

主机安全 操作指南 产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

操作指南

安全概览

资产概览

主机列表

资产指纹

漏洞管理

基线管理

文件查杀

异常登录

密码破解

恶意请求

高危命令

本地提权

反弹 Shell

Java 内存马

核心文件监控

 监控规则配置

 告警列表

网络攻击

勒索防御

日志分析

授权管理

访问管理指引

混合云安装指引

 概述

 配置非腾讯云机器

 连接专线 VPC

 热点问题

新手常见问题

操作指南

安全概览

最近更新时间：2024-08-13 16:29:50

本文将为您介绍安全概览页的功能和操作。

概述

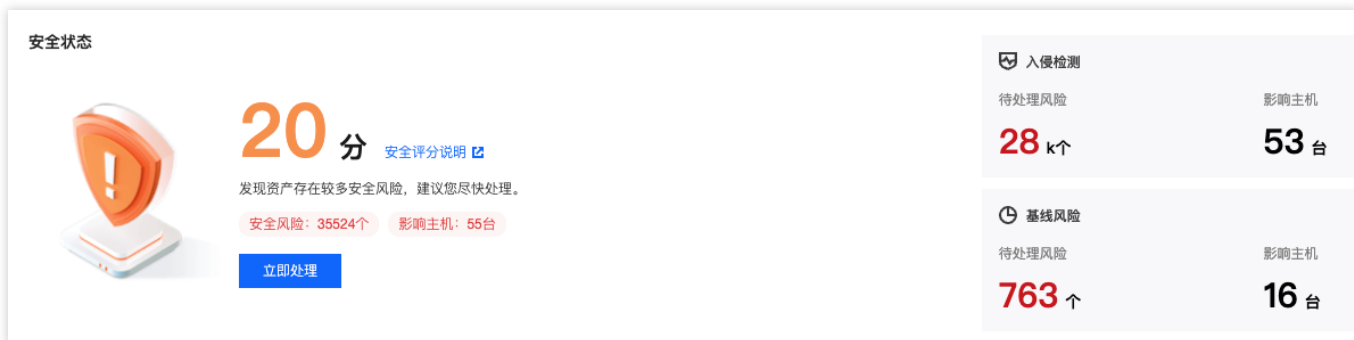
安全概览是主机安全的首页，实时展示您的主机安全评分、待处理风险、安全防护状态、风险趋势以及主机安全的实时动态；推送安全播报，方便您了解主机安全最新威胁情报；提供帮助文档和服务建议，帮助您抵御黑客入侵及攻击威胁，保障企业主机安全。

操作指南

1. 登录 [主机安全控制台](#)。
2. 单击左侧导航中的**安全概览**，各功能说明如下。

安全状态

1. 在**安全状态**区域中，可查看安全评分结果和风险情况，并提供快捷处理入口。



安全评分：基于安全事件的威胁等级和事件数量两个维度进行综合评分，具体评分标准请参见 [安全评分说明](#)。

风险情况：划分为入侵检测、漏洞风险、基线风险三类，统计并展示待处理风险数和受影响主机数。

入侵检测：包含文件查杀、异常登录、密码破解、恶意请求、反弹 Shell、本地提权、高危命令。

漏洞风险：包含漏洞管理中的Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。

基线风险：仅含基线管理。

网络风险：统计攻击事件待处理风险数和受影响主机数。

2. 单击**立即处理**，将打开风险处理详情弹框，可以查看入侵检测、漏洞风险、基线风险和网络风险具体详情。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：

等级	安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马文件、爆破成功、恶意请求	-40分	-50分
高危	严重漏洞、高危漏洞、严重基线、高危基线、异常登录（高危）、本地提权、反弹 Shell	-10分	-20分
中危	中危漏洞、中危基线	-3分	-10分
低危	低危漏洞、低危基线	-2分	-5分
其他	基础版防护、未安装主机安全客户端	-1分	-5分

安全播报

在**安全播报**区域中，将展示功能更新、行业荣誉、紧急通知和版本发布信息的播报内容。

安全播报

更多

全新上线

漏洞防御 | 免重启、精准防御，腾讯安全泰石引擎RASP+方案上线

2024-07-09 11:16:48

安全公告

企业终端安全一体化，办公终端IOA来帮忙，限时免费领

2023-08-11 18:43:36

最佳实践

你的服务器都是怎么被拿下的？ | 攻防演练真实案例

2023-07-07 17:11:00

安全公告

Apache Solr代码执行漏洞自助处置手册

2023-04-25 18:55:29

单击**播报标题**，可查看播报详情；单击**更多**，可查看历史安全播报。

安全防护

在**安全防护**区域中，展示了主机安全应对入侵所提供的全流程解决方案（预防-防御-检测-响应），明确了各流程所需的安全防护项。

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

在防护详情区域中，展示了主机安全各项服务的使用情况统计。

防护详情

腾讯云主机安全已防护 1223 天 • 防护中

■ 未安装55台 [安装](#)

■ 在线47台

■ 关机/离线20台

多云资产接入： 101 14 0 0 0 0 0 1 0 [接入云外主机](#)日志分析使用： 31.97GB/50GB [升级扩容](#)

网页防篡改授权：已使用3个/已购100个

安全防护引擎：

病毒库更新时间：2024-07-09 00:00:05

主机更新时间：2024-07-09 11:16:48

漏洞库更新时间：2024-07-08 16:28:45

防护天数：指服务器安装主机安全客户端的时间并集。

主机总数：指腾讯云服务器（云服务器、轻量应用服务器、黑石物理服务器1.0、边缘计算机器）及非腾讯云服务器的总数。

防护主机数：由于基础版防护程度相对较弱，防护主机数仅包含专业版、旗舰版防护的主机。

安全防护引擎：若您已购买专业版/旗舰版防护授权，将自动开启6个防护引擎：查杀引擎、BinaryAI 引擎、TAV 引擎、异常行为、威胁情报、攻击防御。

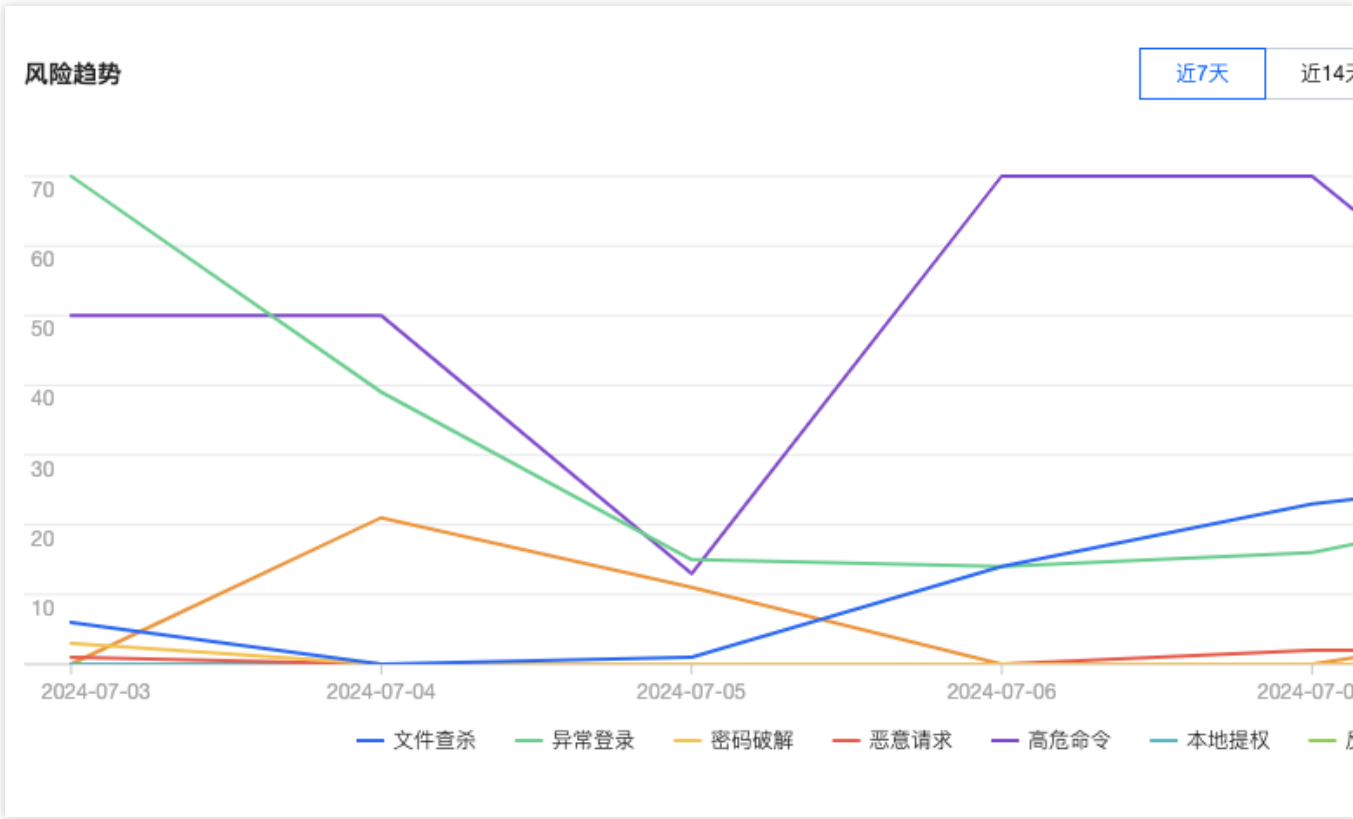
病毒库更新时间：每日零点自动更新病毒库。

主机更新时间：可点击右上角**立即更新**，可手动更新主机列表信息。

漏洞库更新时间：不定时更新。

风险趋势

在**风险趋势**区域中，各项风险数的统计通过折线图展示，直观呈现了主机的风险趋势。



支持筛选近7天、近14天、近30天或自定义时间段查看，单击**下载**，将导出所选时间段内的各项风险数。

说明：

风险数为当日新增待处理事件数，每小时更新一次。

实时动态

在**实时动态**区域中，将实时展示最新发现的安全事件。

实时动态

告警行为	威胁等级	发现时间
异常登录 主机 10.10.10.10 异常登录	可疑	2024-0
高危命令 主机 10.10.10.10 执行了高危命令: cat /etc/passwd	中危	2024-0
高危命令 主机 10.10.10.10 执行了高危命令: rm -rf /	中危	2024-0
异常登录 主机 10.10.10.10 异常登录	可疑	2024-0
异常登录 主机 10.10.10.10 异常登录	可疑	2024-0

共 30 条

单击主机 IP 或查看详情，将跳转至该主机详情页对应风险项处。

资产概览

最近更新时间：2024-08-13 16:29:49

本文将为您介绍资产概览页的功能和操作。

概述

资产概览是从资产维度对主机及16项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。

限制说明

所有腾讯云用户均可查看资产概览。但由于资产指纹的采集受版本限制，资产概览可统计的数据存在差异。仅付费防护版本的主机才可采集资产指纹数据，基础版主机须先[升级版本](#)。

各版本采集的资产指纹如下：

防护版本	采集的资产指纹
基础版（免费）	不支持
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、系统安装包

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。

操作指南

1. 登录 [主机安全控制台](#)。
2. 单击左侧导航中的**资产概览**，各功能说明如下。

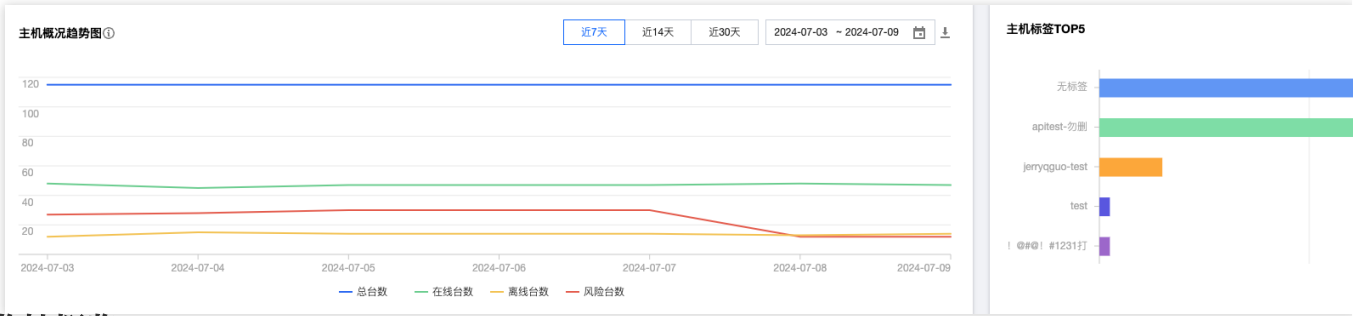
资产概况

在**资产概况**区域中，可查看全部资产及资产指纹的统计情况。

资产概况			
资产指纹采集 最近采集时间：2024-07-09 03:01:32			
全部主机	账号	端口	Web应用
115台	70个	145个	0个
今日新增	0	0	0
进程	软件	数据库	Web框架
678个	23个	4个	0个
今日新增	0	0	0

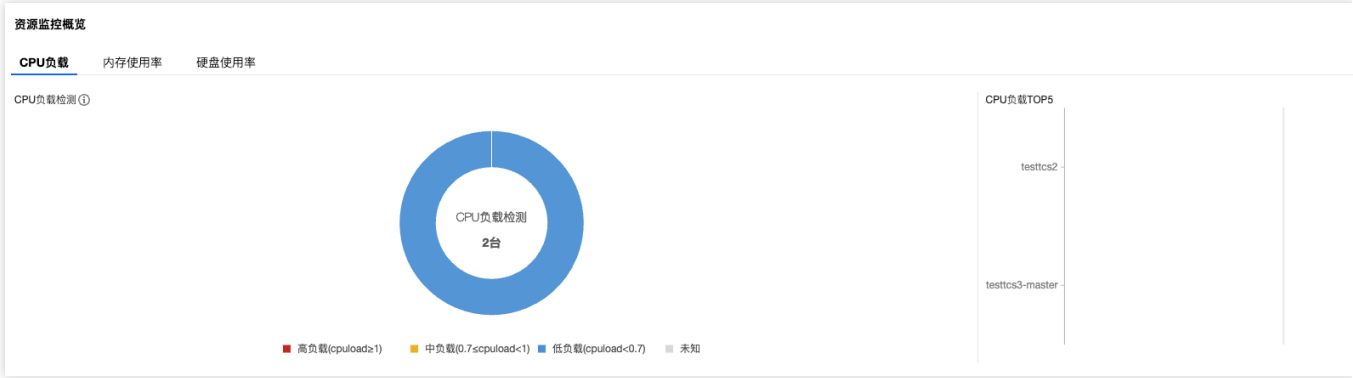
主机概况趋势

主机概况趋势图（总台数、在线台数、离线台数、风险台数）支持一年内任意时间段的查询，支持下载导出；主机标签 TOP5，可查看所有主机中使用最多的前5个标签；支持近7天、近14天、近30天或自定义时间段（最长不超过近3个月）查询；单击**下载**，将导出所选时间范围内主机每天的数据情况。



资源监控概览

在资源监控概览区域中，可查看系统负载、内存使用率、硬盘使用率的分布情况及相应TOP 5。

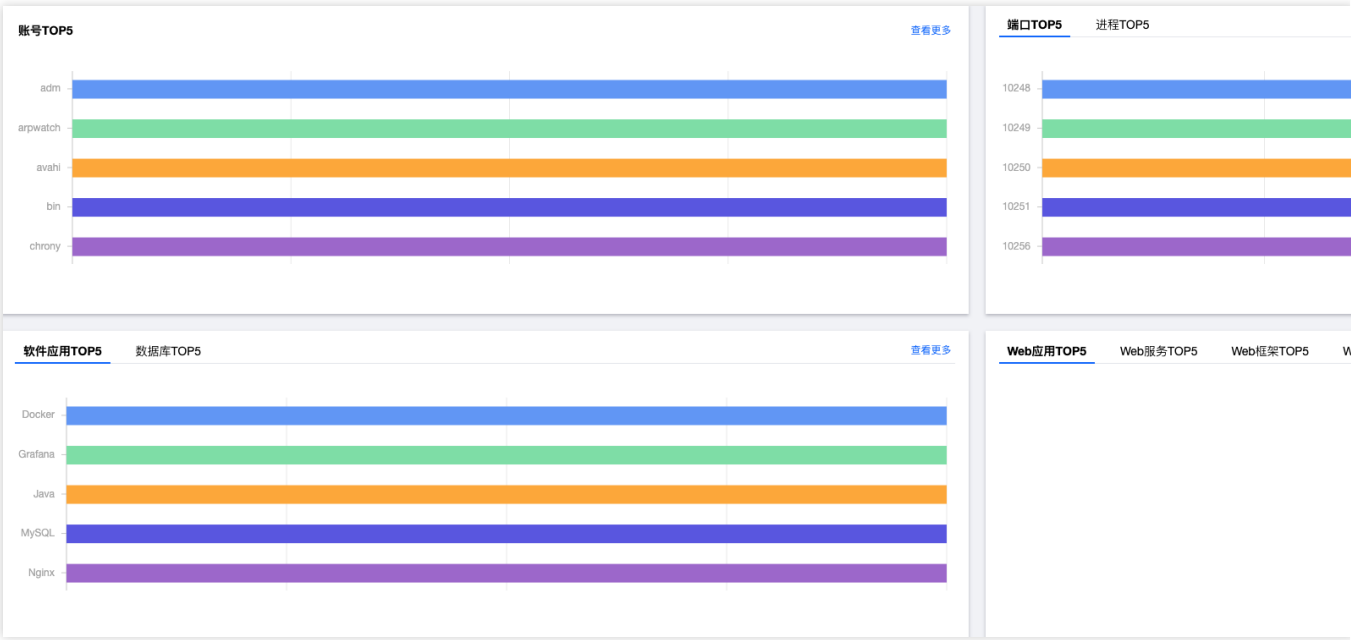


说明：

仅 Linux 服务器支持统计系统负载，Windows 服务器暂无法支持。

资产指纹TOP5

在**资产指纹TOP5**中，统计展示了账号、端口、进程、软件应用、数据库、Web 应用、Web 服务、Web 框、Web 站点的TOP5数据。



主机列表

最近更新时间：2024-08-13 16:29:50

主机列表是主机安全服务的核心组成部分，提供了全面的、可视化的主机统一管控界面，帮助安全管理员更高效地响应主机安全风险。本文档将为您介绍如何接入和管理主机。

限制说明

可接入主机安全的主机范围：

主机类型	具体主机类型	Linux 系统	Windows 系统
腾讯云主机	云服务器 CVM、轻量应用服务器 Lighthouse、边缘计算机器 ECM、黑石物理服务器1.0	支持架构：x86、arm 可接入方式：VPC 网络、基础网络	支持架构：x86 可接入方式：VPC 网络、基础网络
非腾讯云主机	阿里云服务器、华为云服务器、Microsoft 服务器、DigitalOcean 服务器、Amazon 服务器、OracleCloud 服务器....其他云服务器、本地 IDC 服务器	支持架构：x86、arm 可接入方式：公网直连、公网代理、专线接入	支持架构：x86 可接入方式：公网直连、专线接入

多云账号主机资产同步范围：当前仅支持通过 AccessKey 同步阿里云账号下的 ECS 机器数据，不限操作系统。（仅同步机器数据，主机安全客户端仍需手动安装）

通过非腾讯云主机的安装方式接入的主机，更换 IP 后，主机安全会检查设备码和 Iplist，若二者均无变化，则不视为新机器，反之会产生一条新的主机数据。

腾讯云主机被销毁、非腾讯云主机被清理后，原风险数据将被清除。

防护状态说明

风险主机：主机存在安全风险。

旗舰版主机：主机已安装主机安全客户端，并绑定了旗舰版授权，处于旗舰版防护中。

专业版主机：主机已安装主机安全客户端，并绑定了专业版授权，处于专业版防护中。

基础版主机：主机仅安装主机安全客户端。

未安装客户端（无防护）：主机属于腾讯云主机，但未安装主机安全客户端。

已离线：

腾讯云主机：主机的主机安全客户端处于离线状态。

非腾讯云主机：主机的主机安全客户端处于离线状态或该主机已关机。

注意：

因非腾讯云主机关机不可知，故归为客户端已离线。
已关机：主机属于腾讯云主机且处于关机状态。

主机配置

- 1. 登录[主机安全控制台](#)，在左侧导航栏，选择[资产中心 > 主机列表](#)。
- 2. 在主机列表页面，可进行安装主机安全客户端、同步资产、关联标签、多云账号管理、升级版本、资产清理等配置操作。

主机列表

剩余防护授权：专业版 1 个，旗舰版 24 个 [前往批量授权](#)

最近同步时间：2024-02-06 14:00

主机状态

主机总数

非腾讯云主机限时0元防护 [领取](#)

142 台

[安装客户端](#) [接入混合云](#)

137

4

0

0

0

0

0

0

0

1

0

已防护的主机

1 台

[购买授权](#)

基础版：61台 | 专业版：1台 | 旗舰版：0台

存在风险的主机

50 台

较昨日：▲ 2

无防护的主机

80 台

[安装客户端](#)

较昨日：

安装主机安全客户端

升级版本

全部服务器

全地域

[多个关键字用竖线分隔](#)

主机防护状态分类

全部主机

142

风险主机

50

旗舰版主机

0

专业版主机

1

基础版主机

60

未安装客户端（无防护）

80

已离线

6

已关机

15

近15日新增

18

标签

请输入标签关键字

Q

腾讯云标签

[管理标签](#)

tke-clusterid:cls-mvpb4uwk

0

主机名称/实例ID	IP地址	操作系统	地域/所属网络	风险状态	入侵检测	漏洞风险	基线风险	网络风险	标签
腾讯云主机	10.0.0.1	Ubuntu 20.04	腾讯云主机	风险	2	停止检测 ①	3	0	标签(1)
腾讯云主机	10.0.0.2	Ubuntu 20.04	腾讯云主机	风险	停止检测 ①	停止检测 ①	0	0	标签(1)
腾讯云主机	10.0.0.3	Ubuntu 20.04	腾讯云主机	风险	3	0	0	0	暂无标签
腾讯云主机	10.0.0.4	Ubuntu 20.04	腾讯云主机	风险	停止检测 ①	0	3	0	标签(1)
腾讯云主机	10.0.0.5	Ubuntu 20.04	腾讯云主机	风险	0	0	0	1	标签(1)
腾讯云主机	10.0.0.6	Ubuntu 20.04	腾讯云主机	风险	停止检测 ①	0	3	0	暂无标签
腾讯云主机	10.0.0.7	Ubuntu 20.04	腾讯云主机	风险	停止检测 ①	0	4	停止检测 ①	暂无标签

安装主机安全客户端：主机安全客户端是腾讯云官方安全插件，是接入主机安全防护的重要前提，您可单击[安装主机安全客户端](#)，选择合适的安装方式进行安装并验证是否安装成功。



同步资产：单击**同步资产**，可更新主机列表最新状态。

关联标签：主机安全兼容腾讯云标签、主机安全标签两套标签，单击标签列中的



图标，可针对该主机关联标签。

腾讯云标签（key:value）：仅可关联腾讯云主机。

主机安全标签（value）：可关联腾讯云主机、非腾讯云主机。

关联标签

正在为主机

关联标签

类型一：腾讯云标签

腾讯云标签仅支持查看，如需进一步管理请点击前往 [标签管理](#)

服务器标签

类型二：主机安全标签

服务器标签

提交

关闭

多云账号管理：通过同步多云账号下的主机资产可以达到简化管理、整合监控、提高风险的可见性和响应效率。

多云账号管理

接入多云账号，掌握全局视角，统一管理云上负载安全。

支持多云类型：阿里云、华为云、亚马逊云，后续将支持更多云类型，敬请期待。

接入混合云账号

阿里云

服务状态：正常

删除

密钥ID：

所属主账号：

阿里云

服务状态：正常

删除

密钥ID：

所属主账号：

接入混合云

选择云类型

阿里云

华为云 (敬请期待)

Amazon

创建子账号的方式

快速配置

1分钟完成，但权限较大，需要配置主账号AK。

手动配置

5分钟完成，更加灵活的控制权限范围，但权限用于子账号配置。

收起配置指引

第 1/3 步

登录阿里云RAM控制台，将鼠标悬停

阿里云

快速配置

手动配置

自定义策略

详细配置

操作指引

快速配置：1分钟完成，但权限较大，需要配置主账号AK。

手动配置：5分钟完成，更加灵活的控制权限范围，但权限用于子账号配置。

主账号SecretID

请输入主账号SecretID（如：AKID0sXFpnQr8E8SAJOIASQJG

主账号SecretKey

请输入SecretKey

为防止主账号AK泄露，请在完成接入流程后创建完子账号自动并

接入权限说明

主机资产

其他设置

配置完成后立即进行一次资产和数据同步

接入

取消

升级版本：免费的基础版防护能力较弱，您可单击[升级版本](#)或[前往批量授权](#)跳转至 [授权管理](#) 页面，您可购买高版本的防护授权并绑定基础版主机便可升级防护。

版权所有：腾讯云计算（北京）有限责任公司

第17 共145页

资产清理：腾讯云主机销毁后将会自动被清理，但主机安全无法知晓非腾讯云主机的销毁状态，您可针对非腾讯云主机设置清理规则，当非腾讯云主机的客户端离线一定时长则自动清理。

资产清理

腾讯云主机销毁后将会自动被清理，但主机安全无法知晓非腾讯云主机的销毁状态，您可针对非腾讯云主机设置清理规则。

清理设置

自动清理

当检测到非腾讯云主机客户端离线一定时间后，将自动清理主机，解绑授权防护。

清理规则

非腾讯云主机离线

8天

则自动清理

自动清理记录

重新安装客户端

删除记录

自动清理时间

自动清理时间

请输入主机名称/实例ID/公网/内网IP搜索

	主机名称/实例ID	IP地址	客户端末次离线时间	自动清理时间	操作
☐		公网	2024-01-27 10:06:00	2024-02-04 12:16:03	删除记录
☐		公网	2024-01-17 15:56:00	2024-01-25 16:01:25	删除记录
☐		公网	2024-01-11 00:53:00	2024-01-19 01:06:45	删除记录
☐		公网	2024-01-17 15:56:00	2024-01-18 17:15:18	删除记录
☐		公网	2024-01-11 00:53:00	2024-01-18 17:15:18	删除记录
☐		公网	2024-01-08 21:19:00	2024-01-18 17:15:16	删除记录
☐		公网	2024-01-16 09:05:00	2024-01-18 17:15:16	删除记录
☐		公网	2024-01-09 11:13:00	2024-01-17 12:15:31	删除记录

主机列表

在主机列表页面，您可查看每台主机的风险状态、防护状态及风险情况。

版权所有：腾讯云计算（北京）有限责任公司

第18 共145页

主机名称/实例ID	IP地址	IPlist①	操作系统	地域/所属网络	风险状态	入侵检测	漏洞风险	基线风险	网络风险	标签	
		0			未知	0	0	0	0	标签(1)	
		0			未知	0	0	0	0	标签(1)	
		0			未知	0	0	0	0	暂无标签	
		0			未知	0	0	0	0	暂无标签	
		0			未知	0	0	0	0	标签(1)	
		0			未知	0	0	0	0	暂无标签	
		0			未知	0	0	0	0	暂无标签	
		5			风险	2	0	3	0	标签(1)	
		15			未知	0	0	0	0	暂无标签	
		1			风险	2	0	0	0	暂无标签	

字段说明：

- 主机名称/实例 ID：主机的名称和实例 ID。
- IP 地址：主机的公网 IP 和内网 IP 地址。
- IPlist：网卡 IP 列表。
- 操作系统：主机的操作系统。
- 地域/所属网络：主机所属地理位置及网络。
- 风险状态：
- 未知：主机未安装客户端、主机仅安装客户端但未发现风险（基础版防护较弱，可能存在潜在风险）。
- 风险：主机已检出风险。
- 入侵检测：统计主机存在文件查杀、异常登录、密码破解、恶意请求、高危命令、本地提权、反弹 Shell 的风险数。
- 漏洞风险：统计主机存在 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞的风险数。
- 基线风险：统计主机未通过基线检测项数。
- 网络风险：统计主机被监测到的网络攻击数。
- 标签：主机已关联的标签信息。
- agent 状态：
- 未防护：主机属于腾讯云主机，但未安装主机安全客户端。
- 防护中：主机已安装主机安全客户端（处于基础版及以上版本）。
- 已离线：腾讯云或非腾讯云主机的客户端已离线，或非腾讯云主机已关机。
- 已关机：腾讯云主机已关机。

防护版本：基础版、专业版、旗舰版、-（代表无防护）。

操作：

安装客户端：针对无防护主机提供安装指引入口。

重新安装：针对客户端已离线、已关机的主机提供安装指引入口。

卸载：针对防护中的主机提供快捷卸载入口。

授权管理：针对付费防护版本的主机提供授权管理入口，单击可跳转至 [授权管理](#) 页面，可进行授权换绑、解绑等操作。

备注：针对无防护的主机提供备注操作，可备注不防护该主机的原因，便于后续管理（若后续安装了客户端，则备注不可见）。

说明：

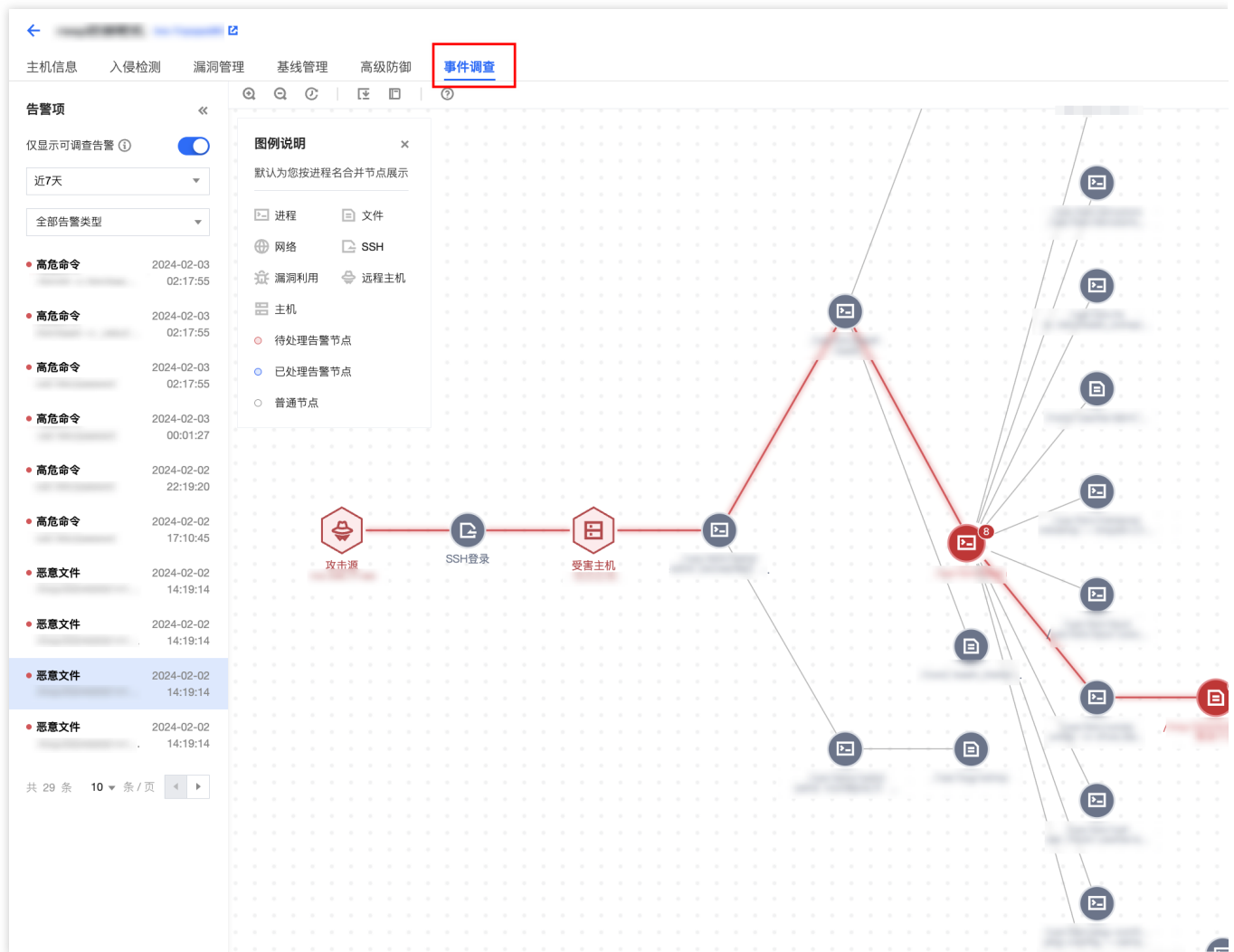
未防护主机、已离线主机满足以下4个条件，单击**安装客户端**或**重新安装**时可一键快速安装。

1. 主机为腾讯云服务器 CVM、轻量应用服务器 Lighthouse。
2. 主机处于开机状态。
3. 主机所属网络为 VPC 网络。
4. 主机已安装 tat 自动化小助手。

单击入侵检测、漏洞风险、基线风险、网络风险的**数值**可跳转查看风险详情。

主机名称/实例ID	IP地址	IPlist ⓘ	操作系统 ▾	地域/所属网络 ▾	风险状态	入侵检测	漏洞风险	基线风险	网络风险	标签
	公 内	13			风险	7	0	3	0	标签(1)

单击**事件调查**，支持可视化查看攻击事件。



操作说明：

针对当前主机，选择一条告警数据，即可在画面中部展示该主机进程运行过程，并高亮展示触发告警的节点。

单击**告警节点**，可查看该节点相关的告警，支持查看告警详情、对待处理的告警进行处理。

若存在合并节点，可对合并节点进行查看。

资产指纹

最近更新时间：2024-08-13 16:29:49

本文将为您介绍资产指纹的功能和操作。

概述

采集资产指纹，可为您提供主机资源监控、账号、端口、进程等详细的资产盘点数据，同时，您也可以基于资产指纹功能，对已发生的安全事件风险影响面进行快速调查。

限制说明

仅付费防护版本的主机才可采集资产指纹数据，基础版主机须先 [升级版本](#)。

各版本支持采集的资产指纹如下：

防护版本	采集的资产指纹
基础版（免费）	不支持
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、系统安装包

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。

操作指南

1. 登录 [主机安全控制台](#)，单击左侧导航中的**资产指纹**。
2. 在资产指纹页面，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

资源监控

账号

端口

软件应用

进程

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

系统安装包

全部CPU负载

全部内存使用率

全部硬盘使用率

仅查看今日新增 (0)

主机名称/实例ID	IP地址	操作系统	CPU信息	CPU负载	内存使用率
tc-1in	公1 内1	TencentOS Server 2.4 (TK4)		16核 低	32 GB 47.38%
tc-1in	公 内	TencentOS Server 2.4 (TK4)	A	16核 低	32 GB 49.37%
tc-1in	公4 内1	CentOS 7.9 64位	Ir	32核 低	63 GB 13.37%
tc-1ins	公1 内1	TencentOS Server 2.4 (TK4)	A	16核 低	32 GB 47.17%
未命名	公-- 内--	--		16核 低	32 GB 37.76%
未命名	公-- 内--	--		16核 低	32 GB 46.76%
t-1li	公1 内1	TencentOS Server 2.4 (TK4)	AI	8核 低	16 GB 20.73%

资产指纹分类说明如下：

资源监控

对服务器系统负载、内存使用、硬盘使用进行数据采集。

资产指纹分类

资源监控

账号

端口

软件应用

进程

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

系统安装包

全部CPU负载

全部内存使用率

全部硬盘使用率

仅查看今日新增 (0)

主机名称/实例ID	IP地址	操作系统	CPU信息	CPU负载	内存使用率
tc-1in	公1 内1	TencentOS Server 2.4 (TK4)		16核 低	32 GB 47.38%
tc-1in	公 内	TencentOS Server 2.4 (TK4)	A	16核 低	32 GB 49.37%
tc-1in	公4 内1	CentOS 7.9 64位	Ir	32核 低	63 GB 13.37%
tc-1ins	公1 内1	TencentOS Server 2.4 (TK4)	A	16核 低	32 GB 47.17%
未命名	公-- 内--	--		16核 低	32 GB 37.76%
未命名	公-- 内--	--		16核 低	32 GB 46.76%
t-1li	公1 内1	TencentOS Server 2.4 (TK4)	AI	8核 低	16 GB 20.73%

账号

对服务器所有账号进行采集。

资产指纹分类

资源监控

账号

端口 +3

软件应用 +26

进程 +515

数据库 +3

Web应用

Web服务

Web框架 +1

Web站点

Jar包 +3

启动服务

计划任务

环境变量 +3

内核模块

系统安装包 +301

全部登录方式

选择最后登录时间

选择最后登录时间

仅查看今日新增 (0)

主机名称/实例ID	IP地址	操作系统	账号名称	UID	账号状态	root权限
	公 1 内 1	CentOS 7.7 64位	NEW	59	禁用	否
	公 1 内 1	CentOS 7.7 64位	NEW	5	禁用	否
	公 1 内 1	CentOS 7.7 64位	lp NEW	4	禁用	否
	公 1 内 1	CentOS 7.7 64位	NEW	38	禁用	否
	公 1 内 1	CentOS 7.7 64位	NEW	11	禁用	否
	公 1 内 1	CentOS 7.7 64位	NEW	0	启用	是
	公 1 内 1	CentOS 7.7 64位	NEW	995	禁用	否

端口

对服务器所有已使用端口进行采集。

资产指纹分类

资源监控

账号

端口 +3

软件应用 +26

进程 +515

数据库 +3

Web应用

Web服务

Web框架 +1

Web站点

Jar包 +3

启动服务

计划任务

环境变量 +3

内核模块

系统安装包 +301

选择进程启动时间

选择进程启动时间

全部端口协议

仅查看今日新增 (3)

主机名称/实例ID	IP地址	操作系统	端口	端口协议	绑定IP
	公 51 内	CentOS 7.7 64位	1 NEW	udp	
	公 5.4 内	CentOS Stream 9 64位		tcp	
	公 4 内 1	CentOS Stream 9 64位		udp	
	公 4 内 1	CentOS Stream 9 64位		udp	
	公 1 内 1	CentOS 7.6 64位	NEW	tcp	
	公 1 内 1	CentOS 7.6 64位	NEW	tcp	
	公 5 内 1	CentOS 7.6 64位	NEW	udp	

进程

对服务器的所有运行进程进行采集。

资产指纹分类

资源监控

账号

端口 +3

软件应用 +26

进程 +515

数据库 +3

Web应用

Web服务

Web框架 +1

Web站点

Jar包 +3

启动服务

计划任务

环境变量 +3

内核模块

系统安装包 +301

选择进程启动时间 选择进程启动时间 日历

☐ 仅查看今日新增 (515)

主机名称/实例ID	IP地址	操作系统	进程名	进程状态	进程版本
	公网	TencentOS Server 2.4 (TK4)	IEW	S (可中断)	8.22
	公网	CentOS 8.4 64位	EW	S (可中断)	--
	公网	Windows Server 2012 R2 数...	exe NEW	--	6.3.9600.19598
	公网	Windows Server 2012 R2 数...	exe NEW	--	--
	公网	Windows Server 2019 数据中...	exe NEW	--	10.0.17763.3232
	公网	Windows Server 2019 数据中...	exe NEW	--	--
	公网	CentOS 8.4 64位	EW	S (可中断)	8.0p1

软件应用

对服务器所有运行中的软件应用进行采集。

资产指纹分类

资源监控

账号

端口 +3

软件应用 +26

进程 +515

数据库 +3

Web应用

Web服务

Web框架 +1

Web站点

Jar包 +3

启动服务

计划任务

环境变量 +3

内核模块

系统安装包 +301

全部应用类型

☐ 仅查看今日新增 (26)

主机名称/实例ID	IP地址	操作系统	应用名称	应用类型	版本
	公网	CentOS 7.9 64位	Nginx①	WEB运维	--
	公网	CentOS 7.9 64位	PHP-FPM①	其他	--
	公网	CentOS 7.9 64位	PHP-FPM①	其他	--
	公网	TencentOS Server 2.4 (TK4)	Nginx①	WEB运维	--
	公网	TencentOS Server 2.4 (TK4)	Nginx①	WEB运维	--
	公网	TencentOS Server 2.4 (TK4)	Nginx①	WEB运维	--
	公网	CentOS 7.6 64位	PHP-FPM①	其他	7.4.30

数据库

对服务器所有运行的数据库进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	全部数据库名 全部端口协议 ☐ 仅查看今日新增 (3)						
	主机名称/实例ID	IP地址	操作系统	数据库名	版本	监听端口	端口协议
	it-1	10.1.1.1	CentOS 7.6 64位	MongoDB NEW	4.2.15		tcp
	it-1	10.1.1.1	CentOS 7.7 64位	MySQL NEW	5.7.42		tcp
	it-1	10.1.1.1	CentOS 7.7 64位	Redis NEW	--		--
	it-1	10.1.1.1	CentOS 7.9 64位	MySQL NEW	5.7.38		tcp
	it-1	10.1.1.1	CentOS 7.6 64位	MongoDB NEW	4.2.15		tcp
	it-1	10.1.1.1	CentOS 7.7 64位	MySQL NEW	5.7.31		tcp
	it-1	10.1.1.1	CentOS 8.0 64位	MySQL	8.0.21		tcp

Web 应用

对服务器所有运行的 Web 应用进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	全部服务类型 ☐ 仅查看今日新增 (0)						
	主机名称/实例ID	IP地址	操作系统	应用名	版本	服务类型	站点域名
	it-1	10.1.1.1	CentOS 7.7 64位	phpMyAdmin①	4.0.10	Nginx	*
	it-1	10.1.1.1	CentOS 7.7 64位	Discuz!ML①	3.4	Nginx	*
	it-1	10.1.1.1	CentOS 8.0 64位	WordPress①	6.2	Apache	*
	it-1	10.1.1.1	CentOS 8.0 64位	phpMyAdmin①	4.9.7	Apache	*
	it-1	10.1.1.1	CentOS 7.9 64位	phpMyAdmin①	5.2.0	Nginx	*
	it-1	10.1.1.1	CentOS 7.9 64位	phpMyAdmin①	4.6.0	Apache	*
	it-1	10.1.1.1	CentOS Linux release 7...	phpMyAdmin①	4.6.0	Apache	*

Web 服务

对服务器所有运行的 Web 服务进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	全部Web服务名		☐ 仅查看今日新增 (0)				
	主机名称/实例ID	IP地址	操作系统	Web服务名	版本	运行用户	二进制路径
		公网	TencentOS Server 2.4 (T...	Nginx	--	--	/usr
		公网	--	Nginx	--	--	/usr
		公网	CentOS 7.6 64位	Nginx	1.20.1	root	/usr
		公网	CentOS 7.9 64位	Apache	2.4.6	root	/usr
		公网	Ubuntu Server 22.04 LT...	Apache	2.4.52	root	/usr
		公网	CentOS Linux release 7....	Apache	2.4.6	root	/usr
		公网	CentOS 7.7 64位	Nginx NEW	1.20.1	--	/usr
		公网					

Web 框架

对服务器所有应用的 Web 框架进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	全部服务类型		☐ 仅查看今日新增 (1)				
	主机名称/实例ID	IP地址	操作系统	框架名	框架语言	框架版本	
		公网	CentOS Linux release 7.9.2009 (C...	vaadin NEW	Java		
		公网	CentOS 7.6 64位	jackson	Java		
		公网	CentOS 7.6 64位	jackson	Java		
		公网	CentOS 7.6 64位	jackson	Java		
		公网	CentOS Linux release 7.9.2009 (C...	velocity	Java		
		公网	CentOS Linux release 7.9.2009 (C...	spring MVC	Java		
		公网	CentOS Linux release 7.9.2009 (C...	spring	Java		
		公网					

Web站点

对服务器所有部署的Web站点进行采集。

资产指纹分类		全部服务类型		全部站点协议		☐ 仅查看今日新增 (0)	
资源监控		主机名称/实例ID	IP地址	操作系统	域名	站点端口	站点协议
账号							
端口	+3		公网	CentOS 7.6 64位			http
软件应用	+26		公网	CentOS 7.6 64位			http
进程	+515		公网	CentOS 7.6 64位			http
数据库	+3		公网	CentOS 7.9 64位			http
Web应用			公网	CentOS 7.6 64位			http
Web服务			公网	CentOS 7.6 64位			http
Web框架	+1		公网	CentOS 7.6 64位			http
Web站点			公网	CentOS 7.6 64位			http
Jar包	+3		公网	CentOS 7.6 64位			http
启动服务			公网	CentOS 7.6 64位			http
计划任务			公网	CentOS 7.6 64位			http
环境变量	+3		公网	CentOS 7.6 64位			http
内核模块			公网	CentOS 7.6 64位			http
系统安装包	+301		公网	CentOS 7.6 64位			http

Jar 包

对服务器所有的 Jar 包进行采集。

资产指纹分类

资源监控

账号

端口 +3

软件应用 +26

进程 +515

数据库 +3

Web应用

Web服务

Web框架 +1

Web站点

Jar包 +3

启动服务

计划任务

环境变量 +3

内核模块

系统安装包 +301

全部类型

☐ 仅查看今日新增 (3)

主机名称/实例ID	IP地址	操作系统	包名	类型	是否可执行
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否
10.10.10.10	公网	CentOS 7.6 64位	1.1.1.jar	NEW 其他	否

启动服务

对服务器所有的启动服务进行采集。

资产指纹分类	全部类型	☐ 仅查看今日新增 (0)					
	主机名称/实例ID	IP地址	操作系统	启动项名	默认启动状态	类型	
	账号						
	端口 +3						
	软件应用 +26						
	进程 +515						
	数据库 +3						
	Web应用						
	Web服务						
	Web框架 +1						
启动服务	Web站点						
	Jar包 +3						
	计划任务						
	环境变量 +3						
	内核模块						
	系统安装包 +301	83407					

计划任务

对服务器所有的计划任务进行采集。

资产指纹分类	全部服务启用状态	☐ 仅查看今日新增 (0)					
	主机名称/实例ID	IP地址	操作系统	执行命令或脚本	执行用户	配置文件路径	
	账号						
	端口 +3						
	软件应用 +26						
	进程 +515						
	数据库 +3						
	Web应用						
	Web服务						
	Web框架 +1						
计划任务	Web站点						
	Jar包 +3						
	计划任务						
	环境变量 +3						
	内核模块						
	系统安装包 +301	8					

环境变量

对服务器所有的环境变量进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	全部环境变量类型 ☐ 仅查看今日新增 (3)		主机名称/实例ID	IP地址	操作系统	环境变量名	环境变量类型
				公内	CentOS 7.7 64位		系统变量
				公内	CentOS 7.7 64位		系统变量
				公内	CentOS 7.7 64位	EW	用户变量
				公内	CentOS 7.7 64位		用户变量
				公内	CentOS 7.7 64位	N	用户变量
				公内	CentOS 7.7 64位	NEW	用户变量
				公内	CentOS 7.7 64位	ES NEW	用户变量
				公内	CentOS 7.7 64位	NEW	用户变量
				公内	CentOS 7.7 64位		

内核模块

对服务器的所有内核模块进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	☐ 仅查看今日新增 (0)		主机名称/实例ID	IP地址	操作系统	名称	描述	路径	版本	大小
				公内	Ubuntu Server 18.04 ...		Mellanox 5th generati...	/	5.4-3.1.0	
				公内	Ubuntu Server 18.04 ...		Mellanox 5th generati...	/	5.4-3.6.8	
				公内	TencentOS Server 2...		Mellanox 5th generati...	/	5.4-3.1.0	
				公内	TencentOS Server 2...		Mellanox 5th generati...	/	5.4-3.1.0	
				公内	Ubuntu Server 22.04 ...	ar	DRM KMS helper	/	--	
				公内	OpenCloudOS Server 8	ar	DRM KMS helper	/	--	
				公内	Ubuntu Server 22.04 ...	ar	DRM KMS helper	/	--	
				公内	Ubuntu Server 22.04 ...	ar	DRM KMS helper	/	--	
				公内	Ubuntu Server 22.04 ...	ar	DRM KMS helper	/	--	

系统安装包

对服务器的系统安装包进行采集。

资产指纹分类 资源监控 账号 端口 +3 软件应用 +26 进程 +515 数据库 +3 Web应用 Web服务 Web框架 +1 Web站点 Jar包 +3 启动服务 计划任务 环境变量 +3 内核模块 系统安装包 +301	选择安装时间		选择安装时间		全部安装包类型		☐ 仅查看今日新增 (301)	
	主机名称/实例ID	IP地址	操作系统	包名	总述	版本		
		公网	TencentOS Server 3.1 (TK4)			2.4.37		
		公网	TencentOS Server 3.1 (TK4)	stem NEW		2.4.37		
		公网	TencentOS Server 3.1 (TK4)	NEW		1.15.7		
		公网	TencentOS Server 3.1 (TK4)	NEW		2.4.37		
		公网	TencentOS Server 3.1 (TK4)	ogo... NEW		85.9		
		公网	CentOS 7.6 64位	NEW		8.1.2		
		公网	CentOS 7.6 64位	NEW		2.7.5		
		公网	CentOS 7.6 64位	W		2.7.5		

漏洞管理

最近更新时间：2024-08-13 16:29:50

本文将为您介绍漏洞管理的功能和操作，帮助您管理服务器中的漏洞风险。

概述

腾讯云主机安全支持对目前主流主机（Windows，Linux 等）上的漏洞进行周期性和及时性的检测功能。主机安全支持对指定主机和漏洞类别的检测，同时支持忽略漏洞等功能，可为您提供漏洞的风险、特征、严重等级及修复建议等信息，可视化界面有助于您更好的管理服务器中的漏洞风险。

限制说明

至少存在1台已绑定防护授权的主机（**专业版/旗舰版**），才可解锁漏洞管理功能。

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	×	×

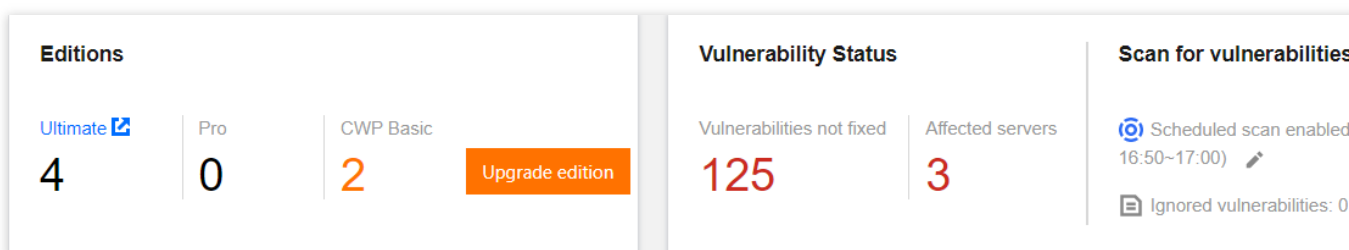
因漏洞修复可能对用户业务造成影响，漏洞自动修复并非检出漏洞后立即进行自动化修复，须用户了解漏洞后单击**修复**并进行数据备份，才可进行自动化修复。

操作指南

1. 登录 [主机安全控制台](#)。
2. 单击左侧导航中的**漏洞管理**，各功能说明如下。

漏洞扫描

在**漏洞扫描**区域中，您可进行一键扫描，获取漏洞扫描的结果，也可设置定时扫描，及时暴露漏洞风险并进行处理。



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，设置后可立即扫描。

一键扫描设置

扫描漏洞类别

☒ 应急漏洞 ☒ Linux软件漏洞 ☒ Windows系统漏洞 ☒ Web-CMS漏洞 ☒ 应用漏洞

漏洞扫描等级

☒ 严重 ☒ 高危 ☒ 中危 ☒ 低危

超时设置 ①

若任务下发后扫描时长超出 小时，即视为扫描失败

选择扫描服务器

服务器分类 ☒ 全部专业版和旗舰版服务器 ☐ 自选服务器

立即扫描

取消

漏洞设置

定时扫描

漏洞防御

忽略漏洞

开启定时扫描

☒

扫描漏洞类别

☒ 应急漏洞 ☒ Linux软件漏洞 ☒ Windows系统漏洞 ☒

漏洞扫描等级

☒ 严重 ☒ 高危 ☒ 中危 ☒ 低危

定时扫描周期

每天

00:00 ~ 02:00

(设置后会在周期选定的时间点开始定时扫描)

选择扫描服务器

服务器分类 ☒ 全部专业版和旗舰版服务器 ☐ 自选服务器

立即应用

取消

单击**扫描设置**或**定时扫描**的编辑图标，可打开**漏洞设置**弹窗并锚点至**定时扫描**，您可对定时扫描开关、定时扫描周期、漏洞等级及漏洞类别进行设置，设置后可立即应用。

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。

漏洞设置

定时扫描漏洞防御忽略漏洞

漏洞防御

防御开关 可防御全网热点攻击漏洞：202个

漏洞防御是腾讯云主机安全为应对频发的0DAY、nDAY漏洞而开发的一套基于虚拟补丁的漏洞防御系统。该系统融合了腾讯前沿的漏洞挖掘技术、实时高危漏洞预警技术，捕捉、分析0DAY漏洞，结合腾讯专家知识，生成虚拟补丁，自动在云主机上生效虚拟补丁，有效拦截黑客攻击行为，为客户修复漏洞争取时间。

防御主机范围 (已选择1台)

主机安全漏洞防御功能可支持腾讯云全网99.9%热点攻击漏洞，该功能属于旗舰版功能，如需防护更多主机资产可点击 升级旗舰版

服务器分类 全部旗舰版主机 (7) 自选旗舰版主机

自选方式 直接勾选

选择区域 全部服务器 全地域

服务器标签 多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

选择主机 选择全部 已选择 1 台主机 清空选择

请输入主机名称/实例ID/IP地址进行搜索			
主机名称/实例ID	IP地址	防护版本	待修复漏洞
☐	公内	旗舰版	0
☐	公内	旗舰版	0
☐	公内	旗舰版	53
☐	公内	旗舰版	25
☐	公	旗舰版	70

请输入主机名称/实例ID/IP地址进行搜索			
主机名称/实例...	IP地址	防护版本	待修复漏洞
	公内	旗舰版	0

立即生效 取消

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。

已防御攻击 (15)

请选择时间

请选择时间

请选择资源属性后输入关键字进行过滤(仅支持单个值)

Q

🔄

☆

⬇️

主机名称/实例ID	IP地址	目标端口	攻击来源IP/地址	漏洞名称	攻击时间	防御次数	操作
...	公	-	...	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)	首次: 2024-01-15 06:12:39 最近: 2024-01-15 06:23:21	3	详情 删除
...	公	-	...	Apache Druid 远程代码执行漏洞 (CVE-2021-25646)	首次: 2024-01-15 06:12:39 最近: 2024-01-15 06:23:16	3	详情 删除
...	公	-	...	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)	首次: 2024-01-14 06:11:28 最近: 2024-01-14 11:35:23	4	详情 删除
...	公	-	...	Apache Druid 远程代码执行漏洞 (CVE-2021-25646)	首次: 2024-01-14 06:11:25 最近: 2024-01-14 11:35:23	4	详情 删除
...	公	-	...	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)	首次: 2024-01-13 06:13:42 最近: 2024-01-13 11:32:23	4	详情 删除
...	公	-	...	Apache Druid 远程代码执行漏洞 (CVE-2021-25646)	首次: 2024-01-13 06:13:41 最近: 2024-01-13 11:32:22	4	详情 删除
...	公	-	...	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)	首次: 2024-01-12 06:11:19 最近: 2024-01-12 17:56:27	24	详情 删除
...	公	-	...	Apache Druid 远程代码执行漏洞 (CVE-2021-25646)	首次: 2024-01-12 06:11:18 最近: 2024-01-12 17:56:25	24	详情 删除
...	公	-	...	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)	首次: 2024-01-11 06:11:27 最近: 2024-01-11	13	详情 删除

漏洞攻击告警详情

已防御

[删除记录](#)

风险主机

主机名称: ... 客户端离线

实例 ID: ...

内: ... 外: ...

告警详情

漏洞名称: [详情](#)

Apache log4j2 远程代码执行漏洞 (CVE-2021-442)

攻击源IP: ...

危害描述

告警描述: 腾讯安全注意到, 一个Apache Log4j2高危漏洞细节已被公开, 触发此漏洞, 成功利用此漏洞可以在目标服务器上执行任意命令。

修复建议

建议方案: 请注意, 只有 log4j-core JAR 文件受此漏洞影响, 仅使用 io 受影响的用户尽快升级到2.16.0及以上版本。
最新安全版本请参考官方安全通告: <https://logging.apache.org/log4j/2.x/download.html>
漏洞缓解措施 (仍会检出漏洞):
(1) 从类路径中删除 JndiLookup 类: `zip -q -d log4j-core`
腾讯云WAF和云防火墙均已支持该漏洞防护
WAF试用: <https://cloud.tencent.com/act/pro/clbwaferterp>
配置WAF: <https://console.cloud.tencent.com/guanjia/tea>
云防火墙试用: <https://console.cloud.tencent.com/cfw/ips>

网络攻击信息

攻击包: ...

漏洞处置

1. 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。

分类下展示热度攻击漏洞, 以及严重/高危漏洞, 需要优先修复处理, 默认统计待修复漏洞数量。您也可以点击 [自定义规则](#)

高优修复漏洞 ①

520 ↑

今日新增 0

全部漏洞

763 ↑

今日新增 0

影响主机

85 台

今日新增 0

网络攻击事件 (近)

1408 ↓

今日新增

网络攻击基于腾讯云安全攻防的恶意流量, 包含攻击成功、

字段说明:

- 高优修复漏洞: 该分类下展示热度攻击漏洞, 以及严重/高危漏洞, 需要优先修复处理, 默认统计待修复漏洞数量。单击自定义规则可对高优修复漏洞进行自定义规则判定。
- 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25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、全部漏洞两类, 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。

应急漏洞

全部漏洞

自动修复

更多处理

全部漏洞标签

高危, 严重

待修复

仅展示高优修复漏洞

判定规则

☐	漏洞名称/标签	检测方式	漏洞类型	威胁等级	全网攻击热度	CVSS	CVE编号	最后扫描时间	影响主机
☐	PostgreSQL JDBC远... 远程利用	版本对比	应用漏洞	严重		9.8	CVE-2...	2023-06-08 11:27:54	1
☐	PostgreSQL JDBC Dri... 远程利用	版本对比	应用漏洞	高危		8	CVE-2...	2023-06-08 11:27:54	1

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）。
- 检测方式：版本对比、POC 验证。
- 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、修复失败。
- 自动修复状态：暂不支持修复、可自动修复（无需重启）、可自动修复（需重启）。
- 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：当前已支持部分 Linux 软件漏洞、Web-CMS 漏洞进行自动修复，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，详情请参见 [漏洞自动修复](#)。
- 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。

基线管理

最近更新时间：2024-08-13 16:29:50

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。

概述

腾讯云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，提供基线和检测项的风险等级和修复建议，提供腾讯云默认基线策略，有助于您更好的管理服务器中的基线安全。

主机安全版本

基础版：首次使用时，支持对默认策略内的全量主机进行检测，只展示5条结果。不支持对基线策略的管理、对策略的一键检测及周期检测。

专业版：支持基线策略的管理，支持用户自己新建或编辑策略，支持对基线策略的周期检测与一键检测功能。

旗舰版：支持基线策略的管理，支持用户自己新建或编辑策略，支持对基线策略的周期检测与一键检测功能。支持弱口令自定义。

操作指南

1. 登录 [主机安全控制台](#)，在左侧导航栏中，选择**基线管理**。
2. 在基线管理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。

腾讯云默认基线策略：腾讯云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：弱密码策略、CIS 基线策略、腾讯云最佳安全实践策略。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7天检测一次（当天零点）。

说明：

策略的通过率 = 已通过该策略下全部检测项的服务器数 / 该策略下全部检测的服务器数



新增基线策略

1.1 基线检测结果展示模块右上角，单击**基线设置**。



1.2 在设置页面的基线策略设置页面，单击**新增策略**。

1.3 在新增基线策略页面，输入策略项名称（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。
腾讯云默认策略会保存在“系统策略”标签内。

← 新增策略

1 创建策略

2 选择应用资产

* 策略名称

请输入策略名称

* 检测周期

每天

09:35:30

🕒

推荐检测时间为：09:35:30，可以避开和其他任务的冲突

* 检测规则

一键全选

全部规则类型

请输入检测规则进行

检测规则	检测规则分类	检测规则说明
✓ 国际标准-CentOS 6安全基线检查Level1	等保合规	国际标准-CentOS 6安全基线检查Level1
✓ 国际标准-CentOS 6安全基线检查Level2	等保合规	国际标准-CentOS 6安全基线检查Level2
✓ 国际标准-CentOS 7安全基线检查Level1	等保合规	国际标准-CentOS 7安全基线检查Level1
✓ 国际标准-CentOS 7安全基线检查Level2	等保合规	国际标准-CentOS 7安全基线检查Level2
✓ 国际标准-CentOS 8安全基线检查Level1	等保合规	国际标准-CentOS 8安全基线检查Level1
✓ 国际标准-CentOS 8安全基线检查Level2	等保合规	国际标准-CentOS 8安全基线检查Level2
✓ 国际标准-Ubuntu 14安全基线检查Level1	等保合规	国际标准-Ubuntu 14安全基线检查Level1
✓ 国际标准-Ubuntu 14安全基线检查Level2	等保合规	国际标准-Ubuntu 14安全基线检查Level2
✓ 国际标准-Ubuntu 16安全基线检查Level1	等保合规	国际标准-Ubuntu 16安全基线检查Level1
✓ 国际标准-Ubuntu 16安全基线检查Level2	等保合规	国际标准-Ubuntu 16安全基线检查Level2

共 90 条

10 条 / 页

1.4 根据实际需求选择应用资产，单击完成。

创建策略配置

2 选择

* 应用资产

☐ 全部专业版和旗舰版服务器 ☐ 自选服务器 ☒ 手动输入IP

* IP地址

示例：192.138.11.00-192.168.11.245、18.16.171.11

0

请输入IP地址或IP段(仅支持内网IP)，手动输入使用回车换行，每行一个；示例：192.138.11.00-192.168.11.245、18.16.171.11
外部复制黏贴多个IP地址，请用英文逗号","分隔；若输入重复IP，后台将自动合并

基线检测

腾讯云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。

说明

若非首次基线检测，需开通 [主机安全专业版或旗舰版](#) 才可进行基线检测。

一键检测

首次检测：当您首次使用基线检测功能时，我们为您提供一次全量基线策略和全服务器的检测服务，协助您发现基线安全风险，并展示其中5条基线风险。若您所需更多的基线安全功能，建议 [升级专业版或旗舰版](#)。

1.1 基线检测结果展示模块，单击**试用检测**。

基线策略

检测服务器

检测项

240 台

0 项

1.2 在“检测提示”弹窗中：

操作1：选择需要检测的基线策略，单击**开始检测**（检测一般持续2 - 5分钟），检测完成后，检测结果会以可视化图表的方式显示在漏洞管理页面。

检测提示

注：默认免费试用检测弱密码口令基线功能一次，扫描您的全部云上主机并提供5条累计基线风险项，如需彻底检测基线风险和满足等保合规的要求，请升级专业版。[了解更多](#)

请选择您要检测的基线策略

☒ 弱密码

☒ 等保二级

☒ 等保三级

☒ CIS基线

☒ 最佳实践

开始检测

立即升级

操作2：单击 [立即升级](#)，跳转至主机安全升级界面，将云服务器升级为专业版。

非首次检测：当您非首次使用基线检测时，选择需要检测的基线策略后，单击 **一键检测**（检测一般持续2 - 10分钟）若您尚未存在专业版服务器，建议立即 [升级专业版](#)。

周期检测

- 1. 在基线管理页面右上角，单击**基线检测设置**。
- 2. 在基线检测设置页签，可以进行周期检测设置并进行忽略检测项管理。

周期检测设置：在检测策略设置标签，您可以新建或编辑策略、设置检测周期，同时可以开启或关闭定期检测策略，支持对用户自定义策略的删除。

策略名称	基线规则数 ↓	基线检查项 ↑	应用服务器数 ↑	检测周期	策略开关
ni			0	间隔1天 11:20:30	☐
			23	间隔1天 14:01:00	☒
			90	间隔1天 22:50:00	☒
			79	间隔1天 01:35:30	☒

忽略检测项管理：在忽略检测项管理标签内，查看已忽略的检测项及其详情，并可进行取消忽略操作。

检测策略设置

检测规则说明

忽略规则设置

自定义弱口令

新增忽略规则

请输入忽略规则

忽略规则	忽略项	应用服务器数 ↓
检测规则视...	MongoDB未授权访问	4
检测规则视...	MySQL 弱口令检测	4
检测规则视...	多个 (118个)	4

基线数据可视化

当您选择基线策略并检测完成后，您可以在 [基线管理](#)，查看本次检测服务器的数量、检测项数量、该基线策略的通过率、基线检测项 TOP5 及服务器风险 TOP5，并按照威胁等级来进行划分。



基线结果列表

在 [基线管理](#) 页下方，可查看基线检测结果列表，支持查看基线详情，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。

检测规则视角

检测项视角

主机视角

选择时间

选择时间

重新检测

全部处理状态

	检测规则	具体检测项	检测服务器数 ↓	首次检测时间 ↑	最后检测时间 ↑
☒	Tomcr	1	50	2023-07-14 08:21:36	2023-07-20 08:10
☒	Activ	1	50	2023-07-14 08:21:36	2023-07-20 08:10
☐	Rsy	1	49	2023-07-14 08:21:36	2023-07-20 08:10

字段说明：

基线名称：基线包名称，包含若干相同类别的检测项。

威胁等级：根据基线的危险程度，将其划分为严重、高危、中危和低危四个等级。

基线检测项：该基线包下所有的检测项合计数量。

影响服务器数：表示在该策略所选服务器和检测项下，被检测服务器未全部通过该基线包下的检测项数量，即该基线包影响服务器的数量。

最后检测时间：取最近一次某台服务器检测出该基线包下的检测项的时间。

处理状态：分为“已通过”、“未通过”、“检测中”

操作：支持查看基线详情并对未通过检测的基线重新检测。

重新检测：

方式1：选择需要检测的基线，在列表左上角单击**重新检测**，将批量对基线进行重新检测。

方式2：在目标基线右侧，单击**重新检测**，将重新对该基线进行检测。

查看详情：

在基线检测结果列表中，找到目标基线，在右侧操作栏，单击**查看详情**，进入基线详情页。

在基线详情页面，可查看该基线的描述信息和威胁等级，同时可查看影响服务器的列表。服务器列表支持对单个服务器模糊搜索、支持状态筛选、支持批量对服务器进行“重新检测”、支持查看单个服务器详情，在目标服务器右侧操作栏，单击**详情**，进入检测详情页。

Windows 用户弱口令检测

首次检测时间 2
规则说明 v

服务器检测结果 关联检测项

重新检测 全部处理状态 请选择资源属性后输入关键字

☐	主机名称/实例ID	IP地址	处理状态	最后检测时间 ↓
☐		公 内	未通过	2023-07-20 08:0
☐		公 内	已通过	2023-07-20 08:0

在检测详情页可查看基本信息，包括基线名称、服务器名称和检测项详情列表。

首次检测时间 2023-08-15 01:37:49

检测项

重新检测 全部威胁等级 全部处理状态 请选择资源属性后输入关键字

☐	检测项	威胁等级	状态	最后检测时
☐	T	高危	已通过	2023-10-24
检测项描述 To 多详情请访问参考链接。				
检测结果描述				
处理建议 修 作）。				

共 1 项 10 条 / 页

列表支持对多个检测项“重新检测”和“忽略”，忽略后的检测项可进入忽略风险项管理 页面进行查看。
支持对检测项的威胁等级筛选和处理状态筛选。

鼠标停留在检测项时，为您提供该检测项的详细描述和处理建议。

文件查杀

最近更新时间：2024-08-13 16:29:50

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 [主机安全控制台](#)，在左侧导航栏选择**入侵检测 > 文件查杀**。
2. 在文件查杀页面，单击右上角处的**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：

该功能属于专业版/旗舰版功能，请先 [购买防护授权](#) 并绑定主机，升级为专业版/旗舰版主机。

文件查杀支持木马文件检测，全部机器可累计免费检测5条恶意文件安全事件，超过则停止检测，升级为专业版或旗舰版主机安全则没有次数限制，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. 在查杀设置页面，支持定时扫描、实时监控、自动隔离设置。

定时检测：单击**开启定时扫描**，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。

查杀设置

专业版/旗舰版主机均支持定时检测和实时监控，自动隔离功能属于旗舰版功能，建议您 [升级版本](#) 启用更多安全防护功能。

定时扫描

实时监控

自动隔离

开启定时扫描 ☒ 定期扫描主机木马病毒文件，增强安全性

检测模式 ⓘ 快速检测 检测运行中进程、关键目录、驱动加载等

异常进程检测 ☒ 深度检测内存中的异常进程，可能造成一定程度的资源占用率升高，请谨慎选择。

检测周期 每天 00:00 ~ 06:00

检测范围

检测范围 ☒ 全部专业版和旗舰版主机 ☐ 自选服务器

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，推荐检测周期选择4小时以上，避免出现扫描不完整或超时情况。

快速检测：Linux系统会检测运行中进程、关键目录、驱动加载等；Windows 会扫描 C 盘。

全盘检测：Linux 系统除快速检测范围外，还会检测系统所有分区；Windows 会扫描 CDEF 盘。

异常进程检测：深度检测内存中的异常进程，可能造成一定程度的资源占用率升高，请谨慎选择。

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：包括全部专业版本服务器和自选服务器。

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。

查杀设置

专业版/旗舰版主机均支持定时检测和实时监控，自动隔离功能属于旗舰版功能，建议您 [升级版本](#) 启用更多安全防护功能。

定时扫描

实时监控

自动隔离

实时监控



实时监控Web目录、系统关键目录，查杀木马病毒文件

启发式引擎



启发式引擎采用最严格模式实时扫描系统Webshell（开启该引擎可能存在极少误报，若用户确认文件正常，添加白名单）

监控模式

标准（推荐）

监控并扫描检测常见目录下增量文件

说明：

监控模式分为标准和推荐两种模式。

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**，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。

查杀设置

专业版/旗舰版主机均支持定时检测和实时监控，自动隔离功能属于旗舰版功能，建议您 [升级版本](#) 启用更多安全防护功能。

定时扫描

实时监控

自动隔离

开启自动隔离



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，请知悉。

主机安全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，建议您检查文件查杀中的告警列表，确保已全离列表中对文件进行恢复。

☐ 隔离并杀掉恶意文件相关进程，建议勾选。

检测设置概览

1. 登录 [主机安全控制台](#)，在左侧导航栏选择**入侵检测** > **文件查杀**。
2. 在文件查杀页面，单击**一键扫描**，开始设置手动检测模式。



3. 在一键扫描设置页面，设置目标检测模式、主机范围和超时时间后，检测可能会因为文件、目录过多，扫描耗时较长，可以设置单次扫描时长，超时则视为扫描失败。



4. 单击**开启检测**后按照检测设置进行检测，可单击**查看详情**查看检测详情信息。

检测详情

22%

正在进行一键检测...

预计剩余时间1小时34分钟

风险主机/目标检测:

开始检测时间

结束检测时间

停止检测

重新检测

全部状态

请选择资源属性后输入关键字进行过滤(

☐	主机名称/...	IP地址	操作系统	检测状态	待处理风险	检测开始时间	检测结5
☐			linux64_Lin...	检测中	0	2024-07-10 16:47:46	-

检测详情列表包含字段说明如下：

影响服务器：目标服务器的 IP 及名称。

操作系统：目标服务器的操作系统。

检测状态：目标服务器检测完成、检测中及检测失败的检测状态，其中检测失败的原因可能是目标服务器检测超时失败，建议增加超时时长后重新检测，检测失败的原因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：目标服务器检测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：目标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目标服务器再次检测，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目标服务器停止检测，您可以单击**停止检测**。

注意：

选中的服务器将不会被检测，可能存在的风险将不会告警提示，请谨慎操作。

查看详情：若想查看目标服务器的检测结果详情，您可以单击**查看详情**。

查看事件列表

1. 登录 [主机安全控制台](#)，在左侧导航栏选择**入侵检测 > 文件查杀**。
2. 在文件查杀页面，可查看当前受保护的服务器中，木马文件检测情况，如下图所示：

☐	服务器IP/名称	路径	病毒名/检出引擎	威胁等级 ▾	首次发现时间 ↕	最近检测时间 ↓
☐			Win32.Virus.Ramnit.Wrp w	严重	2021-12-14 09:21:30	2022-04-02 05:31
☐			Win32.Virus.Ramnit.Efxx w	严重	2021-12-14 09:21:31	2022-04-02 05:31

事件列表包含字段说明如下：

服务器 IP /名称：当前检测的目标服务器 IP 和名称。

路径：目标风险文件的文件路径，单击



复制路径信息、单击



下载目标风险文件。

病毒名/检出引擎：入侵目标风险文件的病毒名。

首次发现时间：首次检测到目标风险文件出现的时间。

最近检测时间：最近一次检测到目标风险文件出现的时间。

处理状态：目标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：

隔离：若确认文件是恶意的，可以对单个文件进行隔离，或者批量选择文件进行一键隔离。当隔离成功后，原始恶意文件将被加密隔离，后期可以通过筛选**已隔离**文件，进行恢复。

信任：若文件是非恶意的，可以选择信任操作，加入信任后，主机安全将不再对该文件进行检测，可以通过筛选**信任文件**，对信任文件进行管理。

删除记录：该操作仅删除日志记录，不会删除文件，操作后无法再查看相关日志信息，建议您先对文件进行“隔离”、“信任”操作，或根据路径找到相应文件进行手动删除。

详情：若想查看目标风险文件的检测结果详情，可以单击**查看详情**。

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 [提交工单](#) 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：2024-08-13 16:29:50

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 [主机安全控制台](#)。
- 2. 单击左侧导航中的**入侵检测 > 异常登录**，各功能说明如下。

事件列表

在**事件列表**中，可查看并处理主机安全监测到的异常登录风险。

标记已处理 忽略 删除 删除全部记录						选择时间
☐	主机名称/实例ID	IP地址	来源IP	来源地	登录用户名	登录时间 ↓
☐	10.10.10.10	10.10.10.10	10.10.10.10	广东省-深圳市	root	2024-07-11 17:01:39
☐	10.10.10.10	10.10.10.10	10.10.10.10	广东省-深圳市	root	2024-07-11 16:52:06
☐	10.10.10.10	10.10.10.10	10.10.10.10	广东省-深圳市	root	2024-07-11 16:38:16

字段说明：

- 服务器IP/名称：被异常登录的服务器。
- 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IP登录。

已加入白名单：登录来源已被添加为白名单（登录源 IP、登录用户名、登录时间及常用登录地）。

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

在白名单管理中，可增/删/改/查异常登录的白名单。

删除 添加白名单						修改时间
☐	服务器IP/名称	来源IP	常用登录地	登录用户名	登录时间	
☐			中国-广东-广州市	--	--	
☐			中国-广东-广州市	--	--	
☐			--	root	00:00 ~ 23:59	

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：加白名单的时间。

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。

添加白名单

登录条件

登录源ip

登录用户名

root

登录时间

选择时间

选择常用登录地

广州市

生效范围

☐ 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）

☒ 自定义服务器范围

选择服务器（已选1台）

事件处理

☒ 批量加白所有符合该白名单规则的事件

☐ 仅对当前事件加白名单

备注

建议您输入规则的备注

字段说明:

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。

添加白名单

IP示例: 1.1.1.1
IP范围示例: 1.1.1.1-1.1.1.10
IP段示例: 172.168.34.1/20
多个用英文, 隔开

登录条件

登录源ip

172.168.34.0/24

登录用户名

支持多个登录用户名

登录时间

选择时间

选择常用登录地

请选择

生效范围

☒ 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)

☐ 自定义服务器范围

选择服务器

事件处理

批量加白所有符合该白名单规则的事件

备注

建议您输入规则的备注

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。

添加白名单

登录条件

登录源ip

支持多个IP/IP范围/IP段

登录用户名

支持多个登录用户名

登录时间

选择时间

选择常用登录地

香港特别行政区

生效范围

☒ 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）

☐ 自定义服务器范围

选择服务器

事件处理

批量加白所有符合该白名单规则的事件

备注

建议您输入规则的备注

说明：

登录条件支持组合。

如何关闭异常登录告警？

请前往 [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。

入侵检测

告警类型	告警状态	告警时间 ⓘ	告警主机范围
文件查杀-恶意文件	☐	☐ 全天 ☐ 09:00 ~ 18:00 ⌚	无
文件查杀-异常进程	☒	☒ 全天 ☐ 09:00 ~ 18:00 ⌚	全部主机 编辑
异常登录	☒	☒ 全天 ☐ 09:00 ~ 18:00 ⌚	按腾讯云标签选 编辑
密码破解	☒	☒ 全天 ☐ 09:00 ~ 18:00 ⌚	按腾讯云标签选 编辑

密码破解

最近更新时间：2024-08-13 16:29:50

本文档将向您介绍如何配置和使用密码破解监测功能，以提高系统的安全性。

概述

主机安全 [密码破解](#) 基于腾讯云网络安全防御和主机入侵检测能力，为主机提供密码破解行为实时监控，实现自动阻断功能，并支持告警查询、筛选、删除、批量导出等操作。

限制说明

监控范围：监控基础版/专业版/旗舰版主机（Linux 系统及 Windows 系统）关于 SSH 协议/RDP 协议的登录行为。
检测规则及阻断模式：各防护版本关于密码破解行为的判断规则及阻断范围不同，见下表。

主机安全防护版本	检测规则	阻断模式								
基础版	情报规则：基于腾讯安全威胁情报库，为您综合进行黑IP推荐，当命中对应黑IP时，将判定为密码破解行为。 检测规则：命中下述任一登录规则时，将判定为密码破解行为。 <table><tr><th>规则名称</th><th>规则内容</th></tr><tr><td>规则1</td><td>1分钟登录失败次数超过10次</td></tr><tr><td>规则2</td><td>5分钟登录失败次数超过20次</td></tr><tr><td>规则3</td><td>20分钟登录失败次数超过60次</td></tr></table> 说明： 基础版默认检测规则仅上图三条，不支持新增和修改。 若因付费版本到期回退基础版，原设置的检测规则仍生效，但不支持新增和修改。	规则名称	规则内容	规则1	1分钟登录失败次数超过10次	规则2	5分钟登录失败次数超过20次	规则3	20分钟登录失败次数超过60次	基础阻断，即仅针对威胁情报黑 IP 的密码破解行为进行阻断，默认阻断 5 分钟。 说明： 若因付费版本到期回退基础版，阻断模式将自动切换为基础阻断。
规则名称	规则内容									
规则1	1分钟登录失败次数超过10次									
规则2	5分钟登录失败次数超过20次									
规则3	20分钟登录失败次数超过60次									
专业版/旗舰版	包含上述情报规则及检测规则（检测规则支持新增和修改）	高级阻断，即结合腾讯安全库对黑 IP 及命中检测规则的密码破解行为进行阻断。								

iptables 规则：开启阻断后，当监测到主机存在密码破解行为时，来源 IP 会自动添加到 iptables 规则中。

密码破解设置

1. 登录 [主机安全控制台](#)，在左侧导航中，选择 **入侵检测** > **密码破解**。

密码破解设置



检测规则：情报规则+登录规则 [设置](#)



自动阻断：



阻断模式：



2. 单击 **设置**，对密码破解行为的判定规则及阻断规则进行设置。

密码破解设置



- 基础版主机安全将默认按照 [默认密码破解规则](#) 进行判断，如需防护更多主机资产可点击 [升级版本](#)
- 若出现误阻断告警事件，请将爆破来源IP添加至[白名单](#)，可1分钟内解除登录阻断，避免后续产生误阻断。[操作指南](#)

检测规则 (下述2类规则为或关系)

- 情报规则**：基于腾讯安全威胁情报库，为您综合进行黑名单IP推荐，当命中对应黑名单IP时，将判断为暴力破解行为。
- 登录规则**：命中下述任一登陆规则时，将判断为暴力破解行为。(已为您默认提供3条规则)

登录规则1： 1分钟 登录失败次数超过 5次 [重置](#) [+ 添加](#)

登录规则2： 5分钟 登录失败次数超过 10次 [重置](#) [删除](#)

阻断规则

自动阻断 ☒

阻断模式 ☐ 基础阻断：仅针对威胁情报黑IP阻断。
☒ 高级阻断：结合腾讯安全库，对黑IP或登录规则阻断，更全面控制暴力破解攻击。 [推荐](#)
(高级阻断仅针对专业版/旗舰版主机生效，如需防护更多主机资产可点击 [升级版本](#))

生效时长 命中爆破规则时，对不在白名单内的来源IP执行自动阻断，阻断生效时长为 小时 [重置](#)

3. 确认无误后，单击 **保存**。

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 [主机安全控制台](#)，在左侧导航中，选择 **入侵检测** > **密码破解**。

2. 在密码破解页面，单击**白名单管理** > **添加白名单**。



3. 在新增白名单页面中，填写来源 IP 及生效范围，单击**确定**。

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。

满足条件

*来源IP

支持单个IP/IP范围/IP段

i

生效范围

☐ 全部服务器（用户APPID下所有服务器）

☒ 自定义服务器范围 [选择服务器](#)

备注

建议您输入规则的备注

参数说明：

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。

查看密码破解事件

登录 [主机安全控制台](#)，在左侧导航中，选择**入侵检测** > **密码破解**，进入密码破解页面，所有暴力破解事件将会在密码破解列表中展示。

☐	服务器IP/名称	实例ID/QUID	来源IP	来源地	协议	登录用户名	端口	首次攻击时间	最近攻击时间	尝试次数	破解
☐				浙江-宁波市	smb	未知	445	2022-01-26 07:48:42	2022-01-26 11:22:15	20	破解
☐			9	浙江-杭州市	ftp	未知	21	2022-01-25 10:55:35	2022-01-25 11:07:05	20	破解

字段说明：

服务器 IP/名称：当前被暴力破解的服务器。

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。

攻击时间：攻击者发起暴力破解时间。

尝试次数：攻击 IP 尝试暴力破解的次数统计。

破解状态：当前服务器被暴力破解成功或失败说明。

阻断状态：针对本次攻击的自动阻断成功或未阻断说明。

操作：

升级版本：当前服务器为升级为专业版主机安全，可单击**升级版本**进行升级。

加入白名单：当出现错误阻断时，可以单击**加入白名单**立即解除阻断。

删除记录：支持删除该事件，删除记录后将不再显示该记录。

开启告警通知

登录 [主机安全控制台](#)，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、微信及企业微信进行通知。

密码破解

☒ 全天 ☐ 09:00 ~ 18:00

登录密码

告警处理

1. 当用户接收密码破解事件告警时，登录 [主机安全控制台](#)，在左侧导航中，选择**入侵检测 > 密码破解**。

2. 在告警列表页面，查看告警事件列表中的对应攻击来源 IP。

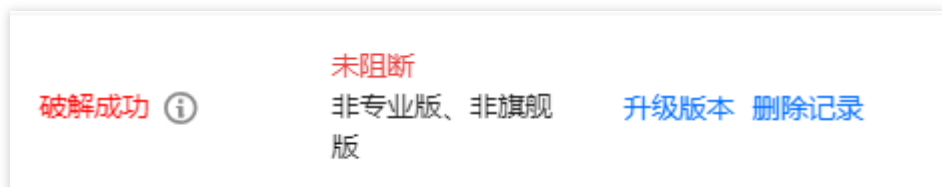
若确认是可信来源 IP，用户需在该事件右侧操作栏中，单击**处理 > 加入白名单**，设置加白名单条件和生效范围（**请用户谨慎添加白名单**）。配置成功后，预计5分钟内生效，后续来自该来源 IP 的密码破解行为将不再进行告警或者阻断。

☐	服务器IP/名称	来源IP	来源地	协议	登录用户名	端口	首次攻击时间	最近攻击时间	尝试次数	破解状
☐	1云			ssh	root			-24	13	破解成
☐	1V			ssh	root			-21	5	
☐	1V			smb	未知 ①			-20	110	
☐	1功			ftp	未知 ①			-20	845	
☐	1功			ftp	未知 ①			-18	823	
☐	1V			smb	未知 ①		14-03-03	14-03-04	8	

☐ 标记已
若您已
☒ 加入白
若您确
则，后
☐ 忽略
仅将本
☐ 删除记
删除该

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。

2.1.1 首先确认当前服务器的主机安全是否已升级为专业版或旗舰版，若未升级为专业版或旗舰版，建议用户在该事件右侧操作栏中，单击**升级版本**，升级为专业版或旗舰版主机安全。



2.1.2 在告警列表上方，开启自动阻断开关，**推荐选择标准阻断**模式，后续来自该攻击来源 IP 将会自动阻断，默认阻断时长15分钟，用户可根据需要自定义时长。

2.1.3 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：2024-08-13 16:29:50

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

- 登录 [主机安全控制台](#)，在左侧导航栏，选择**入侵检测** > **恶意请求**。
- 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。

标记已处理 忽略 删除记录 全部命中策略类型 全部状态 选择时间 选择时间 请选择资源属性后输入关键字搜索(仅									
☐	主机名称/实例ID	IP地址	命中策略类型	命中策略	恶意请求域名	请求次数	危害描述	最近请求时间	状态
☐	腾讯云主机	192.168.1.1	系统策略①	系统规则(标准)	恶意域名	2	发现主机/容器外连矿...	2023-10-25 12:25:57	待处理
☐	腾讯云主机	192.168.1.1	系统策略①	系统规则(标准)	恶意域名	143	发现主机外联Burp C...	2023-10-24 23:52:51	已处理
☐	腾讯云主机	192.168.1.1	系统策略①	系统规则(标准)	恶意域名	2	发现主机/容器外连矿...	2023-10-24 20:20:19	已处理
☐	腾讯云主机	192.168.1.1	用户自定义策略	自定义规则	恶意域名	2	发现主机存在访问恶...	2023-10-24 20:06:45	已拦截

筛选：支持按命中策略类型、状态、最近请求时间、状态及关键字进行筛选。

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：系统策略为腾讯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。

恶意请求详情

待处理

标记已处理

加入白名单

创建拦截策略

忽略

删除记录

风险主机

主机名称

实例 ID

公

内

客户端在线

首次请求时间

最近请求时间

2023-10-25 00:02:57

2023-10-25 14:26:23

恶意请求详情

恶意请求域名

polling.oastify.com

标签特征

--

进程

MD5

PID

命令行

请求次数

87

危害描述

告警描述

发现主机外联Burp Collaborator自带dnslog平台，如果不是您的主动行为，您的主机可能正在被burp渗透测试。Burp Suite 是用于web渗透测试的集成平台，oastify.com主要用于dns回显，漏洞验证。

修复建议

建议方案

1.检查恶意进程及非法端口，删除可疑的启动项和定时任务；
2.隔离或者删除相关的木马文件；
3.对系统进行风险排查，并进行安全加固，详情可参考如下链接：
【Linux】<https://cloud.tencent.com/document/product/296/9604>
【Windows】<https://cloud.tencent.com/document/product/296/9605>

参考链接

暂无

处理：标记已处理、加入白名单、创建拦截策略、忽略、删除记录。

标记已处理 推荐

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 NEW

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 NEW

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。

确认

取消

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。

创建策略

删除

全部策略类型

全部执行动作

全部生效状态

请选择资源属性后输入关键字搜索(仅

☐	策略名称	策略类型	黑/白名单	域名详情	生效主机	更新时间	执行动作	生效状态
☐	系统规则(重保)	系统策略①	黑名单	10.10.10.10	全部专业版、旗舰版主机	--	告警	☒
☐	系统规则(标准)	系统策略①	黑名单	10.10.10.10	全部专业版、旗舰版主机	--	告警	☒
☐	10.10.10.10	用户自定义策略	黑名单	10.10.10.10	1 台	2023-10-24 20:00:58	拦截	☒
☐	10.10.10.10	用户自定义策略	黑名单	10.10.10.10	全部旗舰版主机	2023-10-24 18:57:16	拦截	☒
☐	10.10.10.10	用户自定义策略	黑名单	10.10.10.10	全部旗舰版主机	2023-10-24 18:52:35	拦截	☒

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。

创建策略

告警、放行策略支持专业版、旗舰版机器；拦截策略仅支持旗舰版机器，可点击 [升级版本](#)

基本信息

策略名称 *

请输入策略名称，限制20个字符以内

策略描述

请输入策略描述，限制200个字符以内

启用状态 *

策略详情

黑/白名单 *

黑名单

白名单

执行动作 *

告警

拦截

放行

当主机尝试对策略范围内的域名进行外联时，将产生告警记录。

域名详情 *

请输入IP/域名/泛域名（如：www.12345.com、*.tencent.com等，暂不支持URL），多个内容以换行分隔

生效主机范围 (已选择111台)

选择主机

全部专业版和旗舰版主机（111）

自选主机

保存

取消

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。

系统自动拦截规则

恶意请求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黑域名和黑 IP，部分内容仍需您手动配置策略。

系统黑名单域名和 IP：主机安全运营专家与算法专家经过沉淀的域名和 IP 名单，此名单中的域名和 IP 可进行自动拦截。

拦截原理说明：恶意请求指的是终止对规则域名/IP的访问过程，它不会结束进程，而是会终止该访问请求。

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或 [联系我们](#)。

系统自动拦截规则仅限**旗舰版用户**使用。

1. 登录 [主机安全控制台](#)，在左侧导航栏选择**入侵检测 > 恶意请求**。

2. 在恶意请求页面，支持如下两种方式开启系统自动拦截规则。

在策略配置页面，单击系统自动拦截规则策略右侧的**生效状态开关**。



在告警列表页面，单击开启**恶意请求自动拦截开关**。



高危命令

最近更新时间：2024-08-13 16:29:50

本文档将为您介绍如何查看并操作高危命令告警列表。

背景信息

基于腾讯云安全技术及多维度多种手段，主机安全可对系统中的命令实时监控，若检测出高危命令，系统会向您提供实时告警通知。此外还可配置策略，对威胁命令进行危险程度的标记并执行相应动作。

前提条件

高危命令仅支持专业版、旗舰版主机，基础版和未防护主机须 [升级专业版或旗舰版](#) 才可使用该功能。

告警列表

1. 登录 [主机安全控制台](#)，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。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、命令内容、登录用户、PID、进程、数据来源、发生时间、处理时间、状态及操作共计14个字段，展示列表字段可进行自定义。

筛选：高危命令事件列表支持选择日期查看相应的告警信息，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，同时支持按命中策略类型、威胁等级、数据来源及状态筛选告警信息。

☐	主机名称/实例ID	IP地址	命中策略类型	命中策略	威胁等级	命令内容	数据来源	发生时间
☐	[模糊]	公网	用户自定义策略	test	中危	[模糊]	实时监控	2023
☐	[模糊]	公网	用户自定义策略	test	中危	[模糊]	实时监控	2023

自定义列表字段：在**高危命令告警列表**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。

自定义列表管理

×

i
请选择列表详细信息字段，最多勾选14个，已勾选13个

☐ 主机名称/实例ID
☒ IP地址
☒ 命中策略类型

☒ 命中策略
☐ 威胁等级
☒ 命令内容

☐ 登录用户
☒ PID
☒ 进程

☒ 数据来源
☒ 发生时间
☒ 处理时间

☐ 状态
☐ 操作

确认

取消

告警列表导出：在高危命令告警列表上方，单击

，可将列表信息导出。

详情 > 告警详情：单击详情，可查看高危命令告警详情页。

版权所有：腾讯云计算（北京）有限责任公司

第73 共145页

高危命令详情待处理

标记已处理

加入白名单

创建拦截策略

忽略

删除记录

告警详情

进程树

事件调查

风险主机

主机名称

实例 ID

公

内

客户端在线

发生时间

处理时间

2023-07-11 14:20:04

2023-07-11 14:20:04

命中策略

命中策略名称

详情

标签特征

威胁等级

-

高危

策略类型

用户自定义策略

数据来源

实时监控

登录用户

0:0

PID

2862

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，会执行恶意文件下载、连接矿池、添加公钥、查看敏感文件等操作。

修复建议

建议方案

1.检查恶意进程及非法端口，删除可疑的启动项和定时任务；
2.隔离或者删除相关的木马文件；
3.对系统进行风险排查，并进行安全加固，详情可参考如下链接：
【Linux】<https://cloud.tencent.com/document/product/296/9604>
【Windows】<https://cloud.tencent.com/document/product/296/9605>

参考链接

暂无

详情 > 进程树：在高危命令告警详情页，选择进程树标签页，可查看以时间倒序排列的三个进程详情。

高危命令详情

待处理

标记已处理

加入白名单

创建拦截策略

忽略

删除记录

告警详情

进程树

事件调查

进程树

最多仅展示3个进程树

ssh(3034)

进程所属用户:

进程所属用户组:

进程文件路径:

进程命令行:

进程启动时间:

bash(3033)

进程所属用户:

进程所属用户组:

进程文件路径:

进程命令行:

进程启动时间:

python2.7(2956)

进程所属用户:

进程所属用户组:

进程文件路径:

进程命令行:

进程启动时间:

详情 > 事件调查：在高危命令告警列表的右侧操作栏，单击**详情**选择**事件调查**标签页，可进入对应主机列表的**事件调查**。

说明

Windows 机器暂不支持事件调查功能。

仅旗舰版支持事件调查功能。

标记已处理：单击**处理** > **标记已处理**，若用户已手动处理了本次高危命令告警，可将该告警标记为已处理。

标记已处理 忽略 删除记录 全部命中策略类型 全部状态 选择时间 选择时间								
☐	主机名称/实例ID	IP地址	命中策略类型	命中策略	威胁等级	命令内容	数据来源	发生时间
☐	1	公 4 内 1	用户自定义策略	test	中危		实时监控	2023-1
☐	1	公 4 内 1	用户自定义策略	test	中危		实时监控	2023-1
☐	1	公 4 内 1	用户自定义策略	test	中危		实时监控	2023-1
☐	1	公 1 内 1	用户自定义策略	test	中危		实时监控	2023-1
☐	1	公 1 内 1	用户自定义策略	test	中危		实时监控	2023-1

加入白名单：单击**处理** > **加入白名单**，可对信任的命令加入白名单，后续该命令再被执行将不再产生告警或拦截。

创建策略

 告警、放行策略支持专业版、旗舰版机器；拦截策略仅支持旗舰版机器，可点击 [升级版本](#) 

基本信息

策略名称 *

策略描述

启用状态 * ☒

策略详情

黑/白名单 * ☐ 黑名单 ☒ 白名单

执行动作 *

当发现主机存在威胁命令时，将不再产生告警或拦截行为。

正则表达式 *

主机安全无法识别alias命令，请输入最终执行命令的正则表达式

生效主机范围 (已选择■台)

选择主机 ☒ 全部专业版和旗舰版主机  ☐ 自选主机

☒ 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

创建拦截策略：单击处理 > 创建拦截策略，可对威胁命令进行自动拦截，并产生拦截记录。

说明

拦截策略仅支持旗舰版主机，基础版、专业版主机须先 [升级旗舰版](#)。

忽略：支持单选或多选高危命令告警信息，仅将本次选中的告警进行忽略，若再有相同情况发生依然会进行告警。

删除记录：支持单选或多选高危命令告警信息，删除选中的告警记录。

标记已处理		忽略	删除记录	全部命中策略类型		全部状态		选择时间	选择时间
主机名称/实例ID	IP地址	命中策略类型	命中策略	威胁等级	命令内容	数据来源	发生时间		
☒	公内	用户自定义策略	test	中危		实时监控	202		
☒	公内	用户自定义策略	test	中危		实时监控	202		
☐	公内	用户自定义策略	test	中危		实时监控	202		

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。

基本信息

策略名称 *

请输入策略名称，限制20个字符以内

策略描述

请输入策略描述，限制200个字符以内

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，基础版、专业版主机请先 [升级旗舰版](#) 才可使用该功能。

策略详情

黑/白名单 *



黑名单



白名单

执行动作 *

告警

拦截

放行

当发现主机存在威胁命令时，将产生告警。

正则表达式 *

主机安全无法识别alias命令，请输入最终执行命令的正则表达式

威胁等级 *

高危

中危

低危

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和旗舰版主机，新增专业版/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。

策略详情

黑/白名单 *



黑名单



白名单

执行动作 *

告警

拦截

放行

当发现主机存在威胁命令时，将不再产生告警或拦截行为。

正则表达式 *

主机安全无法识别alias命令，请输入最终执行命令的正则表达式

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。

创建策略

删除

全部策略类型

全部执行动作

全部生效状态

☐	策略名称	策略类型	黑/白名单	正则表达式	威胁等级	生效主机	更新时间
☐		系统策略①	黑名单		无	全部专业版、旗舰版主机	2023-02-16 12:41:17
☐		系统策略①	黑名单		无	全部专业版、旗舰版主机	2023-01-09 09:57:30
☐		用户自定义策略	黑名单		中危	全部专业版、旗舰版主机	2023-07-19 10:53:42

共 3 项

字段说明：

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](#) 进行加白处理或 [联系我们](#)。

系统自动拦截规则仅限**旗舰版用户**使用。

- 登录 [主机安全控制台](#)，在左侧导航栏选择**入侵检测 > 高危命令**。
- 在**高危命令**页面，支持如下两种方式开启系统自动拦截规则。
在策略配置页面，单击系统自动拦截规则策略右侧的**生效状态开关**。

高危命令

告警列表策略配置

策略配置说明

策略配置说明

配置详情说明

创建策略删除全部策略类型全部执行动作全部生效状态

策略名称	策略类型	黑白名单	正则表达式	威胁等级	生效主机	更新时间	执行器
系统默认告警策略	系统策略	黑名单	腾讯云恶意命令库	无	全部旗舰版主机	2023-02-16 12:42:39	告
系统规则(重保)	系统策略	黑名单	腾讯云恶意命令库	无	全部旗舰版主机	2022-09-08 12:28:39	告
系统自动拦截规则	系统策略	黑名单	腾讯云恶意命令库	无	全部旗舰版主机	2024-06-19 17:35:35	拦截

在告警列表页面，单击开启**高危命令自动拦截**开关。

高危命令

告警列表策略配置

功能使用说明

功能操作指引

功能介绍

1 升级专业版/旗舰版

高危命令检测属于专业版/旗舰版功能。请先升级版本。
升级版本

2 开启自动拦截/配置自定义策略

建议您开启自动拦截功能，自动拦截系统高危命令，您也可以根据业务情况配置自定义策略（旗舰版机器功能）。
自动拦截应用中配置自定义策略

3

前往产生前往

高危命令自动拦截：开启 旗舰版专享 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。如发现误拦截情况，可 创建自定义策略 或 联系我们

版权所有：腾讯云计算（北京）有限责任公司

第82 共145页

本地提权

最近更新时间：2024-08-13 16:29:50

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。

前提条件

本地提权仅支持专业版、旗舰版主机，基础版和未防护主机须 [升级专业版或旗舰版](#) 才可使用该功能。

操作步骤

告警列表

1. 登录 [主机安全控制台](#)，在左侧导航栏选择**入侵检测** > **本地提权**，进入本地提权的**告警列表**标签页。
2. 在本地提权的**告警列表**标签页，可查看本地提权告警事件列表，并进行相关操作。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、操作（详情 | 处理）共8个字段，展示列表详情信息可进行自定义。

筛选/查询：本地提权告警列表支持选择日期查看相应的告警信息，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。

标记已处理		忽略	删除记录	选择时间		选择时间	状态:待处理
☐	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
☐		公 网	0	bash	1002	2023-07-04 16:35:08	全部状态
☐		公 网	0	bash	1002	2023-07-04 16:34:00	待处理
☐		公 网	0	bash	1002	2023-07-04 16:32:45	已加入白名单
☐		公 网	0	bash	1002	2023-07-04 16:31:45	已处理
☐		公 网	0	bash	1002	2023-07-04 16:31:29	已忽略
☐		公 网	0	bash	1002	2023-07-04 16:31:29	待处理
☐		公 网	0	bash	1002	2023-07-04 16:31:29	待处理

自定义设置列表字段：在本地提权告警列表上方，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。

自定义列表管理

请选择列表详细信息字段，最多勾选8个，已勾选8个

☒ 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☐ 操作

确认**取消**

事件导出：在本地提权告警列表上方，单击

，可将列表导出。

详情 > 告警详情：在本地提权告警列表的右侧操作栏，单击**详情**选择**告警详情**标签页，可查看告警详情。

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

事件调查NEW

风险主机

主机名称

实例 ID

公 - 内

客户端在线

发现时间

2023-07-04 16:35:08

提权主机

进程提权信息

进程名

标签特征

启动用户

文件权限

用户所属组

文件路径

新增权限

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，详情可参考如下链接：
【Linux】<https://cloud.tencent.com/document/product/296/9604>
【Windows】<https://cloud.tencent.com/document/product/296/9605>

参考链接

暂无

详情 > 进程树：在本地提权告警列表的右侧操作栏，单击详情选择进程树标签页，可查看以时间倒序排列的三个最新进程详情。

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

事件调查

NEW

进程树 ⓘ 最多仅展示3个进程树

find(22659)

进程所属用户:

进程所属用户组:

进程文件路径:

SSH服务:

登录源:

进程命令行:

进程启动时间:

bash(22622)

进程所属用户:

进程所属用户组:

进程文件路径:

SSH服务:

登录源:

进程命令行:

进程启动时间:

su(22621)

进程所属用户:

进程所属用户组:

进程文件路径:

SSH服务:

登录源:

进程命令行:

进程启动时间:

详情 > 事件调查：在本地提权告警列表的右侧操作栏，单击详情选择事件调查标签页，可进入对应主机列表的事件调查。

说明

Windows 机器暂不支持事件调查功能。

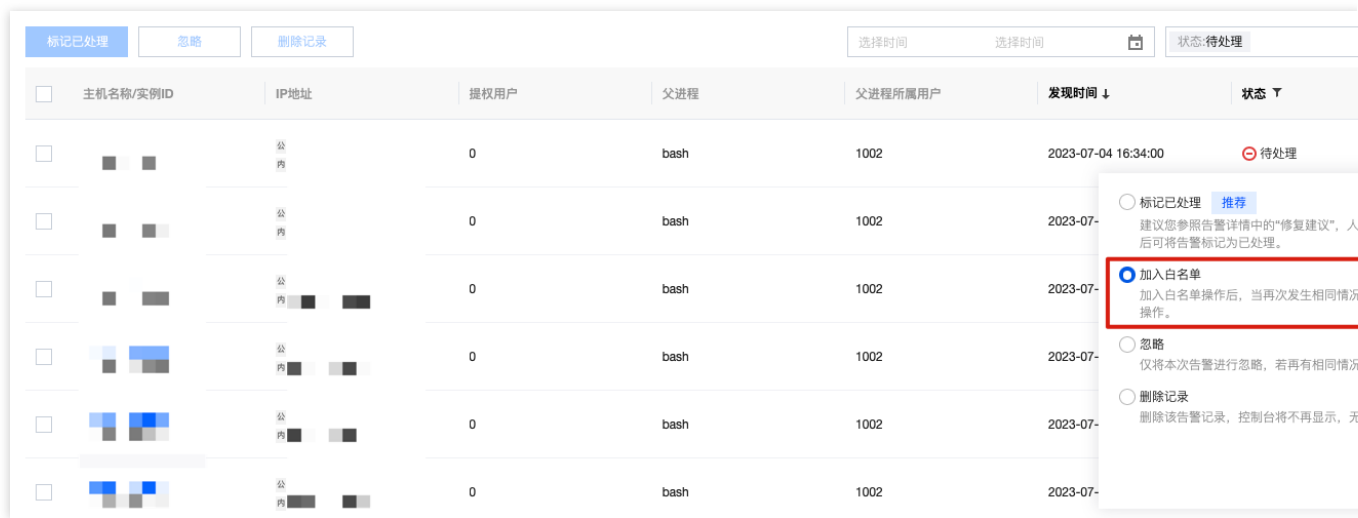
仅旗舰版支持事件调查功能。

标记已处理：支持单选或多选本地提权告警信息，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：

2.1.1 如需将本地提权告警事件加入白名单，可在告警信息列表的右侧操作栏，单击**处理** > **加入白名单**，或在详情页单击**加入白名单**。



2.1.2 在新增白名单页面，填写服务器范围后单击**确定**，即可将该本地提权告警加入白名单。

← 新增白名单

提权条件

☒ 带S权限的进程

☒ 提权进程：

备注：勾选两个条件时，需要同时满足才能命中白名单规则

服务器范围：

忽略：支持单选或多选本地提权告警信息，仅将本次选中的告警进行忽略，若再有相同情况发生依然会进行告警。

删除记录（慎重操作）：支持单选或多选本地提权告警信息，删除选中的告警记录，控制台将不再显示且无法恢复记录。

标记已处理 忽略 删除记录

选择时间 选择时间

状态:待处理

	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
☒		公网	0	bash	1002	2023-07-04 16:34:00	待处理
☒		公网	0	bash	1002	2023-07-	
☐		公网	0	bash	1002	2023-07-	
☒		公网	0	bash	1002	2023-07-	
☒		公网	0	bash	1002	2023-07-	
☒		公网	0	bash	1002	2023-07-	

☐ 标记已处理

☒ 加入白名单

☐ 忽略

☒ 删除记录

建议您参照告警详情中的“修

后可将告警标记为已处理。

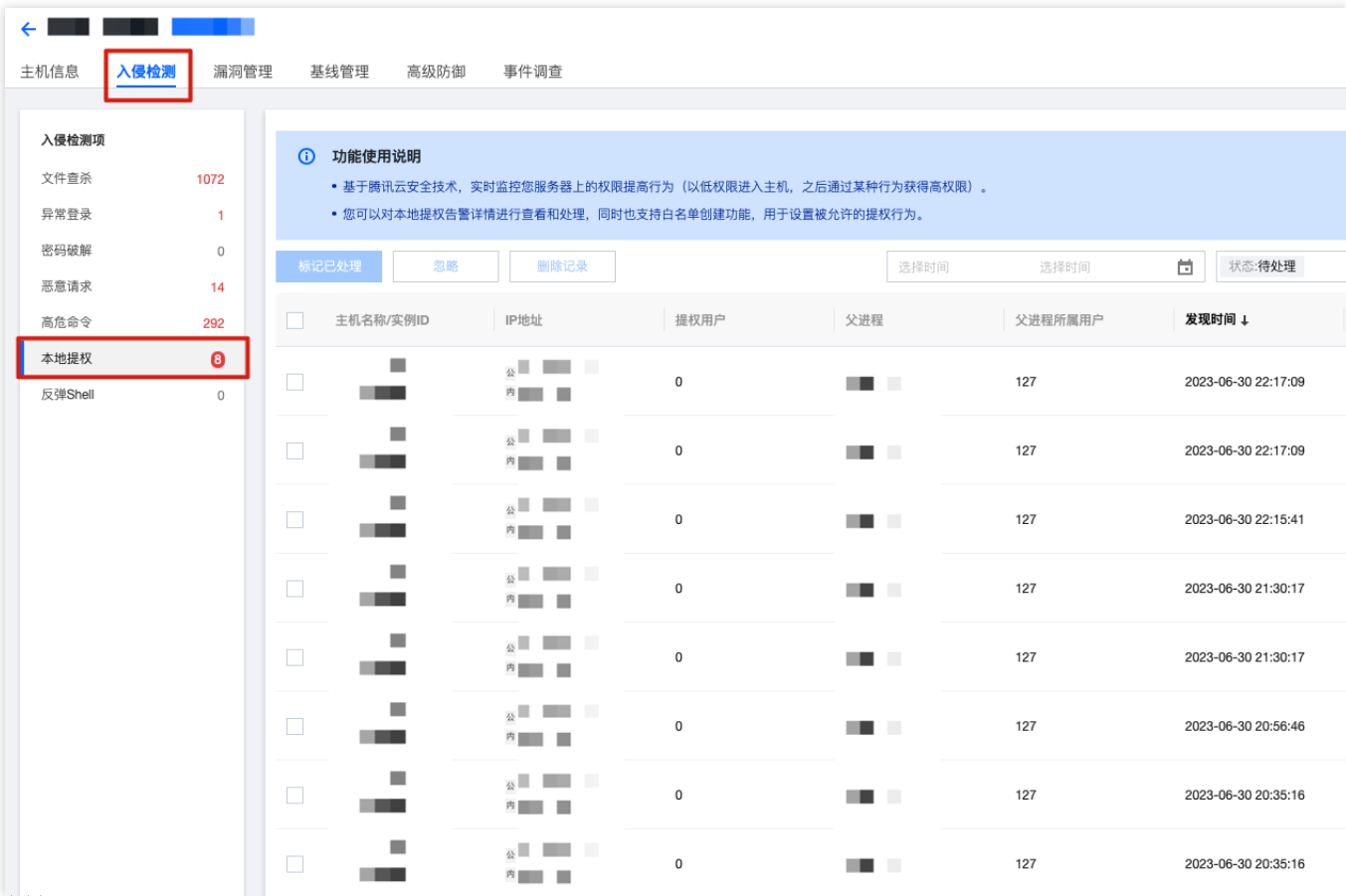
加入白名单操作后，当再次

操作。

仅将本次告警进行忽略，若

删除该告警记录，控制台将

3. 单击本地提权告警的主机名称/实例ID，可查看该主机列表入侵检测标签页详情。



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 [主机安全控制台](#)，在左侧导航栏，选择入侵检测 > 本地提权。
- Log in to the [Host Security Console](#), and in the left navigation bar, select **Intrusion Detection > Local Privilege Escalation**.
2. 在本地提权页面，单击白名单管理 > 添加白名单。



3. 在新增白名单页面，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。

新增白名单

提权条件

☐ 带S权限的进程

☐ 提权进程：

支持多个进程名，以英文逗号分隔

备注：勾选两个条件时，需要同时满足才能命中白名单规则

服务器范围：

☐ 全部服务器（用户APPID下所有服务器）

☒ 自定义服务器范围 [选择服务器](#)

4. 设置完成后，可在白名单管理列表查看该条件，且在事件列表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：已配置的黑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。

删除	添加白名单	请选择资源属性			
☐	服务器	提权进程	是否带S权限 ▾	创建时间	更新时间
☐			是	2023-07-11 19:20:20	2023-07-11 19:20:20
☐			否	2023-03-20 17:07:08	2023-06-26 15:07:08
共 2 项					

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。

自定义列表管理

请选择列表详细信息字段，最多勾选6个，已勾选6个

☒ 服务器

☒ 提权进程

☒ 是否带S权限

☒ 创建时间

☒ 更新时间

☐ 操作

确认

取消

编辑：在目标白名单的右侧操作栏，单击**编辑**，可对已创建在白名单进行编辑。

删除：在白名单列表中，支持单选或多选已配置在白名单进行删除。

删除

添加白名单

请选择资源属性后输入关键字进行过滤

☒	服务器	提权进程	是否带S权限	创建时间	更新时间
☒			否	2023-0	11
☒			否	2023-0	39

已选 2 项共 2 项

10 条 / 页

反弹 Shell

最近更新时间：2024-08-13 16:29:50

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 功能是基于腾讯云安全技术及多维度多手段，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。

前提条件

反弹 Shell 功能仅专业版主机与旗舰版主机支持，基础版主机须 [升级专业版或旗舰版](#) 才可使用该功能。

告警列表

- 1. 登录 [主机安全控制台](#)，在左侧导航栏，选择[入侵检测](#) > [反弹 Shell](#)，进入反弹 Shell 的告警列表页面。
- 2. 在告警列表页面，可查看反弹 Shell 告警事件，并进行相关操作。

标记已处理

忽略

删除记录

选择时间

选择时间

☐	主机名称/实例ID	IP地址	连接进程	执行命令	威胁等级	父进程	目标主机	目标端口
☐	腾讯云主机名称	IP地址	sh	反弹 Shell 命令	高危	bash	目标主机	3389
☐	腾讯云主机名称	IP地址	bash	反弹 Shell 命令	高危	bash	目标主机	3389
☐	腾讯云主机名称	IP地址	sh	反弹 Shell 命令	高危	bash	目标主机	3389

筛选：支持按发现时间、状态及关键字进行筛选。

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：被攻击者反弹 Shell 控制的主机名称/实例ID。

IP 地址：被攻击者反弹 Shell 控制的主机IP。

连接进程：主机进行反弹 Shell 连接的进程。

执行命令：主机执行的反弹 Shell 连接的命令。

威胁等级：高危(目标主机 IP是公网 IP)、中危（目标主机 IP 是局域网 IP）。

父进程：连接进程的父进程。

目标主机：反弹 Shell 连接的目标主机。

目标端口：反弹 Shell 连接的目标端口。

发现时间：检测到反弹 Shell 行为的时间。

检测方法：

行为分析：通过监视系统和网络活动方式来检测潜在的威胁或异常行为。

命令特征检测：通过对命令分析（如：高权限命令、非常规命令、异常参数等）以识别和监测可能与反弹Shell相关的命令行为。

状态：待处理、已加入白名单、已处理、已忽略。

详情：可查看反弹Shell的详细情况，含风险主机信息、连接进程信息、危险描述、修复建议。

反弹Shell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

事件调查

NEW

风险主机

主机名称

实例 ID

公

内

客户端在线

发现时间

2023-06-06 22:01:50

目标主机

106.55.235.95

连接进程信息

进程名

sh

标签特征

-

启动用户

文件路径

用户所属组

执行命令

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，会让受害主机创建一个交互式shell并连接黑客的远程控制服务器，黑客通过建立的通道，可以向受害主机发送指令并获得执行结果。

修复建议

建议方案

1、检查系统是否存在异常的网络连接；
2、隔离或者删除相关的木马文件；
3、对系统进行风险排查，并进行安全加固，详情可参考如下链接：
【Linux】<https://cloud.tencent.com/document/product/296/9604>
【Windows】<https://cloud.tencent.com/document/product/296/9605>

参考链接

暂无

处理：标记已处理、加入白名单、忽略、删除记录。

☒ 标记已处理

推荐

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。

确认

取消

3. 反弹 Shell 内网告警展示。

3.1 由于内网反弹 Shell 告警数量较大，针对内网反弹 Shell 的检测引擎默认处于关闭状态。如需开启，请单击页面右上角的**反弹 Shell 设置**进行配置。

3.2 在反弹 Shell 设置页面，您可以自定义是否开启内网反弹 Shell 检测。开启后，系统将支持检测并上报告警数据；关闭后，将停止检测。

反弹Shell设置

检测范围

内网告警检测

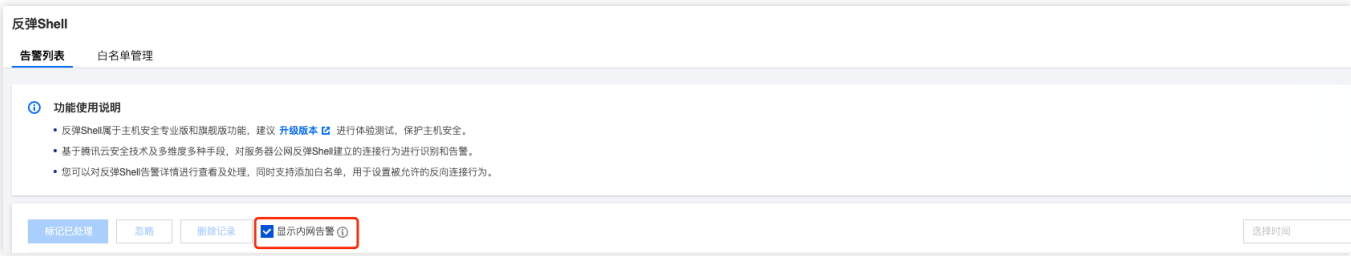


开启后，后台将检测内网反弹Shell告警，此类告警量较大，建议谨慎开启。



显示内网告警：在告警列表中显示已检出的内网反弹Shell告警。

3.3 同时，支持可以在反弹 Shell 配置页面抽屉或告警列表上方设置是否显示内网告警数据。勾选后，告警列表将展示内网告警数据；取消勾选，则不展示内网告警数据。



白名单管理

在反弹 Shell 页面上方选择白名单管理，进入白名单管理页面。

删除 添加白名单					
☐	服务器	连接进程	目标主机	目标端口	创建时间
☐		全部进程		8080	2023-10-26 09:52:00
☐		全部进程		8080	2023-10-26 09:52:00
☐		全部进程		8080	2023-10-25 18:09:29

筛选：支持按连接进程进行筛选。

自定义展示列：单击



，可设置策略列表展示字段。

字段说明：

服务器：生效白名单的服务器。

连接进程：加入白名单的连接进程。

目标主机：反弹 Shell 的目标主机。

目标端口：反弹 Shell 的目标端口。

创建时间：该白名单创建时间。

更新时间：该白名单更新时间。

编辑：对该白名单进行编辑。

删除：删除该白名单。

添加白名单：

新增白名单

反弹Shell条件

满足条件:

☐

目标主机:

IP

端口

☐

连接进程:

支持多个进程名，以英文逗号分隔

备注:

IP 格式：单个IP（1.1.1.1）、单个IP范围（1.1.1.1-1.1.1.10）、单个IP段（172.168.34.1/20）

端口格式：80,8080(支持多个, 不限端口请留空, 若端口留空请填写进程名)

服务器范围:

☐

全部服务器（用户APPID下所有服务器）

☒

自定义服务器范围

[选择服务器](#)

注意：

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 下所有服务器添加该白名单，请谨慎操作。

Java 内存马

最近更新时间：2024-08-13 16:29:50

本文档将为您介绍如何使用 Java 内存马功能。

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，结合腾讯云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。

前提条件

Java 内存马属于主机安全旗舰版功能，须 [升级旗舰版](#) 才可使用该功能。

操作步骤

1. 登录 [主机安全控制台](#)，在左侧导航栏，选择**高级防御** > **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，结合腾讯云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。

启用插件 关闭插件				
☐	服务器IP/名称	Java内存马插件	插件状态 ▾	首次开启时间
☐			全部正常	2022-05-26 17:35:23
☐			未开启	2022-05-27 11:17:17
☐			未开启	2022-05-27 11:17:17

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）、错误日志。

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

标记已处理		忽略	删除	删除全部记录	选择首次发现时间	
☐	服务器IP/名称	Java内存马类型 ▾	说明		首次发现时间	最近检测时间
☐		Servlet型	检测到java进程 2462317/org.apache.catalina.startup.Bootstrap start 中加载的 org.apache.jsp.bebinder_005fshell...		2022-05-26 19:08:25	2022-05-2
☐		Servlet型	检测到java进程 2462317/org.apache.catalina.startup.Bootstrap start 中加载的 webshell_servlet 类中存在木马		2022-05-26 19:08:25	2022-05-2
☐		Servlet型	检测到java进程 2308007/org.apache.catalina.startup.Bootstrap start 中加载的 org.apache.jsp.test95273_jsp 类中存在...		2022-05-24 20:42:55	2022-05-2

字段说明：

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。

Java内存马详情



类名

样本详情

[查看文件](#)

所属类加载器

类文件大小

5.73 KB

类文件MD5

父类名

继承的接口

注释

进程PID

进程命令行

进程路径

危害描述

事件描述

检测到Java服务进程中存在Java内存木马。Java内存马能长期驻留在内存中, 接收攻击者输入, 从而达到长期服务器的目的。

修复建议

建议方案

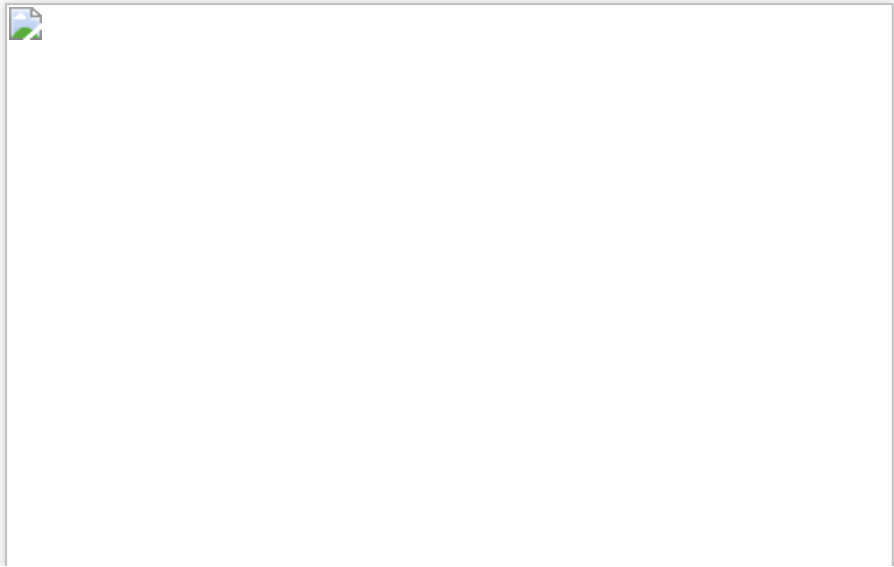
检查Java服务访问日志,评估内存马是否被访问; 检查主机高危漏洞,修复高危漏洞并重启java服务。

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。

反编译Java文件

```
1. /*
2.  * Decompiled with CFR 0.152.
3.  *
4.  * Could not load the following classes:
5.  * javax.el.ExpressionFactory
6.  * javax.servlet.Servlet
7.  * javax.servlet.ServletConfig
```

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

监控规则配置

最近更新时间：2024-08-13 16:29:50

核心文件监控的监控规则分为系统规则和自定义规则。系统规则为腾讯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，建议 [升级旗舰版](#)，保护主机安全。

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。

新增规则

1. 登录 [主机安全控制台](#)，在左侧导航栏，选择高级防御 > 核心文件监控 > 监控规则配置。
2. 在监控规则配置页面，单击左上角处的新增规则。
3. 在新增规则页面，依次配置基础设置、规则内容设置和生效服务器范围参数。

基础信息

基础信息

* 规则名称

请输入规则名称

* 威胁等级

高危

中危

低危

无

* 启用状态

参数说明：

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。

版权所有：腾讯云计算（北京）有限责任公司

第102 共145页

规则内容设置



支持对您的核心文件进行读取/修改监控，产生对应告警：

建议默认勾选修改文件，若勾选读取文件监控，告警量预计会偏大，系统资源占用也会偏高，请您根据实际需求开启

【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/*

顺序	监控行为	进程路径	文件路径
1	☒ 修改文件 ☐ 读取文件	请输入进程路径	请输入文件路径
2	☒ 修改文件 ☐ 读取文件	请输入进程路径	请输入文件路径

添加规则

参数说明：

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](#) 页面，选择所需规则，单击操作列的**编辑**。

☐	规则名称	规则类型	规则威胁等级	生效服务器	创建时间	最近编辑时间
☐		自定义规则	高危	全部服务器	2021-12-15 16:06:40	2021-12-15 16:0
☐		自定义规则	高危	1	2021-11-17 00:21:45	2021-11-25 10:0
☐		自定义规则	高危	1	2021-11-05 11:23:59	2021-11-05 11:2

2. 在编辑规则页面，修改相关参数，单击**保存**即可。

复制规则

1. 在 [核心文件监控](#) > [监控规则配置](#) 页面，选择所需规则，单击操作列的**复制**。

☐	规则名称	规则类型	规则威胁等级	生效服务器	创建时间	最近编辑时间
☐		自定义规则	高危	全部服务器	2021-12-15 16:06:40	2021-12-15 16:0
☐		自定义规则	高危	1	2021-11-17 00:21:45	2021-11-25 10:0
☐		自定义规则	高危	1	2021-11-05 11:23:59	2021-11-05 11:2

2. 在复制规则页面，修改相关参数，单击**保存**即可。

删除规则

1. 在 [核心文件监控](#) > [监控规则配置](#) 页面，支持删除单个规则或批量删除规则，具体操作如下。

单个：选择单个规则，单击操作列的**删除**，弹出“**确认删除**”弹窗。

☐	规则名称	规则类型	规则威胁等级	生效服务器	创建时间	最近编辑时间
☐		自定义规则	高危	全部服务器	2021-12-15 16:06:40	2021-12-15 16:06
☐		自定义规则	高危	1	2021-11-17 00:21:45	2021-11-25 10:03
☐		自定义规则	高危	1	2021-11-05 11:23:59	2021-11-05 11:23

批量：选择所需规则，单击**删除**，弹出“**确认删除**”弹窗。

新增规则

开启

关闭

删除

自定义规则

☐	规则名称	规则类型	威胁等级	规则内容	生效主机	创建时间	最近编辑时间
☒		自定义规则	低危			2023-08-01 19:16:41	2023-08-18
☒		自定义规则	高危			2023-07-20 14:50:00	2023-08-01
☐		自定义规则	高危		各服务器	2023-06-07 16:08:31	2023-07-19

2. 在“**确认删除**”弹窗中，单击**确认**，即可完成删除规则。

注意：

删除后，规则将无法恢复，请谨慎操作。

告警列表

最近更新时间：2024-08-13 16:29:50

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。

说明：

核心文件监控属于主机安全旗舰版功能，建议 [升级旗舰版](#)，保护主机安全。

核心文件监控目前暂只支持 Linux 内核版本为3.10以上的操作系统。

处理告警记录

1. 登录 [主机安全控制台](#)，在左侧导航栏，选择高级防御 > 核心文件监控 > 告警列表。
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。

标记已处理 忽略 删除			全部处理状态		选择时间		选择时间			
☐	主机名称/实例ID	IP地址	规则类别	命中规则名称	威胁等级	威胁行为	告警描述	发生时间	最	↓
☐	公内	公内	系统规则	系统策略-篡改计划任务 ①	高危	修改文件	检测到系统计...	2023-08-17 17:24:00	20	17
☐	公内	公内	系统规则	系统策略-篡改用户配置 ①	高危	修改文件	检测到用户配...	2023-08-17 17:08:03	20	17
☐	公内	公内	系统规则	系统策略-篡改用户配置 ①	高危	修改文件	检测到用户配...	2023-08-16 16:10:30	20	16
☐	公内	公内	系统规则	系统策略-篡改计划任务 ①	高危	修改文件	检测到系统计...	2023-08-11 14:53:52	20	14
☐	公内	公内	系统规则	系统策略-篡改用户配置 ①	高危	修改文件	检测到用户配...	2023-08-09 15:06:09	20	15
☐	公内	公内	系统规则	系统策略-篡改计划任务 ①	高危	修改文件	检测到系统计...	2023-08-01 00:57:30	20	18

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。

3. 在“二次确认”对话框中，单击确认，即可对告警记录进行处理。
4. 告警列表也支持批量处理告警记录，选中一个或多个告警记录后，单击左上角的标记已处理或忽略，经过二次确认后，即可对选择的告警记录进行处理。

标记已处理

忽略

删除

全部处理状态

选择时间

选择时间

	主机名称/实例ID	IP地址	规则类别	命中规则名称	威胁等级	威胁行为	告警描述	发生时间	最新
		公内	系统规则	系统策略-篡改计划任务	高危	修改文件	检测到系统计...	2023-08-17 17:24:00	2017
		公内	系统规则	系统策略-篡改用户配置	高危	修改文件	检测到用户配...	2023-08-17 17:08:03	2017

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，单击处理 > **删除记录**，弹出确认删除对话框。

标记已处理		忽略	删除	全部处理状态		选择时间		选择时间		📅
☐	主机名称/实例ID	IP地址	规则类别	命中规则名称	威胁等级	威胁行为	告警描述	发生时间	最近	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改用户配置 ①	高危	🔗 修改文件	检测到用户配...	2023-08-17 17:08:03	2023-08-17 08:03	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改用户配置 ①	高危	🔗 修改文件	检测到用户配...	2023-08-16 16:10:30	2023-08-16 10:30	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改计划任务 ①	高危	🔗 修改文件	检测到系统计...	2023-08-11 14:53:52	2023-08-11 4:53	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改用户配置 ①	高危	🔗 修改文件	检测到用户配...	2023-08-09 15:06:09	2023-08-09 15:06	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改计划任务 ①	高危	🔗 修改文件	检测到系统计...	2023-08-01 00:57:30	2023-08-01 00:57	
☐	主机名称/实例ID	公网IP地址	系统规则	系统策略-篡改用户配置 ①	高危	🔗 修改文件	检测到用户配...	2023-08-01 17:41:57	2023-08-01 17:41	

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**确认**，即可删除所选告警记录。

说明：

删除选中告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

网络攻击

最近更新时间：2024-08-13 16:29:50

网络攻击基于腾讯云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

- 登录 [主机安全控制台](#)，在左侧导航栏，选择**高级防御** > **网络攻击**。
- 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、模板端口等信息。

标记已处理 忽略 删除记录 全部攻击状态 选择时间 选择时间 请选择资源属性后输入关键词							
☐ 主机名称/实例ID	IP地址	目标端口	攻击来源IP/地址	漏洞名称 ⓘ	攻击状态	最近攻击时间 ↓	攻击
☐ te ir	公 1 内 1	8080	IP 4 5	Apache log4j2 远程代码执行... • 支持漏洞防御(未开启)	尝试攻击	2023-12-30 09:11:45	
☐ te ir	公 1 内 1	8080	IP 4 5	Apache log4j2 远程代码执行... • 支持漏洞防御(未开启)	尝试攻击	2023-12-30 09:05:07	
☐ d ir	公 1 内 1	80	IP 4 5	Apache log4j2 远程代码执行... • 支持漏洞防御(已开启)	尝试攻击	2023-12-29 16:03:38	

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。

网络攻击详情待处理

标记已处理

开启漏洞防御

加入白名单

忽略

删除记录

告警详情

进程树

事件调查

主机名/IP [详情](#)

客户端在线

内 外

最近攻击时间

2023-12-30 09:11:45

攻击次数

1

目标端口

8080

告警详情

攻击状态

尝试攻击

攻击源IP

6

攻击源地址

漏洞名称

[Apache log4j2 远程代码执行漏洞 \(CVE-2021-44228\)](#)

漏洞CVE编号

CVE-2021-44228

漏洞全网攻击热度

支持漏洞防御(未开启)

服务进程

node /root/tcs/tcs-installer/frontend/frontend-platform/server.js

攻击数据包

危害描述

告警描述

告警说明该端上已经有发现恶意网络攻击流量，请注意相关防护，否则可能会存在被入侵风险。
该告警是在主机侧感知到来自外部的使用热门漏洞攻击的请求，若非自行扫描则通常代表该主机网络服务对外暴露，且正在被攻击/探测。

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 [网络攻击页面](#)，选择所需告警，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。

标记已处理

忽略

删除记录

全部攻击状态

选择时间

选择时间

请选择资源属性后

☐ 主机名称/实例ID	IP地址	目标端口	攻击来源IP/地址	漏洞名称	攻击状态	最近攻击时间
☐	公网IP	8080	攻击来源IP	Apache log4j2 远程代码执行... 支持漏洞防御(未开启)	尝试攻击	2023-12-30 09:11:45
☐	公网IP	8080	攻击来源IP	Apache log4j2 远程代码执行... 支持漏洞防御(未开启)	尝试攻击	2023-12-30 09:05:07
☐	公网IP	80	攻击来源IP	Apache log4j2 远程代码执行... 支持漏洞防御(已开启)	尝试攻击	2023-12-29 16:03:38

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”。

开启漏洞防御：操作后处理状态自动变为“已处理”，支持勾选将该漏洞防御覆盖到的主机相关的待处理告警均标记为“已处理”。

加入白名单：可将攻击来源 IP 进行加白，可编辑生效主机范围；处理后状态自动变为“已加白”，支持对历史告警批量加白。

创建白名单

添加白名单后，当对应来源IP对生效范围内的主机产生网络攻击时，将不产生告警，请谨慎操作。

基本信息

来源IP

115

单个IP示例：1.1.1.1、IP范围示例：1.1.1.1-1.1.1.10、IP段示例：172.168.34.1/20，多个用英文“;”分隔

备注

请输入备注信息

告警处理

☒ 批量加白所有符合该白名单条件的告警

生效主机范围 (已选择1台)

选择主机

☐ 全部专业版和旗舰版主机 (79)

☒ 自选主机

自选方式

直接勾选

选择区域

全部服务器

全地域

服务器标签

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

选择主机

选择全部

已选择 1 台主机

请输入主机名称/实例ID/IP地址进行搜索

主机名称/实例ID	IP地址	防护版本
☐		旗舰版

请输入主机名称/实例ID/IP地址进行搜索

主机名称/实例ID	IP地址	防护版本
☒		基础版

保存

取消

忽略：选择该项后，处理状态由“待处理”变为“已忽略”，后续有相同攻击仍会告警。
删除记录：将当前告警记录删除，无法恢复。

勒索防御

最近更新时间：2024-08-13 16:29:50

勒索病毒是一种恶意软件,它会加密用户的重要文件,并要求用户支付赎金以解密文件。勒索防御通过诱饵文件+定期备份功能,可有效监控勒索病毒的入侵攻击,保护用户的重要数据免受勒索,遭受勒索后也可及时恢复备份。

说明：

该功能灰度中,如有防勒索需求,请 [联系我们](#) 开白使用。

限制说明

仅支持专业版或旗舰版的腾讯云服务器 (Linux 只支持内核版本为3.10以上的操作系统)。

1台主机仅可绑定1条勒索防御策略。

计费说明

主机安全防护版本：使用勒索防御功能,主机须先绑定专业版授权或旗舰版授权,可在 [主机安全购买页](#) 中购买和绑定。

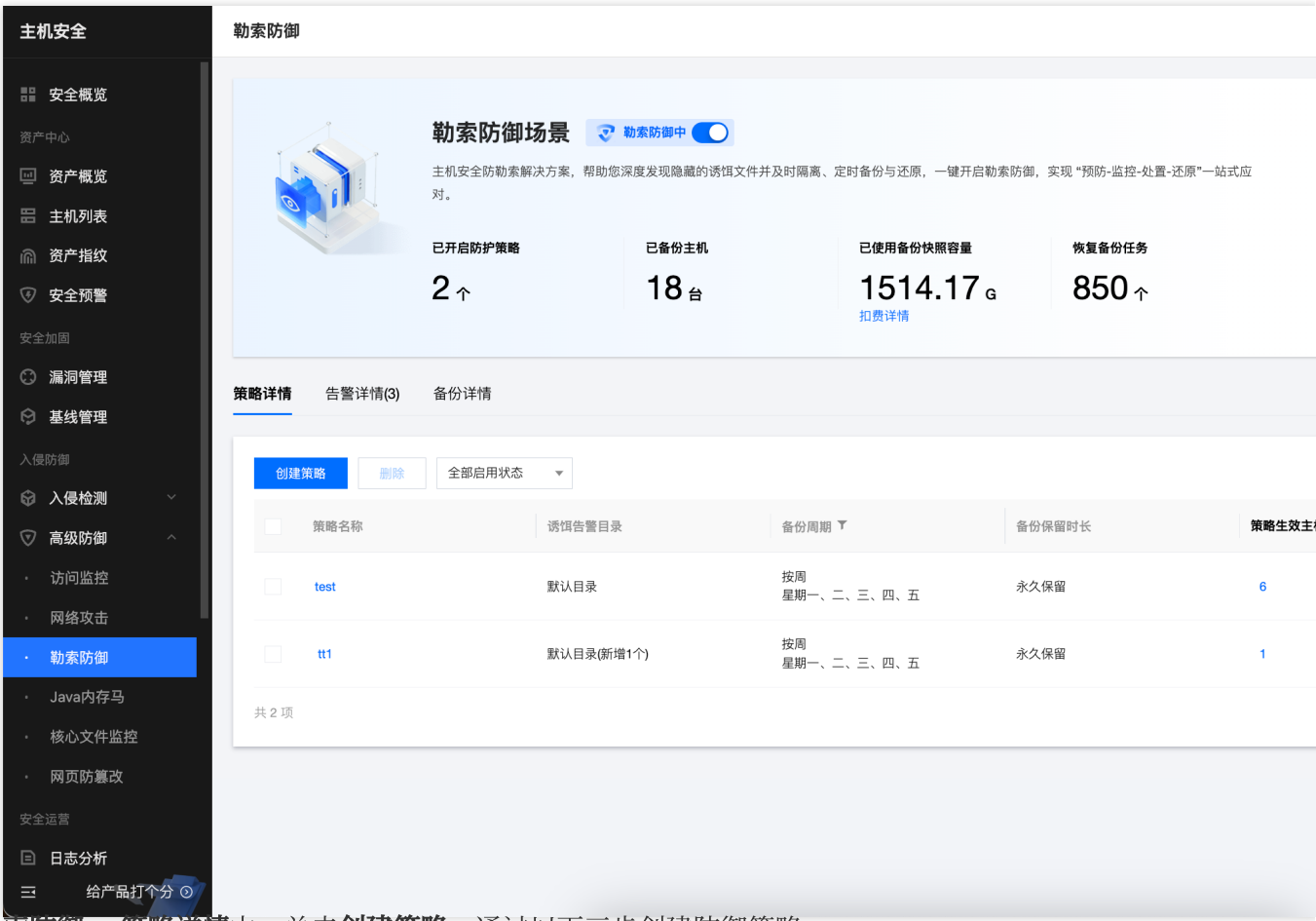
快照：备份将以腾讯云快照方式执行,采用后付费方式扣费,每小时进行一次结算,详情可查看 [价格总览](#)。

防御原理

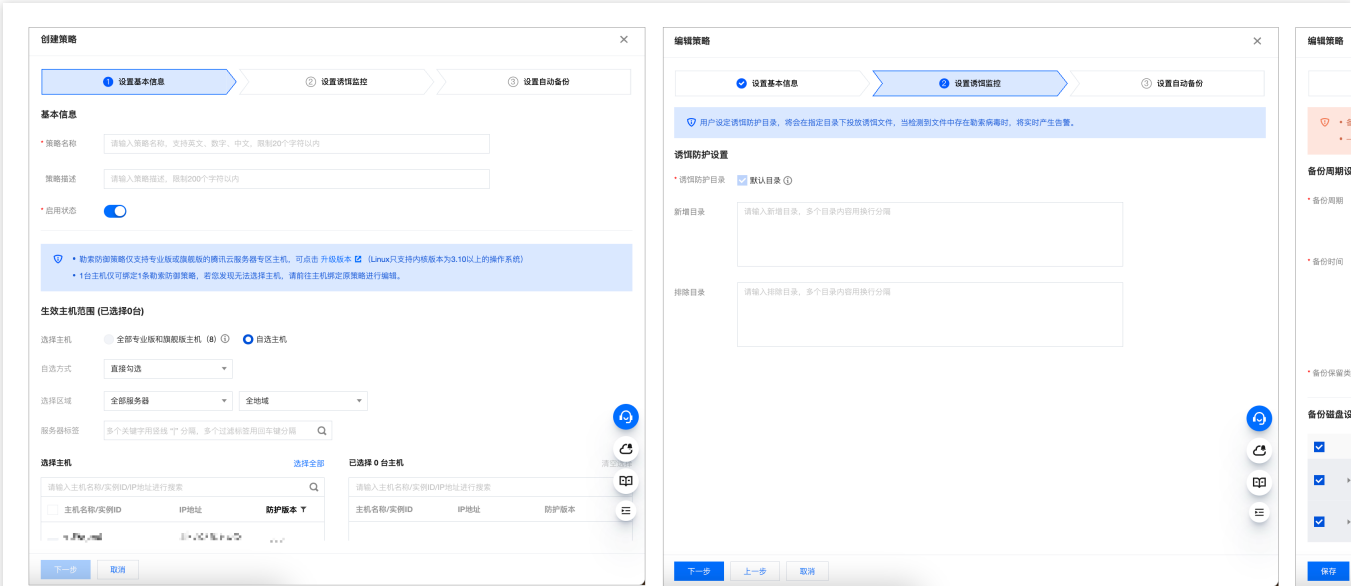
1. 监控诱饵文件：在特定目录下释放诱饵文件,定时检测诱饵文件名、HASH 值等信息释放被篡改加密,若发现异常,实时告警用户。
2. 监控非诱饵文件：基于文件检测、进程检测识别是否存在修改、删除、加密等行为,若发现异常,实时告警用户。
3. 定期快照备份：提供一键快照功能,支持用户配置定时快照,为数据被加密后的恢复兜底。

操作步骤

1. 登录 [主机安全控制台](#),在左侧导航栏中选择**高级防御** > **勒索防御**。



2.在勒索防御 > 策略详情中，单击创建策略，通过以下三步创建防御策略。



说明：

诱饵文件默认目录：

Windows 操作系统：C:\\ProgramData。

Linux操作系统：YunJing。

3.创建好策略后，可查看当前策略、告警、防御率的统计情况，支持一键停用所有勒索防御策略。

勒索防御

勒索防御场景

勒索防御中

主机安全防勒索解决方案，帮助您深度发现隐藏的诱饵文件并及时隔离、定时备份与还原，一键开启勒索防御，实现“预防-监控-处置-还原”一站式应对。

已开启防护策略

2个

已备份主机

18台

已使用备份快照容量

1514.17G

[扣费详情](#)

恢复备份任务

850个

勒索防御功能仅针对腾讯云和旗舰版主机

勒索防

查看详情：单击详情可查看告警详情、危害描述、解决方案及进程树信息。

版权所有：腾讯云计算（北京）有限责任公司

第115 共145页

勒索病毒详情待处理

恢复备份

标记已处理

信任

删除记录

告警详情

进程树

事件调查

主机名/IP [详情](#)

客户端在线

首次发现时间 2024-01-05 10:52:59

最近检测时间 2024-01-05 10:52:59

内

外

告警详情

告警关联策略

被篡改文件名

诱饵路径

恶意进程文件大小

恶意进程文件MD5

恶意进程ID

恶意进程路径

运行命令行参数

恶意行为

恶意进程启动时间

加密勒索

2024-01-05 10:52:54

危害描述

告警描述

发现主机上存勒索病毒，您的主机可能有被勒索风险。
勒索病毒通常会执行挖矿、文件删除、信息窃取和网络攻击等恶意行为。通过窃取您的数据来获取高昂赎金。

解决方案

1. 确认告警

总体上，勒索病毒是根据文件行为威胁程度进行打分的，这个文件本身具有一定的危险特征，但并不完全保证一定是一个网站后门，也可能是一些包含可疑代码的正常网站文件。建议您[登录服务器](#)进行文件及恶意代码内容核实。如果是自己部署放置的，可以选择忽略。

处理：在告警详情中，单击处理，支持对主机进行如下操作。

恢复备份：若主机已被勒索攻击，单击后可选择备份列表中的快照进行恢复。

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。

信任：信任操作后，仅对当前主机上该文件（MD5）或进程进行加白信任，同时将对对应的所有告警进行信任处理，后续不再告警，请谨慎操作。

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。

5.在备份详情中，可查看各主机备份的情况，含关联策略、已备份数、近一次备份状态及时间，可查看备份详细记录，可选择其中一个快照恢复备份。

版权所有：腾讯云计算（北京）有限责任公司

第116 共145页

策略详情 告警详情(3) 备份详情

选择时间 选择时间 

主机名称/实例ID	IP地址	主机标签	当前关联策略	已备份数 	近一次备份状态 
腾讯云主机实例	内 IP: 192.168.1.1 外 IP: 192.168.1.1	 标签(1)	 启用中	76次	 备份成功
腾讯云主机实例	内 IP: 192.168.1.1 外 IP: 192.168.1.1	 多个(2)	 启用中	64次	 备份成功
腾讯云主机实例	内 IP: 192.168.1.1 外 IP: 192.168.1.1	 多个(2)	 启用中	51次	 备份成功
腾讯云主机实例	内 IP: 192.168.1.1 外 IP: 192.168.1.1	 多个(2)	 启用中	11次	 备份成功
腾讯云主机实例	内 IP: 192.168.1.1 外 IP: 192.168.1.1	 多个(2)	 启用中	14次	 备份成功

日志分析

最近更新时间：2024-08-13 16:29:50

日志分析是主机安全防护解决方案的重要组成，提供主机相关安全事件日志，支持 SQL 检索与查询，并提供可视化报表与统计，帮助用户快速排查入侵、溯源定位等安全运营工作。本文档将为您介绍如何使用日志分析功能。

限制说明

可收集日志数据，受主机防护版本限制如下。

日志大类	日志类型	日志描述	支持版本
主机资产日志	主机信息	包含主机实例 ID、IP、操作系统、地域、VPC、实例状态、是否安装主机安全客户端等主机信息。 说明： 仅主机的“同步时间”变更，其余信息不变，不会产生日志流水。	全部主机
	资产指纹	包含资源监控、账号、端口、软件应用、进程、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、系统安装包。 说明： 仅资产指纹的“数据更新时间”变更，其余信息不变，不会产生日志流水。	专业版、旗舰版
客户端上报日志	客户端上报	主机原始日志（包含如：系统认证和授权信息、系统安全信息、系统消息、系统审计信息等内容）；DNS 日志、进程快照日志、网络五元组日志、文件监控日志、登录流水日志。	基础版及以上
告警日志	入侵检测	文件查杀（恶意文件）、文件查杀（异常进程）、异常登录、密码破解、恶意请求、高危命令、本地提权、反弹 Shell。	专业版、旗舰版
	漏洞管理	应急漏洞、Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。	专业版、旗舰版
	基线管理	安全基线。	专业版、旗舰版
	高级防御	核心文件监控、Java 内存马、网络攻击	旗舰版
	客户端相关	客户端离线、客户端卸载。	基础版及以上

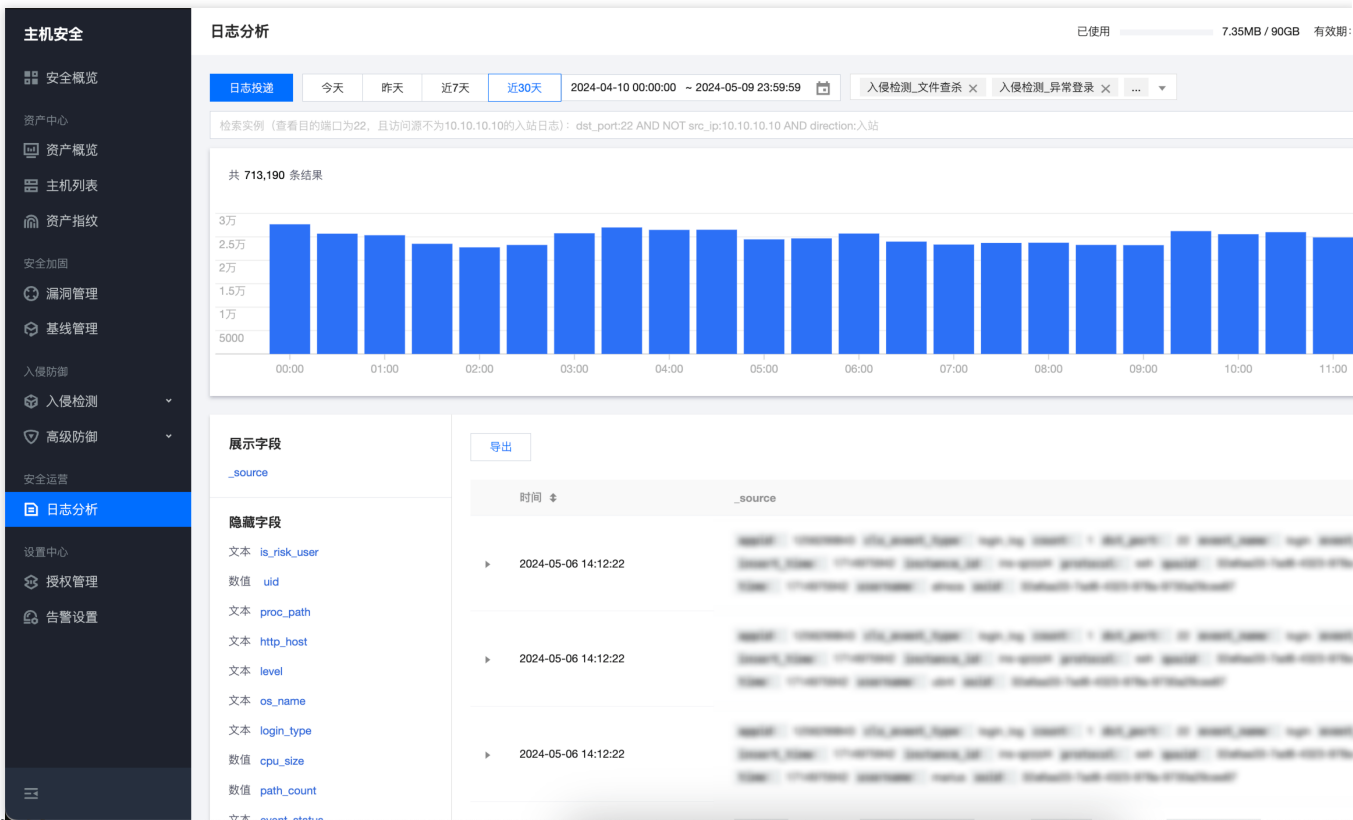
使用日志投递功能，须先 [购买腾讯云消息队列 Ckafka 实例](#)，按照需要投递的日志量来选购对应 Ckafka 实例规格。

日志投递功能，仅支持使用一个消息队列 Ckafka 账号进行投递。

根据《网络安全法》规定，日志存储时长不少于6个月，推荐每台服务器配置20-40GB存储容量，以便采集和留存日志数据。

操作指南

1. 登录 [主机安全控制台](#)。
2. 在左侧导航栏，选择**日志分析**，可进行日志查询、日志投递等操作。



日志存储

单击**日志存储设置**，弹窗如下，在**存储设置**中，可查看当前日志存储情况，可对存储内容、存储时长进行配置。在**存储记录**中，可查看历史每月最后一天零点日志存储的情况，默认倒序展示。

日志存储设置

存储设置

存储记录

已使用/存储总量

18.92GB / 50GB

扩容

日志分析开始时间

2024-03-28

日志分析截止时间

2024-12-31

续期

存储设置

存储内容

☒全部主机资产日志

☒全部客户端上报日志

☒全部告警日志

存储时长

不限（存储至日志服务到期）

1天

30天

60天

90天

180天

您每月仅有2次修改存储时长的机会，超出存储时长的日志我们会为您自动清除。

存储时长保存后，修改内容将在1小时左右生效。

日志存储设置

存储设置

存储记录

记录历史每月最后一天的日志存储情况（仅显示近3个月）

年份/月份

2024年04月

2024年03月

共 2 条

查看日志

在日志分析页面，支持按照如下方式筛选日志。

按时间或类型筛选：在日志分析页面上方，支持按时间和日志类型筛选日志，选定时间范围或日志类型，单击**确定**即可。

日志投递

今天

昨天

近7天

近30天

2024-05-09 00:00:00 ~ 2024-05-09 14:25:26

入侵检测_文件查杀 x 入侵检测_异常登录 x ...

检索实例（查看目的端口为22，且访问源不为10.10.10.10的入站日志）：dst_port:22 AND NOT src_ip:10.10.10.10 AND direction:in

共 213,111 条结果

1.4万

1.2万

1万

8000

6000

4000

2000

00:00

01:00

02:00

03:00

04:00

05:00

06:00

07:00

08:00

09:00

10:00

11:00

入侵检测

☒文件查杀

☒恶意请求

☒反弹SHELL

☒异常登录

☒高危命令

☒密码破解

☒本地提权

基线管理

☒安全基线

客户端相关

☒客户端离线

☒客户端卸载

漏洞管理

☒应急漏洞

☒Web-CMS漏洞

☒Linux软件漏洞

☒应用漏洞

☒Windows系统漏洞

高级防御

☒核心文件监控

☒全选

已选择 16 项

确定

取消

按字段值筛选：在日志分析页面上方，支持搜索框输入字段值筛选、选择字段匹配筛选两种方式。

搜索框输入字段值筛选：参考下图示例，在搜索框中输入想要搜索的字段和字段值，单击



即可进行筛选。

检索语法与示例

语法	语义	示例
key:value	键值搜索，value支持?、*模糊搜索，支持key:(value1 OR value2)	src_ip:10.0.0.1 ; src_ip:(10.0.0.1 OR 10.10.0.1)
A AND B	“与”逻辑，返回A与B的交集结果	src_ip:10.0.0.1 AND protocol:TCP
A OR B	“或”逻辑，返回A或B的并集结果	src_ip:10.0.0.1 OR protocol:TCP
NOT B	“非”逻辑，返回不包含B结果	NOT src_ip:10.0.0.1
A NOT B	“减”逻辑，返回符合A但不符合B的结果，即A-B	src_ip:10.0.0.1 NOT protocol:TCP
*	模糊搜索关键字，匹配零个、单个或多个任意字符，不支持开头*，输入abc*，返回以abc开头的结果	src_ip:10.10*
?	模糊搜索关键字，特定位置匹配单个字符，输入ab?c*，返回以ab为开头，以c为结尾的结果，且两者间有且只有一个字符	src_ip:10.1?.0.1
> < >= <=	大于、小于、大于等于、小于等于，针对数值类型的字段	src_ip:>=100 ; src_ip:(>=10 AND <20)
[] { }	范围查询，中括号 [] 表示闭区间，{ }表示开区间	src_ip:[1 TO 5}
()	布尔运算符不遵循优先级规则，当使用多个运算符时，使用括号指定优先级	src_ip:10.0.0.1 AND (protocol:TCP OR src_port:80)

• 语法关键词区分大小写

选择字段匹配筛选：单击



，在下拉列表中选择合适的字段和操作符，再输入对应的字段值，单击**确定**即可进行筛选。

port

模糊匹配字符

2

value

模糊匹配字符

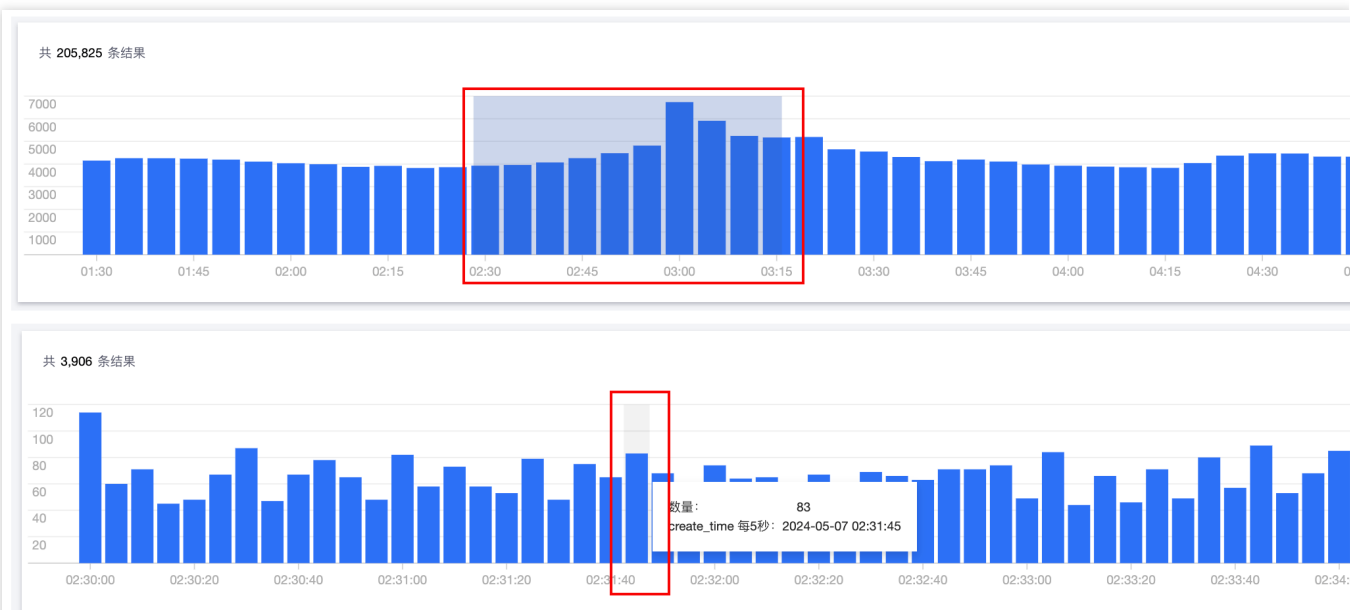
2

确定

取消

说明：

针对常用的检索可**保存检索**，下次直接单击**快速检索**，选中要原先保存的检索内容进行筛选即可。
在日志分析页面，鼠标单击柱状图或单击后滑动，可快速选定时间范围，进行下钻查看。



在日志分析页面，在列表左侧的字段导航中，可自定义展示字段和隐藏字段。

展示字段	导出
数值 uid	
文本 proc_path	隐藏
隐藏字段	
文本 is_risk_user	显示
文本 http_host	
文本 level	
文本 os_name	
文本 login_type	

时间	_source
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -

单击**导出**，可将满足检索条件的日志导出为文件，并通过浏览器下载到本地。

说明：

单次最多支持导出60000条日志，最大支持每种类型导出10000条数据。

日志投递

在日志分析页面，您可配置主机安全不同日志类型分别投递到指定 **Ckafka** 实例的不同 **Topic** 中。

- 单击左上角的**日志投递**，打开日志投递配置弹窗，首次若未授权 **Ckafka** 服务，须先单击**前往授权**，同意服务授权后才可进行更多日志投递配置。



- 同意授权服务后，须选择消息队列实例、网络接入方式，输入所选消息队列实例的用户名和密码，并进行连通性测试。

配置日志投递

Ckafka授权状态

已授权

网络接入方式

公网域名接入

支撑环境接入

内网投递

消息队列实例

请选择

用户名

.com

公网域名接入

请选择

密码

连通性测试

开始测试

3. 选择网络接入方式。

网络接入方式	描述	可选路由说明
公网域名接入	通过公网进行日志投递。	是消息队列实例中所定的接入方式。
支撑环境接入	通过腾讯云内网进行日志投递，性能更高。	是消息队列实例中所定的接入方式，但暂不支持 PLAINTEXT 接入方式。
内网投递	通过腾讯云内网进行日志投递，但路由无需用户在 kafka 中进行配置，会自动创建一个不可见的内部路由来支持接入。	-

说明：

网络接入方式若选择“公网域名接入”、“支撑环境接入”，还需要选择接入路由，路由策略对应 Ckafka 实例列表 详情中的接入方式。

日志投递

查看用户文档 前往消息队列控制台

1. 购买消息队列Ckafka实例，推荐按照需要投递的日志量来选购对应Ckafka实例规格

2. 根据消息队列Ckafka文档指引，开通白名单实例公网域名接入 或 支撑环境接入

3. 按照本文页面上方指引完成日志投递配置，仅支持使用同一消息队列实例进行投递

配置日志投递

Ckafka授权状态

已授权

网络接入方式

公网域名接入

支撑环境接入

内网投递

消息队列实例

请选择

用户名

.com

公网域名接入

请选择

密码

连通性测试

开始测试

消息队列 Ckafka 版

topic管理 Consumer Group 监控 事件中心 HTTP接入 ACL策略管理

基本信息

名称 云恢复测试环境

ID kafka-xxxxxxxxxxxx

实例版本 最新

网络与端口 公网IP: 10.10.10.10

地域 广州

可用区 广州三区

状态 健康

标签 云恢复测试环境

系统维护时间 每周一、二、三、四、五、六、日 23:30

支持的数据压缩算法 lz4,snappy

接入方式

选择路由策略

接入类型	接入方式	网络	备注	操作
VPC网络	PLAINTEXT	10.10.10.10	10.10.10.10	删除 查看所有IP和端口
基础网络	PLAINTEXT	10.10.10.10	10.10.10.10	删除 查看所有IP和端口
支撑环境(后)	PLAINTEXT	10.10.10.10	10.10.10.10	删除 查看所有IP和端口

网络信息

公网网络 基础网络

最大连接数 100000

配置信息

规格 4C16GB

峰值带宽 400Mbps

磁盘容量 1000GB

已部署Topic数 1000

已创建分区数 1000

消息配置 100

实例计费信息

计费方式 按量付费

创建时间 2019-07-15 14:44:22

到期时间 2024-05-15 14:44:22

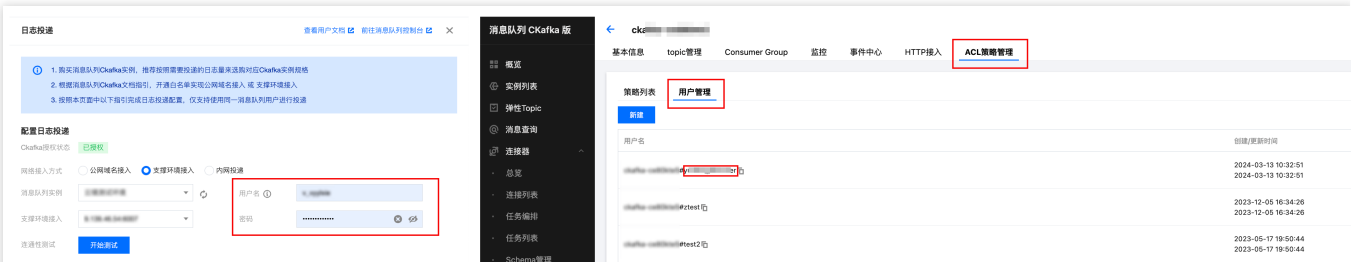
消息配置

默认消息保留时长 30天

默认最大消息大小 1MB

自动创建Topic

网络接入方式若选择“公网域名接入”、“支撑环境接入”，还需要填写 Ckafka 实例的用户名和密码，用户名密码在 Ckafka 实例列表 详情中的 ACL 策略管理 > 用户管理 添加。（在配置日志投递时，仅填写#后的用户名即可，无需填写#及其前的 Ckafka 实例 ID。）



4. 完成上述 Kafka 配置后，可进行连通性测试，测试通过后，您可对要进行投递的日志配置不同的 Topic（不进行投递的日志类型，可以不选择 Topic ID）。

安全模块	日志类型	Topic ID/名称 ⓘ
入侵检测	密码破解, 恶意请求 ▼	请选择 ▼
漏洞管理	Windows系统漏洞, Web-CM... ▼	请选择 ▼
基线管理	安全基线 ▼	请选择 ▼
高级防御	核心文件监控 ▼	请选择 ▼
客户端相关	客户端离线, 客户端卸载 ▼	请选择 ▼

5. 日志投递配置完成后，再次单击**日志投递**，可查看日志投递详情。

日志投递

前往消息队列控制台

实例名称

实例ID

地域

可用区

所属网络

所在子网

接入方式

接入地址

状态

版本

峰值带宽

磁盘容量

用户名

配置列表

重新配置

查看监控

安全模块	日志类型	TopicID/名称	投递开关	投递状态	操作
入侵检测	-	:		未开启	编辑 查看监控
漏洞管理	-	:		未开启	编辑 查看监控
基线管理	-	:		未开启	编辑 查看监控
高级防御	核心文件监控	TopicID: 123456789		未开启	编辑 查看监控
客户端相关	-	:		未开启	编辑 查看监控

基本信息：展示 Ckafka 实例的基本信息。

说明：

您需要关注“状态”字段，当展示告警或异常时，请单击**查看监控**，查看 Ckafka 服务是否异常，或者是否配额不足。

投递开关：用于控制指定的日志类型，启动或停止日志投递任务，您可以在**投递开关**列，通过开关按钮控制日志投递任务。

投递状态：正常、异常（此状态会中止投递）、未开启。

编辑：单击**编辑**，可再次编辑要投递的日志类型和 Topic ID。

查看监控：单击**查看监控**，会跳转至消息队列 Ckafka 控制台的监控页面，您可以查看网络流量、峰值带宽、消息条数、磁盘占用等情况。

重新配置：在日志投递列表上方，单击**重新配置**，将回到已同意 Ckafka 授权服务后的状态，您可对消息队列实例、网络接入方式、日志类型、Topic ID 等进行重新配置。

说明：

重新配置，会中断当前的投递进程。

授权管理

最近更新时间：2024-08-13 16:29:50

防护授权是基于主机安全客户端提供的安全防护服务，购买防护授权并绑定到已安装客户端的主机上，主机即可获得全方位的安全防护，包括入侵检测、漏洞管理、基线管理等功能。防护授权具有灵活的管理机制，可实现自动续费、自动绑定以及自动加购等操作，简化了用户对防护授权管理的压力。

限制说明

防护授权仅支持绑定到已安装主机安全客户端的主机上。

关联腾讯云标签、所属项目的对象是防护授权订单，而非具体授权和主机。

开启**新增主机设置**中的自动回溯开关后，仅旗舰版主机支持自动回溯近**14**天内的入侵告警数据。

仅专业版-按量计费授权订单支持缩容、销毁操作。

说明：

因计费模式调整，主机安全从**2023年11月30日**起下线专业版的按量计费模式，调整后，不再支持新购按量计费模式的专业版，已购按量计费订单仍可正常使用、扩容等。

购买防护授权

1. 登录 [主机安全控制台](#)，在左侧导航栏，选择**授权管理**。
2. 在授权管理页面，单击**购买防护授权**，前往[主机安全购买页](#)，选择防护版本、时长、授权数并绑定主机，完成支付后，防护即自动生效。

说明：

也可先购买防护授权，再前往 [授权管理页](#) 对主机进行绑定。

若在[主机安全购买页](#)中设置了防护授权数（前提）、勾选了自动绑定或自动加购项并支付成功，该配置将同步至[授权管理页](#)中。

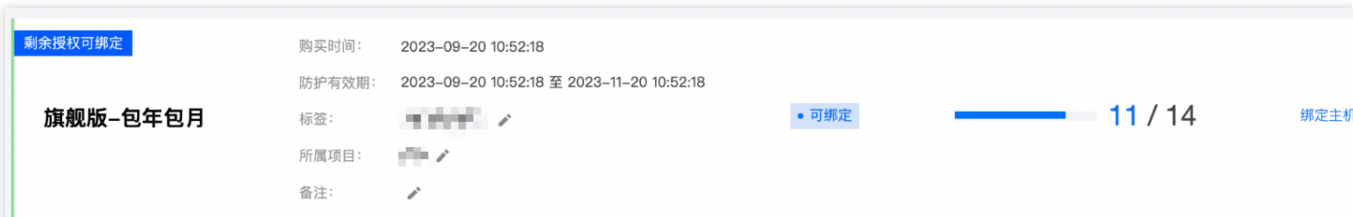


设置自动续费

方式一：在 [授权管理页面](#)，勾选需要自动续费的授权订单，开启自动续费开关即可。



方式二：在 [授权管理页面](#) 的授权列表中，针对需要自动续费的授权订单，勾选自动续费项即可。



方式三：在 [费用中心 > 续费管理](#) 中，针对需要自动续费的授权订单资源，设为自动续费即可。



说明：

以上三种自动续费方式默认按1个月续费，自动续费后，防护版本、授权数均与原订单保持一致。

若用户在 [费用中心 > 续费管理](#) 中，修改了自动续费周期，以上三种方式的自动续费，均以用户修改后的续费周期进行续费。

部分客户具备到期不停服特权，若关闭自动续费，则针对相应授权订单的不停服特权将失效，到期后将不再自动续费。

设置自动绑定

在 [授权管理页面](#)，单击开启 **自动绑定** 开关，即可在检测到新增基础版主机时，自动绑定剩余可用授权。

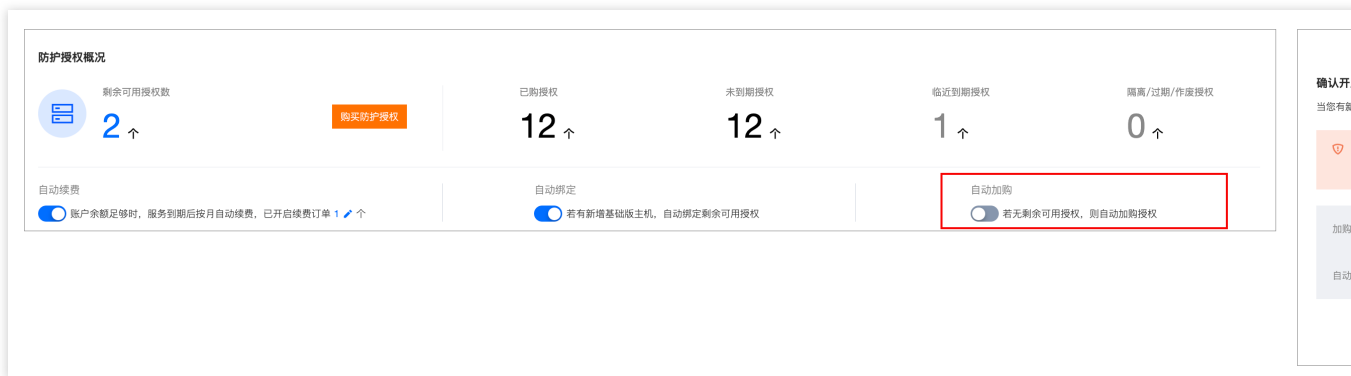


说明：

新增基础版主机：指从未绑过付费版授权的基础版主机（不包括因解绑付费版授权而回退基础版的主机）。
若存在多个不同版本和时长的防护授权订单，优先绑定高版本且到期时间晚的授权。

设置自动加购

在 [授权管理页面](#)，配置加购防护版本，开启 **自动绑定** 和 **自动加购** 开关后，当自动绑定无剩余授权可绑时，将自动为您扩容/新购授权并绑定新增基础版主机。



说明：

自动加购生效的前提是自动绑定和自动加购开关均已开启，否则实际不会进行自动加购。
用户所设加购防护版本，若在授权订单列表中存在多个相应版本订单，则优先扩容到期时间晚的授权订单。反之，若在授权订单列表中无相应版本订单，则新购授权，默认购买1个月。

防护授权概况

在 [授权管理页面](#)，防护安全概况统计展示剩余可用授权数、已购授权数、未到期授权数、临近到期授权数、隔离/过期/作废授权数，提供自动续费、自动绑定、自动加购开关。

防护授权概况

剩余可用授权数

1 ↑

购买防护授权

已购授权

12 ↑

未到期授权

12 ↑

自动续费

账户余额足够时，服务到期后按月自动续费，已开启续费订单 1 个

自动绑定

若有新增基础版主机，自动绑定剩余可用授权

字段说明：

- 剩余可用授权数：当前未使用的授权总数。
- 已购授权数：历史购买的授权总数，含未到期授权数、临近到期授权数、已过期/作废的授权数（不统计被删除记录的过期/作废授权）。
- 未到期授权数：未到期的授权总数。
- 临近到期授权数：15天内即将到期授权总数。
- 隔离/过期/作废授权数：即包年包月到期或按量计费欠费进入隔离期、过期、作废的授权总数。

防护授权列表

在 [授权管理页面](#) 的授权列表中可查看所有已购授权订单，支持对授权进行如下操作。

绑定/解绑/更换授权

绑定：单击**绑定主机**，将授权绑定到主机上，即可获得相应版本的防护服务。

剩余授权可绑定

专业版-包年包月

购买时间：2024-04-24 15:47:04

防护有效期：2024-04-24 15:47:04 至 2024-05-24 15:47:04

标签：

所属项目：

备注：

可绑定

0 / 1

绑定主机

解绑/更换：单击**授权详情**可查看当前授权绑定情况，可对主机进行解绑/更换授权操作。解绑后，主机将回退为基础版；更换授权，仅可更换成同版本或更高版本的授权。

专业版-包年包月

购买时间：2024-04-24 15:47:04

防护有效期：2024-04-24 15:47:04 至 2024-05-24 15:47:04

标签：

所属项目：

备注：

使用中

1 / 1

授权详情

续费

扩容

升级旗舰版

自动续费 ①

已绑定主机 (1)

批量解绑

批量更换授权

主机名称/实例ID	IP
x-xxxxxxxxxxxx	10.0.0.1

共 1 条

说明：

每月每个授权订单累计可解绑 + 更换次数 = 该授权订单的授权数 × 2。

升级/扩容

升级：针对专业版-包年包月授权订单，单击**升级旗舰版**并确定升级，可将其升级为旗舰版。

剩余授权可绑定

专业版-包年包月

购买时间：2023-10-27 16:49:23
防护有效期：2023-10-27 16:49:23 至 2023-11-27 16:49:23
标签：
所属项目：
备注：

可绑定

0 / 1

绑定主机 | 授权详情 | 续费 | 扩容 | 升级旗舰版 | 自动续费 ①

升级旗舰版

正在对以下授权订单进行升级旗舰版操作：

资源ID	产品描述/备注
	专业版-包年包月

总计费用：

扩容：单击**扩容**，输入扩容后的授权数并确定扩容，即可对当前授权订单进行扩容。

剩余授权可绑定

旗舰版-包年包月

购买时间：2023-09-20 10:52:18
防护有效期：2023-09-20 10:52:18 至 2023-11-20 10:52:18
标签：
所属项目：
备注：

可绑定

11 / 14

绑定主机 | 授权详情 | 续费 | 扩容 | 自动续费 ①

扩容

正在对以下授权订单进行扩容操作：

资源ID	产品描述/备注	产
	旗舰版-包年包月	总

总计费用：

访问管理指引

最近更新时间：2024-08-13 16:29:50

背景信息

如果您在腾讯云中使用到了多款产品服务，这些服务由不同人分管，但都共享最高权限的主账号密钥，将存在以下问题：

密钥由多人共享，泄密风险高。

无法限制其它人的访问权限，易产生误操作造成安全风险。

此时，您可通过 [访问管理](#)（Cloud Access Management，CAM）新建多个用户，以实现不同人管理不同服务。并且可以通过关联策略，让不同用户拥有在各个服务控制台上进行查看和操作的权限。本文档提供了主机安全查看和操作权限的示例，指导用户如何使用主机安全的访问策略。

操作示例

全读写策略

如果您希望用户拥有主机安全产品所有接口的读写权限，可对该用户关联名称为：QcloudCWPFullAccess 的策略。具体操作步骤参考 [授权管理](#)，将预设策略 QcloudCWPFullAccess 授权给用户。

只读策略

如果您希望用户拥有查询主机安全的权限，但是不具有新增、删除、修改等操作的权限，可对该用户关联名称为：QcloudCWPRedOnlyAccess 的策略。该策略是通过给用户开放以"Describe"、"Get"、"Check"、"Export"为开头的接口访问权限来达到目的。

具体操作步骤参考 [授权管理](#)，将预设策略 QcloudCWPRedOnlyAccess 授权给用户。

自定义策略

如果您觉得预设策略不能满足您的要求，您可以通过 [创建自定义策略](#) 达到目的。

说明：

新建的用户默认不关联主机安全任何策略，即不具备任何权限。了解更多详见 [访问管理用户指南](#)。

混合云安装指引

概述

最近更新时间：2024-08-13 16:29:50

背景信息

随着企业上云率提升，更多中大型企业选择公有云+私有云的混合云模式，兼具公有云成本低、敏捷、灵活、使用方便及私有云可控、安全、高可用部署的优点。混合云管理功能能够支持用户接入非腾讯云机器，更好地帮助用户统一管理 and 监控主机安全。

功能概述

支持腾讯云的边缘计算机器、轻量应用服务器自动接入主机安全。

支持非腾讯云服务器，如：私有云、阿里云、华为云、青云、亚马逊云、UCloud 等云服务器手动接入主机安全。

客户端支持版本说明

Linux 系统支持版本

RHEL：Versions 6.1+（64 bit）

CentOS：Versions 6.3+（64 bit）

Ubuntu：9.10+（64 bit）

Debian：6+（64 bit）

Windows 系统支持版本

Windows server 2012, 2016, 2019

Windows server 2008+ R2

Windows server 2003（limited support）

配置非腾讯云机器

最近更新时间：2024-08-13 16:29:50

步骤1：安装主机安全客户端

1. 登录 [主机安全控制台](#)，在左侧导航栏，单击[主机列表](#) > [安装主机安全客户端](#)，在右侧弹窗中查看安装指引详情。



2. 在安装指引中选择服务器类型、服务器系统及推荐安装方式，如果是通过专线打通云上云外的话，选择专线安装方式，否则选择公网的安装方式。

通过公网接入：单击



图标复制并执行相应命令，即可安装主机安全客户端，**需注意命令有效期**。

选择合适的安装方式

服务器类型

服务器系统

推荐安装方式 [了解专线](#)

Windows 2008及以上系统适用

命令有效期

po 2021-06-25

通过专线接入：选择已连专线的 VPC，单击



图标复制并执行相应命令，即可安装主机安全客户端，**需注意命令有效期**。

说明：

如需了解专线相关，可单击[了解专线](#)跳转专线接入控制台。

如防火墙需开放目标 IP，参考图片中④对命令中 IP 开放访问权限。

选择合适的安装方式

服务器类型

服务器系统

推荐安装方式 [了解专线](#) ①

已连专线的VPC

复制并执行相应命令 ④

`wget http://172.16.0.2/ydeyes_linux64_mix.tar.gz -O ydeyes_linux64_mix.tar.gz && tar` ②

命令有效期 ③

2021-06-25

步骤2：确认是否安装成功

1. 按照安装指引-判断是否安装成功的命令执行。

Linux

执行命令：`ps -ef | grep YD` 查看 YDService, YDLive 进程是否有运行。

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root      16216 21992  0 14:33 pts/3      00:00:00 grep --color=auto YD
root      32707   1   0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root      32724   1   0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

进程无运行, root 用户可手动启动程序, 执行命令：`/usr/local/qcloud/YunJing/startYD.sh` 或者 `/var/lib/qcloud/YunJing/startYD.sh`。

Windows

打开任务管理器查看 YDLive 进程是否有运行。

进程无运行, 可通过任务管理器手动启动服务。

2. 安装成功后在 [主机列表](#) 页面, 单击**全部服务器专区** > **非腾讯云服务器专区**, 即可查看对应服务器。

说明：

检查服务是否上线, 先检查客户端是否安装成功, 然后在 [主机列表](#) 可查看, 服务器属“防护中”即服务已上线。

如未正常上线, 请 [联系我们](#) 获得支持。



步骤3：升级主机安全版本

1. 单击选择**非腾讯云服务器专区**, 即可查看对应服务器, 单击**授权管理**即可进入授权管理页面升级为主机安全**专业版**或**旗舰版**。

安装主机安全客户端	升级版本	非腾讯云服务器专区	1 地域						
全部主机	18	服务器IP/名称	操作系统	风险状态	防护状态	入侵检测	漏洞风险	查	
风险主机	6		CentOS Linux release 7.9.2009 (Core)	未知	已离线	停止检测	0	情	
旗舰版主机	8								
专业版主机	0		CentOS Linux release 8.2.2004 (Core)	未知	已离线	停止检测	停止检测	情	
基础版主机	10		CentOS Linux release 7.9.2009 (Core)	风险	已离线	8	2	0	
未安装客户端 (无防护)	0								
已离线	15		Windows_Server_2016_Datacenter-Server...	风险	已离线	2	0	4	

2. 升级后可测试主机安全专业版或旗舰版功能，支持功能包括：资产同步、木马扫描、漏洞扫描、异常登录、密码破解（非腾讯云环境不支持阻断）、反弹 Shell、本地提权、高危命令、恶意请求等。

连接专线 VPC

最近更新时间：2024-08-13 16:29:50

背景信息

目前 VPC 专线接入暂时只支持华南地区（广州）、华北地区（北京）、华东地区（上海、上海金融、南京），西南地区（成都），已经支持公有云与客户机房网络在VPC内互通，可以直接安装客户端。

若需要接入的地区不在 VPC 专线接入的范围之内，需要通过云联网，将专线网关（VPN）与 VPC打通。专线网关需要客户另行购买和搭建完成对 VPC 专线接入的工作。

操作指南

步骤1：确认是否需要通过云联网进行接入

1. 登录 [主机安全控制台](#)，在左侧导航栏，单击[主机列表](#) > [安装主机安全客户端](#)，在右侧弹窗中查看安装指引详情。



2. 在安装指引中，服务器类型单击选择[非腾讯云](#)，推荐安装方式单击选择[专线](#)。

说明：

服务器系统按照用户的操作系统，选择相对应 Linux 或 Windows 操作系统。



3. 如您在华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区：

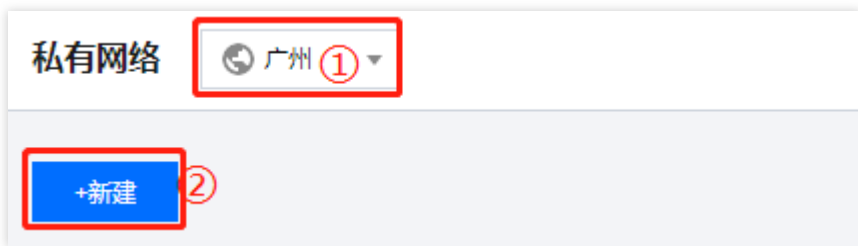
已有和非腾讯云机房网络互联的 VPC，则选择已连接专线的 VPC 网络，直接使用安装命令安装。

没有找到相应的 VPC 网络与您的非腾讯云机房网络进行互联，可参考 [步骤2](#) 云联网。

步骤2：确认用于连接专线的私有网络

1. 如您在当前华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区没有 VPC 网络，则登录 [私有网络](#) 控制台，单击**私有网络**进入私有网络页面。

2. 在私有网络页面中，单击“下拉框”选择所需区域，单击**新建**，弹出新建 VPC 弹窗。



3. 在新建 VPC 弹窗中，输入所需参数单击**确定**，即可完成新建 VPC。

步骤3：通过云联网实现VPC和已连专线的非腾讯云机房网络互通

1. 如已存在和非腾讯云机房通信的云联网，则将 [步骤2](#) 中选择的 VPC 实例添加到云联网中。

a. 登录 [私有网络](#) 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。

b. 在云联网页面，单击右侧**管理实例 > 关联实例**，进入关联实例页面。

c. 在关联实例页面，单击**新增实例**，将 [步骤2](#) 中选择的 VPC 实例添加到云联网中，单击**确定**即完成关联实例。

2. 如尚未配置云联网，则需要新建。

a. 登录 [私有网络](#) 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。

b. 在云联网页面中，单击**新建**，弹出新建云联网实例弹窗。

c. 在新建云联网实例弹窗，输入所需参数单击**确定**，即可完成新建云联网实例。

说明

专线网关：请选择您和非腾讯云机房通信连接的专线网关。

私有网络：请选择 [步骤2](#) 中选择的 VPC 实例。

如出现 IP 地址段冲突，请返回 [步骤2](#) 重新选择或新建一个不会冲突的 VPC 实例。

3. 回到 [主机安全控制台](#)，参考 [步骤1](#) 获取安装命令进行安装。您的非腾讯云机房需要放通对 [步骤1](#) 中描述的 IP 的 5574、8080、80、9080 共4个端口的访问。

热点问题

最近更新时间：2024-08-13 16:29:50

混合云是否对主机安全的版本有要求？

有的，必须是**专业版或旗舰版**才支持混合云的功能。

如何将主机安全升级至专业版或旗舰版？

1. 登录 [主机安全控制台](#)，在左侧导航栏，选择**授权管理**>**购买防护授权**，进入购买页面。
2. 在购买页面里，可输入要购买的授权数（旗舰版或专业版），根据需求选择后单击**立即购买**。购买成功后再前往授权管理页面，为需要防护的主机绑定授权即可。授权操作详情请参见授权管理。

选择配置

防护版本

专业版

旗舰版

版本功能对比

功能介绍

重点提供高级威胁检测+防御修复能力，满足重保护网、入侵溯源等场景安全需求。

- 资产管理：提供资产暴露面分析，支持自动化资产清点，支持15种资产指纹上报，支持分类展示TOP5统计，帮助用户了解资产全貌。
- 入侵检测：支持7大入侵检测功能（文件查杀、密码破解、异常登录、恶意请求、本地提权、反弹shell、高危命令），覆盖200+入侵检测点，百万级溯源。
- 漏洞管理：支持4大漏洞类型检测，覆盖10w+高危漏洞库，提供一键检测与漏洞修复功能，共享腾讯应急漏洞服务。
- 安全基线：支持CIS、等保二级、三级基线合规要求，支持一键检测、定时检测和自定义基线检测，并提供专业修复建议。
- 高级防御：支持4大高级威胁检测和防御功能（核心文件监控、rootkit、内存马、勒索防御，部分待发布），保护用户核心资产。
- 安全运营：提供安全预警等功能，支持大屏可视化，以及入侵溯源分析等功能。

计费模式

包年包月

旗舰版仅支持包年包月计费方式，时间越长折扣优惠越高。

防护时长

1个月

2个月

3个月

半年

1年

2年

3年

自动续费

☒ 账户余额足够时，服务到期后按月自动续费

防护授权

-

85

+

个

检测到您目前尚有85台主机暂未开通防护，建议您购买≥85的授权

☐ 立即绑定主机（已选择 0 台）

若不选择立即绑定主机，可返回控制台<设置中心-授权管理>再进行主机绑定，开启旗舰防护

安全防护 0元

增值服务 0.00元

立即购买

专线连接到云端，目标地址和开放端口是多少？

请参考下图的目标地址和开放端口，放通防火墙权限。

说明：

地址和开放端口是不会变化。

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

基础网络域名	s.yd.qcloud.com、l.yd.qcloud.com、u.yd.qcloud.com	基础网络端口	5574、8080、80、
VPC网络域名	s.yd.tencentyun.com、l.yd.tencentyun.com、 u.yd.tencentyun.com	VPC网络端口	5574、8080、80、
公网域名	sp.yd.qcloud.com、lp.yd.qcloud.com、up.yd.qcloud.com		
公网端口	5574、8080、80、443、9080		

非中国大陆地区的 IDC 是否支持安装 Agent?

支持的，目前只要机器能够联网，系统满足要求，就可以安装主机安全 Agent。

安装 Agent 后，控制台目前多久会展示非腾讯云机器？

目前是秒级支持。

非腾讯云机器，需要另外购买控制台吗？

不需要的，统一在公有云控制台进行管理、计费。

需要开 IDC 到云上的网络端口访问权限，目标 IP 和端口是什么？

目标 IP 是安装命令内的 IP，端口5574 80 8080 9080。

内网机器，无法访问公网或者没有专线的情况下是不是无法使用主机安全？

目前是的。

混合云的客户端会和 Zabbix 进程冲突吗？

我们没有对 Zabbix 做特殊处理，也没有注入等，可以关注下机器上是否有其他的客户端安装驱动。

新手常见问题

最近更新时间：2024-08-13 16:29:50

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、DDoS 木马程序，消耗大量系统资源，导致服务器不能提供正常服务。

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，服务器可能已被黑客入侵并留下了后门程序。

检查服务器安全状况，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，并修改服务器登录密码，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](#)。

根据实际情况决定是否需要对服务器进行重置，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。

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，用户需要对服务器进行详细的安全检查。

服务器显示防护状态显示离线原因及解决方案？

腾讯云服务器安全组件未连接服务端，导致后台显示离线，建议重新下载安全组件进行安装，离线的可能原因如下：

服务器启用了防火墙规则。

服务器安装了第三方恶意软件，导致安全防护程序被破坏。

如何处理木马文件？

如需处理木马文件，请参见 [木马文件操作处理](#)。

未能成功检测出木马（漏报）如何解决？

若发现有未检测出来的木马文件，可通过 [工单](#) 联系提交给腾讯云安全团队，由腾讯云安全团队快速鉴定。

如何卸载腾讯云主机安全组件？

登录 [主机安全控制台](#)，在左侧导航栏选择[资产中心](#) > [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。

如何通过一键快照自动备份数据？

快照是腾讯云提供的一种数据备份方式，通过对指定云硬盘进行完全可用的拷贝，使该备份独立于云硬盘的生命周期。客户定期创建快照，可以在出现数据意外丢失等情况下帮助客户快速恢复数据。

使用控制台创建快照步骤：

1. 登录 [云硬盘控制台](#)。
2. 在云硬盘页面，找到需要创建快照的实例所在行，单击**创建快照**。



ID/名称	监控	状态	可用区	属性	数据保护	类型	容量	关联实例
lve...		使用中	广...	系统盘	否	通用型SSD云硬盘	50GB	ir...
d...		使用中	广...	系统盘	否	通用型SSD云硬盘	50GB	in...

3. 在创建快照页面确认相关信息，填写快照名称，单击**提交**，等待创建快照即可。

更多信息请参见 [快照概述](#) 及 [创建快照](#) 文档。

如何降低主机被入侵概率？

及时修复高危漏洞及基线相关问题。

设置强密码，避免爆破攻击。

定期巡检账号、权限、端口并及时处理 [主机安全控制台](#) 的告警信息。

定期做快照备份。

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。

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。

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。

腾讯云平台提供 [安全组功能](#)，建议您只放行业务协议和端口，不建议放行所有协议所有端口。

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。