

天翼云·容器安全 用户使用指南

天翼云科技有限公司

目 录

1 产品介绍	4
1.1 什么是容器安全服务	4
1.2 功能特性	6
1.3 产品优势	8
1.4 服务版本差异	8
1.5 应用场景	9
1.6 用户权限	10
1.7 访问与使用	10
1.7.1 如何访问	10
1.7.2 如何使用	10
1.8 与其他云服务的关系	11
2 开通集群防护	13
2.1 服务授权	13
2.2 购买容器安全配额	14
2.3 开启集群防护	16
3 （可选）安全配置	18
4 镜像安全	21
4.1 管理本地镜像漏洞	21
4.2 管理私有镜像仓库漏洞	24
4.3 管理官方镜像仓库漏洞	26
4.4 查看恶意文件检测详情	28
4.5 查看基线检查详情	29
5 查看运行时安全详情	31
6 管理镜像信息	35
6.1 管理本地镜像	35
6.2 管理私有镜像仓库	38
6.3 管理官方镜像仓库	45
7 查看防护列表	49

8 关闭集群防护	51
9 审计	52
9.1 支持云审计的 CGS 操作	52
9.2 查看审计日志	53
10 权限管理	54
10.1 CGS 自定义策略	54
10.2 CGS 权限及授权项	55
11 常见问题	57
11.1 如何开启集群防护	57
11.2 如何关闭集群防护	58
11.3 容器集群节点的 Shield 状态离线如何处理？	59
11.4 无服务授权权限和创建委托失败的原因？	59
11.5 镜像、容器、应用的关系是什么？	59
A 修订记录	61

1 产品介绍

1.1 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。

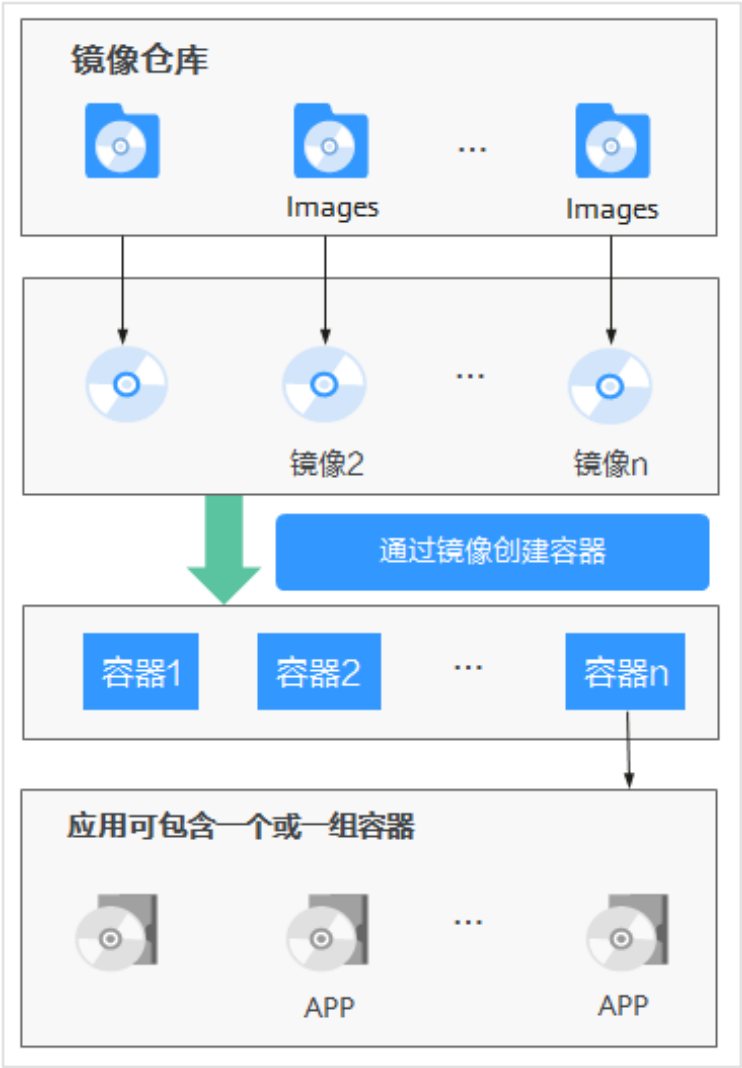
- 容器

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

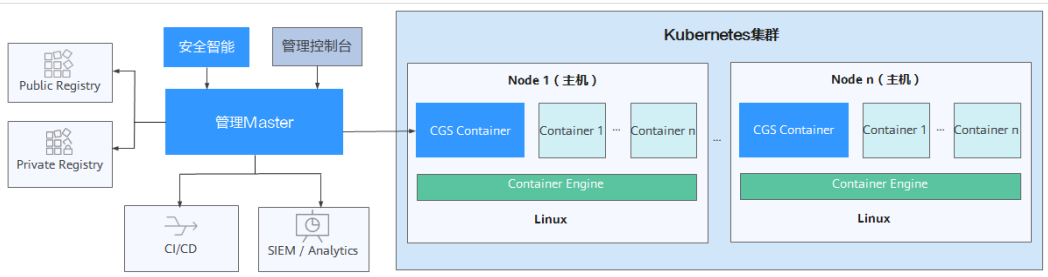


表1-1 容器安全服务关键组件功能说明

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。

1.2 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1-2 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	- 每日凌晨自动检测 - 手动检测

功能项	功能描述	检测周期
	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。	
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1-3 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1-4 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

功能项	功能描述	检测周期
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

1.3 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

满足等保合规

满足等保入侵防范条款和恶意代码防范条款

1.4 服务版本差异

容器安全服务提供了基础版和企业版两种服务版本。各版本支持的功能如表 1-5。详细的功能介绍，请参见 1.2 功能特性。

- **基础版**免费使用，用户登录 CGS 管理控制台同意服务授权后，即可免费体验基础版功能。

基础版仅提供检测私有镜像仓库漏洞和官方镜像仓库漏洞的漏洞详情和解决方案。

- **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。用户同意服务授权并在防护列表界面开启集群防护后，即可使用企业版功能。

表1-5 服版本功能说明

服务功能	功能项	基础版	企业版
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	√	√

1.5 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。

满足等保合规

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

1.6 用户权限

系统默认提供两种权限策略：系统策略和自定义策略。系统策略是 IAM 预置的策略，用户只能使用不能修改。若系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。

用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

1.7 访问与使用

1.7.1 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 > 容器安全服务”访问。

1.7.2 如何使用

容器安全服务使用流程说明如表 1-6 所示。

表1-6 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。

1.8 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1-7 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
授权访问	cgs	registeCgsAgency
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》。

2 开通集群防护

2.1 服务授权

容器安全服务支持云容器引擎服务（CCE）集群进行安全防护和对容器镜像服务（SWR）镜像仓库中的镜像进行安全扫描。

首次使用容器安全服务的用户需要进行服务授权。

约束与限制

- 容器安全服务不支持跨区域使用。待检测的镜像和待防护的集群必须和容器安全服务在同一区域。
- 已获取登录管理控制台的帐号和密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“服务授权”界面。

图2-1 服务授权



步骤3 单击“同意授权”，完成服务授权。

同意授权后，CGS将在统一身份认证服务为您创建名为 `cgs_admin_trust` 的委托，授权成功后，您就可以使用容器安全服务。

说明

若创建委托失败，则需要您登录到“统一身份认证服务”管理控制台，对委托进行删除或联系管理员增加限额。

----结束

2.2 购买容器安全配额

容器安全服务提供基础版、企业版以及按需防护三个版本供您选择。

- 用户同意服务授权后，即可免费体验**基础版**。
基础版仅提供检测私有镜像仓库漏洞、官方镜像仓库漏洞的漏洞详情和解决方案。
- 了解集群镜像安全和容器运行时安全，可选择**按需防护**。按需防护版本开启集群防护功能即可使用。
按需防护暂不提供恶意检测、基线检测、软件信息以及文件信息检测。
- 为及时和深入了解资产安全状况，确保云上资产安全，建议您选择**企业版**。
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。

容器安全服务按照防护的容器集群的节点个数收费，一个防护配额可以为一个集群节点提供防护。

本章节介绍购买企业版容器安全配额。

约束与限制

- 已同意 CGS 服务授权。
- 容器安全服务不支持跨区域使用。待检测的镜像和待防护的集群必须和容器安全服务在同一区域。
- 已获取管理控制台的登录帐号与密码。

操作步骤

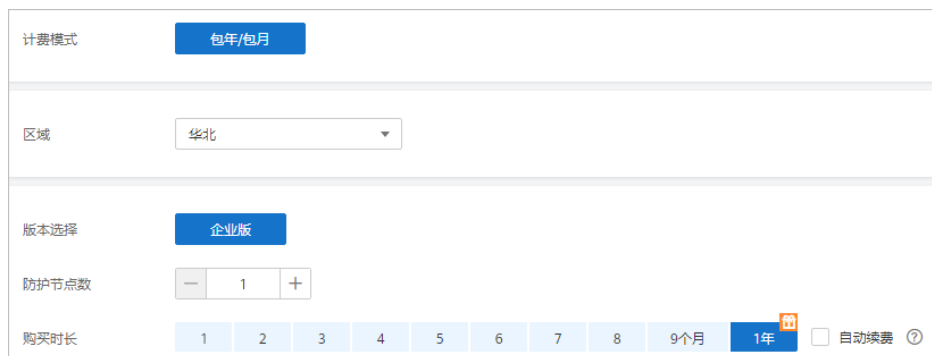
步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在界面右上角，单击“购买容器安全”。

步骤 4 进入“购买容器安全配额”界面，如图 2-2 所示，请根据表 2-1 进行配置。

图2-2 购买容器安全配额



该截图展示了“购买容器安全配额”的配置界面。界面包含以下配置项：

- 计费模式**：包含一个“包年/包月”的蓝色按钮。
- 区域**：显示为“华北”的下拉菜单。
- 版本选择**：包含一个“企业版”的蓝色按钮。
- 防护节点数**：包含减号、数字“1”和加号的输入框。
- 购买时长**：包含从1到8的按钮，以及“9个月”和“1年”的按钮。其中“1年”按钮右侧有一个“自动续费”复选框。

表2-1 参数说明

参数	参数说明
计费模式	支持按“包年/包月”的方式进行购买。
区域	在下拉框中选择区域。
版本选择	支持“企业版”。
防护节点数	购买容器安全的配额。 说明 ● 首次购买配额时，至少购买 10 个。 ● 一个防护配额可以为一个集群节点提供防护。
购买时长	支持 1 个月~1 年的时长。 说明 “自动续费”为可选项。勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤 5 确认参数配置无误后，在页面右下角，单击“立即购买”。

步骤 6 在详情界面确认订单无误后，单击“去支付”，完成购买操作。

如果订单填写有误，用户可以单击“上一页”，回到参数配置页面，修改配置信息后再继续购买。

----结束

2.3 开启集群防护

集群开启防护的同时系统将会自动为该集群安装容器安全 shield 插件。CGS shield 以 daemonset 插件方式安装，在集群的每个计算节点上启动容器用于监控本节点上其他容器的状态和事件。

集群开启防护后，如果集群新增了节点，容器安全服务将为新增的节点自动开启防护，并对新增的节点提供防护。

检测周期

容器安全服务每日凌晨进行全量检测。

若您在检测周期前开启防护，您需要等到次日凌晨检测后才能看到检测结果。

前提条件

- 已在云容器引擎成功创建集群。
- 集群的“集群防护状态”为“未开启”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在需要开启防护的集群所在行的“操作”列，单击“开启防护”。

说明

单击集群名称，进入“节点列表”界面，用户也可以在节点列表上方，单击“开启防护”。

步骤 4 在弹出的对话框中，确认“集群名称”和“集群可用节点数”并单击“是”，完成开启防护操作。

开启防护后，集群的“集群防护状态”为“已开启”，说明该集群中的所有可用节点都已开启防护。

图2-3 “开启防护”提示框



说明

- 集群开启防护后，如果集群新增了节点，容器安全服务将为新增的节点自动开启防护，并对新增的节点提供防护。
- 集群开启防护时，系统将自动为该集群安装容器安全插件。

----结束

3 （可选）安全配置

您可以通过自定义安全策略，配置进程白名单（添加容器内允许执行的程序文件路径）和文件保护（添加容器内只读的文件的完整路径），有效预防容器运行时安全风险事件的发生，提高系统和应用的安全性。

前提条件

已开启集群防护功能。

添加策略

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中选择“安全配置”进入“安全配置”界面，选择“策略配置”页签，单击“添加策略”，如图 3-1 所示。

图3-1 添加策略



步骤 4 在“添加策略”页面，配置策略内容，如图 3-2 所示，相关参数说如表 3-1 所示。

图3-2 “添加策略” 页面

添加策略

* 策略名称

test

请输入以字母开头，数字、中划线（-）组成，24个字符以内

进程白名单

请输入容器内允许执行的程序文件路径，以换行符相隔（不可重复），最多可以添加50个。

文件保护

请输入容器内只读的文件完整路径，以换行符相隔（不可重复），最多可以添加50个。

确定

取消

表3-1 参数说明

参数名称	说明
策略名称	策略的名称。
进程白名单	用户自定义。 指容器内允许执行的程序文件路径，设置白名单能有效阻止异常进程、提权攻击、违规操作等安全风险事件的发生。
文件保护	用户自定义。 指容器内需要只读保护的文件目录，设置文件保护列表能有效预防文件篡改等安全风险事件的发生。

步骤 5 单击“确定”，完成添加策略操作。

----结束

选择关联镜像

添加策略后，您可以选择策略关联的镜像，将添加的策略规则应用到关联的镜像。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击, 选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“安全配置”，进入“安全配置”界面，选择“策略配置”页签，在需要设置关联镜像的策略所在行的“操作”列，单击“关联镜像”，如图 3-3 所示。

图3-3 关联镜像



步骤 4 在“关联镜像”对话框中，选择需要应用策略的镜像，如图 3-4 所示。

图3-4 “关联镜像”对话框



步骤 5 勾选目标镜像选框，单击“确定”，完成选择关联镜像操作。

----结束

其他相关操作

- 查看策略
在策略列表中，单击策略名称，查看策略内容。
- 编辑策略
在需要修改的策略所在行的“操作”列，单击“编辑”，修改策略名称、进程名称和文件保护信息。
- 删除策略
在需要删除的策略所在行的“操作”列，单击“删除策略”，删除策略。

4 镜像安全

4.1 管理本地镜像漏洞

本章节指导用户查看本地镜像上存在的漏洞，并判断是否需要“忽略”漏洞。

检测方式

用户开启集群防护后，容器安全服务**自动执行**安全扫描。

前提条件

已开启集群防护功能。

查看漏洞列表

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面，选择“镜像漏洞 > 本地镜像漏洞”页签，如图 4-1 所示。

图4-1 进入本地镜像漏洞



步骤 4 查看漏洞概览。

- 漏洞占比：按“漏洞修复紧急度”进行统计的漏洞数量及占比。
- TOP5 风险的镜像：漏洞数 TOP5 的镜像及各紧急度的漏洞数量。

图4-2 本地镜像漏洞概览



说明

单击某风险镜像，即可查看该风险镜像的漏洞概况，包括漏洞名称、修复紧急度、处理状态、软件信息以及根据漏洞修复紧急度修复镜像或忽略漏洞。

步骤 5 查看漏洞列表，各参数说明如表 4-1 所示。

表4-1 参数说明

参数名称	说明	操作
漏洞名称	-	- 单击 ，查看漏洞详情，包括漏洞 ID、漏洞分值、漏洞披露时间和漏洞描述。 - 单击漏洞名称，查看该漏洞的基本信息以及受该漏洞影响的镜像列表，具体请参见步骤 6。
修复紧急度	提示您是否需要立刻处理该漏洞。	-
当前未处理镜像数（个）	显示受该漏洞影响的镜像是否全部处理。	-
历史受影响镜像数（个）	显示受该漏洞影响的镜像个数。	-
解决方案	针对该漏洞给出的解决方案。	单击“解决方案”列的链接，查看修复意见。

步骤 6 单击漏洞名称，查看该漏洞的基本信息及受该漏洞影响的镜像列表，如图 4-3 和图 4-4 所示。

图4-3 漏洞的基本信息（本地）

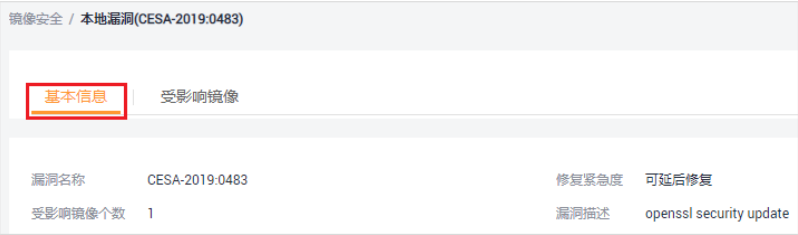


图4-4 受漏洞影响的镜像列表



----结束

忽略漏洞

针对已判断无风险或风险较小的漏洞，可以“忽略”该漏洞。忽略漏洞后，镜像将不再统计该漏洞，但漏洞列表中仍可见。

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面。
- 步骤 4 选择“镜像漏洞 > 本地镜像漏洞”页签。
- 步骤 5 忽略漏洞在所有镜像上的影响，或忽略漏洞在某一镜像上的影响，具体操作请参见表 4-2。

表4-2 忽略漏洞

忽略漏洞	操作步骤
忽略漏洞在所有镜像上的影响	- 在漏洞列表中，勾选需要忽略的漏洞，单击漏洞列表左上角的“忽略”。 - 在弹出的对话框中，单击“确定”，忽略选中的漏洞。
忽略漏洞在某一镜像上的影响	- 方式一： - 在漏洞列表中，单击漏洞名称，查看受该漏洞影响的镜像

忽略漏洞	操作步骤
	列表，在镜像所在行的操作列，单击“忽略”。 2. 在弹出的对话框中，单击“确定”，忽略该漏洞。 方式二： 1. 单击镜像名称，查看该镜像上存在的漏洞及处理情况，在漏洞所在行的操作列，单击“忽略”。 2. 在弹出的对话框中，单击“确定”，忽略该漏洞。

----结束

取消忽略漏洞

- 进入漏洞列表，选中已忽略的漏洞，单击漏洞列表左上角的“取消忽略”，撤销忽略漏洞的操作。
- 进入受漏洞影响的镜像列表，在镜像所在行的操作列，单击“取消忽略”，撤销忽略漏洞的操作。
- 进入镜像上存在的漏洞列表，在漏洞所在行的操作列，单击“取消忽略”，撤销忽略漏洞的操作。

4.2 管理私有镜像仓库漏洞

本章节指导用户查看私有镜像仓库存在的漏洞，并根据修复建议对漏洞进行修复。

前提条件

已同意 CGS 服务授权。

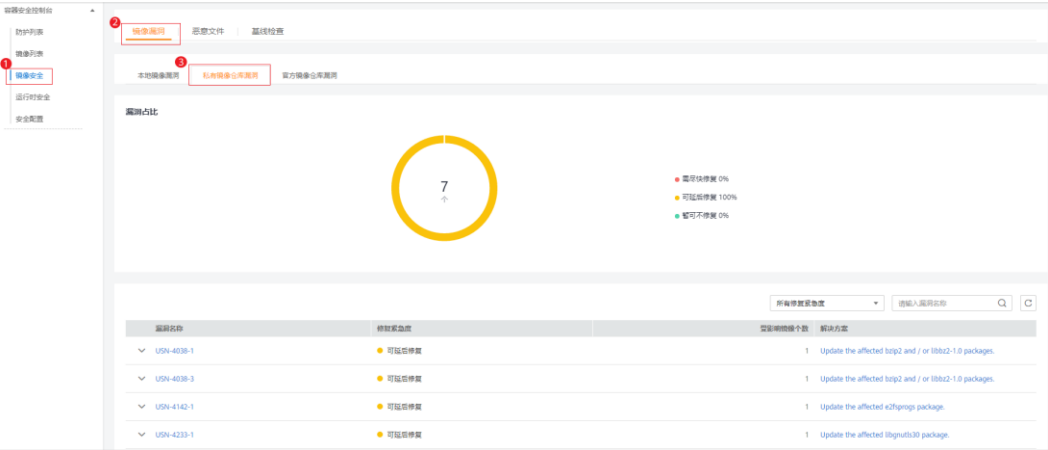
查看漏洞列表

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面，选择“镜像漏洞 > 私有镜像仓库漏洞”页签，如图 4-5 所示。

图4-5 进入私有镜像



- 步骤 4 查看漏洞占比。
- 按“漏洞修复紧急度”进行统计的漏洞数量及占比。
- 步骤 5 查看漏洞列表，各参数说明如表 4-3 所示。

表4-3 参数说明

参数名称	说明	操作
漏洞名称	-	- 单击，查看漏洞详情，包括漏洞 ID、漏洞分值、漏洞披露时间和漏洞描述。 - 单击漏洞名称，查看该漏洞的基本信息以及受该漏洞影响的镜像列表，具体请参见步骤 6。
修复紧急度	提示您是否需要立刻处理该漏洞。	-
受影响镜像个数	显示受该漏洞影响的镜像个数。	-
解决方案	针对该漏洞给出的解决方案。	单击“解决方案”列的链接，查看修复意见。

- 步骤 6 单击漏洞名称，查看该漏洞的基本信息及受该漏洞影响的镜像列表，如图 4-6 和图 4-7 所示。

图4-6 漏洞的基本信息（私有）

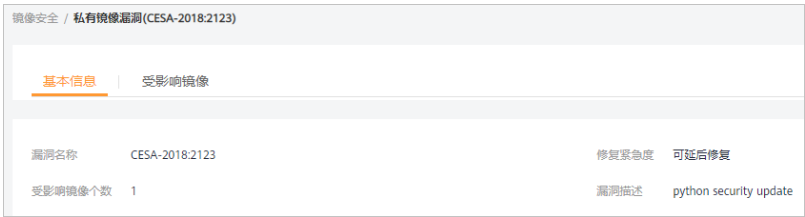
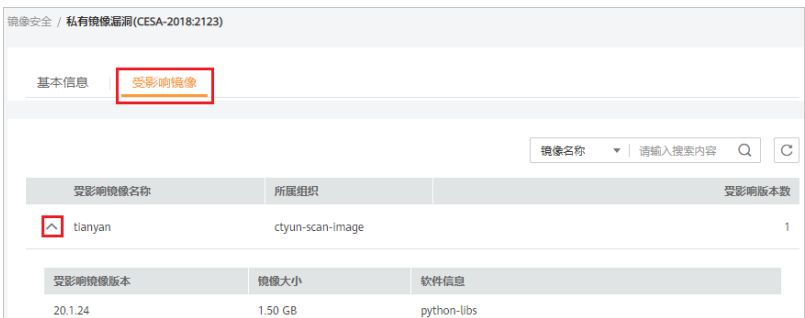


图4-7 受漏洞影响的镜像列表（私有）



----结束

4.3 管理官方镜像仓库漏洞

本章节指导用户查看官方镜像仓库存在的漏洞，并根据修复建议对漏洞进行修复。

前提条件

已同意 CGS 服务授权。

查看漏洞列表

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面，选择“镜像漏洞 > 官方镜像仓库漏洞”页签，如图 4-8 所示。

图4-8 进入官方镜像仓库漏洞



步骤 4 查看漏洞占比。按“漏洞修复紧急度”进行统计的漏洞数量及占比。

步骤 5 查看漏洞列表，各参数说明如表 4-4 所示。

表4-4 参数说明

参数名称	说明	操作
漏洞名称	-	- 单击 ，查看漏洞详情，包括漏洞 ID、漏洞分值、漏洞披露时间和漏洞描述。 - 单击漏洞名称，查看该漏洞的基本信息以及受该漏洞影响的镜像列表，具体请参见步骤 6。
修复紧急度	提示您是否需要立刻处理该漏洞。	-
受影响镜像个数	显示受该漏洞影响的镜像个数。	-
解决方案	针对该漏洞给出的解决方案。	单击“解决方案”列的链接，查看修复意见。

步骤 6 单击漏洞名称，查看该漏洞的基本信息及受该漏洞影响的镜像列表，如图 4-9 和图 4-10 所示。

图4-9 漏洞的基本信息（官方）



图4-10 受漏洞影响的镜像列表（官方）

基本信息		
受漏洞影响		
镜像名称 请输入搜索内容		
受影响镜像名称	所属组织	受影响版本数
 tianyan	ctyun-scan-image	1
受影响镜像版本	镜像大小	软件信息
20.1.24	1.50 GB	python-libs

----结束

4.4 查看恶意文件检测详情

容器安全服务能自动检测私有镜像仓库恶意文件，为您展示资产中存在的安全威胁，大幅降低您使用镜像的安全风险。

检测周期

容器安全服务**每日凌晨**自动执行一次全面的检测。

前提条件

已开启集群防护功能。

操作步骤

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面。
- 步骤 4 选择“恶意文件”页签，查看私有镜像仓库恶意文件详细信息，并根据检测结果删除恶意文件，重新制作镜像。
 - 恶意文件类型如：Trojan、Worm、Virus 病毒和 Adware 垃圾软件等类型。
 - 在“镜像版本”列，单击某个镜像版本号，可查看该镜像版本的漏洞报告详情。

图4-11 恶意文件

镜像漏洞

恶意文件

基线检查

建议不要使用携带恶意文件的镜像启动容器。请删除恶意文件后重新制作镜像。

请输入文件名称搜索

恶意文件名称	路径	描述	镜像类型	所属组织	镜像名称	镜像版本
aes	/root/	Miner	私有镜像	test	ubuntu_malware_test	1.0.0
aes2	/root/	Miner	私有镜像	test	ubuntu_malware_test	1.0.0

----结束

4.5 查看基线检查详情

基线检查功能自动检测您私有镜像仓库中存在的配置风险，针对所发现的问题为您提供加固建议，帮助您正确地处理镜像内的各种风险配置信息，降低入侵风险并满足安全合规要求。

检测周期

容器安全服务**每天凌晨**自动进行一次全面的检查。

前提条件

已开启集群防护功能。

操作步骤

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击, 选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在左侧导航树中，选择“镜像安全”，进入“镜像安全”界面。
- 步骤 4 选择“基线检查”页签，查看或根据风险等级搜索检测到的配置风险及其详细信息。
在基线检查列表右上方的下拉框中，您可选择“所有风险等级”或“High”或“Medium”或“Low”，查看镜像中存在的配置风险。

图4-12 查看基线检查详情

镜像漏洞 恶意文件 基线检查			
所有风险等级 ⌵ 🔄			
检测项	风险等级	受影响镜像个数	检测方式
✓ 确保系统中不存在账号名或UID相同的账号	High	0	检查系统中/etc/passwd文件，确保不存在账号名相同或者UID相同的账号。
✓ UID为0的非root账号检查	High	0	UID为0的账号具有root权限，只允许root账号的UID为0。
✓ 硬编码口令检查	High	0	检查系统中是否存在硬编码账号密码
✓ 确保系统中不存在相同密码哈希值的账号	High	0	检查系统中/etc/shadow文件，确保不存在密码哈希值相同的账号

步骤 5 单击检测项前的 ，查看该检测项的详情，查看检测项存在的问题和提供的加固建议，并根据加固建议修复有风险的配置信息，如图 4-13 所示。

图4-13 检测项详情

检测项	风险等级	受影响镜像个数	检测方式		
√ 确保配置了密码有效期	High	2	该设置确定在系统要求用户更改密码之前可以使用该密码的期限（以天为单位）。此策略使得攻击...		
镜像组织	镜像名称	镜像版本	检测完成时间	检测项存在的问题	加固建议
mytest	ubuntu_malware_test	1.0	2020-11-18 11:00:09 GMT+08:00	PASS_MAX_DAYS 99999.	设置配置文件/etc/login.defs的PASS_MAX_DAYS...
mytest	mysql-server	latest	2020-11-20 15:42:24 GMT+08:00	PASS_MAX_DAYS 99999.	设置配置文件/etc/login.defs的PASS_MAX_DAYS...

----结束

5 查看运行时安全详情

开启集群防护后，CGS shield 以 daemonset 插件方式安装在每个集群节点上，对容器集群节点中的容器运行状态进行监控，并对异常事件进行告警和提供解决方案。

运行时安全监测包括：逃逸检测、高危系统调用、异常进程检测、文件异常检测、容器环境检测。

检测周期

容器安全服务**实时监控**容器集群中运行的容器，用户可随时查看容器异常事件详情。

前提条件

集群的“集群防护状态”为“已开启”。

检测原理

表5-1 运行时安全漏洞检测原理说明

检测项	原理说明
逃逸检测	- 逃逸漏洞攻击 CGS 监控到容器内进程行为符合已知漏洞的行为特征时（例如：“脏牛”、“bruteforce”、“runc”、“shocker”等），触发逃逸漏洞攻击告警。 - 逃逸文件访问 CGS 监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，CGS 仍然会触发告警。
高危系统调用	Linux 系统调用是用户进程进入内核执行任务的请求通道。CGS 监控容器进程，如果发现进程使用了危险系统调用（例如：“open_by_handle_at”、“ptrace”、“setns”、“reboot”等），触发高危系统调用告警。

检测项	原理说明
异常进程检测	- 容器恶意程序 CGS 监控容器内启动的容器进程的行为特征和进程文件指纹，如果特征与已定义的恶意程序吻合则触发容器恶意程序告警。 - 容器异常进程 容器业务通常比较单一。如果用户能够确定容器内只会运行某些特定进程，可以在 CGS 控制台配置安全策略设置进程白名单并将策略关联容器镜像。 对于已关联的容器镜像启动的容器，CGS 只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。
文件异常检测	CGS 监控容器内已配置文件保护策略的容器镜像文件状态。如果发生文件修改事件则触发文件异常告警。
容器环境检测	CGS 监控新启动的容器，对容器启动配置选项进行检测，当发现容器权限过高存在风险时触发告警。容器环境检测触发的告警只是提醒容器启动风险，并不是发生实际攻击。如果黑客利用容器配置风险执行了真实攻击，仍然会触发 CGS 运行时监控的其他检测告警。 CGS 支持以下容器环境检测： - 禁止启动特权容器(privileged:true) 特权容器是指容器以最大权限启动，类似与操作系统的 root 权限，拥有最大能力。docker run 启动容器时携带 “- privileged=true” 参数，或者 kubernetes POD 配置中容器的 “securityContext” 配置了 “privileged:true”，此时容器会以特权容器方式启动。 CGS 告警内容中提示：“privileged:true”，表示该容器以特权容器模式启动。 - 需要限制容器能力集 (capabilities:[xxx]) Linux 系统将系统权限做了分类，通过授予特定的权限集合，能控制容器进程的操作范围，避免出现严重问题。容器启动时默认开启了一些常用能力，通过修改启动配置可以放开所有系统权限。 CGS 告警内容中提示：“capabilities:[xxx]”，表示该容器启动时拥有所有能力集过大，存在风险。 - 建议启用 seccomp (seccomp=unconfined) Seccomp(secure computing mode)是 Linux 的一种内核特性，用于限制进程能够调用的系统调用，减少内核的攻击面。如果容器启动时设置 “seccomp=unconfined”，将不会对容器内的系统调用执行限制。 CGS 告警内容中提示：“seccomp=unconfined”，表示该容器启动时没有启动 seccomp，存在风险。 说明 启用 seccomp 后，由于每次系统调用 Linux 内核都需要执行权限校验，如果容器业务场景会频繁使用系统调用，开启 seccomp 对性能会有一定影响。具

检测项	原理说明
	体影响建议在实际业务场景测试分析。 - 限制容器获取新的权限(no-new-privileges:false) 进程可以通过程序的 <code>suid</code> 位或者 <code>sgid</code> 位获取附加权限，通过 <code>sudo</code> 提权执行更高权限的操作。容器默认配置限制不允许进行权限提升。 如果容器启动时指定了 “ <code>- no-new-privileges=false</code> ”，则该容器拥有权限提升的能力。 CGS 告警内容中提示：“no-new-privileges:false”，表示该容器关闭了提权限制，存在风险。 - 危险目录映射(mounts:[...]) 容器启动时可以将宿主机目录映射到容器内，方便容器内业务直接读写宿主机上的资源。这是一种存在风险的使用方式，如果容器启动时映射了宿主机操作系统关键目录，容易造成从容器内破坏宿主机系统的事件。 CGS 监控到容器启动时 <code>mount</code> 了宿主机危险路径时触发告警，CGS 定义的宿主机危险目录包括：“/boot”，“/dev”，“/etc”，“/sys”，“/var/run”等。 CGS 告警内容中提示： “mounts:[{"source":"xxx","destination":"yyy"...}” ，表示该容器映射的文件路径存在风险。 说明 对于 docker 容器常用的需要访问的宿主文件如 “/etc/hosts”、“/etc/resolv.conf” 不会触发告警。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“运行时安全”，进入“运行时安全”界面。

步骤 4 选择不同页签（“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”），查看容器异常监控趋势图和异常事件列表。

图5-1 容器异常监控趋势图

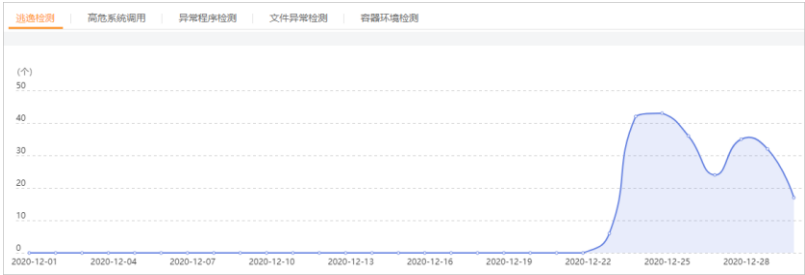


图5-2 容器异常事件列表

全部异常类型							
最近7天		容器实例名称		请输入关键字			
容器实例名称	容器名称	节点名称	集群名称	异常类型	异常描述	触发时间	解决方案
/k8s_container-0_he...	sha256b57e4fbbbe...	cmcc-test-07299-tw...	cmcc-test	逃逸漏洞攻击	Namespace of pid3...	2020-12-30 11:43:00...	杀掉了攻击进程，或者...
/k8s_container-0_he...	sha256b57e4fbbbe...	cmcc-test-07299-tw...	cmcc-test	逃逸漏洞攻击	Namespace of pid1...	2020-12-30 09:05:30...	杀掉了攻击进程，或者...

- 容器异常监控趋势图呈现“最近 1 个月”的异常监控信息。
- 异常事件列表您可以查看“最近 1 天”、“最近 3 天”、“最近 7 天”的异常情况，并根据解决方案处理异常事件。

----结束

6 管理镜像信息

6.1 管理本地镜像

本地镜像为用户 CCE 集群中使用并启动了容器的镜像，容器安全服务可对这些镜像执行安全扫描。本地镜像列表显示了镜像基本信息和安全状况。

本章节指导用户查看本地镜像基本信息、漏洞报告和管理关联策略。

前提条件

- 已同意 CGS 服务授权。
- 已开启集群防护。

查看本地镜像列表

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。

步骤 4 选择“本地镜像”页签。

表6-1 本地镜像列表参数说明

参数	说明	操作
镜像名称	镜像的名称。	单击镜像名称前的  ，可查看该镜像的版本列表。
镜像 ID	镜像的 ID。	-
扫描状态	镜像扫描的状态。	-
漏洞个数	镜像上存在的漏洞数量	-

参数	说明	操作
关联策略个数	镜像应用的策略数量。	-

----结束

查看本地镜像基本信息

步骤 1 登录管理控制台。

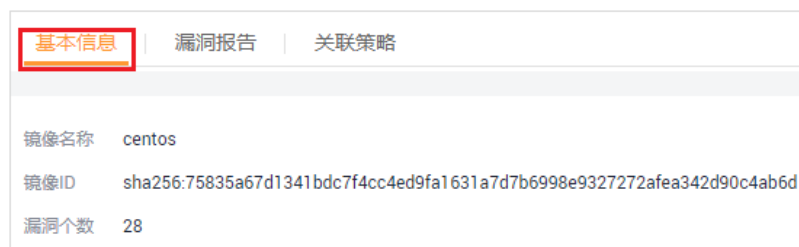
步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。

步骤 4 选择“本地镜像”页签，单击镜像名称，查看该镜像的基本信息。

步骤 5 该镜像版本的基本信息，如图 6-1 所示。

图6-1 本地镜像基本信息



----结束

查看本地镜像的漏洞

扫描完成后，可查看漏洞报告。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。

步骤 4 选择“本地镜像”页签，在需要查看漏洞报告的镜像所在行的“操作”列，单击“漏洞报告”。

步骤 5 在“漏洞报告”页签下查看扫描出的镜像漏洞。

您可执行以下操作：

- 查看漏洞概览：按“漏洞修复紧急度”进行统计的漏洞数量及占比。
您可以查看漏洞整体个数、需尽快修复、可延后修复和暂可不修复个数。
- 查看漏洞列表信息
您可以查看漏洞名称、修复紧急度、软件信息、漏洞位置以及解决方案。
- 搜索漏洞
您可在**漏洞列表**上方，通过筛选漏洞修复紧急度（需尽快修复、可延后修复、暂可不修复、所有修复紧急度），搜索漏洞名称、软件名称定位到相关的漏洞。

说明

漏洞名称和软件名称都支持模糊搜索。

- 查看漏洞基本信息和受漏洞影响的镜像
单击漏洞名称进入漏洞基本信息页面，查看漏洞更加详细的信息及受漏洞影响的镜像详细信息。

图6-2 漏洞报告



----结束

管理本地镜像的策略

您可以将添加的安全策略应用到本地镜像。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。

步骤 4 选择“本地镜像”页签，单击镜像名称，进入“基本信息”页面。

步骤 5 选择“关联策略”页签，单击“应用策略”，如图 6-3 所示。

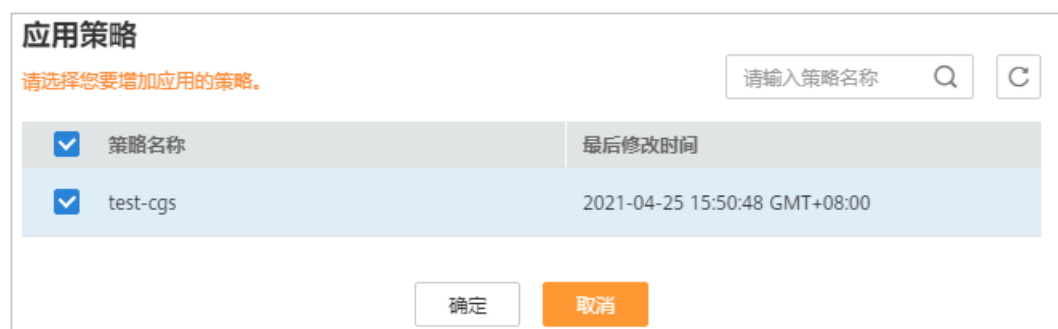
图6-3 应用策略



步骤 6 在弹出的“应用策略”对话框中，勾选需要应用的策略，单击“确定”，如图 6-4 所示。

如果您需要取消应用的策略，可以在策略所在行的“操作”列，单击“取消应用”。

图6-4 选择策略



----结束

6.2 管理私有镜像仓库

私有镜像仓库中的镜像来源于容器镜像服务(SWR)的自有镜像，容器安全服务可对这些镜像执行安全扫描并提供漏洞报告和解决方案。还提供恶意文件、软件信息、文件信息和基线检查功能。

说明

在同意服务授权后，用户可以免费使用私有镜像漏洞扫描功能，恶意文件、软件信息、文件信息和基线检查功能需要用户购买容器安全配额。

使用须知

- 已同意 CGS 服务授权。

查看私有镜像仓库列表

步骤 1 登录管理控制台。

- 步骤 2** 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3** 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。
- 步骤 4** 选择“私有镜像仓库”页签，如图 6-5 所示。

 说明

单击“从 SWR 更新镜像”，可以同步 SWR 所有自有镜像。

图6-5 私有镜像仓库



表6-2 私有镜像列表参数说明

参数	说明	操作
镜像名称	镜像的名称。	单击镜像名称前的  , 可查看该镜像的版本列表。
镜像 ID	镜像的 ID。	-
所属组织	镜像所属组织名称， 镜像组织由容器镜像 服务负责管理。	-
版本数	镜像版本数量。	-

----结束

查看私有镜像基本信息

- 步骤 1** 登录管理控制台。
- 步骤 2** 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3** 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的, 展开镜像版本列表。

步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。

步骤 5 查看该镜像版本的基本信息，如图 6-6 所示。

图6-6 私有镜像基本信息

基本信息	漏洞报告	关联策略	恶意文件	软件信息	文件信息	基线检查
镜像名称	tianyan	所属组织	ctyun-scan-image			
镜像版本	20.1.24	镜像版本ID	sha256:7d52da74b7d1ef3d36d43d9e2178b32c3ceb5db38d9ceefaf2d24b11dcd748a9			
镜像大小	1.50 GB	镜像版本最后更新时间	2021-05-31 11:06:36 GMT+08:00			
漏洞个数	31	最近一次扫描完成时间	2021-07-14 17:08:13 GMT+08:00			
扫描状态	扫描完成					

----结束

扫描私有镜像

容器安全服务对私有镜像仓库**每日凌晨**进行一次全面的安全扫描。您也可以单击某个镜像对单个镜像进行安全扫描。

安全扫描的时长主要取决于镜像的大小。一般情况下扫描一个镜像可以在三分钟之内完成。

扫描完成后，单击“漏洞报告”查看漏洞报告。本小节介绍镜像版本安全扫描操作步骤。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。

步骤 4 单击目标镜像版本操作列的“安全扫描”。

图6-7 安全扫描

镜像名称	镜像ID	所属组织	版本数				
^ tianyan	7d52da74b7d1ef3d36d43d9e2178b32c3ceb5db38d9ceefaf2d24b11dcd748a9	ctyun-scan-image					
镜像版本	镜像大小	镜像版本最后更新时间	最近一次扫描完成时间	漏洞个数	关联策略个数	扫描状态	操作
20.1.24	1.50 GB	2021-05-31 11:06:36 GMT+08:00	2021-07-14 17:08:13 GMT+08:00	31	1	扫描完成	安全扫描 漏洞报告

步骤 5 在弹出的提示框中单击“确定”，启动扫描任务。

----结束

查看私有镜像的漏洞

扫描完成后，可查看漏洞报告。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。

步骤 4 单击目标镜像版本操作列的“漏洞报告”，如图 6-8 所示。

图6-8 查看漏洞报告

镜像名称	镜像ID	所属组织	版本号				
^ alpine	cd98d1859c1b6b33ec70507249d34bacf888d59c24df32040579a5c7...	mytest	1				
镜像版本	镜像大小	镜像版本最后更新...	最近一次扫描完成...	漏洞个数	关联漏洞个数	扫描状态	操作
latest	5.53 MB	2021-01-09 11:05...	2021-01-12 14:51...	3	2	扫描完成	安全扫描 漏洞报告

步骤 5 进入漏洞报告信息界面，查看该镜像版本的漏洞概览。

- 漏洞占比：按“漏洞修复紧急度”进行统计的漏洞数量及占比。
- 漏洞分布个数：按“漏洞修复紧急度”进行统计的漏洞数量。
- 漏洞列表：展示漏洞的详细信息以及解决方案。

图6-9 漏洞报告



----结束

管理私有镜像的策略

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。

步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。

步骤 5 选择“关联策略”页签，单击“应用策略”，如图 6-10 所示。

图6-10 应用策略



步骤 6 在弹出的“应用策略”对话框中，勾选需要应用的策略，单击“确定”，如图 6-11 所示。

如果您需要取消应用的策略，可以在策略所在行的“操作”列，单击“取消应用”。

图6-11 选择策略



----结束

查看私有镜像的恶意文件

扫描完成后，可查看镜像上存在的恶意文件。本节介绍查看镜像版本中存在的恶意文件。

查看全局私有镜像中存在的恶意文件，详细步骤，请参见：4.4 查看恶意文件检测详情。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的 ，展开镜像版本列表。

步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。

步骤 5 选择“恶意文件”页签，查看镜像上存在的恶意文件，如所示。

图6-12 恶意文件（私有）

基本信息	漏洞报告	关联策略	恶意文件	软件信息	文件信息	基线检查
镜像版本 3.12.1.3 最近一次扫描完成时间 2021/06/09 14:28:14 GMT+08:00 重新扫描						
请输入文件名称						
恶意文件名称	路径	文件大小	描述			
entrypoint.sh	/	902B	cgs-test			

----结束

查看私有镜像的软件信息

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。

步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。

步骤 5 选择“软件信息”页签，查看该镜像版本包含的软件、软件类型和软件中存在的漏洞数，如所示。

图6-13 软件信息

基本信息	漏洞报告	关联策略	恶意文件	软件信息	文件信息	基线检查
镜像版本 1.0 最近一次扫描完成时间 2021-06-18 11:00:13 GMT+08:00						
请输入软件名称搜索						
软件名称	类型	版本	漏洞个数			
adduser	DEB	3.113+nmu3ubuntu4	0			
aerospike-server-community	DEB	3.12.1.3-1	0			

步骤 6 单击软件名称前的，可查看该软件中漏洞的漏洞名称、修复紧急度和解决方案。

----结束

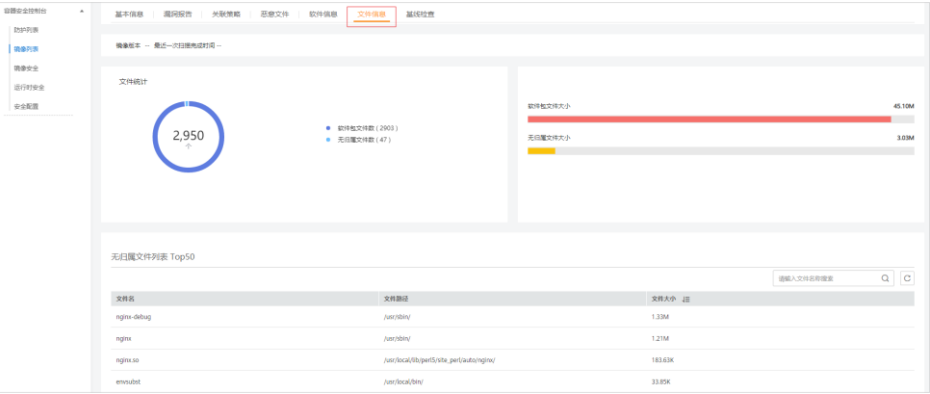
查看私有镜像的文件信息

步骤 1 登录管理控制台。

- 步骤 2** 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3** 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。
- 步骤 4** 单击目标镜像版本名称，进入镜像“基本信息”页面。
- 步骤 5** 单击“文件信息”页签，查看镜像上的文件信息，如图 6-14 所示。

包含：软件包文件数、无归属文件数、软件包文件大小、无归属文件大小和无归属文件 Top50 列表。

图6-14 文件信息



----结束

查看私有镜像的基线检查详情

- 步骤 1** 登录管理控制台。
- 步骤 2** 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3** 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。
- 步骤 4** 单击目标镜像版本名称，进入镜像“基本信息”页面。
- 步骤 5** 单击“基线检查”页签，查看镜像基线检查详情，并根据加固建议修复有风险的配置信息。

图6-15 私有镜像基线检查详情



----结束

6.3 管理官方镜像仓库

官方镜像仓库中的镜像来源于容器镜像服务(SWR)的镜像中心，容器安全服务可对这些镜像执行安全扫描。

本章节指导用户查看官方镜像列表、镜像版本基本信息、镜像漏洞和管理官方镜像的策略。

说明

在同意服务授权后，用户可以免费使用官方镜像漏洞扫描功能，容器安全服务自动执行安全扫描。

查看官方镜像列表

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。

步骤 4 选择“官方镜像仓库”页签。

----结束

查看官方镜像基本信息

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“官方镜像仓库”页签，单击镜像名称前的 ，展开镜像版本列表。

步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。

步骤 5 查看该版本的镜像基本信息，如图 6-16 所示。

图6-16 官方镜像基本信息

基本信息 漏洞报告 关联策略			
镜像名称	alpine	所属组织	mytest
镜像版本	latest	镜像版本ID	sha256:cd98d1859c1beb33ec705072
镜像大小	5.53 MB	镜像版本最后更新时间	2020-11-09 11:05:28 GMT+08:00
漏洞个数	0	最近一次扫描完成时间	2020-11-12 14:51:04 GMT+08:00
扫描状态	扫描完成		

----结束

查看官方镜像的漏洞

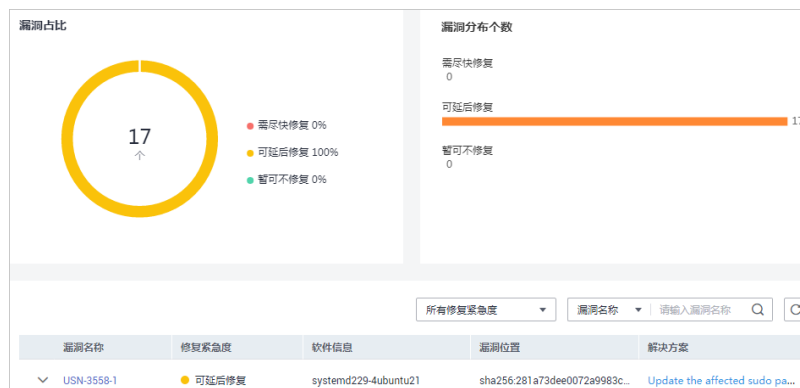
步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“官方镜像仓库”页签，单击镜像名称前的，展开镜像版本列表。

步骤 4 单击目标镜像版本操作列的“漏洞报告”，查看镜像上存在的漏洞。

图6-17 官方镜像漏洞



步骤 5 单击漏洞名称前的，查看漏洞详细信息。

图6-18 漏洞详细信息

漏洞名称	修复紧急度	软件信息	漏洞位置	解决方案
USN-3558-1	可延后修复	systemd229-4ubuntu21	sha256:281a73dee0072a9983c...	Update the affected sudo pa...
CVEID	CVSS分值	披露时间	漏洞描述	
CVE-2017-15908	5	2017/10/26 00:00:00 GMT+08:00	In systemd 223 through 235, a remote DNS server can re...	

----结束

管理官方镜像的策略

您可以将添加的安全策略应用到官方镜像。

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“官方镜像仓库”页签，单击镜像名称前的 ，展开镜像版本列表。
- 步骤 4 单击目标镜像版本名称，进入镜像“基本信息”页面。
- 步骤 5 选择“关联策略”页签，单击“应用策略”，如图 6-19 所示。

图6-19 应用策略



- 步骤 6 在弹出的“应用策略”对话框中，勾选需要应用的策略，单击“确定”，如图 6-20 所示。

如果您需要取消应用的策略，可以在策略所在行的“操作”列，单击“取消应用”。

图6-20 选择策略

应用策略

请选择您要增加应用的策略。

请输入策略名称

Q

C

☒ 策略名称	最后修改时间
☒ test-cgs	2021-04-25 15:50:48 GMT+08:00

确定

取消

----结束

7 查看防护列表

防护列表展示了云容器引擎（CCE）中集群的安全防护状态、节点的防护状态和防护配额状态，帮助您实时了解集群的安全状态和配额状态。

集群列表中可获得集群和节点的基本信息，防护配额列表中可获得配额状态、到期时间、续费和退订信息。

前提条件

已同意 CGS 服务授权。

查看集群列表

- 步骤 1 登录管理控制台。
- 步骤 2 在页面上方选择“区域”后，单击，选择“安全 > 容器安全服务”，进入“防护列表”界面。
- 步骤 3 在“防护列表”界面，选择“集群列表”页签，查看集群防护状态，集群列表参数说明如表 7-1 所示。

表7-1 集群列表参数说明

参数名称	说明
集群名称	集群的名称。 说明 单击名称可进入“节点列表”界面。
节点总数/可用节点/Shield 在线数	- 节点总数：集群中总的节点数量。 - 可用节点：“节点状态”为“运行中”的节点数量。 - Shield 在线数：“Shield 状态”为“在线”的节点数量。
集群防护状态	集群的防护状态，包括：

参数名称	说明
	- 未开启 - 已开启

步骤 4 单击集群名称，进入“节点列表”界面。

步骤 5 节点列表详情页面包含以下内容

- 节点状态：运行中、不可用。
- Shield 状态：未注册、在线、离线。

----结束

查看防护配额

在“防护列表”界面，选择“防护配额”页签，查看防护配额详细信息，如图 7-1 所示。

图7-1 防护配额

集群列表		防护配额	
配额版本	配额ID	配额状态	操作
容器安全企业版	721effa3-2393-4cb3-bc07-a40ab46d4f46	➕ 正常	续费 退订

详情页面包含以下内容：

- 配额状态：正常、已过期、已冻结。
- 到期时间：容器安全配额防护剩余时间。
- 操作：续费、退订。

8 关闭集群防护

若用户不需要防护容器安全服务时，请参照本章节关闭集群防护。

关闭集群防护系统会自动卸载该集群上安装的容器安全插件。

前提条件

- 已同意 CGS 服务授权。
- 集群的“集群防护状态”为“已开启”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在需要关闭防护的集群所在行的“操作”列，单击“关闭防护”。

说明

单击集群名称，进入“节点列表”界面，用户也可以在节点列表上方，单击“关闭防护”。

步骤 4 在弹出的提示框中，单击“是”。

关闭集群防护后，集群的“集群防护状态”为“未开启”，说明该集群中的所有可用节点都已关闭防护。

说明

关闭防护系统会自动卸载该集群上安装的容器安全插件。

----结束

9 审计

9.1 支持云审计的 CGS 操作

容器安全服务通过云审计服务（Cloud Trace Service，CTS）为用户提供云服务资源的操作记录，记录内容包括用户从管理控制台发起的云服务资源操作请求以及每次请求的结果，供用户查询、审计和回溯使用。

云审计服务支持的 CGS 操作列表如表 9-1 所示。

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
授权访问	cgs	registeCgsAgency
手动执行镜像扫描	cgs	scanPrivateImage
从 SWR 拉取镜像并执行扫描	cgs	syncSwrPrivateImage

9.2 查看审计日志

开启了云审计服务后，系统开始记录 CGS 资源的操作。云审计服务管理控制台保存最近 7 天的操作记录。

查看 CGS 的云审计日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤 3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤 4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。
在下拉框中选择查询条件。
 - “事件类型”选择“管理事件”。
 - “事件来源”选择“CGS”。
 - “筛选类型”选择“事件名称”时，还需选择某个具体的事件名称；选择“资源 ID”时，还需选择或者手动输入某个具体的资源 ID；选择“资源名称”时，还需选择或手动输入某个具体的资源名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- “事件级别”：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- “时间范围”：可在页面右上角选择查询最近 1 小时、最近 1 天、最近 1 周及自定义时间段的操作事件。

步骤 5 单击“查询”，查看对应的操作事件。

步骤 6 在需要查看的记录左侧，单击  展开该记录的详细信息

步骤 7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，显示了该操作事件结构的详细信息。

----结束

10 权限管理

10.1 CGS 自定义策略

如果系统预置的 CGS 权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考 10.2 CGS 权限及授权项。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON 视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写 JSON 格式的策略内容。

具体创建步骤请参见：。本章为您介绍常用的 CGS 自定义策略样例。

CGS 自定义策略样例

- 示例 1：授权用户查询集群列表信息

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cgs:cluster:list"
      ]
    }
  ]
}
```

- 示例 2：拒绝用户修改配置信息

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在 Allow 和 Deny，则遵循 **Deny 优先原则**。

如果您给用户授予“CGS FullAccess”的系统策略，但不希望用户拥有“CGS FullAccess”中定义的修改配置信息权限，您可以创建一条拒绝修改配置信息的自定义策略，然后同时将“CGS FullAccess”和拒绝策略授予用户，根据 Deny 优先原则，则用户可以对 CGS 执行除了修改配置信息外的所有操作。拒绝策略示例如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cgs:configuration:operate"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- 示例 3：多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cgs:cluster:list",
        "cgs:quota:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:accountCracks:unblock",
        "hss:commonIPs:set"
      ]
    }
  ]
}
```

10.2 CGS 权限及授权项

如果您需要对您所拥有的容器安全服务（Container Guard Service，CGS）进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果登录帐号已经能满足您的要求，不需要创建独立的 IAM 用户，您可以跳过本章节，不影响您使用 CGS 服务的其它功能。

默认情况下，新建的 IAM 用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是 IAM 最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的 Action，在自定义策略中的 Action 中写入授权项，可以实现授权项对应的权限功能。

权限	授权项	依赖的授权项
查询容器安全配额统计信息	cgs:quota:get	-
查询包周期配额列表	cgs:quota:list	-
订购容器安全包周期配额	cgs:quota:operate	-
查询集群列表信息	cgs:cluster:list	• cce:addonInstance:* • cce:node:list • cce:cluster:list
容器集群开启或关闭防护	cgs:cluster:operate	• cce:addonInstance:*
查询镜像列表信息	cgs:images:list	-
执行镜像同步和扫描	cgs:images:operate	-
查询容器镜像信息	cgs:images:get	-
查询配置信息	cgs:configuration:list	-
修改配置信息	cgs:configuration:operate	-
查询镜像安全信息	cgs:imageSecure:list	-
操作镜像安全事件	cgs:imageSecure:operate	-
获取镜像扫描结果	cgs:imageSecure:get	-
查询运行时事件列表	cgs:runtimeSecure:list	-
查询运行时监控信息	cgs:runtimeSecure:get	-
处理运行时监控事件	cgs:runtimeSecure:operate	-
操作容器安全委托授权	cgs:privilege:operate	-
查询容器安全授权	cgs:privilege:get	-

11 常见问题

11.1 如何开启集群防护

开启集群防护的同时，系统会自动为该集群安装容器安全插件。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在需要开启防护的集群所在行的“操作”列，单击“开启防护”。

说明

单击集群名称，进入“节点列表”界面，用户也可以在节点列表上方，单击“开启防护”。

步骤 4 在弹出的对话框中，确认“集群名称”和“集群可用节点数”并单击“是”，完成开启防护操作。

开启防护后，集群的“集群防护状态”为“已开启”，说明该集群中的所有可用节点都已开启防护。

图11-1 “开启防护” 提示框



说明

- 集群开启防护后，如果集群新增了节点，容器安全服务将为新增的节点自动开启防护，并对新增的节点提供防护。
- 集群开启防护时，系统将自动为该集群安装容器安全插件。

----结束

11.2 如何关闭集群防护

关闭集群防护的同时，系统会自动卸载该集群上的容器安全插件。

步骤 1 登录管理控制台。

步骤 2 在页面上方选择“区域”后，单击 ，选择“安全 > 容器安全服务”，进入“防护列表”界面。

步骤 3 在需要关闭防护的集群所在行的“操作”列，单击“关闭防护”。

说明

单击集群名称，进入“节点列表”界面，用户也可以在节点列表上方，单击“关闭防护”。

步骤 4 在弹出的提示框中，单击“是”。

关闭集群防护后，集群的“集群防护状态”为“未开启”，说明该集群中的所有可用节点都已关闭防护。

说明

关闭防护系统会自动卸载该集群上安装的容器安全插件。

----结束

11.3 容器集群节点的 Shield 状态离线如何处理？

如果集群节点的 Shield 状态为离线，请检查以下情况：

- 集群是否安装了 CGS 插件
在 CGS 控制台为指定集群开启防护时，CGS 自动为该集群安装插件，关闭防护时自动卸载插件。如果集群当前未开启防护则 Shield 为离线。
- 集群节点状态是否正常
只有安装了插件并且集群节点状态是运行中，Shield 才会在线。如果节点状态异常，请到云容器引擎（CCE）处理状态异常的节点。
- 集群初次安装插件后，Shield 从启动到状态显示为在线需要最长 5 分钟的时间间隔。开启防护后，请您稍等一段时间再查看 Shield 状态。

11.4 无服务授权权限和创建委托失败的原因？

IAM 用户进入容器安全服务控制台界面时，发现服务授权页面“同意授权”按钮呈灰色状态，表示该 IAM 用户无服务授权权限，请联系拥有 Security Administrator 权限的管理员授予权限或使用帐号开通服务授权。

创建委托失败的原因：账户委托数量满额。

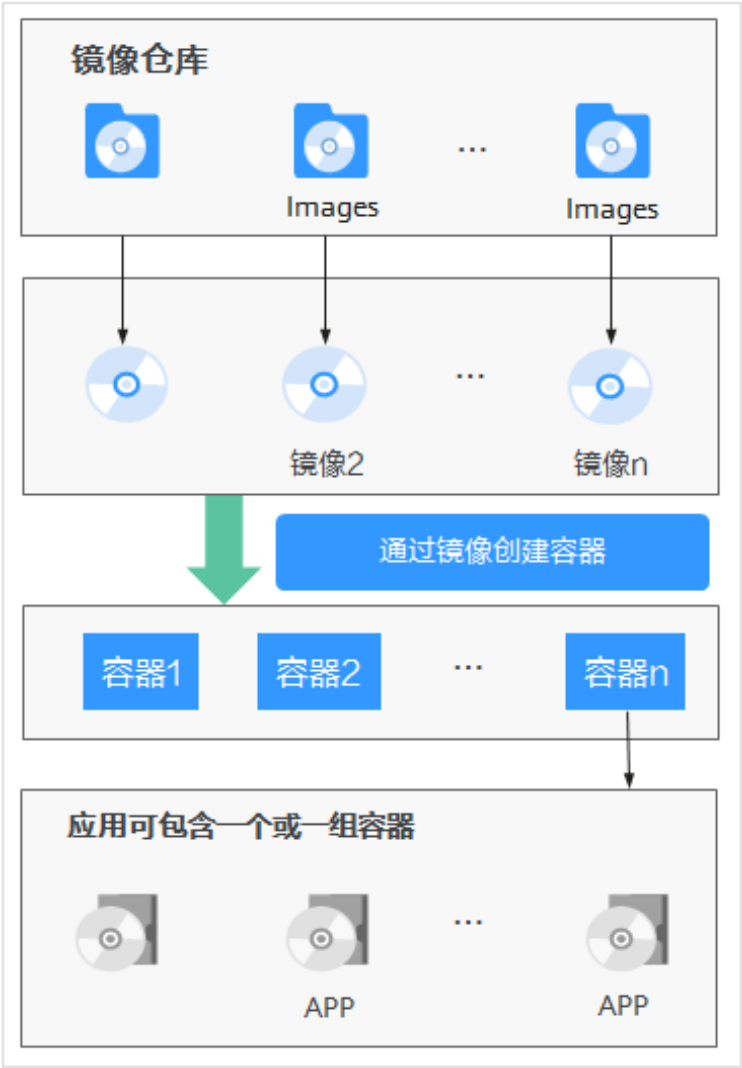
处理方式：登录到“统一身份认证服务”管理控制台，对委托进行删除或联系统一身份认证服务增加限额。

11.5 镜像、容器、应用的关系是什么？

- 镜像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（如匿名卷、环境变量、用户等）。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。
- 容器和镜像的关系，像程序设计中的实例和类一样，镜像是静态的定义，容器是镜像运行时的实体。容器可以被创建、启动、停止、删除、暂停等。
- 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。

镜像、容器、应用之间的关系如图 11-2 所示。

图11-2 镜像、容器、应用的关系



A 修订记录

发布日期	修改说明
2021-09-10	第一次正式发布。