云容器实例(CCI) 2.0

产品介绍

文档版本 01

发布日期 2025-11-21

华为云计算技术有限公司

商标声明


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。

目 录

1 什么是云容器实例

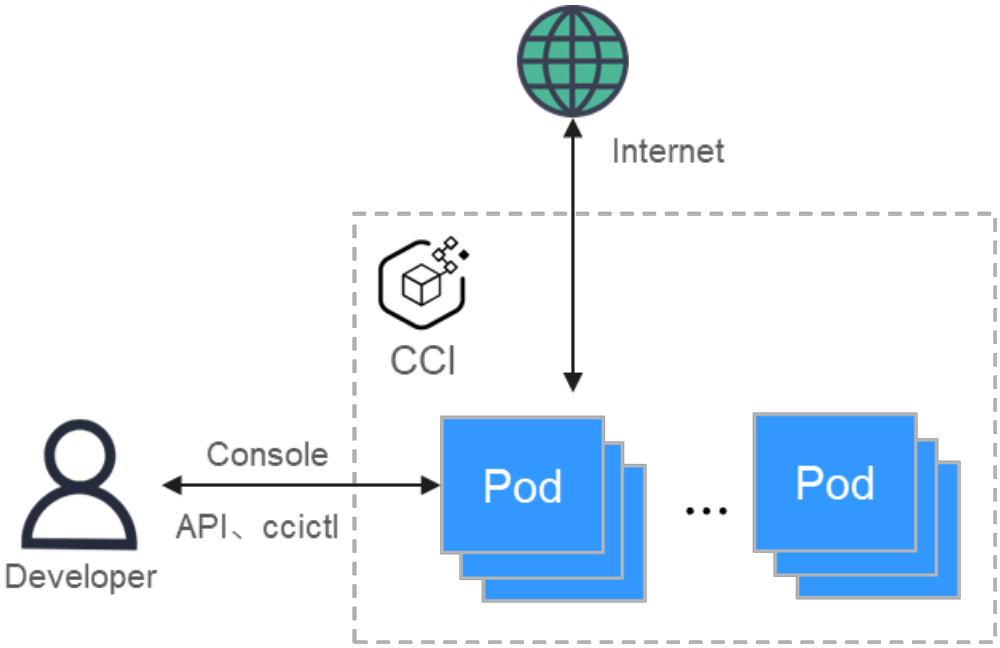
什么是云容器实例

云容器实例（Cloud Container Instance，CCI）服务提供Serverless Container（无服务器容器）引擎，让您无需创建和管理服务器集群即可直接运行容器。

Serverless是一种架构理念，是指不用创建和管理服务器、不用担心服务器的运行状态（服务器是否在工作等），只需动态申请应用需要的资源，把服务器留给专门的维护人员管理和维护，进而专注于应用开发，提升应用开发效率、节约企业IT成本。传统上使用运行容器，首先需要创建运行容器的服务器集群，然后再创建容器负载。

云容器实例的Serverless Container就是从使用角度，无需创建、管理集群，也就是从使用的角度看不见服务器，直接通过控制台、API、ccictl创建和使用容器负载，且只需为容器所使用的资源付费。

图 1-1 使用云容器实例



产品功能

一站式容器生命周期管理

使用云容器实例，您无需创建和管理服务器集群即可直接运行容器。您可以通过控制台、API、ccictl创建和使用容器负载，且只需为容器所使用的资源付费。

支持网络访问方式

云容器实例提供网络访问方式，支持四层负载均衡，满足客户的访问诉求。

支持持久化存储卷

云容器实例支持将数据存储在云服务的云存储上，当前支持的云存储：极速文件存储卷（SFS Turbo）。

支持极速弹性扩缩容

云容器实例支持用户自定义弹性伸缩策略，实现秒级弹性扩缩容，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。

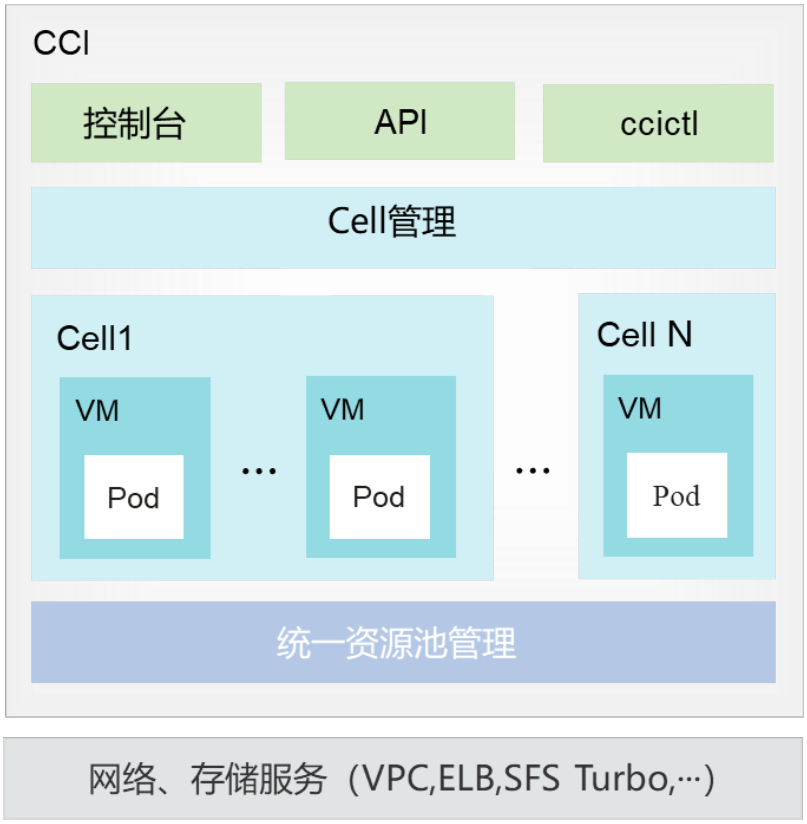
全方位容器状态监控

云容器实例支持监控容器运行的资源使用率，包括CPU、内存的使用率，方便您实时掌控容器运行的状态。

产品架构

云容器实例提供Serverless Container服务。CCI Serverless融合资源池集成了网络、存储等服务，让您方便地通过控制台、API创建和使用容器负载。

图 1-2 产品架构



- 基于云平台底层网络和存储服务，提供丰富的网络和存储功能。

- 基于擎天软硬协同架构提供高性能基础设施，带来极致的性能体验。
- 通过虚拟化技术实现安全隔离，结合自有硬件虚拟化加速技术和定制化容器操作系统，提供高性能容器实例。
- 资源统一管理，容器负载统一调度，使用上无需感知集群存在。
- 提供负载快速部署、弹性负载均衡、极速弹性伸缩等多种能力加速业务迭代。

云容器实例学习路径

您可以借助云容器实例**成长地图**，快速了解产品，由浅入深学习使用和运维CCI。

2 产品优势

随启随用

业界领先的Serverless Container架构。CCI Serverless融合资源池集成了网络、存储等服务，您无需创建服务器集群，通过控制台、API、ccictl即可创建和使用容器负载。

极速弹性

云容器实例支持高性能HPA引擎，能够提供秒级弹性伸缩能力，让您能够轻松应对业务快速变化，稳健保障业务SLA。

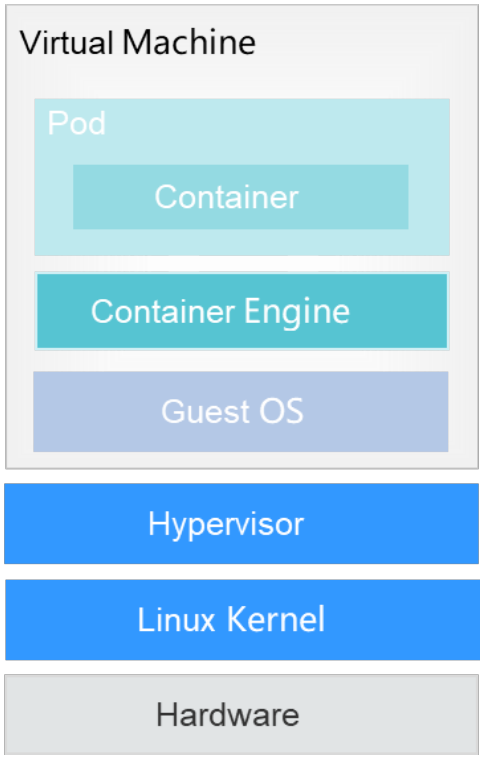
按需秒级计费

根据实际使用的资源数量，按需按秒计费，避免业务不活跃时段的费用开销，降低用户成本。

高安全

云容器实例同时具备容器级别的启动速度和虚拟机级别的安全隔离能力，提供更好地容器体验。

图 2-1 虚拟机级别的安全隔离



3 应用场景

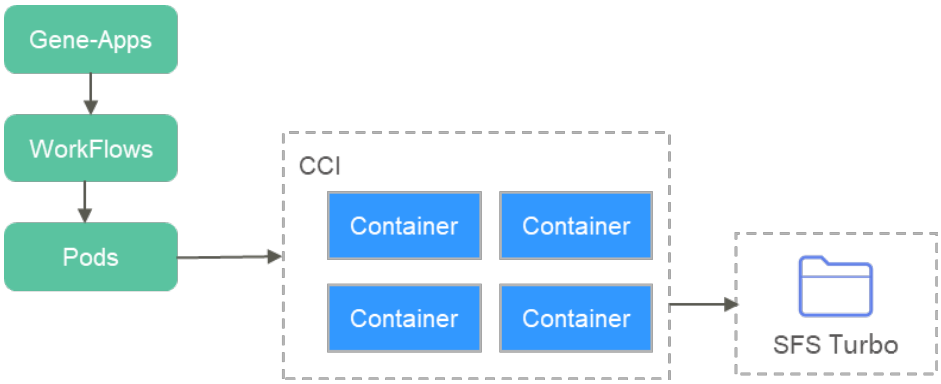
生物基因、药物研发等科学计算

生物基因、药品研发等领域需要高性能、密集型计算，同时对成本较敏感，需要低成本、免运维的计算平台。科学计算一般都是任务型计算，快速申请大量资源，完成后快速释放。

云容器实例提供如下特性，能够很好地支持这类场景。

- **高性能计算**：提供高性能计算、网络和高I/O存储，满足密集计算的诉求
- **极速弹性**：秒级资源准备与弹性，减少计算过程中的资源处理环节消耗
- **免运维**：无需感知集群和服务器，大幅简化运维工作、降低运维成本
- **随启随用、按需付费**：容器按需启动，按资源规格和使用时长付费

图 3-1 科学计算



DevOps 持续交付

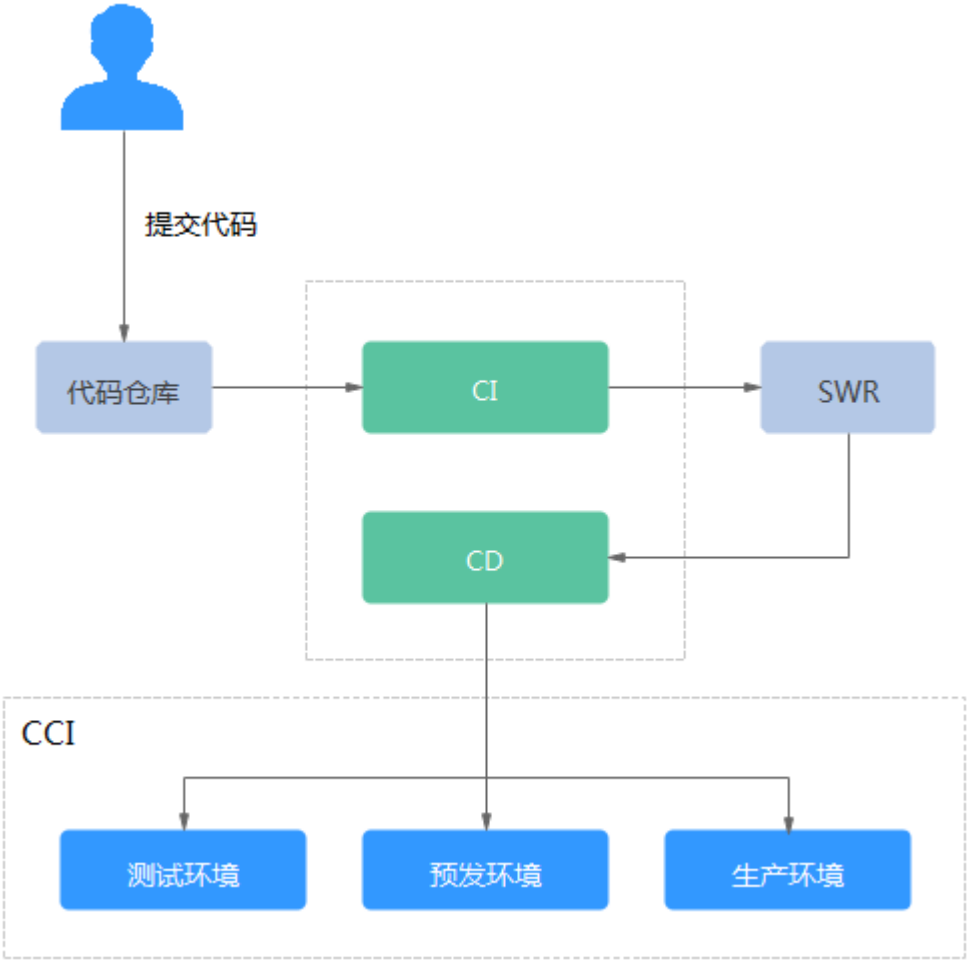
软件开发型企业，希望构建从代码提交到应用部署的DevOps完整流程，提高企业应用迭代效率。DevOps流程一般都是任务型计算，如企业CI/CD（持续集成/持续发布）流程自动化，需要快速申请资源，完成后快速释放。

云容器实例提供如下特性，能够很好地支持这类场景。

- **流程自动化**：无需创建和维护集群，实现从CI/CD的全流程自动化

- **环境一致性**：以容器镜像交付，可以无差别地从开发环境迁移到生产环境
- **随启随用、按需付费**：容器按需启动，按资源规格和使用时长付费

图 3-2 DevOps 持续交付



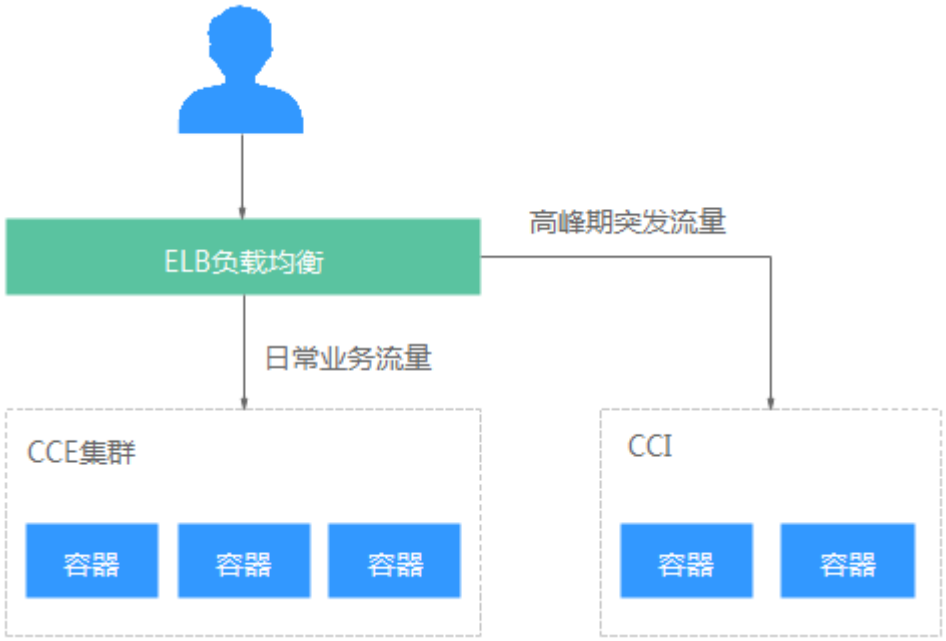
高弹性业务

业务波峰波谷较明显的业务，日常流量稳定，高峰期又需要快速扩展资源，并对成本有一定诉求，如视频直播、媒体资讯、电商、在线教育等应用。

云容器实例提供如下特性，能够很好地支持这类场景。

- **快速弹性伸缩**：业务高峰时，业务能够快速从CCE弹性扩展到CCI，保障业务稳定运行
- **低成本灵活计费**：业务平稳期在CCE上包周期计费，节省成本；高峰期弹性扩容到CCI上，按需计费，高峰期结束后又可以快速释放资源，降低成本

图 3-3 弹性扩展



4 安全

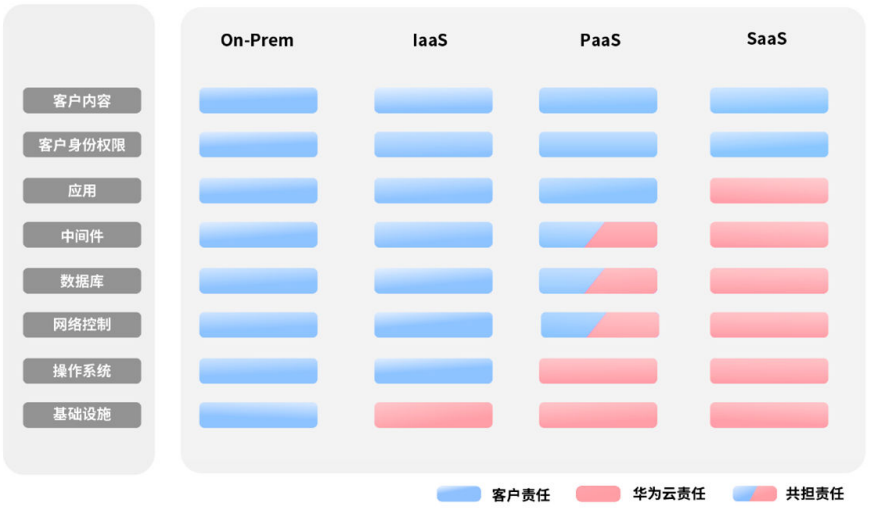
4.1 责任共担

华为云秉承“将公司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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图4-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况下，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 4-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图4-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好PaaS服务中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

传统本地部署(On-Prem)：由客户在自有数据中心内部署和管理软件及IT基础设施，而非依赖于远程的云服务提供商；

基础设施即服务(IaaS)：由云服务提供商提供计算、网络、存储等基础设施服务，如**弹性云服务器 ECS**、**虚拟专用网络 VPN**、**对象存储服务 OBS**；

平台即服务(PaaS)：由云服务提供商提供应用程序开发和部署所需要的平台，客户无需维护底层基础设施，如**AI开发平台 ModelArts**、**云数据库 GaussDB**；

软件即服务 (SaaS)：由云服务提供商提供完整应用软件，客户直接应用软件而无需安装、维护应用软件及底层平台和基础设施，如**华为云会议 Meeting**。

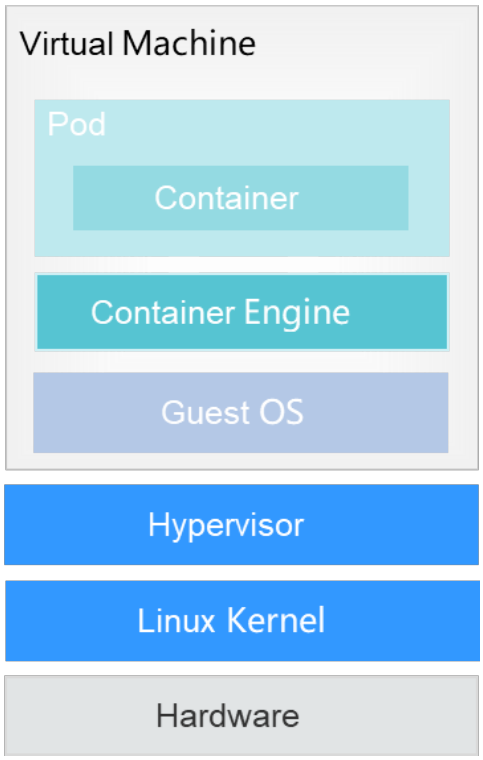
4.2 数据保护技术

云容器实例通过多种数据保护手段和特性，保障数据的安全可靠。

虚拟机隔离

云容器实例同时具备容器级别的启动速度和虚拟机级别的安全隔离能力，提供更好地容器体验。

图 4-2 虚拟机级别的安全隔离



Secret

Secret是一种加密存储的资源对象，用户可以将认证信息、证书、私钥等保存在密钥中，在容器启动时以环境变量等方式加载到容器中。

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并创建和配置追踪器后，CTS可记录您从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。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

日志

CCI为用户提供可选的日志管理功能，用户可配置容器的日志路径和日志上报地址，CCI会从日志路径采集日志，并上报到LTS，详细介绍和配置方法，请参见**日志管理**。

整体上CCI的安全日志能力已对接LTS服务，其后续相关安全性、完整性等能力由相关承载服务跟踪。

4.4 监控安全风险

通过 AOM 查看 Pod 监控数据

为使用户更好的掌握工作负载的运行状态，CCI配合AOM提供可选的Pod监控能力。

通过AOM界面您可监控CCI的基础资源和运行在CCI上的应用。

更多内容，请参见**监控管理**。

Pod 资源监控指标

CCI支持Pod资源基础监控能力，提供CPU、内存、磁盘、网络等多种监控指标，满足对Pod资源的基本监控需求。

- CCI支持的资源监控指标，请参见**资源监控指标**。
- Pod资源基础监控能力，请参见**Pod资源监控指标**。

5 权限管理

如果您需要对华为云购买的CCI资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云资源的访问。

通过IAM，您可以在您的云账号中给员工创建IAM用户，并授权控制用户对云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望用户拥有CCI的使用权限，但是不希望用户拥有删除CCI等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CCI，但是不允许删除CCI的权限，控制用户对CCI资源的使用范围。

如果您的云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CCI服务的其它功能。

IAM是云平台提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品介绍**。

CCI 权限

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。

CCI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（如华北-北京四）对应的项目（cn-north-4）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CCI时，需要先切换至授权区域。

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。由于云平台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CCI服务，管理员能够控制IAM用户仅

能对某一类云容器实例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。

如表5-1所示，包括了CCI的所有系统策略。角色与策略授权场景的系统策略和身份策略授权场景的并不互通。

表 5-1 CCI 系统策略

策略名称	描述	策略类别
CCI FullAccess	云容器实例所有权限，拥有该权限的用户可以执行云容器实例所有资源的创建、删除、查询、更新操作。	系统策略
CCI ReadOnlyAccess	云容器实例只读权限，拥有该权限的用户仅能查看云容器实例资源。	系统策略
CCI CommonOperations	云容器实例普通用户，拥有该权限的用户可以执行除network和namespace子资源创建、删除、修改之外的所有操作。	系统策略
CCI Administrator	云容器实例管理员权限，拥有该权限的用户可以执行云容器实例所有资源的创建、删除、查询、更新操作。	系统角色

CCI FullAccess策略权限如下：

表 5-2 CCI FullAccess 策略主要权限

操作（Action）	说明
cci:*:*	CCI（云容器实例）服务的所有权限
vpc:*:*	VPC（虚拟私有云）服务的所有权限
elb:*:*	ELB（弹性负载均衡）服务的所有权限
sfs:*:*	SFS（弹性文件服务）服务的所有权限
obs:*:*	OBS（对象存储服务）服务的所有权限
evs:*:*	EVS（云硬盘）服务的所有权限
aom:*:*	AOM（应用运维管理）服务的所有权限
apm:*:*	APM（应用性能管理）服务的所有权限
swr:*:*	SWR（容器镜像服务）服务的所有权限
nat:*:*	NAT（NAT网关）服务的所有权限
kms:cmk:*	DEW（数据加密服务）服务的所有权限

CCI ReadOnlyAccess策略权限如下：

表 5-3 CCI ReadOnlyAccess 策略主要权限

操作（Action）	说明
cci:*:get	CCI（云容器实例）所有资源详情的查看权限
cci:*:list	CCI（云容器实例）所有资源列表的查看权限
vpc:*:get	VPC（虚拟私有云）所有资源详情的查看权限
vpc:*:list	VPC（虚拟私有云）所有资源列表的查看权限
ecs:*:get	ECS（弹性云服务器）所有资源详情的查看权限
ecs:*:list	ECS（弹性云服务器）所有资源列表的查看权限
elb:*:get	ELB（弹性负载均衡）所有资源详情的查看权限
elb:*:list	ELB（弹性负载均衡）所有资源列表的查看权限
sfs:*:get*	SFS（弹性文件系统）所有资源详情的查看权限
sfs:*:list	SFS（弹性文件系统）所有资源列表的查看权限
obs:*:get*	OBS（对象存储服务）服务所有资源详情的查看权限
obs:*:list	OBS（对象存储服务）服务所有资源列表的查看权限
evs:*:get*	EVS（云硬盘）服务所有资源详情的查看权限
evs:*:list	EVS（云硬盘）服务所有资源列表的查看权限
aom:*:get	AOM（应用运维管理）服务所有资源详情的查看权限
aom:*:list	AOM（应用运维管理）服务所有资源列表的查看权限
amp:*:get	APM（应用性能管理）服务所有资源详情的查看权限
apm:*:list	APM（应用性能管理）服务所有资源列表的查看权限
swr:*:get	SWR（容器镜像服务）服务所有资源详情的查看权限
swr:*:list	SWR（容器镜像服务）服务所有资源列表的查看权限
nat:*:get	NAT（NAT网关）服务所有资源详情的查看权限
nat:*:list	NAT（NAT网关）服务所有资源列表的查看权限
kms:cmk:get	查询密钥信息
kms:cmk:list	查询密钥列表

CCI CommonOperations策略权限如下：

表 5-4 CCI CommonOperations 策略主要权限

操作（Action）	说明
cci:namespace:get	查询所有namespaces
cci:namespace:list	列出所有namespaces
cci:network:get	查询network详情
cci:network:list	查询network列表
cci:namespaceSubResource:*	namespace子资源的所有权限
cci:addonTemplate:*	插件模板的所有权限
cci:addonInstance:*	插件实例的所有权限
vpc:*:*	VPC（虚拟私有云）服务的所有权限
elb:*:*	ELB（弹性负载均衡）服务的所有权限
sfs:*:*	SFS（弹性文件服务）服务的所有权限
obs:*:*	OBS（对象存储服务）服务的所有权限
evs:*:*	EVS（云硬盘）服务的所有权限
aom:*:*	AOM（应用运维管理）服务的所有权限
apm:*:*	APM（应用性能管理）服务的所有权限
swr:*:*	SWR（容器镜像服务）服务的所有权限
nat:*:*	NAT（NAT网关）服务的所有权限
kms:cmk:*	DEW（数据加密服务）服务的所有权限

表5-5列出了CCI常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 5-5 常用操作与系统权限的关系

操作	CCIFullAccess	CCIReadOnlyAccess	CCI CommonOperations
创建命名空间	√	x	x
删除命名空间	√	x	x
查询命名空间列表	√	√	√
查询命名空间详情	√	√	√
创建network	√	x	x

操作	CCIFullAccess	CCIReadOnlyAccess	CCI CommonOperations
删除network	√	x	x
查询network列表	√	√	√
查询network详情	√	√	√
更新network	√	x	x
创建Pod	√	x	√
删除Pod	√	x	√
查询Pod列表	√	√	√
查询Pod详情	√	√	√
更新Pod	√	x	√
进入Pod执行命令	√	x	√
查询Pod输出	√	√	√
创建ConfigMap	√	x	√
删除ConfigMap	√	x	√
查询ConfigMap列表	√	√	√
查询ConfigMap详情	√	√	√
更新ConfigMap	√	x	√
创建Secret	√	x	√
删除Secret	√	x	√
查询Secret列表	√	√	√
查询Secret详情	√	√	√
更新Secret	√	x	√
创建Service	√	x	√
删除Service	√	x	√
查询Service列表	√	√	√
查询Service详情	√	√	√
更新Service	√	x	√
创建Deployment	√	x	√
删除Deployment	√	x	√
查询Deployment列表	√	√	√

操作	CCIFullAccess	CCIReadOnlyAccess	CCI CommonOperations
查询Deployment详情	√	√	√
更新Deployment	√	x	√
创建HorizontalPodAutoscaler	√	x	√
删除HorizontalPodAutoscaler	√	x	√
查询HorizontalPodAutoscaler列表	√	√	√
查询HorizontalPodAutoscaler详情	√	√	√
更新HorizontalPodAutoscaler	√	x	√
创建PersistentVolume	√	x	√
删除PersistentVolume	√	x	√
查询PersistentVolume列表	√	√	√
查询PersistentVolume详情	√	√	√
更新PersistentVolume	√	x	√
创建PersistentVolumeClaim	√	x	√
删除PersistentVolumeClaim	√	x	√
查询PersistentVolumeClaim列表	√	√	√

操作	CCIFullAccess	CCIReadOnlyAccess	CCI CommonOperations
查询PersistentVolumeClaim详情	√	√	√
更新PersistentVolumeClaim	√	x	√
查询StorageClass列表	√	√	√
创建ImageSnapshot	√	x	√
删除ImageSnapshot	√	x	√
查询ImageSnapshot列表	√	√	√
查询ImageSnapshot详情	√	√	√

CCI服务支持身份策略授权。如表5-6所示，包括了CCI基于策略授权中的所有系统策略。身份策略授权场景的系统身份策略和角色与策略授权场景的并不互通。

表 5-6 CCI 系统身份策略

系统身份策略名称	描述	策略类别
CCIFullAccessPolicy	云容器实例服务所有权限	系统身份策略
CCIReadOnlyPolicy	云容器实例服务只读访问权限	系统身份策略

CCIFullAccessPolicy身份策略权限如下：

表 5-7 CCIFullAccessPolicy 策略主要权限

操作（Action）	说明
cci:*:*	CCI（云容器实例）服务的所有权限
vpc:subnets:create	VPC（虚拟私有云）服务的创建子网权限
vpc:subnets:get	VPC（虚拟私有云）服务的查询子网详情权限
vpc:subnets:update	VPC（虚拟私有云）服务的更新子网权限
vpc:subnets:delete	VPC（虚拟私有云）服务的删除子网权限

操作（Action）	说明
vpc:vpcs:create	VPC（虚拟私有云）服务的创建虚拟私有云权限
vpc:vpcs:get	VPC（虚拟私有云）服务的查询虚拟私有云详情权限
vpc:vpcs:list	VPC（虚拟私有云）服务的查询虚拟私有云列表权限
vpc:vpcs:update	VPC（虚拟私有云）服务的更新虚拟私有云权限
vpc:vpcs:delete	VPC（虚拟私有云）服务的删除虚拟私有云权限
vpc:ports:get	VPC（虚拟私有云）服务的查询端口详情权限
vpc:ports:list	VPC（虚拟私有云）服务的查询端口列表权限
vpc:quotas:list	VPC（虚拟私有云）服务的查询资源配额权限
vpc:securityGroups:get	VPC（虚拟私有云）服务的查询安全组详情权限
vpc:securityGroupRules:get	VPC（虚拟私有云）服务的查询安全组规则详情权限
swr:namespace:list*	SWR（容器镜像服务）服务的共享版仓库查询组织列表权限
swr:namespace:get*	SWR（容器镜像服务）服务的共享版仓库获取组织权限和组织详情权限
swr:repo:list*	SWR（容器镜像服务）服务的共享版仓库所有镜像资源的列表权限
swr:repo:get*	SWR（容器镜像服务）服务的共享版仓库所有镜像资源的详情权限
swr:repo:download	SWR（容器镜像服务）服务的共享版仓库下载镜像权限
swr::listQuotas	SWR（容器镜像服务）服务的共享版仓库获取配额信息权限
swr::getDomainOverview	SWR（容器镜像服务）服务的共享版仓库获取租户总览信息权限
swr::getDomainResourceReports	SWR（容器镜像服务）服务的共享版仓库获取租户资源统计信息权限
swr:instance:get*	SWR（容器镜像服务）服务的查询所有实例相关资源的详情权限
swr:instance:list*	SWR（容器镜像服务）服务的查询所有实例相关资源的列表权限

表 5-8 CCIReadOnlyPolicy 策略主要权限

操作（Action）	说明
cci:*:get*	CCI（云容器实例）服务的查询所有资源详情权限

操作（Action）	说明
cci:*:list*	CCI（云容器实例）服务的查询所有资源列表权限
vpc:subnets:get	VPC（虚拟私有云）服务的查询子网详情权限
vpc:vpcs:get	VPC（虚拟私有云）服务的查询虚拟私有云详情权限
vpc:vpcs:list	VPC（虚拟私有云）服务的查询虚拟私有云列表权限
vpc:ports:get	VPC（虚拟私有云）服务的查询端口详情权限
vpc:ports:list	VPC（虚拟私有云）服务的查询端口列表权限
vpc:quotas:list	VPC（虚拟私有云）服务的查询资源配额权限
vpc:securityGroups:get	VPC（虚拟私有云）服务的查询安全组详情权限
vpc:securityGroupRules:get	VPC（虚拟私有云）服务的查询安全组规则详情权限
swr:namespace:list*	SWR（容器镜像服务）服务的共享版仓库查询组织列表权限
swr:namespace:get*	SWR（容器镜像服务）服务的共享版仓库获取组织权限和组织详情权限
swr:repo:list*	SWR（容器镜像服务）服务的共享版仓库所有镜像资源的列表权限
swr:repo:get*	SWR（容器镜像服务）服务的共享版仓库所有镜像资源的详情权限
swr:repo:download	SWR（容器镜像服务）服务的共享版仓库下载镜像权限
swr::listQuotas	SWR（容器镜像服务）服务的共享版仓库获取配额信息权限
swr::getDomainOverview	SWR（容器镜像服务）服务的共享版仓库获取租户总览信息权限
swr::getDomainResourceReports	SWR（容器镜像服务）服务的共享版仓库获取租户资源统计信息权限
swr:instance:get*	SWR（容器镜像服务）服务的查询所有实例相关资源的详情权限
swr:instance:list*	SWR（容器镜像服务）服务的查询所有实例相关资源的列表权限

表5-9列出了CCI常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

表 5-9 常用操作与系统身份策略的关系

操作	CCIFullAccessPolicy	CCIReadOnlyPolicy
创建命名空间	√	x
删除命名空间	√	x
查询命名空间列表	√	√
查询命名空间详情	√	√
创建network	√	x
删除network	√	x
查询network列表	√	√
查询network详情	√	√
更新network	√	x
创建Pod	√	x
删除Pod	√	x
查询Pod列表	√	√
查询Pod详情	√	√
更新Pod	√	x
进入Pod执行命令	√	x
查询Pod输出	√	x
创建ConfigMap	√	x
删除ConfigMap	√	x
查询ConfigMap列表	√	√
查询ConfigMap详情	√	√
更新ConfigMap	√	x
创建Secret	√	x
删除Secret	√	x
查询Secret列表	√	√
查询Secret详情	√	√
更新Secret	√	x
创建Service	√	√
删除Service	√	√
查询Service列表	√	√

操作	CCIFullAccessPolicy	CCIReadOnlyPolicy
查询Service详情	√	√
更新Service	√	x
创建Deployment	√	x
删除Deployment	√	x
查询Deployment列表	√	√
查询Deployment详情	√	√
更新Deployment	√	x
创建HorizontalPodAutoscaler	√	x
删除HorizontalPodAutoscaler	√	x
查询HorizontalPodAutoscaler列表	√	√
查询HorizontalPodAutoscaler详情	√	√
更新HorizontalPodAutoscaler	√	x
创建PersistentVolume	√	x
删除PersistentVolume	√	x
查询PersistentVolume列表	√	√
查询PersistentVolume详情	√	√
更新PersistentVolume	√	x
创建PersistentVolumeClaim	√	x
删除PersistentVolumeClaim	√	x
查询PersistentVolumeClaim列表	√	√
查询PersistentVolumeClaim详情	√	√
更新PersistentVolumeClaim	√	x
查询StorageClass列表	√	√
创建ImageSnapshot	√	x
删除ImageSnapshot	√	x
查询ImageSnapshot列表	√	√
查询ImageSnapshot详情	√	√

CCI细粒度鉴权系统策略关联Actions如下：

表 5-10 CCI 细粒度鉴权系统策略关联 Actions

操作（Action）	说明
cci:namespace:create	创建namespace
cci:namespace:delete	删除Namespace
cci:namespace:list	查询Namespace列表
cci:namespace:get	查询Namespace详情
cci:network:create	创建Network
cci:network:delete	删除Network
cci:network:list	查询Network列表
cci:network:get	查询Network详情
cci:network:update	更新Network
cci:pod:create	创建Pod
cci:pod:delete	删除Pod
cci:pod:list	查询Pod列表
cci:pod:get	查询Pod详情
cci:pod:update	更新Pod
cci:pod:exec	进入Pod执行命令
cci:pod:getLog	查询Pod输出
cci:configmap:create	创建ConfigMap
cci:configmap:delete	删除ConfigMap
cci:configmap:list	查询ConfigMap列表
cci:configmap:get	查询ConfigMap详情
cci:configmap:update	更新ConfigMap
cci:secret:create	创建Secret
cci:secret:delete	删除Secret
cci:secret:list	查询Secret列表
cci:secret:get	查询Secret详情
cci:secret:update	更新Secret
cci:service:create	创建Service
cci:service:delete	删除Service

操作（Action）	说明
cci:service:list	查询Service列表
cci:service:get	查询Service详情
cci:service:update	更新Service
cci:deployment:create	创建Deployment
cci:deployment:delete	删除Deployment
cci:deployment:list	查询Deployment列表
cci:deployment:get	查询Deployment详情
cci:deployment:update	更新Deployment
cci:horizontalpodautoscaler:create	创建HorizontalPodAutoscaler
cci:horizontalpodautoscaler:delete	删除HorizontalPodAutoscaler
cci:horizontalpodautoscaler:list	查询HorizontalPodAutoscalert列表
cci:horizontalpodautoscaler:get	查询HorizontalPodAutoscaler详情
cci:horizontalpodautoscaler:update	更新HorizontalPodAutoscaler
cci:persistentvolume:create	创建PersistentVolume
cci:persistentvolume:delete	删除PersistentVolume
cci:persistentvolume:list	查询PersistentVolume列表
cci:persistentvolume:get	查询PersistentVolume详情
cci:persistentvolume:update	更新PersistentVolume
cci:persistentvolumeclaim:create	创建PersistentVolumeClaim
cci:persistentvolumeclaim:delete	删除PersistentVolumeClaim
cci:persistentvolumeclaim:list	查询PersistentVolumeClaim列表
cci:persistentvolumeclaim:get	查询PersistentVolumeClaim详情
cci:persistentvolumeclaim:update	更新PersistentVolumeClaim
cci:storageclass:list	查询StorageClass列表
cci:imagesnapshot:create	创建ImageSnapshot
cci:imagesnapshot:delete	删除ImageSnapshot

操作（Action）	说明
cci:imagesnapshot:list	查询ImageSnapshot列表
cci:imagesnapshot:get	查询ImageSnapshot详情

6 约束与限制

本章介绍CCI相关的使用限制，以便于您更好地使用CCI。

CCI 2.0 镜像拉取使用限制

CCI 2.0场景下，用户通过SWR拉取镜像，需要借助VPCEP。当前CCI 2.0暂不支持帮用户自动创建VPCEP，因此用户使用CCI 2.0前，需手动创建关联的VPCEP，否则创建容器组和无状态负载时会报拉取镜像失败错误。

通过SWR仓库拉取镜像涉及创建的VPCEP如下:

- SWR企业仓库镜像拉取，需要购买OBS VPCEP。
- SWR公共镜像仓库镜像拉取，需要购买SWR VPCEP和OBS VPCEP。
  详细指导参考**购买云服务VPCEP**章节。

CCI 2.0 实例限制

下表为CCI 2.0实例相关的使用限制。

表 6-1 CCI 支持 Pod 规格表

容器实例 核/vCPU	容器实例 内存/GiB
0.25	0.5，1，2
0.5	0.5，1，2，3，4
1	1~8，1GiB为步长
2	2~16，1GiB为步长
4	4~32，1GiB为步长
8	8~64，4GiB为步长
16	16~128，8GiB为步长
32	32，64，128，256
48	96，192，384

容器实例 核/vCPU	容器实例 内存/GiB
64	128，256，512

说明

在CCI 2.0运行的pod，辅助pod容器运行的系统组件会占用少量底层资源，因此在某些场景下，pod会出现实际内存使用无法达到pod规格内存的情况。如果您需要使用完整规格的资源，CCI 2.0提供了预留系统开销的功能，详情请参考**增加预留系统开销**章节。

Pod 存储空间限制

如果没有挂载EVS等磁盘，应用数据存储在容器的rootfs，每个Pod默认存储空间限制如下所示：

表 6-2 每个 Pod 存储空间限制

Pod类型	存储空间限制
通用型Pod	30G

说明

因系统本身及平台预留资源占用，实际使用时，用户磁盘使用量无法达到默认存储空间限制量，且用户选择的Pod规格越大，系统占用资源越高。默认场景下，若您需要的Pod临时存储空间超过20G，CCI 2.0提供了扩容Pod存储空间的功能，建议您对Pod存储空间进行按需扩容，详情请参考**如何扩展临时存储空间**章节。

约束与限制

- CCI 2.0服务当前仅支持创建LoadBalancer类型的Service，支持配置独享型ELB，不支持配置共享型ELB。使用LoadBalancer类型的Service，CCI 2.0当前仅支持配置后端IP地址为IPV4类型，不支持IPV6类型。
- 如果使用CCE集群中的Bursting插件对接CCI 2.0服务，支持配置独享型ELB的Ingress和Service。CCE突发弹性引擎（对接 CCI）插件1.5.5以下版本不支持配置ELB类型的Service。

7 与 CCI 1.0 对比

CCI 2.0和CCI 1.0均围绕Kubernetes生态，提供Serverless 容器的服务。CCI 2.0在CCI 1.0的能力基础上，扩大了资源供给规模，丰富了算力种类，提升了容器弹性速度。此外，CCI 2.0在CCI 1.0的基础上进一步精简API，提供Kubernetes Like APIs。

CCI1.0 vs CCI2.0 API差异如下：

表 7-1 CCI1.0 vs CCI2.0 API 差异

K8s Like API资源对象	CCI1.0	CCI2.0
Namespace	√	√
Pod	√	√
Service	√	√
ConfigMap	√	√
Secret	√	√
Event	√	x
PersistentVolume	x	√
PersistentVolumeClaim	√	√
ReplicaSet	√	√
Deployment	√	√
Job	√	x
StorageClass	√	√
HorizontalPodAutoscaler	x	√
StatefulSet	x	x
CronJob	√	x
Ingress	√	x

K8s Like API资源对象	CCI1.0	CCI2.0
ClusterRole	√	x
RoleBinding	√	x
ResourceQuota	√	x
Endpoint	√	x

8 基本概念

云容器实例围绕Kubernetes生态，提供了Kubernetes Like APIs，支持通过控制台、API创建关联资源。为了更好的理解云容器实例，建议您在使用云容器实例前，先了解相关的基本概念。

镜像（Image）

容器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（Container）

镜像和容器的关系，就像是面向对象程序设计中的类和实例一样，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。

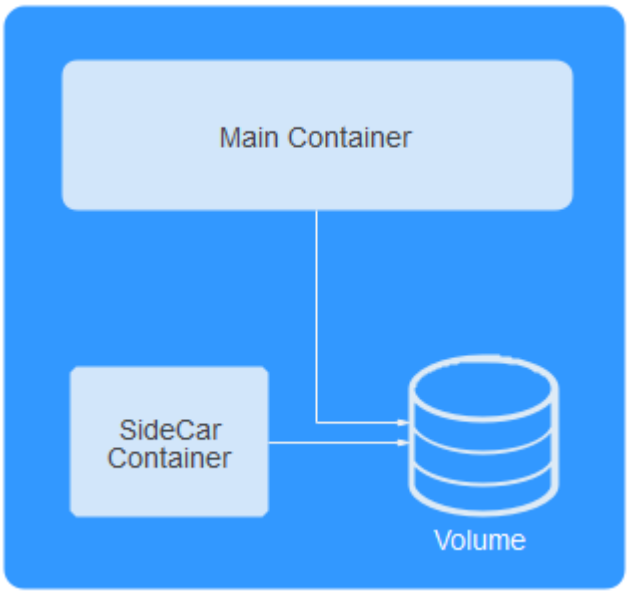
命名空间（Namespace）

命名空间是一种在多个用户之间划分资源的方法。当你的项目和人员众多的时候可以考虑根据项目属性，例如生产、测试、开发划分不同的namespace。

容器组（Pod）

容器组是创建或部署的最小单位。一个容器组封装一个或多个容器、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。

图 8-1 Pod



容器组使用主要分为两种方式：

- 容器组中运行一个容器。这是最常见的用法，你可以将容器组视为单个封装的容器，是直接管理容器组而不是容器。
- 容器组中运行多个需要耦合在一起工作、需要共享资源的容器。

实际使用中很少直接创建容器组，而是通过基础负载创建和管理Pod，例如Deployment。基础负载可以创建和管理多个Pod，提供副本管理、滚动升级和自愈能力。通常，基础负载会使用Pod Template来创建相应的Pod。

Init 容器（Init-Containers）

Init-Containers，即初始化容器，顾名思义容器启动的时候，会先启动一个或多个容器，如果有多个，那么这几个Init Container按照定义的顺序依次执行，只有所有的Init Container执行完后，主容器才会启动。由于一个Pod里的存储卷是共享的，所以Init Container里产生的数据可以被主容器使用到。

Init Container可以在多种K8S资源里被使用到如Deployment、Job等，但归根结底都是在Pod启动时，在主容器启动前执行，做初始化工作。

详细信息请参见**Init容器**。

标签

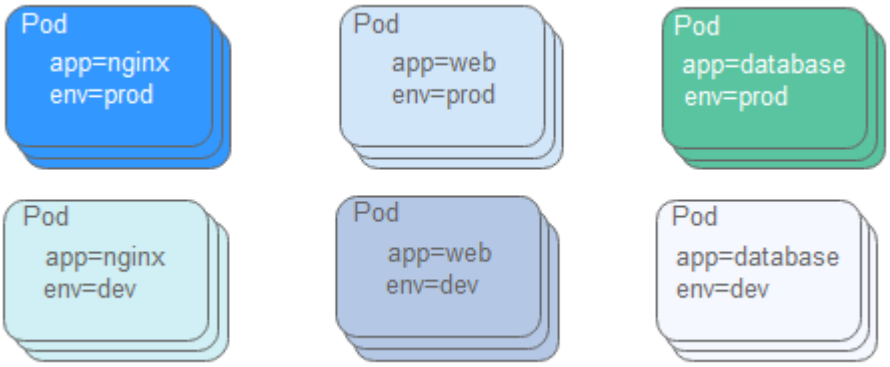
Label（标签）是一组附加在对象上的键值对，用来传递用户定义的属性。

标签常用来从一组对象中选取符合条件的对象，这也是Kubernetes中目前为止最重要的节点分组方法。

比如，你可能创建了一个“tier”和“app”标签，通过Label（tier=frontend，app=myapp）来标记前端Pod容器，使用Label（tier=backend，app=myapp）标记后台Pod。然后可以使用Selectors选择带有特定Label的Pod，并且将Service或者Deployment应用到上面。

详细信息请参见**Label**。

图 8-2 使用 Label 组织的 Pod



无状态负载（Deployment）

Deployment是基础负载的一种。

一个Deployment可以包含一个或多个Pod，每个Pod的角色相同，所以系统会自动为Deployment的多个Pod分发请求。Deployment中的所有Pod共享存储卷。

使用Deployment时，您只需要在Deployment中描述您想要的目标状态是什么，Deployment就会帮您将Pod的状态改变到目标状态。

详细信息请参见**Deployment**。

服务（Service）

Pod是有生命周期的，它们可以被创建，也可以被销毁，然而一旦被销毁生命就永远结束。通过Pod Controller能够动态地创建和销毁Pod（例如，需要进行扩缩容，或者执行滚动升级）。每个Pod都会获取它自己的IP地址，但这些IP地址不总是稳定可依赖的。 这会导致一个问题：如果一组Pod（称为backend）为其它Pod（称为frontend）提供服务，那么那些frontend该如何发现，并连接到这组Pod中的哪些backend呢?

Service是将运行在一个或一组Pod上的网络应用程序公开为网络服务的方法。每个Service对象定义端点的一个逻辑集合（通常这些端点就是Pod）以及如何访问这些Pod的策略。

举个例子，考虑一个图片处理backend，它运行了3个Pod副本。这些副本是可互换的（frontend不需要关心它们调用了哪个backend副本）。 然而组成这一组backend的Pod实际上可能会发生变化，frontend不应该也没必要知道，而且也不需要跟踪这一组backend的状态。Service定义的抽象就是用来解耦这种关联。

详细信息请参见**Service**。

ConfigMap

ConfigMap用于保存配置数据的键值对，可以用来保存单个属性，也可以用来保存配置文件。ConfigMap跟Secret很类似，但它可以更方便地处理不包含敏感信息的字符串。

详细信息请参见**ConfigMap**。

Secret

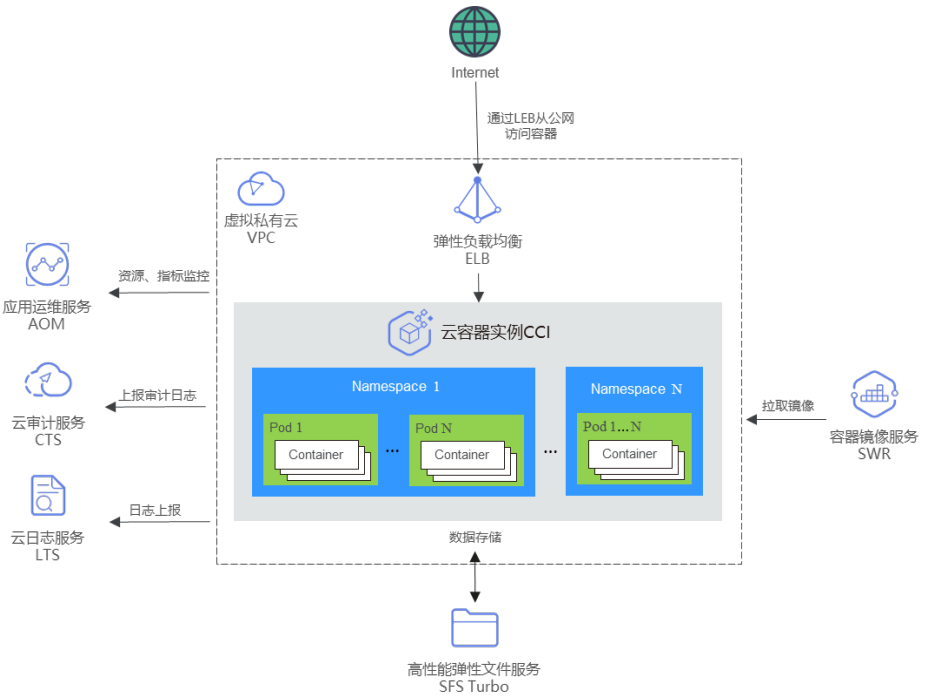
Secret是一种加密存储的资源对象，用户可以将认证信息、证书、私钥等保存在密钥中，在容器启动时以环境变量等方式加载到容器中。

详细信息请参见**Secret**。

9 与其他服务的关系

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

图 9-1 云容器实例与其他服务的关系



- **容器镜像服务**

  容器镜像服务（Software Repository for Container，SWR）是一种支持容器镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务。

  您可以使用容器镜像服务中的镜像创建负载。

- **虚拟私有云**

  虚拟私有云（Virtual Private Cloud，VPC）是用户在云平台上申请的隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性IP搭建业务系统。

您创建命名空间时，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。

- **弹性负载均衡**

  弹性负载均衡（ Elastic Load Balance，ELB ）将访问流量自动分发到多台云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错。

  您可以通过弹性负载均衡，从外部网络访问容器负载。

- **应用运维管理**

  应用运维管理（ Application Operations Management，AOM ）为运维人员提供一站式立体运维平台，实时监控应用、资源运行状态，通过数十种指标、告警与日志关联分析，快速锁定问题根源，保障业务顺畅运行。

  云容器实例基于AOM采集容器基础监控指标，方便您进行资源监控。

- **高性能弹性文件服务**

  高性能弹性文件服务（ Scalable File Service Turbo，SFS Turbo ）提供按需扩展的高性能文件存储（ NAS ），能够弹性伸缩至320TB规模，具备高可用性和持久性，为海量的小文件、低延迟高IOPS型应用提供有力支持。

  您可以使用高性能弹性文件服务作为容器的日志存储，在创建任务负载的时候挂载到容器上。

- **云日志服务**

  云日志服务（ Log Tank Service，LTS ）是高性能、低成本、功能丰富、高可靠的日志平台，提供多种接入方式实现海量日志接入LTS，支持日志搜索引擎、SQL分析引擎、日志加工引擎。

  云容器实例基于LTS采集容器日志，日志文件转储到LTS中，方便您查看和检索。

- **云审计服务**

  云审计服务（ Cloud Trace Service，CTS ）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。

10 区域和可用区

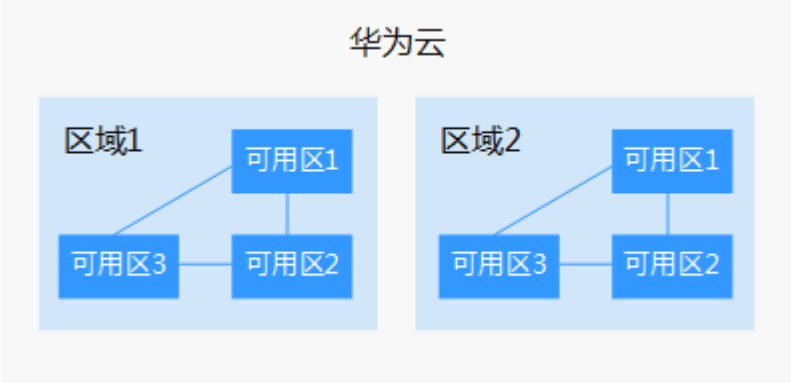
什么是区域、可用区?

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。

图10-1阐明了区域和可用区之间的关系。

图 10-1 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。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。

- 云服务之间的关系
  如果多个云服务一起搭配使用，需要注意：
  - 不同区域的弹性云服务器、关系型数据库、对象存储服务内网不互通。
  - 不同区域的弹性云服务器不支持跨区域部署在同一负载均衡器下。
- 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**。