容器安全服务

最佳实践

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或95716。

文档目录

最佳实践
容器安全等保测评解读

最近更新时间：2024-03-05 11:29:31

腾讯容器安全服务（Tencent Container Security Service, TCSS）产品符合等级保护2.0标准体系主要标准。在一般测评实施过程中能够帮助企业满足容器、镜像、主机、Kubernetes 资产层面的杀毒、主动入侵防御、定期漏洞扫描等方面要求。

根据《网络安全等级保护基本要求》（GB/T 22239-2019），腾讯容器安全服务满足第三级及以下安全要求：

序号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	安全区域边界—入侵防范	8.1.3.3 b）	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	容器安全可实时监控容器内的攻击行为，对恶意命令、横向渗透、反弹 Shell 等类型的异常进程进行实时告警及拦截。
2	安全区域边界—入侵防范	8.1.3.3 c）	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	容器安全可对容器、镜像、kubernetes 资产环境进行实时检测，对容器逃逸、集群漏洞、挖矿病毒等新型攻击行为和新型样本进行检测告警。
3	安全计算环境—安全审计	8.1.4.3 a）	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	容器安全支持对高危命令、高危操作进行审计，并支持对容器 bash 日志、容器启动日志和 k8s api 请求日志进行审计和记录（灰度中）。
4	安全计算环境—入侵防范	8.1.4.4 e）	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	容器安全支持检测镜像及集群中存在的安全漏洞，评估风险级别并提供修复建议。
5	安全计算环境—入侵防范	8.1.4.4 f）	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	容器安全支持检测容器内的入侵行为，主要包括容器逃逸，反弹 Shell，恶意文件，异常进程启动，文件篡改，高危系统调用等，提高告警及部分主动拦截能力。
6	安全计算环境—恶意代码防范	8.1.4.5	应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和	容器安全支持恶意文件查杀功能，实时监测容器内木马病毒并支持隔离恶意文件。

			病毒行为，并将其有效阻断。	

镜像漏洞扫描和漏洞管理

最近更新时间：2023-09-26 21:05:07

镜像安全是容器稳定运行的必备条件，当镜像存在安全风险时，风险镜像运行的容器随时可能遭受攻击、影响线上运行业务稳定性。因此在业务上线之前，需对即将应用到的镜像进行安全风险评估，确认无风险后再投入使用。
镜像安全风险主要涉及漏洞、木马和敏感信息泄漏，其中涉及到的镜像漏洞及漏洞管理问题尤其重要。在对镜像漏洞进行扫描和管理时，主要分为两个阶段进行管理：上线前、上线后。

- 上线前：镜像存储在仓库，客户需要对仓库镜像的安全性进行保障。
- 上线后：拉取到云服务器的镜像称为本地镜像，业务方需及时评估最新漏洞、应急漏洞等是否影响到运行业务的镜像。

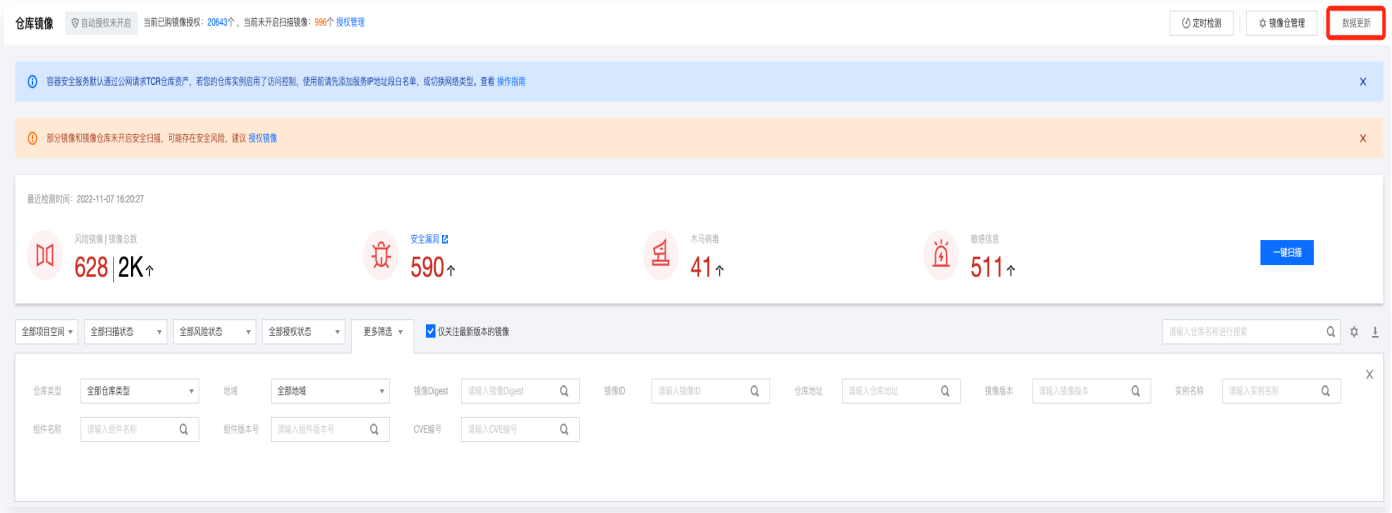
仓库存储阶段

镜像上线之前，客户将打包或下载好的镜像存储在仓库，入仓时需对新入仓的镜像进行整体安全评估，**如存在安全问题，建议修复后再入仓管理**。

拉取仓库镜像

腾讯云容器安全服务支持的仓库类型包括：腾讯云 TCR 镜像、腾讯云 CCR 镜像、Harbor 镜像。

- TCR 和 CCR 镜像默认自动拉取，当有新镜像入仓时，在 仓库镜像页面 ，单页右上角的**数据更新**即可更新资产。



- 当客户镜像存储在 Harbor 仓库时，客户**需手动接入仓库再拉取镜像资产**。在 仓库镜像页面 ，单页右上角的**镜像仓管理 > 新增镜像仓**，按要求验证仓库基本信息、连接地址等即可。

扫描与查看仓库镜像漏洞

在 仓库镜像页面，勾选新增的待评估镜像进行授权并扫描镜像。扫描完成，进入 漏洞管理页面 查看扫描出的漏洞。

如需查看全部漏洞，依次单击**系统漏洞**和**应用漏洞**，导出所有漏洞列表，在列表中查看影响仓库镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有EXP、POC、远程利用、在野利用等标签等。

- POC（Proof of Concept）：可通过一段描述或样例来证明漏洞确实存在。
- EXP（Exploit）：一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。
- 远程利用漏洞：指攻击者可以直接通过网络发起攻击并利用的软件漏洞。例如这类软件漏洞中的 RCE（远程代码执行）漏洞危害极大，攻击者能随心所欲地通过此漏洞对远端计算机进行远程控制，此类漏洞也是蠕虫病毒主要利用的漏洞。

- 本地利用漏洞：指攻击者必须在本机具有访问权限的前提下才能攻击并利用的软件漏洞。比较典型的是没有网络服务功能的本地软件漏洞，以及本地权限提升漏洞。例如本地提权漏洞能让普通用户获得最高管理员权限甚至系统内核的权限。
- 在野利用：该类漏洞存在在野利用或腾讯云上存在在野攻击（数据来源：we-detect 和 cisa）。

按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击，在列表中查看影响仓库镜像的漏洞，对存在应急漏洞的仓库镜像进行修复。

按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击，选择**仅导出筛选结果**，在列表中查看影响仓库镜像的漏洞，对存在这些标签的仓库镜像进行修复。

除了上述标签，客户在筛选仓库镜像漏洞时，也可利用“仅展示影响最新版本的镜像”、“威胁等级”、“CVSS”评分等条件进行综合筛选。

本地应用阶段

镜像安全风险问题在仓库存储阶段得到监控和修复后，在本地应用阶段则仅需关注新增漏洞的问题。本地镜像如存在严重的漏洞问题，可能直接影响线上业务。

授权与扫描本地镜像

容器安全服务会在每天的资产自动更新时，默认更新云服务器上存在的镜像，无需客户手动拉取。客户如需关注重点业务镜像的安全风险，可按如下步骤操作：

步骤1：授权镜像

1. 在仓库镜像，单击页面上方的**授权管理**。

2. 在授权管理页面中，镜像范围筛选选择**仅关注关联容器数不为0的镜像**，并搜索所需内网 IP，配置相关参数，单击**确认授权**。

说明

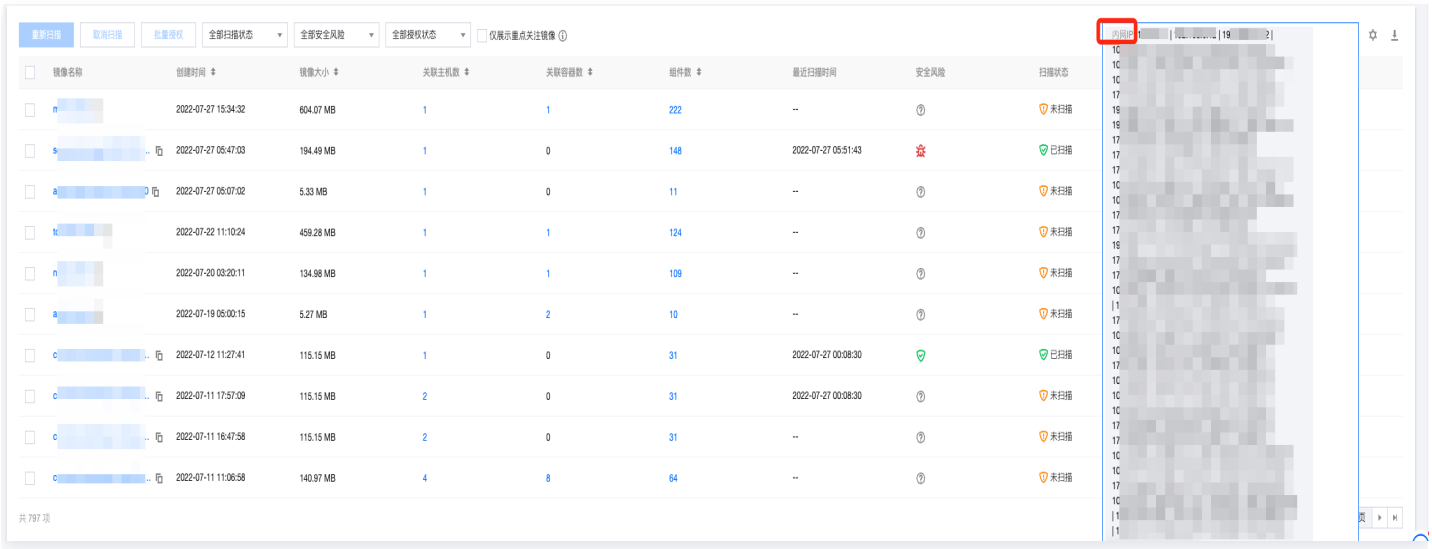
授权镜像时，可支持多内网 IP 进行检索，筛选关注节点、且运行有容器的镜像：多内网 IP 检索时，使用英文“|”对 IP 进行分隔，可使用文档替换工具，批量将列表中的换行符替换为“|”。目前前端限制

多 IP 检索的数量为200个，建议不要超过这个量，否则数据量大的时候容易检索超时。

步骤2：扫描镜像

在完成授权操作后，可保证授权的镜像仅为筛选的节点上的镜像，且镜像有容器在运行。在实际业务运行中，节点上镜像是否运行容器、是否新增，可通过在本地镜像列表进行筛选。

客户可在 本地镜像页面 ，通过内网多 IP 检索、以及选择已授权镜像的方式，选择需要扫描漏洞风险的本地镜像。



查看本地镜像漏洞

扫描漏洞任务完成后，进入 漏洞管理页面 查看扫描出的漏洞。

如需查看全部漏洞，依次单击**系统漏洞**和**应用漏洞**，导出所有漏洞列表，在列表中查看影响本地镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有EXP、POC、远程利用、在野利用等标签等。

按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击 ，在列表中查看影响本地镜像的漏洞，对存在应急漏洞的本地镜像进行修复。

按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击 ，选择**仅导出筛选结果**，在列表中查看影响本地镜像的漏洞，对存在这些标签的本地镜像进行修复。

除了上述标签，客户在筛选本地镜像漏洞时，如只需查看运行容器的本地镜像漏洞时，可打开“仅展示影响容器的漏洞”开关，或在导出的漏洞列表中筛选关联容器大于0的镜像。同时也可以利用“威胁等级”、“CVSS”评分等条件进行综合筛选。