漏洞扫描系统

用户使用指南

天翼云科技有限公司

前言

本文将覆盖漏洞扫描系统的所有功能点，并详细介绍它的主要功能模块和使用方法。

本手册仅作为使用指导，实际产品可能会由于版本升级或其他原因，与手册描述有略微差异。

修订记录

日期	修订版本	修改记录
2025-01-23	02	内容增加： 1、添加了“产品简介”章节； 2、系统管理下的服务部分新增了“系统升级”、“系统服务”及“用户相关”章节； 功能取消： 1、 任务管理的任务列表中移除了“配置加固”功能； 2、 模板管理下的“缺陷模板”和“加固知识库”功能被取消； 3、 系统管理中去掉了最大使用带宽配置、专业参数配置、WSUS 配置和 syslog 同步设置； 4、 取消了任务配置下的系统加固/回滚并发数配置功能
2024-05-10	01	初次发布。

目录

1 产品简介

漏洞扫描（以下简称 VSS）能够高效、全方位的检测网络中的各类脆弱性风险，全面发现信息系统存在的安全漏洞，并提供专业、有效的安全分析和修补建议。

还支持对 Web 脆弱性进行评估，通过全面模拟网站访问的各种行为，自动获取网站目录和所有页面元素，结合自身完善的检测能力和权威的漏洞知识库输出有效扫描分析报告，为用户提供及时可靠的安全扫描服务。

2 仪表盘

仪表盘，顾名思义就是能够让管理员在一眼能及的视线范围内查看被扫描服务器、主机的各种统计数据，随时了解服务器、主机的安全风险情况。

仪表盘数据来源于所有资产最后一次扫描完后的风险数据分析，漏洞扫描系统根据管理员下发的扫描任务对各服务器、主机执行完扫描任务后，管理员可以通过漏洞扫描系统提供的仪表盘功能，查看目标服务器、主机扫描结果的各种风险统计信息。

系统管理员组通过仪表盘可以查看全局资产统计数据，其他普通管理员通过仪表盘只能查看自己权限范围内资产的统计数据。管理员可以自定义仪表盘上显示的统计信息。

2.1 仪表盘配置

系统管理员组和其他新建普通管理员通过仪表盘配置功能，可以定制仪表盘数据的统计周期和显示内容。系统管理员组可配置全局，新建普通管理员只能配置权限范围内的数据来源。

进入 **仪表盘** > **仪表盘** 页面，单击【配置】按钮，配置仪表盘显示参数即可。参数说明如表 2-1 所示。

表 2-1 仪表盘显示参数

配置项	描述
显示项	仪表盘上显示的项目，系统默认显示全部项目。各项目介绍请参见 仪表盘展示。 说明 单击仪表盘中各显示项右上角的图标，可快速关闭该显示项，若要恢复对显示项的展示，必须在该处进行勾选。
周期粒度	数据统计周期的粒度。可选项有：天、周和月。
周期时间	数据统计周期的时长。根据周期粒度的选择，向前显示最近几天/几周/几个月的统计数据。周期时长不能大于 30。
数据源	仪表盘中统计数据的来源方式。 可选项有：指定资产 IP 范围、从资产树中选择以及从任务列表中选择。
IP 范围	当数据源选择指定资产 IP 范围时，指定数据源的来源 IP 范围。

配置项	描述
	说明 IP 范围必须属于该管理员允许扫描的 IP 范围。
选择资产	当数据源选择从资产树中选择时，指定数据源的来源资产。 说明 资产 IP 必须属于该管理员允许扫描的 IP 范围。
选择任务	当数据源选择从任务列表中选择时，指定数据源的来源扫描任务。 说明 扫描任务中的目标主机地址必须属于该管理员允许扫描的 IP 范围。

2.2 仪表盘展示

仪表盘展示的内容如表 2-2 所示。

表 2-2 仪表盘

统计项	描述
资产风险值	可以查看统计周期和当前权限范围内所有主机的风险值的安全信息和风险值分数。 • 配置风险值：当前所有主机进行配置扫描后的平均配置风险值。 • 整体风险值：当前所有主机配置扫描后的整体风险值，包括配置风险值和漏洞风险值（包括系统漏洞、Web 应用漏洞）。 • 漏洞风险值：当前所有主机进行漏洞扫描（包括系统漏洞、Web 应用漏洞）后的平均漏洞风险值。 单击饼图，在弹出的对话框中，可以查看相应风险等级的所有主机的相应风险值的详情。
主机风险等级分布	可以查看统计周期和当前权限范围内主机的风险等级分布情况。 • 配置风险值等级分布：当前所有主机进行配置扫描后的配置风险等级分布图。 • 整体风险值等级分布：当前所有主机配置扫描后的整体风险等级分布图，包括配置风险和漏洞风险（包括系统漏洞、Web 应用漏洞）。 • 漏洞风险值等级分布：当前所有主机进行漏洞扫描（包括系统漏洞、Web 应用漏洞）后的漏洞风险等级分布图。 鼠标悬停于整体风险等级分布图内时，将显示整体风险的统计百分比、统计样本及安全性。单击饼图，在弹出的对话框中，可以查看相应风险等级的所有统计主机的风险值的详情。
资产风险值趋势	可以查看统计周期和当前权限范围内主机的风险值趋势。 • 配置风险值趋势：当前所有主机进行配置扫描后的配置风险值趋势图。 • 整体风险值趋势：当前所有主机配置扫描后的整体风险值趋势图，包括配置

统计项	描述
	风险和漏洞风险（包括系统漏洞、Web 应用漏洞）。 • 漏洞风险值趋势：当前所有主机进行漏洞扫描（包括系统漏洞、Web 应用漏洞）后的漏洞风险值趋势图。 鼠标悬停于风险值趋势的节点时，将显示节点的风险值及评估日期。单击该节点，在弹出的对话框中，可以查看得出该风险值的所有数据源主机的风险值详情。
资产风险分布趋势	可以查看统计周期和当前权限范围内主机的漏洞分布趋势和不合规检查项分布趋势。 • 鼠标悬停于检查项分布柱状图（左），将显示此风险的风险个数及风险程度（高中低），单击该柱状图，将显示得出该风险值的所有数据源主机的风险值详情。 • 鼠标悬停于漏洞分布柱状图（右），将显示目标主机上漏洞（包括系统漏洞、Web 应用漏洞）的分布个数，单击各个级别的柱状图，将显示该级别漏洞在所有数据源主机上的分布详情。
资产统计-系统类型 TOP10	对存活主机资产的系统类型进行统计；以饼图的方式，展示统计周期内数量最多的 TOP10 系统类型对应的主机资产数量及其占比。
资产统计-开放端口 TOP10	对存活主机资产的开放端口进行统计；以柱状图的方式，展示统计周期内数量最多的 TOP10 开放端口对应的主机资产数量。
资产统计-Web 服务器 TOP10	对存活 Web 资产（站点设备）的服务器类型进行统计；以饼图的方式，展示统计周期内数量最多的 TOP10 Web 服务器类型对应的 Web 资产（站点设备）数量及其占比。
资产统计-组件框架 TOP10	对存活 Web 资产（站点设备）的组件框架进行统计；以柱状图的方式，展示统计周期内数量最多的 TOP10 组件框架对应的 Web 资产（站点设备）数量。
资产统计	以数字的方式，展示当前漏洞库总数和资产 IP 总数。

3 告警管理

告警管理为扫描提供闭环操作，对获取的资产风险进行告警，具体包括漏洞风险、配置不合规检查项、非法的进程以及系统脆弱帐号。

告警整改

在接收到告警后，用户可以查询告警的详细信息，跟踪并参与告警风险的处理，对处理后的风险进行验证，如表 3-2 所示。

表 3-1 告警整改

状态/动作	描述
新建	表示该告警对应的风险尚未被处理。
确认	将新建的告警修改为“确认”状态，表示告警对应的风险确实存在。
误报	将新建的告警修改为“误报”状态，表示该告警已经被资产管理员确认为误报。
忽略	将新建的告警修改为“忽略”状态，表示不对该告警做任何处理直接忽略，被忽略的告警会从告警列表中删除，若没有修改告警配置条件，下次扫描发现后仍会新建一条告警。
已修复	被确认为“确认”的告警，可将告警设置为已修复。
已修正	被确认为“误报”的告警，可将告警设置为已修正。
	可以风险状态为“已修复”或“已修正”的告警，下发整改任务，检测风险是否仍旧存在。

4 资产管理

管理员通过资产管理功能可以对目标网络中的所有信息资产设备进行资产风险管理。根据目标网络的组织结构和网络拓扑，以规范的命名方式映射至漏洞扫描系统的资产树中对网络资产进行统一管理。

资产设备（无论是主机还是站点设备）在资产管理中都是以 IP 地址做唯一标识的。系统管理员 admin 可以对所有资产进行操作，具有资产查看权限的系统管理员或普通管理员只能查看自己权限内的资产，具有资产管理权限的系统管理员或普通管理员只能对自己权限内的资产进行操作。

本章主要介绍漏洞扫描系统设备资产管理的相关信息，主要包括以下内容：

功能	描述
资产视图	介绍如何从逻辑上对资产进行分类管理。
添加资产	介绍如何添加资产设备信息。
资产操作	介绍除添加、查询以外的其他操作。

4.1 资产视图

资产视图用于从逻辑上对资产进行分类管理，目前支持的资产视图如表 4-1 所示。

表 4-1 资产视图

资产视图	描述	可以执行的操作
组织结构视图	按需以组织结构维度管理资产。 需要手动添加节点和资产。添加资产后，评估任务、Web 应用扫描任务、主机资产探测任务 和 Web 资产探测任务（若检测到关联的主机资产） 会将探测到该资产信息刷新至该视图下中。	所有资产管理操作
操作系统视图	按需以操作系统维度管理资产。 需要手动添加节点和资产。添加资产后，评估任务、Web 应用扫描任务、主机资产探测任务 和 Web 资产探测任务（若检测到关联的主机资产） 会将	所有资产管理操作

资产视图	描述	可以执行的操作
	探测到该资产信息刷新至该视图下中。	
设备类型视图	以设备类型维度管理资产。漏洞扫描系统提供默认的视图节点，不支持修改。 漏洞扫描系统自动获取 评估任务、主机资产探测任务 和 Web 资产探测任务 （若检测到关联的主机资产）探测到的资产并添加至该视图下；可以查看探测到的资产信息。	仅支持“刷新资产树”操作

4.2 添加资产

资产树由网络节点、已登记设备和未登记设备组成。资产中的设备来源于历史扫描任务和用户添加，用户添加的设备为已登记设备（可以编辑管理信息），未登记的设备可以通过登记设备进行登记。

网络节点从逻辑上对资产设备进行管理，管理资产时，需要添加网络节点后，才能添加资产设备。

4.3 添加网络节点

进入 **资产管理 > 资产管理** 页面，弹出添加父/子网络节点对话框（如下方式），配置参数即可。网络节点参数的说明如表 4-2 所示。

- 添加父网络节点：单击【操作 > 添加节点】按钮。
- 添加子网络节点：鼠标悬停于父网络节点，单击图标。

表 4-2 节点参数

配置项	描述
节点名称	网络节点的名称，最多可输入 40 个字符。
IP 范围	网络节点的 IP 地址范围，支持 IPv4 地址和 IPv6 地址。
节点管理员	该网络节点的管理员，最多可输入 30 个字符。
邮箱	该网络节点管理员的邮箱，若填写多个邮箱请用逗号分隔，最多可填写 5 个电子邮箱地址。
备注	该网络节点的备注信息。

4.4 添加资产设备

进入 **资产管理 > 资产管理** 页面，弹出添加设备对话框（如下方式），配置参数即可。设备参数的说明如表 4-3 所示。

- 根目录下添加设备：单击【操作 > 添加设备】按钮。
- 网络节点下添加设备：鼠标悬停于父网络节点，单击图标。

表 4-3 设备参数

配置项	描述
设备名称	资产设备的名称，最多可输入 40 个字符。
IP 地址	资产设备的 IP 地址，支持 IPv4 地址和 IPv6 地址。
设备添加到	管理节点可以理解为上级网络节点，根节点可以理解为最顶层的网络节点。 举例说明选择管理节点和根节点的区别：添加设备的 IP 地址是 1.1.1.1，系统中一个网络节点的 IP 范围是 1.1.1.*，另一个网络节点的 IP 范围是*.*.*.*。此处若选择管理节点，则设备添加到网络节点 1.1.1.*下；若选择根节点，则设备添加到网络节点*.*.*.*下。
操作系统	该资产的操作系统类型。
权重	主机和网络风险等级计算时所采用的变量，权重越高资产越重要，计算出来的风险等级越高。
设备管理员	该资产设备的管理员，最多可输入 30 个字符。
邮箱	该资产设备管理员的邮箱，若填写多个邮箱请用逗号分隔，最多可填写 5 个电子邮箱地址。
备注	该资产设备的备注信息。
配置认证信息	具体请参见 认证管理。

4.5 资产操作

添加网络节点和资产设备后，还可以对其进行查询、修改、删除和如表 4-4 所示的操作。

表 4-4 资产设备操作

类别	操作	含义
资产树	导入资产树	导入资产树将覆盖原有资产树并清空所有资产数据。进入 **资产管理 > 资产管理** 页面，单击【操作 > 导入资产树】按钮，选择资产树文件即可。 说明 资产树模板的获取方式：请先导出资产树，在导出文件的格式上进行编辑后，保存为需要导入的资产树文件。

类别	操作	含义
	导出资产树	单击【操作 > 导出资产树】按钮，将资产树保存至本地。
	清空资产树	单击【操作 > 清空资产树】按钮，勾选需要删除的资产树信息即可。 • 清空管理节点和主机资产的基本信息 • 清空与资产关联的登录认证信息 • 清空与资产关联的配置检查信息
	刷新资产树	将当前扫描任务的结果数据刷新至资产管理中。
网络节点或资产设备		修改网络节点或资产设备的信息。
		删除网络节点或资产设备。
		下达评估任务，扫描目标是当前网络节点或当前资产设备，新建评估任务的具体步骤请参见 新建任务。
	单击网络节点/资产设备	查看资产报表，具体请参见 资产报表。
资产设备		登记当前资产设备为可以管理。
		取消登记当前资产设备。

5 任务管理

任务是漏洞扫描系统设备主动对网络中的资产进行漏洞检测、配置检查、脆弱帐号猜测的依据。

本章主要介绍任务管理的相关信息，主要包括以下内容：

功能	描述
新建任务	介绍新建各类任务的详细信息。
任务列表	介绍查看漏洞扫描系统任务列表的详细信息。

5.1 新建任务

漏洞扫描系统的任务分为远程扫描和本地配置扫描任务，下面分别介绍新建各种任务的详细步骤。

除口令猜测任务外，扫描任务包括系统默认任务和自定义任务两类。新建任务时，只配置扫描目标、其他配置项均保持默认值，则该任务为系统默认任务。

5.1.1 远程扫描（选择任务类型）

漏洞扫描系统系统通过快速选择任务类型，远程对在线目标进行漏洞（系统漏洞和 Web 应用漏洞）、配置合规和脆弱帐号检查，然后在线展示检查结果。

5.1.1.1 评估任务

评估任务可以对扫描目标进行漏洞扫描和主机的配置扫描，能够发现扫描目标中存在的漏洞（系统漏洞）以及主机配置不合规信息。同时可以将网络安全评估结果发送至指定邮箱或 FTP 服务器中，提醒管理员进行修复。并支持直接输出任务报表，方便管理员下载后分析资产风险。

进入 **新建任务** 页面，选择 **评估任务**，配置任务参数即可创建一个任务。评估任务参数的说明如表 5-1、表 5-3、表 5-3、表 5-5 和表 5-6 所示。

表 5-1 基本选项参数

配置项	描述
扫描目标	支持通过如下方式配置扫描目标设备，最多可输入 10000 行扫描目标信息。 • IP：多个 IP 范围或独立 IP 之间使用“,”、“;”、回车、空格分隔。如果 IP 地址前加“!”，表示不扫描该 IP 或 IP 段。具体请参见界面的。 • 域名：域名格式如 www.example.com，多个域名之间使用“,”、“;”、回车、空格分隔。若扫描的域名都指向同一个 IP 地址，还需选中“虚拟主机”。具体请参见界面的。 • 资产树导入：单击【从资产树导入】，在弹出的对话框中选择扫描目标。 • 文件导入：单击【浏览】按钮，选择导入文件，单击【导入】按钮，完成从文件导入扫描目标信息。支持导入 txt 文本中的 IP 地址，txt 文本内容的格式同 IP 地址。
任务名称	扫描目标确定后，系统会自动定义任务名称，用户也可以自行定义任务名称。取值范围为 1~256 个字符。
执行方式	• 立即执行：即时评估任务。需要立即进行网络安全评估时，可以下达即时评估任务。 • 定时执行：定时评估任务。需要避开业务高峰期对网络进行安全评估时，可以下达定时评估任务。 • 每天一次、每周一次、每月一次（按日期）或每月一次（按星期）：周期评估任务。需要定期（每天、每周或每月）对网络系统做安全评估时，可以下达周期评估任务。 • 高级配置：配置【周期时间】，单击图标，选择多个时间段执行周期扫描任务。
漏洞模板	在漏洞模板下拉列表框中，选择用于漏洞扫描的漏洞模板。 • 若选择“自动匹配扫描”，则对所有漏洞模板进行匹配扫描。 • 若选择“无模板”，则不做漏洞扫描。 • 若选择“网络信息收集”，则漏洞扫描系统仅进行网络信息的收集，不执行漏洞配置扫描。 • 若选择“全量信息收集模板”，则漏洞扫描系统仅对安装 Agent 的目标机进行信息收集，不执行漏洞配置扫描。 单击文字链接【漏洞模板管理】，弹出 漏洞模板 页面，可以配置及查看漏洞模板。
自动漏洞验证	启用后，通过 POC 漏洞验证原理，使用可验证漏洞扫描模板，比较准确的验证资产中是否存在漏洞。
全量 Agent 扫描	目标机安装 Agent 后，Agent 每间隔 4 小时向漏洞扫描系统/平台上报一些目标机的信息；启用“全量 Agent 扫描”后，漏洞扫描系统仅对最新上报的信息进行漏洞扫描。
扫描时间段	无论任务是何种执行方式，漏洞扫描系统只能在该时间段内执行扫描任务。
调度优先级	漏洞扫描系统根据调度优先级数值和后台算法判断执行任务的顺序。

表 5-2 基本选项-登录检查

配置项	描述
漏洞登录检查	登录扫描目标检查是否存在系统漏洞。
配置登录检查	登录扫描目标检查是否存在配置不合规项。 • 精确核查：通过具体的配置模板检查扫描目标是否存在配置不合规项。 • 智能核查：仅支持“系统管理员”角色的帐号进行配置，通过配置模板行业进行信息探测并自动核查扫描目标是否存在配置不合规项。 • 信息收集：仅支持“系统管理员”角色的帐号进行配置，对扫描目标的系统环境进行探测。
批量登录测试	批量登录已添加的目标主机，测试目标主机是否存活。
启用 SSH 免密登录	• 不启用：漏洞扫描系统通过使用用户名和密码来登录任务中所需登录的目标机或跳板机。 • 启用：漏洞扫描系统通过使用统一密钥对来登录任务中所需登录的目标机或跳板机。启用前，需要配置导入密钥对，可以单击文字链接【点击设置】，跳转至任务配置页面，进行 ssh 密钥导入操作；启用后，在添加主机认证信息时，无需配置登录密码。

表 5-3 基本选项-登录检查-主机认证信息参数

项目	配置项	描述
【添加】/【导入】	-	启用“登录检查”后，漏洞扫描系统登录检查模块会自动读取认证管理中的主机认证信息。 • 可以通过手动添加和导入的方式添加主机认证信息。 • 漏洞扫描系统不会导入不在扫描目标范围内的主机认证信息。 • 可以【导出】主机认证信息至本地保存。
基本信息	IP	扫描目标的 IP 地址或地址段信息。 扫描目标的 IP 必须在扫描目标参数范围内。
	用户名/密码	预登录扫描目标的用户名和密码。漏洞扫描系统使用系统内加密存储，保证信息安全。
	获取	单击【获取】按钮，从与漏洞扫描系统设备联动的堡垒机上获取主机登录密码。 堡垒机联动配置请参见 认证管理配置。
	登录协议/登录端口	登录扫描目标使用的登录协议和端口信息。 HTTP、HTTPS 和 WinRM 协议仅支持进行配置核查，不支持进行漏洞扫描。
	主机跳转	适用于漏洞扫描系统可以直接或使用相同的跳板机登录目标机的场景。若多个目标机使用同一个跳板机进行跳转登录，则启用“跳板机设置”后，可以进行统一的跳板机配置。 • 在漏洞扫描系统不能直接登录目标主机时，可以使用跳转主机进行扫描，需要预先配置跳转主机的认证信息。

项目	配置项	描述
		• 需要保证跳转主机能够连接到目标主机。 • 只有在通过 SSH、Telnet 方式登录目标主机时，才能配置主机跳转功能。
	登录路径/站点 Cookie	通过 HTTP 或 HTTPS 来登录扫描目标时，需要配置登录路径和预设用来记录登录会话标识的站点 Cookie。 单击【登录预录制】按钮，按照相应提示进行浏览器的代理配置、抓取 Cookie 即可。如果目标站点需要软证书，则需要先导入软证书再进行登录预录制。
	登录验证	单击【登录验证】按钮，可以验证登录信息是否正确，保证漏洞扫描系统可以登录至目标主机进行本地扫描。
状态模板	状态模板	不视为不合规项的白名单信息。 单击【状态模板管理】，进入状态模板列表页面。如何新建状态模板请参见 状态模板。
认证	同步到认证管理	启用后，会覆盖 认证管理中相同 IP 地址的主机认证信息。

表 5-4 基本选项-口令猜测参数

配置项	描述
口令猜测	启用口令猜测后，单击【详细配置】，配置口令猜测参数。 • 漏洞扫描系统通过脆弱帐号成功登录目标主机后，会执行本地漏洞扫描。 • 若未对主机进行登录扫描，漏洞扫描系统将根据 密码字典 的内容对扫描目标进行口令破解。只有存活的主机才可以执行口令猜测任务。
服务类型	选择需要口令猜测的协议，标准模式是用户名和密码使用同一个字典，组合模式是用户名字典和密码字典组合使用。 说明 单击【密码字典管理】，可以对默认密码字典进行编辑。 口令猜测顺序以密码字典里的用户名或密码顺序为准，先猜用户自定义密码字典，然后猜系统默认密码字典。 启用口令猜测有可能导致某些主机帐户因扫描中多次登录失败而被锁定，请谨慎启用。
口令猜测时间	一个口令猜测插件的最长运行时间，达到设定的时间则该插件终止运行。
口令猜测频率	对相同目标的相同协议的相邻口令猜测的时间间隔。
猜测次数	对单个资产设备进行口令猜测的次数，0 表示不限制猜测次数。
最大并发线程数	对单个服务进行口令猜测时的并发线程个数。值越大，探测速度越快。

表 5-5 任务报表参数

配置项	描述
报表类型	生成报表的类型，支持 HTML、Word、Excel、PDF、XML 格式。
报表内容	• 综述报表：从整体上对评估任务进行综合分析、风险描述和分类展示，并根据不同视角出具漏洞统计图表、操作系统分布、帐号信息和评估标准等。 • 主机报表：针对单个主机进行风险分析和详细描述。包括单个主机的扫描数据的统计信息、各种 Profile 信息、漏洞列表与解决方案等。若需要分析扫描任务中出现的问题，请生成主机报表。
综述/主机报表模板	如果没有合适的报表模板，可以单击“报表模板管理”链接，进入报表模板页面后，添加报表模板，具体请参见 报表模板。
自动生成报表	• 启用后，任务结束时，生成指定类型的离线报表，并根据配置发送报表。此外，生成的离线报表将保存至 报表列表 中。 • 无论是否启用“自动生成报表”，任务结束时，都自动生成 HTML 格式的在线报表，具体内容请参见 评估任务报表。
FTP 上传	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动将离线报表上传到指定的报表 FTP 服务器。此时需要配置报表 FTP 服务器，具体操作请参见 报表 FTP 设置。
发送报表	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动向指定的电子邮箱发送离线报表，此时需要配置邮件服务器，具体操作请参见 邮件服务器设置。 • 报表类型：报表文件的格式。 • 邮箱地址：接收报表的电子邮箱地址，支持配置 5 个以内的电子邮箱地址，多个电子邮箱地址之间使用“,”、“;”、回车、空格分隔。

表 5-6 高级选项参数

功能	配置项	描述
端口扫描	端口扫描策略	• 标准端口扫描：只扫描 端口列表 中记录的端口。 • 快速端口扫描：只扫描 1~1024 端口。 • 指定端口范围：只扫描指定的端口。 • 全端口扫描：扫描所有端口。 说明 全端口扫描发包量较大，请在不会影响网络环境时使用。
	端口扫描速度	扫描速度越慢，获取的端口开放信息也将会越准确，同时花费时间可能就会越长。
	TCP 端口扫描方式	CONNECT：通过直接建立完整的 TCP 连接来判断端口开放情况，此方法快而准确。 SYN：向目标端口发送 SYN 包，依据对方是否回复 ACK 报文来判断端口开放情况。

功能	配置项	描述
	UDP 扫描	只有选中此项，在 端口列表 中定义的 UDP 端口才会被扫描。启用 UDP 扫描将会大大增加扫描时间，因此不建议选择此项。
主机存活测试	主机存活测试	勾选启用后，还需设置存活测试使用的具体方法和测试端口。
	存活探测速度	存活探测速度越慢，获取的主机存活信息也将会越准确，同时花费时间可能就会越长。
扫描限制	扫描深度	设置评估任务的扫描深度，值越大，插件获取的信息可能就越多，扫描时间越长。 建议使用缺省配置。
	插件超时限制	单个插件在指定时间内如果未正常结束，将会被调入引擎终止。 单位为秒，取值范围为 1～300 秒。
	Socket 超时限制	从网络层读数据时，等待的最大超时值。 此选项对扫描速度和准确度有较大影响，局域网建议 5 秒，ADSL 建议 15 秒。 可视网络速度情况设置 Socket 超时限制，若网速慢，则 Socket 超时限制需要设置得久一些。
其他	危险插件扫描	此类插件可能导致系统崩溃或服务中断，通常情况下不建议使用，只有在特定情况下启用（例如：产品评测）。
	扫描前提示被扫描主机	勾选后，在扫描前将在主机中弹出提示信息，用户可按照需要修改提示信息的内容。 说明 被扫描主机开启 Messenger 服务才能收到扫描通知消息。
	深度扫描重要网络设备	启用此功能可能导致某些特定型号的网络设备在扫描中出现故障，请谨慎启用。
	扫描调度忽略插件依赖关系	通常情况下，不建议选择此项。 漏洞扫描系统内部不同插件有不同分工，例：1 号插件负责判断目标操作系统类型，2 号插件负责扫描 Windows 系统的某一漏洞，那么如果 2 号插件依赖于 1 号插件的扫描结果，则在 1 号插件发现目标系统不是 Windows 时引擎可以直接跳过对 2 号插件的调度，从而提高扫描速度和扫描准确度。
	Openssh 版本扫描	通常情况下，不建议选择此项。 启用后，漏洞扫描系统对 OpenSSH 进行版本扫描。
	NTP 远程版本扫描	• 启用：对 NTP 进行远程版本扫描。 • 不启用：不对 NTP 进行远程版本扫描。
	Oracle 漏洞深度扫描	• 不勾选：漏洞扫描系统只报出 oracle 相关服务识别和原理扫描漏洞。 • 勾选：漏洞扫描系统报出所有漏洞，包括本地 oracle 漏洞。此时需要 手动新建认证信息，启用并配置漏扫

功能	配置项	描述
		策略的 Oracle 相关参数。
	调试模式	预防出现扫描任务异常时，可以配置该参数。记录扫描任务的执行信息，当任务执行异常，导出异常信息并发送给公司的技术支持人员进行错误分析。
语言编码	目标系统使用的语言编码	目标系统使用的语言编码，可选项有：简体中文（GBK）和 Unicode（UTF-8）。

5.1.1.2 口令猜测任务

可以对存活的主机执行口令猜测任务。漏洞扫描系统使用 密码字典 中的用户名和密码登录目标主机，若登录成功说明目标主机中存在脆弱帐号。

进入 **新建任务** 页面，选择 **口令猜测任务**，配置参数即可新建一个口令猜测任务。口令猜测任务参数的详细信息如表 5-1、表 5-4、表 5-6 所示。

5.1.1.3 Web 应用扫描任务

漏洞扫描系统的 Web 应用扫描功能为用户的互联网网站提供远程安全扫描和安全检查，能够根据站点管理者的监管要求，对目标站点进行不间断的页面爬取、分析、匹配，为构建安全的网站提供完善的监测方案。

进入 **新建任务** 页面，选择 **Web 应用扫描**，配置任务参数即可创建一个任务。Web 应用扫描任务参数的说明如表 5-7、表 5-8、表 5-9、表 5-10、表 5-11、表 5-12、表 5-13 和表 5-14 所示。

表 5-7 Web 应用扫描任务 - 基本参数

配置项	描述
扫描目标	支持通过如下方式配置扫描任务的扫描目标，建议每行只输入一个扫描目标，具体请参见界面的。 • 手动输入扫描目标。 • txt 文件导入：单击【浏览】按钮，选择导入文件，单击【导入】按钮，导入扫描目标。txt 文本文件中每行只能输入一个扫描目标。 内容格式如下： • 仅支持 HTTP 和 HTTPS 协议的 URL。 • 多个 URL 之间使用“,”、“;”、回车、空格分隔。 • 若进行目录限制扫描，则需要输入完整的限制目录，如 http://www.example.com/test/。 • 格式示例： http://fe80::1a03:73ff:feaf:8b3c:8080 https://[fe80::]:8080 https://www.test.com https://192.168.1.1
任务名称	扫描目标确定后，系统会自动定义任务名称，用户也可以自定义任务名称。

配置项	描述
	取值范围：1~256 个字符。
扫描范围	爬虫并扫描的范围。 • 按域名扫描： – 整站扫描：扫描父域名及子域名下的所有 URL。 – 扫描子域名：只扫描父域名及此处配置的子域名下的所有 URL，不扫描其它子域名。 – 不扫描子域名：不扫描此处配置的子域名，只扫描父域名及其它子域名下的所有 URL。 • 扫描当前目录及子目录：扫描“扫描目标”及所有子目录中的 URL。 • 只扫描任务目标链接：只扫描“扫描目标”中的 URL。
执行方式	• 立即执行：即时任务。需要立即进行 Web 应用扫描时，可以下达即时任务。 • 定时执行：定时任务。需要避开业务高峰期对站点进行扫描时，可以下达定时任务。 • 每天一次、每周一次、每月一次（按日期）或每月一次（按星期）：周期任务。需要定期（每天、每周或每月）对站点进行扫描时，可以下达周期任务。 • 高级配置：配置【周期时间】，单击图标，选择多个时间段执行周期任务。
任务最大运行时长	扫描一个站点最长时间限制，范围为-1、60（1 小时）~525600（365 天）的正整数，-1 表示不限制。
漏洞模板	在下拉列表框中选择用于扫描的漏洞模板。漏洞模板的相关操作请参见 漏洞模板。可选项有：自动匹配扫描、系统默认模板和当前管理员有权加载的自定义模板。 • 若选择“自动匹配扫描”，则对所有漏洞模板进行匹配扫描。 • 若选择“可验证漏洞扫描”，则仅对漏洞扫描系统支持验证的漏洞进行扫描；若扫描结果中存在相应的漏洞，则管理员可以对漏洞执行操作。 • 若其他模板中包含漏洞扫描系统支持验证的漏洞，且扫描结果中存在相应的漏洞，则管理员可以对漏洞执行操作。
自动漏洞验证	启用后，通过 POC 漏洞验证原理，使用可验证漏洞扫描模板，比较准确的验证资产中是否存在漏洞。
扫描时间段	无论任务是何种执行方式，漏洞扫描系统只能在该时间段内执行扫描任务。
调度优先级	漏洞扫描系统根据调度优先级数值和后台算法判断执行任务的顺序。
调试模式	预防出现扫描任务异常时，可以配置该参数。记录扫描任务的执行信息，当任务执行异常，导出异常信息并发送给公司的技术支持人员进行错误分析。

表 5-8 Web 应用扫描任务 - 认证参数

配置项	描述
扫描目标	与表 5-7 中的扫描目标保持一致。
协议认证	扫描目标使用的认证协议，可选项有：自动识别、NTLM 认证、BASIC 认证或 Digest-MD5 认证。
登录扫描	启用后，漏洞扫描系统会使用配置的登录信息来登录扫描目标进行扫描。

配置项	描述
	• 若选择预设 Cookie，则需要设置用来记录登录会话标识的 Cookie。例：action=login&username=admin&password=admin88 • 若选择登录预录制，则需要单击【开始录制】按钮，然后按照弹出对话框的内容进行操作，漏洞扫描系统会记录相关的 Cookie 信息。
自定义链接	强制指定必须扫描的 URL，可以是外部链接。多个 URL 之间使用“,”、“;”、回车、空格分隔。
排除链接	执行 Web 应用扫描任务过程中，无需爬取的 URL。
表单填充	执行 Web 应用扫描任务过程中，当页面中存在表单时，是否对表单进行填充，以获取更多的 URL，从而发现更多的漏洞信息。 启用后，需要配置填充项信息。单击  ，添加填充项。

表 5-9 Web 应用扫描任务 – 代理参数

配置项	描述
代理类型	代理服务器的类型，可选项：SOCKS 4、SOCKS 5、HTTP。
协议认证	代理服务器使用的认证协议，可选项：NTLM、Basic、Digest-MD5。
服务器地址/端口	代理服务器 IP 地址/端口号，服务器地址可以是 IP 地址或域名。
用户名/密码	代理服务器的登录用户名和密码。必须同时配置用户名和密码。
【连通测试】	测试与代理服务器是否连接正常。

表 5-10 Web 应用扫描任务 - 任务报表参数

配置项	描述
报表类型	生成的报表的类型，支持 HTML、Word、Excel、PDF 格式。
报表内容	• 综述报表模板：从整体上对任务进行综合分析、风险描述和分类展示，并根据不同视角出具风险统计图表、漏洞分布和参考标准等。 • 单站点报表模板：针对单个站点进行风险分析和详细描述。包括单个站点的风险分类统计、Web 风险分布、漏洞详情等。若需要分析扫描任务中出现的问题，请生成单站点报表。
综述/单站点报表模板	如果没有合适的报表模板，可以单击“报表模板管理”链接，进入报表模板页面后，添加报表模板，具体请参见 报表模板。
自动生成报表	启用后，任务结束时，生成指定类型的离线报表，并根据配置发送报表。此外，生成的离线报表将保存至 报表列表 中。 无论是否启用“自动生成报表”，任务结束时，都自动生成 HTML 格式的在线报表，具体内容请参见 Web 应用扫描任务报表。
FTP 上传	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动将离线报表上传到指定的报表 FTP 服务器。

配置项	描述
	此时需要配置报表 FTP 服务器，具体操作请参见 报表 FTP 设置。
发送报表	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动向指定的电子邮箱发送离线报表，此时需要配置邮件服务器，具体操作请参见 邮件服务器设置。 • 报表类型：报表文件的格式。 • 邮箱地址：接收报表的电子邮箱地址，支持配置 5 个以内的电子邮箱地址，多个电子邮箱地址之间使用“,”、“;”、回车、空格分隔。

表 5-11 Web 应用扫描任务 – Web 扫描选项&Web 访问策略参数

配置项	描述
扫描级别	• 深度扫描：扫描插件调用所有检测逻辑，耗时较长。 • 快速扫描：扫描插件不会调用耗时严重的检测逻辑，耗时较短。 • 智能扫描：耗时一般。
并发线程数	进行 Web 应用扫描时，Web 扫描插件的并发扫描线程数，数值越大，扫描速度越快。 说明 配置并发线程数需要考虑网络带宽以及服务器的处理能力，过大的数值会影响目标服务器的正常运行。
超时限制	扫描一个页面的最长时间限制。
请求失败重试次数	扫描请求发送失败后重试的次数。
网页编码方式	为了能够正常访问扫描目标，需要正确匹配扫描目标中网页的编码方式。 • 自动检测：自动匹配网页的编码方式。 • 手动检测：手动指定扫描目标的网页编码方式。可选项为：简体中文（GB18030）、BIG5、Unicode（UTF-8）。
自定义 User-Agent	执行 Web 应用扫描任务时，使用指定的浏览器或搜索引擎访问扫描目标。启用该参数后，才可在文本框中进行编辑。
自定义 header	在爬取和扫描的时候可以使用自定义的请求 header。单击，可以添加自定义 header。 适用于特定站点必须要有特定的 header 才能检测到漏洞的情况。

表 5-12 Web 应用扫描任务 - Web 检测策略参数

配置项	描述 （扫描目标中存在一些无法爬虫到的敏感文件时，可以通过 Web 检测对其进行安全扫描。）
目录猜测范围	每个目录下常见敏感目录、敏感文件的猜测范围。

配置项	描述 （扫描目标中存在一些无法爬虫到的敏感文件时，可以通过 Web 检测对其进行安全扫描。）
	• 0 表示不猜测。 • 范围值越大，猜测的范围越广，可能猜测出的目录、文件越多，但是扫描时间会更长。
目录猜测深度	敏感目录、敏感文件的猜测层次深度，该参数值不能大于“目录深度”的参数值。 说明 “目录深度”的说明请参见表 5-13。
备份文件检查类型	需要检查哪些类型的文件中存在备份文件，多个类型之间用“,”分隔。
备份文件检查扩展名	备份文件的扩展名，与“备份文件检查类型”配合使用，多个类型之间用“,”分隔。
自定义弱口令	用于检测站点是否存在弱口令。 • 单击，可以添加自定义弱口令。 • 支持【导入】.txt 格式的弱口令文件。

表 5-13 Web 应用扫描任务 - Web 爬行策略参数

配置项	描述
爬行顺序	扫描过程中采取的 URL 获取方式。
单目录文件数	当选择链接消重时，每个目录下被扫描的文件个数的最大值。 取值范围大于等于-1 的整数，“-1”表示不限制。
目录深度	扫描时，爬虫获取的目录层次深度。 • “-1”表示不限制。 • 目录层次深度：从根目录开始，在 URL 中第几个“/”就是第几层。目录层次深度的数值越大，扫描越深入，消耗的时间越长，因此需要适当限制目录层次深度。
链接总数	限制获取到的 URL 的总个数。取值范围大于等于-1 的整数，“-1”表示不限制。
排除后缀	指定爬虫在爬取时，无需爬取的文件后缀，由数字和字母组成，多个后缀之间使用英文逗号隔开。
区分大小写	在扫描过程中是否区分 URL 的大小写字母。
解析 Flash 文件	是否开启 Flash 相关扫描，目前只支持解析 Flash 10 以下的版本。
执行 JavaScript	爬取页面时，是否执行页面中的 JavaScript 脚本代码以获取 URL。 • 是：表示需要执行 javascript 代码，并且模拟触发各类事件。 • 否：表示禁止执行 javascript 代码，这样会提高扫描速度，但是会有部分 URL 不被爬取。

配置项	描述
链接消重策略	指定 URL 消重策略的等级。 一般来说，一个 URL 地址由一个五元组（page，method，query-name，query-value，post-data）组成，消重策略的等级指定了对 URL 地址五元组中的哪些元素敏感，从而区分不同 URL 地址。 以 URL：http://www.test.com/test.php?login=admin 为例： • page=http://www.test.com/test.php（page=协议+域名+路径文件） • method=GET • query-name=login • query-value=admin • post-data=NULL 那么对于消重等级来说： • 0：对 page 敏感 • 1：对 page，method 敏感 • 2：对 page，method，query-name 敏感 • 3：对 page，method，query-name 和 query-value 敏感 • 4：对 page，method，query-name，query-value 和 post-data 敏感 消重等级越高，则 URL 地址的相同因素就要越多，当设定等级为 0 时，只要两个 URL 的 page 相同，就认定这两个 URL 是同一个 URL，无需再考虑后续的参数值。

表 5-14 渲染爬取策略

配置项	描述
模拟浏览器渲染页面	开启该选项后，爬虫会模拟人类的交互智能分析爬取页面。
并发页面数	限制渲染爬虫并发页面的个数，不同设备对应的数量也不同。 • 硬件设备：E 型号和 H 型号是 1-5，S 型号是 1-2 • 虚拟化设备：根据内存不同，8G 以下无此选项，8G 以上 16G 以下是 1-2, 16G 及以上是 1-5

5.1.1.4 配置扫描任务

配置扫描任务能够发现扫描目标中存在安全配置不合规信息。同时可以将扫描结果发送至指定邮箱或 FTP 服务器中，提醒管理员进行修复。并支持直接输出任务报表，方便管理员下载后分析资产安全配置存在的风险。

进入 **新建任务** 页面，选择 **配置扫描**，配置任务参数即可创建一个任务。配置扫描任务参数的说明如表 5-1、表 5-3、表 5-3、表 5-5 和表 5-6 所示。

5.1.1.5 镜像扫描任务

暂未开启此功能

镜像扫描任务能够发现 Docker 镜像文件中存在的系统漏洞和配置不合规项。目前每个镜像扫描任务仅支持对 3 个镜像标签进行扫描。

进入 **新建任务** > **镜像扫描** 页面，配置镜像扫描任务参数即可。镜像扫描任务参数如表 5-15 所示。

表 5-15 镜像扫描任务参数

配置项	描述
扫描目标	镜像扫描：镜像扫描多用于扫描公有仓库中的镜像标签。 镜像标签：对于镜像标签的配置要求请参见界面中的描述。
	仓库扫描：多用于扫描私有仓库中的镜像标签。 • 仓库地址：仓库的地址，格式要求请参见界面中的描述。 • 仓库用户名/仓库密码：登录仓库的用户名和密码。 • 仓库类型：仓库的类型，目前仅支持“docker_v2”。 • 【获取镜像列表】：在镜像列表中展示仓库中存放的镜像标签。
任务名称	扫描目标确定后，系统会自动定义任务名称，用户也可以自行定义任务名称。取值范围为 1~256 个字符。
执行方式	• 立即执行：即时镜像扫描任务。需要立即进行镜像扫描时，可以下达即时镜像扫描任务。 • 定时执行：定时镜像扫描任务。需要避开业务高峰期对镜像进行扫描时，可以下达定时镜像扫描任务。 • 每天一次、每周一次、每月一次（按日期）或每月一次（按星期）：周期镜像扫描任务。需要定期（每天、每周或每月）对镜像进行扫描时，可以下达周期镜像扫描任务。 • 高级配置：配置【周期时间】，单击图标，选择多个时间段执行周期扫描任务。
漏洞扫描	是否对镜像进行漏洞扫描。
配置扫描	是否对镜像进行配置合规扫描。单击文字链接【查看镜像配置模板】，弹出查看模板对话框，可以查看漏洞扫描系统提供的镜像配置核查模板。
调度优先级	漏洞扫描系统根据调度优先级数值和后台算法判断执行任务的顺序。

5.1.1.6 代码审计任务

暂未开启此功能

代码审计任务能够发现代码文件中存在的安全缺陷和不符合编码规范的内容。

进入 **新建任务** 页面，选择 **代码审计**，配置代码审计任务参数即可创建一个任务。代码审计任务参数的说明如表 5-16 所示。

表 5-16 代码审计参数

配置项	描述
任务名称	代码审计任务的名称。取值范围为 1~256 个字符。
代码来源	手动上传：对本地的代码文件进行安全缺陷和编码规范进行审计。
	SVN 获取：对 SVN 仓库中的代码文件进行安全缺陷和编码规范进行审计。 • 认证方式：目前仅支持“密码”方式。 • 仓库地址：存放代码文件的 SVN 的 URL 路径，格式要求请参见界面。 • 用户名/密码：登录仓库地址的用户名和密码。 • 【连通测试】：单击按钮后，可以测试漏洞扫描系统与仓库的连接是否正常。
	GIT 获取：对 GIT 仓库中的代码文件进行安全缺陷和编码规范进行审计。 • 仓库地址：存放代码的 GIT 地址，格式要求请参见界面。 • 认证方式：从 GIT 获取代码文件的登录认证方式，不同认证方式配置的参数不同。 – 用户名/密码（密码方式）：登录仓库地址的用户名和密码。 – 密钥（密钥方式）：通过密钥登录仓库地址。 – TOKEN（TOKEN 方式）：通过 TOKEN 认证登录仓库地址。 – 无：无需认证方式，即可登录仓库地址。 • 【连通测试】：单击按钮后，可以测试漏洞扫描系统与仓库的连接是否正常。
缺陷模板	请根据代码文件的语言或内容，选择合适的缺陷模板进行审计。
执行方式	• 立即执行：即时代码审计任务。需要立即进行代码审计时，可以下达即时代码审计任务。 • 定时执行：定时代码审计任务。需要避开业务高峰期对镜像进行扫描时，可以下达定时代码审计任务。 • 每天一次、每周一次、每月一次（按日期）或每月一次（按星期）：周期代码审计任务。需要定期（每天、每周或每月）对镜像进行扫描时，可以下达周期代码审计任务。 • 高级配置：配置【周期时间】，单击图标，选择多个时间段执行周期扫描任务。
调度优先级	漏洞扫描系统根据调度优先级数值和后台算法判断执行任务的顺序。
不扫描文件	不需要对仓库中的“不扫描文件”进行审计。
不扫描文件夹	不需要对仓库中的“不扫描文件夹”进行审计。
任务说明	对代码审计任务的备注说明。取值范围为 0~256 个字符。

5.1.1.7 主机资产探测任务

暂未开启此功能

主机资产探测支持探测主机的存活、开放端口、服务应用等相关信息。探测到资产信息将自动记录至设备类型视图，同时更新组织架构视图和操作系统视图中的已有资产信息。

进入 **新建任务** 页面，选择 **主机资产探测**，配置主机资产探测任务参数即可创建一个任务。主机资产探测任务参数的说明如表 5-1、表 5-5、表 5-6 和表 5-17 所示。

表 5-17 主机资产探测任务

页面	配置项	描述
基本选项	扫描模板	在下拉列表框中，选择用于扫描的资产标记模板。
	关联 Web 资产探测	若主机开放 Web 端口（即存在 Web 应用），则漏洞扫描系统会同时探测并记录 Web 资产（站点设备）的相关信息。
高级选项	关键页面总数	仅支持配置为“1”，表示仅对主机资产已开放的 Web 端口对应的 URL 进行探测。

5.1.1.8 Web 资产探测任务

暂未开启此功能

Web 资产探测支持探测 Web 站点的组件框架、title、logo 等信息。探测到资产信息将自动记录至设备类型视图，同时更新组织架构视图和操作系统视图中的已有资产信息。

进入 **新建任务** 页面，选择 **Web 资产探测**，配置 Web 资产探测任务参数即可创建一个任务。Web 资产探测任务参数的说明如表 5-7、表 5-10 和表 5-18 所示。

表 5-18 Web 资产探测任务

页面	配置项	描述
基本选项	关联主机探测	启用后，会将探测到的 Web 资产（站点设备）所在主机的 IP、系统、开放端口和服务应用等信息更新至资产管理模块。不启用则不更新。
高级选项	关键页面总数	仅支持配置为“1”，表示仅对 Web 资产对应的 URL 进行探测。
	插件超时限制	单个插件在指定时间内如果未正常结束，将会被调入引擎终止。 单位为秒，取值范围为 1～300 秒。
	调试模式	预防出现扫描任务异常时，可以配置该参数。记录扫描任务的执行信息，当任务执行异常，导出异常信息并发送给公司的技术支持人员进行错误分析。

5.1.1.9 已有任务配置

漏洞扫描系统还可以通过加载已有任务来新建扫描任务。

进入 **新建任务** > **评估任务** 页面，选择 **评估任务/口令猜测任务/Web 应用扫描任务/配置扫描任务/主机资产探测/Web 资产探测**，在已有任务配置区域，选择任务名/IP，在“搜索”下拉列表框中选择所需的任务/IP，编辑需要修改的任务参数、下发扫描任务即可。其中，单击【设置默认模板】按钮，可以将该任务设置为任务模板，再次新建任务时，将自动调用该任务参数（除扫描目标外）来新建任务。

5.1.2 远程扫描（快速入口）

漏洞扫描系统支持通过快速选择“漏洞模板”来新建评估任务，帮助用户明确快速明确使用场景，从而简化用户的操作。

通过各漏洞模板新建评估任务的操作类似，这里以新建存活主机任务为例进行介绍。

进入 **新建任务** 页面，选择 **存活主机扫描**，配置端口扫描的选项即可新建一个快速任务。

漏洞扫描系统支持的快速任务如下：

- 攻防演练高平高危漏洞扫描（系统）
- 攻防演练高频高危漏洞扫描（Web）
- 存活主机扫描
- 系统/Web 漏洞验证扫描：通过 POC 漏洞验证原理，使用可验证漏洞扫描模板，比较准确的验证资产中是否存在漏洞。（暂未开启此功能）
- 全部漏洞扫描。
- 紧急漏洞扫描
- 云计算漏洞扫描（暂未开启此功能）
- 大数据漏洞扫描（暂未开启此功能）
- 物联网漏洞扫描（暂未开启此功能）

5.1.3 本地配置扫描

远程扫描仅适用于在线的目标主机，如果要检查离线主机配置的合规情况，需要首先从漏洞扫描系统系统中下载离线检查工具到目标主机，然后在目标主机本地运行该工具进行本地配置扫描，最后将扫描结果导入漏洞扫描系统系统。

离线检查工具与用户导入的证书关联，只有被授权的工具才可以下载。

以网络设备的操作为例，介绍如何进行本地配置扫描，其他类型的离线检查工具的使用方法请参见解压后的扩展名为.txt 的文件。本地配置扫描的具体操作如下：

步骤 1 在漏洞扫描系统中下载离线检查工具。

a. 进入下载页面。

- 进入 **新建任务** 页面，选择 **配置扫描 > 离线扫描**，单击【离线检查工具】。
- 进入 **模板管理 > 离线检查工具 > 网络设备** 页面。

b. 单击操作栏中图标  ，下载对应的离线检查工具或 SecureCRT 插件。

（可选）若被下载工具中的配置模板的分组类型为等保模板分组，还需要选择等保级别。

步骤 2 在目标设备上执行本地配置检查任务。

打开本地的 Securecrt 软件，进入 **脚本 > 执行** 页面，选择已经下载的离线检查工具。执行成功后，会在本地离线检查工具所在的相同级别的目录下生成 *IP_UUID_chk.xml* 格式的配置检查结果文件。

步骤 3 在漏洞扫描系统中导入配置检查结果文件。

a. 进入导入任务页面。
   - 进入 **新建任务** 页面，选择 **配置扫描 > 离线扫描**。
   - 进入 **任务列表 > 任务列表** 页面。

b. 选择配置检查结果文件，单击【导入】按钮，将扫描结果导入任务列表，系统自动生成任务，并在任务列表中保存本地配置检查结果。

说明	系统支持导入 xml、普通文本和 zip 格式的文件。

----结束

5.2 任务列表

系统以分页的形式列出用户可见的所有任务，管理员可对任务进行各种管理操作。

5.2.1 任务列表简介

进入 **任务列表 > 任务列表** 页面，列表介绍如表 5-19 所示。

表 5-19 任务参数

配置项	描述
任务号	漏洞扫描系统系统内部给每个任务分配的唯一标识编号。
任务名称	当前任务的名称。表示无扫描数据。
任务类型	通过下拉菜单可以筛选不同的任务。 • 任务类型：漏洞配置扫描、评估任务、配置扫描、Web 应用扫描、口令猜测、镜像扫描、代码审计、主机资产探测、Web 资产探测。 • 任务状态：立即执行任务、周期任务、定时任务、导入任务。
开始时间/结束时间	当前任务的开始和结束时间。对于尚未结束的任务，只显示其开始时间。
进度	当前任务执行的进度情况。 • 100%：当前任务已经结束。 • 百分比：当前任务正在进行中、任务执行中被暂停。单击百分比数字，可以查看当前任务的详细信息。 • 0%：当前任务尚未开始执行。
操作	可以对当前任务执行的操作。

5.2.2 任务操作

新建任务后，可以对任务列表中的任务进行管理，如表 5-20 所示。按照任务状态可以执行的操作如下：

- 未开始执行的任务，可以对其进行删除、停止操作。
- 正在扫描的任务，可以对其进行删除、暂停、停止操作。
- 暂停扫描的任务，可以对其进行删除、继续扫描、停止操作。
- 扫描完毕的任务，可以对其进行编辑、删除、断点续扫和重新扫描操作。
- 扫描异常的任务，可以对其进行编辑、删除和重新扫描操作。
- 导入的任务，可以对其进行编辑和删除操作。
- 父任务，可以对其进行编辑、删除和重新扫描操作。

表 5-20 任务操作

操作	描述
编辑	代码审计任务不支持编辑任务功能。 单击任务名称，进入任务参数页面，单击【修改任务】按钮，即可修改任务。修改成功后，会自动生成一个新任务。
删除	• 单个删除：单击操作栏中的图标。 • 批量删除：勾选多个任务，单击【任务操作 > 批量删除】按钮。 • 全部删除：单击【任务操作 > 全部删除】按钮。
查询	只有拥有任务列表权限的系统管理员能够查询其他用户下达的扫描任务，普通管理员用户只能查看其创建的任务。 • 查询指定任务：单击 查询 图标，配置查询参数即可查询指定任务。 • 查看任务详情：管理员可以查看指定任务的详细信息，具体操作请参见 任务报表。
暂停	镜像扫描任务不支持批量暂停操作。 • 单个暂停：单击操作栏中的图标。 • 批量暂停：勾选多个任务，单击【任务操作 > 批量暂停】按钮。
继续扫描	单击操作栏中的图标。
停止	• 单个停止：单击操作栏中的图标。 • 批量停止：勾选多个任务，单击【任务操作 > 批量停止】按钮。
导出	• 单个导出：单击操作栏中的图标/单击任务名称，进入任务参数页面，单击【导出任务】按钮。 • 批量导出：勾选多个任务，单击【任务操作 > 批量导出】按钮。
导入	系统支持【导入】xml、普通文本和 zip 格式的文件，自动生成报表。 系统中既可以导入单个主机的扫描结果文件（格式通常为“.xml”），也可以导入单个模板多台主机的扫描结果文件（以 zip 包方式批量导入）。

操作	描述
【导出调试信息】	单击任务名称，进入任务参数页面，单击【导出调试信息】按钮，保存调试信息至本地。
【重新扫描】	在保留原来的扫描结果基础上，调用原始任务的参数，再创建新任务执行扫描。重新扫描之后，生成父任务，原始任务和新任务都为父任务的子任务。父任务的报表是最近一次结束的子任务数据的综合统计，起止时间为重新扫描后的时间。 本操作支持停止、正常完成的普通任务，导入任务和重新扫描生成的父任务。不支持子任务和周期任务。 可通过查看父任务的对比分析模块比较子任务的扫描结果差异。 • 单个重新扫描：单击操作栏中的图标/单击任务名称，进入任务参数页面，单击【重新扫描】按钮。 • 批量重新扫描：勾选多个任务，单击【任务操作 > 重新扫描】按钮。
断点续扫	单击操作栏中的图标，对已完成的扫描任务中没有被覆盖的目标重新下发扫描任务，不会对完成扫描的目标下发扫描任务。断点续扫之后，会自动生成一个新任务。 代码审计任务、Web 应用扫描任务、周期评估任务、子任务和导入任务不支持断点续扫操作。
汇总查看	为了便于多个任务结果的统一分析，漏洞扫描系统提供了汇总查看的功能，用于将多个任务结果合并到同一个任务中。关于汇总查看的详细操作请参见 任务报表。 代码审计任务不支持汇总查看功能。
报表输出	勾选需要输出报表的任务，单击【报表输出】按钮，生成报表。 关于报表的详细操作请参见 报表管理。

6 报表管理

漏洞扫描系统的报表系统基于扫描任务的结果数据。在报表中，显示最近一次扫描的各项统计数据，并以图表及摘要描述等方式清晰呈现出网络安全状况。

本章主要介绍报表管理的相关信息，包括以下内容：

功能	描述
任务报表	介绍任务报表的详细信息。

功能	描述
资产报表	介绍资产报表的详细信息。
报表输出	介绍离线报表的相关操作。

6.1 任务报表

系统管理员 admin 和拥有报表管理权限的系统管理员可以查看所有扫描任务的在线报表，拥有报表管理权限的普通管理员只能查看自己创建的任务报表。不同状态下的任务，查看报表的方法也各不相同。

- 等待调度的任务

  由于任务尚未开始执行，因此无法查看扫描结果。
- 已结束的任务/正在执行的任务/被中途停止的任务/处于暂停状态的任务

  在任务列表中，单击任务名称，即可查看当前任务的在线报表。

说明	• 任务被中途停止有两种情况：扫描异常停止和管理员手动停止。 • 处于正在执行状态、被中途停止状态以及暂停状态的任务，由于整个扫描过程未能执行完成，因此扫描结果并不全面，不建议作为参考标准。

6.1.1 查看方式

支持查看单个和多个任务的报表详情。

- 查看单个任务详情

  进入 **任务列表 > 任务列表** 页面，单击需要查看报表详情的任务名称，进入单个任务报表详情页面，选择页签查看报表数据。
- 查看多个任务合并信息

  进入 **任务列表 > 任务列表** 页面，勾选需要查看报表详情的多个任务名称，单击【汇总查看】按钮，弹出多个任务数据合并后生成的报表详情页面，选择页签查看报表数据。

常用的报表操作如下：

- 单击【刷新缓存】按钮，刷新当前页面。
- 单击 图标，打包下载当前页面至本地。
- 单击 、 、 、 、 图标，以相应格式输出当前报表至 报表列表。

说明	如果某 IP/站点/镜像标签/URL 在多个任务中重复出现，则以任务号最大的扫描结果为准。

6.1.2 评估任务报表

评估任务报表由综述报表和主机报表组成，根据漏洞扫描任务、配置扫描任务、弱口令猜测的扫描结果进行报表的数据展示。

6.1.2.1 综述报表

综述报表从整体上描述被扫描网络的安全状况，是评估任务扫描结果的综合展示。不同评估任务的报表内容略有不同，具体请以界面展示为准，下面以执行漏洞配置扫描、弱口令猜测的综合任务的扫描数据为例，介绍综述报表的详情，如表 6-1 所示。

表 6-1 综述报表

页签	统计项	描述
任务参数	基本信息	展示评估任务参数。
	高级选项/按钮	可以对任务执行相应操作，具体内容请参见 任务操作。
综述信息	任务信息	任务信息包括网络风险（风险值、风险等级）、任务名称、任务类型、时间统计、漏洞扫描模板、配置检查模板列表、主机统计和系统版本信息。
	风险分布	风险分布信息包括主机漏洞风险等级分布、主机整体风险等级分布、主机配置风险等级分布、漏洞高中低风险分布和不合规检查项高中低风险分布。
	漏洞风险类别	按照不同分类统计高、中、低风险的漏洞数量，以及所有风险分类的总数统计。单击列表中的数值，即可查看相应的漏洞详细信息。若要在同一页面中将以上内容全部列出，只需单击标签中的“全部”即可。
	配置风险类别	配置风险类别包括不合规项在应用程序中的分布和不合规项在操作系统中的分布。
	资产综述	资产综述中展示资产操作系统的统计数量和比例。
主机信息	主机风险等级列表	展示当前被扫描全部主机的风险等级。 • 如果列表中的主机数量很多，可以通过风险等级过滤（非常危险、比较危险、比较安全、非常安全）对主机筛选。 • 单击 IP 地址前的“⊞”查看使用的扫描模板信息。 • 单击 IP 地址可以查看主机报表，具体请参见 主机报表。
漏洞信息	漏洞分布	展示当前任务中所有风险等级的漏洞信息，包括漏洞名称和出现次数等。 • 如果列表中的漏洞数量很多，可以通过漏洞类别过滤（高风险、中风险、低风险）对漏洞进行筛选。 • 在漏洞验证区域，展示可验证[已验证个数/可验证个数]漏洞的个数。 • 单击漏洞前的“⊞”展开该漏洞的详细信息，不同漏洞包含的详细信息参数项有所不同。单击某个受影响主机，查看主机报表，主机报表详情请参见 主机报表。 • 原理扫描：对于原理扫描漏洞，在漏洞名称中通过【原理扫

页签	统计项	描述
		描】进行标识。 • 可验证：对于支持漏洞验证的漏洞，在漏洞名称中通过【可验证】进行标识。单击“⊞”展开该漏洞后，可以查看漏洞的验证方法。
配置信息	-	展示当前任务中所有风险等级的配置不合规信息。 单击某个不合规主机，查看主机报表，主机报表详情请参见 主机报表。
脆弱帐号	应用脆弱帐号	展示该任务中所有扫描出来的脆弱帐号信息。 单击某个 IP 地址，查看主机报表，主机报表详情请参见 主机报表。
参考标准	-	展示系统风险等级标准，包括单一漏洞风险等级评定标准、单一配置检查项等级评定标准、主机风险等级评定标准、网络风险等级评定标准以及安全建议。
对比分析	-	只有父任务的报表会展示这个页签，父任务报表的内容为正常完成扫描后任务号最大的子任务的报表信息。默认显示最后两次子任务的对比数据。 • 在任务的下拉列表框中可以选择子任务，对比指定的子任务的扫描数据。 • 单击漏洞信息对比区域中漏洞前的“⊞”展开该漏洞的详细信息，不同漏洞包含的详细信息参数项有所不同。 • 单击漏洞信息对比区域中的某个影响主机、脆弱帐号对比区域中的某个 IP 地址，查看主机报表，主机报表详情请参见 主机报表。

6.1.2.2 主机报表

管理员可以查看主机的详细风险报表（即主机报表），包括主机概况、漏洞信息、配置合规信息、状态合规信息等。

若评估任务启用了“全量 Agent 扫描”，则在主机报表的主机概况中会增加展示信息“数据来源”和“Agent 数据采集时间”。

此外，漏洞扫描系统还支持对如下资产类型进行识别展示：

- 摄像头：支持识别海康威视、大华、亚安、天地伟业、汉邦高科、景阳、D-link；在 **1.主机概况** 中进行展示。
- 国产化操作系统：支持识别深度、中标麒麟；在 **5.3 操作系统类型** 中进行展示。
- 国产化应用：支持识别织梦、PHPCMS、金蝶；在 **5.2 安装软件信息** 中进行展示。
- 国产化数据库：支持识别达梦、人大金仓；在 **5.2 端口 Banner** 中进行展示。

查看方式

可以通过如下方式查看主机报表：

- 在 综述报表 的主机信息页签下，单击主机风险等级列表下的某个主机 IP。

- 在 综述报表 的漏洞信息页签下，单击漏洞前的“⊞”展开该漏洞的详细信息，单击某个受影响主机。
- 在 综述报表 的配置信息页签下，单击某个不合规主机。
- 在 综述报表 的脆弱帐号页签下，单击某个 IP 地址。
- 在 综述报表 的对比分析页签下，单击漏洞信息对比区域中的某个影响主机、脆弱帐号对比区域中的某个 IP 地址。

误报修正 – 漏洞

扫描结果中的漏洞信息，可能会有误报，也可能管理员需要忽略某些漏洞，这时可以对其进行修正。修正后的漏洞将不再显示在漏洞列表中，但再次执行扫描任务后，该漏洞仍然会出现在漏洞列表中，必须再次修正才能不在漏洞列表中显示。

在主机报表中，选择 **漏洞信息 > 漏洞概况**，展开漏洞概况区域，单击某条漏洞右侧的图标，显示漏洞的返回值和可执行的误报修正操作：

- 选择“修正此 IP”，表示修正从所属评估任务下的此 IP 地址中发现的该漏洞。
- 选择“修正此任务”，表示修正从所属评估任务下的所有 IP 地址中发现的该漏洞。

误报修正 – 配置项

扫描结果中的不合规项，可能会有误报，也可能管理员需要忽略某些不合规项，这时可以对其进行修正。经过修正的不合规项将被删除，不在列表中显示。但是，扫描任务再次执行后，该不合规项仍然会出现在列表中，必须再次修正才能不在列表中显示。

在主机报表中，选择 **配置合规信息**，展开配置合规信息区域，选择“修正此不合规项”，修正从所属评估任务下的此 IP 地址中发现的该不合规项即可。

6.1.3 口令猜测任务报表

口令猜测任务报表由综述报表和主机报表组成，根据扫描结果进行报表的数据展示。

综述报表仅包含任务参数和脆弱帐号两个页签，展示内容与评估任务报表类似，具体请参见评估任务的 综述报表 中的这两项描述，这里不赘述了。

主机报表详情请参见评估任务的 主机报表。

6.1.4 Web 应用扫描任务报表

Web 应用扫描任务报表由综述报表和站点报表组成，根据 Web 应用扫描任务的扫描结果进行报表的数据展示。

6.1.4.1 综述报表

综述报表从整体上描述被扫描站点的安全状况，是扫描结果的综合展示，如表 6-2 所示。

表 6-2 Web 综述报表

页签	统计项	描述
任务参数	基本信息	展示任务参数。

页签	统计项	描述
	高级选项/按钮	可以对任务执行相应操作，具体内容请参见 任务操作。
综述信息	任务信息	任务信息包括网络风险（风险值、风险等级）、任务名称、任务类型、漏洞扫描模板、信息统计、域名统计、时间统计、版本信息。
	风险分布	风险分布信息包括站点风险等级分布（扫描站点数量大于等于 2 个时，才会展示该信息）、页面风险级别分布、漏洞高中低风险分布。
	风险类型	按照不同分类统计高、中、低风险的漏洞数量，以及所有风险分类的总数统计。
	高危漏洞最多的页面 Top10	展示站点中包含高危漏洞最多的页面 Top10 及对应的高危漏洞个数。
站点列表	站点风险等级列表	默认列出当前被扫描全部站点、每个站点的已扫描链接数、扫描耗时、包含的高中低风险数量、风险值。 • 如果站点列表中的站点数量很多，可以通过风险等级过滤（非常危险、比较危险、比较安全、非常安全）对站点进行筛选。 • 单击某个站点名称，可以查看站点报表，具体请参见 站点报表。
漏洞列表	漏洞分布	默认列出当前任务中所有风险等级的漏洞信息，包括漏洞名称、影响页面个数、出现次数。 • 如果漏洞列表中的漏洞数量很多，可以通过漏洞类别过滤（高风险、中风险、低风险）对漏洞进行筛选。 • 在漏洞验证区域，展示可验证[已验证个数/可验证个数]漏洞的个数。 • 单击漏洞前的“⊞”展开该漏洞的详细信息，不同漏洞包含的详细信息参数项有所不同。单击某个受影响站点，查看站点报表，站点报表详情请参见 站点报表。 • 原理扫描：对于原理扫描漏洞，在漏洞名称中通过【原理扫描】进行标识。 • 可验证：对于支持漏洞验证的漏洞，在漏洞名称中通过【可验证】进行标识。单击“⊞”展开该漏洞后，可以查看漏洞的验证方法。
参考标准	-	列出了 Web 应用风险等级标准。
对比分析	-	只有父任务的报表会展示这个页签，父任务报表的内容为正常完成扫描后任务号最大的子任务的报表信息。默认显示最后两次子任务的对比数据，包括任务信息对比、漏洞信息对比。 • 在任务的下拉列表框中可以选择子任务，对比指定的子任务的扫描数据。 • 单击漏洞信息对比区域中漏洞前的“⊞”展开该漏洞的详细信息，不同漏洞包含的详细信息参数项有所不同。 • 单击漏洞信息对比区域中的某个影响站点，可以查看站点报表，具体详情请参见 站点报表。

6.1.4.2 站点报表

管理员可以查看站点的详细风险报表（即站点报表），包括站点概况、风险分类统计、Web 风险分布、站点树等。

查看方式

可以通过如下方式查看站点报表：

- 在 综述报表 的站点列表页签下，单击站点风险等级列表下的某个站点名称。
- 在 综述报表 的漏洞列表页签下，单击漏洞前的“⊞”展开该漏洞的详细信息，单击某个受影响站点。

误报修正

若怀疑某些漏洞属于误报，可以使用误报修正功能对漏洞进行修正处理，修正后的漏洞将不再显示在漏洞列表中。但再次执行扫描任务后，该漏洞仍然会出现在漏洞列表中，必须再次修正才能不在漏洞列表中显示。

在站点报表中，选择 **Web 风险分布 > Web 应用漏洞**，展开 Web 应用漏洞区域，单击漏洞前的“⊞”展开该漏洞的详细信息，执行误报修正操作：

- 在漏洞信息中，鼠标移到 URL 地址处，自动显示误报修正按钮，单击该按钮即可修正该链接对应的漏洞。
- 勾选需要修正的某些链接对应的漏洞，单击【批量误报修正】按钮，批量修正漏洞。

6.1.5 配置扫描任务报表

配置扫描任务报表由综述报表和主机报表组成，根据扫描结果进行报表的数据展示。

综述报表展示内容与评估任务报表类似，包含除漏洞信息外的其他所有页签。

- 配置扫描任务的综述报表的具体查看方法请参见评估任务的 综述报表，这里不再赘述。
- 配置扫描任务的主机报表详情请参见评估任务的 主机报表，这里不再赘述。

6.2 资产报表

系统管理员 admin 和拥有报表管理权限的系统管理员可以查看所有资产的报表，拥有报表管理权限的普通管理员只能查看自己创建的任务中目标资产的资产报表。只有已经结束的任务产生的结果数据才能生成资产报表。

进入 **资产管理 > 资产管理** 页面，鼠标左键选择网络节点或资产设备后，在页面右侧显示相应的资产报表。资产报表由网络节点报表和资产设备报表组成，报表数据来自漏洞扫描任务、配置扫描任务、弱口令猜测、Web 应用扫描任务的扫描结果。

常用的报表操作如下：

- 单击  图标，打包下载当前页面至本地。
- 单击  图标，以相应格式输出当前报表至 报表列表。

6.2.1 网络节点报表

网络节点报表从整体上描述该网络节点下所有资产设备的整体安全状况，是扫描结果的综合展示，展示的内容如表 6-3 所示。

表 6-3 网络节点报表

页签	统计项	描述
综述信息	资产信息	展示网络节点的风险等级、风险值。
	风险分布	展示主机整体风险等级分布、主机漏洞风险等级分布、主机配置风险等级分布。
	漏洞风险类别	展示当前网络节点下所有资产设备的漏洞统计数据，其展示方式与评估任务报表中的类似，具体请参见 综述报表 > 综述信息 > 漏洞风险类别。
下级节点信息	下级节点风险等级列表	展示当前网络节点的所有下级网络节点的风险情况。
	风险分布	以饼图的方式，展示不同风险等级节点的个数和占比。
属性	节点属性	展示当前网络节点的基本信息。
其他页签	主机信息、系统漏洞信息、配置信息、脆弱帐号	分别展示当前网络节点下所有资产设备的风险情况、高中低系统漏洞、所有风险等级的配置不合规信息、存在的脆弱帐号信息，其展示方式与评估任务报表中的类似，具体请参见 综述报表 > 主机信息、漏洞信息、配置信息、脆弱帐号。
	Web 漏洞信息	展示当前网络节点下所有用作站点的资产设备的高中低 Web 应用漏洞，其展示方式与 Web 应用扫描任务报表中的类似，具体请参见 综述报表 > 漏洞列表。

6.2.2 资产设备报表

资产设备（无论是主机还是站点设备）在资产管理中都是以 IP 地址做唯一标识的。资产设备报表是以 IP 地址为基础，对该资产设备的评估任务、口令猜测任务、Web 应用扫描任务、主机资产探测任务和 Web 资产探测任务的扫描数据的综合统计。

表 6-4 资产设备报表

页签	描述
设备信息	展示资产的操作系统、端口、服务应用、安装软件、MAC 和主机名等探测到信息。
风险信息	设备风险信息包括：主机概况、漏洞信息（系统漏洞、Web 应用漏洞）、配置合规信息、状态合规信息、站点详情、其他信息（端口信息、操作系统类型等）。其数据来源于主机报表和站点报表，内容详情和相关操作请参见主机报表、站点报表。
风险对比信息	管理员可以将不同时间的资产设备的扫描数据进行对比，从而了解该资产设备的安全情况变化。 在对比时间处，选择需要对比安全情况的时间点，单击【对比】按钮，显示对比后的数据（风险对比概况、漏洞信息对比、不合规配置信息对比、扫描 URL 信息对比等）。
历史任务信息	默认展示该资产设备的最后一次的扫描任务数据，管理员可以选择主机扫描时间，查看该资产设备的指定的任务信息。 不同的任务展示的信息不同，具体请以界面显示为准。
属性	展示当前资产设备的基本信息。
关联信息	若主机资产探测任务中，启用“关联 Web 资产探测”，则展示探测到的 Web 资产（站点设备）信息。 若 Web 资产探测任务中，启用“关联主机探测”，则展示探测到的主机资产信息。

6.3 报表输出

管理员可以将扫描结果根据需要、配置报表输出条件，以离线报表形式输出指定的报表。只有已经结束的任务产生的结果数据才能生成离线报表。

6.3.1 输出离线报表

漏洞扫描系统输出的离线报表格式如表 6-5 所示。

表 6-5 漏洞扫描系统输出的离线报表格式

任务类型	HTML	WORD	EXCEL	PDF	XML
评估任务	√	√	√	√	√
口令猜测任务	√	√	√	√	√
Web 应用扫描	√	√	√	√	×

任务类型	HTML	WORD	EXCEL	PDF	XML
配置扫描	√	√	√	√	√

从报表输出页面输出

进入 **报表输出 > 报表输出** 页面，配置报表输出参数即可。报表输出参数说明如表 6-6 所示。

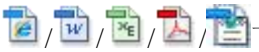
- 在报表输出过程中，若需要终止报表输出，单击【停止输出】按钮即可。
- 当报表输出成功  后，单击  下载或查看离线报表；单击【下载最近输出的报表】，进入报表列表页面，下载或查看离线报表。

表 6-6 报表输出参数

项目	配置项	描述
任务内容	输出范围	• 普通扫描任务：根据评估任务、口令猜测任务、本地配置扫描任务的扫描数据生成离线报表。 • Web 应用扫描任务：根据 Web 应用扫描任务的扫描数据生成离线报表。 • 镜像扫描任务：根据镜像扫描任务的扫描数据生成离线报表。 • 代码审计任务：根据代码审计任务的扫描数据生成离线报表。 • 主机资产探测任务：根据主机资产探测任务的扫描数据生成离线报表。 • Web 资产探测任务：根据 Web 资产探测任务的扫描数据生成离线报表。
	显示最近	显示最近的扫描任务的数量。此处的设置影响任务列表中显示的任务数、筛选主机中显示的主机数。
	任务列表	选择一个或多个扫描任务。
	筛选主机	单击【筛选主机>>】，显示扫描任务中包含的被扫描主机。选择需要输出报表数据的主机。 若主机数据过多，可以通过风险等级、操作系统等对显示的主机进行过滤。
离线报表	报表类型	报表的输出格式。
	报表内容	输出报表中包含的内容，可选项有综述报表和主机报表。 综述和主机报表都需要配置报表模板和报表标题。 如果没有合适的报表模板，可以单击“报表模板管理”链接，进入报表模板页面后，添加报表模板，具体请参见 报表模板。 镜像扫描任务和代码审计任务不允许修改报表模板。 主机资产探测任务、Web 资产探测任务不允许修改报表模板和报表标题。

项目	配置项	描述
合并报表	单任务输出	所选单个任务的报表名称。仅需配置报表名称。
	多任务输出	需要配置输出方式（合并输出和批量输出）和报表名称。 • 合并输出：统计所选任务的所有扫描数据，在一张报表中展示。 • 批量输出：对每个任务生成一张报表。
子任务模式	子任务模式	• 不启用：报表中仅统计父任务下最新的子任务的扫描数据。 • 启用：选择需要统计的父任务下的子任务，报表中对所选子任务的扫描数据进行统计。

新建任务时配置输出

代码审计任务不支持从新建任务时配置输出离线报表。

新建任务时输出离线报表的操作请参见 远程扫描。输出的报表在 报表列表 中查看。

从任务综述报表页面输出

从任务综述报表页面输出报表是按照系统默认的报表输出格式输出。

进入 **任务列表** > **任务列表** 页面，单击任务名称/对多个任务进行【汇总查看】，进入任务综述报表页面，在除任务参数和参考标准外的其他页签，单击右下方的 、 、 、 、 即可生成报表。

- 在报表输出过程中，若需要终止报表输出，单击【停止输出】按钮即可。
- 报表输出成功 后，单击 / / / / 下载或查看离线报表；单击【下载最近输出的报表】，进入报表列表页面，下载或查看离线报表。

从任务列表页面输出

从任务列表页面输出报表是按照系统默认的报表输出格式输出。

进入 **任务列表** > **任务列表** 页面，对多个任务进行【报表输出】，配置合并报表名称并单击【合并输出】按钮后即可生成报表。

- 在报表输出过程中，若需要终止报表输出，单击【停止输出】按钮即可。
- 报表输出成功 后，单击 / / / / 下载或查看离线报表；单击【下载最近输出的报表】，进入报表列表页面，下载或查看离线报表。

6.3.2 报表列表

所有的离线报表将保存至报表列表中，进入 **报表输出** > **报表列表** 页面，可以对生成的离线报表执行查询、列表筛选、下载（ / / / / ）、删除和清空等操作。

7 认证管理

认证管理主要对系统扫描的信息进行管理。认证信息通过 IP 地址与资产进行关联，在新建任务的时候输入 IP 地址或者范围后可以直接调用认证信息进行扫描。

可以通过如下方式添加主机认证信息：

- 手动添加、导入、更新
- 新建扫描任务时，勾选“同步到认证管理”，相关操作请参见 评估任务 和 配置扫描任务
- 添加资产设备时，单击蓝色链接文字“配置认证信息”，相关操作请参见 添加资产设备。

添加认证信息后，可以执行导出、查询、编辑、删除和清空的操作。

7.1 手动新建认证信息

进入 **认证管理** > **认证管理** 页面，单击【添加主机】按钮，配置参数即可新建一条认证信息。主机认证信息参数的说明如表 5-3 和表 7-1 所示。

表 7-1 主机认证信息参数

项目	配置项	描述
漏扫策略	ORACLE	启用后，可以进行 Oracle 漏洞深度扫描，同时需要在高级选项中启用“启用 oracle 漏洞深度扫描”参数。
WEBLOGIC 策略	WEBLOGIC	启用后，可以进行 WEBLOGIC 漏洞深度扫描。
		系统登录：通过搭建 WEBLOGIC 服务的设备后台来访问 WEBLOGIC。 • Linux/Windows：操作系统类型。 • Weblogic Version：Weblogic 的版本。 • Weblogic User：WEBLOGIC 的用户名。 • Weblogic Wls Path：weblogic 的 Wls 的安装路径。
		界面登录：通过 Web 界面访问 WEBLOGIC。 • 用户名/密码：WEBLOGIC 的用户名和密码。 • 路径：WEBLOGIC 的 URL。

项目	配置项	描述
	主机	主机指安装了操作系统的计算机。单击模板项进行选择，配置模板参数即可。 • 操作系统模板：需要匹配操作系统类型。 • 虚拟化设备模板：需要匹配虚拟化设备类型。 • 应用程序模板：需要匹配已经安装的应用程序类型。 • 数据库模板：需要匹配已经安装的数据库类型。 • 大数据模板：需要匹配已经安装的大数据软件或平台类型。
	网络设备	网络设备指除主机外连接到网络中的物理实体，如交换机、路由器等。 • 单击模板项进行选择，配置模板参数即可。 • 需要匹配网络设备的类型。
状态模板	状态模板	不视为不合规项的白名单信息。 单击【状态模板管理】，进入状态模板列表页面。如何新建状态模板请参见 状态模板。

7.2 导入认证信息

进入 **认证管理** > **认证管理** 页面，单击【Excel 模板下载】，编辑并保存认证信息；单击【浏览】按钮，选择完成编辑的 Excel 模板，单击【导入】按钮，导入主机认证信息即可。

7.3 更新认证信息

进入 **认证管理** > **认证管理** 页面，更新新建任务时的认证信息至认证管理中。

- 单个更新：单击操作栏中的图标。
- 批量更新：勾选需要更新的主机认证信息，单击【批量操作】 > 【批量更新】按钮。
- 全部更新：单击【批量操作】 > 【全部更新】按钮。

8 模板管理

模板管理主要对漏洞扫描系统系统中的各类扫描模板进行管理，用户通过模板管理可以对所有在任务执行过程中被扫描的内容进行管理。

图标含义如下：

-  ：默认的系统模板，只支持查看、另存为操作。不允许修改、导出、删除。
-  ：另存为的系统模板，模板所有者可以任意编辑。
-  ：用户模板，模板所有者可以任意编辑。

本章将介绍漏洞扫描系统模板管理的相关知识，主要包括以下内容：

功能	描述
漏洞模板	介绍漏洞模板的相关操作。
资产标记库模板	介绍资产标记库模板的相关操作。
配置模板	介绍配置模板的相关操作。
状态模板	介绍状态模板的相关操作。
报表模板	介绍报表模板的相关操作。
密码字典	介绍密码字典的相关操作。
端口列表	介绍端口列表的相关操作。
离线检查工具	介绍离线检查工具的相关操作。
ActiveX	介绍 ActiveX 的相关操作。
离线加固工具	介绍离线加固工具的相关操作。

8.1 漏洞模板

漏洞模板是漏洞扫描的基础，是一个扫描插件集。漏洞扫描系统覆盖近乎所有类型的漏洞扫描插件，管理员可以根据需要指定相应的扫描插件进行漏洞扫描。从而加快扫描任务的运行速度，提高扫描结果的准确性和覆盖度。

进入 **模板管理 > 漏洞模板 > 系统扫描模板/Web 扫描模板** 页面，单击【添加】按钮/图标，可以新建一个漏洞模板。漏洞模板参数的说明如表 8-1 和表 8-2 所示。新建漏洞模板后，可以进行查询、查看、编辑、另存为、删除、导出和导入的操作。

表 8-1 基本参数

配置项	描述
模板名称	由英文字母、数字或-、_字符组成，区分大小写。取值范围为 1~64 个字符。同一用户不允许创建相同名称模板，不同用户间可以创建相同名称模板。
模板描述	对模板的补充说明。

表 8-2 模板类型参数

配置项	描述
普通模板	管理员根据扫描插件的类型选择扫描任务所需要的插件。包含所有漏洞扫描系统支持的插件。有两种方法选择指定漏洞插件。 • 查询指定漏洞后勾选漏洞插件。 • 在漏洞列表下拉列表框中选择插件的类型，然后根据扫描任务需要勾选扫描插件。
	查询参数： CVE ID/BUGTRAQ ID/CNCVE ID/CNVD ID/CNNVD ID /MS 编号（Web 扫描模板无此项）：世界知名漏洞知识库中漏洞的编号。 • 风险等级：漏洞的风险级别。 • 漏洞名称（系统扫描模板）：系统漏洞的名称。 • 漏洞描述（Web 扫描模板）：对 Web 应用漏洞的具体描述。 • 危险插件：是，此类插件可能导致系统崩溃或服务中断。 • 发布日期：发现漏洞的时间。
	漏洞验证：是否为漏洞扫描系统支持验证的漏洞。
高级模板(过滤器模板)	管理员根据如下条件筛选扫描任务所需要的插件。 • 风险级别：漏洞的风险级别。 • 收录组织：收录漏洞信息的组织。 • 发现时间：发现漏洞的时间。 • 系统类别：漏洞所属的操作系统类型。 • 应用类别：漏洞所属的应用类型。 • 威胁类别：漏洞的攻击方式。 配置上述待选条件后，单击图标，将其加入已选条件中，扫描时根据已选条件选择漏洞扫描插件执行扫描任务。 配置筛选规则后，可以单击【预览】按钮，查看扫描插件。
【添加到模板】	将“漏洞列表”中所需的漏洞插件添加到“添加结果”中，应用为模板。

8.2 资产标记库模板

资产标记库模板是主机/Web 资产探测任务的基础扫描模板，目前漏洞扫描系统仅支持使用内置默认的模板，不支持自定义内容。

进入 **模板管理 > 资产标记库模板 > 资产标记模板/资产标记库** 页面，即可查看模板及其内容。

8.3 配置模板

配置模板是配置检查的基础，包含完善详细的安全配置检查点及其权重。同时支持管理员根据需要或者行业标准自定义各种目标系统的安全配置检查模板。

8.3.1 新建模板分组

为了方便管理员根据需要管理配置模板，漏洞扫描系统支持自定义模板分组。例：用户可以将用于检测某种类型设备的配置模板放在一个模板分组下管理。

进入 **模板管理 > 配置模板 > 操作系统/数据库/应用程序/网络设备/虚拟化设备/大数据** 页面，单击【管理分组】按钮，单击【新建】按钮，配置分组名称、描述信息、分组类型，即可新建一个分组。新建分组后，可以进行编辑和删除的操作。

8.3.2 新建配置模板

8.3.2.1 新建模板

进入 **模板管理 > 配置模板 > 操作系统/数据库/应用程序/网络设备/虚拟化设备/大数据** 页面，单击【模板操作 > 新建/新建等保】按钮/图标，可以新建一个模板。

- 基本属性：用于管理配置模板的基本参数。参数说明如表 8-3 所示。

表 8-3 基本属性参数

分类	配置项	描述
基本信息	模板名称	配置模板的名称。不允许重名。
	模板分组	该配置模板所属的分组。
	检查类型	该配置模板所属的检查类型。
	系统归类/模板类型	该配置模板检查对象所属的类型/所适用的模板类型。
变量列表	【添加变量】	添加自定义变量。
	引用名称	在命令中被引用时使用的名称。
	显示名称	在创建任务时界面显示的名称。

分类	配置项	描述
	类型	该变量的显示类型。 文本类型：表示该变量显示为明文，且该变量的值被记录在日志中。 密码类型：表示该变量显示为密文（以“*”表示），且该变量的值在日志中不被记录。
	描述	对变量的补充说明。
初始化命令	文本框	系统在执行扫描任务过程中登录目标主机后执行的命令，适用于一些需要完成初始化命令的情况，如切换到高权限帐号等。

- 配置检查项：用于检查目标主机是否合规，检查结果将显示在报表中。
  - 系统根据配置检查项列表中的先后顺序依次对目标主机进行检查。
  - 单击【新建】按钮，可以新建一个配置检查项。配置检查项的参数说明如表 8-4、表 8-5 和表 8-6 所示。
  - 新建配置检查项后，可以进行编辑和删除的操作。
  - 可以改变列表中检查项的排序，单击上移图标，向上移动一个位置；单击下移图标，向下移动一个位置。

表 8-4 配置检查项参数

配置项	描述
索引	默认值是 1、2、3……，按照检查项添加的顺序依次递增。用户也可以根据具体需要自定义索引。
检查项名称	配置检查项的名称。
检查项分类（只支持非等保模板配置）	检查项所属类别。
风险值	配置检查项的风险等级。数值越大，风险等级越高。
控制点索引（只支持等保模板配置）	控制点的索引值。
控制点分类（只支持等保模板配置）	控制点所属的配置检查类别。
等保级别（只支持等保模板配置）	控制点的等级保护级别。
控制点描述（只支持等保模板配置）	控制点需要包含的检查项内容。

表 8-5 配置检查项检查点参数

配置项	描述
【添加检查点】	新建一个检查点。新建检查点后，可以进行编辑、删除和加到与或规则里面的操作。

配置项		描述
描述信息		该检查点的概要描述。
配置方法		该检查点的配置方法。
检查方法		• WIN 检查类型的检查方法包括：执行命令、端口检查、文件内容检查、注册表检查、XML 配置文件检查。 • UNIX 检查类型的检查方法包括：执行命令、端口检查、文件内容检查、XML 配置文件检查、文件权限检查、进程检查。
匹配规则		该检查点合规的匹配规则。
执行命令	执行命令	系统在目标主机上获取相关配置信息的命令。
	正则表达式	系统通过此处配置的“正则表达式”对“执行命令”返回的结果逐行进行匹配，筛选出需要的信息。 • 使用括号()：表示需要读取的部分，例如 DEBUG=(\d)，括号中的子表达式内容将被读取。 • 不使用括号()：如果该正则表达式单行显示，则将读取匹配该正则表达式的整行内容；否则只需在换行处用“\n”进行标识，即可实现多行匹配，例：DEBUG=win\ndows，则将读取到多行内容。
	期望值	该检查点合规的期望值。“期望值”与“匹配规则”配合使用，对通过“正则表达式”匹配到的内容进行合规检查。 使用正则表达式匹配规则时，“期望值”的输入模式为“/期望值/”。例：“/DEBUG=\d+/”表示期望值是“DEBUG=\d+”。 • 不区分大小写表达式：//i。例：输入期望值“/DEBUG=\d+/i”，表示不区分该模式的大小写。 • 元字符（.）匹配任何字符表达式：//s。例如：输入期望值“/DEBUG=.*/s”，表示（.）匹配任何字符。 • 多行匹配表达式：\n。
端口检查	类型	待检查端口的传输协议。
	端口号	待检查的端口号。
	期望值	该检查点合规的期望值。 “期望值”与“匹配规则”配合使用，对通过“类型”和“端口号”匹配到的内容进行合规检查。
文件内容检查	文件路径	待检查的文件的绝对路径。
	文件内容	“文件内容”要求填写正则表达式，用于对执行命令返回的结果逐行进行匹配，筛选出需要的信息。 • 使用括号()：表示需要读取的部分。例：DEBUG=(\d)，括号中的子表达式内容将被读取。 • 不使用括号()：取回匹配该正则表达式的整行内容。
	期望值	该检查点合规的期望值。 “期望值”与“匹配规则”配合使用，对通过“文件内容”匹配到的内容进行合规检查。
文件权限	文件路径	待检查的文件的绝对路径。
	期望值	该检查点合规的期望值。

配置项		描述
检查		“期望值”与“匹配规则”配合使用，对通过“文件路径”匹配到的内容进行合规检查。
进程检查	进程名称	待检查的进程名称。
	期望值	该检查点合规的期望值。 “期望值”与“匹配规则”配合使用，对通过“进程名称”匹配到的内容进行合规检查。
XML配置文件检查	xml 文件路径	需要取得的数据所在 xml 文件的完整路径。
	节点	xml 文件的节点（支持标准的 xpath 语法，可以不输入属性值）。
	属性	xml 文件节点的属性（可以不填写）。
	期望值	该检查点合规的期望值。 “期望值”与“匹配规则”配合使用。
【调试】		测试系统是否能够在目标主机执行检查，并返回检查结果。可以随时单击【停止】按钮，停止调试操作。调试检查点参数请参见表 5-3。
【编辑加固信息】		管理加固点。在弹出的对话框中，单击【添加加固点】按钮，可以新建一个加固点。参数说明请参见界面具体提示。新建加固点后，可以进行编辑和删除的操作。

表 8-6 配置检查项检查点逻辑关系

配置项	描述
AND	逻辑与
OR	逻辑或
NOT	逻辑非
（和）	用于提高优先级，表示优先执行括号内的检查点。
←	用于清除逻辑表达式配置框内最后一个输入的检查点。
图标	将检查点添加到逻辑表达式配置框内。
文本框	通过、【AND】、【OR】、【NOT】、【（】、【）】或者【←】计算逻辑关系，检查项的真值结果等于检查点真值的逻辑运算。例：“a and b”表示当检查点 a 和 b 都为真时，检查项结果才为真（即合规）。

- 附录检查项：附录检查项的目的并不是用来检查目标主机是否合规，而是通过附录检查项获取目标主机的相应信息，然后将其作为“辅助信息”展示在报表中。
  - 单击【新建】按钮，可以新建一个附录检查项。附录检查项的参数说明如表 8-7 所示。
  - 新建附录检查项后，可以进行编辑和删除的操作。

表 8-7 附录检查项参数

配置项	描述
检查项名称	附录检查项的名称。
执行命令	需要枚举信息的命令。
行匹配表达式	用来匹配一条记录的正则表达式，一条记录为一行时可以使用“.+”，一行有多条记录根据实际情况填写。
列名称	单击【添加】按钮，在文本框中添加列名称。
列拆分正则	用来匹配一条记录中需要提取的各个字段，使用括号()来表示需要提取的列字段(和列名一一对应)。例：(column1)\s+(column2)\s+(column3)。 当记录有多种模式时，可以填写多个列匹配表达式。单击【添加】按钮，在文本框中添加表达式。

8.3.2.2 配置模板操作

- admin 和用户创建的系统管理员有权限管理所有配置模板，普通管理员只能管理自己创建的配置模板。但是在配置任务时，对配置模板的使用不做限制。
- 如果自定义模板后并没有立即生成模板，则系统会将该模板自动保存到模板列表中，管理员可以后续再对其进行编辑或者直接生成模板。但是管理员在配置任务时不可以使用没有生成的模板。
- 新建配置模板后，可以进行查询、查看、编辑、删除、另存为和导出的操作。
- 导入：单击【浏览】按钮，选择“.dat”文件，单击【导入】按钮，导入模板至系统。支持将一台漏洞扫描系统的配置模板导入另一台具有相同行业以及相同模板授权的漏洞扫描系统设备使用。

8.4 状态模板

系统执行扫描任务时，默认目标主机中运行的所有脆弱帐号和端口都是非法的。若希望目标主机中开放的信任用户信息和端口不作为风险信息检测出来，管理员可以将其配置到状态模板的帐号白名单和端口白名单中，漏洞扫描系统系统将视其为合法帐号和端口。

进入 **模板管理 > 状态模板 > 状态模板** 页面，单击【添加】按钮，可以新建一个状态模板。状态模板的参数如表 8-8 所示。新建状态模板后，可以进行查询、另存为、查看、编辑、删除、导出和导入操作。

表 8-8 状态模板参数

配置项	描述
名称	状态模板的名称。取值范围为 1~20 个字符。
帐号	帐号白名单。勾选表示不进行风险扫描。

配置项	描述
	在【帐号】和【备注信息】文本框中，输入帐号名称及其备注信息，单击图标即可。
端口进程	端口白名单。勾选表示不进行风险扫描。 在【进程】、【端口】、【备注信息】文本框中，输入进程名称、端口号及其备注信息，单击图标即可。

8.5 报表模板

通过配置报表模板可以自定义生成的报表中显示的内容。漏洞扫描系统报表模板的分类如下所示：

- 系统扫描任务报表模板：用于评估任务
  - 综述报表模板：体现目标网络安全情况的统计信息。
  - 主机报表模板：体现单个资产设备的安全情况。
- Web 扫描任务报表模板：用于 Web 应用扫描任务
  - 综述报表模板：体现目标 Web 站点安全情况的统计信息。
  - 站点报表模板：体现单个 Web 站点的安全情况。

漏洞扫描系统支持用户自定义报表模板。以新建系统扫描任务的综述报表模板为例介绍如何新建报表模板。

进入 **模板管理 > 报表模板 > 系统扫描任务报表模板 > 综述报表模板** 页面，单击【添加】按钮，可以新建一个报表模板。新建报表模板后，可以进行查询、查看、编辑和删除操作。

- 选择“基本信息”页签，配置模板名称、模板描述、报表标题、封面 Logo、报表页眉和报表页脚参数。

  配置模板名称由英文字母、数字或中文、-、_字符组成，区分大小写，取值范围为 1~20 个字符。配置模板名称不能重复。
- 选择“报表内容”页签，勾选需要在生成的报表中展示的内容。

8.6 密码字典

在新建口令猜测任务时，配置服务类型中的密码字典，那么漏洞扫描系统在扫描过程中将根据密码字典中的内容尝试登录目标设备，若目标设备的登录用户名和密码与密码字典中的内容匹配，则认为目标设备存在脆弱帐号。

密码字典包括系统密码字典（包含一些常见的脆弱帐号，只能进行查看和另存为，不可编辑和删除）和用户自定义密码字典。

进入 **模板管理 > 密码字典 > 密码字典** 页面，单击【添加】按钮，配置参数即可新建一个密码字典。密码字典参数的详细信息如表 8-9 所示。新建密码字典后，可以进行查看、编辑、删除和另存为的操作。

表 8-9 **密码字典参数**

配置项	描述
字典名称	由英文字母、数字或中文、-、_字符组成，区分大小写。取值范围为 1~64 个字符。新建字典名称不允许与已有字典名称相同。
类别	• 用户名字典：用于扫描具有风险的弱用户名称。 • 密码字典：用于扫描具有风险的密码。 • 用户名密码组合字典：用于扫描具有风险的用户名称及其密码。
字典内容	字典内容以回车作为分隔符。建议文本框输入不超过 1 万行，如果超过 1 万行，请使用文件导入方式。 用户名密码组合字典内容格式为“用户名:密码”。例：administrator:test。
字典文件	txt 格式的文本文件导入，建议导入文件大小不超过 20M： • 文件名由英文字母、数字或-、_字符组成，区分大小写。 • 内容输入要求同字典内容。支持 UTF-8 和 ASCII 编码的文件。 • 单击【浏览】按钮，选择密码字典文件，单击【导入】按钮，完成导入操作。 说明 如果导入的字典文件内容不正确，那么在任务运行时将不予猜测字典中的用户名/密码。
描述信息	对字典的补充说明。

8.7 端口列表

端口列表展示了被扫描设备监听端口的端口号、服务类型及其运行协议的相关信息。例：80 端口对应 http 服务。

若在新建评估任务时配置端口扫描策略，那么扫描过程中将只检测端口列表中的端口。

端口列表包括系统端口（包含一些通用的端口信息）和用户自定义端口。在自定义端口列表中，管理员可以在系统端口列表基础上增加自定义端口。

进入 **模板管理 > 端口列表 > 端口列表** 页面，可以通过手动和智能端口挖掘两种方式新建端口信息。新建端口信息后，可以进行查询、刷新、编辑和删除的操作。

- 手动新建自定义端口信息。配置端口参数、单击图标即可。参数说明如表 8-10 所示。

表 8-10 端口参数

配置项	描述
服务名	由英文字母、数字或-字符组成，区分大小写。取值范围为 1~18 个字符。
端口	取值范围为 0~65535 的整数。
协议	端口运行的协议类型。

- 智能端口挖掘。单击【智能端口挖掘】按钮，从漏洞扫描和配置检查的历史扫描结果中获取所有被扫描设备的端口信息。

8.8 离线检查工具

离线检查工具用于本地检查目标主机的配置情况。下载离线检查工具和进行本地配置扫描的具体操作请参见本地配置扫描。

离线检查工具中的模板由配置模板生成，如何配置配置模板请参见配置模板。

8.9 ActiveX

ActiveX 用来检测本地设备的配置是否正确，只支持 IE 浏览器。只有拥有 ActiveX 用户权限的管理员才有权新建 ActiveX 检查任务。

进入 **模板管理 > ActiveX > ActiveX** 页面，配置参数即可。ActiveX 的参数说明如表 8-11 所示。

- 初次使用时，系统提示用户安装 ActiveX 控件。
- ActiveX 任务的检测结果显示在任务列表中，只有拥有任务列表用户权限的管理员才有权限查看。
- ActiveX 任务的报表输出在报表输出的报表列表页面，只有拥有报表输出权限的管理员才有权限查看离线报表。

表 8-11 ActiveX 参数

配置项	描述
任务名称	ActiveX 配置任务的名称。
配置规范模板	用于检测设备配置是否合规的模板。
报表类型	报表输出的格式有 HTML、EXCEL、PDF 和 WORD。其中，HTML 是系统默认的报表格式。
报表内容	• 综述报表：从整体上进行综合分析、风险描述和分类展示。 • 主机报表：针对单个主机进行风险分析和详细描述。若需要分析扫描任务中出现的问题，请生成主机报表。 • 报表模板：具体请参见 报表模板。

配置项	描述
自动生成报表	• 启用后，任务结束时，生成指定类型的离线报表，并根据配置发送报表。此外，生成的离线报表将保存至 报表列表 中。 • 无论是否启用“自动生成报表”，任务结束时，都自动生成 HTML 格式的在线报表，具体内容请参见 评估任务报表。
FTP 上传	启用：扫描任务完成后，自动将离线报表上传到指定的报表 FTP 服务器。
发送报表	生成报表的类型、接收报表的有效邮箱。 若新建 ActiveX 任务的管理员无任务列表用户权限，建议配置该参数，将报表发送至邮箱查看。
任务说明	对任务的补充说明。

8.10 离线加固工具

公司针对勒索软件“WannaCry”，为用户提供了自动添加主机防火墙阻断规则的一键加固工具，能够起到有效的防护作用。

进入 **模板管理 > 离线加固工具 > Windows 加固工具** 页面，单击文字链接【WannaCry 病毒一键加固工具】，下载加固工具至本地。以管理员身份运行 bat 脚本，按照脚本提示进行操作即可。

9 系统管理

本章主要介绍漏洞扫描系统管理的相关内容，主要包括：

功能	描述
状态	介绍漏洞扫描系统状态及授权注册信息的查看方法。
配置	介绍漏洞扫描系统网络、路由、系统及任务配置的方法。
服务	介绍漏洞扫描系统升级、还原及系统服务管理的具体方法。
用户	介绍漏洞扫描系统的用户权限及用户管理方法。
常用工具	介绍漏洞扫描系统提供的常用工具及使用方法。

9.1 状态

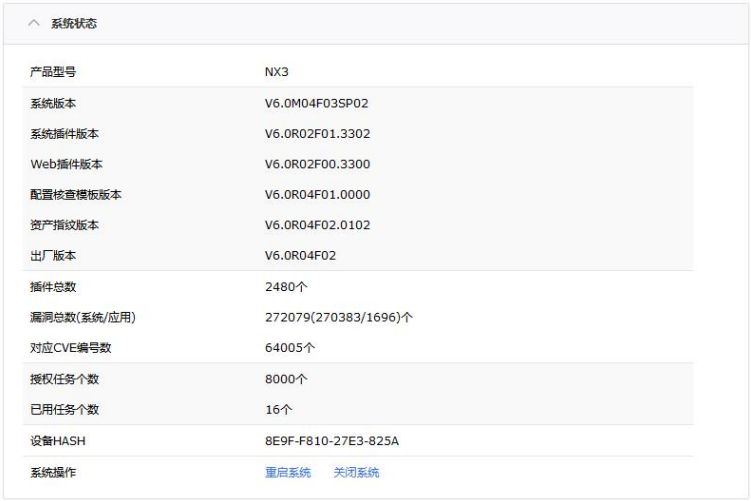
通过查看状态，管理员可以了解当前漏洞扫描设备的系统状态、授权注册信息、网络状态，并能进行基本的操作。

9.1.1 查看漏洞扫描状态

9.1.1.1 查看系统状态

进入 **系统管理** > **状态** 页面，如图 9-1 所示，管理员不仅可以查看当系统状态，还可以单击重启系统、关闭系统，对设备进行重启、关闭操作。

图 9-1 系统状态

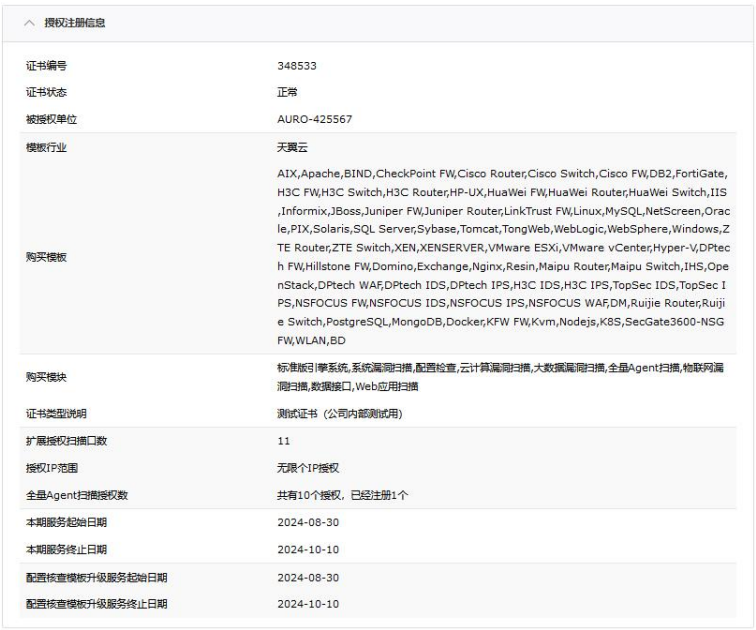


9.1.1.2 查看授权注册信息

进入 **系统管理** > **状态** > **状态** > **状态** 页面，管理员可以查看设备的授权注册信息，如图 9-2 所示。

注意	• 证书的有效时间从“本期服务起始日期”的 0 点到“本期服务终止日期”的 24 点。 • 正式证书的日期指的是产品升级授权服务日期，测试证书为产品的使用日期。 • 正式证书到期后，产品可以正常使用，但不能升级；测试证书到期后，漏洞扫描系统自动跳转到证书导入界面，且不能进行其他任何功能操作。正式证书和测试证书在证书日期内都可以升级，定制产品根据项目要求确定。 • 正式证书终止日期前一个月提醒用户当前证书的到期日期，并提醒用户更换证书；证书过期后，将提醒用户过期天数。测试证书不予提醒。

图 9-2 授权注册信息



9.1.2 查看网络状态

进入 **系统管理 > 状态 > 网络状态** 页面，如图 9-3 所示。选择需要查看的“接口”，在网络流量图中展示当前 20 分钟内的接口接收和发送流量。

将鼠标放置在图中节点处，展示该时间点的具体接口流量数据。

图 9-3 网络状态

9.2 配置

配置包括网络配置、路由配置、系统配置、任务配置。

9.2.1 网络配置

在网络配置功能模块，管理员可以对漏洞扫描设备的各个网络扫描接口进行管理和配置 DNS 服务器。

网络扫描接口，就是设备用于与其他设备交换扫描结果数据并相互作用的部分，其功能就是完成设备之间的数据交换。物理接口真实存在、有相应的硬件支持，如漏洞扫描系统支持的 eth1、eth2、eth3、eth4、eth5、eth6。

说明	扫描接口的可用数量由证书控制，管理员只能对证书授权的扫描接口进行配置。

9.2.1.1 接口配置

进入 **系统管理 > 配置 > 配置　网络** 页面，如图 9-4 所示。单击接口列表操作栏中的**【编辑】**，编辑接口基本参数即可。参数说明如表 9-1 所示。接口基本参数配置完成后，管理员可以进行**【启用网口】**和**【禁用网口】**的操作。

图 9-4 网络

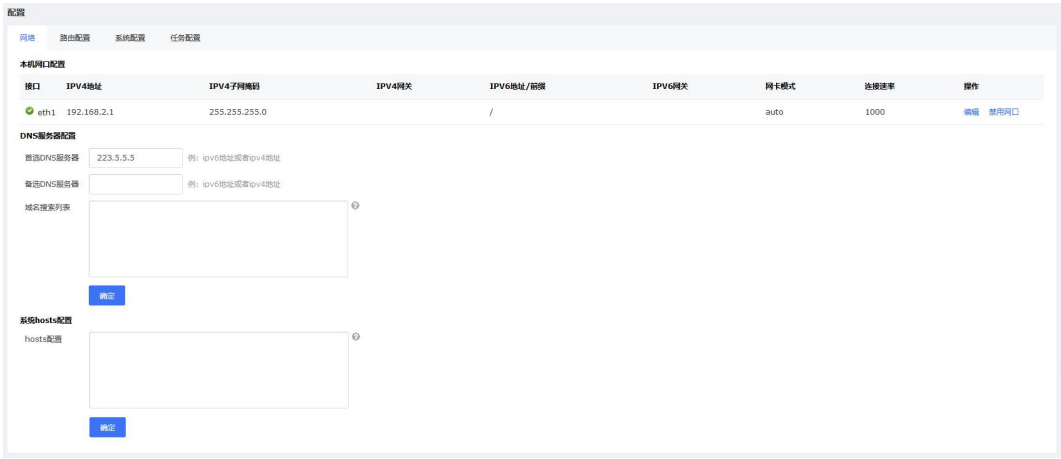


表 9-1 接口基本参数

配置项	说明
接口名称	接口的名称，不能修改。
IPV4 配置方式	IPV4 地址的配置方式，可选项有：手动配置和自动获取。
IPV4 地址	接口的 IPV4 地址。 仅当配置方式选择“手动配置”时需要手动配置接口的 IPV4 地址。
IPV4 子网掩码	接口的 IPV4 子网掩码。

配置项	说明
IPV4 网关	接口的 IPV4 网关。 如果需要跨网段进行扫描，则必须正确配置网关地址。
缺省网关	是否启用 IPV4 缺省网关。
IPV6 配置方式	IPV6 地址的配置方式，可选项有：手动配置和自动获取。
IPV6 地址	接口的 IPV6 地址。 仅当配置方式选择“手动配置”时需要手动配置接口的 IPV6 地址。
IPV6 前缀长度	接口的 IPV6 地址前缀长度。 IPV6 地址中的前缀相当于 IPV4 地址中的网络 ID，前缀长度即 IPV6 地址中用于表示路由的位数。设备间想要不经过路由器直接通信，要求前缀相同。
IPV6 网关	接口的 IPV6 网关。 如果需要跨网段进行扫描，则必须正确配置网关地址。
缺省网关	是否启用 IPV6 缺省网关。
网卡模式	设置接口的网卡模式。可选项有：auto、半双工、全双工。
连接速率	接口的连接速率。

9.2.1.2 DNS 服务器配置

进入 **系统管理 > 配置> 网络** 页面，在 DNS 服务器配置区域，如图 9-5 所示，配置参数即可。DNS 服务器参数如表 9-2 所示。

图 9-5 DNS 服务器配置

表 9-2 DNS 服务器参数

配置项	说明
首选 DNS 服务器	漏洞扫描设备使用的首选 DNS 服务器。

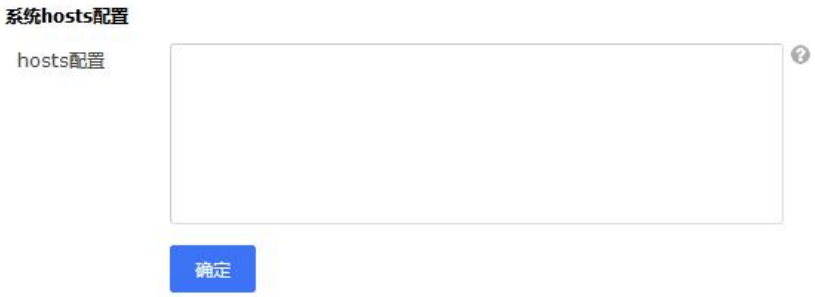
配置项	说明
	有些扫描插件和系统功能依赖站点解析，所以必须正确配置站点服务器。
备选 DNS 服务器	漏洞扫描设备的备选 DNS 服务器。 有些扫描插件和系统功能依赖站点解析，所以必须正确配置站点服务器。
域名搜索列表	若内网环境存在域的划分，在访问目标站点时会存在跳转，为了避免跳转地址使用不完整域名（未包含域部分），造成域名解析失败的问题，可以配置域名搜索列表。 多个独立域名之间可用英文符号“,”、“;”、空格分隔符隔开。

9.2.1.3 系统 hosts 配置

Hosts 的作用是将一些常用的域名与其对应的 IP 地址建立一个关联“数据库”，扫描域名时，漏洞扫描会自动从 Hosts 配置中寻找对应的 IP 地址进行扫描，若无法找到，则提交至 DNS 域名解析服务器进行解析。

进入 **系统管理 > 配置 > 网络** 页面，在系统 hosts 配置区域，如图 9-6 所示，按照界面提示配置 hosts 配置参数即可。

图 9-6 系统 hosts 配置



9.2.2 路由配置

路由是系统根据路由表中的路径，将网络中的数据包从一个源地址转发到另一个目的地址的过程。

漏洞扫描设备中路由的主要工作是为经过它的每个数据包寻找下一跳路由设备或目的主机，并把这些数据包转发出去。

管理员可以手动设置漏洞扫描设备中的静态路由。进入 **系统管理 > 配置 > 路由配置** 页面，单击**【添加】**按钮，配置路由参数即可新建一条路由，如图 9-7 所示。参数说明如表 9-3 所示。

- 新建路由后，可以执行编辑和删除等操作。
- 单击**【路由信息表】**按钮，可跳转到菜单 **系统管理 > 常用工具 > 路由信息**，查看详细的路由信息。

图 9-7 路由配置

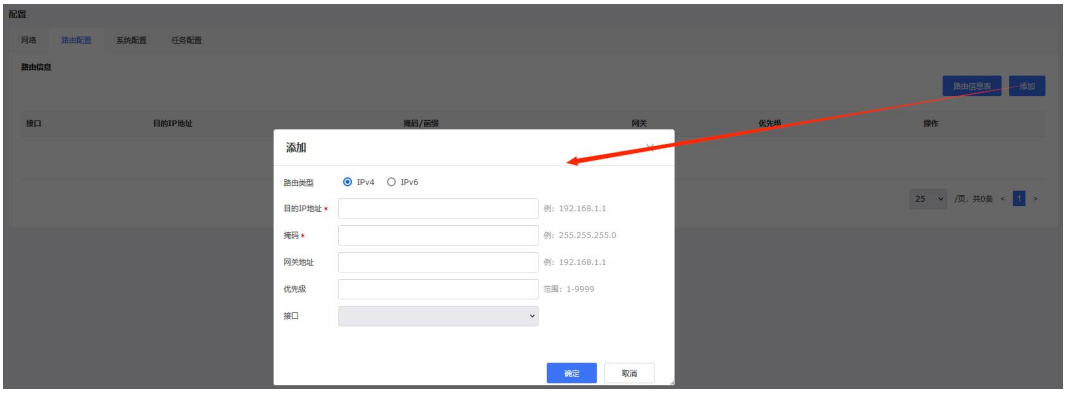


表 9-3 路由参数

配置项	描述
路由类型	路由的类型，可选项有 Ipv4 和 Ipv6。
目的 IP 地址	数据包要被送达的目的主机或目的网段的 IP 地址。 IP 地址类型必须与路由类型中的设置匹配。
掩码/前缀	目的地址（IPv4）的子网掩码或目的地址（IPv6）的前缀。
网关地址	网络接口的下一跳 IP 地址。
优先级	路由条目的优先级，取值范围为 1~9999，数据越小表示其优先级别越高。当到达同一目的的多条路由条目的管理距离相同时，表示实现多链路的负载均衡。
接口	漏洞扫描转发数据包的出口接口。

9.2.3 系统配置

系统配置主要是关于系统参数的配置。

9.2.3.1 系统时间同步设置

漏洞扫描系统的内置时钟，是系统记录日志信息、下发扫描任务等操作的时间基准，因此时间的精确性会对这些事件产生直接影响。漏洞扫描为了解决此类问题提供了系统时间管理功能，导入正式证书后，管理员才能配置系统时间。

进入 **系统管理 > 配置> 配置 > 系统配置** 页面，在“系统时间同步设置”区域，配置参数即可，如图 9-8 所示。时间参数说明如表 9-4 所示。

图 9-8 系统时间同步设置

表 9-4 系统时间参数

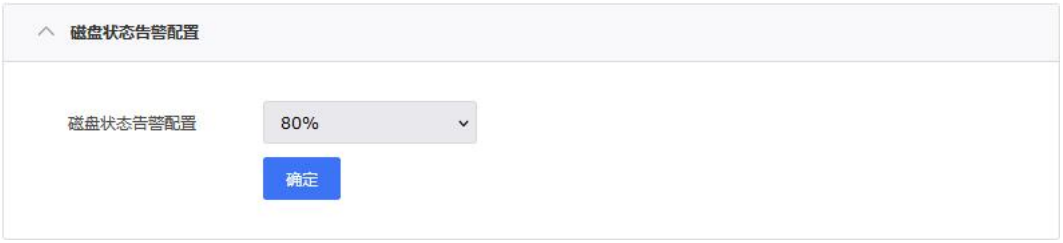
配置方式	配置项	说明
与NTP服务器同步	同步时间配置	配置时间服务器的站点或 IP 地址，单击【确定】按钮。
	自动同步	勾选后，自动同步该设备的时间。
	【同步】	立即与时间服务器同步。
手动修改	修改当前时间	手动设置漏洞扫描设备的当前日期和时间。 时间格式：2013-05-08 10:27:04。

9.2.3.2 磁盘状态告警配置

磁盘中存储的数据达到磁盘状态告警配置中设置的百分比，系统将发出告警，通知管理员。

进入 **系统管理 > 配置 >系统配置** 页面，在“磁盘状态告警配置”区域，配置告警百分比即可，系统默认值为 80%，如图 9-9 所示。

图 9-9 磁盘状态告警配置



9.2.3.3 登录失败配置

为了保证漏洞扫描设备安全性，防止恶意的多次尝试密码登录，系统设置了登录失败控制功能，管理员可以设置允许的最大登录重试次数、超过最大重试次数后的处理方法，并且可以解锁被锁定的 IP 或帐号。

进入 **系统管理 > 配置 > 系统配置** 页面，在“登录失败配置”区域，配置参数即可，如图 9-10 所示。登录失败参数说明如表 9-5 所示。

帐号被锁定后，单击【解锁 ip/帐号】按钮，可以选择需要解锁的 IP 或帐号进行解锁。

图 9-10 登录失败配置

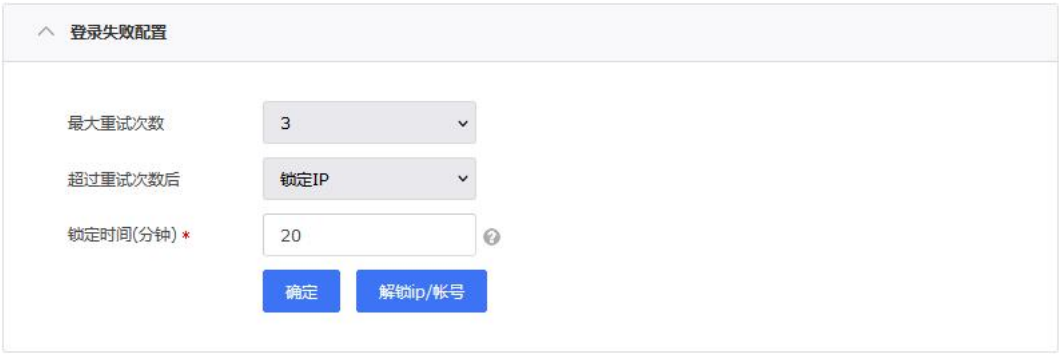


表 9-5 登录失败参数

配置项	说明
最大重试次数	系统允许的最大登录重试次数，可选值为 3～10。
超过重试次数后	超过最大重试次数后系统将会采取的处理方式。可选项有：不处理、锁定 IP 和锁定帐号。
锁定时间（分钟）	设定 IP 或帐号的锁定时间，默认为 20 分钟。仅当“超过重试次数后”选择锁定 IP 或锁定帐号时该参数配置生效。

9.2.3.4 密码策略配置

为了保证漏洞扫描系统安全，通过设定密码策略控制管理员密码安全系数，从登录源头对系统安全进行控制。

进入 **系统管理 > 配置 >系统配置** 页面，在“密码策略配置”区域，配置参数即可，如图 9-11 所示。密码策略参数说明如表 9-6 所示。

图 9-11 密码策略配置

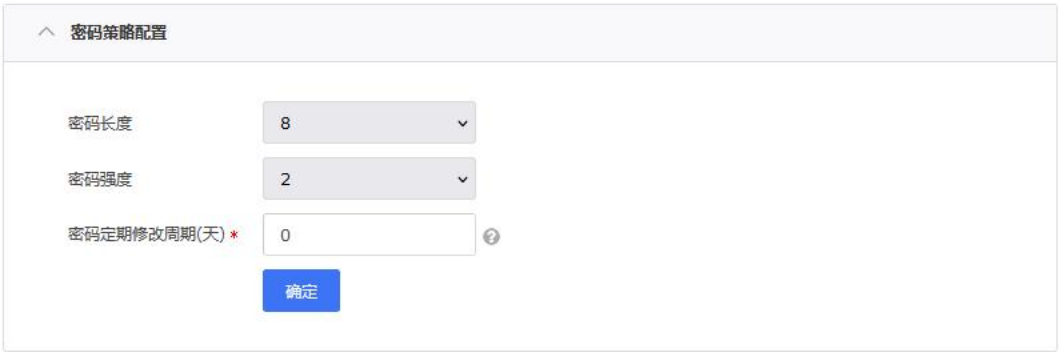


表 9-6 密码策略参数

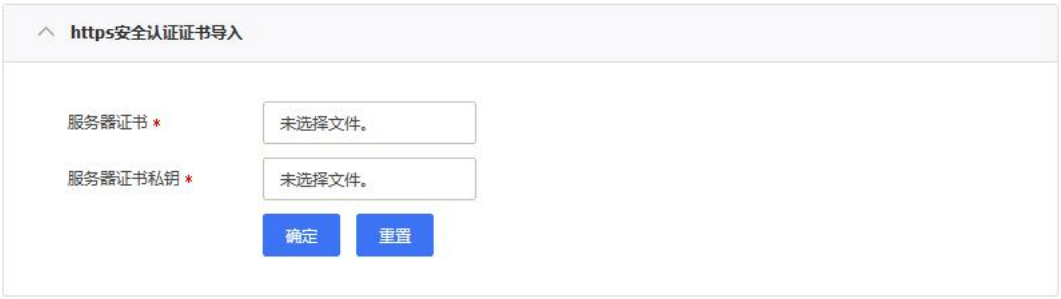
配置项	描述
密码长度	管理员密码的最小长度。长度范围 8～32 个字符。
密码强度	漏洞扫描管理员密码强度。密码强度范围 1～4。 • 1：至少包含小写字母、大写字母、数字、特殊字符（@、#、$、^、_）中的 1 种字符。 • 2：至少包含小写字母、大写字母、数字、特殊字符（@、#、$、^、_）中的 2 种字符。 • 3：至少包含小写字母、大写字母、数字、特殊字符（@、#、$、^、_）中的 3 种字符。 • 4：至少包含小写字母、大写字母、数字、特殊字符（@、#、$、^、_）中的 4 种字符。
密码定期修改周期(天)	漏洞扫描管理员密码定期修改的周期。

9.2.3.5 https 安全认证证书导入

通过 https 安全认证证书可以激活 https 安全认证协议，实现客户端和漏洞扫描之间的数据通信加密，防止数据信息的泄露。

进入 **系统管理 > 配置 >系统配置** 页面，在“https 安全认证证书导入”区域，导入服务器证书（.crt）和服务器证书私钥（.key）即可，如图 9-12 所示。

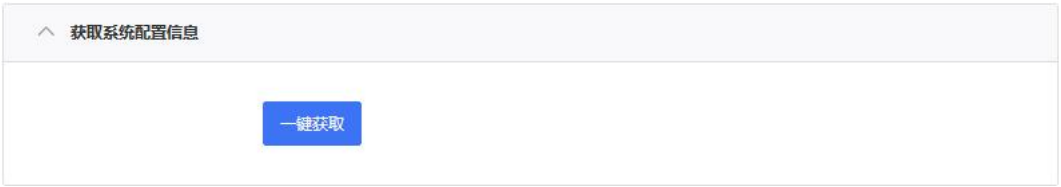
图 9-12 https 安全认证证书导入



9.2.3.6 获取系统配置信息

进入 **系统管理 > 配置 >系统配置** 页面，在“获取系统配置信息”区域，如图 9-13 所示，单击【一键获取】按钮，下载压缩包至本地保存；使用密码“漏洞扫描设备的 HASH”，解压压缩包，查看系统信息即可。

图 9-13 获取系统配置信息



9.2.3.7 SNMP Trap 设置

漏洞扫描系统支持 SNMP（Simple Network Management Protocol，简单网络管理协议）管理，漏洞扫描设备可以响应 SNMP 管理主机的查询，向 SNMP 管理主机返回相应的运行状态信息，同时也可以主动地向 SNMP 管理主机发送 Trap 消息。

进入 **系统管理 > 配置 >系统配置** 页面，在“SNMP Trap 设置”区域，如图 9-15 所示，配置 SNMP Trap 参数即可。参数说明如表 9-8 所示。

图 9-14 SNMP Trap 设置

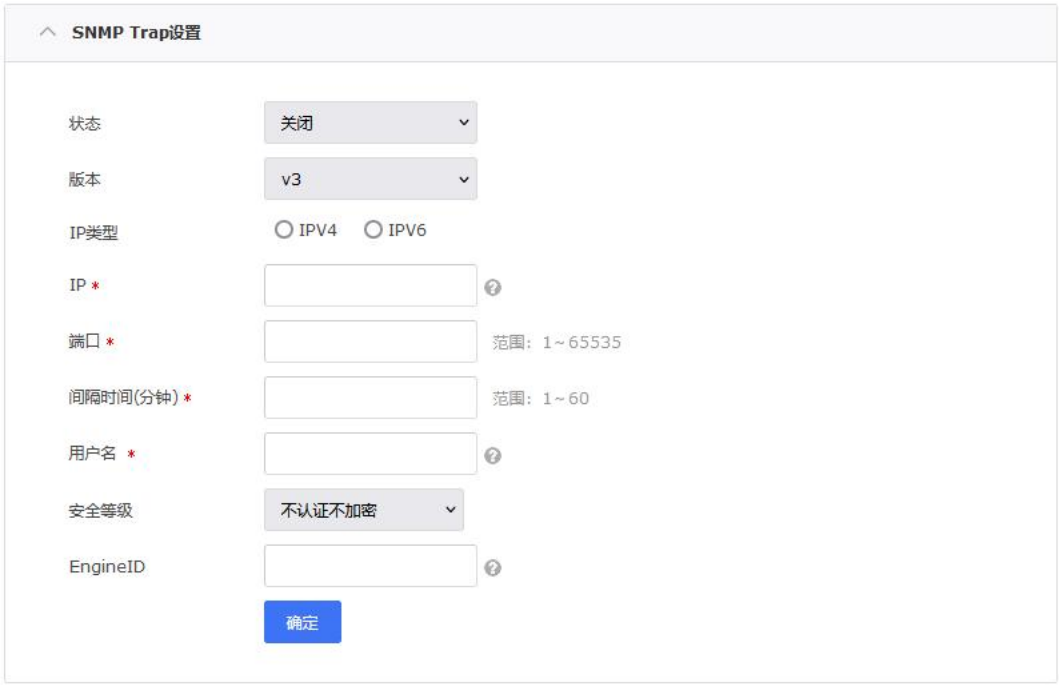


表 9-7 SNMP Trap 参数

配置项	说明
状态	设备作为 SNMP Trap 的状态。可选项有：关闭、开启。
版本	设备支持的 SNMP 协议版本。可选项有：v1、v2 和 v3。
IP 类型	SNMP 管理主机的 IP 地址类型，支持 IPv4 和 IPv6。

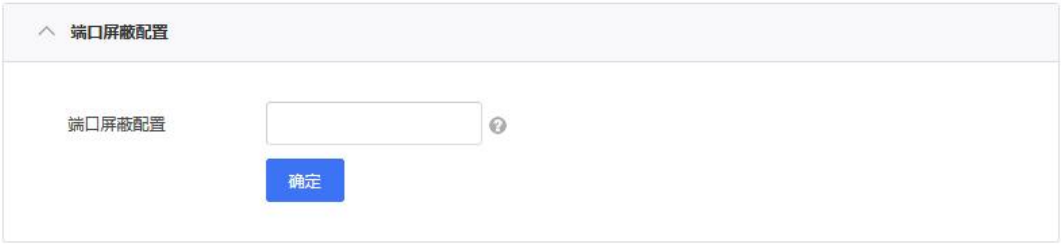
配置项		说明
IP		IPv4 或 IPv6 地址，格式可参考界面帮助文字。
端口		设备用于和 SNMP 管理主机通信的端口号。
间隔时间（分钟）		与 SNMP 管理主机通信的间隔时间。
v1/v2	Community	SNMP 管理主机访问漏洞扫描设备时使用的团体名。
v3	用户名	SNMP v3 用户的名称。至少 8 位，不包含中文及特殊字符。
	安全等级	SNMP v3 认证的安全级别，可选项有：不认证不加密、只认证、认证且加密。
	认证协议	进行认证时使用的认证协议，可选项：MD5 和 SHA。
	认证 Key	进行认证时使用的认证密码。密码至少 8 位，由数字和字母组成。
	加密协议	加密传送信息时使用的加密算法，可选项：DES 和 AES。
	加密 Key	进行信息加密时使用的密码。密码至少 8 位，由数字和字母组成。
	EngineID	SNMP 引擎的 SnmpEngineID，十六进制数，长度范围为 10~64 个字符，例 0x1234567890。

9.2.3.8 端口屏蔽配置

漏洞扫描进行扫描时，将跳过端口屏蔽设置中的端口。

进入 **系统管理 > 配置 >系统配置** 页面，在“端口屏蔽配置”区域，如图 9-16 所示，配置端口屏蔽参数即可。可配置多个端口（用逗号隔开）及连续端口（例：11-200）。

图 9-15 端口屏蔽配置

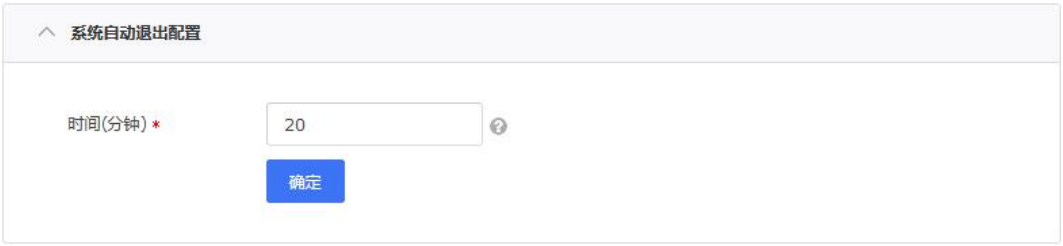


9.2.3.9 系统自动退出配置

为保证漏洞扫描设备安全性，系统还提供了系统自动退出时间设置。当管理员登录 Web 界面对系统进行管理时，如果在设定的自动退出时间内无任何操作，系统将自动退出，管理员再次进行操作时，系统会跳转到登录页面。

进入 **系统管理 > 配置 >系统配置** 页面，在“系统自动退出配置”区域，设置自动退出时间即可，如图 9-17 所示。系统自动退出时间设置范围为 0～999999 分钟，0 表示关闭自动退出检查功能，默认系统自动退出时间为 10 分钟。

图 9-16 系统自动退出配置



9.2.3.10 认证管理配置

漏洞扫描设备支持与堡垒机进行联动，正确配置堡垒机信息后，漏洞扫描设备可以从堡垒机获取被扫描主机的认证信息。

进入 **系统管理 > 配置 >系统配置** 页面，在“认证管理配置”区域，如图 9-18 所示，配置参数即可。堡垒机参数说明如表 9-9 所示。

图 9-17 认证管理配置

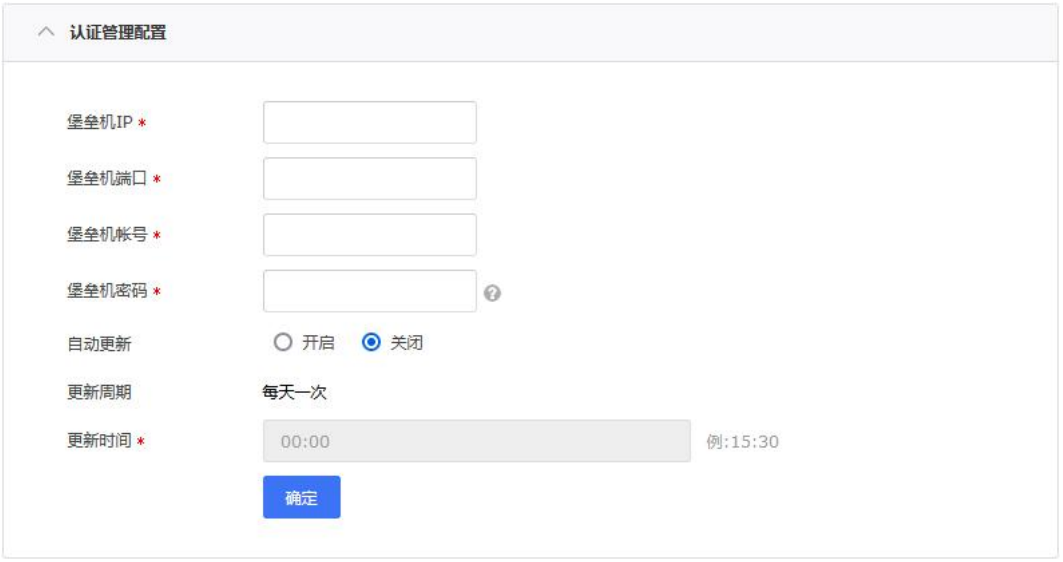


表 9-8 堡垒机参数

配置项	说明
堡垒机 IP	堡垒机的 IP 地址。
堡垒机端口	堡垒机的 SSH 协议端口号，默认为 22，需要与堡垒机的配置保持一致。
堡垒机帐号	登录堡垒机使用的帐号。
堡垒机密码	登录堡垒机使用的帐号的密码。
自动更新	自动从堡垒机更新主机信息的时间。更新周期默认“每天一次”，管理员

配置项	说明
更新周期	可以配置每天进行自动更新的具体时间。
更新时间	

9.2.3.11 http host 头配置

开启该功能可以增强系统防御力。开启后，只有使用 http host 列表中以及网口配置中的 IP 或域名才能访问漏洞扫描，无法通过其他域名或者 IP 访问漏洞扫描。

进入 **系统管理 > 配置 >系统配置** 页面，在“http host 头配置”区域，如图 9-19 所示，开启“http host 头防御”，配置“自定义 Host 头”，单击【添加】按钮，将自定义 Host 头记录至列表中即可。

示例：漏洞扫描的 IP 地址为 10.65.20.172，添加自定义的 HOST 头 aaa.com 后，可以使用 https://aaa.com 访问该漏洞扫描。

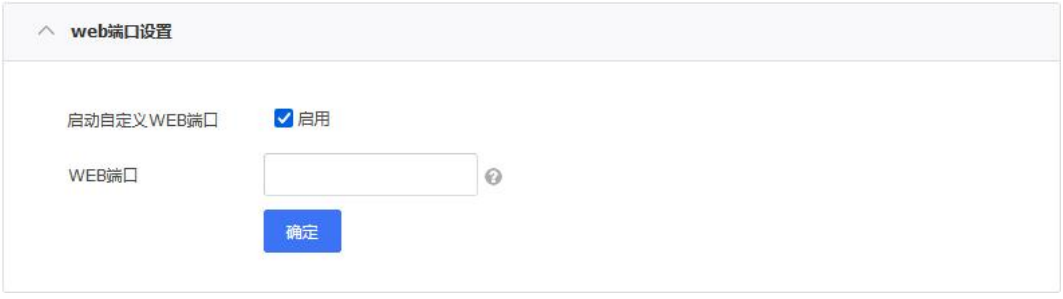
图 9-18 http host 头配置

9.2.3.12 web 端口设置

用户启动自定义 WEB 端口后，需要通过该自定义 WEB 端口访问漏洞扫描。

进入 **系统管理 > 配置 >系统配置** 页面，在“web 端口设置”区域，如图 9-20 所示，勾选“启用”，配置自定义的“WEB 端口”即可。

图 9-19 web 端口设置



9.2.4 任务配置

任务配置主要是任务相关参数的配置。

9.2.4.1 邮件服务器设置

漏洞扫描设备可以存储一定数量的离线报表，以供管理员后期查看，由于设备自身存储空间有限，漏洞扫描同时支持使用邮件服务器来辅助存储报表。邮件服务器也可以用于邮件告警。

使用邮件服务器存储离线报表功能以及邮件告警功能的启用都依赖于正确配置报表邮件服务器。

进入 **系统管理 > 配置 > 任务配置** 页面，在“邮件服务器设置”区域，如图 9-21 所示，配置邮件服务器参数即可。参数说明如表 9-10 所示。

图 9-20 邮件服务器设置

表 9-9 邮件服务器参数

配置项	说明
认证方式	登录邮件服务器的认证方式。
邮件服务器地址	邮件服务器的 IP 地址。地址可以是 IP 地址（支持 IPV4 和 IPV6），也可以是域名。
端口	邮件服务器用于发送邮件的端口。
邮箱帐号	用户登录邮件服务器的邮箱。
密码	用户登录邮件服务器的邮箱密码。
【测试邮箱配置】	漏洞扫描会向邮箱帐号发送一封邮件，测试邮件服务器的配置是否正确。

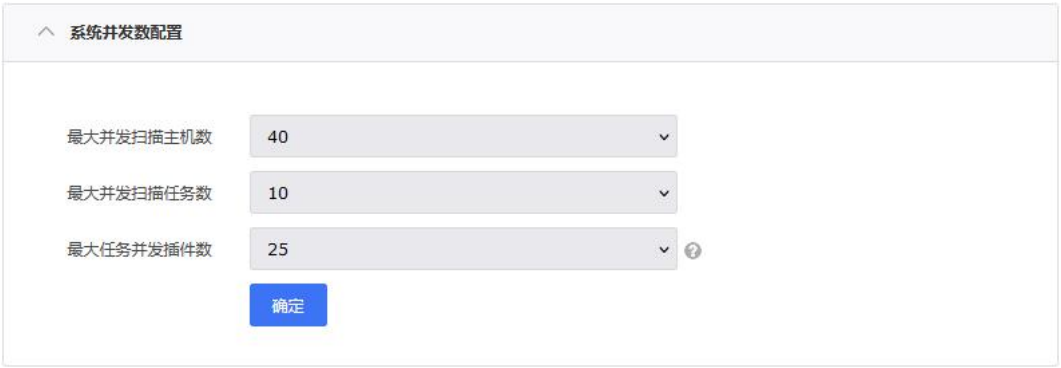
9.2.4.2 系统并发数配置

并发任务是指同一时间内多个任务请求可以得到处理，漏洞扫描系统支持系统任务并发。

进入 **系统管理 > 配置 > 任务配置** 页面，在“系统并发数配置”区域，如图 9-22 所示，配置参数即可。

- 最大并发扫描主机数是指，同一时间内系统支持执行的多个扫描任务中所有主机的最大数目。
- 最大并发扫描任务数是指，同一时间内系统支持执行扫描任务的最大数目。
- 最大任务并发插件数是指，同一时间内系统支持执行的多个扫描任务中所有插件的最大数目。

图 9-21 **系统并发数配置**



9.2.4.3 风险值计算标准配置

进入 **系统管理 > 配置 > 任务配置** 页面，在“风险值计算标准配置”区域，单击【配置】按钮，配置各类评定标准和进行权重配置即可制定个性化的风险值计算标准即可，如图 9-23 所示。

- 主机风险等级

  主机风险等级是按照主机的漏洞、配置风险值对主机进行的风险等级划分。首先漏洞扫描按照公司风险评估模型计算得到主机风险值，然后按照主机风险等级评定标准将主机威胁划分为非常危险、比较危险、比较安全和非常安全四个类别。

- 网络风险等级

  网络风险等级是网络中所有主机威胁分值的加权平均值。首先漏洞扫描按照公司风险评估模型计算得到网络风险值，然后按照网络风险等级评定标准将网络中所有主机划分为非常危险、比较危险、比较安全和非常安全四个类别。

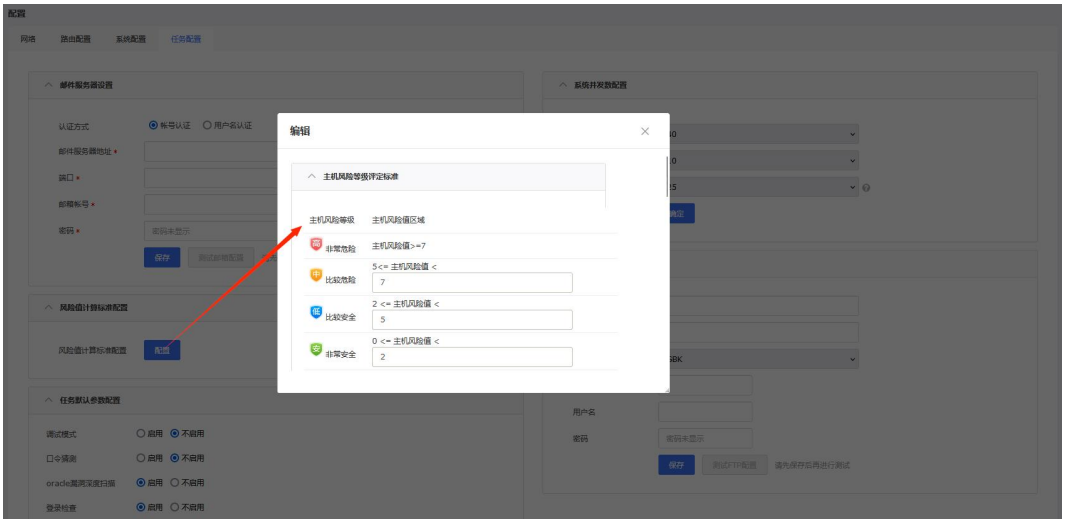
- 站点风险等级

  站点风险等级是根据当前站点的威胁分值计算得出的。首先漏洞扫描按照公司风险评估模型计算得到站点威胁分值，然后按照站点风险等级评定标准，将网络中所有站点划分为非常危险、比较危险、比较安全和非常安全四个类别。

- 主机风险值权重

主机综合风险值根据漏洞风险和配置风险所占比重，按照公司风险评估模型计算得到。所以首先需要配置漏洞风险和配置风险在评估模型中所占的比例。

图 9-22 风险值计算标准配置



9.2.4.4 报表 FTP 设置

将报表备份到 FTP/SFTP 服务器功能的实现是以正确配置 FTP/SFTP 服务器为前提的。

进入 **系统管理 > 配置 > 任务配置** 页面，在“报表 FTP 设置”区域，如图 9-24 所示，配置服务器参数即可。FTP/SFTP 服务器的参数如表 9-11 所示。

图 9-23 报表 FTP 设置

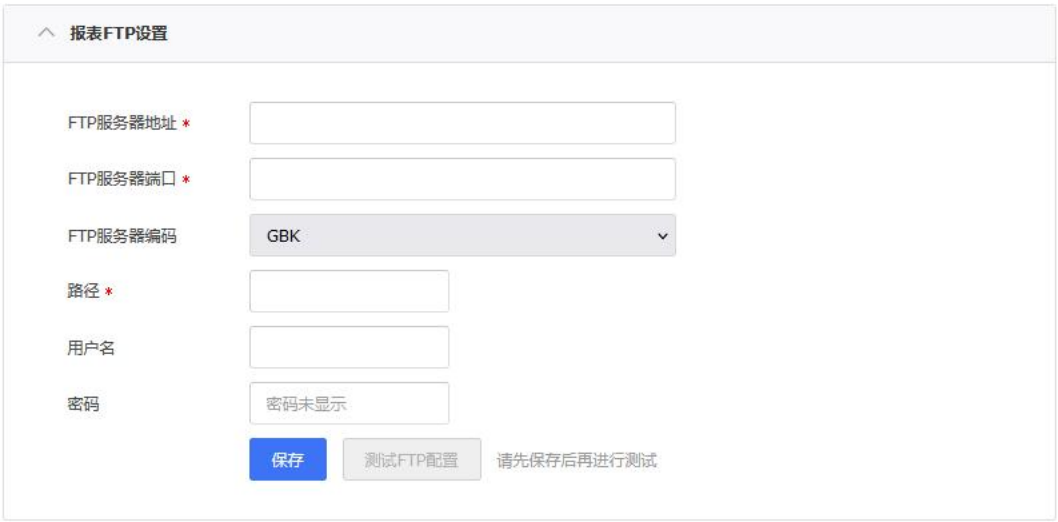


表 9-10 FTP/SFTP 服务器参数

配置项	描述
FTP 服务器地址/端口	FTP/SFTP 备份服务器的 IP 地址/端口。服务器地址可以是 IP 地址（支持 IPV4 和 IPV6），也可以是域名。
FTP 服务器编码	FTP/SFTP 服务器存储报表的编码方式。 若 FTP/SFTP 服务器为 Windows 服务器，且 FTP/SFTP 服务器编码为 UTF-8，则 新建任务 的“任务名称”必须为英文、并启用“自动生成报表”和“FTP 上传”，FTP/SFTP 服务器才能正常接收扫描任务的报表。
路径	将日志信息备份到 FTP/SFTP 服务器的哪个目录下。根目录使用“/”表示。
用户名/密码	登录 FTP/SFTP 服务器的用户名及其密码。该帐号必须具有读写权限。
【测试 FTP 配置】	漏洞扫描会向 FTP 服务器上传一个文件，测试 FTP 服务器的配置是否正确。

9.2.4.5 任务默认参数配置

进入 **系统管理 > 配置 > 任务配置** 页面，在“任务默认参数配置”区域，如图 9-25 所示，可以对部分任务参数的默认值进行统一管理。默认参数的参数说明如表 9-12 所示。

图 9-24 任务默认参数配置

表 9-11 默认参数

配置项	描述
调试模式	默认不启用。 预防出现扫描任务异常时，可以启用该参数。记录扫描任务的执行信息，当任务执行异常，导出异常信息并发送给公司的技术支持人员进行错误分析。
口令猜测	默认不启用。 开启口令猜测后，若未对主机进行登录扫描，漏洞扫描将根据 密码字典 的内容对扫描目标进行口令破解。
oracle 漏洞深度扫描	默认启用。

配置项	描述
	• 不启用：漏洞扫描只报出 oracle 相关服务识别和原理扫描漏洞。 • 启用：漏洞扫描报出所有漏洞，包括本地 oracle 漏洞。此时需要 手动新建认证信息，启用并配置漏扫策略的 Oracle 相关参数。
登录检查	默认启用。 启用后，在新建评估任务时，默认启用“登录检查”主机的配置是否合规。
OpenSSH 远程版本扫描	默认不启用。 • 启用：对 OpenSSH 进行远程版本扫描。 • 不启用：不对 OpenSSH 进行远程版本扫描。
NTP 远程版本扫描	默认不启用。 • 启用：对 NTP 进行远程版本扫描。 • 不启用：不对 NTP 进行远程版本扫描。

9.2.4.6 免密登录 SSH 密钥导入

进行免密登录 SSH 密钥导入后，漏洞扫描系统可以通过密钥对直接登录目标机，无需单独配置登录的用户名和密码。

免密登录 SSH 密钥导入具体操作如下：

步骤 1 （可选）若免密登录的目标机需要配置公钥信息，进入 **系统管理 > 配置 > 任务配置** 页面，在“免密登录 SSH 密钥导入”区域，单击文字链接【一键获取公钥】，使用下载后的公钥文件完成目标机的配置。

步骤 2 （可选）获取密钥对。

a. 若目标机无密钥对，利用密钥生成工具或者命令，生成密钥对。

b. 在目标主机中配置支持密钥登录及公钥信息，使用公钥对漏洞扫描系统的登录进行验证。

步骤 3 进入 **系统管理 > 配置 > 任务配置** 页面，在“免密登录 SSH 密钥导入”区域，导入本地的漏洞扫描系统登录目标机的密钥对后，漏洞扫描系统可以使用私钥直接登录目标主机。

成功导入密钥对后的页面如图 8-2 所示。

图 9-25 **成功导入密钥对**

----结束

9.3 服务

在服务模块，可以升级/还原系统和对漏洞扫描提供的服务进行管理。

9.3.1 系统升级

漏洞扫描系统支持定时自动升级、立即升级（管理员手动检查升级服务器中是否存在新的升级包，在检查到新升级包后漏洞扫描立即升级设备）和手动升级（管理员手动上传升级包升级）。

9.3.1.1 定时升级

若漏洞扫描设备能够与升级服务器正常连接通信，可以定时自动升级设备。

进入 **系统管理 > 服务 > 系统升级** 页面，在“定时升级”区域，如图 9-26 所示，配置定时升级参数即可。参数说明如表 9-13 所示。

图 9-26 定时升级

表 9-12 自动升级参数

配置项	描述
升级站点	设备获取升级包文件的升级服务器地址。
升级周期	每天一次，系统每天检查一次升级服务器中是否有新的升级包。
更新时间	系统每天检查升级服务器中是否有新的升级包的时间。 更新时间的格式如 12:38。
安装方式	指检查到升级服务器中有新升级包时，升级包的安装方式。 • 自动安装：如果检查到了新升级包，则将其提交到升级队列，然后系统会自动升级。 • 提醒：检测到新升级包不自行更新，通过 Web 管理界面右下角提示【有可用升级包】，单击后进入系统升级管理页面，可以根据需要 立即升级 设备。 • 关闭自动更新：禁用定时自动升级功能。
使用 HTTP 代	当漏洞扫描设备需要通过 HTTP 代理才能连接到升级服务器时，必须启用该功能

配置项	描述
理	后，配置代理服务器的地址、端口、登录用户名和登录密码。

9.3.1.2 立即升级

立即升级是指管理员手动检查升级服务器中是否有新的升级包，漏洞扫描在检查到新升级包后立即升级设备。

进入 **系统管理 > 服务 > 系统升级** 页面，在“立即升级”区域，选择需要升级的升级包类型，单击【立即更新】按钮即可。

- 单击【检查更新】按钮，系统立刻连接到升级服务器中并检测是否有新的升级包，并显示可用更新个数；单击该个数，可以查看升级包信息。
- 单击【历史更新】，可以确认更新是否成功及查看系统进行过的所有更新操作。
- 单击【*0* 个可用更新】，可以查看可用升级包。

图 9-27 立即升级

9.3.1.3 手动升级

当漏洞扫描设备无法正常连接到升级服务器时，通常需要管理员手动升级设备。

进入 **系统管理 > 服务 > 系统升级** 页面，在“手动升级”区域，选择升级包文件进行升级即可，如图 9-28 所示。

升级包的下载路径请参见界面介绍。

说明	• 当手动升级时，系统存在正在执行的扫描任务，则不能进行升级。 • 当手动升级时，系统存在正在执行的还原操作，则不能进行升级。 • 手动升级的过程中，需要根据升级包的版本依次升级。

图 9-28 手动升级

9.3.2 系统服务

通过漏洞扫描系统提供的系统服务功能，在导入远程协助组件后，管理员可以便捷开启远程协助、专家诊断、DNS 缓存、诊断日志 Debug 模式，下载诊断日志，进行网络抓包。

漏洞扫描远程协助组件请联系天翼云工作人员获取。

9.3.2.1 DNS 缓存

为提高 Web 扫描性能，系统提供 DNS 缓存功能，即将已扫描域名对应 IP 缓存到本地，DNS 缓存每 15 分钟更新一次。默认该功能不开启。

进入 **系统管理 > 服务 >系统服务** 页面，在“DNS 缓存”区域，如图 9-29 所示，可以开启/关闭 DNS 缓存功能。

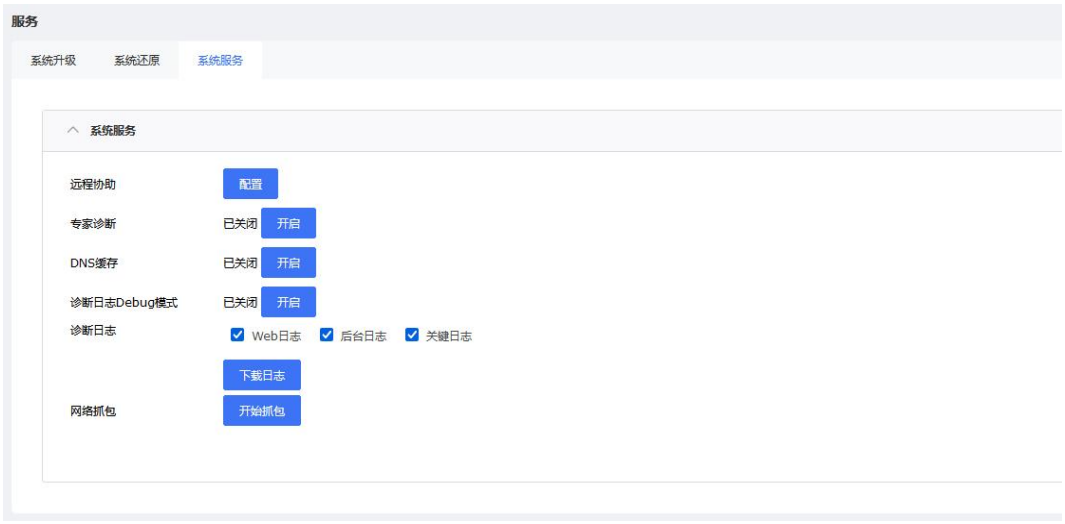
图 9-29 DNS 缓存

9.3.2.2 诊断日志 Debug 模式

系统默认记录 INFO 及以上级别的诊断日志，开启诊断日志 Debug 模式后，则记录 Debug 及以上级别的诊断日志。

进入 **系统管理 > 服务 >系统服务** 页面，在“诊断日志 Debug 模式”区域，如图 9-30 所示，可以开启/关闭诊断日志 Debug 模式。

图 9-30 **诊断日志 Debug 模式**

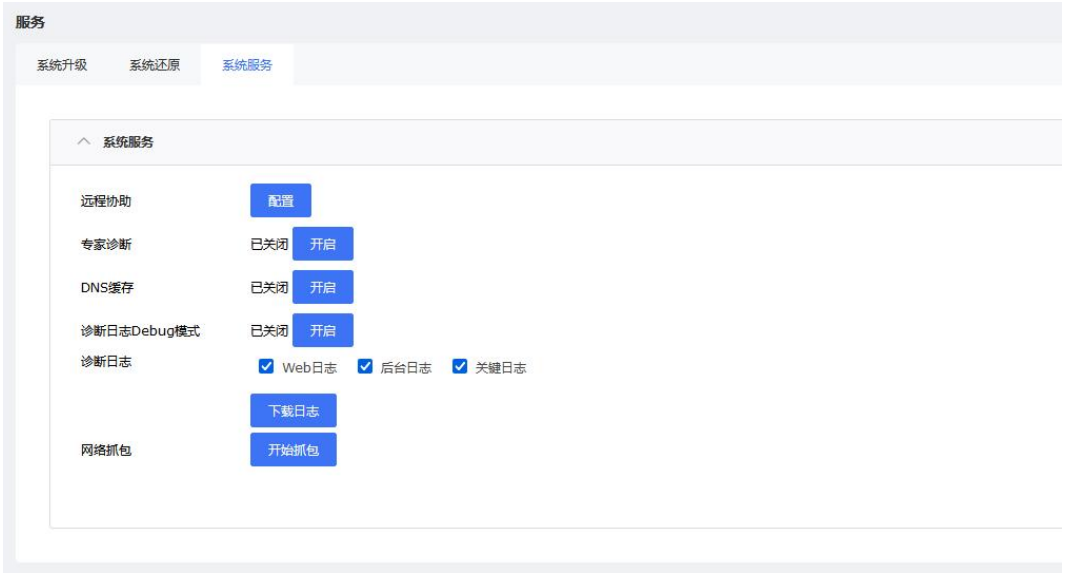


9.3.2.3 **诊断日志**

当系统出现问题时，管理员可以下载诊断日志，并将其提交给技术支持人员以便分析系统问题，建议管理员忽略诊断日志的内容。

进入 **系统管理 > 服务 >系统服务** 页面，在“诊断日志”区域，如图 9-31 所示，根据需要勾选日志类型，单击【下载日志】按钮，保存至本地即可。

图 9-31 **诊断日志**



9.4 用户

9.4.1 用户权限

初始状态下，系统中只有系统管理员 admin 以及审计管理员 auditor 两个系统用户。系统管理员 admin 可以新建两种角色（系统用户和普通用户）的用户。具体的用户权限如表 9-14 所示。

表 9-13 用户权限

用户角色	权限
系统管理员（admin）	除日志管理外的所有权限。
审计管理员（auditor）	系统默认禁用审计管理员（auditor），只有系统管理员（admin）可以启用 auditor。启用后不允许禁用，同时需要修改 auditor 的登录密码。 • 日志管理的全部权限。 • 查看和修改自身用户信息的权限。 • 导入/导出证书的权限。
系统管理员（只支持由 admin 创建）	• 系统管理员 admin 为其分配的用户权限；若未分配、则默认拥有除仪表盘配置、系统管理（用户管理）和日志管理之外的全部权限。 • 查看和修改自身用户信息的权限。
普通管理员（只支持由 admin 创建）	• 系统管理员 admin 为其分配的用户权限；若未分配、则默认拥有系统管理（状态和常用工具）、除其他系统管理菜单&联动管理&日志管理&仪表盘配置之外的全部权限。 • 查看和修改自身用户信息的权限。

9.4.2 新建用户

进入 **系统管理 > 用户 > 管理员列表** 页面，单击【**添加**】按钮，即可添加一个用户，默认启用，如图 9-32 所示。参数说明如表 9-15 所示。新建用户后，可以进行的操作如表 9-16 所示。

图 9-32 添加用户

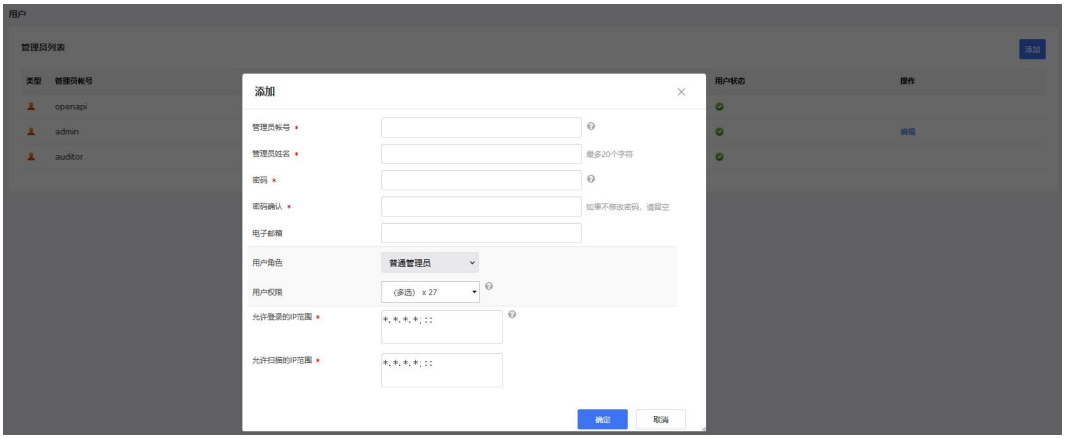


表 9-14 管理员参数

配置项	描述
管理员帐号	管理员登录系统时输入的用户名。 管理员帐号必须以字母开头，并且是字母与数字、下划线的组合，不能超过 20 个字符。
管理员姓名	管理员的姓名。不能超过 20 个字符。
密码	管理员登录漏洞扫描设备 Web 管理页面的密码。 有关密码安全性的配置请参见 密码策略配置 的相关介绍。
密码确认	再次输入管理员的登录密码确认。
电子邮箱	新建管理员的电子邮箱。
用户角色	管理员帐号隶属的用户角色。从下拉框中选择，可选项有系统管理员和普通管理员。
用户权限	管理员帐号拥有的操作权限。从下拉框中选择，可多选。 说明 • 用户角色为系统管理员时，可在所有模块权限中任意配置。 • 用户角色为普通管理员时，系统默认普通管理员拥有部分权限（认证管理、系统状态和常用工具等），可根据需要添加其他三项权限（资产管理、数据接口和证书管理）。
允许登录 IP 范围	管理员允许登录系统的 IP 范围(*.*.*.*;::表示任意 IP 地址)。支持 IPV4 地址和 IPV6 地址，多个 IP 范围或多个独立 IP 之间用逗号、分号、回车空行或空格分隔，单个 IP 地址前的“！”表示排除此 IP 地址。 • IPV4 的格式如下： 192.168.1.1 192.168.1.1-254 192.168.1/24 192.168.1.* 192.168.1-10.*

配置项	描述
	!192.168.1.1 • IPV6 格式如下： 2001::db8:2003 2001::db8:2003/96 !2001::db8:2003
允许扫描的 IP 范围	管理员被允许进行扫描的 IP 范围。 IP 地址的设置注意事项与“允许登录 IP 范围”一致，请参见表格上一行。

表 9-15 用户操作

操作	说明
启用/禁用	单击操作栏的【启用帐号】/【禁用帐号】，可以管理用户的有效性。
编辑	每个用户均可以通过单击快捷键操作栏中的***管理员帐号*** > **设置帐号**，管理自身信息。 系统管理员 admin 可以管理 admin、系统管理员和普通管理员的信息。
删除	仅系统管理员 admin 可以删除新建的用户。
重置密码	仅系统管理员 admin 可以重置新建用户的密码。 确认重置后，漏洞扫描随机生成新的密码，关闭对话框后无法查询，admin 需要及时手动复制密码并通知相应用户，如下图所示。 

9.5 常用工具

漏洞扫描提供常用工具用于设备的诊断和排错，本节介绍常用工具的使用方法。

进入 **系统管理** > **常用工具** 页面，即可使用常用工具查看当前网络的连接状态和网卡状态等信息。

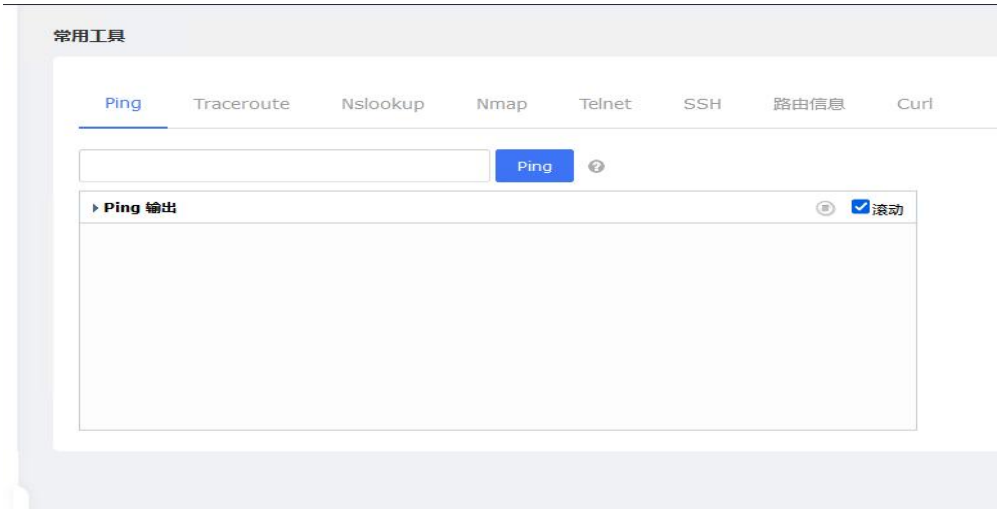
9.5.1 Ping

Ping 命令用于检测设备存活或与网络中其他设备的连接情况，帮助分析、判定网络故障。

如图 9-33 所示，在文本框中输入 IPv4 地址、IPv6 地址或主机名，单击【Ping】按钮，稍后可见执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出 Ping 命令的执行结果。

图 9-33 Ping



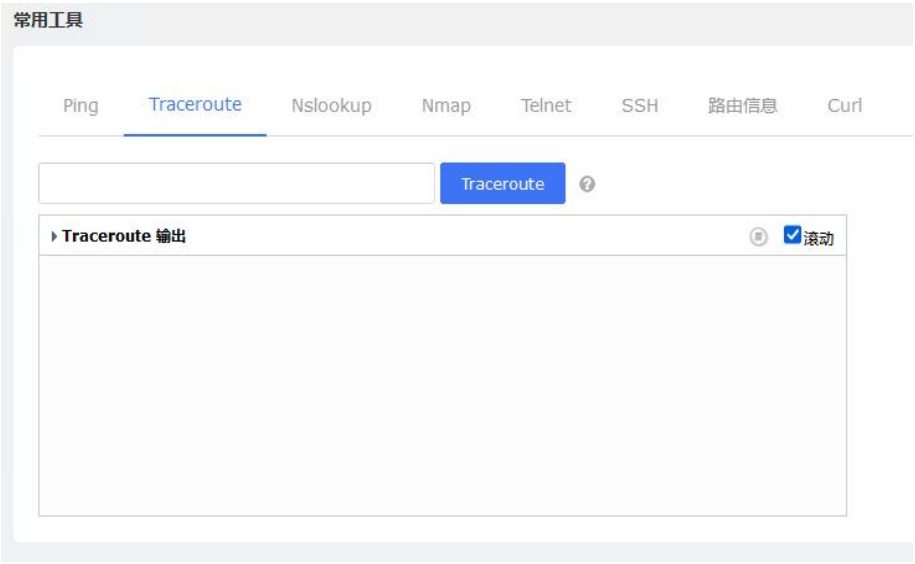
9.5.2 Traceroute

Traceroute 命令即路由追踪，用于侦测漏洞扫描设备到达目标主机所经过的路由条数。

如图 9-34 所示，在文本框中输入目标主机的 IPv4 地址、IPv6 地址或主机名，单击【Traceroute】按钮，稍后可见执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出 Traceroute 命令的执行结果。

图 9-34 Traceroute



9.5.3 Dig

Dig 是 Bind 工具的一部分（Bind 工具官方网站 http://ww.isc.org），用于从 DNS 服务器中收集信息并进行故障诊断。在文本框中输入 DNS 服务器的 IPv4 地址、IPv6 地址或主机名，单击【Dig】按钮，稍后可见执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出 Dig 命令的执行结果。

9.5.4 Nmap

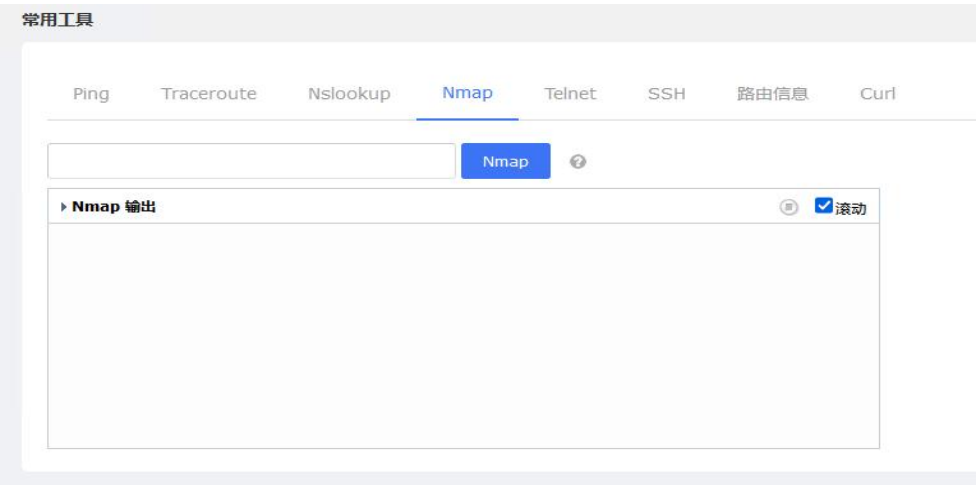
Nmap（Network Mapper）即端口扫描，是 Linux 环境下的网络扫描和嗅探工具。主要有以下三个功能：

- 探测主机是否在线。
- 扫描主机端口，嗅探端口提供的网络服务。
- 推断主机所用的操作系统。

如图 9-36 所示，在文本框中输入即将扫描主机的 IPv4 地址、IPv6 地址或主机名，单击【Nmap】按钮，稍后可见执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出 Nmap 命令的执行结果。

图 9-35 Nmap



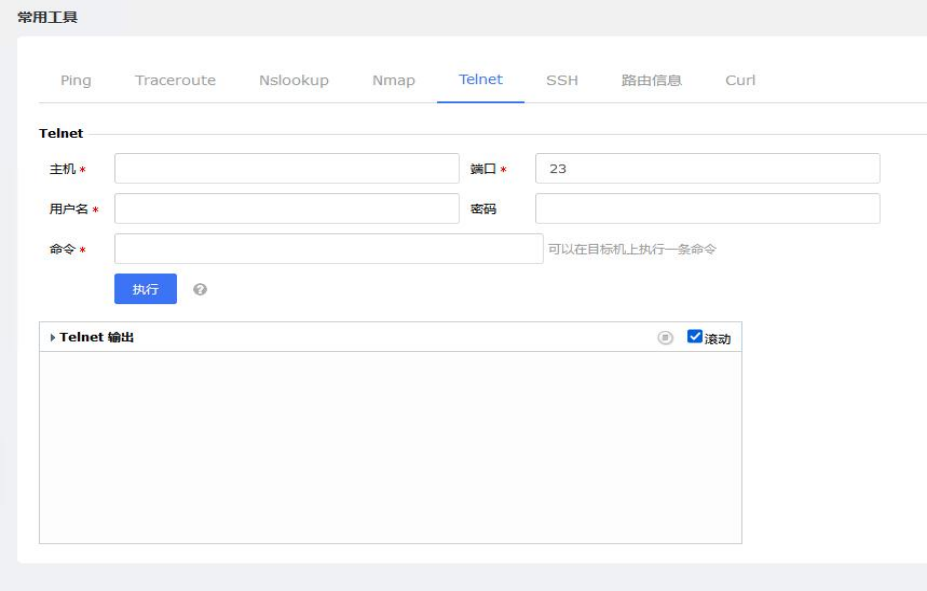
9.5.5 Telnet

Telnet 是 Internet 远程登录服务的标准协议和主要方式，主要用于远程管理漏洞扫描。

如图 9-37 所示，配置主机、端口（Telnet 默认使用 23 端口）、用户名、密码和命令后单击【执行】按钮，若用户名及密码正确，则输出命令执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出命令的执行结果。

图 9-36 Telnet



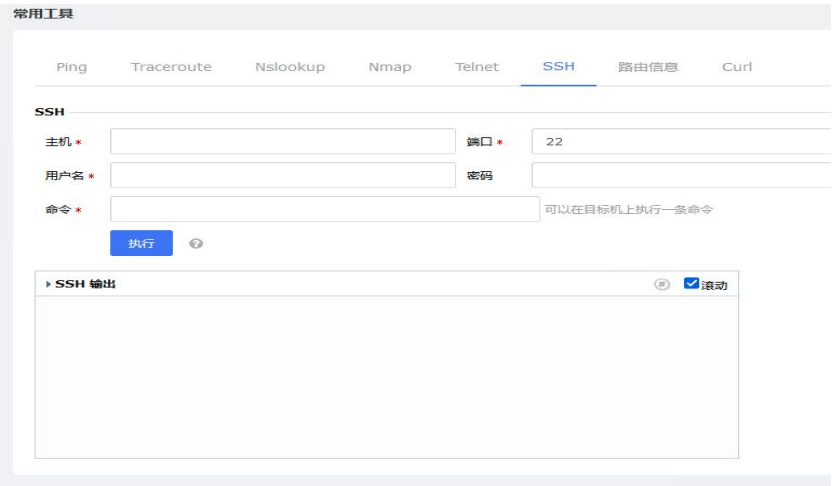
9.5.6 SSH

SSH 工具是一种基于 SSH 协议对漏洞扫描进行远程管理的工具。

如图 9-38 所示，配置主机、端口（SSH 默认使用 22 端口）、用户名、密码和命令后单击【执行】按钮，若用户名及密码正确，则输出命令执行结果。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出命令的执行结果。

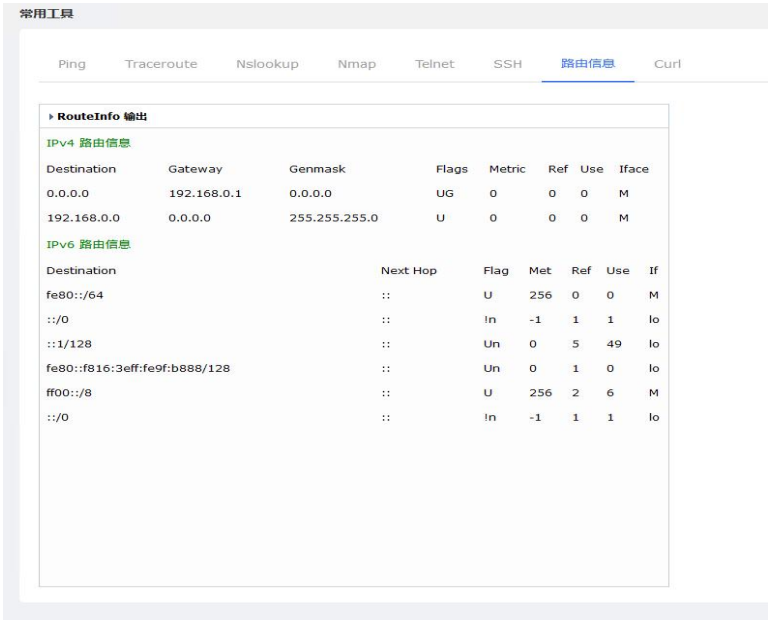
图 9-37 SSH



9.5.7 路由信息

路由信息是漏洞扫描中的实时路由信息，如图 9-39 所示。

图 9-38 路由信息



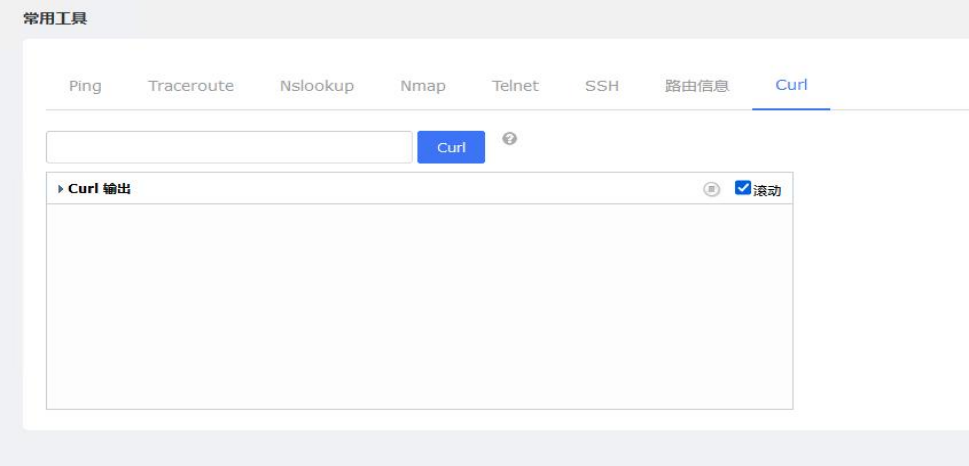
9.5.8 Curl

Curl 是利用 URL 语法在命令行方式下工作的文件和数据传输工具，支持很多协议，如 FTP、FTPS、HTTP、HTTPS 等。目前漏洞扫描只支持用户通过使用 Curl 7.15.1 来获取站点信息。

如图 9-40 所示，在文本框中输入目标站点的 URL（支持的格式请参见界面说明），单击【Curl】按钮，获取站点信息。

单击图标可停止执行当前命令，勾选/反选“滚动”可选择是否滚动输出命令的执行结果。

图 9-39 Curl


常用工具
Ping
Traceroute
Nslookup
Nmap
Telnet
SSH
路由信息
Curl
Curl
Curl 输出
滚动

10 日志管理

只有审计管理员 auditor 拥有日志管理的权限。

auditor 需要使用单点登录账号或 admin 账号激活，在**系统管理 > 用户 > 管理员列表 > 解禁账号**页面激活。

漏洞扫描对管理员登录及在设备上的所有操作进行严格审计，并以日志形式输出审计记录。漏洞扫描输出的日志类型主要包括四类：登录日志、操作日志、异常日志和升级日志。

本章主要内容包括：

功能	描述
日志审计	介绍审计员 auditor 查询、备份以及清空日志的具体方法。
日志配置	介绍审计员 auditor 配置日志阈值、日志备份方式的具体方法。

10.1 日志审计

10.1.1 查询日志

进入 **日志管理 > 日志审计 > 日志列表** 页面，设定查询条件，查看符合查询条件的日志即可，如图 10-1 所示。通过查看各类日志信息，可以帮助审计员获取以下漏洞扫描相关信息：

- 登录日志

  了解漏洞扫描设备的登录情况（包括登录成功、登录失败以及退出登录），及时发现未授权用户的尝试登录。

- 操作日志

  审查所有管理员的操作行为，包括证书管理、网络配置、用户管理等等。

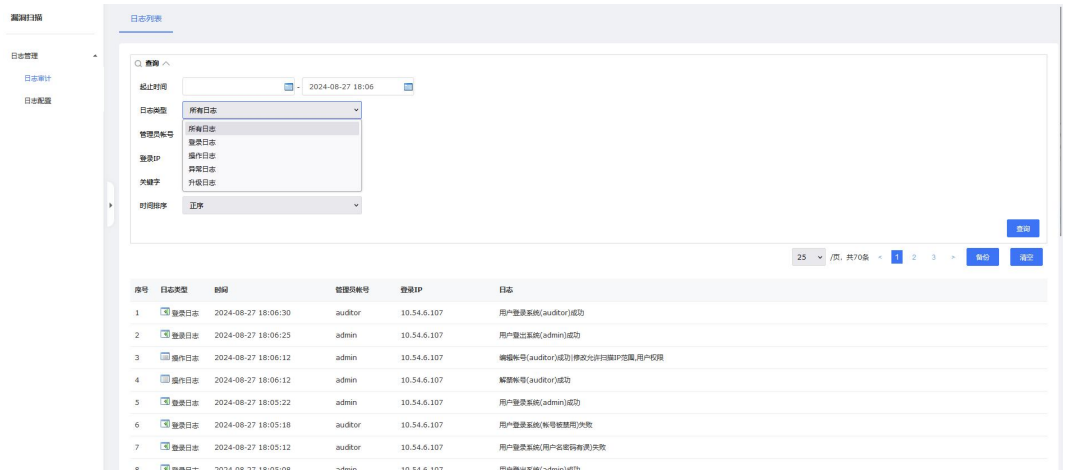
- 异常日志

  系统日志记录了解系统异常情况（包括网络不通、引擎异常、系统异常重启以及导致系统无法正常工作的各种异常日志），有助于解决系统错误。

- 升级日志

漏洞扫描的系统版本及版本升级情况。

图 10-1 日志列表



10.1.2 备份日志

漏洞扫描支持审计员手动备份日志，审计员可以按照设定的日志备份方式将系统所有类型的日志以.txt 格式备份到设备、FTP 服务器中，以便导出、查看日志，分析系统运行状况。

进入 **日志管理 > 日志审计 > 日志列表** 页面，单击【备份】按钮，配置备份选项即可，如图 10-2 所示。参数说明如表 10-1 所示。

图 10-2 日志备份

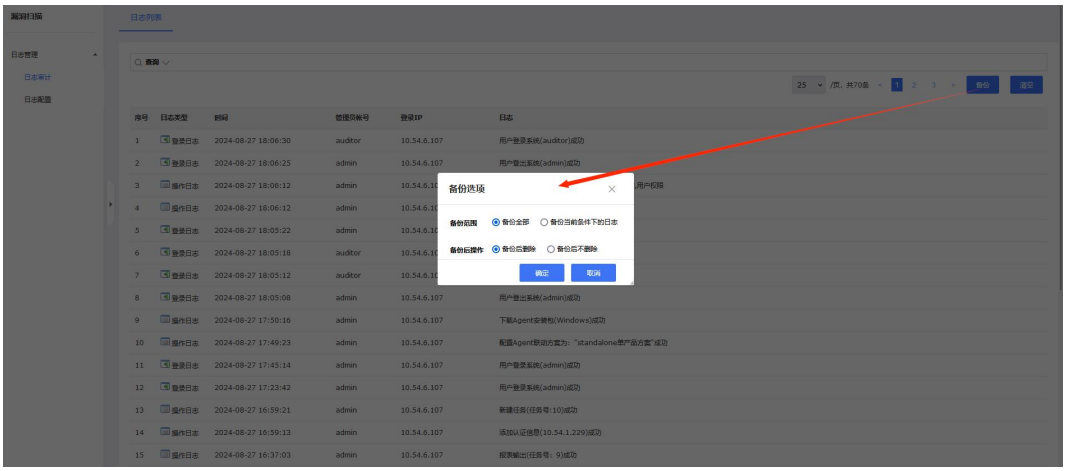


表 10-1 备份参数

配置项	描述
备份范围	备份日志的范围。

配置项	描述
	• 备份全部：备份当前系统内的所有日志记录。 • 备份当前条件下的日志：备份满足查询条件的日志记录。
备份后操作	日志备份后的操作。 • 备份后删除：日志备份后删除已备份的日志记录。 • 备份后不删除：日志备份后保留已备份的日志记录。

10.1.3 清空日志

进入 **日志管理 > 日志审计 > 日志列表** 页面，单击【清空】按钮，即可直接清空所有的日志。

说明	执行清空日志操作将会产生一条最新的操作日志。

10.2 日志配置

审计员 auditor 可以对漏洞扫描设备的日志管理方式进行配置，包括设置日志备份方式、日志备份阈值等。

10.2.1 日志阈值

日志备份阈值用于判定漏洞扫描设备是否需要进行日志备份，当备份周期达到时或者设备中的日志条数达到设定数目时，系统将按照设定的备份方式自动进行备份或通知管理员进行手动备份。备份方式的配置请参见 备份方式，本节主要介绍如何进行日志阈值配置。

进入 **日志管理 > 日志配置 > 日志配置** 页面，配置日志阈值即可，如图 10-3 所示。日志阈值参数如表 10-2 所示。

图 10-3 日志阈值

表 10-2 日志阈值

配置项	描述
备份周期(天)	系统将按照设定周期进行自动备份并清空日志。范围为 1～365 天，系统默认 30 天。
日志数量(条)	设备记录的日记条数达到阈值后，将自动备份并清空日志。阈值范围为 5000～50000 条，系统默认 5000 条。

10.2.2 备份方式

漏洞扫描设备自身支持存储一定量的日志信息，但是为了避免日志文件占用磁盘空间过大的问题，审计员可以将其备份到本地或专用 FTP 备份服务器中。

进入 **日志管理 > 日志配置 > 日志配置** 页面，配置备份参数即可，如图 10-4 所示。备份参数如表 10-3 所示。

图 10-4 备份方式

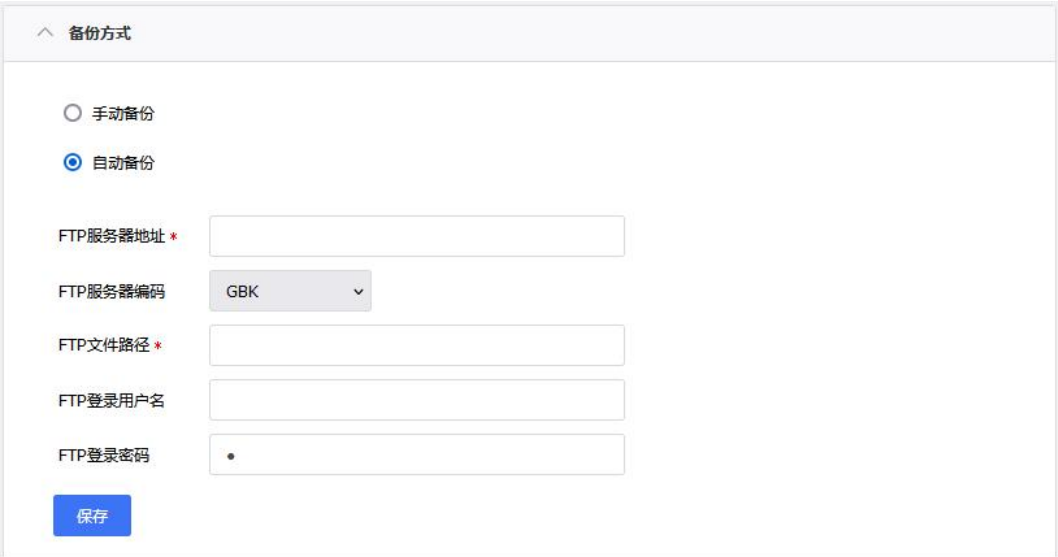


表 10-3 备份参数

备份方式	配置项	描述
手动备份	手动备份	审计员 auditor 手动备份日志信息时，只能将日志备份到访问漏洞扫描设备使用的用户本地电脑上。当漏洞扫描设备中存储的日志达到或将要达到设定阈值后，审计员登录 Web 管理界面系统将提示进行日志手动备份。
自动备份	自动备份	自动备份方式下，当备份条件满足时，系统自动将所有日志信息备份到设定的 FTP 服务器地址，同时清空“日志审计”中的相关日志，无需人工干预。 当系统进行自动备份日志后，会产生两条新的审计日志，一条是自动备份日志，另一条是清空日志。
	FTP 服务器地址	用于备份日志的 FTP 服务器的 IPv4 地址或 IPv6 地址。
	FTP 服务器编码	FTP 服务器采用的编码格式。
	FTP 文件路径	日志文件在 FTP 服务器上存储的具体目录。 根目录使用“/”表示。
	FTP 登录用户名	登录 FTP 服务器的用户名。该帐号必须具有读写权限。
	FTP 登录密码	登录 FTP 服务器的用户密码。