解决方案实践

DaoCloud 应用现代化多云协同解决方案实践

文档版本 1.0

发布日期 2024-05-24

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

DaoCloud应用现代化多云协同解决方案（Multi-Cloud cooperation for Application Modernization）（以下简称“解决方案”、“多云方案”或“方案”）是以应用现代化方法体系为核心思想，帮助客户实现数字化转型所需的应用现代化落地，支撑客户分布式业务应用跨云跨地域统一协同治理的解决方案，包括多云集群管理、多云应用编排、多云服务网格。

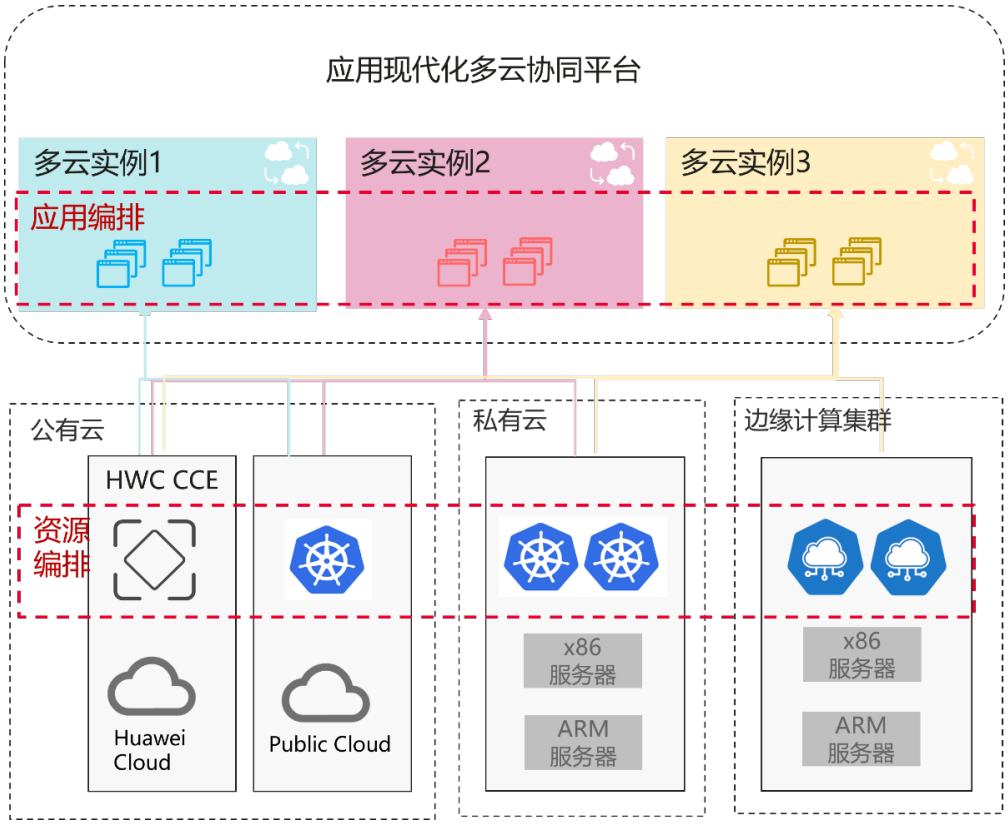
该解决方案可实现多云和混合云的集中管理，支持包含华为云CCE、多个云厂商的容器云以及自建K8s集群的统一管理；帮助用户实现跨云的应用部署、发布和运维的能力；降低跨云微服务应用迁移成本、简化运维管理、提质增效；帮助用户实现基于集群资源的应用弹性扩缩，实现全局负载均衡；支持跨云跨集群东西向互通，跨云跨集群的双模微服务治理，灰度发布，流量治理可视化，丰富的应用流量路由策略；支持X86和ARM芯片架构所构建云平台的统一管理；为用户提供故障恢复的能力，解决多云应用灾备的问题；帮助组织构建更加高效、轻量、智能、开放、弹性和韧性的现代化应用。

应用场景

DaoCloud应用现代化多云协同解决方案主要应用于多云统一管理、多云多实例管理、集群一键导入、多云应用分发、应用故障切换、可观测性、对接全局管理权限等。主要场景如下：

- **场景1：多云资源与应用统一编排管理**

图 1-1 多云资源与应用统一编排管理



客户痛点：

随着企业私有云与异构公有云的集群增加，多云集群与应用管理困难的问题日益突出。

- **集群繁多**：面临繁琐重复的集群配置、云厂商的集群管理差异、碎片化的API访问入口等挑战。
- **业务分散**：被应用在各集群的差异化配置、业务跨云访问、集群间的应用迁移等问题困扰。
- **集群的边界限制**：资源调度受限于集群、应用可用性受限于集群、弹性伸缩受限于集群。
- **被云厂商绑定**：缺少中立的多集群管理平台。

解决方案：

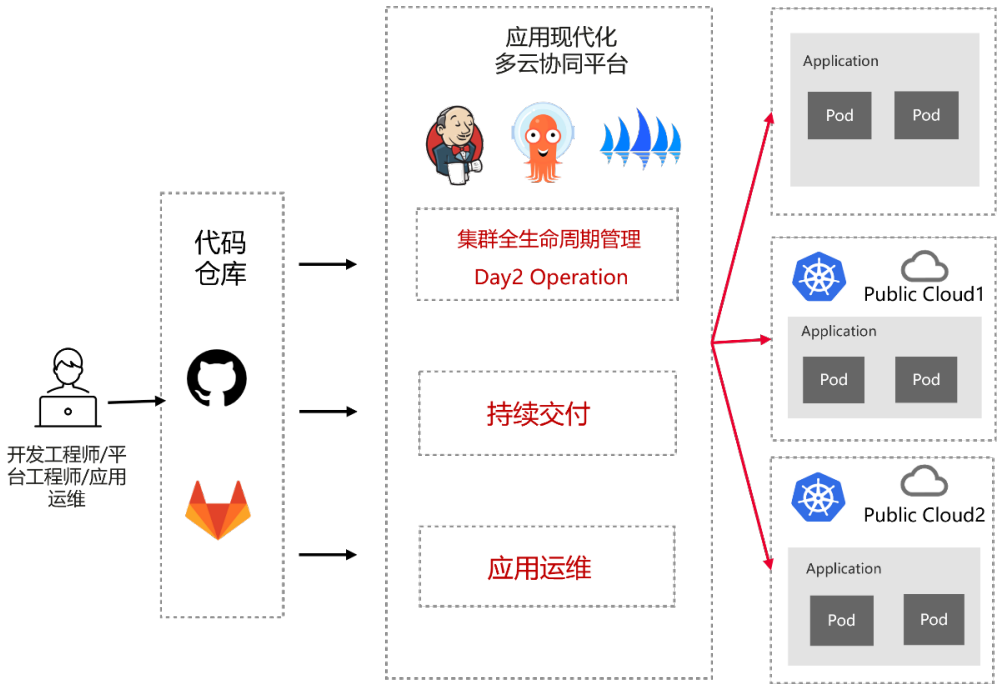
通过DaoCloud的应用现代化多云协同解决方案实现多云资源与应用统一编排管理，分布式资源协同调度能力，支持从最小单元到超大规模资源节点下的集群，和应用跨云自动弹性伸缩，实现跨地域跨服务商条件下的应用特殊化部署，帮助客户实现云成本最优解。

- **多云资源统一管理**：支持多云资源的一键接入，并实时同步接入的集群最新信息，获取多云资源动态，协助用户感知集群、工作负载等资源变化，实现在统一的界面下可视化管理和运维不同厂商提供的各种类型的云资源。
- **多云应用编排管理**：将多个云服务集群资源抽象为多云实例，实例之间隔离工作，互不感知、互不影响；可对所有云上应用进行统一发布和运维管理，支持多维度调度策略，跨云实现应用透明互访及弹性伸缩。
- **应用一键升级**：单云应用一键升级为多云应用，零迁移成本。

- **避免厂商锁定**：可自由选择多个公有云厂商和私有云解决方案，避免受限于单一云厂商，达到云成本特出化的效果。

- **场景2： 多云资源编排与应用交付运维一体化**

图 1-2 多云资源编排与应用交付运维一体化



客户痛点：

- **管理复杂度高**：随着企业采用多云策略，不同云平台在操作和管理上的差异性使得配置和管理的复杂度不断升级。
- **集群全生命周期管理的挑战**：集群管理不仅涉及部署和运行，还包括更新、扩展、监控和最终的下线，要同时手动管理多个集群比较耗时且容易出错。
- **业务需求的复杂性和多样性带来的部署挑战**：随着业务扩展和多样化，业务应用需要在不同的云平台上灵活部署，以满足各种性能、合规性和地理位置的需求。这种需求的复杂性和多样性使得跨多云环境的持续交付面临巨大挑战。

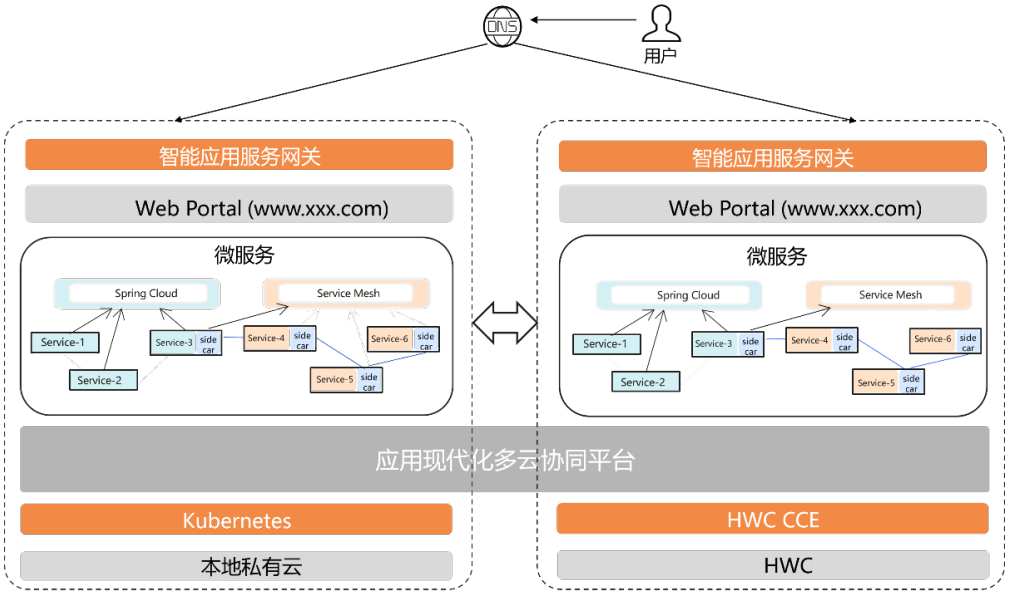
解决方案：

通过DaoCloud应用现代化多云协同解决方案提供GitOps新运维范式融合实现多云架构下的运维全生命周期的一体化与自动化。包括：

- **声明式云资源编排**：云平台工程师可通过声明式代码编写云基础设施资源定义与资源编排规则定义，通过GitOps驱动编排任务的执行，实现集群全生命周期管理与Day2 Operation。
- **GitOps应用交付：**通过更彻底地使用代码定义整个应用的发布交付过程，结合 K8S能够利用自动交付流水线将更改应用到指定的任意多个集群中，从而解决跨云部署的一致性问题。
- **声明式应用运维**：使用配置代码方式对于应用资源和应用状态的定义，通过编排引擎驱动应用运维的自动化执行。

- **场景3：多云应用服务治理**

图 1-3 多云应用服务治理



客户痛点:

应用分布式的部署在不同的异构云上，由非常多的服务组成。不同服务之间相互调用，组成复杂的调用链路，缺少有效的服务治理能力。

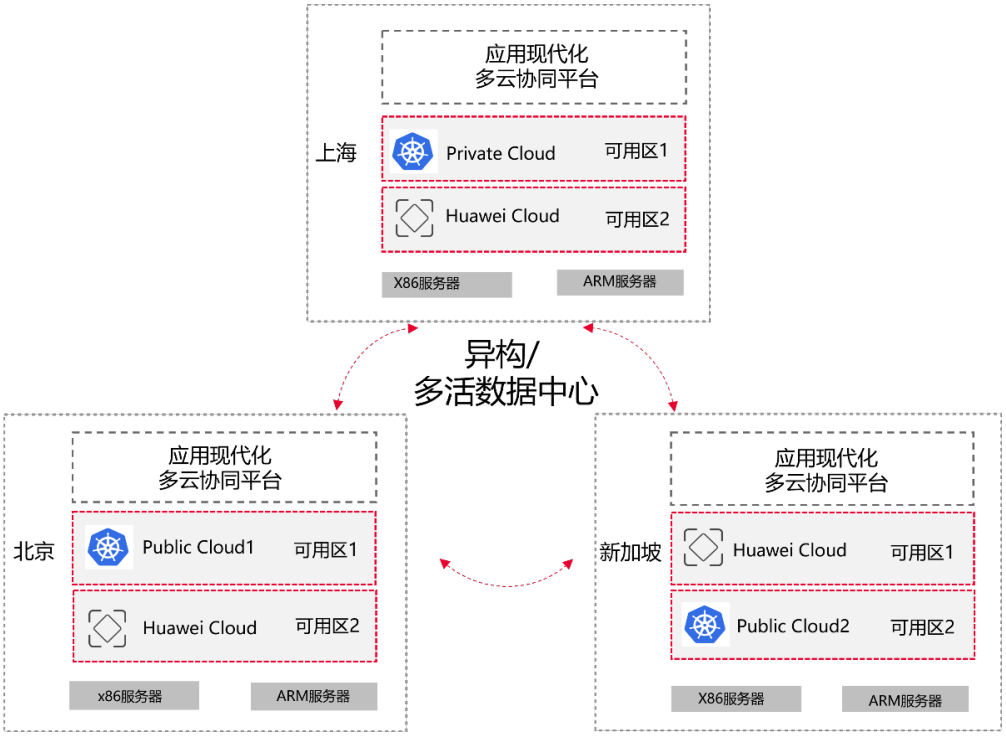
解决方案:

通过DaoCloud的应用现代化多云协同解决方案实现应用服务的统一治理，为多云架构下的应用提供具备高度兼容性的透明通讯与流量治理能力、双模微服务治理能力及全链路观测能力。

- **跨云应用透明与健壮通信：**基于 Service Mesh 技术实现跨云跨集群流量治理能力，提供一致透明的应用层服务发现、请求路由、健康检查、以及超时、重连、限流等通讯容错管理能力。
- **双模微服务治理：**支持传统微服务与新一代微服务技术融合，统一管理。
- **多云应用全链路观测：**对于多云环境下的现代化微服务应用，提供完整的应用全链路观测能力和应用数据分析与可视化能力。
- **跨云应用服务认证访问控制**：以 service-based 的认证与授权机制，在跨多云环境下实现统一可控的服务认证与访问控制管理。

- **场景4：跨云业务连续性：应用多活、多云容灾**

图 1-4 跨云业务连续性：应用多活、多云容灾



客户痛点：

为保障业务连续性，实现应用跨云高可用面临技术复杂性、可扩展性、可用性和弹性挑战。

解决方案：

DaoCloud的应用现代化多云协同解决方案提供应用跨云多活能力，可部署业务应用到不同区域集群，避免单个区域的故障造成应用不可用；平台的统一多云资源管理中心自动监控每个集群的健康状态，出现单个云环境故障时，可以快速自动完成跨云迁移及流量切换。

方案架构

业务架构

该方案的软件部分的业务架构如下：

图 1-5 业务架构

- 该方案的软件部分是架构现代化中的多云协同平台，该平台的底层技术架构采用华为云产品，包括

  原生服务：云容器引擎CCE、容器镜像服务SWR；

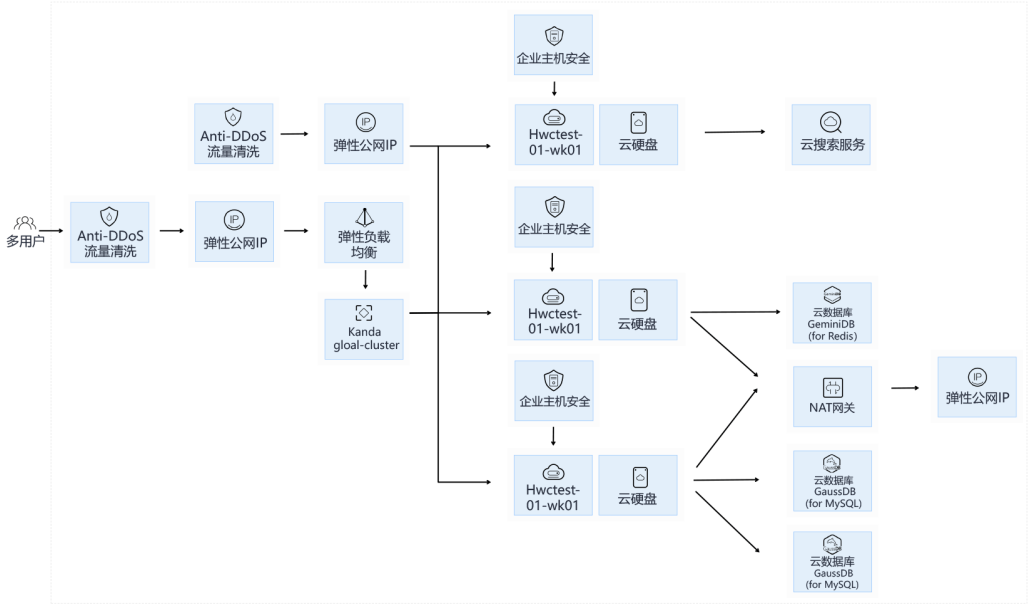
  数据服务：云搜索服务CSS、GaussDB for MySQL、GaussDB for Redis；

  基础云服务：弹性云服务器ECS、企业主机安全HSS、NAT网关、弹性负载均衡ELB、弹性公网IP EIP、弹性文件服务SFS、云硬盘EVS、硬盘备份VBS。
- 该解决方案的软件部分（方案平台软件）在典型场景部署中运行的功能组件如上，包含：全局管理Global management组件、UI组件、应用工作台Workspace组件、容器管理与镜像仓库Container Management组件、服务网格与微服务引擎Service Governance组件、可观测Insight组件、多云编排Karmada Management组件、网络组件、存储Local Storage System组件以及ElasticSearch（ES）中间件（可使用云搜索服务CSS）、MySQL Database（可使用GaussDB for MySQL）中间件。
- 这些组件分别以容器形式运行，通过集群内网络交互，ES和MySQL对内部组件提供数据存储能力；与底层PaaS（华为云容器引擎CCE）通过网络组件及存储组件进行交互，网络组件通过容器标准网络接口CNI自动与CCE的网络层连接，存储组件通过容器标准存储接口CSI自动与CCE连接。
- 方案平台软件的安全、监控和高可用主要由自身提供，也可按需求结合华为云相关服务。
- 方案平台软件的用户主要为租户（运维人员、应用开发/发布人员、存储管理员、网络管理员）和管理员（全局管理员）。
- 方案平台软件对外连接客户已有公有云或私有数据中心的容器云或自建K8s集群，与这些集群的连接可通过公网或VPN专线连接。

部署架构

本部署架构使用华为云的云原生服务、数据服务及基础云服务等为解决方案提供计算、存储和网络资源，DaoCloud多云协同部分是该解决方案最终落地实施的软件平台部分，为现代化应用提供多云集群管理、多云应用编排、多云服务网格。部署架构图如下：

图 1-6 部署架构图



- **华为云服务层**
  - 云容器引擎CCE和弹性云服务器ECS：该解决方案的软件部分以容器形式运行在CCE集群之上，华为云容器CCE服务的底层使用华为弹性云服务ECS部署。
  - NAT网关：该解决方案的软件部分的相关组件（如：多云实例、容器管理）需要和外部被纳管集群的API-Server通信，同时，这些组件可被调度到集群任意节点，因此，这些节点上都配置了NAT网关以确保对外的网络联通，也可根据实际安全需求配置安全组或更严格的互联网访问策略。
  - Anti-DDos流量清洗：通过对互联网访问公网IP的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS为用户生成监控报表，清晰展示网络流量的安全状况。
  - 弹性负载均衡ELB：为应对不同场景下的访问压力，该解决方案采用华为云弹性负载均衡ELB服务，将访问流量自动分发到全局集群的多个容器上，扩展平台对外的服务能力。
  - 弹性公网IP EIP：在弹性负载均衡ELB、NAT网关资源上绑定EIP，使得该解决方案的内部组件可以对互联网提供服务。
  - 企业主机安全HSS：集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。
  - 云硬盘EVS：使用高可靠、高性能、规格丰富并且可弹性扩展的块存储服务并对运行容器提供本地数据库逻辑卷服务。
  - 云搜索服务CSS：华为云ELK生态的一系列软件集合，为多云协同方案提供ELK服务。

- GaussDB for MySQL：用于存储多云协同方案的关键业务数据。
- GaussDB for Redis：用于多云协同方案的缓存数据。

- **多云协同方案平台软件层**
  - 软件功能：主要部署的软件功能组件包括全局管理组件、容器管理组件、服务网格组件、可观测组件、多云编排组件、镜像仓库组件、微服务引擎组件、应用工作台组件、网络组件、存储组件。以上组件以容器形式部署，计算资源、存储资源和网络连接通过CCE提供。其中，网络组件通过容器网络接口CNI自动与CCE的网络层连接，存储组件通过容器存储接口CSI自动与CCE交互，以使得可以使用底层云硬盘EVS的存储资源，并对运行容器提供本地数据库逻辑卷服务。
  - 运维方式：用户和管理员通过该解决方案的平台门户登录进行使用和运维操作，方案平台软件本身可通过云容器引擎CCE提供的门户进行运维操作，可以借助方案平台软件的可观测组件实时监控应用及资源使用情况并配置告警规则及时发现运行问题。
  - 安全防护：主要包括静态安全（容器镜像）和动态安全（容器运行时），方案平台软件各组件的静态安全由DaoCloud维护和保障，动态安全由云原生安全模块进行监测。方案平台软件之上的安全可以结合华为云提供的DDoS防护AAD、Web应用防火墙WAF或第三方相关服务，之下的安全（如底层运行环境安全）可以结合华为云企业主机安全服务HSS或第三方相关服务实现。
  - 高可用部署：该方案平台软件的各组件基于同AZ集群内部署方式，以多副本方式分布在多节点上；使用的GaussDB for MySQL数据库服务，基于跨AZ主备部署，具有主备能力。
  - 备份方案

    云搜索服务CSS的备份：CSS中存放平台及平台应用容器的监控指标、链路数据、日志。为避免数据丢失，将集群的索引数据进行备份，当数据发生丢失或者想找回某一时间段数据时，可以通过恢复索引操作快速获得数据。详细内容请参考：**https://support.huaweicloud.com/intl/zh-cn/usermanual-css/css_01_0033.html**

    GaussDB for MySQL的备份：GaussDB for MySQL中存放平台相关配置数据。定期进行全量备份和增量备份，用户可恢复数据到任意时间节点。详细内容请参考**https://support.huaweicloud.com/intl/zh-cn/usermanual-gaussdbformysql/gaussdbformysql_03_0060.html**

    应用现代化多云协同平台的备份：平台的备份包括平台自身和应用部署信息的备份与恢复，具体操作为定期通过备份集群ETCD和通过ETCD进行恢复。

- **部署要点**
  - 在接入层，使用华为云ELB的负载均衡能力，用户可通过EIP从公网访问该方案的平台门户入口，对于安全高要求的场景，建议通过VPN接入；
  - 在VPC内部，该方案平台不涉及客户最终业务和数据，因此应用和数据通常不划分到不同子网区域；
  - 对于安全高要求的场景，可划分DMZ区，将平台门户入口前置到DMZ区，构建独立的供运维人员和平台用户专用接入的运维区。也可以通过VPN通道供平台用户和运维人员接入；
  - 在对外网络安全方面，如果将该方案平台门户对外暴露，使用华为云WAF和DDos云服务进行防护；
  - 该方案平台的应用资源和数据资源，通过以多副本方式分布在底层K8s集群的多个节点上具备高可用和灾备能力，即该方案平台软件自身的设计以及底层K8s集群的伸缩和调度能力实现；

- 该方案平台软件的运维运营主要通过自有能力—可观测组件实现，在极端情况下如果平台软件无法访问，应通过底层K8s集群的控制台进行运维操作；
- 该方案平台软件使用的中间件包括ElasticSearch和MySQL，使用云搜索服务CSS和云数据库GaussDB for MySQL替换；
- 该方案平台软件的数据存储借助自身存储组件提供的提供本地数据库逻辑卷能力实现，以满足高速存取的需求；
- 该方案平台软件不涉及华为云IoT和AI服务能力，使用华为云的PAAS即云容器引擎CCE服务能力；
- 该方案平台软件的身份认证、访问权限、账号管理以及加密通过内部自有能力实现，也支持基于LDAP和OIDC协议的单点登录以及通过对接身份提供商使用企业或组织已有的账号体系。

方案优势

解决方案优势：

- **效能升级**

  管理超过 50 万个节点和 200 万个Pod海量容器集群统一管理；集群检索性能提升 10 倍；降低企业 IT 基础设施投资成本 50% 以上。

- **第三方云中立**

  遵循中立的原则，客户可为不同的业务选择有特定优势的云服务商，降低对云巨头的依赖；与华为云在多云格局与自主可控市场中均无业务合作禁区。

- **解决方案独特功能**

  跨云故障转移、双模微服务应用统一治理、单云应用一键升级为多云应用、应用跨云迁移、应用跨云调度、高性能多集群检索。

- **多云管理技术指引**

  在解决方案所包含核心开源项目参与公司贡献度世界前列，具备核心代码维护能力，包括多云协同 Karmada 全球第二、服务网格 Istio全球第三（2022年度管理委员会指导席位)、 Kubernetes 近一年全球第三、自主开源多云检索 Clusterpedia、自主开源多云压测工具Kwok；拥有如果干多云协同发明专利。

- **应用现代化标准指引**

  面向全球发布应用现代化方法体系白皮书，深度参与《 应用现代化建设指南 》和《 应用现代化成熟度标准 》编撰。

解决方案对于客户的价值：

- **跨云平台一体化体验**

  支持纳管主流厂商及开源云原生集群，跨云统一管理配置，丰富的企业级权限管理，多云运维监控。

- **分布式资源协同**

  支持协同调度的节点资源超过五十万，跨云自动弹性伸缩，应用跨云故障迁移，实现不同地理位置、资源等条件下的应用特出化部署。

- **智能路由与弹性流量管理**

  支持跨云跨集群东西向互通，跨云跨集群的双模微服务治理，灰度发布，流量治理可视化，丰富的应用流量路由策略。

2 资源和成本规划

本节介绍解决方案实践中资源规划情况，包含以下内容：

说明

客户可根据不同场景及规模，部署规划阶段进行相应调整

表 2-1 资源和成本规划

云资源	名称	规格	数量	每年费用$
云容器引擎	CCE	CCE容器集群 | 混合集群 | 50节点 | 高可用	1	2,448.96
弹性云服务器	ECS	X86计算 | 通用计算型 | s3.4xlarge.2 | 16核 | 32GB	3	8,763.84
云数据库 GaussDB for MySQL（可选）	GaussDB for MySQL	MySQL 8.0 | 多可用区 | 独享型 | x86 | 4C16GB | 2节点 | 100G	1	6,304.48
云数据库 GaussDB for Redis（可选）	GaussDB for Redis	Redis 5.0及以下 | 12GB | 共享型 | geminidb.redis.medium.4 (1 vCPU) | 3节点	1	1,225.44
云搜索服务（可选）	CSS	Elasticsearch 7.6.2 | 3节点 | 通用计算型 ess.spec-8u32g | 高IO 500G	1	11,957.40
企业主机安全	HSS	企业版	3	414.00
云硬盘	EVS	通用型SSD | 300 GB	3	1,080.00
NAT网关	NAT	小型	1	889.87

云资源	名称	规格	数量	每年费用$
弹性负载均衡	ELB	共享 | 全动态BGP | 按流量计费 | 1TB x 1 共享 | 全动态BGP | 按流量计费 | 6TB x 1	2	928.56
弹性公网IP	EIP	独享 | 全动态BGP | 按带宽计费 | 5Mbit/s x 1 独享 | 全动态BGP | 按带宽计费 | 1Mbit/s x 3	4	912.00
费用总计	34,924.54			

3 操作流程

本章节介绍如何在HWC进行应用现代化多云协同平台搭建。

图 3-1 构建用现代化多云协同平台搭建流程图

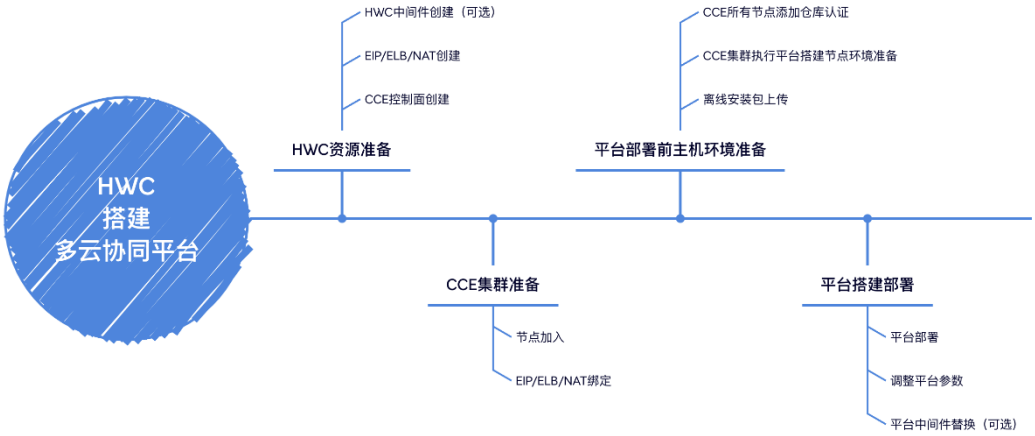


表 3-1 构建应用现代化多云协同平台搭建流程说明

序号	步骤	说明
1	HWC资源准备	在HWC界面进行环境准备： 1. CCE控制面创建； 2. EIP/ELB/NAT创建； 3. HWC中间件创建（ MySQL/Redis/ES ）。
2	CCE集群准备	在CCE控制面进行环境准备： 1. 1. CCE集群添加工作节点； 2. 2. EIP1与其中1节点绑定，EIP2/3与ELB1/2进行绑定，EIP4与NAT网关绑定，NAT网关与CCE集群剩余节点绑定。

序号	步骤	说明
3	平台部署前主机环境准备	在CCE工作节点进行环境准备： 1. 上传平台搭建离线安装包； 2. CCE集群执行平台搭建工作节点进行环境准备，包括Kubectl权限获取、部署配置文件修改、安装部署前置依赖； 3. CCE集群所有节点添加私有镜像仓库认证。
4	平台搭建部署	平台搭建部署： 1. 执行命令进行平台部署； 2. 调整平台参数（绑定ELB地址等）； 3. 平台中间件替换为HWC中间件。

4 实施步骤

4.1 CCE 环境准备

HWC 部署 CCE 集群

本章节介绍如何HWC在部署CCE集群

步骤1 创建虚拟私有云

选择“网络控制台”-> “虚拟私有云” -> “我的VPC”，创建虚拟私有云；

自定义填写参数，完成VPC创建。

步骤2 创建云容器引擎（CCE集群控制面）

使用前面创建的虚拟私有云；

规格确认，进行创建。

步骤3 CCE集群添加节点

进入创建好的CCE集群，进行节点创建；

图 4-1 CCE 集群添加节点

确认资源，完成创建。

----结束

HWC 创建 EIP

本章节介绍如何在HWC进行 EIP创建

选择“弹性公网IP EIP” -> “购买弹性公网IP”

- 多云协同平台搭建需要两个EIP地址：
  - EIP1用于多云协同平台地址访问，并该EIP需要绑定一个ELB
  - EIP2用于多云协同平台数据监控访问，并该EIP需要绑定一个ELB
- CCE集群节点访问互联网需要两个EIP地址

HWC 创建 ELB

本章节介绍如何在HWC进行 EIP绑定ELB

步骤1 选择“弹性负载均衡”-> “负载均衡器”，购买弹性负载均衡

步骤2 负载均衡器绑定创建的eip地址

----结束

HWC 部署 NAT 网关

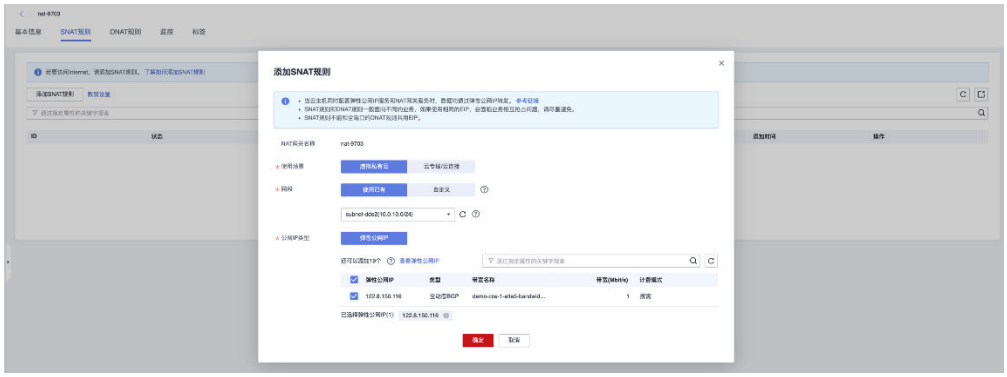
本章节介绍如何在HWC界面进行 EIP绑定NAT网关

步骤1 NAT绑定EIP地址，使CCE集群无弹性IP主机可达互联网完成创建。

图 4-2 HWC 部署 NAT 网关

步骤2 自定义填写参数，为NAT网关绑定SNAT规则。

图 4-3 添加 SNAT 规则



步骤3 绑定完成后，可进入CCE集群无弹性公网IP主机进行互联网地址访问测试。

----结束

HWC 部署中间件（可选）

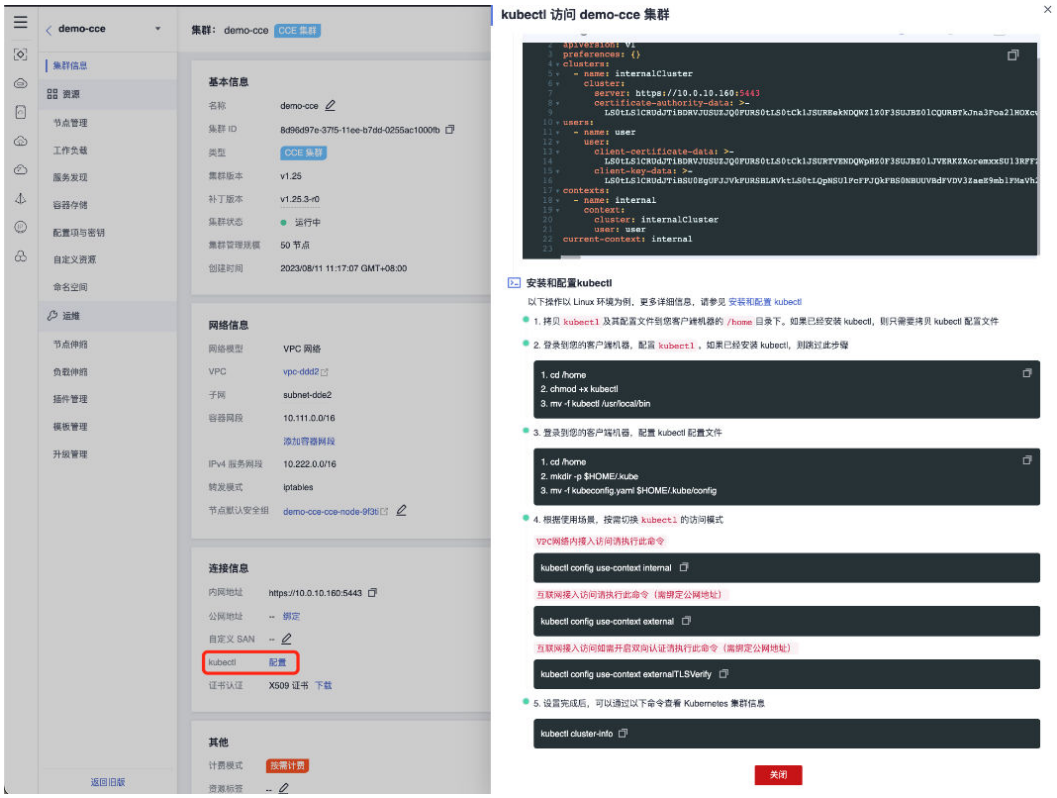
多云协同平台搭建会自动部署容器化中间件，但生产环境下推荐使用HWC外置中间件，中间件与平台独立，提升平台的稳定性。

- 部署GaussDB for MySQL
  HWC界面选择GaussDB for MySQL进行MySQL中间件创建（1套）
- 部署GaussDB for Redis
  HWC界面选择GaussDB for Redis进行Redis中间件创建（1套）
- 部署CSS
  HWC界面选择CSS进行ES中间件创建（1套）

CCE 集群工作节点 Kubectl 权限设置

参照创建的CCE集群“连接信息”“kubectl”配置进行工作节点Kubectl操作权限配置

图 4-4 CCE 集群工作节点 Kubectl 权限设置



4.2 部署应用现代化多云协同平台

模块组件安装

本章节介绍如何在CCE上进行多云协同平台安装

前提条件:

- CCE版本（k8s）> v1.22.x

- 准备一个集群网络可达且存储>50GB的私有镜像仓库

离线安装：

步骤1 登录至CCE集群某节点。

步骤2 下载全模式离线包，可以在**下载中心**下载最新版本。

CPU架构	版本	下载地址
AMD64	v0.10.0	**https://proxy-qiniu-download-public.daocloud.io/DaoCloud_Enterprise/dce5/offline-v0.10.0-amd64.tar**
ARM64	v0.10.0	**https://proxy-qiniu-download-public.daocloud.io/DaoCloud_Enterprise/dce5/offline-v0.10.0-arm64.tar**

步骤3 下载完毕后解压离线包：

```
##以 amd64架构离线包为例：
tar -vxf offline-v0.10.0-amd64.tar
```

步骤4 安装nerdctl命令（可选，如果cr为containerd，需CCE集群内每个工作节点安装）：

```
wget https://github.com/containerd/nerdctl/releases/download/v1.4.0/nerdctl-1.4.0-linux-amd64.tar.gz
tar -zxvf nerdctl-1.4.0-linux-amd64.tar.gz
cp -a nerdctl /usr/local/bin/
```

步骤5 设置集群配置文件 clusterConfig.yaml，可以在离线包 offline/sample 下获取该文件并按需修改。

参考配置为：

```
apiVersion: provision.daocloud.io/v1alpha3
kind: ClusterConfig
metadata:
creationTimestamp: null
spec:
loadBalancer:
type: cloudLB # 建议 cloudLB
istioGatewayVip: 10.5.14.XXX/32（创建的EIP地址1）
insightVip: 10.5.14.XXX/32（创建的EIP地址2）
fullPackagePath: /home/offline # 离线包目录
imagesAndCharts:
type: external
externalImageRepo: http://release.daocloud.io # 私有镜像仓库地址
```

步骤6 配置 manifest 文件，可以在离线包 offline/sample 下获取该文件并按需修改（可选）

如果要开启hwameiStor存储，请确保当前集群中没有默认 StorageClass，如果当前集群中已有默认StorageClass，需要去掉默认StorageClass的配置。

如果不开启hwameiStor存储，可使用CCE自动创建的 StorageClass，此时需要参考如下2个步骤操作：

1. CCE集群可调整自动创建的csi-disk为默认SC：
   ```
   kubectl patch storageclass csi-disk  -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
   ```
2. 修改/offline/sample/manifest.yaml文件，关闭hwameiStor存储：

图 4-5 修改/offline/sample/manifest.yaml 文件

```
[root@demo-cce-82122-fhd8s sample]# cat manifest.yaml
apiVersion: manifest.daocloud.io/v1alpha1
kind: DCEManifest
metadata:
  creationTimestamp: null
global:
  helmRepo: https://release.daocloud.io/chartrepo
  imageRepo: release.daocloud.io
infrastructures:
  hwameiStor:
    enable: false
    version: v0.10.4
    policy: drbd-disabled
```

步骤7 所有工作节点进行私有镜像仓库认证：

Docker：daemon.json文件中添加认证；

Containerd：containerd配置文件中添加认证；

步骤8 执行部署动作节点

1. 安装前置依赖

   进入解压后的offline目录,执行以下操作：

   ```
   cd /xxx/offline/utils
   ./install_prerequisite.sh online full
   ```

   等待安装执行

2. 安装多云协同平台

图 4-6 安装多云协同平台

```
[root@demo-cce-1-kfxlv utils]# ls
checkCommunityManifest.sh  get_latest_helms.sh      offline-export.sh        remove_terminating_ns.sh
download_packages.sh       install_prerequisite.sh  offline_image_handler.sh  update_sample_manifest.sh
[root@demo-cce-1-kfxlv utils]# ./install_prerequisite.sh online full
Current package url: https://files.m.daocloud.io/get.helm.sh/helm-v3.11.1-linux-amd64.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    93  100    93    0     0     37      0  0:00:02  0:00:02 --:--:--    37
100 14.3M  100 14.3M    0     0   872k      0  0:00:16  0:00:16 --:--:-- 1330k
Current package url: https://files.m.daocloud.io/github.com/lework/skopeo-binary/releases/download/v1.11.1/skopeo-linux-amd64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   129  100   129    0     0     52      0  0:00:02  0:00:02 --:--:--    52
  0     0    0     0    0     0      0      0 --:--:--  0:00:05 --:--:--     0Warning: Transient problem: timeout Will retry in 1 seconds. 10 retries left.
100 33.1M  100 33.1M    0     0  1317k      0  0:00:25  0:00:25 --:--:-- 1396k
Current package url: files.m.daocloud.io/dl.k8s.io/release/v1.26.5/bin/linux/amd64/kubectl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   103  100   103    0     0    242      0 --:--:-- --:--:-- --:--:--   242
100 45.8M  100 45.8M    0     0  1198k      0  0:00:39  0:00:39 --:--:-- 1273k
Current package url: https://files.m.daocloud.io/github.com/mikefarah/yq/releases/download/v4.31.1/yq_linux_amd64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
```

```
/offline/dce5-installer install-app -m ./offline/sample/manifest.yaml -c ./offline/sample/
clusterConfig.yaml
```

说明

部分参数介绍，更多参数可以通过 ./dce5-installer --help 来查看：

- -z 最小化安装
- -c 指定集群配置文件，使用 NodePort 暴露控制台时不需要指定 -c
- -d 开启 debug 模式
- -m 指定安装使用的manifest文件
- --serial 指定后所有安装任务串行执行

步骤9 安装完成后，命令行会提示安装成功。恭喜您！ 现在可以通过屏幕提示的 URL 使用默认的账户和密码（admin/changeme）探索全新的多云协同平台啦！

图 4-7 URL 使用默认的账户和密码（admin/changeme）

步骤10 根据提示URL访问界面，使用获取到的license文件进行平台激活。

----结束

验证平台就绪

本章节介绍在协同平台部署就绪后，验证平台是否就绪

按照所提示访问地址信息进行平台访问，并完成激活。

界面功能正常使用无报错，平台就绪。

图 4-8 验证平台就绪

4.3 调整协同平台中间件（可选）

本章节介绍在协同平台部署就绪后，修改所依赖的中间件环境信息为HWC中间件。

前提条件：

- 已具备HWC创建的MySQL/Redis/ES中间件
- 中间件与CCE集群网络可达

说明

平台中间件调整后，会自动初始化数据至新中间件内存放。

- Ipavo相关调整:
  a. 在MySQL数据库中创建ipavo库以及对应的登录用户ipavo；
  b. 调整Ipavo配置文件中的中间件地址（MySQL），并重启Ipavo服务。
- Ghippo相关调整：
  a. 在MySQL数据库中创建ghippo/audit/keycloak三个库，且三个库对应的登录用户名为ghippo/audit/keycloak；
  b. 调整Ghippo配置文件中的中间件地址（MySQL），并重启Ghippo服务。
- Kpanda相关调整：
  a. 在MySQL数据库中创建kpanda库以及对应的登录用户kpanda；
  b. 调整Kpanda配置文件中的中间件地址（MySQL与Redis），并重启Kpanda服务。
- Insight相关调整：
  a. 在MySQL数据库中创建insight库以及对应的登录用户insight；
  b. 调整Insight配置文件中的中间件地址（MySQL与ES），并重启Insight服务。
- Skoala相关调整：
  a. 在MySQL数据库中创建skoala库以及对应的登录用户skoala;

b. 调整Skoala配置文件中的中间件地址（MySQL），并重启Skoala服务。

- Amamba相关调整：
  a. 在MySQL数据库中创建amamba库以及对应的登录用户amamba;
  b. 调整Amamba配置文件中的中间件地址（MySQL），并重启Amamba服务。

5 附录

背景信息

表 5-1 常见名词介绍

简介	名称	解释	组件
CR	Container Runtime	容器运行时是负责运行容器的组件	Docker Containerd
SC	StorageClass	StorageClass 是管理员用来描述可用的不同存储类型的一种方法	NFS HostPath Disk
CNI	Container network interface 容器网络接口	容器网络接口插件是遵循 appc/CNI 协议的一类网络插件	Calico Cilium Macvlan
VPC	Virtual Private Cloud 虚拟私有云	为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境	“/”
Registry	镜像仓库	容器镜像仓库是一种存储库（或存储库集合），用于存储 Kubernetes、DevOps 和基于容器的应用开发的容器镜像	私有仓库 公有仓库

常见问题

- **无法通过配置的EIP（isito-ingressgatewayVIP）访问多云协同平台**
  访问EIP时，界面无法正常打开，自动重定向跳转至了VPC的内网地址
  此时需要替换并修改Ghippo模块中定义的地址信息：

```
helm -n ghippo-system get values ghippo > /tmp/ghippo
helm -n ghippo-system upgrade ghippo ghippo/ghippo --values=/tmp/ghippo --set
global.reverseProxy=https://119.x.x.x（该地址为设置isito-ingressgatewayVIP的EIP）
```

- **重启集群（虚拟机）istio-ingressgateway无法启动**

图 5-1 报错提示

可能原因：RequestAuthentication ghippo CR 的 jwtsUri 地址无法访问， 导致 istiod 无法下发配置给 istio-ingressgateway

解决方法：

a. 备份 RequestAuthentication ghippo CR
```
kubectl get RequestAuthentication ghippo -n istio-system -o yaml > ghippo-ra.yaml
```

b. 删除 RequestAuthentication ghippo CR
```
kubectl delete RequestAuthentication ghippo -n istio-system
```

c. 重启 Istio
```
kubectl rollout restart deploy/istiod -n istio-system
kubectl rollout restart deploy/istio-ingressgateway -n istio-system
```

d. 重新 apply RequestAuthentication ghippo CR
```
kubectl apply -f ghippo-ra.yaml
## apply RequestAuthentication ghippo CR 之前，请确保 ghippo-apiserver 和 ghippo-keycloak 服务已经正常启动。
```

- **MySQL故障**

CR 创建数据库失败报错：

数据库运行正常，使用 CR 创建数据库出现了报错，此类问题的原因有：mysql root 密码有特殊字符

图 5-2 CR 创建数据库失败报错

解决方法：

a. 获取查看原密码：
```
[root@master-01 ~]$ kubectl get secret -n mcamel-system mcamel-common-mysql-cluster-secret -o=jsonpath='{.data.ROOT_PASSWORD}' | base64 -d
```

如果密码含有特殊字符 - ，进入MySQL的shell输入原密码出现以下错误

```
bash-4.4# mysql -uroot -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
```

b. 清理重建：

- 方法一：清理数据目录，删除 Pod 等待 sidecar running 以后，再删除一次数据目录，再删除 Pod 即可恢复:

```
[root@master-01 ~]# kubectl exec -it mcamel-common-mysql-cluster-mysql-1 -n mcamel-system -c sidecar -- /bin/sh
```

```
sh-4.4# cd /var/lib/mysql
sh-4.4# ls | xargs rm -rf
```

- 方法二：删除 PVC 再删除 Pod，只需要处理一次,即可恢复：

```
kubectl delete pvc data-mcamel-common-mysql-cluster-mysql-1 -n mcamel-system
kubectl delete pod mcamel-common-mysql-cluster-mysql-1 -n mcamel-system
```

6 修订记录

表 6-1 修订记录

发布日期	修订记录
2024-05-24	第一次正式发布。