主机安全

常见问题

腾讯云

文档目录

常见问题
购买相关

最近更新时间：2023-11-29 19:09:52

如何购买主机安全专业版与旗舰版？

可以进入 主机安全购买页 进行升级，详情请参见 购买指南 。

如何关闭主机安全专业防护或旗舰防护服务？

进入 授权管理页面 ，查看授权详情，可对已绑定授权的主机进行如下操作：

- 专业版-按量计费：您可执行解绑或者关闭专业版操作。解绑：每台主机每月仅有一次解绑机会；关闭专业版：关闭后授权数将-1（若仅有1个授权的情况，关闭专业版后则直接销毁该授权订单）。

> **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，已购旧按量计费订单仍可正常使用、扩容。
> - 若销毁相关按量计费旧订单，则将无法在旧订单上以按量计费模式扩容。

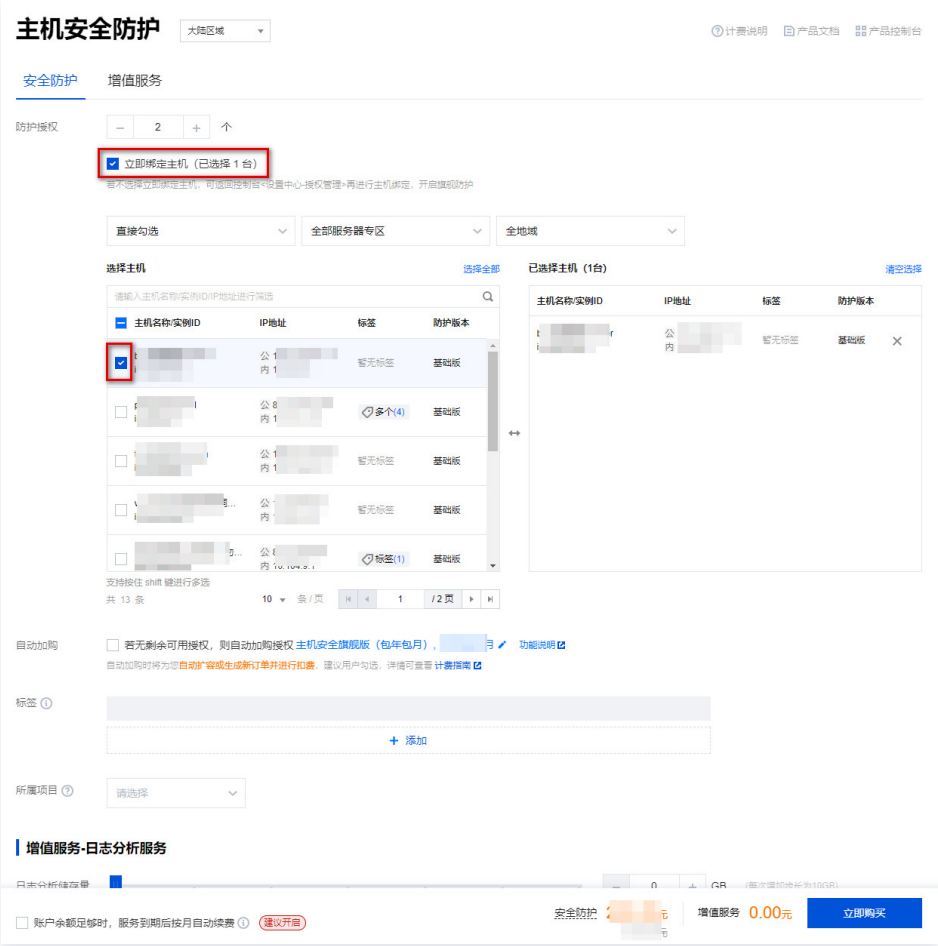
- 专业版-包年包月和旗舰版-包年包月：您可执行解绑操作。解绑：每台主机每月仅有一次解绑机会。

> **注意**
> - 云服务器到期或手动销毁后，主机安全专业版/旗舰版防护授权将自动解绑，空闲出来的授权可以去绑定其他主机。
> - 关闭主机安全专业防护与旗舰防护服务后，将不再提供对该主机的高危漏洞监控预警服务。
> - 主机安全是否扣费以实际购买的授权数为准，与授权是否绑定了主机、主机是否开机无关。

购买安全防护授权，会自动绑定主机吗？

根据实际情况，分为如下三种类型：

- 若用户在购买防护授权时，选择了绑定主机，购买授权后会自动绑定主机。



- 若用户在购买防护授权时，没有选择绑定主机，购买后须前往 授权管理页面 进行绑定。
- 若用户开启了自动绑定开关，在有剩余授权的情况下，会自动为客户的主机执行绑定操作。

新购云服务器，为何会自动生成主机安全专业防护的子订单？

若在主机安全控制台的 授权管理 中，打开自动升级防护的开关，新增加的云服务器都会自动升级为专业防护版，订单中会自动生成购买主机安全专业防护的子订单。

腾讯云账号实名认证出现问题要如何处理?

若在使用主机安全的过程中，遇到腾讯云账号相关问题，详情请参见 账号相关文档 。

主机安全产品是否与其他安全产品冲突?

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

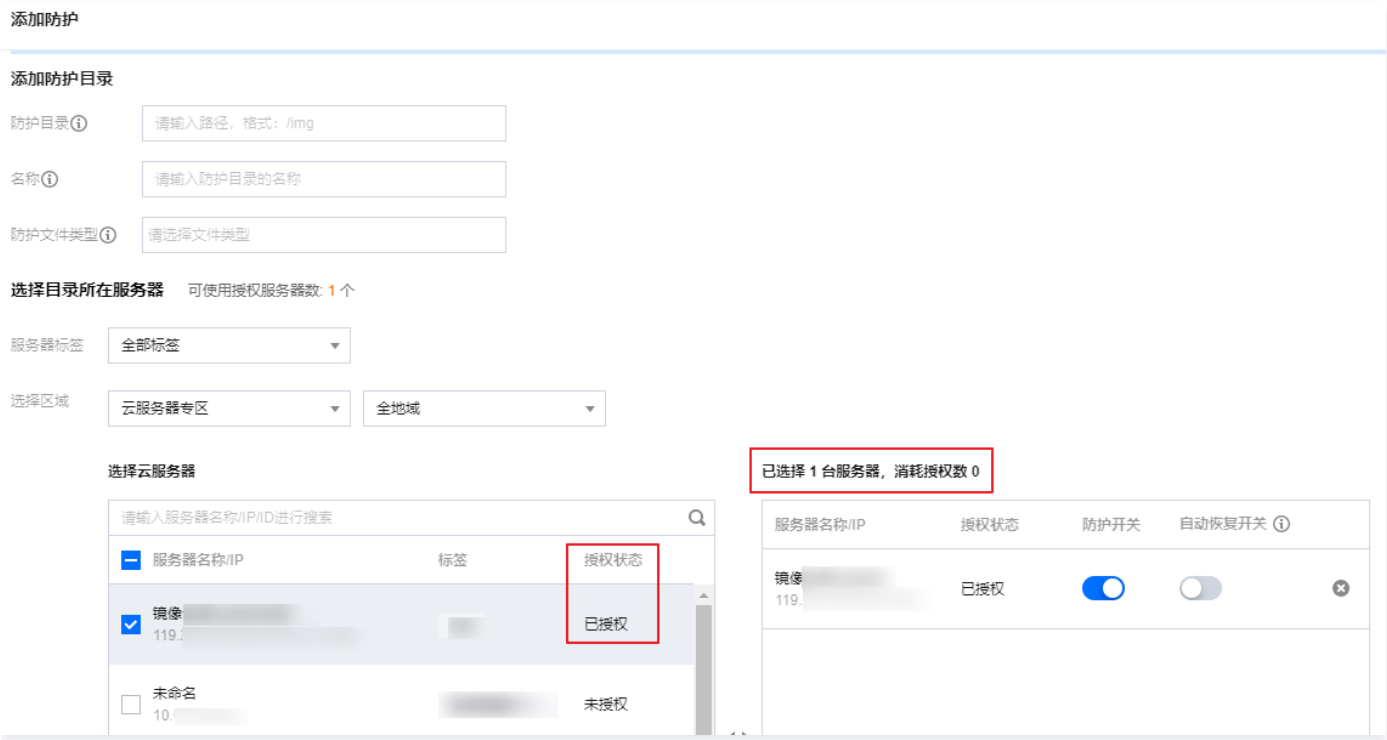
如何卸载腾讯云服务器主机安全客户端?

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**，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。

添加新的防护目录是否会消耗网页防篡改防护授权?

授权是以机器维度进行计算，即2台机器消耗2个授权。支持用户1台机器配置多个防护目录，总文件数限制为10000个。

在 网页防篡改 的添加防护目录页面，选择目录所在服务器时，可在服务器右侧查看授权状态，若为已授权服务器，不消耗授权数，选择未授权状态的服务器，则会提示消耗授权。



功能相关

最近更新时间：2023-09-25 09:28:33

病毒库及漏洞库更新周期是多久？

病毒库：每天00:00更新。
漏洞库：不定时更新。

为什么 Jar 包类的漏洞多次扫描时，每次检测结果可能不一致？

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

主机安全扫描频率是多少？

- 主机安全基础版：提供一次性检测。
- 主机安全专业版：可自定义周期。
- 主机安全旗舰版：可自定义周期。

如何对木马文件进行处理？

在 文件查杀 页面，可对木马文件进行如下处理：

- 删除：单击 复制木马文件路径，定位木马并手动删除该文件。

- 信任：您可执行信任操作，后续主机安全将不再对该机器的该文件进行检测。
- 隔离：当前尚不支持拦截木马，仅支持事中或事后检测并告警，但可对该文件执行隔离操作，防止该文件再次被启动。

概览页安全评分机制是怎样的？

概览页安全评分机制，请参见 安全概览 文档。

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**。

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。

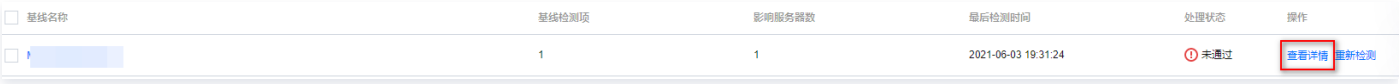
更多信息请参见 快照概述 及 创建快照 文档。

安全基线在产品设置过后，多久可以生效？

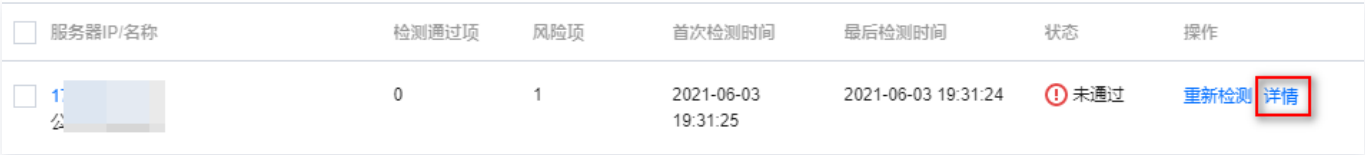
安全基线在产品设置后，即时生效。

主机安全基线检测“未通过”怎么处理？

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



2. 在详情页面，选择所需服务器 IP，单击**详情**，进入检测详情页面。



3. 在检测详情页面，将鼠标放置ⓘ处，即可查看该基线的对应处理建议。

主机安全发现漏洞木马等攻击是否会进行通知？

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

入侵相关

最近更新时间：2023-09-25 09:28:34

以下视频将为您介绍保护主机安全的意义、防范措施及解决方案等常见问题解析：
观看视频

- **入侵常见问题**
  - 云服务器被入侵有哪些危害?
  - 如何降低云服务器被入侵概率?
  - 云服务器被入侵后要如何防护?
  - 如何做好云服务器防范措施?
- **木马类问题**
  - 主机安全发现漏洞木马等攻击是否会进行通知?
  - 未能成功检测出木马（漏报）如何解决?
  - 如何处理木马及病毒文件?
- **异常登录类问题**
  - 云服务器显示登录异常怎么解决?
  - 如何处理异常登录告警?
  - 正常登录行为被误报为异常登录，要如何消除误报?
  - 是否可以关闭异常登录检测?
- **密码泄露类问题**
  - 云服务器被暴力破解如何处理?
  - 提示密码被暴力破解成功之后该如何解决?
- **防护状态离线类问题**
  - 云服务器的防护状态显示离线要如何解决?

云服务器被入侵有哪些危害?

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

如何降低云服务器被入侵概率?

- 及时修复高危漏洞及基线相关问题。
- 设置强密码，避免暴破攻击。
- 定期巡检账号、权限、端口并及时处理 主机安全控制台 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。
- 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。

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。

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 联系提交给腾讯云安全团队，由腾讯云安全团队快速鉴定。

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 。

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。

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。

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。

云服务器的防护状态显示离线要如何解决？

腾讯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 。