

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	
1.1	核心功能	
1.2	网络架构图	7
二. 安全	首页	
三. Linux	<	
3.1	资产清点	
	3.1.1 主机资产	
	3.1.2 进程端口	
	3.1.3 系统账号	21
	3.1.4 硬件配置	
	3.1.5 软件应用	
	3.1.6 Web 服务	
	3.1.7 数据库	
	3.1.8 Web 站点	
	3.1.9 Web 应用	40
	3.1.10 Web 应用框架	
	3.1.11 安装包和类库	46
	3.1.12 其他	
3.2	风险发现	错误!未定义书签。
	3.2.1 风险总览	
	3.2.1 安全补丁	63
	3.2.2 漏洞检测	
	3.2.3 弱密码	75
	3.2.4 应用风险	
	3.2.5 系统风险	
	3.2.6 账号风险	
3.3	入侵检测	
	3.3.1 入侵总览	
	3.3.2 暴力破解	
	3.3.3 异常登录	
	3.3.4 反弹 Shell	
	3.3.5 本地提权	
	3.3.6 后门检测	
	3.3.7 Web 后门	
	3.3.8 可疑操作	
3.4	合规基线	
	3.4.1 基线检查	
	3.4.2 查看检查结果	
	3.4.3 新建检查	
	3.4.4 凭证管理	
	3.4.5 查看白名单	

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

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

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,能够在全球范围内轻易部署。 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



windows 首页



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。



speech-dispatch	10 011 55 11	数据库应用分布			Web服务应用分布		
	10.211.55.14	MySQL	18		Apache	23	
suy	172.31.9.203	Redis	9		Nginx	12	
YS		MemCache	4		IBoss 3		
	172.31.9.203	MongoDB	2		WebLogic 0		
unlinkd	172.18.0.1	Oracle 0			Websphere 0		
x-window-manage	192.168.197.101	HBase 0			Wildfly 0		
					Jetty 0		
Veb站点		•• Web应用			Web框架		
localhost	17	WordPress		7	spring		2
*	14	PHPCMS		4	freemarker		1
localhost.localdomain	5	Discuz! X		3	struts		1
	4	lenkins		2	struts2		1
- www.iavasec.cn 外	2	phpMvAdmin		2	velocity		1
www.gingtengdemoapach	e.com 2	Typecho		1			
siteA com	1	IBoss					
机资源消耗	毛统负载Top5	内存使用率分布	内存使用Top5		磁盘使用率分布	磁盘使用Top5	
	₽ 192,168,1,31		9 192,168,8-23	77.97%		₽ 172,31,9,203	77.25%
	□ 102 168 2 172 000		192 168 133 1	75.0205		192 168 247 127	70.00%
	- 132.100.2.172 0.0		Q 192.100.122.1	75.82%			70.83%
	및 1/2.22.208.151 0.0/	1核	L 192.168.124.133	75.28%		· ↓ 192.168.122.1	65.12%
高: 0 由: 0	☐ 192.168.201.148	4核 ■ 80%-100%: 0 ■ 50%-80%・20	9 192.168.80.130	74.53%	80%-100%: 0	192.168.78.131	64.26%
	10.31.91.192		🖵 192.168.192.165	70.83%	 20% 50% 36 	I92.168.200.130	60.06%

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;
- 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;
- 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。

概范视图 分班视图		数据更新于: 2018-10-18 06:30:01 统计更新于: 2018-10-18 06:30:03	更多 ~
▶ 主机资产	ř	◙ 进程第□	Ý
▲ 系统账号	~	✿ 硬件配置	×
88 软件应用	~	Ƴ Web服务	~
■ 数据库	~	Web%hefi	~
☑ Web应用	~	【〕 Web应用框架	~
■ 安装包和浅库	~		~

共有 12 个功能模块,分别为:

- 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;

概览视图 分级视图	数据更新于	☆ 2018-10-23 06:30:01 统计更新于: 2018-10-23 06:30:03 よう 展开 直找主机	更多 Y
🔓 主机资产	^	. 进程端口	~
✓ 托管主机 85台 在线	3台	✿ 硬件配置	~
商総 已停用	82台 0台	▶ Web服务	~
 > 操作系统 38个 > 业务组 15个 		🜒 Web站点	~
 > agent代理 3个 > bash攝件安装 2类 		[] Web应用框架	~
 > 主机标签 10种 > 資产等级 3级 		₩ 其他	~
 > 负责人 2位 > 机房位置 2处 			

点击展开 📲 标钮, 可以将全部模块的内容展开。

概范视图 分级视图	欺振更新于: 2018-10-23 06:30:01 統計更新于: 2018-10-23 06:30:03 <mark>x⁴ 收起 査技主机 更多 ∨</mark>
1. 主机资产 ^	◎ 进程端口 ^
 > 托警北県: 85台 > 通作系紙: 38个 > 当号祖: 15个 > agent代理: 3个 > bash通件交接: 2共 > 主印応志: 10种 > 進中等級: 13% 	金郎派行班程 470钟 全部派[1服券 412个 对外域[1服务 33个 roottO限运行进程 4532个 個平进程 19个 IO Walting进程 10个 非物实研进程 1060个
> 机焊位置 235	✿ 德件配置 ^
▲ 系統账号 ^	主切硬件和置 85台 > CPU 30种
全部系統課号 243钟 全部間P田 305钟 root既号 131个 sudo既号 108个	 > CPU協会 4种 > 硬盘大小 5映 > 硬盘使用車 5映 > 内容大小 5映

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。

🛃 主机资产	^
✔ 托管主机 85台	
在线	3台
离线	82台
已停用	0台

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

查找主机				
业务组:全部▼	主机状态:全部▼	主机IP: 全部 Q	主机名: 全部 Q	
内网IP: 全部 Q	外网IP: 全部 Q	连接IP: 全部 Q		
主机状态	主机IP	主机名	业务组	操作
● 在线	172.22.208.151	iz0xi0cq37i0f3ud	未分组主机	查看
 在线 	172.27.0.15	VM_0_15_centos	产品组/xiaotong	查看
 离线 	192.168.122.1	localhost.localdo	hao.yan	查看
 ・ ・ ・	10.31.91.192	sevck_linux	演示	查看
 离线 	192.168.197.50	localhost.localdo	sstest	查看
 离线 	192.168.197.245	localhost.localdo	未分组主机	查看
 ·	192.168.201.133	localhost.localdo	未分组主机	查看
 离线 	192.168.199.119	localhost.localdo	未分组主机	查看
				关闭

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"。

概览视图		数据更新于: 2018-10-23 06:30:01 统计更新于: 2018-10-23 06:30:03 🖉 展开	査找主机 更多 マ
🐍 主机资产	~	☞ 进程端口	更新统计更新数据
▲ 系统账号	~	• 硬件配置	~
器 软件应用	~	▶ Web服务	Ŷ
■ 数据库	~	📵 Web站点	~
▶ Web应用	~	[] Web应用框架	~
● 安装包和美库	~	₩ 其他	~

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。

┃运行进利			(视图 📃 🖵
进程分类	É: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 5	18 -	
477 項	σ		更新数据	全部导出
	进程名	进程分类	主机数	Ш
	titanagent	其它	79	
	titan_monitor	其它	78	
	dbus-daemon	其它	75	
	sshd	系统架构	71	
	rsyslogd	其它	71	
	dhclient	其它	70	
	bash	其它	66	

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。

托管主	「托智主机」€					
主机状	志:全部 ▼ 标签:全部 ▼	资产等级:全部 1	▼ 操作系统:全部 ▼ 更多 ▼	1		2 3
24 I	5					更新数据
	主印即	主机状态	主机名	主机标签	业务组	操作系统 ④ III
0	₽ 192.168.122.1	 在线 	bogon		centos	CentOS Linux release 7.5.1804 (Core),64-bit
	₽ 172.16.6.62	• 高线	bigdata-3-1.qingteng.cn	[)到试服务器则试测试	lu	CentOS release 6.9 (Final),64-bit
	192.168.30.157	 高线 	localhost.localdomain		未分组主机	CentOS Linux release 7.3.1611 (Core),64-bit
	₽ 192.168.202.133	• 高线	localhost.localdomain		未分组主机	CentOS release 6.5 (Final),64-bit
	₽ 192.168.202.183	• 高线	centos-6.3-I386		未分坦主机	CentOS release 6.3 (Final),32-bit
	♀ 192.168.202.130	● 离线	ubuntu		未分组主机	Ubuntu 16.04 LTS,64-bit
	9 192.168,202.159	 高线 	localhost.localdomain		未分组主机	CentOS release 5.4 (Final),64-bit
	♀ 192.168.202.132	• 高线	localhost.localdomain		未分组主机	CentOS release 6.5 (Final),64-bit

- ① 筛选/搜索区:根据不同票票,对列表内容进行筛选;
- ③ 全部导出按钮:点击 ,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;

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;

6	主机资产	^
>	托管主机 86台	
>	操作系统 38个	
>	业务组 15个	
>	agent代理 3个	
>	bash插件安装 2类	
>	主机标签 10种	
>	资产等级 3级	
>	负责人 3位	
>	机房位置 3处	

主机详细信息,如下:

┃ 托管主	「托管主机」を					
业务组	1:全部 ▼ Agent代理:全部	『▼ 标签:全	:部▼ 资产等级:全部▼	主机名:全部 Q 更多 ▼		
85 I	<u>5</u>					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	攝作系统 Ⅲ
	및 172.22.208.151	● 在线	iz0xi0cq37i0f3udnr94dlz	【Web】 数据库】 XXX1 【XXX2】 XXXX3 【XXXXD5	未分组主机	CentOS Linux release 7.3.1611 (Cor
	Q 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	 高线 	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	 高线 	localhost.localdomain		未分组主机	CentOS release 6.6 (Final),64-bit
	🖵 192.168.199.119	 高线 	localhost.localdomain		未分组主机	Red Hat Enterprise Linux Server rel
	🖵 192.168.199.151	 高线 	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;

v	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;

\sim	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;

\sim	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
	хохогб	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₽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 1			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	
titanagent	其它	78	
titan_monitor	其它	77	
dbus-daemon	其它	74	
dhclient		70	
sshd sshd	系统架构	70	
rsyslogd	其它	70	

进程 titanagent 详细信息	1
--------------------	---

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P:全部 Q 更多 ▼

79 Ij	<u>٦</u>							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 III
	Q 10.31.91.192	s	3.1.7-3.45.1-Rel	/titan/agent/tit	否	17867	root	1117738d88b2f268f84f3
	192.168.199.77	S	3.0.0a23-3.10.0	/titan/agent/tit	否	4847	root	095a86eedaf34a2c3a28e
	172.27.0.15	S	3.2.0-3.49.1-Rel	/titan/agent/tit	否	23128	root	99ff948cf3629222451faa
	☐ 172.31.4.28	S	3.0.0b4-3.14.0	/titan/agent/tit	否	26699	ec2-user	9b4f3372b062971d70f85
	□ 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 🗮 🛙	2
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 ▼ 主切UP:全部 Q 更多 ▼		
78 I	Ð		更新数据 全部导出	
	主机IP	进程数		I
	🖵 192.168.8.23	182		
	☐ 172.31.9.203	160		
	I92.168.197.101	148		
	□ 172.18.0.1	141		
	🖵 10.211.55.8	140		

主机19	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	5 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	ш
	gdm-session-wo	r	s	3.14.1-7	/usr/lib/gdm3/g	是	63331	root	
	gdm-session-wo	r	S	3.14.1-7	/usr/lib/gdm3/g	是	63237	root	
	gdm-session-wo	r	s	3.14.1-7	/usr/lib/gdm3/g	是	59738	root	
	ssh		s		/usr/local/bin/ssh	否	59737	root	
	gdm-session-wo	r	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 1	🖵 🧮 🛤
頭口访问性:全部 ▼ 业务组:全部 ▼	
412 项	更新数据 全部导出
□ · 第□号: 进程名	主切取 Ш
68:dhclient	70
22:sshd	69
631:cupsd	38
25:master	35
5353:avahi-daemon	27
80:httpd	21

68:dhclient详细信息 👠

端□访问性:全部 ▼	协议:全部 ▼	业务组:全部 ▼	主机IP:全部 Q	主机名:全部 Q	更多 🔻

73 I	页						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	111
	모 192.168.199.77	?	UDP	3600	root	2017-09-02 19:57:12	
	Q 172.27.0.15	?	UDP	1266	root	2018-09-28 18:30:26	
	및 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 🛍		视图 🗮 🖵
端□访问性:全部 ▼ 业务组:全部 ▼	主初い:全部 Q 主初い:全部 Q	
78 项		全部导出
□ 主机IP	第二次	Ш
□ □ 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	

19

主机1	主机192.168.197.101端口服务详细信息 €							
端口访	5问性:全部 ▼ 协议:全部	部▼ PID:全部 Q						
92 I	顷							全部导出
	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	ш
	22:sshd	?		TCP	15062	taibai	2017-08-22 02:29:40	
	22:sshd	?	0.0.0.0	TCP	15062	taibai	2017-08-22 02:29:40	
	53:named	内	192.168.197.101	TCP	15402	bind	2017-10-09 00:11:51	
	53:named	内	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 × 业务组:全部 ▼ 調口号:全部 Q 进程名:全部 Q		视图 📃 🖵
47 项		更新数据 全部导出
前口号: 进程名	主机数	ш
22:sshd	22	
80:httpd	4	
23:xinetd	3	
111:rpcbind	3	
9300:java	2	
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 1			视图 📃 🖵
进程分类:全部 ▼ root X 是君	5是包安装:全部 ▼ 主机数:全部 ▼ 进程名:全部 Q 更多	*	
367 项			更新数据 全部导出
□ 进程名	进程分类	主机数	ш
titanagent	其它	73	
titan_monitor	其它	72	
dhclient		66	
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。

僵尸与	● 第二日の Waiting进程 1. □ 近原原本:金師 Y 単行用中:金師 Y 二十月中:金師 Y 二 × 王和中:金師 Q 更多 ▼											
19 13	1930 1930										1	
	主机P	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	還行用户	进程启动时间	ш	
	□ 172.31.3.33	login	其它	z		/proc/13954/exe	百	13954	root	2017-08-23 12:44:53		
	♀ 172.31.0.27	login	**	z	**	/proc/14178/exe	晋	14178	root	2017-11-15 13:14:48		
	□ 172.31.6.36	login	其它	Z		/proc/9779/exe	香	9779	root	2017-08-31 13:35:13		
	□ 172.31.11.104	login	877-0	z	175.1	/proc/12121/exe	T	12121	root	2017-11-30 04:43:27		
	₽ 172.31.0.27	login	**	Z		/proc/14230/exe	首	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	27.2	z		/proc/19435/exe	晋	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 Waitin	g进程。
---------------------------------	------

【僵尸与	印与IO Waiting进程 t_										
进程版	本:全部 ▼ 是否是包安装:全部	◎ ▼ 运行用户:全	≣ ▼ D×	主机IP:全部 Q	主机名:全部 Q 更	\$ -					
10 琐	Ĩ										Е
	主机P	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	Ш
	□ 172.31.4.28	in.teinetd		D		/proc/1389/exe	КU	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	112	D	94 C	/proc/7618/exe	西	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 1			税图 🗮 🖵
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 Q		
210 项			更新数据 全部导出
□ 进程名	进程分类	主机数	ш
L titanagent	其它	π	
titan_monitor	其它	76	
vmtoolsd	-	30	
vmware-vmblock-	其它	23	
UGAuthService	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

●援	۰.									(12) 📰 🖵
账号材	志:全部 ▼	root权限:全部 平	登录方式:全部 ▼	sudo权限:全部 ▼	账号名:全部 Q	更多 🔻				
243	项								更新数据	全部导出
	账号名						主机数			
	root						78			
	lp						78			
	mail						78			
	daemon						77			
	games						77			
	bin						77			

账号re	账号root详细信息 1											
最后登	读时间:全部 ▼ 账号状态:全部	節▼ root权限::	全部 🔻 登录方式:	:全部 🝸 GID : :	全部 Q UID:全部	5 Q 更多 🔻						
78 1	78 项											
	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	
	Q 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	
			-		_				10.44			

主机视角

┃主机则	K₩ L					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	页					全部导出
	主机IP	账号数			最后登录	ш
	192.168.122.1	67			qingteng 2017-11-13 16:53:35 :0 pts/0	
	192.168.192.165	65			root 2018-08-03 23:48:20 192.168.198.111 pts/28	
	🖵 192.168.197.101	64			root 2017-11-18 02:45:15 192.168.197.89 pts/14	
	□ 192.168.8.23	62			root 2017-11-09 18:21:06 :0 pts/2	
	및 192.168.100.162	61			root 2017-10-27 11:32:56 192.168.197.25 pts/2	
	🖵 10.211.55.8	56			root 2018-08-29 21:57:25 :0 pts/3	
	₽ 192.168.122.1	49			root 2017-09-14 15:28:16 192.168.201.1 pts/3	
	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 🗈

最后到	録时间: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 I	Ð									全部导出
0	账号名	UID	GID	账号状态	root权限	登录方式	Home目录	shell	操作	
	userlock	0	1004	◎ 禁用	是	不可登录	/home/userl	/bin/bash	查看详情	
	root	0	0	⊘ 启用	是	只允许密码登录	/root	/bin/bash	查看详情	
	qingteng	0	0	⊘ 启用	是	只允许密码登录	/home/qingt	/bin/bash	查看详情	
	weakuser1	0	1008	⊘ 启用	是	只允许密码登录	/home/weak	/bin/bash	查看详情	
	bin	1	1	● 禁用	否	不可登录	/bin	/sbin/nologin	查看详情	
	daemon	2	2	● 禁用	否	不可登录	/sbin	/sbin/nologin	查看详情	
	adm	3	4	ᇢ 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 ▲ 业务组:全部 ▼ 用户组:全部 		视图 📃 🖵
305 项		更新数据
□ 用户组	主机数	ш
audio	78	
disk	78	
utmp	78	
tty	78	
🗆 lp	78	
daemon	78	

用户组audio详细信息 🚺	用户组audio详细信息 1									
业务组:全部 ▼ GID:全部 Q	主机IP:全部 Q 主机名:全部 Q									
78 项			:							
ロ 主机 P	GID	包含账号	Ш							
□ 모 172.27.0.15	63									
10.31.91.192	63									
192.168.199.77	63	gdm								
□ 및 192.168.248.141	63									
□ □ 192.168.197.102	29	pulse, speech-dispatcher								

3.1.3.3 Root 账号

账号	t							视图 📃 🖵
账号状	态:全部 ▼	Root权限 🗙	登录方式:全部 ▼	sudo权限:全部 ▼	更多 ▼			
34 IJ	页					1	更新数据	全部导出
	账号名				主机数			Ш
	root				78			
	qt				4			
	test				4			
	userroot				4			
	usersudo				4			
	ec2-user				3			
	zhiwei				2			

3.1.3.4 sudo 账号

账号					100 📃 🖂
账号状态:全部 🔻	root权限:全部 🔻	登录方式:全部 ▼	Sudo权限 🗙	更多 🔻	
24 项					更新数据 全部导出
□ 账号名				主机数	ш
🗆 root				74	
🗆 qt				4	
userroot				4	
usersudo usersudo				4	
D zhiwei				2	
user user				2	

3.1.3.5 交互登录账号

登援 ポ号状	▲	root权限:全部 ▼	登录方式:全部 ▼	sudo权限:全部 ▼	账号名:全部 Q	更多 ▼			视图 📃 🖵
可交互	i登录 ×								
65 I	页							更新数据	全部导出
	账号名				主机数				Ш
	root				47				
	test				14				
	qt				7				
	weblogic				6				
	admin				5				
	taibai				5				
	user				5				
	weakuser1				4				
	ec2-user				4				

3.1.3.6 启用账号

┃账号	E						视图 📃 🖵
启用	× root权限:全部 ▼	登录方式:全部 ▼	sudo权限:全部 ▼	账号名:全部 Q	更多 🔻		
87 I	页					更新数据	全部导出
	账号名				主机数		ш
	root				77		
	test				19		
	admin				8		
	qt				7		
	weblogic				6		
	taibai				6		
	user				6		
	guest				6		
	usersudo				5		

3.1.3.7 过期账号

过期与	过期与密码锁定账号 1									
密码修	啟时间: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IF	:全部 Q 更多 🛪				
已过期	E过期 X									
2 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	111
	□ 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	
	🖵 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 1									
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: 金	全部 ▼ 主机IP	:全部 Q 更多 ·	-			
已锁定 🗙									
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	Ш
□ □ 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	
□	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		ш				
ort-forw lu.shen		RSA1	6						
AAAAB3NzD+4RKbAZ	taibaiyifeng@outlook.com	ssh-rsa	4						
AAAAB3Nzmf8LWw==	guanpeng@qt	ssh-rsa	3						
AAAAB3NzsqLBOw==	ms@qt	ssh-rsa	3						
AAAAB3NzBedGGQ==	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;

۵	硬件配置	^
	主机硬件配置 85台	
>	CPU 30种	
>	CPU核心 4种	
>	硬盘大小 5类	
>	硬盘使用率 5类	
>	内存大小 5类	
>	内存使用率 5类	
>	系统负载 4类	

硬件详细信息,如下:

● 硬件配置 内存大小:	硬件配置 1 内存大小:全部▼ 硬盘大小:全部▼ 内存使用率: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	ш	
	₽ 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;

\sim	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

v	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
	硬盘大小 5类 0-40GB 40GB-100GB 100GB-1TB 1TB以上 0或未知

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

\sim	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	
	育同	0台
	中	0台
	低	33台
	定	53台

3.1.5 软件应用

分级视图中,软件应用模块清点了所有安装 Agent 的主机上运行着的应用。

器 软件应用	^
✓ 全部软件应用 49种	
SSH	70个
pickup	33个
rsyslog	31个
Apache	23个
ModemManager	21个
Python	20个
MySQL	18个
xinetd	17个
Sendmail	16个
Nginx	15个

目前支持的应用类型,如下表:

azip	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 L			视图 📃 🖵
应用类	別:全部 ▼ 业务组:全部 ▼ 应用名:全部 Q			
49 IJ	Σ.			更新数据 全部导出
	应用名	应用类别	主机数	
	SSH	系统架构	70	
	pickup	其它	33	
	rsyslog	系统应用	31	
	Apache	Web运维	23	
	ModemManager	其它	21	
	Python	其它	20	
	MySQL	数据库	18	
	xinetd	其它	17	
	Sendmail	系统应用	16	

应用SSH详细信息 1

版本号	:全部 ▼ 业务组:全部 ▼	二进制路径:全部 Q	配置文件路径:全部	◎ Q 更多 ▼				
75 1							全	部导出
	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	I
	— 10.10.10.13	SSH	5.3p1	root	/usr/sbin/sshd	/etc/ssh/sshd	1	
	□ 10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd		1	
	및 10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd	/etc/ssh/sshd	1	
	10.10.10.24	SSH	5.3p1	root	/usr/sbin/sshd		1	

root

主机视角

10.31.91.192

SSH

5.3p1

主机软件应用 👠		视图 🗮 🖵
应用类别:全部 ▼ 业务组:全部 ▼	应用名:全部 Q	
78 项	更新	数据 全部导出
□ 主机IP	应用数	ш
□ □ 192.168.192.165	26	
□ □ 192.168.197.101	21	
□ □ 192.168.78.131	13	
□ 모 10.31.91.192	12	
□ 및 172.31.11.104	12	

/usr/sbin/sshd

/etc/ssh/sshd_... 1

Ш

主机192.168.192.165 应用详细信息								
26 项								全部导出
	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	Ш
	rsyslog	系统应用	7.4.4-1ubuntu2.6	syslog	/usr/sbin/rsyslogd		1	
	Bluetoothd	其它	4.101-0ubuntu1	root	/usr/sbin/blueto		1	
	Bind	系统应用	1:9.9.5.dfsg-3ub	bind	/usr/sbin/named		1	
	Memcache	数据库	1.4.14-0ubuntu9.1	memcache	/usr/bin/memca		1	
	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:

 $\label{eq:approx_star} Apache \ \ Nginx \ \ Tomcat \ \ Weblogic \ \ JBoss \ \ Wildfly \ \ Jetty \ \ WebSphere \ .$

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 #	投务 11 勝名:全部 ▼ 版本:全部 ▼	启动用户:全部 🎙	2 业务组:全部 ▼	7 更多 ▼				视图 📃 🖵
40 项	ą						更新数据	全部导出
	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	Ш
	🖵 10.31.91.192	Apache	2.2.15	apache	/usr/sbin/httpd	/etc/httpd/co	21	
	및 10.211.55.8	Apache	2.4.6	apache	/usr/sbin/httpd	/etc/httpd/co	8	
	□ 172.16.6.142	Tomcat	8.0.24	root	/usr/local/jav	/usr/local/to	1	
	□ 172.16.6.142	Nginx	1.10.2	root	/usr/sbin/nginx	/etc/nginx/ng	11	
	□ 172.17.43.79	Nginx	1.10.3	nginx	/usr/local/ngi	/usr/local/ngi	2	
	□ 172.18.0.2	Nginx	1.10.2	nginx	/usr/sbin/nginx	/etc/nginx/ng	2	
	및 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P:全部 Q 主机名:全部 Q	
33 项		全部导出
□ 主机IP	Web服务数	Ш
□ □ 192.168.192.165	3	
□ □ 172.16.6.142	2	
□ 및 172.31.0.27	2	
□ 및 192.168.197.101	2	

主机10.31.91.192上httpd服务关联的进程									
运行用户	9:全部 ▼ 进程启动时间:全部	▼ 进程版本:全部 ▼ PID:台	全部 Q 更多 ▼						
21 项					:				
	PID	进程路径	运行用户	进程启动时间	ш				
	356	/usr/sbin/httpd	apache	2018-08-03 08:05:55					
	1768	/usr/sbin/httpd	apache	2018-08-09 09:29:12					
	6577	/usr/sbin/httpd	apache	2018-08-08 07:53:58					
	6586	/usr/sbin/httpd	apache	2018-08-08 07:53:59					
	6587	/usr/sbin/httpd	apache	2018-08-08 07:53:59					

3.1.6.2 Apcache

~	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 × 版本:全部 ▼	启动用户:全部 🔻 💵	务组:全部 ▼ 3	更多 🔻				
23 项						更新数据	全部导出
□ 主机』P	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	ш
□ □ 10.31.91.192	Apache	2.2.15	apache	/usr/sbin/httpd	/etc/httpd/con	21	
□ □ 172.22.208.151	Apache	2.4.6	root	/usr/sbin/httpd	/etc/httpd/con	9	
□ □ 172.27.0.15	Apache	2.4.6	apache	/usr/sbin/httpd		11	
□ □ 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 🎚	路 1							视图 📃 🖵
Nginx	★ 版本:全部 ▼	启动用户:全部 ▼ 业务:	组:全部 ▼ 更多 ▼					
11 项	Į						更新数据	全部导出
	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	Ш
	□ 172.16.6.142	Nginx	1.10.2	root	/usr/sbin/nginx	/etc/nginx/ngin	11	
	172.17.43.79	Nginx	1.10.3	nginx	/usr/local/ngin	/usr/local/ngin	2	
	₽ 172.18.0.2	Nginx	1.10.2	nginx	/usr/sbin/nginx	/etc/nginx/ngin	2	
	및 172.27.0.15	Nginx	1.12.2	nginx	/usr/sbin/nginx	/etc/nginx/ngin	2	
	🖵 172.31.11.176	Nginx	1.12.1	nginx	/usr/sbin/nginx	/etc/nginx/ngin	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 ∦	股务 ▲							视图 📃 🖵
Tomca	t × 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
	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	Ш
	□ 172.16.6.142	Tomcat	8.0.24	root	/usr/local/java/j	/usr/local/tomc	1	
	I92.168.182.128	Tomcat					0	
	□ 192.168.192.165	Tomcat	5.5.36	root	/usr/lib/jvm/jdk	/root/apache-t	1	
	□ □	Tomcat	8.0.46	root	/usr/java/jdk1.8	/usr/local/tomc	1	
	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 肌	磅 🕇							视图 📃 🖵
JBoss	× 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
	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	Ш
	₽ 172.31.0.27	JBoss					0	
	₽ 172.31.9.203	JBoss	4.2.3.GA	root	/usr/lib/jvm/jav		1	
	□ 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	9						
同上;								
3.1.6.	10 IHS							
	~	IHS I 1种						
		8.5.5.16				1个		
Web 服	务 1							视图 📃 🖵
ihs 🗙	8.5.5.16 🗙 启动用户:	全部 ▼ 业务组:全部 ▼	配置文件路径:全部(2 更多 ▼				
1 项							更新数据	全部导出
	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	Ш
	• 192.168.16.165	IHS	8.5.5.16	root	/opt/IBM/HTTPServ	/opt/IBM/HTTPServ	4	

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。

-	:数据库	^
	全部政调库 35个	
>	MongoDB 2种	
>	postgres 2种	
>	Redis 3种	
>	MySQL 13种	
>	MemCache 3种	

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	1.										628	
政策市	名:全部 🔻	版本:全部 🔻	這行用户:全部 ▼	調口访问性:全部 ▼	配置文件路径:全部 Q	日志文件路径:全部 Q	更多 🔻					
35 IJ	۶										更新数据	1
	主机P		数据库名	版本	当听馈□	运行用户		配置文件路径	日志文件路径	操作		BI.
	♀ 192.168	1.248.145	mysql		3306	mysql		/etc/my.cnf		查查详情		
	및 192.168	1.248.145	mysql		3306	mysql		/etc/my.cnf		查看详情		
	₽ 192.168	1.247.137	mysql	5.1.73	3306	mysql		/etc/my.cnf		查看详情		
	₽ 192.168	1.247.134	mysql	5.1.73	3306	mysql		/etc/my.cnf		查查详情		
	₽ 192.168	I.201.133	memcache	1.4.13	11211	root				查費详情		
	♀ 192.168	1.197.101	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 1		视图 🗮 🖵
运行用户:全部 ▼ 业务组:全部 、	▼ 主机iρ:全部 Q 主机名:全部 Q	
26 项		:
主机IP	2014年1月25日 2014年1月11日 2014年1月11日 2014年1月11日 2014 2014 2014 2014 2014 2014 2014 2014	ш
I 192.168.197.101	5	
□ □ 192.168.192.165	5	
□ □ 192.168.8.23	3	
I 10.31.91.192	2	

| 主机192.168.197.101数据库详细信息 1

数据库	名:全部 ▼ 版本:全部	3 ▼ 运行用户:全部 ▼	配置文件路径:全部(Q 日志文件路径:全部 C	● 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	Ш
	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

\sim	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 🗸									
MySQ	L数据库 1								视图	
------	-----------------	-----------	----------	-----------	-------	-------------	-----------------	------	------	---
端口访问	问性:全部 ▼ 版本:全部 ▼	运行用户:全部 🔻	业务组:全部 🔻	主机ip:全部 Q	更多 🔻					
18 项	Ę								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		ш
	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 1								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 Q	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	撮作		ш
	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		
	I72.31.11.104	redis	2.8.3	6379	root			查看详情		

3.1.7.4 MongoDB

1个
1个

調口切問性:金部 ▼ 販店:金部 ▼ 販売用:金部 ▼ 販売預放REST接口:金部 ▼ 主机容:金部 Q 更多 2 项	Mong	oDB数据库 1											视图 🗄	
2.项 □ 主印	第口访	同性:全部 ▼ 版本:全部 ▼	运行用户:全部 🎙	是否开放RES	「接口:全部 ▼	主机ip:全部 Q	主机名:全部 Q 更多	w.						
	2 16												西島がありた	
□ 主机/P 数据库英型 版本 监听阑口 运行用户 配置文件器 目志文件器 是高升放(Meb级 安全认证 操作 Ⅲ	2 44												2011203	
		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援 口	安全认证	操作		Ш
□ □ 192.168.197.101 mongod 3.0.15 27017 mongodb /etc/mongod /var/log/mon false false disabled 查書評情		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 查面對情		Q 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

Mem 端口说	Cache数据库 1_ 问性:全部 Y 版本:全部 Y	运行用户:全部 🔻	业务组:全部 ▼ 主	机ip:全部 Q 更多 ▼				视图	=
4 项	Į							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		ш
	192.168.201.133	memcache	1.4.13	11211	root		查看详情		
	I92.168.197.101	memcache	1.4.14-0ubuntu9.1	11211	memcache		查看详情		
	I92.168.192.165	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	
1.1-2ubuntu2	2	5个
8.4.20		1个

postgr	res数据库 1									视图 :	Q
蒴囗访	问性:全部 ¥版本:全部 ¥	运行用户:全部 🔻	业务组:全部 ▼	主机ip:全部 Q	主机名:全部 Q	更多 🔻					
6项										更新数据	+
	主机P	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		Ш
	🖵 192.168.197.101	postgres	1.1-2ubuntu2	15432	postgres-xc		/		查看详情		
	9192.168.197.101	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		
	<pre>I92.168.192.165</pre>	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。



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 1			视图	≣ 🖵
服务类型:全部 ▼ 第口访问性: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
	站而初期	站点数		ш
localhost	Welcome to nginxi	15		
□ ·		14		
localhost.localdomain	400 Bad Request	5		
•	Apache2 Ubuntu Default Page: It works	4		
www.javasec.cn	400 Bad Request	2		
www.qingtengdemoapache.com	Apache HTTP Server Test Page powered by CentOS	2		
www.manli.info	Index of /	1		
siteA.com	502 Bad Gateway	1		

│ localhost域名站点详细信息											
服务类	服务类型:全部 ▼ 第口访问性:全部 ▼ 运行用户:全部 ▼ 所有者权限:全部 ▼ 第口:全部 Q 更多 ▼										
16 I	Φ										全部导出
	主机IP	服务类型	站点满口	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	Ш
	192.168.247.137	Tomcat	8080	未知	HTTP	root	/usr/local/to	root	rwxr-xr-x	查看详情	
	192.168.219.131	Nginx	8888	未知	HTTP	nginx				查看详情	
	192.168.201.133	Tomcat	8080	未知	HTTP	root	/usr/local/to	root	rwxr-xr-x	查看详情	
	192.168.197.245	Nginx	80	未知	HTTP	www				查看详情	
	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
	域名	站点标题	站点数	Ш
	www.javasec.cn	400 Bad Request	2	
	*		2	
	www.example.com	Apache HTTP Server Test Page powered by	1	
	www.qingtengdemoapache.com	Apache HTTP Server Test Page powered by	1	
	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‡					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 項	Φ		I	更新数据	全部导出
	域名	站点标题	站点数		ш
	localhost	Apache Tomcat/8.5.8	7		
0	localhost *	Apache Tomcat/8.5.8	7 2		

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 1			视图 📃 🖵
服务类型:全部 ▼ 端口访问性:全部 ▼ 运行	用户:全部 ▼ rwxrwxrwx X 更多 ▼		
1 项		更新数据	全部导出
□ 域名	站点标题	站点数	ш
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 <u>术</u>			视图	
服务类	型:全部 🔻 业务组:全部 🔻 应用名:全部 Q			
8项			更新数据	:
	应用名	主机数 ↓		ш
	WordPress	7		
	PHPCMS	4		
	Discuz! X	3		

WordF	Press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 Q	更多 🔻				
9 项								:
0	主机IP	版本	服务类型	站点域名	根目录	虚拟路径	插件数	ш
	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/ngin	/usr/share/ngin	2	

主机视角

┃ 主机Web应用统计 🚹						视图 🔝 🖵
服务类型:全部 ▼ 业务组:全	a部 ▼ 主机IP:全部 Q 更多	õ v				
13 项						:
□ 主机IP	应用数					ш
10.31.91.192	2					
□ □ 172.16.6.142	3					
□ □ 192.168.2.135	1					
主机172.16.6.142的Web应用详细值	息 1					
服务类型:全部 ▼ 版本号:全部 ▼	应用名:全部 Q 站点域名:全部	Q 更多 ▼				
3 项						:
□ 应用名 版本	服务类型	站点域名	根目录	虚拟路径	插件数	Ш
WordPress 4.5.2	2 Nginx	www.centos.baid	/root/data/www/	/root/data/www/	2	
WordPress 4.7	Nginx	admin.php.com	/root/data/www/	/root/data/www/	2	
WordPress 4.4.6	5 Nginx	local.admin.com	/root/data/www/l	/root/data/www/l	2	

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、Codelgniter、BEdita、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 <u>成</u>	用框架统计				视图 📃 🖵
框架语	吉:全部 ▼ 业务组:全部 ▼ 框架名:全部 Q				
26 Ij	Į.			更新数据	全部导出
	框架名	框架语言	主机数		Ш
	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	ŧ.
----------------	----

服务类型:全部 ▼ 业务组:全部 ▼	7 版本:全部 Q 主机IP:全部 Q 主机	名:全部 Q 更多 ▼		
1 项				全部导出
□ 主机IP	框架版本	服务类型	应用路径	ш
• 192.168.220.133	1.2.44	JBoss		

主机视角

│ 主机Web应用框架统计		视图 🗮 🕻
业务组:全部 ▼ 主机IP:全部 Q	主机名:金部 Q	
3 项		全部导出
□ 主机P	框架数	
• 192.168.220.133	23	
• 192.168.220.137	4	
• 192.168.220.128	2	

主机19 框架语	主机192.168.220.133的Web应用框架详细信息 種架语言:全部 ▼						
23 项	۵				全部导出		
	框架名	框架语言	框架版本	应用路径	Ш		
	spring	java	2.5.6.SEC03,3.0.5.RELEASE,4.3.2.RELEASE,				
	Freemarker	java	2.3.13,2.3.26,2.3.19				
	hibernate	java	3.3.1.GA,5.3.7.Final,3.6.6.Final				
	turbine	java	2.3.1				
	struts	java	1.3.10				
	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 🛍		视图	1 📃 🖵
业务组:全部 Y 框架名:全部 Q			
23 项		更新数据 全	部导出
	主机数		Ш
Freemarker	1		
vertx	1		
stripes	1		
i jackson	1		
webwork	1		

Freemarker框架详细信息 🚹

服务类型:全部 ▼ 业务组:全部 ▼	版本:全部 Q 主机P:全部 Q 主机名	:全部 Q		
1 项				全部导出
□ 主机IP	框架版本	服务类型	关联jar包数	111
• 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 ▼ 脱	版本:全部 Q 主机IP:全部 Q	主机名:全部 Q		
1项	框架Jar包信息			全部导出
□ 主机IP 框	包名	绝对路径	关联jar包数	
• 192.168.220.133 2.	freemarker-2.3.13.jar	/root/jboss-6.1.0.Final/server/default/tmp	4	
	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		
	_	筑		

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	
3 项		全部导出
□ 主机IP	框架数	ш
• 192.168.220.130	23	
• 192.168.220.133	23	
• 192.168.220.137	1	

主机19	92.168.220.133的Java语言框架详细信息	Ł			
服务类	型:全部 🔻 版本:全部 Q 框架名:全	部 Q			
23 项 全部导出					
	框架名	框架版本	服务类型	关联jar包数	Ш
	spring	2.5.6.SEC03,3.0.5.RELEASE,4.3.2.RELEASE,	JBoss	4	
	Freemarker	2.3.13,2.3.26,2.3.19	JBoss	4	
	hibernate	3.3.1.GA,5.3.7.Final,3.6.6.Final	JBoss	4	
	turbine	2.3.1	JBoss	1	
	struts	1.3.10	JBoss	1	

主机19	2.168.220.133的Java语言框架详细	暗息 1			
服务类型	型:全部 ▼ 版本:全部 Q 相	架名:全部 Q			
23 项		框架Jar包信息			全部导出
		包名	绝对路径	关联jar包数	
	spring	spring-core-2.5.6.SEC03.jar	/root/jboss-6.1.0.Final/server/default/tmp	4	
_	Froomarkor	spring-core-3.0.5.RELEASE	/root/jboss-6.1.0.Final/server/default/tmp	4	
	rieemarker	spring-core-4.3.2.RELEASE	/root/jboss-6.1.0.Final/server/default/tmp	4	
	hibernate	spring-core-2.5.6.jar	/root/jboss-6.1.0.Final/server/default/tmp	4	
	turbine			1	
	struts			1	
	struts2		确症	4	
	webwork		JBoss	1	

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 1			视图 📃 🖵
业务组:全部 Y 枢梁名:全部 Q			
3 项		更新数据	全部导出
□ 框架名	主机数		Ш
ThinkPHP	2		
CdvPHP	1		
CanPHP CanPHP	1		

Т	ThinkPHP框加详细信息	1 to 1

服务类型	:全部 🝸 业务组:全部 🍸	版本:全部 Q 主机IP:全部 Q	主机名:全部 Q 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	Ш
	• 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PH	IP语言框架 1					视图 🗮 다
业务组	:全部 🍸 主机IP:全部 Q	主机名:全部 Q				
2 项						全部导出
	主机IP	框架数				Ш
	• 192.168.220.137	4				
	• 192.168.220.128	2				
主机19 服务类	22.168.220.137的PHP语言框架的 型:全部 ▼ 版本:全部 Q	祥细信息 ▲ 框架名:全部 Q 根目录:全部 Q	更多 ▼			
4 项						全部导出
0	框架名	框架版本	服务类型	根目录	应用路径	ш
	CdvPHP	4.0	Nginx	/var/www/html/	/var/www/html/cdvphp-maste	r
	CanPHP	3.0	Nginx	/var/www/html/	/var/www/html/canphp-maste	r
	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;

● 安装包和类库	^
◇ 系統安装包 8130种	
rpm包	50566个
dpkg恒	25213个
java包	8个
∽ Jar包 817种	
应用程序	33个
系統类庫	12个
Web服务自带库	632个
其它依赖包	182个

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	Weit t-			908 📰 🖵
安装包括	4型:金部 ▼ 公共相:金部 ▼ 和高:金部 Q			
8130	项	,	物而数据	全部导出
	包括	王昭政		ш
	sed	79		
	tzdata	79		
	findutiis	79		
	gzip	79		
	tar	79		
	curl	79		
	iptables	79		
	logrotate	79		

	SE: Em T Standig: Em	▼ 业务组:全部 ▼ 主机P:全部 Q	主机名:全部 Q			
79 项						全部导出
	主机IP	总述	版本	安装时间	安装包美型	ш
	□ 192.168.19.133	The GNU sed stream editor	4.2.2-4ubuntu1	2018-08-31 19:29:18	dpkg8	
	₽ 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	
	🖵 192.168.122.1	A GNU stream text editor	4.2.2-5.el7	2018-07-30 20:24:47	rpm包	
	I92.168.122.1	A GNU stream text editor	4.2.2-5.el7	2018-07-30 20:24:47	rpm包	

主机视角

安装包 _{安装包}	统计 1	+机P:全部 Q →机名:全部 Q	视图 🗮 🖵
80 项	Į		全部导出
	主机IP	安装包数	Ш
	🖵 192.168.8.23	3128	
	192.168.199.221	2391	
	192.168.192.165	2011	
	192.168.197.101	1908	
	192.168.248.129	1851	
	<pre> 192.168.32.136 </pre>	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	k			
3128	3 项					全部导出
	包名	总述	版本	安装时间	安装包类型	111
	attr	Utilities for manipul	1:2.4.47-2		dpkg包	
	axel	light download accel	2.4-1		dpkg包	
	apt-utils	package manageme	1.0.9.10+kali1~r2u1		dpkg包	
	aspell-en	English dictionary fo	7.1-0-1.1		dpkg包	
	arduino	AVR development b	2:1.0.5+dfsg2-4		dpkg包	
	apktool	A tool for reverse en	1.5.2-1kali1		dpkg包	
	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	t _		视图 📃 🖵
业务组:全	全部 ▼ 类型:全部 ▼ 包名:全部 Q		
817 项	查询类型 Q	更新数	据全部导出
	应用程序 包名 系统类库	主机数	
	web服务目带库 esources. 其他依赖包	2	
D js	sse.jar	2	
	ocaledata.jar	2	
c	ldrdata.jar	2	
🗆 ja	ce.jar	2	
□ s	unec.jar	2	
□ s	unpkcs11.jar	2	
	tjar	2	
□ s	unjce_provider.jar	2	
	og4j-1.2-api-2.11.1.jar	1	
🗆 n	netty-transport-4.1.16.Final.jar	1	

Jar包sunec.jar详细信息 🚹

奕型:全部 ▼ 是合可执行:全部 ▼ 业务组:全部 ▼ 更多	类型:全部 ▼	▼ 是否可执行:全部	βŢ	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	111
	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 👠		视图 🗮 🖵
类型:全部 ▼ 业务组:全部 ▼	主机IP:全部 Q 更多 ▼	
4 项		全部导出
□ 主机IP	包数	Ш
□ □ 192.168.200.130	688	
□ 🖵 172.27.0.15	141	
□ 및 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 Q 更多 ▼							
688 1	项						全部导出
	包名	类型	是否可执行	版本	绝对路径	操作	Ш
	OracleIdentityCl	Web服务自带库	否		/home/bert/Do	查看详情	
	_wl_cls_gen.jar	其他依赖包	否		/home/bert/Do	查看详情	
	_wl_cls_gen.jar	其他依赖包	否		/home/bert/Do	查看详情	
	_wl_cls_gen.jar	其他依赖包	否		/home/bert/Do	查看详情	
	_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 版本: 1.8.0_131 绝对路径: /usr/java/jdk1.8 MD5: 390fa11cc6e25577 引用情况 进程列表:	类型 是否 :.0_131/jre/lib/jsse.ja '21358f0c5eafd973	类型: 其他依赖包 是否可执行: 否 /Jsse-jar fd973		
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		
		确定		

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。

₩ 其他	^
◇ 启动项 200种	
系统启动项	185种
Xinetd网络托管服务	15种

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 默认启	(动功) ▲ (用状态:全部 ▼ 业务组:全部 ●	▼ 启动项名:全部 Q			视图 📃 🖵
117	项			更新数据	全部导出
	启动项名		启动项数		ш
	netconsole		12		
	network		12		
	sshd		5		
	auditd		5		
	halt		5		
	reboot		5		
	single		5		
	rdisc		4		
启动项	netconsole详细信息 💶				
单用户	自启动(rcs) : 全部 ▼ 停机(rc0) :	全部 ▼ 单用户模式(rc1):全部 ▼ 多	5用户无NFS模式(rc2): 全部 🔻	更多 🔻	
12 项	٦				全部导出
	主机IP	默认启动模式	默认启用状态		
	• 192.168.202.133	桌面模式(rc5)	未启用		
	• 192.168.199.16	完全多用户模式(rc3)	未启用		
	• 192.168.19.135	桌面模式(rc5)	未启用		
	• 192.168.122.1	桌面模式(rc5)	未启用		
	• 192.168.122.1	桌面模式(rc5)	未启用		
	• 192.168.122.1	完全多用户模式(rc3)	未启用		
	• 192.168.122.1	桌面模式(rc5)	未启用		
	192 168 100 220		土户田		

 主机系统启动项 ▲ 默认启动模式: 全部 ▼ 默认启动状态	::全部 ▼ 业务组:全部 ▼ 主机P:全部 Q 更	š 🔻	视图 📰 🖵
13 项			更新数据 全部导出
□ 主机IP	默认启动模式	启动项数	
• 172.16.2.240	桌面模式(rc5)	69	
• 192.168.202.133	桌面模式(rc5)	56	
• 10.9.191.52	完全多用户模式(rc3)	52	
• 172.16.2.241	多用户无NFS模式(rc2)	29	
• 192.168.199.16	完全多用户模式(rc3)	23	
• 172.16.4.190	完全多用户模式(rc3)	17	
• 10.211.55.8	桌面模式(rc5)	4	
• 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 ▼ 単用户自启动(rcs):全部 ▼ 係	亭机(rc0):全部 ▼ 単用户模式(rc1):全部 ▼ 更多 ▼	
69 Ij	Ę		全部导出
	启动项名	默认启用状态	III
	vmware-tools-thinprint	启用	
	local	启用	
	rpcbind	启用	
	abrtd	启用	
	sshd	启用	
	jexec	启用	
	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
□ 服务名	服务数	ш
rsync	4	
time-dgram	1	
time-stream	1	
telnet	1	
daytime-dgram	1	
C chargen-stream	1	

服务rsy	ync详细信息	t _		
启用状	态:全部 ▼	业务组:全部 🔻	主机IP:全部 Q	主机名:全部 Q
4项				
	主机IP		启用状态	
	• 192.168.2	202.133	未启用	
	• 192.168.1	199.16	未启用	
	• 172.16.2.	240	未启用	
	• 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P:全部 Q 主机名:全部 Q	
4 项		更新数据 全部导出
□ 主机IP	服务数 ↓	Ш
• 172.16.2.240	13	
192.168.202.133	1	
• 192.168.199.16	1	
• 10.9.191.52	1	

主机1	72.16.2.240的Xinetd网络托管服务	ŧ.
-----	--------------------------	----

启用状:	志:全部 ▼ 服务名:全部 Q		
13 项	Į		全部导出
	服务名	启用状态	111
	tcpmux-server	未启用	
	chargen-stream	未启用	
	echo-dgram	未启用	
	time-stream	未启用	
	telnet	未启用	
	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

Cronta 业务组	Crontab计划任务 ▲ 视图 - 业务组:全部 ▼ 执行脚本:全部 Q				
12 IJ	ų		更新数据	全部导出	
	执行脚本	计划任务数		Ш	
	/etc/cron.hourly/0anacron	12			
	/etc/titanagent/agent_update.sh	11			
	/etc/titanagent/agent_monitor.sh	11			
	/etc/titanagent/agent_update_exception.sh	11			
	/usr/sbin/raid-check	10			
	/usr/lib64/sa/sa2	9			
	/usr/lib64/sa/sa1	9			

|执行/etc/cron.hourly/0anacron脚本的计划任务 🚹

执行用所	□:全部 ▼	服务启用状态:全部	◎ ▼ 业务组:全部 ▼	が 执行周期:全部 Q	更多 🔻			
12 项	ī						全部	3导出
	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	Ш
	• 192.168	3.202.133	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	8.199.16	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	.19.135	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	.122.1	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	3.122.1	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	.122.1	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 192.168	.122.1	启用	01 * * * *	/etc/cron.hourly/	root	/etc/cron.d/0hourly	
	• 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				视图 🗮 🖵
服务启用状态:全部 ▼ 业务组:全部	Ŧ			
13 项			更新数据	全部导出
□ 主机IP	服务启用状态	计划任务数		Ш
• 192.168.202.133	启用	4		
• 192.168.199.16	启用	4		
• 192.168.122.1	启用	14		
• 192.168.122.1	启用	7		
• 192.168.122.1	启用	7		
• 192.168.122.1	启用	13		
• 192.168.100.220	启用	13		

主机19	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 Q	执行脚本或命令:全部 Q 配置文件:	全部 Q					
4项					全部导出			
	执行周期	执行命令或脚本	执行用户	配置文件路径	Ш			
	01 * * * *	/etc/cron.hourly/0anacron	root	/etc/cron.d/0hourly				
	*/10 * * * *	/usr/lib64/sa/sa1 1 1	root	/etc/cron.d/sysstat				
	53 23 * * *	/usr/lib64/sa/sa2 -A	root	/etc/cron.d/sysstat				
	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 业务组 :	计划任务统计 ▲ :全部 ▼					
85 项					更新数据	全部导出
	主机IP	启用状态		计划任务数 ↓		111
	₽ 192.168.100.162	启用		2		
	🖵 192.168.219.131	启用		1		
	및 192.168.122.1	启用		0		
	모 10.31.91.192	启用		0		
	<pre>□ 192.168.197.50</pre>	启用		0		
主机192	.168.100.162定时性计划任务组	充计 1_				
执行用户	≒:全部 ▼ 执行时间:全部	▼ 脚本路径:全部	Q			
2 项						全部导出
	执行时间		脚本路径	执行用户		111
	1963-11-18 19:31:44		/var/spool/at/a0000204132578	0x001		
	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
□ 主机IP	启用状态	计划任务数 🔸	111
□ □ 192.168.122.1	启用	0	
🔲 📮 10.31.91.192	启用	0	
192.168.197.50	启用	0	
□ □ 192.168.197.245	启用	0	

3.1.12.3 环境变量

资产视角

□ 环境变 环境变	量统计 1				视图 📃 🖵
204	项			更新数据	全部导出
	环境变量名	环境变量类型	主机数		ш
	OPTERR	用户变量	78		
	BASH_VERSION	用户变量	78		
	DIRSTACK	用户变量	78		
	IFS	用户变量	78		

环境变量OPTERR统计 🚹

	量类型:全部 ▼ 业务组:全部	▼ 用户:全部 Q	更多 ▼			
251	项					全部导出
	主机IP	用户	环境变量值	环境变量名	环境变量类型	
	192.168.248.145	test	1	OPTERR	用户变量	
	192.168.248.145	root	1	OPTERR	用户变量	
	192.168.248.145	root	1	OPTERR	用户变量	
	192.168.248.145	test	1	OPTERR	用户变量	

主机视图

主机环	境变量统计 1		视图 🗮 🖵
业务组	:全部 ▼ 主机IP:全部 Q	主机名:全部 Q	
86 I	Σ		全部导出
	主机IP	环境变量数	ш
	192.168.122.1	90	
	Q 10.31.91.192	34	
	192.168.197.50	73	
	192.168.197.245	32	

主机19 环境变	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 Q 环境变量值:全部 Q					
90 辽	σ					全部导出
	主机IP	用户	环境变量名	环境变量值	环境变量类型	ш
	□ 192.168.122.1	root	BASH	/bin/bash	用户变量	
	및 192.168.122.1	admin	BASH	/bin/bash	用户变量	
	192.168.122.1	admin	BASHOPTS	cmdhist:extquote:f	用户变量	
	192.168.122.1	root	BASHOPTS	cmdhist:extquote:f	用户变量	

3.1.12.4 内核模块

资产视角

主机内核模块统计				视图 📃 🖵
模块名称:全部 Q				
350 项			更新数据	全部导出
□ 模块名称	模块描述	主机数		Ш
□ tcp_diag		76		
☐ inet_diag		76		
i2c_piix4	PIIX4 SMBus driver	72		
ata_piix	SCSI low-level driver for Intel PIIX/ICH A	64		
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 Q 主机IP	:全部 Q 更多 🔻				
72 项	۶.						全部导出
	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	提作	111
	192.168.91.132	/lib/modules	43597	1	0	查看详情	
	192.168.152.145	/lib/modules	24576	0	0	查看详情	
	192.168.197.55	/lib/modules	22106	1	0	查看详情	
	192.168.199.119	/lib/modules	12608	1	0	查看详情	
	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 Q	主机名:全部 Q
80 Ij	Σ	
	主机IP	内核模块数
	192.168.122.1	106
	D 10.31.91.192	46
	192.168.197.50	61
	192.168.197.245	44

主机19	92.168.122.1内核模	快查询 🚹						
模块版:	本:全部 ▼ 模块	名称:全部 Q 模块	·路径:全部 Q					
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	Ш
	xt_conntrack	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				
想想理灵分布 		修复影响分布 	 系統重向:128 服务重向:697 无策重向:183 未初影响:357 	
✓ 业务组:所有▼ 危险程度:所有▼ 修复影响:所有▼	业务影响:所有 ▼			3 💁
670 项				(S) ④ 立即检查 检查业务影响 导出 ::
□ 危险程度 补丁名添 个		风险特征		影响主机数 🔿 III
CentOS 5 / 6 / 7 : bash (CESA-2014	1:1293)	[送程利用] 存在EXP] [奚皖重启]		2
CentOS 5 / 6 / 7 : bash (CESA-2014	1:1306)	[远程利用] (存在EXP) (系统重用)		2
CentOS 5 / 6 / 7 : bind (CESA-2014	:1984)	「設理利用」「服务里启」		2
CentOS 5 / 6 / 7 : bind (CESA-2016	:0073)	[远程利用] [服务重向]		5
日本 CentOS 5 / 6 / 7 : bind (CESA-2016	:0459)	[近程利用] [服务重启]		5
CentOS 5 / 6 / 7 : bind (CESA-2016	:1944)	运程利用]存在EXP 服务重启		5
CentOS 5 / 6 / 7 : firefox (CESA-20	16:0695)	[透曜利用] [无業重寫]		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

业务组:所有 ▼ 危险程度:所有 ▼ 修复影响:所有 ▼ 业务影响:所有 ▼ 补丁名称:所有 Q 更多 ▼

③ 状态统计图按钮:点击 按钮,收起/展开统计图区域;

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

⑤ 更多设置按钮:点击 按钮,显示全部;

⑥ 排序按钮: 鼠标移入列名,点击按钮对数据进行排序,点击 按升序排列, 按降序排列; 设置显示列按钮:点击 Ⅲ,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.险概范 风险分析	全部日
58 安全评级为E,存在较多严重问题,请立即修复! ^{发展 2059 个风剧课,影响 26 台主机 查查告诉记录}	理新于 2019-11-07 16-57-01
● 安全补丁 发现安全补丁 1942 个,其中危急补丁 32 个,影响主机 24 台	~
发现存在exp且可远程利用的补丁 360 个,影响主机 24 台	0
发现存在exp的补丁 536 个,影响主机 24 台	0
发现内核级别的补丁 315 个,影响主机 16 台	0
发现可被运程利用的补丁 1420 个,影响主机 24 台	0
未发现内核级别旦可本她爆权的补丁	٥
发现可本地提权的补丁 3 个,影响主机 5 台	0
弱密码应用 发现弱密码应用 <u>4</u> 个,影响主机 <u>12</u> 台	~
波现MySQL服务存在弱密码 27 个	0
发现Redis服务存在调密码 2 个	0
发现vsftpd服务存在弱密码 10 个	0
未发现OpenVPN服务存在弱密码	٥
未发现rsync服务存在调查码	0
发现SSH服务存在弱密码 34 个	0
查看更多	٥
对外访问性 发现对外访问性1个,影响主机2台	~
未发现MongoDB服务的对外访问性风险	0
专 指词 Memcache 服 经 的 对 体 访 后 性 团 险	•

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;

全部扫描	查找主机	更多 🔻
全部扫描		
按业务组扫描		
按主机IP扫描		

选择业	务组[2/59]	
	业务组	主机数
	未分组主机	0
	zllinux	5
	dongxiaohui	3
	lu_linux	2
	hp_linux01	1
	hp_linux02	1
	lh.huang.linux	2
	tianwen.zhan-linux	5
	fan	0
	sw-linux	1
		取消 立即扫描

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;

业务	组: 全部 🔻	操作系统:全部 🔻	主机状态:全部 ▼	主机IP: 全部 Q	主机名:全部 Q
	主机状态	主机IP	主机名	操作系统	业务组
~	• 在线	192.168.159.1	28 hostB	CentOS releas	e 6.4 gxy-groupB
~	• 在线	192.168.159.1	29 localhost.local	dom Red Hat Enter	prise gxy-groupB
	● 在线	192.168.228.1	37 ubuntu	Ubuntu 16.04	LTS, lu_linux
	● 在线	192.168.159.1	33 GXY	Ubuntu 14.04	LTS, gxy-groupA
	● 在线	172.16.4.65	localhost.local	dom CentOS Linux	relea hp_linux02
	● 在线	192.168.80.17	9 dongxiaohui-v	rirtu Ubuntu 14.04.	.5 LT dongxiaohui
	• 在线	192.168.80.13	0 localhost.local	dom CentOS Linux	relea dongxiaohui
	● 在线	192.168.80.14	9 host01	CentOS releas	e 6.4 ww-linux
	● 在线	172.16.2.238	" "	CentOS releas	e 6.1 tianwen.zhan-linux

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。

查找主机					
业务组:全部 ▼	主机状态:全部 ▼	主机IP: 全部 Q	主机名:全部 Q		
主机状态	主机IP	主机名	业务组	操作	
 在线 	192.168.159.128	hostB	gxy-groupB	查看	
● 在线	192.168.159.129	localhost.localdom	gxy-groupB	查看	
● 在线	192.168.228.137	ubuntu	lu_linux	查看	
 在线 	192.168.159.133	GXY	gxy-groupA	查看	
 在线 	172.16.4.65	localhost.localdom	hp_linux02	查看	
 在线 	192.168.80.179	dongxiaohui-virtual	. dongxiaohui	查看	
 在线 	192.168.80.130	localhost.localdom	dongxiaohui	查看	
• 在线	192.168.80.149	host01	ww-linux	查看	
					关闭

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。

	2019-10-28 20:12:23	账号风险扫描 全	部主机 qi	ingteng@qingte	8€9	❷扫描成功	成功 4 台,失败 3 台	失败主机详情	
条	记录支持对	失败主机的	详情进行到	查看,点音	击"失败主	机详情"	按钮可查	看失败主机	列表。
全部风	≥ 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 Q	执行对象:全部 Q						
160	项								
	开始扫描时间	任务名		执行对象		总耗时	失败房	因	111
	2019-11-07 04:36:32	SSH服务Aut	horizedKeysFile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Aut	horizedKeysFile配置名称	192.168.131.13	36	0秒	agent	不支持此脚本	
	2019-11-07 04:36:32	SSH服务Aut	horizedKeysFile配置名称	• 192.168.199.22	2	0秒	agent	不支持此脚本	

总耗时

23分1秒

22分17秒

1分51秒

扫描状态

○扫描中

⊘扫描成功

⊘扫描成功

⊘扫描成功

0秒

执行结果

成功0台,失败0台

成功 6 台,失败 10 台

成功4台,失败6台

成功4台,失败4台

操作

弱密码讲度

失败主机详情

agent不支持此脚本

弱密码进度 失败主机详情

弱密码进度 失敗主机详情

111

2019-11-07 04:36:32 SSH服务AuthorizedKeysFile配置项存... 192.168.131.136 0.Pb 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

• 192.168.199.85

弱密码	扫描进度详情 👠					
8 4	\$次弱密码扫描的进度为: 100.00%					
总耗时	:全部 ▼ 任务名:全部 Q	扫描主机:全部 Q				
15 Iļ	页					
	开始扫描时间	任务名	扫描主机	总耗时	账号扫描进度	Ш
	开始扫描时间 2019-10-29 10:19:06	任务名 vsftpd服务存在制密码	扫描主机 • 192.168.80.141	总耗时 5秒	账号扫描进度 1/1	Ш
	开始扫描时间 2019-10-29 10:19:06 2019-10-29 10:19:06	任务名 vsftpd服务存在调密码 vsftpd服务存在调密码	扫描主机 • 192.168.80.141 • 172.16.2.229	总相时 5秒 5秒	账号扫描进度 1/1 3/3	III
	开始白丽时间 2019-10-29 10:19:06 2019-10-29 10:19:06 2019-10-29 10:19:06	任务名 vsftpd服务存在弱密码 vsftpd服务存在弱密码 vsftpd服务存在弱密码	扫描主机 192.168.80.141 172.16.2.229 192.168.80.149	总和时 5秒 5秒 5秒	账号扫描进度 1/1 3/3 1/1	111

查看弱密码执行进度情况。

执行记录 🛍

69 项

开始扫描时间

D 2019-10-29 12:16:00

D 2019-10-29 10:19:05

D 2019-10-29 04:30:02

D 2019-10-28 20:52:30

2019-11-07 04:36:32

总耗时:全部 ▼ 扫描状态:全部 ▼ 开始时间:全部 ▼

执行内容

弱密码扫描

弱密码扫描

全部风险扫描

应用风险扫描

执行范围

全部主机

全部主机

全部主机

全部主机

SSH服务AuthorizedKeysFile配置项存...

执行者

system

qingteng@qingte...

gingteng@gingte...

qingteng@qingte...

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	攻击途径:远程/本地
评分维度	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

安全补丁		祝園 📒	Ģ
想能理定日本	影响分布 25.5% 1.1% ● 联防器曲: 277 · 无管型机: 269 · 氯铁墨血: 219		
立内垣:金部 ▼ 作用系向:金部 ▼ 立内系向:金部 ▼ 立内系向:金部 ▼ 口川(日本) 立内垣:金部 ▼ 印石(日本) 九回(日本) 中田(日本) 中田(日本) 中田(日本) 中田(日本) 中田(日本) <			9 .
865 项		立即扫描 检查业务影响 全部导出	:
2 危給程度 补丁名称		风险特征 影响主机数	ш
Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerabilities (USN-2364-1)		這程利用]存在 1	
D Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 14.10 / 12.10 : memcached运程代码执行面向		远程利用 服务 1	
Oracle Linux 7 : glibc (ELSA-2016-0176)		运程利用 存在 1	
CentOS 6 / 7 : blnd (CESA-2015:1513)		远程利用 存在 1	
Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerabilities (USN-2380-1) (Shellshock)		远程利用」存在… 1	
Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerability (USN-2362-1) (Shellshock)		远程利用] 存在 1	
CentOS 6 : glibc (CESA-2016:0175)		這程利用」存在 1	

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。

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulne	rabilities (USN-2380-1) (Shellshock)影响的主机 🗈		
业务相分布 2 1 0 haoyan	业务影响分布		
	' 业务组;全部 ▼ 主机P:全部 Q 主机名:全部 Q		Э.
1 项			全部导出
□ 主机IP 业务组	业运动影响	发现时间	补丁详情 Ⅲ
 192.168.30.147 hao.yan 	228	2018-09-06 04:30:04	查看

存在业务影响时,可点击可查看进程影响的详情。

tOS 5 / 6 / 7 : bash (CESA	-2014:1306)影响的主机	1					
业务组分布	影响的业务进程列表						
	PID 端口/协议	绑定IP	进程名	启动参数	依赖包	包版本	
	2567		bash	-bash	bash	4.1.2-14.el6	
	3163		bash	bash	bash	4.1.2-14.el6	
o ww-linux	17660		bash	bash	bash	4.1.2-14.el6	
	17646		bash	bash	bash	4.1.2-14.el6	
时间:全部 ▼ 资产等级:4							
φ							全部导
							补丁详情
• 192.168.101.134							直看
• 192.168.80.149						164:53	查看

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

安全补丁					祝恩 🗮 🖵
主机状态:全部 ▼ 业务影响:全	#部 ▼ 业务组:全部 ▼ 主机#	?:全部 Q 主机名:全部 Q			۹.
26 项				(正在检查 :	全部导出
□ 主机IP	风脸项分布				Ш
9 192.168.2.172	4	208		134	11
• 172.16.146.132	2	89	79		3
• 192.168.192.165	1	99		62	2
• 192.168.19.135	47		89		7
• 10.211.55.21	37		73		8
0 10.211.55.26	37		73		8
9 192.168.30.147	3	54	39		8

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。

主机192.168.192.16	5的补丁 🐛				
危险程度分布	业务影响分布				
37.89	1000 0005 0005 0005 0005 0005 0005 0005				
危险程度:全部 🔻	业务影响:全部 Y 发现时间:全部 Y 应用:全部 Y CVE编号:全部 Q 朴丁な称:全部 Q	更多 🔻			۵.
164 项					全部导出
□ 危险程度	补丁缩称	风险特征	业务影响	发现时间	补丁详情 Ⅲ
1 危急	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 14.10 / 12.10 : memcached运程代码执行雇用	[近程利用] [服务重启]	50 C	2018-10-25 04:30:12	查看
- X1	Ubuntu 14.04 LTS : linux-Its-xenial vulnerability (USN-3220-2)	家純重启	228	2018-10-25 04:30:11	查看
<u>الله الم</u>	Ubuntu 14.04 LTS : linux-Its-xenial vulnerabilities (USN-3291-3)	内核风险(系统重启)	228	2018-10-25 04:30:11	查看
<u>المجامعة</u>	Ubuntu 14.04 LTS : linux-Its-xenial, linux-aws vulnerabilities (USN-3509-2) (Dirty COW)	存在EXP	528	2018-10-25 04:30:12	查看
高能	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : requests vulnerability (USN-3790-1)	服务重启	53	2018-10-25 04:30:12	查목
- <u>K</u> t	Ubuntu 14.04 LTS : linux-Its-xenial vulnerabilities (USN-3169-2)	存在EXP)系統重由	528	2018-10-25 04:30:11	查查
- 20	Ubuntu 14.04 LTS : linux-its-xenial vulnerabilities (USN-3469-2)	存在EXP 系統重启	528	2018-10-25 04:30:11	查看
	THE SEA OF THE AND A THE AND AN AN AN ANALYSIS COMMAND STRAIN AS	(#@10) (*** ##)		2018-10-25	±#

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。

安全补丁修复历史 🐿						
概览 修复情况分析]				最近一次扫描时间:2019-04-0	9 02:47:01 过去7天 过去30天 过去3个月
修复补丁统计	危险程度分布	修复时长统计				
14	2 。商告:12	1.7 • 危急: 0.057d • 高危: 2.019d				
修复补丁数	 中陰:0 危急 低色:0 	 ● 中應: ● 平均修复时长(天) ● 低饱: 				
危险程度:全部 ▼ 应用	: 全部 🔻 修复耗时: 全部 🔻 远程和	训用:全部 ▼ 补丁名称:全部 Q	主机IP:全部 Q 更多 ▼			
2019.01.09 ~ 2019.04.09 🗙	存在EXP:全部 ▼ 内核风险:全部	▼ 本地提収:全部 ▼ 资产等级	Q:全部 Y 发现时间:全部 Y	业务组:全部 ▼ 主机名:全部	Q CVE编号: 全部 Q	
14 项						全部导出
□ 危险程度	补丁名称	主机IP	业务组	发现时间	修复时间	修复耗时(天)
高危	Apache Tomcat 6/7/8 - Privilege Escala	tion 0 192.168.202.142	centos	2019-03-02 01:31:06	2019-03-03 01:31:05	1.0
高度	Apache Tomcat 7/8/9 Security Bypass \	/uln 0 192.168.202.142	centos	2019-03-02 01:31:07	2019-03-03 01:31:05	1.0
高危	Apache Tomcat 6/7/8/9 -regression(QT	JAV 0 192.168.202.142	centos	2019-03-02 01:31:07	2019-03-03 01:31:05	1.0
同時の	Apache Tomcat 6/7/8 - Privilege Escala	tion © 192.168.202.142	centos	2019-02-26 15:48:42	2019-02-27 01:31:10	0.4
商務	Apache Tomcat 7/8/9 Security Bypass \	/uln 0 192.168.202.142	centos	2019-02-26 15:48:42	2019-02-27 01:31:10	0.4
局部	Apache Tomcat 6/7/8/9 -regression(QT	JAV 0 192.168.202.142	centos	2019-02-26 15:48:42	2019-02-27 01:31:10	0.4
高危	Apache Tomcat 6/7/8 - Privilege Escala	tion 0 172.16.2.240	centos	2019-01-22 18:06:47	2019-01-29 03:31:17	6.4
高危	Apache Tomcat 7/8/9 Security Bypass \	/uln 0 172.16.2.240	centos	2019-01-22 18:06:47	2019-01-29 03:31:17	6.4
同商権	Apache Tomcat 6/7/8/9 -regression(QT	JAV 0 172.16.2.240	centos	2019-01-22 18:06:47	2019-01-29 03:31:17	6.4

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

既览 修复情况分析			最近一次扫描时间:	: 2019-04-09 02:47	01 过去7天 过去30天 过
▶丁总数超势 ⅲ	业务组分布	修复时长分布			
		15	1.0		
01-22 01-23 01-29 0	2-27 03-03 test	centos —天内	1至7天	7至30天	30天以上

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 印可进入白名单规则设置页面。

白名单规则 €			
条件:所有 Q 范围:所有 Q 受影响主机P:所有 Q			
1项			新建白名单规则
□ 条件	范围	受影响对象	操作
□ □ 通同特征为:本地通问	全部主机	532	/ 1

▶ 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 1			
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 		
	O 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						祝四 :==
高洞检测支持可	「自走义漏洞检查任务,您可以进入 作业管理 进行漏洞作业的创建、删除、修改和	0执行.				
漏洞通知 GoAhead远程命令 Tomcat开放重定师 Git任意代码执行酒 glibc整数溢出漂洞 Jenkins远程命令步	24以子廣調(CVE-2017-17562) 均周四(CVE-2018-11784) 相同(CVE-2018-17456) (ICVE-2016-4655) NF透調(CVE-2016-6786)	聖智更多 2019-03-03 2019-03-05 2019-03-05 2019-03-05 2019-03-05	羅明統計 16 13 □ 6 可這種利用	10 狩在exp	3 可本地提权	2 PSHERTAR
业务组:全部 ▼	危险程度:全部 ▼ 应用:全部 ▼ 羅同名称:全部 ▼]	総洞夾型:全部 ▼				
16 项						作业管理 全部导出 更多
危險程度	混詞名称	满洞头型		識洞特征		影响主机数
意識	Linux内核本地提权(航牛)漏洞(CVE-2016-5195)	本地提权		存在EXP	内核风险 本地提权 重启系统	3
急急	OpenSSL Heartbleed溝洞(CVE-2014-0160)	敏感信息泄露		存在EXP	远程利用 重启服务	1
意識	Bash环境变量远程命令执行通同(CVE-2014-6271)	命令执行		存在EXP	远程利用 重启系统	1
意為	Samba远程代码执行漏洞(CVE-2015-0240)	代码执行		存在EXP	远程利用 重启服务	1
きたものの	OpenSSLASN.1编译器内存损坏漏洞(CVE-2016-2108)	代码执行		运程利用	重启服务	1
高危	Linux内核信息泄露漏洞(CVE-2016-9555)	敏感信息泄露		运程利用	内核风险 重启系统	4
高度	Oracle MySQL远程代码执行濡洞(CVE-2016-6662)	代码执行		存在EXP	远程利用重启服务	3
高危	Sudo本地权限提升漏洞(CVE-2017-1000367)	本地提权		存在EXP	本地緩权	3
高危	Bash本地命令执行漏洞(CVE-2016-7543)	命令执行		运程利用	里向系统	2
ena.cn/next/#/risk	-discoverv/vulnerabilitv/detail/check/0T042019000010/-1			-	(mente)	

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

	百春田冬	》唐书为自论系列于
导出统计报表		
全选		
☑ 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
□ 受影响系统	🗌 漏洞利用链接	□ 参考链接
□ CVSS评分	□ CVSS详情	☑ 影响主机数
文件將下載到本地, 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		1
 ✓ 主机状态 ✓ 业务组 □ 外网IP □ 负责人 漏洞详情:全选 	 ✓ 主机IP □ 资产等级 □ 操作系统 □ 负责人邮箱 	 ✓ 主机名 □ 内网IP □ 主机标签 □ 备注
 ✓ 危险程度 ✓ 远程利用 ✓ 本地提权 ✓ 修复影响 文件将下载到本地,也可稍后調 	 漏洞名称 存在EXP 漏洞描述 登证信息 前往下载记录下载。 	 ✓ 漏洞类型 ✓ 内核风险 ✓ 修复建议 ✓ 影响应用 取消

3.2.3.1 主机视图

漏洞检查						视	8 📰 🖵
1 漏洞检测支持可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。						×
黒同連知 Apache Soli武程命令执行無同(CVE-2019-0193) Jackson-databind远程代码执行無同(CVE-2019-12384) FastJSON成程代码执行面间 Apache AXIS远程命令执行面间 Oracle WebLogic wis9-asyncl即件反序列化远程命令执行篇同(CVE-2019-2729)	書書 2019-06 2019-06 2019-06 2019-06 2019-06	■ ■ ■ ■ ■ ■ ■ ■ ■ 16 ■ ■ ■ ■ 16 ■ ■ ■ 16 ■ ■ ■ ■ 16 ■ ■ 16 16 16 16 16 16 16 16 16 16	48 可运程利用	24 存任exp	4 可本地提权	3内核风险	
业务组:全部 ▼	第 ▼ 主机名称:全部 ▼				f	和 全部导出	更多▼
□ 主机P	业务组			漏洞数			På
• 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 1_							
自定义作业全局作业							
创建时间:全部 ▼	▼ 执行范围:全部 ▼						
4 项						(新建作业
□ 创建时间	作业名称	是百自用	执行范围	检查项数	最后执行时间	操作	ľ6
D 2018-10-24 20:30:58	uWSGI PHP目录穿越漏洞(CVE-20	一是	全邸主机	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	作业详情 执 编辑	
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	扐 删除	
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	管理 1_									
自定	自定义作业 全局作业									
创建时	间:全部 ▼ 作业名称:全部	Ŧ								
7项	Į									
	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			Pò
	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	7
	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	1
	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	7
	2018-08-29 10:20:12	反序列漏洞检查	是	全部主机	5	2018-09-06 10:04:05	执行	查看结果	作业详情	1
	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	V
	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	V

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。

编辑作业 🐿						
作业基本信息	检测项信息					
作业名:	uWSGI PHP目录穿	越漏洞(CVE-2018-7490)-20181024084930				
定时作业:	○ 清输入定时表	联大式	0			
执行范围:	 全部主机 					
	O 选择业务组	请选择业务组	v			
	O 选择主机	请选择主机IP	Ψ			
是否启用:	信用					
备注:	请输入备注信息					
				取消	保存	保存并执行

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】

作业执行结果				総图 🧮 🖵
拒绝股务漏洞检查 创建时间:2018-09-0516:19:57 最后时间:99:2019-04-0411:31:14 检查和时:38	かられま 4 2 痛用の数 創作主が取	15 15 松泉町成数 ● あり7	2 (1) (2) (2) (1) (2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	
业务値:金部 ▼ 急焓程度:金部 ▼ 広用:金部 ▼	存在EXP:全部 ¥ 」 远程利用:全部 ¥ 内核风险	::全部 ▼	25 V	
4 项				全部导出
危险程度 通同名称	選詞类型	漏洞特征	影响主机数	Pè
□	675) 拒绝服务攻击	内核风险	2	
〇 高館 Oracle MySQL远程安全漏洞(CVE-2018-2)	562) 拒绝服务攻击	這種利用」「重自服务」	1	
□ 中能 BIND远程拒绝服务漏洞(CVE-2018-5740)	拒绝服务攻击	[這程利用] (重 自服务)	2	
□ 中胞 BIND远程拒绝服务漏洞(CVE-2017-3145)	拒绝服务攻击	运程利用] 重点服务	2	

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】
作业执行结果			報21 🗮 🖵
辺程代码执行清洞检查 創課前面:2019-07-24 1025-24 最回防行时间:2019-05-11 23:20:15 检查判例:29秒	执行结果 8 2 扁用色致 影响主机政	执行備兒 (73) 检測咳嗽 ● 5 执行成功主机	(109) 與行外攻主机 (査司)
资产等级:全部 ▼ 业务组:全部 ▼ 主机状态:全	部 ▼ 主机IP:全部 ▼ 主机名称:全部 ▼		
2 项			全部导出
□ 主机P	业勞组	漏洞数	Ρģ
• 10.211.55.21	产品组	8	
• 172.17.0.17	xiaotong	1	

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

新建作业 1		
作业基本信息	检测项信息	
作业名:	请输入作业名	
定时作业:	○ 潘榆入定时表达式	0
执行范围:	 全部主机 	
	O 选择业务组 请选择业务组	·
	O选择主机 请选择主机IP	
是否启用:	<○ 启用	
备注:	请输入衛注信息	
		取消 创建 创建并执行

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

5建作业 € 作业基本信息							
50 项						添加档	金卿项
□ 类別 检测项名称	检测方式 0	执行风险	发布时间	是否加入全局	输入参数	操作	ľå
□ 跨站脚本攻击 Struts2 S2-002 跨站脚本潇洞	版本对比	无风险	2008-03-04	是		删除	
□ 未授权访问 Mysql_Mariadb 认证统过漏洞(CVE-2012-2122)	版本对比	无风险	2012-06-11	是		删除	
□ 代码执行 Samba运程代码执行需同(CVE-2012-1182)	版本对比	无风险	2013-03-08	是		删除	
□ 命令执行 Struts2 S2-016远程命令执行瀧侗(CVE-2013-2251)	版本对比	无风险	2013-07-09	是		删除	
□ 命令执行 Struts2 S2-020命令执行圊洞(CVE-2014-0094)	POC验证	无风险	2014-03-11	是		删除	
□ 較應信息泄露 OpenSSL Heartbleed 漏洞(CVE-2014-0160)	版本对比	无风险	2014-04-07	是		删除	
□ 命令执行 Struts2 S2-021命令执行漏洞(CVE-2014-0113)	版本对比 ▼	无风险	2014-04-24	是		删除	
□ 服务뻀请求伪造 Weblogic SSRF漏洞(CVE-2014-4210)	☑ 版本对比	无风险	2014-07-17	是		删除	
□ 代码执行 glibc缓冲区溢出漏洞(CVE-2014-5119)	□ POC 塑业	无风险	2014-08-05	是		删除	
□ 代码执行 ElasticSearch	版本对比 ▼	无风险	2014-09-11	是		删除	
□ 命令执行 Bash环境变量远程命令执行漏洞(CVE-2014-6271)	版本对比 ▼	无风险	2014-09-24	是		删除	
□ 命令执行 Bash环境变量远程命令执行漏洞(CVE-2014-7169)	版本对比 ▼	无风险	2014-09-24	是		删除	
□ 代码执行 Bash远程代码执行漏洞(CVE-2014-6278)	版本对比	无风险	2014-09-24	是		删除	
□ 代码执行 Bash沅绿代码执行挪测(CVF-2014-6277)	版本对比	无风险	2014-09-24	₽ ₽		删除	

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。

白名单规则 14_			
祭件:全部 Q. 范围:金部 Q.			
1 项			新建白名单规则
中报 □	范围	受影响对象	操作
□ 况间在中包含:OpenSSL Heartbleed 提问(CVE-2014-0160)	全部主机	查看详情	× 11

• 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: 请输入漏洞名称	
	□ 漏洞特征: 请选择漏洞特征	Ŧ
	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

规则受	影响对象 👠				
9项					
	危险程度	識詞名称	主机IP	小發租	I
	高危	Ghostscript命令执行(沙箱绕过)漏洞(CVE-2018-15910)	• 192.168.122.1	product	
	危急	Linux内核本地提权(脏牛)漏洞(CVE-2016-5195)	• 192.168.167.129	ops	
	高危	glibc本地权限提升漏洞(CVE-2018-1000001)	• 192.168.122.1	product	
	商商	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	• 192.168.122.1	product	
	高危	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	• 192.168.1.132	Ybkuo	
	高危	MySQL、MariaDB本地权限提升漏洞(CVE-2016-6664)	• 192.168.167.129	ops	
	商店	Linux内核本地拒绝服务漏洞(CVE-2018-10675)	• 192.168.167.129	ops	
	高危	Sudo本地权限提升遥洞(CVE-2017-1000367) 0	• 192.168.167.129 0	ops	
	商危	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;

调密码列表		视图 🗮 🖵
周期性检测系统中各类应用存在的第口令情况,查看支持检测的应用列表		×
应用為:金部 ▼ 业务相:金部 ▼		9 .
8项		立即扫描 全部导出 :
□ 意用	弱密码数量	操作
SSH SSH	35	查看
MySQL	13	查看
vsftpd	5	查看
D PPTP	4	查看
UNC VNC	2	查看
Redis	2	查看
Tomcat	1	杏石

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

自动专行的复数		
弱密悄修复历史	1 L	

 概先 修复情况 修复期密码统计 61 修复第密码数 	分析 5.7 平均修築时长(天) 외	码关型分布 0 0 1 0 系统默认) 0 5用户客相同	61 常见翻卷码		最近一次扫描	3阅:2019-04-09 02:47:01	过去7天 过去30天	过去3个月
发现时间:全部 ▼ 账号状态:全部 ▼	2019.01.09 ~ 2019.04.09 🗙 应 修复耗时:全部 🔻 业务组:全部	用:全部 ▼	类型:全部 ▼ 账号	名:全部 Q 主机IP	:全部 Q 更多 ▼				
61 项									全部导出
□ 应用	主机IP	业务组	账号名	账号状态	弱密码类型	发现时间	修复时间	修复耗时 (天)	Ш
MySQL	• 192.168.122.1	centos	ml_db	❷ 启用	常见弱密码	2019-03-18 01:34:52	2019-03-19 01:38:01	1.0	
Redis	• 192.168.122.1	centos		❷ 启用	常见弱密码	2019-03-18 01:33:49	2019-03-19 01:38:01	1.0	
Redis	• 192.168.122.1	centos		❷ 启用	常见弱密码	2019-02-21 01:39:11	2019-03-17 01:33:45	24.0	
MySQL	• 192.168.122.1	centos	ml_db	❷ 启用	常见弱密码	2019-02-21 02:07:07	2019-03-17 01:33:45	24.0	
Tomcat	• 172.16.2.240	centos	tomcat-user	♥ 启用	常见弱密码	2019-03-06 01:35:44	2019-03-07 01:32:43	1.0	
Tomcat	• 172.16.2.240	centos	tomcat	♥ 启用	常见弱密码	2019-03-06 01:35:44	2019-03-07 01:32:43	1.0	
MySQL	• 172.16.2.240	centos	root	❷ 启用	常见弱密码	2019-03-06 01:35:33	2019-03-07 01:32:41	1.0	
vsftpd	• 172.16.2.240	centos	wentao.ma	❷ 启用	常见弱密码	2019-03-06 01:35:49	2019-03-07 01:32:40	1.0	

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

概览 修复情况分析		最近一次扫描时间:2019-04-09 02:47:01 过去7天 过去30天 过去3个月
弱密码修复趋势 🔛	应用分布 🏭	业务组分布 🏭
	75	25
01-28 01-29 01-30 02-04 02-12 02-13 02-27 03-07 03-17 03	SSH MySQL Redis Tomcat vsftpd	ubuntu centos

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。

白名单规则 1_			
条件:所有 Q 范围:所有 Q 受影响主机P:所有 Q			
1项			新建白名单规则
日 条件	范围	受影响对象	操作
□ 账号状态为:不可登录	全部主机	0	Z 11

▶ 新建白名单规则

新建日名甲规则 1	-	
条件列表:	□ 应用包含:	请输入弱密码的应用,多个以逗号隔开
	□ 应用账号中包含:	请输入弱密码应用的账号,多个以逗号隔开
	□ 账号状态:	请选择账号状态
	□ 弱密码类型:	请选择弱密码类型
	则将风险项加入白名单	
规则范围:	● 全部主机	
	○ 自定义范围	
	□ 业务组: 请道	5年业务组 ▼
	□ 主机: 请	起译主机IP
	创建取消	

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

白名单规则			
条件:所有 Q. 范園:所有 Q. 愛歌納主切P:所有 Q.			
1项			新建白名单规则
□	范围	受影响对象	操作 Ⅲ
□ 账号状态为:不可整录	全部主机	0	/ 1
▶ 删除白名单规则			
日名が規則 企 単件:所有 Q 范囲:所有 Q ジャンティー (100)			
1 项			新建白名单规则
中 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	范围	受影响对象	操作 Ⅲ
□ 账号状态为:不可整录	全部主机	0	/ 1

3.2.4.4 简单密码字典

单击右侧 ⁱ 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;

自定	义简单密码 🛛	简单密码字典说明	扖	导出
01	列表为空 , 请添	简单密码子典,检查用户的密码设置为该密码子典中 的任意密码,则判定为弱密码		
02		编辑字典		
03		点击编辑框直接输入密码,每行为一个弱密码		
04		导入字典		
05		• 仅支持TXT格式文件导入;		
06		• 每个弱密码以换行分割;		
07		• 每次导入将完全覆盖原密码字典 ;		
08		• 每次导入最多识别前3000个弱密码,其后将忽略		
09		导出字典		
10		导出字典将导出所有弱密码为TXT文件,换行分隔;		
11			_	
12				
13				
0/300	D	取	消	确定

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:

自定	义组合密码 🛛	组合密码字典说明	
前缀	密码 连接符	组合密码指组合密码符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:	
01 02 03	jieyuechina@2	 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; 前缀是多可添加8个,连接符9个,后缀19个,均使用换行符稿开 	
04		例如 检测某账号: admin:	
06		动态密码字典:前缀为abc;连接符为@;后缀为123 则络拾音如下朝密码: admin@123:admin@:	
07		admin123 ; admin ; abc@123 ; abc123 ; abc@ ; @123 : abc : @ : 123 :	
09		,,.,.,.,.,	
10			_
11			
12			
1 /8		取消	确定

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

<u> </u>	加密		视图 :== +
\$	思验程度分布 20	2009 00% 00% 	
危险档	腹:全部 ▼	应用:全部 ▼	۵.
5 项			立即扫描 全部导出 :
	危险程度	风脸淡名	影响主机数 111
	高危	SSH服务用户home目录中存在未加密礼码	2
	高危	MongoDB服务未开曲认证	1
	高危	nginx 是否开由同源策略和referer检测	1
	中危	httpd 非常规扩展名詞本解析配置检测 0	1
	低危	httpd host失攻击检查	2

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

系统风险		视图	= 🖵
危強程度分布 42.9%	14.3% 2869		
危险程度:全部 ▼ 应用	:金部 Y 业务组:金部 Y 风险项名:金部 Q		٩.
7项		立即扫描 全部导出	:
□ 危险程度	风险质名	影响主机数	Ш
□ 危急	服务确时间收益	2	
高危	諸由转发功能开启	2	
日間を	/var/spool/cron目录所有者、组所有者读写执行权限	1	
□ 中 念	/etc/gshadow权限检查	1	
低危	umask值异常	7	
低危	Bash未使用安全审计Bash	6	
□ 低意	grub密码设置	6	

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。

账号风险		视图	
危险程度分布	66.7% - 危急:0 - 市商:2 - 低盘:1		
危险程度:全部 ▼ 应用:	全部 Y 业务组:全部 Y 风险须名:全部 Q		٩.
9项		立即扫描 全部导出	:
□ 危险程度	风始淡省	影响主机数	ш
商商	未设置应码编试次数概定	6	
商商	账户家目录任意读写	6	
高商	未设置當時度会處預制	6	
日間で	非wheel组用户使用SU切除root	6	
高危	账号未设置过期时间	4	
高商	无密码可sudo的账号	1	
中位	/etc/shadow{0現检查	1	
中危	存在非本机PAM认证方式	1	

3.2.7.1 白名单规则

• 新建白名单规则

新建白名单规则 1		
新建规则		
条件列表:	风险名中包含: 请输入风险名称	
	□ 风险的危害程度: 请选择危害程度 🗸	
	则将风险项加入户名单	
规则范围:	 全部注机 白空以范围 	
	□ 业务组: 请选择业务组 ▼	
	□ 主机: 请选择主机 P	
	新活建 取21日	

白名单规则说明

规则	说明
条件列表	风险名中包含:用户自定义输入要加入白名单的风险名称 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
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 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: 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

•

白名单规则 12			
条件:所有 Q. 范围:所有 Q. 受影响主机P:所有 Q.			
1项			新建白名单规则
□ 条件	范围	受影响对象	操作
□ 危害程度为-抵危	全部主机	3	× i

• 删除白名单规则

名单	规则	_	
514 : A	新有 Q	范围:所有 Q	受影响主机IP:所有 Q
1项			
	条件		
	危害程度	€为:低危	

3.3 入侵检测

通用操作描述,以暴力破解页面为例:

暴力破	解						
6 溪 月 如	时监控主机上发生的 1户可以查看并处理制 1果来源 IP 处于非解	的爆破行为,并发送通知,同时 重力破解事件,也可以对暴力感 封成功的状态中,则无法加入(提供對標準破末調P的能力。 (1) 均將從自动對學机制和服务设置,並行配到 自名单,请格來源 IP 解封成功后再加入自	Ē. 3名单。	2		×
服务类	型:全部 ▼ 主	博学状态:全部 ▼ 时间区	⊠间:全部 ▼ 业务组:全部 ▼	攻击来源:全部 Q 5	ē\$ ▼	(3 4
33 IJ	٦						服务设置 查看白名单 :
	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	
	SSHD	2019-04-16 04:30:49	193.201.224.82 (乌克兰)	• 172.17.0.17	⊗ 3	解释出于	
	SSHD	2019-04-15 20:10:19	219.146.152.154 (中国,	• 172.17.0.17	⊘ 1	解释主节	6
	SSHD	2019-04-15 19:50:13	104.131.184.67 (美国)	• 172.17.0.17	⊘ 3	育样建立	6
	SSHD	2019-04-15 14:28:49	211.206.101.113 (韩国)	• 172.17.0.17	© 2	解封	6 8

- 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;

业务组:所有 ¥ 时间区间:所有 ¥ 服务类型:所有 ¥ 封停状态:所有 ¥ 攻击来源:所有 Q 攻击目标:所有 Q 更多 ¥

- 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 Ⅲ,可设置显示列,控制列表中的数据显示/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。

入侵总览	业资组 ▼ 2019-03-20-2019-04-19 ▼ 查找主机
数据总筑 2.83% 反动主机出比 - 夏双立主机:4 - 王明母政:106 - 世間句政.61	告偿时间分布 []
受攻击影响主机TOP5 192.168.20616.1 172.17.0.17 2.47 192.168.30.169 2.4	実时協設 第編集多 2019-04-18 11-51-10 ・ 気程電費・主規 192.168.30.169 渡伊 192.168.30.1 (周越岡) 以账号24昇増営量 2019-04-17 102-142 の 反第5-661 半年期 192.168.30.169 波生反第5-661, 運転目标为192.168.30.151,4444 2019-04-17100721 ・ 気報管理・主規 192.168.30.169 微中 192.168.30.1 (周城岡) 以账号24月増営集 2019-04-161724611 ・ 気報管理・主規 172(17)-017 後中 59.111.198.102 (浙江市州) 以账号root异常管集
入侵事件分布	 2019-04-16 17:26:45 2019-04-16 17:26:45 2019-04-16 17:26:46 2019-04-16 17:26:46 2019-04-16 17:26:46 2019-04-16 17:26:47 2019-04-16 17:26:45 2019-04-16 17:16:40 2019-04-16 17:16:4
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。

暴力破解							
● 实时监控主机上发生的曝暖行为,并发送通知,同时提供封停爆成实施P的能力。 用户可以查考并经理等力能转事件,也可以对基力能转弯,自动封停,指制用,服务设置,进行适置。 如果实语,P处于非斜封成功的状态中,则无法加入自各单, 能将实语,P 解封成功后再加入自各单。							
服务类型:全部 🔻	封停状态:全部 ▼ 时间	区间:全部 ▼ 业务组:全部 ▼	攻击来源:全部 Q	更多 🔻			
33 项						服务设置 查看白名单 :	
□ 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	
SSHD	2019-04-16 04:30:49	193.201.224.82 (乌克兰)	• 172.17.0.17	⊘ 3	解封	6	
SSHD	2019-04-15 20:10:19	219.146.152.154 (中国,	• 172.17.0.17	⊘ 1	解封	6 🖻	
SSHD	2019-04-15 19:50:13	104.131.184.67 (美国)	• 172.17.0.17	⊘ 3	解制	6	

手动解封按钮 🏾 🕏

手动封停按钮 🌀

加入白名单按钮 尾

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 诺钮,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<sup>③ 3</sup> 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	ᇢ 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	ᇢ 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
2010 02 11		
		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
	VSFTPD	安全FTP服务
	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

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	
	O 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

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 1					
攻击来源:所有 Q 攻击使用账号:	:所有 Q 范围:所有 Q				
2 项					加建白名单规则
□ 200	攻击来源	攻击时间	攻击使用弊号	受影响对众	操作 III
 10.44.188.101 	攻击来源 140.205.201.32	政士6月间 	攻立使用账号 	受影响过众 0	現在 III

• 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。

白名单规则列表					
攻击京源: 所有 Q 攻击使用账号: A	新有の、「加固・新有の」				
2 顷					新建白名華規則
0 58					
1814	取击米32	18(日前1月)	20日間10日10日10日	登録時対機	题作 III
10.44.188.101	取击来32			5 4 4 4 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5	

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。

主机配	雪枪刻 14									
8 检	测各联务在主机上的配置情况,Ag	gent将根据检测的情况自适	应地监控服务当前配置的复	録日志、若修改了主机服务	治配置,则需重启对应的A	gent来获取最新的配置情况	2.			×
SSHD	VSFTPD									
日志監護	20次る:全部 🍸 封停:全部	▼ 业务组:全部 ▼	主们P:全部 Q	主机名:全部 Q						
1 项									重新检测 配置说明	:
	主机IP	主机名	业务组	置名访问	本地访问	虚拟用户	封停	日志监控状态	登录日志路径	Ш
	• 192.168.192.165	Ubuntu14-2	未分组主机	不允许	允许	启用	不允许	正常监控	/var/log/vsftpd.log	

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;

暴力破	解							
1日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	● 菜时试控土机上发生的爆破行为,并发送滤和,同时提供封等爆破束油P的能力。 用户可以查查并处理最力级解事件,也可以对最力级解的自动封夺,机构和 医务役置 进行配置。 如果来源:P 处于非解射或动的状态中,则无法加入自各单,当将来源:P 解射成边后再加入自各单。							
服务类	型:全部 🔻	封停状态:全部 🔻 时间区	间:全部 ▼ 业务组:全部 ▼	攻击来源:全部 Q	更多 ▼			
< 2	/ 240 项						加入白名单 导出	
	服务类型	最近攻击时间	攻击来源	攻击目标	黑计攻击次数	封停状态	操作 Ш	
	SSHD	2019-04-18 08:01:57	142.93.83.136 (加拿大)	• 172.16.0.4	⊘ 2	未处理	6 R	
	SSHD	2019-04-17 20:06:41	193.112.125.195 (英国)	• 172.16.0.4	S 13854	封停	6	
	SSHD	2019-04-17 09:11:43	193.201.224.158(乌克兰…	• 172.16.0.4	S 397	未处理	6	

全部导出:单击 法钮选择"全部导出"。

暴力破解						
实时监控主机上发生 用户可以宣看并处理 如果来源IP处于非端	的想破行为,并发送通知,同时 暴力成解事件,也可以对暴力缓 ¥封成功的状态中,则无法加入;	排供封停爆破来源IP的能力。 設解的 自动封停 机制和 服务设置 进行配置 白名单,请将来源 IP 解封成功后再加入白线	5单.			×
服务类型:全部 ▼	封停状态:全部 ▼ 时间区	図问:全部 ▼ 业务组:全部 ▼	攻击来源:全部 Q)	£\$ ▼		
240 项						服务设置查:自动封停设置
□ 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 主机配置检测
SSHD	2019-04-18 08:01:57	142.93.83.136 (加拿大)	• 172.16.0.4	© 2	未处理	全部导出
SSHD	2019-04-17 20:06:41	193.112.125.195 (英国)	• 172.16.0.4	S 13854	封停	9
SSHD	2019-04-17 09:11:43	193.201.224.158(乌克兰	• 172.16.0.4	S 397	未处理	6 8

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。

异常登录									
 ● 素別協控主机上发生的异常登录行为。例如非常用制向登录、非常用地会登录等异常登录、开发送邮件通知、 用户可以置着这些异常登录单件、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吸认为是异常登录行为。 									
异带登录类型:全部 ▼ 2019.04.18 ~ 20	19.04.18 🗙 业务组:全部 🔻	主机IP:全部 Q 登录账号:	全部 Q 更多 ▼						
1 项				正常登录规则设置 告警设计	a :				
□ 时间	主机IP	登录派号	来题P	登录区域	Ш				
2019-04-18 11:51:10	• 192.168.30.169	zk	192.168.30.1	周域网					

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。

正常登录规则 1						
登录区域:全部 Q 登录IP:全部	Q 范围:全部 Q 登録	8账号:全部 Q				
6 项						新建正常登录规则
□ 范国	豐豪IP	登录区域	登录时间	登录账号	受影响刘彖	操作 III
□ 全部主机	10.10.10.1-10.10.10.10				查看详肯	/ i
□ 全部主机	123.123.123.123		07:00-10:00(周日,周二,		宣君详情	× 1
hao.yan	自定义内网ip组				查看详肯	/ 1

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
	□ 登录区域:	请设置登录区域
	□ 登录账号:	<mark>₩ 三</mark> 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: 谱	选择业务组 ▼
	□ 主机: 误	选择主机IP
描:老.	田白"涼子"王2019-04	19年7年4月11日
1田12:	出广 洪示 于2019-04	10前注印正帝豆来规则
	创建取消	

正常登录规则说明

规则类型	说明
规则的条	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。
件列表	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;
	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;
	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;
	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
	λ_{\circ}
规则的适	规则范围是指以上条件的适用范围。
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

• 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。

正常登	录规则 1							
登录区	城:全部 Q 登录IP:全部 (Q 范围:全部 Q 登录)	张号:全部 Q					
6 项							新建正常	假就氛带
	范围	登录IP	登录区域	登录时间	登录账号	受影响对象	操作	ш
	全部主机	10.10.10.1-10.10.10.10				重看详情	1	î.
	全部主机	123.123.123.123		07:00-10:00(周日,周二,		查看详情	1	ĩ
	hao.yan	自定义内网ip组				查看详情	1	î

• 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。

正常登录规则 1

登录区	城:全部 Q 登录IP:全部 (Q. 范国:全部 Q. 登录	账号:全部 Q					
6项							新建正常登	录规则
	范围	登录IP	登录区域	登录时间	号洲乐篮	受影响对象	操作	111
	全部主机	10.10.10.1-10.10.10.10				查看详情	/	1
-								-
	全部主机	123.123.123.123		07:00-10:00(周日,周二,		直看详情	/	ii 👘
_		de administrativa da como das				-		-
	hao.yan	自定义内网ip组				查看详情	/	

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。

告警设置	24 	
	功能项	描述
	内网告警	启用后对判定为内网IP的异常登录行为进行上报并通知
		确定

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;

异常登3	2									
6 实 用	● 实时监验主机上发生的异常管果行为。例如非常用时间管果。非常用线点管果等异常包裹,并发送和伴送机。 用户可以直看这些异常登录事件。也可以是正常整要无规则规定都些为正常的登录行为。正常差录分的行为将被认为是异常登录行为。									
异常登录	20	019.04.18 ~ 2019.04.18	3 × 业务	组:全部 ▼	主机P:全部 Q	登录账号:全部 Q	更多 🔻			
< 1/	1项								今出	
~	时间		主机IP		登录账号		来源IP	登录区域	Ш	
	2019-04-18 11:51:10		• 192.168.30	0.169	zk		192.168.30.1	层域网		

全部导出:单击 法钮选择"全部导出"。

异常登录								
 ● 实时监控主机上发生的异常意识行为。例如非常用时间登录、非常用地点登录等异常意识、并没送邮件通知。 用户可以直看这些异常登录审件,也可说真正操业未规则规定都些为正常的登录行为,正常登录外的行为将嵌认为是异常登录行为。 								
异常登录美型:全部 ▼ 2019.04.18~2019	04.18 🗙 业务组:全部 🔻	主机P:全部 Q 登录账号:全部 (Q 更多 ▼					
1 项				正常登录规则设置主机器	紀置检測			
口 时间	主机P	登录账号	来源IP	受录区域 全部	3 出			
2019-04-18 11:51:10	• 192.168.30.169	zk	192.168.30.1	尾城网				

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。

反弹sh	ell									
6 实	◎ 实时监控主机上所有利用Shell进行反应连接的行为。当有反问连接发生时,系统将发送邮件调机,用户可以查着并处理这些反弹事件。									
连接进	呈:全部 ▼ 发现时间:全部 ▼	业务组:全部 🔻 主机名:全	部 Q 蹦口:全部 Q 更多 🔻							
1项						告警设置	:			
	发现时间	主机IP	连接进程	目标主机端口	操作		ш			
	2019-03-21 18:56:31	• 192.168.252.134	bash	192.168.252.136:1234	查看详情		:			

3.3.4.1 查看详情

1

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 目标主机: 192.168.30.151 标准I/O信息:	发现时间: 2019-04-18 12:11:32 目标端口: 4444
连接进程信息	
连接进程: python(20266) 进程路径: /usr/bin/python2.7 父进程: bash(3349) 进程树:	运行用户: zk 用户所属组: zk 父进程路径: /bin/bash
systemd(1) \rightarrow sshd(2653) \rightarrow sshd(273) 0266) \rightarrow sh(20299)	$(39) \rightarrow sh(3229) \rightarrow bash(3349) \rightarrow python(2)$
	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。

连接进程:所	病 Q 范围: 新有 Q	目标主机:所有 Q. 第口:所有 (λ			
2 项						新建白名单规则
口范	10	进程树	连接进程	目标主机	受影响记录	漫作 三日
0 10	.104.11.223			47.94.244.178:4444	0	/ 1
0 10	1.8.8.8			124.53.128.76:3303	0	/ î

• 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。

所建规则			
名称	请输入规则名称		
条件列表:	□ 连接进程:	请选择连接进程	*
	□ 进程树:	请填写进程树,以英文逗号隔开,例如:init,watchdog,sh	
	□ 目标主机:	请输入目标主机。可多选 添加	
	目标端口:	请添加目标3端口 添加	
使用范围:	● 全部主机		
	O 自定义范围		
	□ 业务组:	请选择业务组	
	□ 主机:	请选择主机IP	
a++1-0	m.h. #h=# = 204	8 10 70 Februar M	

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,条件之间为"与"关系。
	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。
	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。
	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。
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 化					
连续进程:所有 Q 范围:所有	Q 目标主机:所有 Q 調口:所有 Q				
2 项					新建白色单规则
□ 范围	进程时	连接课程	目标主机:諾口	受影响记录	提作 III
10.104.11.223	**		47.94.244.178:4444	0	/ 1
10.8.8.8	-		124.53.128.76:3303	0	/ 1

• 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。

白名单规则 1					
连接退程:所有 Q 范围:所有 Q	目标主机:所有 Q 論□:所有 Q				
2 项					新建白名星规则
口 范围	进程间	连接进程	目标主机器口	反影响记录	股件 III
□ 10.104.11.223					
			47.94.244.178.4444	Б	/ =

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。

告警设置	H	
	功能项	描述
	内网告警	启用后对目标IP为内网IP的反弹shell行为进行上报并通
		确定

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;

反弾sh	ell								
● 疾	③ 实时监控主机上所有利用Shell进行反应连接的行为。当有反向连接发生时,系统将发送却件研究,用户可以查着并处理这些反弹事件。							×	
连接进	程:全部 ▼	发现时间:全部 🔻	业务组:全部 ▼	主机名:全部 Q	端口:全部 Q	更多 🔻			
< 1,	/1项								寺出
	发现时间		主机IP	连接	进程		目标主机端口	線作	ш
	2019-03-21 18:56:31		192.168.252	2.134 bash			192.168.252.136:1234	查若详情	:

全部导出:单击 法钮选择"全部导出"。

反弹sh	ell					
8 🕸	时监控主机上所有利用Shell进行反向连接的行	为。当有反向连接发生时,系统将	发送邮件通知,用户可以查看并处理这些反弹手	神.		×
连接进	2:全部 ▼ 发现时间:全部 ▼ 业	务组:全部 ▼ 主机名:全	部 Q 端口:全部 Q 更多 🔻			
1 项						宣看白名单
	发现时间	主机IP	连接进程	日标主机、端口	操作	全部导出
	2019-03-21 18:56:31	• 192.168.252.134	bash	192.168.252.136:1234	直看详情	:

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。

本地提权

	6							
ि ज	3时记录用户以低权限进 3提权行为很有可能是黑	驻入主机,之后通过某种行为获得高权 R客的网络攻击行为,系统将发送邮件i	R的事件。 副知,用户可以查看并处理这些社	是权事件。				×
业务组	:全部 🔻 发现时	揃:全部 ▼ 主机P:全部 Q	提权进程:全部 Q	提权用户:全部 Q				
29 Ij	Ð						白名	单规则
	发现时间	主机IP	提权进程	提权用户	父进程	父进程所属用户	操作	ш
	2018-10-25 17:11:59	I92.168.30.148	sh	root	sh	test	查看详情	加入白名单
	2018-10-25 17:01:48	192.168.30.136	su	test	dcow	test	查看详情	加入白名单
	2018-10-23 17:08:25	192.168.30.148	sh	root	sh	test	查看详情	加入白名单
	2018-10-18 18:41:01	192.168.30.136	su	qt	dcow	qt	查看详情	加入白名单
	2018-10-15 23:31:28	192.168.30.158	2.6.18-194	root	bash	test	查看详情	加入白名单
	2018-10-10 14:38:53	I92.168.30.136	su	test	dcow	test	查看详情	加入白名单
	2018-10-10 14:37:36	192.168.30.136	su	test	dcow	test	查看详情	加入白名单
	2018-10-10 14:37:28	I92.168.30.136	su	test	dcow	test	查看详情	加入白名单

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。

白名単	规则 🐔					
范围:1	全部 Q 提权进程:全部 Q					
2 项						新建规则
	范围	操权进程	是否为带s权限的进程	受影响对象	操作	
	192.168.192.20	sh	是	査 者详病	编辑	删除
	10.0.2.15	avahi-autoipd	좀	查看详情	编辑	910 :

白名单规则设置 1	
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。

白名单	规则 1_					
范围:全	治部 Q 提权进程:全部 Q					
2 项					1	新建规则
	70/80	操权进程	是否为带s权限的进程	受影响对象	操作	ш
	192.168.192.20	sh	是	查看详情	编辑	删除
	10.0.2.15	avahi-autoipd	Æ	查看详情	编辑	80 R

• 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。

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。

白名单	规则 🐀				
范围::	全部 Q 提权进程:全部 Q				
2 项					新建规则
	70.00	提权进程	是否为带s权限的进程	受影响对象	操作 III
	192.168.192.20	sh	是	查看详情	编辑 删除
	10.0.2.15	avahi-autoipd	否	查看洋情	编辑 删除

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;

I	本地提	权						
	11:95-03	:所有 〒 223	1211月:新有 Y 主机P:8	F# Q 透松出标:所有 Q	勝权用户:新有 Q			
	< 1/	/1项						加入印名帝 寻出
	~	发现时间	主机IP	提权进程	爆役用户	父进程	父进程所属用户	操作
	2	2018-04-24 15:21:37	□ 10.0.2.15	bash	root	bash	test	查看订情 加入白紫单

全部导出:单击 诺按钮选择"全部导出"。

本地語	叔						
196	:所有 🍸	发现时间:所有 Y	主机 P: 新有 Q 提权进程:	新有 Q 提択用户:所有 Q			
1 琐							白名《金田寺出
	发现时间	主机IP	提权进程	提权用户	父进程	父进程所属用户	i要作 III
	2018-04-24 15:21:37	□ 10.0.2.15	bash	root	bash	test	查看详情 加入白名单

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。

后门检测							
● 通过实时监控发现各主机创建的进程是否包含后门文件,通过定期扫描关键路径发现Rootkit、Bootkit和其他后门监	2月• ×						
业务组:全部 ▼ 可倍度:全部 ▼ 后门类型:全部 ▼	• •						
25 项	全部号出 重新检测 修复历史 更多 -						
□ 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.ztree. 其对应运行进程: ps ●	◎ 192.168.105 2019-04-10 衰者详情 下载 10.06-18						
■ LINUX/Setag 发现LINUX/Setag.ztrec, 其对应运行进程: ashd ●	● 192.168.105 ● 2019-04-10 支電導情 下載 10.05:18 · · · · · · · · · · · · · · · · · · ·						
■ LINUX/Setag 发现LINUX/Setag.ztrec. 其对应运行进程: getty ●	◎ 192.168.105 2019-04-10 或者评情 下载 10.05:18 · · · · · · · · · · · · · · · · · · ·						
□ ● LINUX/Setag 发现LINUX/Setag.ztrec,其对应运行进程: ps ●	◎ 192.168.105 2019-04-10 立者详情 下載 10.05:18 · · · · · · · · · · · · · · · · · · ·						
■ Pootkit 系统检测ssh命令可抗行文件中含有*^/bin/*.sh\$*内容,请尽快确认	● 192.168.105 2019-03-07 或者详情 下歌 03.40.47 · · · · · · · · · · · · · · · · · · ·						
□ ● Rootkit 系统检测ssh命令可执行文件中含有*^/birv.*.sh\$*内容,请尽快确认	■ 192.168.105 2019-03-07 查看详情 下載 03:40:47 ***						

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 的数据进行比对,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;

入侵	检测					хус 🚨	- 4
一后门	〕检测						
0	通过实时监控发现各主机创建的进行	程是否包含后门文件,通过定期扫描关键路径发现Rootkit、Bootkit和其他后门应用	₽.				×
11:9	6组:全部 ▼ 可信度:全部	▼ 后门类型:全部 ▼ 受感染主机:全部 ▼ 发现时间:全部 ▼	• •••				
Ē	1选 2/25 项				导出 加入自	3名单	
C] 后门类型	说明	受感染主机	发现时间	操作		ľģ
~	LINUX/Setag.ztrec	发现LINUX/Setag.ztrec,其对应运行选程: ps 💿	192.168.105.142	2019-04-10 10:06:18	查看详情 下非	ę	
	LINUX/Setag.ztrec	发现LINUX/Setag.ztrec,其对应运行选程:.sshd 💿	192.168.105.142	2019-04-10 10:05:18	查看详情 下新	R	
C	INUX/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 下都	R	
C	INUX/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	查看洋情 下#	£	
C] • 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 下非	ę	
] • 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 下非	ę	

全部导出:单击 诺按钮选择"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P:全部 Q	更多 💌		
32 项				Ŧ	修复记录
□ 后门类	2 说明	被感染主机IP	发现时间	操作	全部导出
Roc	kit 通过检测strings命令成功后,利用	用strings 및 192.168.192.111	2018-08-03 03:31:14	详情 加入白名单	宣有日名甲
Roc	kit 通过检测strings命令成功后,利用	Ħstrings 및 192.168.29.131	2018-08-15 03:32:56	详情 加入白名单	
Roc	kit 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	

3.3.6.3 查看白名单

单击 ⁱⁱ 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。

检查"/bin/chsh"命令	192.168.192.119	ĩ
检查"/bin/tar"命令	192.168.192.20	ĩ
检查"/bin/tar"命令	10.0.2.15	Ĩ
检查"/usr/bin/chsh"命令	192.168.19.128	Ĩ
检查"/usr/bin/chsh"命令	192.168.197.27	Î

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。

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 Q 更多 ▼	
1页	
□ 友報時回 「「「「東雪」「「東雪」」「「「東雪」」「「「「「」」「「「」」「「「」」「「	
□ 2018-09-12 2018-10-29 17.27.07 10.41:90 ● Rootkit 系统检查sh命令可执行文件 □ 192.168.192.203 直看详情	

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。

翰认 LINUX/Setag.ztrec ▲						
基本信息 质染主机: 192.168.105.142 命中规则: 1 对应文件: /bin/ps		发现时间: 运行进程: SHA256:	2019-04-10 10:06:18 ps b743c1c5960107a8c45f9dab4f234e646e	e0003b5771b8f8440	14436717171 toe	
检测说明 静态信息 进程信息						
检测库 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/S	Setag.ztreo		删除文件	2018-08-23 00:00:00	
翰认 LINUX/Setag.ztrec						
2 - M -						
新今山歌 感染主机: 192.168.105.142 命中规则: 1 对应文件: /bin/ps	:	发现时间: 运行进程: SHA256:	2019-04-10 10:06:18 ps b743c1c5960107a8c45f9dab4f234a646ee	0003b5771b8f84401	44357f7f710e	
检测说明 静态信息 进程信息						
文件基本書 regular file 文件表示 regular file 文件技巧 755 文什大小 1.17MB 文什大小 1.17MB 文件大乐调门户 red 文件大乐调门户 red 文件大乐调门户 red 文件大乐调门户 red 文件大乐调门户 red 文件大小小 red 文学大小小 red 文学大小 red 文学大小 red 文学大小 red 文学大小 red 文学・ red 资学、 red 资学、 red <tr< td=""></tr<>						
逐本信息 感染主机:192.168.105.142 命中规则:1 对应文件:/bin/ps		发现时问: 运行进程: SHA256:	2019-04-10 10:06:18 ps b743c1c5960107a8c45f9dab4f234a646ee	v0003b5771bBfB440	144357f7f71ce	
检测说明 静态信息 进程信息						
基本信息 父进程: bash 父进程路位: /bin/bash 进程启动用户: root 进程路位: /bin/pa 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。

侵检测				xy	c 👤
Veb后门					
通过检测主机We 提供实时检测和 白名单有两种设置	b目灵下的文件內容,发现是否存在有Web匠门,并对发现的后门进行备誉通知。 立即检查的方式未发现后门,并支持多种检测引擎。用户可以查看和处理发现的We 置方式:一种是于响加入白名单,这是以文件 MDS 做规则进行过滤:二是创建白剑	后门,还能够查看Web.后门的具体文件信息并下就后门3 始规则,如果有高级规则设置需求诱使用这种方法。	文件。		>
▶务组:全部 🔻	可信度:全部 ▼ 后门类型:全部 ▼ 文件名:全部 ▼ 受感3	Ε机:全部 ▼			
12 项			全部导出	开始扫描 更多	÷
□ 后门类型	文件名	文件修改时间 受感染主机	发现时间	操作	I
□ • 代码执行	/var/www/html/wordpress/webtest/shell.php	2019-03-21 15:16:06 • 192.168.1	05 2019-03-21 15:16:08	详情	
 代码执行 	/var/www/html/wordpress/webtest/shell02.php	2019-03-21 15:12:01 0 192.168.1	05 2019-03-21 14:59:37	详情	
 代码执行 	/var/www/html/wordpress/webtest/test00.php	2019-03-20 10:29:56 • 192.168.1	05 2019-03-20 10:29:58	详情	
 代码执行 	/var/www/html/wordpress/webtest/webshell.php	2019-03-18 15:42:27	05 2019-03-18 15:46:03	详情 ***	
 系统执行 	/opt/tomcat/webapps/webtest/test05.jsp	2019-03-16 11:18:47 • 192.168.1	05 2019-03-18 15:14:33	详情	
 系统执行 	/opt/tomcat/webapps/webtest/test04.jsp	2019-03-16 10:57:34 0 192.168.1	05 2019-03-18 15:14:33	详情	
 系統执行 	/opt/tomcat/webapps/webtest/test02.jsp	2019-03-15 19:31:45 0 192.168.1	05 2019-03-15 19:33:58	详情 +++	
 代码执行 	/opt/tomcat/webapps/webtest/test01.jsp	2019-03-15 19:06:06 0 192.168.1	2019-03-15 19:07:48	详情	
 特性后门 	/var/www/html/wordpress/webtest/hello01.php	2019-03-15 0 192.168.1	05 2019-03-15	详情	

开始扫描按钮:即用户主动对单独该项进行扫描。

点击 ⁱ 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

功能设置列表	
是否开启	功能名
	Web后门动态监控 📀
	模式分析引擎检测
	取消 确定

3.3.7.2 查看白名单

白各单规则 •_			
規則内容: 全部 Q 使用范間: 全部 Q			
2 项			新建白名单规则
ALTO PYEF	范围	受影响对象	操作 Ш
□ 文件	全部主机	宣看详情	/ i
□ 文件MD5:f9d7df915d369e41c02acd8cb686544b	192.168.2.172	查看详情	/ i

• 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	
	O 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 	
	O 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	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。
	• 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。
	• 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	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。
	• 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。

修复记	录 1_								
首次发	现时间:全部 ▼	修复时间:全部 🔻	类型:全部 🔻	业务组:全部 ▼	主机IP:全部 Q 更多 ▼				
20 Ij	页								
	首次发现时间	修复时间	类型	主机IP	文件名	说明	域名	操作	ш
	2018-10-22 18:29:23	2018-10-22 18:29:41	代码执行	₽ 192.168.2.13	5 /var/www/html/web	eval代码执行	www.example.com	B	
	2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	₽ 192.168.2.13	5 /var/www/html/test0	gzdeflate&base	www.example.com	Ð	
	2018-10-15 14:38:56	2018-10-15 14:41:05	代码执行	₽ 192.168.2.13	5 /var/www/html/test0	GLOBALS GET POST	www.example.com	B	
	2018-10-15 14:38:55	2018-10-15 14:41:05	代码执行	₽ 192.168.2.13	5 /var/www/html/test0	间接变量调用	www.example.com	6	

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 法钮选择"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。

自定义目录 1						
监控目录:全部 Q	应用范围:全部 Q					
48 项					新建自定义	【目录
□ 监控目录		最近修改时间	应用范围	状态	操作	ш
/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	❷ 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

ĴĴ	所建自定义目录 1		
	④ 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:	请输入监控目录,支持输入多个,多个以英文逗号隔开	0
	应用范围:	请选择主机IP	
		创建并同步 取消	

• 编辑自定义目录

自定义目录 1				
益控目录:全部 Q 应用范围:全部 Q				
48 项				新建自定义目录
□ 监控目录	最近修改时间	应用范围	状态	38/1° III
/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编編 規印余
/bin	2018-10-24 17:54:19	172.27.0.15	📀 同步成功	城福 删除

▶ 删除自定义目录

自定义目录 11_				
监控目录:全部 Q 应用范围:全部 Q				
48 项				新建自定义目录
□ 监控目录	最近修改时间	应用范围	状态	39.1°F III
/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编辑 预除
/bin	2018-10-24 17:54:19	172.27.0.15	◎ 同步成功	编辑 题除

3.3.7.6 查看详情

Web/后门								
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誓通知。 报供实时检测和立即检查估方式未发更后门,并支持多种检测引擎。用户可以查看和处理发更的Web后门,还能够查看Web后门的具体文件信息并下载后门交件。 白名串有再种设置方式:一种是于动加入白名单,这是以文件 MDS 做规则进行过滤;二是创建白名串规则,如果有离级规划设置票示请使用这种方法。								
业务组:全部 ▼ 可信度:全部 ▼	全部 💌 🚥							
12 项				全部导出	开始扫描	更多 🔻		
□ 后门类型 文件名	文件修改	受感染主机	发现时间	隔离/删除状态	操作	Pè		
● 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			
□ ● 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			
■ ● 已知后() /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。

I MARKETT A CO				
Webja] > 11	3.马执行详情		加入白名单	下载文件
基本信息				
感 欲主机: 17:	2 16 2 188	发现时间: 2019-02-26 14·20·35		
域名:	and the second the second s	可信度: 可疑		
Web后门文件:	/home/yangwu/wu/webshell/monitor/plugin.php	命中规则: 1		
MD5: bb9c95	5148eda27df11628934ac5e3963	SHA256: e83508e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e8	8610c31d	
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为脚本代码进行执行		收起 🔺	
41 42	return Şarr;			
43				
44	function get_plugin(Spluginname) { Sf = file_oet_contents(UC_ROOT,"./plugin/Spluginname/plugin.xml");			
46	include_once UC_ROOT.'./lib/xml.class.php';			
47	return xml_unserialize(\$f);			
49				
50	function get_plugin_by_name(Spluginname) { Sdir = UC_BOOT / /plugin':			
52	\$s = file_get_contents(\$dir.'/'.\$pluginname.'/plugin.xml');			
53 54	return xml_unserialize(\$s, TRUE);			
55	1			
56	function orderby_tabindex(\$arr1) {			
58	sarr2 = array(); st = array();			
【Web后门 → 代	代码执行详情		加人白名单	下载文件
基本信息				
成约金和·47				
SEARCTED ST. 114	2 16 2 188	第四时间· 2019-02-26 14:20:35		
域名:	2.16.2.188	发现时间: 2019-02-26 14:20:35 可信度: 可受		
域名: Web后门文件:	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php	发现时间: 2019-02-26 14:20:35 可信度: 可嗓 命中规则: 1		
域名: Web后门文件: MD5: bb9c95	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148odag27df11628634ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可喻 命中规则: 1 SHA256: e83500e55c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9t	/homs/yangwu/wu/webshell/monitor/plugin.php 1148ede27df11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可聲 命中規则: 1 SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c95	/homs/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中规则: 1 SHA256: e83508e5c252d1b40fe999a704edac9842af3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c96 检测说明	2.16.2.188 /homs/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963 静态信息	发现时间: 2019-02-26 14:20:35 可信度: 可喻 命中规则: 1 SHA256: e83506e6c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9f 检测说明 文件基本详情	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963 静态信息	发现时间: 2019-02-26 14:20:35 可信度: 可疑 命中规则: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8810c31d	
域名: Web后门文件: MD5: bb9c9(检测说明 文件基本详情 文件类	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963 静态信息	发现时间: 2019-02-26 14:20:35 可信度: 可疑 命中规则: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9t 检测说明 文件基本详情 文件类 文件场同场	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27d111628934ac5e3963 静心信息 総正: php 現: php	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中规则: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(检测说明 文件基本详情 文件表文件类 文件访问教 文件并	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963 静心信息 総正: php 現: php 現: php 現: php 現: php 現: php 現: php 現: php 現: php	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中規則: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(检测说明 文件基本详情 文件无因尽称 文件开展 文件开展用户 文件开展用户	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中規則: 1 SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(检测说明 文件基本详情 文件形词环 文件形词环 文件形词下 文件所属 文件形词下 文件系	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中规则: 1 SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(检测说明 文件基本详情 文件形词环 文件形词环 文件形词环 文件形词印 文件环题 文件所词印 文件环题 文件环题	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27df11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中规则: 1 SHA256: e83508e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(位演说明 文件基本详情 文件基本详情 文件形词称 文件形词称 文件形词称 文件形词称 文件形词称 文件形词称	2.16.2.188 /homs/yangwu/wu/webshell/monitor/plugin.php 5148edx827df11628934ac5e3963 静念信息 経営: php 現: php 現: php 現: php 現: php 現: php 現: php 現: php 現: php 日:	发现时间: 2019-02-26 14:20:35 可信度: 可能 命中规则: 1 SHA256: e83508e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9f 检测说明 文件基本详情 文件基本详情 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称 文件方词称	2.16.2.188 /homs/yangwu/wu/webshell/monitor/plugin.php 5148edat27df11628834ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可喻 命中规则: 1 SHA256: e83506e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9e9t 检测说明 文件基本详情 文件表现 文件不同和子 文件所属用 文件不同和子 文件所属用 文件不同和子	2.16.2.188 /homs/yangwu/wu/webshall/monitor/plugin.php 5148edat27dt11628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: 可喻 命中规则: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c9(MD5: bb9c9(文件 文件或規制 文件资本详慎 文件方词书 文件开展 文件方词书 文件开展 文件方词书 文件开展 文件方词书 文件所属用 文件方明 文件所属用	2.16.2.188 /homs/yangwu/wu/webshell/monitor/plugin.php 5148edat27d111628934ac5e3963	发现时间: 2019-02-26 14:20:35 可信度: <u>可能</u> 命中規則 1 SHA256: e83500e5c252d1b40fe999a704edac9842at3fed5c46e10b64a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c8t 文件基本详慎 文件基本详慎 文件所属用 文件所属用 文件所属用 文件所属用 文件所属用 文件所属用 文件所属用 文件所属用	2.16.2.188 /homs/yangwu/wu/webshell/monitor/plugin.php 5148edat27d111628934ac5e3963	変現时间: 2019-02-26 14:20:35 可信度: 9% 命中規則: 1 SHA256: e83500e5c252d1b40fe999a704edac9842af3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c8t 他演说眼 文件基本详情 文件态词称 文件亦同称 文件亦同称 文件亦同称 文件亦同称 文件亦同称 文件亦同称 文件亦同称 文件亦同称 文件亦同称	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27d111628934ac5e3963	安現时间: 2019-02-26 14:20:35 可慎度: 可慎度: 可慎度: 可慎度: 可能 和中規則: 1 SHA256: e835006e5c252d1b40fe999a704edac9842ad3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c8t 文件基本详情 文件基本详情 文件表词称 文件表词和 文件系属用 文件系属用 文件系码 文件系码 文件系码 文件系码 文件系列 文件系列 文件系列	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27d111628934ac5e3963	安現时间: 2019-02-26 14:20:35 可慎: 可慎: 可慎: 可慎: 可慎: 可能 和中規則: 1 SHA256: e83500e5c252d1b40fe999a704edac9842ad3fed5c46e10b84a4177e	8610c31d	
域名: Web后门文件: MD5: bb9c8t 文件基本详情 文件基本详情 文件基本详情 文件书码本 文件书码 文件书码 文件书码 文件书码 文件书码 文件书码 文件书码 文件书码	2.16.2.188 /home/yangwu/wu/webshell/monitor/plugin.php 5148eda27d111628934ac5e3963	安現时间: 2019-02-26 14:20:35 可信度: 9% 命中規則: 1 SHA256: e83500e5c252d1b40fe999a704edac9842a/3fed5c46e10b84a4177e	8610c31d	

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。

J疑操	作									
8 9	I 疑操作记录执行的sh	ell命令,您可以对操作进行	"筛选,也可以自定义规则发现可	题操作。当有可疑操作执行时,我们	门将发送邮件通知。				×	
包险程	184程度: 全部 ▼ 単模状态: 全部 ▼ 时间区间: 全部 ▼ 业务组: 全部 ▼ 命令内容: 全部 Q 更多 ▼									
30 Ij	۵									
	操作时间	命中规则	命令内容	操作主机IP	登录用户	의듗硿	审核状态	操作	ш	
	2018-09-06 07:36:11	• nc rule	nc -I 4444	9 192.168.30.155	root	192.168.30.1 (局域网)	⊖ 未审核	B	۵	
	2018-08-09 19:03:12	• nc rule	nc -w -l 1234	10.31.91.192	root	124.204.36.26 (中国北京)	😋 审核通过		U	
	2018-08-09	 nc rule 	nc -vv -l 1234	10.31.91.192	root	124.204.36.26 (中国北京)	日 軍核未通过		0	

3.3.8.1 详情查看

单击 皆钮,可以查看该条命令执行的日志详情

nc -1 4444 命中规则列表 [1] 规则名 危险程度 描述 nc rule • 中危	日志详情 操作主机IP: 192.168.30.15 登录用户: root 执行命令用户: root 实际执行命令进程: sshd 命令内容:	55	操作时间: 2018-09-06 07:36:11 登录IP: 192.168.30.1 (局域网) 执行命令进程: bash 产生命令的登录终端(TTY): pts/2	
规则名 危险程度 描述 nc rule ・中た	nc - 1 4444 命中规则列表 [1]			
	规则名 nc rule	危险程度 中危 	描述	

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。

审计规则配置 自定义规则	t.				
危险程度:全部	▼ 规则名:全部 Q				
85 项					
□ 是否同	用 规则名	危险程度	规则内容	说明	ш
	vipw修改shadow文件	 商范 	^(vipw \/usr\/sbin\/vipw)\s+-+s	通过vipw修改shadow文件, 例: vipw -s	
	利用变量统过执行系统命令	• 高危	^\w+=\\$[']*]\\x20.+[']*]\&\&.+\\$\w+	使用特殊符号统过执行系统命令	

▶ 新建审计规则

用户可以自行配置审计规则,判定可疑操作。

新建审计规则 1			
新建规则			
条件列表:	规则名:	请输入规则名	
	正则表达式:	请输入正则表达式	
	危险程度:	请选择危险程度	*
使用范围:	◉ 全部主机		
	O 自定义范围		
	□ 业务组:	请选择业务组	Ŧ
	□ 主机:	请选择主机IP	
描述:	用户"演示"于2018	-10-29添加该审计规则	
	创建取消		

审计规则说明

规则	说明									
规则条件	审计规则条件内容由以下三个条件组成。									
	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	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。									
	• 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

审计规则配置 1 自定义规则系统规则 危险程度:全部 ▼ 规则招:全部 Q 范围:全部 Q 1 项 新建审计规则 □ 是否启用 规则名 危险程度 正则表达式 范围 修改时间 操作 III 123 2018-09-11 16:51:17 × 1 高危 123 全部主机

▶ 删除审计规则

审计规则	■ 审计规则和置 1 1 由定义规则 系统规则										
危险程度	复:全部 ▼ 规则络:全部	Q 范围:全部 Q									
1 项							新建制	制制则	1		
	是否启用	规则名	危险程度	正则表达式	范围	修改时间	操作		Ш		
		123	 高危 	123	全部主机	2018-09-11 16:51:17	/	Î			

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;

可疑操	作									
8 ia	● 记录主机上执行的shell命令,实时监控被审计规则判断为危险的操作,并发送邮件通知。用户可以监管操作并对操作进行申核,也可以对审计规则的按自己的需求进行配置。 ×									
危险程	度:全部 🔻 👔	申核状态:全部 ▼ 时间区	间:全部 🔻 业务组:全的	8 平 更多 マ						
< 2	/ 14 项						导出 审核通过	审核不通过		
	操作时间	命中规则	命令内容	操作主机P	登录用户	登录IP	审核状态	操作		
	2019-04-12 20:38:54	 330ltstest 	ps aux grep vnc	• 192.168.228.130	root	192.168.228.1 (局域网)	□ 未审核	B 🛡		
	2019-04-12 20:38:30	● test_v3.1.0独	ps aux	• 192.168.228.130	root	192.168.228.1 (局域网)	😄 未审核	B 🛡		
	2019-04-12 19:27:20	● test_v3.1.0 <u>9</u>	ps -A afjgrep *v	• 192.168.228.130	root	192.168.228.1 (局域网)	😄 未审核	B 🛡		
	2019-04-12 19:27:12	• test_v3.1.0独	ps - A aflgrep "	9 192.168.228.130	root	192.168.228.1 (局域网)	😄 末审核	B U		

全部导出:单击 法钮选择"全部导出"。

可疑操	ľF								
8 12	● 记录主机上执行的shell命令,实时监控被审计规则判断为危险的操作,并发送邮件通知。用户可以监查操作并对操作进行审核,也可以对审计规则的按自己的需求进行配置。								
危险程度	衰:全部 ▼	审核状态:全部 ▼ 时间	区间:全部 ▼ 业务组:全	部 🍸 更多 🔻					
14 項	ī							审计规则预置	
	操作时间	命中规则	命令内容	操作主机IP	登录用户	의륫笠	审核状态	环境变量配置	
	2019-04-12 20:38:54	 330ltstest 	ps aux grep vnc	9 192.168.228.130	root	192.168.228.1 (局域网)	😄 未审核	全部停出	
	2019-04-12 20:38:30	● test_v3.1.0独	ps aux	• 192.168.228.130	root	192.168.228.1 (局城网)	😄 未审核	B 🔍	
	2019-04-12 19:27:20	● test v3.1.0驻	ps -A af grep "v	I92.168.228.130	root	192.168.228.1 (局城网)	😑 未审核	B 🛡	

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。

Web命令执行								
发现时间:全部 🔻	执行进程:全部 ▼ 进程命令行:全部 ▼	父进程:全部 ▼	受影响主机:全部 🔻					
66099 项						白名单规则	全部导出	监控管理
□ 发现时间	执行进程	进程命令行		父进程	受影响主机	操作		På
2019-08-08 15:57:24	ifconfig(21256)			php(21250)	•	查看详情	加入白名单	
2019-08-08 15:57:24	ifconfig(21256)			php(21250)	• • •	查看详情	加入白名单	
2019-08-08 15:57:22	ifconfig(21248)			php(21247)	•	查看详情	加入白名单	
2019-08-08 15:57:22	ifconfig(21248)			php(21247)	• 1.11	查看详情	加入白名单	
2019-08-08 15:57:20	ifconfig(21241)			php(21236)	• 1.11	查看详情	加入白名单	
2019-08-08 15:57:20	ifconfig(21241)			php(21236)	• • •	查看详情	加入白名单	
2019-08-08 15:57:17	ifconfig(21222)			php(21211)	• • • • •	查看详情	加入白名单	
2019-08-08 15:57:17	ifconfig(21222)			php(21211)	• •	查看详情	加入白名单	

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。
Web 命令执行

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

()) 进程名:	php(21250)	进程命令行:
		进程用户: root
		进程所属用户组: root
		进程uid: 0
		进程文件路径: /usr/local/qingteng/php/bin/php
		进程文件权限:
\downarrow		进程执行用户: root
(1) 讲程名:	ifconfig(21256)	光田在 太仁,
ALIT LI.	100111g(21200)	
		进程用户· POt
		进程所属用户组: root
		进程uid: 0
		进程文件路径:
		进程文件权限: 0
		进程执行用户: root

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。

关闭

,	监控管理					>
	主机IP:全部 ▼ 监控状态:	:全部 ▼ 业务组:全部 ▼ ₽	为网IP:全部 ▼			
	125 项				关闭监控 开启	自监控
	主机IP	业务组	监控状态	操作		P ₆
	• = • = •		禁用	0		
	• • • • •		禁用	0		
	• •		禁用	0		
			禁用			
			禁用			
		未分组主机	禁用			
		未分组主机	禁用			
		未分组主机	禁用			
		未分组主机	禁用			
			禁用			
		未分组主机	禁用	0		
		± 0.753.15	44 m	~		
						关闭

×

开启监控

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

×

关闭监控

主机范围:	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。

×

新建	白名单规则	Ŋ						
	条件列表:	* 父进程	请输入父进程名称,以严格匹配方式进行匹配;支持输入多个,以英文逗号隔开					
		* 执行进程	请输入执行进程的名称,以严格匹配方式进行匹配;支持输入多 ⁴	卜,以英文逗号隔开				
		执行命令	请输入执行命令,以正则表达式进行匹配(选填)					
	主机范围:	⊙ 全部主材	L					
		○ 业务组	请选择业务组	▼				
		○ 主机	请选择或输入主机IP	▼				

	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。 		

- o 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。

备注: 用户"演示"于2019-08-09添加该白名单

- 应用范围。
 - o 应用范围有三个选择方式:全部主机、业务组、主机。
 - o 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。

113

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。

检查首页		新建检查 更多 🗸
- 基线规则:全部 ▼ 业务组:全部 ▼ 操作系统:全部 ▼ 检查名称:全部 ▼ 主机 P :全部 ▼ 主机 A 称:全部 ▼ …		凭证管理 查看白名单
检查会称 	最后执行时间 2019-04-09 15:20:01	0 2 / 1
eemaa eesaa eesa eesaa eesaa ees	最后执行时间 2019-04-08 14:31:11	0 2 / 1
检查会称 001	最后执行时间 2019-04-08 14:22:30	0 2 / 1

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。

合规基线	CentOS 检	查						×
检查首页	创建时间: 201 执行时间: 201	8-12-21 10:08:12 8-12-21 11:03:32	检查范围 描述: 测	: 全部主机 试基线功能				
	通过率	基线规则	成功主机	最后执行时间	操作			L
centOS 检查	47.7%	中国等保-Centos 7-三级主机安全合规检查	1	2018-12-21 11:03:32	0	Z	Î	
	54.3%	中国等保-Centos 7-二级主机安全合规检查	1	2018-12-21 11:02:42	0	Ľ	Î	I.
	51.8%	CIS Centos 7 Level 2	1	2018-12-21 11:02:42	0	Z	Î	1
	51.3%	CIS Centos 7 Level 1	1	2018-12-21 11:02:42	0	Z	Î	1
								L
								1
							关闭	8

▶ 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。

^{检查会称} 基线检查任务	最后执行时间 2019-04-09 18:30:54	
		开始检查

▶ 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。

^{检查名称} 基线检查任务	最后执行时间 2019-04-09 18:30:54	 〇 2 × 音 941服表
▶ 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。

^{检查省称} 基线检查任务	最后执行时间 2019-04-09 18:30:54) 🖸 🖊 📋
> 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。	
^{长面白彩} 基线检 <u>查任务</u>	最后执行时间 2019-04-09 18:30:54	• 2 / 🔳

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。

检查首页 → CentOS 检查							
中国等保-Centos 7-三级主机安全合规检查						≔	< >
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 查看	47.7% ^{通过率} ①	21 通过项	23 未通过项	0 _{失败项}	
检查项视角 主机视角							
类別:全部 ▼ 检查名称:全部 ▼							
44 项						Ě	注部导出
□ 检查项名			类别	检查结果(通过率)	操作	ľ\$
□ 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不存在			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	

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。

删除

合规基线	检查用户默认的u	mask值是否为0	22				×
┃ 检查首页 > 武汉青藤CentOS基线测试	通过率 🕕	通过项	未通过项	失败项			
安信证券 Linux系统安全配置	100% 主机IP:全部	2 主机名:全部	0 ● 业务组:全部 ● 	0 检查结果:全部 ▼			
最后执行时间: 2019-03-21 10:57:28 检查耗时: 15秒	□ 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	❷ 通过	查看详情	
10本方面の	• 192.16	8.122.1	localhost.localdomain	未分组主机	❷ 通过	查看详情	
 ★別:全部 ▼ 检查名称:全部 ▼ 							
18 项							
□ 检查项名							
□ 检查用户默认的umask值是否为022							
□ 检查是否禁用不必要的系统账户							
□ 检查是否禁止Control+Alt+Delete直接重度							
□ 检查是否禁用使用usb存储设备	已选0/2 加入白名	単					关闭
□ 检查是否配置记录用户上次登录时间							Z KI

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。

合规基线	检查用户默认的umask值	通过 检查用户默认的umask值是否为022 - 安全配置	×
┃ 检查首页 > 武汉青朝 安信证券 Linux;	通过率 0 通过项 100% 2	检查内容 用户默认的umask值为022,不应修改 检查结果,172.31.17.136	
最后执行时间: 2019 检查耗时: 15秒	□ ±机P □ • 172.31.17.136	默认用户umask是022 修复建议 已通过,元需修复	
检查项视角 主 关别:全部 ▼	• 192.168.122.1	检查说明 默认umask确定用产创建的文件的权限。创建文件的用户有权通过chmod命令使他们的文件和目录可被其他人读取。希望他们的文件和目录默认被他人可 用户可以通过在主目录中的标准shell配置文件插入umask命令选择不同的默认umask。 引用信息 翻示引用信息	「读的
18 项			
□ 检查是否禁用不 □ 检查是否禁止Ce			
检查是否禁用使	已选0/2 加入白名单	*	关闭

▶ 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。

检查首页 > 武汉青藤CentOS基线测试						
安信证券 Linux系统安全配置						≔ < >
最后执行时间: 2019-03-21 10:57:28 检查耗时: 15秒	13 _{检查主机}	11 失败主机 ^{宣看}	22.2% ^{通过率} 0	8 通过项	28 _{未通过项}	0 失败项
检查项视角 主机视角						
主机IP:全部 ▼ 主机名:全部 ▼ 业务组:全部 ▼						
2 项						全部导出
□ 主都山 P	业务组			检查结果	(通过率) 操	ife Ita
• 172.31.17.136	未分组主机			-	22.2% 🛓	看详情
• 192.168.122.1	未分组主机			-	22.2%	看详情

3.4.3 新建检查

单击"新建检查"按钮,进入新建检查页面。

检查名称:	输入检查名称		
执行范围:	◎ 全部主机		
	O选择业务组	• •	
	O选择主机 请选择或输入主机IP		
描述:	请输入备注信息		
启用定时检查:	▲ 请输入定时表达式	0	
基线规则 🕕			
选择基线规则:	Q、搜索规则		
	+ 添加基线规则		

▶ 添加主机规则

检查首页 > 新建检查 	
☆ C LiS Level 1 合合信息 CIS Level 1 CIS Level 2	
	vel 1 evel 1 evel 1
○ 造産业务组 (15 Level 2 ○ 造産生約 (15 Level 2 ○ 造産主約 (15 Level 2 ○ 造産主約 (15 Level 2 ○ 造産主約 (15 Level 2 ○ 法様主約 (15 Level 2 ○ (15 Level 2 (15 Level 2	vel 2 vel 2 evel 2 evel 2
編誌: 新聞人会社信息 (申用金村絵畫:) 新聞人会社会社 (中国等定) (日本国等定) (二级王机安全合规检查 二级王机安全合规检查 二级王机安全合规检查 u16
法律基础规则: Q, 世法规则 + 満加基础规则 + 満加基础规则	三级王机安全局领险重 三级王机安全局领险重 16.三级王机安全台局险重

新建检查功能说明

功能	说明
检查名称	输入基线的检查名称
执行范围	全部主机: 主账号可选全部主机, 子账号不可选全部主机。(子账号不显示
	"全部主机"选项)选择业务组:可选择该账号管辖范围内的业务组。选择
	主机:选择该账号管辖范围内的主机 IP,也可手动输入主机 IP
	【说明】需要先选择检查范围后,才能选择基线规则。选择了检查范围后,
	将根据所选主机匹配出适用的应用基线,有多少主机缺少账号授权,并提供
	设置入口。提示例如:您选择的主机中包含20台主机缺少账号授权,点击
	设置。
基线规则	系统将根据所选主机匹配出适用的基线规则。分为系统基线和应用基线两大
	类,每类下又细分为 CIS 和等保基线,基线可多选
	【说明】基线选择后,若为数据库类型应用基线,则提示该规则中是否有需
	要添加账号授权的基线,若有,则提示,例如:该规则中的60个检查项需
	要账号授权
	目前支持的系统基线有: centos6/7 rhe16/7 ubuntu12/14/16
	支持的应用基线有: Apache Apache2 MySQL MongoDB Nginx
定时检查	打开定时检查开关,则可以输入定时表达式,且定时表达式为必填。定时表
	达式为 crontab 格式,点击"创建并执行"时,需要校验该格式是否正确,
	校验规则请参考"任务系统=》新建作业中 crontab 格式"。
	鼠标移动到定时表达式后的 i,则显示定时表达式的输入说明。
	关闭定时检查开关,则不可以输入定时表达式。
描述	输入对该基线的描述。

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	
系统在进行数据库基线等检查时,需提供检 行检查。请输入密码使用该功能	查对象的账号密码方可进
请输入账号密码	
	取消 确定

凭证管理管理的凭证用于对应的应用基线的检测。

检查首页 > 凭证管理					
系统在进行基线检查时,需提供检查对象	的账号密码等信息方可进行检查				×
应用类别	1 项				添加授权
MySQL [1]	□ 用户名	数据库端口	逐用范围	操作	12
WebLogic [0]					
	qingteng@qingteng.cn	82	全部主机	编辑 删除	

▶ 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。

合規基线	添加授权 - MySQL	×
▲ 检查普页 > 凭证管理	* 用户名 :请输入用户名	
系统在进行基线检查时,需提供检查对象的影号密码等信息方可进行检查	在码: 诸输入进码	
应用类别 1 项	数据库编□: 济输入数据库销□	
MySQL[1] WebLogic[0] □ text 82 全部主机	 ・ 法理业务组 第四法子业务组 ・ 法理业务组 第四法子业务组 ・ 法理主机 <u>約法</u>学成金入土ポリア 	* *
		取消 建结合

▶ 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。

应用类别	1项				添加授权
MySQL [1]		数据库端目	通用范围	操作	PA.
WebLogic [0]		50,310+391L		2001-	14
	test test	82	全部主机	编辑 删除	

▶ 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。

应用类别	1项				添加授权
MySQL [1]	□ 用户名	数据库端□	通用范围	操作	P\$
WebLogic [0]	test	82	全部主机	编辑 删除	

3.4.5 查看白名单

单击 ᢧ 按钮,选择"查看白名单",进入"白名单列表"页面。

▲ 检查首页 > 白名单列表			
1项			新建白名单规则
+12 日本 - 12 HA	范围	操作	ľ\$
□ 检查项:检查SSH空闲墓时间隔是否设置 - SSH服务截置(中国等保-Ubuntu 16-二级主机安全合规检查)	全部主机	查看受影响对象编辑	删除

▶ 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

┃ 检查首页 > 白名的	ف列表 ゝ 新建的	日名单规则				
规则信息						
* 检 <u>查</u> 项:			精确检索			
执行范围:	◎ 全部主机					
	0选择业务组	请选择业务组	~			
	○ 选择主机	请选择或输入主机IP	Ψ			
					取消	创建

点击"精确搜索",联动选择检查规则-检查类型-检查项。

合规基线	精确检索	×
▲ 检查首页 > 白名单列表 > 新建白名单规则	* 检查规则:CIS Centos 6 Level 1 ▼	
规则信息	* 检查类型: 请选择检查的基线规则	
* 检查项: 请选择检查项	* 检查项: 调选浮主机. · · · · · · · · · · · · · · · · · · ·	
执行范围: 💿 全部主机		
○ 选择业务组 请选择业务组		
○选择主机 请选择或输入主机IP		
	取消	諚

▶ 查看受影响对象

查看现有规则影响的对象。

合規基线	受影响的检查项列表	×
检查首页 > 白名单列表	基线规则:金部 ▼ 基线检查名:金部 ▼ 主印P:金部 ▼	
1项	基线规则 检查项名 基线检查名 所属主机P 主机名 业务组	
□ 条件	中國等保-Ubuntu 检查SSH空闲超时间 ● 192.168.200.1 ubuntu mfq	
□ 检查项:检查SSH空闲超时间隔悬否设置。SSH服务配置(中国等保-Ubuntu 16-二级主机安全会		

▶ 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。

1项			新建白名单规则
	范围	操作	1%
□ 检查页:检查SH空闲稳时间隔是否设置 - SSH服务配置 (中国等保-Ubuntu 16-二项主机安全合规检查)	全部主机	查看受影响对象 编辑 删	除

▶ 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。

1项		新建白名单规则
□ 魚件	范围	操作
□ 检查项:检查SSH空闲缩时间属是否设置 - SSH服务配置(中国等保-Ubuntu 16-二级主机安全合规检查)	全部主机	查看受影响对象编辑 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;

121.42.182.208主机详	青 1			
主机资产安全风险	入侵事件安全日志		最后更新时间:2018-08-10 09:59:02 更新数:	倨
主机信息	基本信息		母田	
系统账号	主机名: sevck_linux	主机状态: 离线	资产等级:重要资产	
	内网IP: 10.31.91.192	安装时间: 2017-03-28 11:36:30	业务组: sstest	
端口服务	外网IP: 121.42.182.208	最后上线时间: 2018-08-08 16:22:38	标签: server	
17-C1#49	操作系统: CentOS release 6.9 (Final),64-bit	最后下线时间: 2018-11-27 17:22:23		
101 J 1211E	内核版本: 2.6.32-696.3.1.el6.x86_64	AgentID: 606906fbdca2f74a		
软件应用	系统启动时间:	Agent版本: 3.0.3-3.30.0-RC-Debug-2018-03-05_	10-26-12-414	
	代理服务器:	Bash插件: 已安装 new 4.1.2		
Web服务				
111 1 AL F	管理信息			
Web站点	负责人: 拉拉	负责人邮箱:zhangsan@qingteng.cn		
Web应用	机房位置: 03-0201	固定资产编号: ah-03		
	备注: server组			
Web框架				
at 100 cm	硬件配置			
<u> </u> 奴()(古)年	生产筒: Alibaba Cloud			
系统安装包	设备型号: Alibaba Cloud ECS			
	序列号: 507b98df-b687-42c3-a6a3-fa150f30c4d3			
Jar包	设备UUID:			
1. 1. 77. 4	内存: 0GB, 使用率: 45.28%			
启动服务	CPU: GenuineIntel 1 Intel(R) Xeon(R) CPU E5-2682 v4 @	D 2.5		
计划任务				
	网卡信息			
环境变量	网卡名称: docker0	网卡名称: eth1	网卡名称: ethO	
	MAC地址: f2:c4:d8:75:a3:63	MAC地址: 00:16:3e:05:3d:48	MAC地址: 00:16:3e:08:36:26	
内核模块	IPv4: 192.168.42.1	IPv4: 121.42.182.208	IPv4: 10.31.91.192	
	IPv6:	IPv6:	IPv6:	

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。

分类导航					数据更新于: 2019-08-09 16:20:01	更新数据
💦 主机管理 5 个 查询	进程管理 5 个 查询		上 账户管理 7 个 查询		器 安装程序与运行应用 3 个 查询	
主机基本信息	运行进程清点		全部账号清点		安装软件清点	
Agent安装查询	进程启动信息		用户组清点		Jar包清点	
高线主机查询)端□ 直 询		账号登录查询	:	运行应用清点	
硬件配置查询	对外端□查询		城账号清点			
Agent代理查询	含监听满口的进程		域账号登录查询			
♥ Web管理 I3 个 否询	▲ 站卢管理 7 个 否询		数据度 2 个 查询		● 启动価値点 2 个 香油	
, mostration and						
Web服务清点	Web站点清点		SQL Server 数据库清点		启动项请点	
Web应用清点	IIS站点清点		Oracle数据库清点		运行服务清点	
Java语言框架请点	Nginx站点清点	:				
	Apache站点清点					
	Tomcatb占点清点					

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。

〉 进程	统计 1				视图 📃 🖵
业务组	:全部 ¥ 进程类型:全部 ¥ 进程名	名:全部 Q			
55 项	Ę				更新数据 全部导出
	进程名	进程说明	进程类型	进程数	ш
	svchost.exe	Windows 服务主进程	后台程序	Q 38	
	csrss.exe	Client Server Runtime Process	后台程序	口 9	
	conhost.exe	控制台窗口主进程	应用程序	中 6	
	winlogon.exe	Windows 登录应用程序	应用程序	口 6	

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。

〉 基本	信息查询 👠					
E	E机在缘状态分布 0.0% 56.7%	● 在线:1 ● 産线:2 ● CFMF10 ● 删除中:0 0	操作系统分布 Windows Server Windows Server (. Windows Server		
主机状	态:全部 ▼ 操作系统:全部 ▼	业务组:全部 🔻 主机	P:全部 Q 更多 ▼ 1			(3) (b)
3 项	5				② 更新数据	全部导出
	主机状态	主机IP	主机名	业务组	操作系统	4
	 ● 在线 	및 192.168.202.128	WIN-PLPKL4TOKFV	阿里云-win	Windows Server 2008 R2 Da	tacenter (b
	 高线 	□ 192.168.202.149	WIN-2G07J71JRMP	未分组主机	Windows Server 2012 R2 Sta	ndard (bui
	 高线 	☐ 172.16.3.201	WIN-2NALM312DAW	未分组主机	Windows Server (R) 2008 Da	tacenter S

- ① 筛选/搜索区:根据不只需要,对列表内容进行筛选;
- ② 更新数据按钮:点击 _{全部异世},手动触发更新当前资产数据;
- ③ 全部导出按钮:点击 ,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

> 离约	主机查询 🚹					
最后右	践时间:全部 ▼ 业务	孫狙:全部 ▼ 主机IP:全部 Q	主机名:全部 Q			
2 项	I				更新数据	全部导出
	最后在线时间	主机IP	主机名	业务组	操作系统	Ш
	2018-09-25 11:02:12	및 172.16.3.201	WIN-2NALM312DAW	未分组主机	Windows Server (R) 200	8 Datacent
	2018-09-17 15:36:51	및 192.168.202.149	WIN-2G07J71JRMP	未分组主机	Windows Server 2012 R	2 Standard





4.1.1.5 Agent 代理查询

> 主材 主机IF	化代理查询 ▲ :全部 Q 代理P:全部 Q				
1 项				更新读	汝据 全部导出
	代理IP		主机数目		Ш
	直连主机		Q 3		
> 没有 操作3	存使用代理服务器的主机 1 6號:全部 ▼ 业务组:全部	▶ ▼ 主机P:金部 Q 主机系:金部 Q			
3 项	ī				全部导出
	主机IP	主机名	业务组	操作系统	Ш
	□ 192.168.202.149	WIN-2G07J71JRMP	未分组主机	Windows Server 2012 R2 Standard (build	9600),64-bit
	□ 192.168.202.128	WIN-PLPKL4TOKFV	阿里云-win	Windows Server 2008 R2 Datacenter (build	d 7600),64-bit
	및 172.16.3.201	WIN-2NALM312DAW	未分组主机	Windows Server (R) 2008 Datacenter Servi	ice 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 1					视图 📃 🖵
业务组	: 全部 ▼ 进程类型: 全部 ▼ 进程名: 全	aff Q				
55 IJ	Φ			更	新数据	全部导出
	进程名	进程说明	进程类型	进程数		Ш
	svchost.exe	Windows 服务主进程	后台程序	Q 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	Ģ 6		
	winlogon.exe	Windows 登录应用程序	应用程序	Ģ 6		

> 进程svchost.exe详情 ▲



> 主机	〕进程统计		视图 🗄
业务组	1:全部 ▼ 主机IP:全部 Q	主机名:全部 Q	
3 项			全部导
	主机IP	井程数	
	및 192.168.202.128	49 66	
	□ 192.168.202.149	40 53	
	및 172.16.3.201	20 50	

> 主机192.168.202.128的进程列表 1

注 44 38 22 11		Copy - State						
进程类	型:全部 🔻 进程名:全部	『 Q 进程说明:全部 Q	进程路径:全部 Q	运行用户:全部 Q 更多	•			9.
66 IJ	ξ							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	III
	6140	cmd.exe	Windows 命令处理程序	应用程序	6.1.7600.16385	C:\Windows\System	Administrator	
	5452	vdsldr.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 🔒				视图 📃 🖵
业务组:全部 🖣	进程类型:全部 ▼ 进程名:全部	Q			
55 项				更新数	据全部导出
□ 进程名		进程说明	进程类型	进程数	Ш
svcho:	texe	Windows 服务主进程	后台程序	₽ 38	
Csrss.e	xe	Client Server Runtime Process	后台程序	모 9	
C conho	st.exe	控制台窗口主进程	应用程序	₽ 6	

> 进程svchost.exe启动信息详情 1

ž	进程版本统计								
	31.6% 34.2%	 6.1.7600.1: 13 6.0.6001.1: 13 6.3.9600.1: 12 							
进程版	本:全部 ▼ 进程启动时间:	全部 ▼ PID:全部 Q	主机IP:全部 Q	主机名:全部 Q	更多 🔻				٩.
38 I	Φ								全部导出
	主机IP	进程启动时间	进程版本	进程路径	运	运行用户	进程启动参数	PID	Ш
	및 192.168.202.149	2018-09-17 12:06:09	6.3.9600.16384	C:\Windows\	System S	YSTEM	C:\Windows\system3	552	

> 主机	运行进程统计 - 启动信息查询	E.	视图
业务组	:全部 ▼ 主机IP:全部 Q	主机条:全部 Q	
3 项			全部
	主机IP	現程数	
	및 192.168.202.128	aa 66	
	192.168.202.149	s3	

> 主机192.168.202.128的进程启动信息 1

1 2 2 1		NORA GOR							
进程启	动时间:全部 🔻	进程名:全部 Q 道	挂程说明:全部 Q 进	辉路径:全部 Q 运行用户:	全部 Q 更多 ▼				٩.
66 I	页							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	ш
	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	1696	java.exe	Java(TM) Platfor	8.0.1810.13	C:\PROGRA~1\Ja	Administrator	C:\PROGRA~1\Java\J	DK18

4.1.2.3 端口查询

资产视角

> │ 端口统计 €		视图 📃 🖵
业务组:全部 Y 第二:全部 Q		
31 项		更新数据 全部导出
□ 朔□ ↑	満口数	Ш
3389	Q 8	
7001	Q 7	
49152	Q 6	

> │ 端口3389详情 1 🖿

端□访问性统计 0.0%	• 内:0 • 外:0 • 未知:8				
业务组:全部 ▼	部 🔻 主机IP:全部 Q	主机名:全部 Q	更多 🔻		٩.
8 项					全部导出
□ 主机IP	端口协议	備口访问性	绑定IP	监听进程 (PID)	Ш
□ □ 192.168.202.149	tcp	「末知」	0.0.0.0	svchost.exe (1564)	

> ±	机端口统计 🚹		40.50 E	: 🖵
业务	9组:全部 ▼ 主机IP:全部	部 Q 主机名:全部 Q		
3	项		全部导致	Ħ
	主机IP	端口数		III
	🖵 192.168.202.128	•€• 44		
	및 192.168.202.149	- ۥ 37		
> ∃	三机192.168.202.128的端口	口列表 1		

端口访问性统计					
15.9% 20% 84.1%	● 内:7 ● 外:0 ● 未刊:37				
第口访问性:全部 ▼ 第口协议:全部 Q	绑定IP:全部 Q 监听进程:全部	Q			٩.
44 项					全部导出
□ 36□	端口协议	端口访问性	绑定IP	监听进程 (PID)	Ш
58956	udp	「末知」	0.0.0.0	QQPCRTP.exe (884)	

4.1.2.4 对外端口查询

业务组:所有 ▼ 第日:所有 Q 主机P:所有 Q 主机S:所有 Q 第日协议:所有 Q 更多 ▼
25 项 数据更新 :
論口 主机P 論口协议 擁超P 监新世程(PID) 目
□ 8098 및172.31.177.178 tcp 0.0.0.0 System (4)
□ 8096 및172.31.177.178 tcp :: System (4)
□ 8092 및172.31.177.178 tcp 0.0.0.0 System (4)
□ 8092 및172.31.177.178 tcp :: System (4)
□ 8081 및192.168.18.133 tcp 0.0.0.0 httpd.exe (1044)
□ 8081 및192.168.18.133 tcp :: http://exe (1044)

4.1.2.5 含监听端口的进程

资产视角

> 含 业务	监听端口的进程统计 1	55 Q.			视图 📃 🖵
14	项			đ	新数据 全部导出
o	进程名	进程说明	进程类型	主机数	ш
0	svchost.exe	Windows 服务主进程	后台程序	Q 17	
	wininit.exe	Windows 启动应用程序	后台程序	Q 3	
	lsass.exe	Local Security Authority Process	后台程序	₽ 3	
	services.exe	服务和控制器应用	后台程序	🖵 3	

> 进程	esvchost.exe监听端口详情	1				
1	进程版本统计	● 61.7600.1:6 ● 6.3.9600.1:6 ● 6.0.6001.1:5				
业务组	1:全部 ▼ 进程版本:全部	▼ PID:全部 Q 主机IP:全部 Q	主机名:全部 Q. 更多 ▼			9.
17 I	页					全部导出
	主机IP	进程版本	进程路径	监听端口列表	PID	Ш
	🖵 192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	[末知] TCP-135	600	
	및 192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	[末知] TCP-49153	788	
	192.168.202.149	6.3.9600.16384	C:\Windows\System32\svchost.exe	(未知) TCP-49154 (未知) UDP-500	824	

>	主机;	含监听端口的进程数 👠						视图 🗮 🖵
	业务组	:全部 🔻 主机IP:全部 Q	主机名:全部 Q					
	3 项							全部导出
		主机IP	进程数					Ш
		192.168.202.128	₩ 16					
		192.168.202.149	aa 11					
>	> │ 主机192.168.202.128的监听端口信息 €							
	进程名:全部 Q 进程説明:全部 Q 进程路径:全部 Q PID:全部 Q							
	16 项	۶.						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	Ш
		4996	TitanAgent.exe	TitanAgent	3.2.2.0	C:\Program Files\TitanA	[末知] TCP-8089	
		4684	360tray.exe	360安全卫士 安全防护中	7.7.3.1631	C:\Program Files (x86)\3	[末知] UDP-3600	
		4392	java.exe	Java(TM) Platform SE bi	8.0.1810.13	C:\PROGRA~1\Java\JDK	内 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 业务组:全部 、	▲ 用户名:全部 C	L					视图 📃 🖵
	6项						更新数据	全部导出
		ž.		账户说明		主机数		ш
	Gues			供来宾访问计算	机或访问域的内置帐户	Q 3		
	Admi	nistrator		管理计算机(域)的	的内置帐户	Q 3		
	flong	test				Q 1		
>	服务Guest	主机运行状态 ▶ み市	• 访察用户:3	账户状态分布	00.0% #用: 3			
	业务组:全部 、	▼ 账户状态:全部 、	▼ 账户类型:全部 ▼	主机IP:全部 Q	用户ID:全部 Q 更多 ▼			4).
	3 项							全部导出
	□ 主机	p	用户ID	所属用户组	账户状态	账户类型	账户主目录	Ш
		92.168.202.149	S-1-5-21-24285765-340	Guests	禁用	访客用户		

> I ±	E 机贝	长号统计 🚹		视图 📰
149	务组:	全部 ▼ 主机IP:全部 Q	主机名: 全部 Q	
3	项			全部导出
	ו	主机IP	账户数	I
	ו	및 192.168.202.128	≜ 5	
	ו	192.168.202.149	1 3	
	ו	172.16.3.201	2 2	

> 主机192.168.202.128的账号列表						
账户继刑公布		账户状本分布				
20.0%	● 标准用户:2 ● 管理员用户:2 ● 访客用户:1	20.0%	0% ● 最用 :	4 1		
业务组:全部 ▼ 账户状态:全部 ▼	▼ 账户类型:全部 ▼	用户名:全部 Q 更多 ▼				9.
5 项						全部导出
□ 用户名	用户ID	所属用户组	账户状态	账户类型	账户主目录	Ш
flong_test	S-1-5-21-2125426864-9	flong-test, Users	启用	标准用户		
flong2	S-1-5-21-2125426864-9	Users	启用	标准用户	C:\Users\flong2	

4.1.3.2 用户组清点

资产视角

>	用户	组统计 1				视图 📃 🖵
	用户组	名:全部 Q				
	32 IJ	Σ			更新数据	全部导出
		用户组名	用户组描述	主机数		Ш
		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,来宾跟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 Q	主机名:全部 Q		
3 项				£
	主机IP		用户列表	
	□ 192.16	58.202.149	WIN-2G07J71JRMP\Guest	
	🖵 192.16	58.202.128	WIN-PLPKL4TOKFV\Guest	
	↓ 172.16	5.3.201	WIN-2NALM312DAW\Guest	

主机视角

> 用户组统计 1		视图 🗮 🖵
业务组:全部 ▼ 主机IP:4	全部 Q. 主机名:全部 Q.	
3 项		全部导出
□ 主机IP	用户组数	Ш
□ □ 192.168.202.128	<u>41</u> 17	
□ □ 192.168.202.149	23	
□ 및 172.16.3.201	24	

> 主	机192.168.202.149的用户组列表 1			
用户	组名:全部 Q			
23	项			全部导出
	用户组名	用户组描述	用户列表	Ш
	WinRMRemoteWMIUsers_	Members of this group can access WMI resources over		
Users		防止用户进行有意或无意的系统范围的更改,但是可以运行大	NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authe	nticated Us
	Replicator	支持域中的文件复制		

4.1.3.3 账号登陆查询

▶₩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 Q	主机名:所有 Q 用户名:所有 Q	账户主目录:所有 Q		
69 Ij	۶.					数据更新
	主机IP	用户名	账户上次登录时间	账户类型	↑ 账户主目录	Ш
	□ 0.0.0.0	Administrator	2018-04-24 22:19:56	管理员用户		
	□ 172.31.177.178	Administrator	2018-04-20 13:32:19	管理员用户		
	□ 10.10.10.15	hack	2018-04-14 19:40:23	管理员用户	⊐ C:\Users\hack	
	□192.168.197.216	test	2018-04-03 02:35:47	标准用户	C:\Users\test	
	□ 169.254.187.69	YPS	2018-04-02 10:04:38	管理员用户	C:\Users\YPS	
	₽192.168.18.135	jary	2018-03-29 11:25:10	管理员用的	⇔ C:\Users\jary	
	□ 10.12.8.181	admin	2018-03-27 18:46:00	管理员用户	⇔ C:\Users\admin	
	🖵 192.168.18.133	Administrator	2018-03-22 14:28:46	管理员用户	C:\Users\Administrator	
	□ 0.0.0.0	admin	2018-03-07 10:49:21	管理员用	≏ C:\Users\admin	
	□0.0.0.0	jk	2018-01-22 13:06:38	管理员用/	≐ C:\Users\jk	
	₽0.0.0.0	Administrator	2017-12-27 18:21:44	管理员用户		

4.1.3.4 域账号清点

〉 域账	号统计				
6 清	点 "城服务器" 中所有城账号,及城管理下的所有主机	1。用户终蹒通过登录"城服务器"中的城账号,可访问有	目同域下管理的主机,获得主机提供的服务。		×
所属域	呂:全部 Q 域服务器IP:全部 Q 主机名:	全部 Q			
0 项					更新数据 全部导出
	域名	域服务器IP	域账户数	操作	ш
	没有账户相关数据				

4.1.3.5 域账号登录查询

> 城账号登录查询 1			
记录访问过"城管理下主机"的所有城账号,并提供城账号登录相关信息。			×
业务组:全部 ▼ 板访问主机P:全部 Q 主机名:全部 Q 所屬城名:全部 Q			
0 项			更新数据 全部导出
□ 被访问主机 P	主机名	最近登录账号	Ш
□ 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	t.							
	账户状态	态:所有 ▼ 上次密码修改时间:	:所有 🝸 账户类型:所有 🍸	主机IP:所有 Q 主机名:)	新有 Q 用户名:所有 Q	更多 🔻				
	10 项	Ĩ							数据更新	-
		主机IP	甩户名	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		Ш
		🖵 192.168.197.216 🏼	admin	启用	2017-06-19 23:39:46	已过期		标准用户		
		9192.168.197.216	Administrator	启用	2017-03-15 14:52:57	已过期	C:\Users\Administrator	管理员用户		
		□ 192.168.197.216	testaaaaaaa	启用	2017-06-19 18:44:38	已过期		标准用户		
		□ 192.168.197.216	user	启用	2017-06-19 18:45:39	已过期		标准用户		
		₽ 192.168.197.149	Administrator	启用	2013-10-01 05:58:31	已过期	C:\Users\Administrator	管理员用户		
		□ 192.168.197.149	test	启用	2013-10-01 07:14:14	已过期		标准用户		
		₽192.168.197.36	Administrator	启用	2009-01-27 02:17:14	已过期	C:\Users\Administrator	管理员用户		
		₽192.168.18.133	Administrator	启用	2013-10-01 05:58:31	已过期	C:\Users\Administrator	管理员用户		
		₽ 192.168.18.133	test	启用	2013-10-01 07:14:14	已过期		标准用户		
		₽ 10.211.55.14	Administrator	启用	2017-01-19	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 1.						
业务组	1:所有 ▼ 主机P:所有 Q	主机名:所有 Q					
22 1	<u>م</u>					数据更新	1
	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		ш
	192.168.197.216	WIN-V65MI2R3R0J	42天		5天		
	©192.168.197.149	WIN-AR79G1VES1A	42天	**	5天		
	□192.168.197.36	WIN-6CLCZAW0GON	42天	022	14天		
	□192.168.106.128	WIN-P2KEDEPH8DJ	27. U		5天		
	⊊192.168.18.135	DESKTOP-QH5LNTS	**		5天		
	□192.168.18.133	WIN-AR79G1VES1A	42天	522 ·	5天		
	□ 192.168.11.160	LAPTOP-82IBIUK2	42天	070	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	\$\$\$(件统计 1 1		408 📃 🖵
业务组	1:所有 ▼ 安徽软件名:所有 Q		
398	项	803	据更新 :
	安装软件名	主机政	Ш
0	Update for Microsoft Office 2013 (KB3039720) 64-Bit Edition	Q 80	
	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Q 15	
	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	₽ 12	
	Google Chrome	₽ 12	
	Security Update for Microsoft Excel 2013 (KB2920753) 64-Bit Edition	Q 10	
	Update for Microsoft Office 2010 (KB2553347) 64-Bit Edition	모 10	
	Mozilla Maintenance Service	Q 10	
	VMware Tools	Ģ 9	
	Update for Microsoft OneDrive for Business (KB3178645) 64-Bit Edition	Q 8	
	Update for Microsoft Visio Viewer 2013 (KB2817301) 64-Bit Edition	Ģ 8	
	Update for Microsoft InfoPath 2013 (KB3114946) 64-Bit Edition	Q 8	

> │ 软件Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161详情 👔 👠



主机视角

> 主机	1软件安装统计 1		视图 😑 🗔
业务组	l:所有 ▼ 主机P:所有 Q	主明名: 所有 Q	
28 1	页		:
	主机IP	安装程序数	111
	₽0.0.0.0	😫 187	
	₽0.0.0.0	✿ 157	
	□ 10.10.10.15	₩ 140	

> 主机192.168.202.1	28的安装软件列表 1					
安装时间分布		软件大小分布				
55.6%	16.7% 9.6% 27.8% 27.8% 9.7天:0 9.73天:5 9.37天:0 9.73天:5 9.30天以上:10	22.2% 50.0 22.2% 5.00	95 0-1MB:9 1-10MB:1 10-100MB:4 100MB-16B:4 100MB-16B:4 1GBULE:0			
业务组:全部 🔻 🕸	件大小:全部 ▼ 安装时间:全部 ▼	安装软件名:全部 Q 更多	•			٩.
18 项						全部导出
安装软件名 安装软件名	安装版本	软件发布者	安装时间	软件大小	安装路径	Ш
Git version 2.1	3.0 2.13.0	The Git Development C	2017-08-21 14:42:11	214.1 MB	C:\Program Files\Git\	

4.1.4.2 Jar 包清点

资产视角

>	Jar包	統计 👠		视图 📃 🖵
	业务组	全部 ▼ 类型:全部 ▼ 包名:全部 Q		
	712 រ	Φ	更新数据	建 全部导出
		包名	主机数	ш
		mina-core-2.0.5.jar	Q 1	
		jboss-interceptors-api_1.1_spec.jar	Q 1	
		jboss-jca.jar	Q 1	
		jaxws-httpserver-httpspi.jar	Q 1	
		bootstrap-1.3.2-core-assets.jar	Q 1	
		jboss-ejb3-proxy-impl.jar	Q 1	

> Ja	r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	ß Q 更多 ▼				
13	页								全部导出
0	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 1

I王机Jar	包統计	1		
类型:全部	T	业务组:全部 ▼	主机IP:全部 Q	主机名:全部 Q
1项				
	主机IP		包数	
	192.168	8.220.135	729	

>	主机192.168.220.135的Jar包详细信息	1

类型::	全部 ▼ 是否可执行:全部	▼ 绝对路径:全	部 Q 版本:全部	Q 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	111
	• 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. 版本: 4.0 绝对路径: C:\Users\adm MD5: b6e6837fed04d 引用情况 进程列表:	0.jar 첫 뒷 iin\Downloads\jboss 4a7bad291caad8756	型: 其他依赖包 译可执行: 否 s-6.1.0.Final\server\default\tmp\vfs\ 6ea	
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

> | 运行应用统计 👠 WB 📃 🖵 运行应用分布 ٠. 业务组:所有 ▼ 应用名:所有 Q 数据更新 10 项 □ 应用名 说明 应用类型 主机数 Ш Chrome Google Chrome 是一款快速、安全且免费的网络浏览器 其它 **Q** 5 U WeChat 微信电脑版 其它 **Q** 4 mysql 数据库 **Q** 4 Mysql是最流行的关系型数据库管理系统 Apache Apache是一个Web服务器软件 Web运维 **Q** 4

其它

Web运维

Q 3

Q 3

> │ 应用IIS详情 1

QQ

IIS

聊天工具

IIS是Internet Information Services的缩写,意为互联网信息…

1 120 131						
KG:	本分布	• 7.5 ; 1 • 8.5 : 1				
业务组:	全部 ▼ 应用版本:全部 ▼	主机IP:全部 Q 主机名:全部 Q	Q 应用安装路径:全部 Q 更多 ▼			٩.
2 项						全部导出
	主机IP	应用版本	应用安装路径	应用配置文件路径	关联进程数	Ш
	및 192.168.202.149	8.5	C:\Windows\System32\svchost.exe		2	

主机视角

▲ 主机运行应用统计		视图 📜
业务组:所有 🔻 主机IP:所有 Q	主机名:所有 Q	
28 项		
□ 主机IP	应用数	I
□ □192.168.11.160	88.6	
□ □ □ 10.10.10.15	88.4	
□ □ 192.168.197.149	88.3	
□ □ 192.168.18.133	88.3	

> 主机192.168.202.149的运行应用列表 1

业务组:全部 🔻	应用版本:全部 ▼ 应用名:全部 Q	应用安装路径:全部 Q 应	立用配置文件路径:全部 Q		
1项					全部导出
□ 应用名	应用版本	应用安装路径	应用配置文件路径	关联进程数	Ш
IIS	8.5	C:\Windows\System32		2	

4.1.5 Web 管理

4.1.5.1 Web 服务清点

资产视角

▶ Web服务 1			视图 📃 🖵
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	
tomcat		Q 1	
🔲 jboss		Q 1	
websphere		Q 1	

> tomcat服务详细信息 1

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	111
192	.168.75.133	7.0.92	C:\Program File	s\Java\jd	C:\Users\admin\Downlo	1	

> | 主机192.168.75.133上tomcat服务关联的进程 1

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页				全部导出
D PID	进程路径	启动用户	进程启动时间	Ш
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 👥			视图 📃 🖵
Webß	済名:全部 ▼ 业务组:全部	▼ 主机P:全部 Q 主机名:全部 Q		
3 项		更 更	新数据	全部导出
	主机IP	Web服务教		Ш
	• 172.16.2.187	1		
	• 192.168.75.133	1		
	• 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
      ●

      □ 主机P
      Web服务名

      Web服务名
      版本

      □ 172.16.2.187
      webghere

      9.0.10
      C:\Program Files\...

      -
      1
```

> | 主机172.16.2.187上websphere服务关联的进程 1

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
PID	进程路径	启动用户	进程启动时间	111
11404	C:\Program Files\IBM\WebSph	er SYSTEM	2019-02-26 10:07:20	

4.1.5.2 Web 应用清点



> Wet	D应用统计 1				视图 📃 🖵
应用名	:全部 Q				
1 项				更新数据	全部导出
	应用名	描述	主机数		111
	Monstra CMS	Monstra CMS是乌克兰软件开发者Sergey Rom	Q 2		

>	Web	应用Monstra CMS统计	±					
	版本:台	全部 🝸 服务类型:全部	3 ▼ 业务组:全部 ▼	主机IP:全部 Q	更多 🔻			
	2项						<u>-</u>	全部导出
		±扣IP	版木	坦悠久	服农举刑	社占博名	虚拟日寻	
	_		/IIXe4e					
		• 192.168.56.1		C:/inetpub/wwwr	lis	*	C:/inetpub/wwwroo	t
		• 192.168.56.1		C:/inetpub/wwwr	IIS	*	C:/inetpub/wwwroo	t

主机视角

>	│ 主机Web应用统计		视图 📃 🖵
	业务组:全部 ▼ 主机P:全部 Q 主机名:全部 Q		
	2 项	I	更新数据 全部导出
	主初いP	应用数	ш
	• 192.168.56.1	## 1	
	• 192.168.56.1	88 1	

> ┃ 主机192.168.56.1Web应用统计 1

版本:	全部 ▼ 服务类型:	全部 ▼ 应用名:	全部 Q 根路径:	全部 Q 更多 ▼				
1 项							오	部导出
	应用名	描述	版本	根路径	服务类型	站点域名	虚拟目录	111
	Monstra CMS	Monstra CMS		C:/inetpub/ww	IIS	*	C:/inetpub/wwwro	ot

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 业务组	框架统计 € :全部 ▼ 框架名:全部 Q		视图 🔚 🖵
23 Ij	页	更新	数据 全部导出
	框架名	主机数	Ш
	Freemarker	Q 1	
	vertx	Q 1	
	spring MVC	Q 1	
	velocity	Q 1	
	zkoss	Q 1	
	shiro	Q 1	

```
> Freemarker服务详细信息
```

Theemarker jjg/si				
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
主机IP	版本	服务类型	关联jar包数	Ш
• 192.168.2	220.135 2.3.13,2.3.19		2	

> 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
□ 主机IP	框架数	Ш
• 192.168.220.135	23	

> | 主机192.168.220.135的Java语言框架详细信息 1

服务类	型:全部 ▼ 框架名:全部 Q				
23 项	Į				全部导出
	框架名	版本	服务类型	关联jar包数	111
	spring	2.5.6.SEC03,3.0.5.RELEASE,4.3.2		4	
	Freemarker	2.3.13,2.3.19		2	
	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

>	Web站点一览 1									
	所有网站遗名[4]	城谷	3站列表 - 所有网站域名							
	• · · · · · · · · · · · · · · · · · · ·									
	dreamstep.co.jp	2	站点端口对外状态		站点协议统计					
	localhost					0.0%				
	www.dreamstep.co.jp		50.0%	50.0%						
			0.0%	● 穴: + ● 内: 0 ● 未知: 4		00.0%	HTTP : 8 HTTPS : 0			
		业务组	:所有 🔻 是否对外:所	有 ▼ 站点协议:所有 ▼	服务类型:所有 ▼	E机P:所有 Q 更多,				٩.
		8 项							数据更新	
			域名	所在主机	站点跳口	是否对外	站点协议	服务类型	站点路径	ш
			*	□ 192.168.197.149	80	未知	HTTP	IIS	C:\inetpub\www.root	
				₽ 192.168.18.133	80	(未)(1)	HTTP	IIS	C:\inetpub\www.root	
			*	₽ 172.31.177.178	8098	所	HTTP	IIS	E:\websites\dreamstepadr	nin
			*	₽ 172.31.177.178	8092	承	HTTP	IIS	E:\websites\dreamstep	
			www.dreamstep.c	₽ 172.31.177.178	80	孙	HTTP	IIS	E:\websites\dreamstep	

4.1.6.2 Web 应用清点

>	Web应用約	充计 1				视图 📃 🖵
	应用名:全部	Q				
	1项				更新数据	全部导出
	□ 应用	洺	描述	主机数		Ш
	word	dpress	WordPress是一种使用PHP语言开发的博客平	口 1		

> | Web应用wordpress统计 1



4.1.6.3 IIS 站点清点

>	IIS站点清点 👠										视图	.
	所有IIS网站域名[3]	站机	新列表 - 所有IIS网站	域名								
	*											
	dreamstep.co.jp	3	品层调口对外状态									
	www.dreamstep.co.jp		33.3%									
			P3 : 0	66.7% 外:	4							
				• A: • 未知	:2							
		是否对	外:所有 ▼ 站	点协议:所有 ▼ 站点程序池桥	2限:所有 ▼ 主	肌P:所有 Q	更多 🔻					٩.
		6 项									数据更新	:
			域名	所在主机	配置站名	站点遡口	是否对外	站点协议	站点应用 程序池	站点程序 池权限	主目录路 径	111
			*	172.31.177.178	dreamstepa	8098	<u></u>	HTTP	dreamstepa	应用池特定	E:\websites\dreams	ste
			*	□172.31.177.178	dreamstep	8092	外	HTTP	dreamstep	应用池特定	E:\websites\dreams	step
			www.dream	₽172.31.177.178	dreamstep	80	外	HTTP	dreamstep	应用池特定	E:\websites\dreams	step
			dreamstep	₽172.31.177.178	dreamstep	80	<u></u>	HTTP	dreamstep	应用池特定	E:\websites\dreams	itep

4.1.6.4 Nginx 站点清点

>	Nginx站点清点 1											视图 🔡	
	所有Nginx网站域名[0]	站点	列表 - 所有Ng	ginx网站域名									
	没有发现站点	是否对外	外:所有 ▼	ModSecurity : 所有 ▼	主机IP:所有 Q	主机名:所有 Q	城名:所有 Q	更多 ▼					
		0项										数据更新	:
			城名	所在主机		站点端口	是否对外		主目录路径	目录所有者	ModSecurity		ш
			没有站点相关	後									

4.1.6.5 Apache 站点清点

>	Apache站点清点 🛍											视图 !	
所有Apache这点城省[2]													
	×	是否对	外:所有 🔻	ModSecurity : 所有 ▼	主机IP:所有 Q	主机名:所有 Q	城名:所有 Q	更多 🔻					
	localhost	2 项									ŝ	收据更新	:
			城名	所在主机		站点端口	是否对外		主目录路径	目录所有者	ModSecurity		ш
			localhost	□0.0.0.0		80	「未知」		C:\xampps\apache\	BUILTIN\Administr	禁用		
			*	⊑0.0.0.0		80	「未知」				禁用		

4.1.6.6 Tomcat 站点清点

>	Tomcat站点清点 1										視图 🧮 🖵
	所有Tomcat站点域名[0]	站点	京列表 - 所有To	mcat站点域名							
ľ	没有发现站点	是否对	外:全部 ▼	站点端口:全部 Q	主机IP:全部 Q	主机名:全部 Q	更多 🔻				
		0 雨								百新数据	全部导出
		0.2								220000	10.04
			域名	所在主机		站点满口	是否对外	主目录路径	目录所有者	站点协议	
			没有站点相关	数据							
4.1.6.7 WebSphere 站点清点

>	WebSphere站点清点 👠											视图 📃 🖵
	所有WebSphere站点域名[0]	站点	1列表 - 所有We	bSphere站点域名								
	没有发现站点	是否对	外:全部 ▼	站点满口:全部(λ 主机IP:全部 Q	主机名:全部 Q	更多 🔻					
		0项									更新数据	全部导出
			城名		所在主机	站点鏑口		是否对外	主目录路径	站点协议		Ш
			没有站点相关	数据								

4.1.6.8 Weblogic 站点清点

>	Weblogic站点清点 1_									视图 📃 🖵
	所有Weblogic站点域各[0]	站点	記列表 - 所有Weblogic站点	城名						
	没有发现站点	是否对	口識点故 🔻 暗全:代	:全部 Q 主机IP:全部 Q	主机名:全部 Q	更多 🔻				
		0项							更新数据	全部导出
			城名	所在主机	站点請口	是否对外	主目录路径	目录所有者	站点协议	Ш
			没有站点相关数据							

4.1.7 数据库

4.1.7.1 SQL Server 数据库查询

>	SQL Server 数据库详细信息 1 创题										视图 📃 🖵		
	业务组:	全部 🔻	数据库目录:全部 Q	6月:全部 Q	主机IP:全部 Q	数据库实例名:全部	Q 更多 🔻						
	0项											更新数据	全部导出
		主机IP	数据	8年英型	数据库实例 S	版本	启用的协议	监听第日	主数据库路径	系统日志路径	错误日志路径	操作	Ш
		智无数据库(18月										

4.1.7.2 Oracle 数据库查询

> 1	Oracl	le数据库详细	田信息 1										视图 📃 🖵
	业务组:	全部 ▼	日志文件路径:全部 Q	主机名:全部 Q	蒴□:全部 Q	主机IP:全部 Q	更多 🔻						
	0项											更新数据	全部导出
		主机IP	数据库:	英型版		监听请口	运行用	∄户	配置文件路径	日志文件路径	数据路径	操作	Ш
		智无数据库伯	言意.										

4.1.8 启动项清点

4.1.8.1 启动项清点

资产视角

> 启动项统计 •	Ka 🔁 🖓
业务组:所有 T 启动版:所有 Q	۵.
50 项	数据更新 :
□ 启动须	主机农 III
MCTAdmin MCTAdmin	口 18
VMware Tools Core Service	Q 9
Microsoft OneDrive Setup	₽ 8
VMware Tray Process	₽ 7
CTF 加報程序	Q 6

▶ 启动项Java Update Scheduler详情



主机视角

> ±	机启动项统计 👠		1071 🗮 🖵
业宪	组:所有 🔻 主机	ルIP:所有 Q 主机名:所有 C	
28	项		:
	主机IP	启动项数	ш
	₽0.0.0.0	① 17	
	₽0.0.0.0	● 16	
	□ 10.10.10.15	● 16	
	□ 10.12.8.181	⊙ 14	
	□0.0.0.0	③ 12	
	□ 192.168.11.16	50 💿 12	
	□ 0.0.0.0	• 7	
	□ 10.128.0.249	⊙ 4	
	₽0.0.0.0	⊙ 4	
	₽ 192.168.18.13	35 💿 4	
	₽0.0.0.0	● 3	
	□0.0.0.0	③ 3	



4.1.8.2 运行服务清点

资产视角

> 服务运行统计 1			188 📃 🖵
服务分布 1 デ : 5 5 6 6 7 7 7 7 7 7 7 7 7 7 7 7 7			
业务组:所有 ▼			9.
439 项			数据更新
□ 服务名	说明	主机数	
System Event Notification Service	监视系统事件并通知订户这些事件的 COM + 事件系统。	Q 22	
UPnP Device Host	允许 UPnP 设备宿主在此计算机上,如果停止此服务,则所有宿主的 UPnP	Q 22	
Workstation	使用 SMB 协议创建并维护客户请网络与远程服务器之间的连接。如果此服务…	₽ 22	
User Profile Service	此服务负责加载和卸载用户配置文件。如果已停止或禁用此服务,用户将无法	₽ 22	
Print Spooler	將文件加戰到內存供稱后打印	Q 22	
┃ 服务Health Key and Certificate Management主机运行状态			
服务状态分布 00.0% ● 停止:3	启动类型分布	服务关型分布	• 共禀进程:3
服务状态:全部 Y 启动类型:全部 Y 服务类型:全部 Y	业务组:全部 ▼ 更多 ▼		9.
3 项			全部导出
□ 主机IP 服务状态 启	动类型 启动用户 路径	PID	服务类型
□ 및 192.168.202.149 停止 延	迟启动 localSystem System Idle Pr	pcess 0	共享进程

主机视角

>	主机服	服务查询 1 _		
3	业务组 :	新有 ▼ 主机IP:所有 Q	主机名:所有 Q	
	28 项			1
		主机IP	服务数	ш
		□ 192.168.11.160	⊘ 264	
		□ 10.12.8.181	© 232	
		□ 192.168.18.135	© 232	
		□0.0.0.0	© 222	
		□0.0.0.0	Ø 191	
		₽ 10.10.10.15	⊘ 185	
		□ 0.0.0.0	⊘ 178	
		□0.0.0.0	Ø 177	
		□ 10.128.0.249	Ø 161	
		□ 0.0.0.0	Ø 161	
		□0.0.0.0	⊘ 156	
		□ 0.0.0.0	⊘ 154	

> | 主机192.168.202.149的运行服务列表 1



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

安全补丁				税图 🗮 🖵
應逾程度分布 21.5% 13% 43.6	3327 ● 版第:70 ● 版第:70 ● 低第:20 ● 低節:4 ● 低節:45	Microsoft Dyna Developer Tools		
业务组:全部 ▼ 危险	程度:全部 T 里向方式:全部 T 补丁修复对象:全部 T	更多 🔻		۵.
191 项		所有条件 补丁特征		开始扫描 全部导出 :
□ 危险程度	补丁名	存在EXP CVE编号	补丁特征	影响主机数
血症急	.NET Framework 中的漏洞可能允许远程执行代码(MS14-057:	KB: 补丁名称 补丁名称	远程代码执行] 可能重启	1
危急	Windows 文件处理组件中的赢同可能允许远程执行代码(MS12	-08 补丁公告号	[远程代码执行] [必须重用]	1
んの	.NET Framework 和 Silverlight 中的漏洞可能允许远程执行代	∃(MS13-052: KB2840631)	(這些代码执行) 无意重度	1
意識	2017-09 适用于基于 x64 的系统的 Windows Server 2012 R2	月度安全质量汇总(KB4038792)	[远程代码执行] (存在EXP) 可能重高	1
意識	2018-09 适用于基于 x64 的系统的 Windows Server 2012 R2	月度安全质量汇总(KB4457129)	拒绝服务 权限提升 (信息注意) 远程代码执行 可能重用	1
6 8	Microsoft Data Access Components 中的漏洞可能允许远程	₩〒代码(MS12-045: KB2698365)	远程代码执行] 可能重同	1
后急	Windows Media 中的漏洞可能允许远程执行代码(MS11-015:	KB2479943)	远程代码执行) 存在EXP 可能重用	1

▶ 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

白名单规则 1			
条件:所有 Q 范围:所有 Q 受影响主机P:所有 Q			
0 项			新建白名单规则
	范围	受影响对象	操作 III
□ 没有发现任何项			

单击"新建白名单规则"按钮,进入新建规则页面

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
	□ 公告号:	请输入公告号
	补丁修复的应用:	请输入补丁修复的应用,多个以逗号隔开
	□ 补丁危害程度:	请选择危吉程度 ▼
	 修复影响: 	请选择修复影响 ▼
	则将风险项加入白名单	
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
	创建取消	

▶ 查看补丁提示信息

点击"补丁名称"后的标识 [●] ,现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





遊产等級分布 250% 75.0% 9 普通资产: 1 3 第要资产: 1		
资产等级:全部 ▼ 主机状态:全部 ▼ 业务组:全部 ▼	主印P:金部 Q	٩.
4 项	开始归须 全部导	щ :
□ 主机P 业务组	补丁分布	ш
□ ● 172.21.181.191 是是是	4 3 1 6	
□ ● 192.168.201 未分组主机	42 66 2 18	
□ ● 192.168.197.92 未分组主机	6	
□ ● 192.168.106 LSL测试	21 23 1 10	

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。

视图 😑 🖵

弱密码检测				
业务组分布 5 4 2 1 0 来分组3	295			
主机状态:全部 ▼ 账号状态:全部	5 Y 业终组:金部 Y 主机P:金部 Q 主机名:金部 Q			9.
2 项		开始	約月描 全部导出	:
□ 主机 P	业务组	弱密码数	操作	Ш
• 172.16.3.158	未分组主机	3	查看	
• 192.168.120.167	未分组主机	2	查看	

4.2.2.1 白名单规则

单击首页右侧 菇钮进入白名单规则页面。

白名单规则			
条件:全部 Q 范围:全部 Q 受影响主机P:全部 Q			
1项			新建白名单规则
□	范围 1	受影响对象	操作 Ⅲ
□ 账号状态为 : 禁用	全部主机	查看详情	/ 1

▶ 新建白名单规则

1	新建白名单规则		
	新建规则		
	条件列表:	□ 账号包含:	请输入账号,多个以逗号隔开
		□ 账号状态:	请选择账号状态 ▼
		□ 弱密码类型:	请选择弱密码类型 ▼
		如果满足上述条件,则将1	比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: 请送	b择业务组 ▼
		□ 主机: 请送	5择主机IP
	描述:	用户"123"于2019-04-1	11添加该白名单
		创建取消	
名单规则词	兑明		
见则	说明		

条件列表	账号包含:用户自定义,输入弱密码应用的账号。 账号状态:启用、锁定和禁用3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

白名单规则 1_			
条件:所有 Q 范ៈ面:所有 Q 受影响主切IP:所有 Q			
1 项			新建白名单规则
□ 条件	范围	受影响对象	操作 Ⅲ
□ 账号状态为:不可登录	全部主机	0	/ ii
▶ 删除白名单规则			
日名仲規則 €_ 条件:所有 Q 范囲:所有 Q 愛歌順主切P:所有 Q			
1 项			新建白名单规则
□ 祭件	范围	受影响对象	操作
□ 账号状态为:不可登录	全部主机	0	/ 1

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;

自定	义简单密码 🛿	简单密码字典说明	扖	导出
01	列表为空 , 请添	简甲密码字典,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		
02		编辑字典		
03		点击编辑框直接输入密码,每行为一个弱密码		
04		导入字典		
05		• 仅支持TXT格式文件导入;		
06		• 每个弱密码以换行分割;		
07		• 每次导入将完全覆盖原密码字典;		
08		• 每次导入最多识别前3000个弱密码,具后将忽略		
09		导出字典		
10		导出字典将导出所有弱密码为TXT文件,换行分隔;		
11				
12				
13				
0/300	0	取	消	确定

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

全部站点								
站点列表	业务组	1:所有 🔻 解析方式	式:所有 ▼ 端口访问性:所有 ▼	类型:所有 ▼ 更	ş •			
◇ 全部站点	22 1	Φ.				开始扫描	全部导出	:
> localhost HOST		时间	主机IP:端口	解析方式/站点	文件名	美型		ш
> * HOST		2018-01-17 23:53:53	2 192.168.197.130 : 80	(HOST) *	C:\openwbs\web.config	配置文	Θ	
		2015-10-05 00:51:06	2 0.0.0.0 : 80	HOST localhost	$\label{eq:c:c:ampps} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	系统文件	Θ	
		2015-10-05 00:51:06	2 0.0.0.0 : 80	HOST localhost	C:\xampps\apache_\htdocs\phpinfo.php	phpinfo	Ð	
		2015-10-05 00:51:06	2 0.0.0.0 : 80	HOST localhost	$\label{eq:classical} C: \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	系统文件	Θ	
		2015-10-05 00:51:06	2 0.0.0.0 : 80	[HOST] localhost	C:\xampps\apache_\htdocs\htaccess	系统文件	Ð	
		2015-10-05 00:51:06	2 0.0.0.0 : 80	HOST localhost	C:\xampps\apache_\htdocs\setup.php	系统文件	θ	
		2017-12-22 17:30:21	7172.31.177.178 : 8093	(HOST) *	E\websites\fwm\web - 副本.config	配置文	Θ	
		2017-12-22 17:30:21	172.31.177.178 : 8096	(HOST) *	E\websites\fwmadmin.com\web - 副本.config	配置文	Θ	
		2017-12-22 18:21:27	2 172.31.177.178	DNS *	E\websites\fwm_virtual\web.config	配置文	Θ	
		2017-12-22 18:21:27	712.31.177.178 : 8093	HOST *	E\websites\fwm\web.config	配置文	Θ	
		2017-12-22 17:30:21	172.31.177.178	DHS *	E\websites\fwm_virtual\web - 副本.config	配置文	Θ	
		2018-01-25 14:13:02	172.31.177.178 : 8098	HOST *	E:\websites\koneyaadmin\Areas\Admin\Views\web.config	配置文	Ð	

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。

暴力破	解						
3 第 月 次	明治控主机上3 护可以查看并如 1果来源 IP 处于	处生的爆破行为,并发送通知,非 处理暴力破解事件,也可以对暴力 非解封成功的状态中,则无法加	同时提供封停爆破京渝IP的能力。 力改解的 自动封停 机制和 服务设置 进 1入白名单,调将求源 IP 解封成功后再打	行配置。 11入白名单。			×
服务类	型:全部 ▼	封停状态:全部 ▼ 时	间区间:全部 ▼ 业务组:全部 1	▼ 攻击来源:全部 Q	更多 🔻		
33 Ij	۵.						服务设置 查看白名单 🔡
	服务类型	最近攻击时间	攻击来源	攻击目标	原计攻击次数	封停状态	操作 III
	SSHD	2019-04-16 04:30:49	193.201.224.82(乌克	≝) • 172.17.0.17	⊘ 3	解理时	6 R
	SSHD	2019-04-15 20:10:19	219.146.152.154 (中国	• 172.17.0.17	© 1	解封	6 R
	SSHD	2019-04-15 19:50:13	104.131.184.67 (美国)	• 172.17.0.17	⊘ 3	解封	6 R

手动解封按钮 🏾 🗟

手动封停按钮 🏾 🖗

加入白名单按钮 통

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^{③ 3} 按钮,可查看该事件聚合的攻击记录详情。

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
2010 02 11		

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。

SSH 登录服务 WINRM Windows 远程管理	服方石	描述
WINRM Windows 远程管理	SSH	登录服务
	WINRM	Windows 远程管理
RDP 远程桌面	RDP	远程桌面

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

新建规则		
条件列表:	口 攻击来源:	请选择攻击来源,可多选
		添加
	口 攻击时间:	请选择攻击时间
		添加
	口 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	
	O 自定义范围	
	□ 业务组: 详	选择业务组
	□ 主机: 详	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

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。

白名单规则列表					
取曲米源:新有 Q 取曲团用所号:新有	6 Q 2001:040 Q				
2 项					新建白名单规则
□ 第34	攻击来源	攻击时间	攻击使用账号	受影响对象	现作 III
10.44.188.101	140.205.201.32			0	× =
10.44.189.101	101.200.222.205			o	× 8

• 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。

白名单规则列表 1_					
波击来源:所有 Q 攻击使刑联号:所有 Q	范围:所有 Q				
2 項					新建自名单规则
1 范围	攻击來證	攻击时间	攻击使用账号	受影响对象	提作 III
 范围 10.44.188.101 	攻击灭望 140.205.201.32	<u> </u>	攻击使汗 脉已 	受影响对象. 0	度作 Ⅲ ▶ ■

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;

暴力破倒	库							
服务类型	2:全部 ▼	封停状态:全部 ▼ 时	间区间:全部 ▼ 业务组:全部 ▼	攻击来源:全部 Q 更多 ▼				
< 1/	1 项						加入白名单	导出
	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	Ш
~	RDP	2018-10-24 11:59:59	192.168.160.1 (局域网)	9 192.168.160.210	◎ 10	未处理	6 8	

全部导出:单击 法钮选择"全部导出"。

暴力破解						
实时监控主机上发生的用户可以宣看并处理暴。 如果来源 IP 处于非解剖	想破行为,并发送通知,同时提供主 力破解事件,也可以对暴力破解的 [加功的状态中,则无法加入白名单	オ伊姆破来源 IP的能力。 自动封停 机制和 服务设置 进行配置。 ,请将来渡 IP 解封成功后再加入白冬	3 9 .			×
服务类型:全部 ▼ 封	亭状态:全部 ▼ 时间区间:全	2部 ▼ 业务组:全部 ▼	攻击来源:全部 Q 更多	Ŧ		
240 项						服务设置查白动封停设置
□ 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	操作主机配置检测
SSHD	2019-04-18 08:01:57	142.93.83.136 (加拿大)	• 172.16.0.4	⊘ 2	未处理	€ 1000
SSHD	2019-04-17 20:06:41	193.112.125.195 (英国)	• 172.16.0.4	◎ 13854	封停	9 9
SSHD	2019-04-17 09:11:43	193.201.224.158 (乌克兰	• 172.16.0.4	S 397	未处理	6

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									
 ● 実利型位主机上发生的异常登录行为,例如非常用时间登录、非常用先点登录等异常登录,并发送如料通知, 用户可以查看这些异常登录中作,也可设置正常登录规则规定哪些力正常的登录行为,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 ▼ 2019.04.14	8~2019.04.18 🗙 业务组:全部 ▼	主机P:全部 Q 登录账号:全部 Q	更多 🔻						
1 项				正常登录规则设置 告誓设置	:				
□ 时间	主机IP	登录账号	来源IP	登录区域	Ш				
2019-04-18 11:51:10	• 192.168.30.169	zk	192.168.30.1	周域网					

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 <u>当</u> 登录区域 10音
	□ 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	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。											
件列表	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;											
	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;											
	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;											
	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											
	λ_{\circ}											
规则的适	规则范围是指以上条件的适用范围。											
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											
规则的适用范围	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											

• 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。

正常3	登录规则 €_								
925	3城:全部 Q 登录IP:全部 Q	Q 范围:全部 Q 登录数	K号:全部 Q						
6 I)	Ĩ						新建正常	(登录规则	
	范围	登录IP	登录区域	登录时间	登录账号	受影响对象	操作	111	
	全部主机	10.10.10.1-10.10.10.10				重看详情	/	Î	
	全部主机	123.123.123.123		07:00-10:00(周日,周二,		查看详情	1	Ϊ.	
	hao.yan	自定义内网ip组				查看详情	1	1	

• 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。

正常登	录规则 1							
登录区	域:全部 Q 登录IP:全部 C	2 范国:全部 Q 登录明	₭号:全部 Q					
6项							新建正常登录制	R.RJ
	范围	登录IP	登录区域	登录时间	登录账号	受影响对象	操作	ш
	全部主机	10.10.10.1-10.10.10.10				查看详情	/ 1	
	全部主机	123.123.123.123		07:00-10:00(周日,周二,		宣若详情	/ 1	
	hao.yan	自定义内网ip组				查看详情	/ 1	

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;

异常登	2										
③ 实 用	时监控主机上发生的5 户可以查看这些异常到	异常登录行为,例如非常用 登录事件,也可 设置正常登	时间登录. 深规则 想	非常用地点登录等 [定那些为正常的登录	异常智 8行为	表,并发送邮件通知 1、正常登录外的行为4]。 将被认为是异常登录	行为。			×
异常登录	2类型:全部 ▼	2019.04.18 ~ 2019.04.1	8 ×	业务组:全部 ▼		主机IP:全部 Q	登录账号:全部	Q 更多 •			
< 1/	1项										导出
	时间		主机IP			登录账号		来源IP		登录区域	ш
	2019-04-18 11:51:10		• 192.	168.30.169		zk		192.168.3	10.1	局域网	

全部导出:单击 按钮选择"全部导出"。

异常登录					
 ● 实时监控主机上发生的异常登录行为,例如非常用时间登录,非常用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端登录事件,也可谈面正常登录规则规定都些为正常的登录行为,正常登录外的行为将领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UP:全部 Q 登录账	<号:全部 Q 更多 ▼		
1 项				正常登录规则设置	記置检测
回 时间	主机IP	登录账号	来源IP	受录区域 全部	2出
2019-04-18 11:51:10	• 192.168.30.169	zk	192.168.30.1	局线网	

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。

入侵检测					×	yc 👤	1
后门检测							
通过实时监控发现各主机创建的进程是否包含后门文件,通过定端扫描系统发现进程、模块、自启动项和映像劫持类型的系	言门。						×
业务组:全部 ▼ 可信度:全部 ▼							
1 项			全部导出	重新检测	修复历史	更多、	
□ 后门类型 说明	受感染主机	发现时间		操作			Pip.
● test_filesize1 发现test_filesize1, 乳对应运行进程: cmd.exe	192.168.105.180	2019-02-20 16:26:47		查看洋情	下载		

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。

确认 test rule 3-dll	٤.					
基本信息 感染主机: 172.16.2.181 发现时间: 2019-02-28 19:40.18 动中取用: 1 近行和职: Jaunchim exe						
章中规则: 1 对应文件: C:\Windows\S	ystem32\LaunchTM.exe		建行班提考: launchtm.exe SHA256: 229bbb4f5582c9a4495236ec	运行进稿: launchtm.exe SHA256: 229bbb4f5582c9a4495236ecf57c667932fd58b1d437cbecb2ab7b3e08954534		
检测说明 静态信息	进程信息					
检测库	病毒名称	说明	修复方法	更新时间		
青藤YARA库	test rule 3-dll	test rule 3-dll	测试用规则,无需修复	2019-02-26 21:31:15		

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。

后门名称		主机IP	
进程w3wp.exe	的System.Web.ni.dll模	央 192.168.199.112	Î

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。

				dev 🚨	199H
E能够查看Web后门的。 如果有高级规则设置制	具体文件信息并下载后广 界求请使用这种方法。]文件。			×
部 👻 🚥					
			全部导出 开始扫描	更新数据依赖 更多	8 •
文件修改	受感染主机	发现时间	隔离/删除状态	操作	ľģ
2018-09-04 15:45:41	• 172.16.5	2018-09-27 10:19:19		详情 ***	
2018-09-04 10:13:43	• 172.16.5	2018-09-27 10:19:19		详情 …	
2018-08-31 18:13:31	◎ 172.16.5	2018-09-27 10:19:19		详情 ***	
2018-07-24 17:59:23	◎ 172.16.5	2018-09-27 10:19:19		详情 …	
2018-09-04 15:48:39	• 172.16.5	2018-09-26 17:40:56		详情	
	E進修査者Web占门約, 如果有高級規則设置者 部 * ··· 文件修改 2018-09-04 10:13:43 2018-09-04 10:13:43 2018-09-04 10:13:43 2018-09-24 17:59:23 2018-09-24 17:59:23	正確協会看Web局门的具体文件信息并下或員行 如果有高級規則设置需求请使用这种方法。 部 ▼ ・・・ 文件修改	E建塔査看Web局门的具体文件信息并下载局门文件。 如果有高級規則設置需求请使用这种方法。 部 ▼ ・・・ 文件修改 受感染主机 変現时何 2018-09-04 © 172.16.5 2018-09-27 10:19:19 2018-09-04 © 172.16.5 2018-09-27 10:19:19 2018-09-04 © 172.16.5 2018-09-27 10:19:19 2018-09-04 © 172.16.5 2018-09-27 10:19:19 2018-07-24 © 172.16.5 2018-09-27 10:19:19 2018-07-24 © 172.16.5 2018-09-27 10:19:19 2018-09-04 © 172.16.5 2018-09-27 10:19:19	E進塔登雪₩web后门的具体文件信息并下電后门文件。 如果有高級規則設置需求请使用这种方法。 部 ▼ ・・・ ② 部号出 子始扫描 文件修改 受帰発主机 爰规时间 隔离/承除状态 2018-09-04 0 172.18.5 2018-09-27 10:19:19 2018-09-04 0 172.18.5 2018-09-27 10:19:19 2018-09-31 0 172.18.5 2018-09-27 10:19:19 2018-09-24 0 172.18.5 2018-09-26 15:48.39 0 172.18.5 2018-09-26	dov ▲ EußwashG10的具体文件信息并下载G10文件。 如果有高级规则设置需求请使用这种方法。 部 ▼ ・・・ ② 部号出 开始扫描 更新数据体裁 更 文件修改 夏感染主机 ② 2018-09-27 2018-09-04 172.16.5 2018-09-04 172.16.5 2018-09-27 详续 *** 2018-09-04 172.16.5 2018-09-27 详续 *** 2018-09-28 172.16.5 2018-09-28 详述 ***

开始扫描按钮:即用户主动对单独该项进行扫描。

点击 ⁱ 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

功能设置列表	
是否开启	功能名
	Web后门动态监控
	模式分析引擎检测
	第三方威胁情报库检测
	取消 确定

4.3.4.2 查看白名单

白名单规则 1				
規則内容:全部 Q 使用范潤:全部 Q				
2 项			新建白名单规	101
M加約率	范围	受影响对象	操作	ш
□ 文件 5% : "\jsp	全部主机	宣看详情	/ 1	
文件MD5:f9d7df915d369e41c02acd8cb686544b	192.168.2.172	查看详情	/ 1	

▶ 新建白名单规则

新建白名单规则 1	t	
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	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。
	• 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。
	• 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	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。
	• 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。

修复记	修复记录 1								
首次发	现时间:全部 🔻	修复时间:全部 🔻	类型:全部 ▼	业务组:全部 🝸 主材	UP:全部 Q 更多 ▼				
20 項	D.								
	首次发现时间	修复时间	类型	主机IP	文件名	说明	域名	操作	ш
	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	E	
	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	9 192.168.2.135	/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	8	

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 1				
监控目录:全部 Q 应用范围:全部 Q				
48 项				新建自定义目录
□ 监控目录	最近修改时间	应用范围	状态	提作 III
/bin	2018-10-24 17:54:19	172.22.208.151	🔮 同步成功	编辑 删除
D /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	编码 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	3, 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:	请输入监控目录,支持输入多个,多个以英文逗号隔开	0
应用范围:	请选择主机P	
	创建并同步 取消	

• 编辑自定义目录

自定义目录 1				
监控目录:全部 Q 应用范围:全部 Q				
48 项				新建自定义目录
□ 监控目录	最近修改时间	应用范围	状态	sitte III
/bin	2018-10-24 17:54:19	172.22.208.151	同步成功	编相 規印余
/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 1				
监控目录:全部 Q 应用范围:全部	Q			
48 项				新建自定义目录
□ 监控目录	最近修改时间	应用范围	状态	39d7= III
/bin	2018-10-24 17:54:19	172.22.208.151	📀 同步成功	编辑 翻除
/bin	2018-10-24 17:54:19	172.27.0.15	同步成功	編編 凱除

4.3.4.7 查看详情

Web后门						
● 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。 发展实时检测其立即检查的方式未发现后门,并支持多种检测引擎,用户可以变着和处理发现给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:一种是于动加入白名单,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。						×
业祭組:全部 ▼ 可倍度:全部 ▼ 后门类型:全部 ▼ 文件名:全部 ▼	部 👻 🚥					
11 项				全部导出 开始扫描	更新数据依赖	更多 ▼
□ 后门类型 文件名	文件修改	受感染主机	发现时间	隔离/删除状态	操作	P\$
□ ● 文件目录… D:\test\JostDC - 副本.php	2018-09-04 15:45:41	172.16.5	2018-09-27 10:19:19		详情	
□ ● 已轮后门 D:\test\class-wp-upgrader - 副本.php	2018-09-04 10:13:43	• 172.16.5	2018-09-27 10:19:19		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 > 文件目录管理详	ń		加入白名单 下载文件
基本信息			
感染主机: 172.16.54.128 域名: Web后门文件: D <testnostdc- MD5: d72a95fbeb6349de9633</testnostdc- 	副本.php ibf238fdd6ad1	沒現时间: 2018-09-27 10:19:19 可信度: <u>考疑</u> 命中現即: 1 SHA256:	
检测说明 静态信息			
类型	説明		
文件目录管理	攻击者可以利用该后门文件进行上传下载文件、查看文件内	1客和查看文件列表等操作	展开 ❤

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。

检查首页		新建检查 更多 🗸
基紙规则:金部 ▼ 业务组:金部 ▼ 操作系统:金部 ▼ 检查条称:金部 ▼ 主机P:金部 ▼ 主机A称:金部 ▼ …		凭证管理 查看白名单
检查各称 	最后执行时间 2019-04-09 15:20:01	0 2 / 1
检查合称 XXX	最后执行时间 2019-04-08 14:31:11	0 2 / 1
检查名称 001	最后执行时间 2019-04-08 14:22:30	0 2 / 1

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。



▶ 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。

^{检查名称} 基线检查任务	最后执行时间 2019-04-09 18:30:54	 D 2 / 前 开始检查
▶ 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。	
^{检查含弱} 基线检查任务	最后执行时间 2019-04-09 18:30:54	 2 / 1 9出版表
▶ 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约	戋规则。
^{检查会除} 基线检查任务	最后执行时间 2019-04-09 18:30:54	 2 / 章 編組
▶ 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。	_
^{绘画会容} 基线检查任务	最后执行时间 2019-04-09 18:30:54	0 2 / Î

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。

检查首页 > CentOS 检查							
中国等保-Centos 7-三级主机安全合规检查							c >
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 查看	47.7% ^{通过率} ¹	21 通过项	23 _{未通过项}	0 失败项	
检查项视角 主机视角							
类別:全部 ▼ 检查名称:全部 ▼							
44 项						全部	7号出
□ 检查项名			类别	检查结果(通过率)	操作	15
□ 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不存在			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/nasswd 中的所有组在 /etc/oroun是否存在			用户和组设要		100%	 香香 送 悟	

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。

合规基线	检查用户默认的u	mask值是否为0	22			>
┃ 检查首页 > 武汉青藤CentOS基线测试	通过率 🕕	通过项	未通过项	失败项		
安信证券 Linux系统安全配置	100%	2	0	0		
最后执行时间: 2019-03-21 10:57:28 检查耗时: 15秒	主机IP:全部 ▼	主机名:全部	 ▼ 业务组:全部 主机名 	▼ 检查结果:全部 业务组	通过结果	操作
	• 172.31.	17.136	ip-172-31-17-136.cn-n	10 未分组主机	⊘ 通过	查看详情
检查项视角 主机视角	• 192.168	3.122.1	localhost.localdomain	未分组主机	❷ 通过	查看详情
关别:全部 ▼ 检查名称:全部 ▼						
18 项						
□ 检查项名						
□ 检查用户默认的umask值是否为022						
□ 检查是否禁用不必要的系统账户						
□ 检查是否禁止Control+Alt+Delete直接重定						
□ 检查是否禁用使用usb存储设备	已洗0/21加入白名	Ê.				**
□ 检查是否都要记录用户上次警录时间						关闭

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。

检查首页 > 武汉青藤CentOS基线测试							
安信证券 Linux系统安全配置						≔ <	>
最后执行时间: 2019-03-21 10:57:28 检查耗时: 15秒	13 ^{检查主机}	11 失败主机 章看	22.2% ^{通过率} 0	8 通过项	28 _{未通过项}	0 失败项	
检查项视角 主机视角							
主机IP:全部 ▼ 主机名:全部 ▼ 业务组:全部 ▼							
2 项						全部导	ш
□ 主机IP	业务组			检查结果(通	<u> </u>	操作	P\$
• 172.31.17.136	未分组主机			-	22.2%	查看详情	
• 192.168.122.1	未分组主机			-	22.2%	查看详情	

4.4.3 新建检查

单击"新建检查"按钮,进入新建检查页面。

金信息							
检查名称:	输入检查名称						
执行范围:	◉ 全部主机						
	○ 选择业务组	请选择业务组		Ŧ			
	O 选择主机	请选择或输入主机IP		Ŧ			
描述:	请输入备注信息	l.					
用定时检查:	○ 请输入会	时表达式	0				
线规则 🕕							
择基线规则:	Q.搜索规则						
		+ 添加基线规则					

▶ 添加主机规则

合规基线	添加基线规则
检查首页 → 新建检查	家純基线 应用基线
检查信度	CIS Level 1
检查名称: 输入检查名称	CIS Level 1
执行范围: ④ 全部主机	CIS Ubuntu 16 Level 1
O 选择生务组 消息将业务组 - O 选择主机 消息将业务组 -	CIS Level 2 CIS Level 2 CIS Level 2 CIS Level 2
描述: 诉输入商注信息	CIS Ubuntu 16 Level 2
	 ↓ 等保二级 □ 中国等保 二级主机安全合规检查 □ 中国等保 二级主机安全合规检查
Material O	中国等保 二级主机安全合规检查 中国等保
法律基线规则: Q. 投影規則	▶ □ 等保三级
+ /8100#49909	□ 中国等保 三级王机安全会规检查 □ 中国等保 三级王机安全合规检查 □ 中国等保 三级王机安全合规检查 □ 中国等保-Ubuntu 16-三级王机安全合规检查
	确定

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

r							
	类,每类下又细分为 CIS 和等保基线,基线可多选						
	【说明】基线选择后,若为数据库类型应用基线,则提示该规则中是否有需						
	要添加账号授权的基线,若有,则提示,例如:该规则中的60个检查项需						
	要账号授权						
	目前支持的系统基线有: windows server 2008/2008 R2/2012/2012 R2						
定时检查	打开定时检查开关,则可以输入定时表达式,且定时表达式为必填。定时表						
	达式为 crontab 格式,点击"创建并执行"时,需要校验该格式是否正确,						
	校验规则请参考"任务系统=》新建作业中 crontab 格式"。						
	鼠标移动到定时表达式后的 i,则显示定时表达式的输入说明。						
	关闭定时检查开关,则不可以输入定时表达式。						
描述	输入对该基线的描述。						

4.4.4 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	
系统在进行数据库基线等检查时,需提供检 行检查。请输入密码使用该功能	查对象的账号密码方可进
清输入账号密码	
	取消 确定

凭证管理管理的凭证用于对应的应用基线的检测。

┃ 检查首页 > 凭证管理					
 系统在进行基线检查时,需提供检查对象 	的账号密码等信息方可进行检查				×
应用类别	1项				添加授权
MySQL [1]	□ 用户名	数据库端口	适用范围	操作	På
	□ ××	8080	全部主机	编辑 删除	

▶ 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。

合规基线	添加授权 - MySQL	×
 检查首页 > 凭证管理 ● 系统应进行基线检查时,需提供检查对象的账号管码等信息方可进行检查 	• 周介名:1994年入用户名 图词:1994年入院词	
④用类别 1 项 MySQL [1] 用や名 取用年編□ 当用で名 ● 水 8080	X33 (新聞) (新聞) (新聞) (新聞) (新聞) (新聞) (新聞) (新聞)	
		取消 確定

▶ 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。

应用类别	1 项				添加授权
MySQL [1]	□ 用户名	数据库端□	适用范围	操作	1%
	□ ××	8080	全部主机	编辑 删除	

▶ 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。

应用类别	1 项				添加授权
MySQL [1]	□ 用户名	数据库端口	這用范围	操作	P&
	□ xx	8080	全部主机	编辑 删除	

4.4.5 查看白名单

单击 _ _ _ _ _ 按钮,选择"查看白名单",进入"白名单列表"页面。

1	检查首页 > 白名单列表			
	1 项			新建白名单规则
	□ 条件	范围	操作	ľø.
	□ 检查须:检查SSH空闲趣时间隔是否设置 - SSH服务配置 (中国等保-Ubuntu 16-二级主机安全会规检查)	全部主机	查看受影响对象编辑 册	除

▶ 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

	单列表 > 新建白名单规则	1日本 (14日本) 前面 (14)h (14)
		规则信息
精确检索		* 检查项:
	● 全部主机	执行范围:
·	O选择业务组 请选择业务组	
v	○ 选择主机 请选择或输入主机ⅠP	

点击"精确搜索",联动选择检查规则-检查类型-检查项。

合规基线	精确检索	×
▲ 检查首页 > 白名单列表 > 新建白名单规则	★ 检查规则:CIS Windows Server 2008 R2 Level 1合规检查 🔹 🔻	
规则信息	* 检查类型: 请选择检查的基线规则	
* 检查项: 清洗探检查项	* 检查项: 请选择主机. 🔻	
执行范围: 💿 全部主机		
〇选择业务组 		
O选择主机 清选择或输入主机IP		
	取消	确定

▶ 查看受影响对象

查看现有规则影响的对象。

合规基线	受影响的检查项列表	×
检查首页 > 白名单列表	聶統规則:全部 ▼ 聶統規則:全部 ▼	
1 项	基线规则 检查项名 基线检查名 所属主机P 主机名	业务组
□ 条件	中国等保-Ubuntu 检查SSH空闲超时间 ● 192.168.200.1 ubuntu	mfq
□ 检查项:检查SSH空闲超时间隔是否设置 - SSH服务配置(中国等保-Ubuntu 16-二级主机安全台		

▶ 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。

1项				新建白名单规则
□ 条件		范围	操作	Pb
检查项:	检查SSH空闲超时间隔是否设置 - SSH服务配置 (中国等保-Ubuntu 16-二级主机安全合规检查)	全部主机	查看受影响对象 编辑 册	除

▶ 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。

1项		新建白	名单规则
□ 祭件	范围	操作	1%
□ 检查项:检查SH空闭脚时间隔是否设置 - SSH服务配置(中国等保-Ubuntu 16-二级主机安全合规检查)	全部主机	查看受影响对象编辑 删除	

4.4.6 更新数据

单击 ^{更多} ♥ 按钮,	选择"更新数据",开始	更新资产	数据。	
) 数据更新中	新建树	金査	更多▼
			凭证	管理
			查看	白名单
			更新	数据
		0	7	

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。

口 10.31.91.192

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	
硬件配答	主机名: DESKTOP-2NABMOJ	Agent状态:在线
	内网IP: 172.16.11.65	安装时间: 2019-04-22 20:53:10
系统账号	外网IP: 58.49.50.122(连接)	最后下线时间:2019-11-11 09:32:34
	操作系统:Windows 10 Home China (buil	最后上线时间: 2019-11-11 09:33:33
アモカメリオ市山	内核版本: 10.0.18362.329	AgentID: 705c8e5e8d803810
运行进程	最后登录用户: 352843424@qq.com	Agent版本: 3.3.10-3.66.0-WIN-Rel-2019
软件应用	最后登录时间: 2017-10-08 10:54:55	系统启动时间:2019-11-01 11:25:55
Wabth	业务信息	
Web/d/	资产等级: 普通资产	
更多资产	业务组:产品组/xiaotong	
	标签:	
	管理信息	
	负责人:	
	负责人邮箱:	
長后面新时间・2010-11.	.11.00-35-01	百新数据 确会

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;
- 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;

Agent 安装		
Linux Windows		
1 安装需求	2 设置主机信息	3 安装引导
 支持主張 Linux版本 系統安装有Curl程序,目版本不低于7.10 系統启动Cron定时任务服务 	 105年土の125股フェ、 ・直注土印、 〇代理注接 ・ 送译土印所属业务组 ・ 	 ・ は取得令
* openssl版本不低于0.9.80 * 直连主机的防火墙需确保可与青藤服务器通信 具体要求	请选择业务组(必填) ▼	
* 代理呈接主則需要相连適管理服务器的sock5代理服务 安装方法		
Agent 安装 Linux Windows		
 安装需求 	2 设置主机信息	3 安装引导
 支持主流 Linux版本 系统交装有Curl握序,目版本不低于7.10 系统空装有Curl握序,目版本不低于7.10 	 ・ 洗择主机连接方式 ○ 直连主机 ● 代理连接 	・ 请以Root权限运行以下命令 生成命令
 * opensl版本不低于0.9.80 * 直连主机的防火墙需确保可与青藤服务器 ・ 直连主人的防火墙需确保可与青藤服务器 	请填写Socks5代理服务器信息 代理地址:诗命入"始合动口",或者"IPv4代图P30口" ④ 用户名:wentao.ma@qingteng.me	
 ・ 代理主接主机需要能连通管理服务器的 sock5代理服务 <u>空装方法</u> 	密码:	域名无击DNS操作?
	请选择业务组(必填) **	

【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;

Agent 安装 Linux Windows		
安装需求 支持主流 Windows版本 直连主机版为火墙,确保可与青颜服务器通信 具件要求 造连主机版为火墙,确保可与青颜服务器通信 具件要求 电描量和测试"命令安装"时,需使用PowerShell组织 安装方法 代理连接的主机型连通管理服务器的sock5代理服务 安装方法	 ② 役置主机信息 ● 進择主机塗検方式 ● 直接主机 ○ 件限準接 ● 造择主机所置业务相 ● 透探主机所置业务相 (必須) ● ■ 加爾塔加业务相, 供由 业务相繁報 	 ・ 請述择安装方式 ・ ・ ・ ・ ・ ・ ・ ・

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;

Agent 安装 Linux Windows		
文弦帶來 · 支持主張 Windows版本 · 直接主机场火境,确保可与曹娜振务器通信 具体要求 · 直接主机场火境,确保可与曹娜振务器通信 具体要求 · 直接主机通过"命令安装"时,需使用PowerShell组件 安波方法 · 代題主義的主机電性遺營理服务器的sockSf代運服务 安差方法	② 设置主机信息 出版主机能放力式 通道主机 〇 代間無線 出版主机所屬並勞組 出版主机所屬並勞組 (約項) 知識素加止勞組 (約項) 	 ③ 安安引导 ● 命令交流 ● 安秋和安流 ● 広行安和程序,将以下生成的参数填入*安禄参款*,点击*安 法*1017

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;

nux Windows 安装需求 • 支持主境 Windows版本 • 面连主印题火港、确保可与胃酸原务器通信 具体要求 • 面连主印题注命令安装*时,需使用PowerShell组件 安認方法 • 代通连接的主机型连道管理服务器的sockS代理服务 安装方法	 2 设置主机信息 选择主机运续方式 通道主机 〇代国运输 选择主机所雇业务组 通送单址例保健业务组 通送单址外组(認識) 或激素如业务组,亦由业务组数据 	 3 安装引号 ● 命を安楽 (● 安装包支架 (● 安装包+命) ● 命を安楽 (● 安装包支架 (● 安装包+命) ● 小店下駅Agent交装程序 ● 定数 ● 安装包位置: 浜岡府在文件夫, 知CADownloads (必須) 日核文件夫: CAProgram Files/TitanAgent ● 存在md中以管理点权限运行以下命令即可
---	--	--

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	5:全部 🔻 代理:全部	▼ Agent版本: 全部 ▼	安装时间:全部 ▼ 更多 ▼				
356 项	۵					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	Ш
	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

主机管理			
Linux Windows			3
业务组列表 ① 十日	主机标签		
查询业务组 Q	testtag1 tag002		
全部主机 [2]			查看更多 👻
> ww-linux [2]	主机状态:全部 ▼ 操作系统:全部 ▼	主机IP:全部 Q 主机名:全部 Q	更多 🗸
未分组主机 [0]	2 项		添加主机 主机信息同步 全部导出 :
	□ 主机IP	业务组 标签	操作 []
	• 192.168.80.150	ww-linux/ww-linux1 (4)	修改移动
	 192.168.80.149 	ww-linux/ww-linux	[tag002] 修改 移动

① 新建业务组

通过单击 + 按钮,可添加业务组。

亲	建业务组			
Ā	务组名*			
100	输入业务组名			
11	MA 14			
14				
				_
			取消	确定
	主机管理			
	Linux	Windows		
	业务组列表		+ 9	
	杏沟山冬归		0	
	三向正为运		2	
		1		
	全部主机 [2]		
			a =	
	> ww-linux	[2] +		
		添加业务组		
	未分组主相	π. [0]	-	

选择己有业务组,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 3 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";

导入业务组 🚱	
● 上传 Excel 文件	 (2) 查看导入结果
~	
L _t J	
选择文件到上传区域	
上传文件	
	取消导入

将填好的文件,上传至系统中即可;

③ 主机标签设置

标签列	表 1_				
标签:	所有 Q				
3 项					新建标签
0	标签	标记主机数	Rid	创建时间	操作
	濱示	37	演示服务器	2018-03-15 15:25:48	/ 1
	数据库	37	数据库	2017-09-12 21:53:38	Z 1
	张福	31	张瑶	2017-09-08 13:55:02	/ 1

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

修改主机信息	
资产等级	
普通资产 🔹	
负责人	负责人邮箱
张三	请输入邮箱
机房位置	固定资产编号
武汉	请输入编号
标签	备注
• Web , ● 数据库 , • XXX1 , 🛛 👻	请输入备注信息
	取送 商会

单击移动按钮移动所选主机到所选业务组。

修改业务组	76				
查询业务组	Q				
全部主机 [12]					
ops [4]					
e mfq [1]					
product [1]					
Ybkuo [1]					
zhailianfeng [1]					
			取消	确定	

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
 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 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 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 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。

規则列表 1		最后执行	行时间: 20	18-08-09	15:38:31
⑦ 通过设置主机规则,您可以就量设置各类主机信息,包括移动业务组、打石签、编辑监理信息等,					×
2项			执行规则	1 新行主	ARRI
1 現所 0	范围	是否启用	操作		ш
□ 如果::"主机在以下范围内:192.168.19.130-192.168.19.132"则:"标记标签::则试图例"	test-cy		修改	删除	移动
□ 如果:"主机运行任—应用:nginx","主机名中构合:nginx",则:"够动到业务组:Test","标记标签:Web",	全部主机		修改	删除	移动

• 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:	请输入主机名关键字
		主机IP在以下范围内:	请添加主机IP或IP段
			添加
则执行以下操作:		移动到业务组:	请选择业务组
		标记标签:	 新建标签
		标记资产等级:	请选择资产等级 ▼
		修改主机负责人:	请输入主机负责人
		修改主机负责人的邮 签·	请输入主机负责人的邮箱
	п	修改主机所在机房:	请输入主机所在机房
	П	修改主机的备注:	请输入主机的备注
	_	收起 ▲	
佐田芬園 。	• 4	と部士却	
1921728	0 1	▶▶●▶●▶●●● <tr< th=""><th>· ·</th></tr<>	· ·
描述:	请辅	认规则描述	
	新	■ 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			
显示的	主机IP:所有 Q			
266 1	σ			自定义IP显示规则
	主机IP	此時相	主机的所有IP	ш
	□ 10.165.18.119 (内网)	(R)sche	10.165.18.119 (内阁) 115.28.85.207 (外阁) 115.28.85.207 (逾線)	
	및 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 (连续)	
	🖵 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 (连娘)	
	📮 10.163.246.177 (内网)	虚拟化环境	10.163.246.177 (内阿) 121.42.12.91 (外网) 121.42.12.91 (连续)	
	🖵 10.144.68.123 (内阿)	1994c48	10.144.68.123 (内网) 115.28.0.20 (外网) 115.28.0.20 (连娘)	
	🖵 192.168.178.152 (内阿)	虚拟化环境	192.168.178.152 (内阿) 183.37.227.38 (连坡)	
	🖵 200.200.66.149 (外网)	19st/t8	200.200.66.149 (外阿) 14.153.223.73 (连续)	
	🖵 11.16.1.26 (外网)	虚拟化环境	11.16.1.26 (外間) 113.99.105.71 (海線)	
	📮 192.168.0.104 (内网)	虚拟化环境	192.168.0.104 (均同) 113.90.17.127 (连接)	
	🖵 192.168.197.110 (内网)	虚拟化环境	192.168.197.110 (内阿) 211.103.231.218 (施擁)	

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	Ł	
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 	
	 山 业务组: 二 主机: 	请选择±机P
	创建并执行	RUB

• 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 🐿				
⑦ 对范围内的主机设置自定义IP显示规则,根据规则优先显示其	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	蔽小的IP,		×
规则IP段:所有 Q 范围:所有 Q				
1 项				新建规则
规则印段	规则范围	修改时间	受影响对象	操作 III
192.168.235.1 - 192.168.235.254	192.168.235.137	2018-04-14 15:25:49	查看洋情	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;

IP组管理		
常用IP组	● 自定义内网ip/组	
自定义内网ip组 [4]	4 项	添加IP或IP段
安全外网ip组 [0]		48.0c III
dfasdfd [0]		site III
测试 [1]	12.12.12.12-13.13.13	/ 1
龙 [0]	111.1.1.1	/ 1
添加自定义IP组	1.2.3.4	/ II
	1.1.1.1-2.2.2	∕ ≣

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(一方面是用户很多时候都不知道在自己的网络环境中有多少主机,另一方面用户也会有一些主机新上线)。主机发现这个功能就是在用户网络环境内通过已经安装了 Agent 的主机发现未安装 agent 的主机,帮用户更全面的了解其网络环境内的主机资源,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 Protecol (ARP) 缓存是用来存放最近 Internet 地址 到硬件地址之间的映射记录。通过在安装了 agent 的主机上查找 ARP 缓存表内存储 IP 信 息来获取和这台主机连接过的主机。方法特殊设置: N/A
- Ping 发现, Ping 发现是通过发送 ping 包的方式来发现新主机,支持系统: Linux, Windows (TBD),方法特殊设置:设置扫描的 IP 段
- Nmap 发现

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。

新建扫描 1_	
基本设置	
任务名 *	
请输入任务名称	
发起主机*	
请选择发起主机	• 0
定时扫描 🕕	
请输入定时表达式	θ
获取操作系统 🕥	
通过操作指纹进行扫描, 会消耗更多资源	
扫描网段 🗌 手动设置	
默认的扫描网段为扫描发起主机的扫描网段	
扫描方式设置	
□ ARP續存方式扫描	
□ Ping方式扫描	
□ Nmap方式扫描 高级设置 >	
更多扫描设置 >	

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cron	tab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";
D.	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i	n的单位执行一次;
提示:	
日期和早期不可以	司时设罢目休的值
001.15*1 (X)
	- ,
一些示例:	
0 17 * * *	每天 17:00 执行
0 17 * * 1	每周——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 * * * *	
0 */1 * * *	毎时0分 毎隔1小时 孤行
2 8-20/3 * * *	8:02,11:02,14:02,17:02,20:02 执行
30 5 1,15 * *	1日 杣 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。

2.1Nmap 方式扫描

Nmap 方式扫描需要分别设置扫描网段、扫描协议和扫描端口。每个设置都有提供默认设置和手动设置。

2.1.1 扫描协议

• 默认设置

在默认设置下,则采用 TCP 协议进行扫描。需要用文字在界面上进行 说明。

• 手动设置

用户可以选择对扫描协议进行手动设置,包括只用 UDP、只用 TCP 和 都用。需要做的容错是用户不可以一个协议都不选择。

2.1.2 端口设置

• 默认设置

默认设置下, 会扫描本系统提供的一些端口。

• 手动设置

如果用户选择使用手动配置,则用户至少需要填写一个端口,并且要对 端口进行一些判定,看端口是否合法。

更多高级设置 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。

设置扫描任务 ▲		
扫描方式:全部 ▼ 扫描名称:全部 Q		新建扫描更新数据依赖
nmap-test Nmap扫描	自定义主机	2018-10-19 17:34:30
flong-test Nmap归描	所有主机	2018-10-10 18:42:17

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

设置扫描任务 ▲ 扫描方式:全部 ▼ 扫描名称:全部 Q		新建扫描	更新数据依赖
nmap-test Nmap扫描	自定义主机 扫描范围	2018-10-19 17:34:30 最后扫描时间)
flong-test Nmap扫描	所有主机 ^{扫描范围}	2018-10-10 18:42:17 最后扫描时间) ¢ ≣

• 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。

设置扫描任务			
扫描方式:全部 ▼ 扫描名称:全部 Q		新建扫描	更新数据依赖
nmap-test Nmap扫描	自定义主机	2018-10-19 17:34:30 最后扫描时间	▶ \$
flong-test Nmap扫描	所有主机 均衡范围	2018-10-10 18:42:17 最后扫描时间	▶ ≎ ≘

• 更新数据依赖

设置扫描任务 1			
扫描方式:全部 ▼ 扫描名称:全部 Q		新建扫描	更新数据依赖
nmap-test Nmap扫描	自定义主机	2018-10-19 17:34:30 最后扫描时间	▶ ≎ ≘
flong-test Nmap扫描	所有主机 目描范围	2018-10-10 18:42:17 最后扫描时间	▶ ≎ ≘

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 ▼ 没	备类型:全部 ▼ 操作系统::	注部 ▼ 更多 ▼			设置扫描任务	主机忽略列表
4 项	i							全部导出
	MAC地址	设备类型	主机IP	摄作系统	发现方法	首次发现时间	最后发现时间	
	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	
	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	
	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	
	00:50:56:F9:09:6B	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。

忽略王	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							
	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 问	ш
	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	
	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	
	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	机 1 型:全部 ▼ 操作	系统:全部 ▼	发现方法:全部 🔻	主机IP:全部 Q				
忽略主 设备类 く 5	机 ▲ 型:全部 ▼ 操作 0/290 项	系统:全部 ▼	发现方法:全部 🔻	主机P:全部 Q				取消忽略
忽略主 设备类 < 5 ☑	れ 全 型:全部 ▼ 操作 0/ 290 项 MAC地址	系统:全部 ▼ 设备类型	发现方法:全部 ▼ 主机IP	主机IP:全部 Q 操作系统	发现方法	首次发现时 问	最后发现时 间	取消忽略
忽略王 设备类 < 5 ☑ ☑	机 型:全部 ▼ 操作 0/290项 MAC地址 00:50:56:C0:0	系统:全部 ▼ 设备类型 VMware	发现方法:全部 ▼ 主机IP 192.168.202.1	主机P:全部 Q 操作系统	发现方法 ARP缓存扫描	首次发现时 问 2017-10-10 16:36:11	最后发现时 问 2017-10-17 11:50:54	取消忽略
忽略王 设备类 く 5 ✓ ✓	机 1 1 操作 型:全部 ▼ 操作 0/290项 MAC地址 00:50:56:C0:0 00:50:56:FD:8	系統:全部 ▼ 设备类型 VMware VMware	发现方法:全部 ▼ 主机IP 192.168.202.1 192.168.202	主机P:全部 Q 操作系统	发现方法 ARP缓存扫描 ARP缓存扫描	首次发现时间 2017-10-10 16:36:11 2017-10-10 16:36:11	最后发现时 间 2017-10-17 11:50:54 2017-10-10 16:36:20	取消忽略 III

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						创建报表
□ 创建时间	报表名称	报表类型	执行范围	最后生成时间	操作	ľ\$
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	下载报表	执行 …
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	下载报表	执行 …
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	下载报表	执行 …
2019-02-13 20:59:05	flong-test-html-detail	安全巡检	全部主机	2019-02-13 20:59:06	下载报表	执行 …
2019-02-13 20:54:47	flong-test-html	安全巡检	全部主机	2019-02-13 21:00:53	下载报表	执行 …

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

現表模版				搜索模版名称C
	Image: State	State State <t< th=""><th>NUMBER NUMBER NUMAR NUMAR NUMAR<th></th></th></t<>	NUMBER NUMAR NUMAR NUMAR <th></th>	
安全	《检报表-Word文档	安全巡检报表-Html	合规基线报表	

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:

#101108050898111#p.		CONTRACTOR NOTICE AND ADDRESS OF A DESCRIPTION OF A DESCR
B = B		AND DESCRIPTION OF A DE
**	**	
0.001	11.01	Sector Contraction of
10.10		
10010-018		
0.01034	5	
11 April 10		(and a
Add Agent Will		
B111 18	17 Lood BILLS	

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。 - 概述 11 评估人员 12 评估时间 13 巡检范围 14 巡检内容 - 遮桧结果擁要 2.1 Agent管理 2.1.1 Agent受装 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 风险发现 2.3 各危险程度风险分布
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。

初表 > 创 か の の の の の の	建报表	2 选择报表范围	③ 填写报表信息 ————————————————————————————————————	(4) 创建成功
择报表范围				
报表模板:	安全巡检报表-Word文档			
报表版本:	概党版			
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

▶ 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。

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	持殊字符 \ / : * ? * < >		
报表描述: 请输入报表描述			
信用定时检查: 🕞 请输入定时表达式	0		
			取消 上一步 创

▶ 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。

报表列表 > 创建报表

送择报表模板	- 🕢 选择报表范围	- 🕢 填写报表信息	- 4 创建成功
	\checkmark		
	创建成功		
	返回列表 执行报表作	Hz.	

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。

创建时间	报表名称	报表类型	执行范围	最后生成时间	操作	12
2019-04-11 18:43:19	报表任务测试	安全巡检	全部主机		下载报表 执行	

▶ 下载报表

执行报表作业后,点击操作的"下载报表"按钮,可以下载最近一次生成的报表。

创建时间	报表名称	报表类型	执行范围	最后生成时间	操作	ľ\$
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	下载报表 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。

操作	E			'¦
下素	报表	执行		
Т	修改			
	删除		-	
下	查看抽	城行记录		

▶ 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。

┃ 报表列表 > 报表任务测试		
 系统保留7天内的执行记录及文件。 		×
报表基本信息 报表名称:报表任务测试 创建时间:2019-04-11 18:43:19 是否定时执行:否 定时执行周期: 最后执行时间:2019-04-11 18:54:16	报表类型: 安全巡检 报表模板: 安全巡检报表-Word文档 执行范围: 全部主机 筛选条件: [统计时间:2019-04-04~2019-04-11]	
执行时间:全部 ▼ 执行耗时:全部 ▼ 执行状态:全部 ▼		
1 项		
执行时间 报表文件	文件大小 执行耗时 执行状态 操作	1%
2019-04-11 18:54:16 报表任务测试_安全巡检报表word版_20190411185416.doc	1.77MB 0秒 🔮 执行成功 下载	

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。

账号管理			
角色:全部 ▼ 用户组:全部 ▼ 账号状态:全部 ▼ 账号名	:全部 Q 姓名:全部 Q 更多 ▼		
2 项			新建账号 LDAP配置
	Art Talmak AT		477 /km 111
	(19)第二,111	账亏状态	3817F III
abc abc	2019-11-11 11:39:12	☑ 允许登录	/ 1
test	2019-11-11 11:50:35	⊖ 萘止登录	× 11

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。

账号状态:所有 ▼	账号名:所有 Q
查询账号状态	Q
禁止登录	
允许登录	
停用	

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。

	更多 ▼				
	清除筛选				
	备注				
│账号管理					
角色:所有 🔻 用户组:所有 🍸	业务组:所有 ▼ 账号状态:所	有 ▼ 账号名:所有 Q	姓名:所有 Q	更多 ▼	
备注:所有 Q			洋	青於筛选	
			~	/ 备汪	

5.4.1.1 新建账号

新建账号		
账号名 *		ž
请输入账号名		ž
初始密码 *		
请输入初始密码		2
🗌 启用LDAP认证 🥥		
姓名 *		ž
请输入使用者姓名		
邮件 *		2
请输入邮件地址		Ť.
	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 Q 姓名:全部 Q 更多 ▼		
2 项			新建账号 LDAP配置
□ 账号名	创建时间	账号状态	擾作
abc abc	2019-11-11 11:39:12	☑ 允许登录	i
			_

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	1				
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:	🔮 允许强	登录 修改		
LDA	P认证:	修改	攵		
所属	用户组:	无			
账号	角色:		64.CL 1		
			用巴 1		
		普通	用户 则	K弓	
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 1		
账号总览 基本信息 修改密码 所属用户组 1	角色设置 管理业务组	
基本信息		
姓名 *		
lizhi		
邮箱 *	手机号 *	
jfsahdfi@asdjd.com	请输入手机号码	
部门	职位	
请输入部门	请输入职位	
公司名称		
请输入公司名称		
公司批批		
请输入公司地址		
各注		
请输入公司备注		
保存		

• 修改密码

账号详情	1					
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	l
壬里志7	7					
	日 夕 *					
jiewe	en					
新密	码*					
请输	入密码					
确认	新密码 *					
请确	认新密码					
E F	自用LDAP认证	0				
(1)	-					
(采4	÷					

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

添加用户组

• 所属用户组

账号详情 1				
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:全部 Q	备注:全部 Q			
0 项				添加用户组
□ 用户组			督注	操作 Ⅲ
□ 没有发现任何	顶			

新增用户组

用户组:所有 Q 备注:所有 Q		
用卢坦	備注	添加
test1	123	
wewe	sdfsdf	
客户	客户演示组	

取消 砌建

账号详情 L 账号总法 基本信息 修改密码 新聞用户信 角色设置 管理业务组		
用户组:所有 Q		
4 项		新增用户组
日用户组	船注	操作
D 111	111	ii i
ztest	ztst	ii i
□ 安全部门	安全管理功能	Û
□ 测	资	Û

• 角色设置

账号详情 1							
账号总范 基本信息	修改密码 所属用户组	角色设置管理业	上务组				
角色名称:所有 Q	备注:所有 Q						
3 项						添加角	静色
□ 角色名称				备注	角色来源	操作	Ш
□ 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	î	
□ 测试				测试	天寺	Ξ.	
123				123	用户组	Ξ.	

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	Vindows业务	组					同步设置	
业务组				备	注	业务组末源	是否可管	管理
全部主机								
未分组主机								
> ww-linux						-		

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

账号详情 1	
账号总览 基本條	總 修改密码 所属用户组 角色设置 管理业务组 访问控制
访问控制	
是否启用:	
规则配置;	□ 溃择允许登录[7组:洗择[7组]
	」
	調査を输入部準約入評加部門加盟, 即使用時行分割, 例如1: 192.168.0.200 192.168.0.021 192.168.0.87-192.168.0.92
9277	

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。

账号管理			
角色:全部 🔻 用户组:全部 🔻	账号状态:全部 ▼ 账号名:全部 Q 更多 ▼		
13 项			新建账号
□ 账号名	创建时间	账号状态	操作 III
aaa aaa	2017-11-23 15:25:05	☑ 允许登录	/ 1
aoe aoe	2017-09-25 11:23:31	⊘ 允许登录	删除标签
	删除账号 ④ 确定删除此账号吗?		
		取消 确定	

需要验证密码才可删除。

账号管理			
角色:全部 🔻 用户组:全部 🍸 🐰	#号状态:全部 ▼ 账号名:全部 Q 姓名:全部 Q 更多 ▼		
2 项			新建账号 LDAP配置
□ 账号名			
abc	2019-11-11 11:39:12	◎ 允许登录	/ 1
🗋 test	· · · · · · · · · · · · · · · · · · ·	⊖ 莱止登录	/ 1
	需要密码验证才能执行此操作		
	账号名: wei.wu@qingteng.cn		
	输入密码: 请输入密码		
	取消	<mark>确定</mark>	

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。

LDAP 配置 1 LDAP 参数	
服务地址 * 请输入LDAP访问的目标地址,可为域名或IP	
目标基址 * 请输入LDAP访问的目录路径,类似于 *ou = xxx, dc = yyy*	
端囗访问 请输入LDAP访问端囗,唯一,可选	
加密方式 ● 无加密 O SSL O TLS	
是否匿名访问 〇 否 ④ 是	
查询用户DN 请输入LDAP的非匿名访问的查询用户名,类似于"CN=xxx,CN=yyy"	
查询用户密码 请输入LDAP的非匿名访问的查询密码	
保存 测试 清除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。

用户组管理			
用户组:全部 Q			
3 项			新建用户组
日用户组	备注	创建时间	操作 III
□ 平安健康	123	2017-09-25 11:26:01	/ 1
□ 环境组	测试业务组1	2017-08-14 17:36:12	/ 1
□ 用户组测试	测试用户组功能	2017-11-24 11:06:08	/ 1

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。

用户组*			
请输入名称			
备注 *			
请输入备注			

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。

田白细等理			
田户组:全部 Q 备注:全部 Q			
3 项			新建用户组
□ 用户组	备注	创建时间	操作
□ 平安健康	123	2017-09-25 11:26:01	1
□ 环境组	测试业务组1	2017-08-14 17:36:12	编标签
□ 用户组测试	测试用户组功能	2017-11-24 11:06:08	/ 1

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。

编辑用户组 🚹	
基本信息 成员管理 角色设置	管理业务组
基本信息	
用户组*	
平安健康	
创建时间	
2017-09-25 11:26:01	
备注	
123	
保存	

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。

编辑用/	9组 1			
基本信息	成员管理 角色设置 管理业务组			
2 项			添加用	户
	用户名称	用户详情	操作	Ш
	zhibin.cai	查看	Î	
	ace	查看	Î	

• 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。

添加用户	
账号名称:所有 Q	
张号 名称	关联
demo	
qingteng	
pan	
mfg	
gyb	
qingteng@qingteng.cn	
qianhai	
	取消 确定

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。

编辑用	≐组 1			
基本信息	成员管理 角色设置 管理业务组			
- T			TL-F	
2 坝			湖知山月	₩
	用户名称	用户详情	操作	Ш
	zhibin.cai	查看	Î	

删除

将对应账号从当前用户组中删除。

编辑用	户组 🚹						
基本信息	成员管理 角色设置	管理业务组					
2 项						添加序	刊户
	用户名称				用户详情	操作	ш
	zhibin.cai				查看	Ĩ	
	aoe				查看	删除用户	

3)角色设置

为当前用户组下的账号添加或者删除角色。

编辑用	户组 🛍				
基本信息	成员管理 角色设置	置 管理业务组			
2 项				潏	动角色
	角色名称		备注	操作	111
	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 👕	
	入侵功能		入侵功能	Î	

• 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。

添加角色			
角色名称:全部 Q	备注:全部 Q		
角色名称		备注	添加
超级管理员		拥有所有功能权限	
2.0		2.0	
sadf		sadf	
test		test	
test_man		test_man	
ztest		ztest	
测试角色		测试角色	
			取消 确定

删除

单击删除按钮即可删除已经创建的角色。

编辑用/	□组 1						
基本信息	成员管理	角色设置	管理业务组				
2 项						添加的	争色
	角色名称				酱注	操作	ш
	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	Î	
	入侵功能				入侵功能	删除标签	

4) 管理业务组

可以给己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。

编辑用户组						
基本信息 成员管理 角色设置 管理业务组						
Linux业务组 Windows业务组			同步设置			
业务组	备注		是否可管理			
未分组主机						
hao.yan	测试					
演示						
sstest						
> aws 云主机	aws 云主机					

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。

用户组管理			
用户组:全部 Q 备注:全部 Q			
3 项			新建用户组
□ 用户组	督注	创建时间	提供下 III
□ 平安健康	123	2017-09-25 11:26:01	/ 🗊
□ 环境组	测试业务组1	2017-08-14 17:36:12	/ 1
□ 用户组测试	测试用户组功能	2017-11-24 11:06:08	/ 1

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 Q	备注:全部 Q		
9项					新建角色
	角色名称		备注	角色状态	操作 Ⅲ
	普通用户		拥有所有普通功能权限,	但不提供任何高	Z 1
	超级管理员		拥有所有功能权限	◎ 启用	× 1
	2.0		2.0	⊘ 启用	/ 1
	sadf		sadf	◎ 启用	/ 1
	test		test	⊘ 启用	/ 1
	test_man		test_man	◎ 启用	/ 1
	ztest		ztest	◎ 启用	/ 1
	入侵功能		入侵功能	◎ 启用	/ 1
	测试角色		测试角色	❷ 启用	/ 1

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 _{角色状} :	理 志:全部 ▼ 角色名称:全部 Q 輸行	主:全部 Q		
9 项				新建角色
	角色名称	备注	角色状态	操作 III
	普通用户	拥有所有普通功能权限,但不提供任何高	◎ 启用	2 î
	超级管理员	拥有所有功能权限	⊘ 启用	Z 1
	2.0	2.0	⊘ 启用	/ 1
	sadf	sadf	❷ 启用	1
	test	test	❷ 启用	编辑标签
	test_man	test_man	◎ 启用	∕ ≣
	ztest	ztest	◎ 启用	/ î
	入侵功能	入侵功能	◎ 启用	/ 1
	测试角色	测试角色	❷ 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		
高用 O 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

编辑角色	<u>4</u>			
基本信息	权限信息 关联账号			
权限名称	R:全部 Q 备注:全部 Q			
9 项			添加	受权
0	权限名称	皆注	操作	ш
	010309-linux-入侵检测-web后门	Web安全中Web后门功能,全部权限已包含该功能	Î	
	010702-linux-系统管理-agent安	仅提供系统管理中Agent安装的权限	Î	

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。

添加授权		
权限名称:所有 Q		
权限名称	备注	授权
010101-linux-资产清点-全部权限	该策略拥有对资产请点所有功能的使用权限	
010102-linux-资产清点-只读权限	该策略拥有资产清点功能的所有只读权限,即可以使用资	
010201-linux-风险发现-全部权限	该策略包括主机风险功能的全部使用权限	
010202-linux-风险发现-只读权限	该策略拥有主机风险的所有只读功能权限	
010203-linux-风险发现-安全补丁	该策略包括安全补丁功能的全部使用权限,但不包含主机	
010204-linux-风险发现-弱密码检查	该策略包括弱密码检查功能的全部使用权限,但不包含主	
010205-linux-风险发现-对外访问性	该策略包括对外访问性功能的全部使用权限,但不包含主	
	取川時	确定

8) 关联账号

用户组列表视图

编辑角色 1	
基本信息 权限信息 关联账号	
用户组名称:全部 Q	
用户组列表 账号列表	新增关联对象
用户组名称	操作
没有发现任何项	

账号列表视图

编辑角色	
基本信息 权限信息 关联账号	
账号名称:全部 Q	
用户组列表 账号列表	新增关联对象
账号名称	操作
没有发现任何项	

新增关联对象

账号
8名称:所有 Q
目名称
-

取消 确定

5.4.3.3 删除

单击右侧"删除"按钮,可删除对应的角色。

角色管	理				
角色状	态:全部 ▼	角色名称:全部 Q 备注	E:全部 Q		
9 项					新建角色
	角色名称		备注	角色状态	操作 III
	普通用户		拥有所有普通功能权限,但不提供任何高	⊘ 启用	/ 1
	超级管理员		拥有所有功能权限	⊘ 启用	/ 1
	2.0		2.0	⊘ 启用	/ 🔳
	sadf		sadf	❷ 启用	删除标签

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。

Agent 管理									
Linux Windows									
安装时间:全部 ▼ 最后上线时间	:全部 🔻 最后下线时间:全部	▼ 资产更新时间:全部 ▼	主机IP:全部 Q I	ŧø ▼					
2 项								全部导出	立即更新
□ 主机IP	主机名 通信状	志 是否频繁掉线	运行级别	日志級别	Agent版本	Bash版本	操作		Ш
 192.168.80.150 	localhost.locald ● 连接	否	正常	正常	3.3.0-3.58.73-Rel	未安装	下载日志 下载运行报言	計删除Agent	:
9 192.168.80.149	host01 ●断开	否	正常	正常	3.3.0-3.58.73-Rel	未安装	下载日志 下载运行报告	删除Agent	:

▲ 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L	ense资源,点击一提删除	×	
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			

最后下线时间

2018-10-12 17:03:26 23天

离线时长

业务组

商线机器

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。

业务组: 全部 ▼ 商线时长: 全部 ▼

192.168.133.129 bogon

主机名

□ 主机IP

1) 设置运行级别:

一正常: Agent 拥有完整能力,执行服务器的任务。

一降级: 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。

一停用: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	战日志				
	起始	时间				
	2018	8-04-02 18:	50:48			
	终止	时间				
	2018	8-04-03 18:	50:48			
				1	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:

系统审计				
操作时间:全部 ▼ 操作类	型:全部 ▼ 所属功能:全部 ▼ 用户类型:全部 ▼	操作用户:全部 🔻 •••		
60 项				全部导出
操作时间	操作用户	操作名称	操作类型	操作 日本
2018-12-25 16:25:45	i 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	i qingteng@qingteng.cn	通用功能-账号认证-登录验证-用户登录	认证	直看详情
2018-12-25 16:20:48	i 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	i 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	i 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	i qingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息	查看	查看评情
2018-12-24 15:24:13	i 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	i 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	i 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	i 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:

系统审计				
操作时间:全部 • 操作类型:全部	▼ 所屬功能:全	NAMES AND DESCRIPTION OF		
60 项	用户操作中间 事件详情		- 1 -	
an et an tang	操作期间: 2018-12-25 16: 遍作实验: 通用功敏,账题()	25:38 事件ID: 5c21e982d41278557149ee 证.需要验证.用 再供源: Console	aa	i sera i l'è
2018-12-25 16:25:45	[1] qing 操作类型:认证 运用 qing 操作类型:认证 运用 qing 运作类型:认证	加全型加強型(14) (14)(15)(15)(15)(15)(15)(15)(15)(15)(15)(15	1	流逝评情
2018-12-25 16:25:38	i qing 请求来源	12119af 2: 40.14D = 727.360.027.44T		查看详细
2018-12-25 16:20:48	II qing 操作用户: qingteng@qing	iteng.cn 请求ID: 9dd82aa916404399942d22	27b1	查察评慎
2018-12-25 16:20:45	来源IP: 172.16.2.24 具作结果	来游区域: 局域网		注意评估
2018-12-25 16:20:40	ging ssmar. 200	481102 1993 7471	_	意志开展
2018-12-24 15:25:32	ing ging		关闭	意若評項
2018-12-24 15:24:13	gingteng@qingteng.cn	Windows-入侵检测-系统后门-直要事件信息	**	唐 聖详稿
2018-12-24 15:24:13	👔 gingteng@qingteng.cn	Windows-入侵检测-系统后门-查看事件信息		政策评决
2018-12-24 15:23:52	i qingteng@qingteng.cn	Windows-入侵检测-动态重键-查看率件信息	nu	放 制计划

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"。

消息列表						
♠ 全部消息	69	发生时间:全部 ▼ 消息内容:全部 Q 标题搜索:全部 Q				
资产清点		全部消息 (共349条, 其中69条未读, 仅查看未读消息)			全部标为已读	
风险发现		□ 満思标题	发生时间	消息类型	消息子类型	I
入侵检测	64	 发现主机192.168.192.165存在异常登录,登录未源为192.168.198.111(局域网) 	2018-10-30 15:14:38	入侵检测	异常登录/Linux	
安全涌告		 发现主机192.168.192.165被内网暴力破解,近30分钟累计534次 	2018-10-30 13:17:12	入侵检测	暴力破解/Linux	
产品动态		□ ● 发现内网暴力破解主机192.168.192.165的sshd服务	2018-10-30 12:52:44	入侵检测	暴力破解/Linux	
系统监控	6	 发现主机192.168.192.165被内网暴力破解,近30分钟累计708次 	2018-10-30 10:47:13	入侵检测	暴力破解/Linux	
其他		□ ● 发现内网暴力碳解主机192.168.192.165的sshd服务	2018-10-30 10:17:12	入侵检测	暴力破解/Linux	
✿ 消息接收配置		 发现主机192.168.192.165被内网暴力破解,近30分钟累计593次 	2018-10-30 10:17:11	入侵检测	暴力破解/Linux	
		□ ● 发现内网暴力碳解主机192.168.192.165的sshd服务	2018-10-30 10:01:04	入侵检测	暴力破解/Linux	
		 发现主机192.168.192.165被内网暴力破解,近30分钟累计20次 	2018-10-29 19:17:04	入侵检测	暴力破解/Linux	

选择"接收人管理"

消息列表							
▲ 全部消息	99+	⑦ 您可在此选择消息接收方	式,风险,入侵,弩	町计等重要消息,建议您乡	务必接收,防止遗漏造f	成损失; 自定义接收人可收到与您完全相同的内容	×
资产清点		消息接收配置(共28条	:)				接收人管理
风险发现				1011			
入侵检测	16		56内18	即作于	短信	按收入	操作
安全日志		资产清点					~
文件完整性	99+	□ 主机运行报告		•		qingteng@qingteng.cn,	/
安全通告		入侵检测					~
产品动态		□ Web后门/Linux	•	•		qingteng@qingteng.cn,	/
系统监控	14	□ Web后门/Win	•	•		qingteng@qingteng.cn,	1
其他		□ Web后门/容器	•	0		qingteng@qingteng.cn,	/
✿ 消息接收配置		□ 可疑操作/Linux	•	٢		qingteng@qingteng.cn,	/
		□ 暴力破解/Linux	•	•		qingteng@qingteng.cn,	1
		□ 后门检测/Linux	•	٢		qingteng@qingteng.cn,	1
		□ 异常登录/Linux	•	•		qingteng@qingteng.cn,	1
		□ 反弹Shell/Linux	•	•		qingteng@qingteng.cn,	/

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。

嵌人:			新增接收
接收人名称	邮箱	手机号码	操作
qingteng@qin	tester@qingteng.cn	15110081407	∕ ≣
ztw-test	1442966857@qq.com	18156268911	/ ii

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
□ 消息分类	站内信	邮件	短信	接收人	操作
资产清点					~
□ 主机运行报告		٢		qingteng@qingteng.cn,	1
入侵检测					~
🔲 Web后门/Linux	•	•		qingteng@qingteng.cn,	1
🔲 Web后门/Win	•	•		qingteng@qingteng.cn,	1
□ Web后门/容器	•	•		qingteng@qingteng.cn,	1
□ 可疑操作/Linux	•	•		qingteng@qingteng.cn,	1
□ 暴力破解/Linux	•	•		qingteng@qingteng.cn,	1
□ 后门检测/Linux	•	•		qingteng@qingteng.cn,	1
□ 异常登录/Linux	•	•		qingteng@qingteng.cn,	1
□ 反弹Shell/Linux	•	•		qingteng@qingteng.cn,	1

修改配置

▲ 各项通知至少要面	己置一位接收人。			
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	Î	
qingteng@qing	tester@qingteng.cn	15110081407	Î	

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。

消息接收配置 (共285) 消防他 消防他人 消防他人 消防他人 消防他人 消防他人 消防他人 消防他人 消防他人 消防他人 消防 1	③ 您可在此选择消息接收方式	;,风	.险,入侵,	审计等重	要消息,	建议您务必接	收,防止遗漏造成排	员失;	自定义接收人可收到与您完全相同的	的内容		×
副 消弱分类 函约 函約 短節 短次 四季 SF:Ric - - - - - - - - - - - </td <td>消息接收配置 (共28条)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>添加接收人</td> <td>移除接收</td> <td>ζĂ</td>	消息接收配置 (共28条)									添加接收人	移除接收	ζĂ
సాగేశు	■ 消息分类	站	内信		邮件		短信		接收人		操作	
● ●	资产清点											~
入侵位列 Q Q Qingteng@qingteng.cn, Qingteng@qingteng.cn, Image: Compare the sector of the sect	✔ 主机运行报告				0				qingteng@qingteng.cn,		1	
Web后门/Linux ● ● ● qingteng@qingteng.cn, Web后门/Win ● ● ● qingteng@qingteng.cn, Image: Space of the space	入侵检测											~
Web后门Win Image: Constraint of the symptotic of the symptot of the symptot of the symptot of the symptot of the s	✔ Web后门/Linux	•			0				qingteng@qingteng.cn,		1	
 添加接收人 · 接收人 · 邮箱 · 手机导码 · · qingteng@qingteng.cn · tester@qingteng.cn · 151100814 · ztw-test · 1442966857@qq.com · 181562689 · 	□ Web后门/Win	•			0				qingteng@qingteng.cn,		1	
●接收人邮箱手机号码✓qingteng@qingteng.cntester@qingteng.cn151100814□ztw-test1442966857@qq.com181562689		i	添加接收	乙人								
Image: symbolqingteng@qingteng.cntester@qingteng.cn151100814Image: symboltester1442966857@qq.com181562689				接收人		由区	箱		手机号码			
ztw-test 1442966857@qq.com 181562689			~	qingteng	g@qing	gteng.cn te	ster@qingteng.c	cn	151100814			
				ztw-test		14	142966857@qq.c	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。

	□ 青藤云安全	
	 ▲ 用户名 ▲ 密码 	
a de la companya de la compa	登录	
	Copyright© 2014-2018 Gingteng, All Rights Reserved. 原 ICP曽15030561号-31 胃器完安全 版初所有	

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: 上次登录时间:	未分组主机 ,未分组主机 ,ucloud-win ,centos ,ubuntu ,test ,test1 ,1 ,阿里云-win ,test-win ,lu 2018-11-02 18:32:37

5.8.2.2 基本信息

资料 1		
本信息		
姓名*		
龙帆		
邮箱*	手机号*	
fan.long@qingteng.cn	18907155131	
部门	职位	
请输入部门	请输入职位	
公司名称		
龙帆		
公司批址		
请输入公司地址		
备注		
 请输λ公司备注		

5.8.2.3 修改密码

※号急流 基本値影 修改密码 修改忠研 原密码 * 请输入原密码 前密码 * 请输入原密码 · 请输入密码 · <	账号资料 1		
修改法码 原密码。 谱输入原密码 新密码。 新密码。 通输入密码 确认新密码。	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			
原密码* 请输入原密码 前密码* 请输入密码	修改密码		
済輸入原密码 新密码・ 清輸入密码 端认新密码・	原密码*		
新密码* 请输入密码 输入新密码 *	请输入原密码		
新世時 ^一 请输入密码。 端认新密码。			
请输入营销 输入新密码 * 请输入新密码	新密码		
總认新送码* 请确认新送码	请输入密码		
清佛认新密码	确认新密码*		
	请确认新密码		
	确定		
Rectarda de la construcción de l			

5.8.2.4 访问控制

账号资料 化	
账号总览 基本	構造 構成性時 (7月15時) (7月15時) (2月15時) (2月15時) (2月15日) (2月151) (2]
访问控制	
是否启用:	0
规则配置:	☑ 造局允许登录》P组:自定义内阁IP组
	□ 手司施入代件登期P:
	请在输入局中输入PRDP范围,且使用换行分割,例如2: 192.168.8.020 192.168.8.021 192.168.0.87-192.168.0.92
保存	

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。

下載记	录					
6 ह	系统保留7天内的导出记	录及文件。				×
文件类	型:全部 ▼ 文	(件名称:全部 Q				
25 IJ	页					
	导出时间	文件类型	文件名称	文件生成状态	操作	Ш
	2018-11-02 08:30:00	风脸报表	linux风险发现_风险详情_20181102.xls	❷ 生成成功	下载	
	2018-11-02 08:30:00	风脸报表	windows风险发现_风险详情_20181102.xls	❷ 生成成功	下载	
	2018-11-01 20:40:45	Jar ⁶ 2	Linux_Jar包-主机视图列表_20181101_fan.long@qingteng.cn.csv	❷ 生成成功	下载	
	2018-11-01 19:53:26	Jar ⁶ 2	Linux_Jar包-主机视图列表_20181101_fan.long@qingteng.cn.csv	❷ 生成成功	下载	
	2018-11-01 19:53:05	Jar ⁶ 2	Linux_Jar包-主机192.168.202.177的Jar包详细信息_20181101_fan.long@qingteng.cn.csv	❷ 生成成功	下载	
	2018-11-01 18:23:06	托管主机	Linux-托管主机列表_20181101.csv	⊘ 生成成功	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;

购买信息 3省主机在正常使用中	
License 总量	100个
License 到期时间	2019-06-20
Agent在线数量 每一个在线的Agent会占用一个 License	3∱
	确定

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。

 \times



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