主机安全使用手册

天翼云科技有限公司

文档说明

产品名称		主机安全	
适用平台/版本			
拟制人	8488	**评审组**	5506
发布人	5888	**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2021-12-15	01	初次发布	8488
2022-01-20	02	◆ 修改 1.7.1 和 1.7.3 章节，增加命令：docker exec -it EDR-center bash ◆ 增加 17 章	8488

目 录

前言

概述

感谢您选择天翼云的网络安全产品。主机安全及管理系统（简称“EDR”或者“EDR”）是天翼云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。

本手册描述主机安全及管理系统的配置方法，主要包括快速入门、许可管理、角色权限、用户认证、首页、资产管理、高级威胁、管理策略、响应处置、风险评估、日志检索、资产全览、多级中心、升级管理、系统管理、平台管理等。

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主机安全及管理系统的读者，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。
- Web 服务器常见设备的基本工作原理和配置、操作。
- 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”。
➢	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”。

内容	说明
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。

1 快速入门

主机安全及管理系统（简称“EDR”或“EDR”）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。EDR 通过自主研发的文件诱饵引擎，有着业界领先的勒索专防专杀能力；能通过内核级东西向流量隔离技术，实现网络隔离与防护；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。

目前产品广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全等各个场景。

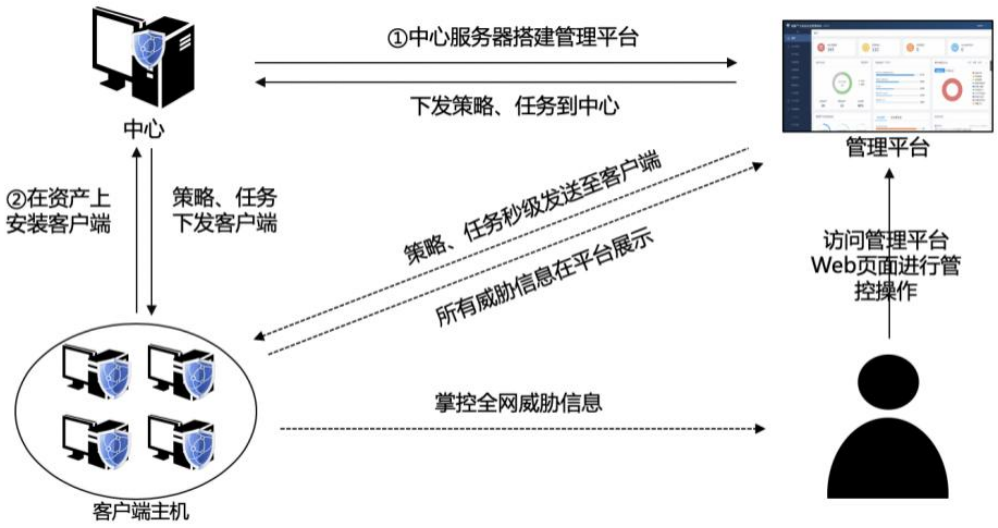
1.1 产品特点

EDR 由管理控制中心和客户端组成。

- 管理控制中心部署在独立提供的 Linux 系统主机上，主要功能是把所有客户端信息集中于一体，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响应以及处置。
- 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。

中心指部署了 EDR 管理中心的 Linux 主机（物理机或虚拟机）；管理平台指 EDR 管理中心的用户操作平台；客户端指部署了 EDR 客户端的主机。

部署示意图如下所示。



1.2 产品功能

EDR 具有以下功能模块：

1. **防御已知和未知类型勒索病毒**

   EDR 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，EDR 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**

   EDR 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，上传资产指纹、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**

   EDR 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**

   EDR 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**

   EDR 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。

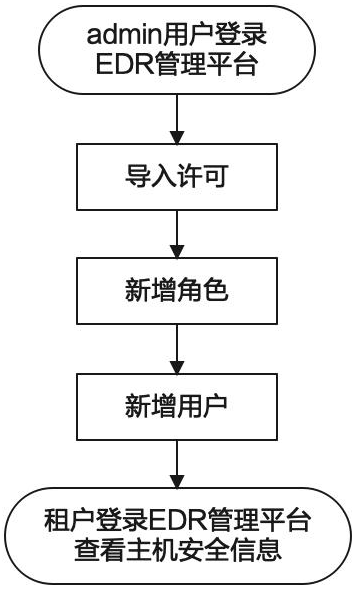
1.3 登录系统

在进行主机安全管理之前，用户需要登录 EDR 管理平台。

在浏览器地址栏输入 https://*管理平台 IP 地址*，以管理员（系统默认用户名为 admin）角色或租户角色访问 EDR 平台。输入账号，密码和验证码，点击<**登录**>。其中 IP 地址是 EDR 管理平台的地址。

1.4 主要业务流程

EDR 主要业务流程如下：



步骤 1. admin 用户登录 EDR 平台。

步骤 2. 导入许可。用户需获得许可授权后使用 EDR 系统，详情请参见许可管理。

步骤 3. 新增角色。EDR 支持自定义用户角色及自定义角色权限功能，可对不同角色赋予不同权限，详情请参见新增角色。

步骤 4. 新增租户。新增角色权限后，用户可根据实际业务需求，自定义创建租户并为租户选择对应角色。详情请参见新增租户。

步骤 5. 租户角色登录 EDR，查看主机安全信息。详情请参考首页。

1.5 用户权限

EDR 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）	◆ 许可管理：导出许可、导入许可。 ◆ 用户认证：新增用户、编辑用户信息、删除用户、登录用户。 ◆ 角色权限：新增角色、编辑角色权限、删除角色。 ◆ 资产全览：查看资产列表及资产详情。 ◆ 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。
租户	◆ 首页：查看系统信息概览。 ◆ 资产管理：资产概况、病毒查杀、网马查杀、漏洞管理、微隔离、移动存储、分组标签。 ◆ 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。 ◆ 响应处置：信息搜索、文件推送、定期巡检、流量画像。 ◆ 风险评估：资产体检、基线检查。 ◆ 日志检索：防护日志、操作日志、运维日志、日志报表。 ◆ 系统管理：添加资产、推广部署、升级管理、许可分配、告警配置、个人中心。

1.6 用户个人中心

用户可在个人中心查看系统版本和授权信息、运维平台、意见反馈、修改密码及查看帮助文档。

1.6.1 查看系统版本和授权信息

以任意角色登录 EDR 管理平台，将光标移至右上角用户名上，在下拉框中选择“**关于**”，即可在弹出框中查看系统版本和授权信息。

1.6.2 意见反馈

步骤 1. 以任意角色登录 EDR 管理平台，将光标移至右上角用户名上，在下拉框中选择“**用户反馈**”。

步骤 2. 在弹出框中查看用户反馈方法及途径。勾选“**加入 用户改善计划**”后点击<**好的**>，平台会收集用户部分样品特征到云端，以助于产品人员更好地提升用户使用体验。

1.6.3 运维平台

以任意角色登录 EDR 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**”，页面跳转至运维平台，用户即可在该平台查看系统运维情况，详情可参考平台管理。

1.6.4 修改密码

步骤 1. 以任意角色登录 EDR 管理平台，将光标移至右上角用户名上，在下拉框中选择“**修改密码**”。

步骤 2. 在弹出框中输入当前密码及新设密码后点击<**确定**>，即可修改密码。

勾选“**加入 用户改善计划**”后点击<**确定**>，平台会收集用户部分样品特征到云端，以助于产品人员更好地提升用户使用体验。

1.6.5 查看帮助文档

以任意角色登录 EDR 管理平台，将光标移至右上角用户名上，在下拉框中选择“**帮助文档**”，页面跳转至 EDR 产品文档页面，用户可在此页面查看 EDR 相关文档。

需有外网访问权限才可访问帮助文档。

1.6.6 注销用户

以任意角色登录 EDR 管理平台，将光标移至右上角用户名上，在下拉框中选择“**注销**”，用户即可退出登录。

2 许可管理

在进行主机安全管理之前，需先进行许可的申请及导入操作。

仅 admin 用户具有许可管理权限。

- **申请并导入许可**

步骤 1. 以 admin 用户登录 EDR 管理平台，在左侧导航栏选择“**许可管理**”，查看并记录系统的机器码。

步骤 2. 输入机器码、用户名（默认为 admin）以及合同信息等填写许可申请表，然后发送邮件至 support@dbappsecurity.com.cn 申请许可。邮件标题：申请版本和许可（例如：XXX 单位 EDR2.0.17 正式合同许可申请）。

步骤 3. 得到许可授权文件后点击<**导入许可**>，上传许可文件即可。

生效日期	授权对象	最大支持数量	当前剩余数量	模块型号	中心型号	到期日	状态
2021-06-03	安恒信息	100	0	DAS-EDR-S800G-MODU...	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-SERVER	EDR-EE-2000	2024-07-31	生效
2021-06-03	安恒信息	100	90	EDR-MODULE-SERVER	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-SERVER-...	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-PC	EDR-EE-2000	2023-06-30	生效

◆ **导出许可**

以 admin 用户登录 EDR 管理平台，在左侧导航栏选择“**许可管理**”，点击<**导出许可**>即可下载许可文件。

生效日期	授权对象	最大支持数量	当前剩余数量	模块型号	中心型号	到期日	状态
2021-06-03	安恒信息	100	0	DAS-EDR-S800G-MODU...	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-SERVER	EDR-EE-2000	2024-07-31	生效
2021-06-03	安恒信息	100	90	EDR-MODULE-SERVER	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-SERVER-...	EDR-EE-2000	2023-06-30	生效
2021-06-03	安恒信息	100	0	EDR-MODULE-PC	EDR-EE-2000	2023-06-30	生效

3 角色权限

EDR 支持自定义用户角色及自定义角色功能，可以根据实际的业务需求，灵活的自定义创建角色并且可以给角色自定义功能权限。通过在同一用户下的多角色的创建，实现多个角色和管理员对终端资产的共同管理，让终端资产管理更精细化、更安全可控。

仅 admin 用户具有角色操作权限。系统默认租户管理员角色，该角色不支持编辑及删除操作。新增的自定义角色支持编辑角色权限和删除角色权限操作。

3.1 新增角色

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**角色权限**”，进入**用户角色**列表页，点击<**新增**>。

步骤 3. 进入**新增角色权限**页面，输入角色名称并选择角色权限，点击<**确认新增**>即可新增角色权限。

3.2 编辑角色

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2.　在左侧导航栏选择“**角色权限**”，进入**用户角色**列表页，点击角色右侧**操作项**的 图标。

步骤 3.　进入**编辑角色权限**页面，修改角色名称及角色权限后点击<**确认修改**>即可修改角色权限。

3.3　删除角色

步骤 1.　以 admin 用户登录 EDR 管理平台，在导航栏选择“**角色权限**”进入**用户角色**列表页。

步骤 2.　选中需要删除的角色，点击<**删除**>。

选择多个用户后点击<**删除**>，可进行多用户角色的批量删除。

步骤 3.　在弹窗中点击<**确定**>，即可删除该角色。


提示
你确定要删除所选记录吗?
取消
确定

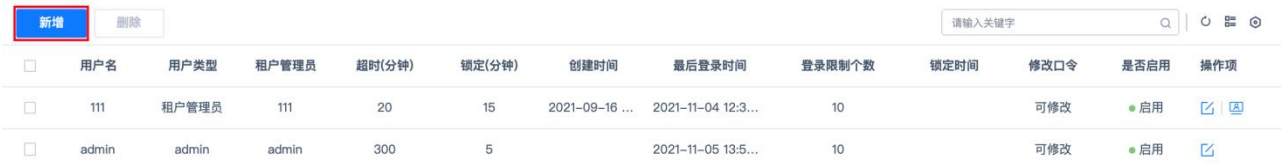
4 用户认证

仅 admin 用户具有用户认证操作权限。

4.1 新增租户

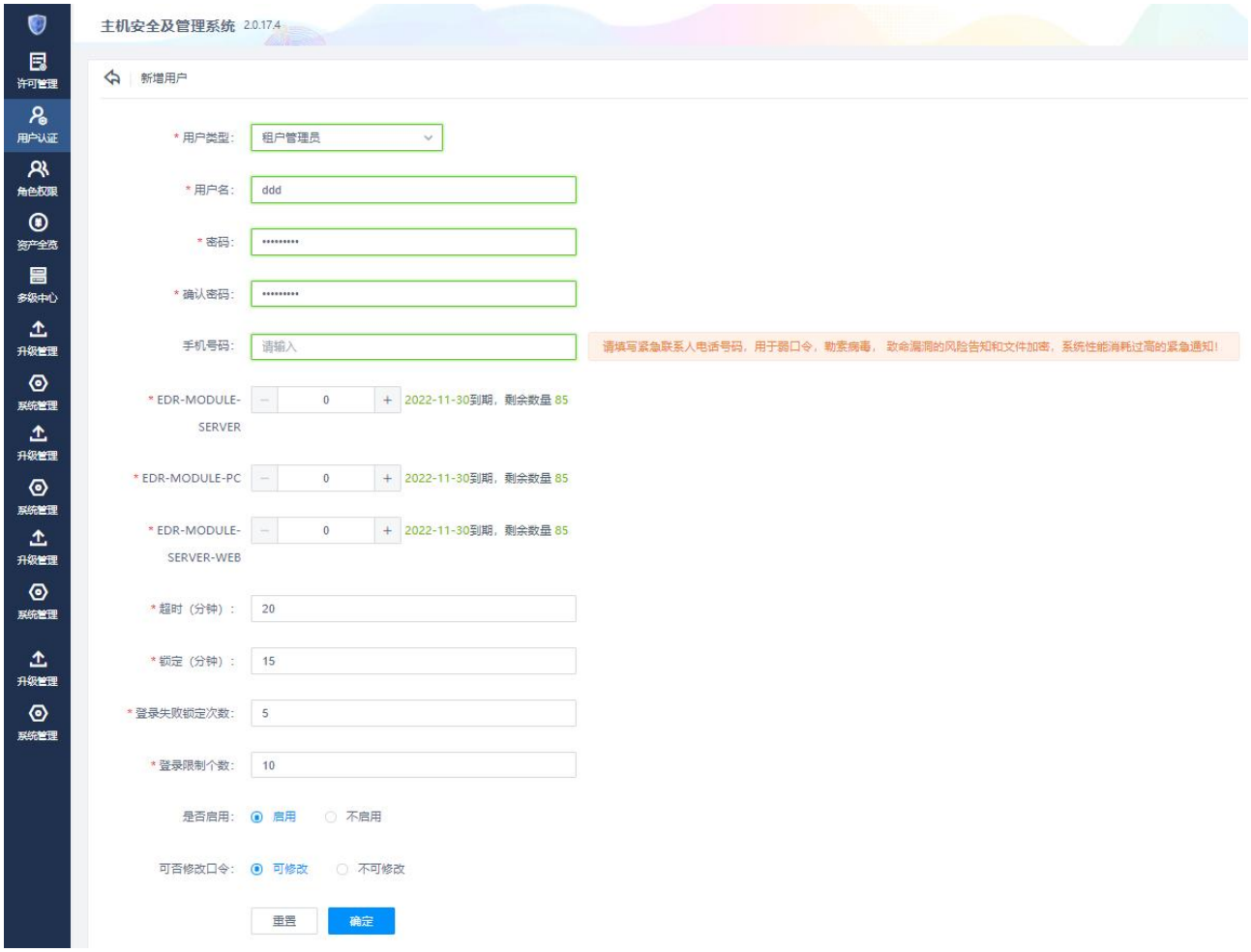
步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**用户认证**”，进入**用户**列表页。点击<**新增**>。



步骤 3. 进入**新增用户**页面，输入租户信息后点击<**确定**>，即可新增租户。

新增租户成功后，可使用该用户账号登录 EDR 管理平台。



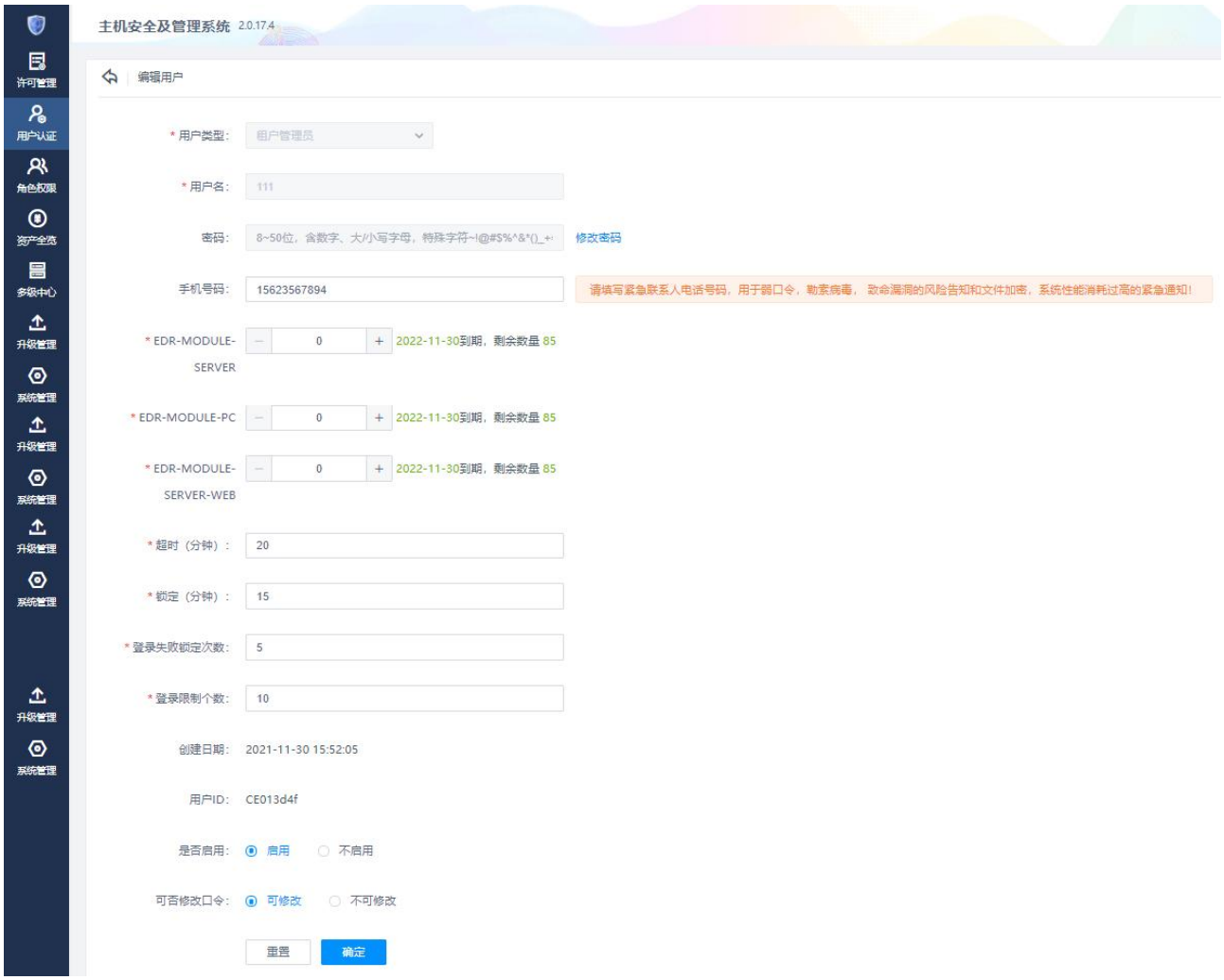
新增用户参数说明如下。

参数	说明
用户类型	为用户选择角色类型，不同角色可设置不同操作权限。详情可参考新增角色。
租户名单	为用户选择租户组，当用户角色为租户时必选。
用户名	用户登录账号。
密码	用户登录密码：8-50 位，含数字、大/小写字母、特殊符号~!@#¥%&*()_·。
手机号码	填写紧急联系人电话号码，用于弱口令、勒索病毒、致命漏洞的风险告知和文件加密、及系统性能消耗过高时的紧急通知。
EDR-MODULE-SERVER	许可模块型号。
EDR-MODULE-SERVER-WEB	许可模块型号。
EDR-MODULE-PC	许可模块型号。
超时（分钟）	用户操作超时时间，时间范围 1~1440。
锁定（分钟）	用户锁定时间，时间范围 1~1440。
登录失败锁定次数	登录失败锁定次数，限制范围 0~100，0 表示不锁定。
登录限制个数	账号登录 IP 限制数，限制个数范围 1~1000。
是否启用	是否启用该账号。
可否更改口令	用户是否可更改口令密码。

4.2 编辑用户

步骤 1. 以 admin 用户登录 EDR 管理平台，在导航栏选择“**用户认证**”进入**用户**列表页，点击右侧**操作项**中的 图标。

步骤 2. 在弹出的编辑框中修改租户信息，点击<**确定**>，即可成功修改租户信息。

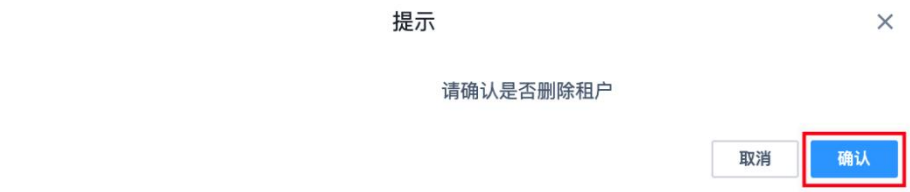


4.3 删除用户

步骤 1. 以 admin 用户登录 EDR 管理平台，在导航栏选择“**用户认证**”进入**用户**列表页。选中需要删除的租户，点击列表上方的<**删除**>。

步骤 2. 在弹出框中点击<**确定**>，即可成功删除该租户。

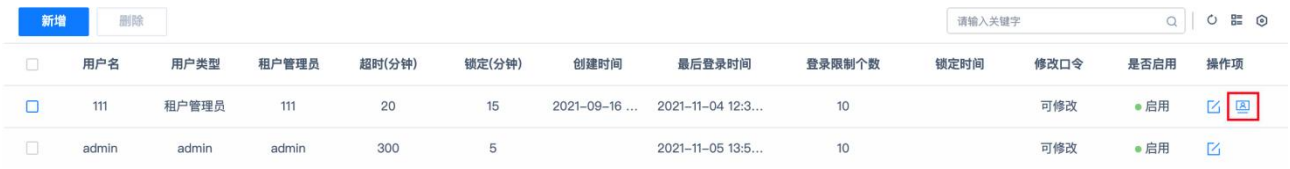
选中多个用户后点击<**删除**>，可进行多用户批量删除。



当前租户有绑定资产的情况下不允许进行删除，需前往租户将资产解绑后再行删除。

4.4 登录用户账号

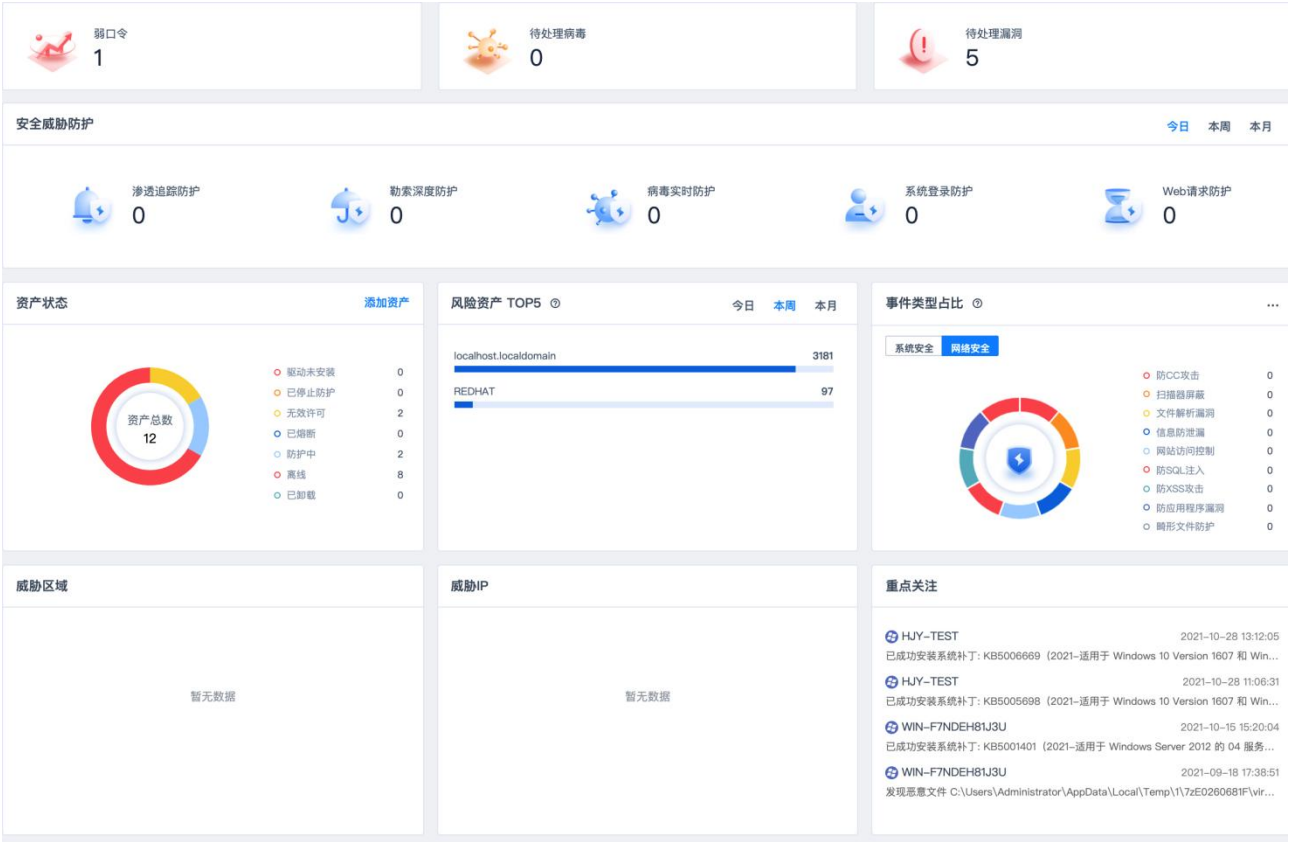
以 admin 用户登录 EDR 管理平台，在导航栏选择“**用户认证**”进入**用户**列表页。选择需要登录的用户，点击右侧**操作项**的 图标，即可使用该租户账号登录 EDR 管理平台进行资产管理。



5 首页

仅租户角色具有查看首页权限。

以租户账号登录 EDR 管理平台，默认进入首页显示主机资产总体安全概览。



具体展示信息说明如下。

信息	说明
弱口令	点击弱口令数字，用户可查看资产的弱口令评估结果。详情可参考。
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_查杀病毒。
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。
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。
资产状态	展示资产总数以及资产状态的占比，包括驱动未安装、已停止防护、无效许可、已熔断、防护中、离线、已卸载。点击右上角<**添加资产**>可进行资产新增操作，详情可参考添加资产。

信息	说明
风险资产	展示本周被攻击次数前五的资产。
事件类型占比	展示本周攻击事件的数据。点击右上角 ••• 图标可查看事件详情。
威胁 IP	展示本周攻击次数前五的源 IP。
威胁区域	展示本周攻击次数前五的区域。
重点关注	展示日志里的重点关注事件。

6 资产管理

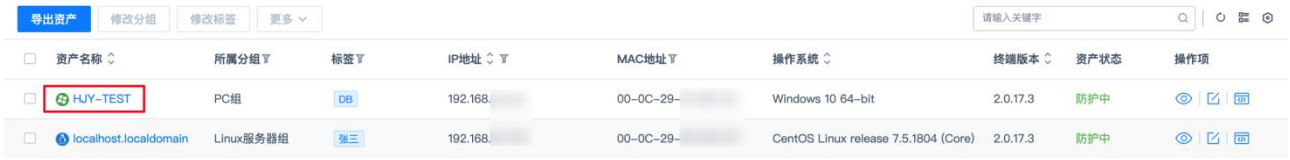
仅租户角色具有资产管理权限。

6.1 管理资产

租户角色可在**资产概况**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，并可进行查看资产详情、编辑资产、查看策略等操作。

6.1.1 查看资产详情

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤资产概况**”进入**资产概况**页面，选择需要查看的主机资产，点击资产名称。



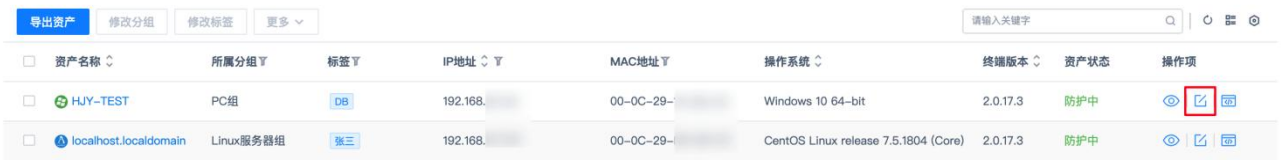
步骤 2. 进入**资产指纹**页面，即可查看该主机资产的详细信息，并可进行远程重启主机、关闭主机及修改远程端口操作。

资产概况说明如下。

资产信息	说明
终端详情	◆ 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、重启主机、IP/MAC 绑定（Windows）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，将会自动绑定回原始 IP，并在运维日志进行告警。**目前只支持对 Windows 系统进行 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，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	对终端资产上端口情况进行实时监控。
运行程序	对终端资产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	对终端资产上所有账号信息进行统计。
软件信息	对终端资产上运行的软件详细信息进行统计。
性能监控	对终端资产上的内存、CPU、磁盘、网络 IO 进行监控统计。
临时封锁 IP	对终端资产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。
启动项	对终端资产上所有的启动项进行统计和管理。

6.1.2 编辑资产

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤资产概况**”进入**资产概况**页面，选择需要编辑的资产，点击右侧**操作项**的图标。



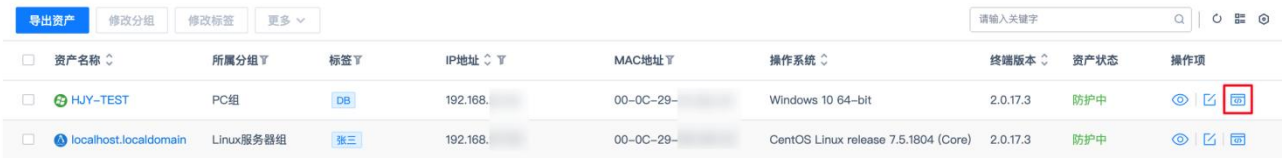
步骤 2. 在弹出框中编辑资产信息，点击<**确定**>，即可编辑资产成功。

编辑资产信息时，若绑定状态调整为关，将解绑该资产，被解绑的资产会从资产列表中删除。

6.1.3 查看策略

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤资产概况**”进入**资产概况**页面。

步骤 2. 选择需要查看的资产，点击右侧**操作项**的 图标，即可对该资产的策略信息进行查看和编辑操作，详情请参考管理策略。



6.1.4 其他操作

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤资产概况**”进入**资产概况**页面。租户可在此页面修改资产分组、修改资产标签并导出资产。

步骤 2. 点击<**更多**>，在弹出的下拉框中选择不同的菜单项，可对资产进行卸载客户端、删除资产、停止防护、启动防护、关闭主机、重启主机、重启客户端、迁移资产、修改远程管理端口、导出资产调试日志等操作。

选择多个资产后点击操作项，可对资产进行批量操作。

具体操作说明如下。

操作	说明
导出资产	可将资产信息以 CSV 格式导出至本地。
修改分组/修改标签	修改所选资产的分组/标签，每个资产必须且只能在一个分组内，可以有多个标签。
设置卸载客户端/删除资产	可对客户端执行相应操作。
停止防护	关闭所选资产当前所有防护。
启动防护	恢复所选资产关闭防护前的状态。
关闭主机/重启主机	对所选资产进行关机或重启。
重启客户端	对客户端 Agent 进行重启。
迁移资产	填写新中心 IP 和 UUID，可对租户内资产进行同中心跨租户迁移以及不同中心间迁移。
修改远程管理端口	填写需要修改的远程管理端口，可选立即重启远程管理服务使之立即生效。
导出资产调试日志	将所选资产的客户端运行日志，异常转储日志，操作系统日志信息导出。

6.2 查杀病毒

用户可在**病毒查杀**页面查看所有资产的病毒查杀情况，并支持以资产视角和病毒视角对病毒进行查杀。

- 支持对所有资产批量进行病毒扫描（快速扫描/全盘扫描/自定义扫描）、停止扫描、处理病毒。

- 支持设置单个资产信任区和模板化设置信任名单，并可查看单个资产的病毒查杀详情。
- 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。

6.2.1 资产视角

6.2.1.1 扫描资产

扫描资产支持快速扫描、全盘扫描、自定义扫描及停止扫描等操作。

- **快速扫描**

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 勾选需要扫描的资产，点击<**快速扫描**>。

步骤 3. 在弹出的确认框中点击<**确定**>，即可对资产进行快速扫描。

选择多个资产后点击<**快速扫描**>，可进行资产批量快速扫描。

- **全盘扫描**

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 选中需要扫描的资产，点击<**全盘扫描**>。

步骤 3. 在弹出的确认框中点击<**确定**>，即可对资产进行全盘扫描。

选择多个资产后点击<**全盘扫描**>，可进行资产批量全盘扫描。

◆ **自定义扫描**

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

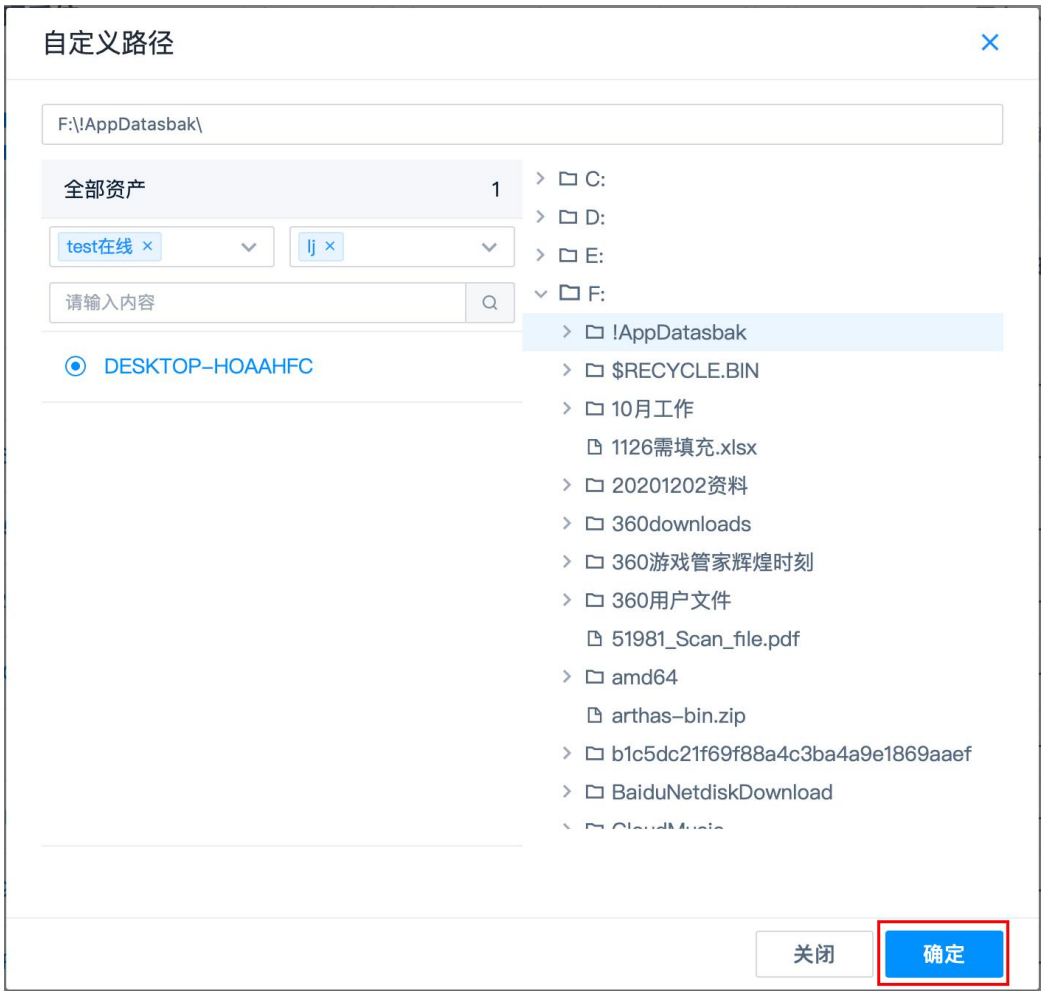
步骤 2. 选中需要扫描的资产，点击<**自定义扫描**>。

步骤 3. 在弹出的确认框中点击<**扫描**>，即可对资产进行全盘扫描。

选择多个资产后点击<**自定义扫描**>，可进行批量资产的自定义扫描。

步骤 4. 在弹出框中点击<**添加一行**>，新增扫描路径。

步骤 5. 选择需要扫描的路径，点击<**确定**>，即可对该自定义路径进行扫描。



◆ **停止扫描**

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 选中正在扫描的资产，将光标移至**更多**，在弹出的下拉框选择“**停止扫描**”。

步骤 3. 在弹出框中点击<**确定**>，即可停止资产病毒扫描。

选择多个正在扫描的资产，点击<**停止扫描**>，即可停止资产扫描。

6.2.1.2 查看扫描结果

租户可查看单个资产扫描结果，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 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 选择需要查看的资产，点击右侧**操作项**的 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资产扫描、查看隔离区、查看信任区操作。

步骤 4. 进入**文件详情**页面，可在此页面查看详细病毒木马文件，并支持对文件进行立即处理及重新扫描操作。

- 选择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。

6.2.1.3 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 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 选中需要处理病毒的资产，点击<**处理病毒**>。

选择多个资产后点击<**处理病毒**>，可批量处理资产病毒。

步骤 3. 在弹出的提示框中点击<**确定**>，即可对该资产病毒进行处理。处理完成后，租户可对隔离区文件进行恢复及删除操作。

6.2.1.4 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 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**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**”，即可将所有资产的病毒扫描报告导出至本地。

选择具体资产后点击<**导出报告**>，可将所选中的资产病毒扫描报告导出至本地。

6.2.1.5 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、压缩包查杀设置及处理方式等。

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2. 点击<**查杀设置**>。

选择多个资产后点击<**查杀设置**>，可对资产病毒查杀模式进行批量设置。

步骤 3. 在弹出框中设置查杀模式，点击<**确定**>即可设置成功。

6.2.1.6 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。

◆ **查看病毒详情**

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

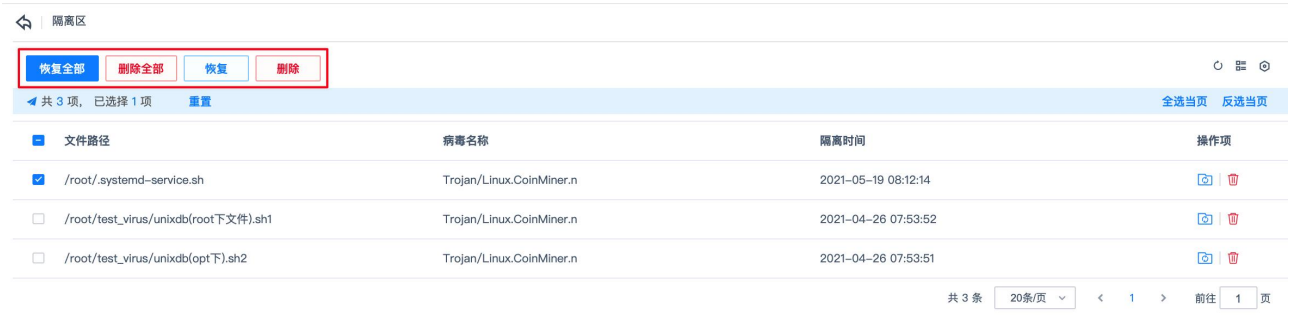
步骤 2.　点击病毒数，即可在弹窗中查看病毒的名称、MD5 值及文件路径。

◆ 配置隔离区

步骤 1.　以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 2.　点击隔离区数字。

步骤 3.　进入**隔离区**页面，选中需要处理的文件，即可对文件进行恢复、删除、恢复全部、删除全部操作。



◆ 配置信任区

步骤 1.　以租户角色登录 EDR 管理平台。

步骤 2.　在左侧导航栏选择“**资产管理➤病毒查杀**”，选择**资产视角**页签。

步骤 3.　点击信任区数字。

步骤 4.　进入**信任区**页面，租户可对新人项目进行添加及删除操作。

6.2.2 病毒视角

6.2.2.1 处理病毒

◆ **方式一：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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 图标，即可对该病毒进行处理。

此方式适合逐条处理病毒。

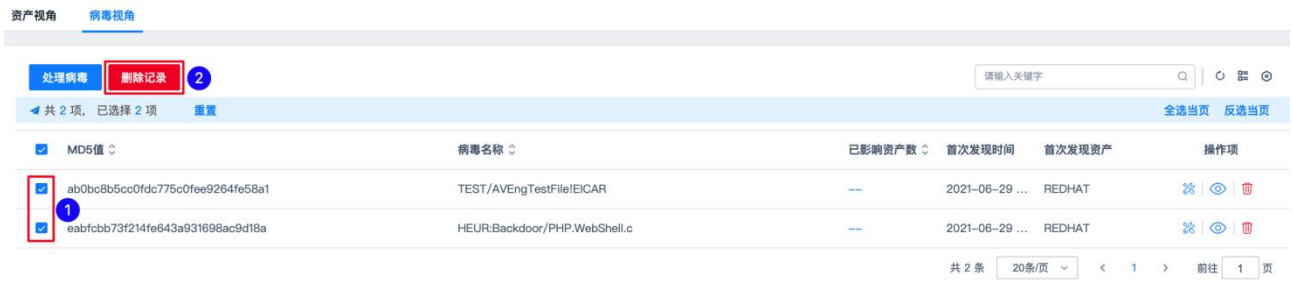
◆ **方式二：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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。

此方式适合批量处理病毒。



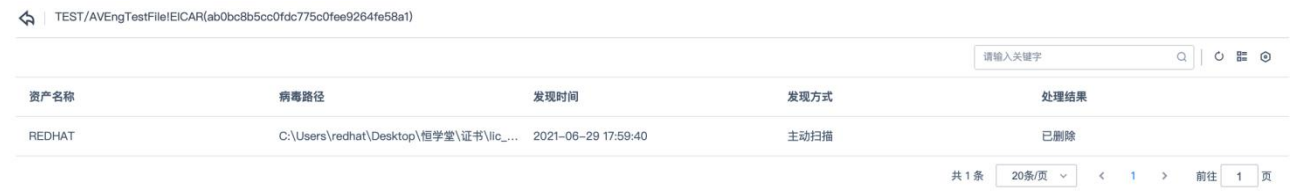
6.2.2.2 查看病毒详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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 图标。

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



6.2.2.3　删除记录

◆ **方式一：**

步骤 1.　以租户角色登录 EDR 管理平台。

步骤 2.　在左侧导航栏选择“**资产管理➤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 图标。

步骤 4.　在弹窗中点击<**确定**>，即可删除该条病毒记录。

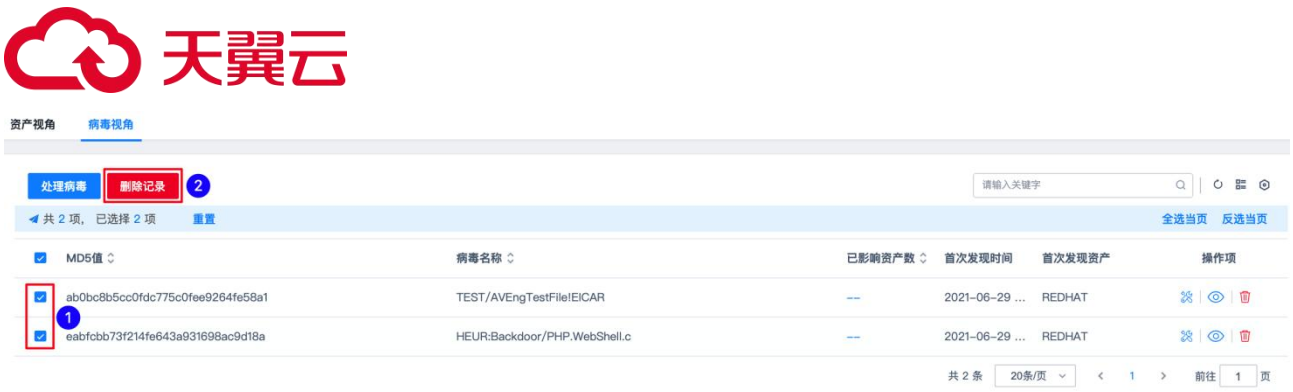
此方式适合逐条删除记录。

◆ **方式二：**

步骤 1.　以租户角色登录 EDR 管理平台。

步骤 2.　在左侧导航栏选择“**资产管理➤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. 在弹窗中点击<**确定**>，即可对所选病毒进行处理。

此方式适合批量处理病毒。

6.3 查杀网马

租户可在“**网马查杀**”页面查看所有资产的网马查杀情况。

- 支持对所有资产批量进行网马扫描、停止扫描、处理网马。
- 支持设置单个资产信任区和模板化管理信任名单，并可查看单个资产的网马查杀页面。
- 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。

6.3.1 扫描资产

步骤 1. 以租户角色登录 EDR 管理平台。

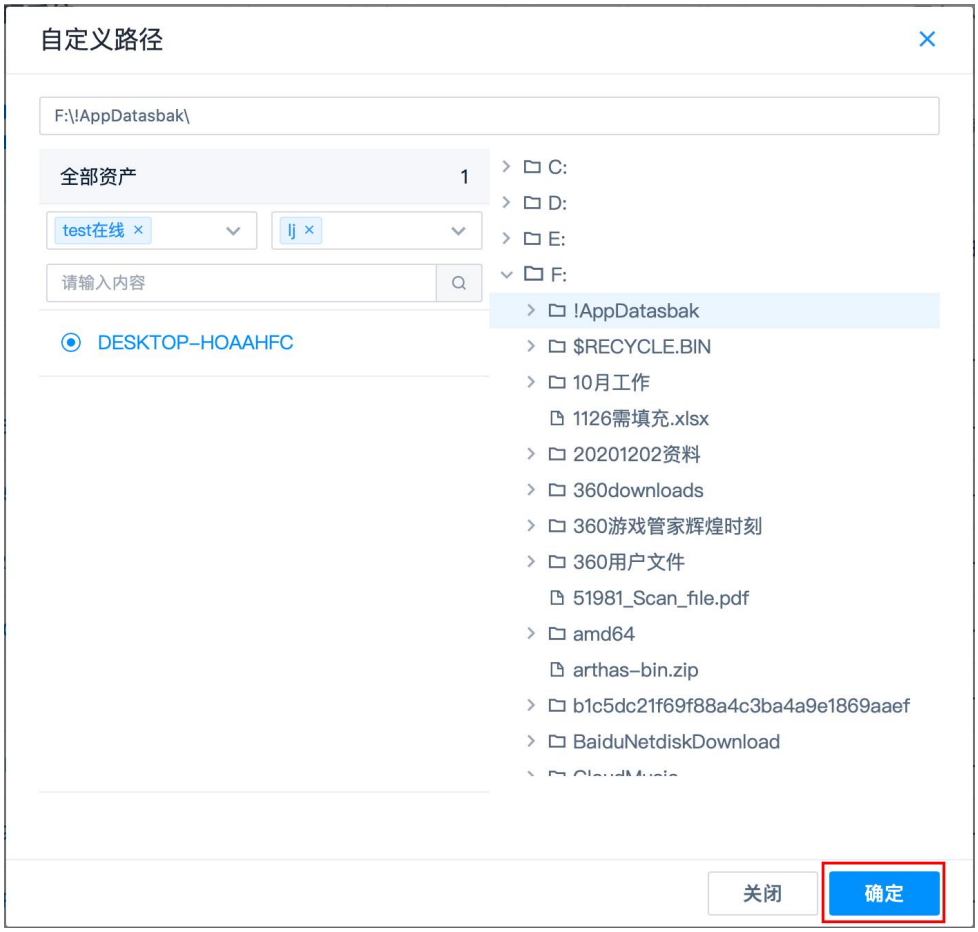
步骤 2. 在导航栏选择“**资产管理➤网马查杀**”，选中需要扫描的资产，点击<**开始扫描**>。

选择多个资产后点击<**快速扫描**>，可进行资产批量扫描。

步骤 3. 在弹出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.　选择需要扫描的资产路径，点击<**确定**>，即可新增自定义路径。



步骤 5.　选中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.　对于正在扫描的资产，点击<**停止扫描**>，在弹出框中点击<**确定**>，即可停止资产网马扫描。

选择多个正在扫描的资产，点击<**停止扫描**>，可进行批量资产停止扫描操作。

6.3.2 查看扫描结果

租户可查看单个资产的网马查杀结果，并可将网马文件加入信任区或进行隔离。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤网马查杀**”，选择需要查看的资产，点击右侧**操作项**的 图标。

步骤 3. 进入**网站后门查杀**页面，可在此页面查看详细网站后门文件，并对文件进行立即隔离。

- 选择多个病毒木马文件后点击<**信任**>或<**隔离**>，可对文件进行批量添加信任区或批量处理操作。
- 点击<**隔离所有**>，可一键处理所有病毒木马文件。

6.3.3 处理网马

租户可对已扫描出的网马进行查杀操作。

步骤 1. 以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤网马查杀**”，选中需要处理网马的资产，点击<**处理网马**>。

选择多个资产后点击<**处理网马**>，可批量进行资产网马查杀。

步骤 2. 在弹出框中点击<**确定**>，即可对资产网马进行处理。

6.3.4 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 EDR 管理平台。

步骤 2. 在导航栏选择“**资产管理➤网马查杀**”，选择具体资产后点击<**导出报告**>，可将所选中的资产网马扫描报告导出至本地。

6.3.5 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 EDR 管理平台，在导航栏选择“**资产管理➤网马查杀**”，点击<**查杀设置**>。

步骤 2. 在弹出框中设置查杀模式，点击<**确定**>即可设置成功。

选择具体资产后点击<**查杀设置**>，可对该资产单独设置网马查杀模式。

6.3.6 相关操作

租户可查看网马查杀的病毒详情，并支持对隔离区和信任区进行添加及删除操作。

◆ **查看病毒详情**

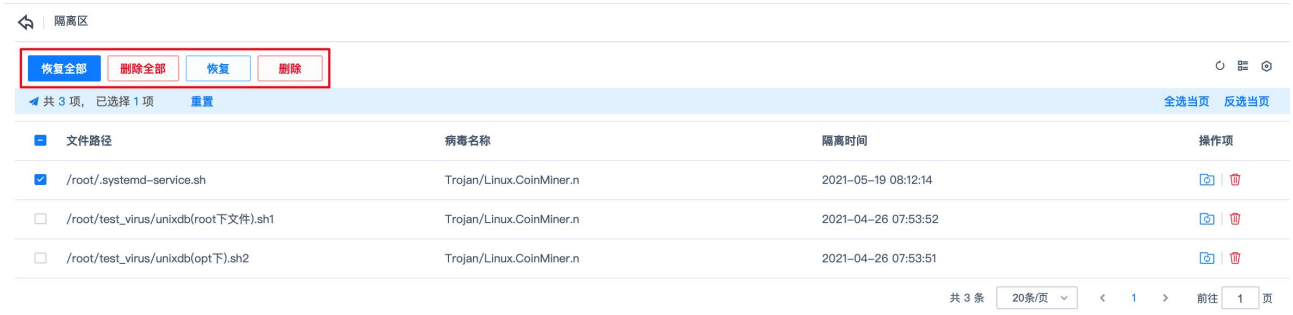
步骤 1. 以租户角色登录 EDR 管理平台，在左侧导航栏选择“**资产管理➤网马查杀**”进入**网马查杀**页面。

步骤 2. 点击网马数，即可在弹窗中查看网马名称及文件路径。

◆ **配置隔离区**

步骤 1. 以租户角色登录 EDR 管理平台，在左侧导航栏选择“**资产管理➤网马查杀**”，点击隔离区数字。

步骤 2. 进入**隔离区**页面，选中需要处理的文件，即可对文件进行恢复、删除、恢复全部、删除全部操作。



◆ **配置信任区**

步骤 1. 以租户角色登录 EDR 管理平台，在左侧导航栏选择“**资产管理➤网马查杀**”，点击信任区数字。

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。

6.4 管理漏洞

租户可在**漏洞管理**页面查看所有资产的漏洞扫描情况，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。

租户还可对所有资产进行批量 Windows 漏洞修复。绿色盾牌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。

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。

6.4.1 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资产操作。

6.4.1.1 资产视角

扫描资产漏洞

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选中需要扫描的资产，点击<**扫描漏洞**>。

步骤 4. 在弹出框中点击<**确定**>，即可对该资产进行扫描。

选择多个资产后点击<**扫描漏洞**>，可对资产进行批量漏洞扫描。

查看扫描结果

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要查看的资产，点击右侧**操作项**的 图标。

步骤 4. 系统进行资产自动扫描，扫描结束后进入**资产漏洞详情**页面。租户可在此页面查看详细漏洞扫描信息，并对资产漏洞进行修复、重新扫描、忽略漏洞及查看漏洞详情操作。

选择多个漏洞后点击<**一键修复**>，可对漏洞进行批量修复。

修复资产漏洞

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要修复的资产，点击<**修复漏洞**>。

步骤 4. 在弹出框中点击<**确定**>，即可修复该资产漏洞。

选择多个资产后点击<**修复漏洞**>，可对批量资产进行漏洞修复。

对于正在修复漏洞的资产，用户可进行停止修复操作。

1) 选中资产后点击<**停止修复**>。

2) 在弹出框中点击<**确定**>，即可停止修复该漏洞。

选择多个正在修复的资产，点击<**停止修复**>，即可批量停止资产漏洞修复。

导出报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**资产视角**页签。

步骤 3. 点击<**导出**>，即可将所有资产的漏洞报告导出至本地。

选择具体资产后点击<**导出**>，可将所选中的资产的漏洞扫描报告导出至本地。

重启资产

对于已进行漏洞修复的资产，租户可进行重启操作。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要重启的资产，点击右侧**操作项**的<**重启**>，即可重启该资产。

6.4.1.2 漏洞视角

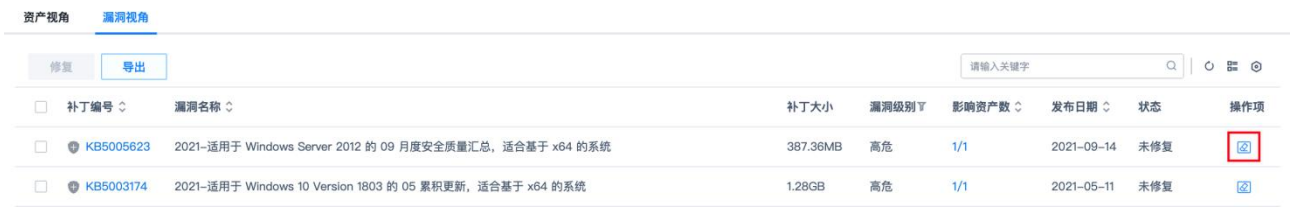
修复资产漏洞

◆ **方式一：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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 图标。



步骤 4. 在弹出框中点击<**确定**>，即可对漏洞进行修复。

此方式适用于修复单个漏洞。

◆ **方式二：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Windows 系统漏洞**”，选择**漏洞视角**页签。

步骤 3. 选中需要修复的漏洞，点击列表上方的<**修复**>，可批量修复资产漏洞。

步骤 4. 在弹出框中点击<**确定**>，即可对漏洞进行修复。

此方式适用于批量修复漏洞。

导出报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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 系统资产的漏洞报告导出至本地。

选择具体资产后点击<**导出报告**>，可将所选中的资产的漏洞扫描报告导出至本地。

6.4.2 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。

6.4.2.1 资产视角

扫描资产

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Linux 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要扫描的资产，点击<**开始扫描**>。

步骤 4. 在弹出框中点击<**确定**>，即可对该资产进行扫描。

选择多个资产后点击<**开始扫描**>，可对资产进行批量漏洞扫描。

导出报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Linux 系统漏洞**”，选择**资产视角**页签。

步骤 3. 点击<**导出**>，即可将所有 Linux 系统资产的漏洞报告导出至本地。

选择资产后点击<**导出**>，可将所选中的资产漏洞报告单独导出至本地。

查看漏洞详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤Linux 系统漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要查看的漏洞类型，点击漏洞数字，即可在弹窗中查看不同等级漏洞的 CVE、漏洞名称及处理建议。

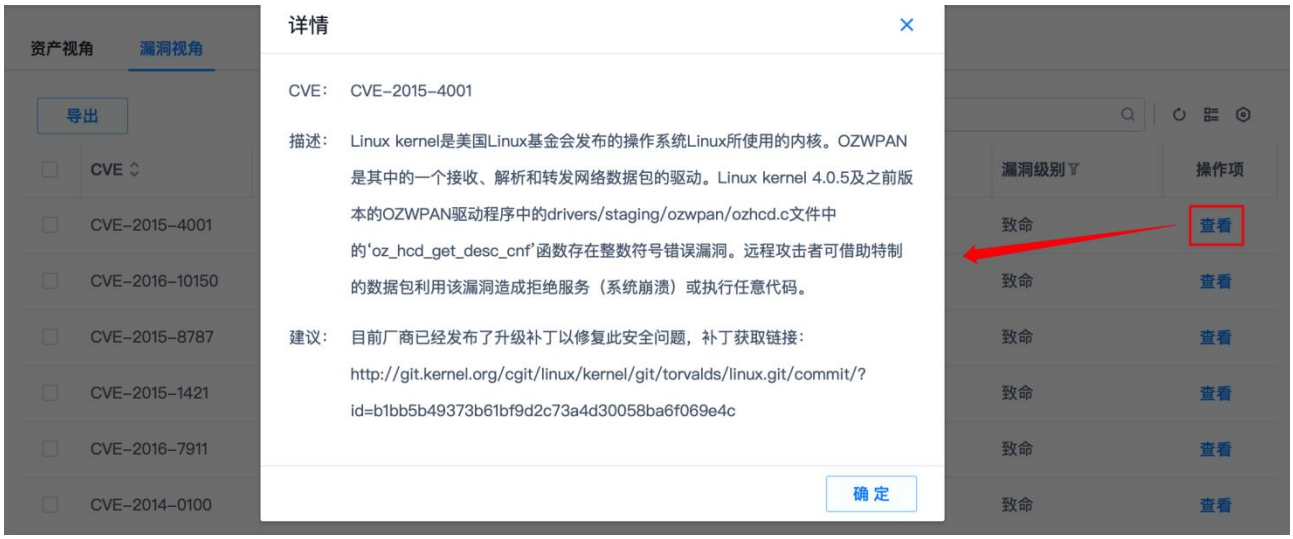
6.4.2.2 漏洞视角

查看漏洞详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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**>，即可在弹出框中查看详细漏洞信息。



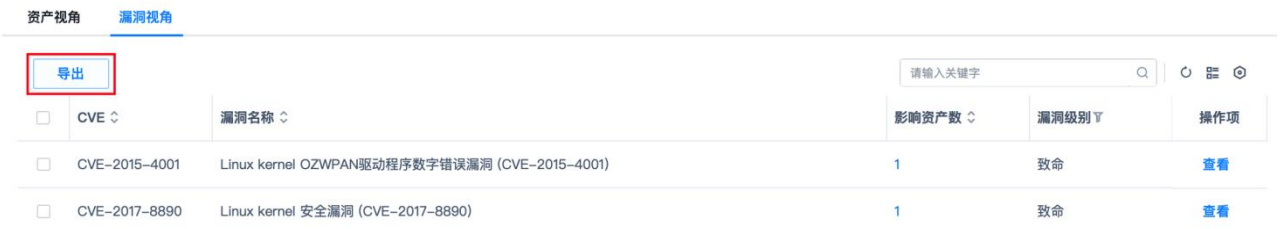
导出漏洞报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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 系统资产的漏洞报告导出至本地。

选择资产后点击<**导出**>，可将该资产漏洞报告单独导出至本地。



6.4.3 其他漏洞

租户可对其他系统漏洞进行扫描及查看漏洞详情操作。

6.4.3.1 资产视角

扫描漏洞

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤其他漏洞**”，选择**资产视角**页签。

步骤 3. 选择需要扫描的资产，点击<**开始扫描**>。

步骤 4. 在弹出框中点击<**确定**>，即可对该资产进行扫描。

选择多个资产后点击<**开始扫描**>，可对资产进行批量漏洞扫描。

导出漏洞报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤其他漏洞**”，选择**资产视角**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。

选择资产后点击<**导出**>，可将该资产漏洞报告单独导出至本地。

6.4.3.2 漏洞视角

查看漏洞详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤其他漏洞**”，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**>，即可在弹出框中查看漏洞详细信息。

导出漏洞报告

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤漏洞管理➤其他漏洞**”，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。

选择资产后点击<**导出**>，可将该资产漏洞报告单独导出至本地。

6.5 管理微隔离

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，租户可针对单条或者选择多条规则进行停用或开启操作，选择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。

6.5.1 新增规则

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤微隔离**”，点击<**新增规则**>。

步骤 3. 进入**新增微隔离**页面。在页面中输入微隔离具体信息，并选择应用资产，点击<**确定**>即可新增成功。

部分参数的说明如下表所示。

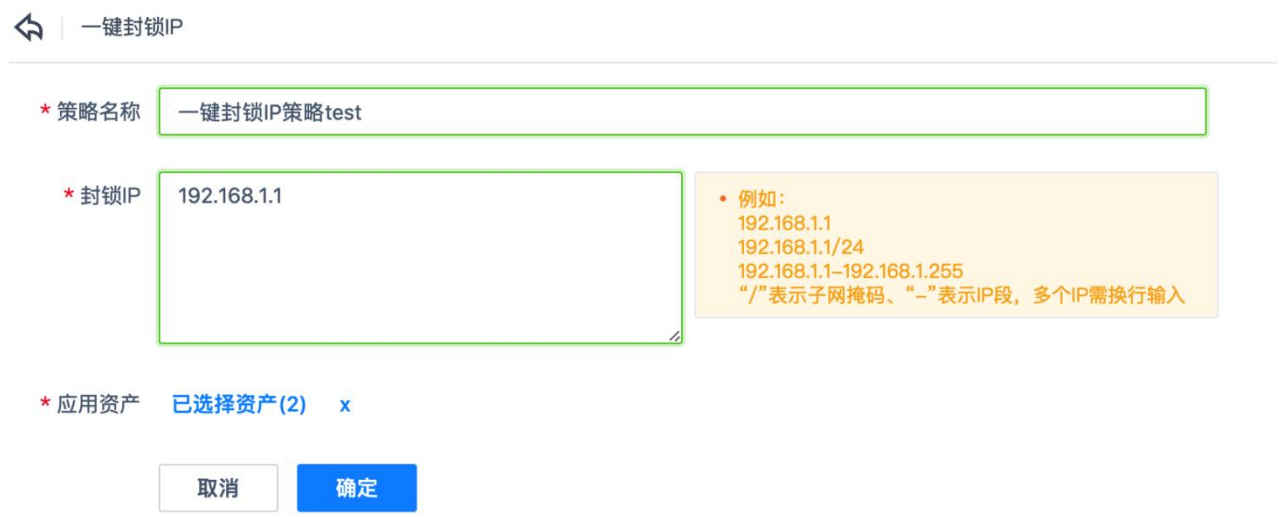
参数	说明
策略类型	◆ 入站：规则仅应用于入站连接，即访问本机的请求。 ◆ 出站：规则仅应用于出站连接，即本机向外发送的请求。 ◆ 双向：规则应用于入站及出站两种连接。
本地 IP	通常是*，多网卡配置不同规则的情况填入具体地址。
本地端口	要限制本机访问其他主机填*，限制其他主机访问本机则填入被访问的相应端口或*（代表全部端口）。
远程 IP	远程主机的 IP 地址或地址段。
远程端口	要限制本机去访问远程主机的端口则填入相应端口或*（代表全部端口），限制远程主机对本机发起访问则填*。
协议类型	通常默认为所有。
处理方式	放行或阻止，放行的优先级高于阻止，可用于屏蔽整段 IP 的访问再开放个别 IP 允许访问。
状态	开启则生效。
应用资产	本条策略应用的相应资产。

6.5.2 一键封锁 IP

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在导航栏选择“**资产管理➤微隔离**”，点击<**一键封锁 IP**>。

步骤 3. 进入**一键封锁 IP** 详细信息页面，在页面中输入 IP 信息并选择应用资产后，点击<**确定**>即可封锁该 IP。



6.5.3 一键关闭端口

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤微隔离**”，点击<**一键关闭端口**>。

步骤 3. 进入**一键关闭端口**详细信息页面，在页面中输入端口信息并选择应用资产后，点击<**确定**>即可关闭该端口。

6.5.4 其他操作

以租户角色登录 EDR 管理平台，在导航栏选择“**资产管理➤微隔离**”，点击相关按钮，可对微隔离规则进行查询、导入、导出、启用、禁用、删除及编辑操作。

选择多个策略后点击相关操作按钮，可对策略进行批量操作。

6.6 设置移动存储

EDR 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带毒入网的问题。
- 支持的格式包括但不限于 FAT32、exFAT、NTFS 等。

6.6.1 设置审批方式

用户可对存储卡进行管控，支持设置自动审批的同时设置设备权限。

步骤 1. 以租户角色登录 EDR 管理平台。

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

步骤 3.　在弹窗中设置是否自动审批和设备权限，点击<**确定**>保存配置。

6.6.2 注册设备

如果需要对特定的移动存储设备开放使用权限，需要进行设备注册。

步骤 1.　登录终端设备，打开主机卫士客户端。主机卫士客户端安装方式请参考添加资产。

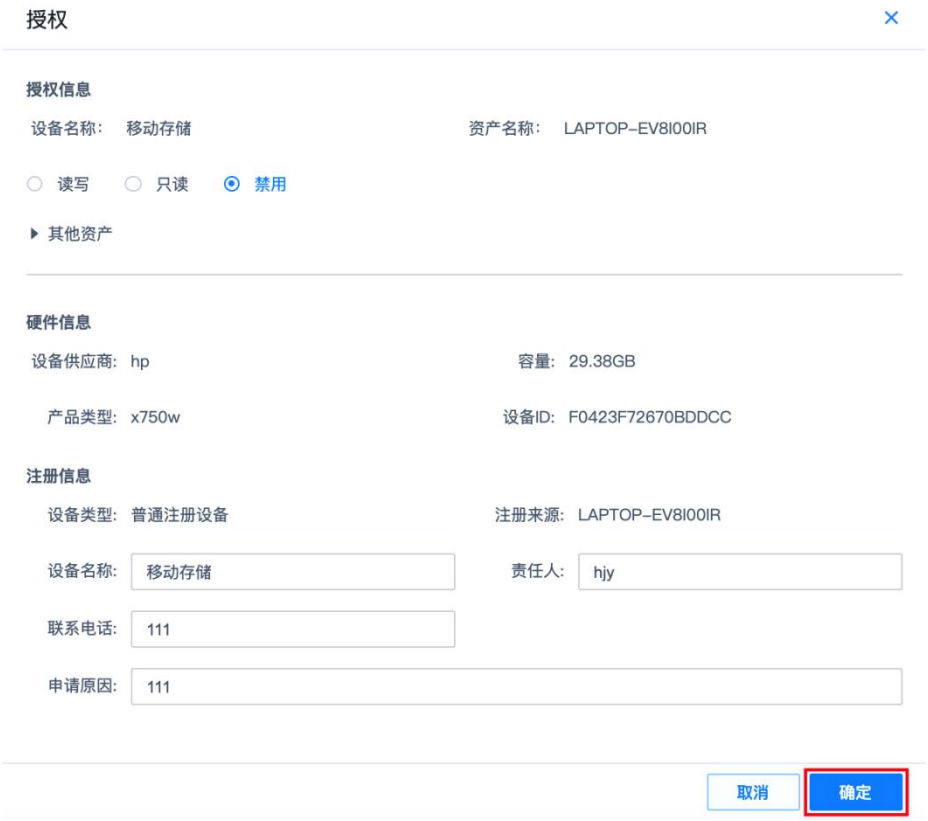
步骤 2.　点击页面右上方的图标，在弹出的下拉框选择“**设备注册**”。

步骤 3.　插入移动存储设备，点击<**申请注册**>提交注册申请。

步骤 4. 以租户角色登录 EDR 管理平台，在左侧导航栏选择“**资产管理➤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 图标。

步骤 6. 在弹窗中选择设备权限，点击<**确定**>，即可完成设备权限设置。



- 注册成功的设备仅对当前资产生效，若需对其他资产生效，可在授权弹窗中为该设备添加**其他资产**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。

6.6.3 其他操作

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤移动存储**”，可对设备进行导出列表及删除设备操作。

- 选择需要删除的设备，点击右侧**操作项**的 图标，即可将该移动存储设备移除。
- 选择多个设备后点击上方的<**删除**>，可批量移除移动存储设备。
- 选择需要导出的移动存储设备，点击<**导出列表**>，即可将所选择的设备列表进行导出。

6.7 管理分组标签

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。同时可为资产选择分组及添加标签，详情请参考编辑资产。

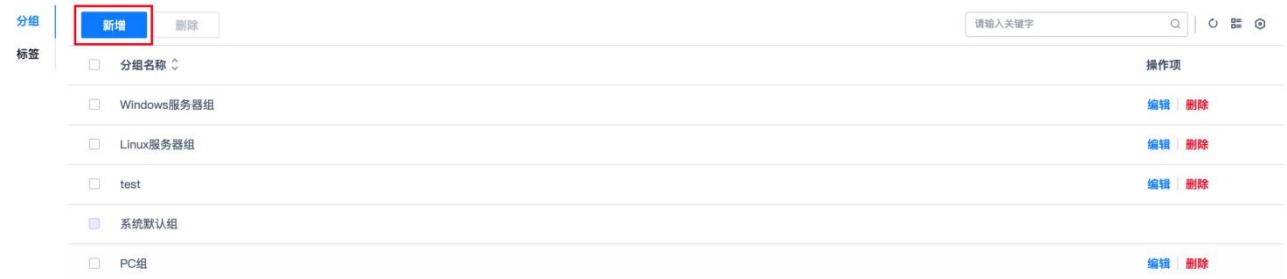
- Windows 7、Windows 8、Windows 10 等操作系统默认划分为 PC 组。
- Windows Server 2003、Windows Server 2008 等操作系统默认划分为 Windows 服务器组。
- Linux 操作系统默认划分为 Linux 服务器组。
- 其他的为系统默认组。

6.7.1 新增分组

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤分组标签**”，选择**分组**页签。

步骤 3. 点击<**新增**>。



步骤 4. 在弹出框中输入组名称后点击<**确定**>，即可新增分组。

6.7.2 新增标签

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤分组标签➤标签**”，选择**标签**页签。

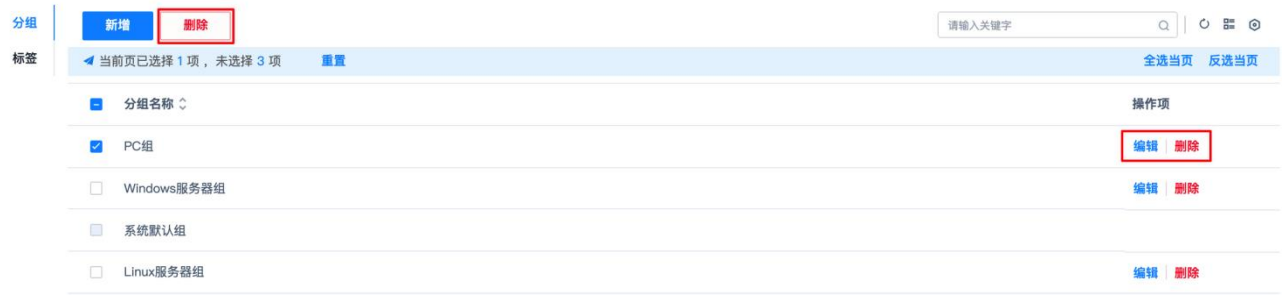
步骤 3. 点击<**新标签**>，在输入框中输入标签名后**回车**，即可新增标签。

6.7.3 其他操作

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产管理➤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。

选择多个分组后点击<**删除**>，可批量删除分组。



步骤 3. 在左侧导航栏选择“**资产管理➤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。

7 高级威胁

仅租户角色具有查看高级威胁操作权限。

7.1 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 EDR 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管理策略。

7.2 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 EDR 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管理策略。

7.3 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 EDR 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管理策略。

7.4 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 EDR 管理平台。

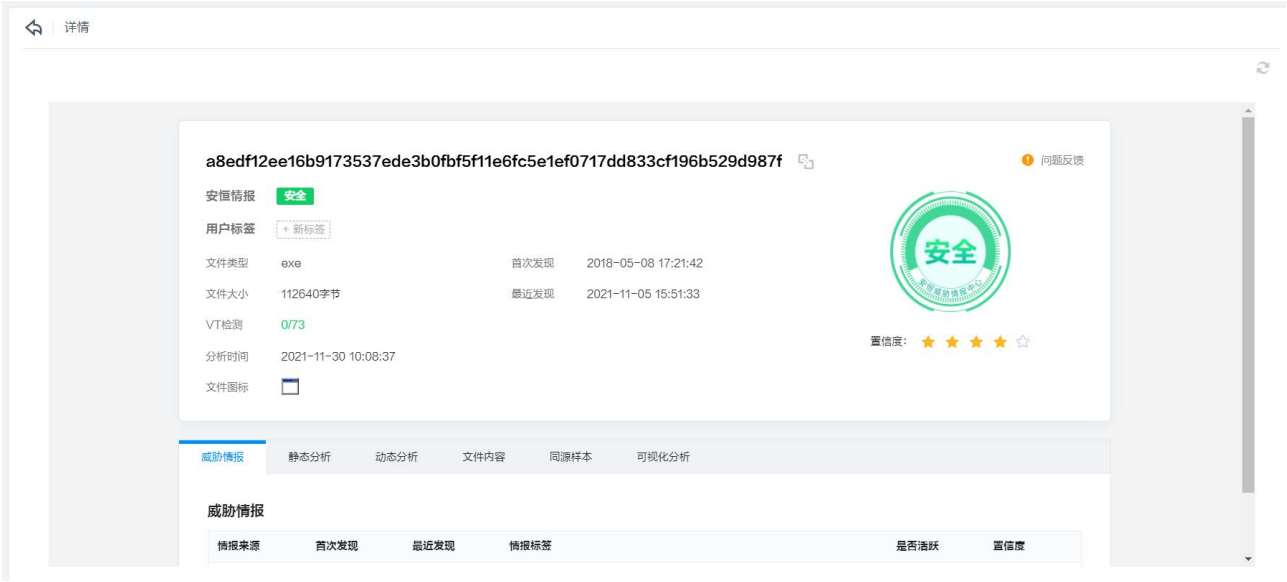
步骤 2. 在左侧导航栏选择“**高级威胁➤情报云脑**”进入**情报云脑**页面。

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。

3) 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。

4) 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。



8 管理策略

策略是 EDR 设备的基本功能，一般分为两部分：匹配条件和执行操作。EDR 会对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。

租户可在**管理策略**页面以模板形式配置主机策略，包括基础信息、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。

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、查看已绑定资产、绑定新资产操作。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。

8.1 新增策略

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**策略管理**”，将光标移至左上角⊕图标，在下拉框中选择“**新增**”。

步骤 3. 在弹出框中填写策略信息，点击<**确定**>，即可新增策略。

8.2 编辑策略

系统默认自带策略模板（内置模板）无法修改保存，只有新增策略模板才可以修改保存。

操作步骤

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**策略管理**”，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。

8.2.1 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：暂无。

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**>。

基础信息配置项和说明如下表。

基础信息配置项	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/字

基础信息配置项	说明
	母/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。

8.2.2 配置系统防护

- 功能：修改策略模板系统防护相关信息。
- 使用场景：适用于需要修改策略模板系统防护场景。
- 使用限制：暂无。

选择**系统防护**页签。

配置项和说明如下表。

配置项	说明	具体请参考
病毒防护	针对网络中流行的病毒、木马进行全面查杀。	配置病毒防护
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。	配置勒索防御
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。	配置挖矿防御
漏洞管理	扫描并且修复系统漏洞，对操作系统进行加固。	配置漏洞管理
系统登录防护	可配置策略对远程登录做限制，对系统账户登录进行细粒度的精准访问控制。	配置系统登录防护

配置项	说明	具体请参考
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。	配置防暴力破解
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。	配置进程防护
文件访问监控	监控目标文件、目录的改写操作。	配置文件访问监控

8.2.2.1 配置病毒防护

- 功能：针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：暂无。

选择**病毒防护**页签。

配置项和说明如下表。

配置项	说明
扫描时机	默认全部勾选，用户可根据实际场景进行勾选。 ◆ 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	病毒防护时的引擎选项： ◆ 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）。

配置项	说明
病毒免疫	用于检测非文件类病毒。
实时扫描	针对实时发现病毒（文件执行、文件修改、存储介质连接时）病毒处理方式： ◆ 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。
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。

8.2.2.2 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：暂无。

选择**勒索防御**页签。

配置项和说明如下表。

配置项	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，

配置项	说明
	避免被勒索病毒破坏。

添加文件保险柜。

步骤 1. 点击<**设置**>。

步骤 2. 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。

8.2.2.3 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：暂无。

操作步骤

步骤 1. 选择**挖矿防御**页签。

步骤 2. 点击图标，即可开启反挖矿引擎，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。

8.2.2.4 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：暂无。

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）**。

8.2.2.5 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：暂无。

操作步骤

- 开启登录防护

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，即可开启系统登录防护。

- 新增登录防护配置信息

步骤 1. 点击<**新增**>。

步骤 2. 弹出**新增规则**对话框，编辑相关信息后，点击<**确定**>。

配置项说明请参见下表。

配置项	说明
登录账号	支持输入“*”，表示所有账户都记录。
IP/IP 范围	访问来源 IP 或者 IP 段。 支持的格式如下： ◆ * ◆ 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。

配置项	说明
处理方式	◆ （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。

8.2.2.6 配置防暴力破解

◆ 功能：对系统登录行为进行一定的限制，防止账号被爆破。
◆ 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：暂无。

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，即可开启防暴力破解。

配置项和说明请参见下表。

配置项	说明
单个 IP 请求时间	触发防暴力破解机制要求：同个 IP 请求时间单位内。
登录失败次数	触发防暴力破解机制要求：IP 登录失败次数。
IP 临时锁定时间	触发防暴力破解机制，被锁定 IP 的时间。

8.2.2.7 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. 将光标移至“**白名单模式**”即可切换黑白名单。

黑白名单配置项和说明如下表。

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 3. 点击<**新增白名单**>。

步骤 4. 在弹窗中输入类型、规则、备注、启用规则，点击<**确定**>即可添加白名单。

配置项和说明如下表。

配置项	说明
类型	文件类型/MD5 值。
规则	输入不超过 255 位的文件路径或者输入不超过 255 位的 MD5 值。
备注	该策略的备注详情。
启用规则	开启或关闭按钮。

8.2.2.8 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：暂无。

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，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。

8.2.3 配置网络防护

- 功能：修改策略模板网络防护相关信息。
- 使用场景：适用于需要修改策略模板网络防护场景。
- 使用限制：暂无。

选择**网络防护**页签。

配置项和说明如下表。

配置项	说明	具体请参考
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。	开启防端口扫描
流量画像	采集资产流量，绘制全景流量图展示主机之间的通讯关系。	开启流量画像
网络分域隔离	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。	新增网络分域隔离

8.2.3.1 开启防端口扫描

- 功能：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。
- 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：暂无。

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 图标，即可开启端口扫描。

配置项和说明如下表所示。

配置项	说明
单个 IP 请求时间范围	触发防端口扫描机制要求：同个 IP 请求时间单位内。
最大扫描端口数量	触发防端口扫描机制要求：最大扫描端口个数。
IP 临时锁定时间	触发防端口扫描机制，被锁定 IP 的时间。

8.2.3.2 开启流量画像

- 功能：采集资产流量，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，即可开启流量画像。

8.2.3.3 新增网络分域隔离

- 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域隔离场景。

◆ 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**网络分域隔离**页签。

步骤 2. 点击<**新增域**>。

步骤 3. 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。

配置项和说明如下表。

配置项	说明
网络域	不大长度超过 10 位的网络域名称。
地址段	地址段可以为 0.0.0.0/24 或者 192.168.1.10-192.168.1.100 或者 192.168.1.1。
备注	对应域的备注详情信息。

8.2.4 配置渗透追踪

渗透追踪包括：单机扩展、隧道搭建、远程持久化、内网探测、痕迹清除。

- 使用场景：适用于需要修改策略模板渗透追踪场景。
- 使用限制：暂无。

配置项的功能如下表所示。

配置项	功能
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泄露。
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。
远程持久化	对失陷后主机远控持久化行为进行检测，可阻断远控。
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。
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。

操作步骤（以单机扩展为例）

步骤 1. 选择**渗透追踪**页签。

步骤 2. 选择**单机扩展**页签，开启单机扩扩展后的 图标，即可开启单机扩展。

步骤 3. （可选）勾选目标防护项目，点击生效方式下的<**仅记录**>可以修改生效方式。

生效方式的说明如下表。

生效方式	说明
仅记录	对产生的威胁项目，不做处理仅记录日志。
关闭	对产生的威胁项目不做任何处置。
阻断并记录	对产生的威胁项目，处理相关防护项目并记录日志。

8.2.5 网页防篡改

此模块为附加功能，需要单独购买许可才有此功能。

- 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：暂无。

操作步骤

- 开启网页防篡改

步骤 1. 选择**网页防篡改**页签。

步骤 2. 点击网页防篡改后的图标，即可开启网页防篡改。

- 新增网页防篡改规则

步骤 1. 选择**网页防篡改**页签，点击<**新增规则**>。

步骤 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。

配置项和说明如下表。

配置项	说明
规则名称	网页防篡改自定义规则名称。
保护目录	网页防篡改自定义规则需要保护的文件目录。
处理方式	触发防篡改自定义规则处理方式： ◆ 阻断并记录：对触发防篡改的规则阻断并记录。 ◆ 仅记录：对触发防篡改的规则不做处理仅记录。
是否启用	网页防篡改自定义规则启用状态。

8.2.6 配置 Web 应用防护

配置 Web 应用防护包括：网站漏洞防护、CC 攻击防护、网站访问控制。

选择 **Web 应用防护**页签。

Web 应用防护的说明如下表。

Web 应用防护	说明	具体请参考
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。	配置网站漏洞防护
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。	配置 CC 攻击防护
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。	配置网站访问控制

8.2.6.1 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：暂无。

选择**网站漏洞防护**页签。

- 开启网站漏洞防护

点击网站漏洞防护后的图标，即可开启网站漏洞防护。

◆ 更改拦截提示内容

步骤 1. 点击<**自定义拦截提示**>。

步骤 2. 在弹窗中输入拦截提醒内容，点击<**确定**>即可更改拦截提示。

◆ 选择防护类型

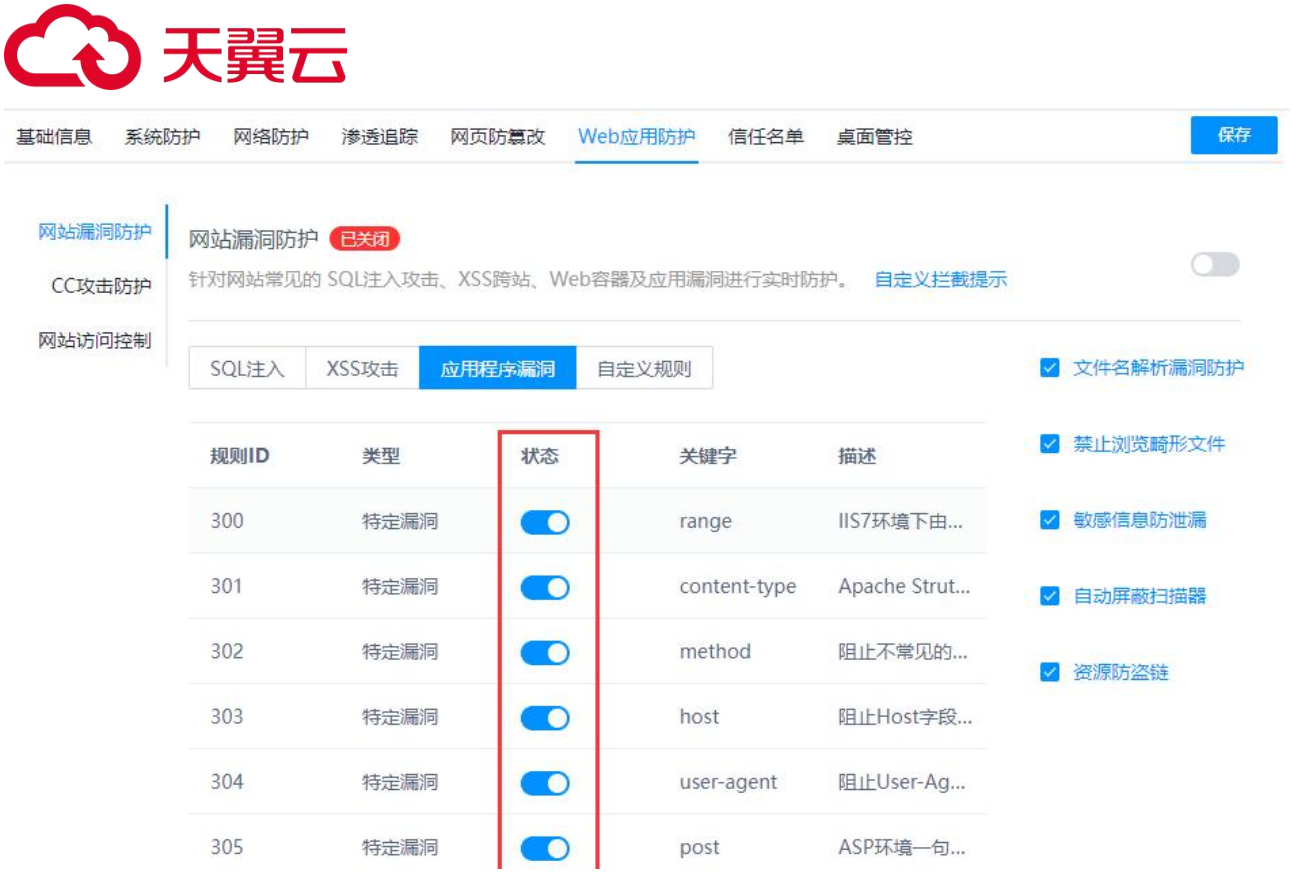
勾选右侧的防护类型即可。

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。

◆ 修改状态

选择目标修改规则 ID，点击**状态**列表下的图标，即可修改状态。



◆ 类型过滤

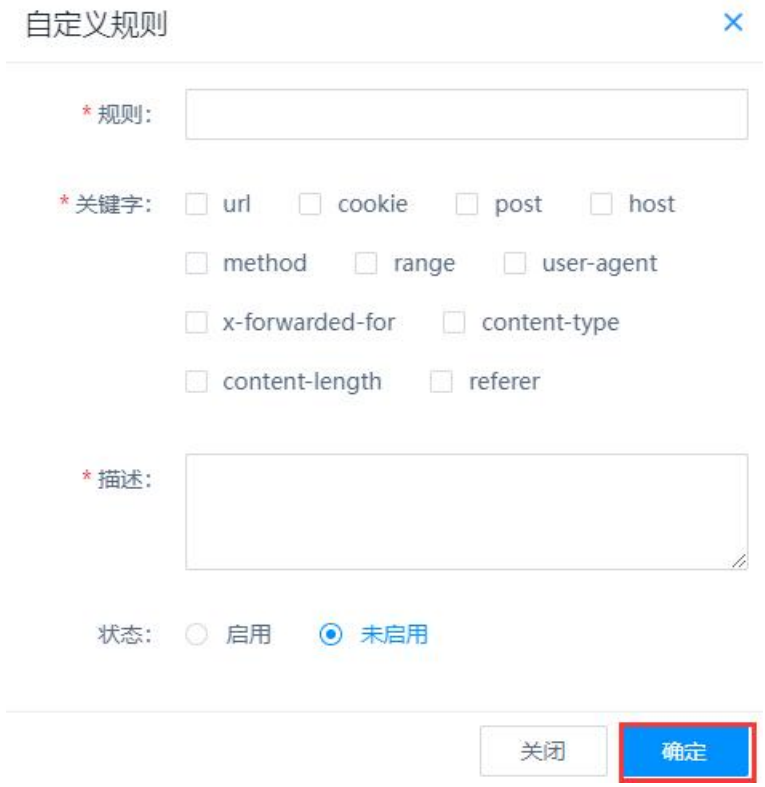
点击**<SQL 注入>/<XSS 攻击>/<应用程序漏洞>**，即可过流出对应的类型。

◆ 自定义规则

步骤 1. 点击<**自定义规则**>。

步骤 2.　点击<**新增**>。

步骤 3.　在弹窗中输入规则、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。



8.2.6.2 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：暂无。

选择 **CC 攻击防护**页签。

- 开启 CC 攻击防护

点击 CC 攻击防护后的 图标，即可开启 CC 攻击防护。

- 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**>。

◆ 防护策略参数说明

防护策略参数的说明如下表。

参数	**说明**
防护策略	◆ 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）

◆ 自定义防护策略

步骤 1. 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”，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。这个选项是为了将正常用户和攻击工具、爬虫类程序进行区分。

8.2.6.3 配置网站访问控制

- 功能：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。
- 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：新增规则前请确认已安装 Web 应用防护插件。

选择**网站访问控制**页签。

- 开启网站访问控制

点击网站访问控制后的图标，即可开启网站访问控制。

◆ 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，编写提示内容后点击<**确定**>。

◆ 新增规则

步骤 1. 点击<**新增**>。

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。

8.2.7 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：暂无。

操作步骤

步骤 1. 选择**信任名单**页签，点击<**新增信任名单**>。

步骤 2. 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。
MD5	对文件 MD5 值匹配，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 匹配，可针对防暴力破解、防端口扫描、Web 防护放行。

8.2.8 配置桌面管控

选择**桌面管控**页签。

各配置项和说明如下表。

配置项	说明	具体请参见
卸载密码	设置客户端卸载密码，防止客户端意外卸载。	配置卸载密码
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。	配置系统性能监控
客户端管理	启用后将显示桌面图标并设置客户端随系统自启动。	配置客户端管理
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。	配置屏幕水印
外设管控	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。	配置外设管理
移动存储管控	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资产详情中操作。	配置移动存储管理
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。	配置违规外联

8.2.8.1 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**卸载密码**页签。

步骤 2. 点击卸载密码后的图标，开启卸载密码。

步骤 3. 输入密码，点击<**保存**>。

8.2.8.2 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：暂无。

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，即可开启系统性能监控。

配置项和说明如下表。

配置项	说明
报警	监控项匹配达到规则阈值进行日志记录。
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。 ◆ 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。

8.2.8.3 配置客户端管理

◆ 功能：启用后将显示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：暂无。

选择**客户端管理**页签。

配置项和说明如下表。

配置项	说明
Windows 桌面快捷方式	启用后将显示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。

8.2.8.4 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：暂无。

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，即可开启屏幕水印。

配置项和说明如下表。

配置项	说明
水印内容	终端显示如下水印内容： ◆ 资产名称 ◆ IP ◆ MAC ◆ 登录用户 ◆ 系统时间
自定义内容	终端显示水印内容除资产名称、IP、MAC、登录用户、系统名称外需要显示额外特定内容。
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。
快间距 mm	终端显示水印内容每块之间的距离，单位是 mm。

8.2.8.5 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，重启系统后方可生效。
◆ 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：暂无。

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，即可开启外设设备。

步骤 3. 选择目标设备，在**权限控制**列选择权限。

8.2.8.6 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。
- 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：暂无。

选择**移动存储管控**页签。

配置项和说明如下表。

配置项	说明
设备读写权限	◆ 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仅可读取权限。

配置项	说明
	◆ 禁用：赋予移动存储设备不可以使用权限。
设备读写权限	◆ 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。

8.2.8.7 配置违规外联

◆ 功能：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。
◆ 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：暂无。

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，即可开启违规外联。

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

步骤 4. 选择“**添加一行**”。输入域名/IP 后点击<**保存**>，再点击<**确定**>，即可保存探测地址。

发现违规外联终端处置方式和说明如下表。

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（重启主机回复网络）	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，需重启方可恢复网络。

8.3 绑定资产

绑定资产是指将策略应用到特定的资产上。创建策略后，必须将策略绑定到资产才会生效。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**策略管理**”，选择需要绑定资产的策略，点击策略右侧的 ••• 图标，选择“**绑定资产**”。

步骤 3. 在弹出框中选择需要绑定的资产，单击<**确定**>，即可将资产绑定至本策略。

有关资产更多信息，请参考资产管理。

8.4 其他操作

以租户角色登录 EDR 管理平台，在导航栏选择“**策略管理**”，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。

9 响应处置

仅租户角色具有响应处置权限。

9.1 检索信息

租户可采集所有终端的监听端口、运行程序、账户信息、软件信息及启动项信息，并支持对信息进行下载。

9.1.1 查看数据详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**响应处置➤信息搜索**”，进入**信息搜索**页面。

步骤 3. 点击<**采集最新数据**>获取资产最新的数据信息。

步骤 4. 选择需要查看的数据类型，点击左侧列表中的具体数据，即可在右侧查看该数据下的详细资产信息。

以查看监听端口为例，选择 22 端口数据，端口下的具体资产信息如下所示。

9.1.2 其他操作

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**响应处置➤信息搜索**”，进入**信息搜索**页面。

步骤 3. 点击右上角↓图标，可以下载当前页面的信息；点击↻图标，可以采集最新数据。

9.2 推送文件

当租户需要下发文件、安装应用程序到资产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 EDR 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>上传所需文件。**
2) **选择执行方式、权限及参数。**
3) **选择被推送的资产。**

步骤 3. 点击<**推送**>即可成功推送该文件。

配置项和说明如下表所示。

配置项	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。
备注	关于此次文件推送的备注信息。
推送资产	选择所需推送的资产。

9.3 设置定期巡检

租户可通过配置定期巡检任务完成定期检测，及时发现资产中的潜在威胁。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。

9.3.1 新增定期巡检任务

步骤 1. 以租户角色登录 EDR 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**页面输入巡检任务信息，点击<**确定**>后即成功新增定期巡检任务。

9.3.2 编辑定期巡检任务

步骤 1. 以租户角色登录 EDR 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 图标。

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。

9.3.3 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**的图标，并在弹出框中点击<**确定**>，即可删除该巡检任务。

多选任务后点击列表上方的<**删除**>，可对巡检任务进行批量删除操作。

9.4 查看流量画像

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，可按资产分组、资产标签、资产名称、资产 IP（且/或）过滤查看。

9.4.1 查看通信关系

租户可在此页面查看资产通信详情，包括资产通信关系图、资产间通信详情及资产全部通信详情。

9.4.1.1 查看资产通信关系图

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**响应处置➤流量画像**”，进入资产展示页面。

步骤 3. 点击需要查看的资产，进入资产**通信关系图**页面，租户可在此页面查看该资产的通信关系。

步骤 4. 点击资产的**指向箭头**，进入资产通信详情页面，可查看两个资产间的通信详情。

9.4.1.2 查看资产通信关系详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**响应处置➤流量画像**”，进入资产展示页面。

步骤 3. 点击需要查看的资产，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资产的所有通信详情，并可根据筛选条件进行通信查询。

9.4.2 自定义模板

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**响应处置➤流量画像**”，点击右侧**自定义模板**列表中的+图标。

步骤 3. 在弹出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。

10 风险评估

租户可使用风险评估功能对资产进行资产评估、勒索评估、挖矿评估及弱口令评估。

- 资产评估：扫描主机弱口令、系统漏洞、恶意进程和高危端口，并进行资产评分。
- 勒索评估：扫描主机弱口令、系统漏洞、恶意进程、资源占用、DNS 历史查询、违规外联记录，并给出勒索风险评级，高风险需立即处置。
- 挖矿评估：扫描主机弱口令、系统漏洞、恶意进程、高危端口、资源占用、DNS 历史查询、违规外联记录，并给出挖矿风险评级，高风险需立即处置。
- 弱口令评估：检查系统中存在的弱口令账号，并展示于风险评估页面。

10.1 资产体检

租户可通过对对应资产进行资产评估、勒索评估、挖矿评估或弱口令评估来及时发现资产中的潜在威胁。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。

10.1.1 资产评估

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**风险评估➤资产体检**”，选择需要评估的资产，点击<**资产评估**>。

步骤 3. 在弹出框中点击<**确定**>，即可对该资产进行资产评估。

选中多个资产后点击<**资产评估**>，可进行批量的资产评估。

10.1.2 勒索评估

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**风险评估➤资产体检**”，选择需要评估的资产，点击<**勒索评估**>。

步骤 3. 在弹出框中点击<**确定**>，即可对该资产进行勒索评估。

选中多个资产后点击<**勒索评估**>，可进行批量资产的勒索评估。

10.1.3 挖矿评估

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**风险评估➤资产体检**”，选择需要评估的资产，点击<**挖矿评估**>。

步骤 3. 在弹出框中点击<**确定**>，即可对该资产进行挖矿评估。

选中多个资产后点击<**挖矿评估**>，可进行批量资产的挖矿评估。

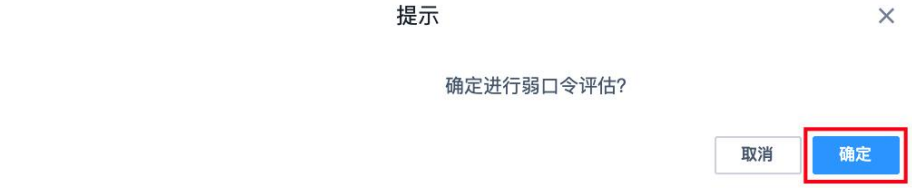
10.1.4 弱口令评估

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**风险评估➤资产体检**”，选择需要评估的资产，点击<**弱口令评估**>。

步骤 3. 在弹出框中点击<**确定**>，即可对该资产进行弱口令评估。

选中多个资产后点击<**弱口令评估**>，可进行批量资产的弱口令评估。



10.1.5 查看评估结果

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**风险评估➤资产体检**”，选择已进行评估的资产，点击资产得分、弱口令下的数字或者勒索风险、挖矿风险下的评估等级，即可查看资产相关风险的详细评估报告。

10.2 基线检查

租户可通过新增任务，批量执行等操作来对指定资产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。

10.2.1 新增任务

步骤 1. 以租户角色登录 EDR 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**>。

步骤 3. 在弹窗中输入任务名称、检查资产、基线策略及执行时间，点击<**确定**>即可生成基线检查任务。

10.2.2 执行任务

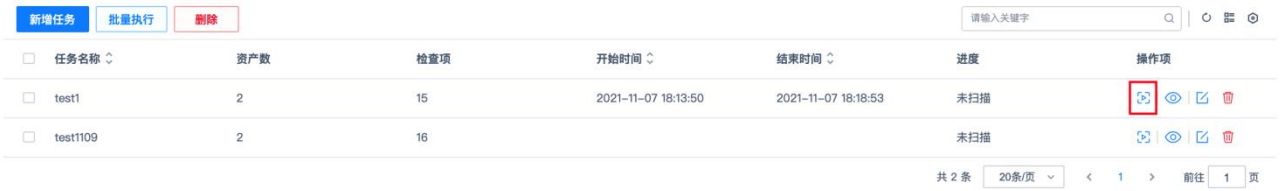
◆ **方式一：**

步骤 1. 以租户角色登录 EDR 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，即可执行该基线检查任务。

此方式适用于执行单个基线检查任务。



◆ **方式二：**

步骤 1. 以租户角色登录 EDR 管理平台。

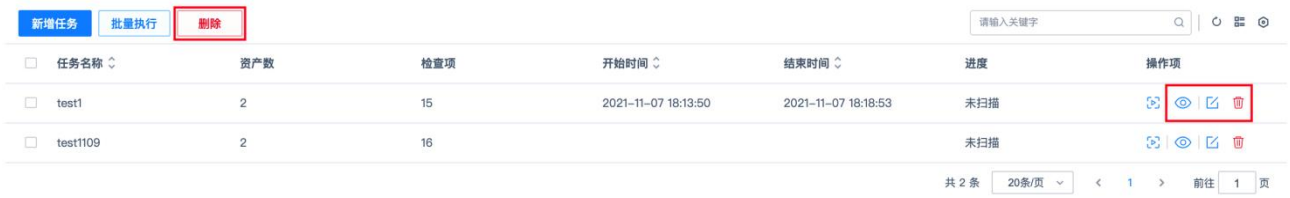
步骤 2. 在左侧导航栏选择“**风险评估➤基线检查**”。

步骤 3. 选中需要执行的任务，点击任务列表上方的<**批量执行**>，即可批量执行基线检查任务。

此方式适用于执行批量基线检查任务。

10.2.3 相关操作

以租户角色登录 EDR 管理平台，在左侧导航栏选择“**风险评估➤基线检查**”，用户可对基线任务进行查看、编辑及删除操作。



11 日志检索

仅租户角色具有日志检索权限。

- 日志：从攻防视角记录包括防护日志、操作日志、运维日志等日志类型。并提供分类和关键字搜索查询功能。
- 报表：对事情趋势、病毒以及风险资产进行图表展示，支持导出各种类型报表。

11.1 防护日志

租户可在**防护日志**页面查看渗透追踪日志、系统防护日志、网络防护日志及 Web 应用防护日志。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**日志检索➤防护日志**”，在筛选框中输入查询条件，点击<**查询**>，即可筛选出符合该条件的防护日志。

可根据资产名称（IP）、关键字、日期、日志类型等信息来进行日志查询。

步骤 3. 点击<**导出日志**>，租户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。

11.2 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、资产解绑日志、启停防护日志及短信发送日志。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**日志检索➤操作日志**”，在筛选框中输入查询条件，点击<**查询**>，即可筛选出符合该条件的操作日志。

可根据资产关键字、日期、日志类型、状态等信息来进行日志查询。

步骤 3. 点击<**导出日志**>，租户可将所查询的操作日志导出至本地。

- 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。

11.3 运维日志

租户可在**运维日志**页面查看资产日志（资产上线、资产离线、资产安装、资产卸载、资产升级、开关机日志、账号创建日志）、性能监控日志（CPU 监控、内存监控、网络 IO 监控、磁盘监控、熔断监控）、外设管控日志（外设使用审计、文件拷贝审计）及运维操作日志（文件推送、病毒扫描、病毒处置、网马扫描、网马处置、漏洞扫描、漏洞修复、弱口令扫描、IP/MAC 绑定）。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**日志检索➤运维日志**”，在筛选框中输入查询条件，点击<**查询**>，即可筛选出符合该条件的操作日志。

可根据资产名称（IP）、关键字、日期、日志类型等信息来进行日志查询。

步骤 3.　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。

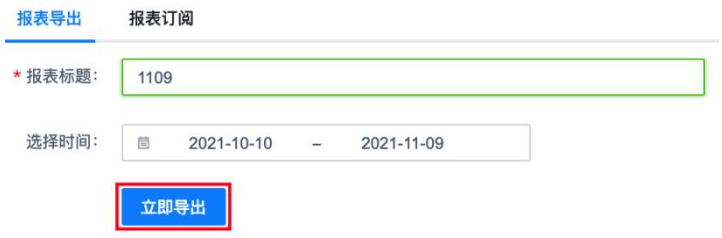
11.4　日志报表

租户可在**日志报表**页面查看事件趋势日志、病毒 Top10 日志、易被勒索 Top10 日志、风险资产 Top10 日志及总体情况日志，日志以图表样式进行展示。

11.4.1　导出报表

步骤 1.　以租户角色登录 EDR 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.　输入报表标题，选择时间后点击<**立即导出**>，即可将所选时间段的日志报表导出至本地。



11.4.2 订阅报表

步骤 1. 以租户角色登录 EDR 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后点击<**保存**>，即可对报表订阅。

订阅后的报表会自动发送至用户所填写的收件人邮箱中。

12 资产全览

可通过资产全览查看全局资产，并根据资产前往指定的租户进行管理。

仅 admin 用户角色具有资产全览权限。

12.1 查看资产详情

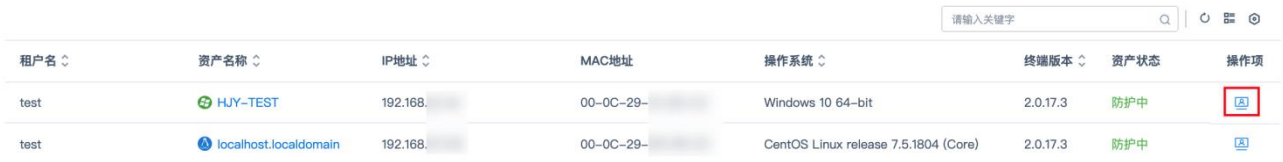
步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产全览**”进入资产列表页面。用户可在此页面查看所有资产的具体信息，包括租户名、资产名称、IP 地址、MAC 地址、操作系统、终端版本、防护状态及操作项等。

12.2 前往租户

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**资产全览**”进入资产列表页面。选择需要登录的租户，点击右侧**操作项**的 图标，即可使用该租户账号登录 EDR 管理平台进行管理。



13 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。

13.1 查看中心详情

步骤 1. 以 admin 用户登录 EDR 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**>。

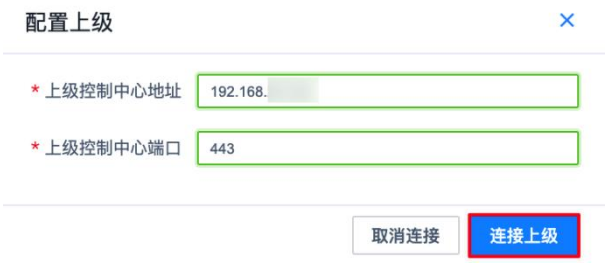
步骤 3. 进入**多级中心详情**页面，可查看该中心数据信息、病毒趋势、资产-病毒排行、资产-漏洞排行、威胁 IP-TOP5 及事件类型占比等数据。

13.2 配置上级中心

步骤 1. 以 admin 用户登录 EDR 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。



13.3 其他操作

步骤 1. 以 admin 用户登录 EDR 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。

选中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。

14 升级管理

admin 用户可在**升级管理**页面进行平台升级、终端软件安装包上传、终端软件更新包上传、病毒库升级及系统漏洞升级操作。

仅 admin 用户具有升级管理操作权限。

14.1 升级管理平台

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 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤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。

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

上传的离线升级包后缀名必须为**.tar.gz**。

14.2 上传终端软件安装包

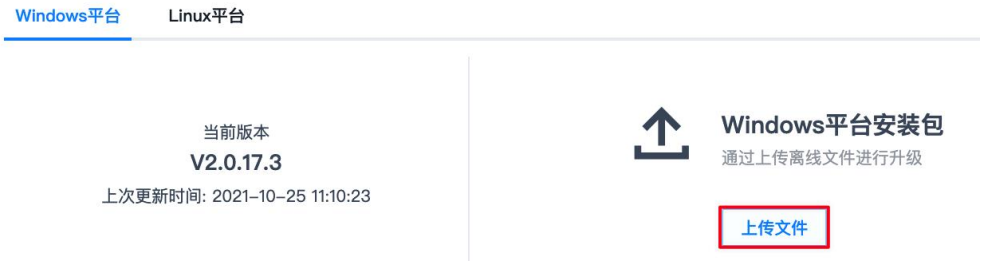
用户可在此页面查看当前终端软件安装包版本，并上传安装包进行离线升级。

14.2.1 Windows 平台

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤终端软件安装包上传**”，选择 **Windows 平台**页签。

步骤 3. 进入 **Windows 平台**页面，点击<**上传文件**>，上传安装包进行 Windows 平台离线升级。



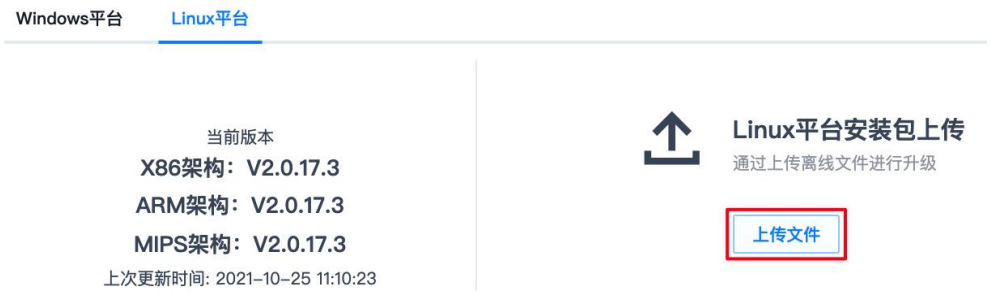
上传的 Windows 平台安装包包名必须为 **win_edr_installer.exe**。

14.2.2 Linux 平台

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤终端软件安装包上传**”，选择 **Linux 平台**页签。

步骤 3. 进入 **Linux 平台**页面，点击<**上传文件**>，上传安装包进行 Linux 平台离线升级。



上传的 Linux 平台安装包包名必须包含 **linux**。

14.3 上传终端软件更新包

用户可在此页面查看 Windows 平台和 Linux 平台终端软件安装包的当前版本，同时可上传终端软件更新包进行离线升级。

14.3.1 Windows 平台

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤终端软件更新包上传**”，选择 **Windows 平台**页签。

步骤 3. 进入 **Windows 平台**页面，点击<**上传文件**>，即可上传更新包进行离线升级。

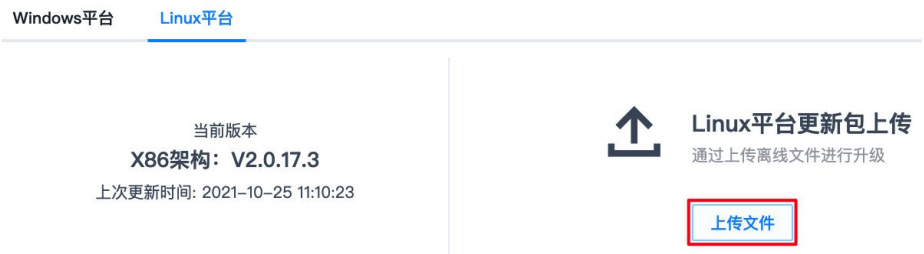
上传的 Windows 平台安装包包名必须包含 **win**。

14.3.2 Linux 平台

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤终端软件更新包上传**”，选择 **Linux 平台**页签。

步骤 3. 进入 **Linux 平台**页面，点击<**上传文件**>，即可上传更新包进行离线升级。



上传的 Linux 平台更新包包名必须包含 **linux**。

14.4 升级病毒库

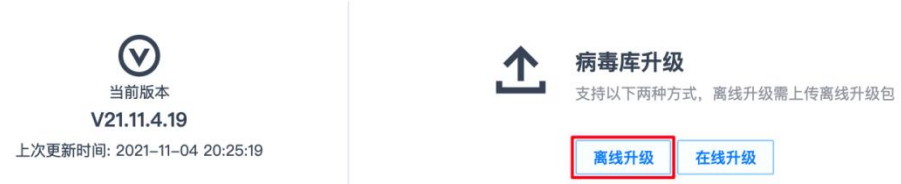
用户可在此页面查看当前病毒库版本，并对病毒库进行离线升级或在线升级。

14.4.1 离线升级

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤病毒库升级**”进入**病毒库升级**页面。

步骤 3. 点击<**离线升级**>，上传离线升级包，即可进行病毒库离线升级。



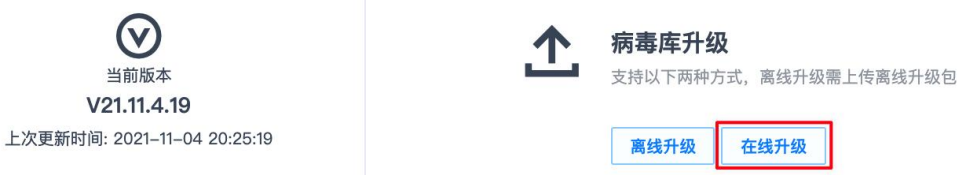
上传的离线升级包包名必须包含 **edr**。

14.4.2 在线升级

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤病毒库升级**”，进入**病毒库升级**页面。

步骤 3. 点击<**在线升级**>，即可进行病毒库在线升级。



14.5 升级系统漏洞

用户可在此页面查看当前系统漏洞库版本，并对系统漏洞库进行离线升级。

14.5.1 离线升级

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤系统漏洞库升级**”进入**系统漏洞库库升级**页面。

步骤 3. 点击<**离线升级**>，上传离线文件可对系统漏洞库进行离线升级。

上传的离线升级包包名必须包含 **msvul**。

14.5.2 在线升级

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**升级管理➤系统漏洞库升级**”进入**系统漏洞库库升级**页面。

步骤 3. 点击<**在线升级**>，即可进行系统漏洞库在线升级。

15 系统管理

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 用户具有配置管理操作权限。
- 仅租户角色具有资产管理操作权限。

15.1 配置管理

admin 用户可在**系统管理**页面进行 Windows 补丁库升级、弱口令库管理、Linux 驱动包上传、配置密码及访问策略等操作。

15.1.1 升级 Windows 补丁库

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。

15.1.1.1 查看已下载补丁

步骤 1. 以 admin 用户登录 EDR 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。

选中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。

15.1.1.2 在线更新补丁

EDR 管理中心可联互联网时，建议在线更新补丁库。

步骤 1. 以 admin 用户登录 EDR 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. 在弹窗中选择操作系统类型及漏洞级别后点击<**确定**>。

15.1.1.3 离线更新补丁

EDR 管理中心无法联互联网时，建议离线更新补丁库。

步骤 1. 以 admin 用户登录 EDR 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。

下载器下载成功后，可通过下载器离线下载补丁包。

步骤 4. 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 EDR 管理平台即可对相应资产进行漏洞修复。

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 EDR 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	◆ 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。详情可参考 Windows 系统漏洞修复资产漏洞部分。
中心和端都不可访问互联网	**admin** 用户登录 EDR 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	◆ 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。

15.1.2 管理弱口令库

用户可在**弱口令库管理**页面查看当前弱口令数量及更新时间，并进行弱口令库离线更新操作。

弱口令库默认随版本更新，一般不需要单独更新。如需要自定义弱口令规则，可按如下步骤进行弱口令库更新：

步骤 1. 进入天翼云社区下载弱口令库文件。

步骤 2. 使用 UE 或者 Nodepad++等编辑类软件打开该文件（编码格式为 Unix，不可使用记事本），将需要添加的弱口令加在文件末尾处，一行一个口令。

步骤 3. 弱口令添加完毕后将该文件打包成 tar.gz 格式的压缩包。

步骤 4. 以 admin 用户登录 EDR 管理平台。

步骤 5. 在左侧导航栏选择“**系统管理➤弱口令库管理**”进入**弱口令管理**页面。

步骤 6. 点击<**上传文件**>上传压缩包，客户端会在 1 小时内同步新的弱口令库。

15.1.3 上传 Linux 驱动包

用户可在 **Linux 驱动包上传**页面查看驱动包详情，并进行驱动包上传及删除操作。

步骤 1. 以 admin 用户登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤Linux 驱动包上传**”进入 **Linux 驱动包上传**页面，点击<**上传驱动包**>。

步骤 3. 选择需要上传的文件后即可完成 Linux 驱动包上传。

上传的驱动包包名必须包含 **edr**。

15.1.4 配置密码及访问策略

用户可在**密码及访问策略**页面配置密码及访问策略。

步骤 1. 以 admin 用户登录 EDR 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、登录 IP 白名单、验证码开关后点击<**提交**>，即可成功配置密码及访问策略。

15.2 资产管理

租户可在此页面进行资产配置、客户端升级、病毒库升级、许可分配、告警配置及添加个人联系方式等操作。

15.2.1 添加资产

租户可在**添加资产**页面查看连接管理中心时所需要的管理员识别码（UUID），并进行系统资产添加。

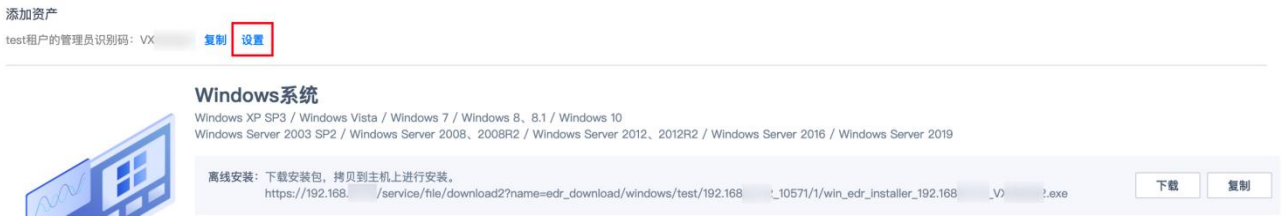
资产添加前可为资产选择分组，不选择的情况下系统会进行自动选择（PC 组、Windows 服务器组、Linux 服务器组）。

15.2.1.1 配置资产

租户在可对新增资产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 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤添加资产**”进入**添加资产**页面，点击<**设置**>。



步骤 3. 在弹窗中配置相关内容，点击<**确定**>保存配置。

15.2.1.2 添加 Windows 系统资产

以租户角色登录 EDR 管理平台，在左侧导航栏选择“**系统管理➤添加资产**”进入**添加资产**页面，租户可在 **Windows 系统**区域进行 Windows 系统资产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资产服务器上，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。以管理员权限登录资产服务器，使用下载链接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。

- **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。

15.2.1.3 添加 Linux 系统资产

以租户角色登录 EDR 管理平台，在左侧导航栏选择“**系统管理➤添加资产**”，进入**添加资产**页面。租户可在 **Linux 系统**区域进行 Linux 系统资产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。

◆ **在线安装**

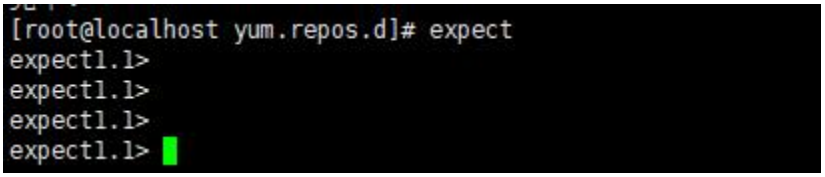
点击**在线安装**的<**复制**>，复制下载链接，在客户端上以管理员权限执行该命令进行安装。

◆ **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**>进行客户端批量安装。

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，执行 **except** 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 except 插件。若没有返回结果，则执行下一步进行插件安装。



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

支持添加的资产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 Server 2003、Windows Server 2008、Windows Server 2008R2、Windows Server 2012、Windows Server 2016、Windows Server 2019 等版本操作系统。
Linux 系统	支持 Centos5.0+、Redhat5.0+、Suse11+、Ubuntu 14+等主流发行版本操作系统。同时支持中标麒麟，银河麒麟，统信 UOS 等国产操作系统。

15.2.2 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按钮后应用到推广页面中。

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤推广部署**”进入**推广部署**页面。

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。

打开推广链接，推广页面如下图所示。

15.2.3 管理资产升级

租户可在**升级管理**页面查看资产详情，并进行主程序升级和病毒库升级操作。

15.2.3.1 查看资产详情

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤升级管理**”进入**升级管理**页面。

步骤 3. 点击**资产名称**可查看该资产的资产指纹详情。

15.2.3.2 升级主程序

◆ **方式一：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤升级管理**”进入**升级管理**页面。

步骤 3. 选中需要升级主程序的资产，点击资产右侧**操作项**的 图标，即可对资产主程序进行升级。

此方式适用于单个资产主程序升级。

◆ **方式二：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤升级管理**”进入**升级管理**页面。

步骤 3. 选中需要升级的资产，点击资产列表上方的<**升级主程序**>，即可对资产主程序进行升级。

此方式适用于批量资产主程序升级。

15.2.3.3 升级病毒库

◆ **方式一：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤升级管理**”，进入**升级管理**页面。

步骤 3. 选中需要升级病毒库的资产，点击资产右侧**操作项**中的 图标，即可对资产病毒库进行升级。

此方式适用于单个资产病毒库升级。

◆ **方式二：**

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2.　在左侧导航栏选择“**系统管理➤升级管理**”，进入**升级管理**页面。

步骤 3.　选中需要升级的资产，点击资产列表上方的<**升级病毒库**>，即可对资产病毒库进行升级。

此方式适用于批量资产病毒库升级。

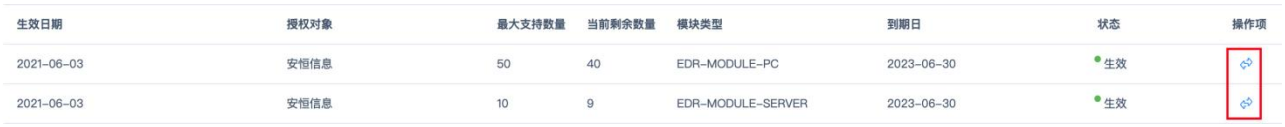
15.2.4　分配许可

租户可在**许可分配**页签对资产进行许可分配。

步骤 1.　以租户角色登录 EDR 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.　选择资产授权对象，点击右侧**操作项**的 图标。



步骤 4.　在弹出框中选择资产，点击<**确定**>即可完成资产许可分配。

15.2.5 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、短信告警配置及 SNMP trap 配置等操作。

15.2.5.1 配置邮件告警

步骤 1. 以租户角色登录 EDR 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。

15.2.5.2 配置 Syslog

步骤 1. 以租户角色登录 EDR 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。

15.2.5.3 配置短信告警

步骤 1. 以租户角色登录 EDR 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**短信告警**页签。

步骤 3. 进入**短信告警**页面，输入短信配置信息后点击<**应用配置**>，即可成功配置短信告警。

另可对短信告警配置进行重置及发送测试短信操作。

15.2.5.4 配置 SNMP trap

步骤 1. 以租户角色登录 EDR 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 **SNMP trap** 页签。

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

另可对 SNMP trap 配置进行重置操作。

15.2.6 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。

15.2.6.1 查看个人信息

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤个人中心**”，选择**个人信息**页签，即可查看个人信息身份。

步骤 3. 点击用户头像，可上传图片切换为自定义头像。

15.2.6.2 配置手机号码

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤个人中心**”，选择**手机号码**页签。

步骤 3. 输入联系电话，并勾选是否启用，点击<**确定**>。

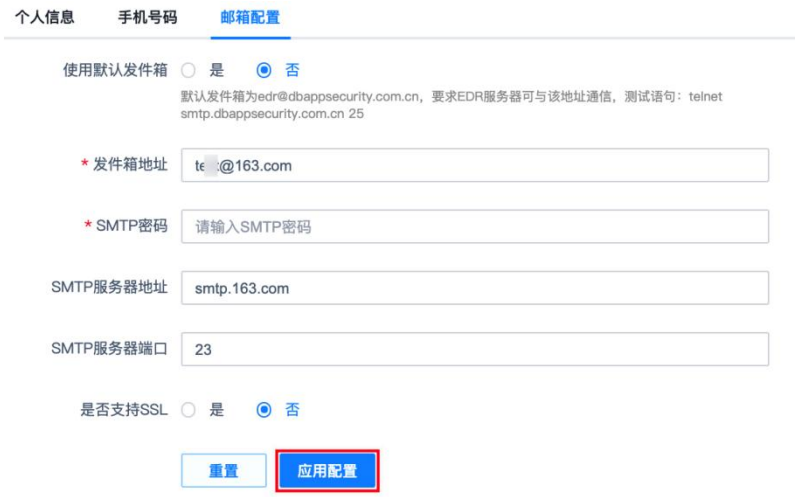
设置为“启用”的手机号码可收取系统紧急通知。

15.2.6.3 配置邮箱

步骤 1. 以租户角色登录 EDR 管理平台。

步骤 2. 在左侧导航栏选择“**系统管理➤个人中心**”，选择**邮箱配置**页签。

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。



16 平台管理

admin 用户可在**运维平台**对 EDR 进行运维诊断、磁盘清理及重置密码操作。

16.1 查看运维诊断结果

步骤 1. 登录 EDR 运维平台。

- **方式一：**登录 EDR 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 EDR 管理平台的 IP 地址。

- 运维平台独立于 EDR 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，请致电天翼云技术支持热线。
- EDR 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 EDR-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**>，可对服务进行重启操作。

选择多个服务后点击<**一键重启**>，可批量重启多个服务。

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**>，可导出该服务的日志信息。

选择多个服务后点击<**导出日志**>，可批量导出多个服务的日志信息。

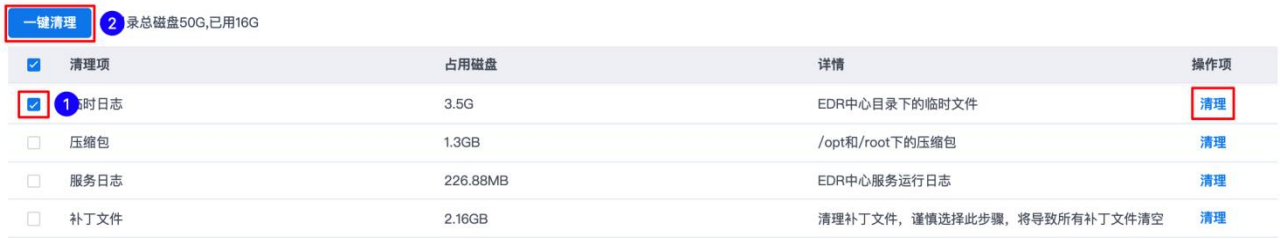
16.2 清理磁盘

步骤 1. 登录 EDR 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。

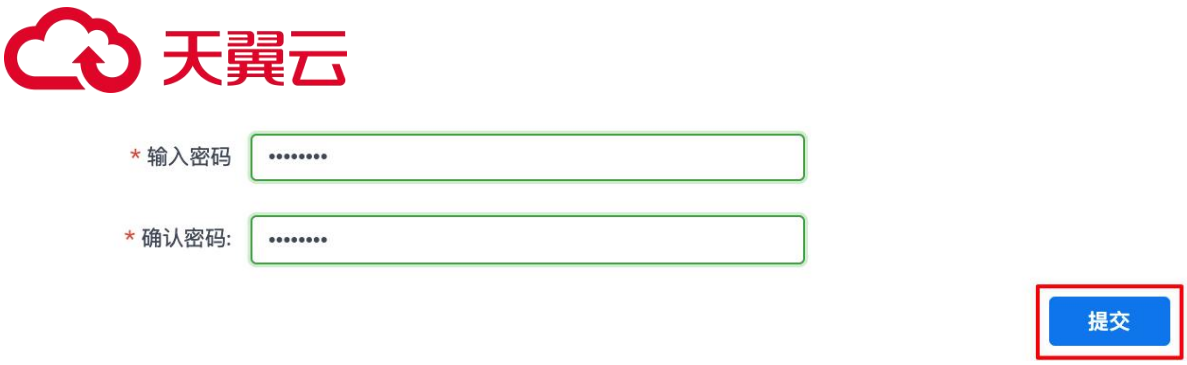
选择多个文件后点击<**一键清理**>，可进行多个文件批量清理。



16.3 重置密码

步骤 1. 登录 EDR 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，用户可对 EDR 管理平台 admin 用户的账户密码进行重置。



16.4 恢复数据

16.4.1 恢复 MySQL 数据

步骤 1. 登录 EDR 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。

◆ **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。

16.4.2 检测 ES 状态

步骤 1. 登录 EDR 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。

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

选中检查项后点击<**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。

17 FAQ

17.1 如何区分 Docker 版本与非 Docker 版本？

EDR V2.0.17 版本分为 Docker 版本与非 Docker 版本两种类型：

- Docker 安装包安装升级通用，且适用于 CentOS 7.x 操作系统。
- 非 Docker 安装包安装升级通用，且适用于 CentOS 6.x 操作系统。

区分方法如下：

使用 root 用户登录 EDR 中心的后台，执行 **docker ps** 命令，若能查看 EDR 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。

18 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。
EDR	端点检测与响应（Endpoint Detection & Response，EDR）是一种主动的安全方法，可以实时监控端点，并搜索渗透到防御系统中的威胁。EDR 是一种新兴的技术，可以更好地了解端点上发生的事情，提供关于攻击的上下文和详细信息。
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。
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。