容器安全服务

产品介绍

文档版本 02

发布日期 2021-07-09

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是容器安全服务

容器安全服务（Container Guard Service，CGS）能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

相关概念

- 镜像

  镜像（Image）是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数。镜像不包含任何动态数据，其内容在构建之后也不会被改变。

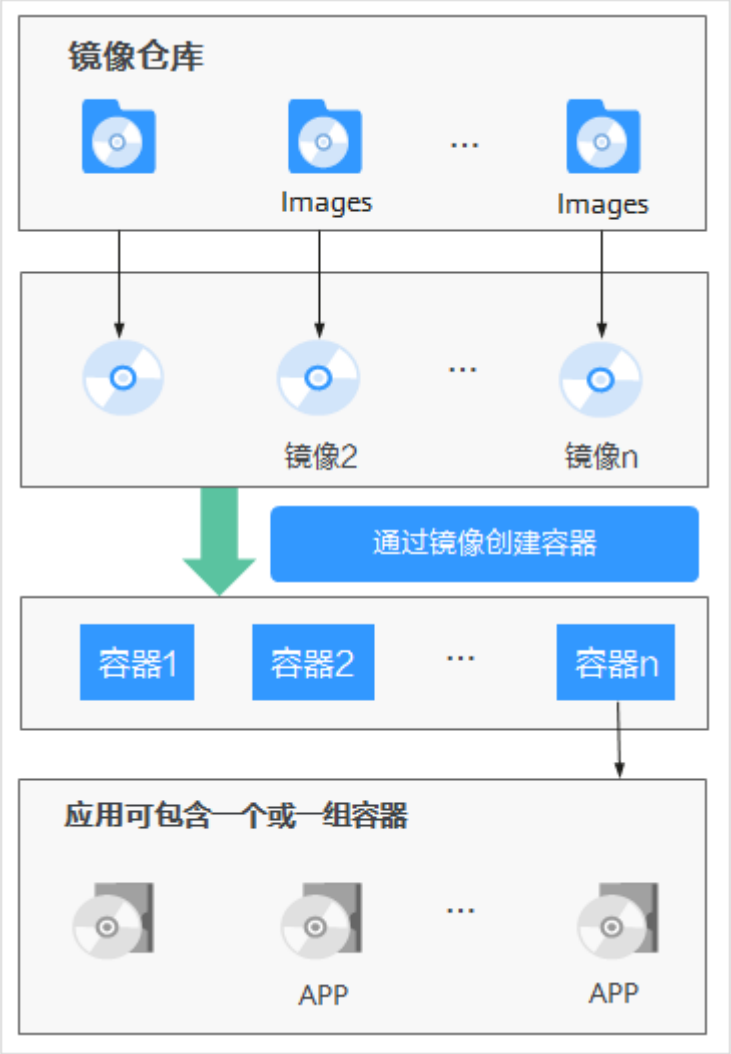
- 容器

  容器（Container）是镜像的实例，容器可以被创建、启动、停止、删除、暂停等。

镜像、容器和应用的关系说明如图1-1所示。

- 一个镜像可以启动多个容器。
- 应用可以包含一个或一组容器。

图 1-1 镜像、容器、应用的关系



部署架构

容器安全服务部署架构如**图1-2**所示，关键组件功能说明如**表1-1**所示。

图 1-2 容器安全服务部署架构

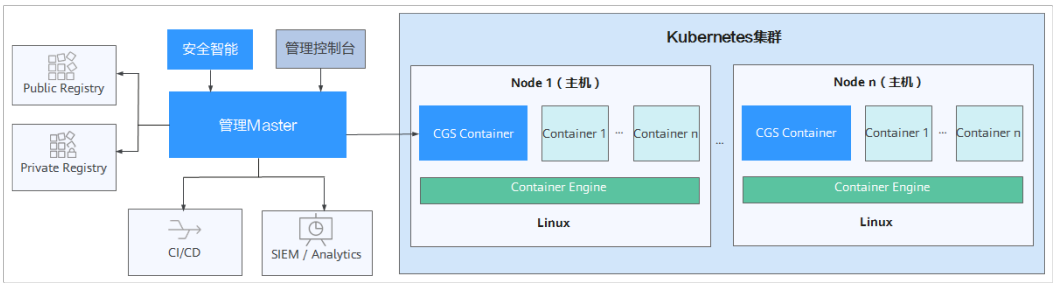


表 1-1 容器安全服务关键组件功能说明

组件	说明
CGS Container	CGS作为一个容器运行在每个容器节点（主机）上，负责节点上所有容器的镜像漏洞扫描，安全策略实施和异常事件收集。
管理Master	负责管理与维护CGS Container。
安全智能	安全智能是安全信息知识库，用于获取漏洞库、恶意程序库等更新，以及大数据AI训练模型等。
管理控制台	用户通过管理控制台使用容器安全服务。

2 功能特性

容器安全服务主要包含容器镜像安全、容器安全策略和容器运行时安全功能。

容器镜像安全

容器镜像安全功能可扫描镜像仓库与正在运行的容器镜像，发现镜像中的漏洞、恶意文件等并给出修复建议，帮助用户得到一个安全的镜像。

须知

CGS支持对基于Linux操作系统制作的容器镜像进行检测。

表 2-1 容器镜像安全

功能项	功能描述	检测周期
镜像安全扫描（私有镜像仓库）	支持对私有镜像仓库（SWR中的自有镜像）进行安全扫描，发现镜像的漏洞、不安全配置和恶意代码。 检测范围如下： ● 漏洞扫描 对SWR自有镜像进行已知CVE漏洞等安全扫描，帮助用户识别出存在的风险。 ● 恶意文件 检测和发现私有镜像是否存在Trojan、Worm、Virus病毒和Adware垃圾软件等类型的恶意文件。 ● 基线检查 检测私有镜像的配置合规项目，帮助用户识别不安全的配置项。 ● 软件信息 统计和展示私有镜像软件。 ● 文件信息 统计和展示私有镜像中不归属于软件列表的文件。	● 每日凌晨自动检测 ● 手动检测
镜像漏洞扫描（本地镜像）	对CCE容器中运行的镜像进行已知CVE漏洞等安全扫描，帮助用户识别出存在的风险。	实时检测
镜像漏洞扫描（官方镜像仓库）	定期对Docker官方镜像进行漏洞扫描。	-

容器安全策略

通过配置安全策略，帮助企业制定容器进程白名单和文件保护列表，确保容器以最小权限运行，从而提高系统和应用的安全性。

表 2-2 容器安全策略

功能项	功能描述	检测周期
进程白名单	将容器运行的进程设置为白名单，非白名单的进程启动将告警，有效阻止异常进程、提权攻击、违规操作等安全风险事件的发生。	实时检测
文件保护	容器中关键的应用目录（例如bin，lib，usr等系统目录）应该设置文件保护以防止黑客进行篡改和攻击。容器安全服务提供的文件保护功能，可以将这些目录设置为监控目录，有效预防文件篡改等安全风险事件的发生。	实时检测

容器运行时安全

容器运行时安全功能实时监控节点中容器运行状态，发现挖矿、勒索等恶意程序，发现违反容器安全策略的进程运行和文件修改，以及容器逃逸等行为并给出解决方案。

表 2-3 容器运行时安全

功能项	功能描述	检测周期
容器逃逸检测	从宿主机角度通过机器学习结合规则检测逃逸行为，简单精确，包括shocker攻击、进程提权、DirtyCow和文件暴力破解等。	实时检测
高危系统调用	检测容器内发起的可能引起安全风险的Linux系统调用。	实时检测
异常程序检测	检测违反安全策略的进程启动，以及挖矿、勒索、病毒木马等恶意程序。	实时检测
文件异常检测	检测违反安全策略的文件异常访问，安全运维人员可用于判断是否有黑客入侵并篡改敏感文件。	实时检测
容器环境检测	检测容器启动异常、容器配置异常等容器环境异常。	实时检测

3 产品优势

容器安全服务是一个用于检测容器镜像生命周期的安全服务，能帮助您高效管理容器与镜像的安全状态，降低容器与镜像面临的主要安全风险。

统一安全管理

统一管理CCE集群中所有节点上运行的容器与镜像的安全状态

丰富漏洞库

漏洞库包含丰富的100,000+漏洞，能够有效检测容器镜像漏洞

轻量 Agent

客户端以容器方式运行，系统资源的占用率极低，正常仅1%，峰值不超过5%

容器防逃逸

内置10大类，100小类容器逃逸行为规则，有效检测容器逃逸

满足等保安全合规

满足等保安全合规入侵防范条款和恶意代码防范条款

4 服务版本说明

容器安全服务提供了企业版版本。支持的功能如表4-1。详细的功能介绍，请参见功能特性。

- **企业版**提供更多种类的检测和监测功能，包含集群防护、镜像漏洞检测及修复、基线检查、恶意文件、容器运行时安全、安全配置等功能。用户购买容器安全防护配额后，即可使用企业版功能。

表 4-1 服务版本功能说明

服务功能	功能项	企业版 （√：支持；×：不支持）
集群防护	集群防护	√
本地镜像	本地镜像漏洞扫描	√
私有镜像	私有镜像漏洞扫描	√
	私有镜像恶意文件	√
	私有镜像软件信息	√
	私有镜像文件信息	√
	私有镜像基线检查	√
官方镜像	官方镜像漏洞扫描	√
运行时安全	逃逸检测	√
	高危系统调用	√
	异常程序检测	√
	文件异常检测	√
	容器环境检测	√
安全配置	进程白名单	√
	文件保护	√

5 应用场景

容器镜像安全

即使在Docker Hub下载的官方镜像中也常常包含了漏洞，而研发人员在使用大量开源框架时更加剧了镜像漏洞问题的出现。

容器镜像安全对镜像进行安全扫描，将镜像中存在的各种风险（镜像漏洞、帐号、恶意文件等）进行展示，提示用户及时修改，消除安全隐患。

容器运行时安全

通常容器的行为是固定不变的，容器安全服务帮助企业制定容器行为的白名单，确保容器以最小权限运行，有效阻止容器安全风险事件的发生。

满足等保安全合规

安全计算环境是等保安全合规的关键项，容器安全服务的核心功能够满足入侵防范与恶意代码防范等保合规条款，能够协助用户保护容器安全、系统安全。

6 计费说明

本章节主要介绍容器安全服务的计费说明，包括计费项、计费模式以及续费等。

计费项

容器安全服务根据您的CGS服务版本、防护节点数和购买时长计费。

表 6-1 计费项说明

计费项	计费说明
服务版本	提供企业版版本支持的功能和开启方式，请参见**服务版本说明**。
防护节点数	根据您购买的个数计费。
购买时长	• 企业版提供包年和包月的购买模式。 • 按需防护按实际使用时长计费。

计费模式

表 6-2 CGS 各服务版本计费方式

服务版本	支持的计费方式	说明	价格详情
企业版	包月/包年	• 相对于按需付费，包月/包年购买方式能提供更大的折扣且功能更全面，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。 • 在使用按需计费方式防护节点时，若您想使用包周期防护，可直接购买防护配额。购买成功后，系统将优先使用配额防护节点。	**产品价格详情**

续费

包年/包月方式购买的CGS防护配额到期后，如果没有按时续费，公有云平台会提供一定的保留期。

当您购买的CGS包周期防护配额到期后，CGS将自动转为按需计费，继续为您开启防护。

如需续费，请在管理控制台**续费管理**页面进行续费操作。详细操作请参考**续费管理**。

到期与欠费

- **服务到期**

  若您购买的防护配额到期后，如果没有按时续费，公有云平台会提供一定的保留期，详细信息请参见**保留期**。

- **欠费**

  若您购买的防护配额已欠费，可以查看欠费详情。为了容器安全和资产安全，建议您及时进行充值，详细操作请参考**欠费还款**。

FAQ

更多计费相关FAQ，请参见**CGS常见问题**。

7 CGS 权限管理

如果您需要对华为云上购买的容器安全服务（Container Guard Service，CGS）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有容器安全服务的使用权限，但是不希望员工拥有删除CGS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CGS，但是不允许删除CGS的权限，控制员工对CGS资源的使用范围。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CGS的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

CGS 权限

默认情况下，系统管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CGS部署时通过物理区域划分，为项目级服务，授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CGS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CGS服务，系统管理员能够控制IAM用

户仅能对某一类云服务器资源进行指定的管理操作。CGS支持的授权项请参见**CGS权限及授权项**。

表 7-1 CGS 系统角色

系统角色/策略名称	描述	类别	依赖关系
CGS Administrator	容器安全服务（CGS）系统管理员，拥有该服务下的所有权限。	系统角色	依赖Tenant Guest策略，在同项目中勾选依赖的策略。
CGS FullAccess	容器安全服务所有权限。	系统策略	无。
CGS ReadOnlyAccess	容器安全服务只读访问权限，拥有该权限的用户仅能查看容器安全服务。	系统策略	无。

相关链接

- **IAM产品介绍**
- **创建用户组、用户并授予CGS权限**
- **CGS权限及授权项**

8 访问与使用

8.1 如何访问

请使用管理控制台方式访问容器安全服务。如果用户已注册，可直接登录管理控制台，单击 ☰，选择“安全与合规 > 容器安全服务”访问。

8.2 如何使用

容器安全服务使用流程说明如表8-1所示。

表 8-1 容器安全服务使用流程说明

序号	子流程	说明
1	开启集群防护	开启防护后即可对集群中所有节点上的镜像和正在运行的容器进行实时检测。
2	（可选）设置安全策略	设置安全策略并将策略应用在镜像上，能有效预防容器运行时安全风险事件的发生。
3	查看漏洞	查看镜像上存在的漏洞，并判断是否需要“忽略”漏洞。
	查看容器运行时安全详情	查看容器运行时的异常行为。

9 与其他云服务的关系

与云容器引擎的关系

云容器引擎（Cloud Container Engine，CCE）基于云服务器快速构建高可靠的容器集群，将节点纳管到集群，容器安全服务通过在集群上安装容器安全Shield，为集群中所可用有节点上的容器应用提供防护。

说明

云容器引擎提供高可靠、高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。更多信息请参见《云容器引擎用户指南》。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录容器安全服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

表 9-1 云审计服务支持的 CGS 操作列表

操作名称	资源类型	事件名称
集群开启防护	cgs	openClusterProtect
集群关闭防护	cgs	closeClusterProtect
添加策略	cgs	addPolicy
编辑策略	cgs	modifyPolicy
删除策略	cgs	deletePolicy
镜像应用策略	cgs	imageApplyPolicy
忽略漏洞影响的所有镜像	cgs	ignoreVul
取消忽略漏洞影响的所有镜像	cgs	cancelIgnoreVul
忽略漏洞影响的镜像	cgs	ignoreImageVul
取消忽略漏洞影响的镜像	cgs	cancelIgnoreImageVul

操作名称	资源类型	事件名称
授权访问	cgs	registerCgsAgency
手动执行镜像扫描	cgs	scanPrivateImage
从SWR拉取镜像并执行扫描	cgs	syncSwrPrivateImage

与容器镜像服务的关系

容器镜像服务（Software Repository for Container，SWR）是一种支持容器镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务，更多信息请参见《容器镜像服务用户指南》。容器安全服务通过扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为容器安全服务提供了权限管理的功能。需要拥有CGS Administrator权限的用户才能使用CGS服务。如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

A 修订记录

发布日期	修改说明
2021-07-09	第二次正式发布。 服务入口刷新。
2021-01-26	第一次正式发布。