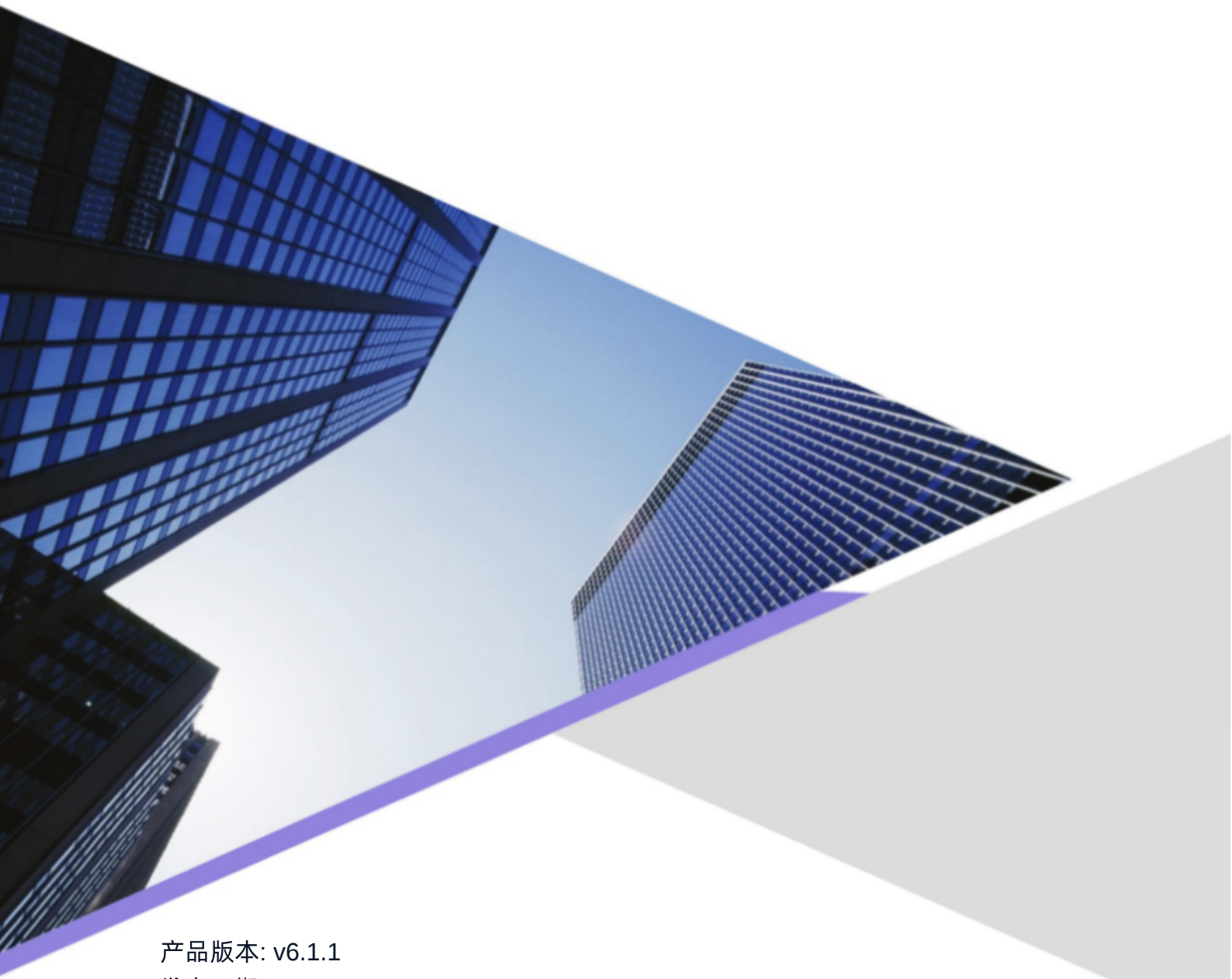
易捷行云
EasyStack

Kubernetes容器服务

产品介绍



产品版本: v6.1.1
发布日期: 2023-07-04

目录

1 产品介绍

1.1 什么是Kubernetes容器服务

Kubernetes容器服务提供高性能的容器应用管理服务，支持企业级Kubernetes容器化应用的生命周期管理，让用户轻松高效地在云端运行Kubernetes容器化应用。

产品优势

- **KCSP认证服务提供商**

  通过CNCF全球认证Kubernetes服务提供商（KCSP）和Kubernetes Training Partner（KTP）一致性验证，可提供专业的支持和服务。

- **Cloud Provider实现基础服务对接**

  Kubernetes通过Cloud Provider可以直接利用云平台实现持久化卷、负载均衡、网络路由、DNS解析以及横向扩展等功能。

- **灵活的应用托管方式**

  支持通过指定镜像、Chart模板、Yaml导入、自动化流水线等多种容器部署方式。

- **集群高可用**

  支持跨可用区部署集群，集群节点分布与多可用区实现高可用灾备。

  集群控制面支持3 Master HA 高可用，保障服务的连续性。

- **多计算架构支持**

  适配x86、Arm计算架构的主流芯片，例如intel、飞腾、鲲鹏。

- **多种部署形态**

  容器服务既能与云基础融合部署，无缝对接底层云平台能力。

主要功能

- **集群管理**

  以统一多集群管理为核心，支持利用底层云基础设施资源一键部署Kubernetes集群，并快速完成节点初始化。针对使用场景可选择部署不同规模的Kubernetes集群，例如：部署单个Master节点的测试环境，或部署多个Master节点的高可用生产环境。每个租户可以创建多个Kubernetes集群，支持对集群进行扩容、监控、删除等管理操作。

- **节点管理**

  支持对集群中的主机节点变更调度状态，在需要进行节点维护时，将节点设置为不可调度，并可将节点上运行的Pod迁移到其他节点上；支持节点的标签管理，创建应用时通过配置主机选择器可将应用部署在指定的节点上运行；用户也可以对节点进行污点设置，污点可以使节点排斥一类特定的Pod。

- **配额管理**

  在创建命名空间时，可选择目标集群，并为命名空间设置资源配额，包括容器 CPU、内存、存储容量、Pod数量等使用上限，从而合理分配资源，避免造成资源的浪费。

- **应用编排**

  支持通过界面或导入Yaml方式创建应用，在研发、运维、测试或生产环境中运行不同类型的业务。云平台的应用（Application）作为Kubernetes的CRD资源，由一个或多个关联的工作负载组成，支持不同的部署和使用需求，可添加的负载类型包括Deployment、DaemonSet和 StatefulSet，并支持网络、存储、监控、健康检查以及其它配置，实现对资源的统一编排和管理。

- **工作负载管理**

  云平台对于Kubernetes生态拥有良好的支持和兼容性，支持Kubernetes原生工作负载资源管理，并支持原生资源上浮到应用管理；支持已有Yaml原生资源导入、导出，轻松实现业务无间断迁移。用户可通过界面或Yaml创建和管理的工作负载包括部署（Deployment）、有状态副本集（StatefulSet）、守护进程集（DaemonSet）、任务（Job）、定时任务（CronJob）等。

- **容器管理**

  云平台提供对容器应用的全生命周期管理，主要功能包括：

  - 容器调度策略：支持指定目标主机调度、通过自定义标签规则进行主机调度及基于标签的亲和性/反亲和性调度。

- 健康检查：支持通过界面对容器设置不同的Liveness Check和Readiness Check规则。
- 伸缩策略：支持手动进行容器扩容和收缩，同时提供基于容器CPU、内存等资源使用率状态数值触发的自动扩缩容。
- 升级策略：可以设置的升级策略包括新旧容器启停顺序、更新批量大小等。
- 回滚：可指定历史部署版本进行一键回滚。
- 查看日志：支持通过界面实时查看容器日志信息。
- 登录终端：支持通过界面直接登录容器终端，方便后台控制人员执行命令行操作容器。
- 容器监控：支持对容器的CPU使用量、内存使用量、网络流入/流出速率等指标进行监控，并通过可视化图表展示。

- **网络管理**
  - 服务：服务是对Kubernetes原生Service资源的管理，支持类型包括ClusterIP、NodePort、LoadBalancer以及ExternalName。服务是容器服务的基本操作单元，将请求进行分发到后端的各个容器应用。对外表现为一个单一访问接口，这给扩展或维护后端带来很大的好处。
  - Ingress：支持对Kubernetes原生Ingress资源的管理，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。
  - 负载均衡：利用底层云基础设施负载均衡资源，可以提供集群内应用负载能力。可以支持四层协议和HTTP(S)七层协议的监听。支持权重、轮询等多种调度算法，支持会话保持，健康检查等设置。

- **存储服务**

  存储服务主要用于持久化存储容器的数据。由于容器服务重启或利用Kubernetes迁移时，数据会丢失，用户的业务程序会受到影响，因此需要用分布式存储块来保存容器内的关键数据。利用Kubernetes的存储支持接口，可以将常用的分布式存储系统动态挂载到容器服务中，在本系统框架中采用云基础设施的云硬盘进行数据存储，集群创建后默认创建一个对接云硬盘的存储类，同时支持对接高性能云存储。

- **配置中心**

  基于Kubernetes的ConfigMap和Secret资源，为容器服务提供配置管理的功能，实现容器中的相关配置的热更新，即不重启容器即可实现配置的即时生效。由于容器创建于镜像，用户在制作应用镜像后，在不同的部署环境下，需要不同的参数配置的设置。通常情况下，用户通过配置文件或环境变量进行设置。而在该云平

台系统下，可以将配置文件文本存放为ConfigMap，在需要时关联挂载到对应的应用容器中。ConfigMap用于普通配置管理，Secret 常用于密码、密钥或者证书的情况。

- **日志管理**

  日志服务模块对日志进行中心化管理，允许用户使用关键字和时间等筛选项完成对容器集群内容器等组件的运行日志的搜索，日志中心会保存用户对容器实例操作生成的日志，并统一化管理。可通过命名空间、所在集群、工作负载名称、容器组名称、容器名称、时间和关键字等进行检索。

- **监控管理**

  容器监控服务提供立体化全景监控功能，运维人员可以对容器集群、节点、服务组件、工作负载及容器组状态进行监控，实时了解集群资源的使用情况以及服务的健康状态，保证业务顺畅运行，帮助企业降低IT成本，提升运维效率。

1.2 使用场景

- **持续交付**

  配合DevOps服务，云平台基于代码源自动完成代码编译、镜像构建、测试、容器化部署等操作，实现一站式容器化交付流程，极大提高软件的发布效率，降低发布风险。

- **批处理任务**

  用户可以在Kubernetes容器集群中创建顺序或并行执行的任务型工作负载，支持一次性短任务和周期性任务。一次性运行的短任务，部署完成后即可执行。周期性任务可按照指定时间周期（如：每天上午8点执行）运行短任务，可进行定期时间同步、数据备份等。

- **微服务架构支持**

  微服务架构适用于构建复杂的应用，将单体应用从不同维度拆分成多个可管理的微服务，并可以自由选择开发技术，每个服务也可独立部署与扩展。应用通过微服务拆分，用户只需关注每个微服务迭代，由平台提供调度、编排、部署和发布能力。

- **弹性伸缩**

  根据访问流量进行业务策略化伸缩，避免流量激增扩容不及时导致系统故障，以及平时闲置资源造成的浪费。工作负载对应的一组Kubernetes Pod的CPU、内存负载平均值超过阈值时，可实现Pod层面的弹性伸缩。当集群资源不足时，可快速扩容集群节点，承载更多容器运行。

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）

Kubernetes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 Kubernetes 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 Kubernetes 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Kubernetes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Kubernetes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。

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。Kubernetes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Kubernetes，您无需修改应用程序即可使用不熟悉的服务发现机制。 Kubernetes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

1. 获取并安装“Kubernetes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“Kubernetes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Kubernetes容器服务。

   在顶部导航栏中，依次选择[产品与服务]-[Kubernetes容器服务]-[任意子菜单]，即可访问服务。

1.5 权限说明

本章节主要用于说明Kubernetes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	√	仅已加入项目	
	创建集群	仅Default/admin项目		
	开始/停止调度	√		
	标签管理	√		
	污点管理	√		
	扩容	√		
	删除	√		
命名空间	信息展示	√	仅已加入项目	
	创建命名空间			
	设置配额			
	设置成员			
	删除			
存储管理	信息展示	√	仅已加入项目	
	查看持久卷Yaml	√		
	删除持久卷	√		
	创建存储类	仅Default/admin项目		

功能		云管理员	部门管理员/项目管理员	普通用户
	设为/取消默认存储类	√		
	查看存储类Yaml	√		
	删除存储类	√		
运维管理	集群状态	√	仅已加入项目	
	日志查询			
应用管理	信息展示	√	仅已加入项目	仅已加入项目
	查看Yaml			
	添加负载			
	关联负载			
	启动/停止			
	重新部署			
	删除			
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			
	创建定时任务			
	容器配置			
	手动伸缩			

功能		云管理员	部门管理员/项目管理员	普通用户
	访问方式			
	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			
	查看Yaml			
	运行/停止定时任务			
	查看容器组Yaml			
	容器组日志			
	容器组终端			
	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			
日志查询	信息展示	√	仅已加入项目	仅已加入项目
	查询			

1.6 与其他服务的关系&区别

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。
计算服务	创建容器集群后平台将自动创建云主机作为集群节点。
块存储	块存储为容器集群提供持久化存储资源。
基础网络服务	选择安装基础网络服务时，它为Kubernetes容器服务提供网络、公网IP、负载均衡等网络资源和相关服务。
SDN网络服务	选择安装SDN网络服务时，它将为Kubernetes容器服务提供网络、公网IP等网络资源和相关服务。
独享型负载均衡服务	选择安装独享型负载均衡服务时，为Kubernetes容器服务提供独占负载均衡资源，能够轻松处理大量的业务访问请求，显著提升业务的容错能力和可用性。通过创建独享型负载均衡服务，可以从外部网络访问容器工作负载。

> 注意：
> - 「基础网络服务」和「SDN基础网络服务/独享型负载均衡服务」不能同时安装。
> - 当需要使用「独享型负载均衡服务」提供LoadBalancer能力时，需要在集群创建之前安装好云产品。

与其他服务的区别

服务	关系说明
安全容器服务	安全容器服务提供无服务容器引擎，用户无需创建和管理服务器集群即可运行容器应用。Kubernetes容器服务提供托管的容器集群及容器应用的全生命周期管理服务。

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)