天翼云

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

内容	时间
新建	2022/7/20
修订	

目 录

1. 产品简介 1
1.1. 产品定义 1
1.1.1 产品定义 1
1.1.2 产品架构 1
1.2. 产品优势 2
1.3. 功能特性 3
1.4. 术语说明 3
1.5. 应用场景 4
1.6. 产品规格 5
1.7. 产品使用限制 7
1.8. 与其他云服务关系 8
2. 快速入门 9
2.1. 注册天翼云账号 9
2.2. 开通服务器安全卫士（原生版） 9
2.3. 购买配额 12
2.4. 安装 Agent 13
2.5. 设置告警通知 15
2.6. 切换版本 16
2.7. 查看检测结果 18
3. 用户指南 20
3.1. 计费操作 20
3.1.1 订购 20
3.1.2 手动续订 23
3.1.3 自动续订 25

3.1.4 退订 27
3.2. 安全概览 29
3.2.1 最近 7 日待处理风险 29
3.2.2 防护状态 30
3.2.3 风险趋势 32
3.2.4 最近 7 日风险动态 33
3.3. 资产管理 33
3.3.1 概览 34
3.3.2 服务器列表 37
3.3.3 资产指纹 41
3.3.4 资产详情 44
3.4. 基线管理 50
3.4.1 基线检测 50
3.4.2 弱口令检测 56
3.5. 漏洞扫描 60
3.6. 入侵检测 69
3.6.1 异常登录 69
3.6.2 暴力破解 74
3.7. 网页防篡改（原生版） 78
3.7.1 防护状态 78
3.7.2 防护管理 80
3.7.3 防护配额 90
3.8. 设置中心 94
3.8.1 配额管理 94
3.8.2 同步资产设置 94
4. 常见问题 96

4.1. 产品类 96
4.2. 计费类 97
4.3. 购买类 97
4.4. 操作类 98
4.5. 系统类 99

1. 产品简介

1.1. 产品定义

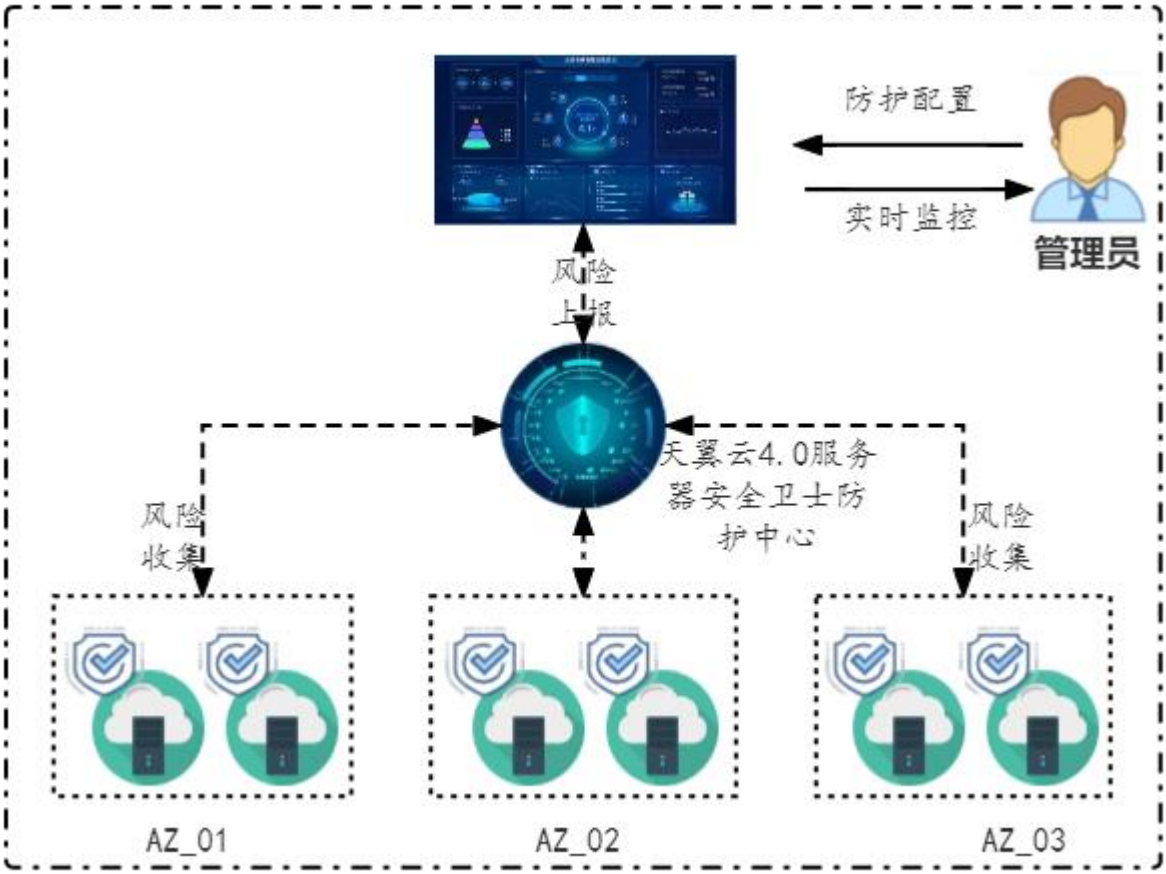
1.1.1 产品定义

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

1.1.2 产品架构

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

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



1.2. 产品优势

统一管理和运维

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

三位一体全面防护

提供事前预防、事中防御、事后检测的全面防护，全面降低服务器入侵风险。

防护资源占用少

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

用户使用方便快捷

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

防护机制安全可靠

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

1.3. 功能特性

天翼云服务器安全卫士（原生版）产品主要包含以下功能：

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

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

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

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

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

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

1.4. 术语说明

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

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

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

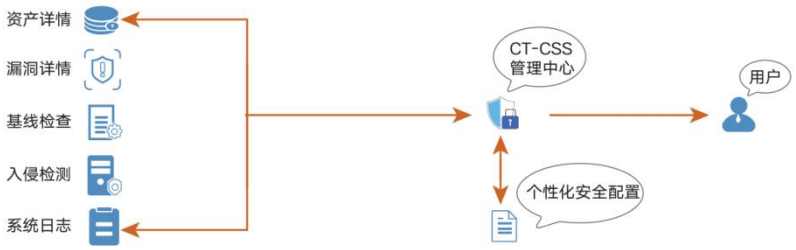
异常登录：采集服务器上 RDP、SSH 登录日志，对合法登录 IP、合法登录事件、合法登录账号和合法登录时段之外的登录行为均提供告警。

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

1.5. 应用场景

场景一：入侵行为检测

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



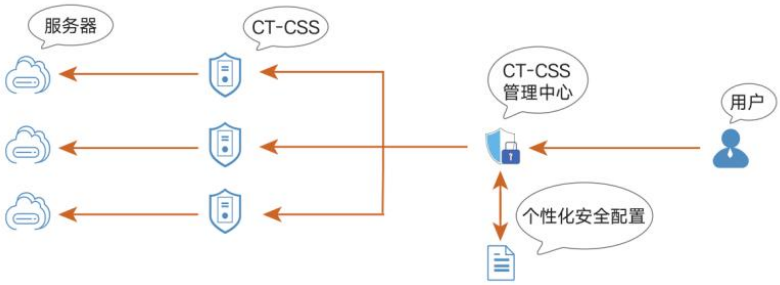
方案优势：

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

提供病毒查杀能力，有效检出恶意病毒文件，并提供病毒文件隔离和删除功能。

场景二：安全管理

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



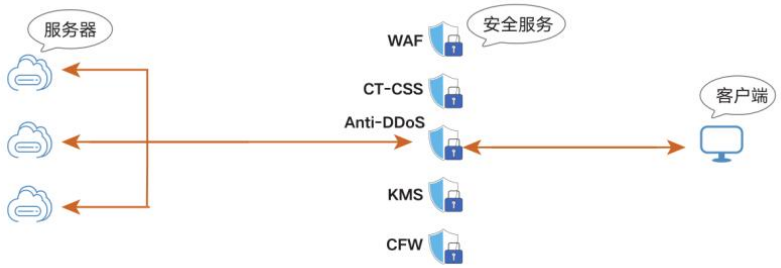
方案优势：

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

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

场景三：等保合规

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



方案优势：

满足入侵防范条款：入侵检测，漏洞管理功能满足等保的主机入侵防范条款。

满足不同行业监管要求：基于基线检测功能，提供多种基线标准模板，企业可自定义基线策略，支持一键检测和定时检测，根据检测结果提供处理建议。

1.6. 产品规格

根据支持功能不同，服务器安全卫士(原生版)分为基础版、企业版和增值服务。

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

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

一级菜单	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	仅展示入侵检测和漏洞风险，不支持切换版本	√	
	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	√	√	

	同步资产	实时同步主机资产	√	√	
入侵检测	异常登录	异常登录情况统计	√	√	
		事件列表	√	√	
		白名单管理	√	√	
	暴力破解	暴力破解情况统计	√	√	
		事件列表	√	√	
		白名单管理	√	√	
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		√	
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	√	√	

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

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

支持的资源池

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

使用条件

每台服务器客户端需安装一个 Agent，且服务器需不低于 1C1G。

1.8. 与其他云服务关系

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

2. 快速入门

2.1. 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）”。

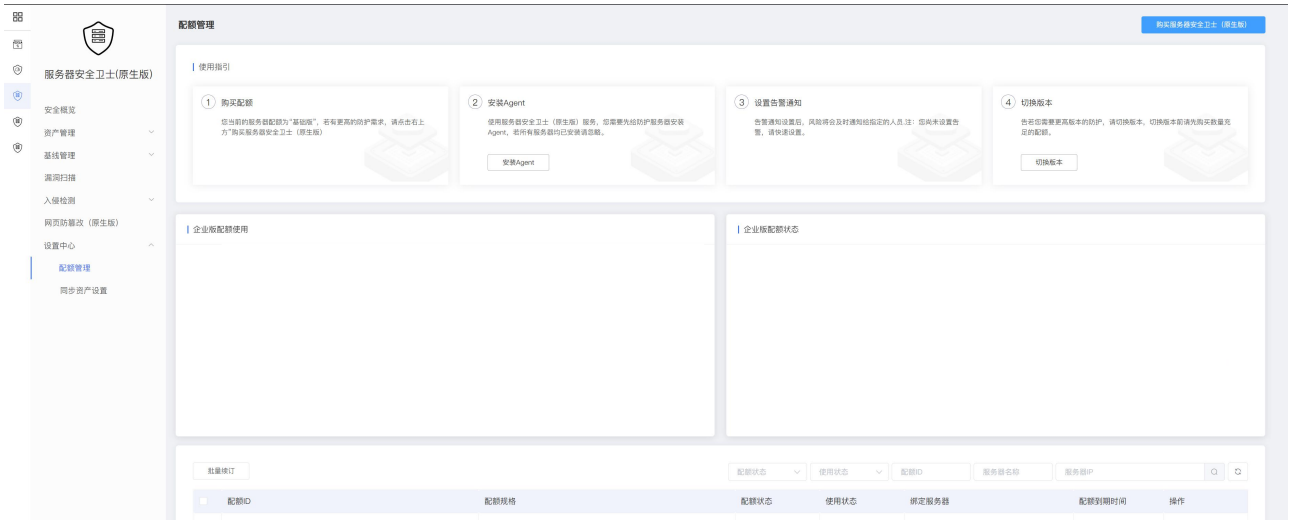
2.2. 开通服务器安全卫士（原生版）

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

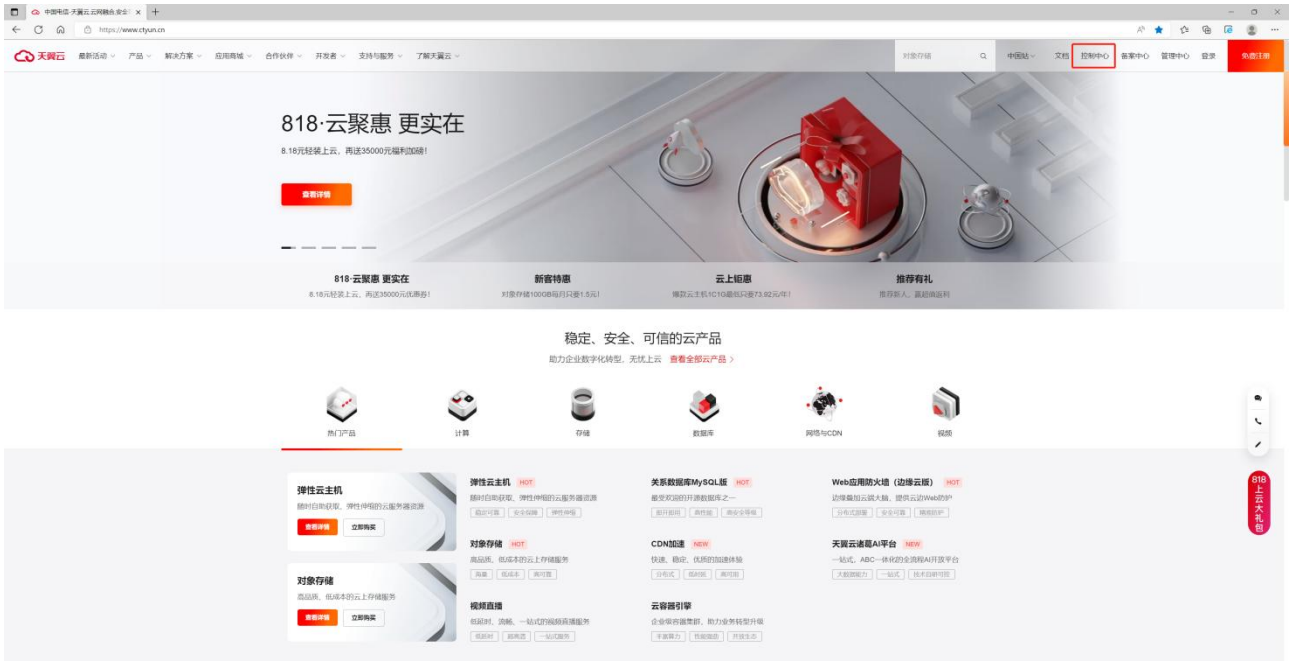
1. 在天翼云官网首页选择“产品->安全->网络安全->服务器安全卫士（原生版）”。进入服务器安全卫士（原生版）产品详情页后，选择“控制台”，如下图所示：

进入控制台后，弹出下方“服务开通申请”对话框：

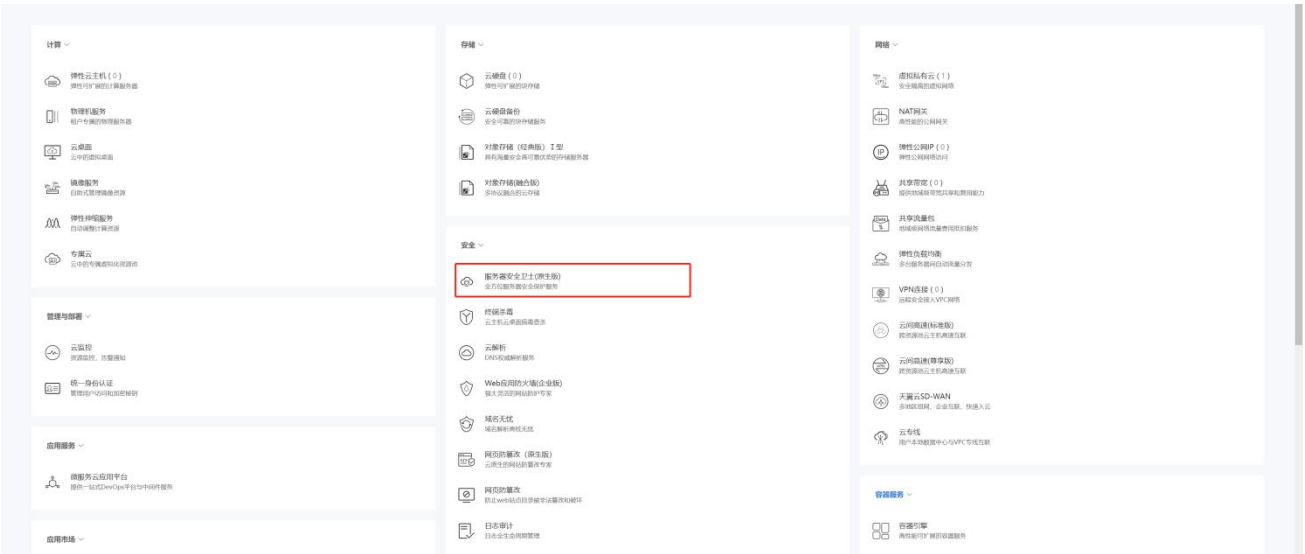
阅读《天翼云服务器安全卫士（原生版）协议》后，勾选我已阅读并同意签署《天翼云服务器安全卫士（原生版）协议》，点击“确定”按钮，即可开通服务器安全卫士（原生版）服务，如下图所示：



2. 在天翼云官网首页选择“控制中心”，如下图所示：

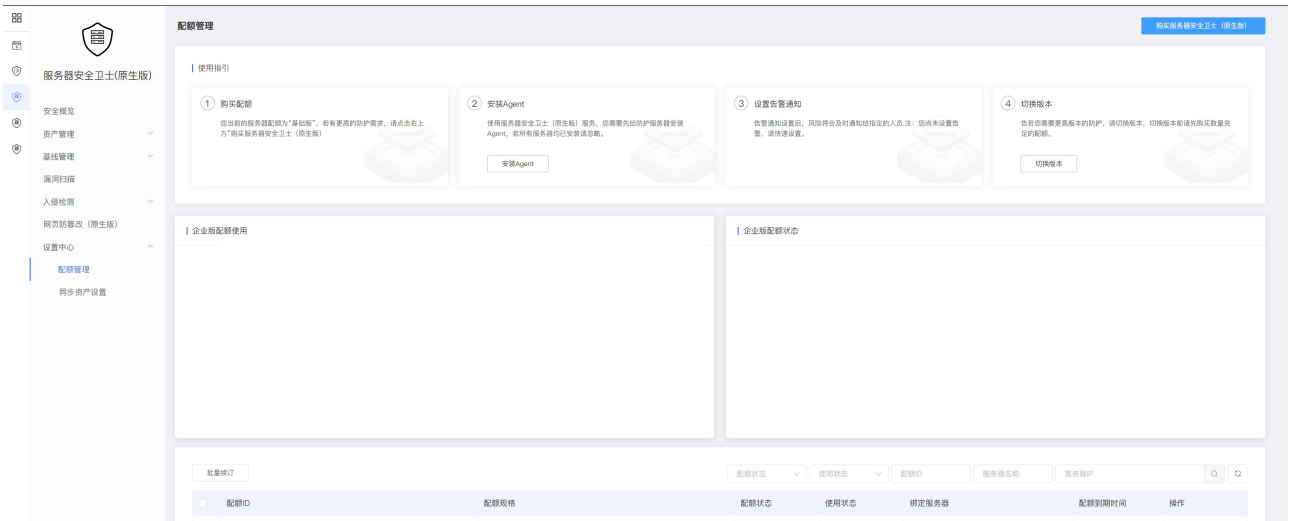


在天翼云控制台中，安全分类下，点击“服务器安全卫士（原生版）”，



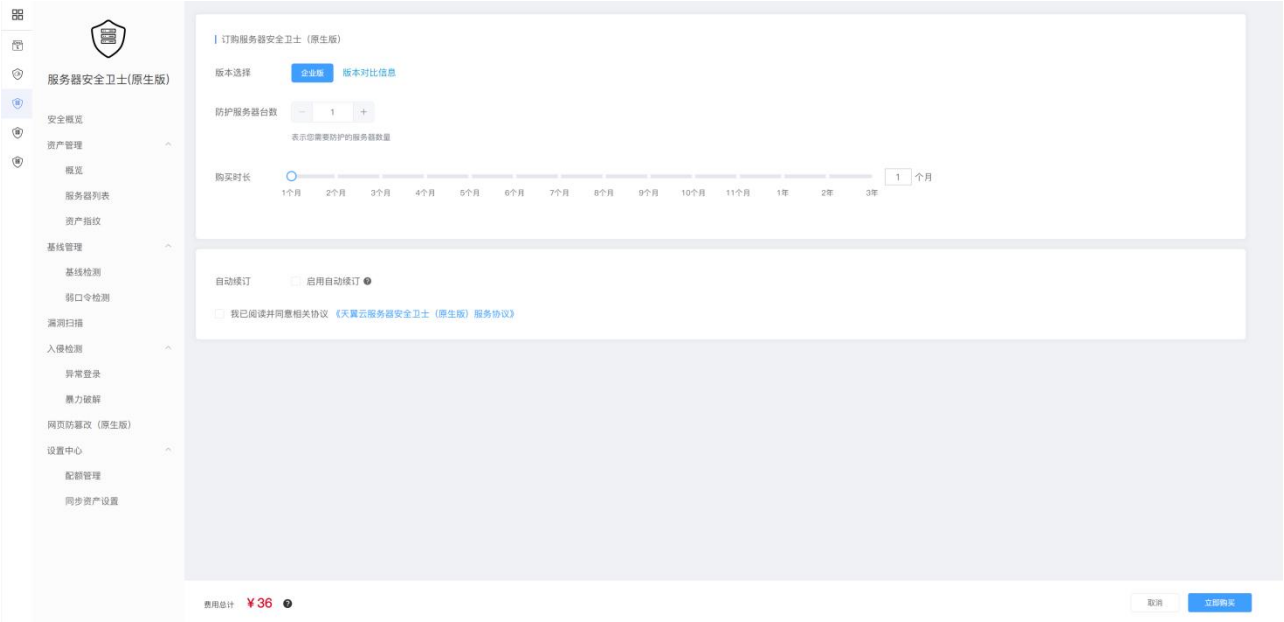
进入服务器安全卫士（原生版）控制台，弹出下方“服务开通申请”对话框：

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

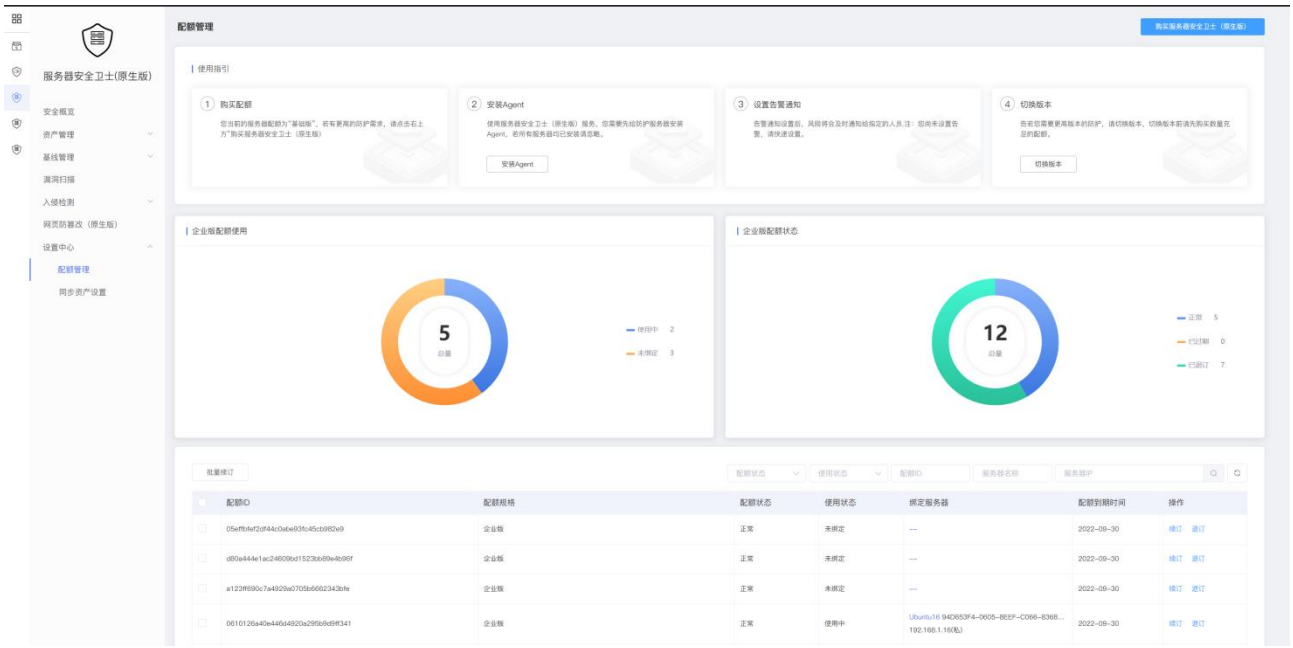


2.3. 购买配额

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

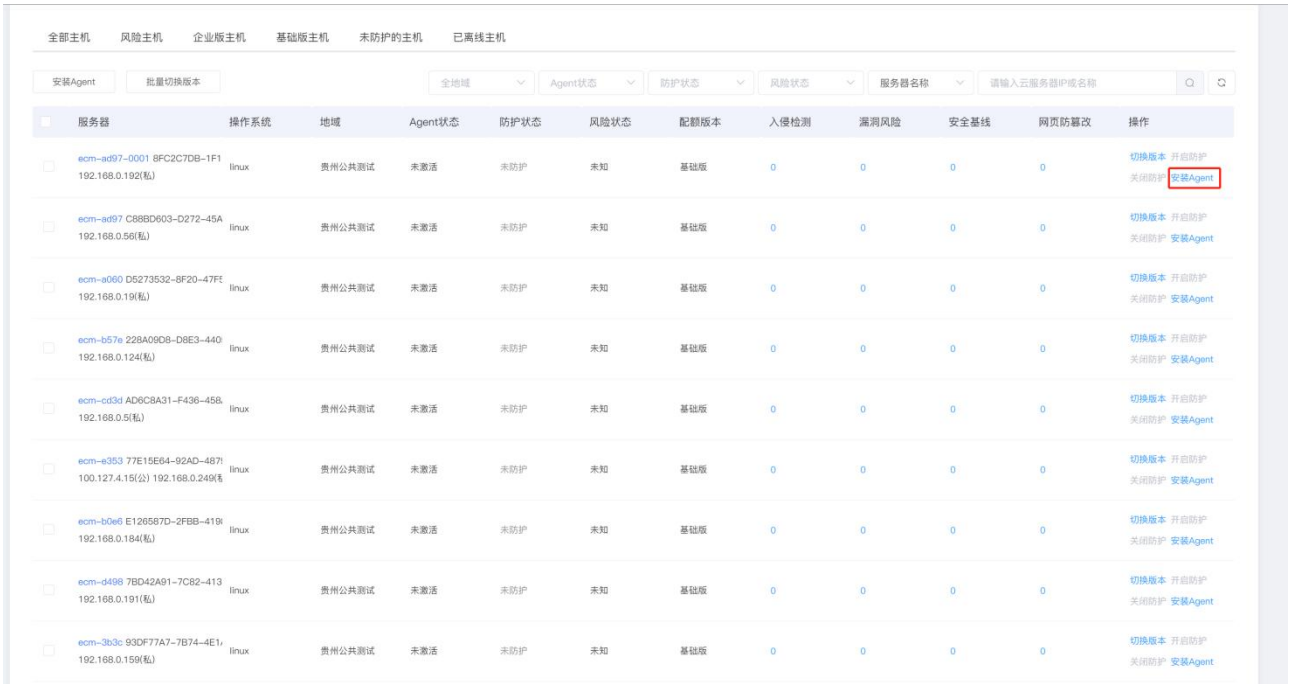


选择购买版本、防护服务器台数、购买时长、自动续订，勾选我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）协议》，点击“立即购买”按钮，购买成功后即可在“配额管理”页面查看已购买的企业版配额，如下图所示：



2.4. 安装 Agent

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



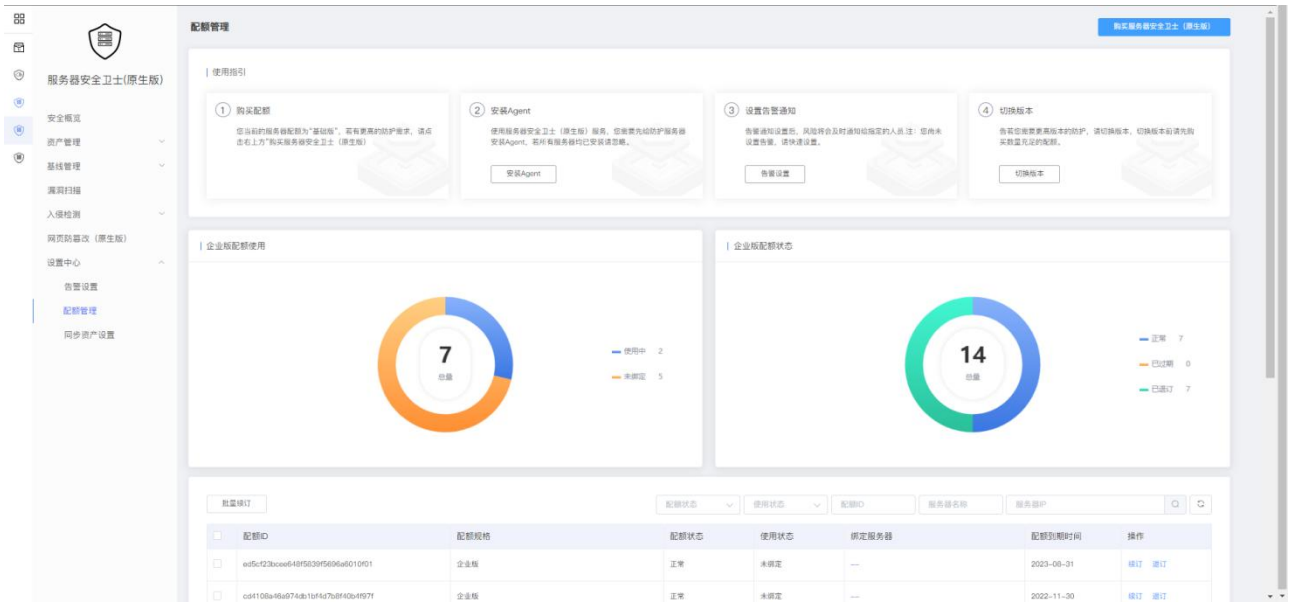
查看服务器列表中的“Agent 状态”：若状态为“在线”，则本台服务器已安装 Agent 且 Agent 服务正常；若状态为“离线”或“错误”，则本台服务器已安装 Agent，但 Agent 与服务器通信异常；若状态为“未激活”，则本台服务器未安装 Agent 或 Agent 未激活。

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

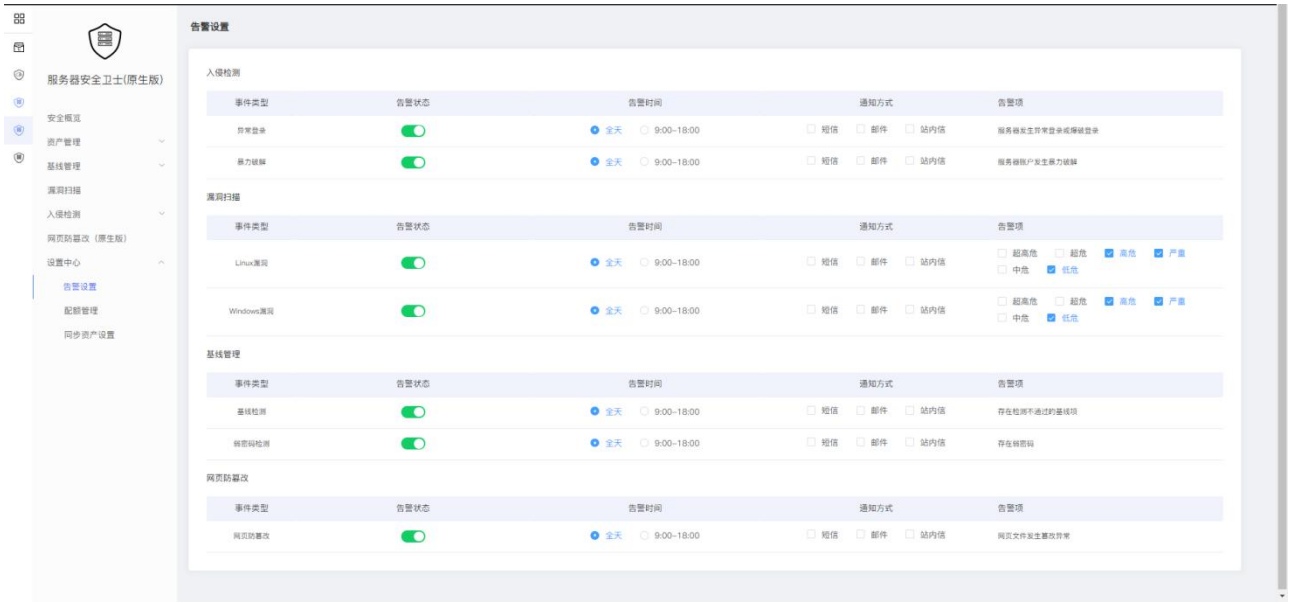
Windows 系统安装命令如下图：

2.5. 设置告警通知

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

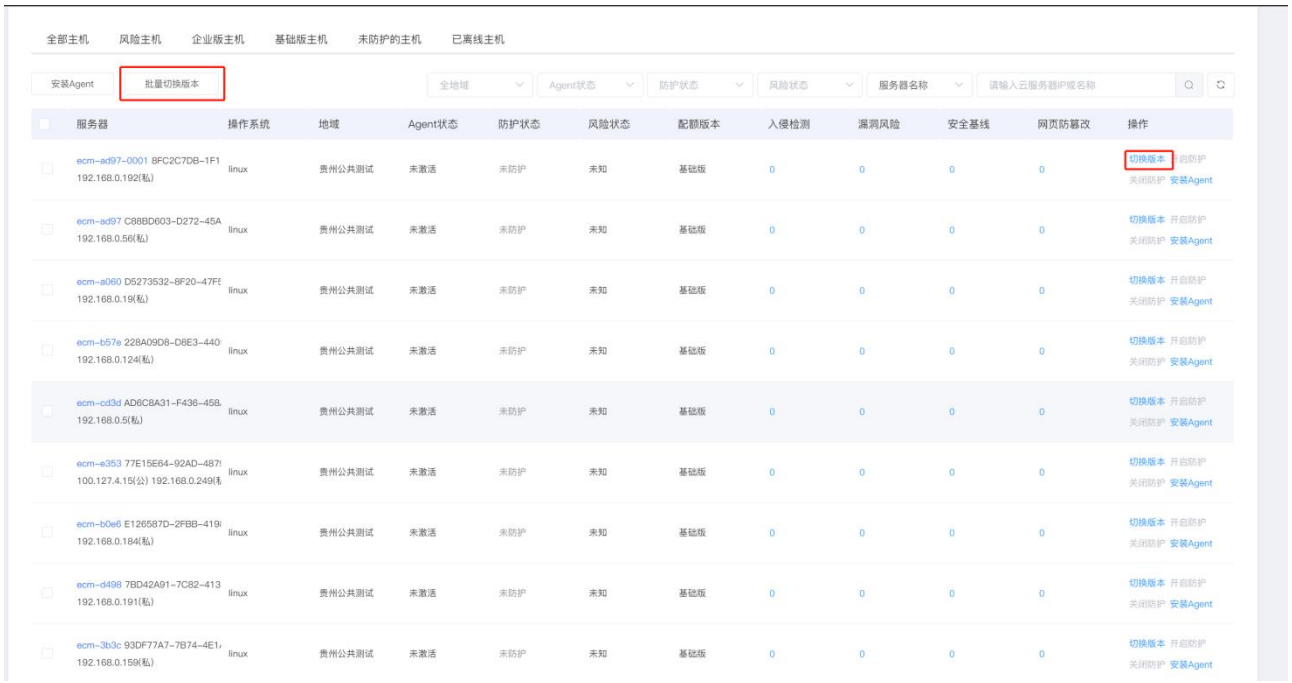


对各个功能的告警状态、告警时间、通知方式和告警项进行选择，如下图所示。告警状态默认打开，告警时间默认全天，通知方式默认邮件和站内信，漏洞告警项默认超高危、超危和高危。



2.6. 切换版本

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



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

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

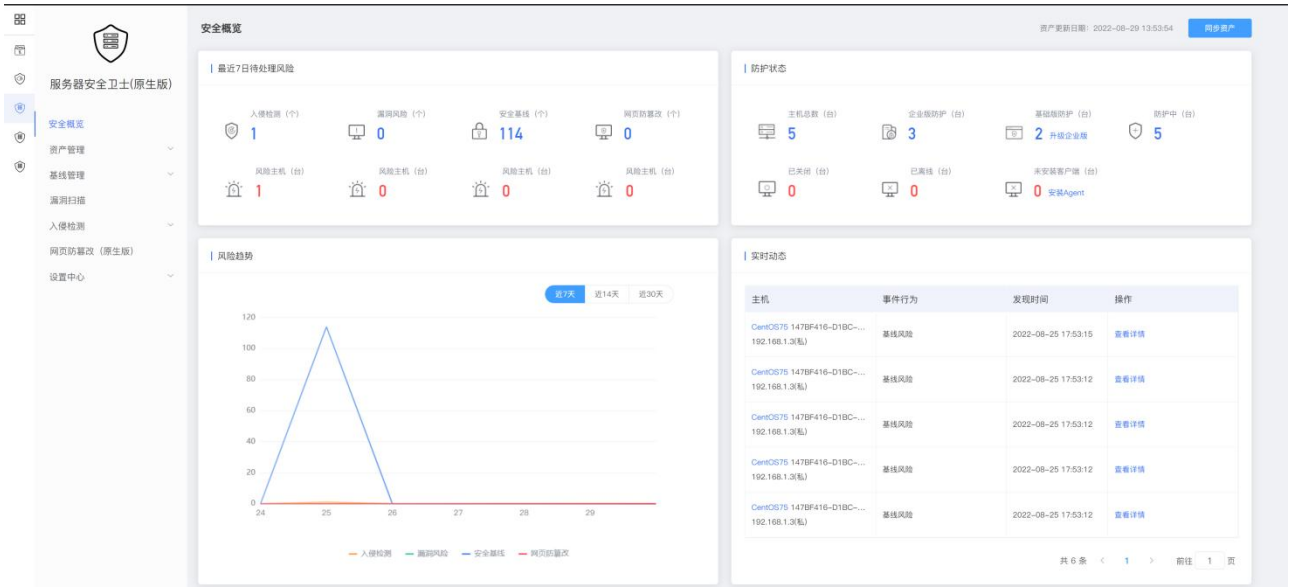
注意：企业版防护服务器不可切换为基础版防护！

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

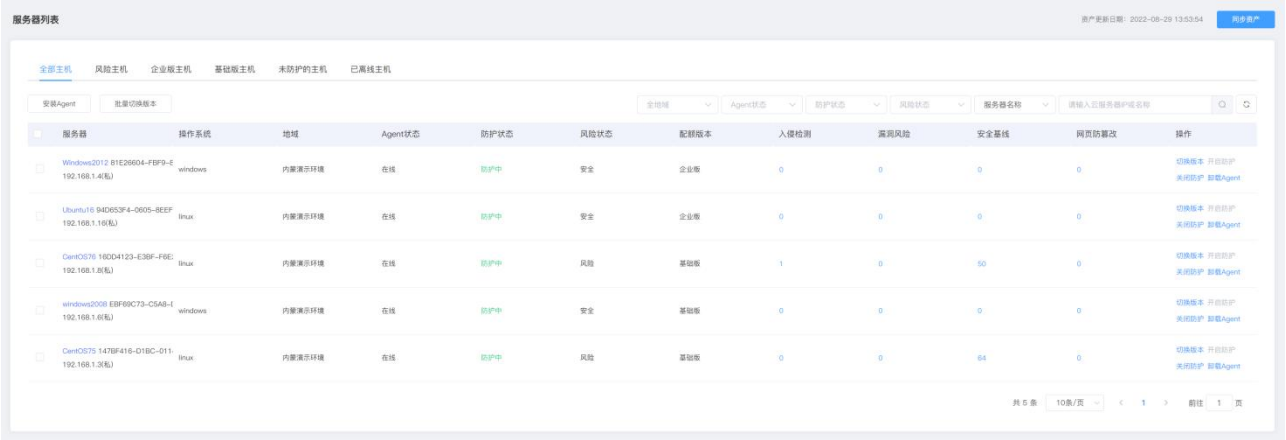
可进行批量切换，在服务器列表中选择需要切换的服务器，点击“批量切换版本”，跳转至下方页面，点击“确定”后，切换为企业版防护，配额和服务器按照顺序一一匹配即可。说明：批量切换版本时，服务器按照图中顺序与配额绑定，配额的绑定顺序为按照到期时间从早到晚进行绑定。

2.7. 查看检测结果

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



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。



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。

3. 用户指南

3.1. 计费操作

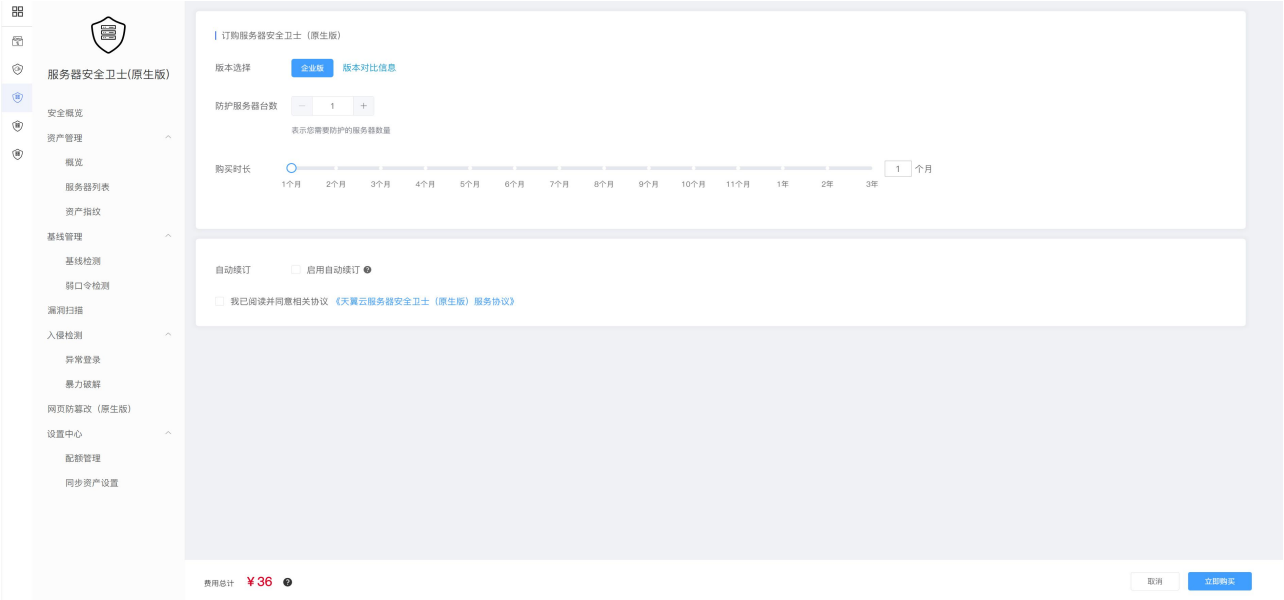
3.1.1 订购

以下为服务器安全卫士（原生版）的购买流程。

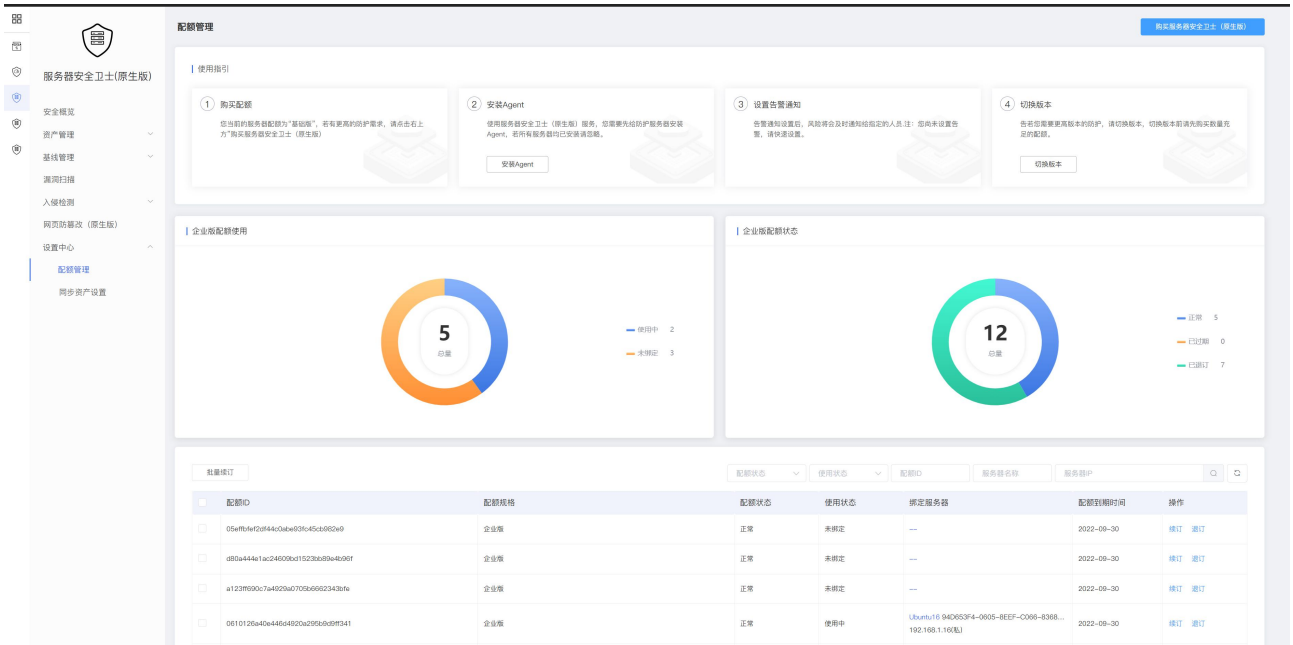
当您具备已通过实名认证的 ctyun 账号后，可以通过以下两种方式开通服务器安全卫士（原生版）：

1. 进入服务器安全卫士（原生版）产品详情页，如下图所示：

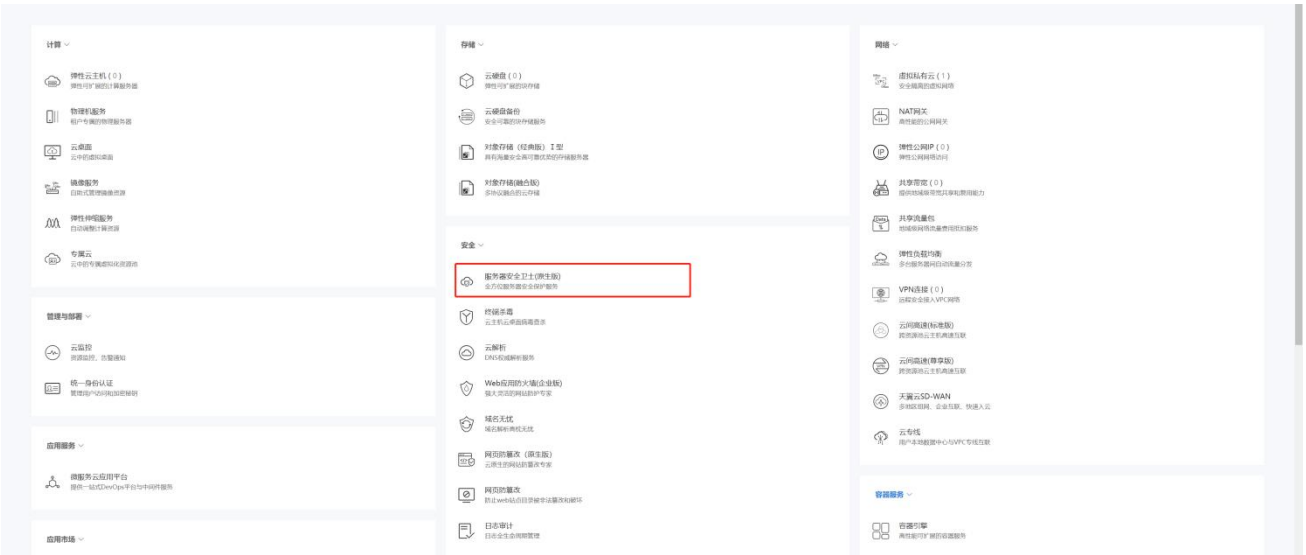
单击【立即开通】，进入到服务器安全卫士（原生版）产品购买页面：



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

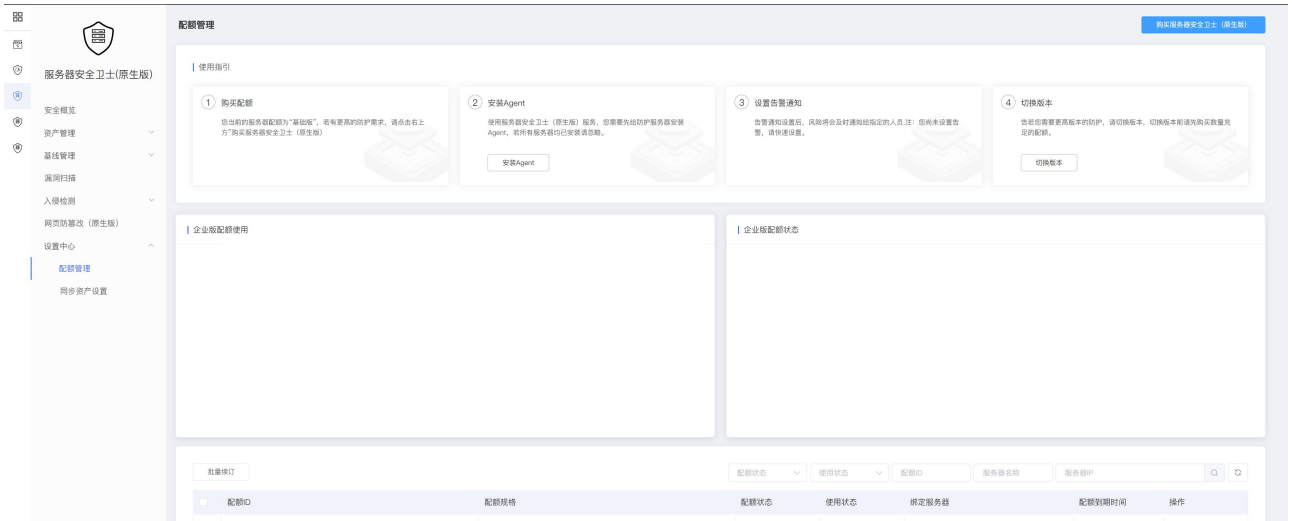


2. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（原生版）”：

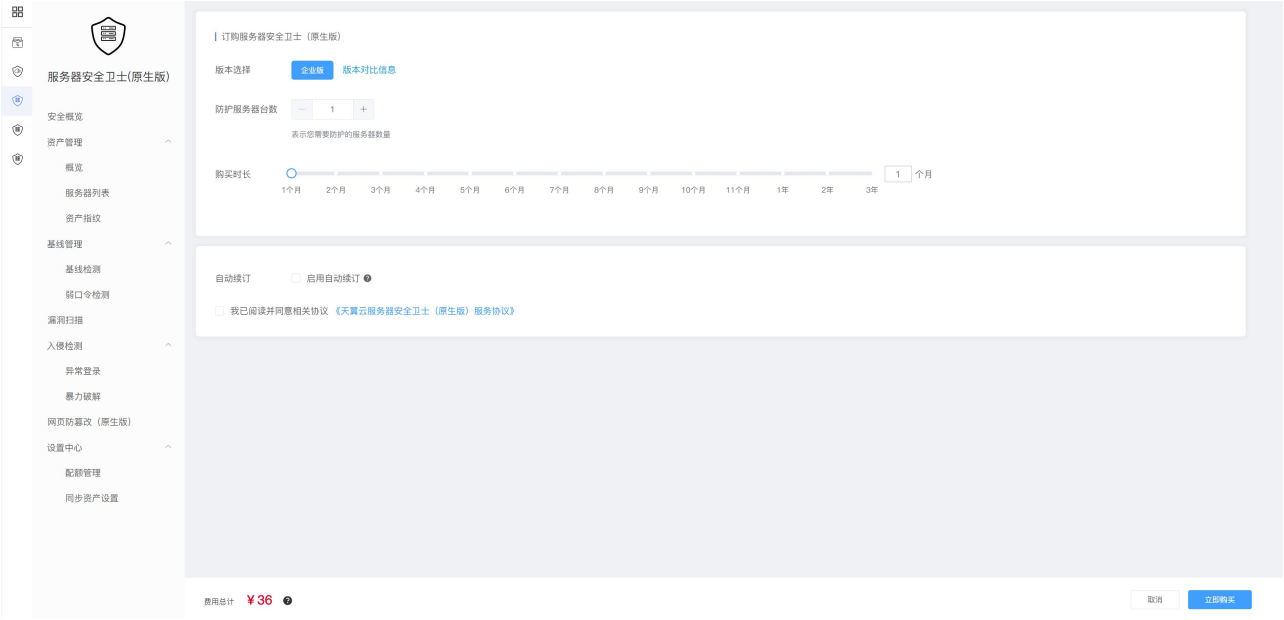


进入服务器安全卫士（原生版）控制台，弹出下方“服务开通申请”对话框：

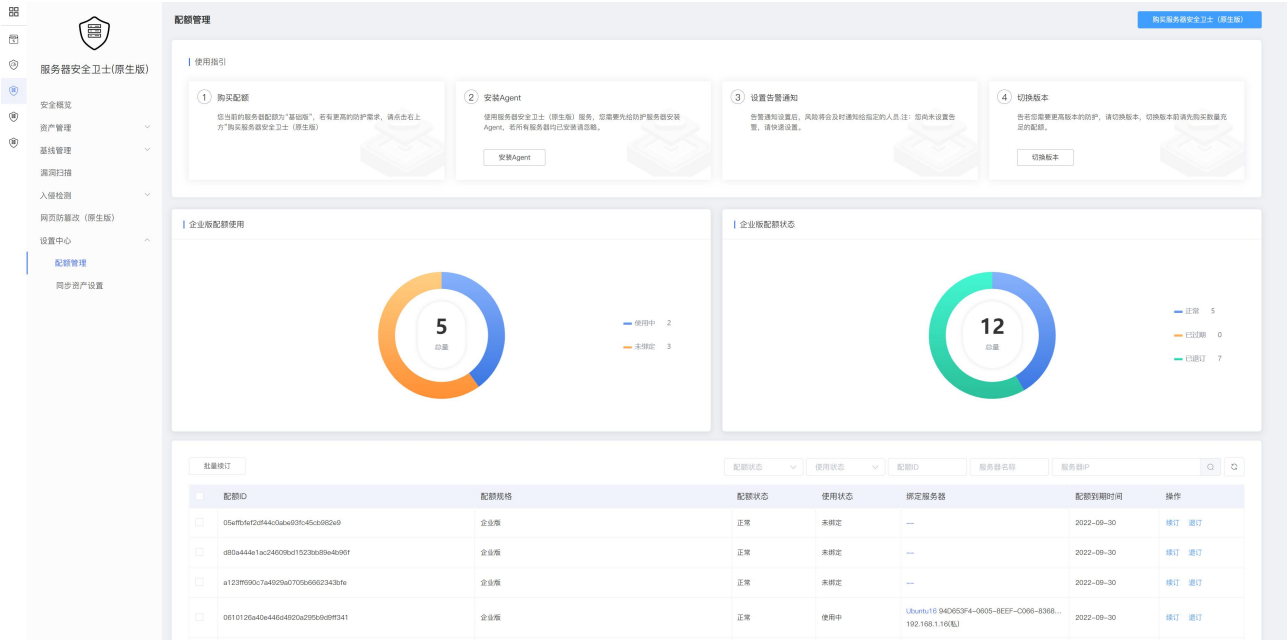
阅读《天翼云服务器安全卫士（原生版）协议》后，勾选我已阅读并同意签署《天翼云服务器安全卫士（原生版）协议》，点击“确定”按钮，即可开通服务器安全卫士（原生版）服务，如下图所示：



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：

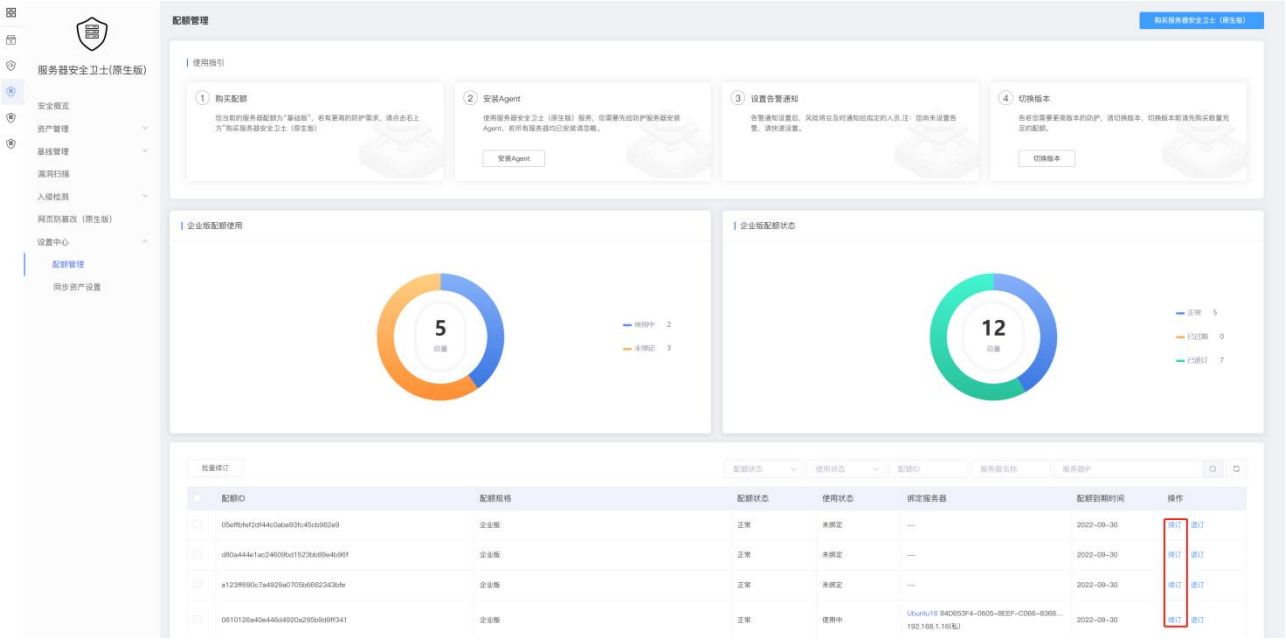


选择购买版本、防护服务器台数、购买时长、自动续订，勾选我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）协议》，点击“立即购买”按钮，购买成功后即可在“配额管理”页面查看已购买的企业版配额，如下图所示：

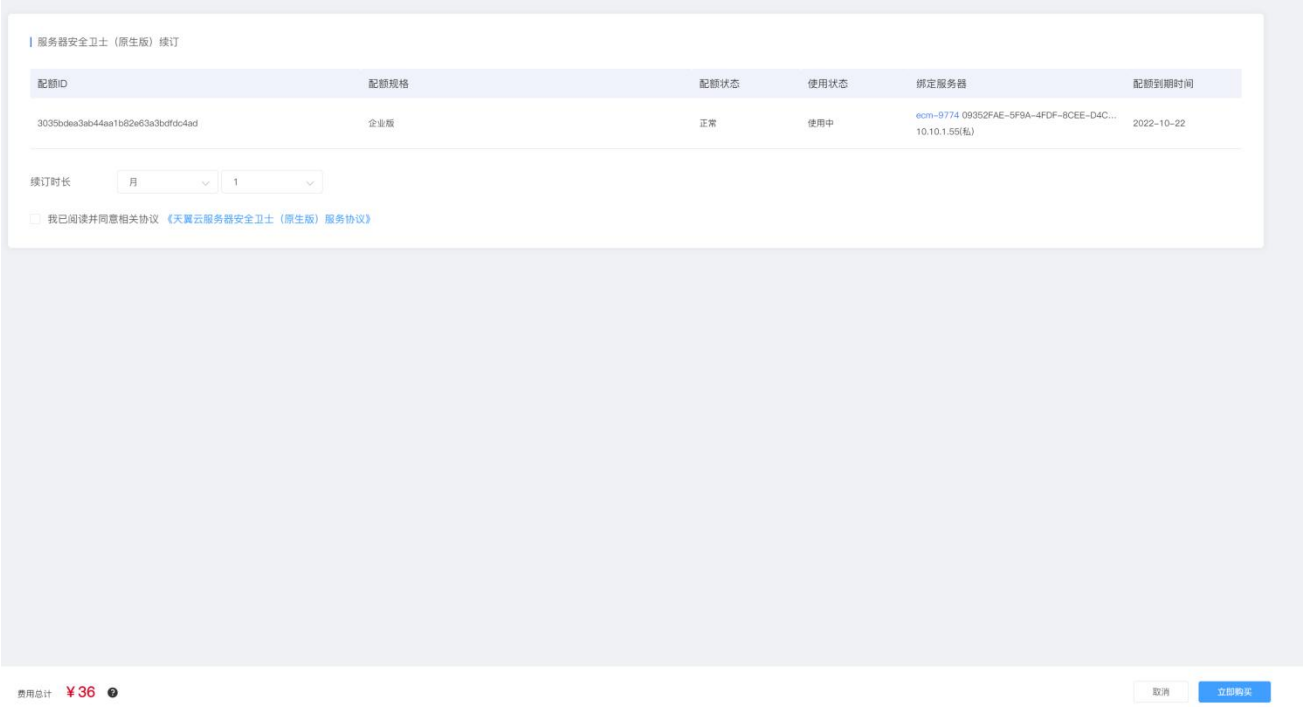


3.1.2 手动续订

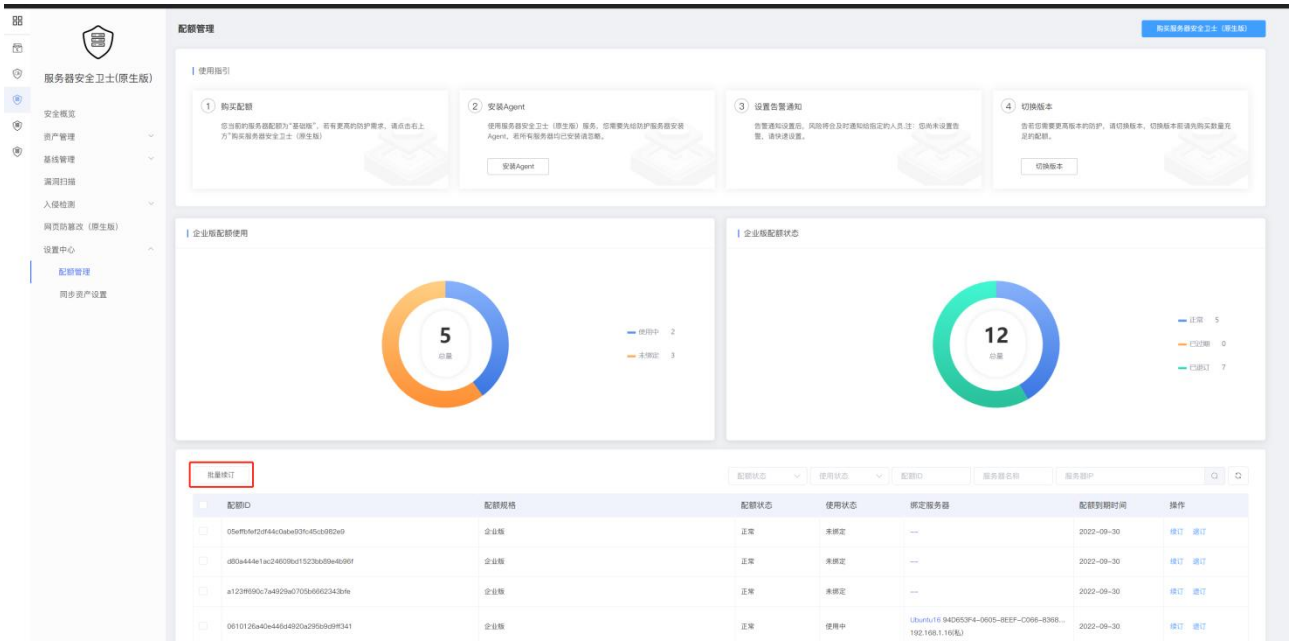
在“设置中心->配额管理”中查看您已经订购的配额，选择所需续订的配额，点击“续订”，如下图所示：



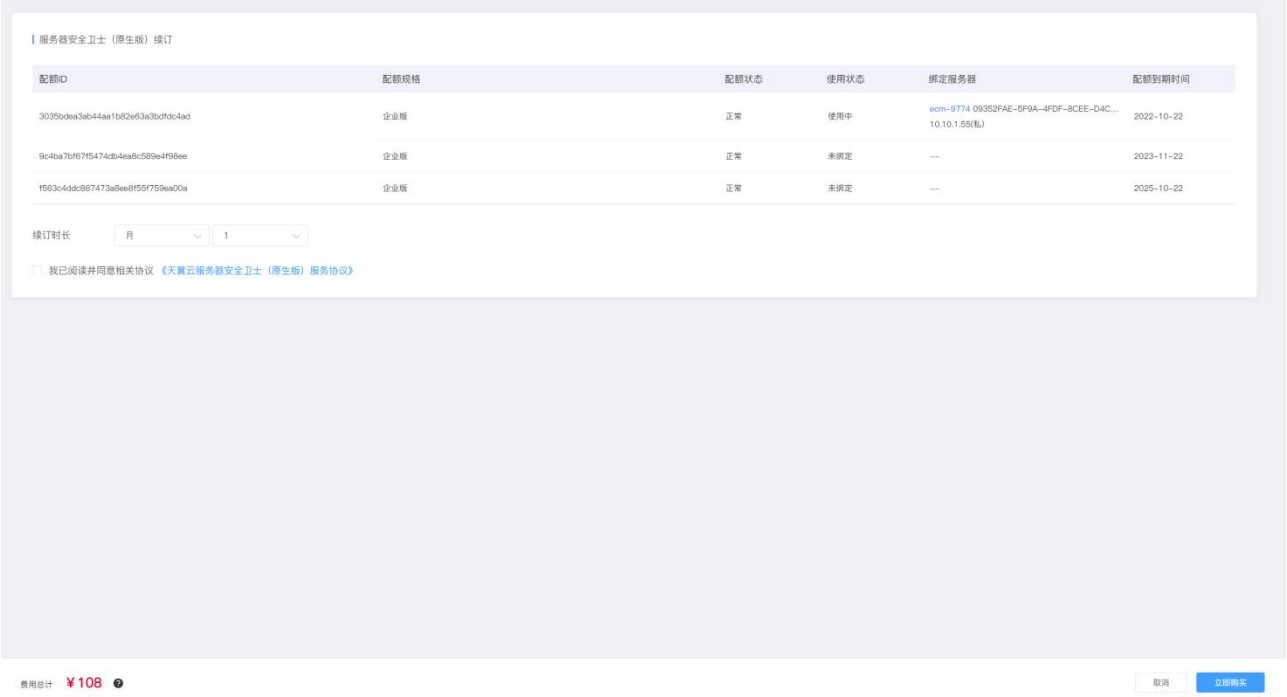
在下图续订页面中，选择续订时长，勾选我已阅读并同意相关协议《天翼云服务器安全卫士（原生版）协议》后，并点击“立即购买”后即可进行续订。当续订周期达到 1 年或以上时，续订单将可享受包年折扣，续订金额显示折后价。



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：



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。



3.1.3 自动续订

开通自动续订

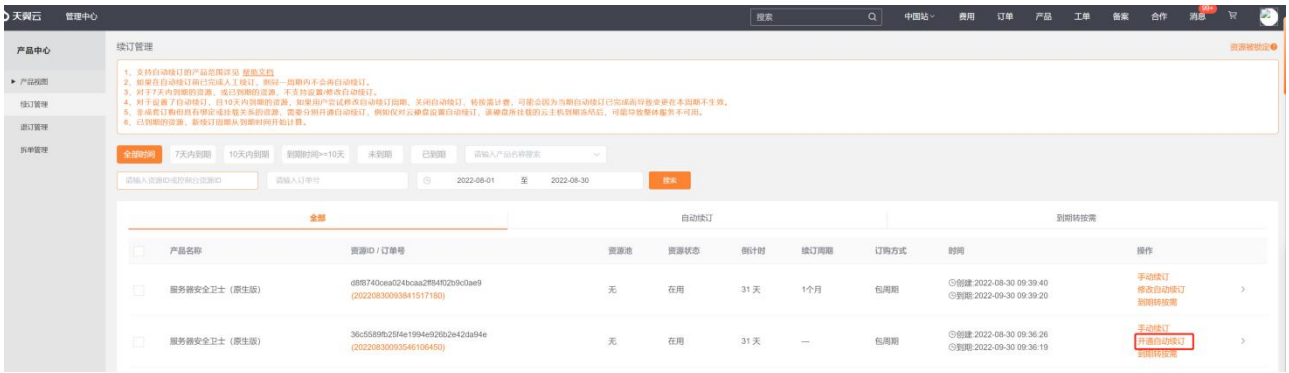
步骤 1 进入“续订管理”页面。

步骤 2 设置查询条件。

可综合利用到期时间、产品类型、是否开通自动续订查询资源。

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

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

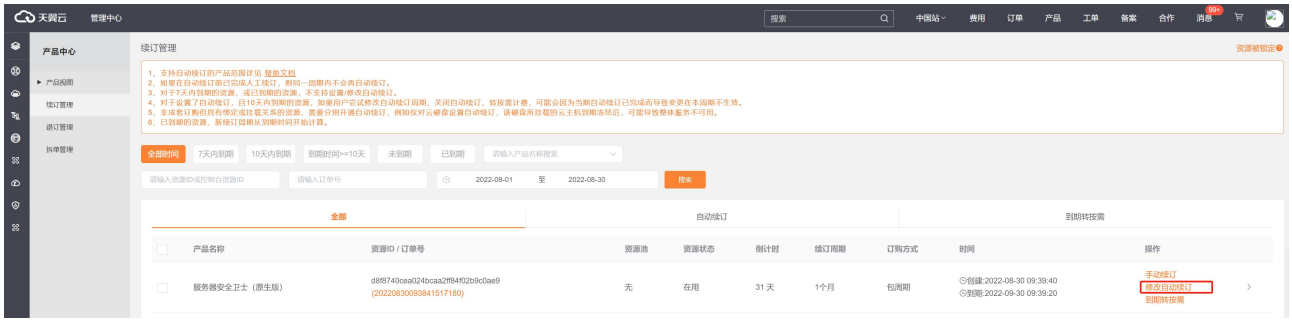


步骤 4 设置“自动续订周期”，仔细阅读《天翼云自动续订服务协议》，如果同意全部约定，则勾选“我已阅读并同意遵守《天翼云自动续订服务协议》的约定”，单击“确定提交”，如下图所示：

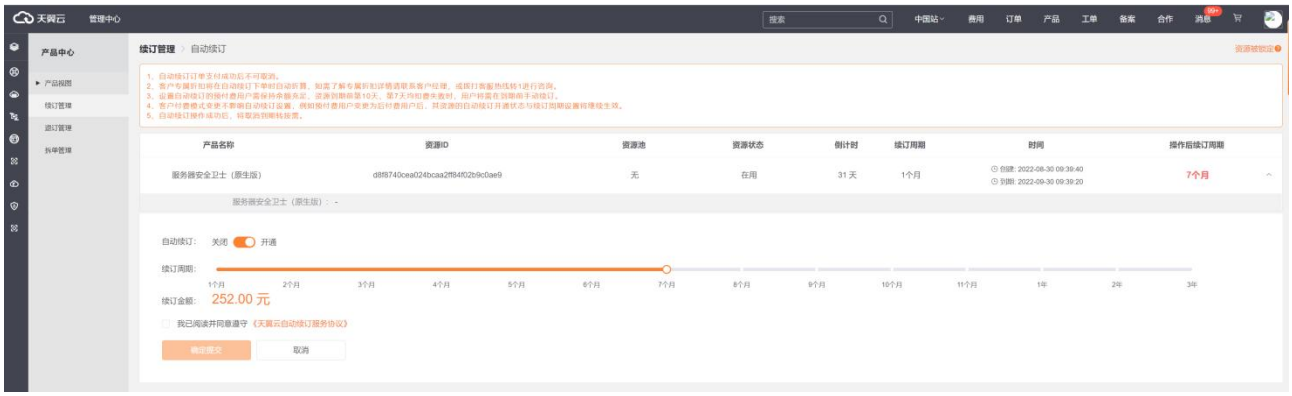
修改自动续订周期

步骤 1 进入“续订管理”页面。

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



步骤 3 拖动“续订周期”可修改自动续订周期。



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

关闭自动续订

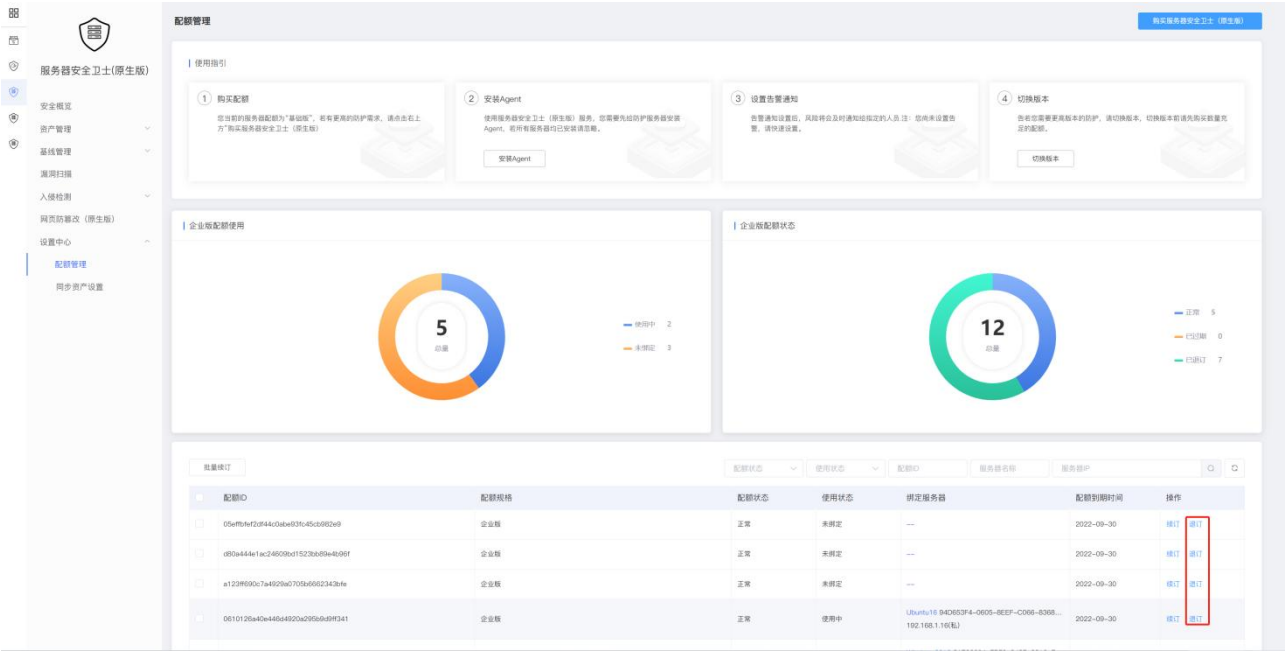
步骤 1 进入“续订管理”页面。

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

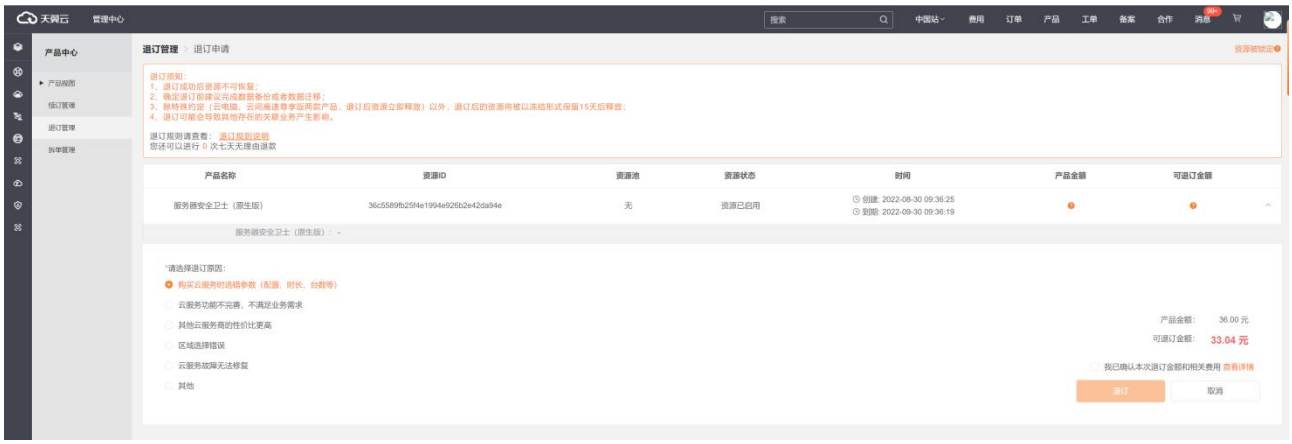
步骤 3 点击“自动续订”后方的关闭/开通按钮，单击“确定提交”。

3.1.4 退订

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

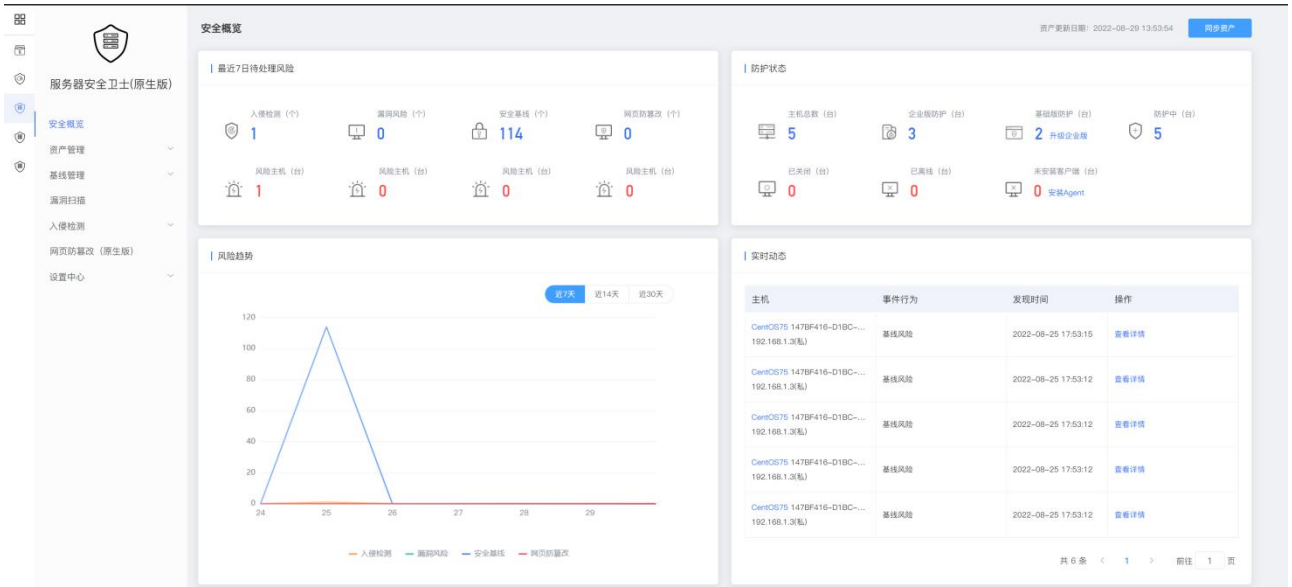


在下图退订页面中，选择退订原因，勾选我已确认本次退订金额和相关费用后，并点击“退订”后即可进行退订。



3.2. 安全概览

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



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

防护状态：展示您服务器的防护情况统计。

风险趋势：展示您服务器风险情况的折线统计图。

实时动态：展示您服务器的实时风险动态。

3.2.1 最近 7 日待处理风险

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

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。

3.2.2 防护状态

如上图所示，防护状态展示您所有服务器的防护情况。

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

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

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

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

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

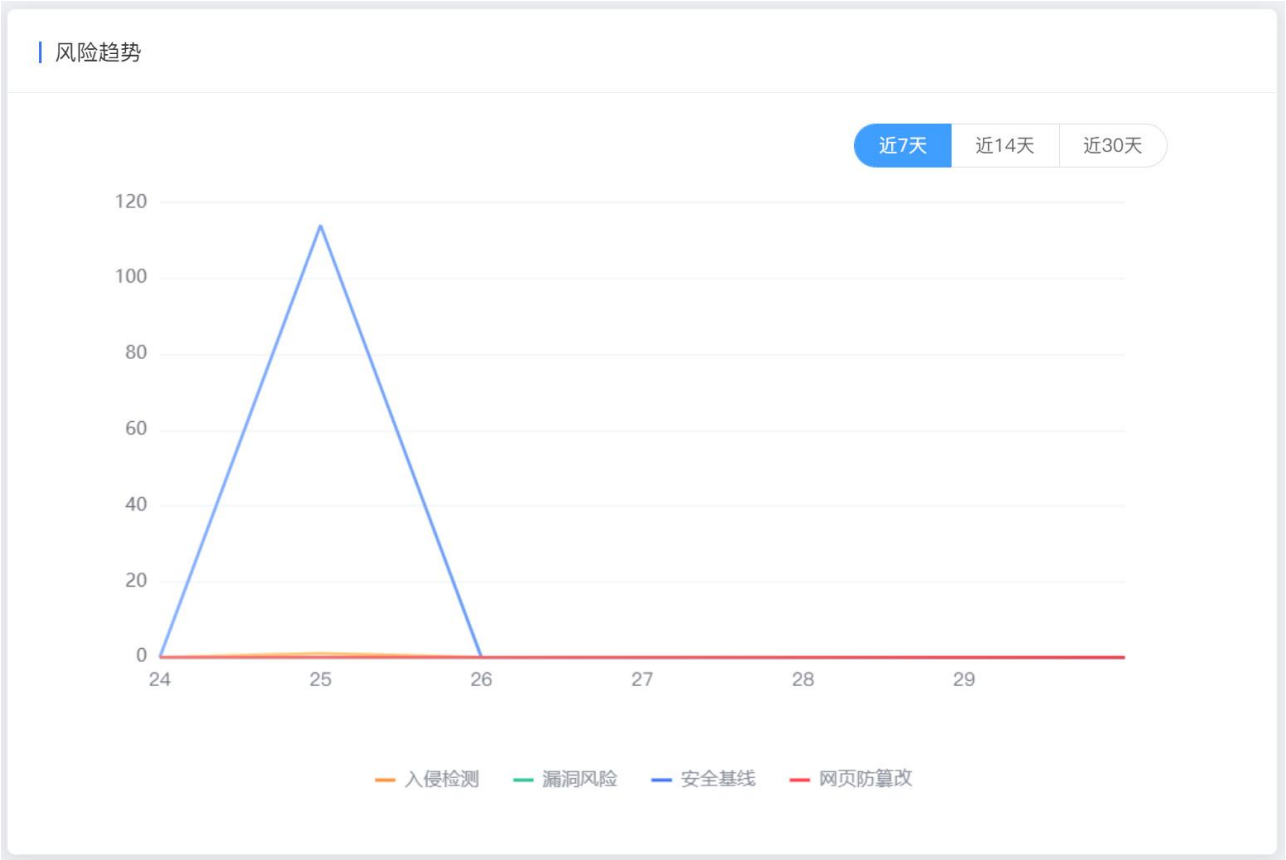
已关闭：服务器防护状态为“已关闭”的数量统计，点击数字时会跳转至“服务器列表-已关闭主机”页面。

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

Linux 系统安装命令如下图：

Windows 系统安装命令如下图：

3.2.3 风险趋势



如上图所示，风险趋势展示您所有服务器的风险统计折线图。

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

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

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

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

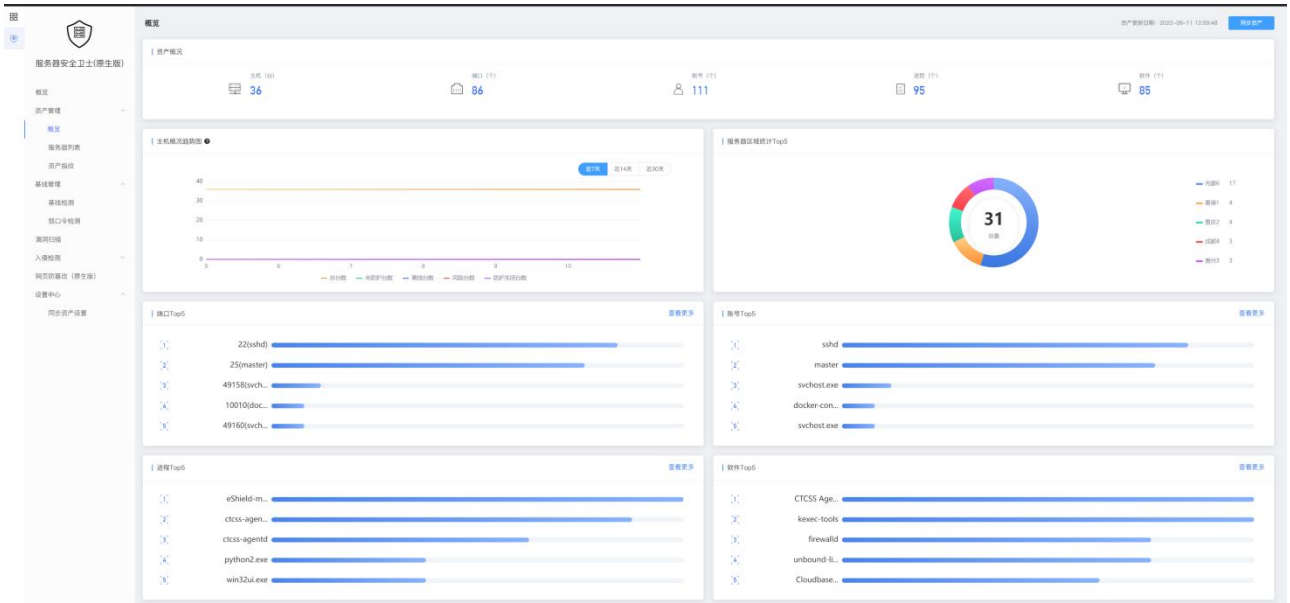
3.2.4 最近 7 日风险动态

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

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

3.3. 资产管理

资产管理分为概览、服务器列表、资产指纹 3 大模块，如下图所示。



3.3.1 概览

1） 资产概况

如上图所示，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。

2） 主机概况趋势图

如上图所示，主机概况趋势图为您展示服务器的防护情况统计折线图。

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

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

总台数：包括全部服务器，每天统计一个值。

未防护台数：防护状态为“未防护”的服务器，每天统计一个值。

离线台数：防护状态“已离线”的服务器，每天统计一个值。

风险台数：风险状态为“风险”的全部服务器，每天统计一个值。

防护关闭台数：防护状态“已关闭”的服务器。

3） 服务器区域统计 Top5

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

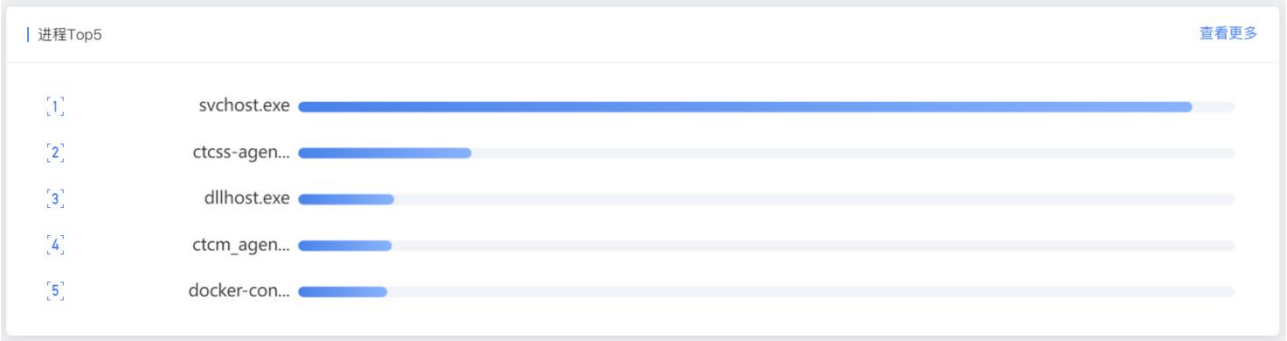
4） 端口 TOP5

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

5） 账号 TOP5

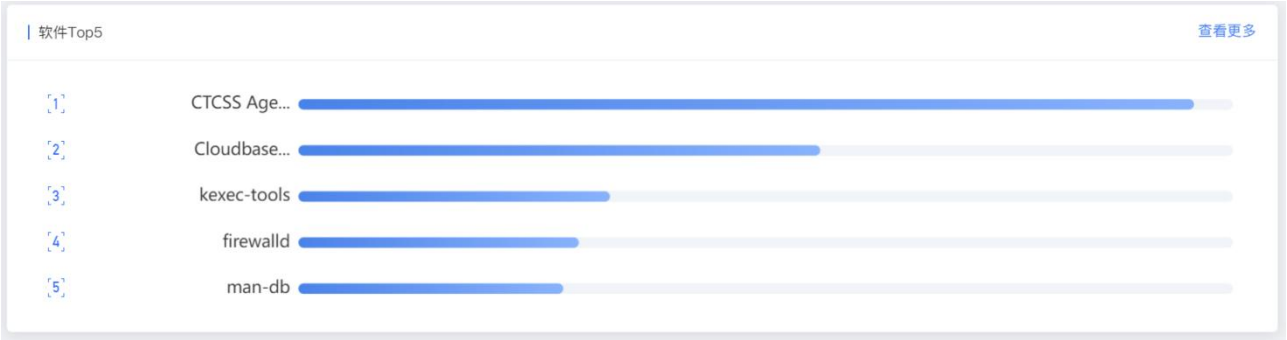
如上图所示，账号 Top5 为您展示服务器账号的统计情况排名 TOP5，点击更多时，会跳转至“资产指纹-账号”页面。

6） 进程 TOP5



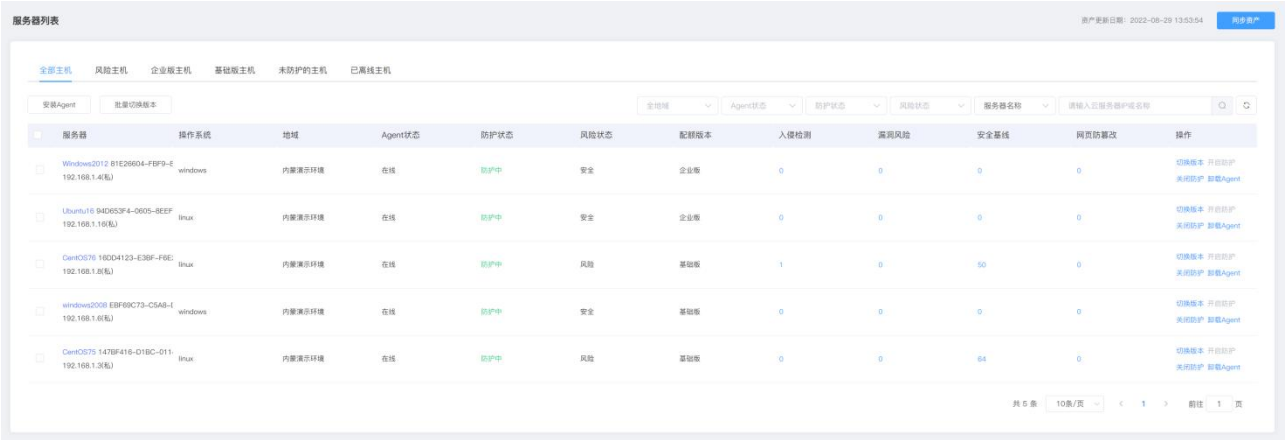
如上图所示，进程 Top5 为您展示服务器运行的进程统计情况排名 TOP5，点击更多时，会跳转至“资产指纹-进程”页面。

7） 软件 TOP5



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

3.3.2 服务器列表



1） 全部主机

该页面为您展示全部服务器的情况。已销毁的服务器不再展示在列表中。

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

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

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

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

防护状态	说明
已离线	表明该服务器与 Agent 通信异常，此时 Agent 状态为离线或错误。
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。

2） 风险主机

如上图展示，风险主机为您展示风险状态为“风险”的服务器。

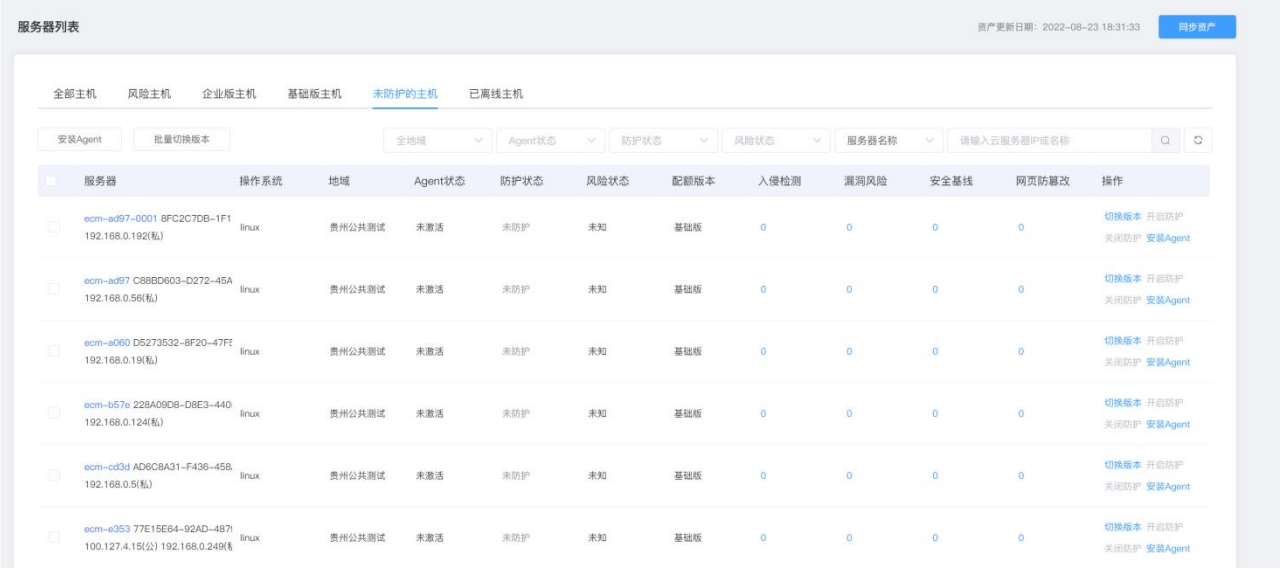
3） 企业版主机

如上图展示，企业版主机为您展示配额规格为“企业版”的服务器。

4） 基础版主机

如上图展示，基础版主机为您展示配额规格为“基础版”的服务器。

5） 未防护的主机



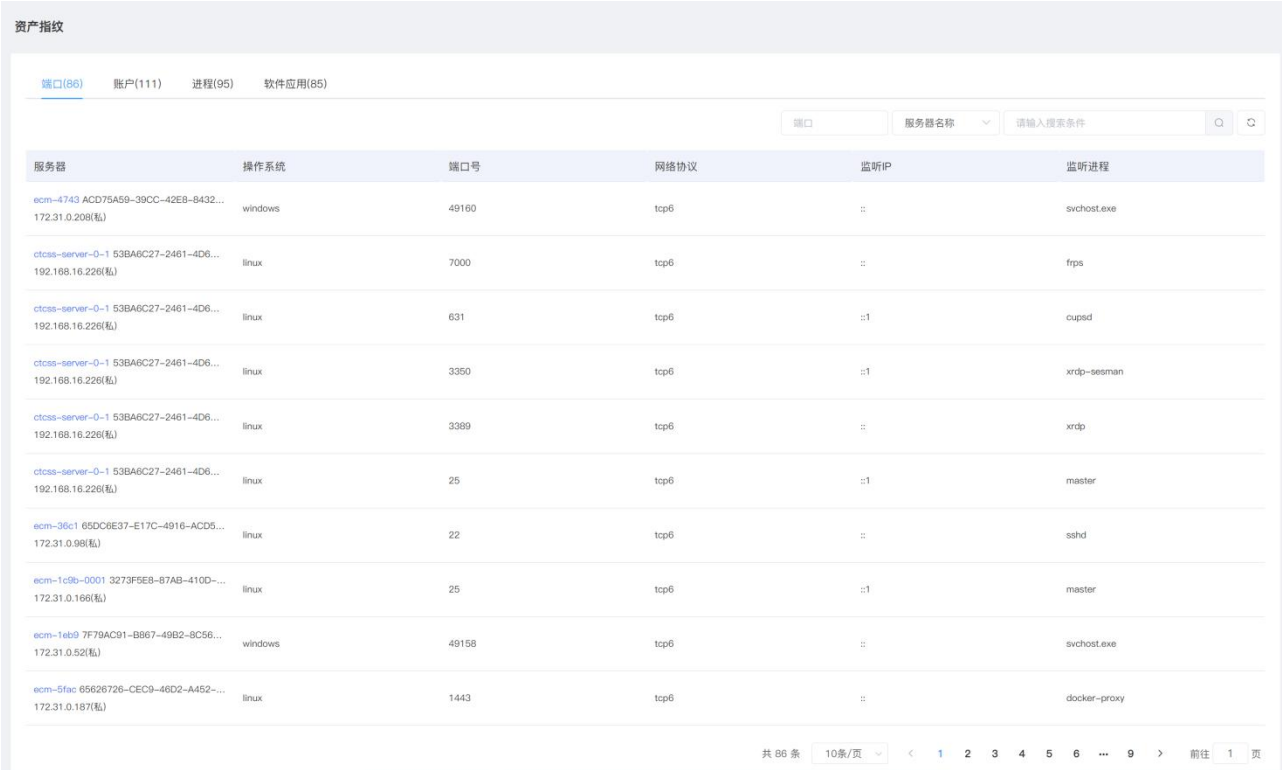
如上图展示，未防护的主机为您展示防护状态为“未防护”的全部服务器。

6） 已离线主机

如上图展示，已离线主机为您展示防护状态为“已离线”的服务器。

3.3.3 资产指纹

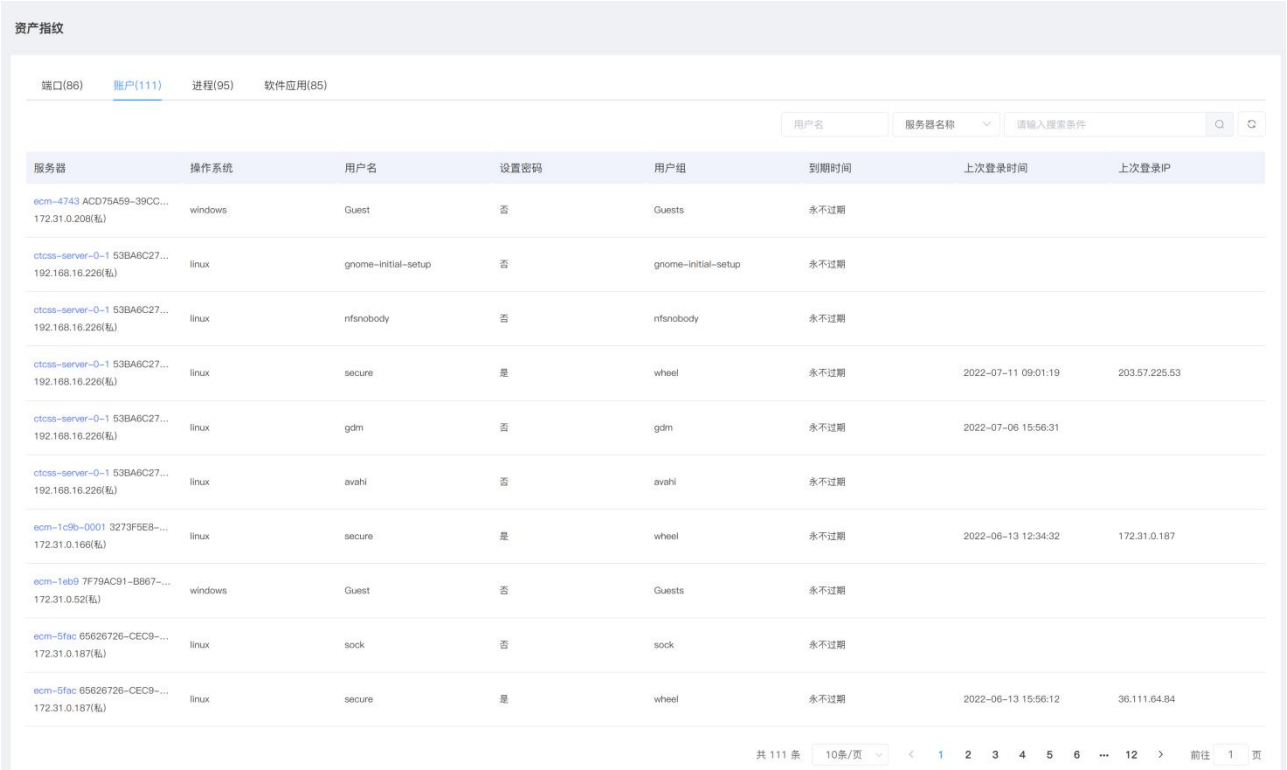
1） 端口



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。

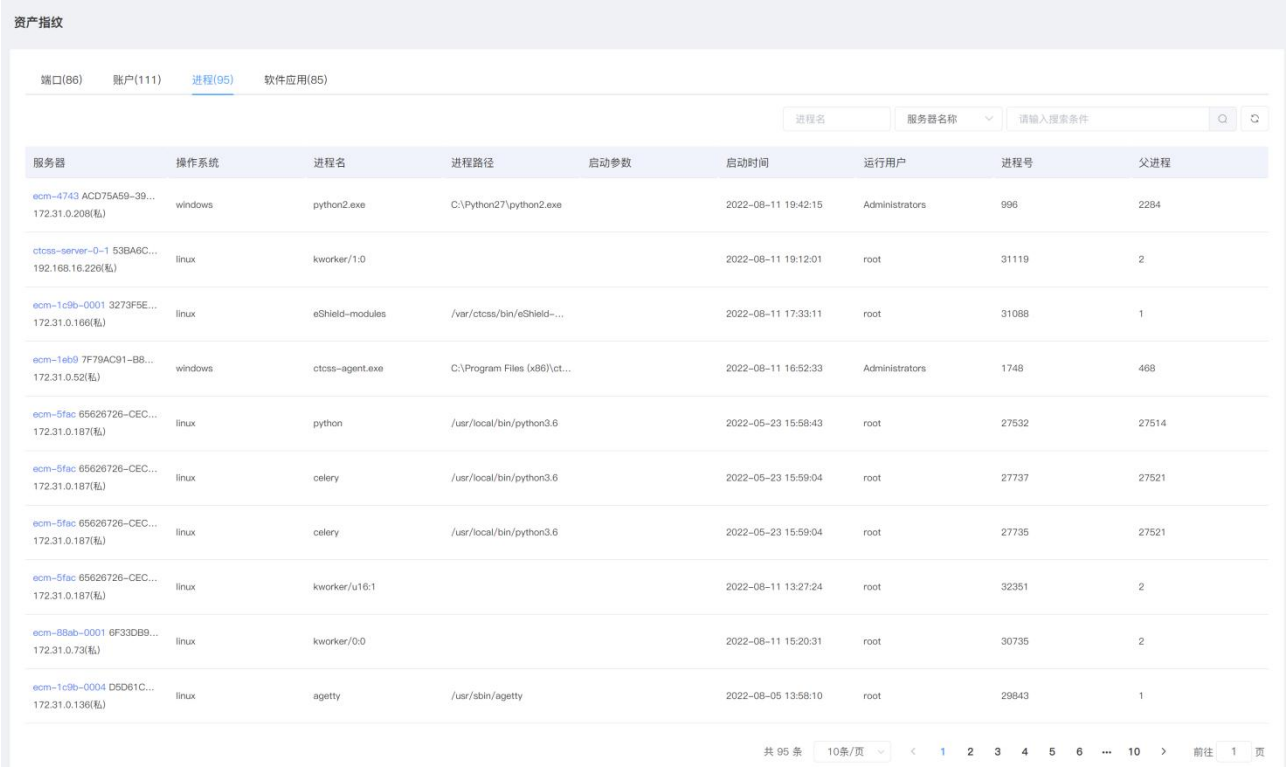
服务器包括服务器名称、UUID、私网 IP 和公网 IP。

2） 账号



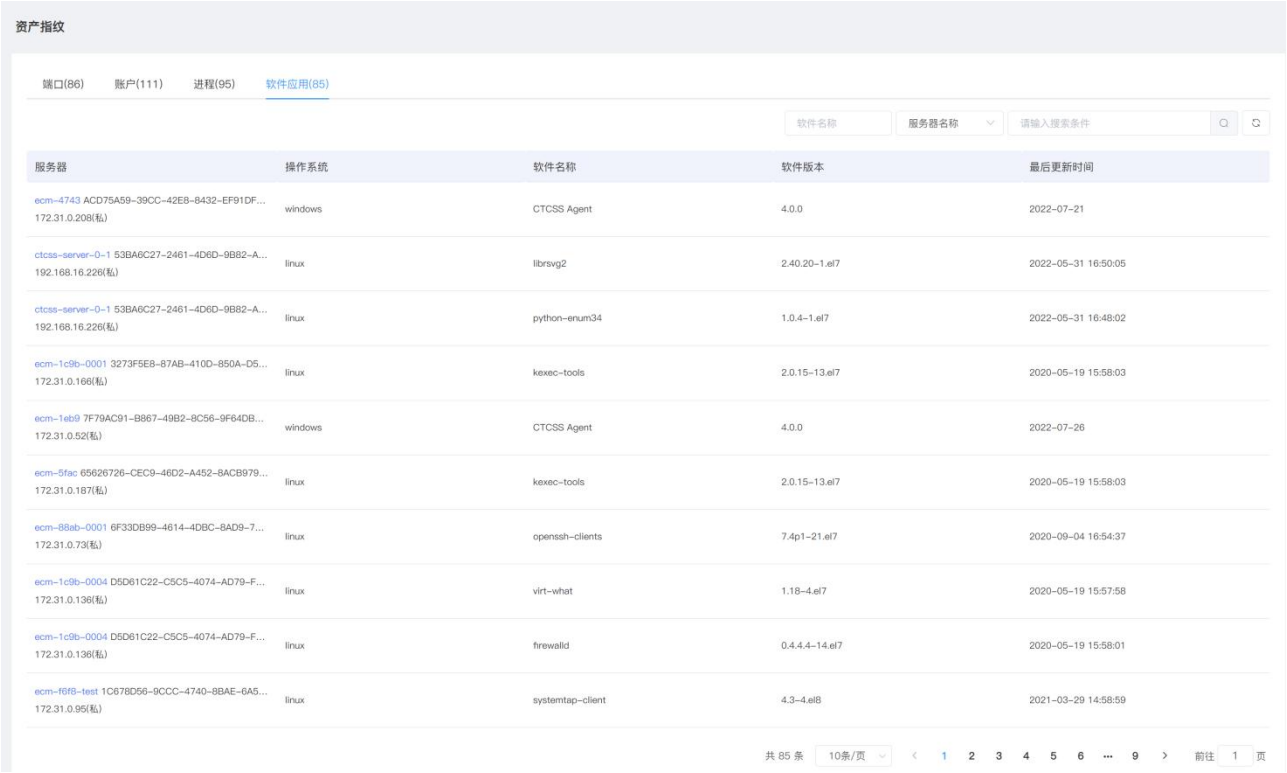
按服务器展示账号信息，包括以下字段：服务器、操作系统、用户名、设置密码、用户组、到期时间、上次登录时间、上次登录 IP。可以按照用户名、服务器名称、服务器 IP 进行搜索。

3） 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。

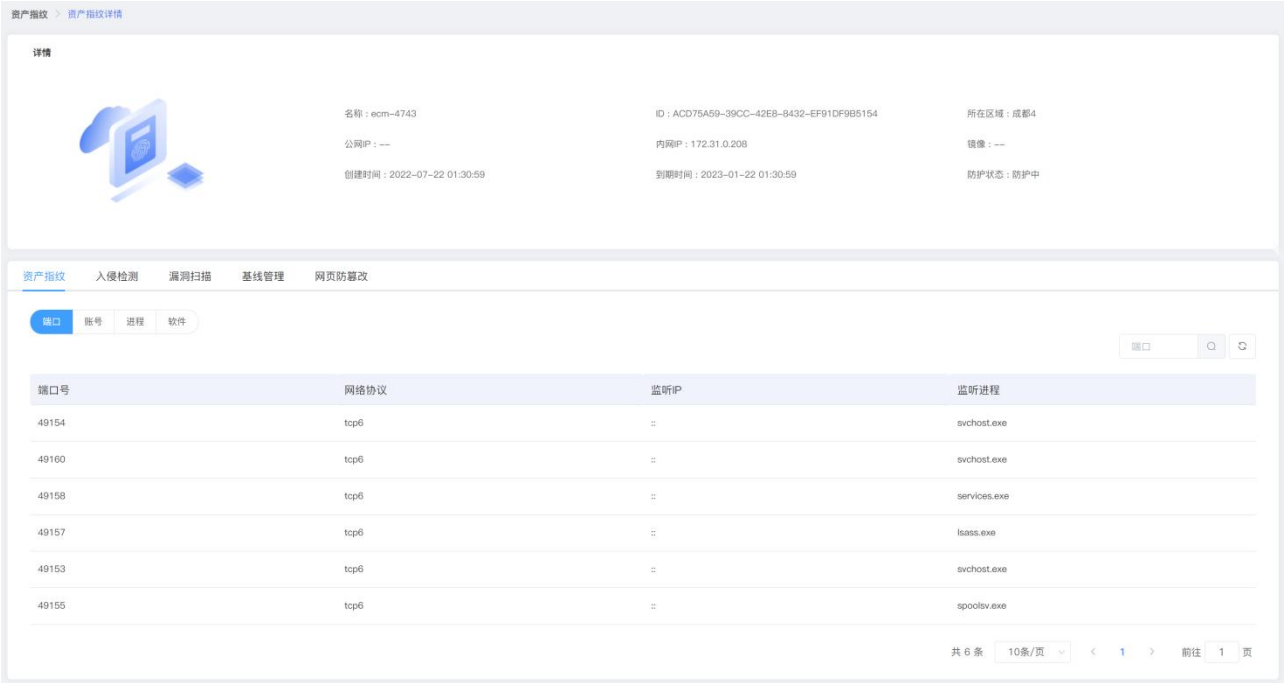
4） 软件



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。

3.3.4 资产详情

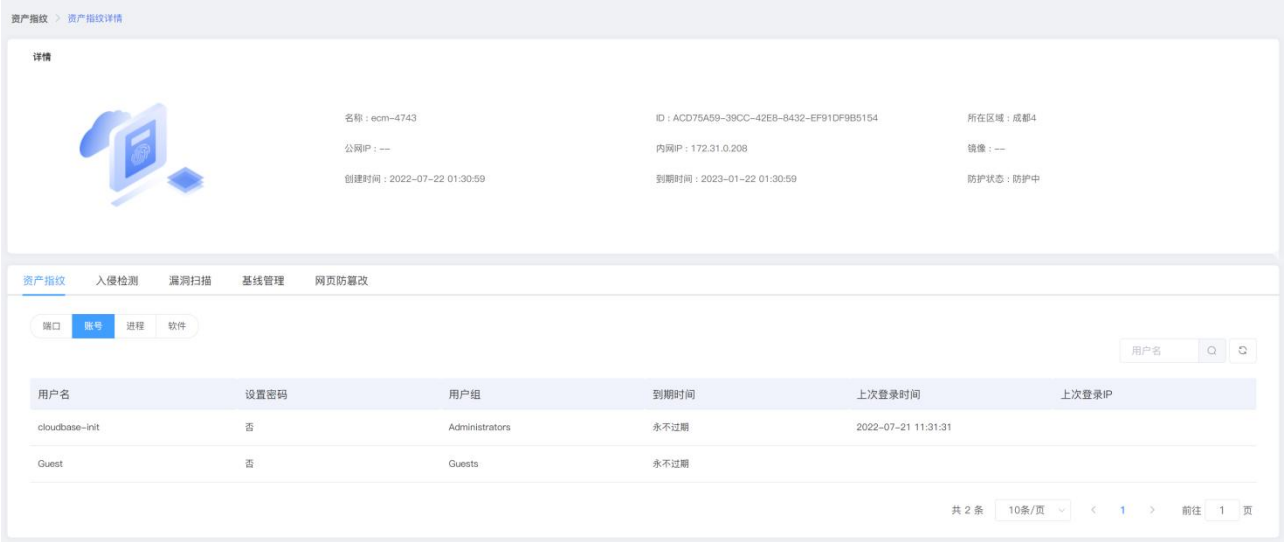
当点击服务器名称时，跳转至该服务器的 “资产指纹详情”页面上，如下图所示。上方展示该服务器的基本信息，包括服务器名称、服务器 ID、所在区域、公网 IP、内网 IP、镜像、创建时间、到期时间和防护状态。下方展示该服务器的资产指纹和风险情况。



1） 端口

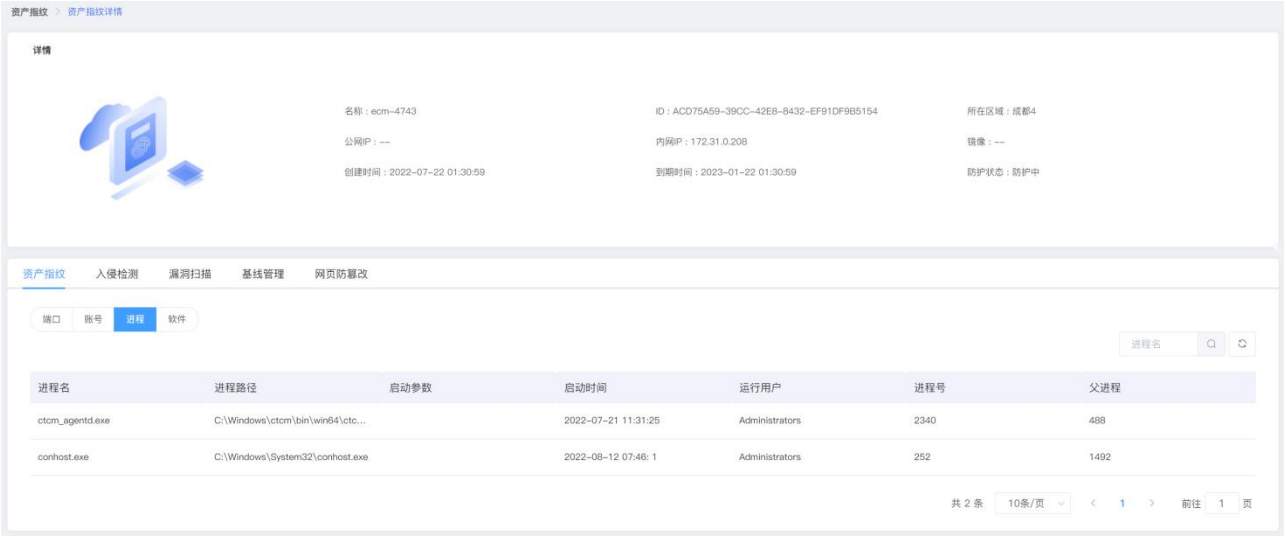
如上图所示，展示该台服务器开放的端口详情。

2） 账号



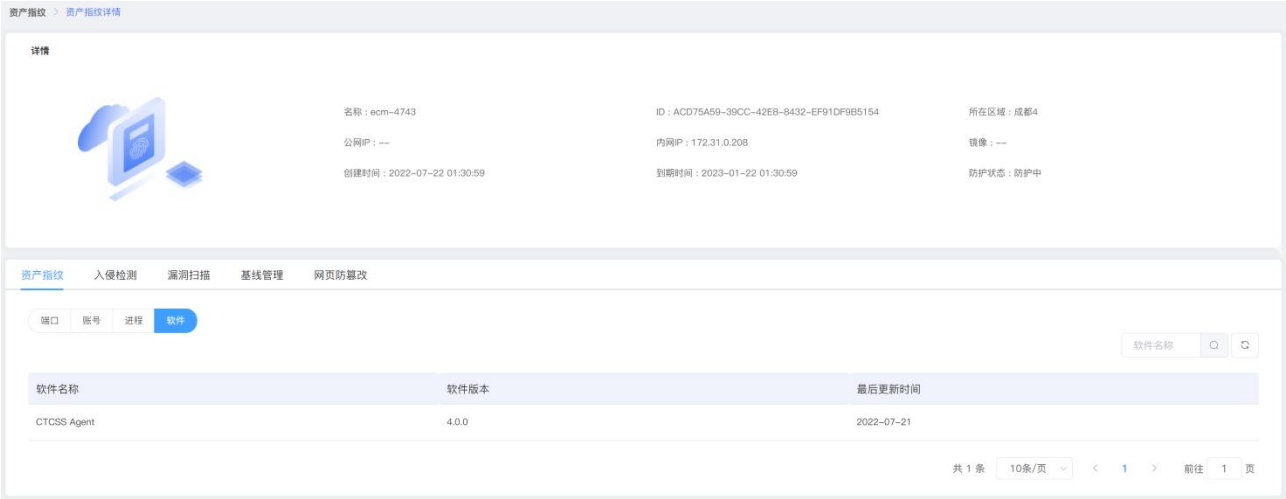
如上图所示，展示该台服务器的账号详情。

3） 进程



如上图所示，展示该台服务器的进程详情。

4） 软件

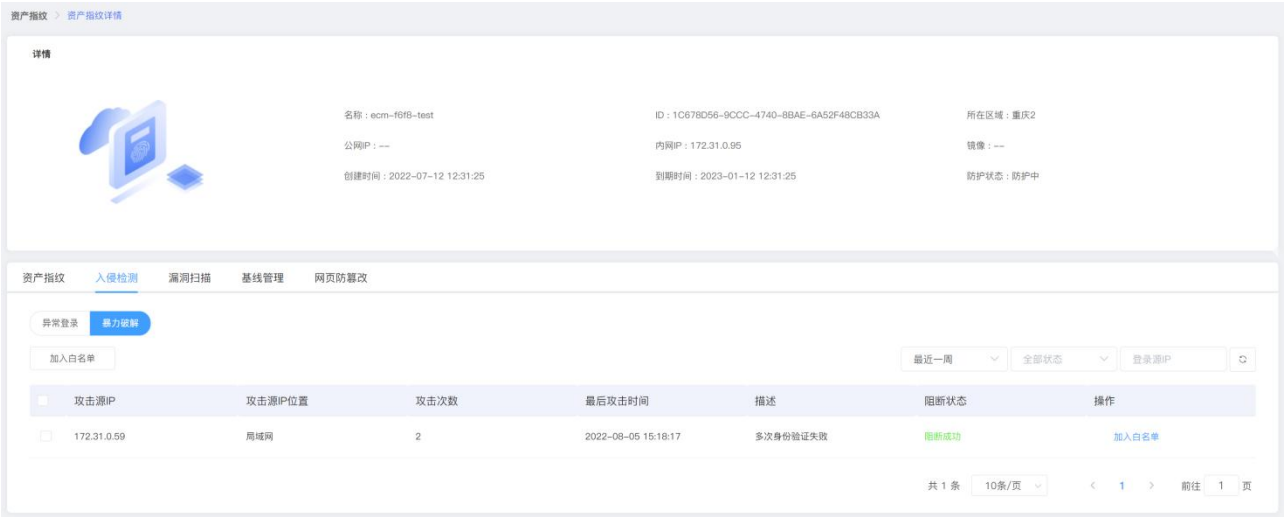


如上图所示，展示该台服务器的软件详情。

5） 异常登录

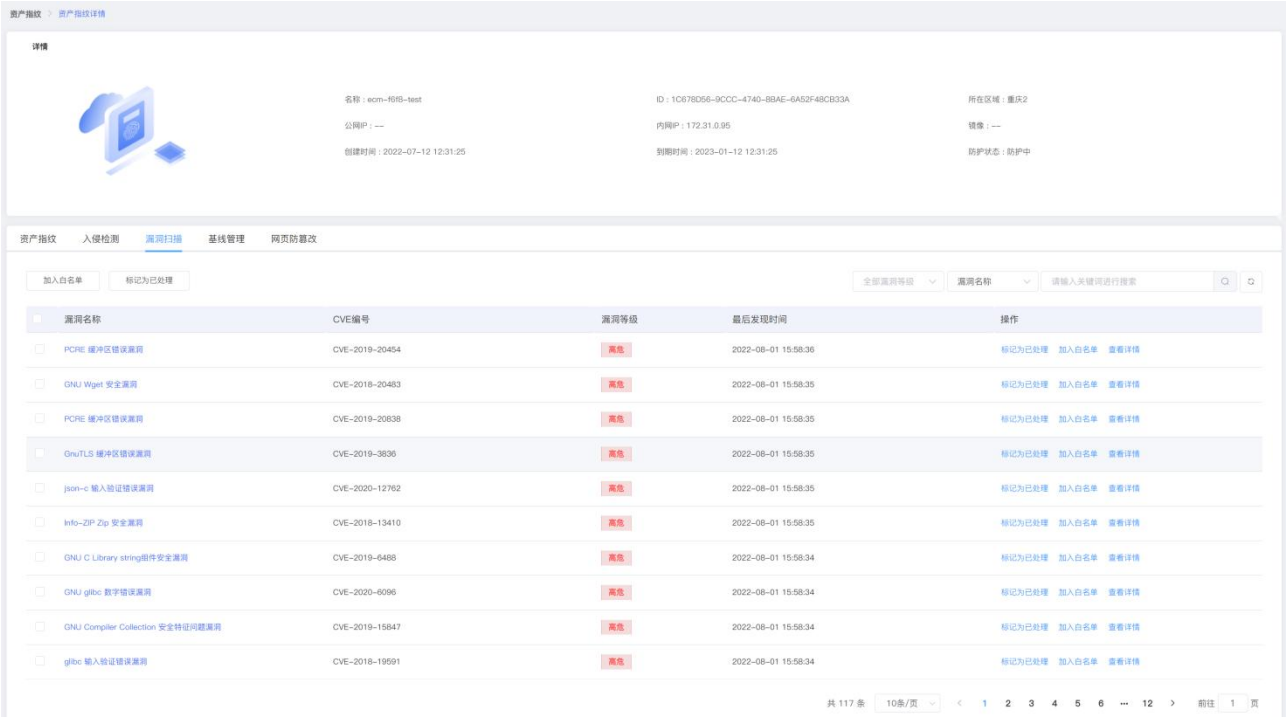
如上图所示，展示该台服务器的异常登录详情。

6） 暴力破解



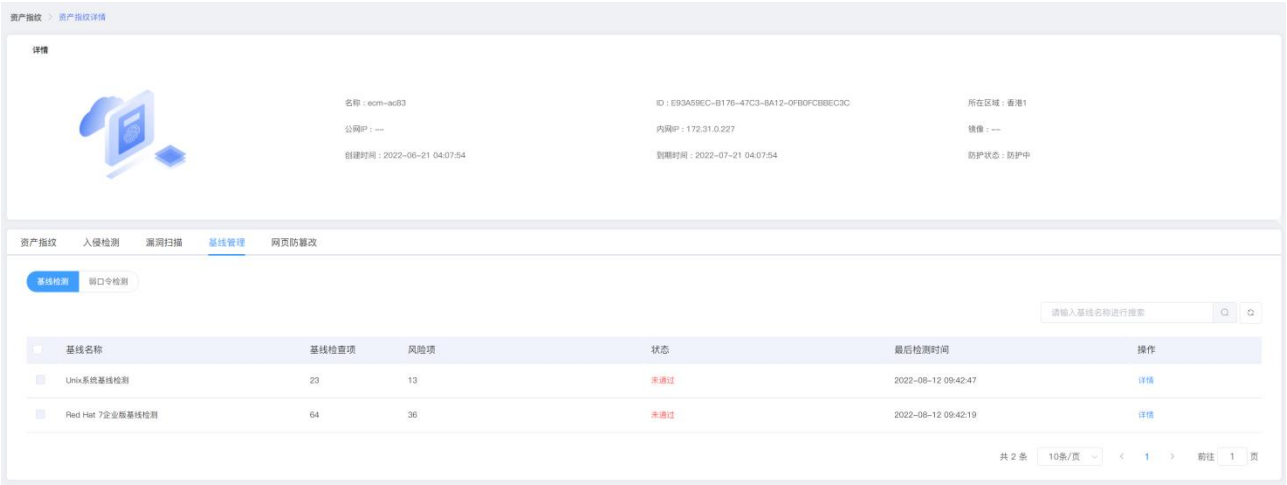
如上图所示，展示该台服务器的暴力破解详情。

7） 漏洞扫描



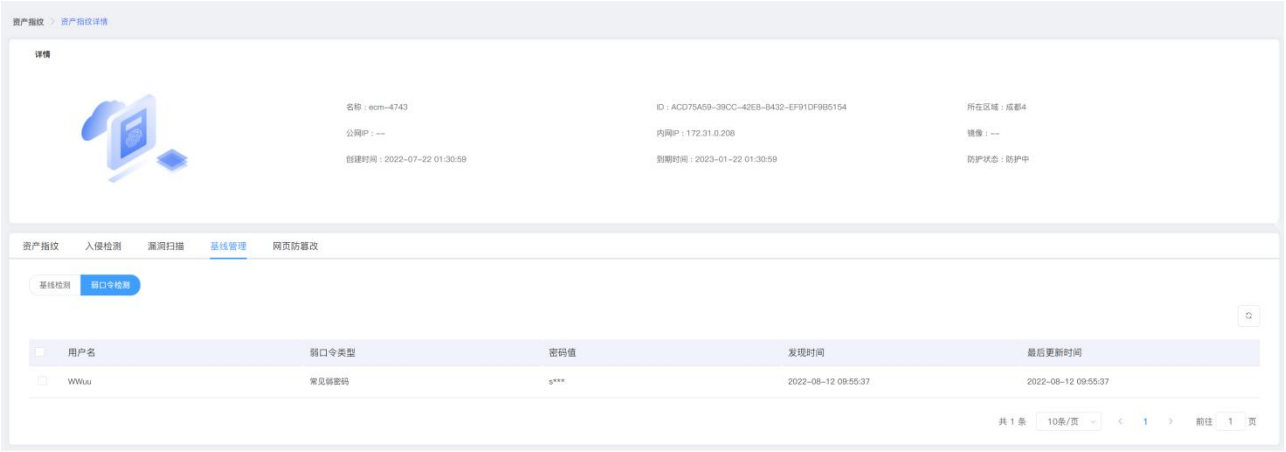
如上图所示，展示该台服务器的漏洞详情。

8） 基线检测



如上图所示，展示该台服务器的基线检测详情。

9） 弱口令检测



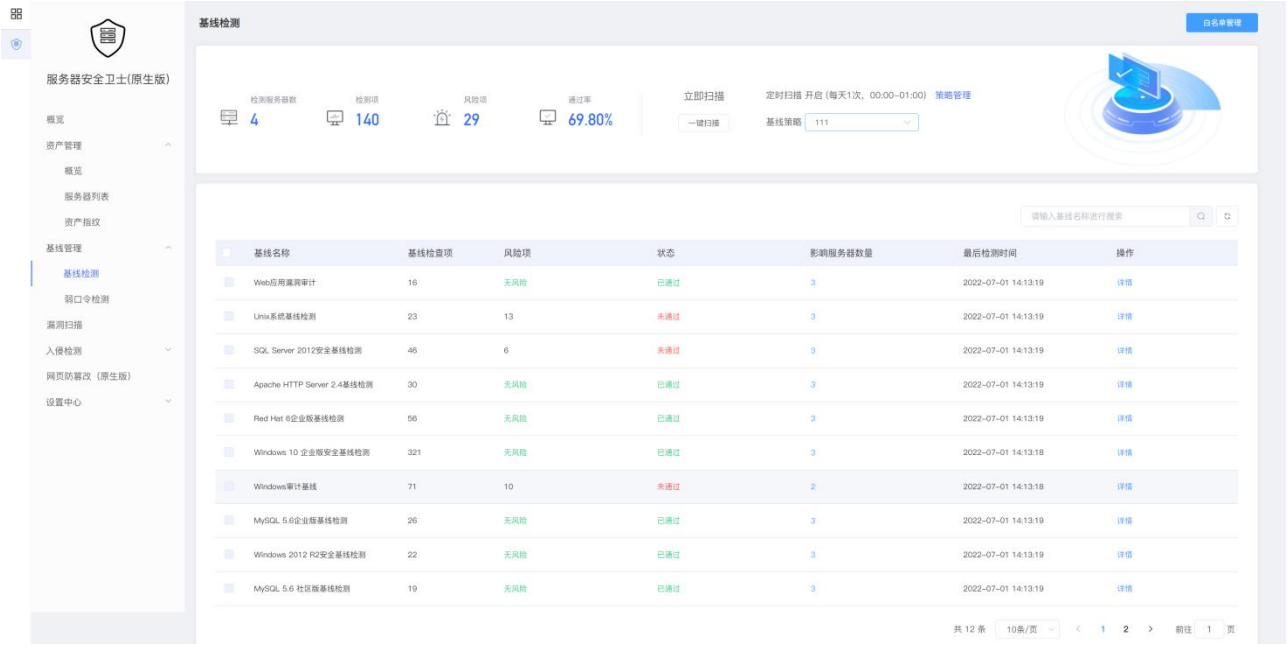
如上图所示，展示该台服务器的弱口令检测详情。

10）网页防篡改

如上图所示，展示该台服务器的网页防篡改详情。

3.4. 基线管理

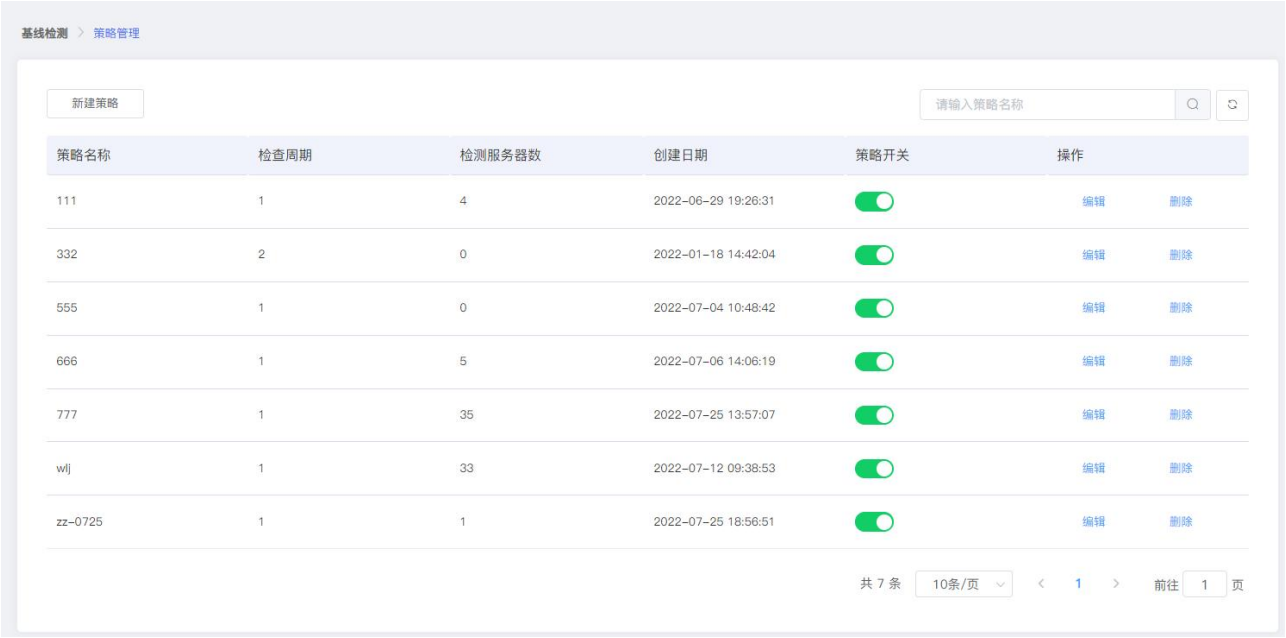
3.4.1 基线检测



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

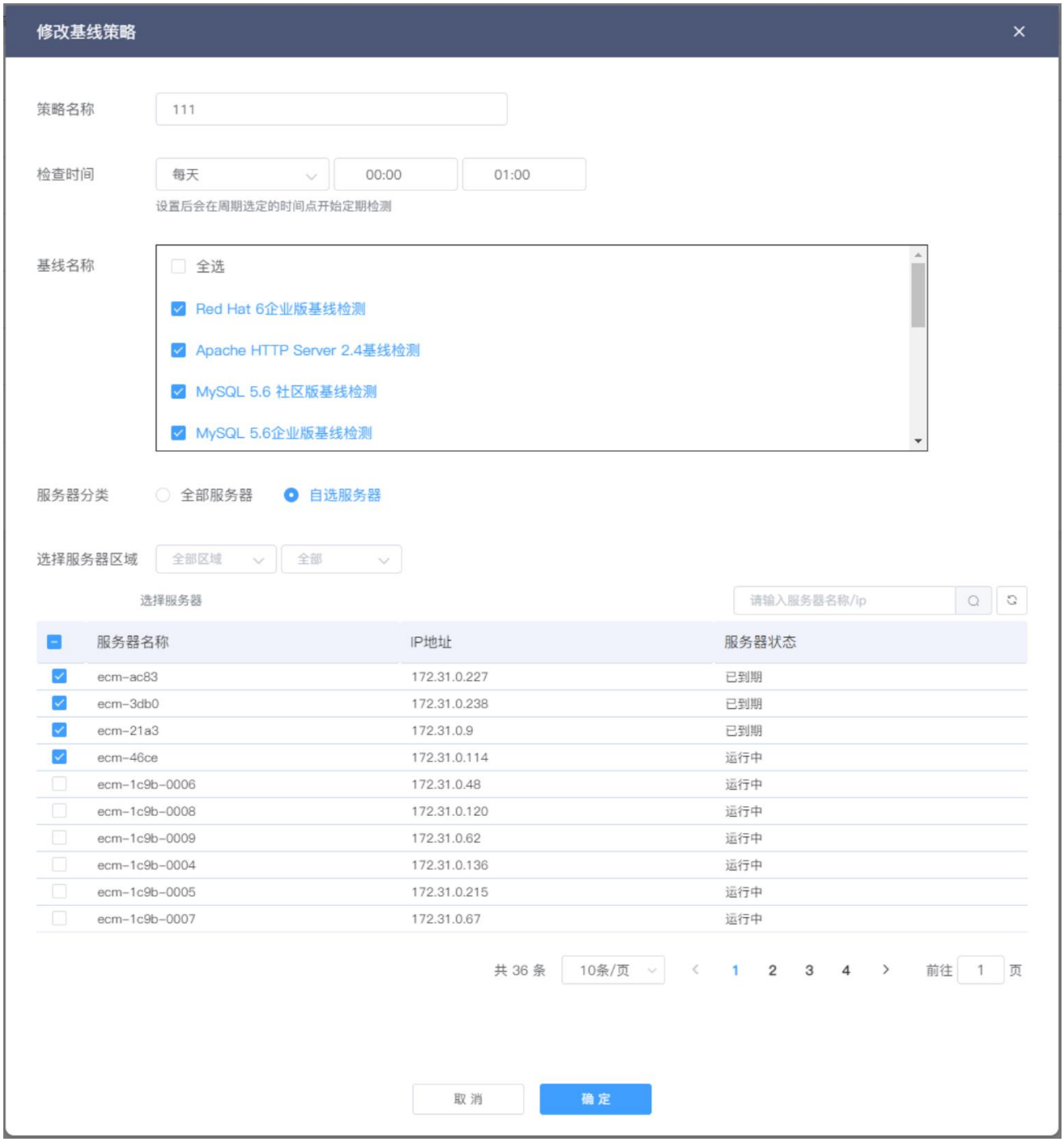
选定一个基线策略后，展示该策略上一次基线检测结果完成后的统计数据，统计情况包括检测服务器数、检测项、风险项、通过率。切换基线策略后，显示切换后的基线检测统计结果。其中，通过率=所有成功主机通过项之和÷（所有成功主机检测通过项+所有成功主机风险项）×100%。

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



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：

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。

请输入基线名称进行搜索

基线名称	基线检查项	风险项	状态	影响服务器数量	最后检测时间	操作
Web应用漏洞审计	16	无风险	已通过	3	2022-07-01 14:13:19	详情
Unix系统基线检测	23	13	未通过	3	2022-07-01 14:13:19	详情
SQL Server 2012安全基线检测	46	6	未通过	3	2022-07-01 14:13:19	详情
Apache HTTP Server 2.4基线检测	30	无风险	已通过	3	2022-07-01 14:13:19	详情
Red Hat 6企业版基线检测	56	无风险	已通过	3	2022-07-01 14:13:19	详情
Windows 10 企业版安全基线检测	321	无风险	已通过	3	2022-07-01 14:13:18	详情
Windows审计基线	71	10	未通过	2	2022-07-01 14:13:18	详情
MySQL 5.6企业版基线检测	26	无风险	已通过	3	2022-07-01 14:13:19	详情
Windows 2012 R2安全基线检测	22	无风险	已通过	3	2022-07-01 14:13:19	详情
MySQL 5.6 社区版基线检测	19	无风险	已通过	3	2022-07-01 14:13:19	详情

共 12 条 10条/页 1 2 前往 1 页

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。

基线检测 > Unix系统基线检测详情

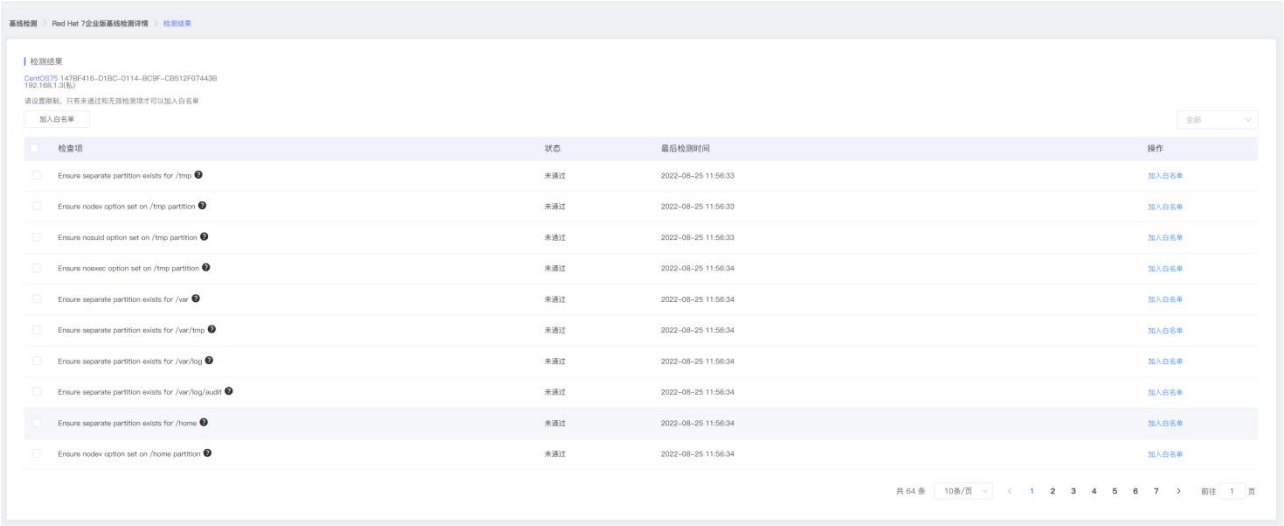
Unix系统基线检测

全部状态 服务器名称 输入搜索条件

服务器	通过项	风险项	无效项	状态	最后检测时间	操作
ecm-21a3 CC858C43-E2FE-47B1... 172.31.0.9(私)	0	0	0	失败	2022-07-01 14:13:25	详情
ecm-3db0 32F1DF23-6685-4475-... 172.31.0.238(私)	3	13	7	未通过	2022-07-01 14:13:28	详情
ecm-46ce CBF2380E-9967-4A8B... 172.31.0.114(私)	0	0	0	失败	2022-07-01 14:13:19	详情

共 3 条 10条/页 1 前往 1 页

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。



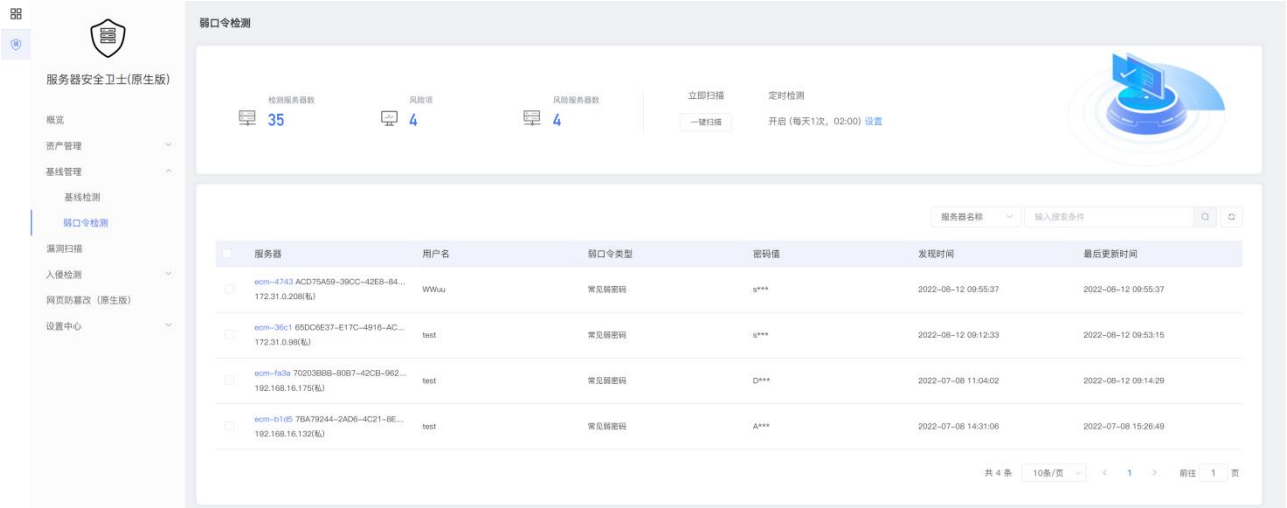
若您检测时需要忽略该检测项，可以对该项进行“加入白名单”操作，点击后弹出对话框，如下图所示：

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。

3.4.2 弱口令检测



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

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

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。

当开始一键扫描或定时扫描后，展示动态检测效果。

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。

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

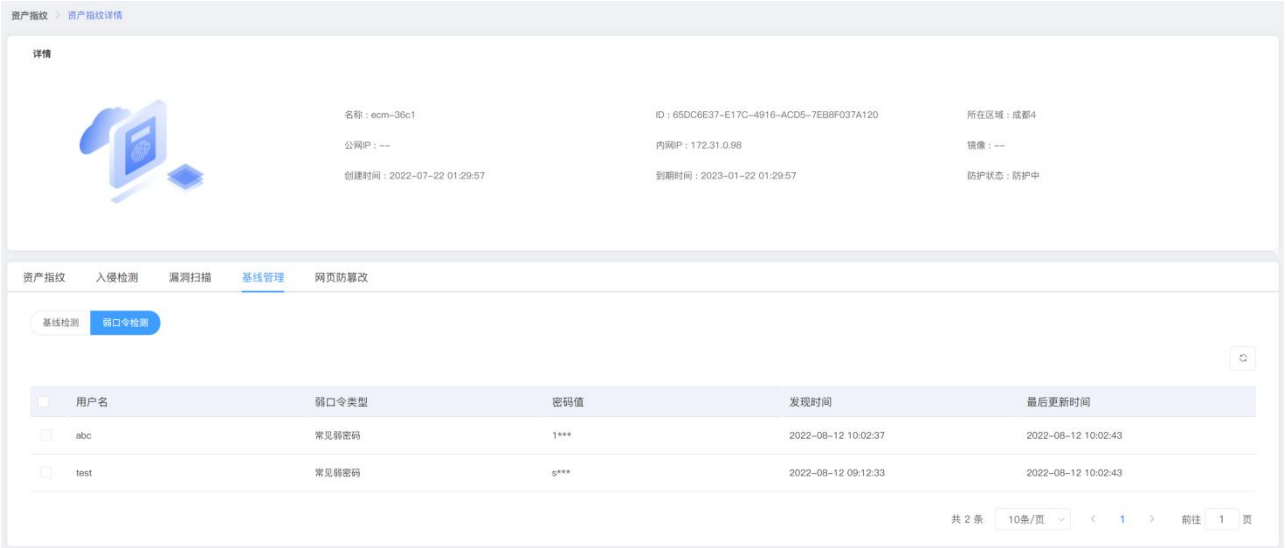
服务器名称 输入搜索条件

服务器	用户名	弱口令类型	密码值	发现时间	最后更新时间
ecm-36c1 65DC6E37-E17C-4916-AC... 172.31.0.98(私)	abc	常见弱密码	1***	2022-08-12 10:02:37	2022-08-12 10:02:43
ecm-36c1 65DC6E37-E17C-4916-AC... 172.31.0.98(私)	test	常见弱密码	s***	2022-08-12 09:12:33	2022-08-12 10:02:43
ecm-4743 ACD75A59-39CC-42E8-84... 172.31.0.208(私)	WWuu	常见弱密码	s***	2022-08-12 09:55:37	2022-08-12 10:02:22
ecm-fa3a 70203BBB-80B7-42CB-962... 192.168.16.175(私)	test	常见弱密码	D***	2022-07-08 11:04:02	2022-08-12 09:14:29
ecm-b1d5 7BA79244-2AD6-4C21-8E... 192.168.16.132(私)	test	常见弱密码	A***	2022-07-08 14:31:06	2022-07-08 15:26:49

共 5 条 10条/页 1 前往 1 页

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

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



资产指纹 > 资产指纹详情

详情

名称：ecm-36c1 ID：65DC6E37-E17C-4916-ACD5-7EB8F037A120 所在区域：成都4

公网IP：-- 内网IP：172.31.0.98 镜像：--

创建时间：2022-07-22 01:29:57 到期时间：2023-01-22 01:29:57 防护状态：防护中

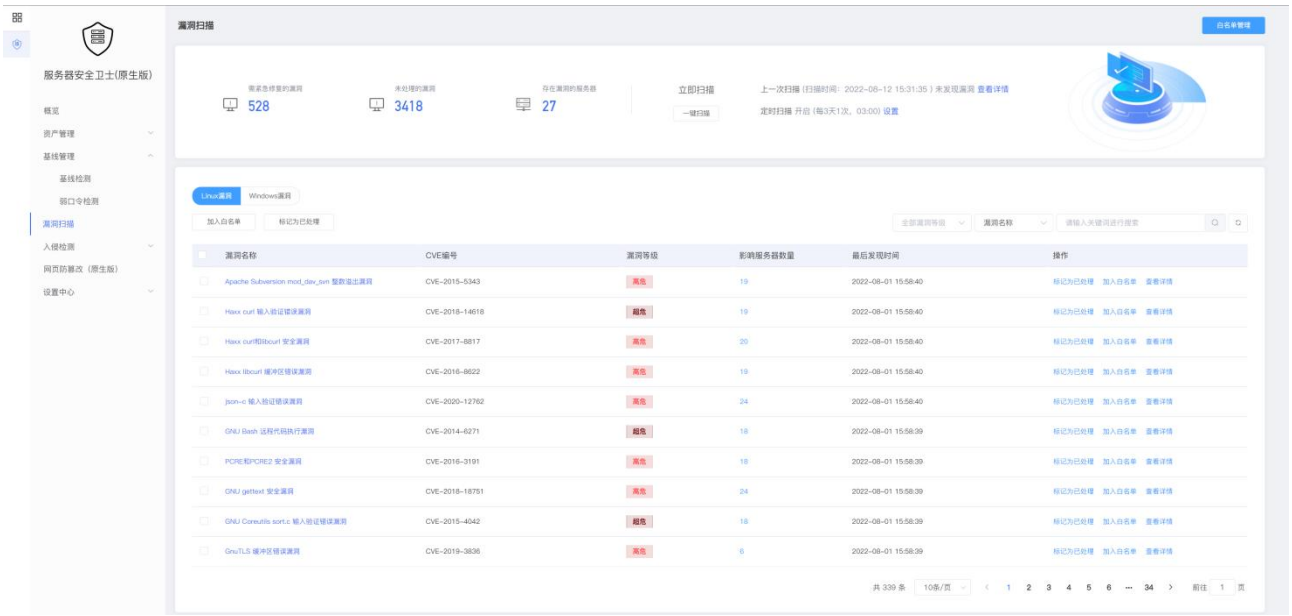
资产指纹 入侵检测 漏洞扫描 基线管理 网页防篡改

基线检测 弱口令检测

用户名	弱口令类型	密码值	发现时间	最后更新时间
abc	常见弱密码	1***	2022-08-12 10:02:37	2022-08-12 10:02:43
test	常见弱密码	s***	2022-08-12 09:12:33	2022-08-12 10:02:43

共 2 条 10条/页 1 前往 1 页

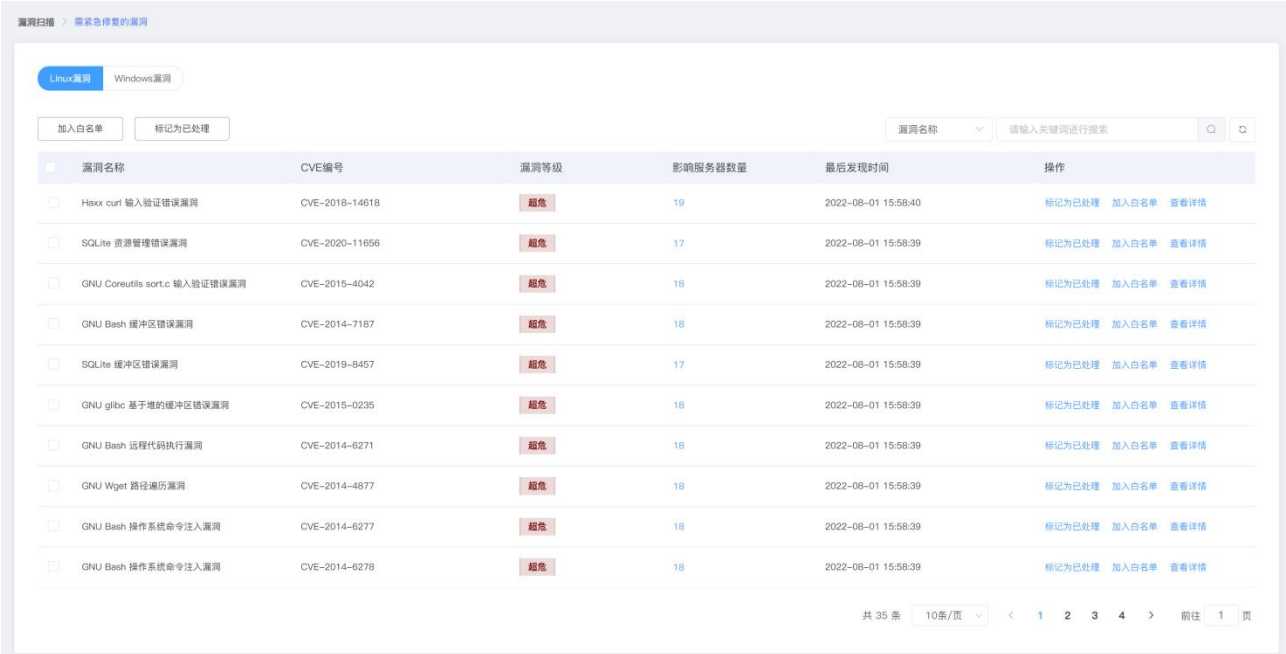
3.5. 漏洞扫描



如上图所示，上方展示漏洞扫描的统计情况和漏洞扫描设置，下方展示漏洞列表。

统计情况包括需紧急修复的漏洞、未处理的漏洞、存在漏洞的服务器。

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



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。

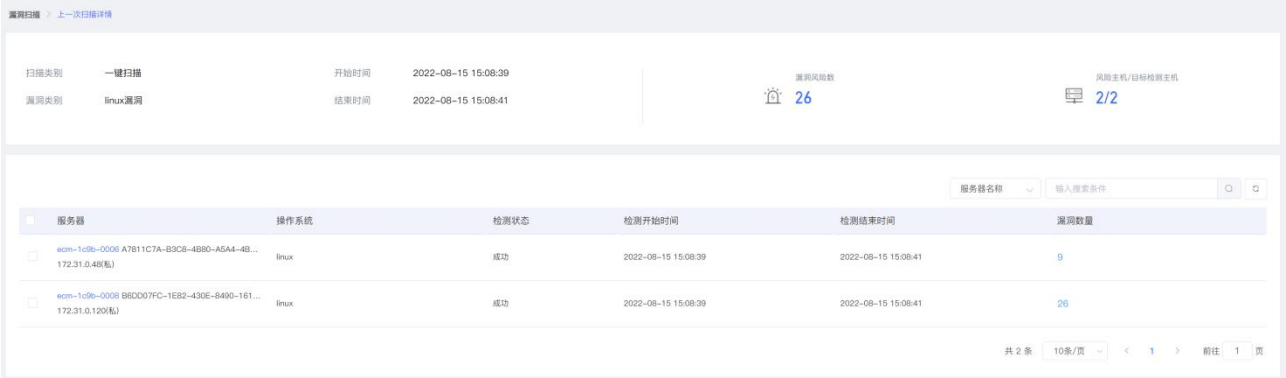
点击定时扫描右侧的“设置”，可进行定时扫描设置。设置选项包括漏洞类别、漏洞扫描等级、定期检测周期、超时设置、服务器选择的设置。其中，超时设置的时间需大于 30 分钟，小于 3 小时。

当开始一键扫描或定时扫描后，页面上展示下图动态效果。

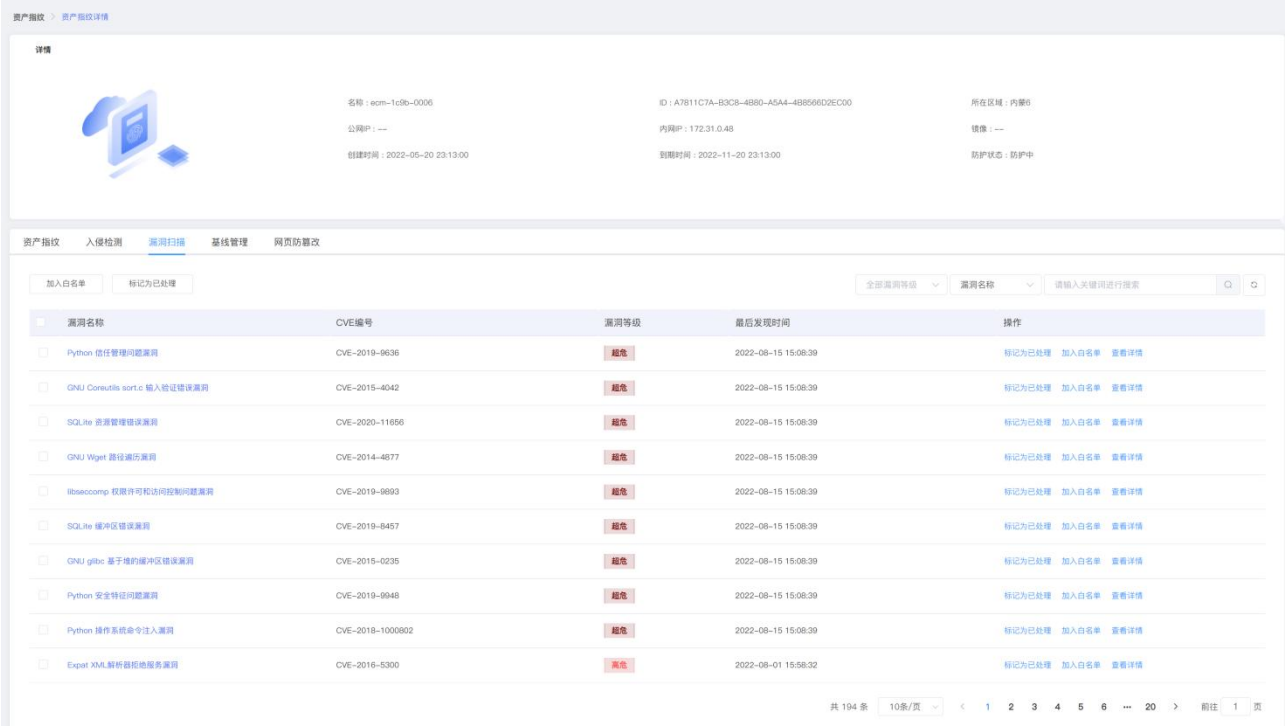
在扫描过程中，可随时点击“停止扫描”，点击“停止扫描”时，弹出如下对话框，点击“确定”后停止扫描。

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。



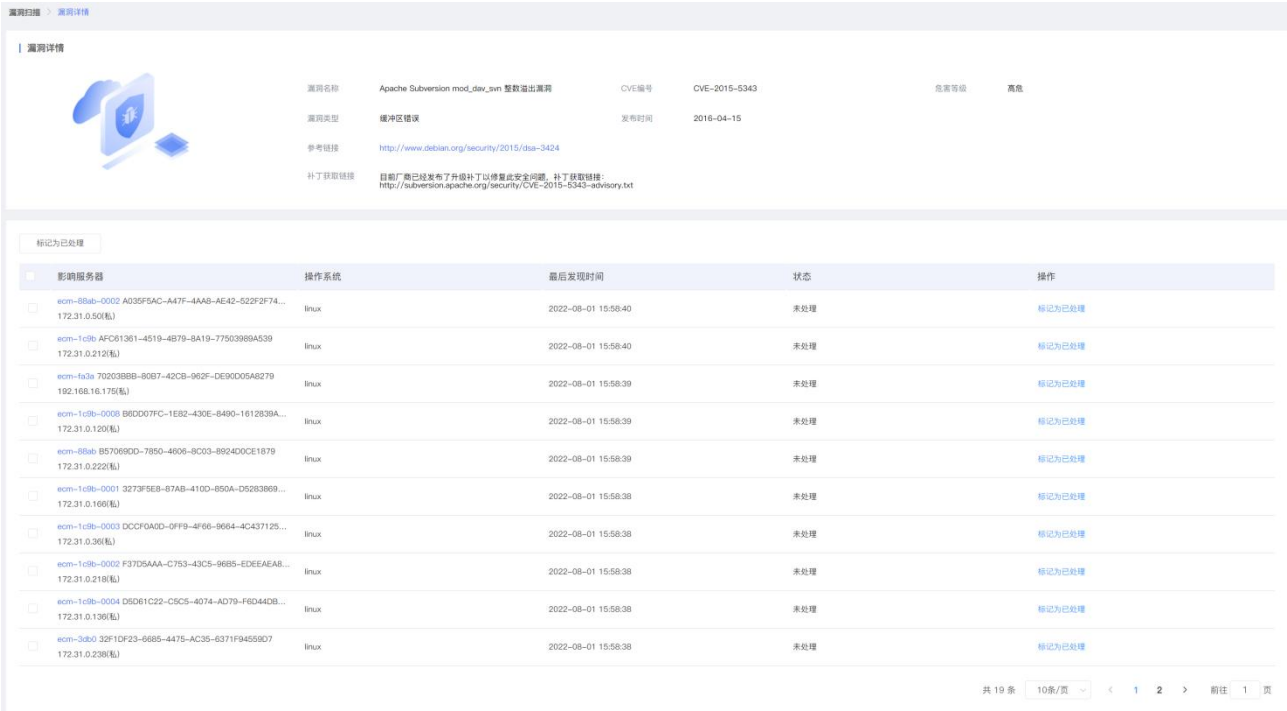
当点击漏洞数量中下方的数字时，跳转至资产详情页面，如下图所示。在资产详情页面，为您展示该服务器的基本信息和漏洞情况。



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，

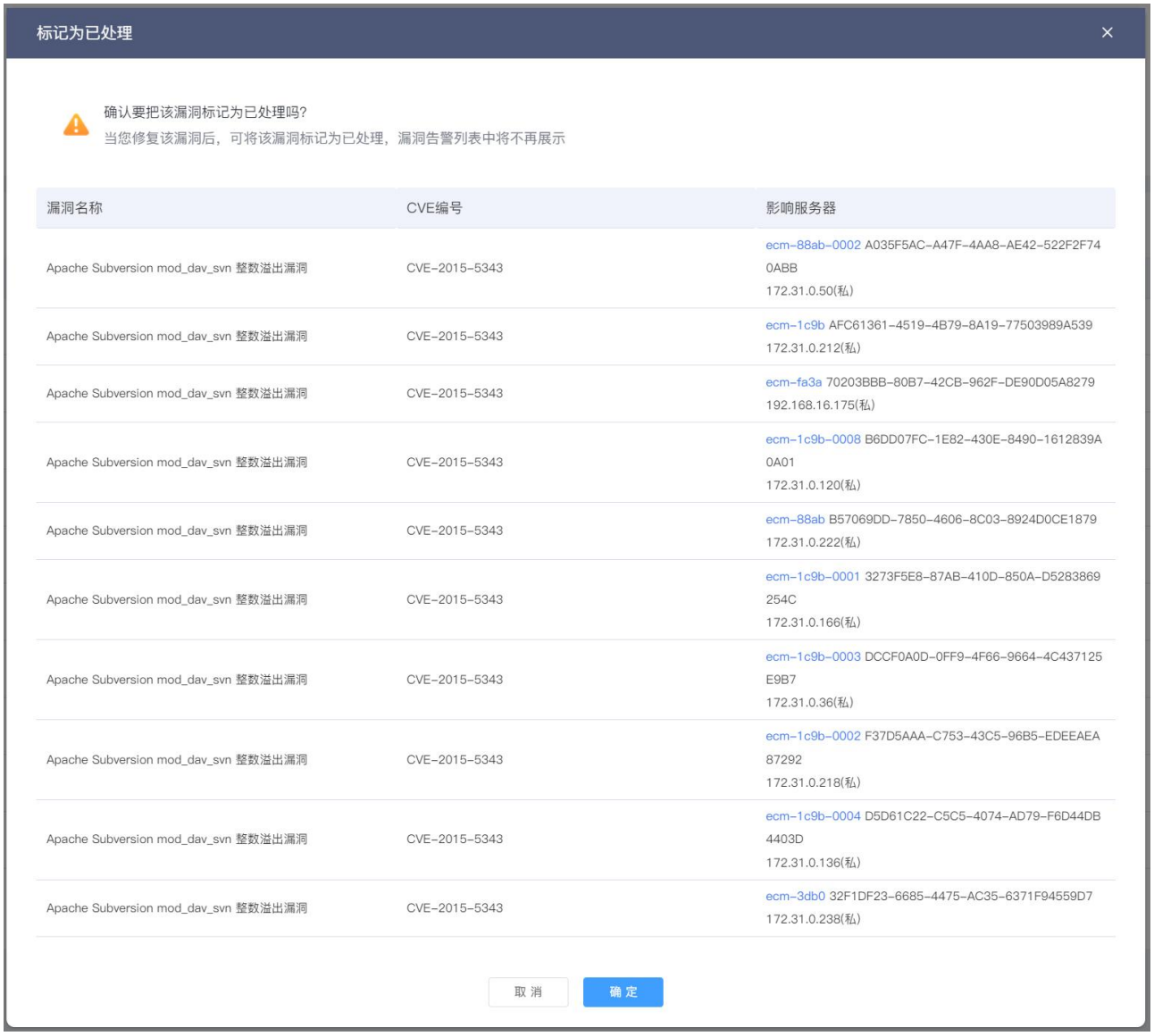
包括漏洞名称、CVE 编号、漏洞等级、影响服务器数量、最后发现时间和操作，列表默认按照最后发现时间排序，最新发现的漏洞位于最上方。漏洞列表可按照漏洞等级、漏洞名称、CVE 编号进行搜索。

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。

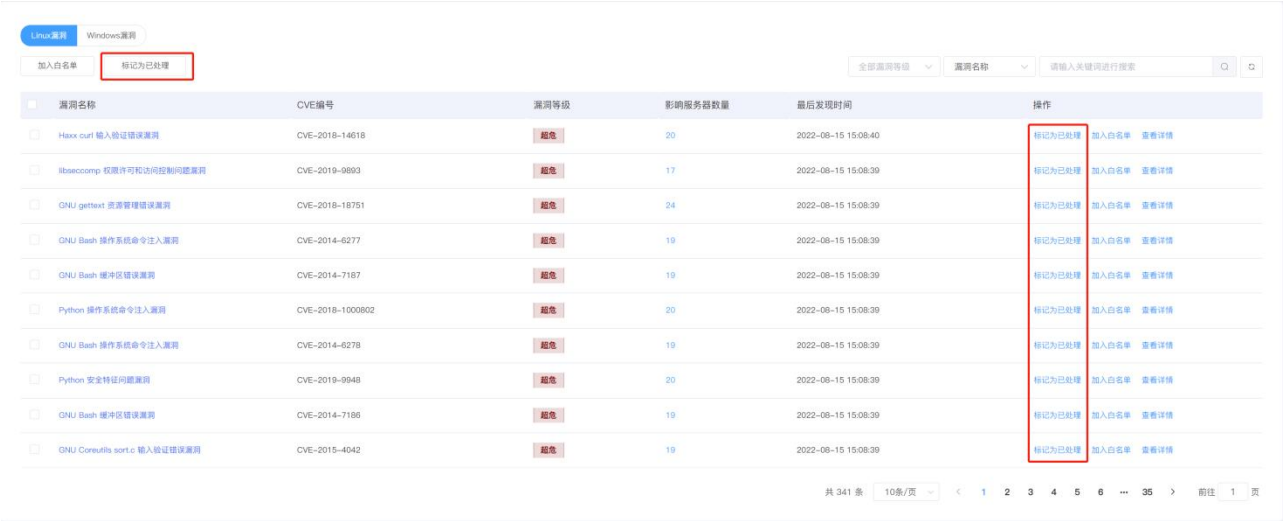


当点击一台服务器后面的“标记为已处理”时，弹出如下对话框，确认后，该条记录的状态变更为“已处理”，且“漏洞扫描”页面上该漏洞影响服务器数量减 1。

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。



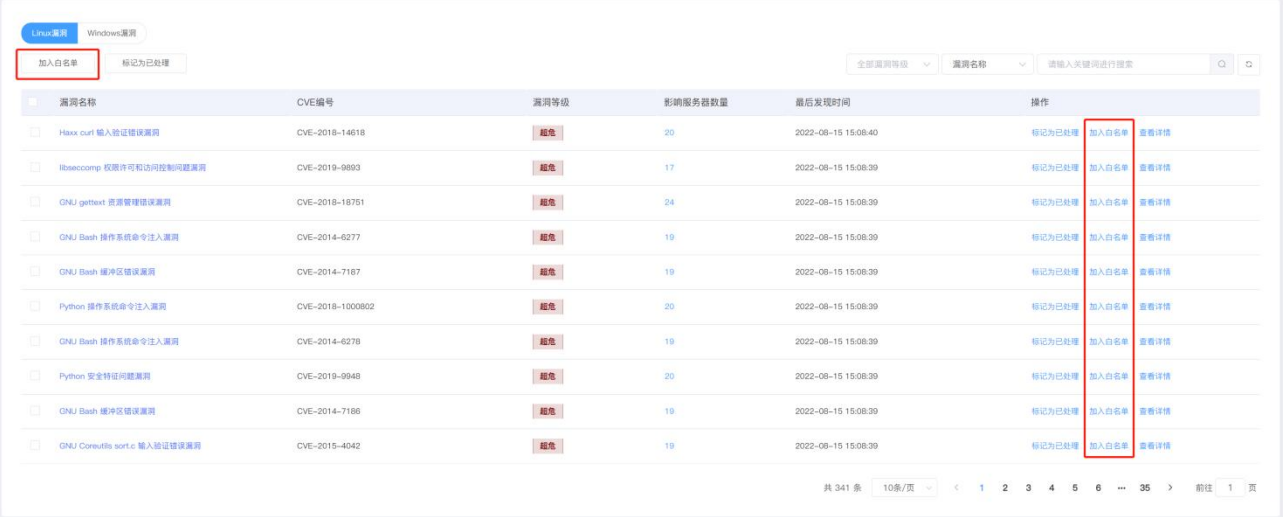
当点击漏洞扫描页面上漏洞列表中的“标记为已处理”时，如下图所示：



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”。

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。

3.6. 入侵检测

3.6.1 异常登录

如上图所示，上方展示异常登录事件的统计情况，下方展示异常登录事件列表。

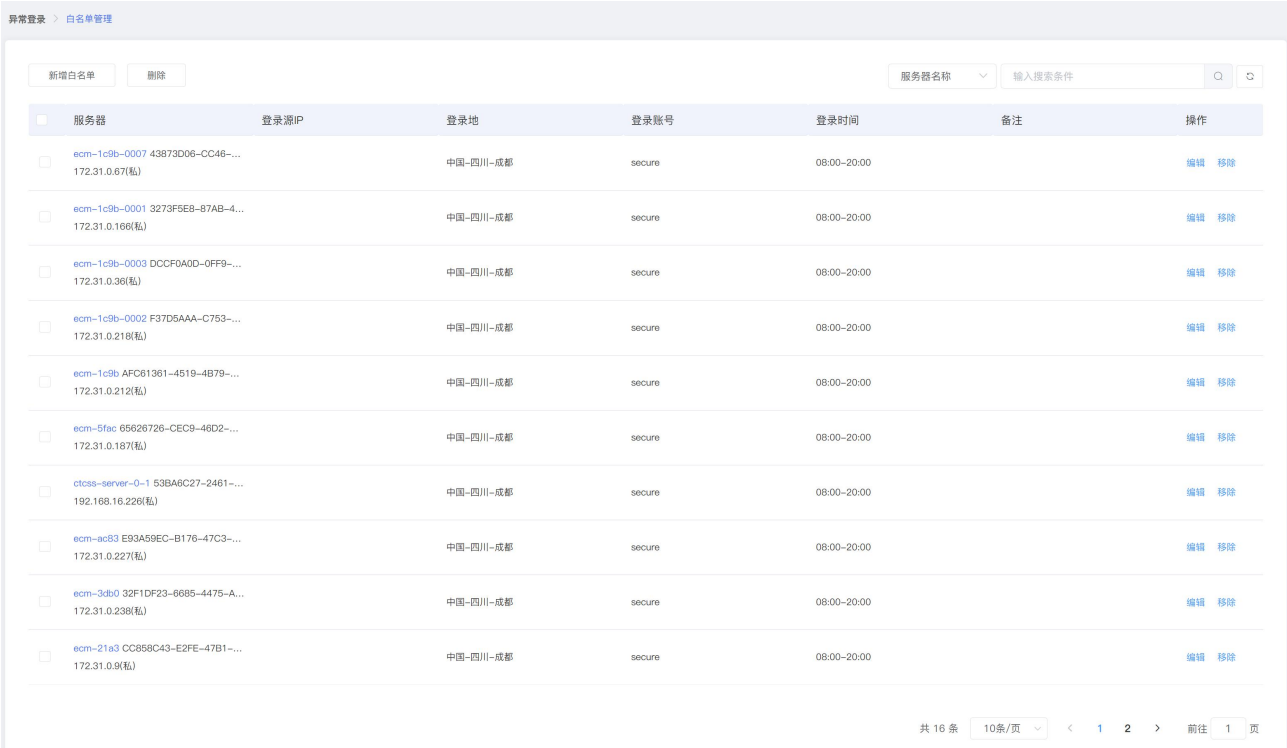
统计情况包括异常登录事件数、爆破登录事件数、存在风险的服务器数，都默认统计最近一周的时间，还可以统计最近一月和最近三月的时间维度。异常登录事件：统计事件列表中的异常登录事件数，爆破登录事件：统计事件列表中的爆破登录事件数，存在风险的服务器：有异常登录和爆破登录事件的服务器数量，如果同一台服务器有不同的事件需要进行去重。

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。

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。

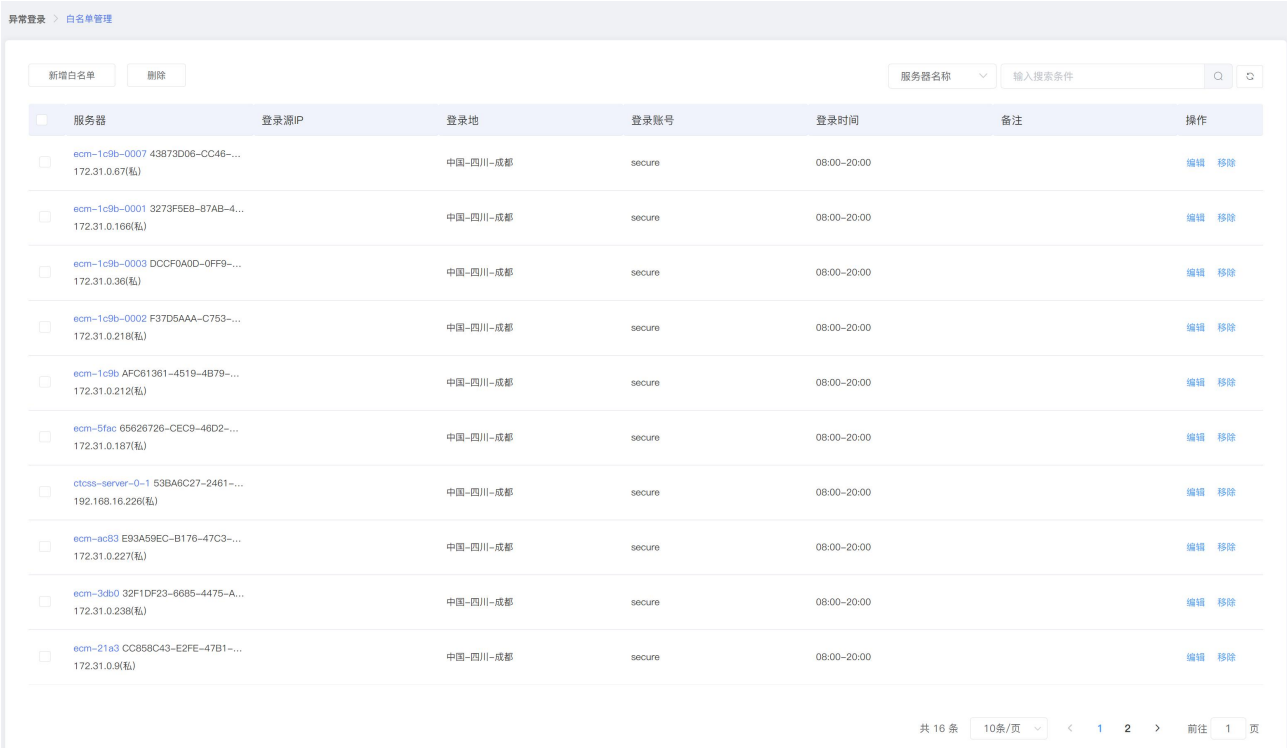
若您需要将某些登录 IP、登录用户名、登录时间和登录地区设置为正常登录，请您点击异常登录页面上的“白名单管理”进行设置，设置后将不再进行异常登录告警。

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。

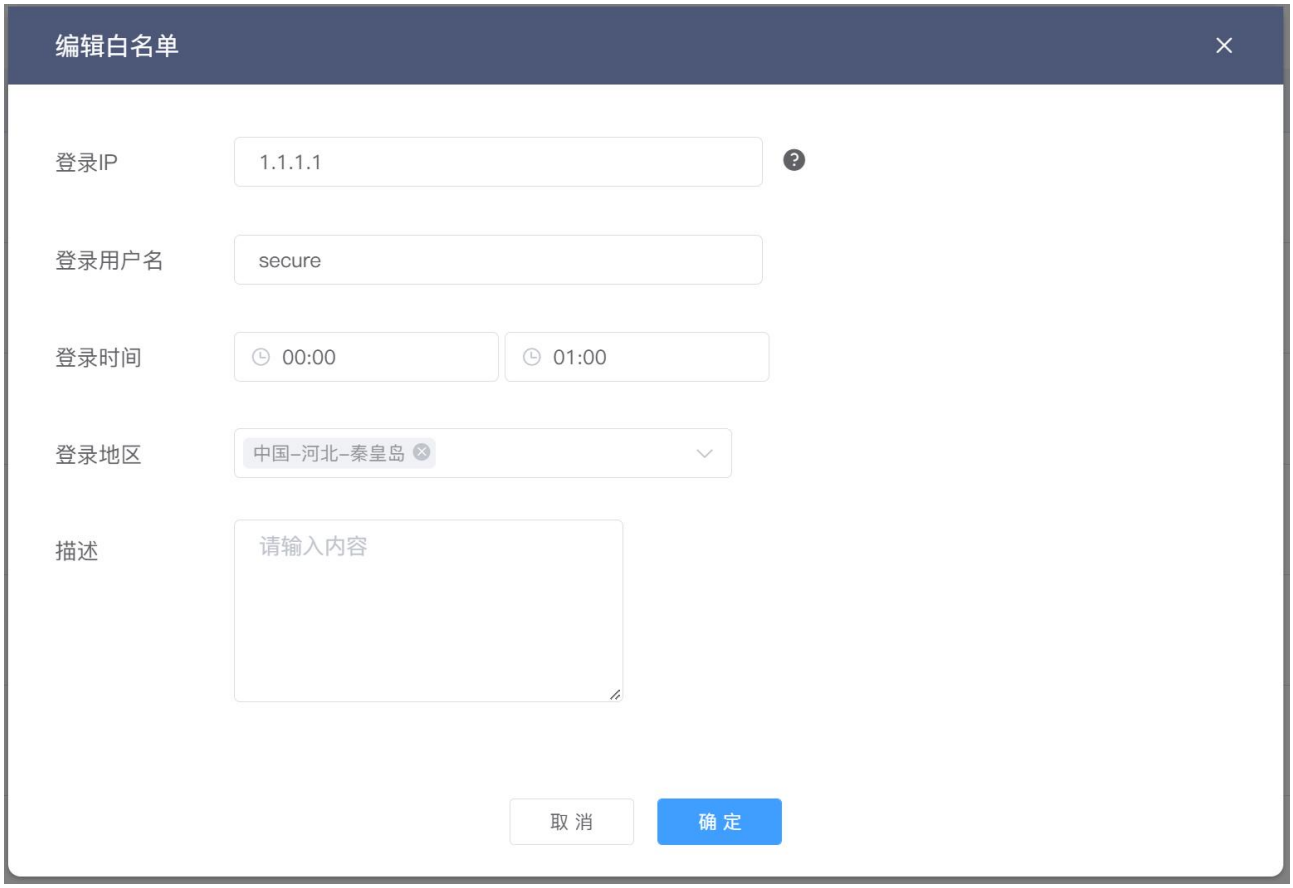


点击“新增白名单”时，弹出如下对话框，可填写登录 IP、登录用户名、登录时间、登录地区、描述，并选择服务器。登录 IP 支持单个 IP（示例：1.1.1.1）、IP 范围（示例：1.1.1.1-1.1.1.10）和 IP 段（示例：172.168.34.1/20）。多个 IP 之间用英文，隔开。登录地可选择多个登录地。登录账号支持输入多个用户名，用英文,隔开。登录时间可选择开始时间和结束时间。服务器可选择全部服务器和部分服务器。以上字段，除去服务器外，均为非必填，但登录 IP、登录用户名、登录时间、登录地区至少需要填写一项，可填写多项。

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：

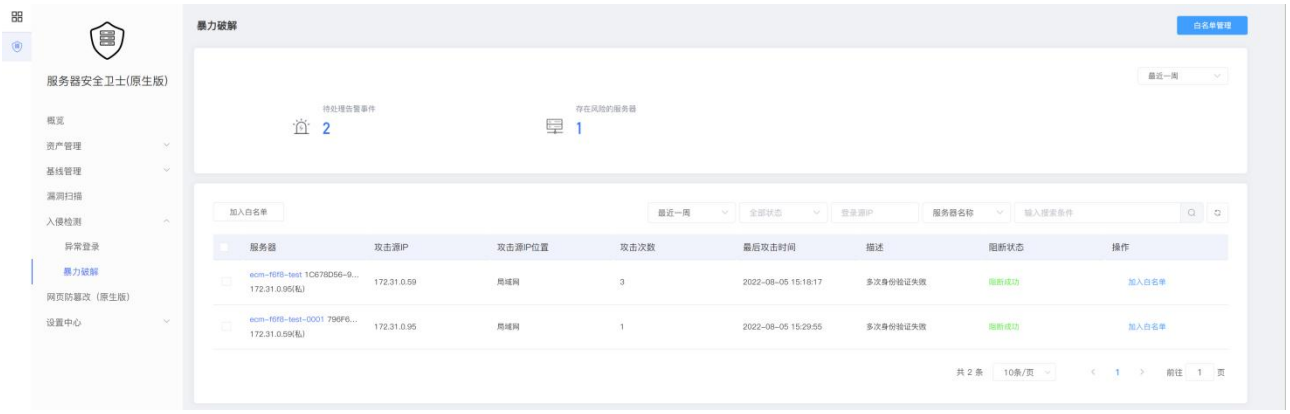


可在操作中，对该白名单规则进行编辑和删除。当点击“编辑”时，弹出如下对话框，可编辑登录IP、登录用户名、登录时间、登录地区、描述，并点击“确定”后即可完成白名单规则的编辑。



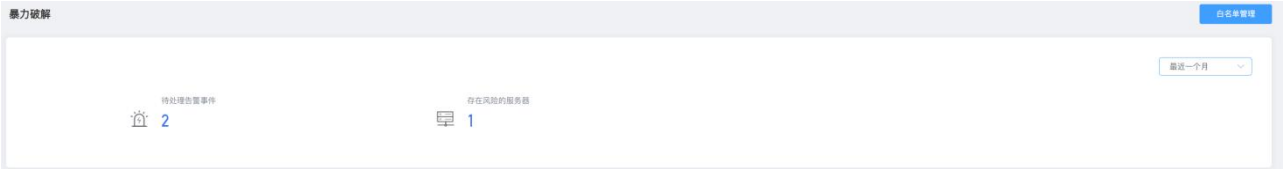
当点击操作中的“删除”时，弹出如下对话框，点击确定后，该白名单规则将被删除。

3.6.2 暴力破解



如上图所示，上方展示暴力破解事件的统计情况，下方展示暴力破解事件列表。

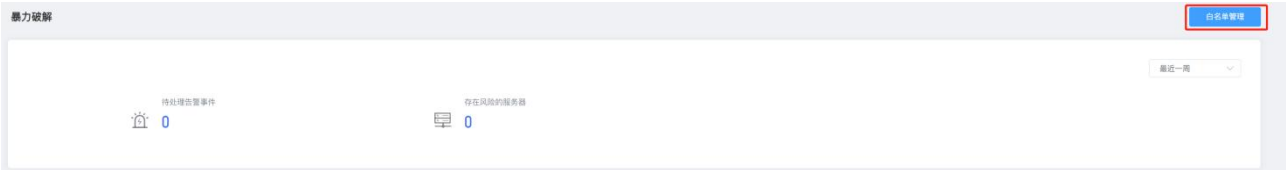
统计情况包括待处理告警事件数和存在风险的服务器数，都默认统计最近一周的时间，还可以统计最近一月和最近三月的时间维度。待处理告警事件：统计事件列表中的事件数，存在风险的服务器：统计有暴力破解事件的服务器数量，如果同一台服务器有不同的事件需要进行去重。



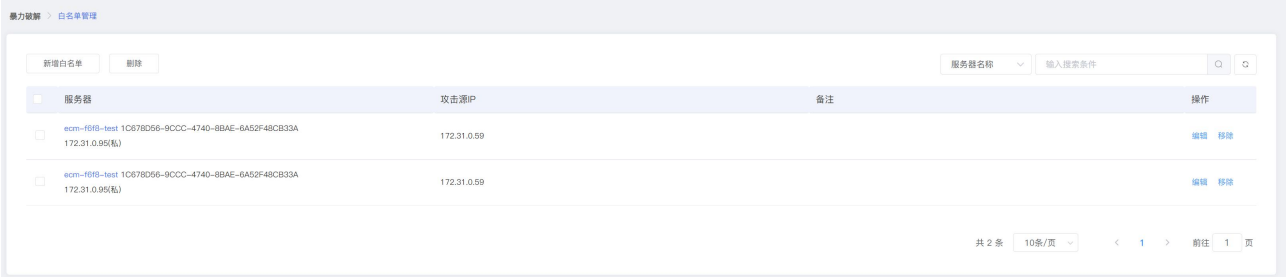
事件列表包括服务器、攻击源 IP、攻击源 IP 位置、攻击次数、最后攻击时间、描述、阻断状态和操作，默认按照最后攻击时间进行排序，最新的事件排在最上方，并默认展示一周内的事件列表。阻断状态分为阻断成功和未阻断两种情况。事件列表可按照时间、状态、攻击源 IP、服务器名称、服务器 IP 进行搜索。

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。

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：



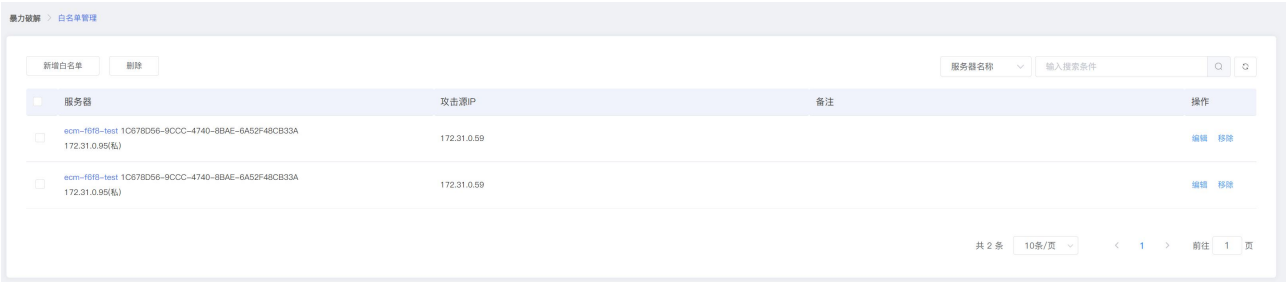
白名单管理中可对暴力破解的白名单规则进行设置，包括白名单规则的新增、编辑和删除。白名单规则列表可根据服务器名称和服务器 IP 进行搜索，若该规则中包含该台服务器，即进行显示。



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。

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：



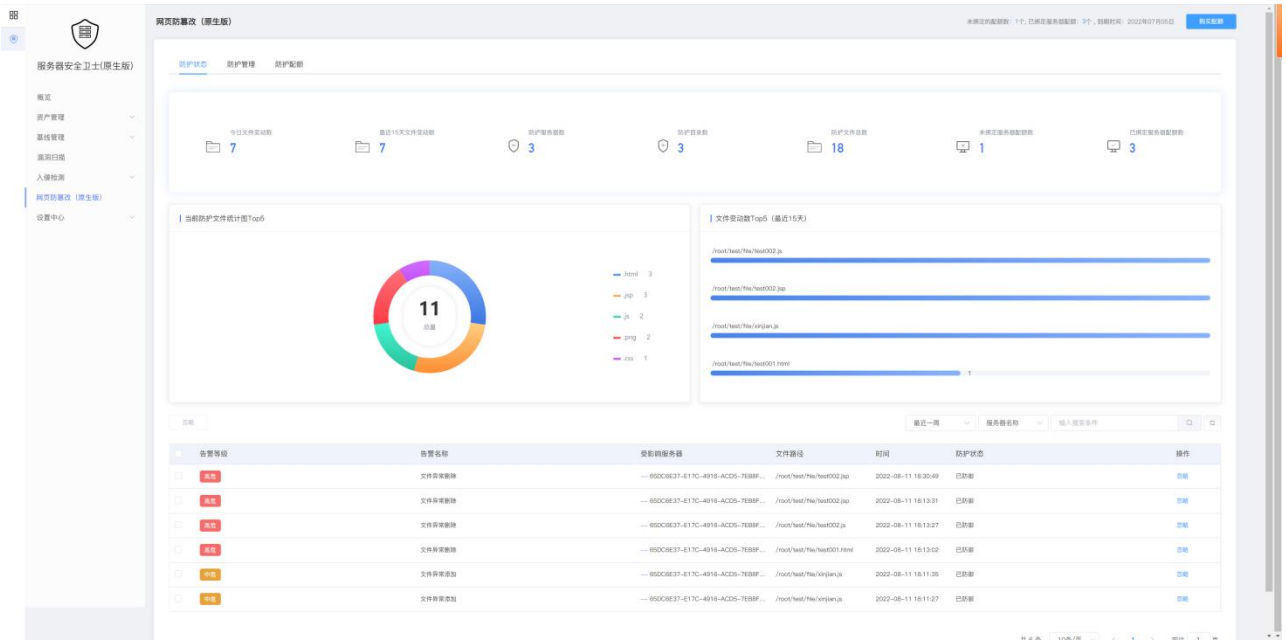
可在操作中，对该白名单规则进行编辑和删除。当点击操作中的“编辑”时，弹出如下对话框，可编辑登录 IP 和描述，点击确定后，该白名单规则编辑完成。

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。

3.7. 网页防篡改（原生版）

网页防篡改（原生版）包含防护状态、防护管理和防护配额 3 大功能模块。

3.7.1 防护状态



如上图所示，防护状态包括防护总览、防护文件状态图和告警列表。

防护总览

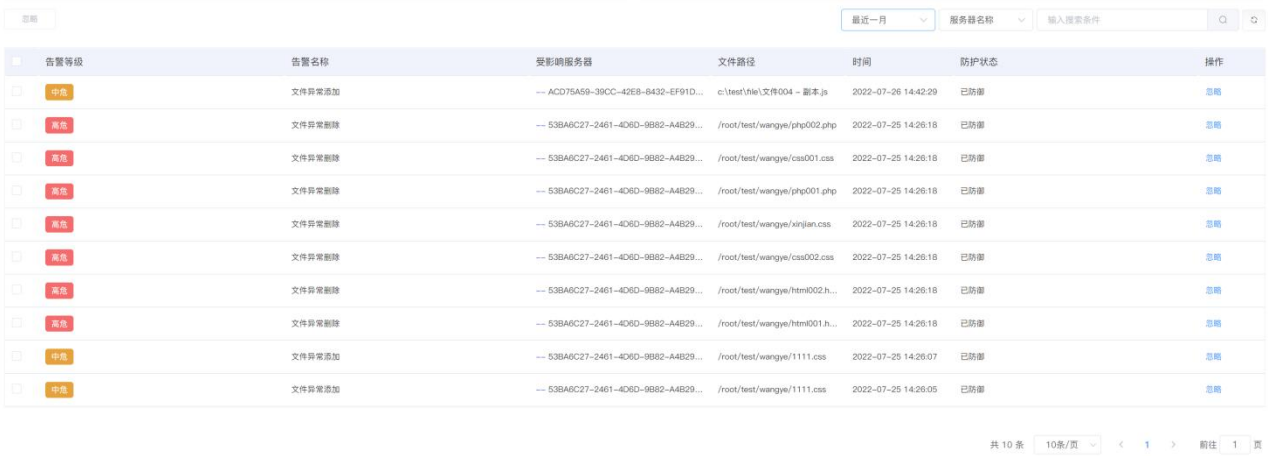
如下图所示，在防护总览中您可查看今日文件变动数、最近 15 天文件变动数、防护服务器数、防护目录数、防护文件总数和未绑定/已绑定服务器配额数。

防护文件状态图

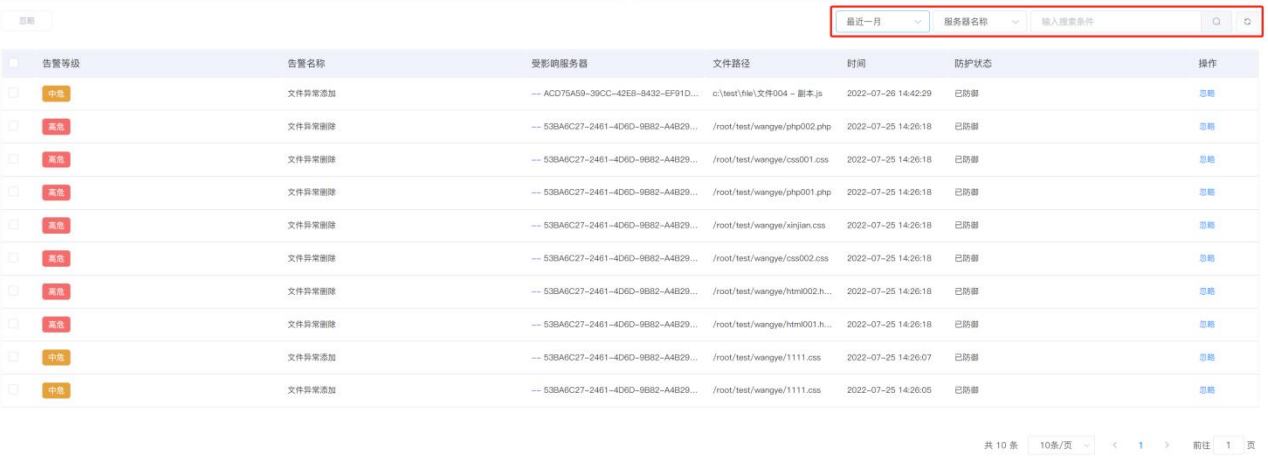
如下图所示，您可查看当前防护文件统计图 Top5（最近 15 天）和文件变动数 Top5（最近 15 天）的统计图。

告警列表

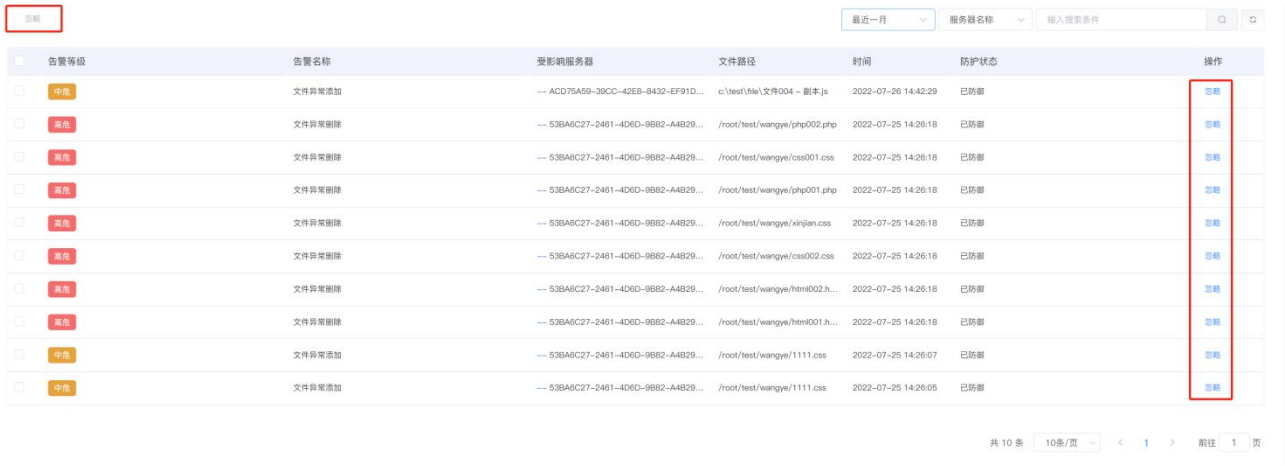
如下图所示，您可查看文件增加、删除、修改异常的告警列表，包括告警等级、告警名称、受影响服务器、文件路径、时间、防护状态和操作。告警列表默认按照时间排列，最后发生的篡改告警排列在最上方。



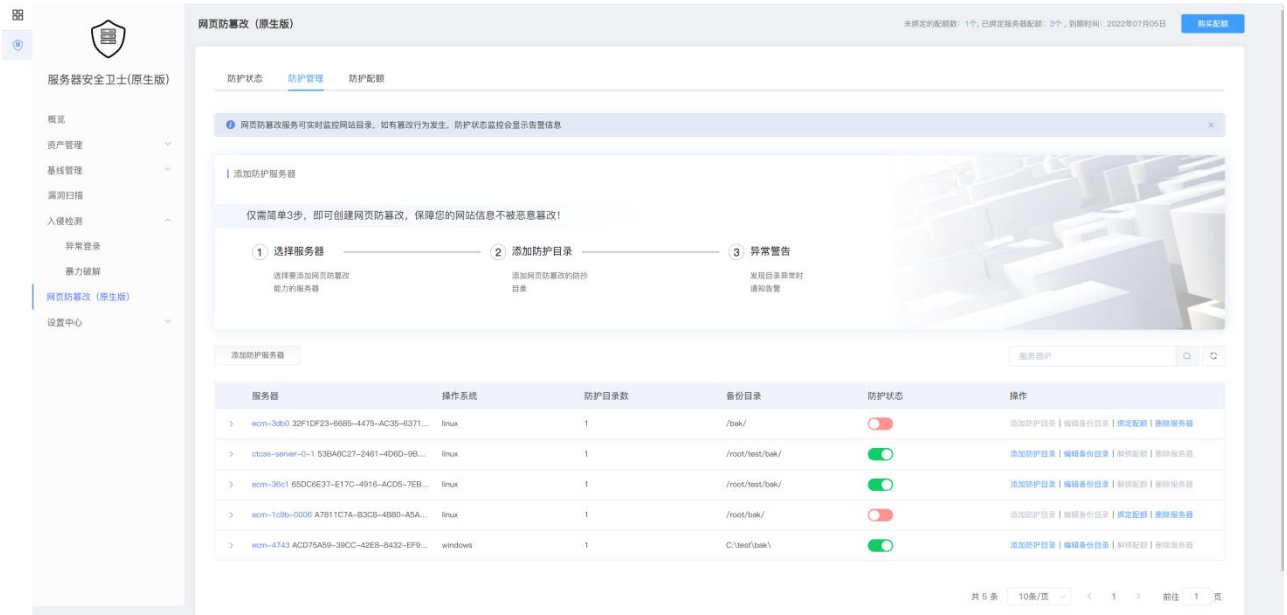
如下图所示，您可根据时间、服务器名称和服务器 IP 进行告警筛选和查询，可选时间为最近一周、最近一月和最近三月。



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：



3.7.2 防护管理



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

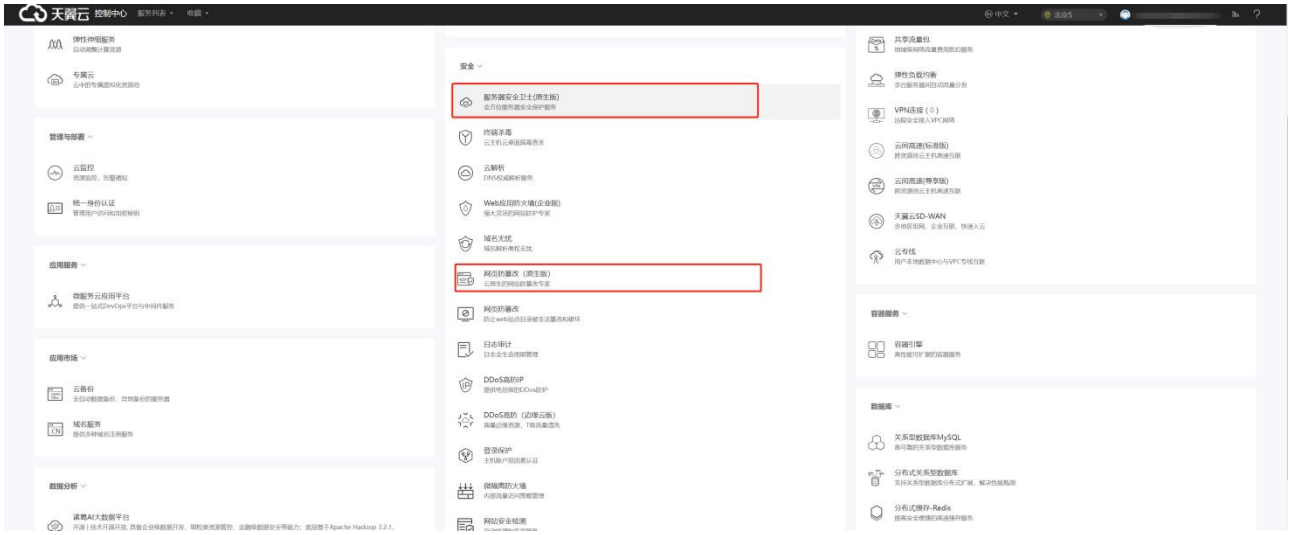
若您尚未添加过防护服务器，则参考下方创建服务器安全卫士步骤；若您已经添加过防护服务器，则参考下方添加防护服务器步骤。

创建网页防篡改

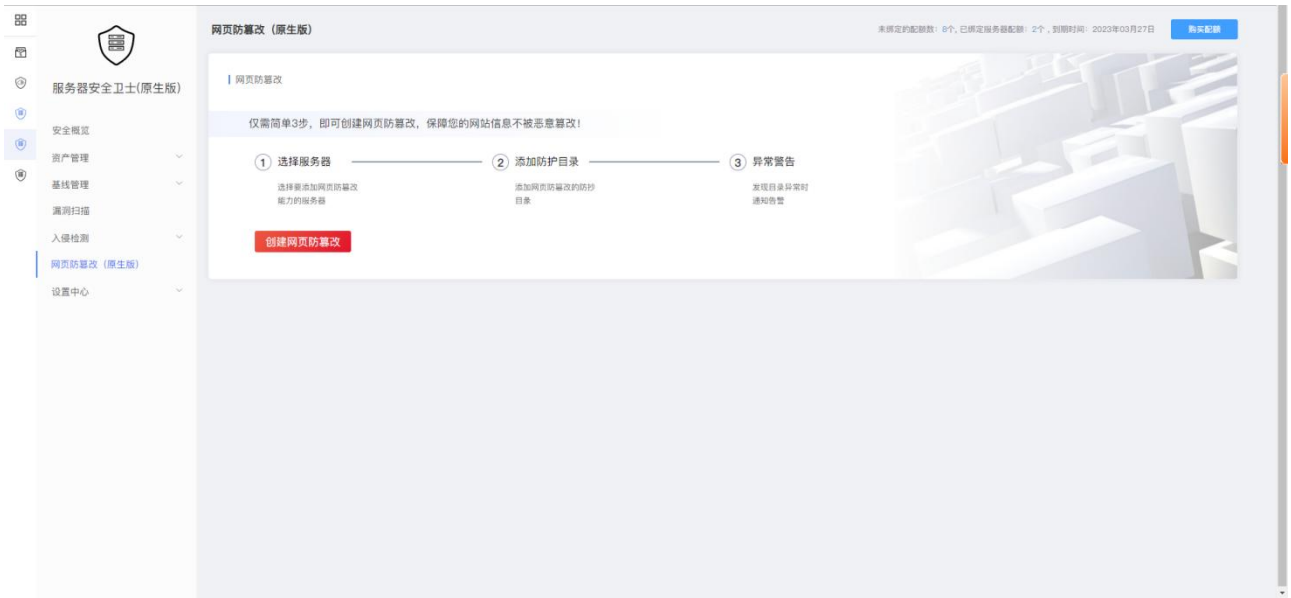
本节为您介绍在控制台创建网页防篡改（原生版）的操作步骤。

操作步骤：

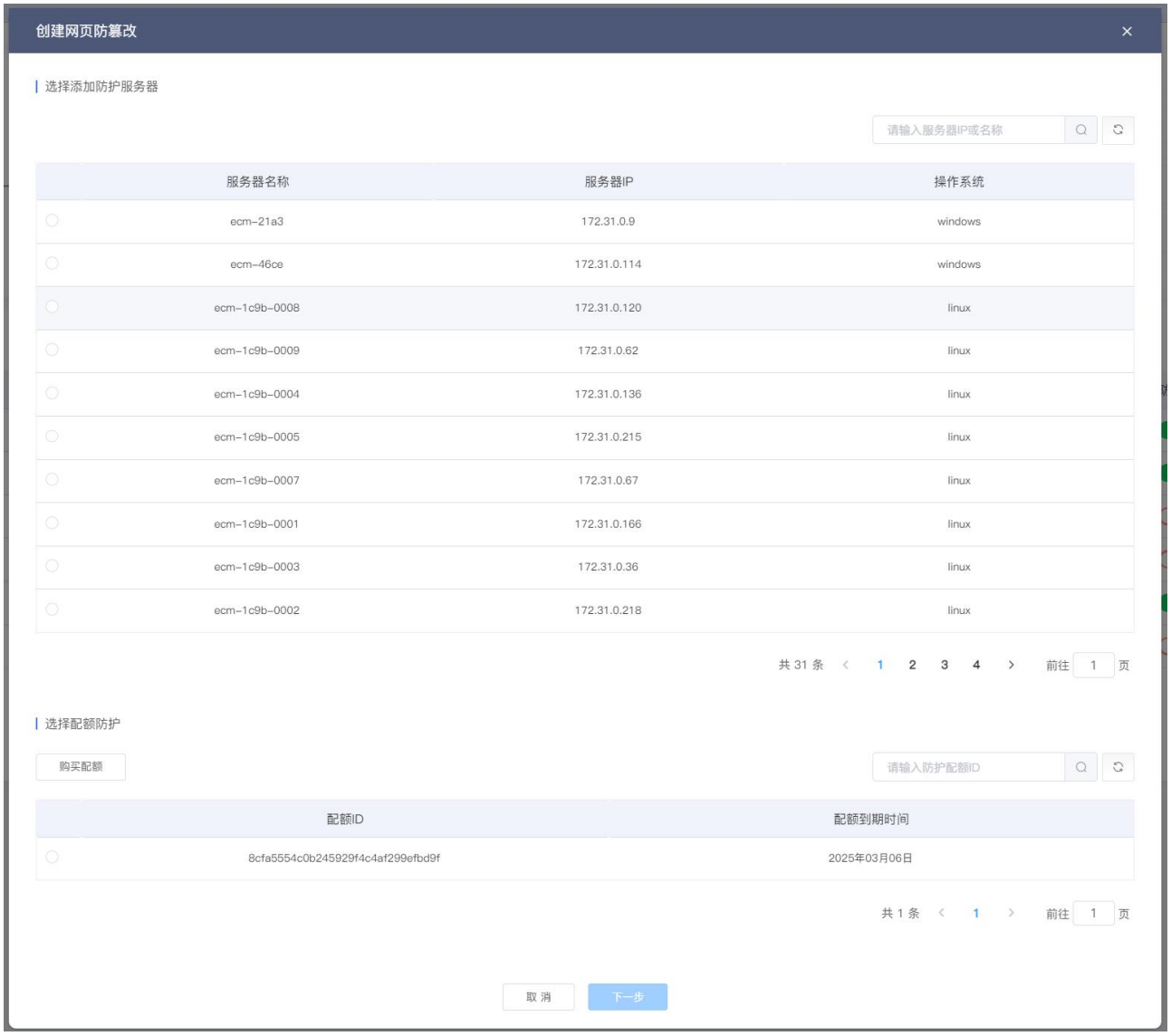
1. 在天翼云控制台中，安全分类下，点击“网页防篡改（原生版）”或“服务器安全卫士（原生版）”；



2. 当您购买网页防篡改（原生版）配额后，进入“创建网页防篡改”页面；



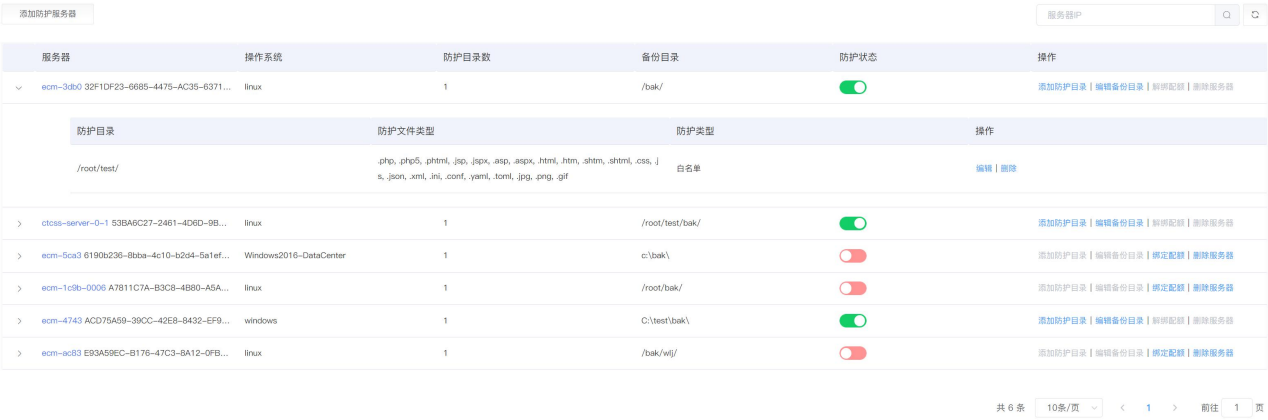
3. 单击**“创建网页防篡改”**，在弹出的创建网页防篡改对话框中，根据页面提示进行配置，配置顺序为：添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护；



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

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

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



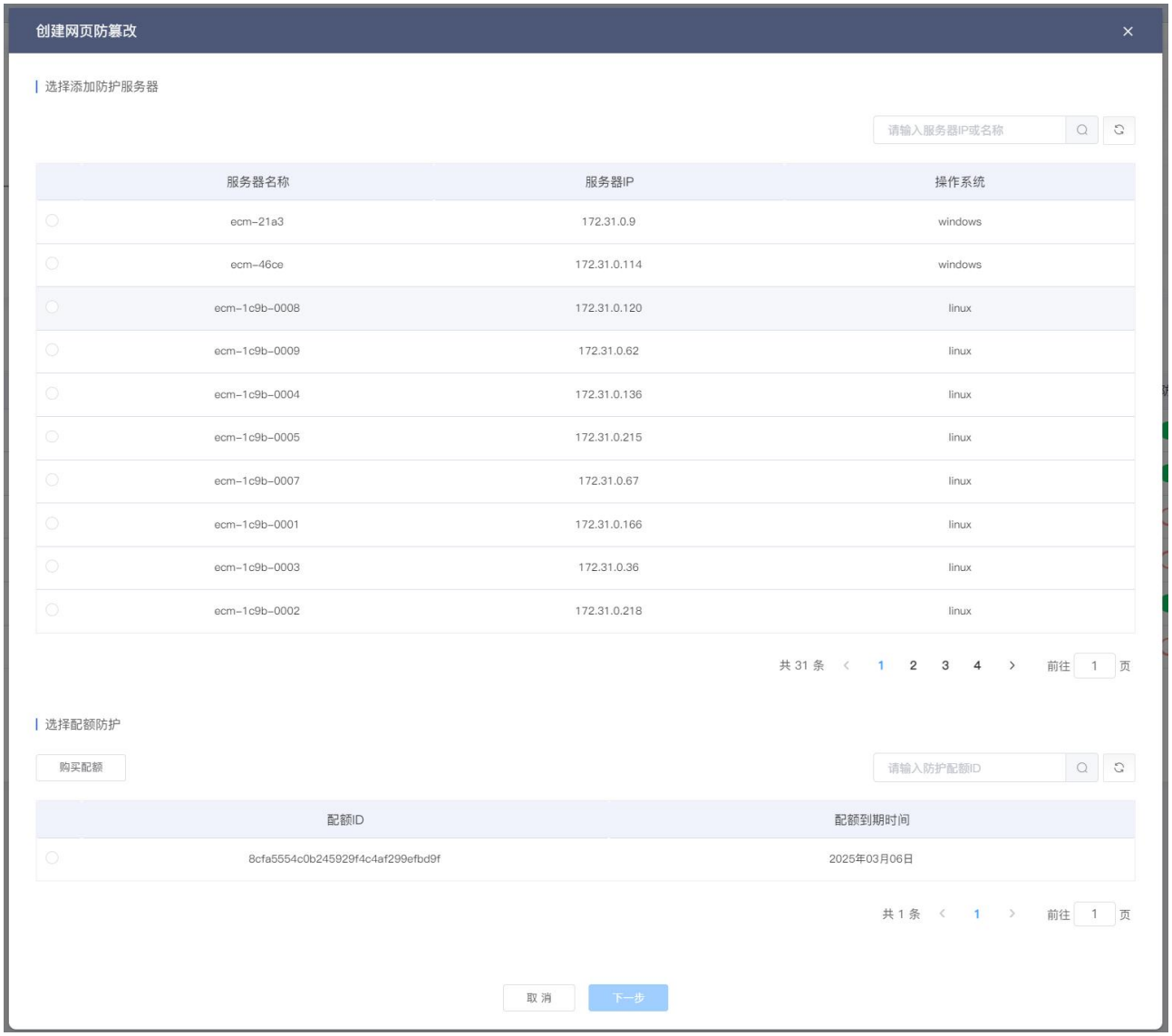
7. 开启防护后，进入防护服务器列表，展示已添加防护的服务器，以及每台服务器已配置的防护目录情况。

添加防护服务器

本节为您介绍添加防护服务器的操作步骤。

1. 点击防护管理页面的“添加防护服务器”，如下图所示：

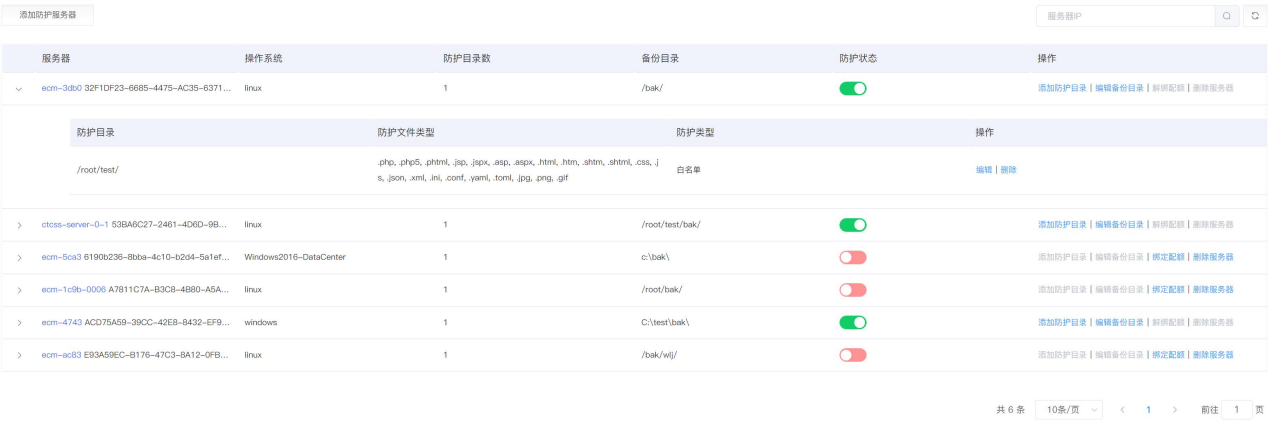
2. 在弹出的对话框中，根据页面提示进行配置，如下图所示。配置顺序为：添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护；



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

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

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

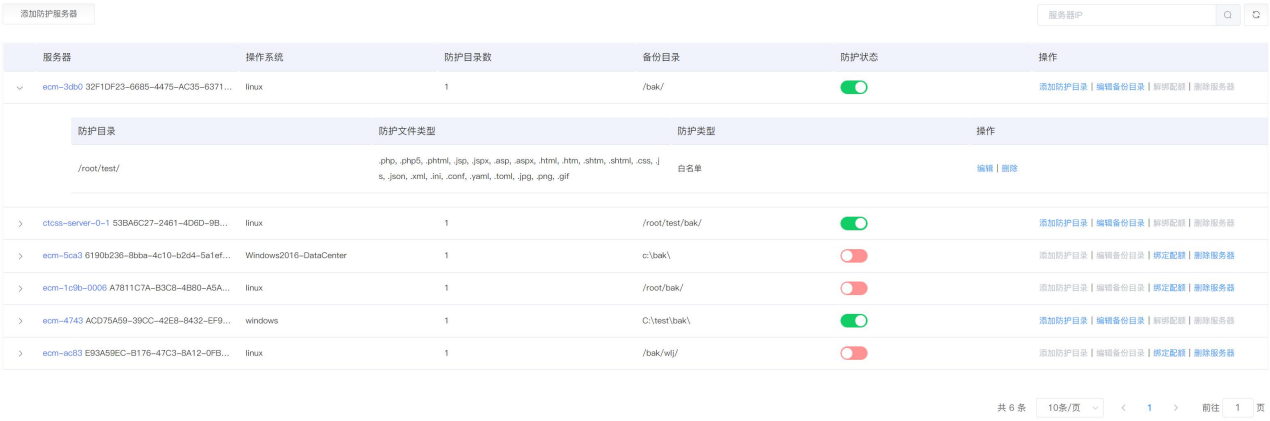


6. 如上图所示，开启防护后，进入防护服务器列表，展示已添加防护的服务器，以及每台服务器已配置的防护目录情况。

防护服务器列表

本节为您介绍已经添加的防护服务器列表。

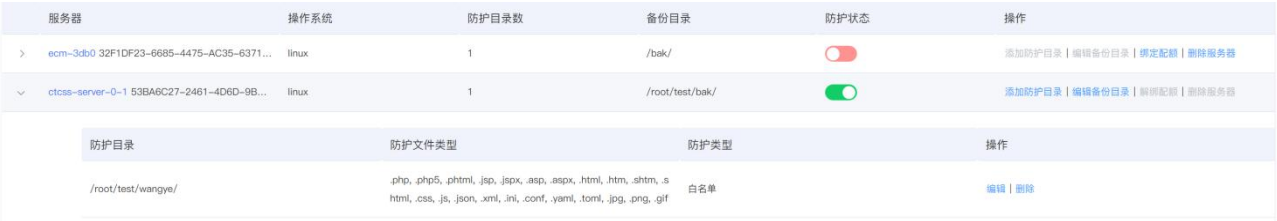
为您展示当前已添加的服务器的列表，包括添加的服务器、操作系统、防护目录数和备份目录、防护状态和操作，可以对该服务器的防护状态进行开启/关闭，并可进行添加防护目录、编辑备份目录、绑定/解绑配额和删除服务器操作。



防护目录管理

本节为您介绍已添加防护服务器的防护目录管理。

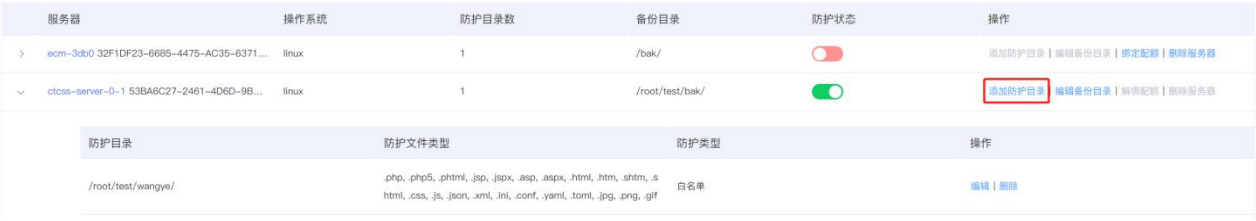
可对服务器已添加的防护目录进行编辑、删除操作，如下图所示：



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。

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。

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：



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。

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：

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：

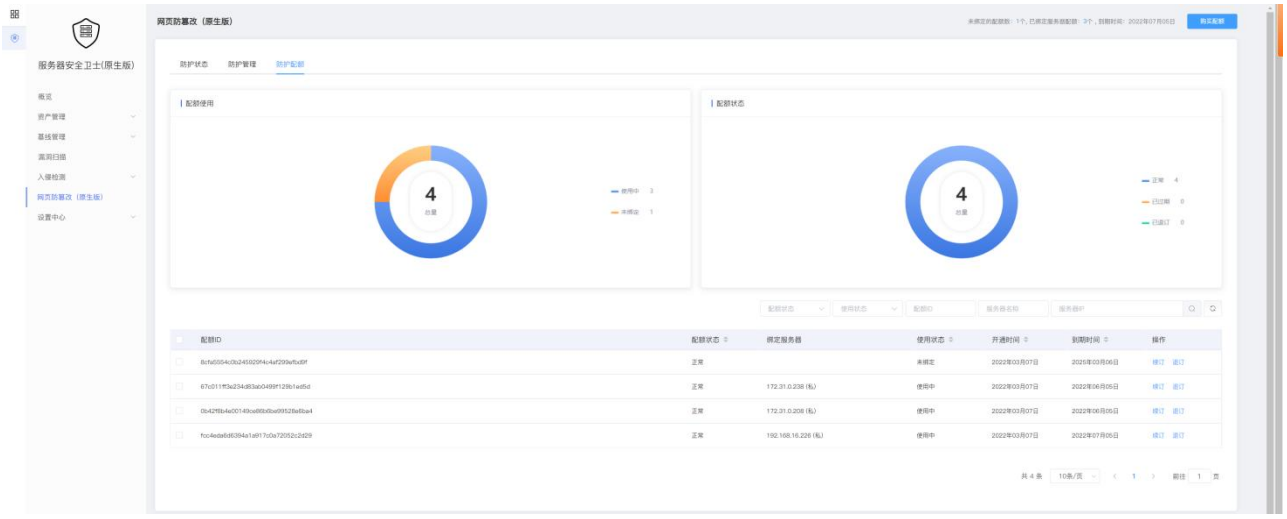
在关闭该服务器的防护后，您可以解绑该服务器的防护配额，点击“解绑配额”，如下图所示：

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。

在解绑配额完成后，可以点击“删除服务器”，如下图所示：

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。

3.7.3 防护配额



如上图所示，防护配额为您展示配额的统计和配额的详情列表。

若您未购买网页防篡改的防护配额，则展示如下页面：

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：

购买完成后，即可进入防护配额页面。

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

如上图所示，配额状态为您展示所有配额的状态统计，分为正常、已过期和已退订 3 种状态。

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

配额计费

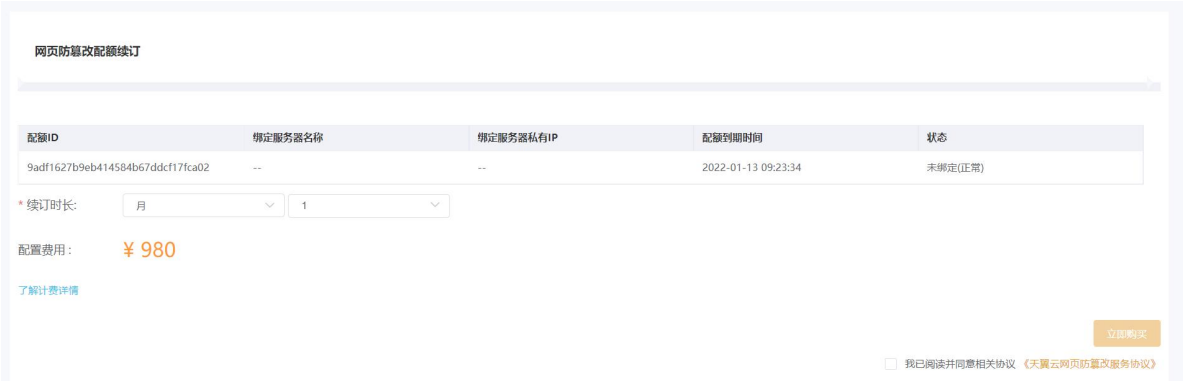
本节为您展示配额计费的相关操作，包括配额订购、配额续订、配额退订和到期处理相关操作。

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。

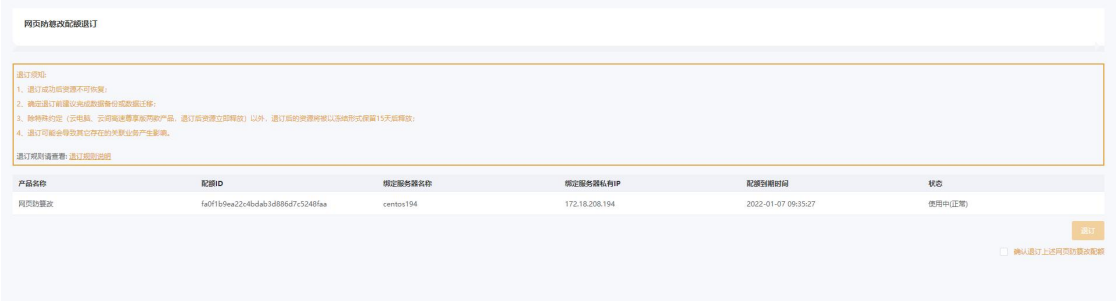
如下图所示，对需要续订的配额，点击“续订”：

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”：

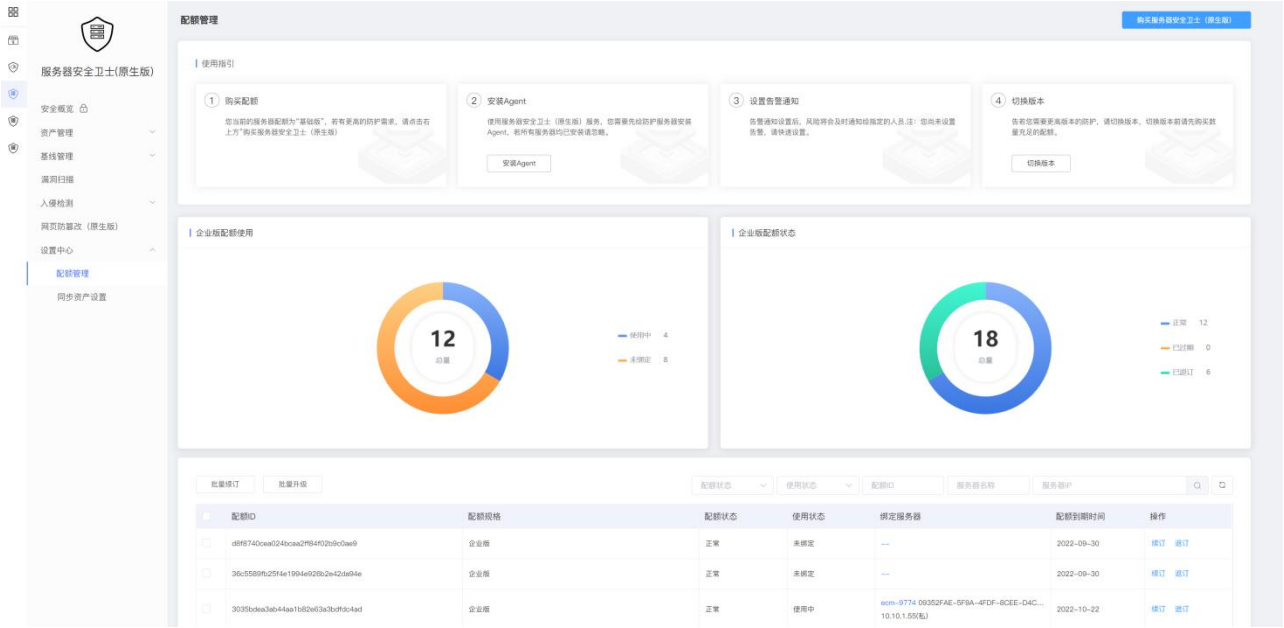
进入“退订”页面后，您需要进行确认退订的规则和金额，点击“退订”按钮，即可对该配额的网页防篡改（原生版）服务进行退订，如下图所示：



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。

3.8. 设置中心

3.8.1 配额管理



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

3.8.2 同步资产设置

如上图所示，同步资产设置为您提供了资产同步时间的设置入口。

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

4. 常见问题

4.1. 产品类

Q：服务器安全卫士（原生版）与 Web 应用防火墙（原生版）有什么区别？

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

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

Q：天翼云服务器安全卫士（原生版）都支持哪些资源池的服务器防护？

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

Q：天翼云服务器安全卫士（原生版）支持跨区域使用吗？

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

Q：什么是 Agent？

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

Q：服务器安全卫士（原生版）漏洞库多久更新一次？

A：每月一次。

4.2. 计费类

Q：服务器安全卫士（原生版）和网页防篡改（原生版）的计费方式是什么？

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

Q：服务器安全卫士（原生版）和网页防篡改（原生版）的计费项是什么？

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

Q：服务器安全卫士（原生版）和网页防篡改（原生版）的配额续费条件是什么？

A：您所需续费的配额，需要为未到期或已到期状态。

4.3. 购买类

Q：网页防篡改（原生版）可以单独购买吗？

A：网页防篡改（原生版）和服务器安全卫士（原生版）配额均可单独购买。

Q：服务器安全卫士（原生版）可以免费使用吗？

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

Q：服务器安全卫士（原生版）可以按天购买吗？

A：不支持，目前只支持包月和包年购买。

4.4. 操作类

Q：服务器的防护状态显示“已离线”要如何解决?

A：建议重新“安装 Agent”。

Q：服务器显示登录异常怎么解决？

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

Q：正常登录行为被误报为异常登录，要如何消除误报？

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

Q：如何减少服务器被爆破登录的风险？

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

Q：如何使用网页防篡改（原生版）？

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

Q：网页防篡改（原生版）添加防护服务器的步骤是什么？

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

4.5. 系统类

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

Q：用户配置的网页防篡改防护策略有什么限制？

A：Linux 系统单个防护目录大小不超过 2G。

Q：安装 agent 会不会对自身的业务稳定性产生影响？

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