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
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。
01	2022/07/20	新建文档。

目 录

1. 产品介绍

1.1. 产品简介

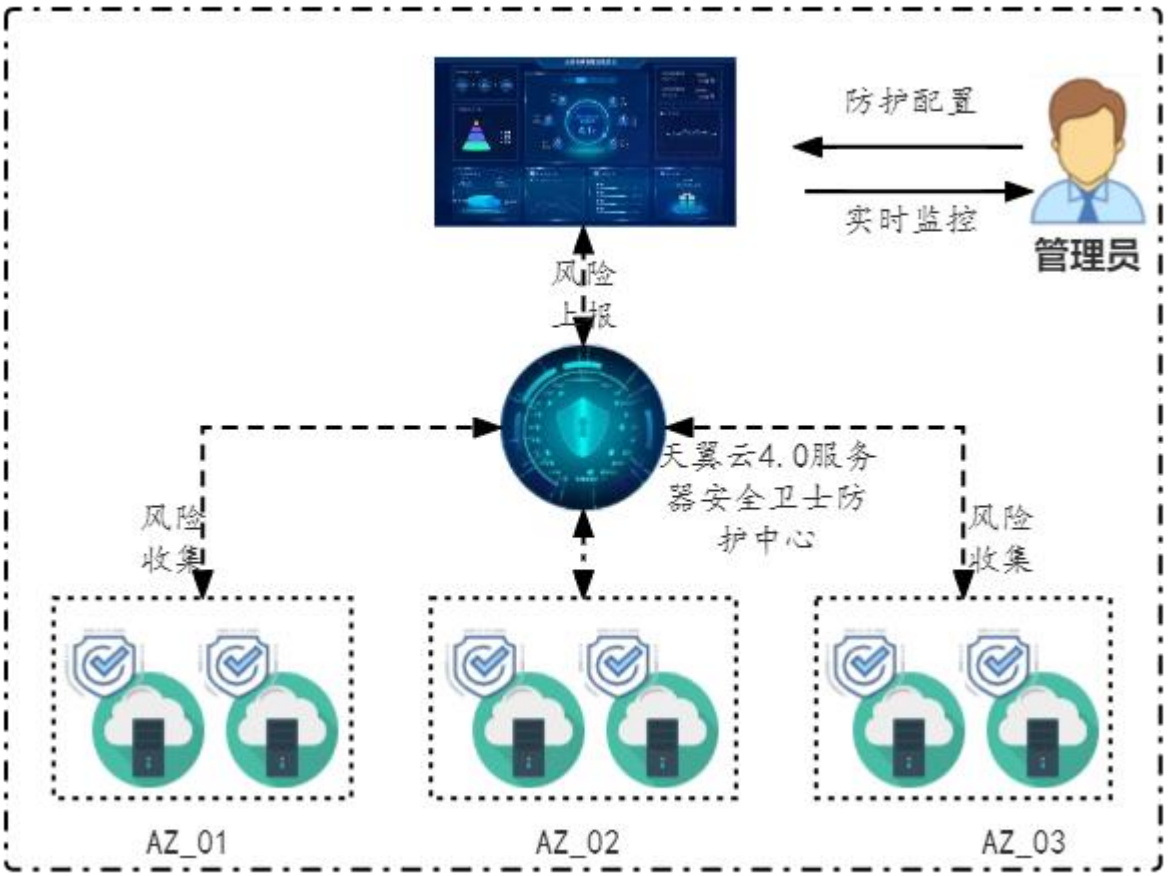
产品定义

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。

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

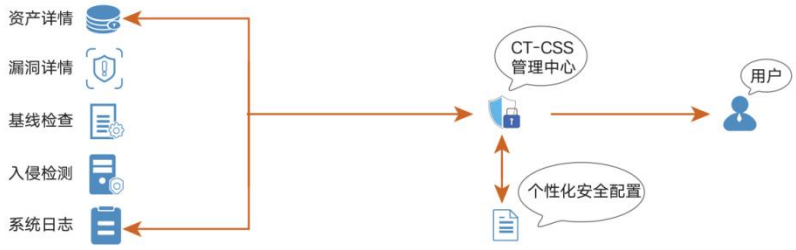
场景一：入侵行为检测

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。



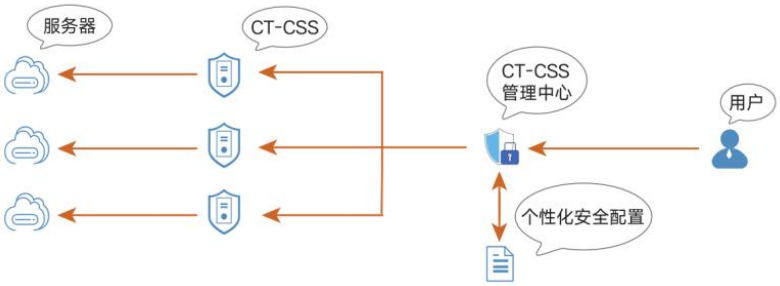
场景二：安全管理

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。



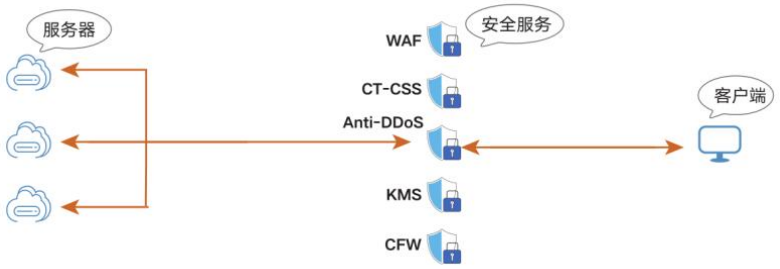
场景三：等保合规

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、企业版和增值服务。

不同规格功能差异为：基础版包含资产管理功能，入侵检测的异常登录、暴力破解功能，和漏洞扫描功能，企业版包含安全概览、资产管理、入侵检测、漏洞扫描、基线管理、病毒查杀、文件完整性保护、文件防勒索等功能，增值服务目前提供了网页防篡改（原生版）服务。

说明：

基础版只支持部分功能的检测能力和防护能力。若需对服务器进行全面防护，您需购买企业版防护。

若需要对云上网站提供网页防篡改防护，您需购买网页防篡改（原生版）增值服务。增值服务可单独购买或者与其他版本共同购买。文件防勒索、文件完整性保护目前处于公测阶段，企业版用户可优先体验。

一级菜单	二级菜单	功能概述	基础版	企业版	增值服务
安全概览	无	查看待处理风险、防护状态、风险趋势、实时动态	√	√	
资产管理	概览	查看资产概况、主机概况趋势图、服务器区域统计，和账号、端口、进程、软件应用的统计情况	√	√	
	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 4 种指纹的详细信息	仅支持查看端口和账户 2 种指纹信息	√	
	同步资产	实时同步主机资产	√	√	
入侵检测	异常登录	实时监控异常登录行为，识别非白名单 IP 登录	√	√	
	暴力破解	检测暴力破解行为，防止云主机因帐户破解被入侵	√	√	
	后门检测	发现主机创建的进程是否包含后门文件	×	√	
	可疑操作	实时检测当前系统中执行的高危命令	×	√	

一级菜单	二级菜单	功能概述	基础版	企业版	增值服务
	反弹 Shell	实时监控分析进程执行命令参数，检测反弹 Shell 行为	×	√	
	进程提权	监控分析进程的权限信息，发现异常提权行为	×	√	
漏洞扫描	无	漏洞情况统计	√	√	
		Linux 漏洞、windows 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	√	√	
		漏洞详情	√	√	
		白名单管理	√	√	
基线管理	基线检测	基线情况统计	×	√	
		一键检查	×	√	
		定时检查	×	√	
		基于基线名称的检测结果列表	×	√	
		基于服务器的检测结果列表	×	√	
		白名单管理	×	√	
		策略设置	×	√	
	弱口令检测	弱口令情况统计	×	√	
		一键检测	×	√	
		定时检测	×	√	
		基于服务器的检测结果列表	×	√	

一级菜单	二级菜单	功能概述	基础版	企业版	增值服务
病毒查杀	病毒查杀	对挖矿木马、蠕虫、勒索病毒等进行有效的检测	×	√	
文件完整性保护	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进行告警	×	√（公测）	
文件防勒索	诱饵防护	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	×	√（公测）	
	备份/恢复	提供数据备份与恢复能力，及时恢复被勒索加密的数据	×	×	√（公测） 仅支持华东1、华北2、西南1、华南2资源池
网页防篡改（原生版）	防护状态	查看防护的总体情况，帮助您实时的掌握所有云上网站被篡改的总体态势	×	×	√
	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	×	×	√
设置	配额管理	展示购买配额的情况	√	√	
	同步资产设置	同步资产周期设置	√	√	
	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	√	√	

1.7. 产品使用限制

支持的服务器

- 天翼云弹性云主机
- 天翼云 GPU 云主机
- 天翼云物理机

支持的系统

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

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

OS	支持的 OS 版本
Kylin 麒麟（X86_64）	Kylin V10 SP1 Kylin V10 SP2

支持的资源池

支持以下共 55 个资源池：上海 7、上海 36、南京 2、南京 3、南京 4、南京 5、杭州 2、杭州 7、芜湖 2、合肥 2、华东 1、九江、南昌 5、青岛 20、佛山 3、广州 6、武汉 3、武汉 4、武汉 41、华南 2、福州 3、福州 4、福州 25、郑州 5、长沙 3、长沙 42、郴州 2、海口 2、南宁 2、南宁 23、北京 5、华北 2、石家庄 20、呼和浩特 3、内蒙 6、太原 4、晋中、辽阳 1、西安 3、西安 4、西安 5、西安 7、中卫 2、中卫 5、兰州 2、西宁 2、乌鲁木齐 27、西南 1、西南 2-贵州、拉萨 3、昆明 2、重庆 2、成都 4、贵州 3、香港 1。

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 1C1G。

1.8. 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

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

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

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

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

2.2. 计费项

天翼云服务器安全卫士（原生版）根据您选择的规格进行计费。

计费说明

版本	计费公式	计费模式
基础版	免费	包年/包月
企业版	服务器台数* 标准资费* 购买时长	包年/包月

说明：

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

计费示例

计费场景：用户需要防护的服务器台数为 1 台，预估资源使用时长 1 个月。

计费示例：60 元/个/月* 1 个月* 6 折优惠=36 元

2.3. 优惠活动

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

2.4. 续订规则

2.4.1. 规则说明

续订限制说明

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

2.4.2. 自动续订规则

为避免由于未及时对配额采取续订操作，配额被到期冻结或超期释放，客户购买包月包年产品后，可设置开通自动续订。开通自动续订后，系统将在配额到期前自动续订，无需客户再手动操作。

适用范围： 自动续订仅针对采用包月、包年计费模式的资源。已到期资源不支持设置/修改自动续订。

开通、变更、关闭自动续订

用户在续订管理页可开通自动续订功能，变更自动续约周期，或关闭自动续订。

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

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

自动续订周期

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

自动续订价格

自动续订下单扣费时按当时的标准价自动续订，续订 1 年或以上可享受包年折扣。

0 元、秒杀等特价促销活动产品订购后，自动续订下单扣费时将恢复标准价。

预付费用户暂不支持代金券支付，仅支持余额支付，用户需确保账户余额充足。

自动续订扣费规则

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

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

自动续订和手动续订的关系

在 7 天或更短时间内到期的资源，或已到期资源，需手动续订，无法设置自动续订。

开通自动续订功能后，也可以进行手动续订。在自动续订扣费日前进行手动续订，系统将按照手动续订后的到期日期，重新计算下一次自动续订的下单时间。

2.5. 退订规则

退订规则见：退订规则说明。

3. 快速入门

3.1. 注册天翼云账号

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

3.2. 开通服务器安全卫士（原生版）

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

方法一：

1. 登录天翼云官网。
2. 选择“产品 > 安全及管理 > 网络安全 > 服务器安全卫士（原生版）”，进入服务器安全卫士（原生版）产品详情页，选择“管理控制台”。

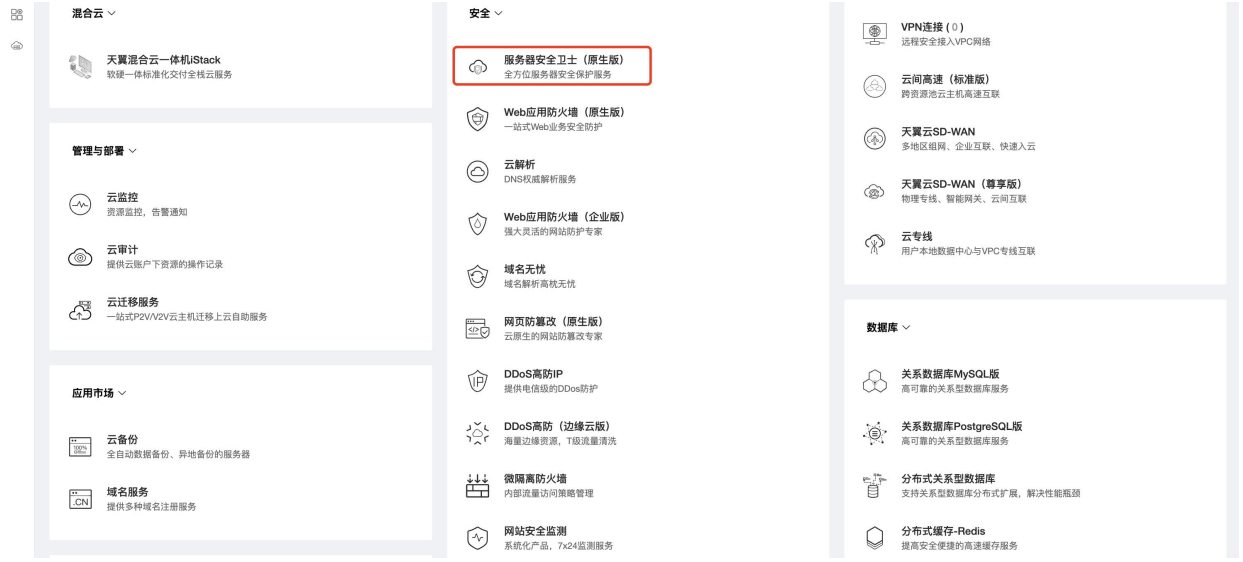
3. 进入服务器安全卫士（原生版）管理控制台后，弹出下方“服务开通申请”对话框。

4. 阅读《天翼云服务器安全卫士（原生版）服务协议》后，勾选"我已阅读并同意签署《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，如下图所示。

方法二：

1. 在天翼云官网首页选择"控制中心"，如下图所示。

2. 在控制中心产品服务列表，选择“安全 > 服务器安全卫士（原生版）”。



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“我已阅读并同意签署《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，如下图所示。

3.3. 购买防护配额

1. 点击“配额管理”页面右上方“购买服务器安全卫士（原生版）”，进入到服务器安全卫士（原生版）产品购买页面。

2. 选择购买版本、防护服务器台数、购买时长、自动续订，勾选“我已阅读，理解并同意《天翼云服务器安全卫士（原生版）服务协议》”，点击“立即购买”按钮。

3. 购买成功后即可在“配额管理”页面查看已购买的企业版配额，如下图所示。

3.4. 安装 Agent

1. 点击“配额管理”页面上的“安装 Agent”按钮，跳转至“资产管理 > 服务器列表”页面。

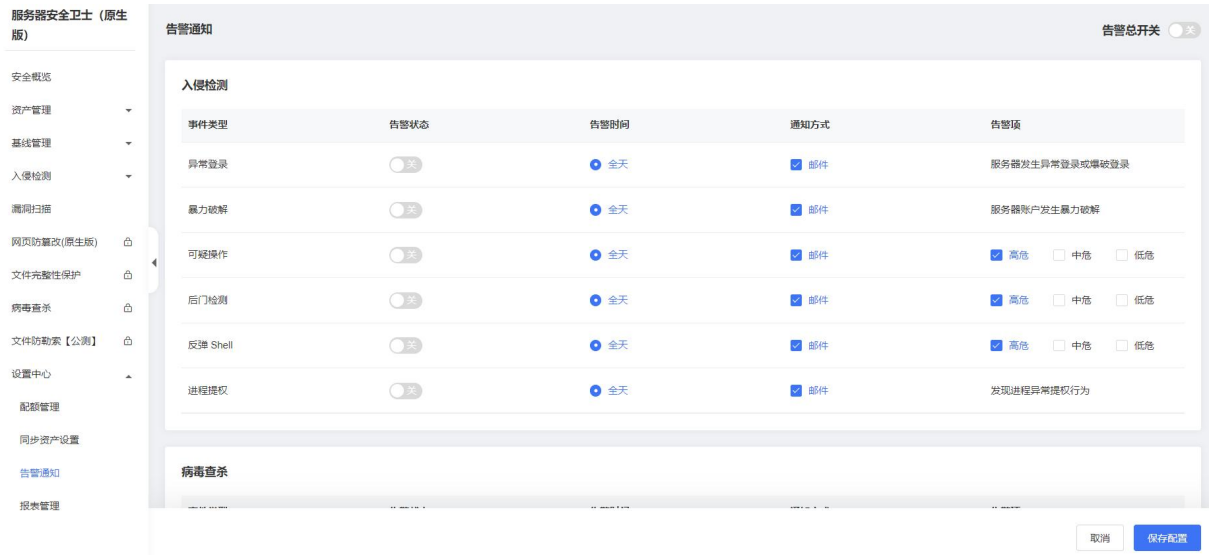
2. 查看服务器列表中的“Agent 状态”：
   - 若状态为“在线”，则本台服务器已安装 Agent 且 Agent 服务正常。
   - 若状态为“离线”或“错误”，则本台服务器已安装 Agent，但 Agent 与服务器通信异常。
   - 若状态为“未激活”，则本台服务器未安装 Agent 或 Agent 未激活。
3. 对于“Agent 状态”为“离线”、“错误”或“未激活”的服务器，需要为该服务器安装 Agent。

Linux 系统安装命令如下图：

Windows 系统安装命令如下图：

3.5. 设置告警通知

1. 在左侧导航选择“设置中心 > 告警通知”，进入告警通知页面，如下图所示。



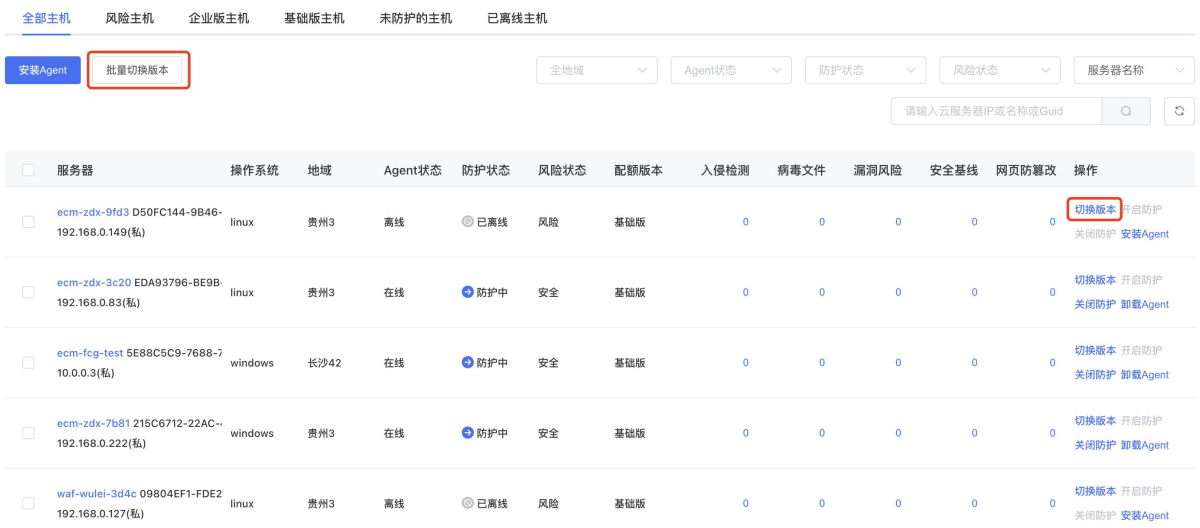
2. 对各个功能的告警状态、告警时间、通知方式和告警项进行选择。

   告警状态默认关闭，告警时间默认全天，通知方式默认邮件，漏洞告警项默认超高危、超危和高危。

3.6. 切换版本

1. 点击“配额管理”页面上的“切换版本”按钮，跳转至“资产管理 > 服务器列表”页面，如下图所示。

   查看服务器配额版本情况，配额版本为“基础版”或“企业版”，不同版本差异具体见产品规格章节。



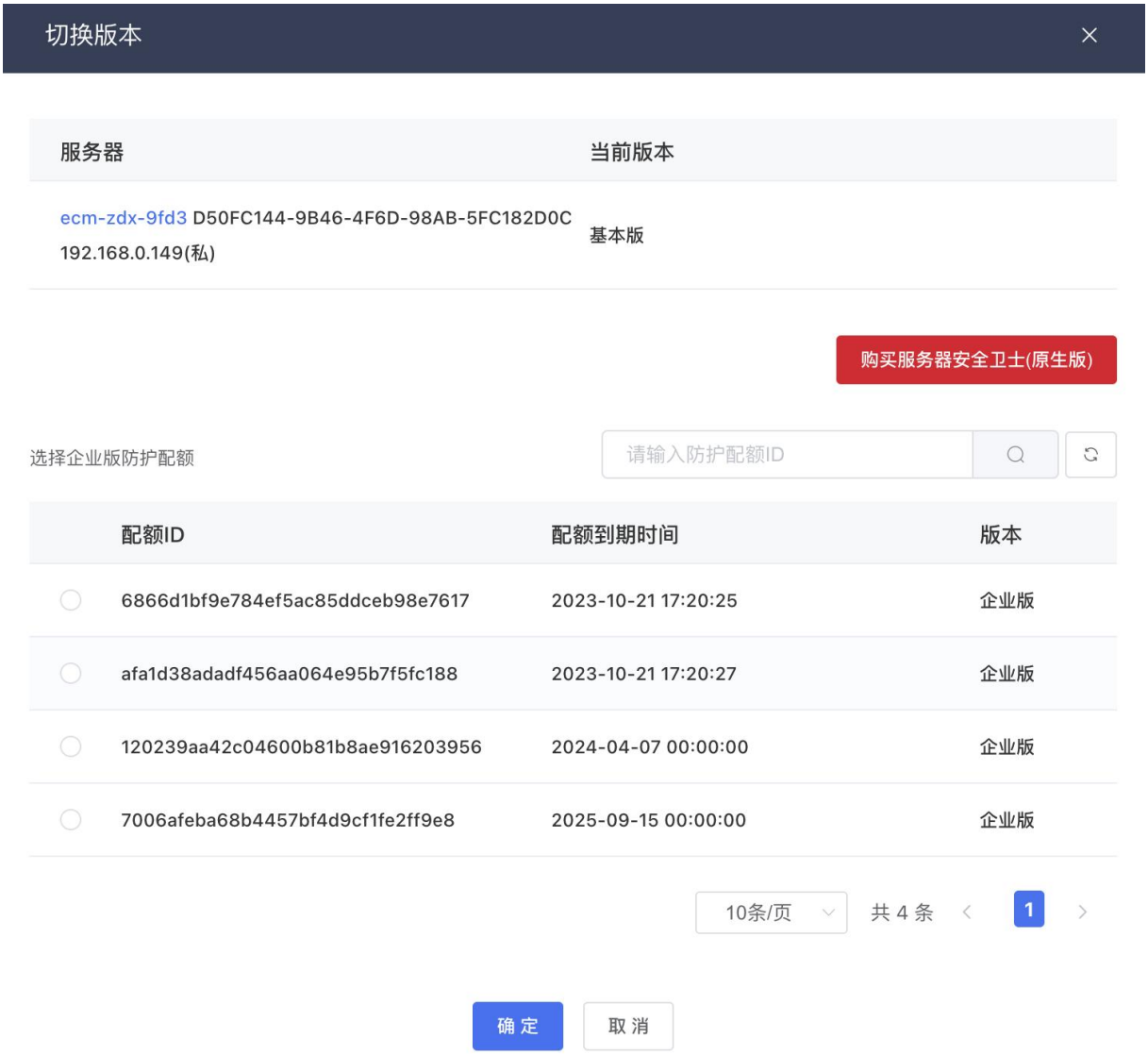
2. 您可对需要防护的服务器进行“切换版本”。选择您需要切换版本的服务器，可进行单台服务器的配额版本切换，也可以选择多台服务器进行批量切换。

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

   注意：

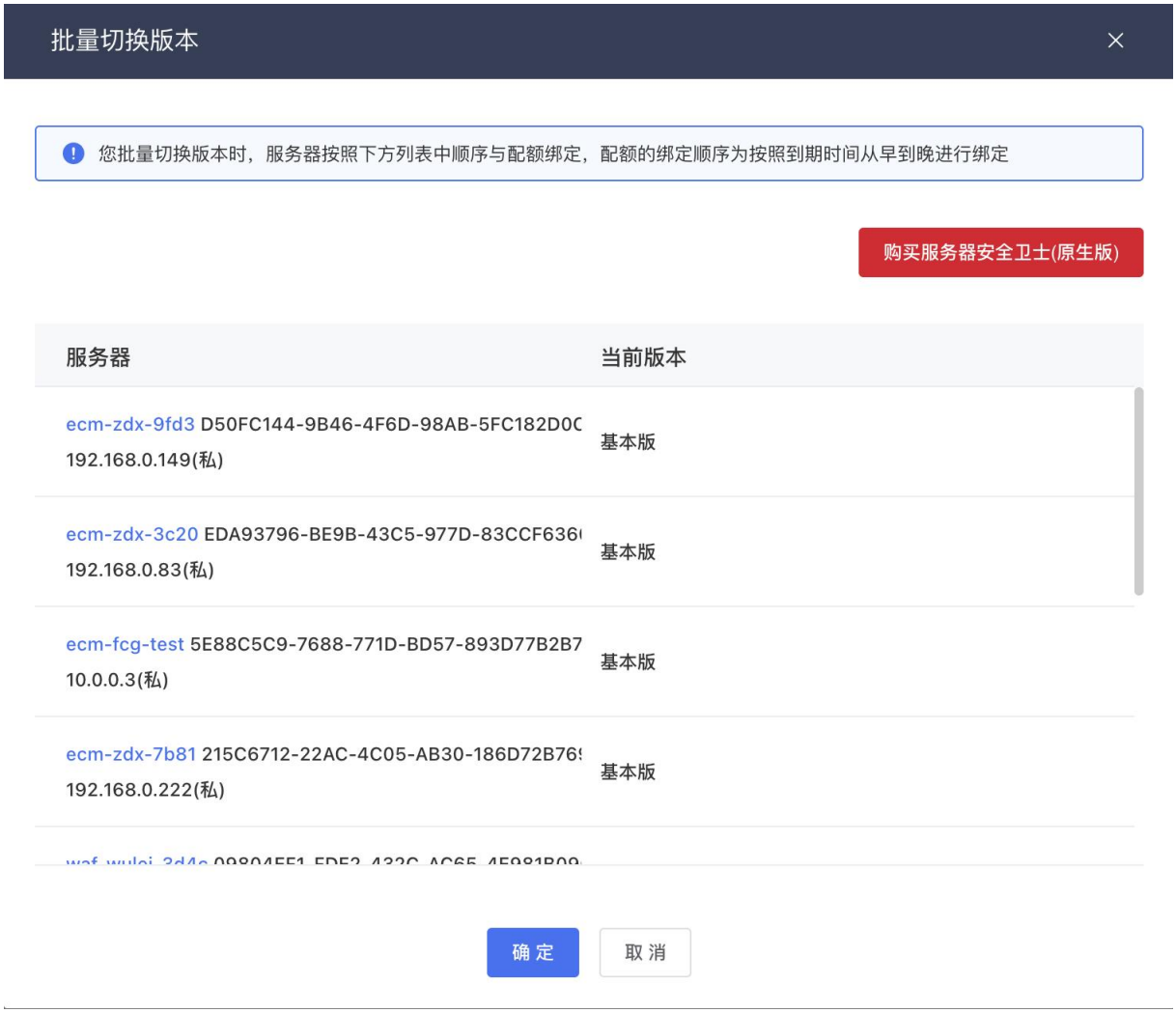
   企业版防护服务器不可切换为基础版防护。

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



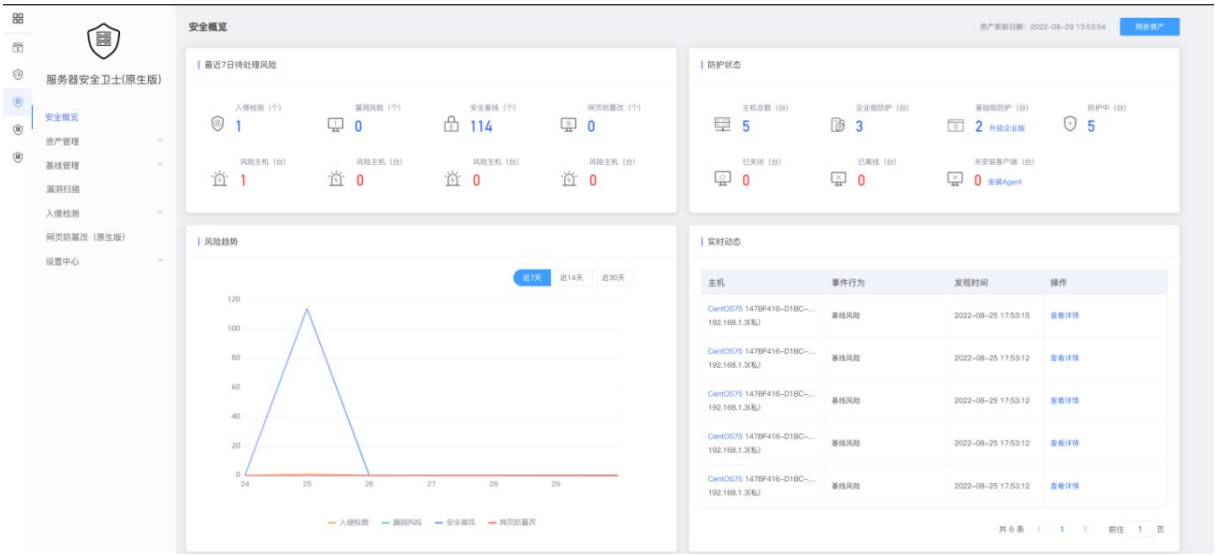
4. 可进行批量切换，在服务器列表中选择需要切换的服务器，点击“批量切换版本”，跳转至下方页面，点击“确定”后，切换为企业版防护，配额和服务器按照顺序一一匹配即可。

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

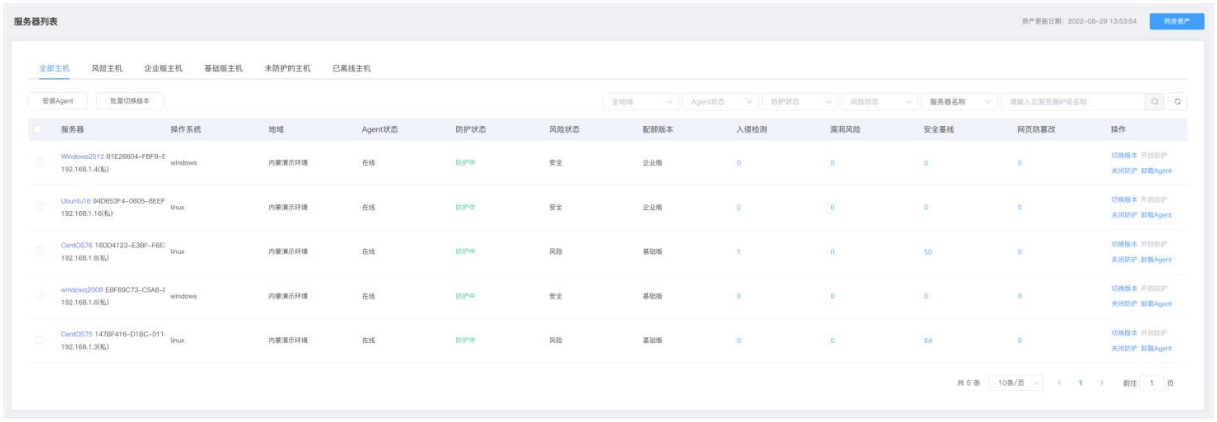


3.7. 查看检测结果

1. 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。



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



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

4. 用户指南

4.1. 计费操作

4.1.1. 订购

以下为服务器安全卫士（原生版）的购买流程。

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

方法一

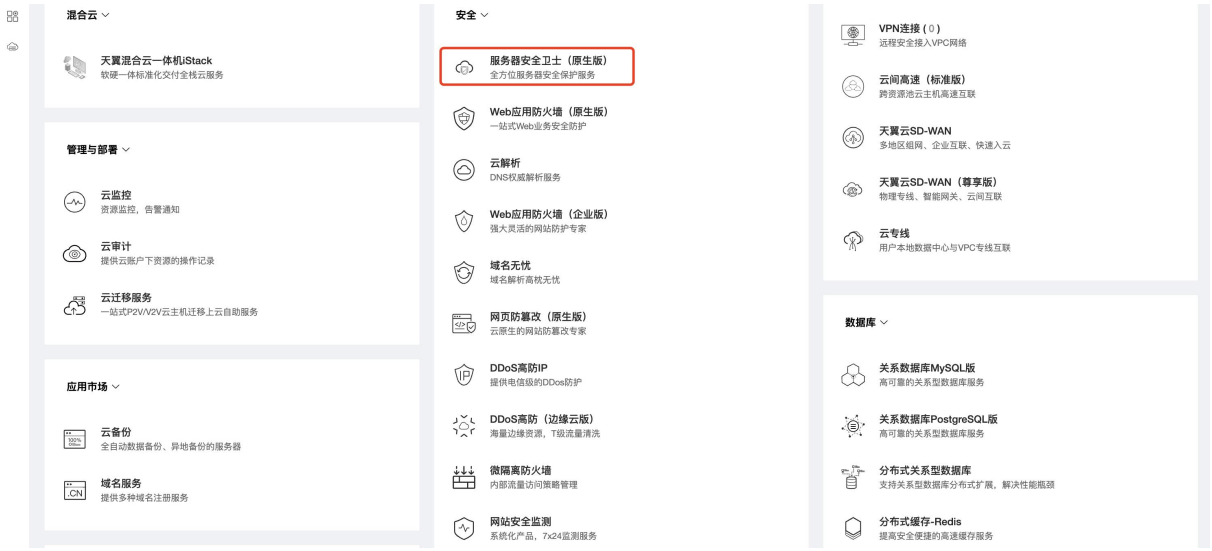
1. 进入服务器安全卫士（原生版）产品详情页。

2. 单击“立即开通”，进入到服务器安全卫士（原生版）产品购买页面。

3. 选择购买版本、防护服务器数量、购买时长、自动续订，勾选“我已阅读，理解并同意《天翼云服务器安全卫士（原生版）协议》”，点击“立即购买”，购买成功后即可在“配额管理”页面查看已购买的企业版配额，如下图所示。

方法二

1. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（原生版）”。



2. 进入服务器安全卫士（原生版）控制台，弹出下方“服务开通申请”对话框。

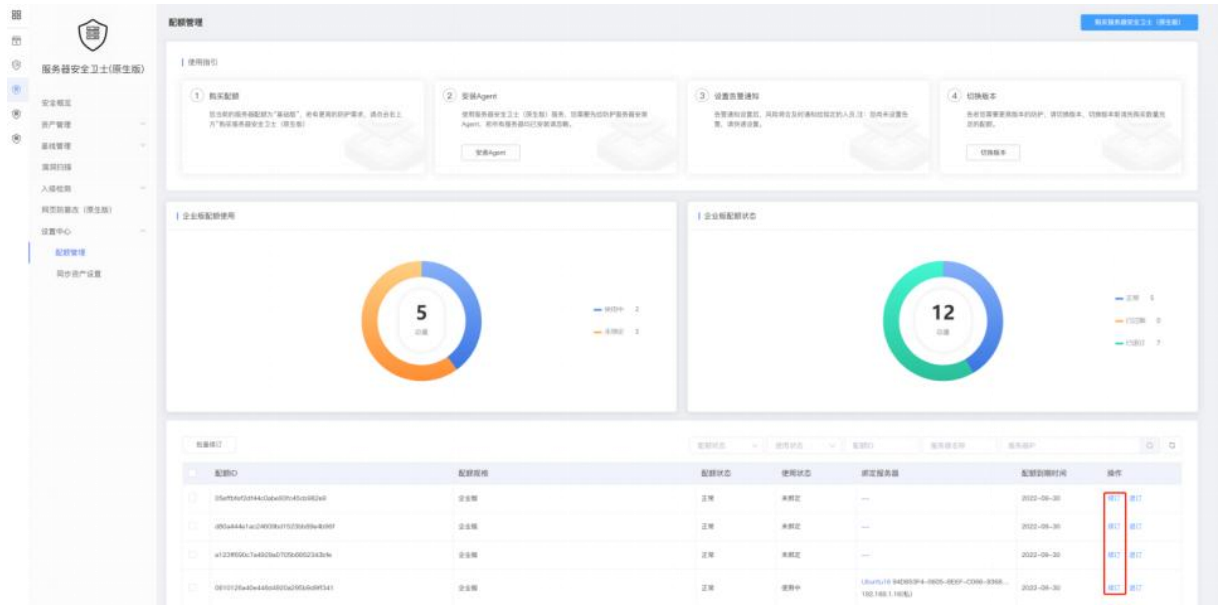
3. 阅读《天翼云服务器安全卫士（原生版）协议》后，勾选“我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）服务协议》”，点击“同意”按钮，即可开通服务器安全卫士（原生版）服务，如下图所示。

4. 点击页面右上方“购买服务器安全卫士（原生版）”，进入到服务器安全卫士（原生版）产品购买页面。

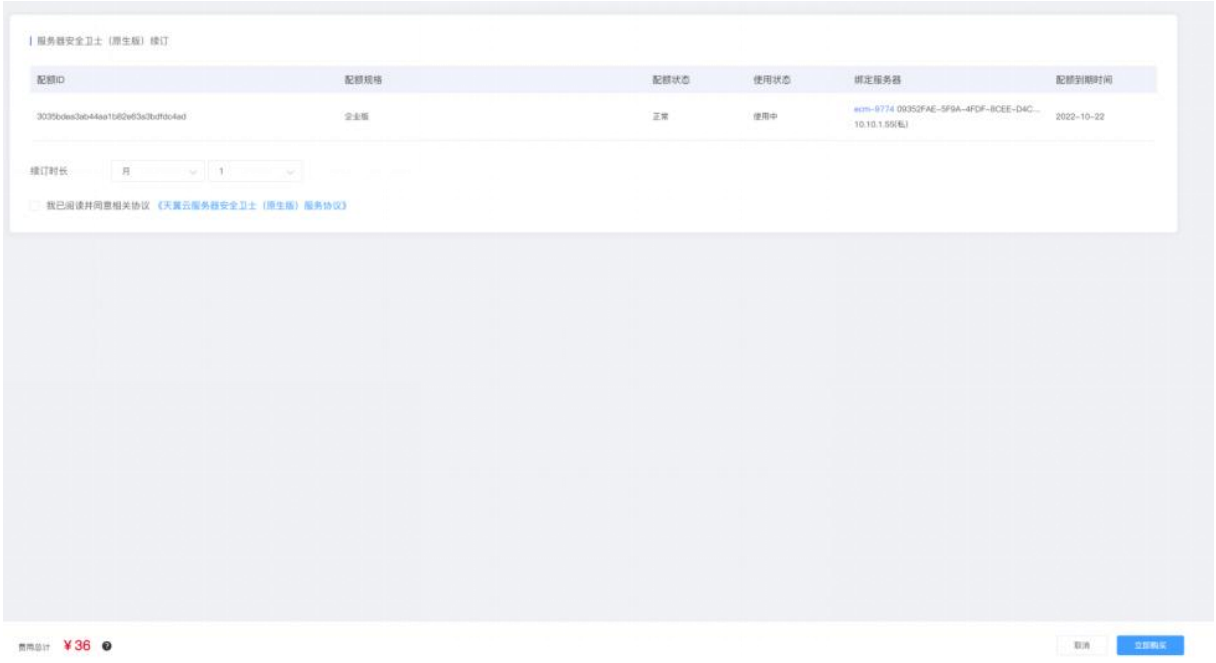
5. 选择购买版本、防护服务器台数、购买时长、自动续订，勾选“我已阅读，理解并同意《天翼云服务器安全卫士（原生版）服务协议》，点击“立即购买”按钮，购买成功后即可在“配额管理”页面查看已购买的企业版配额，如下图所示。

4.1.2. 手动续订

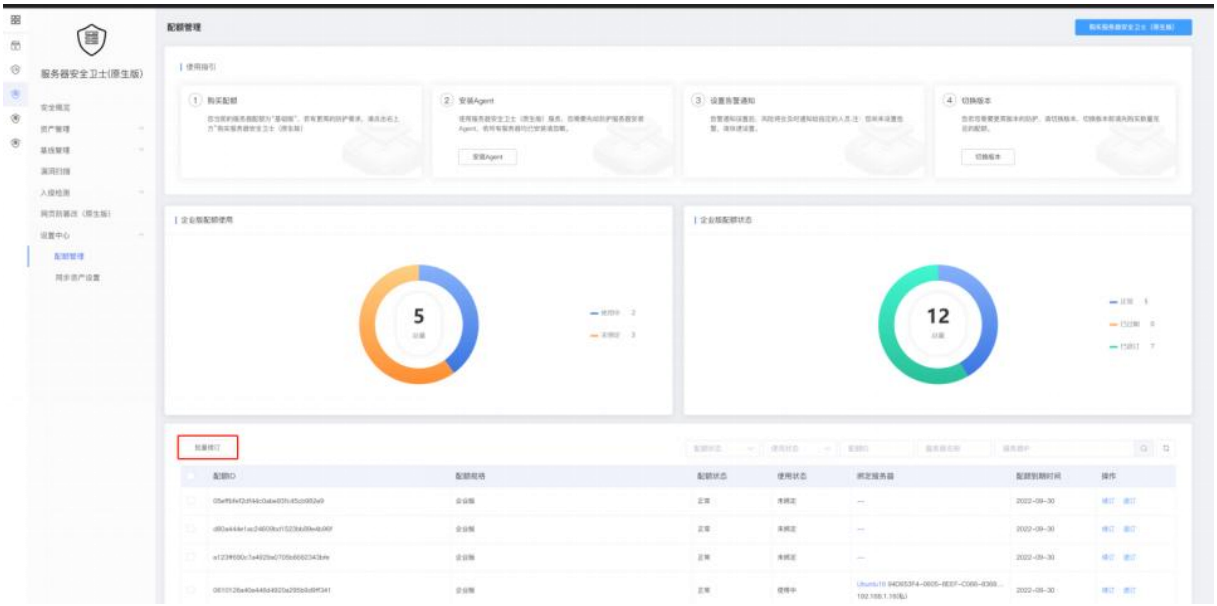
1. 在“设置中心 > 配额管理”中查看您已经订购的配额，选择所需续订的配额，点击“续订”，如下图所示。



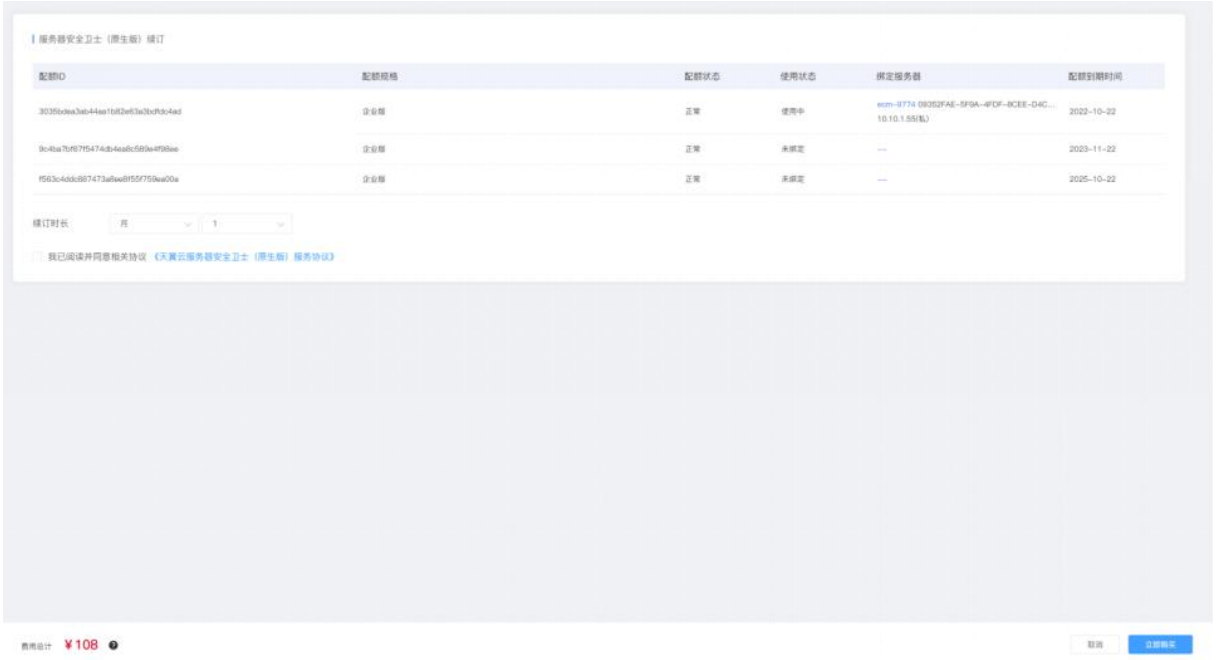
2. 在下图续订页面中，选择续订时长，勾选“我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）服务协议》”后，点击“立即购买”即可进行续订。当续订周期达到 1 年或以上时，续订单将可享受包年折扣，续订金额显示折后价。



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



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



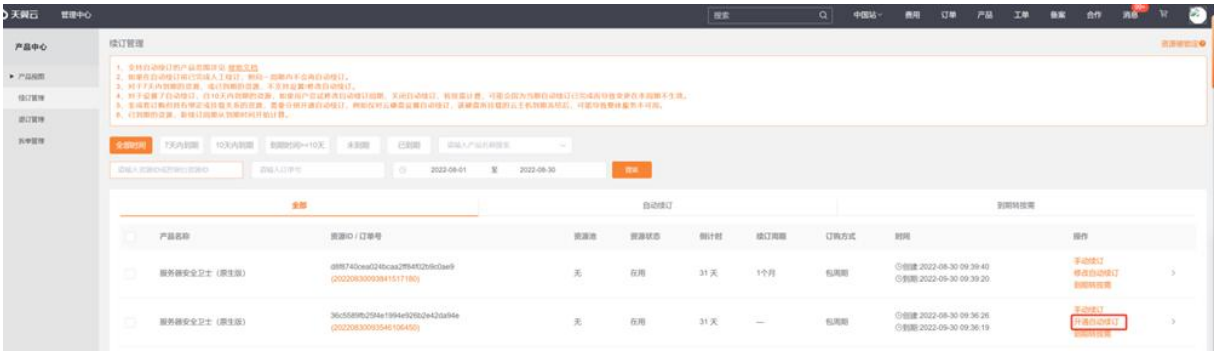
4.1.3. 自动续订

开通自动续订

1. 进入“续订管理”页面。
2. 设置查询条件。

   可综合利用到期时间、产品类型、是否开通自动续订查询资源。

   由于自动续订两次下单时间为到期前 10 天和前 7 天，建议您选择“到期时间≥10 天”，“未开通自动续订”的服务器安全卫士（原生版）。
3. 在资源页面找到待续订的资源，单击操作列的“开通自动续订”，如下图所示。



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

修改自动续订周期

1. 进入“续订管理”页面。
2. 在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”。

3. 拖动“续订周期”可修改自动续订周期。

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

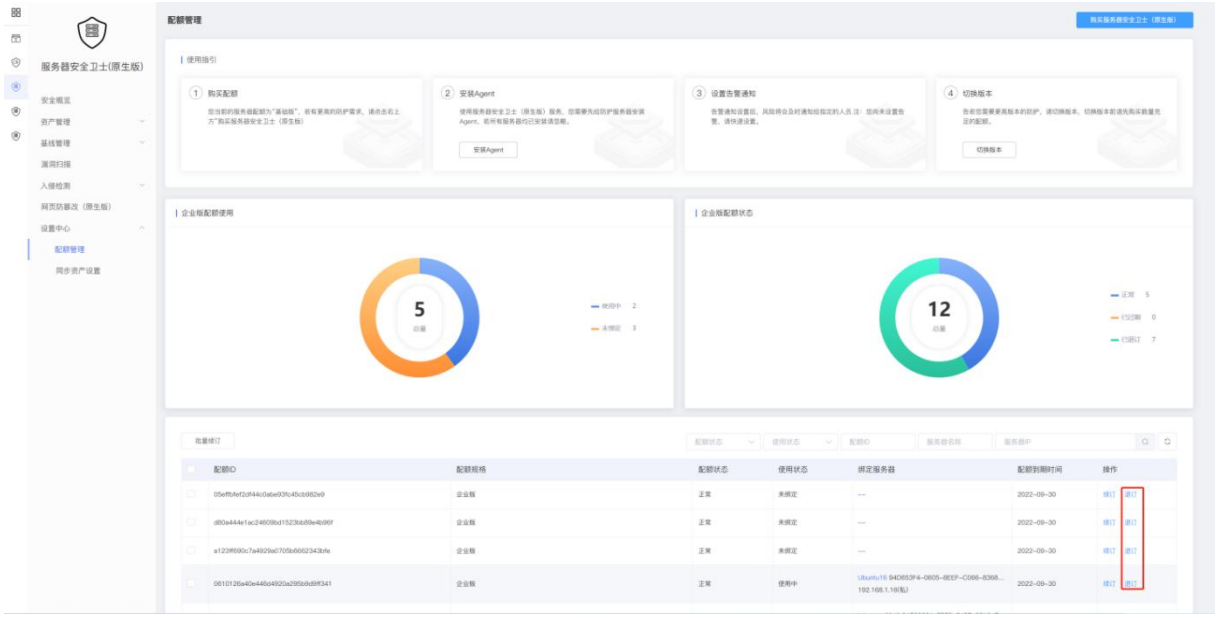
关闭自动续订

1. 进入“续订管理”页面。
2. 在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”。

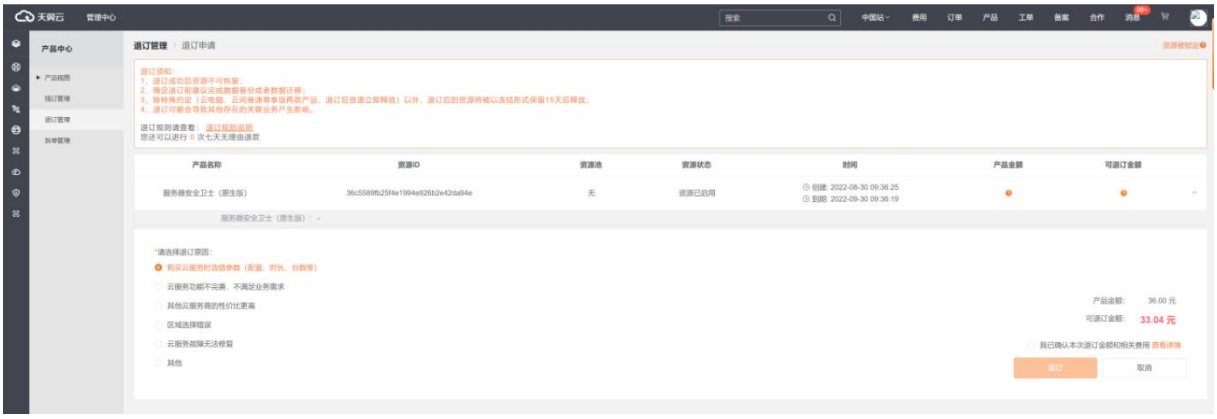
3. 点击“自动续订”后方的关闭/开通按钮，单击“确定提交”。

4.1.4. 退订

1. 在“设置中心 > 配额管理”中查看您已经订购的配额，选择所需退订的配额，点击“退订”，如下图所示。



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



4.2. 安全概览

4.2.1. 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->异常登录”首页；风险主机统计 7 日内有入侵风险的服务器，包括所有的云主机和物理机，同一台服务器有不同的入侵风险时不重复叠加。
- **漏洞风险|风险主机**：展示 7 日内所有未操作的漏洞风险个数，点击数字时会跳转到漏洞扫描首页；风险主机统计 7 日内有漏洞风险的服务器，包括所有的云主机和物理机，同一台服务器有不同的漏洞风险时不重复叠加。
- **安全基线|风险主机**：展示 7 日内所有未操作的安全基线个数，包括基线检测和弱口令检测个数之和，点击数字时会跳转到基线检测首页；风险主机统计 7 日内有基线风险的服务器，包括所有的云主机和物理机，同一台服务器有不同的基线风险时不重复叠加。
- **网页防篡改|风险主机**：若您订购了网页防篡改（原生版），展示 7 日内所有未忽略的文件异常的事件数，点击数字时会跳转到服务器安全卫士检测首页；风险主机统计 7 日内有网页篡改事件的服务器，包括所有的云主机和物理机。若您未订购网页防篡改（原生版），则统计数字均显示为 0。

4.2.2. 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“服务器列表-全部主机”页面。主机总数和以下几种状态的主机数相加总和相等。
- **企业版防护**：展示您使用企业版规格配额防护的主机数量，点击数字时会跳转至“服务器列表-企业版主机”页面。

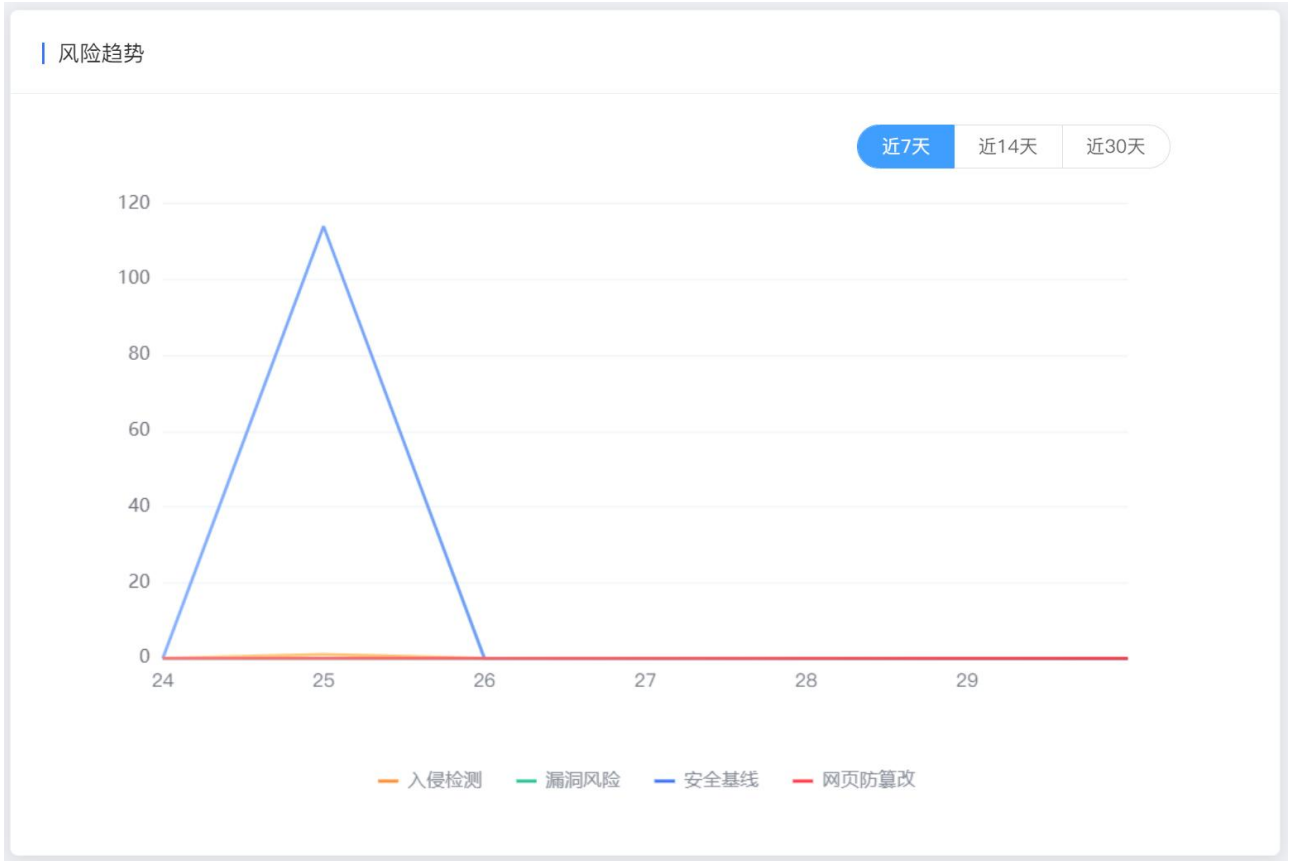
- **基础版防护**：展示您使用基础版规格配额防护的主机数量，点击数字时会跳转至“服务器列表-基础版主机”页面。
- **防护中**：服务器防护状态为“防护中”的服务器数量统计，点击数字时会跳转至“服务器列表-已防护主机”页面。
- **已离线**：服务器防护状态为“已离线”的数量统计，点击数字时会跳转至“服务器列表-已离线主机”页面。
- **已关闭**：服务器防护状态为“已关闭”的数量统计，点击数字时会跳转至“服务器列表-已关闭主机”页面。
- **未防护**：服务器防护状态为“未防护”的数量统计，点击数字时会跳转至“服务器列表-未防护主机”页面。

Linux 系统安装命令如下图：

Windows 系统安装命令如下图：

4.2.3. 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。

4.2.4. 最近 7 日风险动态

如下图所示，最近 7 日风险动态风险趋势展示您所有服务器的未处理的风险动态。

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

4.3. 资产管理

4.3.1. 资产概览

资产概况

如下图所示，资产概况为您展示服务器和资产指纹的统计情况。

- **主机台数**：您服务器的总台数，单击蓝色数字时跳转到“服务器列表”页；
- **端口**：展示所有服务器所有已使用端口的数量之和，单击蓝色数字时跳转至“资产指纹-端口”页；
- **账号**：展示所有服务器所有账号的总数量，单击蓝色数字时跳转至“资产指纹-账号”页；
- **进程**：展示所有服务器所有进程的数量之和，单击蓝色数字时跳转至“资产指纹-进程”页；
- **软件**：展示所有服务器所有软件应用的数量之和，单击蓝色数字时跳转至“资产指纹-软件应用”页。

主机概况趋势图

如下图所示，主机概况趋势图为您展示服务器的防护情况统计折线图。

分近 7 天、近 14 天、近 30 天 3 个选项，默认展示近 7 天。

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

为您展示服务器总台数、未防护台数、离线台数、风险台数、防护关闭台数统计趋势。

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

服务器区域统计 Top5

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

端口 TOP5

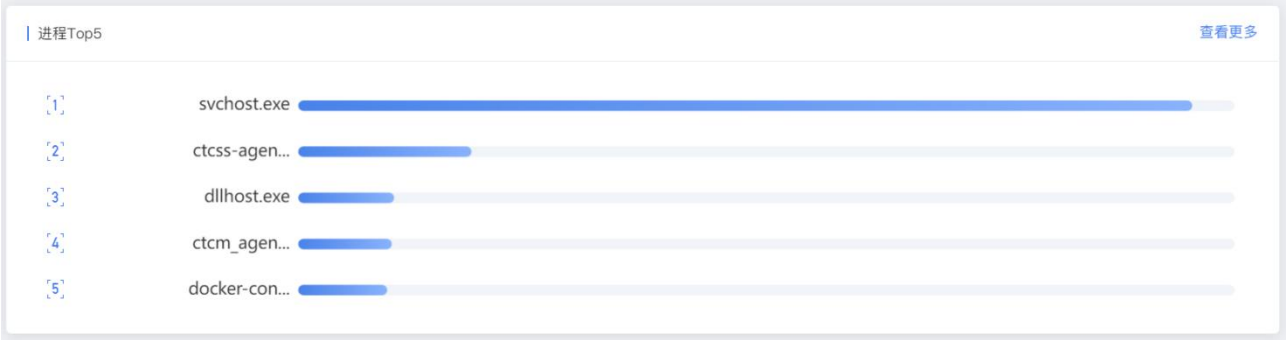
如下图所示，端口 Top5 为您展示服务器开放端口的统计情况排名 TOP5，点击更多时，会跳转至“资产指纹-端口”页面。

账号 TOP5

如下图所示，账号 Top5 为您展示服务器账号的统计情况排 TOP5，点击更多时，会跳转至“资产指纹-账号”页面。

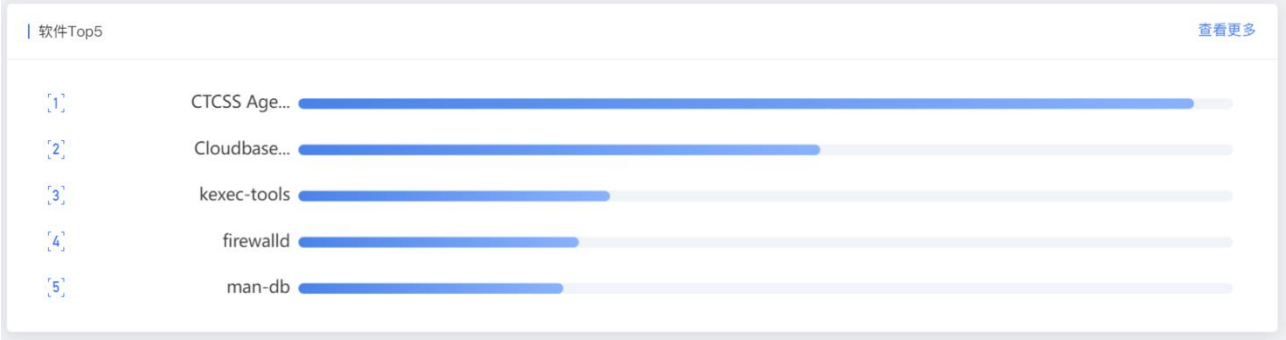
进程 TOP5

如下图所示，进程 Top5 为您展示服务器运行的进程统计情况排名 TOP5，点击更多时，会跳转至“资产指纹-进程”页面。



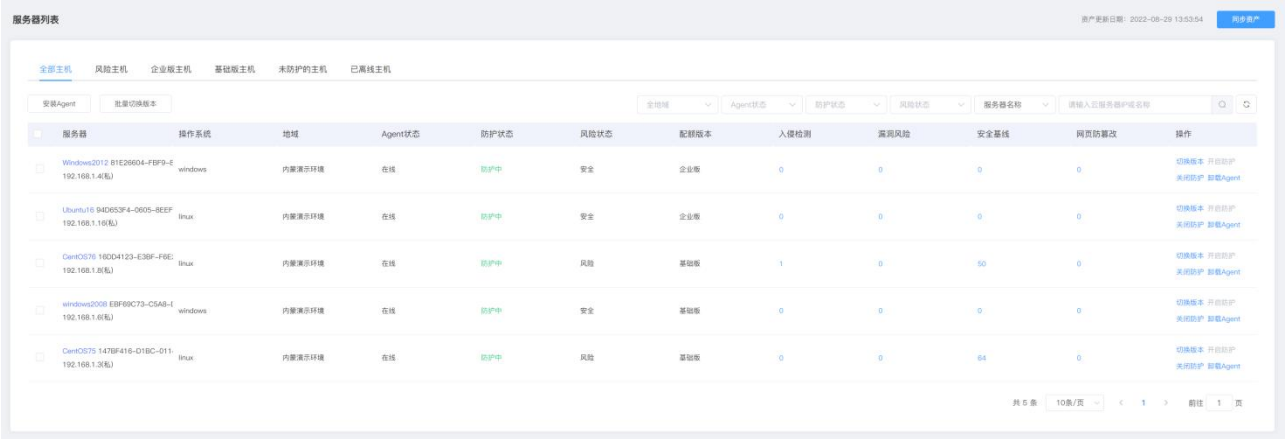
软件 TOP5

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



4.3.2. 服务器列表

服务器列表如下图所示：



全部主机

该页面为您展示全部服务器的情况。已销毁的服务器不再展示在列表中。

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

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

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

Agent 状态	说明
错误	Agent 控制通路连接异常。

防护状态	说明
防护中	表明该服务器处于正常防护中，此时 Agent 状态为在线且已经为该台服务器开启防护。
已离线	表明该服务器与 Agent 通信异常，此时 Agent 状态为离线或错误。
已关闭	表明该服务器已经关闭防护，此时 Agent 状态为在线且已经为该台服务器关闭防护。
未防护	表明该服务器已经关闭防护，此时 Agent 状态为未激活。

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

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

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

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

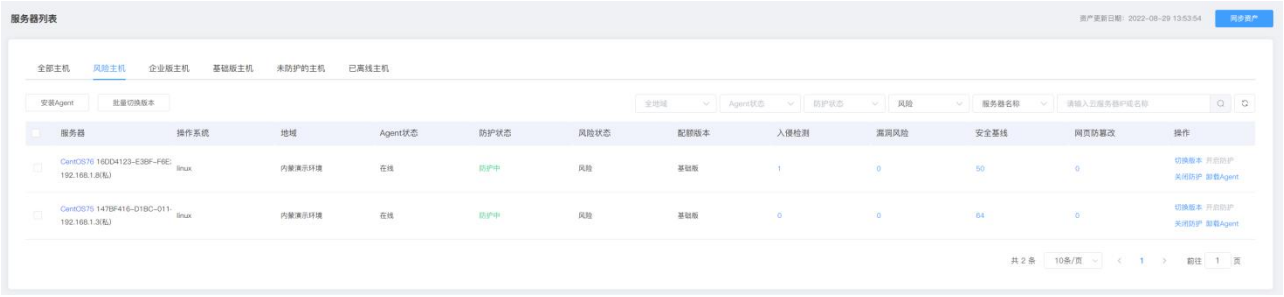
Linux 系统安装命令如下图：

Windows 系统安装命令如下图：

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

风险主机

如下图展示，风险主机为您展示风险状态为“风险”的服务器。



企业版主机

如下图展示，企业版主机为您展示配额规格为“企业版”的服务器。

基础版主机

如下图展示，基础版主机为您展示配额规格为“基础版”的服务器。

未防护的主机

如下图展示，未防护的主机为您展示防护状态为“未防护”的全部服务器。

已离线主机

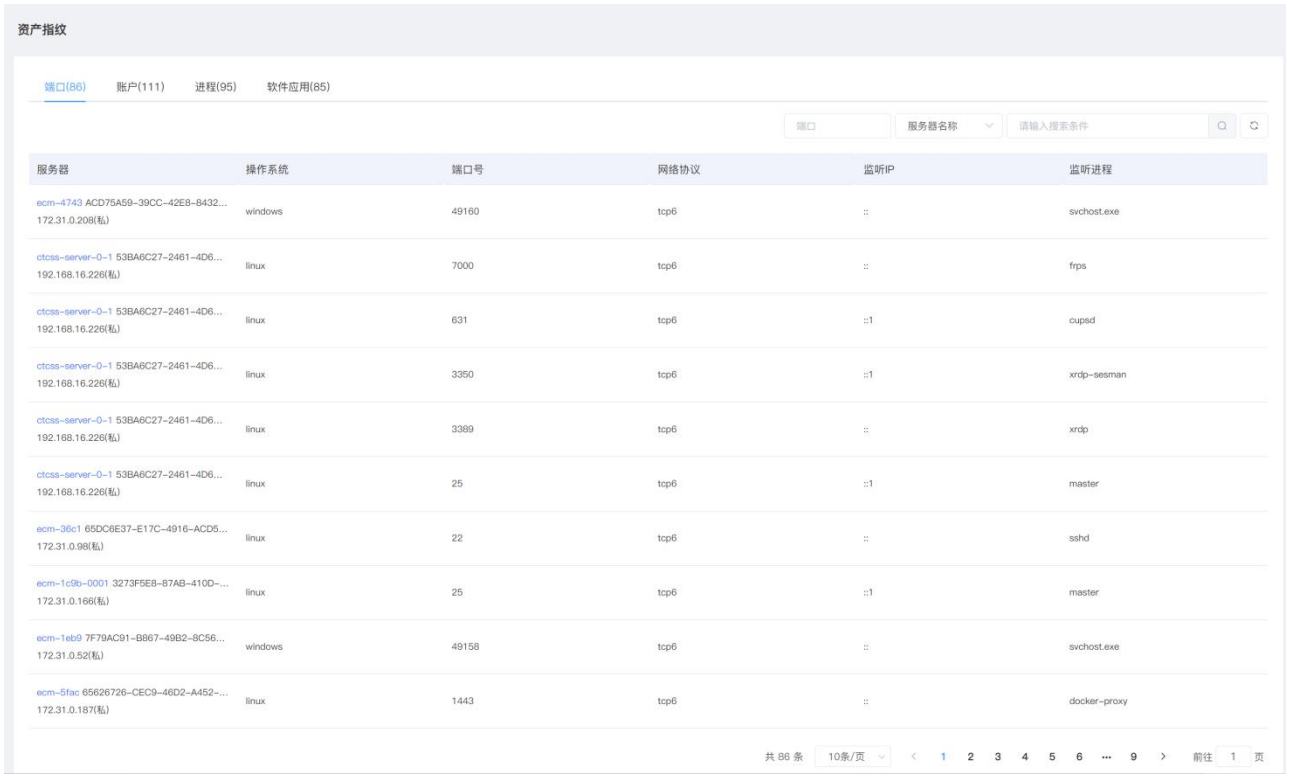
如下图展示，已离线主机为您展示防护状态为“已离线”的服务器。

4.3.3. 资产指纹

端口

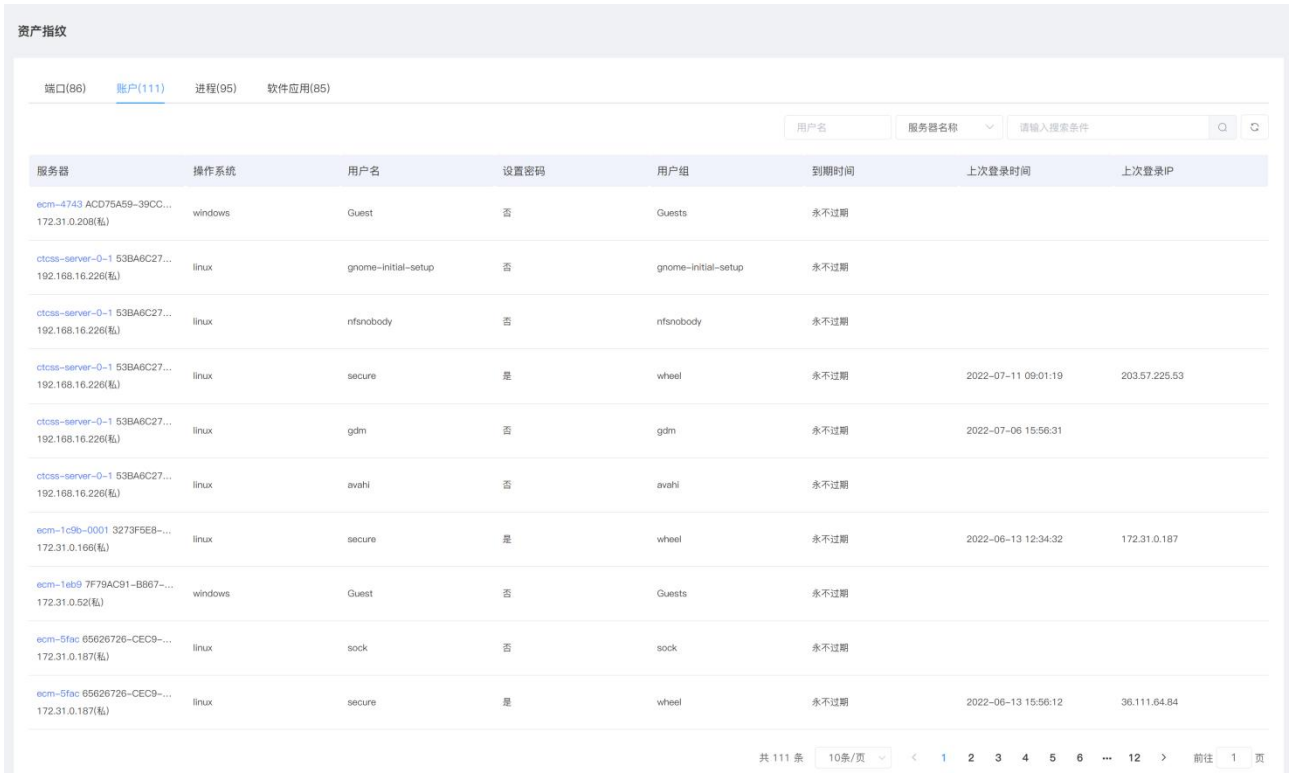
按服务器展示端口信息，包括以下字段：服务器、操作系统、端口、网络协议、监听 IP、监听进程、进程号。可以按照端口号、服务器名称、服务器 IP 进行搜索。

服务器包括服务器名称、UUID、私网 IP 和公网 IP。



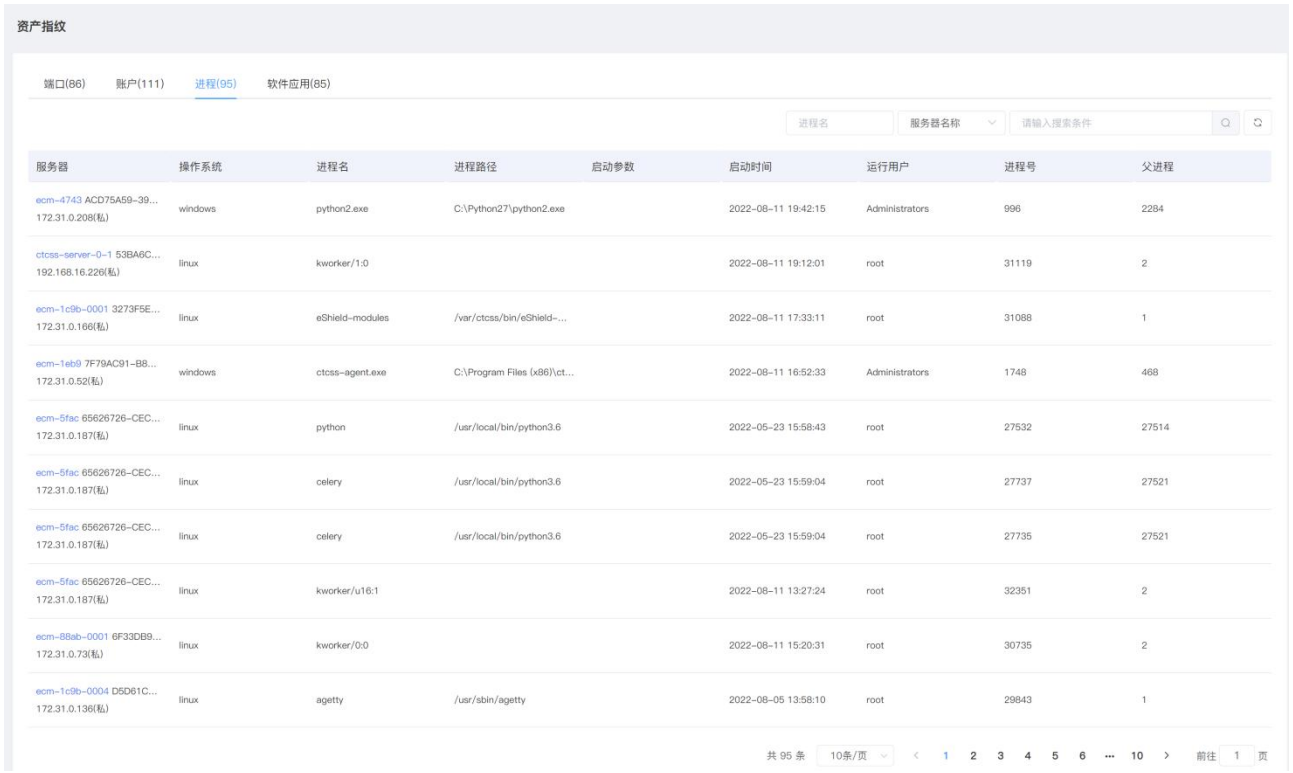
账号

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



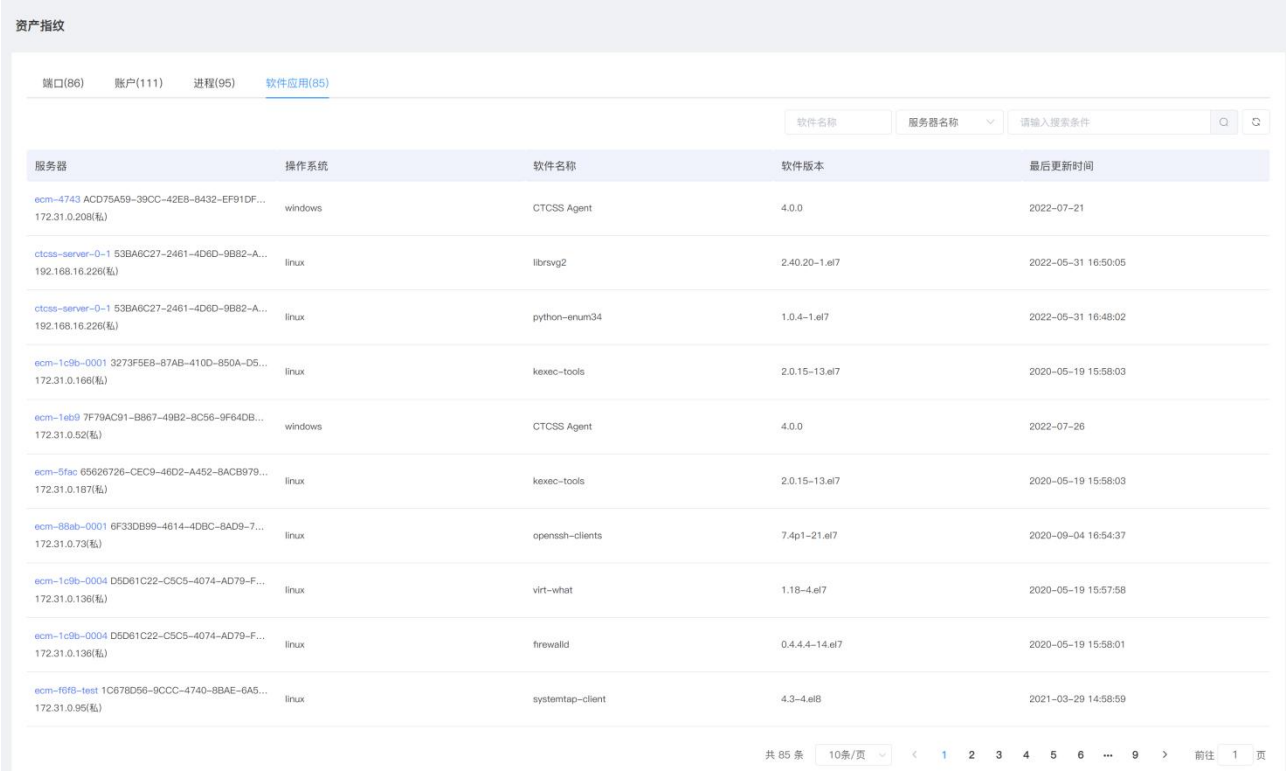
进程

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



软件

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

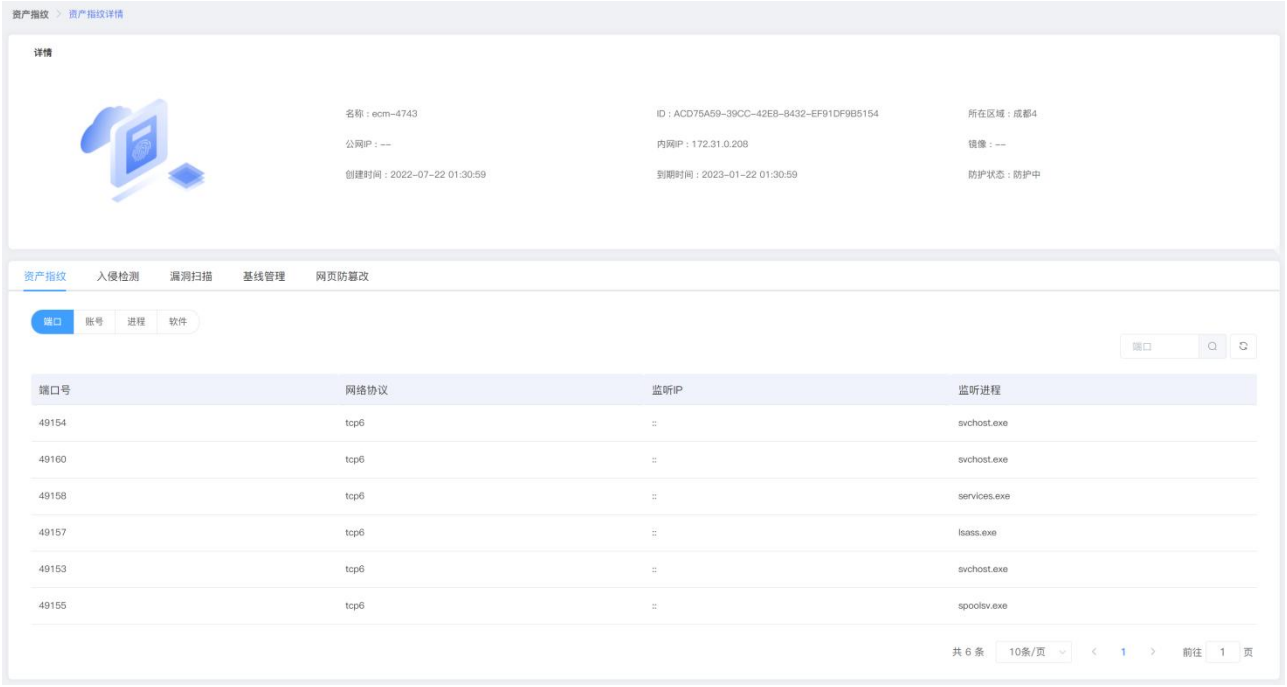


4.3.4. 资产详情

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

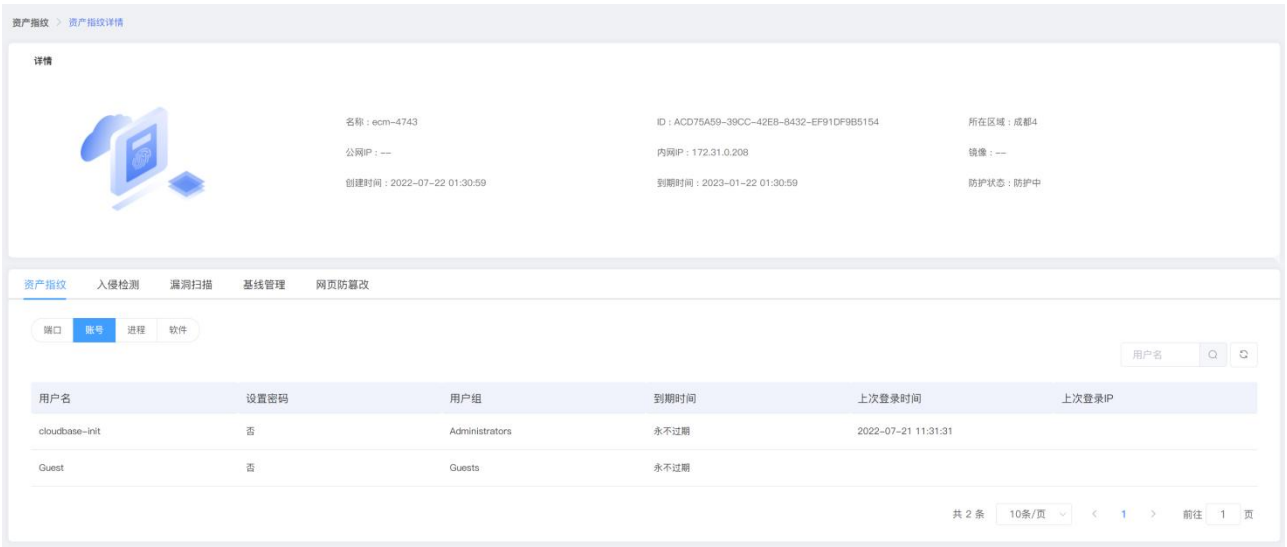
端口

如下图所示，展示该台服务器开放的端口详情。



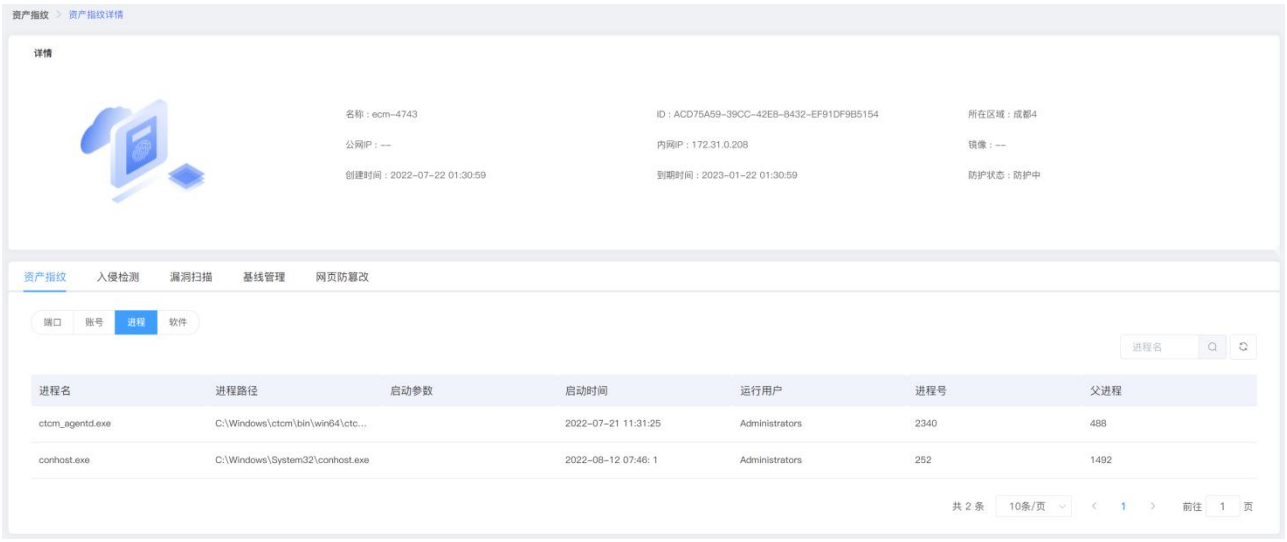
账号

如下图所示，展示该台服务器的账号详情。



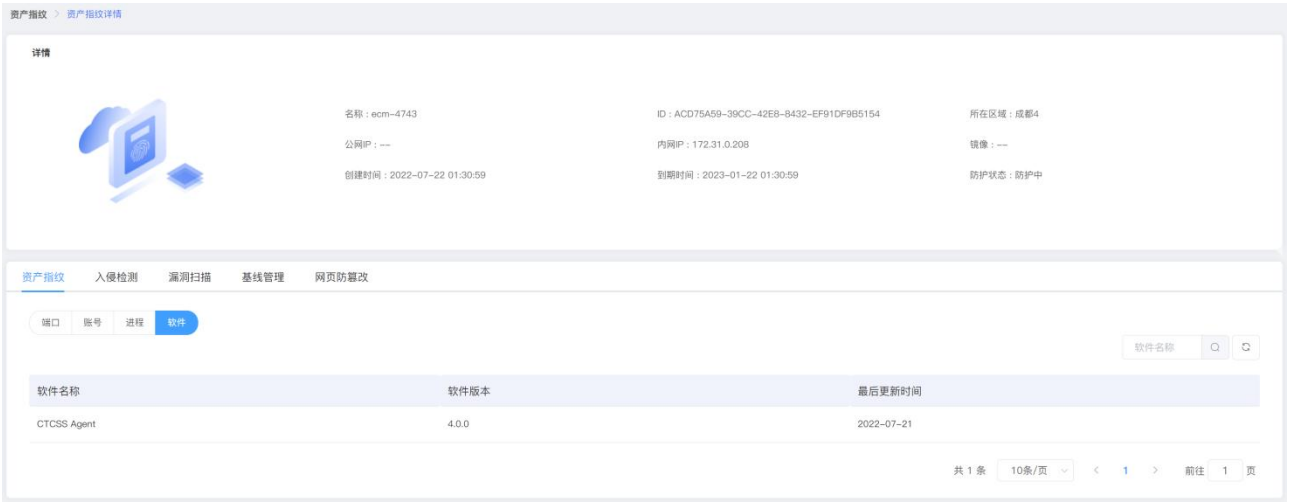
进程

如下图所示，展示该台服务器的进程详情。



软件

如下图所示，展示该台服务器的软件详情。



异常登录

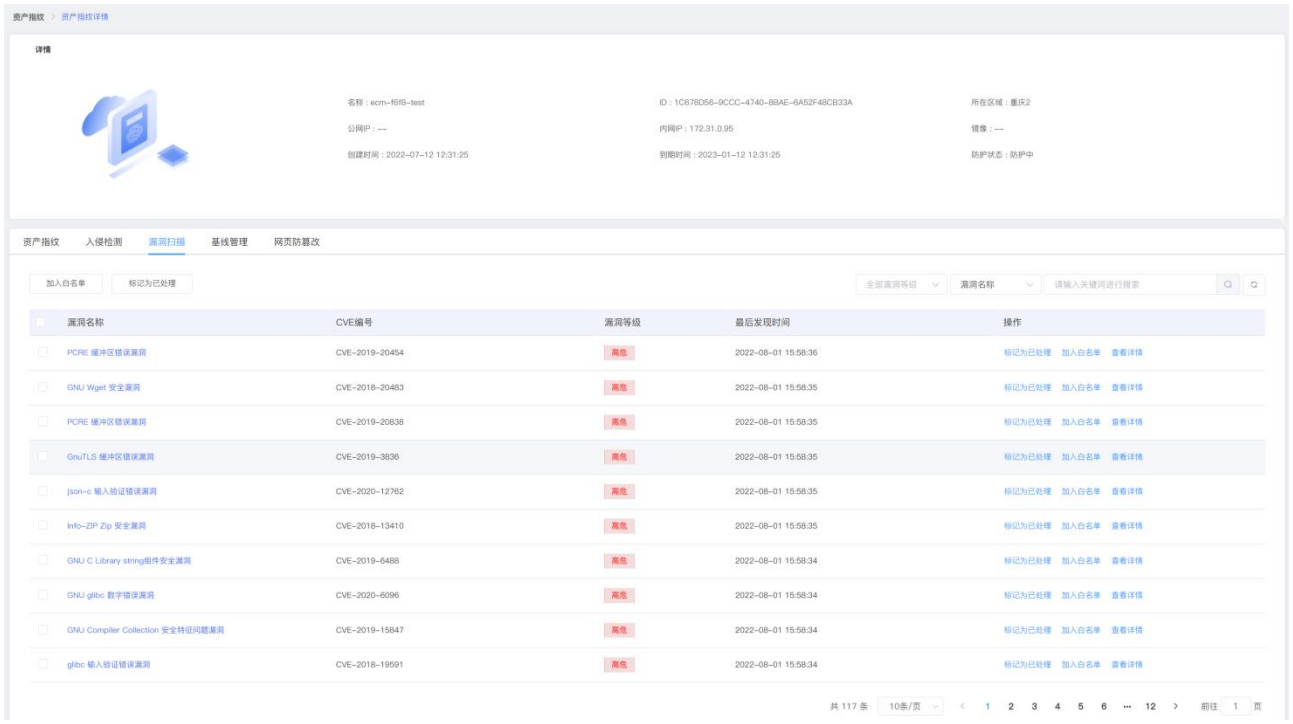
如下图所示，展示该台服务器的异常登录详情。

暴力破解

如下图所示，展示该台服务器的暴力破解详情。

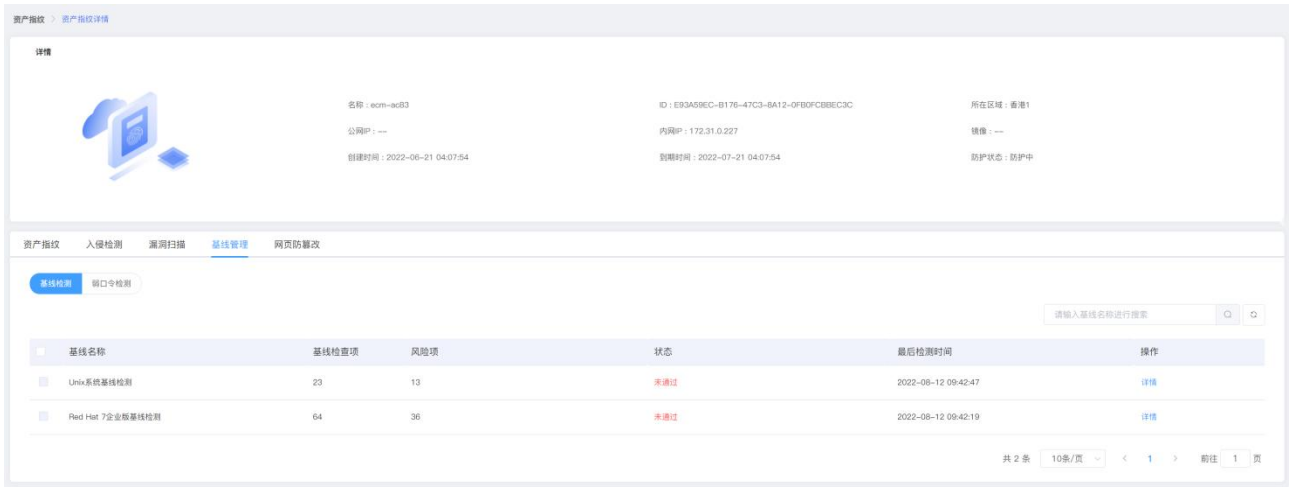
漏洞扫描

如下图所示，展示该台服务器的漏洞详情。



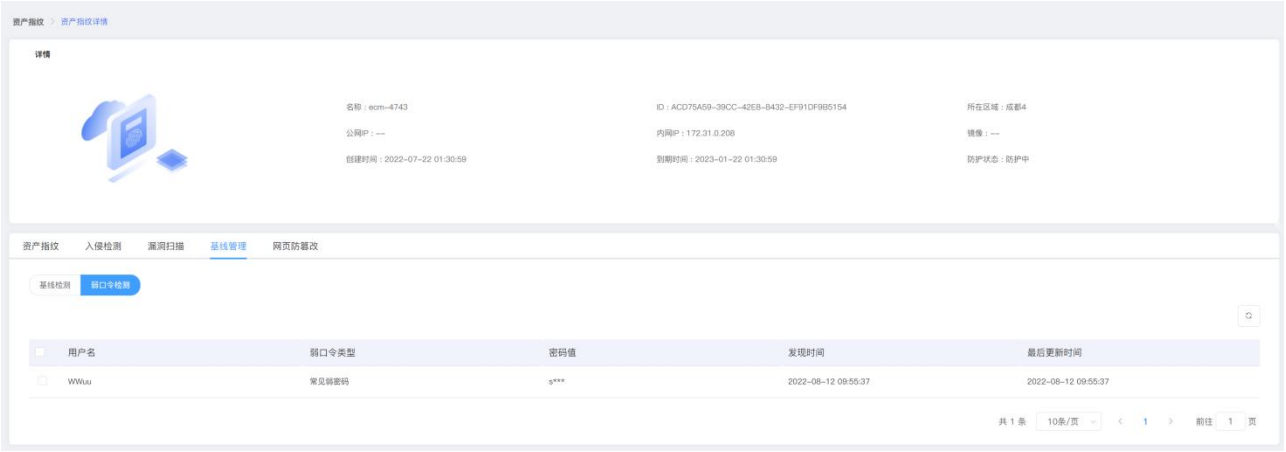
基线检测

如下图所示，展示该台服务器的基线检测详情。



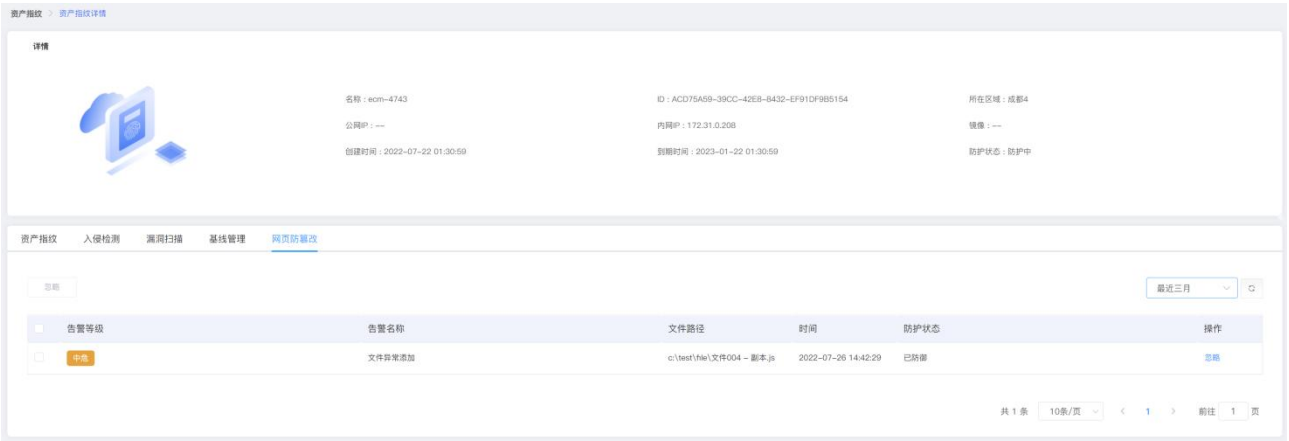
弱口令检测

如下图所示，展示该台服务器的弱口令检测详情。



网页防篡改

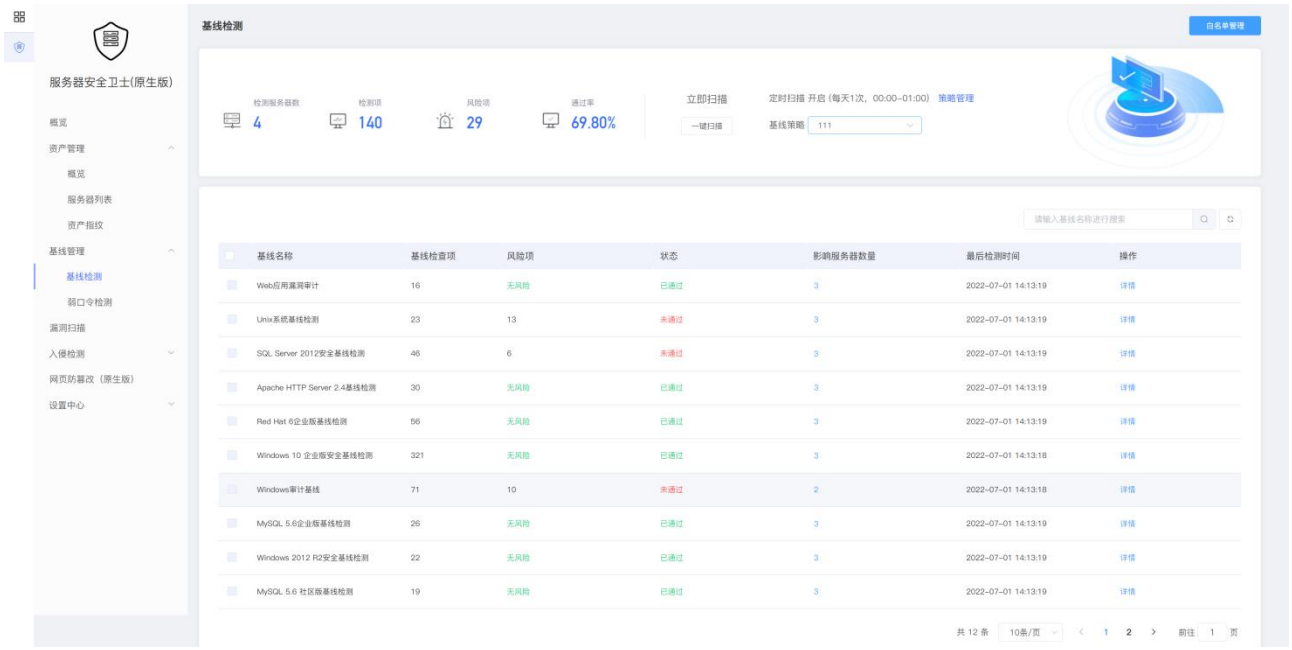
如下图所示，展示该台服务器的网页防篡改详情。



4.4. 基线管理

4.4.1. 基线检测

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



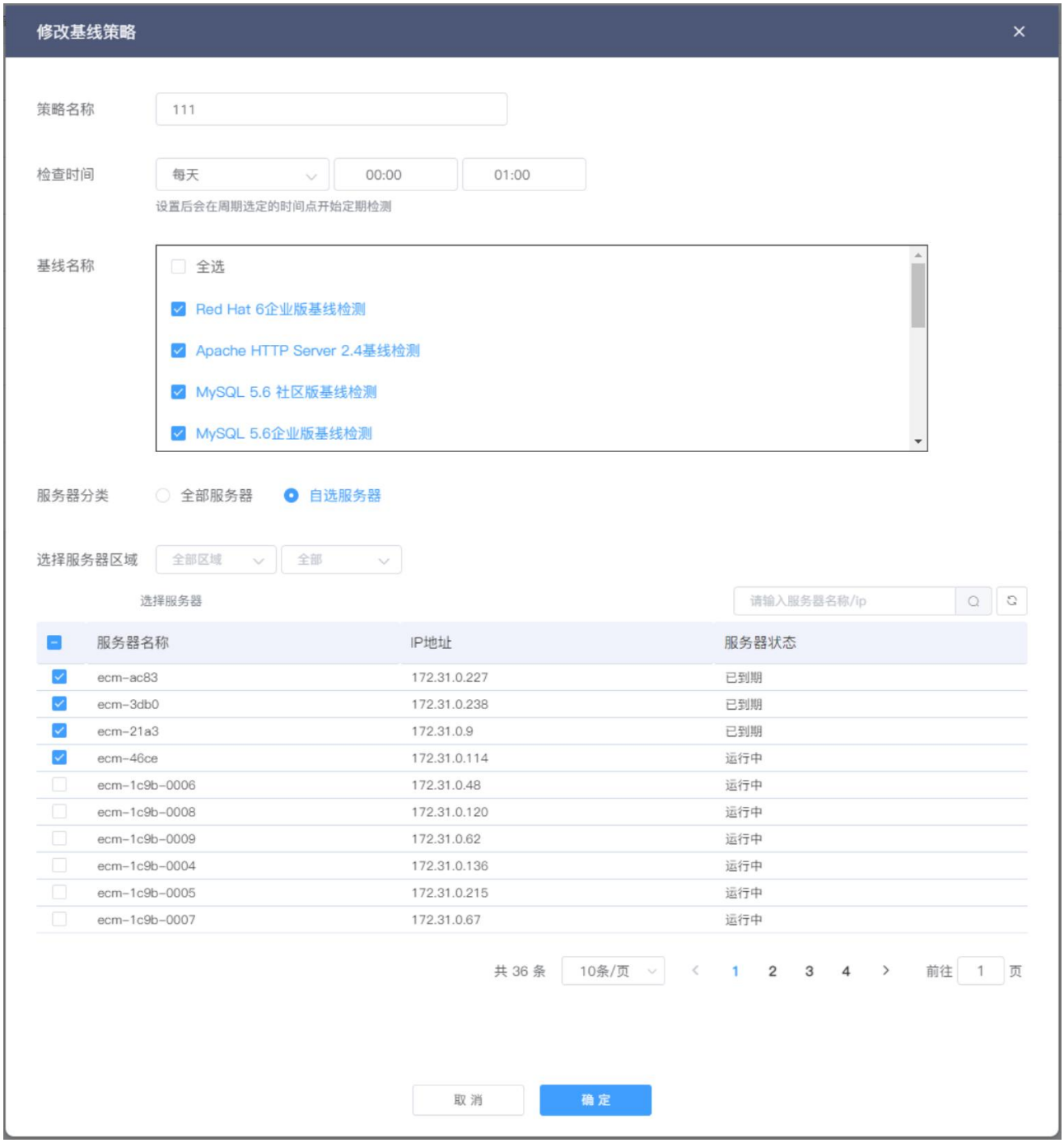
选定一个基线策略后，展示该策略上一次基线检测结果完成后的统计数据，统计情况包括检测服务器数、检测项、风险项、通过率。切换基线策略后，显示切换后的基线检测统计结果。其中，通过率=所有成功主机通过项之和÷（所有成功主机检测通过项+所有成功主机风险项）×100%。

基线检测设置

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

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

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



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

基线检测操作

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

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

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

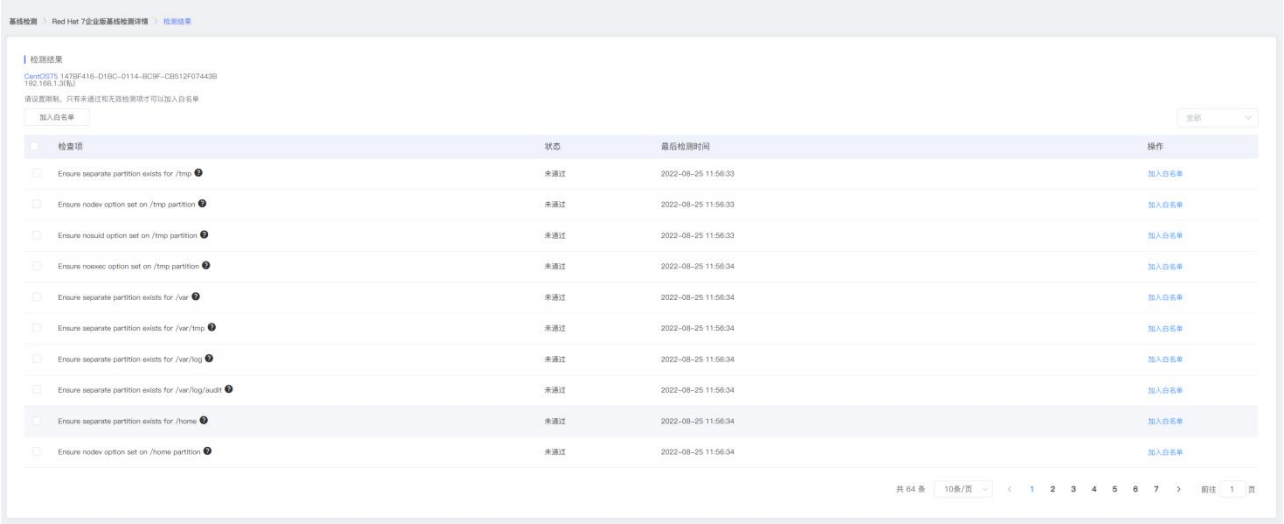
基线检测结果

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

若本次检测失败，则展示“检测失败”，基线检测结果列表只展示表头，检测结果为空。

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

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



白名单管理

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

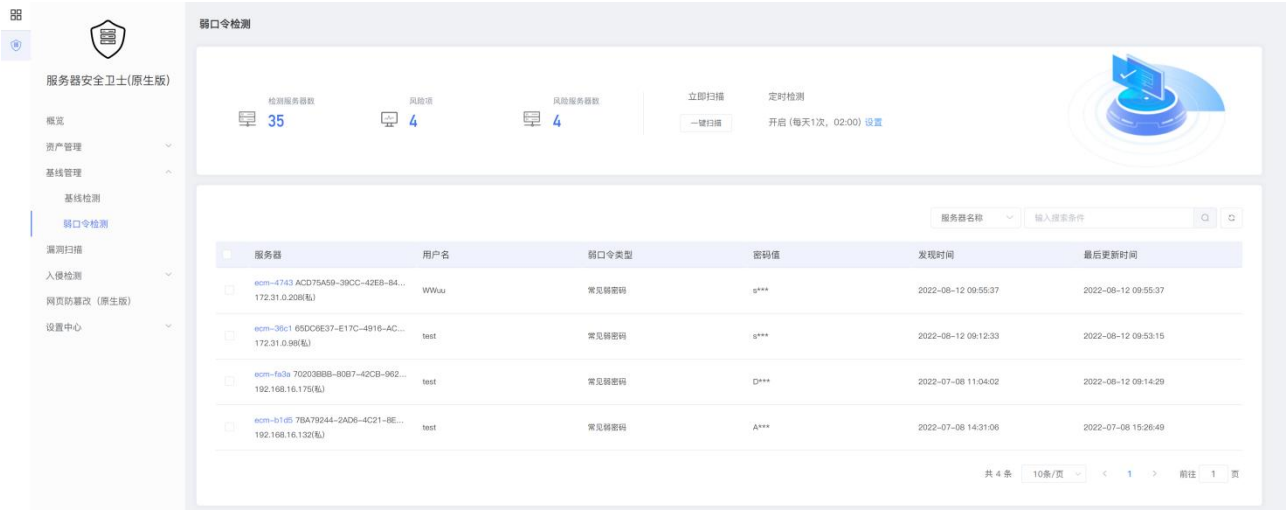
若您需要将已加入白名单的检测项移除白名单，可点击主页的“白名单管理”，如下图所示：

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

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

4.4.2. 弱口令检测

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



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

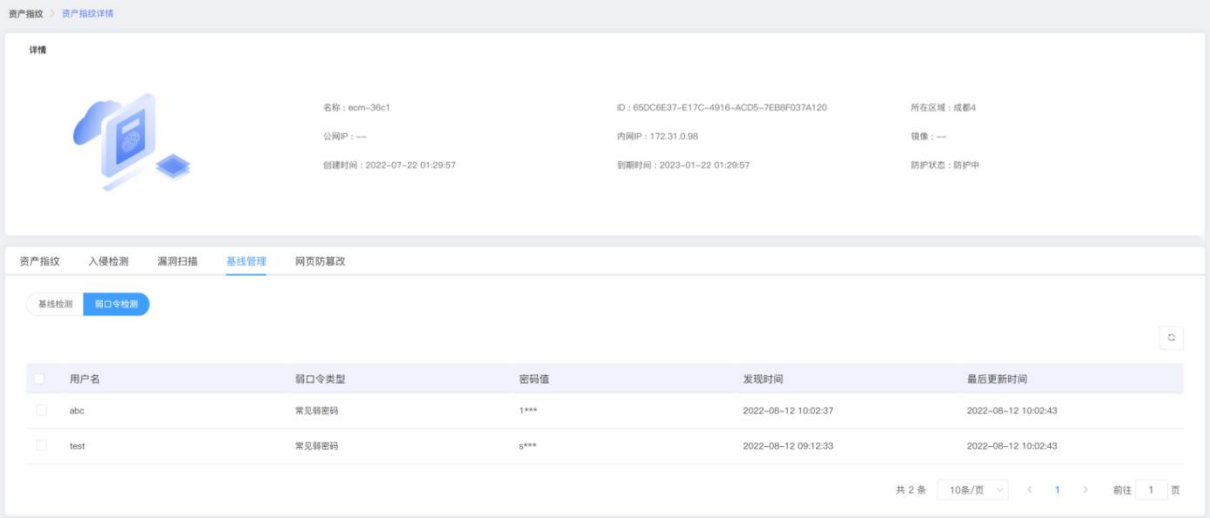
2. 定时检测设置如下图，可开启定时检测，并进行定期检测周期、服务器选择的设置。关闭定时扫描开关后，下方的所有设置项消失，不再能进行检测设置。点击确定后，定时检测设置完成。

3. 当开始一键扫描或定时扫描后，展示动态检测效果。

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

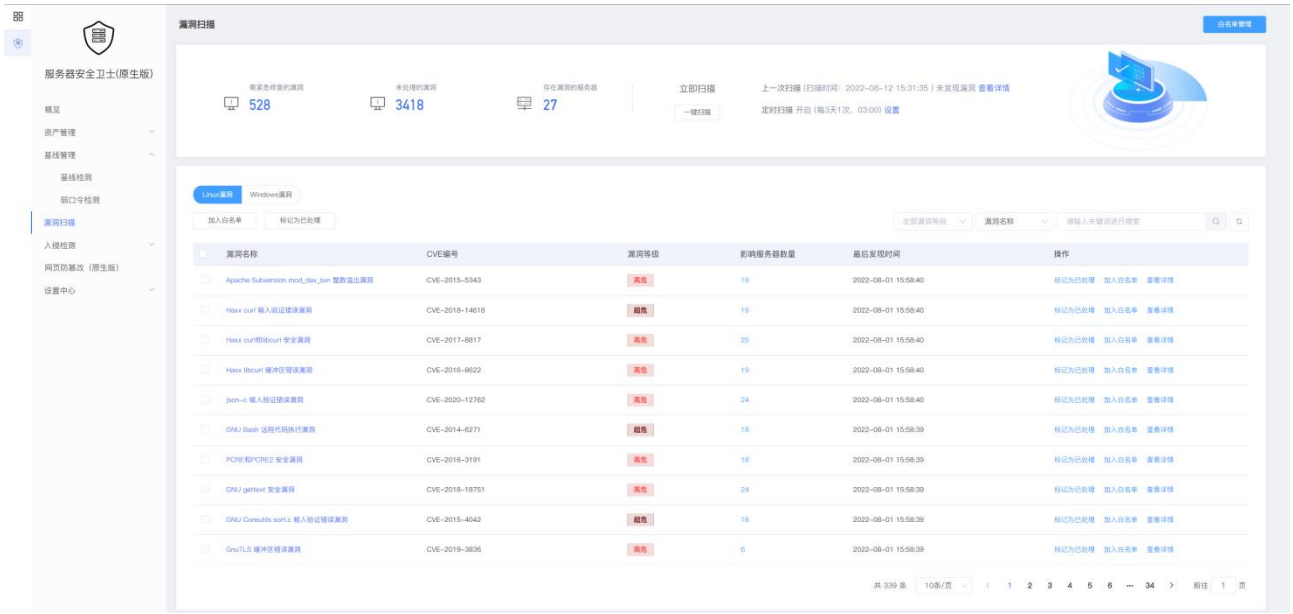
5. 若检测完成后，下方弱口令列表展示本次检测完的结果，在未完成扫描时展示上次的扫描结果，如下图所示。

6. 检测结果包括影响服务器、用户名、弱口令类型、密码值、发现时间、最后更新时间。点击上图列表中的服务器名称，跳转至下方资产详情页面。在该页面，为您展示该服务器的基本信息和弱口令检测情况。



4.5. 漏洞扫描

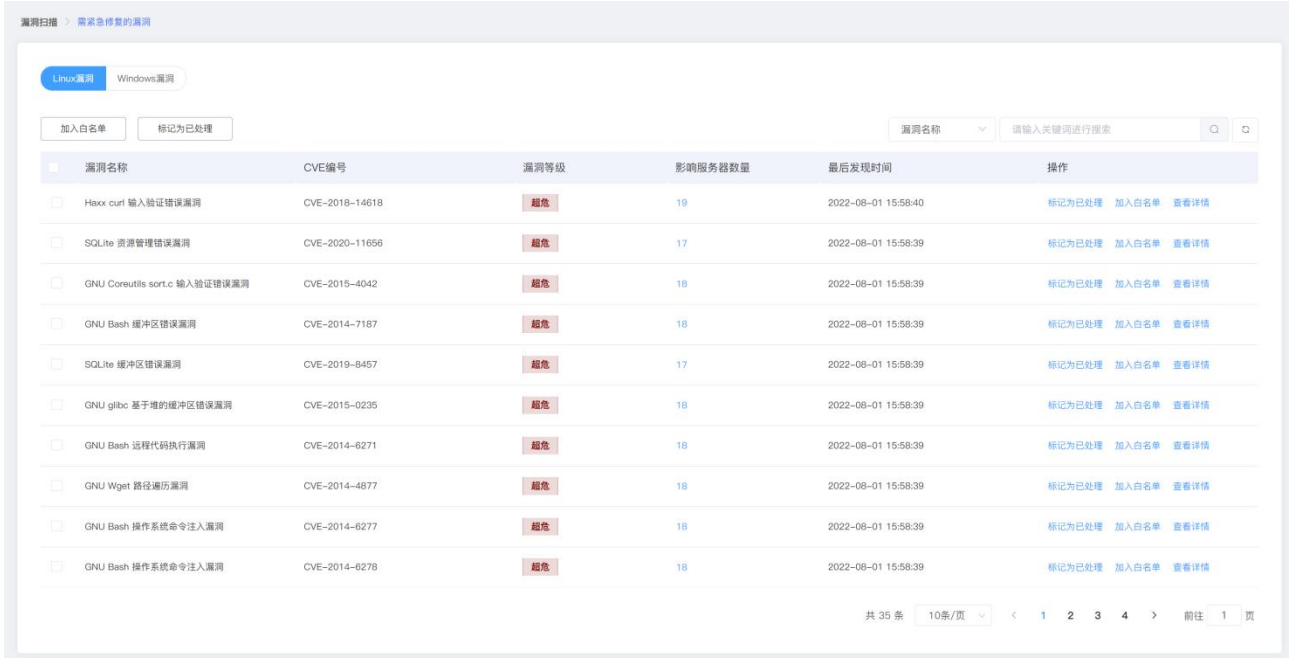
如下图所示，上方展示漏洞扫描的统计情况和漏洞扫描设置，下方展示漏洞列表。



统计情况包括需紧急修复的漏洞、未处理的漏洞、存在漏洞的服务器。

需紧急修复的漏洞

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



漏洞扫描设置

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

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

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

漏洞扫描操作

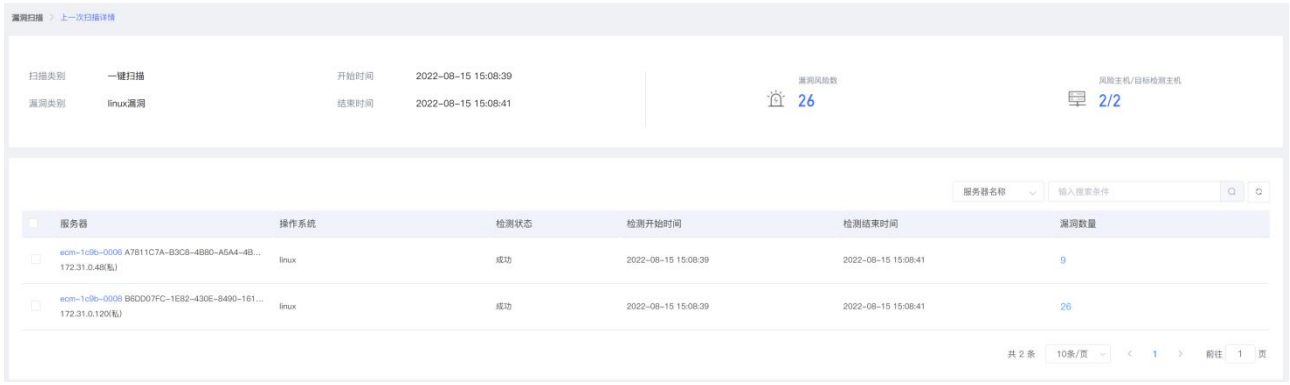
当开始一键扫描或定时扫描后，页面上展示下图动态效果。

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

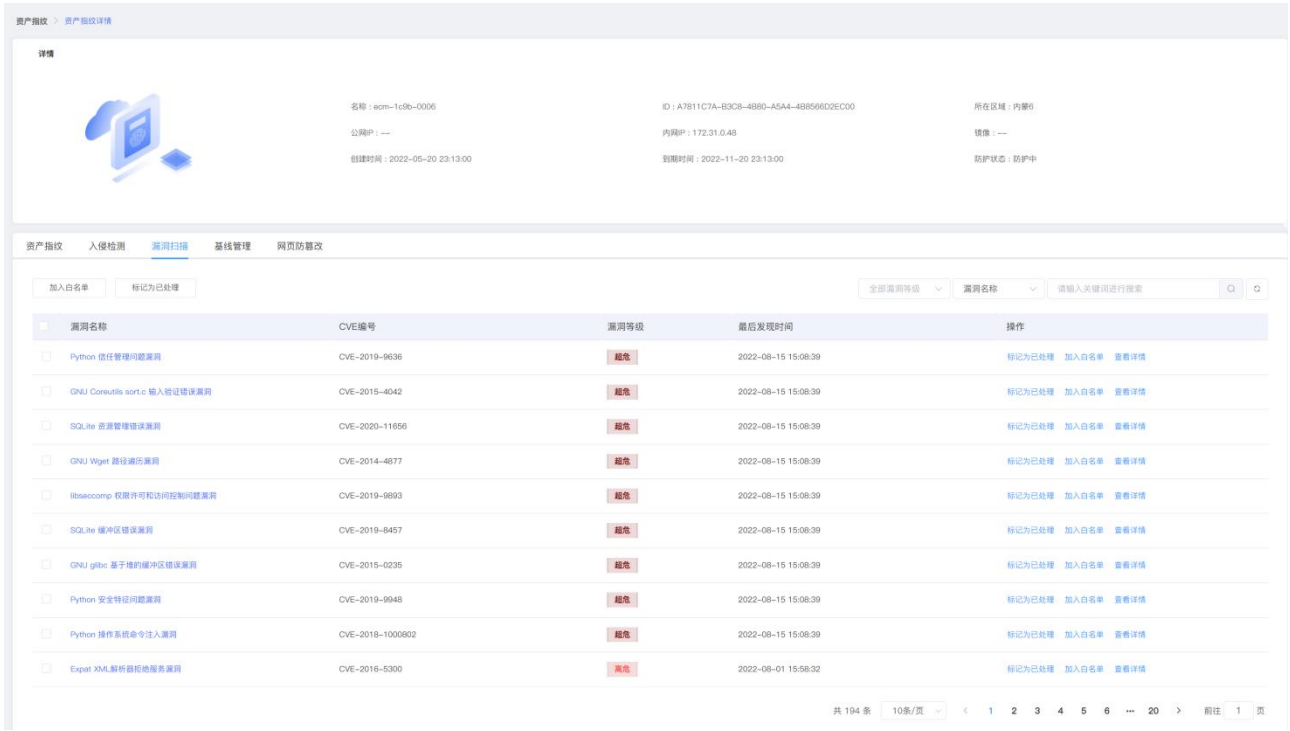
漏洞扫描结果

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

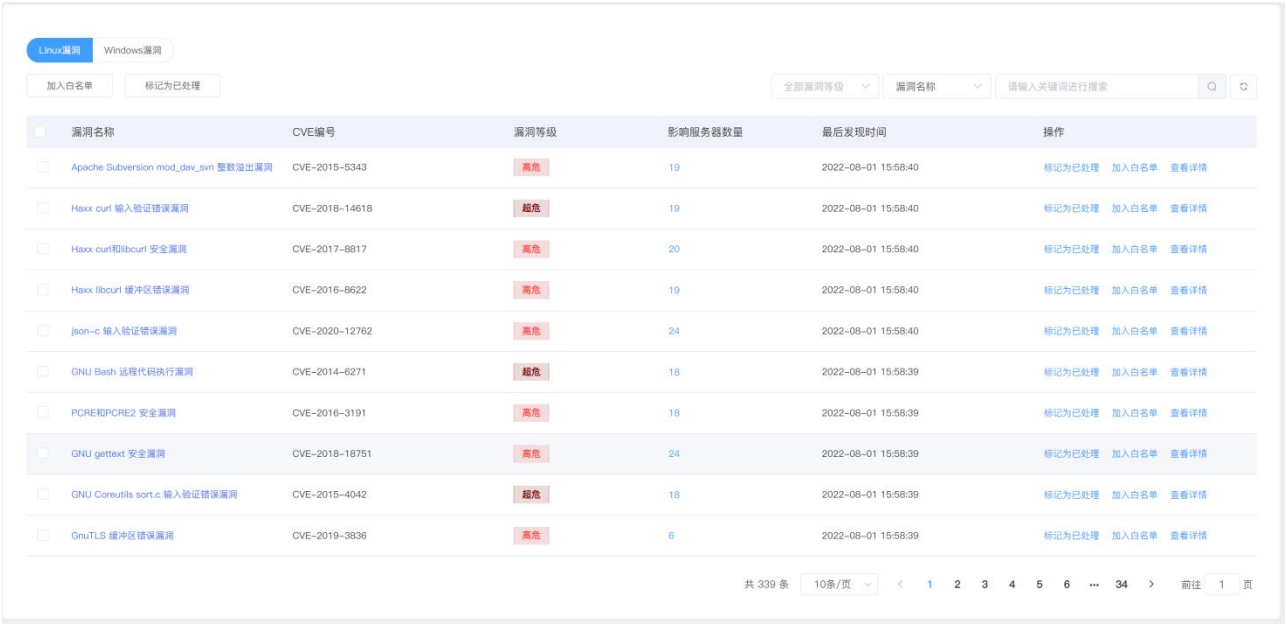
点击“查看详情”，可以查看上一次扫描的统计情况和基于主机展示的漏洞列表。在统计情况中，可以查看扫描类别、漏洞类别、开始时间、结束时间、漏洞风险数和风险主机/目标检测主机。在基于主机展示的漏洞列表中，为您展示服务器、操作系统、检测状态、检测开始时间、检测结束时间和漏洞数量。



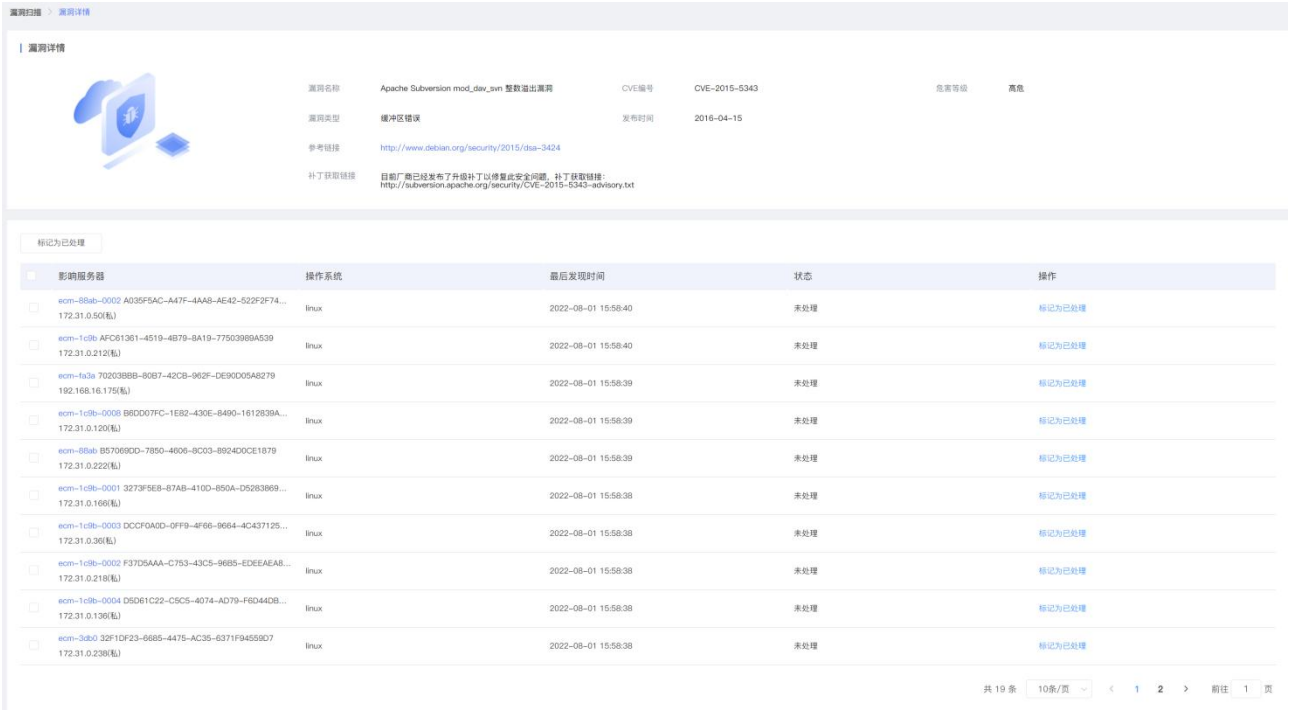
当点击漏洞数量中下方的数字时，跳转至资产详情页面，如下图所示。在资产详情页面，为您展示该服务器的基本信息和漏洞情况。



漏洞扫描主页下方的漏洞列表中展示本次扫描的漏洞情况，按照 Linux 和 windows 漏洞分别展示，包括漏洞名称、CVE 编号、漏洞等级、影响服务器数量、最后发现时间和操作，列表默认按照最后发现时间排序，最新发现的漏洞位于最上方。漏洞列表可按照漏洞等级、漏洞名称、CVE 编号进行搜索。



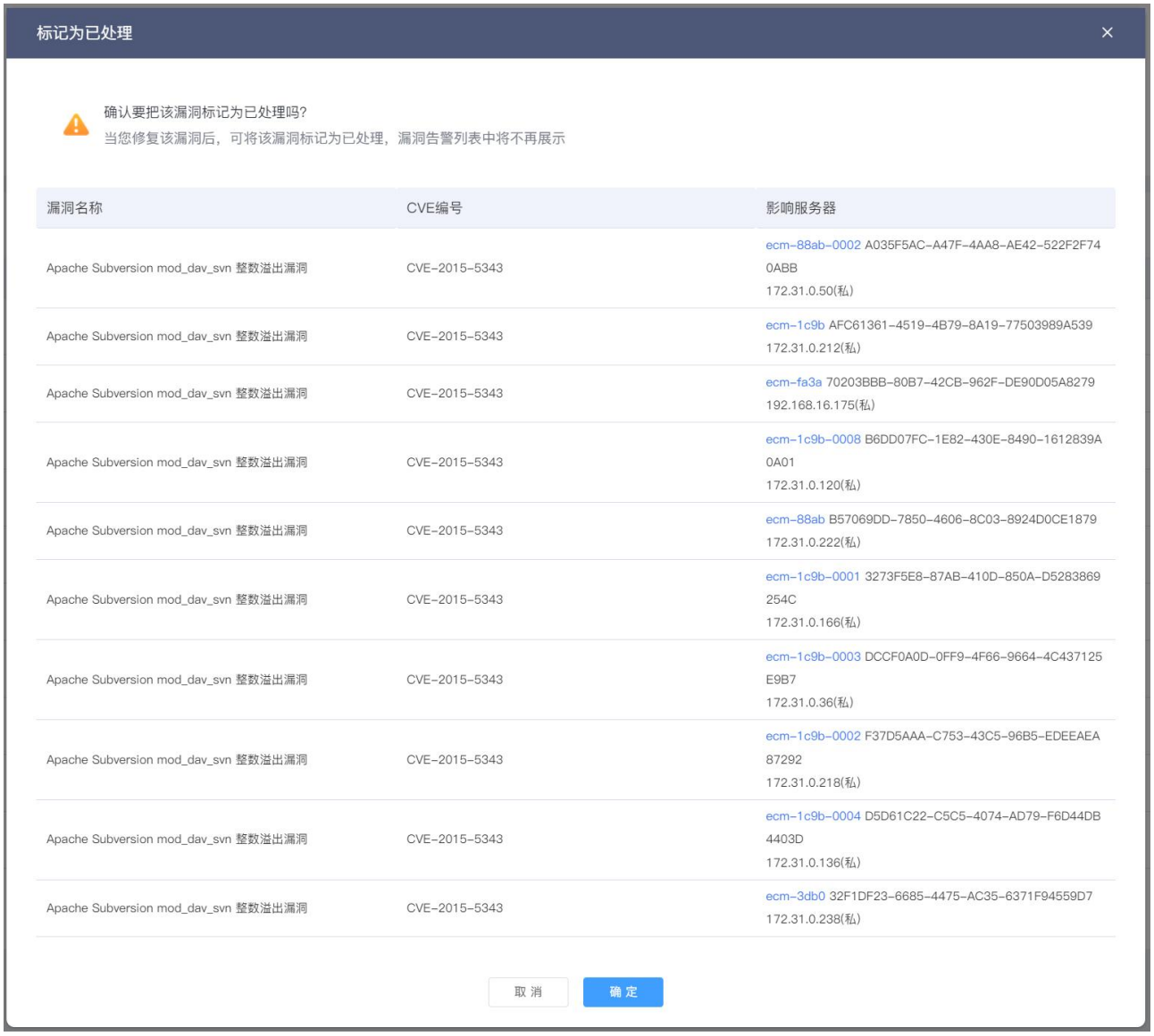
当点击“漏洞名称”、“影响服务器数量”或“查看详情”时，跳转至下方的漏洞详情页面。该页面包括漏洞的基本信息和影响服务器列表，基本信息包括漏洞名称、CVE 编号、危害等级、漏洞类型、发布时间、参考链接、补丁获取链接，影响服务器列表包括影响服务器、操作系统、最后发现和操作。



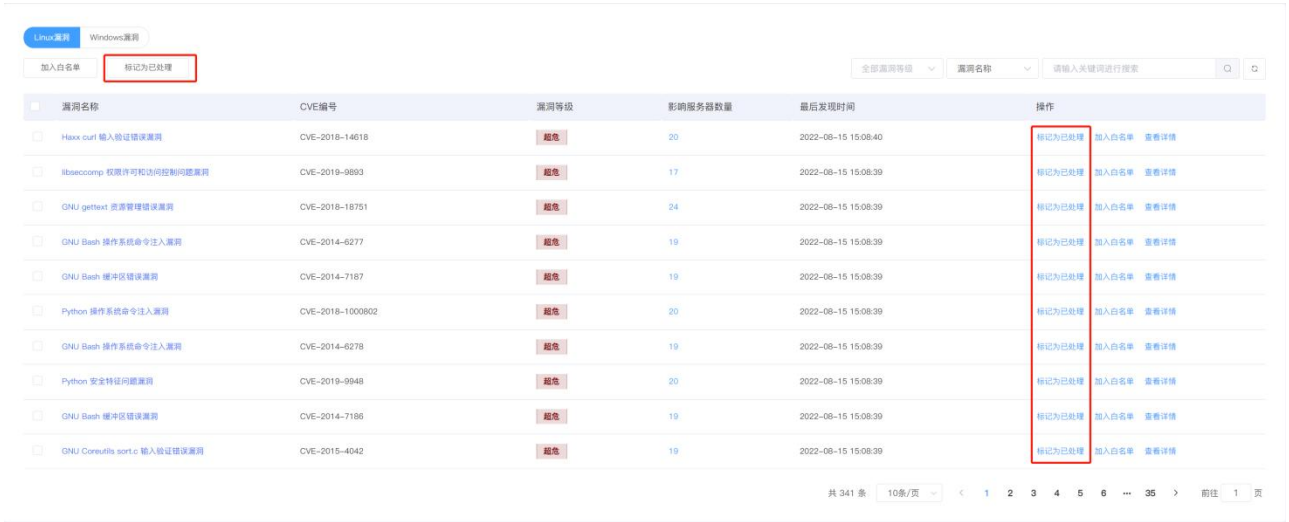
漏洞标记处理

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

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



当点击漏洞扫描页面上漏洞列表中的“标记为已处理”时，如下图所示：

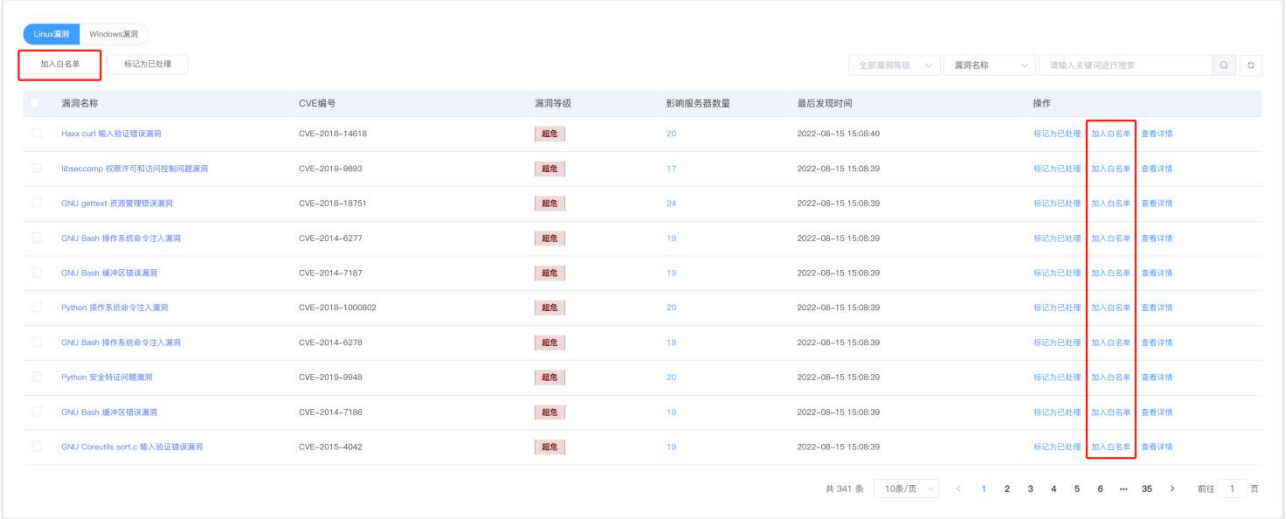


若选择一个漏洞操作“标记为已处理”，弹出如下对话框，确认后，该漏洞不再展示在漏洞列表中，且漏洞详情页面所有服务器的状态均变更为“已处理”。

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

白名单管理

当点击漏洞扫描页面上漏洞列表中的“加入白名单”，如下图所示：



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

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

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

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

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

4.6. 入侵检测

4.6.1. 异常登录

如下图所示，上方展示异常登录事件的统计情况，下方展示异常登录事件列表。

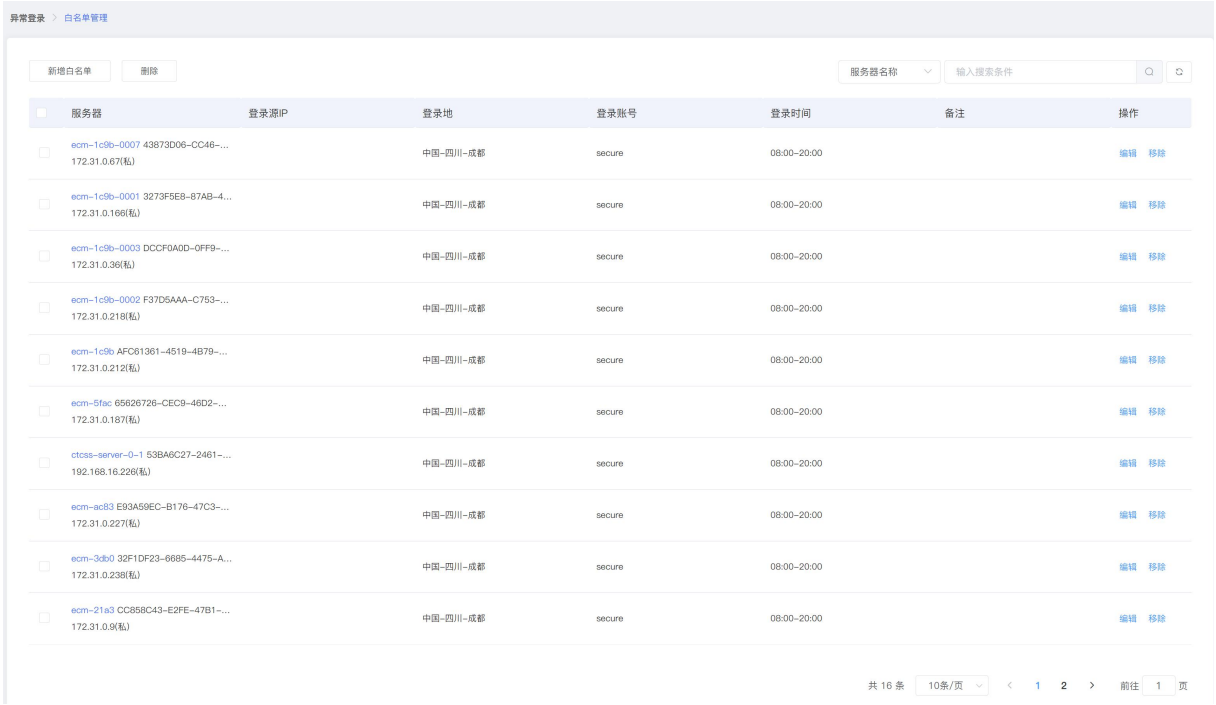
1. 统计情况包括异常登录事件数、爆破登录事件数、存在风险的服务器数，都默认统计最近一周的时间，还可以统计最近一月和最近三月的时间维度。异常登录事件：统计事件列表中的异常登录事件数，爆破登录事件：统计事件列表中的爆破登录事件数，存在风险的服务器：有异常登录和爆破登录事件的服务器数量，如果同一台服务器有不同的事件需要进行去重。

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

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

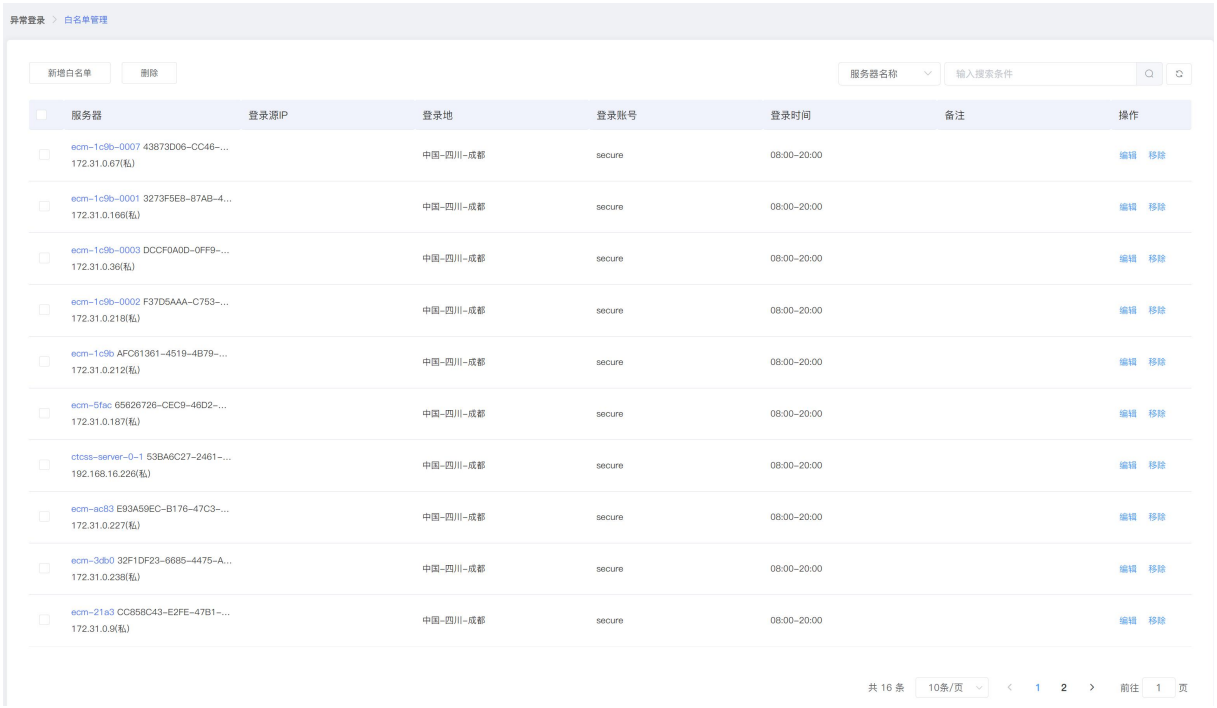
4. 若您需要将某些登录 IP、登录用户名、登录时间和登录地区设置为正常登录，请您点击异常登录页面上的“白名单管理”进行设置，设置后将不再进行异常登录告警。

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



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

7. 当所有字段都选择完成后，会生成白名单规则，显示在白名单列表中，如下图所示：

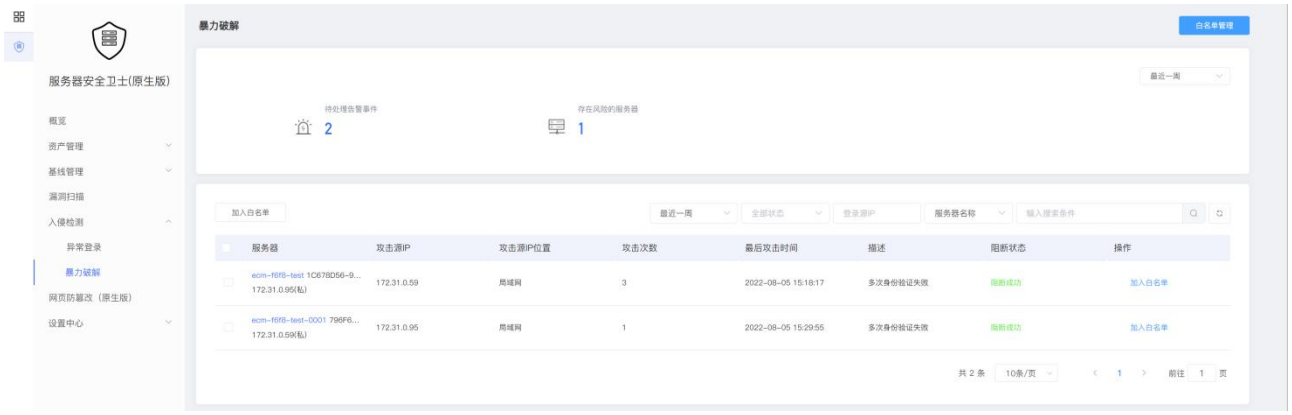


8. 可在操作中，对该白名单规则进行编辑和删除。当点击“编辑”时，弹出如下对话框，可编辑登录IP、登录用户名、登录时间、登录地区、描述，并点击“确定”后即可完成白名单规则的编辑。

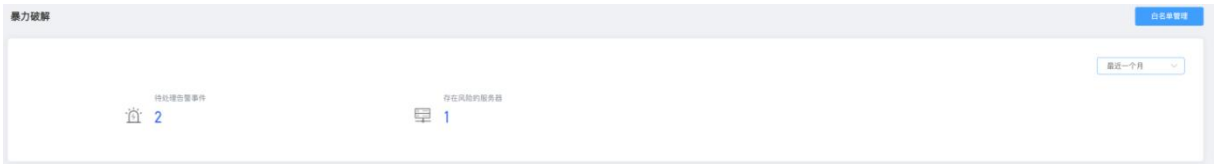
9. 当点击操作中的“删除”时，弹出如下对话框，点击确定后，该白名单规则将被删除。

4.6.2. 暴力破解

如下图所示，上方展示暴力破解事件的统计情况，下方展示暴力破解事件列表。



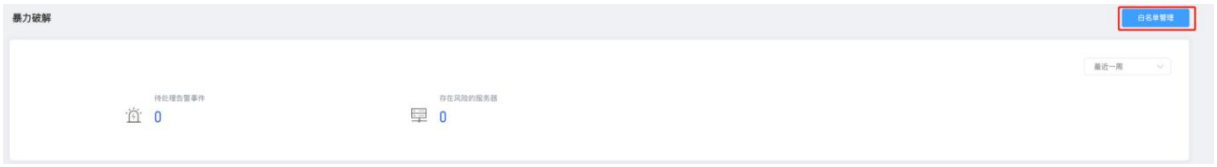
1. 统计情况包括待处理告警事件数和存在风险的服务器数，都默认统计最近一周的时间，还可以统计最近一月和最近三月的时间维度。待处理告警事件：统计事件列表中的事件数，存在风险的服务器：统计有暴力破解事件的服务器数量，如果同一台服务器有不同的事件需要进行去重。



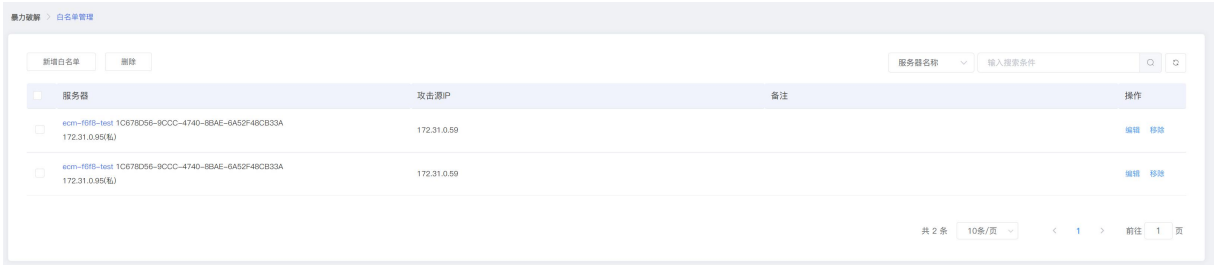
2. 事件列表包括服务器、攻击源 IP、攻击源 IP 位置、攻击次数、最后攻击时间、描述、阻断状态和操作，默认按照最后攻击时间进行排序，最新的事件排在最上方，并默认展示一周内的事件列表。阻断状态分为阻断成功和未阻断两种情况。事件列表可按照时间、状态、攻击源 IP、服务器名称、服务器 IP 进行搜索。

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

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

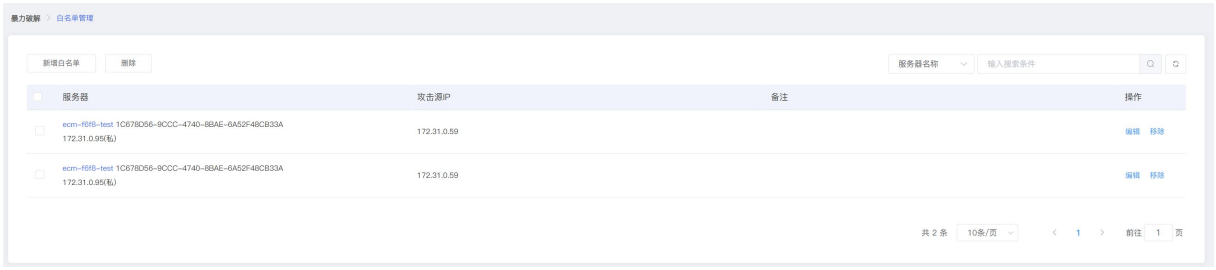


5. 白名单管理中可对暴力破解的白名单规则进行设置，包括白名单规则的新增、编辑和删除。白名单规则列表可根据服务器名称和服务器 IP 进行搜索，若该规则中包含该台服务器，即进行显示。



6. 点击“新增白名单”时，弹出如下对话框，可填写来源 IP、描述，并填写服务器分类。登录 IP 支持单个 IP（示例：1.1.1.1）、IP 范围（示例：1.1.1.1-1.1.1.10）和 IP 段（示例：172.168.34.1/20）。多个 IP 之间用英文, 隔开。服务器可选择全部服务器和部分服务器。登录 IP 和服务器均为必填选项。

7. 当所有字段都选择完成后，会生成白名单规则，显示在白名单列表中，如下图所示：



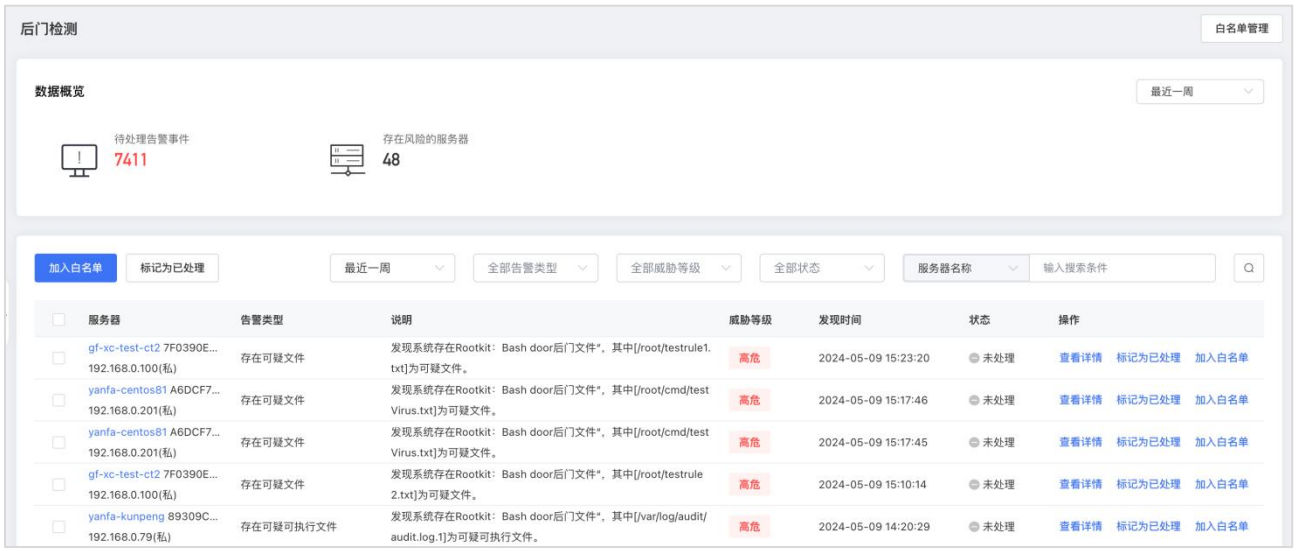
8. 可在操作中，对该白名单规则进行编辑和删除。当点击操作中的“编辑”时，弹出如下对话框，可编辑登录 IP 和描述，点击确定后，该白名单规则编辑完成。

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

4.6.3. 后门检测

说明：后门检测属于企业版功能，请先购买企业版配额并绑定主机后，才能正常使用。

登录服务器安全卫士（原生版）控制台，在左侧导航栏选择入侵检测->后门检测。如下图所示，上方展示告警事件和风险服务器的统计情况，下方展示告警事件详情。



告警详情

告警事件列表展示字段包括服务器、告警类型、告警说明、威胁等级、发现时间、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。

单击查看详情查看后门文件详细信息，包括静态信息和进程信息。静态信息：文件类型、文件访问权限、文件大小、文件所属用户、文件所属用户组、文件 SHA1、文件 MD5、文件 SHA256、状态修改时间、修改时间、最近访问时间；进程信息：进程名、进程所属用户、进程所属用户组、进程文件路径、文件权限、进程命令行。

处理方式

- 标记为已处理：人工对告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：经过分析后确认为误告警，可将此告警加入白名单，后续检测到相同文件后不再进行告警。

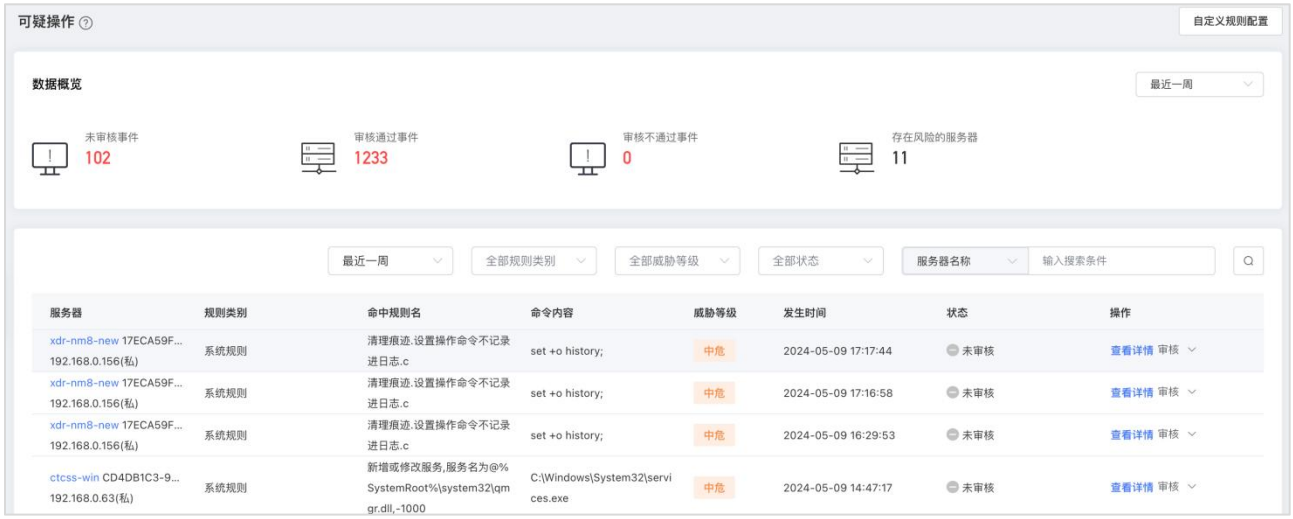
白名单管理

将告警进行加白操作后，可进入白名单管理页面对白名单规则进行管理，包括白名单规则的新增、编辑和删除。同时白名单规则列表可根据服务器名称和服务器 IP 进行搜索，若该规则中包含该台服务器或 IP，即进行显示。

4.6.4. 可疑操作

说明：可疑操作属于企业版功能，请先购买企业版配额并绑定主机后，才能正常使用。

登录服务器安全卫士（原生版）控制台，在左侧导航栏选择入侵检测->可疑操作。如下图所示，上方展示可疑告警事件和风险服务器的统计情况，下方展示告警事件详情。



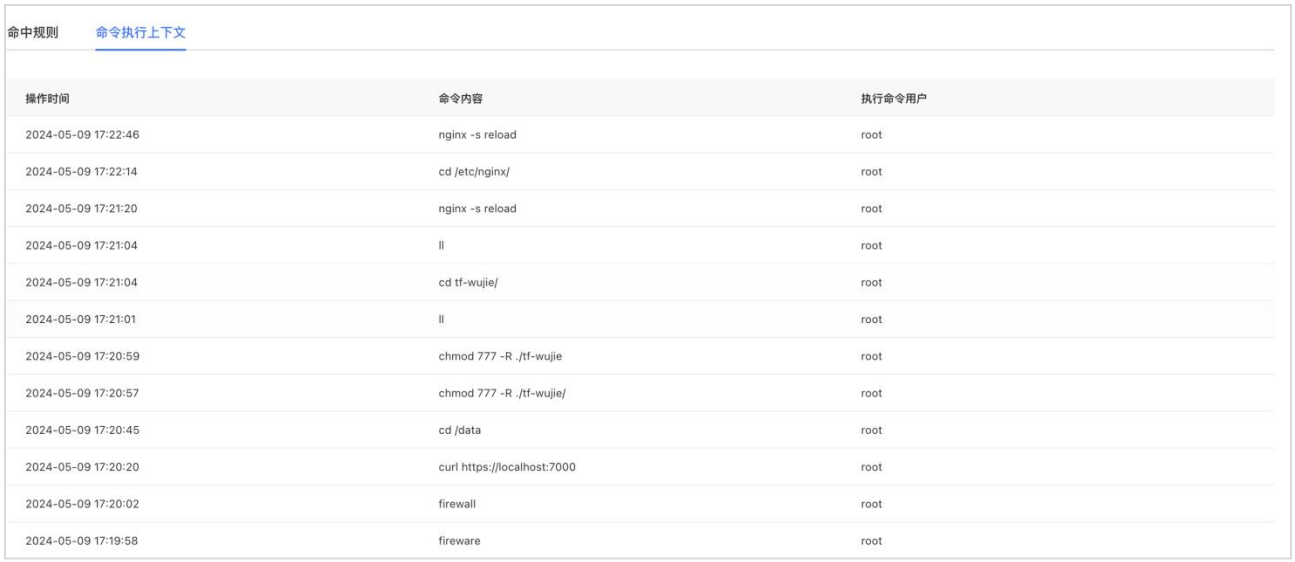
告警详情

告警事件列表展示字段包括服务器、规则类别、命中规则名、命令内容、威胁等级、发生时间、状态和操作。告警事件支持按发现时间、规则类别、威胁等级、处理状态、服务器名称、服务器 IP、命中规则名、命令内容、进行搜索。

单击查看详情按钮查看可疑操作详细信息。

命中规则：命中规则名称、威胁等级、规则类别、命令内容、登录用户、登录 IP、执行命令进程、实际执行命令进程、产生命令的登录终端（TTY）、PID。

命令执行上下文：



处理方式

- 审核通过：人工对告警进行处理，处理后将告警标记为审核通过。
- 审核不通过：审核不通过则确认告警不存在风险。

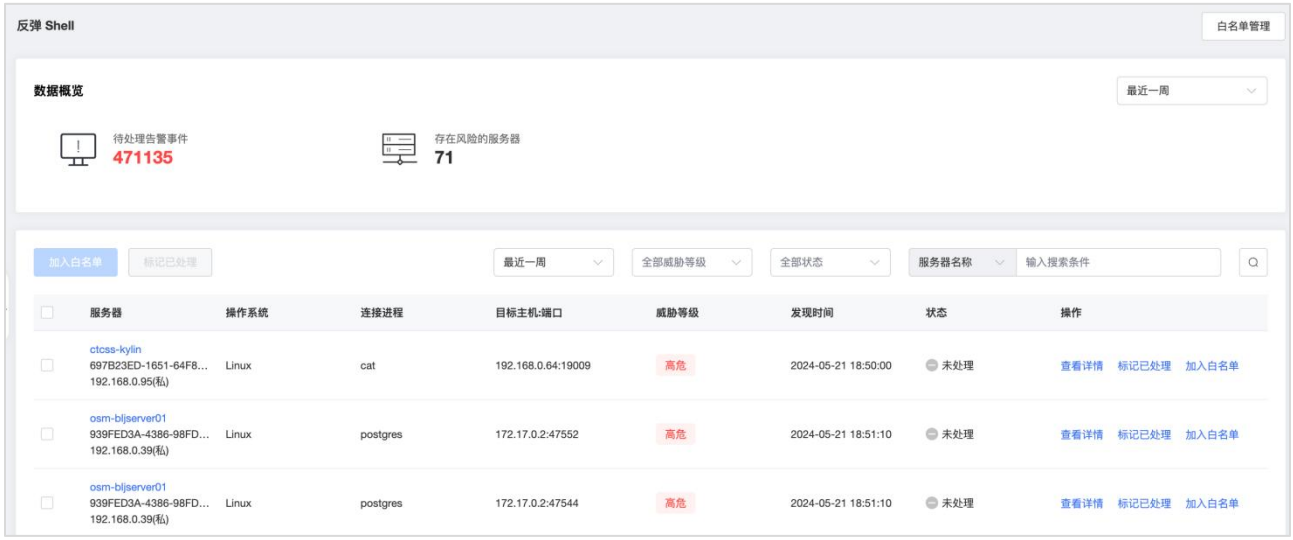
自定义规则

进入自定义规则配置管理页面，支持创建自定义规则，规则发布后命中规则内容即进行告警。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。

4.6.5. 反弹 Shell

说明：反弹 Shell 属于企业版功能，请先购买企业版配额并绑定主机后，才能正常使用。

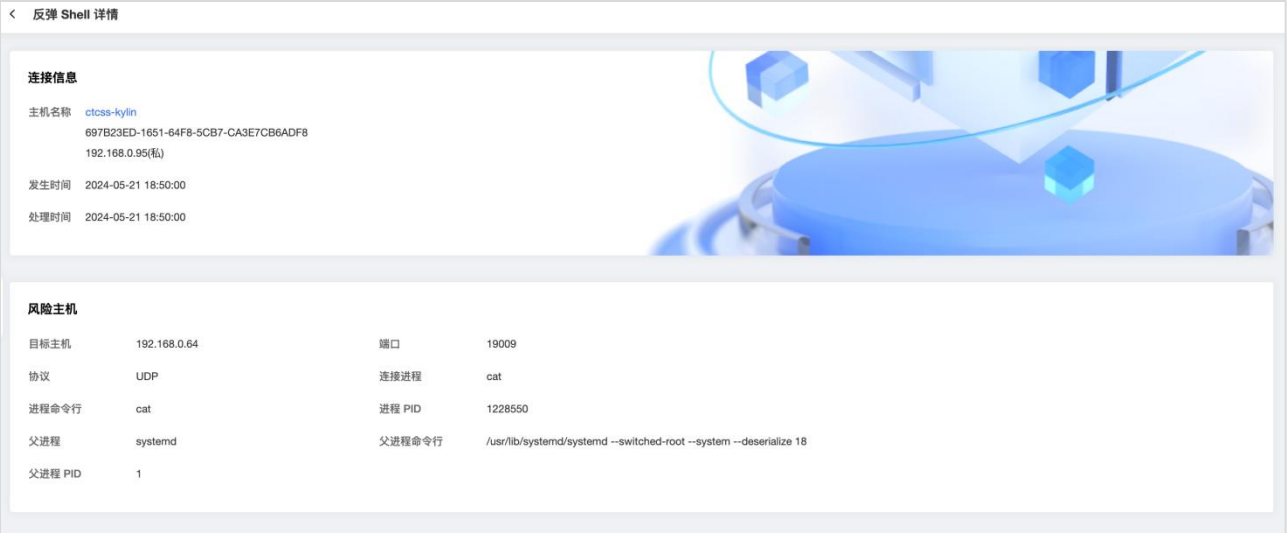
登录服务器安全卫士（原生版）控制台，在左侧导航栏选择入侵检测->反弹 Shell。如下图所示，上方展示告警事件和风险服务器的统计情况，下方展示告警事件详情。



告警详情

告警事件列表展示字段包括服务器、操作系统、连接进程、目标主机：端口、威胁等级、发现时间、状态和操作。告警事件支持按发现时间、威胁等级、处理状态、服务器名称、服务器 IP、连接进程、目标主机端口进行搜索。

单击查看详情查看反弹 Shell 详细信息，包括目标主机、端口、协议、连接进程、进程命令行、进程 PID、父进程、父进程命令行、父进程 PID。



处理方式

- 标记为已处理：人工对告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：经过分析后确认为误告警，可将此告警加入白名单，后续检测到相同反弹 Shell 行为后不再进行告警。

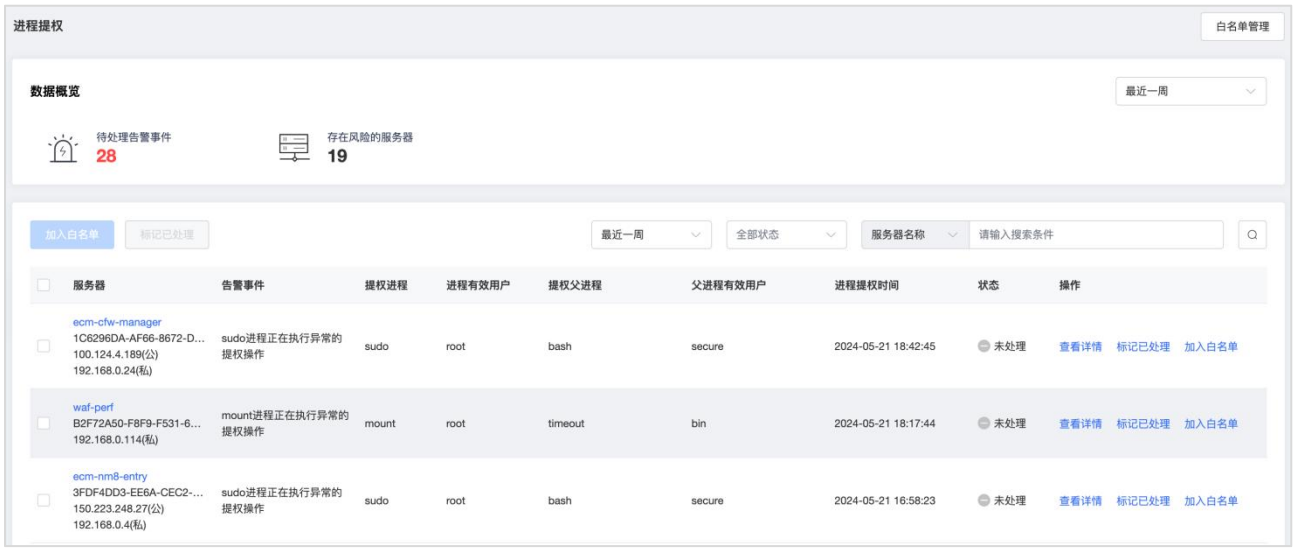
白名单管理

将告警进行加白操作后，可进入白名单管理页面对白名单规则进行管理，支持删除白名单规则。同时白名单规则列表可根据服务器名称、服务器 IP、连接进程或目标主机端口进行搜索，若该规则中包含该台服务器、IP、连接进程或目标主机端口，即进行显示。

4.6.6. 进程提权

说明：进程提权属于企业版功能，请先购买企业版配额并绑定主机后，才能正常使用。

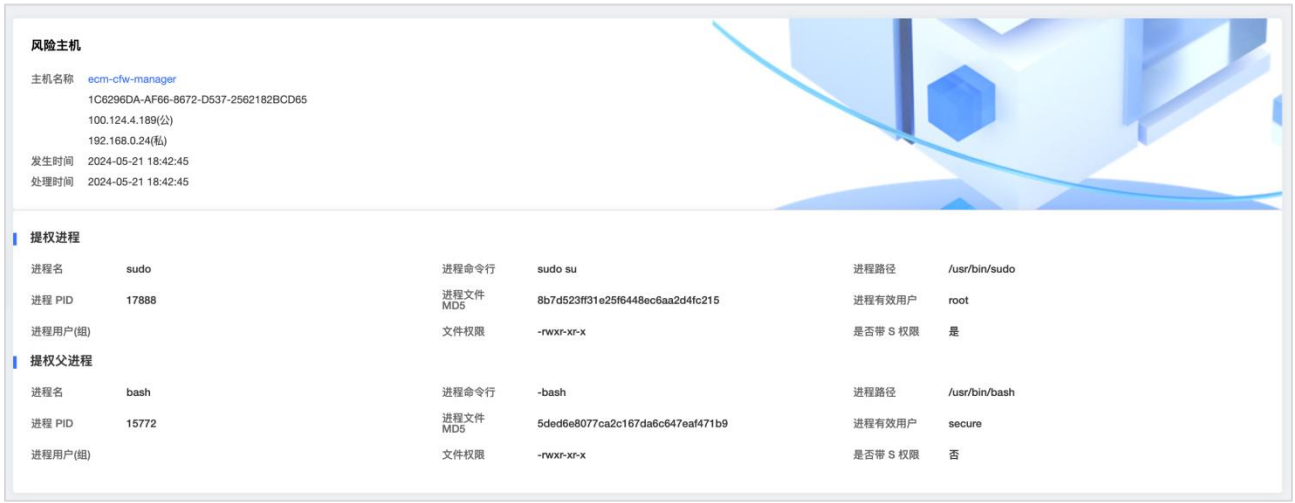
登录服务器安全卫士（原生版）控制台，在左侧导航栏选择入侵检测->进程提权。如下图所示，上方展示告警事件和风险服务器的统计情况，下方展示告警事件详情。



告警详情

告警事件列表展示字段包括服务器、提权进程、进程有效用户、提权父进程、父进程有效用户、进程提权时间、状态和操作。告警事件支持按发现时间、处理状态、服务器名称、服务器 IP 和提权进程进行搜索。

单击查看详情查看进程提权详细信息，包括风险主机、提权进程和提权父进程详细信息。



通过溯源分析能够展示具体告警进程，及进程的上下父子进程信息，并以进程树可视化的展示方式帮助分析人员对威胁进行追踪溯源，确认问题根源以及该恶意行为带来的影响。

处理方式

- 标记为已处理：人工对告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：经过分析后确认为误告警，可将此告警加入白名单，后续检测到相同进程提权行为后不再进行告警。

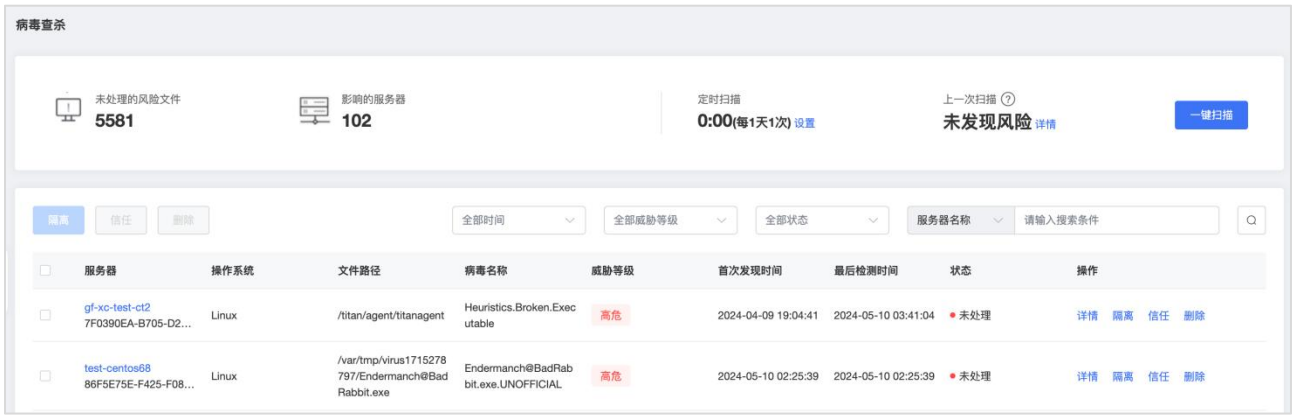
白名单管理

将告警进行加白操作后，可进入白名单管理页面对白名单规则进行管理，支持删除白名单规则。同时白名单规则列表可根据服务器名称或服务器 IP 进行搜索，若该规则中包含该台服务器或 IP，即进行显示。

4.7. 病毒查杀

说明：病毒查杀属于企业版功能，请先购买企业版配额并绑定主机后，才能正常使用。

登录服务器安全卫士（原生版）控制台，在左侧导航栏选择病毒查杀。如下图所示，上方展示告警事件和风险服务器的统计情况，下方展示告警事件详情。



病毒扫描

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，病毒扫描提供快速扫描、全盘扫描、自定义扫描三种扫描方式。

- 快速扫描：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。
- 全盘扫描：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。
- 自定义扫描：根据用户设置的指定目录有选择性的进行扫描。

防护策略

提供一键扫描和定时扫描两种防护策略，方便用户基于实际使用场景进行操作。

- 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、超时时间、生效范围。

  - 检测模式：可选择快速检测、全盘检测、自定义检测。
  - 超时时间：设置扫描任务时长，超过设置时长即为扫描失败。
  - 生效范围：自定义选择需要执行病毒扫描任务的服务器。

- 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，按照用户设置的检测周期执行扫描任务。

  - 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。
  - 超时时间：设置扫描任务时长，超过设置时长即为扫描失败。
  - 生效范围：自定义选择需要执行病毒扫描任务的服务器。

处理方式

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。

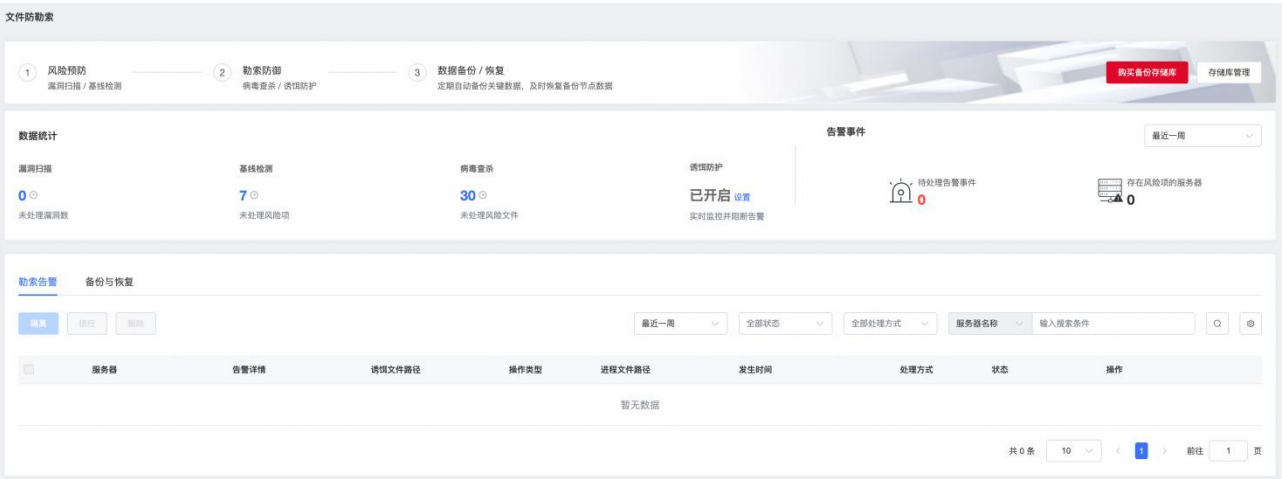
告警详情

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。

单击查看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。

4.8. 文件防勒索

说明：文件防勒索目前处于公测阶段，企业版用户可优先体验，请先购买企业版配额并绑定主机后，才能正常使用。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。



登录服务器安全卫士（原生版）控制台，在左侧导航栏选择文件防勒索。

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。

- 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。

- 勒索防御

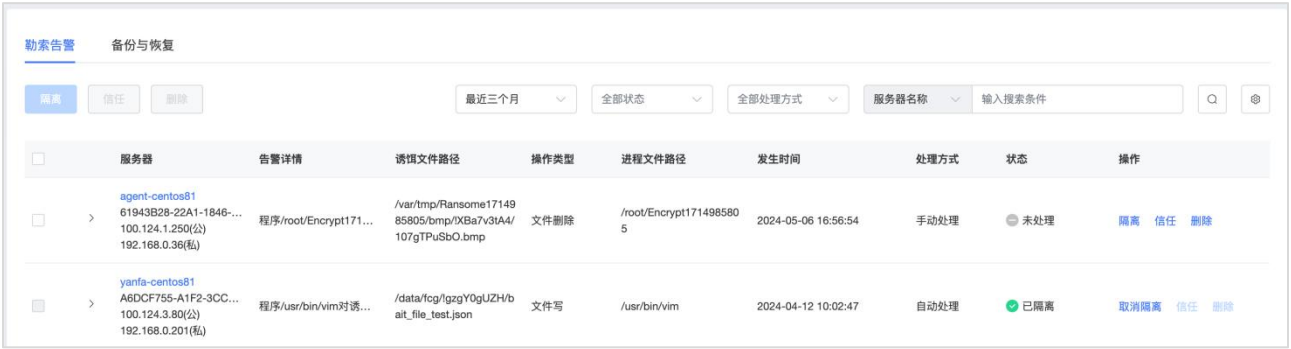
  页面展示病毒查杀最后一次扫描结果，如存在风险需单击未处理风险文件进入告警详情页进行处置；开启诱饵防护，在系统关键位置投放诱饵文件，实时捕捉勒索行为，阻止勒索病毒对数据的加密。

- 数据备份/恢复

  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。

勒索告警

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。



防护设置

启用诱饵防护：自动在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。

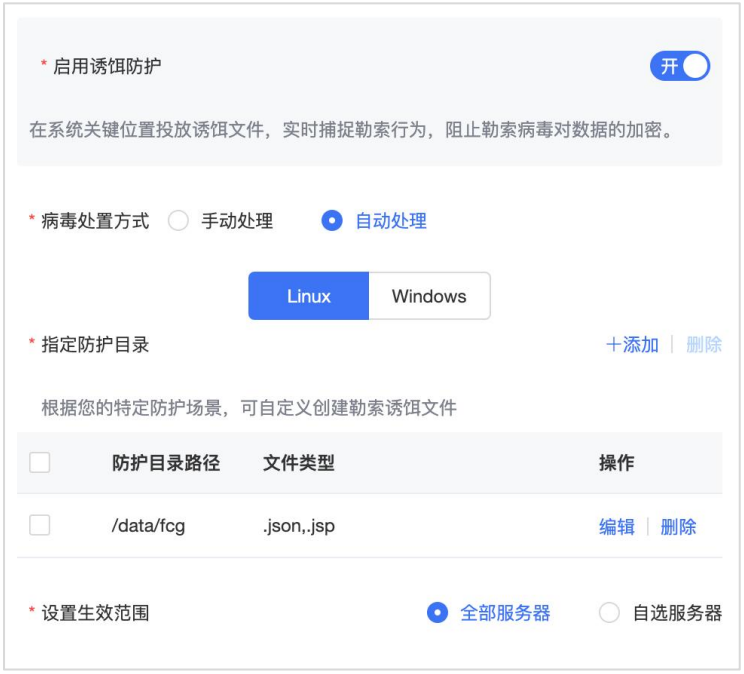
病毒处置方式：支持手动处理和自动处理。

- 手动处理：人工手动对勒索病毒文件进行处理。
- 自动处理：检测出勒索病毒文件自动隔离。

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。



处理方式

提供隔离、删除、信任三种病毒文件处理方式。

- 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。

数据备份/恢复

说明：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。

1. 云备份 Agent

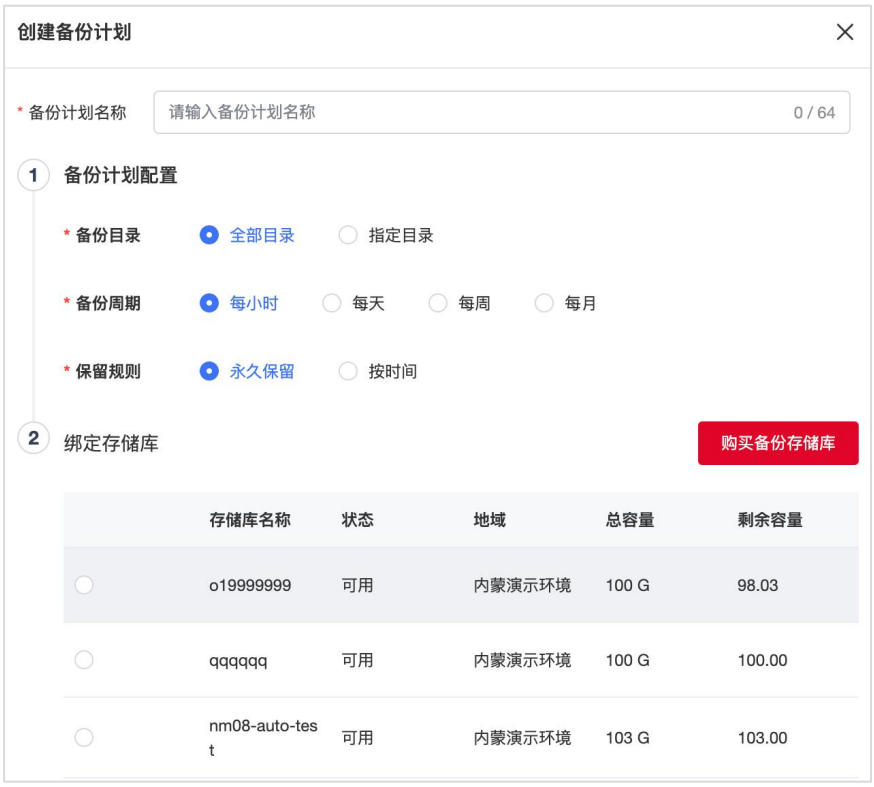
   选择需要进行数据备份的服务器，单击“安装备份 Agent”，Agent 状态为“已激活”则安装成功。

   如需卸载 Agent，可单击“卸载备份 Agent”。

2. 创建备份计划

   单击“备份计划”，按照设置的策略进行周期性数据备份。

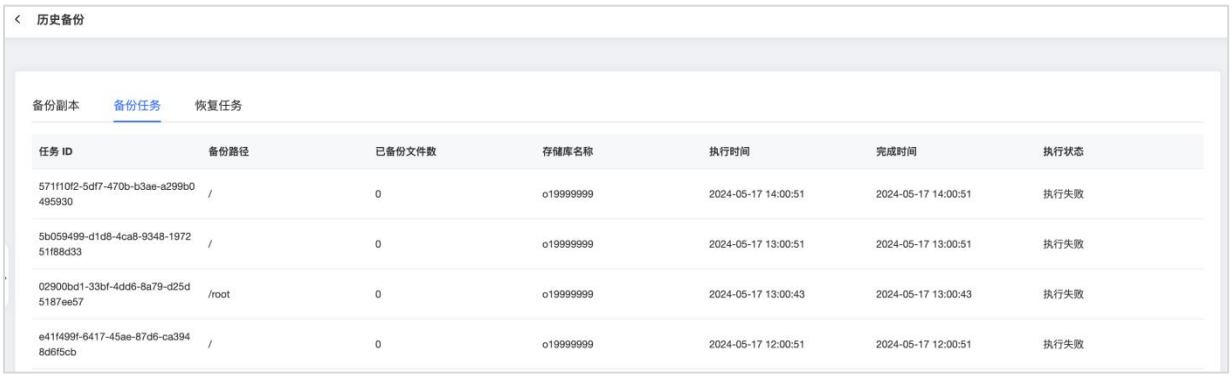
   - 备份目录：可指定全部目录或自定义目录进行数据备份。
   - 备份周期：可选择每小时、每天、每周或月设置备份周期。
   - 保留规则：可设置备份计划生效时间，支持永久保留和自定义设置时间。
   - 绑定存储库：选择一个可用状态的存储库，备份数据大小应大于存储库剩余容量。



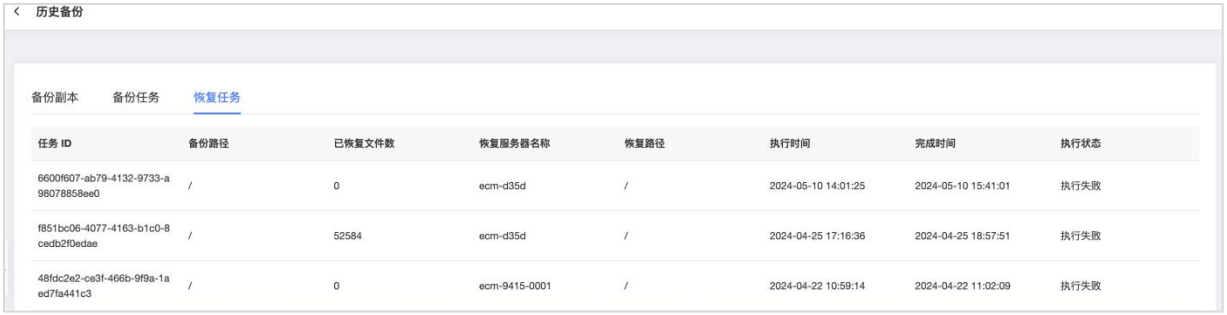
3. 历史备份

备份副本：按用户创建的备份计划自动生成备份副本，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。

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。



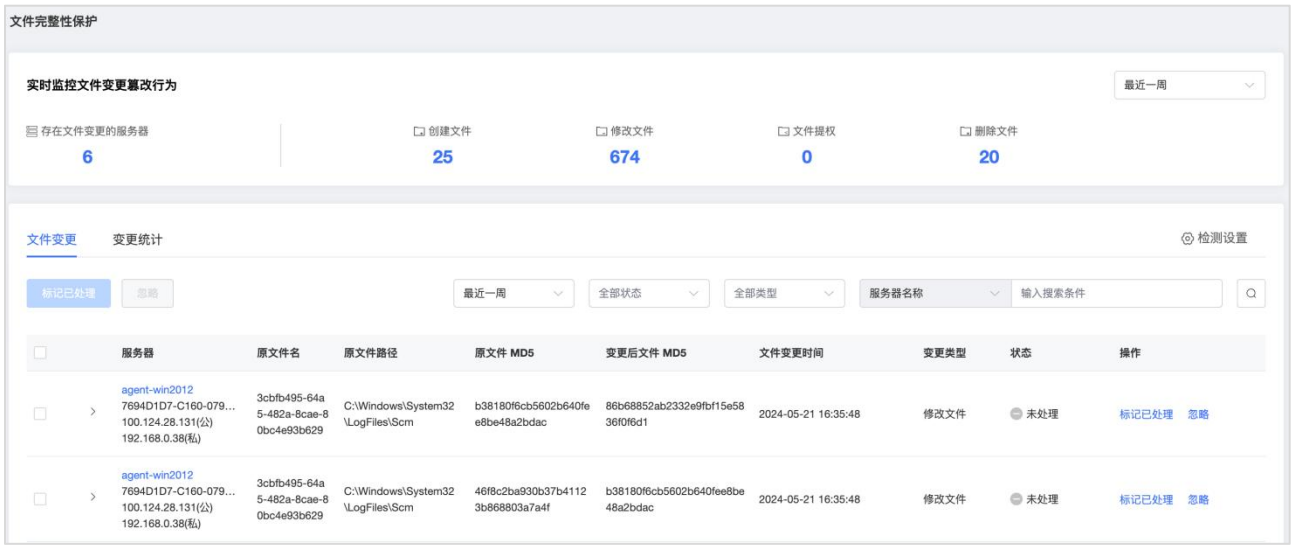
恢复任务：列表中展示用户下发恢复任务的状态及详情，包括备份路径、已恢复文件数、恢复服务器名称、恢复路径、执行时间、完成时间、执行状态。



4.9. 文件完整性保护

说明：文件完整性保护目前处于公测阶段，企业版用户可优先体验，请先购买企业版配额并绑定主机后，才能正常使用。

登录服务器安全卫士（原生版）控制台，在左侧导航栏选择文件完整性保护。如下图所示，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，下方展示告警事件详情。



告警详情

告警事件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、状态和操作。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。监控的文件变更行为包括创建文件、修改文件、文件提权、删除文件。

检测设置

- 文件监控设置
  - 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。
- 生效范围设置

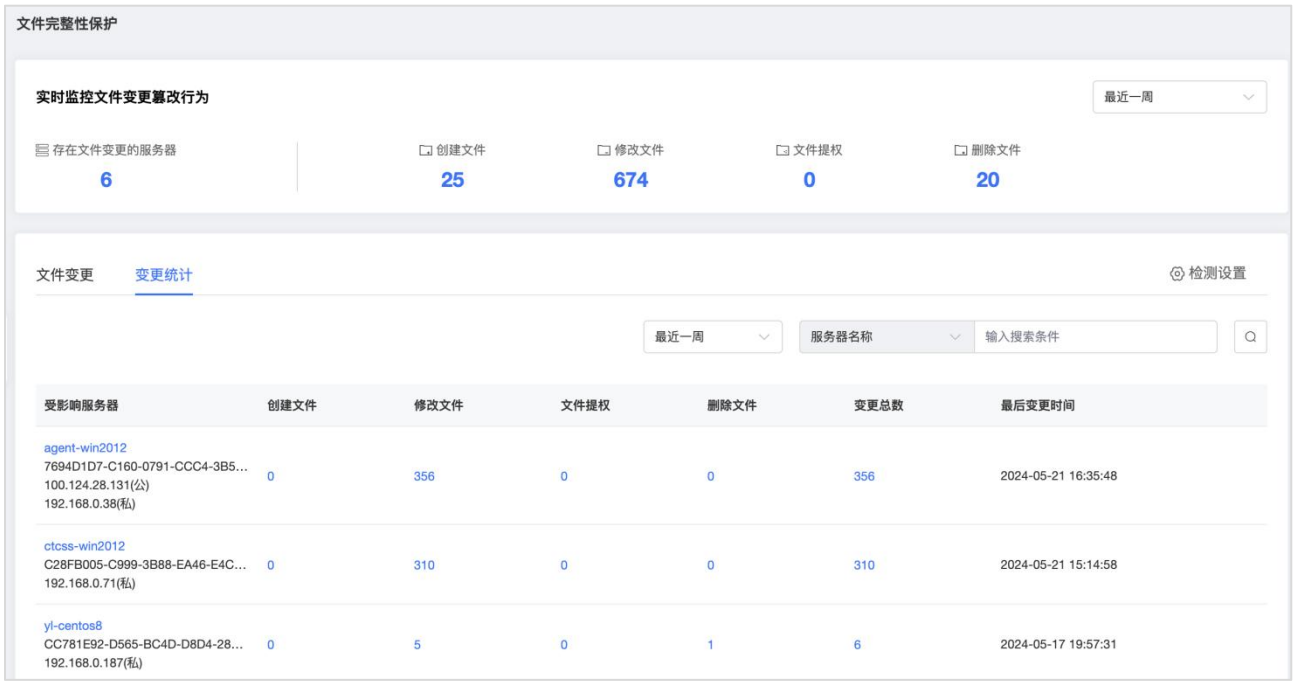
  自定义选择需要执行文件变更篡改行为监控的服务器。

处理方式

- 标记为已处理：人工对告警进行处理，处理后可将告警标记为已处理。
- 忽略：忽略本次文件变更篡改告警，如再次监控到文件变更篡改行为，将正常进行告警。

变更统计

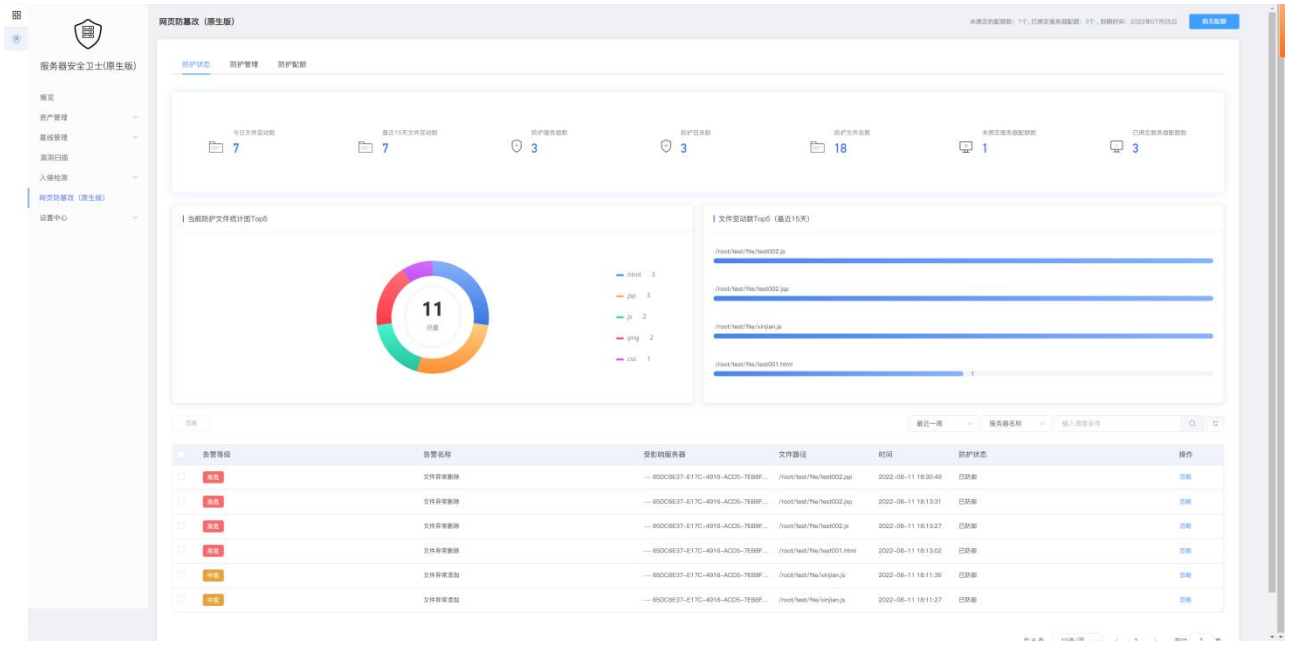
系统帮助您自动统计出所有存在文件变更篡改行为的服务器，单击文件变更类型可查看详情。



4.10. 网页防篡改（原生版）

4.10.1. 防护状态

如下图所示，防护状态包括防护总览、防护文件状态图和告警列表。

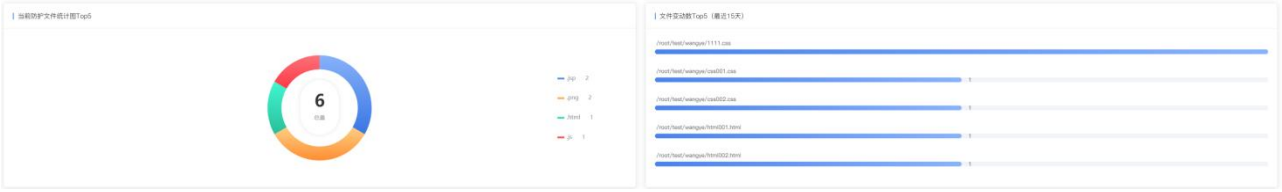


防护总览

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

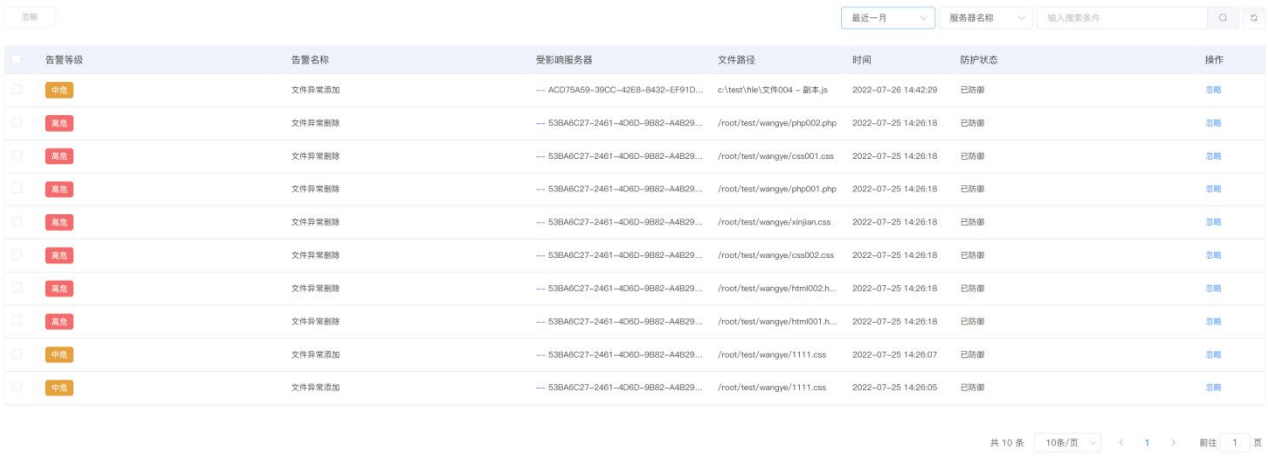
防护文件状态图

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

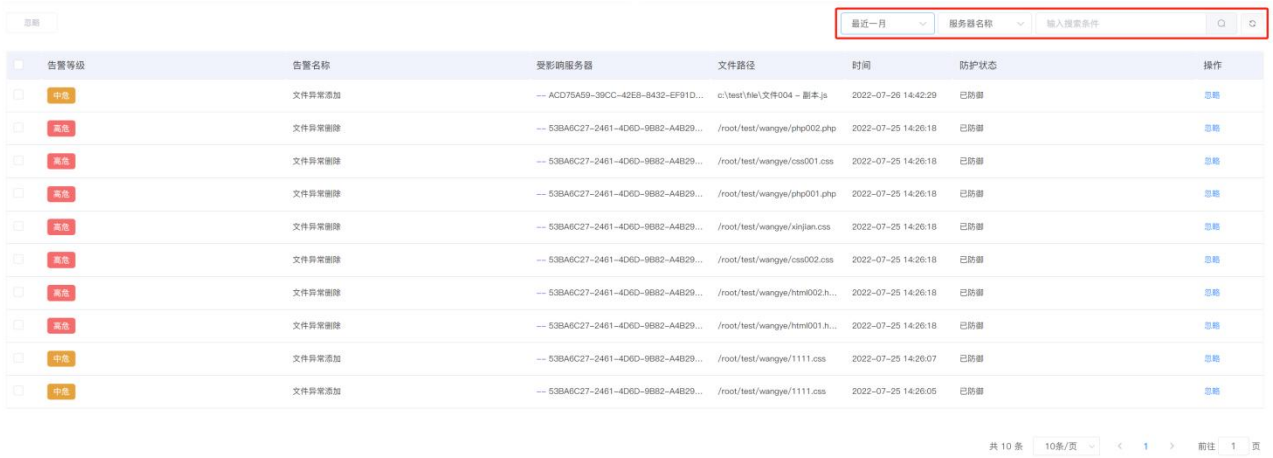


告警列表

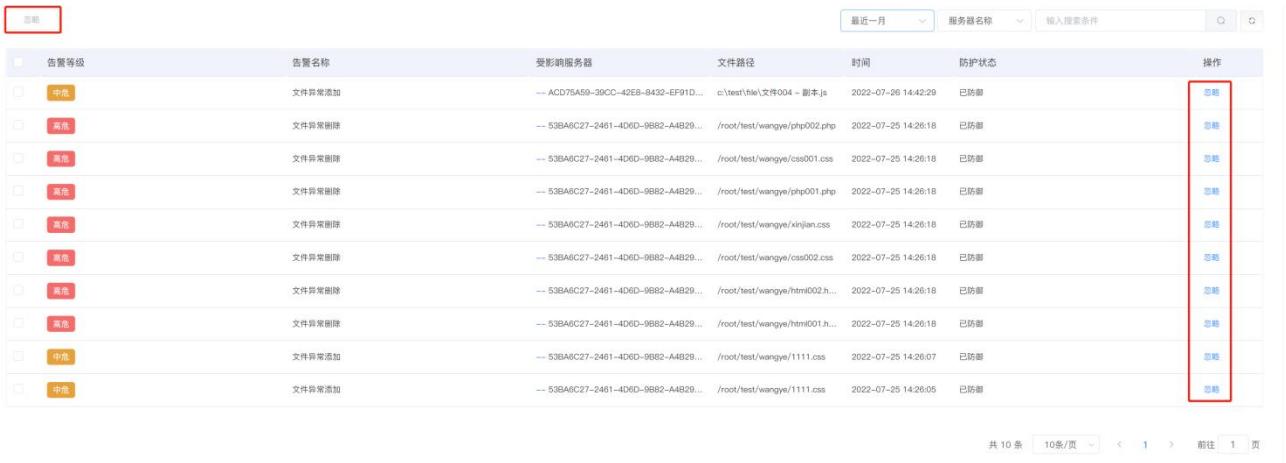
如下图所示，您可查看文件增加、删除、修改异常的告警列表，包括告警等级、告警名称、受影响服务器、文件路径、时间、防护状态和操作。告警列表默认按照时间排列，最后发生的篡改告警排列在最上方。



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

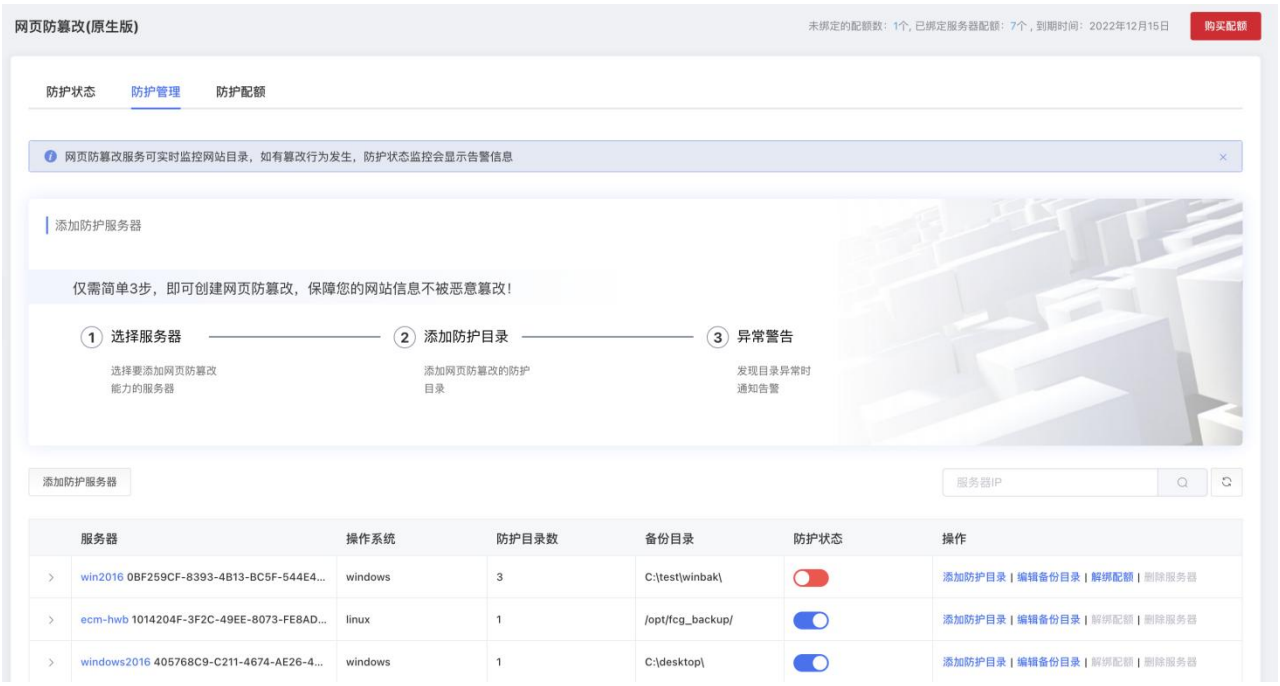


若当前告警不需要再展示，选择忽略或批量忽略操作后，则该告警不再展示在列表中，如下图所示：



4.10.2. 防护管理

如下图所示，防护管理页面为您展示添加防护服务器的引导步骤和已添加的防护服务器列表。



添加防护服务器

1. 点击防护管理页面的“添加防护服务器”，如下图所示。

2. 在弹出的对话框中，根据页面提示进行配置，选择需要防护的服务器，并选择配额后，方可进入下一步。

   在服务器列表中，展示用户所有的服务器；配额列表中，展示用户当前所有的配额。

3. 添加防护目录。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：

白名单模式添加防护目录、防护文件类型和本地备份目录，点击“开启防护”后，即开始对配置的文件进行防护。

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，点击“开启防护”后，即开始防护目录下所有未排除的子目录、文件类型和指定文件。其中，防护目录和本地备份目录为必填选项。

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

防护服务器管理

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

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

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

3. 在关闭该服务器的防护后，您可以解绑该服务器的防护配额，点击“解绑配额”，如下图所示。

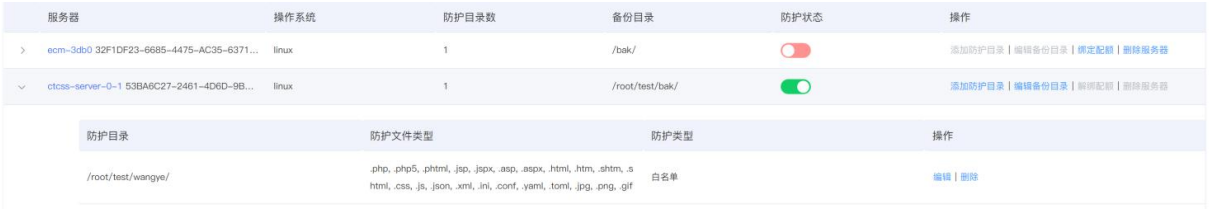
4. 点击后弹出如下对话框，确定后该配额与服务器解绑。解绑后该配额可以与其他服务器进行绑定，为其他服务器提供防护。

5. 在解绑配额完成后，可以点击“删除服务器”，如下图所示。

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

防护目录管理

1. 可对服务器已添加的防护目录进行编辑、删除操作，如下图所示。



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

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

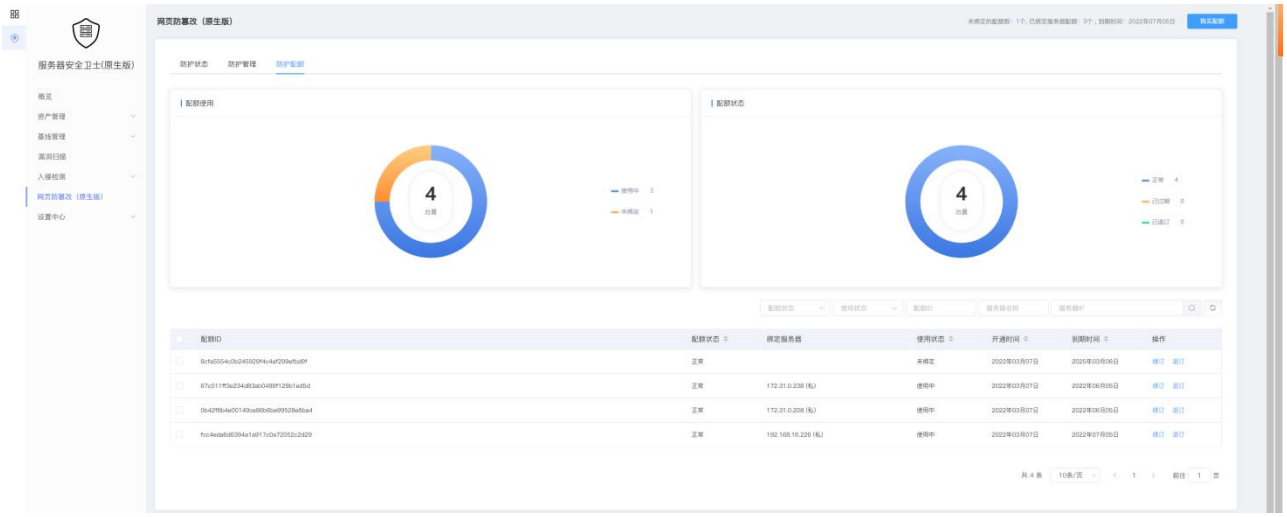
4. 若您需要为已添加防护的增加防护目录，请点击操作中的“添加防护目录”，如下图所示：

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

4.10.3. 防护配额

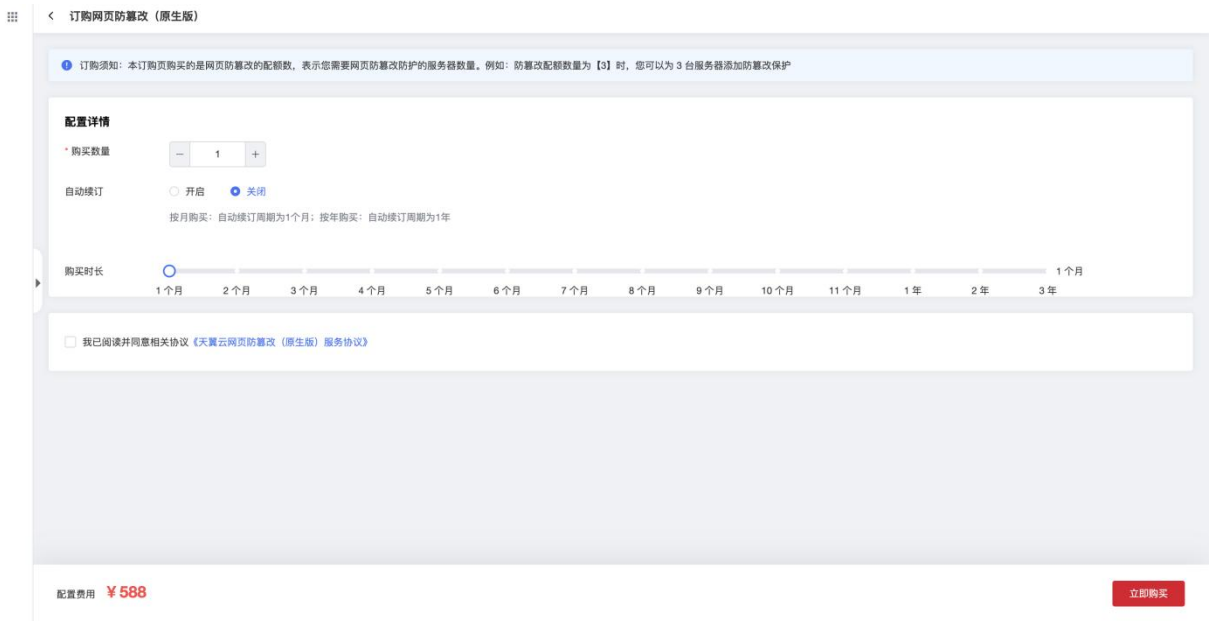
配额详情

如下图所示，防护配额为您展示配额的统计和配额的详情列表。



若您未购买网页防篡改的防护配额，则展示如下页面：

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



2. 购买完成后，即可进入防护配额页面。配额使用统计为您展示正常配额的使用情况统计，分为使用中和未绑定 2 种状态。

3. 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。

4. 配额列表展示正常、已到期、已退订 3 种状态的配额，销毁的配额不展示在列表中，包括配额 ID、配额状态、绑定服务器、使用状态、开通时间、到期时间、操作等信息。该列表可根据配额状态、使用状态、配额 ID、服务器名称和服务器 IP 进行查询。

配额计费

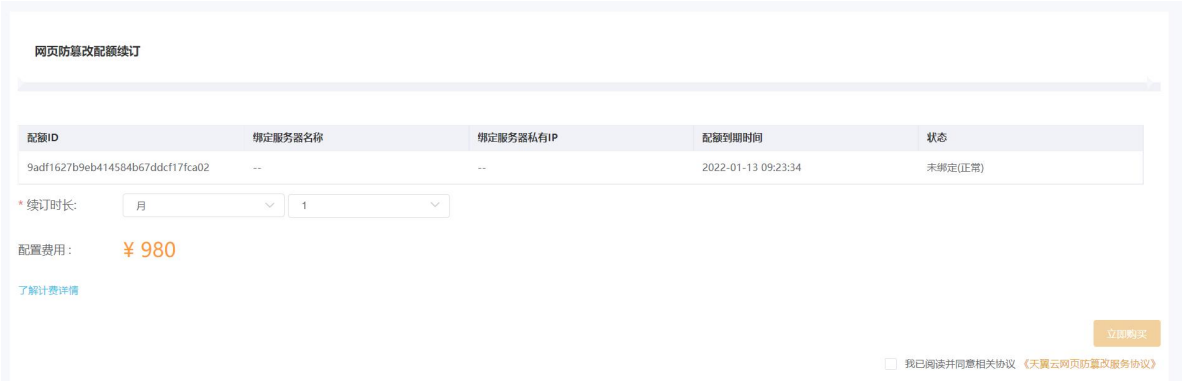
本节为您展示配额计费的相关操作，包括配额订购、配额续订、配额退订和到期处理相关操作。

配额订购：前面已详述，此处不再赘述。

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

如下图所示，对需要续订的配额，点击“续订”：

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



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

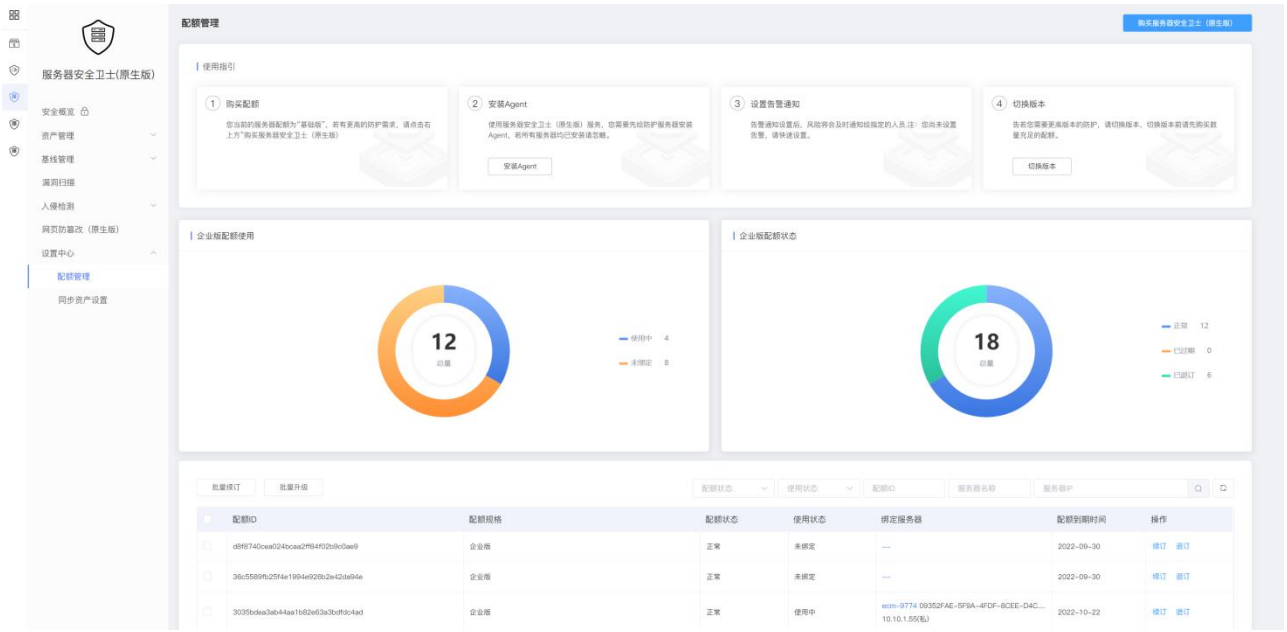
进入“退订”页面后，您需要进行确认退订的规则和金额，点击“退订”按钮，即可对该配额的网页防篡改（原生版）服务进行退订，如下图所示：

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。

4.11. 设置中心

4.11.1. 配额管理

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



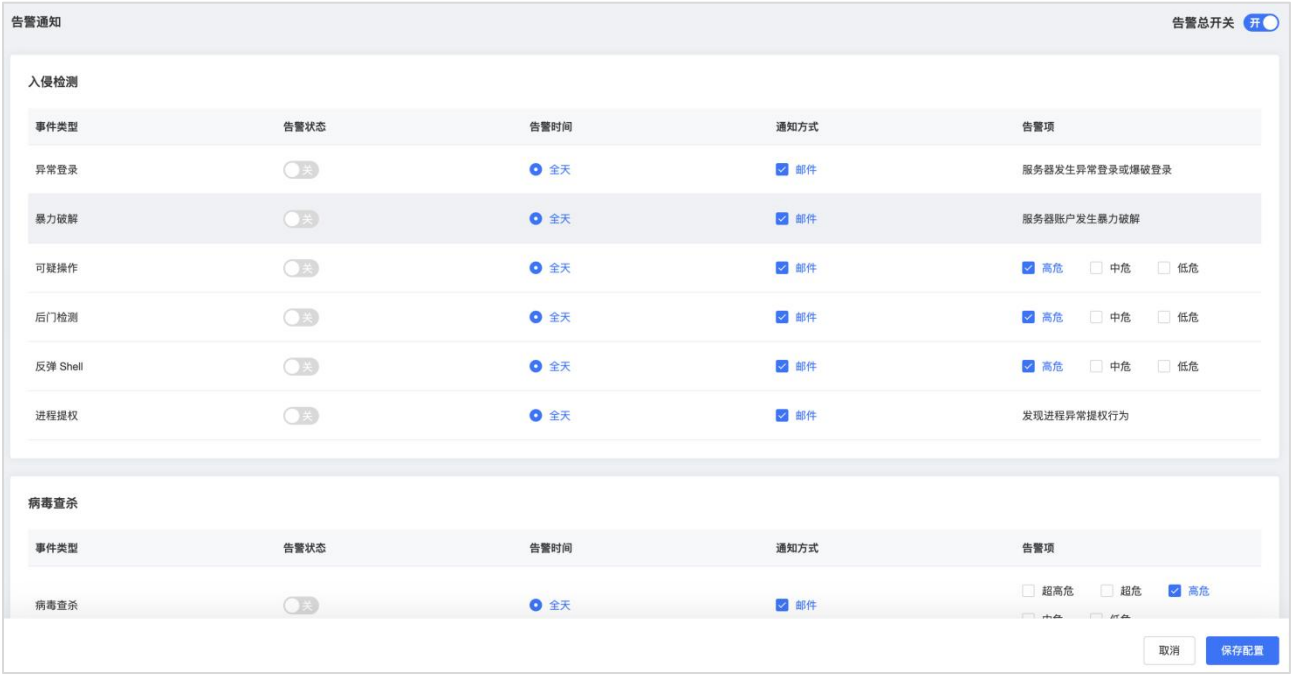
4.11.2. 同步资产设置

如下图所示，同步资产设置为您提供了资产同步时间的设置入口。

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

4.11.3. 告警通知

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->告警通知。



告警通知配置

根据您的使用场景进行告警通知配置，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。

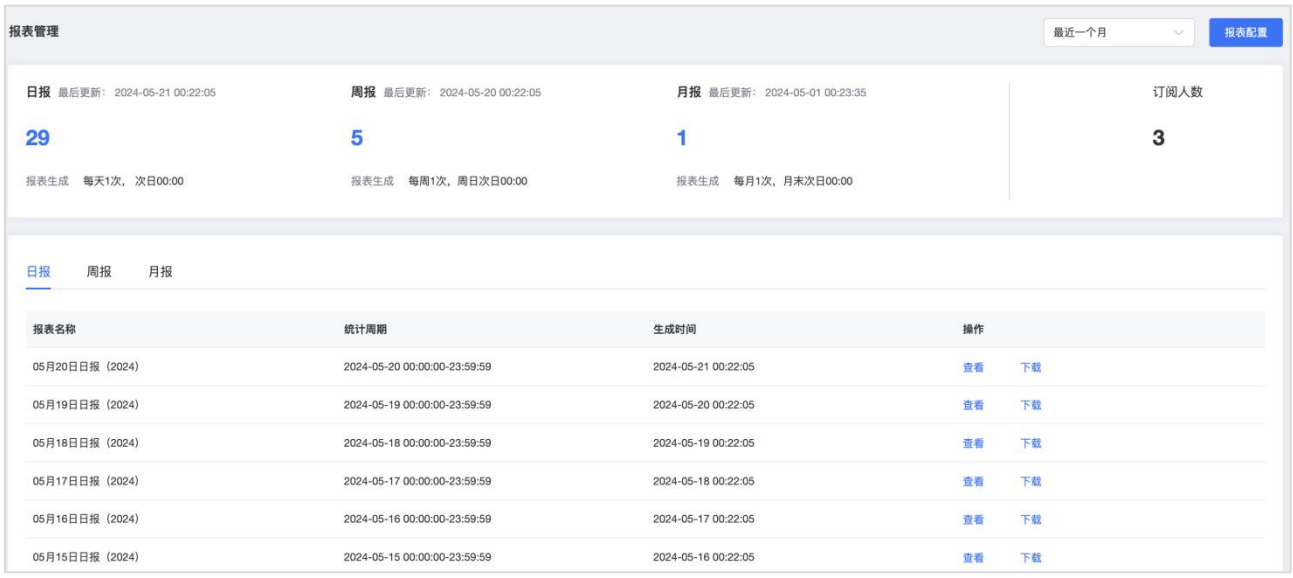
配置项	说明
告警开关	自定义开启需要通知的事件类型
告警时间	事件发生时实时发送告警通知
通知方式	通过邮件方式发送告警通知
告警项	根据威胁等级自定义发送通知

4.11.4. 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。

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

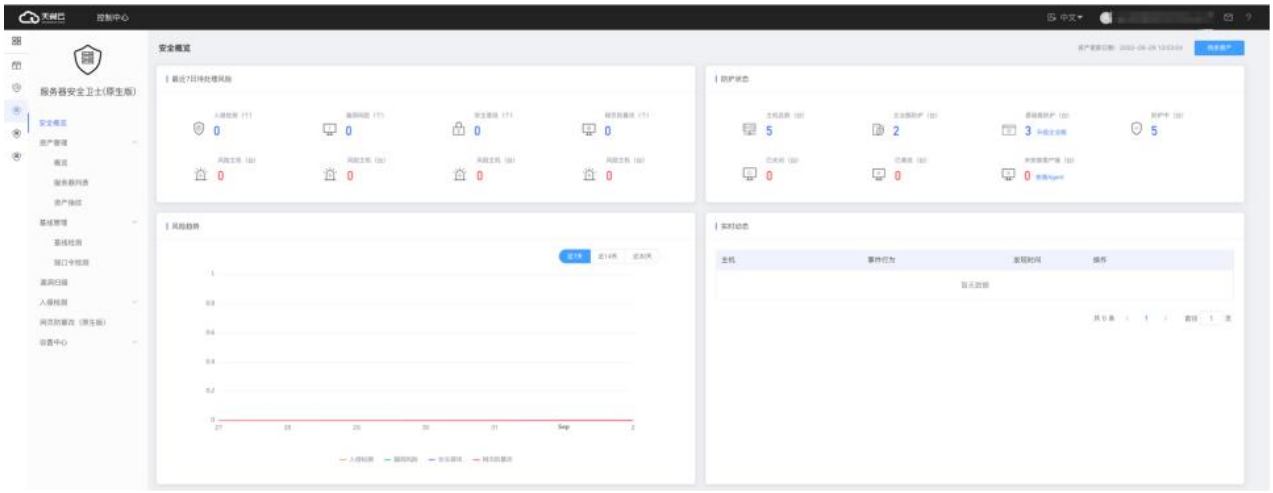
报表管理页面生成安全报表后，提供安全报表查看和下载能力。

5. 最佳实践

5.1. 快速掌握服务器安全态势

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

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

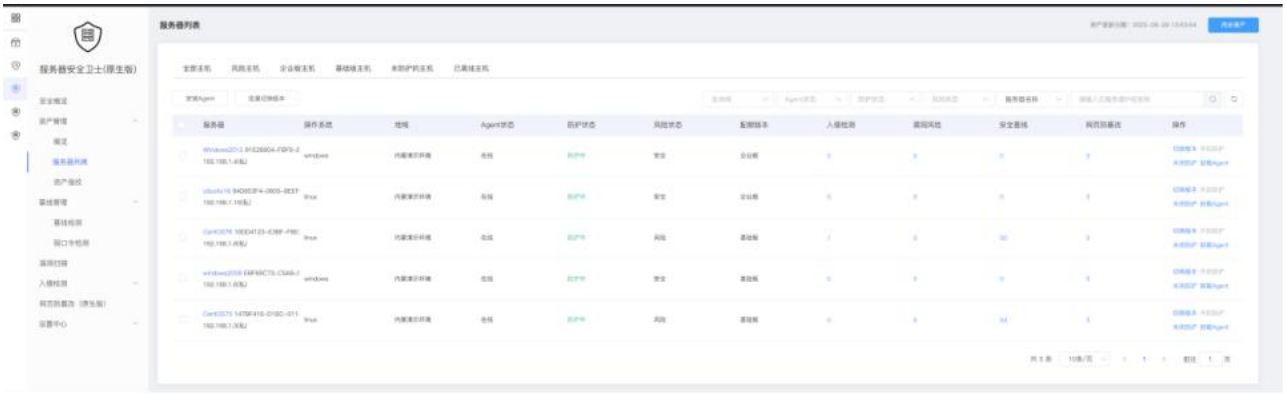


风险统计	说明
最近 7 日待处理风险	您可以查看入侵检测、漏洞风险、安全基线、网页防篡改及对应的风险主机情况
防护状态	您可以查看用户资产情况，包括主机总数、企业版防护、基础版防护、防护中、已关闭、已离线、未安装客户端的云主机台数
风险趋势	您可以查看近 7 天、14 天、30 天的风险趋势图

风险统计	说明
实时动态	您可以查看当前最新发现的风险事件详情

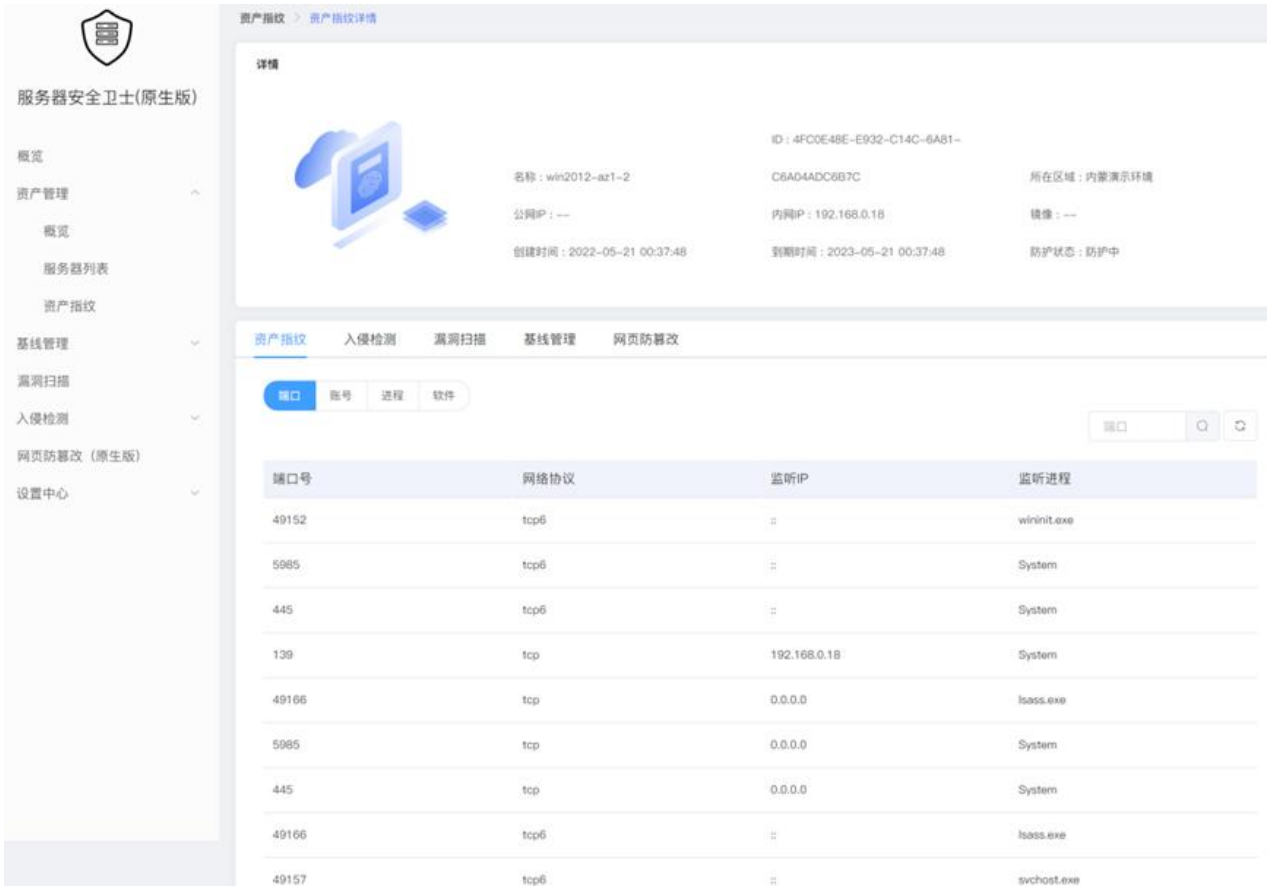
5.2. 查看单台服务器风险

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

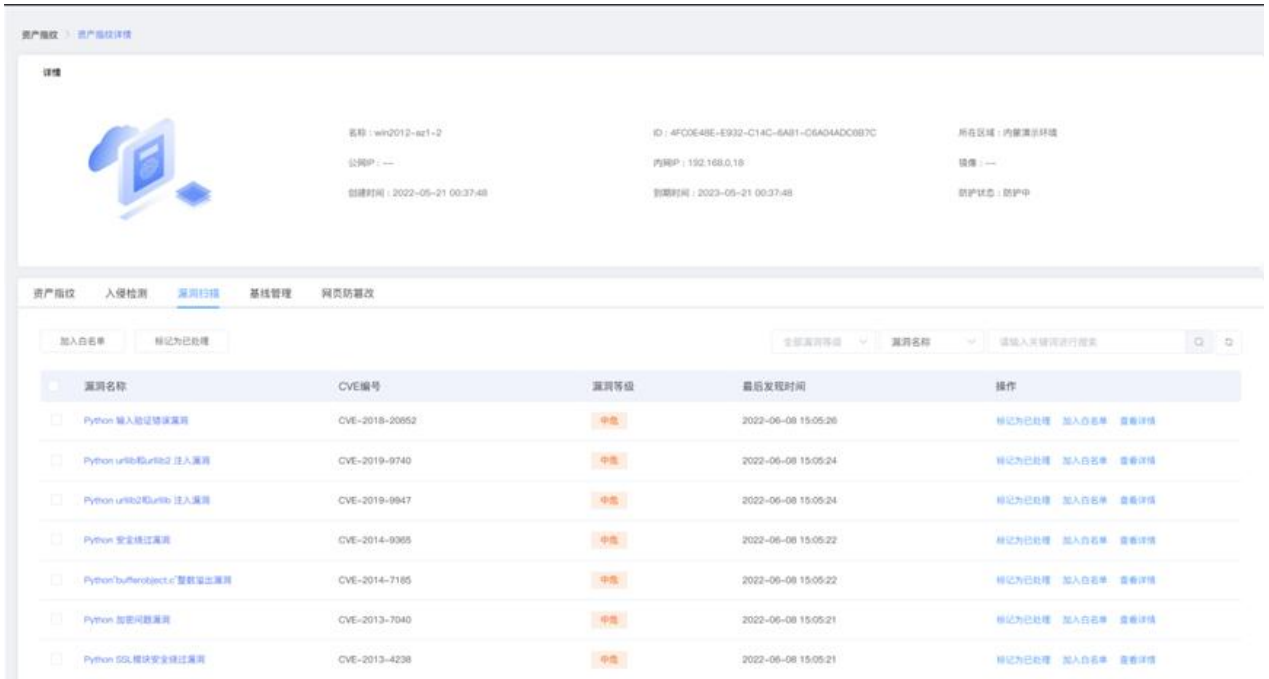


2、在搜索框中输入您需要查看的服务器名称或 IP，则显示出该服务器的名称、ID、IP、操作系统、地域、Agent 状态、防护状态、风险状态、入侵检测风险数、漏洞风险风险数、安全基线风险数、网页防篡改风险数和操作。

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



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



5.3. 弱口令安全最佳实践

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

弱口令带来的危害

在服务器系统中使用弱口令可能会造成以下危害：

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

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

如何避免设置弱口令

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

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

并且建议您每隔 3 个月更改一次口令。

常见系统口令修改方式

1、 Linux 系统

登录 Linux 系统命令行，执行命令：passwd 根据提示修改用户口令

2、 Windows 系统

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

3、MySQL 数据库

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

4、Redis 数据库

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

5、PostgreSQL 数据库

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

5.4. 漏洞扫描最佳实践

什么是漏洞?

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

对企业的危害

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

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

对用户的危害

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

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

对社会的危害

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

如何进行漏洞扫描

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

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

漏洞扫描支持的方式

1、定期扫描：

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

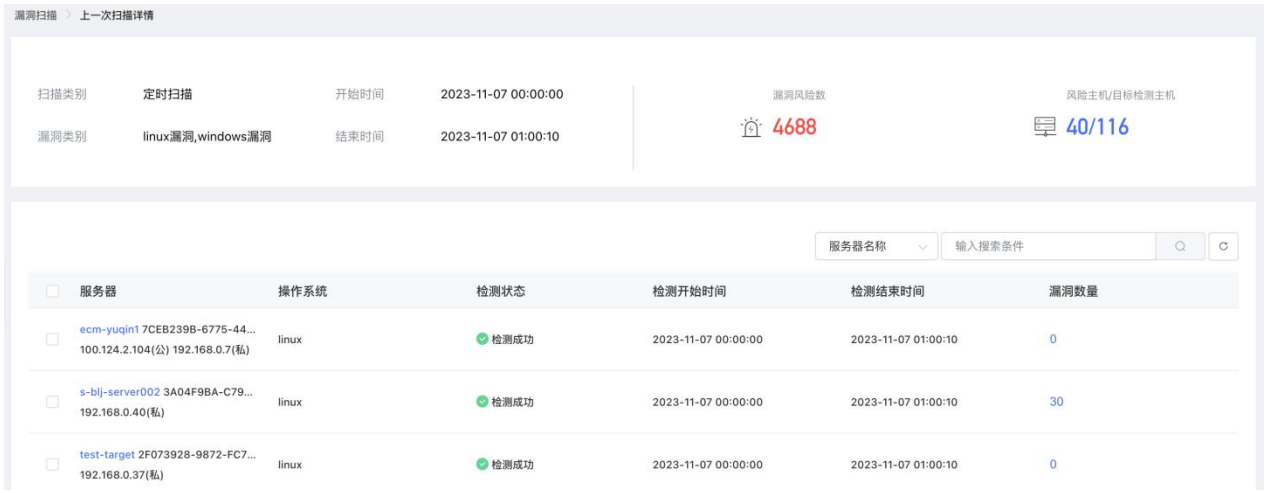
2、立即扫描：

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。

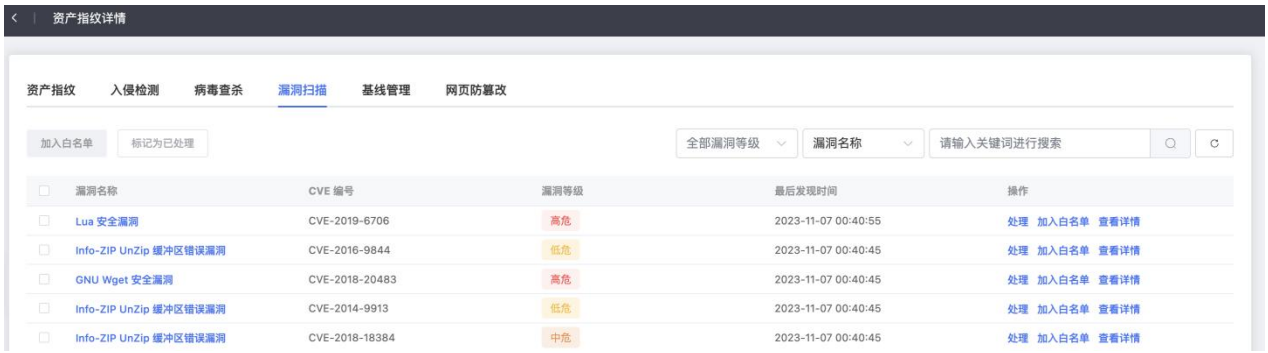
查看漏洞扫描结果

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



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

1、标记处理

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

2、加入白名单

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

3、移除白名单

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

修复漏洞事件

您可以根据参考链接或补丁获取链接进行漏洞修复。

5.5. 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:

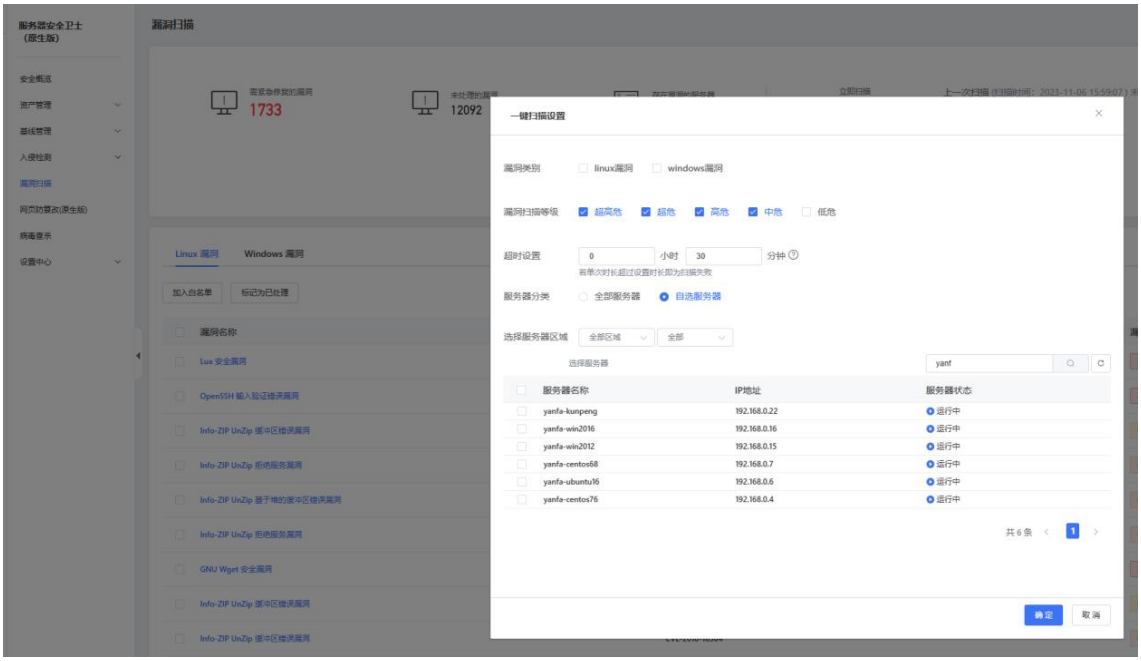
http://www.openssh.com/

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

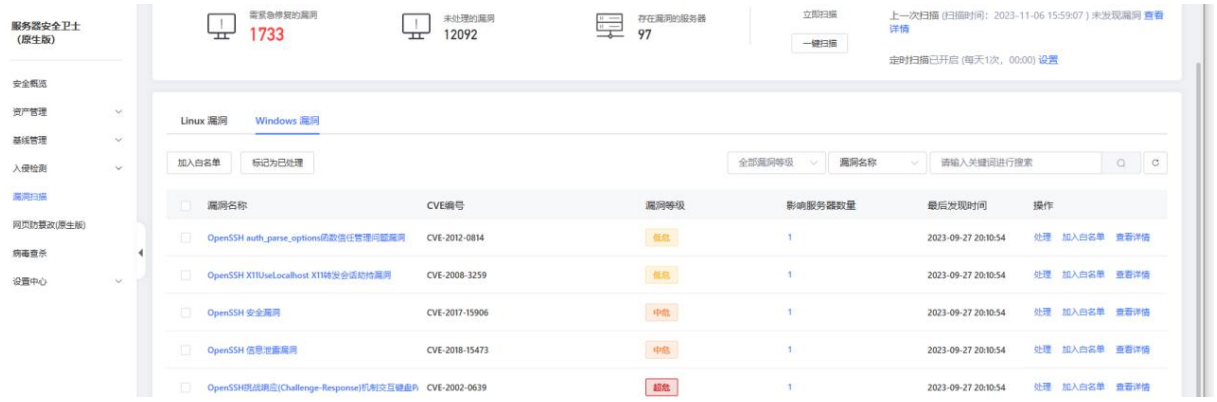
检测与修复建议

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“手动检测”，验证该漏洞是否修复成功。

5.7. 等级保护测评合规最佳实践

等级保护测评背景

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

安全计算环境要求

服务器安全卫士（原生版）在等级保护测评（三级）“安全计算环境”中可满足项：

- 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。

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）产品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）分为基础版和企业版，基础版提供服务器资产梳理、漏洞扫描、异常登录、暴力破解检测等基础安全功能；企业版在基础版功能的基础上提供后门检测、可疑操作、病毒查杀、基线检查、反弹 Shell 检测等功能，满足用户在等保合规、攻防实战等场景的安全需求。

Q：天翼云服务器安全卫士（原生版）都支持哪些资源池的服务器防护?

A：目前天翼云服务器安全卫士（原生版）为您提供服务器的资源池共 33 个，包括：上海 7、上海 36、南京 2、南京 3、南京 4、南京 5、杭州 2、杭州 7、芜湖 2、合肥 2、华东 1、九江、南昌 5、青岛 20、佛山 3、广州 6、武汉 3、武汉 4、武汉 41、华南 2、福州 3、福州 4、福州 25、郑州 5、长沙 3、长沙 42、

郴州 2、海口 2、南宁 2、南宁 23、北京 5、华北 2、石家庄 20、呼和浩特 3、内蒙 6、太原 4、晋中、辽阳 1、西安 3、西安 4、西安 5、西安 7、中卫 2、中卫 5、兰州 2、西宁 2、乌鲁木齐 27、西南 1、西南 2-贵州、拉萨 3、昆明 2、重庆 2、成都 4、贵州 3、香港 1。

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）否可以申请试用?

A：服务器安全卫士（原生版）企业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）购买后遇到问题后如何解决？

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：如何快速使用服务器安全卫士（原生版）

1. 注册天翼云账号

   在创建和使用服务器安全卫士（原生版）之前，需要先注册天翼云门户的账号并进行实名认证。

2. 开通服务器安全卫士（原生版）

   进入到服务器安全卫士（原生版）管理控制台，阅读并同意《天翼云服务器安全卫士（原生版）服务协议》

3. 购买配额

进入到服务器安全卫士（原生版）产品购买页面，选择购买版本、防护服务器台数、购买时长进行购买。

4. 安装 Agent

   安装 Agent 后才可以正常开启安全防护功能。

5. 设置告警通知

   发现告警后，用户可及时收到服务器安全卫士（原生版）发送的告警通知。

6. 查看检测结果

   在功能告警页面可以查看风险详情，并支持对威胁进行处置。

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，详情见下表：

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

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

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”。

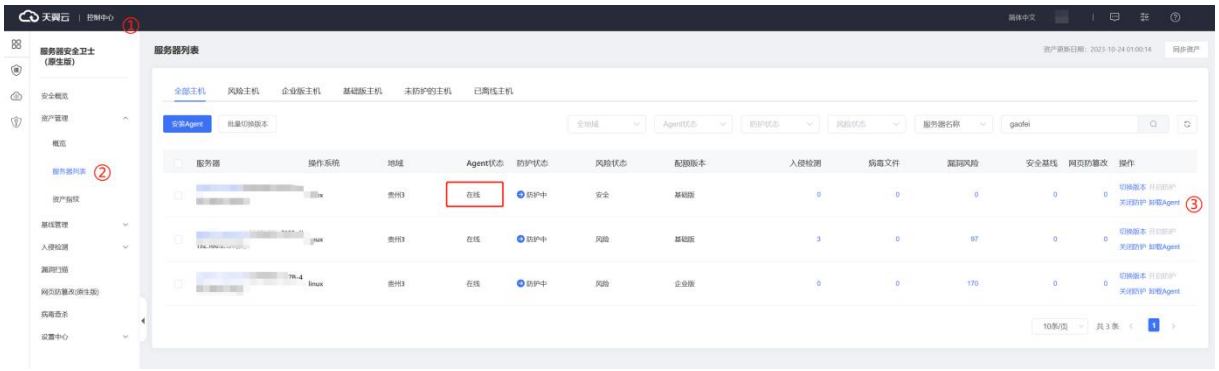
- 若状态为“在线”，则本台服务器已安装 Agent 并自动激活，Agent 服务正常。
- 若状态为“离线”、“错误”、未激活”，则需要为服务器重新安装 Agent。
  - Linux 系统安装命令

  - Windows 系统安装命令

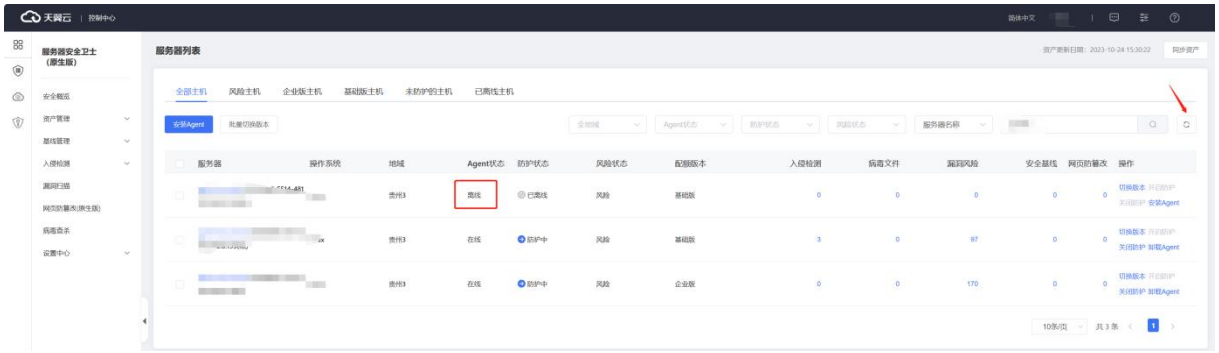
Q：如何卸载 Agent

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：

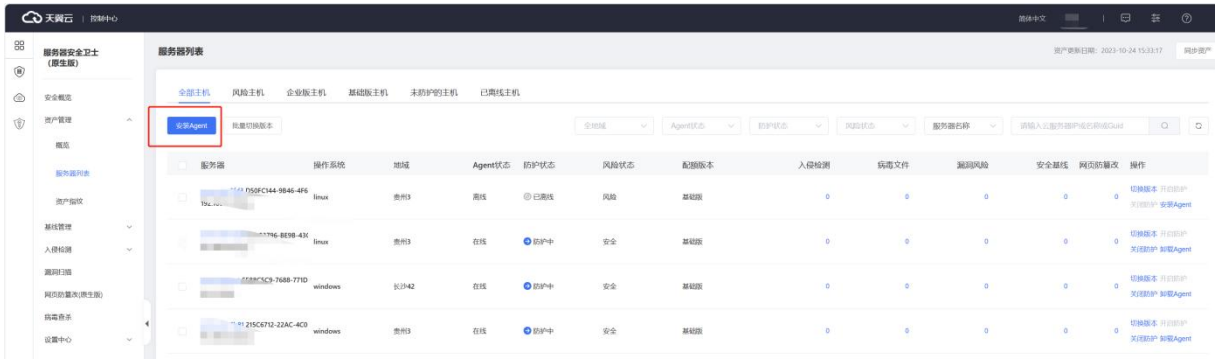
  登录到 Windows 云主机，在”控制面板 -> 程序和功能“中找到“CTCSS Agent"或"CTCSSAgen”，右键点击，选择卸载，按照提示卸载。

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。

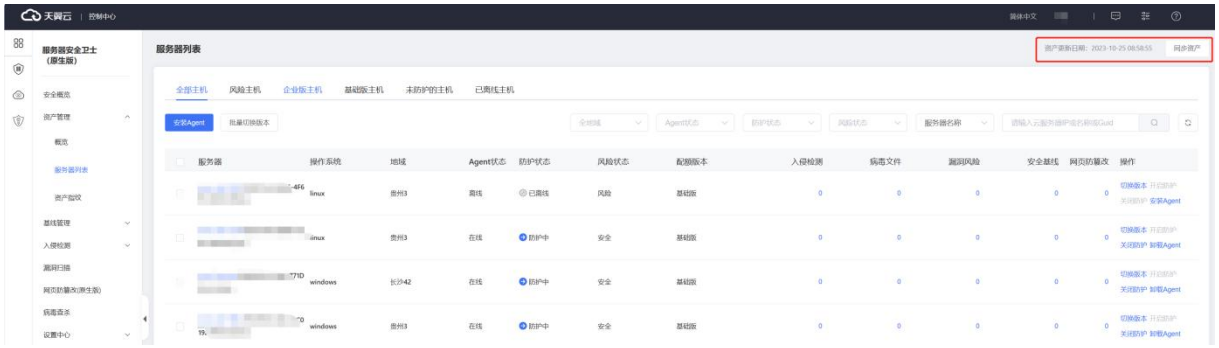
3、 卸载 Agent 后再次尝试安装

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?

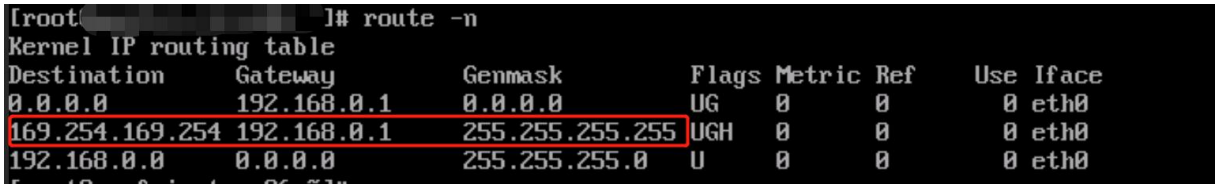
若安装 Agent 后，在服务器安全卫士界面无法找到安装 Agent 的云主机，或者 Agent 状态仍然为“离线”状态，则可能 Agent 与服务端无法正常通信，状态异常。可按以下方法排查解决：

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，参见服务器安全卫士支持的系统。

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。



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，“未防护的主机”页面为您展示防护状态为“未防护”的全部服务器。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
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?

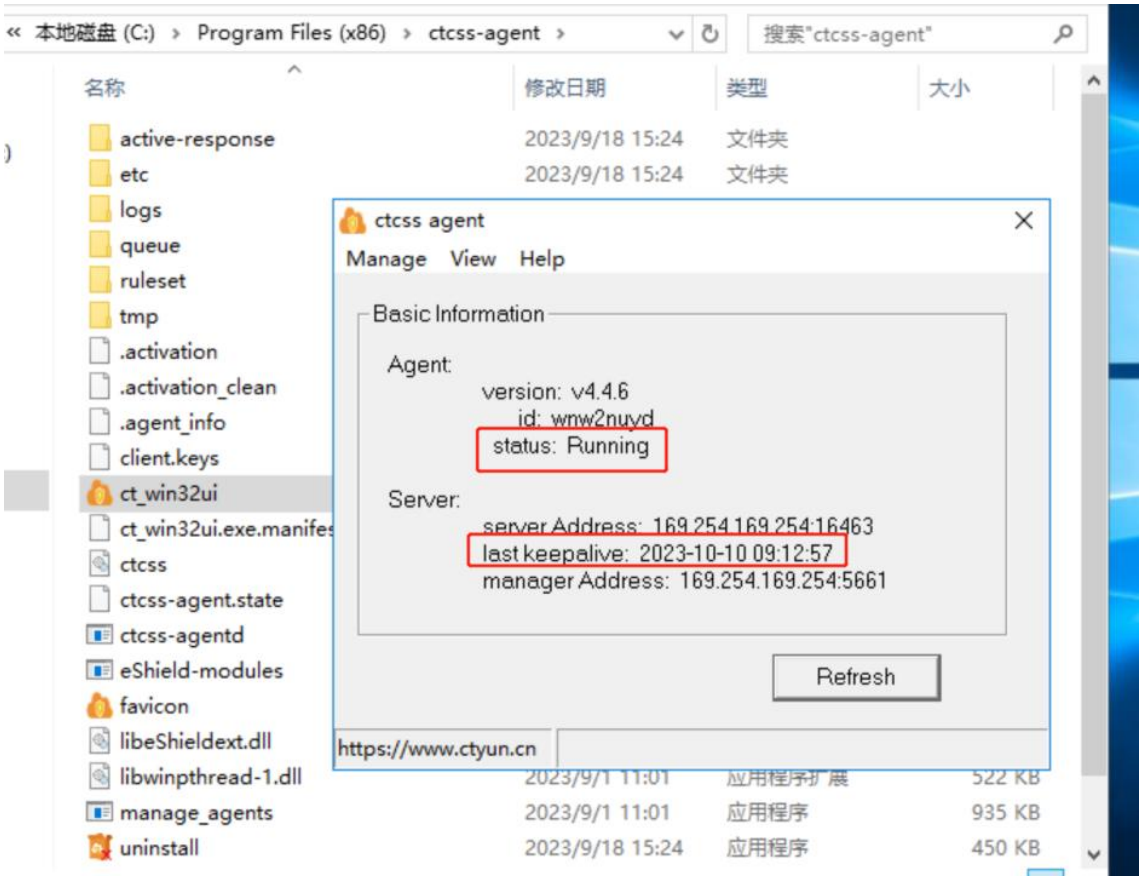
共用一个 Agent，在天翼云控制台上统一下发管理防护策略，Agent 执行监控与处置。

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

```
[root@ecm-3b9b logs]# service ctcss status
Running
[root@ecm-3b9b logs]#
```

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

```
[root@gaofei-ctcss06 logs]# systemctl status ctcss
● ctcss.service - Ctcss agentd
   Loaded: loaded (/etc/systemd/system/ctcss.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-09-18 14:39:04 CST; 3 weeks 0 days ago
 Main PID: 3710115 (ctcss-agentd)
    Tasks: 15 (limit: 512)
   Memory: 42.3M (limit: 500.0M)
      CPU: 25min 53.871s
   CGroup: /system.slice/ctcss.service
           ├─ 329095 /var/ctcss/bin/eShield-modules
           └─3710115 /var/ctcss/bin/ctcss-agentd

Sep 18 14:39:04 gaofei-ctcss06.novalocal systemd[1]: Started Ctcss agentd.
```

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）

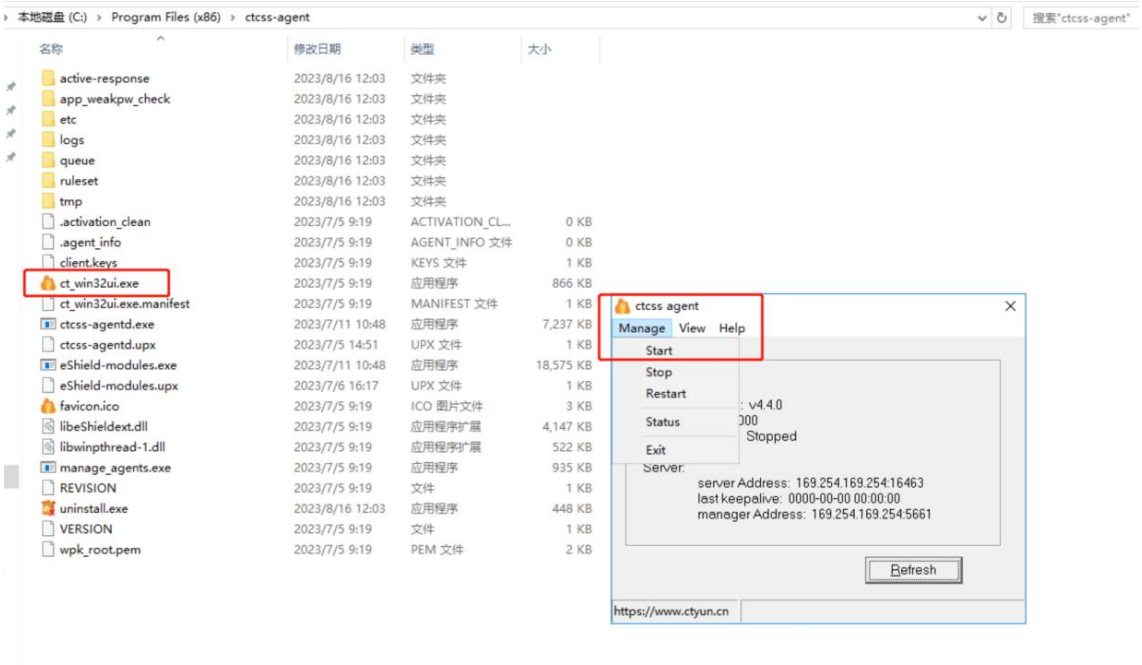
```
[root@ecm-3b9b logs]# cat /var/ctcss/var/run/eShield-agent.state
# State file for eShield Agent

# Last time a keepalive was sent
last_keepalive='2023-10-10 10:00:54'
```

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。

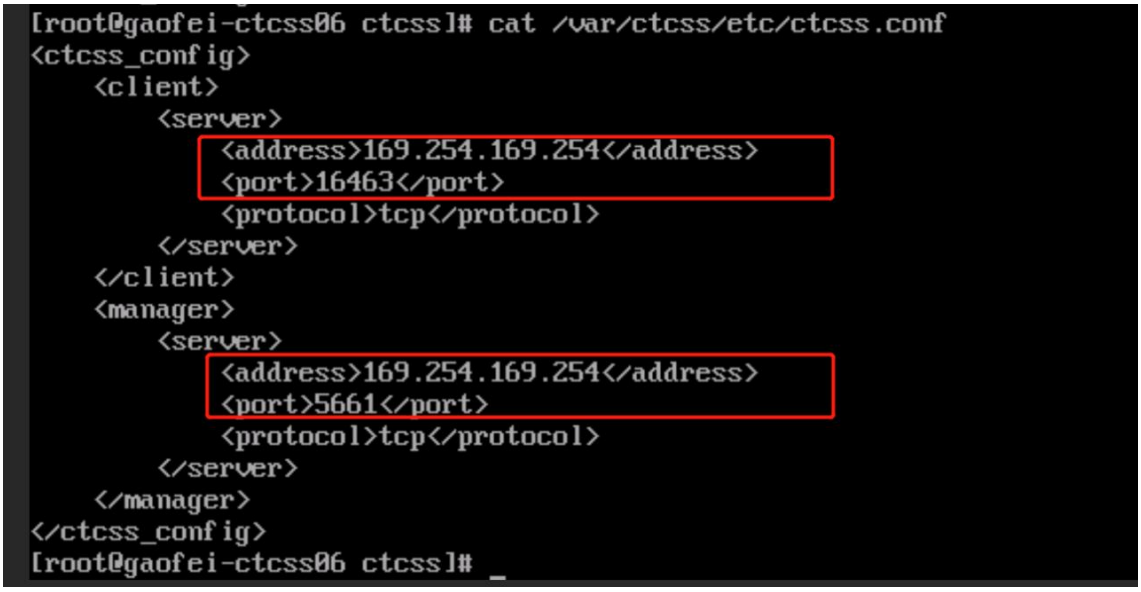
3. 检查安全卫士 Agent 配置。

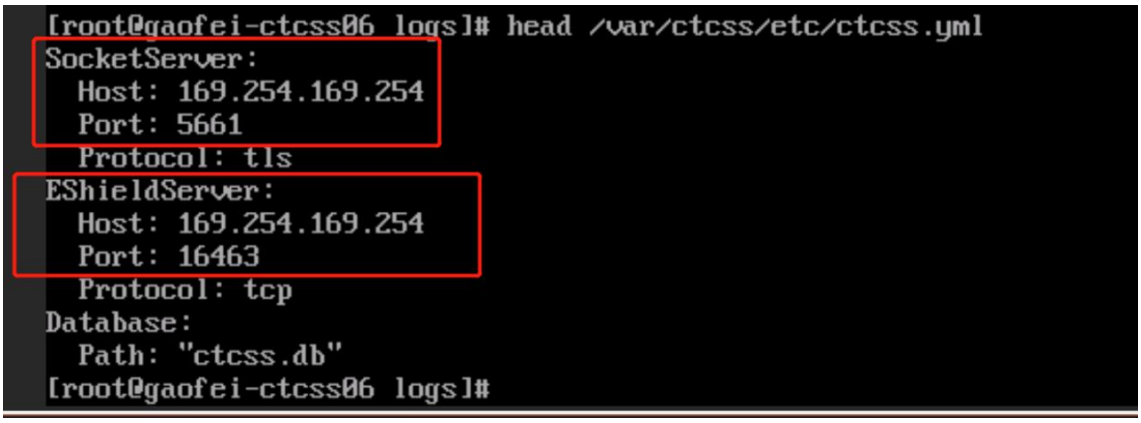
若 Agent 处于 running 状态，但 last keepalive 时间未更新，则可能为配置文件错误。

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）。





配置修改完成后需按前述步骤重新启动 Agent。

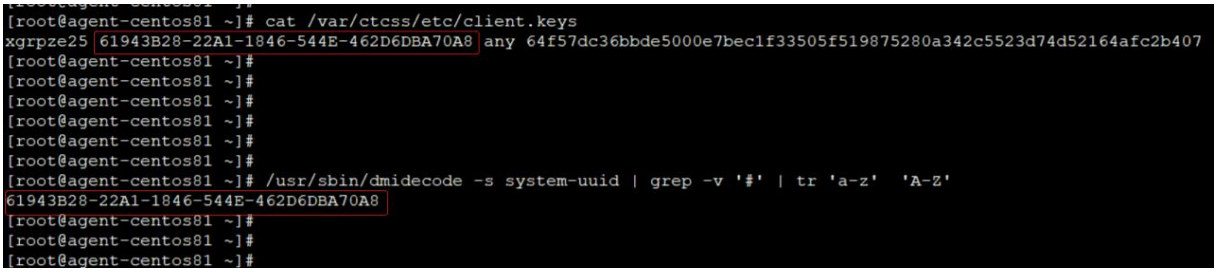
4. 检查 Agent 的激活文件中的信息。

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）均为包周期计费，分为按月和按年 2 种方式。

Q：服务器安全卫士（原生版）和网页防篡改（原生版）的计费项是什么？

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

Q：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。

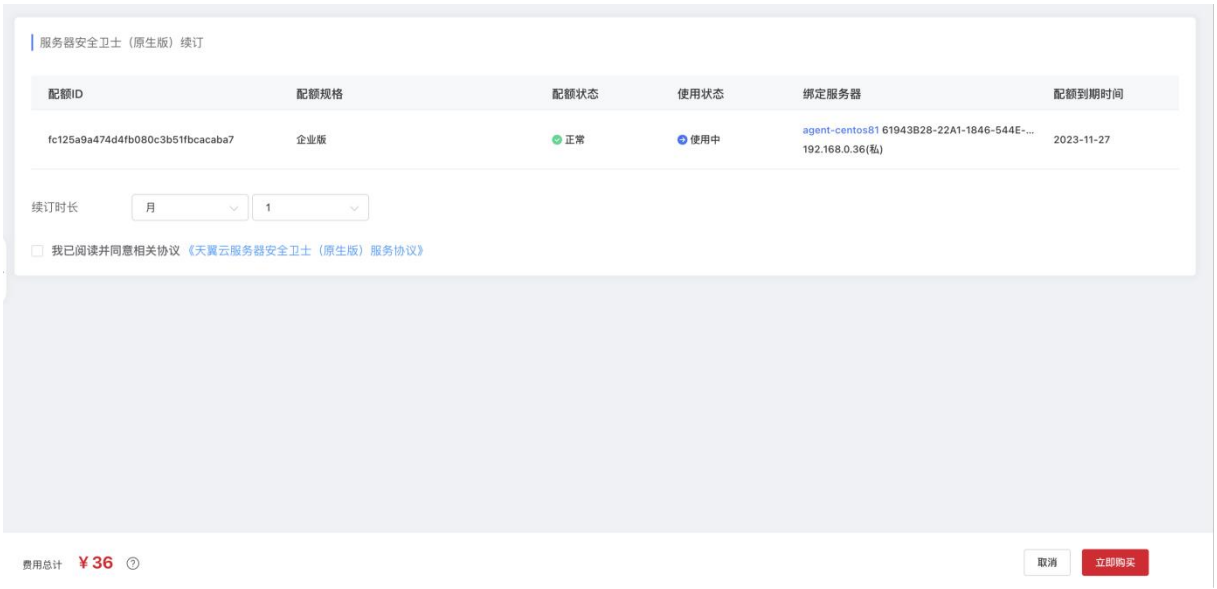
Q：服务器安全卫士（原生版）可以按天购买吗？

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. 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，在配置管理页面查看您已经订购的配额，选择所需续订的配额，点击“续订。

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



Q：服务器安全卫士（原生版）安全服务如何退订?

1. 您可以登录服务器安全卫士（原生版）控制台，在左侧导航中选择设置中心 -> 配额管理，在配置管理页面查看您已经订购的配额，选择所需退订的配额，点击“退订。

2. 在退订页面中，选择退订原因，勾选我已确认本次退订金额和相关费用后，并点击“退订”后即可进行退订。

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

Q：如何绑定网页防篡改防护配额?

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

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. 在添加防护服务器中选择要添加的防护服务器，并选择防护配额，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。

操作步骤：添加防护目录、防护文件类型和本地备份目录，点击“开启防护”后，即开始对配置的文件进行防护。

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：单个防护目录大小不超过 2GB,可支持同时添加多个防护目录。

Q：开启网页防篡改后，如何修改文件?

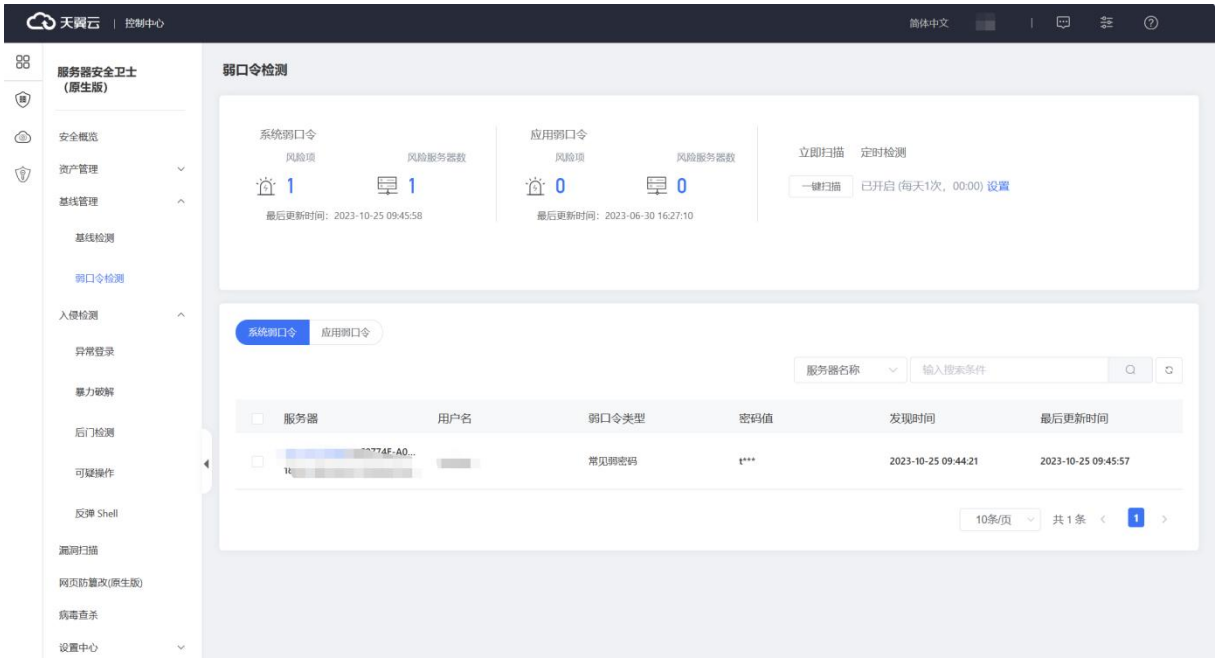
A：网页防篡改功能开启后，防护目录中的文件不可修改，如果需要修改文件或更新网站，请暂时关闭网页防篡改功能，完成修改或更新后再重新开启。关闭网页防篡改期间，文件存在被篡改的风险，更新文件后请及时开启网页防篡改。

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“标记为已处理”，即可消除本条告警记录。同时，您可以点击“白名单管理->新增白名单”，将您常用的登录源 IP、登录地区、登录账号、登录时间加入白名单，则下次不会再进行异常登录告警。

Q：如何查看异地登录的源 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?

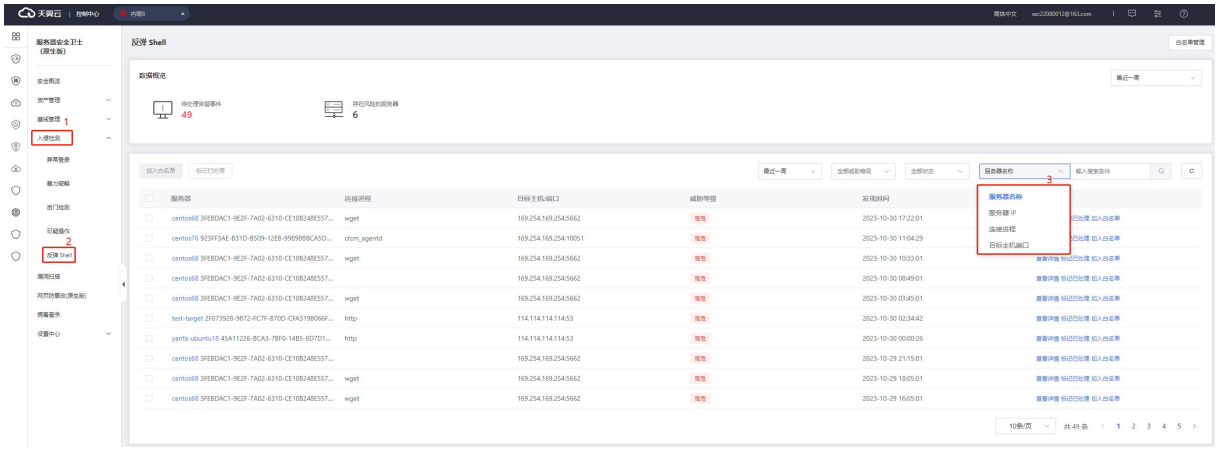
反弹 Shell 是一种网络安全攻击技术，也被称为"反向连接"。它的原理是通过在受害者的计算机上执行一个恶意程序（通常是一个后门程序），并使其与攻击者的计算机建立一个反向连接。这样，攻击者就可以获取对受害者计算机的控制权，并执行各种命令、操作和访问敏感信息。

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 -> 反弹 Shell，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。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，您可以点击“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?

反弹 Shell 是企业版的功能，您需要开通企业版防护，才会开启反弹 Shell 检测。开通企业版防护后，将自动开启反弹 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：

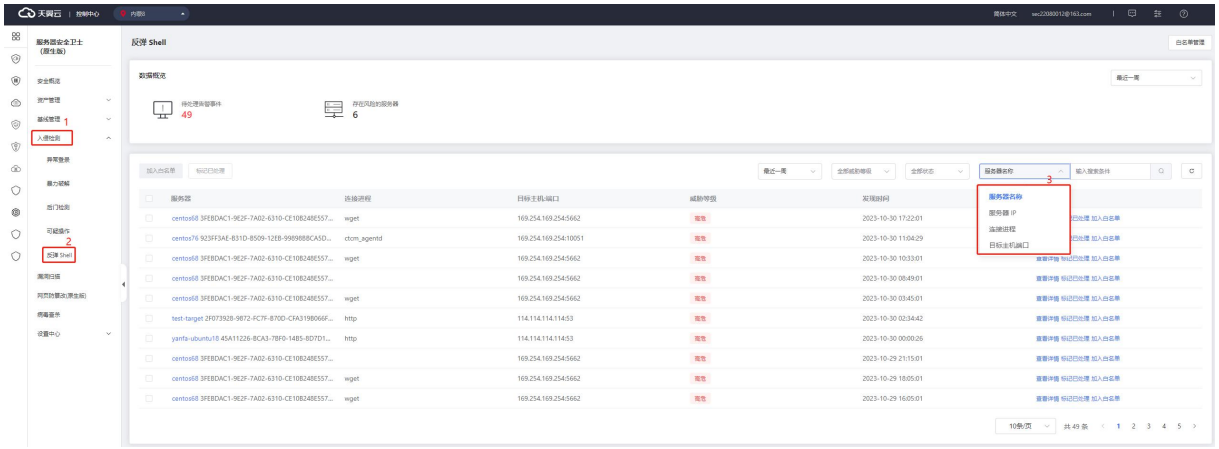
操作系统	工具	反弹名称	技术类别
Linux	bash	bash 反弹	标准输入输出重定向 socket
	exec	exec TCP 反弹	标准输入输出重定向 socket
		exec UDP 反弹	应用程序命令中转
		exec TCP 反弹	应用程序命令中转

操作系统	工具	反弹名称	技术类别
	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 -> 反弹 shell，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。

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。单击“标记为已处理”，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?

1. 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。
2. 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。
3. 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
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？

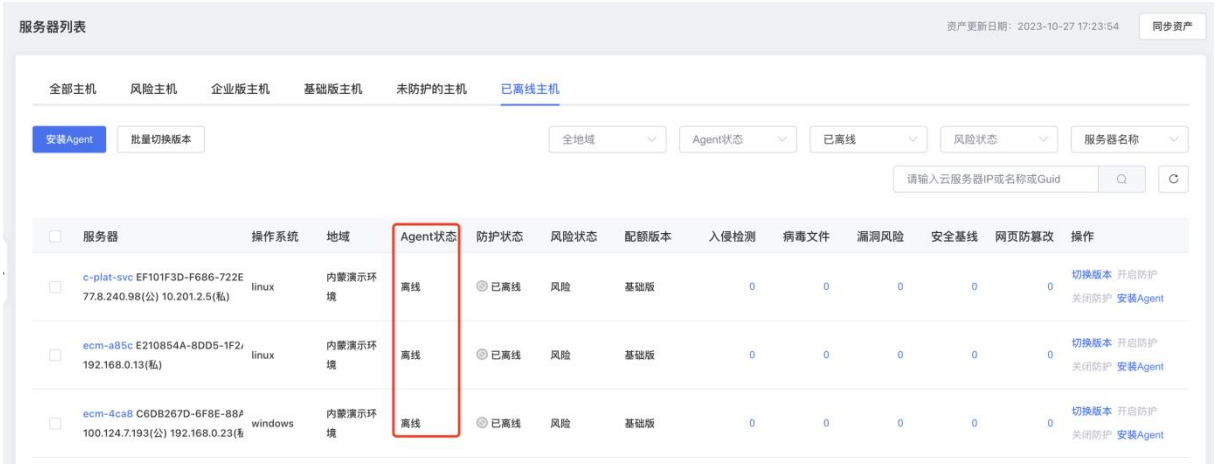
1、进入服务器安全卫士（原生版）控制中心

2、进入基线管理->基线检测页面，找到策略管理设置。

3、创建基线策略，选择服务器分类并自选服务器下发检测任务。

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：漏洞扫描时间过长怎么办？

为防止漏洞扫描时间过长影响业务正常使用，您可以配置超时设置，单次漏洞扫描任务超过设置的时长即为扫描失败，自动结束扫描任务。超时设置支持用户自定义配置。

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。

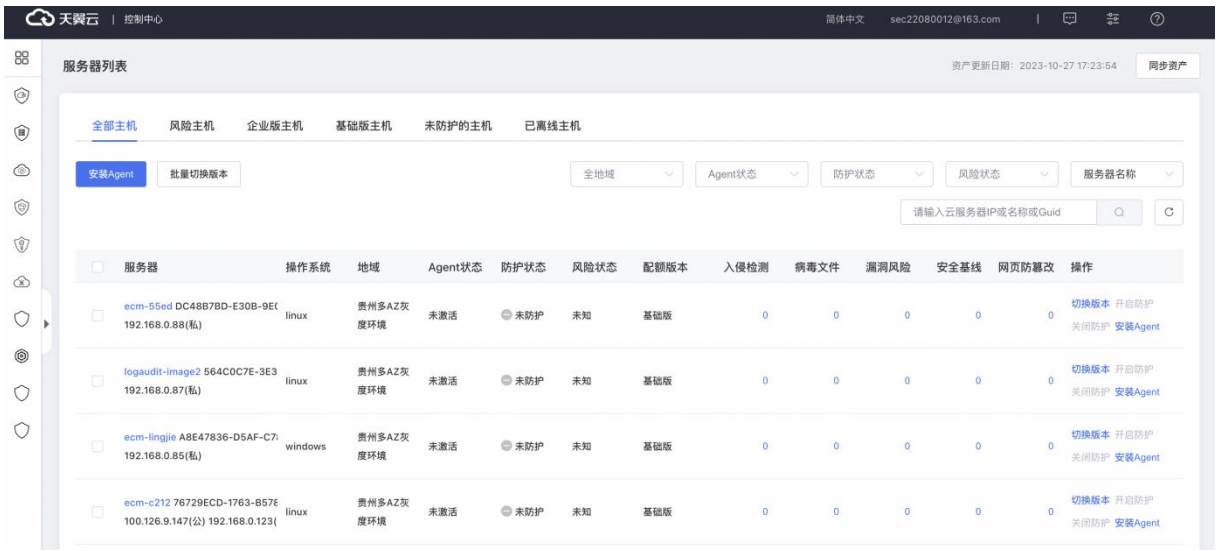
Q：如何评估漏洞对主机的影响范围?

您可以登录服务器安全卫士（原生版）控制台，在左侧导航中选择漏洞扫描，在漏洞扫描页面告警列表通过漏洞名称、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、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，在服务器列表页面选中任意一台服务器。



2、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

1、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。

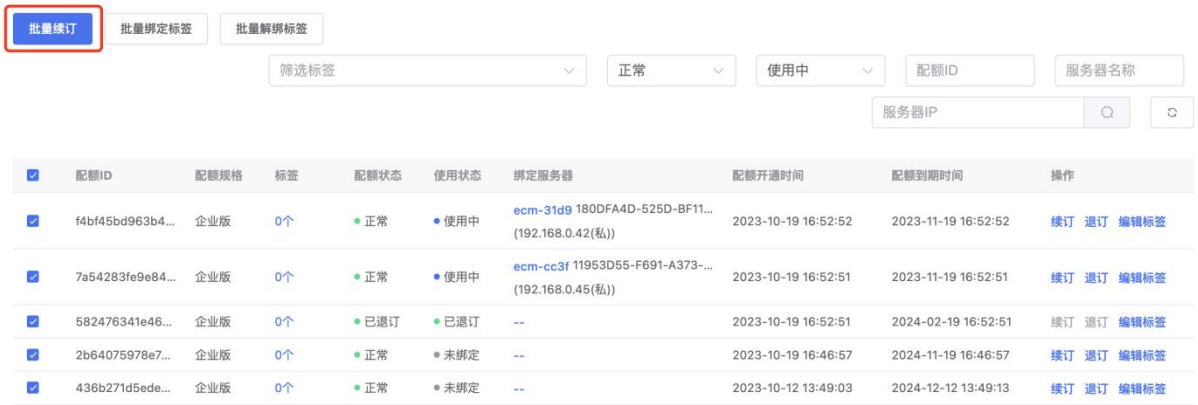
2、手动同步是用户主动触发资产同步，立即同步您账户下的所有资产。

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。

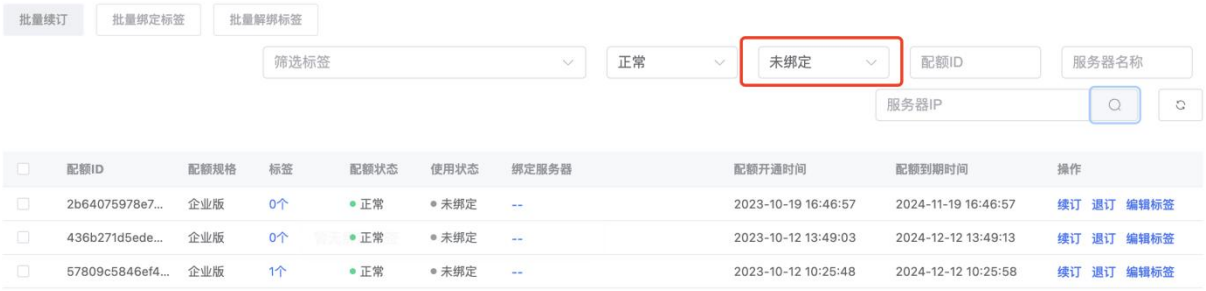
Q：如何延长服务器安全卫士（原生版）防护配额有效期?

您可在服务器安全卫士（原生版）控制台-设置中心-配额管理中，对需要续订的云服务器配额进行批量续订。



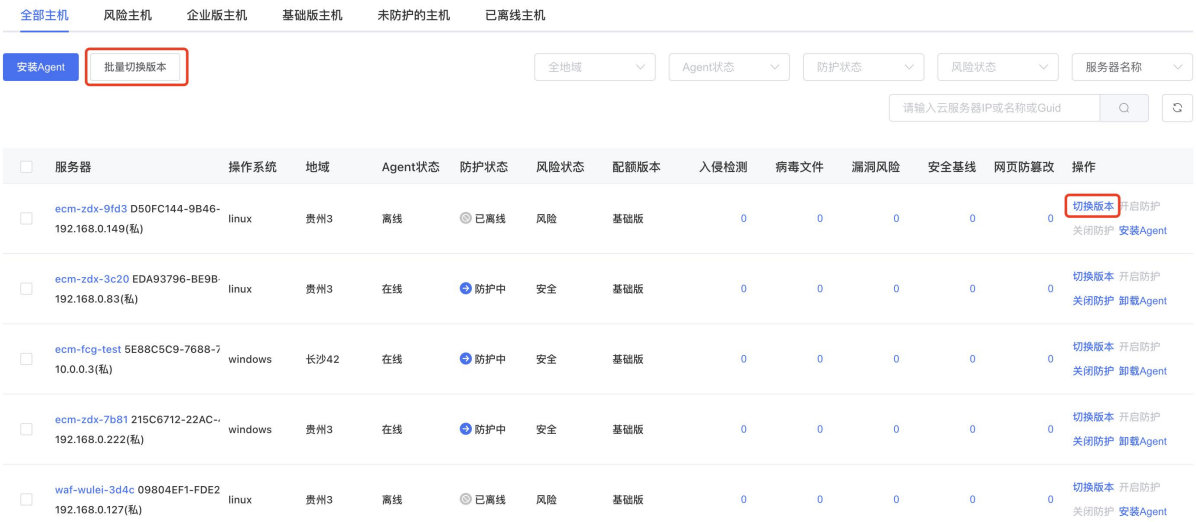
Q：如何筛选未绑定配额的主机？

您可在服务器安全卫士（原生版）控制台-设置中心-配额管理中，通过“使用状态”筛选查看未绑定主机。



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，配额版本为“基础版”或“企业版”，



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

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，且可在服务器安全卫士（原生版）控制台-资产管理-服务器安全列表中查看服务器信息及是否安装 Agent。