

容器安全服务

常见问题



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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或 95716。

常见问题

最近更新时间：2025-04-14 14:33:02

如何防护容器安全？

容器安全服务能通过对镜像及镜像仓库提供一键检测，支持对漏洞、木马病毒及敏感信息等多维度安全扫描，帮助用户解决防护镜像安全。同时容器安全提供容器逃逸、进程黑白名单、文件访问控制等安全功能，保护容器运行时安全，并提供安全运营日志，帮助企业实现容器安全可视化。

如何监控容器的健康状况？

通过容器安全服务的安全运营功能，可帮助企业实现容器安全可视化，并提供安全策略等功能，提高企业安全运营质量及效率。

容器安全服务和其他安全产品是否冲突？

不冲突，传统的主机安全产品仅仅对 OS（操作系统）一层有效，无法深入识别容器内的安全问题。传统防火墙主要是为了南北向业务模型所设计，无法细粒度管理到容器环境如此海量和复杂的业务。

容器安全服务的漏洞库多久更新一次？

容器安全服务的漏洞库，每天更新一次，容器安全服务会实时获取官方发布的漏洞信息，在每天 00:00 将漏洞更新至漏洞库中。

容器安全服务支持线下及跨平台部署吗？

支持。详情请参见 [混合云安装指引](#)。

镜像与容器之间有什么关系？

- 镜像是一个包含程序运行必要依赖的环境和代码的只读文件，镜像是容器运行的基础。容器在启动或者创建时，依赖于镜像。不同的镜像可以构造出不同的容器，同一个镜像，我们也可以通过配置不同参数来构造出不同的容器。
- 容器是用镜像创建的运行实例。每个容器都可以被启动、开始、停止及删除，同时容器之间相互隔离，保证应用运行期间的安全。