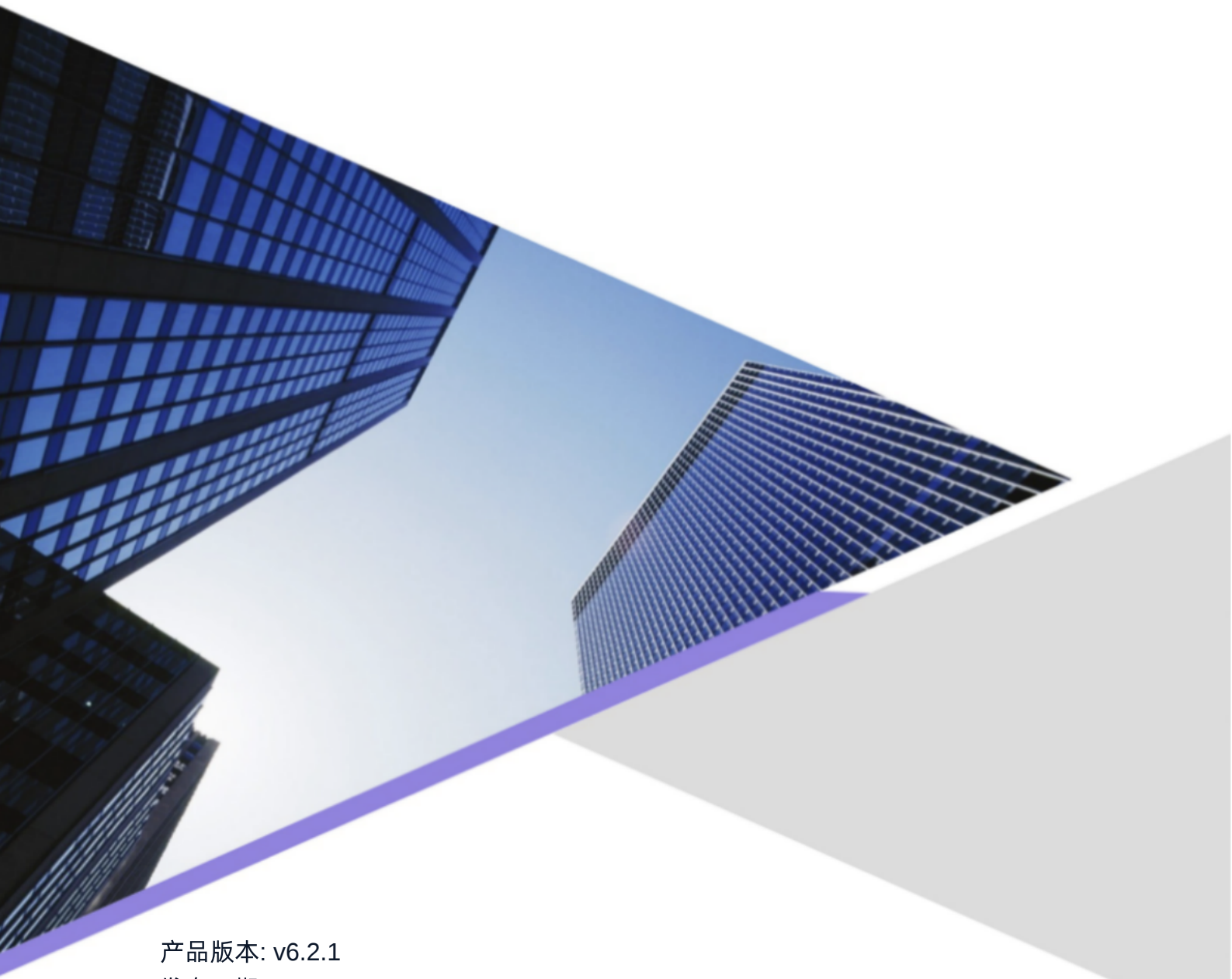
EasyStack
易捷行云

# 安全容器服务

## 产品介绍



产品版本: v6.2.1

发布日期: 2024-06-05

# 目录

# 1 产品介绍

## 1.1 什么是安全容器服务

安全容器服务基于成熟、轻量的安全容器运行时和SDN网络服务，提供卓越的不可信应用隔离、故障隔离、性能隔离以及多租户应用网络隔离等能力，以便用户轻松高效地在云端运行安全容器化应用。

## 产品优势

- **安全且故障隔离**

  基于安全容器运行时，提供超强的不可信应用隔离、故障隔离等能力。

- **云资源网络互通**

  安全容器与计算、存储、网络等资源内网互通，以便容器可以分配到虚拟网卡、公网IP和负载均衡等资源，同时也方便传统云主机应用与容器应用之间网络互通。

- **标准适配**

  在网络、日志、监控、存储等方面有着和普通容器一样的用户体验，并具备极速启动和优秀的兼容性、稳定性等特点。

- **网络隔离**

  基于SDN网络服务，在安全容器运行时上增加多租户应用网络隔离能力。

- **统一权限管理**

  为防止资源误操作，将资源的操作能力和云平台的授权管理服务结合，一体化实现。

- **统一配额管理**

  为防止资源滥用，将资源的配额管理能力和云平台的配额管理结合，一体化管理。

## 主要功能

- **配额管理**

  为防止资源滥用，云平台支持设置安全容器相关资源的配额，对各项目的可用资源数量和容量做出限制，配额项包括CPU、内存、存储容量、GPU等。

- **容器负载**

  支持对部署容器实例的全生命周期管理，包括启动/停止、重新部署、配置更新、历史版本回滚、终端操作、查看监控与日志、删除等操作。

- **弹性伸缩**

  基于HPA（Horizontal Pod Autoscaler）能力，根据容器当前使用的CPU与内存压力自动扩缩容。

- **滚动升级**

  当通过控制器部署多副本的工作负载时，支持设置自定义滚动更新策略。

- **负载均衡**

  当用户服务是通过控制器部署时，使用负载均衡可将传入流量分配到部署中的各个容器实例，当部署发生变化时，云平台会自动从负载均衡器中添加和删除实例。

- **GPU调度**

  提供NVIDIA GPU设备的发现与管理能力，云平台在创建容器时将依据指定GPU使用需求自动调度GPU资源。

- **持久化存储**

  提供数据持久化存储满足容器运行过程中需要保存数据的需求，并支持普通容量型以及高性能型两种存储类型（使用高性能存储类型时需要搭配高性能云存储产品）。在创建工作负载时支持添加多个存储卷，以及为每个存储卷指定存储类型和容量，并支持挂载存储卷到容器的指定路径。

# 1.2 使用场景

- **替换传统虚拟机业务**

  传统虚拟机部署应用，虽然安全性较高，但无法享用到镜像和容器带来的技术红利，并且传统虚拟机的损耗开销较大，交付效率分钟级，难以脱离虚拟机镜像，网络自建和交付不统一等难题，安全容器为解决以上痛点，通过精简的虚拟机，启动在秒级内，复用容器管理平台上的多种资源，包括CNI，CSI等通用化网络，存储方案。

- **隔离不可信应用与故障**

  由于在同一节点中，普通容器通常都混部着不同的业务和租户应用，这些容器都共享同一内核。所以，当内核或者运行时出现漏洞时，恶意代码将会逃逸到对宿主机产生不可逆影响，甚至会导致系统瘫痪。安全容器服务提供超强的不可信应用隔离、故障隔离、性能隔离以及多租户应用网络隔离等能力，保障用户轻松高效地在云端运行安全容器化应用。

- **业务应用运行独占操作系统内核**

  安全容器服务提供内核级的进程隔离机制，天然满足容器独占内核的需求。

# 1.3 基本概念

## 集群（Cluster）

一个集群指容器运行所需要的云资源组合，关联了若干服务器节点、存储、网络等基础资源。

## 节点（Node）

安全容器集群中的节点包括Master节点和Worker节点两种类型，每一个节点对应一个云主机。Master节点是安全容器集群的管理者，运行着一些用于保证集群正常工作的组件，如 kube-apiserver、kube-scheduler等。Worker节点是 安全容器集群中承担工作负载的节点，承担实际的 Pod 调度以及与管理节点的通信等。一个Worker节点上运行的组件包括containerd运行时组件、kubelet、Kube-Proxy等。

## 命名空间（Namespace）

在同一个集群内可以创建不同的命名空间，不同命名空间中的数据彼此隔离，使它们既可以共享同一个集群的服务，也能够互不干扰，为集群提供资源逻辑隔离作用。

## 容器组（Pod）

容器组即Pod，是安全容器服务部署应用或服务的最小的基本单位。一个容器组封装多个容器（也可以只有一个容器）、存储资源、网络资源以及管理控制容器运行方式的策略选项。

## 工作负载

工作负载是安全容器服务对一组Pod的抽象模型，用于描述业务的运行载体，包括部署（Deployment）、有状态副本集（StatefulSet）、守护进程集（DaemonSet）、任务（Job）、定时任务（CronJob）。

- 部署：即Kubernetes中的“Deployment”，部署支持弹性伸缩与滚动升级，适用于容器组完全独立、功能相同的场景，如nginx。
- 有状态副本集：即Kubernetes中的“StatefulSet”，有状态副本集支持容器组有序部署和删除，支持持久化存储，适用于实例间存在互访的场景，如ETCD等。
- 守护进程集：即Kubernetes中的“DaemonSet”，守护进程集确保全部（或者某些）节点都运行一个容器组，支持容器组动态添加到新节点，适用于容器组在每个节点上都需要运行的场景，如fluentd、Prometheus

Node Exporter等。

- 任务：即Kubernetes中的“Job”，任务是一次性运行的短任务，部署完成后即刻执行。
- 定时任务：即Kubernetes中的“CronJob”，定时任务是按照指定时间周期运行的任务。

# 安全工作负载

安全工作负载拥有独立的操作系统内核以及安全隔离的虚拟化层。通过安全工作负载，不同容器之间的内核、计算和网络资源均相互隔离，保护Pod的资源和数据不被其他Pod抢占和窃取。

# 服务（Service)

由于每个容器组都有自己的IP地址，并且可能随时被删除重建，如果这个容器组要为其它容器组提供服务，则如何找出并跟踪要连接的IP地址会非常麻烦。安全容器服务针对这个问题给出的方案是服务（Service）。Service是将运行在一组Pods上的应用程序公开为网络服务的抽象方法。使用安全容器服务，您无需修改应用程序即可使用不熟悉的服务发现机制。 安全容器服务为Pods提供自己的IP地址和一组Pod的单个DNS名称，并且可以在它们之间进行负载平衡。

# 路由（Ingress）

Ingress是一组将集群内服务暴露给集群外服务的路由规则集合。一个ingress对象能够配置具备为服务提供外部可访问的URL、负载均衡流量、卸载 SSL/TLS，以及提供基于名称的虚拟主机等能力。

# 持久化存储

- **持久卷（PV）**

  持久卷描述的是持久化存储卷，主要定义的是一个持久化存储在宿主机上的目录，独立于容器组生命周期。具体到本平台，一个持久卷对应一个云硬盘。

- **持久卷声明（PVC）**

  持久卷是存储资源，而持久卷声明（PVC) 是对持久卷的请求。持久卷声明跟容器组类似：容器组消费节点资源，而持久卷声明消费持久卷资源；容器组能够请求CPU和内存资源，而持久卷声明请求特定大小和访问模式的持久卷。

- **存储类（StorageClass）**

存储类可以实现动态供应持久卷，即能够按照用户的需要，自动创建其所需的存储。

# 配置（ConfigMap）

ConfigMap用于将非机密性的数据保存到键值对中。使用时，容器组可以将其用作环境变量、命令行参数或者存储卷中的配置文件。ConfigMap将环境配置信息和容器镜像解耦，便于应用配置的修改。

# 密钥（Secret）

密钥（Secret）是一种包含认证信息、密钥等敏感信息的资源类型，可以用作工作负载的环境变量、加密配置文件。将数据放在密钥对象中，可以更好地控制它的用途，并降低意外暴露的风险。

# 标签（Label）

标签是一对 key/value，被关联到对象上，比如节点、容器组。通过标签可以方便地标识及筛选对象。

# 1.4 产品获取

## 前提条件

在执行下述产品获取操作步骤前，请确保以下条件均已满足：

- 已成功获取并安装“计算服务”、“块存储”、“SDN网络服务”和“容器镜像服务”云产品。获取并安装云产品的具体操作说明，请参考“产品与服务管理”帮助中的相关内容。
- 如需获取正式版云产品，请提前将已获取的许可文件准备就绪。

## 操作步骤

1. 获取并安装“安全容器服务”云产品。

   在顶部导航栏中，依次选择[产品与服务]-[产品与服务管理]-[云产品]，进入“云产品”页面获取并安装“安全容器服务”云产品。具体的操作说明，请参考“产品与服务管理”帮助中“云产品”的相关内容。

2. 访问安全容器服务。

   在顶部导航栏中，依次选择[产品与服务]-[安全容器服务]-[任意子菜单]，即可访问该服务的各项功能。

# 1.5 权限说明

本章节主要用于说明安全容器服务各功能的用户权限范围。其中，√ 代表该类用户可对云平台内所有项目的操作对象执行此功能，**XX项目** 代表该类用户仅支持对XX项目内的操作对象执行此功能，未标注代表该类用户无权限执行此功能。

| 功能 | | 云管理员 | 部门管理员/项目管理员 | 普通用户 |
|---|---|---|---|---|
| 集群管理 | 信息展示 | √ | | |
| 节点管理 | 信息展示 | √ | | |
| | 开始/停止调度 | | | |
| | 标签管理 | | | |
| | 污点管理 | | | |
| 命名空间 | 信息展示 | √ | 仅已加入项目 | |
| | 创建命名空间 | | | |
| | 删除 | | | |
| 存储管理 | 信息展示 | √ | 仅已加入项目 | |
| | 查看存储类Yaml | | | |
| | 查看持久卷Yaml | | | |
| | 删除持久卷 | | | |
| 工作负载 | 信息展示 | √ | 仅已加入项目 | 仅已加入项目 |
| | 创建部署 | | | |
| | 创建有状态副本集 | | | |
| | 创建守护进程集 | | | |
| | 创建任务 | | | |

| 功能 | | 云管理员 | 部门管理员/项目管理员 | 普通用户 |
|---|---|---|---|---|
| | 创建定时任务 | | | |
| | 容器配置 | | | |
| | 手动伸缩 | | | |
| | 版本回滚 | | | |
| | 升级策略 | | | |
| | 伸缩策略 | | | |
| | 调度策略 | | | |
| | 网络设置 | | | |
| | 标签设置 | | | |
| | 编辑Yaml | | | |
| | 启动/停止 | | | |
| | 重新部署 | | | |
| | 删除 | | | |
| | 运行/停止定时任务 | | | |
| | 查看容器组Yaml | | | |
| | 容器日志 | | | |
| | 容器终端 | | | |
| | 删除容器组 | | | |
| 持久卷声明 | 信息展示 | √ | 仅已加入项目 | 仅已加入项目 |
| | 创建持久卷声明 | | | |
| | 编辑Yaml | | | |
| | 删除 | | | |

| 功能 | | 云管理员 | 部门管理员/项目管理员 | 普通用户 |
| --- | --- | --- | --- | --- |
| 配置中心 | 信息展示 | √ | 仅已加入项目 | 仅已加入项目 |
| | 创建配置 | | | |
| | 更新配置 | | | |
| | 编辑配置Yaml | | | |
| | 删除配置 | | | |
| | 创建密钥 | | | |
| | 更新密钥 | | | |
| | 编辑密钥Yaml | | | |
| | 删除密钥 | | | |
| 网络管理 | 信息展示 | √ | 仅已加入项目 | 仅已加入项目 |
| | 创建服务 | | | |
| | 更新服务 | | | |
| | 编辑服务Yaml | | | |
| | 删除服务 | | | |
| | 创建Ingress | | | |
| | 更新Ingress | | | |
| | 编辑Ingress Yaml | | | |
| | 删除Ingress | | | |
| 自定义资源管理 | 信息展示 | √ | 仅已加入项目 | 仅已加入项目 |
| | 使用Yaml导入自定义资源描述 | | | |
| | | | | |

| 功能 | | 云管理员 | 部门管理员/项目管理员 | 普通用户 |
| --- | --- | --- | --- | --- |
| | 使用Yaml导入自定义资源 | | 仅已加入项目 | 仅已加入项目 |
| | 删除自定义资源 | | 仅已加入项目 | 仅已加入项目 |

# 1.6 使用限制

- 在Arm架构的云平台中，容器不支持使用GPU。
- 目前云平台支持在安全容器中使用英伟达GPU和百度昆仑XPU。

## 英伟达（NVIDIA）GPU

英伟达（NVIDIA）GPU均直接采用预装的450.80.02版本的NVIDIA GPU驱动，并且该驱动不支持卸载。该GPU驱动兼容的CUDA版本和支持的GPU设备如下表所示：

| 类型 | 型号 |
| --- | --- |
| 英伟达（NVIDIA）GPU设备 | Tesla V100 |
| | Tesla P100 |
| | Tesla P40 |
| | Tesla P6 |
| | Tesla P4 |
| | Tesla M60 |
| | Tesla M10 |
| | Tesla M6 |
| | Tesla T4 |
| | Quadro RTX 8000 |
| | Quadro RTX 6000 |
| CUDA版本 | CUDA 11.2及以下 |

## 百度昆仑XPU

百度昆仑XPU驱动支持的GPU设备如下表所示：

| 类型 | 型号 |
| --- | --- |
| 百度昆仑XPU设备 | R200-8F |

# 1.7 与其他服务的关系

| 服务 | 关系说明 |
| --- | --- |
| 容器镜像服务 | 创建工作负载时需要为容器指定所使用的容器镜像。 |
| 块存储 | 块存储为容器集群提供持久化存储资源。 |
| SDN网络服务 | 为安全容器服务提供网络、公网IP、负载均衡等网络资源及相关服务。 |

**咨询热线：400-100-3070**

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)