

主机安全 常见问题 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。

常见问题

最近更新时间：2023-12-26 15:28:20

本文将为您介绍主机安全的常见问题。

购买相关

如何购买主机安全专业版与旗舰版？

请参见 [购买防护授权](#)。

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。

如何关闭主机安全专业版或旗舰版防护？

登录 [主机安全控制台](#)，在左侧导航栏中，选择 **授权管理**，搜索需要关闭专业版或旗舰版的主机，操作列中点击**解绑**操作，即可以关闭专业版或旗舰版服务。请参见 [授权管理](#)。

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 **主机列表**，找到您要卸载的主机，单击操作列**卸载**操作，即可卸载（约10分钟后会同步最新状态）。

功能相关

病毒库及漏洞库更新周期是多久？

病毒库：每日零点更新。

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。

在文件查杀功能中，文件的扫描频率是多少？

文件的扫描频率可由用户自行配置，请参见 [文件查杀](#)。

安全评分机制是怎样的？

请参见 [安全评分说明](#)。

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 [基线管理](#)，筛选未通过的检测项，单击[查看详情](#)，打开检测项详情弹窗。

<input type="checkbox"/> Baseline name	Check items	Affected servers	Last checked	Proc
<input type="checkbox"/> International Standard-CentOS 8 Safety baseline check Level1	86	1	2022-08-10 08:20:05	! f
<input type="checkbox"/> International Standard-CentOS 8 Safety baseline check Level2	118	1	2022-08-10 08:20:05	! f

2. 在检测项详情弹窗中，可见当前受影响的服务器，单击某服务器操作列的[详情](#)，打开检测结果弹窗。

<input type="checkbox"/> Server IP/Name	Passed items	Risk items	First checked	Last checked	Status
<input type="checkbox"/> 	51	35	2022-07-28 19:56:04	2022-08-10 08:20:05	! Fai

Total items: 1 10 / page

3. 在检测结果弹窗中，可查看基线修复建议。

Basic information

Baseline name: International Standard-CentOS 8 Safety baseline check Level1

Server Name: 国际4

Ensure that locks with failed password attempts have been configured

Description

Lock out the user after n consecutive failed login attempts.

Handling Suggestions (perform backup before handling)

Create or edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to contain the following:

Auth required pam_faillock.so preauth silent deny=5 unlock_time=900

Auth required pam_faillock.so authfail deny=5 unlock_time=900

	Status	Last checked
Ensure that locks with failed password attempts have been configured ⓘ	Failed	2022-08-10 08:00
Ensure that the default user shell timeout is 900s or less ⓘ	Failed	2022-08-10 08:00

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，您可在 [告警设置](#) 中设置。