

服务器安全卫士 (原生版)

用户使用指南





修订记录

文档版本	发布日期	修改说明
02	2024/03/15	主要修改点:补充计费说明和最佳实践。
01	2022/7/20	新建文档。



目 录

1.	产品介	绍	1
	1.1.	产品简介	1
		1.1.1 产品定义	1
		1.1.2 产品架构	1
	1.2.	产品优势	2
	1. 3.	功能特性	3
	1.4.	术语说明	3
	1.5.	应用场景	4
	1. 6.	产品规格	5
	1.7.	产品使用限制	7
	1.8.	与其他云服务关系	8
2.	计费说	明	9
	2.1.	计费模式	9
	2. 2.	计费项	9
	2. 3.	优惠活动1	0
	2. 4.	续订规则1	0
		2.1.1 规则说明1	0
		2.1.2 自动续订规则	1
	2. 5.	退订规则1	2
3.	快速入	۲ًا ۱	2
	3.1.	注册天翼云账号	2
	3. 2.	开通服务器安全卫士(原生版)1	2
	3. 3.	购买配额1	5
	3. 4.	安装 Agent	6

€₹

	3. 5.	设置告警通知18	3
	3. 6.	切换版本19	?
	3. 7.	查看检测结果	I
4.	用户指	南	3
	4. 1.	计费操作	3
		4.1.1 订购	3
		4.1.2 手动续订	5
		4.1.3 自动续订	3
		4.1.4 退订)
	4. 2.	安全概览	2
		4.2.1 最近7日待处理风险	2
		4.2.2 防护状态	3
		4.2.3 风险趋势	5
		4.2.4 最近7日风险动态	5
	4. 3.	资产管理	5
		4.3.1 概览	7
		4.3.2 服务器列表)
		4.3.3 资产指纹	1
		4.3.4 资产详情	7
	4.4.	基线管理	3
		4.4.1 基线检测	3
		4.4.2 弱口令检测	?
	4. 5.	漏洞扫描	3
	4. 6.	入侵检测	2
		4.6.1 异常登录	2
		4.6.2 暴力破解	7

€₹

	4. 7.	网页防篡改(原生版)	31
		4.7.1 防护状态	31
		4.7.2 防护管理	33
		4.7.3 防护配额	7 3
	4. 8.	设置中心	? 7
		4.8.1 配额管理	? 7
		4.8.2 同步资产设置	? 7
5.	最佳实	践	79
	5.1.	快速掌握服务器安全态势	9
	5. 2.	查看单台服务器风险)0
	5.3.	弱口令安全最佳实践)2
	5.4.	漏洞扫描最佳实践)3
	5.5.	0penSSL 漏洞修复最佳实践)8
	5. 6.	0penSSH 用户枚举漏洞修复最佳实践 11	1
	5.7.	等级保护测评合规最佳实践 11	3
6.	常见问	题11	15
	6.1.	产品类11	15
	6. 2.	计费类 11	6
	6. 3.	购买类11	6
	6. 4.	操作类11	17
	6. 5.	系统类11	8



1. 产品介绍

1.1. 产品简介

1.1.1 产品定义

服务器安全卫士(原生版)(CT-CSS, Cloud Security System)是一款全方位保障云上服务器安全的 产品,能全面识别并管理服务器中的信息资产、实时监测服务器风险并阻止非法入侵行为,当发现服务器 出现安全问题时,第一时间向您发出告警通知。主要包括资产清点、漏洞扫描、入侵检测、基线检查、弱 口令检测、病毒查杀等功能,帮助您构建服务器安全防护体系。

1.1.2 产品架构

服务器安全卫士(原生版)整体架构主要包括3个部分,分别为统一管理平台、数据汇总节点和服务 器客户端 Agent。

- 1) 统一管理平台:客户管理员通过统一管理平台,查看所有的服务器信息和安全状态,并下发安全策略 配置信息。
- 资源池数据汇总节点:服务器客户端 Agent 从被监控服务器中采集系统信息,上报给相应的数据汇总 节点。
- 3) 服务器客户端 Agent: 使用服务器安全卫士(原生版)产品时,每台服务器需要安装一个 Agent。

€₹



1.2. 产品优势

统一管理和运维

在天翼云控制台上统一查看服务器资产和各项风险,快速构建安全可视化运维平台。自动收集云上服 务器数据,实现云上安全威胁实时管控,让安全没有死角。

三位一体全面防护

提供事前预防、事中防御、事后检测的全面防护,全面降低服务器入侵风险。

防护资源占用少

正常的系统负载情况下, CPU 占用率低,内存占用小,消耗极低;在系统负载过高时, Agent 会主动 降级运行,严格限制对系统资源的占用,确保业务系统正常运行。

用户使用方便快捷

无需登录云主机进行安装,简单配置防护策略即可实现防护;全部操作都有可视化界面,方便用户使 用;平台级产品,用户无需切换资源池即可查看全部情况。

防护机制安全可靠

こ 美天 ふう

有先进的检测技术和丰富的检测库,提供精准防御,做到全方位安全防护;对 Agent 进程加壳防护, 防止被篡改,采用加密传输与服务端通信,保证数据安全。通过 5000+台服务器的运行实践,稳定性高达 99.9%,2 分钟内离线自动重启机制,保障系统始终处于检测状态。

1.3. 功能特性

天翼云服务器安全卫士(原生版)产品主要包含以下功能:

安全概览:全方位查看服务器安全数据及状态,包括服务器数量统计、服务器安全状态统计、待处理 告警、服务器运行状况统计、服务器资产清点统计及排名。

资产管理:查看服务器列表信息及服务器详情信息,支持为服务器开启/关闭防护;自动清点主机内部 资产如进程、端口、账号、应用等,实时掌握主机内部资产变化,为安全分析提供数据基础。

基线检测:对系统基线进行全面检查,支持一键检测和定时检测方式,可自定义基线策略,支持对基 线进行白名单设置。

漏洞扫描:精准扫描 Linux 和 Windows 漏洞,支持一键扫描和定时扫描方式,可查看漏洞详细信息, 并提供漏洞修复建议。

入侵检测:包括异常登录和爆破登录,和查看各类入侵防御记录及拦截结果。实时异常登录监控,发现异常 IP、区域、时间等的异常登录,并发送告警通知;实时暴力破解多层次监控,支持暴力破解拦截功能,支持查看拦截记录。

弱口令检测:检测系统中的弱口令,包括常见弱口令、空口令、系统默认口令、口令中包含用户名等场景。

1.4. 术语说明

漏洞:是指在操作系统实现或安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问、 破坏系统,或者窃取数据。

基线:指为了满足安全要求,相关操作系统、数据库及中间件等必须达到的一定标准和基本要求。通 过对不同配置和策略的具体项目来评估是否达到安全基线,评估结果反映了服务器的安全性。

弱口令:指容易被攻击者破解的口令,一旦被攻击者破解,可用来直接登录系统,将使得系统及服务 面临非常大的风险。

异常登录:采集服务器上 RDP、SSH 登录日志,对合法登录 IP、合法登录事件、合法登录账号和合法 登录时段之外的登录行为均提供告警。

3

こ 美天 うう

暴力破解:攻击者对密码进行破解的行为,破解成功登录主机后,便可获得主机的控制权限,进行窃 取用户数据、勒索加密、植入挖矿程序等恶意操作,严重危害主机的安全。

1.5. 应用场景

场景一:入侵行为检测

实时监测发现云服务器的漏洞、异常登录、暴力破解、弱口令等问题,全面了解服务器的安全状态, 实现服务器安全的持续保护。



方案优势:

提供异常登录、暴力破解的告警和防御,可以快速的发现黑客对企业服务器的渗透扫描行为,及时预 警。

提供病毒查杀能力,有效检出恶意病毒文件,并提供病毒文件隔离和删除功能。

场景二:安全管理

提供统一的服务器安全管理能力,帮助用户更方便地管理云服务器的安全配置和安全事件,降低安全 风险和管理成本。



方案优势:

支持多操作系统:支持在 Windows、CentOS、Ubuntu 等多种操作系统的物理/虚拟主机上部署。

统一的安全管理能力:帮助用户同意查看所有的服务器资产、资产指纹以及安全事件,便于精细化安 全运营。

こ 美天 うう

场景三: 等保合规

服务器安全是等保合规的关键项,服务器安全卫士提供的入侵检测功能,能协助各企业保护企业云服 务器账户、系统的安全。



方案优势:

满足入侵防范条款:入侵检测,漏洞管理功能满足等保的主机入侵防范条款。

满足不同行业监管要求:基于基线检测功能,提供多种基线标准模板,企业可自定义基线策略,支持 一键检测和定时检测,根据检测结果提供处理建议。

1.6. 产品规格

根据支持功能不同,服务器安全卫士(原生版)分为基础版、企业版和增值服务。

不同规格功能差异为:基础版包含资产管理功能,入侵检测的异常登录、暴力破解功能,和漏洞扫描 功能,企业版包含安全概览、资产管理、入侵检测、漏洞扫描、基线管理和设置功能,增值服务目前提供 了网页防篡改(原生版)服务。

说明:基础版只支持部分功能的检测能力和防护能力。若需对服务器进行全面防护,您需购买企业版 防护。若需要对云上网站提供网页防篡改防护,您需购买网页防篡改(原生版)增值服务。增值服务可单 独购买或者与其他版本共同购买。

一级菜单	级菜单 二级菜单 功能概述		基础版	企业版	增值服务
安全概览	览 无 查看待处理风险、防护状态、风险 √				
资产管理	概览	查看资产概况、主机概况趋势图、 服务器区域统计,和账号、端口、 进程、软件应用的统计情况		\checkmark	
	服务器列表	查看主机资产信息、安全风险等功 能,支持模糊检索、筛选、开启防 护、关闭防护、切换版本,方便用 户快速管理服务器	仅展示入侵检 测和漏洞风 险,不支持切 换版本	\checkmark	
	资产指纹	查看账号、端口、进程、软件应用 4 种指纹的详细信息	\checkmark	\checkmark	



	同步资产	实时同步主机资产	\checkmark	\checkmark	
		异常登录情况统计	\checkmark	\checkmark	
	异常登录	事件列表	\checkmark	\checkmark	
2 /ヨ 4人 1回		白名单管理	\checkmark	\checkmark	
八反位测		暴力破解情况统计	\checkmark	\checkmark	
	暴力破解	事件列表	\checkmark	\checkmark	
		白名单管理	\checkmark	\checkmark	
		漏洞情况统计	\checkmark	\checkmark	
		Linux 漏洞、windows 漏洞	\checkmark	\checkmark	
	无	一键扫描	\checkmark	\checkmark	
漏洞扫描		定时扫描	\checkmark	\checkmark	
		基于漏洞名称的扫描结果列表	\checkmark	\checkmark	
		基于服务器的扫描结果列表	\checkmark	\checkmark	
		漏洞详情	\checkmark	\checkmark	
		白名单管理	\checkmark	\checkmark	
		基线情况统计		\checkmark	
		一键检查		\checkmark	
		定时检查		\checkmark	
基线管理	基线检测	基于基线名称的检测结果列表		\checkmark	
		基于服务器的检测结果列表		\checkmark	
		白名单管理		\checkmark	
		策略设置		\checkmark	
	弱口令检测	弱口令情况统计		\checkmark	

こ 美子 (つ)

		一键检测		\checkmark	
		定时检测		\checkmark	
		基于服务器的检测结果列表		\checkmark	
网页防篡改 (原生版)	防护状态	查看防护的总体情况,帮助您实时 的掌握所有云上网站被篡改的总体 态势			\checkmark
	防护管理	可为您账号下的云主机和物理机添 加防护目录,可采用白名单或黑名 单的方式进行添加。可展示当前已 添加的服务器的防护目录和备份目 录,并进行添加、编辑和删除			\checkmark
	防护配额	展示订购配额的总体情况,同时可 进行配额订购、续订和退订			\checkmark
设置	配额管理	展示购买配额的情况	\checkmark	\checkmark	
	同步资产设置	同步资产周期设置	\checkmark	\checkmark	

1.7. 产品使用限制

支持的服务器

天翼云弹性云主机

天翼云 GPU 云主机

天翼云物理机

支持的系统

天翼云服务器安全卫士(原生版)产品支持 64 位系统的服务器的防护,详情见下表:

OS	支持的 0S 版本
Windows(64 位)	Windows 2008 Windows 2012 Windows 2016
CentOS(64 位)	CentOS 6 系列 CentOS 7 系列 CentOS 8 系列

こ 美天 🖸

OS	支持的 0S 版本
Ubuntu(64 位)	Ubuntu 16.04 Ubuntu 18.04
UOS 统信(X86_64)	UOS V20
AnolisOS 龙蜥(X86_64)	Anolis OS 7.9 Anolis OS 8.4
Debian (X86_64)	Debian 9.0.0
openEuler (X86_64)	openEuler 20.03
Kylin 麒麟(X86_64)	Kylin V10 SP1 Kylin V10 SP2

支持的资源池

支持以下资源池:湖南_长沙3、福建_福州3、陕西_西安3、浙江-杭州2、上海7、云南_昆明2、内 蒙6、北京5、四川_成都4、宁夏_中卫2、安徽_芜湖2、山西_晋中1、广东_佛山3、广西_南宁2、江苏_ 南京3、江苏_南京4、江西_九江、河北_雄安2、海南_海口2、湖北_武汉4、湖北_荆州、湖南_郴州2、 甘肃_兰州2、福建_福州4、西藏_拉萨3、重庆2、陕西_西安4、青海_西宁2、香港1、福建_厦门3、湖 北_宜昌、福建_泉州、湖北_襄阳。

使用条件

每台服务器客户端需安装一个 Agent, 且服务器需不低于 101G。

1.8. 与其他云服务关系

网页防篡改(原生版)产品是服务器安全卫士(原生版)的增值产品,使用相同的技术架构。



2. 计费说明

2.1. 计费模式

服务器安全卫士(原生版)产品提供包年包月计费方式。包年包月是一种先付费后使用的计费方式,订 单周期越长,享受的优惠越大。

根据支持防护的功能不同, 服务器安全卫士(原生版)分为基础版和企业版 2 种规格, 具体价格如下表。

计费项	计费单位	标准资费
基础版	元/个/月	0
企业版	元/个/月	60

针对一次性包年付费服务,服务器安全卫士(原生版)的优惠政策为:1年85折、2年7折、3年5折。 6折优惠促销活动与包年订购折扣不能同享,取低者计算。

2.2. 计费项

天翼云服务器安全卫士 (原生版) 根据您选择的规格进行计费。

计费说明

版本	计费公式
基础版	免费
企业版	服务器台数*标准资费*购买时长



说明:

对注册天翼云账号的用户免费自动开通基础版,您可随时升级至企业版,安全防护能力更强。

计费示例

计费场景:用户需要防护的服务器台数为1台,预估资源使用时长1个月。 计费示例:60元/个/月*1个月*6折优惠=36元

2.3. 优惠活动

自产品上线之日起,服务器安全卫士(原生版)产品订购享受6折优惠。包年订购折扣与本次活动不能 同享,取低者计算(如包1年折扣为85折的,按照包一年6折计算;包3年折扣为5折的,按照5折 计算)。

2.4. 续订规则

2.1.1 规则说明

续订限制说明

- 1. 只有通过实名认证的客户,才可以执行续订操作。
- 2. 按需资源、包年/包月转按需(已完成转按需或正在进行转按需)的资源不可续订。
- 3. 未完成订单中的资源不允许续订,如开通中的资源、规格变更中的资源、退订中的资源。
- 4. 已退订或释放的资源不可续费。
- 5. 若资源到期后续费,续费周期自资源续订解冻开始,计算新的服务有效期,按照新的服务有效期计算费用。例如,客户资源2020年9月30号到期,10月11号续订1个月,那么资源新的服务开始时间为10月11号,到期时间为11月10号。相关费用自10月11号开始计算。



2.1.2自动续订规则

为避免由于未及时对配额采取续订操作,配额被到期冻结或超期释放,客户购买包月包年产品后,可设置开通自动续订。开通自动续订后,系统将在配额到期前自动续订,无需客户再手动操作。 适用范围:自动续订仅针对采用包月、包年计费模式的资源。已到期资源不支持设置/修改自动续订。

开通、变更、关闭自动续订

用户在续订管理页可开通自动续订功能,变更自动续约周期,或关闭自动续订。

不关闭自动续订的情况下,只要预付费账户余额充足,或为后付费客户,系统将持续按设定的周期自动 续订下去。

预付费用户可在官网自主控制自动续订功能的开通、变更、关闭。后付费用户需要客户经理协助开启自 动续订权限后才可以自主管理。

自动续订周期

包月产品默认自动续订周期为3个月,包年产品默认自动续订周期为1年,用户可按需调整自动续订周期。

自动续订价格

自动续订下单扣费时按当时的标准价自动续订,续订1年或以上可享受包年折扣。 0元、秒杀等特价促销活动产品订购后,自动续订下单扣费时将恢复标准价。 预付费用户暂不支持代金券支付,仅支持余额支付,用户需确保账户余额充足。

自动续订扣费规则

支付方式及支付时间:将在资源到期前10天和前7天进行两次自动续订下单及扣费。



自动续订订单出账后不可取消。客户如有问题,可发起退订,自动续订订单的退订与退订规则保持一致, 退订的同时,该资源的自动续订自动关闭。

自动续订和手动续订的关系

在7天或更短时间内到期的资源,或已到期资源,需手动续订,无法设置自动续订。 开通自动续订功能后,也可以进行手动续订。在自动续订扣费日前进行手动续订,系统将按照手动续订 后的到期日期,重新计算下一次自动续订的下单时间。

2.5. 退订规则

退订规则见:退订规则说明。

3. 快速入门

3.1. 注册天翼云账号

在创建和使用服务器安全卫士(原生版)之前,您需要先注册天翼云门户的账号,注册步骤见 <u>https://www.ctyun.cn/document/10000036/10464864</u>。如果您拥有天翼云的账号,请跳转到下一节"开 通服务器安全卫士(原生版)"。

3.2. 开通服务器安全卫士(原生版)

当您具备已通过实名认证的 ctyun 账号后,可以通过以下两种方式开通服务器安全卫士(原生版):

 在天翼云官网首页选择"产品->安全->网络安全->服务器安全卫士(原生版)"。进入服务器 安全卫士(原生版)产品详情页后,选择"控制台",如下图所示:



◆ 天翼云 最新活	动 产品 解决方案 应用商城 合作	伙伴 开发者 支持与服务 了解	天翼云	Q 中国	國站 文档 控制中心 备案中心 管理	里中心 💎 我的
						2110
服务 天翼云服务器 安全的产品, 现服务器出现 配、暴力破解 立即开通	会安全卫士(原生版)(CT-CSS, C 度全卫士(原生版)(CT-CSS, C 能全面识别并管理服务器中的信息 安全问题时,第一时间向客户发出 三載、基线检查、弱口令检测、病 控制台 产品文档 >	京生版) Cloud Security System)是一勤 资产、实时监测服务器风险并限 告警通知。主要包括资产管理。 适直杀等功能,帮助客户构建服务	2全方位保障云上服务器 且止非法入侵行为,当发 漏洞扫描、异常登录提 务器安全防护体系。	21102624		88上四大光图
					2110200	

进入控制台后,弹出下方"服务开通申请"对话框:

服务开通申请
服务器安全卫士(原生版)服务开通申请
1.开通前请认真阅读《天翼云服务器安全卫士(原生版)服务协议》 2.服务器安全卫士(原生版)开通后,默认为您开通基础版免费服务,开通即可使用,基础版不支持续订、退订操作。 3.服务器安全卫士(原生版)开通成功后,服务器默认处于"基础版"防护状态。
□ 我已阅读并同意相关协议《天翼云服务器安全卫士(原生版)服务协议》
退出同意

阅读《天翼云服务器安全卫士(原生版)协议》后,勾选我已阅读并同意签署《天翼云服务器安全 卫士(原生版)协议》,点击"确定"按钮,即可开通服务器安全卫士(原生版)服务,如下图所示:

	配额管理			的实现多稳安全卫士(原生版)
団 国务務安全卫士(原生版) ③ 服务務安全卫士(原生版) ④ 25名度2 ◎ 混印管理 ○ 周辺目 ○ 三	1 使用用引 1 使用用引 ① 购买配題 型出版和能理的服务者的思う。並且完成,在使用的的学者求,供会生自上 力"和某者者的定义上(注意用) 全主版記録使用	② 安裝Agent 使用服务型文型11(09:00) 服务, 如果常力点的产量外型改革 Agent, 在户标量的量和已正常调查器。 按照Agent	③ 収留合葉通知 含素和加速度。元度中心力学物理版在201人点:1: 50米半波音 素、中心成正 ・全点販売業額は50	• UARE • UARE • CORRER • CORRER • CORRER • CORRER
	1.単成172.目前の	彩颜度感	 ▲2回水志 ◇ (北川水志 ◇) 和田の ● (北川水志 ◇) 和田の ● (北田水志 使用水志 明定服务器 	

2. 在天翼云官网首页选择"控制中心",如下图所示:





在天翼云控制台中,安全分类下,点击"服务器安全卫士(原生版)",

(1)回 ~	存拢~	関語 ~
第增五主机(0) 增担计学 MESSI 得起的面		第三 面印成有云(1) 第三 空全編員的意味時間
「 同 「 物理性 に 多 の の の の の の の の の の の の の の の の の の	·····································	
元句照 元句明的(a)	21常行後(任美国)12 具有先期医会会同意式发行开展影响器	Image: Provide a contract of the second se
· · · · · · · · · · · · · · · · · · ·	7127746(00:2150) S146(20):637746(00:2150)	
A00. 增性/中国医师 自动问题:特征用		日本 またの時間は最新市時に1985
(2) 专展云 元中的专家成功法定资源	要金 ∨ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	2. 建性化和可能量的
		VPNAEE (0) HARRANN AVVORT
前班ə称册 ~	○ ○ ○ □ ○ □	
示照控 资源品件, 改要进程	CANADA CONTRACTOR	(二) 元(何高統(日存取)) 1995年二日 2月4日日
(注) 就由19/2019年8月	Web原用的大编(企业组) 集化类型资料组织的学校案	→ FigasO-WAN
	◎ 端名形式 場名解析曲线无线	◎ 五城
应用服务 ~		A Re-Assesse-operation
人。 图成为五应用平台 图成一起20xx00x平台2014间时服用	 	容滅振荡 ~
应用传话 ∨	Eðuli Heitsmann	C Harry Minazan

进入服务器安全卫士(原生版)控制台,弹出下方"服务开通申请"对话框:



服务开通申请
服务器安全卫士(原生版)服务开通申请
1.开通前请认真阅读《天翼云服务器安全卫士(原生版)服务协议》 2.服务器安全卫士(原生版)开通后,默认为您开通基础版免费服务,开通即可使用,基础版不支持续订、退订操作。 3.服务器安全卫士(原生版)开通成功后,服务器默认处于"基础版"防护状态。
□ 我已阅读并同意相关协议《天翼云服务器安全卫士(原生版)服务协议》
退出同意

阅读《天翼云服务器安全卫士(原生版)协议》后,勾选我已阅读并同意签署《天翼云服务器安全

卫士(原生版)协议》,点击"确定"按钮,即可开通服务器安全卫士(原生版)服务,如下图所示:

88	俞	配额管理					的实际	(务務安全卫士(原生版)
88 10 10 10 10 10 10 10 10 10 10 10 10 10		2. 使用指引 (使用指引) ① 約天記録 ① 約天記録 ① 約天記録 ① 約天記録(使名記法)*福廷等, 市有東京時的学業, 通点点上 介有市場有福廷法)*福廷等, 市有東京時的学業, 通点点上	② 安装Agent 供用の方型を立上(原生板)原あ、信用用丸均均平原用協会相 Agent 若特局的自己安定道道用。 安認Agent	 ③ 设置告票書句 合言書を以降に、用助呼合及可書知出作定定 第 通知者意思 (1) 企业物記様状合 	RALLIE: GRARGE	 ④ 切除版本 会会需要求成本: 皮的形式 型 () () () () () () () () () () () () ()	2000 2010 2010 2010 2010 2010 2010 2010	<mark>务器交全卫士(</mark>	815) X
		杜麗的行		(証明状态 ~) (使用状态 ~ ~)		服务器会称	81P	Q	0
		記题D	配额现格	配额状态 使用状态	绑定服务器	1	配额到期时间 掛	effE	

3.3. 购买配额

点击"配额管理"页面右上方"购买服务器安全卫士(原生版)",进入到服务器安全卫士(原生版)产品购买页面,面右上方"购买服务器安全卫士(原生版)",进入到服务器安全卫士(原生版) 产品购买页面:



88		订购服务器安全卫士 (原生版)
19 19 19 19 19	KB B B B B C B C B C B C B C	1 ThERBAREALE ((現在)) 版4 法課 ● 1 +
		RRBH ¥36 •

选择购买版本、防护服务器台数、购买时长、自动续订,勾选我已阅读并同意相关协议《天翼云服 务器安全卫士(原生版)协议》,点击"立即购买"按钮,购买成功后即可在"配额管理"页面查看已 购买的企业版配额,如下图所示:

Ê	配额管理						的复数务器安全卫士 (原生	E.16)
服务器安全卫士(原生版)	使用指引							
安全概覧 资产管理 ~ 基线管理 ~ 満済日編	① 物理在2日 金融初始発売後に約7.54881、648年期的約月前年、後点当日上 为7.98年最終度が全当土(9年期)	② 受張Agent 使用原系描述定工士(排生用) 服务, 在国家九边的户能外提供 Agent, 在时间包括有目已经放在包裹。 安藤Agent	 (3) 设置台票通知 合管通知设置前,风险并合 原、消化进设置。 	Q时港和站指定的人员注: 如何先设置音	④ 切换版本 生在台湾需要更高 足的配部。	8.807153P, 1817194644, 1	7换版本前请先购买数量充	
入使控制 《 與贡防篡改 (原生版) 设置中心 ~ 記録管理 用地密产设置	全北市松田市市		企业级配额状态					
	5	- 10/00- 2 - Amiz 3			12 .0#		 - 관차 5 - CEDMI 0 - CENT 7 	
	11.最终57			KS ~	服务群合称	务批P	0 8	G
	O 1888 O	配额规格	記額状态 使	用状态 绑定服务器		配额到期时间	操作	
	05effb4ef2df44c0abe93fo45cb982e9	全山坡	正常 未	椗 —		2022-09-30	相切 激灯	
	d80p444e1ac24609bd1523bb80e4b96f	全山坂	正常 未約	1定		2022-09-30	MAST WAST	
	a123ff690c7a4929x0705b6602343bfe	210	王常 朱1	啶		2022-09-30	续订 题订	
	0610126a40a446d4920a296b8d3#041	全业版	正常 使月	Ubuntu16 94D653P4 192.168.1.16(%)	-0605-8EEF-C066-8368	2022-09-30	续订 进订	

3.4. 安装 Agent

点击"配额管理"页面上的"安装 Agent"按钮,跳转至"资产管理->服务器列表"页面。



安	装Agent 批量切换版本			全地域	 ✓ Agen 	t状态 ~	防护状态 🗸	风险状态	~ 服务器名称	✓ 请输入:	云服务器IP或名称	0 0
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	漏洞风险	安全基线	网页防篡改	操作
	ecm-ad97-0001 8FC2C7DB-1F1 192.168.0.192(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	o	切换版本 开启防护 关闭防护 <mark>安装Agent</mark>
	ecm-ad97 C88BD603-D272-45A 192.168.0.56(%)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	o	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-a060 D5273532-8F20-47F5 192.168.0.19(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-b57e 228A09D8-D8E3-440 192.168.0.124(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	D	切换版本 开启防护 关闭防护 安装Agent
	ecm-cd3d AD6C8A31-F436-458, 192.168.0.5(指)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	o	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-e353 77E15E64-92AD-487 100.127.4.15(公) 192.168.0.249(者	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-b0e6 E126587D-2FBB-419i 192.168.0.184(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-d498 7BD42A91-7C82-413 192.168.0.191(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-3b3c 93DF77A7-7B74-4E1/ 192.168.0.159(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent

查看服务器列表中的"Agent 状态":若状态为"在线",则本台服务器已安装 Agent 且 Agent 服务 正常;若状态为"离线"或"错误",则本台服务器已安装 Agent,但 Agent 与服务器通信异常;若状态 为"未激活",则本台服务器未安装 Agent 或 Agent 未激活。

对于 "Agent 状态"为 "离线"、 "错误"或 "未激活"的服务器, 需要为该服务器安装 Agent。 Linux 系统安装命令如下图:

安装Agent	x
Linux系统 Windows系统	
支持的OS版本	
CentOS(64位): CentOS 6, CentOS 7和CentOS 8 Ubuntu(64位): Ubuntu 16, Ubuntu 18 Windows(64位): Windows 2008, Windows 2012和Windows 2016	
在您的服务器中以管理员权限执行以下命令进行安装 curl -k -s -L 'http://169.254.169.254:5662/download/eShield-agent/eShield-install-agent.sh'lbash	
复制 关闭	

Windows 系统安装命令如下图:



安装Agent	×
Linux系统 Windows系统	
安装方式	
1、远程登录到服务器。 2、请用浏览器访问http://169.254.169.254:5662/download/msi/CTCSSInstaller.msi,下载最新Agent到服务器,以管理员权限运行Agent安装程序	Þ
提示:通过IE浏览器访问时需要将用到的网站加入受信任的站点。	
关闭	

3.5. 设置告警通知

点击"配额管理"页面上的"告警设置"按钮,跳转至"设置中心->告警设置"页面,如下图所示:

	配额管理					购买服务银安全卫士 (原生城)
33 単学会部定 ※ 服务器安全卫士(原生版) ※ 安全地定 第二管理 ※ 第二管理 ※ 減費目提 ※ 減費目提 ※ 減費目提 ※ 減費目提 ※ 減費目提 ※ <	使用時3 ① 1 取品 型品計算具有変形が可能的、可能用用的計算者、単立 会社力で指定用の学品上(単立的) 企业和配料使用 】 () 企业和配料使用 】 () 企业和配料使用 () () () () () () () () () () () () () (श्री BRAGNET प्रसाप स्वरण्ड मेराव्य प्रसाप स्वरण प्रसाप स्वरण प्रसाप स्वरण प्रसाप प्रस प्रसाप प्रसाप प्र	 ③ 送気気変通の 発展など起き、外球が及 注意き、キャルは中心 注意き、キャルは中心 ● 第日2章 ● 第日2章 ● 全地転差がする 	rauusenas: era	UX換結本 外で空間意思系がかか、AUX (7)除命主	ARAF, GRAKFRIGTAR - 正天 7 - 日辺河 0 - 日辺河 7
	REGT REG	R280266 R280426	 ・ 使用状态 ・ 使用状态 ・ ・ ・	記録の 最差弱名称 研定服务器	服务部門 配額別期时间	Q C 操作
	ed5ct23bcce648f5839f5696a6010f01	企业版 正常	未诩定		2023-08-31	推过 第11

对各个功能的告警状态、告警时间、通知方式和告警项进行选择,如下图所示。告警状态默认打开, 告警时间默认全天,通知方式默认邮件和站内信,漏洞告警项默认超高危、超危和高危。



88	•	生素消毒				
67		告書设置				
0	服务器安全卫士(原生版)	入侵检测				
۲		事件类型	告警状态	告票时间	通知方式	告聲项
۲	安王取见 资产管理 ~	经保证		❹ 金天 ○ 9:00~18:00	□ 短信 □ 邮件 □ 站内信	服务器发生异常登录或爆破登录
۲	基线管理 🗸	暴力破解		● 全天 ○ 9:00-18:00	□ 短信 □ 邮件 □ 站内信	服务提供户发生暴力破解
	運用扫描 入価約消 ·	漏洞扫描				
	网页防算改 (原牛坂)	事件类型	告警状态	告警时间	通知方式	告警项
	网页的基C (原生版) 设置中心 ^	Linux運到		● 全天 ○ 9:00-18:00	□ 短信 □ 邮件 □ 站内信	- 超高能 - 超能 - 2 高能 - 2 严重 - 中能 - 2 任先
	記録管理	Windows潮洞		 	□ 短信 □ 邮件 □ 站内信	- 超高能 - 超能 - 國高能 - 國 戸屋 - 中能 - 國 低能
	1952 D.C. 10.44	基线管理				
		事件类型	告璧状态	告繁时间	通知方式	告警项
		基线检测		● 全天 ○ 9:00-18:00	□ 短信 □ 邮件 □ 站内信	存在检测不通过的基础项
		報密码检测		● 全天 ○ 9:00-18:00	□ 短信 □ 邮件 □ 站内信	存在發票員
		网页防篡改				
		事件类型	告酬状态	告誓时间	通知方式	告警项
		用页防器改		● 全天 ○ 9:00-18:00	□ 短信 □ 邮件 □ 站内信	用页文件发生篡改异常

3.6. 切换版本

点击"配额管理"页面上的"切换版本"按钮,跳转至"资产管理->服务器列表"页面,如下图所示。查看服务器配额版本情况,配额版本为"基础版"或"企业版",不同版本差异具体见 1.6 版本对 比章节。

安日	装Agent 批量切换版本			全地域	~ Ag	ent状态 ~	防护状态 >	风险状态	∨ 服务器名称	~ 请输2	人 云服务器IP或名称	α :
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	漏洞风险	安全基线	网页防篡改	操作
	ecm-ad97-0001 8FC2C7DB-1F 192.168.0.192(私)	1 linux	责州公共测试	未激活	未防护	未知	基础版	0	0	0	O	切换版本 于启防护 关闭防护 安装Agent
	ecm-ad97 C888DD603-D272-45 192.168.0.56(私)	A linux	贵州公共测试	未激活	未防护	未知	基础板	0	0	0	o	切换版本 开启防护 关闭防护 安装Agent
	ecm-e060 D5273532-8F20-47f 192.168.0.19(私)	E línux	责州公共测试	未激活	未防护	未知	基础版	0	0	0	D	切换版本 开启防护 关闭防护 安装Agent
	ecm-b57e 228A09D8-D8E3-44 192.168.0.124(私)	D: linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-cd3d AD6C8A31-F436-45 192.168.0.5(私)	B. Ilnux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-e353 77E15E64-92AD-48 100.127.4.15(公) 192.168.0.249(71 linux 礼	责州公共测试	未激活	未防护	未知	基础版	0	0	0	O	切换版本 开启防护 关闭防护 安装Agent
	ecm-b0e6 E126587D-2FBB-41 192.168.0.184(私)	9: linux	责州公共测试	未激活	未防护	未知	基础版	0	0	0	O	切换版本 开启防护 关闭防护 安装Agent
	ecm-d498 7BD42A91-7C82-41 192.168.0.191(私)	3 linux	责州公共测试	未激活	未防护	未知	基础版	0	0	0	O	切换版本 开启防护 关闭防护 安装Agent
	192.168.0.191(私) ecm-3b3c 93DF77A7-7B74-4E 192.168.0.159(私)	l, linux	5777275789国 贵州公共测试	未激活	未防护	未知	新程版	0	0	0	0	关闭防护 安 切换版本 开

您可将需要防护的服务器进行"切换版本"。选择您需要切换版本的服务器,可进行单台服务器的 配额版本切换,也可以选择多台服务器进行批量切换。若您选择基础版防护服务器"切换版本",则可



将基础版防护切换至企业版;若您选择企业版防护服务器"切换版本",则可将该服务器更换企业版配额。

注意:企业版防护服务器不可切换为基础版防护!

针对您需要切换版本的服务器,点击操作中的"切换版本",基础版或企业版配额服务器均可选择, 点击后跳转至如下页面,选择企业版配额并点击"确定"后,基础版防护服务器切换为企业版防护,而 企业版防护服务器更换为新的企业版配额。

切换版本 × 服务器 当前版本 ecm-ad97-0001 8FC2C7DB-1F17-47A5-94CA-9F4A11184F3A 基本版 192.168.0.192(私) 购买服务器安全卫士(原生版) 选择企业版防护配额 请输入防护配额ID 5 配额ID 配额到期时间 版本 ○ 58225ff8f1594dbcbe9c8(2022-11-22 00:00:00 企业版 O d5d5d59354d34a9faeb4c 2022-11-22 00:00:00 企业版 ○ e4a2a4a383eb4b8aba9b; 2023-08-22 00:00:00 企业版 12112a8b9e524a07ab41 2023-08-22 00:00:00 企业版 9c4ba7bf67f5474db4ea8 2023-11-22 00:00:00 企业版 ○ f563c4ddc887473a8ee8f 2025-10-22 00:00:00 企业版 共6条 10条/页 1 > 前往 1 页 取消 确定

可进行批量切换,在服务器列表中选择需要切换的服务器,点击"批量切换版本",跳转至下方页面,点击"确定"后,切换为企业版防护,配额和服务器按照顺序一一匹配即可。说明:批量切换版本时,服务器按照图中顺序与配额绑定,配额的绑定顺序为按照到期时间从早到晚进行绑定。



批量切换版本		×
 您批量切换版本时,服务器按照下方列表中顺序与配额绑定,配 	硕的绑定顺序为按照到期时间从早到晚进行绑定 购买服务器安全卫士(原生版)	
服务器	当前版本	
ecm-ad97-0001 8FC2C7DB-1F17-47A5-94CA-9F4A11184F3A 192.168.0.192(私)	基本版	
ecm-ad97 C888D603-D272-45A9-BD06-57C7D9DC0FEC 192.168.0.56(私)	基本版	
ecm-a060 D5273532-8F20-47F5-B13A-923D11DA3729 192.168.0.19(私)	基本版	
取消	确定	

3.7. 查看检测结果

选择"安全概览",进入安全概览界面,可查看已开启防护的服务器风险统计,包括最近7日待处 理风险、防护状态、风险趋势和实时动态。

		安全概览	預序更新日期: 2022-08-29 1353.54 同9 頁/
 ³服务器安全卫士(原生) 	±版)	量近7日待处理风险	i Kevita
 安全規定 资产管理 基线管理 漏洞扫描 	×	Althouse (*) MIRRAR (*) MIRRAR (*) MIRRAR (*) MIRRAR (*) Image: 1 Image: 1	XHLAR (B) 2 ± 48050° (B) ЖЦАВОР (B) ЖЦАВОР (B) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D) Image: Solid (D)
入侵枢湖 ~ (岡页防幕改(原生版) 设置中心 ~ (风险趋势	। মধ্যক্ষ
			主机 単件行为 发現时间 操作 CentC0575 14776F416-D18C 192.108.1.3(%) 基社风险 2022-08-25 17.53.15 量音计结
		20	Cert0575 1478/F416-D18C 192.168.1.3(%) 基线风险 2022-08-25 17:53:12 常音计结
		40	Cert0675 1478F416-D18C 192.168.1.3(私) 基线风险 2022-08-25 17.53.12 昆音环络
		20	Ceref0576 1478F416-D18C~ 基结系动 2022-08-25 17:53:12 度低17%
		0 / 24 25 28 27 28 29	Cent0635 1478F416-D18C-, 192.168.1.3(%) 超线风险 2022-08-25 17:53.12 宜音计制
		- 人間に同一 副同時に - 安全部に - 同時間の	共6条 < 1 > 前住 1 页



也可以选择"资产管理->服务器列表",查看防护服务器的入侵检测、漏洞风险、安全基线和网页 防篡改的检测结果。

全部	主机 风险主机 企业场	主机 基础版主机	未防护的主机	己离线主机								
安装	Agent 批量切换版本						±18%€ ~ Agen	us - spus	~ AB045	~ 服务基名称	· 请输入后报务器中或名称	
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配額版本	入侵检测	漏洞风险	安全基线	同页防篡改	操作
	Windows2012 81E26604-FBF9-E 192.168.1.4(%)	windows	内蒙漠示环境	在线	85%中	安全	全位版	0	0	0	0	切换版本 开始防护 关闭防护 卸载Ager
	Ubuntu16 94D653F4-0605-8EEF 192.168.1.16(%)	linux	内装滚示环境	在线	股桥中	安全	企业版	ō	0	0	0	切换版本 开西热护 关闭防护 卸载Age
	CentOS76 160D4123-E38F-F6E: 192.168.1.8(%)	Tinux	内蒙演示环境	在线	153°4+	风险	基础版	1	0	50	0	切换版本 开启热护 关闭防护 卸载Age
	windows2008 EBF69C73-C5A8-L 192.168.1.6(%)	windows	内蒙演示环境	在战	159°0	安全	基础版	0	0	0	0	切换版本 开自结中 关闭防护 卸载Ager
	CentOS75 1478F416-D18C-011 192.168.1.3(%)	linux	内蒙濱示环境	在线	防护中	风险	基础版	0	0	64	ō.	切换版本 开启结护 关闭防护 目载Age

也可以通过分别选择"基线管理"、"漏洞扫描"、"入侵检测"和"网页防篡改(原生版)"功能,分别查看护服务器的基线检测、漏洞管理、入侵检测和网页防篡改的检测结果。



4. 用户指南

4.1. 计费操作

4.1.1 订购

以下为服务器安全卫士(原生版)的购买流程。

当您具备已通过实名认证的 ctyun 账号后,可以通过以下两种方式开通服务器安全卫士(原生版):

1. 进入服务器安全卫士(原生版)产品详情页,如下图所示:

→ 天翼云 最新活动	动 产品 解决方案 应用商城 合作	Q 中国	国站 文档 控制中心 备案中心 '	管理中心 🧖 我的		
21102624	21102624	21102624	21102624	21102624	21102624	21107
服务 天翼云服务器4 安全的产品,角 现服务器出现好 醒、暴力破解拧 立即开通	安全卫士 (原生版) (CT-CSS, 陸立) (原生版) (CT-CSS, 陸道の説明用管理服务器中的信息 全问题时,第一时间向客户发出 全问题时,第一时间向客户发出 金城台。弱口令检测、廊 陸脚台 产品文档 >	京生版) Cloud Security System)是一部 资产、实时监测服务器风险并照 告警通知。主要包括资产管理。 毒査杀等功能,帮助客户构建服	处全方位保障云上服务器 目止非法入侵行为,当发 漏洞扫描。异常登录提 务器安全防护体系。	21102624	22/10/624	2110262

单击【立即开通】,进入到服务器安全卫士(原生版)产品购买页面:

88	\sim	
<pre>C</pre>		[7] 羽服英務委全立士 (原生版)
۲	服务器安全卫士(原生版)	版本选择 全盘路 版本对比信息
© © ®	 服务器安全卫士(県生版) 安全戦災 現代管理 4 現代局現代 夏が得理 の 基管理 の 基管理 名 基管理 4 第4日や管 第4日 第4	版本3排 255 K4541248 新学展务组合数 1 + RATAR RATAR RATAR BARAK 0 0 0 0 0 1 ↑ Å BARAK 0 0 0 0 0 1 1 ↑ Å BARAK 0 0 0 0 0 0 1 10 1 1 1 ↑ Å BARAK 0 0 0 0 0 0 1 10 1
		東周告計 ¥36 ●



选择购买版本、防护服务器台数、购买时长、自动续订,勾选我已阅读并同意相关协议《天翼云服 务器安全卫士(原生版)协议》,点击"立即购买"按钮,购买成功后即可在"配额管理"页面查看已 购买的企业版配额,如下图所示:

88	Î	配额管理						购买服务器安全卫士 (原生版)
0	服务器安全卫士(原生版)	使用指引						
•	安全概又 新学修理 ~ 基法管理 ~ 加用江湖 ~ 内元江海石 ~ 同元34名(原生3) 名	① 約元2組 日本町日度有名に称う"単ない"、年年更和の計畫書、第点点日上 力"市家屋商業定当上"(第五回) 【全主承記記録項用	 ② 安林Quet 型紙県県安全工作(1954) 展示、改革用水は65年84年85年 (東京山田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	 ③ 総理合素単和 合素用和の成式)、株 市 相切の成式)、株 市 相切の成式)、株 市 相切の成式)、株 	助育会及针播和约氮工的人员	II: SORFIERE	REMIFICIP, BOOSMER, CO #	 正元 5 - 12元 0 - 12元 0 - 12元 0 - 12元 0 - 12元町 7
		我繼续订		EERS ~	使用状态 ~	配额D 服务器名称	服务器P	00
		置数1D	配额规格	配额状态	使用状态	绑定服务器	配额到期时间	操作
		05effb1ef2df44cQabe93fc45cb862e9	企业版	正常	未搬定		2022-09-30	续订 退订
		d80a444e1ac24609bd1523bb93e4b96f	全业版	正常	未樹定	-	2022-09-30	续订 退订
		a123ff690c7a4929a0708b6662343bfe	全业物	正常	未绑定	-	2022-09-30	续订 邀订
		0610128a40a446d4920a295b8d9#341	全业版	正常	使用中	Ubuntu16.94D653F4-0805-8EEF-C086-8368 192.168.1.16(ML)	2022-09-30	線灯 港灯

2. 在天翼云控制台中,安全分类下,点击"服务器安全卫士(原生版)":

计图 ~	登場し	関係 ~
(金) 得性元王和(0) 则也可定当时最初为组	云破鏡(0) 按约-95	等 <u>定</u> 唐印码有云(1) 空运 空云编局的图4网络
□□ 1 100 ⁻⁰ 100 ⁻⁰ 100 ⁻⁰ 100 ⁻⁰ 100 ⁻⁰	· 元· 元· · · · · · · · · · · · · · · · ·	
○ 元章應 元中仍成以進品	対象行格(住兵助臣)1型: 利息市谷市(市民大学行社報告告報)	(p) 391122400 (0) 99112240403044
· · · · · · · · · · · · · · · · · · ·		
A00. 增性伸缩服务 口间使物组织		
(國) 专展云 云中哲学教师部派法图图		2. 通信负担协制 多分振发系用自动电振分发
篮球与邮册 ~	於「「「」」 於「」 北保美書 二 立主教品中面称调查系 二 二 立主教品中面称调查系	⑦ 方印刷具(Fackto) (2010年8月 年間)
云窗腔 用资源的, 古聖德和	C 元解析 DIFF60LRHY服然	
[1] 「「二」「「二」」、「二」」、「二」」、「二」、「二」、「二」、「二」、「二」、	WebERERS/XMI/Add/#E0 第2元回归社会中专家	FRIZED-WAN SMACHA, GALLE, MEAZ
	每日元代 场合和行用机元式	○ 云明
应用服务 ~	 研究所構成(係電版)	.W. Виллийнооголсанын
《 國際方法EEII平台 图示一起ChevOpaFi会中间片服用	○ 网页防罐式 国山水中的总目录接守法署改和附环	容器勝利 ~
島現李培 ∽	日本公司(1) 日本公式会同期期代報	Antary without the states

进入服务器安全卫士(原生版)控制台,弹出下方"服务开通申请"对话框:



服务开通申请
服务器安全卫士(原生版)服务开通申请
 开通前请认真阅读《天翼云服务器安全卫士(原生版)服务协议》 服务器安全卫士(原生版)开通后,默认为您开通基础版免费服务,开通即可使用,基础版不支持续订、退订操作。 服务器安全卫士(原生版)开通成功后,服务器默认处于"基础版"防护状态。
□ 我已阅读并同意相关协议《天翼云服务器安全卫士(原生版)服务协议》
退出同意

阅读《天翼云服务器安全卫士(原生版)协议》后,勾选我已阅读并同意签署《天翼云服务器安全 卫士(原生版)协议》,点击"确定"按钮,即可开通服务器安全卫士(原生版)服务,如下图所示:

				购买服务器安全卫士 (原生版)
で び	【 使用紙引 ① 第天在紙 単語的形成 新知識で、 年年度和500万年度、 後の生た 5 7 10年8月6日を定まま (10月10) ▲ 全地家記録使用	P RAyert PREASEY21: (05:8) BS, SUBRISHDYBARKE Aver. Offender Barles Status Reference Status	③ 设置高度通知 合意知知意思,风险分泌が感知は気が入れば、飲みや設置を 素、成功を改正 ① 企业販売額状态	④ 切換版本 由全地需要更成本的加卡,通过抽版本, 切換版本和通知指实验量度 加速度本
	料理時代 「記録の」	記錄現格	配額状态 (2用状态 62回の 配額状态 使用状态 研定服务器	服务部の Q Q Q 配务部の 4/10 株件

点击页面右上方"购买服务器安全卫士(原生版)",进入到服务器安全卫士(原生版)产品购买 页面:



8		订购服务器变全卫士 (原生版)
۲	服务器安全卫士(原生版)	版本选择 全藏版 版本对比信息
© ©	http://display.com/ http://display.com/ for 管理 ^ 版先程列表 · 版介留理 ^ 基线管理 ^ 基线管理 ^ 基线管理 ^ 基线管理 · 私徒管理 · 和口令检测 · 和口令检测 · 和口令检测 · 和口令检测 · 和同時編 · 和助編 · 和助加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加	APWBABAN - 1 + ACSERDATIVISADARE APAT 2018 0018 0018 10018 11018 12 28 1
		±250 €

选择购买版本、防护服务器台数、购买时长、自动续订,勾选我已阅读并同意相关协议《天翼云服 务器安全卫士(原生版)协议》,点击"立即购买"按钮,购买成功后即可在"配额管理"页面查看已 购买的企业版配额,如下图所示:

88		配额管理						9买服务器安全卫士(原生版)			
0	服务器安全卫士(原生版)	【使用施引									
8	安全模	 約天在総 日本時の代表的に知う、私の客、私日本内の日本事、私合止し 力、市政和政府部立上上(第三条)) 全全術記録使用 	② 安装Agent 成用医名型全卫士(伊生斯)图务, 这里来先给你产业务者安培 Agent。把外销员者自己主要者语题。 安装Agent	 ③ 设置告票通知 会常就说没意乐,和 前,请你送设意。 ③ 企业版配额状态 	业等会及时通知给指定的人员	(4) 009664 6555897 20026 00864	MEESSP, HOMEF, OMEFRIAARSBER				
]	総計で 記録第項 両参点が設置	5	- 6月中 2 - 未初定 3			12 at					
		北疆统17		記録状态 ~	使用状态 🗸 🖂	記録D 服务器名称	8务数P	a à			
		回 開始 D	配额规格	配额状态	使用状态	绑定服务器	配額到期时间	操作			
		05effbfef2df44c0abe83fc45cb882e9	企业额	正常	未树定		2022-09-30	续订 进订			
		d80a444e1ac24609bd1523bb99e4b96f	企业版	正常	未期定		2022-09-30	4817 1817			
		a123ff690c7a4929a0705b6662243bfe	金星版	正常	未胡定		2022-09-30	ARIT IBIT			
		0610126a40e446d4920a296b8d9tt341	全並預	正常	使用中	Ubuntu16 94D653F4-0805-8EEF-C086-8388 192.168.1.16(M)	2022-09-30	續订 過订			

4.1.2 手动续订

在"设置中心->配额管理"中查看您已经订购的配额,选择所需续订的配额,点击"续订",如下 图所示:



	配額管理						购买服务器安全卫士(哪生
服务器安全卫士(原生版)	(使用描写)						
安全规定 资产管理 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	① 购买配置 包含的印刷书记程为"单记的"、者有要用的估学意味、现合生在上 为"你呆服书记学上上"(包工程)	② 安裝Agent 使用服务型生生(原生用) 最先,但面積為近的产能先因安保 Apent,在市场服务和行己公式且做。 安積Agent	③ 设置告贸通知 合管通知过重点。风险将会 重、消快速设置。	及对通知给指定的人员,这: 如今未说置告	④ 切换版本 当时空景要要原版本 呈的影響。 切换版本	的历护,请切换版本,1	初换越本面请先购买致量克
病页防箱改(原生版) 设置中心- へ 配額管理	全业级政策使用		企业版配额状态				
同步的广设直	5	- 6095 - 2 - 4092 - 3			12		- 12.7% 5 - C2.0310 0 - C2.0817 7
	RBRT		REALIZE V SERIE	10, v 12, 200 1	E务群名称 图为1	3P	
	一般的の	配線現格	配額状态 佳!	明状态 绑定服务器	1	已粮到期时间	操作
	05effbfef2df44c0abe93fc45cb982e9	企业版	正常 未想	и д —	2	022-09-30	線灯 銀灯
	d80e444e1ac24509bd1523bb89e4b86f	全业版	正常 来想		2	022-09-30	续订 跟订
	a123#690c7a4929e0705b66652343b/e	全业版	正常 未約	12 -	2	022-09-30	续订 进订
	0610126±40=44654020±29559549494341	全世際	正常 使用	日中 Ubuntu16 94D653F4-0	505-8EEF-C066-8368 2	022-09-30	線订 遗订

在下图续订页面中,选择续订时长,勾选我已阅读并同意相关协议《天翼云服务器安全卫士(原生版)协议》后,并点击"立即购买"后即可进行续订。当续订周期达到1年或以上时,续订单将可享受 包年折扣,续订金额显示折后价。

服务器安全卫士(原生版)续订					
配额iD	配额规格	配额状态	使用状态	绑定服务器	配额到期时间
3035bdea3ab44aa1b82e63a3bdfdc4ad	企业版	正常	使用中	ecm-9774 09352FAE-5F9A-4FDF-8CEE-D4C 10.10.1.55(%)	2022-10-22
续订时长 月 🗸 1					
我已阅读并同意相关协议 《天翼云服务器安告》	è卫士 (原生版) 服务协议》				

您也可以对多个配额进行批量续订。在"设置中心->配额管理"中查看您已经订购的配额,选择所 需续订的配额,点击"批量续订",如下图所示:



	配额管理				购买服务器安全工	2± 093.6
服务器安全卫士(原生版)	使用指引					
安全概算 资产管理 ~ 基线管理 ~ 漏洞扫描	 	② 受張Agent 但用原為原文主土(約2.8) 原系、日常見は回り至れ原文書 Agent. 名用有限方面にご定知真正案。	③ 设置告票通知 合置通知设置后,风险符合及时通 量、油件进设置。	(4) UMAGA SEGERAALI: DA4225 SEGERALI: CAMPI	AW+DOP, HOMS+, OMS+EHANG t	6数量充
人はを回め ~ 同页防幕改(原生版) 设置中心 ~ 配額管理	全业级配额使用		全业级配额状态			
同步变产设置	5	- 8000 - 2 - A002 - 3		12	- 13% - 520 - 580	5 II 0 I 7
	RARKT		■ 200 ×	× 2000 服务器名称	雇务部P	0 0
	「「「「」」の「「」」	配额规格	配额状态 使用状态	绑定服务器	配额到期时间 操作	
	05#ftbfet2df44c0abe03fc45ab982e0	205	正常 未認定		2022-09-30 (217 2017	
	d80a444e1ac24609bd1523bb80e4b86f	全山版	正常 未規定		2022-09-30 1217 2017	
	a123ff690c7a4929a0705b0862243bfe	全拉版	正缘 未認定		2022-09-30 #17 #17	
	0610126x40x446rt4920x296bi9rt98341	令计频	7.9 (###	Ubuntu16 94D653F4-0505-8EEF-C066-8368.	" 2022_00_30 (817 #17	

在下图续订页面中,选择续订时长,勾选我已阅读并同意相关协议《天翼云服务器安全卫士(原生版)协议》后,并点击"立即购买"后即可进行续订。当续订周期达到1年或以上时,续订单将可享受 包年折扣,续订金额显示折后价。

19年期中会 五上 (唐片坂) (奈)す					
NYSGXTTT (NXTNK) 2411					
記额D	配额规格	配额状态	使用状态	绑定服务器	配额到期时间
3035bdea3ab44aa1b82e63a3bdfdc4ad	企业版	正常	使用中	ecm-9774 09352FAE-5F9A-4FDF-8CEE-D4C 10.10.1.55(%)	2022-10-22
9c4ba7bf67f5474db4ea8c589e4f98ee	企业版	正常	未揭定	-	2023-11-22
f563c4ddc887473a8ee8f55f759ea00a	企业版	正常	未例定		2025-10-22
款打封长 月 - 1					

4.1.3 自动续订

开通自动续订



步骤1进入"续订管理"页面。

步骤2设置查询条件。

可综合利用到期时间、产品类型、是否开通自动续订查询资源。

由于自动续订两次下单时间为到期前 10 天和前 7 天,建议您选择"到期时间≥10 天","未开通 自动续订"的服务器安全卫士(原生版)。

步骤 3 在资源页面找到待续订的资源,单击操作列的"开通自动续订",如下图所示:

)天興云 🕯	管理中心				投索		Q 中国	站~ 费用	订单	产品 工单	备案 合	作潮感	я 🛐
产品中心	续订管理												资源被财富●
 产品初期 地口管理 	1、支持自动地订例产品范围译员 <u>建造支档</u> 2、规定在当地订闭已完成人工统订、则同一周期 3、对于式方明期的资源、成已期的资源、不去时 4、对于设置了自动地订、目行天内到期的资源 5、此后期的资源、数位订阅期从到面的同开始计算。	內不会與自动條订。 容置將整合自动後订。 服用戶管試得改自动修订問題。关闭自动修订,转提當计會,可能会因为 分别开過自动除订,例如仅对云鄉會當驚負的條订,這總是所住我的云主!	当期自动歧灯已完成而导 机到期运结后,可能导致 机	也变更在本因期不生的 8体服务不可用。	α,								
医曲菌斑	全部3000 7天内到期 10天内到期 到期 前最入资源的电信控制合资源的 高級入口	対詞>>10天 未刻期 已創期 高NA/P品的将数本 中付 ⊙ 2022-08-01 至 20	22-08-30	技 系									
		全部		自动倾订						到期转按需			
	产品名称	资源10/订单号	资源池	资源状态	但行时	续订周期	订购方式	1931年1			操作		
	服务器安全卫士(原生版)	d8/8740cea024bcaa2f84102b9c0ae9 (20220830093841517180)	无	在用	31 天	1个月	包周期	©刨鍵 2 ©到期 2	022-08-30 09:3 022-09-30 09:3	39:40 39:20	手动的 修改目 到期初	的 動態订 波響	>
	服务器安全卫士 (原生版)	36c5589fb28/4e1994e926b2e42da94e (20220830093546106450)	无	在用	31天	π.	包周期	③创建:2 ④到期:2	022-08-30 09.3 022-09-30 09:3	96:26 36:19	手动机 开通自 到期拜	灯 助映订 液開	2

步骤 4 设置"自动续订周期",仔细阅读《天翼云自动续订服务协议》,如果同意全部约定,则勾选"我已阅读并同意遵守《天翼云自动续订服务协议》的约定",单击"确定提交",如下图所示:

→ 天開云 常理中心				授索		Q 中國站	・ 费用	订单 产品 工	单 善案	合作 消息	R
产品中心	续订管理 > 自动续订										资源被批定
▶ 产品级图	 自动坡行订单支付成功后不可服消。 客户专属折扣将在自动坡行下单时自动折算。如常了解专 2、客户专属折扣将在自动按行下单时自动折算。如常了解专 	鋼匠扣評情请联系客户经境,或復打客服法线转1进行 第10天 第7天时和第七角时,周口常常在周期第三时	答例。 extr								
续订管理	3、或量目的保持的期份部份下部转行添加方法,但通过的所 4、客户付费模式全更不够施自动执行设置。例如预付费用户 5、自动独行操作成功后,将取消到期转按需。	第10人、第1人均加强关款时,由户标准在自新用于40 更更为后付费用户后,其资源的自动接订开通状态与续	行還用設置將種種生效。								
退订管理 列举管理	产品名称	资源ID	资源池	资源状态	例后十年月	续订用期		时间		操作后续订两期	
	服务器安全卫士(原生版)	36c5589fb25f4e1994e926b2e42da94e	无	在用	31天		0 @ 0 Ø	(ill: 2022-08-30 09:36:26 (ill): 2022-09-30 09:36:19		1个月	
	服务器安全卫士 (原生版) - •										
	自动续订: 矢闭 🌅 开通										
	续订周期: O 1个月 2个月 续订金额: 36.00 元	3个月 4个月 6个月	6个月 7个月	8个月	9个月	10个月	11个月	1年	24	34	
	我已阅读并同意遵守(天翼云自动读订服务协议)										
	No. disc										

修改自动续订周期

步骤1进入"续订管理"页面。

步骤 2 在资源页面找到待修改自动续订的资源,单击操作列的"修改自动续订"。

€る天露云	: 管理中心							搜索		Q 🕈	国站~ 费用	订单 产品	3 I#	备案	合作	消息		2
	×ΰ	续订管理															资源被制	定€
⊕ ► ##888	289	1、支持自动倾订的产品范围详见 <u>帮助文档</u> 2、如果在自动倾订前已完成人工续订,则同	一周期内不会再自动续订。															
(金) (秋日前)	THE	3、对于7天内到期的资源,或已到期的资源, 4、对于设置了自动续订,目10天内到期的资 5.主成来订购但目有绑定或注载关系的资源	不支持設置/修改日动续订。 1题,如果用户尝试修改自动续订周期。 、需要分别开通自动续订,例如仅对:	关闭自动续订、转按需计 2.硬盘设置自动级订、该硬	· 费,可能会因为当期自动组 虚所社费的云主机到相冻结	(订已完成而导 后、可能导致)	致变更在本周期不生) 修体服务不可用。	k.										
· 通订管理	ERE	6、已到期的资源,新续订周期从到期时间开	始计算。															
50年間	ETAN	全部时间 7天内到期 10天内到期	到期时间>=10天 未到期	EBDI IAMAA	品名称搜索													
Ô		请输入资源D或控制合资源D	加入订单号	③ 2022-08-01	至 2022-08-30		HERE											
© 			全部				自动续订						到期转按需					
		产品名称	资源ID / 订单号			资源池	资源状态	倒计时	续订用期	订购方式	时间			1	操作			
		服务器安全卫士 (原生版)	d8f8740cea024b (2022083009384	caa2ff84f02b9c0ae9 11517180)		无	在用	31天	1个月	包周期	〇创雄:2 〇到期:2	022-08-30 09:39:40 022-09-30 09:39:20		Ģ	手动续订 修改自动续订 到期转按需	ī	>	



步骤 3 拖动"续订周期"可修改自动续订周期。

3天翼云 管理中心	i			被索		Q 中国站	- 费用 计	订单 产品 工의	1 备案	合作 消息	я 🦻
产品中心	续订管理 > 自动续订										338820 0
▶ 产品报题	 自动倾订订单支付成功后不可取消。 套户专属折扣将在自动按订下单时自动折算。如 	需了解专 属 折肌详销清职系备户经理。或原打套服热线转1进行咨	а.								
续订管理	 近重日市項目的預付費用戶審保持來額充定。当 各户付書模式充更不影响自动吸订设置。例如發 自动哑订操作成功后,将取运到期转按照。 	遭到順便藥10天,第7天均但費失數則,用戶符審在對單面手頭保 因費用戶变更为后付費用戶后,其資源的自动被订并通状态与接订	1日。 1問期设置将继续生效。								
ati就通 除中營道	产品名称	资源ID	资源地	资源状态	倒计时	续订用期		时间		操作后续订周期	
	服务器安全卫士 (原生版)	d8f8740cea024bcaa2ff84f02b9c0ae9	无	在用	31天	1个月	() 创 () 到	建: 2022-08-30 09-39-40 期: 2022-09-30 09-39-20		7个月	^
	服务器安全卫士(原生版)										
	自动续订: 关闭 🍋 开通										
	1个月 2个月 续订金额: 252.00 元	3个月 4个月 5个月	6个月 7个月	8个月	9个月	10个月	11个月	tá:	24	34	
	 我已阅读并同意道守《天真云自动放订提》 我注意文 取消 	\$1920 									

步骤 4 勾选"我已阅读并同意遵守《天翼云自动续订服务协议》的约定",点击"确定提交"。

关闭自动续订

步骤1进入"续订管理"页面。

步骤 2 在资源页面找到待修改自动续订的资源,单击操作列的"修改自动续订"。

公天第三	管理中心						搜索			中国站~	费用 订4	単 产品	工単	备案	合作	消息		2
	5	续订管理															资源被制	定●
● 产品税器	1	 支持自动续订的产品范围详见<u>帮助文档</u> 如果在自动续订前已完成人工续订,则同一周期内存 	~会再自动续订。															
(STEN	1	3、对于7天内到期的资源,或已到期的资源,不支持设 4、对于设置了自动级订,目10天内到期的资源,如果1 5、非成套订购但具有绑定或挂载关系的资源,需要分别	置/修改日初级订。 目户尝试修改自动级订周期、关闭自动级订、转按需计费 开调自动级订,例如仅对云哪盘设置自动级订,该硬盘	F. 可能会因为当期自动领订 所挂载的云主机到期冻结后。	已完成而导致 . 可能导致数	g变更在本周期不生效 MK服务不可用。												
·2 送订前班		6、已到期的资源,新续订周期从到期时间开始计算。																
新単語環		全部时间 7天内到期 10天内到期 到期时间	D>=10天 未到期 已到期 请输入/26	8合称搜索 ~														
e		请输入资源D或控制合资源ID 请输入订单	G 2022-08-01	至 2022-08-30		18500												
0						malan						70	(100000000					
38			50°			1014059c3J						20	140451696					
		产品名称	资源ID / 订单号		资源池	资源状态	倒计时	续订周期	订购方式	it D	时间			损	H作			
		服务器安全卫士 (原生版)	d8f8740cea024bcaa2f84f02b9c0ae9 (20220830093841517180)		无	在用	31 天	1个月	包周期		③创建:2022-08-3 ③到期:2022-09-3	30 09:39:40 30 09:39:20		手 他 至	F动续订 B改自动续订 则期转按需	ī	>	

步骤 3 点击"自动续订"后方的关闭/开通按钮,单击"确定提交"。

天翼云 管理中	×0			搜索		Q 中国站~	費用 て	7单 产品	Тŧ	後期 合作	消息	ेष <mark>ह</mark>
产品中心	续订管理 > 自动续订											资源被印度
 产品规则 续订答理 	 自动使订订单支付成功后不可取消。 客户专属折扣将在自动使订下单时自动折锁。 设置自动块订的预付费用户需评持未要方法。 客户 ተ营业式定要不影响自动块订设器。例如 	10第7號を履折印译碼语联系者户经理,或與打客服供结转1包行咨询。 含辦到關南第10天、第7天均指擔失敗时,用戶帶著在到期前干涉條訂。 例付數用戶來更为后付費用戶售,其资源的自动指訂开递成本与後订到	明设窗词提续生效。									
間に丁酸物	 自动接订操作成功后,将取前到顺转投算。 产品名称 	资源ID	资源地	资源状态	倒计时	续订周期		时间		3	操作后续订阅期	E.
heega	服务器安全卫士 (原生版)	d8f8740cea024bcaa2ff84f02b9c0ae9	无	在用	31天	1个月	() () () ()	#: 2022-08-30 09-39- F: 2022-09-30 09-39-	40 20		7个月	
	服务器安全卫士(原生国	0 : -										
	自动续订: 关闭 🔵 开道											
	我已阅读并同意遵守《天翼云自动读订报	最多协议》										
	101410.00 B239											

4.1.4 退订

在"设置中心->配额管理"中查看您已经订购的配额,选择所需退订的配额,点击"退订",如下 图所示:



	配额管理						购买服务器安全卫士 (原生
服务器安全卫士(原生版)	使用指引						
安全根览 第产管理 ~ 基础管理 ~ 選用扫描	() BARM STRUGGEROTION, STRUGTER, HAARL N'BARMEREZ'T (STR)	(2) SEAgent REMEASENCE IN THE DESCRIPTION OF A DESCRIPTION Agent. EVERENCE OF SEARCH SEARC	③ 设置告赞通知 告告通知设置后,风险将 管,清快速设置。	给及时通知给你定的人员 这:它将未必重要	 ④ 切換版本 当者志宗養更高 足的配部。 切換版本 	版本的防护,通切换版本,	切換版本前请先购买数量克
(供給測 ~ (()))(())(()()()()()()()()()()()()()()	全业委配题使用		企业版配额状态				
同步资产设置							
		5 a 1997 2 a 1992 3		(12 38		— Еля 5 — Сызын 0 — емяст 7
	LUNT:	5 a 492 2	REH.C ~ C	RK5 v KB0	12 .a	服务部門	- E270 5 - CEUM 0 - E2981 7
		5 a 4927 2 a 4922 3	RENEYS -	市社会 / 私知の 使用状态 が定販券者	12 38	能動制料	 二次 5 - C20日 0 - C20日 7
		5 a 4927 2 a 4922 3	■ 2x 1	和化さ ~ 私知o 使用状态 が定版を引 44英2 ~	12 .a	能急速产 配额到期时间 2022-00-30	- 377 5 - 12月1日 0 - 12月1日 7 - 12月11日 7 - 12 11 11 11 11 11 11 11 11 11 11 11 11 1
	EERT EERT CommunitySet400440314502450246 0064564411x25020012228269440941	5 2 2 3 5 5 5 5 5 5 5 5 5 5 5 5 5	 私知水5 ~ (4) 私祖水5 ~ (4) 王京 4 王京 4 王京 4 	NUC5 ン 私助の 取用状态 対応服务部 実現定 実現定	12 at	総合部門 記録到時时间 2022-09-30 2022-09-30	- 1377 5 - 02581 0 - 02587 7 - 02687 7 - 02687 7 - 02687 - 02687 - 02687 - 02687 - 02687 - 02687 - 02687 - 02687 - 02688 - 026888 - 02688 - 026888 - 02688 - 026888 - 0268888 - 0268888 - 0268888 - 0268888 - 0268888 - 02688888
	#ERIC ERIC OhmbarDankoototototototototototototototototototo	5 2 3 5 5 5 5 5 5 5 5 5 5 5 5 5		RUCS V 記知の 使用状态 対応服务部 終期定 未規定 未規定	12 32	 記録型時時间 記録型時時间 2022-09-30 2022-09-30 2022-09-30 2022-09-30 	- 1377 5 - (2578 0 - (25787 7 - (2578 7 - (

在下图退订页面中,选择退订原因,勾选我已确认本次退订金额和相关费用后,并点击"退订"后 即可进行退订。

产品中心	退订管理 > 退订申请						
 产品規制 位に其後 追い並用 	進订第21: 1. 超订成功后资源不可恢复: 2. 微计通过问题,这只是成数器合价或者数据计科 3. 影特殊的说: (工作组、云明编语考定或常言 4. 固订可能会考察试验存在会发来是分子。 通订规则请考着: <u>通订规则资源</u> 按订可以进行 0.2 十元天在曲组数	5; 27 品。道订后资源立即释放)以外,道订后的资源将被以添结形3 间。	《保留15天运释放 ;				
314 BAE	产品名称	资源ID	资源池	资源状态	时间	产品金额	可過订金額
	服务器安全卫士 (原生版)	36c5589fb25f4e1994e926b2e42da94e	无	资源已启用	 ③ 創建: 2022-08-30 09:36:25 ④ 劉期: 2022-09-30 09:36:19 		
	服务器安全卫士 (原生)	Ð : •					
	"请选择跟订方汉: 《 影庆云晚外时动情参数 (承重、时先、台 《 里想势文城行大局、不满是业务海求 》 其他五路为有的性幼儿来高 《 医试验解取误 、 正是外达场子式传载 》 其他	89)				- 39-2 <i>0</i>	产品金额: 36. 可退订金额: 33.0 以本次进订金额和相关费用 1 取消


4.2. 安全概览

安全概览分为最近7日待处理风险、防护状态、风险趋势、实时动态四大模块,如下图所示。

	安全構筑	潤 /* 更新日期: 2022-08-29 13:53:54 同步素/*
 服务器安全卫士(原生版) 	最近7日待处理风险	防护状态
 ● 受金概況 ● 受金概況 ○ 市产管理 ~ ■ 基线管理 ~ ■ 漏別扫描 → 446年 ~ 	● 1 □ □ 0 □ 114 □ 0 NREER((*) ◎ 1 □ □ 0 □ □ 114 □ 0 NREER((*) RREER((*) RREER((*) RREER((*) □ 1 □ □ 0 □ □ 0 □ □ 0 □ □ 0	2 REASE (8) 2 2 REASE (8) 2 2 REASEP (8) 2 2 REASEP (8) 2 2 REASEP (8) 2 REASEP
网页防篡改 (原生版) 设置中心 ~	[风险趋势]	双 转动态 土地 斯 德汗动 别用时间 结件
	120	Cent/05/75 14/194146-0106 Mittage 2022-08-25 17/53.15 REF# Cent/05/75 14/194146-0106 Mittage 2022-08-25 17/53.15 REF#
	80	Conc0275 1478F410-018C 単純同胞 2022-08-25 17:53:12 配音評核 Conc0275 1478F410-018C 単純同胞 2022-08-25 17:53:12 配音評核
		Cem05751478F416-D18C 截线风险 2022-08-2517:53:12 夏香祥林 192188.1.3(%)
	24 25 28 27 28 29	Cent0575 1478F416-D18C 192168.1.3(私) 截线风险 2022-08-25 17:53:12 章管详统
	一入現於到 一 施利和於 一 安全基地 一 與氘防蓄液	共6条 < 1 > 前任 1 页

最近7日待处理风险:展示您服务器最近7日的风险统计,和对应服务器情况的统计。

防护状态:展示您服务器的防护情况统计。

风险趋势:展示您服务器风险情况的折线统计图。

实时动态:展示您服务器的实时风险动态。

4.2.1 最近7日待处理风险

最近7日待处理风险			
入侵检测(个) ① 1	漏洞风险(个)	安全基线(个)	网页防篡改(个) ①
风险主机(台) <u> </u> (台)	风险主机(台) <u> (台)</u> (台)	风险主机(台)	风险主机(台) <u> </u>

如上图所示,最近7日待处理风险展示您服务器的入侵检测、漏洞、安全基线和网页防篡改风险, 和该项风险对应的服务器数量。

→ 天翼云

入侵检测|风险主机:展示7日内所有未操作的入侵检测事件个数,点击数字时会跳转到"入侵检 测->异常登录"首页;风险主机统计7日内有入侵风险的服务器,包括所有的云主机和物理机,同一台 服务器有不同的入侵风险时不重复叠加。

漏洞风险|风险主机:展示7日内所有未操作的漏洞风险个数,点击数字时会跳转到漏洞扫描首页; 风险主机统计7日内有漏洞风险的服务器,包括所有的云主机和物理机,同一台服务器有不同的漏洞风 险时不重复叠加。

安全基线|风险主机:展示7日内所有未操作的安全基线个数,包括基线检测和弱口令检测个数之和, 点击数字时会跳转到基线检测首页;风险主机统计7日内有基线风险的服务器,包括所有的云主机和物 理机,同一台服务器有不同的基线风险时不重复叠加。

网页防篡改|风险主机:若您订购了网页防篡改(原生版),展示7日内所有未忽略的文件异常的事件数,点击数字时会跳转到服务器安全卫士检测首页;风险主机统计7日内有网页篡改事件的服务器,包括所有的云主机和物理机。若您未订购网页防篡改(原生版),则统计数字均显示为0。

防护状态	2						
	主机总数(台) 5		企业版防护(台) 3		基础版防护(台) 2 升级企业版	(+)	防护中(台) 5
ੁ	已关闭(台) 0	Ě	已离线(台) 〇	Ě	未安装客户端(台) <mark>0</mark> 安装Agent		

4.2.2 防护状态

如上图所示,防护状态展示您所有服务器的防护情况。

主机总数:展示您的服务器总数,包括所有的云主机和物理机,点击数字时会跳转至"服务器列表-全部主机"页面。主机总数和以下几种状态的主机数相加总和相等。

企业版防护:展示您使用企业版规格配额防护的主机数量,点击数字时会跳转至"服务器列表-企业 版主机"页面。

基础版防护:展示您使用基础版规格配额防护的主机数量,点击数字时会跳转至"服务器列表-基础 版主机"页面。

防护中:服务器防护状态为"防护中"的服务器数量统计,点击数字时会跳转至"服务器列表-已防 护主机"页面。



已离线: 服务器防护状态为"已离线"的数量统计,点击数字时会跳转至"服务器列表-已离线主机" 页面。

已关闭:服务器防护状态为"已关闭"的数量统计,点击数字时会跳转至"服务器列表-已关闭主机" 页面。

未防护:服务器防护状态为"未防护"的数量统计,点击数字时会跳转至"服务器列表-未防护主机" 页面。

Linux 系统安装命令如下图:

安装Agent	×
Linux系统 Windows系统	
支持的OS版本	
CentOS(64位): CentOS 6, CentOS 7和CentOS 8 Ubuntu(64位): Ubuntu 16, Ubuntu 18 Windows(64位): Windows 2008, Windows 2012和Windows 2016	
在您的服务器中以管理员权限执行以下命令进行安装 curl -k -s -L 'http://169.254.169.254:5662/download/eShield–agent/eShield–install–agent.sh'lbash	
复制 关闭	

Windows 系统安装命令如下图:

安装Agent	×
Linux系统 Windows系统	
安装方式	
1、远程登录到服务器。 2、请用浏览器访问http://169.254.169.254:5662/download/msi/CTCSSInstaller.msi,下载最新Agent到服务器,以管理员权限运行Agent安装程序	F
提示:通过IE浏览器访问时需要将用到的网站加入受信任的站点。	
关闭	



4.2.3 风险趋势



如上图所示,风险趋势展示您所有服务器的风险统计折线图。

为您展示入侵检测、漏洞风险、安全基线、网页防篡改的风险趋势,可以展示近7天、近14天、近 30天的统计折线,默认展示近7天统计折线图。网页防篡改的统计折线需要您订购了网页防篡改,否则 无该统计。

近7天:以当前时间向前推7天,分别展示入侵检测、漏洞风险、安全基线、网页防篡改的风险个数,每天展示一个统计点。

近 14 天: 以当前时间向前推 14 天,分别统计入侵检测、漏洞风险、安全基线、网页防篡改的风险 个数,每天展示一个统计点。

近 30 天: 以当前时间向前推 30 天,分别统计入侵检测、漏洞风险、安全基线、网页防篡改的风险 个数,每天展示一个统计点。



4.2.4 最近7日风险动态

实时动态			
主机	事件行为	发现时间	操作
ecm-4743 ACD75A59-39CC-42E8-8432-EF 172.31.0.208(私)	网页篡改	2022-07-26 14:42:29	查看详情
ctcss-server-0-1 53BA6C27-2461-4D6D-9 192.168.16.226(私)	网页篡改	2022-07-25 14:26:18	查看详情
ctcss-server-0-1 53BA6C27-2461-4D6D-9 192.168.16.226(私)	网页篡改	2022–07–25 14:26:18	查看详情
ctcss-server-0-1 53BA6C27-2461-4D6D-9 192.168.16.226(私)	网页篡改	2022–07–25 14:26:18	查看详情
ctcss-server-0-1 53BA6C27-2461-4D6D-9 192.168.16.226(私)	网页篡改	2022–07–25 14:26:18	查看详情
		共 1	5条 < 1 2 > 前往 1 页

如上图所示,最近7日风险动态风险趋势展示您所有服务器的未处理的风险动态。

为您展示未操作的异常登录、暴力破解、漏洞风险、基线检测、弱密码检测、服务器安全卫士的实 时事件,包括服务器、事件行为、发现时间、操作,分页进行展示。点击"查看详情"时,跳转至相应 的事件主页面。

4.3. 资产管理

资产管理分为概览、服务器列表、资产指纹3大模块,如下图所示。



	板定				87*8346381 2022-08-11 12:59:48
	1 资产概况				
服务器安全卫士(原主版) 取其 资产管理	. mm (m) ⊒ 36	B6 (71	A 111	an (*) 95	885 (*)
毗 放 服务器列表	I IKHKRANAME		服务器区规统计Top5		
 京产鉄改 基式管理 承试电源 第二号位第 第二号位第 第二号位第 ※ ※ ※ 第二号位第 ※ ※ 第二号位第 ※ ※ ※ 第二号位第 	** ** **	- 427/01 - Wales - 120/01 - 127/0200	212 2144 EMR	31	- 6,86 (7) - 6,86 (4) - 6,852 (4) - 6,864 (3) - 6,863 (3)
设置中心 个 同步资产设置	I MICITop6		亚相更多 账号Top5		<u></u>
	1) 22(shd) 2) 25(snate) 3) 49158(seh) 4) 10010(sec) 3) 4916(seh)			shid anater and a shift and a	
	過程Top5		2010月3 欧伟Top5		2823
	1 eShield m 2 ctcs-agen 3 ctcs-agen 4 python2.exe 5 win32.u.exe			TCSS Age	

- 4.3.1 概览
- 1) 资产概况

资产概况				
主机 (绘) 36	潮口 (个) 86	^{服号 (介)} 名 111	通程(个) ≌ 95	数件 (介) デ 85
如上图所示,资	^立 概况为您展示服务	务器和资产指 纹的统订	十情况。	
主机台数: 您服	务器的总台数,单击	占蓝色数字时跳转到	"服务器列表"页;	

端口:展示所有服务器所有已使用端口的数量之和,单击蓝色数字时跳转至"资产指纹-端口"页;

账号:展示所有服务器所有账号的总数量,单击蓝色数字时跳转至"资产指纹-账号"页;

进程:展示所有服务器所有进程的数量之和,单击蓝色数字时跳转至"资产指纹-进程"页;

软件:展示所有服务器所有软件应用的数量之和,单击蓝色数字时跳转至"资产指纹-软件应用"页。

2) 主机概况趋势图





如上图所示,主机概况趋势图为您展示服务器的防护情况统计折线图。

为您展示服务器总台数、未防护台数、离线台数、风险台数、防护关闭台数统计趋势,分近7天、 近14天、近30天3个选项,默认展示近7天。

近7天:以当前时间向前推7天,分别进行统计,每天统计一个总数显示。近14天:以当前时间向 前推14天,分别进行统计,每天统计一个总数显示。近30天:以当前时间向前推30天,分别进行统计, 每天统计一个总数显示。

总台数:包括全部服务器,每天统计一个值。 未防护台数:防护状态为"未防护"的服务器,每天统计一个值。 离线台数:防护状态"已离线"的服务器,每天统计一个值。 风险台数:风险状态为"风险"的全部服务器,每天统计一个值。 防护关闭台数:防护状态"已关闭"的服务器。

3) 服务器区域统计 Top5

服务器区域统计Top5	
41 Am	 内蒙6 17 南京3 13 查港1 4 重庆2 4 成都4 3

如上图所示,服务器区域统计 Top5 为您展示服务器的地域分布统计情况。包括当前全部服务器数量的排名,分别按照资源池进行统计,只展示 Top5。

4) 端口 TOP5



如上图所示,端口 Top5 为您展示服务器开放端口的统计情况排名 TOP5,点击更多时,会跳转至"资 产指纹-端口"页面。

5) 账号 TOP5





如上图所示,账号 Top5 为您展示服务器账号的统计情况排名 TOP5,点击更多时,会跳转至"资产指 纹-账号"页面。

6) 进程 TOP5



如上图所示,进程 Top5 为您展示服务器运行的进程统计情况排名 TOP5,点击更多时,会跳转至"资 产指纹-进程"页面。

7) 软件 TOP5



如上图所示,软件 Top5 为您展示服务器运行的软件应用统计情况排名 TOP5,点击更多时,会跳转至 "资产指纹-软件应用"页。



4.3.2 服务器列表

全部:	E机 风险主机 企业和	§主机 基础版主机	1、 未防护的主机 6	已离线主机								
安装	Agent 批量切换版本						全地利 ~ Agent	15 - NPK5	~ R0085	服务署名称	/ 请输入云服务器户或名称	
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	漏洞风险	安全基线	同页防篡改	操作
	Windows2012 81E26604-FBF9-8 192.168.1.4(%)	windows	内蒙漠示环境	在线	85.9°中	安全	全业版	0	0	0	0	切换版本 开启防护 关闭防护 智能Agent
	Ubuntu16 94D653F4-0605-8EEF 192.168.1.16(%)	linux	内嚴漢示环境	在线	版新中	受金	全业版	0	0	0	0	切换版本 开启热护 关闭防护 卸载Agent
	CentOS76 160D4123-E38F-F6E 192.168.1.8(%)	linux	内蒙演示环境	在线	1539-44	RM	38-013 MS	1	0	50	0	切换版本 开启协护 关闭防护 副机Agent
	windows2008 EBF69C73C5A8-I 192,168.1.6(%)	^I windows	内蒙演示环境	在战	防护中	安全	基础版	.0	0	0	o	切缺版本 并自然中 关闭防护 副和Agent
	CentOS75 1478F416-D18C-011 192.168.1.3(%)	linux	内蒙漠示环境	在线	防护中	风险	13 (15 M)	0	0	64	0	切换版本 开启结护 关闭防护 智载Agent

1) 全部主机

该页面为您展示全部服务器的情况。已销毁的服务器不再展示在列表中。

服务器列表包括以下字段:服务器、操作系统、地域、Agent 状态、防护状态、风险状态、入侵检测、 漏洞风险、安全基线、服务器安全卫士和操作。

服务器包括服务器名称、UUID、私网 IP、公网 IP; Agent 状态包括在线、离线、未激活、错误 4 种; 防护状态包括防护中、已离线、已关闭、未防护 4 种状态;风险状态包括安全、风险、未知 3 种状态; 入侵检测、漏洞风险、安全基线、服务器安全卫士分别展示当前该服务器未操作过的入侵检测、漏洞风 险、安全基线和网页篡改事件数,若您未订购服务器安全卫士,则统计数字均显示为 0;操作包括开启防 护、关闭防护、安装 Agent 和卸载 Agent。

Agent 状态	说明
在线	Agent 控制通路和数据通路均连接正常。
离线	Agent 控制通路连接正常,数据通路连接正常一段时间后异常。
未激活	Agent 控制通路连接正常,数据通路未建立连接。
错误	Agent 控制通路连接异常。

防护状态	说明
防护中	表明该服务器处于正常防护中,此时 Agent 状态为在线且已经为该台 服务器开启防护。



防护状态	说明
已离线	表明该服务器与 Agent 通信异常,此时 Agent 状态为离线或错误。
口头臼	表明该服务器已经关闭防护,此时 Agent 状态为在线且已经为该台服
	务器关闭防护。
未防护	表明该服务器已经关闭防护,此时 Agent 状态为未激活。

风险状态	
安全	表明该服务器无基线、漏洞、入侵和网页篡改的风险。
风险	表明该服务器有基线、漏洞、入侵和网页篡改的一种或几种风险,具 体可查看入侵检测、漏洞风险、安全基线和服务器安全卫士下方的统 计数字。
未知	表明该服务器的基线、漏洞、入侵和网页篡改风险情况未知。

开启防护: 该服务器的防护状态需要为"已关闭"。点击"开启防护",等待几秒后该服务器防护 状态变更为"防护中"。

关闭防护:该服务器的防护状态需要为"防护中"。点击"关闭防护",弹出如下对话框,您选择 "确定"后,等待几秒后该服务器防护状态变更为"已关闭"。

关闭			×
确定对所选服务器关闭防护吗?			
服务器名称	操作系统	防护状态	
ecm-4743	windows	防护中	
	取消 确定		

安装 Agent: 安装 Agent: 点击"安装 Agent",跳转至安装 Agent 页面,分为 Linux 和 Windows 系统的不同安装指令。



Linux 系统安装命令如下图:

安装Agent	×
Linux系统 Windows系统 支持的OS版本	
CentOS (64位) : CentOS 6, CentOS 7和CentOS 8 Ubuntu (64位) : Ubuntu 16, Ubuntu 18 Windows (64位) : Windows 2008, Windows 2012和Windows 2016	
在您的服务器中以管理员权限执行以下命令进行安装 curl -k -s -L 'http://169.254.169.254:5662/download/eShield-agent/eShield-install-agent.sh'lbash	
复制关闭	

Windows 系统安装命令如下图:

安装Agent	×
Linux系统 Windows系统	
安装方式	
1、远程登录到服务器。 2、请用浏览器访问http://169.254.169.254:5662/download/msi/CTCSSInstaller.msi,下载最新Agent到服务器,以管理员权限运行Agent安装程序。	
提示:通过IE浏览器访问时需要将用到的网站加入受信任的站点。	
关闭	

卸载 Agent: Agent 状态为"在线"的服务器有此操作。点击"卸载 Agent", 弹出如下对话框, 您选择"确定"后, 进行 Agent 卸载。



卸载				×
▲ 确定对 卸载Ag	听选服务器进行卸载吗? ent,会使服务器失去安装监	空,处于安装风险中,请您谨慎操作!		
服务器名称		操作系统	防护状态	
ecm-1eb9 7F79A0 DBFDD377 172.31.0.52(私)	C91-B867-49B2-8C56-9F64	windows	防护中	
		取消 确定		

2) 风险主机

器列表										资 ^产 更新日期: 2022-01	3-29 13:53:54 R #
全部主机 <mark>风险主机</mark> 安装Agent 批量切换质	企业版主机 基础版主机	1. 未防护的主机	日离线主机			全线域 ~ Agent	K6 ~ BP85	~ 风险	< 服务総名称 √	请输入云服务物中或名称	0
服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	激调风险	安全基线	同页防篡改	操作
CentOS76 160D4123-E38 192.168.1.8(%)	9F-F0E: linux	内蒙演示环境	在线	防护中	风险	基础版	1	0	50	o	切換版本 开启陆护 关闭防护 卸载Agent
CentOS75 1478F416-D1E 192.168.1.3(%)	9C-011- linux	内酸演示环境	在线	ISS*中	P6.82	基础版	0	0	84	ø	切换极本 开启防护 关闭防护 國幕Agent
									共2条	10条/页 ~ < 1	> 10注 1

如上图展示,风险主机为您展示风险状态为"风险"的服务器。

3) 企业版主机

列表										资产更新日期: 2022-08	-29 13:53:54 R 9
全部主机 风险主机	2业版主机 基础版主机	1、 未防护的主机	已离线主机								
安装Agent 批量切换版=						全地址 · Age	ana ~ Directo	~ Rens	▽ 服务器名称 ○	· 请输入云服系统产业名称	0
服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	演词风险	安全基线	同页防篡改	操作
Windows2012 81E28604-F 192,168.1.4(%)	8F9-E windows	内蒙漠示环境	在线	防护中	安全	企业线	o	o	o	0	切映版本 开启助护 关闭防护 卸载Agent
Ubuntu16 94D653F4-0605- 192.168.1.16(8)	SEEF Inux	内酿课示环境	在线	防御中	安全	企业版	0	o	o	0	切映版本 开启助护 关闭助护 即和Agent

如上图展示,企业版主机为您展示配额规格为"企业版"的服务器。

4) 基础版主机



服务器	根										書产更新日期: 2022-08-	29 13:53:54
á	郁主机 风险主机 企业	发主机 基础版主机	未防护的主机 已算	拔主机								
	RigAgent 就量切换版本						全地域 ~ Ag	ontikā v Birkā	~ Revs	/ 服务器名称 /	请输入云服务费印或名称	0 0
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	灌洞风险	安全基线	网页防篡改	操作
	CentOS76 16DD4123-E3BF-F68 192.168.1.8(私)	5 linux	内蒙漠示环境	在成	際把中	风险	基础版		0	50	0	切換版本 开启防护 关闭防护 卸载Agent
	windows2008 EBF69C73-C5A8- 192.168.1.6(制)	{ windows	内酿灌示环境	在线	前# ¹ 中	安全	重动态	0	0	0	0	切换版本 开启防护 英间防护 卸载Agent
	CentOS75 1478F416-D18C-011 192.188.1.3(%)	l. linux	内蒙漠示环境	在线	防护中	风险	基础版	o	0	64	0	切换版本 开启防护 关闭防护 卸载Agent
										共3条 1	0条/页 < 1	> 前往 1 页

如上图展示,基础版主机为您展示配额规格为"基础版"的服务器。

5) 未防护的主机

安装	Agent 批量切换版本			全地域 ~	Agent状态	~ 防护状态		风险状态 🗸	服务器名称	~ 请输入;	云服务器中或名称	0 0
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	配额版本	入侵检测	漏洞风险	安全基线	网页防篡改	操作
	ecm-ad97-0001 8FC2C7DB-1F1 192.168.0.192(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-ad97 C88BD603-D272-45A 192.168.0.56(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agant
	ecm-a060 D5273532-8F20-47F5 192.168.0.19(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	o	0	0	o	切换版本 开启防护 关闭防护 安装Agent
	ecm-b57e 228A09D8-D8E3-440 192.168.0.124(私)	linux	贵州公共测试	未激活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护 关闭防护 安装Agent
	ecm-cd3d AD6C8A31-F436-458	linux	唐州公共测试	未邀活	未防护	未知	基础版	0	0	0	0	切换版本 开启防护

如上图展示,未防护的主机为您展示防护状态为"未防护"的全部服务器。

6) 已离线主机

全部	主机 已防护主机 已关	闭主机 已离线主机	未防护的主机									
安装	&Agent					全地域 >	在线 🗸	风险状态	服务器名称 🗸	请输入云服务器P或名称		
	服务器	操作系统	地域	Agent状态	防护状态	风险状态	入侵检测	漏洞风险	安全基线	网页防篡改	操作	
	ctcss-server-0-1 53BA6C27-246 192.168.16.226(私)	linux	南京3	南线	已离线	风险	o	٥	0	0	开启防护 安装Agont	eranan

如上图展示,已离线主机为您展示防护状态为"已离线"的服务器。

4.3.3 资产指纹

1) 端口

こ 美美

理产指纹					
端口(86) 账户(111) 进程(95	i) 软件应用(85)				
				□ 服务器名称 ∨ 请输入担	1家条件 Q Q
服务器	操作系统	端口号	网络协议	监听IP	监听进程
ecm-4743 ACD75A59-39CC-42E8-8432 172.31.0.208(私)	windows	49160	tcp6	n	svchost.exe
ctcss-server-0-1 53BA6C27-2461-4D6 192.168.16.226(私)	linux	7000	tcp6	z	frps
ctcss-server-0-1 53BA6C27-2461-4D6 192.168.16.226(私)	linux	631	tcp6	±1	cupsd
ctcss-server-0-1 53BA6C27-2461-4D6 192.168.16.226(私)	linux	3350	tcp6	in .	xrdp-sesman
ctcss-server-0-1 53BA6C27-2461-4D6 192.168.16.226(私)	linux	3389	tcp6	H.	xrdp
ctcss-server-0-1 53BA6C27-2461-4D6 192.168.16.226(私)	linux	25	tcp6	:1	master
ecm-36c1 65DC6E37-E17C-4916-ACD5 172.31.0.98(私)	linux	22	tcp6	÷	sshd
ecm-1c9b-0001 3273F5E8-87AB-410D 172.31.0.166(私)	linux	25	tcp6	:1	master
ecm-1eb9 7F79AC91-B867-49B2-8C56 172.31.0.52(%)	windows	49158	tcp6	ii.	svchost.exe
ecm-5fac 65626726-CEC9-46D2-A452 172.31.0.187(私)	linux	1443	tcp6	8	docker-proxy
			共	86条 10条/页 -> < 1 2 3 4 5	6 … 9 > 前往 1 页

按服务器展示端口信息,包括以下字段:服务器、操作系统、端口、网络协议、监听 IP、监听进程、 进程号。可以按照端口号、服务器名称、服务器 IP 进行搜索。

服务器包括服务器名称、UUID、私网 IP 和公网 IP。

2) 账号

こ 美美

「指纹								
端口(86) 账户(111)	进程(95) 软件应用(85)							
					用户名 服务器名	除 ∨ 请输入搜索条件		0
服务器	操作系统	用户名	设置密码	用户组	到期时间	上次登录时间	上次登录IP	
ecm-4743 ACD75A59-39CC 172.31.0.208(私)	windows	Guest	否	Guests	永不过朝			
ctcss-server-0-1 53BA6C27 192.168.16.226(私)	linux	gnome-initial-setup	否	gnome-initial-setup	永不过期			
ctcss-server-0-1 53BA6C27 192.168.16.226(私)	linux	nfsnobody	否	nfsnobody	永不过期			
ctcss-server-0-1 53BA6C27 192.168.16.226(抵)	linux	secure	是	wheel	永不过朝	2022-07-11 09:01:19	203.57.225.53	
ctcss-server-0-1 53BA6C27 192.168.16.226(私)	linux	gdm		gdm	永不过朝	2022-07-06 15:56:31		
ctcss-server-0-1 53BA6C27 192.168.16.226(私)	linux	avahi	8	avahi	永不过朝			
ecm-1c9b-0001 3273F5E8 172.31.0.166(私)	linux	secure	是	wheel	永不过期	2022-06-13 12:34:32	172.31.0.187	
ecm-1eb9 7F79AC91-B867 172.31.0.52(私)	windows	Guest	8	Guests	永不过期			
ecm-5fac 65626726-CEC9 172.31.0.187(私)	linux	sock	A	sock	永不过朝			
ecm-5fac 65626726-CEC9 172.31.0.187(私)	linux	secure	是	wheel	永不过期	2022-06-13 15:56:12	36.111.64.84	
				共 11	11 条 10条/页 ~ < 1	23456.	12 > 前往	1 页

按服务器展示账号信息,包括以下字段:服务器、操作系统、用户名、设置密码、用户组、到期时间、上次登录时间、上次登录 IP。可以按照用户名、服务器名称、服务器 IP 进行搜索。

3) 进程

产指纹											
端口(86) 账户(111)	进程(95) 软件应	用(85)									
						进程名	ł	服务器名称	< │ 请输入援	康条件	0
服务器	操作系统	进程名	进程路径	启动参数	启动时间		运行用户		进程号	父进程	
ecm-4743 ACD75A59-39 172.31.0.208(私)	windows	python2.exe	C:\Python27\python2.exe		2022-08-11	19:42:15	Administrat	tors	996	2284	
ctcss-server-0-1 53BA6C 192.168.16.226(私)	linux	kworker/1:0			2022-08-11	19:12:01	root		31119	2	
ocm-1c9b-0001 3273F5E 172.31.0.166(私)	linux	eShield-modules	/var/ctcss/bin/eShield		2022-08-11	17:33:11	root		31088	1	
ecm-1eb9 7F79AC91-B8 172.31.0.52(私)	windows	ctcss-agent.exe	C:\Program Files (x86)\ct		2022-08-11	16:52:33	Administrat	tors	1748	468	
ecm-5fac 65626726-CEC 172.31.0.187(私)	linux	python	/uar/local/bin/python3.6		2022-05-23	15:58:43	root		27532	27514	
ecm-5fac 65626726-CEC 172.31.0.187(私)	linux	celery	/usr/local/bin/python3.6		2022-05-23	15:59:04	root		27737	27521	
ecm-5fac 65626726-CEC 172.31.0.187(私)	linux	celery	/usr/local/bin/python3.6		2022-05-23	15:59:04	root		27735	27521	
ecm-5fac 65626726-CEC 172.31.0.187(私)	linux	kworker/u16:1			2022-08-11	13:27:24	root		32351	2	
ecm-88ab-0001 6F33DB9 172.31.0.73(私)	linux	kworker/0:0			2022-08-11	15:20:31	root		30735	2	
acm-1c9b-0004 D5D61C 172.31.0.136(私)	linux	agetty	/usr/sbin/agetty		2022-08-05	13:58:10	root		29843	S18	
					共名	5条 10条	/页 ~	1 2	3 4 5	6 ··· 10 >	前往 1



按服务器展示进程信息,包括以下字段:服务器、操作系统、进程名、进程路径、启动参数、启动 时间、运行用户、进程号、父进程。可以按照进程名、服务器名称、服务器 IP 进行搜索。

4) 软件

资产指纹				
端口(86) 账户(111) 进程(95) 💲	文件应用(85)			
			软件名称 服务器名称 >>	请输入援索条件 Q C
服务器	操作系统	软件名称	软件版本	最后更新时间
ecm-4743 ACD75A59-39CC-42E8-8432-EF91DF 172.31.0.208(指)	windows	CTCSS Agent	4.0.0	2022-07-21
ctcss-server-0-1 53BA6C27-2461-4D6D-9B82-A 192.168.16.226(私)	linux	librsvg2	2.40.20-1.el7	2022-05-31 16:50:05
ctcss-server-0-1 53BA6C27-2461-4D6D-9B82-A 192.168.16.226(私)	linux	python-enum34	1.0.4-1.el7	2022-05-31 18:48:02
ecm-1c9b-0001 3273F5E8-87AB-410D-850A-D5 172.31.0.166(\bar{L})	linux	kexec-tools	2.0.15-13.el7	2020-05-19 15:58:03
ecm-1eb9 7F79AC91-B867-49B2-8C56-9F64DB 172.31.0.52(私)	windows	CTCSS Agent	4.0.0	2022-07-26
ecm-5fac 65626726-CEC9-46D2-A452-8ACB979 172.31.0.187(抵)	linux	kexec-tools	2.0.15-13.el7	2020-05-19 15:58:03
ecm-88ab-0001 6F33DB99-4614-4DBC-8AD9-7 172.31.0.73(%)	linux	openssh-clients	7.4p1-21.el7	2020-09-04 16:54:37
ecm-1c9b-0004 D5D61C22-C5C5-4074-AD79-F 172.31.0.136(指)	linux	virt-what	1.18-4.el7	2020-05-19 15:57:58
ecm-1c9b-0004 D5D61C22-C5C5-4074-AD79-F 172.31.0.136(抵)	linux	firewalld	0.4.4.4-14.el7	2020-05-19 15:58:01
ecm-f6f8-test 1C678D56-9CCC-4740-8BAE-6A5 172.31.0.95(%)	linux	systemtap-client	4.3-4.el8	2021-03-29 14:58:59

共85条 10条/页 < 1 2 3 4 5 6 … 9 > 前往 1 页

按服务器展示软件应用信息,包括以下字段:服务器、操作系统、软件名称、软件版本、最后更新 时间。可以按照软件名称、服务器名称、服务器 IP 进行搜索。

4.3.4 资产详情

当点击服务器名称时,跳转至该服务器的 "资产指纹详情"页面上,如下图所示。上方展示该服务器的基本信息,包括服务器名称、服务器 ID、所在区域、公网 IP、内网 IP、镜像、创建时间、到期时间和防护状态。下方展示该服务器的资产指纹和风险情况。



资产指纹 💈 🛛	問 ^內 指纹详情			
详情				
	CA.	名称:ecm-4743	ID: ACD75A59-39CC-42E8-8432-EF91DF9B5154	所在区域:成都4
		公网吧:	内网IP:172.31.0.208	镜像 :
		創建时间: 2022-07-22 01:30:59	到期时间:2023-01-22 01:30:59	防护状态:防护中
资产指纹	入侵检测 漏洞扫描 基线管理	网页防篡改		
(業内)	账号 进程 软件			
	101 0 101 000 000 000 000 000 000 000 0			
總口是		5月4年十九3 11	ith risk in	1년 8년 2월 20
40154			un el u	
49154		тере	8	svcnost.exe
49160		tcp6	2	svchost.exe
49158		tcp6	1	services.exe
49157		tcp6	2	Isass.exe
49153		tcp6	8	sychost.exe
49155		tcp6	2	spoolsv.exe
				开6条 10条/贝 ◇ 〈 1 〉 前往 1 页

1) 端口

如上图所示,展示该台服务器开放的端口详情。

2) 账号

1								
	名	段:ecm-4743	ID : ACD75A59-39CC-42E8-843	32-EF91DF9B5154	所在区域:成都4			
	公	MIP :	内网 (P: 172.31.0.208		镜像:			
	81	建时间:2022-07-22 01:30:59	到期时间:2023-01-22 01:30:59		防护状态:防护中			
指数 入侵检测 漏洞扫描	基线管理 网页防第	22						
前文 入侵检测 漏洞扫描 和	基线管理 网页防器	改				J	用户名	Q
(1) 入侵检测 漏洞扫描 (1) 机等 进程 软件	基线管理 网页防御 设置密码	政用户组	31JN011 (4)	上次登录时间	-	j 上次登录IP	用户名	Q
Bit 入侵检测 混测扫描 EI 瓶等 进程 软件 户名	基线管理 网页防第 设置密码 否	改 用户组 Administrators	到期时间 永不过期	上次登录时间 2022-07-21 11:31:31	-	j 上次登录IP	用户者	α

如上图所示,展示该台服务器的账号详情。

3) 进程



资产指纹 〉 资产指纹详情						
详情						
E.	•	名称:ecm-4743 公网P: 创建时间:2022-07-22 01:30:59	ID:ADD75A55 内间IP:172.31 到期时间:202	39CC42E88432EF91DF985154 .0.208 3-01-22 01:30:59	所在区域:成都4 镇像: 防护状态:防护中	
资产指纹 入侵检测 漏洞 第二 账号 选程 软件	扫描 基线管理 网页	防御改				通程会 〇 〇
进程名	进程路径	启动参数	启动时间	运行用户	进程号	父进程
ctcm_agentd.exe	C:\Windows\ctcm\bin\win6-	4\ctc	2022-07-21 11:31:25	Administrators	2340	488
conhost.exe	C:\Windows\System32\conf	nost.exe	2022-08-12 07:46: 1	Administrators	252	1492
					共 2 条 10条/页 🔗	〈 1 〉 前往 1 页

如上图所示,展示该台服务器的进程详情。

4) 软件

资产指纹 > 资产指纹详情				
详情				
	名称:ecm-4743	ID: ACD75A59-39CC-42E8-8432-EF91DF9B5154	所在区域:成都4	
	公阿叩:	内阙IP:172.31.0.208	镜像:	
	创建时间:2022-07-22 01:30:59	到期时间:2023-01-22:01:30:59	防护状态:防护中	
资产指纹 入侵检测 漏洞扫描 基线管理	网页防篡改			
A11-01 02/01 1410 00/01				
1日山 1851年 2014年 2014年				
· · · · · · · · · · · · · · · · · · ·				软件名称 Q C
102-102-179 22.022 23.559	10.0 K +	电二面 经分约		软件名称 Q C
14日11 18579 2014 887 7 软件名称	软件版本	最后更新时间		软件名称 Q Q
NEL NET 2018 NET	软件版本 4.0.0	最后更新时间 2022-07-21		软件名称 Q Q
NELL NETTY Zoter 和TH	软件版本 4.0.0	最后更新时间 2022-07-21	共1条 10条/页 ∨ <	软件名称 ○ C 1 > 前往 1 页

如上图所示,展示该台服务器的软件详情。

5) 异常登录



详情						
	ID : 53BA6C27-246	1-4D6D-9B82-A4B2958DCDCA	所在区域:南京3			
	公閒吧:	内岡沪: 192.168.16.	226	镜像:		
	创建时间:20220228 16:51:46	到期时间:2025-08-	-28 16:51:46	防护状态:防护中		
-						
资产指纹 入侵检测 漏洞扫描 基线管理	网页防篡改					
资产指纹 入侵检测 漏洞扫描 基线管理 第 常 常 系力统容	网页防篡改					
资产指纹 入侵检测 漏洞扫描 基线管理 <u>算文章章</u> 最力级时 和印知中的理	网页防凝改	~四古蜀井		25	paka -	
资产指纹 入侵检测 漏洞扫描 基线管理 用实包杂 图力磁解 称记为已处理	网页的墓改	全部省盟共	型 > <mark>最近三个月</mark> > 全部状	iá ~) 型条道P	型条账号 C	0
 第四产指纹 入侵检测 潮洞扫描 基线管理 第五章 和力統新 株にわられ様 各警类型 登录源P 	网页的篇改 登录地区	全部告誓片 登录账号	2 > 最近三个月 > 全部状 最后登录时间	志 > 型泉源P 状态 操作	2.9.8.9 C	0
 资产指纹 入侵检测 漏洞扫描 基线管理 第常登录 最力级新 希応力已处理 各警类型 登录源P 身常登录 203.57.225.53 	网页防器改 登录地区 中回-广东-*	全部告望共 登录账号 secure	2022-07-08 22:29:24	 ご ・ 登泉部戸 	2 () () () () () () () () () (0
 資产指纹 入侵检測 藻洞扫描 基线管理 新文章を 最力波軒 新ご为已处理 告警类型 登录源P 异常登录 203.57.225.53 	网页防墓改 昼录地区 中四-广东-*	全部告閲共 登录账号 secure	2型 ~ 量近三个月 ~ 全部状 最后登录时间 2022-07-06 22:29:24	 ・ 登录第中	登録版寺 C	8

如上图所示,展示该台服务器的异常登录详情。

6) 暴力破解

資产指纹 > 资产指纹详情							
详情							
	名称:ecm-	f6f8-test	ID : 1C678D56-9	ID : 1C678D56-9CCC-4740-8BAE-6A52F48CB33A			
	〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇 〇			.31.0.95 镜像:			
	创建时间:2	022-07-12 12:31:25	到期时间:2023-	01-12 12:31:25	防护状态:防护中		
资产指纹 入侵检测 漏洞扫描	基线管理 网页防篡改						
异常登录 暴力破解							
加入白名单					最近一周 > 全部状态	>> 登录源P ○	
攻击源IP	攻击源IP位置	攻击次数	最后攻击时间	描述	阻断状态	操作	
172.31.0.59	局域网	2	2022-08-05 15:18:17	多次身份验证失败	阻断成功	加入白名单	
					共 1 条 10条/页 ∨	< 1 > 前往 1 页	

如上图所示,展示该台服务器的暴力破解详情。

7) 漏洞扫描



指纹 > 资产指纹详情					
3年1月					
	名称:ecm-f6f8-test 公開中:	ID : 106 内阔阳 :	78D56-9CCC-4740-8BAE-8A52F48CB33A 172.31.0.95	所在区域:重庆2 项像:	
	创建时间:2022-07-12 12:31:25	到期时间	: 2023-01-12 12:31:25	防护状态:防护中	
产指纹 入侵检测 漏洞扫描 基线管理 R	殉页防器改				
加入自名单标记为已处理				全部還用等級 > 漏消名称 > 请输入关键词进行搜索	a :
漏洞名称	CVE编号	漏洞等级	最后发现时间	操作	
PCRE 缓冲区错误意向	CVE-2019-20454	高危	2022-08-01 15:58:36	标记为已处理 加入自名单 重着详情	
GNU Wget 安全源商	CVE-2018-20483	莱克	2022-08-01 15:58:35	标记为已处理 加入白名单 查看详情	
PCRE 缓冲区错误赢得	CVE-2019-20838	業務	2022-08-01 15:58:35	标记为已处理 加入白名单 麻香详情	
GnuTLS 缓冲区错误漏洞	CVE-2019-3836	高悠	2022-08-01 15:58:35	标记为已处理 加入白名单 腐者评情	
json-c 输入验证错误漏洞	CVE-2020-12762	高危	2022-08-01 15:58:35	标记为已处理 加入白名单 重着评情	
Info-ZIP Zip 安全罪将	CVE-2018-13410	高度	2022-08-01 15:58:35	标记为已处理 加入白名单 直着详情	
GNU C Library string租件安全漏洞	CVE-2019-6488	高度	2022-08-01 15:58:34	标记为已处理 加入白名单 皇香详情	
GNU glibc 数字错误漏洞	CVE-2020-6096	高危	2022-08-01 15:58:34	移记为已处理 加入白各座 查看详情	
GNU Compiler Collection 安全特征问题源用	CVE-2019-15847	高危	2022-08-01 15:58:34	杨记为已处理 加入白名单 查看详情	
glibc 输入验证错误漏洞	CVE-2018-19591	高度	2022-08-01 15:58:34	标记为已处理 加入白名单 章衡详情	
			共 117 条	10魚/页 ◇ 〈 1 2 3 4 5 6 … 12 〉 前往	1

如上图所示,展示该台服务器的漏洞详情。

8) 基线检测

资产指纹 > 资产指纹详情					
详情					
	名称:ecm-	-acB3	D:E93A59EC-B176-47C3-BA12-OFB0FCBBEC3C	所在区域:查港1 铺像:	
	创趣时间 :2	2022-06-21 04:07:54	劉期时间:2022-07-21 04:07:54	防护状态:防护中	
1					
资产指纹 入侵检测 漏洞扫描 基线管理 网页	防篡改				
然结检测 弱口令检测					
					请输入基线名称进行搜索 Q Q
基线名称	基线检查项	风险项	状态	最后检测时间	操作
Unix系统基纯检测	23	13	末通过	2022-08-12 09:42:47	irta
Red Hat 7企业版基线控制	64	36	未通过	2022-08-12 09:42:19	译情
				共 2 条	10条/页

如上图所示,展示该台服务器的基线检测详情。

9) 弱口令检测



費产播放 > 资产指纹详情								
评慎								
E.	名称:ecm-4743 D:ACD75A59-30CC-42E8-0432-EF91DF985154 所在近後:成単4 公用9: 内周P:172.31.0.208 成量: 位観野月:2022-07-22 01:30:59 関朝町月:2022-07-22 01:30:59 国朝町月:2022-07-22 01:30:59							
资产指纹 入侵检测 漏洞扫描 基线管理	网页防糖改							
基线检测 新口令检测				٥				
用户名	弱口令类型	密码值	发现时间	最后更新时间				
WWuu	常见辨密码	5***	2022-08-12 09:55:37	2022-08-12 09:55:37				
				共1条 10条/页 · · · 前往 1 页				

如上图所示,展示该台服务器的弱口令检测详情。

10) 网页防篡改

资产指纹 > 资产指纹详统					
详情					
1	名称:ecm443 公用の: 信服时用(: 2022-07-22 01:00:50	12 : ACD19A59-39CC-42ER-6432-EF91D4985154 PJRP : 172.31.0.208 9388936 : 2023-01-22 01.30.59		所在区域:成都4 链像: 防护状态:防护中	
资产指纹 入侵检测 漏洞扫描 基线管理 网页防暴改					
36					最近三月 〜 0
告票等级	告辦名称	文件路径 时间	防护状态		操作
	文件异常添加	c:\test\file\文件004 - 副本.js 2022-07-26 14:42:29	已防御		意格
				共1条 10条/页 ~ <	1 > 前往 1 页

如上图所示,展示该台服务器的网页防篡改详情。



4.4. 基线管理

4.4.1 基线检测

		基线检测							自名单要理
服务器安全卫士(病 概定 资产管理 概定	〔生版〕	Ę.	检测服务器数 检测项 4 <u>一</u> 140	_{风险调} ① 29	^{通过率} 59.80%	立即扫描 定时扫描 一時扫描	音 开启 (每天1次, 00.00-01:00) 第載 音 111 ~ 〕		
服务器列表 资产指纹								请输入基线名称进行	複素 Q C
基线管理			基线名称	基线检查项	风险项	状态	影响服务器数量	最后检测时间	操作
基线检测			Web应用漏洞审计	16	无风险	已通过	з	2022-07-01 14:13:19	iata
調用扫描			Unix系統基线检测	23	13	未通过	3	2022-07-01 14:13:19	ista
入侵检测	~		SQL Server 2012安全基线检测	46	6	未通过	3	2022-07-01 14:13:19	1418
网页防篡改(原生版)	(生版)		Apache HTTP Server 2.4基线检测	30	无风险	已通过	3	2022-07-01 14:13:19	ista
设置中心			Red Hat 6企业版基线检测	56	无风险	已通过	3	2022-07-01 14:13:19	19 fā
			Windows 10 企业版安全基线检测	321	无风险	已通过	3	2022-07-01 14:13:18	1.译作
			Windows审计基线	71	10	未通过	2	2022-07-01 14:13:18	ivia
			MySQL 5.6企业版基线检测	26	无风险	已通过	3	2022-07-01 14:13:19	(¥łā
			Windows 2012 R2安全基线检测	22	无风险	已通过	3	2022-07-01 14:13:19	评情
			MySQL 5.6 社区版基线检测	19	无风险	已通过	3	2022-07-01 14:13:19	1710
								共 12 条 10条/页 ~ < 1	2 > 前往 1 页

如上图所示,上方展示基线检测的统计情况和基线检测设置,下方展示基线检测结果列表。

选定一个基线策略后,展示该策略上一次基线检测结果完成后的统计数据,统计情况包括检测服务 器数、检测项、风险项、通过率。切换基线策略后,显示切换后的基线检测统计结果。其中,通过率=所 有成功主机通过项之和÷(所有成功主机检测通过项+所有成功主机风险项)×100%。

基线检测设置分为一键检测和定时检测。当您需要进行基线检测时,先设置您需要的基线策略。点击"策略管理",进入策略管理页面,如下图所示。该页面展示了已经设置好的基线策略,包括策略名称、检测周期、检测服务器数、创建日期、策略开关和操作。可以新建、编辑和删除基线策略。

€₹

基线林	金测 〉 策略管理						
	新建策略				请输入策略名称		QQ
	策略名称	检查周期	检测服务器数	创建日期	策略开关	操作	
	111	1	4	2022-06-29 19:26:31		编辑	删除
	332	2	0	2022-01-18 14:42:04		编辑	删除
	555	1	0	2022-07-04 10:48:42		编辑	删除
	666	1	5	2022-07-06 14:06:19		编辑	删除
	777	1	35	2022-07-25 13:57:07		编辑	删除
	wlj	1	33	2022-07-12 09:38:53		编辑	删除
	zz-0725	1	1	2022-07-25 18:56:51		编辑	删除
					共7条 10条/页 ~	1 >	前往 1 页

当您新建基线策略时,点击"新建策略",弹出如下对话框,可以设置策略名称、检查时间、选择 基线名称和服务器,设置完成后点击"确定"即可完成新建基线策略。

新建基线策略		×
策略名称	请输入策略名称	
检查时间	每天 00:00 01:00 设置后会在周期选定的时间点开始定期检测	
基线名称	 全选 Red Hat 6企业版基线检测 Apache HTTP Server 2.4基线检测 MySQL 5.6 社区版基线检测 MySQL 5.6企业版基线检测 	
服务器分类	 全部服务器 自选服务器 取消 确定 	

→ 天翼云

若您需要对已有的基线策略进行编辑,点击该策略操作中的"编辑",弹出如下对话框,可以修改 策略名称、检查时间、修改已选择的基线名称和服务器,修改完成后点击"确定"即可完成基线策略编 辑。

修改基线策	長略		×
策略名称	111		
检查时间	每天 00:0	00 01:00	
基线名称 服务器分类	 全选 Red Hat 6企业版基线检测 Apache HTTP Server 2.4基线 MySQL 5.6 社区版基线检测 MySQL 5.6企业版基线检测 全部服务器 自选服务器 	检测	
选择服务器团	区域 全部区域 ~ 全部 ~ 选择服务器		请输入服务器名称/ip Q C
- 服約	务器名称	IP地址	服务器状态
ecr	m-ac83	172.31.0.227	已到期
ecr	m-3db0	172.31.0.238	已到期
ecr	m-21a3	172.31.0.9	已到期
ecr	m-46ce	172.31.0.114	运行中
ecr	m-1c9b-0006	172.31.0.48	运行中
ecr	m-1c9b-0008	172.31.0.120	运行中
ecr	m-1c9b-0009	172.31.0.62	运行中
ecr	m-1c9b-0004	172.31.0.136	运行中
ecr	m-1c9b-0007	172.31.0.67	运行中
		共 36 条 10条/页 ~ < 取 消 稳 定	1 2 3 4 > 前往 1 页

若您需要删除已有的基线策略,点击该策略操作中的"删除",弹出如下对话框,点击"确定"即 可完成基线策略删除。



删除策略	8			×
A	确认删除该基线策略吗?	2		
		取 消	确定	

基线策略设置完成后,定时检测设置完成,系统会根据已设置的基线策略定时进行检测。

若您需要一键检测时,选择需要检测的基线策略,并点击"一键检测",系统即开始执行本次检测 任务,如下图所示:

基线检测									白名单管理
1	会测服务器数 1	<u>⊥</u>	^{检测项} 95	Ť	风险项 0	Ş	通过率 0.00%	扫描中	

当一键检测或定时检测完成后,会展示本次基线检测结果。若检测成功,则会提示"执行完毕"; 否则提示"执行失败",如下图所示:

基线检测				臣 中5	♀ ◆ 执行完毕 × 自名单管理
^{地加度系指数} 地加印 單 1 空 95	Ribin i 道 0 晕(nom 立即扫描 0.00% 一wrom	定时扫描 开启(每天1次,00.00-01.00) 策略管理 基线策略 zz-0725		

若本次检测成功,基线检测结果列表如下图,包括基线名称、基线检测项、风险项、状态、影响服 务器数、最后检测时间、操作。当该基线检测通过时,风险项和影响服务器数分别展示为无风险和已通 过;当该基线检测未通过时,风险项和影响服务器数分别展示为风险数和未通过。列表可通过基线名称 查询。若本次检测失败,则展示"检测失败",基线检测结果列表只展示表头,检测结果为空。

こ 美天 (つ)

					请输入基线	名称进行搜索	Q
基线名称	基线检查项	风险项	状态	影响服务器数量	最后检测时间	操作	
Web应用漏洞审计	16	无风险	已通过	3	2022-07-01 14:13:19	详情	
Unix系統基线检测	23	13	未通过	3	2022-07-01 14:13:19	详情	
SQL Server 2012安全基线检测	46	6	未通过	3	2022-07-01 14:13:19	详情	
Apache HTTP Server 2.4基线检测	30	无风险	已通过	3	2022-07-01 14:13:19	详情	
Red Hat 6企业版基线检测	56	无风险	已通过	3	2022-07-01 14:13:19	详情	
Windows 10 企业版安全基线检测	321	无风险	已通过	3	2022-07-01 14:13:18	详情	
Windows审计基线	71	10	未通过	2	2022-07-01 14:13:18	详情	
MySQL 5.6企业版基线检测	26	无风险	已通过	3	2022-07-01 14:13:19	详情	
Windows 2012 R2安全基线检测	22	无风险	已通过	3	2022-07-01 14:13:19	详情	
MySQL 5.6 社区版基线检测	19	无风险	已通过	3	2022-07-01 14:13:19	详情	
					共12条 10条/页 🗸	(1 2)	前往 1

点击基线名称或者操作中的"详情"时,跳转到该基线名称的检测详情,如下图所示,可以查看本 基线中所有服务器具体的检测情况,包括服务器、通过项、风险项、无效项、状态、最后检测时间和操 作,整个列表可以根据状态、服务器名称、服务器 IP 进行查询。

Unix系统基线检测								
				全部状态	✓ 服务器名称 ✓ 输入搜索条件		Q	G
服务器	通过项	风险项	无效项	状态	最后检测时间	操作		
ecm-21a3 CC858C43-E2FE-47B1 172.31.0.9(私)	0	0	0	失败	2022-07-01 14:13:25	详情		
ecm-3db0 32F1DF23-6685-4475 172.31.0.238(私)	3	13	7	未通过	2022-07-01 14:13:28	详情		
ecm-46ce CBF2380E-9967-4A8B 172.31.0.114(私)	0	0	0	失败	2022-07-01 14:13:19	详情		
					共 3 条 10条/页 🗸	< 1 >	前往 1	ī

若您需要查看某台服务器的检测详情,点击操作中的"详情",可以查看该基线名称下该台服务器的检测详情。如下图所示,可以查看检查项、状态、最后检测时间和操作。整个列表可以基于状态进行 筛选。



基结绘图 〉 Red Hat 7企业振荡结验而评博 > 检测结束				
全国活気 第 Cperf2755 14796-418-0-0114-2019CB812F074438 1921-0183 1420 第二次日本通道105-CB81度のす可い30人自名単 加入自名単				- 新生 - 新生
检查项	状态	最后检测时间		操作
Ensure separate partition axists for /tmp 🕘	未通过	2022-08-25 11:56:33		加入白名单
Ensure nodex option set on /tmp partition	未通过	2022-08-25 11:56:33		加入高名单
Ensure nosuid option set on /tmp partition	未通过	2022-08-25 11:56:33		加入白名单
Ensure neeses option set on /tmp partition 🛛	未通过	2022-08-25 11:56:34		加入自名单
Ensure separate partition exists for /var \varTheta	未通过	2022-08-25 11:56:34		加入自名单
Ensure separate partition exists for /var/tmp	未通过	2022-08-25 11:56:34		加入合名单
Ensure separate pertition exists for /var/log 0	未通过	2022-08-25 11:56:34		加入白名单
Ensure separate partition exists for /var/log/audit	未通过	2022-08-25 11:56:34		加入白名单
Ensure separate partition exists for /home	未通过	2022-08-25 11:56:34		加入自名单
Ensure nodev option set on /home partition	未通过	2022-08-25 11:56:34		加入白名单
			共64条 10条/页 ~ (1 2 3 4 5 6	37 > 前往 1 页

若您检测时需要忽略该检测项,可以对该项进行"加入白名单"操作,点击后弹出对话框,如下图

所示:

加入白名单	×
 确认将当前所选检测项加入白名单? 确认后,该检测项将不再进行检测。加入白名单后,可在白名单管理处取消加白。 	
取消 确定	

若您需要将已加入白名单的检测项移除白名单,可点击主页的"白名单管理",如下图所示:

基线检测						白名牛對理
^{他演漫美语放} 單 1	^{检测项} 分子	RANNATI 百一 0	^{通过率} 5.00%	立即扫描 一键13版	走时扫描 开启 (极天1)汉,0000-01.00) 新闻的智慧 基结测器 22-0725 ✓	

可以看到已加入白名单的基线项,包括基线名称、加入白名单的检查项名称和操作,可以基于检测 项名称进行搜索:

基线名称	检查项名称	操作
MySQL 5.6企业版基线检测	Disable Interactive Login	移除白名单
MySQL 5.6企业版基线检测	Verify That 'MYSQL PWD' is Not Set in Users's Profiles	移除白名单



可将加入白名单的检查项移除白名单,点击"移除白名单",弹出如下对话框,确定后该检查项移 除白名单。

移除白名单 确认移除白名单吗? 确认后,该检测项将继续进行检测。 取消 确定	×	
除白名单 ▲ ^確 ₹	确认移除白名单吗? 确认后,该检测项将继续进行检测。 取消 确定	

4.4.2 弱口令检测

*		弱口令检测					
服务器安全卫士(原 概定 亦产管理	(生版)	检测服务器数 9 35	风险项 壶 4	R脸烟苏甜致 甲 4	立即扫描 定时检测 一谜扫描 开启 (每天1次,02:00)	9 2	
基线管理 基线检测 弱口令检测						服务器名称 🗸 🐇	2 の 2
漏洞扫描		服务器	用户名	弱口令类型	密码值	发现时间	最后更新时间
入侵检测 网页防篡改(原生版)	~	ecm-4743 ACD75 172.31.0.208(私)	A59-39CC-42E8-84 WWuu	常见弱密码	5***	2022-08-12 09:55:37	2022-08-12 09:55:37
入侵检测 网页防墓改(原生版) 设置中心	×	ecm-38c1 65DC6 172.31.0.98(私)	E37-E17C-4916-AC test	常见弱密码	S***	2022-08-12 09:12:33	2022-08-12 09:53:15
		ocm-fa3a 702038 192.168.16.175(%)	BB-8087-42CB-962) test	常见磷密码	D***	2022-07-08 11:04:02	2022-08-12 09:14:29
		ecm-b1d5 7BA79) 192.168.16.132(1)	244-2AD8-4C21-8E) test	常见磷密码	A***	2022-07-08 14:31:06	2022-07-08 15:26:49
						共4条 10)条/页 ~ < 1 > 前往 1 页

如上图所示,上方展示弱口令检测的统计情况和弱口令检测设置,下方展示弱口令检测结果列表。 统计情况包括检测服务器数、风险项、风险服务器数。

弱口令检测设置分为一键检测和定时检测。一键检测设置如下图,可进行服务器选择的设置,选择 完要检测的服务器后点击"确定",立刻开始本次弱口令检测。



一键检测设置			×
服务器分类 〇 全部服务	5器 ● 自选服务器		
选择服务器区域 全部区域	く 全部 く		
选择服务器		请输入服务器名称/ip	0 3
服务器名称	IP地址	服务器状态	
ecm-ac83	172.31.0.227	已到期	
ecm-3db0	172.31.0.238	已到期	
ecm-21a3	172.31.0.9	已到期	
ecm-46ce	172.31.0.114	运行中	
ecm-1c9b-0006	172.31.0.48	运行中	
ecm-1c9b-0008	172.31.0.120	运行中	
ecm-1c9b-0009	172.31.0.62	运行中	
ecm-1c9b-0004	172.31.0.136	运行中	
ecm-1c9b-0007	172.31.0.67	运行中	
ecm-1c9b-0001	172.31.0.166	运行中	
	共 32 条 10条/页 ∨ <	1 2 3 4 >	前往 1 页
	取消	定	

定时检测设置如下图,可开启定时检测,并进行定期检测周期、服务器选择的设置。关闭定时扫描 开关后,下方的所有设置项消失,不再能进行检测设置。点击确定后,定时检测设置完成。



定时检测设置 × 开启定时扫描 ● 定期检测周期 每天 00:00 设置后会在周期选定的时间点开始定期检测 服务器分类 ● 全部服务器			
 け检测设置 F启定时扫描 			
定时检测设置 开启定时扫描 定期检测周期 服务器分类	每天 00:00 02 02 00:000 00:000 00:00 00:000 00:000000		
服务器分类	● 全部服务器 ○ 自选服务器		
	取 消	确定	

当开始一键扫描或定时扫描后,展示动态检测效果。

弱口令检测				
松洞服务器数 望 32	风险湖 💮 5	风流虽为湖政 日 4	扫描中	Ritta@

在扫描过程中,可随时点击"停止检测",点击后弹出如下对话框,点击"确定"后停止检测。

提示		? 测的主机将不会被检测,可能存在的风险将不会告警提示,请谨慎操作。 取消 确定
提示 确认停止扫描吗? 确认后,还未检测的主机将不会被检测,可能存在的风险将不会告警提示,请谨慎操作。 取消 确定		
	取消 确定	

若检测完成后,下方弱口令列表展示本次检测完的结果,在未完成扫描时展示上次的扫描结果,如 下图所示。



				服务器名称 > 输入搜索的	6件 (2 0
服务器	用户名	弱口令类型	密码值	发现时间	最后更新时间	
ecm-36c1 65DC6E37-E17C-4916-AC 172.31.0.98(私)	abc	常见弱密码	1***	2022-08-12 10:02:37	2022-08-12 10:02:43	
ecm-36c1 65DC6E37-E17C-4916-AC 172.31.0.98(私)	test	常见弱密码	S***	2022-08-12 09:12:33	2022-08-12 10:02:43	
ecm-4743 ACD75A59-39CC-42E8-84 172.31.0.208(私)	WWau	常见弱密码	5***	2022-08-12 09:55:37	2022-08-12 10:02:22	
ecm-fa3a 70203BBB-80B7-42CB-962 192.168.16.175(私)	test	常见弱密码	D***	2022-07-08 11:04:02	2022-08-12 09:14:29	
ecm-b1d5 7BA79244-2AD6-4C21-8E 192.168.16.132(私)	test	常见弱密码	A***	2022-07-08 14:31:06	2022-07-08 15:26:49	
				共5条 10条/页	< 1 → 前往	1 页

检测结果包括影响服务器、用户名、弱口令类型、密码值、发现时间、最后更新时间。

点击上图列表中的服务器名称,跳转至下方资产详情页面。在该页面,为您展示该服务器的基本信 息和弱口令检测情况。

资产指纹 > 资产指纹详情						
详情						
	名称:ecm30c1 公開中: 创建时间:2022-07-22 01:29:57		ID:65DC6E37-E17C4916 内岡中:172.31.0.98 到期時间:2023-01-22 01:2	-ACD5-7EB8F037A120 9:57	所在区域:成都4 镜像: 防护状态:防护中	
资产指纹 入侵检测 漏洞扫描 基线管理 基质检测 朝口令检测	网页防器改					٥
用户名	弱口令类型	密码值		发现时间	最后更新时间	
abc	常见弱密码	1***		2022-08-12 10:02:37	2022-08-12 10:02:43	
test	常见弱密码	S***		2022-08-12 09:12:33	2022-08-12 10:02:43	
					共 2 条 10条/页 ~ 〈 1 〉 前f	主 1 页



4.5. 漏洞扫描

88			漏洞扫描							自名单键理
	服务器安全卫士(原生) 概范 初产管理 基线管理	版)		கம்தற்கள் 3418 🖳 27	潮洞的區角縣	立即扫描 一號扫描	上一次扫描 (扫描时间: 2022-08-12 定时扫描 开启 (每3天1次, 03:00) 设	15-31-35)未发现展展 查看详情 置		
1	基线检测 第口令检测 篇洞扫描		Linea展 Windown選用 加入自名章 特征力に処理					全部週間皆很 > 週間名称 >	课输入关键词进行搜索	Q Q
	入侵检测		漏洞名称	CVE编号	漏洞铸纫	80	峭服务器数量 最后发现时	间	操作	
	回页防篡改(原生版)		Apache Subversion mod_dav_sun 整数道出其同	CVE-2015-5343	88	19	2022-08-01	15:58:40	标记为已处理 加入白名单 愛者详情	
	10240		Hax out 输入验证错误服用	CVE-2018-14618	超焦	19	2022-08-01	1 15:58:40	标记为已处理 加入自名单 查看详情	
			Haxx curf印的curf 安全原间	CVE-2017-8817	高魚	20	2022-08-01	15:58:40	经记为已处理 加入白客单 查看评情	
			Hass libourt 緩冲区線 探潮洞	CVE-2016-8622	#8	19	2022-08-01	1 15:58:40	标记为已处理 加入自名单 查看详情	
振务器安全卫士(原生版) 概定 第門管理 - 基紙管理 - 道氏地理 - 現日や地理 - 和目的第四 (原生版) 设置中心		json-a 输入检证感误罪弱	CVE-2020-12762	高危	24	2022-08-01	1 15:58:40	标记为已处理 加入白名单 查看详情		
			GNU Bash 這程代码执行意識	CVE-2014-8271	#R	18	2022-08-01	1 15:58:39	标记为已处理 加入白名单 查看详情	
			PCPE和PCRE2 安全課程	CVE-2016-3191	X 2	18	2022-08-01	1 15:58:39	标记为已处理 加入自名单 查看详续	
			GNU gettext 安全課目	CVE-2018-18751	高欣	24	2022-08-01	15:58:39	际记为已处理 加入自名单 重着详情	
	服务務安全卫土(原土紙) 低近 同产管理 ~ 基廷管理 ~ 基廷管理 ~ 国内管理 ~ 风内防御衣 (登生版) 後重中心 ~		GNU Coreutits sort.c 输入验证错误意识	CVE-2015-4042	超危	18	2022-08-01	1558.39	师记为已处理 加入自名单 重要详情	
			GnuTLS 缓冲区错误激励	CVE-2019-3836	高名	6	2022-08-01	1 15:58:39	标记为已处理 加入自名单 重要评估	
							# 33	9条 10条/页 - (1 2 3	4 5 6 34 >	前往 1 页

如上图所示,上方展示漏洞扫描的统计情况和漏洞扫描设置,下方展示漏洞列表。

统计情况包括需紧急修复的漏洞、未处理的漏洞、存在漏洞的服务器。

点击需紧急修复的漏洞下方的数字,跳转至下方页面,该页面只展示 Linux 和 Windows 的超高危和 超危漏洞,包括漏洞名称、CVE 编号、漏洞等级、影响服务器数量、最后发现时间和操作,操作包括标记 为已处理、加入白名单和查看详情。该列表可根据漏洞名称或 CVE 编号进行搜索。

借 > ₿	需紧急修复的漏洞							
Linux3	初 Windows 漏洞							
加入	自名单标记为已处理				漏洞名称 ~	请输入关键词进行搜索	Q	
	漏洞名称	CVE编号	漏洞等级	影响服务器数量	最后发现时间	操作		
	Haxx curl 输入验证错误漏洞	CVE-2018-14618	超危	19	2022-08-01 15:58:40	标记为已处理 加入白名单	查看详情	
	SQLite 资源管理错误漏洞	CVE-2020-11656	超危	17	2022-08-01 15:58:39	标记为已处理 加入白名单	重着详情	
	GNU Coreutils sort.c 输入验证错误漏洞	CVE-2015-4042	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU Bash 缓冲区错误漏洞	CVE-2014-7187	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	SQLite 缓冲区错误漏洞	CVE-2019-8457	超危	17	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU glibc 基于堆的缓冲区错误漏洞	CVE-2015-0235	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU Bash 远程代码执行漏洞	CVE-2014-6271	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU Wget 路径遍历漏洞	CVE-2014-4877	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU Bash 操作系统命令注入漏洞	CVE-2014-6277	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
	GNU Bash 操作系统命令注入漏洞	CVE-2014-6278	超危	18	2022-08-01 15:58:39	标记为已处理 加入白名单	查看详情	
					共 35 条 10条/页 🗸	1 2 3 4 >	前往 1	1

漏洞扫描设置可进行一键扫描设置和定时扫描设置,并展示上一次扫描的结果,如下图所示:



立即扫描	上一次扫描 (扫描时间: 2022-08-12 15:31:35) 未发现漏洞 查看详情
一键扫描	定时扫描 开启 (每3天1次,03:00) 设置



点击"一键扫描",弹出如下设置对话框,可进行漏洞类别、漏洞扫描等级、超时设置、服务器选择的设置。其中,超时设置的时间需大于 30 分钟,小于 3 小时。

一键扫描设置				×
漏洞类别	linux漏洞	windows漏洞		
漏洞扫描等级	超高危	超危 高危	中危 低危	
超时设置	0 若单次时长超过设置时	小时 0 时长即为扫描失败	分钟 🕑	
服务器分类	● 全部服务器	○ 自选服务器		
			取消 确定	

点击定时扫描右侧的"设置",可进行定时扫描设置。设置选项包括漏洞类别、漏洞扫描等级、定 期检测周期、超时设置、服务器选择的设置。其中,超时设置的时间需大于 30 分钟,小于 3 小时。



定时扫描设置		×
开启定时扫描		
漏洞类别	linux漏洞 windows漏洞	
漏洞扫描等级	□ 超高危 □ 超危 □ 高危 □ 中危 □ 低危	
定期检测周期	每天 v 00:00 设置后会在周期选定的时间点开始定期检测	
超时设置	○ 小时 ○ 分钟 ● 若单次时长超过设置时长即为扫描失败 </td <td></td>	
服务器分类	● 全部服务器 ○ 自选服务器	
描述	请输入内容	
	取消 确定	

当开始一键扫描或定时扫描后,页面上展示下图动态效果。

漏洞扫描				白色和玻璃
総成金の知り無用 (素) 354	ялениян 2922	осаломин 125	150 A.	9-234

在扫描过程中,可随时点击"停止扫描",点击"停止扫描"时,弹出如下对话框,点击"确定" 后停止扫描。

提示		×
A	确认停止扫描吗? 确认后,还未扫描的主机将不会被检测,可能存在的风险将不会告警提示,请谨慎操作。	
	确 定	

扫描完成后,扫描结果展示在"上一次扫描"处。如下图所示,包括扫描时间、漏洞情况和查看详 情。



立即扫描	上一次扫描(扫描时间: 2022-08-15 14:44:12)漏洞数27 查看详情	
一键扫描	定时扫描 开启 (每3天1次,03:00) <mark>设置</mark>	

点击"查看详情",可以查看上一次扫描的统计情况和基于主机展示的漏洞列表。在统计情况中, 可以查看扫描类别、漏洞类别、开始时间、结束时间、漏洞风险数和风险主机/目标检测主机。在基于主 机展示的漏洞列表中,为您展示服务器、操作系统、检测状态、检测开始时间、检测结束时间和漏洞数 量。

漏洞扫描	上一次扫描详情						
扫描步 漏洞步	18) 一键扫描 18) Inux通用	开始时间 结束时间	2022-08-15 15:08:39 2022-08-15 15:08:41		жжала С. 26	风能主机/旧杨松期主机 空 2/2	
						服务器名称 → 输入推案条件 Q	0
	服务器	操作系统	检测状态	检测开始时间	检测结束时间	漏洞数量	
	ecm-1c9b-0006 A7811C7A-B3C8-4B80-A5A4-4B 172.31.0.48(紙)	linux	成功	2022-08-15 15:08:39	2022-08-15 15:08:41	9	
	ecm-1c9b-0008 B6DD07FC-1E82-430E-8490-161 172.31.0.120(%)	linux	成功	2022-08-15 15:08:39	2022-08-15 15:08:41	26	
						共 2 条 10 条/页 ~ < 1 > 前往 1	1 页

当点击漏洞数量中下方的数字时,跳转至资产详情页面,如下图所示。在资产详情页面,为您展示 该服务器的基本信息和漏洞情况。

资产指纹 > 资产指纹详情				
详惯				
1	名称::exm-1c80-0008 公開中: 住田町所::2022-05-20 23.13.00	10 : A7811C 193801 : 172 89881101 : 20	7A-B3C8-4880-A5A4-48856602eC00 310.48 322-11-20 2313:00	州在1544:内部6 银旗:
资产指纹 入侵检测 漏洞扫描 基线管理 网页防算	自改			
加入白名单标记为已处理				全面濃調等级 > 漏洞名称 > 荷植入关键词进行推索 Q C
漏洞名称	CVE编号	漏洞等级	最后发现时间	操作
Python 信任管理问题满词	CVE-2019-9636	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 豐豐祥儀
GNU Coreutils sort.c 输入给证错误漏洞	CVE-2015-4042	题危	2022-08-15 15:08:39	标记为已处理 加入自名单 查看详情
SQLIto 资源管理错误源源	CVE-2020-11656	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 靠着详情
GNU Wget 路径遮历漏洞	CVE-2014-4877	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 重要详情
libseccomp 权限许可和访问控制问题激消	CVE-2019-9893	超化	2022-08-15 15:08:39	标记为已处理 加入自名单 靈香详情
SQLite 维冲区错误兼用	CVE-2019-8457	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 重香详情
GNU glibe 基于维的缓冲区错误漏洞	CVE-2015-0235	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 重看详情
Python 安全特征问题潇漪	CVE-2019-9948	超危	2022-08-15 15:08:39	新记为已处理 加入自名单 重香洋绣
Python 操作系统命令注入漏洞	CVE-2018-1000802	超危	2022-08-15 15:08:39	标记为已处理 加入自名单 靈香详情
Expet XML解析器拒绝服务漏洞	CVE-2016-5300	高危	2022-08-01 15:58:32	标记为已处理 加入白名单 童者详情
			共 194	条 10条/页 ~ < 1 2 3 4 5 6 … 20 > 前往 1 页

漏洞扫描主页下方的漏洞列表中展示本次扫描的漏洞情况,按照 Linux 和 windows 漏洞分别展示,



包括漏洞名称、CVE 编号、漏洞等级、影响服务器数量、最后发现时间和操作,列表默认按照最后发现时间排序,最新发现的漏洞位于最上方。漏洞列表可按照漏洞等级、漏洞名称、CVE 编号进行搜索。

加入白名	单 标记为已处理				全部漏洞等级 > 漏洞名称 > 请输入	关键词进行搜索		Q	
漏》	司名称	CVE编号	漏洞等级	影响服务器数量	最后发现时间	操作			
Apa	che Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	高危	19	2022-08-01 15:58:40	标记为已处理 加入自	名单 查看详	in .	
Hav	x curl 输入验证错误漏洞	CVE-2018-14618	超危	19	2022-08-01 15:58:40	标记为已处理 加入自	名单 查看详	情	
Hax	x curl和libcurl 安全漏洞	CVE-2017-8817	高危	20	2022-08-01 15:58:40	标记为已处理 加入自	名单 查看详	情	
Hax	x libcurl 缓冲区错误漏洞	CVE-2016-8622	高危	19	2022-08-01 15:58:40	标记为已处理 加入自	名单 查看详	情	
jsor	i-c 输入验证错误漏洞	CVE-2020-12762	高危	24	2022-08-01 15:58:40	标记为已处理 加入自	名单 查看详	ită.	
GN	J Bash 远程代码执行漏洞	CVE-2014-6271	超危	18	2022-08-01 15:58:39	标记为已处理 加入自	名单 查看详	情	
PCI	RE和PCRE2 安全漏洞	CVE-2016-3191	高危	18	2022-08-01 15:58:39	标记为已处理 加入自	名单 責看详	情	
GN	J gettext 安全漏洞	CVE-2018-18751	高危	24	2022-08-01 15:58:39	标记为已处理 加入自	名单 直看详	h	
GN	J Coreutils sort.c 输入验证错误漏洞	CVE-2015-4042	超危	18	2022-08-01 15:58:39	标记为已处理 加入自	名单 查看详	in .	
Gnu	TLS 缓冲区错误漏洞	CVE-2019-3836	高危	6	2022-08-01 15:58:39	标记为已处理 加入自	名单 查看详	in .	

当点击"漏洞名称"、"影响服务器数量"或"查看详情"时,跳转至下方的漏洞详情页面。该页 面包括漏洞的基本信息和影响服务器列表,基本信息包括漏洞名称、CVE 编号、危害等级、漏洞类型、发 布时间、参考链接、补丁获取链接,影响服务器列表包括影响服务器、操作系统、最后发现和操作。

漏洞	重到详情									
	60		Apache Subversion mod_dav_svn 整数溢出测	1.71	CVE编号	CVE-2015-5343		危害等级	高危	
			缓冲区错误		发布时间	2016-04-15				
		参考链接	http://www.debian.org/security/2015/dsa-5	3424						
		补丁获取链接	目前厂商已经发布了升级补丁以修复此安全问题 http://subversion.apache.org/security/CVE-	想,补丁获取链接: -2015-5343-adviso	ry.txt					
870	2为已处理									
	影响服务器	操作系统		最后发现时间			状态			操作
	ecm-88ab-0002 A035F5AC-A47F-4AA8-AE42-522F2F74 172.31.0.50(%)	linux		2022-08-01 15:5	8:40		未处理			标记为已处理
	ecm-1c9b AFC61361-4519-4B79-8A19-77503989A539 172.31.0.212(%)	linux		2022-08-01 15:5	8:40		未处理			标记为已处理
	ecm-fa3a 70203888-8087-42C8-962F-DE90D05A8279 192:168.16.175(私)	linux		2022-08-01 15:5	8:39		未处理			标记为已处理
	ecm-1c9b-0008 B6DD07FC-1E82-430E-8490-1612839A 172.31.0.120(%)	linux		2022-08-01 15:5	8:39		未处理			后记为已处理
	ecm-88ab B57069DD-7850-4606-8C03-8924D0CE1879 172.31.0.222(%)	linux		2022-08-01 15:5	8:39		未处理			标记为已处理
	ecm-1c9b-0001 3273F5E8-87AB-410D-850A-D5283869 172.31.0.166(紙)	linux		2022-08-01 15:5	8:38		来处理			标记为已处理
	ecm-1c9b-0003 DCCF0A0D-0FF9-4F66-9664-4C437125 172.31.0.36(%)	linux		2022-08-01 15:5	8:38		未处理			标记为已处理
	ecm-1c9b-0002 F37D5AAA-C753-43C5-96B5-EDEEAEA8 172.31.0.218(¾)	linux		2022-08-01 15:5	8:38		未处理			标记为已处理
	ecm-1c9b-0004 D5D61C22-C5C5-4074-AD79-F6D44DB 172.31.0.136(紙)	linux		2022-08-01 15:5	8.38		未处理			标记为已处理
	ecm-3db0 32F1DF23-6685-4475-AC35-6371F94559D7 172.31.0.238(%)	linux		2022-08-01 15:5	8:38		未处理			标记为已处理

当点击一台服务器后面的"标记为已处理"时,弹出如下对话框,确认后,该条记录的状态变更为 "已处理",且"漏洞扫描"页面上该漏洞影响服务器数量减 1。


标记为已处理		×
确认要把该漏洞标记为已处理吗? 当您修复该漏洞后,可将该漏洞标记为已处理,	漏洞告營列表中将不再展示	
漏洞名称	CVE编号	影响服务器
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-88ab-0002 A035F5AC-A47F-4AA8-AE42-522F2F74 0ABB 172.31.0.50(私)
	取消 确定	

当选择多台服务器并"标记为已处理"时,弹出如下对话框,确认后,这些服务器记录的状态变更 为"已处理",且"漏洞扫描"页面上该漏洞影响服务器数量减去已处理的数量。

标记为已处理	标记为已处理							
 确认要把该漏洞标记为已处理吗? 当您修复该漏洞后,可将该漏洞标记为已处理 	1, 漏洞告警列表中将不再展示							
漏洞名称	CVE编号	影响服务器						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-88ab-0002 A035F5AC-A47F-4AA8-AE42-522F2F74 0ABB 172.31.0.50(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b AFC61361-4519-4B79-8A19-77503989A539 172.31.0.212(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-fa3a 70203BBB-80B7-42CB-962F-DE90D05A8279 192.168.16.175(紙)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b-0008 B6DD07FC-1E82-430E-8490-1612839A 0A01 172.31.0.120(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-88ab B57069DD-7850-4606-8C03-8924D0CE1879 172.31.0.222(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b-0001 3273F5E8-87AB-410D-850A-D5283869 254C 172.31.0.166(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b-0003 DCCF0A0D-0FF9-4F66-9664-4C437125 E9B7 172.31.0.36(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b-0002 F37D5AAA-C753-43C5-96B5-EDEEAEA 87292 172.31.0.218(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-1c9b-0004 D5D61C22-C5C5-4074-AD79-F6D44DB 4403D 172.31.0.136(私)						
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	ecm-3db0 32F1DF23-6685-4475-AC35-6371F94559D7 172.31.0.238(私)						
	取消 确定							

当点击漏洞扫描页面上漏洞列表中的"标记为已处理"时,如下图所示:



Linux運算 Windows運算 加入自名单 标记为已处理				全部產黨等值 > 講調名称	> 请输入关键词进行搜索 Q Q Q
漏洞名称	CVE编号	漏洞等级	影响服务器数量	最后发现时间	操作
Haxx curl 输入验证错误漏消	CVE-2018-14618	超危	20	2022-08-15 15:08:40	标记为已处理 加入白名单 查看详情
libseccomp 权限许可和访问控制问题展刊	CVE-2019-9893	超危	17	2022-08-15 15:08:39	标记为已处理 加入向名单 查看详情
GNU gettext 资源管理错误漏洞	CVE-2018-18751	超危	24	2022-08-15 15:08:39	标记为已处理 加入自名单 查香详情
GNU Bash 操作系统命令注入灌洞	CVE-2014-6277	超急	19	2022-08-15 15:08:39	标记为已处理 加入自名单 查香详情
GNU Bash 缓冲区错误漏洞	CVE-2014-7187	超危	19	2022-08-15 15:08:39	标记为已处理 加入自名单 查香详情
Python 操作系统命令注入漏洞	CVE-2018-1000802	超危	20	2022-08-15 15:08:39	标记为已处理 加入白名单 虛香详情
GNU Bash 操作系统命令注入漏洞	CVE-2014-6278	超危	19	2022-08-15 15:08:39	标记为已处理 加入自名单 查香详情
Python 安全特征问题意识	CVE-2019-9948	超危	20	2022-08-15 15:08:39	标记为已处理 加入白名单 索香详情
GNU Bash 缓冲区错误漏洞	CVE-2014-7186	超危	19	2022-08-15 15:08:39	标记为已处理 加入自名单 查香详情
GNU Coreutils sort.c 输入验证错误顺用	CVE-2015-4042	超危	19	2022-08-15 15:08:39	标记为已处理 加入白名单 虛看详情
				共 341 条 10条/页 ~ 1 2	3 4 5 6 … 35 > 前往 1 页

若选择一个漏洞操作"标记为已处理",弹出如下对话框,确认后,该漏洞不再展示在漏洞列表中, 且漏洞详情页面所有服务器的状态均变更为"已处理"。

标记为已处理			×
确认要把该漏洞标记为已处理吗? 当您修复该漏洞后,可将该漏洞标记为已处理,	漏洞告警列表中将不再展示。		
漏洞名称	CVE编号	影响服务器数量	
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	19	
	取 消		

若选择多个漏洞操作"标记为已处理",弹出如下对话框,确认后,这些漏洞不再展示在漏洞列表 中,且这些漏洞详情页面所有服务器的状态均变更为"已处理"。



标记为已处理			×
确认要把该漏洞标记为已处理吗? 当您修复该漏洞后,可将该漏洞标让	己为已处理,漏洞告警列表中将不再展示。		
漏洞名称	CVE编号	影响服务器数量	
Haxx curl 输入验证错误漏洞	CVE-2018-14618	20	
libseccomp 权限许可和访问控制问题漏洞	CVE-2019-9893	17	
GNU gettext 资源管理错误漏洞	CVE-2018-18751	24	
	取消 确定		

当点击漏洞扫描页面上漏洞列表中的"加入白名单",如下图所示:

Linux還親 Windows:濕潤 加入白名单 标记为已处理				全部周期等级 > 選び	特名称 > 調整入关键词运行器索 Q C
漏洞名称	CVE编号	漏洞等级	影响服务器数量	最后发现时间	操作
Haxx curt 输入验证错误漏洞	CVE-2018-14618	超急	20	2022-08-15 15:08:40	标记为已处理 加入自名单 查看详情
libseccomp 权限许可和访问控制问题展用	CVE-2019-9893	超危	17	2022-08-15 15:08:39	标记为已处理 加入自名单 查看详情
GNU gettext 资源管理错误源词	CVE-2018-18751	題危	24	2022-08-15 15:08:39	标记为已处理 加入自名单 重新详情
GNU Bash 操作系统命令注入源则	CVE-2014-6277	超危	19	2022-08-15 15:08:39	标记为已处理 加入自名单 重香详情
GNU Bash 缓冲区错误展网	CVE-2014-7187	超危	19	2022-08-15 15:08:39	标记为已处理 加入白名单 宣奏详情
Python 操作系统命令注入漏洞	CVE-2018-1000802	題危	20	2022-08-15 15:08:39	标记为已处理 加入自名单 重着详情
GNU Both 操作系统命令注入漏洞	CVE-2014-6278	超危	19	2022-08-15 15:08:39	标记为已处理 加入自名单 重着详情
Python 安全特征问题漏洞	CVE-2019-9948	超危	20	2022-08-15 15:08:39	标记为已处理 加入自名单 重新详情
GNU Bash 缓冲区错误震测	CVE-2014-7186	超炮	19.	2022-08-15 15:08:39	标记为已处理 加入自名单 宣誓详情
GNU Consultis sort.c 输入验证错误漏洞	CVE-2015-4042	超危	19	2022-08-15 15:08:39	标记为已处理 加入白名单 宣誓详情
				共 341 条 10条/页 🗸 🤇	1 2 3 4 5 6 … 35 > 前往 1 页

若选择一个漏洞操作"加入白名单",弹出如下对话框,确认后,该漏洞进入白名列表中。

			×	
确认要把该漏洞加入白名单吗? 该漏洞加入白名单后,将不再检测全部资产中是否存在该漏洞,您可以前往白名单管理中查看。				
漏洞名称	CVE编号	影响服务器数量		
Apache Subversion mod_dav_svn 整数溢出漏洞	CVE-2015-5343	19		
	取消 确定			



若选择多个漏洞操作"加入白名单",弹出如下对话框,确认后,这些漏洞进入白名列表中。

加入白名单			×
 确认要把该漏洞加入白名单吗? 该漏洞加入白名单后,将不再检测 	全部资产中是否存在该漏洞,您可以前往白名单	管理中查看。	
漏洞名称	CVE编号	影响服务器数量	
GNU gettext 资源管理错误漏洞	CVE-2018-18751	24	
GNU Bash 操作系统命令注入漏洞	CVE-2014-6277	19	
	取 消		

若您需要将已加入白名单的漏洞进行移除,请点击漏洞扫描页面上方的"白名单管理",如下图所

示:								
漏洞扫描								
Ŀ.	電索急修复的漏洞] 564	Ţ	未处理的漏洞 3432	Ţ	存在激调的服务器	立即扫描 一键扫描	上一次扫描(日相助词):2022-08-15 15:08:41) 道湾截28 宜者详细 定时扫描 开启 (每天1次, 02:00) 设置	

点击"白名单管理"后跳转至如下页面,可以查看已加入白名单的漏洞列表,包括漏洞名称、CVE 编 号、系统分类、漏洞等级、加入白名单服务器数量和操作。

漏洞扫描 > 白名单管理					
移出白名单				漏洞名称 > 【请输入关键词进行搜索	Q Q
周 漏洞名称	CVE编号	系统分类	漏洞等级	加入白名单服务器	操作
Haxx curl 输入验证错误源明	CVE-2018-14618	Linux濾洞	超危	20	移出白名单
				共1条 10条/页 ~ (1	> 前往 1 页

您可以选择需要移除的漏洞,点击操作中的"移出白名单",弹出如下对话框,点击"确认"后该 漏洞被移除白名单。

是否移除			×
漏洞名称		CVE编号	
Haxx curl 输入验证错误漏洞		CVE-2018-14618	
H	取 消	确定	



4.6. 入侵检测

4.6.1 异常登录

88	â	异常登录					白名单管理
服务器5 服务器5 概见 资产管理 其体管理	服务器安全卫士(原生版) 概览 资产管理 ~ 基线管理 ~	Demosion 1		编统会派等 使于 0	'n	argalitaniki 1	御 说三个月 ∨)
1	漏洞扫描 入侵检测 ~ 异常登录	新记为已处理 合爱关型 服务器	全部告등 첫 월 → 물近 三 个 月 출 录 源 P	 全部状态 ~ 登录地区 	2.5.2.P 2.5.15 2.5.15	服务器名称 ~ 输入要素条件 最后登录时间 状态 操	2 Q
	暴力破解 网页防篡改(原生版) 设置中心 ~		203.57.225.53	中国-广东-*	secure	2022-07-08 22:29:24 未批理 共 1 条 10条/页 ~	##記加已处理 < 1 → 前往 1 页

如上图所示,上方展示异常登录事件的统计情况,下方展示异常登录事件列表。

统计情况包括异常登录事件数、爆破登录事件数、存在风险的服务器数,都默认统计最近一周的时间,还可以统计最近一月和最近三月的时间维度。异常登录事件:统计事件列表中的异常登录事件数, 爆破登录事件:统计事件列表中的爆破登录事件数,存在风险的服务器:有异常登录和爆破登录事件的 服务器数量,如果同一台服务器有不同的事件需要进行去重。

异常登录		白名单鞭理
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	海拔型斗争作 至 <u>五</u> 0	■近三个月 > の在ス制が成方品 日 1

事件列表包括告警类型、服务器、登录源 IP、登录地区、登录账号、最后登录时间、状态和操作, 默认按照最后登录时间进行排序,最新的事件排在最上方,并默认展示一周内的事件列表。事件列表可 按照告警类型、时间、状态、登录源 IP、登录账号、服务器名称、服务器 IP 进行搜索。

481	己为已处理			全部告警类型 ~	最近三个月		全部状态		豐豪選伊	登录账号	服务器名标	8 V	输入搜索条件			0
	告警类型	服务器	型录源IP	登录地区			Ť	全录账号			最后登录时间	状态	操作			
	5月常登录 5月常登录 192.168.16.226(私)		203.57.225.53	中国-广东-*		54	secure		2022-07-08 22:29:24	未处理	标记为已处理					
												共1条	10条/页 ~ 1	> 前4	住 1	页

操作为标记为已处理,当该事件为"未处理"状态时,可进行点击,点击后弹出如下对话框,在对 话框中点击"确认"后,事件列表中该事件状态变更为已处理。



标记为已处理				×
🔒 确认	要把该事件设置为已处理吗?			
警告类型	服务器	登录地区	登录账号	最后登录时间
异常登录	ctcss-server-0-1 53BA 192.168.16.226(私)	广东	secure	2022-07-08 22:29:24
		取消确定	2	

若您需要将某些登录 IP、登录用户名、登录时间和登录地区设置为正常登录,请您点击异常登录页 面上的"白名单管理"进行设置,设置后将不再进行异常登录告警。

异常登录		白色の取 現
левано () 1	ante ano	単式三个月 ✓ 行在风险的服务器 日 1

白名单管理中可对异常登录的白名单规则进行设置,包括白名单规则的新增、编辑和删除,如下图 所示。白名单规则列表可根据服务器名称和服务器 IP 进行搜索,若该规则中包含该台服务器,即进行显 示。

€₹

异常登录	> 白名单管理							
¥	增白名单					服务器名称 >		0 0
	服务器	登录源IP	登录地	登录账号	登录时间	备注	操作	
	ecm-1c9b-0007 43873D06-CC46 172.31.0.67(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-1c9b-0001 3273F5E8-87AB-4 172.31.0.166(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-1c9b-0003 DCCF0A0D-0FF9 172.31.0.36(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-1c9b-0002 F37D5AAA-C753 172.31.0.218(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-1c9b AFC61361-4519-4B79 172.31.0.212(私)		中国四川成都	secure	08:00-20:00		编辑	移除
	ecm-5fac 65626726-CEC9-46D2 172.31.0.187(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ctcss-server-0-1 53BA6C27-2461 192.168.16.226(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-ac83 E93A59EC-B176-47C3 172.31.0.227(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-3db0 32F1DF23-6685-4475-A 172.31.0.238(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除
	ecm-21a3 CC858C43-E2FE-47B1 172.31.0.9(私)		中国-四川-成都	secure	08:00-20:00		编辑	移除

共16条 10条/页 < 1 2 > 前往 1 页

点击"新增白名单"时,弹出如下对话框,可填写登录 IP、登录用户名、登录时间、登录地区、描述,并选择服务器。登录 IP 支持单个 IP (示例: 1.1.1.1)、 IP 范围 (示例: 1.1.1.1-1.1.1.10)和 IP 段 (示例: 172.168.34.1/20)。多个 IP 之间用英文,隔开。登录地可选择多个登录地。登录账号支持 输入多个用户名,用英文,隔开。登录时间可选择开始时间和结束时间。服务器可选择全部服务器和部分 服务器。以上字段,除去服务器外,均为非必填,但登录 IP、登录用户名、登录时间、登录地区至少需 要填写一项,可填写多项。



新增白名单				×
登录IP	支持单IP、IP范围和IP段		0	
登录用户名	支持多个用户名,用英文,	扇开		
登录时间	© 00:00	© 01:00		
登录地区	请选择	~		
服务器分类	● 全部服务器 ○ 自议	先服务器		
描述	请输入内容			
		1		
		取消确定		

当所有字段都选择完成后,会生成白名单规则,显示在白名单列表中,如下图所示:



异常登录	■ 2 ◇ 白名単審理									
	新增白名单 删除					服务器名称	× 1	》入搜索条件		2 0
	服务器	登录源IP	登录地	登录账号	登录时间		备注	E	操作	
	ecm-1c9b-0007 43873D06-CC46 172.31.0.67(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-1c9b-0001 3273F5E8-87AB-4 172.31.0.166(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-1c9b-0003 DCCF0A0D-0FF9 172.31.0.36(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-1c9b-0002 F37D5AAA-C753 172.31.0.218(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-1c9b AFC6136145194B79 172.31.0.212(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-5fac 65626726-CEC9-46D2 172.31.0.187(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ctcss-server-0-1 53BA6C27-2461 192.168.16.226(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-ac83 E93A59EC-B176-47C3 172.31.0.227(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-3db0 32F1DF23-6685-4475-A 172.31.0.238(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除
	ecm-21a3 CC858C43-E2FE-47B1 172.31.0.9(私)		中国-四川-成都	secure	08:00-20:00				编辑	移除

共16条 10条/页 < 1 2 > 前往 1 页

可在操作中,对该白名单规则进行编辑和删除。当点击"编辑"时,弹出如下对话框,可编辑登录 IP、登录用户名、登录时间、登录地区、描述,并点击"确定"后即可完成白名单规则的编辑。

编辑白名单			×
登录IP	1.1.1.1		0
登录用户名	secure		
登录时间	© 00:00	© 01:00	
登录地区	中国-河北-秦皇岛	~	
描述	请输入内容		
		取消 确定	
			-



当点击操作中的"删除"时,弹出如下对话框,点击确定后,该白名单规则将被删除。

是否移除					×
A	此操作将永久删除改配置,是否继续?				
		取 消	确定		

4.6.2 暴力破解

88	Ê		暴力破解								白名单管理
服务器安全卫士(原生 服宽 资产管理 基线管理		反) ~ ~	^{神化增会} 第 百 2	1/F	⁹⁶ 旦 1	风险的服务器				量近一周	
	漏洞扫描 入侵检测 异常登录		加入白名单服务器	攻击源iP	双击簿iP位置	最近一周 攻击次数	✓ 全部状态 ✓ 墨后攻击封间	至录录户 服务管 描述	1名称 Y 输入提索条件 阻断状态	操作	Q Q
I	暴力滅解 网页防篡改(原生版)		ecm-f8f8-test 1C678D56-9 172.31.0.95(私)	172.31.0.59	周城间	3	2022-08-05 15:18:17	多次身份验证失败	陶新成功	加入自名单	
	设置中心	×	ecm-f678-test-0001 798F6 172.31.0.59(&)	172.31.0.95	局域网	1	2022-08-05 15:29:55	多次身份验证失败	陶新成功 共 2 条 10条/页 ~	加入自名单 < 1 > 前往	1页

如上图所示,上方展示暴力破解事件的统计情况,下方展示暴力破解事件列表。

统计情况包括待处理告警事件数和存在风险的服务器数,都默认统计最近一周的时间,还可以统计 最近一月和最近三月的时间维度。待处理告警事件:统计事件列表中的事件数,存在风险的服务器:统 计有暴力破解事件的服务器数量,如果同一台服务器有不同的事件需要进行去重。

暴力破解		<u> 68498</u>
		「島送一个月 〜」
時处理物業事件	асальная П	

事件列表包括服务器、攻击源 IP、攻击源 IP 位置、攻击次数、最后攻击时间、描述、阻断状态和操 作,默认按照最后攻击时间进行排序,最新的事件排在最上方,并默认展示一周内的事件列表。阻断状 态分为阻断成功和未阻断两种情况。事件列表可按照时间、状态、攻击源 IP、服务器名称、服务器 IP 进 行搜索。



tet	白名单				最近一个月 ∨ 全部状态	シ 登录道P	服务器名称 > 输入搜索条件	0 0	1
	服务器	攻击源IP	攻击源IP位置	攻击次数	最后攻击时间	描述	阻断状态	操作	
	ecm-f6f8-test 1C678D56-9CCC 172.31.0.95(私)	172.31.0.59	局城网	3	2022-08-05 15:18:17	多次身份验证失败	阻断成功	加入白名单	
	ecm-f6f8-test-0001 796F6310-B 172.31.0.59(私)	172.31.0.95	局城网	5	2022-08-05 15:29:55	多次身份验证失败	眼前成功	加入白名单	
							共 2 条 10条/页 ~	< 1 > 前往 1 页	π

操作为加入白名单,点击后弹出如下对话框,在对话框中点击"确认"后,事件列表中该事件状态 变更为"已加白"。该事件的服务器和攻击源 IP 加入白名单,成为一条白名单策略。

þ	口入白名	。 3.单		×
	A	确认要把该规则加入白名单吗? 该规则加入白名单后,命中白名单规则的事件将被补	见作正常,请谨慎添加。	
	服务器		攻击源IP	
	ecm-f6f 172.31.0	8 <mark>-test</mark> 1C678D56-9CCC-4740-8BAE-6A52F48CB3… 9.95(私)	172.31.0.59	
		取消	确定	

若您需要将加入白名单的策略进行移除,请点击暴力破解主页的"白名单管理",如下图所示:

暴力破解		白名单管理
1953週前日 1011 0	ота Яльтия ва 早 0	最近一局 🗸

白名单管理中可对暴力破解的白名单规则进行设置,包括白名单规则的新增、编辑和删除。白名单规则列表可根据服务器名称和服务器 IP 进行搜索,若该规则中包含该台服务器,即进行显示。

新埠	自名单 删除		服务器名称	◇ 输入搜索条件 (a a
	服务器	攻击源IP	备注	操作	
	ecm-f6f8-test 1C676D56-9CCC-4740-8BAE-8A52F48CB33A 172.310.95(%)	172.31.0.59		編朝	移动
	ecm-f6f8-test 1C678D56-9CCC-4740-8BAE-6A52F48CB33A 172.310.95(‰)	172.31.0.59		1944 BU	移除

点击"新增白名单"时,弹出如下对话框,可填写来源 IP、描述,并填写服务器分类。登录 IP 支持 单个 IP(示例:1.1.1.1)、IP 范围(示例:1.1.1.1-1.1.1.10)和 IP 段(示例:172.168.34.1/20)。



多个 IP 之间用英文, 隔开。服务器可选择全部服务器和部分服务器。登录 IP 和服务器均为必填选项。

新增白名单				
登录IP	支持单IP、IP范围	和IIP段	0	
服务器分类	○ 全部服务器	● 自选服务器		
选择服务器区域	全部区域 🗸	全部 🗸		
	选择服务器		请输入服务器名称/lp Q	C
服务器	名称	IP地址	服务器状态	
ecm-ac	:83	172.31.0.227	已到期	
ecm-3c	0db	172.31.0.238	已到期	
ecm-21	1a3	172.31.0.9	已到期	
ecm-46	бсе	172.31.0.114	运行中	
ecm-1c	:9b-0006	172.31.0.48	运行中	
ecm-1c	9b-0008	172.31.0.120	运行中	
ecm-1c	c9b-0009	172.31.0.62	运行中	
ecm-1c	:9b-0004	172.31.0.136	运行中	
ecm-1c	9b-0005	172.31.0.215	运行中	
ecm-1c	c9b-0007	172.31.0.67	运行中	
	共《	55 条 10条/页 ~ 《	1 2 3 4 > 前往 1	页
描述	请输入内容			
		,		
		取消 确定		

当所有字段都选择完成后,会生成白名单规则,显示在白名单列表中,如下图所示:

暴力敏解 > 白名单管理				
新增白名单 副除		腰	务器名称 > 输入搜索条件	0
服务器	攻击源IP	备注		操作
ecm-1618-1861 10678D56-90CCC-4740-8BAE-6A52F48CB33A 172.31.0.95(私)	172.31.0.59			编辑 移除
ecm-f6f8-test 1C878D56-9CCC-4740-8BAE-6A52F48CB33A 172.31.0.95(%)	172.31.0.59			编辑 移除
			共 2 条 10条/页 🗸	1 〉 前往 1 页

可在操作中,对该白名单规则进行编辑和删除。当点击操作中的"编辑"时,弹出如下对话框,可 编辑登录 IP 和描述,点击确定后,该白名单规则编辑完成。



编辑白名单				×
留录IP	172.31.0.59		0	
描述	请输入内容			
		取消	确定	

当点击操作中的"删除"时,弹出如下对话框,点击确定后,该白名单规则将被删除。

	删除设置	×
C	🔔 此操作将永久删除该配置项,是否继续?	
	取消通定	



4.7. 网页防篡改(原生版)

网页防篡改(原生版)包含防护状态、防护管理和防护配额3大功能模块。

4.7.1 防护状态

88		网页防篡改(原生版)							未成立的最短数 1个,已经已最多级配数 31	5.到期时间: 2022年07月05日 的工业日	
服 (点)(点)(点),(二),(二),(二),(二),(二),(二),(二),(二),(二),(二),(二),(二),(-),(-),(-),(-),(-),(-),(-),(-),(-),(-	3务器安全卫士(原生版)	時代状态 助行管理 防护配额									
	13 产管理 ~ /約費理 ~ /約月間 /梁松淵 ~	913.78548 7	ашыққараа Т 7	Sivere	C 3	x	8472988 18		*RTEROLON	CHERSELE 2 3	
1	200840 (R王敏) 200	当前防护文件统计图Top6				文件变动数Top5	(最近15天)				
						/root/test/file/test0	02.js				
					- pp 3	/root/test/Ne/test0	02.jsp				
			a la		— js 2	/root/test/file/sinjla	n.ja				
					- cn 1	/root/test/Ne/test0	D1.html				
		100						根近一周	✓ 撮务器名称 ✓ 能入技業目	a <u>D</u> n	
		日 告誓等级	告誓名称		受影响服务器		文件路径	时间	防护状态	操作	
		C	文件异常删除		65DC6E37-E17C-2	1916-ACD5-7EBBF	/root/test/His/test002.jsp	2022-08-11 18:30:49	Elta	2.0	
		D	文件异常删除		65DC8E37-E17C-4	1916-ACO5-7EB8F	/root/test/file/test002.jsp	2022-08-11 18:13:31	Eta	0.0	
		28	文件异浓删除		65DC6E37-E17C-4	016-ACD5-7EBBF	/root/fast/file/bast002.js	2022-08-11 18:13:27	Citrat .	246	
		C 48	文件异宗图题		65DC8E37-E17C-4	1016-AC05-7EB8F	/root/test/file/test001.html	2022-08-11 18:13:02	EIM	0.00	
			文件异常添加		65DC6E37-E17C-4	1916-ACDS-7EBIF	/root/test/file/xinjian.js	2022-08-11 18:11:35	elter	240	
		0 98	文件研究原则		650C8E37-E17C-4	1916-AC05-7EB8F	/root/fest/file/xinjisn.js	2022-08-11 18:11:27	EMB	0.6	

如上图所示,防护状态包括防护总览、防护文件状态图和告警列表。

防护总览

如下图所示,在防护总览中您可查看今日文件变动数、最近 15 天文件变动数、防护服务器数、防护 目录数、防护文件总数和未绑定/已绑定服务器配额数。



防护文件状态图

如下图所示,您可查看当前防护文件统计图 Top5(最近 15 天)和文件变动数 Top5(最近 15 天)的统计图。

当相同护文件供计图Top5	文件探惑號(Top5 (編216天)
	/tout/web/webput/1111.cm
- 10 - 2	/vst/wet/wetga/cst012.ss
6	/vst/het/weigst/csbf22.ss
	/nst/wat/watguthtm0013emi
	/rost/twst/warque/htm/002.tml



告警列表

如下图所示,您可查看文件增加、删除、修改异常的告警列表,包括告警等级、告警名称、受影响 服务器、文件路径、时间、防护状态和操作。告警列表默认按照时间排列,最后发生的篡改告警排列在 最上方。

38					最近一月 🗸	服务器名称 > 输入搜索条件	0 0
	告警等级	告警名称	受影响服务器	文件路径	时间	防护状态	操作
	中危	文件异常添加	ACD75A59-39CC-42E8-8432-EF91D	c:\test\file\文件004 - 副本.js	2022-07-26 14:42:29	已防御	26
	高危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/php002.php	2022-07-25 14:26:18	已防御	26
	商危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/css001.css	2022-07-25 14:26:18	已防御	忽略
	商危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/php001.php	2022-07-25 14:26:18	已防御	26
	高念	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/xinjian.css	2022-07-25 14:26:18	已防御	忽略
	R 2	文件异常删除	53BA8C27-2461-4D6D-9B82-A4B29	/root/test/wangye/css002.css	2022-07-25 14:26:18	已防御	忽略
	高危	文件异常删除		/root/test/wangye/html002.h	2022-07-25 14:26:18	已防御	忽略
	高危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/html001.h	2022-07-25 14:26:18	已防御	忽略
	中危	文件异常添加	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/1111.css	2022-07-25 14:26:07	已防御	忽略
	中意	文件异常添加		/root/test/wangye/1111.css	2022-07-25 14:26:05	已防御	忽略

共10条 10条/页 · · · 前往 1 页

如下图所示,您可根据时间、服务器名称和服务器 IP 进行告警筛选和查询,可选时间为最近一周、 最近一月和最近三月。

28				[最近一月、、、、	服务器名称 ~ 输入搜索条件	0 0
	告警等级	告警名称	受影响服务器	文件路径	时间	防护状态	操作
	中急	文件异常添加	ACD75A59-39CC-42E8-8432-EF91D	c:\test\file\文件004 - 副本.js	2022-07-26 14:42:29	己防御	思略
	高仓	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/php002.php	2022-07-25 14:26:18	己防御	3略
	高位	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/css001.css	2022-07-25 14:26:18	己防御	216
	高危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/php001.php	2022-07-25 14:26:18	己防御	316
	毫後	文件异常删除	53BA6C27-2461-4D6D-9B82-A4829	/root/test/wangye/xinjian.css	2022-07-25 14:26:18	已防御	意略
	高高	文件异常删除	538A6C27-2461-4D6D-9B82-A4829	/root/test/wangye/css002.css	2022-07-25 14:26:18	己防御	忽略
	亮色	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/html002.h	2022-07-25 14:26:18	己防御	2.85
	幕危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/html001.h	2022-07-25 14:26:18	已防御	凯略
	中應	文件异常添加	538A6C27-2461-4D6D-9B82-A4829	/root/test/wangye/1111.css	2022-07-25 14:26:07	己防御	思略
	中危	文件异常添加	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/1111.css	2022-07-25 14:26:05	己防御	216

共 10 条 10条/页 ~ < 1 > 前往 1 页

若当前告警不需要再展示,选择忽略或批量忽略操作后,则该告警不再展示在列表中,如下图所示:

€₹

28					最近一月 🗸	服务器名称 > 输入搜索条件	Q Q
告望	警等级	告警名称	受影响服务器	文件路径	时间	防护状态	操作
0	危	文件异常添加	ACD75A59-39CC-42E8-8432-EF91D	c:\test\file\文件004 - 副本.js	2022-07-26 14:42:29	已防御	忽略
	1. Contraction of the second sec	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/php002.php	2022-07-25 14:26:18	已防御	08
	ß	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/css001.css	2022-07-25 14:26:18	已防御	忽略
	危	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/php001.php	2022-07-25 14:26:18	已防御	3B
	危	文件异常删除	53BA6C27-2461-4D6D-9882-A4829	/root/test/wangye/xinjian.css	2022-07-25 14:26:18	已防御	20.95
	a	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/css002.css	2022-07-25 14:26:18	已防御	2385
	8	文件异常删除	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/html002.h	2022-07-25 14:26:18	已防御	88
	危	文件异常删除	53BA6C27-2461-4D6D-9B82-A4B29	/root/test/wangye/html001.h	2022-07-25 14:26:18	已防御	28
() ()	fo.	文件异常添加	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/1111.css	2022-07-25 14:26:07	已防御	28
•	龍	文件尋常添加	538A6C27-2461-4D6D-9882-A4829	/root/test/wangye/1111.css	2022-07-25 14:26:05	已防御	忽略

共10条 10条/页 ~ < 1 > 前往 1 页

4.7.2 防护管理



如上图所示,防护管理页面为您展示添加防护服务器的引导步骤和已添加的防护服务器列表。 若您尚未添加过防护服务器,则参考下方创建服务器安全卫士步骤;若您已经添加过防护服务器, 则参考下方添加防护服务器步骤。

创建网页防篡改

本节为您介绍在控制台创建网页防篡改(原生版)的操作步骤。

操作步骤:

在天翼云控制台中,安全分类下,点击"网页防篡改(原生版)"或"服务器安全卫士(原生版)";



◆ 天翼云 2010年0 至25月末 - 秋葉 -		⊕中文 • ● #Los •
COD Internet internet	94 v	井井県豊田 市場時の中国北東市内町の時の
(面)	■ ■教育な上工(信号版) 上行成長者などが学校。	→ 時代最初時 (100) (100)(100)(100)(100)(100)(100)(100
推躍与前編 ~	於職等項 云主和已何張與電音系	
血液酸酶 ~	WERKE MERINARIZA	XHALDO-INAL SHIR HERATE XHALDO-INAL XHALDO-IN
A 開始する日間中台 同一回Dowopyを目的目的		容弱服务 ~
应用市场 ✓	E Bidilit Decisionation	
二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	ODOSANOP ODOSANO	数据库 ~
	Elementation and a second seco	
활化分析 → はRA/大式放平台 (※) 「おり (16月3月1日、自然会合成部月日、昭元史出版第三、金融和新聞会合号能力、取出版下Apenter Hadrogs 1.2.1、 (※) 「おり (16月3月1日、自然会合成部月日、昭元史出版第三、金融和新聞会合号能力、取出版下Apenter Hadrogs 1.2.1、 (※) (※) (※) (※) (※) (※) (※) (※) (※) (※)		3133.87888850-0-5.07.00, N-210688 Q 205.07897-0-64 106.02-990704894988

2. 当您购买网页防篡改(原生版)配额后,进入"创建网页防篡改"页面;

		网页防篡改(原生版)	未應定的記號数: 6个,已應定服务器記號: 2个,到期时间: 2023年03月27日 務支記録	
•	服务器安全卫士(原生版)	與贡防篡改		Start E
۲	安全概览	仅需简单3步,即可创建网页防篡改,保障您的网站信息不被恶意篡改!		
•	资产管理	 (1) 选择服务器(2) 添加防护目录 	3 异常警告	
v	基线管理	选择要选加深的需收 危加积的防御 能力的服务器 目录	发现目录异常时 递知告誓	
	入侵检测 ~ ~ < 网页防篡改 (原生版)	创建网页的事改		

 4击"创建网页防篡改",在弹出的创建网页防篡改对话框中,根据页面提示进行配置,配置 顺序为:添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护;



创建网页防篡改				×
选择添加防护服务器				
			请输入服务器IP或名称 Q	C
	服务器名称	服务器IP	操作系统	
	ecm-21a3	172.31.0.9	windows	
	ecm-46ce	172.31.0.114	windows	
	ecm-1c9b-0008	172.31.0.120	linux	
	ecm-1c9b-0009	172.31.0.62	linux	
	ecm-1c9b-0004	172.31.0.136	linux	
	ecm-1c9b-0005	172.31.0.215	linux	
	ecm-1c9b-0007	172.31.0.67	linux	
	ecm-1c9b-0001	172.31.0.166	linux	
	ecm-1c9b-0003	172.31.0.36	linux	
	ecm-1c9b-0002	172.31.0.218	linux	
			共 31 条 く 1 2 3 4 > 前往	1 页
┃ 选择配额防护				
购买配额			请输入防护配额ID Q	C
	配额ID		配额到期时间	
	8cfa5554c0b245929f4c4af299efbd9f		2025年03月06日	
			共1条 < 1 > 前往	1 页
		取消下一步		

 如上图所示,该服务器列表中,展示用户所有的防护列表的服务器;配额列表中,展示用户所 有的配额。选择需要防护的服务器,并选择配额后,方可进入下一步;

创建网页防篡词	<u>م</u>							
📕 建议您使用白名	单模式,在该模式下,会对添加的防护目录和文件类型进行保护。黑名单模式下,会防护目录下所有未排除的子目录、文件类型和指定文件。 黑名单模式							
* 防护目录:	产目录: 请输入需要防护的目录,目录当前最大支持2G							
* 防护文件类 型:	.php @ .php5 @ .phtml @ .jsp @ .jspx @ .asp @ .aspx @ .html @ .htm @ .shtm @ .shtml @ .css @ .js @ .json @ .xml @ .ini @ .conf @ .yaml @ .toml @ .jpg @ .png @ .gif @ .lco @ .cgi @	~						
* 本地备份目 录:	请输入需要备份的指定目录							
	取 消 开启防护							

€₹

 添加防护目录分为添加白名单或添加黑名单2种模式,上图为白名单模式。填写防护目录、防 护文件类型和本地备份目录,点击"开启防护"后,即开始对配置的文件进行防护;

创建网页防篡改	ι	×						
■ 建议您使用白名	单模式,在该模式下,会对添加的防护目录和文件类型进行保护,黑名单模式下,会防护目录下所有未排除的子目录、文件类型和指定文件。 <mark>自名单模式</mark>							
*防护目录:	请输入需要防护的目录或文件, 目录当前最大支持2G							
排除子目录:	请输入无需防护的子目录,采用相对路径填写方式							
排除文件类型:	log 🕲 .txt 🛞 ldb 🛞	\sim						
排除指定文件:	请输入无需防护的文件全目录地址,多个文件之间用逗号隔开							
*本地备份目	请输入需要备份的指定目录							
录:								
	取 消 开启防护							

 6. 上图为黑名单模式。选择防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录,点击"开启防护"后,即开始防护目录下所有未排除的子目录、文件类型和指定文件。其中,防护目录和本地备份目录为必填。

濁加防护服务器				服务器P Q C
服务器 操作系统	防护目录数	备份目录	防护状态	操作
ecm-3db0 32F1DF23-6685-4475-AC35-6371 linux	1	/bak/		添加防护目录 编辑备份目录 解绑配额 删除服务器
防护目录	防护文件类型	防护类型		操作
/root/test/	.php, php5, phtml, jsp, jspx, asp, aspx, html, htm, st s, json, xml, ini, conf, yaml, toml, jpg, png, gif	htm, .shtml, .css, .j 白名单		SATE MIR
> ctcss-server-0-1 53BA6C27-2461-4D6D-98 linux	1	/root/test/bak/		添加防护自录 编辑备份自录 解明配版 删除服务器
> ecm=5ca3 6190b236=8bba=4c10=b2d4=5a1ef Windows2016=DataCenter	1	c:\bak\		激加防护目录 编辑备份目录 绑定配额 删除服务器
> ecm-1c9b-0006 A7811C7A-B3C8-4B80-A5A linux	1	/root/bak/		添加防护目录 编辑备份目录 绑定配额 删除服务器
> ecm-4743 ACD75A59-39CC-42E8-8432-EF9 windows	1	C:\test\bak\		激加防护目录 编辑备份目录 解绑配额 删除服务器
> ecm-ec83 E93A59EC-B176-47C3-BA12-0FB linux	1	/bak/wlj/		派加防护目录 编辑备份目录 胡定配额 删除服务籍

共 6 条 10条/页 < 1 > 前往 1 页

 开启防护后,进入防护服务器列表,展示已添加防护的服务器,以及每台服务器已配置的防护 目录情况。

添加防护服务器

本节为您介绍添加防护服务器的操作步骤。

1. 点击防护管理页面的"添加防护服务器",如下图所示:



潮	0防护服务	2						服务费户	0
	服务器		操作系统	防护目录数	备份目录	防护状态		操作	
~	ecm-3	db0 32F1DF23-6685-4475-AC35-6371	linux	1	/bak/			添加防护目录 编辑各份目录 复供配题 表体》	8318
		防护目录		防护文件类型	防护类型		操作		
		/root/test/		.php, .php5, .phtml, .jsp, .jspx, .asp, .aspx, .html, .htm, .shtm, .shtml a, .json, .xml, .ini, .conf, .yaml, .toml, .jpg, .png, .gif	,.css,.j 白名单		編輯】副除		
>	ctcss-s	server-0-1 53BA6C27-2461-4D6D-9B	linux	1	/root/test/bak/			添加防护目录 编辑备份目录 解訴配結 服持部	181
>	ecm-5	ca3 6190b236-8bba-4c10-b2d4-5a1ef	Windows2016-DataCenter	3	c:\bak\			添加防护目录 编辑备份目录 师定配额 删除	8务器
>	ecm-1	9b-0008 A7811C7A-B3C8-4B80-A5A	linux	1	/root/bak/			原加防护目录 编辑备份目录 绑定配额 删除	服务器
>	ecm-4	743 ACD75A59-39CC-42E8-8432-EF9	windows	1	C:\test\bak\			添加防护目录 编辑备份目录 解绑配新 测踪	E6B
>	ecm-ad	83 E93A59EC-B176-47C3-8A12-0FB	linux	1	/bak/wlj/			添加防护目录 编辑备份目录 师定配额 删除	發展調

共6条 10条/页 ~ < 1 > 前往 1 页

在弹出的对话框中,根据页面提示进行配置,如下图所示。配置顺序为:添加服务器->添加防 护目录->添加防护文件类型->添加本地备份目录->开启防护;

创建网页防篡改			×
选择添加防护服务器			
			请输入服务器IP或名称 Q S
	服务器名称	服务器IP	操作系统
	ecm-21a3	172.31.0.9	windows
	ecm-46ce	172.31.0.114	windows
	ecm-1c9b-0008	172.31.0.120	linux
	ecm-1c9b-0009	172.31.0.62	linux
	ecm-1c9b-0004	172.31.0.136	linux
	ecm-1c9b-0005	172.31.0.215	linux
	ecm-1c9b-0007	172.31.0.67	linux
	ecm-1c9b-0001	172.31.0.166	linux
	ecm-1c9b-0003	172.31.0.36	linux
	ecm-1c9b-0002	172.31.0.218	linux
			共 31 条 〈 1 2 3 4 〉 前往 1 页
选择配额防护			
购买配额			请输入防护配额ID Q C
	配额ID		配额到期时间
	8cfa5554c0b245929f4c4af299efbd9f		2025年03月06日
			共1条 〈 1 〉 前往 1 页
		取 消 下一步	



如上图所示,在服务器列表中,展示用户所有的服务器;配额列表中,展示用户当前所有的配额。选择需要防护的服务器,并选择配额后,方可进入下一步;

创建网页防篡改	ά 	×
📑 建议您使用白名	单模式,在该模式下,会对添加的防护目录和文件类型进行保护。黑名单模式下,会防护目录下所有未排除的子目录、文件类型和指定文件。 <mark>黑名单模式</mark>	
*防护目录:	请输入需要防护的目录,目录当前最大支持23	
* 防护文件类 型:	.php @ .php5 @ .phtml @ jsp @ .jspx @ .asp @ .aspx @ .html @ .htm @ .shtm @ .shtml @ .css @ .js @ .json @ .xml @ .ini @ .conf @ .yaml @ .toml @ .jpg @ .png @ .gif @ .ico @ .cgi @	~
* 本地备份目 录:	请输入需要备份的指定目录	
	取消开始防护	

 添加防护目录分为添加白名单或添加黑名单 2 种模式,上图为白名单模式。选择防护目录、防 护文件类型和本地备份目录,点击"开启防护"后,即开始对配置的文件进行防护;

创建网页防篡改	τ	×								
建议您使用白名	螺 建议您使用白名单模式,在该模式下,会对添加的防护目录和文件类型进行保护。黑名单模式下,会防护目录下所有未排除的子目录、文件类型和指定文件。 白名单模式									
*防护目录:	请输入需要防护的目录或文件,目录当前最大支持2G									
排除子目录:	3录: 请输入无需防护的子目录,采用相对路径填写方式									
排除文件类型:	log @ .txt @ lob	\sim								
排除指定文件:	请输入无需防护的文件全目录地址,多个文件之间用逗号隔开									
*本地备份目	请输入需要备份的指定目录									
录:										
	取 消 开启防护									

 上图为黑名单模式。选择防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目 录,点击"开启防护"后,即开始防护目录下所有未排除的子目录、文件类型和指定文件。其 中,防护目录和本地备份目录为必填选项。

汤加	防护服务	3							服务器P	0
	服务器		操作系统		防护目录数	备份目录	防护状态		操作	
~	ecm-3d	b0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/			添加防护目录 编辑备份目录 解绑配额 删除服	务器
		防护目录		防护文件类型		防护类型		操作		
		/root/test/		.php, .php5, .pht s, .json, .xml, .ln	ml, .jsp, .jspx, .asp, .aspx, .html, .htm, .shtm, .shtml, i, .conf, .yaml, .toml, .jpg, .png, .gif	.css, j 白名单		编辑丨删除		
>	ctcss-s	erver-0-1 53BA6C27-2461-4D6D-9B	linux		1	/root/test/bak/			添加防护目录 编辑备份目录 解绑配额 删除服	诱器
>	ecm-50	a3 6190b236-8bba-4c10-b2d4-5a1ef	Windows2016-DataCenter		1	c:\bak\			添加防护目录 编辑备份目录 绑定配额 删除服	绣器
>	ecm-1c	9b-0006 A7811C7A-B3C8-4B80-A5A	linux		1	/root/bak/			添加防护目录 [编辑备份目录] 绑定配额 删除服	绣器
>	ecm-47	743 ACD75A59-39CC-42E8-8432-EF9	windows		1	C:\test\bak\			漆加防护目录 编辑备份目录 解绑配锁 删除服	绣器
>	ecm-ac	83 E93A59EC-B176-47C3-BA12-0FB	linux		1	/bak/wlj/			添加防护目录 编辑备份目录 鄉定配額 删除服	绣背

共 6 条 10条/页 ~ < 1 > 前往 1 页

こ 美天 うう

如上图所示,开启防护后,进入防护服务器列表,展示已添加防护的服务器,以及每台服务器
 已配置的防护目录情况。

防护服务器列表

本节为您介绍已经添加的防护服务器列表。

为您展示当前已添加的服务器的列表,包括添加的服务器、操作系统、防护目录数和备份目录、防 护状态和操作,可以对该服务器的防护状态进行开启/关闭,并可进行添加防护目录、编辑备份目录、绑 定/解绑配额和删除服务器操作。

添加	防护服务	10							印器务器印	۵ ۵
	服务器		操作系统		防护目录数	备份目录	防护状态		操作	
~	ecm-3d	db0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/			添加防护目录 编辑备份目录 解绑配额 删除服	3务器
		防护目录		防护文件类型	!	防护类型		操作		
		/roat/test/		.php, .php5, .p s, .json, .xml, .	html, .jsp, .jspx, .asp, .aspx, .html, .htm, .shtm, .shtml, ni, .conf, .yaml, .toml, .jpg, .png, .gif	.css, j 白名单		编辑 删除		
>	ctcss-s	server-0-1 53BA6C27-2461-4D6D-9B	linux		t	/root/test/bak/			添加防护目录 编辑备份目录 解绑配额 删除服	(务器
>	ecm-50	ca3 6190b236-8bba-4c10-b2d4-5a1ef	Windows2016-DataCenter		1	c:\bak\			添加防护目录 编辑备份目录 绑定配额 删除服	网络
>	ecm-10	c9b-0006 A7811C7A-B3C8-4B80-A5A	linux		1	/root/bak/			添加防护目录 编辑备份目录 绑定配额 删除器	3务器
>	ecm-41	743 ACD75A59-39CC-42E8-8432-EF9	windows		1	C:\test\bak\			添加防护目录 编辑备份目录 解绑配额 删除器	研題
>	ecm-ad	83 E93A59EC-B176-47C3-BA12-0FB	linux		1	/bak/wlj/			添加防护目录 编辑备份目录 绑定配额 删除器	務部

共 6 条 10条/页 < 1 > 前往 1 页

防护目录管理

本节为您介绍已添加防护服务器的防护目录管理。

可对服务器已添加的防护目录进行编辑、删除操作,如下图所示:

	服务器		操作系统		防护目录数	备份目	录	防护状态		操作
>	ecm-3	b0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/				添加防护目录 编辑备份目录 绑定配额 删除服务器
~	ctcss-s	erver-0-1 53BA6C27-2461-4D6D-9B	linux		1	/root/te	est/bak/			添加防护日录 编辑备份日录 解绑配版 删除服务器
		防护目录		防护文件类型			防护类型		操作	7
		/root/test/wangye/		.php, .php5, .ph html, .css, .js, .j	tml, .jsp, .jspx, .asp, .aspx, .html, .htm, .s son, .xml, .ini, .conf, .yaml, .toml, .jpg, .pr	htm, .s ng, .gif	白名单		编辑	

点击操作中的"编辑"时,弹出"编辑防护目录"对话框,如下图所示,可对您已经添加的防篡改 策略进行修改。



编辑防护目录		×
▲ 建议您使用白名!	单模式,在该模式下,会对添加的防护目录和文件类型进行保护。黑名单模式下,会防护目录下所有未排除的子目录、文件类型和指定文件。 <mark>黑名单模式</mark>	
*防护目录:	/root/test/	
* 防护文件类 型:	php @ php5 @ phtml @ jsp @ jspx @ asp @ aspx @ html @ htm @ shtml @ .css @ js @ json @ .xml @ ini @ .conf @ .yaml @ .toml @ jpg @ .png @ .gif @	~
* 本地备份目 录:	/bak/	
	取 消 开启防护	

点击操作中的"删除"时,弹出"删除"对话框,可对您已经添加的防篡改策略进行删除。

删除	,	×
A	确认要删除该防护目录?	
	取消 确定	

若您需要为已添加防护的增加防护目录,请点击操作中的"添加防护目录",如下图所示:

	服务器		操作系统		防护目录数	备份目录	防护状态		操作
>	ecm-3d	b0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/			添加防护目录 编辑备份目录 绑定配额 删除服务器
~~	ctcss-si	erver-0-1 53BA6C27-2461-4D6D-9B	linux		1	/root/test/bak/			漆加防护目录 编辑备份目录 解绑配额 删除服务器
		防护目录		防护文件类型		防护类型		操f	乍
		/root/test/wangye/		.php, .php5, .ph html, .css, .js, .js	tml, .jsp, .jspx, .asp, .aspx, .html, .htm, son, .xml, .ini, .conf, .yaml, .toml, .jpg, .	shtm, .s 白名单 png, .gif		1944	a 1 mire

点击后弹出如下对话框,输入防护目录、防护文件类型后,可为本台服务器增加一条新的防护策略。



添加防护目录	×
▲ 建议您使用白名单 类型和指定文件。 黑	模式,在该模式下,会对添加的防护目录和文件类型进行保护。黑名单模式下,会防护目录下所有未排除的子目录、文件 <mark>名单模式</mark>
* 防护目录:	请输入需要防护的目录,目录当前最大支持2G
* 防护文件类 型:	.php S .phtml S .jsp S .jsp S .asp S .aspx S .html S .htm S .shtm S .shtml S .css S .js S .json S .xml S .ini S .conf S .yaml S .toml S .jpg S .png S .yaml S .gif S .ico S .cgi S
*本地备份目	/root/test/bak/
录:	
	取 消 开启防护

若您需要修改已添加防护服务器的本地备份目录,请点击操作中的"编辑备份目录",修改本地备份目录后,点击确定后即可完成编辑,如下图所示:

修改备份目录		×
一 一世名 (1) 日 日		
本地备份目录 /root/test/bak/		
100t/ test/ bak/		
	取 消 确 定	

若您某台服务器不再需要网页防篡改防护,可以关闭该服务器的防护状态,如下图所示:

	服务器		操作系统		防护目录数	备份目录		防护状态		操作
>	ecm-3c	b0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/				添加防护目录 编辑备份目录 绑定配额 删除服务器
~	ctcss-s	erver-0-1 53BA6C27-2461-4D6D-9B	linux		1	/root/test/bak/	[漆加防护目录 编辑备份目录 解绑配额 删除服务器
		防护目录		防护文件类型		防护类	型		操作	E
		/root/test/wangye/		.php, .php5, .ph html, .css, .js, .j:	tml, .jsp, .jspx, .asp, .aspx, .html, .htm, .sh son, .xml, .ini, .conf, .yaml, .toml, .jpg, .pn	ntm, .s ig, .gif			编辑	1 808



在关闭该服务器的防护后,您可以解绑该服务器的防护配额,点击"解绑配额",如下图所示:

服务器	操作系统	防护目录数	备份目录	防护状态	操作
> ecm-3db0 32F1DF23-6685-4475-4	C35-6371 linux	1	/bak/		添加防护目录 编辑备份目录 佛定配额 删除服务器
 ctcss-server-0-1 53BA6C27-2461- 	4D6D-9B linux	1	/root/test/bak/		添加防护目录 编编备份目录 解绑配額 删除服务器
防护目录		防护文件类型	防护类型		操作
/root/test/wangye/		.php, .php5, .phtml, .jsp, .jspx, .asp, .aspx, .l html, .css, .js, .json, .xml, .ini, .conf, .yaml, .	.htmi, .htm, .shtm, .s .tomi, .jpg, .png, .gif		9648 2010

点击后弹出如下对话框,确定后该配额与服务器解绑。解绑后该配额可以与其他服务器进行绑定, 为其他服务器提供防护。

解绑				×
A	确定要解绑机器吗?			
		取消	确定	

在解绑配额完成后,可以点击"删除服务器",如下图所示:

	服务器		操作系统		防护目录数	备份目去	Ř	防护状态		操作
Σ	ecm-3d	b0 32F1DF23-6685-4475-AC35-6371	linux		1	/bak/				添加防护目录 编辑备份目录 绑定配额 删除服务器
Ŷ	ctcss-s	erver-0-1 53BA6C27-2461-4D6D-9B	linux		1	/root/te	st/bak/			添加防护目录 编辑备份目录 绑定配额 删除服务器
		防护目录		防护文件类型			防护类型		操作	Ę
		/root/test/wangye/		.php, .php5, .pht html, .css, .js, .jt	ml, .jsp, .jspx, .asp, .aspx, .html, .htm, .s son, .xml, .ini, .conf, .γaml, .toml, .jpg, .pi	shtm, .s ing, .gif	白名单		184	5 10100



点击后弹出如下对话框,确认后该服务器删除完成,即该服务器不再展示在防护服务器列表中。若 需要为该服务器重新添加防护,需要重新添加服务器。

删除服约	5器	×
A	您确认要删除服务器吗?	
	取 消 确 定	

4.7.3 防护配额

	网页防篡改(原生版)			来那边的配数数: 1个,已那边服务都配数: 2个,到期时间:	2022/07/R05E
服务器安全卫士(原生版)	時护状态 防护管理 <u>防护配置</u>				
版页 资产管理 ~ 基达管理 ~	1.8289299	I RESIL			
業第日増 人運始調 ~ 同売防算改 (原生紙) 设置中心 ~	4	= 850 1 = 450 1	4		- EN 4 - EDR 0 - EDR 0
			erts - trats - erts	服务符名符 撤货费用	0 0
	A2MID	配额状态 =	御定服务器 使用状态 >	开通时间 0 初期时间 0	编作
	Bcra0054c0b24502094c4ar209wtbc0f	2.8	未調定	2022/00/078 2026/00/8068	1817 1817
	67c011#3e234d83ab04991129b1ed5d	正常	172.31.0.238 (%) 使用中	2022年03月07日 2022年06月05日	(第12) (第12)
	0b4218b4eC0140ce88b5be90525e8be4	2.11	172.31.0.208 (私) 使用中	2022年03月07日 2022年00月05日	1817 IB17
	Too-4ed#8d5394e11e917c0a72052c2829	2x	192.108.16.228 (私) 使用中	2022年03月07日 2022年07月06日	1817 1817
				其4条 <u>10条/賞、</u> <	1 日 前任 1 页

如上图所示,防护配额为您展示配额的统计和配额的详情列表。 若您未购买网页防篡改的防护配额,则展示如下页面:



 部 部 服务器安全卫士(原生版) 概定 	网页防器改 (原生版) 网络政治者者关合针用规定曲线中夺在的源源,通过在网页中每人中法地特列网页内容进行描改等力式,进行中点年标成者思想应至为市场品。 网页被岩质器改合影响应正常功问网页内容,进可能会导致严重的经济统外、血模块关系呈更就出风险,同页防御器 服务,可定时正因其由且技术通过备付需要需要因效力交相目录。 保護重要系统的间站或者不被恶意意识。 防止出现转马,展展、带法输入功物运動、 色情等内容,
 第二管理 へ 概辺 最外部列表 第二門指纹 基线管理 ~ 減用目摘 入侵检測 ~ 网気防器改(博生版) 设置中心 ~ 	空対防部 定文別が用意えた年、発気、及気気度振びが常略 含単安全領域、支持境所回防庁、快速物理安全的域、満足安全合成温質、技術服客的攻击体部 第二日の「「「「」」」」」「「」」」」」「」」」「」」」「」」」」「」」」」「」」

点击"立即升级",进入订购页面,勾选我已阅读,理解并接受《天翼云网页防篡改(原生版)协 议》,点击"立即购买"按钮,即可开通网页防篡改(原生版)服务,如下图所示:

	制中心服务列	表▼ 收藏▼	Ä						Ē)中文 🔻	◎ 保定	💌 📀 H	ie 🔻	lt. ?
订购网页防篡改														
丁购须知: 本订购	页购买的是网页防算	<u>創政的配額数</u> ,非	表示您需要网页防	5篇改防护的服务	器数量。例如,	防篡改配额数量i	受置为3时,您可	以为3台服务器漆	加防篡改保护。					
购买时长:	 2个月	〇 3个月	 4个月] 5个月	 6个月		 8个月	 9个月	 10个月		 1年	 2年	1	3个月 E
购买数量: -	1 +													
_{費用总计} 2940元														
											1 我已阅读并	同意相关协议 🤇	取消 天擴云网页防	立即购买

购买完成后,即可进入防护配额页面。

配额使用		
		一 使用中 3
	4 ^{总量}	— 未绑定 1

如上图所示, 配额使用统计为您展示正常配额的使用情况统计, 分为使用中和未绑定 2 种状态。



配额状态		
		正常 4
	4	— 已过期 0
		━ 已渡汀 0

如上图所示,配额状态为您展示所有配额的状态统计,分为正常、已过期和已退订3种状态。 配额列表展示正常、已到期、已退订3种状态的配额,销毁的配额不展示在列表中,包括配额 ID、 配额状态、绑定服务器、使用状态、开通时间、到期时间、操作等信息。该列表可根据配额状态、使用 状态、配额 ID、服务器名称和服务器 IP 进行查询。

		肥料状态 ~	< 0	と用状态	后期の	服务器名称	服务器中			0 0
R28iD	配额状态 🔅	绑定服务器			使用状态 🗘	开通时间 🗘	到期时间 0	操作	È.	
8cfa5554c00c245929f4c4at299arbd0f	正常				未绑定	2022年03月07日	2025年03月08日	線式	r Bit	
67c011ft3a234d83ab0409f126b1ed5d	正常	172.31.0.238 (私)			使用中	2022年03月07日	2022年06月05日	1917	au	
0642169-4001149cx88868xx8986828x86xx4	正常	172.31.0.208 (私)			使用中	2022年03月07日	2022年06月05日	探口	r unti	
foc4eda6d8304a1a617c0a72052c2d29	正常	192.168.16.226 (%))		使用中	2022年03月07日	2022年07月05日	線に	r iett	

共 4 条 10条/页 · (1) 前往 1 页

配额计费

本节为您展示配额计费的相关操作,包括配额订购、配额续订、配额退订和到期处理相关操作。

配额订购:前面已详述,此处不再赘述。

配额续订:您可对已订购的网页防篡改(原生版)配额进行续费,需要此配额此时的状态为未到期、 已到期。

如下图所示,对需要续订的配额,点击"续订":

		entis - entis -	12810	服务器名称	服务部の		0 0
R280D	配额状态 0	绑定服务器	使用状态 🗢	开通时间 ⇔	至[期85]间 0	操作	
8cfa5554c0b245929f4c4af299efbd9f	正常		未明定	2022年03月07日	2025年03月06日	续订 退订	I
67c011ff3q234d83ab0499ff29b1ad5d	正常	172.31.0.238 (%)	使用中	2022年03月07日	2022年06月05日	AR17 2017	I
0b42f8b4e00140ce86b8be9952Be6ba4	正常	172.31.0.208 (約)	使用中	2022年03月07日	2022年06月05日	校订 进订	t
1cc-4eda8d8394a1a917cQa72052c2d29	正常	192,168.16.226 (%)	使用中	2022年03月07日	2022年07月05日	续订一进订	Ţ

共4条 10条/页 -> < 1 > 前往 1 页

进入"续订"页面后,选择该配额需续订的时长,勾选我已阅读,理解并接受《天翼云网页防篡改 (原生版)协议》,点击"立即购买"按钮,即可对该配额的服务器安全卫士(原生版)服务进行续费, 如下图所示:

€天翼云

网页防篡改配备	领续订						
配额ID		绑定服务器名称		绑定服务器私有IP	配额到期时间	状态	
9adf1627b9eb41	4584b67ddcf17fca02				2022-01-13 09:23:34	未绑定(正常)	
续订时长:	月	× 1	~				
2置费用:	¥ 980						
解计费详情							
							立即购到
						我已阅读并同意相关协议 《天	夏云网页防算改服务协议

配额退订:根据您的需求,可对正常状态的配额进行退订,遵循天翼云统一的退订规则。如下图所示,对需要退订的配额,点击"退订":

		記録状态 ~ 使用状态	Esto.	服务器名称	服务器中		2 0
配額の	配额状态 🗘	绑定服务器	使用状态 ≑	开通时间 0	数(期)时(ii) 令	操作	
8cfa5554c0b24592914o1af299efbd91	ΞŦ		未期定	2022年03月07日	2025年03月06日	续订 退订	
67c011ff3a234d63sb0499f129b1ed5d	王常	172.31.0.238 (紙)	使用中	2022年03月07日	2022年06月05日	線订 銀订	
Ob4218b4e00149ce98be8be99529e8be4	王家	172.31.0.208 (私)	使用中	2022年03月07日	2022年06月05日	续订 退订	
fcc4eda6d6394a1a917c0a72052c2d29	王宗	192.168.16.226 (私)	使用中	2022年03月07日	2022年07月05日	HALT MAIN	
87c0111562344836804399128014056 0x421834600148x68805055868564 ftco4es809603441601720872205222829	王幣 王幣 王幣	172.31.0.238 (板) 172.31.0.208 (板) 192.168.16.226 (板)	使用中 使用中 使用中	2022年03月07日 2022年03月07日 2022年03月07日	2022#06月05日 2022#06月05日 2022#07月05日	線訂 期訂 续訂 題訂 銀訂	

共 4 条 10条/页 · (1) 前往 1 页

进入"退订"页面后,您需要进行确认退订的规则和金额,点击"退订"按钮,即可对该配额的网 页防篡改(原生版)服务进行退订,如下图所示:

网页防篡改配被退订						
出了原铅: 出了原铅:出现品的出资源不可称复; 2、确定品订前指数:中点发展指令成发展: 3、除特殊的定 (云电乱,云阳能进着算单 4、出订可能会导致其它存在的关系业务产 出订双对读者者;进行原始出统	98. 1月20日 - 通行新史建立和明白) しか、通行新的史道所有以多点的引 生意意。	2個篇15天戲釋放:				
产品名称	配額ID	绑定服务器名称	鄉定服务器私有IP	配額到期时间	KS.	
网页防装改	fa0f1b9ea22c4bdab3d886d7c5248faa	centos194	172.18.208.194	2022-01-07 09:35:27	使用中(正常)	
						建订 以退订上述用页防算改配模

到期处理: 您购买的全部配额均到期后, 进入网页防篡改(原生版)页面后, 会提醒您进行购买。



4.8. 设置中心

4.8.1 配额管理

88		配額管理				购买服务器交全卫士 (原生版)
 一一一股 一次1 一次1 ※ <li< th=""><th>服务器安全卫士(原生版) 安全概定 ① 资产管理 ~ 基线管理 ~</th><th>(使用指引 (1) 約米配約 効果的時時時期起来的**単純素、有有資源的時件資素、資産者有 上力**約末期時期定定上と(時生物)</th><th> (2) 安慰Agent 市田県市会社上(第五部)局所, 四葉県売島四戸県外田安府 みの中, 利用市場発展的ご公式県委員路。 「安認Assent」 </th><th>③ 设置音整通知 合整通知设置后、风险符合则 合型、规构进设置。</th><th>(4) UARSA Refer Re</th><th>irasətar, sansətarata M.</th></li<>	服务器安全卫士(原生版) 安全概定 ① 资产管理 ~ 基线管理 ~	(使用指引 (1) 約米配約 効果的時時時期起来的**単純素、有有資源的時件資素、資産者有 上力**約末期時期定定上と(時生物)	 (2) 安慰Agent 市田県市会社上(第五部)局所, 四葉県売島四戸県外田安府 みの中, 利用市場発展的ご公式県委員路。 「安認Assent」 	③ 设置音整通知 合整通知设置后、风险符合则 合型、规构进设置。	(4) UARSA Refer Re	irasətar, sansətarata M.
	満利日福 入価检測 ~ 同页防器改(原生版) 设置中心 ^	1 全山和田田市市		企业版配額状态		
	用步克产设置	12	- 6070 4 - 4082 8		18	- 2311 12 - 12311 0 - 123117 6
		和關係订 批關升級		enus - anus	<	user a a
		DI的名	配额规格	記続状态 使用状态	纲定服务器	配额到期时间 操作
		d8f8740cea024bcaa2f84f02b9c0ae9	企业版	正常 未捞足		2022-09-30 標訂 過订
		36c5589fb25f4e1994e926b2e42da94e	企业版	正常 未생定		2022-09-30
		3035bdex3ab44aa1b82e63a3bdfdc4ad	企业版	正常 使用中	ecm-9774 09352FAE-5F9A-4FDF-8CEE-D4C 10.10.1.55(%)	2022-10-22 接订 脱订

如上图所示,配额管理为您提供了服务器安全卫士(原生版)配额的管理入口。最上方展示了服务 器安全卫士(原生版)配额购买入口,您可以根据 2.3 节的订购流程进行购买;其次展示了使用指引, 您可以根据使用步骤去进行操作;中间位置展示了配额的统计情况,左边展示的是正常配额的使用情况, 分使用中和未绑定 2 种;右边展示了除已销毁以外的所有配额,分为正常、已过期和已退订 3 种情况。 最下方是订购配额的详细列表,展示了配额 ID、配额规格、配额状态、使用状态、绑定服务器、配额到 期时间和操作。该列表可以根据配额状态、使用状态、配额 ID、服务器名称和 IP 去进行查询。

4.8.2 同步资产设置

88	Ê	同步资产设置		
		设置项目	同步周期	详情
	服务器安全卫士(原生版)	同步页/*	0 12小时 0 24小时	按周期走时同步忽服户下的所有资产
	概览			
	资产管理 ~			
	基线管理			
	基线检测			
	弱口令检测			
	漏洞扫描			
	入侵检測			
	网页防篡改(原生版)			
	设置中心			
	同步资产设置			

如上图所示,同步资产设置为您提供了资产同步时间的设置入口。



您可选择自动同步资产的时间,分为12小时和24小时,默认24小时1次,默认每次同步开始时间 为01:00。



5. 最佳实践

5.1. 快速掌握服务器安全态势

服务器安全卫士(原生版)提供的服务是一个用于保障主机整体安全的安全服务,能实时监测主机中的 风险并阻止非法入侵行为、一键核查漏洞及基线、全面识别主机中的信息资产,帮助您管理主机的安全 状态。

在"服务器安全卫士(原生版) > 概览"页面查看最近7日待处理风险、防护状态、风险趋势和最近7 日风险动态,帮助您实时了解云主机的安全状态和存在的安全风险。

俞	安全概定							PERDE DIS-DE-INVESTOR
服务器安全卫士(原生版)	1. 截至7日14年1月1日				1 mmm			
P241	() 0			·····································	1 Same 101	2 and a second second	Bianor ini	9 5
載式 設計款門書 由产体は	Ante un 首 <mark>0</mark>	Allette (a) 近 <mark>0</mark>	Anten wu 首 <mark>0</mark>	AURITE (86) 1월 0	0	Cen III 0	0 1810-8 101	
- RANG	1 830.000				1 setue			
1813-942.00 674540	a			E148 23/8	26	8002	8.000004 +22.00	£5
								NOB (1 (80) 1
	1,	1 2	9 F	Sep 2				

风险统计	说明
最近7日待处理风险	您可以查看入侵检测、漏洞风险、安全基线、网页防篡改及 对应的风险主机情况
防护状态	您可以查看用户资产情况,包括主机总数、企业版防护、基 础版防护、防护中、已关闭、已离线、未安装客户端的云主 机台数
风险趋势	您可以查看近7天、14天、30天的风险趋势图



风险统计	说明
实时动态	您可以查看当前最新发现的风险事件详情

5.2. 查看单台服务器风险

1、通过点击"资产管理>服务器列表",进入服务器列表详情页面,可以看到全部主机的防护状态和风险情况,包括全部主机、风险主机、企业版主机、基础版主机、已离线主机、未防护的主机。

	8587A										RTERIOR INC. OR	
₩男樹安全卫士(原生報)	2255 RMEM. 20	wan Buyan	R REPRES	ORMER								
FIRE	ER-gen ER-DHS-						2.01 × April	et - tret	- 3350	- BRESS	88-1289-591	0 0
R/*#18	878	展在系统	115	Apert212	EPU.C	8827.5	ESU3	人學性制	#8548	9285	NUMBER	85
現況 <u>第书刊</u> 作派	WYNERSCH BE20004-7070 102.103.1-682	-d anges	NEEDER	45	-	*1	2-14W	1	3	1	2	tanga semit Antir Mitoret
- 87年8位 第15年9日 -	100.01610 0+000039+-0000-001 100.1006(7.1006)	IT WAR	NRATIN	4n	-	**	2118	*			3	CREE FIRM
基48531 前口115531	Gardone Mobartzs-6368-49 19().198.1.40(0	e	100004	ais	1.01	***	#14%		3			CARE FIRT
ERITA -	winteraction Exercise Constant	undoes	NEEDER	- 61	1179	**	#12.6					CHART ADDR
株式加載市 (地头板) 単数中心 -	Controls Nationale Analysis	T	A83274	65	124	201	810.6			140		CREA HEAVY

2、在搜索框中输入您需要查看的服务器名称或 IP,则显示出该服务器的名称、ID、IP、操作系统、地域、 Agent 状态、防护状态、风险状态、入侵检测风险数、漏洞风险风险数、安全基线风险数、网页防篡改 风险数和操作。

单击主机名,进入该服务器资产指纹详情页面。通过此页面,可以快速地查看该服务器的资产详情,包 括端口、账号、进程、软件详情。



â	资产指纹 > 资产指纹详情			
\bigcirc	171N			
服务器安全卫士(原生版)				
板笼	64	名称:win2012-az1-2	ID : 4FC0E48E-E932-C14C-6A81- C6AD4ADC687C	所在区域:内蒙演示环境
资产管理 ^		公间户:	内间沪: 192.168.0.18	绕像:
截览 服务器列表 途产活动		创建时间:2022-05-21 00:37:48	劉期 時前前: 2023-05-21 00:37:48	防护状态:防护中
基线管理 ~	资产指纹 入侵检测 黨洞扫描	基线管理 网页防篡改		
嘉洞扫描	第二 至号 进程 软件			
入侵检测 ~				0 Q
网页防篡改(原生版)	緒口号	网络协议	监听IP	监听进程
双重中心	49152	tcp6		wininit.exe
	5985	tcpő	-	System
	445	tcp6	4	System
	139	tcp	192.168.0.18	System
	49166	tcp	0.0.0.0	Isass.exe
	5985	tcp	0.0.0.0	System
	445	tcp	0.0.0.0	System
	49166	tcp6	4	lsass.exe
	49157	tcp6		sychost.exe

3、同时,可以快速查看各个风险事件,包括入侵检测、漏洞扫描、基线管理及网页防篡改的风险情况。

P.A.	肥和::win2012-az1-2	10 : 4FC	06-48E-E932-C14C-6A81-C6A04ADC087C	所在区域:内酿造训环境	
	(c)000 :	19,68,00	192.168.0.18	· · · · · · · · · · · · · · · · · · ·	
	包括他们间: 2022-05-21 00:37:48	3(201)	i : 2023-05-21 00:37:48	$\mathrm{BM}_{\mathrm{P}}(\mathbf{K}^{\mathrm{B}}):\mathrm{BM}_{\mathrm{P}}\Phi$	
指纹 入侵检测 深圳扫描 基	线管理 闷页防篡改				
NUMBER NOTION					
高人は日東 静謐力に取得			全部国际市场 > 第四名	5件 > 读输入关键评语行提供	Q
第12752年 東羽名称	CVE编号	重具等级	1933月7日 ~ 第月8 最后发现时间	6時 · 當地入市協同的行用來 操作	Q
 第125年 新にわじた用 重調名称 Pytion 職入批説物は実用 	CVE编号 CVE-2018-20852	羅興等级 中面	2世界市市6 → 展示名 最后发現时间 2022-06-08 15:05:26	5時	Q
	CVE#8号 CVE-2018-20052 CVE-2019-9740	重用符级 中面 中面	2022-06-08 15:05:24 2022-06-08 15:05:24	5年 学 信知入来研究的対象 第作 単にから見て 加入のそ年 日日 単にから見て 加入のそ年 日日 単にかられて 加入のそ年 日日	Q IntA
INCOLORING INCOLORING INCOLORING INCOLORING INCOLORING INCOLORING INCOLORING	CVE編号 CVE-2018-20852 CVE-2019-9740 CVE-2019-9647	展用等级 98 98 98		58 - dalaration 58 - d	C C C C C C C C C C C C C C C C C C C
	CVE編号 CVE-2018-20552 CVE-2019-0740 CVE-2019-0947 CVE-2014-0905	第三百百位 中在 中在 中在 中在	北京市中田 マ 東京 取用名 和京 和 和京 和 和	58	C. RMA RMA RMA RMA RMA
KARDEN KARDEN KARDEN KARDEN KARDEN Pytton MAREER Pytton MAREER Pytton WERER Pytton WERER Pytton WERER Pytton WERER Pytton WERER Pytton Statement Pytton Statement	CVE編号 CVE-2018-20852 CVE-2019-9740 CVE-2019-9847 CVE-2014-9885 CVE-2014-7185	展開等級 98 98 98 98 98	ま版設現計編 2022-06-08 15:05:24 2022-06-08 15:05:24 2022-06-08 15:05:24 2022-06-08 15:05:22 2022-06-08 15:05:22 2022-06-08 15:05:22 2022-06-08 15:05:22		CQ INTA INTA INTA INTA INTA



5.3. 弱口令安全最佳实践

随着互联网信息化进程的不断加深,用户服务器上运行的应用服务不断增加,而大多数服务都使用账户+ 口令的方式进行鉴权。黑客常以暴力破解的方式去尝试登录暴露在公网上的服务,如果您设置为弱口令 登录,黑客可能会非法登录您的服务器,窃取服务器数据或破坏服务器。因此,定时检查服务器中存在 的弱口令问题,并及时修改为强口令对服务器安全至关重要。本文介绍如何提升登录口令的安全性以及 常见系统登录口令的修改方法。

弱口令带来的危害

在服务器系统中使用弱口令可能会造成以下危害:

1、普通账户使用的弱口令可能会被猜解或被破解工具破解,从而泄露个人隐私信息,甚至造成财产损失。

2、系统管理员账户弱口令可能会导致整个系统被攻击、数据库信息被窃取、业务系统瘫痪,造成所有用 户信息的泄露和巨大的经济损失,甚至可能引发群体性的网络安全危害事件。

如何避免设置弱口令

服务器安全卫士提供系统弱口令和应用弱口令两类弱口令检测,可帮您快速发现主机中存在的弱口令风 险,详细操作参见弱口令检测操作指南。若检测出弱口令,可按以下规则设置复杂口令:

- 密码长度不少于 8 位
- 包含大小写字母、数字及特殊字符
- 密码不包含用户名
- 密码中不含连续的字母或数字

并且建议您每隔3个月更改一次口令。

常见系统口令修改方式

1、 Linux 系统

登录 Linux 系统命令行,执行命令: passwd 根据提示修改用户口令



2、 Windows 系统

登录 Windows 系统,左下角搜索栏搜索打开"设置"窗口,点击"账户",在左侧导航栏中,点击" 登录选项",并根据提示修改口令。

3、MySQL数据库

登录 MySQL 数据库,执行命令:SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');修改 弱口令后,再执行命令:flush privileges;刷新用户信息,使口令修改生效。

4、Redis 数据库

打开 Redis 数据库配置文件 redis.conf,找到" requirepass "配置行,修改弱口令 (password 为登录口令)。

5、PostgreSQL数据库

登录 PostgreSQL 数据库,执行命令: ALTER USER WITH PASSWORD;修改弱口令。

5.4. 漏洞扫描最佳实践

什么是漏洞?

漏洞也被称为软件漏洞或安全漏洞,是指在软件或系统的设计和实现过程中存在的未被发现或被忽视的 缺陷,可以被攻击者利用来获取未授权的访问、修改或删除敏感数据,或对系统进行破坏。漏洞的危害 主要体现在以下几个方面:

对企业的危害

经济损失:漏洞可导致企业遭受不同程度的经济损失。攻击者可以通过恶意代码或其他手段窃取敏感数据、财务信息和客户信息,导致企业面临巨大财务损失。

品牌声誉受损:一旦遭受漏洞攻击,企业的品牌声誉不可避免地会遭受影响。如果数据泄露或其他风险 引起公众关注,相应的负面宣传会对企业造成巨大的损害。

103


对用户的危害

个人信息泄露:攻击者可以通过利用漏洞窃取用户的个人信息,如姓名、地址、手机号、信用卡信息等, 导致用户面临财务损失和其他风险。

盗用身份信息:通过漏洞,攻击者可以盗用他人的身份,访问用户的账号、甚至是社交媒体等,对用户 造成心理困扰和隐私泄露的问题。

对社会的危害

因为漏洞的存在,攻击者可以轻松地进行各种网络犯罪行为,如网络诈骗、恶意软件植入、网络钓鱼等, 给用户、企业、甚至是整个社会带来不可挽回的后果。

如何进行漏洞扫描

漏洞扫描支持定期扫描和立即扫描,同一时间只支持1个漏洞扫描任务。如配置了定期扫描且定期扫描 已经开始执行了,执行立即扫描将会提示您已有任务在执行。如果配置了定期扫描,但是定期扫描开始 执行时,有立即扫描任务在执行,定期扫描任务将不会执行。

建议您配置针对全部服务器每3天凌晨开始执行的定期扫描任务,如果再有对特定的一些服务器的立即 扫描需求,可配置立即扫描任务进行漏洞扫描。

漏洞扫描支持的方式

1、定期扫描:

支持按每天,每3天,每7天指定时间执行了漏洞扫描任务,建议设置为每3天的凌晨2点到凌晨5点 期间进行扫描,一般凌晨2点到5点为业务低谷期间。



定时扫描设置	×
开启定时扫描	
漏洞类别	linux漏洞 windows漏洞
漏洞扫描等级	□ 超高危 □ 超危 □ 高危 □ 中危 □ 低危
定期检测周期	7天 03:00 设置后会在周期选定的时间点开始定期检测
超时设置	0 小时 0 分钟 ⑦ 若单次时长超过设置时长即为扫描失败
服务器分类	● 全部服务器 ○ 自选服务器
描述	请输入内容
	确定取消

2、立即扫描:

根据您的需求随时下发漏洞扫描任务,可点击一键扫描按钮,进行漏洞扫描设置,立即下发漏洞扫描任务。 务。



一键扫描设置		×
漏洞类别	linux漏洞 windows漏洞	
漏洞扫描等级	□ 超高危 □ 超危 □ 高危	□ 中危 □ 低危
超时设置	0 小时 0 若单次时长超过设置时长即为扫描失败	分钟 ?
服务器分类	● 全部服务器 ○ 自选服务器	
		确定取消

查看漏洞扫描结果

漏洞扫描任务完成后,扫描结果展示在"上一次扫描"处。如下图所示,包括扫描时间、漏洞情况和查看详情。

漏洞扫描				白名单管理
!」 需紧急修复的漏洞	[] 未处理的漏洞 0	□□□ 存在漏洞的服务器 → 0	立即扫描 一键扫描	上一次扫描 (扫描时间:2023-11-07 01:00:10) 漏洞 数4688 查看详情 定时扫描已开启 (每天1次,00:00) 设置

点击"查看详情",可以查看上一次扫描的统计情况和基于主机展示的漏洞列表。在统计情况中,可以 查看扫描类别、漏洞类别、开始时间、结束时间、漏洞风险数和风险主机/目标检测主机。在基于主机展 示的漏洞列表中,为您展示服务器、操作系统、检测状态、检测开始时间、检测结束时间和漏洞数量。



漏洞扫描 〉 上一次扫描	苗详情					
扫描类别 漏洞类别	定时扫描 linux漏洞,windows漏洞	开始时间	2023-11-07 00:00:00 2023-11-07 01:00:10	ŭ,	漏洞风险数 4688	风险主机目标检测主机 1 40/116
			10 million		服务器名称 > 输入:	提索条件 (2) (2)
服务器 ecm-yuq	in1 7CEB239B-6775-44	操作系统 linux	检测状态	检测开始时间 2023-11-07 00:00:00	检测结束时间 2023-11-07 01:00:10	漏洞数量 0
100.124.: s-blj-ser 192.168.0	2.104(公) 192.168.0.7(私) ver002 3A04F9BA-C79 0.40(私)	linux	⊘ 检测成功	2023-11-07 00:00:00	2023-11-07 01:00:10	30
192.168.0	et 2F073928-9872-FC7 D.37(私)	linux	✓ 检测成功	2023-11-07 00:00:00	2023-11-07 01:00:10	0

当点击漏洞数量中下方的数字时,跳转至资产详情页面,如下图所示。在资产详情页面,为您展示该服

务器的基本信息和漏洞情况。

く 📋 资产指纹详情				
资产指纹 入侵检测 病毒查杀	漏洞扫描 基线管理 网页阶	方篡改		
加入白名单标记为已处理			全部漏洞等级 > 漏洞名称 > 〕	青输入关键词进行搜索 Q C
漏洞名称	CVE 编号	漏洞等级	最后发现时间	操作
Lua 安全漏洞	CVE-2019-6706	高危	2023-11-07 00:40:55	处理 加入白名单 查看详情
Info-ZIP UnZip 缓冲区错误漏洞	CVE-2016-9844	低危	2023-11-07 00:40:45	处理 加入白名单 查看详情
GNU Wget 安全漏洞	CVE-2018-20483	高危	2023-11-07 00:40:45	处理 加入白名单 查看详情
Info-ZIP UnZip 缓冲区错误漏洞	CVE-2014-9913	低危	2023-11-07 00:40:45	处理 加入白名单 查看详情
Info-ZIP UnZip 缓冲区错误漏洞	CVE-2018-18384	中危	2023-11-07 00:40:45	处理 加入白名单 查看详情

处理漏洞事件

1、标记处理

您可以选择多个漏洞,批量标记为已处理,也可以针对单个漏洞标记为已处理。标记为已处理后,漏洞 扫描的漏洞个数和未处理漏洞数、存在漏洞的服务数量均会减少,但是后续扫描仍然会扫描出这个漏洞。

2、加入白名单

您可以选择多个漏洞,批量加入白名单,也可以针对单个漏洞标记为加入白名单。加入白名单后,漏洞 扫描的漏洞个数和未处理漏洞数、存在漏洞的服务数量均会减少,后续扫描不会扫描出这个漏洞。

3、移除白名单



点击白名单管理,进入白名单管理界面,您可以选择多个漏洞扫描白名单,批量移除白名单,也可以针 对单个漏洞扫描白名单移除白名单。移除白名单后,后续扫描会扫描出这个漏洞。

修复漏洞事件

您可以根据参考链接或补丁获取链接进行漏洞修复。

5.5. 0penSSL 漏洞修复最佳实践

OpenSSL 简介

OpenSSL 是一个开放源代码的软件库包,应用程序可以使用这个包来进行安全通信,避免窃听,同时确认另一端连接者的身份。这个包广泛被应用在互联网的网页服务器上,因此需要注重 OpenSSL 安全漏洞的修复。

OpenSSL 用途

1、加密和解密数据: OPENSSL 支持对称和非对称加密算法, 可以用于安全的数据加密和解密操作。

2、数字签名: OPENSSL 可以对数据进行数字签名,提高数据的可信度和合法性。还可以验证数字签名和证书的有效性。

3、SSL/TLS 协议实现: OPENSSL 支持 SSL、TLS 等协议,可以用于建立安全的网络连接,对数据进行加密传输,提高网络的安全性。

4、生成和管理数字证书: OPENSSL 可以生成和管理各种类型的数字证书,包括服务器证书、客户端证书等。数字证书是实现安全通信的重要工具之一。

5、伪随机数生成器: OPENSSL 可以生成高质量的伪随机数, 用于各种密码算法中的随机数种子。

6、其他的密码学工作:除了上述主要用途外,OPENSSL还包括了各种密码学工具和库,可以实现密码 算法的实现和分析。

108



依赖 OpenSSL 的软件或协议

- 1、MongoDB 4.4
- 2、 Nginx
- 3、KeepAlived
- 4、Https
- 5、 OpenSSH
- 6、SSH
- 7、VPN
- 8、 电子邮件

OpenSSL 漏洞扫描

您可以参考漏洞扫描最佳实践进行漏洞扫描。

OpenSSL 常见漏洞

1、CVE-2016-0705 OpenSSL DSA 代码双重释放漏洞

a.漏洞危害

OpenSSL 1.0.2 及更早版本、1.0.1 及更早版本解析畸形 DSA 密钥中存在双重释放漏洞,可导致受影响

应用拒绝服务或内存破坏。

b.影响版本

OpenSSL 1.0.2 及更早版本

OpenSSL 1.0.1 及更早版本

c.修复建议

目前厂商已经发布了升级补丁以修复此安全问题,补丁获取链接:

http://openssl.org/news/secadv/20160301.txt

2、CVE-2016-0799 OpenSSL 'BIO_*printf' 函数安全漏洞



a.漏洞危害

OpenSSL 1.0.2 及更早版本、1.0.1 及更早版本在 BIO_*printf 函数的实现上存在内存破坏漏洞,可导致 内存泄露等。

b.影响版本

OpenSSL 1.0.2 及更早版本

OpenSSL 1.0.1 及更早版本

c.修复建议

目前厂商已经发布了升级补丁以修复此安全问题,补丁获取链接:

http://openssl.org/news/secadv/20160301.txt

3、CVE-2016-2842 OpenSSL doapr_outch 函数拒绝服务漏洞

a.漏洞危害

OpenSSL 1.0.1 < 1.0.1s、1.0.2 < 1.0.2g 版本, crypto/bio/b_print.c/doapr_outch 函数未验证某些

内存分配结果,这可使远程攻击者造成拒绝服务。

b.影响版本

OpenSSL 1.0.1 < 1.0.1s

OpenSSL 1.0.2 < 1.0.2g

c.修复建议

目前厂商已经发布了升级补丁以修复此安全问题,补丁获取链接:

http://openssl.org/news/secadv/20160301.txt

4、CVE-2016-2108 OpenSSL ASN.1 编码器内存破坏漏洞

a.漏洞危害

OpenSSL 中的 ASN.1 解析器在对数据解析时没有正确处理特定标签,当遇到 V_ASN1_NEG_INTEGER 和 V_ASN1_NEG_ENUMERATED 标签时,ASN.1 解析器也会将其视作 ASN1_ANY 类型,从而解析其 中的数据。当数据再次编码序列化时,可能造成数据越界写入,引起内存损坏。。

b.影响版本



OpenSSL Project OpenSSL 1.0.2 OpenSSL Project OpenSSL 1.0.1

c. 不受影响版本

OpenSSL Project OpenSSL 1.0.2c

OpenSSL Project OpenSSL 1.0.10

d.修复建议

目前厂商已经发布了升级补丁以修复此安全问题,补丁获取链接:

https://www.openssl.org/news/secadv/20160503.txt

OpenSSL 安全版本

OpenSSL Project OpenSSL 1.0.1 且>=1.0.1s

OpenSSL Project OpenSSL 1.0.2 且>=1.0.2g

5.6. 0penSSH 用户枚举漏洞修复最佳实践

漏洞编号

CVE-2018-15473

漏洞名称

OpenSSH 用户枚举漏洞(CVE-2018-15473)

漏洞描述

OpenSSH (OpenBSD Secure Shell) 是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具,该工具是 SSH 协议的开源实现,支持对所有的传输进行加密,可有效阻止窃听、连接劫持以及 其他网络级的攻击;



OpenSSH 7.7 及之前版本中存在用户枚举漏洞,该漏洞源于程序会对有效的和无效的用户身份验证请求 发出不同的响应,攻击者可通过发送特制的请求利用该漏洞枚举用户名称。

影响范围

OpenSSH 7.7 及之前版本

官方解决方案

1、应用如下补丁可以修复此漏洞,需要重新编译。

https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

2、新版本 OpenSSH-7.8 已经修复这个安全问题,请到厂商的主页下载,下载链接:

http://www.openssh.com/

http://www.openssh.com/portable.html

检测与修复建议

1888-28-20-2-1 漏洞扫描

服务器安全卫士(原生版)已支持对对该漏洞的检测与修复。需要在服务器安装部署 Agent,并已开启 安全防护。

您可以登录服务器安全卫士(原生版)控制台,在左侧导航中选择漏洞扫描,进入漏洞扫描页面。

漏洞扫描详情页面点击"一键扫描"按钮,进入一键扫描设置页面,勾选相应参数设置进行漏洞扫描。

(Instance)					
安全概范			8 (立即扫描	上一次扫描(13回时间: 2023-11-06 15:59:0
资产管理		L 1733 12092	一键扫描设置		×
基线管理					
入侵检测	~				
Marine and			漏洞类别 linux漏洞 windows漏洞	3	
附贝防量数(原生版)			漏洞扫描等级 🗹 超高能 🗹 超能 🗹 高	危 🧧 中急 🗌 低危	
病毒重乐					
设置中心	~	Linux (#20) Windows (#20)	超时设置 0 小时 30 ====================================	分钟②	
		如入向名单 后语为已终于			
			服劳器分类 2 至部服务器 9 目述服务器		
		漏洞名称	选择服务器区域 全部区域 > 全部		
	۲	Lua安全黨符	选择服务器		yanf Q C
		OpenSSH 输入验证继续展示	服务器名称	IP地址	服务器状态
			yanfa-kunpeng	192.168.0.22	 运行中
		Info-ZIP UnZip 建中区镭发展用	yanfa-win2016	192.168.0.16	0 运行中
			yanfa-win2012	192.168.0.15	 ○ 進行中 ○ 法行中
		- mo-th-output statisticated	yanfa-ubuntu16	192.168.0.6	 通行中
		Info-ZIP UnZip 基于维的资本区错误属制	yanfa-centos76	192.168.0.4	◎ 還行中
		Info-ZIP UnZp 拒绝服务案项			共6条 < 1 >
		GNU Wget 安全黨用			
		Into-ZIF UnZp 第中区情况展现			制定 取消
		□ Info-ZIP UnZp 使冲区情况展到	C12200-1000		



在漏洞扫描详情页面, Wir	ndows 系统漏洞列表中已检测出主机存在的 OpenSSH 漏	詷。
----------------	----------------------------------	----

器安全卫士 生版)		業系急等复約属列 1733	+处理的漏洞 12092	→ 存在應问的服务器 97	立即扫描 一键扫描	上一次扫描 (扫描时间: 2023- 羊情 余时扫描已开启 (每天1次, 00	11-06 15:59:07) 未述 00) 设置	2现漏洞 <u>重</u> 看
照 近						Postantine Contraction Contraction Contraction	ooy shakk	
理 (理	÷	Linux 漏洞 Windows 漏洞						
RI	~	加入白名单标记为已处理			全部進同等级 🗸 週间名称	~ 请输入关键词进行搜	家	Q C
H		漏洞名称	CVE编号	漏洞等级	影响服务器数量	最后发现时间	操作	
[政(原生版)	4	OpenSSH auth_parse_options函数信任管理问题意间	CVE-2012-0814	65	1	2023-09-27 20:10:54	处理 加入白名单	查看洋信
	~	OpenSSH XIIUseLocalhost XII转发会运动协编词	CVE-2008-3259	68	1	2023-09-27 20:10:54	处理 加入白名单	查着洋情
		OpenSSH 安全展网	CVE-2017-15906	中國	1	2023-09-27 20:10:54	处理 加入白名单	查看详情
		OpenSSH 信息泄露展词	CVE-2018-15473	中意	1	2023-09-27 20:10:54	处理 加入白名单	查看洋情
		OpenSSH排战调应(Challenge-Response)机制交互键值	P CVE-2002-0639	107ft	1	2023-09-27 20:10:54	处理 加入白名单	查看洋情

检测完成后,可点击"查看详情",跳转到详情页面,可以一键修复漏洞。 修复过程需要花费一段时间,修复完成后,请重启云主机使补丁生效。 重启云主机后,再次单击"手动检测",验证该漏洞是否修复成功。

5.7. 等级保护测评合规最佳实践

等级保护测评背景

网络安全等级保护测评是按照 GB/T 22239-2019 网络安全等级保护要求对各行业单位网络信息系统进行等级测评,以满足相关等级安全要求。云服务器需满足等级保护测评中安全计算环境要求,服务器安全卫士 (原生版)提供相关安全能力,满足客户合规需求。

安全计算环境要求

服务器安全卫士(原生版)在等级保护测评(三级)"安全计算环境"中可满足项:

1、身份鉴别

a. 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换。

满足情况:

满足。服务器安全卫士(原生版)通过基线检测功能帮助用户检测密码策略相关满足情况,协助用户完成策略配置;通过弱口令检测功能保障口令复杂度满足管理情况。



b.应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连 接超时自动退出等 相关措施。

满足情况:

满足。服务器安全卫士(原生版)通过基线检测功能帮助检测实现账户锁定策略相关满足情况,协助用 户完成策略配置。

2、入侵防范

a. 应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞。

满足情况:

满足。服务器安全卫士(原生版)通过扫描功能能够发现可能存在的已知漏洞,且能够出具修补建议帮助用户修补漏洞。

b.应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。

满足情况:

满足。服务器安全卫士(原生版)通过异常登录、暴力破解、后门检测、可疑操作、反弹 Shell 等功能对 主机进行实时监控,发现入侵行为进行告警。

3、 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒 行为,并将其有效阻断。

满足情况:

满足。服务器安全卫士(原生版)通过病毒查杀功能可对恶意代码进行查杀,满足该项要求。

说明:

其余测评项需用户通过云主机操作系统本身的策略设置满足,服务器安全卫士(原生版)可通过基线 检测功能协助客户进行策略检测。



6. 常见问题

6.1. 产品类

Q: 服务器安全卫士(原生版)与 Web 应用防火墙(原生版)有什么区别?

A: 天翼云的服务器安全卫士(原生版)与 Web 应用防火墙(原生版)产品,帮助您全面从主机、业务站 点等层面防御风险和威胁,提升系统安全指数,建议搭配使用。两个产品的差异见下表:

服务名称	防护对象	功能差异
服务器安全卫士 (原生版)	提升服务器整体安全性。	 资产管理 漏洞扫描 入侵检测 基线检测 弱口令检测 网页防篡改(原生版)
Web 应用防火墙 (原生版)	保护业务站点的可用性、安 全性。	 Web 基础防护 CC 攻击防护 精准访问防护

Q: 天翼云服务器安全卫士(原生版)都支持哪些资源池的服务器防护?

A:目前天翼云服务器安全卫士(原生版)为您提供服务器的资源池共 33 个,包括:湖南_长沙 3、福建_ 福州 3、陕西_西安 3、浙江-杭州 2、上海 7、云南_昆明 2、内蒙 6、北京 5、四川_成都 4、宁夏_中卫 2、 安徽_芜湖 2、山西_晋中 1、广东_佛山 3、广西_南宁 2、江苏_南京 3、江苏_南京 4、江西_九江、河北_ 雄安 2、海南_海口 2、湖北_武汉 4、湖北_荆州、湖南_郴州 2、甘肃_兰州 2、福建_福州 4、西藏_拉萨 3、 重庆 2、陕西_西安 4、青海_西宁 2、香港 1、福建_厦门 3、湖北_宜昌、福建_泉州、湖北_襄阳。

Q: 天翼云服务器安全卫士(原生版)支持跨区域使用吗?

A: 支持。天翼云服务器安全卫士(原生版)是平台级服务, 您通过控制台可以查看所有资产情况和风险 情况, 不需要切换资源池。

Q: 什么是 Agent?



A: Agent 是部署到用户服务器操作系统中的轻量化进程,主要功能是根据用户配置的安全策略,上报服 务器存在的安全风险和新增的安全事件数据,同时响应用户和安全卫士防护中心的指令,实现对服务器 上的安全威胁清除和恶意攻击拦截。

Q: 服务器安全卫士(原生版)漏洞库多久更新一次?

A: 每月一次。

6.2. 计费类

Q:服务器安全卫士(原生版)和网页防篡改(原生版)的计费方式是什么?A:服务器安全卫士(原生版)和网页防篡改(原生版)均为包周期计费,分为按月和按年2种方式。

Q: 服务器安全卫士(原生版)和网页防篡改(原生版)的计费项是什么?

A: 网页防篡改(原生版)是服务器安全卫士(原生版)的增值产品,计费项均为您订购的防护服务器台数,您选定防护台数和订购时长后,系统可自动计算出您的计费情况。

Q: 服务器安全卫士(原生版)和网页防篡改(原生版)的配额续费条件是什么?

A: 您所需续费的配额,需要为未到期或已到期状态。

6.3. 购买类

Q: 网页防篡改(原生版)可以单独购买吗?

A: 网页防篡改(原生版)和服务器安全卫士(原生版)配额均可单独购买。

Q: 服务器安全卫士(原生版)可以免费使用吗?

A: 您购买天翼云的服务器后,可以免费使用服务器安全卫士(原生版)的基础版服务。

Q: 服务器安全卫士(原生版)可以按天购买吗?

A: 不支持, 目前只支持包月和包年购买。



6.4. 操作类

Q: 服务器的防护状态显示"已离线"要如何解决?

A: 建议重新"安装 Agent"。

Q: 服务器显示登录异常怎么解决?

A: 查看服务器安全卫士(原生版)异常登录日志,根据日志中的登录源 IP、登录地区、登录账号、登录 时间进行检查,若非管理员登录,密码可能已经泄露,您需要对服务器进行详细的安全检查。

Q: 正常登录行为被误报为异常登录, 要如何消除误报?

A: 您可以登录服务器安全卫士(原生版)控制台,在左侧导航中选择入侵检测 -> 异常登录,在异常登录页面,找到被定义为异常登录的记录,在右侧操作栏中,单击"标记为已处理",即可消除本条告警记录。同时,您可以点击"白名单管理->新增白名单",将您常用的登录源 IP、登录地区、登录账号、登录时间加入白名单,则下次不会再进行异常登录告警。

Q: 如何减少服务器被爆破登录的风险?

A: 在给服务器设置密码的时候要避免弱口令,在公网上布置的机器要特别注意,如果暴力破解的事件很
 多,需要引起用户重视,关注攻击的源和 ip 地址。

Q: 如何使用网页防篡改(原生版)?

A: 您首先需要根据所需防护的服务器上的网站情况,订购网页防篡改(原生版)配额,每台服务器需订 购 1 个配额。订购成功后创建网页防篡改(原生版),根据您的网站情况进行防护策略的配置后,即可 开启网页防篡改(原生版)防护服务。

Q: 网页防篡改(原生版)添加防护服务器的步骤是什么?

A:具体步骤为添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护,详情见 添加防护服务器的操作步骤详情。



6.5. 系统类

Q: 支持的系统 0S 有哪些?

A: 天翼云服务器安全卫士(原生版)产品支持 64 位的 Linux 和 windows 系统服务器的防护,详情见下表:

0S	支持的 0S 版本
Windows(64 位)	Windows 2008 Windows 2012 Windows 2016
CentOS(64 位)	CentOS 6 系列 CentOS 7 系列 CentOS 8 系列
Ubuntu(64 位)	Ubuntu 16.04 Ubuntu 18.04
UOS 统信(X86_64)	UOS V20
AnolisOS 龙蜥(X86_64)	Anolis OS 7.9 Anolis OS 8.4
Debian (X86_64)	Debian 9.0.0
openEuler (X86_64)	openEuler 20.03
Kylin 麒麟(X86_64)	Kylin V10 SP1 Kylin V10 SP2

Q: 用户配置的网页防篡改防护策略有什么限制?

A: Linux 系统单个防护目录大小不超过 2G。



Q: 安装 agent 会不会对自身的业务稳定性产生影响?

A:不会。agent 是纯应用层的,不会给系统装任何的驱动; agent 的带宽和资源占用很小; agent 已经通 过各种业务场景长时间运行测试,不会影响系统的稳定性。