

主机安全

用户使用指南

天翼云科技有限公司

概述

天翼云主机安全系统（简称“主机安全系统”或者“系统”）是在深入分析与研究常见黑客入侵技术的基础上，总结归纳大量的安全漏洞信息和攻击方式后，研制开发的新一代终端安全防护产品。

本手册描述天翼云主机安全系统的配置方法，主要包括快速入门、Web 配置页面简介、许可管理、角色权限、用户认证、首页、终端监控大屏、终端管理、发布端管理、高级威胁、策略管理、响应处置、屏幕溯源、风险评估、安全策略、日志检索、终端全览、多级中心、升级管理、系统管理、运维平台等。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用天翼云主机安全系统的读者，包括服务工程师、系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- ◆ TCP/IP、SNMP 等基础网络通讯协议。
- ◆ 终端防护类产品基本原理。
- ◆ 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- ◆ 安全防护策略的基本工作原理和配置。





格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如：“在菜单栏选择‘ 系统状态 ’进入 系统状态 页面，选择 接口状态 页签”。
<>	Web 界面上的按钮。例如：“微信认证失败，点击< 我要上网 >不弹出微信认证界面”。

内容	说明
➤	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等）。 例如：“在菜单栏选择‘策略配置➤认证管理➤认证策略’查看是否开启了认证策略”。
斜体字	可变参数，必须使用实际值进行替代。例如：“在浏览器地址栏输入‘http://管理IP’，回车后进入系统 Web 管理平台登录页面”。

本手册图标格式约定如下。

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

修订记录

日期	修订版本	修改记录
2025-01-20	02	优化文档结构和部分描述。
2023-06-30	01	初次发布。

目录

1 快速入门	1
1.1 产品简介	1
1.2 产品功能	1
1.3 登录系统	2
1.4 角色与权限说明	2
2 Web 配置页面简介	3
3 操作日志	4
3.1 Admin 账户操作日志	4
3.1.1 查询操作日志	4
3.1.2 导出操作日志	4
4 联动管理	5
4.1 数据外发	5
4.1.1 日志外发	5
4.1.2 API 接口	6
5 首页	7
6 态势大屏	9
6.1 设置大屏模式	9
6.1.1 图表模式	9
6.1.2 列表模式	9
6.2 安全概况大屏	10
6.3 终端管控大屏	11
7 终端管理	12
7.1 管理终端	12
7.1.1 查看终端详情	12
7.1.2 编辑终端	13
7.1.3 查看策略	14
7.1.4 终端登记	14

7.1.5 远程协助	17
7.1.6 其他操作	18
7.2 移动存储	20
7.2.1 注册设备	20
7.2.2 设置自动授权	22
7.2.3 其他操作	22
7.3 管理分组标签	22
7.3.1 新增分组	23
7.3.2 新增标签	23
7.3.3 其他操作	24
7.4 主机发现	24
7.4.1 新建主机发现任务	25
7.4.2 执行主机发现任务	25
7.4.3 查看主机发现扫描结果	26
7.4.4 其他操作	26
7.5 容器安全	26
7.5.1 查看容器详情	26
7.5.2 启动容器防篡改防护	27
7.5.3 暂停容器防篡改防护	27
7.5.4 停止容器防篡改防护	28
7.6 敏感词检索	28
7.6.1 新增任务和相关操作项	28
7.6.2 其他操作项	30
7.7 网站备份	30
7.7.1 新增任务和相关操作项	31
7.7.2 其他操作项	32

7.8 网站恢复.....	33
7.8.1 新增任务.....	33
8 资产盘点.....	34
8.1 资产盘点.....	34
8.1.1 进行资产盘点.....	34
9 风险评估.....	36
9.1 查杀病毒.....	36
9.1.1 终端视角.....	36
9.1.2 病毒视角.....	44
9.2 网马查杀.....	46
9.2.1 扫描终端的网马.....	47
9.2.2 查看扫描结果.....	49
9.2.3 处理网马.....	49
9.2.4 导出报告.....	50
9.2.5 设置查杀模式.....	50
9.2.6 相关操作.....	51
9.3 漏洞管理.....	53
9.3.1 Windows 系统漏洞.....	53
9.3.2 Linux 系统漏洞.....	58
9.3.3 Windows 应用漏洞.....	60
9.3.4 Linux 应用漏洞.....	62
9.4 终端体检.....	64
9.4.1 终端评估.....	64
9.4.2 勒索评估.....	65
9.4.3 挖矿评估.....	65
9.4.4 弱口令评估.....	66
9.4.5 查看评估结果.....	66

9.5 基线检查	67
9.5.1 新增任务	67
9.5.2 执行任务	67
9.5.3 相关操作	68
9.6 定期巡检任务	68
9.6.1 新增定期巡检任务	68
9.6.2 编辑定期巡检任务	69
9.6.3 删除定期巡检任务	70
9.7 弱口令检测	70
9.7.1 应用弱口令	70
9.7.2 新增定期巡检任务	71
9.7.3 新增定期巡检任务	71
10 入侵检测	73
10.1 攻击矩阵	73
10.1.1 攻击热力图	73
10.1.2 受攻击主机热力图	73
10.1.3 受攻击工作组热力图	74
10.2 入侵告警	74
10.2.1 入侵告警信息	75
10.2.2 入侵告警处理	76
10.3 检测规则	82
10.3.1 检测规则	82
10.3.2 信任列表	82
10.3.3 处置方式	83
10.4 模型	83
10.4.1 新增信任模型	84
10.4.2 查看信任模型	85

11 威胁情报	87
11.1 智能鉴定.....	87
11.2 沙箱分析.....	87
12 发布端管理	88
12.1 管理发布端.....	88
12.1.1 新增发布端.....	88
12.1.2 修改发布端信息.....	89
12.1.3 其他操作.....	90
12.2 配置发布信息.....	90
12.2.1 新增发布目录.....	90
12.2.2 配置发布端策略.....	92
12.2.3 其他操作.....	93
13 高级威胁	94
13.1 设置勒索防御.....	94
13.2 设置挖矿防御.....	94
13.3 设置渗透追踪.....	95
13.4 查看情报云脑.....	96
14 策略管理	98
14.1 终端策略.....	98
14.1.1 新增策略.....	98
14.1.2 编辑策略.....	99
14.1.3 绑定终端.....	145
14.1.4 其他操作.....	146
14.2 容器策略.....	147
15 响应处置	149
15.1 微隔离.....	149
15.1.1 混合模式.....	149
15.1.2 白名单模式.....	154

15.1.3 黑名单模式.....	156
15.2 流量画像.....	159
15.2.1 查看通信关系.....	159
15.2.2 自定义模板.....	162
15.3 文件推送.....	163
15.4 事件调查.....	164
15.4.1 搜索事件数据.....	164
15.4.2 配置数据采集.....	164
16 日志检索.....	167
16.1 防护日志.....	167
16.1.1 查看防护日志.....	167
16.1.2 导出防护日志.....	167
16.1.3 统计分析.....	168
16.2 操作日志.....	168
16.2.1 查询操作日志.....	169
16.2.2 导出操作日志.....	169
16.3 运维日志.....	169
16.3.1 查询运维日志.....	169
16.3.2 导出运维日志.....	169
16.4 篡改分析.....	170
16.5 日志报表.....	171
16.5.1 导出报表.....	171
16.5.2 订阅报表.....	171
17 终端全览.....	173
17.1 查看终端详情.....	173
17.2 前往租户.....	173
17.3 导出.....	173

18 多级中心	175
18.1 查看中心详情	175
18.2 配置上级中心	176
18.3 其他操作	176
19 系统管理	177
19.1 Admin 账户系统管理	177
19.1.1 客户端及库升级	177
19.1.2 管理平台升级	180
19.1.3 Windows 补丁库	181
19.1.4 密码及访问策略	185
19.1.5 部署管理	187
19.1.6 个性化	188
19.2 租户账户系统管理	189
19.2.1 部署管理	189
19.2.2 许可分配	196
19.2.3 告警配置	196
19.2.4 个人中心	198
20 运维平台	199
20.1 查看运维诊断结果	199
20.2 清理磁盘	200
20.3 重置密码	201
20.4 恢复数据	201
20.4.1 恢复 MySQL 数据	201
20.4.2 检测 ES 状态	202
21 FAQ	204
21.1 如何区分 Docker 版本与非 Docker 版本?	204
22 术语&缩略语	205

1.1 产品简介

天翼云主机安全系统是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。主机安全系统有着业界领先的文件诱饵勒索专防专杀能力；能通过内核级东西向流量隔离技术，实现云主机隔离与防护；并拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。

主机安全系统由管理控制中心和客户端组成。

- ◆ 管理控制中心部署在独立云主机上，主要功能是把所有客户端信息和管理集中于一体，便于集中监管和配置安全策略，聚合客户端情报信息进行后续的反应以及处置。管理控制中心采用 B/S 架构，安装完成后，用户可以在任意与管理控制中心网络可达的计算机上访问管理控制中心的 Web 页面，对终端进行管控。
- ◆ 客户端软件是一个独立的本地可执行程序，安装在需要被管控的主机上，并完成管理员通过管理控制中心下发的任务和策略。

1.2 产品功能

主机安全系统具有以下功能模块：

1. 防御已知和未知类型勒索病毒

主机安全系统不仅可以阻止已知勒索病毒的执行，而且面对传统杀毒软件束手无策的未知类型勒索病毒时，主机安全系统采用诱饵引擎，在未知类型勒索病毒试图加密时发现并阻断加密行为，有效守护主机安全。

2. 防御高级威胁全流程攻击

主机安全系统根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，包括单机扩展、隧道搭建、内网探测、远控持久化、痕迹清除。不仅可以做到威胁攻击审计，而且还可以防止黑客进行渗透攻击，实现攻防对抗 360 度防御。

3. 管控全局终端安全态势

服务器、PC 和虚拟机等终端安装了客户端软件后，上传终端指纹、病毒木马、高危漏洞、违规外联、安全配置等威胁信息到管理控制中心。用户在管理控制中心可以看到所有安装了客户端软件的主机及安全态势，并进行统一任务下发，策略配置。

4. 全方位的主机防护体系

主机安全系统不仅包含传统杀毒软件的病毒查杀、漏洞管理、性能监控功能，在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控，还支持网络防护、Web 应用防护、勒索挖矿防御、外设管理等多个功能点。

5. 流量可视化，安全可见

主机安全系统通过流量画像的流量全景图，展示内网所有流量和主机间通信关系，梳理通信逻辑，以全局视角对策略进行规划，便于用户第一时间发现威胁，一键清除威胁。

6. 简单配置，离线升级，补丁管理

主机安全系统支持用户自主进行安全配置，能够明确、有效的进行主机防护。主程序、病毒库、漏洞库、补丁库、Web 后门库、违规外联黑名单库全部支持离线导入升级包、一键自动升级，可在专网使用。

1.3 登录系统

产品仅支持从天翼云平台页面单点登录主机安全的 web 管理页面。

1.4 角色与权限说明

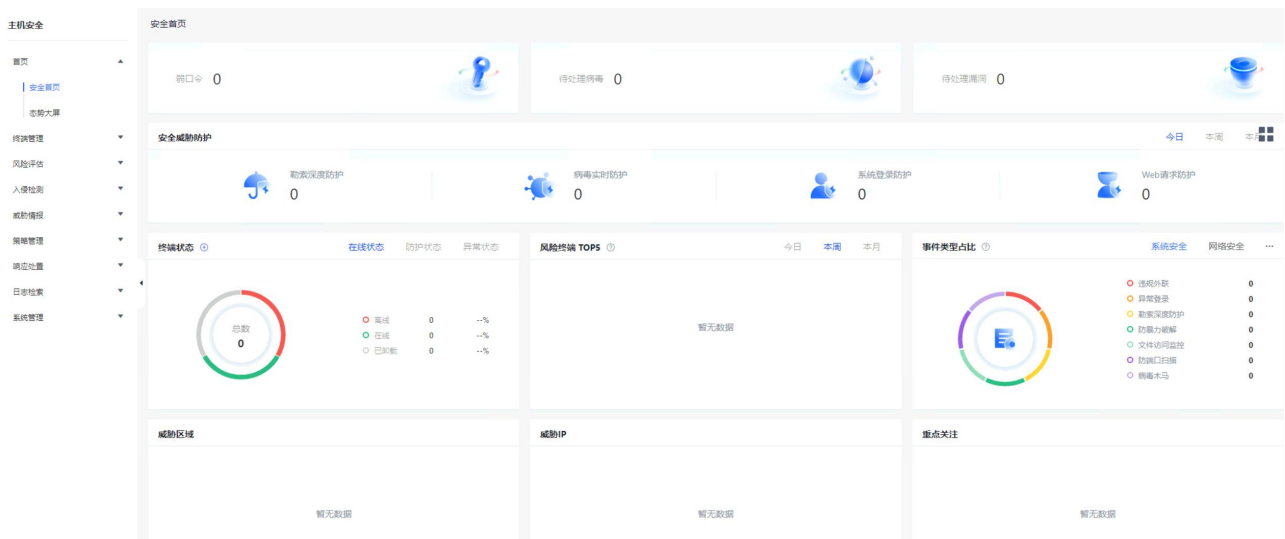
主机安全系统中，管理员角色与租户角色拥有不同的操作权限。

角色	权限
管理员 (admin)	<ul style="list-style-type: none"> ◆ 用户认证：新增用户、编辑用户信息、删除用户、登录用户、用户权限。 ◆ 联动管理：产品联动配置、数据外发配置。 ◆ 终端全览：查看终端列表及终端详情。 ◆ 操作日志：查看用户登录、编辑、删除等操作 ◆ 多级中心：配置上级、查看多级中心详情、编辑下级中心信息、删除下级中心。 ◆ 升级管理：管理平台升级、终端软件安装包上传、终端软件更新包上传、病毒库升级、系统漏洞库升级。 ◆ 系统管理：Windows 补丁库管理、弱口令库管理、Linux 驱动包上传、密码及访问策略。 ◆ 运维平台：查看运维诊断结果、清理磁盘、重置密码、恢复数据。
租户	<ul style="list-style-type: none"> ◆ 首页：查看系统信息概览。 ◆ 终端管理：终端概况、病毒查杀、网马查杀、漏洞管理、微隔离、移动存储、分组标签。 ◆ 发布端管理：管理发布端、配置发布信息。 ◆ 高级威胁：勒索防御、挖矿防御、渗透追踪、情报云脑。 ◆ 策略管理：基础信息、系统防护、网络防护、渗透追踪、网页防篡改、Web 应用防护、信任名单、桌面管控、终端体检。 ◆ 响应处置：信息搜索、文件推送、定期巡检、流量画像。

角色	权限
	<ul style="list-style-type: none"> ◆ 屏幕溯源：对通过屏幕拍照、屏幕截图泄密数据进行溯源，确定泄密的终端信息。 ◆ 风险评估：终端体检、基线检查。 ◆ 安全策略：容器篡改防护。 ◆ 日志检索：防护日志、操作日志、运维日志、日志报表。 ◆ 系统管理：添加终端、推广部署、升级管理、许可分配、告警配置、个人中心。 ◆ 运维平台：查看运维诊断结果、清理磁盘、重置密码、恢复数据。

2 Web 配置页面简介

系统提供简便的 Web 配置页面，主要包括四部分：1.产品信息；2.用户个人中心；3.导航栏；4.操作区。下图以租户管理员的 Web 配置页面举例说明。



各区域的详细说明请参见下表。

序号	名称	说明
1	产品信息	产品名称及版本信息，点击此区域可返回 Web 管理平台主页。
2	用户个人中心	用户可在此区域进行以下操作：查看系统版本和授权信息、反馈意见、登录运维平台、修改密码、退出系统、身份验证器。
3	导航栏	提供了各类管理功能的配置入口，方便用户根据实际需要进行切换。
4	操作区	该区域主要用于信息展示以及相关功能的配置。

3 操作日志

租户用户可在此页面查看租户用户的操作审计记录。

3.1 Admin 账户操作日志

Admin 可在操作日志页面查看用户、操作 IP、日志类型、描述、时间、状态等日志信息。

3.1.1 查询操作日志

步骤 1. 以 Admin 角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“操作日志”，设置查询条件（如关键字、日期等），点击<查询>，即可查询符合该条件的操作日志。

用户	操作IP	日志类型	描述	时间	状态
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:19:55	成功
admin	10.11.1.1	用户登录	admin登录成功	2022-11-28 10:19:53	成功
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:17:54	成功
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:09:52	成功
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:09:44	成功
admin	10.11.1.1	用户登录	admin登录成功	2022-11-28 10:09:41	成功
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:00:04	成功
admin	10.11.1.1	用户登录	admin登录成功	2022-11-28 09:59:19	成功
admin	10.24.1.1	用户登录	admin登录失败	2022-11-27 14:51:20	失败
admin	10.11.1.1	用户登录	admin登录成功	2022-11-25 19:26:50	成功

3.1.2 导出操作日志

点击<导出日志>，选择文件格式（CSV 或 Excel），可将所查询的操作日志导出至本地。

用户	操作IP	日志类型	描述	时间	状态
admin	10.11.1.1	日志操作	读取了admin-总操作日志数据记录	2022-11-28 10:19:55	成功



- ◆ 支持导出 CSV 格式和 Excel 格式。
- ◆ 支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。


4 联动管理

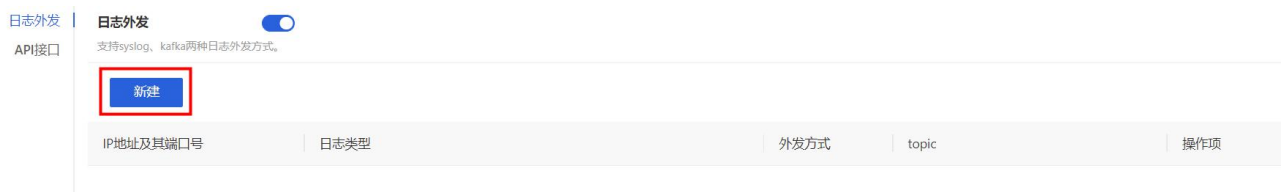
用户可在该功能快速配置与 Ailpha、APT、-Gateway、堡垒机、蜜罐产品联动。

4.1 数据外发

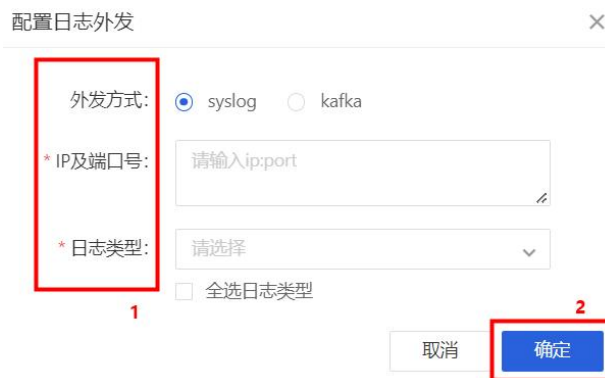
用户可在该功能快速配置 syslog、kafka 日志外发及 OpenAPI 调用。

4.1.1 日志外发

步骤 1. 以 Admin 角色登录主机安全系统管理平台，在导航栏选择“联动管理>数据外发>日志外发”进入页面点击  按钮后，开启此功能；再点击<新建>按钮。




步骤 2. 在弹窗中外发方式、IP 及端口号、日志类型后，点击<确定>按钮即可。



- ◆ 该位置配置的日志外发功能是所有租户的日志统一由一个出口汇总发出。
- ◆ 如需要单个租户的相应日志外发功能，请到租户-系统管理-告警配置-Syslog 处配置对应外发策略。
- ◆ V3.0R23C11 版本开始支持入侵检测 syslog 外发，勾选对应日志类型即可。
 - ◆ Kafka 外发支持 AiXDR 产品的 topic。

4.1.2 API 接口

步骤 1. 以 Admin 角色登录主机安全系统管理平台，在导航栏选择“**联动管理**▶**数据外发**▶**API 接口**”
进入页面点击  按钮开启此功能即可。

日志外发

API接口

OpenAPI调用



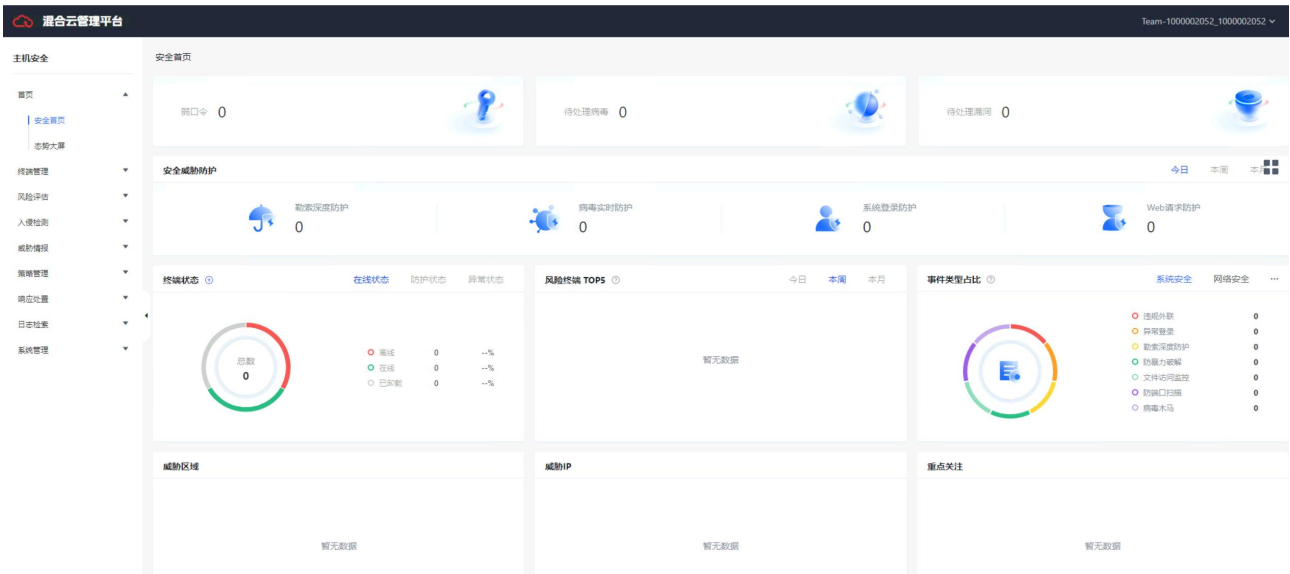
产品支持第三方平台OpenAPI调用，关闭可增强产品安全性。产品联动关联使用OpenAPI，如关闭则联动同步关闭。



只要有任意一个如上产品联动必须开启此 api 接口按钮。

仅租户角色具有查看首页权限。

以租户账号登录主机安全系统管理平台，默认进入“安全首页”显示主机终端总体安全概览。



具体展示信息说明如下。

信息	说明
弱口令	点击弱口令数字，用户可查看终端的弱口令评估结果。详情可参考 弱口令评估 。
待处理病毒	点击待处理病毒数字，用户可查看病毒查杀详情。详情可参考 病毒查杀 。
待处理漏洞	点击待处理漏洞数字，用户可查看详细漏洞信息。详情可参考 漏洞管理 。
安全威胁防护	包括渗透追踪防护、勒索深度防护、病毒实时防护、系统登录防护、Web 请求防护，点击防护数字可查看详细防护日志。详情可参考 防护日志 。
终端状态	展示终端总数以及终端状态的占比，包括防护中、停止防护、熔断、隔离中、驱动未安装、授权过期等。 <div style="display: flex; align-items: center;"> <div style="margin-right: 20px;"> <p>终端状态</p> <p>总数</p> <p>5</p> </div> <div> <p>在线状态 防护状态 异常状态</p> <ul style="list-style-type: none"> ● 离线 0 0.0% ● 在线 5 100.0% ● 已卸载 0 0.0% </div> </div>
威胁区域	展示本周攻击次数前五的区域。
事件类型占比	展示本周攻击事件的数据。点击右上角 *** 图标和“系统安全”、“网络安全”可查看事件详情。

信息	说明														
	<p>事件类型占比 🔍 系统安全 网络安全 ...</p>  <table border="1" style="margin-left: 200px;"> <tr><td>违规外联</td><td>0</td></tr> <tr><td>异常登录</td><td>0</td></tr> <tr><td>勒索深度防护</td><td>1</td></tr> <tr><td>防暴力破解</td><td>1</td></tr> <tr><td>文件访问监控</td><td>0</td></tr> <tr><td>防端口扫描</td><td>197</td></tr> <tr><td>病毒木马</td><td>1</td></tr> </table>	违规外联	0	异常登录	0	勒索深度防护	1	防暴力破解	1	文件访问监控	0	防端口扫描	197	病毒木马	1
违规外联	0														
异常登录	0														
勒索深度防护	1														
防暴力破解	1														
文件访问监控	0														
防端口扫描	197														
病毒木马	1														
风险终端 TOP5	默认展示本周被攻击次数前五的终端。可调整统计时间为“今日”或“本月”。														
威胁 IP	展示本周被攻击次数前五的终端 IP 及被攻击次数。														
重点关注	展示日志里的重点关注事件。														

仅租户角色具有终端监控大屏操作权限。




态势大屏以可视化的方式展示资产的状态以及安全概况，方便租户快速掌控资产的安全态势。

6.1 设置大屏模式

6.1.1 图表模式

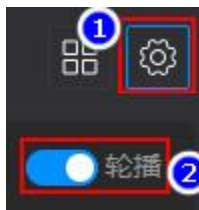
步骤 1. 在首页页面上方点击<态势大屏>。




步骤 1. 进入大屏界面后，点击图标进入图表模式，点击图标或图标可切换要展示的大屏。



步骤 2. 点击图标，点击开关，开启或关闭轮播功能。开启轮播功能，系统会自动切换大屏。



6.1.2 列表模式

点击图标进入列表模式，点击对应图片即可展示对应大屏。



6.2 安全概况大屏

安全概况大屏展示终端的总体的安全态势。



详细信息请参见下表。

编号	名称	说明
1	终端分布图	以立体图片的形式展示终端分布情况，可切换展示“全部节点”和“风险节点”。
2	防护概况	展示风险总数、今日新增风险数量以及风险等级分布图。
3	入侵检测	展示安全防护类型及事件数量统计。
4	防护风险趋势	展示最近一周安全防护事件变化趋势。
5	最近发现的风险终端	展示最近发现的5个风险终端，包括终端名称、IP地址、风险类型、风险等级和发现时间。
6	检测概况	统计弱口令数量、待处理病毒数量、待处理网马数量和待修复漏洞数量。
7	威胁IP	展示被攻击次数最多的终端TOP5，包括IP地址和被攻击次数。
8	安全动态	展示所有终端最新的病毒防护等安全事件。

6.3 终端管控大屏

进入终端管控可视化大屏，滚动展示终端部署、防护、资源、告警等信息。



详细信息参见下表。

编号	名称	说明
1	终端状态	终端近期在线、离线状态统计。
2	终端分组统计	终端分组的终端数量统计（包括 Linux 服务器组、系统默认组和 Windows 组和其他自定义分组）。
3	设备系统分类	终端设备按操作系统分布图，包括设备数量及占比。
4	终端安全态势图	包括总装机量、防护率，并滚动展示各分组的设备类型、安装量和防护率。
5	最新安装主机、最新发现主机	展示最新安装的主机和最新发现的主机信息，包括终端名称、IP、操作系统等信息。
6	版本统计	统计 Windows 版本信息及 Linux 版本信息。
7	标签统计	统计终端标签信息。
8	客户端告警	展示客户端告警信息，主要包括客户端各类防护告警信息。

仅租户角色具有终端管理权限。

7.1 管理终端

租户角色可在**终端概况**页签查看所有绑定该中心的主机信息，包括名称、分组、标签、IP、操作系统、终端版本等，并可进行查看终端详情、编辑终端、查看策略等操作。

7.1.1 查看终端详情

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**终端管理**▶**终端概况**”进入**终端概况**页面，选择需要查看的主机终端（须确保终端为在线状态），点击终端名称或者点击**操作项**列中的“**查看**”图标。



步骤 2. 进入**终端详情**页面，即可查看该主机终端的详细信息，并可进行远程重启主机、关闭主机及修改远程端口操作。



终端概况说明如下。

终端信息	说明
终端详情	<ul style="list-style-type: none"> 对终端进行详细信息展示：包括网络信息、环境信息、其他信息等；并支持远程关闭主机、重启主机、IP/MAC 绑定（适用于 Windows 主机）等操作。 点击网络信息的 图标，可对终端进行 IP/MAC 绑定操作。设置好需要进行绑定的 IP 以及对应的 MAC。绑定后如果 IP 被修改，将会自动退回至绑定的 IP，并在运维日志进行告警。目前只支持对 Windows 系统主机 进行 IP/MAC 绑定。 点击远程管理端口的 图标，可修改终端远程管理端口。修改完毕后，

终端信息	说明
	需要重启远程管理服务才能生效，重启过程中将会断开已连接会话。
监听端口	对终端上端口情况进行实时监控。
运行程序	对终端上进程运行情况进行实时监控，并支持远程结束相关进程。
账号信息	对终端上所有账号信息进行统计。
运行应用	对终端上运行的软件应用信息进行统计。
性能监控	对终端上的内存、CPU、磁盘、网络 IO 进行监控统计。
临时封锁 IP	对终端上因为防暴力破解和防端口扫描而引发的临时封锁 IP 进行管理。
注册表启动项	对终端上所有的注册表启动项进行统计和管理。
Web 框架	对终端上运行的 Web 框架进行统计。
Web 服务	对终端上运行的 Web 服务进行统计。
数据库	对终端上运行的数据库进行统计。
Web 应用	对终端上运行的 Web 应用进行统计。
在线统计	对终端的在线时间进行统计。
安装软件	对终端安装包名、版本号、类型、发布者、安装时间等进行统计。
Jar 包	对终端安装所关联的 jar 包进行统计。
计划任务	对终端被制定了哪些计划任务进行统计。
环境变量	对终端的环境变量进行统计。
内核模块	对终端内核模块名称、版本号、模块路径和大小、模块依赖等进行统计。
Windows 证书	对终端的各种证书进行统计。

7.1.2 编辑终端

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>终端概况”进入终端概况页面，选择需要编辑的终端，点击右侧操作项列中的“编辑”图标。



终端名称	所属分组	标签	IP地址	MAC地址	操作系统	终端版本	在线状态	防护状态	绑定策略	最近一次离线时间	sss	操作项
DESKTOP-...	PC组	DB	10.23...	FC-34-97-B...	Windows 10 Enterp...	3.0.7.104	在线	防护中	ttt	2023-10-11 14:46:35	2233333	查看 编辑 策略 远程协助

步骤 2. 在弹出的对话框中编辑终端信息，点击<确定>，即可修改终端信息。

编辑终端信息时，若绑定状态开关的状态调整为关闭，将解绑该终端，被解绑的终端会从终端列表中删除。

编辑终端 ×

基本信息

* 终端名称:

* 所属分组:

标签:

绑定状态: 开

默认开启, 关闭绑定状态, 该终端将从终端列表中移除。

IP地址: 192.1[...]

操作系统: CentOS Linux 7 (Core)

终端版本: 3.0.2.104

登记信息

7.1.3 查看策略

- 步骤 1. 以租户角色登录主机安全系统管理平台, 在导航栏选择“终端管理>终端概况”进入终端概况页面。
- 步骤 2. 选择需要查看的终端, 点击右侧操作项的“策略”图标, 即可对该终端的策略信息进行查看和编辑操作, 详情请参考[策略管理](#)。

终端名称	所属分组	标签	IP地址	MAC地址	操作系统	终端版本	在线状态	防护状态	绑定策略	最近一次离线时间	sss	操作项
DESKTOP-...	PC组	DB	10.23[...]	FC-34-97-B...	Windows 10 Enterp...	3.0.7.104	在线	防护中	ttt	2023-10-11 14:46:35	2233333	查看 编辑 策略 远程协助

7.1.4 终端登记



终端登记功能仅适用于 Windows 系统终端。

租户管理员可向客户端下发登记指令, 客户端用户提交登记信息后, 租户管理员可在“终端管理>终端概况”页面的列表中查看登记信息, 方便租户管理员了解终端的信息。

步骤 1. 租户管理员下发终端登记指令。

- 以租户角色登录主机安全系统管理平台, 在导航栏选择“终端管理>终端概况”进入终端概况页面, 点击<登记管理>。



- 进入登记管理页面, 将是否启用登记终端后的开关置于开启状态, 点击<新增>。



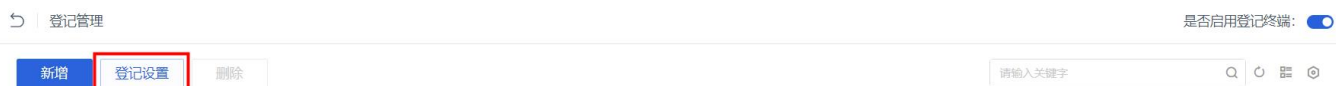
3) 在弹出的**新增登记信息**对话框中编辑相关信息，点击<确定>。



详细配置请参见下表。

配置项	说明
登记信息	不超过 15 字符。
是否启用	必须将 是否启用 后的开关置于开启状态，才能使登记信息生效。
是否必填	设置是否为必填项。
输入类型	<ul style="list-style-type: none"> ◆ 输入框。 ◆ 下拉框：需要添加数据，以供选择。


4) 点击<登记设置>。

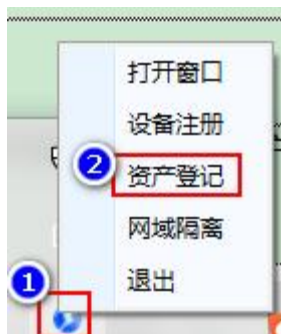


5) 在弹出的**登记设置**对话框中选择提醒方式（对于未完成登记信息的终端，会在终端的操作系统界面弹出登记信息弹窗，提醒用户完成终端登记操作），点击<确定>。



步骤 2. 终端用户提交登记信息。

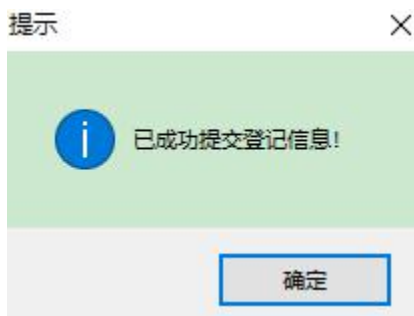
- 1) 终端用户在系统托盘右键点击主机安全系统客户端图标, 选择“资产登记” (以 Windows 10 系统举例说明)。



- 2) 在弹出的对话框中编辑登记信息, 点击<提交>。



- 3) 在弹出的对话框中点击<确定>。



步骤 3. 租户管理员查看终端登记信息。

以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>终端概况”进入终端概况页面，可查看终端登记信息。

所属分组	标签	IP地址	MAC地址	操作系统	终端版本	终端状态	所属部门	终端负责人
系统默认组		10.20.11.16	3C-52-82-47...	Windows 10 64-bit	3.0.2.104	防护中	财务部	张三

7.1.5 远程协助

租户管理员可向客户端下发远程协助指令，客户端接收到远程协助命令后，租户可以对其进行远程协助。

步骤 1. 租户管理员下发远程协助指令。

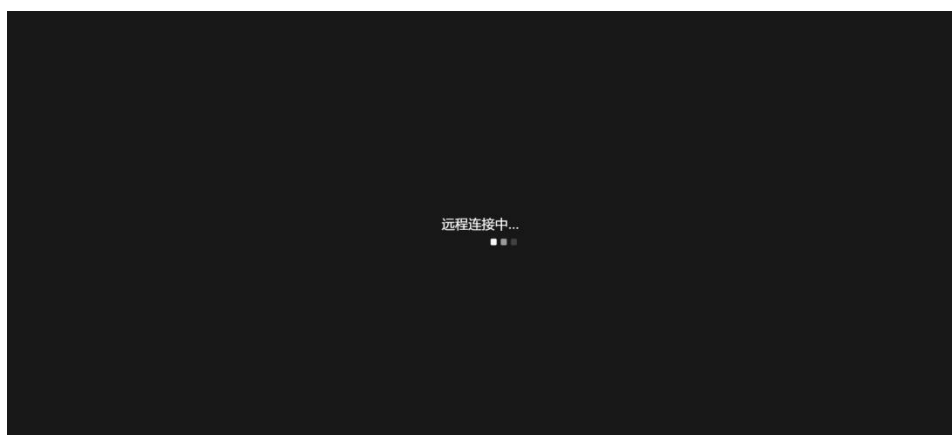
- 1) 以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>终端概况”进入终端概况页面，点击<远程协助>。

DESKTOP...	PC组	192.168.27.143	00-0C-29-10...	Windows 10 64-bit	3.0.3.107	防护中	hjj	查看	编辑	策略	远程协助
------------	-----	----------------	----------------	-------------------	-----------	-----	-----	----	----	----	------

- 2) 弹出是否确定远程协助页面，点击<确认>即可进行远程协助。



- 3) 在浏览器新页签等待连接建立。



远程协助该功能默认被控终端强制服从远程连接指令；



勾选<admin 账户-系统管理-密码及访问策略-高危操作二次验证>后建立连接需要输入身份验证器的验证码；

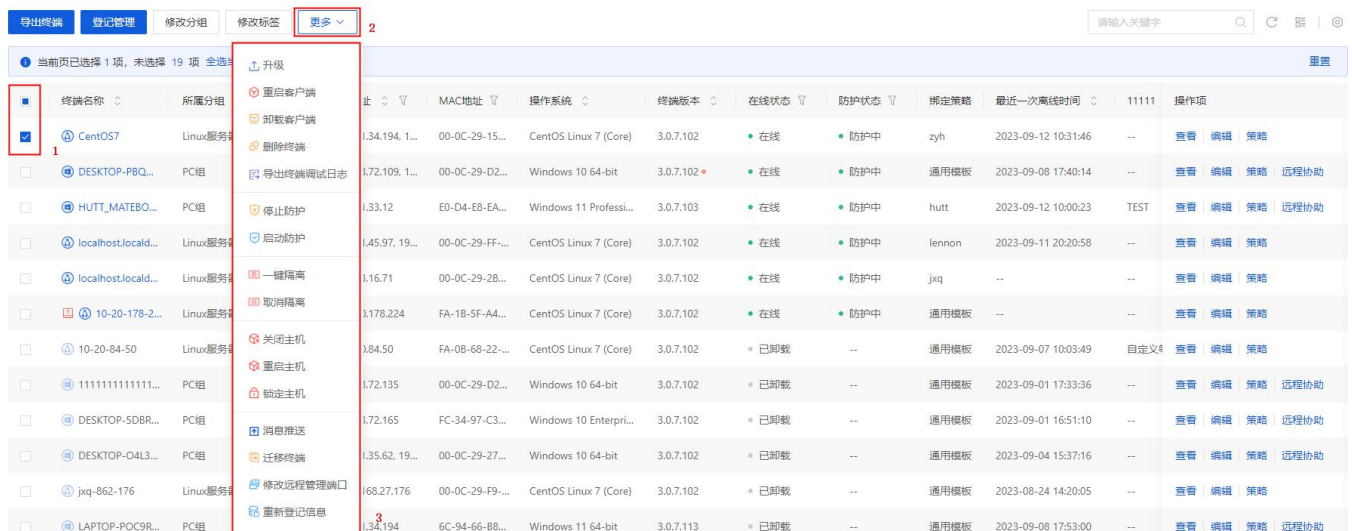
<策略管理-终端管理-远程协助-应答方式>可以设置：自动应答和用户响应。

7.1.6 其他操作

- ◆ 以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>终端概况”进入终端概况页面。租户可在此页面修改终端分组、修改终端标签、导出终端、登记管理操作。



- ◆ 勾选终端，点击<更多>，在弹出的下拉框中选择不同的菜单项，可对终端进行卸载客户端、删除终端、停止防护、启动防护、关闭主机、重启主机、重启客户端、迁移终端、修改远程管理端口、导出终端调试日志、消息推送、一键隔离、取消隔离等操作。



具体操作说明如下。

操作	说明
导出终端	可将终端信息以 CSV 格式导出至本地。
修改分组/修改标签	修改所选终端的分组/标签，每个终端必须且只能在一个分组内，可以有多个标签。
登记管理	设置终端登记信息，详情请参见 终端登记 。
卸载客户端	卸载终端上的主机安全系统客户端软件。
删除终端	删除终端后，主机安全系统不能对终端进行管控，许可也将释放。终端信息以及相关日志将会删除，但部分防护依然有效。
停止防护	关闭所选终端当前所有防护。
启动防护	启动对终端的防护。
关闭主机/重启主机	对所选终端进行关机或重启。
重启客户端	对客户端进行重启。

操作	说明
锁定主机	锁定目标客户端。
迁移终端	<p>填写新中心 IP 和 UUID，点击<确定>，可对租户内终端进行同中心跨租户迁移以及不同中心间迁移。</p>  <p>迁移终端对话框包含以下元素： - 标题：迁移终端 - 输入框：* 新中心IP (提示：请输入，填写格式为127.0.0.1:10571) - 输入框：* 新租户UUID (提示：请输入) - 按钮：取消、确定</p>
修改远程管理端口	<p>填写需要修改的远程管理端口，勾选立即重启，点击<保存>即可修改远程管理端口。</p>  <p>修改远程管理端口对话框包含以下元素： - 标题：修改远程管理端口 - 提示框：修改完毕后，需要重启远程管理服务才能生效，重启过程中将会断开已连接会话。 - 输入框：* 远程管理端口: (提示：请输入) - 复选框：立即重启 - 按钮：关闭、保存</p>
导出终端调试日志	<p>将所选终端的客户端运行日志，异常转储日志，操作系统日志信息导出。</p>  <p>导出终端调试日志对话框包含以下元素： - 标题：导出终端调试日志 - 提示框：导出终端日志，方便分析终端的各类异常情况。 - 复选框列表： - <input type="checkbox"/> 客户端运行日志 - <input type="checkbox"/> 客户端异常转储日志 - <input type="checkbox"/> 操作系统事件日志 - 按钮：关闭、保存</p>
升级	对客户端主程序进行升级操作。
消息推送	<p>对客户端所在终端进行消息推送（仅适用于 Windows 主机）。</p>  <p>消息推送对话框包含以下元素： - 标题：消息推送 - 提示框：对Windows主机进行消息弹窗提醒 - 输入框：* 消息内容: (提示：请输入消息内容) - 提示时间：持续提示 - 0 + 秒 - 按钮：取消、确定</p>
重新登记信息	对客户端重新登记资产信息。

操作	说明
一键隔离	对选定客户端进行一键断网。
取消隔离	对选定客户端取消一键断网策略。

7.2 移动存储


主机安全系统默认对移动存储不进行控制（即默认读写权限），若要对移动存储进行控制，需要对未授权的设备进行审批。

- ◆ 支持管理员对入网的移动存储介质进行注册，并且对已注册的移动介质进行管理。可以有效防止数据外泄以及移动存储携带病毒入网的问题。
- ◆ 支持的移动存储介质格式包括但不限于 FAT32、exFAT、NTFS 等。

7.2.1 注册设备

当在**移动存储管控**中（详情请参考[配置移动存储管理](#)）设置了禁用移动存储设备，需要在客户端注册移动存储设备，用户才能在终端上使用移动存储设备。

步骤 1. 登录终端设备，运行**主机卫士**客户端。主机卫士客户端的安装方式请参考[添加终端](#)。

步骤 2. 点击页面右上方的图标，在弹出的下拉框选择“**设备注册**”。



步骤 3. 插入移动存储设备，编辑责任人、联系电话和申请原因，点击<**申请注册**>提交注册申请。

设备注册 ✕

盘符: 移动存储 (F:)

设备名称: 移动存储

容量: 14.66GB

厂商: multiple

产品型号: card_reader

责任人: 设备保管责任人

联系电话: 设备保管人联系电话

申请原因: 请向管理员注明申请原因

申请注册

步骤 4. 以租户角色登录主机安全系统管理平台，在左侧导航栏选择“终端管理>移动存储”，可在设备列表中查看到该设备即表示注册成功。

步骤 5. 点击设备右侧操作项的“授权”图标。

设备名称	注册来源	设备类型	责任人	联系电话	容量	设备供应商	产品类型	设备ID	状态	操作项	
<input type="checkbox"/>	移动存储	--	普通注册设备	成都技术	--	57.73GB	kingston	datatraveler_3.0	1B3A912E...	已授权	删除 授权

步骤 6. 在弹出的授权对话框中选择设备权限，点击<确定>，即可完成设备权限设置。

授权 ✕

授权信息

设备名称: 移动存储 终端名称:

读写
 只读
 禁用

▶ 其他终端

硬件信息

设备供应商: kingston 容量: 57.73GB

产品类型: datatraveler_3.0 设备ID: 1B3A912EB567DDCC

注册信息

设备类型: 普通注册设备 注册来源:

设备名称: 责任人:

联系电话:

申请原因:

取消
确定



- ◆ 注册成功的设备仅对当前终端生效，若需对其他终端生效，可在**授权**对话框中配置**其他终端**选项，为其他终端添加移动存储设备的权限。
- ◆ 如果审批设置为未通过或者停用设备，则该设备的权限与未授权设备权限一致。

7.2.2 设置自动授权

当在**移动存储管控**中（详情请参考[配置移动存储管理](#)）设置了禁用移动存储设备，需要开启自动审批功能，才能在终端上使用移动存储设备。设置自动审批的操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**终端管理**▶**移动存储**”进入**移动存储**页面，点击<设置>。



步骤 3. 在弹出的对话框中设置是否开启自动审批，并设置设备权限、时间策略等，点击<确定>。



7.2.3 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**终端管理**▶**移动存储**”，可进行以下操作。

- 选择需要删除的设备，点击右侧**操作项**的“**删除**”图标，在弹出的对话框中点击<确定>，即可将该移动存储设备删除。
- 勾选多个设备，点击上方的<删除>，在弹出的对话框中点击<确定>，可批量删除移动存储设备。
- 勾选需要导出的移动存储设备（可勾选多个），点击<导出列表>，即可将所选择的设备列表进行导出。



7.3 管理分组标签

对终端设置分组、标签，方便对终端进行分类管理以及对终端进行批量操作。

租户可对分组及标签进行管理，包括新增、编辑和删除等操作。同时可为终端选择分组及添加标签，详情请参考[编辑终端](#)。

- ◆ Windows 7、Windows 8、Windows 10、Windows11 等操作系统终端默认划分为 PC 组。
- ◆ Windows Server 2003、Windows Server 2008 等操作系统终端默认划分为 Windows 服务器组。
- ◆ Linux 操作系统终端默认划分为 Linux 服务器组。
- ◆ 其他的为系统默认组。

7.3.1 新增分组

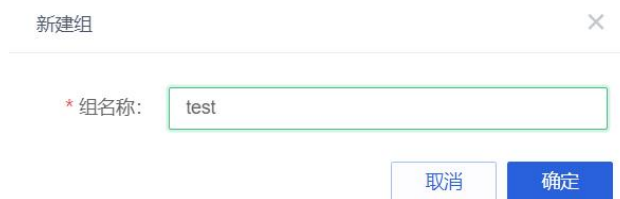
步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“终端管理>分组标签”，选择分组页签。

步骤 3. 点击<新增>。



步骤 4. 在弹出的对话框中输入组名称，点击<确定>，即可新增分组。



7.3.2 新增标签

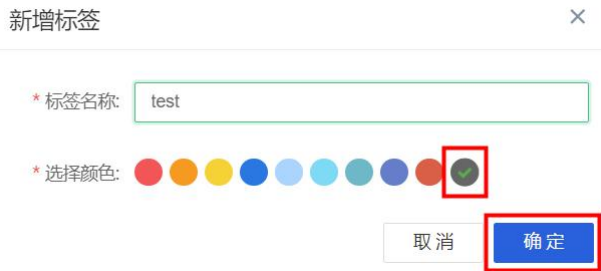
步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“终端管理>分组标签>标签”，选择标签页签。

步骤 3. 点击<新增>。



步骤 4. 在弹出的对话框中输入标签名称，选择颜色，点击<确定>，即可新增标签。

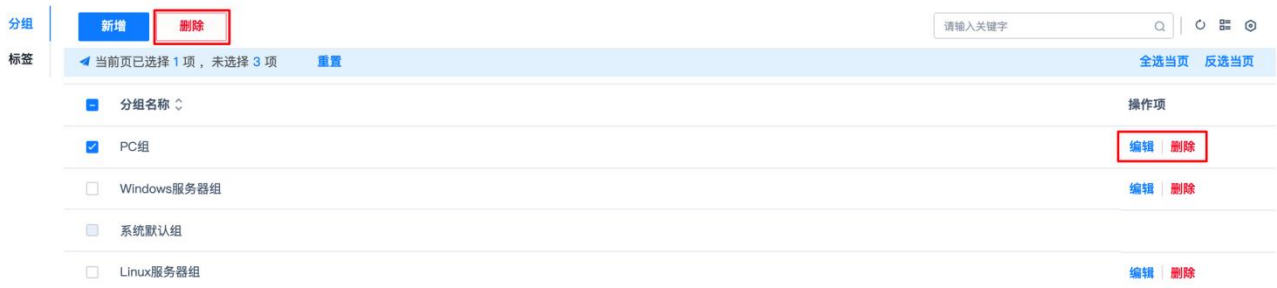


7.3.3 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台。

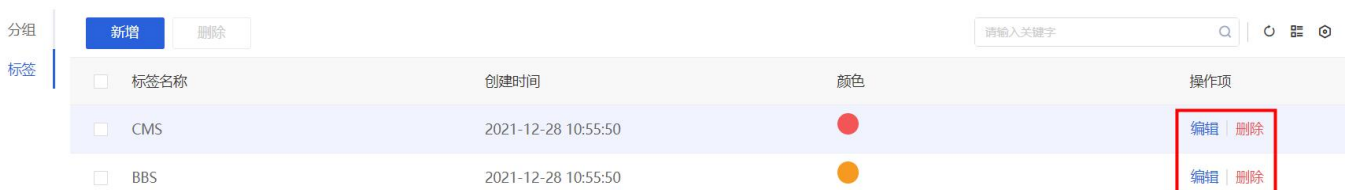
步骤 2. 在左侧导航栏选择“终端管理>分组标签”，选择分组页签，租户可在此页面对分组进行编辑及删除操作。

- 点击操作项列中的<编辑>，在弹出的对话框中修改组名称，即可编辑分组。
- 点击操作项列中的<删除>，在弹出的对话框中点击<确定>，即可删除分组。
- 勾选分组（可勾选多个），点击列表上方的<删除>，在弹出的对话框中点击<确定>，即可批量删除分组。



步骤 3. 在左侧导航栏选择“终端管理>分组标签”，选择标签页签，租户可在此页面对标签进行编辑和删除操作。

- 点击操作项列中的<编辑>，在弹出的对话框中修改标签名称和颜色，点击<确定>，即可编辑标签。
- 点击操作项列中的<删除>，在弹出的对话框中点击<确定>，即可删除标签。
- 勾选需要删除标签（可勾选多个），点击列表上方的<删除>，在弹出的对话框中点击<确定>，即可批量删除标签。



7.4 主机发现

租户可对网段内的终端进行扫描，扫描后可查看主机名、IP、MAC、设备类型、操作系统、安装版本、发

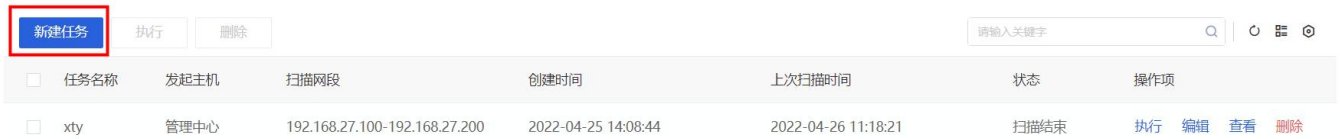
现时间。

7.4.1 新建主机发现任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“终端管理>主机发现”。

步骤 3. 点击<新建任务>。



步骤 4. 在弹出的对话框中编辑任务名称、发起主机、扫描网段，点击<确定>即可新建主机发现任务。

创建扫描任务

* 任务名称

发起主机

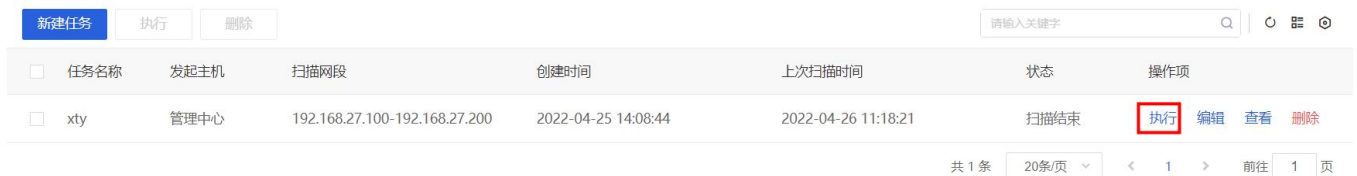
* 扫描网段

7.4.2 执行主机发现任务

支持单个执行和批量执行主机发现任务两种方式。

◆ 单个执行：

在主机发现任务列表点击操作项列中的<执行>，在弹出的对话框中点击<确定>。



◆ 批量执行：

勾选需要执行的任务（可勾选多个），点击列表上方的<执行>，在弹出的对话框中点击<确定>。



7.4.3 查看主机发现扫描结果

步骤 1. 在主机发现任务列表中点击**操作项**列中的<查看>。



任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行 查看 删除
test	管理中心	192.168.22.1-192.168.22.100	2022-08-12 10:51:46	-	-	执行 编辑 删除

步骤 2. 即可查看主机发现扫描结果，包括主机名、IP、MAC 等信息。



主机名	IP	MAC	设备类型	操作系统	安装版本	发现时间
	192.168.27.100	00:0C:29:26:11:18	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53
	192.168.27.101	00:0C:29:4E:11:18	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53
DESKTOP-8U...	192.168.22.100	00:0C:29:11:18:53	general purpose	Windows 10.0.1...	3.0.2.104	2022-04-26 11:18:53
	192.168.22.101	00:0C:29:11:18:53	general purpose	Linux 3.2 - 4.9	未安装	2022-04-26 11:18:53

7.4.4 其他操作

- ◆ 点击**操作项**列中的<编辑>，在弹出的对话框中修改相关信息，点击<确定>，即可编辑主机发现任务。
- ◆ 点击**操作项**列中的<删除>，在弹出的对话框中点击<确定>，即可删除主机发现任务。



任务名称	发起主机	扫描网段	创建时间	上次扫描时间	状态	操作项
xty	管理中心	192.168.27.100-192.168.27.200	2022-04-25 14:08:44	2022-04-26 11:18:21	扫描结束	执行 编辑 查看 删除
test	管理中心	192.168.22.1-192.168.22.100	2022-08-12 10:51:46	-	-	执行 编辑 删除

7.5 容器安全

主机安全系统可对云工作负载保护平台下的容器提供全生命周期安全管控及防护。

7.5.1 查看容器详情

步骤 1. 在左侧导航栏选择“**终端管理**▶**容器安全**”，进入容器安全页面，查看容器名称、镜像、容器 ID、容器所在终端、容器创建时间、运行状态、篡改防护状态等信息。点击**操作项**列中的“查看”图标。

刷新列表 请输入关键字

容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项
<input type="checkbox"/> mysql-test	mysql	5a55...	ubuntu	2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止
<input type="checkbox"/> gracious_robinson	mysql	b5a08...	ubuntu	2022-10-19 07:39:47	停止	未防护	查看 启动 暂停 停止

步骤 2. 可查看容器详情信息。

容器详情

容器名称: cocky_galileo

资产名称: jxq-862-176

所属分组: 系统默认组

标签:

容器ID: 810296c4c322

镜像: nginx

启动参数: "/bin/bash"

创建时间: 2020-07-13 13:18:45

状态: 运行

端口: 80/tcp

开始时间: 2020-11-10 19:23:17

结束时间: 2020-11-10 19:18:55

关闭

7.5.2 启动容器防篡改防护

点击操作项列中的<启动>，可启动对容器的防篡改防护功能。

刷新列表 请输入关键字

当前页已选择 1 项, 未选择 1 项 重置

容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项
<input checked="" type="checkbox"/> mysql-test	mysql	5a596c209c2a	ubuntu	2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止

7.5.3 暂停容器防篡改防护

点击操作项列中的<暂停>，可暂停容器防篡改防护功能。

刷新列表 请输入关键字

当前页已选择 1 项, 未选择 1 项 重置

容器名称	镜像	容器ID	终端名称	创建时间	状态	篡改防护	操作项
<input checked="" type="checkbox"/> mysql-test	mysql	5a596c209c2a	ubuntu	2022-10-19 07:40:08	停止	未防护	查看 启动 暂停 停止

7.5.4 停止容器防篡改防护

点击操作项列中的<停止>，可停止容器防篡改防护功能。

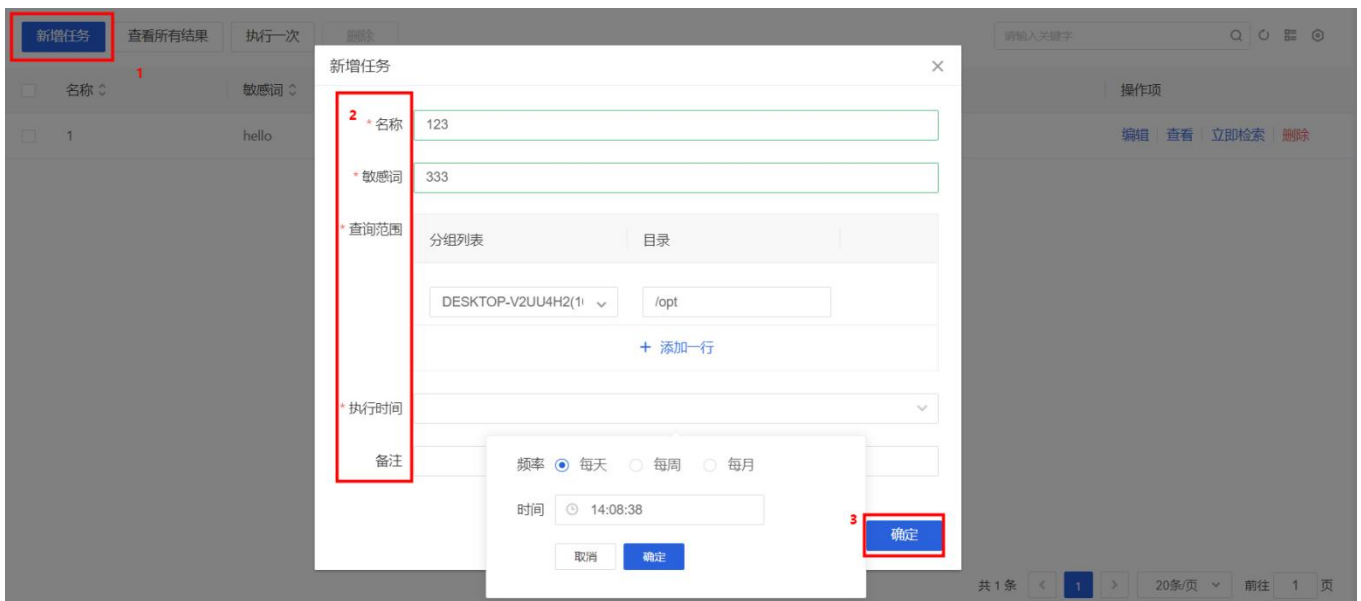


7.6 敏感词检索

主机安全系统可对资产目录下敏感词汇进行检索和统计。

7.6.1 新增任务和相关操作项

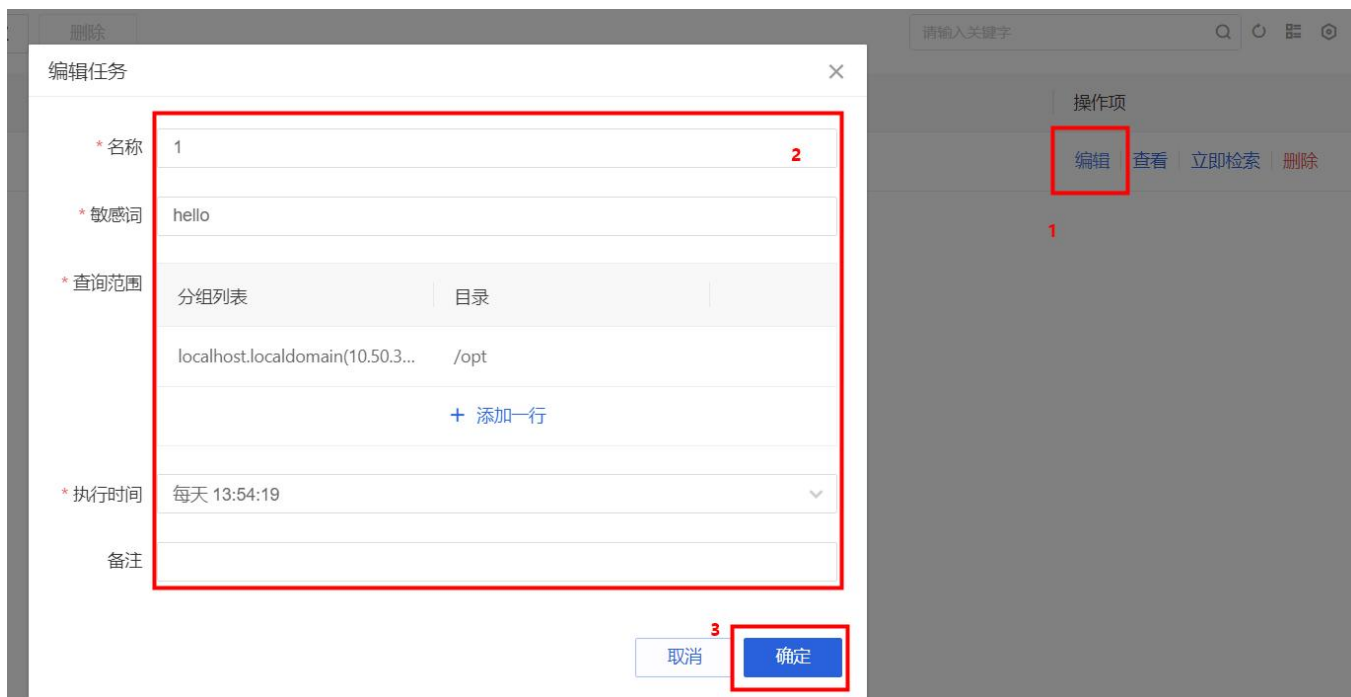
步骤 1. 在左侧导航栏选择“终端管理>敏感词检索”，进入检索页面，点击“新增任务”按钮，填写名称、敏感词、查询范围、执行时间、备注等相关信息后点击确定。



步骤 2. 可查看配置的任务详情信息。



步骤 3. 点击操作项的“编辑”按钮，编辑需要修改的相关信息后点击确定。



步骤 4. 点击操作项的“立即检索”按钮，即可对其配置任务进行敏感词检索操作。



步骤 5. 点击操作项的“查看”按钮，即可对计划执行完毕后结果进行查阅。





步骤 6. 点击操作项的“删除”按钮，即可对该计划进行删除操作。

<input checked="" type="checkbox"/>	名称	敏感词	执行时间	状态	完成时间	操作项
<input checked="" type="checkbox"/>	1	hello	每天 13:54:19	未开始	--	编辑 查看 立即检索 删除

7.6.2 其他操作项

步骤 1. 点击列表上方<查看所有结果>按钮，可对所有计划执行完毕后结果进行查阅。

<input type="checkbox"/>	名称	敏感词	执行时间	状态	完成时间	操作项
<input type="checkbox"/>	1	hello	每天 13:54:19	未开始	--	编辑 查看 立即检索 删除

步骤 2. 点击列表上方<执行一次>按钮，可启动勾选计划并执行一次操作。

<input checked="" type="checkbox"/>	名称	敏感词	执行时间	状态	完成时间	操作项
<input checked="" type="checkbox"/>	1	hello	每天 13:54:19	未开始	--	编辑 查看 立即检索 删除

步骤 3. 点击列表上方<删除>按钮，可对勾选计划执行删除操作。

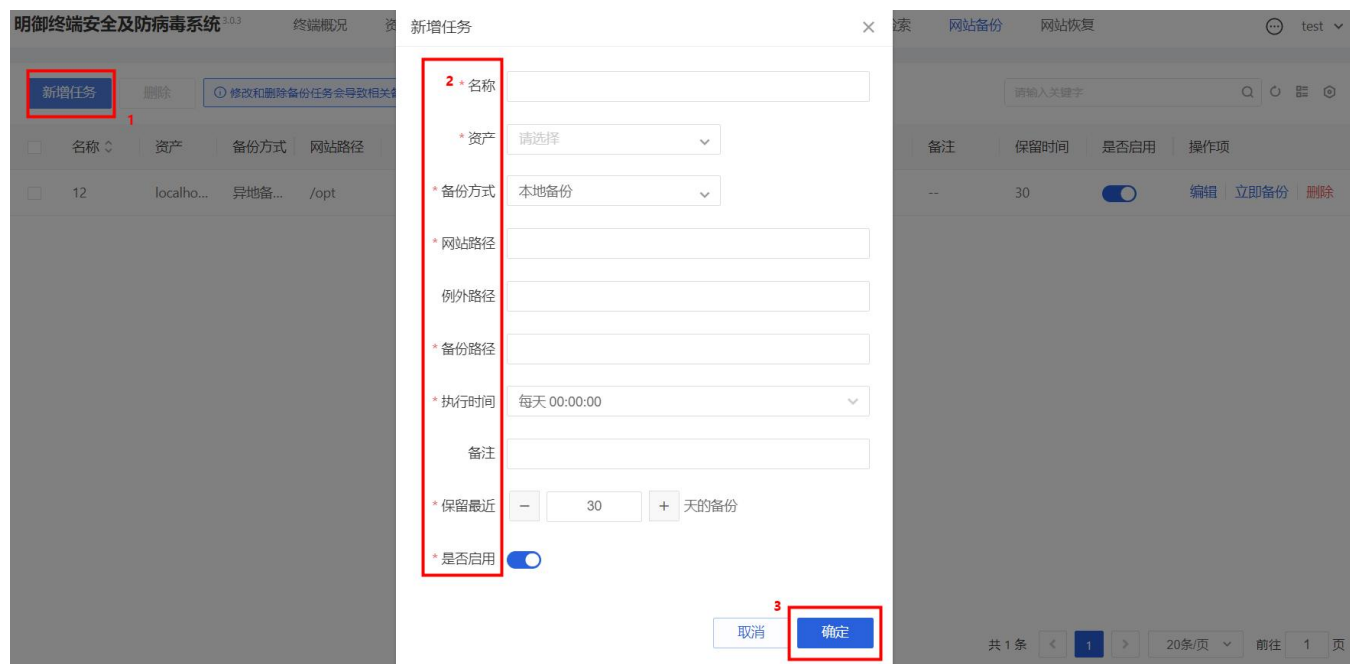
<input checked="" type="checkbox"/>	名称	敏感词	执行时间	状态	完成时间	操作项
<input checked="" type="checkbox"/>	1	hello	每天 13:54:19	未开始	--	编辑 查看 立即检索 删除

7.7 网站备份

主机安全系统可对资产提供相关目录备份服务。

7.7.1 新增任务和相关操作项

步骤 1. 在左侧导航栏选择“终端管理▶网站备份”，进入备份页面，点击“新增任务”按钮，填写名称、资产、备份方式、网站路径、例外路径等相关信息后点击**确定**。



步骤 2. 可查看配置的任务详情信息。



步骤 3. 点击操作项的“编辑”按钮，编辑需要修改的相关信息后点击**确定**。

编辑任务 ×

* 名称

* 资产

* 备份方式

* 备份服务器

* 网站路径

例外路径

* 备份路径

* 执行时间

备注

* 保留最近 天的备份

* 是否启用

步骤 4. 点击操作项的“立即备份”按钮，即可进行备份操作。

名称	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态	备注	保留时间	是否启用	操作项	
<input type="checkbox"/>	12	localho...	异地备...	/opt	DESKTOP-C...	--	/opt	每天 00:...	2022-11...	未开始	--	30	<input checked="" type="checkbox"/>	编辑 立即备份 删除

步骤 5. 点击操作项的“删除”按钮，即可对该任务进行删除操作。

名称	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态	备注	保留时间	是否启用	操作项	
<input checked="" type="checkbox"/>	12	localho...	异地备...	/opt	DESKTOP-C...	--	/opt	每天 00:...	2022-11...	未开始	--	30	<input checked="" type="checkbox"/>	编辑 <input type="button" value="立即备份"/> 删除

7.7.2 其他操作项

步骤 1. 勾选任务后点击列表上方<删除>按钮，可对勾选任务执行删除操作。

名称	资产	备份方式	网站路径	备份服务器	例外路径	备份路径	执行时间	更新时间	状态	备注	保留时间	是否启用	操作项	
<input checked="" type="checkbox"/>	12	localho...	异地备...	/opt	DESKTOP-C...	--	/opt	每天 00:...	2022-11...	未开始	--	30	<input checked="" type="checkbox"/>	编辑 <input type="button" value="立即备份"/> 删除

主机安全系统可对云工作负载保护平台下的容器提供全生命周期安全管控及防护。



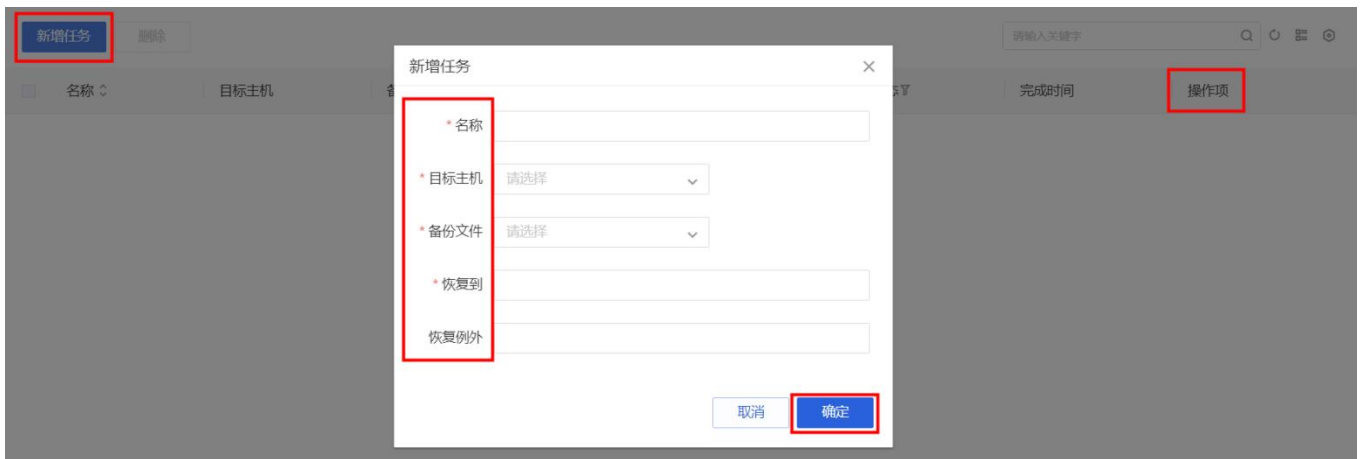
修改和删除备份任务会导致相关备份文件删除。

7.8 网站恢复

主机安全系统可对资产提供相关目录备份后恢复服务。

7.8.1 新增任务

步骤 1. 在左侧导航栏选择“**终端管理**►**网站恢复**”，进入恢复页面，点击“**新增任务**”按钮，填写名称、目标主机、备份主机、恢复到、恢复例外等相关信息后点击**确定**；点击右方**操作项**相关按钮，执行同上网站备份通理相关操作。



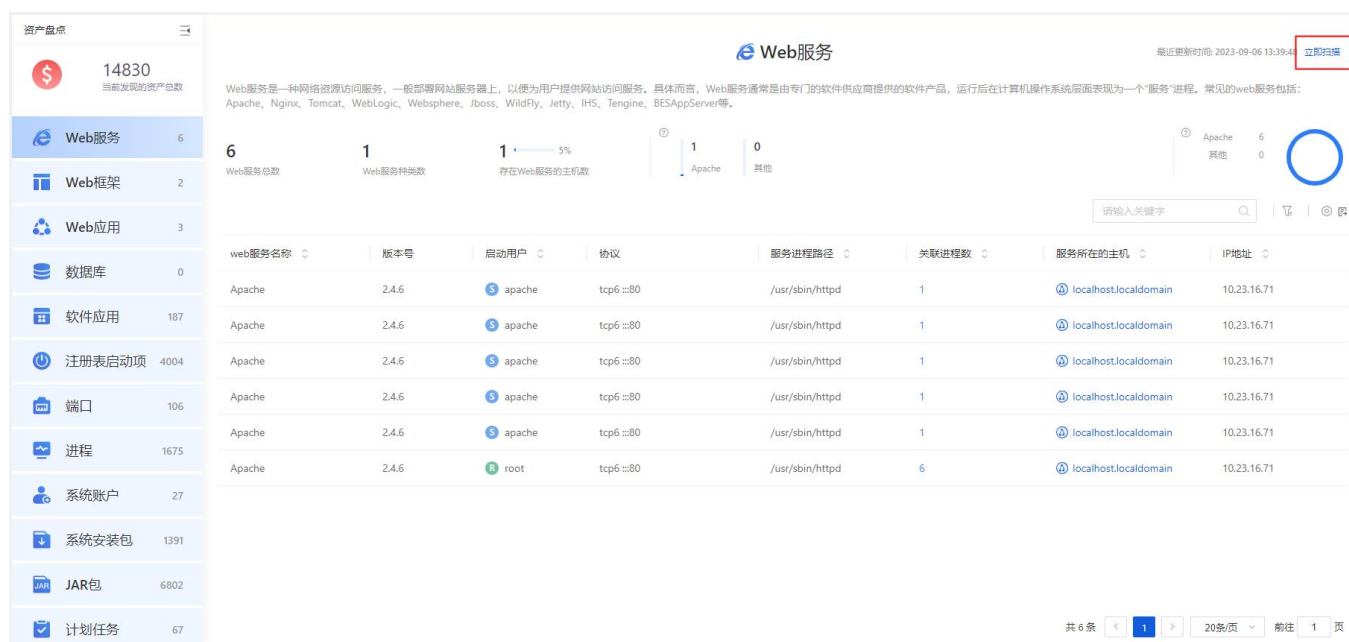
仅租户角色具有资产盘点权限。

8.1 资产盘点

租户可以通过**资产盘点**功能对资产详细情况进行盘点，包括 **WEB** 、数据库、软件、注册表、端口、进程、账户、安装包、jar 、计划任务、环境变量、内核、证书等。

8.1.1 进行资产盘点

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**资产盘点**”进入**资产盘点**页面，点击右上角“**立即扫描**”按钮即可对资产进行扫描任务下发。



The screenshot shows the 'Asset Inventory' (资产盘点) page. On the left sidebar, there is a summary of assets: 14830 total assets, with 6 Web Services (Web服务), 2 Web Frameworks (Web框架), 3 Web Applications (Web应用), 0 Databases (数据库), 187 Software Applications (软件应用), 4004 Registry Startups (注册表启动项), 106 Ports (端口), 1675 Processes (进程), 27 System Accounts (系统账户), 1391 System Install Packages (系统安装包), 6802 JAR Packages (JAR包), and 67 Scheduled Tasks (计划任务).

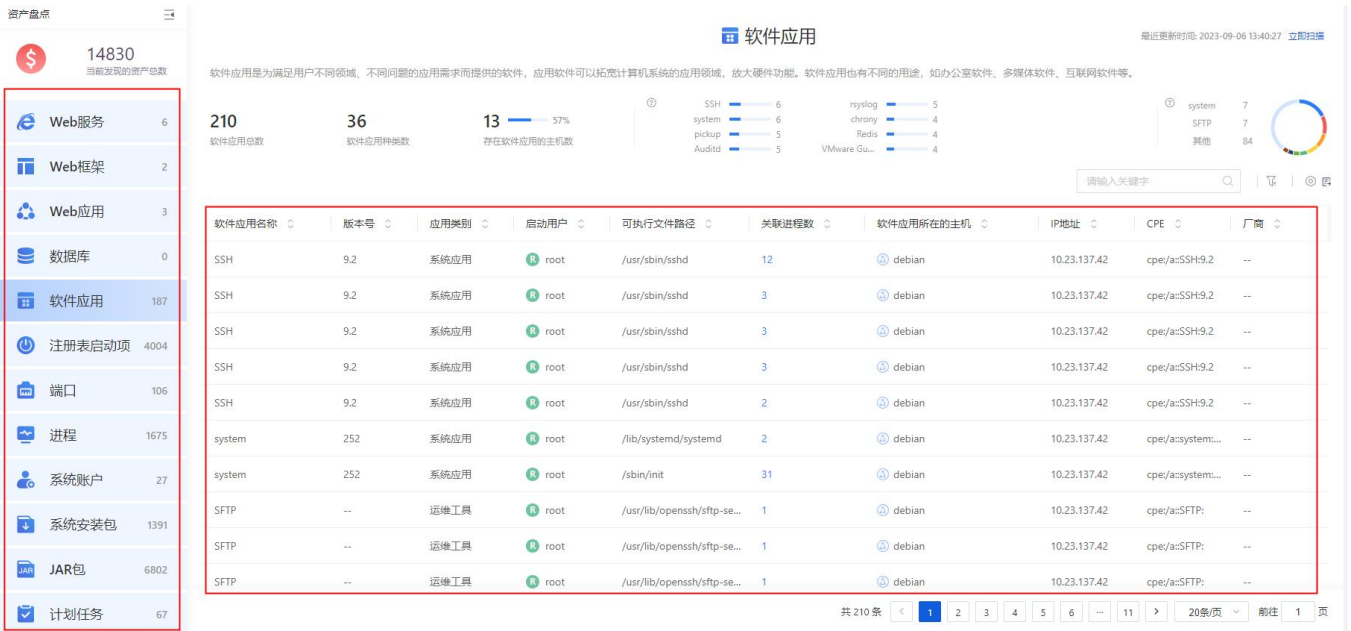
The main content area is titled 'Web Services' (Web服务). It includes a brief description: 'Web services are a type of network resource access service, deployed on website servers to provide website access services. Specifically, web services are software products provided by specialized software vendors, running on the computer operating system level as a 'service' process. Common web services include: Apache, Nginx, Tomcat, WebLogic, Websphere, Jboss, WildFly, Jetty, IHS, Tengine, BESAppServer, etc.'

Summary statistics for Web Services: 6 total services, 1 service type, 1 host with services (5%), 1 Apache instance, and 0 other instances.

web服务名称	版本号	启动用户	协议	服务进程路径	关联进程数	服务所在的主机	IP地址
Apache	2.4.6	apache	tcp6 ::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
Apache	2.4.6	apache	tcp6 ::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
Apache	2.4.6	apache	tcp6 ::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
Apache	2.4.6	apache	tcp6 ::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
Apache	2.4.6	apache	tcp6 ::80	/usr/sbin/httpd	1	localhost.localdomain	10.23.16.71
Apache	2.4.6	root	tcp6 ::80	/usr/sbin/httpd	6	localhost.localdomain	10.23.16.71

At the bottom right, it shows '共 6 条' (Total 6 items) and '20条/页' (20 items per page).

步骤 2. 进入**资产盘点**页面，即可查看所有主机的相关 **WEB** 、数据库、软件、注册表、端口、进程、账户、安装包、jar 、计划任务、环境变量、内核、证书等信息。



资产盘点说明如下。

终端信息	说明
端口	对终端上端口情况进行实时监控。
进程	对终端上进程运行情况进行实时监控，并支持远程结束相关进程。
系统账户	对终端上所有账号信息进行统计。
软件应用	对终端上运行的软件应用信息进行统计。
注册表启动项	对终端上所有的注册表启动项进行统计和管理。
Web 框架	对终端上运行的 Web 框架进行统计。
Web 服务	对终端上运行的 Web 服务进行统计。
数据库	对终端上运行的数据库进行统计。
Web 应用	对终端上运行的 Web 应用进行统计。
系统安装包	对终端安装包名、版本号、类型、安装包路径、安装时间等进行统计。
Jar 包	对终端安装所关联的 jar 包进行统计。
计划任务	对终端被制定了哪些计划任务进行统计。
环境变量	对终端的环境变量进行统计。
内核模块	对终端内核模块名称、版本号、模块路径和大小、模块依赖等进行统计。
Windows 证书	对 Win 终端的证书进行统计。

仅租户角色具有终端管理权限。

9.1 查杀病毒

用户可在**病毒查杀**页面查看所有终端的病毒查杀情况，并支持以终端视角和病毒视角对病毒进行查杀。

- ◆ 支持对所有终端批量进行病毒扫描（快速扫描/全盘扫描/自定义扫描）、停止扫描、处理病毒。
- ◆ 支持设置单个终端信任区和模板化设置信任名单，并可查看单个终端的病毒查杀详情。
- ◆ 支持查杀设置，包括查杀模式（极速模式、低资源占用模式）、多引擎设置（默认引擎、深度扫描引擎）、压缩包扫描设置及处理方式等。
- ◆ 支持扫描后导出病毒查杀的结果报告。

9.1.1 终端视角

9.1.1.1 扫描终端

扫描终端支持快速扫描、全盘扫描、自定义扫描及停止扫描等操作。

9.1.1.1.1 快速扫描

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择**终端视角**页签。

步骤 2. 勾选需要扫描的终端（可勾选多个），点击<快速扫描>。



步骤 3. 在弹出的对话框中点击<确定>，即可对终端进行快速扫描。



9.1.1.1.2 全盘扫描

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择**终端视角**页签。

步骤 2. 勾选需要扫描的终端（可勾选多个），点击<全盘扫描>。



步骤 3. 在弹出的对话框中点击<确定>，即可对终端进行全盘扫描。



9.1.1.1.3 自定义扫描

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

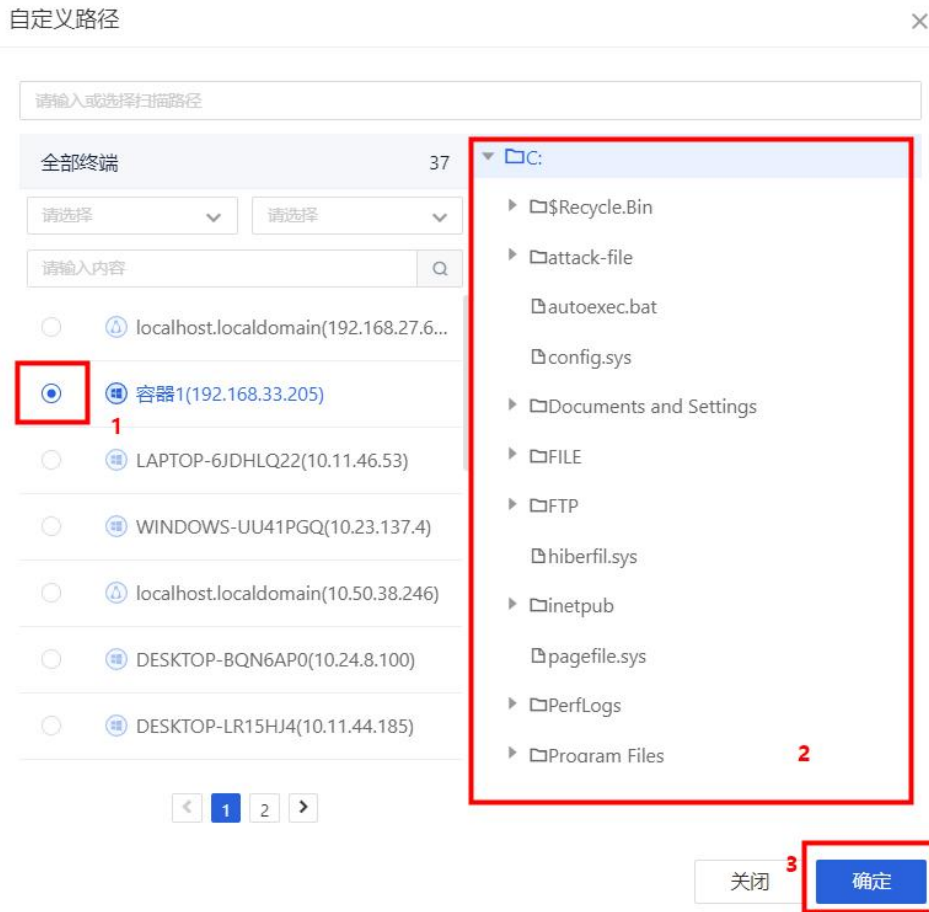
步骤 2. 勾选需要扫描的终端（可勾选多个），点击<自定义扫描>。



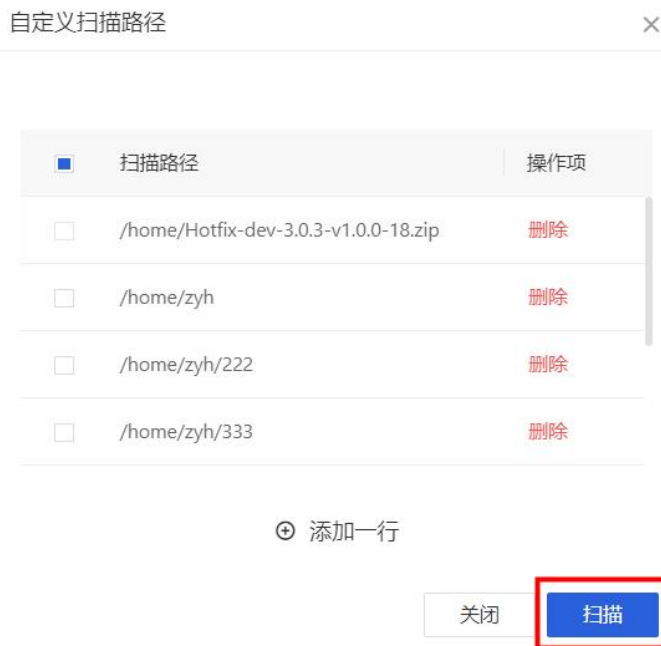
步骤 3. 在弹出的对话框中点击<添加一行>，新增扫描路径。



步骤 4. 选择终端，再选择需要扫描的路径，点击<确定>，即可新增自定义扫描路径。



步骤 5. 点击<扫描>，即可进行自定义扫描。



9.1.1.1.4 停止扫描

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

步骤 2. 勾选正在扫描的终端（可勾选多个），将光标移至**更多**，在弹出的下拉框选择“**停止扫描**”。



步骤 3. 在弹出的对话框中点击<**确定**>，即可停止终端病毒扫描。



9.1.1.2 查看扫描结果

租户可查看单个终端扫描结果，并可对扫描结果进行添加信任、处理病毒或重新扫描操作。

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**风险评估>病毒查杀**”，选择**终端视角**页签。

步骤 2. 选择需要查看的终端，点击右侧**操作项**的“**查看**”图标。



步骤 3. 进入**病毒查杀**页面，点击<**查看扫描结果**>。

租户也可在此页面进行终端扫描、查看隔离区、查看信任区操作。



步骤 4. 进入扫描结果页面，可在此页面查看详细病毒木马文件，支持以下操作。

- ◆ 勾选多个病毒木马文件后点击<**信任**>或<**处理**>，可对文件进行批量添加信任区或批量处理操作。
- ◆ 点击<**处理所有**>，可一键处理所有病毒木马文件。
- ◆ 点击<**立即处理**>，可对病毒文件进行处理。
- ◆ 点击<**重新扫描**>，在弹出的对话框中设置扫描路径，点击<**确定**>可重新对终端进行病毒扫描。



共扫描 54206个文件，发现 938个病毒木马文件
扫描时间：2022-06-16 09:45:49

[立即处理](#) [重新扫描](#)

文件路径	病毒名称
<input checked="" type="checkbox"/> 病毒木马文件2/938 信任 处理 处理所有	
<input checked="" type="checkbox"/> /root/aspx/nishang/Utility/Add-Persistence.ps1	HackTool/PS.Nishang
<input checked="" type="checkbox"/> /root/aspx/nishang/Utility/Invoke-Encode.ps1	Backdoor/Meterpreter.q
<input type="checkbox"/> /root/aspx/nishang/Utility/Base64ToString.ps1	HackTool/PS.Nishang
<input type="checkbox"/> /root/aspx/nishang/Utility/Download.ps1	HackTool/PS.Nishang

9.1.1.3 处理病毒

租户可对已扫描出的病毒文件进行处理，处理后的文件会被放至隔离区。

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

步骤 2. 勾选需要处理病毒的终端（可勾选多个），点击<处理病毒>。



步骤 3. 在弹出的对话框中点击<确定>，即可对该终端病毒进行处理。处理完成后，租户可对隔离区文件进行恢复及删除操作。



9.1.1.4 导出报告

租户可导出病毒扫描结果报告。

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

步骤 2. 将光标移至更多，在弹出的下拉框选择“导出报告”，即可将所有终端的病毒扫描报告导出至本地。

勾选终端（可勾选多个），点击<导出报告>，可将所勾选的终端病毒扫描报告导出至本地。



9.1.1.5 升级病毒库

可升级终端上的病毒库，方便租户查杀最新的病毒。操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**风险管理**▶**病毒查杀**”，选择**终端视角**页签。

步骤 2. 勾选需要升级病毒库的终端（可勾选多个），将光标移至**更多**，在弹出的菜单栏中选择“**升级病毒库**”，即可升级所勾选终端上的病毒库。



◆ 列表中“病毒库版本”支持排序，支持模糊匹配搜索。

9.1.1.6 设置查杀模式

租户可进行自定义病毒查杀模式，包括扫描模式、多引擎设置、压缩包查杀设置及处理方式等。

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**风险管理**▶**病毒查杀**”，选择**终端视角**页签。

步骤 2. 点击<**查杀设置**>对所有终端设置查杀模式。

选择多个终端后点击<**查杀设置**>，可对终端病毒查杀模式进行批量设置。



步骤 3. 在弹出的对话框中设置查杀模式，点击<**确定**>即可设置成功。



详细配置请参见下表。

配置项	说明
扫描模式	<ul style="list-style-type: none"> ◆ 极速扫描：根据系统硬件配置，自适应扫描速度，对低配主机性能有一定影响。 ◆ 低资源占用：限制扫描时 CPU 使用率低于设置值，仅适用于 Linux 系统主机。
多引擎设置	<ul style="list-style-type: none"> ◆ 默认引擎：高性能跨平台通用病毒扫描引擎，建议开启。 ◆ 深度扫描引擎：开启后将占用 200MB 磁盘空间，深度扫描引擎占用内存更多，但扫描速度更快（进行压缩包扫描时需要选择“深度扫描引擎”）。
压缩包扫描设置	设置压缩包的扫描深度，对大于设置值的压缩包不扫描。
处理方式	对病毒文件的处理方式： <ul style="list-style-type: none"> ◆ 自动处理：优先修复并恢复文件，如修复失败则隔离病毒文件。 ◆ 由用户自行选择：由用户自行选择病毒文件的处理方式。 ◆ 删除：删除病毒文件。

9.1.1.7 其他操作

租户可查看病毒查杀的病毒详情，并支持对隔离区和信任区进行添加及删除操作。

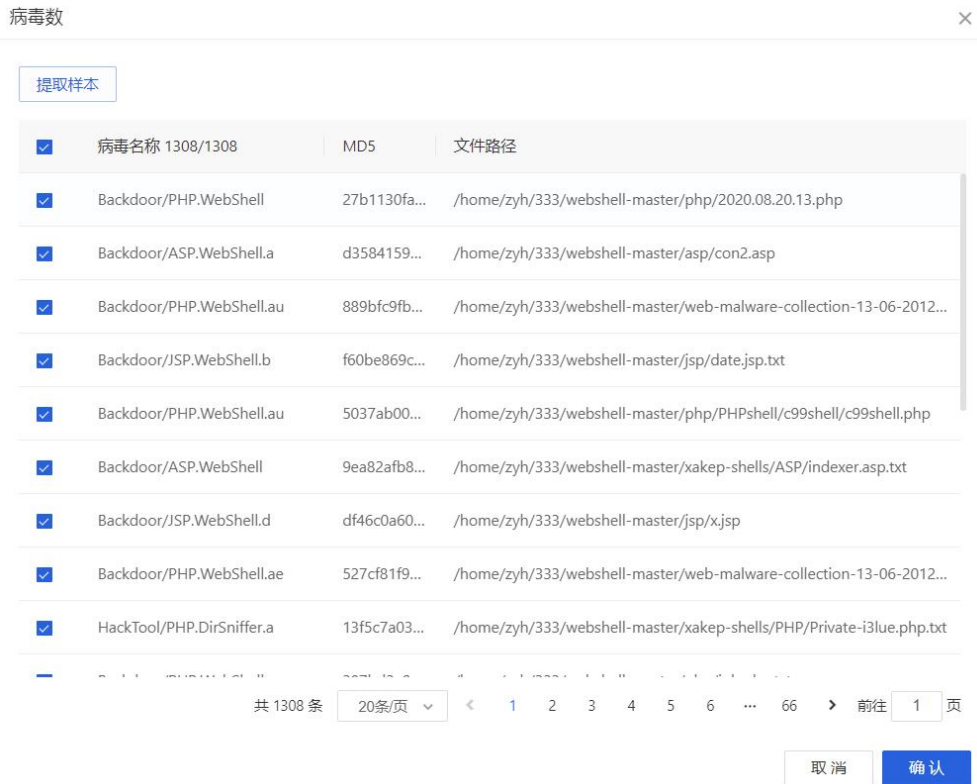
9.1.1.7.1 查看病毒详情

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

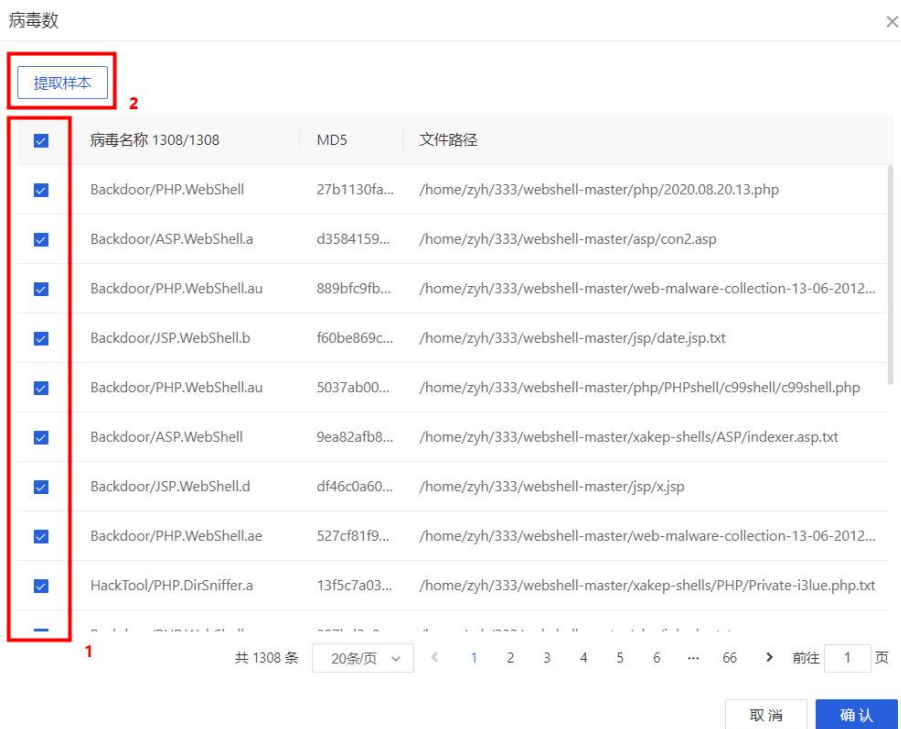
步骤 2. 点击待处理病毒数。



步骤 3. 在弹出的对话框中查看病毒的名称、MD5 值及文件路径。



步骤 4. 勾选病毒文件（可勾选多个），点击<提取样本>，即可下载病毒文件至本地。



9.1.1.7.2 处理隔离区中的文件

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>病毒查杀”，选择终端视角页签。

步骤 2. 点击操作项列中的<隔离区>。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>病毒查杀”，选择病毒视角页签。

步骤 3. 选择需要处理的病毒，点击右侧操作项的“立即处理”图标，即可对该病毒进行处理。

MD5值	病毒名称	已影响终端数	首次发现时间	首次发现终端	操作项
--	Backdoor/Meterpreter.q	3	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
01227ed2792dae420c158f5c3d8cb0a	HEUR:Backdoor/ASP.WebShell.a	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
0152de452f92423829e041af2d783e3f	Backdoor/ASPK.WebShell	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
0176c418103f6acf9b0845429abb52	Backdoor/PHP.WebShell.h	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
02e8597a4ddade7b69f6fa546ebfe170	Backdoor/Agent.jz	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0396bb6a40674c40fb260aa80525c86f	Backdoor/PHP.WebShell.aj	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
03b06b4183cb9947ccda2c3d636406d4	Trojan/GenericD2D6A525789210DD	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0421445303cfd0ec6b20b384630ff0	Backdoor/PHP.B374k.b	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0477aac059f4f125816e25b207ae50c4	Trojan/Generic2981D80C24C5E222	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录

◆ 方式二：批量处理

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>病毒查杀”，选择病毒视角页签。

步骤 3. 选中需要处理的病毒，点击病毒列表上方的<处理病毒>，即可对所选病毒进行处理。

MD5值	病毒名称	已影响终端数	首次发现时间	首次发现终端	操作项
--	Backdoor/Meterpreter.q	3	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
01227ed2792dae420c158f5c3d8cb0a	HEUR:Backdoor/ASP.WebShell.a	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
0152de452f92423829e041af2d783e3f	Backdoor/ASPK.WebShell	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
0176c418103f6acf9b0845429abb52	Backdoor/PHP.WebShell.h	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
02e8597a4ddade7b69f6fa546ebfe170	Backdoor/Agent.jz	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0396bb6a40674c40fb260aa80525c86f	Backdoor/PHP.WebShell.aj	2	2022-11-16 1...	CentOS7	立即处理 查看 删除记录
03b06b4183cb9947ccda2c3d636406d4	Trojan/GenericD2D6A525789210DD	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录

9.1.2.2 查看病毒详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>病毒查杀”，选择病毒视角页签。

步骤 3. 选择需要查看的病毒，点击右侧操作项的“查看”图标。

MD5值	病毒名称	已影响终端数	首次发现时间	首次发现终端	操作项
--	Backdoor/Meterpreter.q	3	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
0061d800aee63ccaf41d2d62ec15985d	Backdoor/ASP.Ace.b	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录
00898cbc3a95544865c6ef3f6dba7506	Backdoor/PHP.WebShell.h	2	2022-06-16 1...	centos5.0-x64-2...	立即处理 查看 删除记录

步骤 4. 即可查看该病毒的详细信息。包括终端名称、病毒路径、发现时间、发现方式及处理结果。

终端名称	病毒路径	发现时间	发现方式	处理结果
centos5.0-x64-2.6.18-8	/root/aspw/nishang/Utility/Invoke-Encode.ps1	2022-06-16 10:12:36	主动扫描	已删除
centos5.0-x64-2.6.18-8	/root/aspw/nishang/Utility/Add-Persistence.ps1	2022-06-16 10:12:36	主动扫描	已删除
ADMIN-PC	[HKLM\System\CurrentControlSet\Services\...]...	2022-09-22 16:36:54	主动扫描	未处理
WIN-8ONSPKIA4B1	[HKLM\System\CurrentControlSet\Services\...]...	2022-09-23 09:49:18	主动扫描	未处理
容器1	[HKLM\System\CurrentControlSet\Services\...]...	2022-10-12 14:20:15	主动扫描	未处理
容器1	[HKLM\System\CurrentControlSet\Services\...]...	2022-10-27 00:34:46	主动扫描	未处理
容器1	c:\windows\mssecsvr.exe	2022-10-27 00:34:46	主动扫描	已删除
容器1	c:\windows\mssecsvc.exe	2022-10-27 00:34:46	主动扫描	已删除
容器1	[HKLM\System\CurrentControlSet\Services\...]...	2022-10-27 00:34:46	主动扫描	未处理

9.1.2.3 删除记录

◆ 方式一：单个删除

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>病毒查杀”，选择病毒视角页签。

步骤 3. 选择需要删除记录的病毒，点击右侧操作项的“删除记录”图标。

步骤 4. 在弹出的对话框中点击<确定>，即可删除该条病毒记录。



◆ 方式二：批量删除

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>病毒查杀”，选择病毒视角页签。

步骤 3. 勾选需要处理的病毒，点击病毒列表上方的<删除记录>。



步骤 4. 在弹出的对话框中点击<确定>，即可删除所勾选的病毒文件记录。



你确定要删除所选记录吗?

取消

确定

9.2 网马查杀

租户可在**网马查杀**页面查看所有终端的网马查杀情况。

- ◆ 支持对所有终端批量进行网马扫描、停止扫描、处理网马。
- ◆ 支持设置单个终端信任区和模板化管理信任名单，并可查看单个终端的网马查杀页面。
- ◆ 支持查杀设置，可进行扫描完成后自动处理。
- ◆ 支持通过路径配置对 Web 应用目录进行深入检测，并对扫描出的风险文件进行立即隔离、添加信任区或删除操作。
- ◆ 支持扫描后导出网马查杀的结果报告。

9.2.1 扫描终端的网马

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择“**风险管理**▶**网马查杀**”，勾选需要扫描的终端（可勾选多个），点击<开始扫描>。

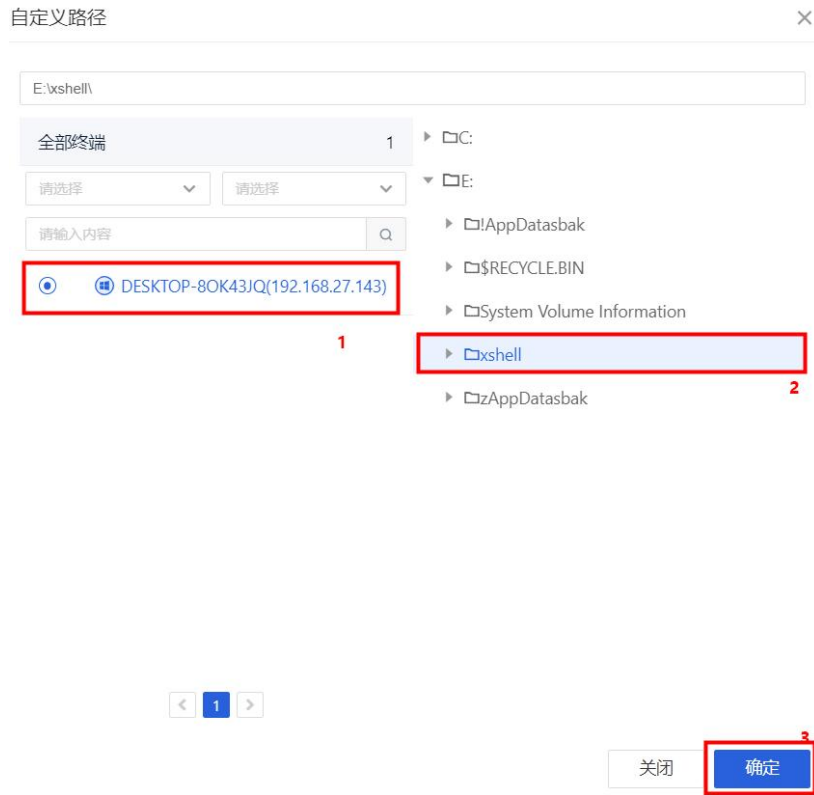


步骤 3. 在弹出的对话框中自定义扫描路径。

点击<添加一行>，新增自定义扫描路径。



步骤 4. 选择终端，选择路径，点击<确定>，即可新增自定义路径。



步骤 5. 勾选需要扫描的自定义路径，点击<扫描>，即可对该路径进行扫描。



步骤 6. 勾选正在扫描的终端（勾选多个），点击<停止扫描>，在弹出的对话框中点击<确定>，即可停止终端网马扫描操作。



提示

×

是否确定处理选中网马?

取消

确定

9.2.4 导出报告

租户可导出网马扫描结果报告。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择“风险评估>网马查杀”，选择终端后点击<导出报告>，可将所选中的终端网马扫描报告导出至本地。

点击<导出报告>，导出所有终端的网马扫描报告。



9.2.5 设置查杀模式

租户可进行自定义病毒查杀模式，包括扫描模式、多引擎设置、网马引擎及处理方式等。

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“风险评估>网马查杀”，点击<查杀设置>。



步骤 2. 在弹出的对话框中编辑相关信息，点击<确定>即可对所有终端设置网马查杀模式。

勾选终端后点击<查杀设置>，可对被勾选终端设置网马查杀模式。

扫描模式: 极速扫描
 根据系统硬件配置, 自适应扫描速度, 对低配主机性能有一定影响

低资源占用, CPU使用率低于 %
 CPU使用率限制设置仅支持Linux系统, Windows通过 智能检测优化各项系统资源占用

多引擎设置: 默认引擎
 高性能跨平台通用引擎

深度扫描引擎
 开启后将占用200MB磁盘空间

网马引擎: 网马专用引擎, 根据网马特征扫描

处理方式: 自动处理 (网马文件隔离到隔离区)
 由用户自行选择
 删除

取消

确定

9.2.6 相关操作

租户可查看网马查杀详情, 并支持对隔离区和信任区进行添加及删除操作。

9.2.6.1 查看网马详情

步骤 1. 以租户角色登录主机安全系统管理平台, 在左侧导航栏选择“风险评估>网马查杀”进入网马查杀页面。

步骤 2. 点击网马数。

终端名称	所属分组	标签	IP地址	网马数	隔离区	信任区	上次扫描时间	状态	操作项
DESKTOP-80K43JQ	PC组		192.168.27.143	62/62	--	--	2022-11-11 16:18:41	--	查看

步骤 3. 在弹出的对话框中查看网马详情, 包括网马名称及文件路径。

网马描述 ×

提取样本

<input checked="" type="checkbox"/>	网马名称 62/62	文件路径
<input checked="" type="checkbox"/>	Worm/Xbash.a	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\9R9 GGOYE\Xbash\31155bf8c85c6c6193842b8d09bda88990d710db9f70efe8 5c421f1484f0ee78
<input checked="" type="checkbox"/>	HVM:Trojan/Swrort.gen!A	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\9R9 GGOYE\VegaLocker\8370b5aaf5d21fdfe7052c90b1e6b8fd3e0fa0bc2600 7badd416b1d4a99bc3cd
<input checked="" type="checkbox"/>	Ransom/LockFile.fe	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\9R9 GGOYE\CryptoMix\cadb8633e114f4b91b9b394878231c780bb305939f2 b2a84b0e0f7b3b464f164
<input checked="" type="checkbox"/>	SVM:TrojanDownloader/JS.Nem ucod.x	C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\9R9 GGOYE\Locky\2504b1f2bdd2839c9c68a29cf9ca9d831234da473a4b4e1 05471523b4981b6a

共 62 条 < 1 2 3 4 > 前往 页

9.2.6.2 管理隔离区中的网马文件

步骤 1. 以租户角色登录主机安全系统管理平台，在左侧导航栏选择“风险评估>网马查杀”，点击隔离区列中的数字。

开始扫描 处理网马 停止扫描 导出报告 查杀设置

共 1 项, 已选择 1 项 全选当页 反选当页 重置

<input checked="" type="checkbox"/>	终端名称	所属分组	标签	IP地址	网马数	隔离区	信任区	上次扫描时间	状态	操作项
<input checked="" type="checkbox"/>	DESKTOP-80K43IQ	PC组		192.168.27.143	61/61	1	--	2022-11-11 16:18:41	处理完成	查看

步骤 2. 进入隔离区页面，可对隔离区中的网马文件进行处理。

- 点击操作项列中的“恢复”图标，在弹出的对话框中点击<确定>，可将此网马文件从隔离区恢复至原始路径。
- 点击操作项列中的“删除”图标，在弹出的对话框中点击<确定>，可删除此网马文件。
- 勾选需要恢复的网马文件（可勾选多个），点击<恢复>，在弹出的对话框中点击<确定>，可将网马文件从隔离区恢复至原始路径。
- 勾选需要删除网马文件（可勾选多个），点击<删除>，在弹出的对话框中点击<确定>，可删除选择的网马文件。
- 点击<恢复全部>，在弹出的对话框中点击<确定>，可将所有网马文件从隔离区恢复至原始路径。
- 点击<删除全部>，在弹出的对话框中点击<确定>，可删除所有网马文件。
- 勾选需要提取样本的网马文件（可勾选多个），点击<提取样本>，即下载网马文件至本地。

恢复全部 删除全部 恢复 删除 提取样本				🔍 📄 🔄
文件路径	网马名称	隔离时间	操作项	
C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\S...	Trojan/VBS.Obfuscated.aa	2022-11-23 13:37:36	恢复 删除	

9.2.6.3 配置信任区

步骤 1. 以租户角色登录主机安全系统管理平台，在左侧导航栏选择“风险评估>网马查杀”，点击信任区列中的数字。

🔍 共 1 项, 已选择 1 项 全选当页 反选当页 重置									
终端名称	所属分组	标签	IP地址	网马数	隔离区	信任区	上次扫描时间	状态	操作项
DESKTOP-8OK43JQ	PC组		192.168.27.143	60/60	1	1	2022-11-11 16:18:41	处理完成	查看

步骤 2. 进入信任区页面，租户可对信任项目进行添加及删除操作。

- 点击<添加>，在弹出的对话框中选择路径，点击<确定>，即可将该路径添加至信任区。
- 勾选信任项目，点击<删除>，在弹出的对话框中点击<确定>，即可删除勾选的信任项目。

添加 删除			🔍 📄 🔄
信任项目	项目类型	操作项	
C:\\$Recycle.Bin\S-1-5-21-126391924-2324691504-621118410-1001\S9GGOVE\Angler\9c39e004e3fbd7b8d...	文件	删除	

9.3 漏洞管理

租户可在漏洞管理页面查看所有终端的漏洞扫描情况，支持的漏洞类型包括但不限于操作系统漏洞（Windows、Linux 等）、数据库漏洞（MySQL 等）、Web 容器漏洞（Tomcat、Apache、Nginx 等）、其他组件漏洞。在查看漏洞扫描情况时，默认进入管理界面时会触发一次扫描。

租户还可对所有终端进行批量 Windows 漏洞修复。带  图标的漏洞补丁表示管理中心已下载该补丁，可直接修复；白色盾牌表漏洞补丁表示管理中心尚未下载该补丁。

Windows系统漏洞 Linux系统漏洞 Windows应用漏洞 Linux应用漏洞									
终端视角 漏洞视角					扫描漏洞 修复漏洞 停止修复 导出				
<input type="text" value="请输入关键字"/> 🔍 📄 🔄									
终端名称	操作系统	IP地址	高危漏洞	可选漏洞	上次扫描时间	上次修复时间	状态	操作项	
DESKTOP-8OK43JQ	Windows 10 64-bit	192.168.27.143	0/0	0/0	2022-11-23 13:41:17	--	扫描完成	查看	



补丁修复存在一定风险，需测试后再进行修复，以免对正常业务造成影响。

9.3.1 Windows 系统漏洞

租户可对 Windows 系统漏洞进行扫描、修复、停止修复、查看扫描结果、导出扫描结果及重启终端操作。

9.3.1.1 终端视角

9.3.1.1.1 扫描终端漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择终端视角页签。

步骤 3. 勾选需要扫描的终端（可勾选多个），点击<扫描漏洞>。



步骤 4. 在弹出的对话框中点击<确定>，即可对勾选的终端进行漏洞扫描。



9.3.1.1.2 查看扫描结果

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择终端视角页签。

步骤 3. 选择需要查看的终端，点击右侧操作项的“查看”图标。



步骤 4. 系统进行终端自动扫描，扫描结束后进入漏洞扫描结果页面。租户可在此页面查看详细漏洞扫描信息，并对终端漏洞进行修复、重新扫描、忽略漏洞及查看漏洞详情操作。

- 勾选多个漏洞，点击<一键修复>，可对漏洞进行批量修复。
- 将光标悬停至漏洞，点击<修复>，可修复该漏洞。
- 将光标悬停至漏洞，点击<忽略>，可忽略该漏洞。
- 将光标悬停至漏洞，点击<详情>，可查看漏洞补丁详情。



9.3.1.1.3 修复终端漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择终端视角页签。

步骤 3. 勾选需要修复漏洞的终端（可勾选多个），点击<修复漏洞>。



步骤 4. 在弹出的对话框中点击<确定>，即可修复所勾选终端的漏洞。



对于正在修复漏洞的终端，用户可进行停止修复操作。

1) 勾选正在修复漏洞的终端（可勾选多个），点击<停止修复>。



2) 在弹出的对话框中点击<确定>，即可停止修复漏洞。



9.3.1.1.4 导出报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择终端视角页签。

步骤 3. 点击<导出>，即可将所有终端的漏洞报告导出至本地。

勾选终端（可勾选多个）点击<导出>，可将所选中的终端的漏洞扫描报告导出至本地。



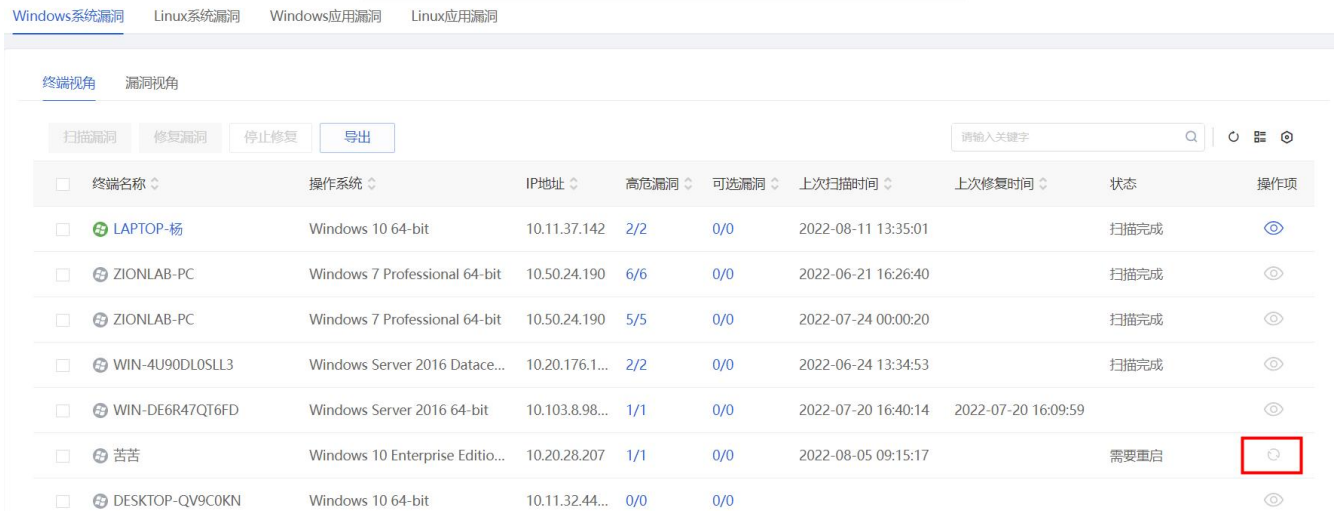
9.3.1.1.5 重启终端

对于已进行漏洞修复的终端，需进行重启操作才能使漏洞修复生效。操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择终端视角页签。

步骤 3. 选择需要重启的终端，点击右侧操作项的“重启”图标，在弹出的对话框中点击<确定>，即可重启该终端。



9.3.1.2 漏洞视角

9.3.1.2.1 修复终端漏洞

◆ 方式一：单个修复

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择漏洞视角页签。

步骤 3. 进入漏洞列表页面，选择需要修复的漏洞，点击右侧操作项的“修复”图标。



步骤 4. 在弹出的对话框中点击<确定>，即可对漏洞进行修复。



◆ 方式二：批量修复

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择漏洞视角页签。

步骤 3. 勾选需要修复的漏洞，点击列表上方的<修复>。



步骤 4. 在弹出的对话框中点击<确定>，即可对漏洞进行批量修复。



9.3.1.2.2 导出报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 系统漏洞”，选择漏洞视角页签。

步骤 3. 点击<导出>，即可将所有 Windows 系统终端的漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所勾选的终端的漏洞扫描报告导出至本地。



9.3.2 Linux 系统漏洞

租户可对 Linux 系统漏洞进行扫描及查看漏洞详情操作。



◆ linux 系统漏洞、应用漏洞扫描结果基于 CVE 编号聚合。

9.3.2.1 终端视角

9.3.2.1.1 扫描终端漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 系统漏洞”，选择终端视角页签。

步骤 3. 勾选需要扫描的终端（可勾选多个），点击<开始扫描>。



步骤 4. 在弹出的对话框中点击<确定>，即可对终端进行漏洞扫描。

提示



确定要开始扫描吗？

取消

确定

9.3.2.1.2 导出报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险管理>漏洞管理>Linux 系统漏洞”，选择终端视角页签。

步骤 3. 点击<导出>，即可将所有 Linux 系统终端的漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选中的终端漏洞报告导出至本地。



◆ 导出报告格式为 csv。

9.3.2.1.3 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 系统漏洞”，选择终端视角页签。选择需要查看的漏洞类型，点击漏洞数字。

终端名称	操作系统	IP地址	致命漏洞	高危漏洞	中危漏洞	低危漏洞	上次扫描时间	状态
localhost.localdom...	CentOS Linux 7 (Core)	192.168.27.141	15	276	357	18	2022-11-23 14:43:04	扫描完成

步骤 3. 在弹出的对话框中查看漏洞详情（可切换漏洞等级），包括 CVE 编号、漏洞名称以及处理建议。

漏洞描述 ×

致命漏洞
高危漏洞
中危漏洞
低危漏洞

CVE	漏洞名称	处理建议	产品
CVE-2019-14901	Linux kernel Marvell WiFi chip driver 缓冲区错误漏洞(centos)(CVE-2019-14901)	目前厂商已发布升级补丁以修复漏洞...	
CVE-2019-16746	Linux kernel 缓冲区错误漏洞(centos)(CVE-2019-16746)	目前厂商已发布升级补丁以修复漏洞...	
CVE-2019-17133	Linux kernel 缓冲区错误漏洞(centos)(CVE-2019-17133)	目前厂商暂未发布修复措施解决此安...	
CVE-2019-14895	Linux kernel Marvell WiFi chip driver 缓冲区错误漏洞(centos)(CVE-2019-14895)	目前厂商暂未发布修复措施解决此安...	

关闭

9.3.2.2 漏洞视角

9.3.2.2.1 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 系统漏洞”，选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞，点击右侧操作项的<查看>。

Windows系统漏洞		Linux系统漏洞		Windows应用漏洞		Linux应用漏洞		
终端视角	漏洞视角							
CVE	漏洞名称	影响终端数	漏洞级别	应用名称	应用版本	操作系统版本	操作项	
<input type="checkbox"/>	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-2019-10126)	1	致命	kernel	3.10.0-862.el7	centos-7	查看
<input type="checkbox"/>	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-2019-10126)	1	致命	kernel-tools	3.10.0-862.el7	centos-7	查看
<input type="checkbox"/>	CVE-2019-10126	Linux kernel 缓冲区错误漏洞(CVE-2019-10126)	1	致命	kernel-tools-libs	3.10.0-862.el7	centos-7	查看
<input type="checkbox"/>	CVE-2019-14895	Linux kernel Marvell WiFi chip driver ...	1	致命	kernel	3.10.0-862.el7	centos-7	查看

步骤 4. 在弹出的对话框中可查看漏洞详情，包括应用名称、应用版本、操作系统版本、CVE 编号、描述及建议等。

详情
×

应用名称: kernel

应用版本: 3.10.0-862.el7

操作系统版本: centos-7

CVE: CVE-2019-10126

描述: Linux kernel是美国Linux基金会发布的开源操作系统Linux所使用的内核。Linux kernel中的drivers/net/wireless/marvell/mwifiex/ie.c文件中的'mwifiex_uap_parse_tail_ies'函数存在基于堆的缓冲区溢出漏洞。攻击者可利用该漏洞造成内存损坏或其他危害。

建议: 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法: <https://www.kernel.org/>

确定

9.3.2.2.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 系统漏洞”，选择漏洞视角页签。

步骤 3. 点击<导出>，即可将所有 Linux 系统终端的漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选择的漏洞报告导出至本地。



The screenshot shows the '漏洞管理' (Vulnerability Management) interface. At the top, there are tabs for 'Windows系统漏洞', 'Linux系统漏洞', 'Windows应用漏洞', and 'Linux应用漏洞'. Below these, there are sub-tabs for '终端视角' and '漏洞视角'. A red box highlights the '导出' (Export) button. Below the button, there is a search bar and a table of vulnerabilities. The table has columns for 'CVE', '漏洞名称', '影响终端数', '漏洞级别', '应用名称', '应用版本', '操作系统版本', and '操作项'. One vulnerability is listed: CVE-2019-10126, Linux kernel 缓冲区错误漏洞(...), 1, 致命, kernel, 3.10.0-862.el7, centos-7, and 查看.

9.3.3 Windows 应用漏洞

租户可对 Windows 应用系统漏洞进行扫描、查看扫描结果、导出扫描结果操作。

9.3.3.1 终端视角

9.3.3.1.1 扫描漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 应用漏洞”，选择终端视角页签。

步骤 3. 勾选需要扫描的终端（可勾选多个），点击<开始扫描>。



步骤 4. 在弹出的对话框框中点击<确定>，即可对终端进行漏洞扫描。



9.3.3.1.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>其他漏洞”，选择终端视角页签。

步骤 3. 点击<导出>，即可将所有其他类型漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选择终端的漏洞报告导出至本地。



9.3.3.2 漏洞视角

9.3.3.2.1 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 应用漏洞”，选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞，点击右侧操作项中的<查看>。

终端视角 **漏洞视角**

<input type="checkbox"/>	CVE	漏洞名称	影响终端数	漏洞级别	漏洞类型	操作项
<input type="checkbox"/>	CVE-2016-6662	Oracle MySQL 远程代码执行漏洞/提权漏洞(centos)(CVE-2016-...	1	致命	数据库漏洞	<input type="button" value="查看"/>

步骤 4. 在弹出的对话框中查看漏洞详细信息，包括 CVE 编号、描述及建议。

详情 ✕

CVE: CVE-2016-6662

描述: Oracle MySQL是美国甲骨文 (Oracle) 公司的一套开源的关系数据库管理系统。该数据库系统具有性能高、成本低、可靠性好等特点。Oracle MySQL中的配置文件 (my.cnf) 存在远程代码执行漏洞。攻击者 (本地或远程) 可通过授权访问MySQL数据库 (网络连接或类似phpMyAdmin的Web接口) 或SQL注入方式, 利用该漏洞向配置文件中注入恶意的数据库配置, 导致以root权限执行任意代码, 完全控制受影响的服务器。以下版本受到影响:Oracle MySQL 5.5.52及之前的版本, 5.6.x至5.6.33版本, 5.7.x至5.7.15版本; MariaDB 5.5.51之前的版本, 10.0.27之前的10.0.x版本, 10.1.17之前的10.1.x版本; Percona Server 5.5.51-38.1之前的版本, 5.6.32-78.0之前的5.6.x版本, 5.7.14-7之前的5.7.x版本。

建议: 目前厂商已经发布了升级补丁以修复此安全问题, 补丁获取链接:
<http://www.mysql.com/products/><https://jira.mariadb.org/browse/MDEV-10465><https://www.percona.com/blog/2016/09/12/percona-server-critical-update-cve-2016-6662/>

9.3.3.2.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Windows 应用漏洞”，选择漏洞视角页签。

步骤 3. 点击<导出>，即可将所有其他类型漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选择终端的漏洞报告导出至本地。

资产视角 **漏洞视角**

<input type="checkbox"/>	CVE	漏洞名称	影响资产数	漏洞级别	漏洞类型	操作项
<input type="checkbox"/>	CVE-2015-0235	GNU glibc 基于堆的缓冲区溢出漏洞	2	致命	其他漏洞	<input type="button" value="查看"/>
<input type="checkbox"/>	CVE-2016-2842	OpenSSL 安全漏洞 (CVE-2016-2842)	1	致命	其他漏洞	<input type="button" value="查看"/>

9.3.4 Linux 应用漏洞

租户可对 Linux 应用系统漏洞进行扫描、查看扫描结果、导出扫描结果操作。

9.3.4.1 终端视角

9.3.4.1.1 扫描漏洞

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 应用漏洞”，选择终端视角页签。

步骤 3. 勾选需要扫描的终端（可勾选多个），点击<开始扫描>。



步骤 4. 在弹出的对话框框中点击<确定>，即可对终端进行漏洞扫描。



9.3.4.1.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 应用漏洞”，选择终端视角页签。

步骤 3. 点击<导出>，即可将所有其他类型漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选择终端的漏洞报告导出至本地。



9.3.4.2 漏洞视角

9.3.4.2.1 查看漏洞详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 应用漏洞”，选择漏洞视角页签。

步骤 3. 选择需要查看的漏洞，点击右侧操作项中的<查看>。

终端视角 漏洞视角

导出

<input type="checkbox"/>	CVE	漏洞名称	影响终端数	漏洞级别	漏洞类型	应用名称	应用版本	操作系统版本	操作项
<input type="checkbox"/>	CVE-2015-9262	libXcursor 安全漏...	1	致命	Unix/Linux漏洞	libdrm	2.4.83-2.el7	centos-7	查看

步骤 4. 在弹出的对话框中查看漏洞详细信息，包括应用名称、应用版本、操作系统版本、CVE 编号、描述及建议等。

详情

应用名称: libdrm

应用版本: 2.4.83-2.el7

操作系统版本: centos-7

CVE: CVE-2015-9262

描述: libXcursor是X.Org基金会运作的一个X窗口系统光标管理库。libXcursor 1.1.15之前版本中的library.c文件的_XcursorThemelInherits存在安全漏洞。远程攻击者可利用该漏洞造成拒绝服务或执行代码。

建议: 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://bugs.freedesktop.org/show_bug.cgi?id=90857

确定

9.3.4.2.2 导出漏洞报告

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>漏洞管理>Linux 应用漏洞”，选择漏洞视角页签。

步骤 3. 点击<导出>，即可将所有其他类型漏洞报告导出至本地。

勾选终端（可勾选多个），点击<导出>，可将所选择终端的漏洞报告导出至本地。

Windows系统漏洞 Linux系统漏洞 Windows应用漏洞 Linux应用漏洞

终端视角 漏洞视角

导出

<input type="checkbox"/>	CVE	漏洞名称	影响终端数	漏洞级别	漏洞类型	应用名称	应用版本	操作系统版本	操作项
<input type="checkbox"/>	CVE-2015-9262	libXcursor 安全漏...	1	致命	Unix/Linux漏洞	libdrm	2.4.83-2.el7	centos-7	查看
<input type="checkbox"/>	CVE-2018-1126	procps-ng 安全漏...	1	致命	Unix/Linux漏洞	procps-ng	3.3.10-17.el7	centos-7	查看

9.4 终端体检

租户可通过对对应终端进行终端评估、勒索评估、挖矿评估或弱口令评估来及时发现终端中的潜在威胁。同时可对各个分配的评估任务的执行结果进行相关的查看操作。

9.4.1 终端评估

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>终端体检”，勾选需要评估的终端（可勾选多个），点击<终端评估>。



步骤 3. 在弹出的对话框中点击<确定>，即可对终端进行终端评估。



9.4.2 勒索评估

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>终端体检”，勾选需要评估的终端（可勾选多个），点击<勒索评估>。



步骤 3. 在弹出框中点击<确定>，即可对该终端进行勒索评估。



9.4.3 挖矿评估

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>终端体检”，勾选需要评估的终端（可勾选多个），点击<挖矿评估>。



步骤 3. 在弹出的对话框中点击<确定>，即可对该终端进行挖矿评估。



9.4.4 弱口令评估

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>终端体检”，勾选需要评估的终端（可勾选多个），点击<弱口令评估>。



步骤 3. 在弹出框中点击<确定>，即可对终端进行弱口令评估。



9.4.5 查看评估结果

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>终端体检”，选择已进行评估的终端，点击终端得分、弱口令下的数字或者勒索风险、挖矿风险下的评估等级，即可查看终端相关风险的详细评估报告。



弱口令扫描结果不展示 windows 类 guest 的空口令；

◆ 标识本地账户和域账户。

9.5 基线检查

基线检查是指对终端操作系统、数据库、软件的配置进行安全检测，并提供检测结果说明和加固建议。系统支持对操作系统、中间件、网络设备、虚拟化设备和数据库五类终端进行基线核查。

租户可通过新增任务，批量执行等操作来对指定终端进行基于基线策略执行时间的基线检查。同时可对各个基线检查任务进行结果查看、执行、编辑和删除操作。

9.5.1 新增任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>基线检查”，点击<新增任务>。



任务名称	终端数	检查项	开始时间	结束时间	进度	操作项
信通院测试	1	37	2022-06-29 13:59:00	2022-06-29 14:04:16	扫描完成	[操作图标]

步骤 3. 在弹出的对话框中输入任务名称（不超过 30 字符）、选择检查终端、基线策略及执行时间，点击<确定>即可生成基线检查任务。



新增任务

* 任务名称: test

* 检查终端: 选择终端

* 基线策略: 等保二级 S2A1G2 / Linux

执行时间: 每月 1、31号 00:00:00

取消 确定

9.5.2 执行任务

◆ 方式一：单个执行

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>基线检查”。

步骤 3. 选择需要执行的任务，点击右侧**操作项**的图标，在弹出的对话框中点击<确定>，即可执行该基线检查任务。



◆ 方式二：批量执行

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“风险评估>基线检查”。

步骤 3. 勾选需要执行的任务（可勾选多个），点击任务列表上方的<批量执行>，在弹出的对话框中点击<确定>，即可批量执行基线检查任务。



9.5.3 相关操作

以租户角色登录主机安全系统管理平台，在左侧导航栏选择“风险评估>基线检查”，可对基线检查任务进行以下操作：

- ◆ 点击**操作项**列中的“查看”图标，可查看基线检查任务的详情。
- ◆ 点击**操作项**列中的“编辑”图标，在弹出的对话框中编辑相关信息，可编辑基线检查任务。
- ◆ 点击**操作项**列中的“删除”图标，在弹出的对话框中点击<确定>，可删除基线检查任务。
- ◆ 勾选需要删除的基线检查任务（可勾选多个），点击列表上方的<删除>，在弹出的对话框中点击<确定>，可批量删除基线检查任务。



9.6 定期巡检任务

租户可通过配置定期巡检任务完成定期检测，及时发现终端中的潜在威胁。同时可对需要定期批量执行的检测任务进行新增、编辑和删除操作。

9.6.1 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>定期巡检”，点击<新增>。



步骤 3. 在**新增定期巡检任务**页面编辑相关信息，点击<确定>后即成功新增定期巡检任务。



详细配置方法请参见下表。

参数	说明
任务名称	最长长度为 30 字符。
任务类别	选择任务类别： <ul style="list-style-type: none"> ◆ 快速查杀：快速扫描终端的默认扫描路径，并依照配置的病毒扫描策略对病毒进行相关处理。 ◆ 全盘查杀：扫描终端所有文件，并依照配置的病毒扫描策略对病毒进行相关处理。 ◆ 网站后门查杀：查杀终端是否有网站的后门程序，并依照配置的网马扫描策略对其进行相关处理。 ◆ 弱口令检测：检测终端的弱口令并展示对应弱口令详情。 ◆ 漏洞扫描：扫描终端的系统漏洞并展示对应漏洞详情。
选择终端	点击 图标，选择要执行定期巡检任务的终端。
执行时间	定期巡检任务的执行时间，周期可为日、每周、每月，并需要设置具体的时间点。

9.6.2 编辑定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>定期巡检”，选择需要编辑的巡检任务，点击右侧**操作项**的“编辑”图标。

名称	创建时间	上次巡检时间	备注	操作项
test	2022-08-15 10:38:59			

共 1 条 20 条/页 < 1 > 前往 1 页

步骤 3. 在**编辑定期巡检任务**页面修改需要更改的任务信息，修改完成后点击<确定>即可更改成功。

编辑定期巡检任务

通过配置定期巡检任务，可及时发现终端中的潜在威胁
提示：定期巡检执行时间以管理中心时间为准

* 任务名称: test

* 任务类别: 快速查杀

* 选择终端: DESKTOP-8OK43JQ
 新增终端将会同步此任务

* 执行时间: 每月 31号 00:00:00

备注: 请输入

取消 **确定**

9.6.3 删除定期巡检任务

◆ 对于已存在的定期巡检任务，点击右侧**操作项**的“删除”图标，在弹出的对话框中点击<确定>，即可删除该巡检任务。

名称	创建时间	上次巡检时间	备注	操作项
1	2022-11-23 16:56:06	--	--	

确定删除该条数据?
取消 **确定**

◆ 勾选多个任务，点击列表上方的<删除>，在弹出的对话框中点击<确定>，可对巡检任务进行批量删除操作。

新增 **删除**

当前页已选择 1 项，未选择 0 项 全选当页 反选当页 重置

名称	创建时间	上次巡检时间	备注	操作项
<input checked="" type="checkbox"/> 1	2022-11-23 16:56:06	--	--	

9.7 弱口令检测

租户可通过配置对终端进行应用弱口令检测、主机弱口令检测、配置管理等操作，发现终端中的弱口令信息，同时可对应用弱口令、主机弱口令、配置管理等进行检查和编辑操作。

9.7.1 应用弱口令

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>弱口令检测>应用弱口令”，点击<立即检测>，即可对终端进行对应应用的弱口令进行检测和查看，包括 tomcat、weblogic、onvif、SIP 等应用。



9.7.2 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>弱口令检测>主机弱口令”，选择对应主机，点击<立即检测>。即可对选中主机进行主机弱口令检测，最终查看左方检测出的弱口令数量。



9.7.3 新增定期巡检任务

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>弱口令检测>配置管理”，点击<更新规则>，上传对应需要更新的弱口令文件即可更新弱口令规则库。

弱口令规则总数 7438

内置规则总数 7438

自定义规则总数 0

更新规则

请输入关键字

弱账号	弱口令	规则类型	针对应用	应用类别	最后更新时间
db2inst1	db2inst1	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123123	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	123456	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	12345678	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	--	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	test	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15
db2inst1	Admin123	<input type="checkbox"/> 系统内置	db2	数据库应用	2022-08-10 09:27:15

共 7438 条 ... 前往 页

10 入侵检测

业内首创提出“Attack Movie”概念，可对攻击过程像“放电影”一样进行回放，提供“叠加分析模式”和“演变分析模式”，令攻击过程及演变历史一目了然。

10.1 攻击矩阵

租户角色可在攻击矩阵页签查看所有攻击手段、攻击演示过程、攻击趋势及攻击总数等信息。

10.1.1 攻击热力图

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“入侵检测►攻击矩阵”进入攻击矩阵页面，点击右方的“攻击热力图”按钮查看攻击热力图。



10.1.2 受攻击主机热力图

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“入侵检测►攻击矩阵”进入攻击矩阵页面，点击右方的“受攻击主机热力图”按钮查看受攻击主机热力图。



10.1.3 受攻击工作组热力图

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“入侵检测►攻击矩阵”进入攻击矩阵页面，点击右方的“受攻击工作组热力图”按钮查看受攻击工作组热力图。



上述三个按钮右方的“仅显示命中计数”和“中/英文版矩阵”可以根据用户需求按需调整。

10.2 入侵告警

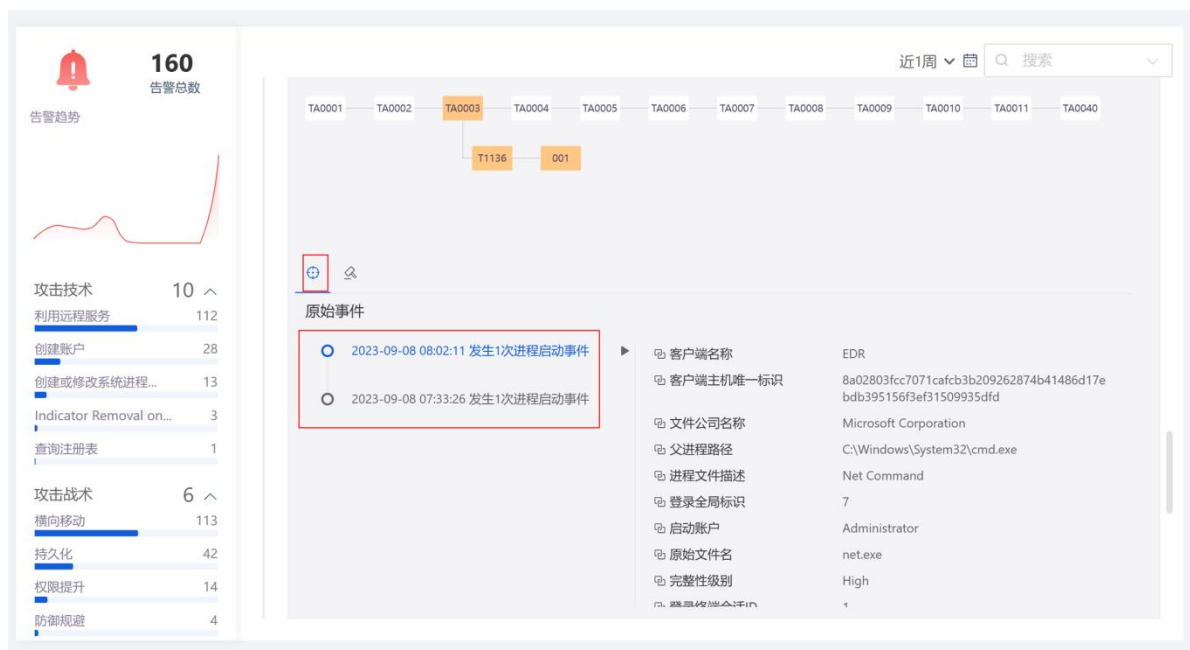
租户角色可在入侵告警页签查看所有告警趋势、告警总数等告警信息。

10.2.1 入侵告警信息

步骤 1. 在左侧导航栏选择“入侵检测▶入侵告警”，进入入侵告警页面。可以看到每条告警信息都会显示当日发生几次原始事件。



步骤 2. 点击 按钮可以看到具体原始事件的相关信息。



步骤 3. 选择告警信息下方的 按钮，即可选择如何处理该告警信息。



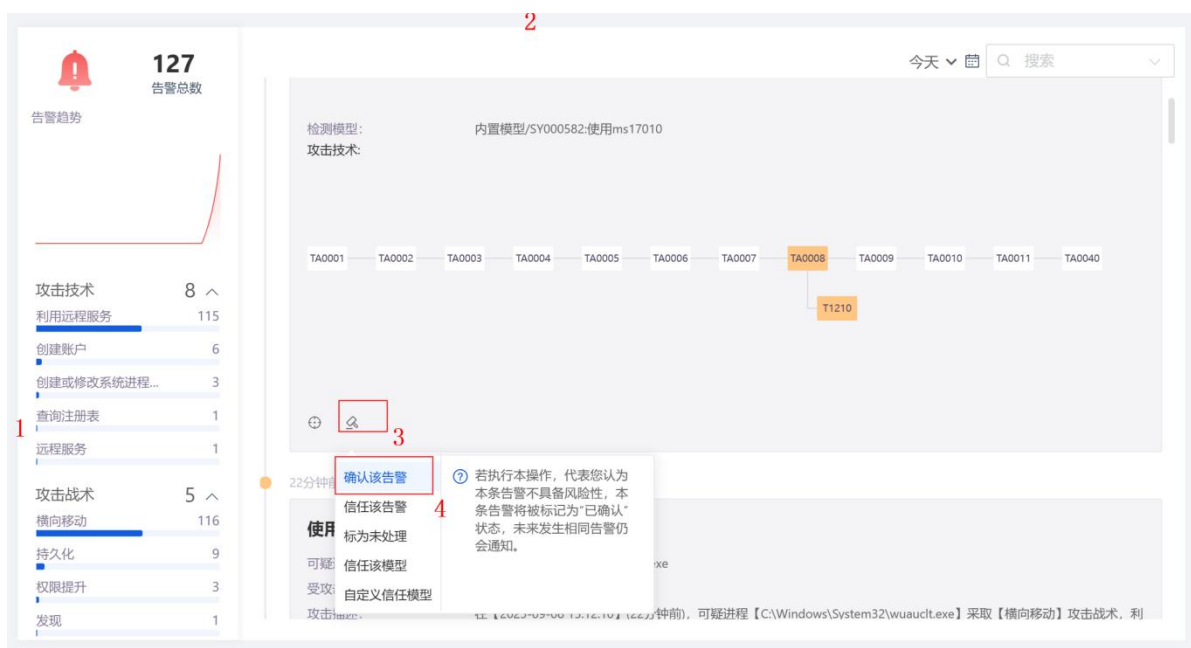
10.2.2 入侵告警处理

若执行本操作，代表您认为本条告警不具备风险性，本条告警将被标记为“已确认”状态，未来发生相同告警仍会通知。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“入侵检测>入侵告警”，进入入侵告警页面

步骤 3. 选择告警信息下方的 按钮，选择**确认该告警**，跳出“操作成功，告警状态已变更！”则确认该告警成功。




10.2.2.1 信任该告警

若执行本操作，代表您认为本条告警不具备风险性，本条告警及未来发生相同告警均标记为“已信任”状态。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“入侵检测>入侵告警”，进入入侵告警页面

步骤 3. 选择告警信息下方的  按钮，选择信任该告警，跳出“操作成功，告警状态已变更！”则信任该告警成功。






10.2.2.2 标为未处理

若执行本操作，代表您暂时无法确定本告警的风险性，本条告警将被标记为“未处理”状态。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“入侵检测>入侵告警”，进入入侵告警页面

步骤 3. 选择告警信息下方的  按钮，选择标为未处理，跳出“操作成功，告警状态已变更！”则标为未处理成功。





10.2.2.3 信任该模型

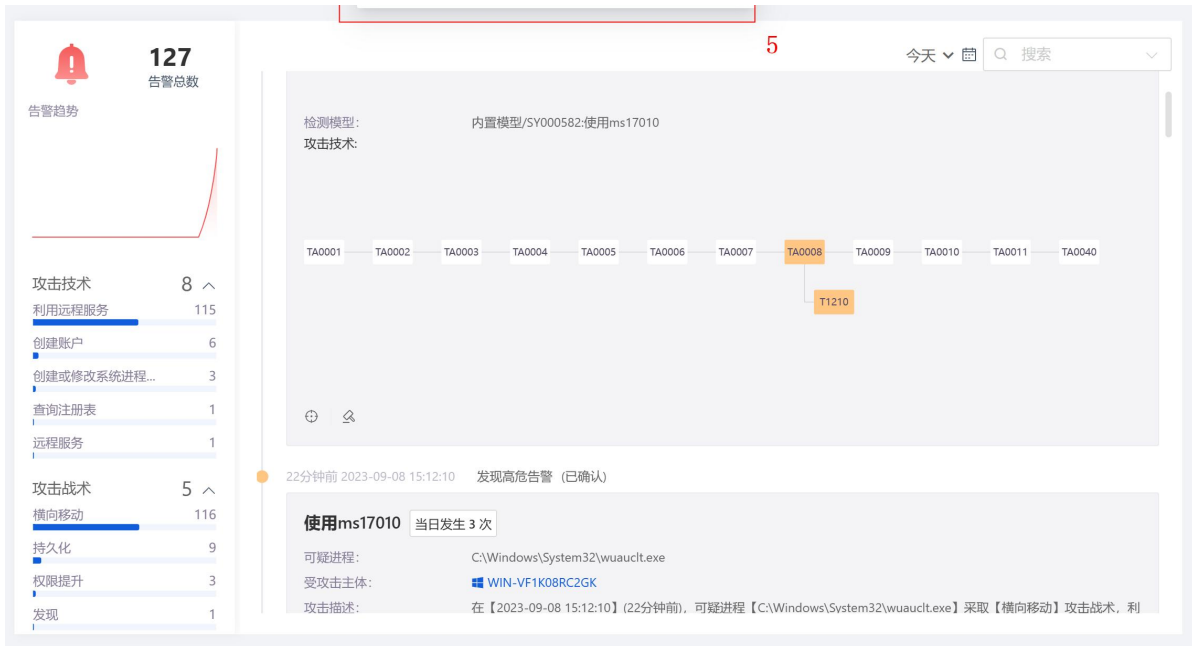
若执行本操作，代表您信任该检测规则，该规则将添加至信任列表，该规则相关告警均标记为“已信任”状态。如需重新启用可前往【检测规则】页面处理。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“入侵检测>入侵告警”，进入入侵告警页面

步骤 3. 选择告警信息下方的 按钮，选择信任该模型，跳出“操作成功，告警状态已变更！”则信任该模型成功。





10.2.2.4 自定义信任模型

若执行本操作，则自动跳转到【模型】页面设置自定义信任模型。

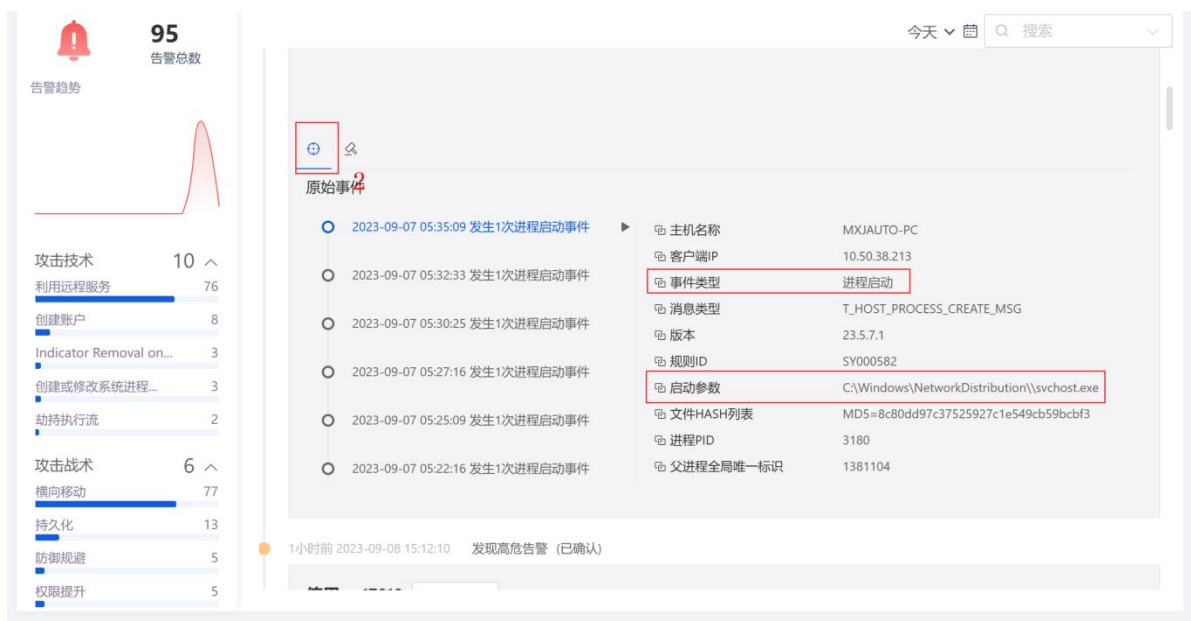
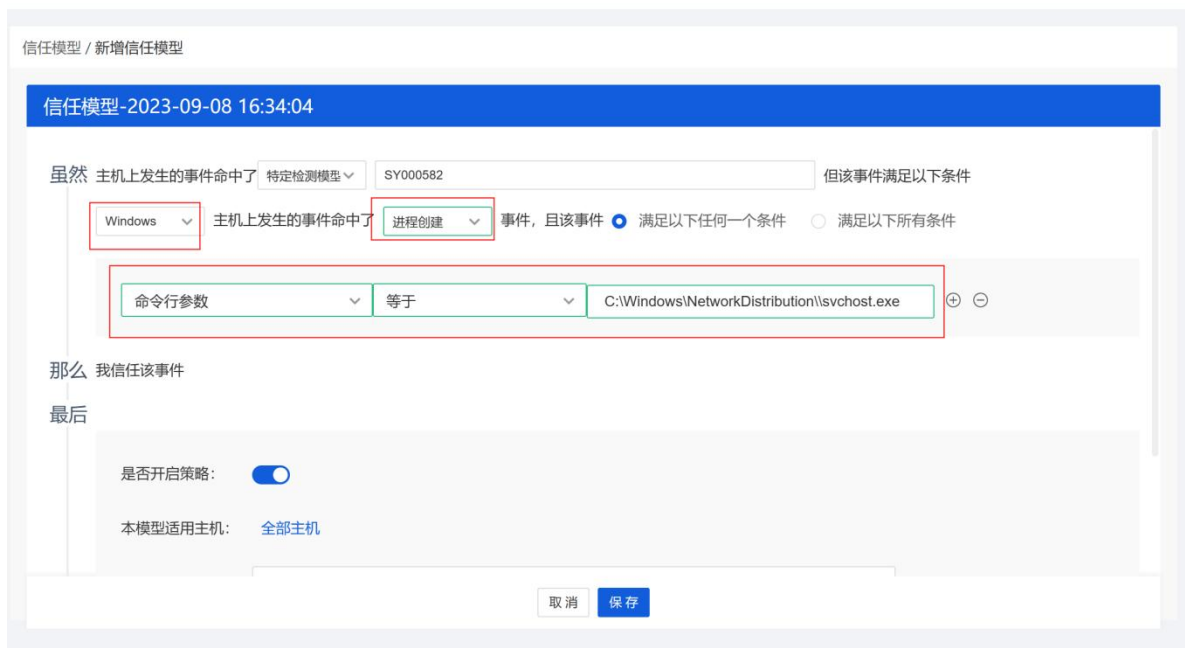
步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“入侵检测>入侵告警”，进入入侵告警页面。

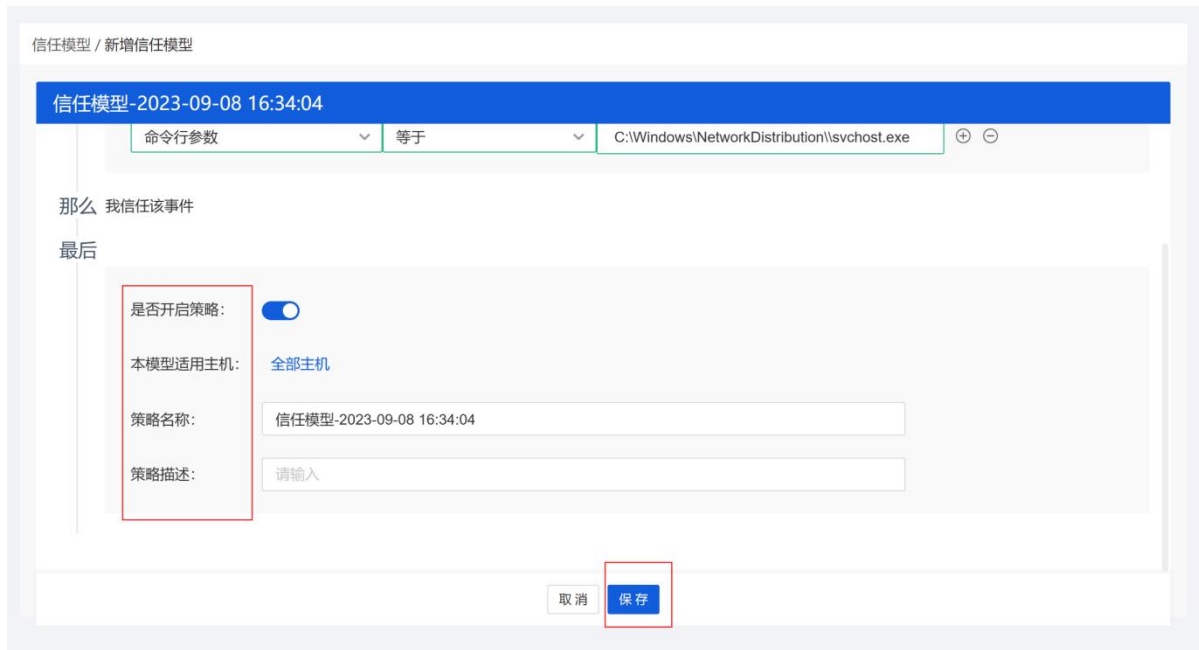
步骤 3. 选择告警信息下方的 按钮，选择自定义信任模型，即自动跳转到【模型】页面设置自定义信任模型。



步骤 4. 选择主机类型和命中的事件类型及相关条件参数（可配置多条件），具体事件类型和参数可以在入侵检测页面查看，如下为例：



步骤 5. 选择是否开启策略、本模型适用主机、策略名称、策略描述后，保存即可完成自定义信任模型配置。



10.3 检测规则

租户角色可在**检测规则**页签查看检测规则详情、信任列表、处置方式等信息。

10.3.1 检测规则

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**入侵检测**►**检测规则**”进入检测规则页面，查看对应检测规则详情，如：初始访问、执行、权限维持、权限提升等。



10.3.2 信任列表

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**入侵检测**►**检测规则**”进入检测规则页面，

点击“信任列表”按钮，即可查看对应添加信任列表的规则。注：信任列表需要通过“入侵检测▶入侵告警”对相关告警实施对应阻断等操作后才会显示需要操作的信任列表。



10.3.3 处置方式

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“入侵检测▶检测规则”进入页面，点击“默认处置方式”按钮，即可设置对应的处理方式，如：默认处置方式、仅记录、关闭等方式。



10.4 模型

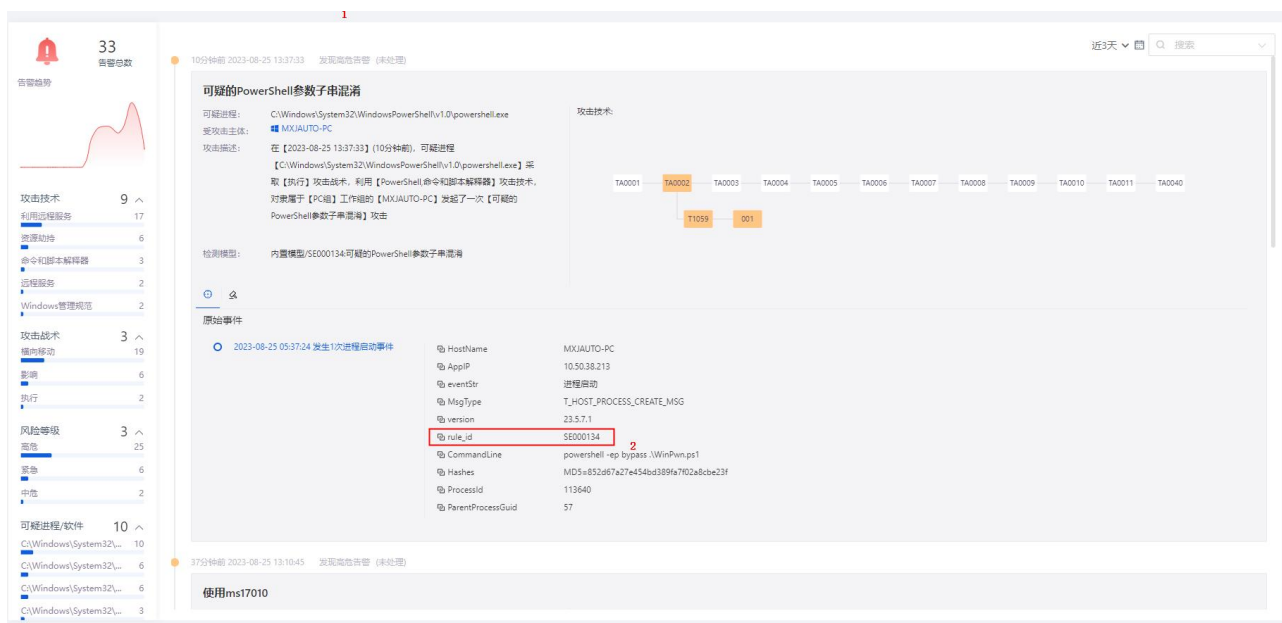
信任模型简单来看可以认为是与“检测模型”起相反的作用。即对某些符合条件的事件，将其定义为是信任的，对这些事件并不生成告警。具体来说信任模型一般在以下场景使用，**场景 1**：某个内置检测模型有误报，可以只针对这个内置检测模型添加一条信任模型，以便排除这个内置检测模型的误报。**场景 2**：希望将符合某条件的事件始终定义为是可信的事件而在告警，在这种场景下，信任模型针对的不是某一个检测模型，而是所有检测模型（包含自定义检测模型）。

自定义信任模型：是“信任模型”的一种，指的是在产品使用期间，由用户自定义添加的那些信任模型，模型的内容由用户自定义确定。

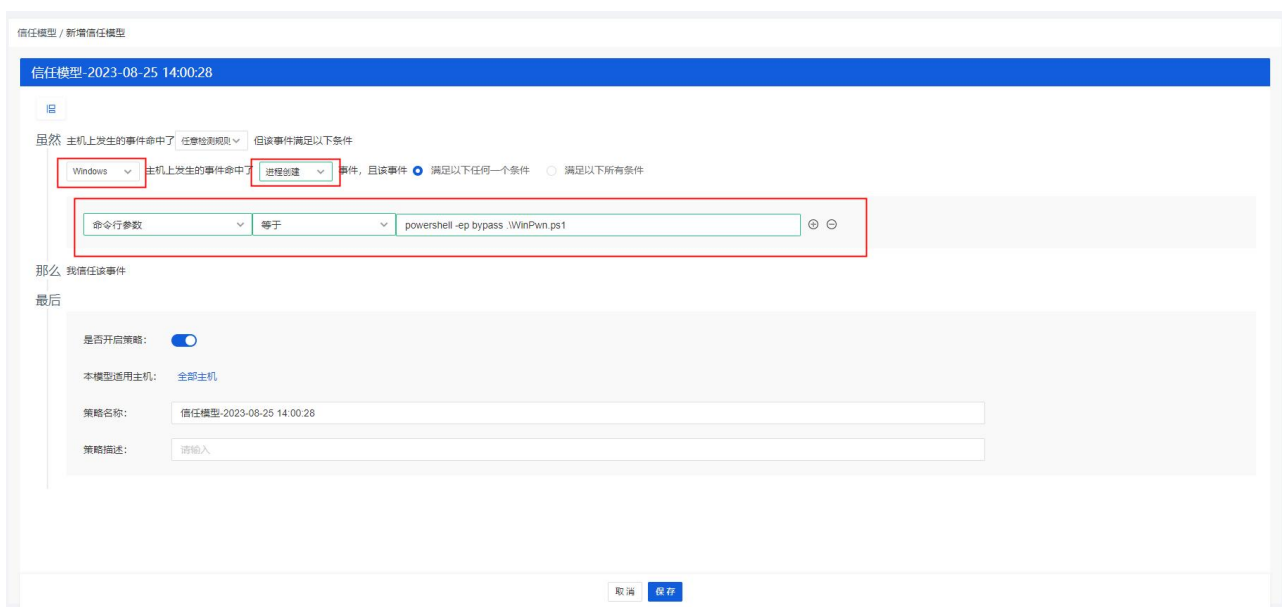
10.4.1 新增信任模型

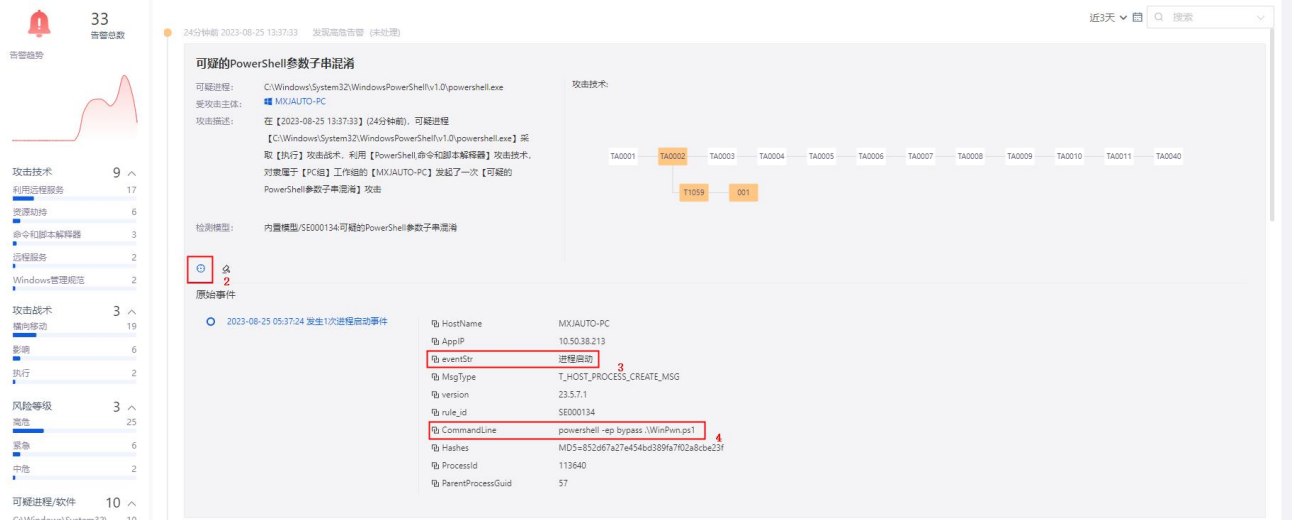
步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 选择【入侵检测】-【模型】-【新增信任模型】，选择任意任意检测规则或特定检测模型（特定检测模型需要填写对应事件 ID，事件 ID 可至入侵告警的 rule ID 查看）。

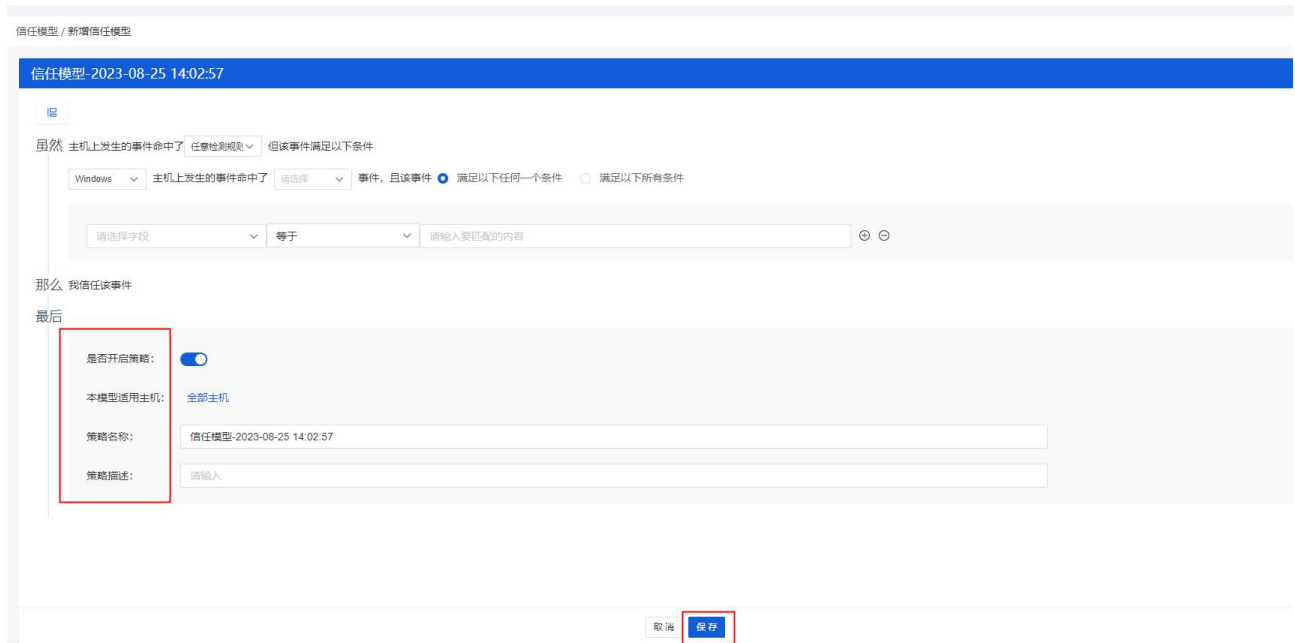


步骤 3. 选择主机类型和命中的事件类型及相关条件参数（可配置多条件），具体事件类型和参数可以在入侵检测页面查看，如下为例：





步骤 4. 选择是否开启策略、本模型适用主机、策略名称、策略描述后吗，保存即可完成信任模型配置。



10.4.2 查看信任模型

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 选择【入侵检测】-【模型】可查看、编辑、删除已经配置信任模型；模型列表中，展示模型名称、模型内容、应用范围、最后修改时间、修改人、操作项。

禁用模型
 启用模型

请输入关键字

模型名称	模型内容	应用范围	最后修改时间	修改人	操作项
<input type="checkbox"/> hsc	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	centos5.6-x64-2.6.18-238等...	2023-08-24 16:05:48	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> zhj	虽然 主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[那么 信任该事件]	LAPTOP-FP3DR87A等1台终...	2023-08-24 15:03:34	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 信任模型-2023-08-25 10:39:49	虽然 主机上发生的事件命中了检测模型[信任模型-2023-08-25 10...]但该事件却满足条件[那么 信任谈...	localhost.localdomain等25...	2023-08-25 10:40:09	autotest	<input checked="" type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> celue	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	localhost.localdomain等1台...	2023-08-25 10:56:41	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> xin1	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	localhost.localdomain等26...	2023-08-25 13:36:08	autotest	<input checked="" type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>

步骤 3. 打开关闭开关或者勾选模型来控制的信任模型的启用或者禁用。

禁用模型
 启用模型

请输入关键字

模型名称	模型内容	应用范围	最后修改时间	修改人	操作项
<input type="checkbox"/> hsc	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	centos5.6-x64-2.6.18-238等...	2023-08-24 16:05:48	autotest	<input checked="" type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> zhj	虽然 主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[那么 信任该事件]	LAPTOP-FP3DR87A等1台终...	2023-08-24 15:03:34	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 信任模型-2023-08-25 10:39:49	虽然 主机上发生的事件命中了检测模型[信任模型-2023-08-25 10...]但该事件却满足条件[那么 信任谈...	localhost.localdomain等25...	2023-08-25 10:40:09	autotest	<input checked="" type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> celue	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	localhost.localdomain等1台...	2023-08-25 10:56:41	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> xin1	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	localhost.localdomain等26...	2023-08-25 13:36:08	autotest	<input checked="" type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>

禁用模型
 启用模型

请输入关键字

共 5 项, 已选择 1 项

模型名称	模型内容	应用范围	最后修改时间	修改人	操作项
<input checked="" type="checkbox"/> hsc	虽然 主机上发生的事件命中了检测模型[任意规则]但该事件却满足条件[那么 信任该事件]	centos5.6-x64-2.6.18-238等...	2023-08-24 16:05:48	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> zhj	虽然 主机上发生的事件命中了检测模型[SE001095]但该事件却满足条件[那么 信任该事件]	LAPTOP-FP3DR87A等1台终...	2023-08-24 15:03:34	autotest	<input type="checkbox"/> 查看 <input type="button" value="编辑"/> <input type="button" value="删除"/>

11.1 智能鉴定

租户角色可在**智能鉴定**页签通过 IP、域名、文件 Hash、漏洞编号在线搜索相关威胁信息；支持对 APT、木马、病毒、蠕虫、后门、勒索、挖矿、僵尸网络、漏洞利用等 10 余种不同类型的威胁进行离线鉴定。。

智能鉴定

支持对APT、木马、病毒、蠕虫、后门、勒索、挖矿、僵尸网络、漏洞利用等10余种不同类型的威胁进行离线鉴定。

域名、IP、文件Hash、漏洞编号

今日 本周 本月

文件

鉴定文件 **129** | 命中文件 **0**

域名

鉴定域名 **30827** | 命中域名 **0**

IP

鉴定IP **22086** | 命中IP **0**

终端

受影响终端数 **0**

请输入关键字

终端名称	IP地址	鉴定内容	威胁类型	告警信息	威胁等级	时间

共 0 条 前往 页

11.2 沙箱分析

管理平台联网时，支持对文件进行在线沙箱、多引擎、情报分析，可在线预览分析结果并支持报告下载。

沙箱分析

管理平台联网时，支持对文件进行在线沙箱、多引擎、情报分析，可在线预览分析结果并支持报告下载。

请输入关键字

<input type="checkbox"/>	文件名称	文件类型	MD5	威胁等级	处理状态	文件上传时间	检测完成时间	操作项
<input type="checkbox"/>	CW.eXe	eXe	60ca507ef4ba7dbbb7effe...	* 高危	检测完成	2023-06-21 14:04:12	2023-06-21 14:06:00	在线预览 下载 删除
<input type="checkbox"/>	loginx789.jsp	jsp	930cd4dd1052d073eedfb...	* 安全	检测完成	2023-06-21 12:34:46	2023-06-21 12:37:00	在线预览 下载 删除
<input type="checkbox"/>	license.lic	lic	a996cc13aad90ef559751...	* 安全	检测完成	2023-06-13 17:00:58	2023-06-13 17:02:01	在线预览 下载 删除
<input type="checkbox"/>	1KEY_HD.rar	rar	9396f900094d4ec5304d9e...	* 高危	检测完成	2023-05-15 00:13:04	2023-05-15 00:15:04	在线预览 下载 删除
<input type="checkbox"/>	文件头.png	png	6455271ad6cf31e625a8d0...	* 未知	检测异常	2023-05-06 11:14:28	2023-05-06 11:30:00	在线预览 下载 删除
<input type="checkbox"/>	2.php	php	587cd9d885339814126cae...	* 安全	检测完成	2023-05-06 11:04:27	2023-05-06 11:06:00	在线预览 下载 删除
<input type="checkbox"/>	1.php	php	97b611ece9ae822bee8a04...	* 未知	检测异常	2023-05-06 10:44:24	2023-05-06 11:00:00	在线预览 下载 删除

共 7 条 前往 页

12 发布端管理

租户可通过配置发布策略，将发布目录下的文件同步到网站目录。



发布端管理为附加功能，需要单独购买许可（模块型号 WPT-EE-ALL）才能使用此功能。

仅租户角色具有发布端管理权限。

12.1 管理发布端

租户可在此页面进行发布端新增、升级、卸载、编辑、查看、启用、修改标签、解除绑定等操作。

12.1.1 新增发布端

12.1.1.1 新增 Windows 系统发布端

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“发布端管理”，进入发布端管理页面。点击<新增>。

发布端名称	标签	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
<input type="checkbox"/> DESKTOP-8JKE...	DB	10.106.15.120	Windows 10 Professional 64-bit	2022-06-10 10:34:31	开启	2.0.17.10	
<input type="checkbox"/> CUNCUN		10.20.18.40	Windows 10 64-bit	2022-03-04 17:36:31	-	2.0.17.7	

步骤 2. 在弹出的对话框的 **Windows 系统** 区域进行 Windows 系统发布端的离线安装。

- ◆ **方式一：** 点击**离线安装**的<下载>，下载客户端安装包，以管理员权限将安装包拷贝到终端服务器上，双击安装程序，执行安装。
- ◆ **方式二：** 点击**离线安装**的<复制>，复制客户端安装包下载链接。以管理员权限登录终端服务器，在浏览器地址栏中粘贴客户端安装包下载链接，即可下载安装包。下载完成后双击安装程序，执行安装。

新增发布端

Windows系统

Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10
 Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 /
 Windows Server 2016 / Windows Server 2019

离线安装：下载安装包，拷贝到主机上进行安装。

https://10.20.178.151/service/file/download2?name=edr_download/windows/test/push/10.20.178.151_10571/1/push_installer_10.20.178.151_LU661a78.exe

下载

复制





客户端主机安装 Windows 系统发布端步骤与主机安全系统客户端安装步骤一致，详情可参考《主机安全及管理系统 V3.0R23C11 软件安装指南》。

12.1.1.2 新增 Linux 系统发布端

步骤 1. 以租户角色登录主机安全系统管理平台。在导航栏选择“发布端管理”，进入发布端列表页面，点击<新增>。

步骤 2. 进行 Linux 系统发布端的离线安装或在线安装。

● 离线安装

选择 CPU 架构以及操作系统位数，点击**离线安装**的<下载>，下载安装包，点击<复制>复制脚本命令。将软件包拷贝到服务器上进行解压，执行脚本命令进行安装即可。



Linux系统
支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统;

离线安装：选择CPU架构以及操作系统位数下载安装包，拷贝到服务器上解压后执行脚本进行安装。

① x86架构
64位操作系统

② 下载 ③ 复制

```
tar --no-same-permissions --no-same-owner -zxvf linux_agent_setup_3.0.1.4.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh
```

● 在线安装

点击**在线安装**的<复制>，复制下载链接，在客户端上以管理员权限执行该命令进行安装。



Linux系统
支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统;

离线安装：选择CPU架构以及操作系统位数下载安装包，拷贝到服务器上解压后执行脚本进行安装。

x86架构
64位操作系统

下载 复制

```
tar --no-same-permissions --no-same-owner -zxvf linux_agent_setup_3.0.1.4.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh
```


在线安装：下载以管理员权限执行以下命令进行安装。

```
wget http://10.20.178.151:10571/download/linux/test/push/10.20.178.151_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && ./agent_setup.sh
```

复制

12.1.2 修改发布端信息

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“发布端管理”，进入发布端管理页面。

步骤 2. 选择需要修改的发布端，点击右侧**操作项**中的图标。

发布端名称	标签	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
<input type="checkbox"/> aigentwin8		192.168.21.78	Windows 8.1 Enterprise Edition 64-bit	2022-06-21 14:57:11	关闭	3.0.1.4	

步骤 3. 在弹出的对话框中编辑发布端信息，点击<确定>即可成功修改发布端信息。

编辑发布端 ✕

* 发布端名称:

标签:

绑定状态: 默认开启, 关闭绑定状态, 该发布端将从发布端列表中移除。

IP地址: 192.168.21.78

操作系统: Windows 8.1 Enterprise Edition 64-bit

发布端版本: 3.0.1.4

12.1.3 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“发布端管理”，进入发布端管理页面。

步骤 2. 租户可在此页面对发布端进行刷新列表、卸载、修改标签、解除绑定、升级等操作。

勾选多个发布端后，可对发布端进行批量卸载、修改标签及解除绑定操作。

发布端名称	标签	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项
<input type="checkbox"/> aigentwin8		192.168.21.78	Windows 8.1 Enterprise Edition 64-bit	2022-06-21 14:57:11	关闭	3.0.1.4	

12.2 配置发布信息

12.2.1 新增发布目录

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“发布端管理”，进入发布端管理页面。

步骤 2. 点击右侧**操作项**中的图标，进入发布目录列表页面。

新增	刷新列表	卸载	修改标签	解除绑定				
发布端名称	标签	IP地址	操作系统	最后在线时间	发布服务状态	版本号	操作项	
<input type="checkbox"/>	aigentwin8	192.168.21.78	Windows 8.1 Enterprise Edition 64-bit	2022-06-21 14:57:11	关闭	3.0.1.4		

步骤 3. 点击**发布服务器**后的开关置于开启状态，开启发布服务器功能。

发布端详情

发布服务器

开启前请确认已安装刚发布服务程序，开启后配置发布目录即可为网站提供发布服务，发布地址：192.168.21.78:10572 [设置](#)

新增 >

名称	发布目录	发布例外	是否启用	操作项
<input type="checkbox"/>	test	C:\Windows	<input checked="" type="checkbox"/>	 

步骤 4. 点击<新增>。

发布端详情

发布服务器

开启前请确认已安装刚发布服务程序，开启后配置发布目录即可为网站提供发布服务，发布地址：192.168.21.78:10572 [设置](#)

新增 >

名称	发布目录	发布例外	是否启用	操作项
<input type="checkbox"/>	test	C:\Windows	<input checked="" type="checkbox"/>	 

步骤 5. 在弹出的对话框中输入发布端需要发布的目录，并设置发布例外（发布例外下的目录文件不会被同步至网站目录），将**是否启用**开关置于开启状态，点击<确定>，即可成功新增发布目录。

新增发布目录 ×

* 名称:

* 发布目录: 选择

发布例外: ⊕ 选择

发布例外的内容不会根据发布配置发布到网站服务器

是否启用:

关闭
确定

12.2.2 配置发布端策略

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“策略管理”，进入策略管理页面。

步骤 2. 选择需要配置的模板，选择发布配置页签，将**发布配置**后的开关置于开启状态，点击<新增>。



步骤 3. 在弹出的对话框中输入发布规则后点击<确定>，即可完成发布策略配置。

新增规则
✕

* 策略名称:

* 发布目录:

同步删除: 是 否 选择是，发布时将删除网站目录下与发布目录不同的文件

同步软链接: 是 否 选择是，发布时将同步文件原有的软链接

同步时机: 事件同步 发布目录的内容变更会立即同步到网站服务器
 定时同步 秒 可输入范围10~3600秒

* 网站目录:

同步例外: ①

开启同步:

规则参数说明如下表所示。

参数	说明
发布目录	选择发布服务器下相应发布目录。
同步删除	选择是否在发布时删除网站目录下与发布目录不同的文件。
同步软链接	选择是否在发布时同步文件原有的软链接。
同步时机	◆ 事件同步：发布目录下的文件只要发生改变，将立即同步更改过的文件内容。

参数	说明
	◆ 定时同步：定时同步发布目录下的文件。
网站目录	选择需要同步的网站服务器下的目录，需写真实目录。

12.2.3 其他操作

进入发布端详情页面，租户可对发布端的 IP 及端口进行设置；选择需要操作的发布目录，可对发布目录进行编辑及删除操作。

支持批量发布目录及单条发布目录删除操作。



仅租户角色具有查看高级威胁操作权限。

主机安全系统具备高级威胁防护功能，主要包括勒索防御、挖矿防御、渗透追踪和情报云脑。

13.1 设置勒索防御

内核级多维度防御引擎，及时发现并阻断勒索病毒，准确高效地实时保护用户关键数据。同时可通过常见问题，了解有关勒索病毒的小知识。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“高级威胁>勒索防御”进入勒索防御页面。

步骤 3. 选择需要设置的引擎类型，点击引擎右侧区域的<去设置>，即可对该引擎进行设置。

详细配置方式可参考[配置勒索防御](#)。

勒索防御

内核级多维度防御引擎，及时发现并阻断勒索病毒，准确高效的实时保护用户关键数据。



勒索防御

内核级多维度防御引擎，及时发现并阻断勒索病毒，准确高效的实时保护用户关键数据。

 <p>勒索诱饵防护引擎 针对勒索病毒遍历文件实施加密的特点，在终端关键目录下放置诱饵文件，当勒索病毒尝试加密诱饵文件时及时中止进程，阻止勒索病毒的进一步加密和扩散。</p> <p>去设置</p>	常见问题 <ol style="list-style-type: none"> 1. 常见勒索软件的类型 2. 如何在事前防御勒索软件 3. 正常软件被勒索防御误报了，怎么加白名单 4. 什么情况下可以解密勒索软件加密的文件
 <p>勒索行为防护引擎 通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统API级别分析，有效抵御未知勒索病毒。</p> <p>去设置</p>	
 <p>文件保险柜 添加访问控制策略，对重要文件或目录进行访问权限控制，仅允许配置的例外进程操作，避免被勒索病毒破坏。</p> <p>去设置</p>	

13.2 设置挖矿防御

通过进程启动防护机制，保护系统不被挖矿类恶意程序非法侵占资源。同时可通过常见问题，了解有关挖矿病毒的小知识。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“高级威胁>挖矿防御”，进入挖矿防御页面。

步骤 3. 点击**反挖矿引擎**右侧区域的<去设置>，即可对该引擎进行设置。

详细配置方式可参考[配置挖矿防御](#)。

反挖矿引擎
通过分析程序行为及其它指标实时发现恶意挖矿程序，无特征，能实时发现未知恶意挖矿程序。

[去设置](#)

- 常见问题**
1. 挖矿病毒是如何传播工作的?
 2. 如何在事前防御挖矿病毒?
 3. 正常软件被挖矿防御误报了，怎么加白名单?
 4. 发现挖矿病毒的常规处理流程?

13.3 设置渗透追踪

根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，实现攻防对抗 360 度防御。同时可通过常见问题，了解渗透追踪的小知识。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“高级威胁>渗透追踪”，进入渗透追踪页面。

步骤 3. 选择需要设置的引擎，点击引擎右侧区域的<去设置>，即可对该引擎进行设置。

详细配置方式可参考[事件响应](#)

- ◆ 功能：检测到终端触发对应规则后，终端会执行相应动作，防止对终端产生危害。
- ◆ 使用场景：适用于需要自定义修改配置策略模板事件响应场景。
- ◆ 使用限制：暂无。

操作步骤

步骤 1. 选择事件响应页签。

步骤 2. 将事件响应后的 图标置于开启状态，开启事件响应功能。



步骤 3. 点击<新增>。



步骤 4. 在弹出的对话框中选择触发条件和执行动作，点击<确定>。

新增
×

触发条件

类型: 文件变更

文件 请输入文件路径 新建

执行动作

告警 是否产生告警日志

删除文件 删除此文件

关闭
确定

详细配置请参见下表。

参数	说明
触发条件	包括文件变更、进程变更、网络连接、账号变更。
执行动作	触发规则后终端执行的动作，包括结束进程、删除文件等。

渗透追踪

根据ATT&CK理论，对攻防对抗的各个阶段进行防护，实现攻防对抗360度防御。

- 单机扩展**

针对本机的扩展行为进行监测，防止提权行为和信息披露。

[去设置](#)
- 隧道搭建**

识别渗透过程中的隧道代理，可阻断隧道代理搭建行为。

[去设置](#)
- 远控持久化**

对失陷后主机远控持久化行为进行检测，可阻断远控。

[去设置](#)
- 内网探测**

对内网的恶意攻击行为进行识别，可阻断恶意探测行为。

[去设置](#)
- 痕迹清除**

可对渗透的收尾阶段的数据清除行为进行识别和阻断。

[去设置](#)

常见问题

1. 了解单机扩展
2. 了解隧道搭建
3. 了解远程持久化
4. 了解内网探测
5. 正常软件被渗透追踪误报了，怎么加白名单?

13.4 查看情报云脑


情报云脑支持对外联 IP、DNS 解析、可疑文件上传至云端进行鉴定，协助分析其是否存在威胁。


同时提供智能鉴定功能，在用户同意云端鉴定的前提下，上传可疑的外联 IP、DNS 解析、可疑文件至云端进行鉴定，并可快速查看鉴定结果。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“高级威胁>情报云脑”进入情报云脑页面。

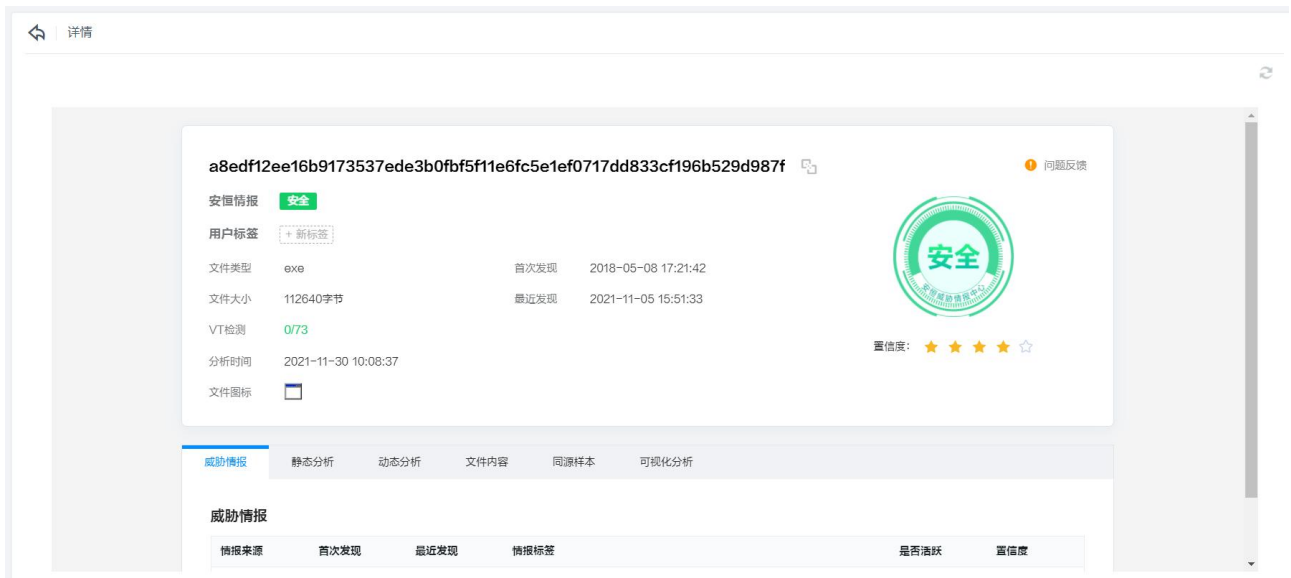
步骤 3. 租户可对可疑域名、可疑外联 IP 或可疑文件进行鉴定。

在输入框中输入需要鉴定的域名、IP、邮箱、文件 Hash 或字符串，点击  图标，即可对该对象进行鉴定。

点击  图标，将文件上传至云端，即可对文件进行鉴定。



步骤 4. 鉴定完毕后，租户可查看详细鉴定结果。



14 策略管理

策略是主机安全系统设备的基本功能，一般分为两部分：匹配条件和执行操作。主机安全系统会根据匹配条件对流量进行检查，并对匹配的流量执行指定的操作。

仅租户具有策略管理操作权限。

租户可在**终端策略**页签以模板形式配置主机策略，包括基础信息、桌面管理、系统防护、终端体检、主机审计、入侵防御、网页防篡改、网站管理、响应处置。

租户可在**容器策略**页签以保护容器镜像内的目录。

内置策略模板有通用模板、业务模板和审计模板，内置策略模板不可进行修改、删除。租户可自定义默认模板，新安装的客户端将自动绑定到默认模板。

租户可对模板进行新增、编辑、查看已绑定终端、绑定新终端操作。同时可通过导出模板的方式对模板进行备份，通过导入备份的模板恢复备份。

14.1 终端策略

14.1.1 新增策略

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**策略模板** > **终端策略**”，将光标移至左上角⁺图标，在下拉框中选择“**新增**”。



步骤 3. 在弹出的对话框中填写策略信息，点击<确定>，即可新增策略。

新增策略
✕

* 策略继承

* 策略名称

备注

取消
确定

14.1.2 编辑策略

操作步骤

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“策略模板>终端策略”，选择需要编辑的策略，点击该策略，进入编辑策略页面。

步骤 3. 编辑需要修改的策略信息，点击<保存>即可成功修改该策略。

策略的详细配置方法请参见下文。



系统默认策略模板（内置模板）无法编辑，仅支持编辑自定义策略。

14.1.2.1 配置基础信息

- ◆ 功能：修改策略模板名称和相关备注信息。
- ◆ 使用场景：适用于需要修改策略模板名称和备注信息的场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**基础信息**页签。

步骤 2. 配置策略名称和备注信息，点击<保存>。



详细配置请参见下表。

参数	说明
策略名称	策略名称为对应的配置模板。请输入 1~200 位字符（支持中文、数字、英文、下横线、横线、“.”、英文括号）。
备注	策略名称对应该的配置模板的备注介绍。不得超过 200 位字符。

14.1.2.2 配置终端管理

选择**终端管理**页签，可对终端设置管控。



各配置项和说明如下表。

配置项	说明
客户端管理	针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速。

配置项	说明
远程协助	针对不同的远程协助场景选择不同的策略，提升远程协助的安全性。
外设管理	按照设备类型以及接口类型对外接设备进行管控，重启系统后方可生效。
移动存储管理	移动存储设备的默认读写权限及使用审计设置，要对具体设备进行个性化设置需要在 查看终端详情 中操作。
屏幕水印	在终端上设置屏幕水印，可以对通过屏幕拍照泄密数据进行溯源，锁定泄密者，挽回损失。
隐形水印	通过安装溯源泄密服务，对通过屏幕拍照、屏幕截图泄密数据进行溯源，锁定泄密者。
系统性能监控	实现监控网络流量、CPU、内存及磁盘的使用状况。


14.1.2.2.1 配置客户端管理

14.1.2.2.1.1 配置卸载密码

- ◆ 功能：设置客户端卸载密码，防止客户端意外卸载。
- ◆ 使用场景：适用于需要自定义修改配置策略模板卸载密码场景。
- ◆ 使用限制：暂无。

操作步骤

步骤 1. 选择**客户端管理**页签。

步骤 2. 点击卸载密码后的  图标置于开启状态，开启卸载密码功能。

步骤 3. 输入密码。

针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速

卸载密码

密码:

桌面快捷方式

Windows: Linux:

升级设置

升级方式: 定时升级

执行时间:

升级内容: 软件版本 病毒库 网马库 漏洞库 威胁情报库 弱口令库

错峰时间: 随机延迟 分钟


下载设置

下载限速: KB/S

14.1.2.2.1.2 配置桌面快捷方式

- ◆ 功能：启用后将显示客户端的桌面图标并设置客户端随系统自启动。
- ◆ 使用场景：适用于需要自定义修改配置策略模板客户端管理场景。
- ◆ 使用限制：无。

步骤 1. 选择**客户端管理**页签。

步骤 2. 点击选择操作系统后的  图标置于开启/关闭状态。

针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速

卸载密码

密码:

桌面快捷方式

Windows: Linux:

升级设置

升级方式: 定时升级

执行时间:

升级内容: 软件版本 病毒库 网马库 漏洞库 威胁情报库 弱口令库

错峰时间: 随机延迟 分钟

下载设置

下载限速: KB/S

详细配置请参见下表。

参数	说明
Windows 桌面快捷方式	启用后将显示客户端的桌面图标并设置客户端随系统自启动，仅针对 Windows 终端生效。
Linux 桌面快捷方式	启用后将在应用程序中显示并设置客户端随系统自启动，仅针对 Linux 终端生效。

14.1.2.2.1.3 配置升级设置

- ◆ 功能：设置客户端定期升级，使客户端及规则库保持最新。
- ◆ 使用场景：适用于需要自定义修改升级场景。
- ◆ 使用限制：暂无。

步骤 1. 选择**客户端管理**页签。

步骤 2. 勾选**定时升级**。

步骤 3. 设置执行时间，选择升级内容，错峰时间。

针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速

卸载密码

密码:

桌面快捷方式

Windows: Linux:

升级设置

升级方式: 定时升级

执行时间:

升级内容: 软件版本 病毒库 网马库 漏洞库 威胁情报库 弱口令库

错峰时间: 随机延迟 分钟

下载设置

下载限速: KB/S

详细配置请参见下表。

配置项	说明
执行时间	可配置自动升级时间，支持按每日、每月、每周，并设置具体时间点。
升级内容	支持软件版本、病毒库、网马库、情报库、漏洞库和弱口令库。
错峰时间	避免批量升级客户端引发升级风暴。将在设置的时间内给绑定的终端随机一个时间升级。

14.1.2.2.1.4 配置下载设置

- ◆ 功能：设置下载限速，保证客户网络环境运行稳定。
- ◆ 使用场景：适用于需要自定义修改升级场景。
- ◆ 使用限制：暂无。

步骤 1. 选择**客户端管理**页签。

步骤 2. 设置下载限速（单位 KB/S）。

针对客户端设置卸载密码、桌面快捷方式、升级方式及内容、下载限速

卸载密码

密码:

桌面快捷方式

Windows: Linux:

升级设置

升级方式: 定时升级

执行时间:

升级内容: 软件版本 病毒库 网马库 漏洞库 威胁情报库 弱口令库

错峰时间: 随机延迟 分钟

下载设置

下载限速: KB/S

14.1.2.2.2 配置远程协助

- ◆ 功能: 管理员可通过远程协助, 处理终端及系统使用问题, 提升管理员的工作效率。
- ◆ 使用场景: 适用于需要自定义修改配置策略模板远程协助场景。
- ◆ 使用限制: 无。

操作步骤

步骤 1. 选择远程协助页签。

步骤 2. 配置用户响应。

针对不同的远程协助场景选择不同的策略, 提升远程协助的安全性。

应答方式: 自动应答 用户响应



- ◆ 自动答应: 无需用户选择响应方式, 用户无感知, 管理员强制远程。
- ◆ 用户响应: 需用户选择响应方式, 用户允许后管理员接管远程。

14.1.2.2.3 配置外设管理

- ◆ 功能: 按照设备类型以及接口类型对外接设备进行管控, 重启终端操作系统后才能生效。
- ◆ 使用场景: 适用于需要自定义修改配置策略模板外设管理场景。
- ◆ 使用限制: 无。

操作步骤

步骤 1. 选择外设管理页签。

步骤 2. 点击外设管控后的 图标置于开启状态, 即可开启外设管控功能。

步骤 3. 选择目标设备，在**权限控制**列选择权限（禁用或放行）。

外设管控 ■ 已关闭

按照设备类型以及接口类型对外接设备进行管控，重启系统后方可生效。

按设备		按接口	
设备类型	权限控制	接口类型	权限控制
无线网卡	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行	USB接口	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行
光驱	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行	串口/并口	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行
软驱	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行	1394控制器	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行
打印机	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行	PCMCIA	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行
调制解调器	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行		
红外设备	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行		
蓝牙设备	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行		
摄像头	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行		
手机/数码设备	<input type="radio"/> 禁用 <input checked="" type="radio"/> 放行		

14.1.2.2.4 配置移动存储管理

- ◆ 功能：移动存储设备的默认读写权限及使用审计设置，利于对移动存储设备进行统一管控。
- ◆ 使用场景：适用于需要自定义修改配置策略模板移动存储设备场景。
- ◆ 使用限制：无。

选择**移动存储管控**页签，设置设备读写权限和设备使用审计。

移动存储设备的默认读写权限及使用审计设置，要对具体设备进行个性化设置需要在“终端管理->移动存储”中操作

设备读写权限: 读写 只读 禁用

设备使用审计: 使用审计 文件拷贝审计

详细配置请参见下表。

参数	说明
设备读写权限	<ul style="list-style-type: none"> ◆ 读写：赋予移动存储设备既可以写入也可以读取权限。 ◆ 只读：赋予移动存储设备既可读取权限。 ◆ 禁用：赋予移动存储设备不可以使用权限。
设备读写权限	<ul style="list-style-type: none"> ◆ 使用审计：移动存储设备使用时对操作进行审计记录。 ◆ 文件拷贝审计：移动存储设备执行文件拷贝对操作进行审计记录。


14.1.2.2.5 配置屏幕水印

- ◆ 功能：可以对通过屏幕拍照泄密数据进行溯源，锁定泄密者，挽回损失。
- ◆ 使用场景：适用于需要自定义修改配置策略模板屏幕水印场景。

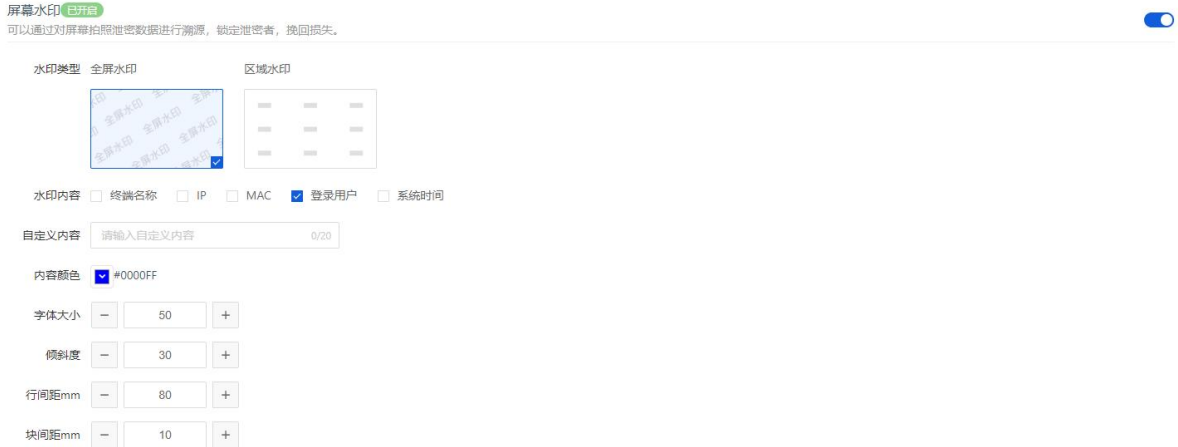
◆ 使用限制：无。

操作步骤

步骤 1. 选择**屏幕水印**页签。

步骤 2. 点击屏幕水印后的  图标置于开启状态，即可开启屏幕水印功能。

步骤 3. 设置水印内容、自定义内容等信息，可配置水印信息。



详细配置请参见下表。

配置项	说明
水印类型	终端支持九宫格展示局部区域水印或者全屏水印。
水印内容	终端显示如下水印内容： <ul style="list-style-type: none"> ◆ 终端名称 ◆ IP ◆ MAC ◆ 登录用户 ◆ 系统时间
自定义内容	不超过 20 个字符。
内容颜色	终端显示水印内容的字体颜色。
字体大小	终端显示水印内容的字体大小。
倾斜度	终端显示水印内容的字体倾斜角度。
行间距 mm	终端显示水印内容每行之间的距离，单位是 mm。
块间距 mm	终端显示水印内容每块之间的距离，单位是 mm。

14.1.2.2.6 配置隐形水印

- ◆ 功能：设置屏幕隐形水印，增强屏幕的溯源效果和溯源能力。
- ◆ 使用场景：适用于需要自定义修改配置策略模板隐形水印功能的场景。
- ◆ 使用限制：该功能需要单独购买屏幕溯源服务许可。

操作步骤

步骤 1. 选择**隐形水印**页签。

步骤 2. 将**隐形水印**后的开关置于开启状态，设置水印强度（取值范围 1~10，数字越大，屏幕水印强度越高），设置是否启用**部分屏增强**功能。



14.1.2.2.7 配置系统性能监控


- ◆ 功能：实现监控网络流量、CPU、内存及磁盘的使用状况。
- ◆ 使用场景：适用于需要自定义修改配置策略模板系统性能监控场景。
- ◆ 使用限制：无。

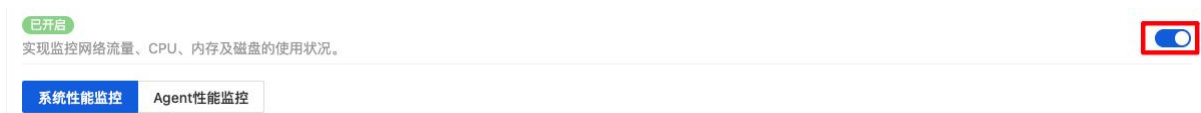
14.1.2.2.7.1 配置系统性能监控

用于监控系统性能监控

操作步骤

步骤 1. 选择**系统性能监控**页签。

步骤 2. 点击**系统性能监控**后的  图标置于开启状态，即可开启系统性能监控。



步骤 3. 选择**系统性能监控** Tab。



步骤 4. 配置具体监控项（CPU 监控、内存监控、网络 IO 监控和磁盘使用监控，本文以 CPU 监控举例说明）。

- 1) 勾选**开启报警**，设置告警阈值。
- 2) 勾选**开启熔断**，设置熔断阈值。
- 3) 勾选**开启恢复**，设置恢复阈值。

详细配置请参见下表。


参数	说明
开启报警	监控项匹配达到规则阈值进行日志记录。
开启熔断	监控项匹配达到规则阈值进行自动熔断，客户端不提供处理能力。
开启恢复	达到熔断条件后匹配达到预设规则将自动恢复客户端能力。

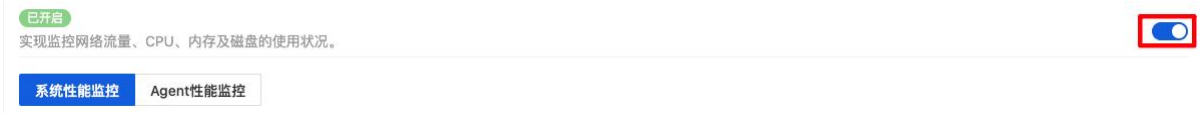
14.1.2.2.7.2 配置 Agent 性能监控

用于监控 Agent 性能监控

操作步骤

步骤 1. 选择**系统性能监控**页签。

步骤 2. 点击**系统性能监控**后的  图标置于开启状态，即可开启系统性能监控。



步骤 3. 选择 Agent 监控 Tab。



步骤 4. 配置具体监控项（CPU 监控、内存监控，本文以 CPU 监控举例说明）。

- 1) 勾选**开启报警**，设置告警阈值。
- 2) 勾选**开启熔断**，设置熔断阈值。
- 3) 勾选**开启恢复**，设置恢复阈值。

详细配置请参见下表。

参数	说明
开启报警	监控项匹配达到规则阈值进行日志记录。
开启熔断	监控项匹配达到规则阈值进行自动熔断，客户端不提供处理能力。
开启恢复	达到熔断条件后匹配达到预设规则将自动恢复客户端能力。

14.1.2.3 配置系统防护

选择**系统防护**页签，可对终端设置防护。

病毒防护 针对网络中流行的病毒、木马进行全面查杀。

勒索防御

挖矿防御

漏洞管理

扫描时机: 文件执行时 文件修改时 存储介质连接时 (Windows)

多引擎设置: 默认引擎
高性能跨平台通用引擎
 深度扫描引擎
开启后将占用200MB磁盘空间

病毒免疫: 开启病毒免疫 (Windows)

实时扫描: 自动处理 (优先进行文件修复, 修复失败后再隔离) 由用户自行选择 删除
针对实时发现病毒 (文件执行、文件修改、存储介质连接时) 的病毒处理方式

智能鉴定: 开启智能鉴定
采集特征到中心进行二次鉴定, 鉴定结果到威胁情报-智能鉴定查看。

各配置项和说明如下表。

参数	说明
病毒防护	针对网络中流行的病毒、木马进行全面查杀。
勒索防御	内核级防御引擎, 第一时间发现并阻断勒索病毒的加密行为, 实时保护用户关键数据。
挖矿防御	通过进程启动防护机制, 保护系统不被挖矿类恶意程序非法侵占资源。
漏洞管理	扫描并且修复系统漏洞, 对操作系统进行加固。

14.1.2.3.1 配置病毒防护

- ◆ 功能: 对网络中流行的病毒、木马进行全面查杀。
- ◆ 使用场景: 适用于需要自定义修改配置策略模板病毒防护场景。
- ◆ 使用限制: 无。

步骤 1. 选择**病毒防护**页签。

步骤 2. 配置扫描时机、多引擎设置、病毒免疫、实时扫描、智能鉴定参数。

针对网络中流行的病毒、木马进行全面查杀。

扫描时机: 文件执行时 文件修改时 存储介质连接时 (Windows)

多引擎设置: 默认引擎
高性能跨平台通用引擎
 深度扫描引擎
开启后将占用200MB磁盘空间

病毒免疫: 开启病毒免疫 (Windows)

实时扫描: 自动处理 (优先进行文件修复, 修复失败后再隔离) 由用户自行选择 删除
针对实时发现病毒 (文件执行、文件修改、存储介质连接时) 的病毒处理方式

智能鉴定: 开启智能鉴定
采集特征到中心进行二次鉴定, 鉴定结果到威胁情报-智能鉴定查看。

详细配置请参见下表

参数	说明
扫描时机	<p>默认全部勾选，用户可根据实际场景进行勾选。</p> <ul style="list-style-type: none"> ◆ 当文件被执行时，将会触发病毒防护功能。 ◆ 当文件被修改时，将会触发病毒防护功能。 ◆ 当存储介质被连接时（Windows），将会触发病毒防护功能。
多引擎设置	<p>病毒防护时的引擎选项：</p> <ul style="list-style-type: none"> ◆ 默认引擎（高性能跨平台通用引擎，建议开启）。 ◆ 深度扫描引擎（开启后将占用 200MB 磁盘空间，深度扫描引擎占用内存更多，但扫描速度更快（进行压缩包扫描时需要选择“深度扫描引擎”）。
病毒免疫	用于检测非文件类病毒，仅适用于 Windows 系统终端。
实时扫描	<p>发现病毒（文件执行、文件修改、存储介质连接时）后的处理方式：</p> <ul style="list-style-type: none"> ◆ 自动处理（优先进行文件修复，修复失败后再隔离）。 ◆ 由用户自行选择。 ◆ 删除（删除病毒文件）。
智能鉴定	采集特征到威胁情报中心进行二次鉴定，鉴定结果请在 查看情报云脑 查看。


14.1.2.3.2 配置勒索防御

- ◆ 功能：内核级防御引擎，第一时间发现并阻断勒索病毒的加密行为，实时保护用户关键数据。
- ◆ 使用场景：适用于需要自定义修改配置策略模板勒索防护场景。
- ◆ 使用限制：无。

步骤 1. 选择勒索防御页签。

步骤 2. 配置生效方式。



步骤 3. 点击引擎后  图标将开关置于开启状态。



详细配置请参见下表。

参数	说明
勒索诱饵防护引擎	针对勒索病毒遍历文件实施加密的特点，在终端关键目录下放置诱饵文件，当有勒索病毒尝试加密诱饵文件时及时中止进程，阻止勒索病毒的进一步加密和扩散。
勒索行为防护引擎	通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统 API 级别分析，有效抵御未知勒索病毒。
文件保险柜	添加访问控制策略，对重要文件进行访问权限控制，仅允许配置的例外进程操作，避免被勒索病毒破坏。

添加文件保险柜的操作方法如下：

步骤 4. 点击<设置>。



步骤 5. 弹出文件保险柜对话框，点击<添加一行>，输入保护项、例外程序后点击<保存>，再点击<确定>，即可添加文件保险柜。



详细配置请参见下表。


参数	说明
保护项	支持模糊匹配，例如输入“bin”，则只要文件名中包含“bin”，该文件就会被加入文件保护柜。
例外程序	文件保险柜保护项中不需要保护的程序，且多个程序用“；”间隔，例如输入“agent.exe”，则该程序就会被加入文件保护柜例外程序。

14.1.2.3.3 配置挖矿防御

- ◆ 功能：通过进程启动防护机制，保护系统不被挖矿类恶意程序非法侵占资源。
- ◆ 使用场景：适用于需要自定义修改配置策略模板挖矿防护场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**挖矿防御**页签。

步骤 2. 点击  图标将开关置于开启状态，即可开启反挖矿引擎。

通过进程启动防护机制，保护系统不被挖矿类恶意程序非法侵占资源。

反挖矿引擎

通过分析程序行为及其它指标实时发现恶意挖矿程序，无特征，能实时发现未知恶意挖矿程序。



开启后可以通过分析程序行为及其它指标实时发现恶意挖矿程序，无特征，能实时发现未知恶意挖矿程序。

14.1.2.3.4 配置漏洞管理

- ◆ 功能：扫描并且修复系统漏洞，对操作系统进行加固。
- ◆ 使用场景：适用于需要自定义修改配置策略模板漏洞管理场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**漏洞管理**页签。

步骤 2. 根据实际情况勾选**扫描后自动修复高危漏洞（Windows）**或者**修复完成后删除补丁文件（Windows）**。

扫描并且修复系统漏洞，对操作系统进行加固。

扫描后自动修复高危漏洞（Windows）

修复完成后删除补丁文件（Windows）

14.1.2.3.5 配置弹窗拦截

- ◆ 功能：自动识别并拦截终端上的广告弹窗。
- ◆ 使用场景：适用于对终端有弹窗拦截需求的场景。
- ◆ 使用限制：无。

步骤 1. 选择**弹窗拦截**页签。

步骤 2. 配置**恶意弹窗防护引擎**按钮。



详细配置请参见下表


参数	说明
恶意弹窗防护引擎	<p>默认勾选，用户可根据自身需求进行勾选。</p> <ul style="list-style-type: none"> ◆ 自动识别并拦截终端上的广告弹窗，覆盖输入法、压缩类、杀毒软件、视频播放、浏览器、游戏助手、模拟器、装机下载、桌面管理、办公学习、聊天通讯、图片编辑、网络工具等 15 大类软件、100+ 款软件，500+ 种广告弹窗。

14.1.2.3.6 配置系统登录防护

- ◆ 功能：对系统账户登录进行细粒度的精准访问控制。
- ◆ 使用场景：适用于需要自定义修改配置策略模板系统登录防护场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**系统登录防护**页签。

步骤 2. 点击系统登录防护后的  图标置于开启状态，即可开启系统登录防护。



步骤 3. 点击<新增>。

已开启

对系统账户登录进行细粒度的精准访问控制。



新增 批量删除

登录账号 访问来源策略 时间策略 处理方式 状态 操作项

步骤 4. 弹出新增规则对话框，编辑相关信息后，点击<确定>。

新增规则
✕

* 登录账号:

访问来源策略

IP/IP范围
 域名

IP/IP范围:

计算机名:

时间策略:

处理方式:

状态: 启用 不启用

详细配置请参见下表。

参数	说明
登录账号	支持输入“*”，表示所有账号都记录。
IP/IP 范围	访问来源 IP 或者 IP 段。 支持的格式如下： <ul style="list-style-type: none"> ◆ * ◆ 192.168.1.1 ◆ 192.168.2.1/24 ◆ 192.168.3.1-192.168.3.255
域名	访问来源域名例：baidu.com。
计算机名	访问来源计算机名例：localhost。
时间策略	访问来源开始时间至结束时间节点。

参数	说明
处理方式	<ul style="list-style-type: none"> ◆ （满足所有策略）允许登录：满足所有配置策略时，允许登录。 ◆ （满足任意策略）禁止登录：满足任意一条策略时，禁止登录。
状态	策略启用状态：启用/不启用。

14.1.2.4 终端体检

选择**终端体检**页签，可对终端设置风险项进行分析统计得分。



各配置项和说明如下表。

配置项	说明
终端感知设置	终端感知设置：自定义终端体检频率及评分上限。
病毒风险感知	针对病毒程序文件风险、系统恶意代码感染风险进行感知。
漏洞风险感知	针对系统漏洞风险、中间件漏洞风险进行感知。
网络风险感知	针对网络变化风险进行感知。
应用合规感知	针对终端上运行的应用、服务、注册表进行感知。
终端健康感知	针对终端整体的健康状态进行感知。

14.1.2.4.1 终端感知设置

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**终端感知设置**页签。

步骤 3. 选择感知频率（每天、每周或每月）。

步骤 4. 选择扣分权重设置。

自定义终端环境感知频率及评分上限

感知频率设置

每天 00:00:00

扣分权重设置

病毒风险感知: - 20 + (建议区间20-50)

漏洞风险感知: - 20 + (建议区间20-50)

应用合规感知: - 20 + (建议区间20-50)

网络风险感知: - 20 + (建议区间20-50)

终端健康感知: - 20 + (建议区间20-50)

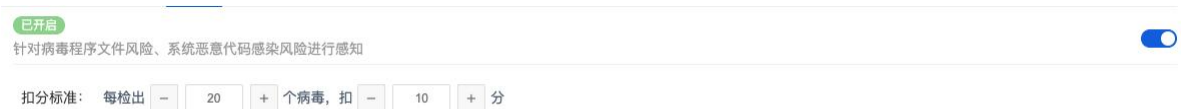
14.1.2.4.2 病毒风险感知

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**病毒风险感知**页签。

步骤 3. 点击**病毒风险感知**后的开关置于开启状态，开启病毒风险感知功能。

步骤 4. 选择扣分标准。



14.1.2.4.3 漏洞风险感知

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**漏洞风险感知**页签。

步骤 3. 点击**漏洞风险感知**后的开关置于开启状态，开启漏洞风险感知功能。

步骤 4. 开启需要评估的漏洞等级（如高危漏洞），选择扣分标准和风险等级。



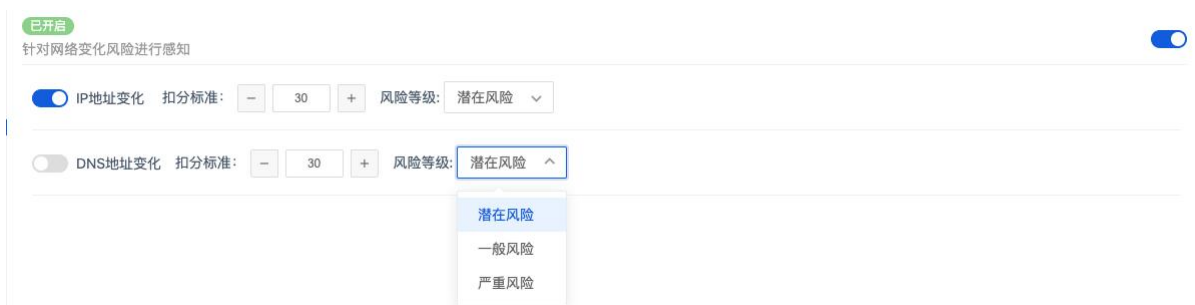
14.1.2.4.4 网络风险感知

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**网络风险感知**页签。

步骤 3. 点击**网络风险感知**后的开关置于开启状态，开启网络风险感知功能。

步骤 4. 开启需要评估的变化参数（例如 IP 地址变化），选择扣分标准和风险等级。



14.1.2.4.5 应用合规感知

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**应用合规设置**页签。

步骤 3. 点击**应用感知**后的开关置于开启状态，开启应用合规检查项感知功能。

步骤 4. 点击对应子功能（包括软件合规风险、服务合规风险、注册表合规风险）后的开关置于开启状态，开启对应子功能。

步骤 5. 设置检测方式（选择**按黑名单检测**或**按白名单检测**，并设置是否开启**按红名单检测**），并设置对应的名单。

步骤 6. 选择扣分标准和风险等级。



名单类型的详细信息请参见下表。

名单类型	说明
------	----

黑名单	针对终端上运行的应用、服务、注册表设置对应黑名单，检测到终端有符合黑名单的应用、服务、注册表时，根据扣分标准进行终端体检扣分。
白名单	针对终端上运行的应用、服务设置对应白名单，检测到终端有白名单之外的应用、服务时，根据扣分标准进行终端体检扣分。
红名单	<p>针对终端上运行的应用、服务、注册表设置对应红名单，需配合黑名单或白名单功能使用。相当于一个例外项。</p> <ul style="list-style-type: none"> ◆ 与白名单功能配合使用时，当检测到终端有符合红名单的应用、服务时，不会扣分。 ◆ 与黑名单功能配合使用时，当检测到终端有符合红名单的应用、服务、注册表时，根据扣分标准进行扣分。

14.1.2.4.6 终端健康感知

步骤 1. 选择**终端体检**页签。

步骤 2. 选择**终端健康感知**页签。

步骤 3. 点击**终端健康感知**后的开关置于开启状态，开启终端健康感知功能。

步骤 4. 开启子功能（例如“登录账号是否存在弱口令”），设置扣分标准，选择风险等级。



14.1.2.5 主机审计

选择主机审计页签，可对终端设置桌面监控。



各配置项和说明如下表。


配置项	说明
开关机审计	审计用户的开关机行为，管理员可配置审计时间段。
系统登录防护	对系统账户登录进行细粒度的精准访问控制。
文件访问监控	监控目标文件、目录的改写操作。

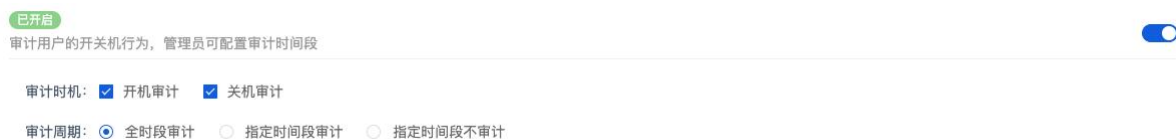
14.1.2.5.1 开关机审计

- ◆ 功能：审计用户的开机、关机行为，管理员可配置审计时间段。
- ◆ 使用场景：适用于需要自定义开关机审计功能的场景。
- ◆ 使用限制：暂无。

操作步骤

步骤 1. 选择开关机审计页签。

步骤 2. 点击开关机审计后的  图标，设置审计时机和审计周期。



详细配置请参见下表。

处置方式	说明
审计时机	<ul style="list-style-type: none"> ◆ 开机审计：审计终端开机事件。 ◆ 关机审计：审计终端关机事件。
审计周期	<ul style="list-style-type: none"> ◆ 全时段审计：审计所有时间段的开机、关机事件。 ◆ 指定时间段审计：审计指定时间段的开机、关机事件，需要设置

处置方式	说明
	时间段（以周为周期）。 ◆ 指定时间段不审计：不审计指定时间段的开机、关机时间，需要设置时间段（以周为周期）。

14.1.2.5.2 配置系统登录审计

- ◆ 功能：对系统账户登录情况进行统计，并针对异常登录场景分析。
- ◆ 使用场景：适用于需要自定义审计登录结果相关场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择系统登录审计页签。

步骤 2. 勾选登录审计成功或者是失败按钮图标后，即可开启系统登录审计的相关策略。



详细配置请参见下表。


参数	说明
登录审计	◆ 审计登录成功：记录登录成功的终端日志。 ◆ 审计登录失败：记录登录失败的终端日志。

14.1.2.5.3 配置文件访问监控

- ◆ 功能：监控目标文件、目录的改写操作。
- ◆ 使用场景：适用于需要自定义修改配置策略模板文件访问监控场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择文件访问监控页签。

步骤 2. 点击文件访问监控后的  图标置于开启状态，开启文件访问控制。



步骤 3. 点击<新增>。



步骤 4. 弹出新增文件访问监控对话框，输入文件路径、备注，点击<确定>即可添加文件访问监控。



14.1.2.6 入侵防御

选择入侵防御页签，可对终端设置暴力行为检测。



各配置项和说明如下表。

配置项	说明
防暴力破解	对系统登录行为进行一定的限制，防止账号被爆破。


配置项	说明
防端口扫描	实时检查入站连接并阻断对本机端口的恶意探测，防止敏感信息泄露。

14.1.2.6.1 配置防暴力破解

- ◆ 功能：对系统登录行为进行一定的限制，防止账号被暴力破解。
- ◆ 使用场景：适用于需要自定义修改配置策略模板防暴力破解场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**防暴力破解**页签。

步骤 2. 点击防暴力破解后的  图标置于开启状态，即可开启防暴力破解。



详细配置请参见下表。

参数	说明
单个 IP 请求时间	相同 IP 请求登录，统计登录失败次数的时间区间，取值范围 1~2147483647，进行阻断或者记录日志。
多个 IP 请求时间	不同 IP 请求登录，统计登录失败次数的时间区间，取值范围 1~2147483647，进行阻断或者记录日志。
IP 临时锁定时间	IP 被锁定 IP 的时间，取值范围 1~2147483647。

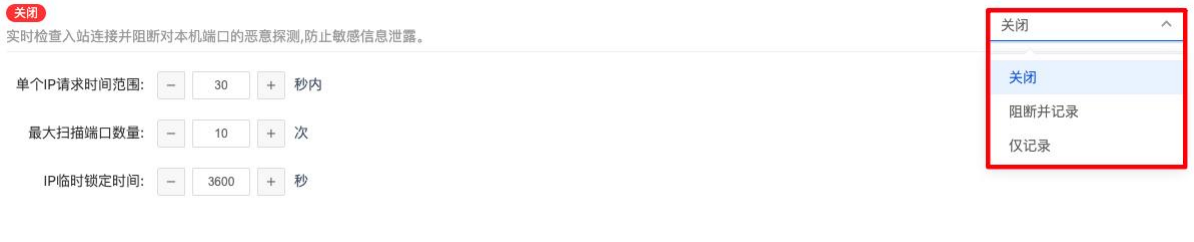
14.1.2.6.2 配置防端口扫描

- ◆ 功能：实时检查入站连接并阻断对主机端口的恶意探测，防止敏感信息泄露。
- ◆ 使用场景：适用于需要自定义修改配置策略模板防端口扫描场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**防端口扫描**页签。

步骤 2. 点击防端口扫描后的服务状态，选择对应的状态。



详细配置请参见下表。

参数	说明
单个 IP 请求时间范围	同个 IP 进行端口扫描请求的统计时间区间，取值范围 10~2147483647。
最大扫描端口数量	最大扫描端口个数，取值范围 2~65535。
IP 临时锁定时间	当 IP 进行端口扫描触发防端口扫描规则，该 IP 被锁定的时间。取值范围 10~2147483647。

14.1.2.7 网页防篡改

- ◆ 功能：保护文件不被篡改，默认保护所有子目录，通过新增白名单可实现对目录的排除。
- ◆ 使用场景：适用于需要修改策略模板网页防篡改场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 开启网页防篡改

- 1) 选择**网页防篡改**页签。
- 2) 点击**网页防篡改**后的 图标置于开启状态，即可开启网页防篡改。



步骤 2. 新增网页防篡改规则。

- 1) 选择**网页防篡改**页签，点击**新增规则**。
- 
- 2) 弹出**新增规则**对话框，输入规则名称、保护目录，选择处理方式、是否启用，点击**确定**即可新增规则。

新增规则
×

* 规则名称:

* 保护目录:

处理方式: 阻断并记录 ▼

是否启用:

关闭
确定

详细配置请参见下表。

参数	说明
规则名称	网页防篡改自定义规则名称，不超过 30 字符。
保护目录	网页防篡改自定义规则需要保护的目录，必须以“/”或“/”结尾。 例如：/etc/
处理方式	触发防篡改自定义规则的处理方式： <ul style="list-style-type: none"> ◆ 阻断并记录：对触发防篡改规则的行为进行阻断并记录日志。 ◆ 仅记录：对触发防篡改规则的行为不做处理仅记录日志。
是否启用	网页防篡改自定义规则启用状态。



网页防篡改作为附加功能，需要单独购买许可（模块型号主机安全系统-MODULE-SERVER-WEB）才能使用此功能。

14.1.2.8 网站管理

选择**网站管理**页签，可对服务器设备上的网站站点攻击行为防护进行配置

基础信息
终端管理
系统防护
终端体检
主机审计
入侵防御
网页防篡改
网站管理
响应处置

发布配置 已开启

通过配置发布策略，可将发布目录下的文件同步到网站目录。

网站漏洞防护

CC攻击防护

网站访问控制

网站IP黑白名单

新增 >

	名称	网站目录	发布端地址	发布目录	同步删除	同步软链接	同步时机	策略状态	操作项
<input type="checkbox"/>									

各配置项和说明如下表。


配置项	说明
发布管理	通过配置发布策略，可将发布目录下的文件同步到网站目录。
网站漏洞防护	针对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。
CC 攻击防护	智能检测并防御 CC 攻击，保证网站正常服务能力。
网站访问控制	灵活配置 IP 或页面路径，可对特定的访问者或页面进行放行或拦截。
网站 IP 黑白名单	<ul style="list-style-type: none"> ◆ 黑名单模式：禁止特定终端用户访问黑名单中的网站页面。 ◆ 白名单模式：仅允许特定终端用户访问白名单中的网站页面。

14.1.2.8.1 发布配置

- ◆ 功能：通过配置发布策略，可将发布目录下的文件同步到网站目录。
- ◆ 使用场景：适用于需要修改策略模板网页发布场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**发布配置**页签。

步骤 2. 点击发布配置后的  图标置于开启状态，即可开启发布配置。



步骤 3. 点击<新增>。



步骤 4. 在弹出的对话框中输入发布规则后点击<确定>，即可完成发布策略配置。

新增规则
×

* 策略名称:

* 发布目录:

同步删除: 是 否 选择是, 发布时将删除网站目录下与发布目录不同的文件

同步软链接: 是 否 选择是, 发布时将同步文件原有的软链接

同步时机: 事件同步 发布目录的内容变更会立即同步到网站服务器
 定时同步 秒 可输入范围10~3600秒

* 网站目录:

同步例外: ①

开启同步:

篡改恢复:

取消
确定

规则参数说明如下表所示。

参数	说明
发布目录	选择发布服务器下相应发布目录。
同步删除	选择是否在发布时删除网站目录下与发布目录不同的文件。
同步软链接	选择是否在发布时同步文件原有的软链接。
同步时机	<ul style="list-style-type: none"> ◆ 事件同步: 发布目录下的文件只要发生改变, 将立即同步更改过的文件内容。 ◆ 定时同步: 定时同步发布目录下的文件。
网站目录	选择需要同步的网站服务器下的目录, 需写真实目录。
同步例外	排除不同步的目录。
开启同步	发布服务的内容会同步到网站服务器。
篡改恢复	用于数据被篡改后将原有数据覆盖篡改内容。

14.1.2.8.2 配置网站漏洞防护

- ◆ 功能: 针对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。
- ◆ 使用场景: 适用于需要自定义修改配置策略模板网站漏洞防护场景。
- ◆ 使用限制: 无。

14.1.2.8.2.1 开启网站漏洞防护

步骤 1. 选择网站漏洞防护页签。

步骤 2. 点击网站漏洞防护后的 图标置于开启状态，即可开启网站漏洞防护功能。



14.1.2.8.2.2 更改拦截提示内容

步骤 1. 点击<自定义拦截提示>。



步骤 2. 在弹出的对话框中输入拦截提醒内容，点击<确定>即可更改拦截提示。



14.1.2.8.2.3 选择防护类型


步骤 1. 勾选右侧的防护类型，即可开启相应防护。



防护类型的说明如下表所示。

防护类型	说明
文件名解析漏洞防护	存在漏洞的 Web 中间件在解析文件名时，由于内置逻辑问题，可能将非脚本类型的文件（扩展名绕过）当做脚本文件执行引发漏洞。
禁止浏览畸形文件	由部分系统保留的特殊字符串创建的文件，普通方法无法直接访问，但是可以被 Web 中间件解析，从而引发漏洞。
敏感信息防泄露	管理员无意中存放在网站目录下的敏感文件，例如日志文件、压缩包、数据库文件等，可能被攻击者通过猜测的方式获取下载地址，引起信息泄露。
自动屏蔽扫描器	可检测各种主流扫描器行为，根据设置屏蔽对本站的扫描。
资源防盗链	采用引用方式防盗链，防止网站内部资源被其他网站引用，造成带宽浪费并消耗系统性能。
网站文件上传防护	部分业务系统存在文件上传功能，对用户上传的文件进行检测，对恶意文件（如网马文件）进行拦截。
网站访问检测	访问网站中的网马文件，例如： http://192.168.1.1/1.php ，访问时会被拦截。

14.1.2.8.2.4 修改规则的启用状态

步骤 1. 选择攻击类型（如 SQL 注入），选择目标修改规则 ID，点击**状态**列表下的图标，即可修改规则的启用状态。

已开启

针对网站常见的 SQL注入攻击、XSS跨站、Web容器及应用漏洞进行实时防护。 [自定义拦截提示](#)



SQL注入 XSS攻击 应用程序漏洞 自定义规则

规则ID	类型	状态	关键字	描述	自定义告警级别
146	sql注入	<input checked="" type="checkbox"/>	url	数据库注释注...	警告信息
147	sql注入	<input checked="" type="checkbox"/>	url	防止对数据库...	警告信息
148	sql注入	<input type="checkbox"/>	url	单引号注入探测	警告信息
100	sql注入	<input checked="" type="checkbox"/>	url	防止非法访问...	警告信息

- 文件名解析漏洞防护
- 禁止浏览畸形文件
- 敏感信息防泄漏
- 自动屏蔽扫描器
- 资源防盗链
- 网站文件上传防护
- 网站访问检测

14.1.2.8.2.5 系统默认规则

步骤 1. 点击<SQL 注入>或<XSS 攻击>或<应用程序漏洞>，可查看系统默认的规则。

已开启

针对网站常见的 SQL注入攻击、XSS跨站、Web容器及应用漏洞进行实时防护。 [自定义拦截提示](#)



SQL注入 XSS攻击 应用程序漏洞 自定义规则

规则ID	类型	状态	关键字	描述	自定义告警级别
146	sql注入	<input checked="" type="checkbox"/>	url	数据库注释注...	警告信息
147	sql注入	<input checked="" type="checkbox"/>	url	防止对数据库...	警告信息
148	sql注入	<input type="checkbox"/>	url	单引号注入探测	警告信息

- 文件名解析漏洞防护
- 禁止浏览畸形文件
- 敏感信息防泄漏
- 自动屏蔽扫描器
- 资源防盗链
- 网站文件上传防护
- 网站访问检测

14.1.2.8.2.6 自定义规则

步骤 1. 点击<自定义规则>。

已开启

针对网站常见的 SQL注入攻击、XSS跨站、Web容器及应用漏洞进行实时防护。 [自定义拦截提示](#)



SQL注入 XSS攻击 应用程序漏洞 自定义规则

[新增](#)

规则ID	类型	状态	关键字	规则	描述	自定义告警级别	操作项
------	----	----	-----	----	----	---------	-----

- 文件名解析漏洞防护
- 禁止浏览畸形文件
- 敏感信息防泄漏
- 自动屏蔽扫描器
- 资源防盗链
- 网站文件上传防护
- 网站访问检测

步骤 2. 点击<新增>。



步骤 3. 在弹出的对话框中输入规则、描述，选择关键字、状态，点击<确定>即可新增网站漏洞防护规则。




14.1.2.8.3 配置 CC 攻击防护

- ◆ 功能：智能检测并防御 CC 攻击，保证网站正常服务能力。
- ◆ 使用场景：适用于需要自定义修改配置策略模板 CC 攻击防护场景。
- ◆ 使用限制：无。

14.1.2.8.3.1 开启 CC 攻击防护

步骤 1. 选择 CC 攻击防护页签。

步骤 2. 点击 CC 攻击防护后的  图标置于开启状态，即可开启 CC 攻击防护。

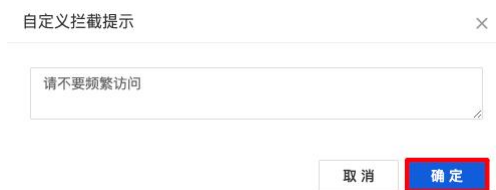


14.1.2.8.3.2 自定义拦截提示

步骤 1. 点击<自定义拦截提示>。



步骤 2. 弹出自定义拦截提示对话框，编辑提示内容后点击<确定>。



14.1.2.8.3.3 设置防护策略

步骤 1. 选择防护策略（低、中、高）。



防护策略的详细信息请参见下表。

参数	说明
防护策略	<ul style="list-style-type: none"> ◆ 高：对每个 IP 的首次访问，需要手动验证，用于识别是否为真实访客浏览行为，适用于网站处于长期性被攻击情况下。 ◆ 中：对每个 IP 的首次访问，自动识别该请求是否为真实访客浏览行为，无需访客参与验证，适用于网站处于间断性被攻击情况下。 ◆ 低：智能验证模式，当请求数达到触发条件时，自动识别该 IP 是否为真实访客浏览行为，解决大部分 CC 攻击问题。可自定义防护配置。

14.1.2.8.3.4 自定义防护配置

步骤 1. 选择防护策略为“低”，点击<设置>。



步骤 2. 弹出 **CC 攻击防护设置** 对话框，设置“单个 IP 每 X（1~36000）秒，请求次数超过 Y（1~999）次，IP 锁定时间 Z（1~36000）秒”，设置是否启用浏览器行为验证，点击<确定>。




浏览器行为验证：当达到规定的访问次数时，如果开启了此选项并且用户是通过浏览器来访问的网站，则说明是正常用户，不会将此 IP 拉黑。此选项是为了将正常用户和攻击工具、爬虫类程序进行区分。

14.1.2.8.4 配置网站访问控制

- ◆ 功能：灵活配置网站访问控制规则，可对特定的访问者或页面进行放行或拦截。
- ◆ 使用场景：适用于需要自定义修改配置策略模板网站访问控制场景。
- ◆ 使用限制：新增规则前请确认客户端已安装 Web 应用防护插件。

14.1.2.8.4.1 开启网站访问控制

步骤 1. 选择**网络访问控制**页签。

步骤 2. 点击**网站访问控制**后的 图标置于开启状态，即可开启网站访问控制。

已开启

灵活配置IP或页面路径，可对特定的访问者或页面进行放行或拦截。 [自定义拦截提示](#)



- 新增规则前请确认已安装Web应用防护插件。
- IP范围字段可为单个IP或IP段，如“192.168.1.*”或“192.168.1.10-192.168.1.20”。通过换行来分隔的多个IP或IP段。
- 页面路径为网页路径，格式形如“192.168.1.100/admin”。

新增

IP范围	页面路径	描述	处理方式	状态	操作项
------	------	----	------	----	-----

14.1.2.8.4.2 自定义拦截提示

步骤 1. 点击<自定义拦截提示>。

已开启

灵活配置IP或页面路径，可对特定的访问者或页面进行放行或拦截。 [自定义拦截提示](#)



- 新增规则前请确认已安装Web应用防护插件。
- IP范围字段可为单个IP或IP段，如“192.168.1.*”或“192.168.1.10-192.168.1.20”。通过换行来分隔的多个IP或IP段。
- 页面路径为网页路径，格式形如“192.168.1.100/admin”。

新增

IP范围	页面路径	描述	处理方式	状态	操作项
------	------	----	------	----	-----

步骤 2. 弹出自定义拦截提示对话框，编写提示内容后点击<确定>。

自定义拦截提示 ×

您的访问权限已被限制

取消 确定

14.1.2.8.4.3 新增规则

步骤 1. 点击<新增>。

已开启

灵活配置IP或页面路径，可对特定的访问者或页面进行放行或拦截。 [自定义拦截提示](#)



- 新增规则前请确认已安装Web应用防护插件。
- IP范围字段可为单个IP或IP段，如“192.168.1.*”或“192.168.1.10-192.168.1.20”。通过换行来分隔的多个IP或IP段。
- 页面路径为网页路径，格式形如“192.168.1.100/admin”。

新增

IP范围	页面路径	描述	处理方式	状态	操作项
------	------	----	------	----	-----

步骤 2. 在弹出的对话框中输入 IP 范围、页面路径、描述，选择处理方式、状态，点击<确定>即可生成访问控制规则。

新增规则
✕

IP范围:

页面路径:

描述:

* 处理方式: 允许 拒绝

* 状态: 启用 未启用

关闭
确定

详细配置请参见下表。

参数	说明
IP 范围	终端的 IP 范围，支持以下格式： <ul style="list-style-type: none"> ◆ “*” 表示所有 IP。 ◆ 单个 IP，例如 192.168.0.1。 ◆ IP 网段，例如 192.168.2.0/24。 ◆ 地址范围，例如 192.168.1.1-192.168.1.100。
页面路径	页面路径为网页路径，例如“192.168.1.100/admin”。
处理方式	<ul style="list-style-type: none"> ◆ 允许：允许 IP 范围内终端访问指定页面。 ◆ 拒绝：禁止 IP 范围内终端访问指定页面。
状态	是否启用规则。

14.1.2.8.5 网站 IP 黑白名单

- ◆ 功能：黑名单模式下禁止特定终端用户访问黑名单内的网站页面；白名单模式下仅允许特定终端用户访问白名单内的网站页面。
- ◆ 使用场景：适用于需要自定义修改配置策略模板网站 IP 黑白名单的场景。
- ◆ 使用限制：新增规则前请确认客户端已安装 Web 应用防护插件。

14.1.2.8.5.1 黑名单模式

步骤 1. 选择网站 IP 黑白名单页签。

步骤 2. 将网站 IP 黑白名单后的开关置于开启状态，选择黑名单模式。

步骤 3. 点击<新增黑名单>。



步骤 4. 在弹出的新增规则对话框中编辑相关信息，点击<确定>。



详细配置请参见下表。

参数	说明
IP 范围	终端的 IP 范围，支持以下格式： <ul style="list-style-type: none"> ◆ “*” 表示所有 IP。 ◆ 单个 IP，例如 192.168.0.1。 ◆ IP 网段，例如 192.168.2.0/24。 ◆ 地址范围，例如 192.168.1.1-192.168.1.100。

参数	说明
页面路径	页面路径为网页路径，例如“192.168.1.100/admin”。
状态	是否启用规则。

14.1.2.8.5.2 白名单模式

步骤 1. 选择网站 IP 黑白名单页签。

步骤 2. 将网站 IP 黑白名单后的开关置于开启状态选择白名单模式。

步骤 3. 点击<新增白名单>。



网站IP黑白名单 已开启

不在白名单规则内的程序都会被阻止。 白名单模式 1

- 新增规则前请确认已安装Web应用防护插件。
- IP范围字段可为单个IP或IP段，如“192.168.1.*”或“192.168.1.10-192.168.1.20”。通过换行来分隔的多个IP或IP段。
- 页面路径为网页路径，格式形如“192.168.1.100/admin”。

新增白名单 3

IP范围	页面路径	状态	操作项
暂无数据			

步骤 4. 在弹出的新增规则对话框中编辑相关信息，点击<确定>。

新增规则
✕

IP范围:

页面路径:

描述:

* 状态: 启用 未启用

关闭
确定

14.1.2.9 响应处置

选择**响应处置**页签，可对威胁事件配置放行等操作。



各配置项和说明如下表。

配置项	说明
信任名单	信任名单添加文件路径或 MD5 值，可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护放行；信任名单添加 IP，可针对防暴力破解、防端口扫描、Web 应用防护放行。
进程防护	匹配黑白名单里的系统进程执行放行与阻止操作。
违规外联	通过探查方式检测主机直接连通互联网或通过其他设备访问互联网。
网络分域隔离	据业务需求，可创建多个网络域供终端操作者选择，同时只能启用一个网络域。
流量发现	采集资产流量，绘制全景流量图展示主机之间的通讯关系。
事件响应	创建满足指定条件，执行终端响应动作。

14.1.2.9.1 配置信任名单

- ◆ 功能：信任名单添加文件路径或 MD5 值，可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护放行；信任名单添加 IP，可针对防暴力破解、防端口扫描、Web 应用防护放行。
- ◆ 使用场景：适用于需要修改策略模板信任名单场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**信任名单**页签。

步骤 2. 点击**信任名单**后的  图标开关置于开启状态，开启信任名单功能。



步骤 3. 点击<新增信任名单>。



步骤 4. 弹出新增信任名单对话框，选择类型，输入信任项、备注，点击<确定>即可生成信任名单。



类型的说明如下表。

类型	说明
文件路径	对文件路径或者文件名匹配，可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护放行。例如：/etc、init.c。
MD5	对文件 MD5 值进行匹配，可针对护网高级威胁、病毒防护、病毒扫描、网马扫描、勒索防护放行。
IP	对 IP 进行匹配，可针对防暴力破解、防端口扫描、Web 防护放行。例如：192.168.1.1、192.168.2.0/24、192.168.3.1-192.168.3.100。

14.1.2.9.2 配置进程防护

- ◆ 功能：匹配黑白名单里的系统进程执行放行与阻止操作。
- ◆ 使用场景：适用于需要自定义修改配置策略模板进程防护场景。
- ◆ 使用限制：暂无。
- ◆ 建议：开启“仅记录”观察一段时间，避免阻止正常的程序，确认无问题后，开启。

操作步骤（以白名单模式为例）

步骤 1. 选择进程防护页签。

步骤 2. 开启进程防护（设置为“阻断并记录”或者“仅记录”）。



步骤 3. 设置为白名单模式。



详细配置请参见下表。

配置项	说明
黑名单模式	不在黑名单规则内的程序都会被放行。
白名单模式	不在白名单规则内的程序都会被阻止。

步骤 4. 点击<新增白名单>。



步骤 5. 在弹出的对话框中中输入类型、进程参数、备注、启用规则，点击<确定>即可添加白名单。



详细配置请参见下表。

参数	说明
类型	支持文件路径和 MD5。
进程参数	对应进程相关参数。
路径匹配模式	当类型选择“文件路径”时，需要设置路径匹配模式： ◆ 全字匹配：文件路径与设置的路径一致时才匹配规则。 ◆ 模糊匹配：文件路径包含设置路径的部分值时匹配规则。
备注	该策略的备注详情。
启用规则	是否启用规则。

14.1.2.9.3 配置违规外联

- ◆ 功能：通过探查方式检测终端直接连通互联网或通过其他设备访问互联网的行为，对非法外联行为进行处置，预防终端访问其他恶意链接造成的相关影响。
- ◆ 使用场景：适用于需要自定义修改配置策略模板违规外联场景。
- ◆ 使用限制：无。

操作步骤

步骤 1. 选择**违规外联**页签。

步骤 2. 点击**违规外联**后的  图标置于开启状态，即可开启违规外联功能。



步骤 3. 点击“已设置探测地址 **X** 个”中的蓝色数字，其中“**X**”表示具体数字。



步骤 4. 在弹出的对话框中点击<添加一行>。输入域名或 IP 后点击<保存>，再点击<确定>，即可保存探测地址。

探测地址 ×

域名/IP	操作项
<input style="width: 95%; border: 1px solid #ccc;" type="text" value="请输入域名/IP"/>	保存

+ 添加一行

取消
确定

步骤 5. 设置处理方式。

已开启

通过探查方式检测主机直接连通互联网或通过其他设备访问互联网

探测地址 已设置探测地址 0 个

发现违规外联终端: 不处理
弹窗提醒用户并关机
弹窗提醒用户并断网 (重启主机恢复网络)

设置探测地址，系统自动检测是否外联探测地址。

发现违规外联终端的处置方式请参见下表。

处置方式	说明
不处理	发现违规外联终端不做任何处理。
弹窗提醒用户并关机	发现违规外联终端，客户端会弹出弹窗进行警告使用者，并进行关机处理。
弹窗提醒用户并断网 (重启主机恢复网络)	发现违规外联终端，客户端会弹出弹窗进行警告使用者，并进行对终端断网处理，需重启终端后方可恢复网络，如发现防护日志出现终端因为违规外联导致断网，需要给该终端重启操作后方可恢复。

14.1.2.9.4 网络分隔隔离

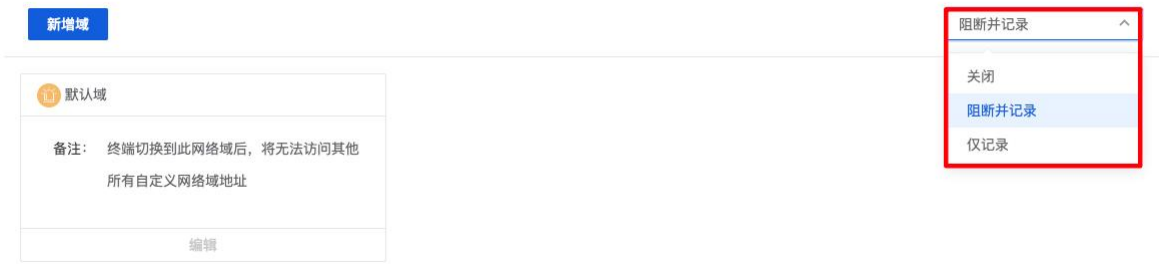
- ◆ 功能：根据业务需求，可创建多个网络域供终端操作者选择，同时只能启用一个网络域。
- ◆ 使用场景：适用于需要自定义修改配置策略模板网络分隔隔离场景。
- ◆ 使用限制：终端切换到此网络域后，将无法访问其他所有自定义网络域地址。

操作步骤

步骤 1. 选择网络分隔隔离页签。

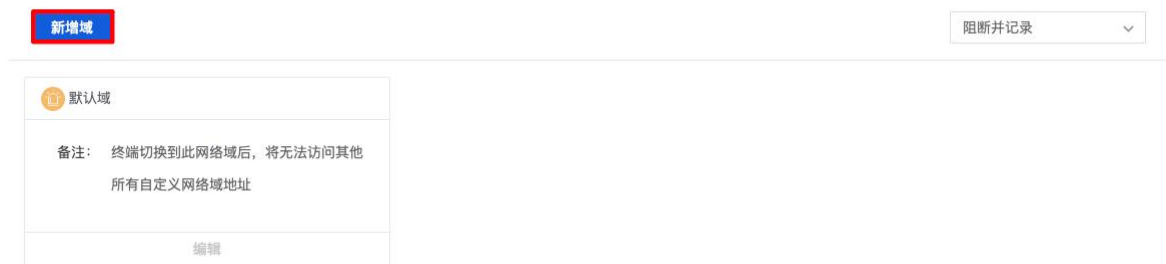
步骤 2. 选择触发网络分隔隔离规则时，系统的处理方式（需要选择“阻断并记录”或“仅记录”）。

根据业务需求，可创建多个网络域供终端操作者选择，同时只能启用一个网络域



步骤 3. 点击<新增域>。

根据业务需求，可创建多个网络域供终端操作者选择，同时只能启用一个网络域



步骤 4. 弹出新增网络域对话框，输入网络域、地址段、备注，点击<确定>即可添加网络域。

新增网络域
×

* 网络域:

* 地址段:

备注:

关闭 确定

详细配置请参见下表。

参数	说明
网络域	字符长度最大为 10 位。
地址段	地址段格式可以为：0.0.0.0/24、192.168.1.10-192.168.1.100、192.168.1.1。
备注	网络域的备注信息。

14.1.2.9.5 流量画像

- ◆ 功能：采集终端流量，绘制全景流量图展示主机之间的通讯关系。
- ◆ 使用场景：适用于需要自定义修改配置策略模板流量画像场景。
- ◆ 使用限制：暂无。

操作步骤

步骤 1. 选择**流量画像**页签。

步骤 2. 点击**流量画像**后的  图标置于开启状态，即可开启流量画像功能。




14.1.2.9.6 事件响应

- ◆ 功能：检测到终端触发对应规则后，终端会执行相应动作，防止对终端产生危害。
- ◆ 使用场景：适用于需要自定义修改配置策略模板事件响应场景。
- ◆ 使用限制：暂无。

操作步骤

步骤 1. 选择**事件响应**页签。

步骤 2. 将**事件响应**后的  图标置于开启状态，开启事件响应功能。



步骤 3. 点击<**新增**>。



步骤 4. 在弹出的对话框中选择触发条件和执行动作，点击<**确定**>。

新增 ×

触发条件

类型:

文件

执行动作

告警 是否产生告警日志

删除文件 删除此文件

详细配置请参见下表。


参数	说明
触发条件	包括文件变更、进程变更、网络连接、账号变更。
执行动作	触发规则后终端执行的动作，包括结束进程、删除文件等。

14.1.3 绑定终端

绑定终端是指将策略应用到特定的终端上。创建策略后，必须将策略绑定到终端才会生效。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“策略模板>终端策略”，进入终端策略页面。

步骤 3. 选择需要绑定终端的策略，点击策略右侧的  图标，选择“绑定终端”。



步骤 4. 在弹出的对话框中选择需要绑定的终端（将终端列表中的终端移动至已选择端列表），单击<确定>，即可将终端绑定至本策略。

The screenshot displays a 'Select Terminal' dialog box with two main sections: 'Terminal List' (3/5) and 'Selected Terminal List' (3/3). Both sections include search filters for 'Please select group', 'Select tag', and 'Terminal name/IP'. The 'Terminal List' section shows a list of terminals with checkboxes, including 'linux-HJY(192.168...)', 'localhost.localdomain(10.11...)', 'WIN-3QFTRUC04HH(10.11...)', 'localhost.localdomain(10.11...)', and 'DESKTOP-8OK43JQ(192.168...)'. The 'Selected Terminal List' section shows the same list with checkboxes checked. At the bottom right, there are '取消' (Cancel) and '确定' (Confirm) buttons.

14.1.4 其他操作

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择“策略模板>终端策略”，进入终端策略页面。

步骤 3. 点击相关按钮，可对策略进行导入、导出、查看、设为默认模板及删除操作。

The screenshot shows the '策略管理' (Strategy Management) page. It features a search bar for '请输入策略名称' (Please enter strategy name). Below is a list of strategy templates: 'HJY-test' (已绑定 3 个终端), '通用模板' (已绑定 0 个终端), '审计模板' (已绑定 0 个终端), '业务模板' (已绑定 0 个终端), 'hutt' (已绑定 1 个终端), and 'xty' (已绑定 1 个终端). A red box highlights the '新增' (Add), '导入' (Import), '导出' (Export), and '删除' (Delete) buttons in the action column.



14.2 容器策略

仅租户角色具有安全策略操作权限。

可在**安全策略**页面对容器目录及子目录内的文件进行篡改防护，支持设置“允许改写的进程”、“放行子

目录”。将容器镜像内的目录保护后，任何以该镜像创建的容器内的目录都将被保护，目录下的内容（包括子目录和文件）都将无法被修改。



建议将日志目录、缓存目录、数据库目录及网站服务需要写入文件的目录做放行处理。

新增容器篡改防护规则的操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“策略模板>容器策略”，进入**容器篡改防护**页面。

步骤 3. 将**容器篡改防护**后的开关置于开启状态，开启容器防篡改功能。



步骤 4. 点击<新增>。



步骤 5. 进入**新增规则**页面，填写规则详细信息后点击<确定>，即可成功新增容器篡改防护规则。

新增规则

* 规则名称

* 保护镜像名 只支持 "*" 号结尾的模糊匹配

* 保护容器目录 只允许配置一个保护目录，配置多个目录需创建多个规则

允许改写进程 请输入允许修改保护容器目录的进程，多个用逗号分隔，不允许配置*号

处理方式

是否启用

放行子目录 允许某些进程修改某些子目录(目录必须以/结尾)或文件，路径和进程用逗号分隔，换行分隔多条配置。例如：
/var/www/logs/*
/var/www/cache/,/bin/java

备注

详细配置请参见下表。

参数	说明
规则名称	最大长度 20 字符。
保护镜像名	被保护的镜像名称，仅支持以 "*" 结尾的模糊匹配，且仅支持英文，最大长度 1024 字符，例如 ops*。
保护容器目录	仅允许设置一个保护目录，例如/bin。
允许改写进程	允许修改保护容器目录的进程，可输入多个，用英文逗号分隔。例如/bin/md。
处理方式	触发规则时系统的处理方式： <ul style="list-style-type: none"> ◆ 仅记录：仅生成防护日志。 ◆ 阻断并记录：阻断改写请求，并生成防护日志。
是否启用	是否启用该规则。
放行子目录	允许修改的子目录，目录必须以 "/" 结尾，也可以是具体文件，进程和路径用英文逗号分隔，多个配置项用回车分隔。

15 响应处置

仅租户角色具有响应处置权限。

响应处置是指对所有终端进行信息采集，对采集的信息进行分析处理后得到流量画像，对采集到的信息提供检索功能。并支持对终端执行文件推送等操作。

15.1 微隔离

微隔离可对不同业务之间进行流量隔离并精确阻断非法流量。租户可启用或停用微隔离规则，停用后的规则不生效。同时租户通过**一键封锁 IP**、**一键关闭端口**输入需要屏蔽的地址或者关闭的端口，可一键生成对应规则。



- ◆ 确保关闭本地端口或屏蔽 IP 不会对业务造成影响后进行相应操作。
- ◆ 微隔离规则放行的优先级高于阻止，在配置时可以先阻止所有端口后，再放行必要的端口。
- ◆ 针对 Linux 终端配置的微隔离规则与本地防火墙规则冲突时，以微隔离配置的规则为准。
- ◆ 微隔离暂不支持 ipv6

15.1.1 混合模式

支持终端规则和标签规则两种配置方式。关于标签的更多信息，请参考[新增标签](#)。

15.1.1.1 终端规则

15.1.1.1.1 新增终端微隔离规则

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>微隔离”，选择终端规则页签。

步骤 3. 选择混合模式，点击<新增规则>。



步骤 4. 进入新增微隔离页面，编辑相关信息，点击<确定>即可新增微隔离规则。

← 新增微隔离

*** 规则名称** • 最多输入30个字符，可用于说明规则的用途

*** 协议类型** 必填项，请选择协议类型

规则类型 双向 进站规则 出站规则 • 进站（默认）表示远程主机访问本地主机，出站表示本地主机访问远程主机

*** 本地IP** • IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.1.1/24
192.168.1.1-192.168.1.255
"/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

*** 本地端口** • 例如:
445
"*"表示所有端口、多个端口换行输入

*** 远程IP** • IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.1.1/24
192.168.1.1-192.168.1.255
"/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

*** 远程端口** • 例如:
445
"*"表示所有端口、多个端口换行输入

处理方式 放行 阻止

状态

*** 应用终端** 选择终端

确定
取消

详细配置请参见下表。

参数	说明
规则名称	可用于说明规则的用途，最多输入 30 个字符
规则类型	<ul style="list-style-type: none"> ◆ 进站：规则仅应用于进站连接，即访问本机的请求。 ◆ 出站：规则仅应用于出站连接，即本机向外发送的请求。 ◆ 双向：规则应用于进站及出站两种连接。
本地 IP	通常设置为“*”，表示所有本地 IP。多网卡配置不同规则的情况请填写具体 IP。
本地端口	本地主机的端口，例如 455，输入多个请用回车间隔，“*”表示所有端口。
远程 IP	远程主机的 IP 地址或地址段。
远程端口	远程主机的端口，例如 455，输入多个请用回车间隔，“*”表示所有端口。
协议类型	支持所有、TCP、UDP 和 ICMP。
处理方式	放行或阻止，放行的优先级高于阻止，可用于阻止整段 IP 的访问再放行个别 IP 允许访问。

参数	说明
状态	开启后规则生效，关闭后规则不生效。
应用终端	点击<选择终端>，设置本条规则应用的终端。

15.1.1.1.2 一键封锁 IP

当需要禁止终端访问目标主机时或禁止目标主机访问终端时，可设置一键封锁 IP。操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在导航栏选择“响应处置>微隔离”，选择混合模式。

步骤 3. 选择终端规则页签，点击<一键封锁 IP>。



步骤 4. 进入一键封锁 IP 页面，编辑相关信息，点击<确定>。



详细配置请参见下表。

参数	说明
规则名称	长度为 1~30 位，支持中文、英文、数字、“_”、“-”、“.”。
封锁 IP	设置终端禁止访问的 IP（被封锁的 IP 也无法访问终端）。可设置多个，用回车分隔，例如：192.168.1.1、192.168.1.0/24、192.168.1.1-192.168.1.254。

参数	说明
应用终端	封锁规则应用的终端。点击<选择终端>，设置规则应用的终端。

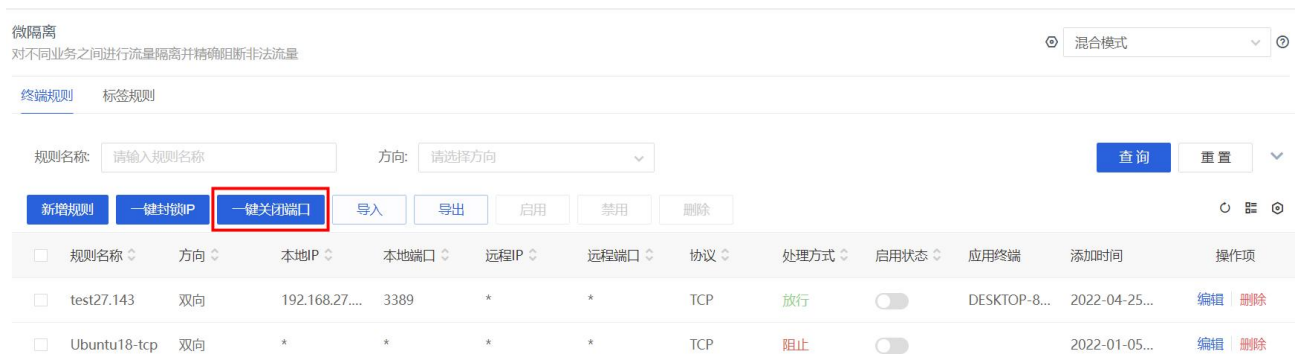
15.1.1.1.3 一键关闭端口

当需要禁止使用终端的指定端口，可设置一键关闭端口。操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>微隔离”，选择混合模式。

步骤 3. 选择终端规则页签，点击<一键关闭端口>。



步骤 4. 进入一键关闭端口页面，编辑相关信息，点击<确定>即可关闭该终端的端口。

← 一键关闭端口

* 规则名称

* 封锁端口 • 例如：
445
多个端口换行输入

* 应用终端 已选择终端(2) x

详细配置请参见下表。

参数	说明
规则名称	长度为 1~30 字符，支持中文、英文、数字、“_”、“-”、“.”。
封锁端口	例如 445，输入多个端口请用回车分隔。
应用终端	选择规则应用的终端。点击<选择终端>，设置规则应用的终端。

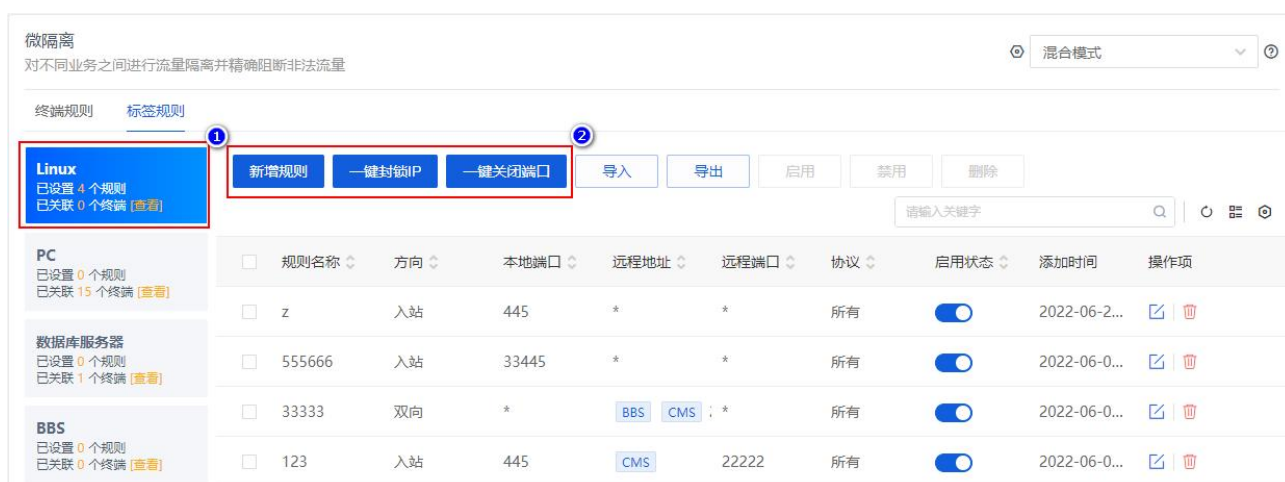
15.1.1.2 标签规则

标签规则是指对某一标签下的终端设置微隔离规则,包括微隔离规则、一键封锁 IP 以及一键关闭端口。

步骤 1. 以租户角色登录主机安全系统管理平台,在导航栏选择“响应处置>微隔离”,选择混合模式,选择**标签规则**页面。

步骤 2. 可执行以下操作。

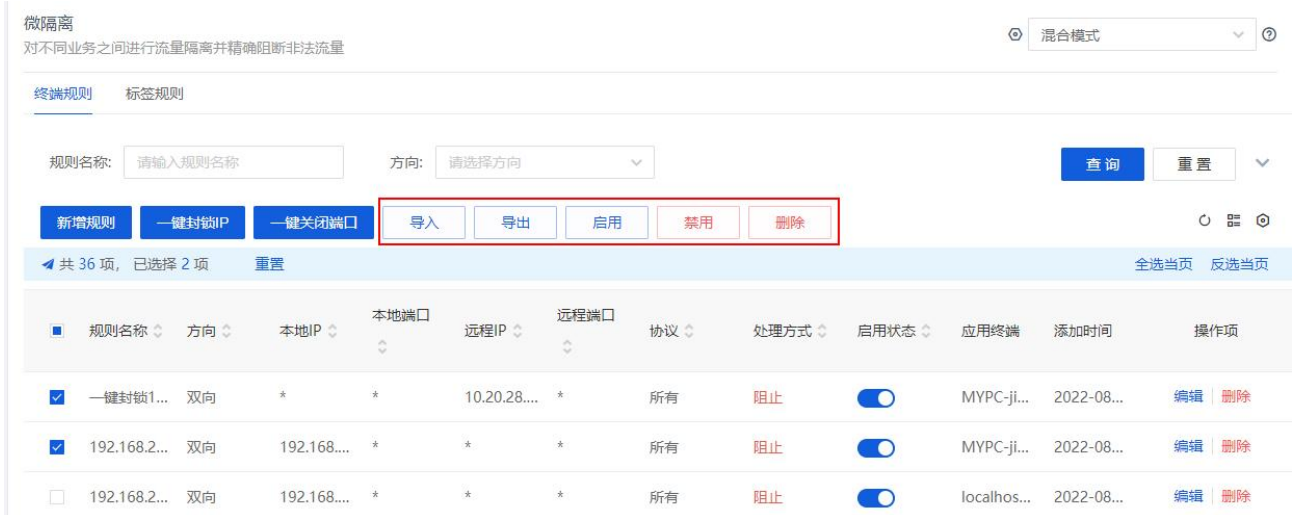
- 选择标签 (如 **Linux**), 点击<新增规则>, 可对标签下的终端新增微隔离规则。
- 选择标签 (如 **Linux**), 点击<一键封锁 IP>, 可对标签下的终端设置一键封锁 IP。
- 选择标签 (如 **Linux**), 点击<一键关闭端口>, 可关闭标签下的终端的相应端口。



15.1.1.3 其他操作

以租户角色登录主机安全系统管理平台,在导航栏选择“终端管理>微隔离”,选择混合模式,可执行以下操作:

- ◆ 点击<导出>, 可导出微隔离规则。
- ◆ 点击<导入>, 选择微隔离规则文件 (已导出的微隔离规则文件), 即可导入微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<启用>, 在弹出的对话框中点击<确定>, 可批量启用微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<禁用>, 在弹出的对话框中点击<确定>, 可批量禁用微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<删除>, 在弹出的对话框中点击<确定>, 可批量删除微隔离规则。



15.1.2 白名单模式

可以在白名单模式下配置标签规则，白名单内的规则默认放行，白名单外的规则默认阻止。

15.1.2.1 新增标签规则白名单

对某一标签下的终端设置微隔离规则白名单，操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>微隔离”，选择白名单模式，选择标签（如 PC），点击<新增规则>。



步骤 2. 在弹出的新增微隔离对话框中编辑相关信息，点击<确定>。

← 新增微隔离

* 规则名称 • 最多输入30个字符，可用于说明规则的用途

* 协议类型 必填项，请选择协议类型

规则类型 双向 进站规则 出站规则 • 进站（默认）表示远程主机访问本地主机，出站表示本地主机访问远程主机

* 本地IP

IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.2.1/24
192.168.3.1-192.168.3.255

• IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.1.1/24
192.168.1.1-192.168.1.255
"/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

* 本地端口

例如:
445

• 例如:
445
"*"表示所有端口、多个端口换行输入

* 远程IP

IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.2.1/24
192.168.3.1-192.168.3.255

• IP支持IPv4, 输入形式例如:
192.168.1.1
192.168.1.1/24
192.168.1.1-192.168.1.255
"/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

* 远程端口

例如:
445

• 例如:
445
"*"表示所有端口、多个端口换行输入

处理方式 放行 阻止

状态

* 应用终端 选择终端

确定
取消

详细配置请参见下表。

配置项	说明
规则名称	不超过 30 字符。
策略类型	<ul style="list-style-type: none"> ◆ 进站：规则仅应用于进站连接，即访问本机的请求。 ◆ 出站：规则仅应用于出站连接，即本机向外发送的请求。 ◆ 双向：规则应用于进站及出站两种连接。
本地端口	本地主机的端口，例如 455，输入多个请用回车间隔，“*”表示所有端口。
远程地址	远程主机的 IP 地址，标签与 IP 必填一项，两者都填则两者均生效。 <ul style="list-style-type: none"> ◆ 选择标签：选择终端标签。 ◆ 填写 IP：远程主机的 IP 地址、地址段、子网。
远程端口	远程主机的端口，例如 455，输入多个请用回车间隔，“*”表示所有端口。
协议类型	支持所有 TCP、UDP 和 ICMP。
状态	开启后规则白名单生效，关闭后规则白名单不生效。

15.1.2.2 其他操作

以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>微隔离”，选择白名单模式，可执行以下操作：

- ◆ 点击<导出>，可导出微隔离规则。
- ◆ 点击<导入>，选择微隔离规则文件（已导出的微隔离规则文件），即可导入微隔离规则。
- ◆ 勾选规则（可勾选多个），点击<启用>，在弹出的对话框中点击<确定>，可批量启用微隔离规则。
- ◆ 勾选规则（可勾选多个），点击<禁用>，在弹出的对话框中点击<确定>，可批量禁用微隔离规则。
- ◆ 勾选规则（可勾选多个），点击<删除>，在弹出的对话框中点击<确定>，可批量删除微隔离规则。



15.1.3 黑名单模式

可以在黑名单模式下配置标签规则，对黑名单内的规则进行阻止。

15.1.3.1 新增标签规则黑名单

对某一标签下的终端设置微隔离规则黑名单，操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“终端管理>微隔离”，选择黑名单模式，选择标签（如 PC），点击<新增规则>。



步骤 2. 在弹出的新增微隔离对话框中，编辑相关信息（配置方法与[微隔离配置](#)相同），点击<确定>。

← 新增微隔离

* 规则名称

* 协议类型 必填项, 请选择协议类型

规则类型 双向 进站规则 出站规则

* 本地IP

IP支持IPv4, 输入形式例如:
 192.168.1.1
 192.168.2.1/24
 192.168.3.1-192.168.3.255

* 本地端口

例如:
 445

* 远程IP

IP支持IPv4, 输入形式例如:
 192.168.1.1
 192.168.2.1/24
 192.168.3.1-192.168.3.255

* 远程端口

例如:
 445

处理方式 放行 阻止

状态

* 应用终端 选择终端

• 最多输入30个字符, 可用于说明规则的用途

• 进站 (默认) 表示远程主机访问本地主机, 出站表示本地主机访问远程主机

• IP支持IPv4, 输入形式例如:
 192.168.1.1
 192.168.1.1/24
 192.168.1.1-192.168.1.255
 "/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

• 例如:
 445
 "*"表示所有端口、多个端口换行输入

• IP支持IPv4, 输入形式例如:
 192.168.1.1
 192.168.1.1/24
 192.168.1.1-192.168.1.255
 "/"表示子网掩码, "-"表示IP段, 多个IP需换行输入

• 例如:
 445
 "*"表示所有端口、多个端口换行输入

确定
取消

15.1.3.2 其他操作

以租户角色登录主机安全系统管理平台, 在导航栏选择“终端管理>微隔离”, 选择黑名单模式页签, 可执行以下操作:

- ◆ 点击<导出>, 可导出微隔离规则。
- ◆ 点击<导入>, 选择微隔离规则文件 (已导出的微隔离规则文件), 即可导入微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<启用>, 在弹出的对话框中点击<确定>, 可批量启用微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<禁用>, 在弹出的对话框中点击<确定>, 可批量禁用微隔离规则。
- ◆ 勾选规则 (可勾选多个), 点击<删除>, 在弹出的对话框中点击<确定>, 可批量删除微隔离规则。

157

微隔离

对不同业务之间进行流量隔离并精确阻断非法流量

黑名单模式

PC
已设置 1 个规则
已关联 15 个终端 [查看](#)

数据库服务器
已设置 0 个规则
已关联 1 个终端 [查看](#)

BBS
已设置 0 个规则
已关联 0 个终端 [查看](#)

新增规则 导入 导出 启用 禁用 删除

请输入关键字

共 1 项, 已选择 1 项 重置 全选当页 反选当页

<input checked="" type="checkbox"/>	规则名称	方向	本地端口	远程地址	远程端口	协议	启用状态	添加时间	操作项
<input checked="" type="checkbox"/>	PC	入站	445	PC 192.168.	445	所有	<input checked="" type="checkbox"/>	2022-08-2...	编辑 删除

共 1 条 20条/页 < 1 > 前往 1 页

15.2 流量画像

流量画像通过绘制内网全景流量图，展示内网主机间的通信关系和内网主机对外通信情况，并可在发现威胁后对主机间通信进行一键阻断。

租户可通过流量画像功能查看全景流量图，并支持通过以下方式进行流量筛选：

- ◆ 通过 Windows 服务器、Linux 服务器、PC 机三类主机和端口、时间进行过滤查看。
- ◆ 通过自定义模板，可按终端分组、终端标签、终端名称、终端 IP（且/或）过滤查看。

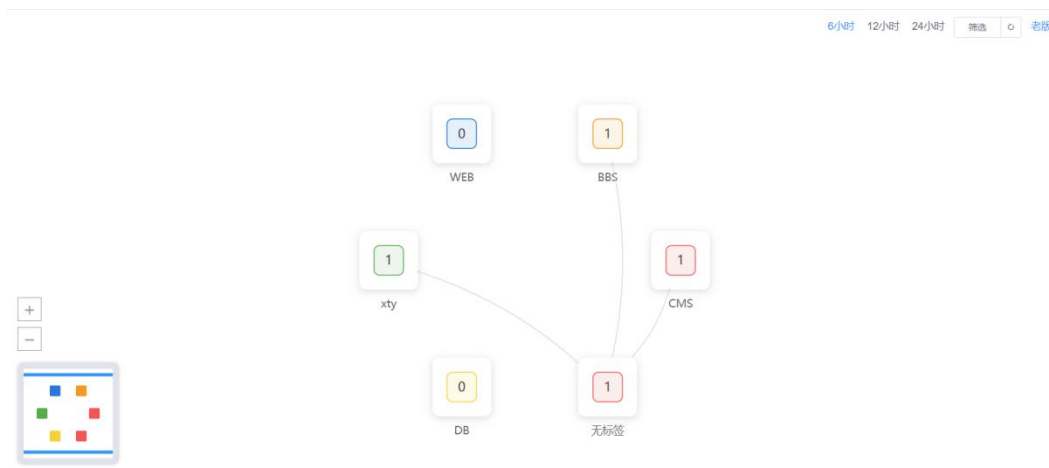
15.2.1 查看通信关系

租户可在此页面查看终端通信详情，包括终端通信关系图、终端间通信详情及终端全部通信详情。

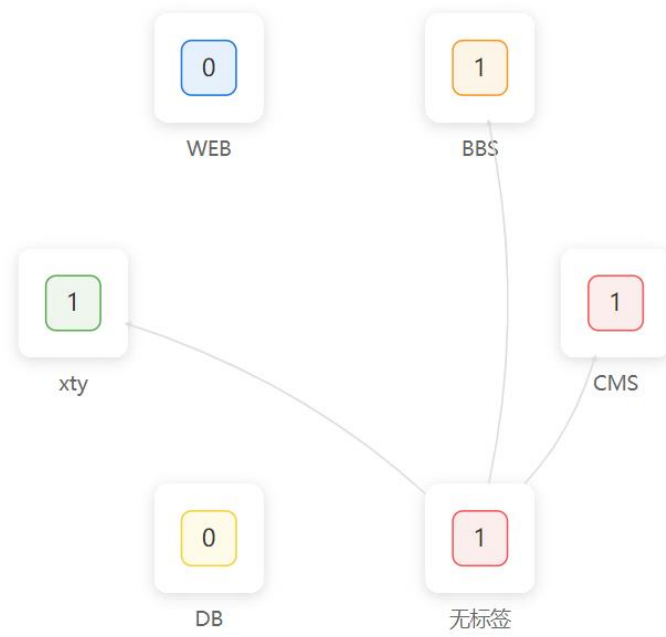
15.2.1.1 查看终端通信关系图

步骤 1. 以租户角色登录主机安全系统管理平台。

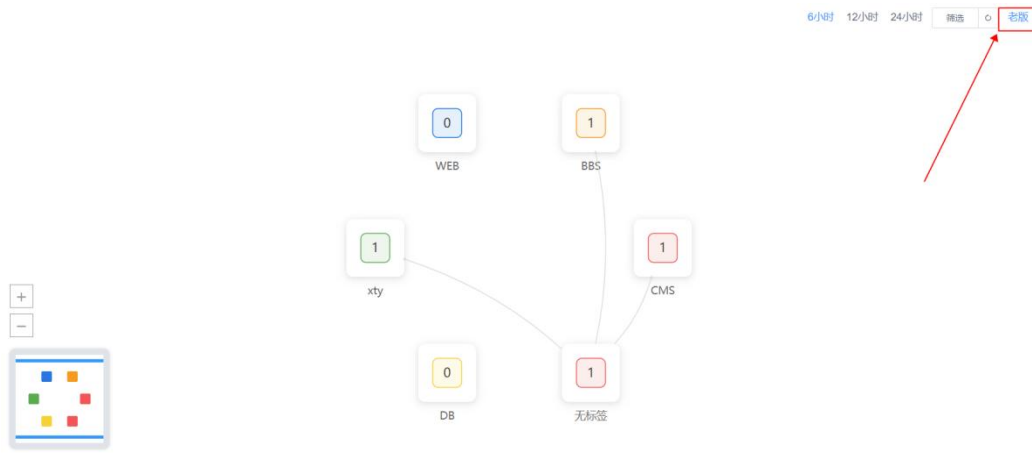
步骤 2. 在左侧导航栏选择“响应处置>流量画像”，进入终端展示页面。



步骤 3. 点击需要查看的终端的分组，可在此页面查看对应分组该终端的相关信息，和各个组之间的通信信息。



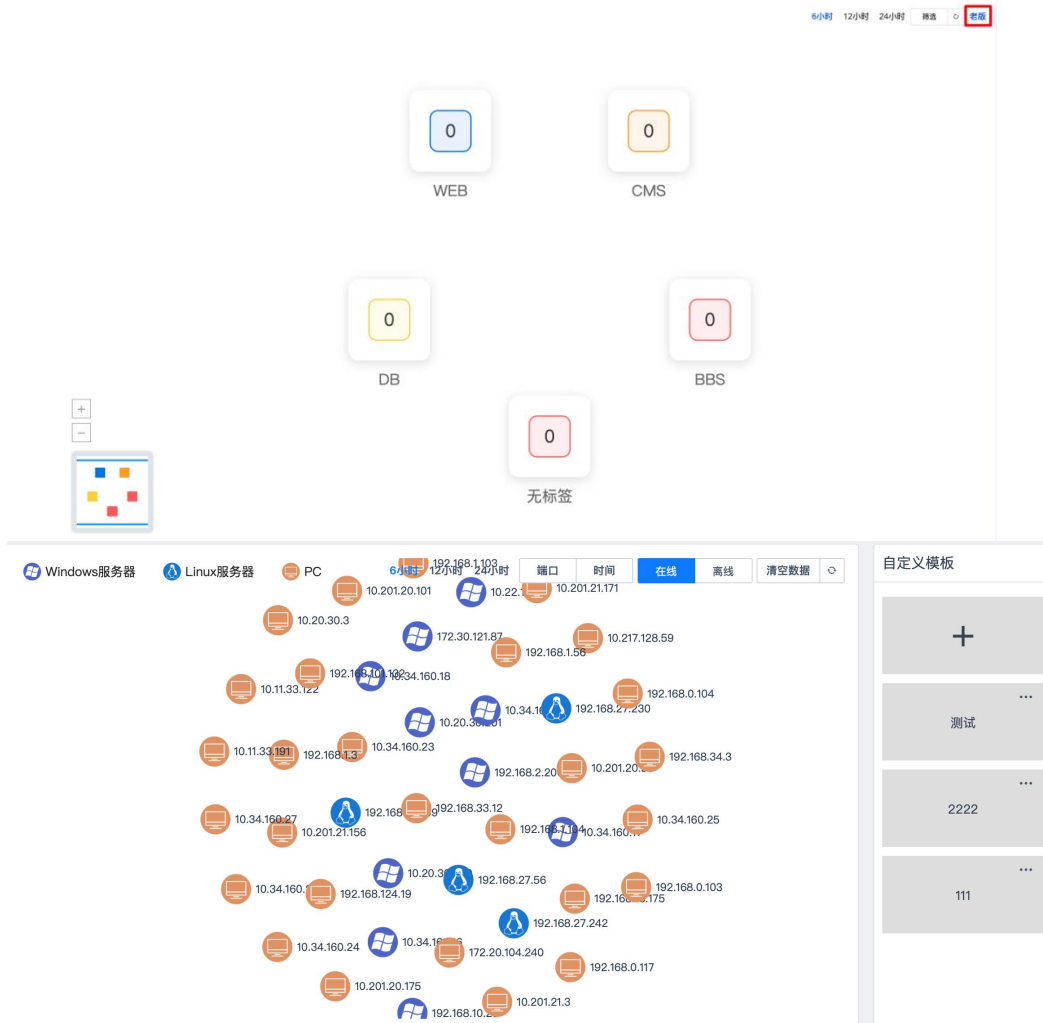
步骤 4. 点击页面右上角的<老版>，即可切换为老版本流量画像的相关功能页面。



15.2.1.2 查看终端通信关系详情

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>流量画像”，点击右上角<老版>，进入终端展示页面。



步骤 3. 点击需要查看的终端，并选择**通信关系列表**页签，进入**通信关系列表**详情页面。租户可在此页面查看该终端的所有通信详情，并可根据筛选条件进行通信查询。

WIN-29
192.168.10.29

通信关系图 **通信关系列表**

本地IP: 远程IP: 本地端口:

远程端口: 开始时间: 开始日期 - 结束日期

方向	本地IP	本地端口	远程IP	远程端口	协议	开始时间	上次通信时间	通信次数
出站	192.168.10.29	64889	120.201.21.171	80	TCP	2020-10-19 12:20:44	2020-10-19 12:20:44	1
出站	192.168.10.29	63145	104.201.21.171	443	TCP	2020-10-19 03:00:03	2020-10-19 03:00:03	1

15.2.2 自定义模板

通过自定义模板可查看对应分组或者标签的终端之间的通信关系。创建自定义模板的操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>流量画像”，点击右上角<老版>，进入终端展示页面，点击右侧自定义模板列表中的+图标。



步骤 3. 在弹出的对话框中输入自定义模板信息后点击<确定>，即可新增自定义模板。



步骤 4. 点击模板右上角的...图标，租户可对自定义模板进行编辑和删除操作。



15.3 文件推送

当租户需要下发文件、安装应用程序到终端上或者远程执行命令时，可以使用文件推送工具。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>文件推送”，进入文件推送页面。

- 1) 点击<上传文件>，选择文件（文件需要小于 20MB），即可上传文件。
- 2) 选择执行方式、执行权限及执行参数。
- 3) 点击<选择终端>，选择被推送的终端。

步骤 3. 点击<推送>即可成功推送该文件。



文件推送

文件上传

文件应该小于20M

下发后立即执行

执行权限 最高权限 当前账号

执行参数

备注:

推送给:

详细配置请参见下表。

参数	说明
上传文件	在此选择上传的文件或脚本，文件应小于 20MB。
下发后立即执行	如果需要立即执行文件，则开启立即执行。
执行权限	默认最高权限，部分程序和脚本无法用 system 权限执行，则选用当前账号。
执行参数	脚本需要执行时携带的参数。该功能必须在开启下发后立即执行选项后才可配置。 <ul style="list-style-type: none"> ◆ 原可执行程序默认执行无需参数时则执行参数选项留空。 ◆ 原可执行程序执行需要配置参数则执行参数选项填写实际参数。如原可执行程序运行命令为 push.sh filename 主机安全系统，则填写 filename 主机安全系统。

参数	说明
备注	关于此次文件推送的备注信息。
推送终端	点击<选择终端>，选择所需推送的终端。

◆ Windows 终端文件推送默认位置:



C:\Program Files \(\x86\)AppSecurity\主机安全系统\config\upload

◆ Linux 终端文件推送默认位置: /usr/local/appsecurity/主机安全系统
/config/upload

15.4 事件调查

能够对终端上的文件、进程、网络连接、DNS 查询、端口监听、账户、启动项、计划任务进行检索，实现相关安全事件的调查。

15.4.1 搜索事件数据

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“响应处置>事件调查”，输入关键字，点击<搜索>，即可搜索符合条件的事件信息。



15.4.2 配置数据采集

步骤 1. 点击页面右上方的<配置数据采集>。

请输入搜索内容 搜索 配置数据采集

全选 文件 进程 网络连接 DNS查询 端口监听 账户 启动项 计划任务



事件搜索·分析追溯

事件搜索数据来源于数据采集策略，搜索试试吧

步骤 2. 点击**状态**列的开关可启用或关闭对应项目的数据采集功能。

配置数据采集

类型	搜索结果	状态	操作项
文件	当文件创建, 修改, 删除时记录文件事件	<input checked="" type="checkbox"/>	设置
进程	当进程创建时记录进程事件	<input checked="" type="checkbox"/>	设置
网络连接	当连接外部IP端口时记录事件	<input checked="" type="checkbox"/>	设置
DNS查询	当查询外部DNS时记录事件	<input checked="" type="checkbox"/>	设置
端口监听	当进程创建监听端口时记录事件	<input checked="" type="checkbox"/>	设置
账户	当账户创建, 提权时记录事件	<input checked="" type="checkbox"/>	设置
启动项	当启动项创建, 删除时记录事件	<input checked="" type="checkbox"/>	设置
计划任务	当计划任务创建, 删除时记录事件	<input checked="" type="checkbox"/>	设置

步骤 3. 点击对应项（例如文件）的<设置>。

步骤 4. 在弹出的对话框中编辑相关信息，点击<确定>，即可设置数据采集策略。

文件设置

×

采集文件:

lic.conf

采集全部请填写*号, 多个对象用分号 (;) 分隔

Linux忽略文件:

Linux忽略路径:

/root

Linux忽略扩展名:

取消

确定

16 日志检索

报表：对事件趋势、病毒以及风险终端进行图表展示，支持导出各种类型报表。方便用户及时了解终端的防护信息。

日志检索是对记录系统以及终端的事件信息，包括防护日志、操作日志、运维日志等日志类型。支持按照分类及关键字进行搜索。

日志检索不同角色拥有不同的操作权限。

- ◆ admin 用户和租户都具有查看各自操作日志的权限。
- ◆ 仅租户角色具有防护日志、运维日志、日志报表等权限。

16.1 防护日志

租户可在**防护日志**页面查看系统防护日志、网络防护日志、Web 应用防护日志及自动响应日志。

16.1.1 查看防护日志

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**日志检索**▶**防护日志**”，设置查询条件（如时间、终端、分组、日志类型、风险评级、概况等），点击<**查询**>，即可查询符合该条件的操作日志。

步骤 3. 点击 > 图标，可查看防护日志详情。

终端名称	IP地址	日志类型	风险概况	风险评级	时间
HIRAMWONG8A70	192.168.1.1...	违规外联防护	已检测到主机存在违规外连行为，探测地址：www.baidu.com，未处理	高风险	2022-11-04 10:18:49
HIRAMWONG8A70	192.168.1.1...	违规外联防护	已检测到主机存在违规外连行为，探测地址：www.baidu.com，未处理	高风险	2022-11-03 16:58:17

步骤 4. 点击终端名称链接，可跳转至**策略管理**页面，详情请参考[策略管理](#)。

终端名称	IP地址	日志类型	风险概况	风险评级	时间
容器1	192.168.1.1...	病毒防护	发现恶意程序 C:\Users\admin\AppData\Roaming\快压\X86\vip.exe (TR/Crypt.Agent.gyhdn)，未处理	高风险	2022-11-10 00:31:51

16.1.2 导出防护日志

点击<**导出日志**>，选择文件格式（支持 CSV 和 Excel），可将所查询的防护日志导出至本地。



◆ 支持导出 CSV 格式和 Excel 格式。

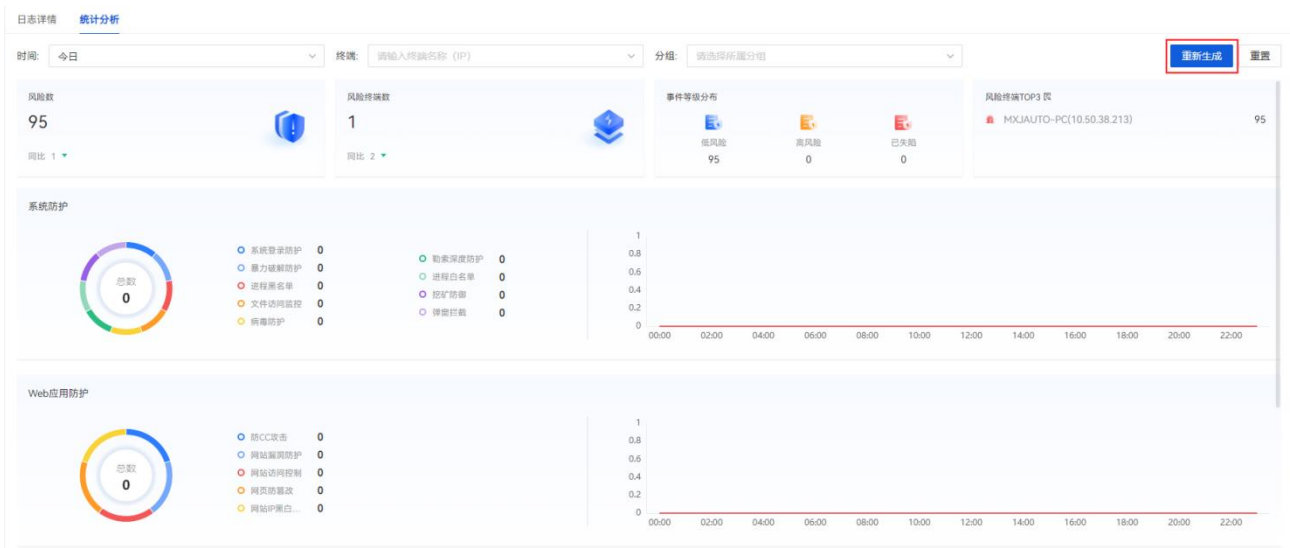


◆ 支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。

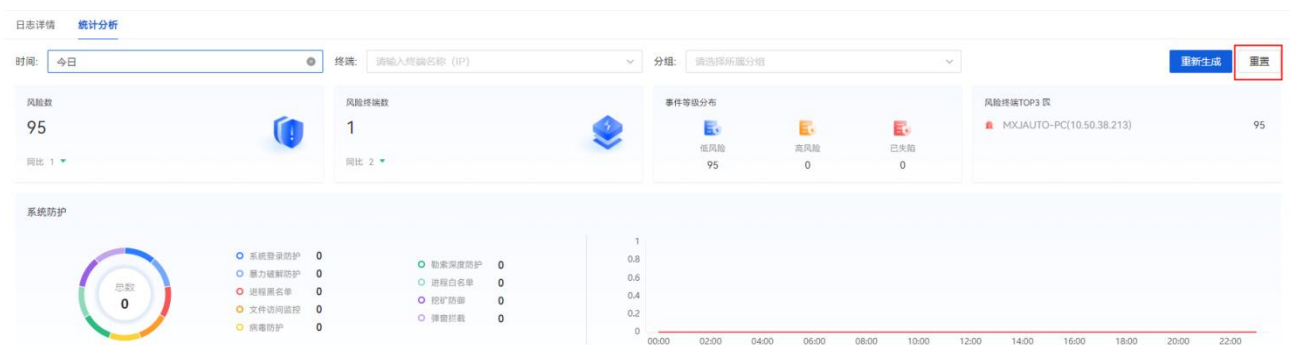
16.1.3 统计分析

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“日志检索>防护日志>统计分析”，选择时间、终端、分组后，点击<重新生成>按钮，即可查询符合该条件的防护日志统计分析结果。



步骤 3. 在左侧导航栏选择“日志检索>防护日志>统计分析”，点击<重置>按钮，即可重置该结果为默认时间统计结果。



16.2 操作日志

租户可在操作日志页面查看用户登录日志、修改密码日志、策略管理日志、分组标签日志、移动存储日志、告警配置日志、终端解绑日志、启停防护日志及短信发送日志。

16.2.1 查询操作日志

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“日志检索>操作日志”，设置查询条件（如时间、状态、日志类型、概况等），点击<查询>，即可查询符合该条件的操作日志。

用户	操作IP	日志类型	描述	时间	状态
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 14:26:21	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 13:59:21	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 10:20:46	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:45:45	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:23:16	成功
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 09:16:41	成功

16.2.2 导出操作日志

点击<导出日志>，选择文件格式（CSV 或 Excel），可将所查询的操作日志导出至本地。

用户	操作IP	日志类型	描述	时间	状态
autotest	10.23.72.115	日志操作	读取了防护日志数据记录	2023-10-12 14:26:21	成功



- ◆ 支持导出 CSV 格式和 Excel 格式。
- ◆ 支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。

16.3 运维日志

租户可在运维日志页面查看终端日志、性能监控日志、外设管控日志及运维日志。

16.3.1 查询运维日志

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“日志检索>运维日志”，设置查询条件（如终端、分组、时间、日志类型、概况等），点击<查询>，即可查询符合该条件的运维日志。

终端名称	IP地址	日志类型	概况	时间
> DESKTOP-FSHBSE6	10.23.72.160	终端升级	版本升级, 升级前的版本 3.0.7.104	2023-10-12 14:10:01
> DESKTOP-FSHBSE6	10.23.72.160	弱口令扫描	系统中有账号存在弱口令: admin	2023-10-12 10:48:48

16.3.2 导出运维日志

点击<导出日志>，租户可将所查询的运维日志导出至本地。



- ◆ 支持导出 CSV 格式和 Excel 格式。
- ◆ 支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。

16.4 篡改分析

- ◆ 需要管理员为租户启用防篡改许可后才具备篡改分析功能。

租户可对数据篡改事件，篡改结果和篡改目标源进行分析，展示攻击防护次数和高危风险终端 TOP10。操作方法如下：

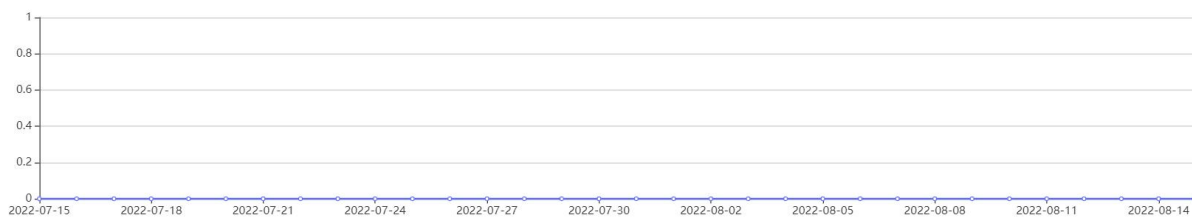
步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“日志检索>篡改分析”，进入篡改分析页面，选择时间，点击<生成报表>，可生成篡改分析报表。

篡改分析报表内容包括防篡改数据、网站篡改分析、篡改源分析、攻击防护次数统计、高危风险终端 TOP10、总体情况。

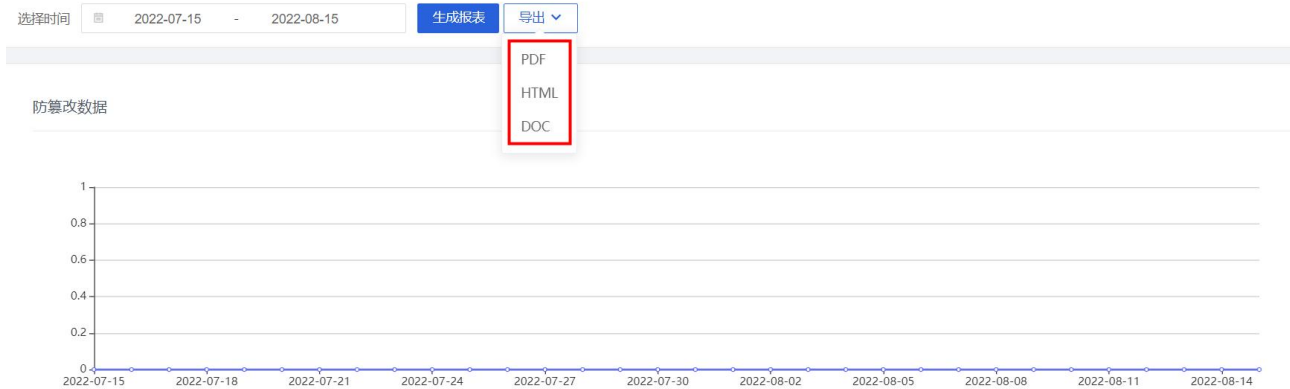


防篡改数据



网站篡改分析

步骤 3. 点击<导出>，选择文件格式（支持 PDF、HTML 和 DOC），可将篡改分析报告导出至本地。



16.5 日志报表

租户可在**日志报表**页面进行报表导出，或者报表订阅操作获取对应报表信息。

16.5.1 导出报表

步骤 1. 以租户角色登录主机安全系统管理平台，在导航栏选择“**日志检索**►**日志报表**”，选择**报表导出**页签。

步骤 2. 编辑报表标题（不超过 30 字符），选择**导出文件类型**（支持 PDF、HTML 和 Word），选择时间，点击<**立即导出**>，即可将所选时间段的日志报表导出至本地。

16.5.2 订阅报表

为方便租户及时了解终端防护状态信息，主机安全系统支持订阅报表功能。开启订阅报表功能后，系统会定期发送终端风险报表至配置的收件人邮箱。

设置报表订阅的操作方法如下：

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**日志检索**►**日志报表**”，选择**报表订阅**页签。

步骤 3. 开启**订阅开关**，配置报表标题、导出类型、执行时间及收件人邮箱，点击<**保存**>。

报表导出 报表订阅

发件箱请前往 [个人中心](#) [修改](#)

订阅开关:

报表标题:

导出类型: 日报 周报 月报

* 执行时间:

收件人邮箱:

文件类型: PDF HTML Word

17 终端全览

admin 用户在**终端全览**页面可查看终端的详细信息，并可以登录租户账号对终端进行管理。

仅 admin 用户角色具有终端全览权限。

17.1 查看终端详情

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**终端全览**”进入终端列表页面。

步骤 3. 可查看所有终端的详细信息，包括租户名、终端名称、IP 地址、MAC 地址、操作系统、终端版本、防护状态及操作项等。

租户名	终端名称	IP地址	MAC地址	操作系统	终端版本	终端状态	操作项
test	localhost.localdomain	10.0.2.15	08:00:27:00:00:0F	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
test	容器1	192.168.1.10	08:00:27:00:00:06	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
test	ADMIN-PC	10.0.2.15	08:00:27:00:00:0D	SUSE Linux Enterprise Server 11 (x86_64)	3.0.2.104	离线	前往租户
test	BOB-OFFICEPC	10.0.2.15	08:00:27:00:00:20	Windows 7 Ultimate Edition 64-bit	3.0.2.106	离线	前往租户
test	BOB-OFFICEPC	10.0.2.15	08:00:27:00:00:82	Windows 10 Professional 64-bit	3.0.2.108	离线	前往租户
test	centos5.0-x64-2.6.18-8	10.0.2.15	08:00:27:00:00:5E	CentOS release 5 (Final)	3.0.3.104	已卸载	前往租户
test	CENTOS7	192.168.1.111.129	08:00:27:00:00:1C	CentOS Linux 7 (Core)	3.0.3.104	离线	前往租户
test	DESKTOP-55U53T2	192.168.1.106.161	08:00:27:00:00:FA	Windows 10 64-bit	3.0.2.106	离线	前往租户
test	DESKTOP-64NLTVC	192.168.1.107.160	08:00:27:00:00:1C	Windows 10 64-bit	3.0.2.106	离线	前往租户

17.2 前往租户

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**终端全览**”进入终端列表页面。

步骤 3. 选择需要登录的终端，点击右侧**操作项**的**前往租户**，即可使用该租户账号登录主机安全系统管理平台对终端进行管理。

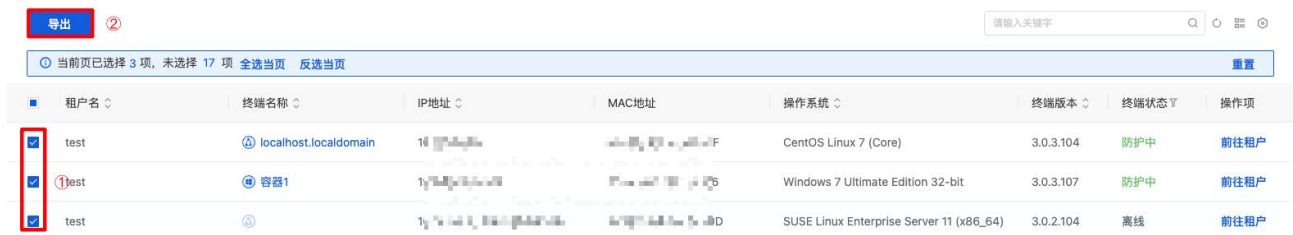
租户名	终端名称	IP地址	MAC地址	操作系统	终端版本	终端状态	操作项
test	localhost.localdomain	10.0.2.15	08:00:27:00:00:0F	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
test	容器1	192.168.1.10	08:00:27:00:00:06	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
test	ADMIN-PC	10.0.2.15	08:00:27:00:00:0D	SUSE Linux Enterprise Server 11 (x86_64)	3.0.2.104	离线	前往租户
test	ADMIN-PC	10.0.2.15	08:00:27:00:00:20	Windows 7 Ultimate Edition 64-bit	3.0.2.106	离线	前往租户

17.3 导出

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“终端全览”进入终端列表页面。

步骤 3. 选择需要导出的资产，点击<导出>，即可完成信息导出。



The screenshot shows a table of terminal assets with columns for tenant name, terminal name, IP address, MAC address, operating system, terminal version, terminal status, and actions. Three rows are visible, each with a checked checkbox in the first column. A red box highlights the '导出' (Export) button in the top left corner.

租户名	终端名称	IP地址	MAC地址	操作系统	终端版本	终端状态	操作项
<input checked="" type="checkbox"/> test	localhost.localdomain	10.10.10.10	08:00:27:00:00:00	CentOS Linux 7 (Core)	3.0.3.104	防护中	前往租户
<input checked="" type="checkbox"/> test	容器1	10.10.10.10	08:00:27:00:00:00	Windows 7 Ultimate Edition 32-bit	3.0.3.107	防护中	前往租户
<input checked="" type="checkbox"/> test		10.10.10.10	08:00:27:00:00:00	SUSE Linux Enterprise Server 11 (x86_64)	3.0.2.104	离线	前往租户



◆ 导出格式为 csv



◆ 不选择资产则默认导出全部内容

18 多级中心

多级中心用于下级中心连接上级中心，上级中心可以查看所有下级中心的部署情况以及风险数据。设置多级中心可减少主服务器的压力，减轻带宽占用，降低管理的成本；并解决分支机构、异地联动、多部门协同的难题。

仅 admin 用户具有多级中心操作权限。

18.1 查看中心详情

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“多级中心”进入多级中心总览页面，点击右上角<详情>。



步骤 3. 进入多级中心详情页面，可查看该中心数据信息、病毒趋势、终端-病毒排行、终端-漏洞排行、威胁 IP-TOP5 及事件类型占比等数据。



18.2 配置上级中心

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“多级中心”进入多级中心总览页面，点击<配置上级>。

步骤 3. 在弹出的对话框中输入上级控制中心地址和端口，点击<连接上级>，即可配置上级中心。

18.3 其他操作

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“多级中心”，进入多级中心总览页面，可对下级中心进行编辑、查看及删除操作。

勾选多个下级中心后点击列表上方的<删除>，可进行批量删除操作。

系统管理是指对系统的维护以及对系统资源进行管理，使系统更好地适配实际使用场景。

在**系统管理**页面，不同角色拥有不同的操作权限。

- ◆ 仅 admin 用户具有控制端系统管理权限。
- ◆ 仅租户角色具有客户端系统管理权限。

19.1 Admin 账户系统管理

admin 用户可在**系统管理**页面进行客户端及库升级、管理平台升级、Windows 补丁库、平台管理、个性化等操作。

19.1.1 客户端及库升级

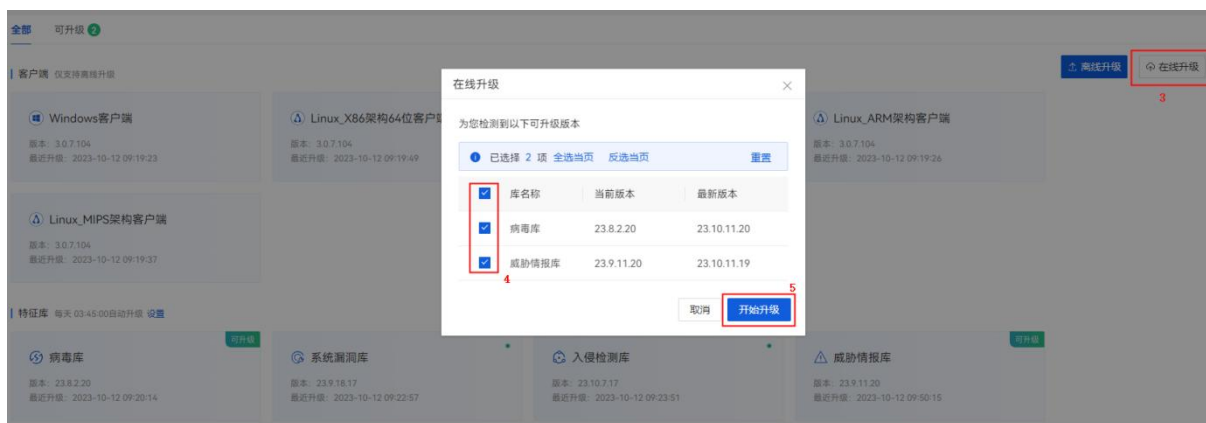
admin 用户可在此页面查看客户端及特征库当前版本信息，并可上传离线包进行离线升级或者在线升级特征库。

19.1.1.1 在线升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理>客户端及库升级**”，进入**客户端及库升级**页面。

步骤 3. 点击<**在线升级**>，选择需要升级的库，点击开始升级即可完成库的在线升级。



步骤 4. 通过每个特征库或者客户端方框**历史记录**，可以查看升级成功或者失败的对应记录。



Linux_X86架构64位客户端

历史升级记录

升级时间	升级前版本	当前版本	方式	是否成功
2023-10-12 09:19:51	3.0.7.104	3.0.7.104	离线升级	升级成功
2023-10-11 13:56:05	--	3.0.7.104	离线升级	升级成功
2023-10-11 13:44:16	--	--	离线升级	升级失败

共 3 条 < 1 > 20条/页 前往 1 页

关闭

19.1.1.2 离线升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>客户端及库升级”，进入客户端及库升级页面。

步骤 3. 点击<离线升级>，上传文件，即可完成客户端及库的离线升级。



上传的离线升级包后缀名必须为.tar.gz。

离线安装升级一体包获取路径：登录社区找到主机安全系统产品，在菜单栏选择“产

品>网络安全基础产品>安全防护产品>天翼云主机安全系统（主机安全系统）”，点击“版本软件”，选择对应中心架构后下载安装升级一体包。

19.1.1.3 自动升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>客户端及库升级”，进入客户端及库升级页面。

步骤 3. 点击<自动升级设置>，可以设置是否在线升级、执行时间、升级代理，点击确定按钮即完成了自动升级设置。



步骤 4. 点击<测试网络>，可以测试当前平台是否可以正常访问升级服务器。

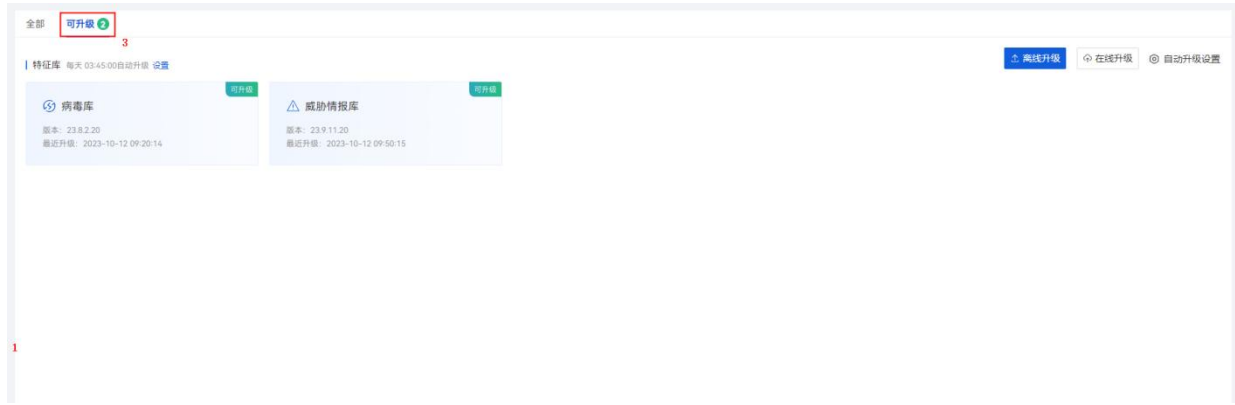


19.1.1.4 可升级

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>客户端及库升级”，进入客户端及库升级页面。

步骤 3. 选择“可升级”，即能看到可升级的客户端及库。



步骤 4. 右上角有可升级标识的说明此库可以进行升级。

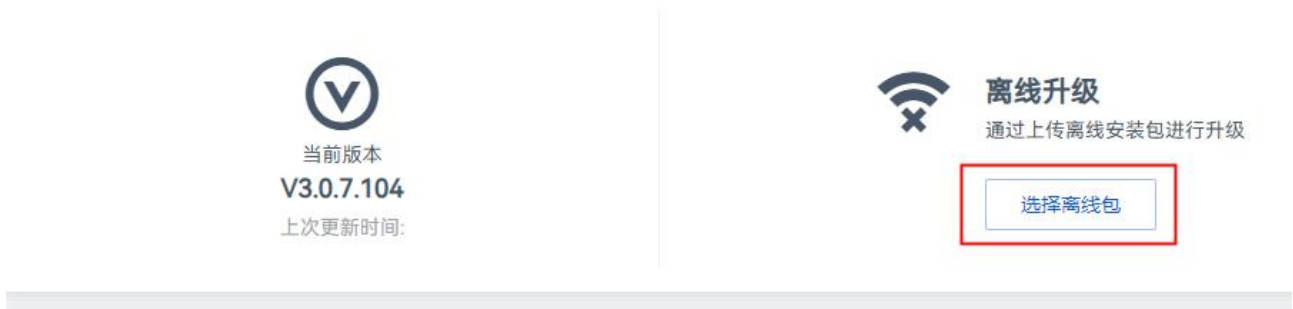


19.1.2 管理平台升级

admin 用户可在此页面查看平台当前版本信息，并可上传离线包对平台进行离线升级。

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>管理平台升级”进入管理平台升级页面。点击<选择离线包>，系统将进行自动清理缓存。



注意事项

- 升级过程平台任务将不能正常进行，请确保升级过程中没有重要的任务进行。
- 升级过程中，请勿刷新浏览器，避免刷新导致升级失败。
- 升级完成后，系统将自动重启。
- 离线升级安装包仅支持.tar.gz格式。

步骤 3. 缓存清理完毕后，在弹出的对话框中点击<点击上传>，上传离线包后即可进行平台离线升级。



19.1.3 Windows 补丁库

- ◆ 上传的离线升级包后缀名必须为.tar.gz。
- ◆ 升级过程中，请勿刷新浏览器，避免刷新导致升级失败。
- ◆ 升级完成后，系统将自动重启。




用户可在 **Windows 补丁库管理** 页面查看补丁详情，并进行在线更新补丁及离线更新补丁操作。

19.1.3.1 查看已下载补丁

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理>Windows 补丁库管理**”，选择**已下载补丁**页签。

步骤 3. 进入**已下载补丁**页面，用户可查看已下载的漏洞补丁列表。同时可在此页面查看漏洞分类及漏洞补丁详情，并对漏洞补丁进行查询、忽略、删除及取消忽略操作。

- 点击**操作项**列中的  图标，在弹出的对话框中点击<确定>，可忽略漏洞补丁。
- 点击**操作项**列中的  图标，在弹出的对话框中点击<确定>，可取消忽略漏洞补丁。
- 点击**操作项**列中的  图标，在弹出的对话框中点击<确定>，可删除漏洞补丁。
- 勾选多个补丁后点击列表上方的<忽略>、<取消忽略>或<删除>，可进行批量忽略、批量取消忽略及批量删除操作。

已下载补丁 在线更新补丁 离线更新补丁

发布日期: 开始日期 - 结束日期 下载日期: 开始日期 - 结束日期 关键字: 请输入关键字

忽略状态: 请选择 ^

 已下载补丁: 80个

<input type="checkbox"/>	漏洞补丁描述	发布日期	补丁大小	适用系统	下载日期	操作项
<input type="checkbox"/>	2022-适用于 Windows 10 Version 1507 的 05 服务堆栈更新, 适合基于 x6...	2022-05-10	11.60MB	win10	2022-05-20	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2022-适用于 Windows 10 Version 1909 的 05 累积更新, 适合基于 x64 的...	2022-05-10	563.35MB	win10	2022-05-20	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 2004 的 12 累积更新, 适合基于 x64 的...	2021-12-14	602.96MB	win10	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 1607 和 Windows Server 2016 的 09 ...	2021-09-13	11.50MB	win2k16	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 1809 和 Windows Server 2019 的 08 ...	2021-08-09	13.60MB	win2k19	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 2004 和 Windows 10 Version 20H2 和...	2021-08-09	14.50MB	win10	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 1909 的 08 服务堆栈更新, 适合基于 x6...	2021-08-09	14.40MB	win10	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>
<input type="checkbox"/>	2021-适用于 Windows 10 Version 1803 的 05 服务堆栈更新, 适合基于 x6...	2021-05-11	13.20MB	win10	2022-01-21	<input type="button" value="刷新"/> <input type="button" value="删除"/>

19.1.3.2 在线更新补丁

主机安全系统管理中心可连接互联网时，可以在线更新补丁。操作方法如下：

- 步骤 1. 以 admin 用户登录主机安全系统管理平台。
- 步骤 2. 在左侧导航栏选择“系统管理>Windows 补丁库管理”，选择在线更新补丁页签。
- 步骤 3. 进入在线更新补丁页面，点击<下载补丁>。



步骤 4. 在弹出的对话框中选择操作系统类型及漏洞级别，点击<确定>。



19.1.3.3 离线更新补丁

主机安全系统管理中心无法连接互联网时，可离线更新补丁库。操作方法如下：

步骤 1. 以 admin 用户登录主机安全系统管理平台。

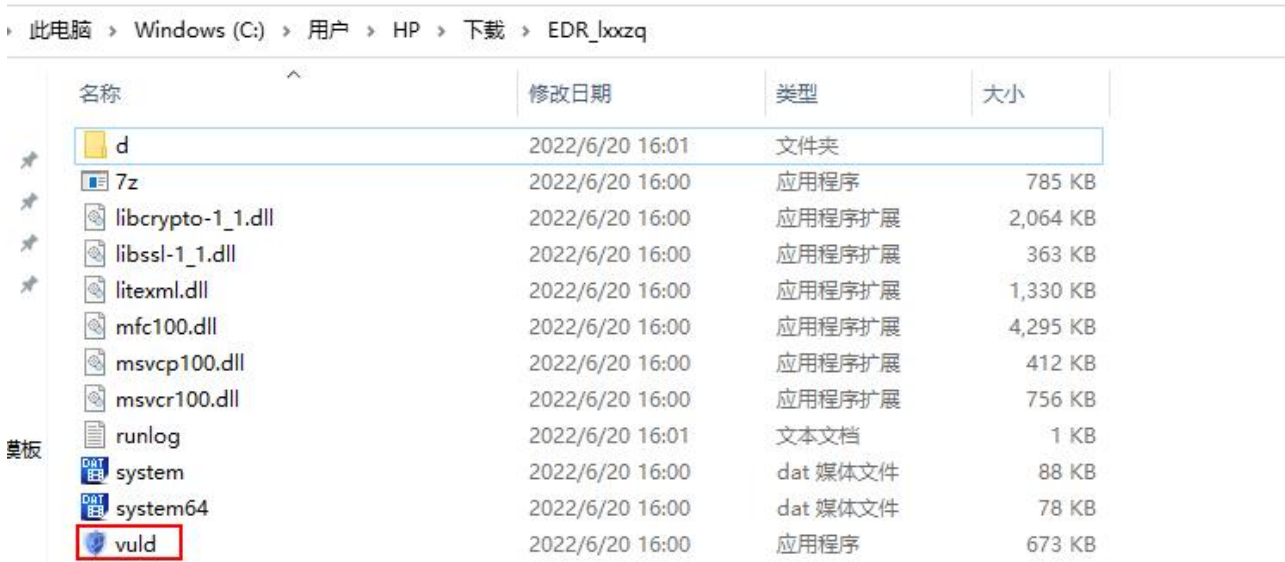
步骤 2. 在左侧导航栏选择“系统管理>Windows 补丁库管理”，选择离线更新补丁页签。

步骤 3. 进入离线更新补丁页面，点击<下载>，下载离线下载器。



步骤 4. 下载器下载成功后，可通过下载器离线下载补丁包。

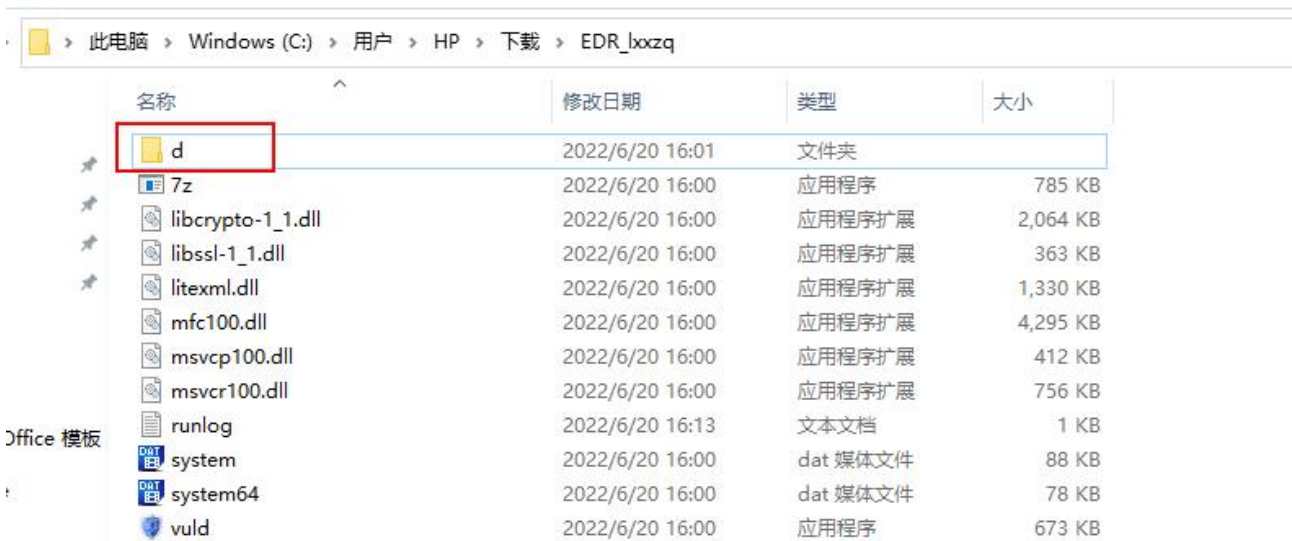
- 1) 解压下载后的压缩包。
- 2) 在解压后的文件中双击“vuld.exe”文件运行下载器程序。



- 3) 在下载器界面中勾选操作系统类型，选择 32 位或 64 位系统补丁，选择漏洞级别，点击<开始下载>，即可离线下载漏洞补丁。



4) 下载的漏洞补丁文件将会保存在解压文件夹目录下。



步骤 5. 点击<上传文件>，可将离线补丁包上传至管理中心，进行补丁离线更新。

上传完成后，租户角色登录主机安全系统管理平台即可对相应终端进行漏洞修复。

EDR管理中心无法联互联网时，建议离线更新补丁库

- ① 下载离线下载器
 下载后，可通过下载器离线下载补丁包
- ② 上传离线补丁包
 上传离线补丁包到管理中心

根据中心和端主机是否可访问互联网的情况，可通过以下方式获取漏洞补丁。

联网情况	获取方式
只有中心可访问互联网	admin 用户登录主机安全系统管理平台，在左侧菜单栏选择“ 系统管理 ▶ Windows 补丁库管理 ”，下载补丁后推送给端主机修复。
只有端可访问互联网	<ul style="list-style-type: none"> ◆ 中心已下载过的补丁仍由中心推送给端主机修复。 ◆ 中心未下载过的由端主机下载进行修复，检测出漏洞后直接点击修复即可。
中心和端都不可访问互联网	admin 用户登录主机安全系统管理平台，离线上传补丁后，中心推送补丁至端主机进行漏洞修复。
中心和端都可访问互联网	<ul style="list-style-type: none"> ◆ 中心已下载过的补丁由中心推送给端主机进行漏洞修复。 ◆ 中心未下载过的补丁由端主机下载后进行漏洞修复。

19.1.4 密码及访问策略

用户可在**密码及访问策略**页面配置密码及访问策略。

19.1.4.1 密码策略

步骤 1. 以 **admin** 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理**▶**密码及访问策略**”进入**密码及访问策略**页面。

步骤 3. 配置密码策略信息，点击<**提交**>，即可配置密码策略。

密码策略

口令最小长度:

至少包括以下几种策略:
密码策略仅包含以下策略组合, 密码中不允许包含空格

策略类型: 大写字母 小写字母 数字 特殊字符

密码有效期: 天
建议设置90天有效期, 过期后用户密码需强制更改
支持设置0-360天, 0表示永不过期

详细配置请参见下表。

参数	说明
口令最小长度	取值范围 8~50。
至少包括以下几种策略	设置密码需要包含的字符类型种类, 取值范围 2~4。
策略类型	密码策略类型
密码有效期	建议设置 90 天有效期, 过期后用户密码需强制更改 支持设置 0-360 天, 0 表示永不过期



- ◆ 新升级到 V3.0.3 版本默认 0 天, 此功能不生效, 需要重新设置;
- ◆ 新安装 V3.0.3 版本默认 90 天。

19.1.4.2 访问策略

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理**”>“**密码及访问策略**”进入**密码及访问策略**页面。

步骤 3. 配置访问策略信息, 点击<**提交**>, 即可配置访问策略。

访问策略

登录限制IP:
192.168.1.1; 192.168.1.1-192.168.1.255
不填表示不限制IP, "*"表示所有IP, "-"表示IP段, 多个IP需换行输入

验证码开关:

身份验证器作用范围: 登录时 高危操作二次认证

详细配置请参见下表。

参数	说明
----	----

参数	说明
登录限制 IP	不填表示不限制 IP，“*”表示所有 IP、“-”表示 IP 段，多个 IP 需换行输入，例如：192.168.1.1；192.168.1.1-192.168.1.255
验证码开关	开启时，用户登录系统 Web 管理平台需要输入验证码。
身份验证器	用户可选择在登录时或者高危操作时使用双因子认证。



身份验证器中高危操作包括文件推送、远程协助、重启终端、关机等操作。

19.1.4.3 租户策略模板

步骤 1. 以 admin 用户登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>密码及访问策略”进入密码及访问策略页面。

步骤 3. 配置租户策略模板信息，点击<提交>，即可配置租户策略模板策略。



详细配置请参见下表。

参数	说明
修改策略模板	设置是否允许租户修改策略模板，同时允许租户修改下支持配置时间段。 例：选择 00:00:00~23:59:59 表示任意时间段租户均可修改策略模板 选择 08:00:00~23:59:59 表示该时间段内租户可修改策略模板，其余时间段不允许 选择“不允许修改”表示任意时间段均禁止修改策略模板

19.1.5 部署管理

用户可在部署管理页面对日志保留天数进行设置。超过日志保留天数后，将清理最早日期的日志。

以 admin 用户登录主机安全系统管理平台，在导航栏选择“系统管理>部署管理”，进入部署管理页面。设置日志保留天数，点击<应用配置>。

日志保留: 天

日志默认保留180天, 可以在此定义日志保留时长, 如您的日志占用磁盘已超过80%, 建议调整日志保留的时间

应用配置

19.1.6 个性化

用户可在**个性化**页面对 Logo、登录背景、厂商公司名称、厂商英文缩写、客户端名称进行设置, 以满足个性化需求或者 oem 需求。

19.1.6.1 个性化

以 admin 用户登录主机安全系统管理平台, 在导航栏选择“**系统管理**▶**个性化**”, 进入**个性化**页面。填写个性化内容, 点击<保存>。

个性化

产品名称:
替换平台产品名称

客户端名称:
替换客户端注册信息、桌面快捷方式、客户端显示名称等。例如: XXX主机卫士

LOGO: 
点击替换图片, 像素256*256, 格式为“.png”, 上传后将更换平台及客户端LOGO图标

登录背景: 
点击替换图片, 像素1920*1080, 格式为“.png”, 上传后将更换WEB管理平台登录背景

厂商公司名称:
替换厂商名称相关标识、注册信息厂商等。例如: XXX有限责任公司

厂商英文缩写:
替换客户端部署目录等信息。例如: XXXSecurity

详细配置请参见下表。

参数	说明
LOGO	像素 256*256, 格式为 “.png”, 上传后将更换平台及客户端 LOGO 图标
产品名称	替换平台产品名称
登录背景	像素 1920*1080, 格式为 “.png”, 上传后将更换 WEB 管理平台登录背景

参数	说明
厂商公司名称	替换厂商名称相关标识、注册信息厂商等。例如：XXX 有限责任公司
厂商英文缩写	替换客户端部署目录等信息。例如：XXXSecurity
客户端名称	替换客户端注册信息、桌面快捷方式、客户端显示名称等。例如：XXX 主机卫士



- ◆ 个性化参数生效于管理中心平台和新装的客户端的终端，个性化参数配置后终端需重装在线/离线部署新生成客户端才能调整为个性化界面和相关名称显示。
- ◆ 支持 openapi 配置个性化相关参数。

19.1.6.2 恢复默认

以 admin 用户登录主机安全系统管理平台，在导航栏选择“系统管理>个性化”，进入个性化页面。点击<恢复默认>以此恢复出厂信息。



19.2 租户账户系统管理

租户可在此页面进行部署管理、许可分配、告警配置及个人中心等操作。

19.2.1 部署管理

19.2.1.1 添加终端

租户可在添加终端页面查看连接管理中心时所需要的管理员识别码（UUID），并进行系统终端添加。终端添加前可为终端选择分组，不选择的情况下系统会自动选择分组（PC 组、Windows 服务器组、Linux 服务器组）。

19.2.1.1.1 配置终端

租户可对新增终端配置并复制联动所需的 APIKEY，并设置离线定期删除、客户端绑定地址、绑定分组。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>部署管理”，选择添加终端页签。

步骤 3. 点击<设置>。



Windows系统

Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10/ Windows 11
Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 / Windows Server 2016 / Windows Server 2019/ Windows Server 2022

离线安装: 下载安装包, 拷贝到主机上进行安装。

https://.../service/file/download2?name=edr_download/windows/ceshi/.../10571/1/win_installer_1.../VR002ae6.exe

下载

复制

在线安装: Win7及以上系统, 以管理员权限运行CMD程序, 复制以下命令进行安装。

```
powershell -executionpolicy bypass -c "$client = new-object System.Net.WebClient; $client.Headers['User-Agent'] = 'edr_agent/2.0(http request using rpc protocol)'; $client.DownloadFile('http://.../10571/download/windows/win_installer.exe', $ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('win_installer.exe')); $proc = Start-Process .win_installer.exe -ArgumentList @{'--uuid VR002ae6 --center ... --ui 0'} -Verb runas -PassThru; $proc.WaitForExit()"
```

复制

步骤 4. 在弹窗中配置相关内容, 点击<确定>保存配置。

×

APIKEY值: 0YmAspPYshWjU3HrWBokdA== [复制](#)

自动删除: 超过 天未上线自动删除离线终端

* 绑定地址: [安装客户端, 默认绑定至IP](#)

自动分组: [安装客户端, 默认绑定至分组](#)

详细配置请参见下表。

参数	说明
自动删除	设置是否开启自动删除策略, 开启后, 当终端未上线时间达到设置值时会删除离线终端。当总终端数量较多且有部分终端长时间离线时建议开启此功能。
绑定地址	安装客户端需要绑定管理中心, 默认不用修改此配置。
自动分组	安装客户端后, 客户端所在终端将绑定至指定分组。默认为自动选择, 请根据实际进行设置。

19.2.1.1.2 添加 Windows 系统终端

以租户角色登录主机安全系统管理平台, 在左侧导航栏选择“系统管理>部署管理”, 选择添加终端页签, 租户可在 **Windows 系统**区域进行 Windows 系统终端的离线安装及在线安装。

◆ 离线安装

- **方式一:** 点击**离线安装**的<下载>, 下载客户端安装包, 以管理员权限将安装包拷贝到终端服务器上, 双击安装程序, 执行安装。
- **方式二:** 点击**离线安装**的<复制>, 复制客户端安装包下载链接。以管理员权限登录终端服务器, 在浏览器地址栏中粘贴下载链接并回车, 进行客户端安装包本地下载。下载完成后双击安装程序, 执行安装。



Windows系统

Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10 / Windows 11
Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022

离线安装: 下载安装包, 拷贝到主机上进行安装。

https://10.105.105.71/service/file/download2?name=edr_download/windows/ceshi/10571/1/win_installer_1_VR002ae6.exe

下载 复制

在线安装: Win7及以上系统, 以管理员权限运行CMD程序, 复制以下命令进行安装。

```
powershell -executionpolicy bypass -c "$client = new-object System.Net.WebClient; $client.Headers['User-Agent'] = 'edr_agent/2.0(http request using rpc protocol)'; $client.DownloadFile('http://10.105.105.71/download/windows/win_installer.exe', $ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('win_installer.exe')); $proc = Start-Process ./win_installer.exe -ArgumentList @('--uid VR002ae6 --center 10.105.105.71 --ui 0') -Verb runas -PassThru; $proc.WaitForExit()"
```

复制

◆ 在线安装

点击**在线安装**的<复制>, 复制安装链接, 在客户端上使用 **cmd** 执行该命令进行一键安装。



Windows系统

Windows XP SP3 / Windows Vista / Windows 7 / Windows 8、8.1 / Windows 10 / Windows 11
Windows Server 2003 SP2 / Windows Server 2008、2008R2 / Windows Server 2012、2012R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022

离线安装: 下载安装包, 拷贝到主机上进行安装。

https://10.105.105.71/service/file/download2?name=edr_download/windows/ceshi/10571/1/win_installer_1_VR002ae6.exe

下载 复制

在线安装: Win7及以上系统, 以管理员权限运行CMD程序, 复制以下命令进行安装。

```
powershell -executionpolicy bypass -c "$client = new-object System.Net.WebClient; $client.Headers['User-Agent'] = 'edr_agent/2.0(http request using rpc protocol)'; $client.DownloadFile('http://10.105.105.71/download/windows/win_installer.exe', $ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('win_installer.exe')); $proc = Start-Process ./win_installer.exe -ArgumentList @('--uid VR002ae6 --center 10.105.105.71 --ui 0') -Verb runas -PassThru; $proc.WaitForExit()"
```

复制

19.2.1.1.3 添加 Linux 系统终端

以租户角色登录主机安全系统管理平台, 在左侧导航栏选择“**系统管理**▶**添加终端**”, 选择**添加终端**页签。租户可在 **Linux 系统**区域进行 Linux 系统终端的离线安装及在线安装。

◆ 离线安装

选择 CPU 架构以及操作系统位数, 点击**离线安装**的<下载>, 下载安装包, 并复制脚本命令。将软件包拷贝到服务器上进行解压, 执行脚本命令进行安装即可。



Linux系统

支持Centos5.0+, Redhat5.0+, Suse11+, Ubuntu 14+, debian等主流发行版本操作系统;
国产系统: 统信UOS、银河麒麟、中标麒麟、中科方德、欧拉、龙芯、深度、凝思、磐石、红旗等。

离线安装: 选择CPU架构以及操作系统位数下载安装包, 拷贝到服务器上解压后执行脚本进行安装。

x86架构 64位操作系统 1
tar --no-same-permissions --no-s 32位操作系统 3,7.104.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh

2 3
下载 复制

在线安装: 下载以管理员权限执行以下命令进行

wget --no-check-certificate http:// 64位操作系统(统信签名deb包) totest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && ./agent_setup.sh
64位操作系统(麒麟签名deb包)

复制

批量安装: 通过SSH远程方式, 批量安装Agent。

上传文件

请下载 批量安装模板, 按照模板要求填写服务器IP等信息, 并上传文件。安装前需保证管理中心已安装expect插件。

◆ 在线安装

点击**在线安装**的<复制>, 复制下载链接, 在客户端上以管理员权限执行该命令进行安装。



Linux系统

支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+、debian等主流发行版本操作系统；
国产系统：统信UOS、银河麒麟、中标麒麟、中科方德、欧拉、龙蜥、深度、凝思、磐石、红旗等。

离线安装：选择CPU架构以及操作系统位下载安装包，拷贝到服务器上解压后执行脚本进行安装。

x86架构 64位操作系统 下载 复制

```
tar --no-same-permissions --no-same-owner -zxvf linux_agent_setup_3.0.7.104.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh
```

在线安装：下载以管理员权限执行以下命令进行安装。

```
wget --no-check-certificate http://10.50.121.11:10571/download/linux/autotest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && ./agent_setup.sh
```

复制

批量安装：通过SSH远程方式，批量安装Agent。

上传文件

请下载 批量安装模板，按照模板要求填写服务器IP等信息，并上传文件。安装前需保证管理中心已安装expect插件。

◆ 批量安装

点击**批量安装**的<下载>，获取批量安装模板。按照模板要求填写服务器 IP 等信息，填写完成后点击<上传文件>，上传编辑好的模板文件，进行客户端批量安装。



Linux系统

支持Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+、debian等主流发行版本操作系统；
国产系统：统信UOS、银河麒麟、中标麒麟、中科方德、欧拉、龙蜥、深度、凝思、磐石、红旗等。

离线安装：选择CPU架构以及操作系统位下载安装包，拷贝到服务器上解压后执行脚本进行安装。

x86架构 64位操作系统 下载 复制

```
tar --no-same-permissions --no-same-owner -zxvf linux_agent_setup_3.0.7.104.x64.tar.gz && chmod +x install_edr.sh && ./install_edr.sh
```

在线安装：下载以管理员权限执行以下命令进行安装。

```
wget --no-check-certificate http://10.50.121.11:10571/download/linux/autotest/10.50.121.11_10571/1/agent_setup.sh -O agent_setup.sh && chmod +x agent_setup.sh && ./agent_setup.sh
```

复制

批量安装：通过SSH远程方式，批量安装Agent。

上传文件

请下载 批量安装模板，按照模板要求填写服务器IP等信息，并上传文件。安装前需保证管理中心已安装expect插件。

上传文件前需保证管理中心已安装 **expect** 插件。查看安装 **expect** 插件的操作步骤如下。

步骤 1. 以 **root** 用户登录管理端服务器的操作系统 CLI 界面，执行 **expect** 命令，查看是否有返回结果。若有返回结果，则说明管理中心已安装 **expect** 插件。若没有返回结果，则执行下一步进行插件安装。

```
[root@localhost yum.repos.d]# expect
expect1.1>
expect1.1>
expect1.1>
expect1.1>
```

步骤 2. 使用 **rpm** 包安装方式安装 **expect** 插件，执行 **rpm -ivh rpm 包文件名** 进行安装。

支持添加的终端操作系统版本如下表所示。

系统	版本
Windows 系统	支持 Windows XP、Windows 7、Windows 8、Windows 10、Windows 11、Windows Server 2003、Windows Server 2008、Windows Server 2008R2、Windows Server 2012、Windows Server 2016、Windows Server 2019、Windows Server 2022 等版本操作系统。
Linux 系统	支持 Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+、debian 等主流发行版本操作系统； 国产系统：统信 UOS、银河麒麟、中标麒麟、中科方德、欧拉、龙蜥、深度、

系统	版本
	凝思、磐石、红旗等。等。

19.2.1.2 推广部署

用户可在**推广部署**页面发布部署通知。

管理员发布部署通知的 Web 页面，填写推广信息后生成推广链接，将推广链接下发后，终端用户可自行部署客户端。推广文案可自定义，修改后需要点击**<重新生成>**更新到推广页面中。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理>管理部署**”，选择**推广部署**页签。

步骤 3. 输入推广标题及推广文案，点击**<重新生成>**，生成最新推广链接。

步骤 4. 点击**<复制>**，复制推广链接进行推广（通过邮件、即时通讯工具进行推广）。



终端用户打开推广链接，在链接页面上执行相关操作即可部署客户端。



19.2.1.3 AD 推送

windows 用户通过 ad 推送工具给账户登录时设置自动化脚本以此达到批量安装效果。

步骤 1. 以租户角色登录主机安全系统管理平台。

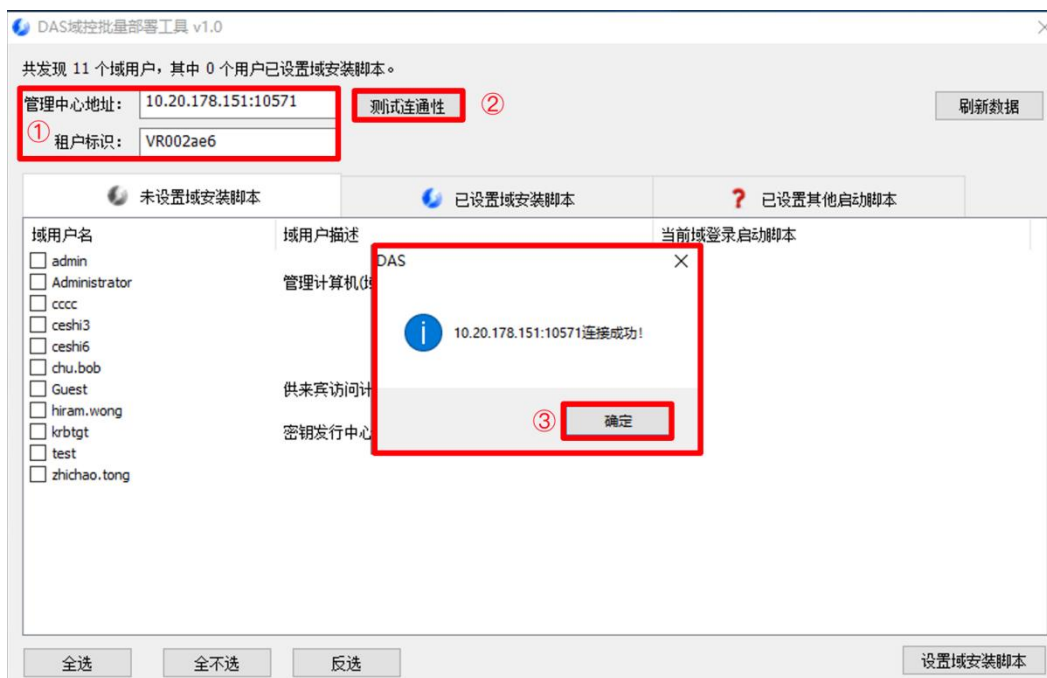
步骤 2. 在左侧导航栏选择“**系统管理**➤**管理部署**”，选择 **AD 推送** 页签。

步骤 3. 点击<**下载域推送工具**>下载工具。

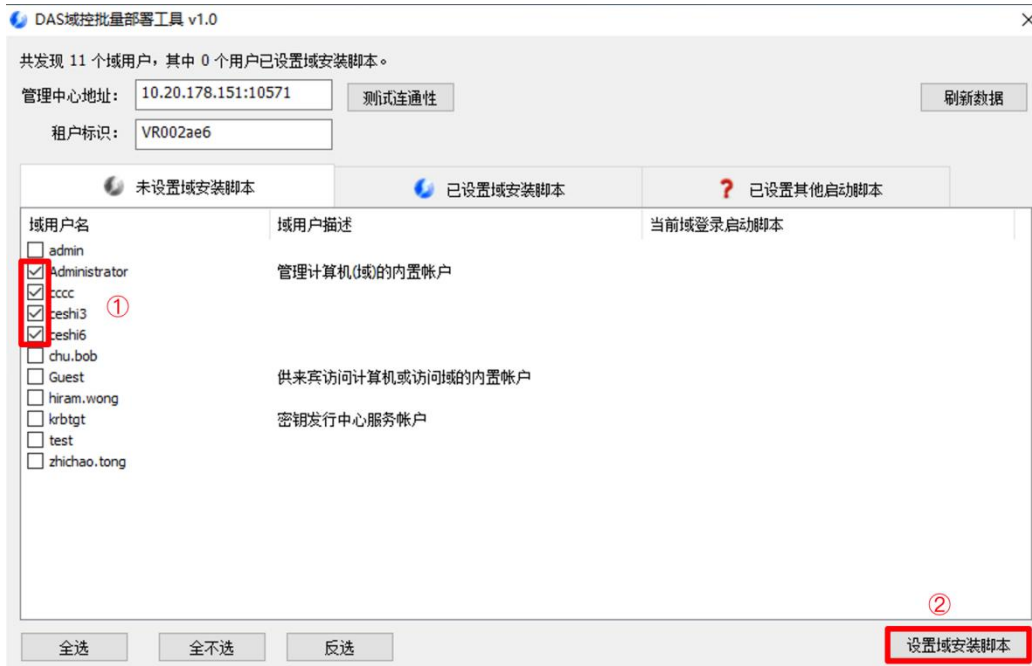


步骤 4. 在域控服务器上打开 **ADTOOL.exe** 工具。

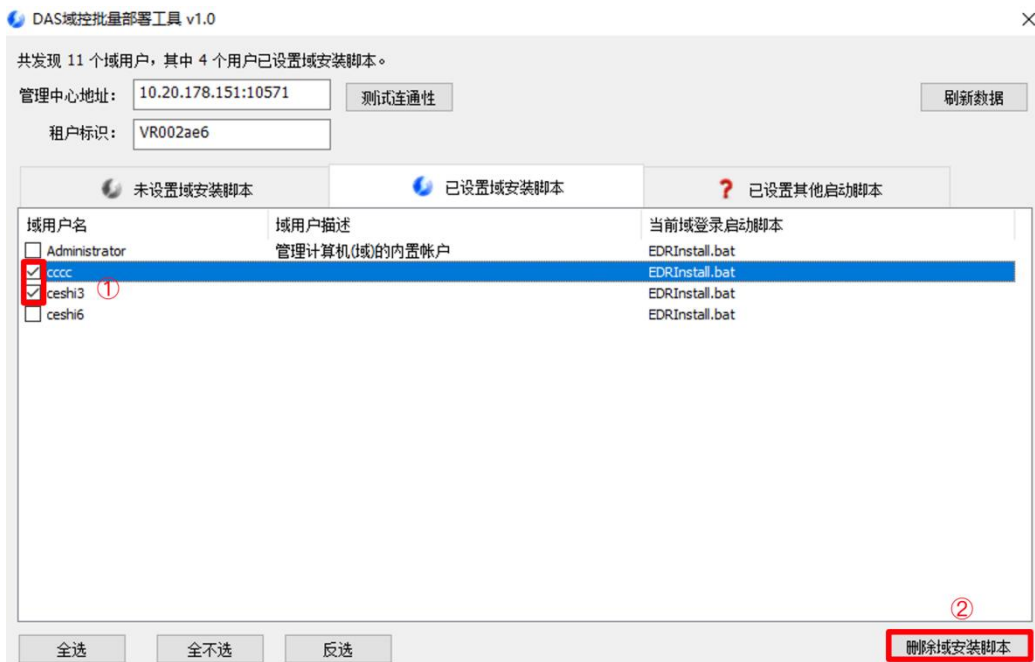
a) 填写管理中心地址和租户标识（租户识别码），点击<**测试连通性**>



b) 选择**未设置域安装脚本**页签，选择域用户,点击<**设置安装脚本**>设置需要安装的域用户



c) 选择已设置域安装脚本页签，选择域用户,点击<删除安装脚本>调整需要安装的域用户



步骤 5. 点击<【终端管理】-【终端概况】>查看是否安装成功





- ◆ 已经登录域账户的终端需要重新退出登录才可以触发安装过程
- ◆ AD 推送工具可通过“全选”“全不部”“反选”快速选择域用户
- ◆ 刷新数据为刷新域控服务器下的域用户

19.2.2 许可分配

租户可在**许可分配**页签对终端进行许可分配。

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理**▶**许可分配**”，进入**许可分配**页面。

步骤 3. 选择终端授权对象，点击右侧**操作项**的 图标。

生效日期	授权对象	最大支持数量	当前剩余数量	模块类型	到期日	状态	操作项
2022-08-10	ceshi	1	0	EDR-SST-CLIETN	2023-08-31	生效	
2022-08-10	ceshi	20	18	EDR-MODULE-PC	2023-08-31	生效	
2022-08-10	ceshi	20	19	WPT-EE-ALL	2023-08-31	生效	
2022-08-10	ceshi	500	497	EDR-MODULE-SERVER	2023-08-31	生效	

步骤 4. 在弹出的对话框中选择终端（在**终端列表**中勾选终端，点击 图标，将终端移动至**已选择终端列表**），点击<确定>，即可完成终端许可分配。

选择终端
×

终端列表 2/2

请选择分组

选择标签

终端名称/IP

终端名称

DESKTOP-8OK43JQ(192.168.1.10)

WIN-3QFTRUC04HH(10.11.1.1, 192.168.1.1)

已选择终端列表 0/2

请选择分组

选择标签

终端名称/IP

终端名称

WIN-3QFTRUC04HH(10.11.1.1, 192.168.1.1)

DESKTOP-8OK43JQ(192.168.1.10)

取消
确定

19.2.3 告警配置

租户可在**告警配置**页面进行邮件告警配置、Syslog 配置。

19.2.3.1 配置邮件告警

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理**➤**告警配置**”，选择**邮件告警**页签。

步骤 3. 进入**邮件告警**页面，输入邮件配置信息后点击<**应用配置**>，即可成功配置邮件告警。

另可对邮件告警配置进行重置邮件操作，重置后将返回上一次配置的结果。



19.2.3.2 配置 Syslog

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“**系统管理**➤**告警配置**”，选择**Syslog** 页签。

步骤 3. 进入**Syslog** 页面，输入 Syslog 配置信息后点击<**应用配置**>，即可成功配置 Syslog。

另可对 Syslog 配置进行重置操作，重置后将返回上一次配置的结果。



19.2.4 个人中心

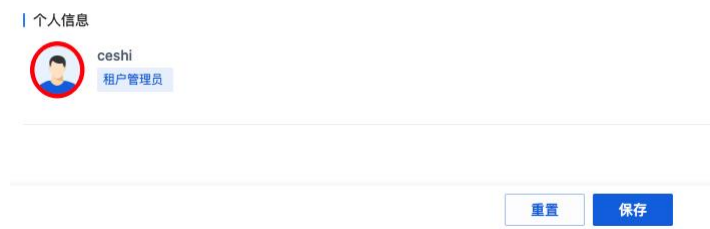
租户可在个人中心页面中查看个人信息、配置联系电话及邮箱。

19.2.4.1 查看个人信息

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>个人中心”，进入个人中心页面。

步骤 3. 点击用户头像，选择头像文件，即可自定义头像，上传文件建议不超过 2MB。



19.2.4.2 配置手机号码

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>个人中心”，进入个人中心页面。

步骤 3. 输入联系电话，选择是否启用，点击<保存>。



手机号码设置为“启用”的手机号码可收取系统紧急通知。

19.2.4.3 配置邮箱

步骤 1. 以租户角色登录主机安全系统管理平台。

步骤 2. 在左侧导航栏选择“系统管理>个人中心”，进入个人中心页面。

步骤 3. 输入是否使用默认邮箱、发件箱地址、SMTP 密码、SMTP 服务器地址、SMTP 服务器端口及是否支持 SSL 等信息后点击<应用配置>，即可成功完成邮箱配置。

邮箱配置

使用默认发件箱 是 否

默认发件箱为edr@dbappsecurity.com.cn, 要求EDR服务器可与该地址通信, 测试语句: telnet smtp.dbappsecurity.com.cn 25

* 发件箱地址

* SMTP密码

SMTP服务器地址

SMTP服务器端口

是否支持SSL 是 否

20 运维平台

admin 用户或者租户都可在**运维平台**对主机安全系统进行运维诊断、磁盘清理及重置密码操作，方便排查系统故障。

20.1 查看运维诊断结果

步骤 1. 登录主机安全系统运维平台。

- ◆ **方式一：**登录主机安全系统管理平台，将光标移至右上角用户名上，在下拉框中选择“**运维平台**”，页面将跳转至运维平台。



- ◆ **方式二：**或在浏览器地址栏输入 <https://IP地址:10579>，以 admin 用户访问运维平台。输入账号和密码，点击<登录>。

其中 IP 地址是主机安全系统管理平台的 IP 地址。



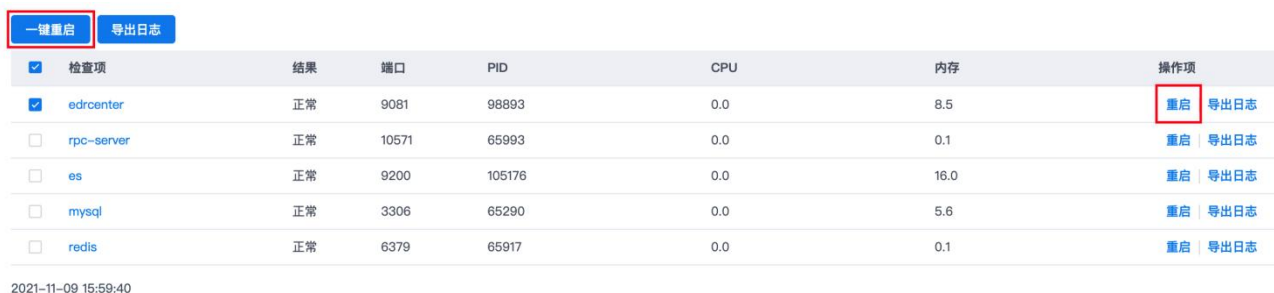
- ◆ 运维平台独立于主机安全系统平台，仅可使用运维平台 admin 账号进行登录，且该 admin 账号密码每日会进行更新。获取最新运维平台账号密码，请致电信息技术支持热线 400-6059-110。
- ◆ 主机安全系统出厂默认关闭且每天 00:00 定时关闭运维平台，用户需在使用前以

root 用户角色登录中心端服务器，执行 `docker start 主机安全系统-ops` 命令进行开启。

步骤 2. 进入**运维平台**，在导航栏选择“**运维诊断**”，进入**运维诊断**页面，用户可查看运维诊断详细结果。

选择需要重启的服务，点击右侧**操作项**的<重启>，在弹出的对话框中点击<确定>，可对服务进行重启操作。

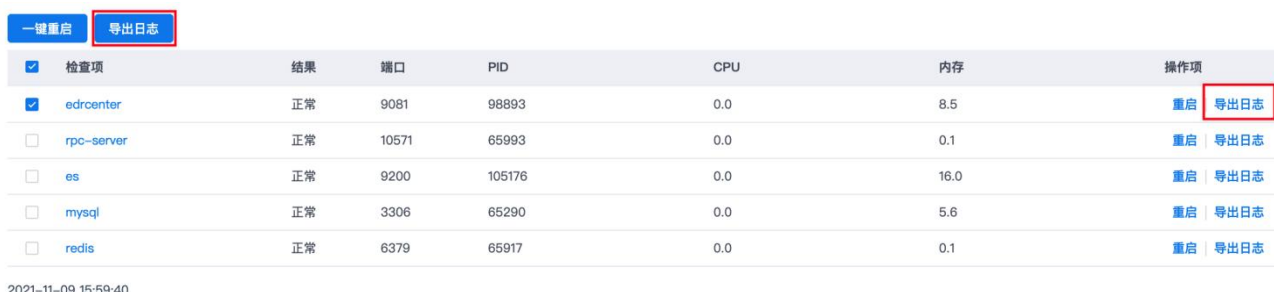
选择多个服务后点击<一键重启>，在弹出的对话框中点击<确定>，可批量重启多个服务。



检查项	结果	端口	PID	CPU	内存	操作项
<input checked="" type="checkbox"/> edrocenter	正常	9081	98893	0.0	8.5	重启 导出日志
<input type="checkbox"/> rpc-server	正常	10571	65993	0.0	0.1	重启 导出日志
<input type="checkbox"/> es	正常	9200	105176	0.0	16.0	重启 导出日志
<input type="checkbox"/> mysql	正常	3306	65290	0.0	5.6	重启 导出日志
<input type="checkbox"/> redis	正常	6379	65917	0.0	0.1	重启 导出日志

步骤 3. 选择需要导出日志的服务，点击右侧**操作项**的<导出日志>，在弹出的对话框中点击<确定>，可导出该服务的日志信息。

勾选多个服务后点击列表上方的<导出日志>，在弹出的对话框中点击<确定>，可批量导出多个服务的日志信息。



检查项	结果	端口	PID	CPU	内存	操作项
<input checked="" type="checkbox"/> edrocenter	正常	9081	98893	0.0	8.5	重启 导出日志
<input type="checkbox"/> rpc-server	正常	10571	65993	0.0	0.1	重启 导出日志
<input type="checkbox"/> es	正常	9200	105176	0.0	16.0	重启 导出日志
<input type="checkbox"/> mysql	正常	3306	65290	0.0	5.6	重启 导出日志
<input type="checkbox"/> redis	正常	6379	65917	0.0	0.1	重启 导出日志

20.2 清理磁盘



清理补丁文件将导致所有补丁文件被清空，请谨慎操作。

步骤 1. 登录主机安全系统管理平台，将光标移至右上角用户名上，在下拉框中选择“**运维平台**”。

步骤 2. 进入**运维平台**页面，在导航栏选择“**磁盘清理**”进入**磁盘清理**页面，用户可查看磁盘详情列表。

步骤 3. 选择需要清理的文件，点击右侧**操作项**的<清理>，可对磁盘进行清理操作。

选择多个文件后点击<一键清理>，可进行多个文件批量清理。

一键清理 2 录总磁盘50G,已用16G

清理项	占用磁盘	详情	操作项
<input checked="" type="checkbox"/> 1 临时日志	3.5G	EDR中心目录下的临时文件	<input type="button" value="清理"/>
<input type="checkbox"/> 压缩包	1.3GB	/opt和/root下的压缩包	<input type="button" value="清理"/>
<input type="checkbox"/> 服务日志	226.88MB	EDR中心服务运行日志	<input type="button" value="清理"/>
<input type="checkbox"/> 补丁文件	2.16GB	清理补丁文件, 谨慎选择此步骤, 将导致所有补丁文件清空	<input type="button" value="清理"/>

20.3 重置密码

步骤 1. 登录主机安全系统管理平台, 将光标移至右上角用户名上, 在下拉框中选择“**运维平台**”。

步骤 2. 进入**运维平台**页面, 在导航栏选择“**忘记密码**”, 进入**忘记密码**页面, 输入密码并确认密码, 点击<**确定**>, 可对主机安全系统管理平台 admin 用户的账户密码进行重置。



密码强度需要符合设置要求, 关于密码强度的详细信息, 请参考[密码及访问策略](#)。

* 输入密码

* 确认密码:

20.4 恢复数据

20.4.1 恢复 MySQL 数据

步骤 1. 登录主机安全系统管理平台, 将光标移至右上角用户名上, 在下拉框中选择“**运维平台**”。

步骤 2. 进入**运维平台**页面, 在导航栏选择“**数据恢复**”进入**数据恢复**页面, 选择 **MySQL 数据库** 页签。

步骤 3. 选择备份文件后对系统数据进行恢复。

◆ 选择历史备份

- 1) 选择历史备份文件。
- 2) 点击<**确定**>, 进行数据恢复。

可通过选择历史的备份数据或者上传备份数据文件，进行数据恢复。该操作将恢复所有资产、配置信息，请谨慎操作。

选择历史备份：

请选择 1

确定 2

上传本地备份：

上传文件

确定

◆ 上传本地备份

- 1) 点击<上传文件>，上传本地备份文件。
- 2) 点击<确定>，进行数据恢复。

可通过选择历史的备份数据或者上传备份数据文件，进行数据恢复。该操作将恢复所有资产、配置信息，请谨慎操作。

选择历史备份：

请选择

确定

上传本地备份：

上传文件 1

确定 2

20.4.2 检测 ES 状态

步骤 1. 登录主机安全系统管理平台，将光标移至右上角用户名上，在下拉框中选择“运维平台”。

步骤 2. 进入运维平台页面，在导航栏选择“数据恢复”进入数据恢复页面，选择 ES 防护日志页签。

步骤 3. 点击<检测>，可对系统 ES 服务状态进行检测。

ES故障恢复，该操作仅恢复为7天内的防护日志/操作日志/运维日志，请谨慎操作。

检测	批量删除	一键恢复			
<input type="checkbox"/> 检查项	说明	占用空间	状态	操作项	
<input type="checkbox"/> cloudbrain2-wyh	租户wyh的	281b	yellow		
<input type="checkbox"/> performance-liuz	租户liuz的性能数据	297b	yellow		

对于检测状态为 **red** 的检查项，勾选检查项后点击<批量删除>，可对检查项进行批量删除操作。

ES故障恢复，该操作仅恢复为7天内的防护日志/操作日志/运维日志，请谨慎操作。

检测 批量删除 一键恢复

<input type="checkbox"/>	检查项	说明	占用空间	状态	操作项
<input type="checkbox"/>	cloudbrainv2-wyh	租户wyh的	281b	yellow	
<input type="checkbox"/>	performance-iliuz	租户iliuz的性能数据	297b	yellow	
<input type="checkbox"/>	ops-test	租户test的运维日志	253.9kb	yellow	

勾选检查项后点击<一键恢复>，可恢复该检查项 7 天内的防护日志/操作日志/运维日志。

ES故障恢复，该操作仅恢复为7天内的防护日志/操作日志/运维日志，请谨慎操作。

检测 批量删除 一键恢复

当前页已选择 1 项，未选择 11 项 重置 全选当页 反选当页

<input checked="" type="checkbox"/>	检查项	说明	占用空间	状态	操作项
<input checked="" type="checkbox"/>	cloudbrainv2-wyh	租户wyh的	281b	yellow	

21.1 如何区分 Docker 版本与非 Docker 版本？

主机安全系统 V3.0.3 版本仅支持 Docker 版本，支持 V2.0.17.x 的 Docker 版本直接升级至 V3.0.3 版本，如若为 V2.0.17.x 及以前的非 Docker 版本，请参考《主机安全及管理平台 V2.0.17.9 维护指南》进行迁移数据库到同版本新中心后（新中心操作系统为 Centos7.x）使用 Docker 包部署后升级至 V3.0.3 版本。

Docker 安装包安装升级通用，且适用于 CentOS 7.x 操作系统。

区分方法如下：

使用 root 用户登录主机安全系统中心的后台，执行 `docker ps` 命令，若能查看主机安全系统中心所有服务的容器，则说明为 Docker 版；若不能执行该命令，则说明为非 Docker 版。

22 术语&缩略语

术语	解释
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack, 简称 DDoS)是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击, 或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的, 这类攻击称为分布式拒绝服务攻击, 其中的攻击者可以有多个。
认证	是一种信用保证形式。按照国际标准化组织(ISO)和国际电工委员会(IEC)的定义, 是指由国家认可的认证机构证明一个组织的产品、服务、管理体系符合相关标准、技术规范(TS)或其强制性要求的合格评定活动。
网马	网马就是在网页中植入木马, 用户打开网页就运行了木马程序, 从而危害用户的终端。网页木马实际上是一个 HTML 网页, 与其它网页不同的是该网页是黑客精心制作的, 用户一旦访问了该网页就会中木马。
虚拟机	虚拟机(Virtual Machine)指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时, 需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的 CMOS、硬盘和操作系统, 可以像使用实体机一样对虚拟机进行操作。