网页防篡改（原生版）

用户使用指南

天翼云科技有限公司

目 录

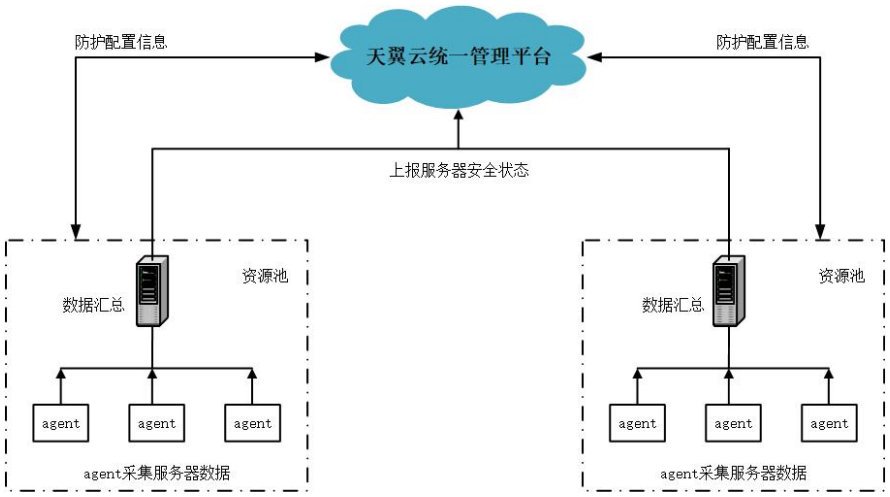
1. 产品介绍

1.1. 产品定义

天翼云网页防篡改（原生版）产品（CT-WT，WebpageTampering）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。

网页防篡改（原生版）整体架构主要包括 3 个部分，分别为天翼云统一管理平台、资源池数据汇总节点和服务器客户端 Agent。

- 天翼云统一管理平台：客户通过统一的天翼云统一管理平台，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，上报给相应的资源池数据汇总节点。
- 服务器客户端 Agent：使用天翼云服务器安全卫士（基础版）产品时，每台服务器客户端需安装一个 Agent。



1.2. 产品功能

天翼云网页防篡改（原生版）产品通过 Agent 进行自动化采集，获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常变动进行告警和恢复。网页防篡改（原生版）产品主要包括以下 4 个功能：

- 篡改监测：针对云主机或物理机防护目录下的异常文件变动进行实时监测；
- 篡改告警：一旦发生异常的文件添加、修改和删除，立即进行客户告警；
- 文件备份：对云主机或物理机防护目录下的目录和文件，系统进行备份；
- 自动恢复：当防护文件发生异常的增删改问题时，通过备份进行实时恢复，保障客户系统的网站信息不被恶意篡改。

1.3. 产品优势

- 方便易用

只需在 Web 服务器一键安装 Agent，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。

- 灵活配置

防护策略支持自定义配置，按需指定防护的进程和文件类型，支持各类网站文件的保护。

- 安全可靠

产品实现自我保护机制，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 99.998%，2 分钟内离线自动重启机制，保障系统始终处于检测状态。

- 节约资源

正常的系统负载情况下，CPU 占用率 <1%，内存占用 <40M，消耗极低 。在系统负载过高时，Agent 会主动降级运行（CPU 占用率 <1%），严格限制对系统资源的占用，确保业务系统正常运行。

1.4. 术语说明

- Agent：是服务器安全卫士（基础版）部署到用户云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云端防护中心的指令，实现对云服务器上的安全威胁清除和恶意攻击拦截。
- 白名单模式：是一种防护配置模式。在白名单模式下，会对添加的防护目录和文件类型进行保护。
- 黑名单模式：是一种防护配置模式。在黑名单模式下，会防护目录下所有未排除的子目录、文件类型和指定文件。

1.5. 应用场景

天翼云网页防篡改（原生版）产品（CT-WT，WebpageTampering）具有广泛的应用场景，以下是三种常见的应用场景。

- 场景一：网站实时监管

政府、金融、交通等行业需要对网站进行实时监测，防止网站被植入涉恐、涉政、暗链、后门等，否则一旦网站出现被篡改问题，会严重影响政府、交通等单位形象，造成企业巨大损失。

- 场景二：重大活动保障

在重大活动保障期间，各行业的官网、业务系统等网站出现非法关键词，导致被监管单位通报，其声誉将受到影响，评分会受到严重影响。

- 场景三：等保合规

信息安全等级保护是我国信息安全保障的一项基本制度，要求网络经营者应符合网络安全等级保护制度的要求。天翼云网页防篡改（原生版）帮助有等保需求的用户，进行安全测评，满足等保合规的要求。

1.6. 产品使用限制

支持的服务器

- 天翼云弹性云主机
- 天翼云 GPU 云主机
- 天翼云物理机

支持的系统

天翼云服务器安全卫士（原生版）产品支持对如下操作系统的服务器进行防护：

类型	架构	芯片	操作系统	系统版本
Windows	x86	Intel	Windows Server	Windows Server 2012 R2 标准版（简体中文）64 位
				Windows Server 2012 R2 数据中心版（简体中文）64 位
				Windows Server 2016 标准版（简体中文）64 位
				Windows Server 2016 数据中心版（简体中文）64 位

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

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

使用条件

每台服务器客户端需安装一个 Agent，且服务器需不低于 2C4G。

1.7. 支持的资源池

一类节点

支持的一类节点区域如下：

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

资源池大区	资源池名称
国际地区	香港 1

二类节点

支持的二类节点区域如下：

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

1.8. 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，可以帮助您安全地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，您只需要为您账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

网页防篡改（原生版）产品提供包年包月计费方式。

标准资费

网页防篡改（原生版）产品的具体价格如下：

计费项	计费单位	标准资费
网页防篡改（原生版）	元/个/月	980

优惠活动

- 针对一次性包年付费服务，网页防篡改（原生版）的优惠政策为：1 年 85 折、2 年 7 折、3 年 5 折。
- 针对购买服务器安全卫士、终端杀毒、网页防篡改的存量用户，若订购网页防篡改（原生版）产品，可享受 7 折优惠。

以上优惠活动不能同享，取低者计算。

2.2. 续订

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

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

4. 在“续订”页面选择该配额需续订的时长。

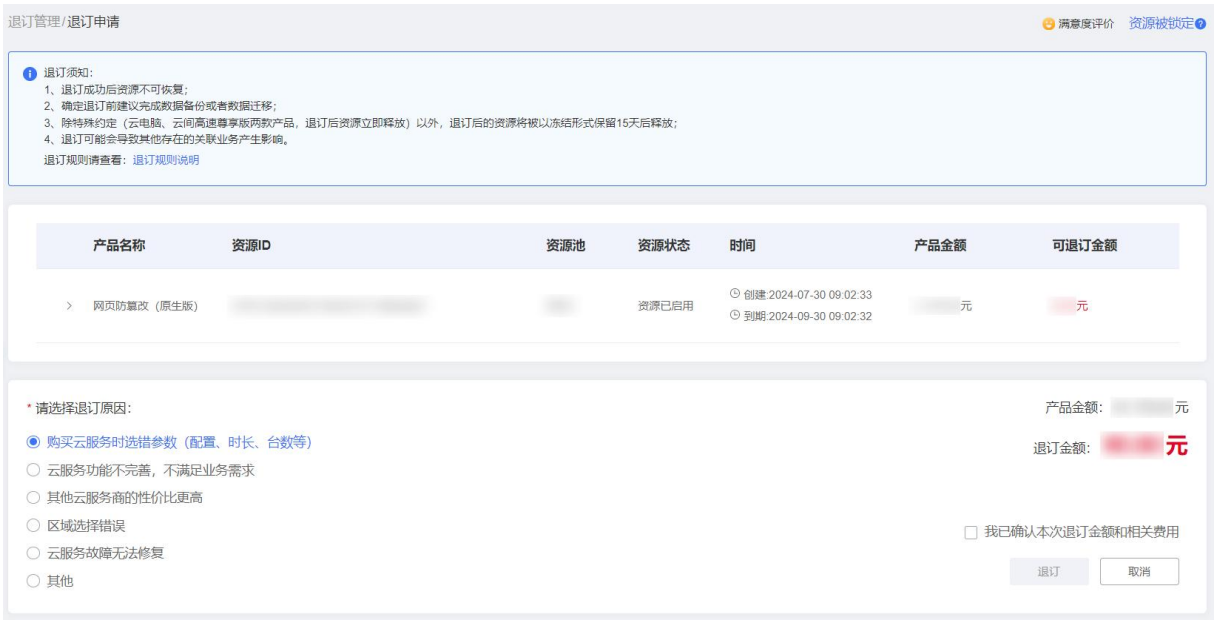
5. 阅读《天翼云网页防篡改（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云网页防篡改（原生版）服务协议》“，单击“立即购买”。
6. 进入“付款”页面，完成付款。

2.3. 退订

根据您的需求，可对正常状态的配额进行退订，遵循天翼云统一的退订规则。

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

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


退订管理/退订申请
满意度评价
资源被锁定
退订须知：
1、退订成功后资源不可恢复；
2、确定退订前建议完成数据备份或者数据迁移；
3、除特殊约定（云电脑、云间高速尊享版两款产品，退订后资源立即释放）以外，退订后的资源将被以冻结形式保留15天后释放；
4、退订可能会导致其他存在的关联业务产生影响。
退订规则请查看：退订规则说明
产品名称
资源ID
资源池
资源状态
时间
产品金额
可退订金额
网页防篡改（原生版）
资源已启用
创建:2024-07-30 09:02:33
到期:2024-09-30 09:02:32
元
元
* 请选择退订原因：
产品金额：
元
购买云服务时选错参数（配置、时长、台数等）
退订金额：
元
云服务功能不完善，不满足业务需求
其他云服务商的性价比更高
区域选择错误
云服务故障无法修复
其他
我已确认本次退订金额和相关费用
退订
取消

3. 快速入门

3.1. 开通网页防篡改（原生版）

网页防篡改功能为付费的增值服务，需要单独购买。

首次使用网页防篡改功能时，请按如下步骤开通网页防篡改功能。

操作步骤

1. 登录网页防篡改（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改 > 防护状态”，在页面右上角单击“购买配额”。

   首次使用网页防篡改功能时，进入如下页面，单击“立即升级”。

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

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

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

5. 进入“付款”页面，完成付款。

   购买完成后，即可进入防护配额页面，查看已购买的配额。

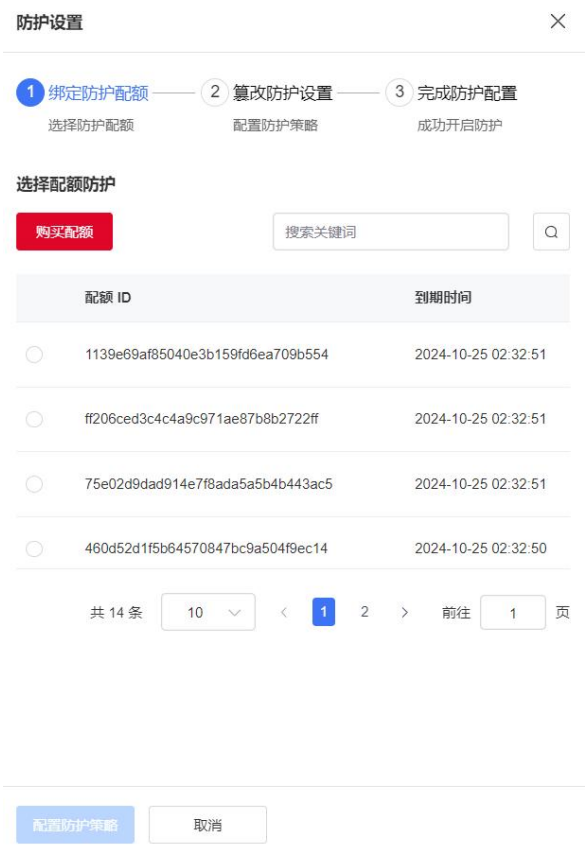
3.2. 创建网页防篡改（原生版）

3.2.1 防护设置

1. 登录服务器安全卫士（原生版）控制台。

2. 在左侧导航栏，选择“网页防篡改（原生版） > 防护管理”，进入防护管理页面。

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



4. 绑定防护配额：选择需要绑定的配额后，单击“配置防护策略”。

5. 篡改防护设置：包括配置防护目录、设置特权进程、设置远端备份。

   - 配置防护目录：可对服务器的防护目录进行管理，包括添加、编辑、删除操作。
   - 设置特权进程：特权进程为您信任的进程文件，可以对防护目录文件进行修改操作。
   - 设置远端备份：启用远端服务器备份功能后，可有效避免备份在本地的文件被攻击者破坏后无法恢复。

6. 配置完成后，单击“完成防护配置”，回到服务器列表页面。

3.2.2配置防护目录

分为添加白名单或添加黑名单两种模式，可根据实际使用场景进行配置。

- 白名单模式：会对添加的防护目录和文件类型进行保护。

- 黑名单模式：会防护目录下所有未排除的子目录、文件类型和指定文件。

说明：

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

白名单模式

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

黑名单模式

黑名单模式支持添加防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，配置完成后，即开始防护目录下所有未排除的子目录、文件类型和指定文件。

设置特权进程

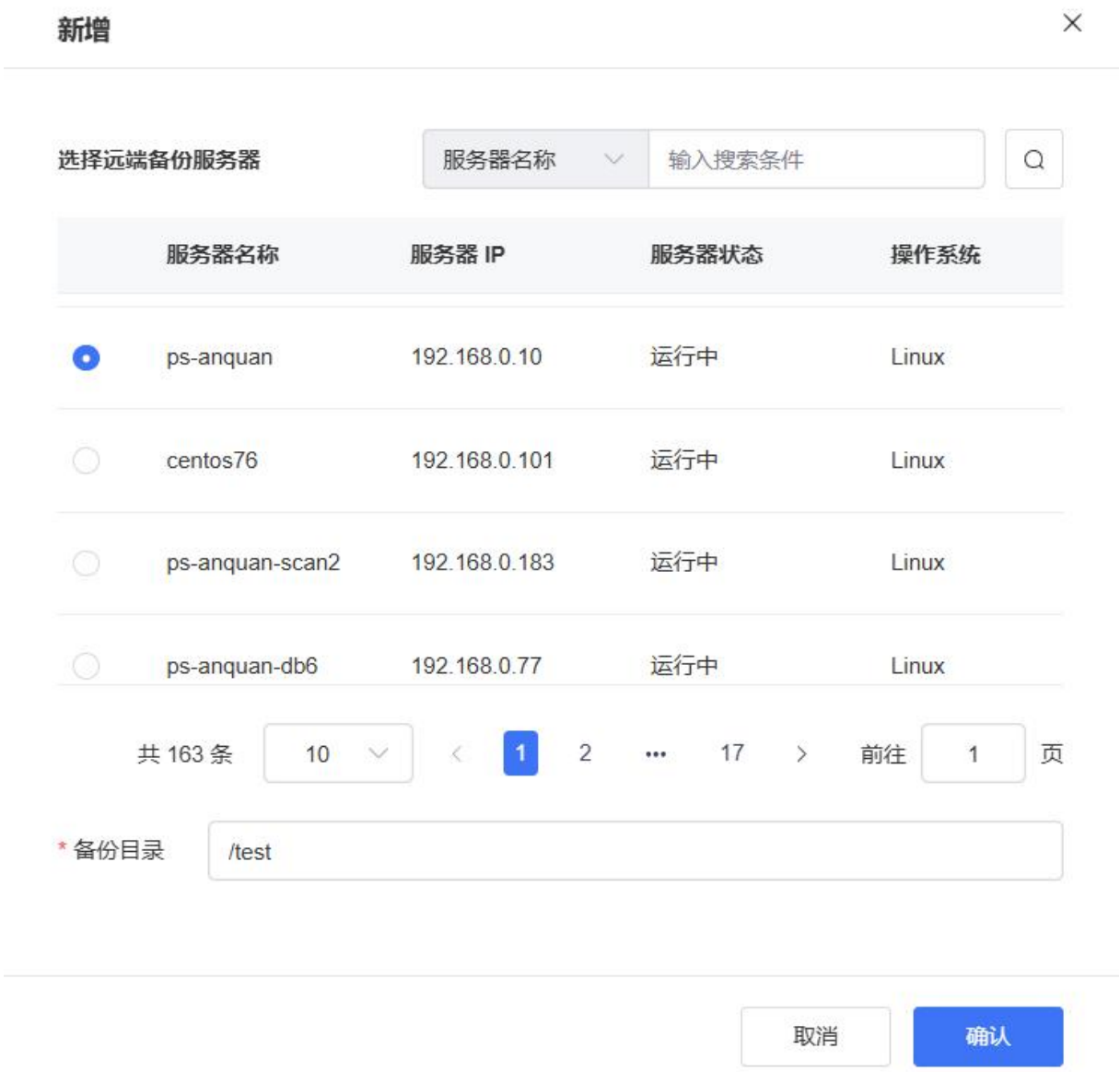
特权进程拥有对防护目录进行操作的权限，请确保特权进程安全可靠。

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

设置远端备份

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

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



开启防护

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

4. 用户指南

4.1. 概述

天翼云网页防篡改（原生版）产品通过 Agent 进行自动化采集，获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常变动进行告警和恢复。

支持的系统

支持 64 位的 linux 和 windows 系统下文件的防篡改，详情见“产品介绍 > 产品使用限制”。

防护状态

可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。

功能	说明
防护总览	● 查看今日文件变动数 ● 查看最近 15 天文件变动数 ● 查看防护服务器数 ● 查看防护目录数 ● 查看防护文件总数 ● 查看未绑定/已绑定服务器配额数
防护文件状态图	● 查看防护文件类型分布（最近 15 天）统计图 ● 查看文件变动数 Top5（最近 15 天）统计图
告警列表	● 展示文件增加、删除、修改异常的告警列表
告警查询	● 根据时间、服务器 IP 和告警名称进行告警筛选和查询
告警忽略	● 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

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。

功能	说明
创建网页防篡改（原生版）	● 适用于首次订购后创建网页防篡改（原生版）
添加防护服务器	● 适用于非首次订购，对需防护的服务器添加防护策略
防护服务器列表	● 显示防篡改实例服务器列表 ● 变更防护状态：开启/关闭 ● 添加防护目录 ● 编辑备份目录 ● 解绑配额 ● 绑定配额
防护目录管理	● 显示服务器防护目录列表 ● 编辑防护目录设置 ● 删除防护目录

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。

功能	说明
配额使用统计	● 正常配额的使用统计
配额状态统计	● 所有配额的状态统计
配额列表	● 展示配额情况的列表，包括配额 ID、配额状态、绑定服务器、使用状态、配额到期时间和操作
配额计费	● 配额订购 ● 配额续订 ● 配额退订 ● 到期处理

4.2. 购买网页防篡改配额

网页防篡改功能为付费的增值服务，需要单独购买。

操作步骤

1. 登录网页防篡改（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改 > 防护状态”，在页面右上角单击“购买配额”。

   首次使用网页防篡改功能时，进入如下页面，单击“立即升级”。

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

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

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

   购买完成后，即可进入防护配额页面，查看已购买的配额。

4.3. 防护状态

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

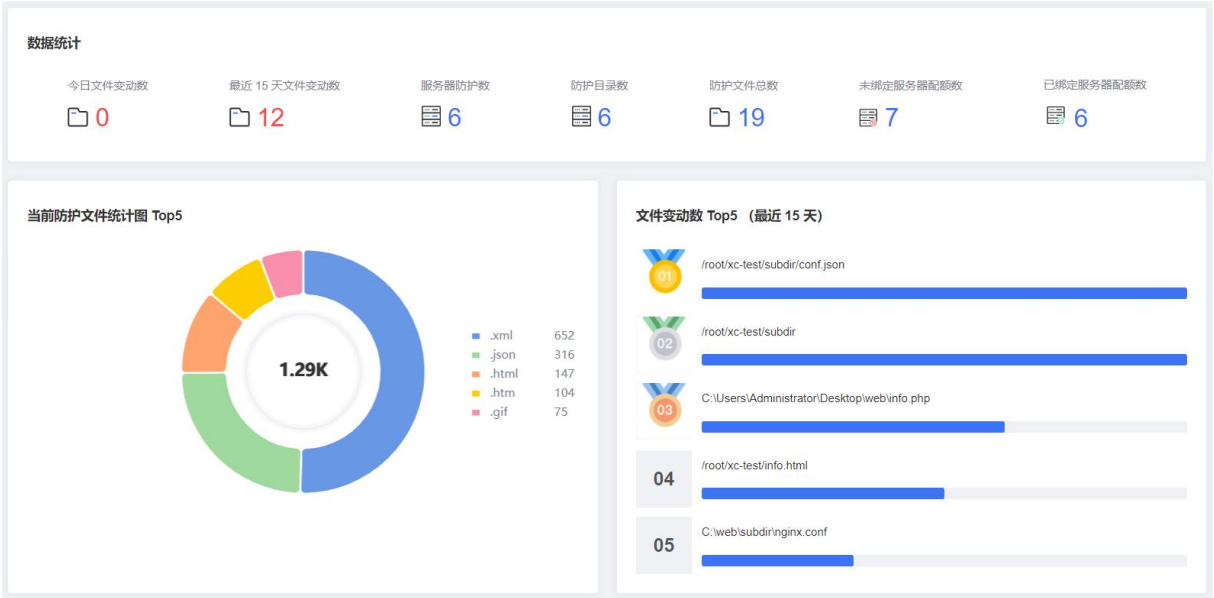
操作步骤

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

防护数据统计

数据统计：您可查看今日文件变动数、最近 15 天文件变动数、防护服务器数、防护目录数、防护文件总数和未绑定/已绑定服务器配额数。

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



告警列表

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

告警列表默认按照时间排列，最后发生的篡改告警排列在最上方。

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

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

4. 4. 防护管理

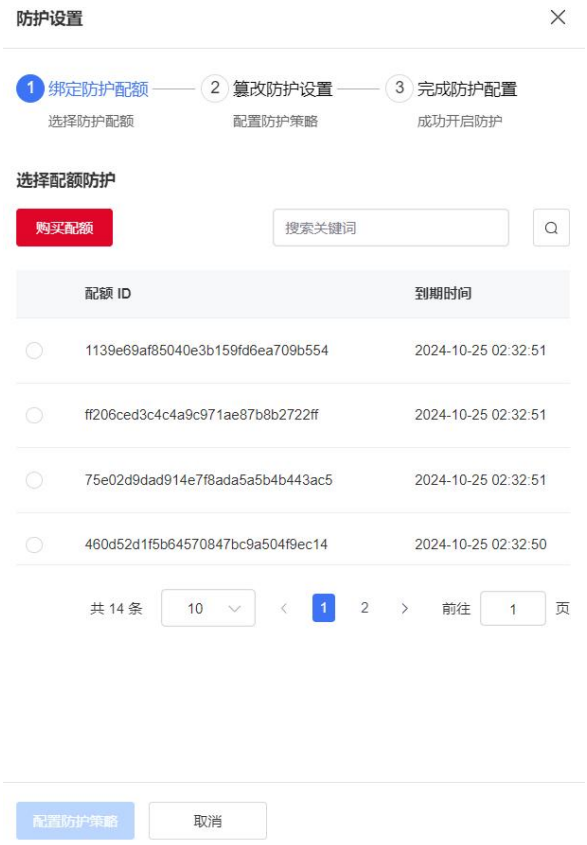
防护管理列表展示用户的服务器列表，包括服务器、操作系统、防护目录数、备份目录、防护配置状态、防护状态。

在防护管理页面，您可以为服务器开启网页防篡改防护，并配置防护目录。

4. 4. 1 防护设置

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

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



4. 绑定防护配额：选择需要绑定的配额后，单击“配置防护策略”。

5. 篡改防护设置：包括配置防护目录、设置特权进程、设置远端备份。

   - 配置防护目录：可对服务器的防护目录进行管理，包括添加、编辑、删除操作。
   - 设置特权进程：特权进程为您信任的进程文件，可以对防护目录文件进行修改操作。

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

6. 配置完成后，单击“完成防护配置”，回到服务器列表页面。

配置防护目录

分为添加白名单或添加黑名单两种模式，可根据实际使用场景进行配置。

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

说明：

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

白名单模式

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

黑名单模式

黑名单模式支持添加防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，配置完成后，即开始防护目录下所有未排除的子目录、文件类型和指定文件。


篡改防护设置
绑定防护配额
选择防护配额
2 篡改防护设置
配置防护策略
3 完成防护配置
成功开启防护
建议您使用白名单模式，在该模式下，会对添加的防护目录和文件类型进行保护。黑名单模式下，会防护目录下所有 未排除的子目录、文件类型和指定件。每台服务器最多可添加 10 个防护目录；每个被防护的目录大小不超过 10 GB; 所有被防护的目录下的文件夹个数不超过 3000 个。
白名单模式
黑名单模式
* 防护目录
+添加
防护目录
防护文件类型
操作
/root/large
.log
编辑 | 删除
* 排除子目录
+添加
排除子目录
操作
/xxx
删除
* 排除指定文件
+添加
排除指定文件
操作
/pp
删除
* 本地备份目录
/root/bak

设置特权进程

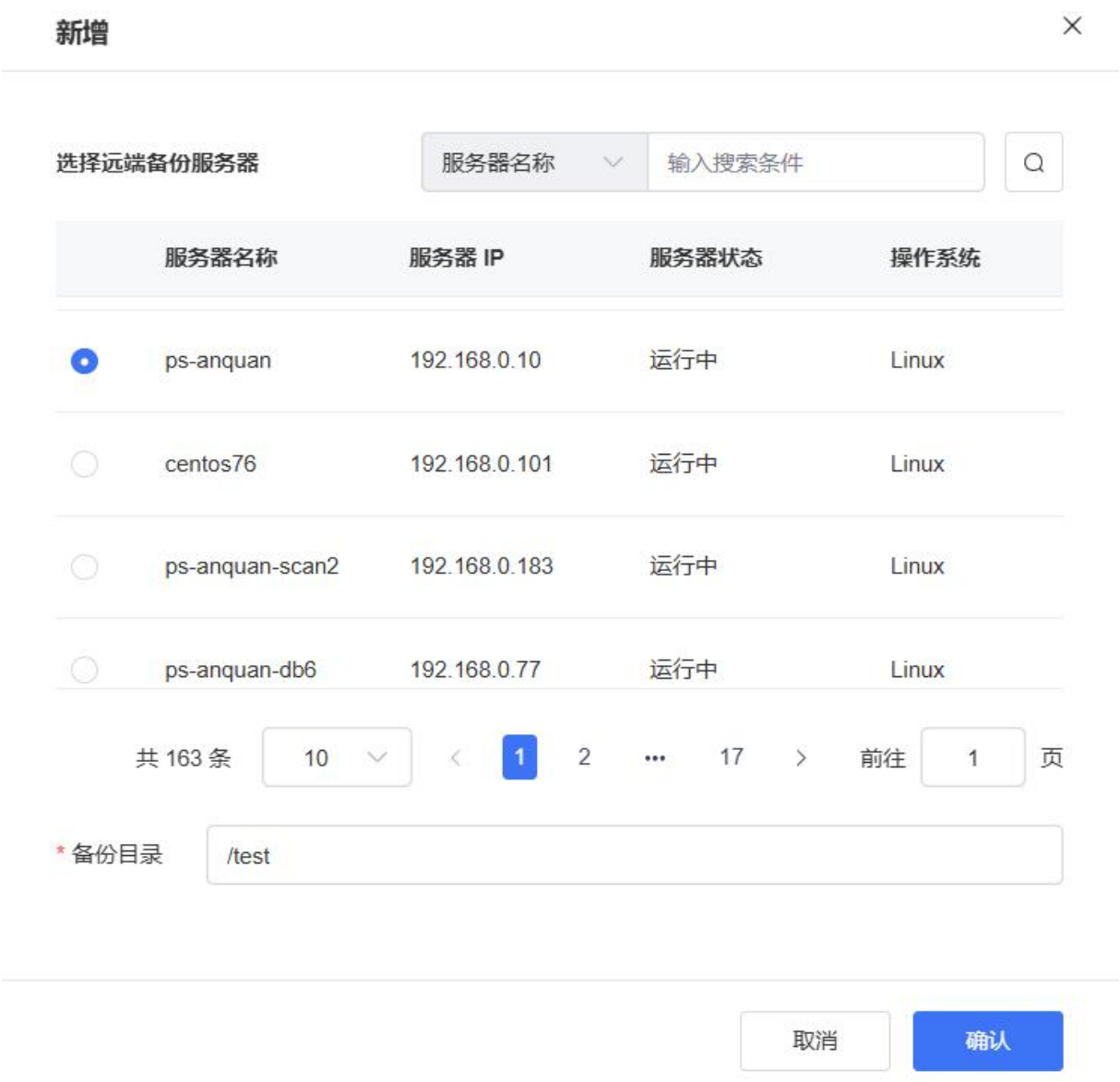
特权进程拥有对防护目录进行操作的权限，请确保特权进程安全可靠。

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

设置远端备份

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

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



4.4.2开启防护

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

4.4.3关闭防护

若您某台服务器不再需要网页防篡改防护，可以关闭防护。

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

4.4.4解绑配额

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

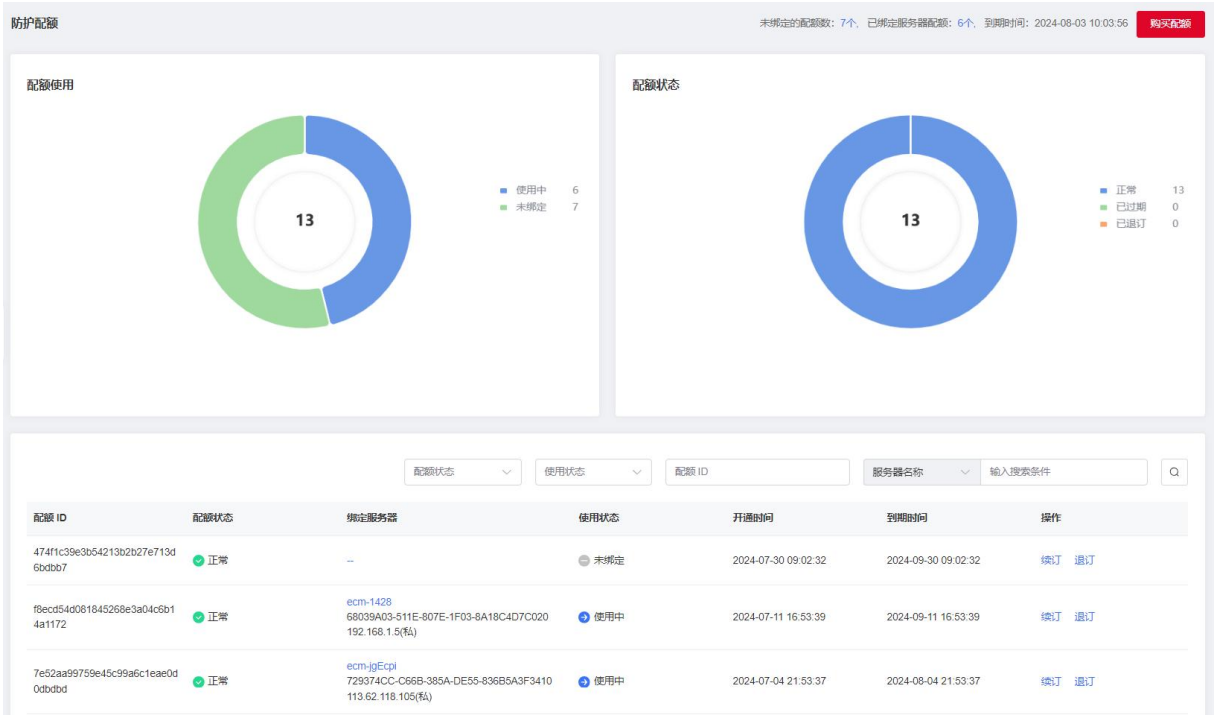
4.5. 防护配额

4.5.1查看配额详情

1. 登录网页防篡改（原生版）控制台。

2. 在左侧导航栏，选择“网页防篡改（原生版）>防护配额”，进入防护配额页面。

   该页面为您展示配额的统计和配额的详情列表。



- 配额使用：为您展示正常配额的使用情况统计，分为使用中和未绑定 2 种状态。
- 配额状态：为您展示所有配额的状态统计，分为正常、已过期和已退订 3 种状态。
- 配额列表：展示正常、已过期、已退订 3 种状态的配额，销毁的配额不展示在列表中，包括配额 ID、配额状态、绑定服务器、使用状态、开通时间、到期时间等信息。

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

4.5.2 管理配额

包括配额订购、配额续订、配额退订和到期处理相关操作。

配额订购

详细操作请参见“购买网页防篡改配额”。

配额续订

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

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

4. 在“续订”页面选择该配额需续订的时长。

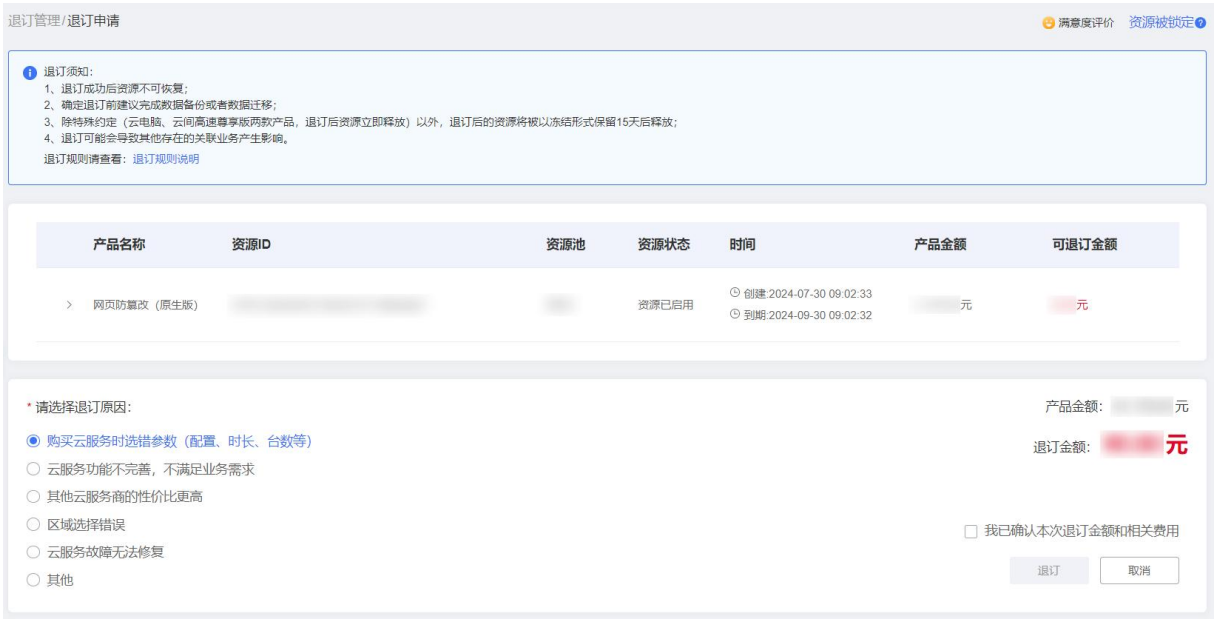
5. 阅读《天翼云网页防篡改（原生版）服务协议》，并勾选“我已阅读并同意相关协议《天翼云网页防篡改（原生版）服务协议》“，单击“立即购买”。
6. 进入“付款”页面，完成付款。

配额退订

根据您的需求，可对正常状态的配额进行退订，遵循天翼云统一的退订规则。

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

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



到期处理

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

5. 常见问题

5.1. 产品咨询

Q：什么是网页防篡改（原生版）

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

Q：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，不会影响系统的稳定性；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。

Q：网页防篡改（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：网页防篡改（原生版） 的计费方式是什么?

A：网页防篡改（原生版）计费方式为包周期计费，包周期计费是一种预付费模式，即先付费在使用，支持包年/包月。

Q：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：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。

5.2. 产品操作

Q：如何使用网页防篡改（原生版）？

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

Q：如何绑定网页防篡改防护配额?

1. 购买成功防护配额后，可在防护配额管理页面查看配额的使用状态、绑定服务器、开通时间、到期时间等信息。
2. 在防护管理页面对需要防护的服务器进行防护设置，在防护设置页面选择防护配额，即可进行绑定。

Q：为什么要添加防护目录?

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

设置防护目录操作步骤如下：

1. 登录服务器安全卫士（原生版）控制台。
2. 在左侧导航栏，选择“网页防篡改（原生版）> 防护管理”，进入防护管理页面。
3. 在列表中选择要进行防护设置的服务器，单击操作列的“防护设置”，进入防护设置页面。
4. 绑定防护配额：选择需要绑定的配额后，单击“配置防护策略”。
   若已经绑定防护配额，可直接进入篡改防护设置页面。
5. 篡改防护设置：包括配置防护目录、设置特权进程、设置远端备份。
   - 配置防护目录：防护目录分为添加白名单和添加黑名单两种模式，可根据实际使用场景进行配置。
     - 白名单模式：会对添加的防护目录和文件类型进行保护。
     - 黑名单模式：会防护目录下所有未排除的子目录、文件类型和指定文件。
   - 其他配置：请参见“网页防篡改（原生版）> 防护管理”。

完成防护设置后，用户即可对服务器开启网页防篡改防护。

Q：网站目录被恶意篡改了怎么办?

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

Q：监控防护目录大小是否有限制?

A：防护目录有如下限制：

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

Q：开启网页防篡改后，如何修改文件?

A：网页防篡改功能开启后，如果需要修改文件或更新网站，有如下两种方式：

- 方式一：暂时关闭网页防篡改功能

  完成修改或更新后再重新开启。关闭网页防篡改期间，文件存在被篡改的风险，更新文件后请及时开启网页防篡改。
- 方式二：设置特权进程

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