云主机安全（龙卫士）

产品文档

文档目录

- 产品简介
  - 龙卫士是什么
  - 为什么需要主机安全
  - 产品优势
  - 基本概念
- 功能介绍
  - 安全概览
  - 资产管理
  - 入侵检测
  - 漏洞管理
  - 基线管理
  - 设置中心
- 操作指南
  - 安全概览
    - 功能简介
    - 安全状态
    - 安全防护
    - 防护详情
    - 风险趋势
    - 实时动态
  - 资产管理
    - 概览
    - 主机列表
    - 资产指纹
  - 入侵检测
    - 文件查杀
    - 异常登录
    - 密码破解
    - 本地提权
    - 反弹Shell
    - 高危命令
    - Java内存马
  - 漏洞管理
    - 背景信息
    - 操作指南

- 基线管理
  - 背景信息
  - 操作指南
- 高级防御
- 设置中心
  - 告警设置
- 授权管理

快速入门

- 入门准备
- 龙卫士安装
  - Windows云服务器环境
  - Linux云服务器环境
- 常见问题
- 故障处理
  - Linux 入侵类问题排查思路
  - Linux客户端离线排查
  - Windows入侵类排查思路
  - Windows客户端离线排查
  - 异常登录的消息提醒

常见问题

- 功能相关
- 入侵相关
  - 入侵常见问题
  - 木马类问题
  - 异常登录类问题
  - 密码泄露类问题
  - 防护状态离线类问题

产品简介
龙卫士是什么

最近更新时间: 2023-08-17 14:33:59

主机安全是一款针对多云主机的安全防护产品，基于安全积累的海量威胁数据，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

最近更新时间: 2023-08-17 14:55:41

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，用户隐私数据被泄漏，造成企业品牌受损和用户流失。
- 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，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。

产品优势

最近更新时间: 2023-08-17 14:55:41

1.基于威胁情报数据源，实时检测黑客攻击行为 。
2.后端集成新一代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。
3.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。
4.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。
5.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。

基本概念

最近更新时间: 2023-08-17 14:44:51

- **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、记录键盘和攻击 DDoS 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。
- **系统组件：** 组件（Component）或者通用组件，在主机安全层面主要泛指服务、应用对应的 Web 容器、软件等，例如 Nginx、Wordpress 等，而系统组件主要指非 Web 类的系统软件。
- **通用组件漏洞：** 通用组件漏洞又称为通用漏洞（Common Vulnerability），主要指通用组件而非业务自开发代码产生的漏洞，例如 WordPress 某个 SQL 注入、组件 Bash 的破壳漏洞等。
- **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：** 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。

功能介绍
安全概览

最近更新时间: 2023-08-17 14:44:51

实时展示主机安全体检得分、防护状态、待处理风险、风险趋势以及主机安全的实时动态。

资产管理

最近更新时间: 2023-08-17 14:44:51

概览： 可查看全部主机及各项资产指纹的统计情况、主机概况趋势图、资源监控概览以及查看账号、端口、进程、软件应用、数据库、Web 应用、Web 服务、Web 框架、Web 站点 TOP5。

主机列表： 主机列表支持按分类筛选主机、查看防护/风险状态、安装/卸载客户端等功能，方便用户统一管理服务器。

资产指纹： 展示资产指纹分类列表，包括各资产指纹项及其对应服务器数量。支持对指纹数据的查询和导出。

入侵检测

最近更新时间: 2023-08-17 14:44:51

 文件查杀：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。提供对二进制可执行类的病毒木马检测。

 异常登录： 支持实时监控异常登录行为，识别非白名单 IP 登录并判定威胁等级，支持白名单配置，条件支持实时检测主机内外联恶意域名请求，提供威胁源信息和事件记录，并自动告警用户。包括：来源 IP、登录用户名、登录时间、登录地和生效服务器范围。

 密码破解：支持对 SSH、RDP 等暴力破解行为进行实时检测、告警、阻断功能，支持登录白名单配置，支持自定义暴破阻断规则，事件记录包含：来源 IP、来源地、登录用户名、攻击时间、尝试次数、阻断状态等信息。

 本地提权：实时监控并告警您服务器上的权限提高事件（以低权限进入主机，之后通过某种行为获得高权限），支持白名单配置；事件记录包含：服务器/名称、提权用户、提权进程、父进程、父进程所属用户、发现时间、文件路径及进程树等。

 反弹Shell：对服务器公网反弹 Shell 建立的连接行为进行识别和告警，并支持白名单配置；事件记录包含：服务器/名称、连接进程、父进程、目标主机、目标端口、发现时间、文件路径、进程树及执行命令等。

 高危命令：记录云服务器上执行的 bash 命令，实时监控被审计规则判断为危险的操作；提供默认规则配置，以及支持用户自定义规则配置；事件记录包含：服务器/名称、命中规则名、危险等级、命令内容、登录用户及操作时间等。 **Java内存马**：实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合建行云攻防经验及专家知识自动识别内存木马，检测到内存马，系统将为您实时告警。

漏洞管理

最近更新时间: 2023-08-17 14:55:41

应急漏洞：支持检测近期紧急漏洞检测（例如 0day 等）。漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。

Linux软件漏洞：支持常用 Linux 软件漏洞检测，提供修复方案，例如：gnutls资源管理错误等 Linux 软件漏洞。漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。

Windows系统漏洞：通过实时同步微软官网补丁源，对 Windows 系统漏洞进行检测并提供修复方案，避免黑客通过 Windows 系统漏洞攻击或威胁您的服务器安全；漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。

Web-CMS漏洞：支持常用 Web 类型的漏洞检测，提供修复方案，例如 phpMyAdmin 及 WordPress 等 Web 类组件；漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。

应用漏洞：提供系统服务弱口令、系统服务和应用服务的漏洞检测服务；漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。

基线管理

最近更新时间: 2023-08-17 14:55:41

- **基线概览**：展示不同基线策略下的检测服务器、检测项、基线通过率、基线检测项 TOP5 和服务器风险 TOP5 检测结果信息，支持一键检测和定期检测。
- **支持基线检测策略**：支持等保二级、三级、国际标准基线、云安全标准、弱口令等基线检测，并提供修复方案。

设置中心

最近更新时间: 2023-08-17 14:55:41

- **告警设置**：支持短信、邮件等告警通知发送方式，支持输出告警事件列表。
- **授权管理**：成功购买主机安全专业版或旗舰版可在授权管理页面绑定要升级防护的主机。已成功升级防护的主机也可进行解绑操作。

操作指南
安全概览
功能简介

最近更新时间: 2023-08-17 14:54:19

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。

安全状态

最近更新时间: 2023-08-20 15:09:08

1.安全状态功能中，展示您的主机安全评分和安全风险情况，并提供快捷处理入口。且将安全风险划分为3大类：

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三个等级：

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、暴破成功、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

安全防护

最近更新时间: 2023-08-20 15:09:08

在安全防护功能中，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

最近更新时间: 2023-08-21 16:07:44

在防护详情功能中，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，目前已防护主机数、旗舰版数量、专业版数量、基础版数量、日志分析使用情况和网页防篡改授权数量，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。

字段说明:

- 单击右上方立即更新，可更新资产信息。
- 单击右上方版本对比，展示主机安全产品提供的基础版、专业版、旗舰版和增值服务防护的功能对比。
- 在未安装客户端主机中，单击安装，界面展示安装引导。
- 单击日志分析右侧的升级扩容或网页防篡改右侧的购买授权，可购买对应的服务。
- 在基础版主机中，单击升级，将跳转到主机安全购买页面，您可以通过购买对基础版主机进行升级，为您的主机提供更为强大的风险威胁抵御能力。

- 安全引擎防护将展示6个引擎图标，分别代表云查杀引擎、BinaryAI 引擎、TAV 引擎、异常行为、威胁情报、攻击防御。若未开启防护功能，对应功能图标处于灰色状态。若有任意一台主机，开通防护功能，则对应功能图标处于点亮状态。

风险趋势

最近更新时间: 2023-08-20 15:14:48

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。

实时动态

最近更新时间: 2023-08-20 15:16:49

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，页面跳转至“主机详情页”的相应子页面；单击事件动态右侧查看详情，将跳转至相应事件处理页面。

资产管理

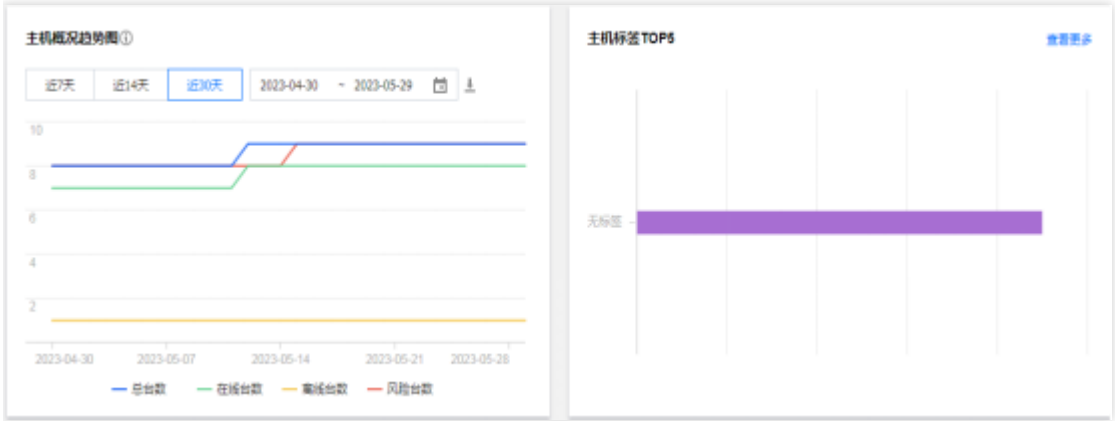
概览

最近更新时间: 2023-08-21 10:46:04

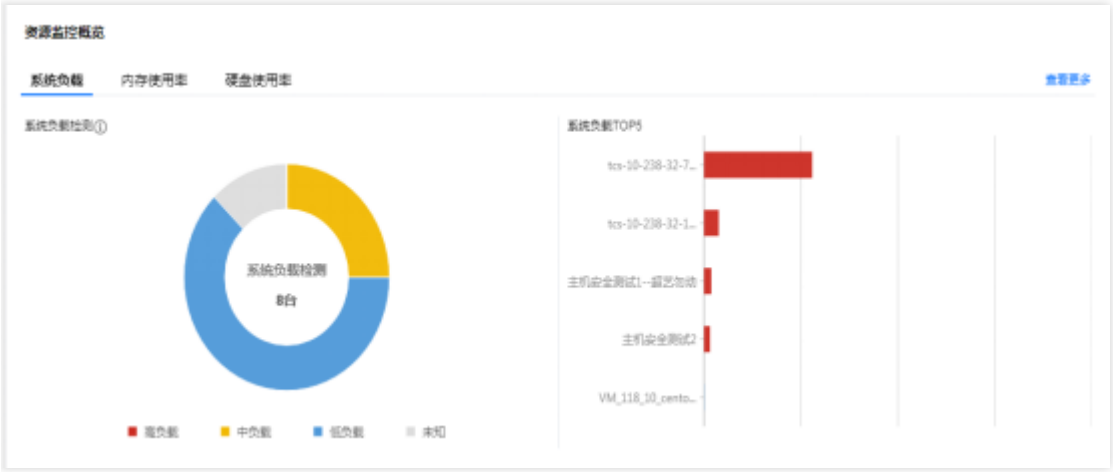
资产概览是从资产维度对主机及15项关键资产指纹数据进行统计盘点、可视化呈现，便于用户了解主机资产情况。

- 登录主机安全控制台，在左侧导航栏，选择资产中管理> 资产概览，可见以下资产统计信息：资产概况面板，可查看全部资产及各项资产指纹的统计情况。

- 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 TOP5，可查看所有主机中使用最多的前5个标签。



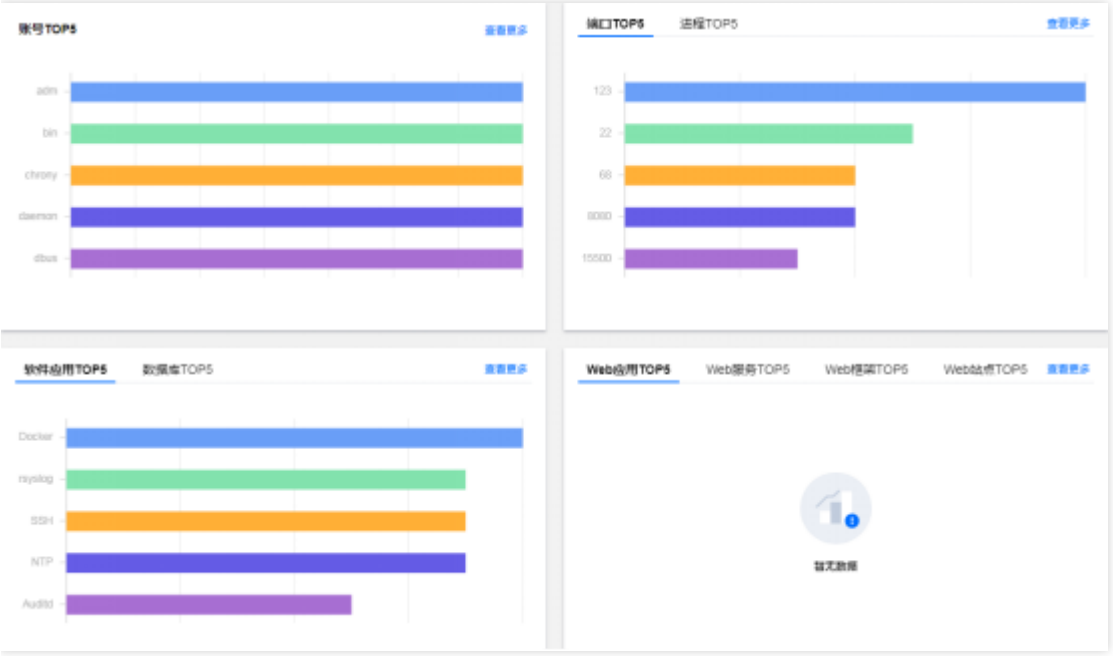
- 资源监控概览，可查看系统负载、内存使用率、硬盘使用率的分布情况及相应TOP5的负载。



说明：

系统负载，仅支持获取 Linux 系统的服务器系统负载，Windows 系统的暂认定为未知。

- 查看账号TOP5、端口TOP5、进程 OP5、软件应用TOP5、数据库TOP5、Web应用TOP5、Web服务TOP5、Web框架TOP5、Web站点TOP5。



主机列表

最近更新时间: 2023-08-21 16:12:52

主机列表

1.登录主机安全控制台，在左侧导航栏，选择资产管理> 主机列表

2.在主机列表页面，可以执行查询资产状态、安装主机安全客户端、升级版本等操作。

主机状态

在资产状态功能中，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，此处仅包含旗舰版与专业版主机数）、存在风险的主机数量、未防护的主机数量和即将到期的主机数量。

- 安装主机安全客户端

升级版本

单击升级版本将跳转至 购买页，您可根据业务需要对主机安全进行选购。

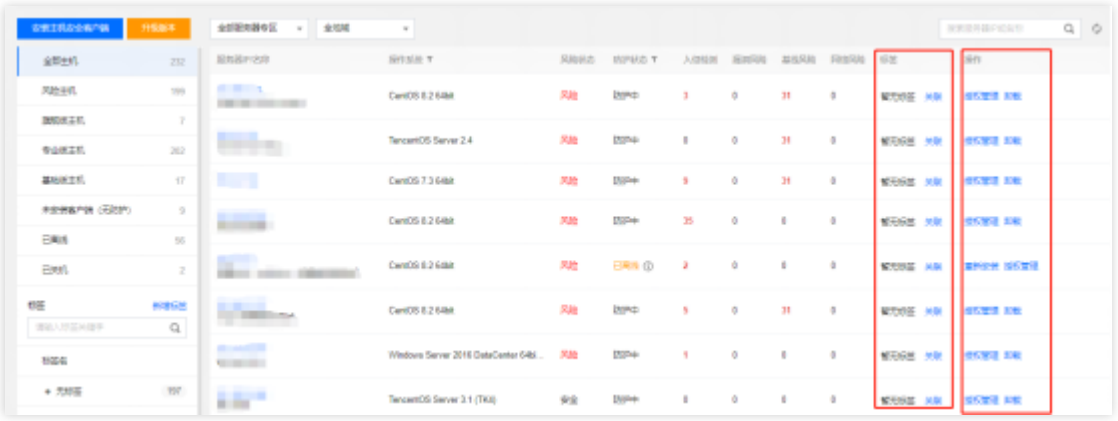
筛选导出

支持筛选服务器专区（云服务器专区、、裸金属、underlay）、地域、主机状态（全部主机、风险主机、旗舰版主机、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。

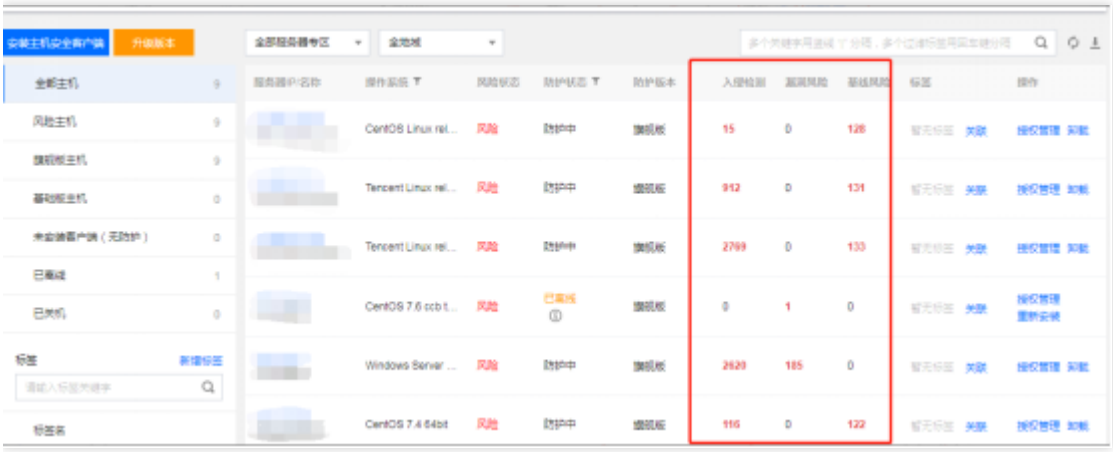
列表操作

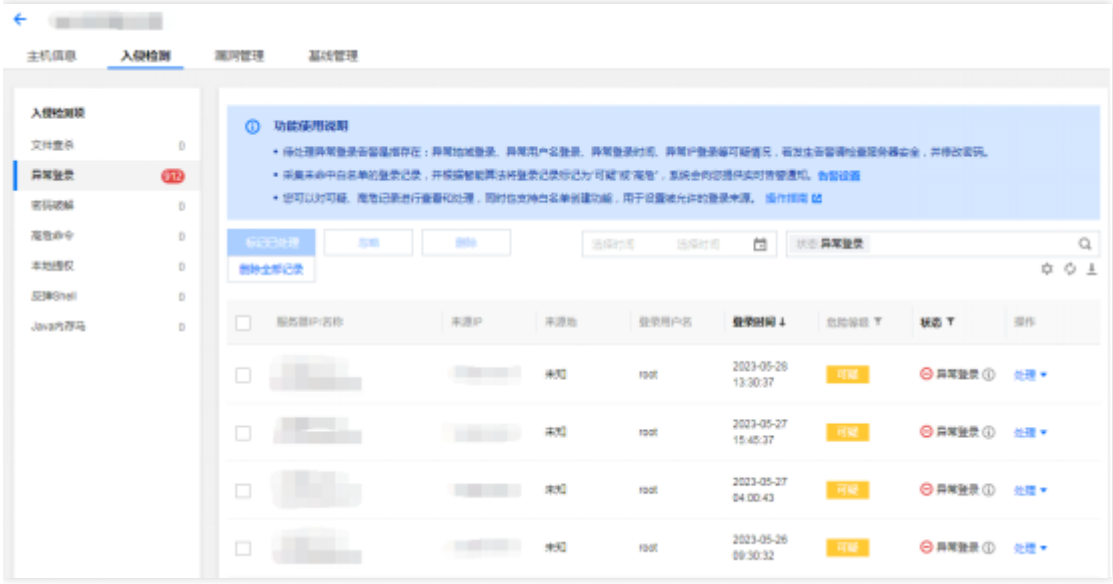
支持设置标签、关联标签。

支持重装/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，进行版本授权换绑、解绑等操作。



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。





资产指纹

最近更新时间: 2023-08-21 11:28:16

1.登录主机安全控制台，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。

入侵检测
文件查杀

最近更新时间: 2023-08-21 11:28:16

登录龙卫士安全控制台，在左侧导航栏选择【入侵检测】>【文件查杀】，即可查看当前受保护的服务器木马文件检测情况，恶意文件处理方式：

1、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。

2、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，可以通过状态菜单下拉筛选信任文件，对信任文件进行管理。

3、删除

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。如下图所示：

异常登录

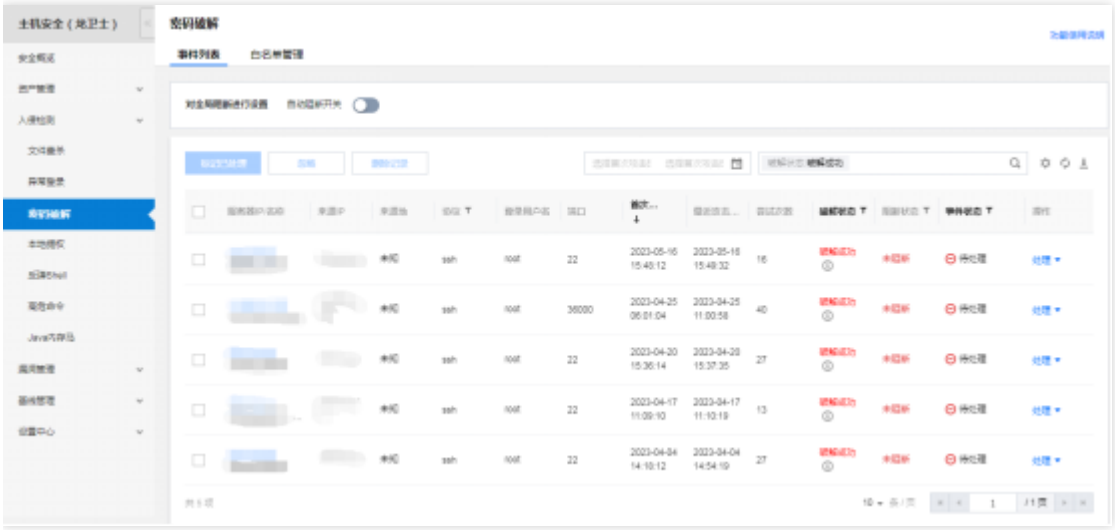
最近更新时间: 2023-08-21 11:28:08

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”。

密码破解

最近更新时间: 2023-08-21 11:28:08

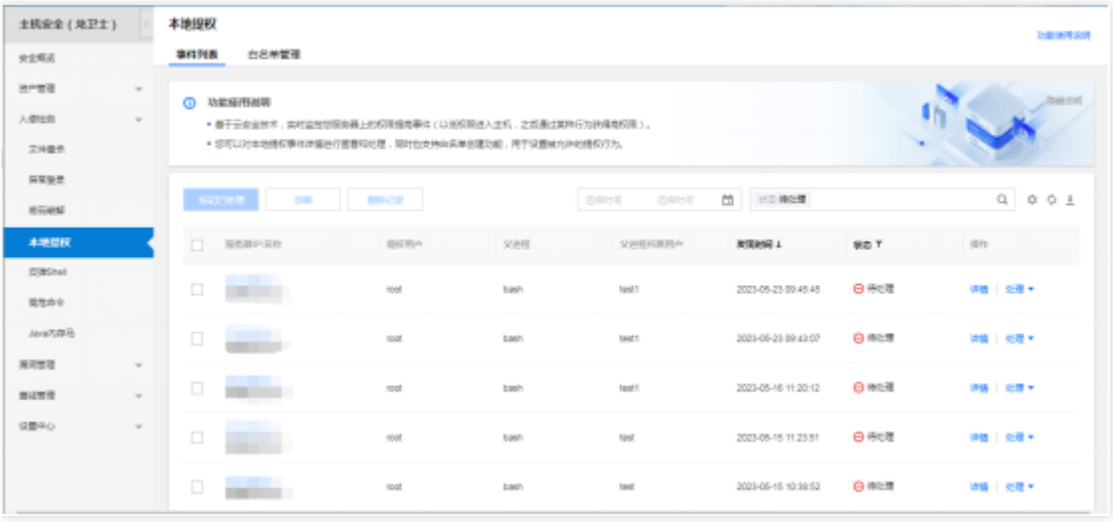
主机安全的密码破解基于云网络安全防御和主机入侵检测能力，为主机提供密码暴力破解行为实时监控，实现自动阻断防御功能。点击密码破解可查看密码破解事件，在操作栏可进行加白名单、删除等操作，白名单管理可新增白名单。



本地提权

最近更新时间: 2023-08-21 11:28:08

点击本地提权可查看本地提权事件，点击服务器IP可查看主机详情。点击操作详情可进行提权事件的查看，也可进行加白以及删除操作，白名单管理可添加新的白名单。



反弹Shell

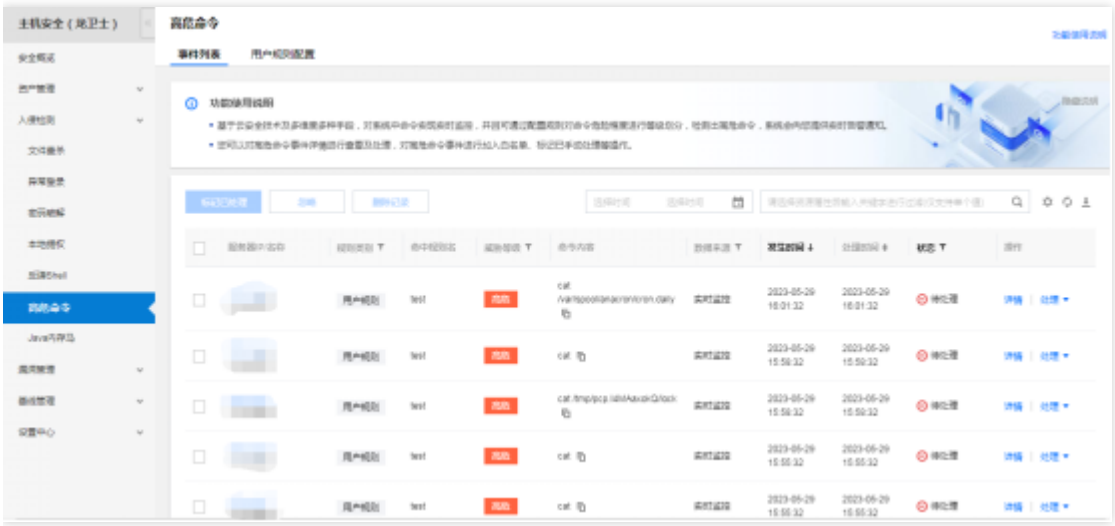
最近更新时间: 2023-08-21 11:28:08

反弹shell可查看产生的反弹shell事件，搜索框可根据进程名及服务器Ip进行查询，点击详情可查看反弹shell事件详情，包含连接进程信息、父进程信息等。

高危命令

最近更新时间: 2023-08-21 11:28:08

高危命令可查看主机上产生的高危命令事件，搜索框可根据IP查看产生的高危命令事件，可点击详情进行查看也可进行加白、删除操作。用户规则配置，用户可根据自身需求设置高危命令规则。



Java内存马

最近更新时间: 2023-08-21 16:15:57

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。

漏洞管理

背景信息

最近更新时间: 2023-08-21 11:28:08

建行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。

操作指南

最近更新时间: 2023-08-21 11:28:08

漏洞防御

漏洞攻击事件列表

基线管理

背景信息

最近更新时间: 2021-09-02 17:05:28

建行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，提供建行云默认基线策略，有助于您更好的管理服务器中的基线安全。

操作指南

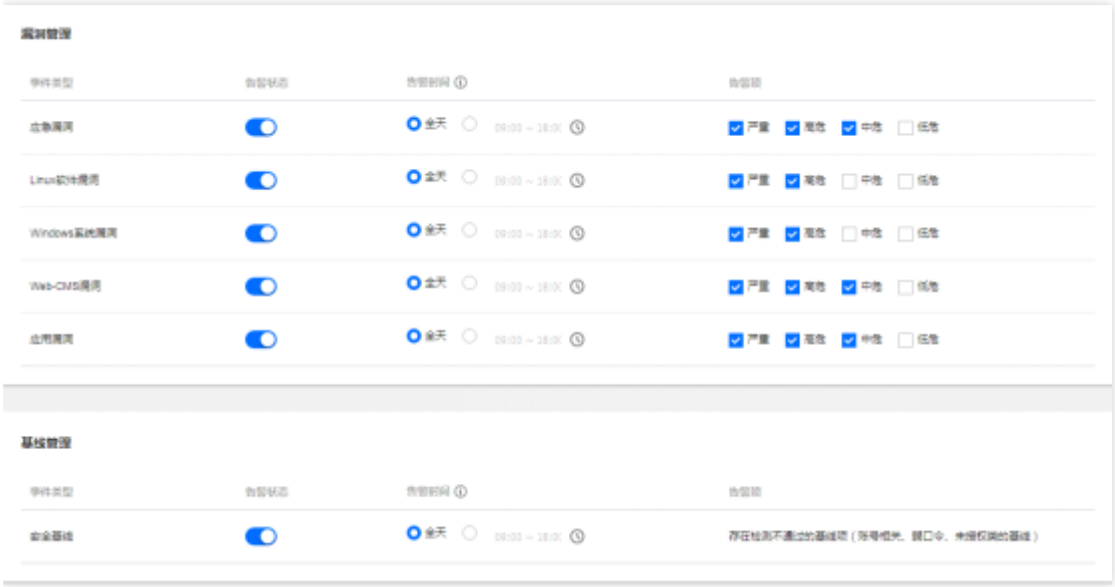
最近更新时间: 2023-08-21 11:28:07

1、登录主机安全控制台，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。

高级防御
设置中心
告警设置

最近更新时间: 2023-08-21 16:17:37

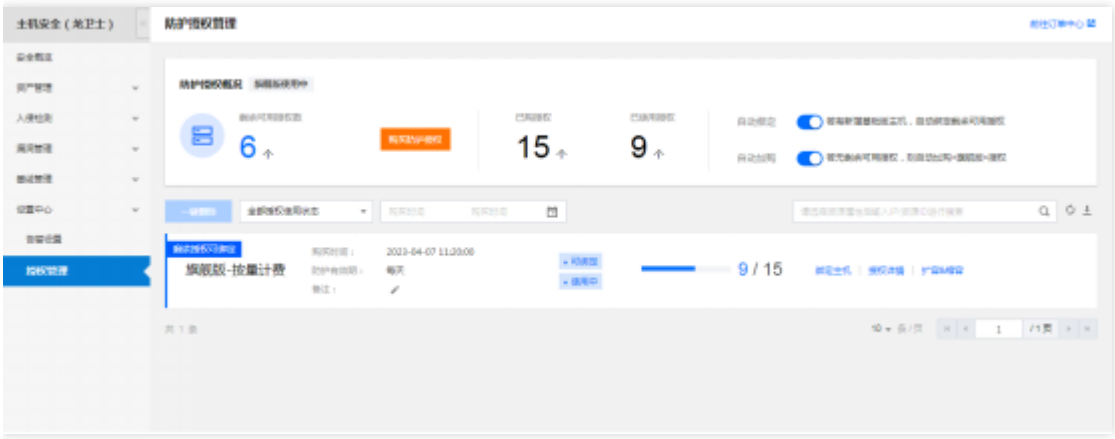
告警设置可进行防护软件离线、发现木马文件、发现异地登录行为、被密码破解成功等告警事件的开启关闭设置。当开启时若产生对应告警事件可以通过短信的方式发送对应的告警信息。



授权管理

最近更新时间: 2023-08-21 11:27:53

查看是否开通旗舰版。



快速入门
入门准备

最近更新时间: 2023-08-21 11:27:53

龙卫士可在建行云创建服务器安装时一同安装。
若需单独进行安装，可以登录龙卫士安全控制台，在左侧导航栏中，选择【资产管理】>【主机列表】安装主机安全客户端。

龙卫士安装
Windows云服务器环境

最近更新时间: 2023-08-21 11:27:53

目前支持的版本：

Windows server 2012

Windows server 2008 R2

Windows server 2003 (limited support)

Windows server 2016

Linux云服务器环境

最近更新时间: 2023-08-21 11:27:53

目前支持的版本：

CentOS: 6, 7, 8(64 bit)

Ubuntu: 9.10 – 20.10(64 bit)

Debian: 6, 7, 8, 9, 10, 11(64 bit)

RHEL: 6, 7(64 bit)

常见问题

最近更新时间: 2023-08-21 16:27:15

1、安装时遇到防火墙拦截要如何处理?

建议防火墙策略放通主机安全后台服务器访问地址：

VPC网络域名：s.yd.yun.ccb.com、l.yd.yun.ccb.com、u.yd.yun.ccb.com

依据区域进行替换：yun/yun002/yun003/yun004/yun005/yunbj01

VPC网络 IP：169.254.0.55

端口：5574、80、9080（公网还需放过443端口）

2、若不使用默认 DNS，要如何设置?

若您不使用默认DNS，则需要将s.yd.yun.ccb.com、l.yd.yun.ccb.com、u.yd.yun.ccb.com 的所有解析转发至默认DNS。

依据区域进行替换：yun/yun002/yun003/yun004/yun005/yunbj01

故障处理

Linux 入侵类问题排查思路

最近更新时间: 2023-08-21 16:54:23

检查隐藏帐户及弱口令

1、检查服务器系统及应用帐户是否存在弱口令：

检查说明：检查管理员帐户、数据库帐户、MySQL 帐户、tomcat 帐户、网站后台管理员帐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帐户记录，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帐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帐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/etc/passwd文件，看是否有非授权帐户登录：

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帐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。

检查恶意进程及非法端口

1、运行netstat －antp查看下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，删除下对应的文件即可。

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。

检查恶意程序和可疑启动项

1、使用chkconfig --list和cat /etc/rc.local命令查看下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。

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，请您限制应用程序帐户对文件系统的写权限，同时尽量使用非 root 帐户运行。 检查说明：使用非 root 帐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。
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，用户可以根据建行云已发布安全通告指导通过 apt-get/yum 等方式进行直接升级修复。
风险性：高。

被入侵后的安全优化建议

1、尽量使用 SSH 密钥进行登录，减少暴力破解的风险。
2、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（lamagoodboy）
3、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
```

4、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。

5、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。 6、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。

7、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。

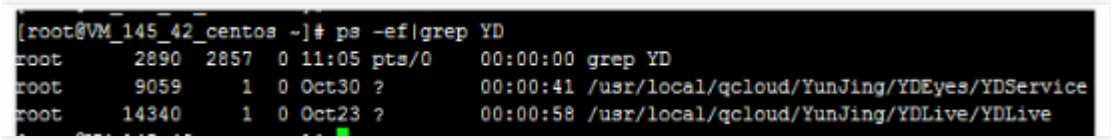
除了您的 home，root 目录外，您还应当备份 /etc 和可用于取证的 /var/log 目录。 8、确保所有主机Agent在线，在发生攻击后，可以了解自身风险情况。

Linux客户端离线排查

最近更新时间: 2023-08-21 16:56:18

1、请查询主机安全进程是否存在。输入：ps -ef|grep YD。

2、正常状态下，主机安全存在两个进程，如下图所示：

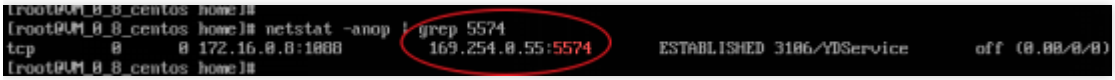


3、如果进程不存在，可能存在以下情况：

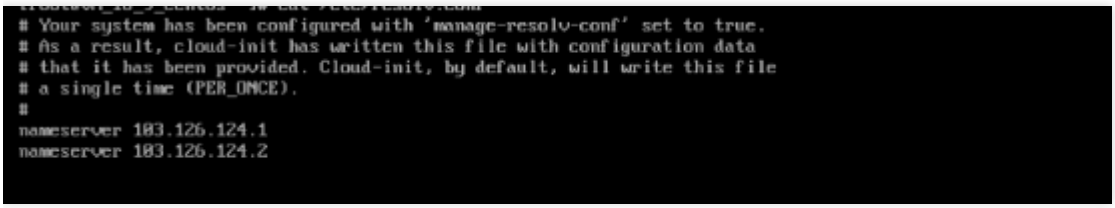
服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

4、排查方法：

（1）通过命令netstat -anop | grep 5574查看监听端口是否正常：



（2）通过ping命令对域名s.yd.yun.ccb.com、l.yd.yun.ccb.com以及u.yd.yun.ccb.com进行ping如果不通可以修改/etc/resolv.conf手动添加域名解析服务，需要添加的域名为：



（3）可查看客户端日志，存放路径：/usr/local/qcloud/YunJing/log。

（4）可执行命令：/usr/local/qcloud/YunJing/YDEyes/YDService &手动运行客户端。

Windows入侵类排查思路

最近更新时间: 2023-08-21 16:49:46

检查账户和弱口令

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。
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号，如有管理员群组的（Administrators）里的新增账户，如有，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用户，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）：
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
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。
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。
再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users。 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。

检查恶意进程和端口

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：
登录服务器，选择【开始】>【运行】。
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。
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。

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：
登录服务器，选择【开始】>【所有程序】>【启动】。
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。
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。
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：检查计算机与网络上的其它计算机之间的会话或计划任务。
检查方法：
登录服务器，选择【开始】>【运行】。
输入 cmd，然后输入 netstat –ano，检查计算机与网络上的其它计算机之间的会话，并确认是否为正常连接。输入 schtasks，检查计算机中的计划任务，并确认是否为正常的计划任务。
风险性：中。

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、开通建行云 Web 应用防火墙防护，查看 Web 应用防护攻击日志。

如何恢复网站或系统

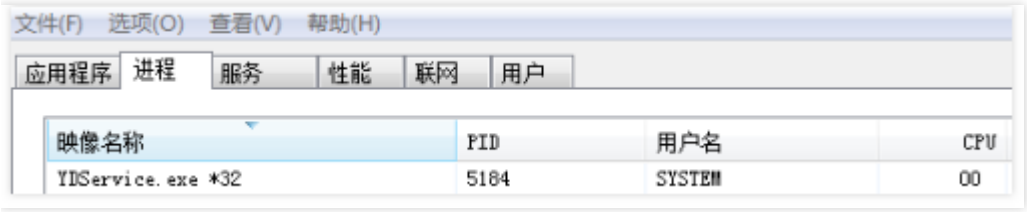
1、系统确认被入侵后，往往系统文件会被更改和替换，此时系统已经变得不可信，最好的方法就是重新安装系统，同时给新系统安装所有补丁。
2、改变所有系统账号的密码为 复杂密码（至少与入侵前不一致）。
3、修改默认远程桌面端口，操作如下：
选择【开始】>【运行】，然后输入 regedit。
打开注册表，进入如下路径：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
KEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp
修改下右侧的 PortNamber 值。
4、配置建行云安全组防火墙只允许 指定 IP 才能访问远程桌面端口。
5、定期备份重要业务数据和文件。
6、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。
7、安装建行云主机安全 Agent 和防病毒软件进行定期体检和扫描。

Windows客户端离线排查

最近更新时间: 2023-08-21 16:49:46

1、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。



2、如果进程不存在，可能存在以下情况：

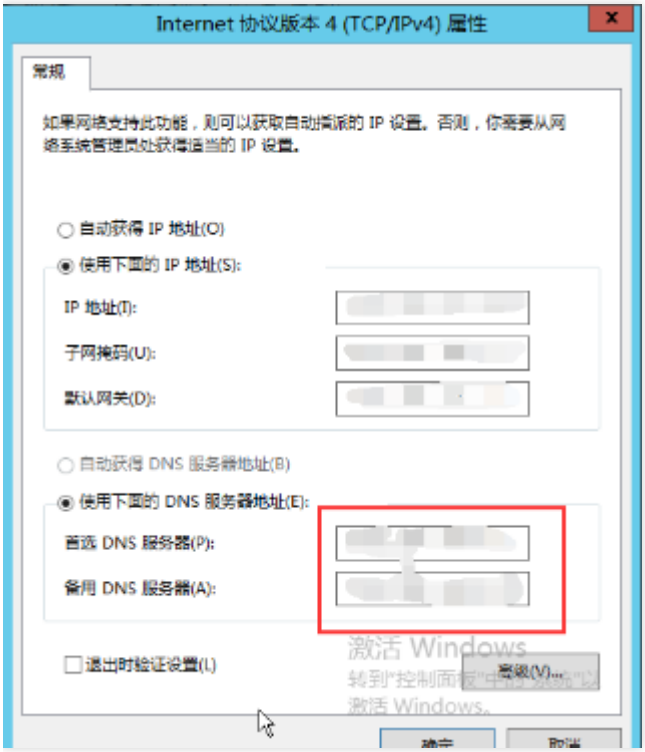
服务器未安装主机安全或者客户端已被卸载，请根据快速入门安装指引，进行客户端安装。 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

3、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。

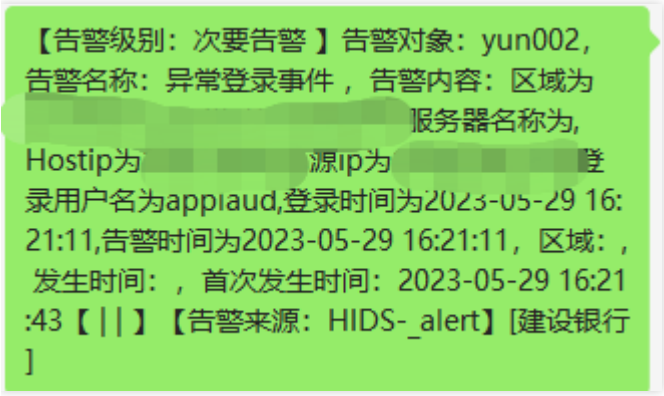
4、若出现类似下图的情况表示无法解析ip地址的情况，可以通过修改DNS的方式



异常登录的消息提醒

最近更新时间: 2023-08-21 16:49:46

用户接收到建行云发送的服务器被异常登录的消息提醒，如下以短信消息为例：



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入侵累排查思路对服务器进行常规排查。

常见问题
功能相关

最近更新时间: 2023-08-21 16:52:42

病毒库及漏洞库更新周期是多久?

病毒库：每周一次。

漏洞库：每周一次。

主机安全扫描频率是多少?

主机安全专业版：可自定义周期。

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、邮件的方式进行告警通知，具体方式您可以在 消息中心 进行设置。

入侵相关
入侵常见问题

最近更新时间: 2021-09-02 17:13:09

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，详情请参见 创建快照。

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。Windows 远程端口修改可以参见 3389服务器远程端口修改怎么操作 ， Linux 远程端口修改可参见 修改 SSH 端口+禁止 ROOT 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。
- 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。

如何做好云服务器防范措施?

建议 升级主机安全专业版 并处理中危及以上的安全事件。

木马类问题

最近更新时间: 2021-09-02 17:13:08

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 进行设置。

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安全团队，由安全团队快速鉴定。

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。
- 更多操作，请参见 木马文件操作处理。

异常登录类问题

最近更新时间: 2023-08-21 11:27:53

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告警项“高危异常”或“可疑异常”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

最近更新时间: 2023-08-21 11:27:53

1.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。
- 主机安全已上线暴力破解阻断功能，可进行有效拦截。

  2、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，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

最近更新时间: 2021-09-02 17:17:57

云服务器的防护状态显示离线要如何解决?

云服务器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。