ALIBABA CLOUD

阿里云

容器服务Kubernetes版

产品简介

文档版本：20220708

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

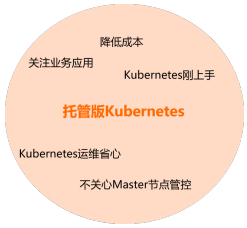
目录

1.什么是容器服务Kubernetes版

阿里云容器服务Kubernetes版（Alibaba Cloud Container Service for Kubernetes，简称容器服务ACK）是全球首批通过Kubernetes一致性认证的服务平台，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，让您轻松高效地在云端运行Kubernetes容器化应用。

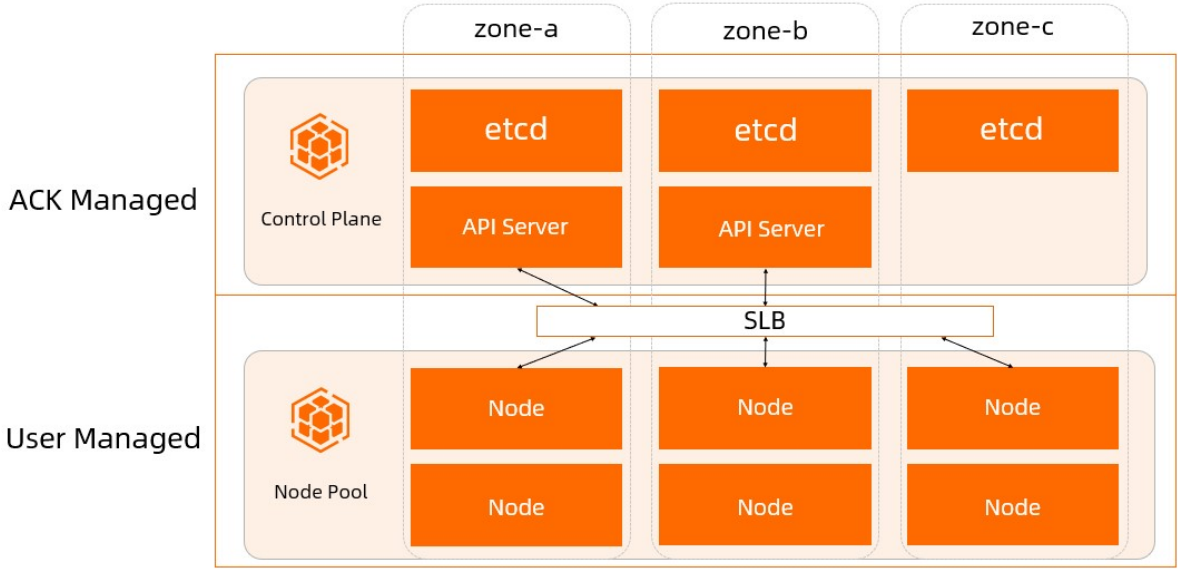
产品形态

ACK包含了专有版Kubernetes（Dedicated Kubernetes）、托管版Kubernetes（Managed Kubernetes）、Serverless Kubernetes三种形态，方便您按需选择。

比较项	专有版Kubernetes	托管版Kubernetes	Serverless Kubernetes
主要特点	您需要自行创建Master节点及Worker节点。	您只需创建Worker节点，Master节点由ACK创建并托管。	您无需创建Master节点及Worker节点。
	可以对集群基础设施进行更细粒度的控制，需要自行规划、维护、升级服务器集群。	简单、低成本、高可用，无需管理Master节点。	无需管理任何节点，可直接启动应用程序。
收费方式	集群管理免费，但需要承担Master节点、Worker节点以及其他基础资源的费用。	• 标准版：集群管理免费，但需要承担Worker节点以及其他基础资源的费用。 • Pro版：按照集群数量方式收费。	按容器实例的使用资源量和时长（秒）计费。
应用场景	适用于所有场景。	适用于所有场景。	适用于批量任务、突发扩容，以及CI/CD测试。
用户画像			

比较项	专有版Kubernetes	托管版Kubernetes	Serverless Kubernetes
集群创建	基本信息 名称、区域、网络、计费 ↓ Master节点 • 规格 • 系统盘 ↓ Worker节点 • 规格 • 数据盘 ↓ 集群配置 • NAT网关 • 公网SLB • 云监控插件 • 日志服务 • 网络插件	基本信息 名称、区域、网络、计费 ↓ Worker节点 • 规格 • 数据盘 ↓ 集群配置 • NAT网关 • 公网SLB • 云监控插件 • 日志服务 • 网络插件	基本信息 名称、区域、网络、计费 ↓ 创建应用

ACK集群系统架构



ACK托管版集群的管控面由ACK管理，向用户提供稳定、高可用、高性能、安全的Kubernetes服务。托管组件包括kube-apiserver、kube-controller-manager、ack-scheduler和etcd，每一个托管集群的管控面包含至少两个kube-apiserver实例和三个etcd实例，并且部署在不同的AZ可用区以提供Region级别的高可用性。ACK管控会持续监控托管组件，保障服务SLA，并且及时修复安全漏洞。

产品功能

- 集群管理
  - 集群创建：您可根据需求创建多种形态集群，选择类型丰富的工作节点，并进行灵活的自定义配置。更多信息，请参见创建ACK Pro版集群、创建Kubernetes托管版集群和创建Kubernetes专有版集群。
  - 集群升级：一键升级K8s版本，统一管理系统组件升级。更多信息，请参见升级ACK集群K8s版本。

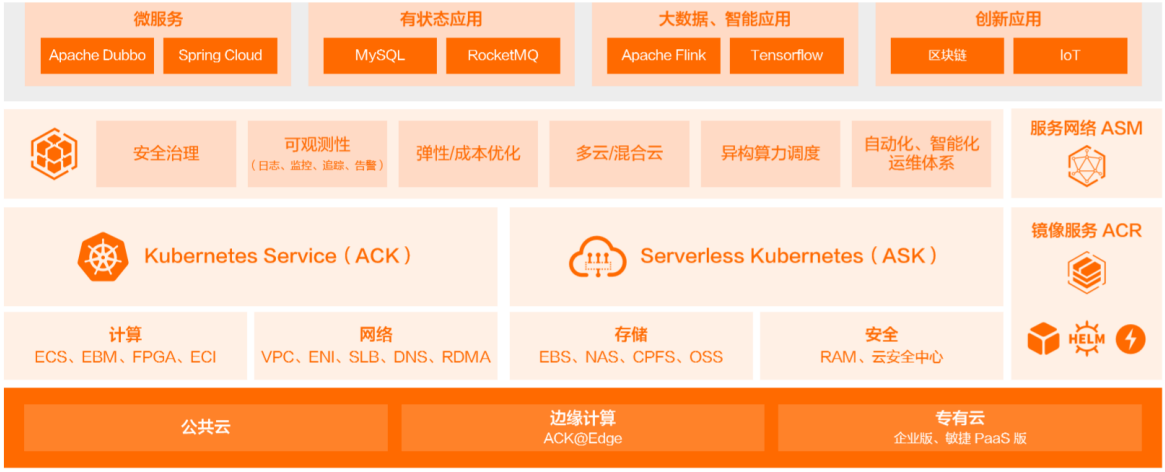
- 弹性伸缩：通过控制台一键垂直扩缩容来快速应对业务波动，同时支持服务级别的亲和性策略和横向扩展。
- 多集群管理：支持线下IDC和多云多区域的集群统一接入实现混合云应用管理。
- 授权管理：支持RAM授权和RBAC权限管理。

- 节点池
  支持节点池生命周期管理，支持在同一集群中配置不同规格的节点池，例如交换机、运行时、OS、安全组等。更多信息，请参见节点池概述。
- 应用管理
  - 应用创建：支持多种类型应用，从镜像、模版的创建，支持环境变量、应用健康、数据盘、日志等相关配置。
  - 应用全生命周期：支持应用查看、更新、删除，应用历史版本回滚、应用事件查看、应用滚动升级、应用替换升级以及通过触发器重新部署应用。
  - 应用调度：支持节点间亲和性调度、应用间亲和性调度、应用间反亲和性调度三种策略。
  - 应用伸缩：支持手动伸缩应用容器实例，HPA自动伸缩策略。
  - 应用发布：支持灰度发布和蓝绿发布。
  - 应用目录：支持应用目录，简化云服务集成。
  - 应用中心：应用部署后，以统一的视角展现整体应用的拓扑结构，同时对于持续部署等场景进行统一的版本管理与回滚。
  - 应用备份和恢复：支持对Kubernetes应用进行备份和恢复。更多信息，请参见备份和恢复应用。
- 存储
  - 存储插件：支持Flexvolume以及CSI存储插件。更多信息，请参见存储CSI概述和存储Flexvolume概述。
  - 存储卷和存储声明：
    - 支持创建块存储、NAS、OSS、CPFS类型的存储卷。
    - 支持持久化存储卷声明（PVC）挂接存储卷。
    - 支持存储卷的动态创建和迁移。
    - 支持以脚本方式查看和更新存储卷和存储声明。
- 网络
  - 支持Flannel容器网络和Terway容器网络。更多信息，请参见网络概述。
  - 支持定义Sevice和Pod的CIDR。
  - 支持NetworkPolicy。更多信息，请参见使用网络策略Network Policy。
  - 支持路由Ingress。
  - 支持服务发现DNS。更多信息，请参见DNS概述。
- 运维与安全
  - 可观测性：
    - 监控：支持集群、节点、应用、容器实例层面的监控；支持prometheus插件。
    - 日志：支持集群日志查看；支持应用日志采集；支持容器实例日志查看。
    - 报警：支持容器服务异常事件报警，以及容器场景指标报警。更多信息，请参见容器服务报警管理。
  - 成本分析：支持可视化集群资源使用量及成本分布，以提升集群资源利用率。
  - 安全中心：支持运行时刻的安全策略管理，应用安全配置巡检和运行时刻的安全监控和告警，提升容器安全整体纵深防御能力。

- 安全沙箱：可以让应用运行在一个轻量虚拟机沙箱环境中，拥有独立的内核，具备更好的安全隔离能力。适用于不可信应用隔离、故障隔离、性能隔离、多用户间负载隔离等场景。
- 机密计算：基于Intel SGX提供的可信应用或用于交付和管理机密计算应用的云原生一站式机密计算平台，帮助您保护数据使用中的安全性、完整性和机密性。机密计算可以让您把重要的数据和代码放在一个特殊的可信执行加密环境。

产品架构

阿里云容器服务产品线的整体架构如下图所示。



- 阿里云容器镜像服务ACR（Alibaba Cloud Container Registry）：提供云原生资产的安全托管和全生命周期管理，支持多场景下镜像的高效分发，与容器服务ACK无缝集成，打造云原生应用一站式解决方案。
- 阿里云服务网格ASM（Alibaba Cloud Service Mesh）：是一个托管式的微服务应用流量统一管理平台，兼容Istio，支持多个Kubernetes集群统一流量管理，为容器和虚拟机应用服务提供一致性的通信控制。
- 阿里云Serverless Kubernetes ASK（Alibaba Cloud Serverless Kubernetes）：是阿里云基于弹性计算架构推出的无服务器Kubernetes容器服务，让您无需管理和维护集群，即可快速创建Kubernetes容器应用。
- 阿里云基因计算AGS（Alibaba Cloud Genomics Service）：是阿里云基于容器Kubernetes技术面向生物行业用户提供的基因大数据计算服务，具有高效、弹性、可靠的优点，相比传统的基因计算过程速度更快，成本更低。
- 阿里云边缘容器服务ACK@Edge：基于标准Kubernetes运行环境，提供云、边、端一体的容器应用交付、运维和管控能力，同时加强在边缘业务场景下自治能力。

客户原声

以下是客户对ACK的评价。

洋葱学院

针对疫情延期开学，洋葱学院作为头部K12在线教育公司，免费向全国师生开放了平台的全部核心课程资源，这期间每天的学习访问人数持续飙升。使用云容器之后，系统在资源利用率上提升了约60%，出现问题后可快速隔离，当面对急剧增长的业务量，也可以在短时间内完成扩容，支撑业务快速发展。

洋葱学院 ONION ACADEMY

申通基于阿里云容器服务ACK搭建了通用云原生计算平台，解决了传统应用升级缓慢、架构臃肿、不能快速迭代等问题。在成本、稳定性、效率、赋能业务等四个维度获得显著成效。目前每天处理订单量在千万级别，处理物流轨迹在亿级别，每天产生的数据量在1T，使用1300+个计算节点来实时处理业务。

申通快递 STO EXPRESS

阿里云是Kubernetes和其他CNCF项目在中国的主要贡献者，所以我们非常信任他们。他们帮我们启动了这次基于阿里云容器服务ACK的云原生转型，开发和运维效率提高了3倍，CPU的资源利用率和存储翻了一番，部署时间从若干小时缩短到若干分钟，故障时间也减少了50%。ACK帮助民生实现创新业务的快速增长。

中国民生银行 CHINA MINSHENG BANK

使用ACK

单击下方按钮可立即使用ACK。

立即使用ACK

ACK用户交流群

如果您在使用ACK过程中有任何疑问，欢迎您点击链接加入组织，然后使用钉钉扫描二维码加入钉钉交流群。

学习资源

- ACK Workshop
- CNCF × Alibaba 云原生技术公开课
- 阿里云云原生容器工程师ACP认证课程
- Kubernetes官网

2.产品优势

本文介绍容器服务ACK的优势以及自建Kubernetes的劣势。

ACK的优势

优势	说明
强大的集群管理	• 三种集群形态：专有版Kubernetes集群、托管版Kubernetes集群、Serverless Kubernetes集群。 • 托管版Kubernetes集群的管控节点默认为3个可用区的高可用部署。 • 单集群支持千量级ECS节点。详细配额，请参见ACK集群配额限制。 • 支持跨可用区集群以及注册外部集群。关于注册集群的介绍，请参见注册集群概述。
极致弹性的资源扩缩	• 根据容器资源使用情况，快速自动地调整容器数量。 • 数分钟内扩展到上千个节点。 • 如果您使用了Serverless Kubernetes 版 (ASK) 和弹性容器实例ECI，可在30秒内启动500个容器组。 • 支持一键垂直扩缩容。 • 支持服务级别的亲和性策略和横向扩展。 • 提供社区标准的HPA、VPA、Autoscaler等能力。 • 提供类似CronHPA的定时伸缩能力，vk-autoscaler的无服务器弹性能力等。 • 针对在线业务提供elastic workload的精细化调度弹性能力。 • 针对不同的弹性场景提供了alibaba-metrics-adapter，实现诸如Ingress网关、Sentinel微服务限流等应用层弹性场景优化。

一站式容器管理	• 应用管理：
	  ◦ 支持灰度发布，蓝绿发布、应用监控，应用弹性伸缩。
	  ◦ 内置应用商店，支持一键部署Helm应用。
	• 镜像仓库（什么是容器镜像服务ACR）：
	  ◦ 高可用，支持大并发。
	  ◦ 支持镜像加速。
	  ◦ 支持大规模P2P分发，可自动执行并优化基本镜像分发流程，最大分发到1万个节点，效率提升4倍。
	  说明 您如果使用自建的镜像仓库，在百万级的客户端同时拉取镜像的时候，会存在镜像仓库崩溃的可能性。使用容器服务ACR可以提高镜像仓库的可靠性，减少运维负担和升级压力。
	• 日志：
	  ◦ 支持日志采集及将采集的日志集成到日志服务。
	  ◦ 支持集成第三方开源日志解决方案。
	• 监控：
	  ◦ 支持容器级别和VM级别的监控。
	  ◦ 支持集成第三方开源监控解决方案。

优势	说明

丰富的工作节点	• 按资源类型划分：
	  ◦ x86计算资源：x86计算类型ECS。
	  ◦ 异构计算资源：GPU ECS、NPU ECS、FPGA ECS。
	  ◦ 裸金属计算资源：神龙服务器。
	  ◦ Serverless计算资源：ACK virtual node。
	  ◦ 边缘节点：ACK@Edge支持统一管理云端和边缘节点，以及统一的应用发布，发布效率提升3倍。
	• 按付费模式划分：
	  ◦ 抢占式实例
	  ◦ 包年包月
	  ◦ 按量付费

最优的IaaS层能力	• 网络：
	  ◦ 提供高性能VPC/ENI网络插件，性能比普通网络方案提升20%。
	  ◦ 支持容器访问策略和流控限制。
	• 存储：
	  ◦ 支持阿里云云盘、文件存储NAS、对象存储OSS，提供标准的CSI驱动。
	  ◦ 支持存储卷的动态创建和迁移。
	• 负载均衡：
	支持创建负载均衡实例（公网、内网）。
	说明 如果您在使用自建Kubernetes集群的过程中，使用自建的Ingress，频繁的业务发布可能会造成Ingress的配置压力并增加出错概率。容器服务ACK的SLB方案支持原生的阿里云高可用负载均衡，可以自动完成网络配置的修改和更新。该方案经历了大量用户长时间的使用，稳定性和可靠性都大大超过自建Ingress方案。

优势	说明

企业级的安全稳定	在开发生命周期之初便集成了多层安全防护功能，从底层基础设施到中间软件供应链，再到顶层运行时环境，为云原生架构提供全面保护。
	• 端到端的安全能力：
	  ○ 基础架构安全：支持全方位网络安全隔离管控和全链路数据加密，提供阿里云主子账号和Kubernetes RBAC权限体系的联动，并支持细粒度的权限管理和完备的审计能力。
	  ○ 软件供应链安全：支持镜像扫描、安全云原生交付链、镜像签名、镜像扫描、镜像同步构成的完整DevSecOps。
	  ○ 运行时安全：提供应用维度的安全策略管理，配置巡检，运行时刻监控和告警，密钥加密和管理等运行时刻的纵深防御能力。
	• 默认安全：
	  ○ 提供容器优化的操作系统镜像，提供经过稳定测试和安全加固的Kubernetes集群和Docker版本。
	  ○ 基于CIS Benchmark和容器安全最佳实践，对集群配置和系统组件/镜像的安全合规进行加固。
	  ○ 节点默认云资源权限的最小化收敛。
	• 安全沙箱：可以让应用运行在一个轻量虚拟机沙箱环境中，拥有独立的内核，具备更好的安全隔离能力。适用于不可信应用隔离、故障隔离、性能隔离、多用户间负载隔离等场景。
	• 机密计算：基于Intel SGX提供的可信应用或用于交付和管理机密计算应用的云原生一站式机密计算平台，帮助您保护数据使用中的安全性、完整性和机密性。机密计算可以让您把重要的数据和代码放在一个特殊的可信执行加密环境。

全天候技术支持	通过工单系统，为您提供7*24小时的专业技术支持。

自建Kubernetes的劣势

- 搭建集群繁琐。
  您需要手动配置Kubernetes相关的各种组件、配置文件、证书、密钥、相关插件和工具，整个集群搭建工作需要花费专业人员数天到数周的时间。
- 在公共云上，需要投入大量的成本实现和云产品的集成。
  与阿里云上其他产品的集成，需要您自己投入成本来实现，如日志服务、监控服务和存储管理等。
- 容器是一个系统性工程，涉及网络、存储、操作系统、编排等各种技术，需要专门的人员投入。
- 容器技术一直在不断发展，版本迭代快，需要不断地试错、升级、测试。

3.应用场景

本文主要为您介绍容器服务 ACK 的常见应用场景。

DevOps 持续交付

最优化的持续交付流程

配合 Jenkins 帮您自动完成从代码提交到应用部署的 DevOps 完整流程，确保只有通过自动测试的代码才能交付和部署，高效替代业内部署复杂、迭代缓慢的传统方式。

能够实现：

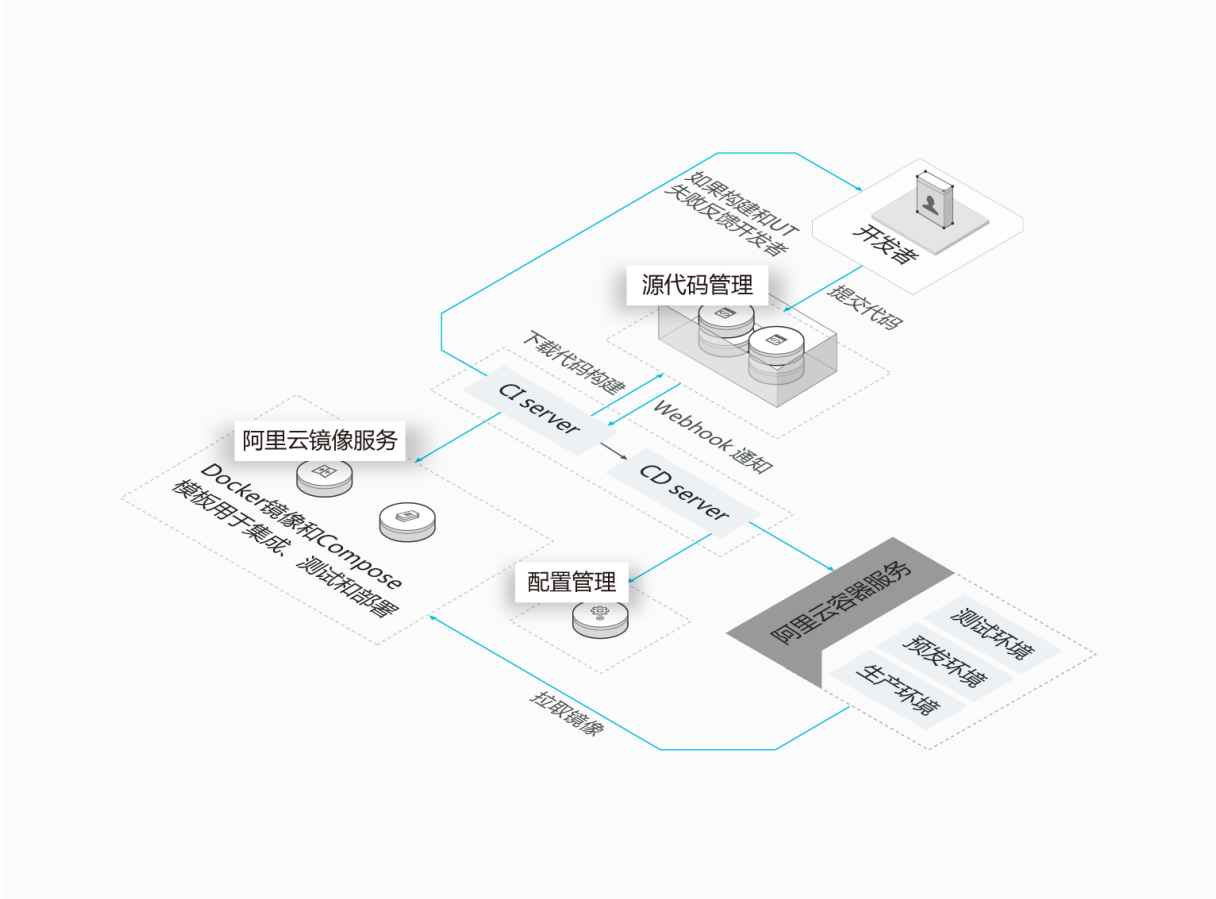
- DevOps 自动化
  实现从代码变更到代码构建、镜像构建和应用部署的全流程自动化。
- 环境一致性
  容器技术让您交付的不仅是代码，还有基于不可变架构的运行环境。
- 持续反馈
  每次集成或交付，都会将结果实时反馈。

推荐搭配使用：

云服务器 ECS + 容器服务

相关文档：

容器应用DevOps for ACK集群



基于云原生技术的机器学习

专注机器学习本身，快速实现从 0 到 1

帮助数据工程师在异构计算资源集群上轻松开发、部署机器学习应用，跟踪试验和训练、发布模型，自动集成多种数据部署在分布式存储系统，加速训练数据读写，无需关心繁琐部署运维，专注核心业务，快速从 0 到 1。

能够实现：

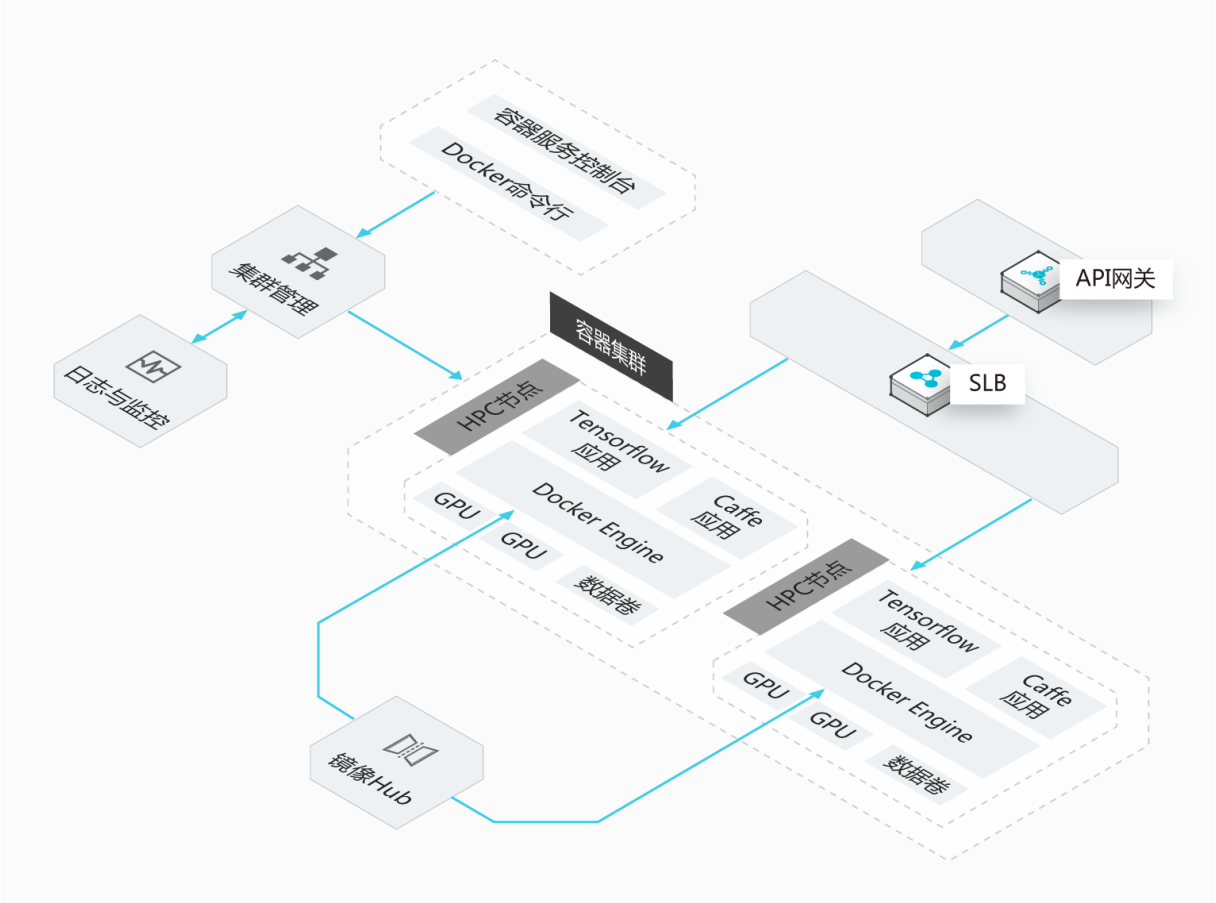
- 支持生态
  内置对 TensorFlow、Caffe、 MXNet、Pytorch 等主流深度学习计算框架支持和优化。
- 快速弹性
  一键部署机器学习开发、训练、推理服务，秒级启动和弹性伸缩。
- 简单可控
  轻松创建、管理大规模 GPU 计算集群，并且可以监控 GPU 利用率等核心指标。
- 深度整合
  无缝接入阿里云存储、日志监控和安全基础架构能力。

推荐搭配使用：

云服务器 ECS / GPU 服务器 EGS / 高性能计算服务 （Alibaba Cloud HPC）+ 容器服务 + 对象存储 OSS / 文件存储 NAS / CPFS

相关文档：

- PyTorch分布式训练
- TensorFlow分布式训练



微服务架构

实现敏捷开发和部署落地，加速企业业务迭代

企业生产环境中，通过合理微服务拆分，将每个微服务应用存储在阿里云镜像仓库帮您管理。您只需迭代每个微服务应用，由阿里云提供调度、编排、部署和灰度发布能力。企业生产环境中，通过合理的微服务拆分，可以享受微服务带来的高内聚、低耦合、高容错性的优势。在微服务上生产的过程，依托于阿里云产品提供的微服务治理能力。

可以在不修改任何代码和配置的情况下，实现：

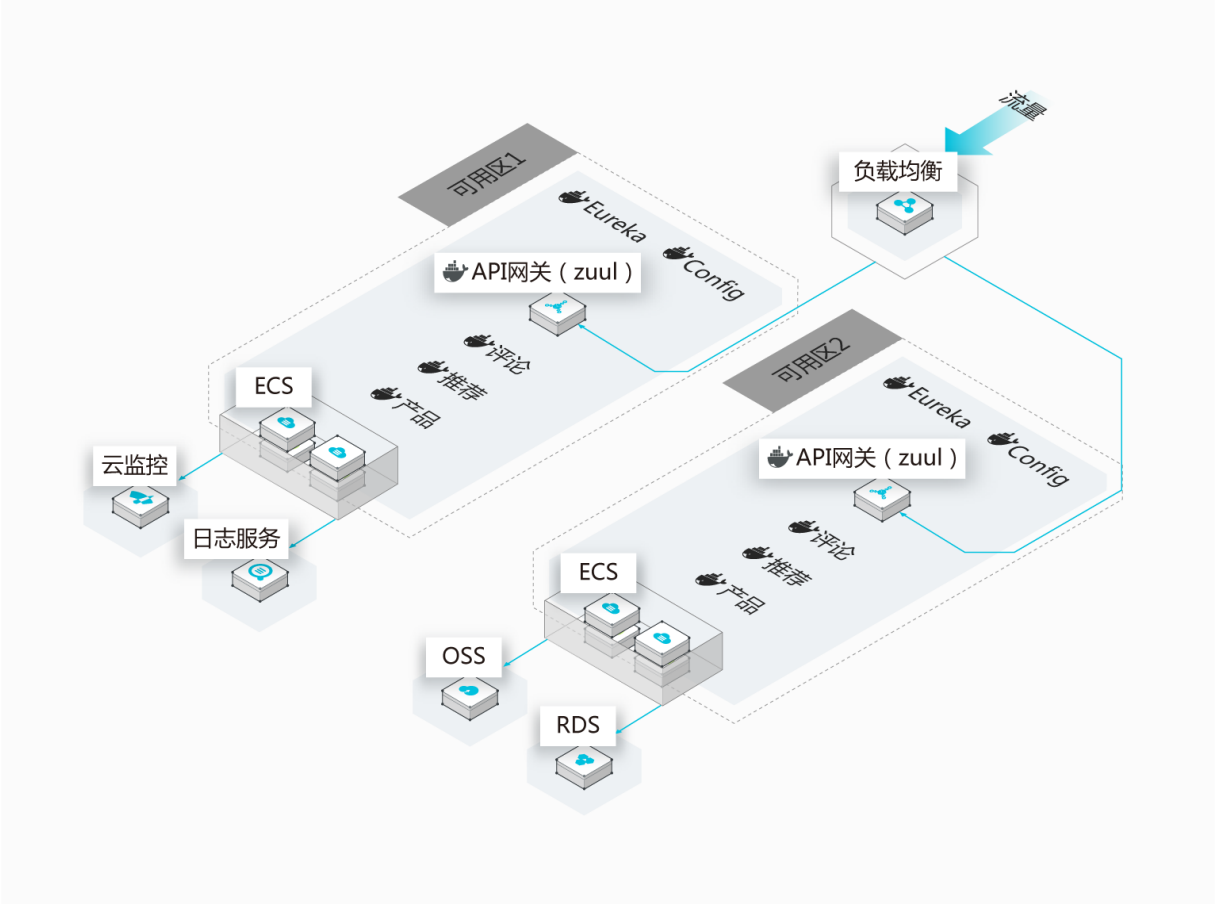
- 全面消除变更过程中的风险
  依托于配置管理、无损上下线和全链路灰度能力，全面消除变更过程中的风险。
- 全面消除偶发问题引发的风险
  依托于限流、降级、熔断、隔离等能力，可以在出现偶发的流量洪峰和依赖服务出异常时，有效地限流保护、削峰填谷、隔离故障、降级保护。
- 低成本实现微服务敏捷开发
  依托于开发环境隔离能力，可以在不增加物理机器成本的前提下，低成本扩展出多套逻辑隔离的开发环境，有效地解决环境抢占和冲突问题，实现敏捷开发。

推荐搭配使用：

微服务引擎 MSE + 云服务器 ECS + 云数据库 RDS 版 + 对象存储 OSS + 容器服务

相关文档：

- 微服务敏捷开发最佳实践
- 基于MSE实现微服务应用无损上下线
- 配置基于Java微服务网关的全链路灰度



混合云架构

统一运维多个云端资源

在容器服务控制台上同时管理云上云下的资源，不需在多种云管理控制台中反复切换。基于容器基础设施无关的特性，使用同一套镜像和编排同时在云上云下部署应用。

能够实现：

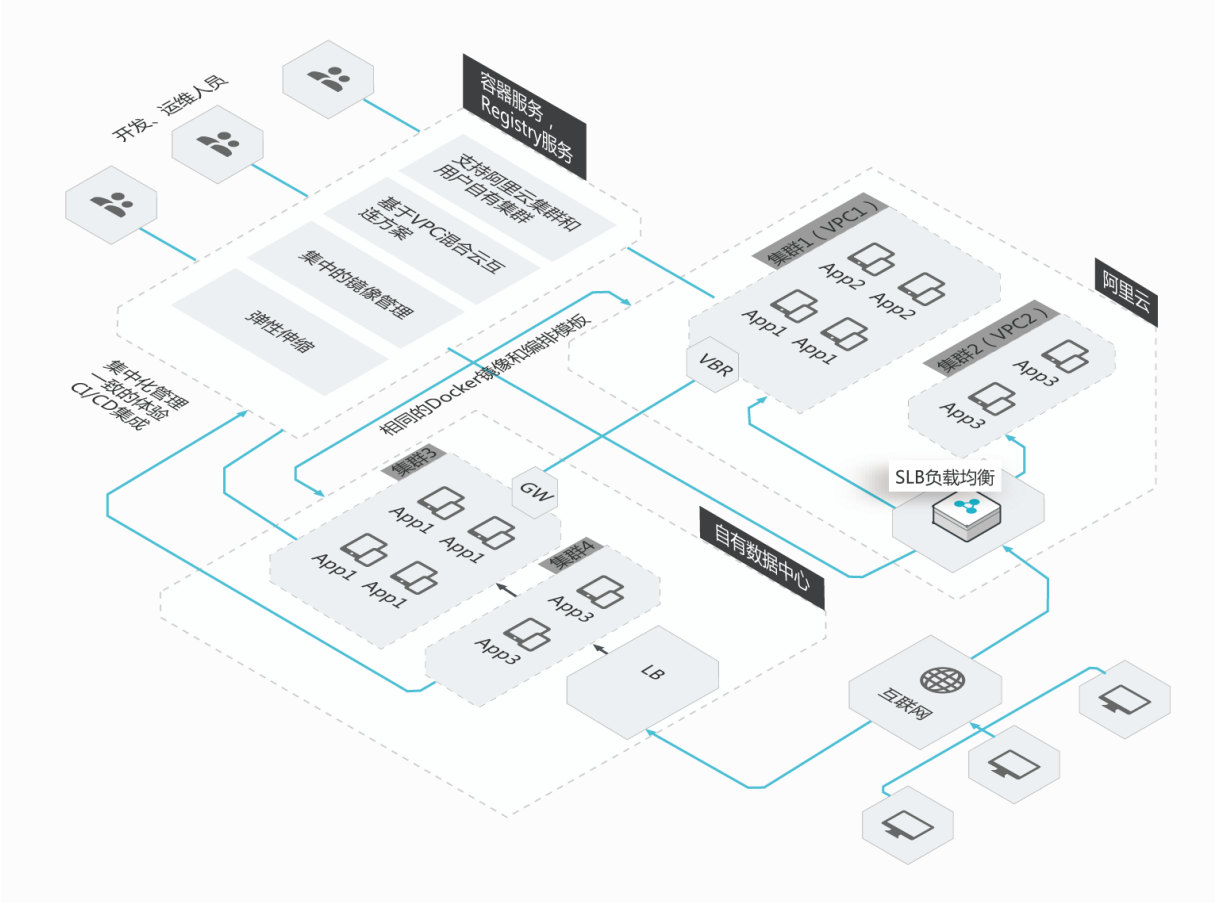
- 在云上伸缩应用
  业务高峰期，在云端快速扩容，把一些业务流量引到云端。
- 云上容灾
  业务系统同时部署到云上和云下，云下提供服务，云上容灾。
- 云下开发测试
  云下开发测试后的应用无缝发布到云上。

推荐搭配使用：

云服务器 ECS + 专有网络 VPC + 高速通道（Express Connect）

相关文档：

- 通过image-syncer工具迁移容器镜像
- 创建混合集群
- 备份中心概述
- 使用配置巡检功能检查注册集群Workload安全隐患
- 使用ACK One构建应用系统的两地三中心容灾方案



弹性伸缩架构

根据业务流量自动对业务扩容/缩容

容器服务可以根据业务流量自动对业务扩容/缩容，不需要人工干预，避免流量激增扩容不及时导致系统崩溃，以及平时大量闲置资源造成浪费。

能够实现：

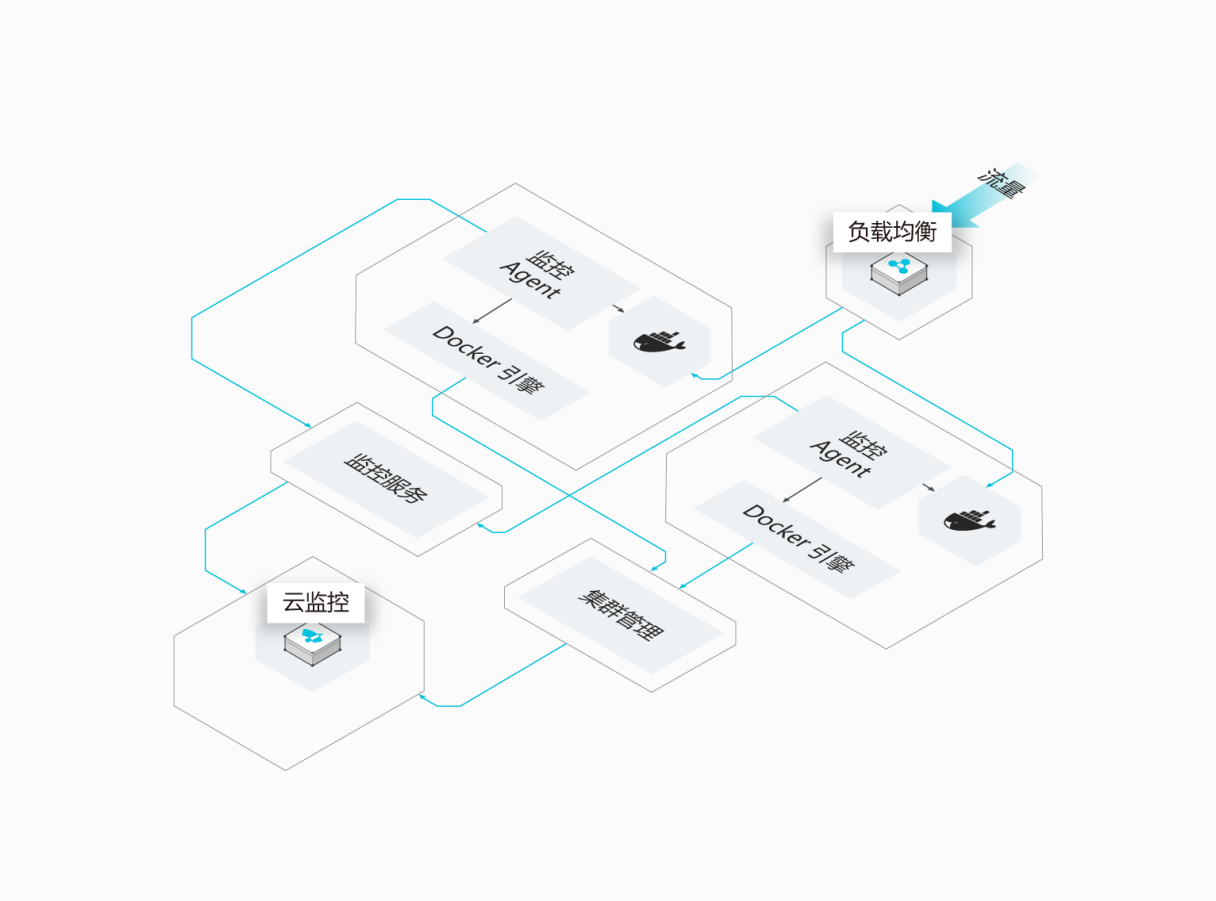
- 快速响应
  业务流量达到扩容指标，秒级触发容器扩容操作。
- 全自动
  整个扩容/缩容过程完全自动化，无需人工干预。
- 低成本
  流量降低自动缩容，避免资源浪费。

推荐搭配使用：

云服务器 ECS + 云监控

相关文档：

- 基于阿里云Prometheus指标的容器水平伸缩
- 通过Nginx Ingress对多个应用进行HPA



4.基本概念

在使用容器服务ACK前，需理解该产品所涉及的概念。本文为您介绍使用容器服务ACK过程中遇到的常用名词的基本概念和简要描述，以便于您更好地理解ACK产品。

集群

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、负载均衡、专有网络等云资源。

ACK支持的集群类型如下表。

集群类型	描述
Pro托管集群	ACK Pro托管集群是在ACK标准托管版基础上针对企业大规模生产环境进一步增强了可靠性、安全性，并且提供可赔付的SLA的Kubernetes集群。
标准托管集群	只需创建Worker节点，Master节点由容器服务创建并托管。具备简单、低成本、高可用、无需运维管理Kubernetes集群Master节点的特点。
专有集群	需要创建3个Master（高可用）节点及若干Worker节点，可对集群基础设施进行更细粒度的控制，需要自行规划、维护、升级服务器集群。
异构计算集群	ACK异构计算集群，是阿里云推出的支持英伟达GPU，含光NPU等异构节点，并且可以与传统CPU节点混合部署的集群，无需关心驱动的安装和管理，支持主流的AI计算框架，并且支持GPU和NPU的多容器共享和隔离。
安全沙箱集群	创建一个以弹性裸金属（神龙）实例为工作节点的集群，神龙服务器为您提供超高性能容器实例，适合高负载、高带宽需求的业务场景。
加密计算集群	创建一个基于Intel SGX加密计算的托管集群，可以保护您的敏感代码和数据，适合隐私数据保护、区块链、密钥、知识产权、生信基因计算等场景。
边缘集群	边缘托管版是针对边缘计算场景推出的云边一体化协同托管方案。边缘托管集群采用非侵入方式增强，提供边缘自治、边缘单元、边缘流量管理、原生运维API支持等能力，以原生方式支持边缘计算场景下的应用统一生命周期管理和统一资源调度。
ASK集群	无需创建和管理Master节点及Worker节点的Serverless集群，即可通过控制台或者命令配置容器实例的资源、指明应用容器镜像以及对外服务的方式，直接启动应用程序。
注册集群	注册集群是用于将本地数据中心Kubernetes集群或其他云厂商Kubernetes集群接入ACK服务平台统一管理的集群形态。

节点

一台服务器（可以是虚拟机实例或者物理服务器）已经安装了Docker Engine，可以用于部署和管理容器。容器服务ACK的Agent程序会被安装到节点上并注册到一个集群上。集群中的节点数量可以伸缩。

节点池

节点池是集群中全都具有相同配置的一组节点，节点池可以包含一个或多个节点。

ACK节点池类型分为节点池和托管节点池。

节点池类型	描述

节点池类型	描述
节点池	节点池是集群中具有相同配置的一组节点，节点池可以包含一个或多个节点。节点池后端与弹性伸缩组实例一比一对应。当对节点池进行扩容和缩容时，ACK通过弹性伸缩服务下发扩容和移除节点的操作。您可以根据自己的需要创建和管理多个节点池。 **注意** 由于默认节点池中安装了部分系统组件，弹性伸缩时可能会造成集群功能的不稳定。如果您需要实现弹性伸缩功能，建议您另建节点池。
托管节点池	托管节点池是ACK全新推出的自动化运维型节点池，可以自动完成部分节点运维操作，如CVE更新、部分故障修复等，从而降低您的节点运维负担。 更多信息，请参见托管节点池概述。

专有网络VPC

专有网络VPC是您自己独有的云上私有网络。您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等，您可以在自己定义的专有网络中使用阿里云资源如云服务器、云数据库RDS版和负载均衡等。

安全组

安全组是一种虚拟防火墙，具备状态检测和数据包过滤能力，用于在云端划分安全域。安全组是一个逻辑上的分组，由同一地域内具有相同安全保护需求并相互信任的实例组成。

应用目录

应用目录功能集成了Helm，提供了Helm的相关功能，并进行了相关功能扩展，例如提供图形化界面。

编排模板

编排模板是一种保存Kubernetes YAML格式编排文件的方式。

Knative

Knative是基于Kubernetes的Serverless框架。其目标是制定云原生、跨平台的Serverless编排标准。

Kubernetes

Kubernetes是一个开源平台，具有可移植性和可扩展性，用于管理容器化的工作负载和服务，简化了声明式配置和自动化。

容器（Container）

打包应用及其运行依赖环境的技术，一个节点可运行多个容器。

镜像（Image）

容器镜像是容器应用打包的标准格式，封装了应用程序及其所有软件依赖的二进制数据。在部署容器化应用时可以指定镜像，镜像可以来自于Docker Hub，阿里云镜像服务，或者用户的私有镜像仓库。镜像ID可以由镜像所在仓库URI和镜像Tag（默认为 `latest` ）唯一确认。

镜像仓库（Image Registry）

容器镜像仓库是一种存储库，用于存储Kubernetes和基于容器应用开发的容器镜像。

管理节点（Master Node）

管理节点是Kubernetes集群的管理者，运行着的服务包括kube-apiserver、kube-scheduler、kube-controller-manager、etcd组件，和容器网络相关的组件。

工作节点（Worker Node）

工作节点是Kubernetes集群中承担工作负载的节点，可以是虚拟机也可以是物理机。工作节点承担实际的Pod调度以及与管理节点的通信等。一个工作节点上的服务包括Docker运行时环境、kubelet、Kube-Proxy以及其它一些可选的组件。

命名空间（Namespace）

命名空间为Kubernetes集群提供虚拟的隔离作用。Kubernetes集群初始有3个命名空间，分别是默认命名空间default、系统命名空间kube-system和kube-public，除此以外，管理员可以创建新的命名空间以满足需求。

容器组（Pod）

Pod是Kubernetes部署应用或服务的最小的基本单位。一个Pod封装多个应用容器（也可以只有一个容器）、存储资源、一个独立的网络IP以及管理控制容器运行方式的策略选项。

副本控制器（Replication Controller，RC）

RC确保任何时候Kubernetes集群中有指定数量的Pod副本在运行。通过监控运行中的Pod来保证集群中运行指定数目的Pod副本。指定的数目可以是多个也可以是1个；少于指定数目，RC就会启动运行新的Pod副本；多于指定数目，RC就会终止多余的Pod副本。

副本集（ReplicaSet，RS）

ReplicaSet（RS）是RC的升级版本，唯一区别是对选择器的支持，RS能支持更多种类的匹配模式。副本集对象一般不单独使用，而是作为Deployment的理想状态参数使用。

工作负载（Workload）

工作负载是在Kubernetes上运行的应用程序。工作负载包括以下几种类型：

工作负载类型	描述
无状态工作负载（Deployment）	无状态工作负载表示对Kubernetes集群的一次更新操作。适用于运行完全独立、功能相同应用的场景。
有状态工作负载（StatefulSet）	有状态工作负载支持应用部署、扩容、滚动升级时有序进行。如果希望使用存储卷为工作负载提供持久存储，可以使用StatefulSet作为解决方案的一部分。
守护进程集（DaemonSet）	守护进程集确保全部（或者某些）节点上运行一个Pod。与Deployment不同，DaemonSet会在指定的节点上都部署定义的Pod，确保这些节点都运行守护进程Pod。适用集群的日志、监控等部署场景。
任务（Job）	Job指运行一次性的任务。您可以使用Job以并行的方式运行多个 Pod。
定时任务（CronJob）	CronJob指根据规划时间周期性地运行反复的任务。适用于执行数据备份或者发送邮件的场景。
自定义资源（CustomResourceDefinitions，CRD）	在庞大的Kubernetes生态系统中，您可以通过CRD添加第三方工作负载资源。CRD资源允许您定义定制资源。

标签（Label）

Labels的实质是附着在资源对象上的一系列Key/Value键值对，用于指定对用户有意义的对象的属性，标签对内核系统是没有直接意义的。标签可以在创建一个对象的时候直接赋予，也可以在后期随时修改，每一个对象可以拥有多个标签，但key值必须唯一。

服务（Service）

Service是Kubernetes的基本操作单元，是真实应用服务的抽象，每一个服务后面都有很多对应的容器来提供支持，通过Kube-Proxy的ports和服务selector决定服务请求传递给后端的容器，对外表现为一个单一访问接口。

路由（Ingress）

Ingress是授权入站连接到达集群服务的规则集合。您可以通过Ingress配置提供外部可访问的URL、负载均衡、SSL、基于名称的虚拟主机等。通过POST Ingress资源到API Server的方式来请求Ingress。Ingress Controller负责实现Ingress，通常使用负载均衡器，它还可以配置边界路由和其他前端，这有助于以高可用的方式处理流量。

配置项（ConfigMap）

配置项可用于存储细粒度信息如单个属性，或粗粒度信息如整个配置文件或JSON对象。您可以使用配置项保存不需要加密的配置信息和配置文件。

保密字典（Secret）

保密字典用于存储在Kubernetes集群中使用一些敏感的配置，例如密码、证书等信息。

卷（Volume）

和Docker的存储卷有些类似，Docker的存储卷作用范围为一个容器，而Kubernetes的存储卷的生命周期和作用范围是一个Pod。每个Pod中声明的存储卷由Pod中的所有容器共享。

存储卷（Persistent Volume，PV）

PV是集群内的存储资源，类似节点是集群资源一样。PV独立于Pod的生命周期，可根据不同的StorageClass类型创建不同类型的PV。

存储卷声明（Persistent Volume Claim，PVC）

PVC是资源的使用者。类似Pod消耗节点资源一样，而PVC消耗PV资源。

存储类（StorageClass）

存储类可以实现动态供应存储卷。通过动态存储卷，Kubernetes将能够按照用户的需要，自动创建其所需的存储。

弹性伸缩（Autoscaling）

弹性伸缩是根据业务需求和策略，经济地自动调整弹性计算资源的管理服务。典型的场景包含在线业务弹性、大规模计算训练、深度学习GPU或共享GPU的训练与推理、定时周期性负载变化等。ACK支持的弹性伸缩服务如下表。

弹性伸缩维度	弹性伸缩分类	描述
调度层弹性	容器水平伸缩（HPA）	ACK容器水平伸缩基于CPU使用率自动扩缩Pod数量。适用于Deployment、StatefulSet等实现了scale接口的对象。
	容器定时伸缩（CronHPA）	应对资源浪费的场景，ACK提供kubernetes-cronhpa-controller组件，实现资源定时扩容。适用于Deployment、StatefulSet等实现了scale接口的对象。此外CronHPA提供了HPA对象的兼容能力，您可以同时使用CronHPA与HPA。

弹性伸缩维度	弹性伸缩分类	描述
	容器垂直伸缩（VPA）	容器垂直伸缩会基于Pod的资源使用情况自动为集群设置资源占用的限制，从而让集群将Pod调度到有足够资源的最佳节点上。容器垂直伸缩也会保持最初容器定义中资源 `request` 和 `limit` 的占比。适用于无法水平扩展的应用，通常是在Pod出现异常恢复时生效。
资源层弹性	节点自动伸缩	ACK的自动伸缩能力是通过节点自动伸缩组件实现的，可以按需弹出普通实例、GPU实例、竞价付费实例，支持多可用区、多实例规格、多种伸缩模式，满足不同的节点伸缩场景。全场景支持，适合在线业务、深度学习、大规模成本算力交付等。

可观测性（Observability）

Kubernetes可观测性体系包含监控和日志两部分，监控可以帮助开发者查看系统的运行状态，而日志可以协助问题的排查和诊断。

Helm

Helm是Kubernetes包管理平台。Helm将一个应用的相关资源组织成为Charts，然后通过Charts管理程序包。

节点亲和性（nodeAffinity）

节点亲和性指通过Worker节点的Label标签控制Pod部署在特定的节点上。

污点（Taints）

污点和节点亲和性相反，它使节点能够排斥一类特定的Pod。

容忍（Tolerations）

应用于Pod上，允许（但并不要求）Pod调度到带有与之匹配的污点的节点上。

应用亲和性（podAffinity）

应用亲和性决定应用Pod可以和特定Pod部署在同一拓扑域。例如，对于相互通信的服务，可通过应用亲和性调度，将其部署到同一拓扑域（例如同一个主机）中，以减少它们之间的网络延迟。

应用反亲和性（podAntiAffinity）

应用反亲和性决定应用Pod不与特性Pod部署在同一拓扑域。例如，将一个服务的Pod分散部署到不同的拓扑域（例如不同主机）中，以提高服务本身的稳定性。

服务网格（Istio）

Istio是一个提供连接、保护、控制以及观测服务的开放平台。阿里云服务网格提供一个全托管式的服务网格平台，兼容社区Istio开源服务网格，用于简化服务的治理，包括服务调用之间的流量路由与拆分管理、服务间通信的认证安全以及网格可观测性能力。

相关文档

关于Kubernetes的更多概念及术语详情，请参见Kubernetes concepts。

5.使用前必读

阿里云容器服务Kubernetes版（简称容器服务ACK）提供容器服务相关的技术架构以及核心组件的托管服务，对于非托管组件以及运行在ACK集群中的应用，不当操作可能会导致业务故障。为了更好地预估和避免相关的操作风险，在使用容器服务ACK前，请认真阅读本文中的建议与注意事项。

使用须知

数据面组件相关

数据面组件指运行在客户ECS服务器上的系统组件，例如CoreDNS、Ingress、kube-proxy、terway、kubelet等。由于数据面组件运行在客户ECS服务器上，因此数据面组件运行的稳定性需要阿里云容器服务与客户共同维护。

阿里云容器服务ACK对数据面组件提供以下支持：

- 提供组件的参数化设置管理、定期功能优化、BugFix、CVE补丁等功能，并给出相应的指导文档。
- 提供组件的监控与报警等可观测能力的建设，部分核心组件会提供组件日志，并通过SLS透出给客户。
- 提供配置最佳实践和建议，容器服务将根据集群规模大小给出组件配置建议。
- 提供组件的定期巡检能力和一定的报警通知能力，检查项包括但不限定于：组件版本、组件配置、组件负载、组件部署分布拓扑、组件实例数等。

您在使用数据面组件时，请遵循以下建议：

- 使用最新的组件版本。组件经常会发布新版本以修复BUG或提供新特性。您需要在新版本的组件发布后，在保证业务稳定的前提下选择合适的时机，遵循组件升级指导文档中的说明进行升级操作。更多信息，请参见组件概述。
- 请在容器服务ACK的报警中心中设置联系人的邮箱地址、手机号码，并设置相应的报警信息接收方式，阿里云将通过这些渠道推送容器服务的报警信息、产品公告等。更多信息，请参见容器服务报警管理和消息接收管理设置。
- 在您收到组件稳定性风险报告后，请及时按照相关指引进行处理，消除安全隐患。
- 当您在使用数据面组件时，请通过容器服务控制台集群管理页面**运维管理 > 组件管理**的方式或者OpenAPI的方式配置组件的自定义参数。通过其他渠道修改组件配置可能会导致组件功能异常。更多信息，请参见管理组件。
- 请勿直接使用IaaS层产品的OpenAPI来变更组件的运行环境，包括但不限定于使用ECS的OpenAPI更改ECS运行状态、修改Worker节点的安全组配置、更改Worker节点的网络配置以及通过负载均衡的OpenAPI修改SLB配置等，擅自改动IaaS层资源可能会导致数据面组件异常。
- 部分数据面组件受上游社区版组件影响，可能存在有Bug或漏洞，请注意及时升级组件，以避免开源组件Bug或漏洞导致您的业务受损。

集群升级相关

请务必通过容器服务ACK的集群升级功能升级集群的K8s版本，自行升级K8s版本可能导致ACK集群的稳定性和兼容性问题。详细操作，请参见升级ACK集群K8s版本。

阿里云容器服务ACK对集群升级提供以下支持：

- 提供集群K8s新版本的升级功能。
- 提供K8s新版本升级的前置检查功能，确保集群当前状态支持升级。
- 提供K8s新版本的版本说明文档，包括相较于前版本的变化。
- 提示升级到K8s新版本时因资源变化可能会发生的风险。

您在使用集群升级功能时，请遵循以下建议：

- 在集群升级前运行前置检查，并根据前置检查结果逐一修复集群升级的阻塞点。

- 详细阅读K8s新版本的版本说明文档，并根据ACK所提示的升级风险确认集群和业务的状态，自行判断升级风险。详细信息，请参见Kubernetes版本发布概览。
- 由于集群升级不提供回滚功能，请做好充分的升级计划和预后备案。
- 根据容器服务ACK的版本支持机制，在当前版本的支持周期内及时升级集群K8s版本。更多信息，请参见版本机制。

Kubernetes原生配置相关

- 请勿擅自修改Kubernetes的关键配置，例如以下文件的路径、链接和内容：
  - */var/lib/kubelet*
  - */var/lib/docker*
  - */etc/kubernetes*
  - */etc/kubeadm*
  - */var/lib/containerd*
- 在YAML模板中请勿使用Kubernetes集群预留的Annotation，否则会造成资源不可用、申请失败、异常等问题。以 `kubernetes.io/` 和 `k8s.io/` 开头的标签为核心组件预留标签。违规示例：pv.kubernetes.io/bind-completed: "yes"。

注册集群相关

- 通过的注册集群功能接入外部Kubernetes集群时，请确保外部集群与阿里云之间的网络稳定性。
- 容器服务ACK提供外部Kubernetes集群的注册接入，但无法管控外部集群自身的稳定性以及不当操作。因此当您通过注册集群配置外部集群节点的Label、Annotation、Tag等信息时，可能导致应用运行异常，请谨慎操作。

应用目录相关

为了丰富Kubernetes应用，容器服务ACK的应用市场提供了应用目录，它们是基于开源软件做了适配和二次开发的应用。ACK无法管控开源软件本身产生的缺陷，请知晓此风险。更多信息，请参见应用市场。

高危操作

在使用容器服务ACK过程中相关功能模块存在高危操作，可能会对业务稳定性造成较大影响。在使用前请认真了解以下高危操作及其影响。

- 集群相关高危操作
- 节点池相关高危操作
- 网络与负载均衡相关高危操作
- 存储相关高危操作
- 日志相关高危操作

集群相关高危操作

分类	高危操作	影响	恢复方案
API Server	删除API Server所使用的SLB。	导致集群不可操作。	不可恢复，请重新创建集群。
	修改集群内节点安全组。	可能导致节点不可用。	将节点重新添加到集群自动创建的节点安全组中，请参见ECS实例加入安全组。
	节点到期或被销毁。	该节点不可用。	不可恢复。

分类	高危操作	影响	恢复方案
Worker节点	重装操作系统。	节点上组件被删除。	节点移出再加入集群。
	自行升级节点组件版本。	可能导致节点无法使用。	回退到原始版本。
	更改节点IP。	节点不可用。	改回原IP。
	自行修改核心组件（kubelet、docker、containerd 等）参数。	可能导致节点不可用。	按照官网推荐配置参数。
	修改操作系统配置。	可能导致节点不可用。	尝试还原配置项或删除节点重新购买。
Master节点（ACK专有版集群）	修改集群内节点安全组。	可能导致Master节点不可用。	将节点重新添加到集群自动创建的节点安全组中，请参见ECS实例加入安全组。
	节点到期或被销毁。	该Master节点不可用。	不可恢复。
	重装操作系统。	Master节点上组件被删除。	不可恢复。
	自行升级Master或者etcd组件版本。	可能导致集群无法使用。	回退到原始版本。
	删除或格式化节点*/etc/kubernetes*等核心目录数据。	该Master节点不可用。	不可恢复。
	更改节点IP。	该Master节点不可用。	改回原IP。
	自行修改核心组件（etcd、kube-apiserver、docker等）参数。	可能导致Master节点不可用。	按照官网推荐配置参数。
	自行更换Master或etcd 证书	可能导致集群无法使用。	不可恢复。
	自行增加或减少Master节点。	可能导致集群无法使用。	不可恢复。
其他	通过RAM执行权限变更或修改操作。	集群部分资源如负载均衡可能无法创建成功。	恢复原先权限。

节点池相关高危操作

高危操作	影响	恢复方案
删除伸缩组。	导致节点池异常。	不可恢复，只能重建节点池。
通过kubectl移除节点。	节点池节点数显示和实际不符。	通过容器服务管理控制台或者节点池相关API移除指定节点（参见移除节点）或者修改节点池的期望节点数缩容（参见调整期望节点数）。

高危操作	影响	恢复方案
直接释放ECS实例。	可能导致节点池详情页面显示异常。开启期望节点数的节点池为维持期望节点数，将会根据相应节点池配置自动扩容到期望节点数。	不可恢复。正确做法是通过容器服务管理控制台或者节点池相关API修改节点池的期望节点数缩容（参见调整期望节点数）或移除指定节点（参见移除节点）。
对开启自动伸缩的节点池手动扩容或缩容。	自动伸缩组件会根据策略自动调整节点数，导致结果与期望不符。	不可恢复。自动伸缩节点池无需手动干预。
修改ESS伸缩组的最大或最小实例数。	可能导致扩缩容异常。	• 对于未开启自动伸缩组的节点池，ESS伸缩组最大和最小实例数改为默认值2000和0。 • 对于开启自动伸缩的节点池，将ESS伸缩组最大和最小实例数修改为与节点池最大和最小节点数一致。
添加已有节点前不做数据备份。	添加前实例上的数据丢失。	不可恢复。 • 手动添加已有节点前必须对要保留的所有数据做提前备份。 • 自动添加节点时会执行系统盘替盘操作，需要您提前备份保存在系统盘中的有用数据。
在节点系统盘中保存重要数据。	节点池的自愈操作可能通过重置节点配置的方式修复节点，因此可能导致系统盘数据丢失。	不可恢复。正确做法是将重要数据存放于额外的数据盘或者云盘、NAS、OSS。

网络与负载均衡相关高危操作

高危操作	影响	恢复方案
修改内核参数 `net.ipv4.ip_forward=0` 。	网络不通。	修改内核参数为 `net.ipv4.ip_forward=1` 。
修改内核参数： • `net.ipv4.conf.all.rp_filter = 1|2` • `net.ipv4.conf.[ethX].rp_filter = 1|2` **说明** `ethX` 代表所有以 `eth` 开头的网卡。	网络不通。	修改内核参数为： • `net.ipv4.conf.all.rp_filter = 0` • `net.ipv4.conf.[ethX].rp_filter = 0`
修改内核参数 `net.ipv4.tcp_tw_reuse = 1` 。	导致Pod健康检查异常。	修改内核参数为 `net.ipv4.tcp_tw_reuse = 0` 。

高危操作	影响	恢复方案
修改内核参数 `net.ipv4.tcp_tw_recycle = 1` 。	导致NAT异常。	修改内核参数 `net.ipv4.tcp_tw_recycle = 0` 。
修改内核参数 `net.ipv4.ip_local_port_range` 。	导致网络偶发不通。	修改内核参数到默认值 `net.ipv4.ip_local_port_range="32768 60999"` 。
安装防火墙软件，例如Firewalld或者ufw等。	导致容器网络不通。	卸载防火墙软件并重启节点。
节点安全组配置未放通容器 CIDR的53端口UDP。	集群内DNS无法正常工作。	按照官网推荐配置放通安全组。
修改或者删除ACK添加的SLB的标签。	导致SLB异常。	恢复SLB的标签。
通过负载均衡控制台修改ACK管理的SLB的配置，包括SLB、监听及虚拟服务器组。	导致SLB异常。	恢复SLB的配置。
移除Service中复用已有SLB的Annotation，即 `service.beta.kubernetes.io/alibaba-cloud-loadbalancer-id: ${YOUR_LB_ID}` 。	导致SLB异常。	在Service中添加复用已有SLB的Annotation。 **说明** 复用已有SLB的Service无法直接修改为使用自动创建SLB的Service。您需要重新创建Service。
通过负载均衡控制台删除ACK创建的SLB。	可能导致集群网络异常。	通过删除Service的方式删除SLB。

高危操作	影响	恢复方案

在安装Nginx Ingress Controller组件的情况下手动删除 kube-system命名空间下的 `nginx-ingress-lb` Service。	Ingress Controller工作不正常，严重时产生崩溃。	使用以下YAML新建一个同名Service。
		`apiVersion: v1`
		`kind: Service`
		`metadata:`
		`  annotations:`
		`  labels:`
		`  app: nginx-ingress-lb`
		`  name: nginx-ingress-lb`
		`  namespace: kube-system`
		`spec:`
		`  externalTrafficPolicy: Local`
		`  ports:`
		`  - name: http`
		`  port: 80`
		`  protocol: TCP`
		`  targetPort: 80`
		`  - name: https`
		`  port: 443`
		`  protocol: TCP`
		`  targetPort: 443`
		`  selector:`
		`  app: ingress-nginx`
		`  type: LoadBalancer`

存储相关高危操作

高危操作	影响	恢复方案
控制台手动解挂云盘。	Pod写入报IO Error。	重启Pod，手动清理节点挂载残留。
节点上umount磁盘挂载路径	Pod写入本地磁盘。	重启Pod。
节点上直接操作云盘。	Pod写入本地磁盘。	不可恢复。
多个Pod挂载相同云盘。	Pod写入本地磁盘或者报错IO Error。	确保一个云盘给一个Pod使用。
手动删除NAS挂载目录。	Pod写入报IO Error。	重启Pod。
删除在用的NAS盘或挂载点。	Pod出现IO Hang。	重启ECS节点。

日志相关高危操作

高危操作	影响	恢复方案
删除宿主机*/tmp/ccs-log-collector/pos*目录。	日志重复采集。	不可恢复。该目录下的文件记录了日志的采集位置。
删除宿主机*/tmp/ccs-log-collector/buffer*目录。	日志丢失。	不可恢复。该目录是待消费的日志缓存文件。
删除aliyunlogconfig CRD资源。	日志采集失效。	重新创建删除的CRD以及对应的资源，但失效期间日志无法恢复。 删除CRD会关联删除对应所有的实例，即使恢复CRD后还需要手动创建被删除的实例。
删除日志组件。	日志采集失效。	重新安装日志组件并手动恢复aliyunlogconfig CRD实例，删除期间日志无法恢复。 删除日志组件相当于删除aliyunlogconfig CRD以及日志采集器Logtail，期间日志采集能力全部丢失。

相关文档

- Nginx Ingress最佳实践
- DNS最佳实践

6.开服地域

地域是指物理的数据中心，资源创建成功后不能更换地域。本文介绍容器服务ACK支持的地域。

ACK各产品开服地域

ACK开服的地域、地域所在城市和Region ID的对照关系如下表所示。

云服务	地域	城市	Region ID	ACK Pro版	ACK标准版	ACK专有版	ASK Pro版	ASK标准版	边缘Pro版	边缘标准版	注册集群
	华北2	北京	cn-beijing	✓	✓	✓	✓	✓	✓	✓	✓
	华北3	张家口	cn-zhangjiakou	✓	✓	✓	✓	✓	✓	✓	✓
	华北5	呼和浩特	cn-huhehaote	✓	✓	✓	✓	✓	✓	✓	✓
	华北6	乌兰察布	cn-wulanchabu	✓	✓	待开放	✓	✓	✓	✓	✓
	华东1	杭州	cn-hangzhou	✓	✓	✓	✓	✓	✓	✓	✓
	华东2	上海	cn-shanghai	✓	✓	✓	✓	✓	✓	✓	✓
	华南1	深圳	cn-shenzhen	✓	✓	✓	✓	✓	✓	✓	✓
	华南2	河源	cn-heyuan	✓	✓	✓	✓	✓	✓	✓	✓
	华南3	广州	guangzhou	✓	✓	✓	✓	✓	✓	✓	✓
	西南1	成都	cn-chengdu	✓	✓	✓	✓	✓	✓	✓	✓

云服务	地域	城市	Region ID	ACK Pro版	ACK标准版	ACK专有版	ASK Pro版	ASK标准版	边缘Pro版	边缘标准版	注册集群
公共云	中国香港	香港	cn-hongkong	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南1	新加坡	ap-southeast-1	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南2	悉尼	ap-southeast-2	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南3	吉隆坡	ap-southeast-3	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南5	雅加达	ap-southeast-5	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南6	马尼拉	ap-southeast-6	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东南7	曼谷	ap-southeast-7	✓	✓	✓	✓	✓	✓	✓	
	亚太南部1	孟买	ap-south-1	✓	✓	✓	✓	✓	✓	✓	✓
	亚太东北1	东京	ap-northeast-1	✓	✓	✓	✓	✓	✓	✓	✓

云服务	地域	城市	Region ID	ACK Pro版	ACK标准版	ACK专有版	ASK Pro版	ASK标准版	边缘Pro版	边缘标准版	注册集群
	亚太东北2	首尔	ap-northeast-2	✓	✓	✓	✓	✓	✓	✓	待开放
	美国西部1	硅谷	us-west-1	✓	✓	✓	✓	✓	✓	✓	✓
	美国东部1	弗吉尼亚	us-east-1	✓	✓	✓	✓	✓	✓	✓	✓
	欧洲中部1	法兰克福	eu-central-1	✓	✓	✓	✓	✓	✓	✓	✓
	英国（伦敦）	伦敦	eu-west-1	✓	✓	✓	✓	✓	✓	✓	✓
	中东东部1	迪拜	me-east-1	待开放	待开放	✓	待开放	待开放	待开放	待开放	待开放
金	华东1金融云	杭州	cn-hangzhou-finance	✓	✗	✓	待开放	✗	待开放	✗	待开放
	华东2金融云	上海	cn-shanghai-finance-1	✓	✗	✓	待开放	✗	待开放	✗	待开放

金融云服务	地域	城市	Region ID	ACK Pro版	ACK标准版	ACK专有版	ASK Pro版	ASK标准版	边缘Pro版	边缘标准版	注册集群
	华南1金融云	深圳	cn-shenzhen-finance-1	✓	✗	✓	待开放	✗	待开放	✗	待开放
	华北2金融云	北京	cn-beijing-finance-1	✓	✗	✓	待开放	✗	待开放	✗	待开放
政务云	华北2阿里政务云1	北京	cn-north-2-gov-1	✓	✗	✓	待开放	✗	待开放	✗	待开放
本地云	南京	南京	cn-nanjing	✓	✗	✗	待开放	✗	待开放	✗	待开放

7.支持时区

由于世界各国家与地区经度不同，地方时也有所不同，因此会划分为不同的时区。本文主要介绍容器服务ACK支持的时区。

世界标准时间

时区	时差
UTC	+00:00

美洲

时区	时差
America/Adak	-10:00
America/Anchorage	-09:00
America/Anguilla	-04:00
America/Antigua	-04:00
America/Araguaina	-03:00
America/Argentina/Buenos_Aires	-03:00
America/Argentina/Catamarca	-03:00
America/Argentina/Cordoba	-03:00
America/Argentina/Jujuy	-03:00
America/Argentina/La_Rioja	-03:00
America/Argentina/Mendoza	-03:00
America/Argentina/Rio_Gallegos	-03:00
America/Argentina/Salta	-03:00
America/Argentina/San_Juan	-03:00
America/Argentina/San_Luis	-03:00
America/Argentina/Tucuman	-03:00
America/Argentina/Ushuaia	-03:00
America/Aruba	-04:00
America/Asuncion	-03:00
America/Atikokan	-05:00

时区	时差
America/Bahia	-03:00
America/Bahia_Banderas	-06:00
America/Barbados	-04:00
America/Belem	-03:00
America/Belize	-06:00
America/Blanc-Sablon	-04:00
America/Boa_Vista	-04:00
America/Bogota	-05:00
America/Boise	-07:00
America/Cambridge_Bay	-07:00
America/Campo_Grande	-04:00
America/Cancun	-05:00
America/Caracas	-04:00
America/Cayenne	-03:00
America/Cayman	-05:00
America/Chicago	-06:00
America/Chihuahua	-07:00
America/Costa_Rica	-06:00
America/Creston	-07:00
America/Cuiaba	-04:00
America/Curacao	-04:00
America/Danmarkshavn	+00:00
America/Dawson	-07:00
America/Dawson_Creek	-07:00
America/Denver	-07:00
America/Detroit	-05:00
America/Dominica	-04:00

时区	时差
America/Edmonton	-07:00
America/Eirunepe	-05:00
America/El_Salvador	-06:00
America/Fort_Nelson	-07:00
America/Fortaleza	-03:00
America/Glace_Bay	-04:00
America/Goose_Bay	-04:00
America/Grand_Turk	-05:00
America/Grenada	-04:00
America/Guadeloupe	-04:00
America/Guatemala	-06:00
America/Guayaquil	-05:00
America/Guyana	-04:00
America/Halifax	-04:00
America/Havana	-05:00
America/Hermosillo	-07:00
America/Indiana/Indianapolis	-05:00
America/Indiana/Knox	-06:00
America/Indiana/Marengo	-05:00
America/Indiana/Petersburg	-05:00
America/Indiana/Tell_City	-06:00
America/Indiana/Vevay	-05:00
America/Indiana/Vincennes	-05:00
America/Indiana/Winamac	-05:00
America/Inuvik	-07:00
America/Iqaluit	-05:00
America/Jamaica	-05:00

时区	时差
America/Juneau	-09:00
America/Kentucky/Louisville	-05:00
America/Kentucky/Monticello	-05:00
America/Kralendijk	-04:00
America/La_Paz	-04:00
America/Lima	-05:00
America/Los_Angeles	-08:00
America/Lower_Princes	-04:00
America/Maceio	-03:00
America/Managua	-06:00
America/Manaus	-04:00
America/Marigot	-04:00
America/Martinique	-04:00
America/Matamoros	-06:00
America/Mazatlan	-07:00
America/Menominee	-06:00
America/Merida	-06:00
America/Metlakatla	-09:00
America/Mexico_City	-06:00
America/Miquelon	-03:00
America/Moncton	-04:00
America/Monterrey	-06:00
America/Montevideo	-03:00
America/Montserrat	-04:00
America/Nassau	-05:00
America/New_York	-05:00
America/Nipigon	-05:00

时区	时差
America/Nome	-09:00
America/Noronha	-02:00
America/North_Dakota/Beulah	-06:00
America/North_Dakota/Center	-06:00
America/North_Dakota/New_Salem	-06:00
America/Nuuk	-03:00
America/Ojinaga	-07:00
America/Panama	-05:00
America/Pangnirtung	-05:00
America/Paramaribo	-03:00
America/Phoenix	-07:00
America/Port-au-Prince	-05:00
America/Port_of_Spain	-04:00
America/Porto_Velho	-04:00
America/Puerto_Rico	-04:00
America/Punta_Arenas	-03:00
America/Rainy_River	-06:00
America/Rankin_Inlet	-06:00
America/Recife	-03:00
America/Regina	-06:00
America/Resolute	-06:00
America/Rio_Branco	-05:00
America/Santarem	-03:00
America/Santiago	-03:00
America/Santo_Domingo	-04:00
America/Sao_Paulo	-03:00
America/Scoresbysund	-01:00

时区	时差
America/Sitka	-09:00
America/St_Barthelemy	-04:00
America/St_Johns	-03:30
America/St_Kitts	-04:00
America/St_Lucia	-04:00
America/St_Thomas	-04:00
America/St_Vincent	-04:00
America/Swift_Current	-06:00
America/Tegucigalpa	-06:00
America/Thule	-04:00
America/Thunder_Bay	-05:00
America/Tijuana	-08:00
America/Toronto	-05:00
America/Tortola	-04:00
America/Vancouver	-08:00
America/Whitehorse	-07:00
America/Winnipeg	-06:00
America/Yakutat	-09:00
America/Yellowknife	-07:00

亚洲

时区	时差
Asia/Aden	+03:00
Asia/Almaty	+06:00
Asia/Amman	+02:00
Asia/Anadyr	+12:00
Asia/Aqtau	+05:00

时区	时差
Asia/Aqtobe	+05:00
Asia/Ashgabat	+05:00
Asia/Atyrau	+05:00
Asia/Baghdad	+03:00
Asia/Bahrain	+03:00
Asia/Baku	+04:00
Asia/Bangkok	+07:00
Asia/Barnaul	+07:00
Asia/Beirut	+02:00
Asia/Bishkek	+06:00
Asia/Brunei	+08:00
Asia/Chita	+09:00
Asia/Choibalsan	+08:00
Asia/Colombo	+05:30
Asia/Damascus	+02:00
Asia/Dhaka	+06:00
Asia/Dili	+09:00
Asia/Dubai	+04:00
Asia/Dushanbe	+05:00
Asia/Famagusta	+02:00
Asia/Gaza	+02:00
Asia/Hebron	+02:00
Asia/Ho_Chi_Minh	+07:00
Asia/Hong_Kong	+08:00
Asia/Hovd	+07:00
Asia/Irkutsk	+08:00
Asia/Jakarta	+07:00

时区	时差
Asia/Jayapura	+09:00
Asia/Jerusalem	+02:00
Asia/Kabul	+04:30
Asia/Kamchatka	+12:00
Asia/Karachi	+05:00
Asia/Kathmandu	+05:45
Asia/Khandyga	+09:00
Asia/Kolkata	+05:30
Asia/Krasnoyarsk	+07:00
Asia/Kuala_Lumpur	+08:00
Asia/Kuching	+08:00
Asia/Kuwait	+03:00
Asia/Macau	+08:00
Asia/Magadan	+11:00
Asia/Makassar	+08:00
Asia/Manila	+08:00
Asia/Muscat	+04:00
Asia/Nicosia	+02:00
Asia/Novokuznetsk	+07:00
Asia/Novosibirsk	+07:00
Asia/Omsk	+06:00
Asia/Oral	+05:00
Asia/Phnom_Penh	+07:00
Asia/Pontianak	+07:00
Asia/Pyongyang	+09:00
Asia/Qatar	+03:00
Asia/Qostanay	+06:00

时区	时差
Asia/Qyzylorda	+05:00
Asia/Riyadh	+03:00
Asia/Sakhalin	+11:00
Asia/Samarkand	+05:00
Asia/Seoul	+09:00
Asia/Shanghai	+08:00
Asia/Singapore	+08:00
Asia/Srednekolymsk	+11:00
Asia/Taipei	+08:00
Asia/Tashkent	+05:00
Asia/Tbilisi	+04:00
Asia/Tehran	+03:30
Asia/Thimphu	+06:00
Asia/Tokyo	+09:00
Asia/Tomsk	+07:00
Asia/Ulaanbaatar	+08:00
Asia/Urumqi	+06:00
Asia/Ust-Nera	+10:00
Asia/Vientiane	+07:00
Asia/Vladivostok	+10:00
Asia/Yakutsk	+09:00
Asia/Yangon	+06:30
Asia/Yekaterinburg	+05:00
Asia/Yerevan	+04:00

欧洲

时区	时差
Europe/Amsterdam	+01:00
Europe/Andorra	+01:00
Europe/Astrakhan	+04:00
Europe/Athens	+02:00
Europe/Belgrade	+01:00
Europe/Berlin	+01:00
Europe/Bratislava	+01:00
Europe/Brussels	+01:00
Europe/Bucharest	+02:00
Europe/Budapest	+01:00
Europe/Busingen	+01:00
Europe/Chisinau	+02:00
Europe/Copenhagen	+01:00
Europe/Dublin	+00:00
Europe/Gibraltar	+01:00
Europe/Guernsey	+00:00
Europe/Helsinki	+02:00
Europe/Isle_of_Man	+00:00
Europe/Istanbul	+03:00
Europe/Jersey	+00:00
Europe/Kaliningrad	+02:00
Europe/Kiev	+02:00
Europe/Kirov	+03:00
Europe/Lisbon	+00:00
Europe/Ljubljana	+01:00
Europe/London	+00:00
Europe/Luxembourg	+01:00

时区	时差
Europe/Madrid	+01:00
Europe/Malta	+01:00
Europe/Mariehamn	+02:00
Europe/Minsk	+03:00
Europe/Monaco	+01:00
Europe/Moscow	+03:00
Europe/Oslo	+01:00
Europe/Paris	+01:00
Europe/Podgorica	+01:00
Europe/Prague	+01:00
Europe/Riga	+02:00
Europe/Rome	+01:00
Europe/Samara	+04:00
Europe/San_Marino	+01:00
Europe/Sarajevo	+01:00
Europe/Saratov	+04:00
Europe/Simferopol	+03:00
Europe/Skopje	+01:00
Europe/Sofia	+02:00
Europe/Stockholm	+01:00
Europe/Tallinn	+02:00
Europe/Tirane	+01:00
Europe/Ulyanovsk	+04:00
Europe/Uzhgorod	+02:00
Europe/Vaduz	+01:00
Europe/Vatican	+01:00
Europe/Vienna	+01:00

时区	时差
Europe/Vilnius	+02:00
Europe/Volgograd	+04:00
Europe/Warsaw	+01:00
Europe/Zagreb	+01:00
Europe/Zaporozhye	+02:00
Europe/Zurich	+01:00

非洲

时区	时差
Africa/Abidjan	+00:00
Africa/Accra	+00:00
Africa/Addis_Ababa	+03:00
Africa/Algiers	+01:00
Africa/Asmara	+03:00
Africa/Bamako	+00:00
Africa/Bangui	+01:00
Africa/Banjul	+00:00
Africa/Bissau	+00:00
Africa/Blantyre	+02:00
Africa/Brazzaville	+01:00
Africa/Bujumbura	+02:00
Africa/Cairo	+02:00
Africa/Casablanca	+01:00
Africa/Ceuta	+01:00
Africa/Conakry	+00:00
Africa/Dakar	+00:00
Africa/Dar_es_Salaam	+03:00

时区	时差
Africa/Djibouti	+03:00
Africa/Douala	+01:00
Africa/El_Aaiun	+01:00
Africa/Freetown	+00:00
Africa/Gaborone	+02:00
Africa/Harare	+02:00
Africa/Johannesburg	+02:00
Africa/Juba	+03:00
Africa/Kampala	+03:00
Africa/Khartoum	+02:00
Africa/Kigali	+02:00
Africa/Kinshasa	+01:00
Africa/Lagos	+01:00
Africa/Libreville	+01:00
Africa/Lome	+00:00
Africa/Luanda	+01:00
Africa/Lubumbashi	+02:00
Africa/Lusaka	+02:00
Africa/Malabo	+01:00
Africa/Maputo	+02:00
Africa/Maseru	+02:00
Africa/Mbabane	+02:00
Africa/Mogadishu	+03:00
Africa/Monrovia	+00:00
Africa/Nairobi	+03:00
Africa/Ndjamena	+01:00
Africa/Niamey	+01:00

时区	时差
Africa/Nouakchott	+00:00
Africa/Ouagadougou	+00:00
Africa/Porto-Novo	+01:00
Africa/Sao_Tome	+00:00
Africa/Tripoli	+02:00
Africa/Tunis	+01:00
Africa/Windhoek	+02:00

太平洋地区

时区	时差
Pacific/Apia	+14:00
Pacific/Auckland	+13:00
Pacific/Bougainville	+11:00
Pacific/Chatham	+13:45
Pacific/Chuuk	+10:00
Pacific/Easter	-05:00
Pacific/Efate	+11:00
Pacific/Enderbury	+13:00
Pacific/Fakaofo	+13:00
Pacific/Fiji	+12:00
Pacific/Funafuti	+12:00
Pacific/Galapagos	-06:00
Pacific/Gambier	-09:00
Pacific/Guadalcanal	+11:00
Pacific/Guam	+10:00
Pacific/Honolulu	-10:00
Pacific/Kiritimati	+14:00

时区	时差
Pacific/Kosrae	+11:00
Pacific/Kwajalein	+12:00
Pacific/Majuro	+12:00
Pacific/Marquesas	-09:30
Pacific/Midway	-11:00
Pacific/Nauru	+12:00
Pacific/Niue	-11:00
Pacific/Norfolk	+12:00
Pacific/Noumea	+11:00
Pacific/Pago_Pago	-11:00
Pacific/Palau	+09:00
Pacific/Pitcairn	-08:00
Pacific/Pohnpei	+11:00
Pacific/Port_Moresby	+10:00
Pacific/Rarotonga	-10:00
Pacific/Saipan	+10:00
Pacific/Tahiti	-10:00
Pacific/Tarawa	+12:00
Pacific/Tongatapu	+13:00
Pacific/Wake	+12:00
Pacific/Wallis	+12:00

大洋洲

时区	时差
Australia/Adelaide	+10:30
Australia/Brisbane	+10:00
Australia/Broken_Hill	+10:30

时区	时差
Australia/Currie	+11:00
Australia/Darwin	+09:30
Australia/Eucla	+08:45
Australia/Hobart	+11:00
Australia/Lindeman	+10:00
Australia/Lord_Howe	+11:00
Australia/Melbourne	+11:00
Australia/Perth	+08:00
Australia/Sydney	+11:00

印度洋地区

时区	时差
Indian/Antananarivo	+03:00
Indian/Chagos	+06:00
Indian/Christmas	+07:00
Indian/Cocos	+06:30
Indian/Comoro	+03:00
Indian/Kerguelen	+05:00
Indian/Mahe	+04:00
Indian/Maldives	+05:00
Indian/Mauritius	+04:00
Indian/Mayotte	+03:00
Indian/Reunion	+04:00

大西洋地区

时区	时差
Atlantic/Azores	-01:00
Atlantic/Bermuda	-04:00

时区	时差
Atlantic/Canary	+00:00
Atlantic/Cape_Verde	-01:00
Atlantic/Faroe	+00:00
Atlantic/Madeira	+00:00
Atlantic/Reykjavik	+00:00
Atlantic/South_Georgia	-02:00
Atlantic/St_Helena	+00:00
Atlantic/Stanley	-03:00

南极洲

时区	时差
Antarctica/Casey	+08:00
Antarctica/Davis	+07:00
Antarctica/DumontDUrville	+10:00
Antarctica/Macquarie	+11:00
Antarctica/Mawson	+05:00
Antarctica/McMurdo	+13:00
Antarctica/Palmer	-03:00
Antarctica/Rothera	-03:00
Antarctica/Syowa	+03:00
Antarctica/Troll	+00:00
Antarctica/Vostok	+06:00

北极地区

时区	时差
Arctic/Longyearbyen	+01:00

8.使用限制

本文主要为您介绍阿里云容器服务Kubernetes版（ACK）集群的使用过程中的一些限制。

限制概述

使用阿里云容器服务ACK产品前，需要注意以下使用限制：

- 购买容器服务ACK实例前，需要进行实名认证。
- 只有当您账户余额和代金券总值不小于100元时，才可创建按量付费的阿里云资源。
- 在创建ACK集群以后，暂不支持以下项：
  - 变更集群的VPC。
  - 变更托管集群为专有集群，以及变更Pro版集群为标准版集群。
  - 变更容器网络插件。
  - 变更存储插件。
  - 在不同命名空间下迁移应用。
- ACK集群中ECS实例的限制如下：
  - 创建的ECS实例目前支持按量付费和包年包月，其他资源（例如负载均衡）为按量付费。您可以通过ECS管理控制台将按量付费实例转换成包年包月实例。
  - 由于ECS等底层依赖产品配额及库存限制，创建、扩容集群，或者自动弹性扩容集群时，可能只有部分节点创建成功。
  - 如果在创建集群时选择的是包年包月ECS实例，因为ECS配额及库存限制可能导致创建失败，已创建出来的包年包月实例无法释放，因此只能加入已有集群进行使用。

    > **说明** 为避免类似问题，建议您在创建集群时选择按量付费实例，创建后通过ECS控制台将按量付费实例转换成包年包月实例。

  - ECS规格要求：CPU大于等于4核，且内存大于等于8 GiB。
- 访问集群管控组件的流量限制如下：
  当您通过API或者命令行访问集群管控组件（API Server以及etcd）时，由于访问带宽的限制，如果您一次性读取大量的集群事件，有可能触发限流从而导致读取失败。建议您使用事件中心查询集群事件，或者在API、命令行中添加分页参数以降低单次请求量（例如：`--chunk-size=500`）。此外，如果您在ACK标准版集群中频繁遇到限流问题，请您将ACK标准版集群迁移至ACK Pro版集群。
  关于事件中心的更多信息，请参见场景一：使用NPD结合SLS的Kubernetes事件中心监控集群事件。
  关于将ACK标准版集群迁移至ACK Pro版集群的具体步骤，请参见热迁移ACK标准版集群至ACK Pro版集群。

ACK集群配额限制

集群类型		单阿里云账号最大集群数	单集群最大节点池数①	单集群最大节点数	单节点最大Pod数②	例外申请方式
ACK托管集群	标准版	2	10	10	256	到配额平台提交申请
	Pro版	100	100	1000	256	到配额平台提交申请

集群类型		单阿里云账号最大集群数	单集群最大节点池数①	单集群最大节点数	单节点最大Pod数②	例外申请方式
ACK专有集群		5	100	1000	256	到配额平台提交申请
ASK集群	标准版	2	不涉及	不涉及	1000③	到配额平台提交申请
	Pro版	100	不涉及	不涉及	10000③	到配额平台提交申请
边缘集群	标准版	2	10	10	256	到配额平台提交申请
	Pro版	100	100	1000	256	到配额平台提交申请
注册集群		5	100	不涉及	256	到配额平台提交申请

①如果您要使申请提高的单集群最大节点池数配额生效，还需要同时申请弹性伸缩产品的伸缩组总数配额，请登录到配额平台提交申请。

②单节点最大Pod数仅适用于Flannel网络模式且不支持申请提高。如果集群使用Terway网络，单节点最大Pod数由该节点可分配IP总数决定。

③ASK集群没有节点，此配额表示单ASK集群支持的最大Pod数，ASK单节点最大Pod数不可提升配额。

> **说明** 本文仅展示了各限制项的默认配额。对于可以调整配额的限制项，您可以前往配额中心申请提升配额。配额中心现已支持多个云产品，具体信息，请参见配额中心支持的云产品。

依赖底层云产品配额限制

限制大类	限制项	普通用户限制	例外申请方式
	阿里云资源编排服务ROS（Resource Orchestration Service）配额	默认100	提交工单
	按量实例vCPU限额	500核	提交工单
	按量实例购买高配规格（大于16c的实例）	vCPU核数少于16（不含16）的实例规格	提交工单
	抢占实例vCPU限额	800核	提交工单
	按量付费转包年包月	以下实例规格（族）不支持：t1、s1、s2、s3、c1、c2、m1、m2、n1、n2、e3	提交工单

限制大类	限制项	普通用户限制	例外申请方式
	弹性伸缩ESS（Elastic Scaling Service）	ESS伸缩组中管理的ECS实例个数不超过2000	提交工单
	操作系统	ACK支持添加以下操作系统的节点： • Alibaba Cloud Linux 2 • CentOS 7.x **说明** 暂不支持CentOS 8.x及以上的操作系统。 • Windows Server 2019和Windows Server Core, version 1809及以上	无
网络	每个路由表中可保有的自定义路由条目	48条	提交工单
	每个VPC实例内可保有的vSwitch数量	24个	提交工单
	可保有的VPC实例数量	10个	提交工单
	单VPC内总私网IP限制	65535	无
	单普通安全组可支持挂载IP限额	2000	无
	弹性网卡（辅助网卡）创建限额	50000	无
	可保有EIP数量	20	提交工单
负载均衡	用户可保有的SLB实例个数	60	提交工单
	每个SLB后端可挂载的服务器数量	200	无
	每个SLB实例可保有的监听数量	50	提交工单
	同一台ECS服务器可重复添加为SLB后端的次数	50	无
块存储	一个账号在所有地域的按量付费云盘数量配额	账号下所有地域的实例数量*5。每个账号最少可以创建10块按量付费云盘。	提交工单

限制大类	限制项	普通用户限制	例外申请方式
块存储	一个账号用作数据盘的按量付费云盘容量配额	和云服务器使用情况、地域、云盘类型有关，您可以在权益配额页面查看，更多信息，请参见查看和提升实例配额。	提交工单

9.开源项目

开源项目扩展了Kubernetes集群的功能。本文介绍阿里云容器服务Kubernetes版主要使用的开源项目。

项目分类	项目名称	项目简介	项目地址	参考文档
核心组件	Kubernetes Cloud Controller Manager for Alibaba Cloud	为Kubernetes应用创建负载均衡，管理节点路由条目。	Cloud-Provider-Alibaba-Cloud	Cloud Controller Manager
网络	Terway CNI Network Plugin	Terway网络插件是阿里云容器服务自研的网络插件，使用原生的弹性网卡分配给Pod，实现Pod网络。	Terway	使用Terway网络插件
	NGINX Ingress Controller	作为反向代理服务器，提供4层和7层负载均衡能力。	Ingress-Nginx	NGINX Ingress Controller
	ExternalDNS	通过云产品Private-Zone提供动态DNS能力。	External-DNS	ExternalDNS
存储	Alibaba Cloud Kubernetes CSI Plugin	容器存储接口，实现存储卷生命周期管理。	Alibaba-Cloud-CSI-Driver	存储CSI概述
	阿里云容器服务Kubernetes Flexvolume插件	提供挂载和卸载Kubernetes存储卷能力的组件（早期版）。	Flexvolume	存储Flexvolume概述
	阿里云盘Volume Provision Controller	提供创建和删除Kubernetes存储卷能力的组件（早期版）。	Alicloud-Storage-Provisioner	阿里云盘Volume Provision Controller
资源优化	Node-Resource-Manager	节点资源管理、上报组件。	Node-Resource-Manager	无
弹性	Kubernetes-CronHPA-Controller	Kubernetes中的容器水平定时伸缩组件。	Kubernetes-CronHPA-Controller	容器定时伸缩（CronHPA）
	Kubernetes Autoscaler	Kubernetes中的容器节点水平伸缩组件。	Autoscaler	节点自动伸缩
	KMS provider plugin for Alibaba Cloud	基于阿里云KMS服务的密钥管理能力，实现Kubernetes Secret的落盘加密能力。	Ack-KMS-Plugin	使用阿里云KMS进行Secret的落盘加密

项目分类	项目名称	项目简介	项目地址	参考文档
安全	Kube2ram	以DaemonSet的形式实现对ECS绑定RAM角色的访问代理，实现Pod维度的RAM角色权限隔离。	Kube2ram	Kube2ram
	ACK RAM Authenticator for Kubernetes	支持基于RAM角色扮演的APIServer认证方式。	ACK-RAM-Authenticator	使用RAM Role对ACK容器集群进行身份验证
	ACK Secret Manager	支持实时导入和同步阿里云KMS凭据管家服务中的密钥数据。	ACK Secret Manager	ACK Secret Manager
	SGX-Device-Plugin	在机密计算场景中，专用于SGX设备EPC加密内存资源扩展的Kubernetes设备插件。	SGX-Device-Plugin	SGX-Device-Plugin
迁移	Derrick	开源S2I工具，通过探测的机制，一键生成Dockerfile与模板。	Derrick	Derrick
	Velero	Velero是一个云原生的集群应用备份、恢复和迁移工具。	Velero-Plugin	Velero-Plugin
	Image Build Specification of Alibaba Cloud Container Service for Kubernetes (ACK)	快速制作符合Kubernetes集群节点要求的自定义镜像的工具。	ACK-Image-Builder	使用自定义镜像创建ACK集群
AI	Arena	Arena是基于Kubernetes的机器学习轻量级解决方案，支持数据准备、模型开发、模型训练、模型预测的完整生命周期。	Arena	Arena
	GPU Sharing Scheduler Extender in Kubernetes	业界首个GPU共享调度器。	GPU Share-Scheduler-Extender	GPU Share-Scheduler-Extender
	Fluid	Fluid是一个开源的Kubernetes原生的分布式数据集编排和加速引擎。	Fluid	Fluid

项目分类	项目名称	项目简介	项目地址	参考文档
应用管理	Kube-eventer	开源Kubernetes事件收集工具，支持Kafka、MySQL、钉钉、飞书等多种离线链路。	Kube-Eventer	事件监控
	Alibaba-Cloud-Metrics-Adapter	Kubernetes云指标转换组件，提供弹性自定义指标支持。	Alibaba-Cloud-Metrics-Adapter	Alibaba-Cloud-Metrics-Adapter
	OpenKruise	Kubernetes应用负载自动化，提供了原地升级、Sidecar管理、高效稳定部署等能力。	Kruise	What is OpenKruise?
	Open Application Model Specification	开放应用模型，为云原生应用管理提供标准化、关注点分离的规范。	Open Application Model	Open Application Model Specification
	KubeVela	一个简单易用且高度可扩展的应用管理平台与核心引擎。	KubeVela	Quick Start
调度	Scheduler Plugins	基于Scheduling Framework扩展并且支持AI、大数据等复杂场景的调度器。	Scheduler Plugins	Scheduler Plugins

10.版本机制

容器服务ACK基于原生的Kubernetes提供以容器为核心的解决方案。由于Kubernetes版本不断升级，因此容器服务ACK会定期发布支持的Kubernetes版本。本文为您介绍容器服务ACK的Kubernetes版本支持机制。

版本支持

从2020年1月1日起，ACK仅发布Kubernetes双数号的大版本。版本支持策略如下：

- **集群创建**
  ACK支持Kubernetes两个大版本的创建，例如v1.16、v1.18。当新版本Kubernetes发布时，较老的一个版本将不再开放创建功能。例如，当v1.20发布时，v1.16将不再开放创建功能。
- **升级和运维保障**
  ACK保障最近的三个Kubernetes大版本的稳定运行，同时支持最新版本往前两个大版本的升级功能，例如当前最新版本为v1.20，则ACK支持v1.18、v1.16的升级功能。过期版本的集群存在运行不稳定和集群升级失败的风险，建议您及时升级Kubernetes版本。
- **工单答疑**
  ACK提供最近的三个Kubernetes大版本的技术支持，例如答疑、在线指导、排查、排错等工作，但对于过期版本的Kubernetes集群，ACK不保证技术支持的质量和有效性。

> 说明
>
> - **ACK支持的大版本**：ACK支持的Kubernetes双数号版本称为大版本，例如v1.18，包含一个该版本下最新的小版本，例如v1.18.8。双数号版本称为大版本，例如v1.14；三数号版本称为小版本，例如v1.14.8。
> - **过期版本**：
>   - 分为过期大版本和过期小版本。
>   - 过期大版本指的是ACK支持的最近的三个Kubernetes大版本再往前的版本。
>   - 过期小版本指的是因CVE漏洞补丁等推出的最新小版本之前的版本。

关于ACK集群的Kubernetes版本的发布记录，请参见Kubernetes版本发布概览。

版本发布周期

- ACK原则上保持每半年更新一次Kubernetes大版本的频率。
- 大版本推出后，由于功能更新以及漏洞修复，ACK会不定期推出小版本的更新。

版本约束

- 版本升级功能当前只支持邻近版本的升级，暂不支持跨多个版本的升级，小版本的升级则不受该限制。
- 小版本的最新版发布后，原则上只提供该小版本的技术支持，对于较老的小版本，请尽快升级以获得完整的支持。

11.与原生Kubernetes名词对照

本文主要为您介绍容器服务ACK与原生Kubernetes名词对照情况。

容器服务ACK	原生Kubernetes	参考链接
集群	Cluster	集群
节点	Node	节点
容器	Container	容器
镜像	Image	镜像
命名空间	Namespace	命名空间
工作负载	Workload	工作负载
容器组	Pod	Pods
无状态工作负载	Deployment	Deployments
有状态工作负载	StatefulSet	StatefulSets
守护进程集工作负载	DaemonSet	DaemonSet
任务	Job	Jobs
定时任务	CronJob	CronJob
自定义资源	CustomResourceDefinition	定制资源
服务	Service	服务
虚拟集群IP	Cluster IP	服务类型
节点端口	NodePort	NodePort类型
路由	Ingress	Ingress
标签	Label	标签和选择算符
配置项	Configmap	ConfigMap
保密字典	Secret	Secret
存储卷	PersistentVolume	持久卷
存储声明	PersistentVolumeClaim	PersistentVolumeClaims
水平弹性伸缩	HPA	Pod水平自动扩缩
负载均衡	LoadBalancer	LoadBalancer类型
节点亲和性	NodeAffinity	节点亲和性

容器服务ACK	原生Kubernetes	参考链接
应用亲和性	PodAffinity	Pod间亲和性与反亲和性
应用非亲和性	PodAntiAffinity	Pod间亲和性与反亲和性
选择器	LabelSelector	标签选择算符
注解	Annotation	注解
触发器	Webhook	Webhook模式
端点	Endpoint	云原生服务发现
资源配额	Resource Quota	资源配额
资源限制	Limit Range	限制范围
模板	Template	Pod模板