执行批量操作（批量删除）。
- **删除任务**：可点击，弹出确认框，点击确认后删除任务。

4.3.2 主机漏洞扫描

主机漏洞扫描功能模块，是执行漏洞扫描任务，查看任务结果的主要工作页面。

4.3.2.1 添加主机扫描任务

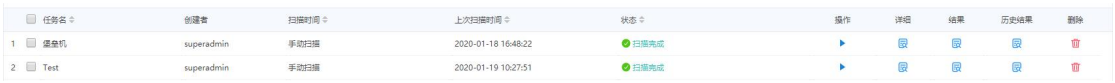
点击页面左上角“添加”，可以在新建的“添加扫描任务”页签中填写扫描任务信息，创建主机扫描任务。

- **任务名（必填）**：命名主机扫描任务（20 字以内）。
- **目标引擎（选填）**：选择任务下发执行的目标引擎，可以选择自动（推荐）或选择具体的引擎（如果是分布式多引擎部署形式）。
- **描述（选填）**：描述任务。
- **资产 IP（必填）**：可手动输入需要扫描的资产的 IP/IP 段，支持多行输入；也可以从“资产管理”中选择已导入的资产。
- **排除 IP（选填）**：可输入一些不扫描的 IP 地址。
- **扫描顺序（选填）**：包括顺序（默认）、逆序和随机顺序。
- **主机扫描模板（必填）**：可选择预置的完全扫描、标准扫描和快速扫描，或者可选择自定义的扫描模板。
- **扫描类型**：可选择手动扫描或周期扫描，手动扫描任务的执行需要人工

启动，周期扫描任务可以按小时、按日、按周、按月执行扫描。

- **预警方式：**提供三种预警方式：
  1. 系统提示：勾选后，将在界面右上角的“预警提示”处提示告警；若不勾选，则系统将不对扫描结果进行告警（即不会出现在“告警日志”中）；
  2. 邮件预警：需要设置邮件服务器地址，勾选后，可输入需要得到扫描结果的邮箱地址；
  3. 短信预警：需要设置短信平台地址，勾选后，可将扫描结果统计概要通过短信发送给指定的手机。
- **预警时间：**可即时发送预警（扫描完后即时报警），也可定时发送预警（可设置每日告警时间）。

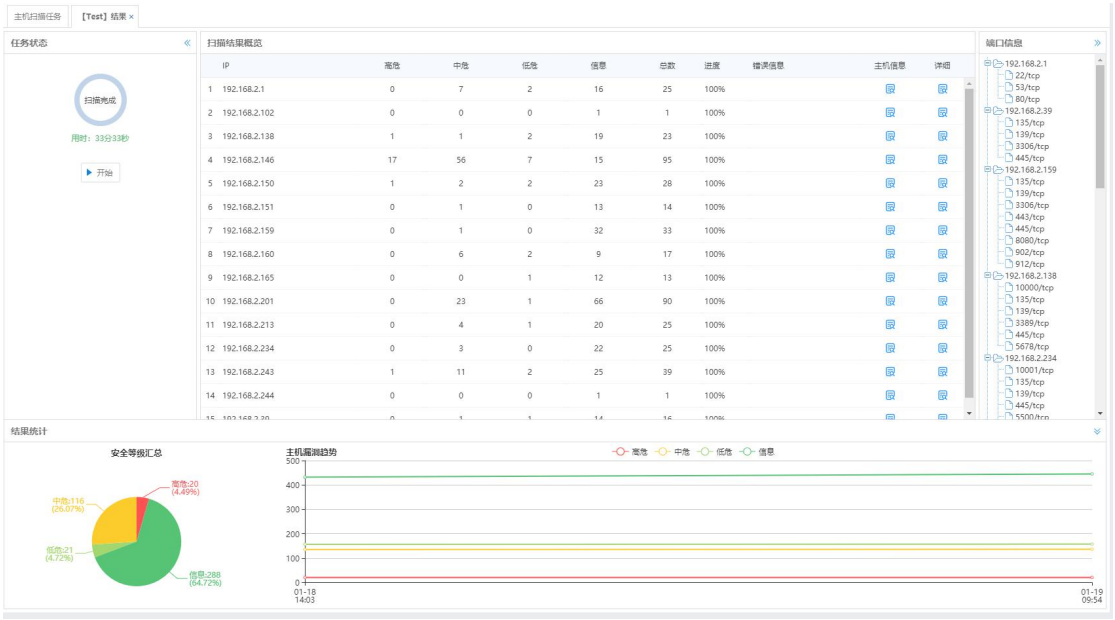
4.3.2.2 主机扫描任务列表



以列表形式展示所有的主机扫描任务。可对每个主机扫描任务执行：

- **启/停：**可通过点击▶/■，来开启资产梳理任务或停止任务。
- **查看任务参数详细：**可点击“详细”列的查看主机扫描任务的任务参数详情。

- **查看扫描任务结果：**可点击“结果”列的查看任务结果详情。

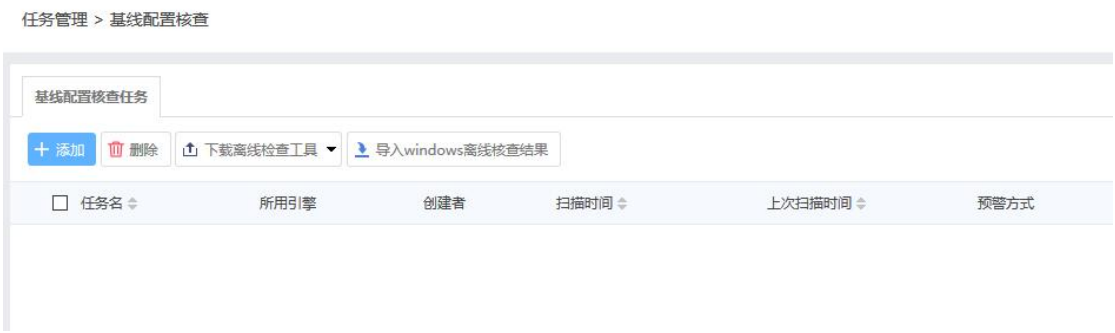


- **查看历史结果：**如果一个任务执行了多于一次，则可点击“历史结果”列的查看历史任务结果的统计信息。

- **勾选任务**：点击每个任务左侧的勾选框，可以选中任务。可对勾选的任务执行批量操作（批量删除）。
- **删除任务**：可点击“删除”列的，弹出确认框，点击确认后删除单个任务。
- **批量删除任务**：如果勾选了多个任务，可点击列表左上方的，并在确认框中确认，从而删除批量任务。

4.3.3 基线配置核查

该模块主要用于管理平台所建的基线扫描任务。以列表的方式显示任务名称、扫描类型、预警方式、告警类型、任务状态等信息。



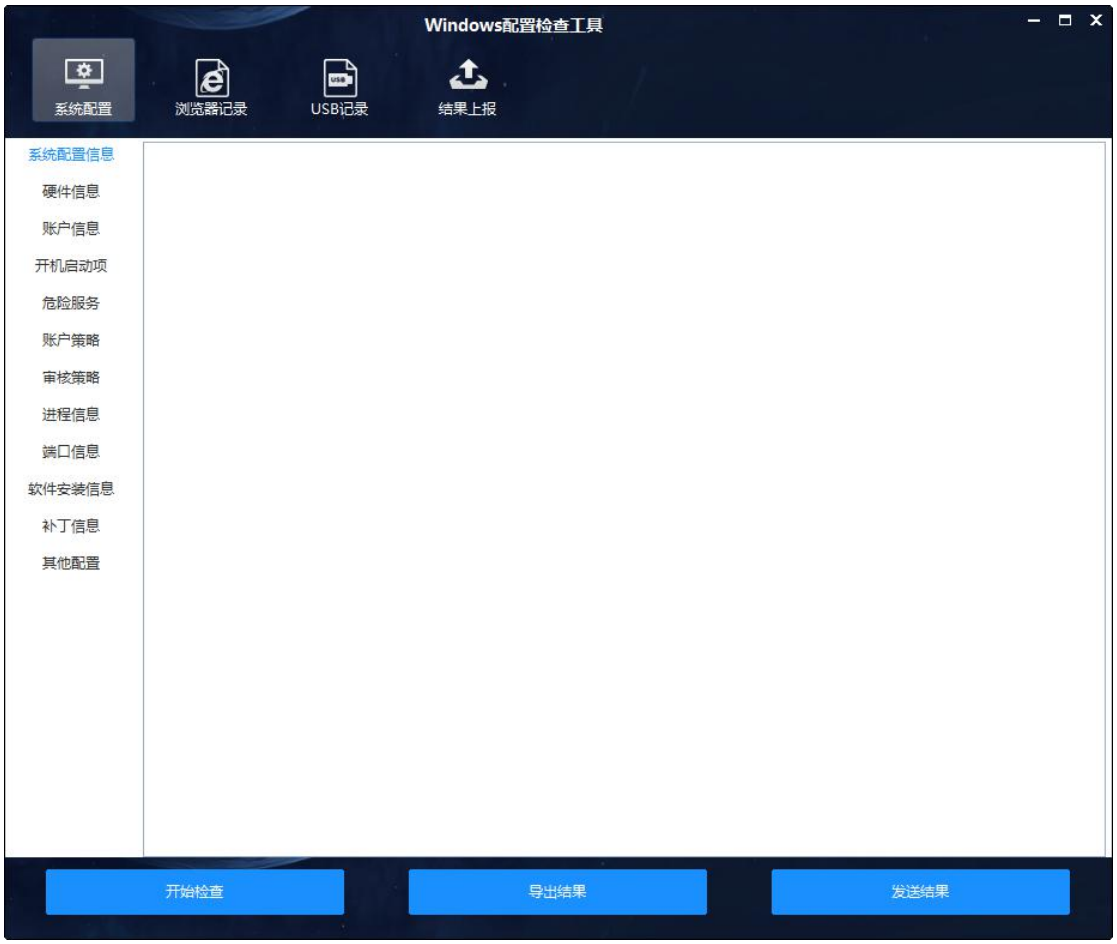
- **点击 添加 按钮，输入信息，即可添加扫描任务；**

- **点击** 

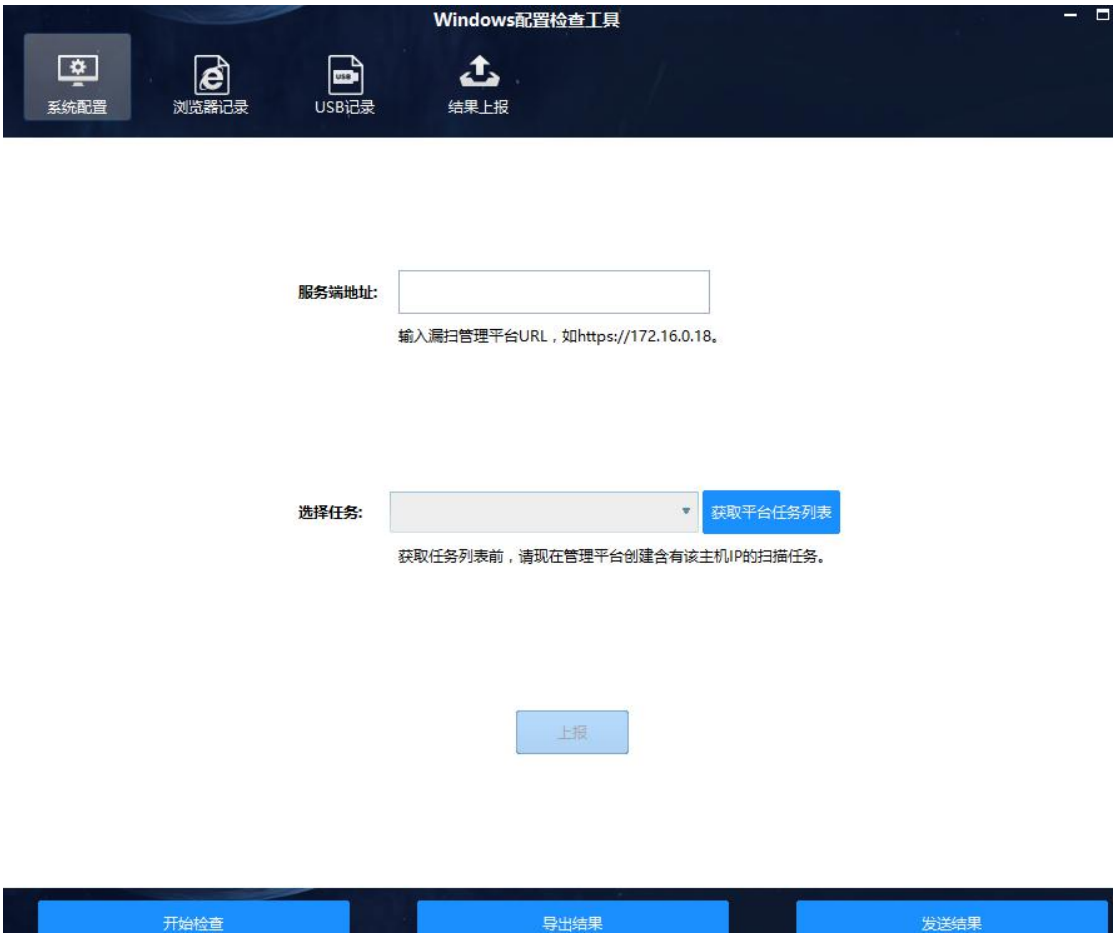
按钮，选择文件，即可上报离线扫描结果；

- **点击** 

按钮，即可下载 Windows 离线检查工具（Windows 离线检查工具即检查本机的配置核查）



点击“开始扫描”即可扫描本机的配置，扫描完成后可“自动上报”也可“导出结果”。自动上报：输入服务端地址和选择任务即可上报。



4.3.4 网站漏洞监控

网站漏洞监控功能模块，是执行漏洞扫描任务，查看任务结果的主要工作页面。

4.3.4.1 添加网站漏洞扫描任务

点击页面左上角“添加”，可以在新建的“添加扫描任务”页签中填写扫描

任 务 信 息 ， 创 建 主 机 扫 描 任 务 。

- **任务名（必填）**：命名主机扫描任务（20 字以内）。
- **目标引擎（选填）**：选择任务下发执行的目标引擎，可以选择自动（推荐）或选择具体的引擎（如果是分布式多引擎部署形式）。
- **描述（选填）**：描述任务。
- **URL（必填）**：可手动输入需要扫描的资产的 IP/IP 段，支持多行输入；也可以从“网站库”中选择已有的资产。
- **扫描类型**：可选择手动扫描或周期扫描，手动扫描任务的执行需要人工启动，周期扫描任务可以按小时、按日、按周、按月执行扫描。
- **扫描内容**：使用默认选项即可。
- **预警方式**：提供三种预警方式：

4. 系统提示：勾选后，将在界面右上角的“预警提示”处提示告警；

若不勾选，则系统将不对扫描结果进行告警（即不会出现在“告警日志”中）；

5. 邮件预警：需要设置邮件服务器地址，勾选后，可输入需要得到扫描结果的邮箱地址；
6. 短信预警：需要设置短信平台地址，勾选后，可将扫描结果统计概要通过短信发送给指定的手机。

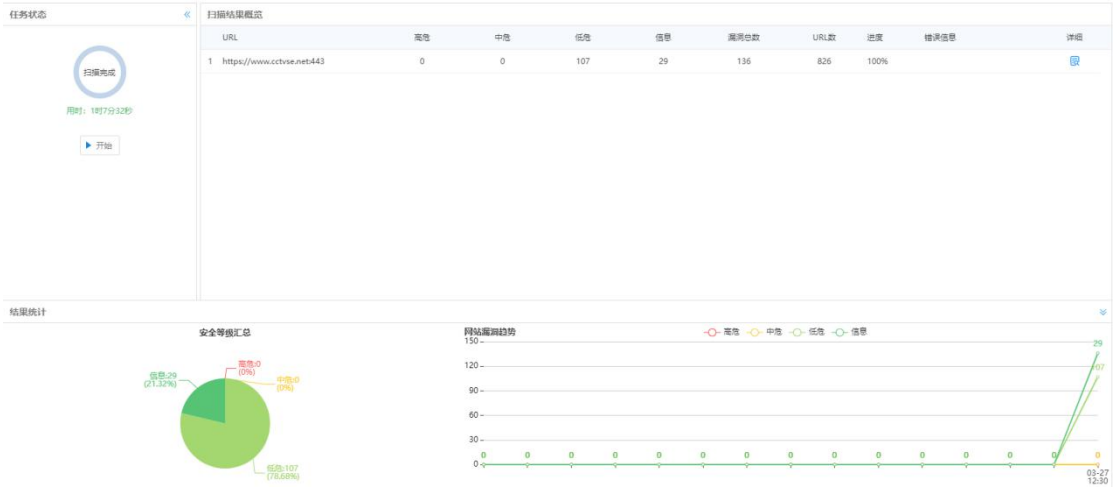
- **预警时间：**可即时发送预警（扫描完后即时报警），也可定时发送预警（可设置每日告警时间）。
- **基本配置：**扫描策略模板推荐选择所有策略。

4.3.4.2 网站扫描任务列表

以列表形式展示所有的主机扫描任务。可对每个主机扫描任务执行：

- **启/停：**可通过点击▶/■，来开启网站扫描任务或停止任务。
- **查看任务参数详细：**可点击“详细”列的查看主机扫描任务的任务参数详情。

- **查看扫描任务结果：**可点击“结果”列的查看任务结果详情。



再次点击详细，可进入该网站的安全漏洞详情页面，可对该网站的结构、安全漏洞情况、此次扫描新发现的漏洞和已修复漏洞进行查看。

点击漏洞右侧的  按钮，可对此漏洞进行 PoC。

- **查看历史结果：**如果一个任务执行了多于一次，则可点击“历史结果”列的查看历史任务结果的统计信息。

- **勾选任务：**点击每个任务左侧的勾选框，可以选中任务。可对勾选的任务执行批量操作（批量删除）。
- **删除任务：**可点击“删除”列的，弹出确认框，点击确认后删除单个任务。

- **批量删除任务**：如果勾选了多个任务，可点击列表左上方的删除，并在确认框中确认，从而删除批量任务。

4.3.5 网站可用性监测

该模块主要用于管理平台所建的网站可用性监测任务。网站可用性监测主要对目标网站的可用性进行 7*24 小时监控。

4.3.6 网站篡改监测

该模块主要用于管理平台所建的网站篡改监测任务。网站篡改监测主要对目标网站的篡改性进行 7*24 小时监控，包括：内容篡改、图片篡改、新增 URL、删

除 URL。

- **任务信息：**

包含任务的基础信息，如扫描目标、扫描内容、手动扫描或者周期扫描等；

- **预警配置：**

配置发现篡改后如何进行预警，包含预警时间、预警方式等；

- **爬行参数：**

爬虫对网站进行爬行的一些参数设置；

- **代理设置：**

主要争对某些网站直接无法访问时，可通过代理进行访问；

➢ **预处理规则：**

对网站进行篡改对比前，需要对网站的内容先进行预处理，例如：某个页面有时间，每次访问该页面时，显示的时间都不同，这样的页面如果直接进行篡改对比，每次都会提示有篡改，争对这样页面，可以先将页面的时间过滤后再进行对比。还有留言板等页面，由于页面不停有用户在进行留言，篡改对比前也需要先将留言内容过滤后再进行对比。

4.3.7 数据库扫描

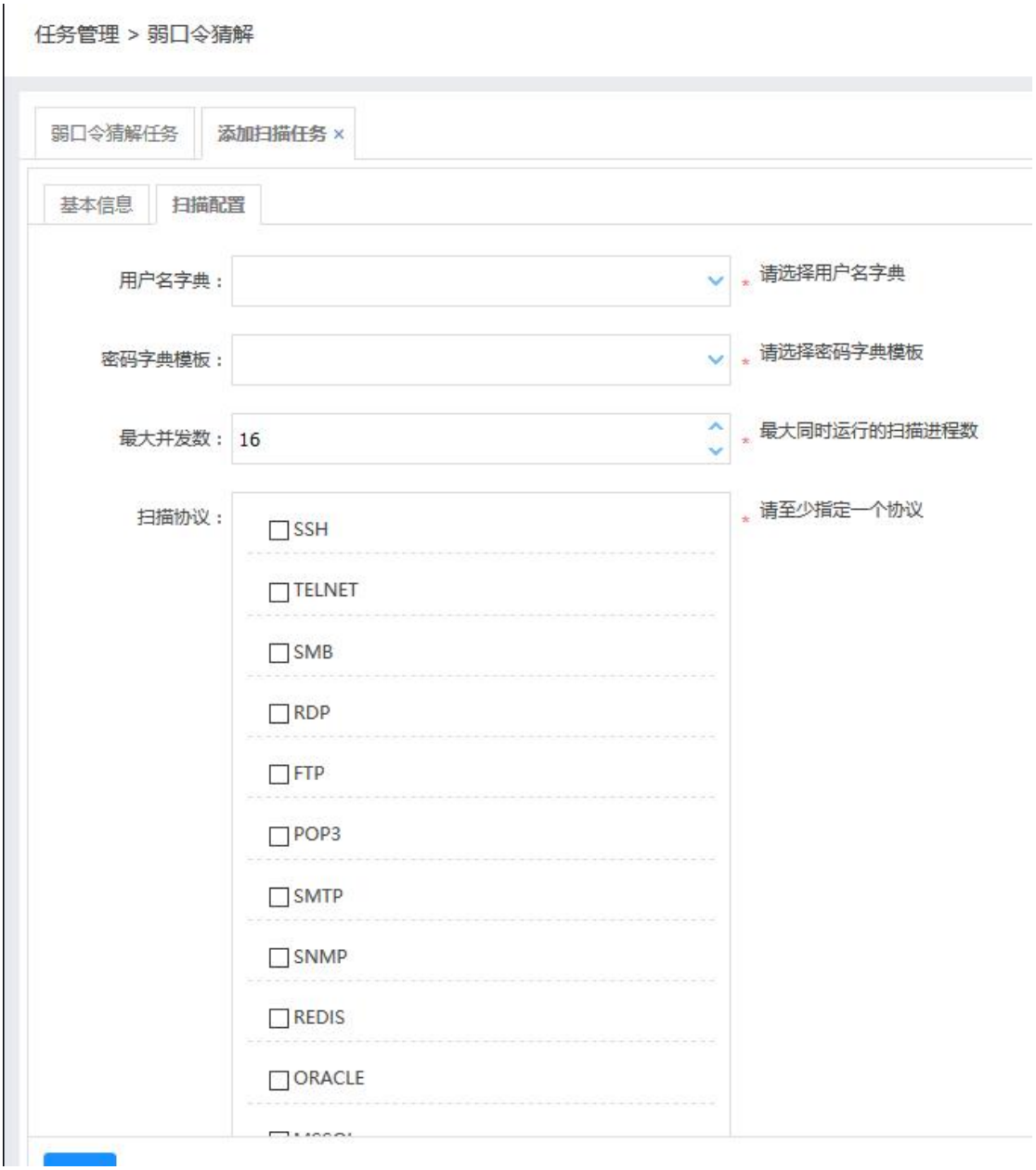
该模块主要用于管理平台所建的数据库扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。

■ **点击**  **按钮，输入信息，即可添加扫描任务；**

4.3.8 弱口令猜解

该模块主要用于管理平台所建的弱口令扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。

■ **点击**  **按钮，输入信息，即可添加扫描任务；**



扫描协议选择（根据目标开启的服务开选择协议）：

SSH：目标开启了 SSH 服务，如 LINUX 系统、网络设备、安全设备等。

TELNET：目标开启了 TELNET 服务，如 LINUX 系统、网络设备、安全设备等。

SMB/RDP：目标为 WINDOWS 操作系统。

FTP：目标开启了 FTP 服务。

POP3/SMTP：目标为邮件服务器。

SNMP：目标开启了 SNMP 服务，如服务器、网络设备、安全设备等。

REDID/ORACLE/MSSQL/MYSQL/POSTGRES/：目标安装了对应的数据库服务。

HTTP：目标为 WEB 服务器，且登陆页面没有验证码。

4.4 等保合规

该模块主要用于管理平台所建的信息系统测评任务。以列表的方式显示信息系统名称、被测单位名称、系统简介、SAG 等级、资产数等信息。

4.4.1 被测单位管理

此处展示被测单位的联系信息。

点击添加可以添加新的被测单位。

4.4.2 测评单位管理

与被测单位相反，这里显示的是测评单位信息。

4.4.3 等保测评任务

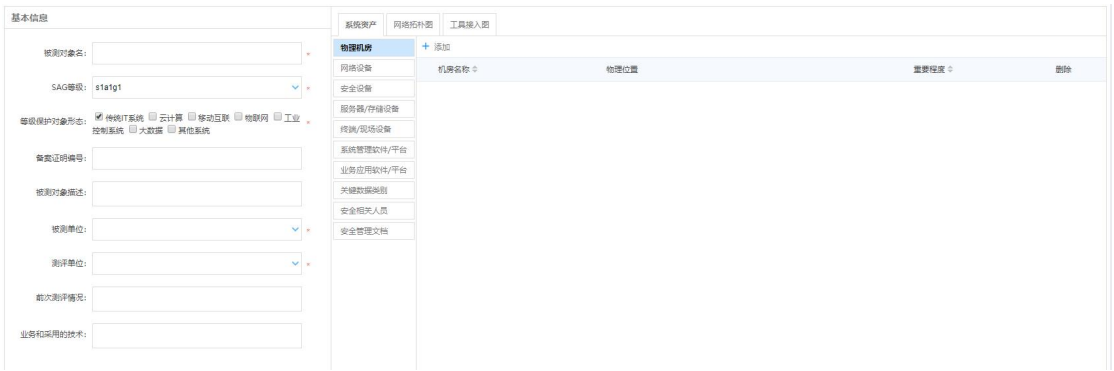
默认此处显示等保测评任务。在

也可以按条件查询测评任务。

4.4.3.1 新建测评任务

点击 

，输入相关信息，即可添加新的测评任务。



- 被测对象名（必填）：命名被测对象。
- SAG 等级（必填）：为被测对象选择对应的等级。G：基本要求类 S：

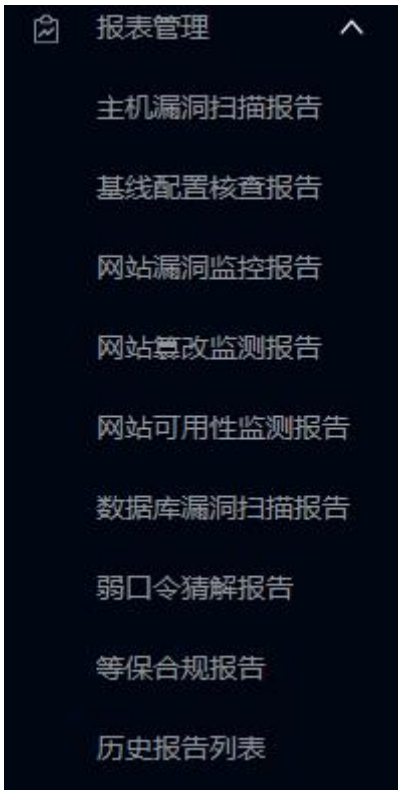
业务信息安全类 A：系统服务保证类，通常某一个级别的系统就必须具备这一级别的基本要求，如 3 级的就是 G3。

- 等级保护对象形态（必填）：为被测对象选择对应的形态。

在此页面右侧对应的页签内添加机房、设备、软件、管理文档、人员情况以及网络拓扑图等。

4.5 报表管理

本功能模块，可生成扫描结果报告，并提供报告的历史查阅、导出下载等功能。



4.5.1 主机漏洞扫描报告

在此页面可以选择主机漏洞扫描任务，命名报告名称，制定报告的页眉、logo 和页脚链接等后，即可定制生成任务报告。

- **扫描任务（必选）**：在扫描任务的下拉框中，选择需要导出为报告的扫描任务。
- **报告名称（必填）**：选择了扫描任务后，系统会自动命名报告名称，如需修改可以在此框中修改。
- **页面设置**：包括页眉文本、页眉 logo 和页脚链接，用户可以自行修改。
- **预览**：点击 预览，将新建页签，并在页签中以 HTML 方式预览报告（需等待一段时间生成报告）。
- **导出报告**：即生成并下载报告，鼠标悬浮于 导出报告 的右侧下拉标识处，将弹出下拉框，供用户选择导出报告格式 (包括 DOC、PDF 和 HTML)。随后选择下载目录，并等待生成报告。
- **生成报告**：即仅生成报告，鼠标悬浮于 生成报告 的右侧下拉标识处，将弹出下拉框，供用户选择生成报告格式（包括 DOC、PDF 和 HTML）。选择格式后，等待生成报告。报告生成后，可以在“历史报告列表”中找到已生成的报告。

4.5.2 基线配置核查报告

用于导出基线配置核查任务产生的报告。

4.5.3 网站漏洞监控报告

用于系统管理人员及监督检查人员，可查看资产存在的整体安全趋势、安全情况以及具体漏洞，便于快速分析所存在的问题，有助于做出正确的安全决策。

4.5.4 网站篡改监测报告

用于导出网站篡改监测任务产生的报告。

4.5.5 网站可用性监测报告

用于导出基线配置核查任务产生的报告。

4.5.6 数据库扫描报告

用于导出数据库扫描任务产生的报告。

4.5.7 弱口令猜解报告

用于导出弱口令猜解任务产生的报告。

4.5.8 等保合规报告

本报告的评估方法、计分标准以及展现方式均严格按照《网络安全等级保护测评报告模板》（2019 版）的要求生成。

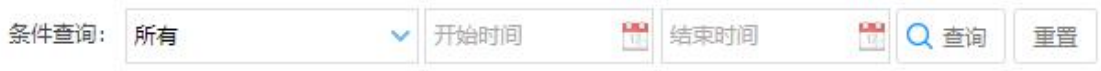
4.5.9 历史报告列表

历史报告列表，展示历次生成或导出的列表，为用户提供报告的归档，以备

日后需要时再次查看或下载。

4.5.9.1 历史报告查询

可通过多条件组合进行历史报告的查询，页面会根据查询条件显示对应的报告记录。



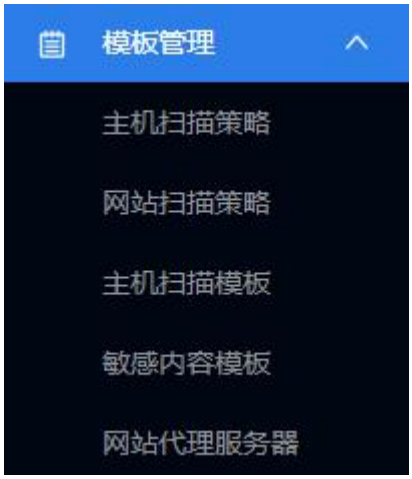
- 可通过以下条件查询历史报告：
  - 时间段：开始时间和结束时间
- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.5.9.2 历史报告操作

- **报告勾选：**可点击每行报告记录最左侧的勾选框，打钩勾选该报告，并执行批量下载或批量删除的操作。
- **下载/批量下载：**勾选报告后，点击 下载 则执行下载/批量下载报告的操作，选择下载目录，即可执行下载过程。
- **删除/批量删除：**勾选报告后，点击 删除 则执行删除/批量删除报告的操作，在进行二次确认后，即可删除报告。

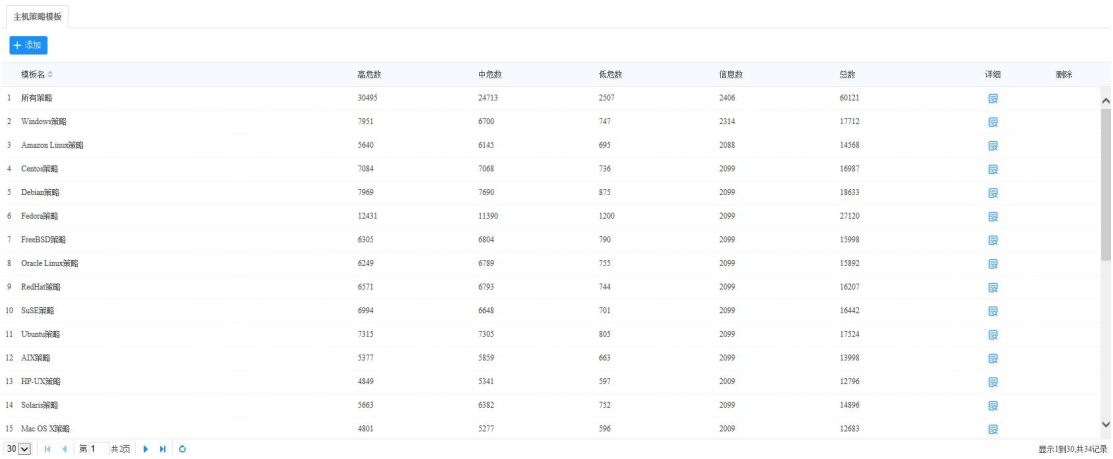
4.6 模板管理

本功能模块，可查看并自定义主机扫描策略（共计 6 万+策略，涵盖 CVE、CNNVD、CNVD、CNCVE、CVSS、BUGTRAQ 等国内和全球漏洞库），以及制定主机扫描模板，在执行主机扫描任务时可选择扫描模板。



4.6.1 主机扫描策略

本功能可供用户查看/添加主机扫描策略集。在此预置的和自定义的扫描策略集，可以应用至“主机扫描模板”中，形成一个自定义的模板，然后对指定的资产/资产组执行漏洞扫描任务。



4.6.1.1 预定义扫描策略集

预定义的主机扫描策略集共 30 种，包含：

- ✓ 第 1 条，所有策略，即涵盖剩余 29 种预置的扫描策略的全集，6 万+条策略。
- ✓ 第 2-15 条，均为主机操作系统策略，涵盖各类 Windows、Linux、Unix 操作系统。
- ✓ 第 16 条，网络设备和防火墙策略，包括主流厂商的网络路由器、交换机、防火墙等设备。
- ✓ 第 17 条，虚拟化设备策略，包括主流的虚拟化平台（VMware vSphere、Citrix XenServer）。
- ✓ 第 18 条，端口扫描策略，主要涵盖各类远程扫描方法。
- ✓ 第 19 条，大数据组件策略，涵盖 Elastic Search、Apache Hadoop 等主流大数据组件的漏洞。
- ✓ 第 20 条，Office 类漏洞，涵盖微软 Office、Apache Open Office、libreoffice、Fedora goffice 等办公软件。
- ✓ 第 21 条，密码爆破和身份认证类漏洞。
- ✓ 第 22 条，缓冲区溢出类漏洞。
- ✓ 第 23-26 条，覆盖常见应用协议的漏洞（FTP、RPC、SMTP 和 SNMP）。
- ✓ 第 27 条，数据库漏洞，涵盖 MySQL、MariaDB、Oracle、PostgreSQL、MSSQL、DB2、SQLite、Sybase、达梦等数据库。

- ✓ 第 28 条，WEB 漏洞，涵盖主流网站、视频会议、后台管理、IP 电话、WEB 应用防火墙、WEB 中间件等漏洞。
- ✓ 第 29 条，云平台漏洞，涵盖 Openstack、VMware vCenter、HP Helion 等云计算平台的漏洞。
- ✓ 第 30 条，NTP 类漏洞，主要针对时间服务存在的漏洞。

4.6.1.2 策略集详情

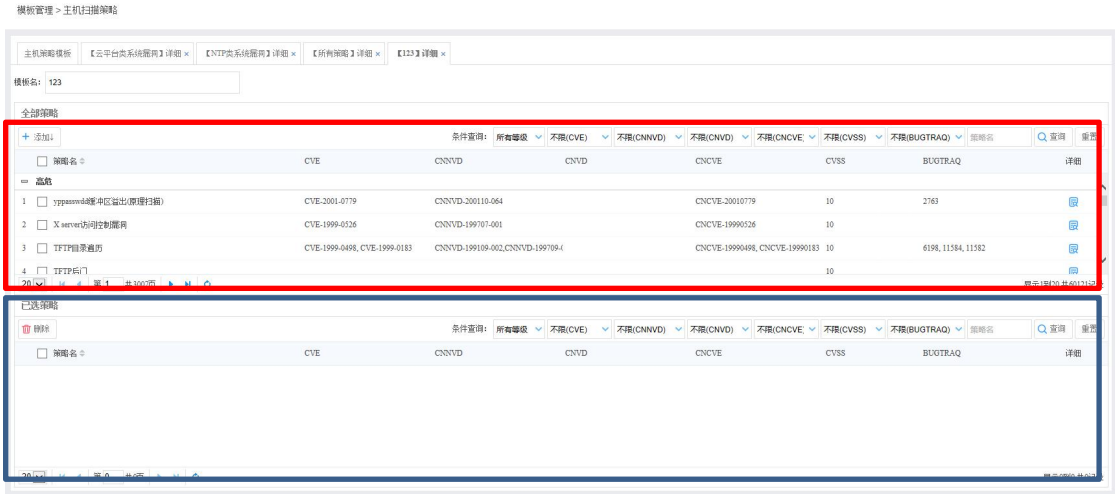
点击每一种扫描策略的“详细”列的，可查看扫描策略具体的策略条目。

- ➢ 蓝框中为本策略集已加入的策略条目，可通过勾选条目，再点击左上角 删除 按钮，移除出本策略集。
- ➢ 红框中为未加入本策略集的策略条目，可通过勾选条目，再点击左上角 添加 按钮，加入到本策略集中。
- ➢ 可通过漏洞等级，是否包含在各个公共漏洞库，以及通过策略名搜索等方式，对已加入策略集的策略条目（蓝框）和未加入策略集的策略条目（红框）进行检索。

4.6.1.3 添加策略集

点击页面左上角 + 添加 按钮，可以在新建页签中添加新的策略集。

输入模板命名，点击确定，进入下一步添加策略的页面。



- 蓝框中为本策略集已加入的策略条目，可通过勾选条目，再点击左上角 删除 按钮，移除出本策略集。
- 红框中为未加入本策略集的策略条目，可通过勾选条目，再点击左上角 + 添加 按钮，加入到本策略集中。
- 可通过漏洞等级，是否包含在各个公共漏洞库，以及通过策略名搜索等方式，对已加入策略集的策略条目（蓝框）和未加入策略集的策略条目（红框）进行检索。

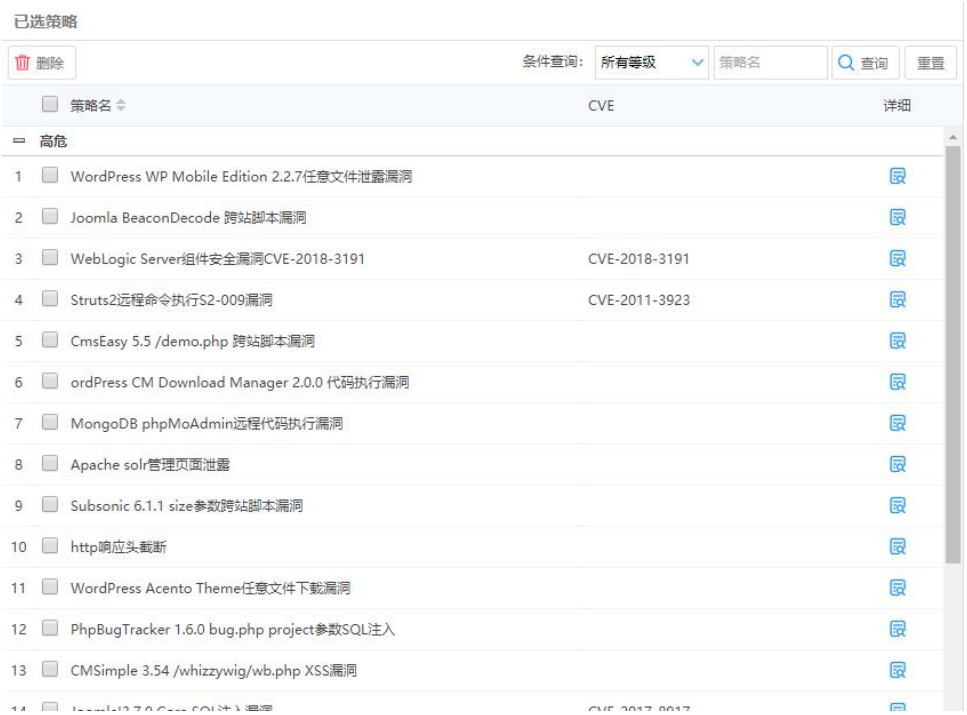
4.6.2 网站扫描策略

在执行网站扫描的时候，需要选择一个扫描模板。当前系统中内置了两个策略模板：

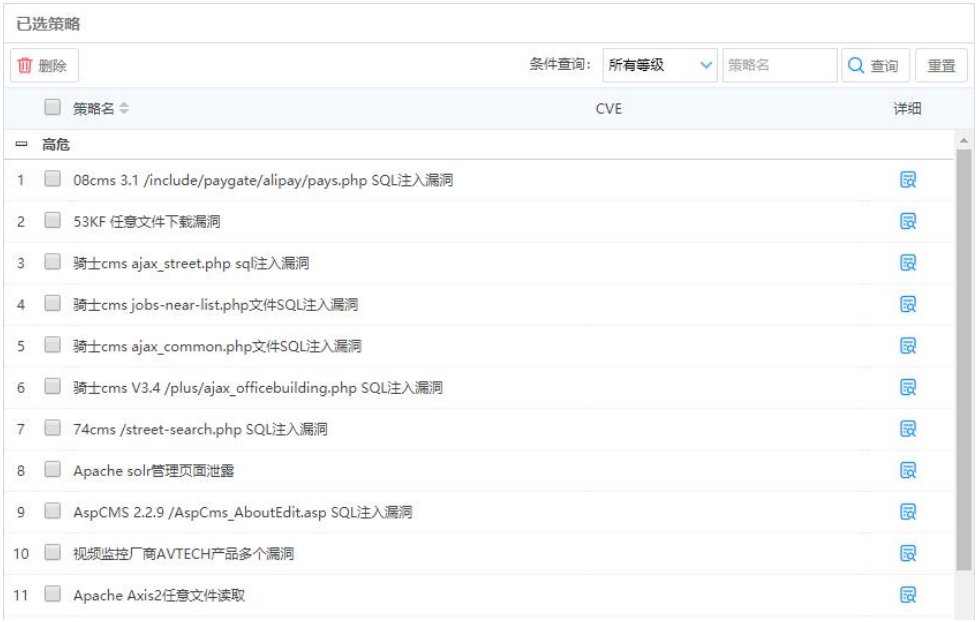
4.6.2.1 预定义扫描策略

系统内置了两个扫描策略模板：系统默认和所有策略。

系统默认模板包含了通用的、比较常见的网站漏洞。

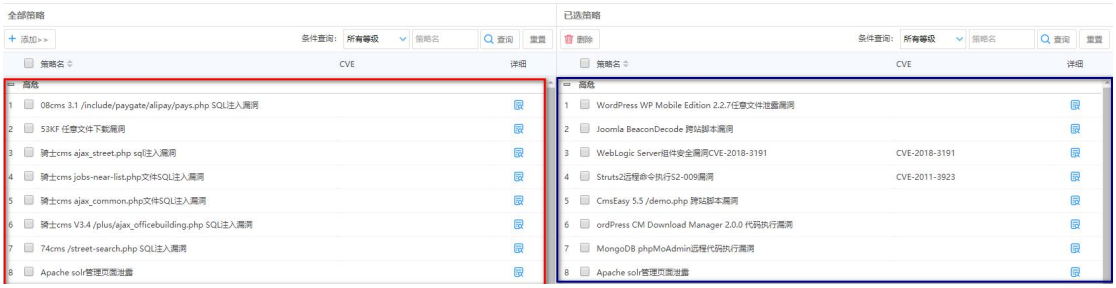


所有策略则包括的更全面一些，如 CSM 类型的网站。使用所有策略进行扫描时会增加扫描时间。



4.6.2.2 模板详情

点击每一种扫描策略的“详细”列的，可查看扫描策略具体的策略条目。

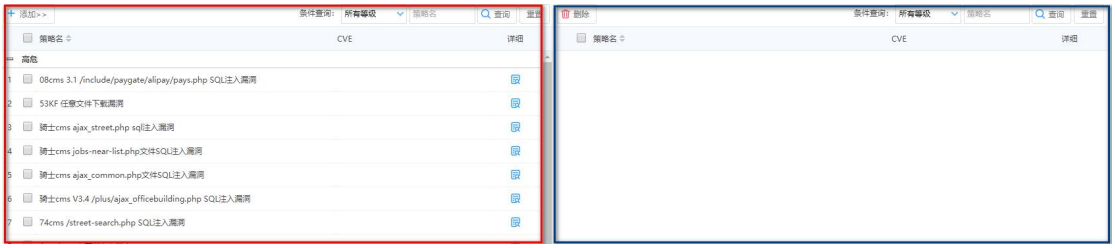


- 蓝框中为本策略集已加入的策略条目，可通过勾选条目，再点击左上角 删除 按钮，移除出本策略集。
- 红框中为所有策略的策略条目，可通过勾选条目，再点击左上角 + 添加↓ 按钮，加入到本策略集中。
- 可通过漏洞等级，是否包含在各个公共漏洞库，以及通过策略名搜索等方式，对已加入策略集的策略条目（蓝框）和未加入策略集的策略条目（红框）进行检索。

4.6.2.3 添加策略集

点击页面左上角  按钮，可以在新建页签中添加新的策略集。

输入模板命名，点击确定，进入下一步添加策略的页面。

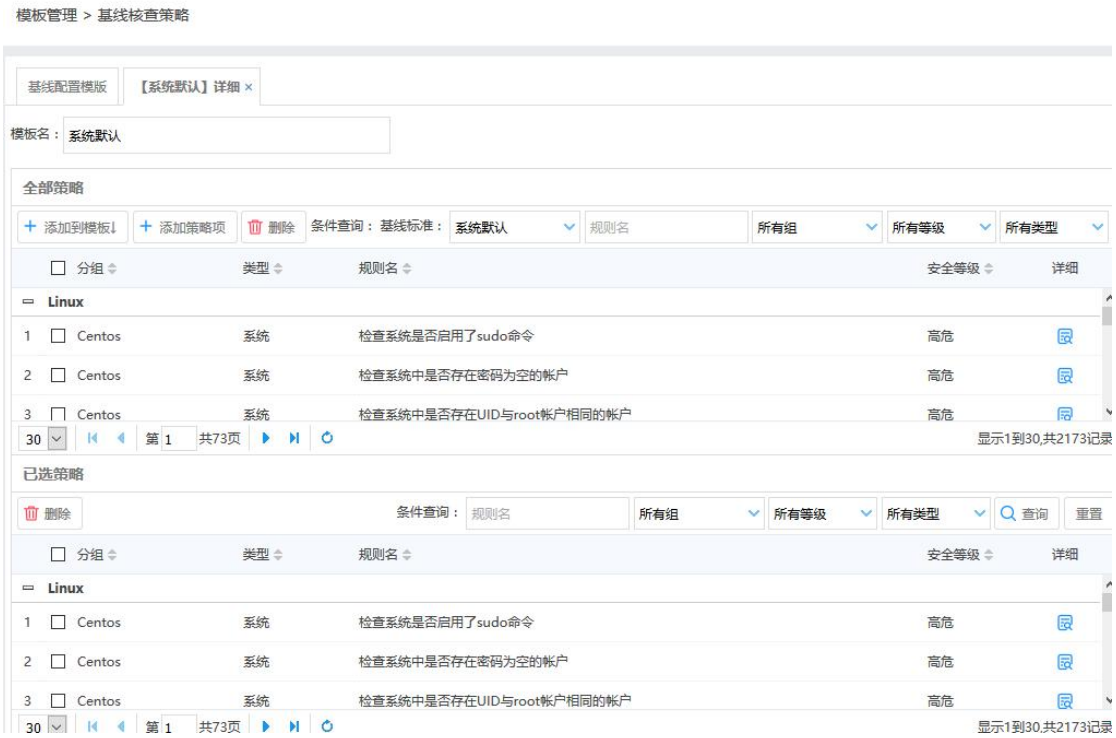


- 蓝框中为本策略集已加入的策略条目，可通过勾选条目，再点击左上角按钮，移除出本策略集。
- 红框中为未加入本策略集的策略条目，可通过勾选条目，再点击左上角按钮，加入到本策略集中。
- 可通过漏洞等级，是否包含在各个公共漏洞库，以及通过策略名搜索等方式，对已加入策略集的策略条目（蓝框）和未加入策略集的策略条目（红框）进行检索。

4.6.3 基线核查策略

该模块以列表的方式显示模板名称、所属分组和策略总数等信息。（基线评估模板不可添加、修改、删除）

■ **点击** **按钮，即可查看模板的详情，以列表的方式显示策略名称、等级、检查点、检查项、所属策略模板、所属策略分组等信息；**



4.6.4 数据库扫描策略

该模块的主要功能是管理数据库策略，以列表的方式显示模板名称、紧急、高危、中危、低危、信息策略数等信息。（数据库策略模板不可添加、修改、删除）

4.6.5 主机扫描模板

本功能模块是管理和维护主机漏洞扫描模板，在建立主机漏洞扫描的任务时，需要选择使用的扫描模板，就是从本功能模块保存的扫描模板中选择的。

4.6.5.1 预定义扫描模板

系统预置了 3 个扫描模板：

1. 快速扫描，扫描的端口较少，使用所有扫描策略；
2. 标准扫描，扫描的端口较多，使用所有扫描策略；
3. 全面扫描，扫描全部端口，使用所有扫描策略。

注意：系统预置的扫描模板不可修改、删除。

属性名	属性值
模板信息	
模板名	快速扫描
端口扫描	
TCP端口	21,22,23,25,53,80,102,110,111,135,139,143,443,445,502,875,1433,1521,2049,3306,3389,5554,6000,6267,7626
UDP端口	53,111,123,161,2049
端口扫描方式	SYN扫描
深度扫描	否
扫描服务版本	否
漏洞扫描	
策略模版	所有策略
扫描不可达的主机	否
扫描打印机	是
主机存活测试	ICMP PING
最大并发策略数	8
策略执行超时(秒)	180
是否登陆扫描	否
用户密码字典	administrator: administrator:123456 admin: admin:123456 guest: guest:123456 root: root:123456
网络连接超时(秒)	10
最大并发主机数	80
安全扫描	是

快速扫描模板

属性名	属性值
模板信息	
模板名	标准扫描
端口扫描	
TCP端口	1-5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-59,61-224,242-248,256-268,280-287,308-322,333,344-700,702,704-707,709-711,721,723,729-731,740-742,744,747-754,758-765,767,769-777,780-783,786-787,789,799-801,808,810,828-829,847-848,860,871,873,886-888,898,900-904,911-913,927,950,953,975,989-100
UDP端口	
端口扫描方式	SYN扫描
深度扫描	否
扫描服务版本	否
漏洞扫描	
策略模版	所有策略
扫描不可达的主机	否
扫描打印机	是
主机存活测试	ICMP PING
最大并发策略数	8
策略执行超时(秒)	180
是否登陆扫描	否
用户密码字典	administrator: administrator:123456 admin: admin:123456 guest: guest:123456 root: root:123456
网络连接超时(秒)	10
最大并发主机数	80
安全扫描	是

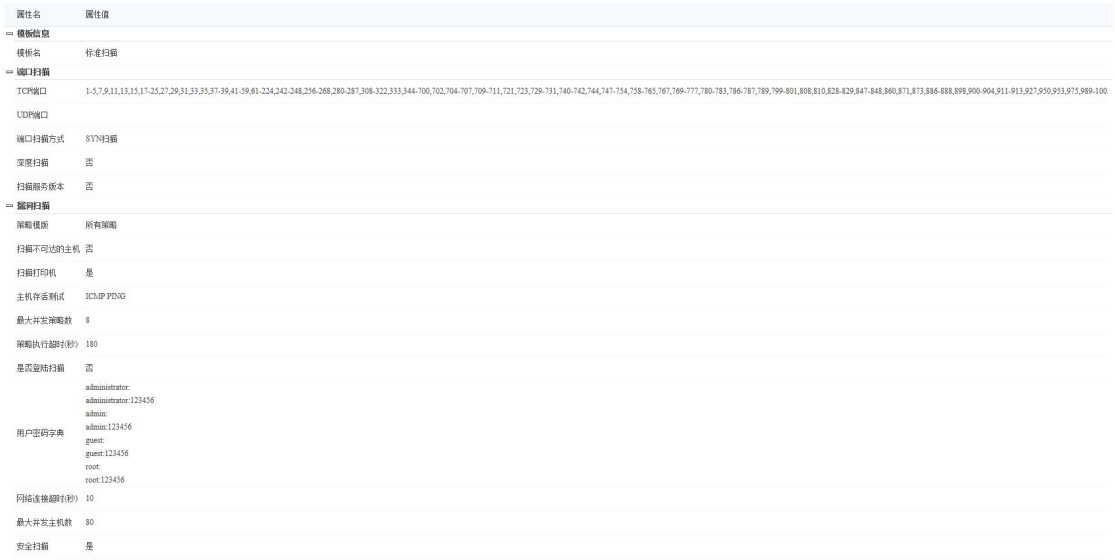
标准扫描模板

属性名	属性值
模板信息	
模板名	全面扫描
端口扫描	
TCP端口	1-10000,50000
UDP端口	53,111,123,2049,137,161
端口扫描方式	SYN扫描
深度扫描	否
扫描服务版本	否
漏洞扫描	
策略模版	所有策略
扫描不可达的主机	否
扫描打印机	是
主机存活测试	ICMP PING
最大并发策略数	8
策略执行超时(秒)	180
是否登陆扫描	否
用户密码字典	administrator: administrator:123456 admin: admin:123456 guest: guest:123456 root: root:123456
网络连接超时(秒)	10
最大并发主机数	80
安全扫描	是

全面扫描模板

4.6.5.2 查看扫描模板详情

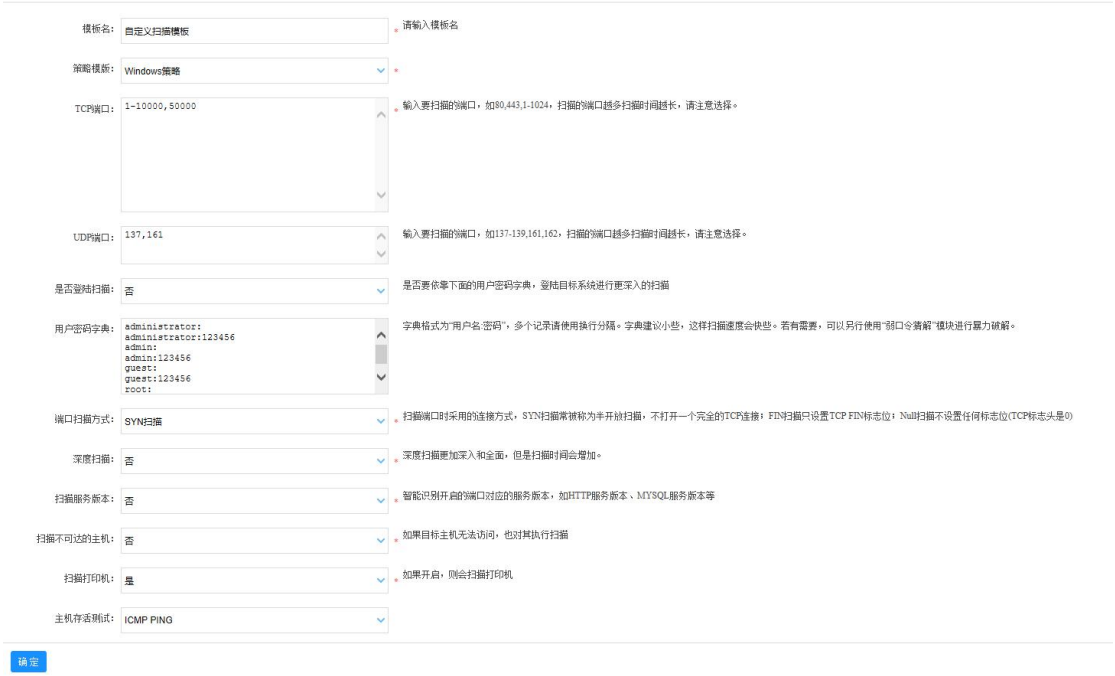
点击列表“详细”列的按钮，可在新建页签中查看扫描模板的详情。



属性名	属性值
模板信息	
模板名	标准扫描
端口扫描	
TCP端口	1-5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-59,61-224,242-248,256-268,280-287,308-322,333,344-700,702,704-707,709-711,721,723,729-731,740-742,744,747-754,758-765,767,769-777,780-783,786-787,789,799-801,808,810,828-829,847-848,860,871,873,886-888,898,900-904,911-913,927,950,953,975,989-100
UDP端口	
端口扫描方式	SYN扫描
深度扫描	否
扫描服务版本	否
策略扫描	
策略模版	所有策略
扫描不可达的主机	否
扫描打印机	是
主机存活测试	ICMP PING
最大并发策略数	8
策略执行超时(秒)	180
是否登陆扫描	否
用户密码字典	administrator: administrator:123456 admin: admin:123456 guest: guest:123456 root: root:123456
网络连接超时(秒)	10
最大并发主机数	80
安全扫描	是

4.6.5.3 添加扫描模板

点击页面左上角的 + 添加 按钮，可在新建页签中设置新添加扫描模板的各项参数。



- **模板名（必填）：** 命名模板名称；
- **策略模板（选择）：** 选择一个策略模板；
- **TCP 端口（必填）：** 输入需要扫描的 TCP 端口，端口间使用英文逗号隔

开；

- **UDP 端口（选填）：** 输入需要扫描的 UDP 端口，端口间使用英文逗号隔开，可留空；
- **是否登录扫描（选择）：** 默认关闭，如选择了启用登录扫描，则需要在“用户密码字典”中填入用户名和密码，以此进行对目标系统更深入的扫描；
- **用户密码字典（选填）：** 如选择了启用登录扫描，则需要输入用户名密码字典，格式为每行通过“:”隔开用户名和密码，形如“admin:123456”。
- **端口扫描方式（选择）：**
  - ✓ TCP 扫描，也称全连接扫描，直接与被扫描目标建立连接，在连接后开始扫描，可能会被主机防火墙防护。
  - ✓ SYN 扫描（默认），也称半连接扫描，也是最常用的扫描方式。
  - ✓ ACK 扫描，可以探测那些阻止 SYN 或 ICMP Echo 请求的主机，提高通过主机防火墙的概率。
  - ✓ FIN 扫描、Xmas Tree 扫描和 Null 扫描，如果 SYN 扫描无法有效的查明端口开放情况，有可能是被防火墙阻拦，可以尝试更换为 FIN、Xmas Tree 或 Null 扫描方式再行尝试。
- **深度扫描（选择）：** 默认关闭，如开启深度扫描，会扫描主机上的应用系统，会呈现更加详细的扫描结果，但是也会相应的增加扫描时间。
- **扫描服务版本（选择）：** 默认关闭，如开启扫描服务版本，系统会智能识别开启的端口所对应的服务版本，如 HTTP 服务版本、MySQL 服务版本等。

- **扫描不可达的主机（选择）：**默认关闭，如开启扫描不可达的主机，即使目标主机无法访问，也会对其进行扫描。
- **扫描打印机（选择）：**默认关闭，如开启扫描打印机，则会对打印机执行扫描。
- **主机存活测试（选择）：**
  - ✓ ICMP Ping（默认），最常使用的判断主机存活的方法；
  - ✓ ARP、TCP Ping、TCP-SYN Ping，如目标主机禁止了 ICMP Ping，则可使用 ARP、ICMP Ping、TCP-SYN Ping 等方式进行探测。
- **最大并发策略数（必填）：**默认为 16，可选择 1-31。
- **策略执行超时（秒）（必填）：**默认为 180 秒，可选择 1-600。
- **网络连接超时（秒）（必填）：**默认为 10 秒，可选择 1-30。
- **最大并发主机数（必填）：**默认为 64 个，可选择 1-128。
- **安全扫描（必选）：**默认开启，如果禁用，将执行可能会影响主机/服务可用性的扫描策略，但是会使扫描更加深入和全面。

4.6.6 敏感内容模板

模块的主要功能是添加、删除网站安全监控中的敏感关键字。系统内置了两个模板，涵盖了大部分的敏感词汇。

如果用户需要自定义敏感词汇，需要点击工具栏中的+添加按钮，即可添加敏感关键字模板。

自定义的关键字使用换行符隔开，如果关键字数量较大，可预先存到一个 txt 文本中，再将其上传至该页面，点击确定完成敏感内容的模板添加。

4.6.7 网站代理服务器

该模块的主要功能的添加、删除访问的网站代理服务器。可导入和导出服务器模板。

点击工具栏中的+添加按钮，即可添加敏感关键字模板。

- 模板名称（必填）：用户自定义一个方便记忆的名称。
- 代理类型（必填）：有 http、https、socks5 三种类型可选，但要与要连接的代理服务器代理类型一致。
- IP 地址（必填）：填写正确的代理服务器地址。
- 端口（必填）：填写正确的代理服务器端口号。

4.6.8 密码字典模板

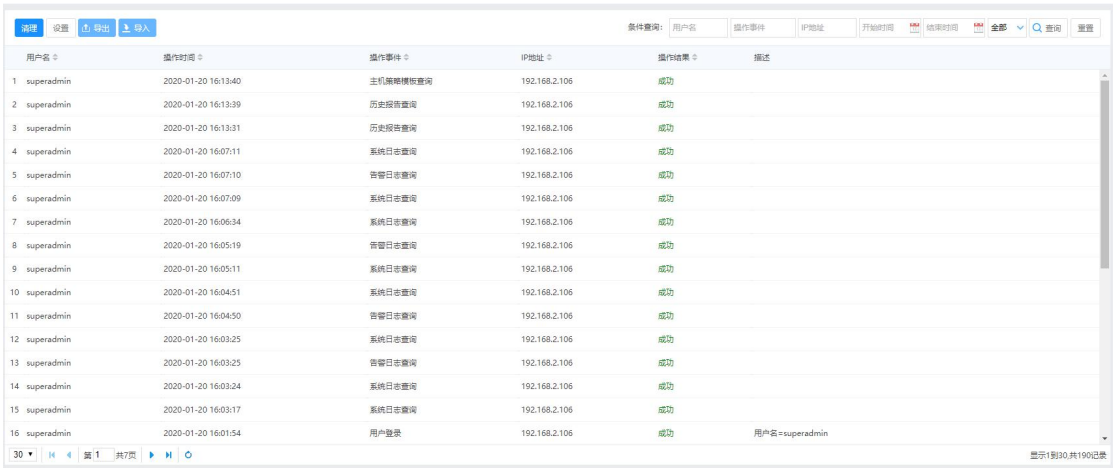
该模块的主要功能为将常用的弱口令字典保存起来，方便直接应用到各个不同的弱口令扫描任务中，以列表的方式显示字典名称、字典类型和字典内容等信息。（系统默认的弱口令字典不可修改、删除）

4.7 日志管理

本功能模块，可查看、导入、导出、清理和设置各类系统产生的日志。日志分为操作日志（记录登录账号操作行为）、系统日志（记录系统自动执行的任务，如周期性扫描任务）和告警日志（记录扫描结果，将扫描出的漏洞以告警形式列出）。

4.7.1 操作日志

操作日志中，记录所有登录管理员的操作行为，并以日志条目的形式展示。



	用户名	操作时间	操作事件	IP地址	操作结果	描述
1	superadmin	2020-01-20 16:13:40	主机策略模板查询	192.168.2.106	成功	
2	superadmin	2020-01-20 16:13:39	历史报告查询	192.168.2.106	成功	
3	superadmin	2020-01-20 16:13:31	历史报告查询	192.168.2.106	成功	
4	superadmin	2020-01-20 16:07:11	系统日志查询	192.168.2.106	成功	
5	superadmin	2020-01-20 16:07:10	告警日志查询	192.168.2.106	成功	
6	superadmin	2020-01-20 16:07:09	系统日志查询	192.168.2.106	成功	
7	superadmin	2020-01-20 16:06:34	系统日志查询	192.168.2.106	成功	
8	superadmin	2020-01-20 16:05:19	告警日志查询	192.168.2.106	成功	
9	superadmin	2020-01-20 16:05:11	系统日志查询	192.168.2.106	成功	
10	superadmin	2020-01-20 16:04:51	系统日志查询	192.168.2.106	成功	
11	superadmin	2020-01-20 16:04:50	告警日志查询	192.168.2.106	成功	
12	superadmin	2020-01-20 16:03:25	系统日志查询	192.168.2.106	成功	
13	superadmin	2020-01-20 16:03:25	告警日志查询	192.168.2.106	成功	
14	superadmin	2020-01-20 16:03:24	系统日志查询	192.168.2.106	成功	
15	superadmin	2020-01-20 16:03:17	系统日志查询	192.168.2.106	成功	
16	superadmin	2020-01-20 16:01:54	用户登录	192.168.2.106	成功	用户名=superadmin

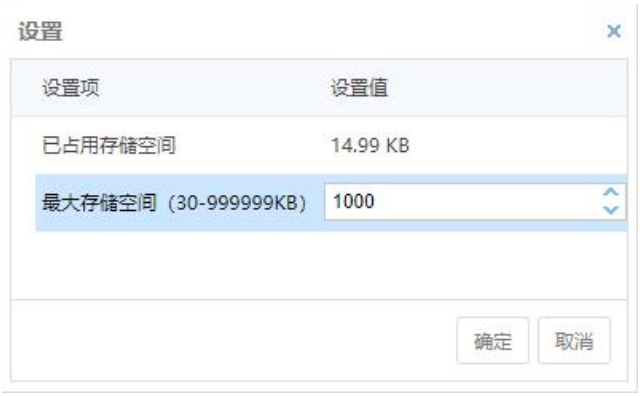
4.7.1.1 日志查询

位于页面右上角，有条件查询组件。

- 可通过以下条件查询日志：
  - 管理员用户名
  - 操作事件（关键字）
  - 登录终端 IP 地址
  - 时间段（开始时间、结束时间）
  - 操作结果（成功、失败）
- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.7.1.2 日志空间设置

页面左上角，点击 设置 按钮，可打开日志空间设置选项。



如图，展示目前已占用的存储空间大小，并可设置最大存储空间。

4.7.1.3 日志导出

页面左上角，点击 导出 按钮，可将目前条件查询到的所有日志条目导出为文件形式，并选择目录下载到登录终端。

4.7.1.4 日志导入

页面左上角，点击 导入 按钮，可将以前导出的日志文件导入至系统（如日志丢失或清理）。

支持日志文件最大 200MB，可将文件拖入文本框进行上传，也可以点击文本框，通过文件浏览器选择日志文件。

4.7.1.5 日志清理

页面左上角，点击清理按钮，可选择清理日志空间。

可选择清理全部日志，或按照时间长度清理，支持：

- ✓ 清理一个月以前的日志
- ✓ 清理三个月以前的日志
- ✓ 清理六个月以前的日志
- ✓ 清理一年以前的日志
- ✓ 清理两年以前的日志
- ✓ 清理自定义设置的日期以前的日志

4.7.2 系统日志

系统日志中，记录所有系统自动执行的任务（如周期性扫描），并以日志条目的形式展示。

4.7.2.1 日志查询

位于页面右上角，有条件查询组件。

- 可通过以下条件查询日志：
  - 操作事件（关键字）
  - 时间段（开始时间、结束时间）
  - 操作结果（成功、失败）
- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.7.2.2 日志清理

页面左上角，点击 

按钮，可选择清理日志空间。

可选择清理全部日志，或按照时间长度清理，支持：

✓ 清理一个月以前的日志

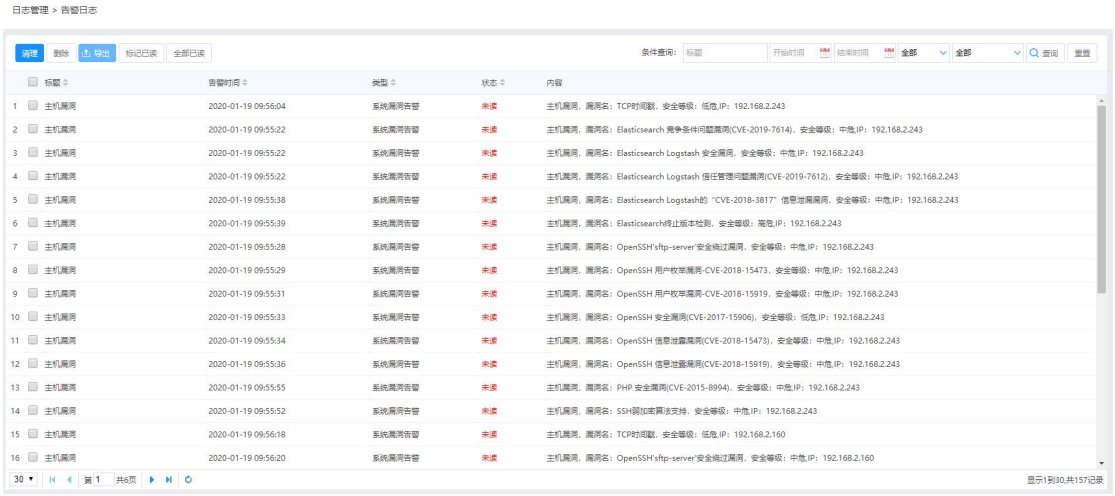
✓ 清理三个月以前的日志

✓ 清理六个月以前的日志

- ✓ 清理一年以前的日志
- ✓ 清理两年以前的日志
- ✓ 清理自定义设置的日期以前的日志

4.7.3 告警日志

告警日志中，记录所有扫描出的漏洞，并可设置告警是否已读，并支持告警日志的导出、删除和清理。



4.7.3.1 日志查询

位于页面右上角，有条件查询组件。

- 可通过以下条件查询日志：
  - ➢ 日志标题
  - ➢ 时间段（开始时间、结束时间）
  - ➢ 告警是否已读（全部、已读、未读）

- 告警类型（全部、系统告警、网站漏洞告警、系统漏洞告警、基线核查告警）

- 选择好条件后，点击“查询”，执行检索。
- 点击“重置”，可重置检索条件。

4.7.3.2 日志标记已读

告警日志在产生之后，会默认处于“未读”状态（处于“未读”状态的日志条目计数，也会显示在界面右上角的告警位置）。

当管理员了解日志条目情况之后，可将日志条目转变为“已读”状态，有两种方式进行该操作：

- 通过勾选日志条目，点击左上角 标记已读 按钮，可将日志条目状态由“未读”变为“已读”。
- 也可以直接点击左上角 全部已读 按钮，将所有状态为“未读”状态的日志条目，转变为“已读”状态。

4.7.3.3 日志导出

页面左上角，点击 导出 按钮，可将目前条件查询到的所有日志条目导出为文

件形式，并选择目录下载到登录终端。

4.7.3.4 日志删除

在勾选日志条目后，点击左上角 删除 按钮，可删除已勾选的日志条目。

4.7.3.5 日志清理

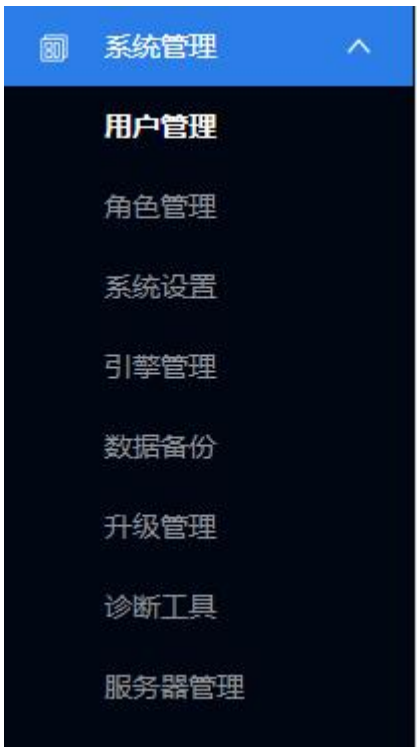
页面左上角，点击 清理 按钮，可选择清理日志空间。

可选择清理全部日志，或按照时间长度清理，支持：

- ✓ 清理一个月以前的日志
- ✓ 清理三个月以前的日志
- ✓ 清理六个月以前的日志
- ✓ 清理一年以前的日志
- ✓ 清理两年以前的日志
- ✓ 清理自定义设置的日期以前的日志

4.8 系统管理

本功能模块，用于进行各类系统自身相关参数的调整，涉及用户与角色、系统还原、系统时间、扫描引擎管理、系统备份恢复、系统升级、系统诊断、系统服务等各方面的管理和配置。



4.8.1 用户管理

以列表的方式显示用户的详细信息，包括用户名、姓名、电话、所属角色、所属区域、锁定状态。（系统默认管理员不可修改、删除、锁定/解锁），点击右侧的 ，可查看该用户的详细信息。

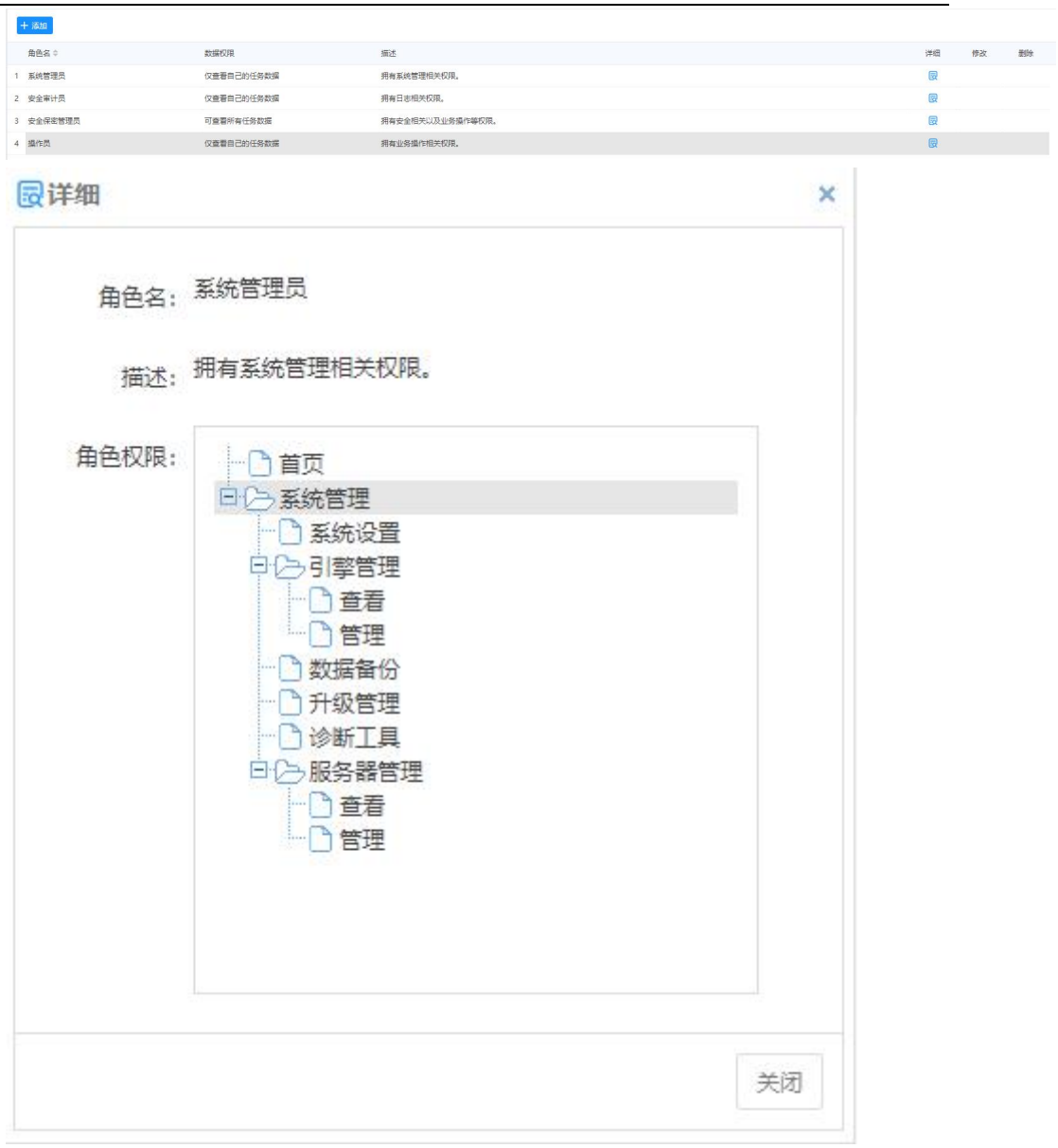
点击 导出 按钮，输入信息，即可添加用户。

点击 

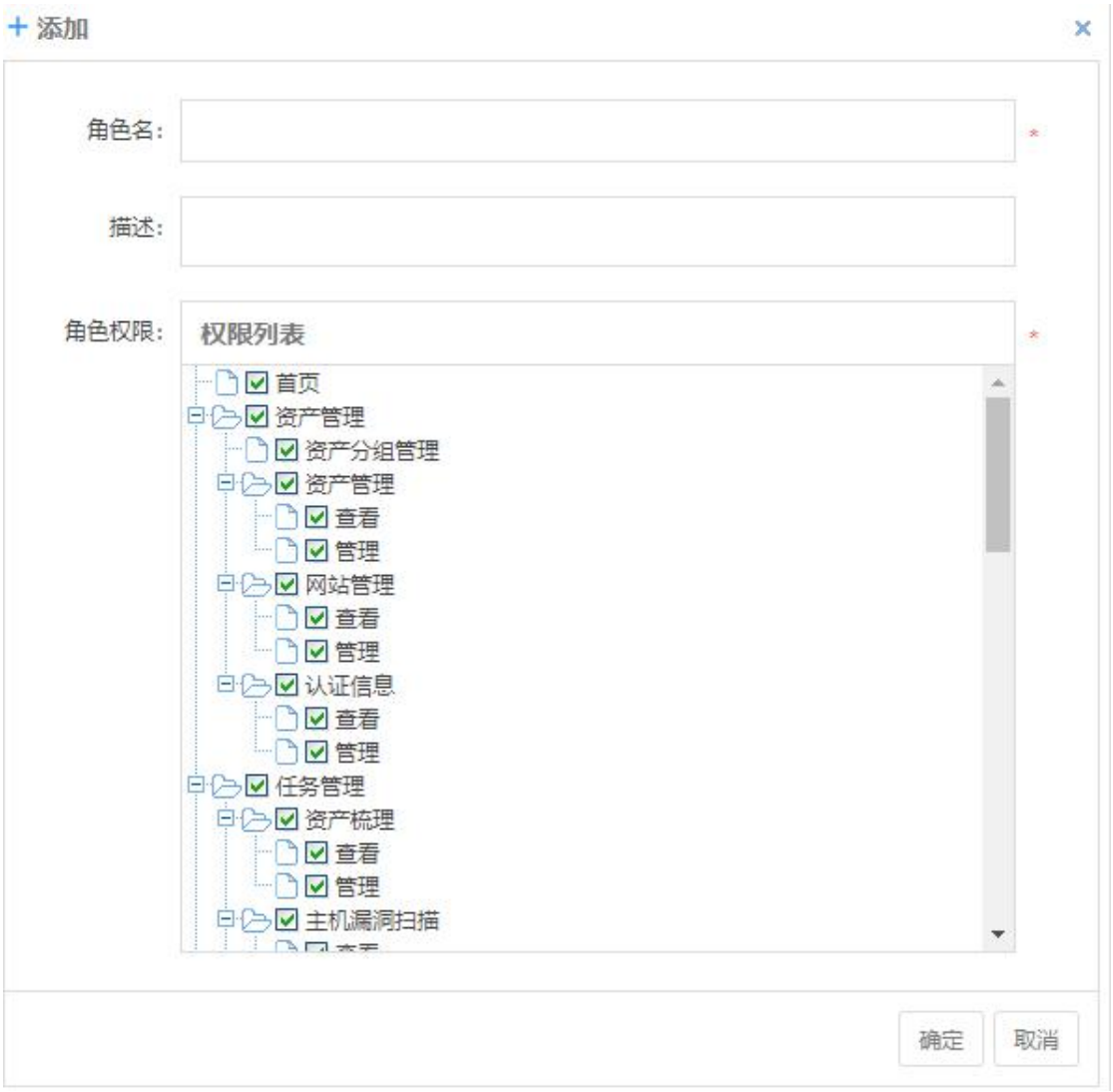
可查询相关用户。

4.8.2 角色管理

以列表的方式显示角色的详细信息，包括角色名、描述和权限。（系统默认管理员、审计员、操作员不可修改、删除）。点击右侧的  ，可以查看该角色所具有哪些权限。



点击 导出 按钮，输入信息，可新建自定义权限的角色。



点击 可对新建的角色进行修改，修改后的角色对应的用户需重新登录才能生效。

4.8.3 系统设置

系统设置功能具备以下设置功能：

- ✓ 设置系统恢复出厂设置
- ✓ 设置会话超时时间
- ✓ 设置系统接口 IP
- ✓ 设置最大并发扫描任务数

✓ 时间设置

4.8.3.1 恢复出厂设置

点击 恢复出厂设置 ，将弹出警示框体，如下图：

点击确定后，系统将恢复出厂设置，即回到系统刚部署完成的状态，所有后建数据（如导入的资产，自定义的扫描策略/模板，已设置的扫描任务，已生成的报表等等）都将被删除。

4.8.3.2 设置会话超时时间

可设置会话超时时间，超过时间未操作，将中断管理连接。再次操作之前需要重新登录。

4.8.3.3 设置接口互动 IP

如存在外部实体需要通过接口方式与本系统互动，则建议在此处填写外部实体的 IP 地址。

注意：如果是在等级保护一体机、云安全管理平台场景下加载了漏洞扫描虚拟机的话，则在此无须填写 IP。

4.8.3.4 最大并发扫描任务数

此处可设置最大并发扫描任务数，依据产品授权不同，允许的最大并发扫描任务数会有变化。会在文本框右侧提示。

4.8.3.5 时间设置

- 可手动设置系统时间
- 可通过 NTP 服务器定期同步时间，需要设置 NTP 服务器地址

注意：请按照实际时间进行手动修改，否则可能会导致产品授权许可过期，导致需要重新导入授权。

4.8.4 引擎管理

此功能模块用于查看扫描引擎的状态，并可对扫描引擎执行重启、开/关机、网卡管理等操作。

4.8.4.1 引擎重启

当出现扫描任务卡死时，可对扫描引擎执行重启操作进行恢复。

- 点击“重启”列的▶按钮，弹出警示框。点击确定后将对扫描引擎执行重启操作。

注意：如果只有一个扫描引擎，在扫描引擎重启后，需要等待一段时间，重新登录系统才可继续使用本系统。

4.8.4.2 引擎关机

当出现扫描任务卡死时，可对扫描引擎执行关机再开机的操作进行恢复。

- 点击“关机”列的按钮，弹出警示框。点击确定后将对扫描引擎执行关机操作。
- 等待

4.8.4.3 网卡管理

可以查看网卡的网络信息，双击图例，则进一步展示网卡的详细信息。

4.8.5 数据备份

可以对系统执行数据备份和恢复。

4.8.5.1 创建系统备份

点击左上角  按钮，在弹出文本框中输入“备份说明”文字，点击确定后即可创建系统备份文件。创建文件时会等待一段时间，创建成功后会生成一条记录。

4.8.5.2 备份文件操作

可针对备份文件执行下载、恢复和删除操作。

- **备份文件下载：**点击列表“下载”列的  按钮，即可选择下载目录，将文件下载至访问终端的指定目录。
- **备份文件恢复：**选择需要恢复的文件记录，点击该记录“恢复”列的按钮，在确认框中进行确认后，即可按此备份文件执行恢复。
- **备份文件删除：**如需删除备份文件，可点击需要删除的备份文件记录“删除”列的  按钮，在确认框中进行确认后，即可删除备份文件。

4.8.5.3 上传文件恢复

点击界面左上角按钮，选择上传文件路径，点击确定后，就可以开始恢复过程。

4.8.6 升级管理

可以对系统执行在线升级的设置，上传升级包进行离线升级，同时也对升级

行为进行记录。

4.8.6.1 升级记录

本页面记录在线或离线的升级记录，并可对升级记录执行清除操作。

点击左上角 清除记录 ，可在确认后删除所有升级记录。

4.8.6.2 在线升级

可在本页面查看到当前版本号。

- 升级方式，包括：
  - ✓ 手动升级，即通过手动方式，点击“检测新版本”按钮，再执行在线升级；

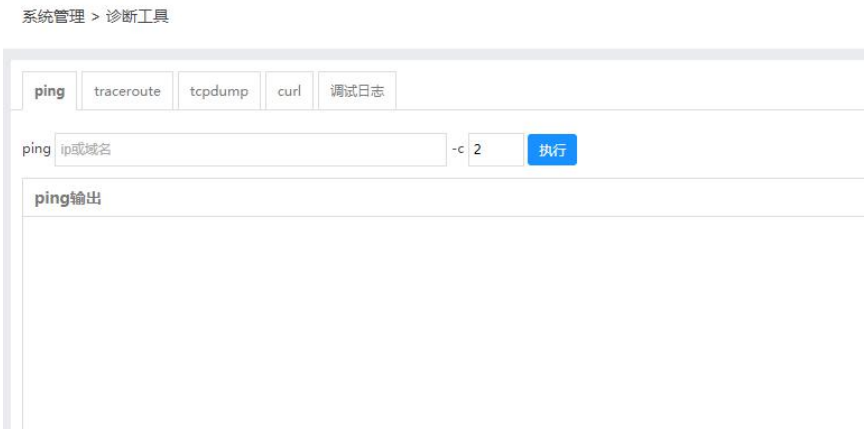
- ✓ 有更新时提醒，即当系统检测到有更新时，会在界面中提醒使用者存在新的升级包，由管理员决定是否升级；
- ✓ 定时升级，可选择每天一个具体的时间（小时和分钟），检测更新并自动进行升级。

- 代理服务器：可选择是否开启代理服务器。如需进行在线升级，则需要开启代理服务器，使用默认字段开启即可。
- 点击检测新版本按钮，如果存在互联网连接或升级代理服务器，可以检测是否存在新版本，并执行升级。

4.8.6.3 离线升级

点击上传升级包按钮，可选择离线升级包执行升级。

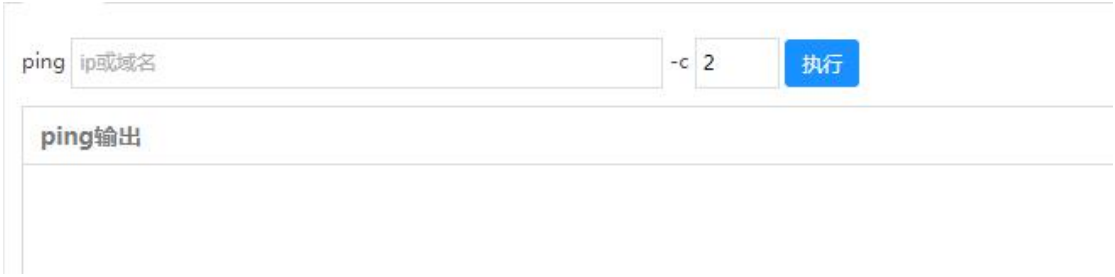
4.8.7 诊断工具



诊断工具提供多种工具：

- Ping 工具：检测资产存活状态；
- Traceroute：定位系统和资产之间存在的所有路由器，查看路由跳数，判断网络情况；
- TCPdump：用于抓包，可用于检测排除网络故障；
- Curl：用于抓取 URL 页面的 HTML 代码，经常用于测试网络和 url 的联通性，模拟正常的网络访问；
- 调试日志：如果系统出现较大问题或故障，且无法通过重启等方式解决，就需要厂商人员下载调试日志，进行诊断。

4.8.7.1 Ping 工具



可输入需要 ping 的 IP 或域名，并在“-c”后输入发包数量，点击执行后，执行结果将在下方面板中显示。

4.8.7.2 Traceroute 工具

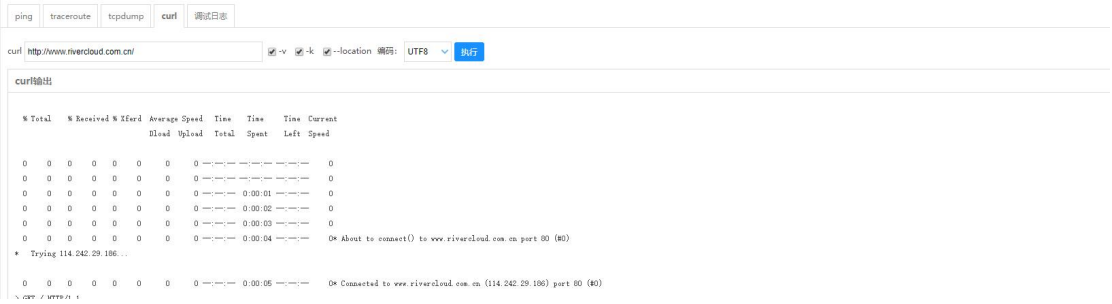
输入需要 traceroute 的 IP 或域名，点击执行后，执行结果将在下方面板中

显示。

4.8.7.3 TCPdump 工具

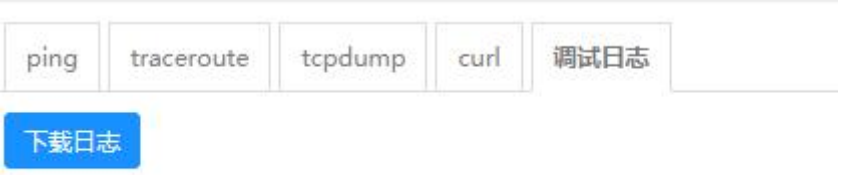
选择网口，并输入 TCPdump 命令，点击执行后，执行结果将在下方面板中显示。

4.8.7.4 Curl 工具



输入需要访问的域名，可选择性的勾选-v（显示 http 通信的整个过程）、-k（访问 HTTPS 网站时可忽略证书不受信问题）、--location（可访问重定向或跳转的主机）。点击执行后，执行结果将在下方面板中显示。

4.8.7.5 调试日志



点击“下载日志”按钮，可选择文件路径，将调试日志下载至指定位置。

4.8.8 服务器管理

服务器管理可设置系统对外开放或对接的各类服务，包括：

- SSH 服务
- SNMP 服务
- 邮件服务
- FTP 服务
- Syslog 服务
- WSUS 服务

4.8.8.1 系统服务

可设置是否开启 SSH 和 SNMP 服务。

- 开启 SSH 服务后，外部终端可以通过 SSH 方式访问系统；
- 开启 SNMP 服务后，系统可以通过 SNMP 方式将自身的可用性信息上报网络管理或安全管理类平台。

4.8.8.2 预警邮件服务器

在本页面可配置预警邮件服务器地址和相关信息。配置后，可以在建立主机漏洞扫描任务时勾选“邮件预警”方式。

- **SMTP 服务器地址**：需要填写邮件服务器地址，并在下拉框中选择邮件服务商。如果下拉框中没有所用的服务商，可选择“其他”。
- **SMTP 服务器端口**：默认为 25，如果自定义修改为其他端口，则需照实填写。此外，如果开启了 SSL 加密通信，也需要开启 SSL。
- **发件箱地址**：需要为漏洞扫描系统配属一个邮件地址，作为发件地址。
- **发件箱密码**：需要为漏洞扫描系统配属一个邮件账号，并键入密码。
- **测试邮箱地址**：提供一个测试的接收邮件的地址，用于测试功能是否正常。

注意：

1、大部分邮件服务器默认是不允许第三方软件直接登录的（如：QQ 等），需要到对应邮件服务器中进行额外设置，部份服务商还只能使用授权码登录(如：QQ)，原密码不允许直接登录。

2、如果配置正确仍然无法正常接收邮件，也有可能是被邮件服务器当作垃

圾邮件过滤掉了，请检查测试邮件是否被投递到了垃圾箱中。

4.8.8.3 FTP 服务器

在本页面可配置 FTP 服务器地址和相关信息。如果产品部署环境中无法连接互联网执行在线升级，且内网中部署了补丁升级 FTP 服务器的话，可以在此页面配置 FTP 服务器相关信息，使漏洞扫描系统和 FTP 服务器完成对接。

- **服务器 IP**：输入 FTP 服务器 IP 地址。
- **端口**：输入 FTP 服务器的端口号。
- **用户名**：输入 FTP 服务的账号。
- **密码**：输入 FTP 服务账号密码。
- **路径**：指明为漏洞扫描升级文件提供的文件路径。
- **测试**：点击测试，测试是否可以连接成功。
- **保存**：点击保存，将 FTP 服务器信息进行保存并生效。

4.8.8.4 Syslog 服务器

本页面可新增并查看 Syslog 日志服务器。如果内网环境中有日志审计系统，或安全管理平台等，需要接收漏洞扫描提供的日志，则需要在此配置 Syslog 服务器信息。

点击新增按钮，可继续配置 Syslog 服务器信息：

- **服务器 IP：**填入 Syslog 服务器地址；
- **协议类型：**选择发送日志的协议方式，默认为 UDP，也可选择 TCP（根据 Syslog 服务器的配置要求）；
- **端口号：**填入 Syslog 服务器接收日志的端口号；

- **发送数据类型**：可选择操作日志和漏洞扫描结果两种；
- **配置保存**：Syslog 服务器信息填好后，可点击保存按钮，将配置信息保存。

4.8.8.5 WSUS 联动

当微软针对 Windows 操作系统发布了更新补丁时，可通过本页面获取到补丁文件和注册表的打包文件，通过一键安装的方式为 Windows 主机更新补丁。

- **服务器地址**：如有 WSUS 服务器，可填写服务器地址。
- **安装方式**：需根据 Windows 主机的更新方式（自动下载并通知安装—提醒安装，或自动下载并计划安装—自动安装），选择对应的安装方式。
- **测试**：可测试系统与 WSUS 服务器是否可连通。
- **下载**：可下载补丁和注册表的打包文件，在目标 Windows 主机上一键执行即可。
- **保存**：保存当前配置。