容器安全服务

常见问题

文档版本 02

发布日期 2022-01-10

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 产品技术类

1.1 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。

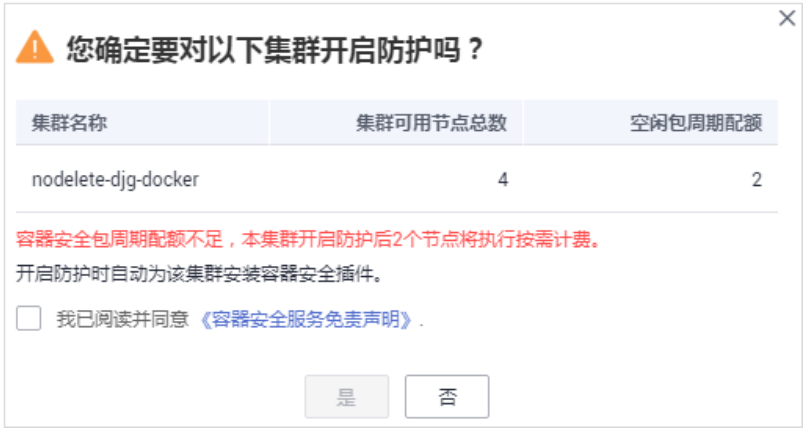
步骤3 在需要开启防护的集群所在行的“操作”列，单击“开启防护”。

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1-1所示。

图 1-1 “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

1.2 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 1-2 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

1.3 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，请到华为云容器引擎服务（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。

1.4 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权限的系统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。

1.5 容器安全服务的漏洞库多久更新一次?

容器安全服务实时获取官方发布的漏洞信息，每天凌晨将漏洞更新至漏洞库中并执行全面的漏洞扫描和给出解决方案。您可根据自身业务情况进行修复或调整有风险的镜像。

- 查看本地镜像漏洞详情和解决方案，请参见：**管理本地镜像漏洞**。
- 查看私有镜像仓库漏洞详情和解决方案，请参见：**管理私有镜像仓库漏洞**。

1.6 容器安全服务的日志处理机制是什么?

容器安全服务每隔10分钟更新一次log文件，如果文件大于30M，则将最近30M的日志信息写入对应的日志备份文件，当前日志文件内容清空。

日志备份文件的文件名为日志源文件名加上“ .last ”后缀，如 “shield.log”的备份文件为 “shield.log.last”。

1.7 容器安全服务的日志路径

CGS日志保存于宿主机系统的 **/var/log/shield**目录下。

日志文件中包含“shield.log”、“message.log”和“defender_audit.log”。

- **shield.log**：记录CGS运行日志、错误日志等信息。
- **message.log**：记录CGS agent与服务端之间的消息通信，如策略下发、告警上报等。
- **defender_audit.log**：记录audit系统日志，由于CGS接管了Linux系统audit消息。如果存在额外手工配置但是并非CGS使用的audit规则，这些规则触发的audit消息记录在该文件中。

1.8 容器安全服务 shield 插件是否会影响业务?

不会影响业务。

容器安全服务shield插件以daemonset插件方式安装，容器化方式运行在集群的每个集群节点上，启动时需要预分配固定资源（CPU：0.3core、内存：300m），启动后只对启动的容器进行监控，不影响您的业务。

2 产品咨询

2.1 CGS 是否支持 Apache Log4j2 远程代码执行漏洞检测?

CGS 新增 Apache Log4j2 远程代码执行漏洞检测能力

12月16日，官方披露低于2.16.0版本除了存在拒绝服务漏洞外，还存在另一处远程代码执行漏洞（CVE-2021-45046）。

Apache Log4j2是一款业界广泛使用的基于Java的日志记录工具。华为云提醒使用Apache Log4j2的用户尽快安排自检并做好安全加固。

参考链接：**https://logging.apache.org/log4j/2.x/security.html**

- 威胁级别：【严重】（说明：威胁级别共四级：一般、重要、严重、紧急）
- 影响版本：2.0-beat9 <= Apache Log4j 2.x < 2.16.0（2.12.2 版本不受影响）
- 已知受影响的应用及组件：spring-boot-starter-log4j2/Apache Solr/Apache Flink/Apache Druid
- 安全版本：Apache Log4j 1.x 不受影响；Apache Log4j 2.16.0。
- 漏洞处置

  目前官方已发布修复版本修复了该漏洞，请受影响的用户尽快升级Apache Log4j2所有相关应用到安全版本：**https://logging.apache.org/log4j/2.x/download.html**

  Java 8（或更高版本）的用户建议升级到 2.16.0 版本；

  Java 7 的用户建议升级到2.12.2版本，此版本是安全版本。

  华为云**容器安全服务CGS**，能够检测私有镜像是否存在该漏洞，基础版免费向客户开放。在华为云容器安全CGS控制台，镜像安全->镜像漏洞->私有镜像仓库漏洞，可以查看私有镜像仓库中的漏洞情况。具体方法参见**管理私有镜像仓库漏洞**。

  说明

  - 无法及时升级的用户，可参考官方建议将JndiLookup类从classpath中去除，并重启服务来进行风险规避：

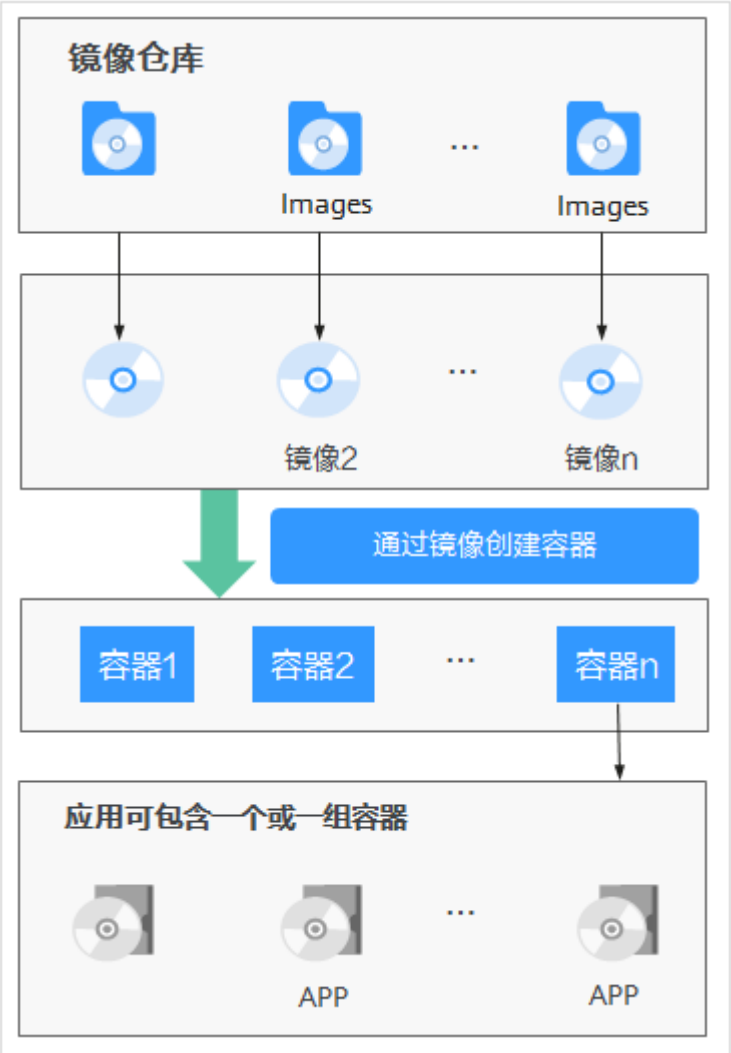
    zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
  - 修复漏洞前请将资料**备份**，并进行充分测试。

2.2 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2-1所示。

图 2-1 镜像、容器、应用的关系



2.3 容器安全服务支持线下及跨平台部署吗?

容器安全服务暂不支持线下及跨平台部署。

容器安全服务支持对华为云上的云容器引擎（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。

2.4 容器安全服务支持多个帐号共享使用吗?

容器安全服务不支持多个帐号共享使用。例如，如果您在某个区域通过注册华为云创建了2个帐号（“domain1”和“domain2”），当您在“domain1”帐号下购买了容器安全服务，则“domain2”帐号不能使用“domain1”的容器安全服务。

在同一区域，一个帐号在IAM上创建的所有IAM用户都可以共用该帐号下的容器安全服务。例如，您在某个区域通过注册华为云创建了1个帐号（“domain1”），且“domain1”帐号在IAM中创建了2个IAM用户（“sub-user01”、“sub-user02”），如果您授权了“sub-user01”和“sub-user02”用户CGS的权限策略，则这2个IAM用户都可以使用“domain1”的容器安全服务。

有关CGS权限管理的详细操作，请参见**创建用户并授权使用CGS**。

3 计费类

3.1 如何为容器安全配额续费?

在容器安全配额到期前，用户可以通过续费操作继续使用容器安全配额。

前提条件

- 登录管理控制台的帐号已授权CGS Administrator、Tenant Guest和BSS Administrator权限策略。
- 已成功购买容器安全配额。

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 选择“防护配额”页签，在需要续费配额的“操作”列，单击“续费”，进入“续费”界面。

步骤4 选择续费时长后，单击“去支付”，完成续费操作。

图 3-1 续费界面

更多关于续费的详细操作，请参见**续费管理**。

----结束

3.2 如何退订容器安全配额?

容器安全服务支持包年/包月付费方式，购买的配额不能直接删除，仅支持退订。如果用户不再使用，请执行退订操作。

前提条件

- 登录管理控制台的帐号已授权CGS Administrator、Tenant Guest和BSS Administrator权限策略。
- 已成功购买容器安全配额。

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 选择“防护配额”页签，在需要退订配额的“操作”列，单击“退订”，进入“退订资源”界面。

步骤4 选择退订原因后，并勾选“我已确认本次退订金额和相关费用”。

更多关于退订的详细操作，请参见**退订管理**。

步骤5 单击“退订”，完成配额退订。

----结束

3.3 什么是容器安全服务的按需计费?

在开启集群防护时，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，超出的节点，每小时按照差额执行按需扣费。

按需计费：按需是每小时计费，先使用后付费。使用方式比较灵活，可以即开即停。

实例从“开启防护”开启计费到“关闭防护”结束计费，按实际使用时长（小时）计费。

按需扣费举例：

- 若用户已购买10个包周期防护配额，实际防护节点总数为15，则每小时按照5个节点执行按需扣费。
- 若用户已购买10个包周期防护配额，实际防护节点总数为10，则不产生按需扣费。

说明

CGS会优先使用您购买的防护配额，在配额不够的情况下开启防护时，才会触发按需计费功能。

4 区域与可用区

4.1 什么是区域和可用区?

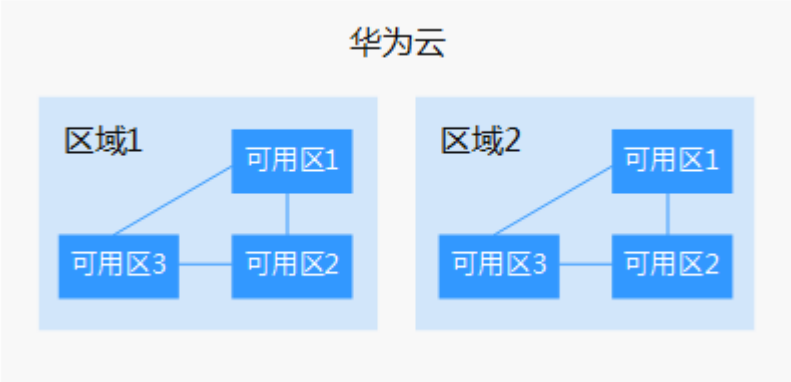
什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图4-1阐明了区域和可用区之间的关系。

图 4-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

A 修订记录

发布日期	修改说明
2022-01-10	第二次正式发布。 新增FAQ：**CGS是否支持Apache Log4j2远程代码执行漏洞检测?**
2021-01-26	第一次正式发布。