容器安全服务

用户指南

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 开通集群防护

1.1 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（拥有全局Security Administrator权限）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“安全与合规 > 容器安全服务”，进入“服务授权”界面。

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系统管理员增加限额。

----结束

1.2 购买容器安全配额

容器安全服务提供企业版供您选择。

- 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、安全配置及告警设置等功能。

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“安全与合规 > 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1-1**所示，请根据**表1-1**进行配置。

图 1-1 购买容器安全配额

表 1-1 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。 **须知** • 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**。

参数	参数说明
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”。

----结束

1.3 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一个POD，用于运行时监控、扫描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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

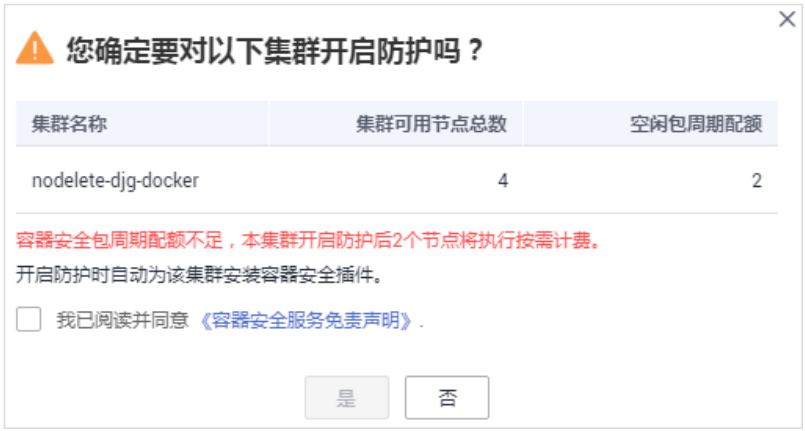
步骤3 在需要开启防护的集群所在行的“操作”列，单击“开启防护”。

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 在弹出的提示框中，阅读《容器安全服务免责声明》后，勾选“我已阅读并同意《容器安全服务免责声明》”并单击“是”，如图1-2所示。

图 1-2 “开启防护”提示框



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。

说明

- 开启集群防护时，若已购买的包周期防护配额小于当前已开启防护的集群节点个数，超出的集群节点将执行按需计费。容器安全服务按需计费请查看：**什么是容器安全服务的按需计费?**
- 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

相关链接

- 开启防护后，您可通过自定义安全策略，配置进程白名单和文件保护，有效阻止容器运行时安全风险事件的发生，提高系统和应用的安全。如何配置安全策略请查看：**（可选）策略配置**。
- 关闭集群防护的详细操作，请参见：**关闭集群防护**。
- Shield状态离线请查看：**容器集群节点的Shield状态离线如何处理**。

1.4 设置告警通知

开启告警通知功能后，您能接收到容器安全服务发送的告警通知邮件和短信，及时了解镜像/容器运行时的安全风险。否则，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警信息。

- 告警通知设置仅在当前区域生效，若需要接收其他区域的告警通知，请切换到对应区域后进行设置。
- 告警通知信息可能会被误拦截，若您未收到相关告警信息，请在信息拦截中查看。
- 告警通知默认发送给账号联系人，新增或修改接收人可到“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”进行配置。

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“安全与合规 > 容器安全服务”。

步骤3 进入“安全配置”页面，选择“告警配置”页签，如图1-3所示。

图 1-3 告警配置

步骤4 开启 “每日告警通知”。

说明

每日告警通知每天发送一次通知，当最近24小时存在告警事件时，发送每日告警。

步骤5 开启 “实时告警通知”并勾选需要的通知项。

说明

- 异常事件发生时立即触发告警。
- 单区域每5分钟最多发送一条实时告警消息，每天最多发送10条实时告警消息。

----结束

2 （可选）策略配置

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“安全与合规 > 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。

步骤4 选择“策略配置”页签，在策略列表上方，单击“添加策略”。

步骤5 在“添加策略”页面，配置策略内容，如图2-1所示，相关参数说如表2-1所示。

图 2-1 “添加策略”页面

表 2-1 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6 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“安全与合规 > 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。

步骤4 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”。

步骤5 在“关联镜像”对话框中，选择需要应用策略的镜像，如图2-2所示。

图 2-2 “关联镜像”对话框

步骤6 勾选目标镜像选框，单击“确定”，完成选择关联镜像操作。

关联镜像设置完后，你可以查看该镜像文件中存在的恶意文件、容器异常监控结果。详细操作，请参见：**查看恶意文件检测详情**和**查看运行时安全详情**。

----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。

3 镜像安全

3.1 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“安全与合规 > 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 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 3-1 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6 查看漏洞列表，各参数说明如表3-1所示。

表 3-1 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7。
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7 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3-2和图3-3所示。

图 3-2 漏洞的基本信息（本地）

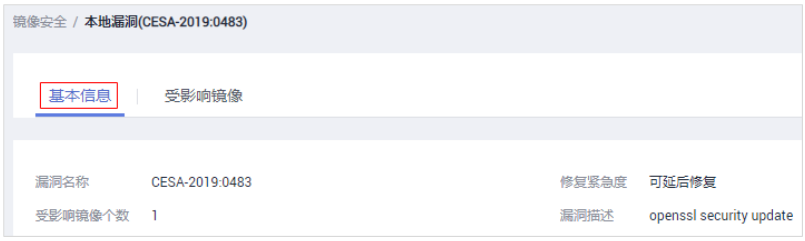


图 3-3 受漏洞影响的镜像列表

----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“安全与合规 > 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3-2。

表 3-2 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	1. 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”。 2. 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： 1. 在漏洞列表中，单击漏洞名称，查看受该漏洞影响的镜像列表，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。

3.2 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“安全与合规 > 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 > 私有镜像仓库漏洞”页签。

步骤5 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6 查看漏洞列表，各参数说明如表3-3所示。

表 3-3 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7。
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7 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3-4和图3-5所示。

图 3-4 漏洞的基本信息（私有）

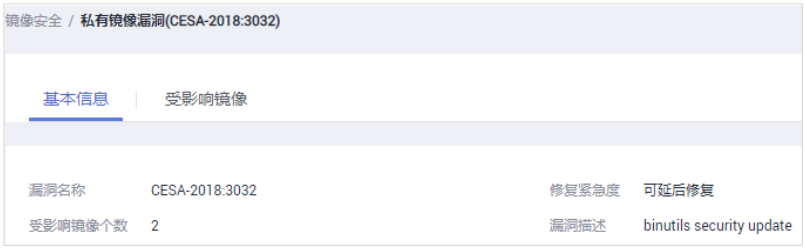


图 3-5 受漏洞影响的镜像列表（私有）

----结束

3.3 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“安全与合规 > 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 > 官方镜像仓库漏洞”页签。

步骤5 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6 查看漏洞列表，各参数说明如表3-4所示。

表 3-4 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7**。
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7 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3-6**和**图3-7**所示。

图 3-6 漏洞的基本信息（官方）

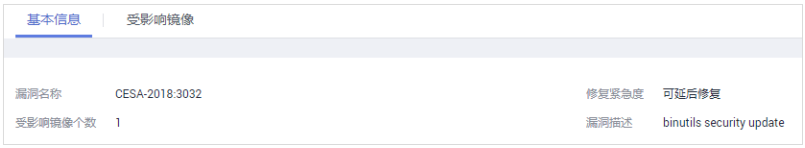


图 3-7 受漏洞影响的镜像列表（官方）

----结束

3.4 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“安全与合规 > 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 3-8 恶意文件

----结束

3.5 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“安全与合规 > 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 3-9 查看基线检查详情

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。

图 3-10 检测项详情

----结束

4 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 4-1 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。

检测项	原理说明
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kubernates 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suid位或者sgid位获取附加权限，通过sudo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“ –no-new-privileges=false”，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mount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。

检测项	原理说明
	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“安全与合规 > 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 4-1 容器异常监控趋势图

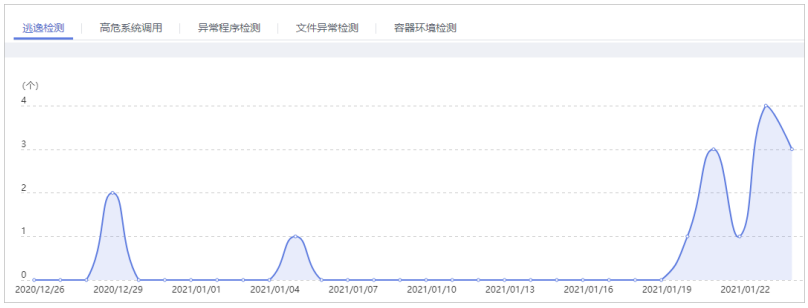


图 4-2 容器异常事件列表

- 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

5 管理镜像信息

5.1 管理本地镜像

本地镜像是用户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“安全与合规 > 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 5-1 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“安全与合规 > 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5-1所示。

图 5-1 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“安全与合规 > 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 5-2 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“安全与合规 > 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5-3所示。

图 5-3 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”。

----结束

5.2 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

同意服务授权后，用户可以免费体验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开启集群防护功能后才可以使用。

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“安全与合规 > 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5-4所示。

说明

单击“从SWR更新镜像”，可以同步SWR所有自有镜像。

图 5-4 私有镜像仓库

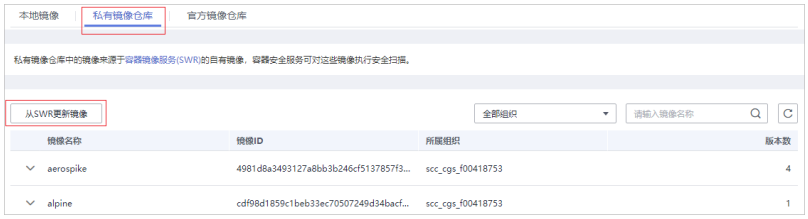


表 5-2 私有镜像列表参数说明

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

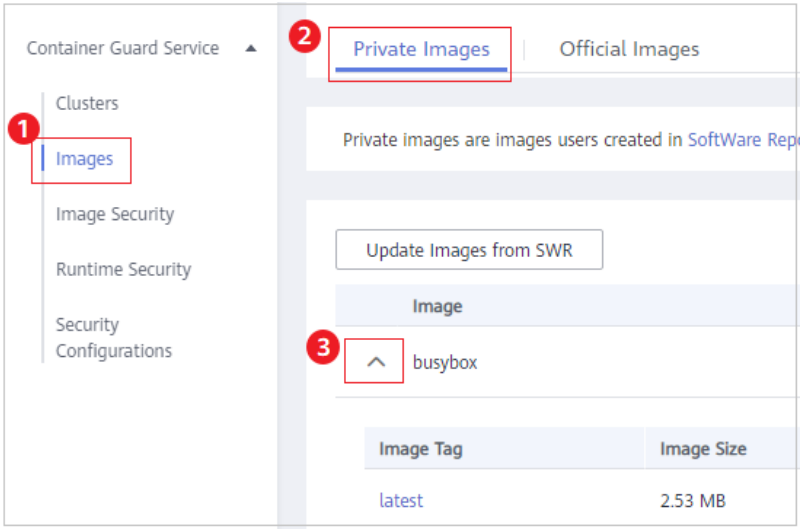
查看私有镜像基本信息

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

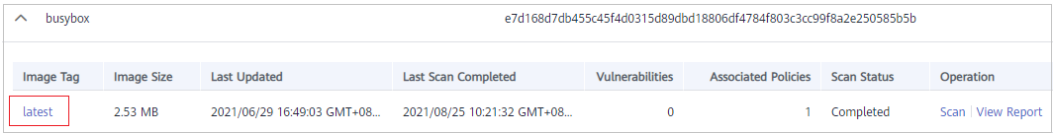
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的∨，展开镜像版本列表，如图5-5所示。

图 5-5 展开镜像



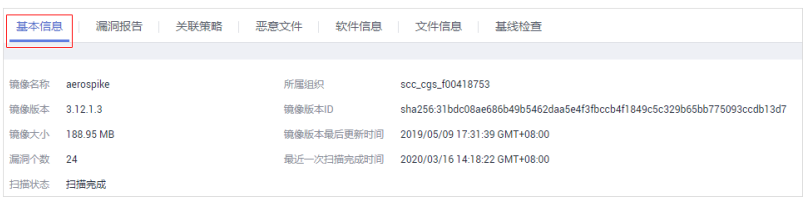
步骤4 单击目标镜像版本名称，如图5-6所示，进入镜像“基本信息”页面。

图 5-6 选择镜像



步骤5 查看该镜像版本的基本信息，如图5-7所示。

图 5-7 私有镜像基本信息



----结束

扫描私有镜像

您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。

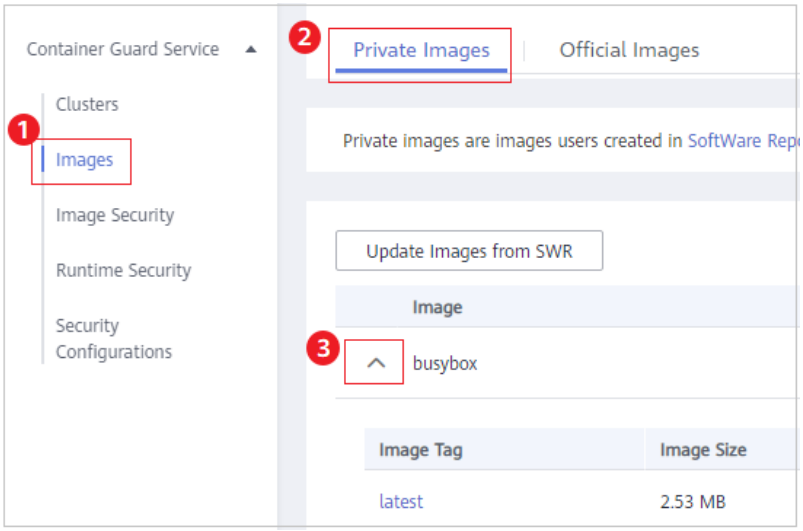
扫描完成后，单击“漏洞报告”查看漏洞报告。本小节介绍镜像版本安全扫描操作步骤。

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“安全与合规 > 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，如图5-8所示。

图 5-8 展开镜像



步骤4 单击目标镜像版本操作列的“安全扫描”。

图 5-9 安全扫描

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

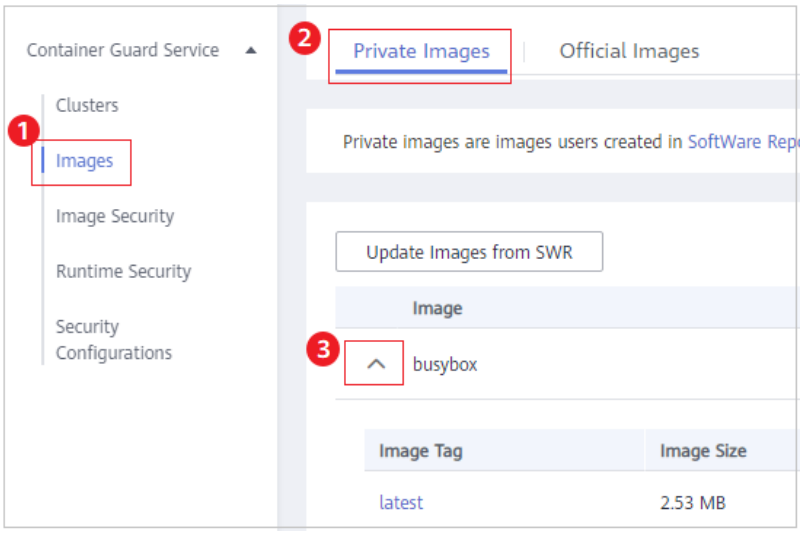
扫描完成后，可查看漏洞报告。

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“安全与合规 > 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，如图5-10所示。

图 5-10 展开镜像



步骤4 单击目标镜像版本操作列的“漏洞报告”。

图 5-11 查看漏洞报告

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 5-12 漏洞报告

----结束

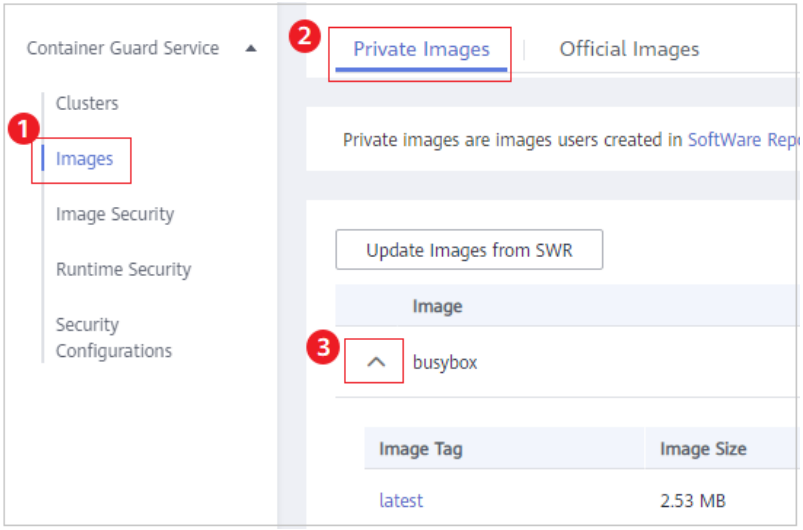
管理私有镜像的策略

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

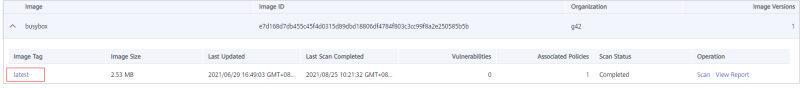
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的∨，展开镜像版本列表，如图5-13所示。

图 5-13 展开镜像



步骤4 单击目标镜像版本名称，如图5-14所示，进入镜像“基本信息”页面。

图 5-14 选择目标镜像



步骤5 选择“关联策略”页签，单击“应用策略”，如图5-15所示。

图 5-15 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”。

----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。

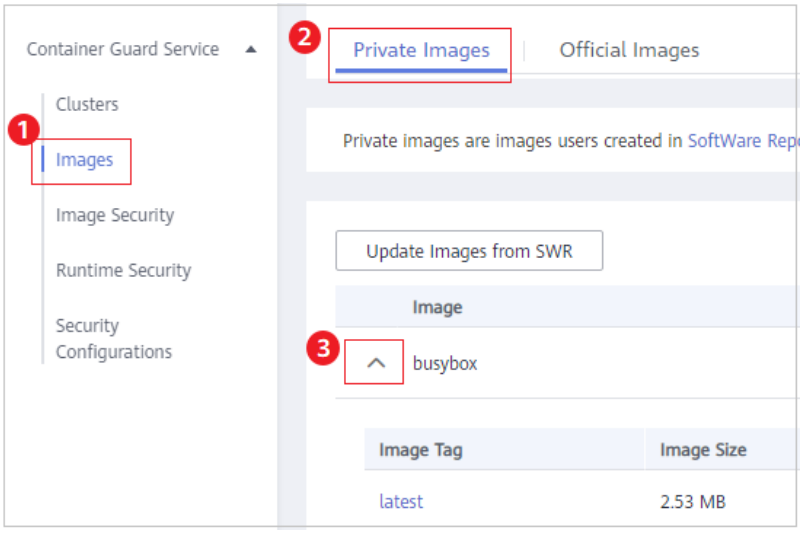
查看全局私有镜像中存在的恶意文件，详细步骤，请参见：**查看恶意文件检测详情**。

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

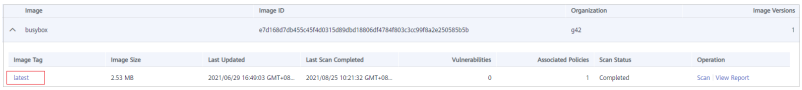
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的 ⌄，展开镜像版本列表，如**图5-16**所示。

图 5-16 展开镜像



步骤4 单击目标镜像版本名称，如**图5-17**所示，进入镜像“基本信息”页面。

图 5-17 选择目标镜像



步骤5 选择“恶意文件”页签，查看镜像上存在的恶意文件，如图5-18所示。

图 5-18 恶意文件（私有）

----结束

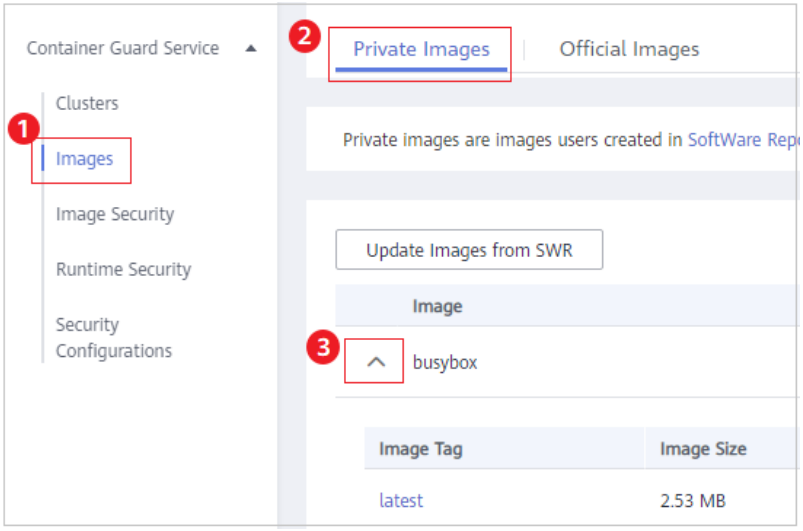
查看私有镜像的软件信息

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

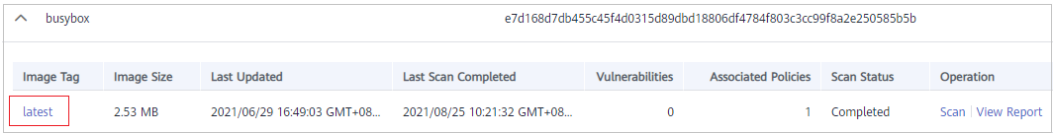
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的 ⌄，展开镜像版本列表，如图5-19所示。

图 5-19 展开镜像



步骤4 单击目标镜像版本名称，如图5-20所示，进入镜像“基本信息”页面。

图 5-20 选择镜像



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，如图5-21所示。

图 5-21 软件信息

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

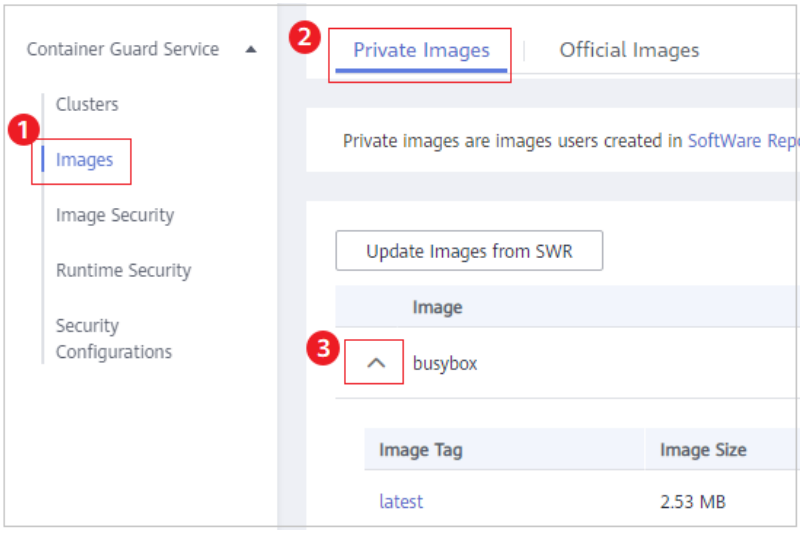
查看私有镜像的文件信息

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

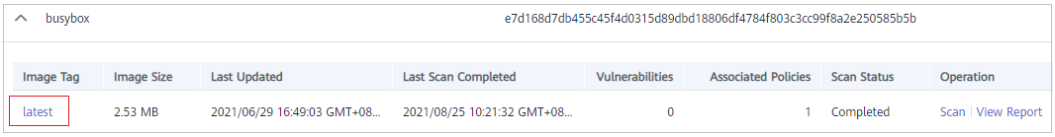
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的，展开镜像版本列表，如图5-22所示。

图 5-22 展开镜像



步骤4 单击目标镜像版本名称，如图5-23所示，进入镜像“基本信息”页面。

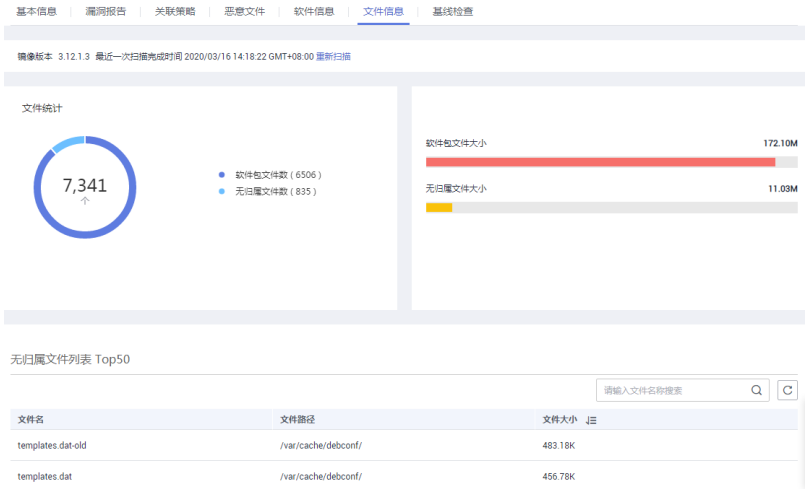
图 5-23 选择镜像



步骤5 单击“文件信息”页签，查看镜像上的文件信息，如图5-24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 5-24 文件信息



----结束

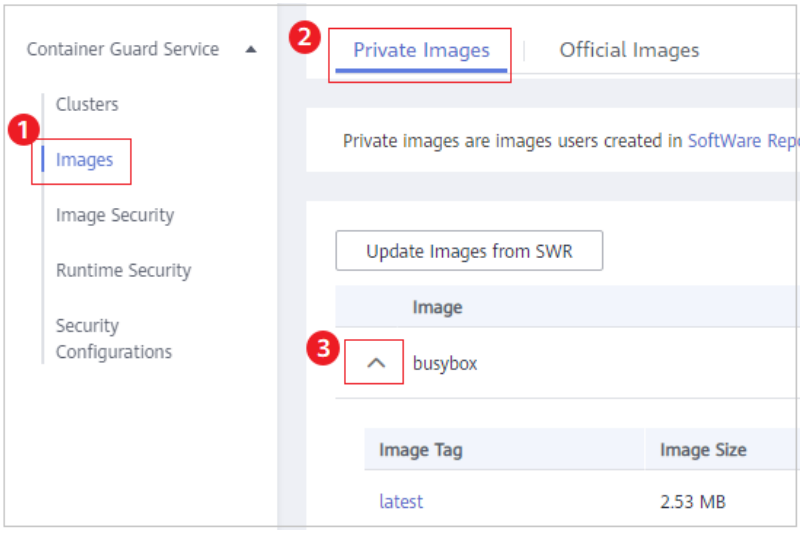
查看私有镜像的基线检查详情

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

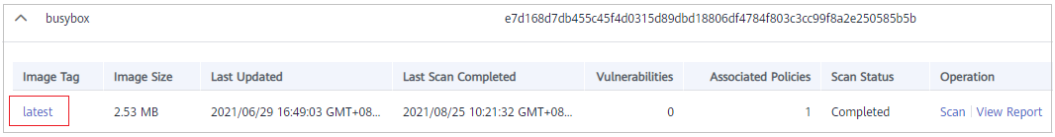
步骤3 在左侧导航树中，选择“镜像列表”，进入“镜像列表”界面。选择“私有镜像仓库”页签，单击镜像名称前的 ⌄，展开镜像版本列表，如图5-25所示。

图 5-25 展开镜像



步骤4 单击目标镜像版本名称，如图5-26所示，进入镜像“基本信息”页面。

图 5-26 选择镜像



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 5-27 私有镜像基线检查详情

----结束

5.3 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“安全与合规 > 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。

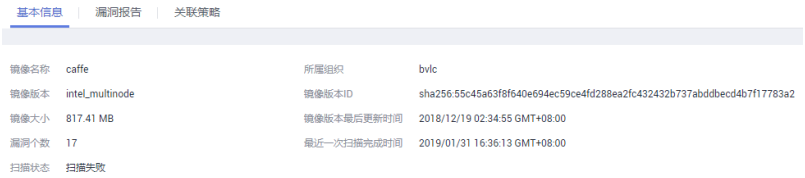
步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全与合规 > 容器安全服务”，进入“防护列表”界面。

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5-28所示。

图 5-28 官方镜像基本信息



----结束

查看官方镜像的漏洞

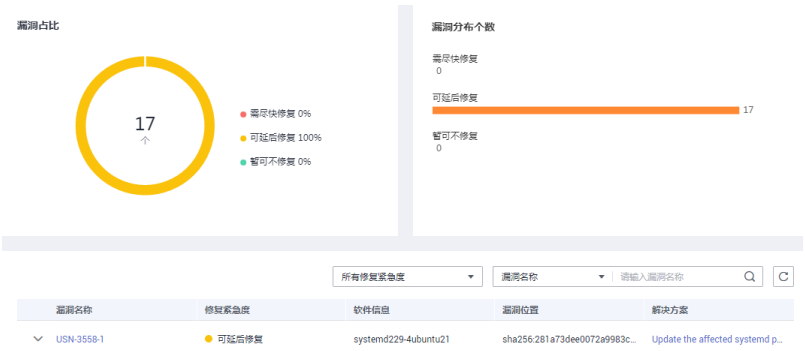
步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全与合规 > 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 5-29 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 5-30 漏洞详细信息

----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“安全与合规 > 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5-31所示。

图 5-31 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”。

----结束

6 查看防护列表

前提条件

已同意CGS服务授权。

查看防护信息

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“安全与合规 > 容器安全服务”，进入“防护列表”界面。

步骤3 查看防护信息。

- 集群防护统计：显示已开启集群防护的集群数量和未开启集群防护的集群数量。
- 节点防护统计：已开启防护的节点个数。
- 我的防护配额：防护配额正常执行防护数、已过期数和已冻结数。

----结束

查看集群列表

步骤1 在页面上方选择“区域”后，单击 ☰，选择“安全与合规 > 容器安全服务”，进入“防护列表”界面。

步骤2 在“防护列表”界面，选择“集群列表”页签，查看集群防护状态。如图6-1所示，集群列表参数说明如表6-1所示。

图 6-1 集群列表

表 6-1 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： • 未开启 • 已开启 **说明** – 开启集群防护时，系统将会自动为该集群安装容器安全插件。开启集群防护详细操作，请参见：**开启集群防护**。 – 关闭集群防护时，系统将会自动卸载该集群上安装的容器安全插件。关闭集群防护详细操作，请参见：**关闭集群防护**。

步骤3 单击集群名称，进入“节点列表”界面，如图6-2所示。

图 6-2 节点列表

步骤4 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。

  Shield离线是指与服务器通信异常，如何处理，请查看：**容器集群节点的Shield状态离线如何处理**。

----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6-3所示。

图 6-3 防护配额

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。

7 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“安全与合规 > 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”。

图 7-1 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

8 审计

8.1 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8-1**所示。

表 8-1 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	registerCgsAgency
手动执行镜像扫描	cgs	scanPrivateImage
从SWR拉取镜像并执行扫描	cgs	syncSwrPrivateImage

8.2 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

9 权限管理

9.1 创建用户并授权使用 CGS

如果您需要对您所拥有的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，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CGS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CGS资源委托给更专业、高效的其他华为云帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

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，您可以跳过本章节，不影响您使用CGS的其它功能。

本章节为您介绍对用户授权的方法。

前提条件

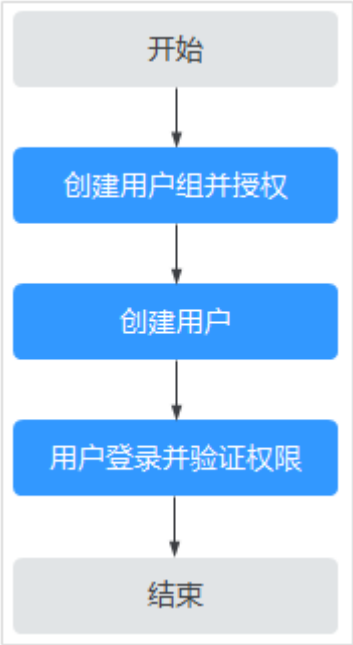
给用户组授权之前，请您了解用户组可以添加的CGS权限，并结合实际需求进行选择，CGS支持的系统权限如**表9-1**所示。

表 9-1 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。

示例流程

图 9-1 给用户授予权限流程



1. **创建用户组并授权**。
   在IAM控制台创建用户组，并授予容器安全服务的系统管理员权限“CGS ReadOnlyAccess”。
2. **创建用户并加入用户组**。
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限。
   新创建的用户登录控制台，切换至授权区域，验证权限：
   验证方式（参考）： 在“服务列表”中选择容器安全服务，进入CGS主界面，单击右上角购买容器安全，尝试购买容器安全配额，如果无法购买容器安全配额（假设当前权限仅包含“CGS ReadOnlyAccess”），表示“CGS ReadOnlyAccess”只读访问权限生效。

9.2 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**CGS权限及授权项**。

目前华为云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：**创建自定义策略**。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"
         ]
      }
   ]
}
```


9.3 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，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最初提供的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，系统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	-

权限	授权项	依赖的授权项
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	-

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。