多云容器平台

用户指南

文档版本 01

发布日期 2022-08-17

华为技术有限公司

版权所有 © 华为技术有限公司 2023。 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。

目 录

1 权限管理.....1
2 使用流程.....3
3 创建 MCP.....5
4 无状态工作负载（Deployment）.....7
5 资源管理.....13
5.1 集群管理.....13
5.1.1 典型场景与网络说明.....13
5.1.2 添加 CCE 集群到 MCP.....14
5.1.3 添加其他公有云集群到 MCP.....15
5.1.4 添加自建 Kubernetes 集群到 MCP.....17
5.1.5 获取 KubeConfig.....19
5.1.6 使用 kubectl 命令行工具访问 MCP.....20
5.1.7 其他操作.....22
5.2 网络管理.....23
5.2.1 网络概述.....23
5.2.2 ClusterIP 访问.....23
5.2.3 NodePort 访问.....25
5.2.4 LoadBalancer 访问.....28
5.2.5 Ingress 访问.....29
5.3 存储声明.....31
5.3.1 使用容器存储.....31
5.4 命名空间.....35
5.5 配置中心.....37
5.5.1 配置项（ConfigMap）.....37
5.5.2 密钥（Secret）.....38
6 策略中心.....41
6.1 部署策略.....41
6.2 差异化策略.....42
6.3 域名访问.....46
7 监控中心.....50
7.1 监控运维.....50

7.1.1 负载 50
7.1.2 实例 51
7.1.3 节点 51
7.2 接入管理 52
7.3 Metrics Server 安装 53
7.4 Prometheus 安装 55
7.5 Prometheus-Adapter 安装 56
8 镜像仓库 58
9 集群控制台 60
9.1 查看集群中节点 60
9.2 为节点添加标签 60
9.3 命名空间 62
9.4 工作负载 64
9.4.1 创建工作负载 64
9.5 创建任务 71
9.6 容器组 73
9.7 配置中心 73
9.7.1 创建配置项 73
9.7.2 创建密钥 75

1 权限管理

创建用户并授权使用 MCP

如果您需要对您所拥有的MCP进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用MCP资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将MCP资源委托给更专业、高效的其他帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用MCP服务的其它功能。

本章节为您介绍通过用户组给IAM用户授权的方法，操作流程如**图1-1**所示。

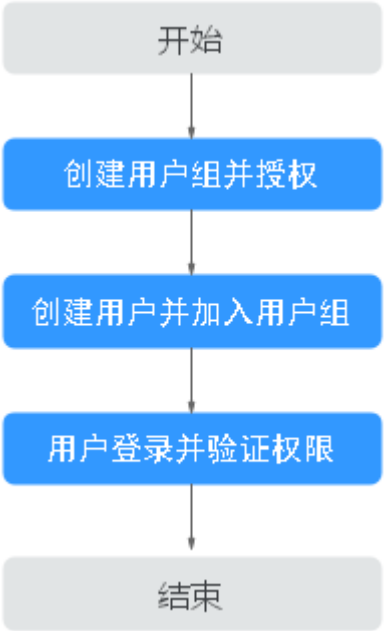
前提条件

- 如您需要创建IAM用户来使用MCP，请先用华为云帐号为当前区域下的MCP服务授权，参见**给MCP授权**。
- 授权前，请您了解IAM用户可以添加的权限，并结合实际需求进行选择。若您需要对除MCP之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

版权所有 © 华为技术有限公司

示例流程

图 1-1 给 IAM 用户授予权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予VPC管理员权限“VPC Administrator”和CCE管理员权限“CCE Administrator”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   – 在“服务列表”中选择多云容器平台，进入MCP主界面，单击右上角“购买MCP”，尝试购买MCP，如果可以购买MCP，表示权限已生效。

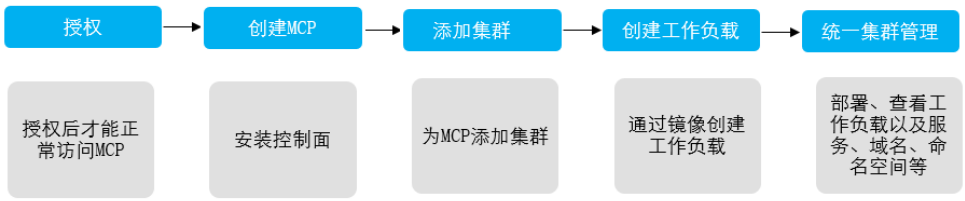
版权所有 © 华为技术有限公司

2 使用流程

使用流程

使用MCP前建议简单了解MCP使用流程如**图2-1**，**立即体验，前往MCP控制台>>**。

图 2-1 MCP 使用流程



步骤1 给MCP授权。

在您开通MCP服务时，需要为其授权。当您进入MCP首页，如果之前没有给MCP授权，则会看到如下提示。请单击“同意授权”进行授权。

图 2-2 服务授权界面

版权所有 © 华为技术有限公司

步骤2 根据功能说明，创建对应的MCP。

- **创建MCP**

步骤3 为MCP添加集群。

- **添加CCE集群到MCP**
- **添加其他公有云集群到MCP**
- **添加自建Kubernetes集群到MCP**

步骤4 创建工作负载。

您可以使用华为云容器镜像服务（SWR）中的镜像、开源镜像中心或第三方镜像来创建工作负载。

步骤5 可以部署工作负载，添加服务、存储声明和命名空间等。

----结束

3 创建 MCP

MCP是华为云基于多年容器云领域实践经验和社区先进的集群技术，提供的容器混合云。

创建 MCP

步骤1 登录多云容器平台。

步骤2 单击右上角的“创建MCP”。

步骤3 填写参数。

- **区域**

  默认选择当前区域。可修改为其他可选区域。

  说明

  请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。

- **MCP名称**

  新建MCP的名称，命名必须唯一。

- **枢纽私有云**

  选择MCP要绑定的虚拟私有云（VPC），绑定VPC后，您可以通过云专线将私有云或其他公有云Kubernetes集群与枢纽VPC连接，还可以通过VPC对等连接将MCP与同区域的CCE集群连接。详细信息请参见网络说明。

  须知

  MCP网段、枢纽VPC网段以及Kubernetes集群的网段之间不能互相冲突，请在添加集群前确保网段不同，否则无法添加集群。

- **MCP网段**

  此网段为MCP内部使用网段。若待加入集群通过公网接入，选择默认网段即可，如需打通待加入集群与MCP网络，通过专线接入，则需要设置此网段，避免和集群中使用网段冲突。

  – MCP网段的掩码固定为22位。推荐使用子网10.253.0.0/22、172.31.0.0/22。
  – MCP网段应避免与这些网段冲突：

版权所有 © 华为技术有限公司

  - 枢纽私有云所使用的网段。
  - 通过非公网方式接入的集群所使用的网段，包括但不限于容器网段、ServiceIP网段、集群Node节点网段。
- 建议从10.2.0.0/16~10.246.0.0/16，10.248.0.0/16~10.255.0.0/16，172.17.0.0/16~172.31.0.0/16覆盖范围中选取一个掩码为22的子网。
- 不推荐使用192.168.0.0/16、172.16.0.0/16、 10.0.0.0/16、10.1.0.0/16、10.247.0.0/16覆盖范围内的22位掩码子网（极易与用户集群环境中网段冲突）。

须知

此参数在MCP创建后不可更改，请谨慎选择。

步骤4 单击“创建”。进入信息确认界面。

单击“提交”。创建MCP大约需要15分钟，请耐心等待。

步骤5 MCP创建成功后，单击“进入MCP控制台”，可进入创建的MCP控制台。

----结束

版权所有 © 华为技术有限公司

4 无状态工作负载（Deployment）

无状态工作负载（Deployment）可以将配置的无状态工作负载（Deployment）自动部署到所选择的Kubernetes集群。

多云容器平台目前支持2种方式创建工作负载：

通过控制台创建

通过Kubectl命令行创建

通过控制台创建

步骤1 登录MCP控制台，在左侧导航栏中单击“工作负载 > 无状态Deployment”，在右侧页面中单击“创建无状态工作负载”。

步骤2 设置工作负载基本信息。

- 工作负载名称：新增工作负载的名称，命名必须唯一。
- 命名空间：选择工作负载所在命名空间。
- 部署集群：选择需要部署工作负载的集群，集群个数请您根据自身业务进行选择。
- 实例部署方式：支持“普通模式”和“权重模式”两种实例部署方式。
- 实例数量：当“实例部署方式”选择为“普通模式”时生效。设置多集群的工作负载中各集群的实例数。用户可以设置具体实例个数，默认为2。每个工作负载实例都由相同的容器部署而成。在MCP中可以通过设置弹性扩缩容策略，根据工作负载资源使用情况，动态调整工作负载实例数。
- 权重比例：当“实例部署方式”选择为“权重模式”时生效。设置多集群的工作负载的总实例数以及各集群的权重、实例范围。

步骤3 单击“下一步”，添加容器。

1. 单击“添加容器”选择需要部署的镜像。

说明

在创建无状态工作负载时如果选择了多个并且跨区域集群时，为了减少镜像上传更新的操作以及加速MCP管理的应用跨区域镜像拉取，则在选择需要部署的镜像时可以使用镜像自动同步功能，具体操作请参考自动同步镜像。

– 我的镜像：按区域展示华为云镜像仓库中的镜像。若无可用的镜像，可单击“上传镜像”进行上传。

    - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
    - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
  - 开源镜像中心：展示了开源镜像仓库中的官方镜像。
    - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
    - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
  - 第三方镜像：MCP支持拉取第三方镜像仓库（即华为云镜像仓库与开源镜像仓库之外的镜像仓库）的镜像创建工作负载。使用第三方镜像时，请确保工作负载运行的节点可访问公网。
    - 若您的镜像仓库不需要认证，密钥认证请选择“否”，并输入“镜像地址”，单击“确定”。
    - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，并输入“镜像地址”，单击“确定”。

      说明

      此处设置的密钥是通用配置。具体集群的密钥，请在“集群差异配置”步骤中，勾选“容器设置”的“差异配置”。在“基本信息”中单击“更换镜像”，并选择正确的密钥。

  若您的工作负载包含多个容器，请单击右上方“添加容器”，再执行添加容器的操作。

2. 设置容器基本信息。
  - 镜像名称：镜像的名称，您可单击“更换镜像”进行更换。
  - 镜像版本：请选择需要部署的镜像版本。
  - 容器名称：容器的名称，可修改。
  - 容器规格：申请和限制的含义如下，详情请参见设置容器规格。
    - 申请：表示容器运行所需最少资源。
    - 限制：若担心容器超载，导致系统故障。建议设容器配额的最高限制。确保容器资源不会超额。
3. 配置生命周期，用于管理容器各阶段需要执行的命令。
  - 启动命令：设置容器启动时执行的命令。
  - 启动后处理：设置容器成功运行后执行的命令，详细配置方法请参见设置容器生命周期。
  - 停止前处理：设置容器结束前执行的命令，通常用于删除日志/临时文件等，详细配置方法请参见设置容器生命周期。
4. 设置健康检查，用于判断容器和用户业务是否正常运行。设置了存活与业务两种探针，详细配置方法请参见容器健康检查。
  - 工作负载存活探针：监测到容器实例不健康时，重启应用。
  - 工作负载业务探针：监测到容器实例不健康时，将工作负载设置为未就绪状态，业务流量不会导入到该容器中。

版权所有 © 华为技术有限公司

5. 设置环境变量。

   在容器中添加环境变量，一般用于通过环境变量设置参数。

   在“环境变量”中，单击“添加环境变量”。

6. 安全设置。

   对容器权限进行设置，保护系统和其他容器不受其影响。

   请输入用户ID，容器将以当前用户权限运行。

7. 数据存储。

   给容器挂载数据存储，适用于需持久化存储、高磁盘IO等场景。详细配置请参见**存储声明**。

步骤4 单击“下一步”，设置访问方式（Service）。

若工作负载需要和其它服务互访，或需要被公网访问，您需要添加服务，设置访问方式。工作负载访问的方式决定了这个工作负载的网络属性，不同访问方式的工作负载可以提供不同网络能力，操作详情请参见**网络管理**。

- ClusterIP：只能集群内访问服务，详细信息见**ClusterIP访问**。
- NodePort：可以通过集群内任意节点访问到服务，详细信息见**NodePort访问**。

步骤5 单击“下一步”，对负载进行高级设置。

- 升级策略：支持“滚动升级”和“替换升级”。
  - 滚动升级：滚动升级将逐步用新版本的实例替换旧版本的实例，升级的过程中，业务流量会同时负载均衡分布到新的和旧的实例上，因此业务不会中断。

    最大无效实例数：每次滚动升级允许的最大无效实例数，如果等于实例数有断服风险（最小存活实例数 = 实例数 - 最大无效实例数）。
  - 替换升级：先删除旧实例，再创建新实例。升级过程中业务会中断。
- 缩容策略：输入时间。为工作负载删除提供一个时间窗，在执行**停止前处理**的命令。若超过此时间窗，进程仍未停止，该工作负载将被强制删除。
- 迁移策略：工作负载实例所在的节点不可用的情况下，将工作负载实例重新调度到其它可用节点的时间窗，默认300秒。
- Pod标签：内置app标签在工作负载创建时指定，暂不支持修改。您可以单击下方的“添加标签”增加标签。

步骤6 单击“下一步”，对选择的集群进行差异化配置。勾选对应集群后的“差异配置”，对容器进行差异化配置，各选项配置请参见**步骤3**，其余请参见**步骤5**。

版权所有 © 华为技术有限公司

图 4-1 集群差异化配置

步骤7 设置完成后，单击“确定”完成创建。

----结束

通过 Kubectl 命令行创建

本节以nginx工作负载为例，说明kubectl命令创建工作负载的方法。

1. 请参见**使用kubectl命令行工具连接MCP**，使用kubectl连接集群。

2. 创建一个名为nginx-deployment.yaml的描述文件。其中，nginx-deployment.yaml为自定义名称，您可以随意命名。

vi nginx-deployment.yaml

在描述文件中插入以下内容：

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  strategy:
    type: RollingUpdate
  template:
    metadata:
```


版权所有 © 华为技术有限公司

```
    labels:
      app: nginx
  spec:
    containers:
    - image: nginx    若使用“我的镜像”中的镜像，请在SWR中获取具体镜像地址。
      imagePullPolicy: Always
      name: nginx
    imagePullSecrets:
    - name: default-secret
```

说明

此处仅为示例，deployment的详细说明请参见**kubernetes官方文档**。

以上yaml字段解释如**表1**。

表 4-1

字段名称	字段说明	必选/可选
apiVersion	表示API的版本号。填写时需要参考当前集群的版本： ● 1.17及以上版本的集群中无状态应用apiVersion格式为**apps/v1** ● 1.15及以下版本的集群中无状态应用apiVersion格式为**extensions/v1beta1**	必选
kind	创建的对象类别。	必选
metadata	资源对象的元数据定义。	必选
name	deployment的名称。	必选
Spec	用户对deployment的详细描述的主体部分都在spec中给出。	必选
replicas	实例数量。	必选
selector	定义Deployment可管理的容器实例。	必选
strategy	升级类型。当前支持两种升级方式，默认为滚动升级。 ● RollingUpdate：滚动升级。 ● ReplaceUpdate：替换升级。	可选
template	描述创建的容器实例详细信息。	必选
metadata	元数据	必选
labels	metadata.labels定义容器标签。	可选

版权所有 © 华为技术有限公司

字段名称	字段说明	必选/可选
spec: containers	● image（必选）：容器镜像名称。 ● imagePullPolicy（可选）：获取镜像的策略，可选值包括Always（每次都尝试重新下载镜像）、Never（仅使用本地镜像）、IfNotPresent（如果本地有该镜像，则使用本地镜像，本地不存在时下载镜像），默认为Always。 ● name（必选）：容器名称。	必选
imagePullSecrets	Pull镜像时使用的secret名称。 ● 需要Pull SWR容器镜像仓库的镜像时，参数值固定为default-secret。 ● 当Pull第三方镜像仓库的镜像时，需设置为创建的secret名称。	若使用私有镜像，该参数为必选。

3. 创建deployment。

kubectl create -f nginx-deployment.yaml

回显如下表示已开始创建deployment。

```
deployment "nginx" created
```

4. 查看deployment状态。

kubectl get deployment

deployment状态显示为Running，表示deployment已创建成功。

```
NAME          READY     UP-TO-DATE   AVAILABLE   AGE
nginx         1/1       1            1           4m5s
```

参数解析：

o NAME：pod的名称

o READY：已经部署完毕的pod副本数

o STATUS：状态

o RESTARTS：重启次数

o AGE：已经运行的时间

5. 若工作负载（即deployment）需要被访问（集群内访问或节点访问），您需要设置访问方式，具体请参见网络管理创建对应服务。

版权所有 © 华为技术有限公司

5 资源管理

5.1 集群管理

5.1.1 典型场景与网络说明

典型场景

MCP可以添加华为云、其他公有云和私有云Kubernetes集群，支持如下三个场景：

- 混合云场景：

  混合云是融合了华为云和自建数据中心Kubernetes集群的场景，即为MCP添加华为云的CCE集群和自建的私有云Kubernetes集群。

  添加方式参考**添加CCE集群到MCP**和**添加自建Kubernetes集群到MCP**。

- 多云场景：

  多云是跨多个云服务商的公有云集群的场景，即为MCP添加华为云的CCE集群和其他公有云运营商的集群，如阿里云、腾讯云等。

  添加方式参考**添加CCE集群到MCP**和**添加其他公有云集群到MCP**。

- 多区域场景：

  多区域是融合了华为云多个区域下CCE集群的场景，即为MCP添加位于不同虚拟私有云、不同区域的CCE集群。

  添加方式参考**添加CCE集群到MCP**。

网络说明

在给MCP添加Kubernetes集群前，您需要先考虑MCP与各集群间的网络访问连接问题。如果MCP与Kubernetes都有公网IP，那二者之间能够通过公网IP互相访问。

除使用公网IP外，MCP还支持无公网IP场景下管理Kubernetes集群。在创建MCP时，您可以绑定一个枢纽VPC（Hub VPC），枢纽VPC与MCP所在VPC建立了**对等连接**（peering），通过枢纽VPC，MCP能够通过如下方式与Kubernetes集群连接。

- 如果集群在枢纽VPC内，那MCP绑定枢纽VPC，集群与MCP就能互相访问。
- 如果集群是在MCP所在区域的其他VPC内，那可以通过建立集群所在VPC与枢纽VPC之间的**对等连接**，实现MCP与集群的互相访问。

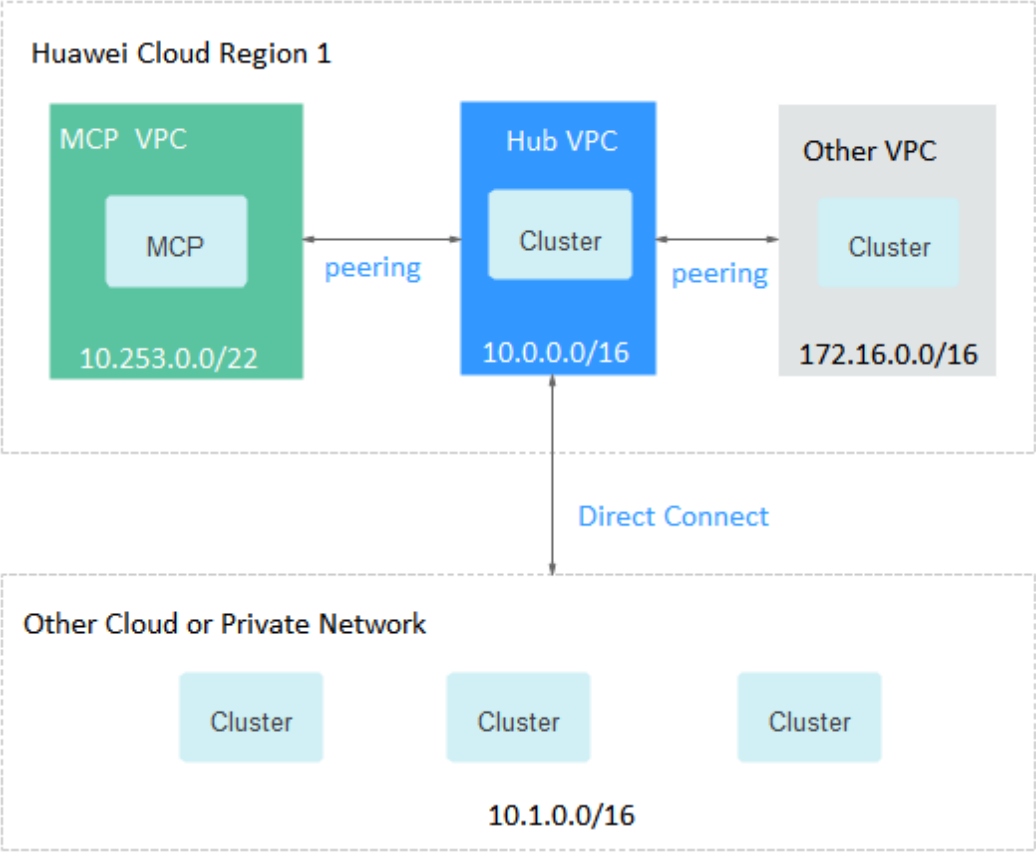
版权所有 © 华为技术有限公司

- 如果集群在其他公有云或私有网络内，那可以通过云专线物理网络打通与枢纽VPC的之间的网络，实现MCP与集群的互相访问。

须知

通过枢纽VPC连接MCP时，MCP网段、枢纽VPC网段以及Kubernetes集群的网段之间不能互相冲突，请在添加集群前确保网段不同，否则无法添加集群。

图 5-1 通过枢纽 VPC 连接 MCP



5.1.2 添加 CCE 集群到 MCP

前提条件

- CCE集群版本号为1.13及以上版本，且集群状态“正常”。
- 保证该集群与MCP网络可连接。

约束与限制

添加CCE集群时不能重复添加同一个CCE集群，即同一个CCE集群不能加入到2个或2个以上的MCP实例中。

版权所有 © 华为技术有限公司

注意

MCP无法识别同一个集群使用不同的连接方式加入MCP实例。例如同时使用公网访问和枢纽私有云接入，或者在公网访问方式时同时使用两种不同的公网IP接入，此类操作均会绕过集群准入校验，导致集群状态异常，请避免此类操作。

操作步骤

步骤1 登录MCP控制台，单击“资源管理”列表，在“集群管理”页面单击“添加集群”。

步骤2 进入添加集群页面，在“选择云服务商”步骤中，单击选择“公有云”下的“华为云”。

步骤3 单击“下一步”，选择集群，设置参数。

- **选择区域**

  默认为当前区域，可以更改，请根据业务需要进行选择。

- **选择集群**

  选择可用的CCE集群。

- **设置集群名称**

  设置集群在MCP中的名称，命名必须全局唯一。

- **选择连接方式**

  支持如下两种方式。

  – 公网访问：MCP通过弹性公网IP访问CCE集群，这要求CCE集群拥有弹性公网IP。

  – 对等链接：MCP通过枢纽私有云访问同一个区域内的CCE集群，当前支持枢纽私有云与CCE集群所在VPC做对等连接方式。枢纽私有云连接说明请参见网络说明。

  说明

  对等连接会自动创建，无需您手动创建。

步骤4 单击“确定”，进入“集群准入校验”页面。准入校验预计需要1分钟。

步骤5 校验通过后，单击“确定”。

添加集群预计需要1分钟。集群添加完成后，在“集群管理”页面中可查看到已添加的集群，且状态为“正常”。

----结束

5.1.3 添加其他公有云集群到 MCP

前提条件

- 存在可用的其他公有云集群，集群版本号为1.13及以上版本，且集群状态“正常”。
- 保证该集群与MCP网络可连接。

约束与限制

添加其他公有云集群时不能重复添加同一个集群，即同一个集群不能添加到2个或2个以上的MCP实例中。

注意

MCP无法识别同一个集群使用不同的连接方式加入MCP实例。例如同时使用公网访问和枢纽私有云接入，或者在公网访问方式时同时使用两种不同的公网IP接入，此类操作均会绕过集群准入校验，导致集群状态异常，请避免此类操作。

操作步骤

步骤1 登录MCP控制台，在左侧导航栏单击“资源管理”列表，选择“集群管理”，单击“添加集群”。

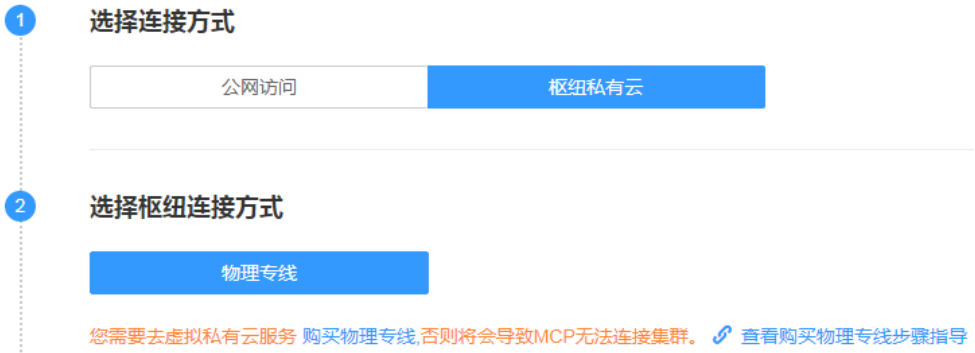
步骤2 进入添加集群页面，选择一个云服务提供商。

步骤3 单击“下一步”，选择连接方式。

支持如下两种方式。

- 公网访问：MCP通过弹性公网IP访问集群，这要求集群拥有公网IP。
- 枢纽私有云：MCP通过**云专线**物理网络打通与枢纽VPC的之间的网络，实现MCP与集群的互相访问。您需要**购买物理专线**，枢纽私有云连接说明请参见**网络说明**。

图 5-2 连接方式



步骤4 上传KubeConfig。

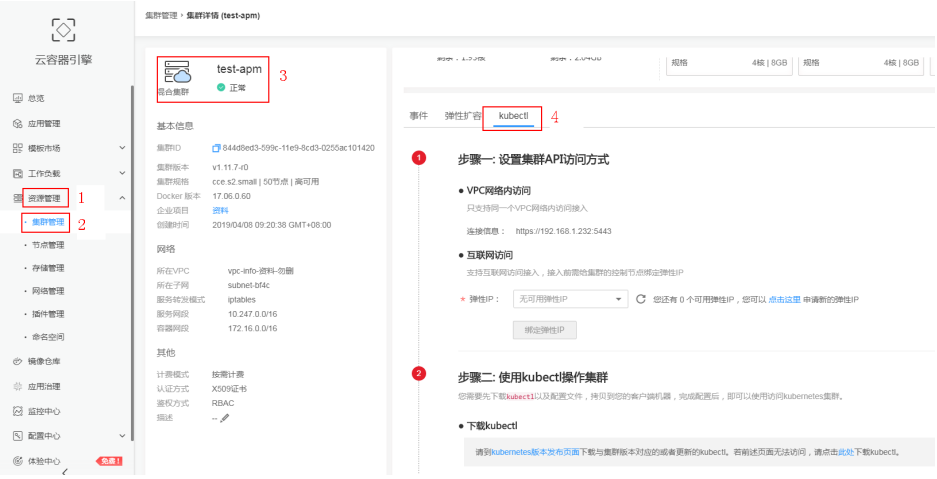
- 获取KubeConfig：对于其他公有云集群不支持直接导出KubeConfig文件或依赖工具解析的场景时，请参考**获取KubeConfig**。
- KUBECONFIG_PATH是存储kubeconfig文件的本地文件路径。如果您使用的是Linux操作系统，在设置了环境变量的情况下，它默认为$KUBECONFIG；否则，默认为$HOME/.kube/config。
- 上传KubeConfig：单击“选择文件”，上传已获取集群的kubeconfig文件，确保此配置文件中的集群网络已连通。文件支持yaml和json的格式。

版权所有 © 华为技术有限公司

说明

集群创建好后生成Kubeconfig文件，获取Kubeconfig文件可以从集群相应位置下载。例如CCE集群的Kubeconfig可在集群管理界面，单击集群名称进入集群详情，kubectl页签中下载。

图 5-3 CCE 证书下载



- 选择Context：选择Context。
- 设置集群名称：添加集群的命名，命名必须全局唯一

步骤5 单击“确定”，进入集群准入校验。

MCP会进行集群准入校验，校验通过后单击“确定”。

步骤6 单击“确定”，添加集群。添加集群预计需要1分钟。

集群添加完成后，在“集群管理”页面中可查看到已添加的集群，且状态为“正常”。

----结束

5.1.4 添加自建 Kubernetes 集群到 MCP

前提条件

- 存在自建Kubernetes集群，集群版本号为1.13及以上版本，且集群状态“正常”。
- 保证该集群与MCP网络可连接。

约束与限制

添加自建Kubernetes集群时不能重复添加同一个集群，即同一个集群不能添加到2个或2个以上的MCP实例中。

版权所有 © 华为技术有限公司

注意

MCP无法识别同一个集群使用不同的连接方式加入MCP实例。例如同时使用公网访问和枢纽私有云接入，或者在公网访问方式时同时使用两种不同的公网IP接入，此类操作均会绕过集群准入校验，导致集群状态异常，请避免此类操作。

操作步骤

步骤1 登录MCP控制台，在左侧导航栏单击“资源管理”列表，选择“集群管理”，单击“添加集群”。

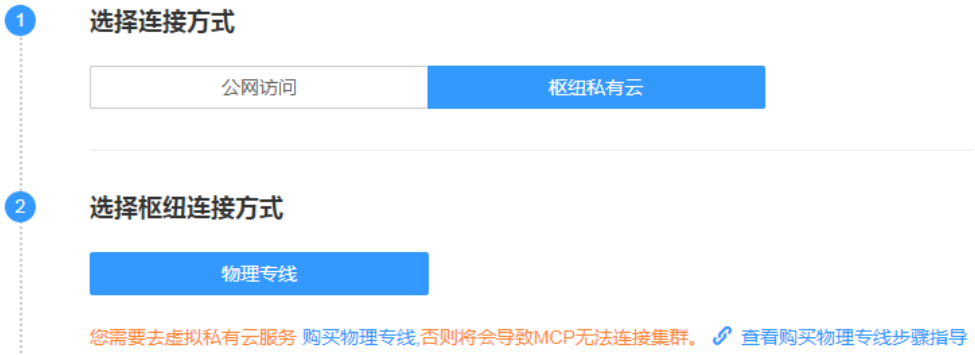
步骤2 进入添加集群页面，在“选择云服务商”步骤中，单击选择“私有云”下的“自建集群”。

步骤3 单击“下一步”，选择连接方式。

支持如下两种方式。

- 公网访问：MCP通过弹性公网IP访问集群，这要求集群拥有公网IP。
- 枢纽私有云：MCP通过**云专线**物理网络打通与枢纽VPC的之间的网络，实现MCP与集群的互相访问。您需要**购买物理专线**，枢纽私有云连接说明请参见**网络说明**。

图 5-4 连接方式



步骤4 上传KubeConfig。

- 获取KubeConfig：集群创建好后生成Kubeconfig文件，获取Kuberconfig文件可以从集群相应位置下载。

  若当前集群不支持直接导出KubeConfig文件或依赖工具解析的场景时，请参考**获取KubeConfig**。
- KUBECONFIG_PATH是存储kubeconfig文件的本地文件路径。如果您使用的是Linux操作系统，在设置了环境变量的情况下，它默认为$KUBECONFIG；否则，默认为$HOME/.kube/config。
- 上传KubeConfig：单击“选择文件”，上传已获取集群的kubeconfig文件，并且该配置文件中网络与控制集群已连通。文件支持yaml和json的格式。
  - 选择Context：选择Context。
  - 设置集群名称：设置集群在MCP中的名称，命名必须全局唯一。

步骤5 单击“确定”，进行集群准入校验。

步骤6 校验通过后单击“确定”，添加集群。

添加集群预计需要1分钟。集群添加完成后，在“集群管理”页面中可查看到已添加的集群，且状态为“正常”。

----结束

5.1.5 获取 KubeConfig

如果您的当前集群不支持直接导出KubeConfig文件，可采用以下方法获取MCP可用的KubeConfig文件。

步骤1 （可选）设置kubectl。

若集群可正常执行kubectl，可跳过本步骤。

```
which kubectl
```

获取kubectl文件的绝对路径**xxx/kubectl**，获取KubeConfig文件路径**yyy/config**。

```
alias kubectl='xxx/kubectl --kubeconfig=yyy/config'
```

步骤2 创建my-user-sa.yaml、my-user-role.yaml、my-user-role-binding.yaml文件。

my-user-role.yaml:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: my-user-role
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - get
```

my-user-role-binding.yaml:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: my-user-role-binding
subjects:
  - kind: ServiceAccount
    name: my-user
    namespace: default
roleRef:
  kind: ClusterRole
  name: my-user-role
  apiGroup: rbac.authorization.k8s.io
```

my-user-sa.yaml:

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: my-user
```

步骤3 在纳管集群上进行操作。

```
kubectl apply -f my-user-sa.yaml
kubectl apply -f my-user-role.yaml
kubectl apply -f my-user-role-binding.yaml
```

步骤4 使用以下命令获取token。

```
kubectl get secret -n default `kubectl get secret -n default | grep my-user | awk '{print $1}'` -oyaml | grep
token: | awk '{print $2}' | base64 -d
```

步骤5 配置KubeConfig文件。

在下面kubeconfig.json中，将“server”参数替换为**步骤1**里“yyy/config”文件中的“server”字段地址，“token”参数替换为**步骤4**中获取的值。

kubeconfig.json:

```
kind: Config
apiVersion: v1
preferences: {}
clusters:
  - name: internalCluster
    cluster:
      server: 'https://119.xxx.xxx.xxx:5443'
      insecure-skip-tls-verify: true
users:
  - name: user
    user:
      token: 'MIIFbAYJKo*****'
contexts:
  - name: internal
    context:
      cluster: internalCluster
      user: user
current-context: internal
```

步骤6 添加集群，使用**步骤5**中配置的KubeConfig文件。成功添加集群后，可以删除**步骤3**中创建的ClusterRole、ClusterRoleBinding以及ServiceAccount。

----结束

5.1.6 使用 kubectl 命令行工具访问 MCP

使用kubectl命令行工具管理具体的MCP，可以操作Deployments等相关资源，也可以作为统一的MCP资源管理工具。

前提条件

互联网访问：您需要准备一台能连接公网的云服务器。

使用 kubectl 命令行工具连接 MCP

步骤1 登录MCP控制台，选择“总览”页面“命令行工具”

步骤2 参照**图5-5**获取MCP访问地址和下载kubectl及其配置文件。

图 5-5 使用 kubectl 命令行工具访问 MCP

步骤3 以Linux环境为例安装和配置kubectl。

1. 拷贝kubectl及其配置文件到您客户机的/home目录下。
2. 登录到您的客户端机器，配置kubectl。
```
cd /home
chmod +x kubectl
mv -f kubectl /usr/local/bin
mkdir -p $HOME/.kube
mv -f kubeconfig.json $HOME/.kube/config
```
3. 根据使用场景，切换kubectl的访问模式。
   - 互联网接入访问请执行
     ```
     kubectl config use-context external
     ```
   - VPC内网接入访问请执行
     ```
     kubectl config use-context internal
     ```
     只有打通了内网连接方式才可以使用，若没有，请使用互联网接入方式。

----结束

使用 kubectl 工具部署工作负载

这边部署的是多集群的工作负载，以下操作以创建nginx工作负载到不同集群为例。

步骤1 参考**使用kubectl命令行工具连接MCP**连接MCP。

步骤2 查询MCP管理的集群。

```
kubectl get clusters
```

步骤3 创建deployment负载。

```
kubectl create deployment nginx --image=nginx
```

步骤4 创建分发策略。

```
cat <<EOF | kubectl apply -f -
apiVersion: policy.karmada.io/v1alpha1
kind: PropagationPolicy
metadata:
  name: nginx-propagation
spec:
  resourceSelectors:
    - apiVersion: apps/v1
      kind: Deployment
      name: nginx
  placement:
    clusterAffinity:
      clusterNames:
        - cluster1    #步骤2查到的集群名
        - cluster2
EOF
```

----结束

5.1.7 其他操作

MCP 升级

MCP新版发布后，您可以升级MCP的组件。

步骤1 登录MCP控制台。

步骤2 将鼠标移至MCP上，单击“升级”。

说明

您还可以在页面右上方单击“升级MCP”。

----结束

移除已添加的集群

移除操作仅是从MCP中移除集群，不会对集群及集群下的计算资源进行删除。

步骤1 登录MCP控制台，在左侧导航栏单击“资源管理”列表，选择“集群管理”。

步骤2 在集群列表中，单击集群后的“移除”，根据页面提示执行移除操作。

----结束

删除已创建的 MCP

删除MCP不会删除MCP下的集群。

步骤1 登录MCP控制台，在左侧导航栏中选择“总览”。

步骤2 在MCP总览页面，单击“更多操作 > 删除MCP”，根据页面提示执行删除操作。

----结束

5.2 网络管理

5.2.1 网络概述

单集群为满足多种复杂场景下工作负载间的互相访问，提供了不同的访问方式，从而满足不同场景提供不同访问通道。在MCP控制台上创建Service、Ingress后，会在所有部署的集群中创建一个同名的Service、Ingress。在集群控制台上对创建的Service、Ingress执行修改或删除操作时，操作提示成功，但最终创建的Service、Ingress会被重建。

- **ClusterIP访问**

  表示工作负载暴露给同一集群内其他工作负载访问的方式，可以通过“集群内部域名”访问。集群内部域名格式为“<自定义的访问方式名称>.<工作负载所在命名空间>.svc.cluster.local”，例如“nginx.default.svc.cluster.local”。

- **NodePort访问**

  表示工作负载可以让同一虚拟私有云内其他工作负载访问，通过“集群节点的IP”访问，主要场景：云上同一虚拟私有云内其他工作负载需要访问Kubernetes集群内部的工作负载。

- **LoadBalancer访问**

  通过弹性负载均衡从公网访问工作负载，一般用于系统中需要暴露到公网的服务。访问方式由公网弹性负载均衡ELB服务地址以及设置的访问端口组成，例如“10.117.117.117:80”。

- **Ingress访问**

  采用了增强型弹性负载均衡，在四层负载均衡访问方式的基础上支持了URI配置，通过对应的URI将访问流量分发到对应的服务。同时，服务根据不同URI实现不同的功能。该访问方式由公网弹性负载均衡ELB服务地址、设置的访问端口组成、定义的URI组成，例如：10.117.117.117:80/helloworld。

5.2.2 ClusterIP 访问

表示工作负载暴露给同一集群内其他工作负载访问的方式，可以通过“集群内部域名”访问。集群内部域名格式为“<自定义的访问方式名称>.<工作负载所在命名空间>.svc.cluster.local”，例如“nginx.default.svc.cluster.local”。

添加方式

您可以在创建无状态工作负载时设置访问方式，也可以在无状态工作负载创建完成后添加访问方式。

- 方式一：创建无状态工作负载时配置，请参见**创建无状态工作负载时创建**。
- 方式二：无状态工作负载创建完成后设置，请参见**无状态工作负载创建完成后设置**。

创建无状态工作负载时创建

步骤1 参考**无状态工作负载（Deployment）**，在“访问设置（Service）”步骤，单击“添加Service”。

- 服务名称：新增服务名称，用户可自定义。
- 访问方式：ClusterIP。
- 协议：请根据业务的协议类型选择。
- 容器端口：容器镜像中应用程序实际监听的端口，需用户确定。例如：nginx程序实际监听的端口为80。
- 访问端口：容器端口映射到集群虚拟IP上的端口，用虚拟IP访问应用时使用，端口范围为1-65535，可任意指定。

步骤2 设置完成后，单击“确定”。

步骤3 单击“下一步”，进行高级设置。

步骤4 单击“下一步”，进行集群差异化配置。设置完成后，单击“确定”。

步骤5 获取访问地址。

1. 单击页面上方的“集群控制台”，进入集群控制台。
2. 在集群控制台，单击“工作负载 > 无状态（Deployment）”，单击所添加工作负载的名称进入详情界面，单击“查看访问方式”，获取访问地址。

步骤6 登录应用所在集群的任意节点，登录方法请参见**登录Linux弹性云服务器**。

步骤7 使用curl命令访问应用，验证应用是否可以正常访问。您可以通过IP或者域名的方式来验证。

说明

只有TCP协议的应用才支持如下验证方式。

- 方式一：通过IP地址验证。

  curl *10.247.84.62:8888*

  其中10.247.84.62:8888为**步骤5**中获取的访问地址。

  回显如下表示应用可正常访问。

```
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

- 方式二：通过域名验证。

  curl *nginx.default.svc.cluster.local:8888*

其中*nginx.default.svc.cluster.local*为**步骤5**中获取的域名访问地址。

回显如下表示应用可正常访问。

```
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

----结束

无状态工作负载创建完成后设置

步骤1 登录MCP控制台，选择左侧导航栏“资源管理”列表的“网络管理”，在“服务（Service）”页签下，单击“添加服务”。

步骤2 设置访问参数。

- 服务名称：自定义服务名称，可与工作负载名称保持一致。
- 命名空间：服务所在命名空间。
- 服务类型：选择“ClusterIP”。
- 关联工作负载：选择关联工作负载。
- 端口配置：
  - 协议：请根据业务的协议类型选择。
  - 容器端口：工作负载程序实际监听的端口，需用户确定。例如：nginx程序实际监听的端口为80。
  - 访问端口：容器端口映射到集群虚拟IP上的端口，用虚拟IP访问工作负载时使用，端口范围为1-65535，可任意指定。
- 部署集群：与所属工作负载的部署集群一致，不可更改。

步骤3 单击“创建”。创建成功后可在“服务（Service）”页签的列表中查看。

----结束

5.2.3 NodePort 访问

表示工作负载可以让同一虚拟私有云内其他工作负载访问，通过“集群节点的IP”访问，主要场景：云上同一虚拟私有云内其他工作负载需要访问Kubernetes集群内部的工作负载。

添加方式

您可以在创建无状态工作负载时设置访问方式，也可以在无状态工作负载创建完成后添加访问方式。

- 方式一：创建无状态工作负载时配置，请参见**创建无状态工作负载时创建**。
- 方式二：无状态工作负载创建完成后设置，请参见**无状态工作负载创建完成后设置**。

创建无状态工作负载时创建

本节以nginx为例进行说明。

步骤1 参考**无状态工作负载（Deployment）**，在“访问设置（Service）”步骤，单击“添加Service”。

- 服务名称：新增服务名称，用户可自定义。
- 访问方式：NodePort。
- 协议：请根据业务的协议类型选择。
- 容器端口：容器镜像中应用实际监听的端口，需用户确定。nginx程序实际监听的端口为80。
- 访问端口：容器端口映射到节点私有IP上的端口，用私有IP访问应用时使用，端口范围为30000-32767，建议选择“自动生成”。
  - 自动生成：系统会自动分配端口号。
  - 指定端口：指定固定的节点端口，默认取值范围为30000-32767。若指定端口时，请确保同个集群内的端口唯一性。

步骤2 设置完成后，单击“确定”。

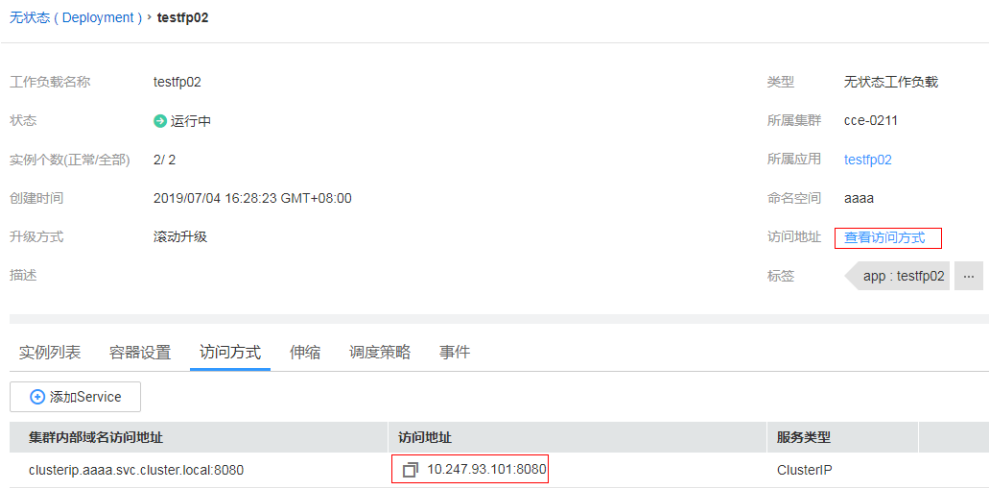
步骤3 单击“下一步”，进行高级设置。

步骤4 单击“下一步”，进行集群差异化配置。设置完成后，单击“确定”。

步骤5 获取访问地址。

1. 单击页面上方的“集群控制台”，进入集群控制台。
2. 在集群控制台，单击“工作负载 > 无状态（Deployment）”，单击所添加工作负载的名称进入详情界面，单击“查看访问方式”，获取访问地址。

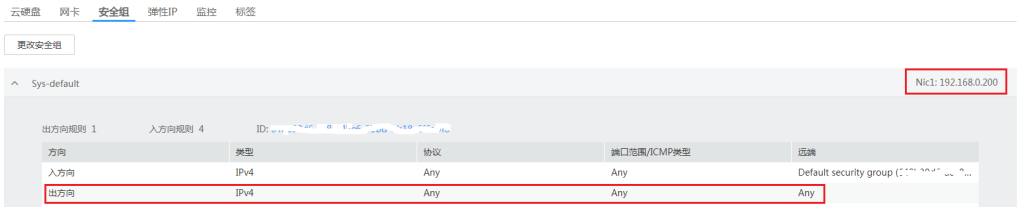
图 5-6 获取节点 IP



步骤6 在华为云控制台首页，单击“计算 > 弹性云服务器”。

步骤7 在弹性云服务器页面，找到同一虚拟私有云内任意一台云服务器，并确认连接到访问地址中IP与端口的安全组是开放的。

图 5-7 确认安全组开放



步骤8 单击“远程登录”，弹出登录页面，输入用户密码登录。

步骤9 使用curl命令访问应用验证应用是否可以正常访问。

说明

NodePort访问方式在集群内也会分配一个集群虚拟IP，即可以在集群内部通过集群虚拟IP的验证方式验证。其中，集群虚拟IP访问端口默认与容器端口一致，例如此示例的访问端口为80端口。

curl *192.168.0.160*:80

其中“192.168.0.160:80”为**步骤5**中获取到的访问地址。

回显如下表示访问成功。

```
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

----结束

无状态工作负载创建完成后设置

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“网络管理”，在“服务（Service）”页签下，单击“添加服务”。

步骤2 设置访问参数。

- 服务名称：自定义服务名称，可与工作负载名称保持一致。
- 命名空间：服务所在命名空间。
- 服务类型：选择“NodePort”。
- 关联工作负载：选择关联工作负载。
- 端口配置：
  - 协议：请根据业务的协议类型选择。
  - 容器端口：工作负载程序实际监听的端口，需用户确定。例如：nginx程序实际监听的端口为80。
  - 容器端口：映射到节点私有IP上的端口，用私有IP访问工作负载时使用，端口范围为30000-32767，建议选择“自动生成”。
    - 自动生成：系统会自动分配端口号。
    - 指定端口：指定固定的节点端口，默认取值范围为30000-32767。若指定端口时，请确保同个集群内的端口唯一性。
- 部署集群：与所属工作负载的部署集群一致，不可更改。

步骤3 单击“创建”。创建成功后可在"服务（Service）"页签的列表中查看。

----结束

5.2.4 LoadBalancer 访问

通过弹性负载均衡从公网访问工作负载，一般用于系统中需要暴露到公网的服务。访问方式由公网弹性负载均衡ELB服务地址以及设置的访问端口组成，例如“10.117.117.117:80”。

前提条件

请确保已有可用的工作负载，若没有请参照**无状态工作负载（Deployment）**先创建工作负载。

添加方式

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“网络管理”，在“服务（Service）”页签下，单击“添加服务”。

步骤2 设置访问参数。

- 服务名称：新增服务的名称，用户可自定义。
- 命名空间：服务所在命名空间。
- 服务类型：选择LoadBalancer。
- 关联工作负载：选择所属工作负载。
- 端口配置：
  - 协议：请根据业务的协议类型选择。
  - 容器端口：工作负载程序实际监听的端口，需用户确定。例如：nginx程序实际监听的端口为80。
  - 访问端口：容器端口映射到负载均衡实例的端口，通过负载均衡对外暴露服务时使用，端口范围为1-65535，可任意指定。

- 域名：输入访问的域名地址。
- 部署集群：与所属工作负载的部署集群一致，不可更改。

步骤3 单击“下一步”，进行差异化配置。支持对每个集群差异化设置增强型负载均衡。

- 华为云：支持使用已有负载均衡实例和自动创建两种方式。选择自动创建时，单击“更改负载均衡实例规格”，可修改待创建增强型负载均衡实例的规格、计费模式和带宽。

图 5-8 LoadBalancer 服务差异化设置-华为云

- 其他云：访问注释支持key/value对格式。以阿里云为例，请您根据自身业务以及厂家要求进行标签配置。

图 5-9 LoadBalancer 服务差异化设置-阿里云

  - 如需创建内部负载均衡器，您需要根据集群的云服务商添加相应的注释，请参考**内部负载均衡器**。

步骤4 单击“创建”。创建成功后可以根据页面提示创建域名访问。通过创建域名访问，可以将LoadBalancer类型的服务对接到云解析DNS服务。

步骤5 获取访问地址。

1. 单击页面上方的“集群控制台”，进入集群控制台。
2. 在集群控制台，单击“工作负载 > 无状态（Deployment）”，单击所添加工作负载的名称进入详情界面，单击“查看访问方式”，获取访问地址。

----结束

5.2.5 Ingress 访问

采用了增强型弹性负载均衡，在四层负载均衡访问方式的基础上支持了URI配置，通过对应的URI将访问流量分发到对应的服务。同时，服务根据不同URI实现不同的功能。该访问方式由公网弹性负载均衡ELB服务地址、设置的访问端口组成、定义的URI组成，例如：10.117.117.117:80/helloworld。

前提条件

请确保已有可用的工作负载，若没有请参照**无状态工作负载（Deployment）**先创建工作负载。

添加方式

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“网络管理”，在“路由（Ingress）”页签下，单击“添加路由”。

步骤2 设置通用配置参数。通用配置指的是对所有部署集群通用性的参数配置。

- 路由名称：新增路由的名称，用户可自定义。
- 命名空间：路由所在命名空间。
- 部署集群：选择需要部署的集群，如果选择CCE集群时，需要先创建NodePort服务，具体可参考**NodePort访问**。

步骤3 单击“下一步”，进入差异化配置，您可以修改需要差异化配置的集群参数。

华为云设置

- 负载均衡：支持使用已有负载均衡实例和自动创建两种方式。
  - 选择已有的负载均衡实例时，请确保此负载均衡实例和所选集群处于相同的虚拟私有云和子网。
  - 选择自动创建时，若待创建负载均衡实例类型为“公网”，可单击“更改负载均衡规格”来修改待负载均衡实例的规格、计费模式和带宽。
- 对外协议：支持HTTP和HTTPS。
- 密钥证书：若对外协议选择HTTPS，请选择密钥证书。
- 对外端口：开放在负载均衡服务地址的端口，可任意指定。
- 域名：输入域名，例如：example.com。
- 路由配置：
  - 路由匹配规则：前缀匹配、精确匹配、正则匹配。
    - 前缀匹配：例如映射URL为/healthz，只要符合此前缀的URL均可访问。例如/healthz/v1，/healthz/v2。
    - 精确匹配：表示精准匹配，只有完全匹配上才能生效。例如映射URL为/healthz，则必须为此URL才能访问。
    - 正则匹配：可设定映射URL规范，例如规范为**/[A-Za-z0-9_.-]+/test**。只要符合此规则的URL均可访问，例如/abcA9/test，/v1-Ab/test。正则匹配规则支持POSIX与Perl两种标准。
  - 映射地址：填写映射地址。
  - 服务名称：选择服务名称。
  - 容器端口：选择容器端口。

其他云设置

- 注释：详细参数请参考对应云服务商的相关资料。
- 对外协议：支持HTTP和HTTPS。
- 密钥证书：若对外协议选择HTTPS，请选择密钥证书。
- 域名：输入域名，例如：example.com。
- 路由配置：
  - 映射地址：填写映射地址。
  - 服务名称：选择服务名称。

- 容器端口：选择容器端口。

步骤4 单击“创建”。创建成功后可在“路由（Ingress）”页签的列表中查看。

步骤5 获取访问地址。

1. 单击页面上方的“集群控制台”，进入集群控制台。
2. 在集群控制台，单击“工作负载 > 无状态（Deployment）”，单击所添加工作负载的名称进入详情界面，单击“查看访问方式”，获取访问地址。

----结束

5.3 存储声明

5.3.1 使用容器存储

使用容器存储时需创建存储声明。存储声明提供容器的持久存储管理能力，提供多云场景的统一的容器存储管理，支持存储按需挂载到容器，保障应用的高可靠。在MCP控制台创建的是存储声明，创建完成后，会在所有部署的集群中创建一个同名的存储声明。在集群控制台上对多集群创建的存储声明执行修改或删除操作时，操作提示成功，但最终创建的存储声明会被重建。

说明

非CCE集群需要具备容器存储功能，请通过下列命令查询对应集群的StorageClass配置及对接的后端存储服务。更多StorageClass相关内容，请参考**存储类**。

```
kubectl get storageclass
```

创建存储声明

步骤1 登录MCP控制台，在左侧导航栏中选择“存储声明”，单击“创建存储声明”。

步骤2 设置通用配置参数。

- 名称：新建存储声明名称，命名必须唯一。
- 命名空间：新建存储声明所属的命名空间。若不选择，默认配置为default。
- 部署集群：选择存储要部署的集群。

图 5-10 选择存储部署集群

步骤3 单击“下一步”，选择创建方式。支持“动态创建”和“标准NFS”两种创建方式。

步骤4 设置集群差异配置。

- 选择“动态创建”创建方式，配置如下参数：

表 5-1 动态创建参数

参数	参数说明
存储来源	当“部署集群”为华为云集群时： – EVS：块存储。MCP支持将EVS创建的云硬盘挂载到容器的某一路径下。当容器迁移时，挂载的云硬盘将一同迁移。这种存储方式适用于需要永久化保存的数据。 – OBS：对象存储。MCP支持创建OBS对象存储卷并挂载到容器的某一路径下，对象存储适用于云工作负载、数据分析、内容分析和热点对象等场景。 – SFS：文件存储。MCP支持创建SFS存储卷并挂载到容器的某一路径下，也可以使用底层SFS服务创建的文件存储卷，SFS存储卷适用于多读多写的持久化存储，适用于多种工作负载场景，包括媒体处理、内容管理、大数据分析和分析工作负载程序等场景。 当“部署集群”为第三方集群时： – 仅支持“第三方存储”。
存储类型	当“存储来源”为“第三方存储”时生效，并且集群支持的存储类型取决于注册集群的实际环境。
存储容量（GB）	新建存储的容量。

版权所有 © 华为技术有限公司

参数	参数说明
访问模式	– 文件存储来源为EVS时，访问模式为ReadWriteOnce (RWO)，即文件存储卷只能以读写模式被单个节点同时加载。 – 文件存储来源为OBS或SFS时，访问模式为ReadWriteMany (RWX)，即文件存储卷能够以读写模式被多个节点同时加载。 – 当部署集群为第三方集群时，访问模式支持ReadWriteOnce (RWO)和ReadWriteMany (RWX)两种模式。
注释	注释以Key/value键值对的形式附加到存储声明对象上。 1. 单击“新增一条注释” 。 2. 输入键、值。

- 选择“标准NFS”创建方式，配置如下参数：

表 5-2 标准 NFS 参数

参数	参数说明
访问模式	访问模式为ReadWriteMany (RWX)，即文件存储卷能够以读写模式被多个节点同时加载。
挂载点地址	填写已有存储服务器地址，格式为：192.168.0.0（ip地址）或www.xx.com(域名)。
挂载点目录	填写已有存储的共享目录，格式为:/dir，必须为绝对路径。

步骤5 单击“创建”创建成功，单击“返回存储声明列表”，查看存储声明状态。

----结束

使用云存储

步骤1 参照**无状态工作负载（Deployment）**，在添加容器后，展开“数据存储”，选择“云存储”页签中，单击“添加云存储”。

步骤2 配置如下参数信息。

表 5-3 挂载文件存储参数配置

参数	参数说明
云存储类型	• 文件存储（NFS） • 其它

参数	参数说明
存储（pvc）名称	选择已创建的存储，若还没有可用存储，可以根据文字和链接指导创建存储声明，您也可以提前创建存储，创建存储步骤请参见创建存储声明。 **须知** ● 选择已有存储时，选择的存储部署集群需与工作负载部署集群相同，否则工作负载实例会调度失败，无法找到存储。 ● 选择的存储必须是实际存在并且可用的，否则工作负载会挂卷失败。
添加容器挂载	1. 子路径：Kubernetes中数据库逻辑卷挂载的subPath，指引用卷内的子路径而不是其根路径。不填写时默认为根路径，目前仅文件存储支持配置子路径。 2. 挂载路径：输入数据库逻辑卷挂载到容器上的路径。可单击“添加容器挂载”添加多个路径。 **须知** – 请不要挂载在系统目录下，如“/”、“/var/run”等，会导致容器异常。建议挂载在空目录下，若目录不为空，请确保目录下无影响容器启动的文件，否则文件会被替换，导致容器启动异常，工作负载创建失败。 – 挂载高危目录的情况下，建议使用低权限帐号启动，否则可能会造成宿主机高危文件被破坏。 3. 设置权限。 – 只读：只能读容器路径中的数据库逻辑卷。 – 读写：可修改容器路径中的数据库逻辑卷，容器迁移时新写入的数据不会随之迁移，会造成数据丢失。

步骤3 单击“确定”。

----结束

相关操作

存储声明创建完成后，您还可以执行表5-4中的操作。

表 5-4 其他操作

操作	说明
删除存储声明	1. 选择需要删除的存储名称，单击操作列的“删除”。也可以批量删除。 2. 根据界面提示完成删除操作。 3. 删除后，部署集群控制台上的存储声明也被删除。
查看YAML	选择需要查看YAML的存储名称，单击操作列的“YAML”。
查看事件	查看存储申明的事件信息。 **说明** 事件保存时间为1小时，1小时后自动清除数据。

5.4 命名空间

命名空间（Namespace）是一种在多个用户（通过资源配额）之间划分集群资源的方法。适用于用户中存在多个团队或项目的环境中。而MCP控制台创建的是多集群命名空间，会在加入MCP实例的所有集群下创建一个同名的命名空间。

须知

- 命名空间可以在集群控制台修改资源配额，并且修改的配额只作用于当前集群，其他集群中的这个命名空间配额不会改变。
- 命名空间在集群控制台被删除后会被重新创建。
- 此章节以下出现的“命名空间”均为“多集群命名空间”。

创建命名空间

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“命名空间”。单击“创建命名空间”。

步骤2 参照表5-5设置命名空间参数。

表 5-5 命名空间基本信息

参数	参数说明
命名空间	新建命名空间的名称，命名必须唯一。
标签	key/value对格式。给命名空间添加标签，定义不同属性，通过这些标签了解各个命名空间的特点
注释	key/value对格式。给命名空间添加注释。
描述	输入对命名空间的描述信息。

步骤3 配置完成后，单击“创建”。

----结束

使用命名空间

在添加Service、Ingress、域名访问、存储声明等都会用到命名空间，以添加Service为例：

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“网络管理”。

步骤2 在“服务（Service）”页签下，单击“添加服务”。

步骤3 在基本信息界面选择服务所在命名空间。

版权所有 © 华为技术有限公司

图 5-11 使用命名空间

----结束

删除命名空间

删除命名空间会删除该命名空间多集群层级相关的所有数据资源，请谨慎操作。

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“命名空间”。

步骤2 在命名空间列表中，选择需要删除的命名空间，单击“删除”。

图 5-12 删除命名空间

根据提示进行删除操作。系统内置的default命名空间不支持删除。

----结束

版权所有 © 华为技术有限公司

5.5 配置中心

5.5.1 配置项（ConfigMap）

配置项允许您将配置文件从容器镜像中解耦，从而增强容器工作负载的可移植性。

配置项价值如下：

- 使用配置项功能可以帮您管理不同环境、不同业务的配置。
- 方便您部署相同工作负载的不同环境，配置文件支持多版本，方便您进行更新和回滚工作负载。
- 方便您快速将您的配置以文件的形式导入到容器中。

而配置项（ConfigMap）是在MCP控制台创建后，会在此MCP中部署的所有集群中创建一个相同名称的配置项。

创建配置项

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“配置中心 > 配置项（ConfigMap）”，单击“创建配置项”。

步骤2 参照表5-6设置新增配置参数。

表 5-6 新建配置参数说明

参数	参数说明
配置项名称	新建的配置项名称，同一个命名空间里命名必须唯一。
命名空间	新建配置项所在的命名空间。若不选择，默认配置为default。
配置数据	工作负载配置的数据可以在容器中使用，或被用来存储配置数据。其中，“键”代表文件名；“值”代表文件中的内容。 1. 单击“添加配置数据”。 2. 输入键、值。
配置标签	标签以Key/value键值对的形式附加到各种对象上（如工作负载、节点、服务等）。 标签定义了这些对象的可识别属性，用来对它们进行管理和选择。 1. 单击“添加标签”。 2. 输入键、值。
描述	配置项的描述信息。
所属集群	使用新建配置项的集群。

版权所有 © 华为技术有限公司

步骤3 配置完成后，单击“创建”。

----结束

使用配置项

配置项创建后，您可以在**无状态工作负载（Deployment）**时将配置项挂载到容器中，然后在容器中挂载路径下就可以读取到配置项的内容。

相关操作

配置项创建完成后，您还可以执行**表5-7**中的操作。

表 5-7 其他操作

操作	说明
YAML	单击配置项名称后的“YAML”，可查看到当前配置项的YAML文件。
更新	1. 单击配置项名称后的“更新”。 2. 根据**表5-6**更改信息。 3. 单击“更新”。
删除	1. 勾选需要删除的配置项。 2. 单击页面左上角的“更多 > 删除”。 3. 单击“确定”。
查看事件	单击配置项名称后的“更多 > 查看事件”，查看配置项的事件信息。 **说明** 事件保存时间为1小时，1小时后自动清除数据。

5.5.2 密钥（Secret）

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资源类型，内容由用户决定。而密钥（Secret）是在MCP控制台创建后，会在此MCP中部署的所有集群中创建一个相同名称的密钥。

创建密钥

步骤1 登录MCP控制台，单击左侧导航栏的“资源管理”列表，选择“配置中心 > 密钥（Secret）”，单击“创建密钥”。

步骤2 参照**表5-8**设置基本信息。

表 5-8 基本信息说明

参数	参数说明
密钥名称	新建的密钥的名称，同一个命名空间内命名必须唯一。

参数	参数说明
命名空间	新建密钥所在的命名空间，默认为default。
所属集群	选择密钥部署集群。
密钥类型	新建的密钥类型。 ● Opaque：一般密钥类型。在高敏感场景下，建议先通过数据加密服务加密敏感数据后，再存入Secret中。 ● kubernetes.io/dockerconfigjson：存放拉取私有仓库镜像所需的认证信息。需要输入镜像仓库地址。 ● IngressTLS：存放7层负载均衡服务所需的证书。 ● 其他：若需要创建其他类型的密钥，请手动输入密钥类型。
密钥数据	工作负载密钥的数据可以在容器中使用。 ● 当密钥为Opaque类型时：输入键、值。其中“值”必须使用Base64编码，单击操作列的“Base64编码”可自动将输入的值转换为Base64编码。Base64编码方法请参见**如何进行Base64编码**。 ● 当密钥为dockerconfigjson类型时：输入私有镜像仓库的帐号和密码。
密钥标签	标签以Key/value键值对的形式附加到各种对象上（如工作负载、节点、服务等）。 标签定义了这些对象的可识别属性，用来对它们进行管理和选择。 1. 单击“添加标签” 。 2. 输入键、值。
描述	新建密钥的描述。

步骤3 配置完成后，单击“创建”。

密钥列表中会出现新创建的密钥。

----结束

使用密钥

密钥创建后，您可以在**无状态工作负载（Deployment）**时将密钥挂载到容器中，然后在容器中挂载路径下就可以读取到密钥的内容。

如何进行 Base64 编码

对字符串进行Base64加密，可以直接使用“echo -n 要编码的内容 | base64”命令即可，示例如下：

```
root@ubuntu:~# echo -n "待编码内容" | base64
******
```

相关操作

密钥创建完成后，您还可以执行表5-9中的操作。

表 5-9 其他操作

操作	说明
YAML	单击密钥名称后的“YAML”，可查看到当前密钥的YAML文件。
更新	1. 单击密钥名称后的“更新”。 2. 根据表5-8更改信息。 3. 单击“更新”。
删除	1. 勾选需要删除的密钥名称。 2. 单击页面左上角的“更多 > 删除”。 3. 单击“确定”。
查看事件	单击密钥名称后的“更多 > 查看事件”，查看密钥的事件信息。 **说明** 事件保存时间为1小时，1小时后自动清除数据。

版权所有 © 华为技术有限公司

6 策略中心

6.1 部署策略

Karmada提供的独立策略API，用来配置资源分发策略。了解更多关于Karmada的信息，请参考**Karmada**。

创建部署策略

步骤1 登录MCP控制台，单击左侧导航栏的“策略中心 > 部署策略”，单击“创建部署策略”。

步骤2 设置部署策略基本信息。

- 部署策略名称：新增部署策略的名称，命名必须唯一。
- 命名空间：选择工作负载所在命名空间。
- 关联资源：单击关联资源，在资源类型中选择关联资源的类型。若为CRD资源，可以在自定义中配置CRD的kind、apiversion和name。
- 选择资源：选择需要关联的资源。

  说明

  需要先在karmada创建资源模板，关联资源才可以选择到。

- 部署集群：表示关联资源可以被调度到的集群，若不设置，任何集群都可以被调度。
- 选择供应商：表示关联资源可以被调度到的供应商，若不设置，任何供应商的集群都可以被调度。
- 选择region：表示关联资源可以被调度到的region，若不设置，任何region的集群都可以被调度。
- 标签设置：表示关联资源可以被调度到的集群需要有的标签，若不设置，调度资源时不考虑标签。
- 污点设置：表示关联资源对集群污点容忍，若不设置，调度时不考虑集群污点。

  说明

  集群污点可以在集群控制台的“集群总览”->“污点管理”中设置。

版权所有 © 华为技术有限公司

Karmada会根据部署集群、供应商、region、标签设置和污点设置综合计算出关联资源可以调度到的集群。

步骤3 设置完成后，单击“创建”。

步骤4 查看调度结果。

1.进入“策略中心”->“部署策略”，单击所添加的部署策略的名称进入详情界面。

2.在集群分布中可以查看关联资源被调度到的集群。

步骤5 单击“集群控制台”，进入被调度集群的控制台，可以查看到关联资源已被调度集群上。

说明

当多个部署策略关联相同的资源时，仅会有一个部署策略生效，策略名称字典序最后的策略生效。不建议多个部署策略关联同一个资源。

----结束

更新部署策略

步骤1 登录MCP控制台，单击左侧导航栏的“策略中心 > 部署策略”。

步骤2 在列表中选择需要更新的部署策略，单击“操作”栏中的“更新”按钮。

步骤3 更新部署策略的标签及污点信息。

- 标签设置：表示关联资源可以被调度到的集群需要有的标签，若不设置，调度资源时不考虑标签。
- 污点设置：表示关联资源对集群污点容忍，若不设置，调度时不考虑集群污点。

步骤4 设置完成后，单击“更新”，可查看到更新策略成功。

----结束

6.2 差异化策略

Karmada提供独立的差异化策略API，用来配置与集群相关的差异化配置。了解更多关于Karmada的信息，请参考**Karmada**。

创建差异化策略

步骤1 登录MCP控制台，单击左侧导航栏的“策略中心 > 差异化策略”，单击“YAML创建”。

步骤2 编辑YAML参数，示例如下：

```
apiVersion: policy.karmada.io/v1alpha1
kind: OverridePolicy
metadata:
  name: nginx-ccecluster-deployment
  namespace: default
spec:
  overriders:
    plaintext:
      - operator: replace
        path: /spec/replicas
        value: 2
      - operator: add
```

```
      path: /spec/template/spec/containers
      value:
        - image: 'nginx:perl'
          imagePullPolicy: IfNotPresent
          name: container-0
          resources:
            limits:
              cpu: 250m
              memory: 512Mi
            requests:
              cpu: 250m
              memory: 512Mi
resourceSelectors:
  - apiVersion: apps/v1
    kind: Deployment
    name: nginx
    namespace: default
targetCluster:
  clusterNames:
    - ccecluster
```

表 6-1 差异化策略参数说明

参数	参数类型	描述
apiVersion	String	API版本，固定值“policy.karmada.io/v1alpha1”，该值不可修改。
kind	String	API类型，固定值“OverridePolicy”，该值不可修改。
metadata	**metadata** object	差异化策略的基本信息，为集合类的元素类型，包含一组由不同名称定义的属性。
spec	**spec** object	差异化策略相关属性详细信息，通过spec的描述来创建或更新对象。

表 6-2 metadata

参数	参数类型	描述
name	String	差异化策略名称，命名必须唯一，需以小写字母开头，由小写字母、数字、中划线(-)组成，长度范围1-56位，且不能以中划线(-)结尾。
namespace	String	差异化策略所在命名空间。

表 6-3 spec

参数	参数类型	描述
overriders	**overriders** object	差异化策略内容。
resourceSelectors	**resourceSelectors** object	选择关联的资源，差异化策略将对符合筛选条件的资源生效。

参数	参数类型	描述
targetCluster	**targetCluster** object	选择差异化策略生效的集群。

表 6-4 overriders

参数	参数类型	描述
plaintext	Array of **plaintext** object	差异化策略的内容，可添加多个策略。

表 6-5 plaintext

参数	参数类型	描述
operator	String	对目标资源进行差异化操作，表示对资源操作路径下的内容进行增、删、改操作。 ● add：在目标资源模板上增加一个字段，字段由操作路径指定。 ● remove：在目标资源模板上删除一个字段，字段由操作路径指定。 ● replace：在目标资源模板上更新一个字段，字段由操作路径指定。 例如下面的示例中，replace操作将目标资源YAML中的/spec/replicas参数修改为2，即实例数修改为2。 - operator: replace path: /spec/replicas value: 2
path	String	操作路径，用于指定目标资源YAML中的差异化位置。 例如，填写“/spec/replicas” 时，表示对目标资源配置中的/spec/replicas字段进行操作。
value	目标资源参数类型	在指定操作路径下，进行增、删、改的内容。 ● operator字段为add：value值为目标资源路径下新增的内容。 ● operator字段为remove：value值可为任意值，删除时无意义。 ● operator字段为replace：value值为目标资源路径下进行替换的新内容。

版权所有 © 华为技术有限公司

表 6-6 resourceSelectors

参数	参数类型	描述
apiVersion	String	目标资源的API版本。
kind	String	目标资源的API类型。
name	String	目标资源的名称。
namespace	String	目标资源所处的的命名空间。

表 6-7 targetCluster

参数	参数类型	描述
clusterNames	Array of strings	差异化策略生效的集群名。

步骤3 YAML内容编辑完成后，单击“创建”。

步骤4 单击“集群控制台”，进入差异化集群的控制台，可以查看到关联资源差异化的结果。

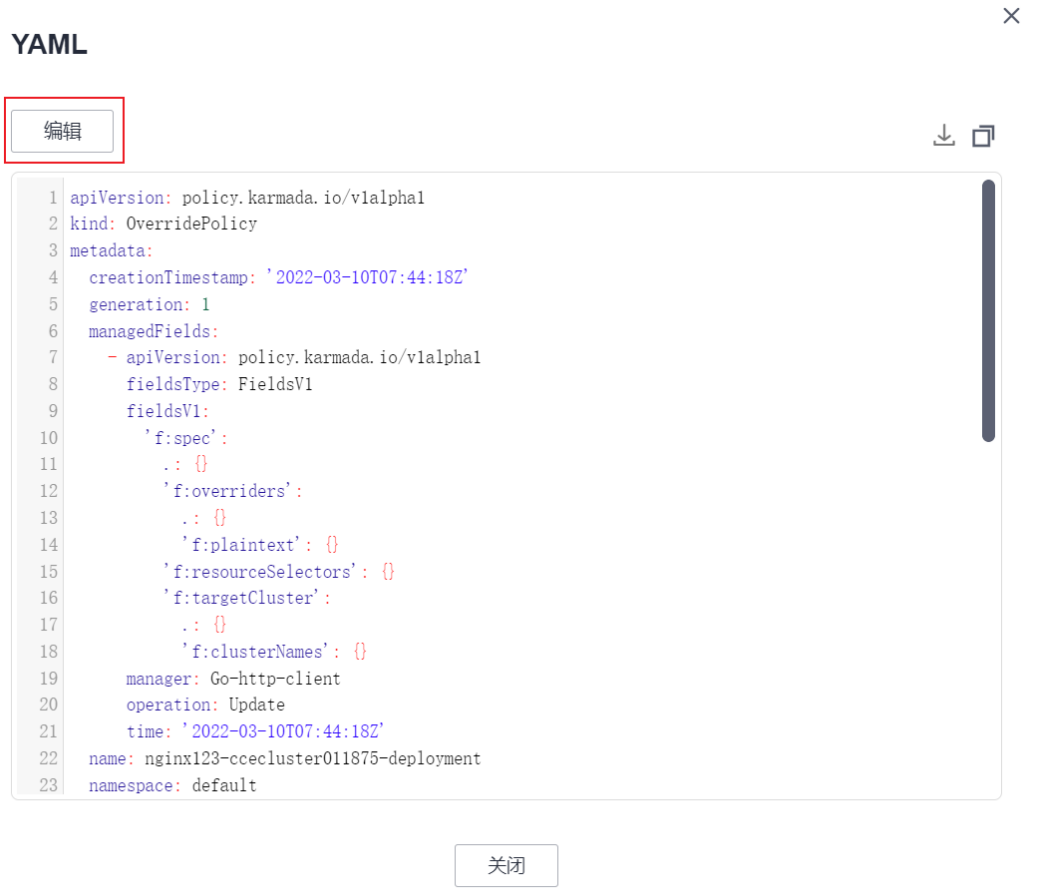
----结束

修改差异化策略

步骤1 登录MCP控制台，单击左侧导航栏的“策略中心 > 差异化策略”。

步骤2 在列表中选择需要更新的差异化策略，单击“操作”栏中的“YAML”按钮。

步骤3 单击弹出窗口中的“编辑”按钮，修改YAML内容。



步骤4 YAML内容修改完成后，单击“更新”。

步骤5 单击“集群控制台”，进入差异化集群的控制台，可以查看到关联资源差异化的结果。

----结束

6.3 域名访问

在多个集群中部署的应用可以通过公网域名实现统一的访问。您可以配置您的公网域名，MCP服务会以此域名作为根域名生成一个完整的应用外部访问域名。您可以通过发布域名访问，将服务，路由自动对接到华为云的云解析DNS服务，以提供多云场景下应用的统一对外访问路径。同时域名访问提供了自定义权重配比等能力，可以根据您的需求控制外部流量的流向比例。

配置域名

步骤1 公网域名解析。

- 若您尚未创建公网域名解析，请**创建公网域名解析**。
- 若您已经创建，请执行**步骤2**。

步骤2 配置域名。

选择已完成以上步骤的域名，单击“配置域名”。

----结束

创建域名访问

根据创建无状态工作负载完成的提示页面，您可以单击“添加服务”，添加LoadBalancer类型的服务，使应用工作负载可以对外提供服务。在LoadBalancer类型的服务创建完成的提示页面中单击“创建域名访问”。

步骤1 登录MCP控制台，在左侧导航栏选择“域名访问”，单击“创建域名访问”。

步骤2 设置“关联服务”参数。

- 命名空间：选择命名空间。
- 目标服务：选择目标服务，若您还没有可以关联的LoadBalancer类型的服务，请先创建服务。详细创建服务步骤见**LoadBalancer访问**。

步骤3 单击“下一步”，配置访问模式。

- 主备模式：流量只会解析到您所选择的主集群中，可以通过修改流量配比功能，修改主备集群。若开启域名流量解析自动切换，主集群发生故障时，DNS流量解析会随机自动切换至备集群。
- 自适应模式：流量解析根据各集群后端实例数量自动分配权重。并且可以配置地域亲和，设置特定区域的用户流量访问特定的集群。
- 自定义模式：您可以自定义配置域名解析到每个集群的权重。并且可以配置地域亲和，设置特定区域的用户流量访问特定的集群。

步骤4 单击“创建”完成域名访问任务创建，完成该任务需要一段时间，请耐心等待。可单击“返回域名访问列表”或“查看域名访问详情”查看创建的域名访问。

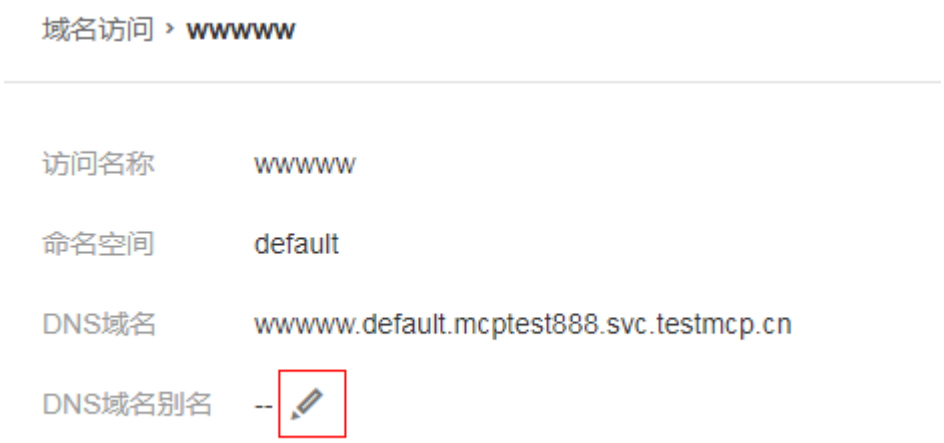
----结束

修改别名

步骤1 登录MCP控制台，选择“域名访问”，单击访问名称，进入域名访问详情界面。

步骤2 单击 填写别名，填写完成后单击 。

图 6-1 修改别名



----结束

修改流量比例

步骤1 登录MCP控制台，选择“域名访问”，单击访问名称，进入域名访问详情界面。

步骤2 在“拓扑图”页签下，单击“修改流量配比”。

步骤3 修改完成后，单击“确定”。

图 6-2 修改流量比例

----结束

查看域名访问地址

域名访问创建完成后，可以在域名访问列表中，查看域名访问地址。

步骤1 登录MCP控制台，选择“域名访问”。

版权所有 © 华为技术有限公司

步骤2 在域名访问列表中“域名地址”即为域名访问地址。

----结束

删除域名访问

步骤1 登录MCP控制台，选择“域名访问”。

步骤2 在右侧域名访问列表最右侧“操作”一列，单击“删除”。

步骤3 在“删除域名访问”页面中单击“是”完成删除操作。

----结束

7 监控中心

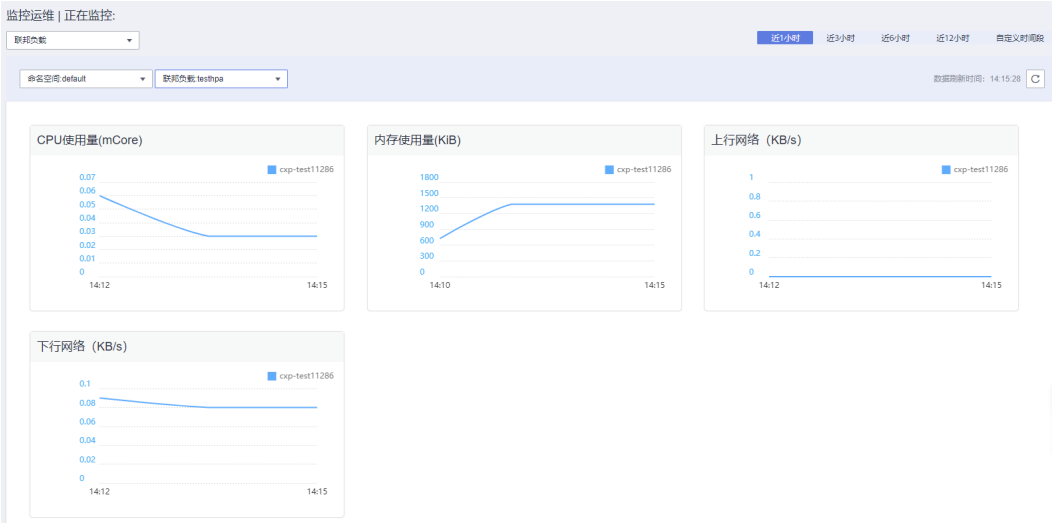
7.1 监控运维

- 当安装Prometheus且接入管理页面，则可以查看所有的监控信息；
- 当只对接Metrics Server，则监控运维只有“节点”项可以查看CPU使用率和内存使用率的监控信息；
- 当未对接Metrics Server，则监控运维页面无监控信息。

7.1.1 负载

步骤1 登录MCP控制台，单击左侧导航栏的“监控中心 > 监控运维”，在“监控运维 | 正在监控:”下拉框选择“负载”。

步骤2 选择负载所在的命名空间以及名称，可以查看负载的CPU使用量、内存使用量、上行网络、下行网络等监控信息。



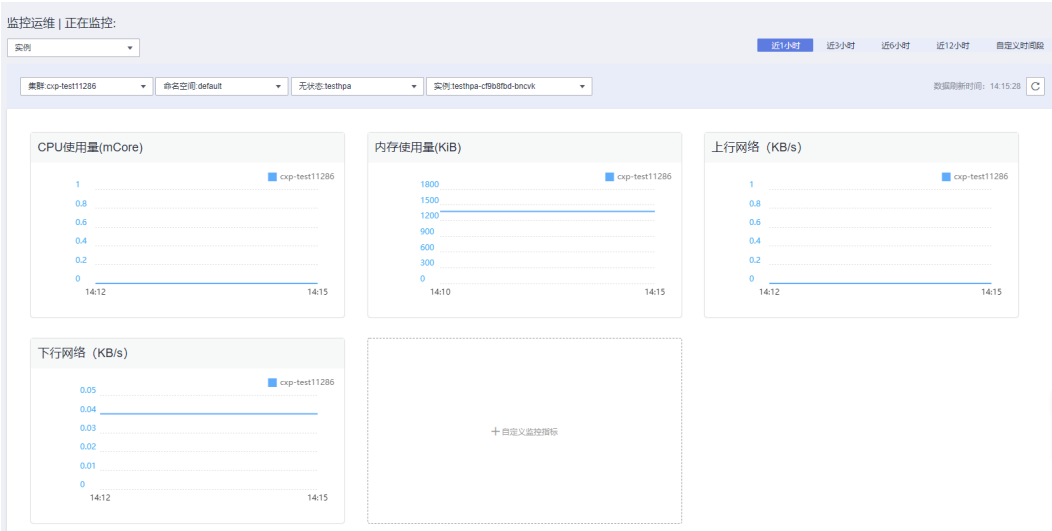
----结束

版权所有 © 华为技术有限公司

7.1.2 实例

步骤1 登录MCP控制台，单击左侧导航栏的“监控中心 > 监控运维”，在“监控运维 | 正在监控:”下拉框选择“实例”。

步骤2 选择实例所在的集群、命名空间、负载名称以及实例名称，可以查看实例的CPU使用量、内存使用量、上行网络、下行网络等监控信息。



步骤3 如果需要新增自定义监控指标，可以单击“自定义监控指标”增加自定义指标。

步骤4 选择指标名称和标签名称，单击“确认”增加自定义指标。

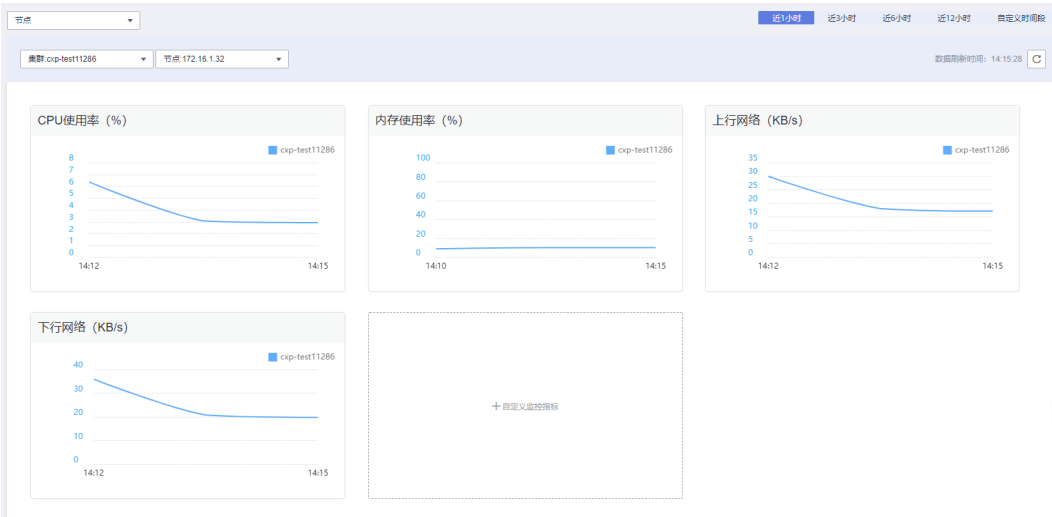
返回监控运维页面会出现新增的监控指标信息。

----结束

7.1.3 节点

步骤1 登录MCP控制台，单击左侧导航栏的“监控中心 > 监控运维”，在“监控运维 | 正在监控:”下拉框选择“节点”。

步骤2 选择集群以及节点，可以查看节点的CPU使用率、内存使用率、上行网络、下行网络等监控信息。



版权所有 © 华为技术有限公司

步骤3 如果需要新增自定义监控指标，可以单击“自定义监控指标”增加自定义指标。

步骤4 选择指标名称和标签名称，单击“确认”增加自定义指标。

返回监控运维页面会出现新增的监控指标信息。

----结束

7.2 接入管理

在MCP上您可以监控添加的Kubernetes集群，查看节点、负载和实例三个维度的监控信息，方便您统一运维。

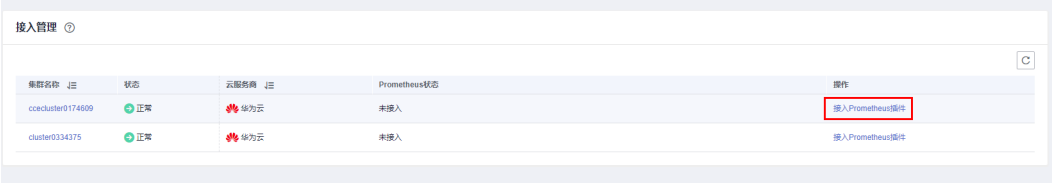
您需要在Kubernetes集群安装Metric Server和Prometheus，这样才能将监控数据上报到MCP。具体安装方法请参见：

- **Metrics Server安装**
- **Prometheus安装**

Prometheus安装完成后，您需要在MCP上操作接入。

步骤1 登录MCP控制台，单击左侧导航栏的“监控中心 > 接入管理”，在“操作”一列单击“接入Prometheus插件”。

图 7-1 接入管理



步骤2 在弹出的窗口中选择Prometheus所在命名空间、服务名称以及端口。

图 7-2 接入 Prometheus 插件

版权所有 © 华为技术有限公司

接入完成后，单击左侧导航栏的“监控中心 > 监控运维”，您就可以看到kubernetes集群的监控信息，可以查看节点、负载和实例三个维度的监控信息。

----结束

7.3 Metrics Server 安装

跨集群HPA基于社区Metric API，获取集群中资源使用情况。使用跨集群HPA前提是集群安装了Metrics Server，Metrics Server通过kubelet summary API获取数据，实现Metrics API。 Metrics API只可以查询当前数据，不提供历史数据。

前提条件

- 集群版本必须大于1.13。
- 安装Metrics Server的虚拟机必须可以连接互联网，并且能用Kubectl操作集群。

Metric Server 安装

步骤1 需要安装Metrics Server的虚拟机开启API聚合层。需要在kube-APIServer中添加启动参数，增加以下配置，开启API聚合层。

说明

CCE 1.11版本集群需要提交工单开启API聚合层，CCE 1.13之后的版本默认开启了API聚合层。

```
--requestheader-client-ca-file=
--proxy-client-cert-file=
--proxy-client-key-file=
--requestheader-allowed-names=aggregator
--requestheader-extra-headers-prefix=X-Remote-Extra-
--requestheader-group-headers=X-Remote-Group
--requestheader-username-headers=X-Remote-User
```

参数说明：

- --requestheader-client-ca-file：根证书绑定包用于在信任--requestheader-username-headers指定的标头中的用户名前，在传入请求上验证客户证书。
- --proxy-client-cert-file：用于证明aggregator或kube-apiserver在请求期间发出呼叫的身份的客户端证书。
- --proxy-client-key-file：用于证明聚合器或kube-apiserver的身份的客户端证书的私钥，当它必须在请求期间调用时使用。包括将请求代理给用户api-server和调用webhook admission插件。
- --requestheader-allowed-names：客户端证书常用名称列表，允许在--requestheader-username-headers指定的标头中提供用户名，如果为空，则允许在--requestheader-client-ca-file文件中通过当局验证的任何客户端证书。
- --requestheader-extra-headers-prefix：要检查的请求标头前缀列表。
- --requestheader-group-headers：要检查组的请求标头列表。
- --requestheader-username-headers：要检查用户名的请求标头列表。

如果Master上没有运行kube-proxy，还需要配置

```
--enable-aggregator-routing=true
```

步骤2 部署metrics server。

```
wget https://github.com/kubernetes-incubator/metrics-server/archive/v0.3.2.tar.gz
tar zxvf v0.3.2.tar.gz
```

```
cd metrics-server-0.3.2
kubectl create -f deploy/1.8+/
```

步骤3 查看pod是否安装成功，保证pod启动。

```
kubectl get pods -nkube-system| grep metric
```

步骤4 如果步骤3中pod未启动，可以执行

```
kubectl logs {pod-name} -nkube-system
```

查询日志，若日志中出现如图7-3报错，可以执行

```
kubectl edit deployment metrics-server -nkube-system
```

添加启动参数“--kubelet-insecure-tls”如图7-4，或者配置正确的证书（需要用户提供k8s集群的CA证书，配置给metrics-server）。

图 7-3 报错日志

```
[root@node1 ~]# kubectl logs metrics-server-7599c4b94f-wnf8q -nkube-system
E0418 06:40:13.651364       1 serving.go:273] Generated self-signed cert (apiserver.local.config/certificates/apiserver.crt, apiserver.local.config/certificates/apiserver.ke
y)
[restful] 2019/04/18 06:40:14 log.go:33: [restful/swagger] listing is available at https://:443/swaggerapi
[restful] 2019/04/18 06:40:14 log.go:33: [restful/swagger] https://:443/swaggerui/ is mapped to folder /swagger-ui/
E0418 06:40:14.429730       1 serve.go:96] Serving securely on [::]:443
E0418 06:41:14.408818       1 manager.go:102] unable to fully collect metrics: unable to fully scrape metrics from source kubelet_summary:192.168.60.240: unable to fetch met
rics from Kubelet 192.168.60.240 (192.168.60.240): Get https://192.168.60.240:10250/stats/summary/: x509: certificate signed by unknown authority (possibly because of "x509:
 invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "192.168.60.240@1554990916")
E0418 06:41:53.644937       1 reststorage.go:129] unable to fetch node metrics for node "192.168.60.240": no metrics known for node
E0418 06:42:02.534423       1 reststorage.go:129] unable to fetch node metrics for node "192.168.60.240": no metrics known for node
E0418 06:42:05.586991       1 reststorage.go:129] unable to fetch node metrics for node "192.168.60.240": no metrics known for node
E0418 06:42:14.404471       1 manager.go:102] unable to fully collect metrics: unable to fully scrape metrics from source kubelet_summary:192.168.60.240: unable to fetch met
rics from Kubelet 192.168.60.240 (192.168.60.240): Get https://192.168.60.240:10250/stats/summary/: x509: certificate signed by unknown authority (possibly because of "x509:
 invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "192.168.60.240@1554990916")
E0418 06:43:14.402756       1 manager.go:102] unable to fully collect metrics: unable to fully scrape metrics from source kubelet_summary:192.168.60.240: unable to fetch met
rics from Kubelet 192.168.60.240 (192.168.60.240): Get https://192.168.60.240:10250/stats/summary/: x509: certificate signed by unknown authority (possibly because of "x509:
 invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "192.168.60.240@1554990916")
E0418 06:44:14.407790       1 manager.go:102] unable to fully collect metrics: unable to fully scrape metrics from source kubelet_summary:192.168.60.240: unable to fetch met
rics from Kubelet 192.168.60.240 (192.168.60.240): Get https://192.168.60.240:10250/stats/summary/: x509: certificate signed by unknown authority (possibly because of "x509:
 invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "192.168.60.240@1554990916")
E0418 06:45:14.402696       1 manager.go:102] unable to fully collect metrics: unable to fully scrape metrics from source kubelet_summary:192.168.60.240: unable to fetch met
rics from Kubelet 192.168.60.240 (192.168.60.240): Get https://192.168.60.240:10250/stats/summary/: x509: certificate signed by unknown authority (possibly because of "x509:
 invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "192.168.60.240@1554990916")
```

图 7-4 添加启动参数

```
      name: metrics-server
    spec:
      containers:
      - args:
        - --kubelet-insecure-tls
        image: k8s.gcr.io/metrics-server-amd64:v0.3.1
        imagePullPolicy: IfNotPresent
        name: metrics-server
        resources: {}
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
        volumeMounts:
        - mountPath: /tmp
          name: tmp-dir
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      serviceAccount: metrics-server
      serviceAccountName: metrics-server
      terminationGracePeriodSeconds: 30
      volumes:
      - emptyDir: {}
        name: tmp-dir
status:
  availableReplicas: 1
  conditions:
```

步骤5 查看是否正确取到数据。

```
kubectl get --raw /apis/metrics.k8s.io/v1beta1/nodes
```

有返回值则说明安装成功。

----结束

7.4 Prometheus 安装

Prometheus是一个用于事件监控和告警的开源软件。

MCP支持使用Prometheus上报Kubernetes集群的监控数据到监控中心，使用此功能您需要在Kubernetes集群中安装Prometheus。

操作步骤

使用Kubernetes charts仓库中prometheus的Chart包进行安装。Chart包中主要包含以下几个组件，可以通过开关控制是否部署，默认为全部部署。本示例中通过配置安装参数，进行自定义部署。

- alertmanager：插件的告警中心，主要用于接收Prometheus发送的告警并通过去重、分组、分发等能力管理告警信息。
- kube-state-metrics：将Prometheus的metrics数据格式转换成K8s API接口能识别的格式。
- node-exporter：每个节点上均有部署，收集Node级别的监控数据。
- pushgateway：用于接收指标的中间组件，Prometheus服务器从上面拉取数据。
- prometheus server：用于监控的数据采集服务器。

Chart包详细介绍可以通过**https://github.com/prometheus-community/helm-charts/tree/main/charts/prometheus**查看。

步骤1 通过kubectl连接集群。

步骤2 安装helm3。

```
wget https://get.helm.sh/helm-v3.6.1-linux-amd64.tar.gz
```

解压文件，将helm二进制放置到/usr/local/bin目录下。

```
tar zxvf helm-v3.6.1-linux-amd64.tar.gz
mv linux-amd64/helm /usr/local/bin/helm
```

步骤3 添加helm镜像仓库。

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm repo update
```

添加成功后，可使用**helm repo list**命令查看：

```
NAME                    URL
prometheus-community    https://prometheus-community.github.io/helm-charts
```

步骤4 创建value.yaml，配置安装参数。

```
vi value.yaml
```

文件内容可参考如下示例配置。

```
pushgateway:
  enabled: false                          # 不安装pushgateway
alertmanager:
  persistentVolume:
    existingClaim: pvc-name                   # PVC需提前创建
server:                                   # Prometheus server的配置
  persistentVolume:                           # 本地持久化存储
    existingClaim: pvc-name
  global:
    external_labels:
```

配置说明：

- pushgateway：一般来说pushgateway不需要部署，可以通过设置pushgateway.enabled: false跳过部署。
- alertermanager：默认使用deployment部署。
  - persistentVolume.existingClaim：使用集群中已经存在的PVC名称，通过持久化存储保存本地数据。

    如果不需要持久化存储可以使用empty-dir来存储数据，则上述文件中的该字段可设置如下：

    ```
    alertmanager:
      persistentVolume:
        enabled: false
    ```
- server：默认使用deployment部署。
  - persistentVolume.existingClaim：使用集群中已经存在的PVC名称，通过持久化存储保存本地数据，一般默认保留15天的数据。

    如果不需要持久化存储可以使用empty-dir来存储数据，则上述文件中的该字段可设置如下：

    ```
    server:
      persistentVolume:
        enabled: false
    ```

步骤5 执行如下命令安装Prometheus。

```
helm install prometheus prometheus-community/prometheus --namespace monitoring --values value.yaml
```

- --namespace：指定Prometheus安装的命名空间，需要提前手动创建。
- --values：指定**步骤4**中Prometheus的安装参数。

```
[root@[illegible] ]# helm install prometheus prometheus-community/prometheus --namespace monitoring --values value.yaml
WARNING: Kubernetes configuration file is group-readable. This is insecure. Location: /root/.kube/config
WARNING: Kubernetes configuration file is world-readable. This is insecure. Location: /root/.kube/config

NAME: prometheus
LAST DEPLOYED: Tue Aug 16 12:03:02 2022
NAMESPACE: monitoring
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
The Prometheus server can be accessed via port 80 on the following DNS name from within your cluster:
prometheus-server.monitoring.svc.cluster.local


Get the Prometheus server URL by running these commands in the same shell:
  export POD_NAME=$(kubectl get pods --namespace monitoring -l "app=prometheus,component=server" -o jsonpath="{.items[0].metadata.name}")
  kubectl --namespace monitoring port-forward $POD_NAME 9090


The Prometheus alertmanager can be accessed via port 80 on the following DNS name from within your cluster:
prometheus-alertmanager.monitoring.svc.cluster.local
```

----结束

7.5 Prometheus-Adapter 安装

使用自定义指标的HPA，需要提供社区标准的Custom Metric API，当前大部分用户使用Prometheus-Adapter来提供Custom Metric API，其主要功能是将接受到custom metric api转换成普罗的请求，从普罗中查询数据返回给API Server，具体的代码仓库地址是**https://github.com/DirectXMan12/k8s-prometheus-adapter**。

前提条件

确保集群中API聚合层已打开，具体操作请参考**配置聚合层**。

安装步骤

使用kubernetes charts仓库中prometheus-adapter的chart包进行安装，Chart包详细介绍可以从**https://github.com/prometheus-community/helm-charts/tree/main/charts/prometheus-adapter**查看。

步骤1 通过kubectl连接集群。

步骤2 安装helm3。

```
wget https://storage.googleapis.com/kubernetes-helm/helm-v3.6.1-linux-amd64.tar.gz --no-check-certificate
```

解压文件，将helm二进制放置到/usr/local/bin目录下。

```
tar zxvf helm-v3.6.1-linux-amd64.tar.gz
mv linux-amd64/helm /usr/local/bin/helm
```

步骤3 添加helm镜像仓库。

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm repo update
```

添加成功后，可使用**helm repo list**命令查看：

```
NAME                    URL
prometheus-community    https://prometheus-community.github.io/helm-charts
```

步骤4 确认配置的参数，写入到value.yaml中。

- adapter连接的prometheus的信息，主要是url和端口，默认值是http://prometheus.default.svc，端口是9090，请根据实际的prometheus server设置。如果按照**Prometheus安装**安装的prometheus，则请使用如下推荐配置。

  创建value.yaml，配置安装参数。

  ```
  vi value.yaml
  ```

  ```
  prometheus:
    url: http://prometheus-server.monitoring.svc
    port: 80
    path: ""
  ```

- 自定义规则配置，主要是配置指标的发现规则，指标与kubernetes资源的对应关系，在api中指标的暴露的名称以及对应的prometheus查询的语句，详细的配置可以查看**https://github.com/DirectXMan12/k8s-prometheus-adapter/blob/master/docs/config.md**。

步骤5 执行如下命令安装Prometheus-Adapter：

```
helm install prometheus-adapter prometheus-community/prometheus-adapter --values value.yaml --
namespace monitoring
```

- --namespace：指定Prometheus-Adapter安装的命名空间，需要提前手动创建。
- --values：指定**步骤4**中Prometheus-Adapter的安装参数。

安装成功后，可以通过下面命令查询所有的自定义指标。

```
kubectl get --raw "/apis/custom.metrics.k8s.io/v1beta1"
```

----结束

8 镜像仓库

镜像仓库是由容器镜像服务（Software Repository for Container）提供的用于存储、管理容器镜像的场所，可以让使用人员轻松存储、管理、部署容器镜像。

- 若您使用华为云的镜像，可以先上传镜像，上传镜像的详细操作请参见通过客户端上传镜像。
- 若您使用第三方镜像，可以在创建无状态工作负载的“集群差异配置”步骤中使用。详细操作参见使用第三方镜像。

使用华为云镜像

在MCP中可以给添加的集群（包括其他云集群）使用华为云镜像。镜像上传成功后，在创建无状态工作负载时可选择“我的镜像”，以2048游戏为例，具体操作如下：

步骤1 登录MCP控制台，在左侧导航栏中单击“工作负载 > 无状态Deployment”，在右侧页面中单击“创建无状态工作负载”

步骤2 输入以下参数，其它保持默认。

- 工作负载名称：game。
- 部署集群：选择应用所要运行的集群。

步骤3 单击“下一步”，添加容器。

单击“添加容器”，在“我的镜像”页签中，选择已上传的镜像，单击“确定”。

说明

若部署的集群有多个，在添加容器时，差异化配置界面，可以对不同的集群进行差异化配置，也可以单独对某个集群更换镜像。

步骤4 更多创建无状态工作负载的步骤请参见无状态工作负载（Deployment）。

----结束

使用第三方镜像

在MCP中可以给添加的集群（包括华为云集群）使用第三方的镜像，在创建无状态工作负载时“集群差异配置”步骤中，勾选“容器设置”的“差异配置”。以2048游戏为例，具体操作如下：

版权所有 © 华为技术有限公司

步骤1 登录MCP控制台，在左侧导航栏中单击“工作负载 > 无状态Deployment”，在右侧页面中单击“创建无状态工作负载”

步骤2 输入以下参数，其它保持默认。

- 工作负载名称：game。
- 部署集群：选择应用所要运行的集群。

步骤3 单击“下一步”，添加容器。

1. 单击“添加容器”，在“选择镜像”页签中，选择第三方镜像。
2. 选择密钥。若没有可用密钥请先创建。
   若您的镜像仓库不需要认证，密钥认证请选择“否”。
3. 输入镜像地址。
4. 单击“确定”。

步骤4 更多创建无状态工作负载的步骤请参见**无状态工作负载（Deployment）**。

----结束

9 集群控制台

9.1 查看集群中节点

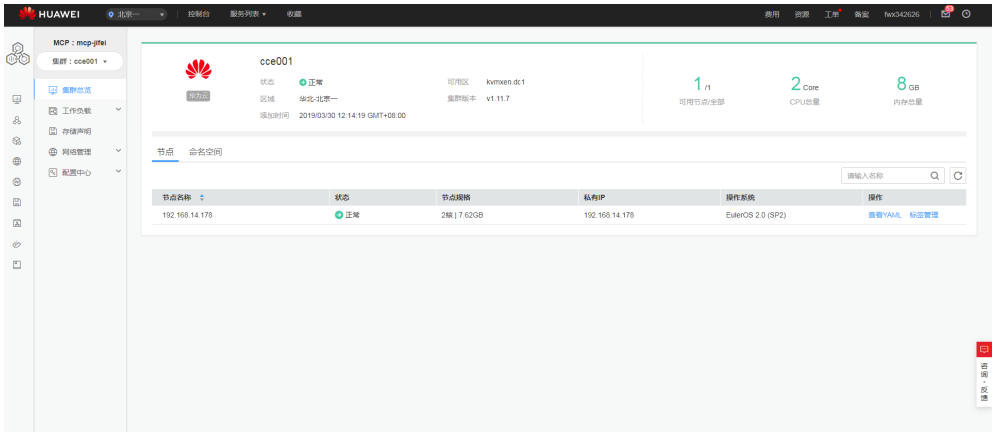
集群添加到MCP后，可在集群控制台查看集群中节点信息。

操作步骤

步骤1 登录集群控制台，选择对应集群。

步骤2 在左侧导航栏中单击“集群总览”，在“节点”页签查看集群中节点信息。

图 9-1 查看集群中节点



----结束

9.2 为节点添加标签

节点标签可以给节点打上不同的标签，给节点定义不同的属性，通过这些标签可以快速的了解各个节点的特点。

节点标签使用场景

节点标签的主要使用场景有两类。

- 节点管理：通过节点标签管理节点，给节点分类。
- 工作负载与节点的亲和与反亲和：
  - 有的工作负载需要的CPU大，有的工作负载需要的内存大，有的工作负载需要IO大，可能会影响其他工作负载正常工作等等，此时建议给节点添加不同标签。在部署工作负载的时候，就可以选择相应标签的节点亲和部署，保证系统正常工作；反之，可以使用节点的反亲和部署。
  - 一个系统可以分为多个模块，每个模块由多个微服务组成，为保证后期运维的高效，可以将节点打上对应模块的标签，让各模块部署到各自的节点模块上，互不干扰、方便开发到各自节点上去维护。

节点固有标签

节点创建出来会存在一些固有的标签，并且是无法编辑和删除的，这些标签的含义请参见表9-1。

表 9-1 节点固有标签

键	值
failure-domain.beta.kubernetes.io/region	表示节点当前所在区域
failure-domain.beta.kubernetes.io/zone	表示节点所在区域的可用区
beta.kubernetes.io/arch	表示节点处理器架构 例如：amd64，表示AMD64位的处理器
beta.kubernetes.io/os	表示节点的操作系统 例如：linux，表示Linux操作系统
kubernetes.io/availablezone	表示节点所在区域的可用区
kubernetes.io/hostname	表示节点主机名称
os.architecture	表示节点处理器架构 例如：amd64，表示AMD64位的处理器
os.name	表示节点的操作系统名称 例如：EulerOS_2.0_SP2，表示欧拉2.2的版本
os.version	表示节点内核版本

添加节点标签

步骤1 登录集群控制台，单击“集群总览 > 节点 ”，可以看到节点列表，单击“标签管理”。

步骤2 单击“添加标签”，填写需要增加标签的“键”和“值”，然后单击“确定”。

如图，填写的键为“deploy_qa”，值为“true”，单击“确定”回到集群总览页面。

图 9-2 添加标签

----结束

删除节点标签

删除标签只能够删除用户添加的标签，节点固有的标签不能删除。

步骤1 登录集群控制台，单击“集群总览 > 节点 ”，可以看到节点列表，单击“标签管理”。

步骤2 单击“删除”，单击“确定”，删除标签。

----结束

9.3 命名空间

集群控制台可以创建只作用于当前集群的命名空间，用于当前集群创建工作负载、创建任务等。可以对命名空间进行配额管理或删除命名空间。但所有操作只作用于当前集群。

- 其中MCP默认创建default命名空间只支持管理配额不支持删除。
- 集群自带的命名空间，如：karmada-cluster、kube-public和kube-system，既不支持管理配额也不支持删除。

命名空间类别

命名空间按创建类型分为四大类：MCP默认创建的、用户创建的、集群默认创建的、用户集群创建的。

- MCP默认创建的：MCP会默认创建default命名空间。不指定命名空间时，默认使用default。
- 集群默认创建的：集群会默认创建kube-public、kube-system、karmada-cluster命名空间。

  - kube-public：用来部署公共插件、容器模板等。
  - kube-system：部署Kubernetes系统组件。
  - karmada-cluster ：用来部署系统组件。
- 用户创建的：用户在MCP控制台创建的命名空间。
- 用户集群创建的：用户在集群控制台创建的命名空间，只作用与当前集群。

创建命名空间

步骤1 登录集群控制台，选择“集群总览”。

步骤2 单击“命名空间 > 创建命名空间”。配置参数。

- 命名空间名称：新建命名空间名称，命名必须唯一。
- 集群名称：展示当前集群，不可更改。
- 描述：对命名空间的描述。
- 配额管理：资源配额可以限制命名空间下的资源使用，进而支持以命名空间为粒度的资源划分。
  - 开启后可设置资源配额。
  - 若暂不启用，可以在命名空间创建后，在列表右侧单击配额管理进行配置。

步骤3 单击“确定 ”。

----结束

删除命名空间

集群控制台只能删除当前集群创建的命名空间，若删除的是在MCP控制台上创建的命名空间，删除后会被重新创建。

删除命名空间将会删除该命名空间相关的所有数据资源，请谨慎操作。

步骤1 登录集群控制台，选择“集群总览”，单击“命名空间”。

步骤2 选择需要删除的命名空间，单击“删除”。

----结束

设置命名空间配额管理

资源配额可以限制命名空间下的资源使用，进而支持以命名空间为粒度的资源划分。

通过设置命名空间级别的资源配额，实现多团队或多用户在共享集群资源的情况下限制团队、用户可以使用的资源总量，包括限制命名空间下创建某一类型对象的数量以及对象消耗计算资源（CPU、内存）的总量。

步骤1 登录集群控制台，在左侧导航栏中单击“集群总览 > 命名空间”。

步骤2 单击对应命名空间后的“配额管理”，单击“编辑配额”。

系统创建的kube-public、kube-system、karmada-cluster命名空间不支持设置资源配额。

步骤3 设置资源配额，单击“确定”。

须知

- 设置资源配额时，请输入整型数值，"0"表示不限制该资源的使用。若限制CPU或内存的配额，则创建工作负载时必须指定CPU或内存请求值。
- 配额累计使用量包含系统默认创建的资源，如default命名空间下系统默认创建的Kubernetes服务（该服务可通过后端kubectl工具查看）等，故建议命名空间下的资源配额略大于实际期望值以去除系统默认创建资源的影响。

- CPU（Core）：限制命名空间下工作负载实例（Pod）能申请CPU资源的最大值。单位为“核”。
- 内存（MiB）：限制命名空间下工作负载实例能申请内存资源的最大值。单位为MiB。
- 有状态工作负载（StatefulSet）：限制命名空间下能创建有状态负载的最大数量。
- 无状态工作负载（Deployment）：限制命名空间下能创建无状态负载的最大数量。
- 普通任务（Job）：限制命名空间下能创建普通任务的最大数量。
- 定时任务（CronJob）：限制命名空间下能创建定时任务的最大数量。
- 实例（Pod）：限制命名空间下能创建实例的最大数量。
- 服务（Service）：限制命名空间下能创建服务的最大数量。

----结束

9.4 工作负载

9.4.1 创建工作负载

工作负载即Kubernetes对一组Pod的抽象模型，用于描述业务的运行载体，包括Deployment、StatefulSet、Job等。

工作负载基本概念

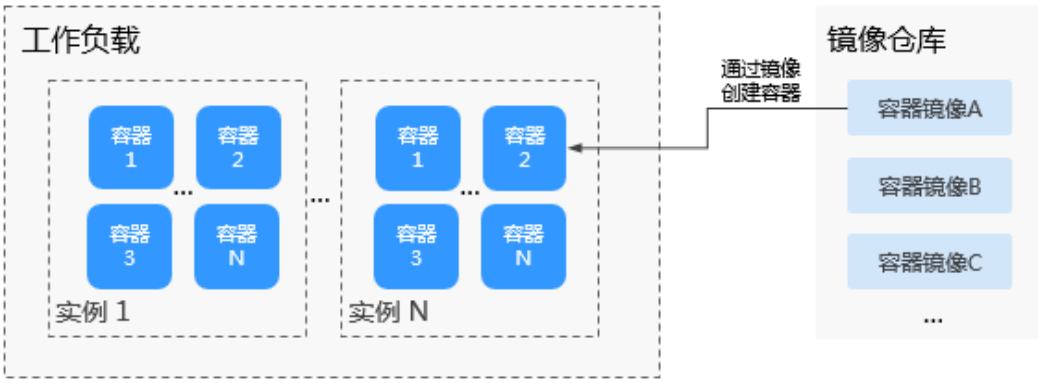
- 无状态工作负载（即Kubernetes中的Deployments）：实例之间完全独立、功能相同，具有弹性伸缩、滚动升级等特性。如：nginx、wordpress，创建无状态工作负载请参见**创建无状态工作负载**。
- 有状态工作负载（即Kubernetes中的StatefulSets）：实例之间不完全独立，具有稳定的持久化存储和网络标示，以及有序的部署、收缩和删除等特性。如：mysql-HA、etcd，创建有状态工作负载请参见**创建有状态工作负载**。

工作负载与容器间的关系

如**图9-3**所示，一个工作负载由一个或多个实例（Pod）组成。一个实例由一个或多个容器组成，每个容器都对应一个容器镜像。对于无状态工作负载，实例都是完全相同的。

版权所有 © 华为技术有限公司

图 9-3 工作负载与容器的关系



工作负载生命周期说明

表 9-2 状态说明

状态	说明
运行中	所有实例都处于运行中才是运行中。
未就绪	所有容器处于pending状态。
升级中	触发升级动作后，工作负载会处于升级中。
已停止	触发停止操作后，工作负载会处于停止状态，实例数变为0。
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。
删除中	触发删除操作后，工作负载会处于删除中状态。

创建无状态工作负载

步骤1 （可选）若基于我的镜像创建工作负载，用户首先需要将镜像上传至容器镜像服务，上传镜像的方式请参考镜像管理。若基于开源镜像中心创建工作负载，则无需上传镜像。

步骤2 在集群控制台选择“工作负载 > 无状态（Deployment）”，单击“创建无状态工作负载”。

步骤3 参照表9-3设置基本信息，其中带“*”标志的参数为必填参数。

表 9-3 工作负载基本信息

参数	参数说明
* 名称	新建工作负载的名称，命名必须唯一。
* 集群名称	新建工作负载所在的集群。

版权所有 © 华为技术有限公司

参数	参数说明
* 命名空间	在单集群中，不同命名空间中的数据彼此隔离。使应用可以共享同个集群的服务，也能够互不干扰。若您不设置命名空间，系统会默认使用default命名空间。
* 实例数量	工作负载的实例数量。工作负载可以有一个或多个实例，用户可以设置具体实例个数，默认为2，可自定义设置为1。 每个工作负载实例都由相同的容器部署而成。设置多个实例主要用于实现高可靠性，当某个实例故障时，工作负载还能正常运行。若使用单实例，节点异常或实例异常会导致服务异常。
描述	工作负载描述信息。

步骤4 单击“下一步”，添加容器。

1. 单击“添加容器”，选择需要部署的镜像。
   - 我的镜像：按区域展示华为云镜像仓库的镜像。若无可用的镜像，可单击“上传镜像”进行上传。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
   - 开源镜像中心：展示了开源镜像仓库中的官方镜像。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
   - 第三方镜像：MCP支持拉取第三方镜像仓库（即华为云镜像仓库与开源镜像仓库之外的镜像仓库）的镜像创建工作负载。使用第三方镜像时，请确保工作负载运行的节点可访问公网。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，并输入“镜像地址”，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，并输入“镜像地址”，单击“确定”。
2. 配置镜像参数。

表 9-4 添加容器参数说明

参数	说明
镜像名称	导入的镜像，您可单击“更换镜像”进行更换。
镜像版本	请选择需要部署的镜像版本。
容器名称	容器的名称，可修改。

参数	说明
容器规格	申请和限制的含义如下，详情请参见设置容器规格。 – 申请：表示容器运行所需最少资源。 – 限制：若担心容器超载，导致系统故障。建议设置容器配额的最高限制。确保容器资源不会超额。

3. 配置生命周期，用于管理容器各阶段需要执行的命令。
   - 启动命令：设置容器启动时执行的命令。
   - 启动后处理：设置容器成功运行后执行的命令，详细配置方法请参见设置容器生命周期。
   - 停止前处理：设置容器结束前执行的命令，通常用于删除日志/临时文件等，详细配置方法请参见设置容器生命周期。
4. 设置健康检查，用于判断容器和用户业务是否正常运行。设置了存活与业务两种探针，详细配置方法请参见容器健康检查。
   - 工作负载存活探针：监测到容器实例不健康时，重启应用。
   - 工作负载业务探针：监测到容器实例不健康时，将工作负载设置为未就绪状态，业务流量不会导入到该容器中。
5. 设置环境变量：在容器中添加环境变量，一般用于通过环境变量设置参数。

   在“环境变量”页签，单击“添加环境变量”。
6. 安全设置：对容器权限进行设置，保护系统和其他容器不受其影响。

   请输入用户ID，容器将以当前用户权限运行。
7. 数据存储：给容器挂载数据存储，适用于需持久化存储、高磁盘IO等场景。详细配置请参见存储声明。

说明

负载创建完成后，您可以登录集群控制台，在工作负载详情页，容器设置页签，单击“修改容器设置”，修改本步骤设置的参数。

步骤5 单击“下一步”，单击“添加服务”，设置工作负载访问方式。

若工作负载需要和其它服务互访，或需要被公网访问，您需要添加服务，设置工作负载访问方式。

工作负载访问的方式决定了这个工作负载的网络属性，不同访问方式的工作负载可以提供不同网络能力。详情请参见网络管理。

- ClusterIP访问

  表示工作负载暴露给同一集群内其他工作负载访问的方式，可以通过“集群内部域名”访问。集群内部域名格式为“<自定义的访问方式名称>.<工作负载所在命名空间>.svc.cluster.local”，例如“nginx.default.svc.cluster.local”。
- NodePort访问

  指工作负载可以让同一虚拟私有云内其他工作负载访问，通过“集群节点的IP”访问，主要场景：云上同一虚拟私有云内其他工作负载需要访问Kubernetes集群内部的工作负载。
- LoadBalancer访问

通过弹性负载均衡从公网访问工作负载，与弹性IP方式相比提供了高可靠的保障，一般用于系统中需要暴露到公网的服务。访问方式由公网弹性负载均衡ELB服务地址以及设置的访问端口组成，例如“10.117.117.117:80”。

步骤6 单击“下一步”，配置高级设置。

- 升级策略：支持“替换升级”和“滚动升级”。
  - 替换升级：先删除旧实例，再创建新实例。升级过程中业务会中断。
  - 滚动升级：滚动升级将逐步用新版本的实例替换旧版本的实例，升级的过程中，业务流量会同时负载均衡分布到新的和旧的实例上，因此业务不会中断。

    最大无效实例数：每次滚动升级允许的最大无效实例数，如果等于实例数有断服风险（最小存活实例数 = 实例数 - 最大无效实例数）。
- 缩容策略：输入时间。工作负载停止前命令的执行时间窗（0-9999秒），默认30秒。
- 迁移策略：输入时间。工作负载实例所在的节点不可用的情况下，将工作负载实例重新调度到其它可用节点的时间窗，默认300秒。
- 调度策略：您可以根据需要自由组合静态的全局调度策略或动态的运行时调度策略来实现自己的需求。
- Pod标签：内置app标签在工作负载创建时指定，暂不支持修改。您可以单击下方的“添加标签”增加标签。

步骤7 配置完成后，单击“创建”。返回无状态工作负载列表查看工作负载状态。

在工作负载列表中，待工作负载状态为“运行中”，工作负载创建成功。

----结束

创建有状态工作负载

步骤1 （可选）若基于我的镜像创建工作负载，用户首先需要将镜像上传至容器镜像服务，上传镜像的方式请参考**镜像管理**。若基于开源镜像中心创建工作负载，则无需上传镜像。

步骤2 在集群控制台选择“工作负载 > 有状态（StatefulSet）”，单击“创建有状态工作负载”。

步骤3 参照**表9-5**设置基本信息，其中带“*”标志的参数为必填参数。

表 9-5 工作负载基本信息

参数	参数说明
* 名称	新建工作负载的名称，命名必须唯一。
* 集群名称	新建工作负载所在的集群。
* 命名空间	在单集群中，不同命名空间中的数据彼此隔离。使应用可以共享同个集群的服务，也能够互不干扰。若您不设置命名空间，系统会默认使用default命名空间。

参数	参数说明
* 实例数量	工作负载的实例数量。工作负载可以有一个或多个实例，用户可以设置具体实例个数，默认为2，可自定义设置为1。 每个工作负载实例都由相同的容器部署而成。设置多个实例主要用于实现高可靠性，当某个实例故障时，工作负载还能正常运行。若使用单实例，节点异常或实例异常会导致服务异常。
描述	工作负载描述信息。

步骤4 单击“下一步”，添加容器。

1. 单击“添加容器”，选择需要部署的镜像。
   - 我的镜像：按区域展示华为云镜像仓库的镜像。若无可用的镜像，可单击“上传镜像”进行上传。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
   - 开源镜像中心：展示了开源镜像仓库中的官方镜像。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，选择对应镜像，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，单击“确定”。若无密钥，请参照创建密钥创建。
   - 第三方镜像：MCP支持拉取第三方镜像仓库（即华为云镜像仓库与开源镜像仓库之外的镜像仓库）的镜像创建工作负载。使用第三方镜像时，请确保工作负载运行的节点可访问公网。
     - 若您的镜像仓库不需要认证，密钥认证请选择“否”，并输入“镜像地址”，单击“确定”。
     - 若您的镜像仓库都必须经过认证（帐号密码）才能访问，请选择密钥，并输入“镜像地址”，单击“确定”。
2. 配置镜像参数。

表 9-6 添加容器参数说明

参数	说明
镜像名称	导入的镜像，您可单击“更换镜像”进行更换。
镜像版本	请选择需要部署的镜像版本。
容器名称	容器的名称，可修改。

版权所有 © 华为技术有限公司

参数	说明
容器规格	申请和限制的含义如下，详情请参见设置容器规格。 – 申请：表示容器运行所需最少资源。 – 限制：若担心容器超载，导致系统故障。建议设置容器配额的最高限制。确保容器资源不会超额。

3. 配置生命周期，用于管理容器各阶段需要执行的命令。
   - 启动命令：设置容器启动时执行的命令。
   - 启动后处理：设置容器成功运行后执行的命令，详细配置方法请参见设置容器生命周期。
   - 停止前处理：设置容器结束前执行的命令，通常用于删除日志/临时文件等，详细配置方法请参见设置容器生命周期。
4. 设置健康检查，用于判断容器和用户业务是否正常运行。设置了存活与业务两种探针，详细配置方法请参见容器健康检查。
   - 工作负载存活探针：监测到容器实例不健康时，重启应用。
   - 工作负载业务探针：监测到容器实例不健康时，将工作负载设置为未就绪状态，业务流量不会导入到该容器中。
5. 设置环境变量：在容器中添加环境变量，一般用于通过环境变量设置参数。

   在“环境变量”页签，单击“添加环境变量”。
6. 安全设置：对容器权限进行设置，保护系统和其他容器不受其影响。

   请输入用户ID，容器将以当前用户权限运行。
7. 数据存储：给容器挂载数据存储，适用于需持久化存储、高磁盘IO等场景。详细配置请参见存储声明。

说明

负载创建完成后，您可以登录集群控制台，在工作负载详情页，容器设置页签，单击“修改容器设置”，修改本步骤设置的参数。

步骤5 单击“下一步”，设置实例间发现服务，如表9-7。

表 9-7 实例间发现服务参数配置

参数	参数说明
服务名称	输入工作负载所对应的服务名称，用于集群内工作负载间的互相访问。该服务主要用于实例的内部发现，不需要有单独的IP地址，也不需要做负载均衡。
端口名称	端口名称用于给容器端口命名，通常以端口用途命名。
容器端口	输入容器的监听端口。

步骤6 单击“添加服务”，设置工作负载访问方式。

若工作负载需要和其它服务互访，或需要被公网访问，您需要添加服务，设置工作负载访问方式。

工作负载访问的方式决定了这个工作负载的网络属性，不同访问方式的工作负载可以提供不同网络能力。详情请参见网络管理。

- ClusterIP访问

  表示工作负载暴露给同一集群内其他工作负载访问的方式，可以通过“集群内部域名”访问。集群内部域名格式为“<自定义的访问方式名称>.<工作负载所在命名空间>.svc.cluster.local”，例如“nginx.default.svc.cluster.local”。

- NodePort访问

  指工作负载可以让同一虚拟私有云内其他工作负载访问，通过“集群节点的IP”访问，主要场景：云上同一虚拟私有云内其他工作负载需要访问Kubernetes集群内部的工作负载。

- LoadBalancer访问

  通过弹性负载均衡从公网访问工作负载，与弹性IP方式相比提供了高可靠的保障，一般用于系统中需要暴露到公网的服务。访问方式由公网弹性负载均衡ELB服务地址以及设置的访问端口组成，例如“10.117.117.117:80”。

步骤7 单击“下一步”，配置高级设置。

- 升级策略：仅支持“滚动升级”。

  说明

  滚动升级将逐步用新版本的实例替换旧版本的实例，升级的过程中，业务流量会同时负载均衡分布到新的和旧的实例上，因此业务不会中断。

- 实例管理策略：支持有序策略和并行策略两种。

  有序策略：默认实例管理策略，有状态负载会逐个的、按顺序的进行部署、删除、伸缩实例，只有前一个实例部署Ready或者删除完成后，有状态负载才会操作后一个实例。

  并行策略：有状态负载并行创建或删除所有的实例，有状态负载发生变更时立刻在实例上生效。

- 缩容策略：输入时间。工作负载停止前命令的执行时间窗（0-9999秒），默认30秒。
- 迁移策略：输入时间。工作负载实例所在的节点不可用的情况下，将工作负载实例重新调度到其它可用节点的时间窗，默认300秒。
- 调度策略：您可以根据需要自由组合静态的全局调度策略或动态的运行时调度策略来实现自己的需求。
- Pod标签：内置app标签在工作负载创建时指定，暂不支持修改。您可以单击下方的“添加标签”增加标签。

步骤8 配置完成后，单击“创建”。返回有状态工作负载列表查看工作负载状态。

在工作负载列表中，待工作负载状态为“运行中”，工作负载创建成功。

----结束

9.5 创建任务

任务概述

任务管理对应Kubernetes中的Job，分为普通任务和定时任务。

普通任务（Job）是Kubernetes用来控制批处理型任务的资源对象。批处理业务与长期伺服业务（Deployment、StatefulSet）的主要区别是批处理业务的运行有头有尾，而长期伺服业务在用户不停止的情况下永远运行。Job管理的Pod根据用户的设置把任务成功完成就自动退出了。成功完成的标志根据不同的spec.completions策略而不同：单Pod型任务有一个Pod成功就标志成功。定数成功型任务保证有N个任务全部成功标志成功。工作队列型任务根据应用确认的全局成功而标志成功。

定时任务（CronJob）即定时任务，是基于时间的Job，类似于Linux系统的crontab，在指定的时间周期运行指定的Job，即：

- 在给定时间点只运行一次。
- 在给定时间点周期性地运行。

CronJob的典型用法如下所示：

- 在给定的时间点调度Job运行。
- 创建周期性运行的Job，例如数据库备份、发送邮件。

创建普通任务

普通任务可用于创建仅执行一次的批处理任务，任务执行完成后会自动退出。使用场景为在创建工作负载前，执行普通任务，将镜像上传至镜像仓库。

步骤1 （可选）普通任务需要基于镜像创建，若选择私有镜像，用户首先需要将镜像上传至镜像仓库。

步骤2 登录集群控制台，选择“工作负载 > 普通任务（Job）”，单击“创建普通任务”。

步骤3 根据界面提示，创建普通任务，详情请参见**创建普通任务**。

步骤4 任务创建完成后，在“普通任务”列表中可查看已创建的普通任务。

待状态为“执行中”，普通任务创建成功。

----结束

创建定时任务

定时任务可用于创建按照设定时间和周期重复执行的任务，任务执行完成后会自动退出。使用场景为在某个固定时间点，为所有运行中的节点做时间同步。

步骤1 （可选）定时任务需要基于镜像创建，若选择私有镜像，用户首先需要将镜像上传至镜像仓库。

步骤2 登录集群控制台，选择“工作负载 > 定时任务（CronJob）”，单击“创建定时任务”。

步骤3 根据界面提示，创建定时任务，详情请参见**创建定时任务**。

步骤4 任务创建完成后，在“定时任务”列表中可查看已创建的定时任务。

待状态为“已启动”，定时任务创建成功。

----结束

9.6 容器组

容器组（Pod）是Kubernetes中最小的可部署单元。一个Pod（容器组）包含了一个应用程序容器（某些情况下是多个容器）、存储资源、一个唯一的网络IP地址、以及一些确定容器该如何运行的选项。Pod容器组代表了Kubernetes中一个独立的应用程序运行实例，该实例可能由单个容器或者几个紧耦合在一起的容器组成。

YAML 创建

步骤1 登录集群控制台，选择“工作负载 > 容器组（Pod）”，单击“YAML创建”。

步骤2 在弹出的“YAML创建容器组”窗中对当前容器组（Pod）的YAML文件进行编辑。

步骤3 单击“创建”，完成YAML创建。

----结束

9.7 配置中心

9.7.1 创建配置项

配置项（ConfigMap）是一种用于存储工作负载所需配置信息的资源类型，内容由用户决定。配置项创建完成后，可在容器工作负载中作为文件或者环境变量使用。

配置项允许您将配置文件从容器镜像中解耦，从而增强容器工作负载的可移植性。

配置项价值如下：

- 使用配置项功能可以帮您管理不同环境、不同业务的配置。
- 方便您部署相同工作负载的不同环境，配置文件支持多版本，方便您进行更新和回滚工作负载。
- 方便您快速将您的配置以文件的形式导入到容器中。

创建配置项

步骤1 登录集群控制台，单击左侧导航栏的“配置中心 > 配置项（ConfigMap）”。您还可以直接创建配置项或基于YAML来创建，若希望通过YAML创建，请跳转至**步骤3**。

步骤2 直接创建配置项。单击“创建配置项”。

参照**表9-8**设置新增配置参数。带“*”号为必填项。

表 9-8 新建配置参数说明

参数	参数说明
*配置项名称	新建的配置名称，同一个命名空间里命名必须唯一。
*集群名称	选择需要创建配置项的集群。

参数	参数说明
*命名空间	新建配置所在的命名空间。若不选择，默认配置为default。
描述	配置项的描述信息。
配置数据	工作负载配置的数据可以在容器中使用。其中，“键”代表文件名；“值”代表文件中的内容。 1. 单击“添加更多配置数据” 。 2. 输入键、值。
标签	标签以Key/value键值对的形式附加到各种对象上（如工作负载、节点、服务等）。 标签定义了这些对象的可识别属性，用来对它们进行管理和选择。 1. 单击“添加标签” 。 2. 输入键、值。

步骤3 基于YAML创建配置项。在创建配置项页面右侧单击“YAML创建”。

说明

若需要通过上传文件的方式创建资源，请确保资源描述文件已创建。MCP支持json或yaml格式，详细请参见**ConfigMap资源文件配置说明**。

您可以导入或直接编写文件内容，格式为YAML或JSON。

- 方式一：导入编排文件。
  单击“上传YAML”，导入格式为YAML或JSON的文件。编排内容中可直接展示YAML或JSON文件的内容。
- 方式二：直接编排内容。
  在编排内容区域框中，输入YAML或JSON文件内容。

步骤4 配置完成后，单击“创建”。

配置项列表中会出现新创建的配置项。

----结束

ConfigMap 资源文件配置说明

ConfigMap资源文件支持json和yaml两种文件格式，且文件大小不得超过2MB。

- json文件格式
  文件名称为configmap.json，配置示例如下：

```
{
  "kind": "ConfigMap",
  "apiVersion": "v1",
  "metadata": {
    "name": "paas-broker-app-017",
    "namespace": "test"
  },
  "data": {
    "context": "{\"applicationComponent\":{\"properties\":{\"custom_spec\":{}},\"node_name\":\"paas-
```

```
broker-app\",\"stack_id\":\"0177eae1-89d3-cb8a-1f94-c0feb7e91d7b\"},\"softwareComponents\":
[{\"properties\":{\"custom_spec\":{}},\"node_name\":\"paas-broker\",\"stack_id\":\"0177eae1-89d3-
cb8a-1f94-c0feb7e91d7b\"}]}"
  }
}
```

- yaml文件格式

  文件名称为configmap.yaml，配置示例如下：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: test-configmap
data:
  data-1: value-1
  data-2: value-2
```

相关操作

配置项创建完成后，您还可以执行表9-9中的操作。

表 9-9 其他操作

操作	说明
查看YAML	单击配置项名称后的“YAML”，可查看到当前配置项的YAML文件。
更新	1. 选择需要更新的配置项名称，单击“更新”。 2. 根据表9-8更改信息。 3. 单击“更新”。
删除	选择要删除的配置项，单击“删除”。 根据系统提示删除。

9.7.2 创建密钥

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。

创建密钥

步骤1 登录集群控制台，单击左侧导航栏的“配置中心 > 密钥（Secret）”。您还可以直接创建密钥或基于YAML来创建，若希望通过YAML创建，请跳转至步骤3。

步骤2 单击“创建密钥”。

参照表9-10设置基本信息。带“*”号为必填项。

表 9-10 基本信息说明

参数	参数说明
*密钥名称	新建的密钥的名称，同一个命名空间内命名必须唯一。

参数	参数说明
*集群名称	选择需要创建密钥的集群。
*命名空间	新建密钥所在的命名空间，默认为default。
描述	密钥的描述信息。
*密钥类型	新建的密钥类型。 ● Opaque：一般密钥类型。 ● kubernetes.io/dockerconfigjson：存放拉取私有仓库镜像所需的认证信息。 ● IngressTLS：存放7层负载均衡服务所需的证书。 ● 其他：若需要创建其他类型的密钥，请手动输入密钥类型。
*密钥数据	工作负载密钥的数据可以在容器中使用。 ● 当密钥为Opaque类型时。 1. 单击“添加更多密钥数据” 。 2. 输入键、值。其中“值”必须使用Base64编码，Base64编码方法请参见**如何进行Base64编码**。 ● 当密钥为dockerconfigjson类型时。输入私有镜像仓库的帐号和密码。 ● 当密钥为IngressTLS类型时。上传证书文件和私钥文件。
标签	标签以Key/value键值对的形式附加到各种对象上（如工作负载、节点、服务等）。 标签定义了这些对象的可识别属性，用来对它们进行管理和选择。 1. 单击“添加标签” 。 2. 输入键、值。

步骤3 基于YAML文件创建密钥。在创建配置项页面右侧单击“YAML创建”。

说明

若需要通过上传文件的方式创建资源，请确保资源描述文件已创建。MCP支持json或yaml格式，详细请参见**Secret资源文件配置说明**。

您可以导入或直接编写文件内容，格式为YAML或JSON。

- 方式一：导入编排文件。
  单击“上传YAML”，导入格式为YAML或JSON的文件。编排内容中可直接展示YAML或JSON文件的内容。
- 方式二：直接编排内容。
  在编排内容区域框中，输入YAML或JSON文件内容。

步骤4 配置完成后，单击“创建”。

密钥列表中会出现新创建的密钥。

----结束

版权所有 © 华为技术有限公司

Secret 资源文件配置说明

本章节主要介绍Secret类型的资源描述文件的配置示例。

例如现在有一个工作负载需要获取帐号密码，可以通过Secret来实现：

- yaml文件格式

  定义的Secret文件secret.yaml内容如下。其中Value需要用Base64，Base64编码方法请参见**如何进行Base64编码**。

```
apiVersion: v1
kind: Secret
metadata:
  name: mysecret          # secret的名称
  namespace: default       #命名空间，默认为default
data:
  username: bXktdXNlcm5hbWUK  #用户名，需要用Base64编码
  password: ******  #需要用Base64编码
type: Opaque      # type建议不要做修改
```

- json文件格式

  定义的Secret文件secret.json内容如下。

```
{
  "apiVersion": "v1",
  "kind": "Secret",
  "metadata": {
    "name": "mysecret",
    "namespace": "default"
  },
  "data": {
    "username": "bXktdXNlcm5hbWUK",
    "password": "******"
  },
  "type": "Opaque"
}
```

相关操作

密钥创建完成后，您还可以执行**表9-11**中的操作。

说明

密钥列表中包含系统密钥资源，系统密钥资源不可更新，也不能删除，只能查看。

表 9-11 其他操作

操作	说明
查看YAML	单击密钥名称后的“YAML”，可查看到当前密钥的YAML文件。
更新密钥	1. 选择需要更新的密钥名称，单击“更新”。 2. 根据**表9-10**更改信息。 3. 单击“更新”。
删除密钥	选择要删除的密钥，单击“删除”。 根据系统提示删除密钥。

版权所有 © 华为技术有限公司

操作	说明
批量删除密钥	1. 勾选需要删除的密钥名称。 2. 单击页面左上角的“删除”，删除勾选的密钥。 3. 根据系统提示删除密钥。

如何进行 Base64 编码

对字符串进行Base64加密，可以直接使用“echo -n 要编码的内容 | base64”命令即可，示例如下：

```
root@ubuntu:~# echo -n "待编码内容" | base64
******
```