服务器安全卫士（原生版）

用户使用指南

天翼云科技有限公司

修订记录

文档版本	发布日期	修改说明
07	2025/02/28	本次主要更新一些截图，优化部分描述。
06	2025/02/19	本次主要修改如下章节： ● 用户指南 > 资产管理 > 防护配额管理 ● 用户指南 > 文件安全 > 病毒查杀
05	2025/02/05	主要修改点如下： ● 调整文档结构 ● 新增如下章节： ■ 安全配置 ■ 告警导出 ■ 端口蜜罐 ● 修改如下章节： ■ 资产管理 ■ 漏洞扫描 ■ 入侵检测
04	2024/05/30	本次新增如下章节： ● 后门检测 ● 可疑操作 ● 反弹 Shell ● 进程提权 ● 病毒查杀 ● 文件防勒索 ● 文件完整性保护 ● 告警通知 ● 报表管理 修改如下章节： ● 产品规格 ● 产品使用限制
03	2024/05/09	主要修改点：更新文档部分截图；更新常见问题。
02	2024/03/15	主要修改点：补充计费说明和最佳实践。

文档版本	发布日期	修改说明
01	2022/07/20	新建文档。

目　录

1. 产品介绍

1.1. 产品简介

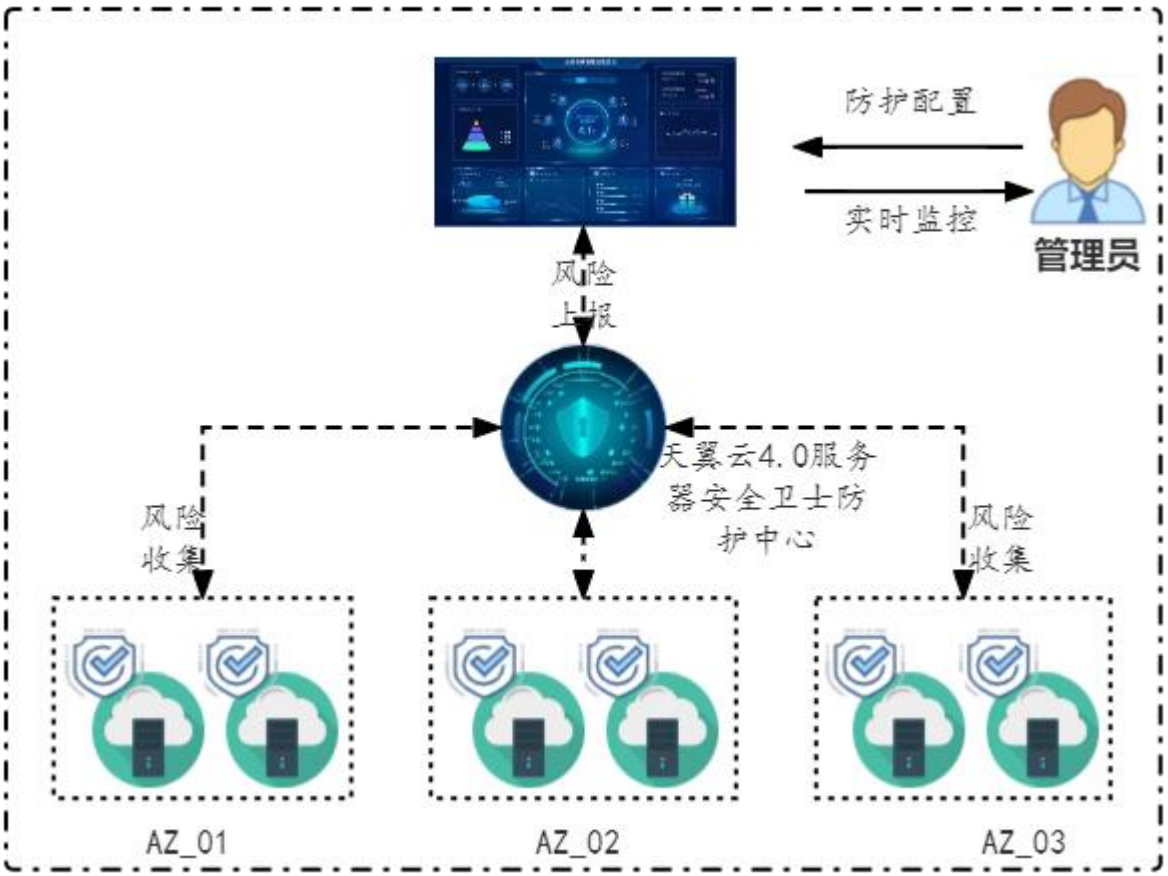
产品定义

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。

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。

- **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。
- **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

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

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。

病毒查杀

支持对挖矿木马、蠕虫、勒索病毒等进行有效的检测，提供灵活的检测方式，支持一键检测和定时检测方式，通过简单操作即可完成对病毒的处理，支持对病毒文件进行隔离、删除和信任。

网页防篡改

实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

勒索防护

在系统关键位置投放诱饵文件，实时捕捉勒索病毒攻击行为，可有效阻止勒索病毒对数据的加密。同时提供数据备份与恢复能力，及时恢复被勒索加密的数据。

文件完整性保护

对系统关键文件、文件路径、文件目录进行实时监控，发现文件变更篡改行为后进行告警，帮助用户及时发现可能遭受攻击的文件更改。

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。

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。

病毒查杀

基于特征病毒检测引擎，通过快速扫描、全盘扫描、自定义扫描三种检测模式对服务器文件进行全面扫描，并提供病毒文件处置能力。

1.5. 应用场景

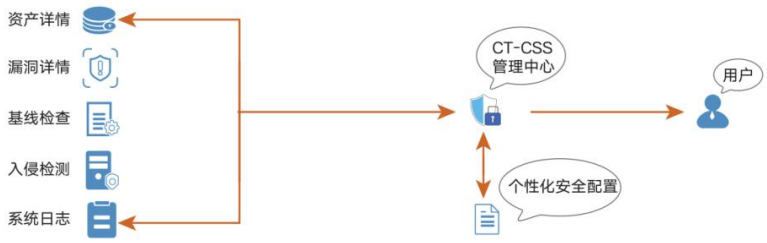
场景一：入侵行为检测

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。



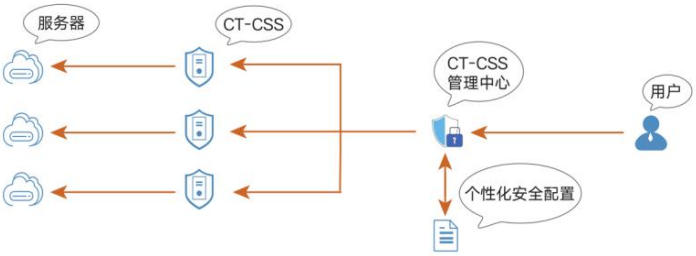
场景二：安全管理

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。



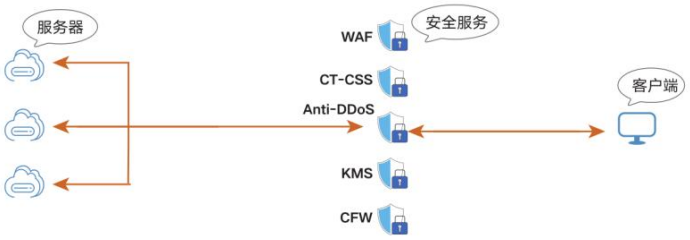
场景三：等保合规

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、旗舰版和增值服务。

不同规格功能差异为：

- 基础版包含安全概览、资产管理、入侵检测（异常登录、暴力破解）、漏洞扫描等功能。
- 企业版包含安全概览、资产管理、入侵检测（异常登录、暴力破解、后门检测、可疑操作、反弹Shell、进程提权、Webshell 检测）、漏洞扫描、基线管理、病毒查杀等功能。
- 旗舰版包含安全概览、资产管理、入侵检测（异常登录、暴力破解、后门检测、可疑操作、反弹Shell、进程提权、Webshell 检测、端口蜜罐）、漏洞扫描、基线管理、病毒查杀、文件完整性保护、文件防勒索等全部功能。
- 增值服务目前提供了网页防篡改（原生版）服务。

说明：

- 基础版只支持部分基础功能的检测能力和防护能力。
- 若需对服务器进行全面防护，您需购买企业版或旗舰版防护。
- 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	二级菜单	功能概述	基础版	企业版	旗舰版	增值服务
安全概览	-	查看待处理风险、防护状态、风险趋势、实时动态	✓	✓	✓	-
资产管理	资产概览	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、自启动项的统计情况	不支持资产指纹统计	✓	✓	-
	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	✓	✓	✓	-
	资产指纹	查看账号、端口、进程、软件应用、自启动项、Web 服务 6 种指纹的详细信息	仅支持采集端口和账户 2 种指纹信息，不支持手动资产指纹采集和资产历史变更	✓	✓	-
风险管理	基线检测	对服务器操作系统、数据库、关键应用软件配置等进行检测，帮助用户提前识别出可能导致安全漏洞的不安全配置项。	×	✓	✓	-

一级菜单	二级菜单	功能概述	基础版	企业版	旗舰版	增值服务
	漏洞扫描	支持扫描 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，并提供漏洞的修复建议和一键修复功能。	仅支持扫描 Win/Linux 漏洞，不支持配置扫描策略，不支持一键修复	✓	✓	-
	弱口令检测	通过与弱口令库对比，检测系统账号和应用账号口令是否属于常用的弱口令，提示用户修改不安全的口令。	×	✓	✓	-
入侵检测	告警中心	汇总所有入侵检测模块的告警信息，帮助用户快速了解整体安全告警概况	仅支持系统暴力破解、异常登录告警	✓	✓	-
	白名单管理	汇总所有白名单规则，可手动新增、删除白名单规则	不支持自定义白名单规则	✓	✓	-
网页防篡改	防护状态	查看防护的总体情况，帮助您实时掌握所有云上网站被篡改的总体态势。	×	×	×	✓

一级菜单	二级菜单	功能概述	基础版	企业版	旗舰版	增值服务
（原生版）	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。	×	×	×	✓
	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。	×	×	×	✓
文件安全	病毒查杀	病毒查杀功能，支持对挖矿木马、蠕虫、勒索病毒等进行有效的检测，通过简单操作即可完成对病毒的处理。	×	✓	✓	-
	文件完整性保护	可实时监控主机上的文件，对创建文件、修改文件、删除文件及文件提权操作进行监控和告警。	×	×	✓	-
设置中心	安全配置	安全配置用于统一管理和配置各防护模块的规则、白名单等。	仅支持异常登录非常用IP登录设置。	不支持端口蜜罐、勒索诱饵防护、文件完整性保护。	✓	-

一级菜单	二级菜单	功能概述	基础版	企业版	旗舰版	增值服务
	配额管理	展示购买配额的情况	✓	✓	✓	-
	告警通知	发生入侵时实时发送告警通知	✓	✓	✓	-
	报表管理	周期性自动生成安全报表	仅周报	✓	✓	-

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）产品支持对如下操作系统的服务器进行防护：

类型	架构	芯片	操作系统	系统版本
Windows	x86	Intel	Windows Server	Windows Server 2012 R2 标准版（简体中文）64 位
				Windows Server 2012 R2 数据中心版（简体中文）64 位

类型	架构	芯片	操作系统	系统版本
				Windows Server 2016 标准版（简体中文）64 位
				Windows Server 2016 数据中心版（简体中文）64 位
				Windows Server 2019 数据中心版（简体中文）64 位
				Windows Server 2022 数据中心版（简体中文）64 位
Linux	x86	Intel	Anolis	Anolis 7.9 64 位
				AnolisOS 8.9 64 位
				Anolis 8.6 QU1 64 位
				AnolisOS 8.6 64 位 ANCK
				AnolisOS 7.9 64 位 RHCK
				Anolis 8.4 64 位
			Debian	Debian 9.0 64 位
				Debian 11.1 64 位
				Debian 12.7 64 位
			CTyunOS	CTyunOS 2.0.1 64 位
				CTyunOS 23.01 64 位
			Ubuntu	Ubuntu 18.04 64 位
				Ubuntu 20.04 64 位
				Ubuntu 22.04 64 位
				Ubuntu16.04 64 位
			CentOS	CentOS 8.0 64 位
				CentOS 7.9 64 位
				CentOS 7.6 64 位
			openEuler	openEuler 20.03 SP4 64 位
				openEuler 22.03 SP2 64 位
			KylinOS	KylinOS V10 SP1 64 位
				KylinOS V10 SP2 64 位
				KylinOS V10 SP3 64 位

类型	架构	芯片	操作系统	系统版本
		海光	KylinOS	KylinOS V10 SP1 64 位
				KylinOS V10 SP2 64 位
				KylinOS V10 SP3 64 位
			UOS	UOS V20 64 位
			CTyunOS	CTyunOS 2.0.1 64 位
				CTyunOS 23.01 64 位
				CTyunOS 22.06 64 位
	Arm	鲲鹏	KylinOS	KylinOS V10 SP1 64 位
				KylinOS V10 SP2 64 位
				KylinOS V10 SP3 64 位
			CTyunOS	CTyunOS 2.0.1 64 位
				CTyunOS 22.06 64 位
				CTyunOS 23.01 64 位
			UOS	UOS V20 64 位
			OpenEuler	OpenEuler 22.03 64 位

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 2C4G。

1.8. 支持的资源池

一类节点

支持的一类节点区域如下：

资源池大区	资源池名称

资源池大区	资源池名称
华东地区	上海 7/上海 15/上海 36/杭州 2/合肥 2/芜湖 2/芜湖 4/南京 2/南京 3/南京 4/南京 5/华东 1/九江/南昌 5/杭州 7
华南地区	福州 3/福州 4/福州 25/佛山 3/佛山 7/广州 6/南宁 2/南宁 23/郴州 2/长沙 3/海口 2/武汉 3/武汉 4/武汉 41/长沙 42/华南 2
西北地区	西安 3/西安 4/西安 5/西宁 2/兰州 2/乌鲁木齐 27/乌鲁木齐 7/乌鲁木齐 4/中卫 5/中卫 2/西安 7/庆阳 2
西南地区	贵州 3/重庆 2/成都 4/昆明 2/拉萨 3/西南 1/西南 2-贵州
北方地区	青岛 20/北京 5/北京 9/晋中/石家庄 20/内蒙 6/华北 2/辽阳 1/郑州 5/太原 4/呼和浩特 3/沈阳 8
国际地区	香港 1

二类节点

支持的二类节点区域如下：

说明：

- 基础版不支持对二类节点资产进行防护。
- 二类节点资产防护请参见“二类节点资产纳管最佳实践”。

资源池大区	资源池名称

资源池大区	资源池名称
华东地区	上海 4/杭州（AZ1）/杭州（AZ2）/苏州（AZ1）/苏州（AZ2）/苏州（AZ3）/芜湖/南昌
华南地区	福州（AZ1）/福州（AZ2）/深圳/南宁/长沙 2（AZ1）/长沙 2（AZ2）/海口（AZ1）/武汉 2（AZ1）/广州 4
西北地区	西安 2（AZ1）/西安 2（AZ2）/西安 2（AZ3）/中卫/乌鲁木齐/西宁/兰州
西南地区	贵州/重庆/成都 3/昆明
北方地区	郑州/青岛（AZ1）/青岛（AZ2）/北京 2/太原/石家庄（AZ1）/石家庄（AZ2）/天津/长春/哈尔滨/沈阳 3/内蒙 3/华北（AZ3）

1.9. 与其他云服务关系

统一身份认证服务

统一身份认证（IAM）服务，是提供用户进行权限管理的基础服务，可以帮助您安全的控制云服务和资源的访问及操作权限。IAM 服务申请开通后免费使用，您只需要为您帐号中的云服务和资源进行付费。

云审计服务

云审计服务（CTS），为用户提供云服务资源操作记录的收集、存储和查询功能，用于支撑安全分析、合规审计、资源跟踪和问题定位，同时提供事件跟踪功能，将操作日志转储至对象存储实现永久保存。云审计服务申请开通后免费使用，事件文件转储功能会使用对象存储服务，会产生对象存储服务费用。

2. 计费说明

2.1. 计费模式

计费模式

服务器安全卫士（原生版）产品支持**包年包月**计费模式。包年包月是一种先付费后使用的计费模式。

计费项

服务器安全卫士（原生版）根据**产品版本、防护服务器数量和购买时长**进行计费。

计费项	说明
产品版本	支持基础版、企业版、旗舰版，不同版本差异请参见产品规格。
防护服务器数量	根据保有的服务器数量，选择实际购买的配额数量。
购买时长	购买时长越长，享受的优惠越大。

计费公式：标准资费 * 防护服务器数量 * 购买时长

标准资费

根据支持防护的功能不同，服务器安全卫士（原生版）提供基础版、企业版、旗舰版，具体价格如下表。

计费项	标准资费	计费单位
基础版	0（免费）	-
企业版	60	元/个/月
旗舰版	180	元/个/月

说明：

对注册天翼云的用户可免费开通基础版，您可随时升级至企业版、旗舰版，安全防护能力更强。

优惠活动

针对一次性包年付费，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。

计费示例

计费场景：用户需要购买企业版防护，防护的服务器数量为 1 台，预估资源使用时长 12 个月。

计费示例：60 元/个/月 * 12 个月 * 85 折优惠=612 元

2.2. 续订

为避免服务器安全卫士（原生版）配额到期后，防护服务自动停止，需要在配额到期前进行手动续费，或设置到期自动续费。

到期说明

到期后，资源进入保留期，您将不能正常访问及使用云服务（资源冻结），但对于您存储在云服务中的数据予以保留。

- 若您在保留期内续费，计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。
- 若保留期到期您仍未续费，存储在云服务中的数据将被删除、云服务资源将被释放。

关于保留期的详细信息，请参见到期处理。

续订说明

订单到期后，若没有续订，将不能继续使用订单中的服务，建议您提前进行续订。更多详情请阅读天翼云续订规则说明。

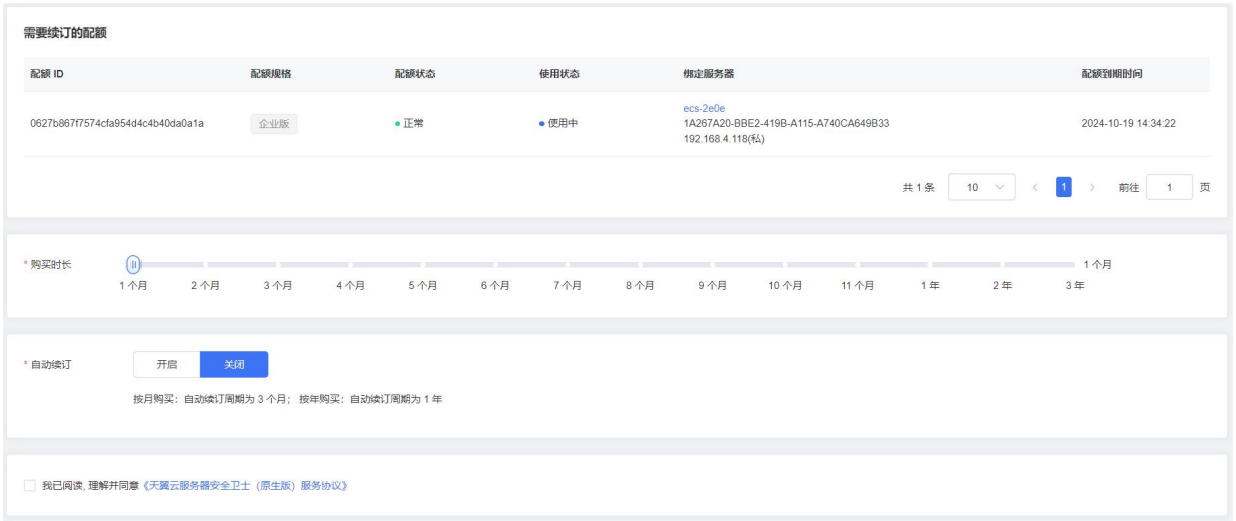
支持的续订方式：

续订方式	说明
手动续订	服务器安全卫士（原生版）在购买之后支持手动续订的方式，您可以随时在服务器安全卫士（原生版）管理控制台中的配额管理页面进行续订，续订后服务器安全卫士（原生版）到期时间将自动延期到续订后的到期时间。
自动续订	服务器安全卫士（原生版）在购买之后支持自动续订的方式，您可以随时在“费用中心 > 订单管理 > 续订管理”页面开启自动续订，自动续订开启后服务器安全卫士（原生版）将会进行自动续订。

手动续订

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。
3. 查看您已经订购的配额，选择所需续订的配额，点击“续订”；或勾选需要续订的配额，单击列表上方的“批量续订”。

4. 进入服务器安全卫士（原生版）续订页面，根据使用需要设置续订时长。



5. 续订时长设置完成后，在页面下方确认支付费用，阅读《天翼云服务器安全卫士（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）服务协议》“，在页面右下角单击“立即购买”。

自动续订

- 方法一：在购买服务器安全卫士（原生版）时，同步开启“自动续订”。
- 方法二：若购买服务器安全卫士（原生版）时未开启“自动续订”，用户也可在购买后，通过天翼云“费用中心 > 订单管理 > 续订管理”页面，开通自动续订。详细操作请参见开通自动续订。

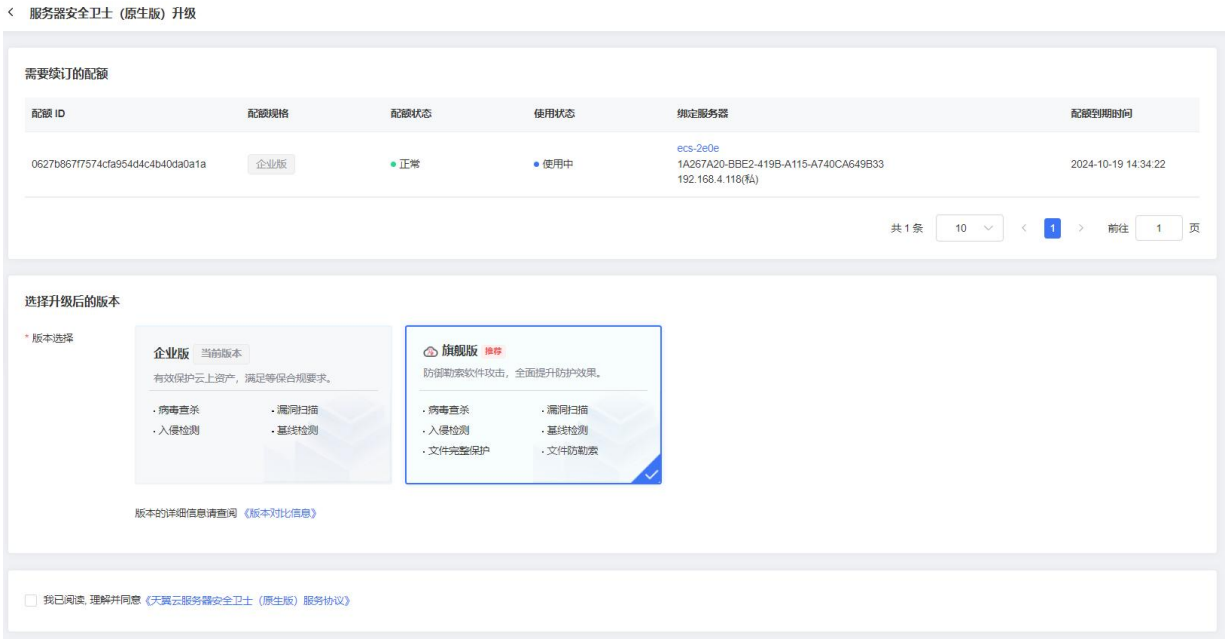
2.3. 升级

购买企业版配额后，可以将企业版配额升级为旗舰版。

操作步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。
3. 查看您已经订购的配额，选择需要升级的企业版配额，点击“升级”。

4. 进入服务器安全卫士（原生版）升级页面。



5. 在页面下方确认支付费用，阅读《天翼云服务器安全卫士（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云服务器安全卫士（原生版）服务协议》“，在页面右下角单击“立即购买”。

2.4. 退订

服务器安全卫士（原生版）支持退订，可通过服务器安全卫士（原生版）控制台、天翼云费用中心发起并完成退订操作。

退订说明

您（天翼云客户）可根据需要，在符合天翼云退订规则的前提下，灵活退订配额。目前退订包含七天无理由全额退订和非七天无理由退订以及其他退订，退订规则详情见退订规则说明。

退订步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。
3. 查看您已经订购的配额，选择需要退订的配额，点击“退订”。

4. 进入退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。

5. 系统提示退订申请提交成功，可前往订单详情查看退订进度。

3. 快速入门

3.1. 开启免费防护

服务器安全卫士（原生版）提供基础版、企业版、旗舰版和增值服务（网页防篡改）供用户选择。其中基础版为免费服务，提供漏洞扫描、异常登录、暴力破解等功能，更多详细信息请参见产品规格。

前提条件

已注册天翼云账号并完成实名认证。

方式一：在服务器安全卫士控制台开启防护

用户首次使用服务器安全卫士（原生版）时，需要先开通服务。开通服务后，服务器默认处于“免费版”防护状态。

1. 登录天翼云官网。
2. 选择“产品 > 安全及管理 > 工作负载安全 > 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，选择“管理控制台”。
3. 进入服务器安全卫士（原生版）管理控制台后，弹出下方“服务开通申请”对话框。

4. 阅读《天翼云服务器安全卫士（原生版）服务协议》后，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）服务协议》”，单击“同意”，即可开通服务器安全卫士（原生版）服务。

方式二：在购买云主机时开启防护

在购买弹性云主机时，当镜像类型选择“公有镜像”，支持开启主机安全防护，此处选择开启“**基础版**”防护。详细操作步骤请参见创建弹性云主机。

弹性云主机创建成功后，**将自动安装服务器安全卫士的 Agent 并开启防护，这个过程需要一定的时间，请耐心等待。**

查看防护状态

开启防护后，需要在服务器列表页面查看云主机资产的防护状态，确保所有待防护的云主机已开启防护。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 查看云主机防护状态：若 Agent 状态为“在线”，防护状态为“免费防护”，表示已正常开启防护。

说明：

若 Agent 状态为“离线”，请参考以下步骤安装 Agent：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 点击“安装 Agent”，弹出安装 Agent 窗口，按需选择安装命令。
   - 支持 Linux 和 Windows 系统。
   - 支持天翼云主机和天翼云外主机。
4. 根据界面提示，完成安装命令执行。

后续操作

常用功能配置：当云主机开启防护后，用户还可以根据业务需求进行防护配置。

3.2. 购买并开启高级防护

服务器安全卫士（原生版）提供基础版、企业版、旗舰版和增值服务（网页防篡改）供用户选择。不同版本差异请参见产品规格。

其中基础版为免费服务，若基础版不满足业务需求，可以购买企业版、旗舰版配额，然后将防护配额切换为企业版、旗舰版防护。

前提条件

已注册天翼云账号并完成实名认证。

方式一：在服务器安全卫士控制台开启防护

步骤一：购买防护配额

用户根据实际业务需求，购买企业版或旗舰版配额。

1. 登录服务器安全卫士（原生版）控制台。

2. 单击页面右上方的“购买服务器安全卫士（原生版）”按钮，进入服务器安全卫士（原生版）产品购买页面。

3. 选择版本、防护服务器数量。

4. （可选）选择是否开启网页防篡改增值服务。

5. 选择购买时长、是否开启自动续订。

6. 在页面左下角确认配置费用后，勾选“我已阅读，理解并同意《天翼云服务器安全卫士（原生版）服务协议》、《天翼云网页防篡改（原生版）服务协议》”，单击“立即购买”。
7. 购买成功后即可在“设置中心 > 配额管理”页面查看已购买的主机防护配额，在“网页防篡改（原生版） > 防护配额”页面查看已购买的网页防篡改防护配额。

步骤二：开通服务

用户首次进入服务器安全卫士（原生版）控制台时，需要先开通服务。开通服务后，服务器默认处于“免费版”防护状态。

1. 登录天翼云官网。
2. 选择“产品 > 安全及管理 > 工作负载安全 > 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，选择“管理控制台”。
3. 进入服务器安全卫士（原生版）管理控制台后，弹出下方“服务开通申请”对话框。

4. 阅读《天翼云服务器安全卫士（原生版）服务协议》后，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）服务协议》”，单击“同意”，即可开通服务器安全卫士（原生版）服务。

步骤三：切换防护配额

将基础版配额切换至企业版、旗舰版。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 您可对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。
   - 单台服务器切换版本

     在服务器列表中找到您需要切换版本的服务器，单击操作列的“切换版本”，弹出切换版本窗口。选择配额版本和配额后，单击“确定”，完成版本切换。
   - 批量切换版本

     在服务器列表中勾选需要切换版本的服务器，单击列表上方的“批量切换版本”，弹出切换版本窗口。选择配额版本，单击“确定”，配额和服务器按照顺序一一匹配。

     说明：

     批量切换版本时，服务器按照图中顺序与配额绑定，配额的绑定顺序按照到期时间从早到晚进行绑定。

方式二：在购买云主机时开启防护

在购买弹性云主机时，当镜像类型选择“公有镜像”，支持开启主机安全防护，此处选择开启“**企业版**”防护。详细操作步骤请参见创建弹性云主机。

弹性云主机创建成功后，**将自动安装服务器安全卫士的 Agent 并开启防护，这个过程需要一定的时间，请耐心等待。**

说明：

- 当前支持开启旗舰版、企业版、基础版防护。
- 具体支持的区域请以控制台显示为准。

查看防护状态

开启防护后，需要在服务器列表页面查看云主机资产的防护状态，确保所有待防护的云主机已开启防护。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 查看云主机防护状态：若 Agent 状态为“在线”，防护状态为“高级防护”，表示已正常开启防护。

说明：

若 Agent 状态为“离线”，请参考以下步骤安装 Agent：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 点击“安装 Agent”，弹出安装 Agent 窗口，按需选择安装命令。
   - 支持 Linux 和 Windows 系统。
   - 支持天翼云主机和天翼云外主机。
4. 根据界面提示，完成安装命令执行。

后续操作

常用功能配置：当云主机开启防护后，用户还可以根据业务需求进行防护配置。

3.3. 常用功能配置

3.3.1. 配置入侵检测

接入防护后，系统默认开启入侵检测防护，部分检测项需用户根据业务实际需求配置自定义检测规则。

配置异常登录白名单

通过配置异常登录白名单，将常用登录地、常用登录 IP 等添加至白名单中，非白名单中的登录操作，将被视为异常登录。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 异常登录”，进入异常登录页面。
3. 单击页面右上角的“白名单管理”，进入白名单管理页面。
4. 单击“新增白名单”，配置白名单参数。当所有字段都选择完成后，单击“确定”，会生成白名单规则，显示在白名单列表中。

参数	说明	是否必选
登录 IP	支持单个 IP、IP 范围和 IP 段。多个 IP 之间用英文逗号（,）隔开。 示例： ● 单个 IP：1.1.1.1 ● IP 范围：1.1.1.1-1.1.1.10 ● IP 段：172.168.34.1/20	登录 IP、登录用户名、登录时间、登录地区，这几个参数至少需要填写一项，可填写多项。
登录用户名	支持输入多个用户名，用英文逗号（,）隔开。	
登录地区	可选择多个登录地。	
登录时间	可选择开始时间和结束时间。	
设置生效范围	可选择全部服务器或自选部分服务器。	必选
备注	白名单的描述信息。	可选

配置可疑操作规则

系统提供默认检测规则，用户也可以自定义检测规则。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 可疑操作”，进入可疑操作页面。
3. 单击页面右上角的“自定义规则配置”，进入自定义规则配置页面。

   同时自定义规则配置列表可根据规则启用状态、威胁等级、规则名称等进行搜索。
4. 单击“新增规则”，配置规则参数。当所有字段都选择完成后，单击“确定”，完成配置。

参数	说明
规则名称	自定义规则的名称。
正则表达式	通过正则表达式匹配满足要求的操作。
威胁等级	配置规则的威胁等级，包括高危、中危、低危。
设置生效范围	可选择全部服务器和自选部分服务器。
备注	规则的描述信息。

关于更多入侵检测功能的介绍及风险处理，请参见入侵检测。

3.3.2. 开启定时漏洞扫描

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 单击定时扫描右侧的“设置”，页面右侧弹出定时扫描设置窗口，可进行定时扫描设置。
4. 设置选项包括漏洞类别、定期检测周期、设置生效范围，详细参数说明如下。

参数	说明
定时扫描	开启或关闭定时扫描。
漏洞类别	支持扫描“Linux 软件漏洞”、“Windows 系统漏洞”、“Web-CMS 漏洞”和“应用漏洞”。
定期检测周期	设置后会在周期选定的时间点开始定期检测。 ● 扫描周期：选择每天、3 天或 7 天。 ● 扫描时间：默认为 02:00，可以手动选择一天中的任一整点时间。
设置生效范围	选择扫描哪些服务器。可以选择“全部服务器”或“自选服务器”。 选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要扫描的服务器。

参数	说明
	说明： 以下服务器不能被选中执行漏洞扫描： ● 非“运行中”状态的服务器。 ● Agent 状态为“离线”的服务器。

5. 单击“确定”，设置完成。

3.3.3. 配置基线检测策略

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。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
3. 单击“策略管理”，进入策略管理页面。

   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。
4. 单击“新建策略”，页面右侧弹出新建基线策略窗口。
5. 设置策略名称、检查时间、选择基线名称和服务器。
6. 设置完成后，单击“确认”即可完成新建基线策略。

3.3.4. 开启弱口令定时检测

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 弱口令检测”，进入弱口令检测页面。
3. 单击定时扫描右侧的“设置”，页面右侧弹出定时检测设置窗口，可进行定时检测设置。
4. 设置选项包括检测周期、弱口令分类、设置生效范围，详细参数说明如下。

参数	说明
定时扫描	开启或关闭定时扫描。
检测周期	设置后会在周期选定的时间点开始定期检测。 ● 扫描周期：选择每天、3 天或 7 天。 ● 扫描时间：默认为 02:00，可以手动选择一天中的任一整点时间。
弱口令分类	支持“应用弱口令”和“系统弱口令”。
设置生效范围	选择检测哪些服务器。可以选择“全部服务器”或“自选服务器”。 选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要检测的服务器。 说明： 以下服务器不能被选中执行漏洞扫描： ● 使用“基础版”的服务器。 ● 非“运行中”状态的服务器。 ● Agent 状态为“离线”的服务器。

3.3.5. 开启定时扫描病毒

定时查杀是用来配置服务器定时启动病毒查杀的功能，按照用户设置的检测周期执行扫描任务。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 单击定时扫描右侧的“设置”，页面右侧弹出弹出病毒查杀设置窗口。
4. 打开定时扫描设置开关，根据界面提示，配置相关参数，详细参数说明如下。

参数	说明
检测模式	可选择快速检测、全盘检测、自定义检测。
检查周期	可选择每天、每 3 天或每 7 天检查周期。
设置生效范围	自定义选择需要执行病毒扫描任务的服务器。

5. 单击“确认”，设置完成。

3.3.6. 设置文件完整性保护检测规则

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件完整性保护”，进入文件完整性保护页面。
3. 单击列表右上方的“检测设置”，进入检测设置页面。
4. 配置相关参数。

参数	说明
启用文件变更检测	开启或关闭文件变更检测功能。
关键文件监控	● 系统内置：对系统关键文件、文件路径、文件目录进行实时监控，发现文件变更篡改行为并进行告警。 ● 自定义：根据用户特定的防护场景，自定义添加监控路径，发现文件变更篡改行为并进行告警。
监控排除设置	对用户添加的信任文件路径不再进行监控，方便用户更加灵活创建检测策略。
设置生效范围	自定义选择需要执行文件变更篡改行为监控的服务器。

5. 配置完成后，单击“确认提交”。

3.3.7. 配置网页防篡改

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版） > 防护管理”，进入防护管理页面。
3. 在列表中选择要开启网页防篡改防护的服务器，单击操作列的“防护设置”，进入防护设置页面。
4. 选择需要绑定的配额后，单击“配置防护策略”。
5. 为服务器配置防护策略，包括配置防护目录和设置特权进程。
   a. 配置防护目录：可对服务器的防护目录进行管理，包括添加、编辑、删除操作。

      分为添加白名单或添加黑名单两种模式，可根据实际使用场景进行配置。一台服务器不能同时使用白名单模式和黑名单模式，建议您使用白名单模式。

- 白名单模式：会对添加的防护目录和文件类型进行保护。配置完成后，即开始对配置的文件进行防护，防护目录下的防护文件被修改时，系统会进行拦截或告警。
- 黑名单模式：会防护目录下所有未排除的子目录、文件类型和指定文件。配置完成后，即开始对防护目录下所有未排除的子目录、文件类型和指定文件进行防护，防护目录下已排除的子目录、文件类型、指定文件被修改时，不会告警或拦截。

b. 设置特权进程：特权进程为您信任的进程文件，拥有对防护目录进行操作的权限，请确保特权进程安全可靠。

单击“添加”，弹出新增特权进程窗口，配置特权进程路径后，单击“确定”，完成特权进程配置。

c. 设置远端备份：启用远端服务器备份功能后，可有效避免备份在本地的文件被攻击者破坏后无法恢复。

单击“添加”，在弹出的窗口中选择远端备份服务器、配置备份目录，单击“确认”，完成远端备份配置。

6. 配置完成后，单击“完成防护配置”，回到防护管理页面。
7. 单击防护状态图标，为服务器开启网页防篡改防护。

3.3.8. 开启告警通知

开启告警通知后，当检测到资产存在风险时，会根据您配置的告警策略，向您发送告警通知，帮助您及时了解资产的安全情况。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 告警通知”，进入告警通知页面。
3. 根据您的使用场景进行告警通知配置。

配置项	说明
告警状态	告警通知的开关，可以开启/关闭需要通知的事件类型。
告警时间	支持“全天”，表示事件发生时实时发送告警通知。
通知方式	支持通过“邮件”方式发送告警通知。
告警项	根据威胁等级自定义发送通知。

4. 配置完成后单击“保存配置”，界面弹出“保存告警设置成功”提示信息，则说明告警通知配置成功。

3.3.9. 订阅报表

服务器安全卫士（原生版）支持生成日报、周报、月报，并支持订阅报表，订阅后系统会在报表生成后将报表发送至您的邮箱。

> 说明：
> 基础版只支持订阅周报，若需要订阅日报、月报，您需购买并使用企业版、旗舰版。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 报表管理”，进入报表管理页面。
3. 在“报表管理”页面右上角，单击“报表配置”，进入报表配置页面。

   报表配置参数说明如下：

参数名称	说明
报表生成	支持生成日报、周报、月报。根据需要进行选择，可多选。
报表订阅	该页面自动列出当前账号及其全部子账号。 勾选需要订阅报表的账号，报表生成后，系统会自动发送报表至订阅账号的邮箱。

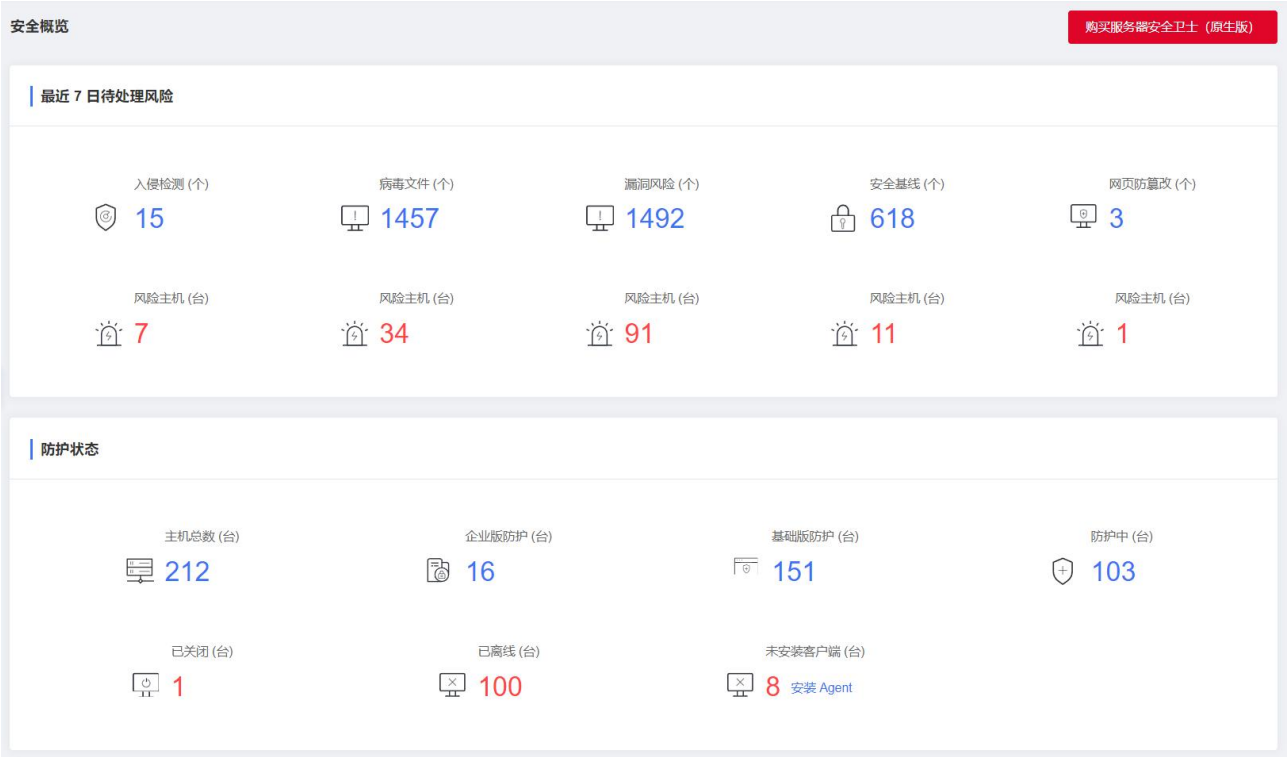
4. 单击“确认”，完成报表配置。

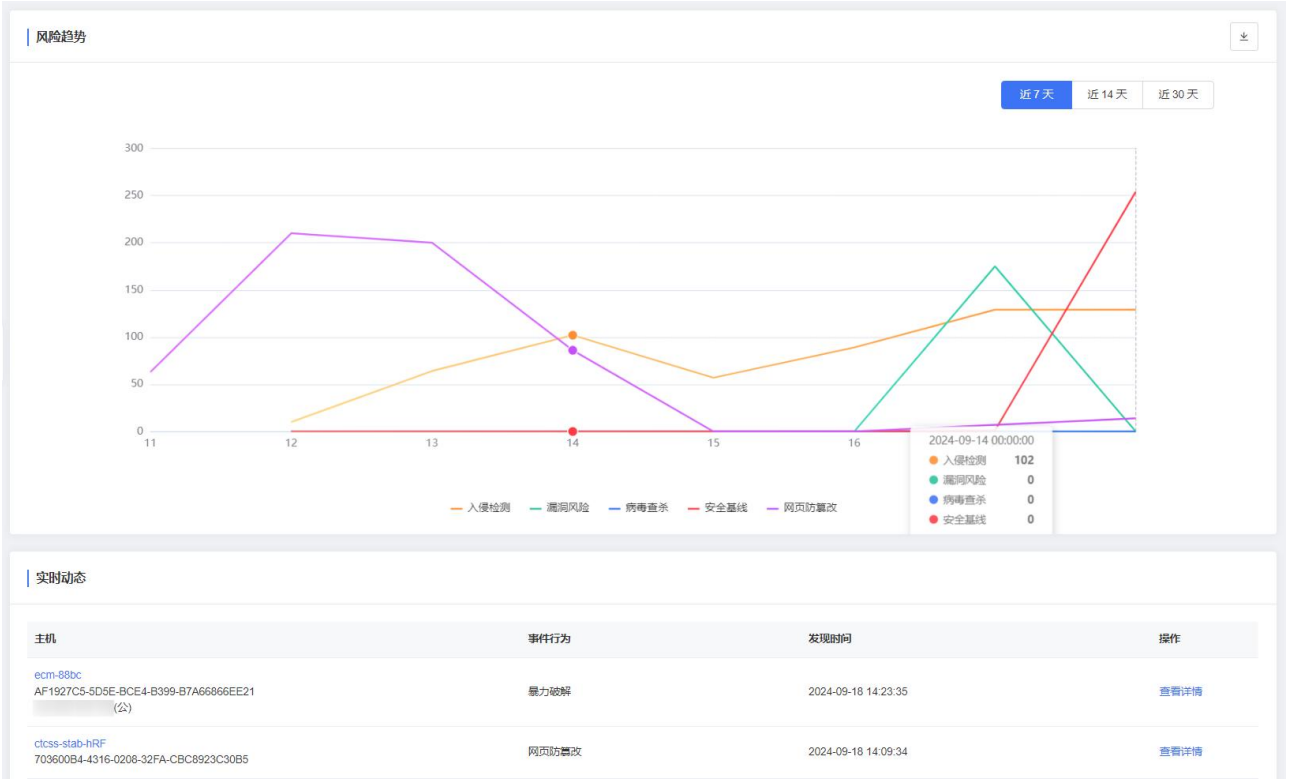
3.4. 快速掌握服务器安全态势

服务器安全卫士（原生版）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。

查看风险统计数据

在左侧导航栏选择“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，帮助您实时了解云主机的安全状态和存在的安全风险。





风险统计	说明
最近 7 日待处理风险	您可以查看入侵检测、病毒文件、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。
实时动态	您可以查看当前最新发现的风险事件详情。

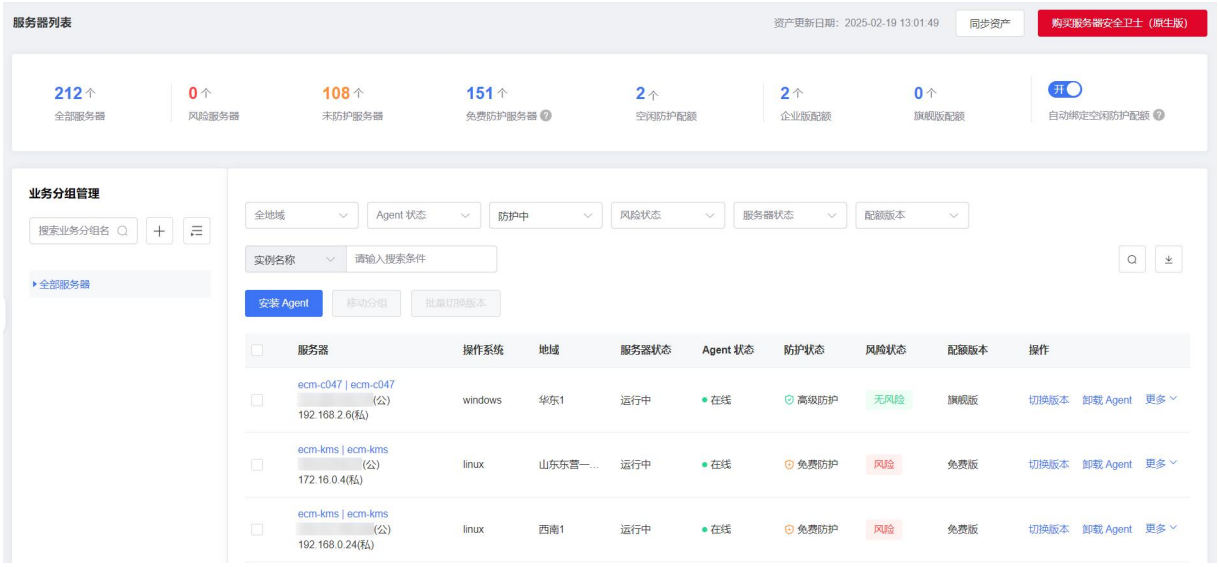
按服务器维度查看风险

支持查看单个云主机的安全风险详情，包括入侵检测、病毒查杀、漏洞风险、安全基线、网页防篡改等风险。

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。

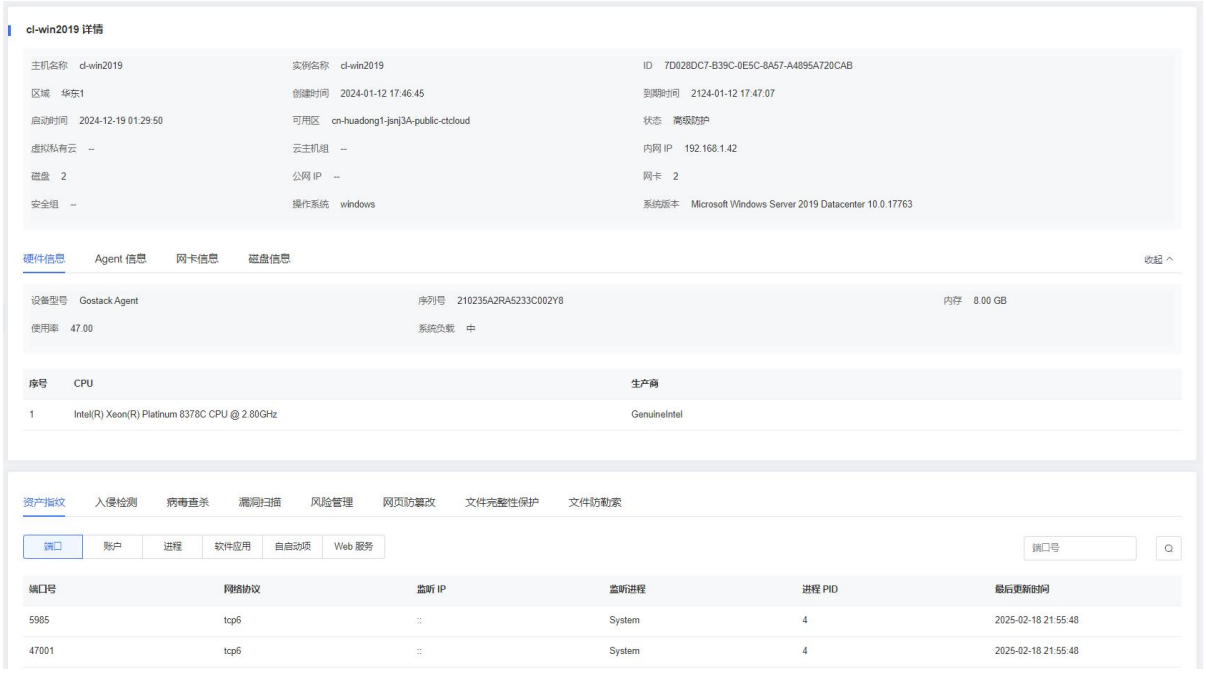
   可以看到全部主机的防护状态和风险情况。



3. 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、服务器 ID、服务器 IP、操作系统、地域、服务器状态、Agent 状态、防护状态、风险状态、配额版本。

4. 点击服务器名称时，跳转至该服务器的 “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；也可以快速查看各个风险事件，包括入侵检测、漏洞扫描、风险管理及网页防篡改的风险情况。



按风险维度查看风险

在左侧导航栏分别选择“风险管理”、“入侵检测”、“网页防篡改（原生版）”、“文件安全”，分别查看防护服务器的检测结果。

4. 用户指南

4.1. 安全概览

4.1.1. 最近 7 日待处理风险

如下图所示，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。

- **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 > 告警中心”页面；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。
- **病毒文件 | 风险主机**：展示 7 日内所有待处理的病毒文件个数，点击数字时会跳转到“文件安全 > 病毒查杀”页面；风险主机统计 7 日内有病毒文件的服务器，包括所有的云主机和物理机，同一台服务器有不同的病毒文件时不重复叠加。
- **漏洞风险 | 风险主机**：展示 7 日内所有待处理的漏洞风险个数，点击数字时会跳转到“风险管理 > 漏洞扫描”页面；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 日内所有未处理的安全基线风险个数，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“风险管理 > 基线检测”页面；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**：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“网页防篡改（原生版）> 防护状态”页面；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。

  说明：

  网页防篡改为增值服务，需要单独购买。若您未订购网页防篡改（原生版），则统计数字均显示为 0。

4.1.2. 防护状态

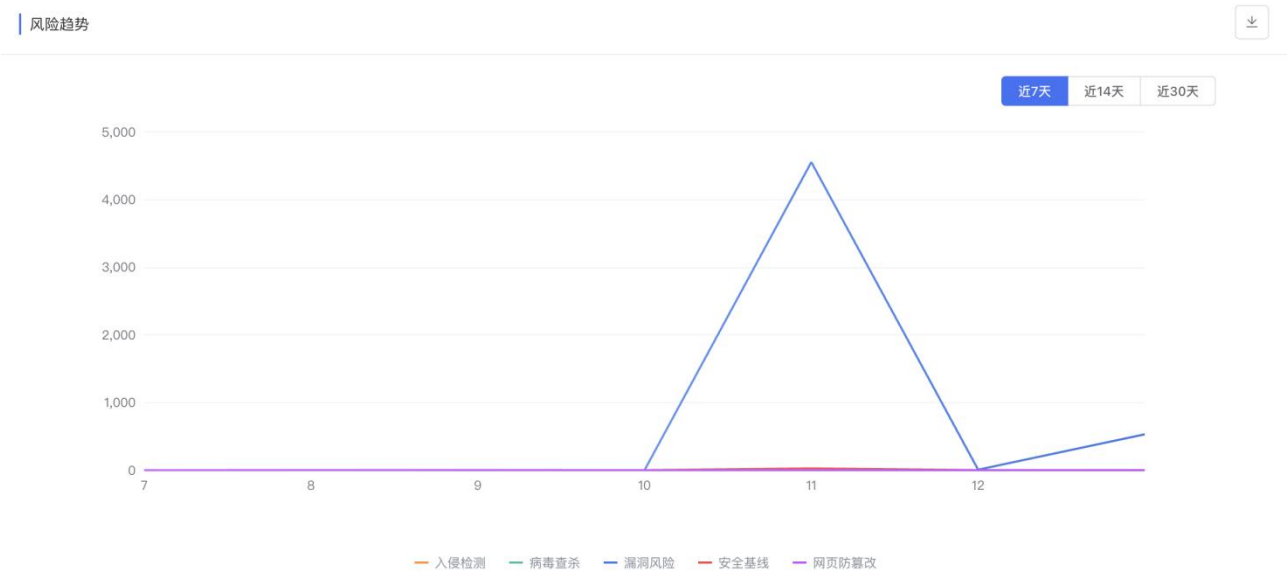
如下图所示，防护状态展示您所有服务器的防护情况。

- **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“资产管理 > 服务器列表”页面。
- **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“资产管理 > 服务器列表”页面，并筛选配额版本为“企业版”的主机。
- **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“资产管理 > 服务器列表”页面，并筛选配额版本为“免费版”的主机。
- **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“资产管理 > 服务器列表”页面，并筛选防护状态为“防护中”的主机。

- **已关闭**：服务器防护状态为“已关闭”的服务器数量统计，点击数字时会跳转至“资产管理 > 服务器列表”页面，并筛选防护状态为“未防护”的主机。
- **已离线**：服务器防护状态为“已离线”的服务器数量统计，点击数字时会跳转至“资产管理 > 服务器列表”页面，并筛选防护状态为“未防护”的主机。
- **未安装客户端**：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“资产管理 > 服务器列表”页面。单击“安装 Agent”，弹出安装 Agent 窗口，复制安装命令后，可以为主机安装 Agent。

4.1.3. 风险趋势

如下图所示，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。

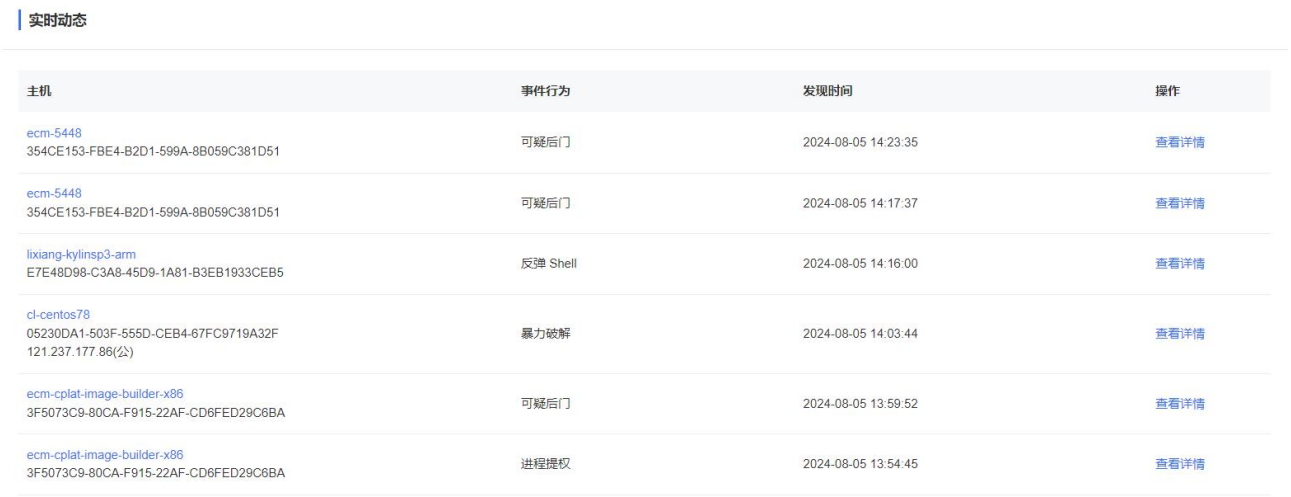
- **近 14 天**：以当前时间向前推 14 天，分别统计入侵检测、漏洞风险、安全基线、网页防篡改的风险个数，每天展示一个统计点。
- **近 30 天**：以当前时间向前推 30 天，分别统计入侵检测、漏洞风险、安全基线、网页防篡改的风险个数，每天展示一个统计点。

- 下载风险趋势数据

  单击“风险趋势”模块右上角的下载按钮，支持下载所选周期内的风险趋势数据（Excel 格式）到本地。

4.1.4. 实时动态

如下图所示，实时动态展示您所有服务器未处理的风险动态，包括服务器、事件行为、发现时间。



- 事件行为包括：基线风险、系统弱口令、异常登录、暴力破解、可疑操作、反弹 Shell、漏洞风险、病毒文件、网页防篡改等。
- 点击主机名称链接或操作列的“查看详情”，可以跳转至目标主机资产指纹详情页面，查看对应事件的详情并对事件进行处理。

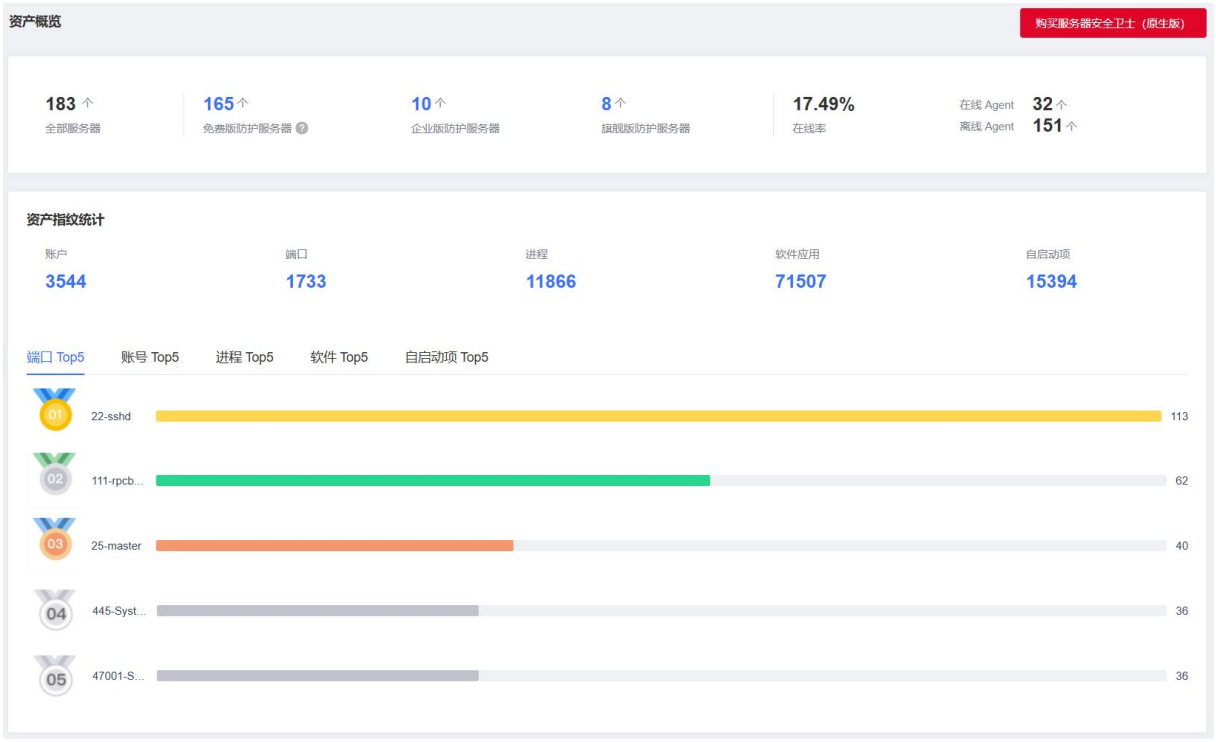
4.2. 资产管理

4.2.1. 资产概览

资产概览页面为您提供服务器资产概况、服务器防护情况、服务器资源池分布、服务器资产指纹等统计信息，可以帮助您了解资产的分布情况、防护状态及安全风险。

查看资产概览

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 概览”，进入资产概览页面。



3. 查看资产统计信息。
   - 防护情况统计

     为您展示全部服务器数量、免费版防护服务器数量、企业版防护服务器数量、旗舰版防护服务器数量；Agent 在线率、在线 Agent 数量、离线 Agent 数量。
   - 资产指纹统计

展示服务器开放端口、账号、服务器运行进程、服务器运行软件、自启动项的数量，以及 Top5 信息。

单击对应模块的数字，会跳转至对应的“资产指纹”页面。

> 说明：
>
> 基础版仅支持查看端口、账户资产指纹信息，如需查看其他指纹信息，需要购买或升级到企业版、旗舰版，具体操作请参见购买防护配额和切换版本。

- 资产分布

  展示各个区域主机资产的分布情况。

- 防护版本

  展示使用基础版（免费版）、企业版、旗舰版防护服务器数量。

- Agent 状态

  展示 Agent 在线和离线状态的服务器数量。

- 操作系统

  展示服务器操作系统分布情况，包括 Linux 和 Windows 系统。

4.2.2. 同步资产

系统默认每天 01:00 自动同步服务器资产信息，您可以根据需要修改自动同步周期，或手动执行同步资产操作。

手动同步资产

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 单击右上角“同步资产”，系统会立即获取最新的服务器资产信息，更新服务器列表。

自动同步资产周期设置

系统默认每天 01:00 自动同步服务器资产信息，您可以根据需要修改同步周期，同步周期支持 12 小时和 24 小时。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 同步资产设置”，进入同步资产设置页面。

3. 选择自动同步资产周期。
   - 12 小时：每天 01:00、13:00 自动同步服务器资产信息。
   - 24 小时：每天 01:00 自动同步服务器资产信息。

4.2.3. 业务分组管理

业务分组管理功能采用树状结构对企业组织架构进行管理，支持创建、编辑、删除、移动等操作。

说明：

- “全部服务器”为根目录，展示全网服务器数量，根目录不支持修改。
- 根目录下默认的“未分组”目录，展示没有被纳入分组的资产，“未分组”目录不可修改。
- 支持在根目录下创建二级分组。二级分组下最多支持创建 5 层级子分组（包含二级分组），同层级下创建分组数没有限制，每层级主机数没有限制。

创建分组

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。

3. 创建二级分组：单击业务分组检索框右侧的“+”按钮，弹出新建业务组窗口。

   配置业务组名称和备注，单击“确认”，完成创建。

4. 创建子分组：鼠标悬停在任意分组时，可以看到操作按钮，单击“+”按钮，弹出新建业务组窗口。

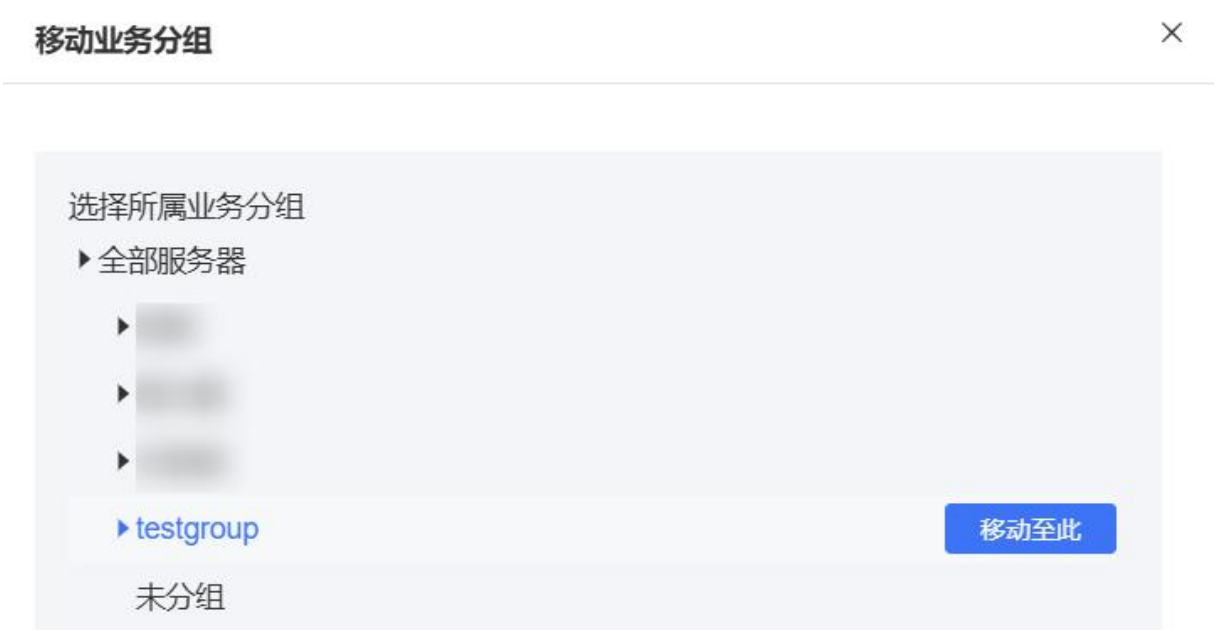
   配置业务组名称和备注，单击“确认”，完成创建。

移动分组

服务器资产默认在“未分组”目录下，用户可根据实际情况对服务器所在分组进行调整。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 找到需要移动分组的服务器，勾选服务器前的复选框，单击列表上方的“移动分组”。

4. 在弹出的移动业务分组窗口中，选择目标分组，单击“移动到此”。



分组管理

- 鼠标悬停在任意分组时，可以看到操作按钮，支持编辑分组、删除分组。

- 单击  图标，可以收起分组。

4.2.4. 查看服务器列表

您可以在服务器列表页面查看所有主机资产的防护状态和服务器详细信息。

> 注意：
>
> 仅支持对 Agent 状态为“在线”，防护状态为“防护中”的云主机进行检测。云主机离线后将不会进行检测。

查看服务器防护状态

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. （可选）选择业务分组，服务器列表将只展示该分组中的服务器。
4. 服务器列表包括以下字段：服务器、操作系统、地域、服务器状态、Agent 状态、防护状态、风险状态、配额版本。

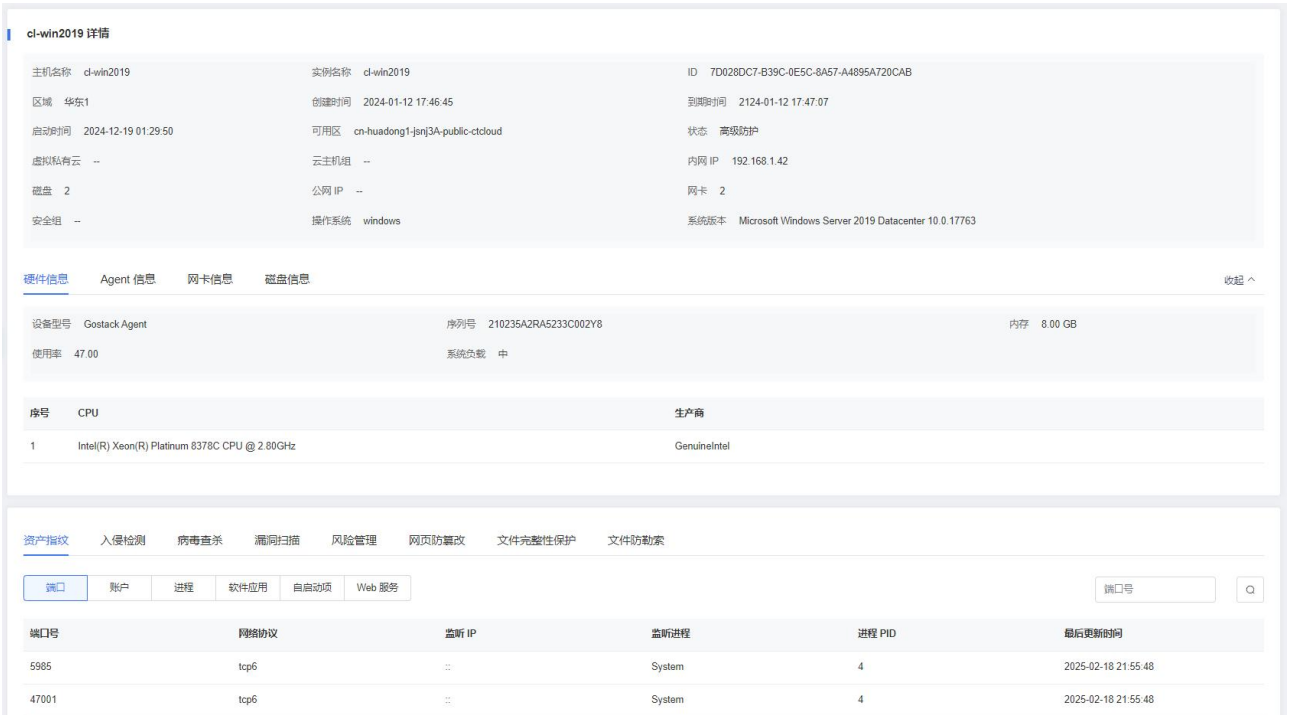
参数	说明
服务器	包括主机名称、实例名称、私网 IP、公网 IP。
操作系统	服务器的操作系统。
地域	服务器所属地域。
服务器状态	包括已关机、运行中。
Agent 状态	包括在线、离线。 ● 在线：Agent 控制通路和数据通路均连接正常。 ● 离线：Agent 控制通路或数据通路连接异常。
防护状态	包括防护中、未防护。 ● 防护中：表明该服务器处于正常防护中，此时 Agent 状态为在线且已经为该台服务器开启防护。防护中又分为“高级防护”和“免费防护”。 ● 未防护：表明该服务器未开启防护或 Agent 已离线。

参数	说明
风险状态	包括安全、风险、未知 3 种状态。 ● 无风险：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。 ● 未知：表明该服务器未开启防护或 Agent 已离线。
配额版本	服务器使用的防护配额版本，包括免费版、企业版、旗舰版。

查看服务器详情

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。



4.2.5. Agent 管理

服务器安全卫士 Agent 是安装在云主机上的一款应用软件，用于检测云主机中存在的安全风险。

- 安装 Agent 后，才能使用服务器安全卫士的防护能力，包括资产管理、风险管理、入侵检测、网页防篡改等。
- 如果不安装 Agent，将无法对云主机进行安全检测。

Agent 支持的操作系统

目前支持安装 Agent 的操作系统请参见支持的操作系统。

> 注意：
>
> 如果您的服务器操作系统不在支持范围内，安装 Agent 后可能存在兼容性问题，无法保证能正常使用服务器安全卫士（原生版）的防护能力。

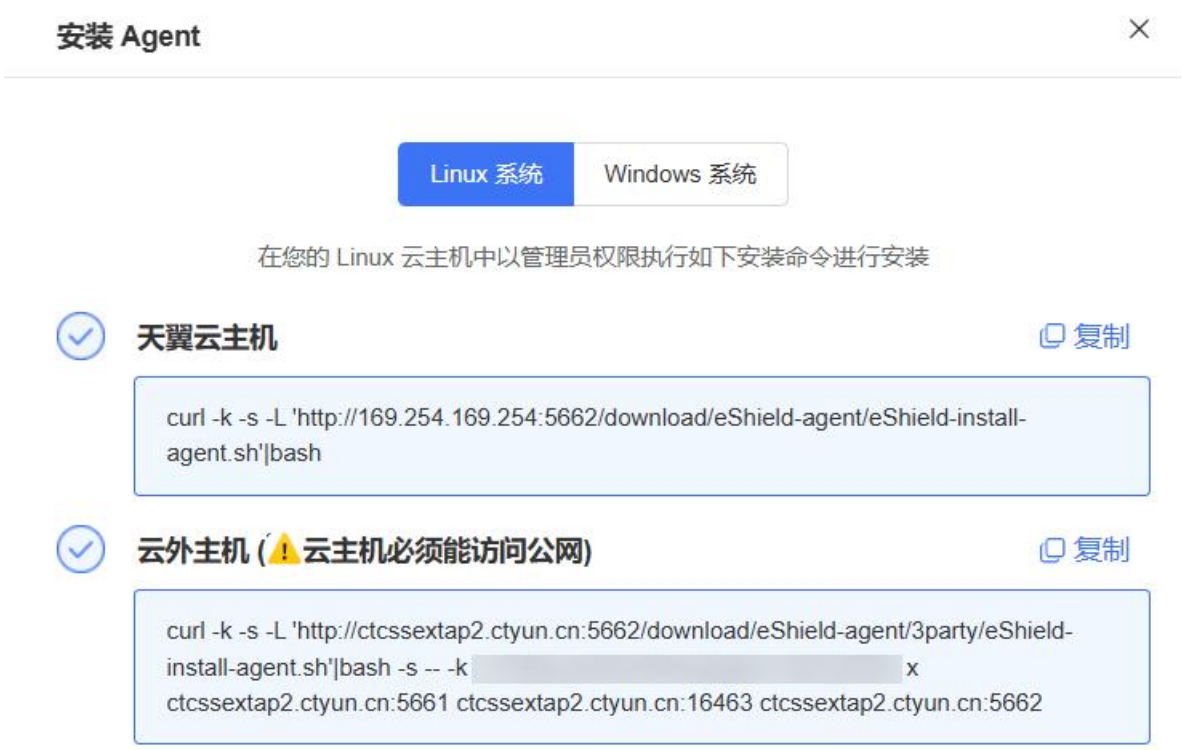
安装 Agent

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。

3. 点击“安装 Agent”，弹出安装 Agent 窗口，按需选择 Linux 和 Windows 系统的安装命令。

Linux 主机安装 Agent

1. 选择 Linux 系统，复制安装命令。

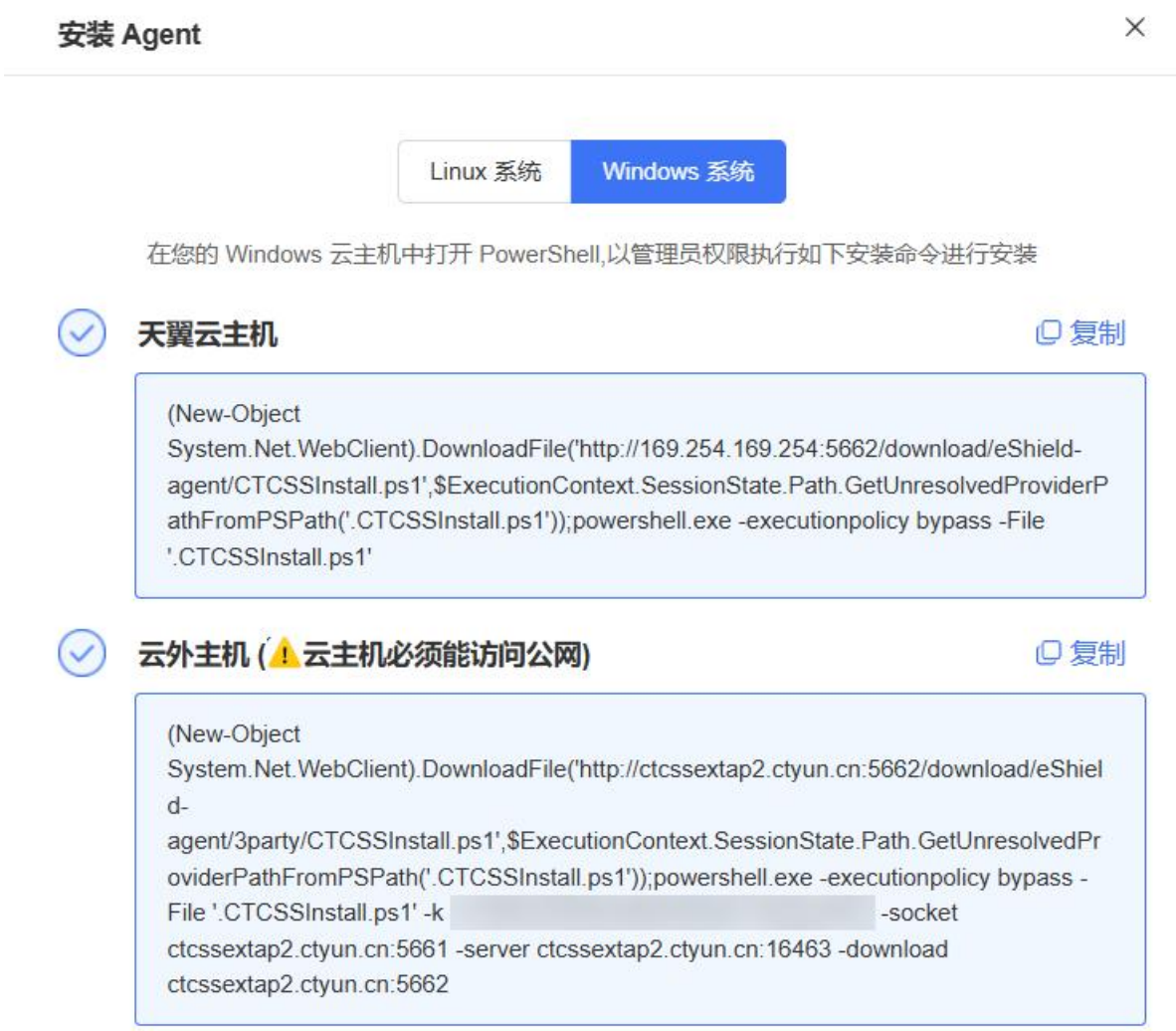


2. 在 Linux 云主机中以管理员权限执行安装命令进行安装。

> 说明：
>
> 手动安装 Agent 后，等待一段时间会自动连接，请耐心等待（无需重启服务器）。

Windows 主机安装 Agent

1. 选择 Windows 系统，复制安装命令。



2. 在 Windows 云主机中打开 PowerShell（按 win + R 组合键打开运行，输入 powershell 执行）。
3. 在打开的 PowerShell 控制台以管理员权限执行安装命令进行安装。

> 说明：
>
> 手动安装 Agent 后，等待一段时间会自动连接，请耐心等待（无需重启服务器）。

卸载 Agent

如果确认服务器无需使用服务器安全卫士（原生版）进行防护，您可以卸载服务器上的 Agent。

说明：

仅支持对“Agent 状态”为“在线”的服务器卸载 Agent。

1. 在服务器列表页面，找到需要卸载 Agent 的服务器，在操作列单击“卸载 Agent”。

2. 在弹出的提示框中，单击“确认”，进行 Agent 卸载。

升级 Agent

如果您服务器的 Agent 版本较低，系统会提示您升级 Agent。

1.在服务器列表页面，找到需要升级 Agent 的服务器，将光标放置在 Agent 版本列“升级”图标上，在悬浮框中单击“请升级 Agent”按钮。

2.根据主机的系统不同，弹出的升级对话框提示也不同。

Windows 主机

在 Windows 云主机中打开 PowerShell（按 win + R 组合键打开运行，输入 powershell 执行），在打开的 PowerShell 控制台以管理员权限执行安装命令进行安装。

Linux 主机

在 Linux 云主机中以管理员权限执行安装命令进行安装。

4.2.6. 防护配额管理

4.2.6.1. 绑定防护配额

服务器安全卫士（原生版）提供“免费版”、“企业版”、“旗舰版”供用户选择，不同版本差异请参见产品规格。

前提条件

已购买企业版或旗舰版配额，且有空闲的防护配额。

手动绑定配额

通过切换版本操作，支持将服务器的配额版本从基础版切换为企业版/旗舰版。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 在服务器列表中找到您需要绑定配额的服务器，单击操作列的“切换版本”。

如果需要批量绑定配额，可以在服务器列表中勾选需要绑定配额的服务器，单击列表上方的“批量切换版本”。

4. 在弹出的切换版本窗口。选择“企业版”或“旗舰版”，单击“确定”。

> 说明：
>
> 批量切换版本时，配额和服务器按照顺序一一匹配，配额的绑定顺序为按照到期时间从早到晚进行绑定。

自动绑定配额

开启“自动绑定空闲防护配额”开关，系统会自动为云主机绑定空闲可用的防护配额。

说明：

- 云主机绑定顺序：优先绑定最新购买的服务器。
- 配额绑定顺序：旗舰版 > 企业版。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 打开“自动绑定空闲防护配额”开关，开启自动绑定配额功能。

4. 系统立即同步资产，并为资产绑定空闲可用的防护配额。

4.2.6.2. 解绑防护配额

通过切换版本操作，支持将服务器的配额版本从企业版/旗舰版切换为基础版，切换完成后立即释放该服务器已使用的防护配额。您可以将释放后的防护配额分配给其他服务器使用。

注意：

为服务器解绑配额后，服务器使用基础版进行防护，基础版为免费版本，其防护功能受限，更多信息请参见产品规格。

前提条件

用户的服务器已绑定企业版/旗舰版防护配额。

操作步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 在服务器列表中找到您需要解绑配额的服务器，单击操作列的“切换版本”。

如果需要批量解绑配额，可以在服务器列表中勾选需要解绑配额的服务器，单击列表上方的“批量切换版本”。

4. 在弹出的切换版本窗口。选择“基础版”，单击“确定”。

4.2.7. 资产指纹管理

服务器器安全卫士支持采集服务器的端口、账户、进程、软件应用、自启动项、Web 服务资产指纹信息，通过资产指纹功能，可以帮助您清点服务器中的资产，及时发现潜在的风险。

版本限制

基础版仅支持查看端口和账户这两种指纹信息。若需要查看进程、软件应用、自启动项、Web 服务资产指纹信息，请升级到企业版、旗舰版，详细操作请参见绑定防护配额。

资产指纹内容

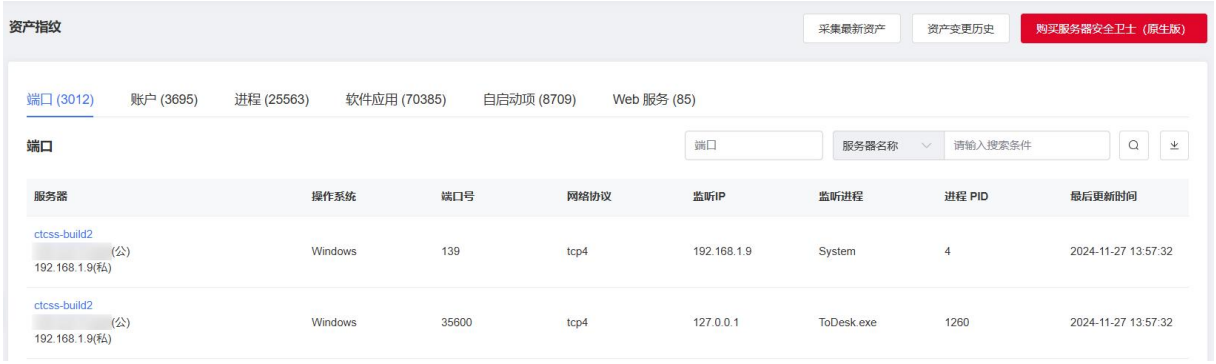
指纹	描述
端口	展示所有服务器中开放的端口列表，帮助用户及时发现主机中的危险端口。 端口信息包括：端口号、网络协议、监听 IP、监听进程。可以按照端口号、服务器名称、服务器 IP 进行搜索。
账户	展示所有服务器中的账号信息，帮助用户进行账户安全性管理。 账号信息包括：用户名、设置密码、用户组、到期时间、上次登录时间、上次登录 IP。可以按照用户名、服务器名称、服务器 IP 进行搜索。
进程	展示所有服务器中正在运行的进程信息，帮助用户及时发现服务器中异常的进程。 进程信息包括：进程名、进程路径、启动参数、启动时间、运行用户、进程号、父进程。可以按照进程名、服务器名称、服务器 IP 进行搜索。
软件应用	展示所有服务器中的软件应用信息，帮助用户清点软件资产，识别出服务器中不安全的软件。 软件应用信息包括：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。
自启动项	展示所有服务器中的自启动项，帮助用户及时发现服务器中异常的自启动项。 自启动项信息包括：自启动项名称、最后更新时间。可以按照自启动项名称、服务器名称、服务器 IP 进行搜索。
Web 服务	展示所有服务器中的 Web 服务，帮助用户及时发现服务器中异常的 Web 服务。 Web 服务信息包括：服务器、操作系统、Web 服务名、版本、PID、启动路径、监听端口、监听状态、监听端口配置路径、最后更新时间。

采集资产指纹

- 自动采集：系统每天会自动采集一次最新资产指纹数据。
- 手动采集：点击“采集最新资产”按钮后立即采集最新资产指纹数据。

查看所有主机资产指纹

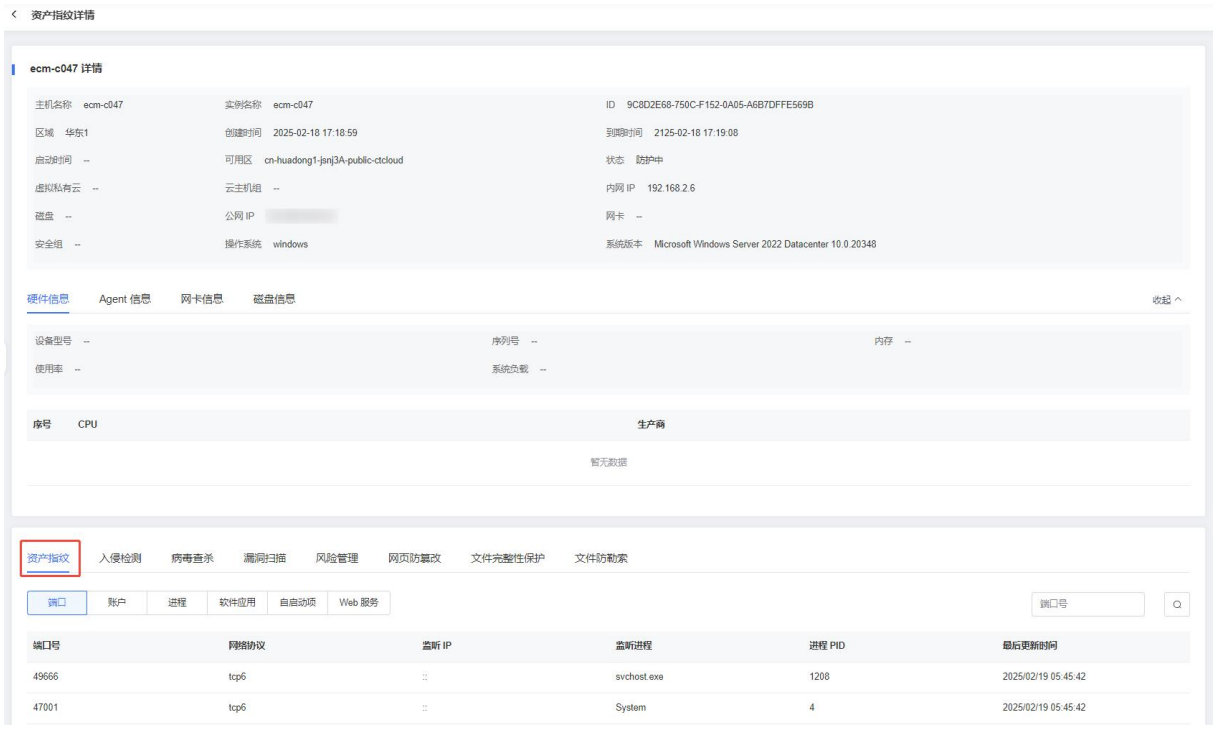
1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 资产指纹”，进入资产指纹页面。



3. 选择要查看的资产指纹页签，查看对应的资产指纹数据。
   - 筛选资产指纹：支持按资产指纹信息、服务器名称、服务器 IP 进行搜索，查找目标指纹信息。
   - 导出资产指纹列表：导出格式为 csv 文件。

查看单台主机资产指纹

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. 点击服务器名称，跳转至该服务器的 “资产指纹详情”页面。
4. 选择“资产指纹”页签，查看对应的资产指纹数据。



查看资产变更历史

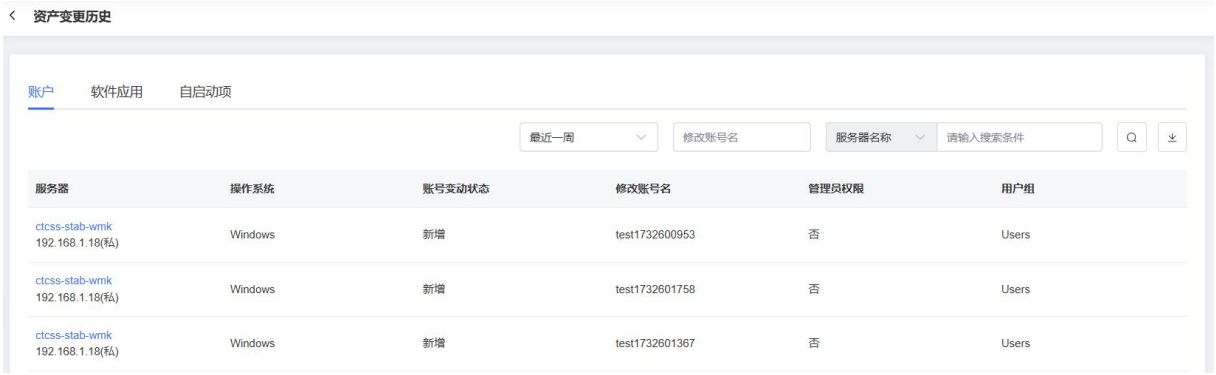
资产变更历史页面记录账户、软件应用、自启动项资产指纹的变更历史。

- 账户：记录新建、删除账号，修改账号名、管理员权限或用户组等信息的变动。
- 软件应用：记录新增软件、删除软件的变动。
- 自启动项：记录新增自启动项以及自启动项的运行周期、属性、hash、路径等改变的变动。

查看资产变更历史步骤如下：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 资产指纹”，进入资产指纹页面。

3. 单击右上角“资产变更历史”，进入变更记录详情页面，查看历史变更记录。



- 支持按时间筛选变更记录：筛选条件包括最近一周、最近一个月、最近三个月。
- 支持导出变更历史数据：导出格式为 csv 文件。

4.3. 风险管理

4.3.1. 基线检测

对服务器操作系统、数据库、关键应用软件配置等进行检测，帮助用户提前识别出可能导致安全漏洞的不安全配置项，例如不必要的服务开启、过时的软件版本、未启用的安全特性等。通过基线检测，可以及时发现并修复这些潜在的安全风险。

版本限制

仅企业版、旗舰版支持基线检测功能。

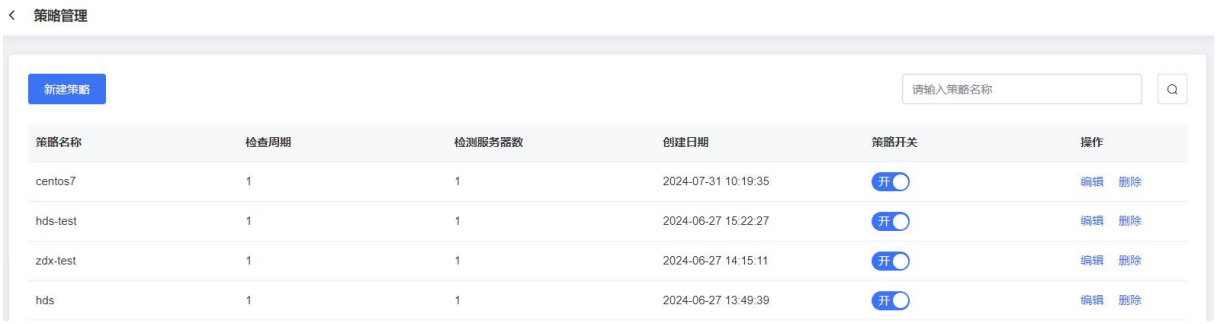
基线检测设置

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。

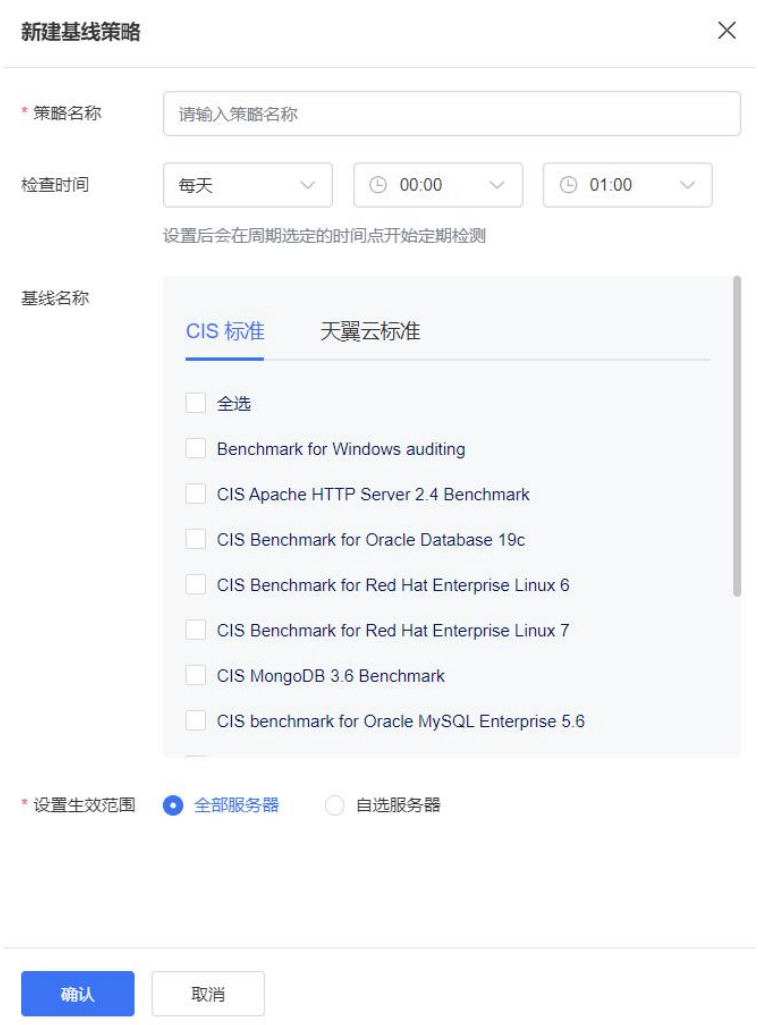
1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。

3. 单击“策略管理”，进入策略管理页面。

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。



4. 单击“新建策略”，页面右侧弹出新建基线策略窗口。



5. 设置策略名称、检查时间、选择基线名称和服务器。
6. 设置完成后，单击“确认”即可完成新建基线策略。

- 编辑基线检测策略

  若您需要对已有的基线策略进行编辑，点击该策略操作列中的“编辑”，可以修改策略的所有信息，包括策略名称、检查时间、已选择的基线名称和服务器，修改完成后点击“确认”即可完成基线策略编辑。

- 删除基线检测策略

  若您需要删除已有的基线策略，点击该策略操作列中的“删除”，在提示框中点击“确认”即可完成基线策略删除。

执行基线检测

- 定时执行基线检测

  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。

- 手动执行基线检测

  若您需要一键检测时，选择需要检测的基线策略，并点击“一键扫描”，系统即开始执行本次检测任务。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
3. 在右上角的下拉框中选择需要使用的基线检测策略，然后单击“一键扫描”。

4. 在弹出的提示框中单击“确定”，立即开始扫描。

查看基线检测结果

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”。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
   - 查看基线检测统计信息

     页面上方展示基线检测的统计情况和基线检测策略设置。

     - 统计情况包括检测服务器数、检测项、风险项、通过率。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%。
     - 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。切换基线策略后，显示切换后的基线检测统计结果。
   - 查看基线检测结果列表
     - 列表可通过基线名称查询。
     - 若本次检测成功，基线检测结果会在列表中展示，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。
       - 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。
     - 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。

   - 查看基线检测详情

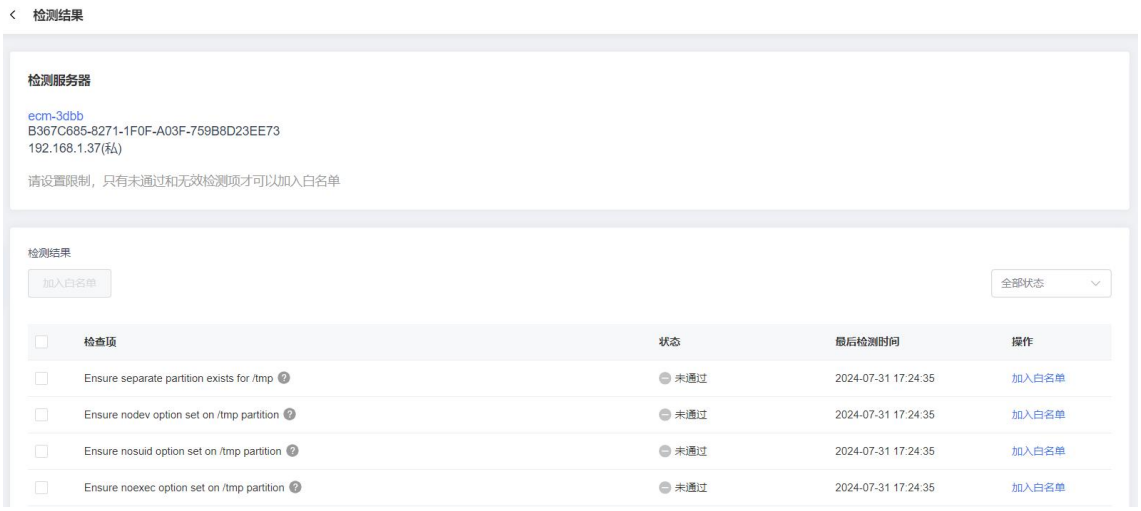
     点击基线列表操作列的“详情”，跳转到基线检测详情页面。

- 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。
- 整个列表可以根据状态、服务器名称、服务器 IP 进行查询。

- 查看某台服务器的基线检测结果

  点击基线检测详情页操作列中的“详情”，可以查看该基线名称下该台服务器的检测详情。

  - 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。



处理基线风险

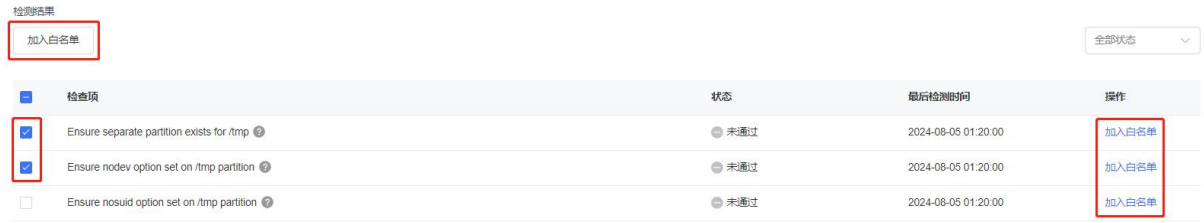
加入白名单

针对检查状态为“未通过”和“无效”的基线检查项，若经确认无需处理，可将其加入基线检测策略白名单。加入白名单后，后续基线检查时，会自动忽略已加入白名单的检查项。

说明：

加入白名单操作，针对的是所有服务器。即将检查项 A 加入白名单后，所有服务器上针对检查项 A 的状态均为“已加白”。

1. 进入服务器的基线检测结果页面。
2. 勾选需要加白的检查项，单击列表上方的“加入白名单”，或单击检查项操作列的“加入白名单”。



3. 在弹出的确认框中，确认检查项信息后，单击“确认”，完成操作。

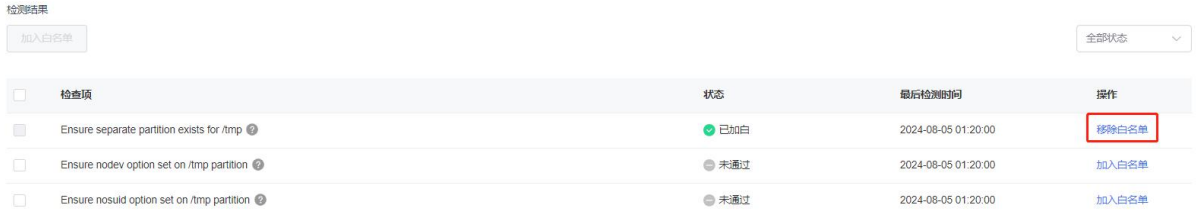
移除白名单

若您需要对已加入白名单的检查项重新进行检查，可将已加入白名单的检查项移除白名单。移除白名单后，该检查项会再次出现在风险列表中。

方法一：

1. 进入服务器的基线检测结果页面。

2. 找到需要移除白名单的的检查项，单击操作列的“移除白名单”。



3. 在弹出的确认框中，确认检查项信息后，单击“确认”，检查项将移除白名单。

方法二：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
3. 单击右上角的“白名单管理”。

4. 进入白名单管理页面。

   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。

   可以基于检查项名称和基线名称进行搜索。

5. 勾选需要移除白名单的检查项，单击列表上方的“移除白名单”，或单击检查项操作列的“移除白名单”。

6. 在弹出的确认框中，确认检查项信息后，单击“确认”，检查项将移除白名单。

4.3.2. 漏洞扫描

4.3.2.1. 概述

服务器安全卫士（原生版）支持扫描 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，并提供漏洞的修复建议和一键修复功能，帮助您及时了解云主机操作系统中存在的风险，及时修复主机漏洞。

漏洞扫描原理

漏洞扫描原理如下：

漏洞分类	原理说明
Linux 软件漏洞	通过与漏洞库进行比对，检测 Linux 操作系统官方维护的软件（非绿色版、非自行编译安装版；例如：kernel、openssl、vim、glibc 等）是否存在漏洞，将存在风险的结果向用户告警。
Windows 系统漏洞	通过同步微软官方的补丁公告，判断服务器上的补丁是否已经更新，并推送微软官方补丁，将存在风险的结果向用户告警。
Web-CMS 漏洞	通过对 Web 目录和文件进行检测，识别出 Web-CMS 漏洞，将存在风险的结果向用户告警。
应用漏洞	通过检测主机上运行的软件发现应用是否存在漏洞，将存在风险的结果向用户告警。

版本规格

以下介绍服务器安全卫士各版本漏洞扫描功能的支持情况。

> 说明：
>
> 免费版仅支持扫描和查看漏洞，不支持一键修复漏洞，您可以参考漏洞详情页面提供的修复建议，登录到您的服务器手动修复漏洞。

功能	免费版	企业版	旗舰版
漏洞情况统计	✓	✓	✓

功能	免费版	企业版	旗舰版
Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞	✓	✓	✓
一键扫描	✓	✓	✓
定时扫描	✓	✓	✓
基于漏洞名称的扫描结果列表	✓	✓	✓
基于服务器的扫描结果列表	✓	✓	✓
查看漏洞详情	✓	✓	✓
一键修复漏洞	×	✓	✓
白名单管理	✓	✓	✓

支持的操作系统

漏洞扫描支持的操作系统请参见产品使用限制 > 支持的操作系统。

漏洞等级

修复优先级	修复建议
高	需紧急修复。
中	可延后修复。
低	可暂不修复。

4.3.2.2. 扫描漏洞

服务器安全卫士（原生版）支持扫描 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，提供如下扫描方式：

- 一键手动扫描漏洞

  如果用户想立即了解服务器当前是否存在漏洞风险，可以执行“一键扫描”，立即手动扫描服务器中的漏洞。

- 定时自动扫描漏洞

  用户可以开启“定时扫描”，配置定时扫描周期和范围，定期对服务器上存在的漏洞进行自动扫描。

约束限制

- 漏洞扫描支持的操作系统请参见支持的操作系统。
- 仅支持对已安装 Agent 且“Agent 状态”为“在线”、“防护状态”为“防护中”的服务器进行漏洞扫描。

一键手动扫描漏洞

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。

3. 单击“一键扫描”，页面右侧弹出一键扫描设置窗口。

4. 设置扫描参数，参数说明如下。

参数	说明
漏洞类别	支持扫描“Linux 软件漏洞”、“Windows 系统漏洞”、“Web-CMS 漏洞”和“应用漏洞”。

参数	说明
设置生效范围	选择扫描哪些服务器。可以选择“全部服务器”或“自选服务器”。 选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要扫描的服务器。 说明： ● 以下服务器不能被选中执行漏洞扫描： ● 非“运行中”状态的服务器。Agent 状态为“离线”的服务器。

5. 单击“确定”，立即开始扫描。

> 说明：
>
> 扫描需要一定的时间，请耐心等待，期间您可以切换页面执行其他操作。等待过程中您可以手动刷新页面查看最新扫描数据。

定时自动扫描漏洞

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。

3. 单击定时扫描右侧的“设置”，页面右侧弹出定时扫描设置窗口，可进行定时扫描设置。

4. 设置选项包括漏洞类别、定期检测周期、设置生效范围，详细参数说明如下。

参数	说明
定时扫描	开启或关闭定时扫描。
漏洞类别	支持扫描“Linux 软件漏洞”、“Windows 系统漏洞”、“Web-CMS 漏洞”和“应用漏洞”。
定期检测周期	设置后会在周期选定的时间点开始定期检测。 ● 扫描周期：选择每天、3 天或 7 天。 ● 扫描时间：默认为 02:00，可以手动选择一天中的任一整点时间。
设置生效范围	选择扫描哪些服务器。可以选择“全部服务器”或“自选服务器”。 选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要扫描的服务器。 说明： 以下服务器不能被选中执行漏洞扫描： ● 非“运行中”状态的服务器。 ● Agent 状态为“离线”的服务器。

5. 单击“确定”，设置完成。

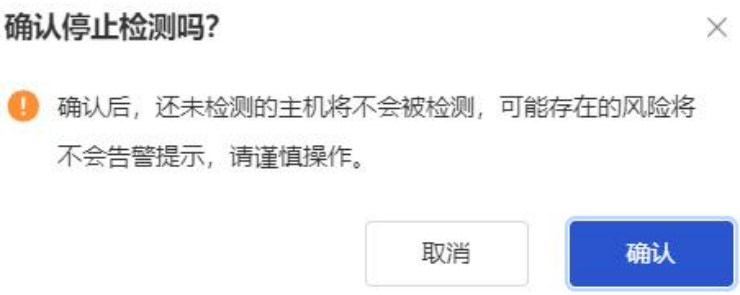
停止扫描

当开始一键扫描或定时扫描任务启动后，页面显示“正在扫描...”。

在扫描过程中，可随时“停止扫描”。

> 注意：
>
> 停止扫描后，还未检测的主机将不会被检测，可能存在的风险将不会有告警提示，请谨慎操作。

1. 单击“停止扫描”，弹出如下提示框。



2. 确认风险提示信息后，点击“确认”将立即停止扫描。

后续操作

- 查看漏洞扫描结果：漏洞扫描结束后，您可在漏洞页面下查看最新的扫描结果。
- 处理漏洞：您可以根据实际情况，对漏洞进行修复、忽略或将漏洞加入白名单。

4.3.2.3. 查看漏洞扫描结果

漏洞扫描完成后，可以在漏洞扫描页面查看服务器中存在的漏洞信息。

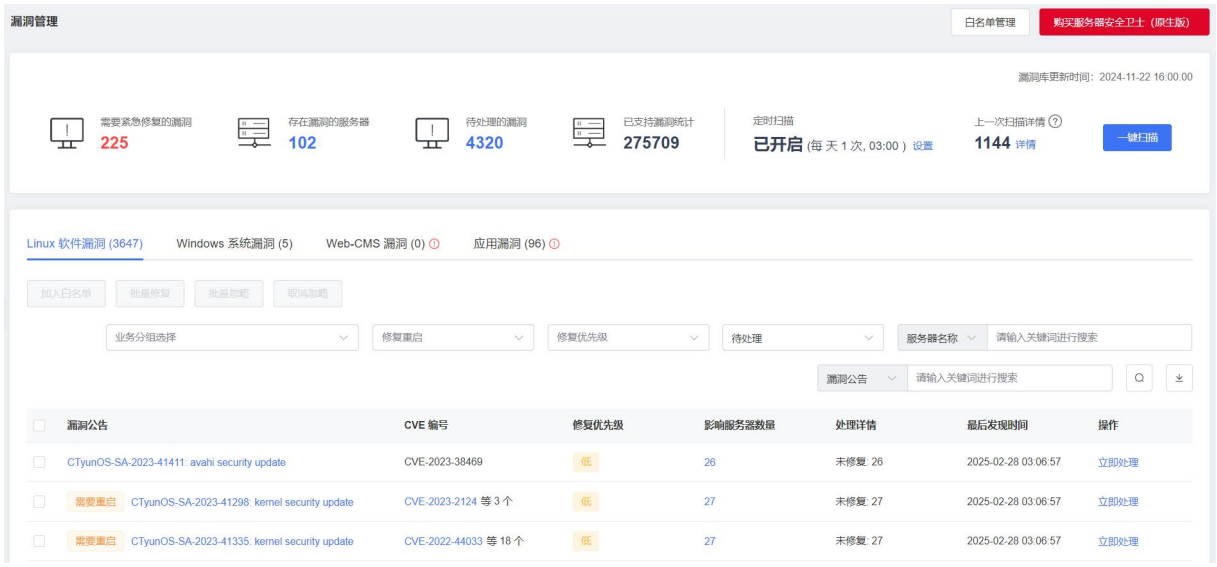
前提条件

已完成漏洞扫描。详细操作请参见扫描漏洞。

查看漏洞列表

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。



3. 在漏洞扫描页面查看漏洞相关信息。

- 查看漏洞扫描结果统计信息

  页面上方展示漏洞扫描的统计情况和漏洞扫描设置，统计情况包括需紧急修复的漏洞、存在漏洞的服务器、待处理的漏洞、已支持漏洞统计。

参数	说明	操作
需要紧急修复的漏洞	展示需要紧急修复的漏洞数量。	单击“需要紧急修复的漏洞”下方的数字，页面下方漏洞列表将筛选出修复优先级为“高”，待处理的漏洞。
存在漏洞的服务器	展示存在漏洞的服务器数量。	单击“存在漏洞的服务器”下方的数字，可以快速查看存在漏洞的服务器列表。
待处理的漏洞	展示所有未处理的漏洞数量。	单击“待处理的漏洞”下方的数字，页面下方漏洞列表将筛选出所有待处理的漏洞。
已支持漏洞统计	展示漏洞库支持的漏洞数量。	-

- 查看最近一次扫描结果

  扫描完成后，最近一次扫描结果展示在“上一次扫描详情”处，如下图所示。

单击“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，可以查看漏洞风险数、风险主机/目标检测主机、扫描类别、漏洞类别、开始时间、结束时间。
- 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。

- 页面下方展示漏洞列表。

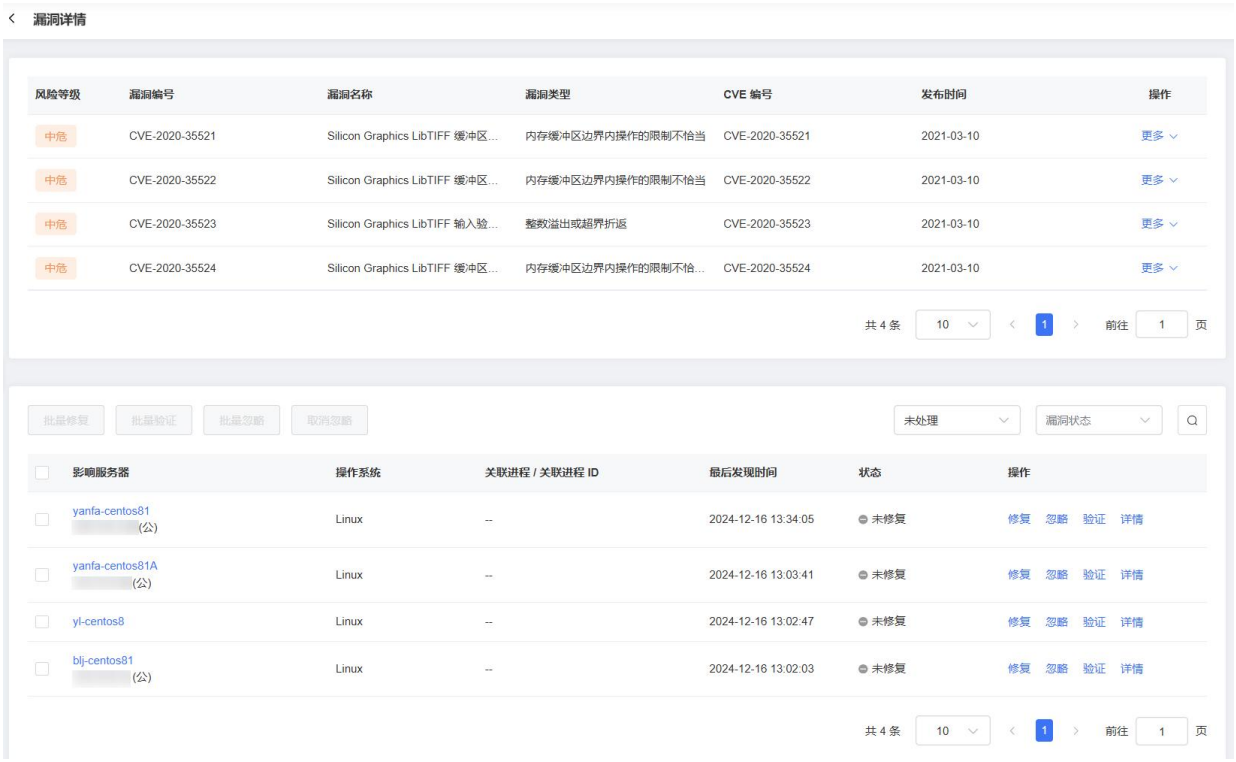
漏洞扫描页面下方的漏洞列表中展示本次扫描的漏洞情况，按照漏洞类别分页签展示，包括漏洞公告、CVE 编号、修复优先级、影响服务器数量、处理详情、最后发现时间。

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。漏洞列表可按照业务分组、修复后是否需要重启、修复优先级、漏洞是否已处理、服务器名称、服务器 IP、漏洞公告、CVE 编号进行搜索。

> 说明：
>
> 仅 Linux 软件漏洞、Windows 系统漏洞支持按照“修复重启”进行筛选，漏洞公告前若有“需要重启”标记，表示修复漏洞后，需要重启云服务器后才生效。

查看漏洞详情

1. 在漏洞列表中，点击“漏洞公告”链接、或操作列的“立即处理”时，可跳转至下方的漏洞详情页面。



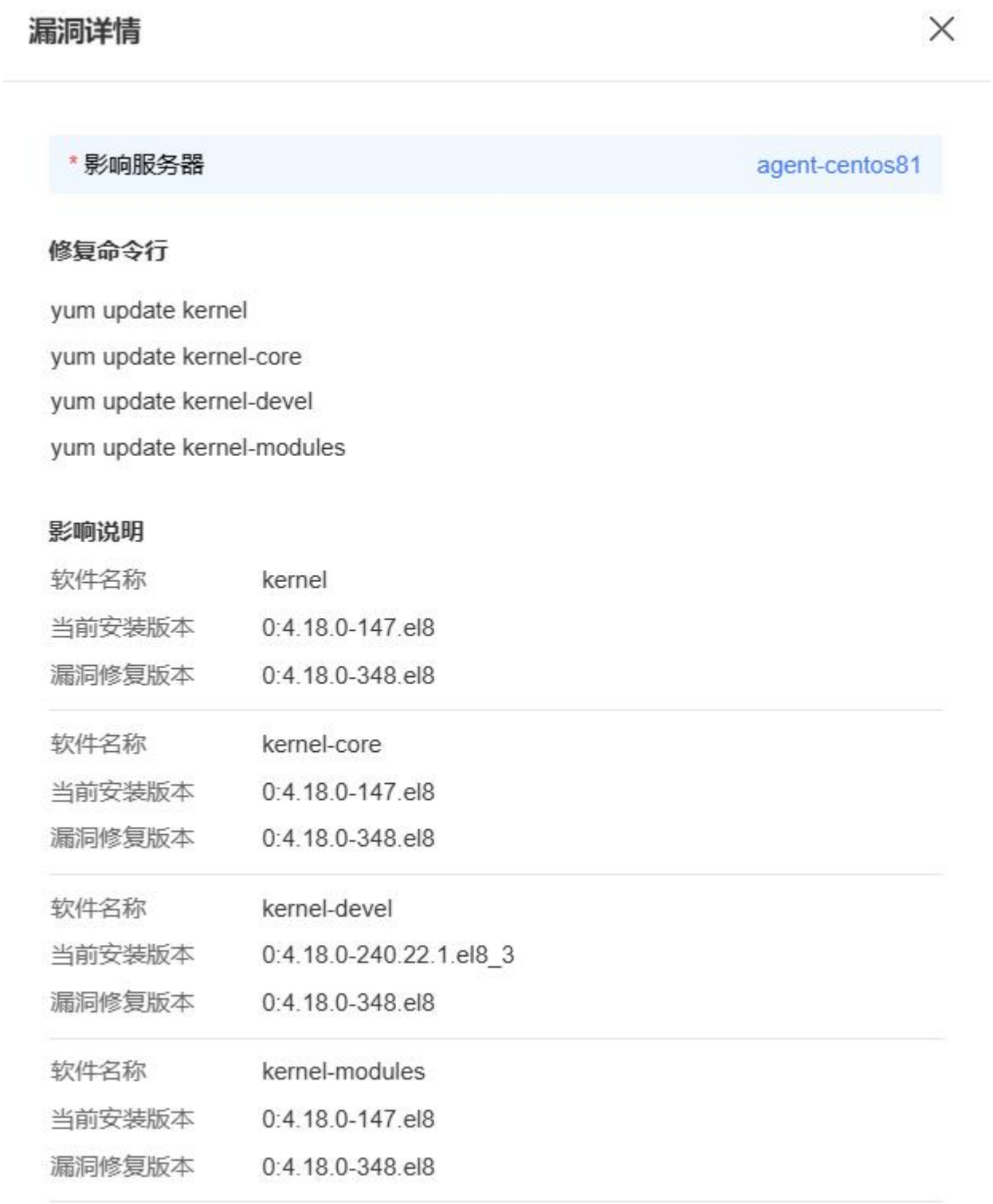
2. 在漏洞详情页面可查看漏洞公告包含的漏洞列表和影响服务器列表。

- 漏洞列表：包括风险等级、漏洞编号、漏洞名称、漏洞类型、发布时间，单击操作列的“更多”可查看漏洞的漏洞描述、参考链接、修复建议。

  风险等级与 CVE 漏洞等级保持一致，包括严重、高危、中危、低危、待定级。

- 影响服务器列表：包括影响服务器、操作系统、关联进程/关联进程 ID、最后发现时间、状态等。通过列表右上角的下拉框，可以根据漏洞是否已处理、漏洞修复状态，对漏洞影响的服务器列表进行筛选。

3. 单击影响服务器列表操作列的“详情”，可以查看漏洞影响的服务器、修复命令行，软件名称、当前安装版本、漏洞修复版本。



导出漏洞列表

说明：

- 支持导出的格式：支持“.csv”格式。
- 约束限制：导出数据不超过 20 万条。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 选择漏洞类型。
4. 单击漏洞列表右上角的“导出”图标，导出漏洞列表。

   若只需要导出部分漏洞，可以先进行筛选，筛选出目标漏洞信息后，再单击“导出”图标，导出您需要的漏洞列表。支持按照业务分组、修复后是否需要重启、修复优先级、漏洞是否已处理、服务器名称、服务器 IP、漏洞公告、CVE 编号进行筛选。

4.3.2.4. 处理漏洞

概述

漏洞处理方式：

处理方式	说明	影响
修复漏洞	如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。您可以在控制台一键自动修复漏洞，或根据漏洞修复建议，登录服务器手动修复漏洞。	-
漏洞加入白名单	如果确认漏洞不会对您的业务造成任何影响，无需修复，您可以将漏洞添加至白名单。	漏洞加入白名单后，漏洞列表不再展示该漏洞信息，在下一次漏洞扫描任务执行时，系

处理方式	说明	影响
		统不会再扫描和展示该漏洞信息。
忽略漏洞	某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某漏洞暂时无害，可以忽略该漏洞。	忽略漏洞后，下一次漏洞扫描任务执行时，系统仍然会扫描并展示该漏洞。
标记已修复	针对 Web-CMS 漏洞、应用漏洞，若您已手动修复，可将其“标记为已修复”。	漏洞标记为已修复后，漏洞列表中将不再展示该漏洞信息，下一次漏洞扫描任务执行时，系统仍然会扫描并展示该漏洞。

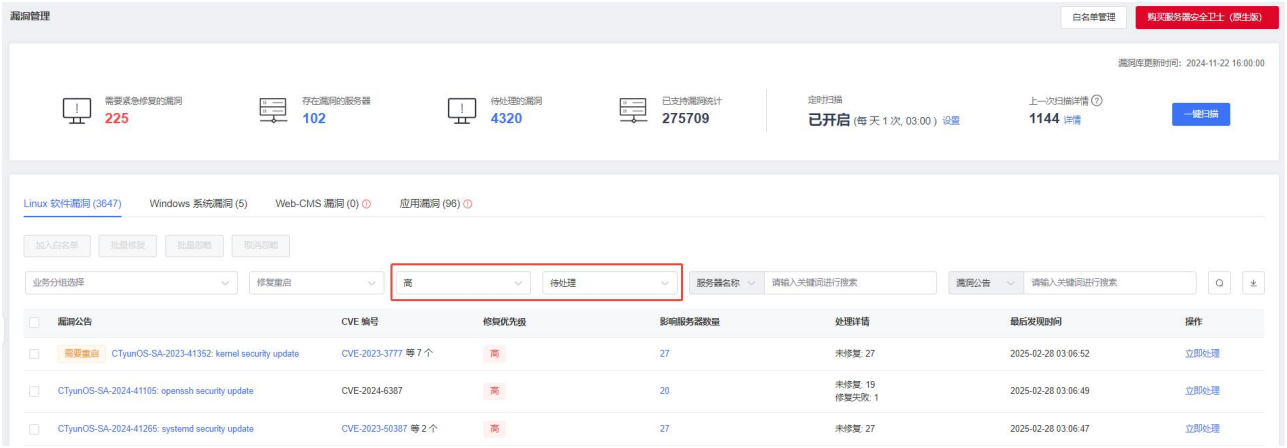
漏洞处理状态：

是否已处理	状态	说明
已处理	修复成功	表示漏洞已成功修复。
	修复成功待重启	表示已修复漏洞，还需要重启服务器。重启服务器同步新的资产后，状态将自动切换为“修复成功”。 说明： 针对 Linux 软件漏洞、Windows 系统漏洞，若漏洞公告前有“需要重启”标签，表示漏洞修复成功后，还需要重启云服务器才生效。
待处理	未修复	表示漏洞待修复。
	修复中	表示漏洞正在修复中。
	验证中	表示正在对漏洞处理状态进行验证。 说明： ● 当 Web-CMS 漏洞、应用漏洞为“未修复”时，可以点击“验证”对漏洞的处理状态进行验证。 ● 当 Linux 软件漏洞、Windows 系统漏洞为“未修复”、“修复失败”时，可以点击“验证”对漏洞的处理状态进行验证。
	修复失败	表示漏洞修复失败，可能是因为漏洞文件已被修改或漏洞文件已不存在。
已忽略	已忽略	漏洞已执行忽略操作，系统将不再对该漏洞进行告警。

查看需紧急修复的漏洞

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。

3. 单击“需紧急修复的漏洞”下方的数字，页面下方漏洞列表将筛选出修复优先级为“高”，待处理的漏洞。



修复漏洞

注意：

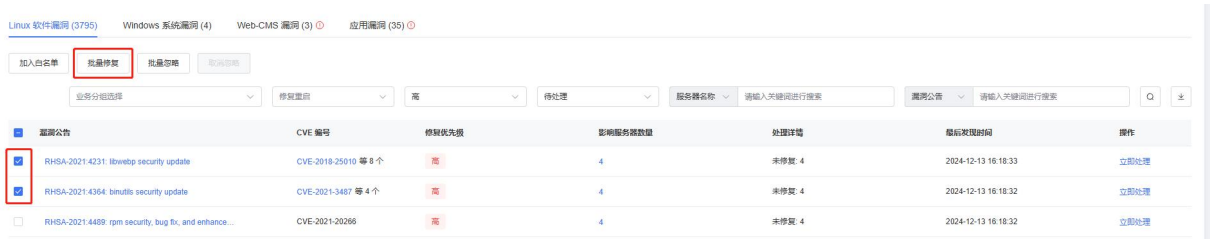
- 主机系统在进行漏洞修复过程中，无论修复成功或者失败，都有一定风险将导致应用业务中断，因此建议您在修复漏洞前为云主机手动创建快照并进行测试，快照支持系统回滚，可进行恢复。
- 执行漏洞修复前，请确认对应操作系统发行版的软件源已配置好（如 yum、zypper、apt-get 或 emerge 等包管理工具对应的软件源）。
- 内核漏洞修复成功后，需要重启服务器使新内核生效。针对 Linux 软件漏洞、Windows 系统漏洞，可根据漏洞公告前的标签进行判断，若有“需要重启”标签，表示漏洞修复成功后，还需要重启云服务器。

一键自动修复

注意：

- 购买企业版或旗舰版后，才支持一键自动修复漏洞。
- Web-CMS 漏洞、应用漏洞暂不支持一键修复，请手动修复相关漏洞。
- 当漏洞处理状态为“未修复”、“修复失败”时，可执行“修复”操作。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 勾选漏洞列表中所有需要修复的漏洞，单击漏洞列表左上角的“批量修复”，一键批量修复漏洞。



4. 在修复对话框中，选择修复所需软件源、确认待修复的漏洞数量和影响资产数量。
   - 软件源支持清华软件源、华为云软件源、阿里云软件源，也可以自配置软件源。若选择自配置软件源，请务必确认已在服务器上配置好对应操作系统发行版的软件源（如 yum、zypper、apt-get 或 emerge 等包管理工具对应的软件源）。
   - 您可以在修复对话框中查看漏洞公告、查看影响服务器数量。
5. 单击“确定”，开始自动修复漏洞。

手动修复漏洞

您可以参考漏洞详情页面的修复建议，登录服务器手动修复漏洞。

说明：

- 漏洞修复完成后需要手动重启服务器，否则系统仍可能为您推送漏洞消息。
- 不同的漏洞请根据修复建议依次进行修复。

执行以下步骤，查看漏洞修复建议：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 单击“漏洞公告”链接、或操作列的“立即处理”，跳转至漏洞详情页面。
4. 在漏洞列表单击操作列的“更多”，查看漏洞的修复建议。

忽略漏洞

某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某漏洞暂时无害，可以忽略该漏洞。

说明：

当漏洞处理状态为“未修复”、“修复失败”、“修复成功”、“修复成功待重启”时，可执行“忽略”操作。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 勾选漏洞列表中所有需要忽略的漏洞，单击漏洞列表左上角的“批量忽略”，一键批量忽略漏洞。

4. 在弹出的对话框中，确认忽略的漏洞数量和影响服务器数量后，单击“确定”。

漏洞忽略后将不再提示，您可在漏洞列表中选择已忽略漏洞进行取消忽略操作。

漏洞加入白名单

如果确认漏洞不会对您的业务造成任何影响，无需修复，您可以将漏洞添加至白名单。漏洞加入白名单后，漏洞列表不再展示该漏洞信息，在下一次漏洞扫描任务执行时，系统不会再扫描和展示该漏洞信息。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 勾选漏洞列表中所有需要加入白名单的漏洞，单击漏洞列表左上角的“加入白名单”，批量对漏洞进行加白。

4. 在弹出的对话框中，确认漏洞公告和影响服务器数量后，单击“确定”。

标记已修复

针对 Web-CMS 漏洞、应用漏洞，若您已手动修复，可将其“标记为已修复”，标记后，漏洞列表中将不再展示。

说明：

当漏洞处理状态为“未修复”时，可执行“标记已恢复”操作。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 选择漏洞类型。仅 Web-CMS 漏洞、应用漏洞支持标记已修复操作。
4. 勾选漏洞列表中所有已手动修复的漏洞，单击漏洞列表上方的“标记已修复”。

5. 在弹出的对话框中，确认漏洞公告和影响服务器数量后，单击“确定”。

修复验证

方式一：

说明：

当漏洞处理状态为“未修复”、“修复失败”时，可执行“验证”操作。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 在漏洞列表中，点击“漏洞公告”链接、或操作列的“立即处理”时，进入漏洞详情页面。
4. 在漏洞详情页面，单击“验证”，对漏洞处理状态进行验证。支持对单个服务器进行验证，或者批量进行验证。

方式二：漏洞处理完成后，可以手动执行一次漏洞扫描，查看漏洞处理结果。

4.3.2.5. 白名单管理

如果确认漏洞不会对您的业务造成任何影响，无需修复，您可以将漏洞添加至白名单。漏洞加入白名单后，漏洞列表不再展示该漏洞信息，在下一次漏洞扫描任务执行时，系统不会再扫描和展示该漏洞信息。

查看白名单列表

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 单击页面右上角的“白名单管理”，进入白名单管理页面。

4. 可以查看已加入白名单的漏洞，包括漏洞公告、CVE 编号、漏洞类别、修复优先级。

添加白名单

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 勾选漏洞列表中所有需要加入白名单的漏洞，单击漏洞列表左上角的“加入白名单”，批量对漏洞进行加白。

4. 在弹出的对话框中，确认漏洞名称和影响服务器数量后，单击“确定”。

移除白名单

您可以随时对已加入白名单的漏洞，从白名单中移除。移除后，下一次进行漏洞扫描时，系统将对该漏洞进行扫描并展示。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 单击页面右上角的“白名单管理”，进入白名单管理页面。
4. 选择需要移除的漏洞，点击操作列中的“移除白名单”，或勾选需要移除的漏洞，单击列表左上角的“移除白名单”，进行批量操作。

5. 在弹出的确认对话框中，单击“确定”，漏洞被移除白名单。

4.3.2.6. 漏洞扫描常见问题及处理方法

对 Linux 软件漏洞或 Windows 系统漏洞进行一键修复时，如果出现修复失败，您可以参照本说明确认失败的原因，根据给出的解决方案解决问题后再次尝试修复漏洞。如果根据错误码未能明确失败的原因，请提工单寻求天翼云技术支持人员协助分析。

错误码处理索引

错误码编号	错误信息	处理方案

错误码编号	错误信息	处理方案
100	无法连接软件源	错误码 100 处理方法。
101	无法连接微软官方服务器	Windows 系统漏洞修复需要连接微软官方服务器获取安全更新，请排查服务器与微软官网的网络是否联通。 可通过浏览器访问相关判断是否联通：测试页面。
102	软件源上没有可用包	错误码 102 处理方法。
103	没有匹配的安全更新	服务器繁忙导致 WUAPI 接口返回数据不准确，无法人为干预，建议稍后再试。
104	磁盘空间不足	检查磁盘使用情况，释放磁盘空间后再次尝试修复漏洞。
105	包管理命令(yum/apt)不存在	错误码 105 处理方法。
200	yum 执行命令失败	yum 执行命令失败原因多样，建议复制该命令到机器上执行，查看返回结果，根据具体情况分析可能的原因。 如果多次失败请提工单技术支持人员协助分析。
201	rpm 数据库损坏	错误码 201 处理方法。
202	yum 锁文件冲突	错误码 202 处理方法。
203	rpm 软件包依赖关系错误	错误码 203 处理方法。
300	apt 执行命令失败	apt 执行命令失败原因多样，建议复制该命令到机器上执行，查看返回结果，根据具体情况分析可能的原因。 如果多次失败请提工单技术支持人员协助分析。
301	apt 锁文件冲突	错误码 301 处理方法。
302	dpkg 依赖关系错误	错误码 302 处理方法。

错误码编号	错误信息	处理方案
500	Windows 更新代理 API 返回错误	参考微软官网 API 说明分析错误原因或提工单技术支持人员协助分析。
501	Windows 下载更新失败	如果是服务器繁忙导致下载失败，建议稍后再试。 如果多次失败建议参考微软官网 API 说明分析错误原因或提工单技术支持人员协助分析。
502	Windows 安装更新失败	如果 Windows 机器长时间未更新，建议登录机器，打开【设置】-【更新和安全】-【检查更新】并安装更新。 如果多次失败建议参考微软官网 API 说明分析错误原因或提工单技术支持人员协助分析。
1000	建议升级 Agent	请参考升级 Agnet 章节，升级 Agent 版本解决。
1001	基础版本不支持漏洞修复，建议升级企业版或者旗舰版	基础版本不支持漏洞修复，建议升级企业版或者旗舰版。
1002	修复超时	修复超时，建议稍后重试，如果多次超时或者失败请提工单技术支持人员协助分析。
1004	下发修复命令失败	下发修复命令失败，请先检查机器是否在线，保证机器在线后再次尝试修复漏洞。

4.3.3. 弱口令检测

通过与弱口令库对比，检测系统账号和应用账号口令是否属于常用的弱口令，提示用户修改不安全的口令。

- Linux 系统支持检测系统弱口令和数据库等应用弱口令。
- Windows 系统仅支持系统账号的弱口令检测。

版本限制

仅企业版、旗舰版支持弱口令检测功能。

执行弱口令检测

弱口令检测提供如下检测方式：

- 一键检测

  如果用户想立即了解服务器当前是否存在弱口令，可以执行“一键扫描”，立即手动检测服务器中的漏洞。

- 定时检测

  用户可以开启“定时扫描”，配置定时检测周期和范围，定期对服务器上存在的弱口令进行自动检测。

一键检测

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 弱口令检测”，进入弱口令检测页面。

3. 单击“一键扫描”，页面右侧弹出一键检测设置窗口。

4. 设置检测参数，参数说明如下。

参数	说明
弱口令分类	支持“应用弱口令”和“系统弱口令”。

参数	说明
设置生效范围	选择检测哪些服务器。可以选择“全部服务器”或“自选服务器”。 选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要检测的服务器。 说明： 以下服务器不能被选中执行弱口令检测： ● 使用“免费版”的服务器。 ● 非“运行中”状态的服务器。 ● Agent 状态为“离线”的服务器。

5. 单击“确认”，立刻开始本次弱口令检测。

> 说明：
>
> 检测需要一定的时间，请耐心等待，期间您可以切换页面执行其他操作。等待过程中您可以手动刷新页面查看最新检测数据。

定时检测

可开启定时检测，并进行定期检测周期、服务器选择的设置。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 弱口令检测”，进入弱口令检测页面。
3. 单击定时扫描右侧的“设置”，页面右侧弹出定时检测设置窗口，可进行定时检测设置。
4. 设置选项包括检测周期、弱口令分类、设置生效范围，详细参数说明如下。

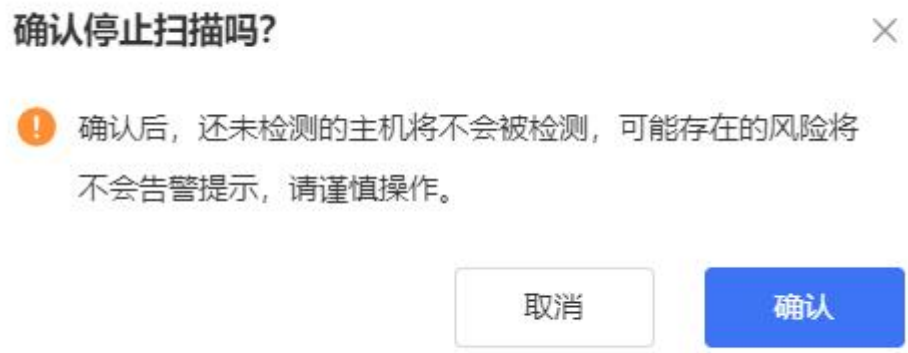
参数	说明
定时扫描	开启或关闭定时扫描。
检测周期	设置后会在周期选定的时间点开始定期检测。 扫描周期：选择每天、3 天或 7 天。 扫描时间：默认为 02:00，可以手动选择一天中的任一整点时间。
弱口令分类	支持“应用弱口令”和“系统弱口令”。
设置生效范围	选择检测哪些服务器。可以选择“全部服务器”或“自选服务器”。

参数	说明
	选择“自选服务器”时，您可以通过区域、服务器名称、服务器 IP 搜索需要检测的服务器。 说明 以下服务器不能被选中执行弱口令检测： ● 使用“免费版”的服务器。 ● 非“运行中”状态的服务器。 ● Agent 状态为“离线”的服务器。

停止检测

当开始一键检测或定时检测任务启动后，页面显示“正在扫描...”，如下图所示。

在扫描过程中，可随时“停止扫描”。单击“停止扫描”后弹出如下对话框，单击“确认”后停止检测。



查看弱口令检测结果

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 弱口令检测”，进入弱口令检测页面。
3. 在弱口令检测页面查看弱口令相关信息。
    - 查看弱口令检测统计信息

页面上方展示弱口令检测的统计情况和弱口令检测设置。统计情况包括系统弱口令和应用弱口令的风险项数量、风险服务器数量。

- 查看弱口令检测结果列表

  页面下方展示最新一次检测完成的弱口令列表，分别按系统弱口令和应用弱口令进行展示。

  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。

- 查看某台服务器的弱口令检测结果

  点击列表中的服务器名称，跳转至资产详情页面。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。

  点击弱口令列表中的服务器名称，可以查看该基线名称下该台服务器的检测详情。

  - 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。

4.4. 入侵检测

4.4.1. 告警中心

告警中心用于汇总展示所有入侵检测模块的告警信息，帮助用户快速了解整体安全告警概况。包括需紧急处理的告警、待处理告警、已处理告警；存在告警的服务器、已隔离文件、已拦截 IP。

前提条件

入侵检测防护模块已开启防护，详细操作请参见安全配置。

查看告警

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 告警中心”，进入告警中心页面。

3. 在页面右上角选择查询告警的时间范围。

   - 支持选择固定周期：最近 24 小时、最近 3 天、最近 7 天、最近 30 天。
   - 也可以自定义时间范围，自定义只能选择 30 天范围内。

4. 查看告警统计信息。页面上方展示所有入侵检测模块告警的统计情况。

统计项	说明	操作
需紧急处理的告警	展示在选择的时间范围内，告警等级为“高危”且“待处理”告警数量。	单击“需紧急修复的告警”的数值，页面下方告警列表将展示告警等级为“高危”且“待处理”的告警。
待处理告警	展示在选择的时间范围内，所有的“待处理”告警个数统计。	单击“待处理告警”的数值，页面下方告警列表将展示所有“待处理”的告警。
已处理告警	展示在选择的时间范围内，所有的“已处理”告警个数统计。	单击“已处理告警”的数值，页面下方告警列表将展示所有“已处理”的告警。
存在告警的服务器	展示在选择的时间范围内，存在告警的服务器个数（展示去重后的个数）。	单击“存在告警的服务器”的数值，页面下方告警列表将展示“待处理”的告警，且每个服务器只展示一条告警（告警展示优先级按照告警等级进行展示，高>中>低，相同等级按照时间最近展示）。
已隔离文件	展示在选择的时间范围内，已隔离的文件个数（展示去重后的个数）。	单击“已隔离文件”的数值，页面下方告警列表将展示“已处理”的告警，且每个文件只展示一条告警（按照时间最近优先展示）。
已拦截 IP	展示在选择的时间范围内，暴力破解阻断状态为“阻断成功”的 IP 个数（展示去重后的个数）。	单击“已拦截 IP”的数值，页面下方告警列表将展示“已处理”的告警，且每个 IP 只展示一条告警（按照时间最近优先展示）。

5. 选择告警分类，支持根据“ATT&CK 攻击阶段”或“告警类型”查看告警统计信息。

- ATT&CK 攻击阶段：展示在选择的时间范围内不同攻击标识的“待处理”告警个数统计。

ATT&CK 攻击阶段	说明
侦察	攻击者收集您的网络或系统中的信息，尝试发现漏洞，以找到攻击入口。
初始访问	攻击者尝试进入您的网络或系统。
执行	攻击者成功进入您的系统，尝试运行恶意软件或命令，以进一步控制系统或窃取数据。
持久化	攻击者采取措施以确保其在系统中的持久存在，以便在需要时重新访问或继续攻击。 可能涉及设置后门、修改系统配置、利用系统漏洞等。
权限提升	攻击者尝试从普通用户权限提升为管理员或系统权限，以便控制整个系统。
防御绕过	攻击者尝试使用各种技术来绕过安全防御措施，避免被检测到。 如使用混淆加密技术对恶意软件进行二次封装、利用系统漏洞进行攻击等。
凭据访问	攻击者收集系统中的敏感数据，如账号名称和密码。
命令与控制	攻击者尝试建立与被攻击机器的通信渠道，以便远程控制机器上的恶意软件或执行其他攻击操作。
影响破坏	攻击者利用收集到的数据或控制的系统，尝试对您的系统造成损害，如数据泄露、系统瘫痪等。

- 告警类型：展示在选择的时间范围内不同告警类型的“待处理”告警个数统计。

告警类型	说明
异常登录	检测“异地登录”和“爆破登录”，如果发生异常登录，则说明您的主机可能被黑客入侵成功。 通过配置异常登录白名单，将常用登录地、常用登录 IP 等添加至白名单中，非白名单中的登录操作，将被视为异常登录。
暴力破解	系统默认阻断尝试暴力破解（在短时间内多次登录失败）的登录 IP。 通过配置暴力破解白名单，将可信任的 IP 添加至白名单中。
后门检测	检测云主机中存在的后门并进行告警，支持告警的类型包括存在可疑文件、存在可疑可执行文件、存在木马文件、Dev 目录异常、存在可疑进程、存在异常端口、存在网卡异常。
可疑操作	检测云主机上的可疑操作并进行告警，系统提供默认检测规则，用户也可以自定义检测规则。
反弹 Shell	检测用户的进程行为，支持对非法连接进程的行为进行告警。
进程提权	检测进程提权操作并进行告警。
WebShell	检测服务器 Web 目录下的文件内容，发现 Web 网站中存在的后门文件，若检测出后门文件，系统会向您提供实时告警。

告警类型	说明
端口蜜罐	通过部署蜜罐，实时监听攻击者对蜜罐端口的扫描行为，若发现异常扫描行为，系统会向您提供实时告警。

6. 查看告警列表，告警列表展示如下信息。

参数	说明
告警等级	告警的等级，包括高危、中危、低危。
告警名称	告警的名称。
告警类型	告警的类型，包括异常登录、暴力破解、后门检测、可疑操作、反弹 Shell、进程提权、WebShell、端口蜜罐。
攻击标识	ATT&CK 攻击阶段，包括侦察、初始访问、执行、持久化、权限提升、防御绕过、凭据访问、命令与控制、影响破坏。
影响资产	受影响的服务器，展示名称和 IP 地址。
发现时间	告警发现时间。
状态	分为已处理和未处理。

处置告警

您可以根据自己的业务需求，自行判断并处理告警，快速清除资产中的安全威胁。告警处理完成后，告警的状态将从“未处理”变为“已处理”。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 告警中心”，进入告警中心页面。
3. 在页面下方的告警列表中，单击告警操作列的“处置”，将进入对应入侵检测页面。
4. 根据告警类型对告警进行处理。

导出告警

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 告警中心”，进入告警中心页面。

3. 单击告警列表右上角的“导出”图标，导出告警。

   如果您只需要导出某个 ATT&CK 攻击阶段的告警或某一类告警，您可以先选中相应的 ATT&CK 攻击阶段或告警事件类型，再单击“导出”图标。

4. 页面右上角会显示导出状态，当导出完成后，单击“下载”，将告警列表下载到本地。

   注意：

   若“关闭”页面，此时告警列表还未下载到本地，若需要下载，则需要重新导出。

4.4.2. 白名单管理

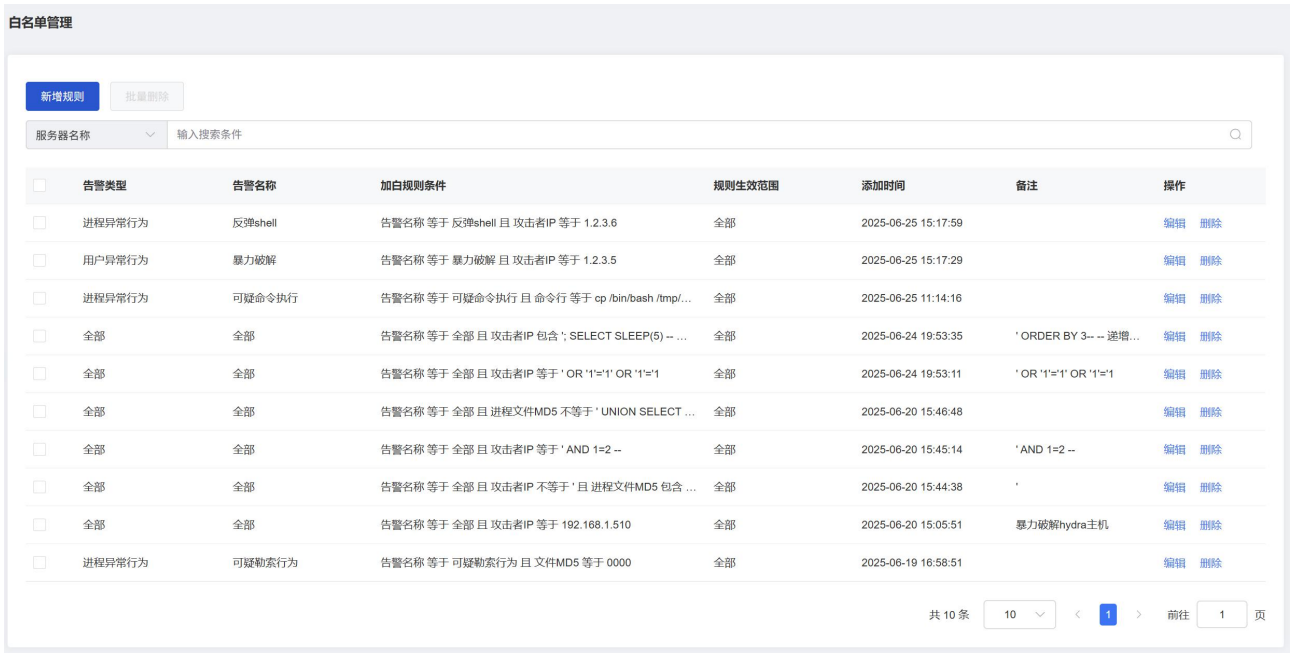
针对已经添加白名单的告警，您可以在白名单管理中对其进行编辑或删除。

编辑白名单

1.登录服务器安全卫士（原生版）控制台。

2.在左侧导航栏，选择“入侵检测 > 白名单管理”，进入白名单管理页面。

展示的字段为告警类型、告警名称、加白规则条件、规则生效范围、添加时间。



3.可通过**服务器名称**、**服务器 IP** 或**告警名称**搜索白名单规则，选择需要编辑的白名单规则，单击“操作”列的“编辑”按钮。

4 在弹出的“白名单编辑”对话框中，可编辑白名单规则的**生效服务器范围**和**备注**。

5.在编辑完成后，单击“确认”即可完成白名单规则编辑。

新增白名单规则

1.登录服务器安全卫士（原生版）控制台。

2.在左侧导航栏，选择“入侵检测 > 白名单管理”，进入白名单管理页面。

3.单击“新增规则”即可开始新增白名单规则。

4.在弹出的对话框中配置白名单规则。

参数	参数说明

参数	参数说明
告警类型	选择该白名单规则适用的告警类型。
告警名称	选择该白名单规则适用的告警名称。
加白规则	自定义加白规则，最多支持添加三条。
设置生效范围	可选择“全部服务器”和“自选服务器”。

5.填写完成后，单击“确定”即可完成白名单规则配置。

删除白名单规则

1.登录服务器安全卫士（原生版）控制台。

2.在左侧导航栏，选择“入侵检测 > 白名单管理”，进入白名单管理页面。

3.搜索需要删除的白名单规则，单击“操作”列的“删除”按钮即可删除白名单规则，若您需要批量删除可勾选白名单规则，单击页面左上角的“批量删除”按钮进行删除。

4.5. 文件安全

4.5.1. 病毒查杀

4.5.1.1. 概述

服务器安全卫士（原生版）的病毒查杀功能，支持对挖矿木马、蠕虫、勒索病毒等进行有效的检测，提供灵活的检测方式，支持一键检测和定时检测方式，通过简单操作即可完成对病毒的处理，支持对病毒文件进行隔离、删除和信任。

病毒检测模式

包含快速检测、全盘检测、自定义检测三种模式。

- 快速检测：扫描耗时短，对系统关键位置文件进行扫描。
- 全盘检测：对主机所有硬盘文件进行扫描，清理更彻底。
- 自定义检测：按指定位置有选择性扫描文件。

病毒扫描方式

提供实时检测、一键扫描、定时扫描三种扫描方式，方便用户基于实际使用场景进行操作。

病毒文件处理方式

服务器安全卫士（原生版）检测到病毒文件会立即产生告警，需要您根据告警详细信息对病毒文件作出处置，处置方式包括以下三种：

- 隔离：将病毒文件或恶意程序移动至隔离区域，进行加密处理，禁止正常运行。对于已隔离的文件，支持取消隔离。
- 删除：永久从系统中删除病毒文件或恶意程序，以确保不再有可能的威胁。

  注意：

  文件删除后将不可恢复，请谨慎操作。

- 信任：经分析后确认为误报，可以选择将文件进行信任，信任后将不再对该文件进行检测告警。

4.5.1.2. 扫描病毒

病毒扫描是服务器执行病毒扫描操作，发现病毒文件并处理的防护机制。

约束限制

请先购买企业版或旗舰版配额并绑定主机后，才能正常使用病毒查杀功能。

一键扫描

一键扫描为手动检测模式，用户需在病毒查杀页面单击一键扫描按钮，设置检测模式、生效范围。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 单击“一键扫描”，页面右侧弹出一键扫描设置窗口。

4. 在一键扫描设置窗口中，设置扫描参数。

参数说明如下：

参数	说明
检测模式	可选择快速检测、全盘检测、自定义检测。 ● 快速检测：扫描耗时短，有效扫描随系统自启动运行的风险文件。主要扫描系统常被利用的位置。 ● 全盘检测：扫描服务器所有磁盘文件，清理磁盘中的木马病毒更彻底，相对比较耗时。 ● 自定义检测：根据用户设置的指定目录有选择性的进行扫描。
设置生效范围	自定义选择需要执行病毒扫描任务的服务器。

5. 单击“确认”，设置完成。

病毒查杀设置

支持配置本地检测引擎开关、实时检测配置、定时扫描配置。

配置步骤如下：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 单击设置按钮或设置图标，页面右侧弹出病毒查杀设置窗口。

4. 根据需要进行病毒查杀设置。

配置项	说明	默认状态
本地检测引擎	本地检测引擎内置 AI 智能识别检测引擎，打开本地检测引擎开关后，实现本地 + 云端双引擎检测模式，检测更精准。	默认关闭
启用实时检测	实时检测系统关键目录下文件与系统进程，及时发现恶意文件及异常进程。 开启实时检测后，还需要设置生效范围，自定义选择需要执行病毒扫描任务的服务器。	默认开启
定时扫描	定时查杀是用来配置服务器定时启动病毒查杀的功能，开启定时扫描后，系统会按照用户设置的检测周期定时执行扫描任务。 ● 检测模式： ■ 快速检测：扫描耗时短，有效扫描随系统自启动运行的风险文件。主要扫描系统常被利用的位置。 ■ 全盘检测：扫描服务器所有磁盘文件，清理磁盘中的木马病毒更彻底，相对比较耗时。 ■ 自定义检测：根据用户设置的指定目录有选择性的进行扫描。 ● 检查周期：可选择每天、每 3 天或每 7 天检查周期。 ● 设置生效范围：自定义选择需要执行病毒扫描任务的服务器。	默认开启 默认每天 07:00 执行快速扫描任务

5. 单击“确认”，设置完成。

4.5.1.3. 查看并处理病毒

前提条件

已完成病毒扫描。详细操作请参见扫描病毒。

查看扫描结果

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 在病毒查杀页面查看病毒相关信息。

- 查看统计信息

  页面上方展示告警事件和风险服务器的统计情况。

- 查看告警列表

  页面下方展示告警事件详情。

  告警事件列表展示字段包括服务器、操作系统、文件路径、病毒名称、威胁等级、首次发现时间、最后检测时间、状态和操作。

  告警事件支持按发现时间、告警类型、威胁等级、处理状态、服务器名称、服务器 IP 进行搜索。

- 查看告警详情

  单击“详情”，查看病毒文件详细信息，包括扫描目录、扫描文件数、扫描路径文件总大小、威胁等级、扫描用时、扫描开始时间、扫描结束时间、告警 ID、告警时间等。

导出病毒文件列表

说明：

- 支持导出的格式：支持“.csv”格式。
- 约束限制：导出数据不超过 20 万条。

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 单击病毒文件列表右上角的“导出”图标，导出病毒文件列表。

   若只需要导出部分病毒文件，可以先进行筛选，筛选出目标信息后，再单击“导出”图标，导出您需要的病毒文件列表。支持按照发现时间、处理状态、服务器名称、服务器 IP、文件 MD5 进行筛选。

4. 页面右上角会显示导出状态，当导出完成后，单击“下载”，将告警列表下载到本地。

> 注意：
>
> 若“关闭”页面，此时告警列表还未下载到本地，若需要下载，则需要重新导出。

处理病毒文件

提供隔离、删除、信任三种病毒处理方式。

- 隔离：手动隔离病毒文件，文件隔离成功后将移动至隔离区并加密，无法再对服务器造成威胁。如用户有恢复需求，可“取消隔离”恢复文件至原路径。
- 删除：手动删除病毒文件，删除文件可能影响业务系统正常运行，文件被删除后无法恢复，请谨慎操作。
- 信任：经分析后确认为误报，可以选择信任文件，信任后该条告警将从告警列表移除，加入信任区。若需要从信任区移除，请参见信任区管理。

> 注意：
>
> 加入信任区的文件，将不再对其进行检测告警，请谨慎操作。

信任区管理

您可以随时对已加入信任区的文件，从信任区中取消信任。取消信任后，该文件将不被信任，正常产生告警。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 病毒查杀”，进入病毒查杀页面。
3. 单击页面右上角的“信任区”，进入信任区管理页面。
4. 选择需要取消信任的文件，点击操作列中的“取消信任”。

   或勾选多个文件，单击列表左上角的“取消信任”，进行批量操作。

5. 在弹出的确认对话框中，单击“确定”，文件从信任区移除。

4.5.2. 文件防勒索

4.5.2.1. 概述

约束限制

请先购买企业版或旗舰版配额并绑定主机后，才能正常使用文件防勒索功能。

数据备份恢复功能目前仅支持华东 1、华北 2、西南 1、华南 2 资源池。

勒索防护手段

围绕事前、事中、事后三个阶段进行防护，可以有效地应对勒索病毒的威胁。

1. 风险预防（事前）

   页面展示漏洞扫描和基线检测最后一次扫描结果，如存在风险需单击未处理漏洞数及未处理风险项进入告警详情页进行处置。

2. 勒索防御（事中）

   页面展示病毒查杀最后一次扫描结果，如存在风险需单击未处理风险文件进入告警详情页进行处置；开启诱饵防护，在系统关键位置投放诱饵文件，实时捕捉勒索行为，阻止勒索病毒对数据的加密。

3. 数据备份/恢复（事后）

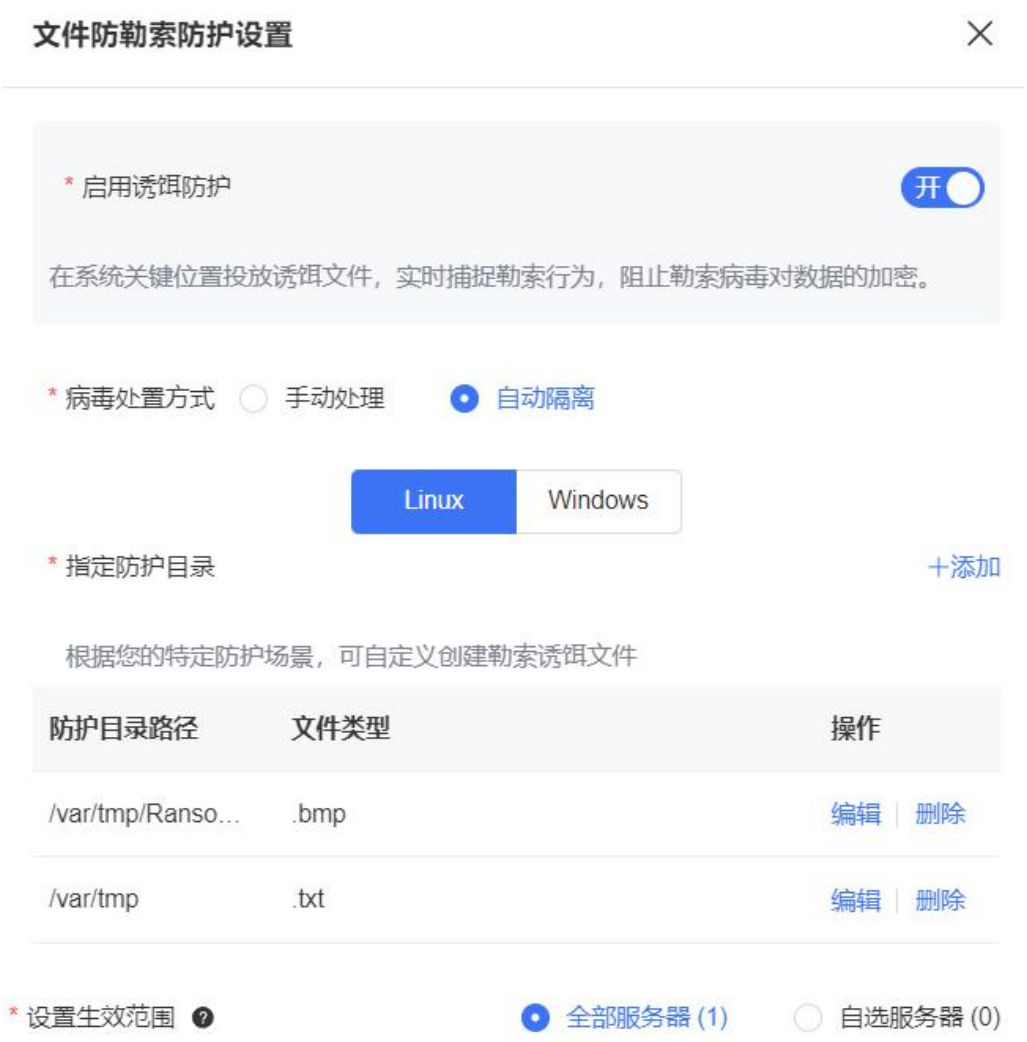
   对关键数据进行备份，在被勒索后，可以对备份节点数据一键恢复。

4.5.2.2. 启用诱饵防护

操作步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 单击诱饵防护模块的“设置”按钮。

4. 在页面右侧弹出的防护设置页面，配置防护参数。



参数说明：

参数	说明
启用诱饵防护	自动在系统关键位置投放诱饵文件，实时捕捉勒索行为并进行阻断。

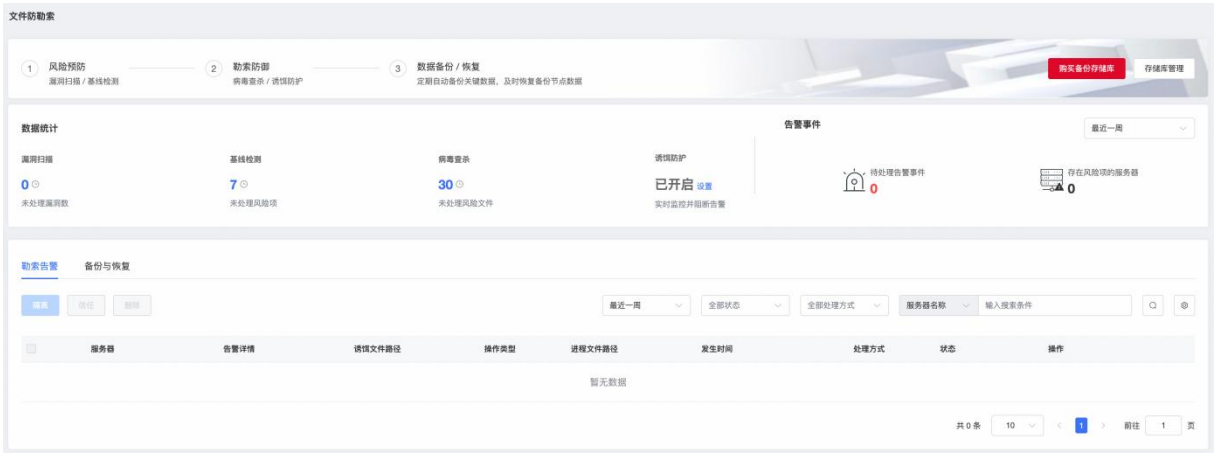
参数	说明
病毒处置方式	配置发现勒索病毒文件后的处理方式。支持手动处理和自动隔离。 ● 手动处理：检测出勒索病毒文件后，仅产生告警。需手动在控制中心对勒索告警进行处理，支持隔离、删除、信任，详细操作请参见处理勒索告警。 ● 自动隔离：检测出勒索病毒文件后产生告警，并自动隔离病毒文件。 说明： 自动隔离后，若出现误报，可在告警列表中对文件进行恢复。
指定防护目录	根据用户的特定防护场景，可自定义创建勒索诱饵文件。
生效范围	自定义选择需要开启诱饵防护的服务器。

5. 配置完成后，单击“确认”。

4.5.2.3. 查看并处理告警

查看勒索告警

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。



3. 告警事件列表展示字段包括服务器、告警详情、诱饵文件路径、操作类型、发生时间、处理方式、状态和操作。告警事件支持按服务器名称和服务器 IP 进行搜索。

处理勒索告警

提供如下处理方式：

- 隔离：手动隔离病毒文件，文件隔离成功后将移动至隔离区并加密，无法再对服务器造成威胁。
- 取消隔离：对已隔离的文件，如用户有恢复需求，可恢复原始文件。
- 删除：手动删除病毒文件，文件被删除后无法进行恢复，请谨慎进行操作。
- 信任：经分析后确认为误报，可以选择将文件进行信任，信任后将不再对该文件进行检测告警。

4.5.2.4. 数据备份/恢复

前提条件

数据备份/恢复属于增值服务，请先购买备份存储库，才能正常使用。

开启勒索备份

为了避免被勒索后数据丢失，请为服务器开启勒索备份，定期备份数据。

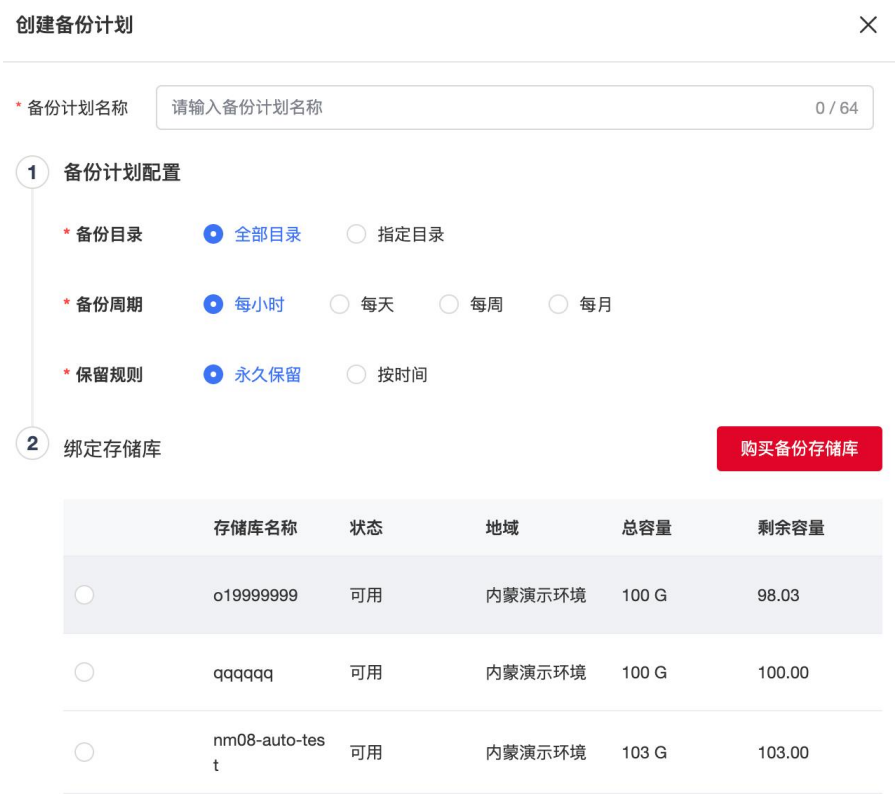
安装备份 Agent

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，选择需要进行数据备份的服务器，单击操作列的“安装备份 Agent”，Agent 状态为“已激活”则安装成功。

   如需卸载 Agent，可单击“卸载备份 Agent”。

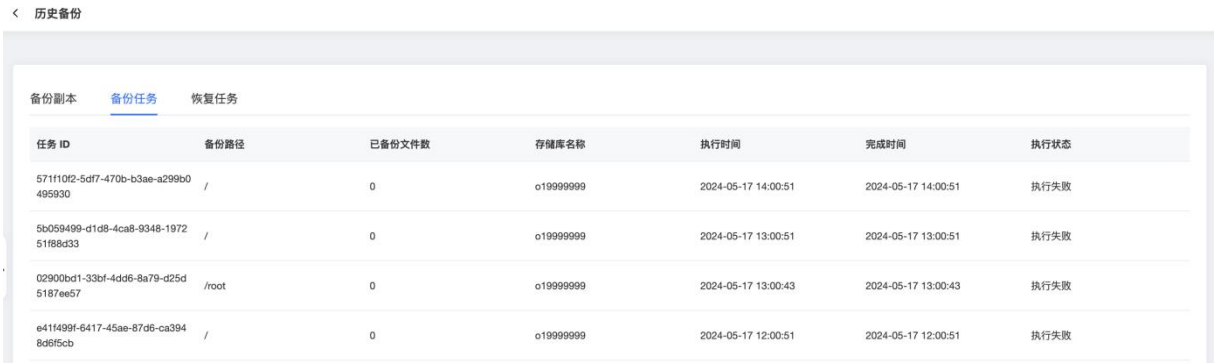
创建备份计划

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，选择需要进行数据备份的服务器，单击“备份计划”，按照设置的策略进行周期性数据备份。
   - 备份目录：可指定全部目录或自定义目录进行数据备份。
   - 备份周期：可选择每小时、每天、每周或每月设置备份周期。
   - 保留规则：可设置备份计划生效时间，支持永久保留和自定义设置时间。
   - 绑定存储库：选择一个可用状态的存储库，备份数据大小应小于存储库剩余容量。



查看备份任务

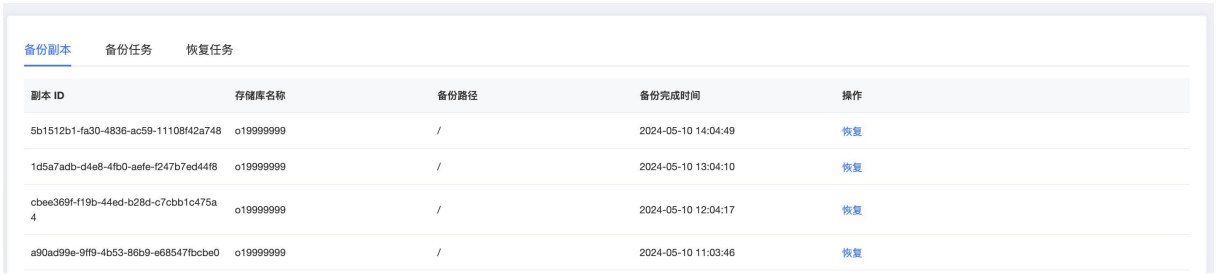
1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，单击目标服务器的“历史备份”，进入历史备份页面。
4. “备份任务”列表中展示执行备份任务的状态及详情，包括备份路径、已备份文件数、存储库名称、执行时间、完成时间、执行状态。



恢复备份数据

查看备份数据

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，选择已进行数据备份的服务器，单击操作列的“历史备份”。
4. “备份副本”列表展示按用户创建的备份计划自动生成的备份数据。



恢复备份数据

用户可选择指定备份副本进行恢复，备份数据支持恢复到原目录或指定目录。

1. 登录服务器安全卫士（原生版）控制台。

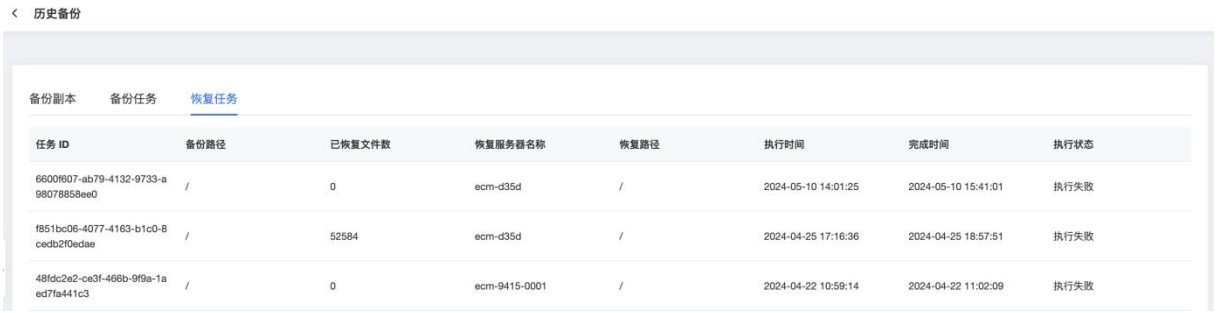
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，选择已进行数据备份的服务器，单击操作列的“历史备份”。
4. 在“备份副本”页面，选择需要恢复的备份副本，单击操作列的“恢复”，对数据进行恢复。

   备份数据支持恢复到原目录或指定目录。

查看恢复任务

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“备份与恢复”页面，选择已进行数据备份的服务器，单击操作列的“历史备份”。
4. 在“恢复任务”页签，可以查看恢复任务的状态及详情。当执行状态为“任务完成”时，表示恢复任务执行成功。

   恢复任务列表中展示用户下发恢复任务的状态及详情，包括备份路径、已恢复文件数、恢复服务器名称、恢复路径、执行时间、完成时间、执行状态。



4.5.3. 文件完整性保护

4.5.3.1. 概述

文件完整性保护功能可实时监控主机上的文件，对创建文件、修改文件、删除文件及文件提权操作进行监控和告警，可帮助用户及时发现非预期的文件变更，及时发现可能遭受的攻击。

约束限制

请先购买旗舰版配额并绑定主机后，才能正常使用文件完整性保护功能。

使用流程

流程	说明
设置检测规则	默认对系统关键文件、文件路径、文件目录进行实时监控，用户也可以自定义配置监控路径。
查看并处理告警	查看文件变更结果并对结果进行处理。

4.5.3.2. 设置检测规则

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件完整性保护”，进入文件完整性保护页面。
3. 单击列表右上方的“检测设置”，进入检测设置页面。

4. 配置相关参数。

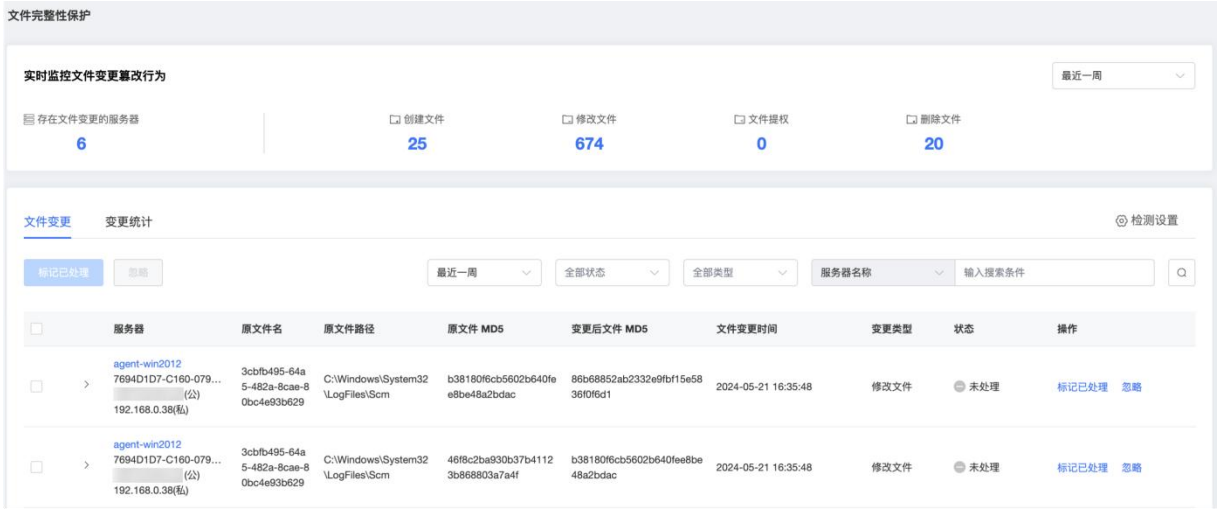
参数	说明
启用文件变更检测	开启或关闭文件变更检测功能。
关键文件监控	● 系统内置：对系统关键文件、文件路径、文件目录进行实时监控，发现文件变更篡改行为进行告警。 ● 自定义：根据用户特定的防护场景，自定义添加监控路径，发现文件变更篡改行为进行告警。
监控排除设置	对用户添加的信任文件路径不再进行监控，方便用户更加灵活创建检测策略。
设置生效范围	自定义选择需要执行文件变更篡改行为监控的服务器。

5. 配置完成后，单击“确认提交”。

4.5.3.3. 查看并处理告警

查看告警

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件完整性保护”，进入文件完整性保护页面。



3. 查看统计数据和变更信息。

- 查看统计信息

  上方展示文件变更篡改行为事件和存在文件变更服务器的统计情况。

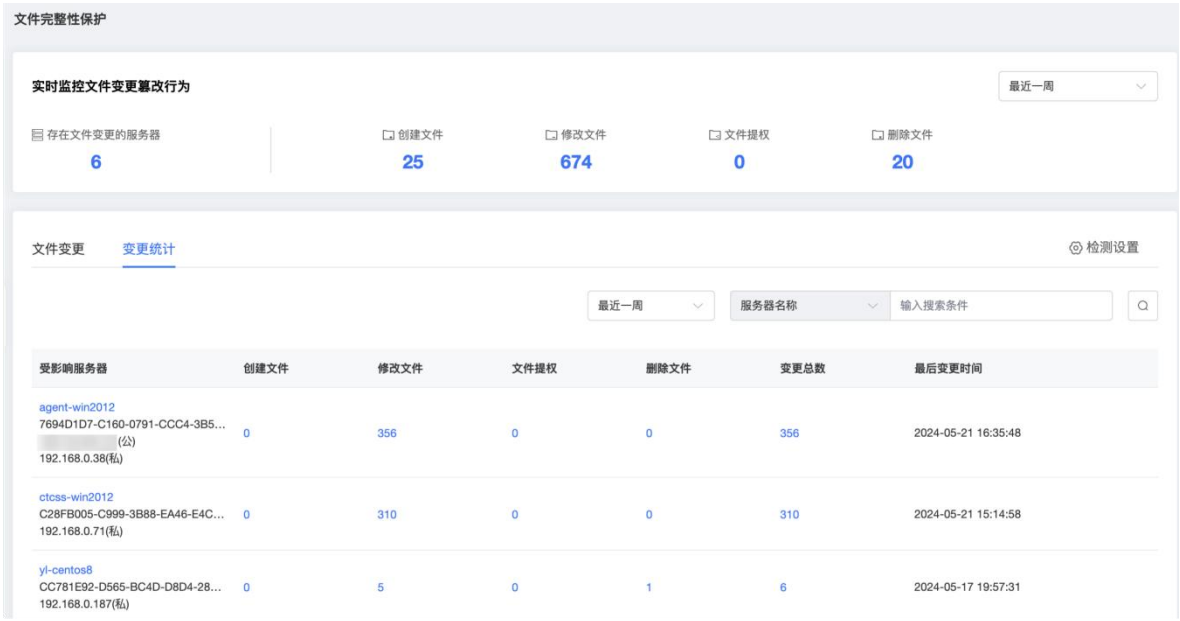
- 查看文件变更信息

  在页面下方的“文件变更”页签，展示文件变更列表，展示字段包括服务器、原文件名、原文件路径、变更后文件 MD5、文件变更时间、变更类型、状态。

  告警事件支持按发现时间、处理状态、变更类型、服务器名称和服务器 IP 进行搜索。

- 查看变更统计信息

  在页面下方的“变更统计”页签，系统帮助您自动统计出所有存在文件变更篡改行为的服务器。单击文件变更类型列的数字可查看详情。



处理告警

标记为已处理

若您已手动处理文件变更告警，可将其“标记为已处理”，标记后，告警的状态将从“未处理”变为“已处理”。具体操作步骤如下：

1. 在文件变更告警列表中，找到目标告警，单击操作列的“标记已处理”，或勾选目标告警，单击列表上方的“标记已处理”进行批量处理。

2. 在弹出的对话框中单击“确定”。

忽略

经过分析后确认文件变更为正常操作，可忽略本次文件变更告警。忽略后，告警的状态将从“未处理”变为“已忽略”，后续再次监控到相同文件变更篡改行为，系统将正常进行告警。

具体操作步骤如下：

1. 在文件变更告警列表中，找到目标告警，单击操作列的“忽略”，或勾选目标告警，单击列表上方的“忽略”进行批量处理。

2. 在弹出的对话框中单击“确定”。

4.6. 导出告警

支持导出的告警：基线检测、漏洞扫描、弱口令检测、异常登录、暴力破解、后门检测、可疑操作、反弹 shell、进程提权、Webshell、端口蜜罐、病毒查杀、文件防勒索、文件完整性保护等告警。

支持导出的格式：支持“.csv”格式。

操作步骤

如下以导出异常登录告警为例，介绍导出告警的详细步骤。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“入侵检测 > 异常登录”，进入异常登录页面。
3. 单击告警列表右上角的“导出”图标，导出告警列表。

   若只需要导出某一类告警或某一段时间内的告警，可以先筛选告警，再进行导出。支持按照告警类型、时间、状态、登录源 IP、登录账号、服务器名称、服务器 IP 进行筛选。

4. 页面右上角会显示导出状态，当导出完成后，单击“下载”，将告警列表下载到本地。

   注意：

   若“关闭”页面，此时告警列表还未下载到本地，若需要下载，则需要重新导出。

4.7. 网页防篡改（原生版）

4.7.1. 购买网页防篡改配额

网页防篡改功能为付费的增值服务，需要单独购买。

操作步骤

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“网页防篡改 > 防护状态”，在页面右上角单击“购买配额”。

   首次使用网页防篡改功能时，进入如下页面，单击“立即升级”。

3. 在订购页面配置购买数量和购买时长。

   - 配置“购买数量”：购买数量需大于等于 1。
   - 支持开启“自动续订”，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。
     - 按月购买，自动续费周期默认为 1 个月。
     - 按年购买，自动续费周期默认为 1 年。

     如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。
   - 选择“购买时长”，可拖动时间轴设置购买时长。

4. 确认配置参数和配置费用，阅读《天翼云网页防篡改（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云网页防篡改（原生版）服务协议》“，单击“立即购买”。
5. 进入“付款”页面，完成付款。

   购买完成后，即可进入防护配额页面，查看已购买的配额。

4.7.2. 防护状态

防护状态包括防护数据统计、防护文件统计图 Top5、文件变动数 Top5 和告警列表。

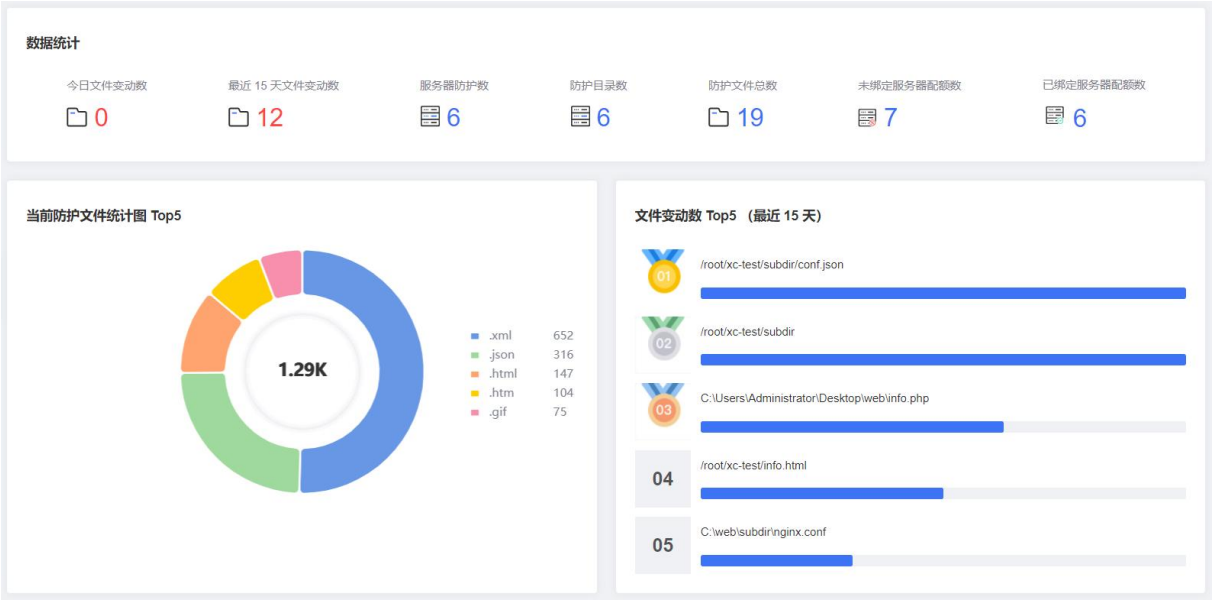
操作步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版） > 防护状态”，进入防护状态页面，查看防护详情。

防护数据统计

数据统计：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：您可查看当前防护文件统计图 Top5 和文件变动数 Top5（最近 15 天）的统计图。



告警列表

您可查看文件增加、删除、修改异常的告警列表，包括受影响服务器、告警等级、告警名称、文件路径、时间、防护状态。

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。

您可根据时间（可选时间为最近一周、最近一月和最近三月）、服务器名称和服务器 IP 进行告警筛选。

若当前告警不需要再展示，可以选择忽略或批量忽略告警，忽略后，该告警不再展示在列表中。

4.7.3. 防护管理

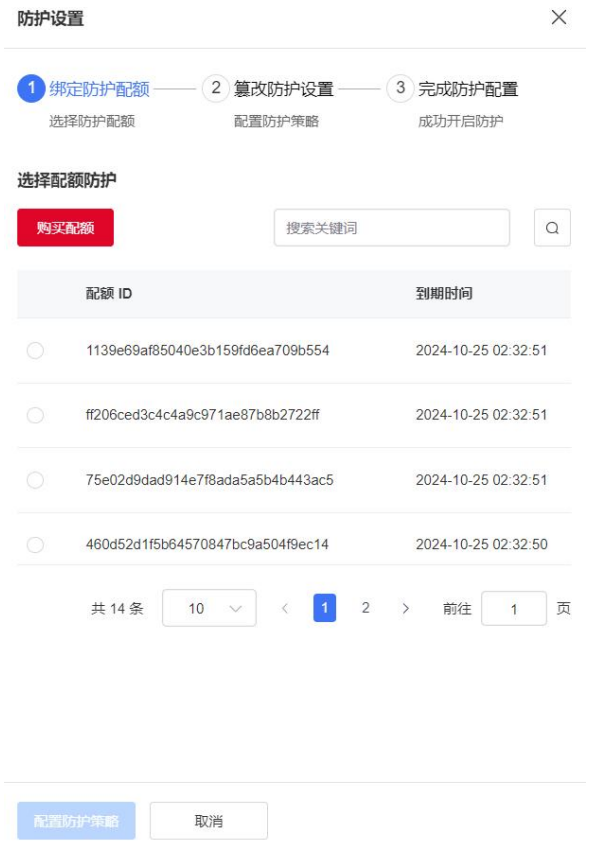
防护管理列表展示用户的服务器列表，包括服务器、操作系统、防护目录数、备份目录、防护配置状态、防护状态。

在防护管理页面，您可以为服务器开启网页防篡改防护，并配置防护目录。

防护设置

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）> 防护管理”，进入防护管理页面。

3. 在列表中选择要添加网页防篡改能力的服务器，单击操作列的“防护设置”，进入防护设置页面。



4. 绑定防护配额：选择需要绑定的配额后，单击“配置防护策略”。
5. 篡改防护设置：包括配置防护目录、设置特权进程、设置远端备份。
   - 配置防护目录：可对服务器的防护目录进行管理，包括添加、编辑、删除操作。
   - 设置特权进程：特权进程为您信任的进程文件，可以对防护目录文件进行修改操作。
   - 设置远端备份：启用远端服务器备份功能后，可有效避免备份在本地的文件被攻击者破坏后无法恢复。
6. 配置完成后，单击“完成防护配置”，回到服务器列表页面。

配置防护目录

分为添加白名单或添加黑名单两种模式，可根据实际使用场景进行配置。

- 白名单模式：会对添加的防护目录和文件类型进行保护。
- 黑名单模式：会防护目录下所有未排除的子目录、文件类型和指定文件。

说明：

- 一台服务器不能同时使用白名单模式和黑名单模式，建议您使用白名单模式。
- 每台服务器最多可添加 10 个防护目录；每个被防护的目录大小不超过 10GB；所有被防护的目录下的文件夹个数不超过 3000 个。

白名单模式

白名单模式添加防护目录、防护文件类型和本地备份目录，配置完成后，即开始对配置的文件进行防护。

黑名单模式

黑名单模式支持添加防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，配置完成后，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。

篡改防护设置

1 绑定防护配额 —— 2 篡改防护设置 —— 3 完成防护配置

选择防护配额　配置防护策略　成功开启防护

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、文件类型和指定件。每台服务器最多可添加 10 个防护目录；每个被防护的目录大小不超过 10 GB; 所有被防护的目录下的文件夹个数不超过 3000 个。

白名单模式　黑名单模式

* 防护目录　+添加

防护目录	防护文件类型	操作
/root/large	.log	编辑 | 删除

* 排除子目录　+添加

排除子目录	操作
/xxx	删除

* 排除指定文件　+添加

排除指定文件	操作
/pp	删除

* 本地备份目录　/root/bak

设置特权进程

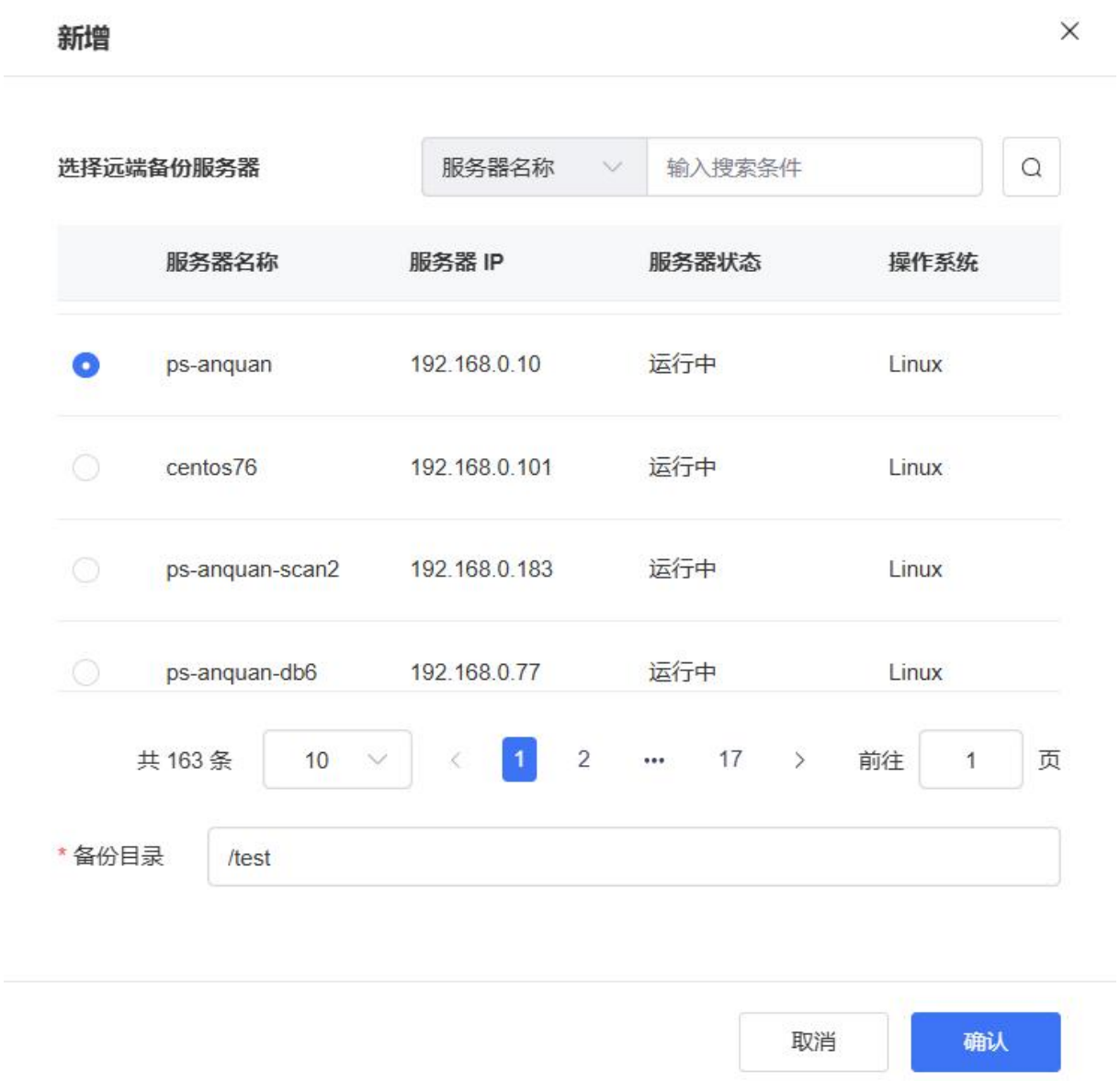
特权进程拥有对防护目录进行操作的权限，请确保特权进程安全可靠。

单击“添加”，弹出新增特权进程窗口，配置特权进程路径后，单击“确定”，完成特权进程配置。

设置远端备份

启用远端服务器备份功能后，可有效避免备份在本地的文件被攻击者破坏后无法恢复。

单击“添加”，在弹出的窗口中选择远端备份服务器、配置备份目录，单击“确认”，完成远端备份配置。



开启防护

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）>防护管理”，进入防护管理页面。
3. 单击防护状态开关，为服务器开启防护。

关闭防护

若您某台服务器不再需要网页防篡改防护，可以关闭防护。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）>防护管理”，进入防护管理页面。
3. 单击防护状态开关，为服务器关闭防护。

解绑配额

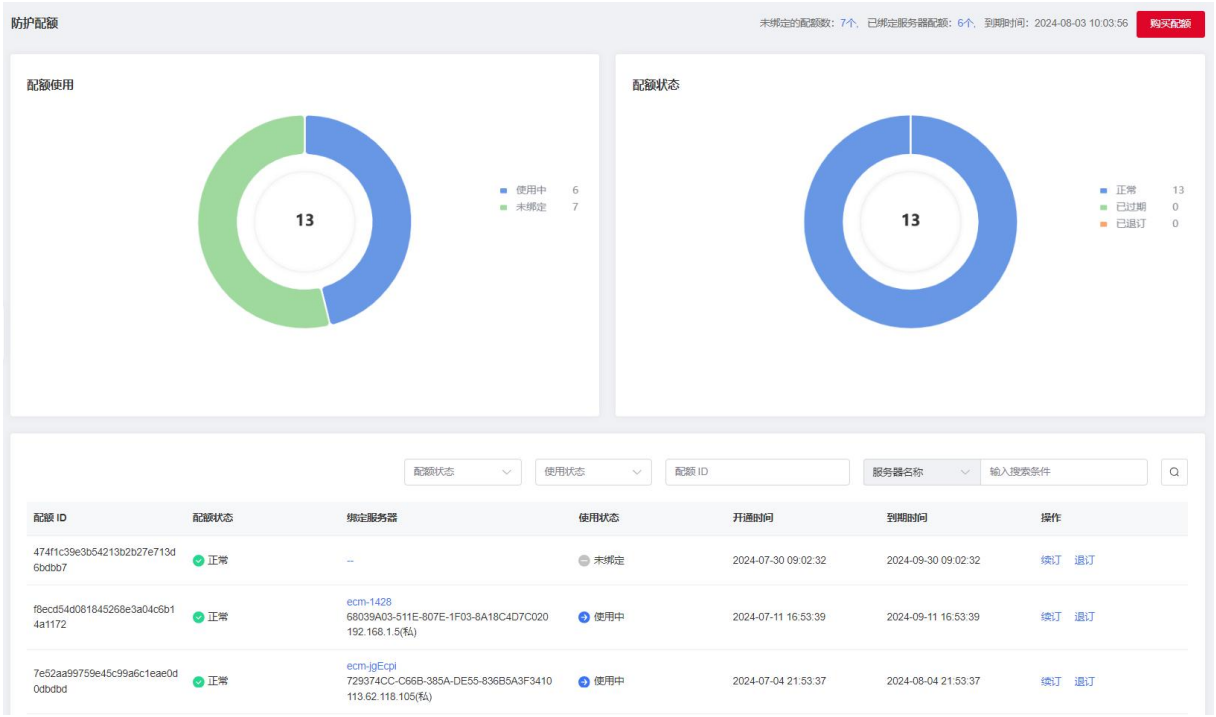
在关闭防护后，您可以解绑该服务器的防护配额，单击“解绑配额”。解绑后，您可以将该配额分配给其他服务器使用，为其他服务器提供防护。

4.7.4. 防护配额

查看配额详情

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）>防护配额”，进入防护配额页面。

该页面为您展示配额的统计和配额的详情列表。



- 配额使用：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：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、已过期、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。

管理配额

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

详细操作请参见“购买网页防篡改配额”。

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。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）>防护配额”，进入防护配额页面。
3. 在页面下方配额列表中，对需要续订的配额，单击操作列的“续订”。

4. 在“续订”页面选择该配额需续订的时长。

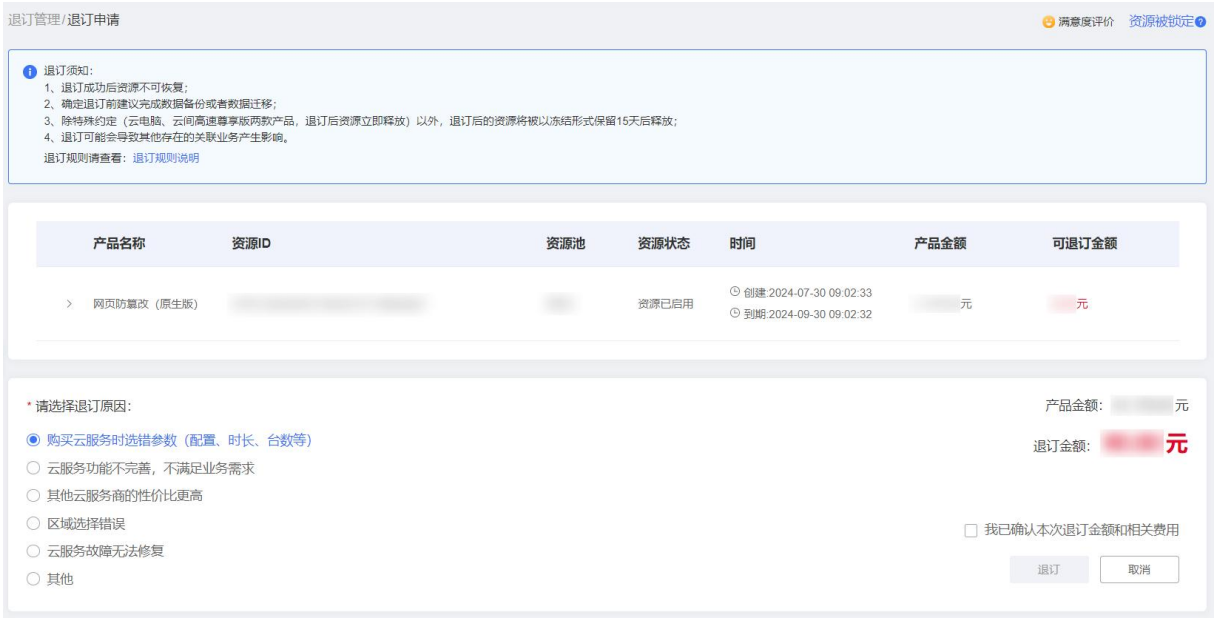
5. 阅读《天翼云网页防篡改（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云网页防篡改（原生版）服务协议》“，单击“立即购买”。
6. 进入“付款”页面，完成付款。

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。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）>防护配额”，进入防护配额页面。
3. 在页面下方配额列表中，对需要退订的配额，单击操作列的“退订”。

4. 进入退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。



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. 安全配置

安全配置用于统一管理和配置各防护模块的规则、白名单等。

修改防护状态

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 安全配置”，进入安全配置页面。
3. 找到目标防护模块，单击防护开关，开启/关闭防护。
   - 

：表示已开启防护。
   -

：表示已关闭防护。

配置防护规则

说明：
WebShell、文件安全功能仅企业版、旗舰版支持配置。
端口蜜罐、勒索诱饵防护、文件完整性保护仅旗舰版支持配置。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 安全配置”，进入安全配置页面。
3. 找到目标防护模块，单击配置按钮，进入相应规则配置页面。
4. 根据具体防护模块对规则进行配置。

4.8.2. 配额管理

在配额管理页面，可以查看并管理服务器安全卫士（原生版）主机防护的配额。

查看配额统计情况

- 配额使用统计：展示配额状态为“正常”的配额的使用情况，分使用中和未绑定 2 种情况。
- 配额状态统计：包括正常、已过期和已退订 3 种情况。
- 配额版本统计：展示已购买的企业版和旗舰版配额数量。

查看配额列表

页面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、配额开通时间、配额到期时间。

该列表可以根据配额状态、使用状态、配额版本、配额 ID、服务器名称和服务器 IP 进行查询。

4.8.3. 同步资产设置

系统默认每天 01:00 自动同步服务器资产信息，您可以根据需要修改同步周期，同步周期支持 12 小时和 24 小时。

设置自动同步资产周期

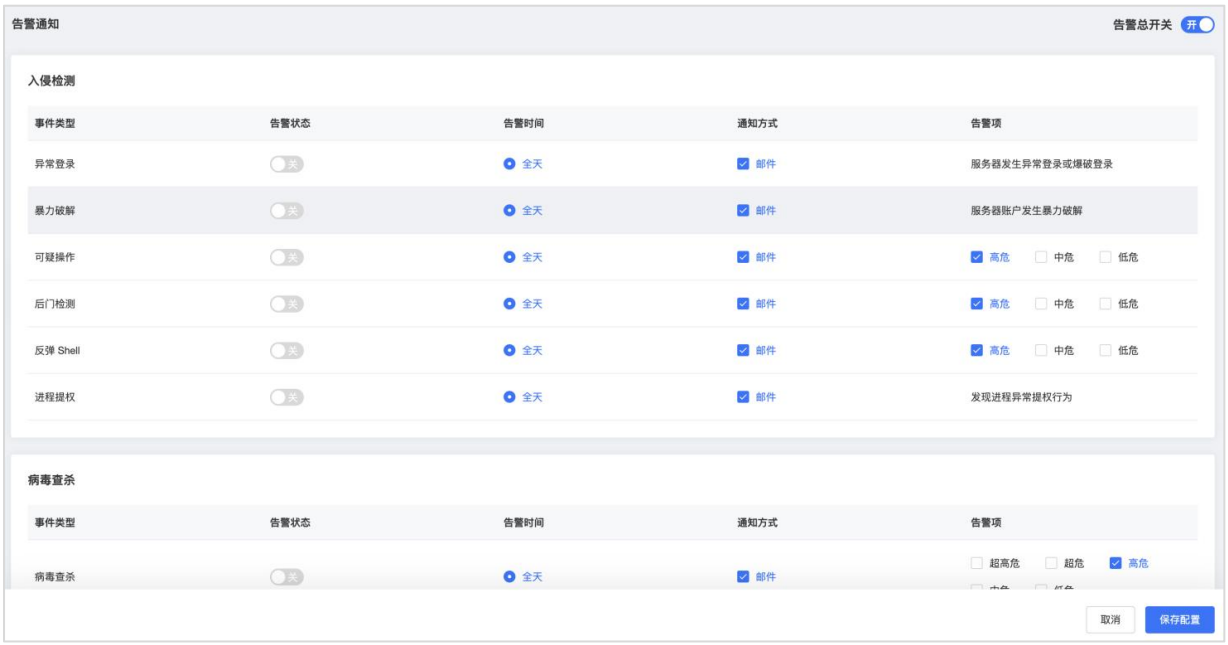
1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 同步资产设置”，进入同步资产设置页面。

3. 选择自动同步资产周期。
   - 12 小时：每天 01:00、13:00 自动同步服务器资产信息。
   - 24 小时：每天 01:00 自动同步服务器资产信息。

4.8.4. 告警通知

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏选择“设置中心 > 告警通知”，进入告警通知页面。



3. 根据您的使用场景进行告警通知配置。

配置项	说明
告警开关	自定义开启需要通知的事件类型。
告警时间	事件发生时实时发送告警通知。
通知方式	通过邮件方式发送告警通知。
告警项	根据威胁等级自定义发送通知。

4. 配置完成后单击“保存配置”，界面弹出“保存告警设置成功”提示信息，则说明告警通知配置成功。

4.8.5. 报表管理

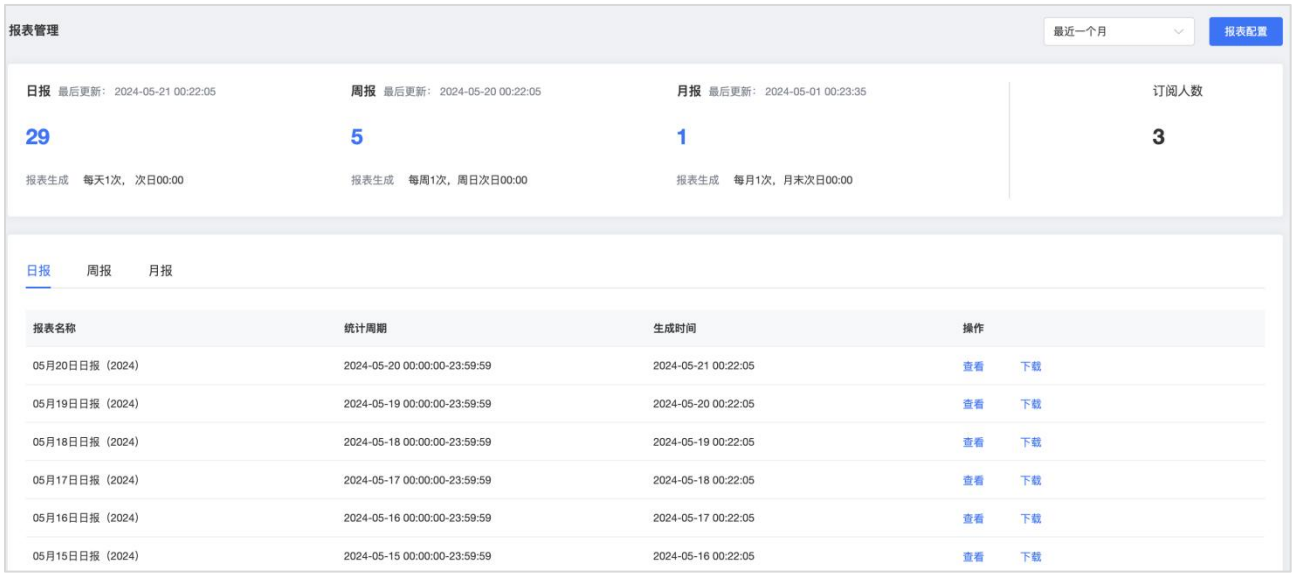
登录服务器安全卫士（原生版）控制台，在左侧导航栏选择“设置中心 > 报表管理”。

约束限制

免费版仅支持订阅周报，企业版、旗舰版支持订阅日报、周报、月报。

报表统计

按时间筛选条件统计已生成的日报、周报、月报数，方便用户查找安全报表，分析主机风险情况。



创建报表

根据您的使用场景进行报表配置，配置完成后周期性自动生成安全报表并发送至订阅邮箱。

报表类型	日报	周报	月报
统计周期	每天 00:00:00-23:59:59	每周一 00:00:00 至周日 23:59:59	每月 1 号 00:00:00 至当月最后一天 23:59:59
发送时间	每天 1 次，次日 00:00	每周 1 次，周日次日 00:00	每月 1 次，月末次日 00:00
报表订阅	设置安全报表订阅账户，发送报告至订阅邮箱		
保存时间	报表默认保存 180 天，请及时下载保存		

管理报表

报表管理页面生成安全报表后，提供安全报表查看和下载能力。

4.9. 权限管理

服务器安全卫士（原生版）通过 IAM（统一身份认证服务，Identity and Access Management）对用户权限进行管理，IAM 可以帮助用户安全地控制服务器安全卫士（原生版）服务的访问及操作权限。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的 IAM 用户没有任何权限。IAM 用户需要加入用户组，并给用户组授权相应策略后，IAM 用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

4.9.1. IAM 应用场景

IAM 策略主要面向同一主账号下，对不同 IAM 用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同 IAM 用户，并授予 IAM 用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。
- 新创建的 IAM 用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

4.9.2. IAM 策略说明

天翼云为服务器安全卫士（原生版）提供如下系统策略。如果系统策略不满足授权要求，可以创建自定义策略。

策略名称	策略描述	类别	授权范围
ctcsscn admin	服务器安全卫士所有权限。	系统策略	全局级
ctcsscn viewer	服务器安全卫士只读权限。	系统策略	全局级

4.9.3. 通过 IAM 授权使用服务器安全卫士（原生版）

以下步骤，以仅授予用户“ctcsscn admin”策略为例，实现用户只能访问、管理服务器安全卫士（原生版）服务，无法访问其他云服务的权限管理目标。

步骤一：创建用户组并授权

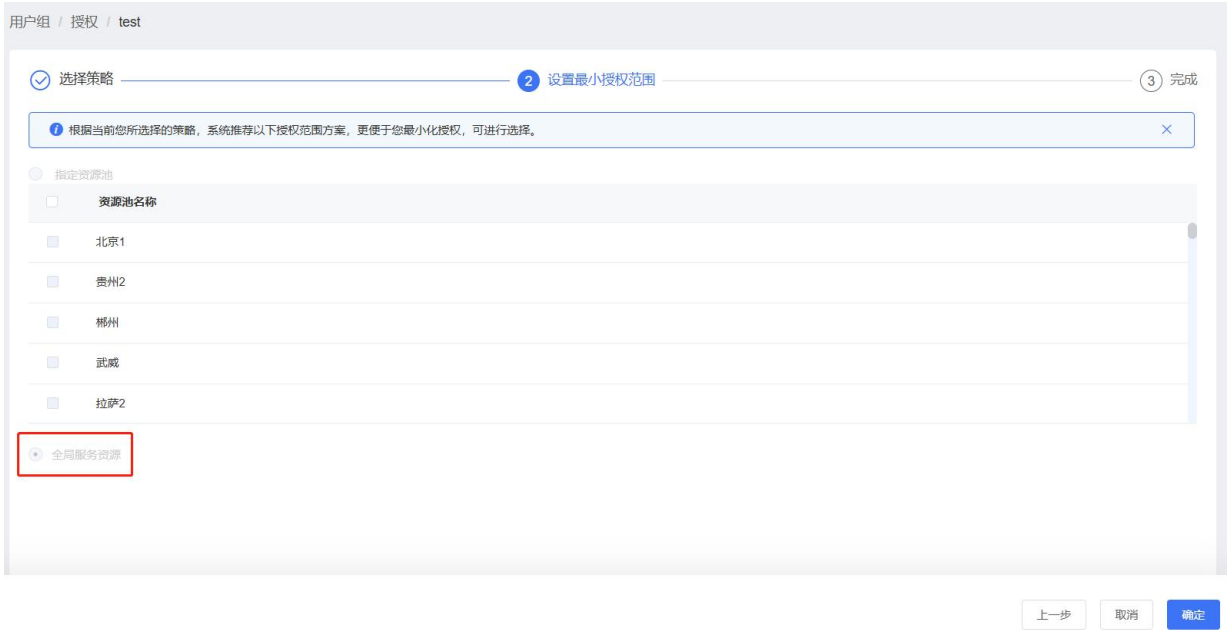
用户组是用户的集合，IAM 通过用户组功能实现用户的授权。

1. 使用主账号登录天翼云控制台，在右上角单击头像选择“账号中心”，在左侧导航中选择“统一身份认证”，或者直接点击 IAM 控制台。
2. 在左侧导航栏，选择“用户组”，单击右上角的“创建用户组”。
3. 在“创建用户组”界面，输入用户组名称和描述。

4. 单击“确定”，完成用户组创建。用户组列表中显示新创建的用户组。
5. 在用户组列表中，单击新建的用户组右侧的“授权”。

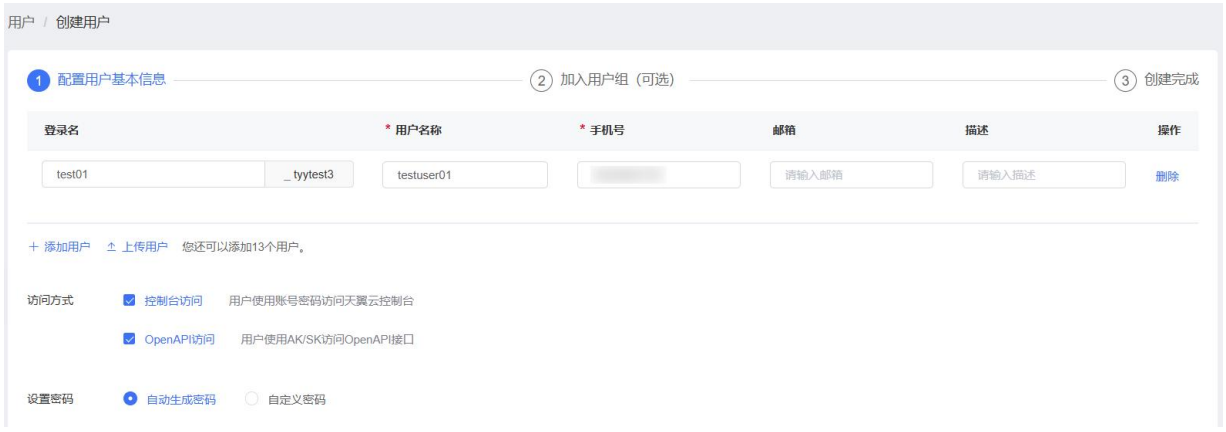
6. 选择策略：以仅授予用户“ctcsscn admin”权限为例。在右上角“请输入策略名称进行搜索”框内输入策略名称进行搜索，勾选需要授予用户组的全局策略“ctcsscn admin”，单击“下一步”。

7. 设置授权范围：由于上一步选择的系统策略，作用范围为全局，因此在设置授权范围时，默认勾选了“全局”选项。单击“确定”完成授权。



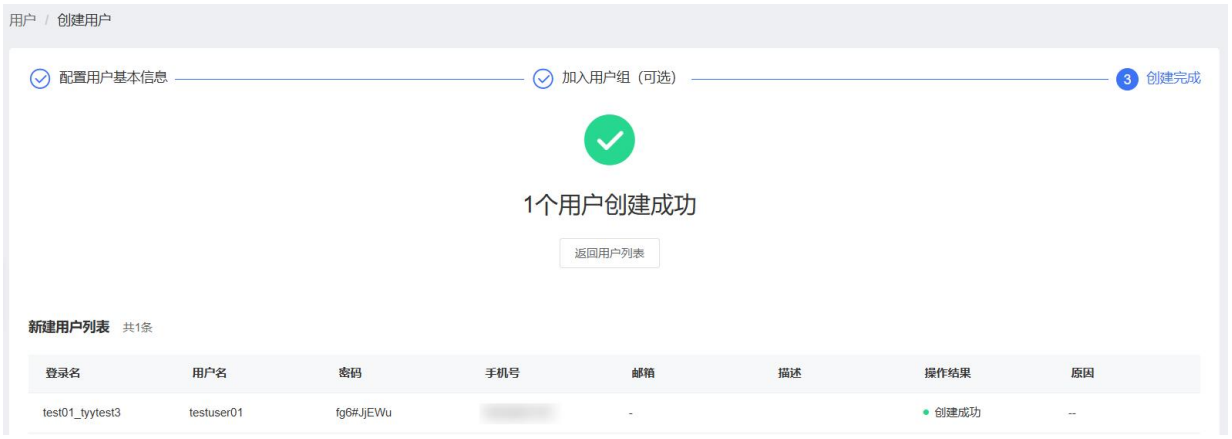
步骤二：创建 IAM 用户并加入用户组

1. 在统一身份认证服务左侧导航栏，选择“用户”，单击右上角“创建用户”。
2. 配置用户基本信息：在“创建用户”界面填写“用户基本信息”，单击“下一步”。
3. 如需一次创建多个用户，可以单击“添加用户”添加多个用户，或单击“上传用户”进行批量创建。



4. 加入用户组：在左侧可选用户组列表中找到刚创建的用户组，单击操作列的“添加”将用户加入到该用户组。

5. 单击“下一步”，等待 IAM 用户创建完成。记录新建的 IAM 用户的登录名和密码。



步骤三：使用创建的 IAM 用户登录并验证权限

完成 IAM 用户创建后，即可以使用登录名和密码登录天翼云，验证权限（当前用户权限仅包含“ctcsscn admin”权限）。

1. 使用新创建的 IAM 用户登录天翼云控制中心。
2. 在登录页面，输入 IAM 用户的登录名及密码。如果登录失败，IAM 用户可以联系主账号重置密码。

3. 执行以下操作，若满足预期结果，表示“ctcsscn admin”权限已生效。

- 在产品服务列表中选择“服务器安全卫士（原生版）”，成功进入服务器安全卫士（原生版）控制台。

- 在产品服务列表中选择除“服务器安全卫士（原生版）”之外的其他服务，提示权限不足。

5. 最佳实践

5.1. 主机安全防护最佳实践

服务器安全卫士（原生版）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。

使用指引

服务器安全卫士（原生版）提供基础版、企业版、旗舰版供用户选择，不同版本差异请参见产品规格。

5.1.1. 基础版防护

若您使用基础版进行防护，使用流程如下：

流程	相关文档	说明
步骤一：开通服务	开通服务器安全卫士（原生版）	用户需开通服务，才能使用基础版（免费）对云主机进行防护。
步骤二：接入防护	查看防护状态	开通服务后，需要在服务器列表页面确认云主机资产的防护状态，确保所有待防护的云主机已开启防护，且 Agent 状态为“在线”，防护状态为“防护中”。
步骤三：防护配置	• 配置入侵检测：配置异常登录白名单 • 开启定时漏洞扫描	当云主机接入防护后，用户可以根据业务需求进行防护配置。 其中入侵检测已默认开启防护，无特殊需求，无需再手动配置。避免异常登录误报，建议将常用登录 IP、登录用户名、登录地区、登录时间等添加到白名单。 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，您需购买并使用企业版或旗舰版进行防护。
步骤四：通知设置	开启告警通知	开启告警通知后，当检测到资产存在风险时，会根据您配置的告警策略，向您发送告警通知，帮助您及时了解资产的安全情况。
步骤五：报表配置	订阅报表	服务器安全卫士（原生版）基础版仅支持订阅周报，订阅后系统会在

流程	相关文档	说明
		周报生成后将周报发送至您的邮箱。 说明 基础版只支持订阅周报，若需要订阅日报、月报，您需购买并使用企业版、旗舰版。

5.1.2. 企业版防护

若基础版不满足业务需求，可以购买企业版配额，然后将防护版本切换为企业版防护，使用流程如下：

流程	相关文档	说明
步骤一：开通服务	开通服务器安全卫士（原生版）	用户需开通服务，才能使用服务器安全卫士（原生版）对云主机进行防护。
步骤二：接入防护	● 查看防护状态 ● 购买防护配额 ● 切换版本	● 开通服务后，需要在服务器列表页面确认云主机资产的防护状态，确保所有待防护的云主机已开启防护，且 Agent 状态为“在线”，防护状态为“防护中”。 ● 购买企业版配额并切换防护版本为企业版后，才能正常使用企业版对云主机进行防护。
步骤三：防护配置	● 配置入侵检测：配置异常登录白名单 ● 开启定时漏洞扫描 ● 配置基线检测策略 ● 开启弱口令定时检测 ● 开启定时扫描病毒	当云主机接入防护后，用户还需要根据业务需求进行防护配置。 其中入侵检测已默认开启防护，无特殊需求，无需再手动配置。避免异常登录误报，建议将常用登录 IP、登录用户名、登录地区、登录时间等添加到白名单。
步骤四：通知设置	开启告警通知	开启告警通知后，当检测到资产存在风险时，会根据您配置的告警策略，向您发送告警通知，帮助您及时了解资产的安全情况。
步骤五：报表配置	订阅报表	服务器安全卫士（原生版）支持生成日报、周报、月报，并支持订阅报表，订阅后系统会在报表生成后将报表发送至您的邮箱。

5.1.3. 旗舰版防护

若基础版、企业版不满足业务需求，可以购买旗舰版配额，然后将防护版本切换为旗舰版防护，使用流程如下：

流程	相关文档	说明
步骤一：开通服务	开通服务器安全卫士（原生版）	用户需开通服务，才能使用服务器安全卫士（原生版）对云主机进行防护。
步骤二：接入防护	• 查看防护状态 • 购买防护配额 • 切换版本	• 开通服务后，需要在服务器列表页面确认云主机资产的防护状态，确保所有待防护的云主机已开启防护，且 Agent 状态为“在线”，防护状态为“防护中”。 • 购买旗舰版配额并切换防护版本为旗舰版后，才能正常使用旗舰版对云主机进行防护。
步骤三：防护配置	• 配置入侵检测：配置异常登录白名单 • 开启定时漏洞扫描 • 配置基线检测策略 • 开启弱口令定时检测 • 开启定时扫描病毒 • 设置文件完整性保护检测规则 • 配置文件防勒索	当云主机接入防护后，用户还需要根据业务需求进行防护配置。 其中入侵检测已默认开启防护，无特殊需求，无需再手动配置。避免异常登录误报，建议将常用登录 IP、登录用户名、登录地区、登录时间等添加到白名单。
步骤四：通知设置	开启告警通知	开启告警通知后，当检测到资产存在风险时，会根据您配置的告警策略，向您发送告警通知，帮助您及时了解资产的安全情况。
步骤五：报表配置	订阅报表	服务器安全卫士（原生版）支持生成日报、周报、月报，并支持订阅报表，订阅后系统会在报表生成后将报表发送至您的邮箱。

5.2. 云上勒索病毒防护实践

5.2.1. 勒索攻击介绍

勒索软件是当前主要网络攻击威胁，一般通过木马病毒的形式传播，将自身掩盖为看似无害的文件，利用钓鱼邮件或软件漏洞等方式进行攻击，攻击后将受害者主机硬盘上的文件进行加密，以此来达到勒索的目的。所有的勒索软件都会要求受害者缴纳赎金以取回对电脑的控制权，或是取回受害者根本无从自行获取的解密密钥以便解密文件，对全球的政府、金融、医疗等各行业都造成了严重损失。

勒索攻击阶段

- 准备阶段：感染准备阶段，包括最初攻击阶段的漏洞利用信息，以及勒索软件自身模块释放之后对环境系统及应用终止，还包括勒索病毒在内网环境的自我扩散等。
- 感染阶段：遍历文件加密阶段，勒索病毒在入侵之后会遍历系统文件，如果有高价值数据、文件，则进入加密环节，完成勒索前重要一步。
- 勒索阶段：弹窗勒索环节，该阶段是勒索病毒的最终下发环节，意味着数据、文件已经被加密，企业如不支付赎金，数据、文件将处于不可用状态。

常见攻击手法

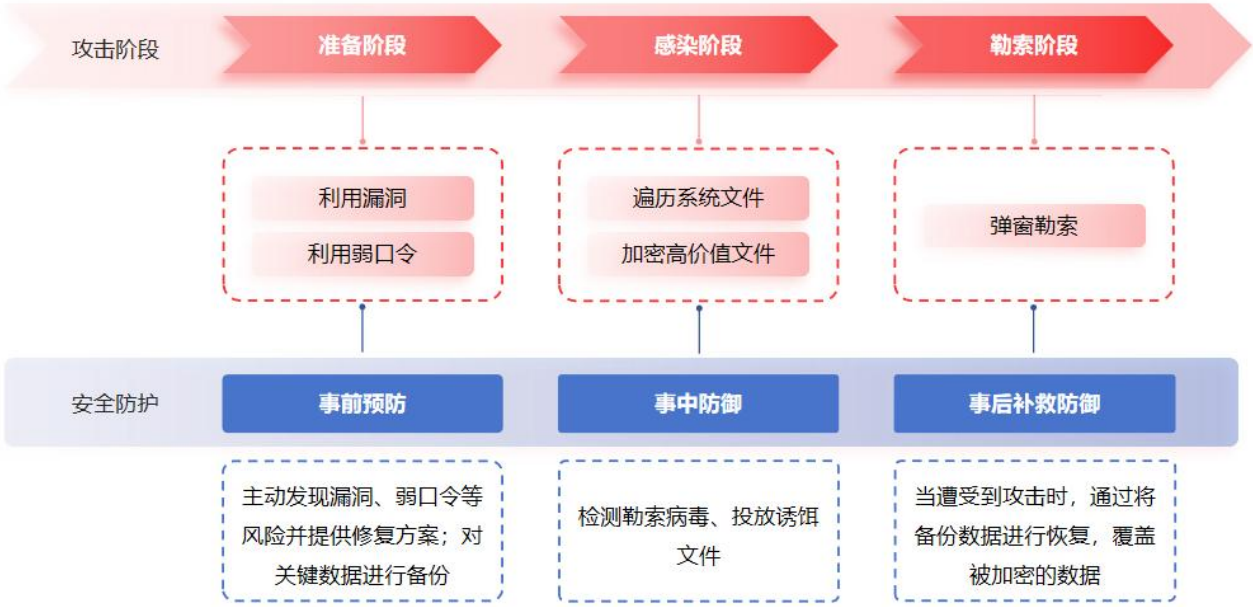
- 暴力破解：对密码进行破解的行为，破解成功登录主机后，便可获得主机的控制权限。
- 漏洞利用：利用系统或者第三方软件存在的已知或未知漏洞实施攻击。
- 钓鱼邮件：发送钓鱼邮件，将恶意脚本/程序掩盖为普通的文件，欺骗受害者下载、运行。

常见风险暴露

- 高危端口暴露：系统暴露高危端口，攻击事件涉及端口暴露最多的如：3389、445、135、139、3306、5800、5900 等。
- 系统存在弱口令：系统或应用密码复杂度低，未定期更新密码，使用统一的密码等，能够被攻击者成功爆破。
- 高危漏洞未修复：系统或者第三方软件存在漏洞，勒索软件利用已知的漏洞实施攻击。
- 社工钓鱼：发送伪装的电子邮件引诱用户下载恶意程序或访问恶意 URL 链接。

5.2.2. 防勒索方案

方案架构



方案防护措施

- 事前预防
  - 提供漏洞检测能力：主动发现系统、应用、数据库等存在的漏洞风险，并支持一键漏洞修复，避免被攻击者利用。
  - 提供基线检查能力：一键核查服务器、数据库等的安全合规配置，如弱口令、配置文件等，消除部分安全隐患。
  - 提供数据备份能力：对关键数据采取实时备份/定时备份等方式对数据进行备份，在被勒索后，可以对备份数据一键恢复，减少损失。
- 事中防御
  - 提供入侵检测和病毒查杀能力：在网络层面阻断勒索病毒的下载传播，在主机层面识别、阻断和隔离勒索病毒，实现对已知勒索病毒的防御。
  - 提供诱饵防护能力（旗舰版功能）：利用投放在关键位置的诱饵文档，实时监控诱饵文档的改动，一旦单位时间内多个诱饵文件连续发生改动，立即产生报警，终止修改诱饵文件的进程，并隔离进程对应的文件，实现对未知勒索病毒的检测和查杀能力。
- 事后补救防御

提供数据恢复能力：遭遇黑客攻击、人为删除等恶性事件时，将备份的特定时间节点数据进行数据恢复，覆盖被加密或损坏的数据。

5.2.3. 防护措施

5.2.3.1. 事前预防措施

提升员工安全意识

- 禁止随便点击邮件中的不明附件或快捷方式，网站链接等。
- 禁止从来历不明的网站下载的一些文档。
- 重要文件或信息（如密码口令等）需要加密，防止泄露。

重要文件定期备份

- 用户自行对重要文档数据与数据库文件做备份。
- 使用备份产品对主机、硬盘、文件目录或数据库进行备份。

定期系统安全巡检

对可疑文件/进程或应用进行清理，如后缀名异常文件、来源不明的应用等。

系统/软件即时更新补丁

及时修复系统漏洞，定期更新。

上线前进行主机安全加固

- 关闭不必要的端口，减少暴露面。
- 关闭不必要的网络访问，减少暴露面。
- 系统安全配置检查：核查系统配置，如设置密码策略、设置用户锁定策略、禁用 Guest 账户、限制匿名用户连接等。

不设置弱密码

设置复杂口令：

- 长度为 8～26 个字符；包含大小写字母、数字及符号 3 种。
- 不能包含与账号名相关的信息。
- 不能使用连续 3 个及以上键位排序字符，如 123，Qwe。
- 不能使用常用的具有特殊含义的字符串等。

5.2.3.2. 检测并修复风险入口

弱口令、基线风险、漏洞常被攻击者利用然后入侵服务器，提前识别并修复相关风险可降低服务器被入侵的风险。

服务器安全卫士（原生版）提供弱口令检测、基线检测、漏洞扫描功能，可以快速识别出服务器上存在的风险。

检测并修复弱口令

检测弱口令：您可以根据需要开启定时弱口令检测、或执行一键检测。弱口令检测支持对系统弱口令和应用弱口令进行检测。

修复弱口令：您可以根据检测出的弱口令对应的服务器、用户名等信息，修复弱口令。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 弱口令检测”，进入弱口令检测页面。
3. 在弱口令检测页面查看当前存在的弱口令。页面下方展示最新一次检测完成的弱口令列表，分别按系统弱口令和应用弱口令进行展示。

   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。
4. 根据检测出的弱口令对应的服务器、用户名等信息，登录服务器修改弱口令。

   弱口令修复完成后，建议您立即重新执行弱口令检测，验证修复结果。

检测并修复基线风险

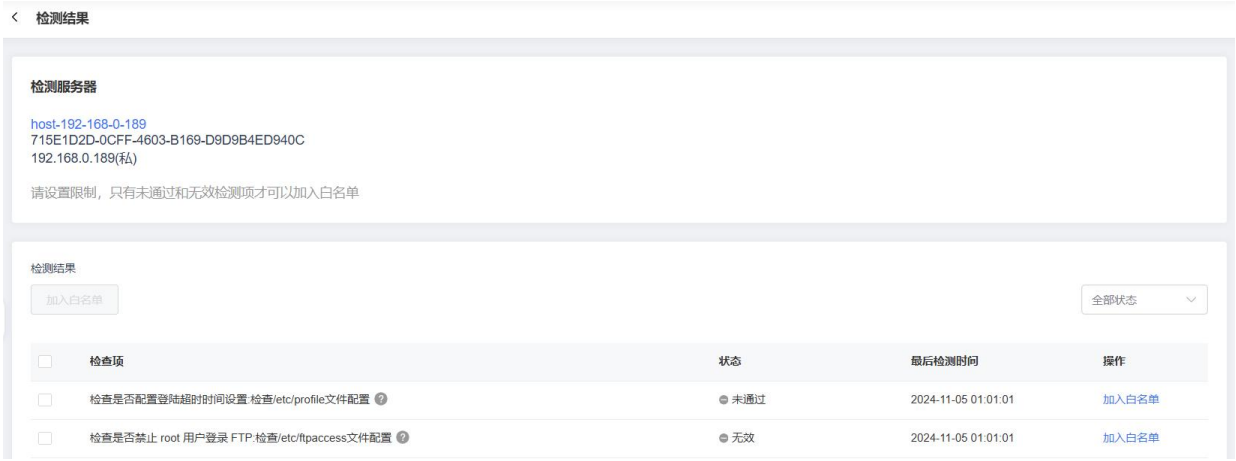
检测基线风险：您可以根据需要新建基线检测策略进行定时检测、或执行一键检测。详细操作请参见基线检测。

修复基线风险：您可以根据基线检测结果，找到有风险的配置，根据给出的修复建议对配置信息进行调整。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
3. 单击基线列表操作列的“详情”，跳转到基线检测详情页面。

4. 单击基线检测详情页操作列中的“详情”，可以查看该基线名称下该台服务器的检测详情。

5. 查看各检测项，通过检测项右侧的问号可以查看修复建议。



6. 登录检测服务器，根据修复建议修改相应的配置。
7. 修复完成后，建议您立即重新执行基线检测，验证修复结果。

扫描并修复漏洞

扫描漏洞：您可以根据需要配置定时自动扫描漏洞、或执行一键手动扫描漏洞。

修复漏洞：漏洞扫描完成后，可以在漏洞扫描页面查看服务器中存在的漏洞信息，如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。

说明：

- 购买企业版或旗舰版后，才支持一键自动修复漏洞。
- Windows 漏洞暂不支持一键修复，请手动修复相关漏洞。

一键自动修复

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 勾选漏洞列表中所有需要修复的漏洞，单击漏洞列表左上角的“批量修复”，一键批量修复漏洞。
4. 在修复对话框中，确认待修复的漏洞数量和影响资产数量、选择修复所需软件源。

   您可以在修复对话框中查看修复命令、查看影响服务器数量。软件源支持清华软件源、华为云软件源、阿里云软件源，也可以自配置软件源。若选择自配置软件源，请务必确认已在服务器上配置好对应操作系统发行版的软件源（如 yum、zypper、apt-get 或 emerge 等包管理工具对应的软件源）。
5. 单击“确定”，开始自动修复漏洞。
6. 修复完成后，建议您立即重新扫描漏洞，验证修复结果。

手动修复漏洞

您可以参考漏洞详情页面的修复建议，登录服务器手动修复漏洞。

说明：

- 漏洞修复完成后需要手动重启服务器，否则系统仍可能为您推送漏洞消息。
- 不同的漏洞请根据修复建议依次进行修复。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“风险管理 > 漏洞扫描”，进入漏洞扫描页面。
3. 单击“漏洞名称”链接、或操作列的“查看详情”，跳转至漏洞详情页面。

4. 在漏洞详情页面可以看到漏洞修复建议。

5. 登录漏洞影响的服务器，根据修复建议进行修复。

6. 修复完成后，建议您立即重新扫描漏洞，验证修复结果。

5.2.3.3. 开启勒索防护并处理勒索告警

若能及时识别并隔离勒索攻击，将能大大降低被攻击的概率。服务器安全卫士（原生版）通过在关键位置投放诱饵文件，实时监控诱饵文件的改动，一旦单位时间内多个诱饵文件连续发生改动，立即产生报警，终止修改诱饵文件的进程，并隔离进程对应的文件，实现对未知勒索病毒的检测和查杀能力。

通过启用诱饵防护和勒索备份，可以增加勒索防护能力，从而降低业务受损风险。

启用诱饵防护

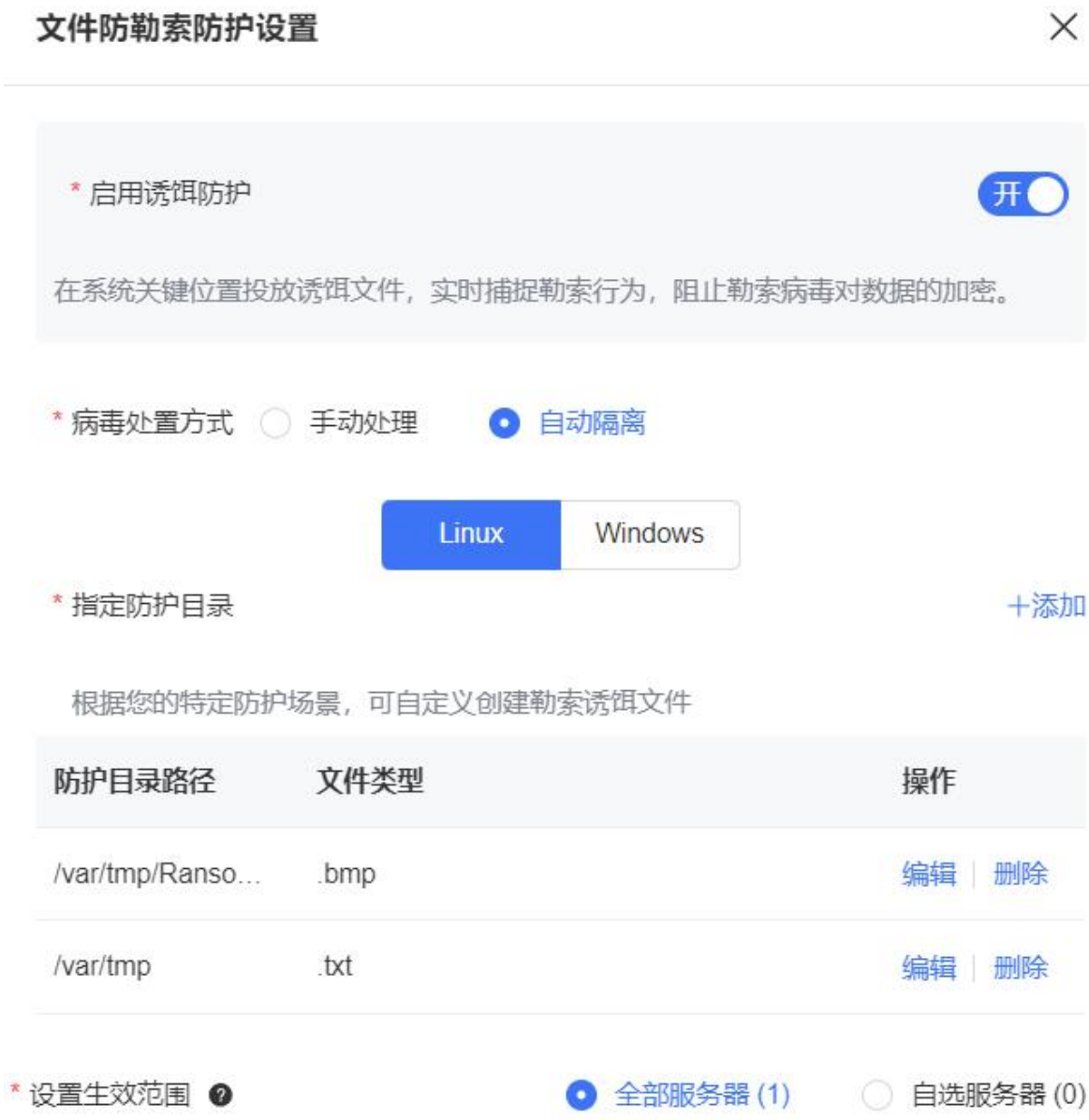
您可以根据业务需求，配置诱饵文件防护目录。

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。

3. 单击诱饵防护模块的“设置”按钮。

4. 在页面右侧弹出的防护设置页面，配置防护参数。



参数说明：

参数	说明
启用诱饵防护	自动在系统关键位置投放诱饵文件，实时捕捉勒索行为并进行阻断。
病毒处置方式	支持手动处理和自动隔离。 ● 手动处理：检测出勒索病毒文件后，仅产生告警。需手动在控制中心对勒索告警进行处理，支持隔离、删除、信任。 ● 自动隔离：检测出勒索病毒文件后产生告警，并自动隔离病毒文件。

参数	说明
	说明： 自动隔离后，若出现误报，可在告警列表中对文件进行恢复。
指定防护目录	根据用户的特定防护场景，可自定义创建勒索诱饵文件。
生效范围	自定义选择需要开启诱饵防护的服务器。

5. 配置完成后，单击“确认”。

开启勒索备份

为了避免被勒索后数据丢失，请为服务器开启勒索备份，定期备份数据。

说明：
数据备份/恢复属于增值服务，如果您未购买存储库，请先购买备份存储库后再开启勒索备份。

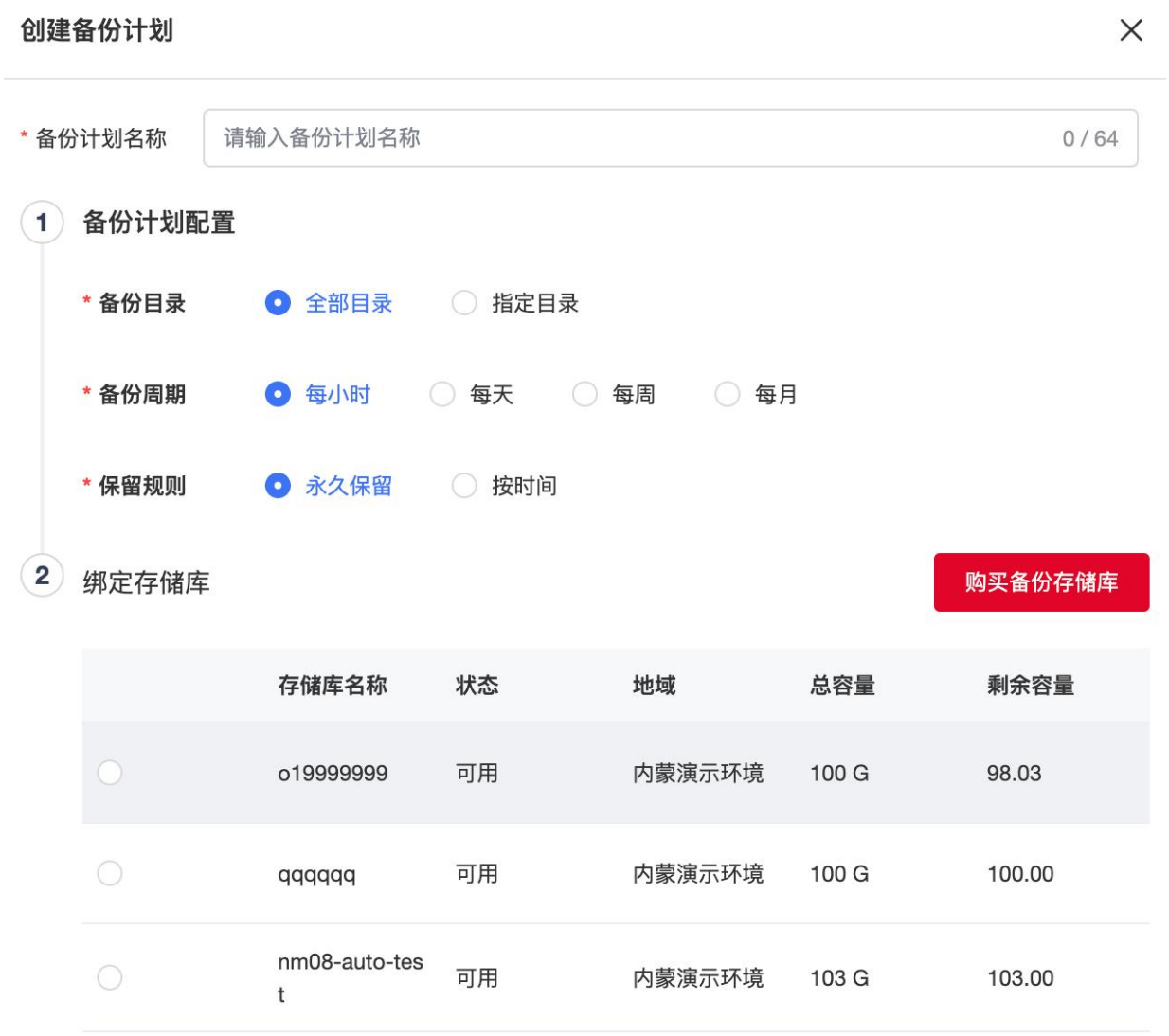
1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 安装备份 Agent。

   在“备份与恢复”页面，选择需要进行数据备份的服务器，单击操作列的“安装备份 Agent”，Agent 状态为“已激活”则安装成功。

4. 创建备份计划。

   在“备份与恢复”页面，选择需要进行数据备份的服务器，单击操作列的“备份计划”，按照设置的策略进行周期性数据备份。

- 备份目录：可指定全部目录或自定义目录进行数据备份。
- 备份周期：可选择每小时、每天、每周或每月设置备份周期。
- 保留规则：可设置备份计划生效时间，支持永久保留和自定义设置时间。
- 绑定存储库：选择一个可用状态的存储库，备份数据大小应小于存储库剩余容量。



处理勒索告警

启用诱饵防护后，请及时处置勒索告警事件，及时发现并隔离阻断勒索病毒运行、扩散。

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。
3. 在“勒索告警”页签，查看勒索攻击告警。

您可以根据告警信息排查主机上是否存在勒索软件。

- 在列表中可以看到告警服务器、告警详情、诱饵文件路径、操作类型、发生时间、处理方式、状态。

- 展开告警，可以查看告警详细信息，包括进程启动命令行、父进程文件路径、父进程 ID、父进程启动命令行。

4. 在告警列表的操作列，选择告警处理方式。

   提供如下处理方式：

   - 隔离：手动隔离病毒文件，文件隔离成功后将移动至隔离区并加密，无法再对服务器造成威胁。
   - 取消隔离：对已隔离的文件，如用户有恢复需求，可恢复原始文件。
   - 信任：经分析后确认为误报，可以选择将文件进行信任，信任后将不再对该文件进行检测告警。
   - 删除：手动删除病毒文件，文件被删除后无法进行恢复，请谨慎进行操作。

5.2.3.4. 恢复备份数据

由于安全的相对性和复杂性，任何工具都不能保障您的服务器 100%避免勒索攻击。若服务器不幸遭遇了勒索攻击，通过恢复之前备份的数据，覆盖被加密或损坏的数据，可以将损失降低。

操作步骤

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“文件安全 > 文件防勒索”，进入文件防勒索页面。

3. 在“备份与恢复”页面，选择已进行数据备份的服务器，单击操作列的“历史备份”。

4. 在“历史备份”页面，查看备份副本。

   备份副本是按用户创建的备份计划自动生成的备份数据。

5. 选择需要恢复的备份副本，单击操作列的“恢复”，对数据进行恢复。

   备份数据支持恢复到原目录或指定目录。

6. 在“恢复任务”页签，可以查看恢复任务的状态及详情。当执行状态为“任务完成”时，表示恢复任务执行成功。

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：

- 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。
- 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。

- 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

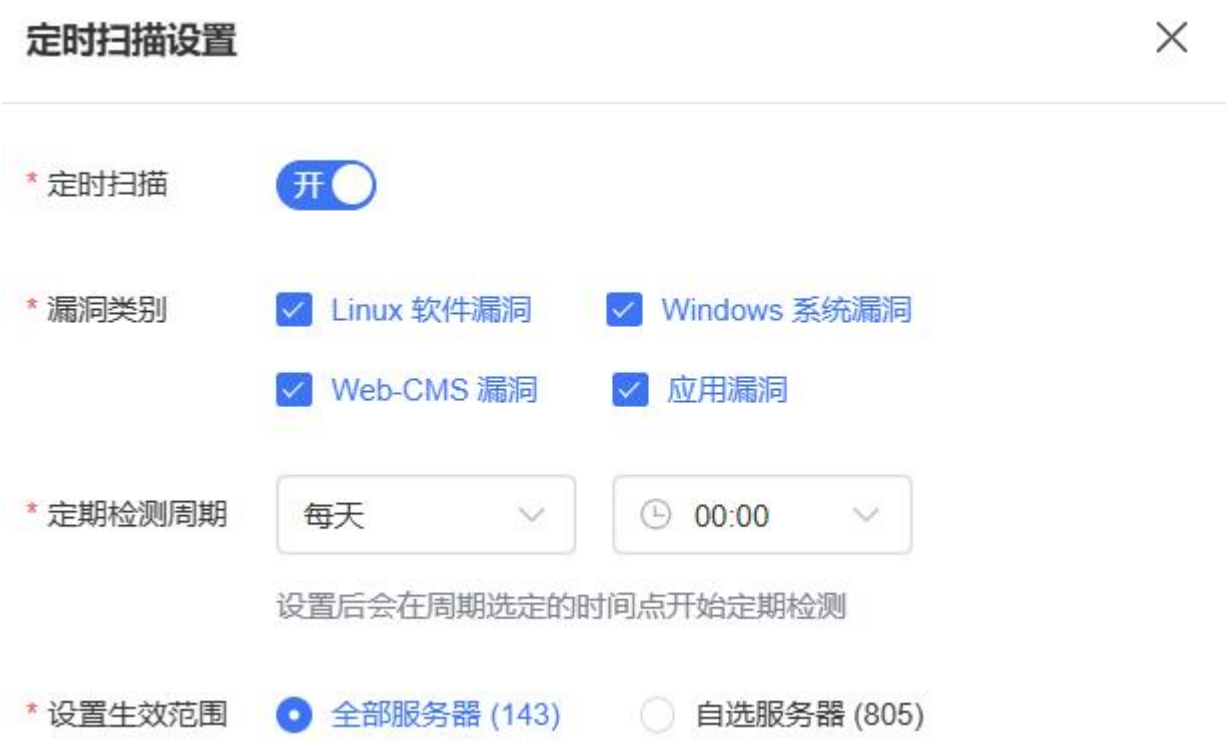
漏洞扫描支持定期扫描和立即扫描，同一时间只支持 1 个漏洞扫描任务。

- 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。

1、定期扫描

支持按每天，每 3 天，每 7 天指定时间执行漏洞扫描任务，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。



2、立即扫描

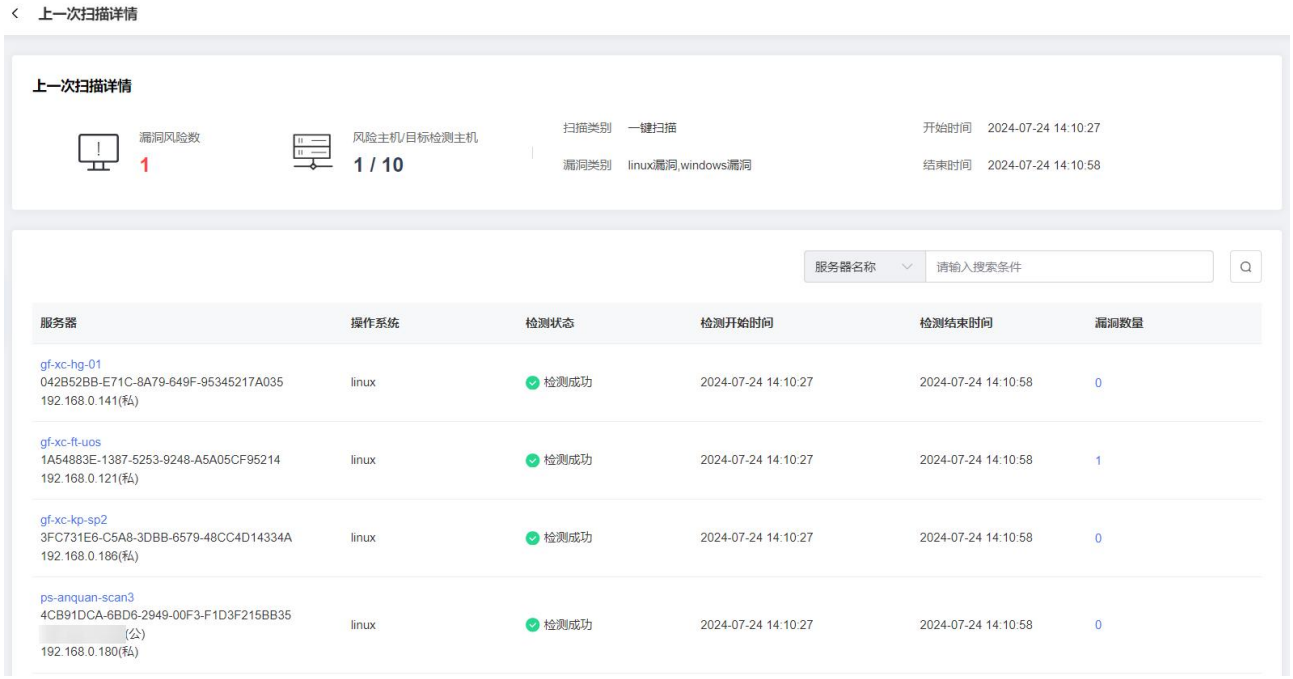
根据您的需求随时下发漏洞扫描任务，可点击一键扫描按钮，进行漏洞扫描设置，立即下发漏洞扫描任务。

查看漏洞扫描结果

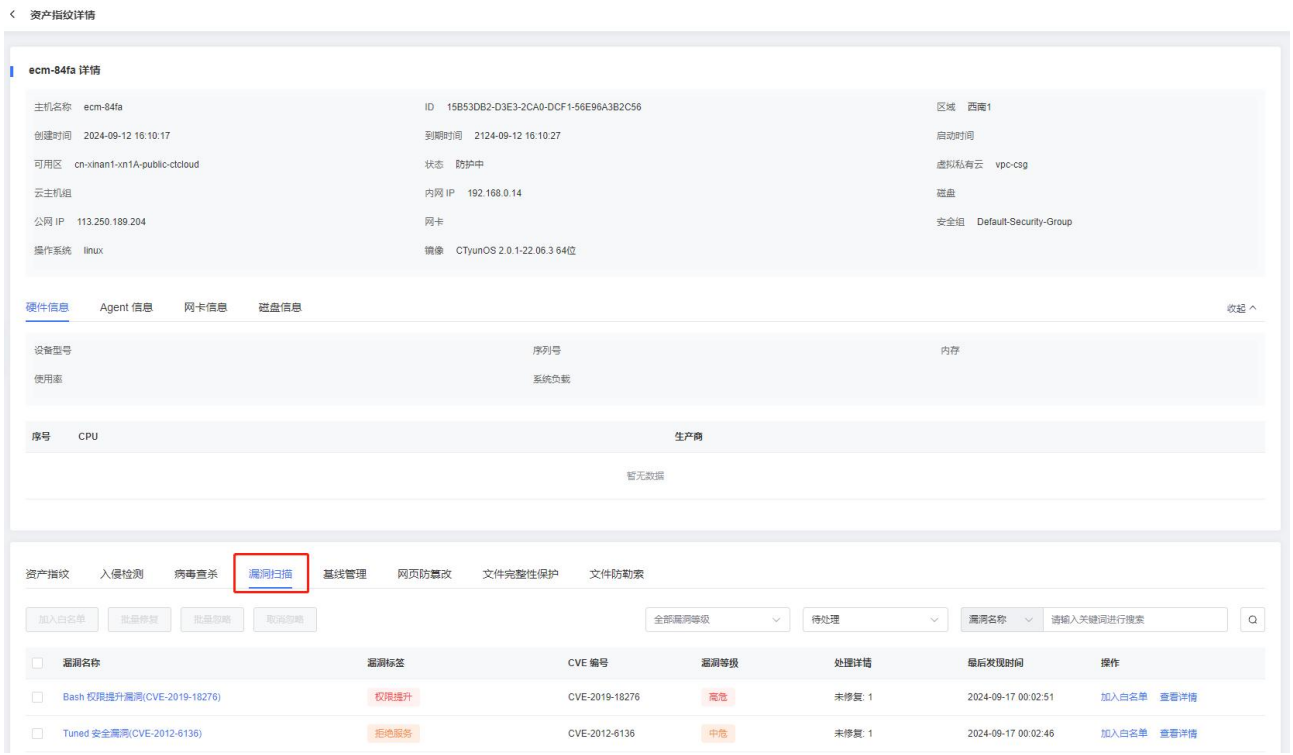
漏洞扫描任务完成后，扫描结果展示在“上一次扫描”处。如下图所示，包括扫描时间、漏洞情况和查看详情。

点击“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。



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。



处理漏洞事件

- 修复漏洞

如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。您可以在控制台一键自动修复漏洞，或根据漏洞修复建议，登录服务器手动修复漏洞。

- 忽略漏洞

  某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某漏洞暂时无害，可以忽略该漏洞。忽略漏洞后，下一次漏洞扫描任务执行时，系统仍然会扫描并展示该漏洞。

- 漏洞加入白名单

  如果确认漏洞不会对您的业务造成任何影响，无需修复，您可以将漏洞添加至白名单。漏洞加入白名单后，漏洞列表不再展示该漏洞信息，在下一次漏洞扫描任务执行时，系统不会再扫描和展示该漏洞信息。

5.5. OpenSSL 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

- 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。
- 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。
- 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。

- 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。
- 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。
- 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。

依赖 OpenSSL 的软件或协议

- MongoDB 4.4
- Nginx
- KeepAlived
- Https
- OpenSSH
- SSH
- VPN
- 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

- CVE-2016-0705 OpenSSL DSA 代码双重释放漏洞
  - 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。
  - 影响版本

OpenSSL 1.0.2 及更早版本

OpenSSL 1.0.1 及更早版本

- 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

- CVE-2016-0799 OpenSSL ‘BIO_*printf’ 函数安全漏洞
  - 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。

  - 影响版本

    OpenSSL 1.0.2 及更早版本

    OpenSSL 1.0.1 及更早版本

  - 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

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

  - 影响版本

    OpenSSL 1.0.1 < 1.0.1s

    OpenSSL 1.0.2 < 1.0.2g

  - 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

- 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 1.0.1o
  - 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. OpenSSH 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

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。

1. 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。
2. 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。

3. 在漏洞扫描详情页面， Windows 系统漏洞列表中已检测出主机存在的 OpenSSH 漏洞。

4. 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。
5. 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。
6. 重启云主机后，再次单击“一键扫描”，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：

- 身份鉴别

- 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。

- 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。

- 入侵防范
  - 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。

  - 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。

- 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。

5.8. 二类节点资产纳管最佳实践

产品订购

服务器安全卫士（原生版）、网页防篡改（原生版）属于平台级产品，不区分资源池，进入产品订购页正常购买防护配额即可纳管二类节点区域的资产。

支持纳管的区域

支持纳管的二类节点区域如下，根据主机所在区域选择不同的纳管方案：

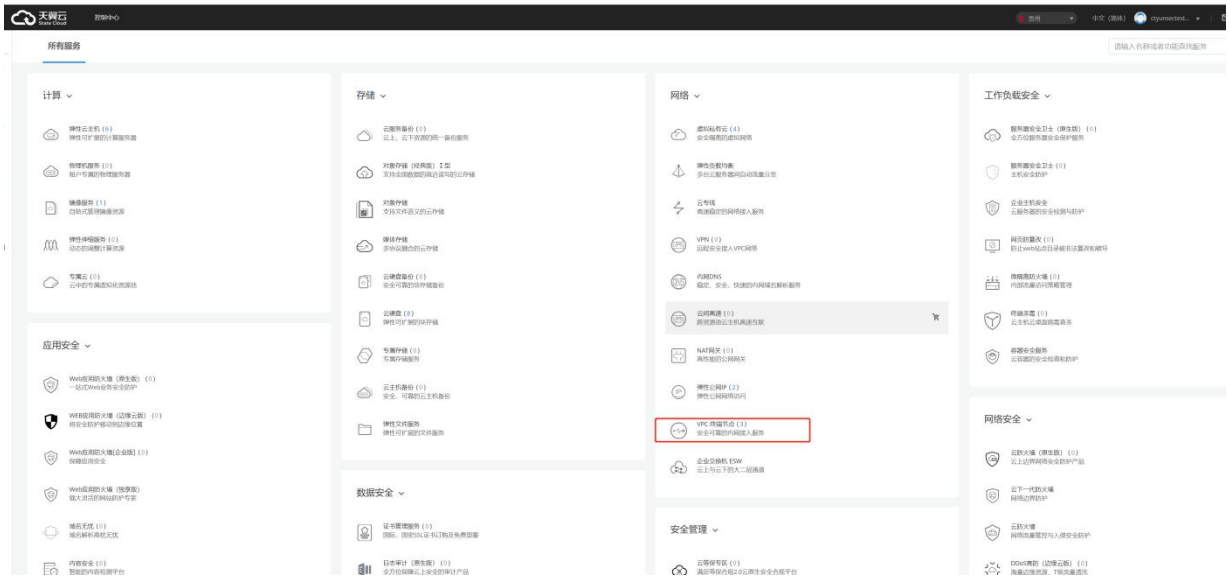
资源池大区	如下区域，使用方案一	如下区域，使用方案二
华东地区	上海 4/杭州（AZ1）/杭州（AZ2）/苏州（AZ1）/苏州（AZ2）/苏州（AZ3）/芜湖	南昌
华南地区	长沙 2（AZ1）/长沙 2（AZ2）/武汉 2（AZ1）/福州（AZ1）/福州（AZ2）/深圳	南宁/海口（AZ1）/广州 4
西北地区	西安 2（AZ1）/西安 2（AZ2）/西安 2（AZ3）/乌鲁木齐/兰州/西宁	中卫
西南地区	贵州/成都 3	重庆/昆明
北方地区	郑州/内蒙 3	青岛（AZ1）/青岛（AZ2）/北京 2/太原/石家庄（AZ1）/石家庄（AZ2）/天津/长春/哈尔滨/沈阳 3/华北（AZ3）

5.8.1. 方案一：通过 VPC 终端节点安装 Agent

创建终端节点

在需要安装服务器安全卫士（原生版）或网页防篡改（原生版）Agent 的主机所在的 VPC 中创建终端节点。

1. 选择主机所在的资源池，进入 VPC 终端节点管理控制台。



2. 在需要安装服务器安全卫士（原生版）或网页防篡改（原生版）Agent 的主机所在的 VPC 中创建终端节点。

   示例：

创建终端节点参数说明：

参数	说明
区域	选择主机所在的区域。
服务类型	选择“按名称查找服务”。
服务名称	请参见下述“终端节点服务名称”列表，获取对应区域的服务名称。
虚拟私有云	选择待安装 Agent 的主机所在 VPC 的名称。
子网	根据实际情况自动填写。
IPv4 地址	可以选择自动分配 IP 地址，或手动指定 IP 地址，为需要安装 Agent 的主机提供服务的 IP。

终端节点服务名称：

资源池大区	资源池名称	终端节点服务名称
华东地区	上海 4	cn-sh1.44a01abc-3fa6-4ac6-9444-43181dc20139
	杭州（AZ1）/杭州（AZ2）	cn-hz1.b4c2cdb9-5b74-4f0b-a323-70e0c0637b23
	苏州（AZ1）/苏州（AZ2）/苏州（AZ3）	cn-jssz1.ctcss.a3a55793-cfed-42bd-9f2f-9a0cf513d215
	芜湖	cn-ahwh1.2368a9c5-4fba-4058-8c4f-288599af47e6
华南地区	长沙 2	cn-hncs1.39dc6f84-6a3d-4a7f-82f9-b5810ec83733
	武汉 2	cn-hbwh1.a8cded11-bc2f-460c-ac6c-b70818dff444
	福州（AZ1）/福州（AZ2）	cn-fz1.f892afa6-05c4-402d-948f-32b377b39c4d
	深圳	cn-sz1.5de5e030-9644-4c5b-b764-0f97f520ab00
西北地区	西安 2（AZ1）/西安 2（AZ2）/西安 2（AZ3）	cn-snxy1.f9a99aa3-5bf8-4b17-acce-cb6019fe74c6
	乌鲁木齐	cn-xjcj1.35b01e6d-420e-4c94-9472-7e281792c4ea
	兰州	cn-gslz1.80129d9f-074f-49d7-84ee-9c76dafbf35b
	西宁	cn-qhxn1.040b1a6c-0524-4979-a0d3-d373f39230ea
西南地区	贵州	cn-gz1.68bf9153-0996-409a-a475-923834f86a09
	成都 3	cn-sccd1.9d84fe68-b3ce-46ea-8344-edb0e88397e8
北方地区	郑州	cn-hazz1.09353e17-7be4-424d-84dd-65dcc94d15a4
	内蒙 3	cn-nmhh1.c1e55989-e719-4b50-ab7e-9a21526ac637

Agent 安装

登录控制台

1. 登录服务器安全卫士（原生版）或网页防篡改（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，单击“安装 Agent”。

Linux 主机安装 Agent

1. 切换到“Linux 系统”选项卡。
2. 复制“云外主机”安装命令，将安装命令中的 ctcssextap2.ctyun.cn 替换成 VPC 内指定终端节点提供服务的 IP。

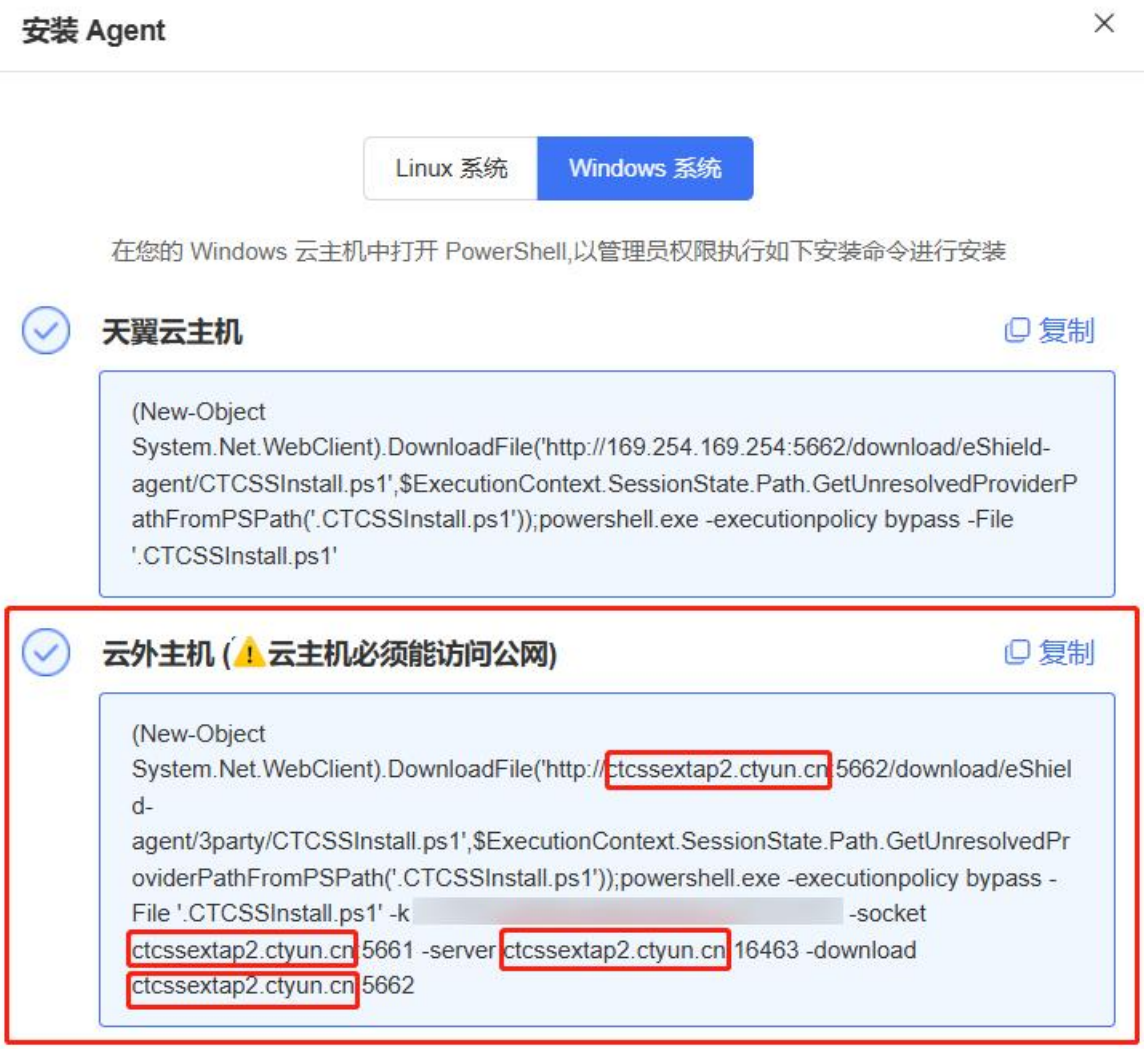
注意：

需要复制客户自己页面的命令后修改关键地址，请勿直接复制控制台或文档中的命令进行执行，否则可能导致 Agent 安装失败。

3. 在 Linux 云主机中，以管理员权限执行修改后的安装命令进行安装。

Windows 主机安装 Agent

1. 切换到“Windows 系统”选项卡。
2. 复制“云外主机”安装命令，将安装命令中的 ctcssextap2.ctyun.cn 替换成 VPC 内指定终端节点提供服务的 IP。



> 注意：
>
> 需要复制客户自己页面的命令后修改关键地址，请勿直接复制控制台或文档中的命令进行执行，否则可能导致 Agent 安装失败。

3. 在 Windows 云主机中打开 PowerShell（按 win + R 组合键打开运行，输入 powershell 执行）。
4. 在打开的 PowerShell 控制台以管理员权限执行安装命令进行安装。

控制台查看

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，在服务器列表页面查看纳管的资产是否存在。
3. 查看资产防护状态是否正常。

4. 对需要防护的服务器切换版本，绑定企业版配额。

5.8.2. 方案二：通过接入公网安装 Agent

前提条件

云外主机通过**公网**接入服务器安全卫士（原生版）控制台或网页防篡改（原生版）控制台，请确保：待纳管的云主机均可以正常连通 ctcssextap2.ctyun.cn 的 5661、5662、16463 三个端口。

接入方式

支持公网直连和代理方式两种接入方式，使用场景区别如下：

接入方式	使用场景
公网直连	● 待接入的服务器较少（小于等于 3 台）。 ● 所有服务器均可以直通公网 ctcssextap2.ctyun.cn 地址。
代理方式	如果待接入的服务器较多（大于 3 台），或者只有部分（至少一台）服务器能连通公网，建议通过代理方式接入。

公网直连

直接为服务器安装部署服务器安全卫士（原生版）的 Agent。

代理方式

使用能连通公网的服务器（配置最低 2C4G）作为代理，其他服务器通过代理做转发，这种方式运维成本较低。

- 代理可以使用所在云平台自身的 NAT 网关功能（具体可以参考对应平台 NAT 网关产品的相关文档）。
- 也可以使用自建的四层负载均衡（传输层 TCP 负载）服务代理 ctcssextap2.ctyun.cn 域名的 5661、5662、16463 三个端口，待接入的服务器通过配置 hosts 解析将 ctcssextap2.ctyun.cn 解析到代理服务器地址即可。此处代理服务器出公网的 IP 也需要保证唯一固定不变。

如下分别提供了基于开源 nginx 和 haproxy 实现四层网络代理的配置文件参考：

基于 nginx 代理的配置参考：

```
worker_processes  auto;user nginx;events {
  worker_connections  10240;
}
stream {
  upstream ctcss_5661 {
    server ctcssextap2.ctyun.cn:5661;
  }
  upstream ctcss_5662 {
    server ctcssextap2.ctyun.cn:5662;
  }
  upstream ctcss_16463 {
    server ctcssextap2.ctyun.cn:16463;
```

```
  }

  server {
    listen 5661;
    proxy_pass ctcss_5661;
  }
  server {
    listen 5662;
    proxy_pass ctcss_5662;
  }
  server {
    listen 16463;
    proxy_pass ctcss_16463;
  }
}
```

基于 haproxy 代理的配置参考：

```
global
    log         127.0.0.1 local2
    pidfile     /var/run/haproxy.pid
    maxconn     500000
    user        haproxy
    group       haproxy
    daemon
nbproc 6


defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          8h
```

```
    timeout server          8h
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 400000


listen socket_server
    bind *:5661
    mode   tcp
    option tcpka
    balance roundrobin
    server socket_server ctcssextap2.ctyun.cn:5661 check inter 3000 rise 2 maxconn 250000 fall 3


listen update_server
    bind *:5662
    mode   tcp
    option tcpka
    balance roundrobin
   server update_server ctcssextap2.ctyun.cn:5662 check inter 3000 rise 2 maxconn 25000 fall 3


listen es_server
    bind *:16463
    mode   tcp
    option tcpka
    balance  roundrobin
    server es_server ctcssextap2.ctyun.cn:16463 check inter 3000 rise 2 maxconn 250000 fall 3
```

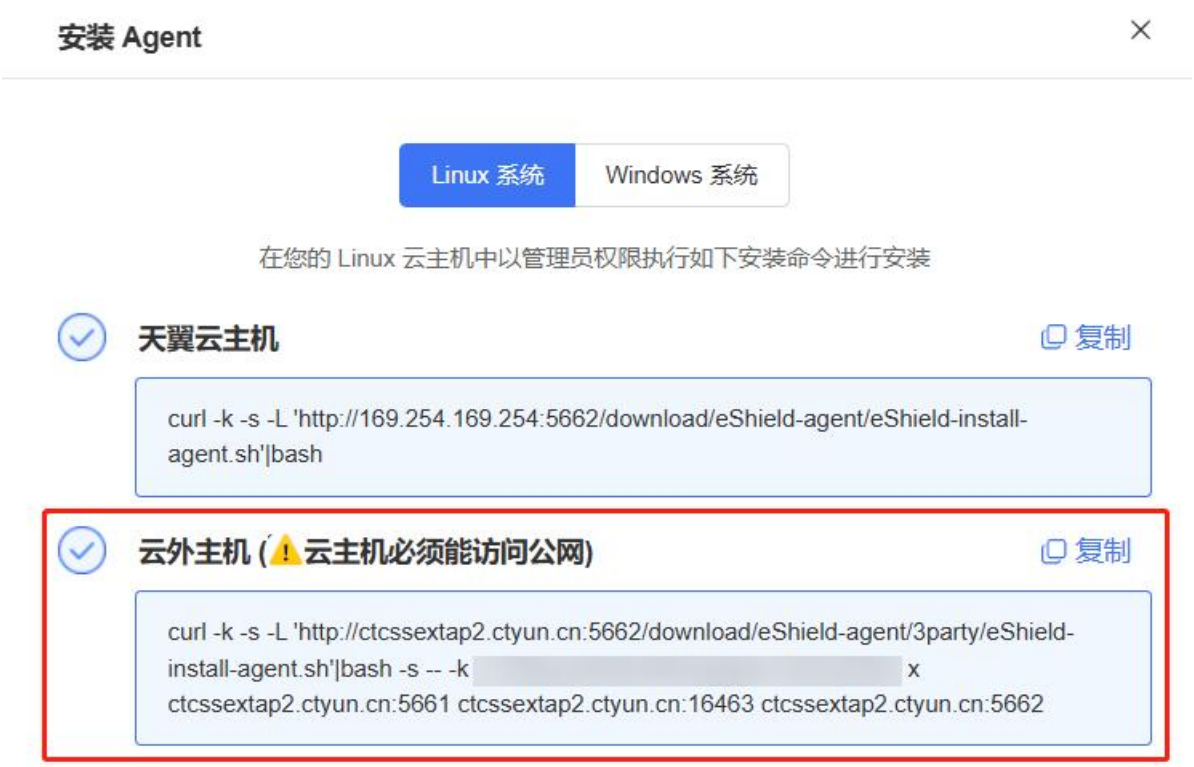
Agent 安装

登录控制台

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，单击“安装 Agent”。

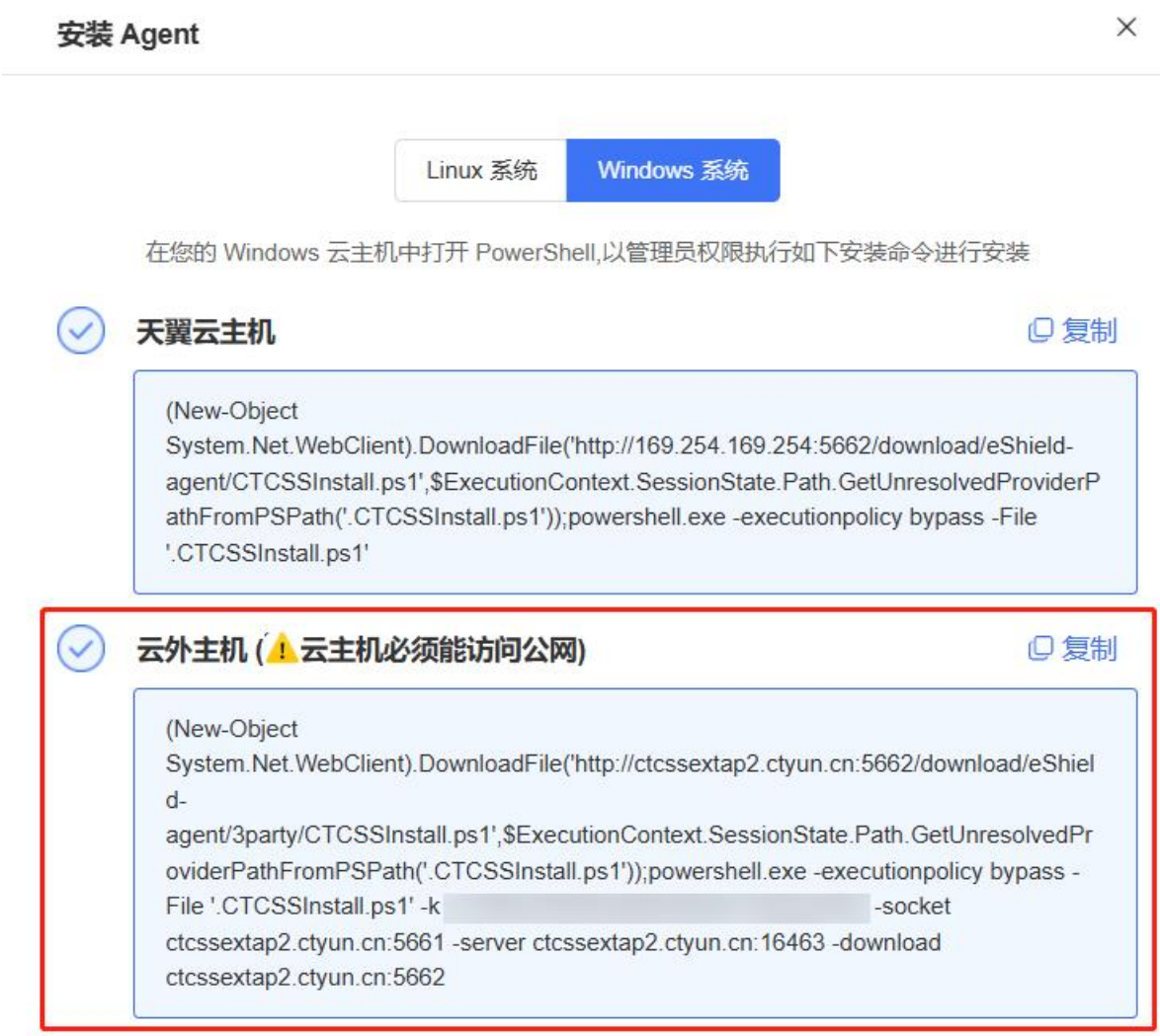
Linux 主机安装 Agent

1. 复制“云外主机”安装命令。
2. 在 Linux 云主机中以管理员权限执行安装命令进行安装。



Windows 主机安装 Agent

1. 复制“云外主机”安装命令。
2. 在 Windows 云主机中打开 PowerShell（按 win + R 组合键打开运行，输入 powershell 执行）。
3. 在打开的 PowerShell 控制台以管理员权限执行安装命令进行安装。



控制台查看

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，在服务器列表页面查看纳管的资产是否存在。
3. 查看资产防护状态是否正常。

4. 对需要防护的服务器切换版本，绑定企业版配额。


安装 Agent
移动分组
批量切换版本
服务器
操作系统
地域
服务器状态
Agent 状态
防护状态
风险状态
配额版本
操作
DESKTOP-V58F60I
172.25.10.193(私)
Windows
云外主机
运行中
在线
免费防护
无风险
免费版
切换版本
卸载 Agent
更多

6. 常见问题

6.1. 产品类

6.1.1. 产品咨询

Q：什么是服务器安全卫士（原生版）

A：服务器安全卫士（原生版）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、弱口令检测等功能，帮助您构建服务器安全防护体系。

Q：什么是网页防篡改（原生版）

A：网页防篡改（原生版）是一款全方位保障云上网站安全的产品，可对网站文件进行监控，若发生篡改时，实时对客户进行告警；同时通过备份恢复被篡改的文件或目录，保障客户系统的网站信息不被恶意篡改。

Q：服务器安全卫士（原生版）是否有版本区分？主要功能有何不同?

A：服务器安全卫士（原生版）提供基础版、企业版、旗舰版和增值服务（网页防篡改）供用户选择：

- 基础版包含安全概览、资产管理、入侵检测（异常登录、暴力破解）、漏洞扫描等功能。
- 企业版包含安全概览、资产管理、入侵检测（异常登录、暴力破解、后门检测、可疑操作、反弹 Shell、进程提权、Webshell 检测）、漏洞扫描、基线管理、病毒查杀等功能。
- 旗舰版包含安全概览、资产管理、入侵检测（异常登录、暴力破解、后门检测、可疑操作、反弹 Shell、进程提权、Webshell 检测、端口蜜罐）、漏洞扫描、基线管理、病毒查杀、文件完整性保护、文件防勒索等全部功能。

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：服务器安全卫士（原生版）是否可以申请试用?

A：服务器安全卫士（原生版）企业版、旗舰版目前暂不支持试用，基础版在您购买天翼云的服务器后，阅读并同意相关协议即可免费开通使用。

Q：服务器安全卫士（原生版）企业版到期后不续费会对业务造成影响吗?

A：不会，服务器安全卫士（原生版）企业版、旗舰版到期后会自动切换到基础版，部分高级功能无法使用，用户仍可使用基础版进行防护。

Q：服务器安全卫士（原生版）企业版回归基础版后，是否需要重新安装 Agent 与配置主机防护信息?

A：不需要，用户无需在控制台进行配置操作，仅对高级功能进行权限控制，同时 Agent 会自动切换成基础版，对用户无影响，可正常使用。

Q：服务器安全卫士（原生版）企业版到期回归基础版后，历史安全事件记录是否仍可查看?

A：服务器安全卫士（原生版）企业版、旗舰版回归基础版后，以往安全事件记录仍可在主机详情中查看。

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：服务器安全卫士（原生版）与非云原生的主机安全软件有何区别?

A：服务器安全卫士（原生版）与非云原生的主机安全软件相比不需要用户自己安装控制中心，即开即用；灵活授权，根据用户业务安全性需要选择不同版本客户端；实时更新，保持最新版本、最新安全能力。

Q：服务器安全卫士（原生版）购买后遇到问题如何解决?

A：天翼云为客户提供 7 天×24 小时客服服务，包括客服的售后热线（400-810-9889）咨询服务和在线工单服务，解答、处理客户在使用天翼云服务过程中遇到的问题，《专用服务条款》另有约定的，适用《专用服务条款》的约定。

Q：服务器安全卫士（原生版）软件版本、病毒库、漏洞库等需要手动更新吗?

A：不需要，在购买服务周期内，系统检测到最新库版本，自动进行更新，用户无需额外操作。

Q：服务器安全卫士（原生版）漏洞库多久更新一次?

A：漏洞规则库每月更新一次。

Q：服务器安全卫士（原生版）支持的系统 OS 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，详见“产品介绍 > 产品使用限制”。

Q：购买了服务器安全卫士（原生版）是否能保证系统通过网络安全等级保护测评（等保）？

A：网络安全等级保护测评为综合性测评，服务器安全卫士（原生版）只是满足等保中安全计算环境部分对云主机安全的相关要求，其他层面的安全要求需要匹配其他安全设备、配置安全策略来满足。

Q：服务器安全卫士（原生版）是否能以软件形式线下交付?

A：不支持线下软件的形式交付。

Q：服务器安全卫士（原生版）和云防火墙一起使用需要注意什么问题?

A：服务器前面有防火墙的话，需注意是否做了源 IP nat，如果有暴力破解会封禁 IP，如果做了 nat 会封禁 nat 后的 IP，可能影响业务。

6.1.2. Agent 问题

Q：什么是 Agent?

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：安装 Agent 会不会对自身的业务稳定性产生影响?

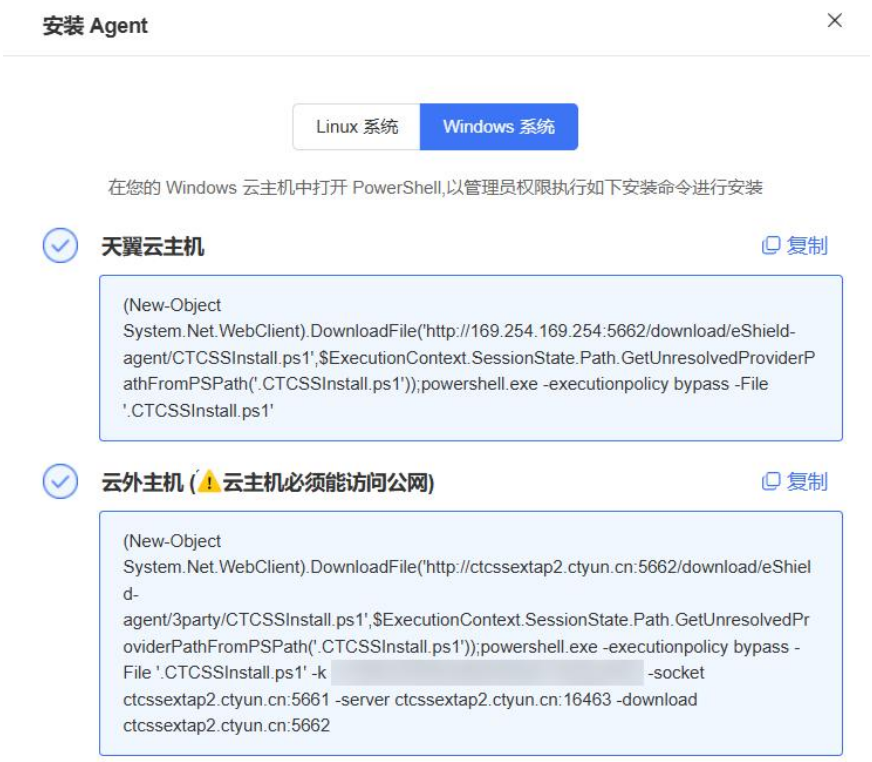
不会。Agent 是纯应用层的，不会给系统装任何的驱动；Agent 的带宽和资源占用很小；Agent 已经通过各种业务场景长时间运行测试，不会影响系统的稳定性。

Q：如何安装 Agent?

开通服务器安全卫士后，在左侧导航中选择“资产管理 > 服务器列表” ，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 并自动激活，Agent 服务正常。
- 若状态为“离线”、“错误”、未激活”，则需要为服务器重新安装 Agent。
  - Linux 系统安装命令

  - Windows 系统安装命令



Q：如何卸载 Agent

支持一键卸载和本地手动卸载两种方式。

1、通过控制台卸载 Agent 时，云主机的 Agent 状态应处于“在线”状态。

- 点击左上角控制中心进入服务器安全卫士（原生版）界面；
- 进入资产管理 -> 服务器列表，找到需卸载的云主机 Agent，点击“操作”列的“卸载 Agent”按钮，并在弹出的卸载 Agent 对话框中，点击“确定”按钮；
- 卸载成功后，Agent 状态应显示为“离线”状态，点击右侧刷新按钮可更新状态（由于缓存原因，Agent 状态更新需等待 10 分钟）。

2、云主机本地卸载 Agent

- 卸载 Linux 版本 Agent：

  以 root 用户登录到 Linux 云主机，任意目录下执行以下命令即可卸载 agent，执行无明显报错信息则卸载成功。

  执行命令卸载： bash /var/ctcss/active-response/bin/uninstall.sh
- 卸载 Windows 版本 Agent：

  登录到 Windows 云主机，在“控制面板 -> 程序和功能”中找到“CTCSS Agent”或"CTCSSAgen”，右键点击，选择卸载，按照提示卸载。

Q：Agent 安装失败如何处理?

Agent 安装失败的可能原因有多种，可按以下方法解决：

1、确认安装命令是否正确

点击”安装 Agent“按钮，即可获取到 Linux 和 Windows 系统安装指令。

2、 确认是否以 root 或管理员权限执行安装命令

Agent 安装需要 root 或管理员权限。

3、 卸载 Agent 后再次尝试安装

若再次安装仍然失败，提工单联系技术支持。

Q：Agent 状态异常如何处理?

若安装 Agent 后，在服务器安全卫士界面无法找到安装 Agent 的云主机，或者 Agent 状态仍然为“离线”状态，则可能 Agent 与服务端无法正常通信，状态异常。可按以下方法排查解决：

1、Agent 安装后，需在控制台右上角点击“同步资产”按钮，等待 5~10s 待同步完成后（按钮旁的资产更新日期会刷新），安装 Agent 的云主机会显示在界面中。

2、 查询 agent 是否支持该云主机操作系统。

3、查看主机网络联通，命令行执行 telnet 169.254.169.254 5661 看是否能正常联通服务端。若不能，执行 route -n (Windows 为 route print）查看主机是否具备到 169.254.169.254 的路由，若缺失该路由，请提工单添加该路由。

```
[root@ ]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
169.254.169.254 192.168.0.1     255.255.255.255 UGH   0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

4、 Agent 服务异常，需重启 Agent 服务。

- Linux 系统 以 root 用户在命令行执行 systemctl restart ctcss (centos6 执行 service ctcss restart);

- Windows 系统 以管理员权限，打开“任务”页签，选中“ctcss-agentd",右键单击，选择”重新启动“，完成 agent 重启。

5、重启 Agent 服务后等待几分钟，刷新页面后若仍然为”离线“状态，请卸载 Agent，并重新安装。

Q：如何查看未防护的主机?

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“资产管理 > 服务器列表”，筛选防护状态为“未防护”的服务器。请您在未防护的主机中安装部署 Agent，并正常开启主机防护功能。

Q：如何查看已离线的主机?

您可以登录服务器安全卫士（原生版）控制台，在左侧导航中选择资产管理 -> 服务器列表，“已离线主机”页面为您展示防护状态为“已离线”的服务器。

请您确定主机网络通信是否正常， Agent 状态为“离线”状态，则可能 Agent 与服务端无法正常通信，状态异常，排查步骤详见常见问题“Agent 状态异常如何处理”。

Q：Agent 默认安装路径是什么?

在 Linux/Windows 操作系统的主机中安装 Agent 时，安装过程中不提供安装路径的选择，默认安装在以下路径中:

操作系统	默认安装路径
Windows	C:\Program Files (x86)\ctcss-agent

操作系统	默认安装路径
Linux	/var/ctcss

Q：Agent 如何升级?

Agent 升级正常情况下为自动升级，当 Agent 发布新版本时，服务端会给 Agent 下发一次升级命令，Agent 收到后自行升级。但服务端下发的指令可能因网络等原因，Agent 未收到，导致仍然为旧版本。用户可卸载 Agent，并重新下载、安装 Agent，确保云主机内运行的 Agent 为最新版本。

Q：Agent 运行过程中占用多少资源?

Agent 运行时，内存占用不超过 500MB，超过 Agent 自动重启；单核 CPU 占用不超过 20%，超过 Agent 暂时挂起。

vCPU 规格	CPU 占用（峰值）	内存占用（峰值）
1vCPU	20%	500MB

Q：Agent 安装以后会访问哪些地址?

Agent 安装后会访问的 IP、端口如下表所示：

源 IP	源端口	目的设备	目的 IP	目的端口	协议
Agent 云主机 IP	随机	服务器安全卫士服务端	169.254.169.254	5661 及 16463	TCP

访问说明：Agent 访问服务器安全卫士服务端，主要是获取服务端下发的策略/配置/指令，上报安全告警事件及资产指纹。

Q：服务器安全卫士（原生版）和网页防篡改（原生版）共用 Agent?

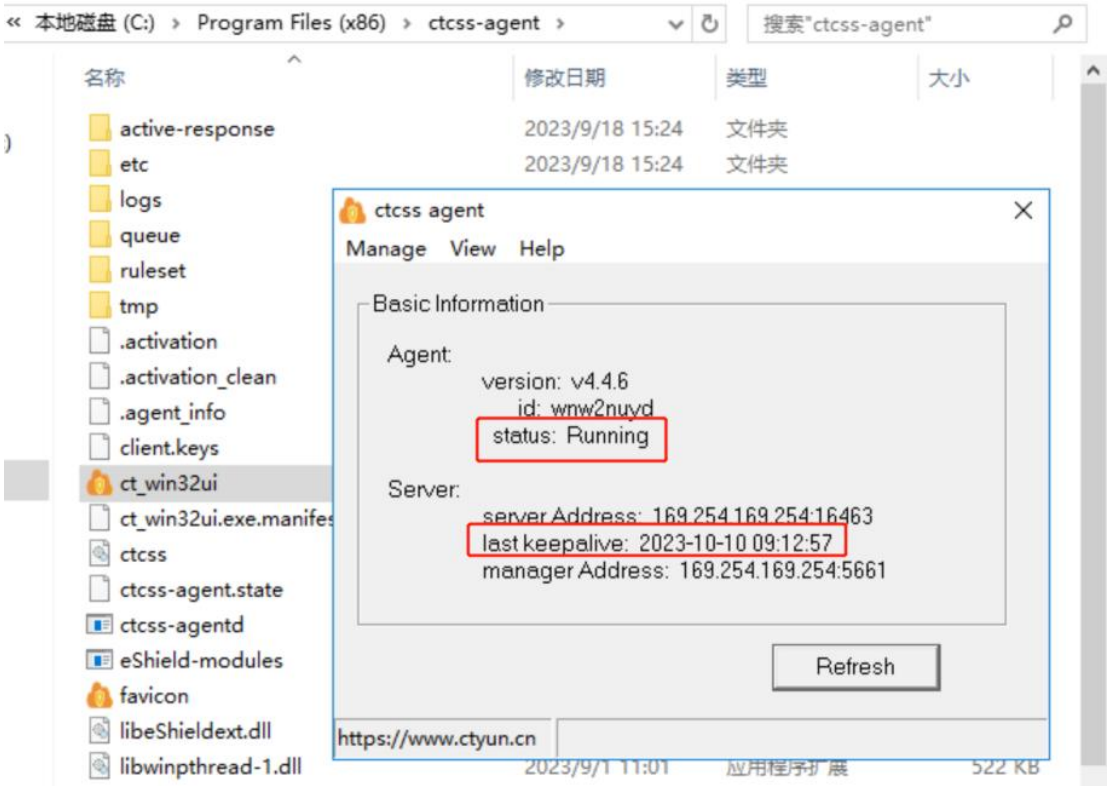
共用一个 Agent，在天翼云控制台上统一下发管理防护策略，Agent 执行监控与处置。

Q：已开通安全卫士，服务器防护状态显示未防护， 如何解决?

1. 查看 Agent 是否启动 。

   Windows:

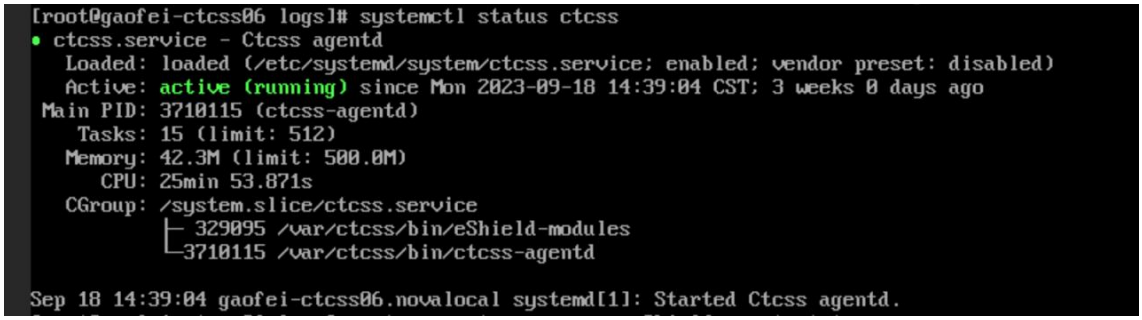
   点击部署目录下的 ct_win32ui.exe ，查看 ui 界面显示的 agent status 应为 Running，last keepalive 是否更新（与当前系统时间相差应不超过 1 分钟）



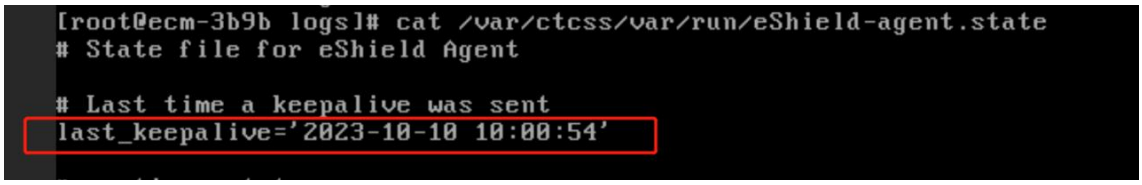
   Linux:

   centos 6 使用 service ctcss status 查看 agent 服务状态是否为 Running

其他 Linux 发行版使用 systemctl status ctcss 查看 Agent 服务状态是否为 active



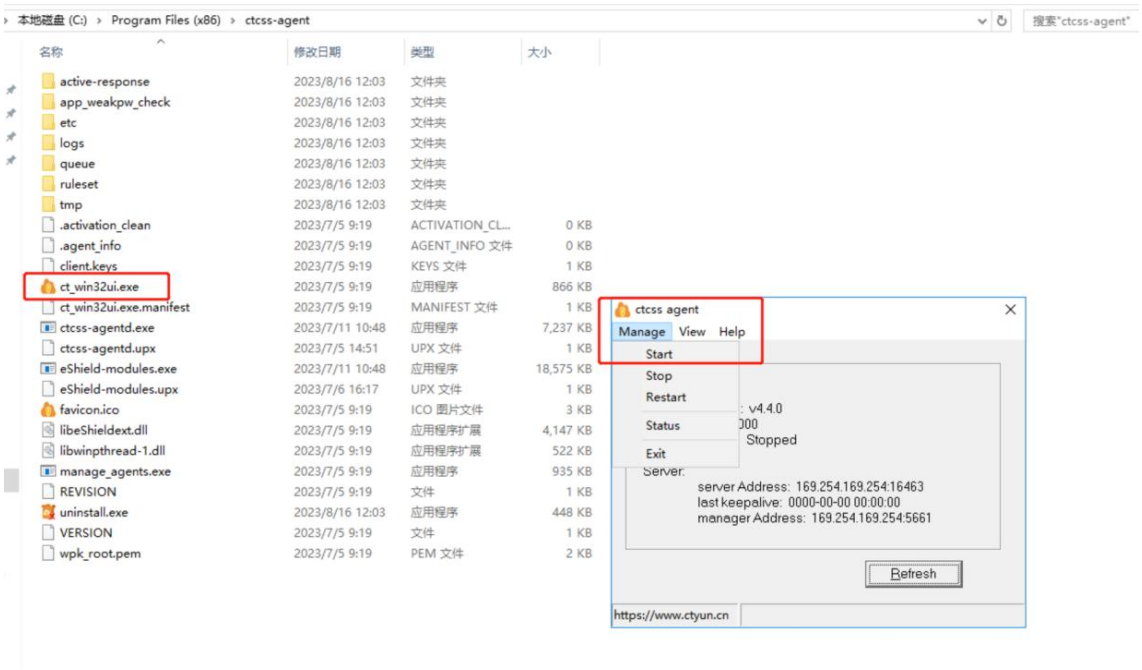
查看 /var/ctcss/var/run/eShield-agent.state 文件中 last keepalive 是否更新（与当前系统时间相差应不超过 1 分钟）



2. Agent 未启动，请按如下方式启动。

Windows：

点击部署目录下的 ct_win32ui.exe ，在弹出的 ui 界面中点击左上角 Manage 选项，可控制 Agent 的启停。



Linux:

centos 6 使用 service ctcss start/stop 启停 Agent；

其他 Linux 发行版使用 systemctl start/stop ctcss 启停 Agent。

3. 检查安全卫士 Agent 配置。

若 Agent 处于 running 状态，但 last keepalive 时间未更新，则可能为配置文件错误。

查看 Agent 配置文件，由于 Agent 版本差异，配置文件路径不同。

- Windows 路径为 C:\Program Files (x86)\ctcss-agent\ctcss.conf 或 C:\Program Files (x86)\ctcss-agent\etc\ctcss.yml 。
- Linux 路径为 /var/ctcss/etc/ctcss.conf 或 /var/ctcss/etc/ctcss.yml；

  其中服务器 IP 应为 169.254.169.254 ，端口分别为 5661 和 16463 。（非公有云场景下，服务端 IP 地址可能有变化，以实际部署信息为准）。

```
[root@gaofei-ctcss06 ctcss]# cat /var/ctcss/etc/ctcss.conf
<ctcss_config>
    <client>
        <server>
            <address>169.254.169.254</address>
            <port>16463</port>
            <protocol>tcp</protocol>
        </server>
    </client>
    <manager>
        <server>
            <address>169.254.169.254</address>
            <port>5661</port>
            <protocol>tcp</protocol>
        </server>
    </manager>
</ctcss_config>
[root@gaofei-ctcss06 ctcss]# _
```

```
[root@gaofei-ctcss06 logs]# head /var/ctcss/etc/ctcss.yml
SocketServer:
  Host: 169.254.169.254
  Port: 5661
  Protocol: tls
EShieldServer:
  Host: 169.254.169.254
  Port: 16463
  Protocol: tcp
Database:
  Path: "ctcss.db"
[root@gaofei-ctcss06 logs]#
```

配置修改完成后需按前述步骤重新启动 Agent。

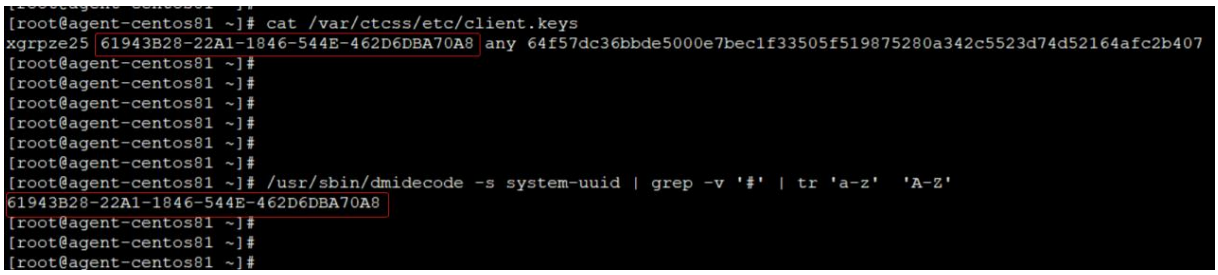
4. 检查 Agent 的激活文件中的信息。

   先检查 client.keys 中 guid 与机器真实 guid 是否一致。

   (1) 执行【 cat /var/ctcss/etc/client.keys 】获取 key 信息，包含四段数据，第二段为 guid，如下图第一个红框。

   (2) 执行 【 /usr/sbin/dmidecode -s system-uuid | grep -v '#' | tr 'a-z' 'A-Z' 】 获取当前机器 guid，如下图第二个红框。

   (3) 对比 guid 是否一致，如果不一致，执行【 rm -f /var/ctcss/var/run/.activation 】删除.activation 文件，之后需按前述“步骤 1”中最后一段描述，重新启动 agent。等 agent 启动之后，再次验证 guid 是否一致，若 guid 一致等待 agent 状态更新即可。



6.2. 计费购买类

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）计费方式均为包周期计费，包周期计费是一种预付费模式，即先付费再使用，支持包年/包月。

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：不购买服务器安全卫士（原生版）能购买网页防篡改（原生版）吗？

A：服务器安全卫士（原生版）企业版与网页防篡改（原生版）不需要绑定购买；网页防篡改（原生版）可在服务器安全卫士（原生版）基础版上升级购买使用。

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。

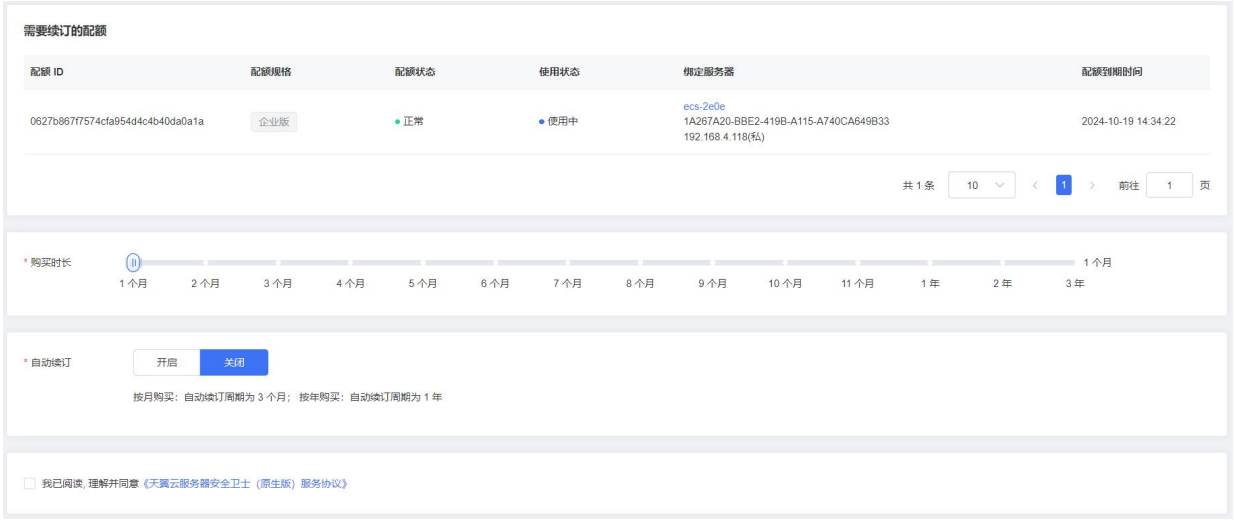
Q：服务器安全卫士（原生版）可以按天购买吗？

A：不支持，目前只支持包月和包年购买。

Q：服务器安全卫士（原生版）安全服务如何续费？

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。
3. 查看您已经订购的配额，选择所需续订的配额，点击“续订”；或勾选需要续订的配额，单击列表上方的“批量续订”。

4. 进入服务器安全卫士（原生版）续订页面，根据使用需要设置续订时长。



5. 续订时长设置完成后，在页面下方确认支付费用，阅读《天翼云服务器安全卫士（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）服务协议》“，在页面右下角单击“立即购买”。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。

Q：服务器安全卫士（原生版）安全服务如何退订?

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。
3. 查看您已经订购的配额，选择需要退订的配额，点击“退订”。

4. 进入退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。

5. 系统提示退订申请提交成功，可前往订单详情查看退订进度。

6.3. 防护操作类

6.3.1. 网页防篡改相关

Q：如何使用网页防篡改（原生版）？

A：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，根据您的网站情况进行防护策略的配置，即可开启网页防篡改（原生版）防护服务。

Q：如何绑定网页防篡改防护配额?

1. 购买成功防护配额后，可在防护配额管理页面查看配额的使用状态、绑定服务器、开通时间、到期时间等信息。

2. 在防护管理页面对需要防护的服务器进行防护设置，在防护设置页面选择防护配额，即可进行绑定。

Q：为什么要添加防护目录?

A：通常攻击者对网站发起攻击都会恶意篡改网页目录中的文件，因此需要添加网站防护目录，网页防篡改（原生版）才能实时监控，发现篡改行为后可以立即告警并自动恢复。

设置防护目录操作步骤如下：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版） > 防护管理”，进入防护管理页面。
3. 在列表中选择要进行防护设置的服务器，单击操作列的“防护设置”，进入防护设置页面。
4. 绑定防护配额：选择需要绑定的配额后，单击“配置防护策略”。

   若已经绑定防护配额，可直接进入篡改防护设置页面。
5. 篡改防护设置：包括配置防护目录、设置特权进程、设置远端备份。
   - 配置防护目录：防护目录分为添加白名单和添加黑名单两种模式，可根据实际使用场景进行配置。
     - 白名单模式：会对添加的防护目录和文件类型进行保护。
     - 黑名单模式：会防护目录下所有未排除的子目录、文件类型和指定文件。
   - 其他配置：请参见“网页防篡改（原生版）> 防护管理”。

完成防护设置后，用户即可对服务器开启网页防篡改防护。

Q：网站目录被恶意篡改了怎么办?

A：网页防篡改（原生版）具备实时监控和备份还原的能力，通过对比本地备份目录文件的指纹，发现网站目录文件被恶意篡改后，可立即对被篡改的文件进行自动还原。

Q：监控防护目录大小是否有限制?

A：防护目录有如下限制：

- 每台服务器最多可添加 10 个防护目录。
- 每个被防护的目录大小不超过 10GB。
- 所有被防护的目录下的文件夹个数不超过 3000 个。

Q：开启网页防篡改后，如何修改文件?

A：网页防篡改功能开启后，如果需要修改文件或更新网站，有如下两种方式：

- 方式一：暂时关闭网页防篡改功能

  完成修改或更新后再重新开启。关闭网页防篡改期间，文件存在被篡改的风险，更新文件后请及时开启网页防篡改。

- 方式二：设置特权进程

  特权进程为您信任的进程文件，可以对防护目录文件进行修改操作。请确保特权进程安全可靠。

6.3.2. 入侵检测相关

Q：出现弱口令告警如何处理?

A：若收到弱口令告警说明当前云主机口令过于简单，与弱口令检测的密码库匹配，存在被入侵的风险，需及时修改弱口令。

进入“基线管理 -> 弱口令检测”页面，可查看检测出的弱口令。

根据检测列表中的服务器信息，弱口令信息，登录出现弱口令的主机，修改弱口令。

常见弱口令修改方式

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

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。

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。

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）。

Q：支持哪些系统或应用的弱口令检测?

- 操作系统：Linux、Windows。
- 数据库：MySQL、Redis、PostgreSQL、Mongo。

Q：如何设置强口令?

可按以下规则设置口令：

- 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
- 不同的机器或应用使用不同的密码
- 定期修改密码，至少每三个月更新一次

Q：弱口令检测是针对操作系统还是服务器承载的应用系统?

服务器安全卫士（原生版）弱口令检测支持操作系统弱口令、应用弱口令检测，并支持一键检测和定时检测。

Q：服务器显示登录异常怎么解决?

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?

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：如何查看异地登录的源 IP?

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”，在异常登录告警列表中查看异地登录的源 IP 地址。

Q：是否可以关闭异地登录检测?

不可以，异地登录是入侵者常见的攻击特效，可以有效发现入侵，如果您不想接收异地登录的告警，可以将登录地点添加到白名单中进行信任。

Q：如何减少服务器被爆破登录的风险?

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：什么是反弹 Shell?

反弹 Shell 是一种网络安全攻击技术，也被称为“反向连接”。它的原理是通过在受害者的计算机上执行一个恶意程序（通常是一个后门程序），并使其与攻击者的计算机建立一个反向连接。这样，攻击者就可以获取对受害者计算机的控制权，并执行各种命令、操作和访问敏感信息。

Q：正常的脚本执行行为被误报为反弹 Shell，要如何消除误报?

您可以通过以下方式消除误报：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航中选择“入侵检测 > 反弹 Shell”。
3. 在反弹 Shell 页面，找到被定义为反弹 Shell 的记录，您可以根据服务器的 IP、端口、进程等进行查询。
4. 在右侧操作栏中，单击“加入白名单”，即可将此反弹 Shell 告警加入白名单，后续相同来源 IP 的相同操作将不会产生告警。

如果您误加入了白名单，您可以单击“白名单管理”，将误加入白名单的记录移除白名单，后续相同来源 IP 的相同操作将会产生告警。

Q：反弹 Shell 是怎么进行检测?

购买企业版或旗舰版配额后，即可开启反弹 Shell 检测。

反弹 Shell 的检测方式是 Agent 定时采集在服务器执行的 Shell 命令，对 Shell 命令进行正则匹配，如果 Shell 命令匹配上了反 Shell 的正则表达式，则会判断出服务器正则受到反弹 Shell 攻击。

Q：支持哪些反弹 Shell 命令检测?

服务器安全卫士（原生版）仅支持对 Linux 服务器的反弹 shell 检测。如下是当前支持的反弹 shell 命令：

操作系统	工具	反弹名称	技术类别
Linux	bash	bash 反弹	标准输入输出重定向 socket
	exec	exec TCP 反弹	标准输入输出重定向 socket
		exec UDP 反弹	应用程序命令中转
		exec TCP 反弹	应用程序命令中转
	awk	awk 反弹	应用程序命令中转
	gawk	gawk 反弹	应用程序命令中转
	python	python 反弹 shell	标准输入输出重定向 socket
			标准输入输出重定向管道
			标准输入输出重定向伪终端
			应用程序命令中转
	rev	rev 反转反弹	标准输入输出重定向 socket
	php	php 反弹 shell	标准输入输出重定向 socket
	perl	perl 反弹 shell	标准输入输出重定向 socket
	ruby	ruby 反弹 shell	标准输入输出重定向 socket
	nc	nc 反弹 shell	标准输入输出重定向管道
		nc -e 反弹 shell	应用程序命令中转
		nc udp 反弹 shell	标准输入输出重定向管道
	telnet	telnet 反弹 shell	标准输入输出重定向管道
	socat	socat 反弹 shell	标准
		socat 反弹 shell	标准输入输出重定向伪终端
		socat 反弹 shell	标准输入输出重定向伪终端
	ICMP	ICMP 反弹	应用命令

Q：如何处理反弹 Shell 告警?

您可以通过以下方式处理反弹 Shell 告警：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航中选择“入侵检测 > 反弹 Shell”。
3. 在反弹 shell 页面，找到被定义为反弹 shell 的记录，您可以根据服务器的 IP、端口、进程等进行查询。
4. 处理反弹 Shell 告警。
   - 加入白名单：在右侧操作栏中，单击“加入白名单”，即可将此反弹 Shell 告警加入白名单，后续相同来源 IP 的相同操作将不会产生告警。
   - 标记为已处理：单击“标记已处理”，即可将本条告警记录标记为已处理，后续相同来源 IP 的相同操作将仍然会产生告警。

Q：云主机遭受攻击为什么没有检测出来?

- 若云主机在安装服务器安全卫士 Agent 之前就已被攻击，服务器安全卫士可能无法检测出来。
- 若云主机安装 Agent 之后，未开启防护，服务器安全卫士可能无法检测出来。
- 服务器安全卫士防护的是主机层面的入侵，若攻击为 Web 层面，服务器安全卫士无法检测防护，可以使用 WAF 等其他安全产品。

Q：检测到入侵行为时，是否能够自动对安全事件进行处理?

不能，服务器安全卫士（原生版）检测到入侵行为后会第一时间告警，处置行为由相关管理员进行，以避免处置行为与正常业务进程相冲突。

Q：使用产品过程中，是否只开启病毒检测就可以了?

不是，在开启病毒检测功能的同时，安全管理员可使用入侵检测功能预防异常登录/暴力破解等非法攻击行为，防止攻击者使用非法手段投放病毒，同时可使用基线管理功能，优化云主机安全基线，预防病毒感染。

Q：检测到病毒文件应如何处理?

服务器安全卫士（原生版）检测到病毒文件会立即产生告警，需要您根据告警详细信息对病毒文件作出处置，处置方式包括以下三种：

- 隔离：将病毒文件或恶意程序移动至隔离区域，进行加密处理，禁止正常运行。
- 删除：永久从系统中删除病毒文件或恶意程序，以确保不再有可能的威胁。
- 信任：将某个文件或程序标记为安全并被信任，以避免将其隔离或删除。

Q：定时检测模式包含哪几种?

包含快速检测、全盘检测、自定义检测三种模式。

- 快速检测：扫描耗时短，对系统关键位置文件进行扫描。
- 全盘检测：对主机所有硬盘文件进行扫描，清理更彻底。
- 自定义检测：按指定位置有选择性扫描文件。

6.3.3. 风险评估相关

Q：什么是基线扫描?

病毒和黑客会利用服务器存在的安全配置缺陷入侵服务器盗取数据或是植入后门。基线扫描功能针对服务器操作系统、数据库、软件的配置进行安全检测，可以帮您加固系统安全，降低入侵风险并满足安全合规要求。

基线扫描功能通过配置不同的基线检查策略，可以帮助您快速对服务器进行批量扫描，发现包括系统、账号权限、数据库等存在的风险点，并提供修复建议。

基线扫描配置：

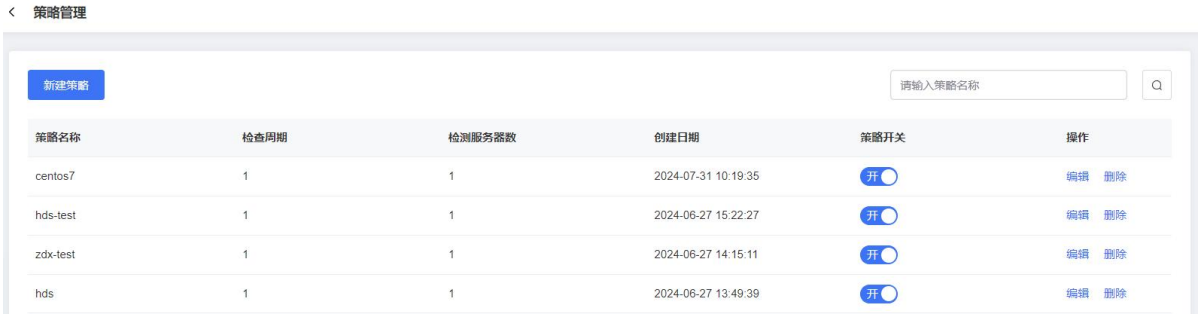
基线分类	检查标准及检查内容	覆盖的系统和服务

基线分类	检查标准及检查内容	覆盖的系统和服务
CIS 基线	基于 CIS 标准的安全基线检查	Unix 系统基线检测 Red Hat 6 企业版基线检测 Red Hat 7 企业版基线检测 Windows 审计基线 Windows 10 企业版安全基线检测 Windows 2012 R2 安全基线检测 Windows 2016 安全基线检测 SQL Server 2012 安全基线检测 MySQL 5.6 社区版基线检测 MySQL 5.6 企业版基线检测 Apache HTTP Server 2.4 基线检测 Web 应用漏洞审计基线

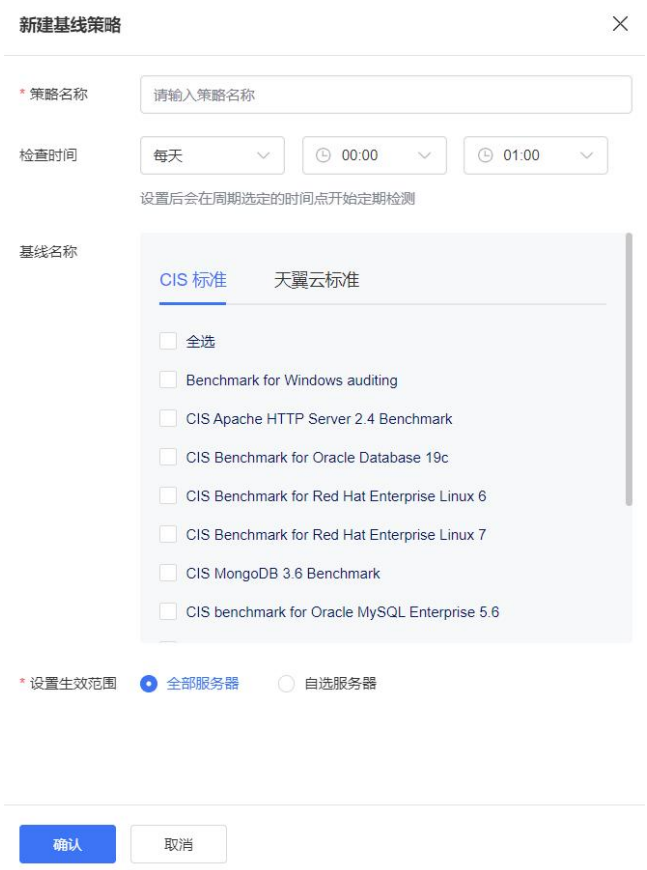
Q：如何对指定服务器下发基线检测任务?

1. 进入服务器安全卫士（原生版）控制中心。
2. 在左侧导航栏，选择“风险管理 > 基线检测”，进入基线检测页面。
3. 单击“策略管理”，进入策略管理页面。

4. 在策略管理页面，单击“新建策略”，页面右侧弹出新建基线策略窗口。



5. 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，单击“确认”。



Q：创建或者修改基线策略时，无法选择目标服务器?

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“资产管理 > 服务器列表”，在服务器列表页面检索目标服务器，查看 Agent 状态是否正常。

Q：扫描到漏洞后能否支持自动修复?

不支持，漏洞修复要经业务方确认对业务无影响后方能进行，如果对业务有影响，需采用其他安全手段削弱该漏洞的风险，而非直接进行漏洞修复。

Q：扫描出漏洞应怎么处理?

1、查看漏洞扫描结果及漏洞危害等级，评估漏洞对主机的影响程度。

2、按照推荐的漏洞修复方案进行处理，支持进行一键修复处置。

3、修复完成后，再次下发漏洞扫描任务对修复结果进行核查。

Q：漏洞修复后，为什么仍然提示漏洞存在?

漏洞扫描是通过获取主机中包管理器中存储的安装软件版本信息去判断是否存在漏洞软件，若漏洞修复时并未更新包管理器中存储的信息（如直接替换软件可执行文件），则漏洞扫描仍会扫出漏洞。若确定漏洞软件已更新，可在漏洞详情页将该漏洞标记为已处理。

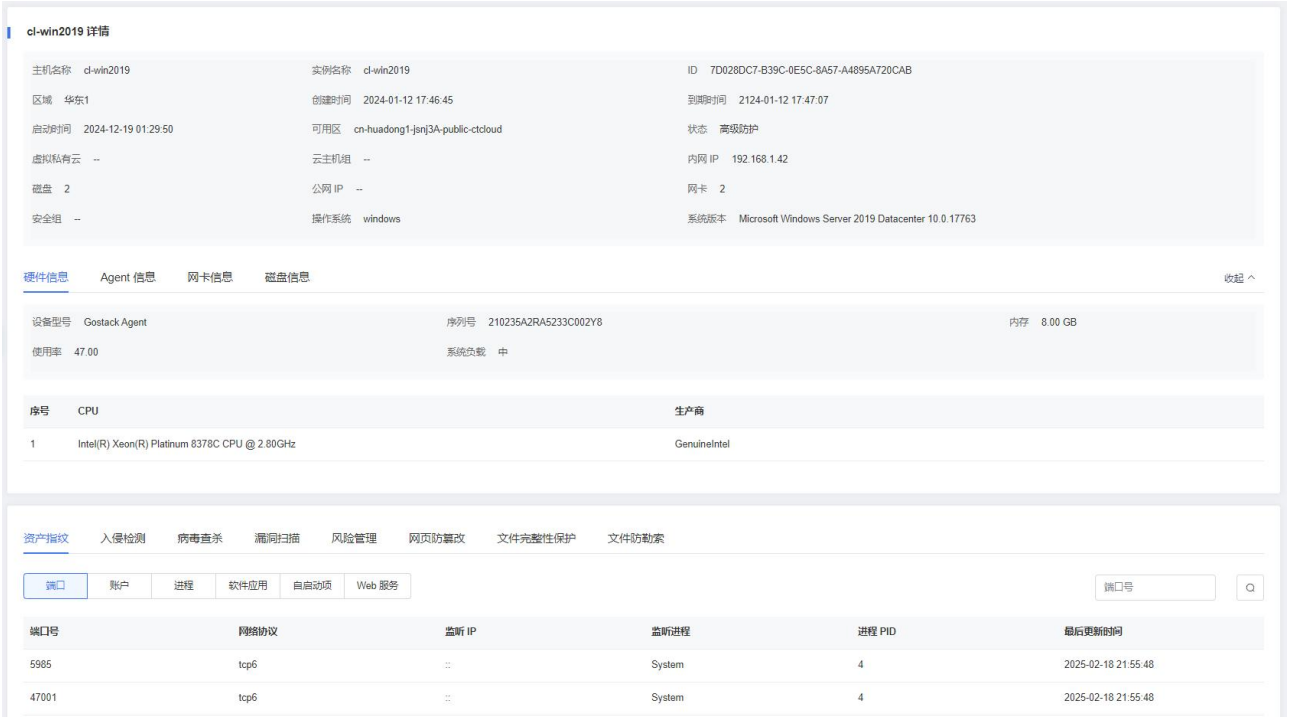
Q：如何评估漏洞对主机的影响范围?

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“风险管理 > 漏洞扫描”，在漏洞扫描页面告警列表通过漏洞公告、CVE 编号等找到该漏洞，单击“影响服务器数量”，即可查看存在漏洞的服务器。

6.3.4. 其他相关问题

Q：如何查看服务器详细信息?

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“资产管理 > 服务器列表”，进入服务器列表页面。
3. （可选）选择业务分组，服务器列表将只展示该分组中的服务器。
4. 在服务器列表页面选中任意一台服务器。点击服务器名称，可查看资产指纹详情。



Q：服务器安全卫士（原生版）资产是实时同步吗？

资产不是实时同步，您可以设置手动同步或定时同步:

- 定时同步周期是 12 小时或 24 小时，按周期定时同步您账户下的所有资产。
- 手动同步是用户主动触发资产同步，立即同步您账户下的所有资产。

Q：服务器安全卫士（原生版）是否支持向用户发送告警通知？

支持。服务器安全卫士（原生版）支持通过邮件方式自动发送风险告警通知。用户可在告警通知功能中自定义设置发送条件，基于防护功能、威胁等级、告警时间等进行配置。

Q：如何延长服务器安全卫士（原生版）防护配额有效期？

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏选择“设置中心 > 配额管理”，进入配额管理页面。

3. 查看您已经订购的配额，选择所需续订的配额，点击“续订”；或勾选需要续订的配额，单击列表上方的“批量续订”。

Q：如何筛选未绑定主机的配额？

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“设置中心 > 配额管理”，通过“使用状态”筛选查看未绑定主机的配额。

Q：如何切换服务器绑定的防护配额版本？

1. 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“资产管理 > 服务器列表”，在服务器列表页面查看服务器配额版本情况。

2. 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。

Q：服务器安全卫士（原生版）会主动收集用户服务器的数据么？是否有敏感信息泄露的风险？

服务器安全卫士（原生版）不会主动收集用户服务器的数据，只针对安全数据进行分析及处理，不会有敏感信息泄露的风险。

Q：如果未安装 Agent，云服务器是否能够被服务器安全卫士（原生版）识别到？

可以，服务器安全卫士（原生版）可识别未安装 Agent 的云主机，且可在“资产管理 > 服务器列表”中查看服务器信息及是否安装 Agent。