主机安全

常见问题

产品文档

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

常见问题

最近更新时间：2020-07-28 10:28:54

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：

点击查看视频

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。

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。

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：

- 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。

> 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。

如何处理木马文件？

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。

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。

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】>【登录审计】，在登录审计页面，单击【异常登录】，找到被定义为异常登录的登录日志，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。

> 注意：
> 目前"加白名单"功能，灰度发布中，发布系统随机筛选账号，仅被选中的账号可以使用该功能。

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。