云容器引擎
Autopilot
抽屉式帮助

文档版本	01
发布日期	2025-06-12

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。

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

1 服务级帮助面板

1.1 工作负载

在Kubernetes中，工作负载是对一组Pod及其运行策略的抽象模型，其定义了业务应用的部署规范、生命周期管理策略和运行时的期望状态。作为业务运行的载体，工作负载通过控制器模式（Controller Pattern）持续观测并动态调整实际Pod实例，确保其始终符合用户声明的目标状态，同时提供版本管理、滚动更新、自动扩缩容等运维能力，使开发者能够以声明式的方式管理从无状态服务到有状态应用、从长期运行服务到批量计算任务等各类业务场景。

CCE Autopilot集群提供基于Kubernetes原生类型的容器部署和管理能力，支持工作负载部署、配置、监控、扩容、升级、删除、服务发现及负载均衡等生命周期管理。

创建工作负载

针对不同业务场景，CCE Autopilot集群支持创建不同类型的工作负载，具体如下：

- **无状态负载（Deployment）**：是一种不依赖本地存储或持久化状态的应用程序，每个Pod实例独立且等效，可以随时替换或扩展。Deployment适用于无需持久化数据的Web服务、API等场景，支持快速扩缩容和滚动更新。
- **有状态负载（StatefulSet）**：是一种需要持久化存储和保留状态的应用程序，每个Pod实例具有唯一标识符和与之关联的持久数据。StatefulSet适用于需要持久化存储和稳定网络标识的应用场景，如数据库和分布式存储系统等。
- **普通任务（Job）**：用于执行一次性或短时运行的批处理任务，任务完成后Pod会自动终止。Job支持并行控制和重试机制，确保任务的可靠执行，典型应用于数据处理、报表生成等场景。
- **定时任务（CronJob）**：用于执行基于时间调度的周期性任务，按照设定的Cron表达式自动触发Job执行。其特点包括精准的定时调度能力和任务历史记录管理，典型应用于日常数据备份、定期报表生成等需要周期执行的批处理场景。

配置工作负载

工作负载支持高级参数配置（如设置环境变量、使用第三方镜像等），以满足您的个性化需求，具体请参见以下链接：

- **配置工作负载**

管理工作负载

工作负载创建后，CCE Autopilot集群提供完整的运维管理能力，包括查看日志、工作负载升级、工作负载回退等，具体请参见以下链接：

- 管理工作负载
- 管理内核参数配置
- 管理自定义资源

工作负载生命周期

工作负载存在以下几种状态，您可以根据通过工作负载状态了解业务运行状况。

表 1-1 状态说明

状态	说明
运行中	所有实例都处于运行中、或实例数为0时显示此状态。
未就绪	容器处于异常、负载下实例没有正常运行时显示此状态。
处理中	负载没有进入运行状态但也没有报错时显示此状态。
可用	当多实例无状态工作负载运行过程中部分实例异常，可用实例不为0，工作负载会处于可用状态。
执行完成	任务执行完成，仅Job存在该状态。
删除中	触发删除操作后，工作负载会处于删除中状态。

1.2 工作负载常见问题

工作负载异常

- 创建工作负载时无法拉取SWR镜像如何解决?
- 创建工作负载时无法拉取公网镜像如何解决?
- 工作负载事件中出现Cluster pod max limit exceeded如何解决?
- 创建工作负载时，Pod不断被重建如何解决?
- 工作负载异常：OOM问题
- Java容器内存虚高以及OOM问题定位

监控日志

- 容器监控的内存使用率与实际弹性伸缩现象不一致

1.3 网络管理

集群网络构成

集群的网络可以分成两部分：

- **容器网络**（为集群内Pod分配IP地址）

  CCE Autopilot集群采用华为云自研的云原生网络2.0模型，该模型基于Kubernetes的IP-Per-Pod-Per-Network架构，深度融合VPC网络能力，具有以下特点：

  - 基于VPC构建容器网络，每个Pod具有独立的网卡及IP地址，易于排查网络问题，且具有最高的性能表现。
  - Pod可直接使用VPC提供的负载均衡、安全组、弹性公网IP等能力。

  关于云原生网络2.0模型的更多信息，请参见**云原生网络2.0模型说明**。

- **服务网络**（为Service分配IP地址）

  在创建Autopilot集群时，您需要预先指定Service的地址范围（即服务网段），该网段将用于为集群中Cluster类型的Service分配固定IP地址。服务网段创建后不支持修改，因此在规划时请确保预留足够的地址空间以满足未来业务扩展需求。

如何访问集群中的 Pod

访问Pod即访问用户的业务，Kubernetes提供**Service**和**Ingress**用来解决Pod的访问问题。

- **Service**

  Service是Kubernetes的一种资源对象，为工作负载（一组Pod）提供稳定的网络访问。它拥有一个固定的IP地址，将流量转发到符合标签选择器的Pod，并自动进行负载均衡，确保流量均匀分配到多个Pod上。Autopilot集群支持为工作负载创建以下类型的Service：

  - **ClusterIP类型**：用于在集群内部互相访问的场景，通过ClusterIP访问Service。
  - **LoadBalancer类型**：用于从集群外部访问的场景，通过一个特定的LoadBalancer访问Service。这个LoadBalancer将请求直接转发到Pod的SubENI，而外部只需要访问LoadBalancer。

- **Ingress**

  Service是基于四层TCP和UDP协议转发的，而Ingress可以基于七层的HTTP和HTTPS协议转发，可以通过域名和路径做到更细粒度的划分。关于路由的更多信息，请参见以下链接：

  - **路由概述**。

从 Pod 访问外部网络

通过合理配置网络策略，可以实现从Pod中访问内网和公网服务，具体如下：

- 从Pod访问内网：在同一VPC下，Pod与其他服务的网络是互通的，但需要注意在对端安全组放通容器网段。
- 从Pod访问公网：
  - **为Pod配置EIP**：创建工作负载时，直接为Pod关联弹性公网IP（EIP），仅绑定EIP的Pod实例具备访问公网的能力。配置EIP可以避免通过NAT进行地址转换，适用于需要将Pod直接暴露给外部网络并与外部系统进行通信的场景。
  - **配置SNAT规则**：在NAT网关中为集群配置SNAT规则后，集群中的Pod实例都将具备访问公网的能力，此时多个Pod共享一个EIP。此方法适用于Pod需要访问外部网络，但不需要对外暴露的场景。

常见问题

- 如何正确配置集群安全组规则?
- 如何确认网卡不被集群占用?

1.4 存储

CCE Autopilot集群的容器存储功能基于Kubernetes容器存储接口（CSI）实现，深度整合云硬盘、文件存储和对象存储等多种云存储服务，并兼容Kubernetes原生存储方案（如EmptyDir）。该功能全面支持有状态应用和AI训练等多样化场景，提供高效且灵活的存储解决方案。

存储类型

从存储介质看，可划分为云存储和本地存储，具体分类如下：

- **云存储**
  - **云硬盘EVS**：为云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，类似PC中的硬盘。
  - **文件存储（仅支持通用文件系统）**：提供按需扩展的高性能文件存储（NAS），可为云上多个服务（如ECS、BMS、CCE）提供共享访问，类似Windows或Linux中的远程目录。
  - **极速文件存储SFS Turbo**：提供一个基于专属计算、专属存储资源池构建的共享文件存储，与公共租户资源物理隔离，能够满足特定性能、应用及安全合规等要求。
  - **对象存储OBS**：提供海量、安全、高可靠、低成本的数据存储能力，可供用户存储任意类型和大小的数据。
- **本地存储**
  - **临时路径（EmptyDir）**：是Kubernetes原生的EmptyDir类型，生命周期与容器实例相同，且支持指定内存作为存储介质。

常见问题

- CCE Autopilot集群中的EVS存储卷被删除或者过期后是否可以恢复?
- 创建存储卷失败如何解决?
- CCE Autopilot集群云存储PVC能否感知底层存储故障?
- 删除动态创建的PVC之后，底层存储有残留如何解决?

1.5 配置项与密钥

Kubernetes通过配置项（ConfigMap）和密钥（Secret）两种核心资源对象，为应用配置和敏感数据管理提供完善的解决方案。它们不仅能够实现配置与容器镜像的解耦，大幅提升部署灵活性，还能通过细粒度的访问控制和加密机制，有效保障集群的安全性和运维效率。

配置项

ConfigMap是Kubernetes中的一种资源类型，用于存储非敏感信息，并以键值对形式保存，供应用程序在运行时使用。ConfigMap具有以下优势：

- 灵活存储：ConfigMap可以存储各种非加密的配置信息，如纯文本、JSON、YAML或属性文件等。
- 使用方式多样：ConfigMap可以作为环境变量、命令行参数或卷中的配置文件供Pod使用。
- 易于更新：配置更新时，无需重新构建容器镜像，只需更新ConfigMap，相关的工作负载即可自动获取最新配置。
- 简化配置管理：ConfigMap支持将配置从应用程序代码中分离出来，使得同一应用可以在不同的环境中使用不同的配置，而无需修改代码。同时，多个应用可以共享同一ConfigMap，从而实现配置的统一化管理，避免配置重复和分散管理。

您可以参考以下链接创建和使用ConfigMap：

- **创建配置项**
- **使用配置项**

密钥

Secret是Kubernetes中专门用于存储和管理敏感信息的资源对象，通过加密存储和访问控制，确保敏感信息的安全性和隐私保护。Secret具有以下优势：

- 安全性：Secret中的数据是经过加密存储的，Kubernetes在存储时会自动进行加密处理，确保敏感信息不会以明文形式保存在集群中。
- 访问控制：通过Kubernetes的角色基础访问控制（RBAC），精确控制哪些服务账户或用户可以访问特定的Secret，从而提高安全性。
- 使用方式多样：Secret可以作为环境变量或卷中的配置文件供Pod使用，这不仅避免在容器镜像中直接存储敏感信息，而且使敏感数据的管理更加简便。
- 易于更新：Secret可以在运行时动态更新，更新后的数据可以立即被相关Pod访问，无需重建容器镜像或重启服务。

您可以参考以下链接创建和使用Secret：

- **创建密钥**
- **使用密钥**

集群系统密钥

除用户自定义的Secret外，CCEAutopilot集群会在每个命名空间下默认创建以下系统密钥，以方便集群的使用。

- default-secret：密钥类型为kubernetes.io/dockerconfigjson，其data内容是登录SWR镜像仓库的凭据，用于从SWR拉取镜像。在CCE Autopilot集群中创建工作负载时，如果需要从SWR拉取镜像，需要配置imagePullSecrets的取值为default-secret。
- paas.elb：密钥类型为cfe/secure-opaque，其data内容是临时AK/SK数据，为Pod和ELB提供动态、短期的安全认证，实现最小权限的云服务访问和自动化资源管理，避免长期密钥泄露风险。

关于集群系统密钥的更多信息，请参见**集群系统密钥说明**。

1.6 应用模板

CCE Autopilot集群提供开箱即用的Helm Chart管理能力，支持通过控制台实现应用模板的一键部署和全生命周期管理，显著提升Kubernetes应用交付效率。您可以通过以下链接了解如何在Autopilot集群中使用Helm模板：

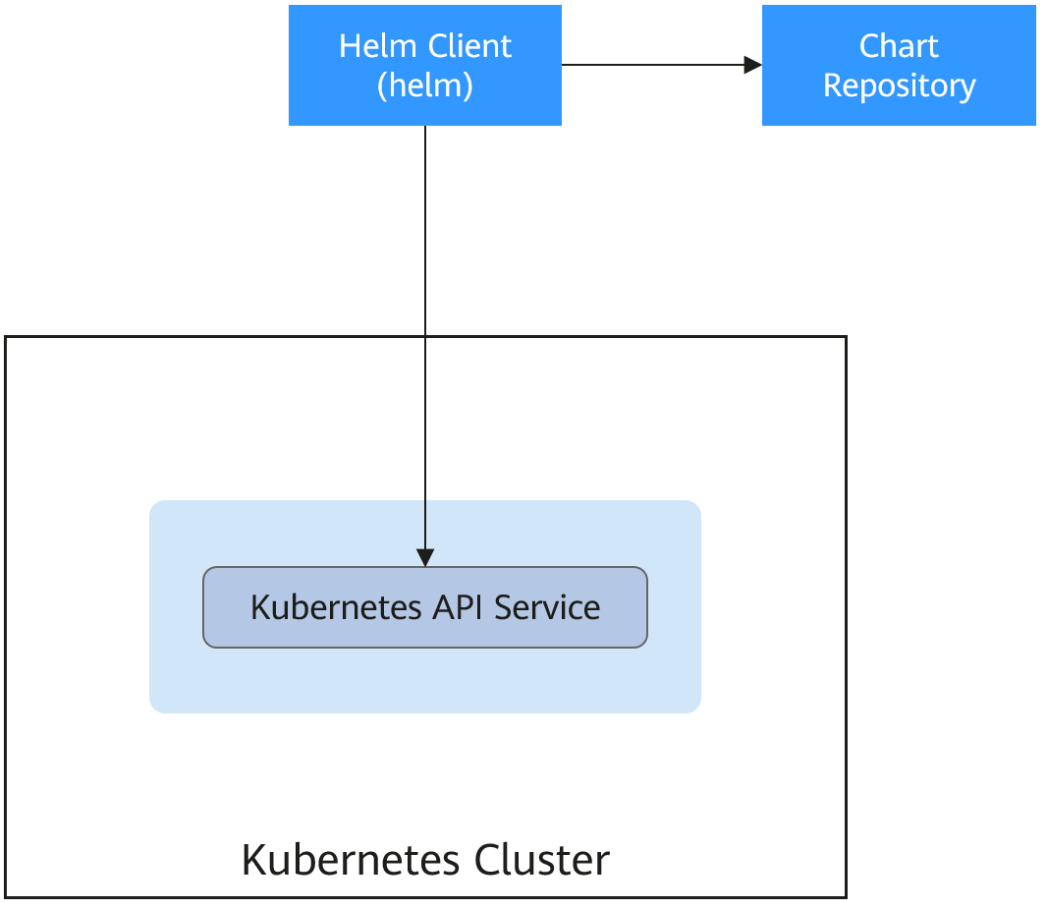
- **通过模板部署应用**。
- **使用模板时的API资源限制**。

Helm 简介

Helm是 Kubernetes 的包管理工具（类比Linux中的apt或yum），用于标准化应用的打包、部署和版本管理。它通过Chart（预配置的模板）定义应用及其依赖关系，支持一键部署复杂应用，并提供版本回滚、依赖管理、多环境适配等能力，大幅提升云原生应用的交付效率和管理体验。Helm的核心作用如下：

- **简化应用部署**：Helm使用Chart描述应用程序的所有Kubernetes资源，包括Pods、Deployments、Services等。Helm使得在Kubernetes上部署和管理应用变得更加简便。
- **动态配置管理**：Helm允许用户使用模板定义Kubernetes资源，这使得用户可以根据不同的需求动态生成资源配置，从而提高灵活性和可扩展性。
- **版本控制与回滚**：Helm支持版本化管理，用户可以轻松回滚到之前的版本，保证应用的可恢复性。
- **依赖管理**：Helm可以管理应用之间的依赖关系，确保依赖的服务或组件在正确的顺序和版本下进行部署。
- **易于共享和分发**：通过Helm Chart，用户可以将自己的应用配置共享给其他人，甚至发布到Helm仓库（类似于包管理的仓库），供他人使用。

Helm的整体架构如下图：



1.7 命名空间

命名空间（Namespace） 是Kubernetes中的一种资源划分和隔离机制。它允许在同一个集群内创建多个逻辑上的“虚拟集群”，每个命名空间都有独立的资源、配置和访问控制。命名空间帮助组织和管理集群中的资源，使得不同的工作负载可以在同一个集群中互不干扰地运行。

命名空间的作用

- **资源隔离**：命名空间可以将不同的应用、环境或团队的资源进行隔离。即使它们在同一集群内运行，资源（如 Pods、Services 等）也可以相互隔离，避免冲突。
- **访问控制和权限管理**：命名空间可以配合Kubernetes的Role-Based Access Control（RBAC）进行细粒度的权限管理，不同的团队或用户只能访问其有权限的命名空间中的资源。
- **资源配额管理**：通过命名空间，可以为每个命名空间设置资源配额（如CPU、内存等），防止某个应用或团队使用过多的资源，影响集群中的其他资源。
- **简化管理**：命名空间有助于对集群内的资源进行分组管理。可以按需创建、删除和管理命名空间，降低集群的复杂性。
- **命名空间与标签的结合**：： Kubernetes允许为命名空间设置标签，以实现资源的灵活组织、管理和标识。通过标签，用户能够实现跨命名空间的资源筛选、分类和搜索，提高集群资源的可维护性和可管理性。

创建和管理命名空间

- 创建命名空间
- 管理命名空间
- 设置资源配额及限制

1.8 集群升级

CCE Autopilot集群严格遵循社区一致性认证，每年发布3个集群版本，每个版本发布后将提供至少24个月的维护周期，确保生产环境的长期稳定运行。强烈建议您在维护周期结束之前升级集群，以持续获得安全更新、漏洞修复及技术支持等关键服务保障。

进行集群升级前，您可以通过**升级概述**和**升级前须知**了解更多信息。

升级路径

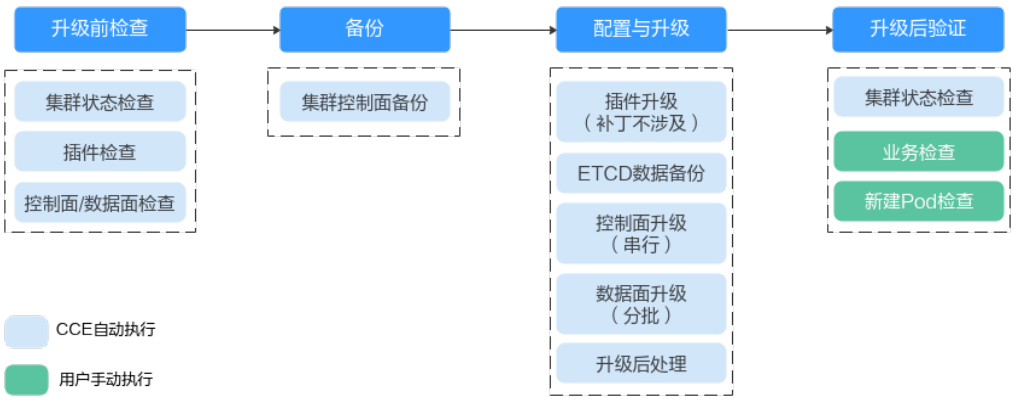
CCE Autopilot集群基于社区Kubernetes版本迭代演进，版本号由社区Kubernetes版本和补丁版本两部分构成，因此提供两类集群升级路径。

- **Kubernetes版本升级**：指集群从当前主版本（如v1.23）升级至更高主版本（如v1.24）的过程，这类升级通常涉及API版本变更、核心功能演进等重大改进。
- **补丁版本升级**：CCE Autopilot集群采取了补丁版本管理策略，旨在不进行大版本升级的情况下，为在维集群提供新的特性、Bugfix和漏洞修复。新的补丁版本发布后，支持一键升级至最新补丁版本。

升级流程

集群升级流程包括升级前检查、备份、升级和升级后验证几个步骤，具体操作步骤请参见**手动升级**。

图 1-1 集群升级流程



1. **升级前检查**：升级集群前，CCE会对您的集群自动进行必要的检查，包括集群状态、插件状态、工作负载兼容性等多方面进行检查，以确保集群满足升级的条件。
2. 备份：CCE将通过硬盘快照的方式帮您备份集群控制面数据，以保存集群的组件镜像、组件配置、Etcd数据等关键数据。

3. 配置与升级：执行升级前，需要对升级参数进行配置，我们已为您提供了默认配置，您也可以根据需要进行配置，升级参数配置完成后，将进入正式升级流程，对插件、控制面、数据面依次进行升级。
4. **升级后验证**：升级完成后，CCE将自动执行集群状态检查。除此之外，您需要手动进行业务验证、新建Pod验证等，以确保升级后集群功能正常。

1.9 插件中心

CCE Autopilot集群提供多种类型的插件，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。

⚠ 注意

CCE Autopilot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。勿直接后台直接修改插件相关资源，以免插件异常或引入其他非预期问题。

插件Pod优先级较高，在集群资源不足时会抢占业务Pod资源，可能导致业务Pod被驱逐重建。

容器调度与弹性插件

插件名称	插件简介
CCE容器弹性引擎插件	CCE容器弹性引擎插件是一款CCE自研的插件，能够基于CPU利用率、内存利用率等指标，对无状态工作负载进行弹性扩缩容。

云原生可观测性插件

插件名称	插件简介
Kubernetes Metrics Server	Kubernetes Metrics Server是集群核心资源监控数据的聚合器。
云原生监控插件	云原生监控插件包含Prometheus-operator和Prometheus组件，提供简单易用的端到端Kubernetes集群监控能力。 使用云原生监控插件可将监控数据与监控中心对接，在监控中心控制台查看监控数据，配置告警等。
云原生日志采集插件	云原生日志采集插件是基于开源fluent-bit和opentelemetry构建的云原生日志采集插件。云原生日志采集插件支持基于CRD的日志采集策略，可以根据您配置的策略规则，对集群中的容器标准输出日志、容器文件日志、节点日志及K8s事件日志进行采集与转发。

容器网络插件

插件名称	插件简介
CoreDNS域名解析插件	CoreDNS域名解析插件是一款通过链式插件的方式为Kubernetes提供域名解析服务的DNS服务器。
NGINX Ingress控制器插件	NGINX Ingress控制器为Service提供应用层转发功能，包括负载均衡、SSL代理和HTTP路由等，支持集群外部直接访问。

容器存储插件

插件名称	插件简介
CCE容器存储插件（Everest）	CCE容器存储插件（Everest）是一个云原生容器存储系统，基于CSI（Container Storage Interface）为Kubernetes集群对接云存储服务的能力。 **说明** 在v1.27.5-r0、v1.28.3-r0及以上版本的CCE Autopilot集群中，该插件由系统自动配置，无需手动安装或更新。

容器安全插件

插件名称	插件简介
CCE密钥管理（对接DEW）插件	CCE密钥管理插件用于对接数据加密服务(Data Encryption Workshop, DEW)。该插件允许用户将存储在集群外部（即专门存储敏感信息的数据加密服务）的凭据挂载至业务Pod内，从而将敏感信息与集群环境解耦，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密。

常见问题

- 如何根据集群中Pod数量调整插件配额?
- NGINX Ingress控制器插件无法使用TLS v1.0和v1.1