



青藤云安全

安全产品使用手册 V3.3.0.3

让安全更有效

二零一九年十一月

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属青藤云安全所有，受到有关产权及版权法保护。任何个人、机构未经青藤云安全的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 版本变更记录

时间	版本	说明	修改人
2018-05-23	V1.0	文档创建	售后部
2018-11-05	V2.0	文档基于 3.2.0 版本更新	产品部
2019-01-03	V2.1	文档基于 3.2.0.2 版本更新	产品部
2019-03-27	V3.0	文档基于 3.3.0 版本更新	产品部
2019-11-15	V3.1	文档基于 3.3.0.2 版本更新	产品部

■ 适用性声明

本文档为北京升鑫网络有限公司（以下简称“青藤云安全”）的用户产品使用手册，适用于相关技术人员准备测试环境时进行参考。

目录

一. 青藤云安全主机监控管理系统概述.....	6
1.1 核心功能.....	6
1.2 网络架构图.....	7
二. 安全首页.....	8
三. Linux.....	9
3.1 资产清点.....	9
3.1.1 主机资产.....	14
3.1.2 进程端口.....	17
3.1.3 系统账号.....	21
3.1.4 硬件配置.....	26
3.1.5 软件应用.....	28
3.1.6 Web 服务.....	31
3.1.7 数据库.....	35
3.1.8 Web 站点.....	38
3.1.9 Web 应用.....	40
3.1.10 Web 应用框架.....	42
3.1.11 安装包和类库.....	46
3.1.12 其他.....	50
3.2 风险发现.....	错误!未定义书签。
3.2.1 风险总览.....	59
3.2.1 安全补丁.....	63
3.2.2 漏洞检测.....	69
3.2.3 弱密码.....	75
3.2.4 应用风险.....	79
3.2.5 系统风险.....	79
3.2.6 账号风险.....	80
3.3 入侵检测.....	81
3.3.1 入侵总览.....	82
3.3.2 暴力破解.....	83
3.3.3 异常登录.....	87
3.3.4 反弹 Shell.....	90
3.3.5 本地提权.....	94
3.3.6 后门检测.....	96
3.3.7 Web 后门.....	99
3.3.8 可疑操作.....	104
3.4 合规基线.....	114
3.4.1 基线检查.....	114
3.4.2 查看检查结果.....	115
3.4.3 新建检查.....	117
3.4.4 凭证管理.....	119
3.4.5 查看白名单.....	120

3.5 单台主机详情.....	122
四. Windows.....	122
4.1 资产清点.....	122
4.1.1 主机管理.....	124
4.1.2 进程管理.....	126
4.1.3 账户管理.....	130
4.1.4 安装程序与运行应用.....	134
4.1.5 Web 管理.....	139
4.1.6 站点管理.....	143
4.1.7 数据库.....	145
4.1.8 启动项清点.....	145
4.2 风险发现.....	148
4.2.1 安全补丁.....	148
4.2.2 弱密码检查.....	150
4.2.3 web 风险文件.....	153
4.3 入侵检测.....	154
4.3.1 暴力破解.....	154
4.3.2 异常登录.....	158
4.3.3 后门检测.....	161
4.3.4 Web 后门.....	162
4.4 合规基线.....	166
4.4.1 基线检查.....	166
4.4.2 查看检查结果.....	168
4.4.3 新建检查.....	169
4.4.4 凭证管理.....	171
4.4.5 查看白名单.....	172
4.4.6 更新数据.....	174
4.5 单台主机详情.....	174
五. 通用功能.....	176
5.1 系统设置.....	176
5.1.1 Agent 安装.....	176
5.1.2 主机管理.....	179
5.1.3 IP 显示管理.....	184
5.1.4 IP 组管理.....	185
5.2 主机发现.....	186
5.2.1 设置扫描任务.....	186
5.2.2 扫描结果列表.....	190
5.2.3 忽略主机列表.....	191
5.3 报表系统.....	191
5.3.1 创建报表.....	192
5.3.2 报表列表.....	195
5.4 权限管理.....	196
5.4.1 账号管理.....	196
5.4.2 用户组管理.....	204

5.4.3 角色管理	208
5.5 服务工具	212
5.5.1 Agent 管理	212
5.6 系统审计	214
5.7 通知系统	215
5.8 通用设置管理	218
5.8.1 账户登录	218
5.8.2 账户信息管理	219
5.8.3 下载记录	221
5.8.4 购买信息	221
5.8.5 关于青藤	222

一. 青藤云安全主机监控管理系统概述

1.1 核心功能

青藤专注于服务端主机的安全防护，提供持续的安全监控、分析和快速响应能力，能够在公有云、私有云、混合云、物理机、虚拟机等各种业务环境下实现安全的统一策略管理和快速的入侵响应能力。

青藤的产品可以很方便地和各种云平台及传统服务器结合，能够在全局范围内轻易部署。使用产品不需要购买硬件，不需要复杂的配置，学习成本低，但精确度极高。青藤的产品向企业的运维和安全人员提供了安全管理海量服务器的能力，使得用户在降低成本、缺乏安全专业知识的前提下，也能极大地提高企业的安全防护能力。

青藤采用的 **Adaptive Security** 架构是 **Gartner** 提出的面向未来十年的企业安全架构，能够在复杂和变化的环境下有效抵御高级攻击，是整个安全行业的发展方向。其创新之处在于：一方面将安全视角转移到防火墙之后的业务系统内部，强调基于业务、自内而外地构建安全体系，另一方面将安全从传统的安全事件防护变成一项持续安全响应和处理过程，从多个维度持续地保护了企业安全。

安全是一个持续化的过程，青藤产品有快速、灵活、可扩展的特点，可以将现有的安全技术与持续运营的安全模型相结合，给用户提供一个持续化的动态安全解决方案。青藤产品提供统一安全管理平台，统一的安全框架和灵活的社区交互能力，将安全的价值最大化。

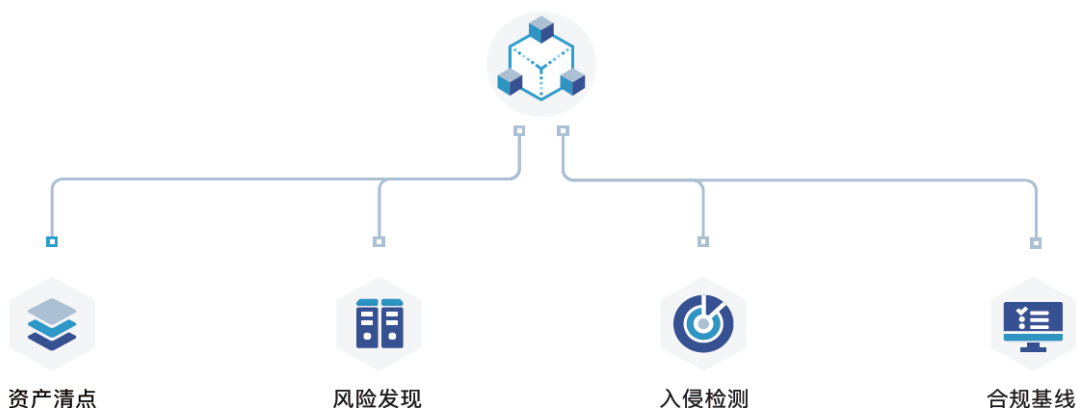


图 1.1 青藤万相·主机自适应安全平台产品体系

青藤的安全产品体系有三大部分组成：

- 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，200 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

入侵检测提供多锚点的检测能力，能够实时、准确地感知入侵事件，发现失陷主机，并提供对入侵事件的响应手段。

- 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。

1.2 网络架构图

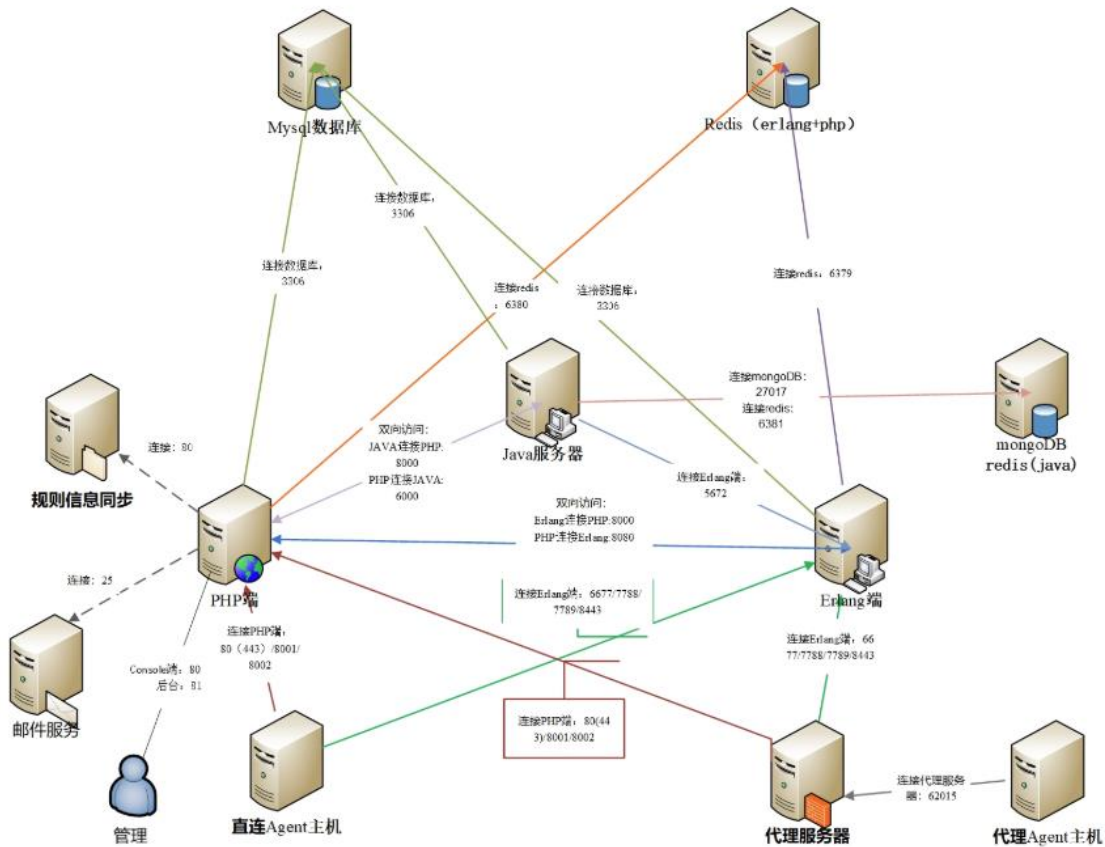


图2.1 网络架构图

青藤云安全主机监控管理系统共分为三部分：**Server** 服务器、**Agent** 主机、代理服务器。**Server** 服务器上承载有主机监控管理系统的绝大部分运行程序，负责对搜集来的数据进行统一的挖掘、分析、控制与呈现。**Agent** 主机为被管理主机，其上安装有青藤主机安全探针，负责对所属主机进行安全巡检以及实时地入侵监控。代理服务器为承载有 **socket** 代理软件的 **CentOS** 主机，用以连接不同网域内 **Agent** 主机。

二. 安全首页

Linux 首页

The screenshot shows the Linux security dashboard homepage. At the top, there are tabs for "Linux" and "Windows", with "Linux" selected. Below the tabs, there are five feature cards arranged in two rows. Each card has an icon, a title, and a brief description. The features are: 资产清点 (Asset Inventory), 风险发现 (Risk Discovery), 入侵检测 (Intrusion Detection), 合规基线 (Compliance Baseline), and 安全日志 (Security Logs). A faint Linux penguin logo is visible in the bottom right corner of the dashboard area.

Linux Windows

- 资产清点**
从安全角度自动化构建粒度资产信息，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
- 风险发现**
精准发现内部风险，快速定位问题并有效解决安全风险，提供详细的资产信息、风险信息以供分析和响应
- 入侵检测**
提供多维度的检测能力，能够实时、准确地感知入侵事件，发现攻击主机，并提供对入侵事件的响应手段
- 合规基线**
构建了国内信息安全等级保护要求和CIS标准要求，覆盖多个版本主流操作系统、Web应用、数据库等
- 安全日志**
从安全角度引导用户对日志进行查询与分析，发现黑客入侵的蛛丝马迹，还原攻击现场

windows 首页

The screenshot shows the Windows security dashboard homepage. At the top, there are tabs for "Linux" and "Windows", with "Windows" selected. Below the tabs, there are five feature cards arranged in two rows. Each card has an icon, a title, and a brief description. The features are: 资产清点 (Asset Inventory), 风险发现 (Risk Discovery), 入侵检测 (Intrusion Detection), 合规基线 (Compliance Baseline), and 安全日志 (Security Logs). A faint Windows logo is visible in the bottom right corner of the dashboard area.

Linux Windows

- 资产清点**
从安全角度自动化构建粒度资产信息，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
- 风险发现**
精准发现内部风险，快速定位问题并有效解决安全风险，提供详细的资产信息、风险信息以供分析和响应
- 入侵检测**
提供多维度的检测能力，能够实时、准确地感知入侵事件，发现攻击主机，并提供对入侵事件的响应手段
- 合规基线**
构建了国内信息安全等级保护要求和CIS标准要求，覆盖多个版本主流操作系统、Web应用、数据库等
- 安全日志**
从安全角度引导用户对日志进行查询与分析，发现黑客入侵的蛛丝马迹，还原攻击现场

三. Linux

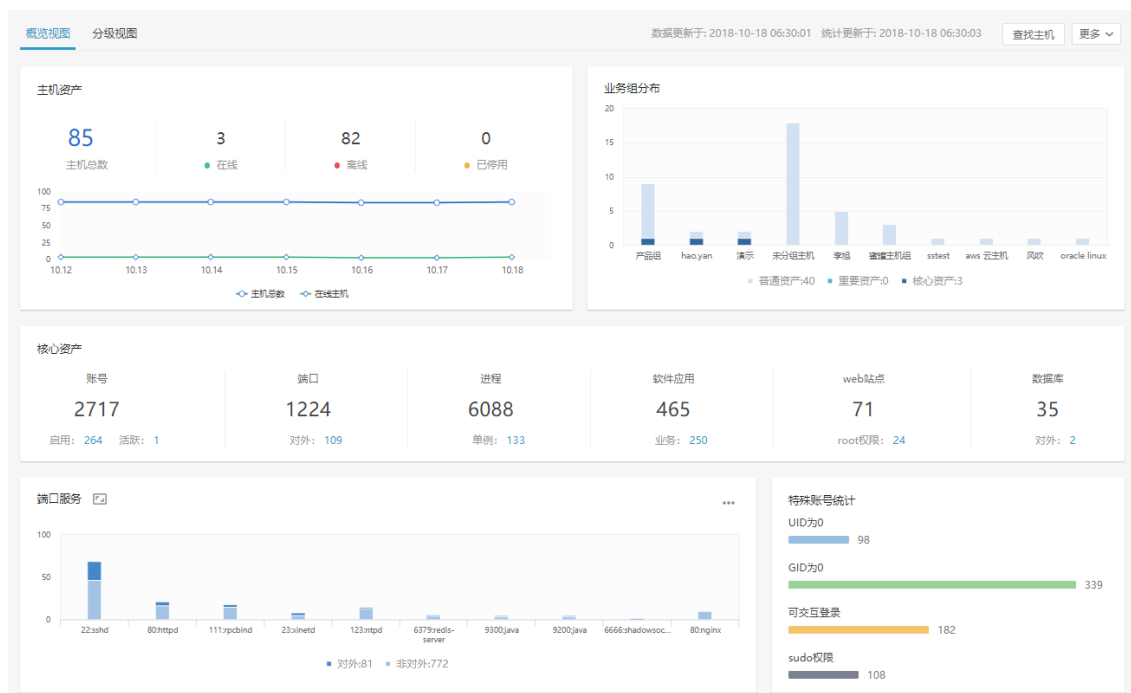
3.1 资产清点

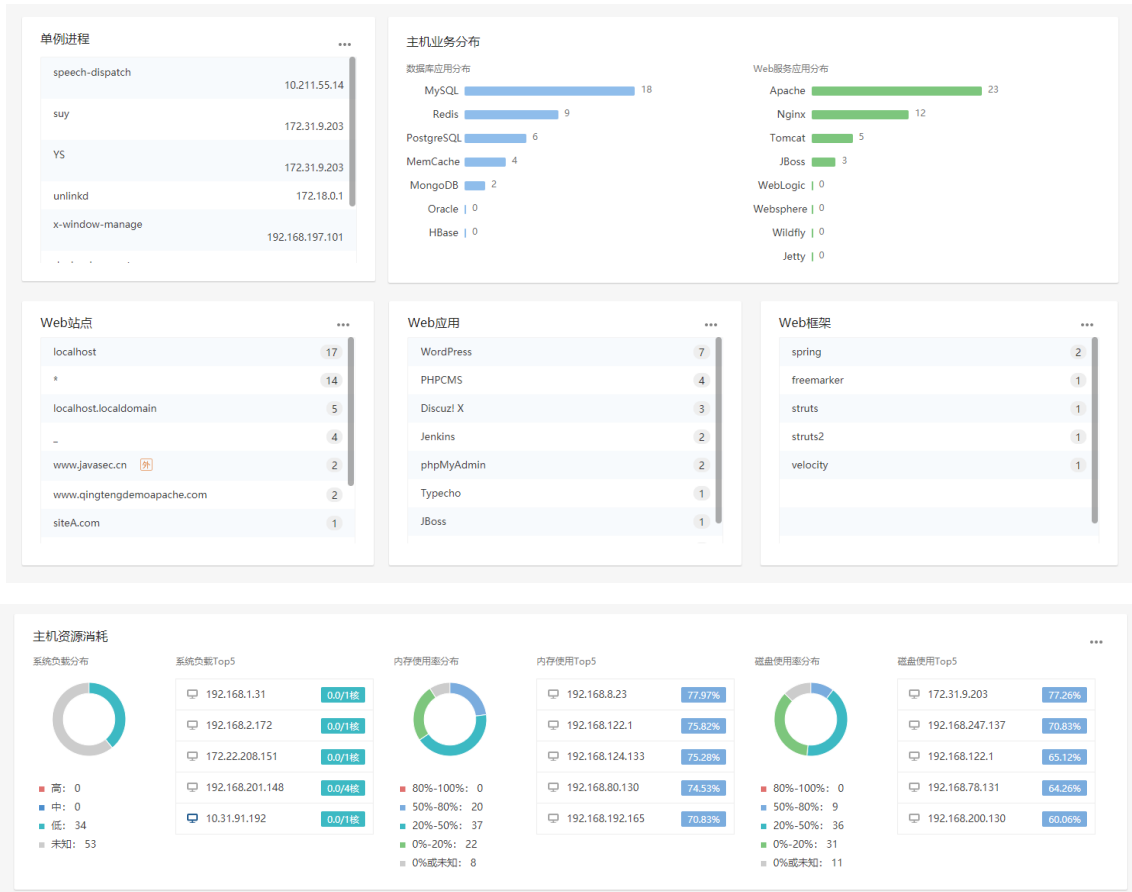
资产清点（Asset Inventory），致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产精准识别和动态感知，让保护对象清晰可见。使用 Agent-Server 架构，提供 10 余类主机关键资产清点，800 余类业务应用自动识别，并拥有良好的扩展能力。

资产清点功能，有两种查询视图：概览视图、分级视图。

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；


分级视图

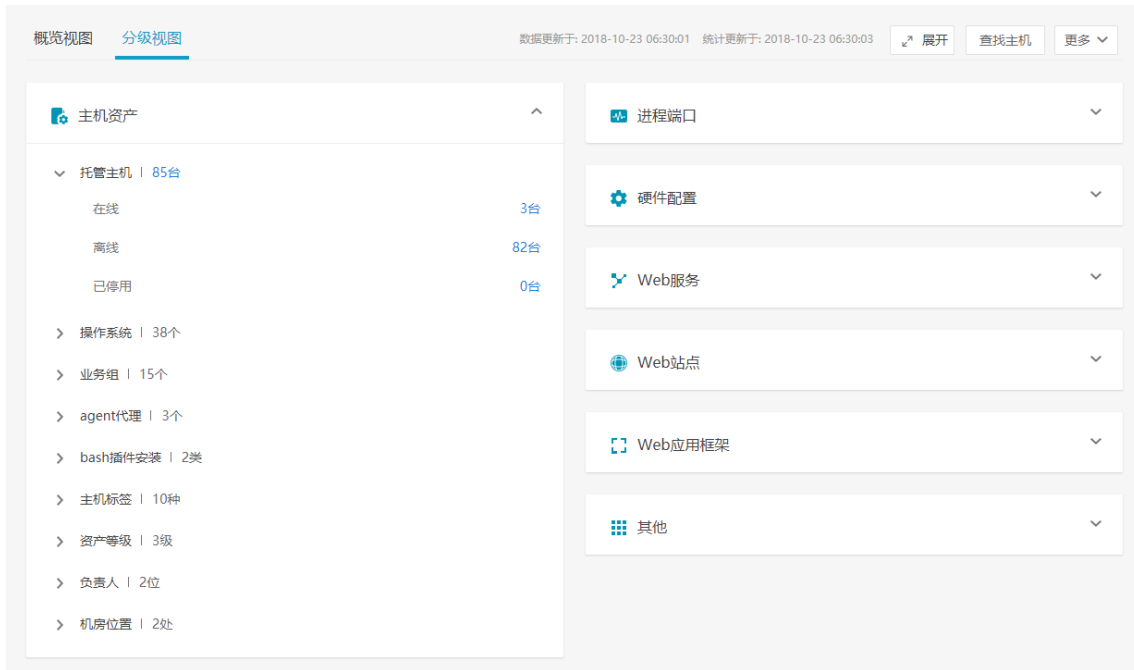
分级视图，是一种系统化的资产查询视图，通过系统化地分类，展示资产的统计情况，帮助用户快速了解资产总体信息；同时，作为分级视图详情的入口，以结构化的方式，有效地引导用户进行索引查询。



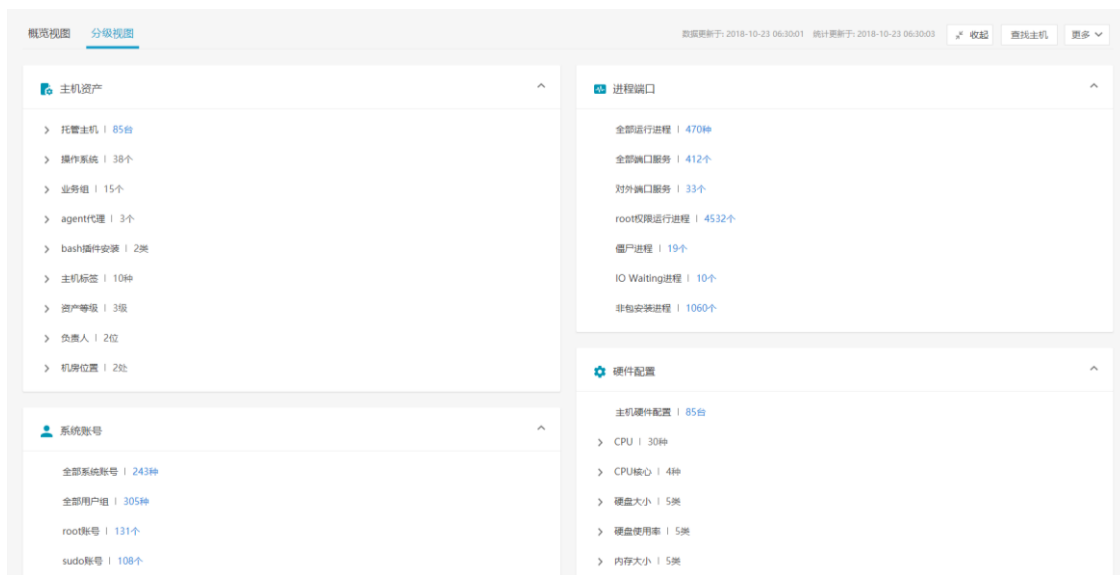
共有 12 个功能模块，分别为：

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；

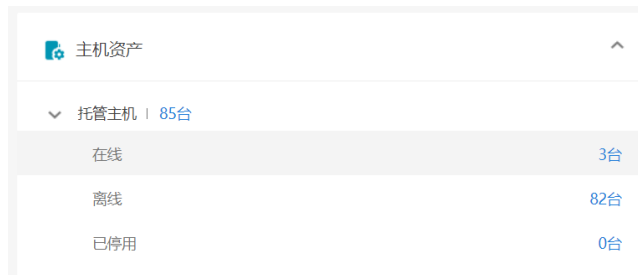
通过点击模块及折叠按钮 ，可展开查看具体资产统计信息；




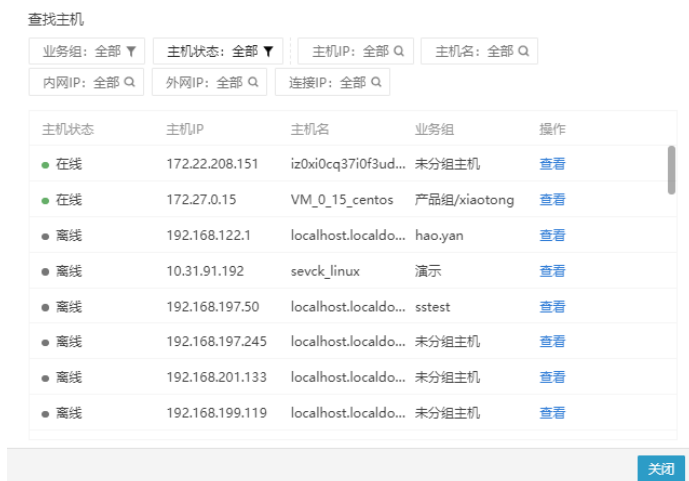
点击展开  按钮，可以将全部模块的内容展开。



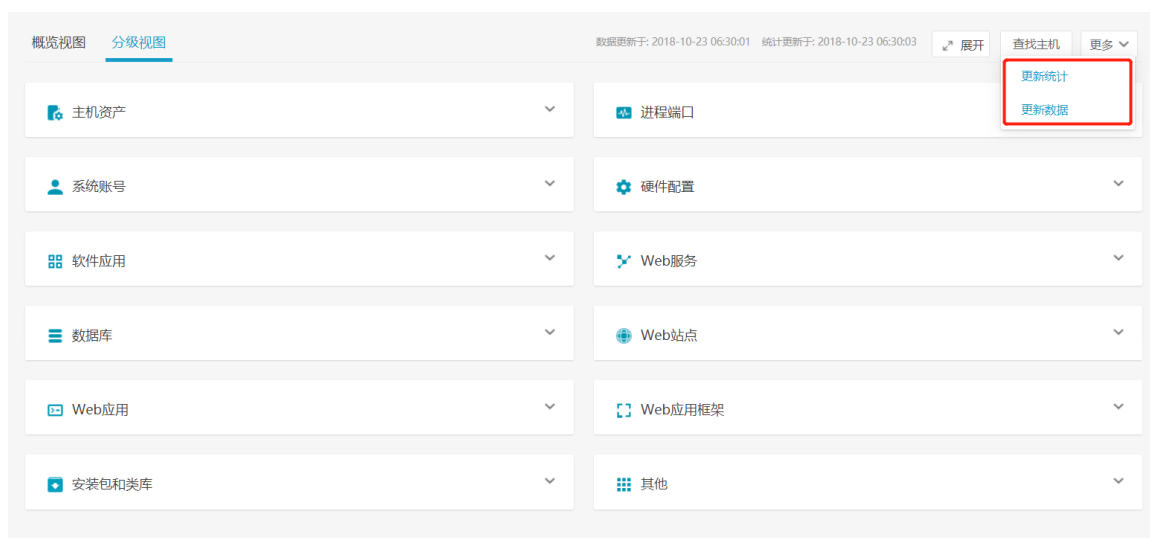
点击模块统计数值，即可跳转到对应的“资产详情页面”，查看所有主机中该资产的详细信息。



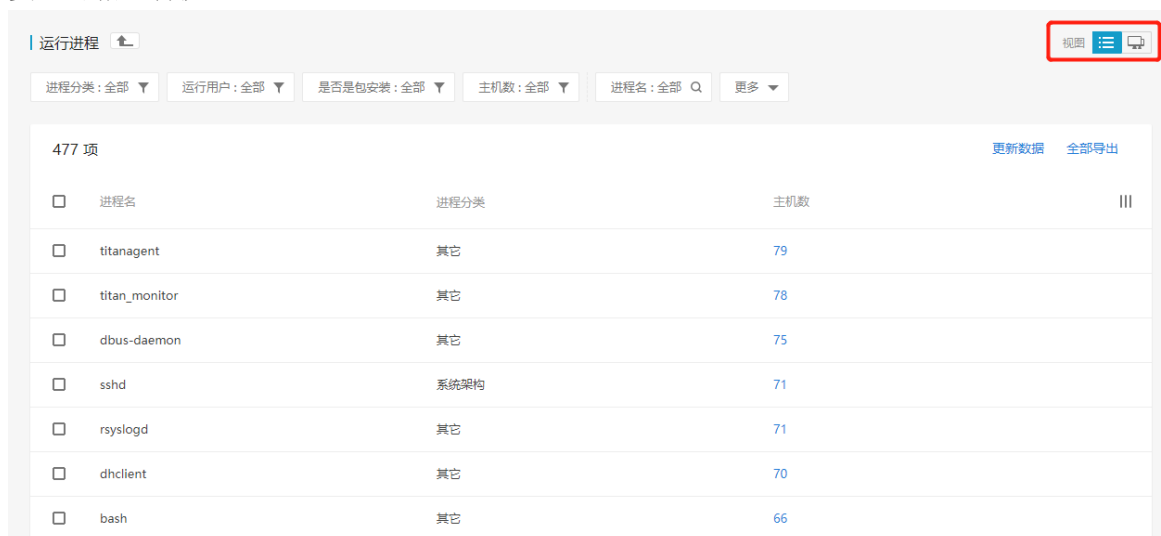
如想仅查看某个主机的资产情况，可以点击“查找主机”  按钮，筛选出该主机后“查看”。



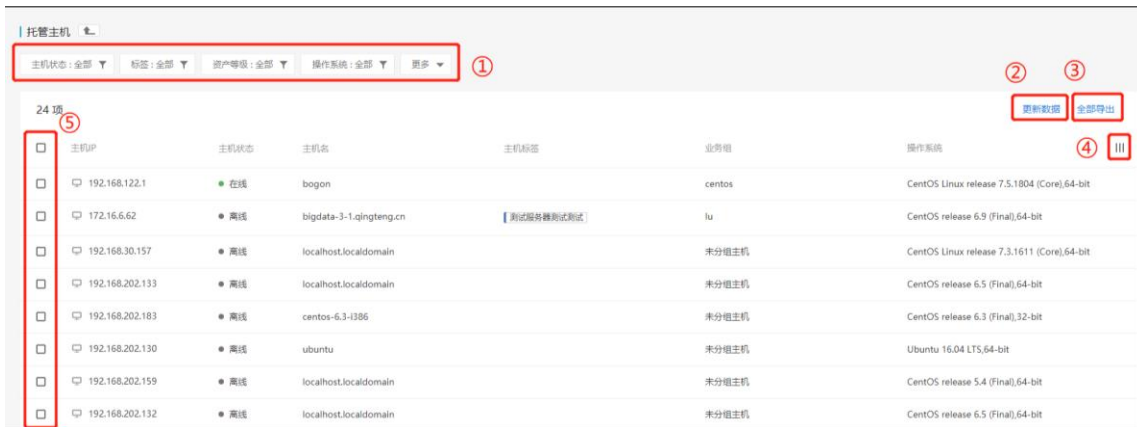
所有主机中的资产信息，每天自动更新一次，如果想获取最新信息，可以点击更多 [更多](#) ”更新数据”按钮，手动触发更新；对于功能中的统计数据，也可以手动触发”更新统计”。



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。



- ① 筛选/搜索区：根据不同需要，对列表内容进行筛选；
- ② 更新数据按钮：点击 [更新数据](#)，手动触发更新当前资产数据；
- ③ 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；
- ④ 设置显示列按钮：点击 [设置显示列](#)，通过勾选列名，控制列表中信息的显示/隐藏；
- ⑤ 复选框按钮：点击复选框，可选中该行数据，进行“导出”等操作；

3.1.1 主机资产

分级视图中“托管主机”为主机资产的查询入口，点击可查看所有主机相关信息；



主机详细信息，如下：

托管主机

业务组: 全部 Agent代理: 全部 标签: 全部 资产等级: 全部 主机名: 全部 更多

85 项 [更新数据](#) [全部导出](#)

主机IP	主机状态	主机名	主机标签	业务组	操作系统
172.22.208.151	● 在线	iz0xi0cq37i0f3udnr94dlz	[Web] [数据库] [XXXT] [XXXZ] [XXXXX3] [XXXXD5]	未分组主机	CentOS Linux release 7.3.1611 (Cor...
172.27.0.15	● 在线	VM_0_15_centos		产品组/xiaotong	CentOS Linux release 7.2.1511 (Cor...
192.168.122.1	● 离线	localhost.localdomain	[Web]	hao,yan	CentOS Linux release 7.2.1511 (Cor...
10.31.91.192	● 离线	sevck_linux	[数据库] [Web]	演示	CentOS release 6.9 (Final),64-bit
192.168.197.50	● 离线	localhost.localdomain		sstest	CentOS release 6.5 (Final),64-bit
192.168.197.245	● 离线	localhost.localdomain	[Web]	未分组主机	CentOS release 6.6 (Final),64-bit
192.168.201.133	● 离线	localhost.localdomain		未分组主机	CentOS release 6.6 (Final),64-bit
192.168.199.119	● 离线	localhost.localdomain		未分组主机	Red Hat Enterprise Linux Server rel...
192.168.199.151	● 离线	localhost.localdomain		未分组主机	Oracle Linux Server release 5.8,64-bit

同时，提供了 9 种维度的统计，可分别看到不同类别的主机数量；

包括：主机状态、操作系统、业务组、agent 代理、bash 插件安装、主机标签、资产等级、负责人、机房位置。

3.1.1.1 托管主机

查询主机中 Agent 的不同状态：

托管主机 | 87台

在线	5台
离线	82台
已停用	0台

3.1.1.2 操作系统

查询所有安装 Agent 主机的操作系统：

操作系统 | 38个

未设置	2台
CentOS release 6.9 (Final)	8台
CentOS release 6.5 (Final)	7台
CentOS Linux release 7.4.1708 (Core)	6台
CentOS release 6.4 (Final)	6台
Amazon Linux AMI release 2017.03	5台
Ubuntu 14.04.5 LTS	5台
CentOS Linux release 7.3.1611 (Core)	4台
CentOS Linux release 7.5.1804 (Core)	4台
CentOS Linux release 7.2.1511 (Core)	4台

[展开全部](#)

3.1.1.3 业务组

查询所有安装 agent 主机的业务组：

业务组 15个	
未分组主机	57台
李旭	5台
hao.yan	4台
产品组/zhiwei/异常登录测试实例	3台
产品组/test-cy	3台
蜜罐主机组	3台
aws 云主机	2台
产品组	2台
演示	2台
产品组/xiaotong	1台
展开全部	

3.1.1.4 Agent 代理

查询所有代理主机的 IP;

agent代理 3个	
直连主机	85台
192.168.248.143	1台
192.168.248.145	1台

3.1.1.5 bash 插件安装

查询所有安装 agent 主机的 bash 插件安装状态;

bash插件安装 2类	
已安装	19台
未安装	67台

3.1.1.6 主机标签

筛选显示所有安装 agent 主机的主机标签;

主机标签 10种	
Web	17台
数据库	4台
user case	3台
测试用例	3台
XXX1	2台
XXX2	2台
XXXX3	1台
XXXXD5	1台
xxxx4	0台
xxxx6	0台

3.1.1.7 资产等级

查询所有安装 agent 主机的资产等级;

资产等级 3级	
核心资产	3台
重要资产	0台
普通资产	84台

3.1.1.8 负责人

查询所有安装 agent 主机的负责人；

负责人 3位	
未设置	3台
张三	50台
李四	34台

3.1.1.9 机房位置

查询所有安装 agent 主机的机房位置；

机房位置 3处	
未设置	3台
武汉	50台
北京	34台

3.1.2 进程端口

分级视图中”进程端口”模块提供了进程、端口相关信息的查询；

进程端口	
全部运行进程 474种	
全部端口服务 445个	
对外端口服务 33个	
root权限运行进程 4605个	
僵尸进程 19个	
IO Waiting进程 11个	
非包安装进程 1098个	

3.1.2.1 全部运行进程

通过资产视图/主机视图两种方式，查看所有安装 Agent 主机的进程运行情况，进程详细信息，如下：

资产视角

运行进程 ↑ 视图 ☰ 🔍

进程分类: 全部 ▼ 运行用户: 全部 ▼ 是否是包安装: 全部 ▼ 主机数: 全部 ▼ 进程名: 全部 Q 更多 ▼

470 项 更新数据 全部导出

进程名	进程分类	主机数
<input type="checkbox"/> titanagent	其它	78
<input type="checkbox"/> titan_monitor	其它	77
<input type="checkbox"/> dbus-daemon	其它	74
<input type="checkbox"/> dhclient	--	70
<input type="checkbox"/> sshd	系统架构	70
<input type="checkbox"/> rsyslogd	其它	70

进程 titanagent 详细信息 ↑

进程版本: 全部 ▼ 是否是包安装: 全部 ▼ 运行用户: 全部 ▼ 进程状态: 全部 ▼ 主机IP: 全部 Q 更多 ▼

79 项 全部导出

主机IP	进程状态	进程版本	进程路径	是否是包安装	PID	运行用户	MD5
<input type="checkbox"/> 10.31.91.192	S	3.1.7-3.45.1-Rel...	/titan/agent/tit...	否	17867	root	1117738d88b2f268f84f3...
<input type="checkbox"/> 192.168.199.77	S	3.0.0a23-3.10.0...	/titan/agent/tit...	否	4847	root	095a86eedaf34a2c3a28e...
<input type="checkbox"/> 172.27.0.15	S	3.2.0-3.49.1-Rel...	/titan/agent/tit...	否	23128	root	99f948cf3629222451faa...
<input type="checkbox"/> 172.31.4.28	S	3.0.0b4-3.14.0-...	/titan/agent/tit...	否	26699	ec2-user	9b4f3372b062971d70f85...
<input type="checkbox"/> 10.211.55.10	S	3.1.10-3.48.0-R...	/titan/agent/tit...	否	17238	root	af2049e662763a743568b...

主机视角

主机运行进程 ↑ 视图 ☰ 🔍

运行用户: 全部 ▼ 是否是包安装: 全部 ▼ 进程状态: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 更多 ▼

78 项 更新数据 全部导出

主机IP	进程数
<input type="checkbox"/> 192.168.8.23	182
<input type="checkbox"/> 172.31.9.203	160
<input type="checkbox"/> 192.168.197.101	148
<input type="checkbox"/> 172.18.0.1	141
<input type="checkbox"/> 10.211.55.8	140

主机192.168.8.23进程详细信息 ↑

是否是包安装: 全部 ▼ 运行用户: 全部 ▼ 进程状态: 全部 ▼ PID: 全部 Q PPID: 全部 Q 更多 ▼

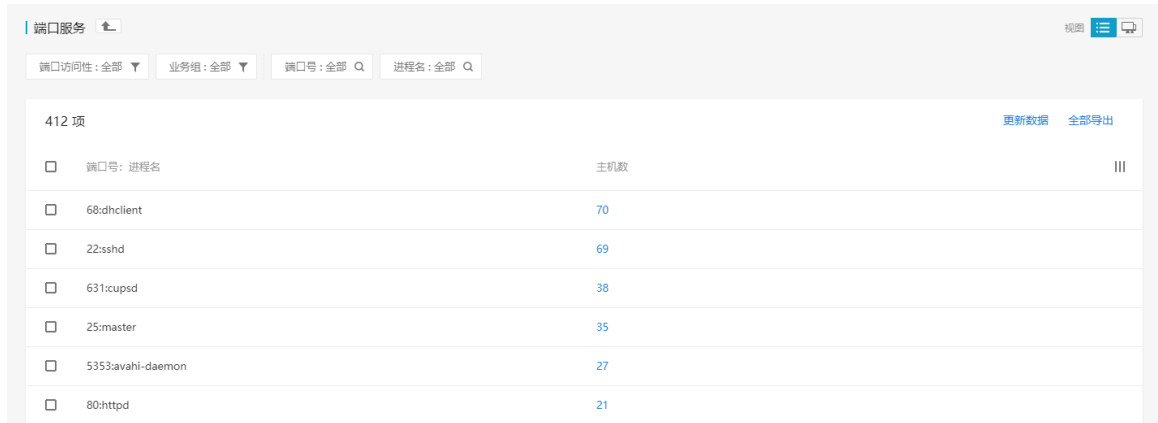
182 项 全部导出

进程名	进程分类	进程状态	进程版本	进程路径	是否是包安装	PID	运行用户
<input type="checkbox"/> gdm-session-wor	--	S	3.14.1-7	/usr/lib/gdm3/g...	是	63331	root
<input type="checkbox"/> gdm-session-wor	--	S	3.14.1-7	/usr/lib/gdm3/g...	是	63237	root
<input type="checkbox"/> gdm-session-wor	--	S	3.14.1-7	/usr/lib/gdm3/g...	是	59738	root
<input type="checkbox"/> ssh	--	S	--	/usr/local/bin/ssh	否	59737	root
<input type="checkbox"/> gdm-session-wor	--	S	3.14.1-7	/usr/lib/gdm3/g...	是	59706	root

3.1.2.2 全部端口服务

可以查看所有安装 agent 主机所开启端口的情况，点击进入详情后可以查看到端口号、端口访问性、绑定 IP，协议和监听进程（PID）。端口详细信息，如下：

端口视角

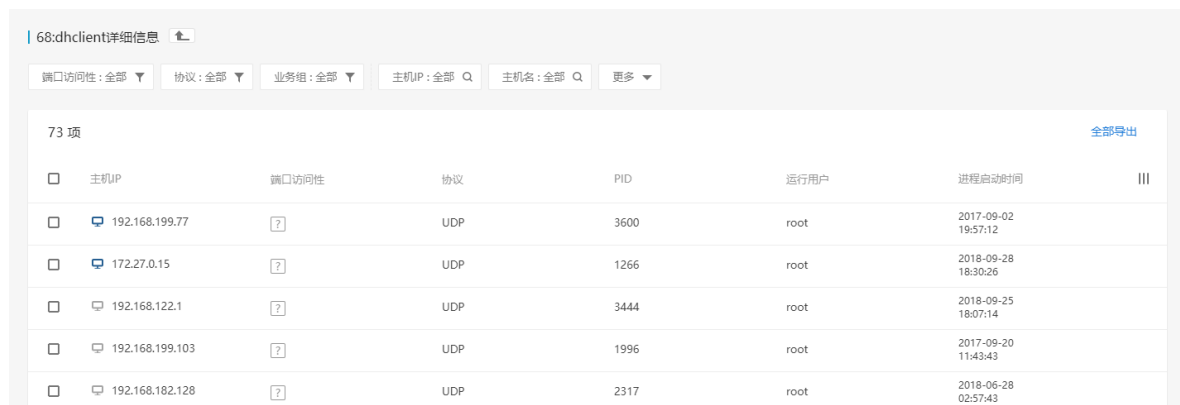


端口服务

端口访问性: 全部 | 业务组: 全部 | 端口号: 全部 | 进程名: 全部

412 项 更新数据 全部导出

端口号: 进程名	主机数
68:dhclient	70
22:sshd	69
631:cupsd	38
25:master	35
5353:avahi-daemon	27
80:httd	21



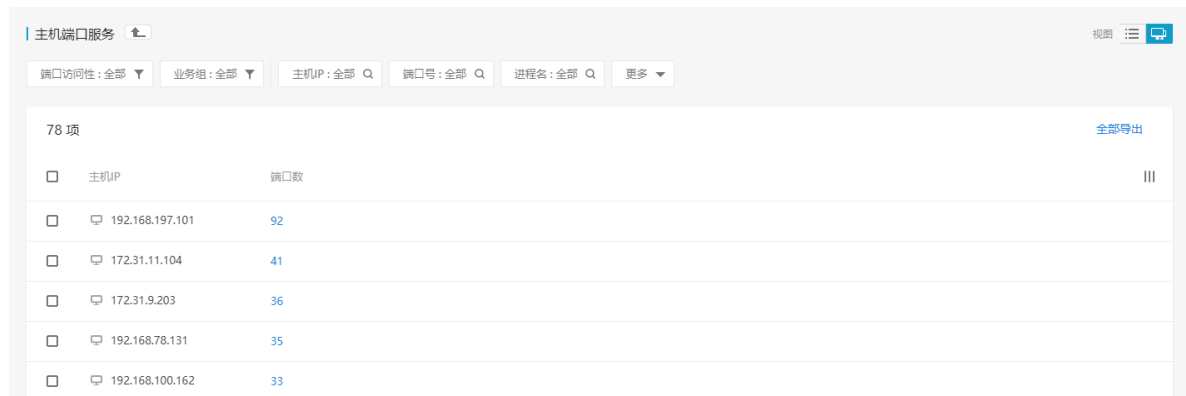
68:dhclient 详细信息

端口访问性: 全部 | 协议: 全部 | 业务组: 全部 | 主机IP: 全部 | 主机名: 全部 | 更多

73 项 全部导出

主机IP	端口访问性	协议	PID	运行用户	进程启动时间
192.168.199.77	?	UDP	3600	root	2017-09-02 19:57:12
172.27.0.15	?	UDP	1266	root	2018-09-28 18:30:26
192.168.122.1	?	UDP	3444	root	2018-09-25 18:07:14
192.168.199.103	?	UDP	1996	root	2017-09-20 11:43:43
192.168.182.128	?	UDP	2317	root	2018-06-28 02:57:43

主机视角



主机端口服务

端口访问性: 全部 | 业务组: 全部 | 主机IP: 全部 | 端口号: 全部 | 进程名: 全部 | 更多

78 项 全部导出

主机IP	端口数
192.168.197.101	92
172.31.11.104	41
172.31.9.203	36
192.168.78.131	35
192.168.100.162	33

主机192.168.197.101端口服务详细信息

端口访问性: 全部 | 协议: 全部 | PID: 全部

92 项 [全部导出](#)

<input type="checkbox"/>	端口号: 进程名	端口访问性	绑定IP	协议	PID	运行用户	进程启动时间	
<input type="checkbox"/>	22:sshd	[?]	::	TCP	15062	taibai	2017-08-22 02:29:40	
<input type="checkbox"/>	22:sshd	[?]	0.0.0.0	TCP	15062	taibai	2017-08-22 02:29:40	
<input type="checkbox"/>	53:named	[因]	192.168.197.101	TCP	15402	bind	2017-10-09 00:11:51	
<input type="checkbox"/>	53:named	[因]	127.0.0.1	TCP	15402	bind	2017-10-09 00:11:51	

3.1.2.3 对外端口服务

可以查询到所有可对外访问的端口。

端口服务

外网可访问 X | 业务组: 全部 | 端口号: 全部 | 进程名: 全部

47 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	端口号: 进程名	主机数	
<input type="checkbox"/>	22:sshd	22	
<input type="checkbox"/>	80:httpd	4	
<input type="checkbox"/>	23:xinetd	3	
<input type="checkbox"/>	111:rpcbind	3	
<input type="checkbox"/>	9300:java	2	
<input type="checkbox"/>	6666:shadowsocks-ser	2	

3.1.2.4 Root 权限运行进程

筛选显示所有以 root 权限运行的进程

运行进程

进程分类: 全部 | root X | 是否是包安装: 全部 | 主机数: 全部 | 进程名: 全部 | 更多

367 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	进程名	进程分类	主机数	
<input type="checkbox"/>	titanagent	其它	73	
<input type="checkbox"/>	titan_monitor	其它	72	
<input type="checkbox"/>	dhclient	--	66	
<input type="checkbox"/>	sshd	系统架构	65	

3.1.2.5 僵尸进程

筛选显示所有安装 agent 的主机存在的僵尸进程。

用户与IO Waiting进程

进程版本: 全部 | 是否是包安装: 全部 | 运行用户: 全部 | Z X | 主机IP: 全部 | 更多

主机IP	进程名	进程分类	进程状态	进程版本	进程路径	是否是包安装	PID	运行用户	进程启动时间
172.31.3.33	login	其它	Z	--	/proc/13954/exe	否	13954	root	2017-08-23 12:44:53
172.31.0.27	login	--	Z	--	/proc/14178/exe	否	14178	root	2017-11-15 13:14:48
172.31.6.36	login	其它	Z	--	/proc/9779/exe	否	9779	root	2017-08-31 13:35:13
172.31.11.104	login	--	Z	--	/proc/12121/exe	否	12121	root	2017-11-30 04:43:27
172.31.0.27	login	--	Z	--	/proc/14230/exe	否	14230	root	2017-11-15 13:15:21
172.31.4.28	login	--	Z	--	/proc/11958/exe	否	11958	ec2-user	2017-09-22 20:45:01
172.31.11.104	login	--	Z	--	/proc/19435/exe	否	19435	root	2017-11-30 05:24:40

3.1.2.6 IO Waiting 进程

筛选显示所有安装 agent 的主机存在的 IO Waiting 进程。

用户与IO Waiting进程

进程版本: 全部 | 是否是包安装: 全部 | 运行用户: 全部 | D X | 主机IP: 全部 | 主机名: 全部 | 更多

主机IP	进程名	进程分类	进程状态	进程版本	进程路径	是否是包安装	PID	运行用户	进程启动时间
172.31.4.28	in.telnetd	--	D	--	/proc/1389/exe	否	1389	ec2-user	2017-10-17 10:12:40
172.31.4.28	login	--	D	2.23.2	/bin/login	是	1412	ec2-user	2017-10-17 10:12:41
172.31.4.28	in.telnetd	--	D	--	/proc/7618/exe	否	7618	ec2-user	2017-09-26 02:23:27
172.31.4.28	login	--	D	2.23.2	/bin/login	是	7729	ec2-user	2017-09-26 02:23:28
172.31.4.28	in.telnetd	--	D	--	/proc/9530/exe	否	9530	ec2-user	2017-09-26 01:33:59
172.31.4.28	login	--	D	2.23.2	/bin/login	是	9719	ec2-user	2017-09-26 01:34:00

3.1.2.7 非包安装进程

非包安装进程指的是不是通过包管理器来安装的应用对应进程。

运行进程

进程分类: 全部 | 运行用户: 全部 | 否 X | 主机数: 全部 | 业务组: 全部 | 进程名: 全部 | 更新数据 | 全部导出

进程名	进程分类	主机数
titanagent	其它	77
titan_monitor	其它	76
vmtoolsd	--	30
vmware-vmblock-	其它	23
VGAuthService	其它	22

3.1.3 系统账号

在分类导航中，“系统账号”模块包含了所有账号、用户组的相关信息，提供 9 种维度的统计，可分别看到对应类别的账号数量，包括：Root 权限账号、sudo 权限账号、交互登录账号、启用账号、过期账号、密码锁定账号、账号公钥 Key。

系统账号

- 全部系统账号 | 243种
- 全部用户组 | 305种
- root账号 | 135个
- sudo账号 | 111个
- 交互登录账号 | 189个
- 启用账号 | 271个
- 过期账号 | 2个
- 密码锁定账号 | 6个
- 账号公钥Key | 40种

3.1.3.1 全部系统账号

通过资产视图/主机视图两种方式，查看所有主机中的账号信息，如下：

资产视角

账号名	主机数
root	78
lp	78
mail	78
daemon	77
games	77
bin	77

主机IP	账号状态	root权限	登录方式	sudo权限	Home目录	shell	最后登录	密码状态	密码修改时间	操作
192.168.199.77	启用	是	不可登录	否	/root	/bin/bash	2017-09-02 ...	正常	--	查看详情
172.27.0.15	启用	是	只允许key登录	是	/root	/bin/bash	2018-10-22 ...	正常	2018-08-27 08:00:00	查看详情
10.31.91.192	启用	是	key和密码	是	/root	/bin/bash	2018-08-09 ...	正常	2016-05-18 08:00:00	查看详情
172.31.3.33	启用	是	不可登录	是	/root	/bin/bash	2017-08-23 ...	正常	--	查看详情
192.168.248.145	启用	是	只允许密码登录	是	/root	/bin/bash	2017-10-24 ...	正常	2017-05-24 08:00:00	查看详情

主机视角

主机账号

视图

最后登录时间: 全部 ▼ 账号状态: 全部 ▼ root权限: 全部 ▼ 登录方式: 全部 ▼ 更多 ▼

80 项 全部导出

<input type="checkbox"/>	主机IP	账号数	最后登录	操作
<input type="checkbox"/>	192.168.122.1	67	qingteng 2017-11-13 16:53:35 :0 pts/0	
<input type="checkbox"/>	192.168.192.165	65	root 2018-08-03 23:48:20 192.168.198.111 pts/28	
<input type="checkbox"/>	192.168.197.101	64	root 2017-11-18 02:45:15 192.168.197.89 pts/14	
<input type="checkbox"/>	192.168.8.23	62	root 2017-11-09 18:21:06 :0 pts/2	
<input type="checkbox"/>	192.168.100.162	61	root 2017-10-27 11:32:56 192.168.197.25 pts/2	
<input type="checkbox"/>	10.211.55.8	56	root 2018-08-29 21:57:25 :0 pts/3	
<input type="checkbox"/>	192.168.122.1	49	root 2017-09-14 15:28:16 192.168.201.1 pts/3	
<input type="checkbox"/>	172.18.0.1	48	ca 2018-09-29 18:49:02 :0 pts/0	

主机192.168.122.1账号详细信息

最后登录时间: 全部 ▼ 账号状态: 全部 ▼ root权限: 全部 ▼ 登录方式: 全部 ▼ GID: 全部 Q 更多 ▼

67 项 全部导出

<input type="checkbox"/>	账号名	UID	GID	账号状态	root权限	登录方式	Home目录	shell	操作	操作
<input type="checkbox"/>	userlock	0	1004	禁用	是	不可登录	/home/user...	/bin/bash	查看详情	
<input type="checkbox"/>	root	0	0	启用	是	只允许密码登录	/root	/bin/bash	查看详情	
<input type="checkbox"/>	qingteng	0	0	启用	是	只允许密码登录	/home/qingt...	/bin/bash	查看详情	
<input type="checkbox"/>	weakuser1	0	1008	启用	是	只允许密码登录	/home/weak...	/bin/bash	查看详情	
<input type="checkbox"/>	bin	1	1	禁用	否	不可登录	/bin	/sbin/nologin	查看详情	
<input type="checkbox"/>	daemon	2	2	禁用	否	不可登录	/sbin	/sbin/nologin	查看详情	
<input type="checkbox"/>	adm	3	4	禁用	否	不可登录	/var/adm	/sbin/nologin	查看详情	

3.1.3.2 全部用户组

用户组

视图

业务组: 全部 ▼ 用户组: 全部 Q

305 项 更新数据

<input type="checkbox"/>	用户组	主机数	操作
<input type="checkbox"/>	audio	78	
<input type="checkbox"/>	disk	78	
<input type="checkbox"/>	utmp	78	
<input type="checkbox"/>	tty	78	
<input type="checkbox"/>	lp	78	
<input type="checkbox"/>	daemon	78	

用户组audio详细信息

业务组: 全部 | GID: 全部 | 主机IP: 全部 | 主机名: 全部

78 项			
<input type="checkbox"/>	主机IP	GID	包含账号
<input type="checkbox"/>	172.27.0.15	63	--
<input type="checkbox"/>	10.31.91.192	63	--
<input type="checkbox"/>	192.168.199.77	63	gdm
<input type="checkbox"/>	192.168.248.141	63	--
<input type="checkbox"/>	192.168.197.102	29	pulse, speech-dispatcher

3.1.3.3 Root 账号

账号

账号状态: 全部 | Root权限: X | 登录方式: 全部 | sudo权限: 全部 | 更多

34 项		更新数据	全部导出
<input type="checkbox"/>	账号名	主机数	
<input type="checkbox"/>	root	78	
<input type="checkbox"/>	qt	4	
<input type="checkbox"/>	test	4	
<input type="checkbox"/>	userroot	4	
<input type="checkbox"/>	usersudo	4	
<input type="checkbox"/>	ec2-user	3	
<input type="checkbox"/>	zhiwei	2	

3.1.3.4 sudo 账号

账号

账号状态: 全部 | root权限: 全部 | 登录方式: 全部 | Sudo权限: X | 更多

24 项		更新数据	全部导出
<input type="checkbox"/>	账号名	主机数	
<input type="checkbox"/>	root	74	
<input type="checkbox"/>	qt	4	
<input type="checkbox"/>	userroot	4	
<input type="checkbox"/>	usersudo	4	
<input type="checkbox"/>	zhiwei	2	
<input type="checkbox"/>	user	2	

3.1.3.5 交互登录账号

账号

账号状态: 全部 root权限: 全部 登录方式: 全部 sudo权限: 全部 账号名: 全部 更多

可交互登录 X

65 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	账号名	主机数	
<input type="checkbox"/>	root	47	
<input type="checkbox"/>	test	14	
<input type="checkbox"/>	qt	7	
<input type="checkbox"/>	weblogic	6	
<input type="checkbox"/>	admin	5	
<input type="checkbox"/>	taibai	5	
<input type="checkbox"/>	user	5	
<input type="checkbox"/>	weakuser1	4	
<input type="checkbox"/>	ec2-user	4	

3.1.3.6 启用账号

账号

启用 X root权限: 全部 登录方式: 全部 sudo权限: 全部 账号名: 全部 更多

87 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	账号名	主机数	
<input type="checkbox"/>	root	77	
<input type="checkbox"/>	test	19	
<input type="checkbox"/>	admin	8	
<input type="checkbox"/>	qt	7	
<input type="checkbox"/>	weblogic	6	
<input type="checkbox"/>	taibai	6	
<input type="checkbox"/>	user	6	
<input type="checkbox"/>	guest	6	
<input type="checkbox"/>	usersudo	5	

3.1.3.7 过期账号

过期与密码锁定账号

密码修改时间: 全部 密码到期时间: 全部 密码锁定时间: 全部 最后登录时间: 全部 主机IP: 全部 更多

已过期 X

2 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	账号名	账号状态	最后登录时间	密码状态	密码修改时间	密码到期时间	密码锁定时间	操作	
<input type="checkbox"/>	10.211.55.14	limily	启用	2018-04-19 20:33:47	已过期	2018-04-19 08:00:00	2018-04-20 08:00:00	--	查看详情	
<input type="checkbox"/>	192.168.122.1	oldboy2	启用	--	已过期	2016-11-23 08:00:00	2016-11-24 08:00:00	--	查看详情	

3.1.3.8 密码锁定账号

过期与密码锁定账号

密码修改时间: 全部 | 密码到期时间: 全部 | 密码锁定时间: 全部 | 最后登录时间: 全部 | 主机IP: 全部 | 更多

已锁定 X

6 项 更新数据 全部导出

主机IP	账号名	账号状态	最后登录时间	密码状态	密码修改时间	密码到期时间	密码锁定时间	操作
192.168.247.137	oldboy	启用	--	已锁定	2017-04-24 08:00:00	2291-02-06 08:00:00	--	查看详情
192.168.247.134	oldboy	启用	--	已锁定	2017-04-24 08:00:00	2291-02-06 08:00:00	--	查看详情
192.168.247.137	oldboy	禁用	--	已锁定	2017-04-24 08:00:00	2291-02-06 08:00:00	--	查看详情
192.168.122.1	oldboy	启用	--	已锁定	2016-11-23 08:00:00	2290-09-07 08:00:00	--	查看详情
172.27.0.15	sunxt	禁用	--	已锁定	2018-08-01 08:00:00	2021-04-27 08:00:00	--	查看详情
192.168.106.129	oldboy	启用	--	已锁定	2017-10-10 08:00:00	2017-10-11 08:00:00	--	查看详情

3.1.3.9 账号公钥 Key

账号key使用情况

加密类型: 全部 | 业务组: 全部

40 项 更新数据

公钥值	公钥备注	加密类型	使用账号数
ort-forw... lu.shen		RSA1	6
AAAAB3Nz...D+4RKbAZ	taibaiyifeng@outlook.com	ssh-rsa	4
AAAAB3Nz...mf8LWw==	guanpeng@qt	ssh-rsa	3
AAAAB3Nz...sqLB0w==	ms@qt	ssh-rsa	3
AAAAB3Nz...BedGGQ==	root@localhost.localdomain	ssh-rsa	3

3.1.4 硬件配置

在分类导航中，“主机硬件配置”为硬件信息的查询入口，点击可查看所有主机 CPU、磁盘、内存等相关信息；



硬件详细信息，如下：

硬件配置

内存大小: 全部 | 硬盘大小: 全部 | 内存使用率: 全部 | 硬盘使用率: 全部 | 更多

86 项 更新数据 全部导出

主机IP	主机状态	CPU信息	系统负载	内存使用率	硬盘使用率	分区数	操作
172.22.208.151	● 在线	GenuineIntel ...	低	1839 MB 22....	40.00 GB 16....	1	查看详情
172.18.0.1	● 在线	GenuineIntel ...	低	3772 MB 43....	30.00 GB 35....	3	查看详情
10.211.55.10	● 在线	GenuineIntel ...	低	985 MB 58.3...	64.00 GB 11....	9	查看详情
192.168.192.165	● 在线	GenuineIntel ...	低	1440 MB 64....	30.00 GB 0.0...	0	查看详情
10.211.55.14	● 在线	GenuineIntel ...	低	1835 MB 76....	64.00 GB 30....	17	查看详情
192.168.122.1	● 离线	GenuineIntel ...	未知	985 MB 65.1...	138.47 GB 9....	8	查看详情

分类导航中提供 7 种维度的统计，可分别看到对应配置的主机数量；

包括：CPU、CPU 核心、硬盘大小、硬盘使用率、内存大小、内存使用率、系统负载。

3.1.4.1 CPU

查询主机中 Agent 的不同状态；

CPU | 30种

GenuineIntel 1 Intel(R) Core(TM) i3-3110M CPU @ 2.40GHz	2台
GenuineIntel 1 Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz	2台
GenuineIntel 1 Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz	2台
GenuineIntel 1 Intel(R) Core(TM) i5-4200U CPU @ 1.60GHz	1台
GenuineIntel 1 Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz	3台
GenuineIntel 1 Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz	6台
GenuineIntel 1 Intel(R) Core(TM) i5-4670 CPU @ 3.40GHz	3台
GenuineIntel 1 Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz	7台
GenuineIntel 1 Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz	4台
GenuineIntel 1 Intel(R) Core(TM) i5-6300HQ CPU @ 2.30GHz	1台

[展开全部](#)

3.1.4.2 CPU 核心

CPU核心 | 4种

1核	59台
2核	13台
4核	6台
未知	8台

3.1.4.3 硬盘大小

硬盘大小 | 5类

0-40GB	59台
40GB-100GB	14台
100GB-1TB	3台
1TB以上	0台
0或未知	10台

3.1.4.4 硬盘使用率

▼ 硬盘使用率 5类	
80-100%	0台
50-80%	9台
20-50%	36台
0-20%	30台
0%或未知	11台

3.1.4.5 内存大小

▼ 内存大小 5类	
0-4GB	76台
4GB-32GB	2台
32GB-128GB	0台
128GB以上	0台
0或未知	8台

3.1.4.6 内存使用率

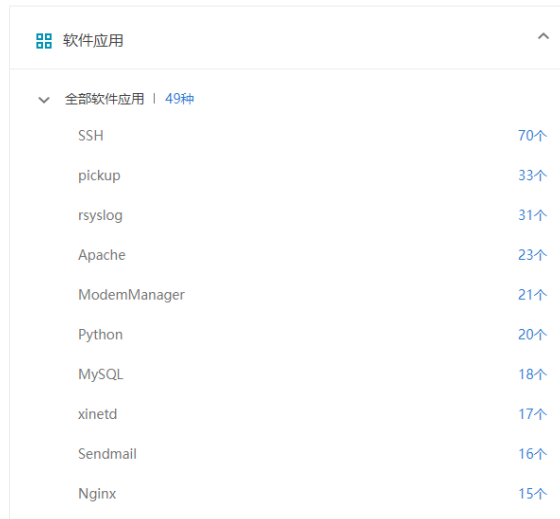
▼ 内存使用率 5类	
80-100%	0台
50-80%	20台
20-50%	37台
0-20%	21台
0%或未知	8台

3.1.4.7 系统负载

▼ 系统负载 4类	
高	0台
中	0台
低	33台
未知	53台

3.1.5 软件应用

分级视图中，软件应用模块清点所有安装 Agent 的主机上运行着的应用。



目前支持的应用类型，如下表：

gzip	NTP	Asterisk	wrapper
klogd	Saltstack	HAProxy	ElasticSearch
syslogd	Tomcat	chrony	Grafana
wget	Jenkins	cgrulesengd	salt-minion
SOCKS	Git	Hadoop-HDFS	slave
Mesos slave	Zabbix	Python	gunicorn
Mesos	xinetd	ModemManager	MongoDB
Auditd	Nessus	bounce	Sendmail
Logger	Apache2	Hadoop-YARN	Nginx
Zabbix Agent	JRuby	hpssd.py	SFTP
FFmpeg	getty	RabbitMQ	rsync
WebSphere	Telnet	Bluetoothd	DNSmasq
Kudu	falcon	Redis-cli	Redis
Libvirt	Logstash	Python2.6	FASTDFS
rsyslog	MySQL	Spark	SSH
GoAhead	Nagios	Bind	beam.smp
Jetty	Heka	Splunk	MooseFS
system	gam_server	kingshard	WebLogic
ActiveMQ	Zimbra	Memcache	PostgreSQL
VNC-SERVER	Java	minerd	Sqoop
VNC-VIRTUAL	Docker	RocketMQ	bbserver
OpenLDAP	Dubbo	PPTP	vsftpd
snmpd	smbd	supervisor	influxDB
Wildfly	Kafka	qemu-kvm	OpenVPN
Python2.7	SVN	ZooKeeper	screen
Jboss	Storm	apt-get	PHP
ProFTPD	Python3	pickup	codis
Oracle	Exim	Ruby	NFS
CVS	hpiod	xfs	Hadoop-HBase
Squid	PHP-FPM	inet_gethost	Apache

3.1.5.1 全部软件应用

可从两种视角，查看有哪些应用分布在主机中，以及某主机中有哪些应用。
资产视角

软件应用 ↑ 视图 ☰ 🗨️

应用类别: 全部 ▼ 业务组: 全部 ▼ 应用名: 全部 🔍

49 项 更新数据 全部导出

<input type="checkbox"/>	应用名	应用类别	主机数	☰
<input type="checkbox"/>	SSH	系统架构	70	
<input type="checkbox"/>	pickup	其它	33	
<input type="checkbox"/>	rsyslog	系统应用	31	
<input type="checkbox"/>	Apache	Web运维	23	
<input type="checkbox"/>	ModemManager	其它	21	
<input type="checkbox"/>	Python	其它	20	
<input type="checkbox"/>	MySQL	数据库	18	
<input type="checkbox"/>	xinetd	其它	17	
<input type="checkbox"/>	Sendmail	系统应用	16	

应用SSH详细信息 ↑

版本号: 全部 ▼ 业务组: 全部 ▼ 二进制路径: 全部 🔍 配置文件路径: 全部 🔍 更多 ▼

75 项 全部导出

<input type="checkbox"/>	主机IP	应用名	版本号	启动用户	二进制路径	配置文件路径	关联进程数	☰
<input type="checkbox"/>	🗨️ 10.10.10.13	SSH	5.3p1	root	/usr/sbin/sshd	/etc/ssh/sshd_...	1	
<input type="checkbox"/>	🗨️ 10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd		1	
<input type="checkbox"/>	🗨️ 10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd	/etc/ssh/sshd_...	1	
<input type="checkbox"/>	🗨️ 10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd		1	
<input type="checkbox"/>	🗨️ 10.31.91.192	SSH	5.3p1	root	/usr/sbin/sshd	/etc/ssh/sshd_...	1	

主机视角

主机软件应用 ↑ 视图 ☰ 🗨️

应用类别: 全部 ▼ 业务组: 全部 ▼ 应用名: 全部 🔍 主机IP: 全部 🔍 更多 ▼

78 项 更新数据 全部导出

<input type="checkbox"/>	主机IP	应用数	☰
<input type="checkbox"/>	🗨️ 192.168.192.165	26	
<input type="checkbox"/>	🗨️ 192.168.197.101	21	
<input type="checkbox"/>	🗨️ 192.168.78.131	13	
<input type="checkbox"/>	🗨️ 10.31.91.192	12	
<input type="checkbox"/>	🗨️ 172.31.11.104	12	

主机192.168.192.165 应用详细信息

应用类别: 全部 | 版本号: 全部 | 二进制路径: 全部 | 配置文件路径: 全部

26 项 全部导出

<input type="checkbox"/>	应用名	应用类别	版本号	启动用户	二进制路径	配置文件路径	关联进程数	
<input type="checkbox"/>	rsyslog	系统应用	7.4.4-1ubuntu2.6	syslog	/usr/sbin/rsyslogd		1	
<input type="checkbox"/>	Bluetoothd	其它	4.101-0ubuntu1...	root	/usr/sbin/blueto...		1	
<input type="checkbox"/>	Bind	系统应用	1:9.9.5.dfsg-3ub...	bind	/usr/sbin/named		1	
<input type="checkbox"/>	Memcache	数据库	1.4.14-0ubuntu9.1	memcache	/usr/bin/memca...		1	
<input type="checkbox"/>	PPTP	系统应用	1.3.4+27+gddb3...	root	/usr/sbin/pptpd		1	

3.1.6 Web 服务

在分类导航中，“Web 服务”模块用于清点安装 Agent 主机中存在的 Web 服务器，及各类型服务器的版本分布情况。



支持清点的 Web 服务器类型，包括：

Apache、Nginx、Tomcat、Weblogic、JBoss、Wildfly、Jetty、WebSphere。

3.1.6.1 全部 web 服务

显示所有安装 agent 的主机上的 web 服务。

资产视角

Web 服务 ↑ 视图 ☰ 🖨

Web 服务名: 全部 ▼ 版本: 全部 ▼ 启动用户: 全部 ▼ 业务组: 全部 ▼ 更多 ▼

40 项 更新数据 全部导出

<input type="checkbox"/>	主机IP	Web 服务名	版本	启动用户	二进制路径	配置文件路径	关联进程数	☰
<input type="checkbox"/>	🖨 10.31.91.192	Apache	2.2.15	apache	/usr/sbin/httpd	/etc/httpd/co...	21	
<input type="checkbox"/>	🖨 10.211.55.8	Apache	2.4.6	apache	/usr/sbin/httpd	/etc/httpd/co...	8	
<input type="checkbox"/>	🖨 172.16.6.142	Tomcat	8.0.24	root	/usr/local/jav...	/usr/local/to...	1	
<input type="checkbox"/>	🖨 172.16.6.142	Nginx	1.10.2	root	/usr/sbin/nginx	/etc/nginx/ng...	11	
<input type="checkbox"/>	🖨 172.17.43.79	Nginx	1.10.3	nginx	/usr/local/ngi...	/usr/local/ngi...	2	
<input type="checkbox"/>	🖨 172.18.0.2	Nginx	1.10.2	nginx	/usr/sbin/nginx	/etc/nginx/ng...	2	
<input type="checkbox"/>	🖨 172.22.208.151	Apache	2.4.6	apache	/usr/sbin/httpd	/etc/httpd/co...	9	

主机视角

主机Web 服务 ↑ 视图 ☰ 🖨

Web 服务名: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 🔍 主机名: 全部 🔍

33 项 全部导出

<input type="checkbox"/>	主机IP	Web 服务数	☰
<input type="checkbox"/>	🖨 192.168.192.165	3	
<input type="checkbox"/>	🖨 172.16.6.142	2	
<input type="checkbox"/>	🖨 172.31.0.27	2	
<input type="checkbox"/>	🖨 192.168.197.101	2	

主机10.31.91.192上httpd服务关联的进程 ↑

运行用户: 全部 ▼ 进程启动时间: 全部 ▼ 进程版本: 全部 ▼ PID: 全部 🔍 更多 ▼

21 项 ☰

<input type="checkbox"/>	PID	进程路径	运行用户	进程启动时间	☰
<input type="checkbox"/>	356	/usr/sbin/httpd	apache	2018-08-03 08:05:55	
<input type="checkbox"/>	1768	/usr/sbin/httpd	apache	2018-08-09 09:29:12	
<input type="checkbox"/>	6577	/usr/sbin/httpd	apache	2018-08-08 07:53:58	
<input type="checkbox"/>	6586	/usr/sbin/httpd	apache	2018-08-08 07:53:59	
<input type="checkbox"/>	6587	/usr/sbin/httpd	apache	2018-08-08 07:53:59	

3.1.6.2 Apache

▼ Apache | 6种

2.2.15	9个
2.4.6	5个
2.2.34	4个
2.4.7	2个
2.2.32	1个
未知版本	2个

Web 服务  视图  

Apache X 版本: 全部 ▼ 启动用户: 全部 ▼ 业务组: 全部 ▼ 更多 ▼




23 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	Web服务名	版本	启动用户	二进制路径	配置文件路径	关联进程数	
<input type="checkbox"/>	 10.31.91.192	Apache	2.2.15	apache	/usr/sbin/httpd	/etc/httpd/con...	21	
<input type="checkbox"/>	 172.22.208.151	Apache	2.4.6	root	/usr/sbin/httpd	/etc/httpd/con...	9	
<input type="checkbox"/>	 172.27.0.15	Apache	2.4.6	apache	/usr/sbin/httpd		11	
<input type="checkbox"/>	 172.31.0.27	Apache	2.2.34	root	/usr/sbin/httpd	/etc/httpd/con...	11	

3.1.6.3 Nginx






▼ Nginx | 8种

1.10.2	3个
1.4.6	2个
1.12.0	1个
1.10.3	1个
1.7.9	1个
1.12.1	1个
1.12.2	1个
未知版本	1个

Web 服务  视图  

Nginx X 版本: 全部 ▼ 启动用户: 全部 ▼ 业务组: 全部 ▼ 更多 ▼

11 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	Web服务名	版本	启动用户	二进制路径	配置文件路径	关联进程数	
<input type="checkbox"/>	 172.16.6.142	Nginx	1.10.2	root	/usr/sbin/nginx	/etc/nginx/nginx...	11	
<input type="checkbox"/>	 172.17.43.79	Nginx	1.10.3	nginx	/usr/local/nginx...	/usr/local/nginx...	2	
<input type="checkbox"/>	 172.18.0.2	Nginx	1.10.2	nginx	/usr/sbin/nginx	/etc/nginx/nginx...	2	
<input type="checkbox"/>	 172.27.0.15	Nginx	1.12.2	nginx	/usr/sbin/nginx	/etc/nginx/nginx...	2	
<input type="checkbox"/>	 172.31.11.176	Nginx	1.12.1	nginx	/usr/sbin/nginx	/etc/nginx/nginx...	2	

3.1.6.4 Tomcat

▼ Tomcat | 5种

5.5.36	1个
8.0.24	1个
8.0.46	1个
7.0.57	1个
未知版本	1个

Web 服务

Tomcat X 版本: 全部 启动用户: 全部 业务组: 全部 更多

5 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	Web服务名	版本	启动用户	二进制路径	配置文件路径	关联进程数	III
<input type="checkbox"/>	172.16.6.142	Tomcat	8.0.24	root	/usr/local/java/j...	/usr/local/tomc...	1	
<input type="checkbox"/>	192.168.182.128	Tomcat					0	
<input type="checkbox"/>	192.168.192.165	Tomcat	5.5.36	root	/usr/lib/jvm/jdk...	/root/apache-t...	1	
<input type="checkbox"/>	192.168.201.133	Tomcat	8.0.46	root	/usr/java/jdk1.8...	/usr/local/tomc...	1	
<input type="checkbox"/>	192.168.247.137	Tomcat	7.0.57	root	/usr/local/java/j...	/usr/local/tomc...	1	

3.1.6.5 JBoss

▼ JBoss | 2种

4.2.3.GA	2个
未知版本	1个

Web 服务

JBoss X 版本: 全部 启动用户: 全部 业务组: 全部 更多

3 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	Web服务名	版本	启动用户	二进制路径	配置文件路径	关联进程数	III
<input type="checkbox"/>	172.31.0.27	JBoss					0	
<input type="checkbox"/>	172.31.9.203	JBoss	4.2.3.GA	root	/usr/lib/jvm/jav...		1	
<input type="checkbox"/>	172.31.11.104	JBoss	4.2.3.GA	root	/usr/lib/jvm/jav...		1	

3.1.6.6 Weblogic

同上;

3.1.6.7 Wildfly

同上;

3.1.6.8 Jetty

同上;

3.1.6.9 WebSphere

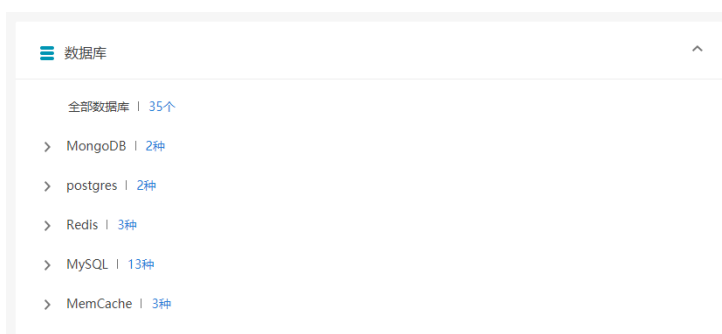
同上；

3.1.6.10 IHS



3.1.7 数据库

在分类导航中，“数据库”模块用于清点安装 Agent 主机中存在的数据库，及各类型数据库的版本分布情况。



支持清点的数据库类型，包括：

MySQL、Redis、Oracle、MongoDB、Memcache、Postgres、HBase。

3.1.7.1 全部数据库

查询所有安装 agent 主机中的数据库，及具体数据库详情。

资产视角

数据库

数据库名: 全部 | 版本: 全部 | 运行用户: 全部 | 端口访问性: 全部 | 配置文件路径: 全部 | 日志文件路径: 全部 | 更多

35 项

主机IP	数据库名	版本	监听端口	运行用户	配置文件路径	日志文件路径	操作
192.168.248.145	mysql		3306	mysql	/etc/my.cnf		查看详情
192.168.248.145	mysql		3306	mysql	/etc/my.cnf		查看详情
192.168.247.137	mysql	5.1.73	3306	mysql	/etc/my.cnf		查看详情
192.168.247.134	mysql	5.1.73	3306	mysql	/etc/my.cnf		查看详情
192.168.201.133	memcache	1.4.13	11211	root			查看详情
192.168.197.101	redis	2.8.4	6379	redis	/etc/redis/redis.conf	/var/log/redis/redis-s...	查看详情

主机视角

主机数据库

运行用户: 全部 | 业务组: 全部 | 主机ip: 全部 | 主机名: 全部

26 项

主机IP	数据库数
192.168.197.101	5
192.168.192.165	5
192.168.8.23	3
10.31.91.192	2

主机192.168.197.101数据库详细信息

数据库名: 全部 | 版本: 全部 | 运行用户: 全部 | 配置文件路径: 全部 | 日志文件路径: 全部 | 更多

5 项

数据库名	版本	监听端口	运行用户	配置文件路径	日志文件路径	操作
redis	2.8.4	6379	redis	/etc/redis/redis.conf	/var/log/redis/redis...	查看详情
postgres	1.1-2ubuntu2	15432	postgres-xc		/	查看详情
postgres	1.1-2ubuntu2	15433	postgres-xc		/	查看详情
mongod	3.0.15	27017	mongodb	/etc/mongod.conf	/var/log/mongodb...	查看详情
memcache	1.4.14-0ubuntu9.1	11211	memcache			查看详情

3.1.7.2 MySQL

MySQL | 12种

5.1.73	4个
5.6.34	1个
5.5.54	1个
10.1.22-MariaDB	1个
5.5.56	1个
5.5.55	1个
5.6.16	1个
5.6.14	1个
5.5.48-log	1个
5.5.52-0+deb7u1	1个

[展开全部](#)

MySQL数据库

视图

端口访问性: 全部 | 版本: 全部 | 运行用户: 全部 | 业务组: 全部 | 主机ip: 全部 | 更多

18 项 更新数据

主机IP	数据库类型	版本	监听端口	运行用户	配置文件路径	日志文件路径	操作
192.168.248.145	mysql	--	3306	mysql	/etc/my.cnf		查看详情
192.168.248.145	mysql	--	3306	mysql	/etc/my.cnf		查看详情
192.168.247.137	mysql	5.1.73	3306	mysql	/etc/my.cnf		查看详情
192.168.247.134	mysql	5.1.73	3306	mysql	/etc/my.cnf		查看详情
192.168.197.55	mysql	5.6.16	3306	mysql	/etc/my.cnf	/var/lib/mysql/...	查看详情

3.1.7.3 Redis

Redis | 4种

2.8.3	6个
2:2.8.4-2	1个
2.8.4	1个
2:2.8.17-1+deb8u1	1个

Redis数据库

视图

端口访问性: 全部 | 版本: 全部 | 运行用户: 全部 | 业务组: 全部 | 主机ip: 全部 | 更多

9 项 更新数据

主机IP	数据库类型	版本	监听端口	运行用户	配置文件路径	日志文件路径	操作
192.168.197.101	redis	2.8.4	6379	redis	/etc/redis/redis...	/var/log/redis/r...	查看详情
192.168.192.165	redis	2:2.8.4-2	6379	redis			查看详情
192.168.8.23	redis	2:2.8.17-1+deb...	0	redis			查看详情
172.31.11.104	redis	2.8.3	6379	root			查看详情

3.1.7.4 MongoDB

MongoDB | 2种

2.7.0	1个
3.0.15	1个

MongoDB数据库

视图

端口访问性: 全部 | 版本: 全部 | 运行用户: 全部 | 是否开放REST接口: 全部 | 主机ip: 全部 | 主机名: 全部 | 更多

2 项 更新数据

主机IP	数据库类型	版本	监听端口	运行用户	配置文件路径	日志文件路径	是否开放REST接口	是否开放Web接口	安全认证	操作
192.168.197.101	mongod	3.0.15	27017	mongodb	/etc/mongod...	/var/log/mon...	false	false	disabled	查看详情
10.31.91.192	mongod	2.7.0	27017	root	/usr/local/mo...	/usr/local/mo...	false	false	enabled	查看详情

3.1.7.5 Memcache

MemCache | 3种

1.4.14-0ubuntu9.1	2个
1.4.21-1.1	1个
1.4.13	1个

MemCache数据库

视图

端口访问性: 全部 版本: 全部 运行用户: 全部 业务组: 全部 主机ip: 全部 更多

4 项 更新数据

主机IP	数据库类型	版本	监听端口	运行用户	日志文件路径	操作
192.168.201.133	memcache	1.4.13	11211	root		查看详情
192.168.197.101	memcache	1.4.14-0ubuntu9.1	11211	memcache		查看详情
192.168.192.165	memcache	1.4.14-0ubuntu9.1	11211	memcache		查看详情
192.168.8.23	memcache	1.4.21-1.1	11211	memcache		查看详情

3.1.7.6 Postgres

postgres | 2种

- 1.1-2ubuntu2 5个
- 8.4.20 1个

postgres数据库

视图

端口访问性: 全部 版本: 全部 运行用户: 全部 业务组: 全部 主机ip: 全部 主机名: 全部 更多

6 项 更新数据

主机IP	数据库类型	版本	监听端口	运行用户	配置文件路径	日志文件路径	pg_hba文件路径	操作
192.168.197.101	postgres	1.1-2ubuntu2	15432	postgres-xc		/		查看详情
192.168.197.101	postgres	1.1-2ubuntu2	15433	postgres-xc		/		查看详情
192.168.192.165	postgres	1.1-2ubuntu2	15432	postgres-xc	/var/lib/postgr...	/var/lib/postgr...	/etc/postgres-x...	查看详情
192.168.192.165	postgres	1.1-2ubuntu2	15433	postgres-xc	/var/lib/postgr...	/var/lib/postgr...	/etc/postgres-x...	查看详情
192.168.192.165	postgres	1.1-2ubuntu2	5432	postgres-xc	/var/lib/postgr...	/var/lib/postgr...	/etc/postgres-x...	查看详情
192.168.91.130	postgres	8.4.20	5432	postgres	/var/lib/pgsql/...	/var/lib/pgsql/...	/var/lib/pgsql/...	查看详情

3.1.7.7 Oracle

同上;

3.1.7.8 HBase

同上;

3.1.8 Web 站点

在分类导航中，“Web 站点”模块用于清点安装 Agent 主机中存在的站点详细信息。

Web 站点

- 全部站点域名 | 33个
- 站点服务类型 | 4种
 - 对外站点 | 7个
 - root权限运行站点 | 22个
 - 目录为777权限站点 | 1个

支持清点的 Web 站点的，服务器类型包括：

Apache、Nginx、Tomcat、Weblogic、JBoss、Wildfly、Jetty、WebSphere。

3.1.8.1 全部站点域名

Web 站点

服务类型: 全部 | 端口访问性: 全部 | 运行用户: 全部 | 所有者权限: 全部 | 业务组: 全部

34 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	域名	站点标题	站点数	操作
<input type="checkbox"/>	localhost	Welcome to nginx!	15	
<input type="checkbox"/>	*		14	
<input type="checkbox"/>	localhost.localdomain	400 Bad Request	5	
<input type="checkbox"/>	_	Apache2 Ubuntu Default Page: It works	4	
<input type="checkbox"/>	www.javasec.cn	400 Bad Request	2	
<input type="checkbox"/>	www.qingtengdemoapache.com	Apache HTTP Server Test Page powered by CentOS	2	
<input type="checkbox"/>	www.manliinfo	Index of /	1	
<input type="checkbox"/>	siteA.com	502 Bad Gateway	1	

localhost 域名站点详细信息

服务类型: 全部 | 端口访问性: 全部 | 运行用户: 全部 | 所有者权限: 全部 | 端口: 全部 | 更多

16 项 [全部导出](#)

<input type="checkbox"/>	主机IP	服务类型	站点端口	端口访问性	协议	运行用户	主目录	主目录所有者	拥有者权限	操作
<input type="checkbox"/>	<input type="checkbox"/> 192.168.247.137	Tomcat	8080	未知	HTTP	root	/usr/local/to...	root	rwXr-xr-x	查看详情
<input type="checkbox"/>	<input type="checkbox"/> 192.168.219.131	Nginx	8888	未知	HTTP	nginx			--	查看详情
<input type="checkbox"/>	<input type="checkbox"/> 192.168.201.133	Tomcat	8080	未知	HTTP	root	/usr/local/to...	root	rwXr-xr-x	查看详情
<input type="checkbox"/>	<input type="checkbox"/> 192.168.197.245	Nginx	80	未知	HTTP	www			--	查看详情
<input type="checkbox"/>	<input type="checkbox"/> 192.168.197.101	Apache	802	未知	HTTP	www-data			--	查看详情

3.1.8.2 web 服务类型



已有的 Web 服务类型分类显示，可以筛选显示对应的 Web 服务。

站点服务类型 | 4种

Nginx	32个
Apache	29个
Tomcat	5个
JBoss	2个

3.1.8.3 对外站点

筛选显示外网可访问的 web 站点

Web 站点 ↑ 视图  



服务类型: 全部 ▼ 外网可访问 ✕ 运行用户: 全部 ▼ 所有者权限: 全部 ▼ 业务组: 全部 ▼

5 项 更新数据 全部导出

<input type="checkbox"/>	域名	站点标题	站点数	⋮
<input type="checkbox"/>	www.javasec.cn	400 Bad Request	2	
<input type="checkbox"/>	*		2	
<input type="checkbox"/>	www.example.com	Apache HTTP Server Test Page powered by...	1	
<input type="checkbox"/>	www.qingtengdemoapache.com	Apache HTTP Server Test Page powered by...	1	
<input type="checkbox"/>	website80.com		1	

3.1.8.4 root 权限运行站点

筛选显示以 root 权限运行的站点

Web 站点 ↑ 视图  



服务类型: 全部 ▼ 端口访问性: 全部 ▼ root ✕ 所有者权限: 全部 ▼ 更多 ▼

17 项 更新数据 全部导出

<input type="checkbox"/>	域名	站点标题	站点数	⋮
<input type="checkbox"/>	localhost	Apache Tomcat/8.5.8	7	
<input type="checkbox"/>	*		2	
<input type="checkbox"/>	tim-wordpress.com	404 Not Found	1	

3.1.8.5 目录为 777 权限站点

筛选显示目录为 777 权限的站点

Web 站点 ↑ 视图  

服务类型: 全部 ▼ 端口访问性: 全部 ▼ 运行用户: 全部 ▼ rwxrwxrwx ✕ 更多 ▼

1 项 更新数据 全部导出

<input type="checkbox"/>	域名	站点标题	站点数	⋮
<input type="checkbox"/>	admin.php.com	timlong	1	

3.1.9 Web 应用

在分类导航中，“Web 应用”模块用于清点安装 Agent 主机中存在的 Web 应用信息。

Web应用	
全部Web应用 8种	
WordPress	9个
PHPCMS	4个
Discuz! X	3个
Typecho	2个
Jenkins	2个
phpMyAdmin	2个
JBoss	1个
Joomla	1个

支持清点的 Web 应用，包括：

PHPMailer、wordpress、ThinkPHP、pan、BigTree、JPress、openwbs、jenkins、ZABBIX、Discuz!、ThinkCMF 等。

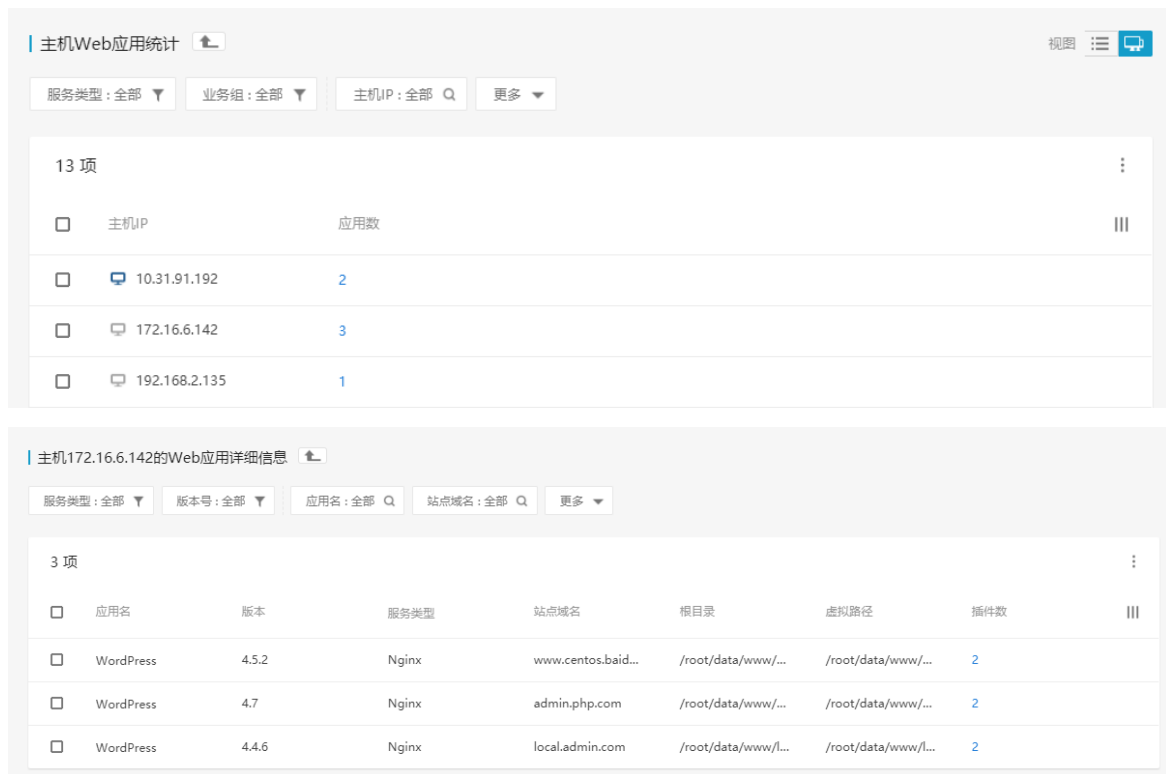
3.1.9.1 全部 Web 应用

对所有安装 agent 主机上的 Web 应用进行统计并显示资产视角

Web应用统计		视图
服务类型: 全部	业务组: 全部	应用名: 全部
8 项		更新数据
应用名	主机数	
WordPress	7	
PHPCMS	4	
Discuz! X	3	

WordPress详细信息							
服务类型: 全部	版本号: 全部	业务组: 全部	站点域名: 全部	更多			
9 项							
主机IP	版本	服务类型	站点域名	根目录	虚拟路径	插件数	
172.16.6.142	4.5.2	Nginx	www.centos.bai...	/root/data/ww...	/root/data/www...	2	
172.16.6.142	4.7	Nginx	admin.php.com	/root/data/ww...	/root/data/www...	2	
172.16.6.142	4.4.6	Nginx	local.admin.com	/root/data/ww...	/root/data/www...	2	
192.168.2.193	4.7.4	Nginx	localhost	/usr/share/nginx...	/usr/share/nginx...	2	

主机视角



3.1.10 Web 应用框架

在分类导航中，“Web 应用框架”模块用于清点安装 Agent 主机中存在的 Web 框架信息。



支持清点的 Web 框架类型，包括：

Java 语言框架：

Struts、struts2、spring、hibernate、webwork、quartz、velocity、tapestry、turbine、freemarker、flexive、stripes、vaadin、vertx、wicket、zkoss、jackson、fastjson、shiro、MyBatis、spring MVC、Jersey、JFinal；

PHP 语言框架：

Drupal、Phalcon、Webasyst、ThinkCMF、Laravel、KYPHP、CodeIgniter、BEedita、Yii、CakePHP、InitPHP、SpeedPHP、ThinkPHP、Cotonti、MODx、Typo3、CanPHP、OneThink、Agile Toolkit、CoreThink、CdvPHP、Flight、PHPixie

Python 语言框架：

Django、Flask、Tornado、web.py、web2py；

3.1.10.1 全部 web 应用框架

对所有安装 agent 的住进上的 web 应用框架进行统计并显示。

资产视角

Web应用框架统计

框架语言: 全部 业务组: 全部 框架名: 全部

26 项 [更新数据](#) [全部导出](#)

框架名	框架语言	主机数
ThinkPHP	php	2
vaadin	java	1
fastjson	java	1
vertx	java	1
shiro	java	1
zkoss	java	1
Freemarker	java	1
Jersey	java	1

fastjson框架详细信息

服务类型: 全部 业务组: 全部 版本: 全部 主机IP: 全部 主机名: 全部 更多

1 项 [全部导出](#)

主机IP	框架版本	服务类型	应用路径
192.168.220.133	1.2.44	JBoss	--

主机视角

主机Web应用框架统计

业务组: 全部 主机IP: 全部 主机名: 全部

3 项 [全部导出](#)

主机IP	框架数
192.168.220.133	23
192.168.220.137	4
192.168.220.128	2

主机192.168.220.133的Web应用框架详细信息

框架语言: 全部 | 版本: 全部 | 框架名: 全部 | 应用路径: 全部

23 项 [全部导出](#)

<input type="checkbox"/>	框架名	框架语言	框架版本	应用路径	
<input type="checkbox"/>	spring	java	2.5.6.SEC03,3.0.5.RELEASE,4.3.2.RELEASE,...	--	
<input type="checkbox"/>	Freemarker	java	2.3.13,2.3.26,2.3.19	--	
<input type="checkbox"/>	hibernate	java	3.3.1.GA,5.3.7.Final,3.6.6.Final	--	
<input type="checkbox"/>	turbine	java	2.3.1	--	
<input type="checkbox"/>	struts	java	1.3.10	--	
<input type="checkbox"/>	struts2	java	2.1.6,2.3.20.3,2.5.16	--	

3.1.10.2 Java 语言框架

统计 Java 语言编写的 Web 框架有哪些，及存在的数量情况，点击可查看详情。

资产视角

Java框架统计

业务组: 全部 | 框架名: 全部

23 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	框架名	主机数	
<input type="checkbox"/>	Freemarker	1	
<input type="checkbox"/>	vertx	1	
<input type="checkbox"/>	stripes	1	
<input type="checkbox"/>	jackson	1	
<input type="checkbox"/>	webwork	1	

Freemarker框架详细信息

服务类型: 全部 | 业务组: 全部 | 版本: 全部 | 主机IP: 全部 | 主机名: 全部

1 项 [全部导出](#)

<input type="checkbox"/>	主机IP	框架版本	服务类型	关联jar包数	
<input checked="" type="checkbox"/>	192.168.220.133	2.3.13,2.3.26,2.3.19	JBoss	4	

Freemarker框架详细信息

服务类型: 全部 | 业务组: 全部 | 版本: 全部 | 主机IP: 全部 | 主机名: 全部

1 项 [全部导出](#)

<input type="checkbox"/>	主机IP	框架版本	服务类型	关联jar包数	
<input checked="" type="checkbox"/>	192.168.220.133	2.3.13,2.3.26,2.3.19	JBoss	4	

框架Jar包信息

包名	绝对路径
freemarker-2.3.13.jar	/root/jboss-6.1.0.Final/server/default/tmp...
freemarker-2.3.26-incubat...	/root/jboss-6.1.0.Final/server/default/tmp...
freemarker-2.3.13.jar	/root/jboss-6.1.0.Final/server/default/tmp...
freemarker-2.3.19.jar	/root/jboss-6.1.0.Final/server/default/tmp...

[确定](#)

主机视角

主机Java语言框架

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

3 项 [全部导出](#)

<input type="checkbox"/>	主机IP	框架数	
<input type="checkbox"/>	• 192.168.220.130	23	
<input type="checkbox"/>	• 192.168.220.133	23	
<input type="checkbox"/>	• 192.168.220.137	1	

主机192.168.220.133的Java语言框架详细信息

服务类型: 全部 | 版本: 全部 | 框架名: 全部

23 项 [全部导出](#)

<input type="checkbox"/>	框架名	框架版本	服务类型	关联jar包数	
<input type="checkbox"/>	spring	2.5.6.SEC03,3.0.5.RELEASE,4.3.2.RELEASE...	JBoss	4	
<input type="checkbox"/>	Freemarker	2.3.13,2.3.26,2.3.19	JBoss	4	
<input type="checkbox"/>	hibernate	3.3.1.GA,5.3.7.Final,3.6.6.Final	JBoss	4	
<input type="checkbox"/>	turbine	2.3.1	JBoss	1	
<input type="checkbox"/>	struts	1.3.10	JBoss	1	

主机192.168.220.133的Java语言框架详细信息

服务类型: 全部 | 版本: 全部 | 框架名: 全部

23 项 [全部导出](#)

<input type="checkbox"/>	框架名	框架版本	服务类型	关联jar包数	
<input type="checkbox"/>	spring	2.5.6.SEC03,3.0.5.RELEASE,4.3.2.RELEASE...	JBoss	4	
<input type="checkbox"/>	Freemarker	2.3.13,2.3.26,2.3.19	JBoss	4	
<input type="checkbox"/>	hibernate	3.3.1.GA,5.3.7.Final,3.6.6.Final	JBoss	4	
<input type="checkbox"/>	turbine	2.3.1	JBoss	1	
<input type="checkbox"/>	struts	1.3.10	JBoss	1	
<input type="checkbox"/>	struts2		JBoss	4	
<input type="checkbox"/>	webwork		JBoss	1	

框架Jar包信息

包名	绝对路径
spring-core-2.5.6.SEC03.jar	/root/jboss-6.1.0.Final/server/default/tmp...
spring-core-3.0.5.RELEASE...	/root/jboss-6.1.0.Final/server/default/tmp...
spring-core-4.3.2.RELEASE...	/root/jboss-6.1.0.Final/server/default/tmp...
spring-core-2.5.6.jar	/root/jboss-6.1.0.Final/server/default/tmp...

确定

3.1.10.3 PHP 语言框架

统计 PHP 语言编写的 Web 框架有哪些，及存在的数量情况，点击可查看详情。

资产视角

PHP框架统计

业务组: 全部 框架名: 全部

3 项 [更新数据](#) [全部导出](#)

框架名	主机数
ThinkPHP	2
CdvPHP	1
CanPHP	1

ThinkPHP框架详细信息

服务类型: 全部 业务组: 全部 版本: 全部 主机IP: 全部 主机名: 全部 更多

4 项 [全部导出](#)

主机IP	框架版本	服务类型	根目录	应用路径
192.168.220.128	--	Apache	/usr/local/apache2/htdocs/	/usr/local/apache2/htdocs/thinkphp
192.168.220.137	--	Nginx	/var/www/html/	/var/www/html/thinkphp
192.168.220.128	5.0.22	Apache	/usr/local/apache2/htdocs/	/usr/local/apache2/htdocs
192.168.220.137	5.0.22	Nginx	/var/www/html/	/var/www/html

主机视角

主机PHP语言框架

业务组: 全部 主机IP: 全部 主机名: 全部

2 项 [全部导出](#)

主机IP	框架数
192.168.220.137	4
192.168.220.128	2

主机192.168.220.137的PHP语言框架详细信息

服务类型: 全部 版本: 全部 框架名: 全部 根目录: 全部 更多

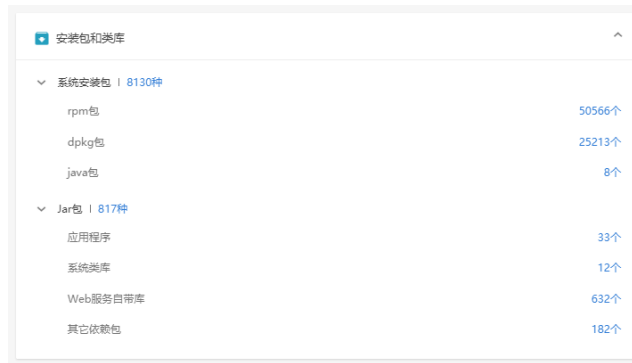
4 项 [全部导出](#)

框架名	框架版本	服务类型	根目录	应用路径
CdvPHP	4.0	Nginx	/var/www/html/	/var/www/html/cdvphp-master
CanPHP	3.0	Nginx	/var/www/html/	/var/www/html/canphp-master
ThinkPHP	--	Nginx	/var/www/html/	/var/www/html/thinkphp
ThinkPHP	5.0.22	Nginx	/var/www/html/	/var/www/html

3.1.10.4 Python 语言框架

3.1.11 安装包和类库

分级视图中“安装包和类库”模块，提供了系统安装包、Jar包相关信息的查询；



3.1.11.1 系统安装包

通过资产视图/主机视图两种方式，查看所有安装 Agent 主机中安装包的情况，安装包详细信息，如下：

资产视角

安装包统计

安装包类型: 全部 | 业务组: 全部 | 包名: 全部

8130 项 [刷新数据](#) [全部导出](#)

包名	主机数
sed	79
tzdata	79
findutils	79
gzip	79
tar	79
curl	79
iptables	79
logrotate	79

安装包sed统计

安装包类型: 全部 | 安装时间: 全部 | 业务组: 全部 | 主机IP: 全部 | 主机名: 全部

79 项 [全部导出](#)

主机IP	描述	版本	安装时间	安装包类型
192.168.19.133	The GNU sed stream editor	4.2.2-4ubuntu1	2018-08-31 19:29:18	dpkg包
192.168.2.135	A GNU stream text editor	4.2.2-5.el7	2018-08-09 20:20:59	rpm包
192.168.19.132	A GNU stream text editor	4.2.2-5.el7	2018-08-02 11:46:14	rpm包
192.168.122.1	A GNU stream text editor	4.2.2-5.el7	2018-07-30 20:24:47	rpm包
192.168.122.1	A GNU stream text editor	4.2.2-5.el7	2018-07-30 20:24:47	rpm包
192.168.247.160	A GNU stream text editor.	4.1.5-5.fc6	2018-07-12 23:51:50	rpm包

主机视角

安装包统计

视图

安装包类型: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 主机名: 全部 Q

80 项 全部导出

<input type="checkbox"/>	主机IP	安装包数	
<input type="checkbox"/>	192.168.8.23	3128	
<input type="checkbox"/>	192.168.199.221	2391	
<input type="checkbox"/>	192.168.192.165	2011	
<input type="checkbox"/>	192.168.197.101	1908	
<input type="checkbox"/>	192.168.248.129	1851	
<input type="checkbox"/>	192.168.32.136	1823	

主机192.168.8.23安装包统计

安装包类型: 全部 ▼ 安装时间: 全部 ▼ 包名: 全部 Q

3128 项 全部导出

<input type="checkbox"/>	包名	总述	版本	安装时间	安装包类型	
<input type="checkbox"/>	attr	Utilities for manipul...	1:2.4.47-2	--	dpkg包	
<input type="checkbox"/>	axel	light download accel...	2.4-1	--	dpkg包	
<input type="checkbox"/>	apt-utils	package manageme...	1.0.9.10+kali1~r2u1	--	dpkg包	
<input type="checkbox"/>	aspell-en	English dictionary fo...	7.1-0-1.1	--	dpkg包	
<input type="checkbox"/>	arduino	AVR development b...	2:1.0.5+dfsg2-4	--	dpkg包	
<input type="checkbox"/>	apktool	A tool for reverse en...	1.5.2-1kali1	--	dpkg包	
<input type="checkbox"/>	autopsy	graphical interface t...	2.24-1	--	dpkg包	

3.1.11.2 Jar 包

通过资产视图/主机视图两种方式，查看所有安装 Agent 主机中 Jar 包的情况，包详细信息，如下：

资产视角

Jar包统计

业务组: 全部 类型: 全部 包名: 全部

817 项 更新数据 全部导出

包名	主机数
resources	2
jsse.jar	2
localedata.jar	2
cldrdata.jar	2
jce.jar	2
sunec.jar	2
sunpkcs11.jar	2
rt.jar	2
sunjce_provider.jar	2
log4j-1.2-api-2.11.1.jar	1
netty-transport-4.1.16.Final.jar	1

查询类型: 应用程序, 系统类库, Web服务自带库, 其他依赖包

Jar包sunec.jar详细信息

类型: 全部 是否可执行: 全部 业务组: 全部 更多

4 项 全部导出

主机IP	类型	是否可执行	版本	绝对路径	操作
172.22.208.151	其他依赖包	否	1.8.0_151	/usr/local/clou...	查看详情
192.168.192.165	系统类库	否	1.7.0_09	/usr/lib/jvm/jd...	查看详情
192.168.200.130	其他依赖包	否	1.7.0_191	/usr/lib/jvm/ja...	查看详情
192.168.200.130	系统类库	否	1.8.0_161	/usr/java/jdk1...	查看详情


主机视角



主机Jar包统计

类型: 全部 业务组: 全部 主机IP: 全部 更多

4 项 全部导出

主机IP	包数
192.168.200.130	688
172.27.0.15	141
192.168.192.165	41
172.22.208.151	30

主机192.168.200.130的Jar包详细信息 

类型: 全部  是否可执行: 全部  包名: 全部

688 项 全部导出

<input type="checkbox"/>	包名	类型	是否可执行	版本	绝对路径	操作	III
<input type="checkbox"/>	OracleIdentityCl...	Web服务自带库	否	--	/home/bert/Do...	查看详情	
<input type="checkbox"/>	_wl_cls_gen.jar	其他依赖包	否	--	/home/bert/Do...	查看详情	
<input type="checkbox"/>	_wl_cls_gen.jar	其他依赖包	否	--	/home/bert/Do...	查看详情	
<input type="checkbox"/>	_wl_cls_gen.jar	其他依赖包	否	--	/home/bert/Do...	查看详情	
<input type="checkbox"/>	_wl_cls_gen.jar	其他依赖包	否	--	/home/bert/Do...	查看详情	

Jar包详情

基本信息

包名: jsse.jar 类型: 其他依赖包
 版本: 1.8.0_131 是否可执行: 否
 绝对路径: /usr/java/jdk1.8.0_131/jre/lib/jsse.jar
 MD5: 390fa11cc6e2557721358f0c5eafd973

引用情况

进程列表:

进程名	PID	启动时间
java	22345	2018-09-06 09:49:45
java	22709	2019-01-21 09:27:31
java	13458	2019-01-10 14:06:25
java	5360	2018-12-17 10:20:26

3.1.12 其他

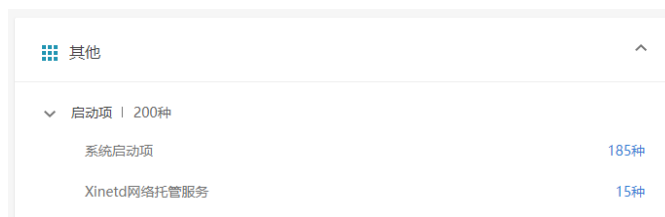
分级视图中“其他”模块，提供了系统安装包、Jar 包相关信息的查询；

 其他 ^

- > 启动项 | 341种
- > 计划任务 | 594个
- > 环境变量 | 204种
- 内核模块 | 350种

3.1.12.1 启动项

包括系统启动项、Xinetd 网络托管启动项。



系统启动项: 展示系统启动项在主机“默认启动模式”下的启动状态, 及在各启动模式下的配置情况;

\

系统启动项
视图

默认启用状态: 全部
业务组: 全部
启动项名: 全部

117 项
更新数据 全部导出

启动项名	启动项数	
<input type="checkbox"/> netconsole	12	
<input type="checkbox"/> network	12	
<input type="checkbox"/> sshd	5	
<input type="checkbox"/> auditd	5	
<input type="checkbox"/> halt	5	
<input type="checkbox"/> reboot	5	
<input type="checkbox"/> single	5	
<input type="checkbox"/> rdisc	4	

启动项netconsole详细信息
更多

单用户自启动(rcs): 全部
停机(rc0): 全部
单用户模式(rc1): 全部
多用户无NFS模式(rc2): 全部

12 项
全部导出

主机IP	默认启动模式	默认启用状态	
<input type="checkbox"/> 192.168.202.133	桌面模式(rc5)	未启用	
<input type="checkbox"/> 192.168.199.16	完全多用户模式(rc3)	未启用	
<input type="checkbox"/> 192.168.19.135	桌面模式(rc5)	未启用	
<input type="checkbox"/> 192.168.122.1	桌面模式(rc5)	未启用	
<input type="checkbox"/> 192.168.122.1	桌面模式(rc5)	未启用	
<input type="checkbox"/> 192.168.122.1	完全多用户模式(rc3)	未启用	
<input type="checkbox"/> 192.168.122.1	桌面模式(rc5)	未启用	
<input type="checkbox"/> 192.168.100.220	桌面模式(rc5)	未启用	

主机系统启动项

视图

默认启动模式: 全部 ▼ 默认启用状态: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 更多 ▼

13 项 更新数据 全部导出

<input type="checkbox"/>	主机IP	默认启动模式	启动项数	
<input type="checkbox"/>	• 172.16.2.240	桌面模式(rc5)	69	
<input type="checkbox"/>	• 192.168.202.133	桌面模式(rc5)	56	
<input type="checkbox"/>	• 10.9.191.52	完全多用户模式(rc3)	52	
<input type="checkbox"/>	• 172.16.2.241	多用户无NFS模式(rc2)	29	
<input type="checkbox"/>	• 192.168.199.16	完全多用户模式(rc3)	23	
<input type="checkbox"/>	• 172.16.4.190	完全多用户模式(rc3)	17	
<input type="checkbox"/>	• 10.211.55.8	桌面模式(rc5)	4	
<input type="checkbox"/>	• 192.168.122.1	桌面模式(rc5)	2	

主机172.16.2.240启动项详细信息

默认启用状态: 全部 ▼ 单用户自启动(rcs): 全部 ▼ 停机(rc0): 全部 ▼ 单用户模式(rc1): 全部 ▼ 更多 ▼

69 项 全部导出

<input type="checkbox"/>	启动项名	默认启用状态	
<input type="checkbox"/>	vmware-tools-thinprint	启用	
<input type="checkbox"/>	local	启用	
<input type="checkbox"/>	rpcbind	启用	
<input type="checkbox"/>	abrttd	启用	
<input type="checkbox"/>	sshd	启用	
<input type="checkbox"/>	jexec	启用	
<input type="checkbox"/>	crond	启用	

Xinetd 网络托管服务: 展示由 Xinetd 托管的启动项, 在 Xinetd 启用时的启动情况:

Xinetd网络托管服务

视图

启用状态: 全部 ▼ 业务组: 全部 ▼ 服务名: 全部 Q

13 项 更新数据 全部导出

<input type="checkbox"/>	服务名	服务数	
<input type="checkbox"/>	rsync	4	
<input type="checkbox"/>	time-dgram	1	
<input type="checkbox"/>	time-stream	1	
<input type="checkbox"/>	telnet	1	
<input type="checkbox"/>	daytime-dgram	1	
<input type="checkbox"/>	chargen-stream	1	

服务rsync详细信息

启用状态: 全部 业务组: 全部 主机IP: 全部 主机名: 全部

4 项 [全部导出](#)

<input type="checkbox"/>	主机IP	启用状态	
<input type="checkbox"/>	● 192.168.202.133	未启用	
<input type="checkbox"/>	● 192.168.199.16	未启用	
<input type="checkbox"/>	● 172.16.2.240	未启用	
<input type="checkbox"/>	● 10.9.191.52	未启用	

主机Xinetd网络托管服务

视图

启用状态: 全部 业务组: 全部 主机IP: 全部 主机名: 全部

4 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	服务数 ↓	
<input type="checkbox"/>	● 172.16.2.240	13	
<input type="checkbox"/>	● 192.168.202.133	1	
<input type="checkbox"/>	● 192.168.199.16	1	
<input type="checkbox"/>	● 10.9.191.52	1	

主机172.16.2.240的Xinetd网络托管服务

启用状态: 全部 服务名: 全部

13 项 [全部导出](#)

<input type="checkbox"/>	服务名	启用状态	
<input type="checkbox"/>	tcpmux-server	未启用	
<input type="checkbox"/>	chargen-stream	未启用	
<input type="checkbox"/>	echo-dgram	未启用	
<input type="checkbox"/>	time-stream	未启用	
<input type="checkbox"/>	telnet	未启用	
<input type="checkbox"/>	discard-stream	未启用	

3.1.12.2 计划任务

包括 **Crontab** 计划任务、**At** 计划任务、**Batch** 计划任务三类

Crontab 计划任务：查询所有安装 agent 主机的 crontab 中具有周期性的计划任务列表。

脚本视角

Crontab计划任务

业务组: 全部 执行脚本: 全部

12 项 更新数据 全部导出

<input type="checkbox"/>	执行脚本	计划任务数	
<input type="checkbox"/>	/etc/cron.hourly/0anacron	12	
<input type="checkbox"/>	/etc/titanagent/agent_update.sh	11	
<input type="checkbox"/>	/etc/titanagent/agent_monitor.sh	11	
<input type="checkbox"/>	/etc/titanagent/agent_update_exception.sh	11	
<input type="checkbox"/>	/usr/sbin/raid-check	10	
<input type="checkbox"/>	/usr/lib64/sa/sa2	9	
<input type="checkbox"/>	/usr/lib64/sa/sa1	9	

执行/etc/cron.hourly/0anacron脚本的计划任务

执行用户: 全部 服务启用状态: 全部 业务组: 全部 执行周期: 全部 更多

12 项 全部导出

<input type="checkbox"/>	主机IP	服务启用状态	执行周期	执行命令或脚本	执行用户	配置文件路径	
<input type="checkbox"/>	● 192.168.202.133	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.199.16	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.19.135	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.122.1	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.122.1	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.122.1	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.122.1	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	● 192.168.100.220	启用	01 ****	/etc/cron.hourly/...	root	/etc/cron.d/0hourly	

主机视角

主机Crontab计划任务统计

服务启用状态: 全部 业务组: 全部

13 项 更新数据 全部导出

<input type="checkbox"/>	主机IP	服务启用状态	计划任务数	
<input type="checkbox"/>	● 192.168.202.133	启用	4	
<input type="checkbox"/>	● 192.168.199.16	启用	4	
<input type="checkbox"/>	● 192.168.122.1	启用	14	
<input type="checkbox"/>	● 192.168.122.1	启用	7	
<input type="checkbox"/>	● 192.168.122.1	启用	7	
<input type="checkbox"/>	● 192.168.122.1	启用	13	
<input type="checkbox"/>	● 192.168.100.220	启用	13	

主机192.168.202.133的Crontab计划任务统计

执行用户: 全部 | 执行周期: 全部 | 执行脚本或命令: 全部 | 配置文件: 全部

4 项 [全部导出](#)

<input type="checkbox"/>	执行周期	执行命令或脚本	执行用户	配置文件路径	
<input type="checkbox"/>	01 ****	/etc/cron.hourly/0anacron	root	/etc/cron.d/0hourly	
<input type="checkbox"/>	*/10 ****	/usr/lib64/sa/sa1 1 1	root	/etc/cron.d/sysstat	
<input type="checkbox"/>	53 23 ***	/usr/lib64/sa/sa2 -A	root	/etc/cron.d/sysstat	
<input type="checkbox"/>	0 1 ** Sun	/usr/sbin/raid-check	root	/etc/cron.d/raid-check	

At 计划任务：查询所有安装 agent 主机的 crontab 中定时执行的计划任务列表。

主机定时计划任务统计

业务组: 全部

85 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	启用状态	计划任务数 ↓	
<input type="checkbox"/>	192.168.100.162	启用	2	
<input type="checkbox"/>	192.168.219.131	启用	1	
<input type="checkbox"/>	192.168.122.1	启用	0	
<input type="checkbox"/>	10.31.91.192	启用	0	
<input type="checkbox"/>	192.168.197.50	启用	0	

主机192.168.100.162定时计划任务统计

执行用户: 全部 | 执行时间: 全部 | 脚本路径: 全部

2 项 [全部导出](#)

<input type="checkbox"/>	执行时间	脚本路径	执行用户	
<input type="checkbox"/>	1963-11-18 19:31:44	/var/spool/at/a0000204132578	0x001	
<input type="checkbox"/>	1963-11-18 19:31:44	/var/spool/at/a0000104132578	0x001	

空闲计划任务：查询所有安装 agent 主机的 crontab 中主机空闲时执行的计划任务列表。

主机空闲计划任务统计

业务组: 全部

86 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	启用状态	计划任务数 ↓	
<input type="checkbox"/>	192.168.122.1	启用	0	
<input type="checkbox"/>	10.31.91.192	启用	0	
<input type="checkbox"/>	192.168.197.50	启用	0	
<input type="checkbox"/>	192.168.197.245	启用	0	

3.1.12.3 环境变量


资产视角





环境变量统计  视图  

环境变量类型: 全部  环境变量名: 全部 





204 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	环境变量名	环境变量类型	主机数	
<input type="checkbox"/>	OPTERR	用户变量	78	
<input type="checkbox"/>	BASH_VERSION	用户变量	78	
<input type="checkbox"/>	DIRSTACK	用户变量	78	
<input type="checkbox"/>	IFS	用户变量	78	

环境变量OPTERR统计 

环境变量类型: 全部  业务组: 全部  用户: 全部  [更多](#) 

251 项 [全部导出](#)

<input type="checkbox"/>	主机IP	用户	环境变量值	环境变量名	环境变量类型	
<input type="checkbox"/>	 192.168.248.145	test	1	OPTERR	用户变量	
<input type="checkbox"/>	 192.168.248.145	root	1	OPTERR	用户变量	
<input type="checkbox"/>	 192.168.248.145	root	1	OPTERR	用户变量	
<input type="checkbox"/>	 192.168.248.145	test	1	OPTERR	用户变量	

主机视图

主机环境变量统计 

业务组: 全部  主机IP: 全部  主机名: 全部 

86 项 [全部导出](#)

<input type="checkbox"/>	主机IP	环境变量数	
<input type="checkbox"/>	 192.168.122.1	90	
<input type="checkbox"/>	 10.31.91.192	34	
<input type="checkbox"/>	 192.168.197.50	73	
<input type="checkbox"/>	 192.168.197.245	32	

主机192.168.122.1环境变量统计

环境变量类型: 全部 | 环境变量名: 全部 | 环境变量值: 全部

90 项 [全部导出](#)

<input type="checkbox"/>	主机IP	用户	环境变量名	环境变量值	环境变量类型	
<input type="checkbox"/>	192.168.122.1	root	BASH	/bin/bash	用户变量	
<input type="checkbox"/>	192.168.122.1	admin	BASH	/bin/bash	用户变量	
<input type="checkbox"/>	192.168.122.1	admin	BASHOPTS	cmdhisttextquote...	用户变量	
<input type="checkbox"/>	192.168.122.1	root	BASHOPTS	cmdhisttextquote...	用户变量	

3.1.12.4 内核模块

资产视角

主机内核模块统计

模块名称: 全部

350 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	模块名称	模块描述	主机数	
<input type="checkbox"/>	tcp_diag		76	
<input type="checkbox"/>	inet_diag		76	
<input type="checkbox"/>	i2c_piix4	PIIX4 SMBus driver	72	
<input type="checkbox"/>	ata_piix	SCSI low-level driver for Intel PIIX/ICH A...	64	
<input type="checkbox"/>	pata_acpi	SCSI low-level driver for ATA in ACPI m...	63	

内核模块i2c_piix4查询

模块版本: 全部 | 业务组: 全部 | 模块路径: 全部 | 主机IP: 全部 | 更多

72 项 [全部导出](#)

<input type="checkbox"/>	主机IP	模块路径	模块版本	模块大小	依赖的进程数	被依赖的模块数	操作	
<input type="checkbox"/>	192.168.91.132	/lib/modules...		43597	1	0	查看详情	
<input type="checkbox"/>	192.168.152.145	/lib/modules...		24576	0	0	查看详情	
<input type="checkbox"/>	192.168.197.55	/lib/modules...		22106	1	0	查看详情	
<input type="checkbox"/>	192.168.199.119	/lib/modules...		12608	1	0	查看详情	
<input type="checkbox"/>	192.168.248.145	/lib/modules...		12608	1	0	查看详情	

主机视角

主机内核模块统计

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

80 项 全部导出

主机IP	内核模块数
192.168.122.1	106
10.31.91.192	46
192.168.197.50	61
192.168.197.245	44

主机192.168.122.1内核模块查询

模块版本: 全部 | 模块名称: 全部 | 模块路径: 全部

106 项 全部导出

模块名称	模块描述	模块路径	模块版本	依赖的进程数	被依赖的模块数	操作
xt_contrack	Xtables: conne...	/lib/modules/3...		1	0	查看详情
xt_addrtype	Xtables: addre...	/lib/modules/3...		0	0	查看详情
xt_CHECKSUM	Xtables: check...	/lib/modules/3...		0	0	查看详情
xfs	SGI XFS with A...	/lib/modules/3...		1	0	查看详情
vsock	VMware Virtua...	/lib/modules/3...	1.0.0.0-k	0	1	查看详情

3.2 风险发现

通用功能描述:

以安全补丁界面为例

安全补丁

危险程度分布

应用分布

修复影响分布

业务组: 所有 | 危险程度: 所有 | 修复影响: 所有 | 业务影响: 所有 | 更多


670 项 立即检测 | 检查业务影响 | 导出



危险程度	补丁名称	风险特征	影响主机数
高危	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	远程利用 存在EXP 系统重启	2
高危	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	远程利用 存在EXP 系统重启	2
高危	CentOS 5 / 6 / 7 : bind (CESA-2014:1984)	远程利用 服务重启	2
中危	CentOS 5 / 6 / 7 : bind (CESA-2016:0073)	远程利用 服务重启	5
中危	CentOS 5 / 6 / 7 : bind (CESA-2016:0459)	远程利用 服务重启	5
高危	CentOS 5 / 6 / 7 : bind (CESA-2016:1944)	远程利用 存在EXP 服务重启	5
高危	CentOS 5 / 6 / 7 : firefox (CESA-2016:0695)	远程利用 无影响	1


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：对单独项目进行扫描；导出：导出单项检查结果

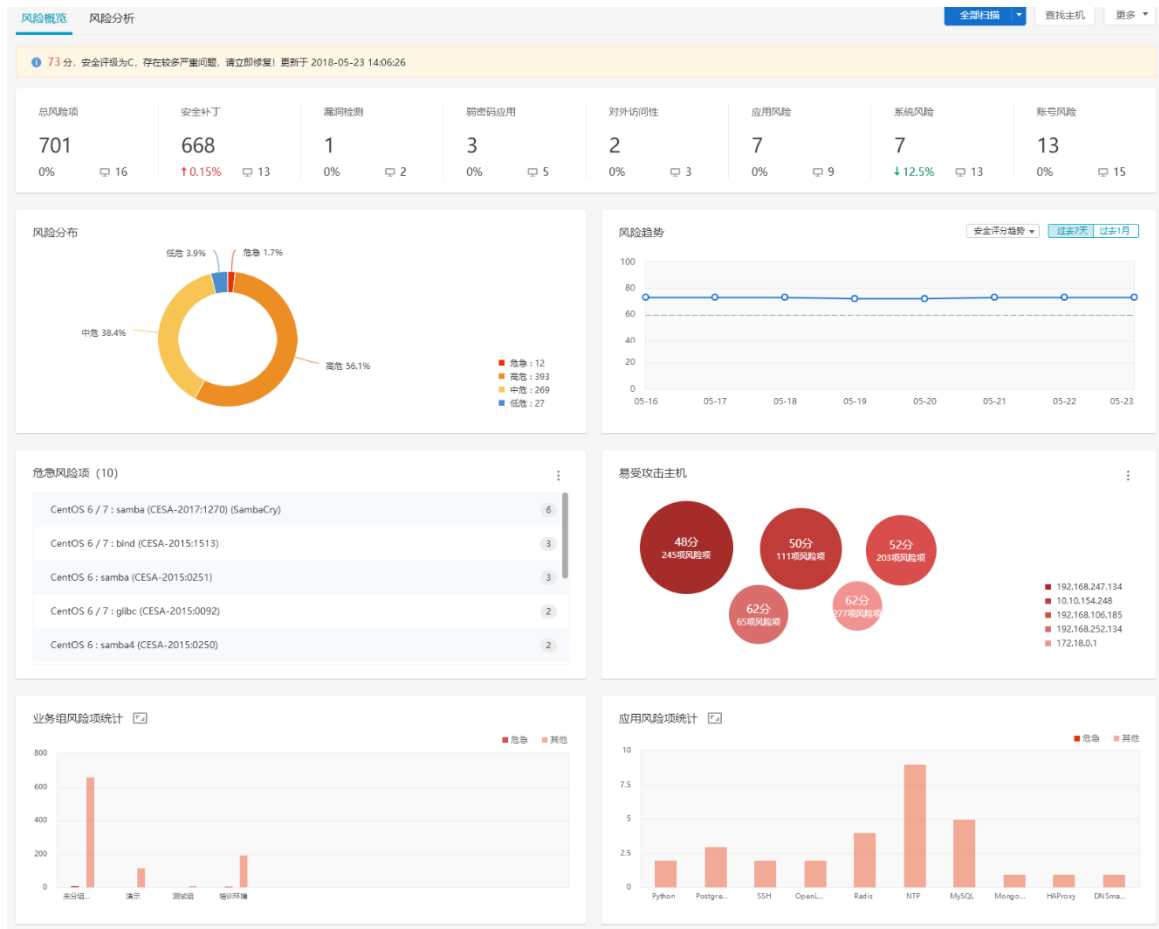
⑤ 更多设置按钮：点击  按钮，显示全部；

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。

3.2.1 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 7 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。
- 对外访问性：检测常见对外访问性风险是否检出，并统计各类型风险的数量及其影响主机数量。
- 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。



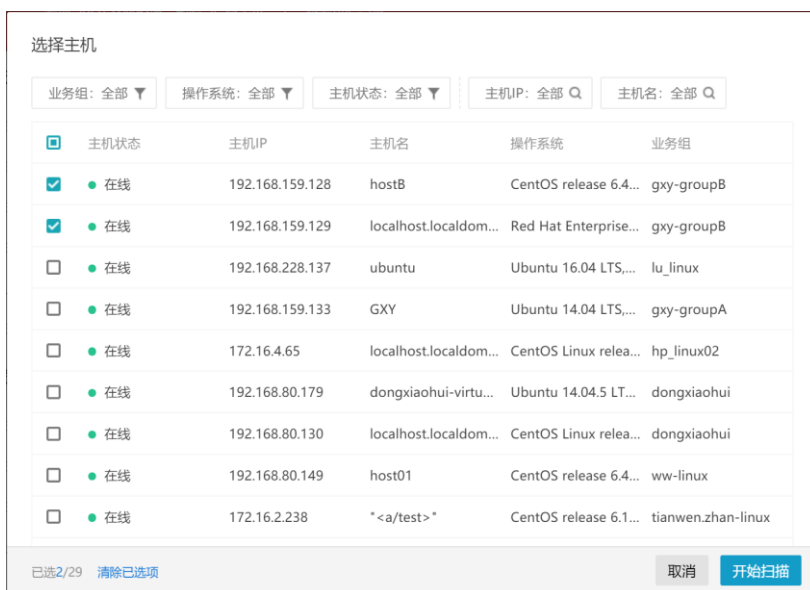
3.2.1.1 全部扫描

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；

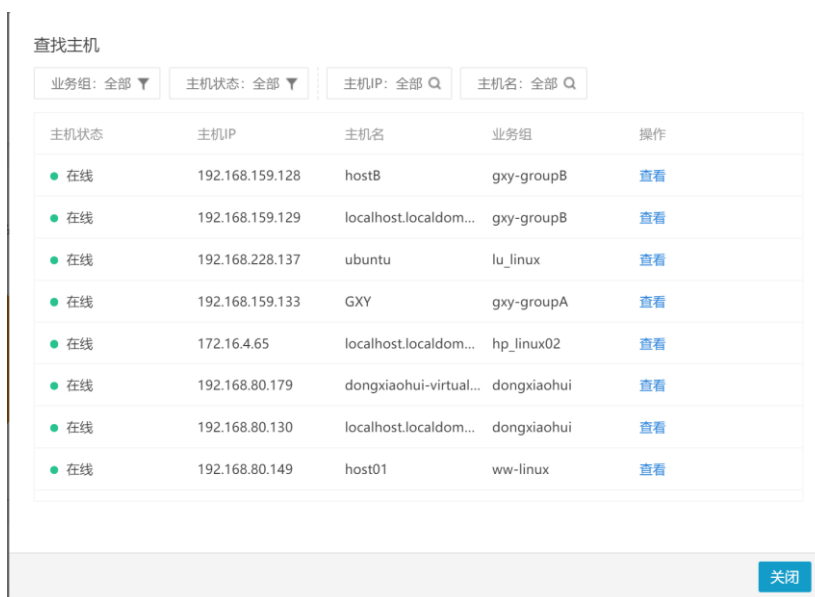


3) 点击“全部扫描”按钮旁的下拉按钮，选择“按主机 IP 扫描”，可对选择的主机进行全部风险的扫描；



3.2.1.2 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。



3.2.1.3 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。

执行记录

总耗时: 全部 | 扫描状态: 全部 | 开始时间: 全部

69 项

开始扫描时间	执行内容	执行范围	执行者	总耗时	扫描状态	执行结果	操作
2019-10-29 12:16:00	弱密码扫描	全部主机	qingteng@qingte...	--	扫描中	成功 0 台, 失败 0 台	弱密码进度
2019-10-29 10:19:05	弱密码扫描	全部主机	qingteng@qingte...	23分1秒	扫描成功	成功 6 台, 失败 10 台	弱密码进度 失败主机详情
2019-10-29 04:30:02	全部风险扫描	全部主机	system	22分17秒	扫描成功	成功 4 台, 失败 6 台	弱密码进度 失败主机详情
2019-10-28 20:52:30	应用风险扫描	全部主机	qingteng@qingte...	1分51秒	扫描成功	成功 4 台, 失败 4 台	失败主机详情
2019-10-28 20:12:23	账号风险扫描	全部主机	qingteng@qingte...	8秒	扫描成功	成功 4 台, 失败 3 台	失败主机详情

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。

全部风险扫描作业的错误任务视图

总耗时: 全部 | 失败原因: 全部 | 任务名: 全部 | 执行对象: 全部

160 项

开始扫描时间	任务名	执行对象	总耗时	失败原因
2019-11-07 04:36:32	SSH服务AuthorizedKeysFile配置名称...	192.168.199.85	0秒	agent不支持此脚本
2019-11-07 04:36:32	SSH服务AuthorizedKeysFile配置名称...	192.168.131.136	0秒	agent不支持此脚本
2019-11-07 04:36:32	SSH服务AuthorizedKeysFile配置名称...	192.168.199.22	0秒	agent不支持此脚本
2019-11-07 04:36:32	SSH服务AuthorizedKeysFile配置读取...	192.168.199.85	0秒	agent不支持此脚本
2019-11-07 04:36:32	SSH服务AuthorizedKeysFile配置项存...	192.168.131.136	0秒	agent不支持此脚本

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。

弱密码扫描进度详情

本次弱密码扫描的进度为: 100.00%

总耗时: 全部 | 任务名: 全部 | 扫描主机: 全部

15 项

开始扫描时间	任务名	扫描主机	总耗时	账号扫描进度
2019-10-29 10:19:06	vsftpd服务存在弱密码	192.168.80.141	5秒	1/1
2019-10-29 10:19:06	vsftpd服务存在弱密码	172.16.2.229	5秒	3/3
2019-10-29 10:19:06	vsftpd服务存在弱密码	192.168.80.149	5秒	1/1
2019-10-29 10:19:06	Redis服务存在弱密码	172.16.4.186	5秒	1/1

3.2.2 安全补丁

“安全补丁”指对于软件系统在使用过程中暴露的问题（一般由黑客或病毒设计者发现）而发布的解决问题的小程序。安全补丁是由软件的原来作者制作的，可以访问网站下载补丁。

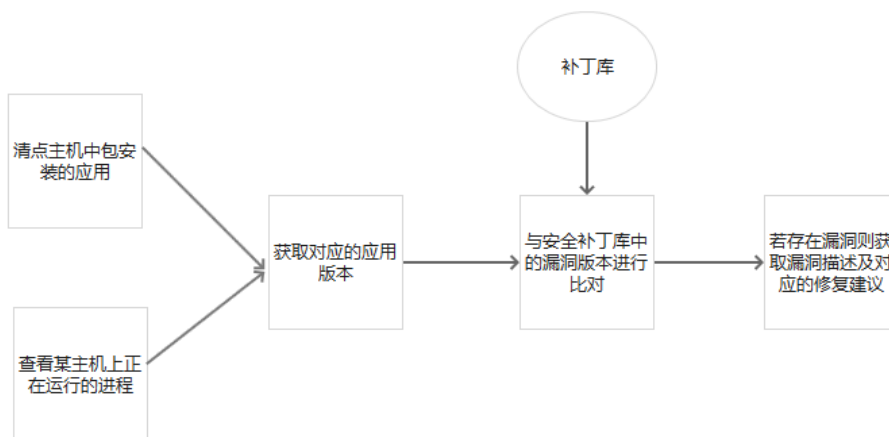
各种应用的漏洞已经成为大规模网络与信息安全事件和重大信息泄露事件的主要原因之一，针对计算机漏洞带来的危害，安装相应的补丁是最有效、也是最经济的防范措施。但打补丁是比较被动的方式，对于企业来说，收集、测试、备份、分发等相关的打补丁流程仍然是一个颇为繁琐的过程，甚至补丁本身就有可能成为新的漏洞。

基于以上问题，安全补丁模块主要是为了解决补丁管理的混乱，而建立一个的一个自动化补丁管理库，拟实现帮助运维人员检测需要打的补丁、自动化打补丁、进行补丁管理。有补丁视图/主机视图两种查看模式。

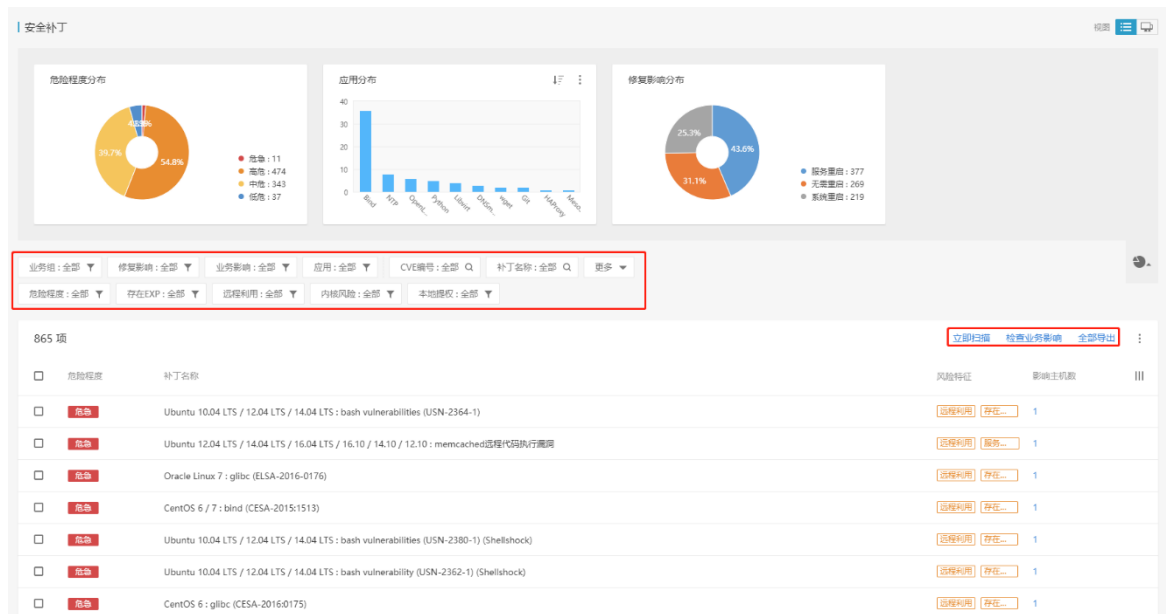
补丁分类说明

影响对象	应用：安全补丁所影响应用 内核：指补丁对应的漏洞影响的对象为 kernel 的 其他：除应用与系统类别外，其他的均归为其他类别。如影响对象为 lib 的补丁属于其他类别。
危险程度	危急：由运营人员定义，是指那些已经验证存在的，明确有危害必须修复的风险项 高危：CVSS 评分为 7.0-10 分的风险项 中危：CVSS 评分为 4.0-6.9 分的风险项 低危：CVSS 评分为 0-3.9 分的风险项
CVSS 评分维度	攻击途径：远程/本地 攻击复杂度：高/中/低 认证：需要/不需要 机密性影响：不受影响/部分/完全 完整性影响：不受影响/部分/完全 可用性：不受影响/部分/完全

3.2.2.1 补丁检测逻辑



3.2.2.2 补丁视图



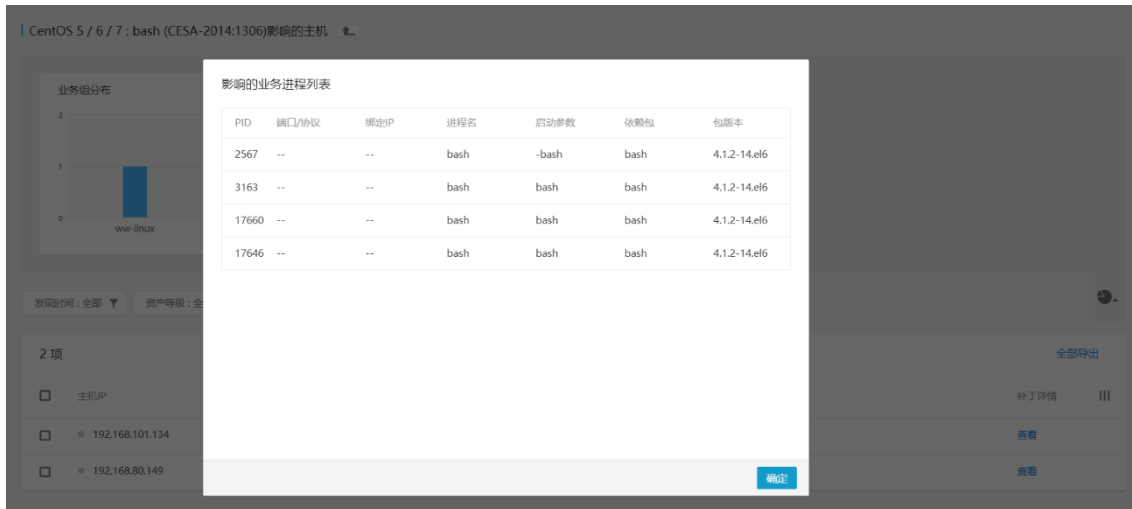
筛选框：可以根据业务组、修复影响、业务影响、应用、CVE 编号、补丁名称、危险程度、存在 EXP、远程利用、内核风险、本地提权来筛选显示；其中“危险程度、存在 EXP、远程利用、内核风险、本地提权”需要点击“更多”来进行筛选。

立即检查：开始对全部在线主机进行安全补丁扫描。

检查业务影响：该操作占用资源较大，建议在业务不繁忙时进行。在补丁视图下，点击“影响主机”业务影响列如果为深色，则表明该漏洞对此业务有影响；如果为灰色则表明没有影响。

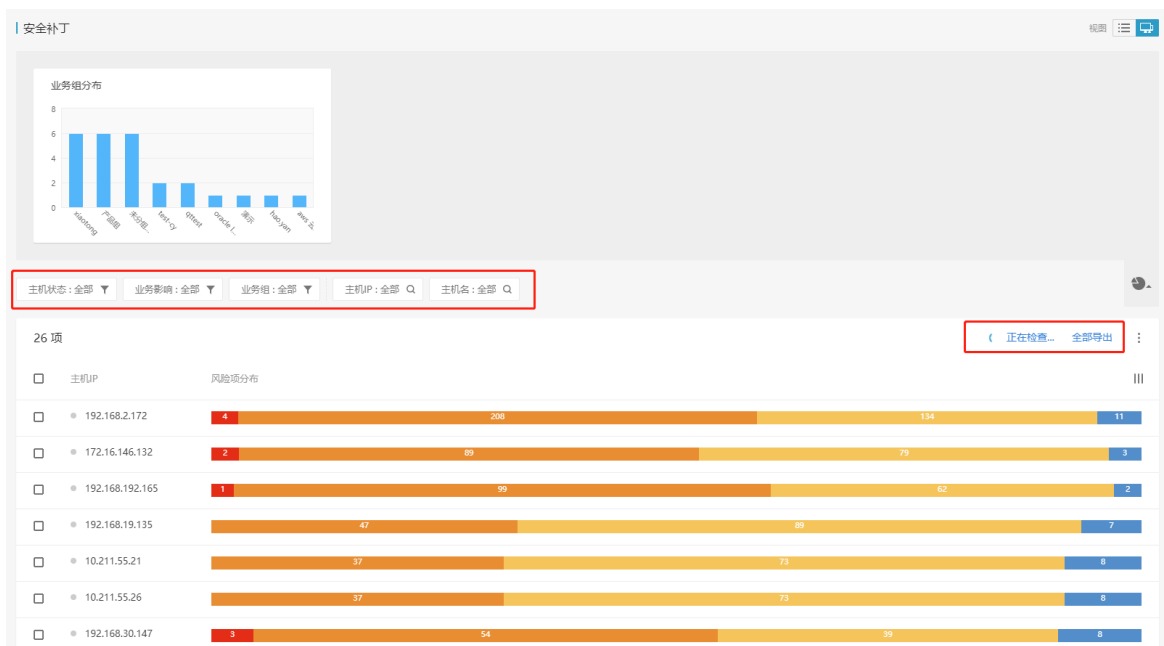


存在业务影响时，可点击查看查看进程影响的详情。



全部导出：导出 csv 格式的补丁视图补丁扫描报表。包括“发现时间、主机状态、主机 IP、主机名、资产等级、业务组、操作系统、内网 IP、外网 IP、负责人、验证信息、危险程度、补丁名、远程利用、存在 EXP、内核风险、本地提权、修复建议、修复命令、修复应用、修复影响、风险描述、漏洞利用参考、CVSS 评分、CVSS 详情、参考信息、影响主机数”

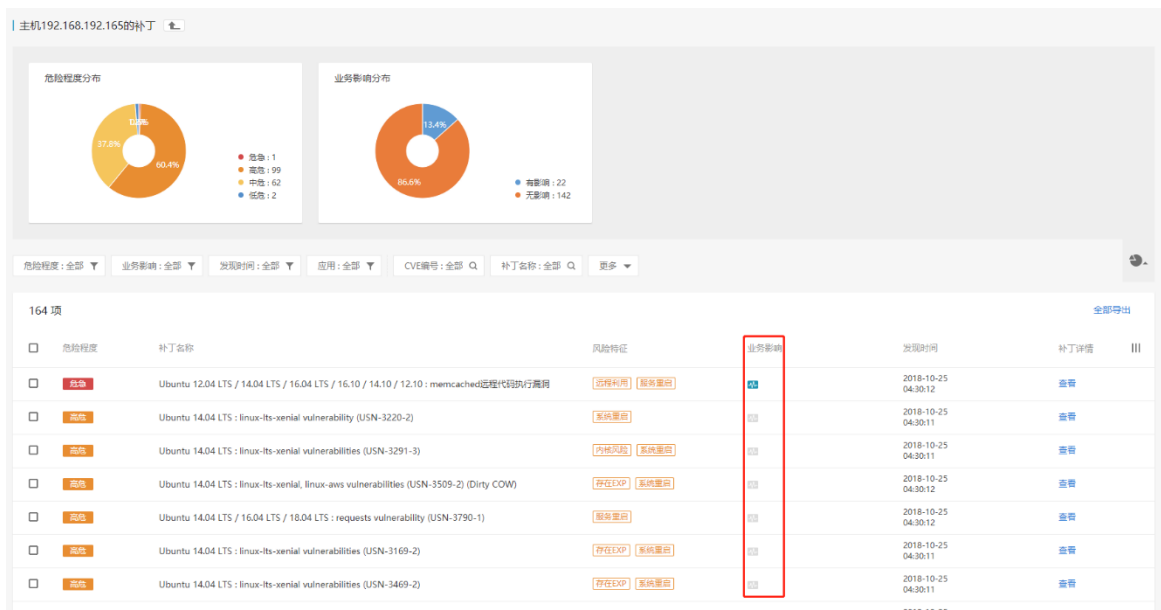
3.2.2.3 主机视图



筛选框：可以根据主机状态、业务影响、业务组、主机 IP、主机名来筛选显示

立即检查：开始对全部在线主机进行安全补丁扫描。

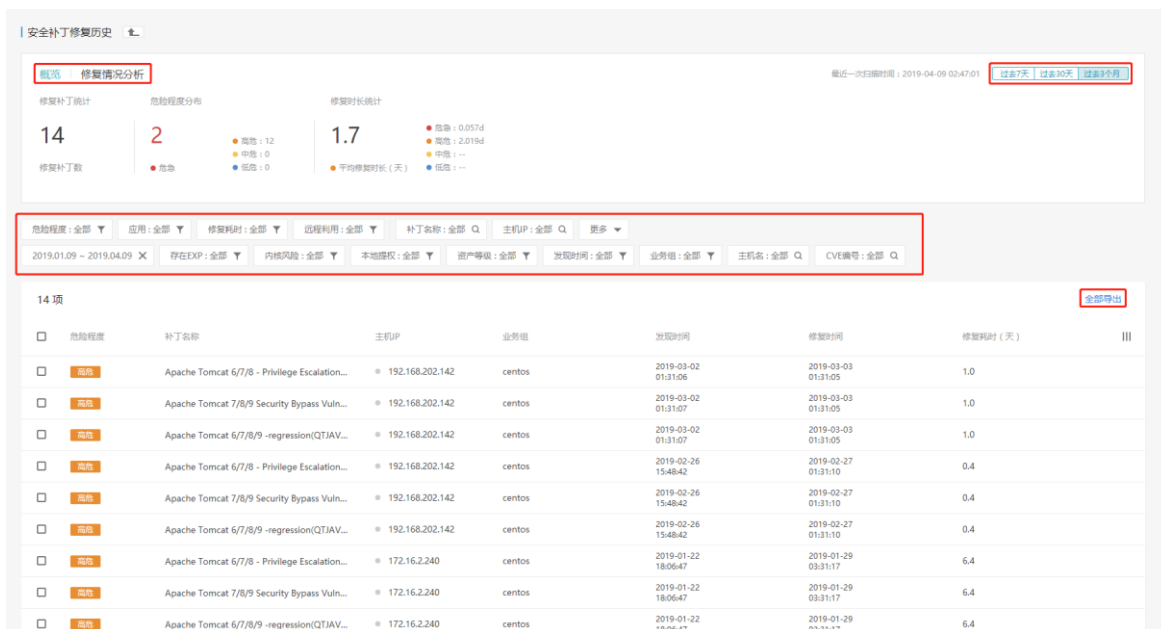
检查业务影响：该操作占用资源较大，建议在业务不繁忙时进行。在主机视图下，单击对应主机，可以查看到影响当前主机的业务影响。



全部导出：导出 csv 格式的主机视图补丁报表。包括“发现时间、主机状态、主机 IP、主机名、资产等级、业务组、操作系统、内网 IP、外网 IP、负责人、危急、高危、中危、低危危险程度、补丁名、远程利用、存在 Exp、内核风险 本地提权、修复建议、修复命令、修复应用、修复影响、风险描述、验证结果、漏洞利用参考、CVSS 评分、CVSS 详情、参考信息”

3.2.2.4 修复历史

补丁视图和主机视图下均有 符号，点进该符号 **修复历史** 即可进入修复历史页面。



选定统计时间：点击右上角的时间按钮，可查看过去 7 天、过去 30 天、过去 3 个月内的修复历史统计情况

修复情况分析：点击统计面板 TAB “修复情况分析” 可查看选定时间内的修复情况分析



筛选框：可以根据业务组、修复时间、发现时间、危险程度、补丁名称、主机 IP、资产等级、应用、修复耗时、远程利用、存在 EXP、内核风险、本地提权、主机名、CVE 编号来筛选显示。其中修复时间默认筛选近三个月，资产等级、应用、修复耗时、远程利用、存在 EXP、内核风险、本地提权、主机名、CVE 编号默认隐藏

全部导出：导出 csv 格式的修复历史报表。包括“危险程度、补丁名称、远程利用、存在 EXP、内核风险、本地提权、主机 IP、内网 IP、外网 IP、主机名、资产等级、业务组、操作系统、标签、备注、负责人、发现时间、修复时间、修复耗时”

3.2.2.5 白名单规则

补丁视图和主机视图下均有 符号，点进该符号 即可进入白名单规则设置页面。



➤ 新建规则

条件列表包括：补丁名称中包含，补丁修复的应用，修复影响（未知影响、无需重启、服务重启、系统重启），补丁危害程度（危急、高危、中危、低危），补丁特征（本地漏洞、远程利用）

各个复选框之间为且的关系

规则范围：全部主机、自定义范围（选择业务组、指定主机 IP）

描述：新建时自动生成，也可手动更改

新建白名单规则

新建规则

条件列表：

- 补丁名中包含： 请输入补丁名称
- 补丁修复的应用： 请输入补丁修复的应用,多个以逗号隔开
- 修复影响： 请选择修复影响
- 补丁危害程度： 请选择危害程度
- 补丁特征： 请选择补丁特征

则将风险项加入白名单

使用范围：

- 全部主机
- 自定义范围
 - 业务组： 请选择业务组
 - 主机： 请选择主机IP

描述： 用户“演示”于2018-10-31添加该白名单

[创建](#) [取消](#)

- 编辑规则：编辑已有规则。
- 删除规则：删除已有规则。
- 查看受影响对象：点击查看详情跳转到“规则受影响对象”界面。

3.2.3 漏洞检测

该功能通过创建作业，使用执行作业的方式通过版本比对或 poc 去验证存在的漏洞，如果该漏洞已经有成熟、无危害可验证 poc 或者应用版本在有漏洞的版本范围内，就会在漏洞检测页面显示出来。

漏洞检查

漏洞检查支持自定义漏洞检查任务，您可以进入 [作业管理](#) 进行漏洞作业的创建、修改和执行。

漏洞通知

- GoAhead进程命令执行漏洞 (CVE-2017-17562) 2019-03-21 [查看更多](#)
- Tomcat开放重定向漏洞(CVE-2018-11784) 2019-03-05
- Git任意代码执行漏洞(CVE-2018-17456) 2019-03-05
- gitk-参数溢出漏洞(CVE-2018-6485) 2019-03-05
- Jenkins进程命令执行漏洞(CVE-2016-0788) 2019-03-05

漏洞统计

16 6 13 10 3 2

可远程利用 存在exp 可本地提权 内网风险

业务组：全部 危险程度：全部 应用：全部 漏洞名称：全部 漏洞类型：全部 ...

16 项 [作业管理](#) [全部导出](#) [更多](#)

危险程度	漏洞名称	漏洞类型	漏洞特征	影响主机数
致命	Linux内核本地提权(致命)漏洞(CVE-2016-5195)	本地提权	存在EXP 内网风险 本地提权 篡改系统	3
致命	OpenSSL Heartbleed漏洞(CVE-2014-0160)	敏感信息泄露	存在EXP 远程利用 篡改服务	1
致命	Bash环境变量溢出漏洞(CVE-2014-6271)	命令执行	存在EXP 远程利用 篡改系统	1
致命	Samba远程代码执行漏洞(CVE-2015-0240)	代码执行	存在EXP 远程利用 篡改服务	1
致命	OpenSSL ASN.1编解码器内存损坏漏洞(CVE-2016-2108)	代码执行	远程利用 篡改服务	1
致命	Linux内核信息泄露漏洞(CVE-2016-9555)	敏感信息泄露	远程利用 内网风险 篡改系统	4
致命	Oracle MySQL远程代码执行漏洞(CVE-2016-6662)	代码执行	存在EXP 远程利用 篡改服务	3
致命	Sudo本地权限提升漏洞(CVE-2017-1000367)	本地提权	存在EXP 本地提权 无漏洞利用	3
致命	Bash本地命令执行漏洞(CVE-2016-7543)	命令执行	远程利用 篡改系统	2

漏洞通知：显示漏洞检测能力，可以查看系统中拥有漏洞检测能力

筛选框：可以根据业务组、危险程度、应用、漏洞名称、漏洞类型、存在 EXP、远程利用、内

核风险、本地提权、修复影响、检测方式进行筛选。

作业管理：点击“作业管理”，跳转到作业管理界面

全部导出：导出 csv 格式的漏洞检测报表，可选择导出统计报表或详情报表。

- 1) 统计报表包括：危险程度、漏洞名称、漏洞类型、远程利用、存在 EXP、内核风险、本地提权、漏洞描述、修复建议、修复影响、影响应用、利用条件、受影响应用版本、漏洞利用链接、参考链接、CVSS 评分、CVSS 详情、影响主机数

导出统计报表

全选

<input checked="" type="checkbox"/> 危险程度	<input checked="" type="checkbox"/> 漏洞名称	<input checked="" type="checkbox"/> 漏洞类型
<input checked="" type="checkbox"/> 远程利用	<input checked="" type="checkbox"/> 存在EXP	<input checked="" type="checkbox"/> 内核风险
<input checked="" type="checkbox"/> 本地提权	<input checked="" type="checkbox"/> 漏洞描述	<input checked="" type="checkbox"/> 修复建议
<input checked="" type="checkbox"/> 修复影响	<input checked="" type="checkbox"/> 影响应用	<input type="checkbox"/> 利用条件
<input type="checkbox"/> 受影响系统	<input type="checkbox"/> 漏洞利用链接	<input type="checkbox"/> 参考链接
<input type="checkbox"/> CVSS评分	<input type="checkbox"/> CVSS详情	<input checked="" type="checkbox"/> 影响主机数

文件将下载到本地, 也可稍后前往[下载中心](#)下载。

取消 导出

- 2) 详情报表包括：主机状态、主机 IP、主机名、业务组、资产等级、内网 IP、外网 IP、操作系统、主机标签、负责人、负责人邮箱、备注、危险程度、漏洞名称、漏洞类型、远程利用、存在 EXP、内核风险、本地提权、漏洞描述、修复建议、修复影响、验证信息、影响应用、利用条件、受影响应用版本、漏洞利用链接、参考链接、CVSS 评分、CVSS 详情

导出详情报表

主机信息：全选

<input checked="" type="checkbox"/> 主机状态	<input checked="" type="checkbox"/> 主机IP	<input checked="" type="checkbox"/> 主机名
<input checked="" type="checkbox"/> 业务组	<input type="checkbox"/> 资产等级	<input type="checkbox"/> 内网IP
<input type="checkbox"/> 外网IP	<input type="checkbox"/> 操作系统	<input type="checkbox"/> 主机标签
<input type="checkbox"/> 负责人	<input type="checkbox"/> 负责人邮箱	<input type="checkbox"/> 备注

漏洞详情：全选

<input checked="" type="checkbox"/> 危险程度	<input checked="" type="checkbox"/> 漏洞名称	<input checked="" type="checkbox"/> 漏洞类型
<input checked="" type="checkbox"/> 远程利用	<input checked="" type="checkbox"/> 存在EXP	<input checked="" type="checkbox"/> 内核风险
<input checked="" type="checkbox"/> 本地提权	<input checked="" type="checkbox"/> 漏洞描述	<input checked="" type="checkbox"/> 修复建议
<input checked="" type="checkbox"/> 修复影响	<input checked="" type="checkbox"/> 验证信息	<input checked="" type="checkbox"/> 影响应用

文件将下载到本地, 也可稍后前往[下载记录](#)下载。

取消 导出

3.2.3.1 主机视图

漏洞检查

漏洞检测支持自定义漏洞检查任务，您可以进入 [作业管理](#) 进行漏洞作业的创建、删除、修改和执行。

漏洞通知

- Apache Solr远程命令执行漏洞(CVE-2019-0193) 2019-08-07
- Jackson-databind远程代码执行漏洞(CVE-2019-12384) 2019-06-24
- FastJSON远程代码执行漏洞 2019-06-22
- Apache AXIS远程命令执行漏洞 2019-06-19
- Oracle WebLogic wls9-async组件反序列化远程命令执行漏洞(CVE-2019-2729) 2019-06-18

漏洞统计

54 48 24 4 3

可远程利用 存在exp 可本地提权 内核风险

业务组: 全部 资产等级: 全部 主机状态: 全部 主机IP: 全部 主机名称: 全部

主机IP	业务组	漏洞数
192.168.192.165	未分组主机	20
172.27.16.13	xiaotong	17
172.22.208.151	未分组主机	17
172.16.146.132	产品组	15
10.8.0.1	未分组主机	14
172.27.0.15	xiaotong	13
10.211.55.26	产品组	13
10.211.55.21	产品组	13
192.168.19.135	test-cy	11

筛选框：业务组、资产等级、主机状态、主机 IP，主机名。

3.2.3.2 作业管理

漏洞视图和主机视图下均有“作业管理”按钮，点进该符号即可进入作业管理页面。

作业管理

自定义作业 全局作业

创建时间: 全部 作业名称: 全部 执行范围: 全部

创建时间	作业名称	是否启用	执行范围	检查项数	最后执行时间	操作
2018-10-24 20:30:58	uWSGI PHP目录穿越漏洞(CVE-20...	是	全部主机	1	2018-10-24 20:30:58	执行 查看结果 ...
2018-10-11 15:24:43	12	是	全部主机	1	2018-10-11 16:28:28	执行 查看结果 ...
2018-09-11 23:11:12	172.19.77.172	是	已选择1台主机	35	2018-09-11 23:11:12	执行 查看结果 ...
2018-08-22 18:14:51	Struts2 S2-057 远程代码执行漏洞...	是	全部主机	1	2018-09-28 14:42:47	执行 查看结果 ...

自定义作业筛选项：可根据创建时间、作业名称、执行范围进行筛选。

作业管理

自定义作业 全局作业

创建时间: 全部 作业名称: 全部

创建时间	作业名称	是否启用	执行范围	检查项数	最后执行时间	操作
2019-02-11 15:42:19	测试删除	是	全部主机	1	2019-03-04 19:02:25	执行 查看结果 作业详情
2018-11-14 15:04:30	Weblogic漏洞检查	是	全部主机	1	2019-02-01 14:58:08	执行 查看结果 作业详情
2018-09-07 14:15:10	Struts2漏洞检查	是	全部主机	11	2018-11-13 20:00:58	执行 查看结果 作业详情
2018-08-29 10:42:45	拒绝服务漏洞检查	是	全部主机	15	2018-09-06 10:04:05	执行 查看结果 作业详情
2018-08-29 10:20:12	反序列化漏洞检查	是	全部主机	5	2018-09-06 10:04:05	执行 查看结果 作业详情
2018-08-29 10:20:04	提权漏洞检查	是	全部主机	11	2018-10-11 16:29:57	执行 查看结果 作业详情
2018-08-29 10:19:56	远程代码执行漏洞检查	是	全部主机	61	2018-09-18 11:57:28	执行 查看结果 作业详情

全局作业筛选项：可根据创建时间、作业名称进行筛选。

【作业管理-操作】

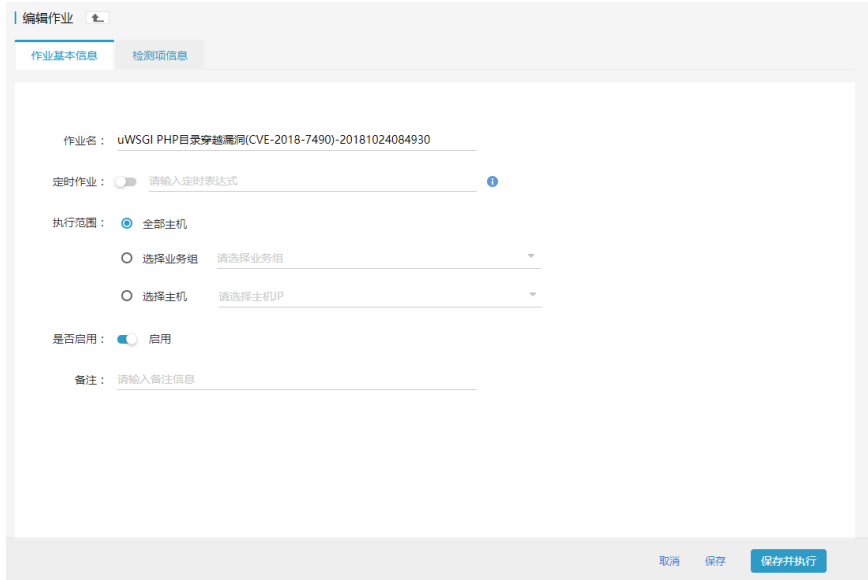
自定义作业-新建作业： 点击新建作业，跳转到新建作业页面。

执行： 点击执行，可执行该作业。

查看结果： 点击查看结果，跳转到该作业的作业执行结果界面。

作业详情： 点击作业详情，跳转到编辑作业页面，所有项均可查看但不可编辑。

自定义作业-编辑： 点击“…-编辑”，可编辑自定义作业，跳转到编辑作业页面。

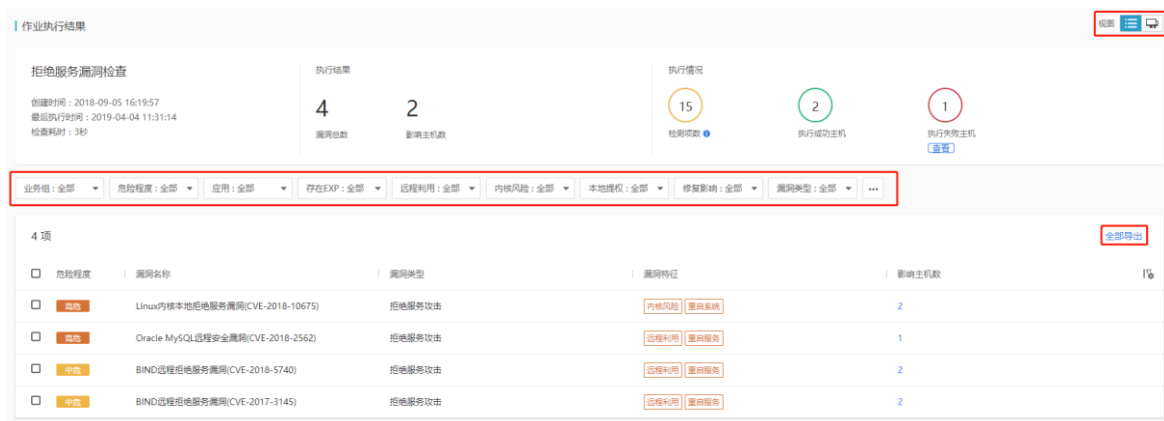


自定义作业-删除： 点击“…-删除”，可删除自定义作业。

3.2.3.3 作业执行结果

在自定义作业或全局作业中，点击操作列的“作业详情”，跳转到作业执行结果界面。

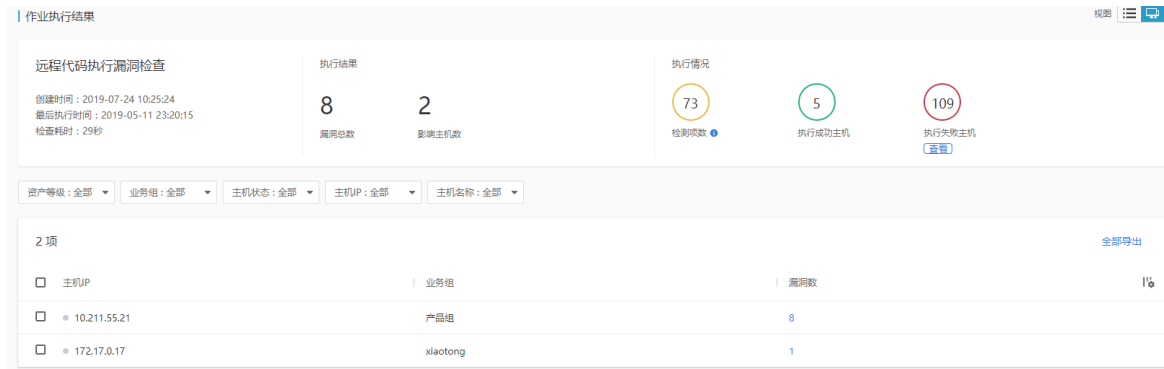
【漏洞视图】



筛选项： 业务组、危险程度、应用、存在 EXP、远程利用、内核风险、本地提权、修复影响、漏洞类型。其中内核风险、本地提权、修复影响、漏洞类型是默认隐藏的。

全部导出： 导出该作业检测出的漏洞，可导出统计视图和详情视图，字段与漏洞视图导出相同。

【主机视图】



筛选项：资产等级、业务组、主机状态、主机 IP、主机名称。

导出：导出该作业检测主机的漏洞，可导出统计视图和详情视图，字段与主机视图导出相同。

3.2.3.4 新建作业

在自定义作业或全局作业中，点击操作列的“新建作业”，跳转到新建作业界面。

- 作业基本信息

输入信息包括：作业名、定时执行表达式、备注

规则范围：全部主机、自定义范围（选择业务组、指定主机 IP）

是否启用：启用禁用作业

- 检测项信息

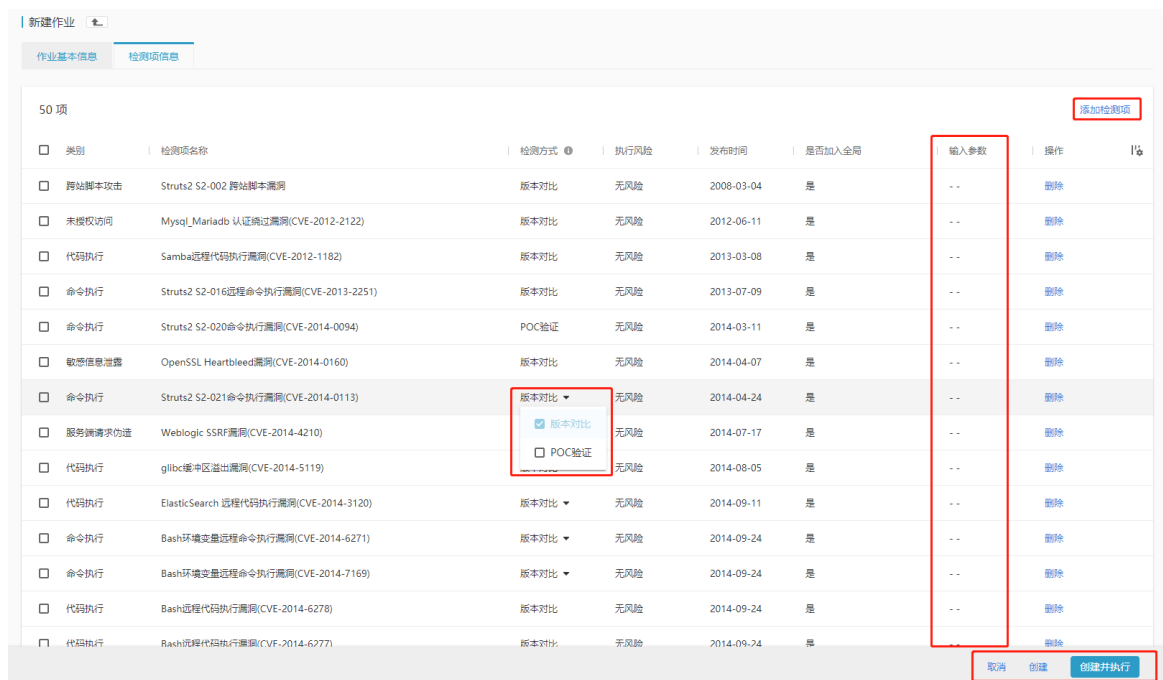
添加检测项：点击“添加检测项”，弹出检测项弹窗，选择检测项。不同检测项可选择不同的检测方式（版本比对、POC 验证）

创建并执行：创建并执行该作业，回到作业管理页面

输入参数：有些检测项需要输入特定的参数，当某个检测项需要输入参数时，对应输入参数一栏将出现参数按钮，点击后弹出输入参数弹窗，可填写用于该检查项的参数 b

创建：创建该作业，回到作业管理页面

取消：取消创建作业，回到作业管理页面



3.2.3.5 白名单规则

漏洞视图和主机视图下均有“更多”按钮，点进“白名单规则”即可进入白名单规则页面。



- 新建白名单规则

条件列表包括：漏洞名称中包含，漏洞特征（本地漏洞、远程利用）

各个复选框之间为且的关系

规则范围：全部主机、自定义范围（选择业务组、指定主机 IP）

描述：新建时自动生成，也可手动更改

新建白名单规则

新建规则

条件列表：

- 漏洞名中包含：
- 漏洞特征：

则将风险项加入白名单

使用范围：

- 全部主机
- 自定义范围
 - 业务组：
 - 主机：

描述：

- 编辑规则：编辑已有规则。
- 删除规则：删除已有规则。
- 查看受影响对象：点击“查看详情”跳转到“规则受影响对象”界面

规则受影响对象

9 项

<input type="checkbox"/>	危险程度	漏洞名称	主机IP	业务组
<input type="checkbox"/>	高危	Ghostscript命令执行(沙箱逃逸)漏洞(CVE-2018-15910)	192.168.122.1	product
<input type="checkbox"/>	高危	Linux内核本地提权(脏牛)漏洞(CVE-2016-5195)	192.168.167.129	ops
<input type="checkbox"/>	高危	glibc本地权限提升漏洞(CVE-2018-1000001)	192.168.122.1	product
<input type="checkbox"/>	高危	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	192.168.122.1	product
<input type="checkbox"/>	高危	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	192.168.1.132	Ybkuo
<input type="checkbox"/>	高危	MySQL、MariaDB本地权限提升漏洞(CVE-2016-6664)	192.168.167.129	ops
<input type="checkbox"/>	高危	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	192.168.167.129	ops
<input type="checkbox"/>	高危	Sudo本地权限提升漏洞(CVE-2017-1000367)	192.168.167.129	ops
<input type="checkbox"/>	高危	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	192.168.192.24	未分组主机

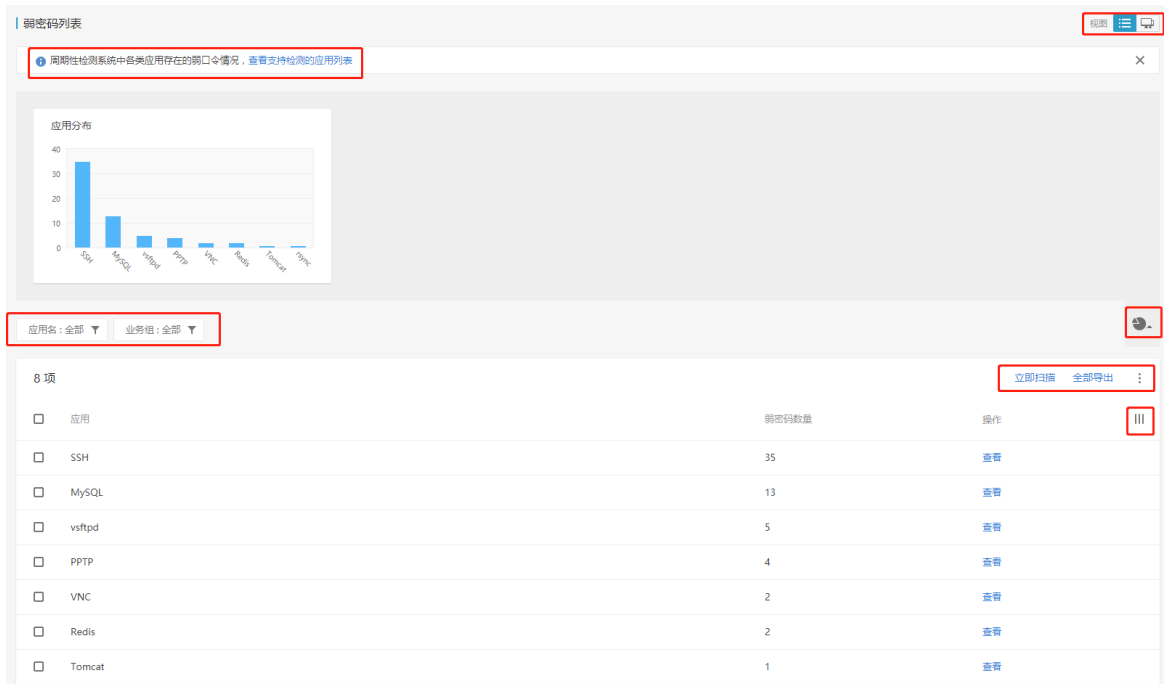
3.2.4 弱密码

弱密码检查用于检查系统中所有弱密码问题，其包括操作系统，应用，Web 站点等，该功能以一个统一的方式配置，检查，展示用户所有的弱密码问题。检查应用存在的弱密码，目前支持的应用类型有：MySQL, PPTP, VNC, SSH, OpenVPN, rsync, Redis, vsftpd, Tomcat, ProFTPD, influDB, SVN, OpenLDAP, Tomcat, Jenkins, Weblogic

3.2.4.1 弱密码检查方式

- 被动检查：用户的密码可以通过一定的方式获得，直接验证账户密码是否为弱密码；验证方式存在以下几种：
- 明文密码检查：密码为明文或可解密为明文，匹配弱密码字典是否为弱密码；

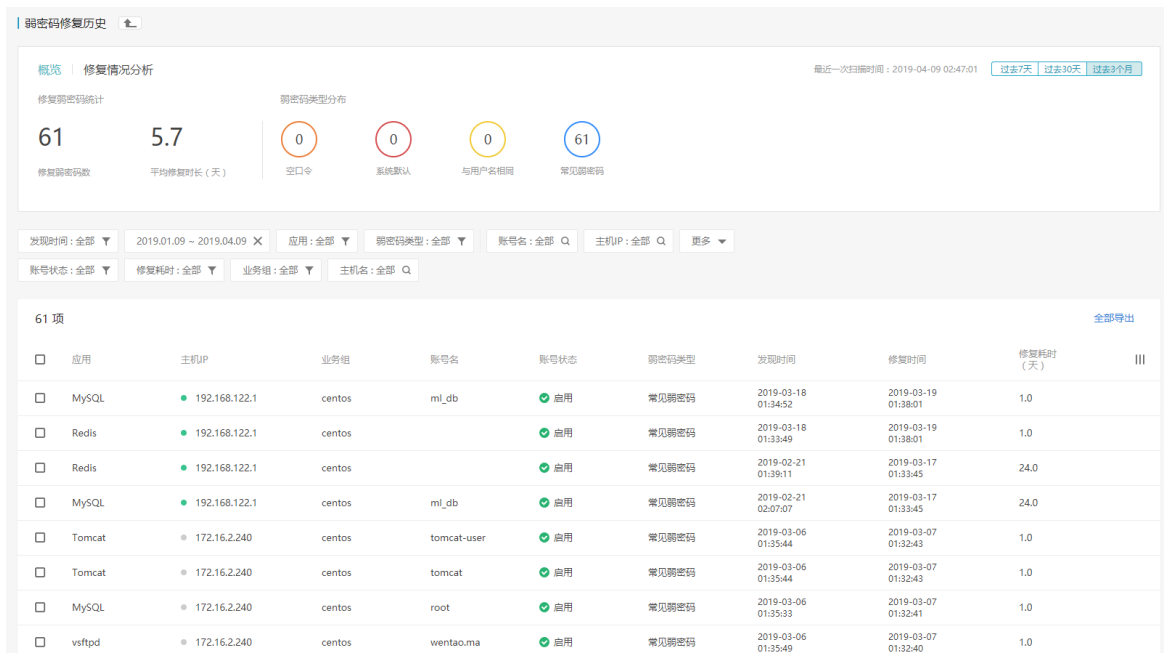
- 哈希密码匹配：密码为哈希计算后保存，在获得哈希类型后，对弱密码字典进行哈希计算，匹配是否为弱密码；
- 主动检查：无法直接获取密码，使用用户的登陆接口主动尝试密码，通常为在线爆破，进行弱密码检查；



3.2.4.2 修复历史

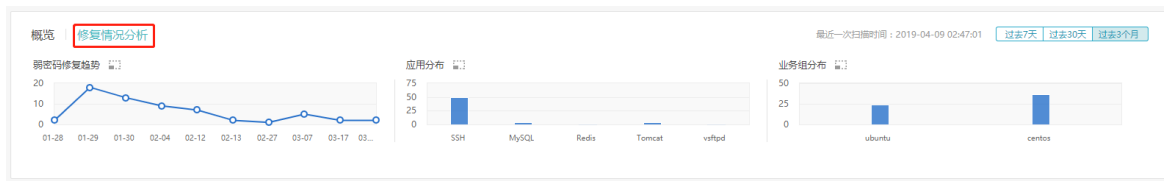
单击右侧 按钮可以看到修复历史、白名单规则、简单密码词典、组合密码词典三个选项。

➤ 修复历史



选定统计时间：点击右上角的时间按钮，可查看过去 7 天、过去 30 天、过去 3 个月内的修复历史统计情况

修复情况分析： 点击统计面板 TAB “修复情况分析” 可查看选定时间内的修复情况分析



3.2.4.3 白名单规则

单击首页右侧 按钮进入白名单规则页面。



➤ 新建白名单规则

白名单规则说明

规则	说明
条件列表	应用包含：用户自定义，输入弱密码的应用名称 应用账号中包含：用户自定义，输入弱密码应用的账号。 账号状态：不可登陆和启用 2 个可选项。 弱密码类型：空口令、系统默认弱密码、密码与用户名相同、常见弱密码 4 个可选项。
规则范围	让用户设置一些 IP 范围，将针对在设置的 IP 范围内的主机的弱密码过滤，设置范围有以下几种方式： 全部主机 自定义范围（业务组主机，单独 IP 主机）


➤ 编辑白名单规则



➤ 删除白名单规则



3.2.4.4 简单密码字典

单击右侧  按钮选择简单密码词典选项。简单密码字典用户检查用户的密码设置为该密码字典中的任意密码，则判定为弱密码。

- 编辑字典： 用户手动一一录入弱密码，每行一个弱密码，编辑框中提供了行号提示弱密码数量；
- 导入字典： 用户可导入弱密码字典，仅支持 **txt** 格式，需以换行分隔，每行均将识别为一个弱密码；仅识别前 **3000** 行，其后将完全忽略；每次导入将完全覆盖原密码设置；
- 导出字典： 用户可将当前存储的所有简单弱密码直接导出为 **txt** 格式，在自行编辑后，再导入系统；



3.2.4.5 组合密码字典

组合密码指组合密码特征进行弱密码检测的字典

本功能当前仅支持前缀+连接符+后缀的组合密码；

密码三部分将自动增加任意部分为空的检测；前缀将自动增加用户名的检测；

前缀最多可添加 **8** 个，连接符 **9** 个，后缀 **19** 个，均使用换行符隔开

例如，检测某账号：**admin**；

动态密码字典： 前缀为 **abc**；连接符为 **@**；后缀为 **123**

则将检查如下弱密码：**admin@123**；**admin@**；**admin123**；**admin**；**abc@123**；**abc123**；

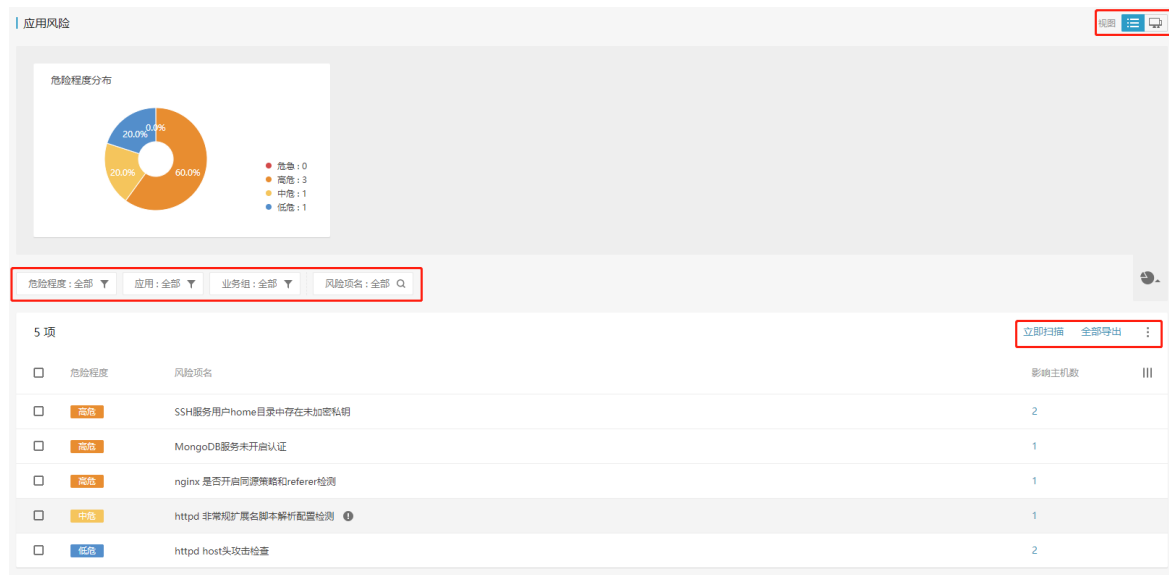
abc@；**@123**；**abc**；**@**；**123**；

截图如下：



3.2.5 应用风险

检查应用的安全配置，目前支持的应用有：JDWP、Jboss、Tomcat、CVS、ElasticSearch、VNC、SVN、redis、apache、apache2、mysql、ssh、ntp、rsync、nginx、mongoDB、Squid、openVPN、Bind、vsftp、NFS、NTP、Memcache、ssh

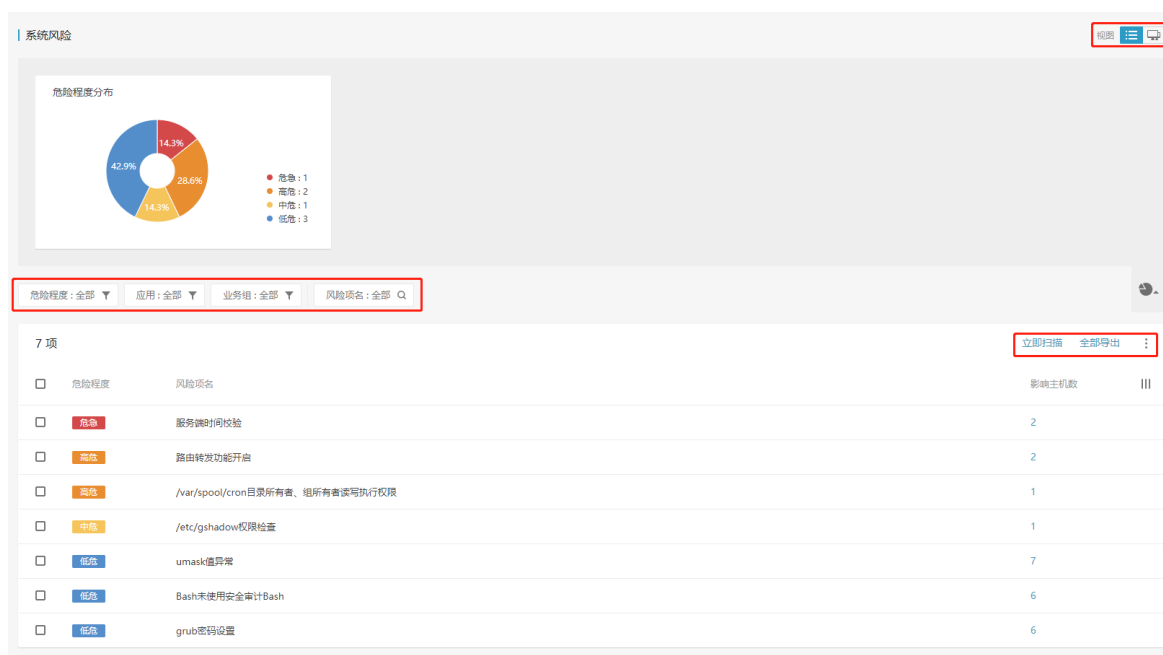


3.2.6 系统风险

3.2.6.1 功能描述

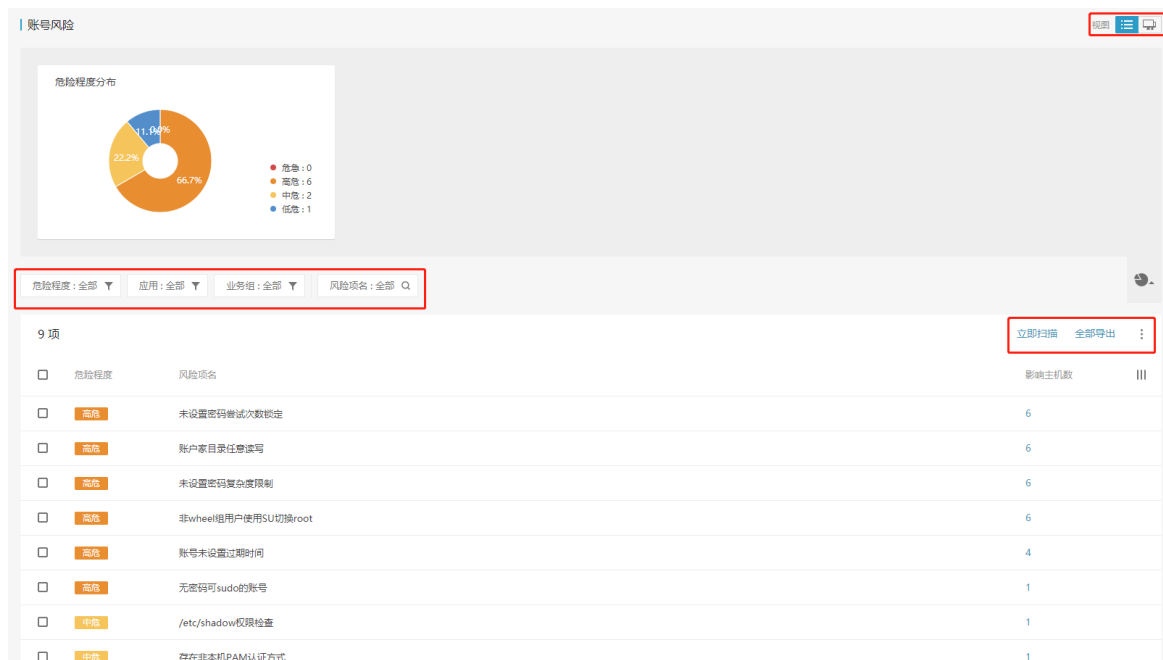
检查系统安全配置，有风险项视图/主机视图两种查看方式。可以导出所有/部分检查结果。

3.2.6.2 页面截图



3.2.7 账号风险

检查系统账号所存在的风险项，通常通过修改配置文件完成修改。有风险项视图/主机视图两种查看方式，可以导出所有/部分检查结果。



3.2.7.1 白名单规则

- 新建白名单规则

白名单规则说明

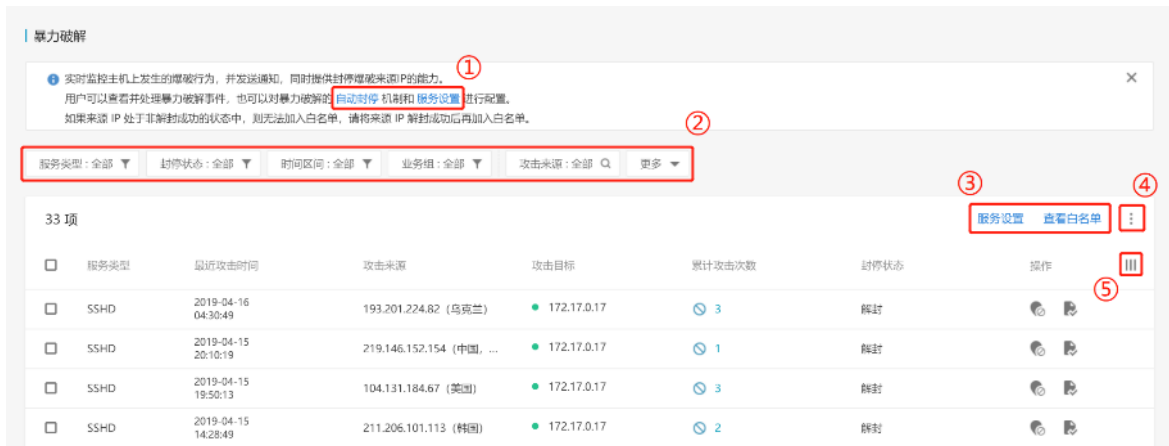
规则	说明
条件列表	<p>风险名中包含：用户自定义输入要加入白名单的风险名称</p> <p>风险的危害程度：有危急、高危、中危、低危 4 个可选项，用户可根据实际情况选择</p>
规则范围	<p>让用户设置一些 IP 范围，将针对在设置的 IP 范围内的主机 Web 目录下的文件进行白名单规则过滤，设置范围有以下几种方式：</p> <p>全部主机</p> <p>自定义范围（业务组主机，单独 IP 主机）</p>

- 编辑白名单规则

- 删除白名单规则

3.3 入侵检测

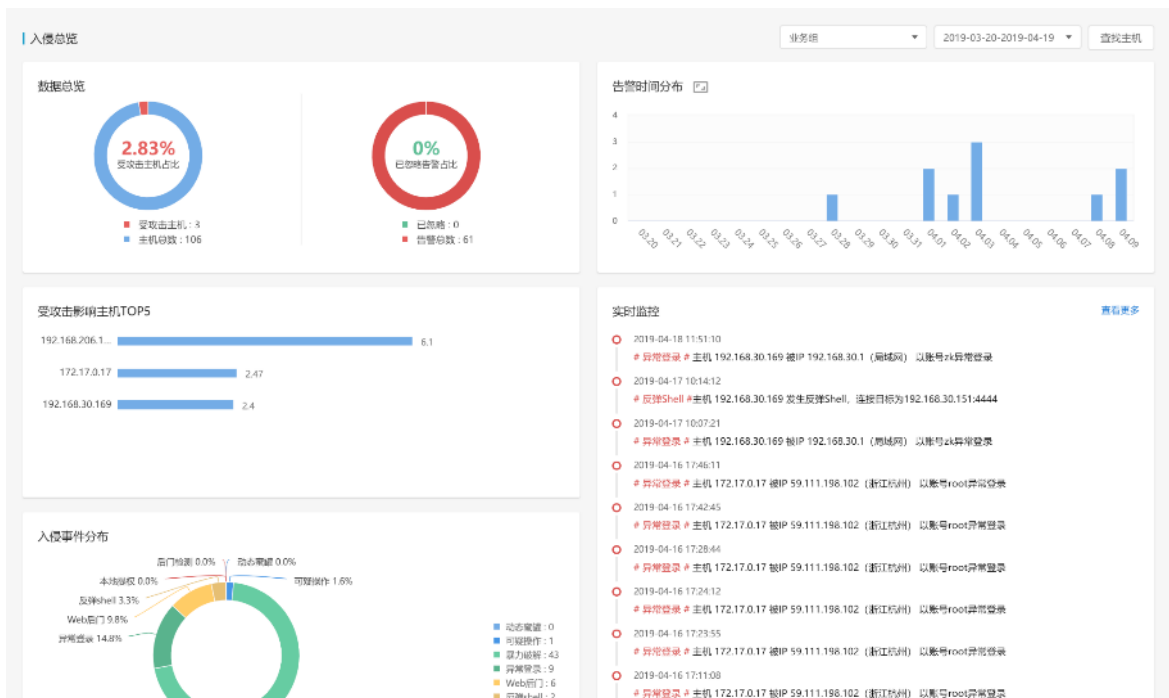
通用操作描述，以暴力破解页面为例：



- ① 功能快捷入口按钮：页面上方提示中，蓝色可点击文字按钮为功能快速入口，点击后可直接跳转至该功能主界面；
- ② 条件筛选框：点击各项筛选项，可根据筛选项支持的方式筛选出对应的数据；
- ③ 功能按钮：点击对应的按钮，可跳转至该功能主界面；
- ④ 更多设置按钮：点击 按钮，显示全部功能按钮；
- ⑤ 设置显示列按钮：点击 ，可设置显示列，控制列表中的数据显/隐藏。

3.3.1 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：

- ① 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；
- ② 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；
- ③ 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；
- ④ 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。

3.3.2 暴力破解

暴力破解用于阻止各类关键应用被暴力破解，尝试登录的行为，防止登录账户被爆破。目前支持 vsftpd 或者 sshd 两个服务的检查。

服务类型	最近攻击时间	攻击来源	攻击目标	累计攻击次数	封停状态	操作
SSHID	2019-04-16 04:30:49	193.201.224.82 (乌克兰)	172.17.0.17	3	封停	
SSHID	2019-04-15 20:10:19	219.146.152.154 (中国, ...)	172.17.0.17	1	封停	
SSHID	2019-04-15 19:50:13	104.131.184.67 (美国)	172.17.0.17	3	封停	

手动解封按钮

手动封停按钮

加入白名单按钮

用户可以选择手动将一条暴力破解记录加入白名单。加入以后这条记录将成为一条规则，这条规则由该暴力破解的登录时间、登录 IP、登录区域三个条件以与关系结合成规则。该规则的适用范围为这条记录的主机 IP。

暴力破解封停条件说明：

条件	说明	时间周期	登录次数N	封堵时间(分钟)	说明
q1	相同IP下同一用户名登录N次	1	6	1	启用
q2	N个IP下同一用户名登录	1	5	1	废弃不用
q3	相同IP下N个不存在的用户名登录	5	3	1	启用
q4	指定时间内重试达到指定N次	10	19	1	启用

单击  按钮，可以看到自动封停设置、主机配置检测、全部导出三个选项。

3.3.2.1 查看攻击记录

点击暴力破解事件列表中各项记录的  按钮，可查看该事件聚合的攻击记录详情。

攻击记录列表[96]

攻击时间	攻击详情	处理结果
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理

[确定](#)

3.3.2.2 服务设置

进入服务设置列表，可以根据需要选择 vsftpd 或者 sshd 两个服务的开启关闭状态。点击“查看主机配置情况”的按钮可跳转至主机配置检测页面，详见 3.3.2.4 主机配置检测。

服务设置列表

是否开启	服务名	描述
<input checked="" type="checkbox"/>	VSFTPD	安全FTP服务
<input checked="" type="checkbox"/>	SSHD	登录服务

[查看主机配置情况](#) [确定](#)

3.3.2.3 查看白名单

选择“查看白名单”进入白名单规则列表。暴力破解白名单是为了将某些登录认定为正常登录而不是暴力破解去上报，防止一些不必要的上报和封停。

- 新建白名单规则

白名单规则设置

新建规则

条件列表:

- 攻击来源: 请选择攻击来源,可多选
添加
- 攻击时间: 请选择攻击时间
添加
- 攻击使用账号: 请输入账号名称,以逗号隔开

使用范围:

- 全部主机
- 自定义范围
 - 业务组: 请选择业务组
 - 主机: 请选择主机IP

描述: 用户“产品使用演示”于2018-10-30添加该白名单

创建 取消

白名单规则设置说明

规则	说明
条件列表	条件列表中各条件之间是与关系，必须满足所有条件才是正常登录。 攻击来源：设置某个 IP、IP 段或系统已有的 IP 组为正常登录 IP，添加方式包括手动添加、常用 IP 组导入； 攻击时间：设置一个或多个时间点为正常登录时间，登录时间设置方式星期加上起止时间； 攻击使用账号：用户手动填写一个或者多个账号。
规则范围	全部主机：指的是所以装有 Agent 的主机； 自定义范围：可以选择业务组与自己输入单台主机 IP 的复合结果。

- 编辑白名单

对于已经保存的单条规则，用户可以选择对其进行修改。

白名单规则修改后，同样需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被修改规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。

遍历数据的限制条件同新建白名单。

白名单规则列表

攻击来源: 所有 | 攻击使用账号: 所有 | 范围: 所有

2 项

规则	攻击来源	攻击时间	攻击使用账号	受影响设备	操作
<input type="checkbox"/>	10.44.188.101	140.205.201.32	--	0	编辑 删除
<input type="checkbox"/>	10.44.188.101	101.200.222.206	--	0	编辑 删除

- 删除白名单

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。在删除时，需要给用户删除确认提示，用户确认后方可删除。

白名单规则被删除后，同样需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被删除规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。

遍历数据的限制条件同新建白名单。



3.3.2.4 自动封停设置

开启该功能后，非内网的攻击主机会被自动封停，需要手动解封。



3.3.2.5 主机配置检测

检测各个服务在主机上的配置情况，可以根据需要导出主机配置信息进行处理。

重新检测：点击后可重新检测主机上的配置信息；

配置说明：点击后弹窗显示正确进行配置的引导信息；

导出：将当前列表内数据导出为文件，支持全部导出和手动勾选批量导出。




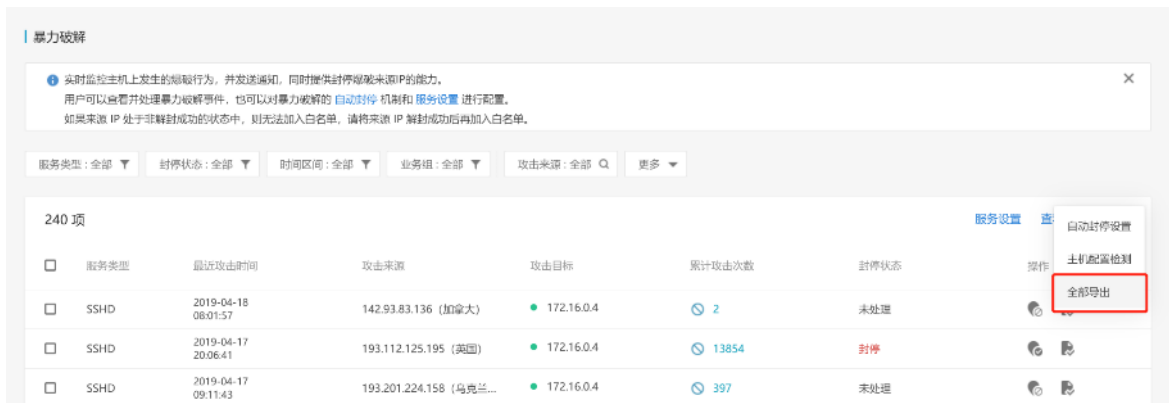
3.3.2.6 导出

暴力破解的数据导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。例如：用户会导出暴力破解数据用于特定的统计处理，对近期的检测数据进行存档等。选择的方式有以下两种：

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；



全部导出：单击  按钮选择“全部导出”。



3.3.3 异常登录

异常登录用于发现系统成功登录的信息中，包含非正常 IP，非正常区域，非正常时间，非常用账号的登录信息。



3.3.3.1 正常登录规则设置

单击“新建正常登录规则”按钮，进入到新建正常登录规则页面。

范围	登录IP	登录区域	登录时间	登录账号	受影响对象	操作
<input type="checkbox"/> 全部主机	10.10.10.1-10.10.10.10	--	--		查看详情	编辑 删除
<input type="checkbox"/> 全部主机	123.123.123.123	--	07:00-10:00(周日,周二,...)		查看详情	编辑 删除
<input type="checkbox"/> hao.yan	自定义内网ip组	--	--		查看详情	编辑 删除

- 新建正常登录规则

新建正常登录规则

新建规则

条件列表:

- 登录IP: 请选择登录IP,可多选 [添加](#)
- 登录时间: 请选择登录时间,可多选 [添加](#)
- 登录区域: 请设置登录区域 [设置](#)
- 登录账号: 请输入登录账号, 多个以英文逗号分开

使用范围:

- 全部主机
- 自定义范围
 - 业务组: 请选择业务组
 - 主机: 请选择主机IP

描述: 用户“演示”于2019-04-18新建的正常登录规则

[创建](#) [取消](#)

正常登录规则说明

规则类型	说明
规则的条件列表	<p>条件列表中各条件之间是与关系，必须满足所有条件才是正常登录。</p> <p>登录 IP：设置某个 IP、IP 段或系统已有的 IP 组为正常登录 IP，添加方式包括手动添加、常用 IP 组导入；</p> <p>登录时间：设置一个或多个时间点为正常登录时间，登录时间设置方式星期加上起止时间；</p> <p>登录区域：设置一些登录区域为正常登录区域，对于非中国地区只到国家层面，对于中国地区可以设置国家级、省级和市级。例子：中国、中国湖北、中国湖北武汉、美国、俄罗斯；</p> <p>登录账号：设置一个或多个认为是正常的登录账号，添加方式为手动输入。</p>
规则的适用范围	<p>规则范围是指以上条件的适用范围。</p> <p>规则范围有是以下两种方式里选择其中一种，且仅可以选择一种：</p>

- | |
|--|
| <ul style="list-style-type: none"> 1) 全部主机：指的是所以装有 Agent 的主机； 2) 自定义范围：可以选择业务组与自己输入单台主机 IP 的复合结果 |
|--|

- 编辑正常登录规则

对于已经保存的单条规则，用户可以选择对其进行修改。



- 删除正常登录规则

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。删除操作要有确认提示，用户确认后方可删除。



3.3.3.2 告警设置

提供内网异常登录的开关，可控制是否上报内网异常登录记录。



3.3.3.3 主机配置检测

与暴力破解的主机配置检测为同一功能，仅提供功能入口。详见 3.3.2.5 主机配置检测。


3.3.3.4 导出

异常登录的数据导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。例如：用户会导出异常登录数据用于特定的统计处理，对近期的检测数据进行存档等。

导出方式有以下两种：

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；



全部导出：单击  按钮选择“全部导出”。



3.3.4 反弹 Shell

反弹 Shell 用于监控主机中所有利用 Shell 进行反向连接的行为，例如黑客入侵了一台服务器后通过设置一个反向 shell 轻松地访问这台远程计算机等攻击行为，方便用户对主机中发生的反弹 Shell 行为进行查看、分析和处理。反弹 Shell 的目标如下：

- 通过实时监控发现反弹 Shell 行为，对用户进行事件告警，并能让其查看结果；
- 提供反弹 Shell 事件的详细信息，方便用户进行分析判断是否为反弹 Shell 事件；
- 提供对反弹 Shell 监控和上报的规则操作，方便用户对判断后的反弹 Shell 事件进行处理。



3.3.4.1 查看详情

点击反弹 Shell 事件列表中各项记录的“查看详情”按钮，可查看该事件的具体详情。

反弹shell详情

基本信息

发起连接主机: 192.168.30.162 发现时间: 2019-04-18 12:11:32
目标主机: 192.168.30.151 目标端口: 4444
标准I/O信息: --


连接进程信息

连接进程: python(20266) 运行用户: zk
进程路径: /usr/bin/python2.7 用户所属组: zk
父进程: bash(3349) 父进程路径: /bin/bash
进程树:

```
systemd(1) → sshd(2653) → sshd(2739) → sh(3229) → bash(3349) → python(20266) → sh(20299)
```

[确定](#)

3.3.4.2 查看白名单

单击  按钮，有查看白名单，全部导出 2 个选项，选择“查看白名单”选项，进入到白名单规则页面。



范围	进程树	连接进程	目标主机/端口	受影响记录	操作
<input type="checkbox"/> 10.104.11.223	--	--	47.94.244.178:4444	0	
<input type="checkbox"/> 10.8.8.8	--	--	124.53.128.76:3303	0	

[新建白名单规则](#)

- 新建白名单规则
单击“新建白名单规则”按钮进入到新建白名单规则页面。

新建白名单规则
↑

新建规则

名称:

条件列表:

连接进程:

进程树:

目标主机:

[添加](#)

目标端口:

[添加](#)

使用范围:

全部主机

自定义范围

业务组:

主机:

描述:

创建
取消

白名单规则设置说明

内容	说明
条件列表	<p>条件列表是具体的条件详细内容，条件之间为“与”关系。</p> <p>连接进程：下拉框选择单个连接进程，连接进程的选项和上报的反弹 Shell 进程联动，即仅上报后才能选择该进程作为白名单条件。</p> <p>进程树：填写进程树信息，多个进程树节点以英文逗号隔开，满足该进程树进行反弹的行为不会上报。</p> <p>目标主机&端口：连向的目标主机 IP 和端口号，IP 可添加 IP、CIDR 和 IP 段，端口号可添加多个端口。</p>
规则范围	<p>规则范围是指以上条件的适用范围。规则范围有是以下两种方式里选择其中一种，且仅可以选择一种：</p> <ol style="list-style-type: none"> 1) 全部主机。指的是所以装有 Agent 的主机。 2) 自定义范围。可以选择业务组与自己输入单台主机 IP 的复合结果。

白名单规则创建后将被立即执行，需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报。

遍历数据的限制条件如下：

遍历记录数量的上限为 10000 条；

若检测结果列表内记录超过上限，则只遍历近三个月的记录，上限同样为 10000 条。

- 编辑白名单规则

对于已经保存的单条规则，用户可以选择对其进行修改。

92



- 删除白名单规则

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。在删除时，需要给用户删除确认提示，用户确认后方可删除。



3.3.4.3 告警设置

提供内网告警的控制开关，可控制是否上报内网的反弹 Shell 记录。



3.3.4.4 导出

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；



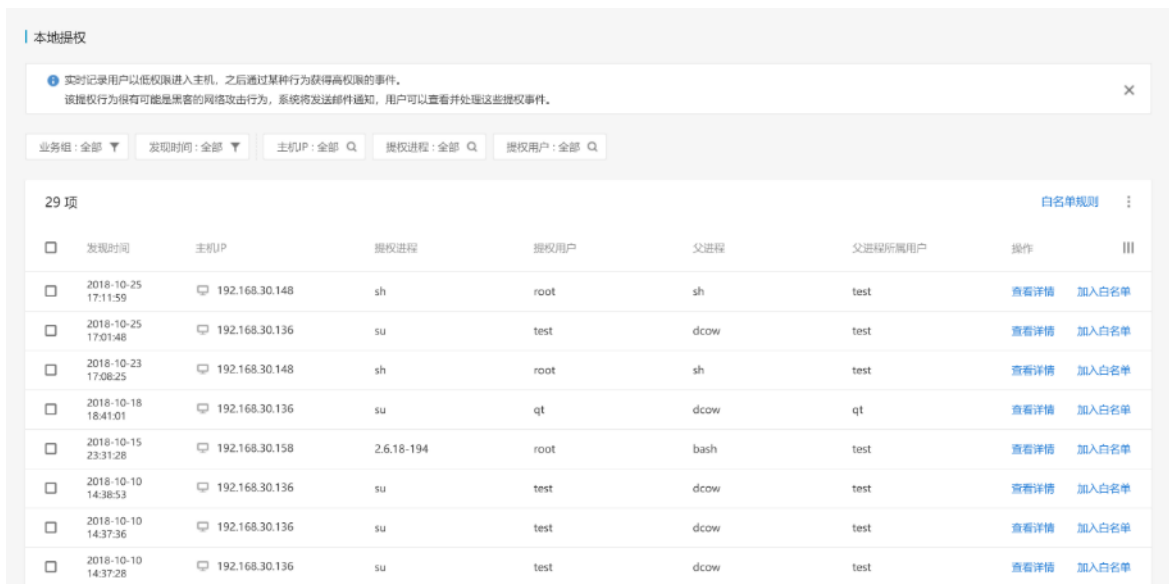
全部导出：单击 按钮选择“全部导出”。



3.3.5 本地提权

当用户以低权限进入主机系统，通过某种行为获得高权限时，该进程很有可能是黑客的网络攻击行为，威胁主机安全。本地提权功能用于对此类行为事件进行记录和统计。包含如下功能点：

- 提权事件记录：实时记录主机中存在的提权行为事件，在列表中查看并筛选/搜索相关信息；
- 白名单管理：对待定的主机和进程的提权行为，设置规则屏蔽；
- 导出功能。



3.3.5.1 白名单规则

单击白名单规则按钮，即可进入到“白名单规则”页面。

- 新建白名单规则

单击右侧“新建规则”按钮，进入到白名单规则设置页面。

白名单规则

范围: 全部 授权进程: 全部

范围	授权进程	是否为带s权限的进程	受影响对象	操作
<input type="checkbox"/> 192.168.192.20	sh	是	查看详情	编辑 删除
<input type="checkbox"/> 10.0.2.15	avahi-autoipd	否	查看详情	编辑 删除

白名单规则设置

新建白名单规则

如果符合下列: 所有条件

条件列表:

- 提权进程: 请输入进程名字, 以英文逗号隔开
- 带s权限的进程

使用范围:

- 全部主机
- 自定义范围
 - 业务组: 请选择业务组
 - 主机: 请选择主机IP

描述: 用户 "opstest" 于2018-10-26添加该白名单

[创建](#) [取消](#)

白名单规则设置说明

内容	说明
条件列表	条件列表是具体的条件详细内容。 提权进程: 以逗号隔开输入一个或者多个进程名字。 带 s 权限的进程: 是否是带 s 权限的进程。
规则范围	规则范围是指以上条件的适用范围。规则范围有是以下两种方式里选择其中一种, 且仅可以选择一种: 1) 全部主机。指的是所以装有 Agent 的主机。 2) 自定义范围。可以选择业务组与自己输入单台主机 IP 的复合结果。

白名单规则创建后将被立即执行, 需要重新遍历检测结果列表内的历史数据, 根据更新后的规则库判断, 对列表内的记录进行更新, 符合更新后规则的记录将不再显示上报。

遍历数据的限制条件如下:

遍历记录数量的上限为 10000 条;

若检测结果列表内记录超过上限, 则只遍历近三个月的记录, 上限同样为 10000 条。

- 编辑白名单规则

对于已经保存的单条规则, 用户可以选择对其进行修改。

白名单规则修改后, 同样需要重新遍历检测结果列表内的历史数据, 根据更新后的规则库判

断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被修改规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。
遍历数据的限制条件同新建本地提权白名单规则。



- 删除白名单规则

对于已经保存的单个或者多条规则，用户可以选择对其进行删除。在删除时，需要给用户删除确认提示，用户确认后方可删除。

白名单规则被删除后，同样需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被删除规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。


遍历数据的限制条件同新建本地提权白名单规则。



3.3.5.2 导出功能

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；



全部导出：单击  按钮选择“全部导出”。



3.3.6 后门检测

后门检测功能用于检测系统是否存在 Booitkit、Rootkit、应用后门、病毒木马等问题。其中

Bootkit、Rootkit 和应用后门依靠扫描来发现，病毒木马则通过实时监控进程来发现。目前病毒木马支持的规则库包括小红伞、ClamAV、青藤 Hash 库、青藤 Yara 库。

后门类型	说明	受感染主机	发现时间	隔离/删除状态	操作
LINUX/Setag...	发现LINUX/Setag.ztrec, 其对应运行进程: ps	192.168.105....	2019-04-10 10:06:18		查看详情 下载
LINUX/Setag...	发现LINUX/Setag.ztrec, 其对应运行进程: sshd	192.168.105....	2019-04-10 10:05:18		查看详情 下载
LINUX/Setag...	发现LINUX/Setag.ztrec, 其对应运行进程: getty	192.168.105....	2019-04-10 10:05:18		查看详情 下载
LINUX/Setag...	发现LINUX/Setag.ztrec, 其对应运行进程: ps	192.168.105....	2019-04-10 10:05:18		查看详情 下载
Rootkit	系统检测ssh命令可执行文件中含有'^/bin/.sh\$'内容, 请尽快确认	192.168.105....	2019-03-07 03:40:47		查看详情 下载
Rootkit	系统检测ssh命令可执行文件中含有'^/bin/.sh\$'内容, 请尽快确认	192.168.105....	2019-03-07 03:40:47		查看详情 下载

筛选框：可以通过业务组，后门类型，检查功能，检查项，主机 IP，主机名进行筛选；详情按钮可以查看到对应后门的检测说明（包含问题原因和修复方法）和静态信息（即文件基本详情，包含被篡改文件的文件名、文件校验码、创建时间、修改时间和文件权限等信息）；点击加入白名单按钮，手动将该条报警加入白名单，不再提示。

3.3.6.1 重新检测

重新检测包括两个方面的功能，其一是重新扫描所有管理主机中是否存在 Bootkit、Rootkit 和应用后门，其二是检测已经发现的病毒木马是否依然存在。重新检测后的数据会和当前列表中的数据进行了对比，如果不存在的数据会进入到修复历史中去。

3.3.6.2 导出

导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；

后门类型	说明	受感染主机	发现时间	操作
<input checked="" type="checkbox"/> LINUX/Setag.ztrec	发现LINUX/Setag.ztrec, 其对应运行进程: ps	192.168.105.142	2019-04-10 10:06:18	查看详情 下载
<input checked="" type="checkbox"/> LINUX/Setag.ztrec	发现LINUX/Setag.ztrec, 其对应运行进程: sshd	192.168.105.142	2019-04-10 10:05:18	查看详情 下载
<input type="checkbox"/> LINUX/Setag.ztrec	发现LINUX/Setag.ztrec, 其对应运行进程: getty	192.168.105.142	2019-04-10 10:05:18	查看详情 下载
<input type="checkbox"/> LINUX/Setag.ztrec	发现LINUX/Setag.ztrec, 其对应运行进程: ps	192.168.105.142	2019-04-10 10:05:18	查看详情 下载
<input type="checkbox"/> Rootkit	系统检测ssh命令可执行文件中含有'^/bin/.sh\$'内容, 请尽快确认	192.168.105.136	2019-03-07 03:40:47	查看详情 下载
<input type="checkbox"/> Rootkit	系统检测ssh命令可执行文件中含有'^/bin/.sh\$'内容, 请尽快确认	192.168.105.136	2019-03-07 03:40:47	查看详情 下载

全部导出：单击 按钮选择“全部导出”。

系统后门


发现时间: 全部 | 后门类型: 全部 | 危险等级: 全部 | 业务组: 全部 | 主机IP: 全部 | 更多

32 项

后门类型	说明	被感染主机IP	发现时间	操作
Rootkit	通过检测strings命令成功后, 利用strings...	192.168.192.111	2018-08-03 03:31:14	详情 加入白名单
Rootkit	通过检测strings命令成功后, 利用strings...	192.168.29.131	2018-08-15 03:32:56	详情 加入白名单
Rootkit	通过检测strings命令成功后, 利用strings...	192.168.29.131	2018-08-15 03:32:56	详情 加入白名单

修复记录
全部导出
查看白名单

3.3.6.3 查看白名单


单击  按钮，有全部导出和查看白名单两个选项，选择“查看白名单”选项，可以查看到所有手动添加到白名单的记录。

系统后门白名单

检查项	主机IP
检查"/bin/chsh"命令	192.168.192.119
检查"/bin/tar"命令	192.168.192.20
检查"/bin/tar"命令	10.0.2.15
检查"/usr/bin/chsh"命令	192.168.19.128
检查"/usr/bin/chsh"命令	192.168.197.27

确定

3.3.6.4 修复记录

单击  按钮，选择“修复记录”选项，可以查看到所有曾经存在过，但是现在已经不存在的系统后门的记录。

修复记录

发现时间: 全部 | 修复时间: 全部 | 后门类型: 全部 | 危险等级: 全部 | 说明: 全部 | 更多

1 项

发现时间	修复时间	后门类型	说明	主机IP	操作
2018-09-12 17:27:07	2018-10-29 10:41:00	Rootkit	系统检查ssh命令可执行文件...	192.168.192.203	查看详情

3.3.6.5 查看详情

点击【查看详情】按钮，可以看到该后门的详细内容，包括基本信息、检测说明、静态信息、进程信息。

确认 LINUX/Setag.ztrec

基本信息

感染主机: 192.168.105.142
命令规则: 1
对应文件: /bin/ps

发现时间: 2019-04-10 10:06:18
运行进程: ps
SHA256: b743c1c5960107a8c45f9dab4f234a646ee0003b5771b8f8440144357f7f71ce

检测说明 静态信息 进程信息

检测率	病毒名称	说明	修复方法	更新时间	
	Avira	LINUX/Setag.ztrec	Contains detection pattern of the Linux virus LINUX/Setag.ztrec	删除文件	2018-08-23 00:00:00

确认 LINUX/Setag.ztrec

基本信息

感染主机: 192.168.105.142
命令规则: 1
对应文件: /bin/ps

发现时间: 2019-04-10 10:06:18
运行进程: ps
SHA256: b743c1c5960107a8c45f9dab4f234a646ee0003b5771b8f8440144357f7f71ce

检测说明 静态信息 进程信息

文件基本详情

文件类型: regular file
文件访问权限: 0755
文件大小: 1.17MB
文件所属用户: root
文件所属用户组: root
文件SHA1: 5ef34ed96c76816e7ba8d6a9b41b6a5896c5a5ad
文件MD5: 8aded0905989790e4b42cd72165dacb9
文件SHA256: b743c1c5960107a8c45f9dab4f234a646ee0003b5771b8f8440144357f7f71ce
状态修改时间: 2019-04-10 10:04:56
修改时间: 2019-04-10 10:04:56
最近访问时间: 2019-04-10 10:05:01

确认 LINUX/Setag.ztrec

基本信息

感染主机: 192.168.105.142
命令规则: 1
对应文件: /bin/ps

发现时间: 2019-04-10 10:06:18
运行进程: ps
SHA256: b743c1c5960107a8c45f9dab4f234a646ee0003b5771b8f8440144357f7f71ce

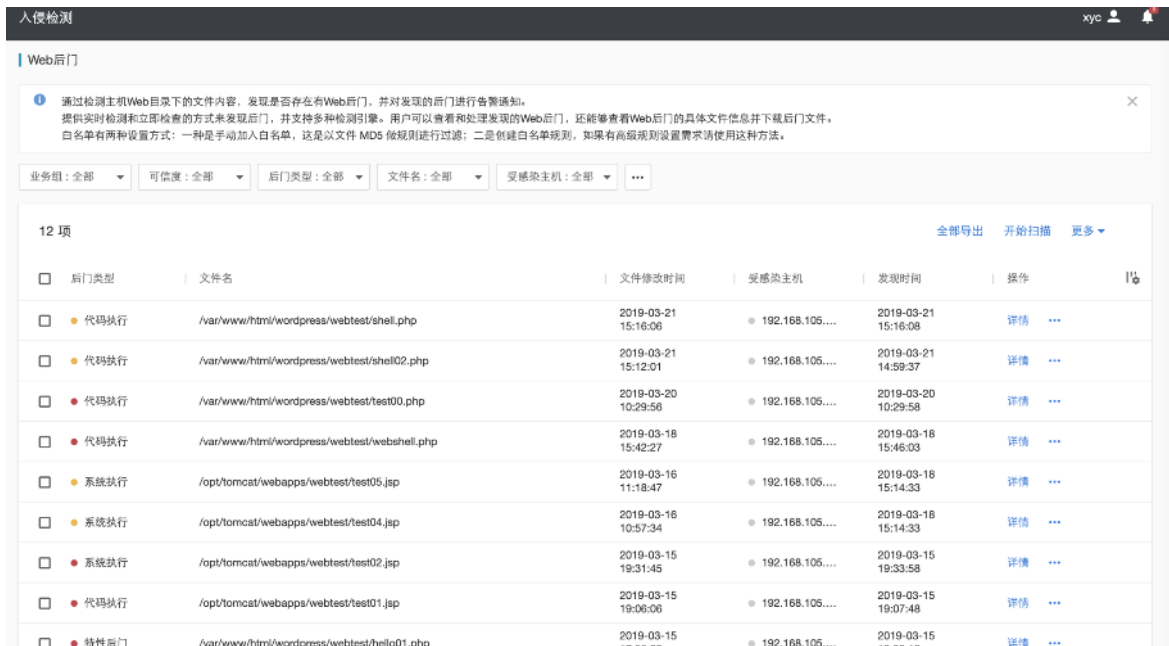
检测说明 静态信息 进程信息

基本信息


父进程: bash
父进程路径: /bin/bash
进程启动用户: root
进程路径: /bin/ps
用户所属组: bash

3.3.7 Web 后门

Web 后门用于检查 Web 网站中存在的后门文件，Web 后门文件为安全威胁检查中即为重要的一环。扫描分 2 种，触发式扫描，即点击界面，用户主动触发的扫描；每日定时扫描，每日定时进行的扫描。



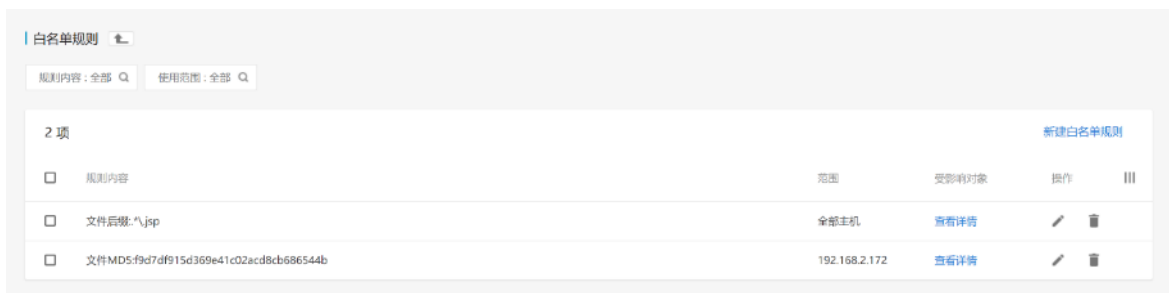
开始扫描按钮：即用户主动对单独该项进行扫描。

点击  按钮，有功能设置，查看白名单，修复记录、全部导出和自定义目录 5 个选项。

3.3.7.1 功能设置



3.3.7.2 查看白名单



- 新建白名单规则

新建白名单规则

新建规则

条件列表：
 文件MD5： 请输入文件MD5,只能输入一个
 自定义文件

文件目录： 请输入目录规则, 多个以英文逗号隔开
 文件后缀： 请输入正则表达式,用英文逗号分隔多个正则,如: *.jsp

则将Web后门加入白名单

使用范围：
 全部主机
 自定义范围

业务组： 请选择业务组
 主机： 请选择主机IP

描述：
 用户“演示”于2018-10-29添加该白名单

创建
取消

白名单规则说明

规则	说明
规则内容	<p>Web 后门白名单的规则内容可以由以下两个条件中的任意一条组成，两个条件为关系互斥。</p> <ul style="list-style-type: none"> • 文件 MD5。设置某些符合条件的文件 MD5 为正常文件 MD5，MD5 与之匹配的文件即视为正常文件，条件内容为文件的 MD5，由用户手动输入或手动添加白名单操作填入。 • 自定义文件。条件内容可以由以下两个条件中的任一条组成或多个条件以与关系组成。 <ul style="list-style-type: none"> • 文件目录。设置某些符合条件的文件目录为正常文件目录，该条件目录下的文件或者目录指向的文件即视为正常文件，条件内容为文件目录的正则表达式，由用户手动输入。 • 文件后缀。设置某些符合条件的文件后缀为正常文件后缀，带有该后缀的文件即视为正常文件，条件内容为文件后缀的正则表达式，由用户手动输入。
规则范围	<p>规则范围是用户自定义规则适用的范围，用户可以按照下面三种方式选择。</p> <ul style="list-style-type: none"> • 全部主机。所有安装 Agent 的主机。 • 自定义范围。可以选择业务组，也可以选择多台主机。

- 编辑白名单规则

对于已经保存的单条规则，用户可以选择对其进行修改。

- 删除白名单规则

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。

3.3.7.3 修复记录

可以查看到所有曾经存在过，但是现在已经不存在的 Web 后门的记录。

首次发现时间	修复时间	类型	主机IP	文件名	说明	域名	操作	III
2018-10-22 18:29:23	2018-10-22 18:29:41	代码执行	192.168.2.135	/var/www/html/web...	eval代码执行	www.example.com	🗑️	
2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	gzdeflate&base...	www.example.com	🗑️	
2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	GLOBALS GET POST ...	www.example.com	🗑️	
2018-10-15 14:38:55	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	间接变量调用	www.example.com	🗑️	

3.3.7.4 全部导出

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；

全部导出：单击 按钮选择“全部导出”。

3.3.7.5 自定义目录

用户可以根据实际情况设置需要额外扫描的目录。

监控目录	最近修改时间	应用范围	状态	操作	III
/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除	
/bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除	
/var/www/html/DirRoot1/testdir1	2018-10-08 19:57:46	192.168.100.162	同步成功	编辑 删除	
/var/www/html/DirRoot1/testdir1	2018-10-08 19:57:46	192.168.199.75	同步成功	编辑 删除	

- 新建自定义目录

新建自定义目录

如果增加监控目录过多，会增加系统性能消耗，所以请谨慎设置监控目录，建议监控目录不超过10个。

监控目录：

应用范围：

- 编辑自定义目录

监控目录	最近修改时间	应用范围	状态	操作
<input type="checkbox"/> 监控目录				
<input type="checkbox"/> /bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除
<input type="checkbox"/> /bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除

➤ 删除自定义目录

监控目录	最近修改时间	应用范围	状态	操作
<input type="checkbox"/> 监控目录				
<input type="checkbox"/> /bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除
<input type="checkbox"/> /bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除

3.3.7.6 查看详情

通过检测主机Web目录下的文件内容，发现是否存在有Web后门，并对发现的后门进行告警通知。提供实时检测和立即检查的方式来发现后门，并支持多种检测引擎。用户可以查看和处理发现的Web后门，还能够查看Web后门的具体文件信息并下载后门文件。白名单有两种设置方式：一种是手动加入白名单，这是以文件 MD5 做规则进行过滤；二是创建白名单规则，如果有高级规则设置需求请使用这种方法。

后门类型	文件名	文件修改...	受感染主机	发现时间	隔离/解除状态	操作
<input type="checkbox"/> 代码执行	/home/yangwu/wu/webshell/monitor/plugin.php	2019-02-25 14:18:29	172.16.2...	2019-02-26 14:20:35		详情 ...
<input type="checkbox"/> 已知后门	/home/yangwu/wu/webshell/monitor/getid15.php	2019-02-14 14:48:23	172.16.2...	2019-02-14 14:48:30		详情 ...
<input type="checkbox"/> 已知后门	/home/yangwu/wu/webshell/monitor/getid14.php	2019-02-14 14:41:23	172.16.2...	2019-02-14 14:41:28		详情 ...

点击【详情】按钮，可以查看这个 Web 后门的详细内容，包括基本说明、检测说明和基本信息。

Web后门 > 代码执行详情 加入白名单 下载文件

基本信息

感染主机: 172.16.2.188	发现时间: 2019-02-26 14:20:35
域名: --	可信度: 可疑
Web后门文件: /home/yangwu/wu/webshell/monitor/plugin.php	命中规则: 1
MD5: bb9c95148eda27df11628934ac5e3963	SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e8610c31d

检测说明 静态信息

类型	说明	
代码执行	攻击者可以利用该Web后门文件将字符串转换为脚本代码进行执行	收起 ^

```

41     return $arr;
42 }
43
44 function get_plugin($pluginname) {
45     $f = file_get_contents(UC_ROOT."/plugin/$pluginname/plugin.xml");
46     include_once UC_ROOT."/lib/xml.class.php";
47     return xml_unserialize($f);
48 }
49
50 function get_plugin_by_name($pluginname) {
51     $dir = UC_ROOT."/plugin/";
52     $s = file_get_contents($dir.$pluginname."/plugin.xml");
53     return xml_unserialize($s, TRUE);
54 }
55
56 function orderby_tabindex($arr) {
57     $arr2 = array();
58     $t = array();

```

Web后门 > 代码执行详情 加入白名单 下载文件

基本信息

感染主机: 172.16.2.188	发现时间: 2019-02-26 14:20:35
域名: --	可信度: 可疑
Web后门文件: /home/yangwu/wu/webshell/monitor/plugin.php	命中规则: 1
MD5: bb9c95148eda27df11628934ac5e3963	SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e8610c31d

检测说明 静态信息

文件基本详情

文件类型:	php
文件访问权限:	rw-rw-r--
文件大小:	2.5KB
文件所属用户:	yangwu
文件所属用户组:	yangwu
文件SHA1:	8c9e954561cd3c5e48554c8878928e44f10de7e0
文件MD5:	bb9c95148eda27df11628934ac5e3963
文件SHA256:	e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e8610c31d
状态修改时间:	2019-02-26 14:20:31
修改时间:	2019-02-25 14:18:29
最近访问时间:	2019-02-26 14:20:35

3.3.8 可疑操作

可疑操作记录执行的 shell 命令，您可以对操作进行筛选，也可以自定义规则发现可疑操作。该功能需要替换青藤 bash。

可疑操作

可疑操作记录执行的shell命令，您可以对操作进行筛选，也可以自定义规则发现可疑操作。当有可疑操作执行时，我们将发送邮件通知。

危险程度：全部 | 审核状态：全部 | 时间区间：全部 | 业务组：全部 | 命令内容：全部 | 更多

30 项

操作时间	命中规则	命令内容	操作主机IP	登录用户	登录IP	审核状态	操作
2018-09-06 07:36:11	nc rule	nc -l 4444	192.168.30.155	root	192.168.30.1 (局域网)	未审核	
2018-08-09 19:03:12	nc rule	nc -vv -l 1234	10.31.91.192	root	124.204.36.26 (中国北京)	审核通过	
2018-08-09 15:30:45	nc rule	nc -vv -l 1234	10.31.91.192	root	124.204.36.26 (中国北京)	审核未通过	

3.3.8.1 详情查看

单击 按钮，可以查看该条命令执行的日志详情

日志详情

操作主机IP: 192.168.30.155 操作时间: 2018-09-06 07:36:11
 登录用户: root 登录IP: 192.168.30.1 (局域网)
 执行命令用户: root 执行命令进程: bash
 实际执行命令进程: sshd 产生命令的登录终端(TTY): pts/2
 命令内容:

```
nc -l 4444
```

命中规则列表 [1]

规则名	危险程度	描述
nc rule	● 中危	--

[确定](#)

3.3.8.2 审核

单击 按钮，会出现“审核通过”和“审核不通过”两个选项，方便审计人员标记操作。

3.3.8.3 审计规则配置

审计规则包含用户自定义规则和系统规则两部分，系统规则为系统内置的审计规则，可选择是否开启使用，自定义规则由用户自行创建，并可进行编辑和删除等操作，具体如下：

➤ 开启/关闭规则

用户可以通过“是否启用”字段下的滑块按钮控制规则是否启用。



➤ 新建审计规则

用户可以自行配置审计规则，判定可疑操作。



审计规则说明

规则	说明
规则条件	<p>审计规则条件内容由以下三个条件组成。</p> <ol style="list-style-type: none"> 1) 规则名。规则的名称。 2) 正则表达式。用来匹配命令使用的正则表达式，仅支持填写一个。 3) 危险程度。用于标识规则的危险程度，有高危、中危、低危三个选项。
规则范围	<p>规则范围是用户自定义规则适用的范围，用户可以按照下面三种方式选择。</p> <ul style="list-style-type: none"> • 全部主机。所有安装 Agent 的主机。 • 自定义范围。可以选择业务组，也可以选择多台主机。

➤ 编辑审计规则



➤ 删除审计规则



3.3.8.4 环境变量配置

当用户使用堡垒机登录时，配置环境变量名称，即可看到真实登录 IP 而非堡垒机 IP。

自定义环境变量配置

登录IP*
请输入字段值

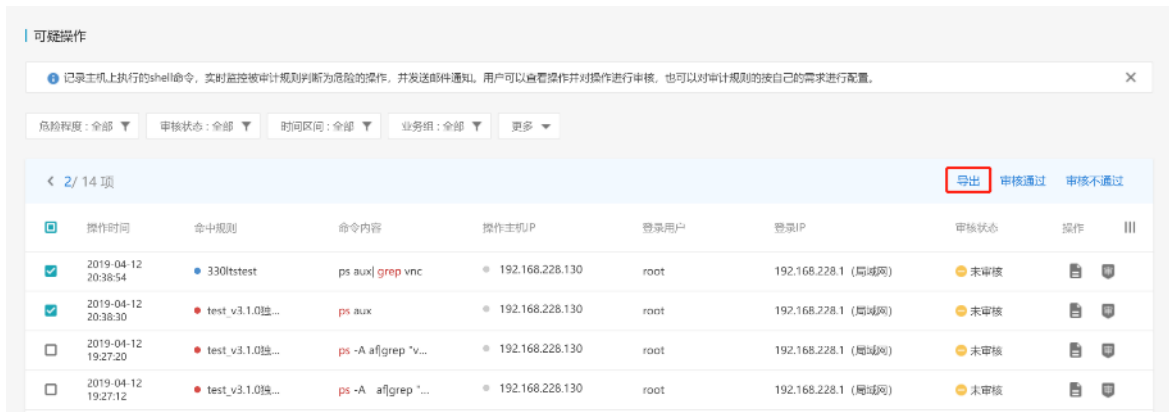
登录主机名*
请输入字段值


登录用户*
请输入字段值

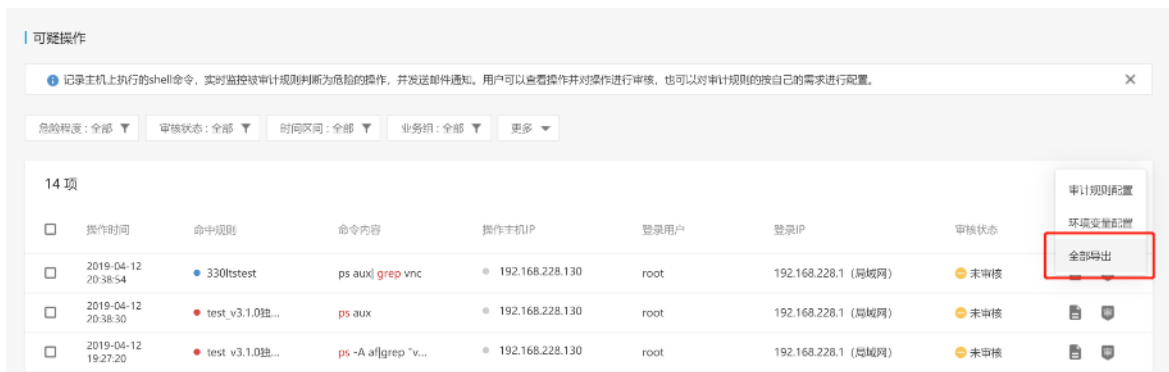
取消 确定

3.3.8.5 导出

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；

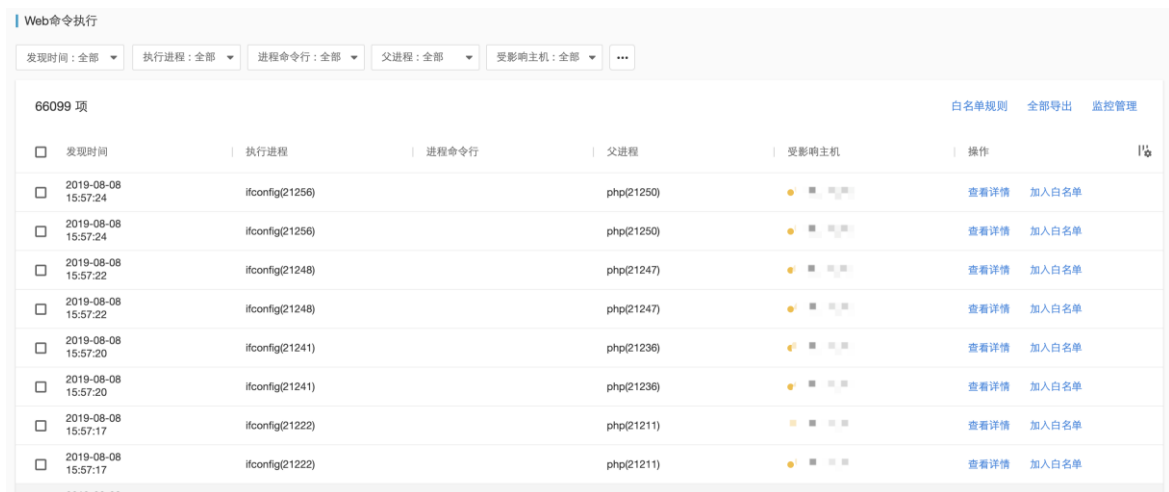


全部导出：单击  按钮选择“全部导出”。



3.3.9 Web 命令执行

Web 命令执行是黑客写入 Web 后门或者执行恶意操作的一种手段。因此，系统需要能够通过发现 Web 程序执行命令，帮助用户发现黑客行为。



3.3.9.1 详情查看

点击【查看详情】按钮，可以查看告警的详细信息。

基本信息

受影响主机: ■ ■ ■

执行命令: --

执行进程: ifconfig(21256)

父进程: php(21250)

进程树信息



关闭

3.3.9.2 监控管理

监控管理是用来设置账号管理主机是否开启该功能，支持批量开启和批量关闭的功能。需要注意的是，目前所有管理主机默认是不开启的。

监控管理



主机IP: 全部

监控状态: 全部

业务组: 全部

内网IP: 全部

125 项

[关闭监控](#) [开启监控](#)

主机IP	业务组	监控状态	操作
		禁用	<input type="checkbox"/>
		禁用	<input type="checkbox"/>
		禁用	<input type="checkbox"/>
		禁用	<input type="checkbox"/>
		禁用	<input type="checkbox"/>
	未分组主机	禁用	<input type="checkbox"/>
	未分组主机	禁用	<input type="checkbox"/>
	未分组主机	禁用	<input type="checkbox"/>
	未分组主机	禁用	<input type="checkbox"/>
		禁用	<input type="checkbox"/>
	未分组主机	禁用	<input type="checkbox"/>

关闭

开启监控



主机范围: 全部主机

业务组

主机

取消

确定

关闭监控



主机范围: 全部主机

业务组 请选择业务组 ▼

主机 请选择或输入主机IP ▼

取消

确定

3.3.9.3 白名单规则

对于用户认为正常的 Web 命令执行，用户可以通过设置白名单规则来进行管理。

条件列表：

* 父进程

* 执行进程

执行命令

主机范围：

全部主机

业务组

主机

备注：

取消

创建

白名单规则填写包括三个部分。

创建一条白名单规则的参数分为三个部分。

- 条件列表。
 - 规则的条件包括执行进程、父进程、执行命令三个参数。
 - 父进程和执行进程是必填的，执行命令是选填的。
 - 父进程和执行进程支持输入多个参数，以英文逗号隔开。
 - 匹配方式为严格匹配。
- 应用范围。
 - 应用范围有三个选择方式：全部主机、业务组、主机。
 - 业务组和主机支持选择多个。
- 备注。对于该白名单规则的备注，默认参数为：用户“XX”于 XXXX（年）-XX（月）-XX（日）新建的白名单规则。

3.4 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。

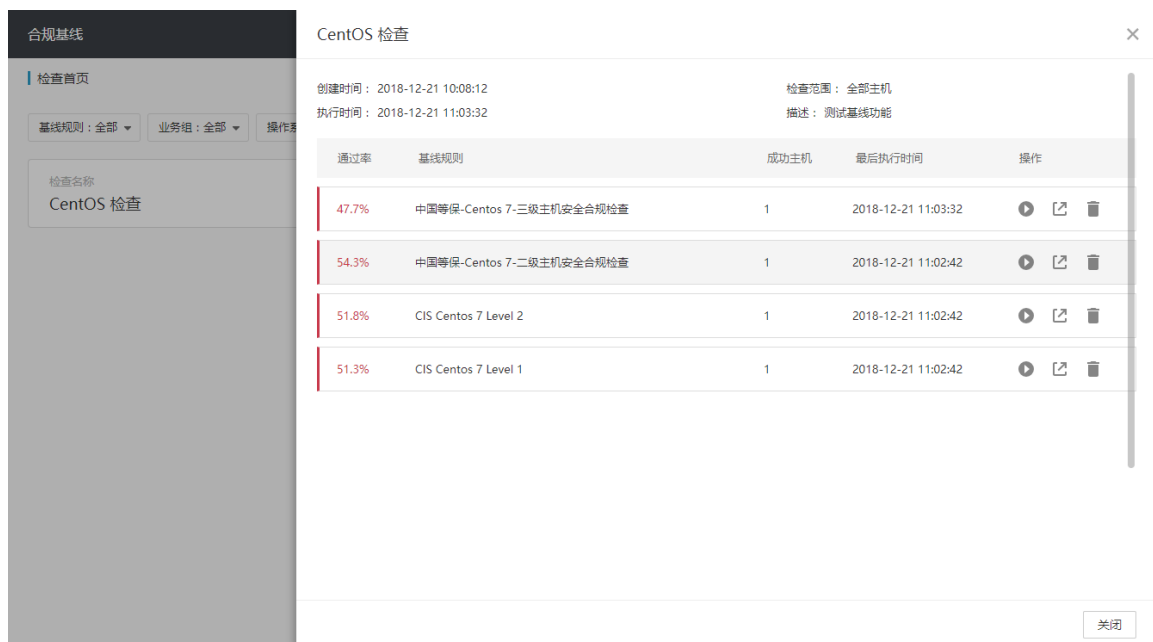


3.4.1 基线检查

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。

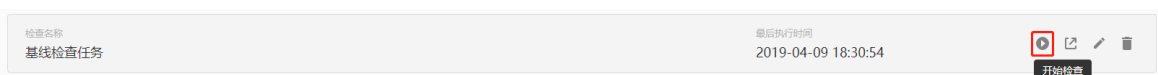
➤ 查看基线检查

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。



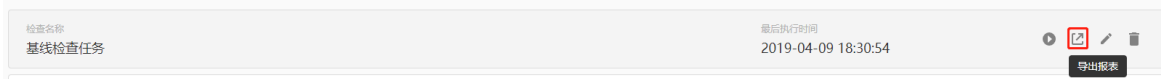
➤ 执行任务

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。



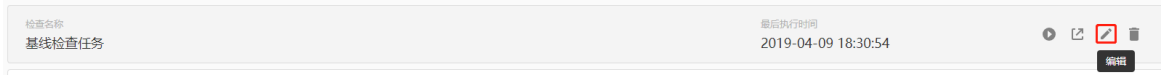
➤ 导出检查结果

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。



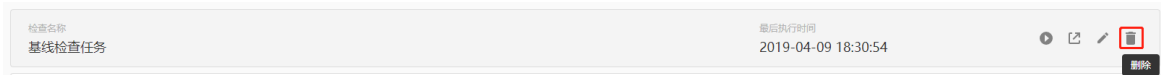
➤ 编辑任务

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。



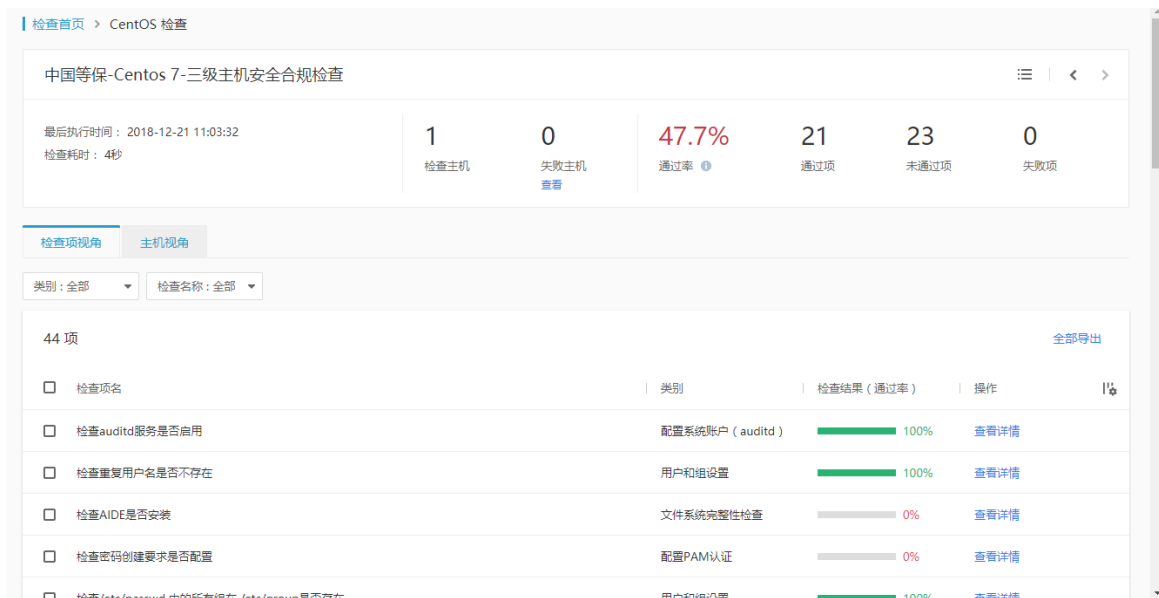
3.4.2 查看检查结果

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。

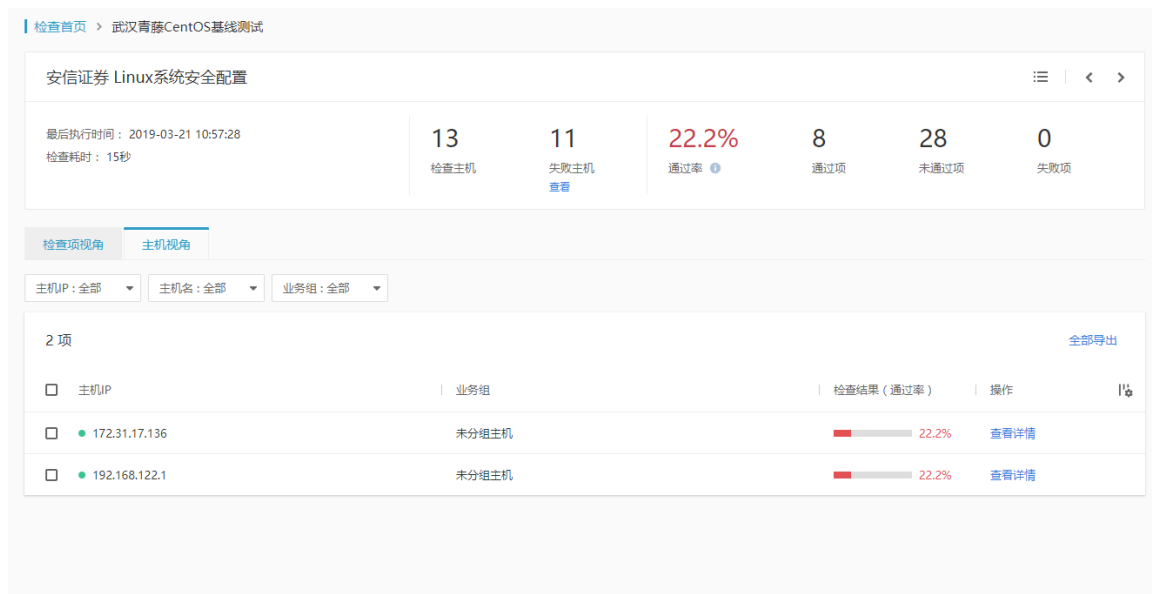


选择一台主机的结果并点击“查看详情”，可以看到该检查项在这台主机上的详细检查结果。其中包含了检查项名，检查内容，建议值和实际值等信息，帮助企业用户理解和合理设置。



➤ 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。



3.4.3 新建检查

单击“新建检查”按钮，进入新建检查页面。

检查首页 > 新建检查

检查信息

检查名称:

执行范围: 全部主机

选择业务组

选择主机

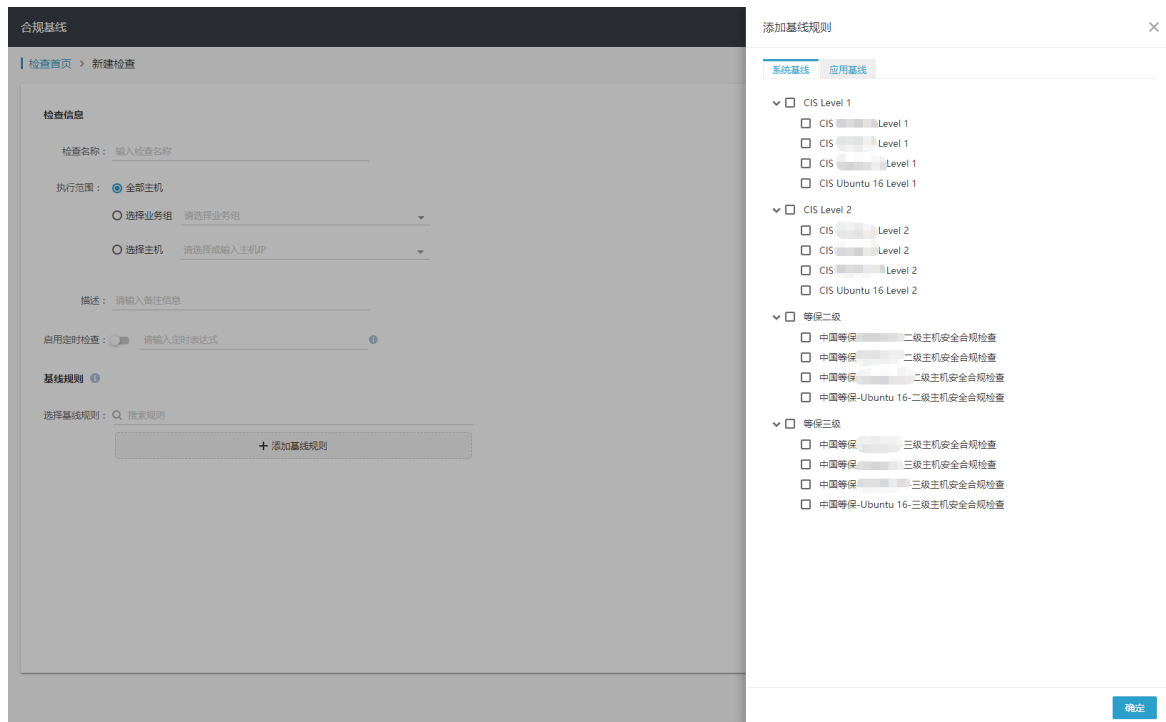
描述:

启用定时检查:

基线规则

选择基线规则:


➤ 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	<p>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</p> <p>【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。</p>
基线规则	<p>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</p> <p>【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</p> <p>目前支持的系统基线有：centos6/7 rhel6/7 ubuntu12/14/16</p> <p>支持的应用基线有：Apache Apache2 MySQL MongoDB Nginx</p>
定时检查	<p>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”。</p> <p>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。</p> <p>关闭定时检查开关，则不可以输入定时表达式。</p>
描述	输入对该基线的描述。

3.4.4 凭证管理

单击  按钮，选择“凭证管理”，输入账号密码后进入“凭证管理”页面。

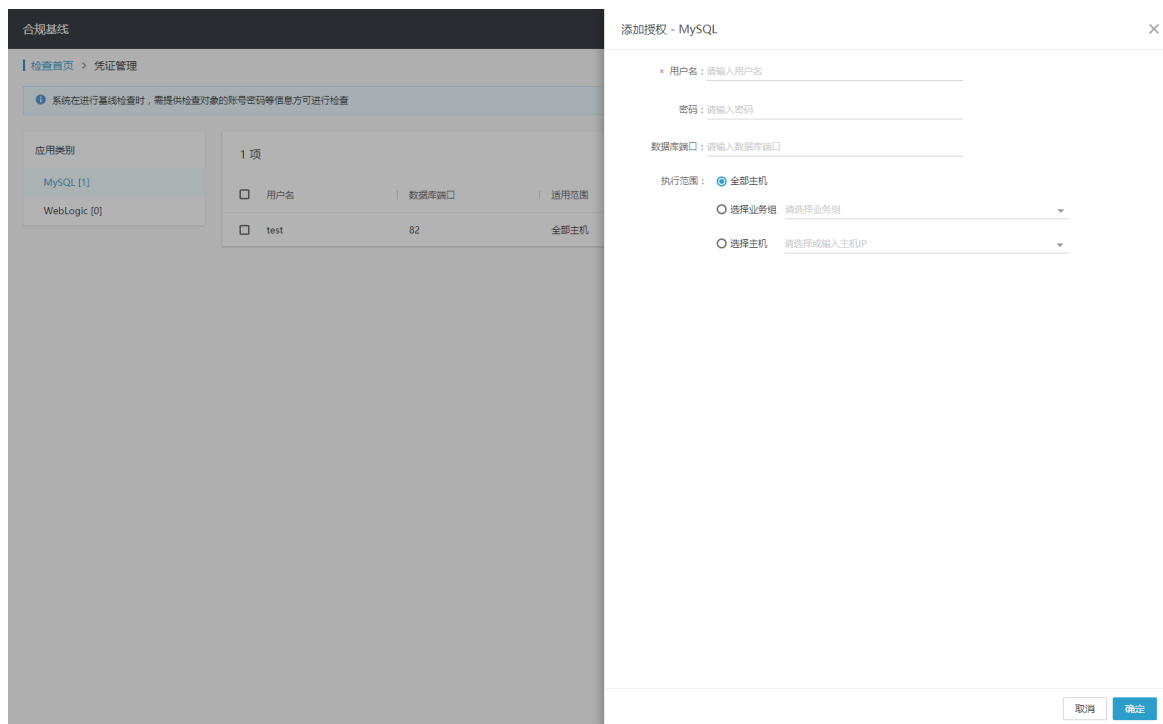


凭证管理管理的凭证用于对应的应用基线的检测。



➤ 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。



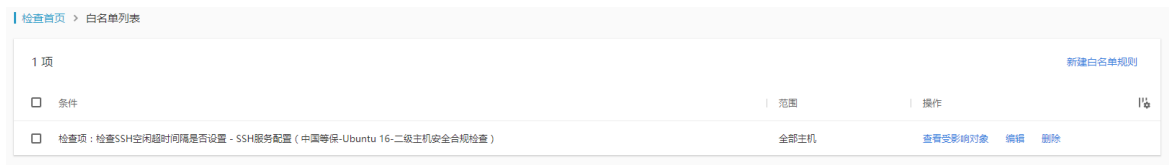
➤ 删除授权

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。



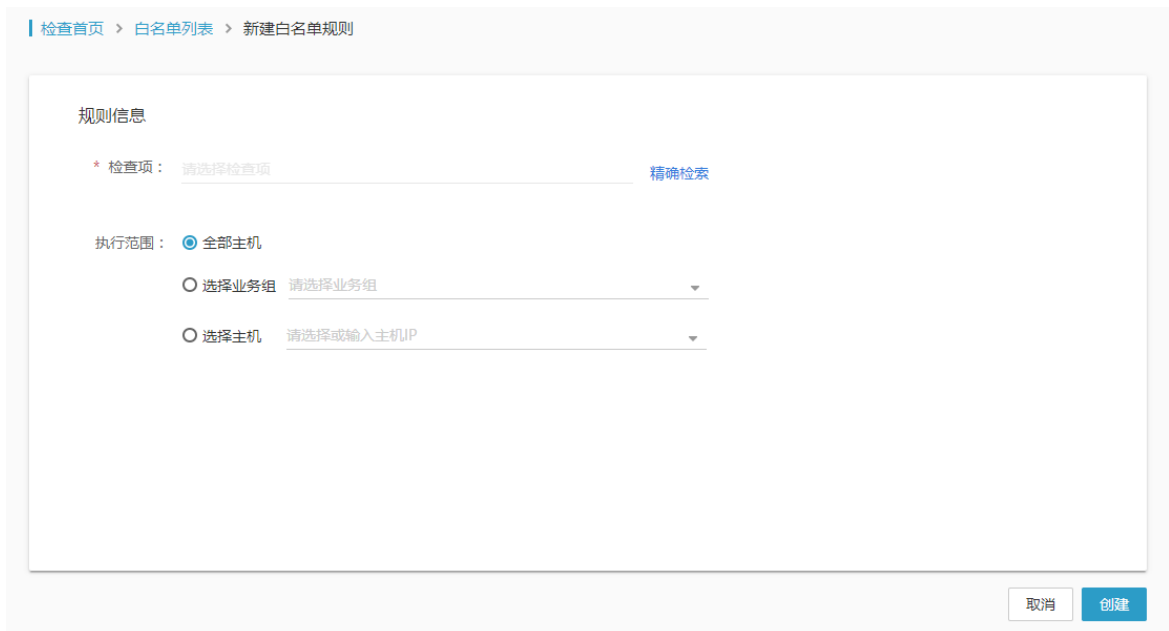
3.4.5 查看白名单

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。



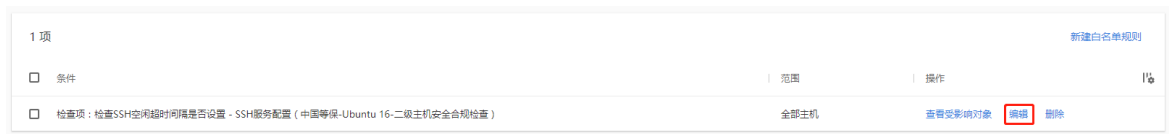
➤ 查看受影响对象

查看现有规则影响的对象。



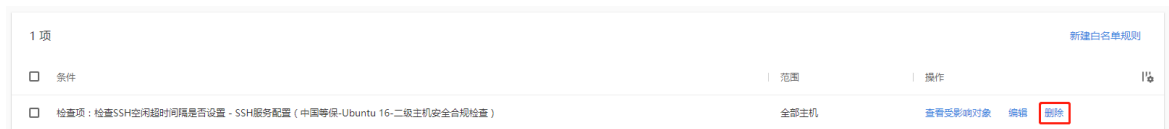
➤ 编辑白名单列表

对于已经保存的单条规则，用户可以选择对其进行修改。



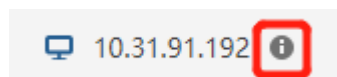
➤ 删除白名单列表

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。



3.5 单台主机详情

在整个产品功能中，点击“主机 IP”后按钮，即可进入“单台主机详情”功能，该功能是主机相关信息的汇总，方便用户对该主机中存在的问题，进行快速排查。



按功能类别可分为 4 个大模块：

- 主机资产：可查询主机基本信息和主机中所有资产信息；
- 安全风险：可查询主机中存在的所有风险；
- 入侵事件：可查询主机中发生的历史入侵事件；

主机信息	基本信息	管理信息	硬件配置	网卡信息
系统账号	主机名: sevck_linux	负责人: 拉拉	生产商: Alibaba Cloud	网卡名称: docker0
端口服务	内网IP: 10.31.91.192	负责人邮箱: zhangsan@qingfeng.cn	设备型号: Alibaba Cloud ECS	网卡名称: eth1
运行进程	外网IP: 121.42.182.208	机房位置: 03-0201	序列号: 507b98df-b687-42c3-a6a3-fa150f30c4d3	网卡名称: eth0
软件应用	操作系统: CentOS release 6.9 (Final),64-bit	备注: server组	设备UUID: --	MAC地址: f2:c4:d8:75:a3:63
Web服务	内核版本: 2.6.32-696.3.1.el6.x86_64		内存: 0GB, 使用率: 45.28%	IPV4: 192.168.42.1
Web站点	系统启动时间: --		CPU: GenuineIntel 1 Intel(R) Xeon(R) CPU E5-2682 v4 @ 2.5...	IPV6: --
Web应用	代理服务器: --			
Web框架				
数据库				
系统安装包				
Jar包				
启动服务				
计划任务				
环境变量				
内核模块				

点击“更新数据”按钮，可重新获取该主机的资产信息。

四. Windows

4.1 资产清点

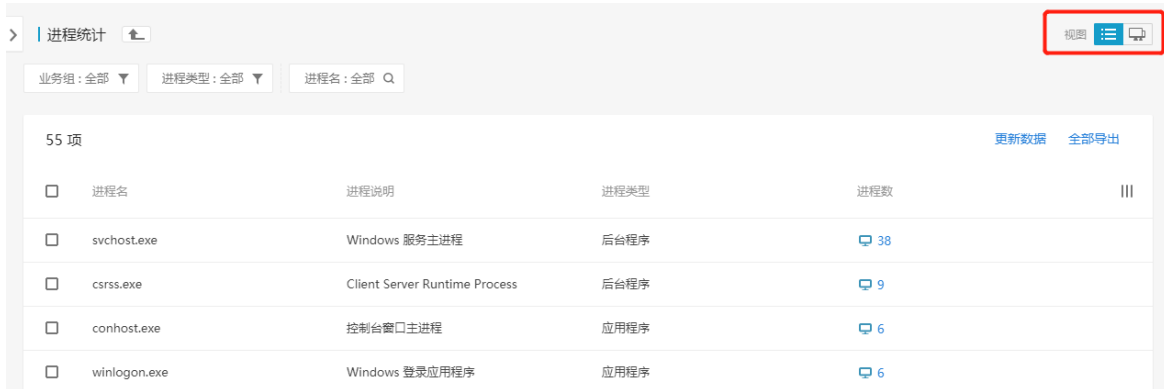
资产清点（Asset Inventory），致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产精准识别和动态感知，让保护对象清晰可见。使用 Agent-Server 架构，提供 10 余类主机关键资产清点，200 余类业务应用自动识别，并拥有良好的扩展能力。



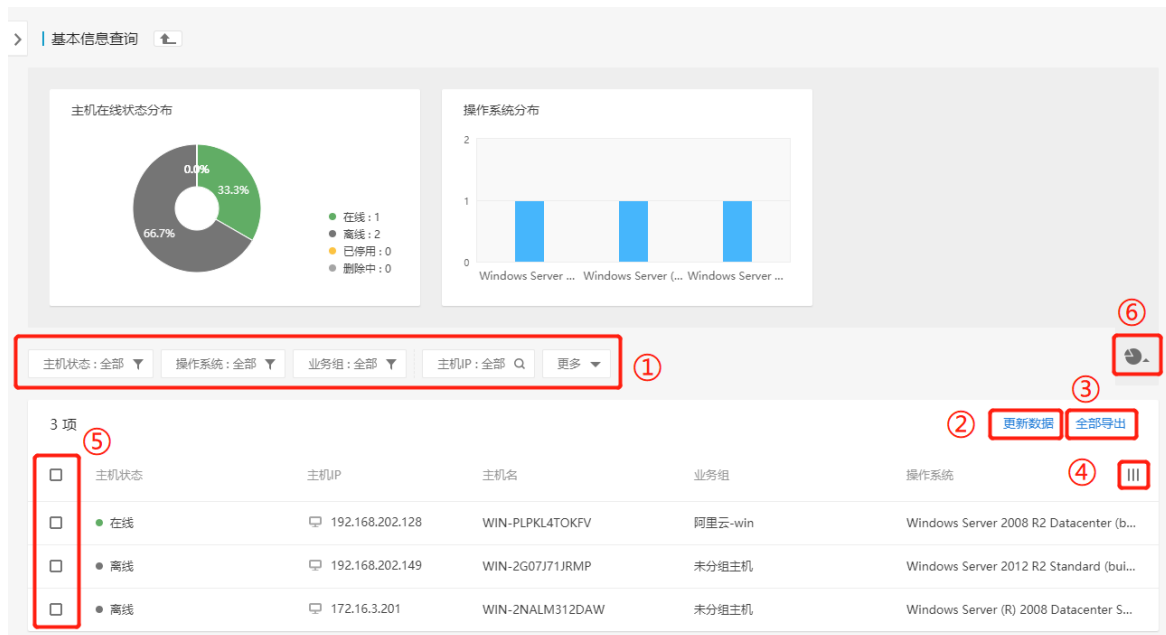
共有 7 个功能模块，分别为：


1. 主机管理：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，模块包含所有主机的硬件配置信息，及硬件消耗情况；
2. 进程管理：模块包含主机中所有进程，及运行进程的端口相关信息；
3. 账户管理：模块包含主机中所有账号，及用户组相关信息；
4. 安装程序与运行应用：模块包含主机中所有软件应用相关信息；
5. **Web** 管理：模块包含主机中 **Web** 相关服务及应用框架等信息；
6. 站点管理：模块包含主机中所有 **Web** 站点相关信息；
7. 数据库：模块包含主机中所有数据库相关信息；
8. 启动项清点：模块包含主机中所有启动项信息；

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。



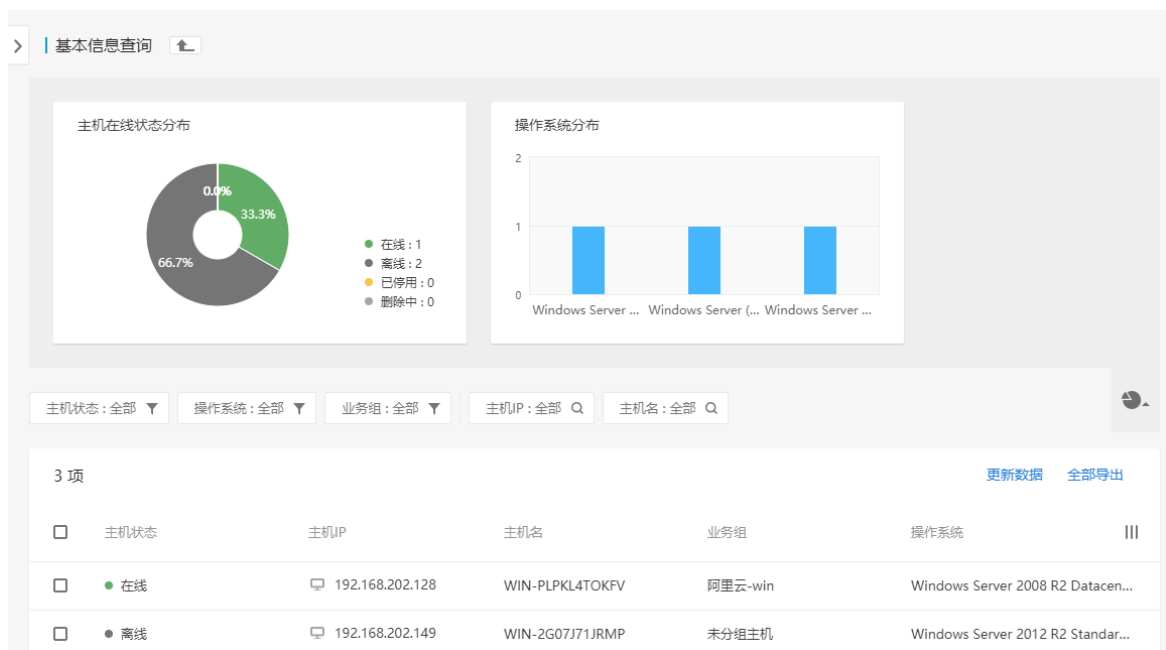
同时在资产详情页面，用户可以对列表进行操作，得到想要的查询结果。



- ① 筛选/搜索区：根据不同需求，对列表内容进行筛选；
- ② 更新数据按钮：点击 [更新数据](#)，手动触发更新当前资产数据；
- ③ 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；
- ④ 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；
- ⑤ 复选框按钮 ：点击复选框，可选中该行数据，进行“导出”等操作；
- ⑥ 显示/隐藏图表区；

4.1.1 主机管理

4.1.1.1 主机基本信息



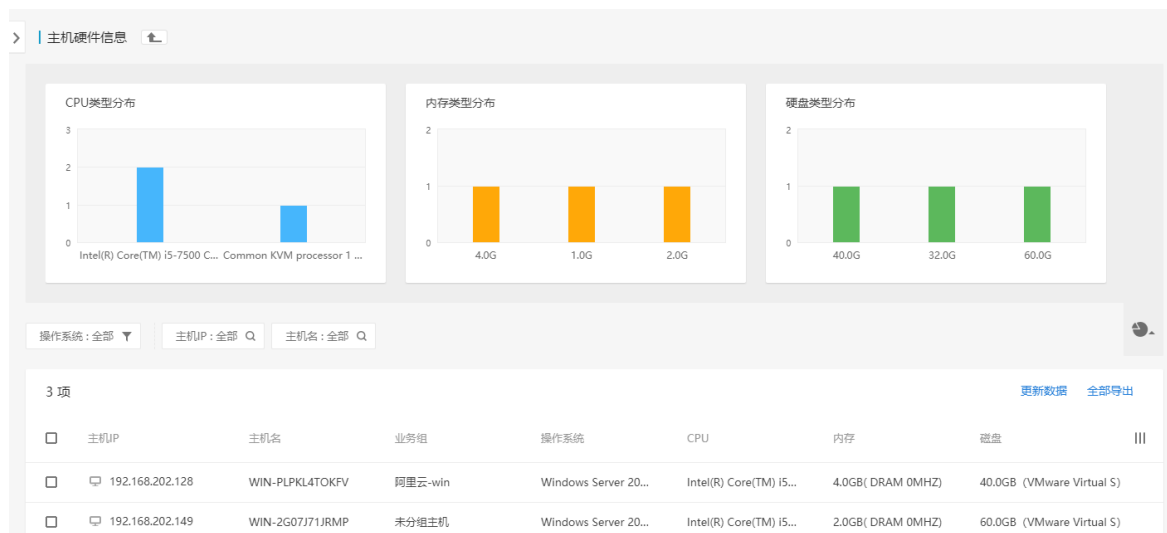
4.1.1.2 Agent 安装查询



4.1.1.3 离线主机查询



4.1.1.4 硬件配置查询



4.1.1.5 Agent 代理查询

> | 主机代理查询

主机IP: 全部 代理IP: 全部

1 项 更新数据 全部导出

<input type="checkbox"/>	代理IP	主机数目	操作
<input type="checkbox"/>	直连主机	3	

> | 没有使用代理服务器的主机

操作系统: 全部 业务组: 全部 主机IP: 全部 主机名: 全部

3 项 全部导出

<input type="checkbox"/>	主机IP	主机名	业务组	操作系统	操作
<input type="checkbox"/>	192.168.202.149	WIN-2G07J71JRM	未分组主机	Windows Server 2012 R2 Standard (build 9600),64-bit	
<input type="checkbox"/>	192.168.202.128	WIN-PLPKL4TOKFV	阿里云-win	Windows Server 2008 R2 Datacenter (build 7600),64-bit	
<input type="checkbox"/>	172.16.3.201	WIN-2NALM312DAW	未分组主机	Windows Server (R) 2008 Datacenter Service Pack 1 (build...	

4.1.2 进程管理

4.1.2.1 运行进程清点

资产视角

> | 进程统计

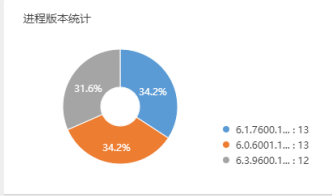
业务组: 全部 进程类型: 全部 进程名: 全部

55 项 更新数据 全部导出

<input type="checkbox"/>	进程名	进程说明	进程类型	进程数	操作
<input type="checkbox"/>	svchost.exe	Windows 服务主进程	后台程序	38	
<input type="checkbox"/>	csrss.exe	Client Server Runtime Process	后台程序	9	
<input type="checkbox"/>	conhost.exe	控制台窗口主进程	应用程序	6	
<input type="checkbox"/>	winlogon.exe	Windows 登录应用程序	应用程序	6	

> | 进程svchost.exe详情

进程版本统计



进程版本: 全部 PID: 全部 主机IP: 全部 主机名: 全部 更多

38 项 全部导出

<input type="checkbox"/>	主机IP	进程版本	进程路径	PID	运行用户	操作
<input type="checkbox"/>	192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	552	SYSTEM	
<input type="checkbox"/>	192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	600	NETWORK SERVICE	

主机视角

主机进程统计

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

3 项 [全部导出](#)

主机IP	进程数
192.168.202.128	66
192.168.202.149	53
172.16.3.201	50

主机192.168.202.128的进程列表

运行用户分布

进程类型: 全部 | 进程名: 全部 | 进程说明: 全部 | 进程路径: 全部 | 运行用户: 全部 | 更多

66 项 [全部导出](#)

PID	进程名	进程说明	进程类型	进程版本	进程路径	运行用户
6140	cmd.exe	Windows 命令处理程序	应用程序	6.1.7600.16385	C:\Windows\System...	Administrator
5452	vsidsr.exe		后台程序	--	--	

4.1.2.2 进程启动信息

资产视角

运行进程统计 - 启动信息查询

业务组: 全部 | 进程类型: 全部 | 进程名: 全部

55 项 [更新数据](#) [全部导出](#)

进程名	进程说明	进程类型	进程数
svchost.exe	Windows 服务主进程	后台程序	38
csrss.exe	Client Server Runtime Process	后台程序	9
conhost.exe	控制台窗口主进程	应用程序	6

进程svchost.exe启动信息详情

进程版本统计

进程版本: 全部 | 进程启动时间: 全部 | PID: 全部 | 主机IP: 全部 | 主机名: 全部 | 更多

38 项 [全部导出](#)

主机IP	进程启动时间	进程版本	进程路径	运行用户	进程启动参数	PID
192.168.202.149	2018-09-17 12:06:09	6.3.9600.16384	C:\Windows\System...	SYSTEM	C:\Windows\system3...	552

主机视角

主机运行进程统计 - 启动信息查询

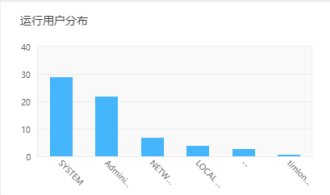
业务组: 全部 | 主机IP: 全部 | 主机名: 全部

3 项 [全部导出](#)

主机IP	进程数
192.168.202.128	66
192.168.202.149	53

主机192.168.202.128的进程启动信息

运行用户分布



进程启动时间: 全部 | 进程名: 全部 | 进程说明: 全部 | 进程路径: 全部 | 运行用户: 全部 | 更多

66 项 [全部导出](#)

进程启动时间	PID	进程名	进程说明	进程版本	进程路径	运行用户	进程启动参数
2018-11-02 17:29:04	4756	cmd.exe	Windows 命令处...	6.1.7600.16385	C:\Windows\Syst...	Administrator	cmd /c "C:\weblogic_root...
2018-11-02 17:29:04	1696	java.exe	Java(TM) Platfor...	8.0.1810.13	C:\PROGRA~1\Ja...	Administrator	C:\PROGRA~1\Java\UDK18...

4.1.2.3 端口查询

资产视角

端口统计

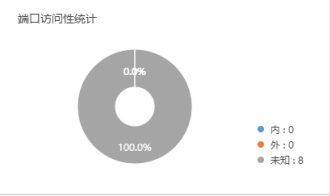
业务组: 全部 | 端口: 全部

31 项 [更新数据](#) [全部导出](#)

端口	端口数
3389	8
7001	7
49152	6

端口3389详情

端口访问性统计

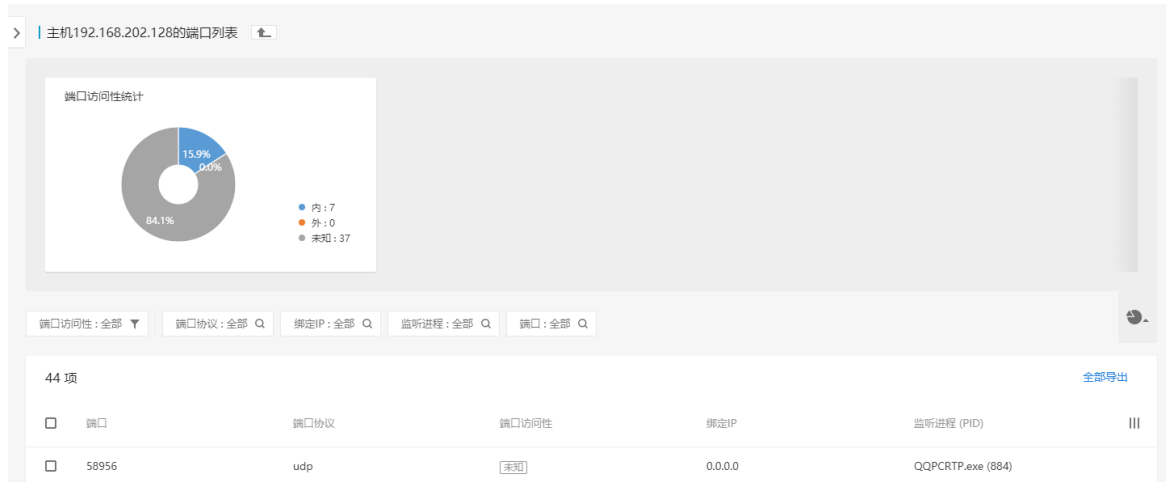
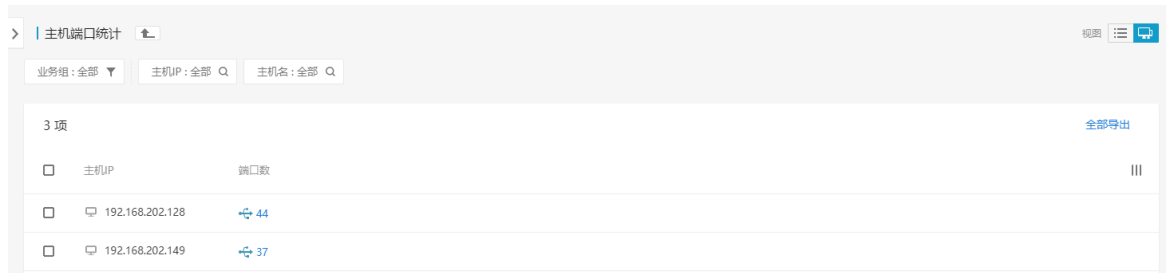


业务组: 全部 | 端口访问性: 全部 | 主机IP: 全部 | 主机名: 全部 | 端口协议: 全部 | 更多

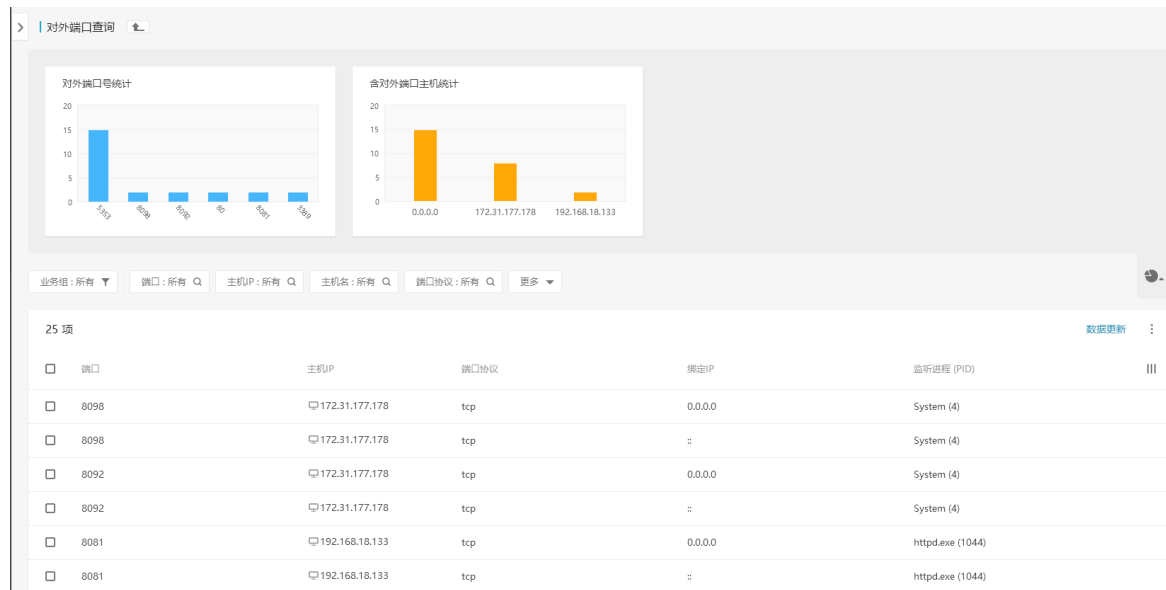
8 项 [全部导出](#)

主机IP	端口协议	端口访问性	绑定IP	监听进程 (PID)
192.168.202.149	tcp	未知	0.0.0.0	svchost.exe (1564)

主机视角



4.1.2.4 对外端口查询



4.1.2.5 含监听端口的进程

资产视角

含监听端口的进程统计

业务组: 全部 | 进程类型: 全部 | 进程名: 全部

14 项 更新数据 全部导出

进程名	进程说明	进程类型	主机数
svchost.exe	Windows 服务主进程	后台程序	17
wininit.exe	Windows 启动应用程序	后台程序	3
lsass.exe	Local Security Authority Process	后台程序	3
services.exe	服务和控制服务应用	后台程序	3

进程svchost.exe监听端口详情

业务组: 全部 | 进程版本: 全部 | PID: 全部 | 主机IP: 全部 | 主机名: 全部

进程版本统计

17 项 全部导出

主机IP	进程版本	进程路径	监听端口列表	PID
192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	TCP-135	600
192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	TCP-49153	788
192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	TCP-49154 UDP-500	824

主机视角

主机含监听端口的进程数

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

3 项 全部导出

主机IP	进程数
192.168.202.128	16
192.168.202.149	11

主机192.168.202.128的监听端口信息

进程名: 全部 | 进程说明: 全部 | 进程路径: 全部 | PID: 全部

16 项 全部导出

PID	进程名	进程说明	进程版本	进程路径	监听端口列表
4996	TitanAgent.exe	TitanAgent	3.2.2.0	C:\Program Files\TitanA...	TCP-8089
4684	360tray.exe	360安全卫士 安全防护中...	7.7.3.1631	C:\Program Files (x86)\3...	UDP-3600
4392	java.exe	Java(TM) Platform SE bi...	8.0.1810.13	C:\PROGRA~1\Java\JDK...	TCP-1527

4.1.3 账户管理

4.1.3.1 账号清点

资产视角

> | 账号统计 🔍 视图 ☰ 🖨

业务组: 全部 ▼ 用户名: 全部 🔍

6 项 更新数据 全部导出

<input type="checkbox"/>	用户名	账户说明	主机数	⋮
<input type="checkbox"/>	Guest	供来宾访问计算机或访问域的内置帐户	3	
<input type="checkbox"/>	Administrator	管理计算机(域)的内置帐户	3	
<input type="checkbox"/>	fiong_test		1	

> | 服务Guest主机运行状态 🔍 视图 ☰ 🖨

账户类型分布

100.0% ● 访客用户: 3

账户状态分布

100.0% ● 禁用: 3

业务组: 全部 ▼ 账户状态: 全部 ▼ 账户类型: 全部 ▼ 主机IP: 全部 🔍 用户ID: 全部 🔍 更多 ▼

3 项 全部导出

<input type="checkbox"/>	主机IP	用户ID	所属用户组	账户状态	账户类型	账户主目录	⋮
<input type="checkbox"/>	192.168.202.149	S-1-5-21-24285765-340...	Guests	禁用	访客用户		

主机视角

> | 主机账号统计 🔍 视图 ☰ 🖨

业务组: 全部 ▼ 主机IP: 全部 🔍 主机名: 全部 🔍

3 项 全部导出

<input type="checkbox"/>	主机IP	账户数	⋮
<input type="checkbox"/>	192.168.202.128	5	
<input type="checkbox"/>	192.168.202.149	3	
<input type="checkbox"/>	172.16.3.201	2	



4.1.3.2 用户组清点

资产视角

> 用户组统计

用户组名: 全部

用户组名	用户组描述	主机数
Distributed COM Users	成员允许启动、激活和使用此计算机上的分布式 COM 对象。	3
Guests	按默认值，来宾用户组的成员有同等访问权，但来宾帐户的...	3
Cryptographic Operators	授权成员执行加密操作。	3

> 用户组Guests详情

主机IP: 全部 | 主机名: 全部

主机IP	用户列表
192.168.202.149	WIN-2G07J71JRMPI\Guest
192.168.202.128	WIN-PLPKL4TOKFV\Guest
172.16.3.201	WIN-2NALM312DAW\Guest

主机视角

> 用户组统计

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

主机IP	用户组数
192.168.202.128	17
192.168.202.149	23
172.16.3.201	24

主机192.168.202.149的用户组列表

用户组名: 全部

23 项 全部导出

<input type="checkbox"/>	用户组名	用户组描述	用户列表	
<input type="checkbox"/>	WinRMRemoteWMIUsers_	Members of this group can access WMI resources over ...		
<input type="checkbox"/>	Users	防止用户进行有意的或无意的系统范围的更改, 但是可以运行大...	NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Us...	
<input type="checkbox"/>	Replicator	支持域中的文件复制		

4.1.3.3 账号登陆查询

账号登录查询

账户上次登录时间: 所有 | 账户类型: 所有 | 主机IP: 所有 | 主机名: 所有 | 用户名: 所有 | 账户主目录: 所有

69 项 数据更新

<input type="checkbox"/>	主机IP	用户名	账户上次登录时间	账户类型	账户主目录	
<input type="checkbox"/>	0.0.0.0	Administrator	2018-04-24 22:19:56	管理员用户	C:\Users\Administrator	
<input type="checkbox"/>	172.31.177.178	Administrator	2018-04-20 13:32:19	管理员用户	C:\Users\Administrator	
<input type="checkbox"/>	10.10.10.15	hack	2018-04-14 19:40:23	管理员用户	C:\Users\hack	
<input type="checkbox"/>	192.168.197.216	test	2018-04-03 02:35:47	标准用户	C:\Users\test	
<input type="checkbox"/>	169.254.187.69	YPS	2018-04-02 10:04:38	管理员用户	C:\Users\YPS	
<input type="checkbox"/>	192.168.18.135	jary	2018-03-29 11:25:10	管理员用户	C:\Users\jary	
<input type="checkbox"/>	10.12.8.181	admin	2018-03-27 18:46:00	管理员用户	C:\Users\admin	
<input type="checkbox"/>	192.168.18.133	Administrator	2018-03-22 14:28:46	管理员用户	C:\Users\Administrator	
<input type="checkbox"/>	0.0.0.0	admin	2018-03-07 10:49:21	管理员用户	C:\Users\admin	
<input type="checkbox"/>	0.0.0.0	jk	2018-01-22 13:06:38	管理员用户	C:\Users\jk	
<input type="checkbox"/>	0.0.0.0	Administrator	2017-12-27 18:21:44	管理员用户	C:\Users\Administrator	

4.1.3.4 域账号清点

域账号统计

请点“域服务器”中所有域账号, 及域管理下的所有主机, 用户将通过登录“域服务器”中的域账号, 可访问相同域下管理的主机, 获得主机提供的服务。

所属域名: 全部 | 域服务器IP: 全部 | 主机名: 全部

0 项 更新数据 全部导出

<input type="checkbox"/>	域名	域服务器IP	域账号数	操作	
<input type="checkbox"/>	没有账户相关数据				

4.1.3.5 域账号登录查询

域账号登录查询

记录访问过“域管理下主机”的所有域账号, 并提供域账号登录相关信息。

业务组: 全部 | 被访问主机IP: 全部 | 主机名: 全部 | 所属域名: 全部

0 项 更新数据 全部导出

<input type="checkbox"/>	被访问主机IP	主机名	最近登录账号	
<input type="checkbox"/>	没有账户相关数据			

4.1.3.6 密码即将到期与已到期账号查询

密码即将到期与已到期账号查询

账户状态: 所有 | 上次密码修改时间: 所有 | 账户类型: 所有 | 主机IP: 所有 | 主机名: 所有 | 用户名: 所有 | 更多

10 项	主机IP	用户名	账户状态	上次密码修改时间	账户密码状态	账户主目录	账户类型	数据更新
<input type="checkbox"/>	192.168.197.216	admin	启用	2017-06-19 23:39:46	已过期		标准用户	
<input type="checkbox"/>	192.168.197.216	Administrator	启用	2017-03-15 14:52:57	已过期	C:\Users\Administrator	管理员用户	
<input type="checkbox"/>	192.168.197.216	testaaaaaaaa	启用	2017-06-19 18:44:38	已过期		标准用户	
<input type="checkbox"/>	192.168.197.216	user	启用	2017-06-19 18:45:39	已过期		标准用户	
<input type="checkbox"/>	192.168.197.149	Administrator	启用	2013-10-01 05:58:31	已过期	C:\Users\Administrator	管理员用户	
<input type="checkbox"/>	192.168.197.149	test	启用	2013-10-01 07:14:14	已过期		标准用户	
<input type="checkbox"/>	192.168.197.36	Administrator	启用	2009-01-27 02:17:14	已过期	C:\Users\Administrator	管理员用户	
<input type="checkbox"/>	192.168.18.133	Administrator	启用	2013-10-01 05:58:31	已过期	C:\Users\Administrator	管理员用户	
<input type="checkbox"/>	192.168.18.133	test	启用	2013-10-01 07:14:14	已过期		标准用户	
<input type="checkbox"/>	10.211.55.14	Administrator	启用	2017-01-19 07:09:02	已过期		管理员用户	

4.1.3.7 主机密码期限

主机账户关键配置

业务组: 所有 | 主机IP: 所有 | 主机名: 所有

22 项	主机IP	主机名	密码最长使用期限	密码最短使用期限	密码过期前提醒天数	数据更新
<input type="checkbox"/>	192.168.197.216	WIN-V65M12R3R0J	42天	--	5天	
<input type="checkbox"/>	192.168.197.149	WIN-AR79G1VES1A	42天	--	5天	
<input type="checkbox"/>	192.168.197.36	WIN-6CLCZAWOGON	42天	--	14天	
<input type="checkbox"/>	192.168.106.128	WIN-P2KDFPH8DJ	--	--	5天	
<input type="checkbox"/>	192.168.18.135	DESKTOP-QH5LNTS	--	--	5天	
<input type="checkbox"/>	192.168.18.133	WIN-AR79G1VES1A	42天	--	5天	
<input type="checkbox"/>	192.168.11.160	LAPTOP-82IBIUK2	42天	--	5天	

4.1.4 安装程序与运行应用

4.1.4.1 安装软件清点

资产视角

安装软件统计

业务组: 所有 | 安装软件名: 所有

398 项 数据更新

安装软件名	主机数
<input type="checkbox"/> Update for Microsoft Office 2013 (KB3039720) 64-Bit Edition	80
<input type="checkbox"/> Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	15
<input type="checkbox"/> Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	12
<input type="checkbox"/> Google Chrome	12
<input type="checkbox"/> Security Update for Microsoft Excel 2013 (KB2920753) 64-Bit Edition	10
<input type="checkbox"/> Update for Microsoft Office 2010 (KB2553347) 64-Bit Edition	10
<input type="checkbox"/> Mozilla Maintenance Service	10
<input type="checkbox"/> VMware Tools	9
<input type="checkbox"/> Update for Microsoft OneDrive for Business (KB3178645) 64-Bit Edition	8
<input type="checkbox"/> Update for Microsoft Visio Viewer 2013 (KB2817301) 64-Bit Edition	8
<input type="checkbox"/> Update for Microsoft InfoPath 2013 (KB3114946) 64-Bit Edition	8

软件Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161详情

安装版本分布

9.0.30729.6161 : 2

软件大小分布

- 0-1MB : 1
- 1-10MB : 0
- 10-100MB : 1
- 100MB-1GB : 0
- 1GB以上 : 0

业务组: 全部 | 安装时间: 全部 | 安装版本: 全部 | 软件大小: 全部 | 主机IP: 全部 | 更多

2 项 全部导出

主机IP	安装版本	软件发布者	安装时间	软件大小	安装路径
<input type="checkbox"/> 192.168.202.149	9.0.30729.6161	Microsoft Corporation	2017-08-18 17:15:35	13.2 MB	

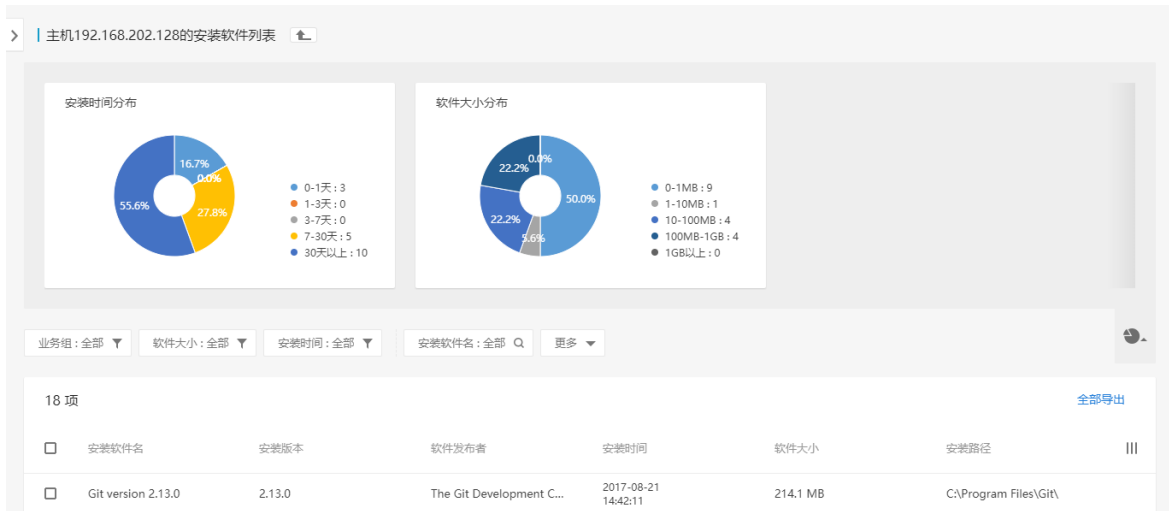
主机视角

主机软件安装统计

业务组: 所有 | 主机IP: 所有 | 主机名: 所有

28 项

主机IP	安装程序数
<input type="checkbox"/> 0.0.0.0	187
<input type="checkbox"/> 0.0.0.0	157
<input type="checkbox"/> 10.10.10.15	140



4.1.4.2 Jar 包清点

资产视角

Jar包统计

业务组: 全部 | 类型: 全部 | 包名: 全部

包名	主机数
mina-core-2.0.5.jar	1
jboss-interceptors-api_1.1_spec.jar	1
jboss-jca.jar	1
jaxws-httpserver-httpspi.jar	1
bootstrap-1.3.2-core-assets.jar	1
jboss-ejb3-proxy-impl.jar	1

Jar包mina-core-2.0.5.jar详细信息

业务组: 全部 | 类型: 全部 | 是否可执行: 全部 | 绝对路径: 全部 | 更多

主机IP	包名	类型	是否可执行	版本	绝对路径	操作
192.168.220.135	mina-core-2....	其他依赖包	否	--	C:\Users\adm...	查看详情

主机视角

主机Jar包统计

类型: 全部 业务组: 全部 主机IP: 全部 主机名: 全部

1 项 [全部导出](#)

主机IP	包数
192.168.220.135	729

主机192.168.220.135的Jar包详细信息

类型: 全部 是否可执行: 全部 绝对路径: 全部 版本: 全部 更多

729 项 [全部导出](#)

主机IP	包名	类型	是否可执行	版本	绝对路径	操作
192.168.220.135	asm-commo...	其他依赖包	否	4.0	C:\Users\adm...	查看详情
192.168.220.135	netty-resolve...	其他依赖包	否	4.1.5.Final	C:\Users\adm...	查看详情
192.168.220.135	scheduler-pl...	Web服务自带库	否	6.1.0.Final	C:\Users\adm...	查看详情
192.168.220.135	jboss-bootstr...	Web服务自带库	否	2.1.0-alpha-6	C:\Users\adm...	查看详情

Jar包详情

基本信息

包名: asm-commons-4.0.jar 类型: 其他依赖包
 版本: 4.0 是否可执行: 否
 绝对路径: C:\Users\admin\Downloads\jboss-6.1.0.Final\server\default\tmp\vfs\...
 MD5: b6e6837fed04d4a7bad291caad8756ea

引用情况

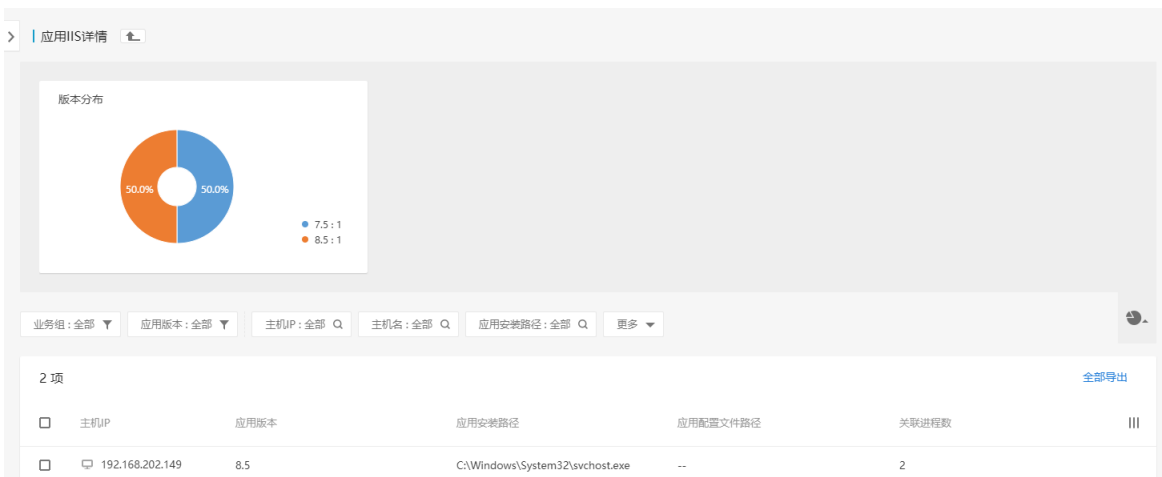
进程列表:

进程名	PID	启动时间
java.exe	4712	2019-01-16 10:01:24

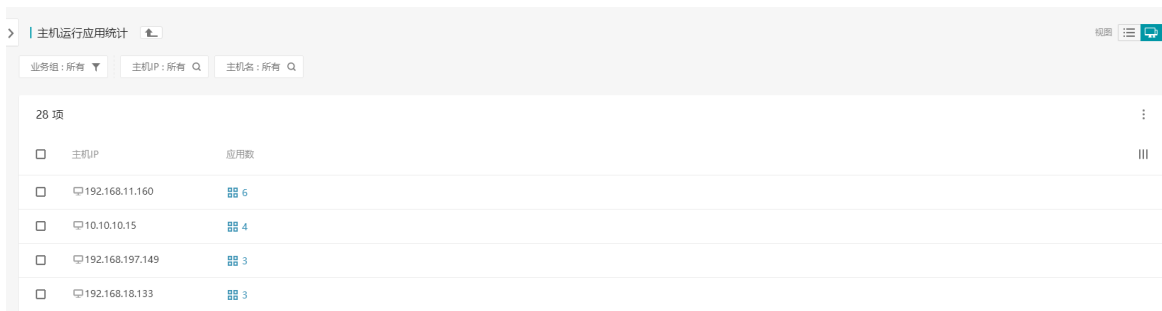
[确定](#)

4.1.4.3 运行应用清点

资产视角



主机视角



4.1.5 Web 管理

4.1.5.1 Web 服务清点

资产视角

> | Web服务

Web服务名: 全部 ▼ 业务组: 全部 ▼ 启动用户: 全部 Q

3 项 更新数据 全部导出

Web服务名	主机数	
<input type="checkbox"/> tomcat	1	
<input type="checkbox"/> jboss	1	
<input type="checkbox"/> websphere	1	

> | tomcat服务详细信息

版本: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 配置文件路径: 全部 Q 更多 ▼

1 项 全部导出

主机IP	版本	二进制路径	配置文件路径	关联进程数	
<input type="checkbox"/> 192.168.75.133	7.0.92	C:\Program Files\Java\jdk...	C:\Users\admin\Downlo...	1	

> | 主机192.168.75.133上tomcat服务关联的进程

进程启动时间: 全部 ▼ 进程版本: 全部 ▼ PID: 全部 Q 进程名: 全部 Q 更多 ▼

1 项 全部导出

PID	进程路径	启动用户	进程启动时间	
<input type="checkbox"/> 4552	C:\Program Files\Java\jdk1.8.0_1...	admin	2018-11-28 17:17:38	

主机视角

> | 主机Web服务

Web服务名: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 主机名: 全部 Q

3 项 更新数据 全部导出

主机IP	Web服务数	
<input type="checkbox"/> 172.16.2.187	1	
<input type="checkbox"/> 192.168.75.133	1	
<input type="checkbox"/> 192.168.220.135	1	

> | 主机172.16.2.187 Web服务详细信息

Web服务名: 全部 ▼ 版本: 全部 ▼ 启动用户: 全部 ▼ 业务组: 全部 ▼ 更多 ▼

1 项 全部导出

<input type="checkbox"/>	主机IP	Web服务名	版本	二进制路径	配置文件路径	关联进程数	
<input type="checkbox"/>	● 172.16.2.187	websphere	9.0.0.10	C:\Program Files\I...	--	1	

> | 主机172.16.2.187上websphere服务关联的进程

进程启动时间: 全部 ▼ 进程版本: 全部 ▼ PID: 全部 Q 启动用户: 全部 Q 更多 ▼

1 项 全部导出

<input type="checkbox"/>	PID	进程路径	启动用户	进程启动时间	
<input type="checkbox"/>	11404	C:\Program Files\IBM\WebSpher...	SYSTEM	2019-02-26 10:07:20	

4.1.5.2 Web 应用清点

资产视角

> | Web应用统计 视图

应用名: 全部 Q

1 项 更新数据 全部导出

<input type="checkbox"/>	应用名	描述	主机数	
<input type="checkbox"/>	Monstra CMS	Monstra CMS是乌克兰软件开发者Sergey Rom...	2	

> | Web应用Monstra CMS统计

版本: 全部 ▼ 服务类型: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 更多 ▼

2 项 全部导出

<input type="checkbox"/>	主机IP	版本	根路径	服务类型	站点域名	虚拟目录	
<input type="checkbox"/>	● 192.168.56.1	--	C:/inetpub/wwwr...	IIS	*	C:/inetpub/wwwroot	
<input type="checkbox"/>	● 192.168.56.1	--	C:/inetpub/wwwr...	IIS	*	C:/inetpub/wwwroot	

主机视角

主机Web应用统计

业务组: 全部 | 主机IP: 全部 | 主机名: 全部

2 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	主机IP	应用数	
<input type="checkbox"/>	● 192.168.56.1	1	
<input type="checkbox"/>	● 192.168.56.1	1	

主机192.168.56.1Web应用统计

版本: 全部 | 服务类型: 全部 | 应用名: 全部 | 根路径: 全部 | 更多

1 项 [全部导出](#)

<input type="checkbox"/>	应用名	描述	版本	根路径	服务类型	站点域名	虚拟目录	
<input type="checkbox"/>	Monstra CMS	Monstra CMS...	--	C:/inetpub/ww...	IIS	*	C:/inetpub/wwwroot	

4.1.5.3 Java 语言框架清点

支持清点的 Java 语言 Web 框架类型，包括：

Struts、struts2、spring、hibernate、webwork、quartz、velocity、tapestry、turbine、freemarker、flexive、stripes、vaadin、vertx、wicket、zkoss、jackson、fastjson、shiro、MyBatis、spring MVC、Jersey、JFinal；

资产视角

Java框架统计

业务组: 全部 | 框架名: 全部

23 项 [更新数据](#) [全部导出](#)

<input type="checkbox"/>	框架名	主机数	
<input type="checkbox"/>	Freemarker	1	
<input type="checkbox"/>	vertx	1	
<input type="checkbox"/>	spring MVC	1	
<input type="checkbox"/>	velocity	1	
<input type="checkbox"/>	zkoss	1	
<input type="checkbox"/>	shiro	1	

> | Freemarker服务详细信息

服务类型: 全部 ▼ 版本: 全部 ▼ 业务组: 全部 ▼ 主机IP: 全部 Q 更多 ▼

1 项 全部导出

<input type="checkbox"/>	主机IP	版本	服务类型	关联jar包数	
<input type="checkbox"/>	● 192.168.220.135	2.3.13,2.3.19	--	2	

主机视角

> | 主机Java语言框架 视图

业务组: 全部 ▼ 主机IP: 全部 Q 主机名: 全部 Q

1 项 全部导出

<input type="checkbox"/>	主机IP	框架数	
<input type="checkbox"/>	● 192.168.220.135	23	

> | 主机192.168.220.135的Java语言框架详细信息

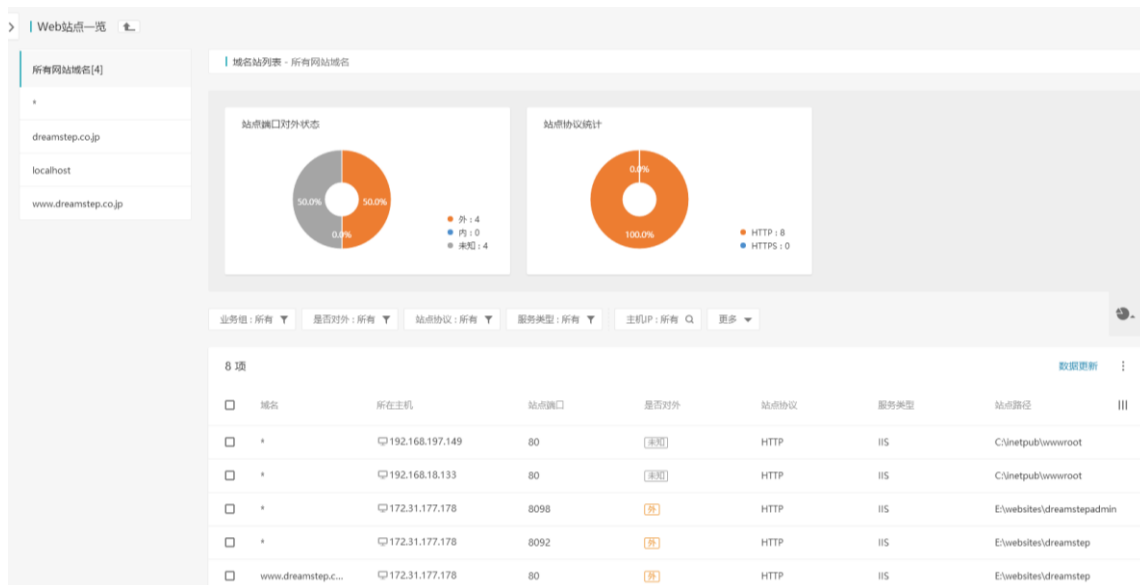
服务类型: 全部 ▼ 框架名: 全部 Q

23 项 全部导出

<input type="checkbox"/>	框架名	版本	服务类型	关联jar包数	
<input type="checkbox"/>	spring	2.5.6.SEC03,3.0.5.RELEASE,4.3.2....	--	4	
<input type="checkbox"/>	Freemarker	2.3.13,2.3.19	--	2	
<input type="checkbox"/>	hibernate	3.6.6.Final,5.3.7.Final,3.3.1.GA	--	3	

4.1.6 站点管理

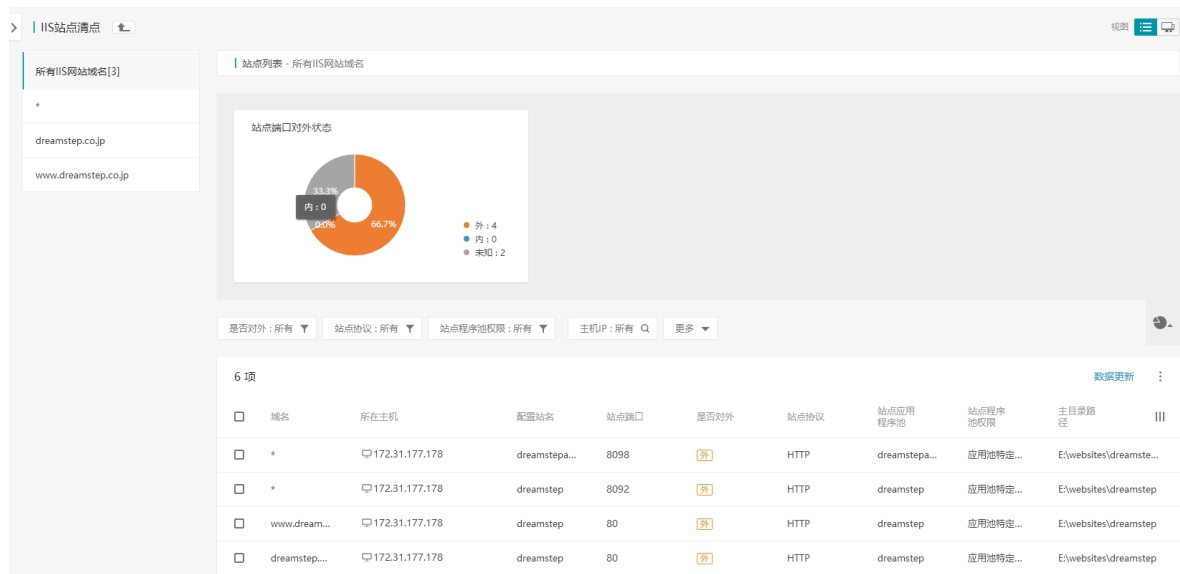
4.1.6.1 Web 站点清点



4.1.6.2 Web 应用清点



4.1.6.3 IIS 站点清点



4.1.6.4 Nginx 站点清点



4.1.6.5 Apache 站点清点



4.1.6.6 Tomcat 站点清点



4.1.6.7 WebSphere 站点清点



4.1.6.8 Weblogic 站点清点

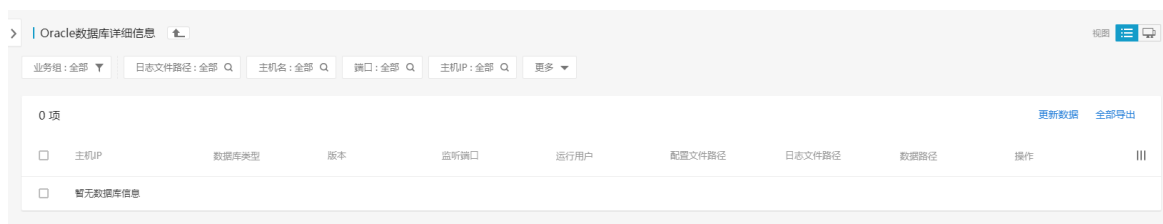


4.1.7 数据库

4.1.7.1 SQL Server 数据库查询



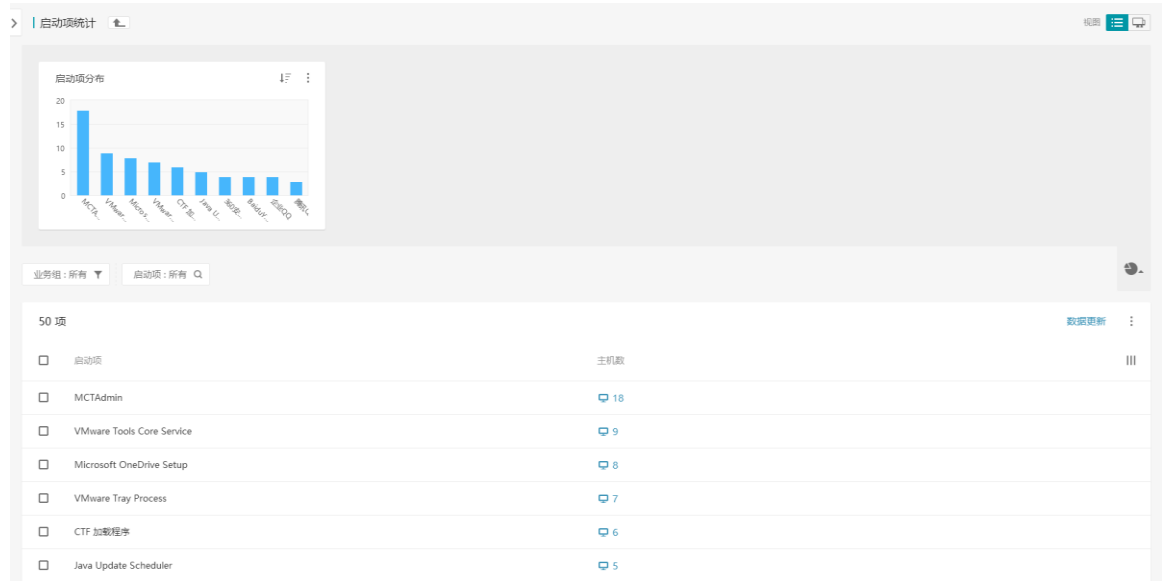
4.1.7.2 Oracle 数据库查询



4.1.8 启动项清点

4.1.8.1 启动项清点

资产视角



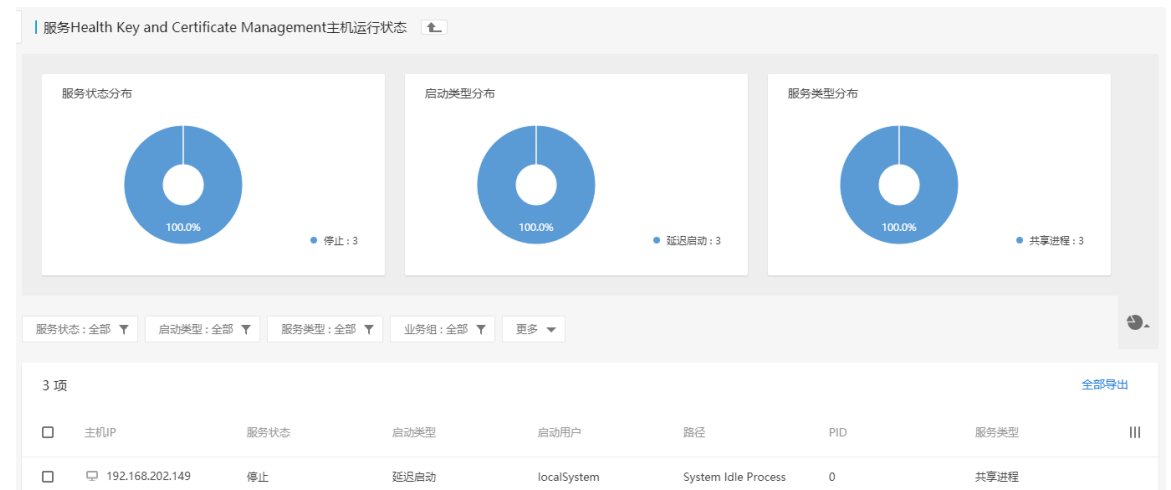
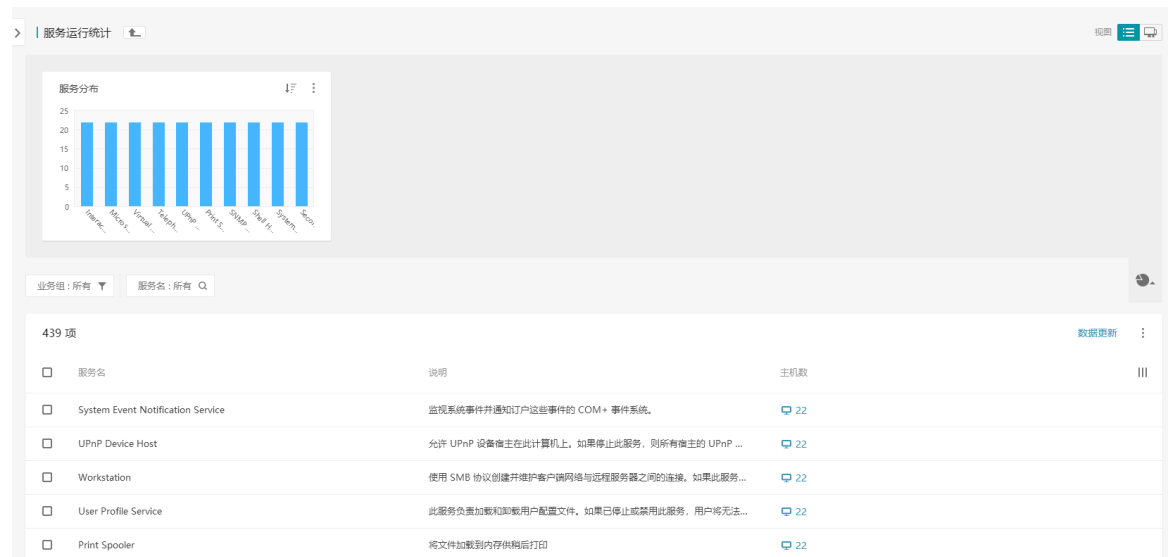
主机视角



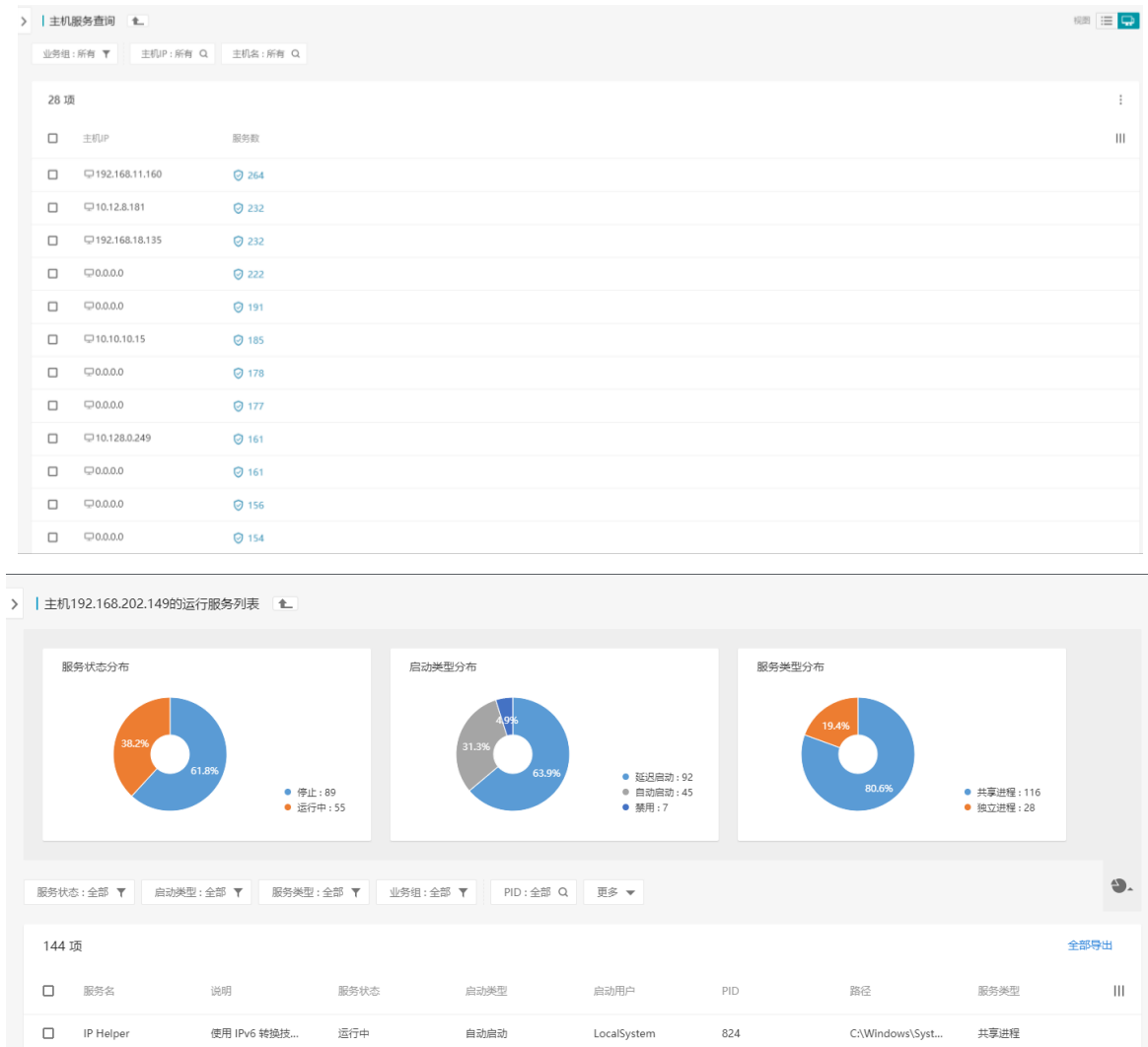


4.1.8.2 运行服务清点

资产视角



主机视角



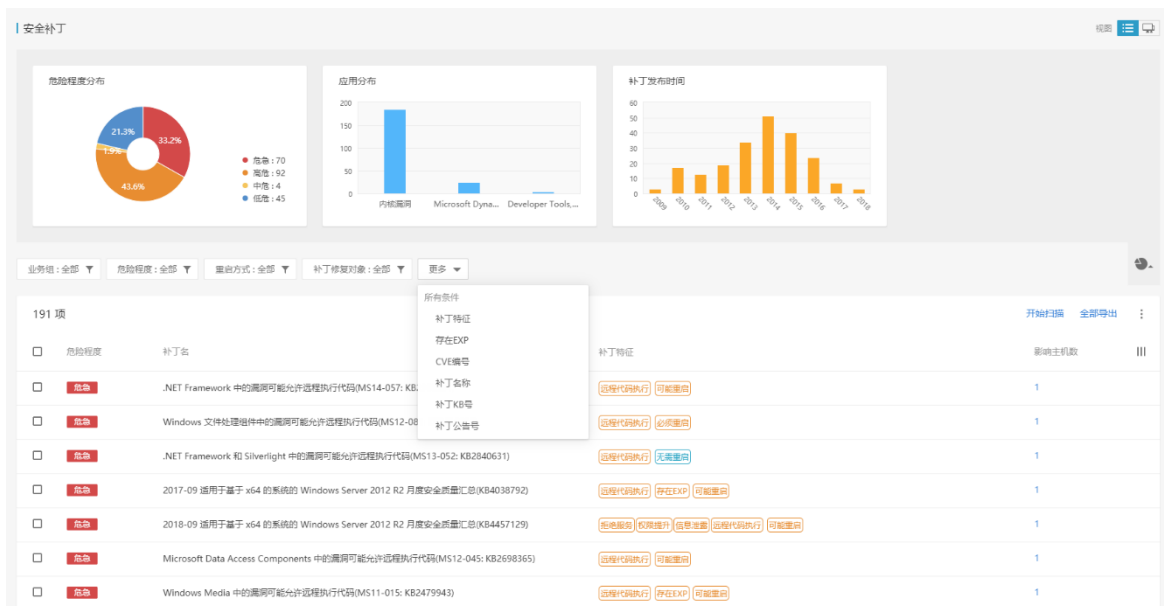
4.2 风险发现

4.2.1 安全补丁

功能概述:

Windows 安全补丁指由微软官方发布的安全类补丁，该类补丁主要针对已公布的漏洞进行安全修复。安全补丁模块主要帮助运维人员检测需要打的补丁、进行补丁管理。有补丁视图/主机视图两种查看模式。

补丁视图




➤ 开始扫描

点击“开始扫描”按钮，出现弹框“您确认开始安全补丁扫描吗？”，点击“确认”后开始扫描

➤ 全部导出

点击“全部导出”按钮，导出全部风险项到 csv 文件


➤ 白名单规则


点击  中的“白名单列表”按钮，转到“白名单规则”页面



单击“新建白名单规则”按钮，进入新建规则页面

➤ 查看补丁提示信息

点击“补丁名称”后的标识 ，显示该补丁的信息提示框，内容包括：补丁描述，补丁公告地址，引用信息：

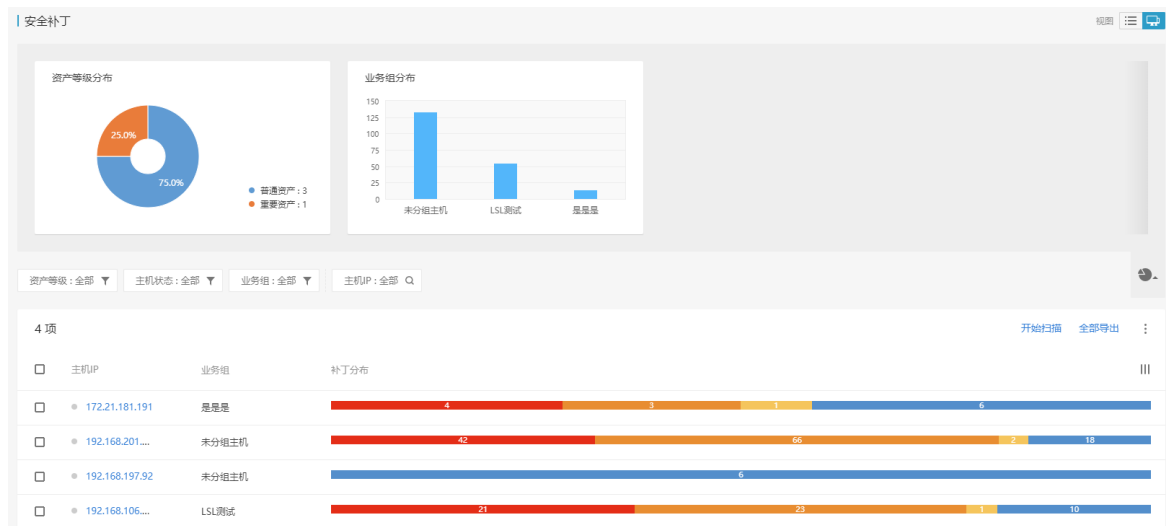
补丁名	补丁特征
.NET Framework 中的漏洞可能允许远程执行代码(MS14-057: KB2968294) 	远程代码执行 可能重启
Windows 文件处理组件中的漏洞可能允许远程执行代码(MS12-081: KB2758855)	可能重启
.NET Framework 和 Silverlight 中的漏洞可能允许远程执行代码(MS13-052: KB2758855)	可能重启
2017-09 适用于基于 x64 的系统的 Windows Server 2012 R2 月度安全质量报告	可能重启
2018-09 适用于基于 x64 的系统的 Windows Server 2012 R2 月度安全质量报告	可能重启
Microsoft Data Access Components 中的漏洞可能允许远程执行代码(MS12-081: KB2758855)	可能重启
Windows Media 中的漏洞可能允许远程执行代码(MS11-015: KB2479943)	可能重启
Windows 内核模式驱动程序中的漏洞可能允许远程执行代码(MS13-081: KB2758855)	可能重启 必须重启

补丁描述
此安全更新可解决 Microsoft .NET Framework 中三个秘密报告的漏洞。如果攻击者将包含国际字符的特制 URI 请求发送到 .NET Web 应用程序，则其中最严重的漏洞可能允许远程执行代码。在 .NET 4.0 应用程序中，容易受到攻击的功能 (iriParsing) 默认情况下被禁用；要利用该漏洞，应用程序必须明确启用此功能。在 .NET 4.5 应用程序中，iriParsing 默认情况下启用，不能被禁用。

补丁公告地址
<https://technet.microsoft.com/zh-cn/library/security/MS14-057>

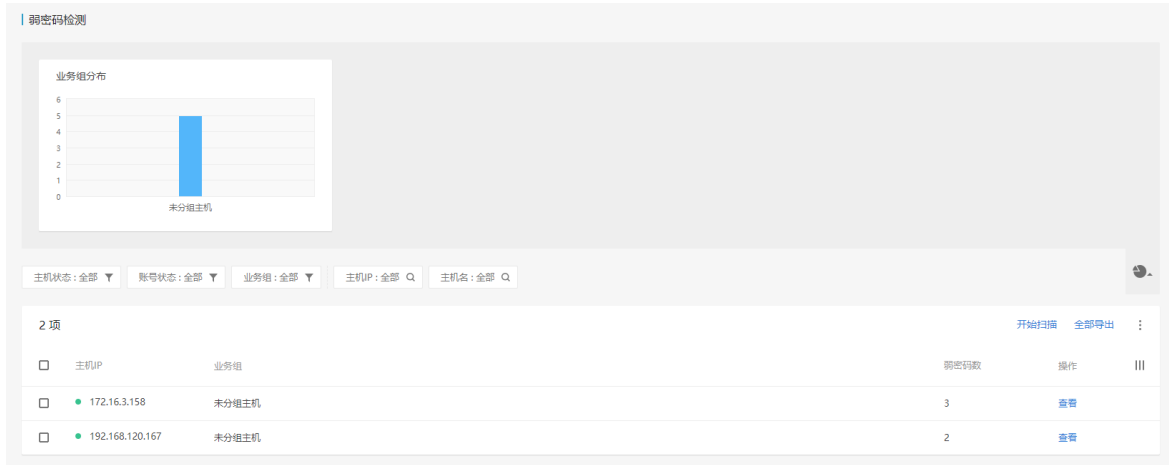
引用信息
CVE-2014-4073, CVE-2014-4121, CVE-2014-4122, 70312, 70313, 70351, 113181, 113185, 113184, MS14-057, 2968292, 2968294, 2968295, 2968296, 2972098, 2972100, 2972101, 2972103, 2972105, 2972106, 2972107, 2978041, 2978042, 2979568, 2979570, 2979571, 2979573, 2979574, 2979575, 2979576, 2979577, 2979578,

主机视图



4.2.2 弱密码检查

检查所有安装 Agent 主机的 Windows 系统弱口令，支持单项 or 批量导出。



4.2.2.1 白名单规则

单击首页右侧 按钮进入白名单规则页面。

条件	范围	受影响对象	操作
账号状态为: 禁用	全部主机	全部主机	查看详情

➤ 新建白名单规则

新建规则

条件列表：

- 账号包含：
- 账号状态：
- 弱密码类型：

如果满足上述条件，则将此类弱密码加入白名单

使用范围：

- 全部主机
- 自定义范围
 - 业务组：
 - 主机：

描述：

白名单规则说明

规则	说明
----	----

条件列表	<p>账号包含：用户自定义，输入弱密码应用的账号。</p> <p>账号状态：启用、锁定和禁用 3 个可选项。</p> <p>弱密码类型：空口令、系统默认弱密码、密码与用户名相同、常见弱密码 4 个可选项。</p>
规则范围	<p>让用户设置一些 IP 范围，将针对在设置的 IP 范围内的主机的弱密码过滤，设置范围有以下几种方式：</p> <p>全部主机</p> <p>自定义范围（业务组主机，单独 IP 主机）</p>


➤ 编辑白名单规则



➤ 删除白名单规则



4.2.2.2 简单密码字典

单击右侧  按钮选择简单密码词典选项。简单密码字典用户检查用户的密码设置为该密码字典中的任意密码，则判定为弱密码。

- 编辑字典： 用户手动一一录入弱密码，每行一个弱密码，编辑框中提供了行号提示弱密码数量；
- 导入字典： 用户可导入弱密码字典，仅支持 **txt** 格式，需以换行分隔，每行均将识别为一个弱密码；仅识别前 **3000** 行，其后将完全忽略；每次导入将完全覆盖原密码设置；
- 导出字典： 用户可将当前存储的所有简单弱密码直接导出为 **txt** 格式，在自行编辑后，再导入系统；



4.2.2.3 组合密码字典

组合密码指组合密码特征进行弱密码检测的字典

本功能当前仅支持前缀+连接符+后缀的组合密码；

密码三部分将自动增加任意部分为空的检测；前缀将自动增加用户名的检测；

前缀最多可添加 8 个，连接符 9 个，后缀 19 个，均使用换行符隔开

例如，检测某账号： admin；

动态密码字典： 前缀为 abc；连接符为 @；后缀为 123

则将检查如下弱密码： admin@123； admin@； admin123； admin； abc@123； abc123；

abc@； @123； abc； @； 123；

截图如下：



4.2.3 web 风险文件

4.2.3.1 功能描述

在实际的网络环境中，由于研发人员开发时的疏忽、Web 所使用开发语言本身的特性以及运维人员的操作失误等原因，会使得 Web 目录下有这样一类文件——一些不应该被其他人可以直接访问和下载的文件却可以被其他人直接访问和下载。这类文件因此特性会产生信息泄露而导致安全问题。

4.2.3.2 原理说明

风险文件的原理是通过一个匹配算法，将符合匹配规则的文件认定为风险文件。匹配算法主要包含两种方式：

➤ 后缀名匹配。

常见的风险文件中，如 office 文档、日志文件、备份文件、配置文件等都是有特定的后缀名的，office 文档的 \.doc\ .docx\ .xls\ .xlsx\ .ppt\ .pptx、日志文件的 \.log 等等。我们采用文件名后缀的匹配方式，找到相应的风险文件。

➤ 内容的匹配。

有一类风险文件的产生是由 Web 开发所选择的开发语言和开发环境所导致的，比如使用 php 开发的 Web 中会有 phpinfo 相关的内容，凡是在文件内容中或者文件名包含有 phpinfo 的

文件都可能含有 php 服务器的配置信息。我们采用正则的内容匹配方式，发现所有文件名或者文件内容中包含 phpinfo 字符串的风险文件。

4.2.3.3 页面截图

时间	主机IP/端口	解析方式/站点	文件名	类型
2018-01-17 23:53:53	192.168.197.130 : 80	HOST *	C:\openweb\web.config	配置文...
2015-10-05 00:51:06	0.0.0.0 : 80	HOST localhost	C:\xampp\apache\...\external\phpids\0.6\lib\DS\vendors\ht...	系统文件
2015-10-05 00:51:06	0.0.0.0 : 80	HOST localhost	C:\xampp\apache\...\htdocs\phpinfo.php	phpinfo...
2015-10-05 00:51:06	0.0.0.0 : 80	HOST localhost	C:\xampp\apache\...\external\phpids\0.6\lib\DS\vendors\ht...	系统文件
2015-10-05 00:51:06	0.0.0.0 : 80	HOST localhost	C:\xampp\apache\...\htdocs\htaccess	系统文件
2015-10-05 00:51:06	0.0.0.0 : 80	HOST localhost	C:\xampp\apache\...\htdocs\setup.php	系统文件
2017-12-22 17:30:21	172.31.177.178 : 8093	HOST *	E:\websites\fwm\web - 副本.config	配置文...
2017-12-22 17:30:21	172.31.177.178 : 8096	HOST *	E:\websites\fwm\admin.com\web - 副本.config	配置文...
2017-12-22 18:21:27	172.31.177.178	HOST *	E:\websites\fwm\virtual\web.config	配置文...
2017-12-22 18:21:27	172.31.177.178 : 8093	HOST *	E:\websites\fwm\web.config	配置文...
2017-12-22 17:30:21	172.31.177.178	HOST *	E:\websites\fwm\virtual\web - 副本.config	配置文...
2018-01-25 14:13:02	172.31.177.178 : 8098	HOST *	E:\websites\koneyadmin\Areas\Admin\Views\web.config	配置文...

4.3 入侵检测

4.3.1 暴力破解

暴力破解用于阻止各类关键应用被暴力破解，尝试登录的行为，防止登录账户被爆破。目前支持 rdp,ssh,winrm 三种服务。

服务类型	最近攻击时间	攻击来源	攻击目标	累计攻击次数	封停状态	操作
SSHID	2019-04-16 04:30:49	193.201.224.82 (乌克兰)	172.17.0.17	3	解封	
SSHID	2019-04-15 20:10:19	219.146.152.154 (中国, ...)	172.17.0.17	1	解封	
SSHID	2019-04-15 19:50:13	104.131.184.67 (美国)	172.17.0.17	3	解封	

手动解封按钮

手动封停按钮

加入白名单按钮

用户可以选择手动将一条暴力破解记录加入白名单。加入以后这条记录将成为一条规则，这条

规则由该暴力破解的登录时间、登录 IP、登录区域三个条件以与关系结合成规则。该规则的适用范围为这条记录的主机 IP。

暴力破解封停条件说明

条件	说明	时间周期	登录次数N	封堵时间(分钟)	说明
q1	相同IP下同一用户名登录N次	1	6	1	启用
q2	N个IP下同一用户名登录	1	5	1	废弃不用
q3	相同IP下N个不存在的用户名登录	5	3	1	启用
q4	指定时间内重试达到指定N次	10	19	1	启用

4.3.1.1 查看攻击记录


点击暴力破解事件列表中各项记录的  按钮，可查看该事件聚合的攻击记录详情。

攻击记录列表[96]

攻击时间	攻击详情	处理结果
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理
2019-03-11 19:34:54	较长的时间内，间断性的尝试账号 usero 的密码，达到指定次数	未处理

确定

4.3.1.2 服务设置

单击  按钮，可以看到服务设置，查看白名单，全部导出三个选项，选择“服务设置”进入服务设置列表，可以根据需要选择 ssh,winrm,rdp 三个服务的开启关闭状态。

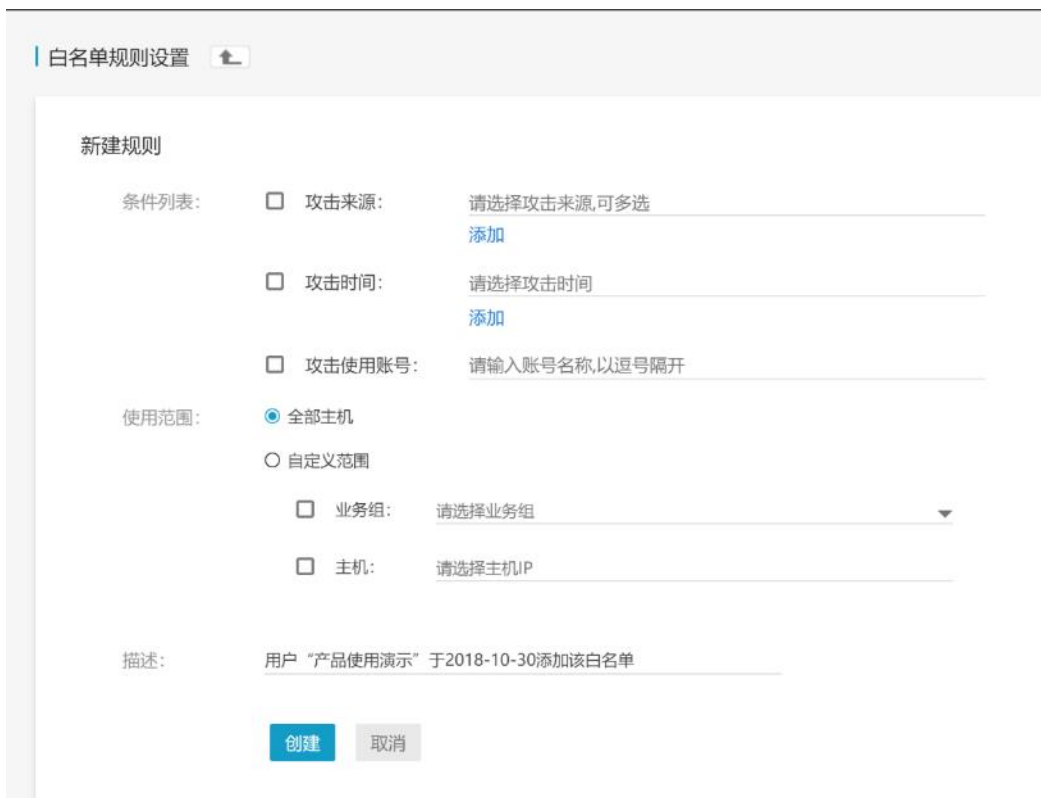


4.3.1.3 查看白名单

单击 按钮，可以看到服务设置，查看白名单，全部导出三个选项，选择“查看白名单”进入白名单规则列表。

暴力破解白名单是为了将某些登录认定为正常登录而不是暴力破解去上报，防止一些不必要的上报和封停。

- 新建白名单规则



白名单规则设置说明

规则	说明
条件列表	条件列表中各条件之间是与关系，必须满足所有条件才是正常登录 攻击来源：设置某个 IP、IP 段或系统已有的 IP 组为正常登录 IP，添加方

	式包括手动添加、常用 IP 组导入、导入 CSV 格式。 攻击时间：设置一个或多个时间点为正常登录时间，登录时间设置方式星期加上起止时间。 攻击使用账号：用户手动填写一个或者多个账号。
规则范围	全部主机：指的是所以装有 Agent 的主机 自定义范围：可以选择业务组与自己输入单台主机 IP 的复合结果

- 编辑白名单

对于已经保存的单条规则，用户可以选择对其进行修改。

白名单规则修改后，同样需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被修改规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。

遍历数据的限制条件同新建白名单。



- 删除白名单

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。在删除时，需要给用户删除确认提示，用户确认后方可删除。

白名单规则被删除后，同样需要重新遍历检测结果列表内的历史数据，根据更新后的规则库判断，对列表内的记录进行更新，符合更新后规则的记录将不再显示上报；被删除规则的受影响记录中不符合更新后规则的将被还原至列表，恢复显示并正常上报。遍历数据的限制条件同新建白名单。




4.3.1.4 导出

暴力破解的数据导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。例如：用户会导出暴力破解数据用于特定的统计处理，对近期的检测数据进行存档等。

选择的方式有以下两种：

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；



全部导出：单击  按钮选择“全部导出”。



暴力破解

实时监控主机上发生的爆破行为，并发送通知，同时提供封禁成功或未成功的能力。
用户可以查看并处理暴力破解事件，也可以对暴力破解的自动封禁机制和服务设置进行配置。
如果来源 IP 处于非解封成功状态中，则无法加入白名单，请将来源 IP 解封成功后再加入白名单。

服务类型: 全部 | 封禁状态: 全部 | 时间区间: 全部 | 业务组: 全部 | 攻击来源: 全部 | 更多

240 项	服务类型	最近攻击时间	攻击来源	攻击目标	累计攻击次数	封禁状态	操作
<input type="checkbox"/>	SSHD	2019-04-18 06:01:57	142.93.83.136 (加拿大)	172.16.0.4	2	未处理	主机配置检测 全部导出
<input type="checkbox"/>	SSHD	2019-04-17 20:06:41	193.112.125.195 (英国)	172.16.0.4	13854	封禁	
<input type="checkbox"/>	SSHD	2019-04-17 09:11:43	193.201.224.158 (乌克兰...)	172.16.0.4	397	未处理	

4.3.2 异常登录

4.3.2.1 功能描述

异常登录用于发现系统成功登录的信息中，包含非正常 IP，非正常区域，非正常时间的登录信息。



异常登录

实时监控主机上发生的异常登录行为，例如非正常时间登录、非正常地点登录等异常登录，并发送邮件通知。
用户可以查看这些异常登录事件，也可设置正常登录规则，规定哪些为正常的登录行为，正常登录外的行为将被认为是异常登录行为。

异常登录类型: 全部 | 2019.04.18 - 2019.04.18 | 业务组: 全部 | 主机IP: 全部 | 登录账号: 全部 | 更多

1 项	时间	主机IP	登录账号	来源IP	登录区域
<input type="checkbox"/>	2019-04-18 11:51:10	192.168.30.169	zk	192.168.30.1	局域网

4.3.2.2 正常登录规则设置

- 新建正常登录规则

新建正常登录规则
↑

新建规则

条件列表:

登录IP: 请选择登录IP,可多选
添加

登录时间: 请选择登录时间,可多选
添加

登录区域: 请设置登录区域
设置

登录账号: 请输入登录账号, 多个以英文逗号分开

使用范围:

全部主机

自定义范围

业务组: 请选择业务组

主机: 请选择主机IP

描述: 用户 "演示" 于2019-04-18新建的正常登录规则

创建
取消

正常登录规则说明

规则类型	说明
规则的条件列表	<p>条件列表中各条件之间是与关系，必须满足所有条件才是正常登录。</p> <p>登录 IP: 设置某个 IP、IP 段或系统已有的 IP 组为正常登录 IP，添加方式包括手动添加、常用 IP 组导入；</p> <p>登录时间: 设置一个或多个时间点为正常登录时间，登录时间设置方式星期加上起止时间；</p> <p>登录区域: 设置一些登录区域为正常登录区域，对于非中国地区只到国家层面，对于中国地区可以设置国家级、省级和市级。例子：中国、中国湖北、中国湖北武汉、美国、俄罗斯；</p> <p>登录账号: 设置一个或多个认为是正常的登录账号，添加方式为手动输入。</p>
规则的适用范围	<p>规则范围是指以上条件的适用范围。</p> <p>规则范围有是以下两种方式里选择其中一种，且仅可以选择一种：</p> <p>1) 全部主机: 指的是所以装有 Agent 的主机；</p> <p>2) 自定义范围: 可以选择业务组与自己输入单台主机 IP 的复合结果</p>

- 编辑正常登录规则

对于已经保存的单条规则，用户可以选择对其进行修改。



• 删除正常登录规则

对于已经保存的单个或者多条规则，用户可以选择对其进行删除。删除操作要有确认提示，用户确认后方可删除。



4.3.2.3 导出

异常登录的数据导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。例如：用户会导出异常登录数据用于特定的统计处理，对近期的检测数据进行存档等。

导出方式有以下两种：

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；

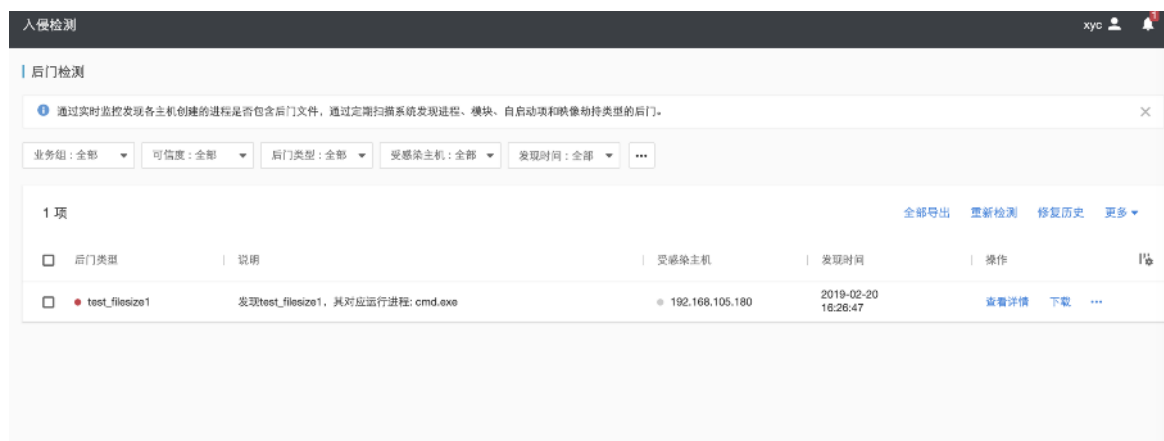


全部导出：单击 按钮选择“全部导出”。



4.3.3 后门检测

后门检测功能用于检测系统是否存在可疑进程、可疑自启动项、映像劫持、病毒木马等问题。其中可疑进程、可疑自启动项、可疑模块、映像劫持依靠扫描来发现，病毒木马则通过实时监控进程来发现。目前病毒木马支持的规则库包括小红伞、ClamAV、青藤 Hash 库、青藤 Yara 库。



4.3.3.1 重新检测

重新检测包括两个方面的功能，其一是重新扫描所有管理主机中是否存在可疑进程、可疑自启动项、可疑模块、映像劫持，其二是检测已经发现的病毒木马是否依然存在。重新检测后的数据会和当前列表中的数据进行比对，如果不存在的数据会进入到修复历史中去。

4.3.3.2 查看详情

可以通过查看详情按钮查看该后门的基本属性和与其相关联的进程或者模块等信息。



4.3.3.3 加入白名单

找到文件确认过不是系统后门后，可以选择加入白名单，在下次扫描时加入白名单的后门不会再提示。



4.3.3.4 导出

异常登录的数据导出功能是用来将列表内的数据以自定义方式导出成数据文件供用户在系统外使用。例如：用户会导出异常登录数据用于特定的统计处理，对近期的检测数据进行存档等。

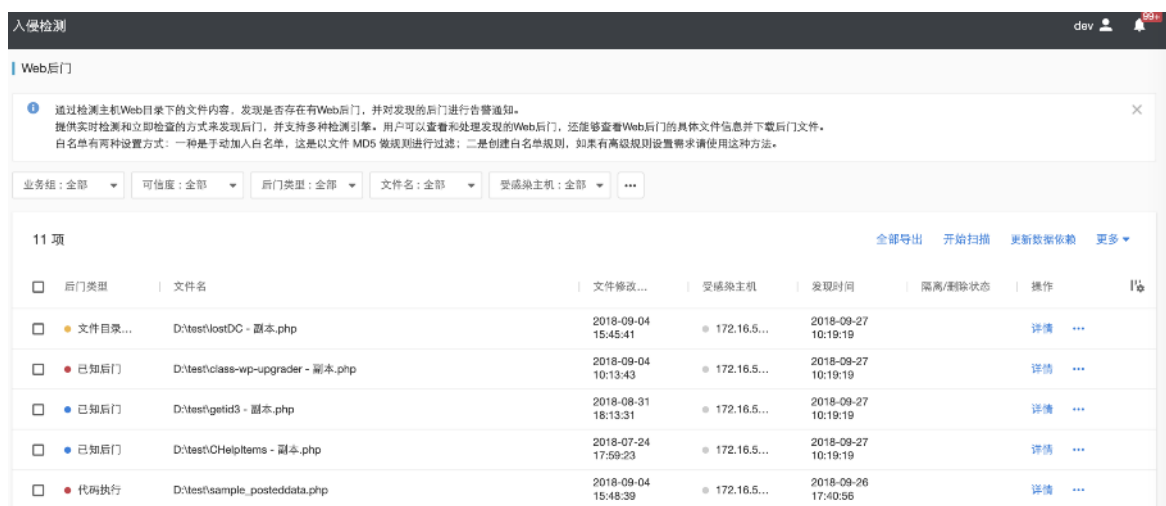
导出方式有以下两种：

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；


全部导出：单击 按钮选择“全部导出”。

4.3.4 Web 后门

Web 后门用于检查 Web 网站中存在的后门文件，Web 后门文件为安全威胁检查中即为重要的一环。扫描分 2 种，触发式扫描，即点击界面，用户主动触发的扫描； 每日定时扫描，每日定时进行的扫描。



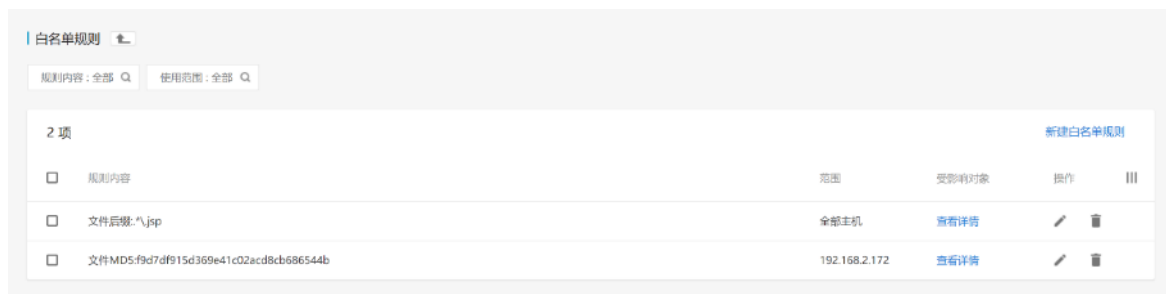
开始扫描按钮：即用户主动对单独该项进行扫描。

点击  按钮，有功能设置、查看白名单、修复记录、全部导出、更新数据依赖和自定义目录 6 个选项。

4.3.4.1 功能设置



4.3.4.2 查看白名单



➤ 新建白名单规则



白名单规则说明

规则	说明
规则内容	<p>Web 后门白名单的规则内容可以由以下两个条件中的任意一条组成，两个条件为关系互斥。</p> <ul style="list-style-type: none">• 文件 MD5。设置某些符合条件的文件 MD5 为正常文件 MD5，MD5 与之匹配的文件即视为正常文件，条件内容为文件的 MD5，由用户手动输入或手动添加白名单操作填入。• 自定义文件。条件内容可以由以下两个条件中的任一条组成或多个条件以与关系组成。<ul style="list-style-type: none">• 文件目录。设置某些符合条件的文件目录为正常文件目录，该条件目录下的文件或者目录指向的文件即视为正常文件，条件内容为文件目录的正则表达式，由用户手动输入。• 文件后缀。设置某些符合条件的文件后缀为正常文件后缀，带有该后缀的文件即视为正常文件，条件内容为文件后缀的正则表达式，由用户手动输入。
规则范围	<p>规则范围是用户自定义规则适用的范围，用户可以按照下面三种方式选择。</p> <ul style="list-style-type: none">• 全部主机。所有安装 Agent 的主机。• 自定义范围。可以选择业务组，也可以选择多台主机。

- 编辑白名单规则

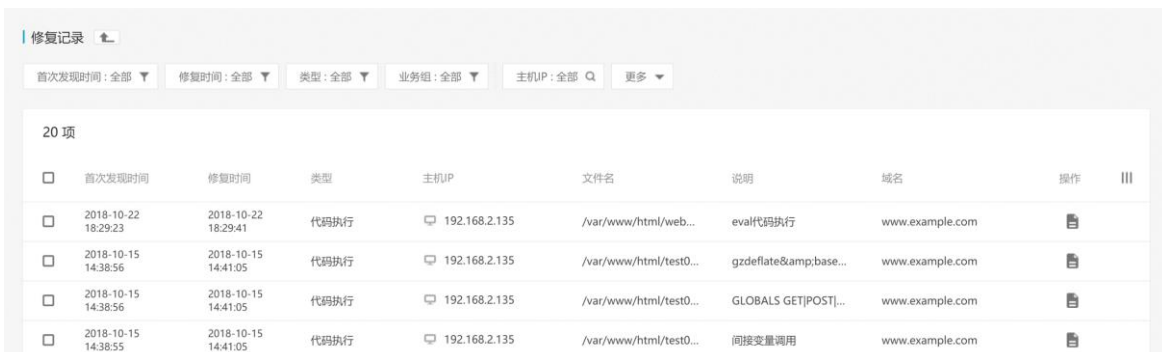
对于已经保存的单条规则，用户可以选择对其进行修改。

- 删除白名单规则

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。

4.3.4.3 修复记录


可以查看到所有曾经存在过，但是现在已经不存在的 Web 后门的记录。



首次发现时间	修复时间	类型	主机IP	文件名	说明	域名	操作
2018-10-22 18:29:23	2018-10-22 18:29:41	代码执行	192.168.2.135	/var/www/html/web...	eval代码执行	www.example.com	
2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	gzdeflate&base...	www.example.com	
2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	GLOBALS GET[POST]...	www.example.com	
2018-10-15 14:38:55	2018-10-15 14:41:05	代码执行	192.168.2.135	/var/www/html/test0...	间接变量调用	www.example.com	

4.3.4.4 全部导出

手动选择：手动勾选取消需要导出的行，选择“导出”按钮导出选中的数据；

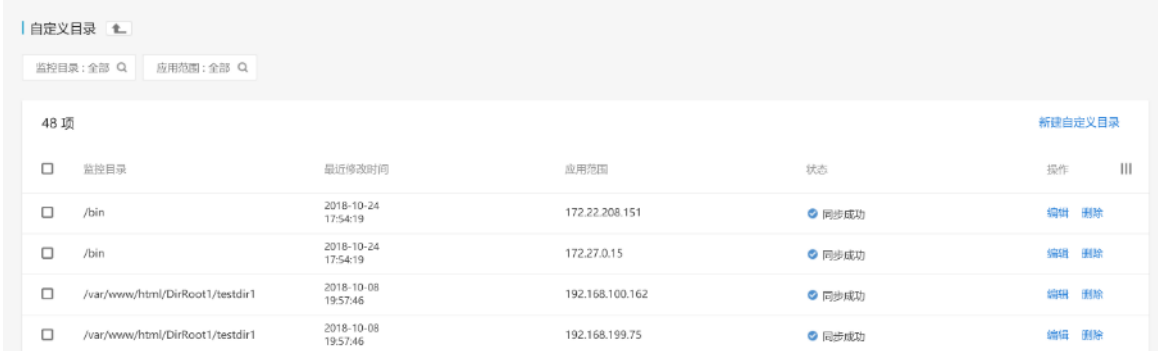
全部导出：单击  按钮选择“全部导出”。

4.3.4.5 更新数据依赖

在线更新 KB 数据。

4.3.4.6 自定义目录

用户可以根据实际情况设置需要额外扫描的目录。



自定义目录

监控目录：全部 应用范围：全部

48 项 新建自定义目录

<input type="checkbox"/>	监控目录	最近修改时间	应用范围	状态	操作	⋮
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除	
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除	
<input type="checkbox"/>	/var/www/html/DirRoot1/testdir1	2018-10-08 19:57:46	192.168.100.162	同步成功	编辑 删除	
<input type="checkbox"/>	/var/www/html/DirRoot1/testdir1	2018-10-08 19:57:46	192.168.199.75	同步成功	编辑 删除	

- 新建自定义目录



新建自定义目录

⚠ 如果增加监控目录过多，会增加系统性能消耗，所以请谨慎设置监控目录，建议监控目录不超过10个。

监控目录：

应用范围：

- 编辑自定义目录



自定义目录

监控目录：全部 应用范围：全部

48 项 新建自定义目录

<input type="checkbox"/>	监控目录	最近修改时间	应用范围	状态	操作	⋮
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除	
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除	

- 删除自定义目录



自定义目录

监控目录：全部 应用范围：全部

48 项 新建自定义目录

<input type="checkbox"/>	监控目录	最近修改时间	应用范围	状态	操作	⋮
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 删除	
<input type="checkbox"/>	/bin	2018-10-24 17:54:19	172.27.0.15	同步成功	编辑 删除	

4.3.4.7 查看详情

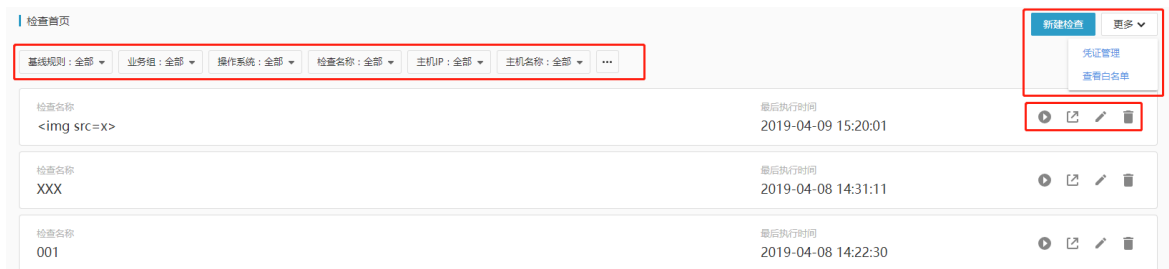


点击【详情】按钮，可以查看这个 Web 后门的详细内容，包括基本说明、检测说明和基本信息。



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。



4.4.1 基线检查

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。

通过率	基线规则	成功主机	最后执行时间	操作
0%	中国等级-Windows Server 2008 R2-三级主机安全合规检查	0	2019-04-11 16:06:28	▶ 📄 🗑️
0%	中国等级-Windows Server 2008 R2-二级主机安全合规检查	0	2019-04-11 16:06:28	▶ 📄 🗑️
0%	CIS Windows Server 2008 R2 Level 2合规检查	0	2019-04-11 16:06:28	▶ 📄 🗑️
0%	CIS Windows Server 2008 R2 Level 1合规检查	0	2019-04-11 16:06:27	▶ 📄 🗑️

➤ 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。

4.4.2 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。

The screenshot shows the 'Check Item View' for the baseline rule '中国等保-Centos 7-三级主机安全合规检查'. It displays the following summary statistics:

- 最后执行时间: 2018-12-21 11:03:32
- 检查耗时: 4秒
- 1 检查主机
- 0 失败主机
- 47.7% 通过率
- 21 通过项
- 23 未通过项
- 0 失败项

Below the summary, there are tabs for '检查项视图' (selected) and '主机视图'. The '检查项视图' tab shows a list of 44 items with columns for '检查项名', '类别', '检查结果 (通过率)', and '操作'. The first few items are:

检查项名	类别	检查结果 (通过率)	操作
检查auditd服务是否启用	配置系统账户 (auditd)	100%	查看详情
检查重复用户名是否存在	用户和组设置	100%	查看详情
检查AIDE是否安装	文件系统完整性检查	0%	查看详情
检查密码创建要求是否配置	配置PAM认证	0%	查看详情
检查/etc/passwd中的所有组在/etc/group是否存在	用户和组设置	100%	查看详情

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。

The screenshot shows the 'Host View' for the check item '检查用户默认的umask值是否为022'. It displays the following summary statistics:

- 通过率: 100%
- 通过项: 2
- 未通过项: 0
- 失败项: 0

Below the summary, there are filters for '主机IP', '主机名', '业务组', and '检查结果'. The '主机IP' filter is selected, showing a table of results:

主机IP	主机名	业务组	通过结果	操作
172.31.17.136	ip-172-31-17-136.cn-no...	未分组主机	通过	查看详情
192.168.122.1	localhost.localdomain	未分组主机	通过	查看详情

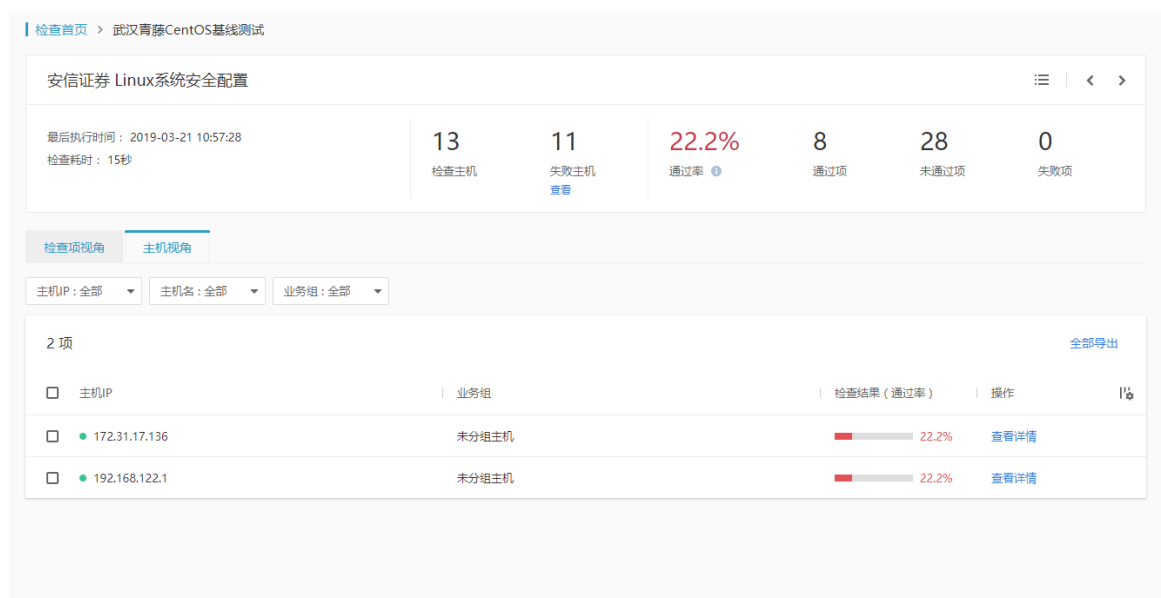
At the bottom, it shows '已选0/2 | 加入白名单' and a '关闭' button.

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。



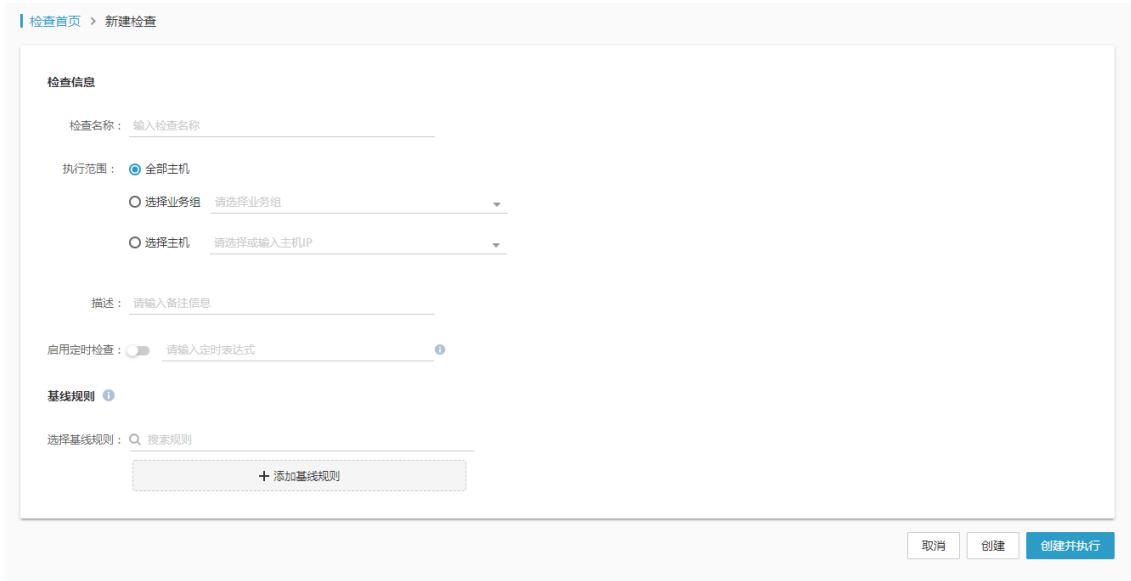
➤ 主机视图

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。

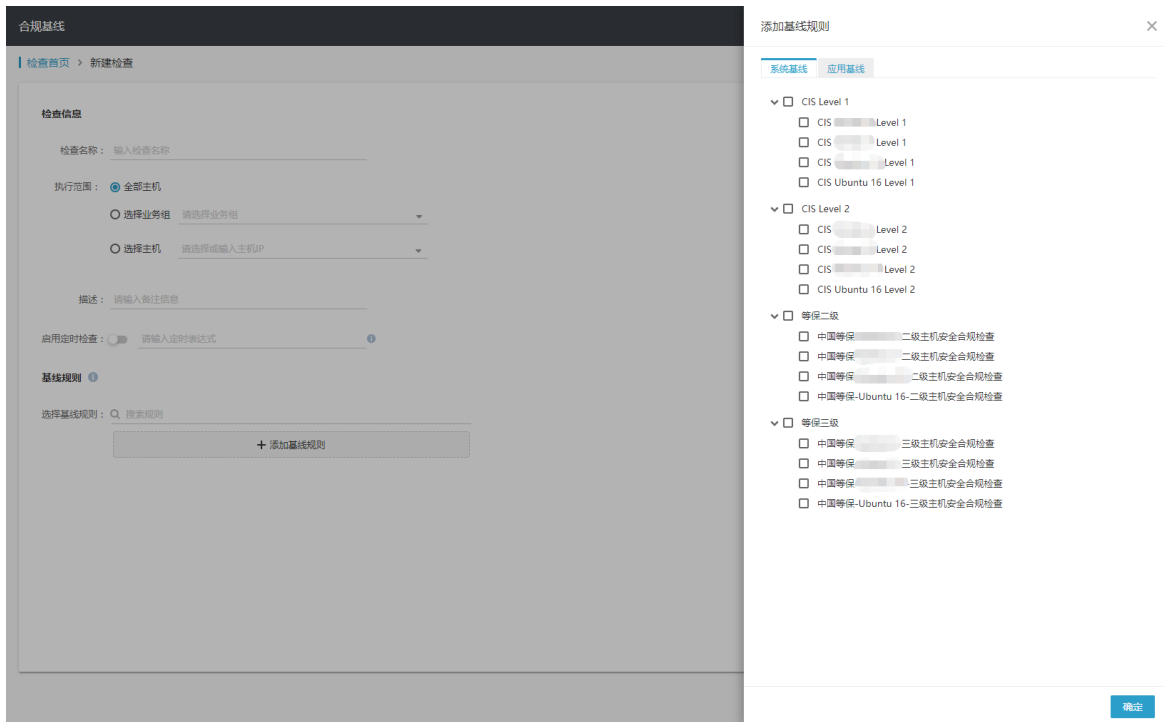


4.4.3 新建检查

单击“新建检查”按钮，进入新建检查页面。



➤ 添加主机规则




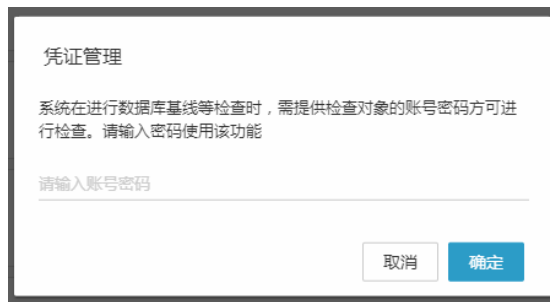
新建检查功能说明

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

	<p>类，每类下又细分为 CIS 和等保基线，基线可多选</p> <p>【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</p> <p>目前支持的系统基线有：windows server 2008/2008 R2/2012/2012 R2</p>
定时检查	<p>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”。</p> <p>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。</p> <p>关闭定时检查开关，则不可以输入定时表达式。</p>
描述	输入对该基线的描述。

4.4.4 凭证管理

单击  按钮，选择“凭证管理”，输入账号密码后进入“凭证管理”页面。

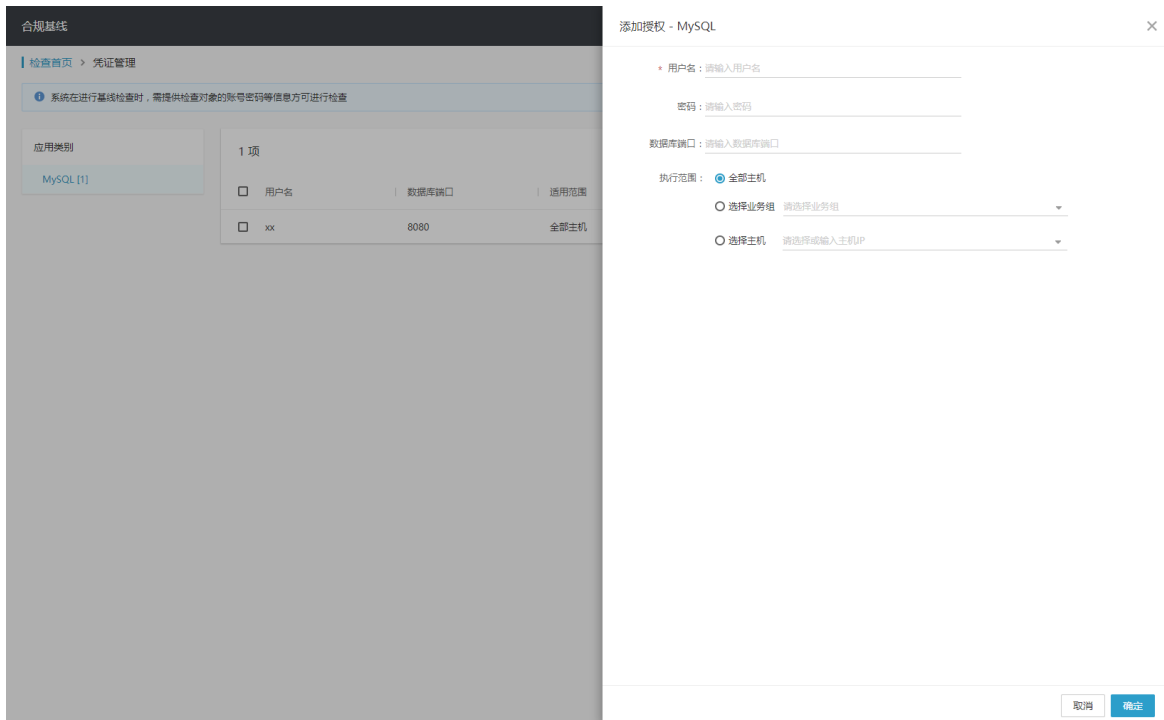


凭证管理管理的凭证用于对应的应用基线的检测。



➤ 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。



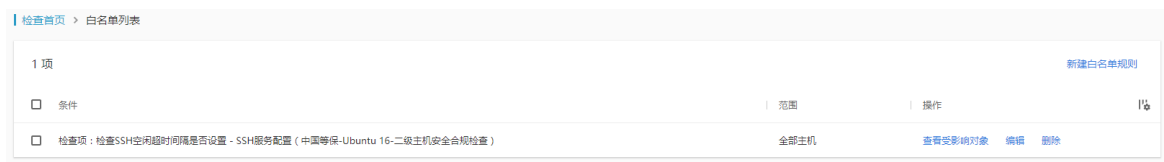
➤ 删除授权

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。



4.4.5 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。



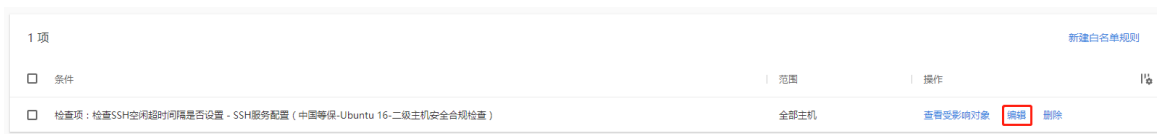
➤ 查看受影响对象

查看现有规则影响的对象。



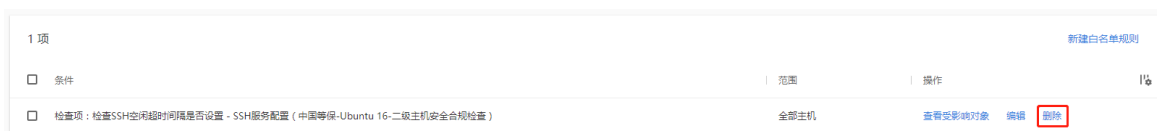
➤ 编辑白名单列表

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。



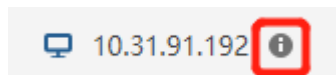
4.4.6 更新数据

单击  按钮，选择“更新数据”，开始更新资产数据。



4.5 单台主机详情

在整个产品功能中，点击“主机 IP”后按钮，即可进入“单台主机详情”功能，该功能是主机相关信息的汇总，方便用户对该主机中存在的问题，进行快速排查。



主要包括 8 个模块：

- 主机信息：主要展示主机相关的信息，包括：基本信息、业务信息、管理信息；
- 硬件配置：主要展示主机的硬件配置信息，包括：硬件信息、网卡信息、磁盘信息；
- 系统账号：主要展示主机中所有的账号列表，资产详情入口 跳转到：账号管理—基本信息查询；
- 开放端口：主要展示主机中所有的端口列表，资产详情入口 跳转到：进程管理—监听端口查询；

- 运行进程：主要展示主机中所有的进程列表，资产详情入口 跳转到：进程管理—基本信息查询；
- 软件应用：主要展示主机中所有的软件应用列表，资产详情入口 跳转到：软件应用—基本信息查询；
- Web 站点：主要展示主机中所有的账号列表，资产详情入口 跳转到：站点管理—Web 站点清点；
- 更多资产：主要汇总展示主机中 “不重要或不常用” 的其它资产，可分为：主机类、业务类，点击跳转到对应页面；

主机信息	基本信息	
硬件配置	主机名: DESKTOP-2NABMOJ	Agent状态: 在线
系统账号	内网IP: 172.16.11.65	安装时间: 2019-04-22 20:53:10
开放端口	外网IP: 58.49.50.122(连接)	最后下线时间: 2019-11-11 09:32:34
运行进程	操作系统: Windows 10 Home China (buil...	最后上线时间: 2019-11-11 09:33:33
软件应用	内核版本: 10.0.18362.329	AgentID: 705c8e5e8d803810
Web 站点	最后登录用户: 352843424@qq.com	Agent版本: 3.3.10-3.66.0-WIN-Rel-2019-...
更多资产	最后登录时间: 2017-10-08 10:54:55	系统启动时间: 2019-11-01 11:25:55
	业务信息	
	资产等级: 普通资产	
	业务组: 产品组/xiaotong	
	标签: --	
	管理信息	
	负责人: --	
	负责人邮箱: --	
最后更新时间: 2019-11-11 09:35:01		
更新数据		确定

点击“更新数据”按钮，可重新获取该主机的资产信息。

五. 通用功能

5.1 系统设置

5.1.1 Agent 安装

Agent 安装提供详细的安装 Agent 方法指引，同时该功能随时检测最新安装的 Agent 主机，用户在安装新 Agent 后，产品中第一时间得到反馈。

Agent 安装说明，用于辅助用户完成 Agent 的基础安装，包含以下几个内容：

1. 安装需求：安装所需的基础环境要求，及必备条件；
2. 设置主机信息：根据用户实际情况，填写待安装主机的相关信息；
3. 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。

5.1.1.1 安装说明

【安装需求】

a. 支持安装的系统版本

1) 支持 64 位 Linux 操作系统，版本包括：

- Oracle: 5、6、7
- RHEL: 5、6、7
- CentOS: 5、6、7
- Ubuntu: 10—16
- SUSE: 11、12
- Debian: 6、7
- OpenSUSE: 10、11、12、13
- NeoKylin (中标麒麟): 6、7
- YHKylin (银河麒麟): 4
- Redflag (红旗): 9
- Deepin (深之度): 15
- iSoft (普华): 4

2) 支持 64 位操作系统，版本包括：

- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Vista
- Windows 7
- Windows 8
- Windows 10

b. 网络通信能力

1) 直连主机

直连主机的防火墙，需确保可与青藤服务器通信；

2) 代理连接

代理连接主机需连通管理服务器的 sock5 代理服务；

c. 其它组件要求

- 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；（openssl 为 Curl 使用的加载库）

【设置主机信息】

选择主机连接方式，包括：直连主机、代理连接；

选择主机所在业务组；



【安装引导】

Linux

点击生成命令，将命令输入到 cmd 中以管理员身份运行。

Windows

有三种安装方法供选择：命令安装、安装包安装、安装包+命令；

1) 命令安装：

——适用于批量安装（需支持 PowerShell 组件）

需传入主机所属"业务组 ID"，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; 可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;



2) 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, 将传入主机所属"业务组 ID"生成的参数, 填入安装程序所需的"安装参数", 点击"安装", 即可安装 Agent;



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

需下载安装包, 传入主机所属"业务组 ID", 和安装包所在位置、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;



5.1.1.2 安装记录

安装成功，可在安装记录中查到相应主机。

操作系统	代理	Agent版本	安装时间	更多		
356 项 刷新 全部导出						
安装时间	主机名	主机IP	操作系统	代理	业务组	
2019-04-08 15:24:50	WIN-PLPKL4TOKFV	已删除主机	Windows Server 2008 R...	直连	flong-win	
2019-03-29 09:58:18	WIN-PLPKL4TOKFV	已删除主机	Windows Server 2008 R...	直连	flong-win	
2019-03-29 09:30:07	192-168-199-148-u...	● 172.16.2.241	Ubuntu 14.04.1 LTS	直连	ubuntu	
2019-03-29 09:29:34	admin.php.com	● 172.16.2.240	CentOS release 6.4 (Final)	直连	centos	
2019-03-28 19:18:46	192-168-199-148-u...	● 172.16.2.241	Ubuntu 14.04.1 LTS	直连	ubuntu	
2019-03-28 19:18:33	admin.php.com	● 172.16.2.240	CentOS release 6.4 (Final)	直连	centos	

5.1.2 主机管理

本页面主要用来管理安装 Agent 的主机，包括新建、编辑、删除业务组；修改主机的业务组划分；修改主机信息；添加主机；添加、编辑、删除主机标签。

5.1.2.1 管理信息设置

The screenshot shows the 'Host Management' (主机管理) interface. On the left, there are tabs for 'Linux' and 'Windows'. Below them is a 'Business Group List' (业务组列表) section with a search bar and a '+' button (labeled 1). The main area shows 'Host Tags' (主机标签) with 'testtag1' and 'tag002' (labeled 3). Below that is a filter section for 'Host Status' (主机状态), 'OS' (操作系统), 'Host IP' (主机IP), and 'Host Name' (主机名). The main table shows 2 items with columns for 'Host IP', 'Business Group', 'Tags', and 'Operations' (labeled 5). The 'Operations' column has 'Modify' (修改) and 'Move' (移动) buttons. A 'Sync Host Information' (主机信息同步) button (labeled 6) is also visible.

① 新建业务组

通过单击 + 按钮，可添加业务组。

新建业务组

业务组名*

请输入业务组名

描述

请输入业务组描述信息

取消 确定

主机管理

Linux Windows

业务组列表 + 刷新

查询业务组 🔍

全部主机 [2]

> ww-linux [2] + ✎ 🗑️

添加业务组

未分组主机 [0]

选择已有业务组，可以添加子业务组，修改业务组，删除业务组。

② 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；

导入业务组

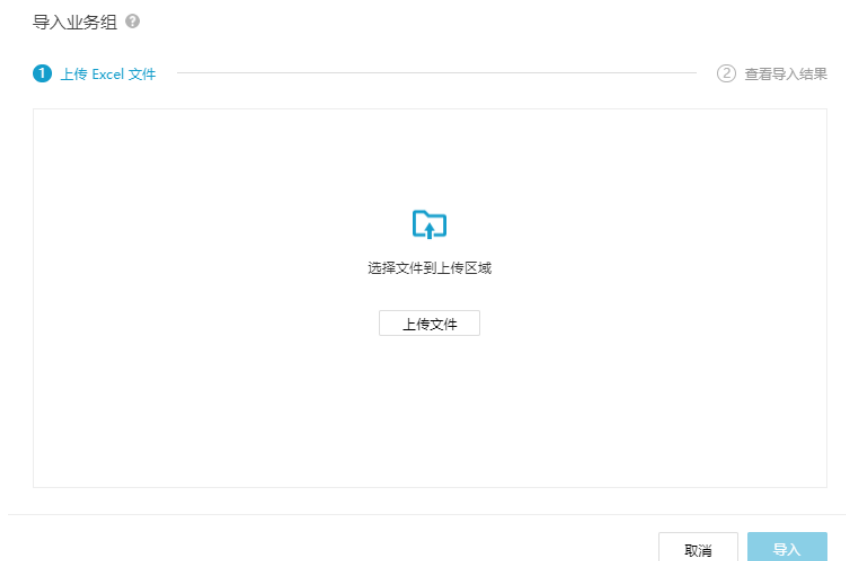
功能说明

1. 使用 Excel 文件导入，批量创建新的业务组。
2. 该功能不可以修改或删除已有业务组，只能用于批量创建新业务组。导入数据包括：业务组名、业务组描述（选填）、适用平台（Linux/Windows二选一，必填）。
3. 为确保能顺利进行导入，Excel 文件请符合以下标准：
 - 请参考 Excel 模板，点击下载当前账号的 [业务组导入模板.xlsx](#)
 - 业务组层级最多为四级
 - 后缀名为 xls 或者xlsx
 - 文件所含数据行数请勿超过1000，系统默认每次仅导入前1000条数据
 - 请务必按照模板中的字段顺序制作表格。不要编辑或删除表格中已有的业务组，若修改了已有的业务组后再导入，将会创建新的业务组，而不是修改已有的业务组。
4. 按照业务组名进行导入，若同级业务组存在重名业务组，将不创建新的业务组。
5. 文件中业务组内容为树形结构，填写方式与系统中的业务组结构一致，模板示例如下：

我知道了，开始导入

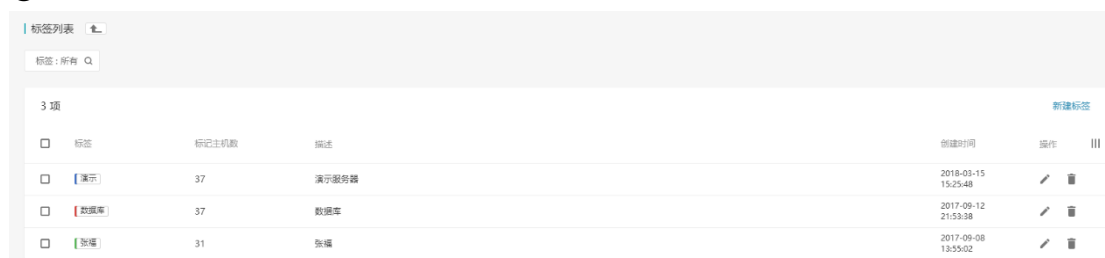
取消

先下载“业务组导入模板”文件，点击“我知道了，开始导入”；



将填好的文件，上传至系统中即可；

③ 主机标签设置



可以新建，编辑，删除标签。

④ 标签按钮

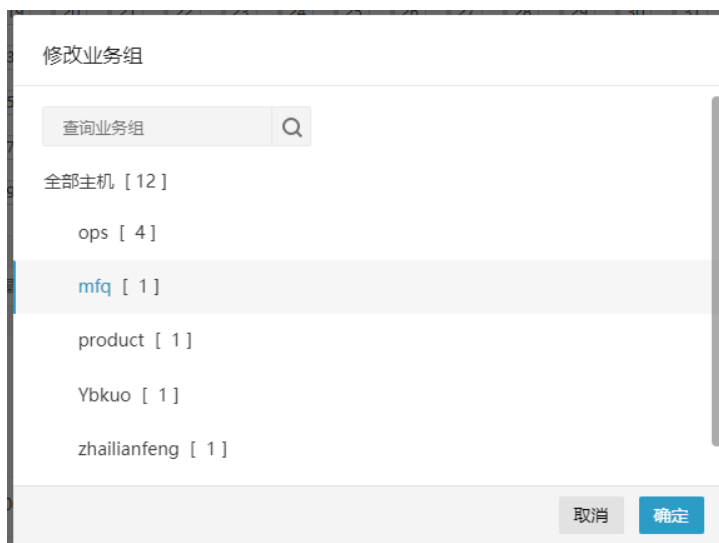
点击标签，可以根据该标签筛选所有拥有该标签的主机。

⑤ 修改移动按钮

单击“修改”进入修改主机信息页面



单击移动按钮移动所选主机到所选业务组。



⑥ 主机信息同步

主机信息同步功能允许用户以主机 IP 或主机名作为唯一标识，使用 Excel 文件批量导入该主机的管理信息。

主机信息同步

功能说明

1. 主机信息同步功能允许用户以主机IP或主机名作为唯一标识，使用 Excel 文件批量导入该主机的管理信息
2. 可同步的管理信息包括：资产等级、负责人、负责人邮箱、机房位置、固定资产编号、标签、备注
3. 为确保能顺利进行导入，Excel 文件请符合以下标准：
 - 请参考 Excel 模板，点击下载 [主机信息同步Excel模板.xls](#)
 - 后缀名为 xls 或者xlsx
 - 文件所含数据行数请勿超过65535，超过可以分多次上传
 - 请务必按照模板中的字段顺序制作表格。其中 Excel 中主机 IP 和主机名为必填字段，其他字段为选填字段，多个标签字段则以英文逗号分隔
4. 按照主机名/主机IP进行同步，某个主机名/主机IP存在多条记录时，导入的是最后一条的数据

[我知道了，开始导入](#)

取消



5.1.2.2 规则设置

通过设置主机规则，可以批量设置各类主机信息，包括移动业务组、打标签、编辑运维信息等。

在首页点击  符号，选择“规则设置”，进入主机规则列表。



- 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。

- 新建规则

点击新建规则，将进入“新建规则”界面：

新建主机规则

同时满足条件： 主机名中包含：

主机IP在以下范围内： [添加](#)

则执行以下操作： 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：

[收起](#)

使用范围： 全部主机

业务组：

描述：

[新建](#) [取消](#)

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。

主机范围： 全部主机、业务组。

描述： 规则描述。

5.1.3 IP 显示管理

该功能使用户可以根据自己主机的网卡情况，自定义设置在界面列表中显示的 IP 信息。

IP显示列表		自定义IP显示规则	
显示的主机IP: 所有			
266 项			
<input type="checkbox"/> 主机IP	业务组	主机的所有IP	
<input type="checkbox"/> 10.165.18.119 (内网)	测试组	10.165.18.119 (内网) 115.28.85.207 (外网) 115.28.85.207 (连接)	
<input type="checkbox"/> 10.29.243.96 (内网)	虚拟化环境	10.29.243.96 (内网) 121.42.227.46 (外网) 121.42.227.46 (连接)	
<input type="checkbox"/> 10.29.243.93 (内网)	虚拟化环境	10.29.243.93 (内网) 121.42.227.6 (外网) 121.42.227.6 (连接)	
<input type="checkbox"/> 10.163.246.177 (内网)	虚拟化环境	10.163.246.177 (内网) 121.42.12.91 (外网) 121.42.12.91 (连接)	
<input type="checkbox"/> 10.144.68.123 (内网)	测试组	10.144.68.123 (内网) 115.28.0.20 (外网) 115.28.0.20 (连接)	
<input type="checkbox"/> 192.168.178.152 (内网)	虚拟化环境	192.168.178.152 (内网) 183.37.227.38 (连接)	
<input type="checkbox"/> 200.200.66.149 (外网)	测试组	200.200.66.149 (外网) 14.153.223.73 (连接)	
<input type="checkbox"/> 11.16.1.26 (外网)	虚拟化环境	11.16.1.26 (外网) 113.99.105.71 (连接)	
<input type="checkbox"/> 192.168.0.104 (内网)	虚拟化环境	192.168.0.104 (内网) 113.90.17.127 (连接)	
<input type="checkbox"/> 192.168.197.110 (内网)	虚拟化环境	192.168.197.110 (内网) 211.103.231.218 (连接)	

5.1.3.1 自定义 IP 显示规则

- 新建规则

定义 IP 段的 IP 地址为优先显示的主机 IP

新建 IP 显示规则

规则内容: 将下面IP段的IP

请输入开始IP _____ — 请输入结束IP _____

优先显示为主机IP

规则范围:

全部主机

自定义范围

业务组: 请选择业务组 _____

主机: 请选择主机IP _____

[创建并执行](#) [取消](#)

- 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。

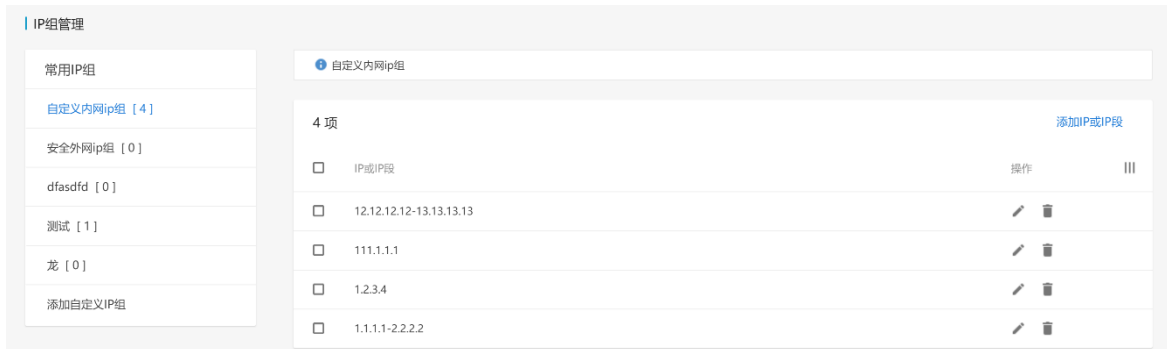
自定义 IP 显示规则					
对范围内的主机设置自定义IP显示规则。根据规则优先显示在规则IP段中的IP信息。如果有多个IP在该IP段内，优先显示较小的IP。					
规则IP段: 所有		范围: 所有			
1 项					新建规则
<input type="checkbox"/> 规则IP段	规则范围	修改时间	受影响对象	操作	
<input type="checkbox"/> 192.168.235.1 - 192.168.235.254	192.168.235.137	2018-04-14 15:25:49	查看详情	编辑	删除

5.1.4 IP 组管理

在全局设置中增加"IP 通用设置", 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:

- 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；
- 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；



5.2 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，其主要场景如下：

1. 发现未安装 agent 的主机
2. 管理/标记发现的主机
3. 自动化的批量部署 agent
4. 定期得到主机的变化通知

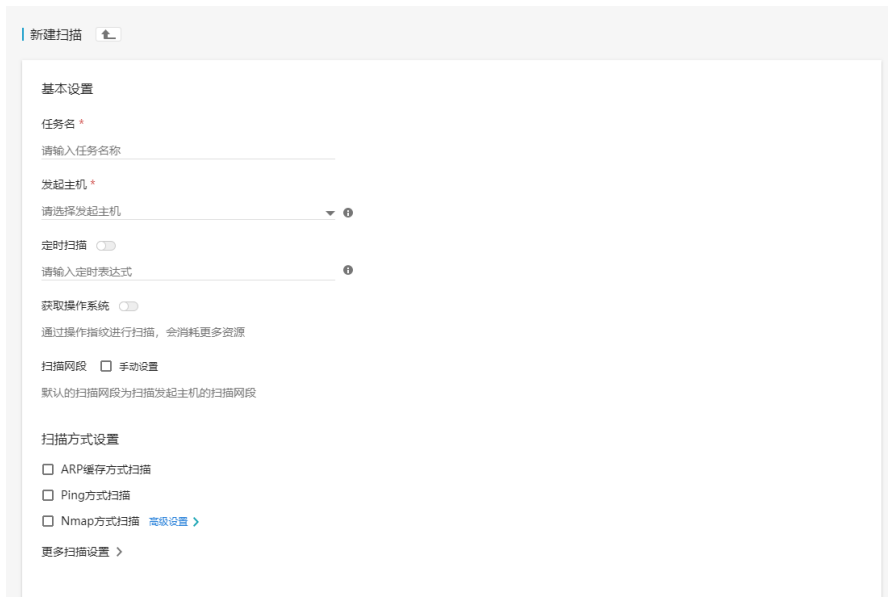
在安装了 agent 主机的主机上，通过定期的主动探测，发现网络内还存在的未安装 Agent 的主机。为了能够更加精准的发现网络内其他的主机，同时还能兼顾在用户网络环境内不会消耗过多资源，用户需要根据每种发现方法不同属性和自身网络环境情况进行设置。主要有以下三种发现方法：

- **ARP 缓存发现：**Address Resolution Protocol（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**

5.2.1 设置扫描任务

- 新建扫描

系统管理-主机发现-扫描任务设置-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。扫描任务的配置包括基本设置和高级扫描设置。



扫描项说明

基本设置

1.1 扫描任务名（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 扫描发起主机（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：

1. 全部主机
2. 业务组
3. 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：

定时表达式

定时执行使用crontab通用语法,有5个字段,分别如下:

1. 分钟,允许值 "0-59" ;
2. 小时,允许值 "0-23" ;
3. 日期,允许值 "1-31" ;
4. 月份,允许值 "1-12" ;
5. 星期,允许值 "0-6" ;

此外每个字段可输入如下特殊字符:

- "*" :表示任何时刻;
- "," :表示分割;
- "-" :表示一个段,例如1-5;
- "/n" :表示每隔n的单位执行一次;

提示:

日期和星期不可以同时设置具体的值。

0 0 1,15 * 1 (X)

一些示例:

```
0 17 * * *      每天 17:00 执行
0 17 * * 1      每周一的 17:00 执行
0,10 17 * * 0,2,3 每周日,周二,周三的17:00和17:10执行
42 4 1 * *      每月1日的 4:42分 执行
0 21 * * 1-6    周一到周六 21:00 执行
*/10 * * * *    每隔10分 执行
0 */1 * * *     每时0分 每隔1小时 执行
2 8-20/3 * * *  8:02,11:02,14:02,17:02,20:02 执行
30 5 1,15 * *   1日 和 15日的 5:30 执行
```

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 操作系统发现(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)。

高级设置

高级扫描设置用来设置用户扫描的方法。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。

2.1 Nmap 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。

更多高级设置 更多高级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. 最大并发扫描数量
2. 每秒最大包数
3. 服务器下发任务的间隔(可以精确到小数点后一位，需要设置上限，以秒为单位)

- 立即运行扫描

立即运行扫描是指的立刻开始某个扫描任务，而不是等待其到相应的时间再开始任务。



- 删除扫描

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



5.2.2 扫描结果列表

展示所有发现的网络环境中，未安装 Agent 的主机资产。

扫描结果

首次发现时间: 全部 ▼ 最后发现时间: 全部 ▼ 设备类型: 全部 ▼ 操作系统: 全部 ▼ 更多 ▼ 设置扫描任务 主机忽略列表

4 项 全部导出

<input type="checkbox"/>	MAC地址	设备类型	主机IP	操作系统	发现方法	首次发现时间	最后发现时间	
<input type="checkbox"/>	00:50:56:C0:00:08	VMware	192.168.80.1		NMAP(TCP)扫描	2019-11-11 11:47:57	2019-11-11 11:47:57	
<input type="checkbox"/>	00:50:56:F3:C4:88	VMware	192.168.80.2		NMAP(TCP)扫描	2019-11-11 11:47:57	2019-11-11 11:47:57	
<input type="checkbox"/>	00:0C:29:47:79:2A	VMware	192.168.80.162		NMAP(TCP)扫描	2019-11-11 11:47:57	2019-11-11 11:47:57	
<input type="checkbox"/>	00:50:56:F9:09:68	VMware	192.168.80.254		NMAP(TCP)扫描	2019-11-11 11:47:57	2019-11-11 11:47:57	

5.2.3 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，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。

忽略主机 ↑

设备类型: 全部 ▼ 操作系统: 全部 ▼ 发现方法: 全部 ▼ 主机IP: 全部 Q

290 项

<input type="checkbox"/>	MAC地址	设备类型	主机IP	操作系统	发现方法	首次发现时间	最后发现时间	
<input type="checkbox"/>	00:50:56:C0:0...	VMware	192.168.202.1		ARP缓存扫描	2017-10-10 16:36:11	2017-10-17 11:50:54	
<input type="checkbox"/>	00:50:56:FD:8...	VMware	192.168.202....		ARP缓存扫描	2017-10-10 16:36:11	2017-10-10 16:36:20	
<input type="checkbox"/>	00:50:56:E1:5...	VMware	134.96.255.254		ARP缓存扫描	2017-10-10 16:36:19	2017-10-10 16:36:19	

忽略主机 ↑

设备类型: 全部 ▼ 操作系统: 全部 ▼ 发现方法: 全部 ▼ 主机IP: 全部 Q

< 50/ 290 项 取消忽略

<input checked="" type="checkbox"/>	MAC地址	设备类型	主机IP	操作系统	发现方法	首次发现时间	最后发现时间	
<input checked="" type="checkbox"/>	00:50:56:C0:0...	VMware	192.168.202.1		ARP缓存扫描	2017-10-10 16:36:11	2017-10-17 11:50:54	
<input checked="" type="checkbox"/>	00:50:56:FD:8...	VMware	192.168.202....		ARP缓存扫描	2017-10-10 16:36:11	2017-10-10 16:36:20	
<input checked="" type="checkbox"/>	00:50:56:E1:5...	VMware	134.96.255.254		ARP缓存扫描	2017-10-10 16:36:19	2017-10-10 16:36:19	

5.3 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。

报表列表

1 报表系统可 **创建报表** 导出报表文件，并对报表任务和报表文件进行管理。

创建时间：全部 | 报表类型：全部 | 报表模板：全部 | 报表名称：全部

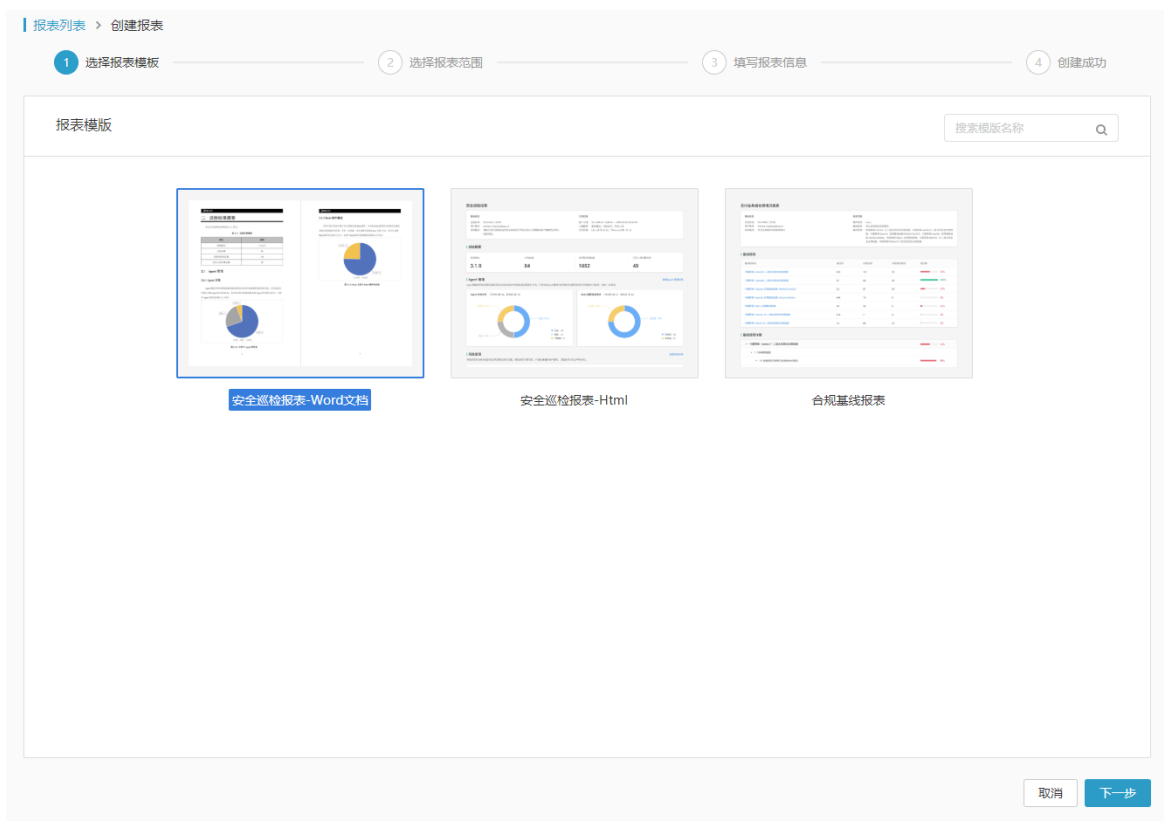
31 项	创建时间	报表名称	报表类型	执行范围	最后生成时间	操作
<input type="checkbox"/>	2019-03-11 15:49:44	合规基线报表	合规基线	全部主机	2019-03-11 15:49:45	下载报告 执行 ...
<input type="checkbox"/>	2019-03-11 15:48:48	安全巡检报表-HTML	安全巡检	全部主机	2019-03-11 15:48:49	下载报告 执行 ...
<input type="checkbox"/>	2019-03-11 15:47:58	安全巡检报表	安全巡检	全部主机	2019-03-11 15:48:02	下载报告 执行 ...
<input type="checkbox"/>	2019-02-13 20:59:05	flong-test-html-detail	安全巡检	全部主机	2019-02-13 20:59:06	下载报告 执行 ...
<input type="checkbox"/>	2019-02-13 20:54:47	flong-test-html	安全巡检	全部主机	2019-02-13 21:00:53	下载报告 执行 ...

[创建报表](#)

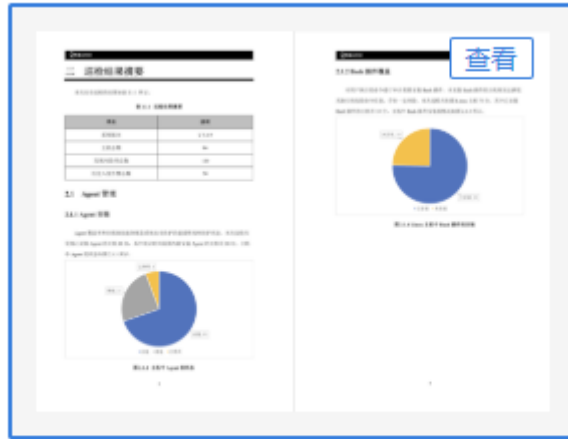
5.3.1 创建报表

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。
悬停点击查看：



安全巡检报表-Word文档

预览报表模板：

安全巡检报表-Word文档

安全巡检主要是通过青藤云安全对评估范围内的服务器和网络、安全设备进行安全扫描，对被评估对象进行一系列的安全分析与探测，以发现目标存在的安全隐患并确实的告知修复建议，是安全体系搭建工作中修复安全风险，提升安全等级的重要工作之一。

一 概述

- 1.1 评估人员
- 1.2 评估时间
- 1.3 巡检范围
- 1.4 巡检内容

二 巡检结果摘要

- 2.1 Agent管理
 - 2.1.1 Agent安装
 - 2.1.2 Bash插件覆盖
- 2.2 风险发现
 - 2.2.1 风险项统计
 - 2.2.2 风险项趋势
 - 2.2.3 各危险程度风险分布
 - 2.2.4 业务组风险情况

关闭
使用模板

➤ 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。

报表列表 > 创建报表

选择报表模板 2 选择报表范围 3 填写报表信息 4 创建成功

选择报表范围

报表模板：安全巡检报表-Word文档

报表版本：概览版

功能范围：Agent管理, 风险发现, 入侵检测

统计时间：请选择时间区域：全部

主机范围： 全部主机

取消 上一步 下一步

➤ 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。

报表列表 > 创建报表

选择报表模板 选择报表范围 3 填写报表信息 4 创建成功

填写报表信息

报表名称：请输入报表名称，不要包含特殊字符 \ / : * ? * < > |

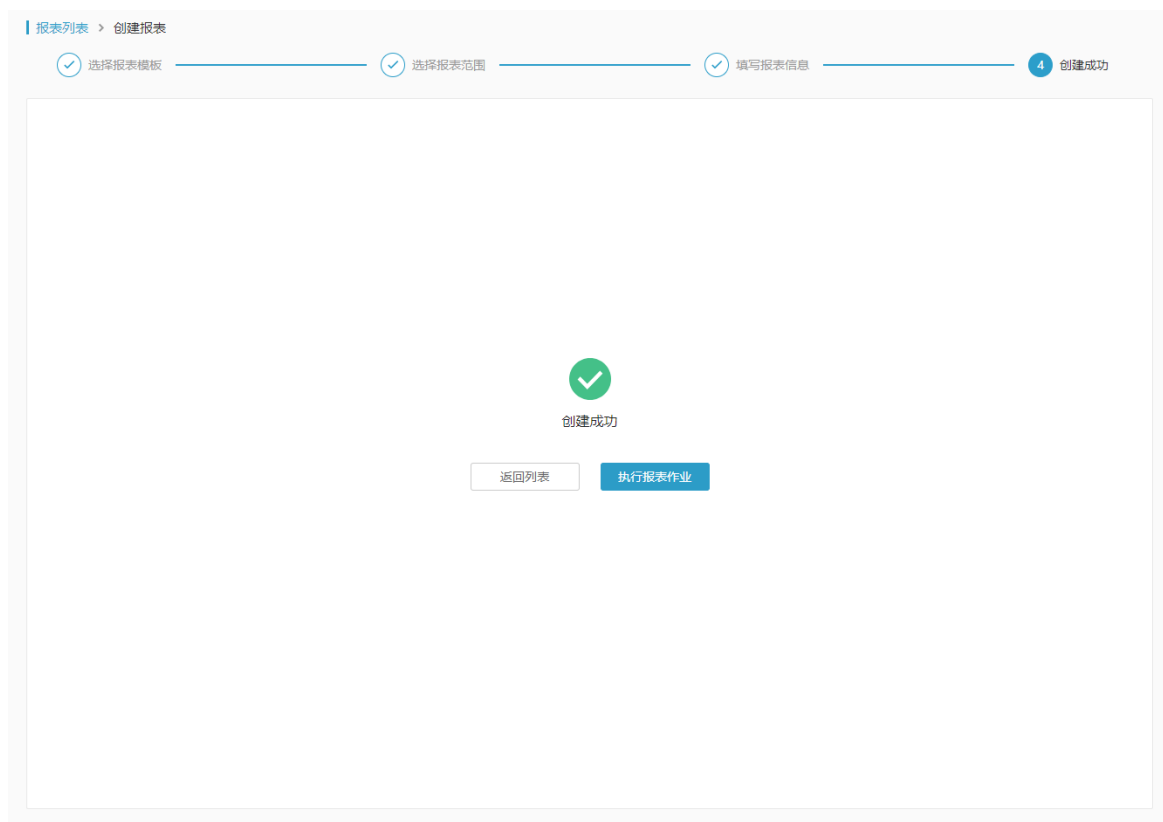
报表描述：请输入报表描述

启用定时检查： 请输入定时表达式 ?

取消 上一步 创建

➤ 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。



5.3.2 报表列表

➤ 执行

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。

<input type="checkbox"/>	创建时间	报表名称	报表类型	执行范围	最后生成时间	操作	🔍
<input type="checkbox"/>	2019-04-11 18:43:19	报表任务测试	安全巡检	全部主机	--	下载报告 执行 ...	

➤ 下载报表

执行报表作业后，点击操作的“下载报告”按钮，可以下载最近一次生成的报表。

<input type="checkbox"/>	创建时间	报表名称	报表类型	执行范围	最后生成时间	操作	🔍
<input type="checkbox"/>	2019-04-11 18:43:19	报表任务测试	安全巡检	全部主机	2019-04-11 18:54:16	下载报告 执行 ...	

➤ 修改/删除任务

点击操作下拉框的“修改/删除”按钮，可以修改或删除报表。



➤ 查看执行记录

点击操作下拉框的“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。



5.4 权限管理

5.4.1 账号管理

管理可以登录前台页面的账号，看到账号名，账号创建时间，账号状态等基本信息。可以通过条件筛选已经存在的用户账号；新建账号；编辑修改已有账号；删除账号。



角色：有默认角色和自定义角色两大类，用户可以通过角色来筛选显示账号。

- 默认角色：不可删除和编辑。
- 自定义角色：不同公司可根据需要新建自定义角色

用户组：账号管理员可以给账号添加其所属的用户组。一个账号可以属于多个用户组。

业务组：账号所属的业务组

账号状态：账号状态有禁止登陆、允许登陆、停用三种状态。

- 禁止登录：账号不允许登录，但产品功能仍在运行，无法登录查看结果或执行操作。若公司账号被禁止登录，则其子账号也被禁止登录。
- 允许登陆：指账号可以正常登录并使用产品功能。
- 停用：账号无法登陆，且账号被停用后无法修改为其他状态。

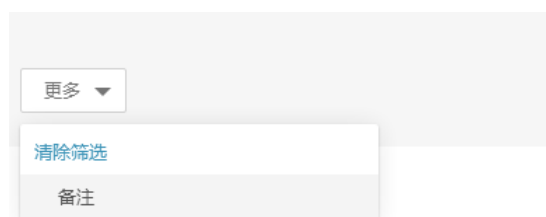


账号名：用户用于登录的字段，其全局唯一。当前使用邮箱作为账号名。这里可以通过账号名查找筛选账号。



姓名：一般为账号拥有者的姓名，可以包含中英文、数字或字符，最长 128 个字节

更多：该下拉菜单可以清除筛选条件；增加显示备注列。



5.4.1.1 新建账号

新建账号

账号名 *
请输入账号名

初始密码 *
请输入初始密码

启用LDAP认证 ⓘ

姓名 *
请输入使用者姓名

邮件 *
请输入邮件地址

取消 确定

新建账号时需要输入以下必选信息：

- 账号名：必须为邮箱。
- 初始密码：创建者自己设定初始密码。
- 选择是否启用 LDAP 认证：使用 LDAP 认证账号身份，开启后需使用 LDAP 的密码登录（需先配置 LDAP 参数信息）；
- 姓名：建议为创建者真实姓名。
- 邮件：用户的联系邮箱，之后会用户接收邮件通知
- 手机号：建议为创建者真实手机号。

以上信息在新建子账号完毕后，自动发送至子账号邮箱。

5.4.1.2 修改账号

账号管理

角色：全部 ▾ 用户组：全部 ▾ 账号状态：全部 ▾ 账号名：全部 🔍 姓名：全部 🔍 更多 ▾

2 项 新建账号 LDAP配置

<input type="checkbox"/>	账号名	创建时间	账号状态	操作
<input type="checkbox"/>	abc	2019-11-11 11:39:12	允许登录	
<input type="checkbox"/>	test	2019-11-11 11:50:35	禁止登录	

择要修改的账号名，单击右侧编辑标签按钮，即可修改当前选定账号信息。

主要选项如下：

- 账号总览：

查看与账号相关信息，包括账号名称，创建时间，账号状态 LDAP 认证，所属用户组，账号角色，业务组，上次登录时间。

账号详情 ↑

账号总览 基本信息 修改密码 所属用户组 角色设置 管理业务组

账号总览

账号名称: jiewen

创建时间: 2017-09-25 11:20:41

账号状态: 允许登录 [修改](#)

LDAP认证: -- [修改](#)

所属用户组: 无

账号角色:

账号角色	来源
普通用户	账号

业务组: aws 云主机, test2

上次登录时间: 2017-09-25 11:44:10

- 基本信息

拥有账号管理权限的用户的账号的基本信息，例如：姓名、邮箱、手机号、部门、职位、公司名称、公司地址、备注，在这里可以输入、修改这些信息。

账号详情 ↑

账号总览 基本信息 修改密码 所属用户组 角色设置 管理业务组

基本信息

姓名 *
lizhi

邮箱 *
jfsahdfi@asdjd.com

手机号 *
请输入手机号码

部门
请输入部门

职位
请输入职位

公司名称
请输入公司名称

公司地址
请输入公司地址

备注
请输入公司备注

[保存](#)

- 修改密码

超级管理员或账号管理员可以修改账号的密码，密码规则见下。修改完毕后，被修改的账号会收到邮件通知，新密码会在邮件中明文显示。

建议用户不定期修改密码（如至少 90 天修改一次），密码要求如下：

长度为 8-20 位

只能包含大小写字母、数字、符号（不能包含空格）

至少包括大小写字母、数字、符号 4 种里的 2 种

密码强度规则如下：

强：8-20 位，包括大小写、数字、符号 4 种；或 11-20 位，包括 4 种里的 3 种

中：8-10 位，包括 4 种里的 3 种；或 11-20 位，包括 4 种里的 2 种

弱：8-20 位，包括 4 种里的 1 种；或小于 8 位，无论包括几种

- 所属用户组

新增用户组

删除用户组

账号详情

账号总览 基本信息 修改密码 所属用户组 角色设置 管理业务组

用户组: 所有 备注: 所有

4 项 新增用户组

<input type="checkbox"/>	用户组	备注	操作
<input type="checkbox"/>	111	111	
<input type="checkbox"/>	ztest	ztest	
<input type="checkbox"/>	安全部门	安全管理功能	
<input type="checkbox"/>	测	测	

- 角色设置

账号详情

账号总览 基本信息 修改密码 所属用户组 角色设置 管理业务组

角色名称: 所有 备注: 所有

3 项 添加角色

<input type="checkbox"/>	角色名称	备注	角色来源	操作
<input type="checkbox"/>	普通用户	拥有所有普通功能权限，但不提供任何高级功能（权限管理，主机管理，主机发现，任务系统），...	用户组	
<input type="checkbox"/>	测试	测试	账号	
<input type="checkbox"/>	123	123	用户组	

账号管理员可以将账号赋予为角色，从而有相应功能权限（如：“超级管理员”“普通用户”“审计员”“只读普通用户”或者其他自定义角色。）

- 管理业务组

账号详情

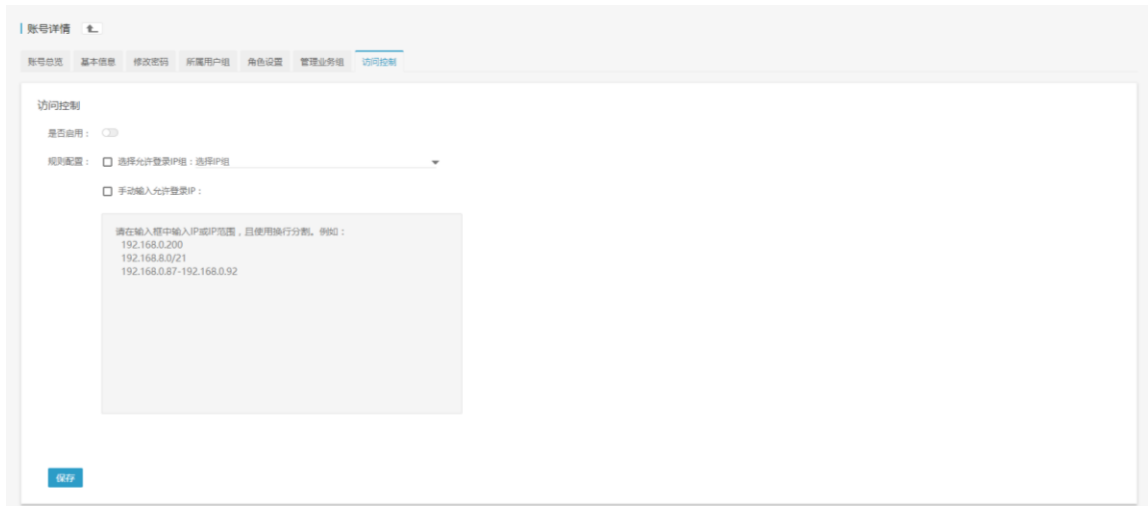
账号总览 基本信息 修改密码 所属用户组 角色设置 管理业务组 访问控制

Linux业务组 | Windows业务组 同步设置

业务组	备注	业务组来源	是否可管理
全部主机	--		<input type="checkbox"/>
未分组主机	--	--	<input type="checkbox"/>
> ww-linux	--	--	<input type="checkbox"/>

账号管理员给账号分配自己管理范围内的业务组，勾选成功后单击“同步设置”即可完成同步。

- 访问控制



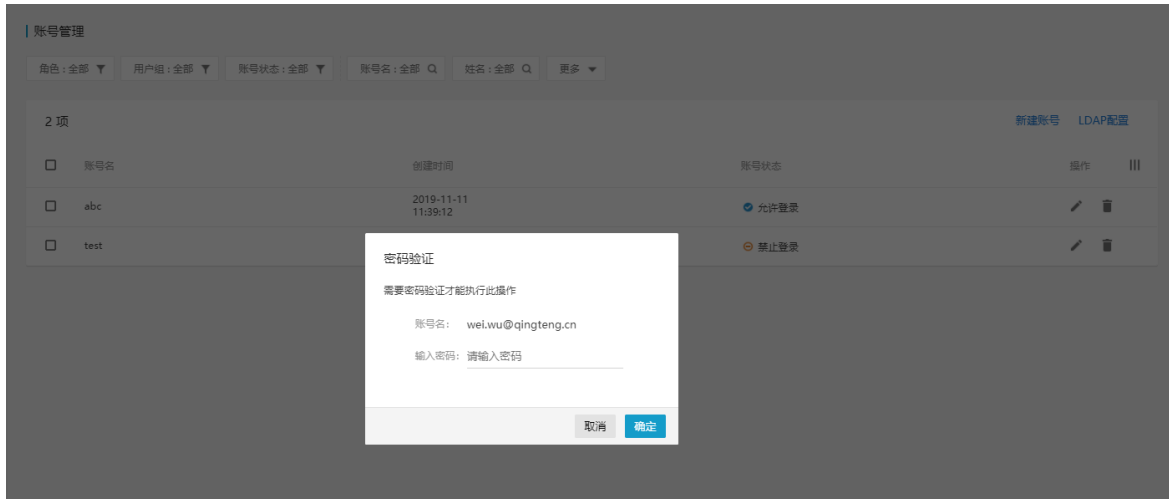
访问控制用于限制登录 IP，用户可设置该账号哪些主机 IP 可进行登录，可选择启用/禁用，未启用时不限制登录的 IP，设置完后需点击“保存”才能保存当前设置。

5.4.1.3 删除账号

用户账号只能在 console 由超管或其创建者删除，删除时需要输入操作者的登录密码进行验证。



需要验证密码才可删除。



5.4.1.4 LDAP 配置

对于使用 LDAP 系统登录的公司，需要配置 LDAP 参数：

- 服务地址：LDAP 访问的目标地址，可为域名或 IP；
- 目标地址：LDAP 访问的目录路径，类似于“ou=xxx, dc=yyy”；
- 端口访问：LDAP 访问端口；
- 加密方式：可选无加密、SSL 加密、TLS 加密；
- 是否匿名访问：是否允许你们访问；
- 查询用户 DN：如为匿名访问时，需输入查询用户 DN，类似于“CN=xxx,CN=yyy”；
- 查询用户密码：如为匿名访问时，需输入查询用户密码；

点击“测试”按钮，可以测试当前配置是否正确，点击“保存”按钮，保存该 LDAP 配置。



5.4.2 用户组管理

用户组概念类似于 Linux 中的用户和用户组概念，账号管理员可以给账号添加其所属的用户组。一个账号可以属于多个用户组。



The screenshot shows a web interface for '用户组管理' (User Group Management). It features search filters for '用户组' and '备注', a '新建用户组' button, and a table with columns for selection, name, remark, creation time, and actions.

<input type="checkbox"/>	用户组	备注	创建时间	操作
<input type="checkbox"/>	平安健康	123	2017-09-25 11:26:01	
<input type="checkbox"/>	环境组	测试业务组1	2017-08-14 17:36:12	
<input type="checkbox"/>	用户组测试	测试用户组功能	2017-11-24 11:06:08	

5.4.2.1 新建用户组

单击“新建用户组”按钮，进入到新建用户组页面，输入用户组名称和备注两项，然后单击“确定”按钮，即可新建一用户组。



The screenshot shows a form titled '新建用户组' (New User Group). It contains two input fields: '用户组 *' (User Group) with the placeholder '请输入名称' (Please enter name), and '备注 *' (Remarks) with the placeholder '请输入备注' (Please enter remarks). At the bottom, there are '取消' (Cancel) and '确定' (Confirm) buttons.

5.4.2.2 修改用户组信息

单击 按钮，进入编辑用户组页面，可以看到有基本信息、成员管理、角色设置、管理业务组四个选项卡。



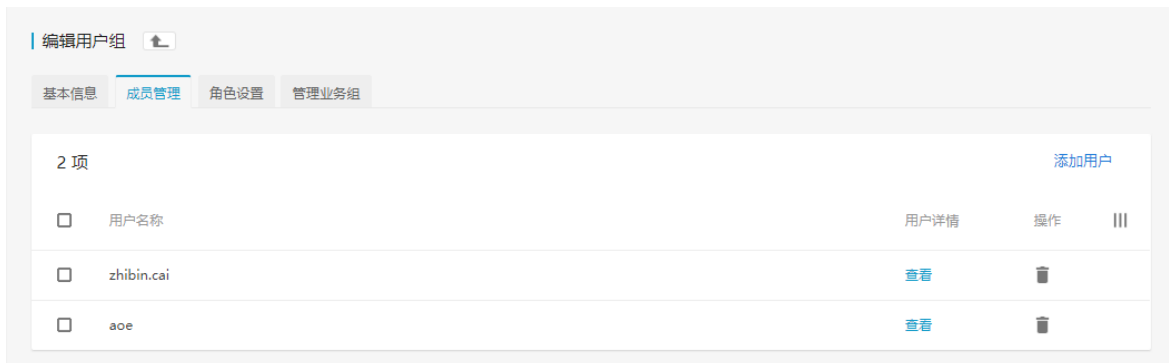
1) 基本信息

基本信息页面可以查看用户、创建用户组的时间、备注。



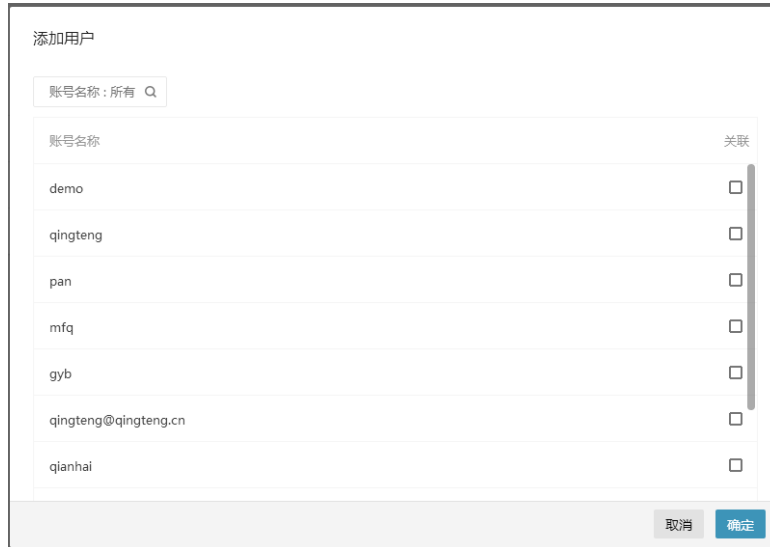
2) 成员管理

可以管理用户组中的成员账号，添加、查看、删除用户组中的成员。



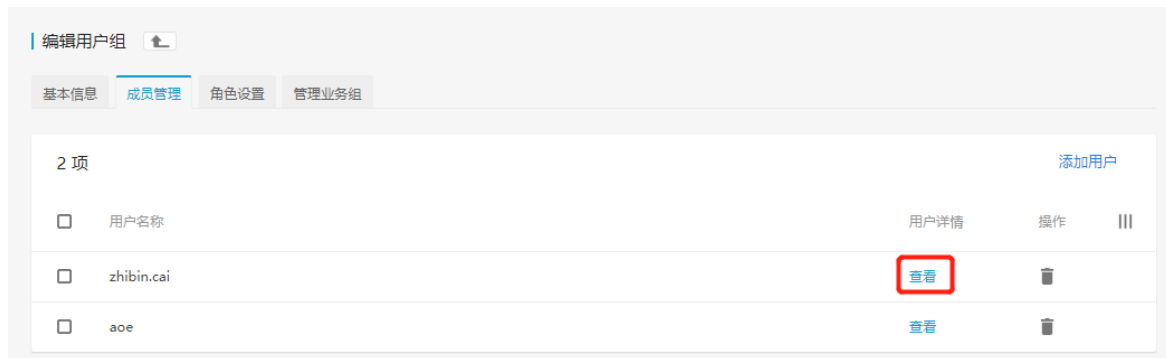
- 添加用户

勾选对应账号后的复选框，即可把勾选的账号添加到当前用户组下。



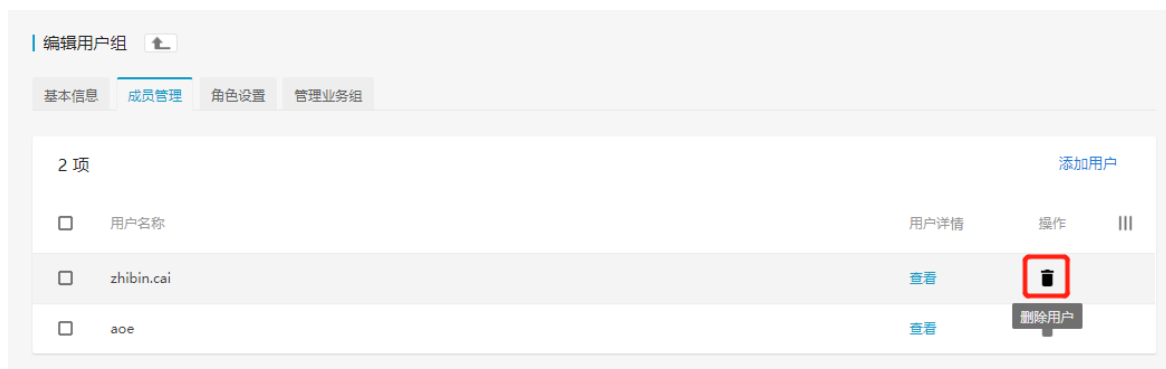
- 查看

此处“查看”按钮是查看对应账号的详细资料跳转到账号资料页面。



- 删除

将对应账号从当前用户组中删除。



3) 角色设置

为当前用户组下的账号添加或者删除角色。



- 添加角色

单击“添加角色”按钮，进入添加角色页面，勾选要添加的角色点击确定。



- 删除

单击删除按钮即可删除已经创建的角色。



4) 管理业务组

可以给已有的用户组管理不同业务组的权限。勾选复选框后单击“同步设置”即可完成同步。



5.4.2.3 删除用户组

单击删除按钮即可删除对应的用户组。



5.4.3 角色管理

角色：有默认角色和自定义角色两大类，用户可以通过角色来筛选显示账号。

- 默认角色：不可删除和编辑。
 - 超级管理员：拥有所有功能权限；
 - 普通用户：拥有所有普通功能权限，但不提供任何高级功能（权限管理，主机管理，主机发现，任务系统）；通知系统仅提供一般通知权限；
 - 审计员：仅可以查看系统的所有功能操作记录；
 - 只读普通用户：拥有所有普通用户功能，仅拥有读权限，无法进行业务操作；
- 自定义角色：不同公司可根据需要新建自定义角色

角色管理

角色状态: 全部 ▼ 角色名称: 全部 🔍 备注: 全部 🔍

9 项 新建角色

<input type="checkbox"/>	角色名称	备注	角色状态	操作	⋮
<input type="checkbox"/>	普通用户	拥有所有普通功能权限，但不提供任何高...	启用		
<input type="checkbox"/>	超级管理员	拥有所有功能权限	启用		
<input type="checkbox"/>	2.0	2.0	启用		
<input type="checkbox"/>	sadf	sadf	启用		
<input type="checkbox"/>	test	test	启用		
<input type="checkbox"/>	test_man	test_man	启用		
<input type="checkbox"/>	ztest	ztest	启用		
<input type="checkbox"/>	入侵功能	入侵功能	启用		
<input type="checkbox"/>	测试角色	测试角色	启用		

5.4.3.1 新建角色

单击新建角色按钮进入新建角色页面。

新建角色

角色名称 *
请输入角色名称

角色状态 *
请选择角色状态

描述
请输入角色描述

取消 确定

5.4.3.2 修改（编辑）

单击编辑按钮即可编辑现有角色，进入角色编辑页面后可看到基本信息，权限信息，关联账号三个选项。

角色管理

角色状态: 全部 ▼ 角色名称: 全部 🔍 备注: 全部 🔍

9 项 新建角色

<input type="checkbox"/>	角色名称	备注	角色状态	操作	⋮
<input type="checkbox"/>	普通用户	拥有所有普通功能权限, 但不提供任何高...	启用		
<input type="checkbox"/>	超级管理员	拥有所有功能权限	启用		
<input type="checkbox"/>	2.0	2.0	启用		
<input type="checkbox"/>	sadf	sadf	启用		
<input type="checkbox"/>	test	test	启用		
<input type="checkbox"/>	test_man	test_man	启用		
<input type="checkbox"/>	ztest	ztest	启用		
<input type="checkbox"/>	入侵功能	入侵功能	启用		
<input type="checkbox"/>	测试角色	测试角色	启用		

5) 基本信息

可以查看或修改当前角色基本信息, 包括角色信息, 角色状态和备注信息。

编辑角色

基本信息 权限信息 关联账号

基本信息

角色名称 *
sadf

角色状态
 启用 禁用

备注
sadf

保存

6) 权限信息

查看修改当前角色拥有什么模块的权限



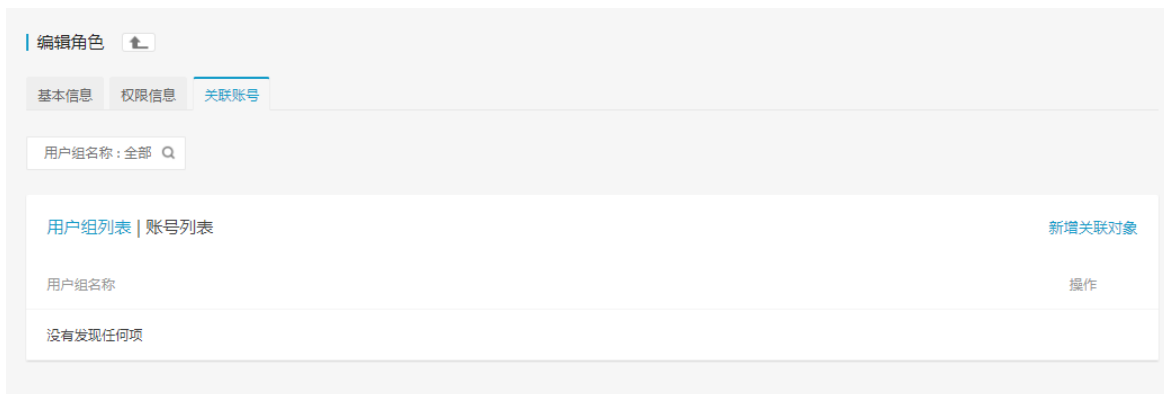
7) 添加授权

单击“添加授权”按钮进入到添加授权页面，可以通过勾选复选框为当前角色添加对应权限。单击“确定按钮”可保存退出。

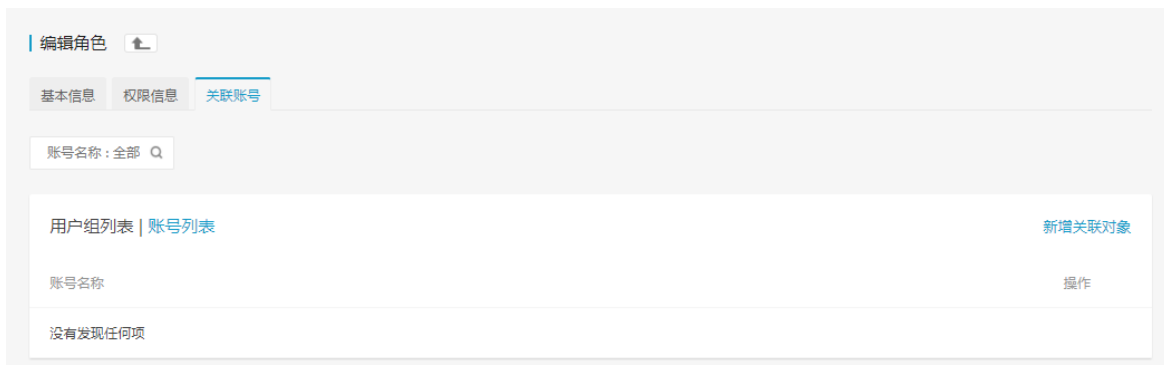


8) 关联账号

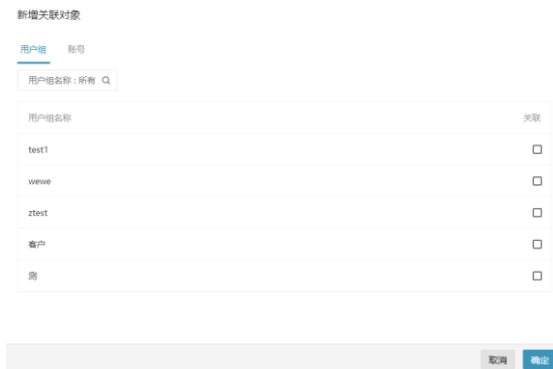
用户组列表视图



账号列表视图



新增关联对象



5.4.3.3 删除

单击右侧“删除”按钮，可删除对应的角色。



5.5 服务工具

5.5.1 Agent 管理

Agent 管理主要用来管理和 Agent 的运行状态，包括：

主机 IP，内网 IP，外网 IP，主机名，通信状态（连通/断开），是否频繁掉线，设备 UUID，Agent ID，业务组，备注，主机标签，运行级别，日志级别，Agent 版本，Bash 版本，系统启动时间，最后上线时间，最后下线时间，Agent 安装时间，Audit 状态，资产更新时间。



发现 125 台主机断开超过 7 天，如不再使用，建议删除 Agent，以释放 License 资源，点击 [一键删除](#)

对于主机离线超过 7 天的主机，提供删除功能，释放 License 资源。

一键删除 1 台长期离线 Agent?

该操作将对产品中该主机的功能数据进行彻底删除，删除成功后数据无法找回，并释放 License 可供其它 Agent 使用。

[取消](#) [选择删除](#) [删除](#)

离线主机列表

业务组: 全部 [▼](#) 离线时长: 全部 [▼](#)

<input type="checkbox"/>	主机 IP	主机名	最后下线时间	离线时长	业务组
<input type="checkbox"/>	192.168.133.129	bogon	2018-10-12 17:03:26	23天	离线机器

已选 0/1 项 [清除已选项](#)

[取消](#) [确定](#)

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）。

设置状态

运行级别

启用 降级 停用

[取消](#) [确定](#)

2) 下载日志

下载日志

起始时间

2018-04-02 18:50:48 [□](#)

终止时间

2018-04-03 18:50:48 [□](#)

[取消](#) [确定](#)

9) 下载运行报告

下载 Agent 运行情况的报告。

4) 重启 Agent

重新启动 Agent，不改变原"主机状态"和"运行级别"。

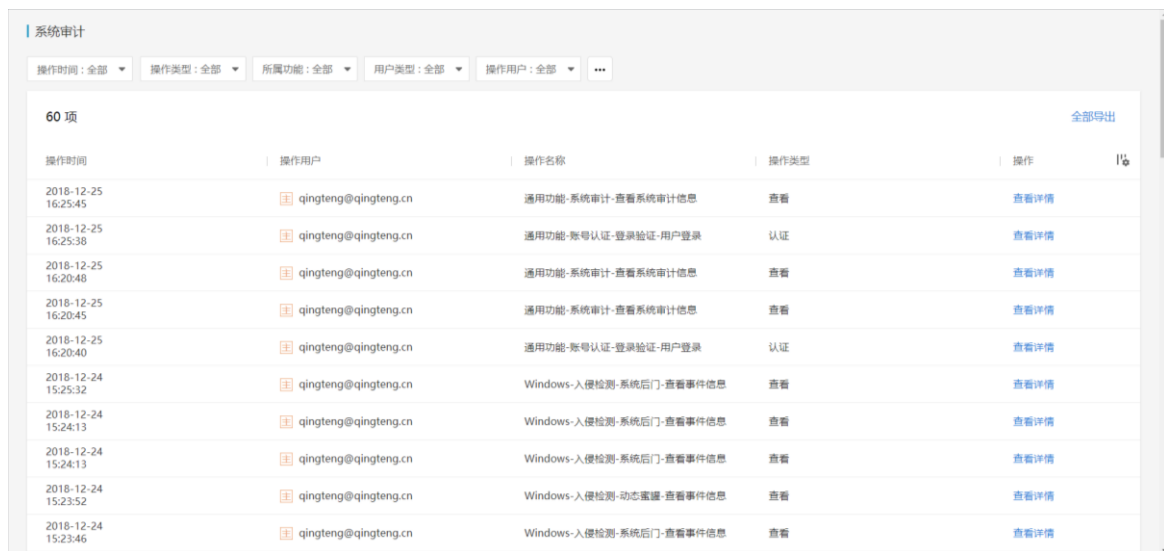
5) 删除 Agent

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"。

5.6 系统审计

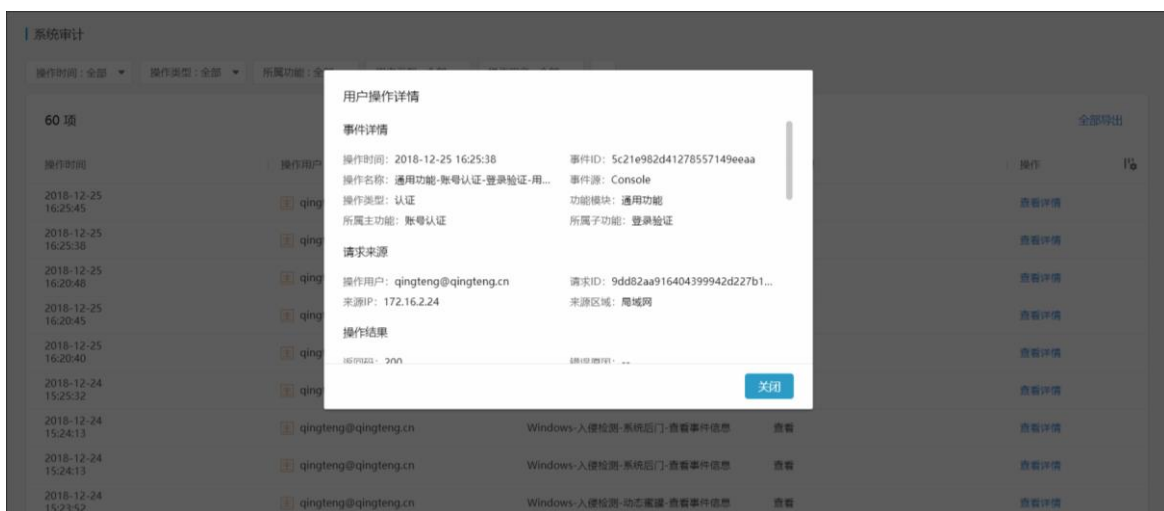
系统审计用于记录用户在使用本产品时产生的操作，用户可在系统审计功能中查看自己历史的操作详情，方便快速地追溯失败操作和误操作的原因。

审计列表主界面：



操作时间	操作用户	操作名称	操作类型	操作
2018-12-25 16:25:45	qingteng@qingteng.cn	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:25:38	qingteng@qingteng.cn	通用功能-账号认证-登录验证-用户登录	认证	查看详情
2018-12-25 16:20:48	qingteng@qingteng.cn	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:20:45	qingteng@qingteng.cn	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:20:40	qingteng@qingteng.cn	通用功能-账号认证-登录验证-用户登录	认证	查看详情
2018-12-24 15:25:32	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:24:13	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:24:13	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:23:52	qingteng@qingteng.cn	Windows-入侵检测-动态蜜罐-查看事件信息	查看	查看详情
2018-12-24 15:23:46	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情

点击查看详情：



操作时间	操作用户	操作名称	操作类型	操作
2018-12-25 16:25:45	qing	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:25:38	qing	通用功能-账号认证-登录验证-用户登录	认证	查看详情
2018-12-25 16:20:48	qing	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:20:45	qing	通用功能-系统审计-查看系统审计信息	查看	查看详情
2018-12-25 16:20:40	qing	通用功能-账号认证-登录验证-用户登录	认证	查看详情
2018-12-24 15:25:32	qing	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:24:13	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:24:13	qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看详情
2018-12-24 15:23:52	qingteng@qingteng.cn	Windows-入侵检测-动态蜜罐-查看事件信息	查看	查看详情

用户操作详情

事件详情

操作时间: 2018-12-25 16:25:38 事件ID: 5c21e982d41278557149eeaa

操作名称: 通用功能-账号认证-登录验证-用... 事件源: Console

操作类型: 认证 功能模块: 通用功能

所属主功能: 账号认证 所属子功能: 登录验证

请求来源

操作用户: qingteng@qingteng.cn 请求ID: 9dd82aa916404399942d227b1...

来源IP: 172.16.2.24 来源区域: 局域网

操作结果

返回码: 200 返回数据: ...

关闭



全部导出：单击“全部导出”按钮，导出当前范围内的全部操作记录。

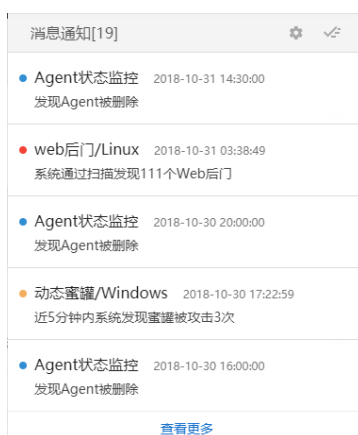
5.7 通知系统

通知系统即消息中心，为整个系统中各类消息汇聚的位置，其主要涉及以下三方面内容：

1. 解决安全系统的资产，风险，威胁功能的消息通知问题
2. 提供便捷的信息发布平台，可以使用该系统（或系统提供的发送能力）发送任何消息
3. 通知系统提供问题的通知，但不提供问题的处理

提供站内信，邮件，短信三种通知方式，可以由用户自行配置接收人。

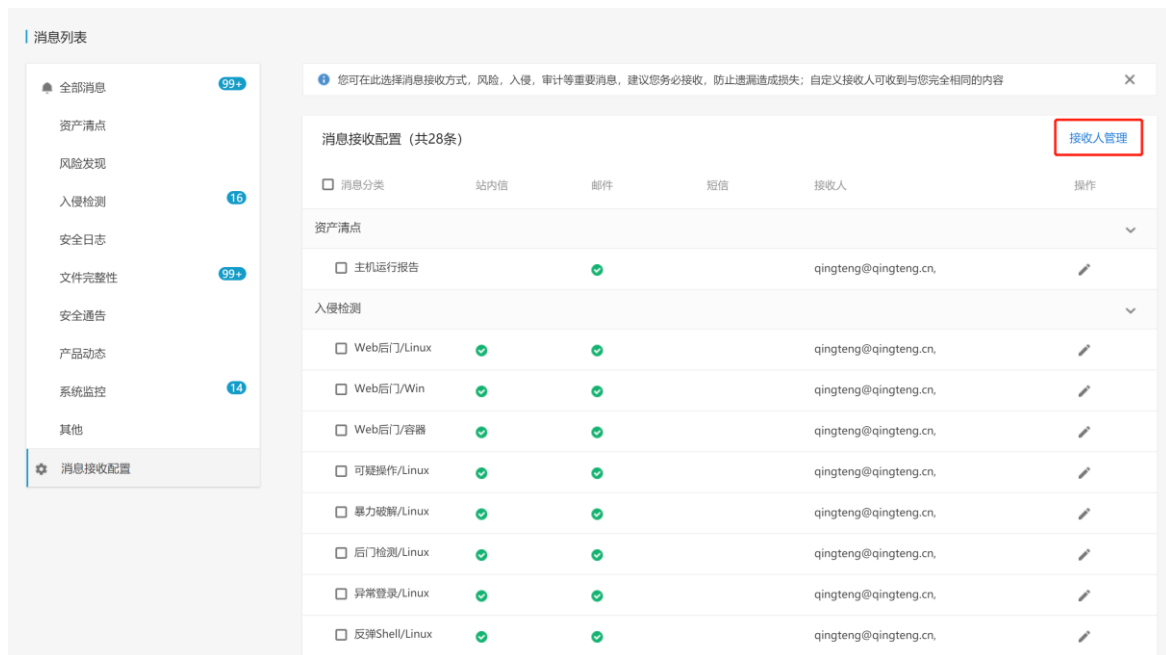
右上角按钮，选择设置按钮



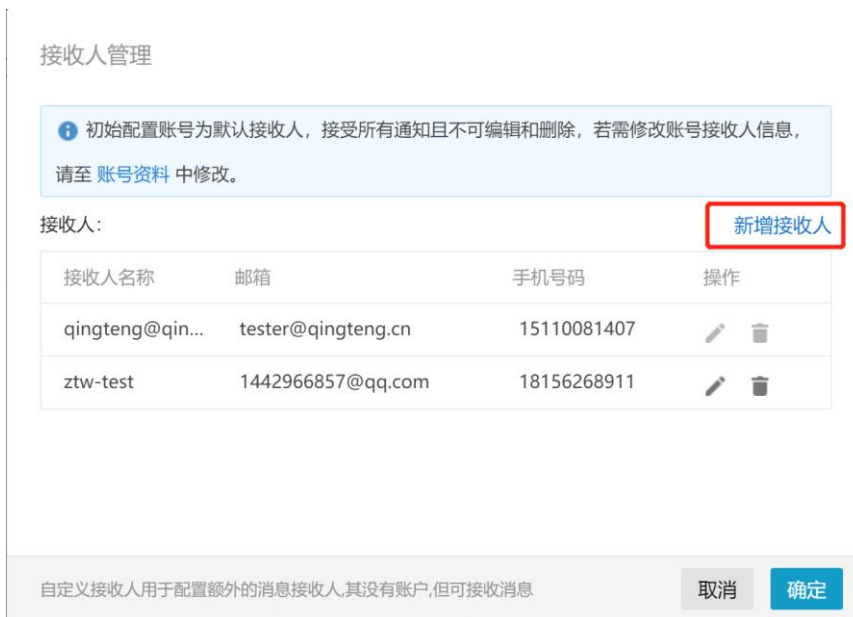
进入到通知系统，选择“消息接收配置”。



选择“接收人管理”



进入到接收人管理页面, 选择“新增加收入”, 输入要添加的接收人名称, 邮箱和手机号码 (非必填), 点击确定按钮。



可以根据需要对不同的事件配置不同的接收人, 或者选择事件发送消息的方式。

消息接收配置 (共28条)					接收人管理
<input type="checkbox"/> 消息分类	站内信	邮件	短信	接收人	操作
资产清点					
<input type="checkbox"/> 主机运行报告		✓		qingteng@qingteng.cn,	
入侵检测					
<input type="checkbox"/> Web后门/Linux	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> Web后门/Win	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> Web后门/容器	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> 可疑操作/Linux	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> 暴力破解/Linux	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> 后门检测/Linux	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> 异常登录/Linux	✓	✓		qingteng@qingteng.cn,	
<input type="checkbox"/> 反弹Shell/Linux	✓	✓		qingteng@qingteng.cn,	

修改配置

各项通知至少要配置一位接收人。

消息类型：

入侵检测 — 异常登录/Linux

接收方式：

站内信 邮件 短信

接收人：

[添加](#)

接收人名称	邮箱	手机号码	
qingteng@qing...	tester@qingteng.cn	15110081407	

取消

确定

支持批量配置各消息项的接收人，勾选需添加/移除接收人的消息项，选择对应的接收人后，点击“确定”即可完成批量配置。

您可在选择消息接收方式，风险，入侵，审计等重要消息，建议您务必接收，防止遗漏造成损失；自定义接收人可收到与您完全相同的内容

消息接收配置 (共28条) 添加接收人 移除接收人

消息分类	站内信	邮件	短信	接收人	操作
资产清点					
<input checked="" type="checkbox"/> 主机运行报告		<input checked="" type="checkbox"/>		qingteng@qingteng.cn,	
入侵检测					
<input checked="" type="checkbox"/> Web后门/Linux	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		qingteng@qingteng.cn,	
<input type="checkbox"/> Web后门/Win	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		qingteng@qingteng.cn,	

添加接收人

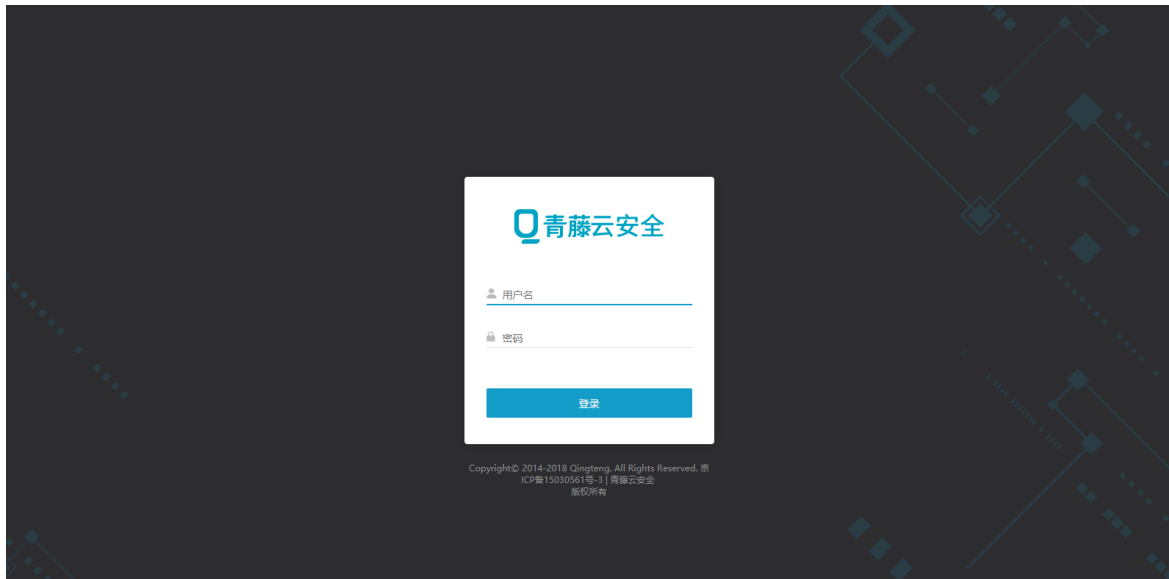
<input type="checkbox"/>	接收人	邮箱	手机号码
<input checked="" type="checkbox"/>	qingteng@qingteng.cn	tester@qingteng.cn	151100814...
<input type="checkbox"/>	ztw-test	1442966857@qq.com	181562689...


取消 确定

5.8 通用设置管理

5.8.1 账户登录

登录页面中，输入“用户名”和“密码”，即可登录到产品功能界面。



在头部的右上角，有点击 ，出现账户管理菜单，包含：账户资料、修改密码、下载记录、购买信息、关于青藤、退出登录。

点击“退出登录”，可退出当前用户，重新返回到产品登录页面。

-  账户资料
-  修改密码
-  下载记录
-  购买信息 ●
-  关于青藤
-  退出登录

5.8.2 账户信息管理

用户可以对自己账户的进行管理，了解账号基本信息，进行修改信息、修改登录密码等。

5.8.2.1 账号资料

账号资料

账号总览 基本信息 修改密码

账号总览

账号名称: fan.long@qingteng.cn

创建时间: 2017-01-10 16:30:41

LDAP认证: 未启用

所属用户组: 暂无所属用户组

账号角色:

账号角色	来源
超级管理员	账号

业务组: 未分组主机, 未分组主机, ucloud-win, centos, ubuntu, test, test1, 1, 阿里云-win, test-win, lu

上次登录时间: 2018-11-02 18:32:37

5.8.2.2 基本信息

账号资料

账号总览 基本信息 修改密码

基本信息

姓名 *
龙帆

邮箱 *
fan.long@qingteng.cn

手机号 *
18907155131

部门
请输入部门

职位
请输入职位

公司名称
龙帆

公司地址
请输入公司地址

备注
请输入公司备注

保存

5.8.2.3 修改密码

账号资料

账号总览 基本信息 修改密码

修改密码

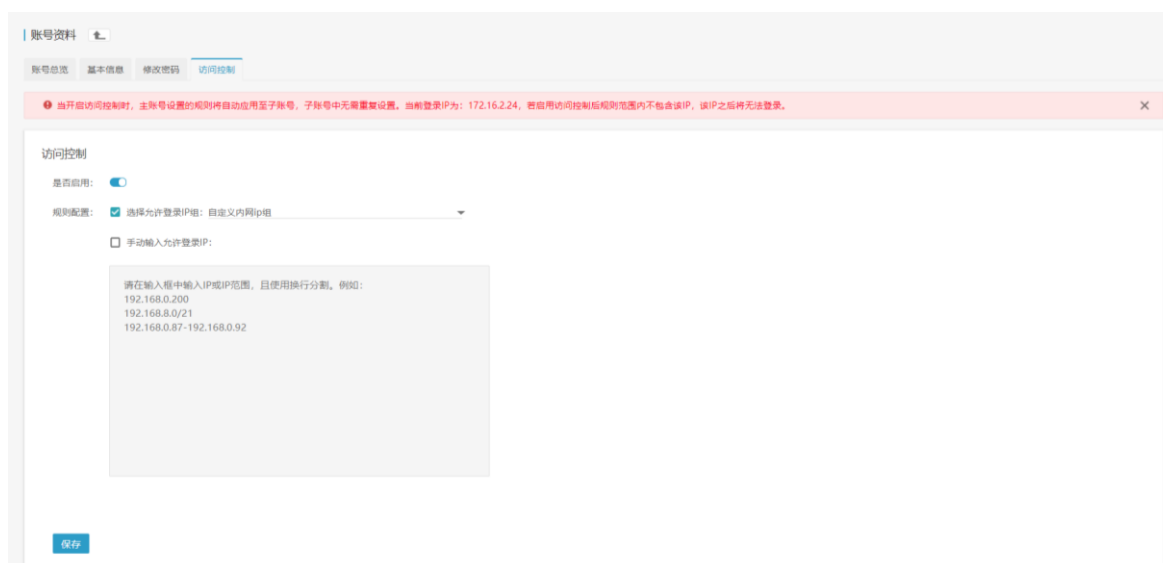
原密码 *
请输入原密码

新密码 *
请输入密码

确认新密码 *
请确认新密码

确定

5.8.2.4 访问控制

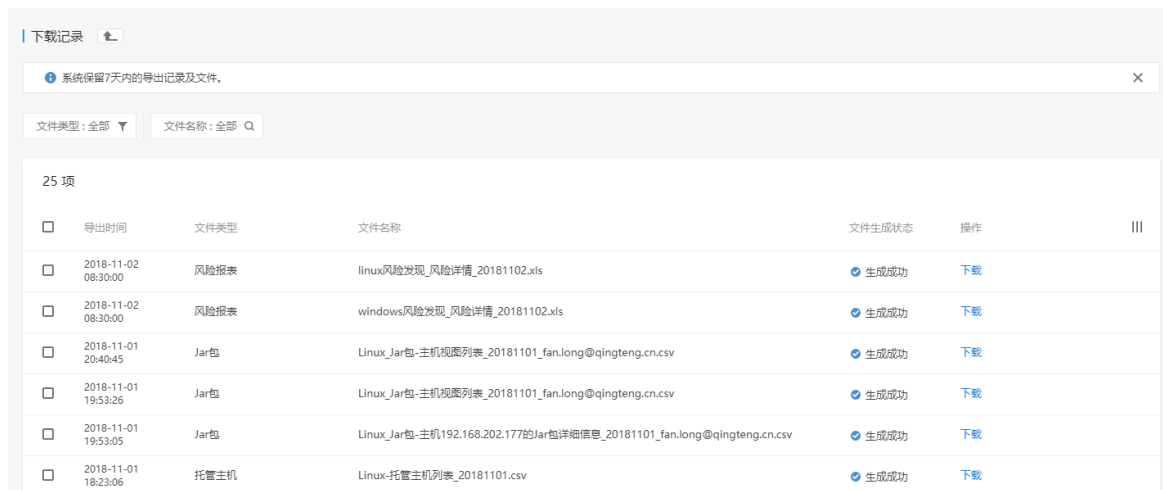


访问控制用于限制登录 IP，用户可设置该账号哪些主机 IP 可进行登录，可选择启用/禁用，未启用时不限制登录的 IP，设置完后需点击“保存”才能保存当前设置。

5.8.3 下载记录

系统会在“下载记录”中保留 7 天内，用户的导出记录及文件。

导出过程采取异步机制，保证要导出的文件可在后台自行生成，如用户离开功能界面，可在此处直接下载。



5.8.4 购买信息

在产品使用过程中，查看当前用户的服务购买信息及使用情况，包括：

- License 总量：购买的可同时在线的 Agent 总量（每个在线 Agent 会占用一个 License）；
- License 到期时间：购买的服务到期时间；
- Agent 在线数量：当前与服务连通的 Agent 数量；



5.8.5 关于青藤

我们的产品功能，会持续地进行“版本迭代”和“规则库更新”，此处展示产品的更新情况及版权相关信息。

×

QINGTENG

青藤云安全

版本 3.2.1

规则库更新：2018-06-14 19:28

© 2014-2018 青藤云安全
版权所有