

云容器引擎

# 产品介绍

文档版本 01  
发布日期 2024-11-30



版权所有 © 华为云计算技术有限公司 2024。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云计算技术有限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，华为云计算技术有限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。

# 华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

---

# 目录

---

<b>1 什么是云容器引擎</b> .....	<b>1</b>
<b>2 产品优势</b> .....	<b>4</b>
<b>3 应用场景</b> .....	<b>9</b>
3.1 容器应用管理.....	9
3.2 秒级弹性伸缩.....	11
3.3 微服务流量治理.....	12
3.4 DevOps 持续交付.....	13
3.5 混合云.....	15
3.6 高性能调度.....	17
<b>4 安全</b> .....	<b>22</b>
4.1 责任共担.....	22
4.2 数据保护技术.....	23
4.3 审计与日志.....	24
4.4 监控安全风险.....	25
4.5 认证证书.....	25
<b>5 权限管理</b> .....	<b>27</b>
<b>6 约束与限制</b> .....	<b>34</b>
<b>7 与其它云服务的关系</b> .....	<b>39</b>
<b>8 区域与可用区</b> .....	<b>42</b>

# 1 什么是云容器引擎

云容器引擎（Cloud Container Engine，简称CCE）是一个企业级的Kubernetes集群托管服务，支持容器化应用的全生命周期管理，为您提供高度可扩展的、高性能的云原生应用部署和管理方案。

## 为什么选择云容器引擎

云容器引擎深度整合高性能的计算（ECS/BMS）、网络（VPC/EIP/ELB）、存储（EVS/OBS/SFS）等服务，并支持GPU、NPU、ARM等异构计算架构，支持多可用区（Available Zone，简称AZ）、多区域（Region）容灾等技术构建高可用Kubernetes集群。

华为云是全球首批Kubernetes认证服务提供商（Kubernetes Certified Service Provider，KCSP），是国内最早投入Kubernetes社区的厂商，是容器开源社区主要贡献者和容器生态领导者。华为云也是CNCF云原生计算基金会的创始成员及白金会员，云容器引擎是全球首批通过CNCF基金会Kubernetes一致性认证的容器服务。

更多选择理由，请参见[产品优势](#)和[应用场景](#)。

## 产品形态

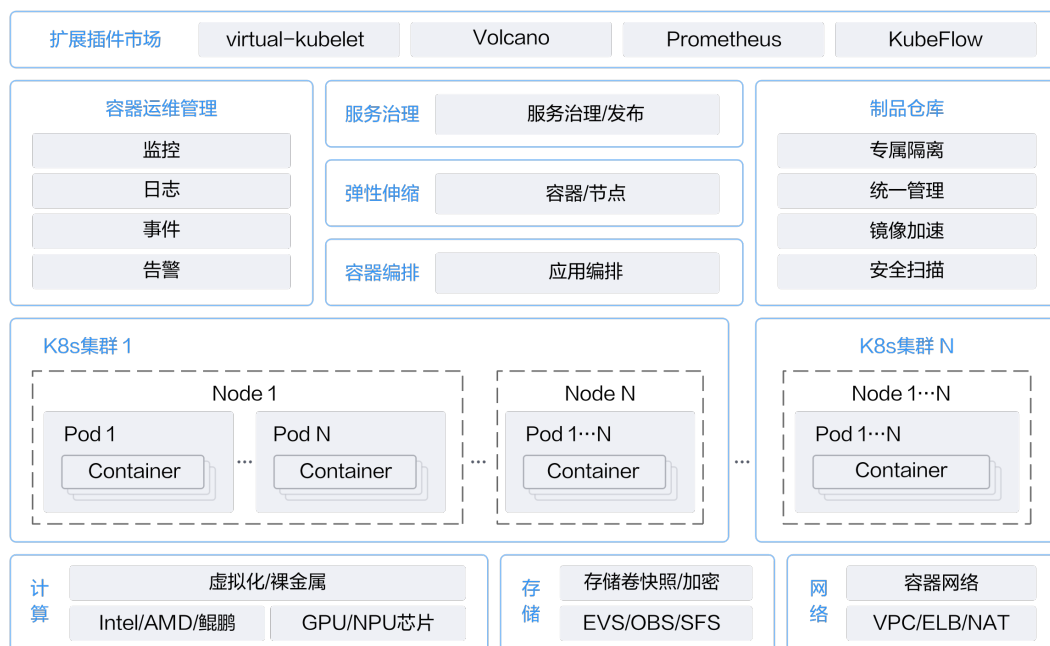
云容器引擎包含多种产品形态。

维度	子维度	CCE Standard	CCE Turbo	CCE Autopilot
产品定位	-	标准版本集群，提供高可靠、安全的商业级容器集群服务。	面向云原生2.0的新一代容器集群产品，计算、网络、调度全面加速。	无用户节点的Serverless版集群，无需对节点的部署、管理和安全性进行维护，并根据CPU和内存资源用量按需付费。

维度	子维度	CCE Standard	CCE Turbo	CCE Autopilot
使用场景	-	面向有云原生数字化转型诉求的用户，期望通过容器集群管理应用，获得灵活弹性的算力资源，简化对计算、网络、存储的资源管理复杂度。	适合对极致性能、资源利用率提升和全场景覆盖有更高诉求的客户。	适合具有明显的波峰波谷特征的业务负载，例如在线教育、电子商务等行业。
规格差异	网络模型	云原生网络1.0：面向性能和规模要求不高的场景。 <ul style="list-style-type: none"> <li>容器隧道网络模式</li> <li>VPC网络模式</li> </ul>	云原生网络2.0：面向大规模和高性能的场景。 组网规模最大支持2000节点	云原生网络2.0：面向大规模和高性能的场景。
	网络性能	VPC网络叠加容器网络，性能有一定损耗	VPC网络和容器网络融合，性能无损耗	VPC网络和容器网络融合，性能无损耗
	容器网络隔离	<ul style="list-style-type: none"> <li>容器隧道网络模式：集群内部网络隔离策略，支持NetworkPolicy。</li> <li>VPC网络模式：不支持</li> </ul>	Pod可直接关联安全组，基于安全组的隔离策略，支持集群内外部统一的安全隔离。	Pod可直接关联安全组，基于安全组的隔离策略，支持集群内外部统一的安全隔离。
	安全隔离性	普通容器：Cgroups隔离	<ul style="list-style-type: none"> <li>安全容器：当前仅物理机支持，提供虚拟机级别的隔离</li> <li>普通容器：Cgroups隔离</li> </ul>	提供虚拟机级别的隔离
	边缘基础设施管理	不支持	支持管理智能边缘小站	不支持

## 产品架构

图 1-1 CCE 产品架构



- **计算**：全面适配华为云各类计算实例，支持虚拟机和裸机混合部署、高性价比鲲鹏实例、GPU 和 华为云独有的昇腾算力；支持 GPU 虚拟化、共享调度、资源感知的调度优化。
- **网络**：支持对接高性能、安全可靠、多协议的独享型 ELB 作为业务流量入口。
- **存储**：对接云存储，支持 EVS、SFS 和 OBS，提供磁盘加密、快照和备份能力。
- **集群服务**：支持购买集群、连接集群、升级集群、管理集群等一系列集群生命周期管理服务。
- **容器编排**：CCE 提供了管理 Helm Chart（模板）的控制台，能够帮助您方便的使用模板部署应用，并在控制台上管理应用。
- **制品仓库**：对接容器镜像服务，支持镜像全生命周期管理的的服务，提供简单易用、安全可靠的镜像管理功能，帮助您快速部署容器化服务。
- **弹性伸缩**：支持工作负载和节点的弹性伸缩，可以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。
- **服务治理**：深度集成应用服务网格，提供开箱即用的应用服务网格流量治理能力，用户无需修改代码，即可实现灰度发布、流量治理和流量监控能力。
- **容器运维**：深度集成容器智能分析，可实时监控应用及资源，支持采集、管理、分析日志，采集各项指标及事件并提供一键开启的告警能力。
- **扩展插件市场**：提供了多种类型的插件，用于管理集群的扩展功能，以支持选择性扩展满足特性需求的功能。

## 云容器引擎学习路径

您可以借助云容器引擎[成长地图](#)，快速了解产品，由浅入深学习使用和运维 CCE。

# 2 产品优势

## 云容器引擎的优势

云容器引擎是基于业界主流的Docker和Kubernetes开源技术构建的容器服务，提供众多契合企业大规模容器集群场景的功能，在系统可靠性、高性能、开源社区兼容性等多个方面具有独特的优势，满足企业在构建容器云方面的各种需求。

### 简单易用

- 通过WEB界面一键创建CCE Standard、CCE Turbo、CCE Autopilot三种集群，支持管理虚拟机节点或裸金属节点，支持虚拟机与物理机混用场景。
- 一站式自动化部署和运维容器应用，整个生命周期都在容器服务内一站式完成。
- 通过Web界面轻松实现集群节点和工作负载的扩容和缩容，自由组合策略以应对多变的突发浪涌。
- 通过Web界面一键完成Kubernetes集群的升级。
- 深度集成应用服务网格、Helm标准模板和插件中心，真正实现开箱即用。

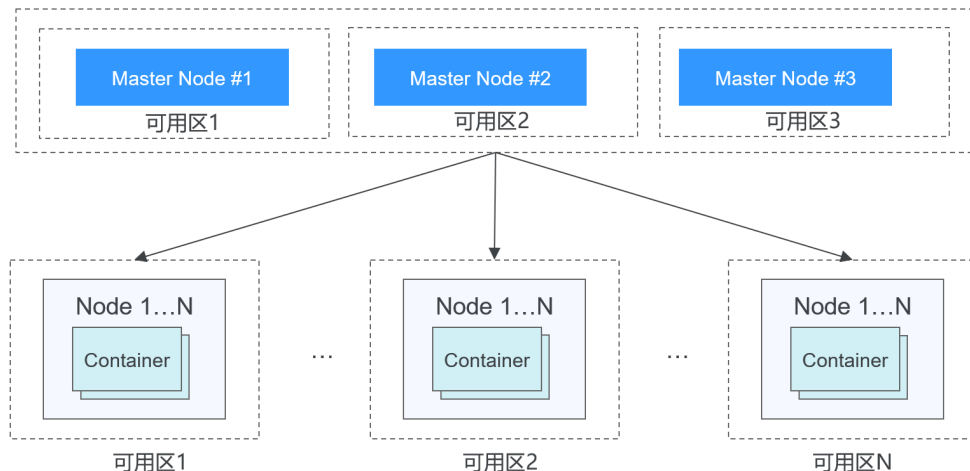
### 高性能

- 基于在计算、网络、存储、异构等方面多年的行业技术积累，提供高性能的容器集群服务，支撑业务的高并发、大规模场景。
- 采用高性能裸金属NUMA架构和高速IB网卡，AI计算性能提升3-5倍以上。

### 安全可靠

- 高可靠：集群控制面支持3 Master HA高可用，3个Master节点可以处于不同可用区，保障您的业务高可用。集群内节点和工作负载支持跨可用区（AZ）部署，帮助您轻松构建多活业务架构，保证业务系统在主机故障、机房中断、自然灾害等情况下可持续运行，获得生产环境的高稳定性，实现业务系统零中断。

图 2-1 集群高可用



- 高安全：私有集群，完全由用户掌控，并深度整合IAM和Kubernetes RBAC能力，支持用户在界面为子用户设置不同的RBAC权限。  
提供安全运行时，为每个容器（准确地说是Pod）都运行在一个单独的微型虚拟机中，拥有独立的操作系统内核，以及虚拟化层的安全隔离。

**开放兼容**

- 云容器引擎在Docker技术的基础上，为容器化的应用提供部署运行、资源调度、服务发现和动态伸缩等一系列完整功能，提高了大规模容器集群管理的便捷性。
- 云容器引擎基于业界主流的Kubernetes实现，完全兼容Kubernetes/Docker社区原生版本，与社区最新版本保持紧密同步，完全兼容Kubernetes API和KubectI。

**云容器引擎对比自建 Kubernetes 集群**

表 2-1 云容器引擎和自建 Kubernetes 集群对比

对比项	自建Kubernetes集群	云容器引擎
易用性	自建Kubernetes集群管理基础设施通常涉及安装、操作、扩展自己的集群管理软件、配置管理系统和监控解决方案，管理复杂。每次升级集群的过程都是巨大的调整，带来繁重的运维负担。	<p><b>简化集群管理，简单易用</b></p> <p>借助云容器引擎，您可以一键创建和升级Kubernetes容器集群，无需自行搭建Docker和Kubernetes集群。您可以通过云容器引擎自动化部署和一站式运维容器应用，使得应用的整个生命周期都在容器服务内高效完成。</p> <p>您可以通过云容器引擎轻松使用深度集成的应用服务网格和Helm标准模板，真正实现开箱即用。</p> <p>您只需启动容器集群，并指定想要运行的任务，云容器引擎帮您完成所有的集群管理工作，让您可以集中精力开发容器化的应用程序。</p>



对比项	自建Kubernetes集群	云容器引擎
可扩展性	自建Kubernetes集群需要根据业务流量情况和健康情况人工确定容器服务的部署，可扩展性差。	<b>灵活集群托管，轻松实现扩缩容</b> 云容器引擎可以根据资源使用情况轻松实现集群节点和工作负载的自动扩容和缩容，并可以自由组合多种弹性策略，以应对业务高峰期的突发流量浪涌。
可靠性	自建Kubernetes集群操作系统可能存在安全漏洞和配置错误，这可能导致未经授权的访问、数据泄露等安全问题。	<b>企业级的安全可靠</b> 云容器引擎提供容器优化的各类型操作系统镜像，在原生Kubernetes集群和运行时版本基础上提供额外的稳定测试和安全加固，减少管理成本和风险，并提高应用程序的可靠性和安全性。
高效性	自建Kubernetes集群需要自行搭建镜像仓库或使用第三方镜像仓库，镜像拉取方式多采用串行传输，效率低。	<b>镜像快速部署</b> 云容器引擎配合容器镜像服务，镜像拉取方式采用并行传输，确保高并发场景下能获得更快的下载速度，大幅提升容器交付效率。
成本	自建Kubernetes集群需要投入资金构建、安装、运维、扩展自己的集群管理基础设施，成本开销大。	<b>云容器引擎成本低</b> 您只需支付用于存储和运行应用程序的基础设施资源（例如云服务器、云硬盘、弹性IP/带宽、负载均衡等）费用和容器集群控制节点费用。

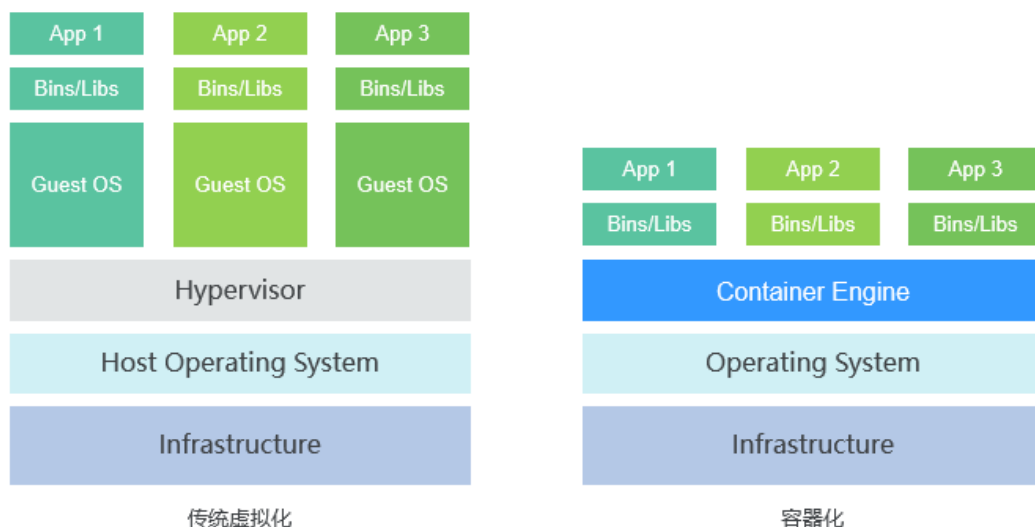
## 容器化的优势

Docker使用Google公司推出的Go语言进行开发实现，基于Linux内核的cgroup，namespace，以及AUFS类的Union FS等技术，对进程进行封装隔离，属于操作系统层面的虚拟化技术。由于隔离的进程独立于宿主和其它的隔离的进程，因此也称其为容器。

Docker在容器的基础上，进行了进一步的封装，从文件系统、网络互联到进程隔离等，极大的简化了容器的创建和维护。

传统虚拟机技术通过Hypervisor将宿主机的硬件资源（如内存、CPU、网络、磁盘等）进行了虚拟化分配，然后通过这些虚拟化的硬件资源组成了虚拟机，并在上面运行一个完整的操作系统，每个虚拟机需要运行自己的系统进程。而容器内的应用进程直接运行于宿主机操作系统内核，没有硬件资源虚拟化分配的过程，避免了额外的系统进程开销，因此使得Docker技术比虚拟机技术更为轻便、快捷。

图 2-2 传统虚拟化和容器化方式的对比



作为一种新兴的虚拟化方式，Docker跟虚拟机相比具有众多的优势：

### 更高效的利用系统资源

由于容器不需要进行硬件虚拟化分配以及运行完整操作系统等额外开销，Docker对系统资源的利用率更高。无论是应用执行速度、内存损耗或者文件存储速度，都要比传统虚拟机技术更高效。因此，相比虚拟机技术，一个相同配置的主机，往往可以运行更多数量的应用。

### 更快速的启动时间

传统的虚拟机技术启动应用服务往往需要数分钟，而Docker容器应用，由于直接运行于宿主内核，无需启动完整的操作系统，因此可以做到秒级、甚至毫秒级的启动时间。大大的节约了开发、测试、部署的时间。

### 一致的运行环境

开发过程中一个常见的问题是环境一致性问题。由于开发环境、测试环境、生产环境不一致，导致有些bug并未在开发过程中被发现。而Docker的镜像提供了除内核外完整的运行时环境，确保了应用运行环境一致性。

### 持续交付和部署

对开发和运维（DevOps）人员来说，最希望的就是一次创建或配置，可以在任意地方正常运行。

使用Docker可以通过定制应用镜像来实现持续集成、持续交付、部署。开发人员可以通过Dockerfile来进行镜像构建，并结合持续集成（Continuous Integration）系统进行集成测试，而运维人员则可以直接在生产环境中快速部署该镜像，甚至结合持续部署（Continuous Delivery/Deployment）系统进行自动部署。

而且使用Dockerfile使镜像构建透明化，不仅开发团队可以理解应用运行环境，也方便运维团队理解应用运行所需条件，帮助更好的生产环境中部署该镜像。

### 更轻松的迁移

由于Docker确保了执行环境的一致性，使得应用的迁移更加容易。Docker可以在很多平台上运行，无论是物理机、虚拟机、公有云、私有云，甚至是笔记本，其运行结果

是一致的。因此用户可以很轻易地将在一个平台上运行的应用，迁移到另一个平台上，而不用担心运行环境的变化导致应用无法正常运行的情况。

### 更轻松的维护和扩展

Docker使用的分层存储以及镜像的技术，使得应用重复部分的复用更为容易，也使得应用的维护更新更加简单，基于基础镜像进一步扩展镜像也变得非常简单。此外，Docker团队同各个开源项目团队一起维护了一大批高质量的官方镜像，既可以直接在生产环境使用，又可以作为基础进一步定制，大大的降低了应用服务的镜像制作成本。

表 2-2 容器对比传统虚拟机总结

特性	容器	虚拟机
启动	秒级	分钟级
硬盘使用	一般为MB	一般为GB
性能	接近原生	弱
系统支持量	单机支持上千个容器	一般几十个

# 3 应用场景

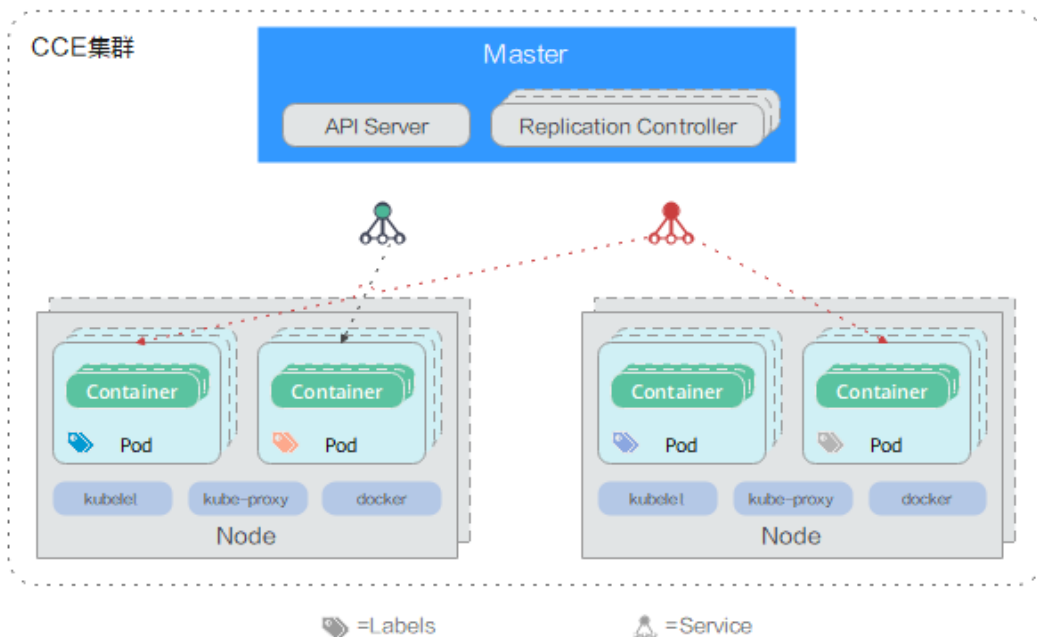
## 3.1 容器应用管理

### 应用场景

CCE集群支持管理X86和ARM资源，能够轻松创建Kubernetes集群、部署容器化应用，并方便地进行管理和维护。

- 容器化Web应用：使用CCE集群，能帮助用户快速部署Web业务应用，对接华为云中间件（如GaussDB、Redis），并支持配置高可用容灾、自动弹性伸缩、发布公网、灰度升级等。
- 中间件部署平台：CCE集群可以作为中间件的部署平台，使用StatefulSet、PVC等资源配置，能够实现应用的有状态化，同时配套弹性负载均衡实例，可实现中间件服务的对外发布。
- 执行普通任务、定时任务：使用容器化方式运行Job、CronJob类型应用，帮助业务降低对主机系统配置的依赖，全局的资源调度既保证任务运行时资源量，也提高集群下整体资源利用率。

图 3-1 CCE 集群



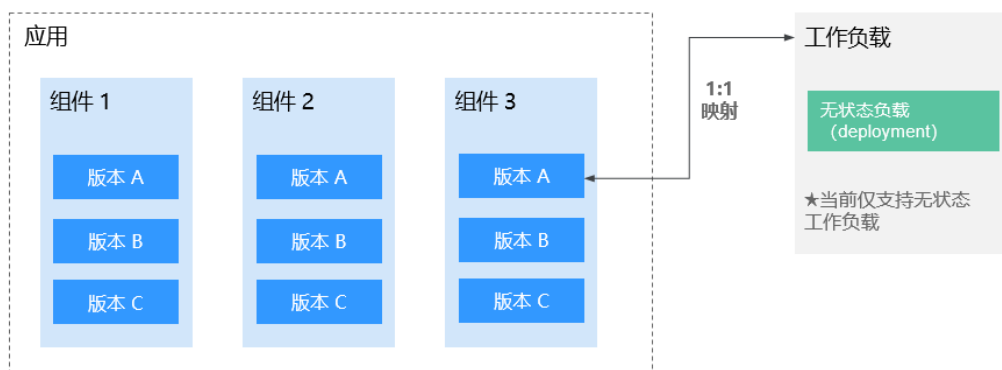
## 价值

通过容器化改造，使应用部署资源成本降低，提升应用的部署效率和升级效率，可以实现升级时业务不中断以及统一的自动化运维。

## 优势

- 多种类型的容器部署  
支持部署无状态工作负载、有状态工作负载、守护进程集、普通任务、定时任务等。
- 应用升级  
支持替换升级、滚动升级（按比例、实例个数进行滚动升级）；支持升级回滚。
- 弹性伸缩  
支持节点和工作负载的弹性伸缩。

图 3-2 工作负载



## 3.2 秒级弹性伸缩

### 应用场景

- 电商客户遇到促销、限时抢购等活动期间，访问量激增，需及时、自动扩展云计算资源。
- 视频直播客户业务负载变化难以预测，需要根据CPU/内存使用率进行实时扩缩容。
- 游戏客户每天中午12点及晚上18:00-23:00间需求增长，需要定时扩容。

### 价值

云容器引擎可根据用户的业务需求预设策略自动调整计算资源，使云服务器或容器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行，节省成本。

### 优势

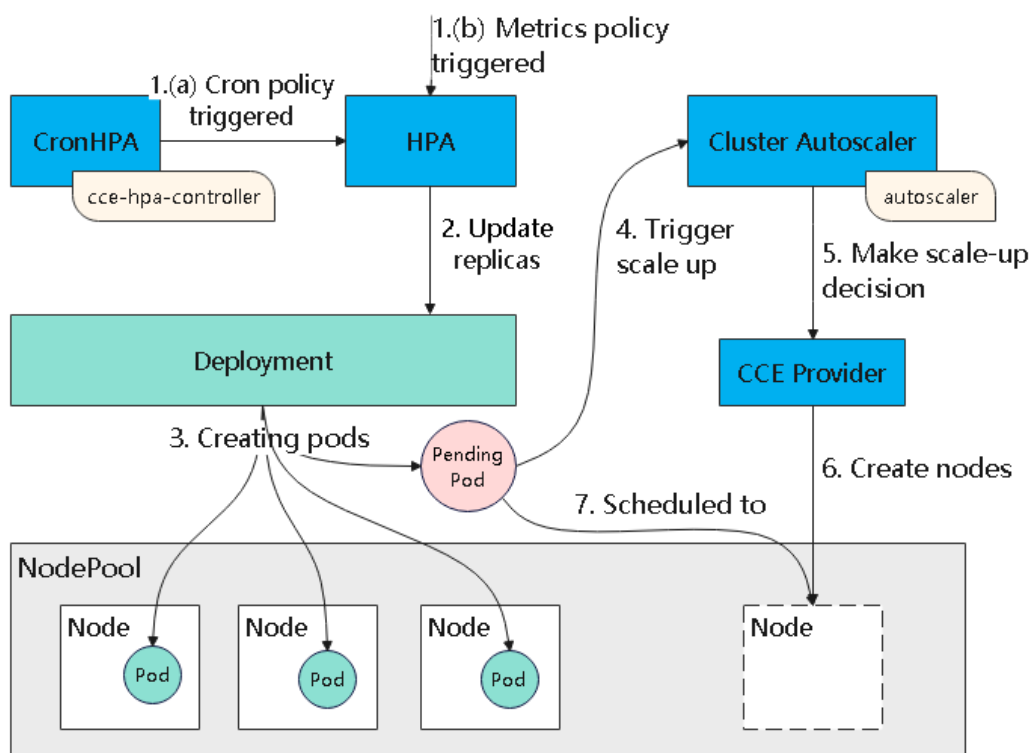
- 自由灵活  
支持多种策略配置，业务流量达到扩容指标，秒级触发容器扩容操作。
- 高可用  
自动检测伸缩组中实例运行状况，启用新实例替换不健康实例，保证业务健康可用。
- 低成本  
只按照实际用量收取云服务器费用。

### 建议搭配使用

插件部署：autoscaler、cce-hpa-controller

- 工作负载弹性：CronHPA ( CronHorizontalPodAutoscaler ) + HPA ( Horizontal Pod Autoscaling )
- 集群节点弹性：CA ( Cluster AutoScaling )

图 3-3 弹性伸缩场景



## 3.3 微服务流量治理

### 应用场景

伴随着互联网技术的不断发展，各大企业的系统越来越复杂，传统的系统架构越来越不能满足业务的需求，取而代之的是微服务架构。微服务是将复杂的应用切分为若干服务，每个服务均可以独立开发、部署和伸缩；微服务和容器组合使用，可进一步简化微服务的交付，提升应用的可靠性和可伸缩性。

随着微服务的大量应用，其构成的分布式应用架构在运维、调试和安全管理等维度变得更加复杂，在管理微服务时，往往需要在业务代码中添加微服务治理相关的代码，导致开发人员不能专注于业务开发，还需要考虑微服务治理的解决方案，并且将解决方案融合到其业务系统中。

### 价值

云容器引擎深度集成应用服务网格，提供开箱即用的应用服务网格流量治理能力，用户无需修改代码，即可实现灰度发布、流量治理和流量监控能力。

### 优势

- 开箱即用  
与云容器引擎无缝对接，一键开启后即可提供非侵入的智能流量治理解决方案。
- 策略化智能路由  
无需修改代码，即可实现HTTP、TCP等服务连接策略和安全策略。

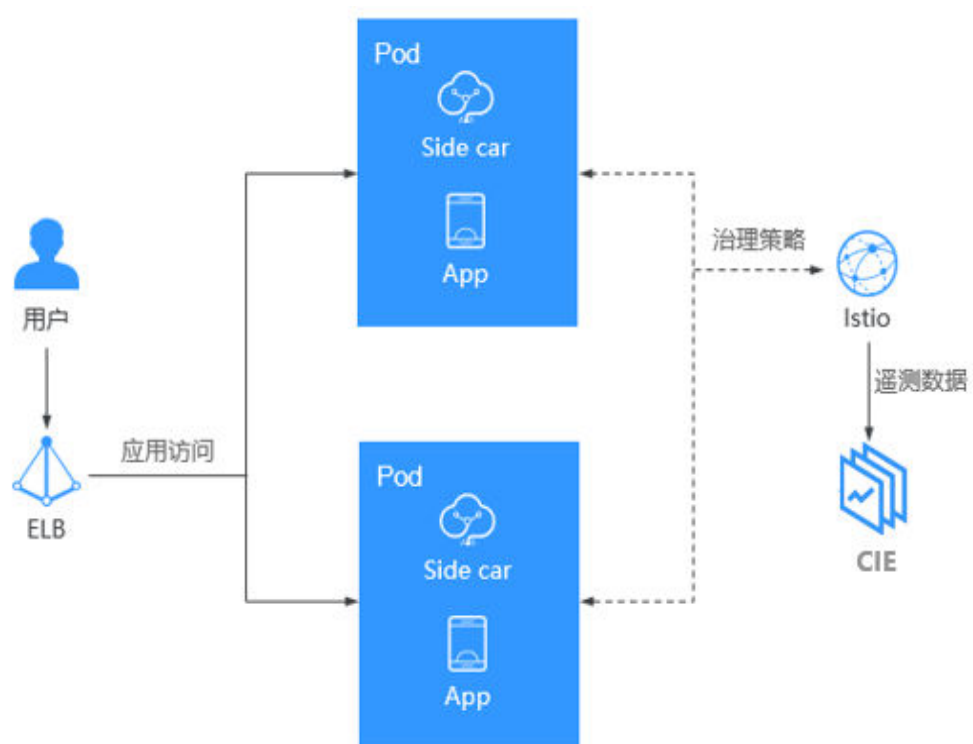
- 流量治理可视化

基于无侵入的监控数据采集，深度整合APM能力，提供实时流量拓扑、调用链等服务性能监控和运行诊断，构建全景的服务运行视图，可实时、一站式观测服务流量健康和性能状态。

## 建议搭配使用

弹性负载均衡ELB + 应用性能管理APM + 应用运维管理AOM

图 3-4 微服务治理场景



## 3.4 DevOps 持续交付

### 应用场景

当前IT行业发展日益快速，面对海量需求必须具备快速集成的能力。经过快速持续集成，才能保证不间断的补充用户体验，提升服务质量，为业务创新提供源源不断的动力。大量交付实践表明，不仅传统企业，甚至互联网企业都可能在持续集成方面存在研发效率低、工具落后、发布频率低等方面的问题，需要通过持续交付提高效率，降低发布风险。

### 价值

云容器引擎搭配容器镜像服务提供DevOps持续交付能力，能够基于代码源自动完成代码编译、镜像构建、灰度发布、容器化部署，实现一站式容器化交付流程，并可对接已有CI/CD，完成传统应用的容器化改造和部署。



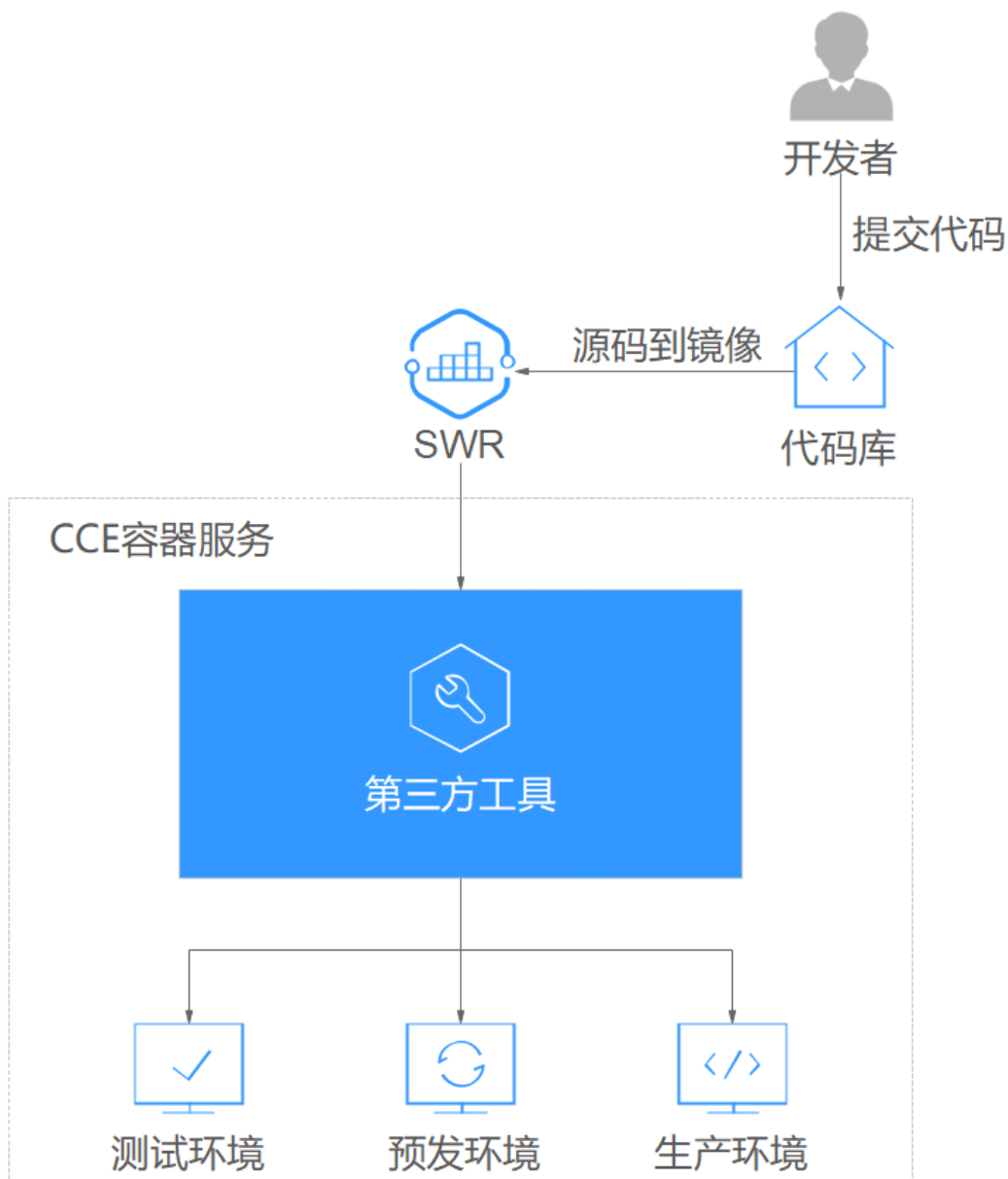
## 优势

- 高效流程管理  
更优的流程交互设计，脚本编写量较传统CI/CD流水线减少80%以上，让CI/CD管理更高效。
- 灵活的集成方式  
提供丰富的接口便于与企业已有CI/CD系统进行集成，灵活适配企业的个性化诉求。
- 高性能  
全容器化架构设计，任务调度更灵活，执行效率更高。

## 建议搭配使用

容器镜像服务SWR + 对象存储服务OBS + 虚拟专用网络VPN

图 3-5 DevOps 持续交付场景



## 3.5 混合云

### 应用场景

- 多云部署、容灾备份  
为保证业务高可用，需要将业务同时部署在多个云的容器服务上，在某个云出现事故时，通过统一流量分发的机制，自动地将业务流量切换到其他云上。
- 流量分发、弹性伸缩  
大型企业客户需要将业务同时部署在不同地域的云机房中，并能根据业务的波峰波谷进行自动弹性扩容和缩容，以节约成本。
- 业务上云、数据本地托管

对于金融、医疗等行业用户，由于安全合规要求，敏感数据要求存储在本地IDC中，而一般业务由于高并发、快响应等方面的特点需要部署在云上，并需要进行统一管理。

- 开发与部署分离  
出于IP安全的考虑，用户希望将生产环境部署在公有云上，而将开发环境部署在本地的IDC。

## 价值

云容器引擎利用容器环境无关的特性，将私有云和公有云容器服务实现网络互通和统一管理，应用和数据可在云上云下无缝迁移，满足复杂业务系统对弹性伸缩、灵活性、安全性与合规性的不同要求，并可统一运维多个云端资源，从而实现资源的灵活使用以及业务容灾等目的。

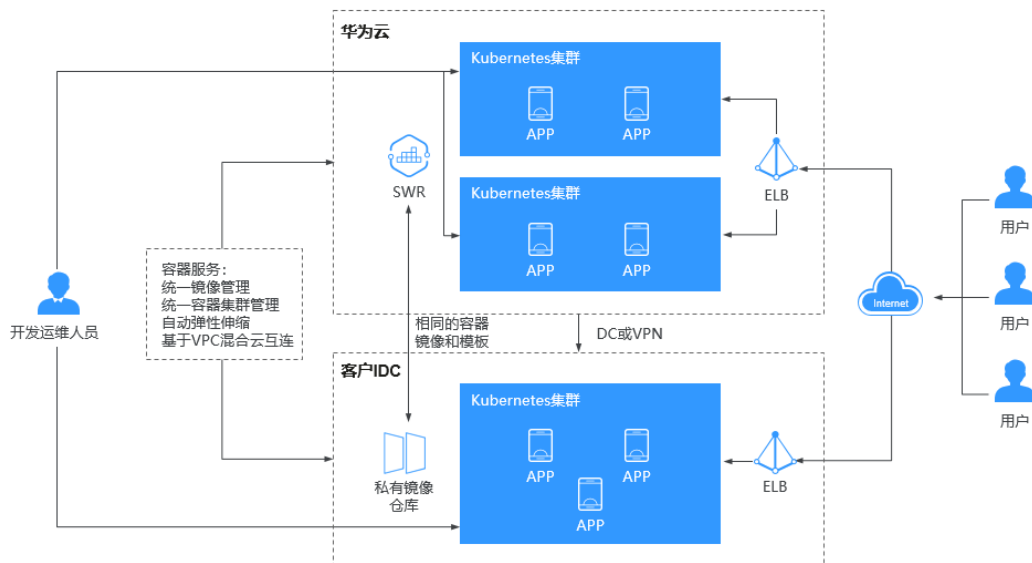
## 优势

- 云上容灾  
通过云容器引擎，可以将业务系统同时部署在多个云的容器服务上，统一流量分发，单云故障后能够自动将业务流量切换到其他云上，并能快速自动解决现网事故。
- 统一架构，高弹性  
云上云下同架构平台，可灵活根据流量峰值实现资源在云上云下的弹性伸缩、平滑迁移和扩容。
- 计算与数据分离，能力共享  
通过云容器引擎，用户可以实现敏感业务数据与一般业务数据的分离，可以实现开发环境和生产环境分离，可以实现特殊计算能力与一般业务的分离，并能够实现弹性扩展和集群的统一管理，达到云上云下资源和能力的共享。
- 降低成本  
业务高峰时，利用公有云资源池快速扩容，用户不再需要根据流量峰值始终保持和维护大量资源，节约成本。

## 建议搭配使用

弹性云服务器ECS + 云专线DC + 虚拟专用网络VPN + 容器镜像服务SWR

图 3-6 混合云场景



## 3.6 高性能调度

CCE通过集成Volcano提供高性能计算能力。

Volcano是基于Kubernetes的批处理系统。Volcano提供了一个针对BigData和AI场景下，通用、可扩展、高性能、稳定的原生批量计算平台，方便AI、大数据、基因、渲染等诸多行业通用计算框架接入，提供高性能任务调度引擎、高性能异构芯片管理、高性能任务运行管理等能力。

### 应用场景 1：多类型作业混合部署

随着各行各业的发展，涌现出越来越多的领域框架来支持业务的发展，这些框架都在相应的业务领域有着不可替代的作用，例如Spark，Tensorflow，Flink等。在业务复杂性不断增加的情况下，单一的领域框架很难应对现在复杂的业务场景，因此现在普遍使用多种框架达成业务目标。但随着各个领域框架集群的不断扩大，以及单个业务的波动性，各个子集群的资源浪费比较严重，越来越多的用户希望通过统一调度系统来解决资源共享的问题。

Volcano在Kubernetes之上抽象了一个批量计算的通用基础层，向下弥补Kubernetes调度能力的不足，向上提供灵活通用的Job抽象。Volcano通过提供多任务模板功能实现了利用Volcano Job描述多种作业类型（Tensorflow、Spark、MPI、PyTorch等），并通过Volcano统一调度系统实现多种作业混合部署，解决集群资源共享问题。

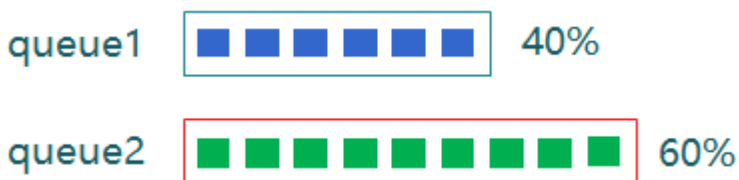


## 应用场景 2：多队列场景调度优化

用户在使用集群资源的时候通常会涉及到资源隔离与资源共享，Kubernetes中没有队列的支持，所以它在多个用户或多个部门共享一个机器时无法做资源共享。但不管在HPC还是大数据领域中，通过队列进行资源共享都是基本的需求。

在通过队列做资源共享时，CCE提供了多种机制。可以为队列设置weight值，集群通过计算该队列weight值占所有weight总和的比例来给队列划分资源；另外也可以为队列设置资源的Capability值，来确定该队列能够使用的资源上限。

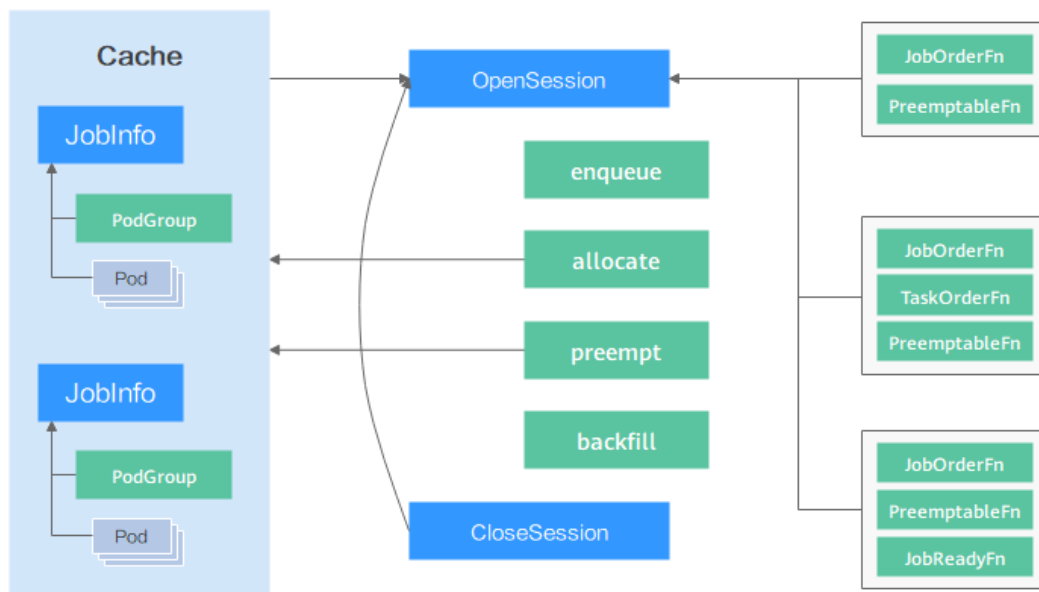
例如下图中，通过这两个队列去共享整个集群的资源，一个队列获得40%的资源，另一个队列获得60%的资源，这样可以把两个不同的队列映射到不同的部门或者是不同的项目中。并且在一个队列里如果有多余的空闲资源，可以把这些空闲资源分配给另外一个队列里面的作业去使用。



## 应用场景 3：多种高级调度策略

当用户向Kubernetes申请容器所需的计算资源（如CPU、Memory、GPU等）时，调度器负责挑选出满足各项规格要求的节点来部署这些容器。通常，满足各项要求的节点并非唯一，且水位（节点已有负载）各不相同，不同的分配方式最终得到的分配率存在差异，因此，调度器的一项核心任务就是以最终资源利用率最优的目标从众多候选机器中挑出最合适的节点。

下图为Volcano scheduler调度流程，首先将API server中的Pod、PodGroup信息加载到scheduler cache中。Scheduler周期被称为session，每个scheduler周期会经历OpenSession，调用Action，CloseSession三个阶段。其中OpenSession阶段加载用户配置的scheduler plugin中实现的调度策略；调用Action阶段逐一调用配置的动作以及在OpenSession阶段加载的调度策略；CloseSession为清理阶段。



Volcano scheduler通过插件方式提供了多种调度Action（例如enqueue, allocate, preempt, backfill）以及调度策略（例如gang, priority, drf, proportion, binpack等），用户可以根据实际业务需求进行配置。通过实现Scheduler提供的接口也可以方便灵活地进行定制化开发。

#### 应用场景 4：高精度资源调度

Volcano 在支持AI，大数据等作业的时候提供了高精度的资源调度策略，例如在深度学习场景下计算效率非常重要。以TensorFlow计算为例，配置“ps”和“worker”之间的亲和性，以及“ps”与“ps”之间的反亲和性，可使“ps”和“worker”尽量调度到同一台节点上，从而提升“ps”和“worker”之间进行网络和数据交互的效率，进而提升计算效率。然而Kubernetes默认调度器在调度Pod过程中，仅会检查Pod与现有集群下所有已经处于运行状态Pod的亲和性和反亲和性配置是否冲突或吻合，并不会考虑接下来可能会调度的Pod造成的影响。

Volcano提供的Task-topology算法是一种根据Job内task之间亲和性和反亲和性配置计算task优先级和Node优先级的算法。通过在Job内配置task之间的亲和性和反亲和性策略，并使用task-topology算法，可优先将具有亲和性配置的task调度到同一个节点上，将具有反亲和性配置的Pod调度到不同的节点上。同样是处理亲和性和反亲和性配置对Pod调度的影响，task-topology算法与Kubernetes默认调度器处理的不同点在于，task-topology将待调度的Pods作为一个整体进行亲和性和反亲和性考虑，在批量调度Pod时，考虑未调度Pod之间的亲和性和反亲和性影响，并通过优先级施加到Pod的调度进程中。

#### 应用场景 5：在线离线作业混合部署

当前很多业务有波峰和波谷，部署服务时，为了保证服务的性能和稳定性，通常会按照波峰时需要的资源申请，但是波峰的时间可能很短，这样在非波峰时段就有资源浪费。另外，由于在线作业SLA要求较高，为了保证服务的性能和可靠性，通常会申请大量的冗余资源，因此，会导致资源利用率很低、浪费比较严重。将这些申请而未使用的资源（即申请量与使用量的差值）利用起来，就是资源超卖。超卖资源适合部署离线作业，离线作业通常关注吞吐量，SLA要求不高，容忍一定的失败。在线作业和离线作业混合部署在Kubernetes集群中将有效的提升集群整体资源利用率。

目前Kubernetes的默认调度器是以Pod为单位进行调度的，不区分Pod中运行的业务类型。因此无法满足混部场景对资源分配的特殊要求。针对上述问题，Volcano实现了基

于应用模型感知的智能调度算法，根据用户提交的作业类型，针对其应用模型对资源的诉求和整体应用负载的情况，优化调度方式，通过资源抢占，分时复用等机制减少集群资源的空闲比例。

## 价值

面向AI计算的容器服务，采用高性能GPU计算实例，并支持多容器共享GPU资源，在AI计算性能上比通用方案提升3~5倍以上，并大幅降低了AI计算的成本，同时帮助数据工程师在集群上轻松部署计算应用，您无需关心复杂的部署运维，专注核心业务，快速实现从0到1快速上线。

## 优势

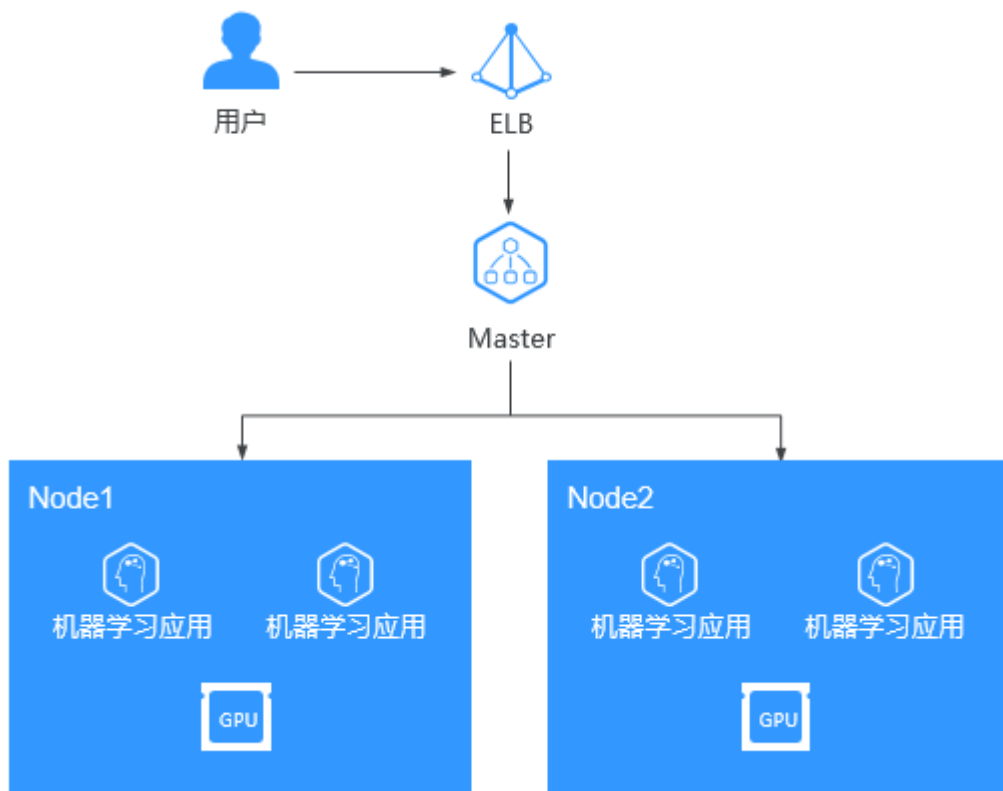
CCE通过集成Volcano，在高性能计算、大数据、AI等领域有如下优势：

- 多种类型作业混合部署：支持AI、大数据、HPC作业类型混合部署。
- 多队列场景调度优化：支持分队列调度，提供队列优先级、多级队列等复杂任务调度能力。
- 多种高级调度策略：支持gang-scheduling、公平调度、资源抢占、GPU拓扑等高级调度策略。
- 多任务模板：支持单一Job多任务模板定义，打破Kubernetes原生资源束缚，Volcano Job描述多种作业类型（Tensorflow、MPI、PyTorch等）。
- 作业扩展插件配置：在提交作业、创建Pod等多个阶段，Controller支持配置插件用来执行自定义的环境准备和清理的工作，比如常见的MPI作业，在提交前就需要配置SSH插件，用来完成Pod资源的SSH信息配置。
- 在线离线业务混部：支持集群内在离线作业混部以及节点CPU和内存资源超卖，提升集群整体资源利用率。

## 建议搭配使用

GPU加速云服务器 + 弹性负载均衡ELB + 对象存储服务OBS

图 3-7 AI 计算





# 4 安全

## 4.1 责任共担

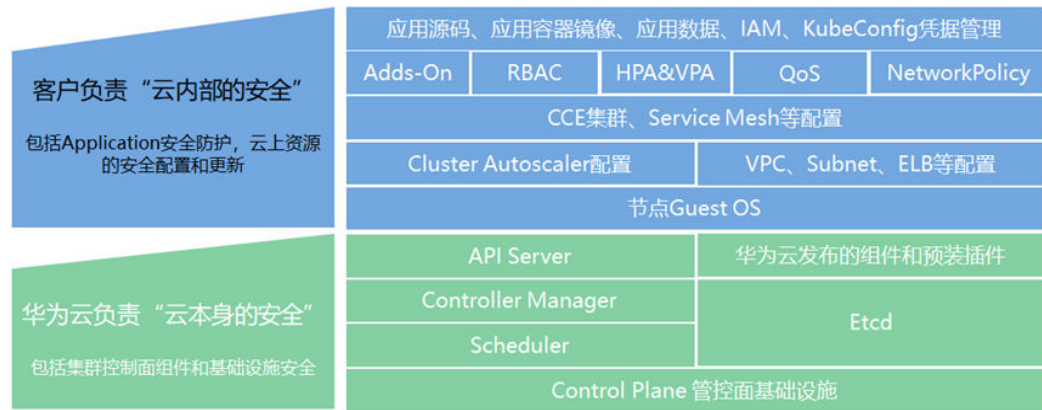
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图4-1所示。

- **华为云**：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务内部的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 4-1 CCE 服务安全责任共担模型



## 4.2 数据保护技术

CCE通过多种数据保护手段和特性，保障数据的安全可靠。

表 4-1 CCE 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
服务发现支持证书配置	CCE集群中的应用服务支持使用HTTPS传输协议，保证数据传输的安全性，您可以根据需求创建四层或七层的访问方式来对接负载均衡器。	<a href="#">七层证书配置</a> <a href="#">四层证书配置</a>
高可用部署	CCE为您提供高可用的部署方案： <ul style="list-style-type: none"> <li>• 集群支持3个控制节点的高可用模式</li> <li>• Node节点支持分布在不同AZ</li> <li>• 创建工作负载时支持选用不同可用区或节点</li> </ul>	<a href="#">容灾部署</a>
磁盘加密	CCE支持多种存储类型，满足各类高可用以及部分存储加密场景，可为您的数据提供强大的安全防护。	<a href="#">存储概览</a>
集群密钥配置	密钥（Secret）是一种用于存储工作负载所需要认证信息、密钥的敏感信息等的集群资源类型，内容由用户决定。资源创建完成后，可在容器工作负载中作为文件或者环境变量使用。	<a href="#">密钥配置</a>
敏感操作保护	CCE控制台支持敏感操作保护，开启后执行删除集群敏感操作时，系统会进行身份验证，进一步保证CCE的安全性。	<a href="#">敏感操作保护介绍</a>

## 4.3 审计与日志

### 审计

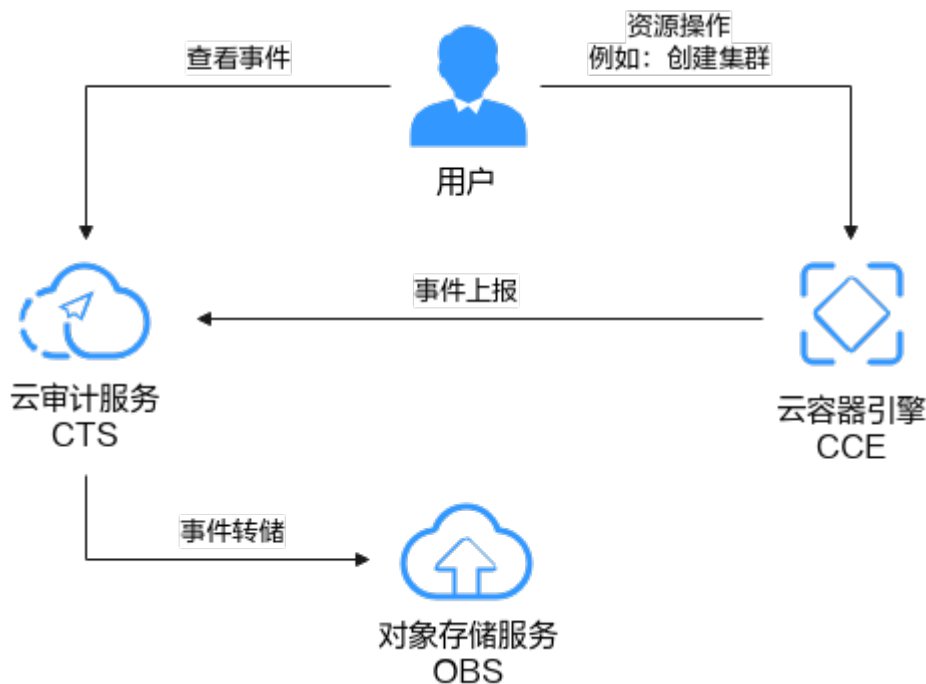
云审计服务（Cloud Trace Service, CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，系统将开始记录CCE资源的操作，并为您保存最近7天的操作记录。CTS支持记录的CCE操作请参见[云审计服务支持CCE操作列表](#)。

CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。

CCE用户查看云审计日志方法，请参见[云审计日志](#)。

图 4-2 云审计服务



### 日志

CCE支持配置工作负载日志策略，便于日志的统一收集、管理和分析，同时支持按周期进行防爆处理。

CCE配合AOM收集工作负载的日志，在创建节点时会默认安装AOM的ICAgent（在集群kube-system命名空间下名为icagent的DaemonSet），ICAgent负责收集工作负载的日志（支持\*.log、\*.trace和\*.out类型的文本日志文件）并上报到AOM，您可以在CCE控制台和AOM控制台查看工作负载的日志。

关于CCE工作负载日志记录的详细介绍和配置方法，请参见[容器日志](#)。

## 4.4 监控安全风险

结合应用运维管理AOM服务，CCE提供基于Kubernetes原生类型的容器监控能力，可实时监控应用及资源，采集各项指标及事件等数据以分析应用健康状态，提供全面、清晰、多维度数据可视化能力。此外，您还可以根据自己的需求，采集和监控工作负载的自定义指标，实现个性化的监控策略。

- 资源监控指标

资源基础监控包含CPU/内存/磁盘等指标数据，您可以全面监控集群的健康状态和负荷程度，具体请参见[监控概述](#)。您可以在CCE控制台从集群、节点、工作负载等维度查看这些监控指标数据，也可以在AOM中查看。

- 自定义指标

CCE支持采集应用程序中的自定义指标并上传到AOM，为您提供个性化的监控服务。您可以根据特定业务需求，扩展监控指标范围，具体使用方法请参见[自定义监控](#)。

## 4.5 认证证书

### 合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行[申请下载](#)合规资质证书。

图 4-3 合规证书下载

### 合规证书下载

请输入关键字搜索

 <p><b>BS 10012:2017</b></p> <p>BS 10012为个人信息管理体系提供了一个符合欧盟GDPR原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。保留或处理与个人相关的个人记录时需要考虑的核心需求。</p> <p><a href="#">下载</a></p>	 <p><b>CSA STAR认证</b></p> <p>CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。</p> <p><a href="#">下载</a></p>	 <p><b>ISO 20000-1:2018</b></p> <p>ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的IT服务来满足客户和业务的需求。</p> <p><a href="#">下载</a></p>
 <p><b>SOC 1 类型II 报告 2022.04.01-2023.03.31</b></p> <p>华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和具独立审计师。</p> <p><a href="#">下载</a></p>	 <p><b>SOC 1 类型II 报告 2022.10.01-2023.09.30</b></p> <p>华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为 2022.10.01-2023.09.30。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和具独立审计师。</p> <p><a href="#">下载</a></p>	 <p><b>SOC 2 类型II 报告 2022.04.01-2023.03.31</b></p> <p>华为云每年滚动发布两期SOC2报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 2报告着重于组织的内部运作与合规，包括安全性、可用性、进程完整性、保密性、隐私性五大控制属性。</p> <p><a href="#">下载</a></p>

## 资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看[资源中心](#)。

图 4-4 资源中心



## 销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看[合规资质证书](#)。

图 4-5 销售许可证&软件著作权证书



# 5 权限管理

CCE权限管理是在统一身份认证服务（IAM）与Kubernetes的角色访问控制（RBAC）的能力基础上，打造的细粒度权限管理功能，支持基于IAM的细粒度权限控制和IAM Token认证，支持集群级别、命名空间级别的权限控制，帮助用户便捷灵活的对租户下的IAM用户、用户组设定不同的操作权限。

CCE的权限管理包括“集群权限”和“命名空间权限”两种能力，能够从集群和命名空间层面对用户组或用户进行细粒度授权，具体解释如下：

- **集群权限**：是基于IAM系统策略的授权，可以通过用户组功能实现IAM用户的授权。用户组是用户的集合，通过集群权限设置可以让某些用户组操作集群（如创建/删除集群、节点、节点池、模板、插件等），而让某些用户组仅能查看集群。集群权限涉及非Kubernetes原生提供的API，支持IAM细粒度策略、企业项目管理相关能力。
- **命名空间权限**：是基于Kubernetes RBAC能力的授权，通过权限设置可以让不同的用户或用户组拥有操作不同Kubernetes资源的权限（如**工作负载、任务、服务等Kubernetes原生资源**）。同时CCE基于开源能力进行了增强，可以支持基于IAM用户或用户组粒度进行RBAC授权、IAM token直接访问API进行RBAC认证鉴权。  
命名空间权限涉及CCE Kubernetes API，基于Kubernetes RBAC能力进行增强，支持对接IAM用户/用户组进行授权和认证鉴权，但与IAM细粒度策略独立，详见[Kubernetes RBAC](#)。

## 注意

- 集群权限仅针对与集群相关的资源（如集群、节点等）有效，您必须确保同时配置了**命名空间权限**，才能有操作Kubernetes资源（如工作负载、任务、Service等）的权限。
- 任何用户创建集群后，CCE会自动为该用户添加该集群的所有命名空间的cluster-admin权限，也就是说该用户允许对集群以及所有命名空间中的全部资源进行完全控制。
- 使用CCE控制台查看集群时，显示情况依赖于命名空间权限的设置情况，如果没有设置命名空间权限，则无法查看集群下的资源。

## 集群权限（IAM 系统策略授权）

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CCE部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CCE时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- **角色：** IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- **策略：** IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CCE服务，租户（Domain）能够控制用户仅能对某一类集群和节点资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，CCE支持的API授权项请参见[权限策略和授权项](#)。

如表5-1所示，包括了CCE的所有系统权限。

表 5-1 CCE 系统权限

系统角色/策略名称	描述	类别	依赖关系
CCE Administrator	具有CCE集群及集群下所有资源（包含集群、节点、工作负载、任务、服务等）的读写权限。	系统角色	<p>拥有该权限的用户必须同时拥有以下权限：</p> <p><b>全局服务：</b> OBS Buckets Viewer、OBS Administrator。</p> <p><b>区域级项目：</b> Tenant Guest、Server Administrator、ELB Administrator、SFS Administrator、SWR Admin、APM FullAccess。</p> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>● 如果同时拥有NAT Gateway Administrator权限，则可以在集群中使用NAT网关的相关功能。</li> <li>● 如果IAM子用户需要对其他用户或用户组进行集群命名空间授权，则该用户需要拥有IAM只读权限。</li> </ul>



系统角色/ 策略名称	描述	类别	依赖关系
CCE FullAccess	CCE服务集群相关资源的普通操作权限，不包括集群（启用Kubernetes RBAC鉴权）的命名空间权限，不包括委托授权、生成集群证书等管理员角色的特权操作。	策略	无
CCE ReadOnly Access	CCE服务集群相关资源的查看权限，不包括集群（启用Kubernetes RBAC鉴权）的命名空间权限。	策略	无

表 5-2 CCE 常用操作与系统权限的关系

操作	CCE ReadOnlyAccess	CCE FullAccess	CCE Administrator
创建集群	x	√	√
删除集群	x	√	√
更新集群，如后续允许集群支持RBAC，调度参数更新等	x	√	√
升级集群	x	√	√
唤醒集群	x	√	√
休眠集群	x	√	√
查询集群列表	√	√	√
查询集群详情	√	√	√
添加节点	x	√	√
删除节点/批量删除节点	x	√	√
更新节点，如更新节点名称	x	√	√
查询节点详情	√	√	√
查询节点列表	√	√	√



操作	CCE ReadOnlyAccess	CCE FullAccess	CCE Administrator
查询任务列表（集群层面的job）	√	√	√
删除任务/批量删除任务（集群层面的job）	x	√	√
查询任务详情（集群层面的job）	√	√	√
创建存储	x	√	√
删除存储	x	√	√
操作所有kubernetes资源。	√（需Kubernetes RBAC授权）	√（需Kubernetes RBAC授权）	√
容器智能分析所有资源查看权限	√	√	√
容器智能分析所有资源操作权限	x	√	√
告警助手所有资源查看权限	√	√	√
告警助手所有资源操作权限	x	√	√
ECS（弹性云服务器）服务的所有权限。	x	√	√
EVS（云硬盘）的所有权限。 可以将云硬盘挂载到云服务器，并可以随时扩容云硬盘容量	x	√	√
VPC（虚拟私有云）的所有权限。 创建的集群需要运行在虚拟私有云中，创建命名空间时，需要创建或关联VPC，创建在命名空间的容器都运行在VPC之内。	x	√	√
ECS（弹性云服务器）所有资源详情的查看权限。 CCE中的一个节点就是具有多个云硬盘的一台弹性云服务器	√	√	√

操作	CCE ReadOnlyAccess	CCE FullAccess	CCE Administrator
ECS（弹性云服务器）所有资源列表的查看权限。	√	√	√
EVS（云硬盘）所有资源详情的查看权限。可以将云硬盘挂载到云服务器，并可以随时扩容云硬盘容量	√	√	√
EVS（云硬盘）所有资源列表的查看权限。	√	√	√
VPC（虚拟私有云）所有资源详情的查看权限。 创建的集群需要运行在虚拟私有云中，创建命名空间时，需要创建或关联VPC，创建在命名空间的容器都运行在VPC之内	√	√	√
VPC（虚拟私有云）所有资源列表的查看权限。	√	√	√
ELB（弹性负载均衡）服务所有资源详情的查看权限。	x	x	√
ELB（弹性负载均衡）服务所有资源列表的查看权限。	x	x	√
SFS（弹性文件服务）服务所有资源详情的查看权限。	√	√	√
SFS（弹性文件服务）服务所有资源列表查看权限。	√	√	√
AOM（应用运维管理）服务所有资源详情的查看权限。	√	√	√
AOM（应用运维管理）服务所有资源列表的查看权限。	√	√	√
AOM（应用运维管理）服务自动扩缩容规则的所有操作权限。	√	√	√

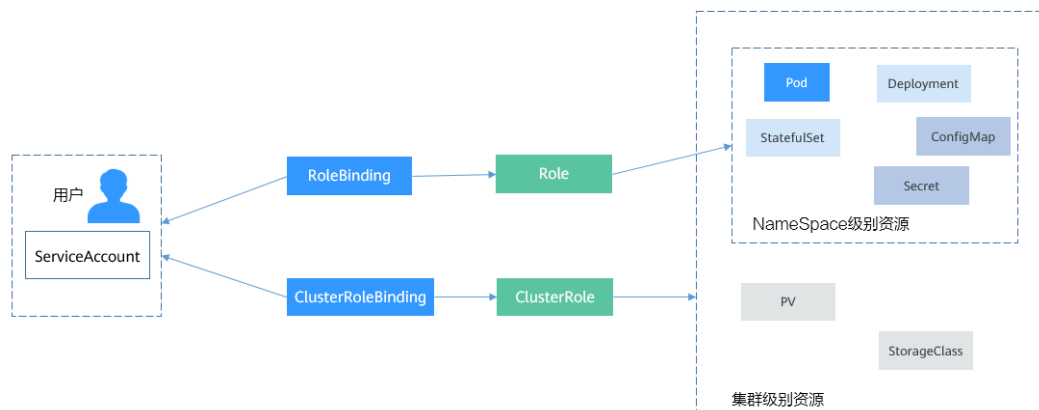
## 命名空间权限（kubernetes RBAC 授权）

命名空间权限是基于Kubernetes RBAC能力的授权，通过权限设置可以让不同的用户或用户组拥有操作不同Kubernetes资源的权限。Kubernetes RBAC API定义了四种类型：Role、ClusterRole、RoleBinding与ClusterRoleBinding，这四种类型之间的关系和简要说明如下：

- Role：角色，其实是定义一组对Kubernetes资源（命名空间级别）的访问规则。
- RoleBinding：角色绑定，定义了用户和角色的关系。
- ClusterRole：集群角色，其实是定义一组对Kubernetes资源（集群级别，包含全部命名空间）的访问规则。
- ClusterRoleBinding：集群角色绑定，定义了用户和集群角色的关系。

Role和ClusterRole指定了可以对哪些资源做哪些动作，RoleBinding和ClusterRoleBinding将角色绑定到特定的用户、用户组或ServiceAccount上。如下图所示。

图 5-1 角色绑定



在CCE控制台可以授予用户或用户组命名空间权限，可以对某一个命名空间或全部命名空间授权，CCE控制台默认提供如下ClusterRole。

- view（只读权限）：对全部或所选命名空间下大多数资源的只读权限。
- edit（开发权限）：对全部或所选命名空间下多数资源的读写权限。当配置在全部命名空间时能力与运维权限一致。
- admin（运维权限）：对全部命名空间下大多数资源的读写权限，对节点、存储卷，命名空间和配额管理的只读权限。
- cluster-admin（管理员权限）：对全部命名空间下所有资源的读写权限。
- drainage-editor：节点排水操作权限，可执行节点排水。
- drainage-viewer：节点排水只读权限，仅可查看节点排水状态，无法执行节点排水。
- geip-editor-role：该权限用于在集群中使用全域弹性公网IP资源，仅对资源geips具有读写权限。
- icagent-clusterRole：该权限用于生成Kubernetes事件日志上报到LTS。

除了使用上述常用的ClusterRole外，您还可以通过定义Role和RoleBinding来进一步对全局资源（如Node、PersistentVolumes、CustomResourceDefinitions等）和命名空

间中不同类别资源（如Pod、Deployment、Service等）的增删改查权限进行配置，从而做到更加精细化的权限控制。

## 相关链接

- [IAM产品介绍](#)
- [创建用户组、用户并授权CCE权限](#)
- [策略支持的授权项](#)

# 6 约束与限制

本文主要为您介绍云容器引擎（CCE）集群使用过程中的一些限制。

## 集群/节点限制

- 集群一旦创建以后，不支持变更以下项：
  - 变更集群类型，例如“CCE Standard集群”更换为“CCE Turbo集群”。
  - 变更集群的控制节点数量，例如非高可用集群（控制节点数量为1）变更为高可用集群（控制节点数量为3）。
  - 变更控制节点可用区。
  - 变更集群的网络配置，如所在的虚拟私有云VPC、子网、容器网段、服务网段、IPv6、kubeproxy代理（转发）模式。
  - 变更网络模型，例如“容器隧道网络”更换为“VPC网络”。
- CCE创建的ECS实例（节点）目前支持“按需计费”和“包年/包月”，其他资源（例如负载均衡）为按需计费。如果资源所属的服务支持将按需计费实例转换成包年/包月实例，您可以通过对应的控制台进行操作。
- 集群中纳管计费模式为“包年包月”的节点时，无法在CCE控制台为其续费，用户需前往ECS控制台单独续费。
- 由于ECS（节点）等CCE依赖的底层资源存在产品配额及库存限制，创建集群、扩容集群或者自动弹性扩容时，可能只有部分节点创建成功。
- ECS（节点）规格要求：CPU  $\geq$  2核且内存  $\geq$  4GB。
- 通过搭建VPN方式访问CCE集群，需要注意VPN网络和集群所在的VPC网段、容器使用网段不能冲突。

## 网络限制

- 节点访问(NodePort)的使用约束：默认为VPC内网访问，如果需要通过公网访问该服务，请提前在集群的节点上绑定弹性IP。
- CCE中的负载均衡（LoadBalancer）访问类型使用弹性负载均衡 ELB提供网络访问，存在如下产品约束：
  - 自动创建的ELB实例建议不要被其他资源使用，否则会在删除时被占用，导致资源残留。
  - v1.15及之前版本集群使用的ELB实例请不要修改监听器名称，否则可能导致无法正常访问。

- 网络策略(NetworkPolicy)，存在如下产品约束：
  - 当前仅**容器隧道网络模型**的集群支持网络策略（NetworkPolicy）。网络策略可分为以下规则：
    - 入规则（Ingress）：所有版本均支持。
    - 出规则（Egress）：v1.23及以上集群版本。
  - 不支持对IPv6地址网络隔离。
  - 通过原地升级到支持Egress的集群版本，由于不会升级节点操作系统，会导致无法使用Egress，此种情况下，请重置节点。

## 存储卷限制

- 云硬盘存储卷使用约束：
  - 云硬盘不支持跨可用区挂载，且不支持被多个工作负载、同一个工作负载的多个实例或多个任务使用。由于CCE集群各节点之间暂不支持共享盘的数据共享功能，多个节点挂载使用同一个云硬盘可能会出现读写冲突、数据缓存冲突等问题，所以创建无状态工作负载时，若使用了EVS云硬盘，建议工作负载只选择一个实例。
  - 1.19.10以下版本的集群中，如果使用HPA策略对挂载了EVS卷的负载进行扩容，当新Pod被调度到另一个节点时，会导致之前Pod不能正常读写。  
1.19.10及以上版本集群中，如果使用HPA策略对挂载了EVS卷的负载进行扩容，新Pod会因为无法挂载云硬盘导致无法成功启动。
- 文件存储卷使用约束：
  - 支持多个PV挂载同一个SFS或SFS Turbo，但有如下限制：
    - 多个不同的PVC/PV使用同一个底层SFS或SFS Turbo卷时，如果挂载至同一Pod使用，会因为PV的volumeHandle参数值相同导致无法为Pod挂载所有PVC，出现Pod无法启动的问题，请避免该使用场景。
    - PV中persistentVolumeReclaimPolicy参数建议设置为Retain，否则可能存在一个PV删除时级联删除底层卷，其他关联这个底层卷的PV会由于底层存储被删除导致使用出现异常。
    - 重复用底层存储时，建议在应用层做好多读多写的隔离保护，防止产生的数据覆盖和丢失。
  - 使用通用文件系统（SFS 3.0）存储卷时，集群中需要安装2.0.9及以上版本的CCE容器存储（Everest）插件。
  - 使用通用文件系统（SFS 3.0）存储卷时，挂载点不支持修改属组和权限，挂载点默认属主为root。
  - 使用通用文件系统（SFS 3.0）时，创建、删除PVC和PV过程中可能存在时延，实际计费时长请以SFS侧创建、删除时刻为准。
  - 通用文件系统（SFS 3.0）使用Delete回收策略时，需要挂载文件系统手动删除所有文件后才可以正常删除PV和PVC。
- 对象存储卷使用约束如下：
  - 使用对象存储时，挂载点不支持修改属组和权限。
  - 使用PVC挂载对象存储时，负载每挂载一个对象存储卷，后端会产生一个常驻进程。当负载使用对象存储数过多或大量读写对象存储文件时，常驻进程会占用大量内存，为保证负载稳定运行，建议负载使用的对象存储卷数量不

超过其申请的内存GiB数量，如负载的申请的内存规格为4GiB，则建议其使用的对象存储数**不超过4**。

- 安全容器不支持使用对象存储。
- 挂载普通桶时不支持硬链接（Hard Link）。
- 本地持久卷使用约束：
  - 本地持久卷仅在集群版本  $\geq$  v1.21.2-r0 时支持，且需要everest插件版本  $\geq$  2.1.23，推荐使用  $\geq$  2.1.23 版本。
  - 移除节点、删除节点、重置节点和扩容节点会导致与节点关联的本地持久存储卷类型的PVC/PV数据丢失，无法恢复，且PVC/PV无法再正常使用。移除节点、删除节点、重置节点和扩容节点时使用了本地持久存储卷的Pod会从删除、重置的节点上驱逐，并重新创建Pod，Pod会一直处于pending状态，因为Pod使用的PVC带有节点标签，由于冲突无法调度成功。节点重置完成后，Pod可能调度到重置好的节点上，此时Pod会一直处于creating状态，因为该PVC对应的底层逻辑卷已不存在。
  - 请勿在节点上手动删除对应的存储池或卸载数据盘，否则会导致数据丢失等异常情况。
  - 本地持久卷不支持被多个工作负载或多个任务同时挂载。
- 本地临时卷使用约束：
  - 本地临时卷仅在集群版本  $\geq$  v1.21.2-r0 时支持，且需要everest插件版本  $\geq$  1.2.29。
  - 请勿在节点上手动删除对应的存储池或卸载数据盘，否则会导致数据丢失等异常情况。
  - 请确保节点上Pod不要挂载/var/lib/kubelet/pods/目录，否则可能会导致使用了临时存储卷的Pod无法正常删除。
- 快照与备份使用约束：
  - 快照功能**仅支持v1.15及以上版本**的集群，且需要安装基于CSI的everest插件才可以使用。
  - 基于快照创建的云硬盘，其子类型（普通IO/高IO/超高IO）、是否加密、磁盘模式（VBD/SCSI）、共享性（非共享/共享）、容量等都要与快照关联磁盘保持一致，这些属性查询和设置出来后不能够修改。
  - 只有可用或正在使用状态的磁盘能创建快照，且单个磁盘最大支持创建7个快照。
  - 创建快照功能仅支持使用everest插件提供的存储类（StorageClass名称以csi开头）创建的PVC。使用Flexvolume存储类（StorageClass名为ssd、sas、sata）创建的PVC，无法创建快照。
  - 加密磁盘的快照数据以加密方式存放，非加密磁盘的快照数据以非加密方式存放。

## 插件限制

CCE插件采用Helm模板方式部署，修改或升级插件请从插件配置页面或开放的插件管理API进行操作。请勿直接后台修改插件相关资源，以免插件异常或引入其他非预期问题。

## CCE 集群配额限制

针对每个用户，云容器引擎的集群在每个地域分配了固定配额。

限制项	普通用户限制	例外
实名认证	实名认证	-
单Region下集群总数	50	请 <a href="#">提交工单</a> 申请扩大配额。
单集群最大节点数（集群管理规模）	可选择50节点、200节点、1000节点或2000节点多种管理规模。	如果已有规模无法满足您的需求，您可以 <a href="#">提交工单</a> 申请扩大集群管理规模，最大支持10000节点。
单节点最大实例数	256 <b>说明</b> CCE Turbo集群中，节点最大实例数由节点可使用的网卡数量决定。	如果您期望提升节点上的部署密度，您可以 <a href="#">提交工单</a> 申请调整节点最大实例数，最大支持修改至512个实例。
单个集群管理的最大Pod数	10万Pod	如果当前支持的Pod数量无法满足您的需求，您可以 <a href="#">提交工单</a> 申请技术支持，帮助您基于业务模型调优集群。

## 集群容量限制

集群规格容量由多种资源共同构成，例如容器组（Pod）、云存储实例（Persistent volume）、服务（Service）等，同时资源对象的大小也会影响集群规格容量。

例如：

- 当Pod对象资源过大时，在一定的规格性能范围内Pod数量上限将相应降低。
- 当Pod数量趋于上限时，集群内其他类型资源上限也将相应降低。

在实际使用环境中，由于集群中多种资源共存，单一的类型资源可能无法达到上限值。因此，您可以通过监控及时查看集群相关使用率，对集群进行适当的规划和管理，以确保所有资源的性能都能够得到最大化的利用。如果当前规格无法满足您的使用需求，可以通过扩容来保证集群的稳定性。

## 依赖底层云产品配额限制

限制大类	限制项	普通用户限制
计算	实例数	1000
	核心数	8000核
	RAM容量 (MB)	16384000
网络	一个用户创建虚拟私有云的数量	5
	一个用户创建子网的数量	100
	一个用户拥有的安全组数量	100
	一个用户拥有的安全组规则数量	5000



限制大类	限制项	普通用户限制
	一个路由表里拥有的路由数量	100
	一个虚拟私有云拥有路由数量	100
	一个区域下的对等连接数量	50
	一个用户拥有网络ACL数量	200
	一个用户创建二层连接网关的数量	5
负载均衡	弹性负载均衡	50
	弹性负载均衡监听器	100
	弹性负载均衡证书	120
	弹性负载均衡转发策略	500
	弹性负载均衡后端主机组	500
	弹性负载均衡后端服务器	500

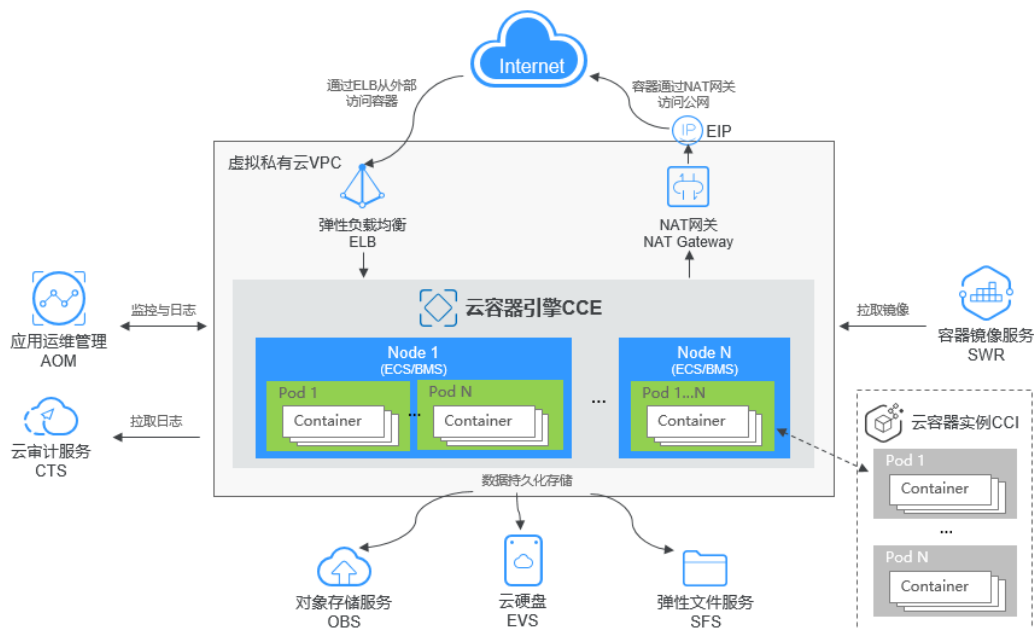
#### 说明

如果当前配额无法满足您的需求，您可以[提交工单](#)申请提升配额。

# 7 与其它云服务的关系

云容器引擎需要与其他云服务协同工作，云容器引擎需要获取如下云服务资源的权限。

图 7-1 云容器引擎与其他服务的关系示意图



## 云容器引擎与其他服务的关系

表 7-1 云容器引擎与其他服务的关系

服务名称	云容器引擎与其他服务的关系	主要交互功能
弹性云服务器 ECS	在云容器引擎中具有多个云硬盘的一台弹性云服务器就是一个节点，您可以在创建节点时指定弹性云服务器的规格。	<ul style="list-style-type: none"> <li>购买节点</li> <li>纳管已有节点到集群</li> </ul>

服务名称	云容器引擎与其他服务的关系	主要交互功能
虚拟私有云 VPC	在云容器引擎中创建的集群需要运行在虚拟私有云中，您在集群中创建节点池时，节点将会从VPC网段内分配私网IP地址，为您的集群提供相对隔离的网络环境。	<a href="#">购买CCE集群</a>
弹性负载均衡 ELB	云容器引擎支持将创建的应用对接到弹性负载均衡，弹性负载均衡可以将外部访问流量分发到不同的后端容器应用中。 您可以通过 <a href="#">弹性负载均衡</a> ，从外部网络访问容器负载。	<ul style="list-style-type: none"> <li>• <a href="#">创建无状态负载 (Deployment)</a></li> <li>• <a href="#">创建有状态负载 (StatefulSet)</a></li> <li>• <a href="#">负载均衡(LoadBalancer)</a></li> </ul>
NAT网关	NAT网关能够为VPC内的容器实例提供网络地址转换（Network Address Translation）服务，SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内的容器实例共享弹性公网IP访问Internet。 您可以通过 <a href="#">NAT网关</a> 设置SNAT规则，使得容器能够访问Internet。	<ul style="list-style-type: none"> <li>• <a href="#">创建无状态负载 (Deployment)</a></li> <li>• <a href="#">创建有状态负载 (StatefulSet)</a></li> <li>• <a href="#">DNAT网关(DNAT)</a></li> </ul>
容器镜像服务 SWR	容器镜像服务提供的镜像仓库是用于存储、管理docker容器镜像的场所，可以让使用人员轻松存储、管理、部署docker容器镜像。 您可以使用 <a href="#">容器镜像服务</a> 中的镜像创建负载。	<ul style="list-style-type: none"> <li>• <a href="#">创建无状态负载 (Deployment)</a></li> <li>• <a href="#">创建有状态负载 (StatefulSet)</a></li> </ul>
云容器实例 CCI	云容器实例的Serverless Container是从使用角度，无需创建、管理Kubernetes集群，也就是从使用的角度看不见服务器（Serverless），直接通过控制台、kubectl、Kubernetes API创建和使用容器负载，且只需为容器所使用的资源付费。 当CCE集群资源不足时，支持将Pod弹性部署到CCI集群。	<ul style="list-style-type: none"> <li>• <a href="#">virtual kubelet插件</a></li> <li>• <a href="#">CCE容器实例弹性伸缩到CCI服务</a></li> </ul>
云硬盘 EVS	可以将云硬盘挂载到云服务器，并可以随时扩容云硬盘容量。 在云容器引擎中一个节点就是具有多个云硬盘的一台弹性云服务器，您可以在创建节点时指定云硬盘的大小。	<a href="#">使用云硬盘存储卷</a>

服务名称	云容器引擎与其他服务的关系	主要交互功能
对象存储服务 OBS	<p>对象存储服务是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、删除对象等。</p> <p>云容器引擎支持创建OBS对象存储卷并挂载到容器的某一路径下。</p>	<a href="#">使用对象存储卷</a>
弹性文件服务 SFS	<p>弹性文件服务提供托管的共享文件存储，符合标准文件协议（NFS），能够弹性伸缩至PB规模，具备可扩展的性能，为海量数据、高带宽型应用提供有力支持。</p> <p>您可以使用弹性文件服务作为容器的持久化存储，在创建任务负载的时候挂载到容器上。</p>	<a href="#">使用文件存储卷</a>
应用运维管理 AOM	<p>云容器引擎对接了AOM，AOM会采集容器日志存储中的“.log”等格式日志文件，转储到AOM中，方便您查看和检索；并且云容器引擎基于AOM进行资源监控，为您提供弹性伸缩能力。</p>	<a href="#">容器日志</a>
云审计服务 CTS	<p>云审计服务提供云服务资源的操作记录，记录内容包括您从公有云管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。</p>	<a href="#">云审计服务支持的CCE操作列表</a>

# 8 区域与可用区

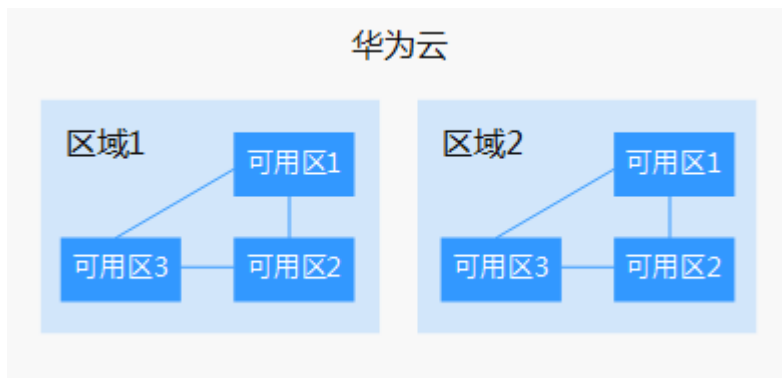
## 什么是区域、可用区？

区域和可用区用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8-1阐明了区域和可用区之间的关系：

图 8-1 区域和可用区



目前，全球多个地域均已开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见[华为云全球站点](#)。

## 如何选择区域？

选择区域时，您需要考虑以下因素：

- 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“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。有关区域和终端节点的更多信息，请参阅[地区和终端节点](#)。