

容器安全服务

常见问题

文档版本

14

发布日期

2020-06-18



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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默示的声明或保证。

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
1.1 如何开启集群防护.....	1
1.2 如何关闭集群防护.....	2
1.3 容器集群节点的 Shield 状态离线如何处理?	3
1.4 无服务授权权限和创建委托失败的原因?	4
1.5 容器安全服务的漏洞库多久更新一次?	4
2 产品咨询	5
2.1 镜像、容器、应用的关系是什么?	5
2.2 容器安全服务支持线下及跨平台部署吗?	6
2.3 哪些区域可以使用容器安全服务?	6
2.4 容器安全服务支持多个账号共享使用吗?	7
2.5 容器安全服务支持跨区域使用吗?	7
2.6 什么是区域和可用区?	7
3 计费类	9
3.1 如何为容器安全配额续费?	9
3.2 如何退订容器安全配额?	10
3.3 什么是容器安全服务的按需计费?	12
A 修订记录	13

1 产品技术类

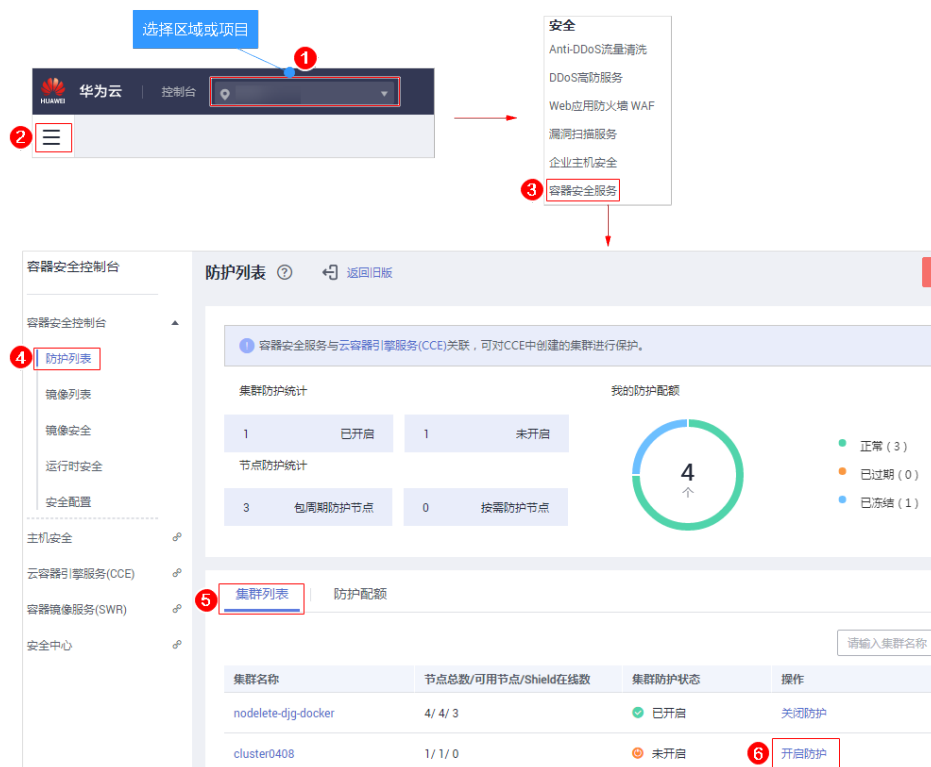
1.1 如何开启集群防护

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 进入开启集群防护入口，如图1-1所示。

图 1-1 进入开启集群防护入口



步骤3 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

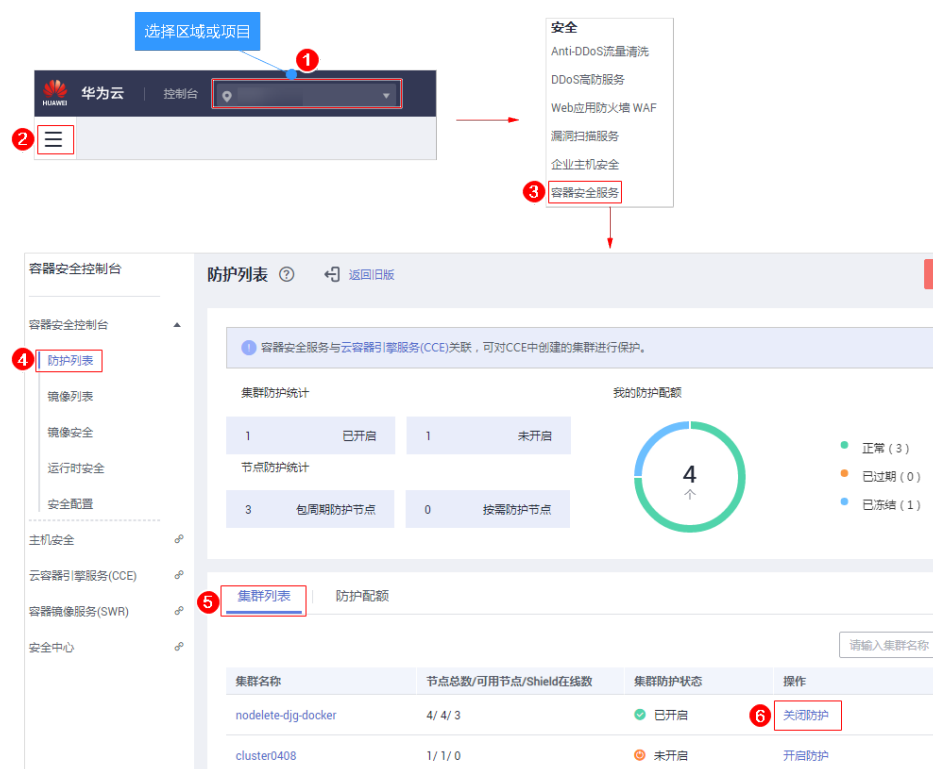
1.2 如何关闭集群防护

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 进入关闭集群防护入口, 如[图1-3](#)所示。

图 1-3 进入关闭集群防护入口



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 1-4 关闭防护

集群名称	节点总数/可用节点/Shield在线数	集群防护状态	操作
nodelete-djg-docker	2/ 2/ 2	已开启	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权限的管理员授予权限或使用账号开通服务授权。

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](#)。

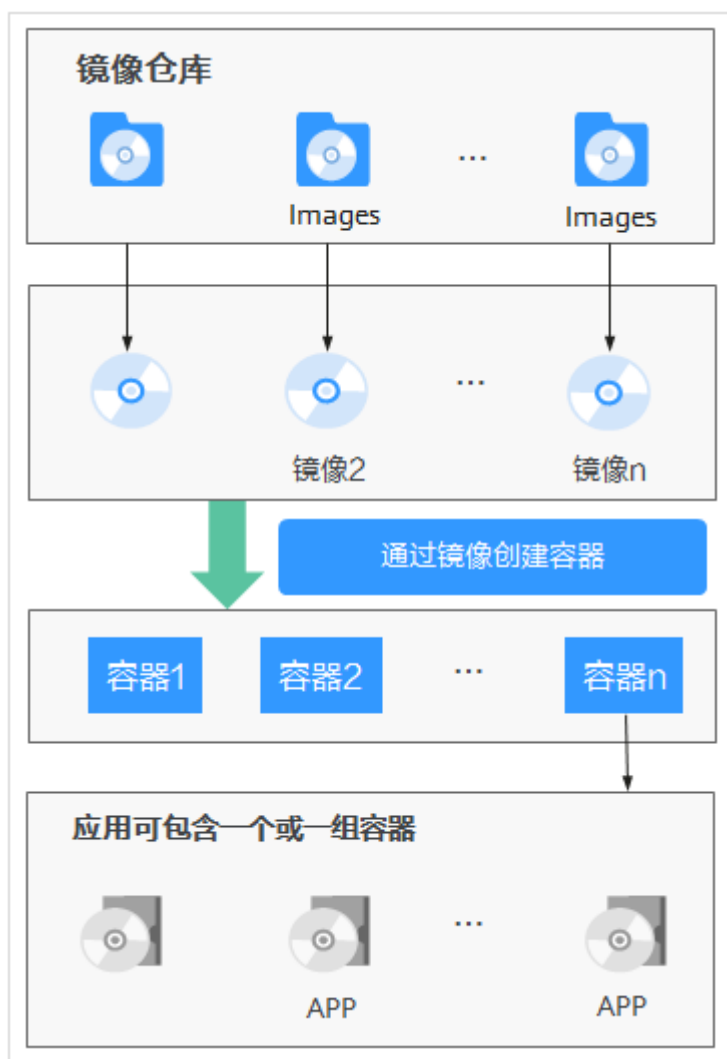
2 产品咨询

2.1 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



2.2 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。

2.3 哪些区域可以使用容器安全服务？

容器安全服务支持的区域说明如下：

- 华北-北京一
- 华北-北京四
- 华南-广州
- 华东-上海一

- 华东-上海二
- 西南-贵阳一

📖 说明

容器安全服务需要获取CCE和SWR的数据，因此，在购买容器安全配额时，请您先确认您选择的区域是否与CCE和SWR所在区域一致，若不在同一区域，您将无法使用容器安全服务。

2.4 容器安全服务支持多个账号共享使用吗？

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

在同一区域，一个账号在IAM上创建的所有IAM用户都可以共用该账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个账号（“domain1”），且“domain1”账号在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](#)。

2.5 容器安全服务支持跨区域使用吗？

容器安全服务不支持跨区域（Region）使用。购买的容器安全配额必须与CCE和SWR区域一致，您才能使用容器安全服务。

如果您购买的容器安全配额在“华北-北京四”，而CCE和SWR在“华东-上海一”，则您将不能使用容器安全服务。

2.6 什么是区域和可用区？

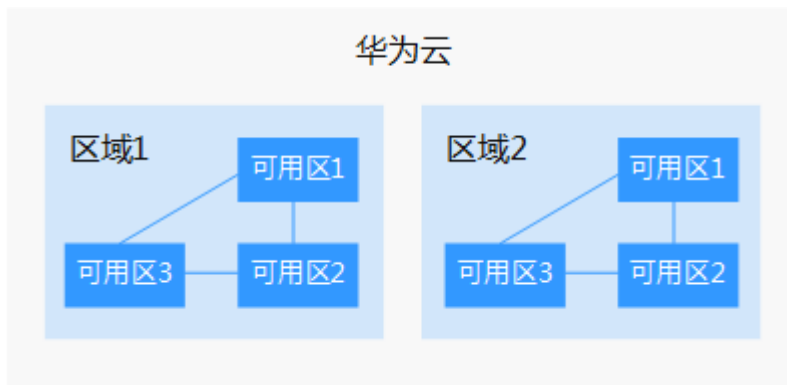
什么是区域、可用区？

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2-2](#)阐明了区域和可用区之间的关系。

图 2-2 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“亚太-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“南非-约翰内斯堡”区域。
 - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”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](#)。

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

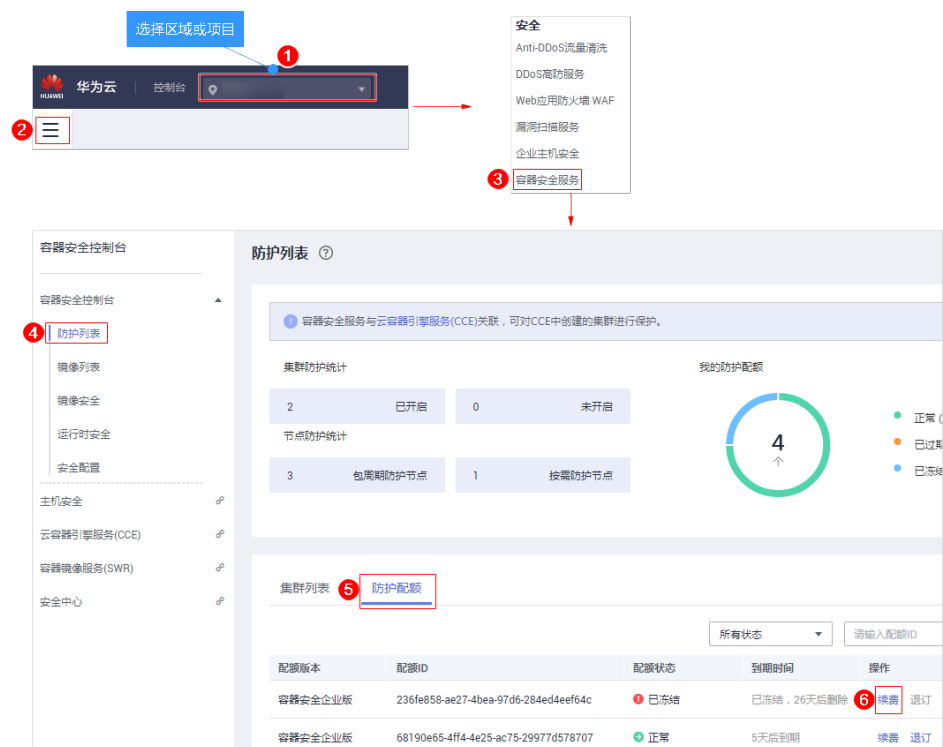
- 登录管理控制台的账号已授权CGS Administrator、Tenant Guest和BSS Administrator权限策略。
- 已成功购买容器安全配额。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 进入容器安全防护配额续费入口，如[图3-1](#)所示。

图 3-1 进入容器安全防护配额续费入口



步骤3 在“续费”界面，选择续费时长后，单击“去支付”，完成续费操作。

图 3-2 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

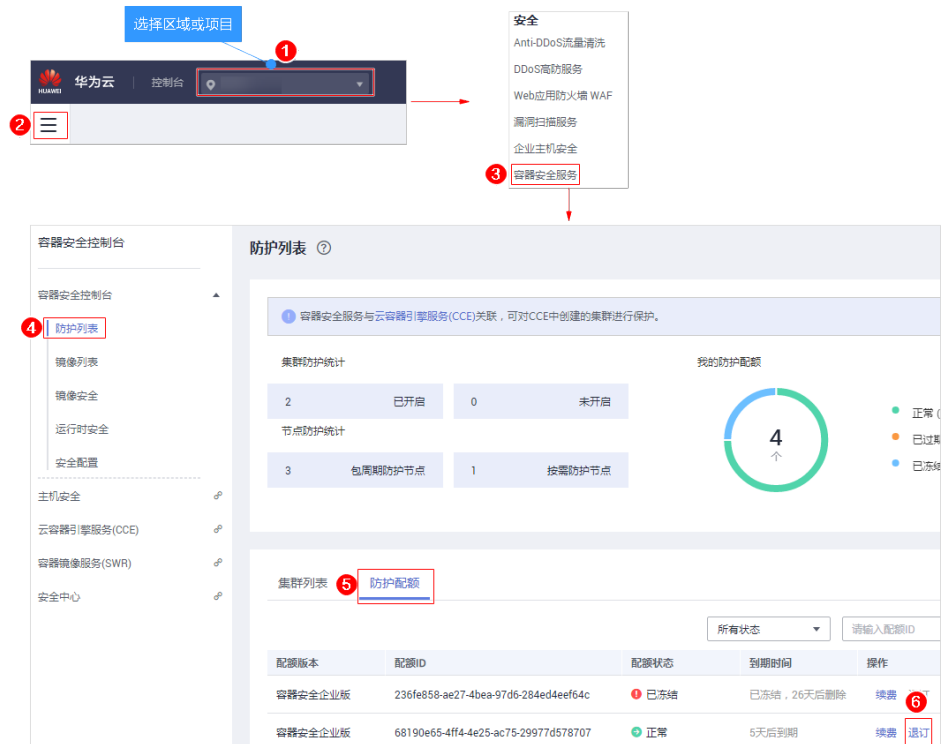
- 登录管理控制台的账号已授权CGS Administrator、Tenant Guest和BSS Administrator权限策略。
- 已成功购买容器安全配额。

操作步骤

步骤1 登录管理控制台。

步骤2 进入容器安全防护配额退订入口，如图3-3所示。

图 3-3 进入容器安全防护配额退订入口



步骤3 在“退订资源”界面，选择退订原因，并勾选“我已确认本次退订金额和相关费用”。

图 3-4 退订资源

退订规则及手续费细则请查看[退订规则说明](#)。

1. 您本次退订属于非6天无理由退订，需收取手续费和已消费金额，已使用的代金券和折扣券不退还。
2. 如果您的订单是通过第三方在线支付的，退订后退款会退还到您的华为云账户。

! 本次操作完成后，2020年12月31日前您还可以进行0次五天无理由退订。

<input checked="" type="checkbox"/>	名称/ID	产品类型	产品规格	云服务区	起止时间	已消费金额(¥)	手续费(¥)	退订金额(¥)
<input checked="" type="checkbox"/>	68190e65-4ff4-4e25-ac75-2...	企业主机安全	容器安全企业版		2020/03... 2020/04...			

*** 请选择退订原因**

购买云服务时选错参数 业务部署后，退订多购买的云服务 业务测试完毕退订

云服务不好用 云服务不满足业务部署需求 云服务故障无法修复

其他

实付金额 ① ¥

已消费金额 ① -¥

手续费 ① -¥

退订金额 ¥

退还余额 ¥

我已确认本次退订金额和相关费用。 [查看详情](#)

退订

更多关于退订的详细操作，请参见[退订管理](#)。

----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。

详细服务资费和费率标准，请查看：[产品价格详情](#)。

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。

A 修订记录

发布日期	修改说明
2020-06-18	第十四次正式发布。 新增 容器安全服务的漏洞库多久更新一次?
2020-06-05	第十三次正式发布。 哪些区域可以使用容器安全服务? ，新增支持使用CGS的区域。
2020-04-01	第十二次正式发布。 更新界面截图。
2020-03-11	第十一次正式发布。 <ul style="list-style-type: none"> • 新增容器安全服务支持跨区域使用吗? • 新增容器安全服务支持多个账号共享使用吗?
2020-01-15	第十次正式发布。 哪些区域可以使用容器安全服务? ，新增支持使用CGS的区域。
2019-11-29	第九次正式发布。 <ul style="list-style-type: none"> • 修改如何为容器安全配额续费?。 • 修改如何退订容器安全配额?。
2019-11-26	第八次正式发布。 <ul style="list-style-type: none"> • 新增什么是容器安全服务的按需计费?。 • 新增容器集群节点的Shield状态离线如何处理?。 • 修改如何开启集群防护，增加按需计费说明。
2019-11-12	第七次正式发布。 <ul style="list-style-type: none"> • 修改如何开启集群防护，优化相关内容描述。 • 修改如何开启集群防护，优化相关内容描述。

发布日期	修改说明
2019-09-25	第六次正式发布。 哪些区域可以使用容器安全服务？ ，优化相关内容描述。
2019-08-30	第五次正式发布。 <ul style="list-style-type: none"> “安装Shield插件”修改为如何开启集群防护。 “卸载Shield插件”修改为如何关闭集群防护。 新增什么是区域和可用区？。
2019-08-23	第四次正式发布。 <ul style="list-style-type: none"> 修改“安装Shield插件”章节。 修改“卸载Shield插件”章节。 新增如何为容器安全配额续费？。 新增如何退订容器安全配额？。
2019-08-13	第三次正式发布。 新增 IAM用户无服务授权权限和创建委托失败的原因？ 。
2019-05-30	第二次正式发布。 <ul style="list-style-type: none"> 修改“安装Shield插件”章节。 修改“卸载Shield插件”章节。
2018-10-18	第一次正式发布。