主机安全（CWP）

产品文档



腾讯云TCE

版权所有：亿算云平台

文档目录

产品简介
- 产品概述
- 产品优势
- 基本概念

快速入门
- 快速入门

产品架构
- 产品架构

操作指南
- 安全概览
- 资产概览
- 主机列表
- 资产指纹
- 文件查杀
- 异常登录
- 密码破解
- 恶意请求
- 本地提权
- 反弹Shell
- 高危命令
- 网络攻击
- Java内存马
- 核心文件监控
- 漏洞管理
- 安全基线

故障处理
- Linux入侵类问题排查思路
- Windows入侵类问题排查思路
- Linux 客户端离线排查
- Windows 客户端离线排查
- 异常登录的消息提醒

常见问题
- 购买相关
- 功能相关
- 入侵相关

版权所有：亿算云平台

云镜软件相关说明
功能行为描述
客户端进程说明
安全基线检测列表

产品简介
产品概述

最近更新时间: 2024-12-19 17:12:00

什么是主机安全

主机安全是一款针对overlay、underlay主机的安全防护产品，基于海量威胁数据，利用机器学习为您提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异常登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。

为什么需要主机安全

服务器一旦被黑客入侵，企业面临以下安全风险：

- **业务被中断**：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- **数据被窃取**：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，造成企业品牌受损和客户流失。
- **被加密勒索**：黑客入侵服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- **服务不稳定**：黑客在服务器中运行挖矿程序，并通过 DDoS 木马程序获取经济利益，消耗大量的系统资源，导致服务器不能提供正常服务。

使用主机安全可以有效预防以上问题，保障企业主机安全。

主机安全主要功能

文件查杀

网站后门木马又叫 Webshell，一般是黑客通过漏洞入侵网站后放置的 ASP、PHP、JSP 等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。 基于机器学习的网站后门检测技术并依托全网恶意文件样本收集能力，主机安全可以实时准确的检测各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，保护您服务器的安全。

异常登录

基于常用登录源 IP、登录用户名、登录时间、登录地四个维度对服务器登录日志进行分析，以识别出登录流水中异常登录的行为，根据智能算法将异常登录记录标记为“可疑”或“高危”，并向您提供实时告警通知。

密码破解

您的云服务器可通过互联网登录，给了不法之徒进行暴力破解尝试入侵您云服务器的机会。主机安全通过多维度多种手段检测云服务器是否被尝试暴力破解其密码。若检测有异常，会通过站内信或者短信等渠道对您进行告知。

恶意请求

主机安全通过对外界请求行为的实时监控及处理能力，实现对恶意请求行为的有效识别。若检测到恶意请求行为，主机安全系统会向您提供实时告警通知。

高危命令

基于安全技术及多维度多种手段，对系统中命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分。若检测出高危命令，主机安全系统会向您提供实时告警通知。

本地提权

若出现以低权限进入系统，并通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到云服务器的安全。主机安全的本地提权功能可实时监控您服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

反弹 Shell

反弹 Shell 功能是基于安全技术及多维度多种手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

漏洞管理

主机安全对云服务器上存在的高危漏洞风险进行实时预警并提供修复方案，包括应急漏洞、Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，帮助企业快速应对漏洞风险。

基线管理

主机安全支持对基线检测项的定期检测和一键检测、支持对指定主机上的指定基线项进行检测、支持通过检测策略了解基线通过率及风险情况，同时可提供基线和检测项的风险等级和修复建议，同时提供默认基线策略，有助于您更好的管理服务器中的基线安全。

高级防御

实时监控网络攻击行为，支持检测的威胁类型包括：Webshell 探测、Struts 漏洞利用、代码仓库拉取、代码注入攻击、命令注入攻击及机器批量控制利用等。

产品优势

最近更新时间: 2024-12-19 17:12:00

主机安全与其他主机安全产品的优势比较如下表所示：

优势	主机安全	其他主机安全产品
黑客行为检测	基于平台全网威胁数据源，实时检测黑客攻击行为 。	基于单一主机行为数据进行判断，检测能力弱，无法快速响应。
木马文件检测	后端集成电脑管家新一代 TAV 反病毒引擎及哈勃分析系统，极速响应未知风险。基于机器学习的 WebShell 检测引擎，有效对抗加密变形类恶意脚本。	可执行恶意文件的检测能力缺失，基于正则、字符逻辑匹配方式对 WebShell 进行检测，误报、漏报风险高。
免安装、维护	自动关联平台服务器运维信息，购买云服务器即可使用相关信息。安全策略云端自动更新，无需人工维护各种安全检测脚本文件。	需要用户登录服务器手动安装，且需要一定安全技术能力的人进行安全策略配置。
集中运维	安全事件可在控制台统一管理，省去登录多台服务器的麻烦。主机资产集中管理，快速构建安全可视化运维平台。	需要登录到服务器上，对单个安全事件进行处理。
低资源占用	自研轻量级 Agent，绝大部分计算和防护在云端进行，对服务器的资源消耗占用低。	软件客户端内存占用高，普遍消耗在100M以上，业务峰期会影响服务器性能。

版权所有：亿算云平台

基本概念

最近更新时间: 2024-12-19 17:12:00

安全基线

安全基线（Security Base Line）指为了满足安全要求，相关系统和服务安全配置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产品是否达到安全基线，包括账号配置安全、口令配置安全、授权配置、日志配置、网络配置等。安全基线评估结果在一定程度上，反映了服务器的安全性。

木马病毒

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和 DDoS 攻击等特殊功能的后门程序。

WebShell

WebShell 就是以 ASP、PHP、JSP 或 CGI 等网页文件形式存在的一种命令执行环境，也称为一种网页后门。黑客在入侵了一个网站后，通常会将 ASP 或 PHP 后门文件与网站服务器 Web 目录下正常的网页文件混在一起，然后使用浏览器来访问 ASP 或者 PHP 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

主机漏洞检测

主机漏洞检测（Host Vulnerability Detection）指基于主机 Agent 在主机内部发现漏洞的一种方式。将漏洞检测模块运行于主机内部，直接进行验证或者采集信息，来判断主机是否存在漏洞。

未授权访问

未授权访问（Unauthorized Access）是不满足安全基线导致的一类问题，主要指相关服务没有对服务的访问条件进行限制，例如设置密码、限制访问来源等，导致任何人都可以直接连接服务进行操作，从而产生安全问题。

异常登录

通过采集服务器上 RDP、SSH 登录日志，上报登录源 IP、登录用户名、登录时间、登录地等信息到云端进行风险评定，对非法登录进行实时告警通知。

隔离文件

通过隔离技术把存在恶意行为的木马、病毒文件进行隔离存储，避免恶意文件持续扩散。

版权所有：亿算云平台

快速入门
快速入门

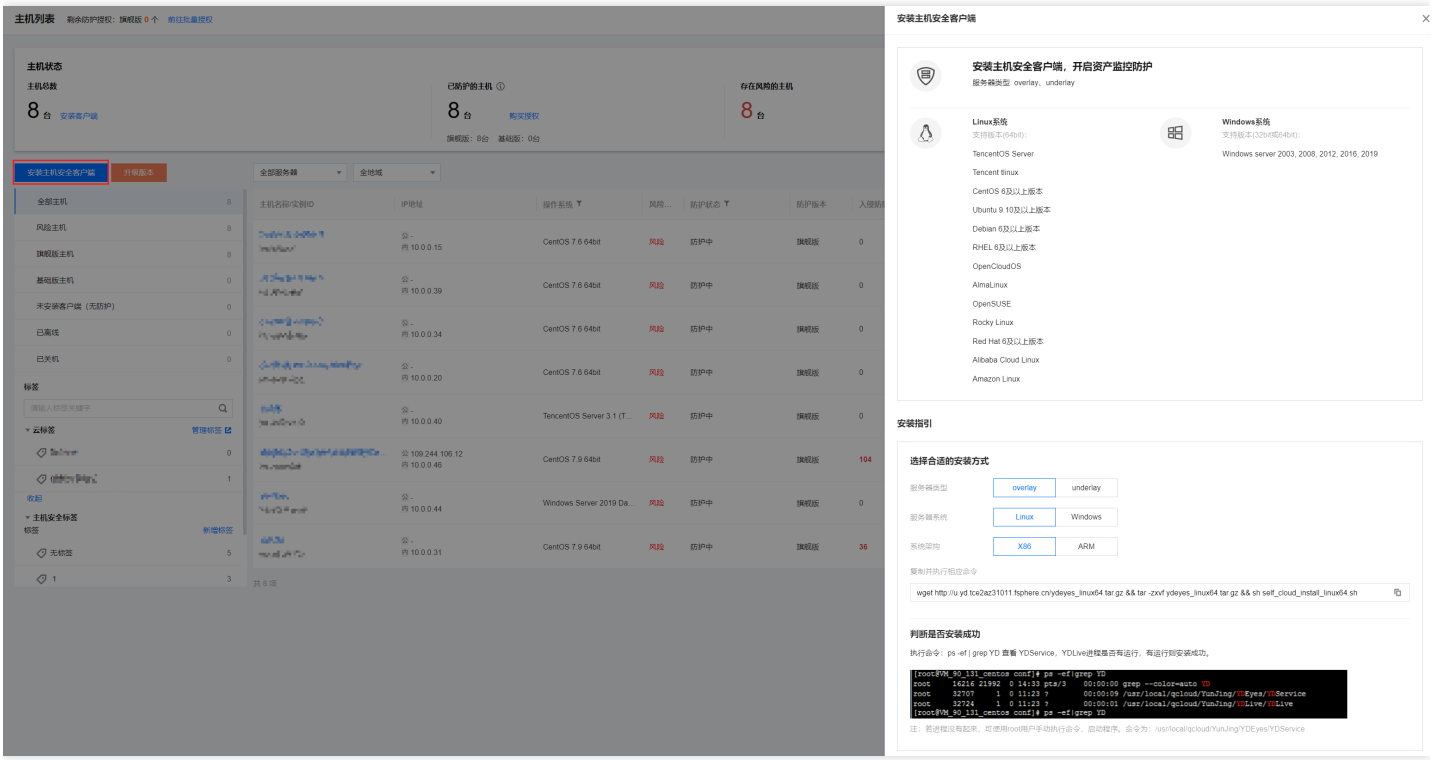
最近更新时间: 2024-12-19 17:12:00

步骤1：安装主机安全

主机安全客户端是主机安全提供的防护插件，使用主机安全功能须先安装该插件。

1.登录租户端控制台，选择【产品管理】 > 【安全】 > 【主机安全】，进入主机安全租户端控制台。

2.在左侧导航中选择【资产管理】>【主机列表】，单击 安装主机安全客户端 可查看安装指引。



步骤2：操作主机安全

主机安全租户端支持展示主机的安全风险事件，支持对木马文件进行检测及隔离、漏洞检测、对可疑的登录行为进行检测识别及加白名单处理、支持对密码破解行为进行阻断设置、同时支持告警设置等操作，详情请参见 操作指

南。

步骤3：故障排除

若主机遭遇入侵，可根据入侵类问题排查指南进行问题排查，恢复网站或系统的正常运行，详情请参见 Linux 入侵类问题排查思路 或 Windows 入侵类问题排查思路。

步骤4：卸载主机安全

若您不再需要主机安全防护，可将主机安全客户端进行卸载，主机安全共有控制台卸载与系统卸载两种方式，下面将为您详细介绍：

控制台中卸载

1.登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】>【主机列表】，查看自己的云服务器是否已安装主机安全。

2.在服务器列表中，选择需要卸载主机安全客户端的服务器，单击右侧操作栏的【卸载】即可。



进入系统卸载

- **Windows 系统**：依照路径 C:\Program Files\QCloud\YunJing\uninst.exe ，找到 uninst.exe 文件，双击即可卸载。
- **Linux 系统**：输入命令： if [-w '/usr']; then /usr/local/qcloud/YunJing/uninst.sh ; else /var/lib/qcloud/YunJing/uninst.sh ; fi 即可卸载。

常见问题

防火墙拦截

建议防火墙策略放过主机安全后台服务器访问地址

overlay域名	s.yd.tce2az31011.fsphere.cn; l.yd.tce2az31011.fsphere.cn; u.yd.tce2az31011.fsphere.cn	overlay端口	5574、8080、80、9080
underlay域名	s.yd.tce2az31011.fsphere.cn; l.yd.tce2az31011.fsphere.cn; u.yd.tce2az31011.fsphere.cn	underlay端口	5574、8080、80、9080

产品架构

产品架构

最近更新时间: 2024-12-19 17:12:00

下图是云镜的产品架构示意图：



云镜Agent

Agent是一个常驻在云主机操作系统中的轻量化进程，部署在需要保护的云主机上，主要功能是根据用户配置的安全策略上报服务器上存在的安全风险数据和新增的安全事件数据，同时响应用户和云镜云端防护中心的指令，实现对云主机上的安全威胁清除和恶意攻击拦截。

云镜防护引擎

基于云平台的大数据处理能力，云端防护中心接收全网Agent上报云主机安全事件和威胁数据，通过云端的多个威胁识别模型，对每一条上报的安全事件进行分析，根据分析结果给Agent下发相关拦截和处理指令，云端防护中心是云镜的中枢神经系统，相关安全威胁的识别算法依赖于腾讯云安全团队的运营和智能调优，云端防护中心同时保存用户自己创建的相关安全策略配置，满足用户个性化的安全防护需求。

版权所有：亿算云平台

用户操作控制台

提供给用户使用的网页版本控制台，主要功能包括云主机资产管理、安全威胁数据处理、安全策略配置、安全报表查看等供用户操作和查看的功能。

操作指南
安全概览

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍安全概览各模块功能及操作步骤。

概述

主机安全的安全概览实时展示您的主机安全评分、待处理风险、安全防护状态、风险趋势以及主机安全的实时动态；提供帮助文档和主机安全升级服务建议，帮助您抵御黑客入侵风险及攻击威胁，保障企业主机安全。

操作指南

1.登录主机安全租户端控制台。

2.在左侧导航中，选择【安全概览】，可查看安全概览信息和相关处理操作，各模块说明如下。

安全状态

1. 在【安全状态】中，展示了您的主机安全评分和以下3类安全风险情况，并提供快捷处理入口。

- 入侵检测：包括入侵检测模块的7个功能，即文件查杀、异常登录、密码破解、恶意请求、反弹 Shell、本地提权、高危命令，合并统计待处理风险数和受影响主机数。
- 漏洞风险：包括 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，合并统计待处理风险数和受影响主机数。
- 基线风险：只统计基线待处理风险数和受影响主机数。



2. 单击 ，将打开风险处理详情弹框，可以查看入侵检测、漏洞风险、基线风险具体详情。单击对应风险卡片，页面将跳转至相对应的风险处理界面。



主机安全状态划分为3个等级：

等级	体检评分	字体颜色	状态说明
优	90分 - 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 - 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 - 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。

> **说明：**
>
> 主机安全状态体检评分最低分数为 20分。

按安全事件分类计算扣分项，安全事件等级分类及扣分规则：

安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马、病毒、暴破成功。	50分
高危	高危漏洞、高危基线、异地登录、本地提权、反弹 Shell、高危命令。	10分
中危	中危漏洞、中危基线。	3分
低危	低危漏洞、低危基线。	2分
其他	基础版（非防护状态）。	1分

安全防护

1. 在【安全防护】中，展示主机安全应对入侵攻击提供的（预防-防御-检测-响应）全流程解决方案，并细化展示各阶段所需的安全防护项。若各防护项均开启，可直观了解您当前主机安全的情况，并提供安全风险快捷处

理入口。



防护详情

在【防护详情】中，可查看目前主机总数、在线主机总数量、关机或离线的主机数量、未安装客户端的主机数、已防护主机数、专业版或旗舰版主机数、基础版主机数，同时提供资产更新时间、病毒库更新时间、漏洞库更新时间以及安全引擎防护等信息。

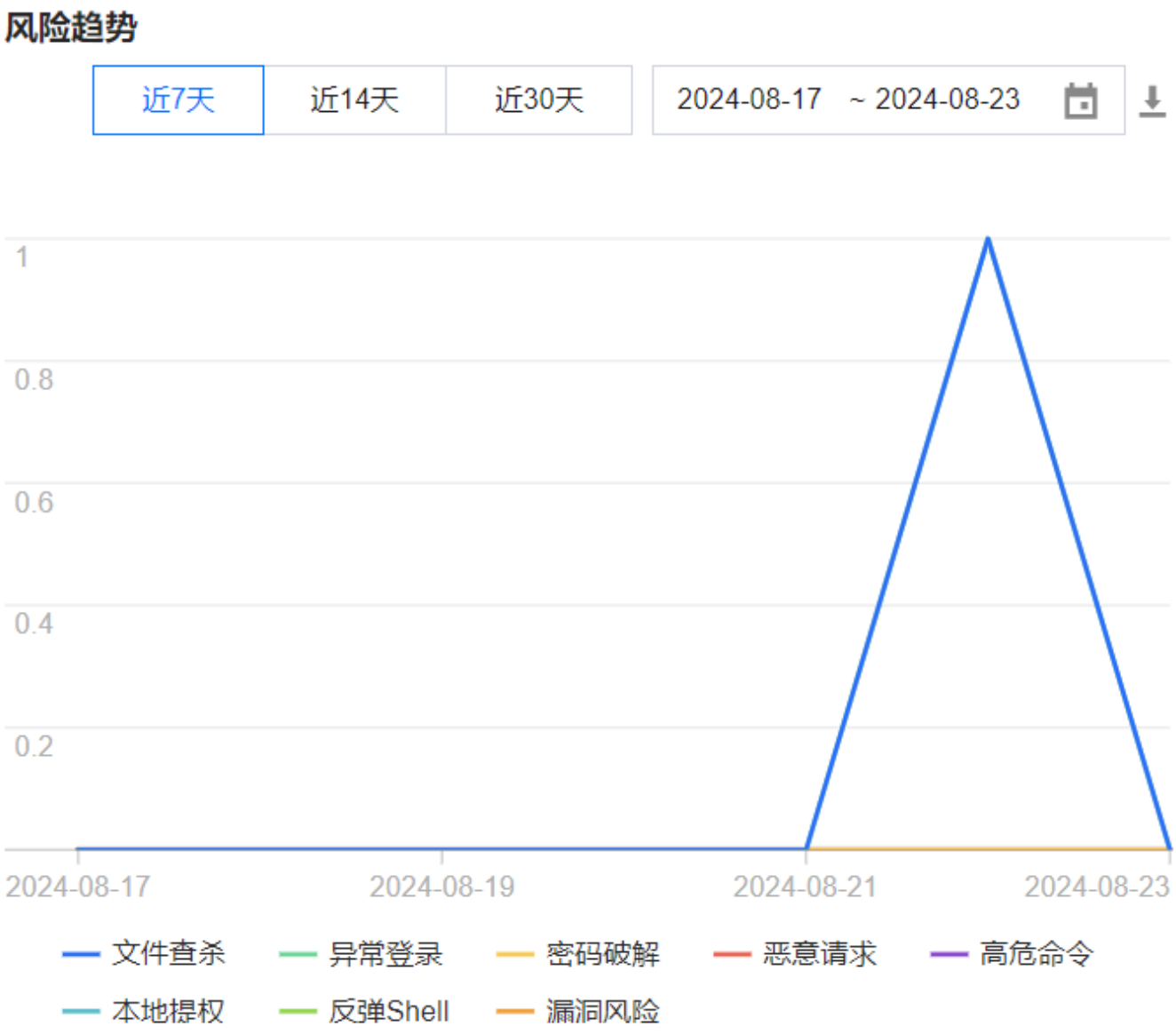
> **说明：**
>
> 由于基础版主机防护程度相对较弱，“防护主机数”仅包含专业版或旗舰版主机。



风险趋势

风险趋势功能通过折线图，为您展示近7天、近14天或近30天的安全风险和威胁发生趋势，并且支持按时间段筛选查看。将鼠标在趋势图中悬停，将显示该日期文件查杀、密码破解、异常登录、漏洞风险、基线风险等安全事件数。单击右上角，支持将所选中日期的安全事件数下载至本地。

> **说明：**
>
> 数据来源为当日新增待处理事件数，每小时更新一次，历史事件数将保留，不再变更。



实时动态

实时动态功能按照时间倒序实时展示发现的主机风险及威胁事件。单击蓝色字段的主机 IP，将跳转至【主机详情】中，可查看该主机安全各类风险情况；单击【查看详情】，将跳转至相应事件处理页面。

实时动态

告警行为	威胁等级	发现时间	操作
异常登录 主机10.0.0.46被113.108.77.63异常登录	可疑	2024-08-22 …	查看详情
异常登录 主机10.0.0.46被119.147.10.183异常登录	可疑	2024-08-16 …	查看详情
异常登录 主机10.0.0.46被113.108.77.62异常登录	可疑	2024-08-15 …	查看详情
异常登录 主机10.0.0.46被113.108.77.62异常登录	可疑	2024-08-14 …	查看详情
异常登录 主机10.0.0.46被119.147.10.186异常登录	可疑	2024-08-08 …	查看详情

共 30 条

1 / 6 页

资产概览

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍资产概览各功能模块及操作。

概述

资产概览是从资产维度对主机及关键资产指纹数据进行统计盘点、可视化呈现，便于用户了解主机资产情况。

前提条件

仅专业版或旗舰版主机支持资产指纹数据采集和同步，基础版或未防护主机则不支持。

背景信息

仅付费防护版本的主机才可采集资产指纹数据。

各版本支持采集的资产指纹如下：

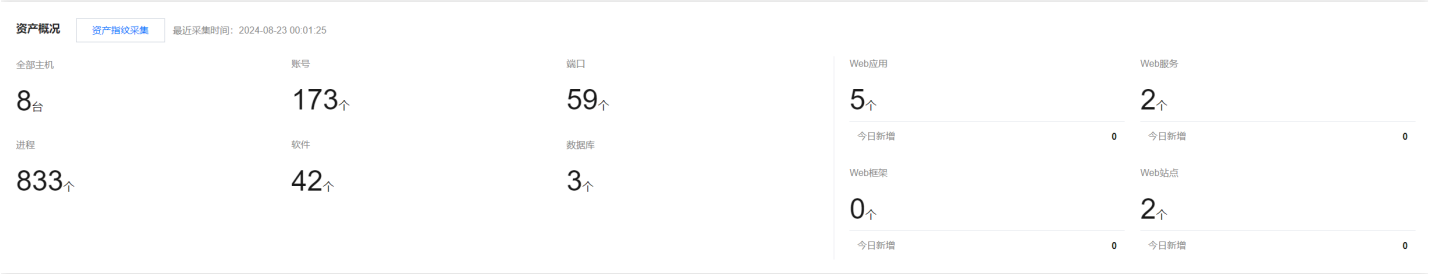
主机安全防护版本	采集的资产指纹项
专业版	10项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点
旗舰版	16项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点、Jar包、启动服务、计划任务、环境变量、内核模块

> **说明：**
>
> 资产指纹数据每隔8小时自动采集一次，支持手动采集。

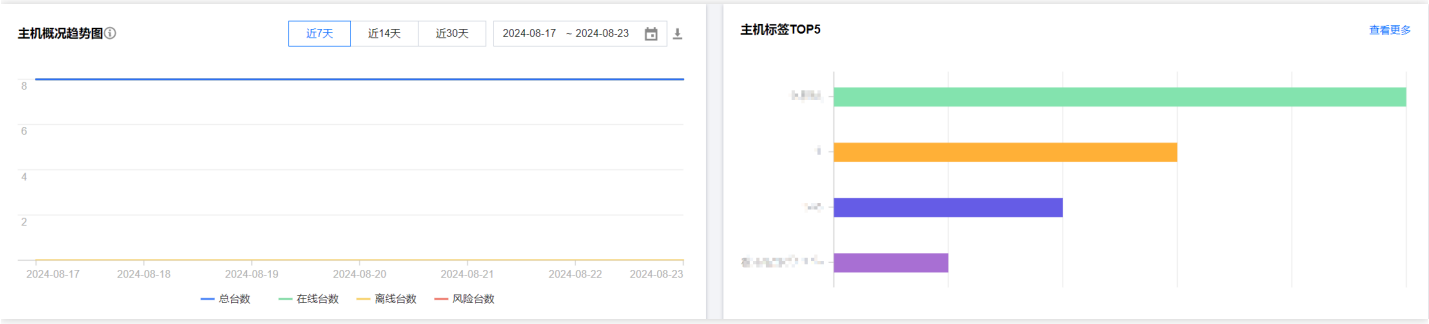
概览

登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】>【概览】，进入概览页面。

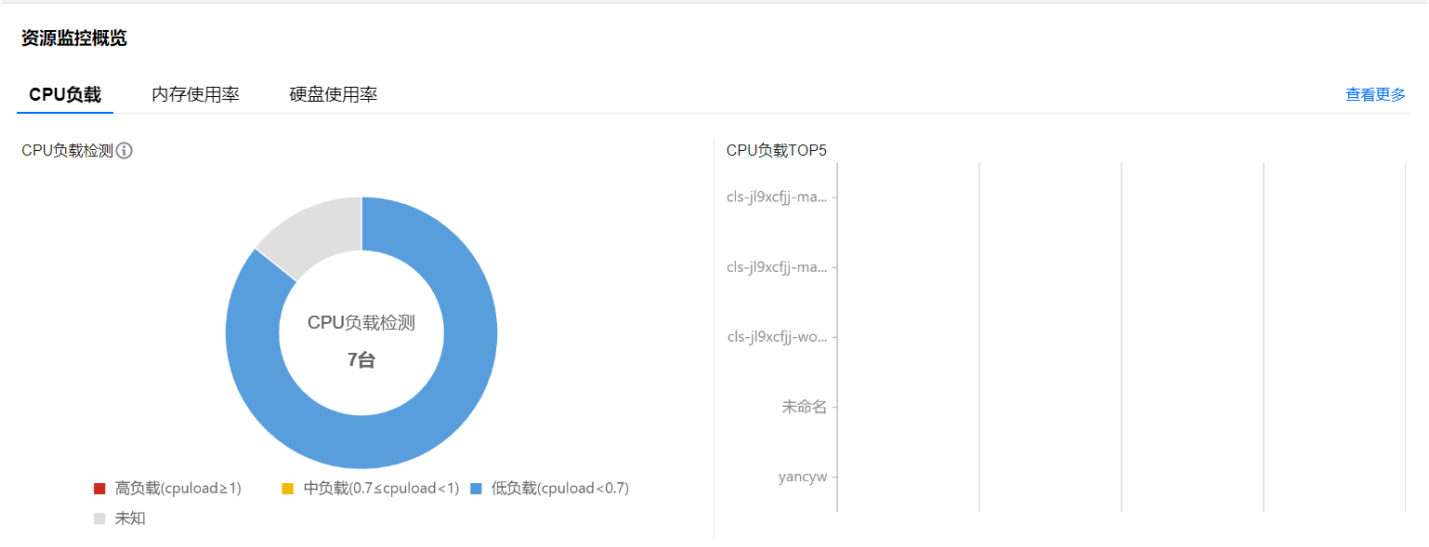
1. 资产概况面板，可查看全部主机及各项资产指纹的统计情况。



2. 主机概况趋势图（总台数、在线台数、离线台数、风险台数）支持最长不超过近3个月时间段的查询，支持下载导出；主机标签 TOP 5，可查看所有主机中使用最多的前5个标签。

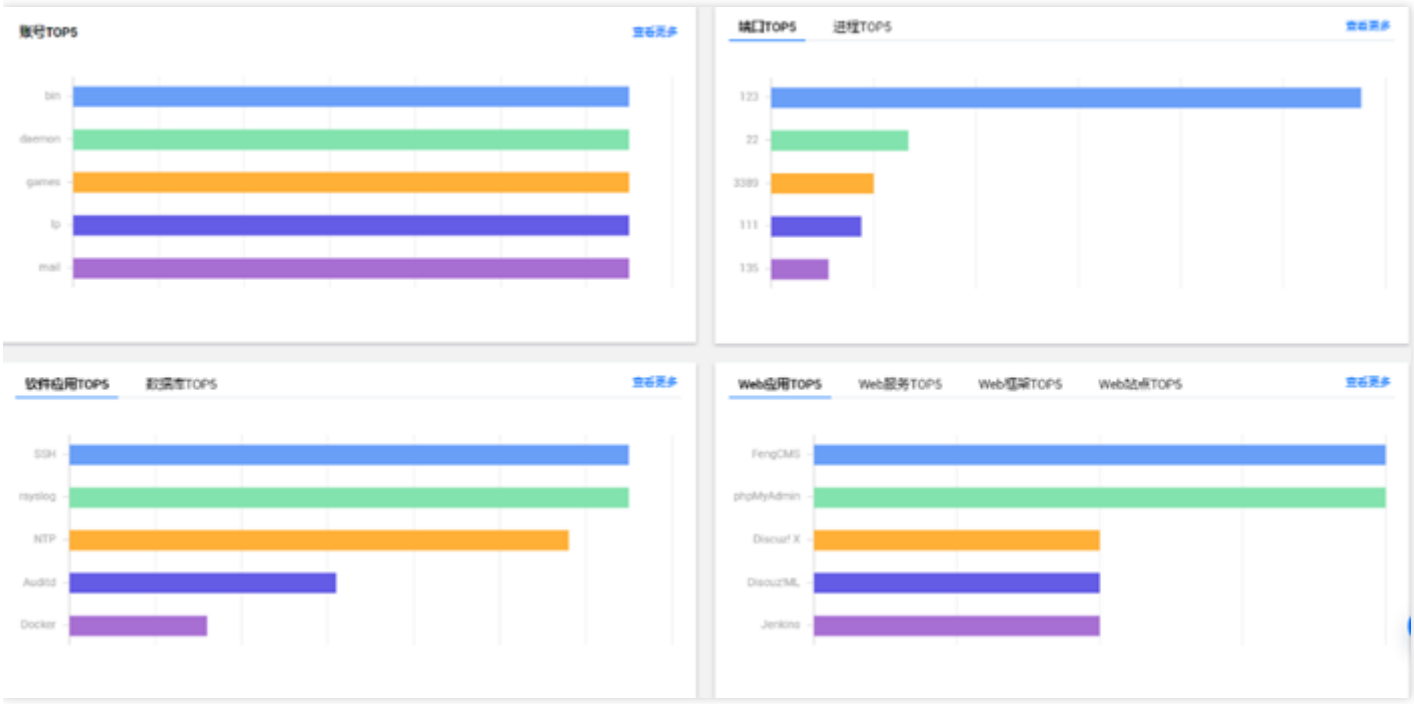


3. 资源监控概览，可查看CPU负载、内存使用率、硬盘使用率的分布情况及相应TOP 5。



> **说明：**
>
> 关于CPU负载，目前仅支持获取Linux系统的服务器CPU负载，Windows系统暂认定为未知。

4. 查看账号TOP 5、端口TOP5、进程TOP 5、软件应用TOP 5、数据库TOP5、Web应用TOP 5、Web服务TOP5、Web框架TOP 5、Web站点TOP5。



> **说明：**
>
> 各资产指纹TOP 5是根据指纹（账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点）所属服务器数量降序排列后，取排名前5项的数据。

主机列表

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍主机列表各功能模块及操作。

概述

主机列表可查看目前已接入主机安全的所有服务器的信息，帮助您全面了解资产的安全状态。

相关限制

可接入主机安全的主机范围：

主机类型	Linux系统	Windows系统
overlay主机	支持架构：x86、arm	支持架构：x86
underlay主机	支持架构：x86、arm	支持架构：x86

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【资产管理】>【主机列表】。
2. 在主机列表页面，可以查询资产状态、安装/卸载主机安全客户端等操作。

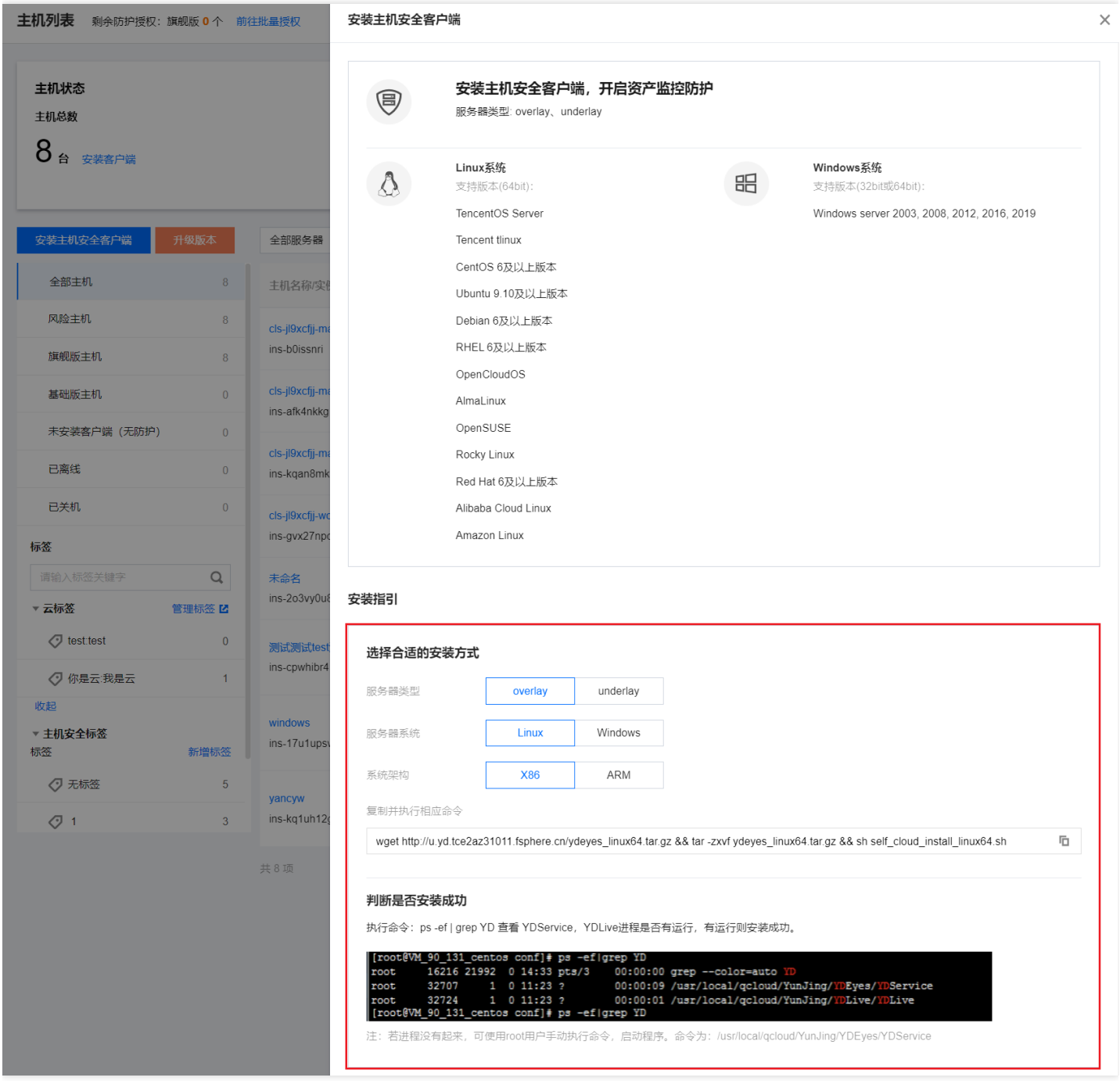
主机状态

在【主机状态】中，可查看目前主机总数、已防护的主机（由于基础版主机防护程度相对较弱，此处仅包含专业版或旗舰版主机数）、存在风险的主机数、无防护的主机数和授权即将到期的主机数。



安装主机安全客户端

单击【安装主机安全客户端】展示主机安全客户端的安装指引，选择服务器类型和操作系统进行正确安装，可接入overlay、underlay服务器，安装完成后，须验证是否安装成功。



升级版本

单击【升级版本】将跳转至【授权管理】页，您可为基础版主机绑定专业版或旗舰版授权，即可开启专业版或旗舰版防护。

筛选导出

- 支持筛选服务器专区、地域、主机状态（全部主机、风险主机、旗舰版或专业版主机、基础版主机、未安装客户端、已离线、已关机）、标签及服务器 IP 或名称搜索。

- 单击 导出按钮，可对当前筛选出来的机器进行数据导出。



列表操作

- 支持设置标签、关联标签。
- 支持卸载主机安全客户端、授权管理，单击【授权管理】，将跳转至授权管理页，支持授权绑定、解绑、扩容等操作。



- 单击入侵检测、漏洞风险、基线风险的【数值】可跳转查看风险详情。



资产指纹

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍如何查看资产指纹统计数据。

概述

资产指纹数据采集，可帮助您快速了解资产的概况和运行状态。

相关限制

仅专业版或旗舰版主机才可采集资产指纹数据。

各版本支持采集的资产指纹如下：

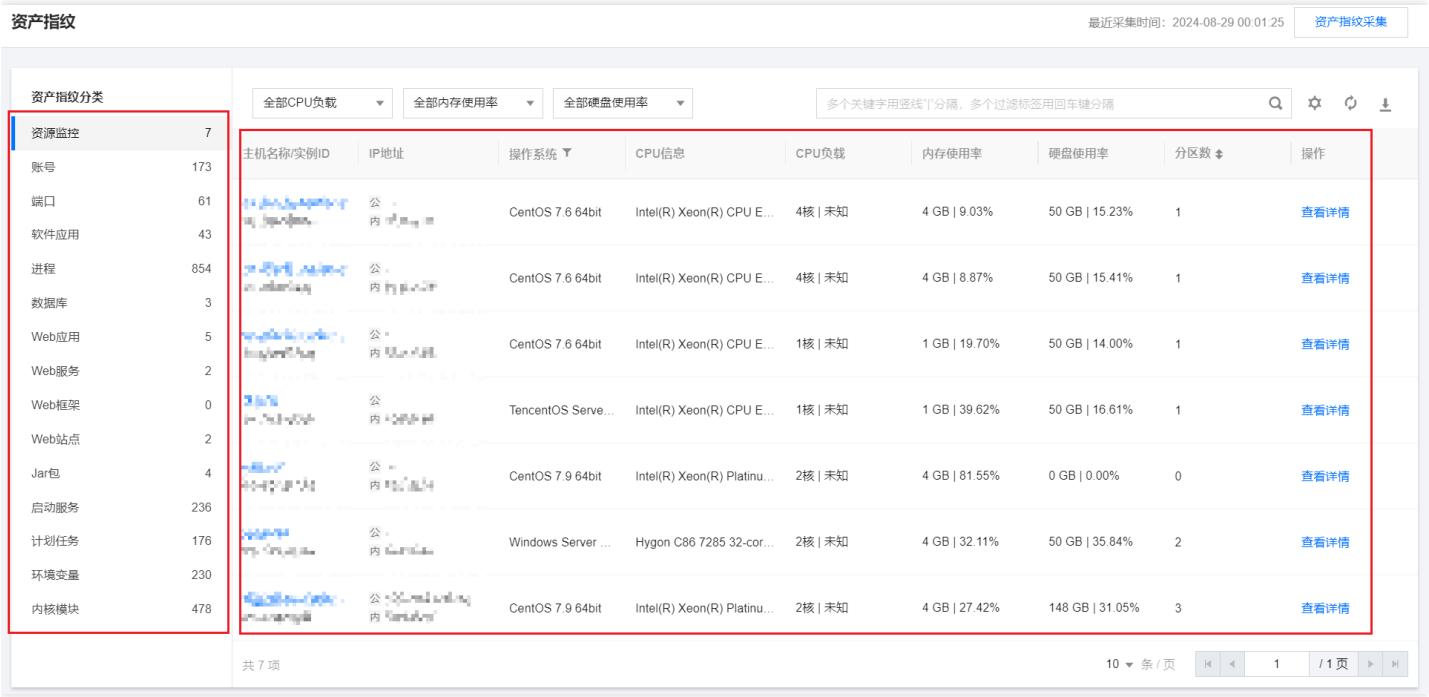
主机安全防护版本	采集的资产指纹项
专业版	10项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点
旗舰版	16项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点、Jar包、启动服务、计划任务、环境变量、内核模块

> **说明：**
>
> 资产指纹数据每隔8小时自动采集一次，支持手动采集。

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】 >【资产指纹】。
2. 在【资产指纹】中，展示了资产指纹分类列表，包括各资产指纹项及其对应服务器数量。在左侧资产指纹分类列表中选中一项后，右侧将展示该指纹详情，支持对指纹数据的查询和导出。

> **说明：**
>
> 各资产指纹搜索功能均支持模糊搜索。

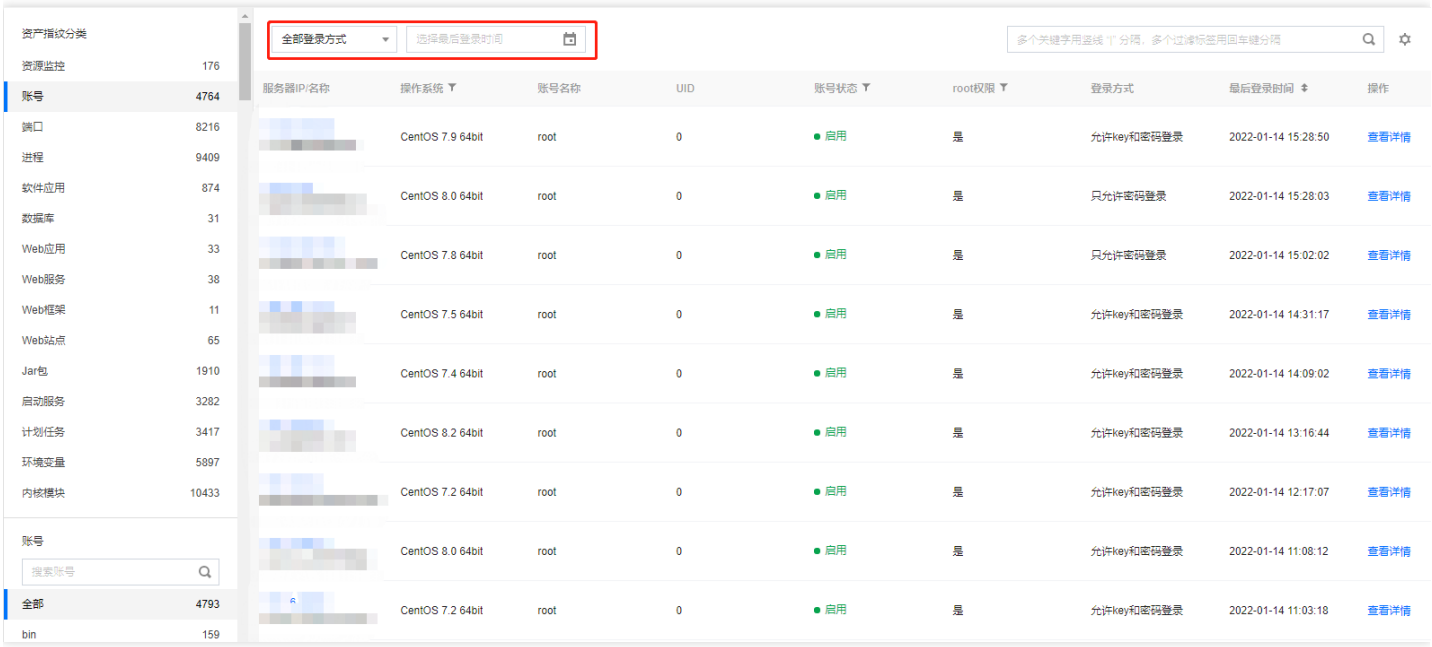


资产指纹分类说明：

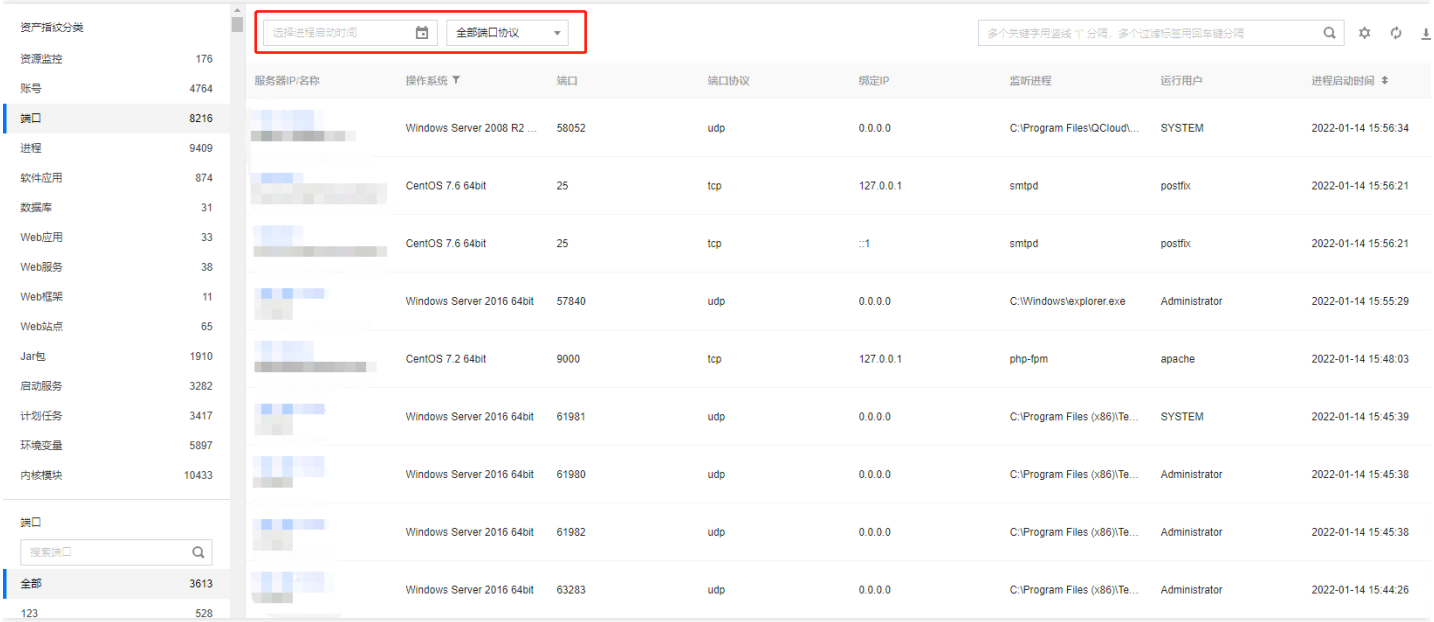
- 资源监控：对服务器CPU负载、内存使用、硬盘使用进行数据采集。



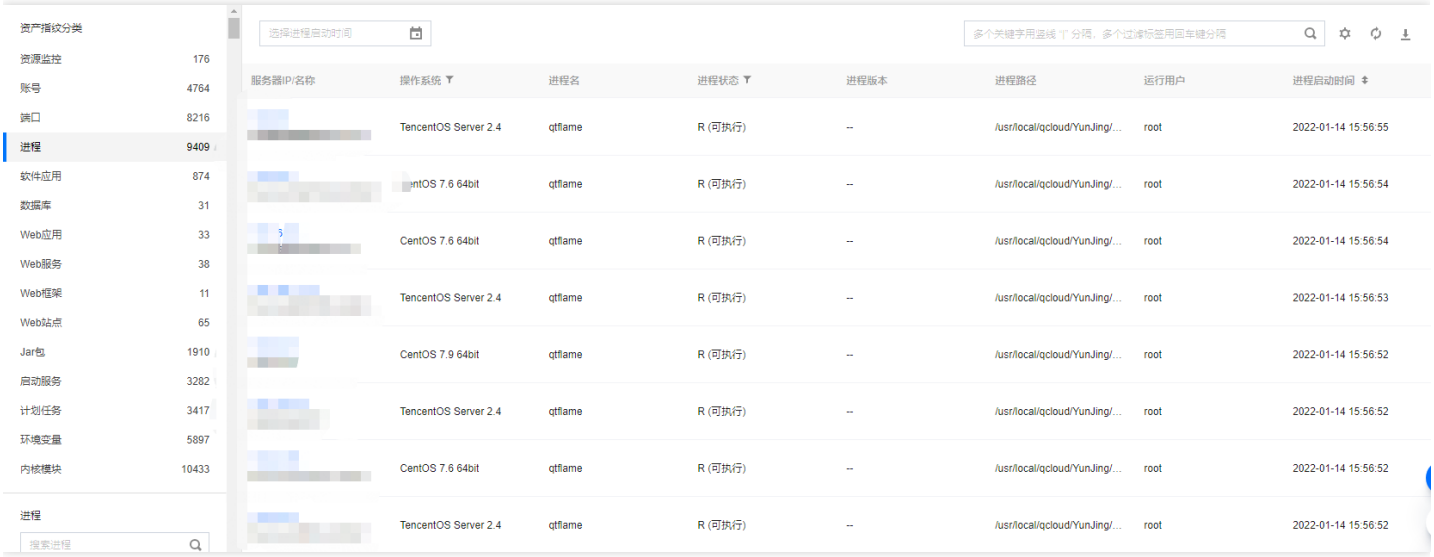
- 账号：对服务器所有账号进行采集。



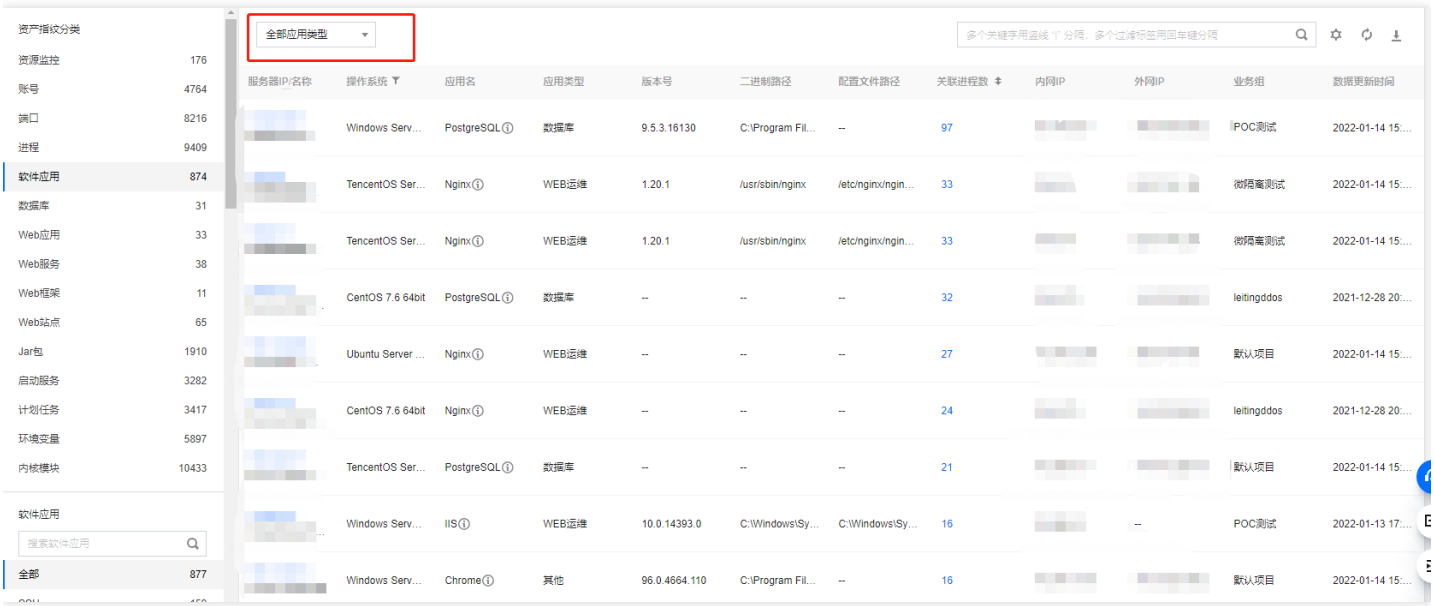
- 端口：对服务器所有已使用端口进行采集。



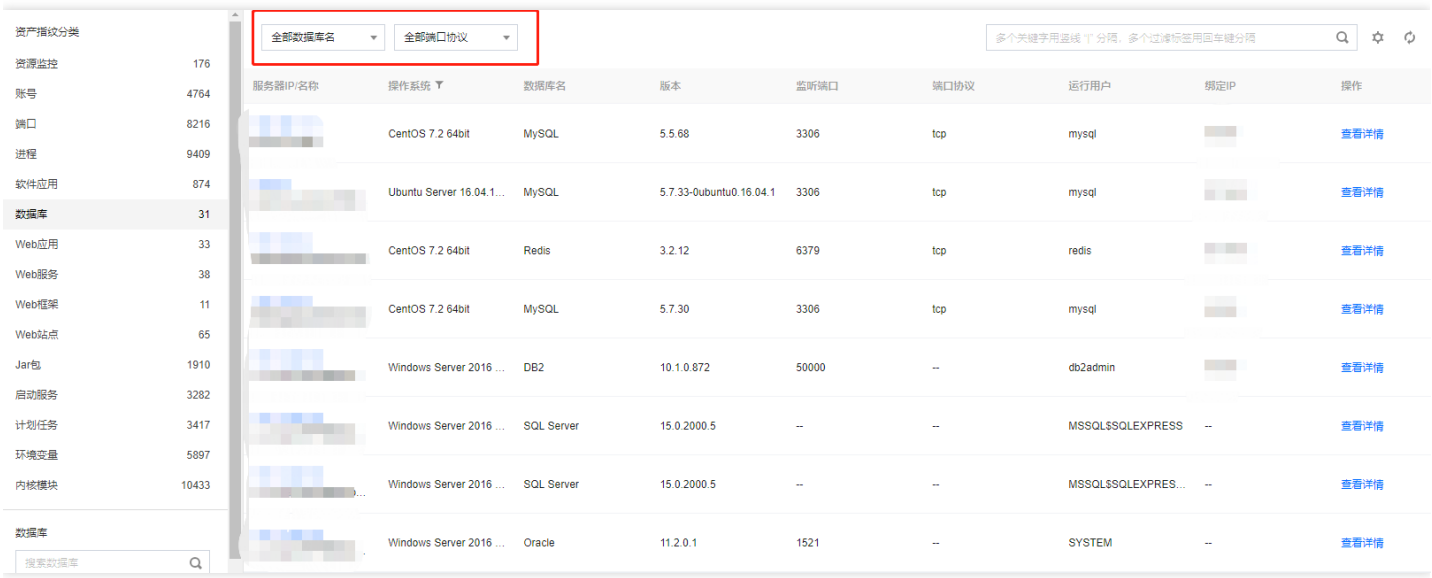
- 进程：对服务器的所有运行进程进行采集。



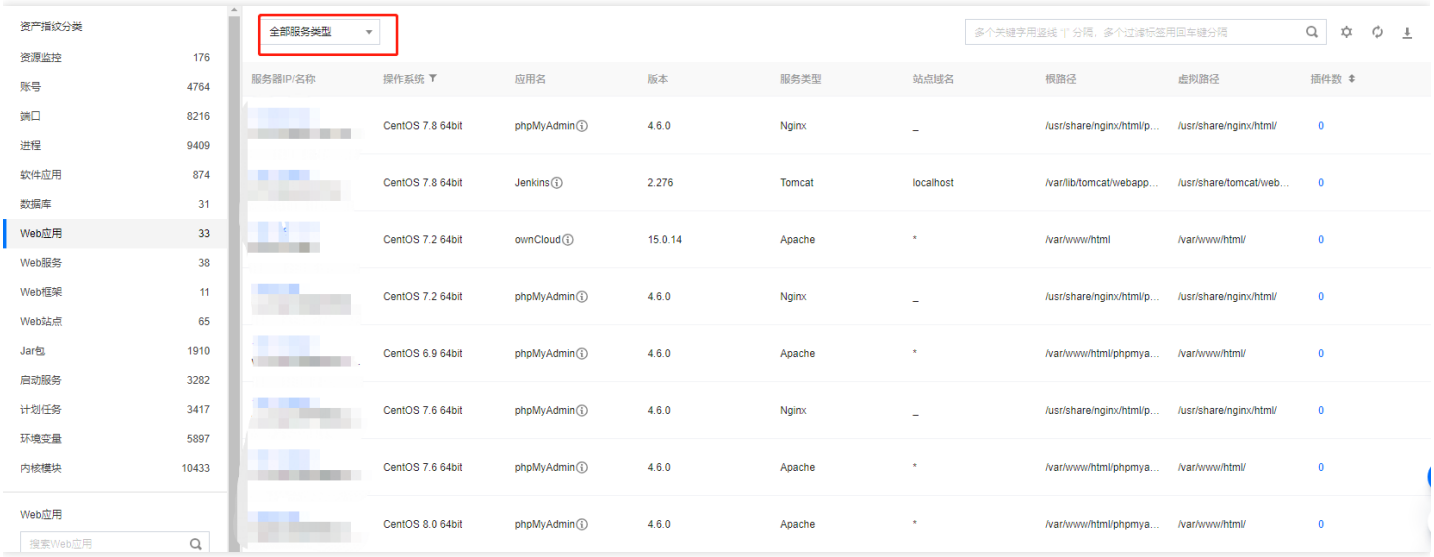
- 软件应用：对服务器所有运行中的软件应用进行采集。



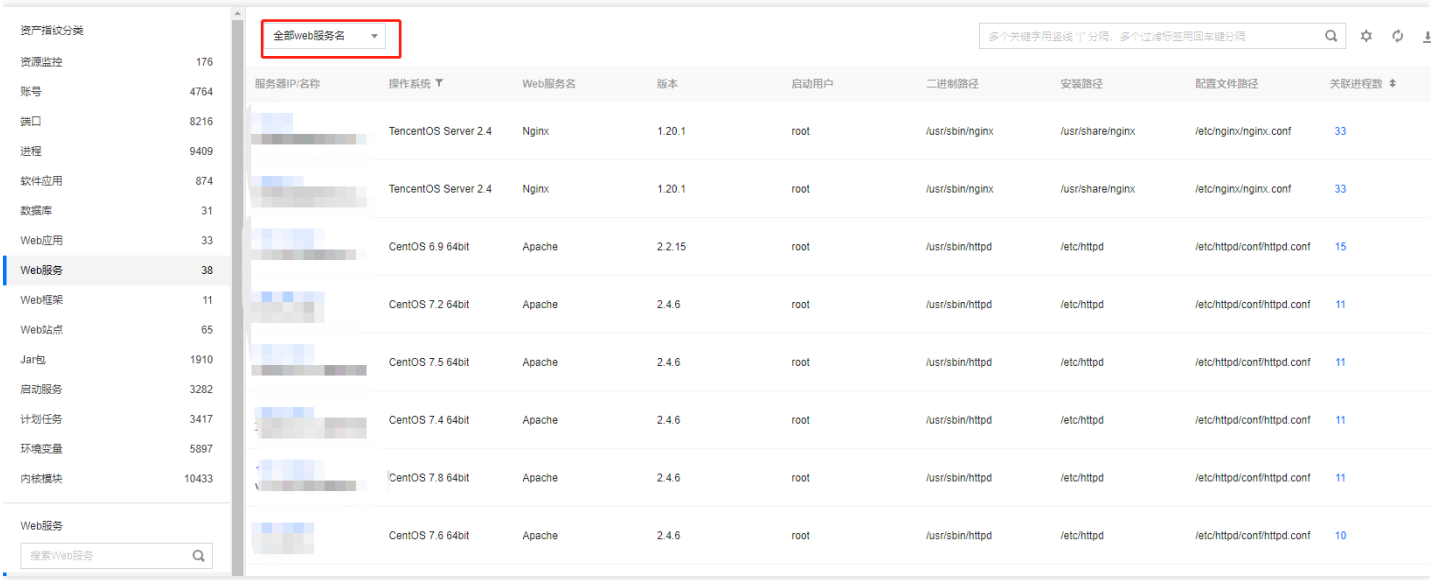
- 数据库：对服务器所有运行的数据库进行采集。



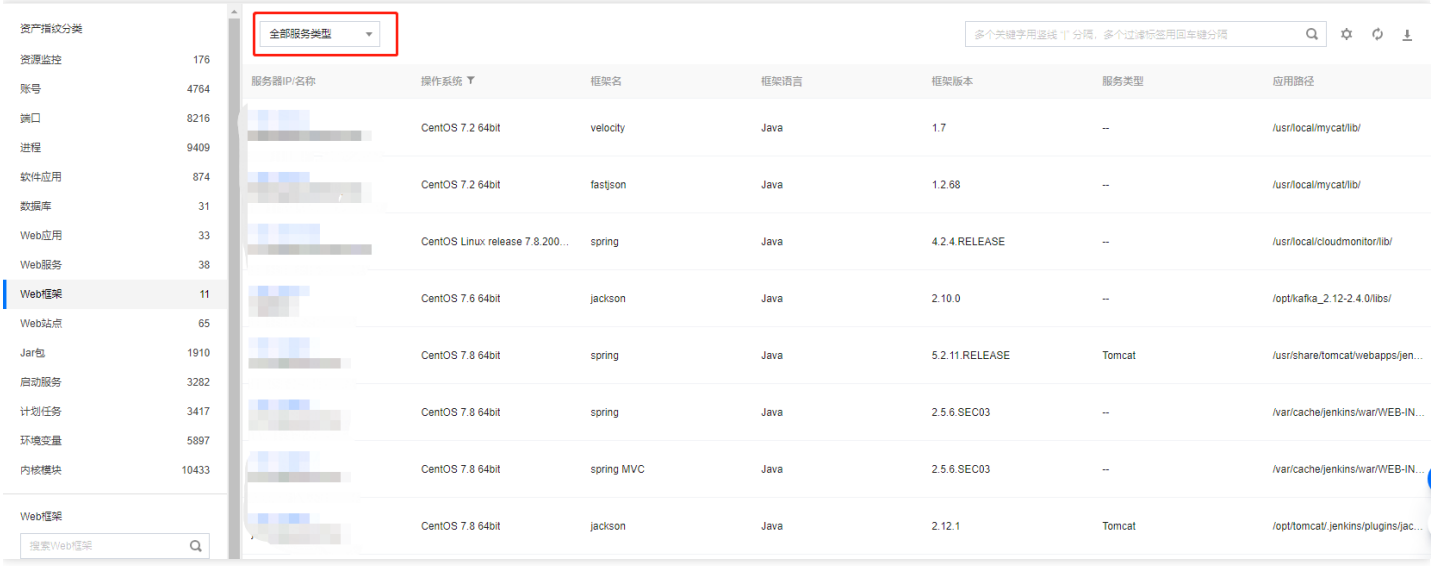
- Web 应用：对服务器所有运行的 Web 应用进行采集。



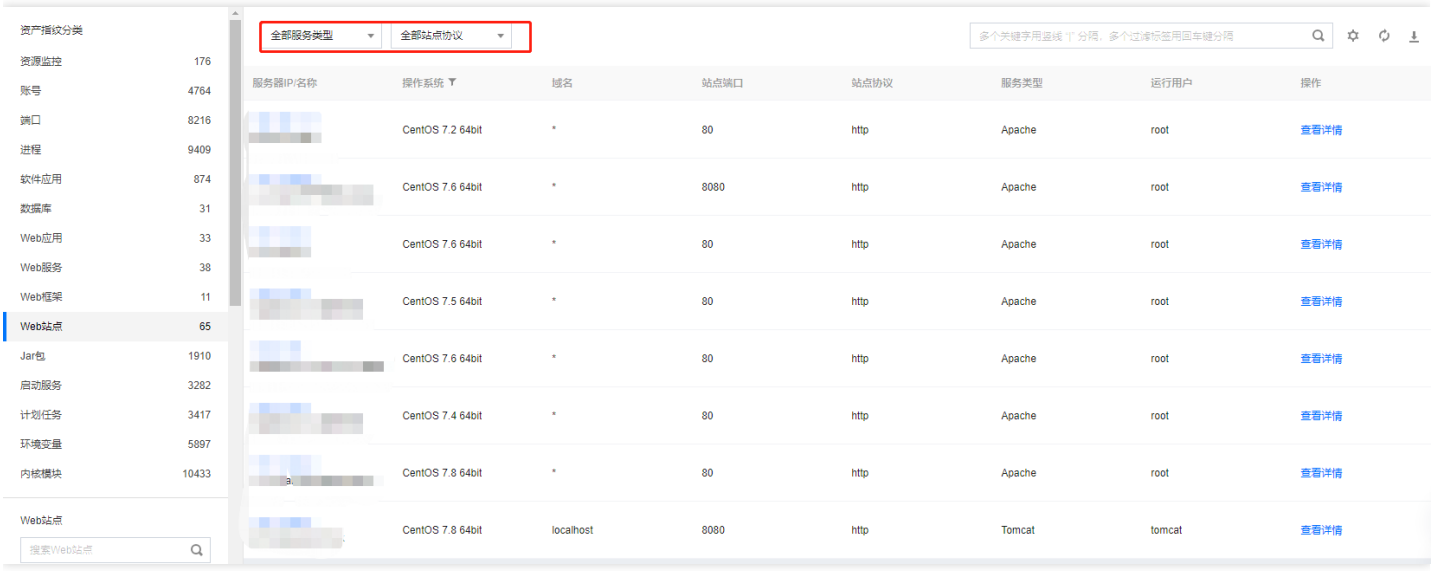
- Web 服务：对服务器所有运行的 Web 服务进行采集。



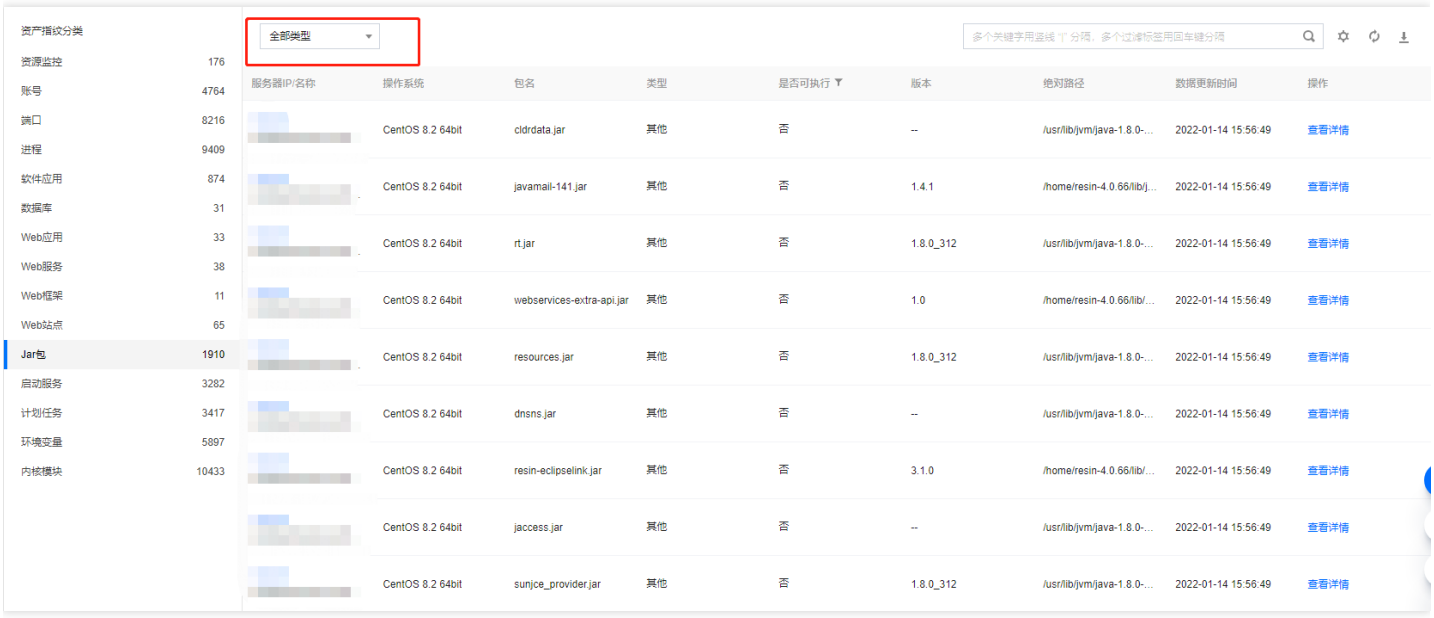
- Web 框架：对服务器所有应用的 Web 框架进行采集。



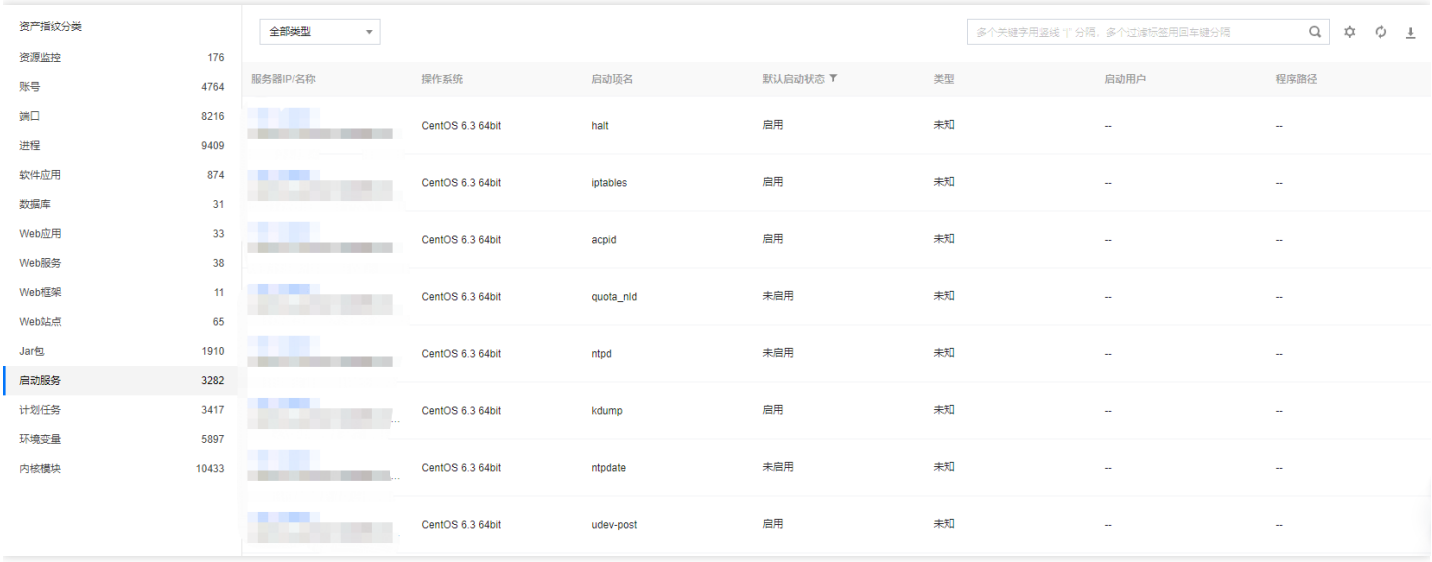
- Web站点：对服务器所有部署的Web站点进行采集。



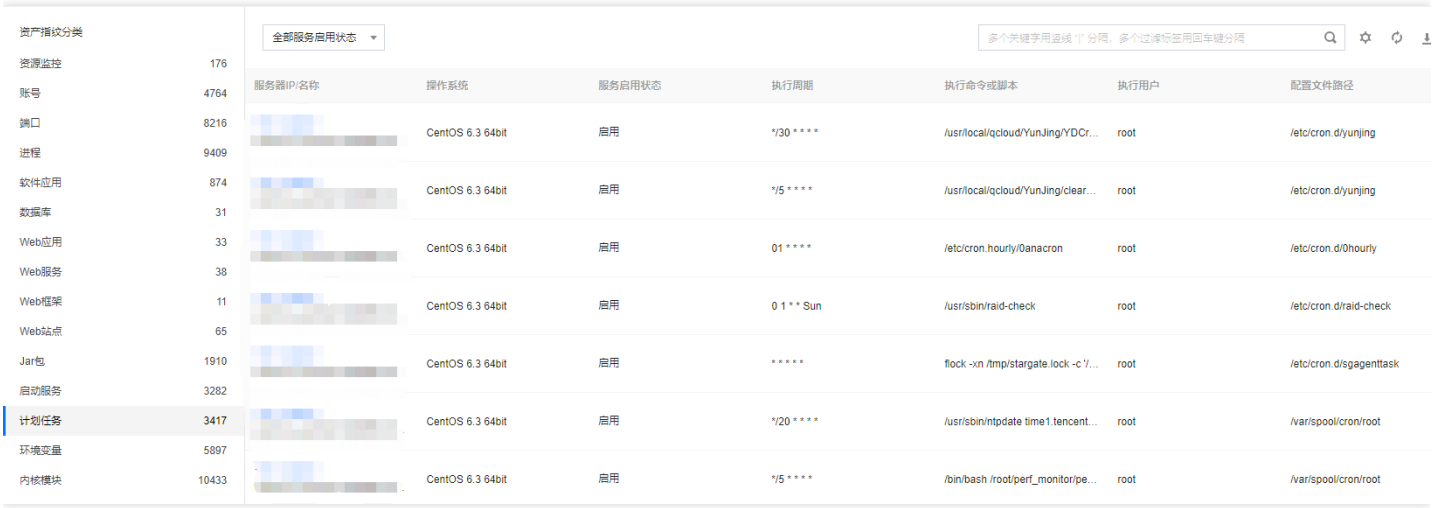
- Jar 包：对服务器所有的 Jar 包进行采集。



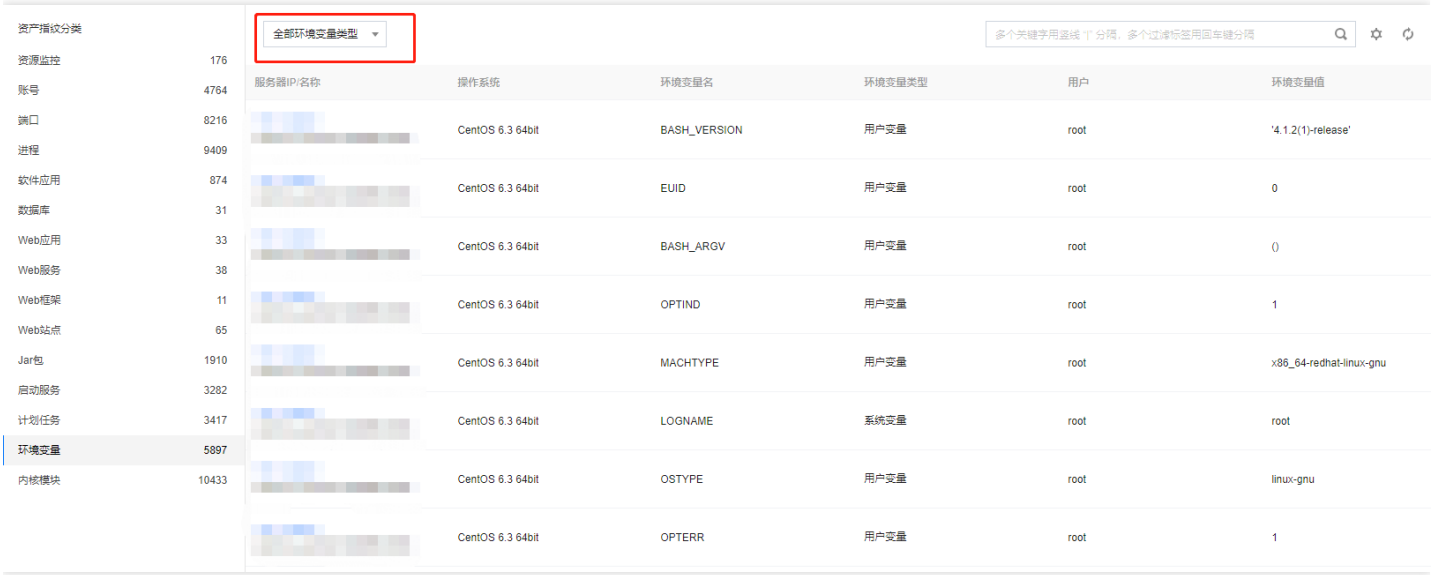
- 启动服务：对服务器所有的启动服务进行采集。



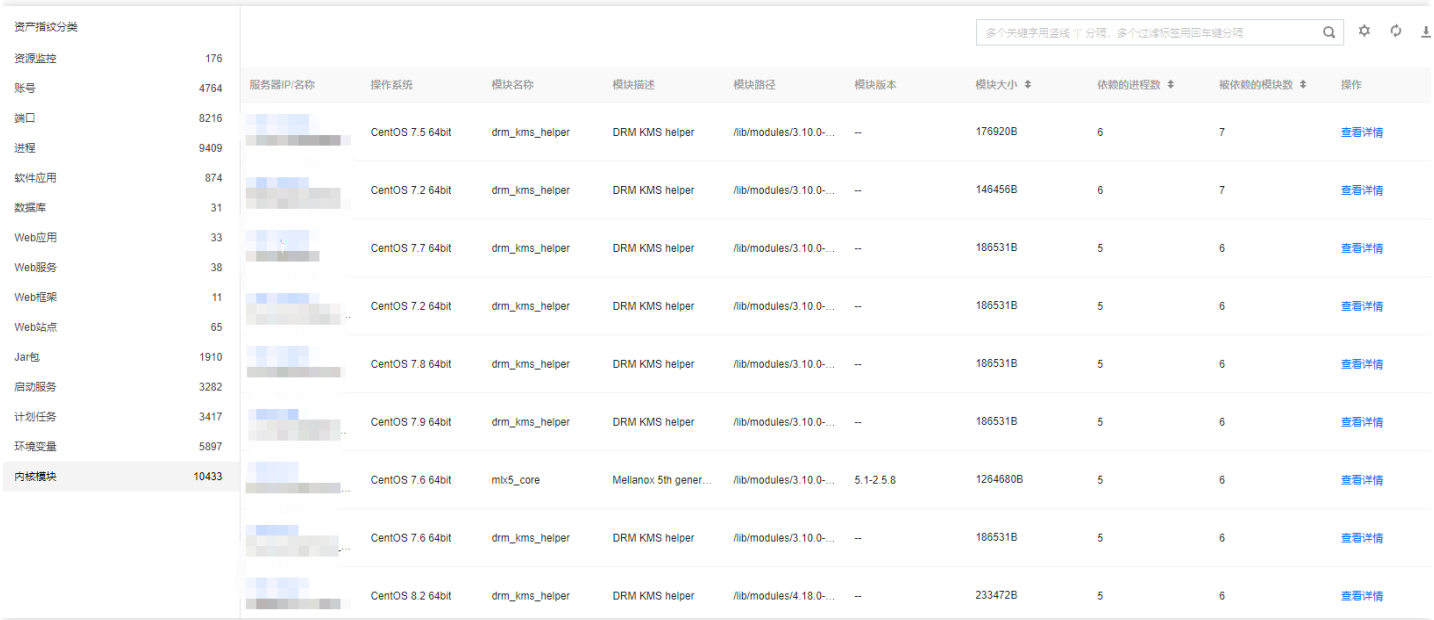
- 计划任务：对服务器所有的计划任务进行采集。



- 环境变量：对服务器所有的环境变量进行采集。



- 内核模块：对服务器的内核模块进行采集。



文件查杀

最近更新时间: 2024-12-19 17:12:00

本文档将指导您如何在主机安全控制台对木马文件进行操作处理。

文件查杀设置

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】>【文件查杀】。
2. 在文件查杀中，单击右上角处【查杀设置】，右侧弹出查杀设置页面，可对查杀模式进行设置。

> **说明：**
>
> - 常见的木马文件检测有以下两种：
> - Webshell 检测：提供常用的 Web 网站类脚本木马后门检测，包含 ASP/PHP/JSP/Python 等脚本语言。
> - 二进制检测：提供对二进制可执行类的病毒木马检测，例如 DDoS 木马、远控、挖矿类软件等，文件类型包括 exe、dll、bin 等，并告警用户。



3. 在【查杀设置】中，支持定时扫描、实时监控、自动隔离设置。

- 定时扫描：单击开启【定时检测】，设置检测模式、周期和检测范围后，单击【保存】，可定期扫描主机木马病毒文件，增强安全性。



字段说明：

- 检测模式：包括快速检测模式和全盘检测模式，可对运行中进程、关键目录、驱动加载等进行检测。其中全盘检测的时长与服务器磁盘文件数量相关，推荐选择4小时以上，避免出现扫描不完整或超时情况。
- 检测周期：可选择每天、每隔3天或每隔7天检测周期。
- 检测范围：支持选择全部专业版或旗舰版服务器、自选服务器。
- 实时监控：单击开启【实时监控】，并选择监控模式后，单击**【保存】**，可实时监控 Web 目录、系统关键目录，查杀木马病毒文件。



字段说明：

- 监控模式：
  - 标准：监控并扫描检测常见目录下增量文件。
  - 深度：监控并扫描检测所有目录下增量文件。
- 自动隔离：单击开启【自动隔离】>【保存】，将自动隔离检测出的恶意文件，部分恶意文件仍需用户手动确认隔离，建议检查文件查杀列表中所有安全事件，确保已全部处理。

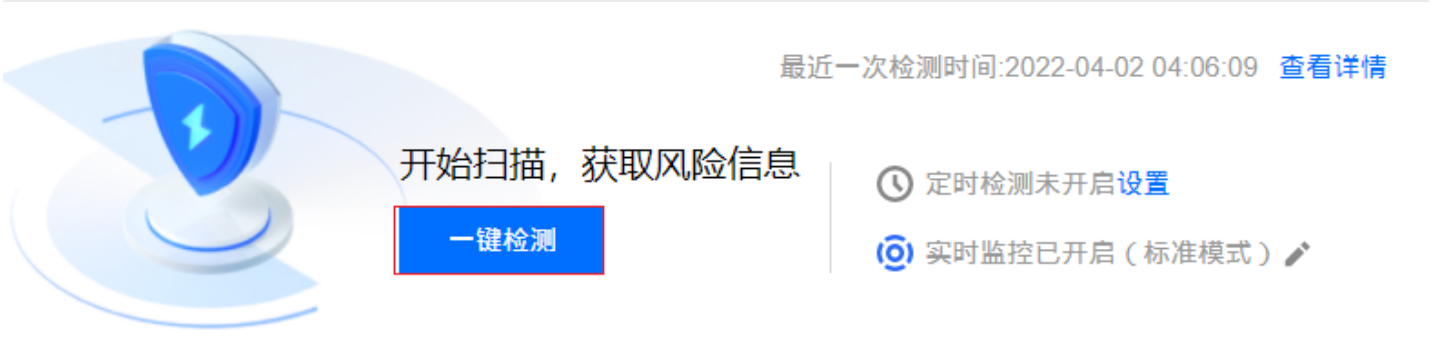
> **说明：**

> 若出现误隔离，请在已隔离列表中对文件进行恢复。开启或关闭自动隔离，均需要进行配置，实际生效存在几分钟延迟。



检测设置概览

1. 登录主机安全租户端控制台 ，在左侧导航栏中，选择【入侵检测】>【文件查杀】。
2. 在文件查杀页面，单击【一键检测】，开始设置手动检测模式。



3. 在【一键检测设置】弹窗中，确定检测模式、引擎模式、主机范围后，还可配置超时时间（检测可能会因为文件、目录过多等原因导致耗时较长）。



4. 单击【开始检测】后将按检测设置进行检测，单击【查看详情】可查看检测详情。





检测详情列表字段说明：

- 影响服务器 ：服务器的 IP 及名称。
- 操作系统 ：服务器的操作系统。
- 检测状态：检测完成、检测中、检测失败（原因：可能是检测超时失败，建议增加超时时间后重新检测；可能是客户端已离线，建议重启或重新安装客户端后重新检测）。
- 待处理风险：服务器检出待处理的风险文件数量。
- 检测开始时间：此次检测开始的时间。
- 检测结束时间：服务器检测结束的时间。
- 操作：
  - 重新检测：若想对检测状态处于检测完成、检测停止和检测失败的服务器再次检测，您可以单击【重新检测】。
  - 停止检测：若想对检测状态处于检测中的服务器停止检测，您可以单击【停止检测】，服务器将不会被检测，可能存在的风险，请谨慎操作。
- 查看详情：若想查看目标服务器的检测结果，您可以单击【查看详情】。

查看告警列表

1. 登录主机安全租户端控制台 ，在左侧导航栏中，选择【入侵检测】>【文件查杀】。
2. 在文件查杀页面，可查看当前受防护的服务器中木马文件的检测情况，如下图所示：



告警列表字段说明：

- 主机名称/实例ID：被检测的服务器名称和实例ID。
- IP地址 ：被检测的服务器IP地址。




- 路径：风险文件路径，单击 复制文件路径、单击 下载风险文件样本。
- 病毒名/检出引擎：入侵风险文件的病毒名。
- 首次发现时间：首次检出该风险文件的时间。

- 最近检测时间：最近一次检出该风险文件的时间。
- 处理状态：风险文件的处理状态，待处理状态的事件会提示最近一次检测该文件时，文件和进程的存在情况。
- 操作：
  - 详情：可查看恶意文件详情。
  - 隔离：隔离此病毒文件，让黑客无法再次启动它，便于您定位病毒文件位置，对其进行查杀。（注意：windows系统下，若该文件正在运行中，会导致隔离失败），支持隔离并杀掉该文件相关进程，建议勾选。
  - 标记已处理：建议您参照告警详情中的"修复建议"进行处理，处理后可将该告警标记为已处理。
  - 加入白名单：若您确认该进程运行属于正常行为，可将该进程添加白名单放行规则，后续再出现该进程运行，将直接放行不再拦截/告警。
  - 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
  - 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

常见问题

木马文件为什么隔离失败？

木马文件隔离失败，一般是由于木马文件对抗安全软件导致的，建议先自行删除服务器中的告警文件。若仍无法处理，请联系我们进行处理，Windows 系统也可尝试使用腾讯电脑管家进行查杀。

后续步骤

- Linux 入侵类问题排查指南，请参见 Linux 入侵类问题排查思路。
- Windows 入侵类问题排查指南，请参见 Windows 入侵类问题排查思路。

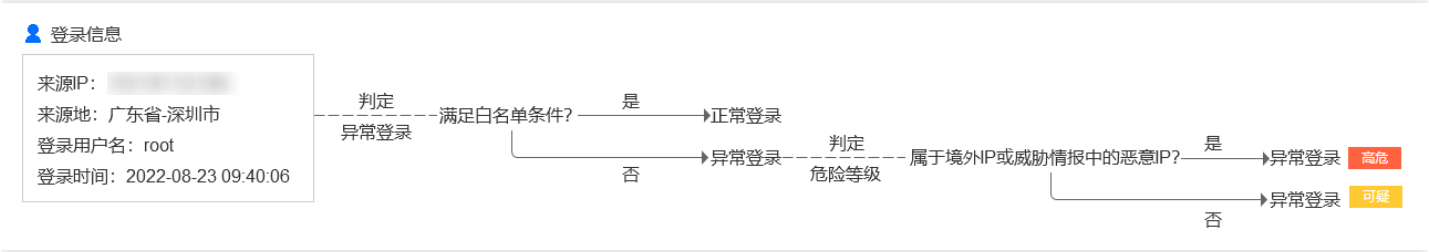
异常登录

最近更新时间: 2024-12-19 17:12:00

本文将为您介绍异常登录的功能和操作。

概述

当检测到存在不满足白名单（常用来源 IP、常用用户名、常用登录地、常用登录时间）的服务器登录行为，将产生异常登录告警。若异常登录来源 IP 属于境外 IP（含中国港澳台地区）或威胁情报中的恶意 IP，将被标记为“高危”，反之则标记为“可疑”。



限制说明

- 已安装主机安全客户端的主机（客户端在线），均会实时监控异常登录行为。
- 主机安全控制台仅保留近6个月的异常登录事件，过期的事件数据将不再展示。

操作指南

1. 登录主机安全租户端控制台。
2. 左侧导航中，选择【入侵检测】>【 异常登录】，各功能说明如下。

告警列表

在告警列表页面中，可查看并处理主机安全监测到的异常登录风险。



字段说明：

- 主机名称/实例ID：被异常登录的服务器。
- IP地址：被异常登录的服务器IP地址。
- 来源 IP：登录来源 IP，一般是公司网络出口 IP 或网络代理 IP。
- 来源地：登录来源 IP 所在的地域。
- 登录用户名：成功登录服务器时使用的登录用户名。
- 登录时间：成功登录服务器的时间（服务器上的时区时间）。
- 危险等级：可疑/高危。
- 状态
  - 异常登录：本次登录存在异常地域、异常用户名、异常登录时间或异常来源 IP 登录。
  - 已加入白名单：登录来源 IP 已被添加至白名单（登录源 IP、登录用户名、登录时间、常用登录地、生效范围的组合构成白名单判定规则）。
  - 已处理：用户已手动处理，并将该事件标记为已处理。
  - 已忽略：用户已忽略本次告警事件。
- 操作
  - 处理
    - 标记已处理：若您已人工对该风险事件进行处理，可将事件标记为已处理。
    - 加入白名单：加入白名单操作后，当再次发生相同事件时将不再进行告警，请谨慎操作。
    - 忽略：仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。
    - 删除记录：删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

白名单管理

在白名单管理页面中，可增/删/改/查异常登录的白名单。



字段说明：

- 服务器 IP/名称：该白名单生效的服务器。
- 来源 IP：加白名单的登录来源 IP。
- 常用登录地：加白名单的登录地。
- 登录用户名：加白名单的用户名。
- 登录时间：加白名单的登录时间段。
- 创建时间：该白名单的创建时间。
- 修改时间：最近一次修改白名单的时间。
- 操作
  - 编辑：可重新编辑登录源 IP、登录用户名、登录时间、常用登录地、生效范围等。
  - 删除：可对白名单进行删除操作。

热点问题

收到异常登录告警后该如何处理？

判断该登录行为是否自己操作。

- 若是自己的登录行为，且您不希望再看到告警，请单击【处理】选择【加入白名单】操作，对常见登录源 IP、登录用户名、登录地、登录时间、生效范围进行设置。



登录源 IP 为空：代表所有来源 IP 对服务器进行登录，均不产生告警。 登录用户名为空：代表对服务器的任何用户名进行登录，均不产生告警。 登录地为空：代表不论登录地域在哪，均不产生告警。 登录时间为空：代表不论何时登录，均不产生告警。

> **注意：**
>
> 登录源IP、登录用户名、登录地、登录时间不能同时为空。

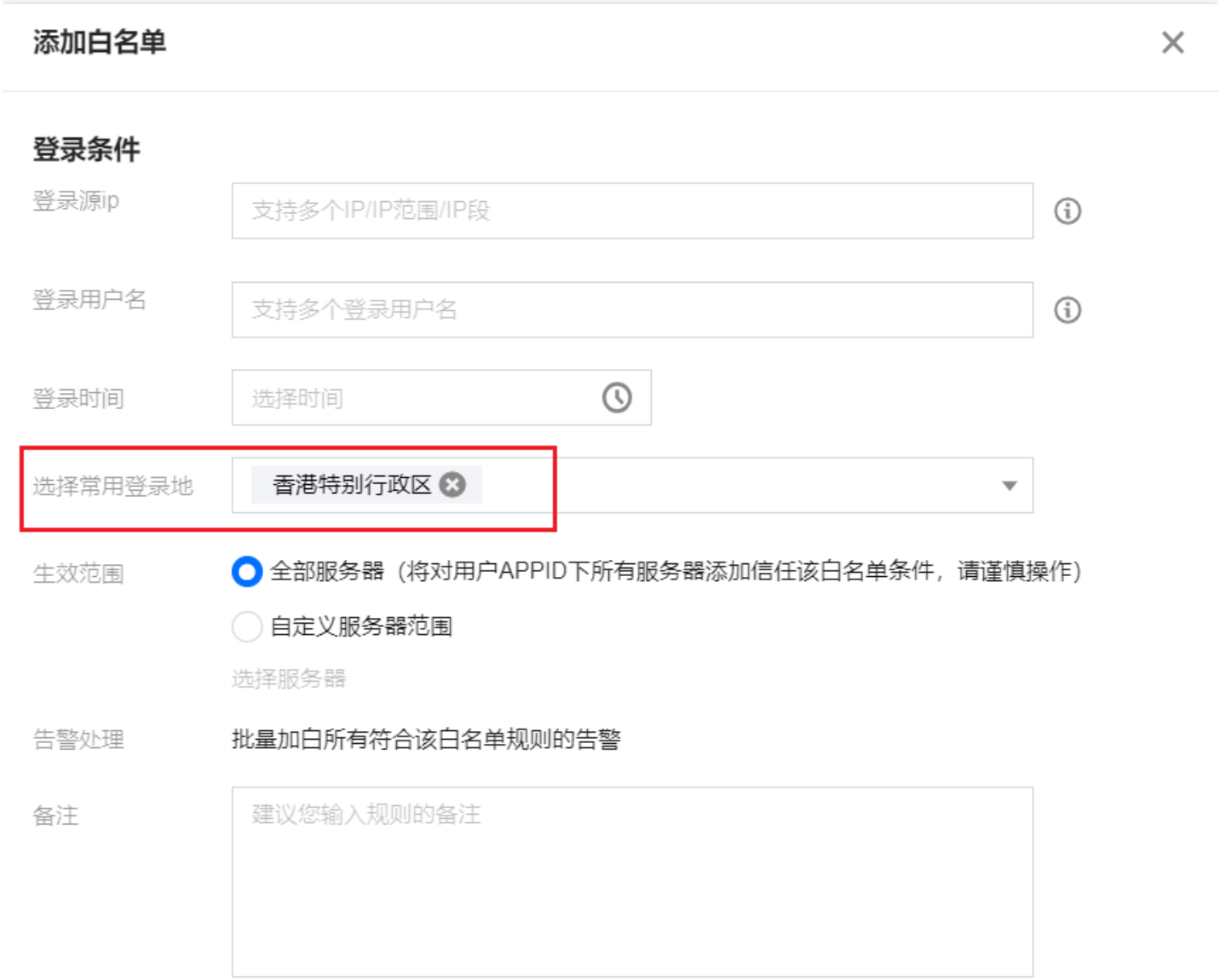
- 若不是自己的登录行为，请立即修改服务器登录密码（建议修改为10位以上，包含大小写字母和特殊字符的强密码）。 服务器被异常登录，登录者很有可能已经入侵您的服务器并留下恶意文件。建议您立即进行文件查杀、漏洞检测、基线检测以加固您的服务器安全。

白名单怎么设置可以满足大部分用户需求？

- 场景1：固定 IP 网段登录源可以使用任一用户名对服务器进行登录，而不产生异常登录告警。 您可在登录源 IP 中输入 IP 段，选择生效服务器范围即可。



- 场景2：登录源 IP 是动态变化的，要支持登录地是中国香港地区的 IP 随时都可以使用任一用户名对服务器进行登录，而不产生异常登录告警。 您可在常用登录地中选择香港特别行政区，选择生效服务器范围即可。



> **说明：**
>
> 登录条件支持组合。

如何关闭异常登录告警？

请前往【设置中心】>【告警设置】对异常登录的告警开关进行关闭。若保持告警开关开启，建议勾选高危选项，仅告警高危的异常登录行为即可。

告警设置

入侵防御

告警类型	告警状态	告警时间	告警项
文件查杀	开	全天 09:00 ~ 18:00	严重 高危 中危 低危 提示
异常登录	开	全天 09:00 ~ 18:00	高危 可疑
密码破解	开	全天 09:00 ~ 18:00	登录密码被破解成功
恶意请求	开	全天 09:00 ~ 18:00	服务器请求了恶意域名
高危命令	开	全天 09:00 ~ 18:00	高危 中危 低危
本地提权	关	全天 09:00 ~ 18:00	系统中出现低权限试图提高权限
反弹Shell	关	全天 09:00 ~ 18:00	服务器上出现Shell反向连接
网络攻击	开	全天 09:00 ~ 18:00	尝试攻击
Java内存马	开	全天 09:00 ~ 18:00	检测到JavaWeb服务进程中存在内存马
核心文件监控	开	全天 09:00 ~ 18:00	高危 中危 低危 无

密码破解

最近更新时间: 2024-12-19 17:12:00

主机安全密码破解基于网络安全防御和主机入侵检测能力，为主机提供密码暴力破解行为实时监控。

操作指南

查看密码破解事件

登录主机安全租户端控制台，在左侧导航中，选择【入侵检测】>【密码破解】，进入密码破解页面，可查看密码破解事件列表。



字段说明：

- 主机名称/实例ID：检测到存在密码破解行为的服务器名称和实例ID。
- IP地址：检测到存在密码破解行为的服务器IP地址。
- 来源 IP：攻击来源 IP 地址。
- 来源地：攻击来源 IP 所在地域。
- 协议：攻击者通过的协议，含 ssh/rdp。
- 登录用户名：攻击者登录使用的用户名。
- 端口：攻击者登录使用的端口。
- 首次攻击时间：主机安全首次监控到密码破解行为的时间。
- 最近攻击时间：该事件最近再次发生的时间。
- 尝试次数：攻击 IP 尝试密码破解的次数统计。
- 破解状态：破解成功、破解失败。
- 阻断状态：阻断、未阻断。
- 告警状态：待处理、已加入白名单、已处理、已忽略。
- 操作：
  - 标记已处理：若您已人工对该告警进行处理，可将告警标记为已处理。
  - 加入白名单：对当前告警的域名创建放行策略，当再次发生相同攻击时将不再进行告警，同时当前告警状态将变更为“已加白”。
  - 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。

- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

配置白名单

配置白名单后，属于白名单来源 IP 的密码破解行为将不会被阻断与告警，操作步骤如下：

1. 登录主机安全租户端控制台，在左侧导航中，选择【入侵检测 】> 【密码破解】，进入密码破解页面。
2. 在密码破解页面，单击【白名单管理】，进入白名单管理页面。
3. 在白名单管理页面，单击【添加白名单】，进入创建白名单页面中。



4. 在右侧弹出窗中，填写来源 IP 及生效范围。

> **注意：**
>
> 添加白名单后，该来源 IP 的密码破解行为将不会被阻断与告警，请慎重操作。若有非白名单来源 IP 尝试登录，并命中暴力破解规则时，系统将自动发出异常告警或阻断。

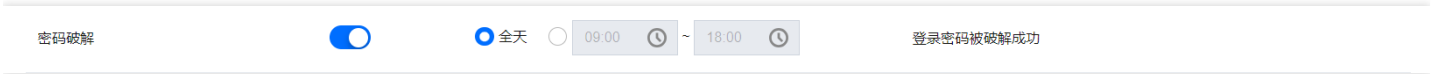


字段说明：

- 来源 IP：支持填写单个 IP、IP 范围（如1.1.1.1-1.1.1.10）或 IP 段（如1.1.1.0/24）。
- 生效范围：
  - 全部服务器（请谨慎选择）：将对用户 AppID 下所有服务器添加信任该白名单条件。
  - 自定义服务器范围：自定义选择添加信任该白名单条件的服务器范围。
- 备注：建议您输入相关规则备注。

开启告警通知

登录主机安全租户端控制台，在左侧导航中，选择【设置中心】>【告警设置】，在告警设置中，开启告警通知开关，当前产生密码破解事件时，会以站内信、短信、邮件、企业微信等方式进行通知。



密码破解事件处置指引

1. 当用户接收密码破解事件告警时，登录主机安全租户端控制台，在左侧导航中，选择【入侵检测】>【密码破解】，进入密码破解页面。
2. 查看告警事件列表中的对应攻击来源 IP。

- 若确认是可信来源 IP，用户需在该事件右侧操作栏中，单击【处理】 >【加入白名单】，设置白名单条件和生效范围（请谨慎添加白名单）。配置成功后，预计5分钟内生效，后续来自该来源 IP 的密码破解行为将不再进行告警或者阻断。



- 若确认是不可信来源 IP，且服务器已被攻击者密码破解成功。

  针对已被密码破解入侵的服务器，建议用户立即重新设置复杂密码（大写+小写+特殊字符+数字组成的12-16位的复杂密码），并检查账号列表中是否存在陌生账号，若存在陌生账号，需将陌生账号删除或者禁用，同时排查系统异常情况。

恶意请求

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍如何查看并操作恶意请求告警列表及策略配置。

背景信息

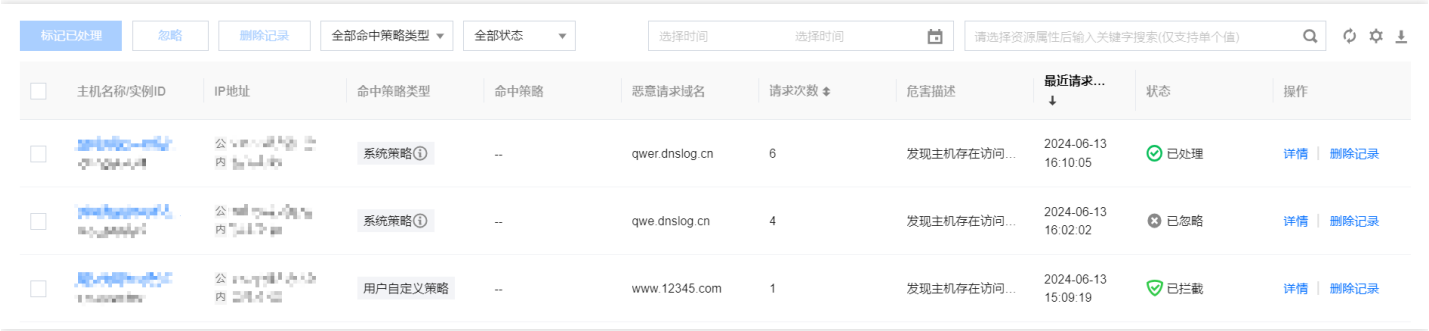
恶意请求功能提供对外界请求行为进行实时监控及处理的能力，有效识别恶意请求行为。若主机向恶意域名发起请求会被识别并记录，检测到此类恶意请求行为，系统会为您提供实时告警。

限制说明

- 恶意请求监测支持专业版、旗舰版主机。
- 恶意请求拦截仅支持 Linux 系统的旗舰版主机，且仅支持拦截服务器做 DNS 查询，不支持拦截流量上的转发。

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】 > 【恶意请求】，进入恶意请求页面。
2. 在恶意请求页面，可查看恶意请求告警列表，并进行相关操作。



- 筛选：支持按命中策略类型、状态、最近请求时间、搜索框输入主机名称、实例 ID、IP 地址、恶意请求域名进行筛选。



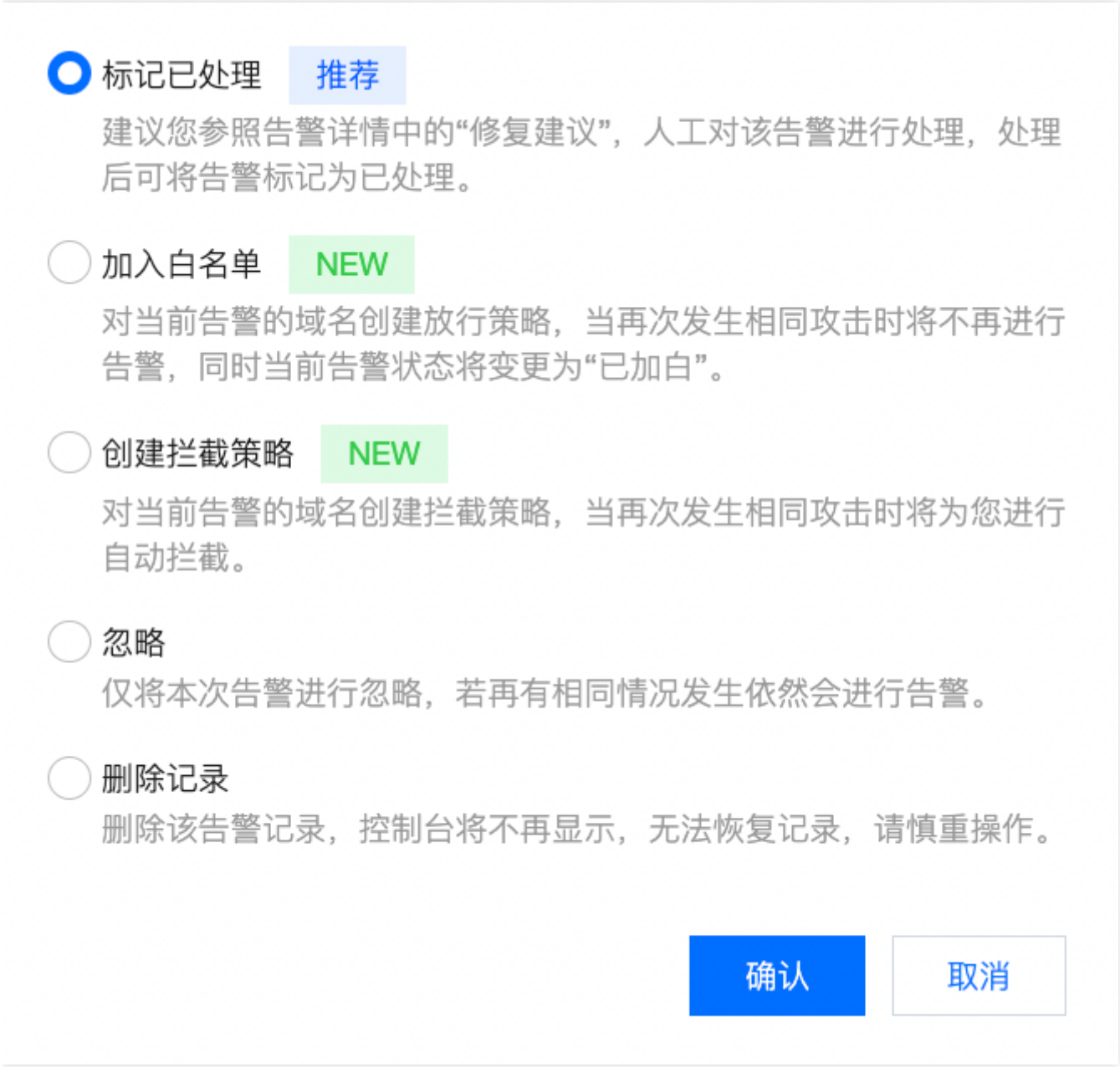
- 自定义展示列：单击 ，可设置告警列表展示字段。



- 导出：单击 ，可导出告警列表详细信息。
- 字段说明：
  - 主机名称/实例 ID：对恶意域名发起请求的主机名称及实例 ID
  - IP 地址：对恶意域名发起请求的主机IP
  - 命中策略类型：
    - 系统策略：系统策略为主机安全运营专家与算法专家经过多模型的规则配置，适用于大部分的恶意请求检测。
    - 用户自定义策略：用户根据业务情况对相关域名设置告警/拦截/放行动作。
  - 命中策略：主机请求恶意域名所命中的策略名称。
  - 恶意请求域名：域名或IP 地址
  - 请求次数：主机请求次数
  - 危害描述：请求该恶意域名可能造成的危害。
  - 最近请求时间：最近一次请求该恶意域名的时间。
  - 状态：待处理、已加白、已处理、已忽略、已拦截。
  - 详情：可查看该恶意请求事件的详细情况，含风险主机信息、恶意请求详情、危险描述、修复建议。



- 处理：标记已处理、加入白名单、创建拦截策略、忽略、删除记录。



策略配置

管理策略

在恶意请求页面上方选择【策略配置】，进入策略配置页面。



- 筛选：支持按策略类型、执行动作、生效状态、关键字进行筛选。
- 自定义展示列：单击 ，可设置策略列表展示字段。
- 导出：单击 ，可导出策略列表的详细信息。
- 字段说明：
  - 策略名称：系统策略固定名称，分别为：系统规则（重保）、系统规则（标准）；用户自定义策略则为用户所设置的策略名称。
  - 策略类型：系统策略、用户自定义策略。
  - 黑/白名单：该策略属于白名单/黑名单。
  - 域名详情：IP/域名或泛域名。
  - 生效主机：该策略生效的主机范围。
  - 更新时间：最近一次更新策略的时间。
  - 执行动作：请求访问域名时命中策略将自动执行的动作（放行/告警/拦截）。
  - 生效状态：策略是否生效。
  - 编辑：对策略进行编辑。
  - 删除：删除该策略。
- 创建策略：
  - 黑名单：当主机请求了黑名单中的域名，将执行告警/拦截动作。
  - 白名单：当主机请求了白名单中的域名，将执行放行动作。



注意：

- 系统策略是内置策略，不支持新增、编辑和删除，仅支持开关。
- 系统策略（标准）建议保持开启状态，系统策略（重保）建议在重保期间按需开启。
- 用户自定义策略中，拦截策略仅对旗舰版主机生效。

本地提权

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍如何对提权事件详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的提权行为。

背景信息

若出现以低权限进入系统，通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到主机安全。本地提权功能可实时监控您云服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

操作步骤

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测 】>【本地提权】，进入本地提权的事件列表标签页。
2. 在本地提权的【告警列表】标签页，可查看本地提权事件列表，并进行相关操作。 在【告警列表】标签页，可查看发生提权事件的主机名称/实例ID、 IP地址、提权用户、父进程、父进程所属用户、发现时间、状态等信息，列表展示字段支持自定义。

- **筛选事件**：本地提权事件列表支持选择日期查看相应的事件，支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）事件，同时支持按状态、筛选事件。



- **自定义设置列表字段**：在本地提权告警列表上方，单击设置图标，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。



- **事件导出**：在本地提权告警列表上方，单击 ，可将本地提权告警列表导出。
- **详情**：在本地提权事件的右侧操作栏，单击【详情】，可查看本地提权事件详情。

本地提权详情 待处理

标记已处理 | 加入白名单 | 忽略 | 删除记录

告警详情 | 进程树 NEW

风险主机

主机名称 [redacted] • 客户端在线
实例 ID [redacted]
公 [redacted] 内 [redacted]

发现时间 2024-06-13 15:22:30
提权主机 10.0.0.46

进程提权信息

进程名
test10

标签特征 -

启动用户 root
用户所属组 1000
新增权限 [redacted]

文件权限 [redacted]
文件路径 [redacted]

危害描述

告警描述 黑客在入侵服务器后，为了进行下一步的恶意操作，会通过特定漏洞提升用户权限，或者直接获取root用户权限。

修复建议

建议方案
1、检查系统是否被添加新用户，或者存在异常权限用户；
2、检查恶意进程及非法端口，删除可疑的启动项和定时任务；
3.隔离或者删除相关的木马文件；
4.对系统进行风险排查，并进行安全加固。

参考链接 暂无

- 标记已处理：若您已人工对该告警进行处理，可将告警标记为已处理。
- 加入白名单：对当前告警服务器添加白名单提权进程，后续再检测到相同提权行为将不再告警。
- 忽略：仅将本次告警进行忽略，若有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请谨慎操作。

白名单管理

本地提权功能支持添加白名单，通过设置白名单提权条件，将满足条件的事件标记为白名单。

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】>【本地提权】，进入本地提权页面。
2. 在本地提权页面，选择【白名单管理】>【添加白名单】。



3. 在添加白名单弹窗中，设置提权条件，包括：带 S 权限的进程、自定义提权进程（支持多个进程名，以英文逗号分隔，例如 123.exe,test.exe），同时选择该条件覆盖的服务器范围，单击【确定】。

> **注意：**
>
> - s 权限： 设置使文件在执行阶段具有文件所有者的权限，相当于临时拥有文件所有者的身份。
> - 勾选两个条件时，需要同时满足才能命中白名单。
> - 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。



4. 设置完成后，可在白名单管理列表查看该条件，告警列表中满足该条件的事件即会被标记为白名单事件。
5. 在白名单管理页面，可对白名单进行筛选删除等操作。

- 筛选：已配置的白名单支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）筛选，同时支持按是否带 S 权限进行筛选。



- 自定义设置列表字段：在白名单列表上方，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- 编辑：在目标白名单的右侧操作栏，单击【编辑】，可对已创建的白名单进行编辑。



- **删除**：在白名单列表中，支持对已配置的白名单进行删除。



反弹Shell

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍如何对反弹 Shell 详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的反向连接行为。

背景信息

反弹 Shell 功能是基于多维度多手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

操作步骤

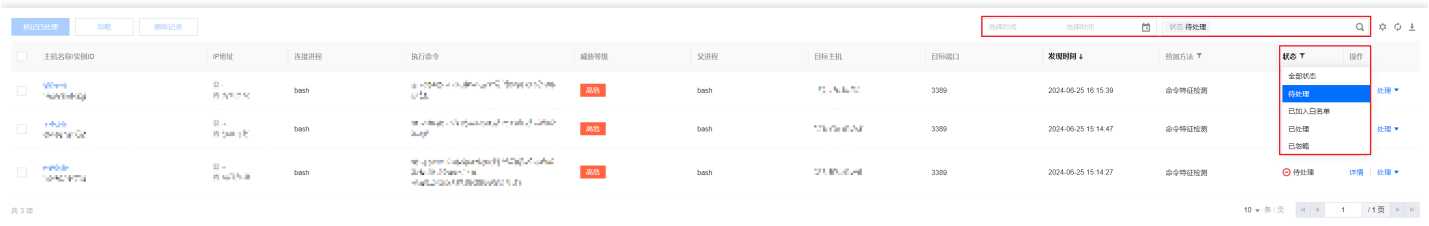
告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】>【反弹 Shell】，进入反弹 Shell 告警列表页。

2. 在反弹 Shell 【告警列表】标签页面，可查看反弹 Shell 事件列表，并进行相关操作。

   可查看发生反弹 Shell 的主机名称/实例ID、IP地址、连接进程等信息，列表展示字段支持自定义。

- **筛选**：反弹 Shell 告警列表支持选择日期查看相应事件，支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）事件，同时支持按状态（全部、待处理及已确认）筛选告警。



- **自定义设置列表字段**：在反弹 Shell 告警列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- **事件导出**：在反弹 Shell 告警列表上方，单击 ，可将反弹 Shell 告警列表导出。
- **详情**：在目标反弹 Shell 事件的右侧操作栏，单击【详情】，可查看反弹 Shell 事件详情。



- 标记已处理：建议您参照告警详情中的“修复建议”，人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：加入白名单操作后，当再次发生相同情况时将不再进行告警，请谨慎操作。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

白名单管理

反弹 Shell 支持添加白名单，通过设置白名单条件，将满足条件的事件标记为白名单。

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】>【反弹 Shell】，进入反弹 Shell 页面。
2. 在反弹 Shell 页面，选择【白名单管理】 > 【添加白名单】。



3. 在添加白名单弹窗中，设置反弹 Shell 条件，包括：目标主机、自定义连接进程（支持多个进程名，以英文逗号分隔），同时选择该条件覆盖的服务器范围，单击确定。



字段说明：

- IP 地址格式：单个 IP（127.0.0.1）、IP 范围（127.0.0.1-127.0.0.254）、IP 网段（127.0.0.1/24）。
- 端口格式：80,8080（支持多个端口并以英文逗号分隔，不限端口请留空）。
- 勾选两个条件时，需要同时满足才能命中白名单。
- 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。

4. 设置完成后，可在白名单管理列表查看该条件，告警列表中满足该条件的事件会被标记为白名单事件。

5. 在白名单管理页面，可对白名单进行筛选删除等操作。

- 筛选：已配置的白名单支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）筛选。



- 自定义设置列表字段：在白名单列表上方，单击 ，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。



- 编辑：在目标白名单的右侧操作栏，单击【编辑】，可对已创建的白名单进行编辑。



- 删除：在白名单列表中，支持对已配置的白名单进行删除。



高危命令

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍如何查看并操作高危命令事件列表。

背景信息

基于多维度多种手段，主机安全可对系统中的命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分，若检测出高危命令，系统会向您提供实时告警通知。

操作步骤

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵检测】>【高危命令】，进入高危命令的告警列表标签页。
2. 在高危命令的【告警列表】标签页，可查看高危命令告警列表，并进行相关操作。在告警列表界面可展示发生高危命令告警的主机名称/实例ID、IP地址、命中策略类型、命中策略、威胁等级等信息，列表展示字段可进行自定义。

- **筛选**：高危命令告警列表支持选择日期查看，支持按关键字及标签查询（多个关键字用竖线 “|” 分隔，多个过滤标签用回车键分隔）事件，同时支持按威胁等级及状态筛选事件。



- **自定义列表字段**：在高危命令事件列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- **事件列表导出**：在高危命令告警列表上方，单击 ，可将高危命令告警列表导出。
- **详情**：单击【详情】，可查看高危命令告警详情及进程树信息。



- 标记已处理：建议您参照告警详情中的“修复建议”，人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：对当前告警的域名创建放行策略，当再次发生相同攻击时将不再进行告警，同时当前告警状态将变更为“已加白”。
- 创建拦截策略：对当前告警的域名创建拦截策略，当再次发生相同攻击时将为您进行自动拦截。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

策略配置

创建自定义策略

高危命令功能支持创建自定义策略，通过设置策略对威胁命令进行相应的处理行为。

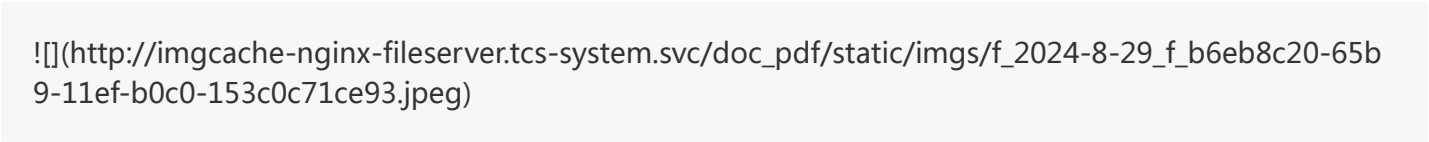
1. 登录主机安全租户端控制台 ，在左侧导航栏选择【入侵检测】>【高危命令】，进入高危命令页面。
2. 选择【策略配置】>【创建策略】，进入创建策略页面。
3. 在创建策略页面，填写策略的基本信息，包括策略名称、策略描述和启用状态。



4. 填写策略详情，包括选择黑名单/白名单及其对应的执行动作，填写正则表达式，选择威胁等级，选择生效主机范围。

- 黑名单规则，指发现主机存在威胁命令时将产生告警通知。

> **说明**
>
> - 拦截策略指当发现主机存在威胁命令时，将对威胁命令的执行进行自动拦截，并告警通知。
> - 拦截策略仅支持旗舰版机器。



- 白名单规则，指对威胁命令进行放行，不再产生告警或拦截行为。

> **说明**
>
> - 若生效主机范围选择全部专业版或旗舰版主机，新增专业版或旗舰版主机时，将自动加入策略生效范围。
> - 可勾选对符合本策略规则的历史“待处理”告警，执行本策略规则的操作。

5. 设置完成后，可在策略列表查看，列表中应用于黑名单的策略会被标记为相应的威胁等级。

6. 在策略列表中可对策略进行筛选、编辑和删除等操作。



- **筛选**：已配置的策略支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）筛选，支持按威胁等级（全部/高危/中危/低危/无），支持按执行动作（告警/拦截/放行），支持按生效状态（已生效/未生效）进行筛选。

- **自定义设置列表字段**：在策略列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。
- **启用状态**：列表支持设置策略的启用状态，可在启用状态列，单击【启用开关】，决定该策略是否启用。
- **编辑**：在策略列表的右侧操作栏，单击【编辑】，可对已创建的策略进行编辑。
- **删除**：在策略列表中，支持对已配置的策略进行删除。

系统策略

高危命令功能新增系统自动拦截规则，开启后，支持自动拦截检测出的系统高危命令，部分内容仍需您手动配置策略。

- 系统高危命令：主机安全运营专家与算法专家经过沉淀的系统高危命令，此名单中的高危命令可进行自动拦截。
- 拦截原理说明：高危命令自动拦截采用查杀命中规则的进程的方式，例如，如果进程 A 尝试创建一个"/bin/bash -i"进程（假设"bash -i"已被列入黑名单），那么这个尝试创建的"/bin/bash"进程将会被终止（或创建失败），而进程 A 本身不会受到影响。

> **说明：**

- 如您发现误拦截情况，可创建自定义策略进行加白处理。
- 系统自动拦截规则仅限旗舰版主机使用。

网络攻击

最近更新时间: 2024-12-19 17:12:00

网络攻击基于安全攻防团队技术支持，为您自动化监测恶意流量。结合入侵过程中产生的恶意行为。实时对攻击和告警进行自动化关联分析，输出攻击流量数据、通知攻击事件。本文档将为您介绍如何查看和处理网络攻击告警。

限制说明

- 检测对象：仅支持专业版/旗舰版的 Linux 主机。
- 检测范围：仅检测部分出现 EXP、且在云上有攻击成功案例的热点漏洞攻击行为。
- 漏洞防御：仅支持旗舰版的 Linux 主机。

防御状态说明

- 支持漏洞防御（未开启）：主机安全支持防御该漏洞，但该主机未对该漏洞开启防御。
- 支持漏洞防御（已开启）：主机安全支持防御该漏洞，且该主机已对该漏洞开启防御。
- 暂不支持漏洞防御：主机安全不支持防御该漏洞。

> 注意：
>
> - 漏洞防御未开启可能原因：防御开关未开启、该主机非旗舰版或不在防御主机范围内。
> - 存在攻击事件表示当前有黑客利用该漏洞的攻击手法进行攻击，并不表示当前机器存在此漏洞。

告警统计

1. 登录主机安全租户端控制台，在左侧导航栏，选择【入侵防御】>【网络攻击】。

2. 在网络攻击页面，支持查看网络攻击中漏洞防御状态，待处理告警相关数据统计及 Top5 情况。



字段说明：

- 漏洞防御状态：体现漏洞防御开关的状态。
- 待处理网络告警：当前待处理的告警数量。
- 受攻击资产：当前待处理告警所涉及到的受攻击资产数。
- 受攻击端口：当前待处理告警所涉及到的受攻击端口数。
- 攻击来源 IP：当前待处理告警的攻击来源 IP 数。

查看告警

在网络攻击页面，支持查看网络攻击详情，包括主机名称/实例 ID、IP 地址、目标端口等信息。



字段说明：

- 主机名称/实例 ID：受攻击的主机的名称和实例 ID。
- IP 地址：指受攻击主机的公网/内网IP。
- 目标端口：受攻击端口。
- 攻击来源 IP/地址：指攻击者的来源 IP及所在地。
- 漏洞名称：指攻击者有利用某漏洞的攻击手法进行攻击，以及目前漏洞防御的开启状态。
- 攻击状态：指攻击者攻击后的结果，尝试攻击（被攻击但未被攻击成功）、攻击成功（实锤攻击）。
- 最近攻击时间：最近检测到攻击行为的时间。
- 攻击次数：累计检测到相同攻击的次数。

- 处理状态：待处理、已处理、已加白、已忽略。
- 详情：支持查看告警详情、危害描述、解决方案。



建议方案

1. 建议相关应用部署WAF防护/云防火墙防护/开启漏洞防御
2. 如果端口应用不需要对外，通过云防火墙或者安全组限制端口对公网暴露
3. 若该告警为自行扫描，则可通过添加来源IP到白名单来过滤告警。

处理告警

1. 在网络攻击告警列表中，单击操作列的【处理】。

> **说明：**
>
> 选中一个或多个告警，可以单击左上角的【标记已处理】【忽略】【删除记录】，进行批量操作。



2. 支持对待处理的告警标记已处理、开启漏洞防御、加入白名单、忽略、删除记录操作。

- 标记已处理：人工对该告警进行处理，处理后可将告警标记为“已处理”。
- 加入白名单：将攻击来源IP加入白名单，后续主机安全将不再对该来源IP的网络攻击行为进行告警，请谨慎操作。



- 忽略：仅将本次告警进行忽略，若再有相同情况发生仍然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

Java内存马

最近更新时间: 2024-12-19 17:12:00

概述

主机安全支持实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合安全攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 > 【Java 内存马】，进入 Java 内存马页面。
2. 选择【插件配置】，插件配置是监测 Java 内存马的前提，您可对旗舰版主机进行插件的开启和关闭，并观测插件的具体运行状态。

> **说明：**
>
> - 启用 Java 内存马插件后，主机安全会自动检测主机上 JavaWeb 服务进程，并注入检测探针到服务进程中，实时监控黑客通过漏洞、Shell 等注入的 Java 内存马。
> - 已成功注入 Java 内存马插件的主机，将实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合安全攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。



字段说明：

- 启用/关闭插件：Java 内存马插件默认关闭，支持用户手动设置开关，可单主机设置，也可多选主机批量设置。
- 插件状态：全部正常、存在异常、未开启。
- 首次开启时间：指首次启用插件的时间。
- 更新时间：指近期启用或关闭插件的时间。

- 详情：可查看当前已注入的 Java 内存马插件运行状态，包括进程 PID、进程主类名、插件状态（注入中、注入成功、插件超时、插入退出、注入失败）、注入日志。

启用 Java 内存马插件后，您可选择【告警列表】查看检测到的 Java 内存马事件，并进行相关处理操作。



字段说明：

- 主机名称/实例ID：被检出存在 Java 内存马的主机名称和实例ID。
- IP地址：被检出存在 Java 内存马的主机IP地址。
- Java 内存马类型：包括 Filter 型、Listener 型、Servlet 型、Interceptors 型、Agent 型、其他。
- 说明：归纳说明 Java 内存马的概况。
- 首次发现时间：该 Java 内存马首次被检测到的时间。
- 最近检测时间：近期检测发现该 Java 内存马仍存在的时间。
- 状态：待处理、已处理、已忽略。
- 操作：
  - 单击【详情】可查看该内存马事件详情。



- 单击 Java 内存马详情中的【查看文件】，可查看落地文件的反编译 Java 文件，支持复制，支持下载反编译 Java 文件或原 Class 文件。



- 单击【处理】可对事件进行标记已处理、忽略、删除记录操作，可单事件处理，也可多选事件批量处理。



核心文件监控

最近更新时间: 2024-12-19 17:12:00

核心文件监控的监控规则分为系统规则和自定义规则。系统规则为主机安全运营专家与算法专家经过多模型沉淀的规则配置，适用于大部分的篡改用户配置监控需求，您也可以根据业务需要自定义规则，自定义规则支持编辑、复制和删除。

> **说明：**
>
> - 核心文件监控属于主机安全旗舰版功能。
> - 核心文件监控目前支持 Linux 内核版本为3.10及以上的操作系统。

新建规则

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 >【核心文件监控】。
2. 在【监控规则配置】页面中，单击左上角处的【新增规则】，右侧弹出新增规则弹窗。
3. 在新增规则弹窗中，依次配置基础设置、规则内容设置和生效服务器范围参数。

- 基础设置



字段说明：

  - 规则名称：自定义名称。
  - 威胁等级：根据实际需求可选择高危、中危、低危或无。
  - 启用状态：可启用或不启用该新增规则。

- 规则内容设置：单击【添加规则】，可添加多行，最大添加20行。



字段说明：

- 监控行为：修改文件/读取文件。
- 进程路径：文件篡改动作发起的进程文件路径，例如程序 /usr/bin/vi，对应规则可以是 */vi。
- 文件路径：例如 /etc/cron.d/attack 对应规则可以是 /etc/cron.d/*。
- 执行动作：告警指的是对文件系统变化产生自动告警事件，记录事件详情；放行指的是对文件系统变化产生事件进行放行操作，记录事件详情。

> **说明：**
>
> 当告警放行进程路径及被访问文件一致，且生效服务器有重叠，重叠部分服务器不产生告警（即优先以放行条件为准）。
>

- 生效主机范围：可根据实际需求选择全部服务器或自选服务器。

4. 配置完成后，单击【保存】即可。

管理规则

编辑规则

1. 在【核心文件监控】>【监控规则配置】中展示了已新增的规则，操作列支持【复制】【编辑】【删除】。



> **注意：**
>
> 删除后，规则将无法恢复，请谨慎操作。

告警列表

告警列表支持查看核心文件异常告警记录，可对告警记录进行处理（标记已处理、加入白名单、忽略），也可对告警记录进行删除。

处理告警记录

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 > 【核心文件监控】。

2. 在【告警列表】页面，选择所需告警记录，单击【处理】，选择标记已处理、加入白名单、忽略或删除记录。



字段说明：

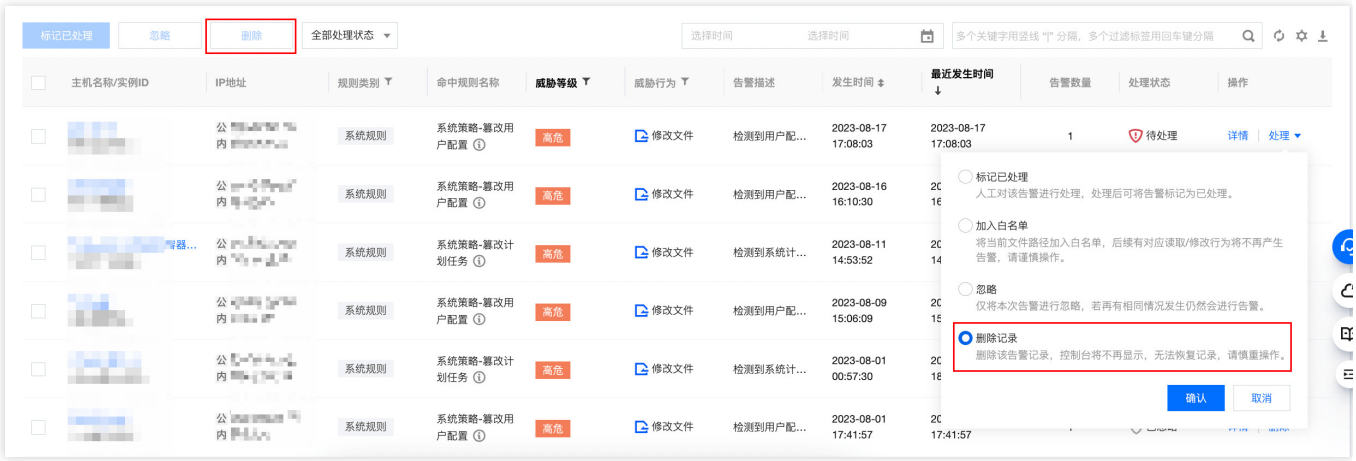
- 标记已处理：人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：将当前文件路径加入白名单，后续有对应读取/修改行为将不再产生告警，请谨慎操作。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生仍然会进行告警。

- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

删除告警记录

1. 在【告警列表】页面，支持单个删除告警记录或批量删除告警记录。

- 单个：选择所需告警记录，单击【删除】，弹出确认删除对话框。



- 批量：选择一个或多个告警记录，单击左上角的【删除】，弹出确认删除对话框。



2. 在确认删除对话框中，单击【确定】，即可删除所选告警记录。

> **说明：**
>
> 删除的告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

漏洞管理

最近更新时间: 2024-12-19 17:12:00

漏洞管理旨在帮助客户扫描系统中存在的安全漏洞并提供漏洞信息及修复建议等信息，部分漏洞可开启精准防御、可自动修复。本文档将为您介绍如何进行漏洞管理。

限制说明

- 漏洞管理范围说明如下：

漏洞管理功能	漏洞类型	Linux 系统	Windows 系统
漏洞扫描 专业版、旗舰版主机适用	Linux 软件漏洞	✓	×
	Windows 系统漏洞	×	✓
	Web-CMS 漏洞	✓	✓
	应用漏洞	✓	✓
漏洞防御 旗舰版主机适用	Linux 软件漏洞	×	×
	Windows 系统漏洞	×	×
	Web-CMS 漏洞	✓仅支持部分漏洞	×
	应用漏洞	✓仅支持部分漏洞	×
漏洞自动修复 旗舰版主机适用	Linux 软件漏洞	✓ 仅支持部分漏洞	×
	Windows 系统漏洞	×	×
	Web-CMS 漏洞	✓ 仅支持部分漏洞	✓ 仅支持部分漏洞
	应用漏洞	×	×

- 因漏洞修复可能对用户业务造成影响，漏洞自动修复并非检出漏洞后立即进行自动化修复，须用户了解漏洞后单击【修复】并进行数据备份，才可进行自动化修复。

漏洞扫描

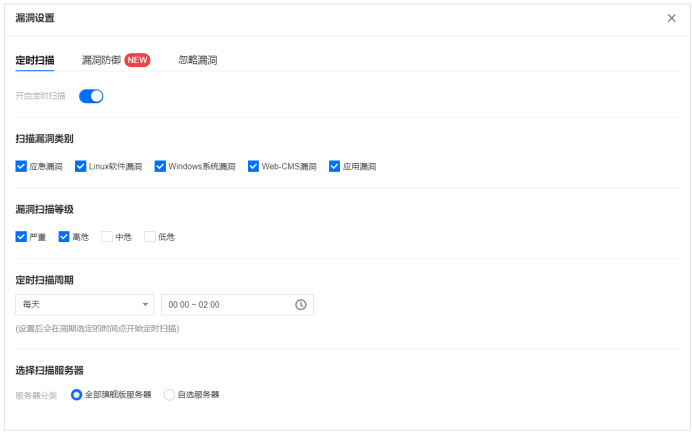
1. 登录主机安全租户端控制台，单击左侧导航中的【漏洞管理】。

2. 在漏洞扫描模块中，支持一键扫描、定时扫描设置。



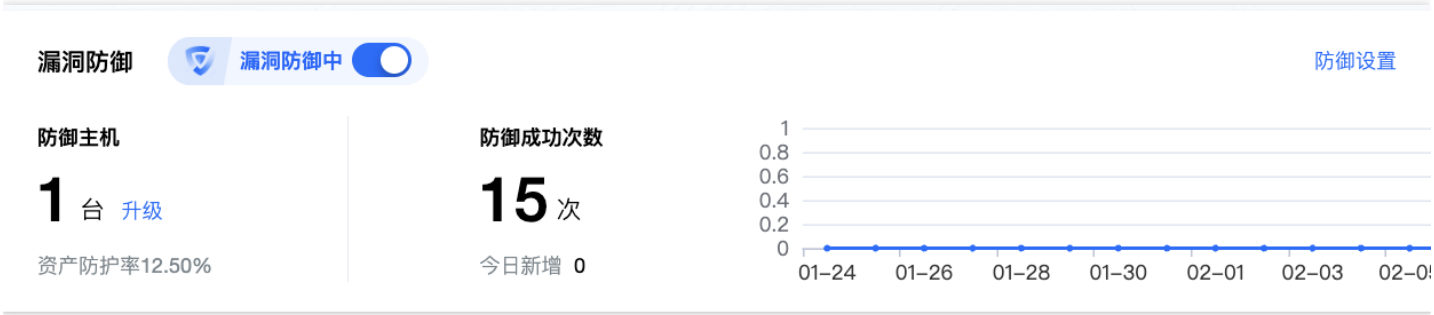
- 单击【一键扫描】**，**将打开一键扫描设置弹窗，您可对本次扫描的漏洞类别、漏洞等级、扫描超时时长、扫描服务器范围进行设置。
- 单击【扫描设置】将打开漏洞设置弹窗并锚点至【定时扫描】，您可对定时扫描开关、周期、漏洞等级及漏洞类别进行设置。
- 单击【详情】可查看上一次扫描的详情，并支持下载 PDF 扫描报告、Excel 扫描结果。





漏洞防御

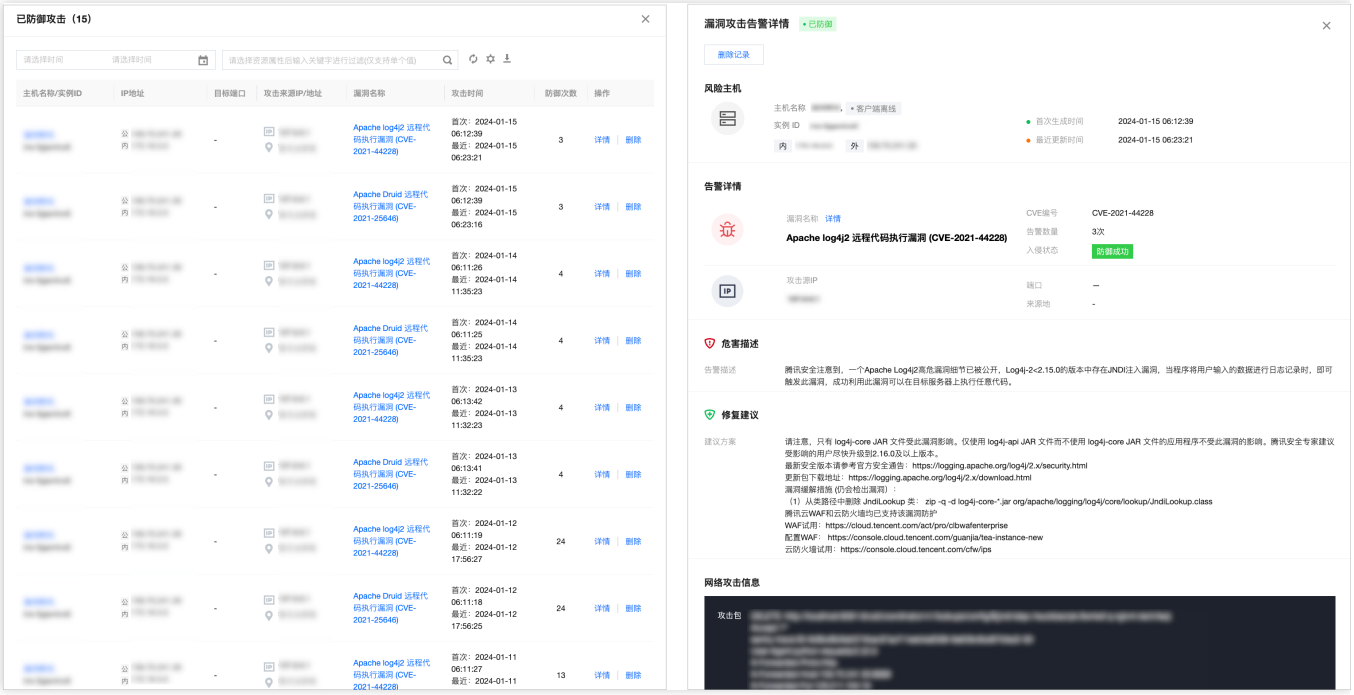
在【漏洞防御】模块中，支持漏洞防御开关启停、查看防御主机台数、防御成功次数及防御趋势情况。



- 单击【防御设置】将打开漏洞设置弹窗并锚点至【漏洞防御】，您可设置漏洞防御开关、查看可防御漏洞、选择防御主机范围、查看防御插件详情。



- 单击【防御成功次数】，您可查看当前已成功防御的攻击，且可查看攻击详情。



漏洞处置

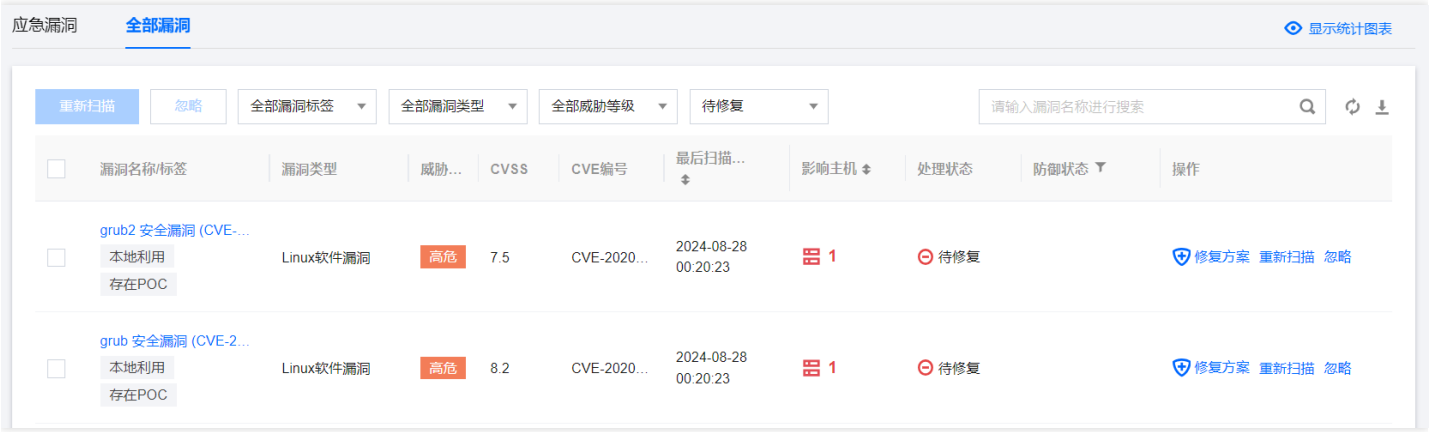
1. 在漏洞管理页下方，您可查看当前检出漏洞的统计情况及详细漏洞列表。
2. 在**【**漏洞概览】**模块中，展示了漏洞检出情况、网络攻击事件次数及今日新增情况，并展示了主机安全漏洞库总数。



字段说明：

- 全部漏洞：检出 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞的数量总和。
- 影响主机：检出漏洞的主机数量。
- 网络攻击事件：统计近1个月内网络攻击事件的数量。
- 已支持漏洞：可查看主机安全支持检测的漏洞库，每日最多可检索20次，单次搜索最多可展示100条结果。

3. 在【漏洞列表】模块中，展示当前检出的具体漏洞，已分为应急漏洞、全部漏洞2类，二者功能无太大差异，下面以【全部漏洞】举例，为您介绍漏洞处置。



字段说明：

- 漏洞名称/标签：漏洞名称指当前检出的漏洞，标签指该漏洞的标签（如：远程利用、服务重启、存在 EXP 等）。
- 漏洞类型：Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。
- 威胁等级：严重、高危、中危、低危。
- CVSS：指通用漏洞评分系统的评分，分数范围从0到10，0代表最不严重，10代表最严重。
- CVE 编号：公共漏洞暴露库中，识别该漏洞的唯一编号。
- 最后扫描时间：最近一次扫描到该漏洞的时间。
- 影响主机：存在该漏洞的主机数量。
- 处理状态：待修复、修复中、扫描中、已修复、已忽略。
- 防御状态：防御中。
- 操作
  - 修复方案：暂不支持自动修复的漏洞，可单击【修复方案】打开漏洞详情弹窗，根据修复方案手动修复漏洞。
  - 自动修复：部分 Linux 软件漏洞、Web-CMS 漏洞支持自动修复，可单击【自动修复】打开漏洞详情弹窗，选择需要修复的服务器进行修复。
  - 更多：重新扫描（重新对该漏洞进行扫描）；忽略（对该漏洞进行忽略，后续不再对该主机扫描该漏洞）。

安全基线

最近更新时间: 2024-12-19 17:12:00

本文档将介绍如何使用基线管理功能，帮助您管理服务器中的基线安全。

背景信息

云平台主机安全支持对基线检测项进行定期检测和一键检测，支持对指定主机上的指定基线项进行检测，支持通过检测策略了解基线通过率及风险情况，提供基线和检测项的风险等级和修复建议，提供默认基线策略，有助于您更好的管理服务器中的基线安全。

操作指南

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【基线管理】>【安全基线】，进入安全基线页面。
2. 在安全基线页面提供基线策略的设置、周期性检测和指定策略的一键检测功能，支持查看基线策略的通过率和风险状况，以及基线检测结果列表，并可查看基线和检测项详情信息及修复方案，可对指定服务器检测项进行忽略。

基线策略

基线策略是基于用户自定义设置的基线检测项的集合，基于策略维度了解基线的通过率及风险情况。

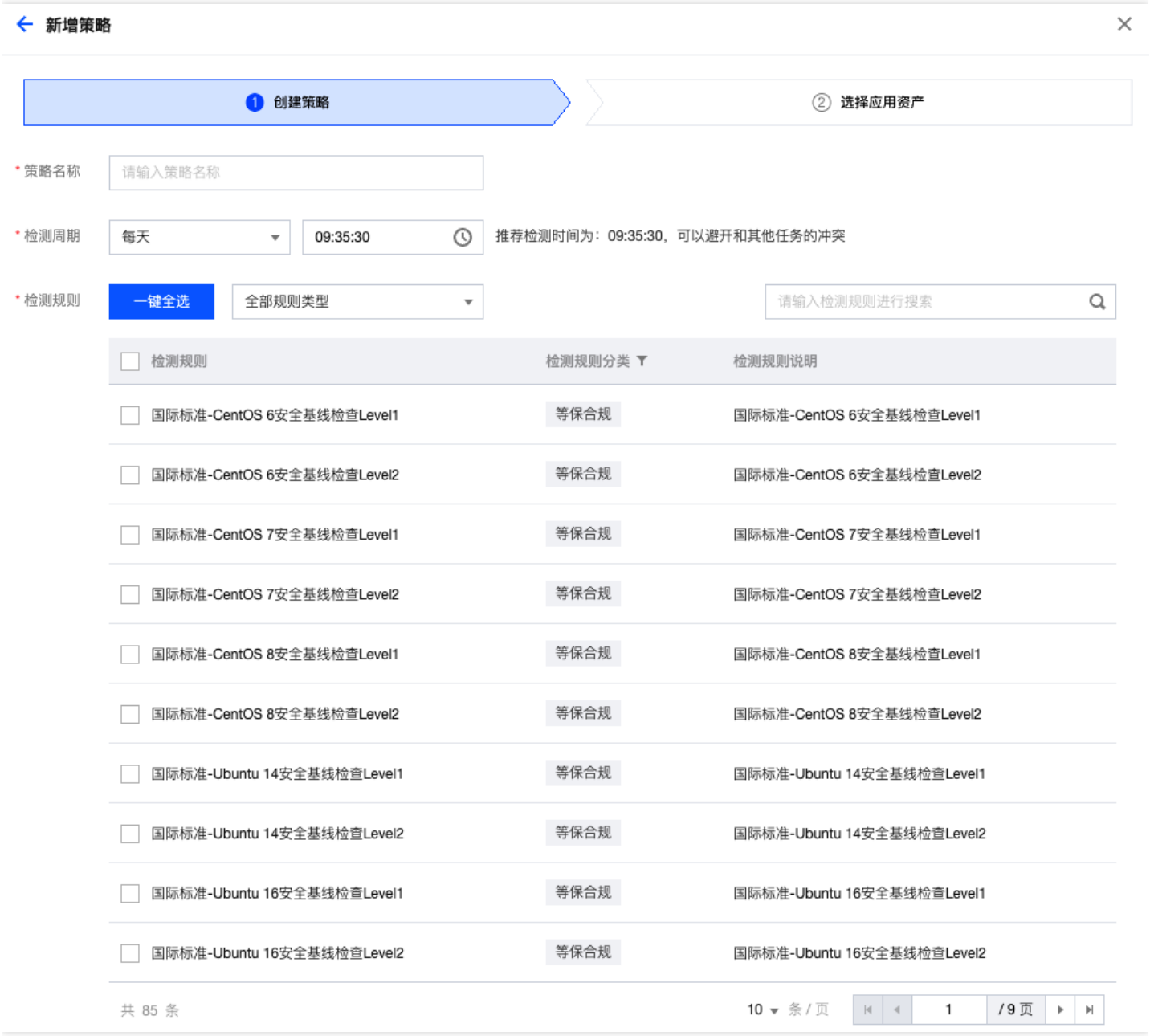
- **云平台默认基线策略**：云平台主机安全根据网络安全主流的基线检测内容为您提供默认基线检测策略，包括：国际标准基线、弱密码、未授权访问、等保二级、等保三级、云安全标准策略。您可以增加默认基线策略中的检测项和需要检测的服务器，该策略默认每隔7天，第7天晚上0点检测全量专业版或旗舰版服务器。
- **新增基线策略**

1. 在安全基线页面右上角，单击【基线检测设置】。
2. 在【检测策略设置】中，单击【新增策略】。



3. 在新增策略弹窗中，输入策略名称（不允许与现存策略名称重复）、选择检测周期、基线选项及应用资产，单击【保存】并更新。

> **说明：**
>
> 主机安全最多支持创建20个基线策略，达到20个后则不允许再创建，但您可以删除现有基线后，再次创建。



基线检测

主机安全支持对基线检测项的定期检测和一键检测，支持对指定云服务器上的指定基线项进行检测。

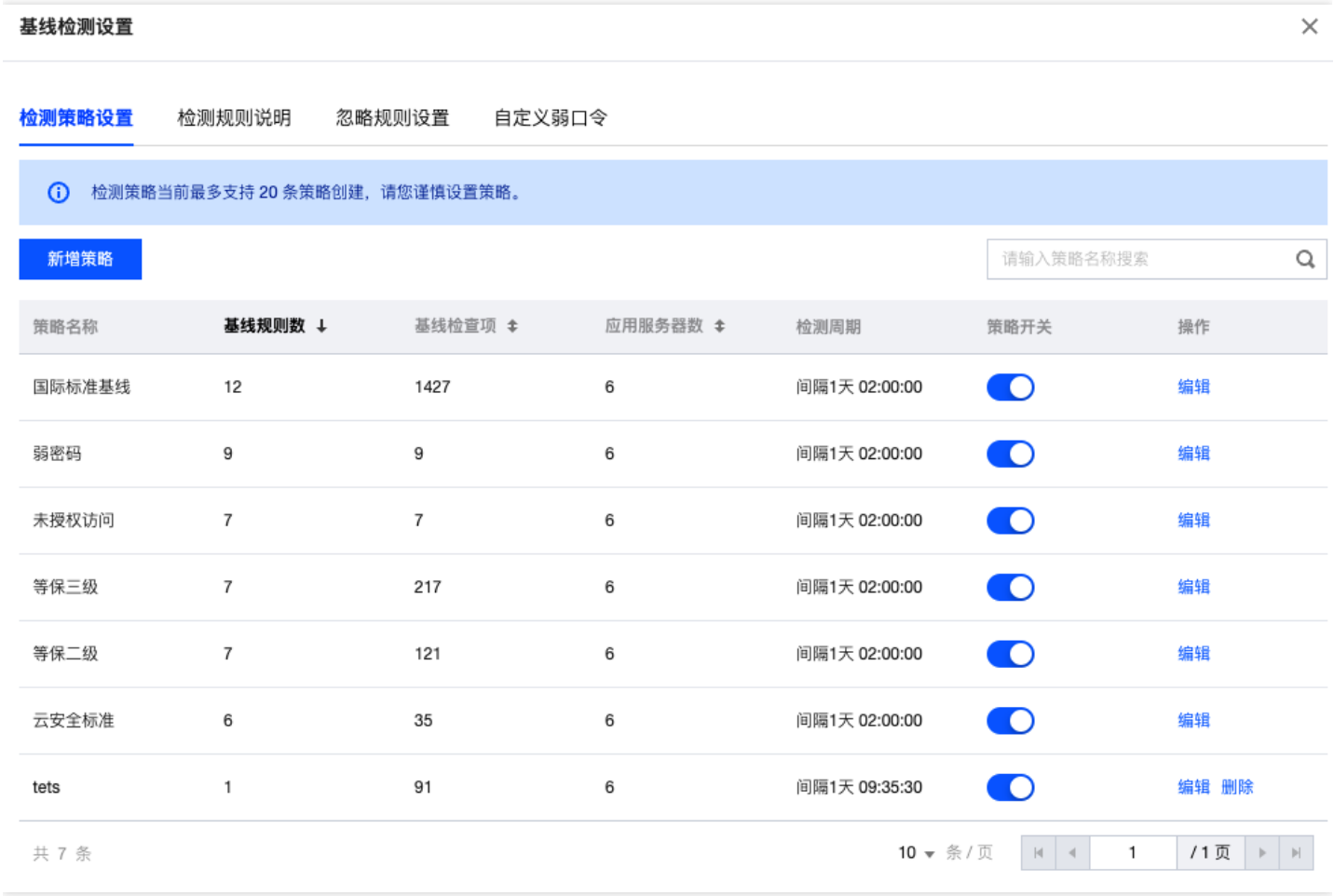
- **一键检测**

1.单击【一键检测】，选择需要检测的基线策略下发检测（检测一般持续2 - 5分钟），检测完成后，检测结果会显示在安全基线页下方。



- **周期检测**

1. 在安全基线页右上角，单击【基线检测设置】。
2. 在检测策略设置中，可以进行周期检测设置。



基线检测结果列表

在安全基线页面下方，可查看基线检测结果列表，支持查看基线检测详情，支持对单个基线进行模糊搜索和状态筛选，并支持对所有表格进行下载。



字段说明：

- 检测规则名称：基线检测规则名称，包含若干相同类别的检测项。
- 具体检测项：该检测规则下所有的检测项合计数量。
- 检测服务器数：该检测规则检测过的服务器数量。
- 最后检测时间：最近一次进行该检测规则检测的时间。

- 处理状态：未通过、已通过。
- 操作：
  - 重新检测：可重新对该检测规则进行检测。
  - 查看详情：可查看服务器检测结果和关联检测项。



故障处理
Linux入侵类问题排查思路

最近更新时间: 2024-12-19 17:12:00

本文档将指导您如何排查 Linux 入侵类问题并提供被入侵后的安全优化建议。

> **说明：**
>
> 若已明确入侵事件属于挖矿或木马，请按 挖矿木马自助清理手册 进行处置。

深入分析，查找入侵原因

一、检查隐藏账户及弱口令

1. 检查服务器系统及应用账户是否存在**弱口令**：

- 检查说明：检查管理员账户、数据库账户、MySQL 账户、tomcat 账户、网站后台管理员账户等密码设置是否较为简单，简单的密码很容易被黑客破解。
- 解决方法：以管理员权限登录系统或应用程序后台，修改为复杂的密码。
- 风险性：高。

2. 使用 `last` 命令查看下服务器近期登录的账户记录，确认是否有可疑 IP 登录过机器：

- 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
- 解决方法：检查发现有可疑用户时，可使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
- 风险性：高。

3. 通过 `less /var/log/secure|grep 'Accepted'` 命令，查看是否有可疑 IP 成功登录机器：

- 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
- 解决方法：使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
- 风险性：高。

4. 检查系统是否采用**默认管理端口**：

- 检查系统所用的管理端口（SSH、FTP、MySQL、Redis 等）是否为默认端口，这些默认端口往往被容易自动化的工具进行暴破成功。

- 解决方法：

  a.在服务器内编辑 /etc/ssh/sshd_config 文件中的 Port 22，将22修改为非默认端口，修改之后需要重启 ssh 服务。

> **注意：**
>
> 当对端口进行修改时，需同时在云服务器控制台上修改对应主机的安全组配置，在其入站规则中，放行对应端口。

b.运行/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian / Ubuntu）命令重启使配置生效。

c.修改 FTP、MySQL、Redis 等的程序配置文件的默认监听端口21、3306、6379为其他端口。

d.限制远程登录的 IP，编辑/etc/hosts.deny 、/etc/hosts.allow两个文件来限制 IP。

- 风险性：高。

5. 检查/etc/passwd文件，看是否有非授权账户登录：

- 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
- 解决方法：使用命令 usermod -L 用户名禁用用户或者使用命令 userdel -r 用户名删除用户。
- 风险性：中。

二、检查恶意进程及非法端口

1. 运行 netstat -antp ，查看服务器是否有未被授权的端口被监听，查看下对应的 pid。

- 检查服务器是否存在恶意进程，恶意进程往往会开启监听端口，与外部控制机器进行连接。
- 解决方法：若发现有非授权进程，运行 ls -l /proc/$PID/exe 或 file /proc/$PID/exe （$PID 为对应的 pid 号），查看下 pid 所对应的进程文件路径。

如果为恶意进程，删除对应的文件即可。

- 风险性：高。

2. 使用 ps -ef 和 top 命令查看是否有异常进程

- 检查说明：运行以上命令，当发现有名称不断变化的非授权进程占用大量系统 CPU 或内存资源时，则可能为恶意程序。

- 解决方法：确认该进程为恶意进程后，可以使用 kill -9 进程名 命令结束进程，或使用防火墙限制进程外联。
- 风险性：高。

三、检查恶意程序和可疑启动项

1. 使用 chkconfig --list 和 cat /etc/rc.local 命令，查看开机启动项中是否有异常的启动服务。

- 检查说明：恶意程序往往会添加在系统的启动项，在用户关机重启后再次运行。
- 解决方法：如发现有恶意进程，可使用 chkconfig 服务名 off 命令关闭，同时检查 /etc/rc.local 中是否有异常项目，如有请注释掉。
- 风险性：高。

2. 进入 cron 文件目录，查看是否存在非法定时任务脚本。

- 检查说明：查看 /etc/crontab ， /etc/cron.d ， /etc/cron.daily ， cron.hourly/ ， cron.monthly ， cron.weekly/ 是否存在可疑脚本或程序。
- 解决方法：如发现有不认识的计划任务，可定位脚本确认是否正常业务脚本，如果非正常业务脚本，可直接注释掉任务内容或删除脚本。
- 风险性：高。

四、检查第三方软件漏洞

1. 如果您服务器内有运行 Web、数据库等应用服务，请您限制应用程序账户对文件系统的写权限，同时尽量使用非 root 账户运行。

- 检查说明：使用非 root 账户运行，可以保障在应用程序被攻陷后，攻击者无法立即远程控制服务器，减少攻击损失。
- 解决方法：进入 web 服务根目录或数据库配置目录。

运行 chown -R apache:apache /var/www/xxxx 、 chmod -R 750 file1.txt 命令配置网站访问权限。

- 风险性：中。
- 具体参考下方网站目录文件权限示例。

2. 升级修复应用程序漏洞

- 检查说明：机器被入侵，部分原因是系统使用的应用程序软件版本较老，存在较多的漏洞而没有修复，导致可以被入侵利用。

- 解决方法：比较典型的漏洞例如 ImageMagick、openssl、glibc 等，用户可以根据已发布的安全通告指导或通过 apt-get/yum 等方式进行直接升级修复。
- 风险性：高。

网站目录文件权限的参考示例如下：场景：** 假设 HTTP 服务器运行的用户和用户组是 www，网站用户为 centos，网站根目录是 `/home/centos/web` 。 **方法/步骤：**

1. 我们首先设定网站目录和文件的所有者和所有组为 centos，www，如下命令：

```
chown -R centos:www /home/centos/web
```

2. 设置网站目录权限为750，750是 centos 用户对目录拥有读写执行的权限，设置后，centos 用户可以在任何目录下创建文件，用户组有有读执行权限，这样才能进入目录，其它用户没有任何权限。

```
find -type d -exec chmod 750 {} \;
```

3. 设置网站文件权限为640，640指只有 centos 用户对网站文件有更改的权限，HTTP 服务器只有读取文件的权限，无法更改文件，其它用户无任何权限。

```
find -not -type d -exec chmod 640 {} \;
```

4. 针对个别目录设置可写权限。例如，网站的一些缓存目录就需要给 HTTP 服务有写入权限、discuz x2 的 `/data/` 目录就必须要写入权限。

```
find data -type d -exec chmod 770 {} \;
```

被入侵后的安全优化建议

- 推荐使用 SSH 密钥进行登录，减少暴力破解的风险。
- 在服务器内编辑 `/etc/ssh/sshd_config` 文件中的 Port 22，将 22 修改为其他非默认端口，修改之后重启 SSH 服务。可使用如下命令重启：

```
/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian/Ubuntu）
```

> **注意：**
>
> 当修改端口时，需同时在云服务器控制台上修改对应主机安全组配置，在其入站规则中放行对应端口。

- 如果必须使用 SSH 密码进行管理，选择一个好密码。
- 无论应用程序管理后台（网站、中间件、tomcat 等）、远程 SSH、远程桌面、数据库，都建议设置复杂且不一样的密码。
- 下面是一些好密码的实例（可以使用空格）： `1qtwo-threeMiles3c45jia`` caser, lanqiu streets`
- 下面是一些弱口令的示例，可能是您在公开的工作中常用的词或者是您生活中常用的词： 公司名+日期（coca-cola2016xxxx） 常用口语（Iamagoodboy）
- 使用以下命令检查主机有哪些端口开放，关闭非业务端口。

```
netstat -antp
```

- 通过安全组防火墙限制仅允许制定 IP 访问管理或通过编辑 `/etc/hosts.deny` 、 `/etc/hosts.allow` 两个文件来限制 IP。
- 应用程序尽量不使用 **root** 权限。 例如 Apache、Redis、MySQL、Nginx 等程序，尽量不要以 root 权限的方式运行。
- 修复系统提权漏洞与运行在 root 权限下的**程序漏洞**，以免恶意软件通过漏洞提权获得 root 权限传播后门。
- 及时更新系统或所用应用程序的版本，如 Struts2、Nginx，ImageMagick、Java 等。
- 关闭应用程序的远程管理功能，如 Redis、NTP 等，如果无远程管理需要，可关闭对外监听端口或配置。
- 定期**备份**云服务器业务数据。
- 对重要的业务数据进行异地备份或云备份，避免主机被入侵后无法恢复。
- 除了您的 home，root 目录外，您还应当备份 /etc 和可用于取证的 /var/log 目录。
- 安装**主机安全 Agent**，在发生攻击后，可以了解自身风险情况。

> **说明：**
>
> 如果以上步骤均不能排查出来问题，建议您联系运维人员进行处理。

Windows入侵类问题排查思路

最近更新时间: 2024-12-19 17:12:00

本文档将指导您如何排查 Windows 入侵类问题。

深入分析，查找入侵原因

一. 检查帐户和弱口令

1. 查看服务器已有系统或应用帐户是否存在弱口令。

- 检查说明：主要检查系统管理员帐户、网站后台帐户、数据库帐户以及其他应用程序（FTP、Tomcat、phpMyAdmin 等）帐户是否存在弱口令。

> **说明：**
>
> 帐户密码建议设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码

- 检查方法：根据实际情况自行确认。
- 风险性：**高。**

2. 查看下服务器内是否有非系统和用户本身创建的账户。

- 检查说明：一般黑客创建的异常账户账户名会在本地用户组显示出来。
- 检查方法：打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增的账户，如有管理员群组的（Administrators）里的新增账户，请立即禁用或删除掉。
- 风险性：**高。**

3. 检查是否存在隐藏账户名。

- 检查说明：黑客为了逃避检查，往往会在您服务器内创建隐藏账户，隐藏账户在本地用户内是查看不到的。

- 检查方法（您也可以通过下载 LP_Check 安全工具检查是否有隐藏账户）：

  a.在桌面打开运行（可使用快捷键 Win + R），输入 regedit，即可打开注册表编辑器。

b.选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认无法查看该选项内容，右键菜单选择权限，打开权限管理窗口。

c.选择当前用户（一般为 administrator），将权限勾选为完全控制，然后确定，关闭注册表编辑器。

d.再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users。

e.在 Names 项下可以看到实例所有用户名，如出现本地账户中没有的账户，即为隐藏账户，在确认为非系统用户的前提下，可删除此用户。

- 风险性：**高。**

二. 检查恶意进程和端口

1. 检查是否存在恶意进程在系统后台运行。

- 检查说明：攻击者在入侵系统后，往往会运行恶意进程与外部进行通信，通过分析外联的进程，即可以找出入侵的控制进程。
- 检查方法：

a.登录服务器，选择**开始** > **运行。**

b.输入 `cmd` ，然后输入 `netstat –nao` 查看下服务器是否有未被授权的端口被监听。

c.打开任务管理器，检查对应的 PID 进程号所对应的进程是否为正常进程，例如通过 PID 号查看下运行文件的路径，删除对应路径文件，您也可以通过微软官方提供的 Process Explorer 工具进行排查。

- 风险性：**高。**

三. 检查恶意程序及启动项

1. 检查服务器内部是否有异常的启动项。

- 检查说明：攻击者在入侵系统后，往往会把恶意程序放到启动项中开机执行。
- 检查方法：

a.登录服务器，选择**开始** > **所有程序**>**启动。**

b.默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

c.选择**开始** > **运行**，输入 `msconfig` ，查看是否存在命名异常的启动项目，若存在则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

d.选择**开始** > **运行**，输入 `regedit` ，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce 检查注册表右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

- 风险性：**高。**

2. 查看正在连接的会话。

- 检查说明：检查服务器与网络上的其它服务器之间的会话或计划任务。
- 检查方法：

a.登录服务器，选择**开始** > **运行。**

b.输入 `cmd` ，然后输入 `netstat -ano` ，检查服务器与网络上的其它服务器之间的会话，并确认是否为正常连接。输入 schtasks，检查服务器中的计划任务，并确认是否为正常的计划任务。

- 风险性：**中。**

四. 检查第三方软件漏洞

1. 如果您服务器内有运行对外应用软件（WWW、FTP 等），请您对软件进行配置，**限制应用程序的权限，禁止目录浏览或文件写权限。**
2. 开通Web 应用防火墙 防护，查看 Web 应用防护攻击日志。

常见问题

如何恢复被入侵后的网站或系统？

系统确认被入侵后，往往系统文件会被更改和替换，此时系统已经变得不可信，最好的方法就是重新安装系统，同时给新系统安装所有补丁。

如何防止网站或系统被再次入侵？

1. 改变所有系统账户的密码为 **复杂密码**（至少与入侵前不一致）。
2. **修改默认远程桌面端口**，操作如下：
3. 选择**开始** > **运行**，然后输入 `regedit`。
4. 打开注册表，进入如下路径： HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
5. KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Tenninal Server\WinStations\RDP-Tcp
6. 修改下右侧的 PortNamber 值。
7. 配置安全组防火墙只允许 **指定 IP 才能访问远程桌面端口。**
8. **定期备份**重要业务数据和文件。
9. **定期更新**操作系统及应用程序组件版本（如 FTP、Struts2 等），防止被漏洞利用。
10. 安装主机安全 Agent 和防病毒软件进行定期体检和扫描。

Linux 客户端离线排查

最近更新时间: 2024-12-19 17:12:00

本文档将指导您进行 Linux 客户端离线排查，包括客户端进程未启动排查及网络故障排查。

客户端进程未启动排查

1. 请查询主机安全进程是否存在。输入： `ps -ef|grep YD` 。

   正常状态下，主机安全存在两个进程，如下图所示：

```
[root@VM_145_42_centos ~]# ps -ef|grep YD
root      9059     1  0 Oct30 ?        00:00:41 /usr/local/qcloud/YunJing/YDEyes/YDService
root     14340     1  0 Oct23 ?        00:00:58 /usr/local/qcloud/YunJing/YDLive/YDLive
```

- 如果进程不存在，可能存在以下情况：
- 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
- 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 若服务器已安装主机安全或者客户端，可采用以下方法排查客户端进程未启动原因：

- 可查看客户端日志，存放路径： `/usr/local/qcloud/YunJing/log` 。
- 可执行命令： `sh /usr/local/qcloud/YunJing/startYD.sh` 启动主机安全服务。

网络故障排查

如果进程存在，但主机安全不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 如果无法访问主机安全域名，可以尝试修改 DNS。可以通过执行如下命令行，排查主机安全域名是否可以访问：

- VPC 网络和黑石服务器环境： `telnet s.yd.gsesgpucloud.com 5574` 。

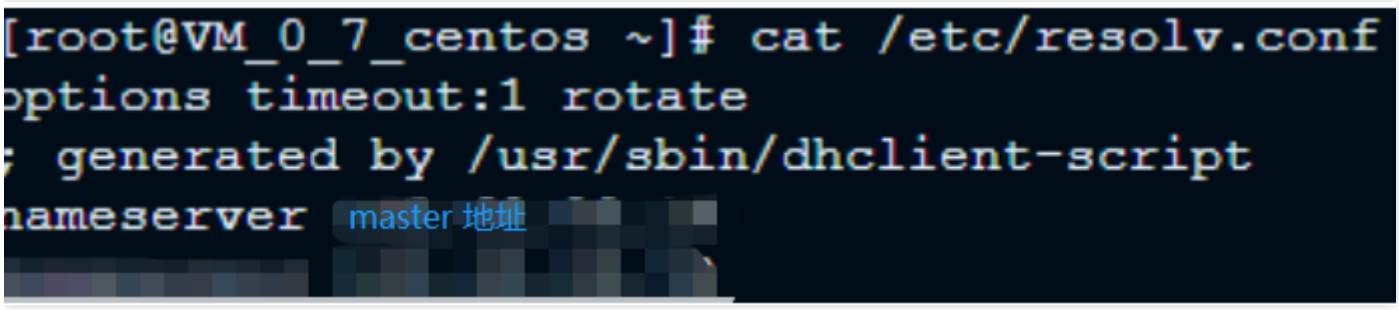
  正常情况下：返回如下图所示结果。



如果无法访问：

a. 可以尝试修改`dns nameserver`字段：`vim /etc/resolv.conf``nameserver master地址`

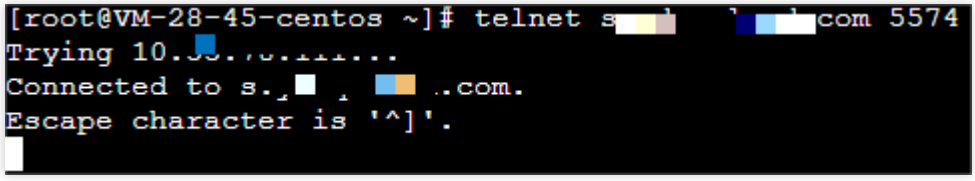
b. 修改完成后，重新执行`telnet s.yd.gsesgpucloud.com 5574`检测能否连通。



c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

- 基础网络环境（非 VPC 上的服务器）：`telnet s.yd.gsesgpucloud.com 5574`。

  正常情况下：返回如下图所示结果。



  如果无法访问：

  a. 可以尝试修改`dns nameserver`字段：`vim /etc/resolv.conf`，先把原有的`nameserver`字段注释，再新增 `nameserver`字段，具体的 nameserver ip 相关内容。

  b. 修改完成后，重新执行`telnet s.yd.gsesgpucloud.com 5574`检测能否连通。

c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

2. 防火墙策略限制，需要在 Linux 客户端开放 TCP 端口：5574、8080、80、9080。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径：`/usr/local/qcloud/YunJing/log`）并联系我们运维人员进行反馈。

Windows 客户端离线排查

最近更新时间: 2024-12-19 17:12:00

客户端进程未启动排查

请查询主机安全进程是否存在。 打开 Windows 任务管理器，查找名为 YDService.exe 的进程是否存在。



1. 如果进程不存在，可能存在以下情况：

- 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
- 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 排查方法：

- 可查看客户端日志，存放路径： C:\Program Files\QCloud\YunJing\log 。
- 可执行命令： sc start ydservice 手动运行客户端。

网络故障排查

如果进程存在，但主机安全客户端不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 检查 DNS 是否被修改，可以通过执行如下命令行进行排查，只要其中一个返回正常结果，则表示 DNS 无问题：

- 基础网络下载地址（非 VPC 服务器）： telnet s.yd.gsesgpucloud.com 5574 。
- VPC 和黑石服务器下载： telnet s.yd.gsesgpucloud.com 5574。

2. 防火墙阻拦导致故障，需要开放5574、8080、80、9080端口。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径： C:\Program Files\QCloud\YunJing\log ）联系我们运维人员进行反馈。

异常登录的消息提醒

最近更新时间: 2024-12-19 17:12:00

现象描述

用户接收到服务器被异常登录的消息提醒，如下以短信消息为例：

> 尊敬的云平台用户，您好！您的云平台账号（账号ID：[redacted]，昵称：[redacted]）下的服务器：[redacted]，实例ID：[redacted]，地域：[redacted]，时间：[redacted]，检测到被（来源IP：[redacted] 来源地：[redacted]）的机器异常登录，危险等级：可疑，请前往主机安全查看详细信息。

可能原因

当您账号下的服务器有登录行为时，主机安全若发现本次登录没有命中登录白名单，会根据智能算法将该登录记录标记为"可疑"或"高危"，并触发实时告警提醒。

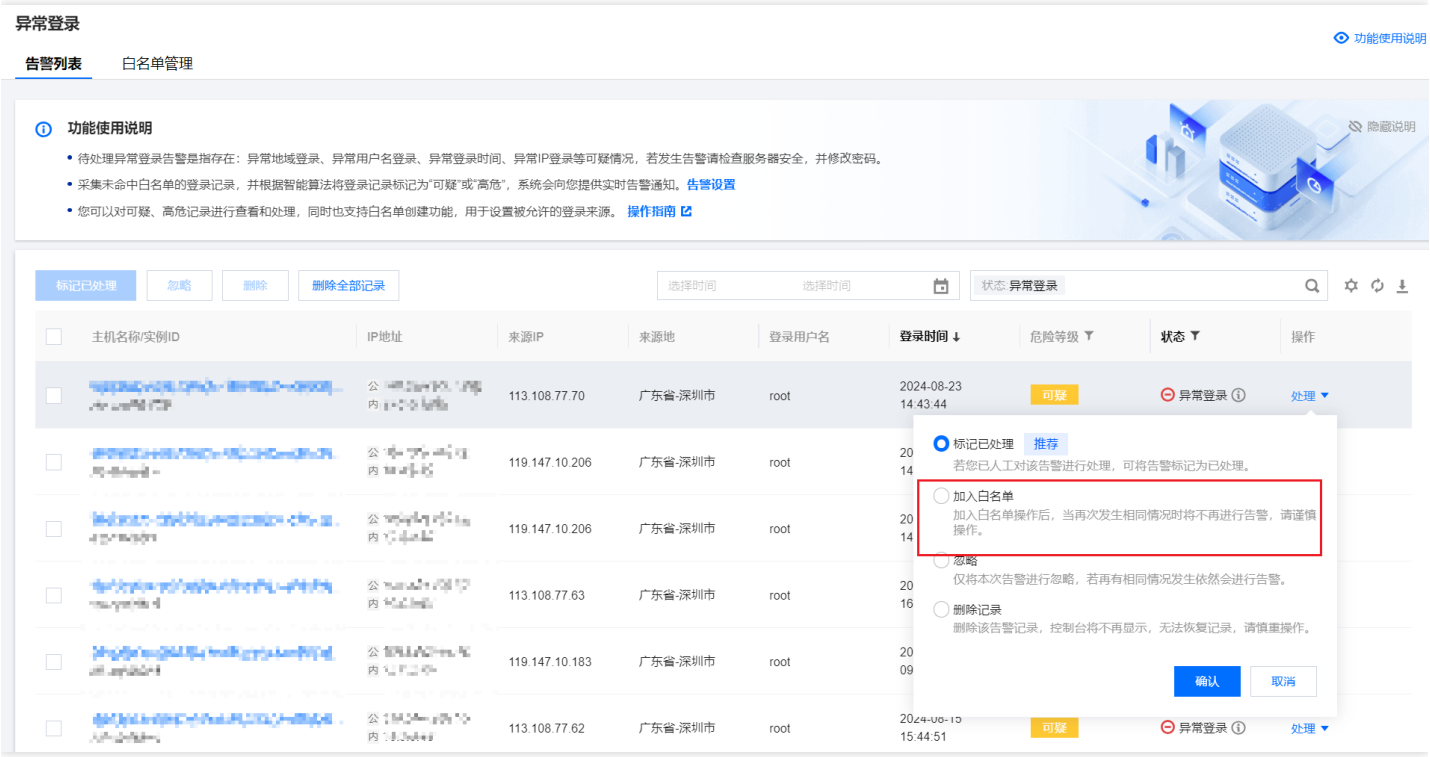
> **说明：**
>
> - 默认仅告警危险等级为"高危"的异常登录事件，可通过【设置中心】> 【告警设置】勾选设置。
> - 异常登录危险等级是依托算法对服务器过往登录情况综合判定。

处理步骤

在收到的异常登录告警提醒后，请您按照下列步骤进行确认：

1. 请确认本次登录行为是否为合法登录。

- 是，请将该登录记录加入白名单，后续该登录行为再次发生，不再产生告警。



- 否，请执行步骤2。

2. 确定为非法登录，初步判断您服务器告警的异常登录事件，是由于不常使用的用户被破解，建议您立即修改登录密码以及服务器上保存过的相关登录凭证。建议参考 Linux 入侵类问题排查思路 和 Windows 入侵类问题排查思路对服务器进行常规排查。

加固方法

后续您可以通过如下加固方法，以提高服务器安全性：

- 服务器设置大写、小写、特殊字符、数字组成的12-16位的复杂密码。
- 修改云服务器 Linux 系统默认远程登录端口，如下所示： 修改文件：/etc/ssh/sshd_config

```
Port 22 #在第三行或第四行，如果前面有井号，请删除，修改为65534以下即可
```

可在远程连接中用 vi 命令，或 sftp 下载到本地修改，修改后使用以下命令重启 ssh 服务。

```
/etc/init.d/sshd restart #centos系统，重启ssh服务命令
/etc/init.d/ssh restart #debian/ubuntu系统，重启 ssh 服务命令
```

平台有安全组功能，建议您仅放行需要的业务协议和端口，不建议放行所有协议所有端口 。

配置云服务器系统防火墙，建议开启云防火墙 。

确保云服务器已安装的防护软件 主机安全客户端进程 处于正常运行状态，并开启实时告警，有异常登录时，及时反馈到您。

及时修复云服务器系统组件与 Web 组件存在的安全漏洞。

> **说明：**
>
> 做好如上云服务器系统安全防护，虽可有效降低安全风险，但也无法保证绝对安全，建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失、或业务不可用。 在安全加固的同时，也强烈建议您制作系统镜像、创建数据快照、自动定期快照。

常见问题

是否可以关闭异常登录检测？

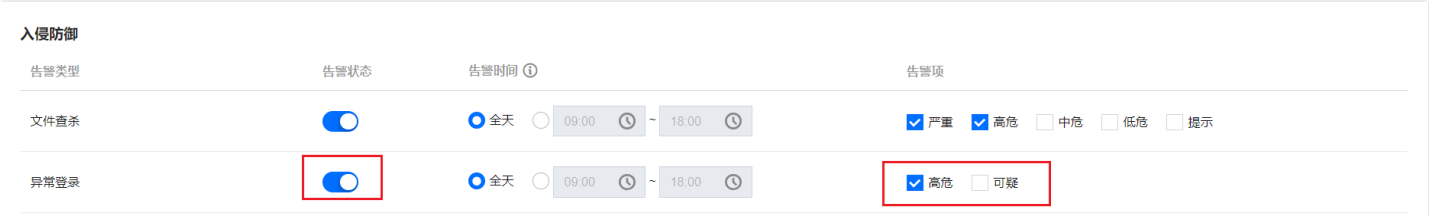
不可以，关闭异常登录检测。

如果您不想接收异常登录的告警通知，您可以尽量配全登录白名单，或者关闭异常登录告警。

配全登录白名单：在【异常登录】页，选择【白名单管理】 >【添加白名单】，将常用登录来源 IP 添加为白名单。



关闭异常登录告警：在【设置中心】页面，将告警状态设为关闭，或取消勾选告警项“高危”或“可疑”即可。



常见问题
购买相关

最近更新时间: 2024-12-19 17:12:00

如何购买主机安全专业版或旗舰版？

可以进入主机安全租户端购买页进行升级。

如何关闭主机安全专业防护或旗舰防护服务？

进入【授权管理】页面，查看授权详情，可对已绑定授权的主机进行如下操作：



主机安全产品是否与其他安全产品冲突？

主机安全与其他安全产品并不冲突，属于不同的防护维度，通过在不同的层面上提供安全能力，保障用户安全。

如何卸载云服务器中的主机安全客户端?

登录主机安全租户端控制台，在左侧导航栏中，选择【资产管理】 > 【主机列表】，在服务器列表，找到需要卸载的云服务器单击【卸载】，或打开安装目录，通过目录中的卸载程序进行卸载。

功能相关

最近更新时间: 2024-12-19 17:12:00

为什么 Jar 包类的漏洞多次扫描时，每次检测结果可能不一致？

Jar 包类漏洞，例如 struts2 漏洞的检测依赖 Jar 包运行态是否加载，未运行服务时是不能检测到漏洞的，运行服务时 Webserver 对于Jar 包的加载分为动态加载和静态加载。在动态加载模式下，struts2 漏洞只有在 Jar 包运行时才能被检测出来，所以每个时段检测结果存在差异。建议您针对高危 Jar 包漏洞进行多次检测，提升检测结果的准确度。

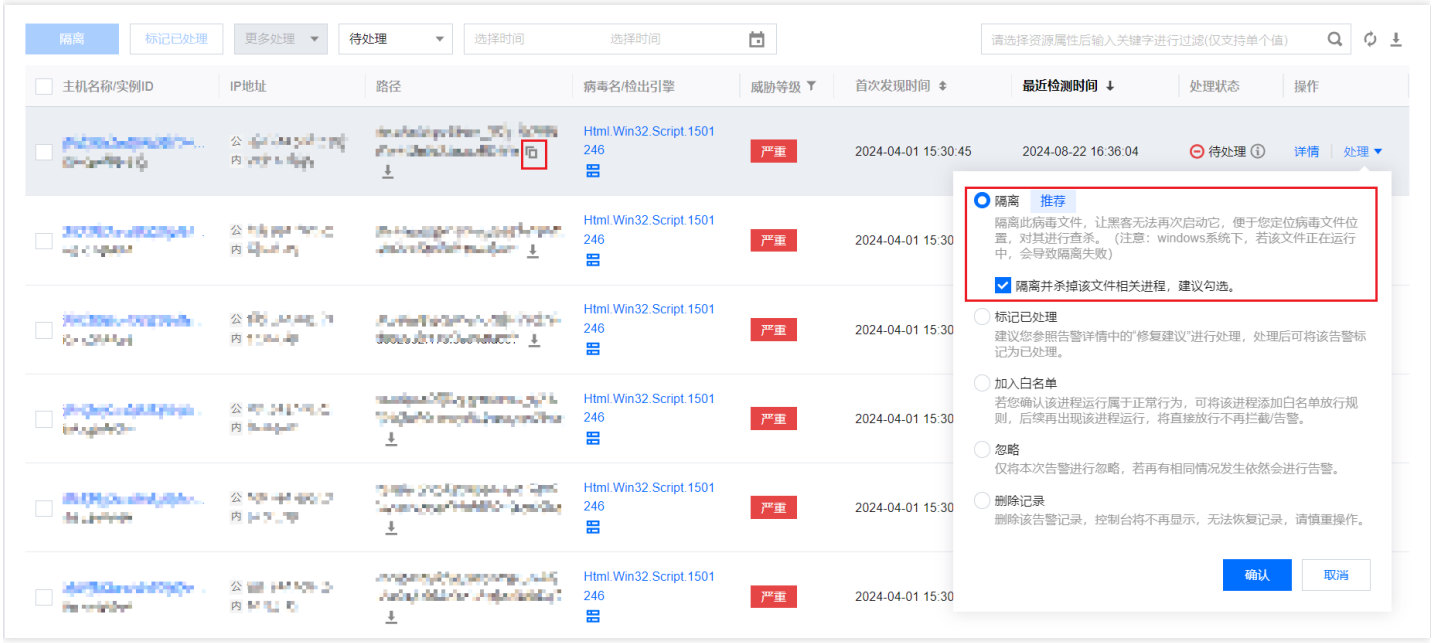
主机安全扫描频率是多少？

可自定义周期扫描，也可手动扫描。

如何对木马文件进行处理？

在【文件查杀】页面，可对木马文件进行如下处理：

- 删除：单击复制木马文件路径，定位木马并手动删除该文件。
- 加入白名单：您可执行加入白名单操作，后续主机安全将不再对该机器的该文件进行检测。
- 隔离：当前尚不支持拦截木马，仅支持事中或事后检测并告警，但可对该文件执行隔离操作，防止该文件再次被启动。



概览页安全评分机制是怎样的？

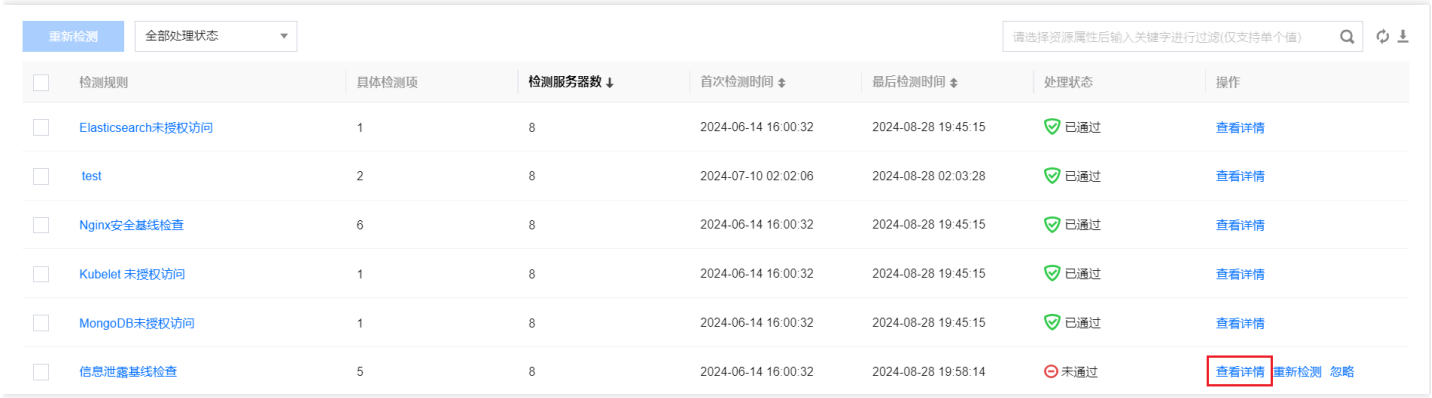
概览页安全评分机制，请参见 安全概览 文档。

安全基线在产品设置过后，多久可以生效？

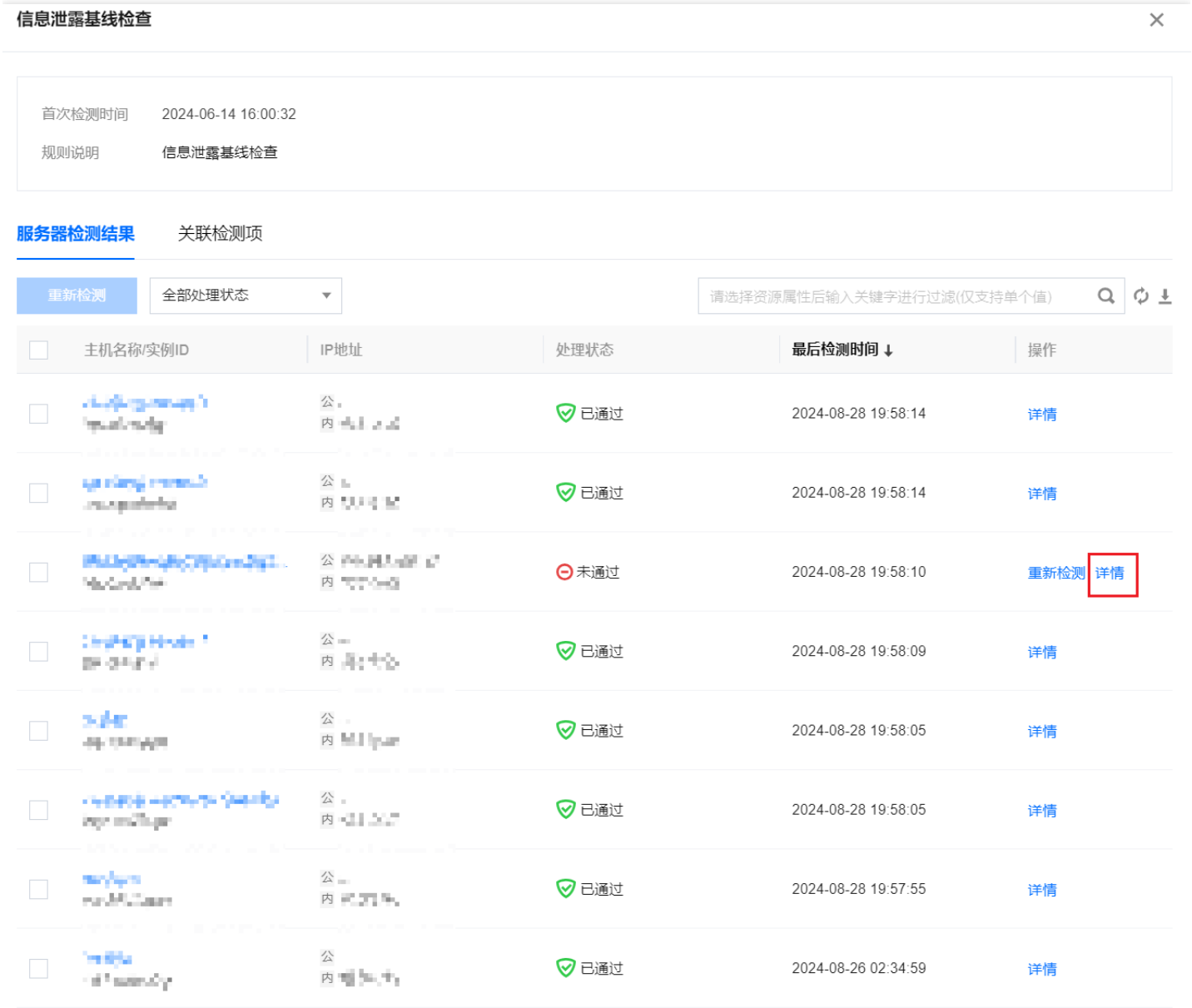
安全基线在产品设置后，即时生效。

主机安全基线检测"未通过"怎么处理？

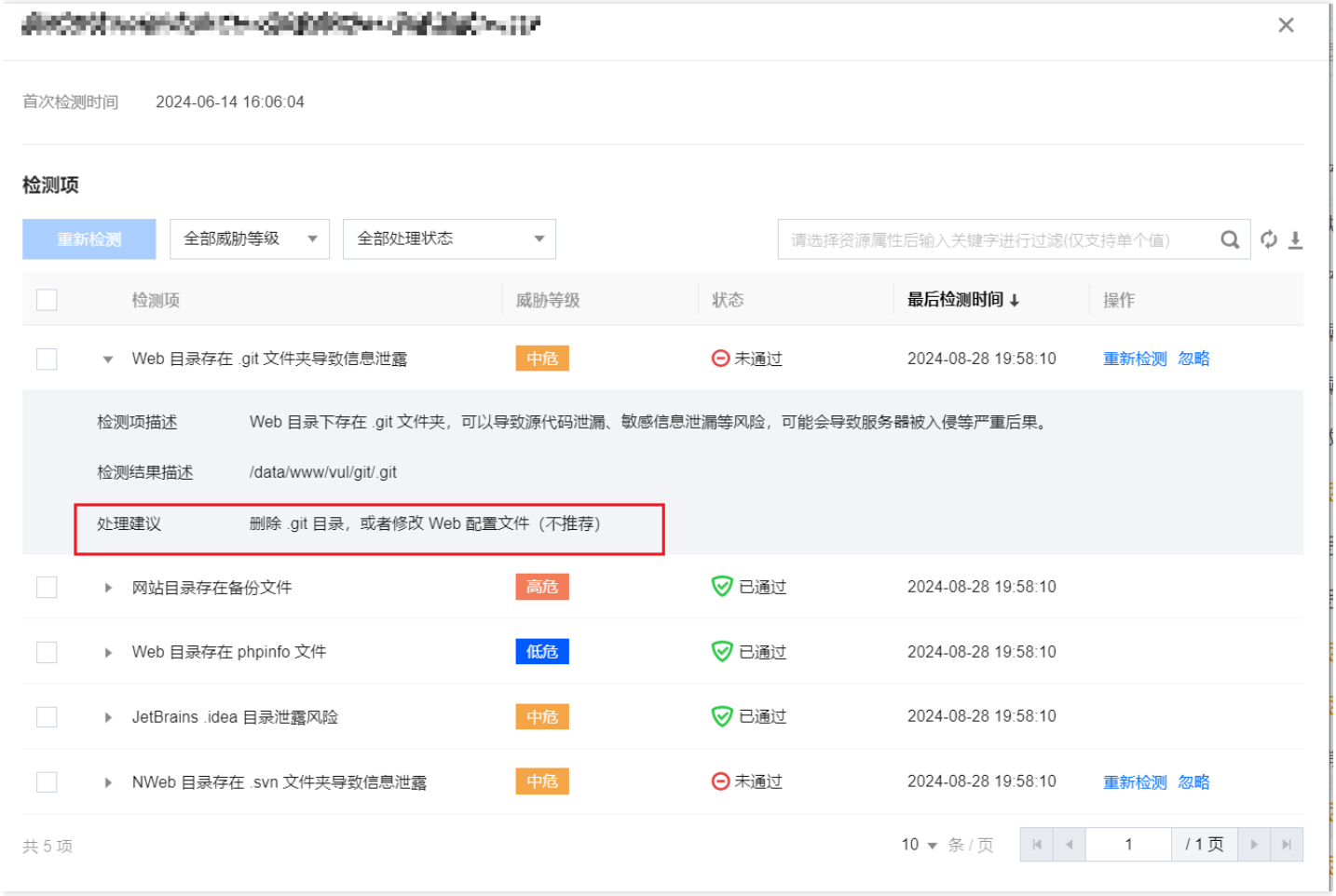
1. 进入【安全基线】页面，选择未通过的检测项，单击操作列下的【查看详情】，进入该检测项的详情页面。



2. 在基线检测结果页面中，选择未通过检测的服务器，单击【详情】，进入检测详情页面。



3. 在检测详情中可查看未通过的检测项，以及处理建议。



主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信方式的方式进行告警通知，具体方式您可以在【消息中心】>【消息订阅】中进行设置。

入侵相关

最近更新时间: 2024-12-19 17:12:00

入侵常见问题

云服务器被入侵有哪些危害？

- 业务被中断：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- 数据被窃取：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，导致企业品牌受损、用户流失。
- 被加密勒索：黑客入侵云服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- 服务不稳定：黑客在云服务器中运行挖矿程序、DDoS 木马程序，消耗大量系统资源，导致云服务器不能提供正常服务。

如何降低云服务器被入侵概率？

- 及时修复高危漏洞及基线相关问题。
- 设置强密码，避免暴破攻击。
- 定期巡检账号、权限、端口并及时处理主机安全租户端控制台上的告警信息。

云服务器被入侵后要如何防护？

防范措施建议如下：

- 云服务器密码设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码。
- 删除云服务器上设置的不需要的用户，且对于不需要登录的用户，请将其权限设置为禁止登录。
- 修改远程登录服务的默认端口号并禁止超级管理员用户登录。
- 针对 Linux 系统较为安全的方法是只使用密钥登录，禁止密码登录。
- 不建议向公网开放核心应用服务端口访问，例如 mysql、redis 等，您可修改为本地访问或禁止外网访问。
- 如果您的本地外网 IP 固定，建议使用安全组或者系统防火墙设置，禁止除了本地外网 IP 之外的所有 IP 的登录请求。

> **注意：**

> 做好日常云服务器系统的安全防护，可以有效加强云服务器系统安全， 但无法保证绝对安全。 建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失或业务不可用。

如何做好云服务器防范措施？

建议升级主机安全专业版或旗舰版，并处理中危及以上的安全事件。

木马类问题

主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信的方式进行告警通知，具体方式您可以在【消息中心】>【消息订阅】中进行设置。

如何处理木马及病毒文件？

- 若发现病毒及木马文件需及时进行隔离或删除相应恶意文件。
- 部分顽固木马、病毒可能存在重复写入的情况，需排查机器上是否存在弱口令、漏洞等异常情况并进行修复，同时删除恶意文件。
- 部分感染型病毒木马极难进行清理，建议定期对机器做快照备份。

异常登录类问题

云服务器显示登录异常怎么解决？

基于管理员的常用登录地进行异常登录判断，请仔细检查登录记录。若非管理员本人登录，密码可能已经泄露，用户需要对云服务器进行详细的安全检查。

如何处理异常登录告警？

1. 首先确认该异常登录是否为业务相关人员进行的登录，若非业务相关人员登录，在控制台确认是否存在木马、漏洞及源占用异常等情况，若有异常情况，请及时处理。
2. 确认该登录账户是否存在密码强度较弱的情况，及时进行修改。
3. 排查机器中的登录账号是否存在异常账号或权限过高的账户，及时禁用账户或调整权限。

正常登录行为被误报为异常登录，要如何消除误报？

您可以登录主机安全租户端控制台，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【加白名单】，通过自定义添加登录白名单，即可消除误报。

是否可以关闭异常登录检测？

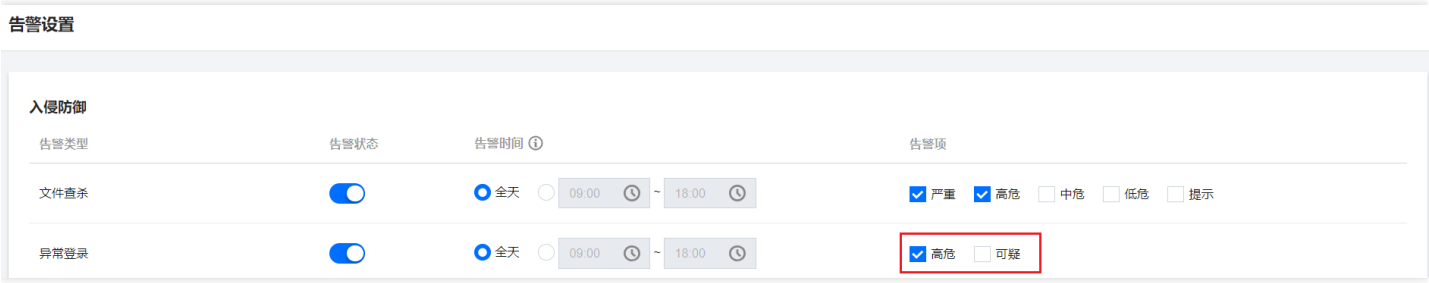
不可以关闭异常登录检测。如果您不想接收异常登录的告警通知，您可以将登录来源添加到白名单，或者取消勾选告警通知，操作步骤如下：

- **方式1**：在【异常登录】页面，选择【白名单管理】>【添加白名单】，将登录来源添加为白名单。



- **方式2**：在【设置中心】>【告警设置】页面，取消勾选异常登录的"高危"和"可疑"告警项即可。

> **注意：**
>
> 如取消勾选，您将不能实时接收到异地登录的告警通知，请谨慎操作。



密码泄露类问题

云服务器被暴力破解如何处理？

若云服务器被暴力破解成功，需尽快排查机器上的异常并进行处理：

- 排查机器中的账户是否存在弱口令，修改口令强度较弱的密码或采用密钥的方式进行登录，同时可通过设置安全组等方式降低被暴力破解的风险。
- 主机安全已上线密码破解阻断功能，可进行有效拦截。

提示密码被暴力破解成功之后该如何解决?

密码破解成功后，云服务器可能已被黑客入侵并留下了后门程序。

- 检查云服务器安全状况，是否还有其它未知账户和木马文件，如果存在请立即删除和修复，并修改云服务器登录密码。
- 根据实际情况决定是否需要对云服务器进行重置，并设置复杂密码，尽量字母、数字、特殊字符3种组合，长度在15位及以上。

防护状态离线类问题

云服务器的防护状态显示离线要如何解决?

主机安全客户端未连接服务端，导致后台显示离线，建议重新下载主机安全客户端进行安装，离线的可能原因如下：

- 云服务器启用了防火墙规则。
- 云服务器安装了第三方恶意软件，导致安全防护程序被破坏。

> **说明：**
>
> 故障排查方式请参见 Linux 客户端离线排查 或 Windows 客户端离线排查。

云镜软件相关说明
功能行为描述

最近更新时间: 2024-12-19 17:12:00

Webshell 检测

Webshell 是黑客入侵过程中常用工具，主机安全客户端会对服务器上新创建的 Web 程序文件进行可疑风险判断，对于少量疑似 Webshell 文件，需要上报到云端，通过云端的机器学习检测引擎模块做进一步检测，检测完成后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程不会提取任何涉及用户隐私的数据。

登录异常提醒

登录异常提醒功能可以帮助用户识别异常的管理员登录行为，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

密码破解提醒

密码破解提醒功能可以告诉用户当前遭受的密码破解事件和破解结果，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

恶意木马和病毒检测

恶意木马和病毒程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。客户端会采集可疑恶意程序的哈希指纹到云端，通过云查杀模块对哈希指纹进行检测，若云端哈希库无该文件记录，需要上报可执行文件到云端，通过云端杀毒引擎进行检测，检测完后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程中不会提取任何涉及用户隐私的数据。

漏洞提醒

版权所有：亿算云平台

目前主机安全支持检测影响面较大的 Linux 和 Windows 双平台的漏洞，以及符合安全要求的基线检测。 漏洞管理功能会显示当前主机上的漏洞风险情况，同时提供修复方案供用户参考。该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间。主机安全默认提供每天漏洞扫描服务，这个过程不会提取任何涉及用户隐私的数据。

升级维护

升级维护功能主要提醒用户对客户端进行升级，以获得最新的安全防护服务，客户端软件需要采集主机安全版本号、操作系统配置信息、安全规则版本号到云端进行判断和提醒，该过程不会提取任何涉及用户隐私的数据。

客户端进程说明

最近更新时间: 2024-12-19 17:12:00

名称	Windows 系统	Linux 系统
程序安装目录	C:\program files\qcloud\yunjing\ydeyes C:\program files\qcloud\yunjing\ydlive	/usr/local/qcloud/YunJing/
进程名称	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDUtils 进程扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件 tcss-agent 容器基线扫描插件 css-scan 容器镜像扫描插件
注册服务名称	YDService YDLive YDEdr	-

客户端程序所占用端口是系统随机返回的，无固定端口范围，若占用端口与用户业务端口冲突，重启客户端程序即可。

- 客户端重启命令（Linux系统）

1. 暂停客户端程序服务

```
/usr/local/qcloud/YunJing/stopYDCore.sh
```

2. 重新启动客户端

```
/usr/local/qcloud/YunJing/startYD.sh
```

- 客户端重启命令（Windows系统）输入以下命令，或打开任务管理器的服务，找到 YDService 服务，右键重启。

1. 暂停客户端程序服务

```
net stop YDService
```

2. 重新启动客户端

```
net start YDService
```

安全基线检测列表

最近更新时间: 2024-12-19 17:12:00

本文档将为您介绍主机安全的安全基线检测列表。

> **注意：**
>
> 安全基线在产品设置后，将即时生效。

Name	Level	Vul_type
CouchDB 未授权访问	高	配置不当
Docker Daemon 2375 管理端口开启	高	远程代码执行
Elasticsearch 未授权访问	高	配置不当
JavaRMI 远程代码执行	高	远程代码执行
Jenkins 未开启认证可导致命令执行	高	远程代码执行
Kubelet 未授权访问	高	安全基线
Linux 系统弱口令检测	高	远程代码执行
MongoDB 未授权访问	高	配置不当
MySQL 弱口令检测	高	弱口令
NFS 错误配置导致可挂载敏感目录	高	配置不当
Redis 基线合规检测	高	远程代码执行
RPCBind 配置不当检测	高	安全基线
Rsync 弱口令检测	高	弱口令
Rsync 无密码访问	高	配置不当
Tomcat 弱口令检测	高	弱口令
Windows 用户弱口令检测	高	弱口令
Xampp 默认 FTP 密码	高	信息泄露
网站目录存在备份文件	高	信息泄露

版权所有：亿算云平台

Name	Level	Vul_type
FTP 匿名登录检测	中	信息泄露
IIS 配置错误导致存在解析漏洞	中	配置不当
Memcached UDP 端口可被利用为 DDOS 放大攻击	中	信息泄露
PHP-FPM 错误配置	中	安全基线
PostgreSQL 合规检测	中	远程代码执行
Web 目录存在 .git 文件夹导致信息泄露	中	信息泄露
Web 目录存在 .svn 文件夹导致信息泄露	中	信息泄露
Windows 隐藏账户检测	中	安全基线
Windows 影子账户检测	中	远程代码执行
ZooKeeper 未授权访问	中	配置不当
Hadoop未授权访问	低	远程代码执行
sudo 无密码用户检测	低	安全基线
Tomcat 样例目录检测	低	安全基线
Web 目录存在 phpinfo 文件	低	信息泄露
Windows 来宾账户状态检测	低	安全基线

版权所有：亿算云平台