权限：保密

默安科技
企业信赖的安全伙伴

【默安】巡哨超级管理员使用手册 V3.2.1

产品技术部

2022 年 03 月

领先的第三方云计算安全服务商
AI驱动的下一代企业安全体系

文档说明

文档负责人	冯河清	文档版本编号	V3.2.0
起草人	嵇传悦	文档起草日期	2021 年 1 月
复审人		复审日期	

版本控制

版本号	版本日期	创建/修订人	说明
V2.12.0	2021 年 1 月	冯河清	创建
V3.0.0	2021 年 6 月	冯河清	修订
V3.0.2	2021 年 8 月	冯河清	修订
V3.1.0	2021 年 11 月	冯河清	修订
V3.2.0	2022 年 1 月	白解	修订
V3.2.1	2022 年 3 月	张莹	修订

版权声明

目　录

1 产品概述

1.1 产品概述

本产品作为一款云计算时代的智能安全产品，面向企业提供优质的 IT 资产安全管理服务，帮助企业自动化运维 IT 资产，全面分析监控企业当前面向互联网所公开的业务、服务、应用、数据等情况，且实时监控企业暴露在外的服务和资产的变化。从漏洞风险，合规检测以及外部威胁情报分析等多个维度持续监控企业安全；并通过短信，邮件，微信等多种渠道第一时间同步安全状况。

2 客户端概述

2.1 登录

Web 管理界面的登录方法：

1）打开浏览器 Google Chrome（目前支持以下浏览器：Google Chrome、IE11）

2) 用 HTTP 方式连接 WEB 管理的地址，如：https://192.168.120.140/login

3) 回车进入登录页面，输入正确的超级管理员用户名、密码和验证码（初始账号及密码为：admin / ms123456），并单击登录。

4) 登录时连续输入密码错误 5 次后，锁定 15 分钟，支持超管后台密码重置。

5) 密码设置 90 天后失效，登录时显示修改密码弹框，需修改为与前两次不同的新密码方可登录。

图表 1 登录

2.2 资产

资产分为网站资产、主机资产、域名资产、云资产四种；

2.2.1 网站资产

用于展示网站资产列表，IPv6 资产的资产地址后显示标识。

1）网站资产列表的风险等级、指纹、网站状态、资产分组、负责人、标签、资产变动、WAF 识别、网站类型、资产来源进行条件筛选，可根据导入时间进行检索，也支持关键字搜索；

网站状态：状态有 200、201、403、404、500、502、504 等；

网站类型：分为 IP 类、域名类；

资产变动：分为新上线（新发现的资产）、有更新（资产有变动，点击查看）、无更新（无任何变动的资产）、已下线（已下线的资产）；

WAF 识别：可筛选出有 WAF 防护规则的网站；

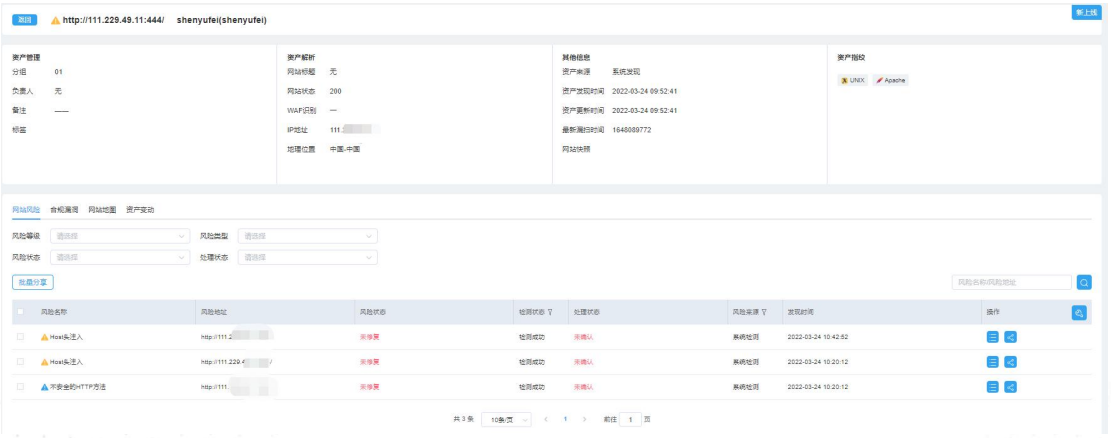
其中，网站列表中展示网站概要、网站信息、网站状态、指纹；

- 网站信息：展示资产分组、资产负责人、资产最新更新时间、标签；
- 网站状态：展示网站状态、资产状态、风险状态；
- 指纹：展示网站资产的服务类型等指纹信息，如 Nginx；

图表 2 网站资产

2）网站资产详情

网站详情展示资产概要、解析信息、其他信息及指纹信息；

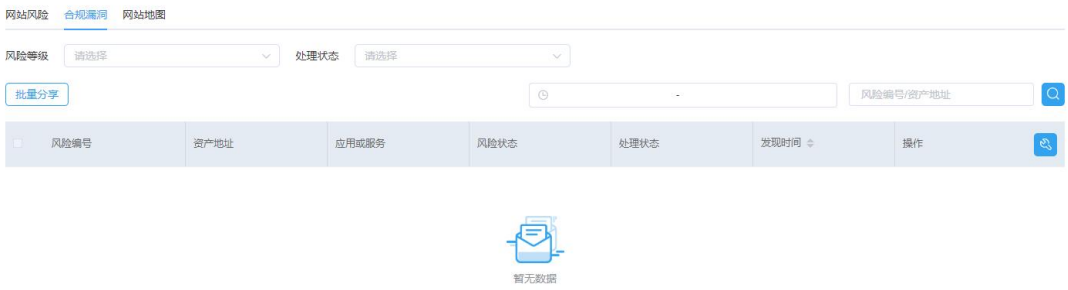


图表 3 网站详情

网站风险展示该网站下的风险项，支持风险等级、风险类型、风险状态、处理状态条件的筛选、查看详情及分享操作；

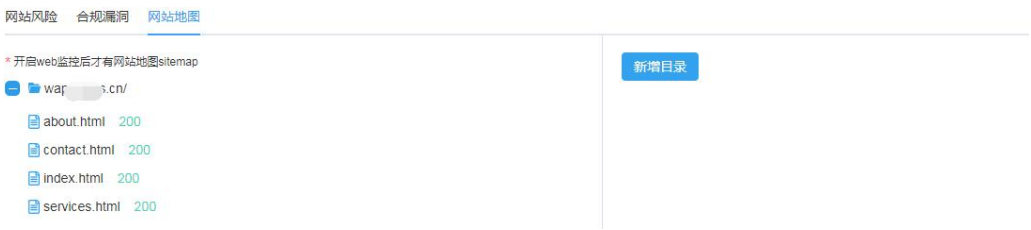
图表 4 网站风险

- 合规漏洞展示该网站的合规风险；



图表 5 网站合规漏洞

- 网站地图展示该网站的网站结构，即 sitemap，点击可跳转打开链接；



图表 6 网站地图

2.2.2 主机资产

用于展示主机资产列表，IPv6 资产的资产地址后显示标识。

1）主机资产列表包括设备类型、资产来源、资产分组、负责人、存活状态、资产变动、地理位置、端口、CDN 识别、风险等级、指纹、标签进行条件筛选，支持 Excel 导出、按导入时间和关键字进行资产搜索；

存活状态：分为存活、关闭；

资产变动：分为新上线（新发现的资产）、有更新（资产有变动，点击查看）、无更新（无任何变动的资产）、已下线（已下线的资产），支持多选；

CDN 识别：支持筛选，可筛选出有 CDN 标识的主机资产；

其中，主机列表中展示主机详情、主机信息、主机状态、指纹；

- 主机详情：展示主机地址、地理位置、主机系统、关联域名、特征；
- 主机信息：展示资产分组、资产负责人、资产发现时间、资产更新时间、标签；
- 主机状态：展示主机状态、资产变动、风险状态；
- 指纹：展示图标、指纹、版本；

图表 7 主机资产列表

1）资产导出

点击导出 Excel，即可将资产列表以 EXCEL 形式生成，可前往报告管理中查看下载；

图表 8 资产列表 Excel 导出

2）主机资产详情

可展示主机资产的相关内容，包括资产管理信息、解析信息、其他信息及指纹信息，也包括该主机对应主机漏洞、合规漏洞、主机服务、主机拓扑信息。

- 主机详情展示主机概要、主机漏洞、主机状态、主机服务；

图表 9 主机详情

- 主机漏洞展示该主机下的基础漏洞，支持各类筛选及批量分享操作

图表 10 主机漏洞

- 主机合规即 CVE 漏洞风险，展示该主机下的 CVE 漏洞，支持各类筛选及批量分享操作；

图表 11 主机合规

- 主机服务，展示该主机下识别到的端口及服务情况；

端口	端口状态	服务名称	版本	备注	来源	更新时间
9000	开启	http	Gunicorn 19.7.1	暂无	系统发现	2020-02-13 17:03:55
6379	开启	redis	Redis key-value store 3.2.3	暂无	系统发现	2020-02-13 17:03:57
4006	开启	http	Mongoose httpd	暂无	系统发现	2020-02-13 17:03:58
9001	开启	http	nginx 1.10.2	暂无	系统发现	2020-02-13 17:04:01
22	开启	ssh		暂无	系统发现	2020-02-13 17:06:26

图表 12 主机服务

- 主机拓扑，展示该主机的风险等级、地理位置，及对应端口服务的链路图；

图表 13 主机拓扑

2.2.3 域名资产

用于展示域名资产列表。

1）域名资产列表包括资产来源、资产分组、解析状态、负责人、资产变动、CDN 识别、泛解析、标签。

支持 Excel 导出，支持关键字搜索；

CDN 识别：支持筛选，可筛选出有 CDN 标识的域名资产；

泛解析：支持筛选，可筛选出泛解析/非泛解析的域名资产；

其中，域名资产列表中展示域名详情、域名信息、域名状态、解析记录；

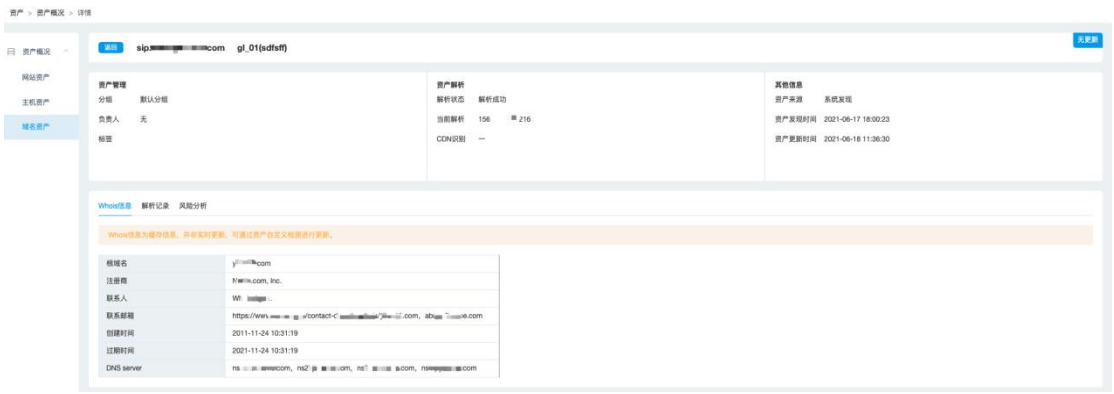
- 域名详情：展示域名地址、资产来源；
- 域名信息：展示资产分组、资产负责人、首次发现时间、最新扫描时间、标签；
- 域名状态：展示解析状态、资产变动；
- 解析记录：展示解析地址、解析时间，默认展示前 10 条；

图表 14 域名资产

2）域名资产详情

可展示域名资产的相关内容，包括资产管理信息、解析信息、其他信息，也包括该域名资产的 Whois 信息、解析记录，泛解析的域名资产会在域名后显示泛解析标识。

- 域名资产详情展示域名资产概要、Whois 信息、解析记录、风险分析；



图表 15 域名详情

- Whois 信息展示该域名资产的根域名、注册商、联系人、联系邮箱、创建时间、过期时间及 DNS server；

图表 16Whois 信息

- 解析记录展示该域名资产的解析地址、解析时间；

图表 17 解析记录

- 风险分析展示该域名资产的子域名接管风险；

图表 18 风险分析

2.2.4 云资产

该模块用于展示用户各云平台资产，本版本支持阿里云、腾讯云、华为云、亚马逊云四大云服务商资产监测。支持监测的各服务商产品类目如下：

阿里云：云服务器 ECS

对象存储 OSS

访问控制 RAM

腾讯云：云服务器 CVM

对象存储 COS

云硬盘 CBS

访问管理 CAM

华为云：弹性云服务器 ECS

对象存储 OBS

云硬盘 EVS

统一身份认证 IAM

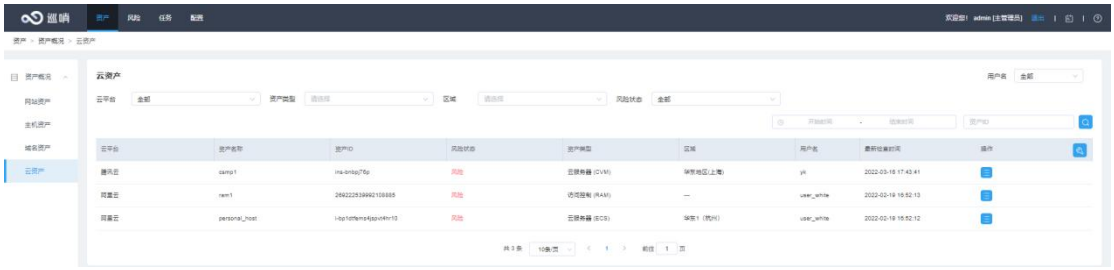
亚马逊云（AWS）：

弹性云服务器 EC2

对象存储 S3

身份和访问管理 IAM

1）当普通用户/普通管理员创建了云资产的检测任务，探测到云上资产后，超管将在此可见。超管可见所有用户的云资产信息，云资产列表展示云上资源所属的云平台、资产名称、资产 ID、风险状态、所属区域、最新检查时间等信息。在此页面可根据云平台、资产类型，所属区域，风险状态，检查时间对特定资产进行检索。点击详情可以查看相应的资产详情。

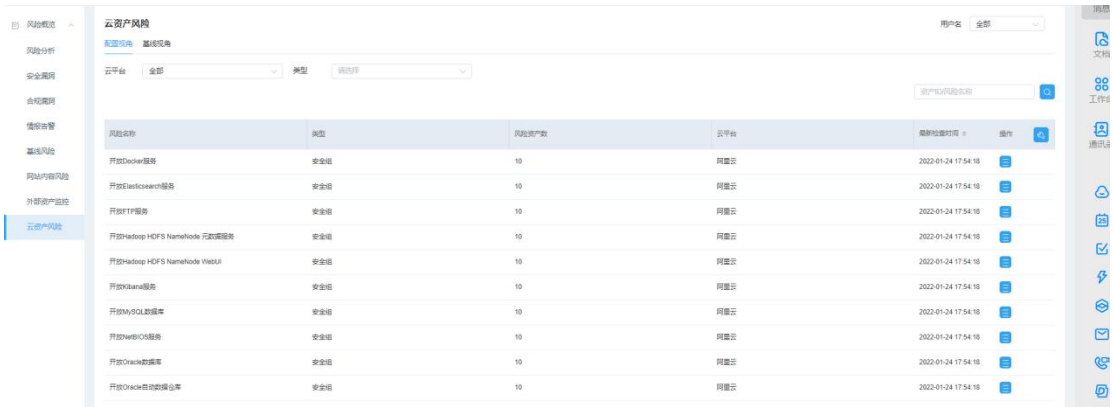


图表 19 云资产列表

2）点击详情可查看该资产的配置检测情况。可以在此查看相应的资产详细信息，包括云主机的安全组规则、vpc 网络；Bucket 的访问控制，加密情况；子账户的密码策略等。以及各个资产配置项的检测通过情况。

图表 20 云资产详情

2.3 风险



2.3.1 安全漏洞

2.3.1.1 安全漏洞列表

点击“安全漏洞”后，可看到已修复、未修复两种漏洞列表。

其中可看到资产风险统计项、未确认风险项、已确认风险项、已忽略风险项四种，四种统计可依次点击。

其中列表内容可根据风险等级、风险类型、处理状态、资产分组、负责人、标签、地理位置进行条件筛选，还可以根据发现时间、最后更新时间、关键词进行搜索，并支持一键导出。

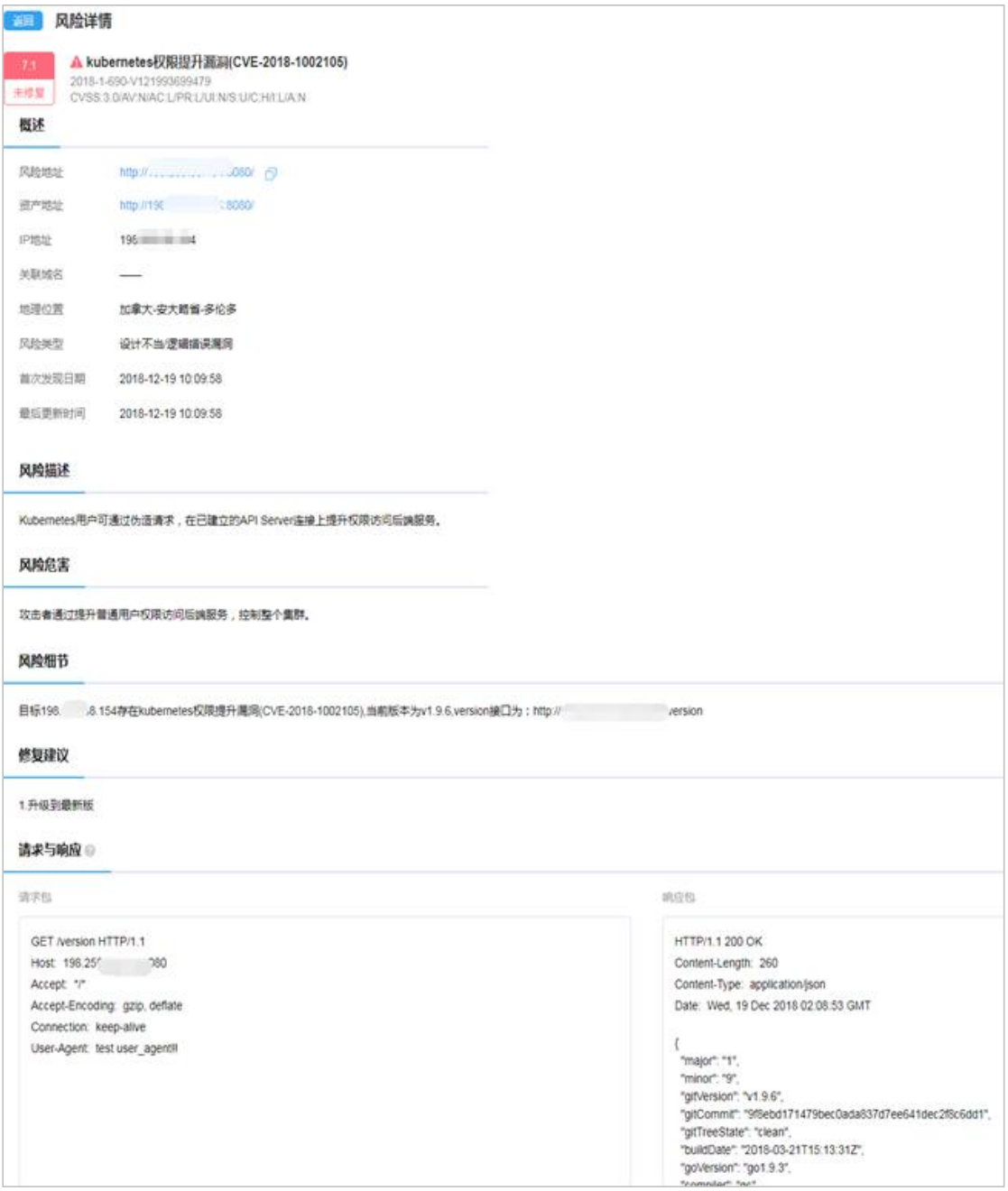
图表 21 安全漏洞

2.3.1.2 安全漏洞详情

列表中点击“查看”后进入风险详情页，可查看到该资产下该漏洞的 cvss 评分、威胁程度、风险概要、风险描述、风险详情、风险危害、修复建议、请求与响应的信息。

其中风险概要介绍该风险的地址、及对应资产地址、风险类型、首次发现时间、最后更新时间；若为用户自定义规则检测出的漏洞，相比于默认规则检测出的漏洞详情中多规则名称字段，如果该规则被删除，规则名称显示为“——”。

请求与响应内容中若响应包过大时将会被截断。



图表 22 安全漏洞详情

2.3.1.3 安全漏洞分享

支持安全漏洞分享给相关修复人员（支持批量分享），点击漏洞分享按钮，设置该漏洞链接的有效时间（1 天/3 天/7 天）后，再点击复制链接后可认为简单的漏洞工单下发。

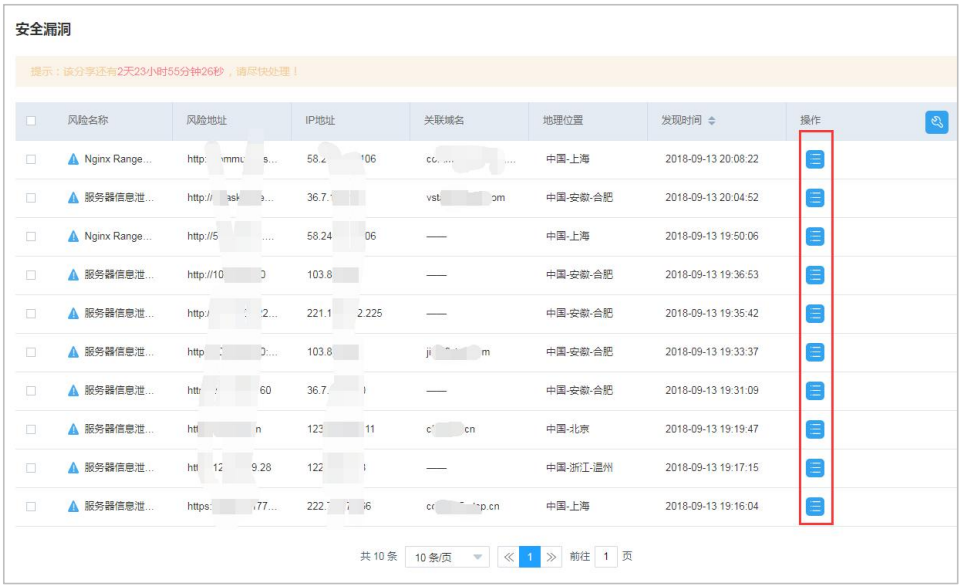
提示：主机合规、外部风险均支持漏洞分享功能。

图表 23 安全漏洞分享

相关修复人员进入该链接地址页，后需要输入正确的分享密码才可看到漏洞列表。

图表 24 安全漏洞分享登录页

输入正确的密码后，在有效日期内可看到本次所需修复漏洞，点击操作-详情按钮可查看安全漏洞详情。



图表 25 安全漏洞分享列表

2.3.2 合规漏洞

对资产进行主机/网站合规 CVE 漏洞监测（可在配置-全局监控配置中设置开关），CVE 风险漏洞列表分为已修复、未修复两种，可进行风险等级、处理状态、资产分组、地理位置、端口、负责人、标签条件筛选，列表中显示合规漏洞的 CVE、CNVD、CNNVD 编号，支持合规漏洞分享、查看该风险详情。

图表 26 合规漏洞列表

其中合规漏洞详情包括风险描述、修复建议、参考链接三部分组成。

图表 27 合规风险详情

2.3.3 情报告警

在 8000 页面开启情报告警功能即可查看此页面，在 8000 页面开启了情报自动获取或在系统配置点击情报获取按钮，获取最新情报时，会对下属用户的主机/网站资产进行一次性的情报风险检测，列表中显示可能存在的情报风险的名称、CVE、CNVD、CNNVD 编号，并支持情报风险分享，可查看该风险详情；

图表 28 情报告警

2.3.4 基线风险

基线风险展示资产违规开放 XX 端口 XX 服务等，列表中可看到已修复、未修复两种状态。其中列表内容可根据资产分组、负责人、标签、处理状态、地理位

置进行条件筛选，支持一键导出。

批量操作仅支持批量分享。

图表 29 基线风险

2.3.5 网站内容风险

对网站进行内容合规风险监控，支持违规内容和篡改内容检测。

列表内容可根据资产分组、风险类型、负责人、处理状态、地理位置及标签进行条件筛选，支持一键导出。

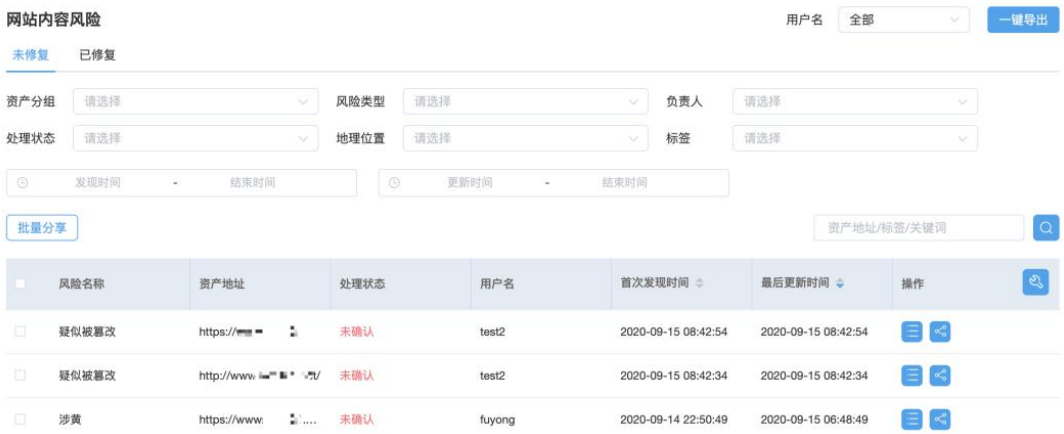
批量操作仅支持批量分享。

涉黄监控：可识别网页中描述或传授性技巧及性行为等淫亵性内容，并建议用户排查；

涉赌监控：网页中包含赌博类内容；

虚假证件：网页中包含违规证件类信息，如虚假身份证等；

防篡改监控：与之前的网页比对，对新加入的内容作分析，若存在恶意关键词、恶意标签便可能被篡改，建议用户排查。

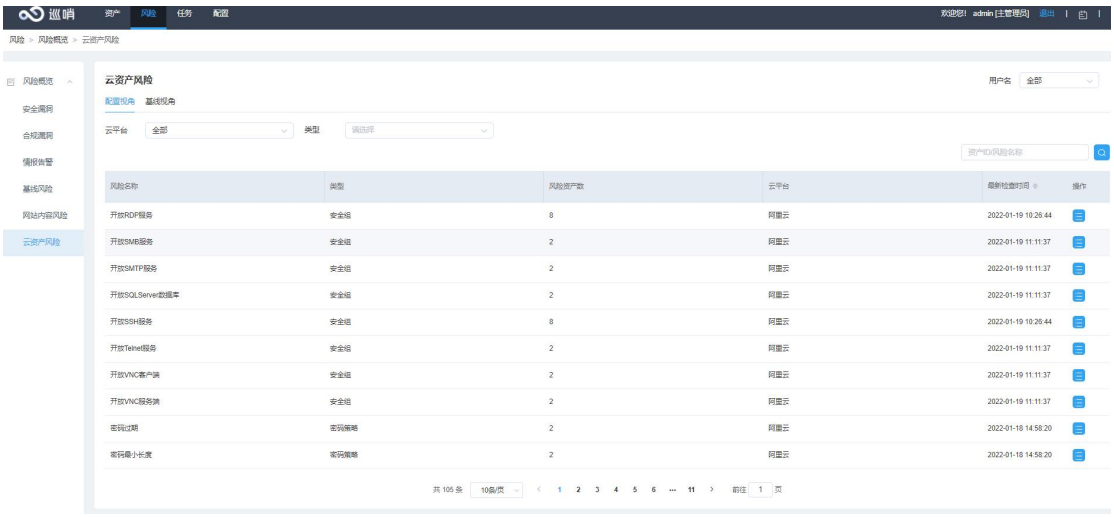


图表 30 网站内容风险

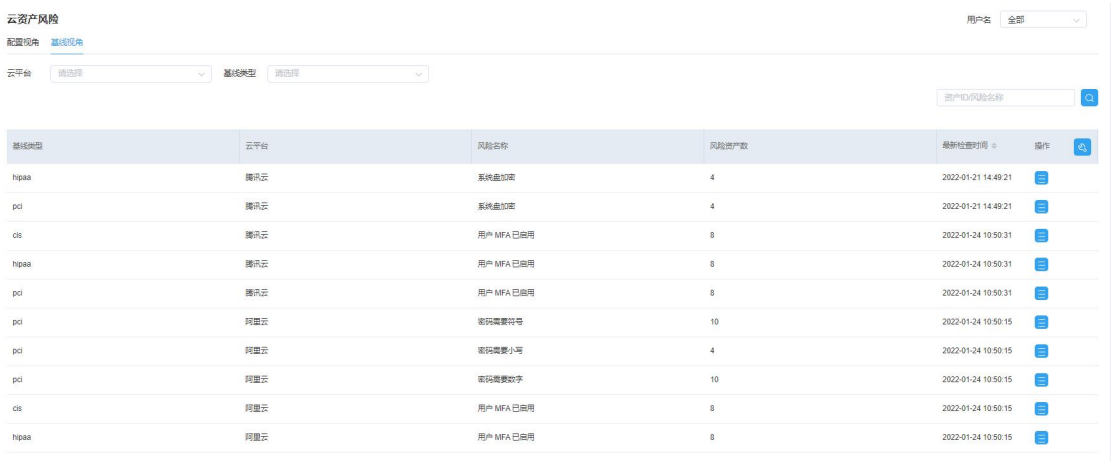
2.3.6 云资产风险

在此模块可以查看各用户扫描出的云资产风险，分为配置视角与基线视角两大模块，其中配置视角按照各配置项展示云资产未通过的各个配置项，基线视角展示触发基线的相关风险。可以根据云平台，风险类型，风险名称等筛选风险项。

点击详情可查看具体风险的详情，包括风险描述，详情，修复建议，参考链接等，在详情页点击资产 ID 可跳转至相应的资产详情页面。



图表 31 云资产风险配置视角



图表 32 云资产风险基线视角

图表 33 配置视角风险详情

图表 34 基线视角风险详情

2.4 任务

2.4.1 风险评估报告

可根据实际需求，用户范围进行相关报告生成。

输入报表名称、选择用户名称（支持选择多个用户）、时间范围（发现时间/更新时间）、风险发现日期、风险范围（已修复/未修复）、风险类型（安全漏洞/合规漏洞）后进行“报表生成”。

图表 35 添加报表

1）报告支持下载、在线查看和删除操作；

图表 36 风险评估报告列表

2）报表详情

风险评估报告：由 4 部分组成：综述、安全漏洞信息、合规风险信息、参考标准。

1）综述：包括报表信息、风险综述、资产综述；

2）安全漏洞信息：包括安全漏洞分布、安全漏洞详情；

3）合规风险信息：包括合规风险分布、合规风险详情；

4）参考标准：包括风险等级、资产评分。


资产风险评估报告-daijandja-20230113
1 综述
1.1 报表信息
1.2 风险综述
1.2.1 概述
1.2.2 风险状态分布
1.3 资产综述
1.3.1 风险网络分布
1.3.2 风险资产TOP10
2 安全漏洞信息
2.1 安全漏洞分布
2.2 安全漏洞详情
3 合规风险信息
2.1 合规风险分布
2.2 合规风险详情
4 参考标准
4.1 风险等级
4.2 资产评分

图表 37 报表详情

2.4.2 报告导出

用户可以根据报表类型，根据用户范围（支持多个用户）生成报告。输入报表名称、选择报表类型（主机资产报表、网站资产报表、域名资产报表、安全漏洞报表、合规漏洞报表、基线风险报表、情报告警报表）、选择用户范围、选择时间范围（发现世界/更新时间），生成。

图表 38 添加报表

报告导出列表：报告支持下载和删除操作。

图表 39 报告导出列表

2.5 配置

2.5.1 监控配置

2.5.1.1 安全漏洞配置

页面显示最新检测结果的监控详情，列表包括监控项（支持对 CMS 应用漏洞、运维安全漏洞、弱口令漏洞进行监控）、并展示对应巡检结果。

1）CMS 应用漏洞可进行监控单项开启/关闭，也支持在全局巡检配置-风险扫描

巡检中进行全局开启/关闭。

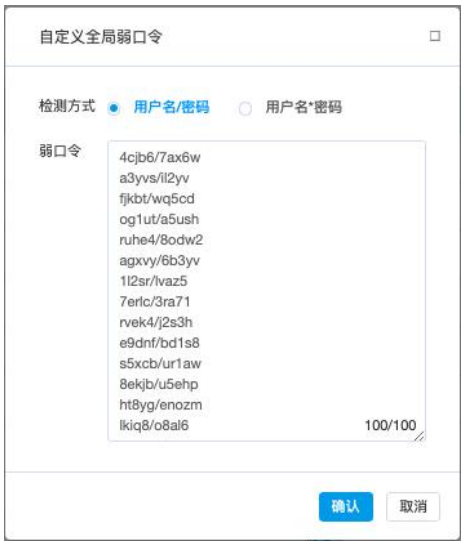
图表 40 安全漏洞配置-CMS 应用漏洞

2）运维安全漏洞可进行监控单项开启/关闭，也支持在全局巡检配置-风险扫描巡检中进行全局开启/关闭。

图表 41 安全漏洞配置-运维安全漏洞

3） 弱口令可进行主机、网站默认弱口令开启关闭，进行自定义弱口令编辑，适用于主机弱口令、网站弱口令，其中自定义弱口令支持账号/密码一一对应输入，也支持账号*密码组合输入。

图表 42 弱口令监控

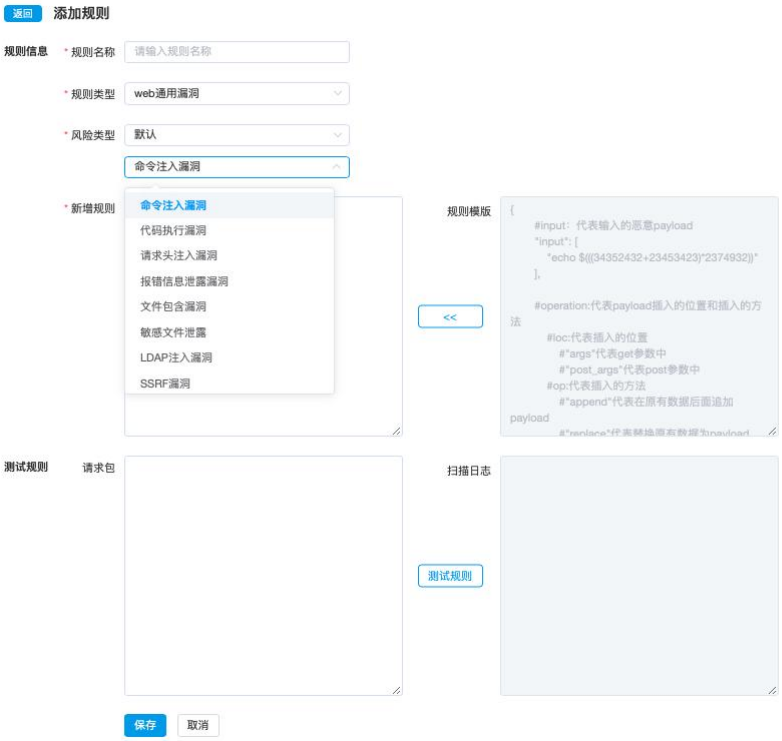


图表 43 弱口令-账号/密码一一对应

图表 44 弱口令-账号*密码组合输入

4）超管可以自定义漏洞检测规则(规则名称不可重复)，添加规则时可选择规则类型(当前仅支持 web 通用漏洞类型)、选择默认/自定义风险类型，如选择默认风险类型，可在下拉框中选择已有默认类型；选择自定义风险类型，需输入风险类型名称、选择风险等级、选填风险描述等信息，根据内置规则模版填写规则信息，可输入请求包进行规则测试，点击保存按钮，完成规则创建；可进行编辑/删除操作(不会删除已检测出的漏洞，删除后对应漏洞的详情将不会展示规则名称)，可通过开关控制规则上线/离线。

图表 45 自定义规则



图表 46 添加默认规则

图表 47 添加自定义规则

2.5.1.2 合规漏洞配置

设置合规漏洞监控开关项、可输入 CVE/CNVD/CNNVD 编号进行是否支持某项合规漏洞检测查询（不支持模糊搜索）。

图表 48 合规漏洞配置

2.5.1.3 Agent 配置

1）DNS 配置

超管可对每个设备添加 15 个公网 nameserver，5 个内网 nameserver，进行域名解析时顺序：用户自定义公网 nameserver->用户自定义内网 nameserver->默

认内置的 20 个 nameserver。

图表 49DNS 配置

添加 nameserver：需选择环境（内网/公网，默认公网），输入 nameserver、测试域名、目标 IP

图表 50 添加 nameserver

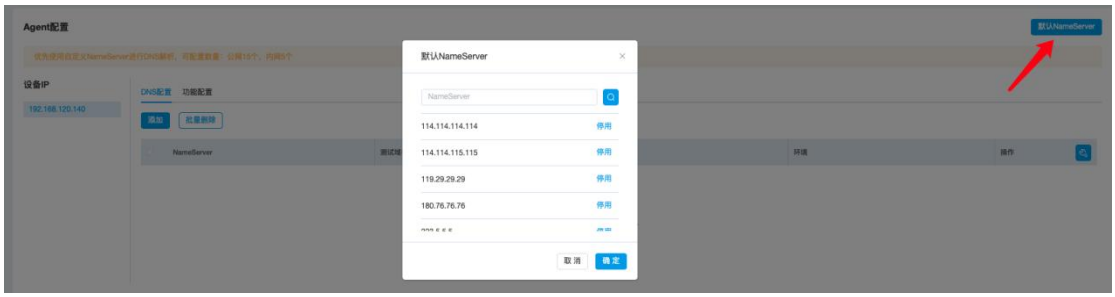
编辑 nameserver：只可编辑测试域名及目标 IP

图表 51 编辑 namesercer

删除 nameserver：弹出确认弹框

图表 52 删除 nameserver

启用/停用默认 nameserver：弹出弹框，选择启用/停用



图表 53 默认 nameserver

2）功能配置

可选择是否开启信息查询接口配置、增强检测能力配置。

信息查询接口配置：此配置为 IP 反查域名、子域名查询功能的服务化接口开关， 如需相关服务，请将“api-sentry.moresec.cn”加入互联网访问名单；

增强检测能力配置：此配置为公网 dnslog 启用开关，开启后会增强风险检测能力，如需相关服务，请将 o0w0o.cc 加入互联网访问名单；若对隐私合规有严格要求，请关闭此功能。

图表 54 功能配置

2.5.1.4 网页内容配置

页面可选是否开启模糊匹配的匹配模式（默认关闭），作用于复用超管配置的用户，开启后检测精度下降，不过模型、只做关键词匹配，可能出现较多误报（可通过批量忽略处理）。

图表 55 网页内容配置

超管可添加自定义风险类型，自定义风险类型无内置关键词字典，需添加待检测关键词至黑名单；自定义风险类型不经过机器模型匹配，仅支持关键词匹配。

图表 56 自定义风险类型

超管可添加关键词黑名单和关键词白名单，可进行删除操作，单个关键词字符上限 20 个（一个汉字占两个字符），单次添加关键词上限 50 个，单个列表关键词上限 500 个，同时添加到黑、白名单的关键词按白名单处理。

- 关键词黑名单-将对该关键词进行网页内容风险监控
- 关键词白名单-不再对该关键词进行网页内容风险监控

图表 57 添加关键词黑名单

图表 58 添加关键词白名单

2.5.2 系统配置

2.5.2.1 账号信息

账号信息页展示当前登录用户信息，可进行用户管理、组织管理、角色管理操作。

1）个人信息：展示当前登录的用户信息（包括用户角色、用户名、当前组织、注册邮箱、联系手机）。

图表 59 账号信息

2）用户管理：超管支持添加每个组织下的管理员、审计管理员以及普通用户，并对其进行管理，包括登录限制、密码重置、用户编辑及删除。支持一键导出、登录状态、过期状态操作，支持切换用户角色，切换用户所属组织。添加用户时，密码口令最小长度为 8 位，必须包含数字、大写字母、小写字母、特殊符号等，默认 90 天内有效期。

图表 60 用户管理

添加管理员：需填写基本信息包括用户名、用户别名、密码及二次密码确认、邮箱、手机号、备注；

用户授权包括风险扫描允许自由配置/复用超管配置、分配资产上限；

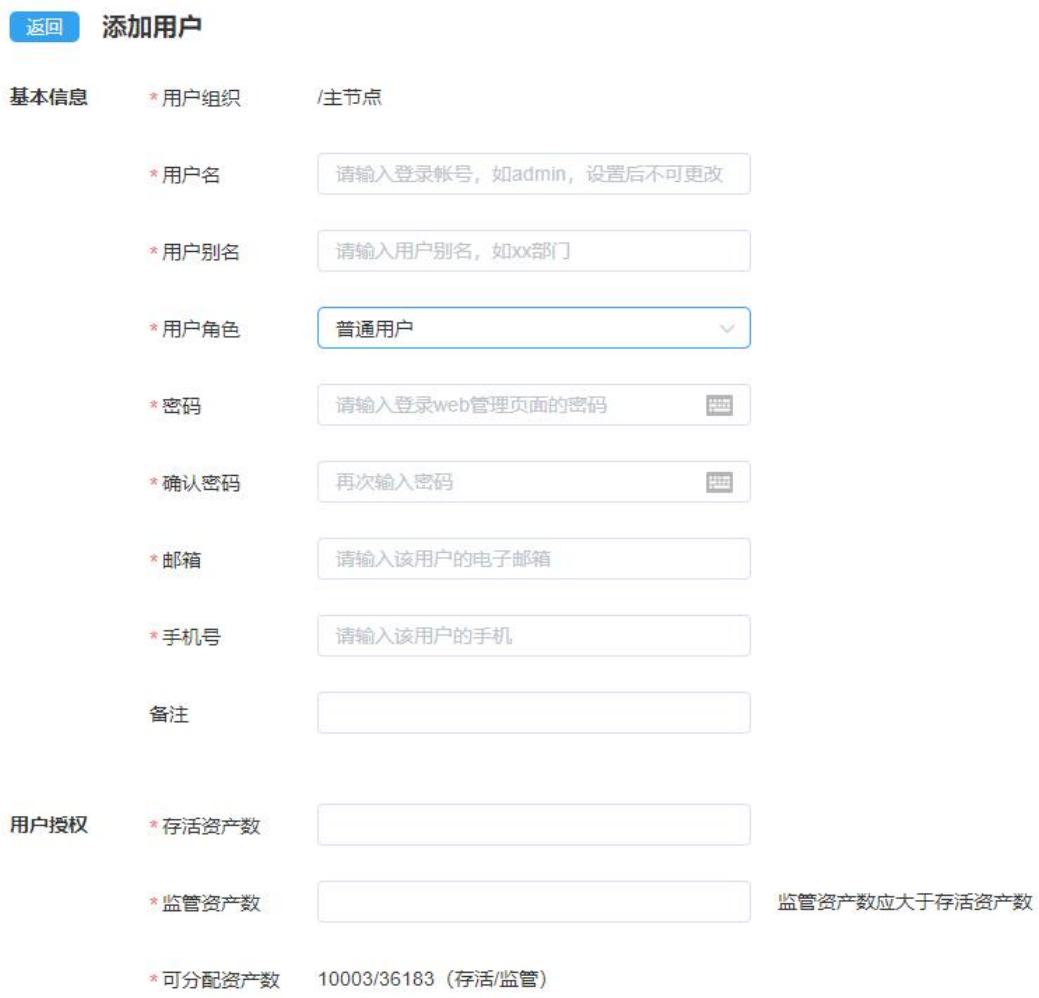
图表 61 添加管理员

添加审计管理员：需填写基本信息包括用户名、用户别名、密码及二次密码确认、邮箱、手机号、备注；

图表 62 添加审计管理员

添加普通用户：需填写基本信息包括用户名，密码及二次密码确认，用户别名，邮箱、手机号、备注；

配置设置包括该普通用户风险扫描规则是否可独立配置，或复用超管配置（详见本文 2.5.1 监控配置）。



图表 63 添加普通用户

切换用户角色：超级管理员在编辑用户信息时可以切换用户角色，只可以切换管理员与普通用户之间的角色。

图表 64 切换用户角色

切换用户所属组织：选中需要切换组织的用户，点击切换组织按钮，可以通过搜索或层级联动选择的方式进行组织筛选，点击确定即可切换用户组织。

图表 65 切换组织

3）组织管理：超管支持添加、编辑、删除组织，添加的组织在左侧以树状图形式展示，选中组织后，右侧显示该组织及以下的组织列表，按层级关系展示。

图表 66 组织管理

添加组织：添加一级组织，填写组织名称、到期日期；添加二级及以下组织，只需要填写组织名称；

图表 67 添加一级组织

图表 68 添加二级及以下组织

编辑组织：编辑一级组织，可以对组织名称、到期日期进行编辑；编辑二级及以下组织，可以对组织名称进行编辑；

图表 69 编辑一级组织

图表 70 编辑二级及以下组织

删除组织：①资产删除操作不可逆；②删除组织后，当前组织（包括下级组织）均消失；③删除组织同时会删除对应的全部用户及数据

图表 71 删除组织

4）角色管理：对主管理员、审计管理员、管理员以及普通用户四种角色的权限进行分配。本期 2.9.0 角色固定，角色对应权限固定，不可更改。

主管理员权限：基础权限-用户、组织全部权限；业务权限-系统全部权限、配置部分权限（安全漏洞配置、合规漏洞配置）；资源权限-全部；

图表 72 主管理员角色权限

管理员权限：基础权限-用户、组织全部权限；业务权限-系统、首页、资产、风险、报表、配置全部权限；资源权限-被分配；

图表 73 管理员角色权限

审计管理员权限：业务权限-系统部分权限（日志审计）；资源权限-被分配；

图表 74 审计管理员角色权限

普通用户权限：业务权限-首页、资产、风险、报表、配置全部权限；资源权限-仅看自己。

图表 75 普通用户角色权限

2.5.2.2 授权管理

授权管理页面包括产品型号、资产上限、机器指纹、维保到期时间、产品到期时间。

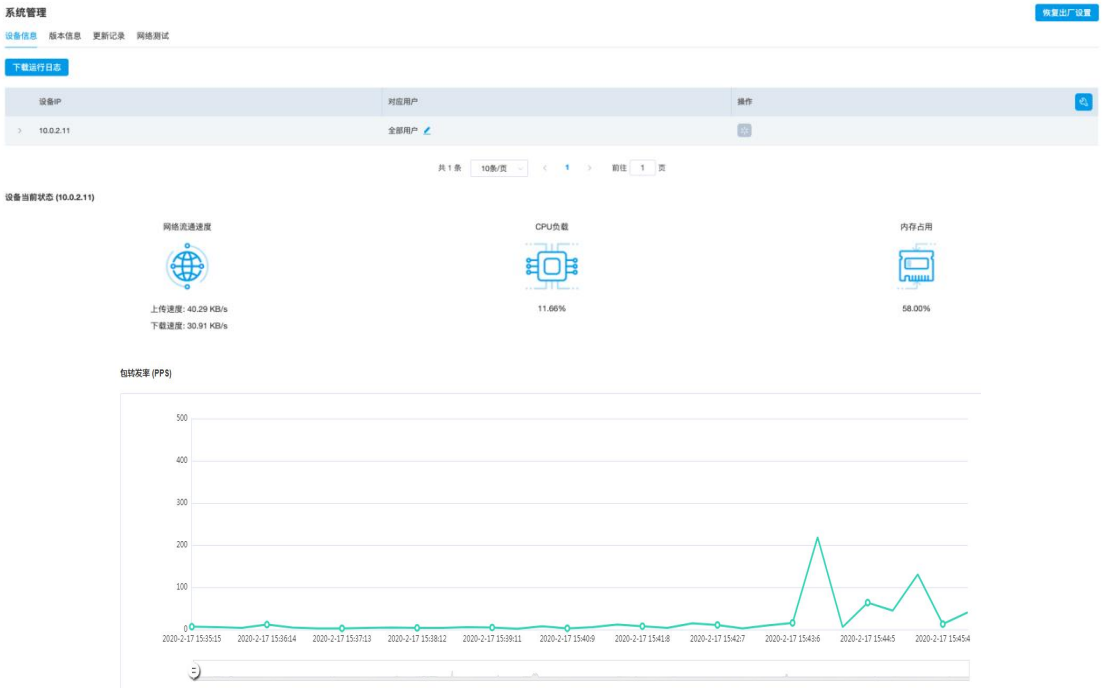
图表 76 授权管理

2.5.2.3 系统管理

系统管理页面中包括设备信息、版本信息、更新记录、系统参数、网络测试。

1）设备信息

展示平台内各个设备 IP、对当前设备进行引擎展示，并展示该设备此时的系统状态：包括网络流通速度（上传速度/下载速度）、CPU 负载率、内存占用率、包转发率 PPS。



图表 77 设备信息

可执行恢复出厂设置操作，将清除所有用户及任务数据，仅保留主管理员信息，慎重操作。

图表 78 恢复出厂设置

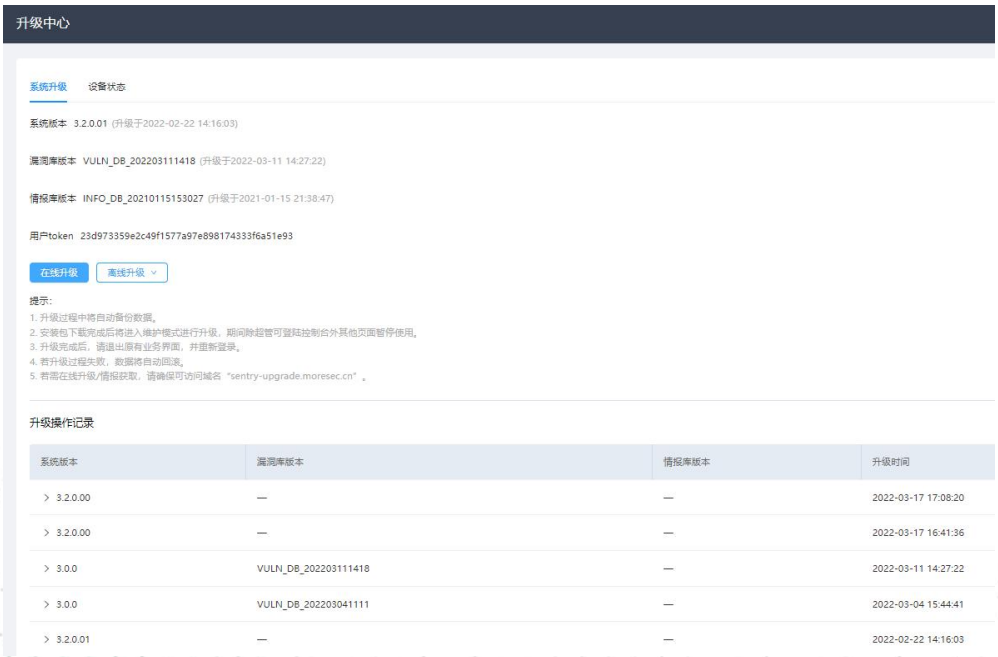
2）版本信息

该系统支持系统版本或漏洞库版本的在线升级和离线升级，其中产品升级可选择是否进行更新提醒通知，点击离线升级上传升级包，若升级过程失败，数据

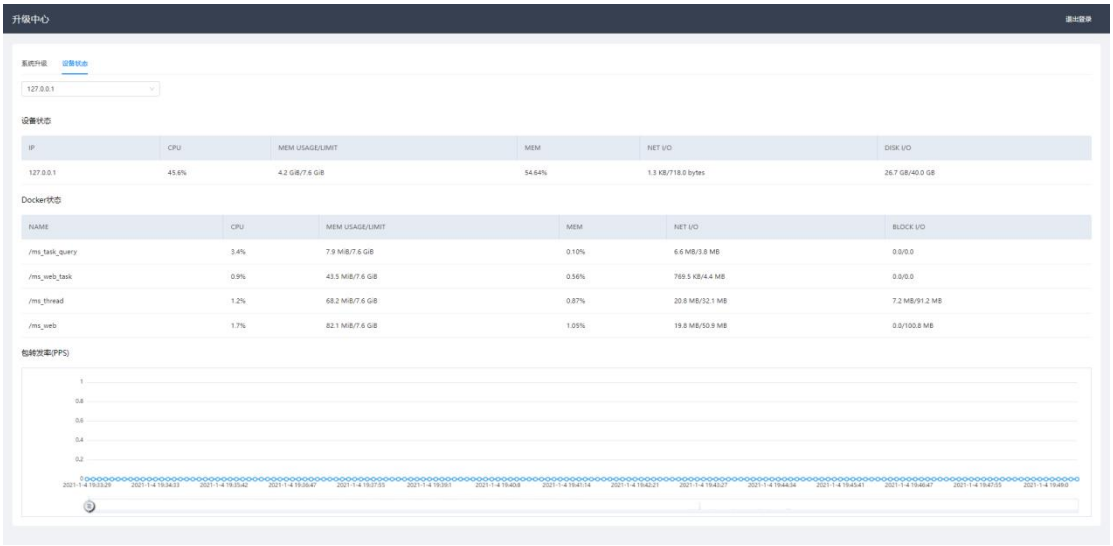
将自动回滚，不会对系统造成任何影响，并可将错误日志进行回传；下拉展开升级操作记录，可查看当前升级的各个模块升级情况，可以下载升级日志进行升级失败排查。

图表 79 版本信息

点击“升级中心”，浏览器打开新页面“在线升级中心”，在线升级中心包含设备状态、版本信息、更新记录、网络测试部分的信息。设备状态包括 CPU 负载，网络流通速度，内存总量及占用情况，磁盘容量及占用情况，磁盘响应时间，包转发率 pps，进程数。

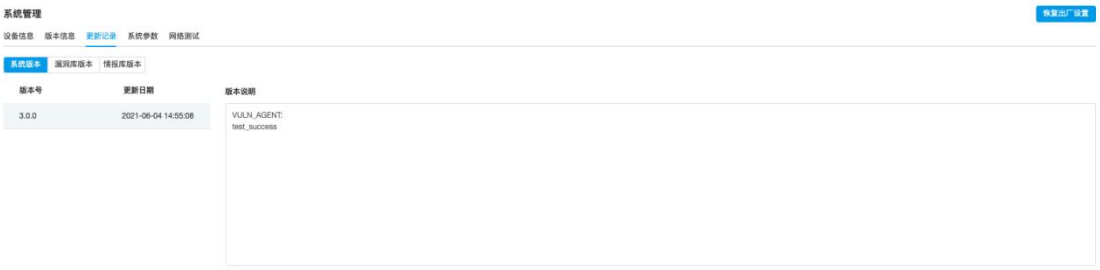


图表 80 升级中心



图表 81 设备状态

3）更新记录



图表 82 更新记录

4）系统参数

可进行合规参数、syslog 设置，需注意：密码更新间隔设置为 0 时，不进行密码更新间隔限制；无操作退出时间不能设置小于 5 分钟；允许登录失败次数设置为 0 时，不进行登录失败次数限制。

图表 83 系统参数

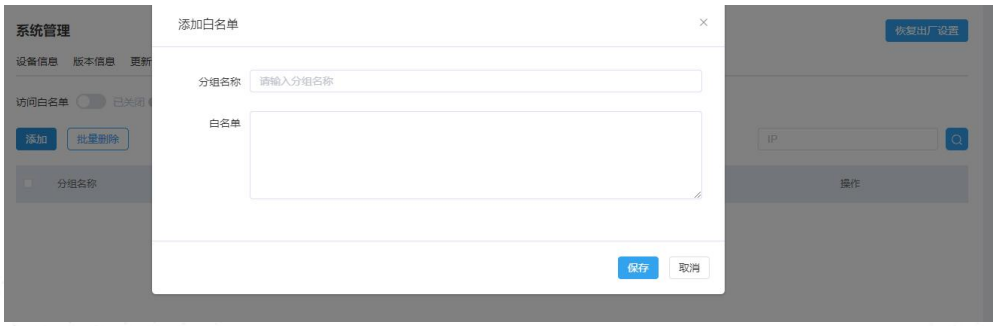
5）网络测试

点击“网络测试”后可输入 IP、域名、URL 地址后进行连通测试。

图表 84 网络测试

6）访问控制

点击“白名单”并添加相应 IP 地址，可设置访问控制，仅允许白名单范围内地址访问巡哨。

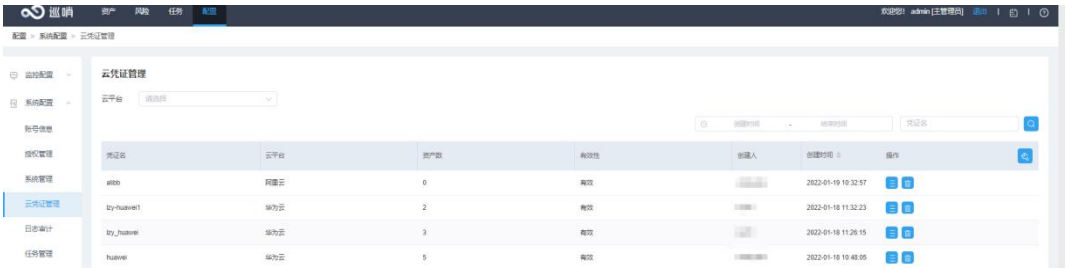


图表 85 访问控制

2.5.2.4 云凭证管理

在此可以查看管理所有用户各个平台的云凭证，云凭证是调用各云厂商接口

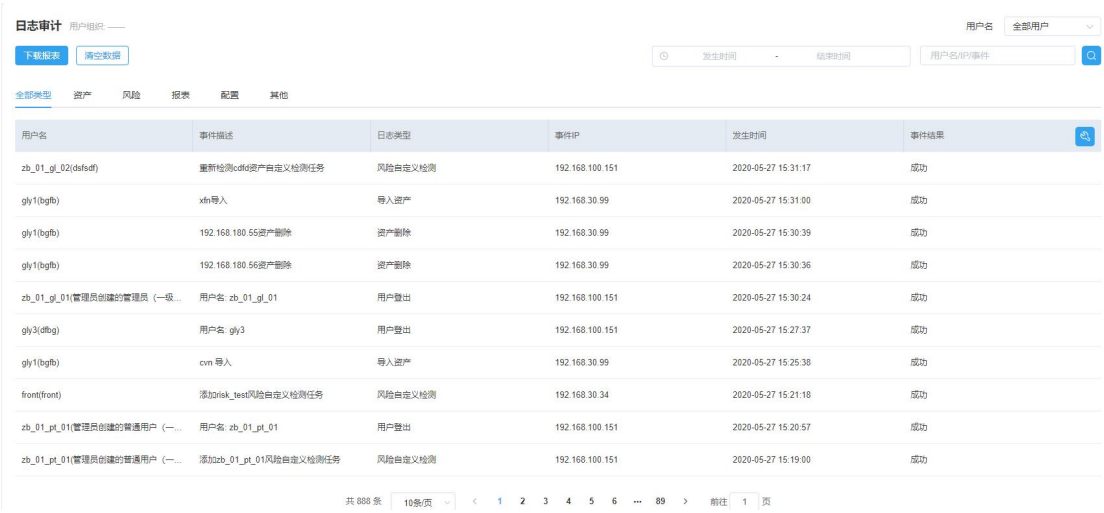
的必要参数，超管可在此对云凭证进行集中化管理该页面展示了用户创建的凭证名，所属平台，资产数，有效性，以及创建时间等信息。可通过创建时间，平台，凭证名对凭证进行搜索。



图表 86 云凭证管理

2.5.2.5 日志审计

日志审计页面记录各个用户的操作日志。日志审计列表包括登录用户名、事件描述、日志类型、事件 IP 以及发生时间。提供数据清空、下载报表、搜索（用户名、IP、事件和时间）功能。



图表 87 日志审计

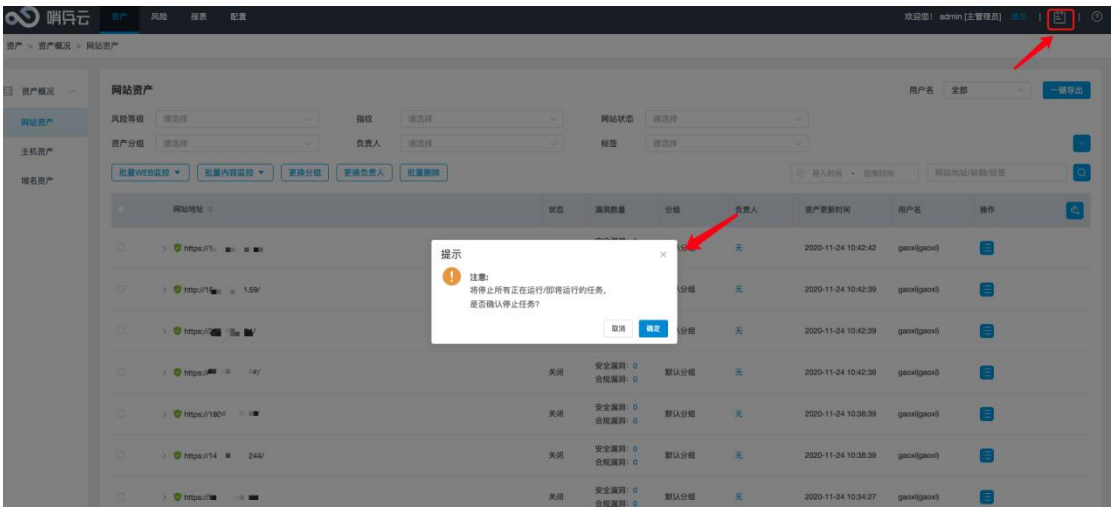
2.5.2.6 任务管理

任务管理页面包括等待中、正在执行以及任务队列，可以根据任务 ID 进行搜索。

图表 88 任务管理

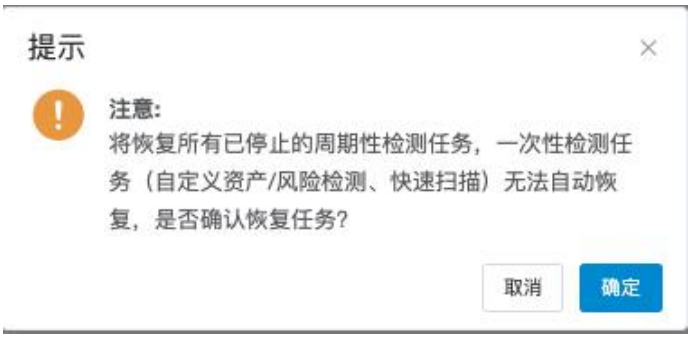
2.5.3 任务配置

主管理员顶部导航栏右上角“停止/恢复任务”按钮，可在有应急需求时一键停止任务队列中所有任务，需输入主管理员密码进行二次确认；停止任务后图标变成红色，再次点击按钮可执行恢复任务操作，注：可恢复所有已停止的周期性检测任务，一次性检测任务（自定义资产/风险检测、快速扫描）无法自动恢复，需要手动继续执行任务。



图表 89 一键停止任务

图表 90 二次确认



图表 91 恢复任务

2.6 帮助中心

帮助中心介绍产品的资产、风险、配置及其他内容。

图表 92 帮助中心

3 关于我们

3.1 公司介绍

默安科技成立于 2016 年，是一家面向云计算时代的新兴网络安全公司，致力于成为客户信赖的安全伙伴。

在云计算科技浪潮下，企业原有的安全体系已经被云的弹性、灵活和共享机制改变，默安科技通过提供与云紧密融合的云平台运营安全方案、混合云安全管理方案、DevSecOps/SDL 方案、云蜜网欺骗防御方案、资产发现与弱点管理方案，帮助客户建立面向云、适应云的新一代安全体系。

凭借领先的技术、卓越的产品理念和完善的产品体系，默安科技荣获 IDC 中国威胁情报安全服务市场创新者、最具投资价值企业 Top50、中国网络安全产业发展及投资价值 60 强、数字中国推动者 TOP100、CCF-GAIR“AI+安全”最佳商用成长奖，以及电子政务优秀案例、企业服务案例 Top50 等荣誉。

3.2 技术实力

ZJCERT 合作支撑单位；

浙江省互联网协会网络安全技术服务支撑单位；

信息安全服务资质证书（安全开发类一级）；

信息安全服务资质认证证书（信息安全风险评估三级服务资质）；

信息安全服务资质认证证书（信息系统安全运维三级服务资质）；

中国通信企业协会通信网络安全服务能力评定证书（一级风险评估能力）；

ISO9001 质量管理体系认证；

杭州市高新技术企业。

2017 年最具投资价值企业；

2018 中国网络安全产业发展及投资价值 60 强；

2018CCF-GAIR“AI+安全”最佳商用成长奖；

2018CSS Future Power 50 安全新锐力量；

2018《互联网周刊》“数字中国推动者 TOP100；

2018 ISC“安全创客汇” 年度十强；

IDC 中国威胁情报安全服务市场创新者；

2018 安全牛“网络安全行业全景图”酷厂商；

2018 年度双 11 企业服务企服英雄榜第 18 位；

政务云安全解决方案获 2018 年广东省电子政务优秀案例；

万科应用系统开发安全项目获 i 黑马 2018 企业服务企服案例 TOP50；

2018 年赛迪网络安全潜力企业榜 80 强；

2019 年杭州准独角兽企业。

除此以外，公司目前拥有十多项专利，数个软件著作权；率先提出了甲方视角的威胁情报理念，并发布业内首个具备自我进化能力的安全大脑——Aida；携手泰隆银行成立“泰隆银行信息安全联合实验室”，这是国内首个由金融机构成立的安全实验室；提出布局全栈云计算安全，成为阿里云云盾专有云合作伙伴。

同时，默安科技也是中国通信企业协会、中国云安全与新兴技术安全创新联盟、中通服云计算联盟、中国网络安全产业联盟、关键信息基础设施联盟、浙江省互联网协会、浙江省软件行业协会、浙江省网络空间安全协会、浙江省信息经济联合会、广东省计算机信息网络安全协会、广东省电子政务技术应用支持联盟等组织的成员单位。

3.3 客户案例

3.4 总部及分支机构


2019
默安科技
总部及分支机构
杭州总部
杭州市余杭区文一西路1378号杭州师范大学科技园E幢10层
华北运营中心
北京市朝阳区东四环中路41号嘉泰国际大厦3层320-321
华南营销中心
广州市海珠区昌岗中路238号达镖国际1017
深圳市福田区祥泰宁的士码头大厦四楼
华中办事处
长沙市天心区芙蓉中路380号汇金国际银座3819-3821
上海办事处
上海市浦东新区世纪大道1196号世纪汇二座8楼