天翼云 · 服务器安全卫士

用户使用指南

中国电信股份有限公司云计算分公司

目 录

1 产品介绍

1.1 产品定义

服务器安全卫士专注于服务端主机的安全防护，通过对主机信息和行为进行持续监控和分析，快速精准地发现安全威胁和入侵事件，并提供灵活高效的问题解决能力，将自适应安全理念真正落地，为用户提供下一代安全检测和响应能力。

服务器安全卫士采用模块化的组织形式，通过资产清点、风险发现、入侵检测、合规基线四大功能的智能集成和协同联动，实现安全的统一策略管理和快速的入侵响应能力。

1.2 术语解释

Agent：指服务器安全监测与防护代理软件，运行在客户服务器操作系统，该安全代理具备严格的权限和运行负载控制，保护服务器的同时对业务运行不产生影响。

弱口令：容易被别人猜测（包括信息泄露导致）或被破解工具破解的口令均为弱口令。

软件漏洞：应用软件、中间件软件或操作系统软件在设计、实现上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个服务器，窃取服务器中的重要资料和信息，甚至破坏系统服务。

Web 后门： Web 后门是一段网页代码，主要以 ASP、PHP、JAVA 代码为主。由于

这些代码都运行在 Web 服务器端，攻击者通过插入这段精心设计的代码，在 Web 服务器端进行某些危险的操作，获得某些敏感的技术信息或者通过渗透、提权获得服务器的控制权。

POC：Proof of Concept 中文意思是“观点证明”。漏洞报告中的 POC 是指一段说明或者一个攻击的样例，使得读者能够确认这个漏洞是真实存在的。

CVSS：Common Vulnerability Scoring System，即“通用漏洞评分系统”，是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。

Rootkit：Rootkit 是一种特殊的恶意软件，它的功能是在目标服务器上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是 Rootkit 一般都和木马、后门等其他恶意程序结合使用。Rootkit 通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。

1.3 产品功能

资产清点

资产清点致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产进行精准识别和动态感知，让保护对象清晰可见。资产清点功能提供 10 余类主机关键资产清点，800 余类业务应用自动识别，并拥有良好的扩展能力。

风险发现

风险发现致力于帮助用户精准发现内部风险，帮助安全团队快速定位问题并有效解决

安全风险，并提供详细的资产信息、风险信息以供分析和响应。

入侵检测

主机入侵检测系统，将视角从了解黑客的攻击方式，转化成对内在指标的持续监控和分析，无论多么高级的黑客其攻击行为都会触发内部指标的异常变化，从而被迅速发现并处理。

合规基线

合规基线构建了由国内信息安全等级保护要求和 CIS（Center for Internet Security）组成的基准要求，涵盖多个版本的主流操作系统、Web 应用、数据库等。结合这些基线内容，一方面，用户可快速进行企业内部风险自测，发现问题并及时修复，以满足监管部门要求的安全条件；另一方面，企业可自行定义基线标准，作为企业内部管理的安全基准。

病毒查杀

结合多个病毒检测引擎，能够实时、准确地发现主机上的病毒进程，并提供多角度的分析结果，和相应的病毒处理能力，对病毒能够快速、准确、高效地实现从检测分析到处理修复的安全工作闭环。

1.4 产品规格

- 支持主流 Linux（64 位）和 Windows server64（位）服务器

  主流 Linux 版本（64 位）如下：

  Oracle：5、6、7

RHEL：5、6、7

CentOS：5、6、7、8

Ubuntu：10-19

SUSE：9-15

Debian：6、7、8、9、10

OpenSUSE：10-15

NeoKylin：6、7

YHKylin：4

Redflag：9

Deepin：15

iSoft：4

- 主流 Windows 版本（64 位）如下：

Windows Server 2008

Windows Server 2012

Windows Server 2016

Windows Server 2019

Windows Vista

Windows 7

Windows 8

Windows 10

- 可提供以下产品规格：

服务器安全卫士产品规格分为三种：基础版、企业版、旗舰版。基础版为免费版本，企业版和旗舰版为付费版本，三个版本产品规格详见表 2-1 所示。

表 2-1 产品规格

产品功能	功能介绍	描述	基础版	企业版	旗舰版
资产清点	资产清点	自动清点主机内部资产如进程、端口、账号、应用等，实时掌握主机内部资产变化，为安全分析提供数据基础。	X	√	√
风险发现	安全补丁	对安全补丁进行周期性自动检测，提供详细补丁说明和修复方案。	X	√	√
	漏洞检测(*)	精准本地分析漏洞，包含精准 POC 探测和版本漏洞探测；支持 CVSS 等漏洞信息详细描述，支持漏洞修复影响检查；提供命令级漏洞修复建议。	**只检测不提供修复建议**	√	√
	弱密码检查	弱口令自动检测，自动匹配账号名相关易猜解密码，支持弱口令字典自定义。	X	√	√
	应用风险(*)	检测 Linux 关键攻击路径上常用应用的配置型风险。	X	X	√
	系统风险(*)	检测 linux 上由于系统配置的产生的安全风险。	X	X	√
	账号	检测 linux 系统中的由于账号的配置	X	X	√

	风险(*)	产生的安全风险。			
入侵检测	暴力破解	实时监控主机上发生的爆破行为，并提供封停爆破来源 IP 的能力。	√	√	√
	异常登录	实时异常登录监控，发现异常 IP、区域、时间等的异常登录。	√	√	√
	反弹 shell	实时监控主机上反向连接的行为，并提供详细的攻击记录。	X	X	√
	后门检测	精准发现系统内后门程序，提供详细后门程序分析报告与修复建议。	X	√	√
	本地提权(*)	支持实时进程提权监测，支持进程提权过程详细记录。	X	X	√
	Web 后门	多维度 Web 后门识别，支持规则匹配、相似度匹配、沙箱检测、模式分析引擎检测等多种机制检测，具备实时监测能力。	X	√	√
	可疑操作(*)	实时对 Bash 命令进行审计，发现可疑的黑客操作，支持自定义审计规则	X	X	√
	Web 命令执行	能够发现 Web RCE 和进程异常的执行事件	X	X	√
病毒查杀	病毒查杀	结合多个病毒检测引擎，能够实时准确地发现主机上的病毒进程，并提供多角度分析结果，以及相应的病毒处理能力，对病毒能够快速、准确、高效地实现从检测分析到处理修复的安全工作闭环。	X	√	√
合规基线	系统基线	对各版本的 linux 系统、windows 系统按照等保、CIS 的基线要求检测，覆盖主流操作系统的检测	X	√	√
	应用基线	支持对常用应用的等保、CIS 基线的检测	X	√	√
	数据库基	支持对主流数据库的等保、CIS 基线的检测	X	√	√

	线				
	自定义基线	支持自定义基线，对于不同的检查基准，灵活制定不同检查强度的标准	X	X	√
快速任务	快速任务	提供一些特定的安全任务，方便用户在日常安全工作中快速执行。	X	X	X
其他功能	主机管理	提供对所有安全服务器的管理功能，可设置主机分组，标签，运维管理信息，方便用户管理主机	√	√	√
	报表系统	提供各类实用美观的安全报表，供汇报时使用，可支持 html，word 格式。	X	X	√
	通知系统	可灵活配置接收的通知类型、通知方式及通知人	√	√	√

注：（*）功能暂不支持 windows 操作系统

1.5 产品优势

扫描速度快

基于 Agent 扫描，执行主机资产清点和风险发现功能，扫描 N 台主机和 1 台所需时间一样。

精准检测

设立数万个监测指标，建立多维度、多层次的纵深检测体系，检测结果精准。

资源占用低

CPU 占用率<1%，内存占用<40M，消耗极低。

强大的统一安全管控平台

服务器安全卫士是安全问题和安全事态的可视化实时分析平台，可实现统一策略管理，分角色管理，分账号管理，有效管理大批量主机系统。

精准查杀

结合多引擎病毒检测引擎，实时监控病毒进程，查杀率高。多方分析“实锤”病毒信息，检测结果一站化体现，坚实可靠。

丰富的扩展功能

根据不同的业务需求（Web 服务器、存储服务器等），选择不同的功能组合，可根据需求灵活定制安全方案做到最佳适应；

根据用户的业务情况，通过用户自身的业务系统与我们的 API 结合，向用户输出 API 集成开发的能力。

1.6 应用场景

主机安全防护

主机安全，是企业网络安全的最后一公里，一旦被攻击会直接影响到企业业务。正因如此，国家相关法律法规对主机的入侵检测和恶意木马的防护都有严格的要求。入侵检测以生产服务器为安全防护中心，横跨物理和虚拟环境，私有云、公有云和混合云等多种云环境下物理机、云主机、虚拟机，甚至容器等工作负载，能够实时、准确地感知入侵事件，发现失陷主机，并根据入侵场景不同，提供了包括自动封停、手动隔离、黑 / 白名单和自定义处理任务等多种处理方式，让用户从根本上 解决入侵事件。有主机的地方就需要主机入侵检测。

发现新型漏洞

至今已积累 30000+的高价值漏洞库，包括系统/应用漏洞、EXP/POC 等大量漏洞，覆盖全网 90% 安全防护。同时，基于 Agent 的持续监测与分析机制，能迅速与庞大的漏洞库进行比对，精准高效地检测出系统漏洞。更新的补丁库以及 Agent 探针式的主动扫描，能及时、精准发现系统需要升级更新的重要补丁，第一时间帮助用户 发现潜在可被黑客攻击的危险。深入检测系统中各类应用、内核模块、安装包等各类软件的重要更新补丁，结合系统的业务影响、资产及补丁的重要程度、修复影响情况，智能提供最贴合业务的补丁修复建议。

等保合规检查

帮助客户实现主机系统安全基线的建立，形成针对不同系统的详细漏洞要求和 Checklist 要求，为标准化的技术安全操作提供了框架和标准，主要的应用场景有新业务系统上线安全检查，合规性安全检查（上级检查)、日常安全检查等。通过对目标主机系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险。

2 购买指南

2.1 价格

服务器安全卫士根据购买的授权数量，按包年包月进行计费，分为基础版、企业版、旗舰版。基础版为免费版本，企业版和旗舰版为付费版本，**不同服务器支持开通不同版本功能。**各版本功能见：产品规格。各版本价格如下：

产品名称	规格	标准价格(元/月/台)
服务器安全卫士	基础版	0
	企业版	60
	旗舰版	200

2.2 开通

登陆云平台，进入产品-安全-服务器安全卫士产品介绍页面，点击“立即开通”，进入订单开通页面。

选择规格、授权数量和订购时长，提交订单，购买成功后即可进入控制中心-“服务器安全卫士”界面进行后续操作。

- **产品介绍界面**

- **订单开通页面-基础版**

- **订单开通页面-企业版**

- 订单开通页面-旗舰版

- 控制中心

2.3 续订

登陆云平台，进入控制中心-“服务器安全卫士”界面，点击需要续订订单对应的“续订”按钮，进入续订页面。选择购买时长，提交订单。

注意：只能延长，不能缩短截止日期。

- **console 页面**

- **续订页面**

2.4 扩容

登陆云平台，进入控制中心-“服务器安全卫士”界面，点击需要扩容订单对应的“扩容”按钮，进入扩容页面。选择要增加的授权数量，提交订单。

注意：只能增加授权数量，不能减少数量。

- **console 页面**

- **扩容页面**

2.5 升级

登陆云平台，进入控制中心-“服务器安全卫士”界面，点击需要升级订单对应的“升级”按钮。

- 当该订单规格为基础版时，点击“升级”，弹出开通服务界面，规格默认“企业版”，可切换规格为“旗舰版”。
- 当该订单规格为企业版时，点击“升级”，弹出开通服务界面，规格只能选择“旗舰版”。
- 当该订单规格为旗舰版时，旗舰版为最高版本，不可再升级。

选择升级规格，提交订单。

注意：只能从基础版升级到企业版或旗舰版，或从企业版升级到旗舰版，不支持降级（比如从旗舰版降为企业版）。

- **console 页面**

- **升级页面-当前版本为基础版**

- **升级页面-当前版本为企业版**

2.6 退订

服务有效期内，支持退订，按已使用天数进行扣费，未使用天数的费用退还。登陆云平台，进入控制中心-“服务器安全卫士”界面，点击需要退订订单对应的“退订”按钮，提交退订订单即可。

注意：已退订的订单，不能再登录控制台。

- **console 页面**

3 快速入门

服务器安全卫士分为基础版、企业版、旗舰版。基础版为免费版本，为您提供漏洞检测、暴力破解、异常登录等功能。企业版和旗舰版为付费版本，提供更全面更强大的功能来保障您的服务器安全。各版本功能见：产品规格

3.1 登录

登陆云平台后， 进入控制中心-“服务器安全卫士”，点击订单对应的“控制台”按钮，可登录服务器安全卫士控制台。

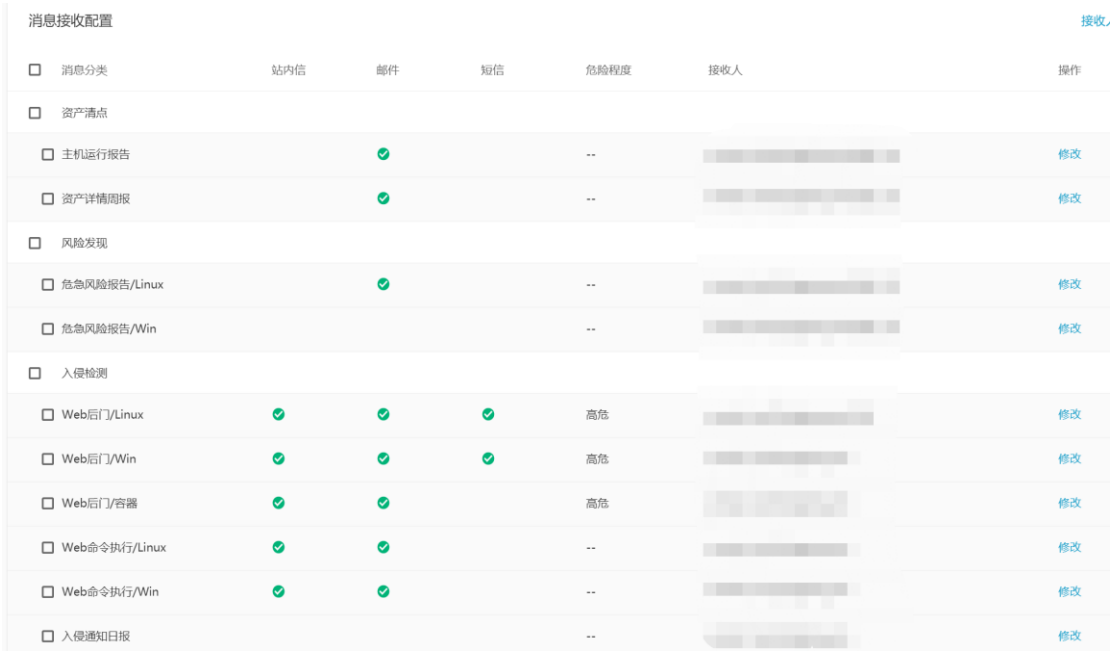
- **console 控制台**

3.2 设置通知方式

产品到期、入侵告警等，支持邮箱、站内信和短信通知。

初次登陆服务器安全卫士时，需要录入手机号和邮箱，以便进行通知。

也可以登录消息中心——消息接收设置界面，设置接收的消息类型、接收方式，或增加接收人。



3.3 安装 Agent

- **前提条件**

Agent 支持主流 64 位操作系统，支持的操作系统见：产品规格。请在安装 Agent 前，确认待安装的服务器是否在可支持范围内。

- **安装方法**

登陆云平台后， 进入控制中心-“服务器安全卫士”，点击订单中的“控制台”，进入服务器安全卫士控制台，选择通用功能-系统设置-Agent 安装，进入 Agent 安装界面，选择对应的操作系统，设置主机信息，按安装引导进行安装即可。

- Linux 仅支持命令安装。

- Windows 支持命令安装、安装包安装、命令+安装包安装。

（1） 命令安装——可适用于批量安装（直连主机需使用 PowerShell 组件）。

（2） 安装包安装——适用于单台安装，用户可使用操作界面安装。

（3） 安装包+命令————适用于批量安装，安装包分发到各主机，批量执行命令

3.4 功能使用

Agent 安装完成后，您可使用服务器安全卫士相关功能。

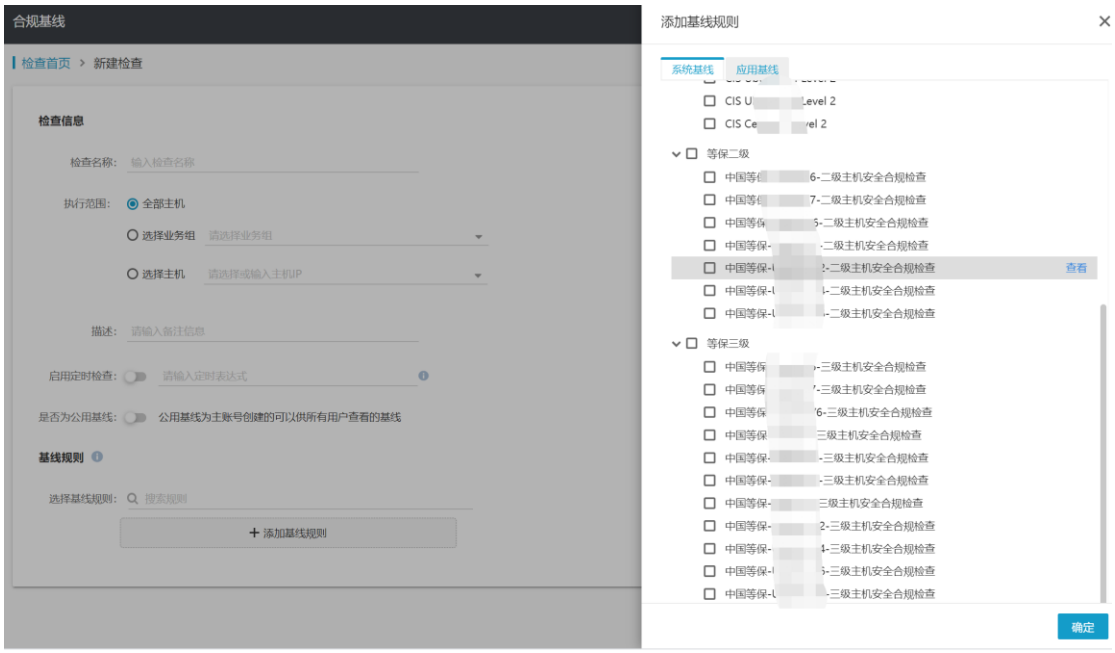
- 您可以在资产清点页面，查看对应操作系统服务器资产清点信息，包括：账号、进程、端口、web 服务、数据库等信息。
- 您可以在风险发现-总览界面，查看您服务器风险概览情况，包括风险项统计、风险分布、风险趋势等。
- 您可以在风险发现下，使用安全补丁、漏洞检测、弱密码检查、应用风险、系统风险、账号风险功能。支持从风险维度和主机维度两种视图下，查看风险信息。
  - 安全补丁：对安全补丁进行周期性自动检测，提供详细补丁说明和修复方案。
  - 漏洞检测：精准本地分析漏洞，包含精准 POC 探测和版本漏洞探测；支持 CVSS 等漏洞信息详细描述，支持漏洞修复影响检查；提供命令级漏洞修复建议。
  - 弱密码检查：弱口令自动检测，自动匹配账号名相关易猜解密码，支持弱口令字典自定义。
  - 应用风险：检测 Linux 关键攻击路径上常用应用的配置型风险。
  - 系统风险：检测 linux 上由于系统配置的产生的安全风险
  - 账号风险：检测 linux 系统中的由于账号的配置产生的安全风险。
- 您可以在入侵检测下，使用暴力破解、异常登录、反弹 shell、本地提权、后门检测、Web 后门、可疑操作、Web 命令执行功能。
  - 暴力破解：实时监控主机上发生的爆破行为，并提供封停爆破来源 IP 的能力，支持自动封停和手

动封停，可设置白名单。

- 异常登录：实时异常登录监控，发现异常 IP、区域、时间等的异常登录，在使用前，必须先设置正常登录规则，否则异常登录功能不起作用，无法进行监控。支持封停和解封。
- 反弹 shell：实时监控主机上反向连接的行为，并提供详细的攻击记录，支持设置白名单规则，支持对反弹 shell 行为进行阻断。
- 本地提权：支持实时进程提权监测，支持进程提权过程详细记录。
- 后门检测：精准发现系统内后门程序，提供详细后门程序分析报告与修复建议。
- Web 后门：多维度 Web 后门识别，支持规则匹配、相似度匹配、沙箱检测、模式分析引擎检测等多种机制检测，具备实时监测能力。
- 可疑操作：实时对 Bash 命令进行审计，发现可疑的黑客操作，支持自定义审计规则
- Web 命令执行：能够发现 Web RCE 和进程异常的执行事件

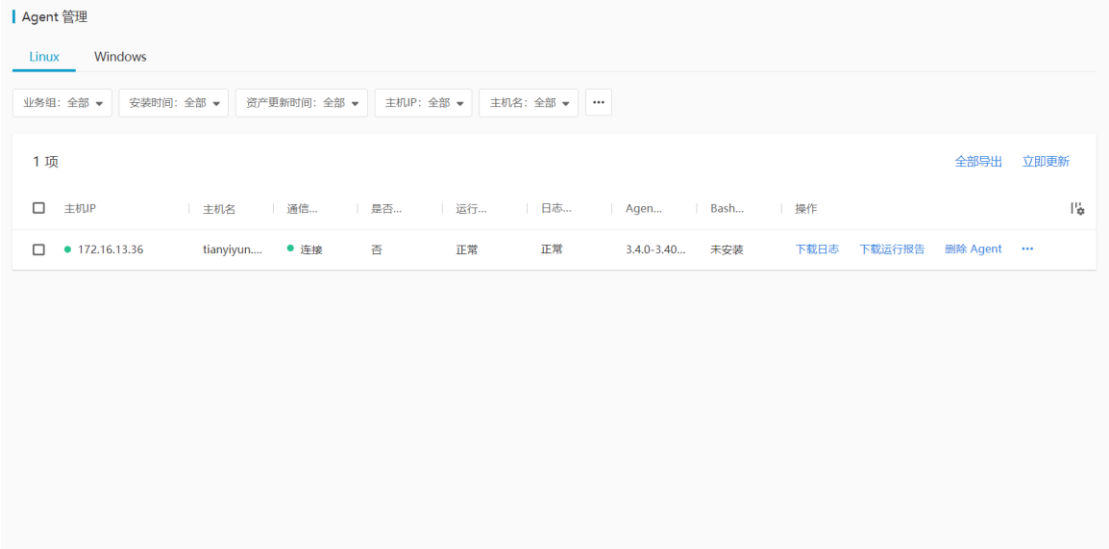
- 您可以在病毒查杀下，设置查杀引擎和处置方式，支持对单台或多台服务器产生的病毒进行自动处置和手动处置。

- 您可以**在合规基线**下，根据等保、CIS 的基线要求设置基线检查任务，支持定时检查，可导出检查结果。



3.5 管理 Agent

登陆云平台，进入控制中心-“服务器安全卫士”界面，点击订单中的“控制台”，进入服务器安全卫士控制台，选择通用功能-服务工具-Agent 管理，进入 Agent 管理界面，即可管理 Agent 运行状态。



在排查问题的过程中，可设置 Agent 运行级别，下载日志和运行报告。

1）设置运行级别：

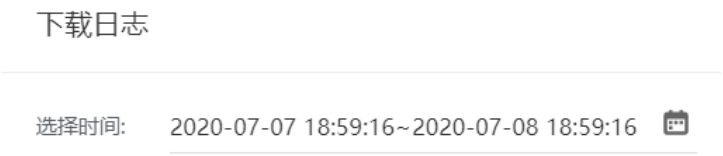
—正常：Agent 拥有完整能力，执行服务器的任务。

—降级：是一种保护模式，Agent 不再接受服务器下发的任务，直至恢复为非"降级"状态。

—停用：停止 Agent 业务功能，只保留基本通信能力和任务执行能力（如：卸载，恢复在线)。

2） 设置日志级别

3）下载日志



4）下载运行报告

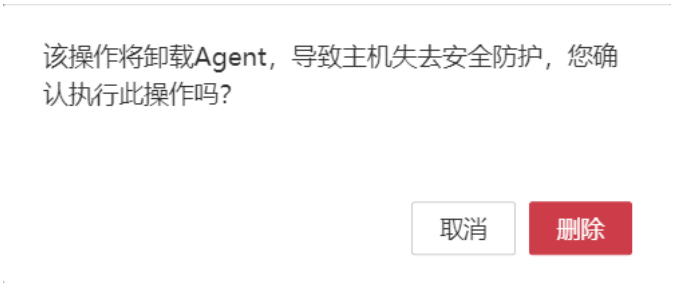
下载 Agent 运行情况的报告。

5）重启 Agent

重新启动 Agent，不改变原"主机状态"和"运行级别"。

3.6 卸载 Agent

登陆云平台，进入控制中心-“服务器安全卫士”界面，点击订单中的“控制台”，进入服务器安全卫士控制台，选择通用功能-服务工具-Agent 管理，进入 Agent 管理界面，点击“删除 Agent”，即可彻底清除产品中该 Agent 所有数据信息，显示为"清除数据中"，清除完成后触发统计更新；并下发"Agent 卸载"命令，释放"AgentID"。



4 操作指南

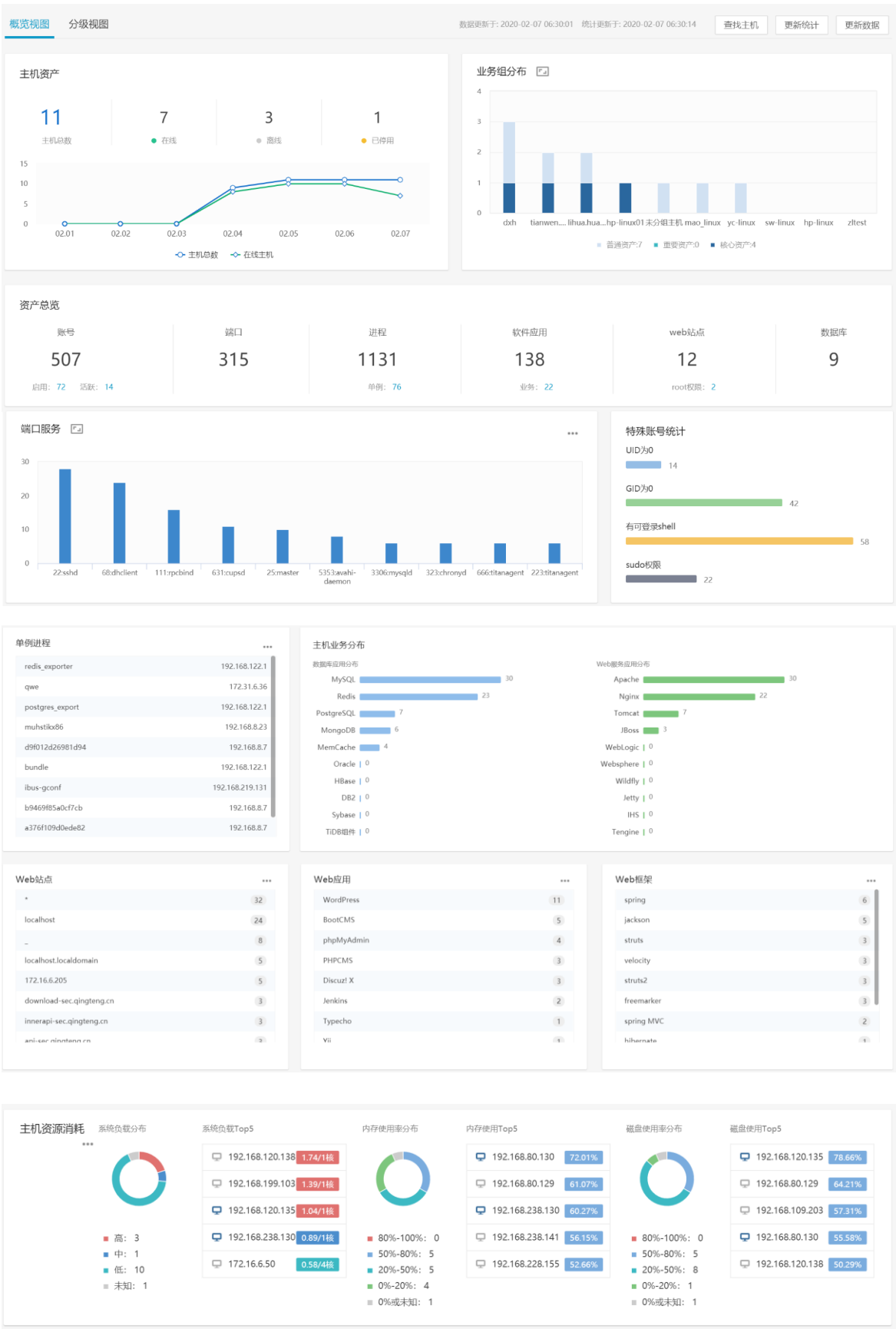
4.1 资产清点

资产清点（Asset Inventory），致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产精准识别和动态感知，让保护对象清晰可见。使用 Agent-Server 架构，提供 10 余类主机关键资产清点，800 余类业务应用自动识别，并拥有良好的扩展能力。

资产清点功能，有两种查询视图：概览视图、分级视图。

4.1.1 概览视图

概览视图作为“资产清点”功能的首页，主要实现对资产信息的可视化，帮助用户更直观地了解资产总体情况，更有效得出对资产的理解或判断。


概览视图
分级视图
查找主机
更新统计
更新数据
主机资产
11
7
3
1
业务组分布
资产总览
账号
507
端口
315
进程
1131
软件应用
138
web站点
12
数据库
9
端口服务
特殊账号统计
UID为0
GID为0
有可登录shell
sudo权限
单例进程
主机业务分布
Web站点
Web应用
Web框架
主机资源消耗
系统负载分布
系统负载Top5
内存使用率分布
内存使用Top5
磁盘使用率分布
磁盘使用Top5

概览视图内容，包含如下几部分：

1. 主机统计：展示被托管主机的相关情况，包括：Agent 运行状态、安装进展变化、及相关管理属性；

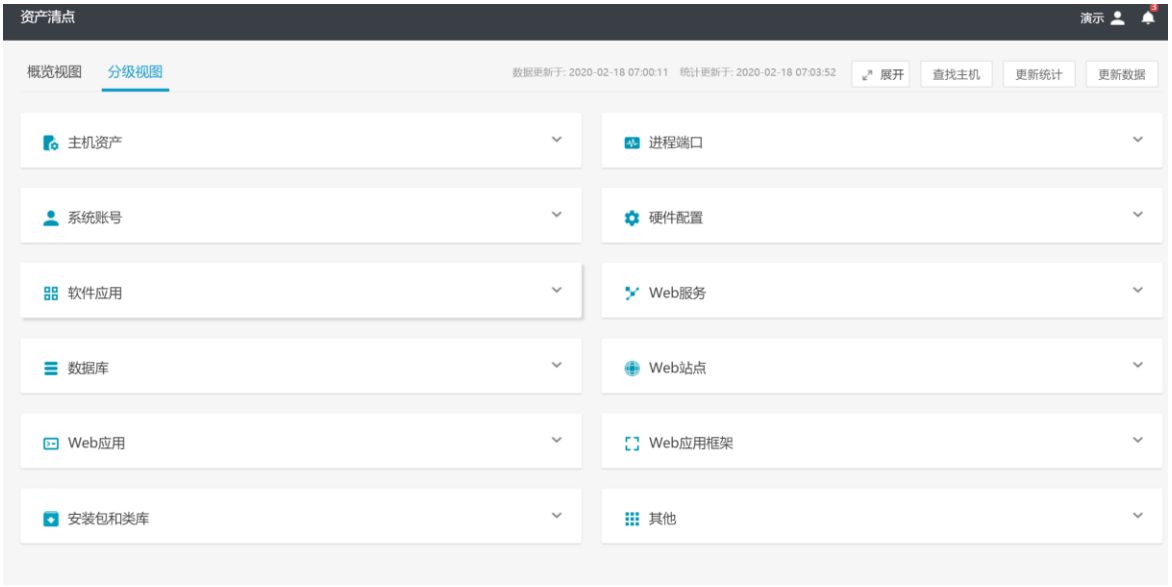
2. 核心资产统计：总览主机中的几大重要资产（账号、端口、进程、软件应用、Web 站点、数据库），体现为资产的总量统计、及特殊关注数量；

3. 资产分布情况：展示上述具体资产的分布及统计情况，包括：基础资产、业务相关应用、Web 资产等：

4. 资源消耗情况：展示主机资源消耗情况，包括：系统负载、内存使用、磁盘使用。

4.1.2 分级视图

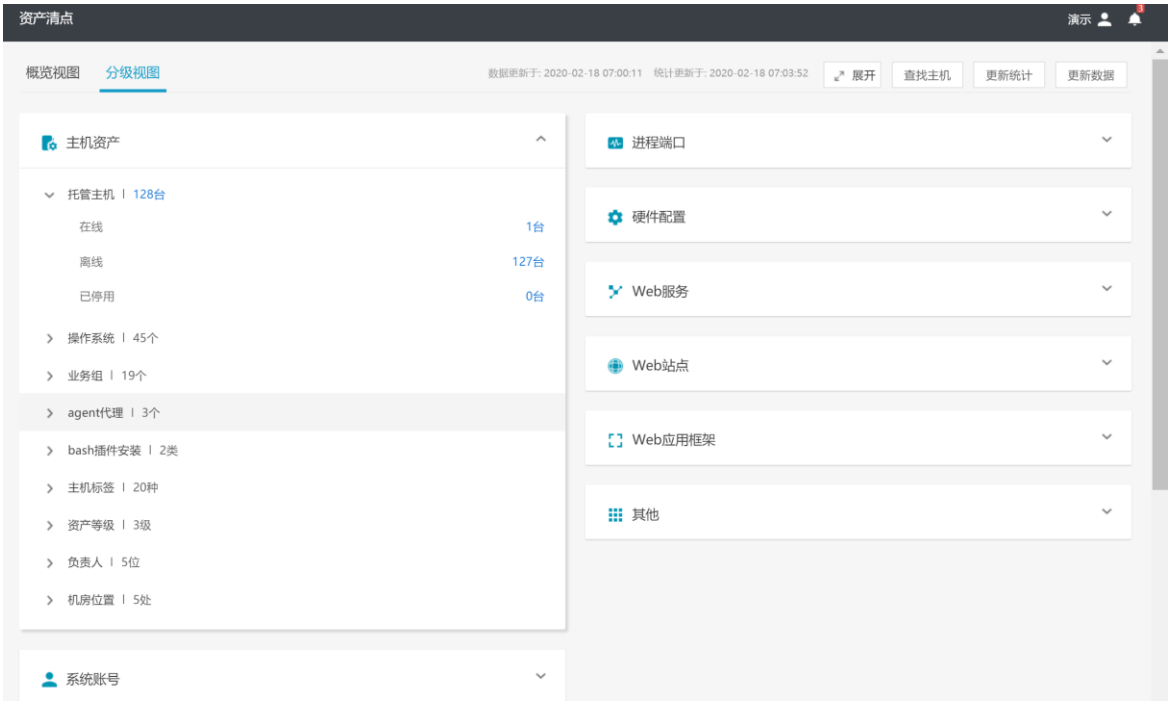
分级视图，是一种系统化的资产查询视图，通过系统化地分类，展示资产的统计情况，帮助用户快速了解资产总体信息；同时，作为分级视图详情的入口，以结构化的方式，有效地引导用户进行索引查询。



共有 12 个功能模块，分别为：

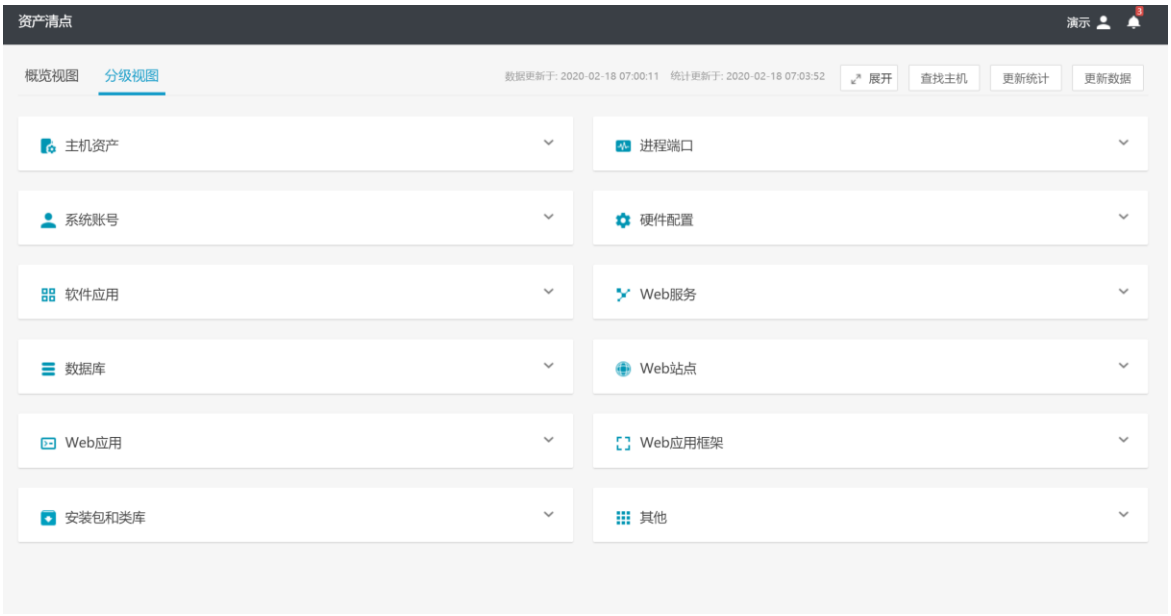
1. 主机资产：模块包含所有主机相关信息，包括基本信息、运维信息、代理信息、Bash 插件安装信息等；
2. 进程端口：模块包含主机中所有进程，及运行进程的端口相关信息；
3. 系统账号：模块包含主机中所有账号，及用户组相关信息；
4. 硬件配置：模块包含所有主机的硬件配置信息，及硬件消耗情况；
5. 软件应用：模块包含主机中所有软件应用相关信息；
6. Web 服务：模块包含主机中所有 Web 服务相关信息；
7. 数据库：模块包含主机中所有数据库相关信息；
8. Web 站点：模块包含主机中所有 Web 站点相关信息；
9. Web 应用：模块包含主机中所有 Web 应用相关信息；
10. Web 应用框架：模块包含主机中所有 Web 框架相关信息；
11. 安装包和类库：模块包含主机中安装包和 Jar 包相关信息；
12. 其它：模块包含了一些非核心的资产信息，包括：启动项、计划任务、环境变量、内核变量等；

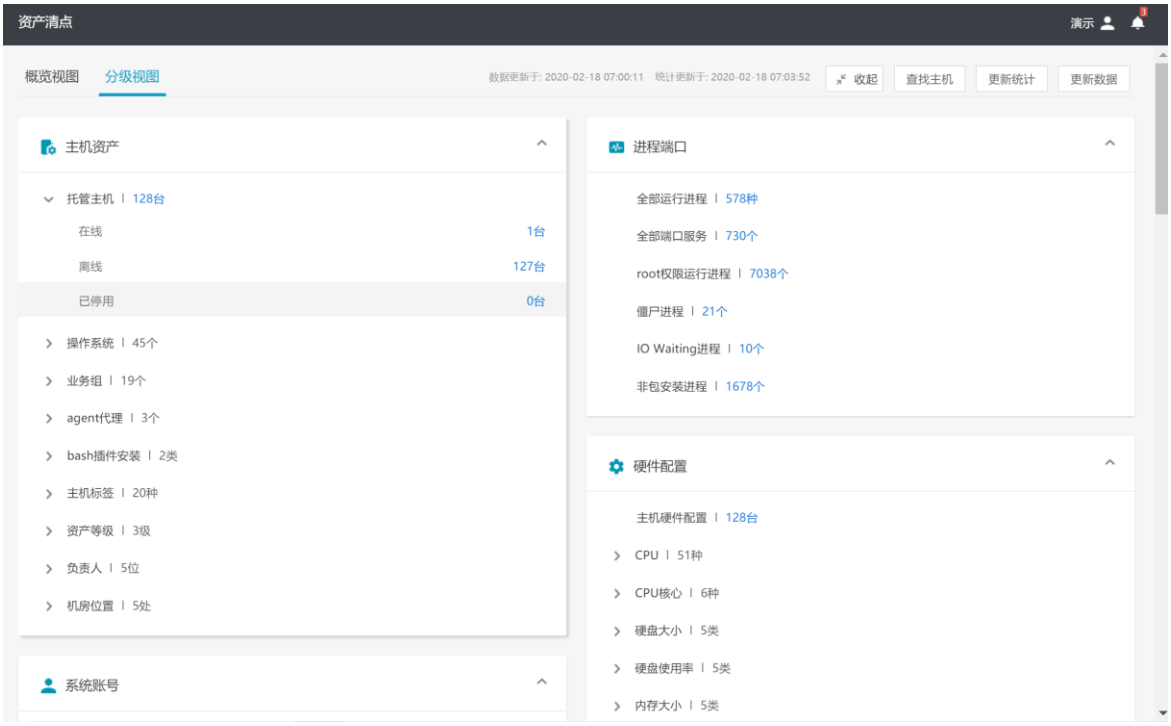
通过点击模块及折叠按钮 › ，可展开查看具体资产统计信息；



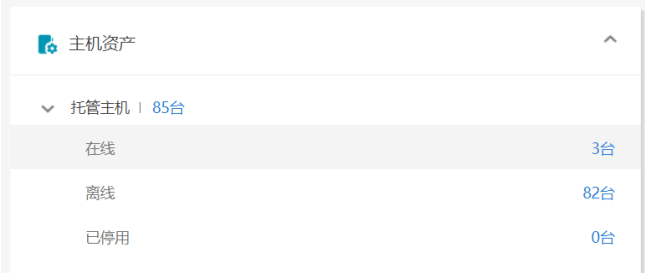
点击右上角的 展开 按钮，可以将全部模块的内容展开；

展开后，右上角按钮变为 收起，点击收起，可以将全部模块的内容收起。

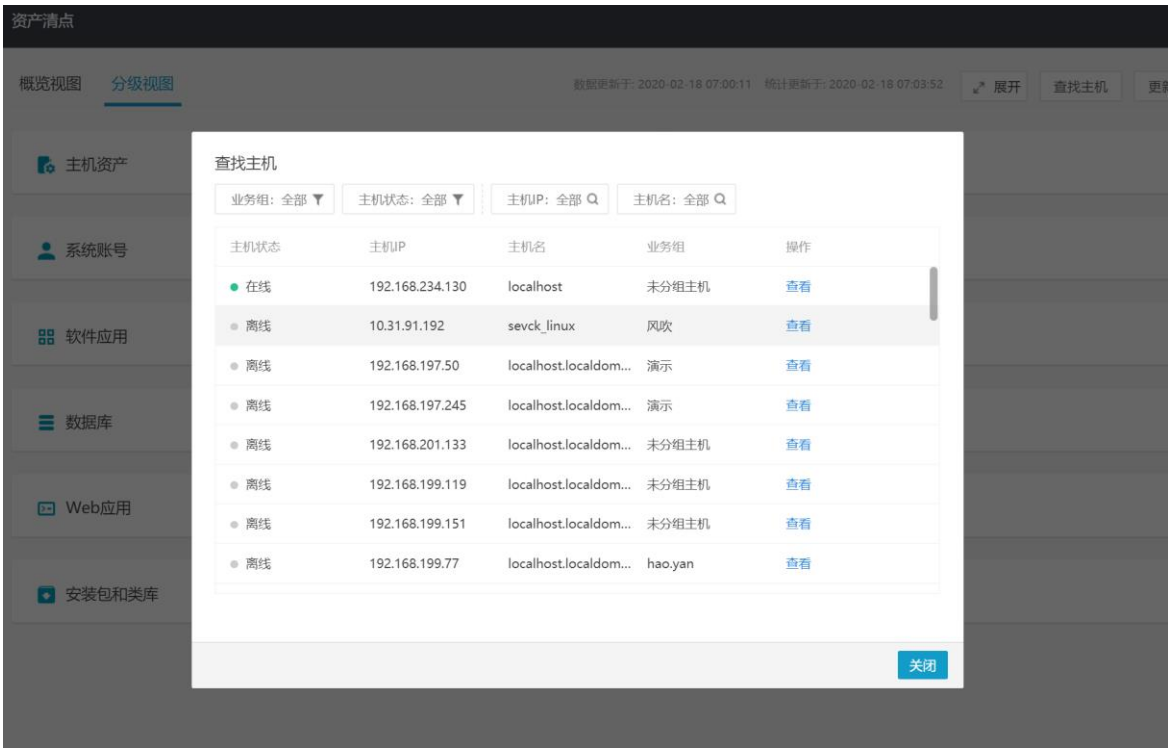




点击模块统计数值，即可跳转到对应的”资产详情页面”，查看所有主机中该资产的详细信息。

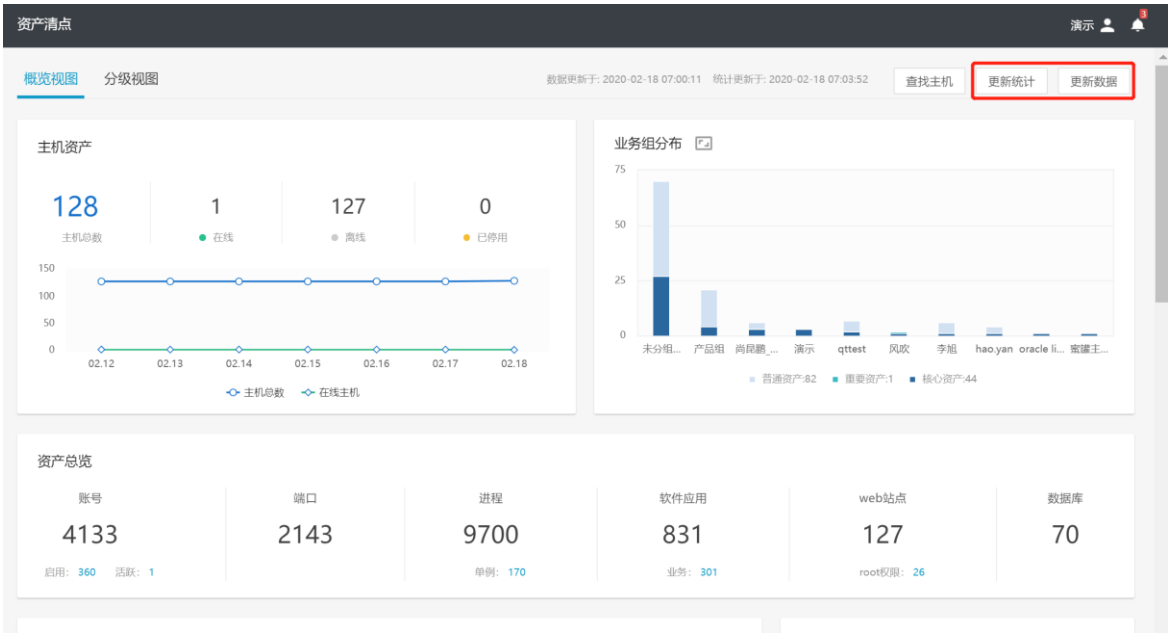


如想仅查看某个主机的资产情况，可以点击”查找主机” 查找主机 按钮，筛选出该主机后”查看”。

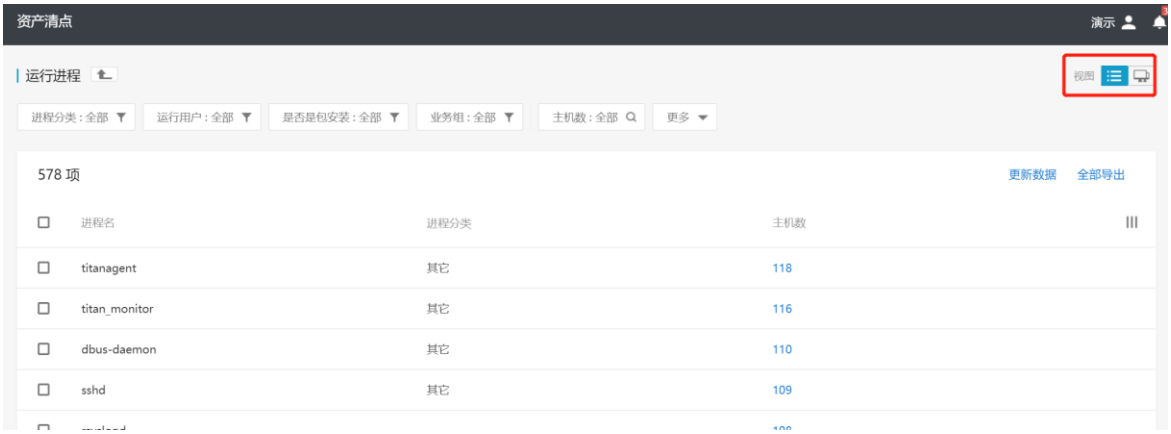


所有主机中的资产信息，每天自动更新一次，如果想获取最新信息，可以点击右上角的

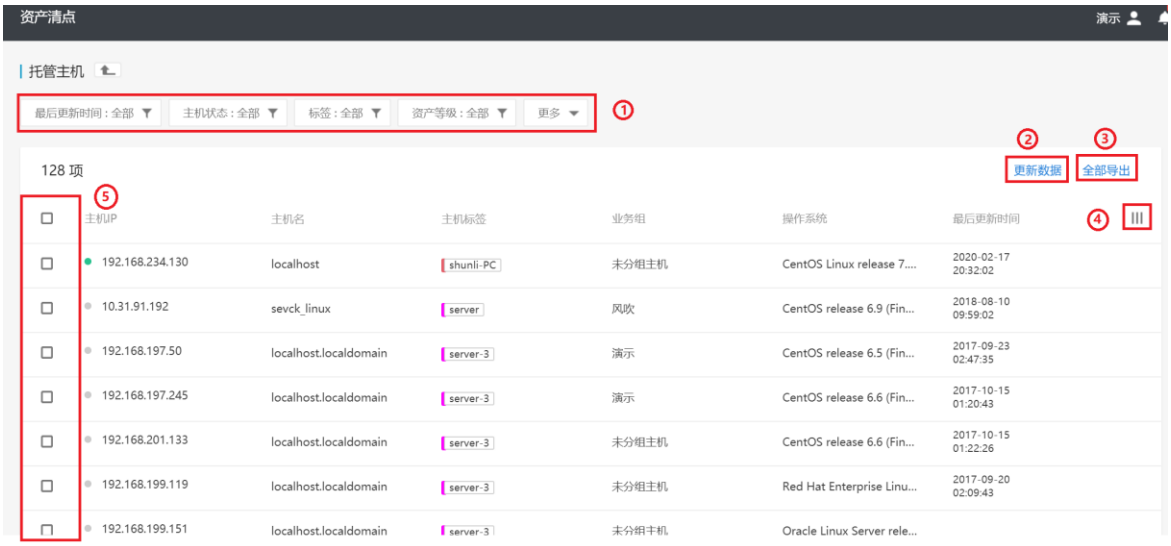
”更新数据”按钮，手动触发更新；对于功能中的统计数据，也可以手动触发”更新统计”。



在资产详细信息查询中，提供了两种视角（资产视角、主机视角），用户基于不同的统计查询需要，可相互切换。



同时在资产详情页面，用户可以对列表进行操作，得到想要的查询结果。



- 筛选/搜索区：根据不同需要，对列表内容进行筛选；
- 更新数据按钮：点击 更新数据 ，手动触发更新当前资产数据；
- 全部导出按钮：点击 全部导出 ，可导出列表中的全部资产数据；
- 设置显示列按钮：点击 ，通过勾选列名，控制列表中信息的显示/隐藏；
- 复选框按钮 □ ：点击复选框，可选中该行数据，进行“导出”等操作；

4.2 风险发现

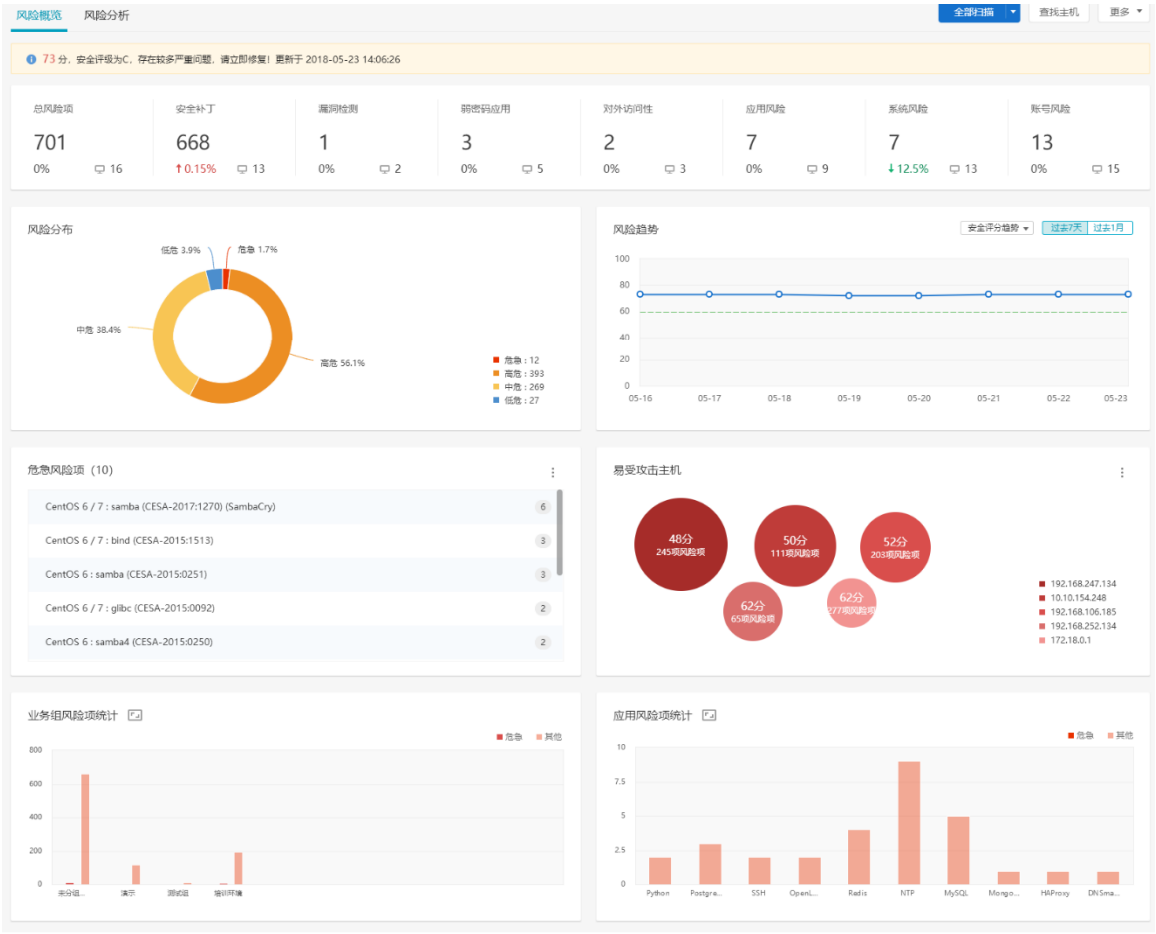
4.2.1 风险总览

- **【风险总览】Tab 页**

以图表形式从总体上预览系统风险项，直观感受到系统现存问题。每项都可以点击进入查看详情。主要由以下 7 个模块组成；

- 风险概况：按照系统总体风险情况进行评估打分。

- 风险趋势：反映过去一段时间风险评分的变化趋势。
- 风险类别统计：反映不同类别的风险项的统计情况。
- 应用的风险项统计：反映不同“应用”的风险项的统计情况，这里的“应用”为泛指，可能是软件应用，如 Redis，MySQL 等等；软件包或依赖库的名称，如 glibc，OpenSSL；补丁名称与系统相关的对象，如 kernel，Linux，bash 等等。
- 易受攻击主机列表：查看最易遭受攻击的主机
- 危急风险项：展示风险最大，最应该被修复的风险项。最应该被修复的衡量标准为危险程度最高（危急），且影响的主机的资产等级高。
- 业务组的风险项统计：反映不同业务组的主机的风险项统计情况。



- **【风险分析】Tab 页**

以概览报表的形式，从总体上统计各类型风险项，每项都可以点击进入查看详情，详情会跟进事件特征进行自动筛选。主要由以下 6 个模块组成：

- 安全补丁：检测各典型类型补丁是否检出，并统计各类型补丁的数量及其影响主机数量。
- 弱密码应用：检测常见弱密码是否检出，并统计各类型弱密码的数量。
- 应用风险：检测常见应用是否存在配置风险，并统计各类型风险的数量及其影响主机数量。

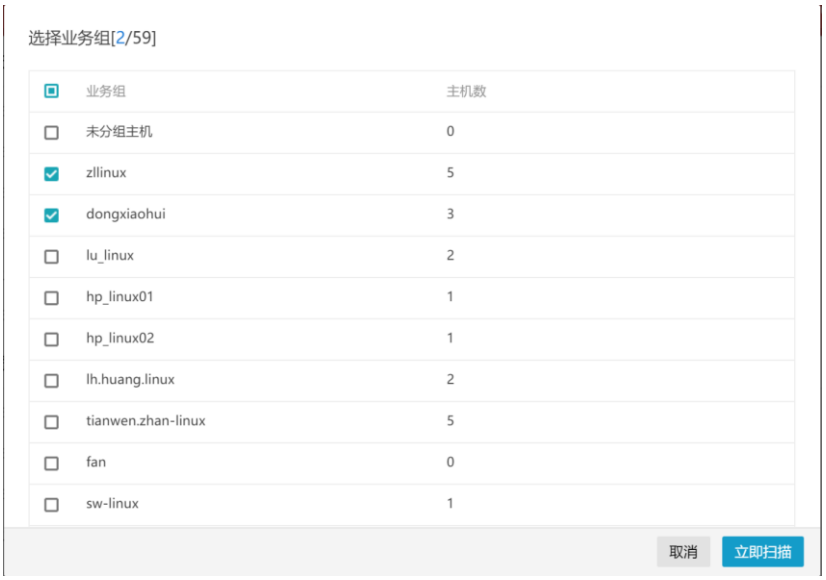
- 漏洞检测：检测各典型类型漏洞是否检出，并统计各类型漏洞的数量及其影响主机数量。
- 系统风险：检测是否存在常见系统配置风险，并统计各类型风险的数量及其影响主机数量。
- 账号风险：检测是否存在常见账号配置风险，并统计各类型风险的数量及其影响主机数量。

全部扫描

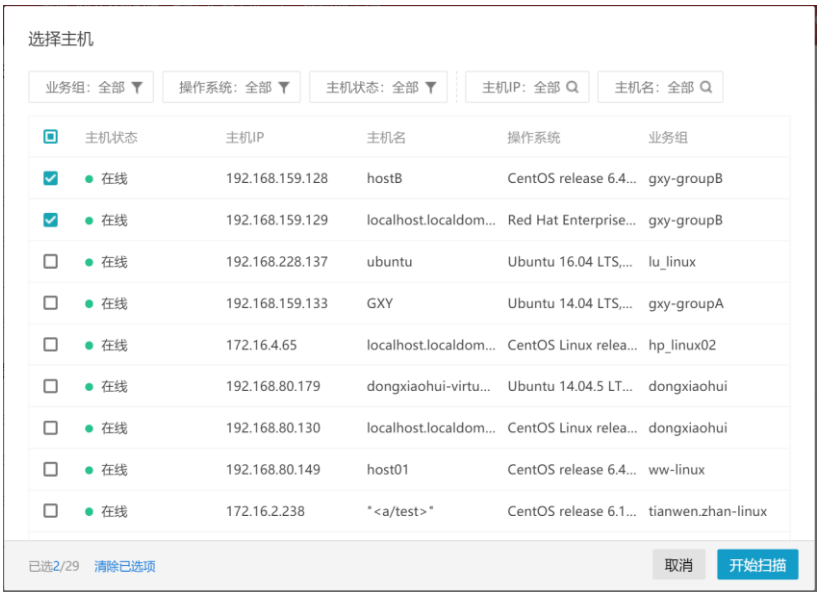
总览界面可对主机发起各类型风险的扫描。提供以下几类扫描方式：

1）点点击“全部扫描”按钮，可对全部主机进行全部风险的扫描；

2）点击“全部扫描”按钮旁的下拉按钮，选择“按业务组扫描”，可对选择的业务组进行全部风险的扫描；

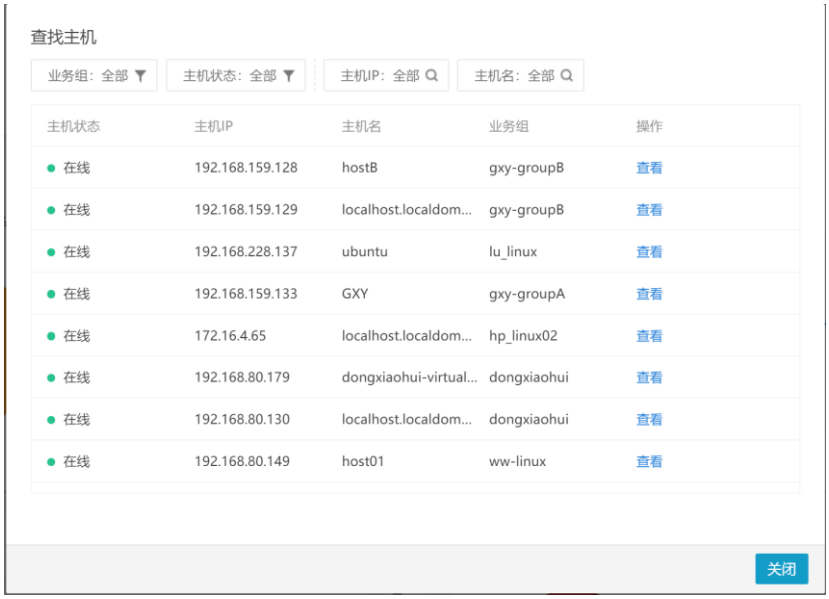


3）点击“全部扫描”按钮旁的下拉按钮，选择“按主机 IP 扫描”，可对选择的主机进行全部风险的扫描；



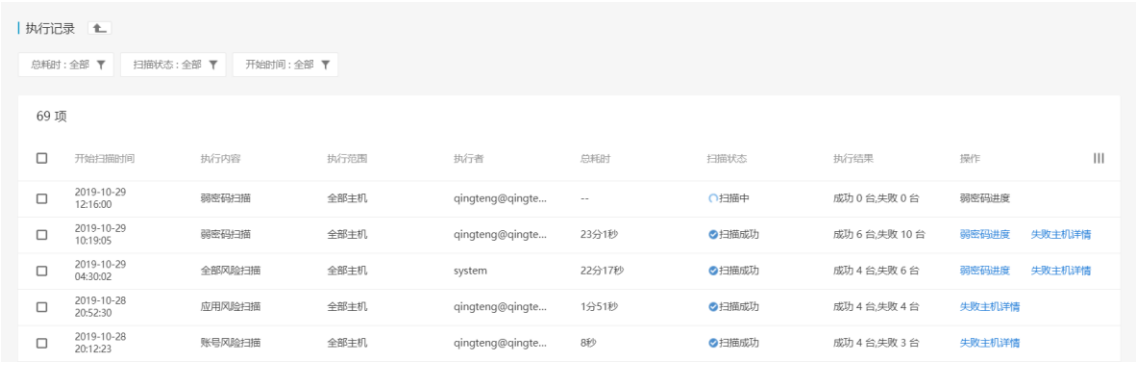
查找主机

总览中可快速查看当前存在风险主机的风险详情，点击“查看主机”，选择需要查看的主机，新开页面跳转至该主机的单台主机详情，并默认展示安全风险事件。

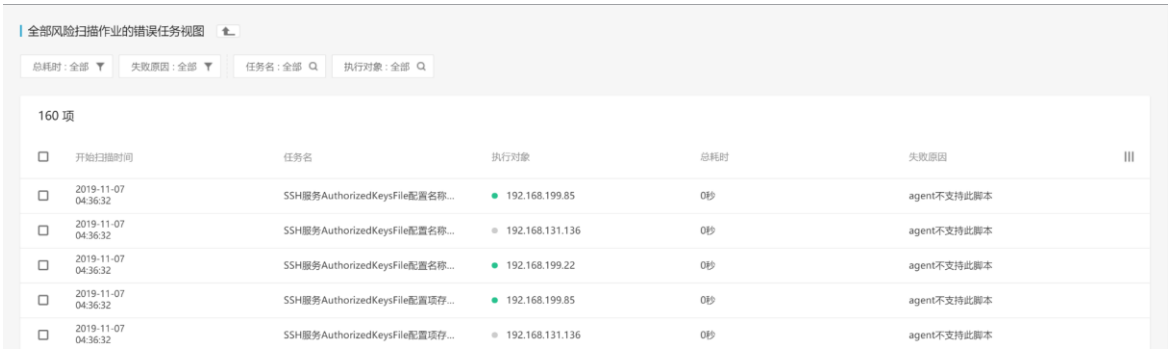


查看执行记录

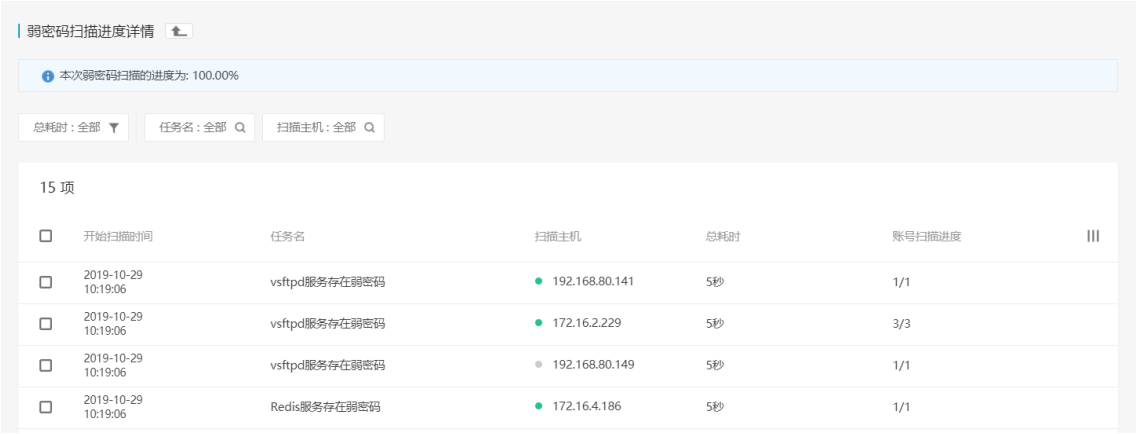
总览界面提供对执行的各类风险扫描查看其执行情况。点击总览界面中的“更多”按钮，选择“查看执行记录”，可查看执行记录列表。



每条记录支持对失败主机的详情进行查看，点击“失败主机详情”按钮可查看失败主机列表。

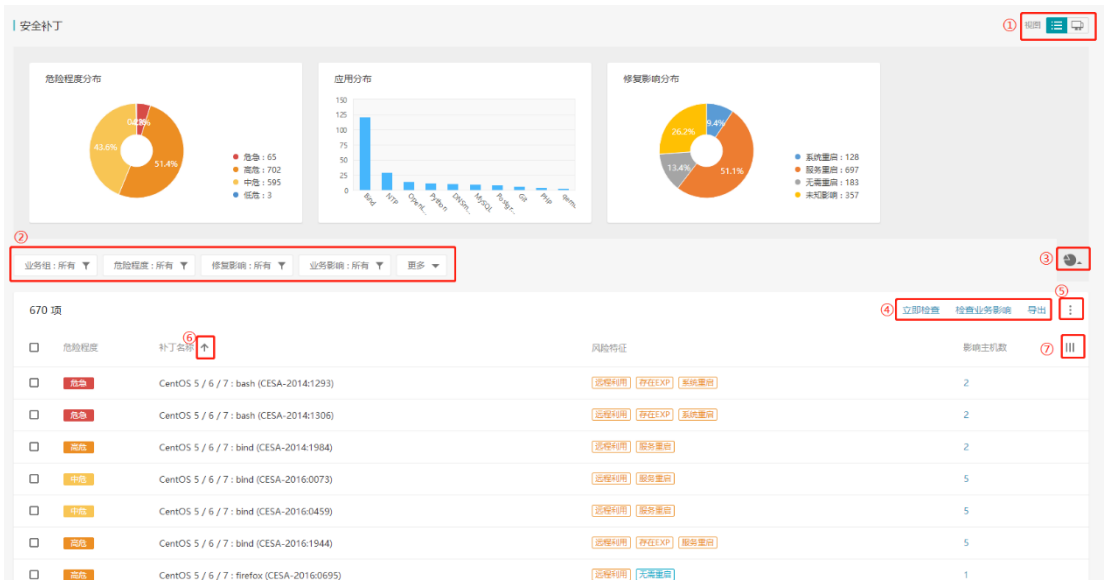


弱密码额外提供对进度的查看，点击执行内容为弱密码扫描记录中的“弱密码进度”按钮，可查看弱密码执行进度情况。



4.2.2 通用功能

以旗舰版为例，风险发现模块主要包含安全补丁、漏洞检测、弱密码、应用风险、系统风险和账号风险六大功能。下面以安全补丁界面为例，进行通用功能介绍，各功能详情，请登录服务器安全卫士控制台进行查看。



① 视图转按钮：包括资产视图、主机视图。点击 按钮，可切换至“主机视图”；

② 条件筛选框

③ 状态统计图按钮：点击 按钮，收起/展开统计图区域；

④ 检查/导出按钮 立即检查 导出 立即检查：对单独项目进行扫描；导出：导出单项检查结果

⑤ 更多设置按钮：点击 按钮，显示全部；

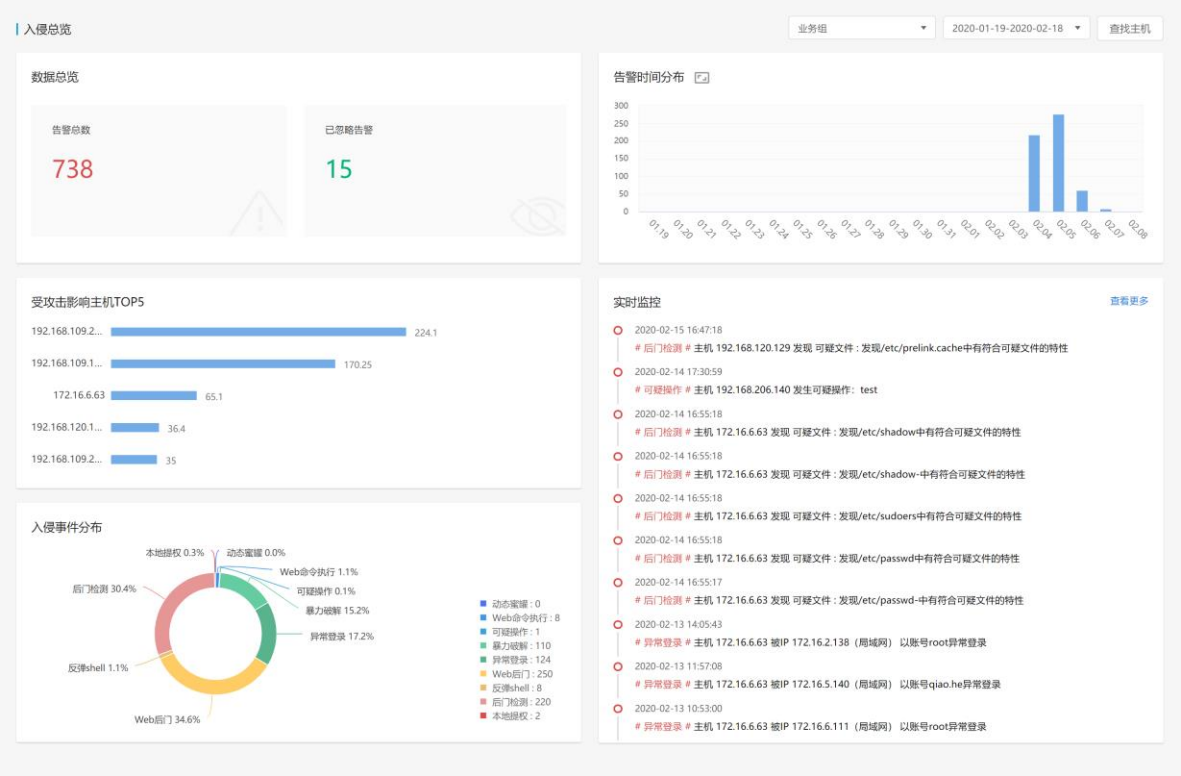
⑥ 排序按钮：鼠标移入列名，点击按钮对数据进行排序，点击↑按升序排列，↓按降序排列；

设置显示列按钮：点击 ，可设置显示列，控制列表中的数据显示/隐藏。

4.3 入侵检测

4.3.1 入侵总览

展示入侵检测功能总体的数据概览信息，支持各项操作来展示不同的统计视图信息。



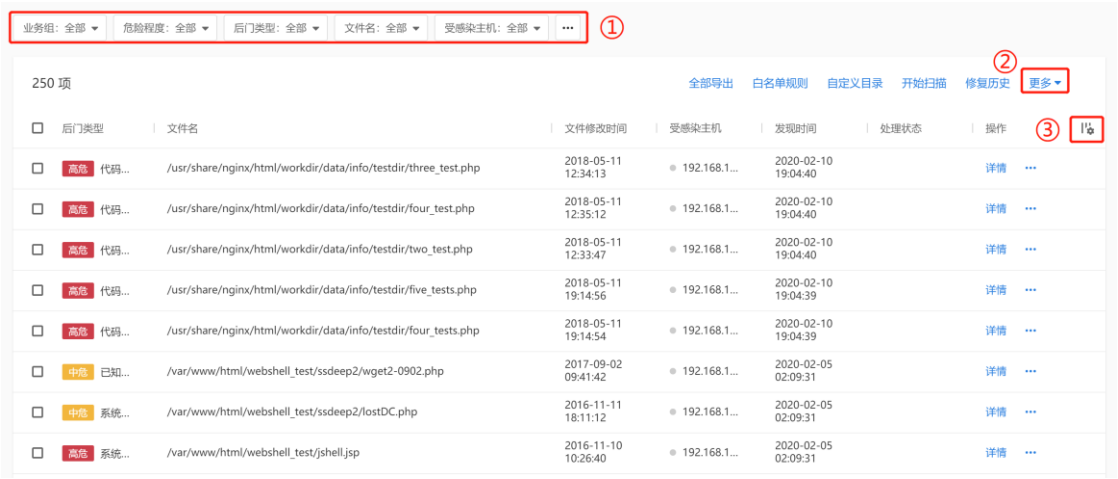
具体操作：

- 筛选：右上角提供两个维度的数据筛选，业务组和时间区间；
    - 业务组：可勾选 Linux 下的业务组，根据选择的业务组信息筛选统计信息重新生成各视图；
    - 时间区间：提供三个时间区间进行选择：24 小时、7 天和 30 天，选择后根据选择的时间区间筛选统计信息重新生成各视图；
- 入侵事件分布模块：可点选图例开启/关闭功能在环形图中是否显示；
- 实时监控模块：点击“查看更多”按钮，跳转至消息中心，默认选择入侵检测 tab，可查看所有入侵的通知消息事件；
- 查找主机：点击右上角“查找主机”按钮，弹出窗口展示当前全部主机的信息，点击各主机的“查看”按钮将新开 Web 选项卡并进入该主机的单台主机详情页中。

4.3.2 通用功能

以旗舰版为例，入侵检测模块主要包含暴力破解、异常登录、反弹 shell、本地提权、后门检测、Web 后门、可疑操作、Web 命令执行八大功能。下面以 Web 后门页面为例，介绍通用功能，各功能详情，请登录服务器安全卫士控制台进行查看。

通用功能



- 条件筛选框

- 更多设置按钮：点击“更多”按钮，显示全部；
- 设置显示列按钮：点击，可设置显示列，控制列表中的数据显示/隐藏；

4.4 合规基线

合规基线首页主要展示用户创建的所有基线检查作业检查结果，并提供新建检查、凭证管理、白名单的入口。

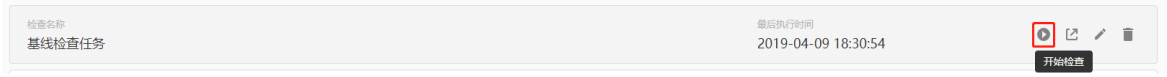
合规基线的首页是用户创建的合规基线任务列表，每个任务展示了基线检查的名称，最后执行时间等信息。可以通过基线规则和基线规则支持的平台等条件进行查询和筛选。也可以对检查任务进行执行、导出报表、编辑、删除等操作。

➢ 查看基线检查

点击某个基线任务，可查看该任务中的基线检查列表。也可对单个基线进行检查。

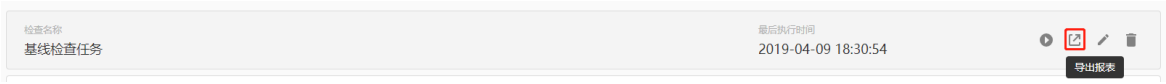
➢ 执行任务

在检查首页页面，选择某一个检查任务，点击后边的“开始检查”按钮后，开始执行该检查任务。



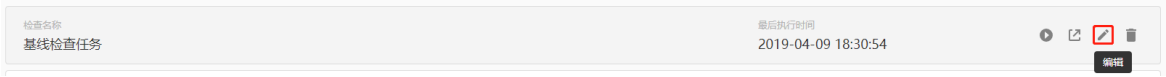
➢ 导出检查结果

点击任务项后边的“导出报表”按钮，可以导出选定的检查任务的检查结果。



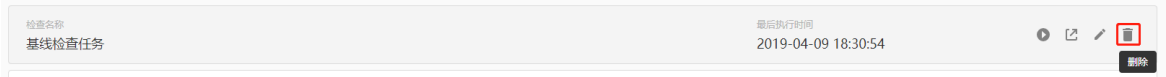
- 编辑任务

点击任务项后边的“编辑”按钮，跳转到编辑页面，可以编辑任务的名称和基线规则。



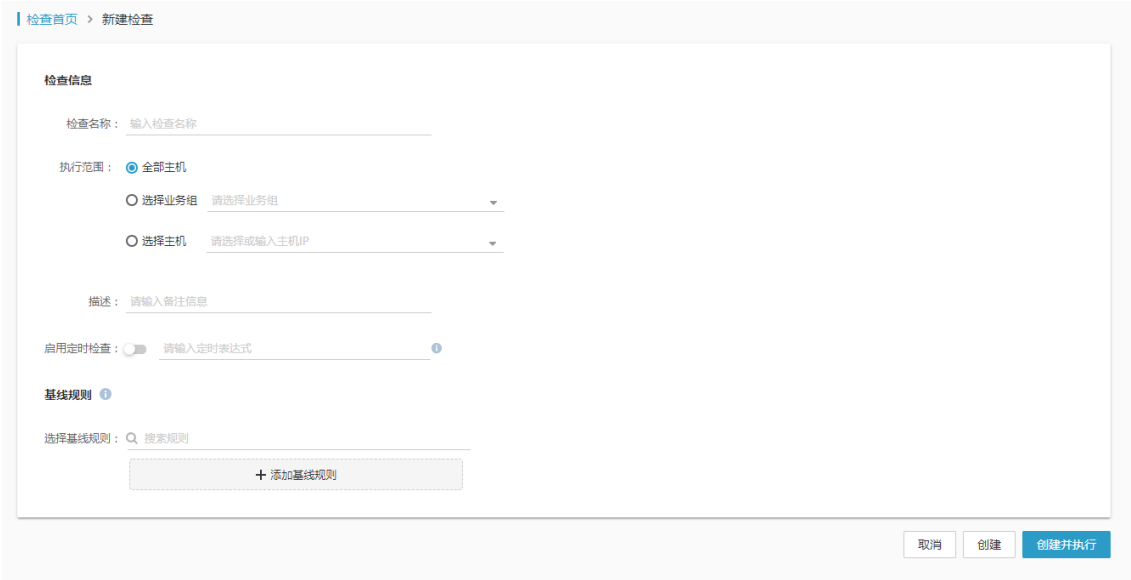
- 删除任务

点击任务项后边的“删除”按钮，可以删除选定的检查任务。

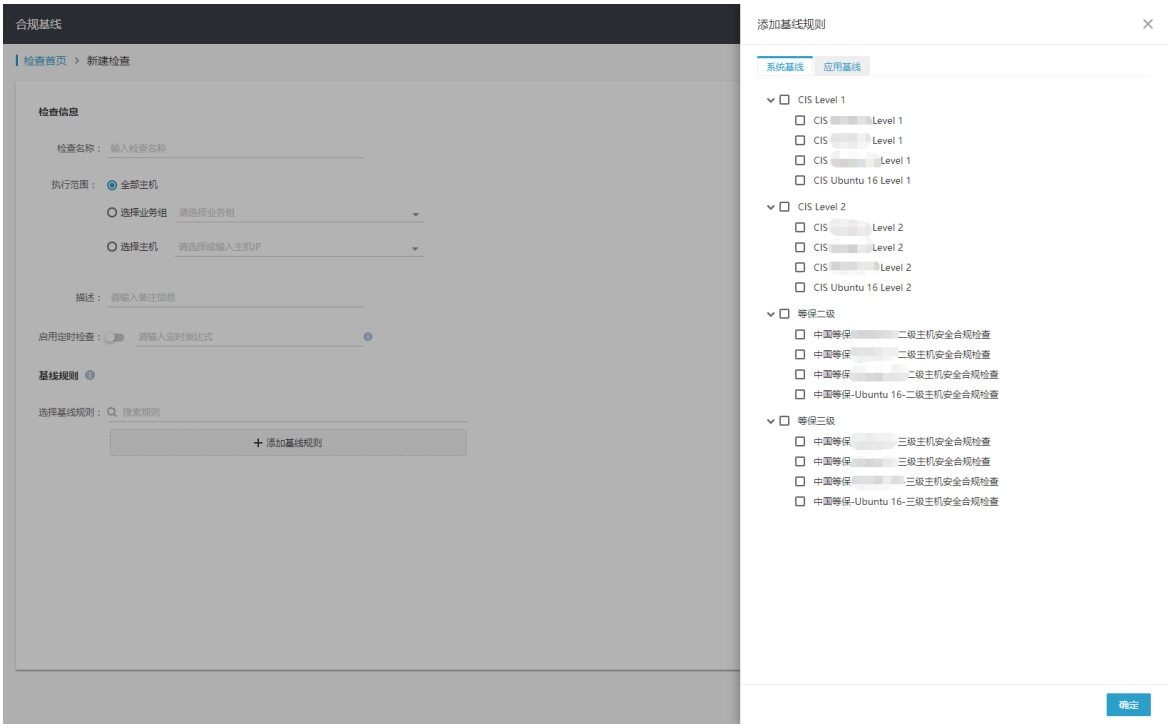


4.4.1 新建检查

单击“新建检查”按钮，进入新建检查页面。



- 添加主机规则



新建检查功能说明

功能	说明
检查名称	输入基线的检查名称
执行范围	全部主机：主账号可选全部主机，子账号不可选全部主机。（子账号不显示“全部主机”选项）选择业务组：可选择该账号管辖范围内的业务组。选择主机：选择该账号管辖范围内的主机 IP，也可手动输入主机 IP 【说明】需要先选择检查范围后，才能选择基线规则。选择了检查范围后，将根据所选主机匹配出适用的应用基线，有多少主机缺少账号授权，并提供设置入口。提示例如：您选择的主机中包含 20 台主机缺少

	账号授权，点击设置。
基线规则	系统将根据所选主机匹配出适用的基线规则。分为系统基线和应用基线两大类，每类下又细分为 CIS 和等保基线，基线可多选 【说明】基线选择后，若为数据库类型应用基线，则提示该规则中是否有需要添加账号授权的基线，若有，则提示，例如：该规则中的 60 个检查项需要账号授权 目前支持的系统基线有：centos6/7 rhel6/7 ubuntu12/14/16 支持的应用基线有：Apache Apache2 MySQL MongoDB Nginx
定时检查	打开定时检查开关，则可以输入定时表达式，且定时表达式为必填。定时表达式为 crontab 格式，点击“创建并执行”时，需要校验该格式是否正确，校验规则请参考“任务系统=》新建作业中 crontab 格式”。 鼠标移动到定时表达式后的 i，则显示定时表达式的输入说明。 关闭定时检查开关，则不可以输入定时表达式。
描述	输入对该基线的描述。

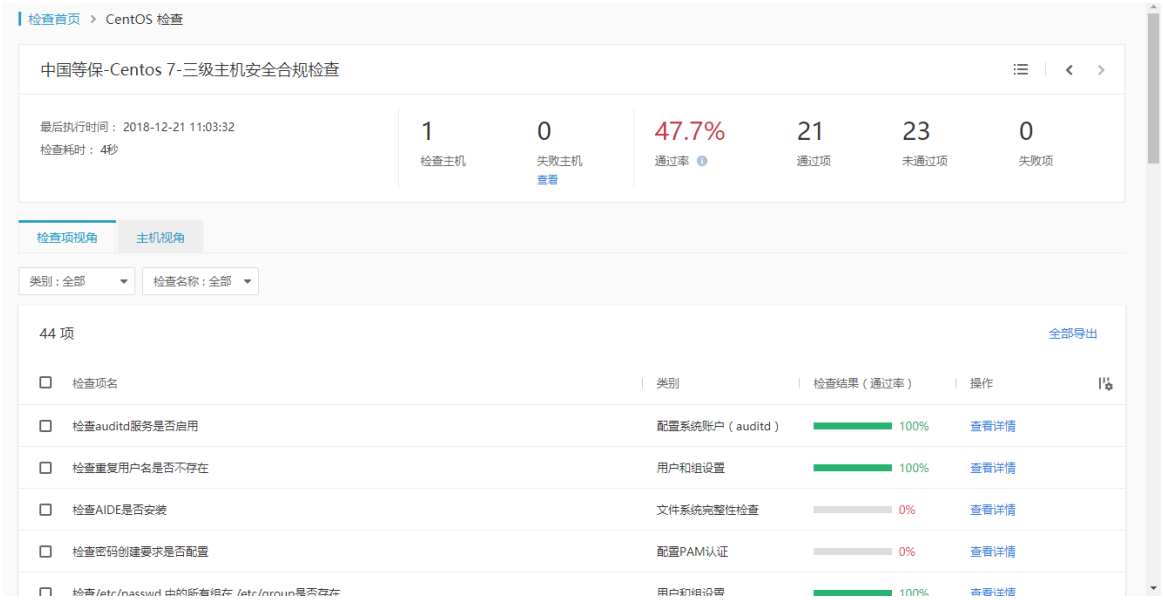
4.4.2 查看检查结果

点击某个任务中的某个基线检查，可以查看该基线检查最后一次的检查结果。

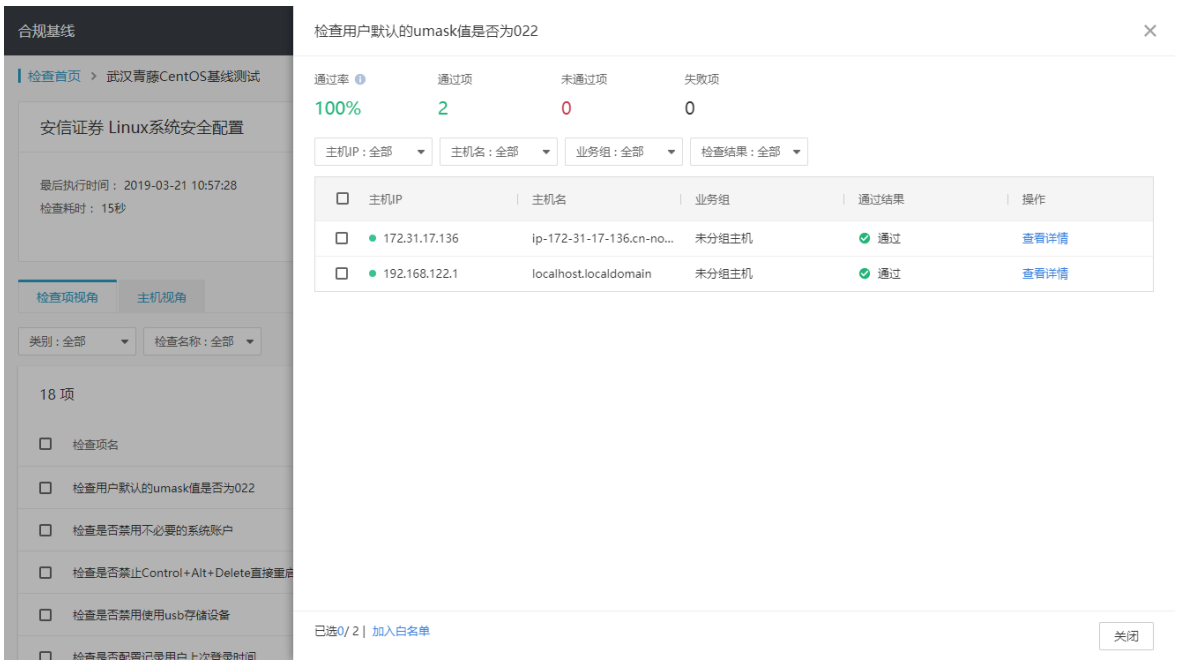
- 检查项视图

跳转后默认是【检查项视图】，检查项视图按照每个检查项的维度展示了该检查项的基本信息，和在主机范围内检查结果的统计，即通过率。

在页面上方，视图展示了该检查项所依赖的基线规则的概要信息，以及检查结果的统计。



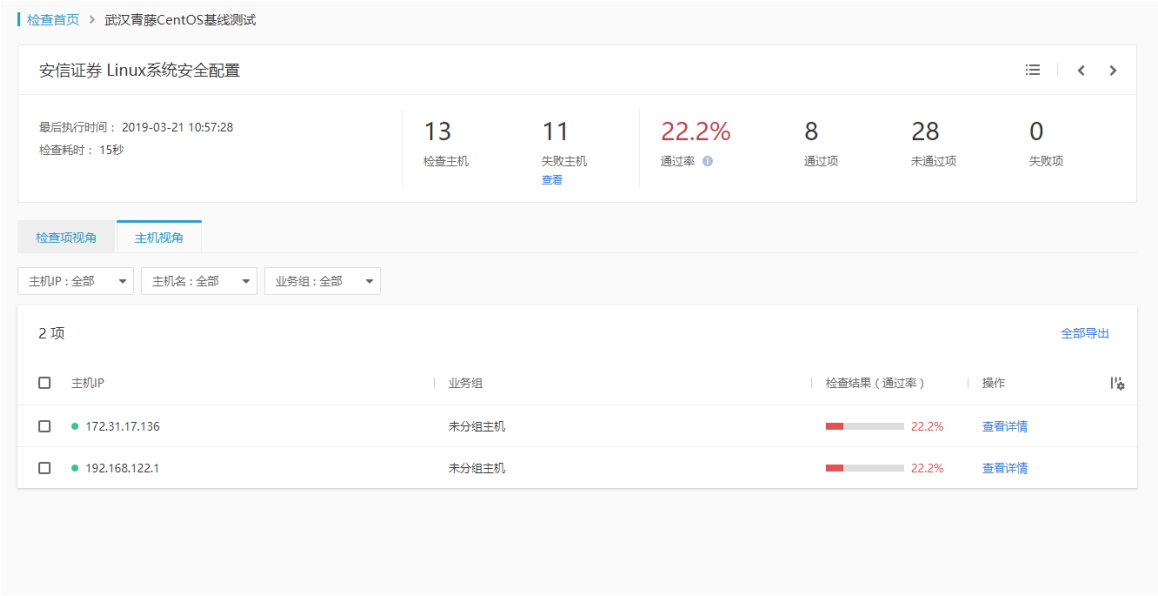
点击查看详情，可查看这个检查项在每台被检查主机上的检查结果。该结果可以通过主机IP、主机名、业务组和检查结果进行查询和筛选。



选择一台主机的结果并点击“查看详情”，可以看到该检查项在这台主机上的详细检查结果。其中包含了检查项名，检查内容，建议值和实际值等信息，帮助企业用户理解和合理设置。

- 主机视图

通过点击【检查项视图】的按钮，可以切换到【主机视图】。【主机视图】按照每台被检查主机的角度，展示了这台主机的基本信息，以及该基线检查所有检查项在该主机上的检查结果统计。可以通过业务组，主机 IP 和主机名进行筛选。



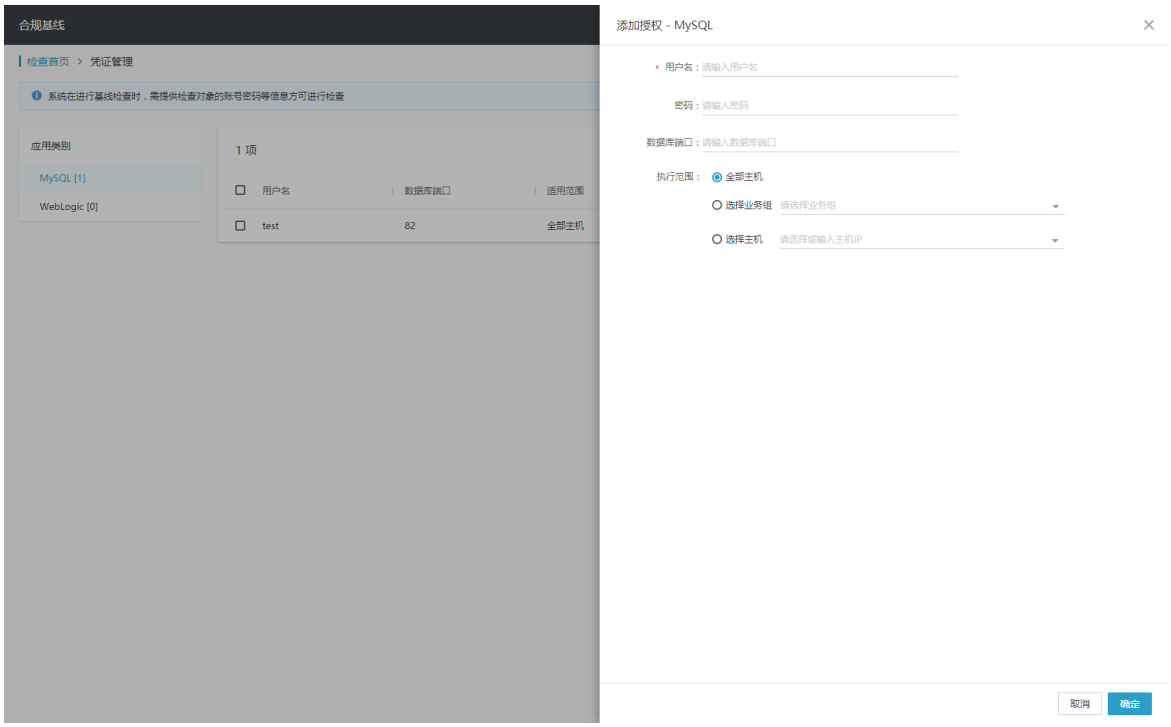
4.4.3 凭证管理

单击 更多 按钮，选择“凭证管理”，输入账号密码后进入“凭证管理”页面。

凭证管理管理的凭证用于对应的应用基线的检测。

- 添加授权

选择需要授权的应用类别，点击列表右上角的“添加授权”按钮，弹出该应用的添加授权弹窗。



➢ 编辑授权

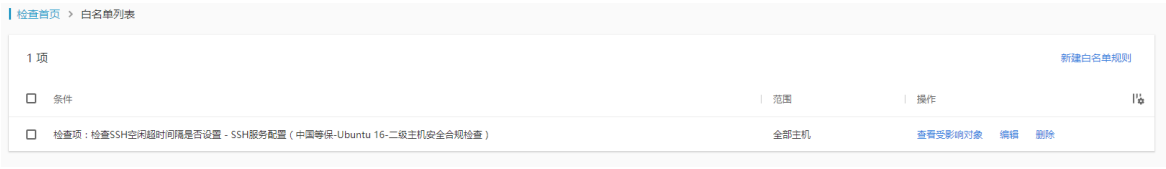
选择需要编辑的授权，点击“操作-编辑”按钮，弹出该应用的编辑授权弹窗。

➢ 删除授权

选择需要删除的授权，点击“操作-删除”按钮，可删除对应的授权。

4.4.4 查看白名单

单击 更多 按钮，选择“查看白名单”，进入“白名单列表”页面。



- 新建白名单规则

单击“新建规则”按钮，进入新建白名单规则页面

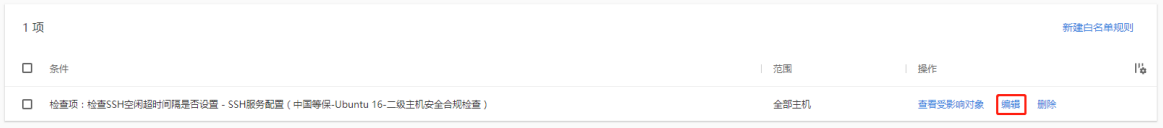
点击“精确搜索”，联动选择检查规则-检查类型-检查项。

- 查看受影响对象

查看现有规则影响的对象。

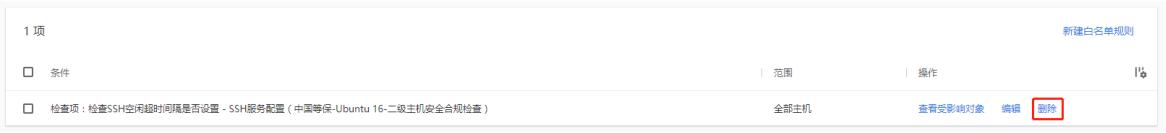
- 编辑白名单列表

对于已经保存的单条规则，用户可以选择对其进行修改。



➢ 删除白名单列表

对于已经保存的单条或者多条规则，用户可以选择对其进行删除。

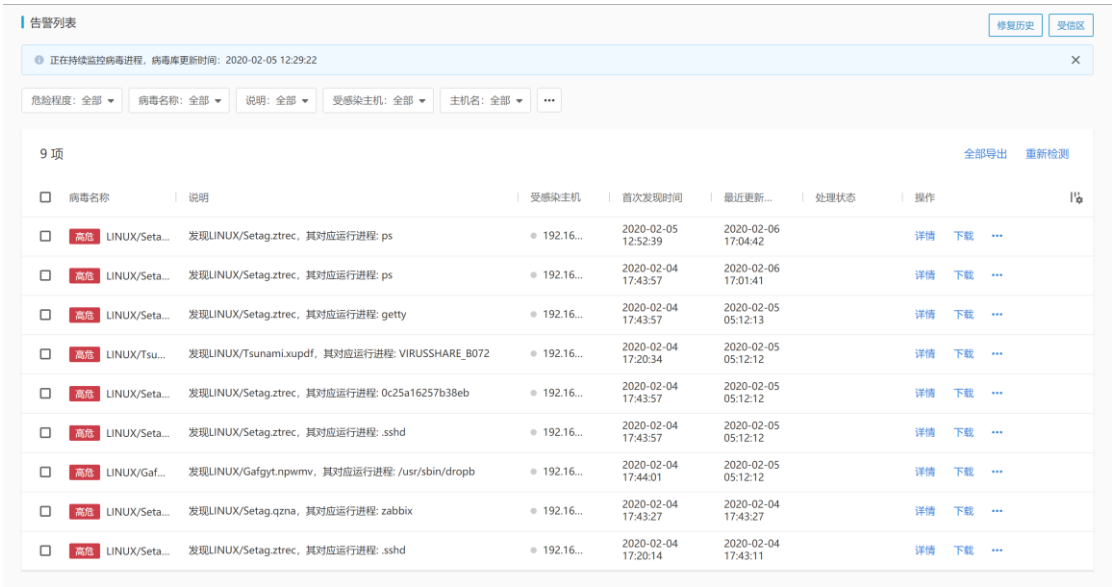


•

4.5 病毒查杀

病毒查杀为产品中新增的独立杀毒模块，满足等保要求，提供对病毒的检测和处理能力，并能够提供一定的主动防御能力。

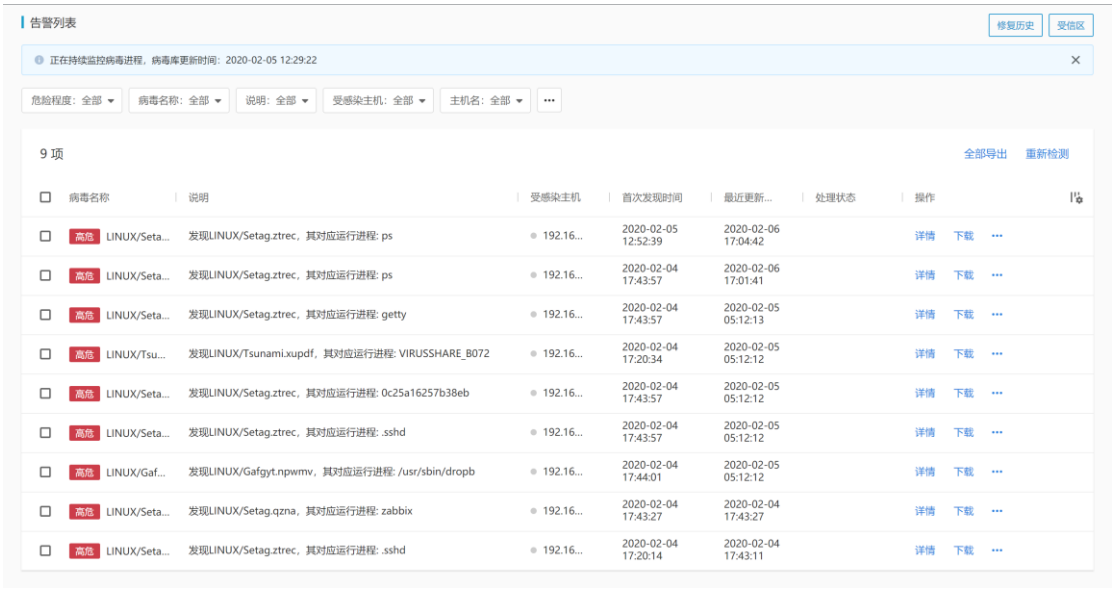
图1-1 病毒查杀-主界面



4.5.1 告警列表

提供对上报告警的病毒事件的查看、分析和处理能力。

图1-2 病毒查杀-告警列表



具体操作：

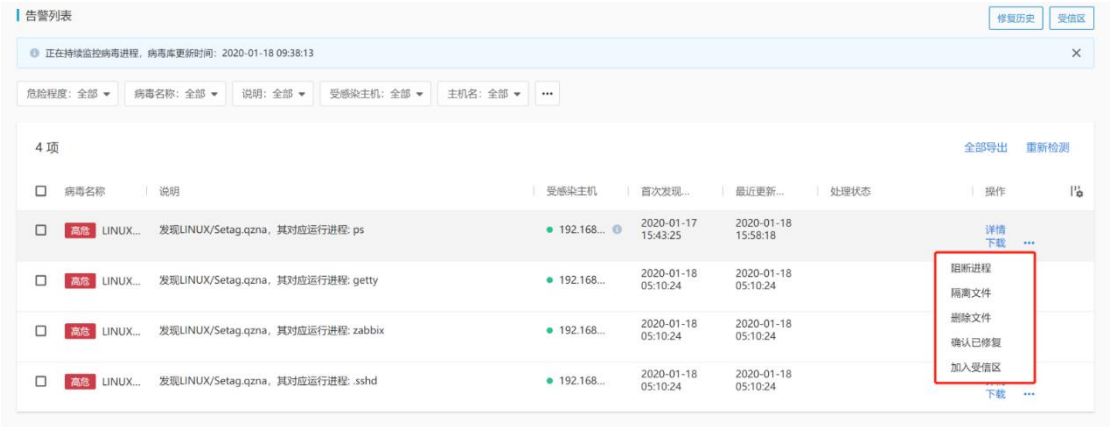
- 查看病毒详情：提供对病毒详细信息的查看，包含病毒引擎分析后的检测说明、病毒文件的静态信息以及病毒进程的进程相关信息；

图1-3 告警列表-病毒详情

- 下载病毒文件：提供对病毒的下载，用户可对想进一步分析的病毒进行下载，病毒文件已上传服务端，故主机上无论是否仍存在该病毒，都可以进行下载，下载的文件为病毒的真实文件，请注意在安全的环境下进行下载；
- 处理病毒：对病毒提供各项处理能力，处理操作皆支持批量，包含：

- 支持对病毒进行进程阻断、文件隔离和文件删除，其中隔离和删除成功后的病毒认为已修复，已修复事件将移出告警列表，可在告警列表的修复历史功能中进行查看；
- 确认为非病毒时可将该事件加入受信任区，加入受信任区后，相同的病毒在该主机上将不再进行告警，可在受信区中查看该事件记录；
- 修复后可将病毒事件标记为已修复，标记为已修复的事件同样将移出告警列表，可在告警列表的修复历史功能中进行查看，其操作人为当时手动操作的账号名。

图1-4 告警列表-处理病毒



- 重新检测病毒：点击重新检测，将对主机上运行的病毒进程进行全部扫描，并同时验证主机上已被修复的病毒事件。重新检测可选择主机的范围，可选择三种范围：全部主机、业务组和自定义主机；

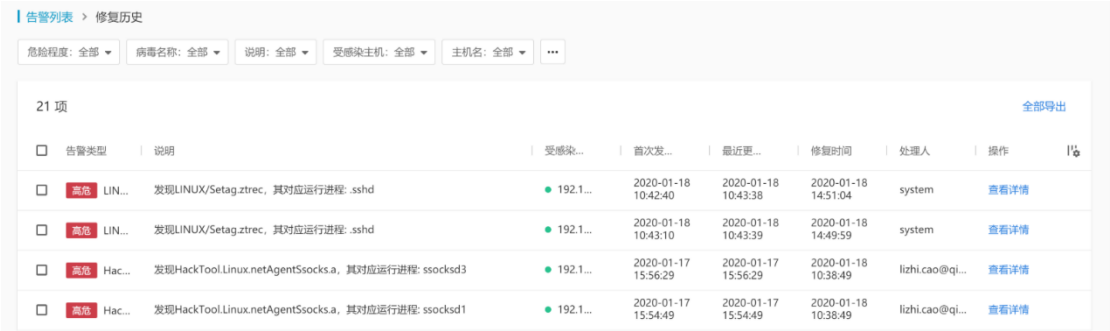
图1-5 告警列表-重新检测自定义范围

- 导出病毒信息：支持对病毒信息进行导出，点击界面的“全部导出”按钮和勾选记录后点击“导出”操作都可导出当前已选范围的数据；

4.5.1.1 修复历史

查看所有已被记录为修复的病毒事件，修复历史同样支持导出和查看详情。

图1-6 告警列表-修复历史



4.5.1.2 受信区

查看所有已被受信任的病毒事件，受信任的事件支持删除。

图1-7 告警列表-受信区

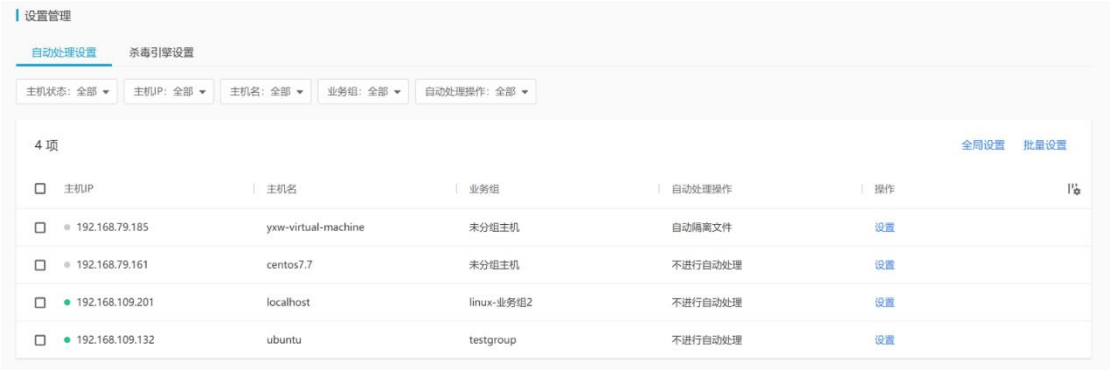
4.5.2 设置管理

可管理自动处理的设置和病毒引擎的设置。

4.5.2.1 自动处理设置

可设置全局的自动处理配置，也可针对某些主机进行特殊的设置，特殊设置后的主机配置结果将展示在列表中。

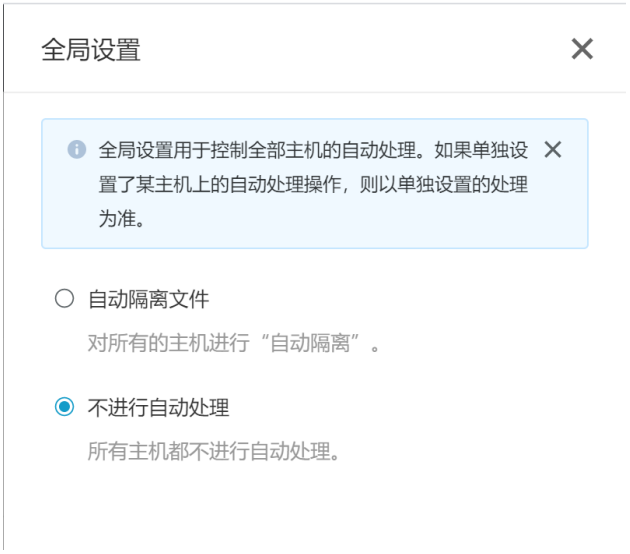
图1-8 设置管理-自动处理设置



具体操作：

- 全局设置：用于控制全部主机的自动处理，该配置为长期生效的状态，对全部主机持续生效，包含新安装的主机。如果单独设置了某主机上的自动处理操作，则以单独设置的处理为准。

图1-9 设置管理-全局设置



- 批量设置：用于批量下发主机上的特殊设置，该配置下发为一次生效的机制，设置的对象为下发时刻的主机范围，不持续生效。设置后的结果会展示在列表中，支持对全部主机、业务组和主机三种类型的范围进行下发。

图1-10 设置管理-批量设置

- 设置：用于修改主机上的特殊设置。

图1-11 设置管理-设置

4.5.2.2 杀毒引擎设置

可设置各病毒引擎的开关状态，方便用户管理杀毒引擎。目前支持小红伞病毒引擎、ClamAV 病毒引擎、T-Sec-反病毒引擎和青藤自研病毒引擎。。

图1-12 设置管理-杀毒引擎设置

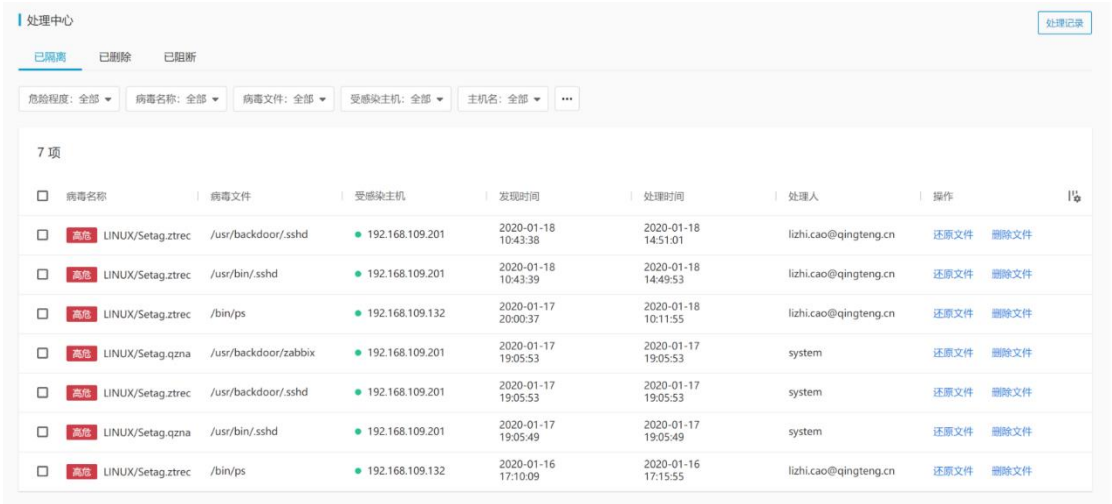
4.5.3 处理中心

可查看和管理已经处理成功的病毒文件，并支持查看每一次对病毒文件的处理操作记录。

4.5.3.1 已隔离

- 查看已隔离成功的病毒文件，可对隔离的文件进行还原和彻底删除；

图1-13 处理中心-已隔离



4.5.3.2 已删除

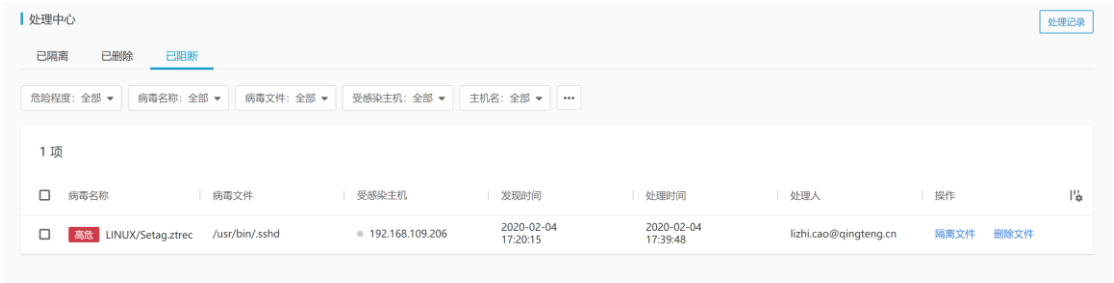
查看已删除成功的病毒文件，被删除的文件不可还原；

图1-14 处理中心-已删除

4.5.3.3 已阻断

查看已阻断成功的病毒文件，阻断后的文件还可以进一步隔离或删除；

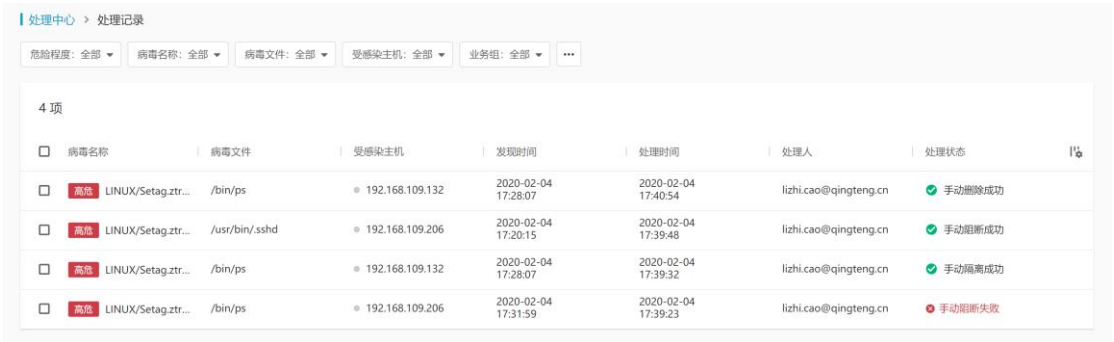
图1-15 处理中心-已阻断



4.5.3.4 处理记录

可查看所有的处理操作记录，方便用户追溯和确认处理的操作是否正常或者合规。

图1-16 处理中心-处理记录



4.6 通用功能

4.6.1 Agent 安装

Agent 安装提供详细的安装 Agent 方法指引：

- 支持操作系统：目前支持 Linux、Windows 和 Unix。
- 支持直连和代理方式连接。
- 安装引导：指导用户选择合适的安装方式，完成安装过程，并对可能遇到的问题给出解决方法。Linux 目前支持命令安装；Windows 支持命令安装、安装包安装、安装包+命令安装；Unix 系统支持命令安装。

4.6.1.1 Linux

- **步骤 1：选择操作系统**

选择 Linux 操作系统时，环境需求如下图所示：

➢ 支持主流 64 位 Linux 版本

1) Oracle：5、6、7
2) RHEL：5、6、7
3) CentOS：5、6、7、8
4) Ubuntu：10-19
5) SUSE：9-15
6) Debian：6、7、8、9、10
7) OpenSUSE：10-15
8) NeoKylin（中标麒麟）：6、7
9) YHKylin（银河麒麟）：4
10) Redflag（红旗）：9
11) Deepin（深之度）：15
12) iSoft（普华）：4

- 系统安装 Curl 程序，且版本不低于 7.10；（Curl 为下载器）
- 系统启动 Cron 定时任务服务
- openssl 版本不低于 0.9.8o
- 直连主机的防火墙需确保可与青藤服务器通信通信要求
- 代理连接的主机需连通管理服务器的 sock5 代理服务

当系统不允许使用 Crontab 任务时，系统常见问题中给出了解决方法，见下图所示：

- **步骤 2：设置主机信息**
- 通信协议：支持 IPv4 和 IPv6
- 连接方式：支持直连和代理连接
- 主机所属业务组：可以选择安装 Agent 主机所属的业务组。可点击快捷链接主机管理，跳转到业务组界面进行业务组管理。

- 代理连接的主机必须确保与服务器安全卫士可通信。
- 代理地址填写时，可输入“域名:端口”或“IPv4 代理 IP:端口”。示例：

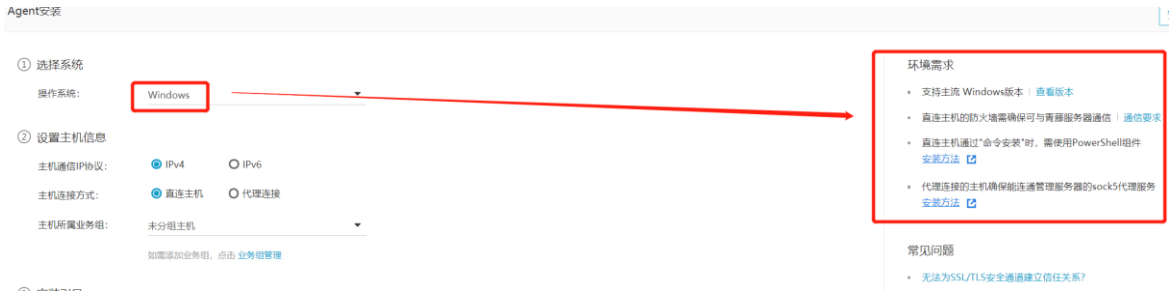
- **步骤 3：安装引导**

Linux 系统仅支持命令安装，见下图所示。步骤 1 和步骤 2 完成后，点击“生成命令”，将命令输入到 cmd 中以管理员身份运行。

4.6.1.2 Windows

- **步骤 1：选择操作系统**

操作系统选择 Windows 时，环境需求见下图所示：



- 支持 64 位 Windows 操作系统，主流版本包括：
  1) Windows Server 2008
  2) Windows Server 2012
  3) Windows Server 2016
  4) Windows Server 2019
  5) Windows Vista
  6) Windows 7
  7) Windows 8
  8) Windows 10
- 直连主机的防火墙需确保可与青藤服务器通信通信要求
- 直连主机通过"命令安装"时，需使用 PowerShell 组件
- 代理连接的主机确保能连通管理服务器的 sock5 代理服务

当无法为 SSL/TLS 安全通道建立信任关系时，系统常见问题时给出了解决方法，见下图所示。

- **步骤 2：设置主机信息**
- 通信协议：支持 IPv4 和 IPv6

- 连接方式：支持直连和代理连接
- 主机所属业务组：可以选择安装 Agent 主机所属的业务组。可点击快捷链接 业务组管理 ，跳转到业务组界面进行业务组管理。

- 代理连接的主机必须确保与服务器安全卫士可通信。
- 代理地址填写时，可输入“域名:端口”或“IPv4 代理 IP:端口”。示例：

- **步骤 3：安装引导**

Windows 支持三种安装方式：命令安装、安装包安装、命令+安装包安装。

【命令安装】

——适用于批量安装（需支持 PowerShell 组件）

选择 Agent 安装到的目录位置（默认为：C:\Program Files\TitanAgent），选择命令执行的应用（CMD 或 Powershell），在应用中以管理员权限运行命令，即可安装 Agent；

【安装包安装】

——适用于单台安装，用户可使用操作界面安装

需下载安装包，按照安装流程操作，填入安装程序所需的"安装参数"，点击"安装"，即可安装 Agent；

【安装包+命令】

——适用于批量安装，安装包分发到各主机，批量执行命令

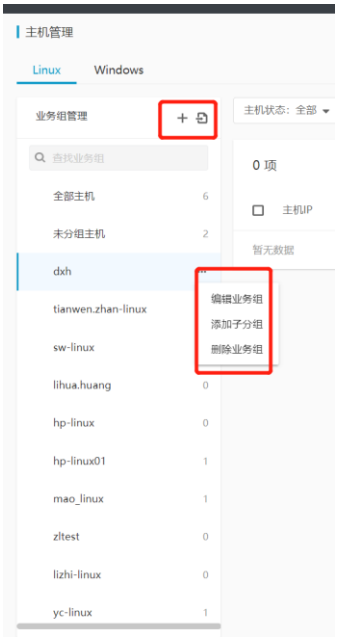
需下载安装包，输入安装包所在位置和 Agent 安装到的目录位置（默认为：C:\Program Files\TitanAgent），才可生成安装命令；生成命令后，在 cmd 中以管理员权限运行命令，即可安装 Agent；

4.6.2 主机管理

主要用来管理安装 Agent 的主机，可以进行：

- 主机所属业务组的管理
- 主机标签管理
- 主机移动所属业务组
- 规则设置：自动同步规则

4.6.2.1 业务组管理

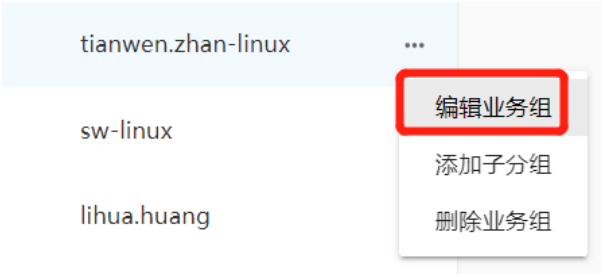


- **新建业务组**

通过单击 + 按钮，可添加业务组。

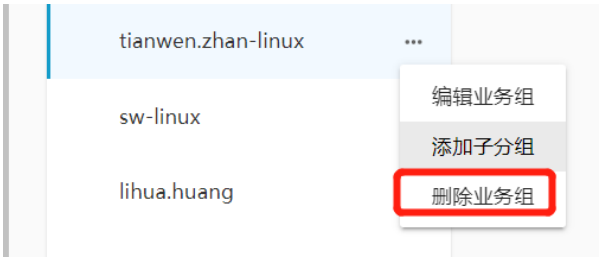
- **编辑业务组**

鼠标移动到要编辑的业务组那一行，右侧出现 ••• ，点击 ••• ，选择“编辑业务组”即可。



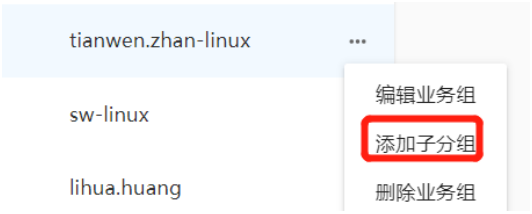
- **删除业务组**

鼠标移动到要删除的业务组那一行，右侧出现 ••• ，点击 ••• ，选择“删除业务组”即可。



- **添加子分组**

鼠标移动到要添加子分组的业务组那一行，右侧出现 ••• ，点击 ••• ，选择“添加子分组”即可。

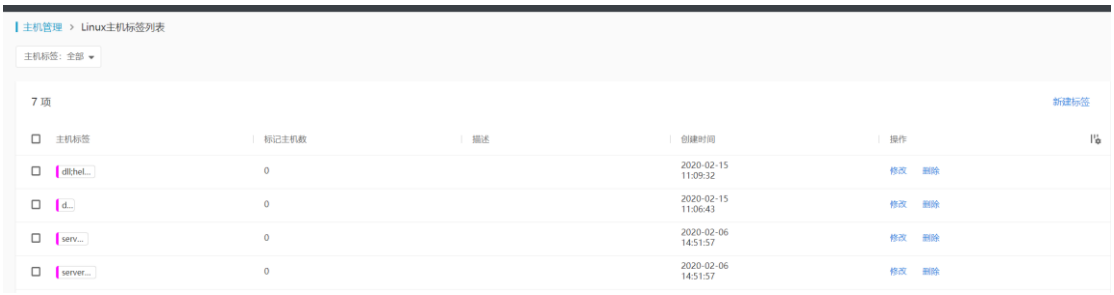


- **导入业务组**

点击 按钮，可以通过导入文件的方式，批量创建业务组。先下载“业务组导入模板”文件，输入要导入的业务组，保存文件后，点击“开始导入”。

4.6.2.2 主机标签设置

可以新建，编辑，删除标签。通过标签速过滤主机。



4.6.2.3 移动业务组

可以单击操作那一栏中的“移出”按钮，移动某个主机所属业务组；也可以勾选复选框，点击右上角“移出”，批量移动主机的所属业务组。

4.6.2.4 规则设置

通过规则设置，可自动将某类主机进行部分操作，包括移动业务组、打标签、编辑运维信息等。

点击界面上的 “规则设置”按钮，进入主机规则列表。

- 新建规则

点击新建规则，将进入“新建规则”界面：

条件列表：主机名中包含、主机 IP 在以下范围内。只有同时满足所有输入的条件时，才会执行所选操作。

执行操作：移动到业务组、标记标签、标记资产等级、修改主机负责人、修改主机负责人的邮箱、修改主机所在机房、修改主机的备注。

规则范围：选择该规则适用的主机范围，可选择全部主机，或通过业务组进行筛选。

描述：规则描述。

- 执行规则

点击执行规则，将依次执行当前列表中的所有规则。

规则执行方式说明：

- 规则根据当前列表中的排序执行，排在最上面的规则最后执行。
- 当两个规则的条件范围发生冲突时，后执行的规则将覆盖先执行的规则。
- 规则默认按照创建时间降序排列，您也可以点击每行规则上的“移动”,可对规则进行上移、下移操作。该操作将会影响规则执行的先后顺序。

4.6.3 IP 显示管理

用于管理主机中存在多网卡 IP 的情况（仅 IPv4 通信主机），定义主机的主显示 IP，支持按 IP 显示和按网卡显示。

4.6.3.1 自定义 IP 显示规则

- 新建规则

- 编辑、删除规则

单击“编辑”“删除”按钮可以对已有规则进行修改或删除。

- 查看详情

单机“查看详情”按钮，可以查看该规则受影响的主机列表。

4.6.3.2 默认 IP 显示规则

IP 显示管理列表界面，点击上方“IP 默认显示规则”，可查看系统默认的 IP 显示规则，如下图所示。

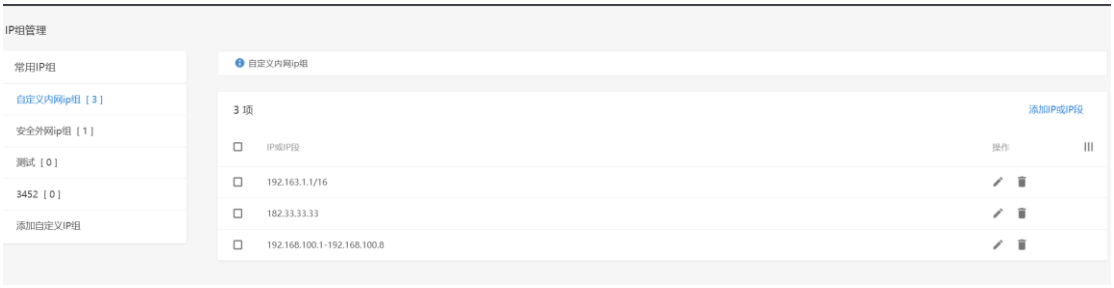
4.6.4 IP 组管理

用户可根据自己需求，对产品中有特定作用和含义的 IP 或者 IP 段，设置为 IP 组进行统一管理，包括：

1） 自定义内网 IP 组：可自定义设置某些"IP 或 IP 段"为内网，则在产品使用中，属于该 IP 组的 IP 会显示为内网 IP；

2） 安全外网 IP 组：可自定义设置某些"IP 或 IP 段"为安全外网；

自定义 IP 组：用户可以自定义 IP 组，以结合自身需求灵活使用。

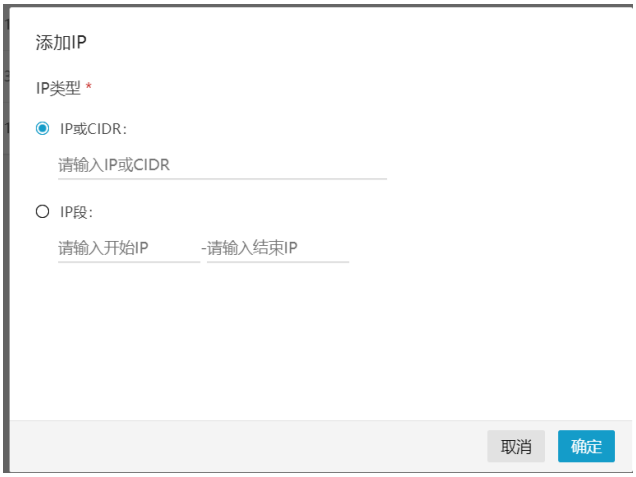


4.6.4.1 分组管理

可自定义 IP 分组，并对其进行编辑和删除，如下图所示。

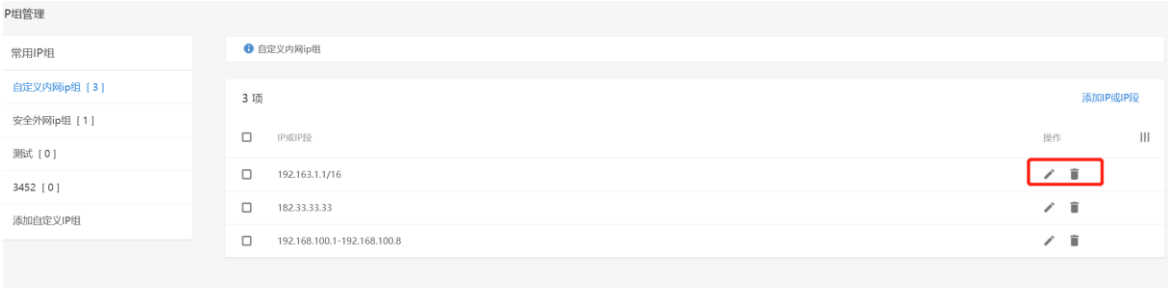
4.6.4.2 添加 IP 或 IP 段

选择分组后，点击“添加 IP 或 IP 段”，弹出添加界面，输入信息，点击“确定”后，可将该 IP 或 IP 组加入该分组。



4.6.4.3 编辑/删除 IP 和 IP 段

分组内已添加的 IP 或 IP 段，希望对其进行编辑或删除，可点击操作出的 和



4.6.5 主机发现

在用户的 IT 运维环境中会在一部分主机上部署青藤的 Agent，用户就需要能够知道还有哪些主机没有部署 Agent（一方面是用户很多时候都不知道在自己的网络环境中有多少主机，另一方面用户也会有一些主机新上线）。主机发现这个功能就是在用户网络环境内通过已经安装了 Agent 的主机发现未安装 agent 的主机，帮用户更全面的了解其网络环境内的主机资源。

主要有以下三种发现方法：

- ARP 缓存发现：Address Resolution Protecol（ARP）缓存是用来存放最近 Internet 地址到硬件地址之间的映射记录。通过在安装了 agent 的主机上查找 ARP 缓存表内存储 IP 信息来获取和这台主机连接过的主机。方法特殊设置：N/A
- Ping 发现：Ping 发现是通过发送 ping 包的方式来发现新主机，支持系统：Linux，Windows（TBD），方法特殊设置：设置扫描的 IP 段
- Nmap 发现

4.6.5.1 扫描任务

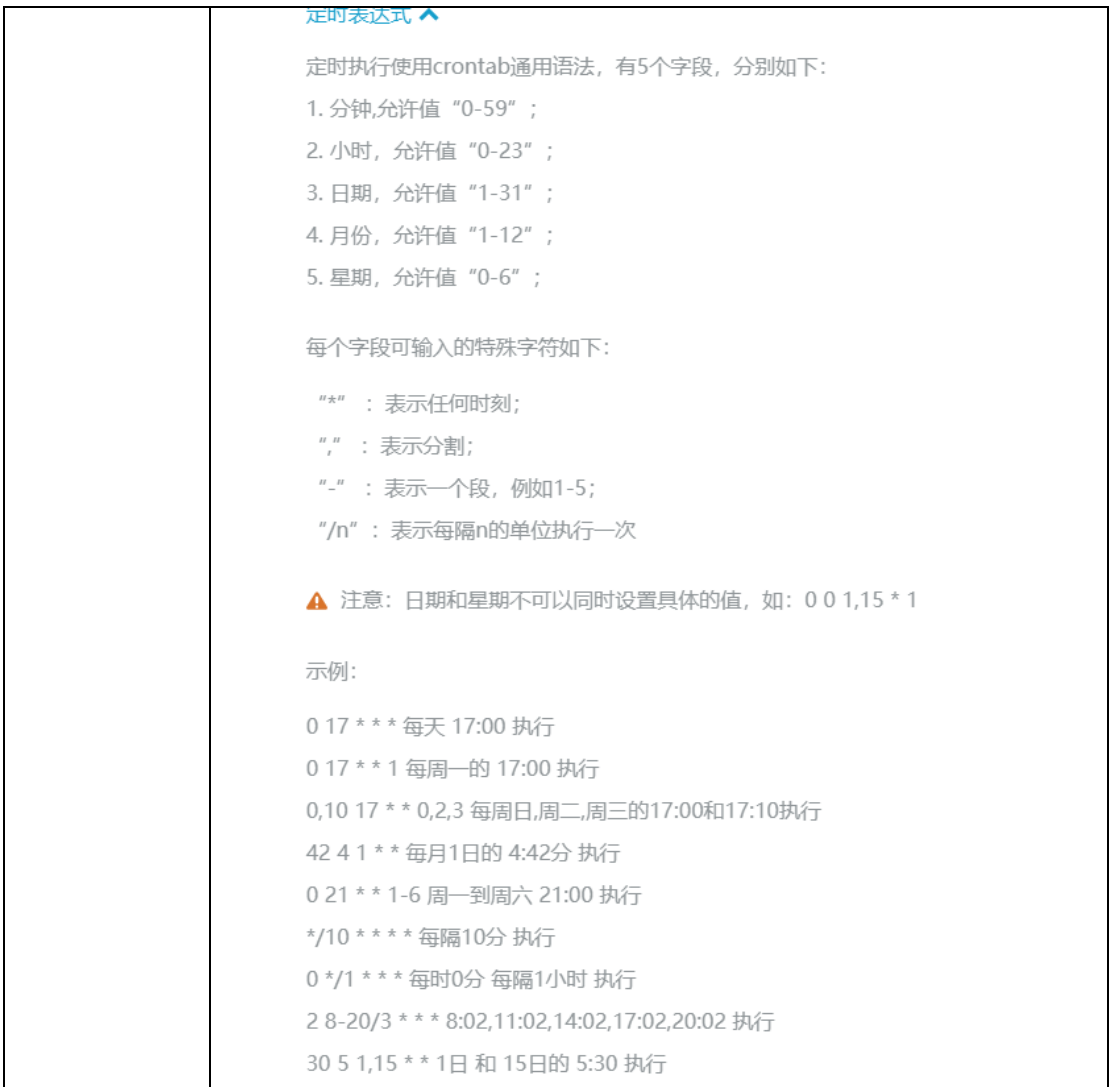
- 新建扫描

系统管理-主机发现-扫描任务-新建扫描，新建扫描功能可以让用户根据其需求配置一个扫描任务。界面如下图所示：

扫描项说明

基本设置	1.1 任务名（必填，不可重复） 扫描任务名是由用户自定义的一个扫描任务的名字，该项目必填不可为空，且任务名是不可重复的。 1.2 发起主机（必填） 扫描发起主机是由用户选择由已经安装 agent 的主机来发起扫描任务，可以选择的对象包括全部主机、某个业务组的机群或是用户自定义组。 发起主机的选项包括： ✧ 全部主机 ✧ 业务组

	✧ 自定义主机 对于发起主机的选择至少需要选择一个，支持多选。 在业务组界面和自定义主机界面可以展示该业务组或者某个主机已经参与的任务，并给出提示，告诉用户主机任务越多，对于性能的开销越大。 1.3 定时扫描（选填） 用户可以对扫描的操作时间可以进行定时扫描，如果不进行设置则会采用默认设置。 • 默认设置 用户如果不进行设置，则采用默认设置，即扫描任务只会被执行一次。 • 手动填写 用户选择对扫描任务进行定时运行设置，即当本次扫描完成以后，间隔规定的时间后会开始一次新的扫描。 扫描时间的填写规则说明如下：



由于扫描时间使用的是 crontab 格式，界面上应该即时对其格式进行校验和显示，如果格式正确则显示器所对应的内容，如果不正确则给出格式错误的提示。

1.4 获取操作系统(选填)

用户可以选择在扫描任务是否需要发现非托管设备的操作系统。

- 默认选择

扫描任务默认是不发现非托管设备的操作系统。

	• 设置发现 设置发现以后，扫描任务会去发现非托管设备的操作系统，但是需要注明这样会使得扫描任务消耗的资源增加。 1.5 扫描网段 扫描网段用来让用户选择设置在 Ping 扫描和 Nmap 扫描下需要扫描的网段，用户可以选择使用默认设置或者手动设置。 • 默认设置 在默认设置下，则负责进行扫描任务的主机去 Scan 其设备所在的网段，需要用文字在界面上进行说明。 • 手动设置 用户手动设置被扫描的网段。在该情况下，则至少需要设置一个网段，也可以添加多个不同的网段。如果是多个网段，需要注意容错处理（比如网段之间的重复、IP 地址是否合法等）。 
扫描方式设置	扫描方法有 ARP 缓存方式扫描、Ping 方式扫描和 Nmap 方式扫描三种方法，用户至少需要选择其中的一种扫描方法，扫描方法支持多

	选。需要在界面注明所选的方法越多，对于机器性能的开销越大。其中，Nmap 方式扫描需要一定的设置，说明如下。 2.1Nmap 方式扫描 Nmap 方式扫描需要分别设置扫描网段、扫描协议和扫描端口。每个设置都有提供默认设置和手动设置。 2.1.1 扫描协议 • 默认设置 在默认设置下，则采用 TCP 协议进行扫描。需要用文字在界面上进行说明。 • 手动设置 用户可以选择对扫描协议进行手动设置，包括只用 UDP、只用 TCP 和都用。需要做的容错是用户不可以一个协议都不选择。 2.1.2 端口设置 • 默认设置 默认设置下，会扫描本系统提供的一些端口。 • 手动设置 如果用户选择使用手动配置，则用户至少需要填写一个端口，并且要对端口进行一些判定，看端口是否合法。
更多扫描设置	更多扫描设置提供了对于以下三种变量的手动设置功能，用户如果不选择手动设置，则使用系统的默认设置。 1. 并发扫描最大数量 2. 每秒最大发包数

	3. 服务器下发任务间隔(可以精确到小数点后一位，需要设置上限，以秒为单位)

- 开始检查

开始检查是指的立刻开始执行某个扫描任务，而不是等待其到相应的时间再开始任务。

- 删除扫描任务

删除扫描功能，会删除当前扫描任务。前提：

1. 普通列表项目不可以删除正在进行的任务。

2. 删除任务不会删除其扫描任务所搜索出来的结果

- 修改扫描

修改扫描，可以让用户重新配置这个扫描的一些配置选项。 关于保存配置和新建扫描是一致的。 前提：

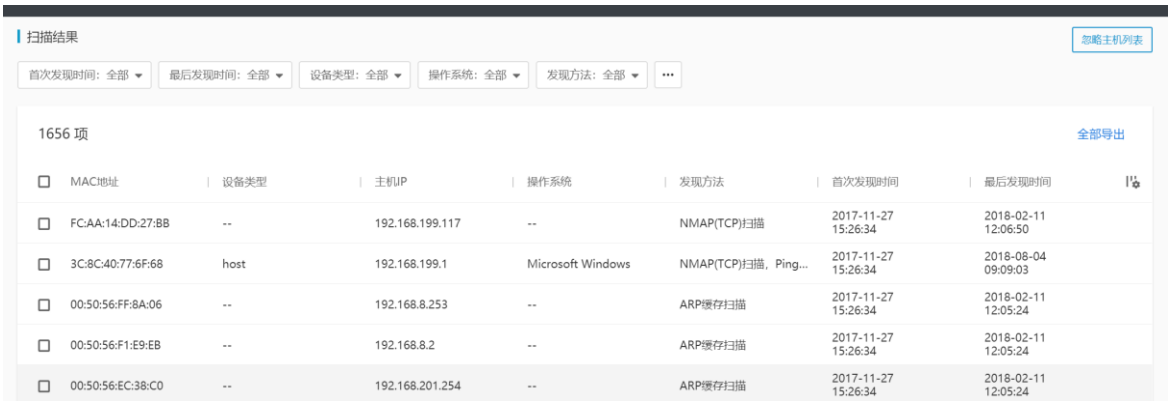
1. 不可以修改正在进行的扫描任务

2. 修改扫描配置不会删除其扫描任务所搜索出来的结果。

- 更新数据依赖

4.6.5.2 扫描结果

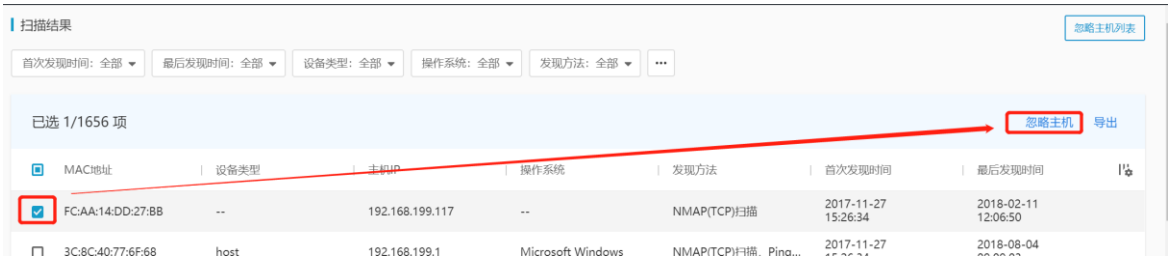
展示所有发现的网络环境中，未安装 Agent 的主机资产。可以根据首次发现时间和最后发现时间等字段进行过滤，筛选出想要的未安装 Agent 主机列表。

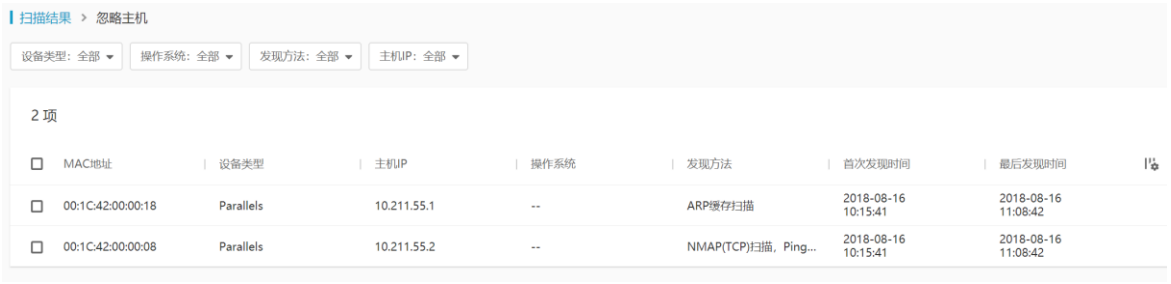


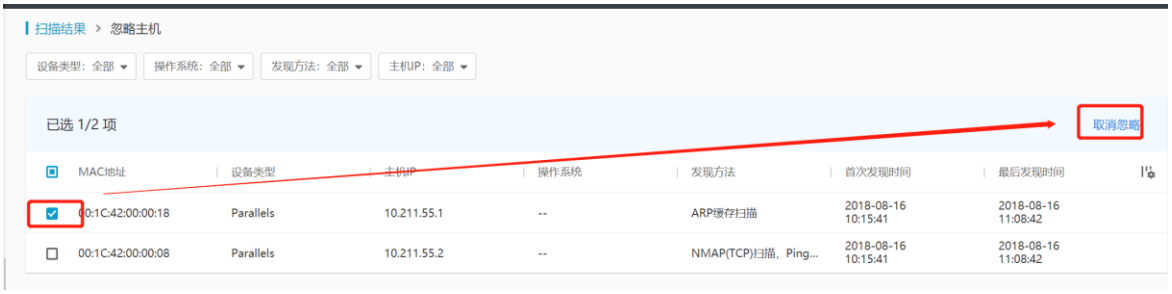
4.6.5.3 忽略主机列表

忽略主机列表指的是在发现主机列表中手动忽略掉的主机。勾选要忽略的主机，点击“忽略主机”按钮即可添加到忽略主机列表中。

加入到忽略主机列表后的主机将不再出现在发现主机列表中，已忽略的主机，可以在忽略主机列表界面取消忽略。







4.6.6 报表系统

报表系统帮助用户进行各类数据的报表导出，对报表文件进行管理。目前有：

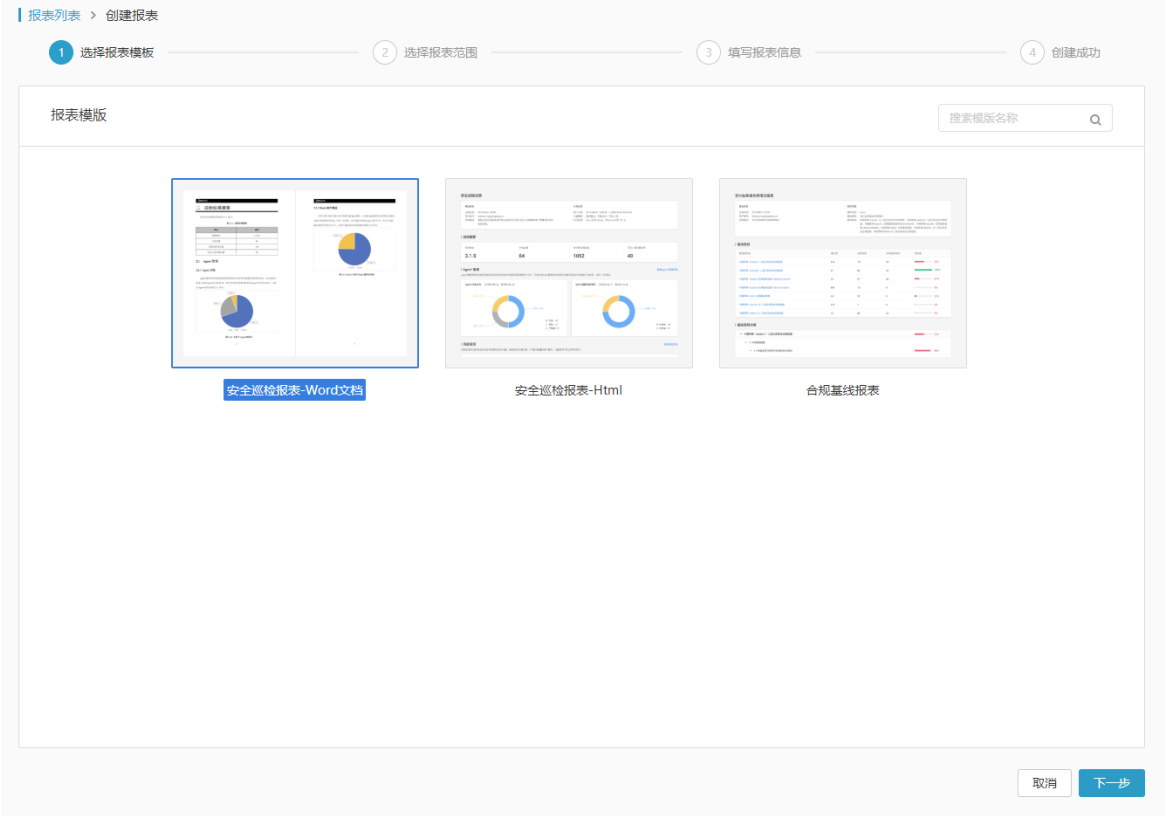
- 安全巡检报表-word 版
- 安全巡检报表-Html
- 合规基线报表

各类报表操作类似，下面以安全巡检报表-word 为例进行介绍。

4.6.7.1 创建报表

单击“创建报表”按钮，进入创建报表页面。

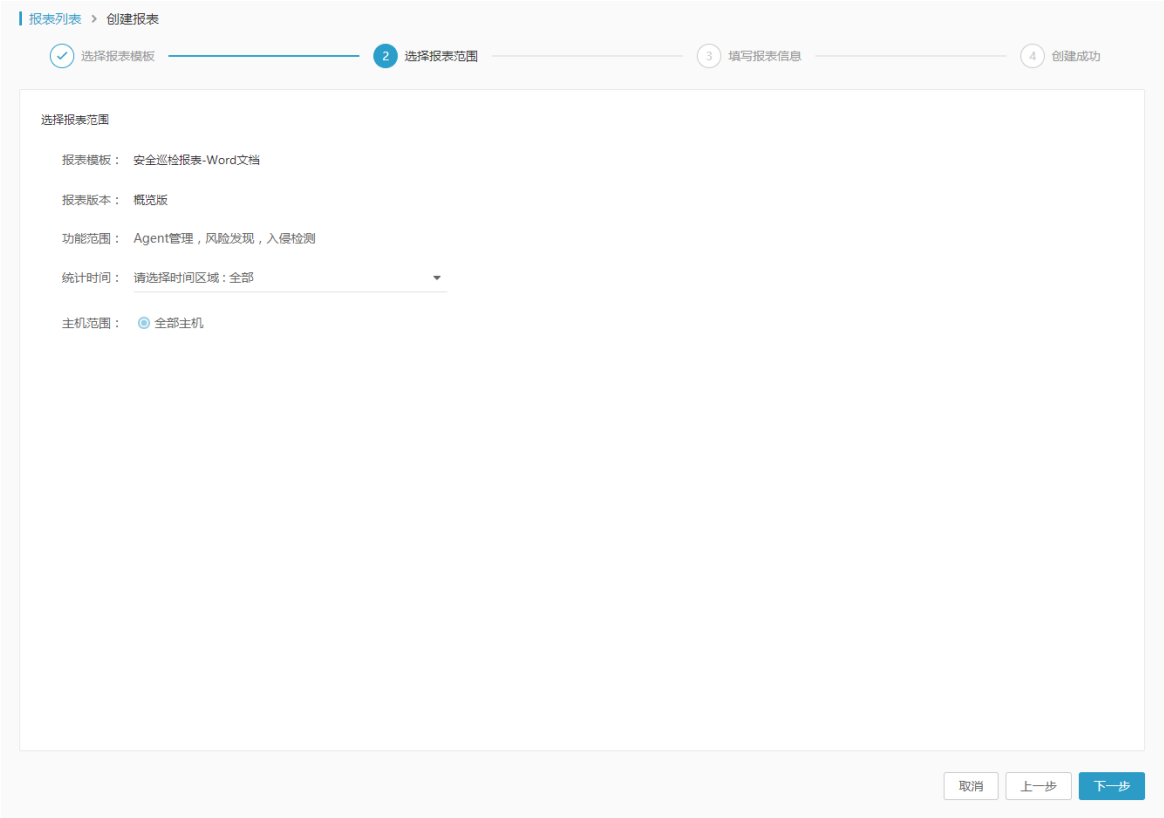
- 选择报表模板



鼠标悬停在模板上，出现“查看”按钮，点击查看可以查看该模板的简介和预览图。

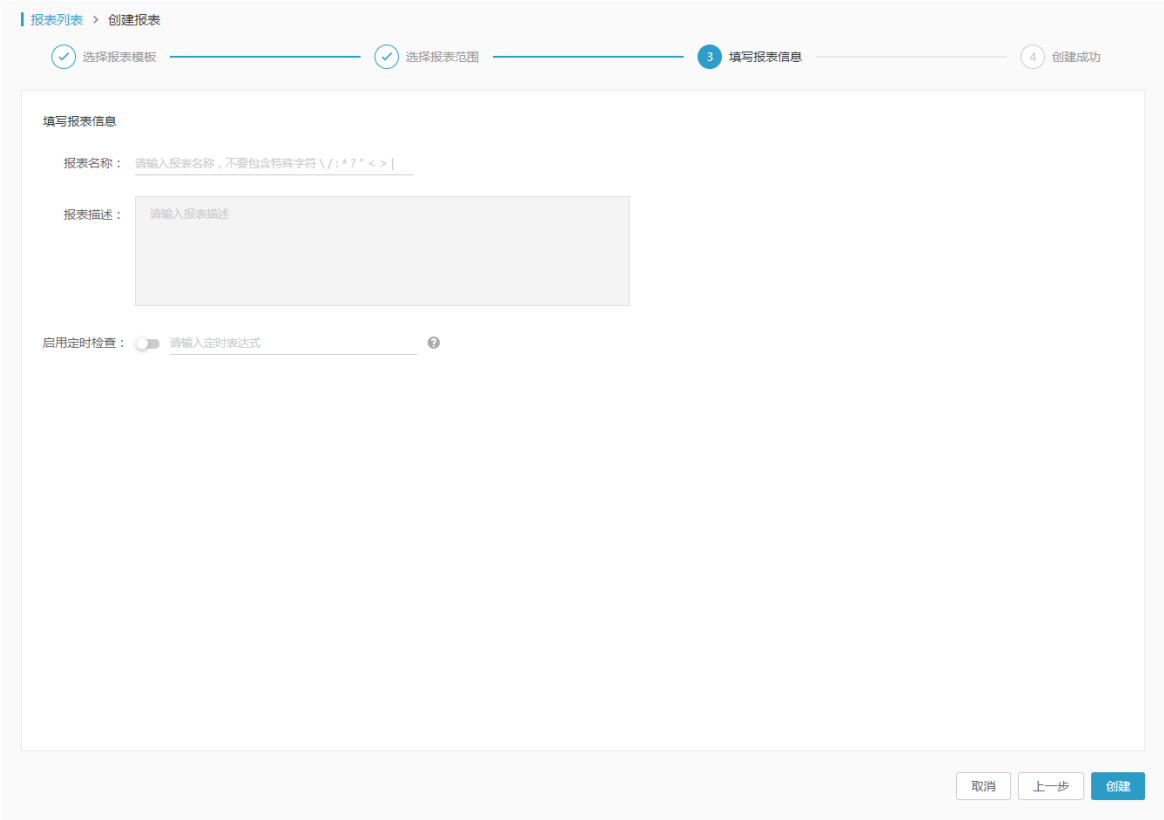
➢ 选择报表范围

不同报表模板对应的报表范围的条件不一样，根据具体的模板选定报表范围。



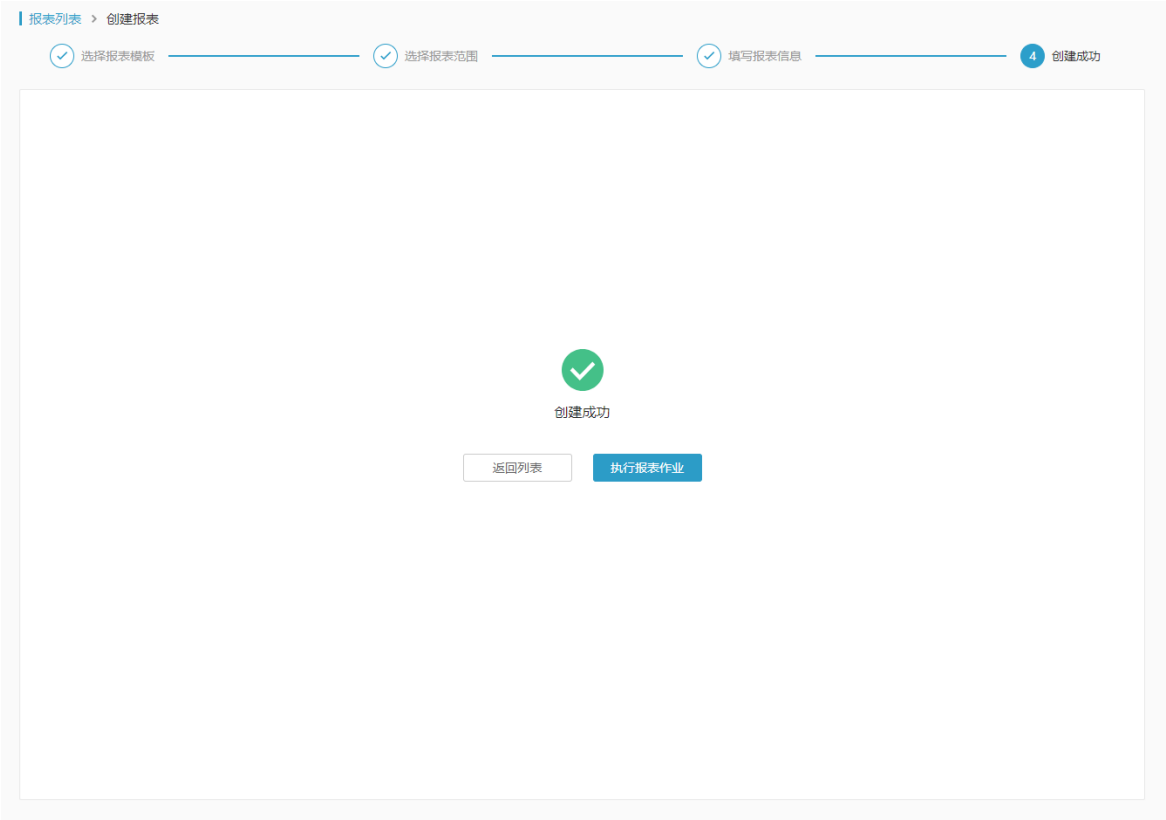
➢ 填写报表信息

填写报表的名称，描述，以及设定定时执行表达式。其中由于报表文件名在本地的限制，故报表名称不支持特殊字符。



➢ 创建成功

报表创建成功后，可返回首页的报表列表，也可以执行刚刚创建的报表作业。



4.6.7.2 执行报表

在报表列表页面，选择某一个报表作业，点击后边的“执行”按钮后，开始执行该报表作业。

4.6.7.3 下载报表

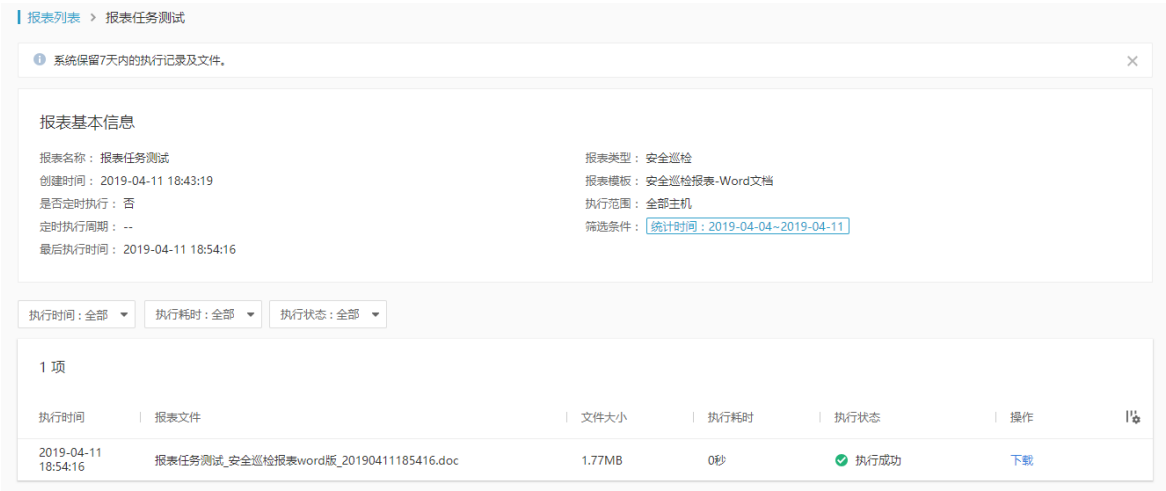
执行报表作业后，点击操作的“下载报表”按钮，可以下载最近一次生成的报表。

4.6.7.4 修改/删除报表

点击操作中的 ••• ，选择下拉框的“修改/删除”按钮，可以修改或删除报表。

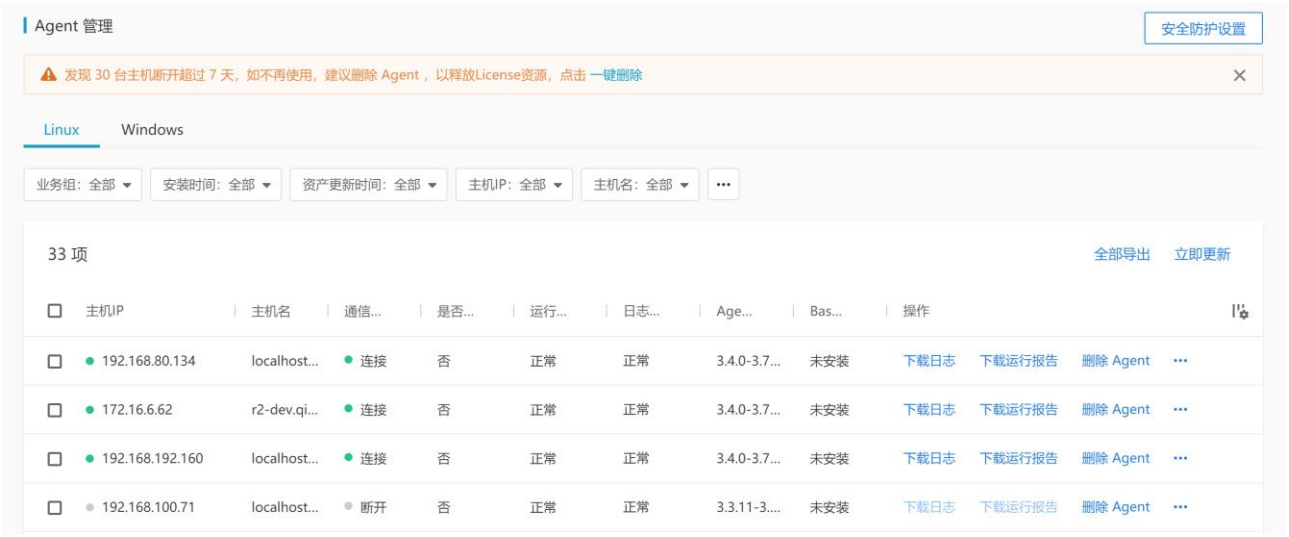
4.6.7.5 查看执行记录

点击操作 ，选择下拉框的“查看执行记录”按钮，可以查看该报表七天内的执行记录，并且下载相应执行记录中的报表文件。

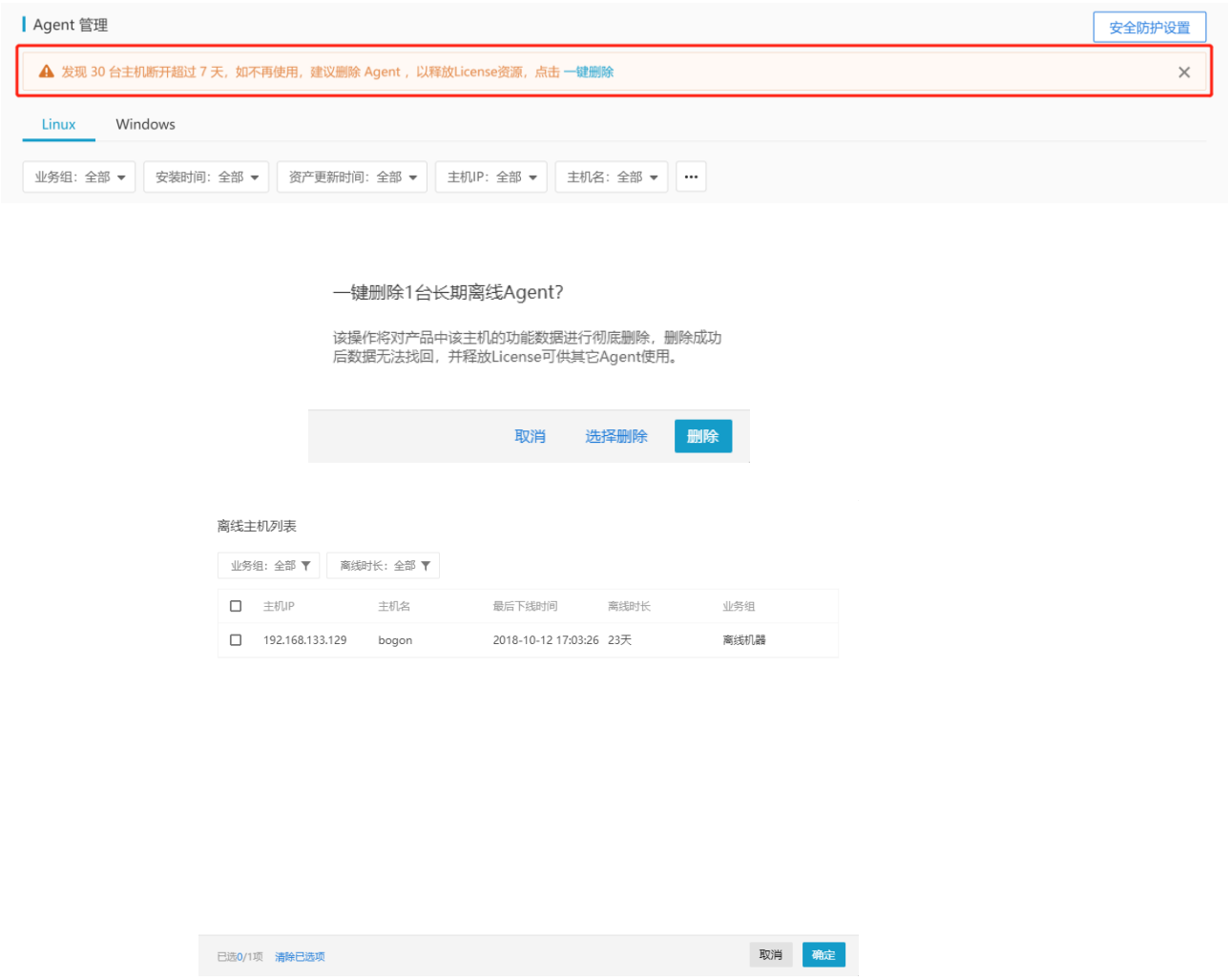


4.6.7 Agent 管理

Agent 服务管理：显示所有 Agent 的状态，并可随时调整 Agent 运行模式，导出 Agent 运行日志与报表，随时分析解决问题。



对于主机离线超过 7 天的主机，提供删除功能，释放 License 资源.



在排查问题的过程中，可设置 Agent 运行级别，下载日志和运行报告。

1）设置运行级别：

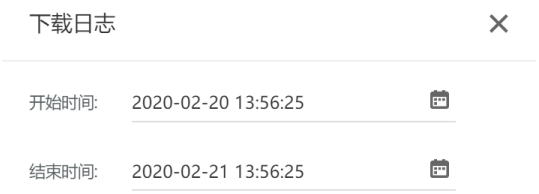
- 正常：Agent 拥有完整能力，执行服务器的任务。
- 降级：是一种保护模式，Agent 不再接受服务器下发的任务，直至恢复为非"降级"状态。
- 停用：停止 Agent 业务功能，只保留基本通信能力和任务执行能力（如：卸载，恢复在线）。

2） 设置日志级别

处理问题时，可设置日志级别为 Debug 模式，该模式下的日志比正常模式下相对较多，方便排查问题。

3）下载日志

可选择时间段，下载该时间段内的日志信息。



4） 下载运行报告

下载 Agent 运行情况的报告。

5）重启 Agent

重新启动 Agent，不改变原"主机状态"和"运行级别"。

6）删除 Agent

彻底清除产品中该 Agent 所有数据信息，显示为"清除数据中"，清除完成后 触发统计更新（详见下文）；并下发"Agent 卸载"命令，释放"AgentID"。

4.6.8 系统审计

系统审计用于记录用户在使用本产品时产生的操作，用户可在系统审计功能中查看自己历史的操作详情，方便快速地追溯失败操作和误操作的原因。可根据时间、操作类型、所属功能模块字段进行筛选。

4.6.9 通知系统

通知中心与接收配置：系统所有告警与通知统一管理，可灵活选择接收的通知，每种通知均提供站内信，邮件，短信，syslog 等多种通知方式。

右上角点击，然后点击，可设置消息接收类型及接收人等信息。

5 常见问题

Q：服务器安全产品能解决什么问题?

A：服务器安全卫士产品是一个完整的服务器安全防护系统，帮助客户建立防御-检测-响应-预测全面安全体系。服务器安全卫士产品能够解决防御的问题，缩小系统攻击面，提升安全等级。也能够解决如何发现黑客的问题，包括:实时黑客行为特征锚点监控，检测黑客常见入侵手段；与业务正常行为结合分析，发现系统内部异常潜伏攻击。

Q：安装 Agent 会不会对自身的业务稳定性产生影响?

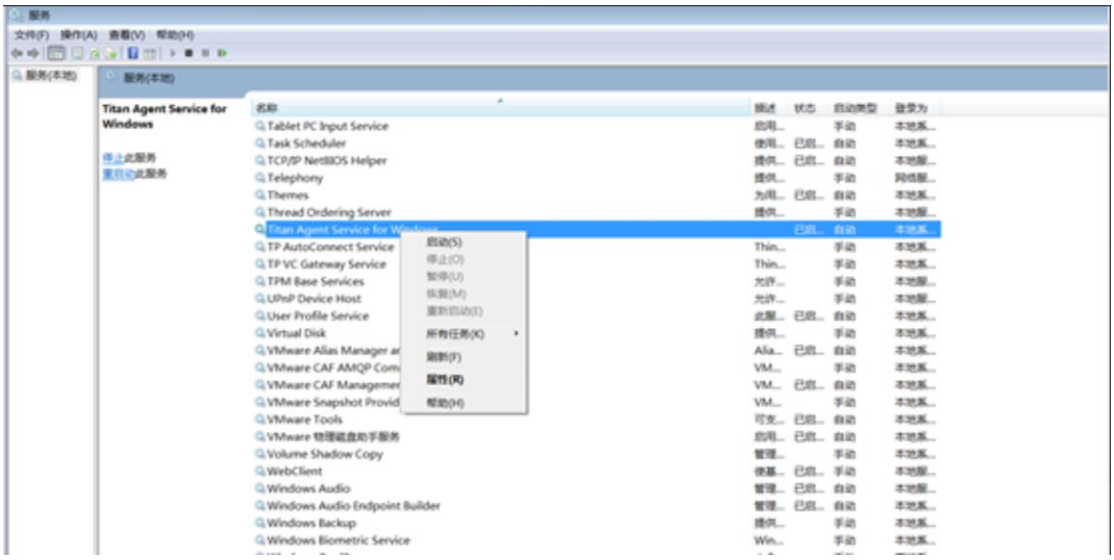
A：不会。Agent 是纯应用层的，不会给系统装任何的驱动，不会影响系统的稳定性；Agent 对系统是只读的，不会改写任何数据；Agent 的带宽和资源占用很小；Agent 已经通过各种业务场景长时间运行测试。

Q：Agent 启动、停止、重启的操作命令是什么?

A：Linux 系统环境下，需进入/titan/agent 目录，操作命令如下：

- Agent 停止命令：./titanagent -s
- Agent 启动命令：./titanagent –d
- Agent 卸载命令：bash install_agent.sh disclean_agent.sh

Windows 系统环境下，打开服务管理器，找到 Titan Agent Service for Windows 服务，右击该服务，即可对 Agent 进行启动、停止和重新启动操作，如下图：



Q：Linux 环境下卸载 Agent

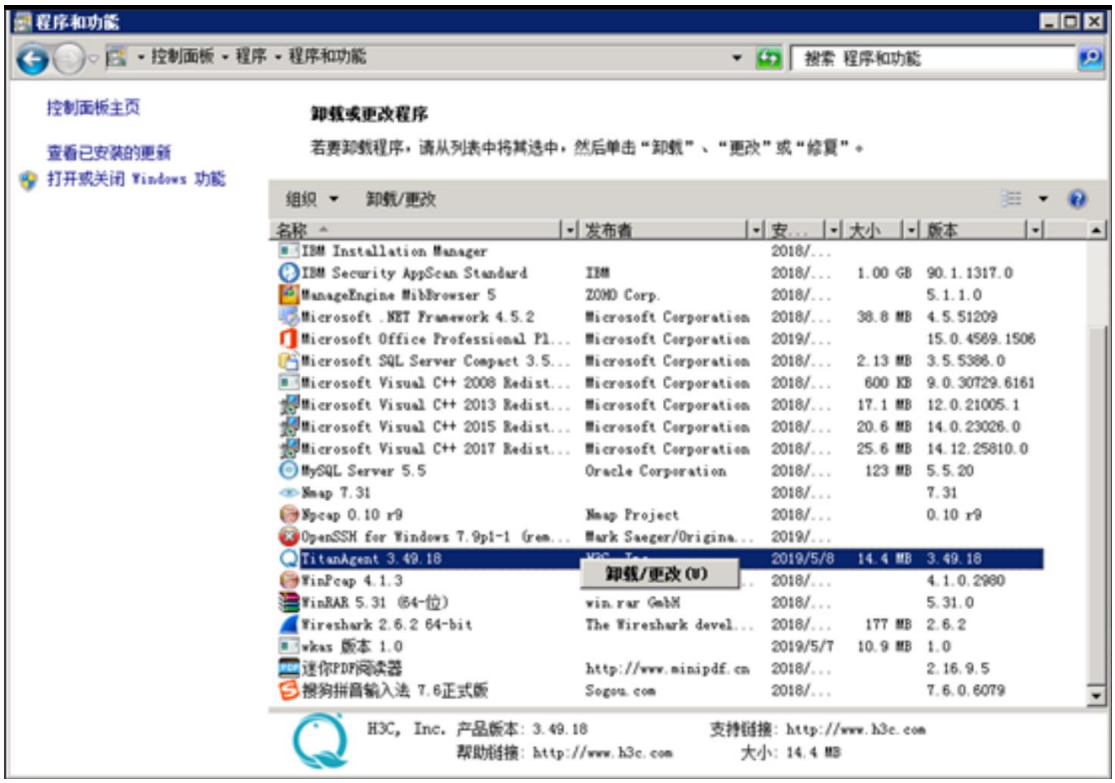
A：本方式在客户端 Agent 在线及离线均生效。

使用账号密码，登录已安装 Agent 的主机，以 root 权限依次执行以下命令即可卸载 Agent：

/titan/agent/titanagent -s

bash /titan/agent/install_agent.sh disclean

Windows 系统环境下，打开控制面板下选择卸载程序，找到 49.18，并右击选择“卸载/更改（U）”，根据引导卸载信息完成卸载。



Q：是否可以对内网主机进行监测防护?

支持。安装 Agent 时设置代理服务器。

Q：订购后如何部署?

A：购买成功后，进入控制中心-“服务器安全卫士”界面，点击“控制台”，进入控制台后，在通用功能-系统设置-Agent 安装界面，根据页面提示安装 Agent 即可。

Q：如何接收监测报告?

A：服务器安全卫士支持以邮件的方式将报告发给客户指定邮箱（首次登陆服务器安全卫

士时控制台需要填写邮箱)。客户可在服务器安全卫士消息中心——消息接收配置界面，配置是否接收报告，也可添加接收人。

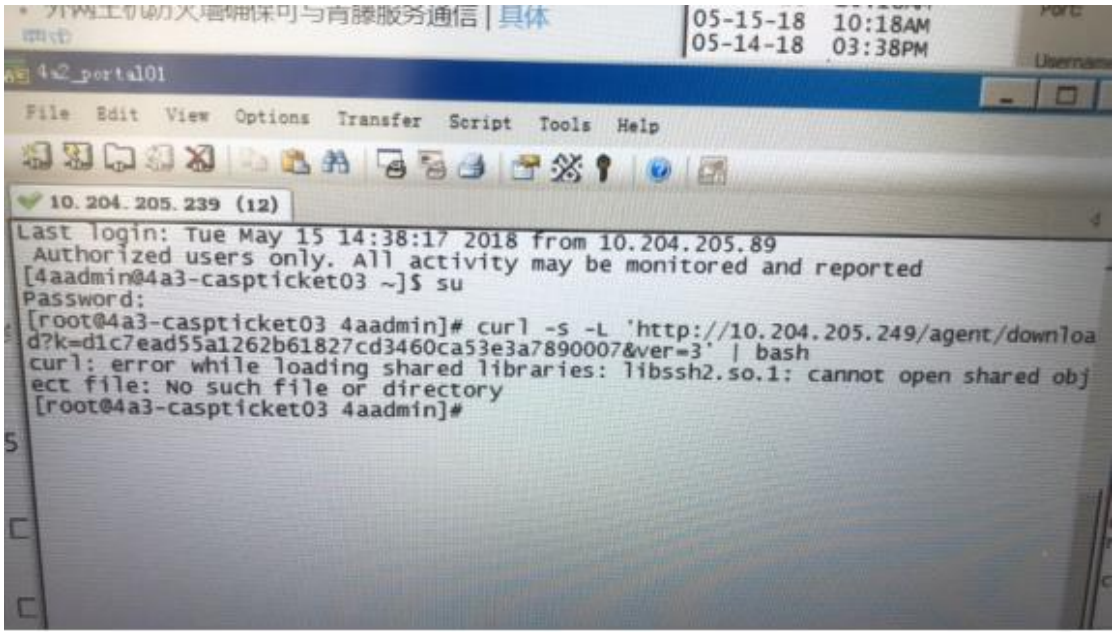
Q：如何接收实时告警?

A：服务器安全卫士支持邮件、短信、站内信方式将告警实时告知客户，客户需要在首次登陆服务器安全卫士控制台时填入接收的邮箱和手机号，也可以在服务器安全卫士消息中心——消息接收配置界面，配置接收通知的消息类型、接收方式和接收人。

Q：Linux 客户端 Agent 安装失败

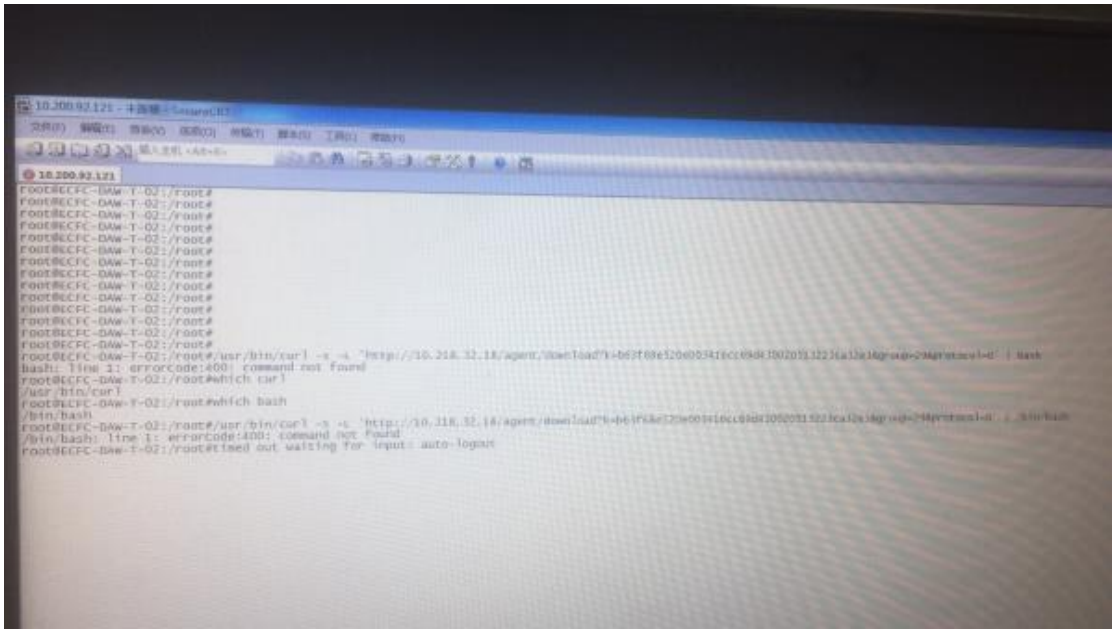
A：待安装服务器的操作系统是否在安全卫士支持列表中；

现象 1：Linux 服务器执行 Agent 安装命令报“[ERROR] curl: error while loading shared libraries ”



解决方案： 登陆前台 Agent 安装页面，查看安装依赖条件是否完备。

现象 2：bash: line 1: errorCode:400: command not found



解决方案：一般错误原因是由于 agent 安装命令中的参数 k 不正确，解决方式：从前台的 Agent 安装页面重新生成安装命令，然后尝试重新安装。

现象 3：Linux 服务器执行安装命令报“ [ERROR] check crond fail”：

解决方案：原因由于 crond 不能写入或 crond 不存在，需要先安装 crond；

现象 4：Linux 服务器执行安装命令报“[ERROR] conf crond fail”

解决方案：

1、用户权限问题，确认一下是否是安装在 root 用户下，不支持普通用户安装。

2:、登录密码过期

Q：Windows 客户端 Agent 安装失败

A：

现象 1：安装时输出 http error code 28

解决方案：

1. 检查与服务端的网络是否正常联通，测试方法：把安装 url 填到浏览器，看看能否正常链接加载内容
2. 检查客户是否配置防火墙进行了拦截
3. 检查客户环境是否有 WAF 进行了拦截操作

现象 2：安装时输出 Installer integrity check has failed....

解决方案：参考 https://zhidao.baidu.com/question/273408240.html

现象 3：检查 sys.log 发现 Can't modify service config 3 这句出现

解决方案：是由于客户操作系统环境注册表写入问题，需要排查是否是禁用注册表写入或是杀毒拦截等原因

现象 4：安装提示 Error Launching installer

解决方案：把安装程序放置到纯英文目录尝试再次安装

现象 5：安装时提示错误：抽取，无法写入文件

解决方案：查看 C 盘磁盘是否已经满了，如果满了，清理一下磁盘

现象 6：

windows 服务器安装 agent 报错下载文件失败，如下图：

telnet server 所有端口都是通的，但是访问

http://32.12.65.139:8002/plugins/v3.58.46-win64/TitanAgent_for_All.exe 失败。

telnet 成功后按 ctrl c 结束时会有 400 返回.

原因：

客户 windows 服务器设置了网络代理，查看方式为打开 ie 浏览器，选择设置→

Internet 选项→连接→局域网设置，如下图 ：

解决办法：

打开 ie 浏览器，选择设置→Internet 选项→连接→局域网设置→高级→在“对于下列字符开头的地址不使用代理服务器”中填写：http://server ip;server ip 如下图：

完成配置后重新打开 cmd 执行安装命令。

现象 7：

windows 安装 agent 时报错“文件或目录损坏且无法读取”；

解决方案：

确认发现是客户使用账号没有权限写 C 盘目录，使用管理员权限问题解决。

现象 8：安装 windows agent 包 NSIS 错误

解决方案：客户系统是 windows 英文版系统，存放安装包的目录带有中文，打开安装包就报错。将安装包移到纯英文目录下就可以正常安装。

Q：非 bash 环境下，入侵功能是否可以使用?

A：入侵功能中仅可疑操作功能和 bash 里的操作相关，故非 bash 环境入侵仅可疑操作功能可能受影响。

Q：后门检测中隔离与删除的区别?

A：隔离与删除的区别在于隔离把文件备份到了 Agent 安装目录下的隔离目录中并进行了加密（AES 对称加密算法），防止其再次运行，之后对原路径下的后门进行删除，因此隔离后的文件是可以通过 Agent 下发还原指令进行恢复的；而删除则直接将原文件删除，并无备份，故删除操作是不可逆的，具备一定风险。

Q：风险扫描耗时很久，此时点击其他界面是否会中断扫描任务?

A：扫描过程中点击其他页面不会中断扫描任务。

Q：审计功能正常，为何前台界面不显示?

A：检查 Agent 所在的服务器时间与标准时间是否一致

Q：资产清点有什么优势?

A：产品支持 Windows，Linux 所有主流的操作系统与版本。包括：Redhat、CentOS、Ubuntu、Oracle Linux、SUSE、Debian、OpenSUSE、Windows Server、Windows 桌面系统等。

产品资产清点的技术优势主要体现在两个方面。

（1）数据的获取速度快，定期清点资产数据放入快速缓存，查询数据或使用数据从快速缓存中获取。

（2）对于变化较为频繁的数据（例如进程，端口），在定时更新的基础上，用户可以按需主动更新，避免因为本地数据库过于陈旧，检测不准确，也避免传统方案不断监控变化（频繁变化的数据在使用时，实际只需要获取最新的状态），导致的无意义性能消耗。

Q：怎么保证检测的漏洞的准确性?

A：漏洞的检测方式为版本比对和 POC 验证两种方式。

（1）版本比对：通过获取应用的包安装版本和进程版本，将其与应用的漏洞版本进行比对。

（2）POC 验证：即对漏洞逐个进行分析，根据漏洞原理编写对应的漏洞验证脚本，逐个漏洞进行检测。