天翼云分布式容器云平台 CCE One

用户操作手册

版本：v2.0.1

天翼云科技有限公司

目 录

1. 产品简介

1.1. 产品定义

分布式容器云平台（简称 CCE One ）是面向多云、多集群等场景推出的企业级容器云平台，支持连接并管理异构的 Kubernetes 集群，提供一致管理体验与云原生兼容接口，实现对集群、应用、数据与服务的统一管控。

1.2. 基本概念

在使用分布式容器云平台 CCE One 前，需理解该产品所涉及的概念。本文为您介绍使用分布式容器云平台 CCE One 过程中遇到的常用名词的基本概念和简要描述，以便于您更好地理解 CCE One 产品。

基本业务包括注册集群、容器舰队、集群联邦等。

- 注册集群：基于自研 HUB 代理网关，帮助您将云下 Kubernetes 集群接入云端，快速搭建混合云集群；可以将本地数据中心 Kubernetes 集群或其他云厂商 Kubernetes 集群接入天翼云分布式容器云平台，进行统一管理，实现全域高效、一致的运维体验。
- 容器舰队：多个集群的集合，您可以使用舰队来实现关联集群的分类。舰队还可以实现多集群的统一管理，包括权限管理、多集群应用编排、多集群服务治理、多集群流量分发等能力。
- 集群联邦：提供多云容器编排能力，旨在管理跨云、跨地域场景下的多集群应用，为您提供多集群统一管理、应用部署、服务发现、弹性伸缩、故障迁移等能力。

1.3. 产品功能

分类	功能点	功能说明
总览	资源总览	统计租户名下所有实例的分类型、分资源池数量分布图表
	资源统计	按照注册集群、舰队、联邦等视图，统计相关资源的总量及使用率等信息

	审计日志	用户关键操作的审计日志，包括但不限于相关实例的创建、删除、绑定解绑等
注册集群	天翼云集群	将 CCE 集群关联到 CCE One，作为 CCE One 中的注册集群
	本地集群	创建自研 HUB Gateway 集群，以便将用户本地 IDC 集群注册到云上来
	三方云集群	创建自研 HUB Gateway 集群，以便将用户三方云上的容器集群，注册到天翼云上来
集群管理	集群列表	注册集群列表展示。默认只展示本资源池列表，可选展示所有资源池注册集群列表
	接入配置	分为[基本信息]、[接入信息]和[连接信息]三部分。其中，基础信息展示注册集群的基本创建信息，并支持调整删除保护、绑定/解绑 EIP；接入信息展示用户三方集群注册到 CCE One 的 YAML 命令，只有非 CCE 注册集群才有展示；连接信息展示注册集群 KubeConfig 文件，支持创建临时、吊销等多种操作
	操作日志	注册集群创建、退订的后端施工日志。由后台对应组件自动生成并写入日志条目中
	退订	退订注册集群
	单集群控制台	保持与 CCE 集群控制台完全一致体验的单集群控制台。其中 CCE 注册集群直接与对应 CCE 集群控制台完全一致；非 CCE 注册集群的控制台，相对精简很多，只保留了通用操作部分，例如总览、标准 K8S 资源的列表查看、创建、修改、删除等操作，以及云上标准运维能力如日志、监控、事件、告警等
舰队管理	舰队列表	展示容器舰队实例列表
	创建舰队	创建容器舰队，可同步选择成员集群以及绑定的联邦实例（若有）
	添加集群	向舰队实例添加成员集群；若舰队有关联联邦，则成员集群会同步加入关联的联邦中
	加入联邦	将舰队与联邦关联，舰队中的成员集群会同步成为对应联邦的成员集群
	单舰队控制台	展示舰队的基础信息、资源统计信息以及成员集群信息，并支持对删除保护、EIP、成员集群等进行操作
	删除	删除容器舰队；要求容器舰队无成员集群、未启用联邦等关联能力
联邦管理	联邦列表	展示租户名下联邦实例列表

	创建联邦	订购联邦实例；将在用户选择的 VPC 下，部署联邦 FED 控制面集群，并按需关联用户成员集群信息
	接入配置	包含[基本信息]和[连接信息]两个标签页。其中基本信息为联邦创建的基础信息和网络信息组合，且支持对删除保护、EIP 等进行操作；连接信息为联邦控制面的 KubeConfig 获取和操作支持创建临时和吊销 KubeConfig 等操作
	添加舰队	向联邦中添加成员舰队，舰队关联的注册集群也会同步成为联邦的成员集群
	操作日志	包括创建、退订、升级三种后端关键日志，由后端组件按需自动生成，前端仅做查询展示
	退订	删除联邦实例。要求联邦实例无任何成员舰队
	单联邦控制台	整体包含[总览]和[联邦资源操作]两部分。其中[总览]支持查询联邦基本信息、资源统计信息以及成员信息，并可进行适当操作；[联邦资源操作]部分借鉴了 CCE 单集群控制台体验，支持在联邦控制面操作命名空间、工作负载、服务/路由、配置、存储等标准 K8S 资源，以及管理 CRD 形式扩展的多集群分发策略以及差异化策略

1.4. 产品优势

- 统一集群纳管

集中管理云端、 IDC 机房的 Kubernetes 集群，提供一致的运营体验。

- 统一资源调度

提供多环境统一调度能力， 赋能业务海量算力。

- 统一数据容灾

支持跨地域集群容灾，结合多活应用架构，全面提升企业业务连续 。

- 统一应用交付

全域应用、任务与资源分发，解决业务分布和数据管控诉求。

1.5. 应用场景

- 分布式云管理

集中一处管理任何位置的 Kubernetes 集群以及多地资源，包括连接、日志、任务等。

- 混合云集群

同一 console 控制台管理云上云下集群资源，打通集群网络，实现云上云下资源共享。基于容器镜像能力，同一套镜像和编排部署应用。

- 跨集群分发

提供以应用为中心的视角，支持一个应用发布到不同地域的多个集群。提供面向多集群优化的任务分发和统一调度能力。

1.6. 使用限制

CCE One 是企业级分布式容器云平台，通过中心化的管控实例，纳管异地兼容 Kubernetes 集群。

使用分布式容器云平台之前需要注意以下一些限制：

- 订购注册集群之前需要实名认证。
- 订购集群联邦之后才可使用集群联邦功能，对分布式集群进行统一应用分发和流量均衡。

2. 计费说明

2.1. 计费概述

- 计费模式

天翼云分布式容器云平台 CCE One 当前只支持按量计费一种模式。

按量计费是一种后付费模式，即先使用再付费，按照天翼云 CCE One 实例使用时长计费，按小时结算；按需计费模式允许您根据实际业务需求灵活地调整服务使用，无需提前购买付费，灵活性高。

- 计费项

使用天翼云分布式容器云平台 CCE One 服务时，CCE One 将向您收取必要的管理服务费用，具体如下表所示：

计费项	计费项说明	计费方式	备注
集群管理服务费	• CCE One 管理服务费用由集群类型（包括天翼云集群、本地集群、三方云集群）、集群 vCPU 数量和注册集群运行中时长决定。 • CCE One 管理服务费不包括任何资源（例如负载均衡、弹性 IP、云主机等）相关费用。	按需计费	计费公式：集群规模 × 规格单价 × 运行中时长

注意：

- 天翼云分布式容器云平台 CCE One 是一个统一管理平台，其包括的费用仅为管理服务费用，由 CCE One 通过话单向您收取。
- 虽然您可以通过 CCE One 控制台注册集群，但是所接入集群涉及的其他云服务、云产品产生的计费项并不归入 CCE One，将由对应云产品直接向您收费。

- 集群 vCPU 数统计

如需查看所接入集群的 vCPU 数量，可以运行如下命令：

```
kubectl get nodes -o jsonpath='{range .items[*]}{.metadata.name}{"\t"}{.status.conditions[?(@.type=="Ready")].status}{"\t"} {.status.capacity.cpu}{"\n"}' | grep True
```

- 需要节点状态为 Ready，若节点状态非 Ready 将不纳入集群规模统计；
- 若节点类型为 VK（通过通用 vk 标签“type: virtual-kubelet”识别）暂不纳入规模统计；
- 集群状态为运行中、已断连、变更中时将持续尝试获取集群规模，其他状态下不统计；

以上统计规则仅为参考，天翼云分布式容器云平台 CCE One 保留后续调整此处统计规则的权利，以便为您提供更合理、更规范的规模统计能力；

- 计费周期

天翼云分布式容器云平台 CCE One 按小时计费，每一个小时整点结算一次费用（以 UTC+8 时间为准），结算完毕后将进入新的计费周期；

计费起点以所创建集群成功接入 CCE One 注册集群时间为准，终点以退订注册集群时间为准；

一个计费周期内，不足一小时将按一小时计费。

2.2. 资费说明

在使用天翼云分布式容器云平台 CCE One 相关功能时，涉及费用包括由 CCE One 向您收取的集群管理服务费，以及由关联云产品向您直接收取的相关云产品费用。具体如下：

- 集群管理服务费

实例类型	集群类型	计费单位	计费方式	按需标准价格（元/vCPU/小时）
注册集群	天翼云集群	vCPU	按量计费	0.0556
	三方云集群	vCPU	按量计费	0.0556
	本地集群	vCPU	按量计费	0.1668
集群联邦	集群联邦	vCPU	按量计费	0

说明：

- 天翼云 CCE One 仅向您收取注册集群管理服务费，集群联邦及其他 CCE One 相关功能免费。

- 关联资源计费

使用 CCE One 相关功能时，需要按需使用一些其他云产品资源，将由对应云产品直接向您计费。

相关计费信息，请参见具体产品的计费说明文档。例如：

- ELB 计费信息参考：弹性负载均衡计费说明
- EIP 计费信息参考：弹性 IP 计费说明

- CT-ECS 计费信息参考：弹性云主机计费说明

具体涉及的关联云产品，请以实际使用情况为准。使用不同 CCE One 功能时，涉及需要开启的关联资源会存在一定差异。

2.3. 计费 FAQ

- 注册集群支持哪些计费方式？

当前仅支持按量计费，暂不支持包年包月。

- 订购集群联邦是否计费？

不计费。CCE One 当前仅针对注册集群收取必要的集群管理服务费，其他功能均免费。

- 订购注册集群或集群联邦有什么限制？

CCE One 注册集群或集群联邦当前均是按量付费模式。按量付费方式的订购，要求您的账户有可用余额，余额需要满足以下要求：

- 不少于 100 元。
- 如果您有其他按量付费资源，余额数量应至少满足下一小时的扣费金额。此限制只在部分资源池生效，具体以资源池可见为准（下单时系统会进行校验，不满足的情况下会给予对应提醒）。

场景 1：用户首次注册，需要通过按量付费方式购买资源，因为用户没有已开通的按量付费资源，用户只需要保证余额不少于 100 元即可。

场景 2：用户已经开通了大量按量付费资源，每小时扣费金额 300 元。如果用户还需要继续下单购买按量付费资源，需要余额不少于 300 元。

场景 3：用户已经开通了少量按量付费资源，每小时扣费金额 50 元。如果用户还需要继续下单购买按量付费资源，需要余额不少于 100 元。

- 账号欠费，是否会发送提醒？

欠费后将冻结您账号下所有的按量资源（包括注册集群和集群联邦），并会发送短信及邮件提

醒您。

欠费冻结状态下，您的相关实例服务将均不可用；为了防止您的业务受到影响，您需要及时关注您的账户余额情况。

- 注册集群“已断联”状态下还会计费吗？

已断联状态下云上云下网络中断，服务异常，将不计费。

3. 快速入门

3.1. 入门指引

分布式容器云平台旨在帮助用户解决跨区域、跨地域和跨云容器集群的管理难题，为用户提供一致的管理体验，提升用户的管理效率，降低运维成本，提高系统的稳定性和可靠性。

- 纳管天翼云集群

分布式容器云平台 CCE One 支持一键关联天翼云 CCE 集群，关联后实现集群的自动接管，快速使用流程如下图所示：

具体步骤参考如下：

1.关联 CCE 集群，具体步骤请参见接入集群管理中的关联 CCE 集群部分。

2.您可根据实际需求管理分布式云，实现多云多集群的应用管理。

- 纳管本地 IDC、第三方公有云集群

分布式容器云平台 CCE One 支持接入本地 IDC、第三方公有云集群， 快速使用流程如下图所示：

具体步骤参考如下：

1.创建天翼云注册集群，通过前端订购方式创建天翼云对应类型（本地、三方）注册集群云上实例。

2.打通三方云集群到天翼云注册集群的公网、内网网络（如果是三方云可参考提供 NAT、EIP

并结合天翼云云间高速产品能力进行配置；若为本地集群，则一般基于 IDC 本地公网出口 IP、VPN 等即可）。

3.本地集群接入云上注册集群：从天翼云注册集群接入配置中，复制对应网络类型接入配置并 Apply 到目标集群中，待 cceone-agent 运行起来后，约 2m 左右即可看到注册集群处于运行中状态；

4.管理分布式容器集群：进一步使用注册集群控制台、容器舰队分组能力、集群联邦分布式调度等功能来管理您的 Kubernetes 容器集群。

4. 用户指南

4.1. 授权管理

4.1.1. 概述

根据权限类型，分布式容器云平台 CCE One 的权限包括资源委托权限、IAM 策略权限和实例 RBAC 权限。您需要为服务账号授予对应的权限，才能正常使用分布式容器云平台 CCE One 的功能。

本章将为您介绍资源委托权限、IAM 策略权限和实例 RBAC 权限关系，以及如何为服务账号授予相应权限。

4.1.2. 权限类型

权限类型	是否必须授权	权限说明
资源委托	首次使用CCE One服务时需要授权，使用天翼云账号（主账号，或者具有管理员权限的子账号）授权一次即可。	授权后，CCE One 服务才能正常访问其他关联云资源，并正常运行。
IAM 策略	主账号无需额外授权，IAM 子账号必须授权；基于 IAM 策略权限，可设置子账号使用分布式容器云平台CCE One的相关接口权限以及实例权限。	授权后，IAM 子账号才能正常使用 CCE One 产品功能，或具备管理某些特定实例生命周期的权限。

实例 RBAC	主账号及实例创建账号（若为子账号）无需额外授权；其他子账号必须授权；	授权后，IAM 子账号才能对 CCE One 相关注册集群及联邦实例内的容器资源进行操作；前提条件是，该 IAM 子账号需要已具备相关实例的 IAM 读权限；

4.1.3. 资源委托

资源委托是云服务在特定情况下，因为运行逻辑/功能需要而获取其他云服务访问权限的 IAM 角色。

例如，CCE One 上创建三方注册集群代理 HUB 或创建集群联邦控制面实例时，需要创建弹性负载均衡 ELB 以及弹性 IP，因此需要这两个产品的相关权限。

使用 CCE One（分布式容器云平台）服务需要授予访问以下云资源的权限：

- 访问计算类服务

  注册集群按需弹性云上资源时会关联创建云服务器，需要获取访问弹性云服务器、弹性裸金属服务器的权限。

- 访问存储类服务

  为注册集群关联云上节点和容器挂载存储，需要获取访问云硬盘、弹性文件、对象存储等服务的权限。

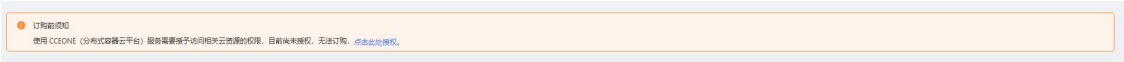
- 访问网络类服务

  为注册集群及联邦提供网络代理及服务对外暴露，需要获取访问虚拟私有云、弹性负载均衡、弹性 IP、NAT 网关等服务的权限。

- 访问容器与监控类服务

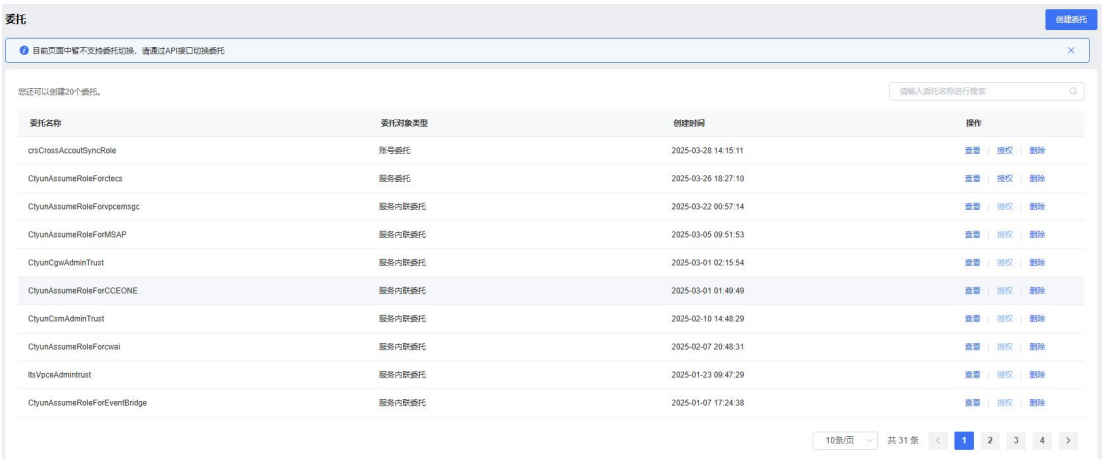
为三方注册集群下容器提供镜像拉取、监控和日志分析等功能，需要获取访问容器镜像、应用运维管理等服务的权限同意授权后，CCE One 将在统一身份认证服务为您创建名为 CtyunAssumeRoleForCCEONE 的委托。在使用 CCE One 服务期间请不要删除或修改 CtyunAssumeRoleForCCEONE 委托，以保证服务正常使用。

若您尚未对 CCE One 进行资源委托授权，在进入 CCE One 任一订购页时，将提示您进行必要的委托授权。



点击【点击此处授权】后，将弹出详细授权说明。

再次点击【确定授权】，后台即开始自动创建分布式容器云平台 CCE One 对应的委托创建。登录 IAM 统一身份认证服务委托对应页面，可以看到 CCE One 对应委托记录如下，委托名“CtyunAssumeRoleForCCEONE”。



4.1.4. IAM 策略

您可以基于 IAM 权限策略，授予子账号部分接口或者特定实例的操作权限，例如允许特定子账号订购注册集群、查询注册集群列表以及退订注册集群，但是限制不允许创建、操作舰队和联邦实例等。

IAM 策略分为接口权限控制和实例权限控制两部分，CCE One 当前均已支持，并提供默认配置模板供选择。

4.2. 注册集群

4.2.1. 概述

CCE One 注册集群可以帮助您快速实现 Kubernetes 集群注册到云端，使用天翼云容器管理控制台对注册集群进行统一管理，赋予云下集群使用云上资源能力。

目前 CCE One 支持注册以下类型的注册集群。

- 天翼云集群：包含天翼云 CCE 专有版、托管版、智算版以及 Serverless 容器引擎 SCE。
- 本地集群： 由 CCE 提供的运行在您数据中心基础设施之上的 Kubernetes

集群，以及满足 CNCF 标准的 IDC 自建的 Kubernetes 集群。

- 三方云集群：三方公有云上提供的 Kubernetes 集群产品，如阿里云（ACK）、腾讯云（TKE）、GCP (GKE)、AWS（EKS）等。

4.2.2. 注册天翼云注册集群

CCE One 支持关联 CCE 专有版、托管版、智算版以及 Serverless 容器引擎 SCE 等天翼云集群，作为分布式容器集群统一管理。

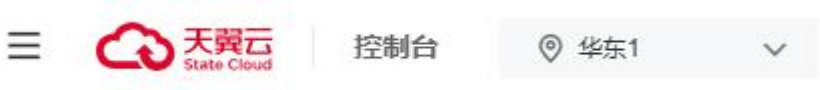
- 前提条件

已创建状态处于运行中待关联的 CCE 专有版、托管版、智算版、SCE 等天翼云集群。

- 操作步骤

1. 登录分布式容器管理控制台，在左侧导航栏选择集群资源>注册集群。

2. 在页面左侧顶部，选择资源池。



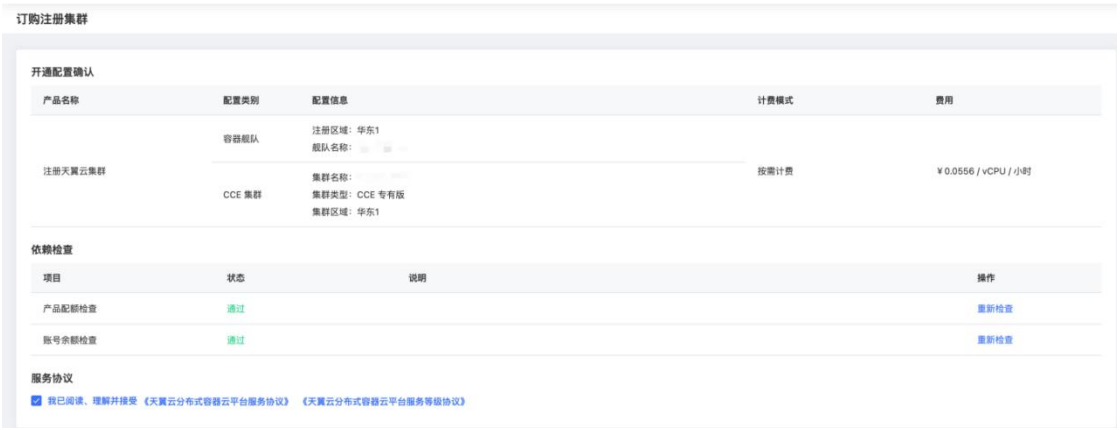
3. 在注册集群指引页面，单击天翼云集群选项卡中的注册集群。

4. 在注册集群订购页面，按照页面指引完成集群配置。

配置项	说明
舰队	关联天翼云集群完成后自动将集群加入指定舰队。关联时可不指定，关联集群后可手动加入舰队。
注册集群	选择待关联的天翼云集群，集群状态必须为运行中。 支持跨资源池关联天翼云集群，包括 CCE One 尚未开通的资源池。注意跨资源池关联的天翼云集群资源池归属与原天翼云集群资源池一致。
企业项目	集群归属的企业项目。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

5. 配置完成后，单击下一步，进入集群确认页面，确认以下信息：

- 确认集群配置是否正确
- 确认依赖检查项是否通过
- 创建集群前，需阅读《天翼云分布式容器云平台服务协议》《天翼云分布式容器云平台服务等级协议》。



6. 配置完成后，单击提交订单。等待集群关联成功。

4.2.3. 注册本地注册集群

CCE One 本地注册集群是用于将本地数据中心 Kubernetes 集群接入天翼云容器服务管理平台统一管理的集群形态， 提供单集群控制台管理能力。

- 前提条件

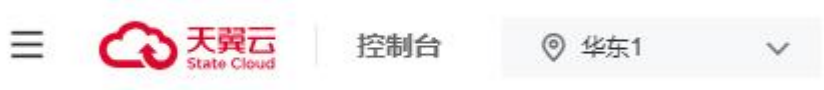
CCE One 注册集群提供公网和内网接入端点。请确保目标集群网络可以正常访问注册集群接入端点的 9443 端口。关于云上云下网络专线接通方案，请参见云专线。

- 操作步骤

创建 CCE One 注册集群

1. 登录分布式容器管理控制台，在左侧导航栏选择集群资源>注册集群。

2. 在页面左侧顶部，选择资源池。所选资源池与用户和资源部署地域的距离越近，网络时延越低，访问速度越快。



3. 在注册集群指引页面，单击本地集群选项卡中的注册集群。

4. 在注册集群订购页面，按照页面指引完成集群配置。

配置项	说明
集群服务商	服务商名称
集群名称	自定义集群的名称，实例名称不允许重复。
舰队	创建注册集群完成后自动将集群加入指定舰队。创建时可不指定，注册集群创建完成后可手动加入舰队。
企业项目	集群归属的企业项目。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
虚拟私有云	配置集群的虚拟私有云 VPC。在已有 VPC 列表中选择已创建的 VPC，或单击创建虚拟私有云创建新的 VPC。
子网	在列表中根据可用区选择已有子网，或单击创建子网创建新的子网。集群控制面与默认节点池将使用此处指定的子网。
安全组	支持选择自动创建安全组、选择已有安全组。 指定已有安全组时，系统默认不会为安全组配置额外的访问规则，可能会导致访问异常，请参考安全组规则列表。

API Server 访问	为 API Server 创建一个按量付费的私网 ELB 实例，作为集群 API Server 的内网连接端点。API Server 提供了各类资源对象（Pod、Service 等）的增删改查及 Watch 等 HTTP Rest 接口。 支持选择是否开放使用 EIP 暴露 API Server。 - 开放：开启后，将为 API Server 私网 ELB 实例绑定一个 EIP，获得从公网访问集群 API Server 的能力。 - 不开放：不会创建 EIP，仅能在 VPC 内使用 KubeConfig 连接并操作集群。 **重要：** - 删除默认创建的 ELB 实例会导致 API Server 无法访问。 - 绑定 EIP 到 ELB 实例后，API Server 可以通过公网接收请求，但集群内的资源无法通过此访问公网。
绑定公网 IP	设置是否启用绑定 EIP。选中此选项，会在集群中自动绑定 EIP，用于建立集群链接。 **说明** - 公网接入必选项；如果云上云下集群已通过专线接入网络，可以不勾选。
集群删除保护	推荐开启集群删除保护，防止通过控制台或 OpenAPI 误删除集群。

5. 配置完成后，单击下一步，进入集群确认页面，确认以下信息：

- 确认集群配置是否正确
- 确认依赖检查项是否通过
- 创建集群前，需阅读《天翼云分布式容器云平台服务协议》《天翼云分布式容

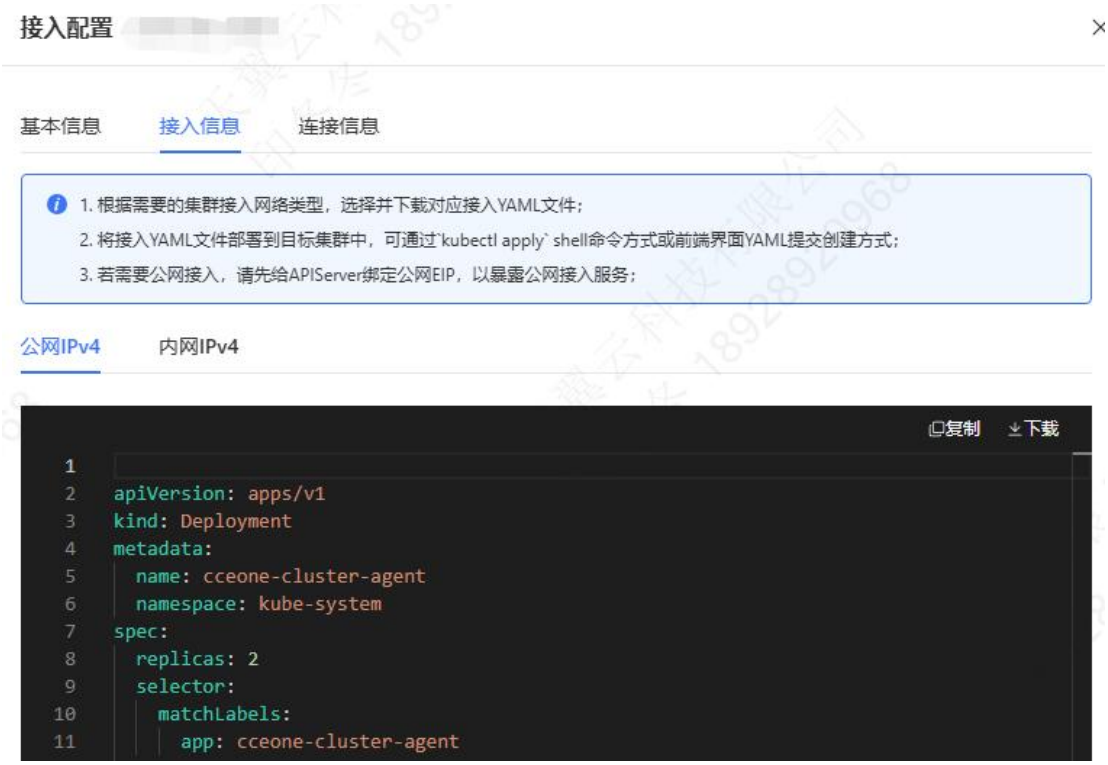
器云平台服务等级协议》。

5. 配置完成后，点击提交订单。提交订单后，可以在集群列表看到创建的注册集群。等待集群创建完成（集群状态：待接入）

将目标集群接入 CCE One 注册集群

找到新创建的 CCE One 注册集群，单击其右侧接入配置。

在接入配置页面单击接入信息页签。在接入信息页签中根据需要选择公网或者私网，然后单击右侧的复制。



将连接信息复制到目标集群的一个文件中，并执行 kubectl 命令，将目标集群注册至新集群中。

例如，您可以新建 agent.yaml 文件，将连接信息复制到 agent.yaml 文件中，并在目标集群中执行 kubectl apply -f agent.yaml 命令。

在目标集群中执行以下命令，查看代理运行状况。

```
kubectl —n kube—system get pod |grep cceone—cluster—agent
```

预期输出：

```
cceone—cluster—agent—98948b75c—27xs6        2/2     Running   0          19s
cceone—cluster—agent—98948b75c—7w9lj        2/2     Running   0          19s
```

注册成功后，您可以在分布式容器管理控制台的集群列表页面，看到该集群的状态为运行中。

- 执行结果

在集群列表页面中，找到对应的 CCE One 注册集群，可使用以下功能：

- 单击集群名称，跳转至集群控制台，进行集群管理。
- 单击接入配置，点击连接信息页签。您可以使用该 KubeConfig 连接目标集群，进行应用负载的部署。

4.2.4. 注册三方云注册集群

CCE One 三方云注册集群是用于将其他云厂商 Kubernetes 集群接入天翼云容器服务管理平台统一管理的集群形态。

- 操作步骤

参考本地注册集群的操作步骤，与本地注册集群接入的操作步骤差异如下：

- 在分布式容器管理控制台，在注册集群指引页面，单击三方云集群选项卡中的注册集群。

- 三方云集群接入后扩展的能力

注册集群是多集群管理能力的基础。

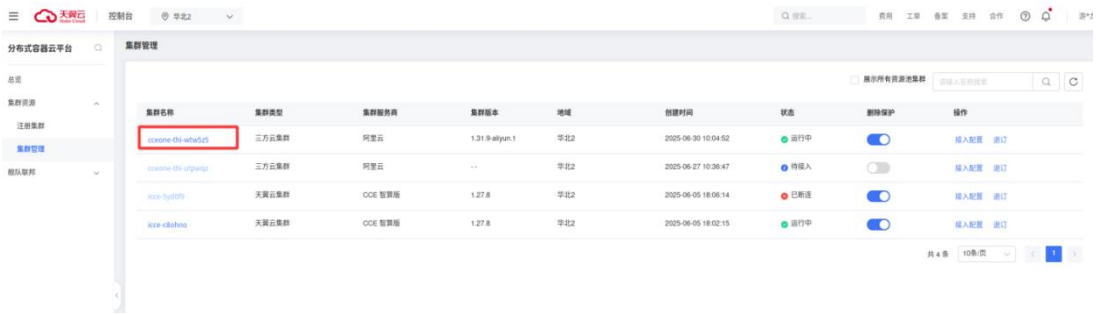
- 三方云接入天翼云后可添加舰队，舰队是多集群统一管理的基础。
- 添加舰队后可开启联邦能力，做多集群资源统一管理。

4.2.5. 注册集群控制台

4.2.5.1 概述

天翼云注册集群分为 CCE 注册集群和非 CCE 注册集群（包括本地注册集群和三方注册集群，以及后续的 AnyWhere）两大类。其中，CCE 注册集群控制台与天翼云 CCE 集群控制台保持完全一致，非 CCE 注册集群则与 CCE 控制台体验保持一致同时，逐步完成相关云上功能往云下的适配，支持了绝大部分云上已有控制台能力。

通过点击集群管理页注册集群名称，即可进入注册集群控制台。



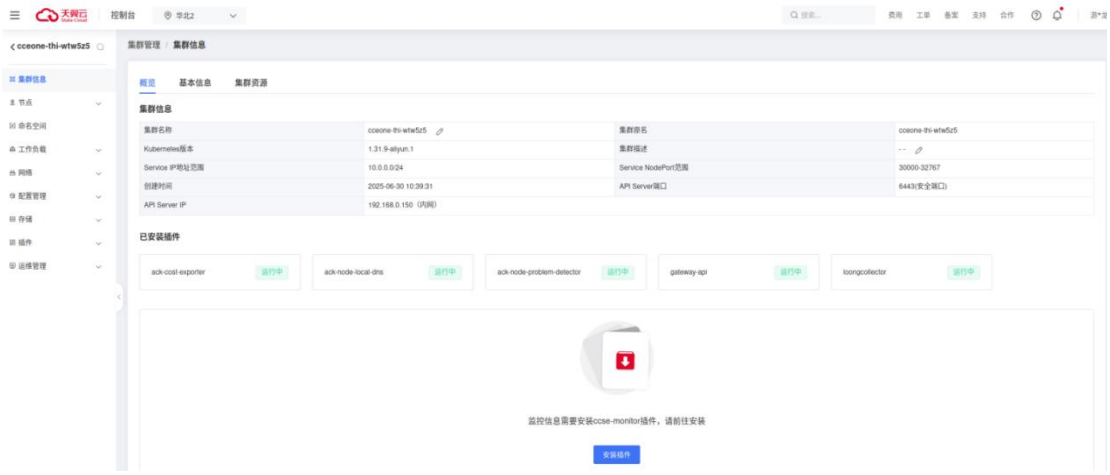
注意：

- 只运行中集群可以点击集群名称进入控制台，其他例如创建中、已断连、接入超时等状态情况下不可点击。

4.2.5.2 通用资源管理

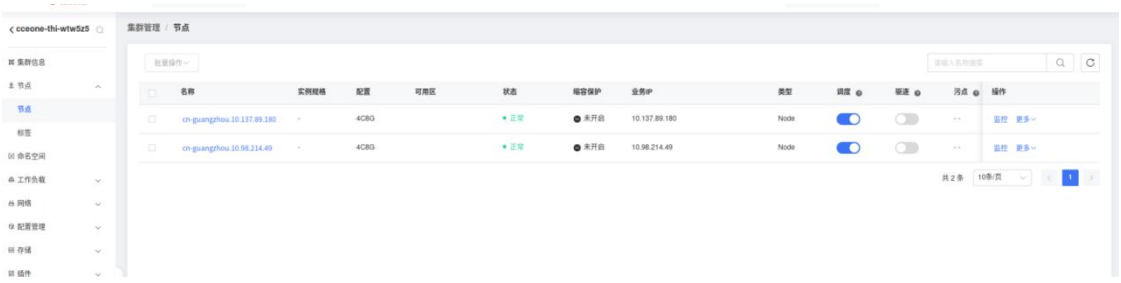
通用资源管理包括集群信息、命名空间、工作负载、网络、配置管理、存储等，

相关功能三方集群控制台与天翼云 CCE 集群控制台保持一致，支持完整的相关功能操作体验。具体参考如下：



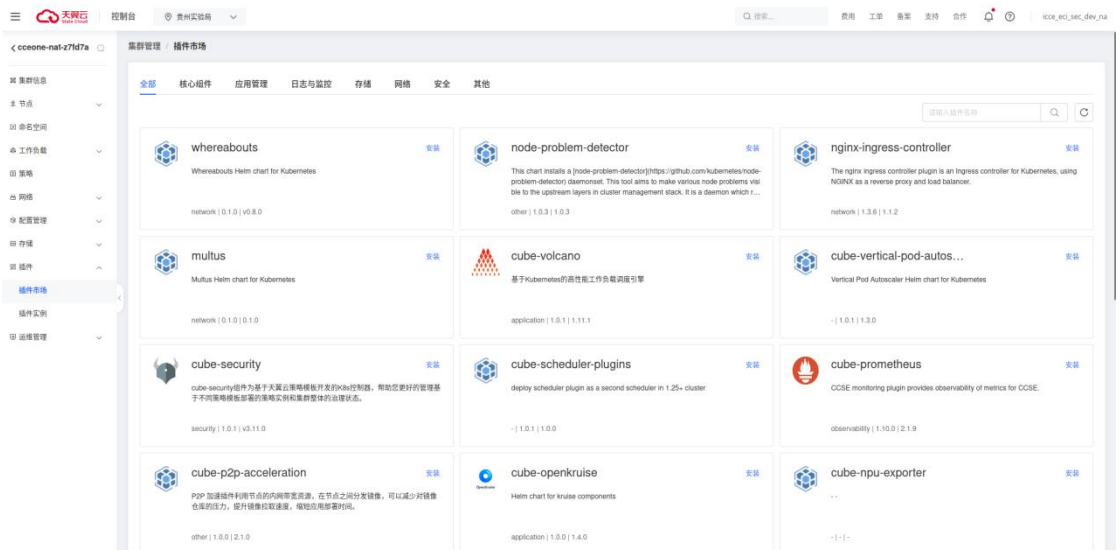
4.2.5.3 节点管理

三方集群节点管理，支持查看节点列表以及管理节点标签。在节点列表页，可查看节点详情、调度及驱逐以及监控污点管理等。



4.2.5.4 插件管理

三方集群控制台支持完整的插件实例生命周期管理能力，包括插件实例安装、卸载及状态查询等能力。同时，三方集群当前已适配了绝大部分 CCE 控制台中插件能力，具体请参考 CCE One 注册集群控制台插件列表。



4.2.5.5 运维管理

4.2.5.5.1 Prometheus 自定义指标监控

分布式容器云平台的集群监控已对接应用性能监控，通过部署 Prometheus 监控服务，支持自定义业务指标的采集上报能力。

前提条件

- 已创建注册集群，具体操作参见 新建注册集群。

说明

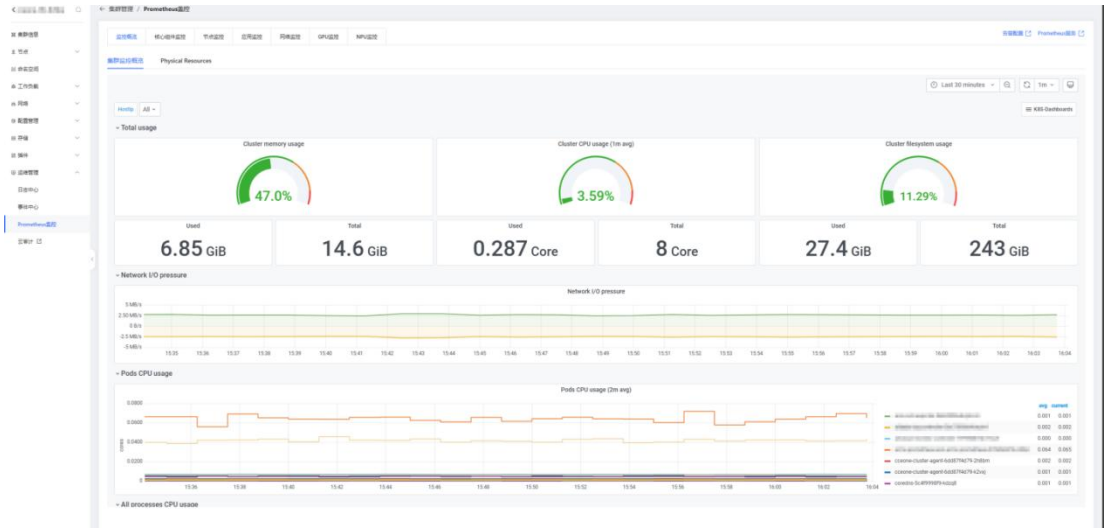
- 通过控制台启用 Prometheus 监控，支持实现自定义业务指标采集上报与 grafana 面板查看。
- 若您需要通过集群中 K8S API 方式查询指标监控（例如 HPA、FederatedHPA 场景等），需要进入集群控制台插件市场，手工安装 metrics-server(metrics.k8s.io)和
- cube-metrics-adapter(custom.metrics.k8s.io)插件。

操作步骤

开启 Prometheus 监控

- 登录分布式容器云平台，进入集群管理页。
- 在集群管理页点击需要查看监控的注册集群，进入集群信息页面。
- 在注册集群详情页面选择 运维管理->Prometheus 监控，若未开通 Prometheus 监控服务，请按照页面指引进行 委托受理->开通应用性能监控->打通应用性能监控网络访问->安装 cube-prometheus 插件。

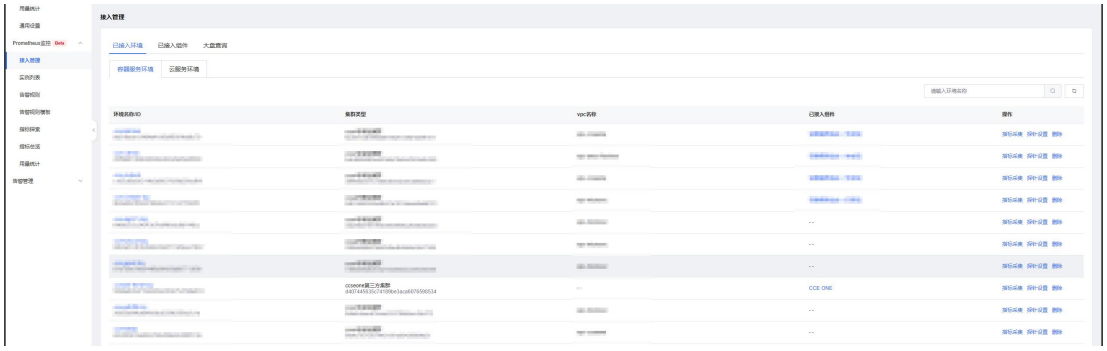
完成操作之后即可进入 Prometheus 监控页面，查看分布式容器云平台提供的预设 Grafana 面板，包括集群概览、核心组件、节点、应用和网络监控，用户可对预设面板进行修改，根据需求定制自己的监控面板。



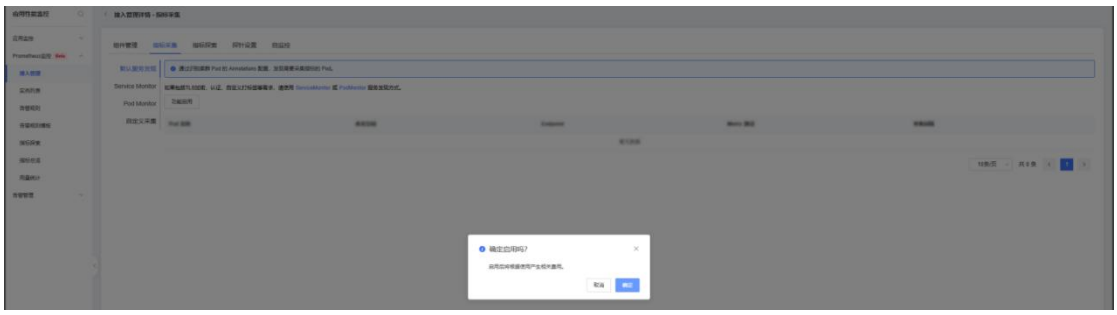
工作负载接入监控

登录应用性能监控控制台，点击进入 Prometheus 监控->接入管理，点击

已接入环境对应的单集群。



在单集群对应的接入管理详情页面，进入指标采集->功能启用，启用后开始收费，对自定义指标上报，使用 ServiceMonitor 或 PodMonitor 服务发现方式进行指标上报。



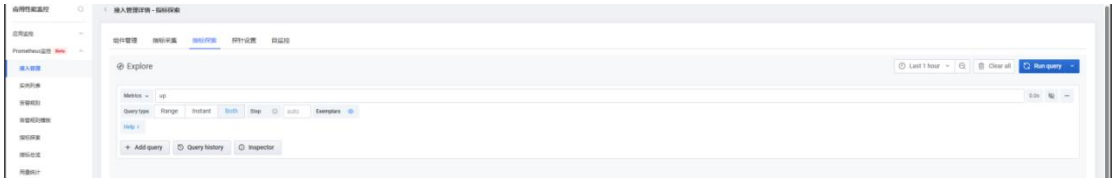
新增 ServiceMonitor

```
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  name: service-monitor1
  namespace: ns1
  annotations:
    arms.prometheus.io/discovery: 'true'
spec:
  endpoints:
  - interval: 60s
    port: metrics # 对应 Service 中定义的端口名称
    path: /metrics
  namespaceSelector:
    any: true # 监控所有命名空间
  selector:
    matchLabels:
      app: app1
```

或者选用新增 PodMonitor

```
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: pod-monitor1
  namespace: ns1
  annotations:
    arms.prometheus.io/discovery: 'true'
spec:
  selector:
    matchLabels:
      app: app1 # 匹配目标 pod 的标签
  namespaceSelector:
    any: true
  podMetricsEndpoints:
  - interval: 60s
    targetPort: 8080
    path: /metrics
```

验证监控指标上报情况，在指标探索页进行搜索对应指标。



4.2.5.5.2 故障诊断

本节介绍了故障诊断的用户指南，分布式容器云平台提供一键故障诊断能力，包括 Service 诊断、节点诊断、Pod 诊断、Ingress 诊断，辅助定位集群中出现的异常问题。

前提条件

- 已完成集群注册，具体操作请参见本地注册集群/三方云注册集群。
- 确保注册集群运行状态处于运行中。

故障诊断功能介绍

云容器引擎提供的故障诊断功能如下表所示：

诊断项	说明
Service 诊断	诊断 Service 相关问题，例如 Service 后端就绪 Pod、异常事件信息等。
节点诊断	诊断节点相关问题，例如 K8s 节点 NotReady 等。
Pod 诊断	诊断 K8s Pod 状态异常相关的问题，例如 Pod 启动失败、Pod 频繁重启等 。
Ingress 诊断	诊断 Ingress 相关流量配置问题。

配置故障诊断

注意

- 使用故障诊断功能时，系统将在您的集群节点上执行数据采集程序并收集检查结果。采集的信息包括系统版本、负载、Docker、kubelet 等运行状态以

及系统日志中的关键错误信息。数据采集程序不会采集您的业务信息及敏感数据。

配置 Service、节点、Pod、Ingress 等诊断操作类似。下文以配置节点诊断为例，介绍如何配置故障诊断功能。

A.登录分布式容器云平台，在左侧导航栏中选择集群资源 > 集群管理，进入注册集群列表页。

B.在注册集群列表中点击需要配置故障诊断的集群，进入集群管理页面。

C.在单集群管理页面导航栏中选择运维管理 > 故障诊断，进入故障诊断页面。

D.在故障诊断页面，点击节点诊断页面，在选择节点面板，选择需要诊断的节点名称，点击确定按钮发起诊断。

在诊断列表页面可查看诊断进展。诊断完成后，诊断页面将显示诊断结果。

查看诊断结果

在故障诊断页面诊断列表的操作列，点击目标诊断报告对应的诊断详情，在诊断详情页面查看详细诊断结果，诊断项状态为异常时，需要确认，如果是引起集群异常的问题需要处理。

注意

- 根据集群配置，具体检查项可能稍有不同。实际结果请以诊断页面结果为准。

4.2.5.5.3 集群巡检

本节介绍了集群巡检的用户指南。

前提条件

- 已完成集群注册，具体操作请参见本地注册集群/三方云注册集群。
- 集群已安装 cube-eye 插件，具体操作请参考插件。

操作步骤

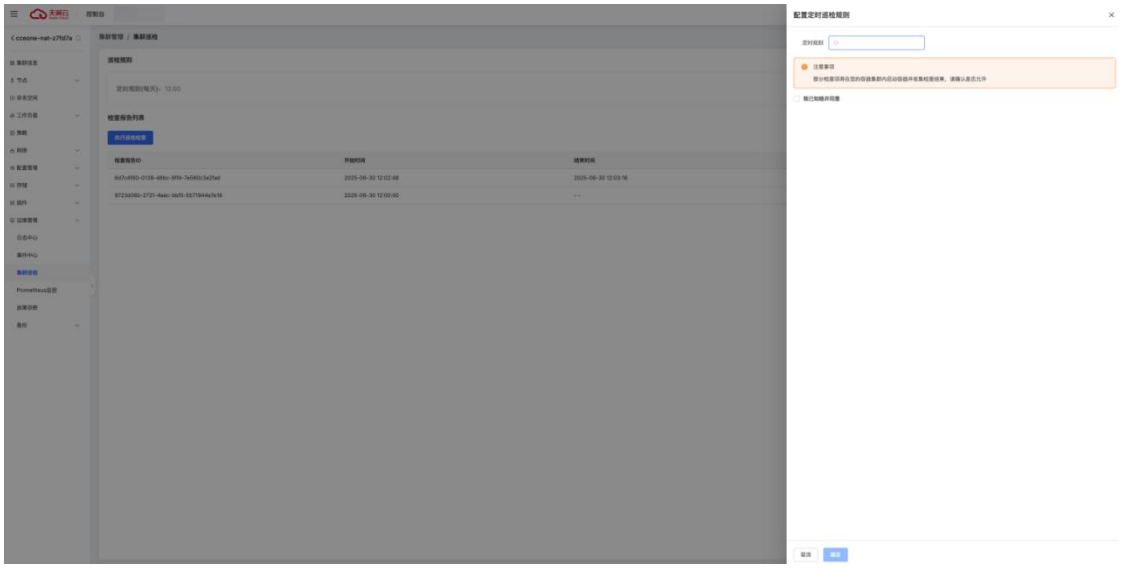
配置集群巡检

登录分布式容器云平台，在左侧导航栏中选择集群资源 > 集群管理，进入注册集群列表页。

在注册集群列表中点击需要配置巡检的集群，进入集群管理页面。

在单集群管理页面导航栏中选择运维管理 > 集群巡检 > 添加 ，进入集群巡检配置页面。

在集群巡检配置页面，设置定时规则 ，阅读注意事项后选择我已知晓并同意 ，然后点击确定。



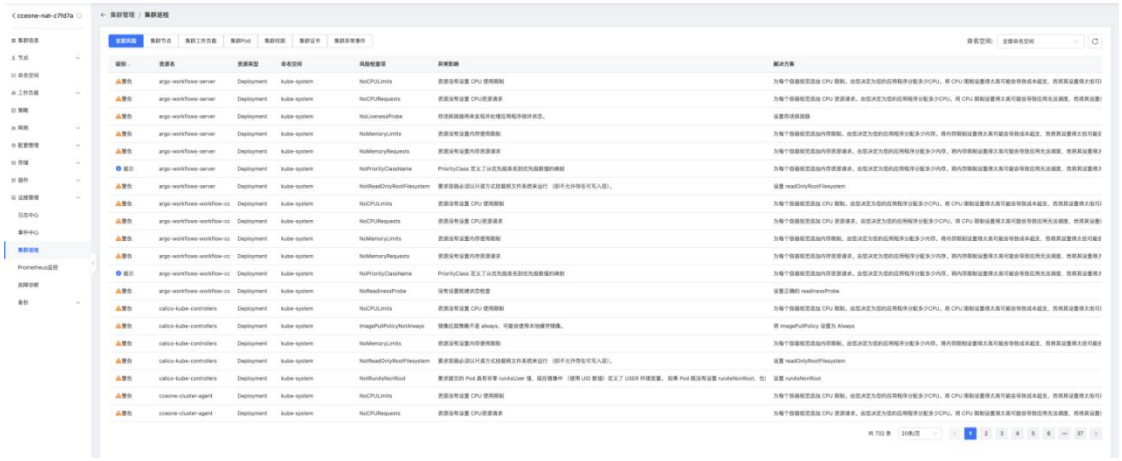
查看巡检结果

登录分布式容器云平台，在左侧导航栏中选择集群资源 > 集群管理，进入注册集群列表页。

在注册集群列表中点击需要查看巡检结果的集群，进入单集群管理页。

在单集群管理页面导航栏中选择运维管理 > 集群巡检 ，选择需要查看的报告，点击查看详情。

报告详情页会展示集群的风险项，可以对风险项的级别、风险类型、命名空间进行筛选，每个风险项都会给出异常影响及解决方案。



巡检项列表

检查项	描述
PrivilegeEscalationAllowed	允许特权升级
CanImpersonateUser	role/clusterrole 有伪装成其他用户权限
CanDeleteResources	role/clusterrole 有删除 kubernetes 资源权限
CanModifyWorkloads	role/clusterrole 有修改 kubernetes 资源权限
NoCPULimits	资源没有设置 CPU 使用限制
NoCPURequests	资源没有设置预留 CPU
HighRiskCapabilities	开启了高危功能，例如 ALL/SYS_ADMIN/NET_ADMIN
HostIPCAllowed	开启了主机 IPC
HostNetworkAllowed	开启了主机网络
HostPIDAllowed	开启了主机 PID
开启了主机 PID	开启了主机端口
ImagePullPolicyNotAlways	镜像拉取策略不是 always
ImageTagIsLatest	镜像标签是 latest
ImageTagMiss	ImageTagMiss
InsecureCapabilities	开启了不安全的功能，例如 KILL/SYS_CHROOT/CHOWN
NoLivenessProbe	没有设置存活状态检查
NoMemoryLimits	资源没有设置内存使用限制
NoMemoryRequests	资源没有设置预留内存
NoPriorityClassName	没有设置资源调度优先级
PrivilegedAllowed	以特权模式运行资源

NoReadinessProbe	没有设置就绪状态检查
NotReadOnlyRootFilesystem	没有设置根文件系统为只读
NotRunAsNonRoot	没有设置禁止以 root 用户启动进程
CertificateExpiredPeriod	将检查 ApiServer 证书的到期日期少于 30 天
EventAudit	事件检查
NodeStatus	节点状态检查
DockerStatus	docker 状态检查
KubeletStatus	kubelet 状态检查

4.3. 容器舰队

4.3.1 概述

容器舰队可提供多集群的统一管理，包括统一的权限管理、统一的安全策略、统一的配置管理以及统一的多集群编排等能力。

使用限制

- 一个注册集群只能加入一个容器舰队。

支持的功能

集群接入分布式容器云平台后，可以加入容器舰队并关联集群联邦能力，进行多集群管理。对容器舰队支持能力如下：

- 创建舰队：舰队是多个集群的集合，可以实现集群的分类，提供多集群的统一管理。
- 添加集群到舰队：舰队提供统一的权限管理、安全策略、配置管理以及统一

的多集群编排等能力。集群加入舰队后，集群关联的权限将被更新为舰队的权限。

- 权限关联：舰队权限配置将同步舰队下所有成员集群。若舰队权限未配置，新签发子账号默认拥有只读权限。权限管理基于 Kubernetes RABC 控制体系的资源权限定义。
- 可观测性：提供舰队资源总览，包括集群数、节点数、CPU 分配率、内存分配率等。
- 舰队关联已有联邦实例：舰队成员集群将自动注册为联邦实例的成员集群，提供集群联邦多集群管理。

4.3.2 创建容器舰队

本文介绍容器舰队的创建、添加集群、关联权限、加入联邦、移除舰队中集群和删除舰队的操作。

创建舰队

登录分布式容器云平台，在左侧导航栏选择 联邦舰队 -> 舰队管理，在舰队管理页签下选择 创建容器舰队。

填写舰队信息：

- 舰队名称。
- 加入联邦：列表中显示当前账户下的联邦实例，可以在创建舰队时加入联邦，也可以在舰队创建完成之后加入。
- 添加集群：列表中显示当前未加入容器舰队的注册集群，可以在创建时添加集群，也可以在创建完成后添加。集群加入舰队后，集群关联的权限与关联舰队的权限保持一致，原集群实例关联权限失效；集群从舰队移除后，则恢

复集群自身绑定权限配置。

- 描述：描述舰队信息。

添加集群

登录分布式容器云平台，在左侧导航栏选择 联邦舰队 -> 舰队管理，在舰队管理页签下选择目标舰队栏中单击 添加集群；或者进入舰队详情页，单击 添加集群。

列表中显示未加入舰队的集群，选择一个或多个注册集群，一个集群只能加入一个舰队。集群加入舰队后，集群关联的权限与关联舰队的权限保持一致，原集群

实例关联权限失效；集群从舰队移除后，则恢复集群自身绑定权限配置。

关联权限

登录分布式容器云平台，在左侧导航栏选择 联邦舰队 -> 舰队管理，在舰队管理页签下选择目标舰队栏中单击 关联权限；或者进入舰队详情页，单击 修改权限。

显示目前舰队已关联权限列表，选择 修改舰队权限，修改权限信息：

- 用户名
- 命名空间：权限作用的命名空间。
- 关联权限：关联已有权限；或者自定义权限，在左侧导航栏选择 平台服务 -> 权限管理 进行操作，自定义权限内容，选择资源对象和操作类型。
- 权限关联：舰队权限配置将同步舰队下所有成员集群。若舰队权限未配置，新签发子账号默认拥有只读权限。权限管理基于 Kubernetes RABC 控制体系的资源权限定义

权限关联：舰队权限配置将同步舰队下所有成员集群。若舰队权限未配置，新签发子账号默认拥有只读权限。权限管理基于 Kubernetes RABC 控制体系的资源权限定义

加入联邦

登录分布式容器云平台，在左侧导航栏选择联邦舰队->舰队管理，在舰队管理页签下选择目标舰队栏中单击加入联邦。

列表中选择已有集群联邦，若还无可用联邦实例，请先在联邦控制台创建。

移除舰队中集群

登录分布式容器云平台，在左侧导航栏选择 联邦舰队->舰队管理，在舰队管理页签下选择目标舰队进入舰队详情页。

选择目标集群，单击集群右侧移出舰队。

删除舰队

当容器舰队不再使用，可以将舰队删除。删除时需要满足两个限制条件：舰队无绑定联邦；舰队中无集群。

- 登录分布式容器云平台，在左侧导航栏选择 联邦舰队 -> 舰队管理，在舰队管理页签下选择目标舰队栏中单击 删除。
- 若舰队中存在集群，先将舰队中集群移除；如果舰队已绑定联邦，先将舰队从联邦中移除。

4.4. 集群联邦

4.4.1 概述

集群联邦实例，是由 CCE One 托管的，旨在管理跨云、跨地域场景下的多集群应用，为您提供多集群统一管理、应用部署、服务发现、弹性伸缩、故障迁移等能力。

功能优势

完全兼容 Kubernetes 原生 API，支持从单集群到多集群零改造升级，无缝集成现有 Kubernetes 工具链生态。

- 丰富的多集群调度策略：集群亲和性调度、多集群拆分/再平衡调度，多维度的高可用部署，包括多 Region、多 AZ、多集群、多云供应商 。提供自动化的多集群故障优雅迁移能力，对故障集群实例进行集中式或分散式的迁移，保证服务实例不跌零
- 多集群流量分发：多集群 Service 实现跨集群的服务发现和访问。多集群 Ingress 提供跨集群的负载均衡和流量路由机制，支持自动切流，可自动摘除故障集群上的流量，保障服务的可用性 。
- 多集群弹性伸缩：基于工作负载的系统指标变动、自定义指标变动或固定的时间周期，实行多集群统一的负载伸缩策略，提升工作负载的可用性和稳定性 。
- 全域容器智能分析：实时监控应用及资源，采集各项指标及事件等数据以分析应用健康状态，提供多集群统一的全栈监控视图，对业务提供端到端追踪和可视化，提供集群健康诊断能力，缩短问题分析定位时间 。

4.4.2 订购集群联邦实例

联邦订购

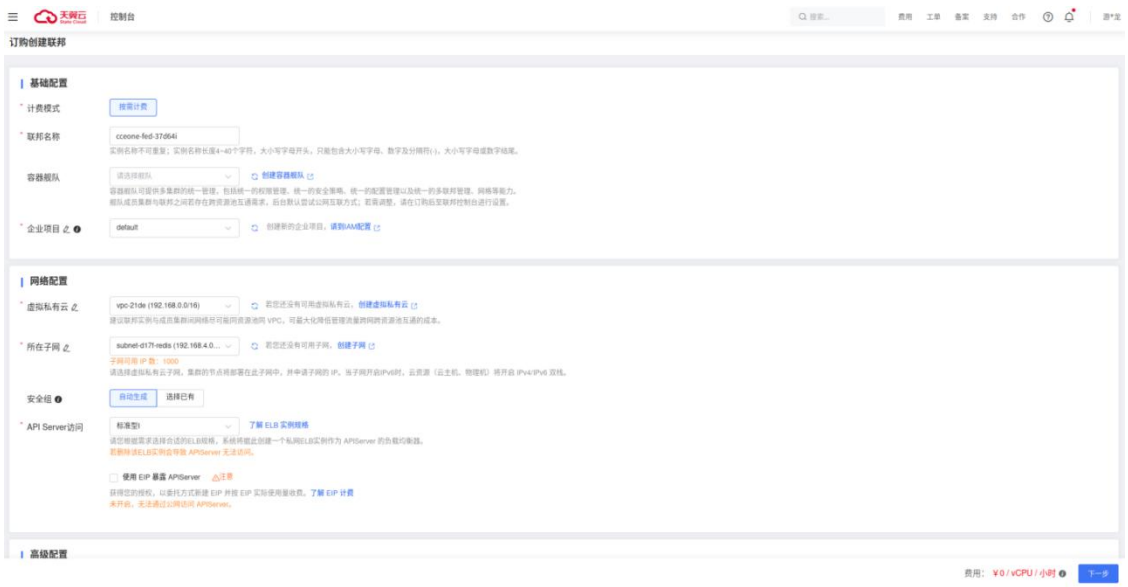
联邦的开通分下面几个步骤：

1.在 CCEONE 控制台右上方点击“创建联邦”按钮

2.在“订购创建联邦”页面，选择计费模式、联邦名称、容器舰队、企业项目、虚拟私有云、所在子网、安全组、ApiServer 访问、是否使用 EIP 暴露 ApiServer、删除保护等参数，选择好了后点击“下一步”

3.在“开通配置”页面确认创建配置符合要求后，勾选同意“服务协议”，勾选好后点击“提交订单”

4.返回 CCEONE 控制台，查看开通状态，待实例处于“运行”状态后开通成功，可点击实例进入控制台操作联邦实例



项目	约束
计费模式	当前只支持“按需计费”模式
联邦名称	实例名称不可重复；实例名称长度 4~40 个字符，大小写字母开头，

	只能包含大小写字母、数字及分隔符（-），大小写字母或数字结尾
容器舰队	容器舰队可提供多集群的统一管理，包括统一的权限管理、统一的安全策略、统一的配置管理以及统一的多联邦管理、网格等能力 舰队成员集群与联邦之间若存在跨资源池互通需求，后台默认尝试公网互联方式；若需调整，请在订购后至联邦控制台进行设置
企业项目	可选择已有企业项目，或者在 IAM 创建新的企业项目
虚拟私有云	建议联邦实例与成员集群间网络尽可能同资源池同 VPC，可最大化降低管理流量跨网跨资源池互通的成本。
所在子网	请选择虚拟私有云子网，集群的节点将部署在此子网中，并申请子网的 IP。当子网开启 IPv6 时，云资源（云主机、物理机）将开启 IPv4/IPv6 双栈
APIServer 访问	请您根据需求选择合适的 ELB 规格，系统将据此创建一个私网 ELB 实例作为 APIServer 的负载均衡器，若删除该 ELB 实例会导致 APIServer 无法访问
安全组	可自动生成或者选择已有安全组，需要确保联邦访问端口在虚拟私有云的子网里为放通状态
是否使用 EIP 暴露 APIServer	获得您的授权，以委托方式新建 EIP 并按 EIP 实际使用量收费，未开启，无法通过公网访问 APIServer
删除保护	防止通过控制台或 API 误删除联邦控制面，删除联邦控制面实例不会对用户容器集群造成任何影响，理论上也不影响已调度完成的应用

联邦退订

联邦的退订分下面几个步骤：

1.在 CCEONE 的控制台联邦列表页，点击要退订的联邦实例最右侧的“退订”按钮

2.在“退订联邦”的页面上的检查项都通过后，勾选“我已阅读并知晓上述信息”，点击“确定按钮”

3.返回到 CCEONE 控制台联邦列表页面查看联邦实例退订状态

项目	约束
运行状态	只支持非订购中状态实例退订
删除保护	只能在关闭安全保护状态下退订
关联资源	联邦实例无成员舰队及集群状态下才能退订

4.4.3 集群联邦控制台

4.4.3.1 概述

资源模板

集群联邦使用 Kubernetes 原生 API 定义联邦资源模板，以便轻松与现有 Kubernetes 采用的工具进行集成。

调度策略

集群联邦提供了一个独立的 Propagation(placement) Policy API 来定义多集群的调度要求。

- 支持 1:N 的策略映射机制。用户无需每次创建联邦应用时都标明调度约束。
- 在使用默认策略的情况下，用户可以直接与 Kubernetes API 交互。

差异化策略

集群联邦为不同的集群提供了一个可自动化生产独立配置的 Override Policy API。例如：

- 基于成员集群所在区域自动配置不同镜像仓库地址。
- 根据集群不同的云厂商，可以使用不同的存储类。

4.5. 平台服务

4.5.1. 权限配置

4.5.1.1 概述

根据权限类型，分布式云容器平台的权限包括服务角色、IAM 权限策略和 RBAC 权限。您需要为服务账号授予对应的权限，才能正常使用分布式云容器平台的功能。本文将为您介绍委托、IAM 权限策略和 RBAC 权限关系，以及如何为服务账号授予相应权限。

权限类型

权限类型	是否必须授权	授权说明
委托	使用开通订购功能时必须授权，使用主账号或子账号授权一次即可。	授权后分布式云容器平台才能访问其他关联的云服务资源。

IAM 系统权限策略	主账号默认拥有所有权限，无需额外授权。而子账号必须授权后才能访问分布式云容器平台。	授权后子账号才能使用分布式云容器平台系统功能。
RBAC 权限	主账号默认拥有所有权限，无需额外授权。子账号可以根据需求授予权限，如果没有授权，则采用默认只读权限。	授权后，子账号才能对分布式云容器平台集群内的 K8s 资源进行操作。

委托

云服务委托是指，在特定业务场景下，云服务为实现特定功能目标，通过获取其他云服务的访问权限，自动化管理关联资源，从而优化整体服务质量的一种协作机制。

例如，在分布式云容器平台上订购注册集群后，需要关联创建 ELB、安全组等资源。分布式云容器平台通过委托机制获取关联服务权限，从而自动地完成配置和关联资源创建，提升订购功能的使用体验。

分布式云容器平台目前提供以下服务角色，具体的策略内容请参见 IAM 控制台。

委托名称	权限说明
CtyunAssumeRoleForCCEONE	分布式云容器平台在集群管控操作中使用该角色访问您在ELB、EIP、安全组等服务中的资源。

IAM 权限策略

默认情况下，子账号在使用云服务时没有任何权限。如果您通过子账号访问分布式云容器平台，需要为其授予相应的操作权限，以确保正常使用分布式云容器平台的功能。分布式云容器平台提供了一些默认的系统权限策略，用于控制全局资源的读写访问，您可以根据业务需求为子账号添加相应的系统策略。

IAM 系统权限策略	权限说明
ccseone-admin	当前账号拥有分布式云容器平台的所有权限
ccseone-user	当前账号拥有注册集群、舰队、联邦等资源的读写权限
ccseone-viewer	当前账号拥有分布式云容器平台的资源的只读权限

RBAC 权限

IAM 系统权限策略仅控制分布式云容器平台资源的操作权限，若子账号需要操作指定集群内的 K8s 资源（比如查询 Pod 信息、修改 ConfigMap 的配置内容），除 IAM 系统权限策略外，还需要获取指定分布式云容器平台集群的 RBAC 权限。赋予 RBAC 权限可以在分布式云容器平台的权限管理页面进行操作，支持赋予预置角色和自定义角色。另外值得注意，如果注册集群加入了舰队，舰队和注册集群都设置了 RBAC 权限，此时该注册集群的 RBAC 权限将以舰队的 RBAC 权限为准。

分布式云容器平台提供以下预置角色：

RBAC 权限	权限说明
管理员	对所有集群资源对象的读写权限。
运维人员	对集群命名空间级别资源对象的读写权限，对其他资源对象的只读权限。
开发人员	对集群命名空间级别控制台可见资源对象的读写权限。
受限人员	对集群命名空间级别控制台可见资源对象的只读权限。

4.5.1.2 服务资源权限（IAM 授权）

分布式容器云平台集群权限是基于 IAM 系统策略和自定义策略的授权，可以通过用户组功能实现 IAM 用户的授权。

注意

- 服务资源权限（IAM 授权）仅针对注册集群、舰队、联邦等服务资源有效，如果您要操作 Kubernetes 资源，您必须确保同时配置了 Kubernetes 集群内权限，才能有操作 Kubernetes 资源（如工作负载、Service 等）的权限。

配置说明

服务资源权限配置，比如创建用户组和具体权限配置，均需要跳转到 IAM 控制台进行具体操作。设置完成后在集群权限页面能看到用户组所拥有的权限。

示例流程

1. 创建用户组并授权。

在 IAM 控制台创建用户组，并授予分布式容器云平台权限，例如 ccseone-viewer。

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。

用户登录控制台，验证权限：

- 单击左侧导航栏“舰队联邦 > 舰队管理”，如果创建舰队时提示无访问权限，表示权限配置已生效。
- 单击左侧导航栏“集群资源 > 注册集群”，如果订购注册集群时提示无访问权限，表示权限配置已生效。

系统角色

角色是分布式容器云平台最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。IAM 中预置的分布式容器云平台系统角色为 ccseone-admin。

- ccseone-admin：系统策略，分布式容器云平台相关资源的所有权限
- ccseone-user：系统策略，分布式容器云平台相关资源读写权限，不包括开通订购注册集群、集群联邦等权限。
- ccseone-viewer：系统策略，分布式容器云平台相关资源只读权限

资源权限与企业项目

分布式容器云平台支持以注册集群、集群联邦为粒度，基于企业项目维度进行资源管理以及权限分配。

如下事项需特别注意：

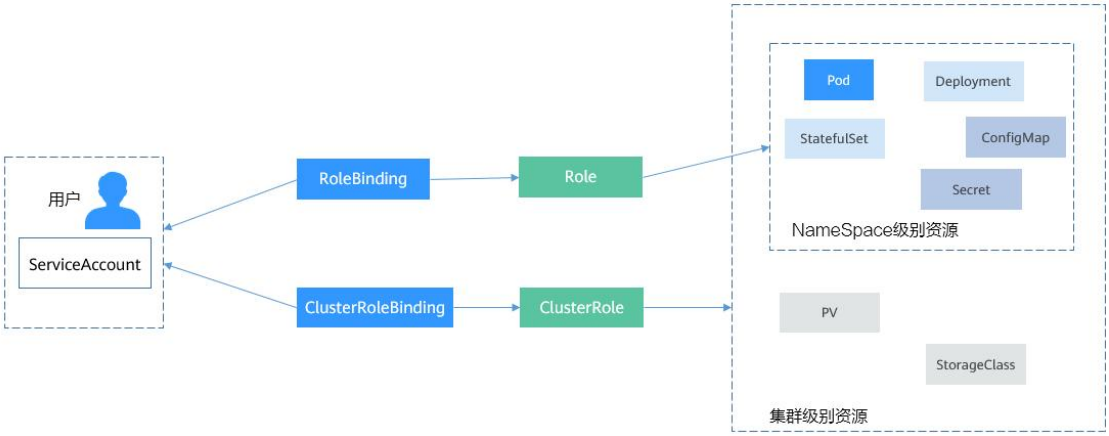
- IAM 项目是基于资源进行管理，而企业项目则是提供资源的全局逻辑分组，更符合企业实际场景，并且支持基于企业项目维度的 IAM 策略管理，因此推荐您使用企业项目。
- IAM 项目与企业项目共存时，IAM 将优先匹配 IAM 项目策略。
- 分布式容器云平台集群基于已有基础资源（VPC）创建集群、节点时，请确保 IAM 用户在已有资源的企业项目下有相关权限，否则可能导致集群或者节点创建失败。

4.5.1.1 Kubernetes RBAC 权限

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

- Role：角色，其实是定义一组对 Kubernetes 资源（命名空间级别）的访问规则。
- RoleBinding：角色绑定，定义了用户和角色的关系。
- ClusterRole：集群角色，其实是定义一组对 Kubernetes 资源（集群级别，包含全部命名空间）的访问规则。
- ClusterRoleBinding：集群角色绑定，定义了用户和集群角色的关系。
- Role 和 ClusterRole 指定了可以对哪些资源做哪些动作，RoleBinding 和 ClusterRoleBinding 将角色绑定到特定的用户、用户组或 ServiceAccount 上。如下图所示。

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



在分布式容器云平台控制台可以授予用户或用户组命名空间权限，可以对某一个命名空间或全部命名空间授权，产品控制台提供如下预置的 ClusterRole。

受限人员：对集群命名空间级别控制台可见资源对象的只读权限。

开发人员：对集群命名空间级别控制台可见资源对象的读写权限。

运维人员：对集群命名空间级别资源对象的读写权限，对其他资源对象的只读权限。

管理员权限：对所有集群资源对象的读写权限。

服务资源权限（IAM 授权）与 Kubernetes RBAC 权限的关系

服务资源权限（IAM 授权）主要覆盖分布式云容器平台系统功能 和 系统资源（比如注册集群、舰队、集群联邦）的权限管理，而 Kubernetes RBAC 权限仅针对该集群的 Kubernetes 资源生效。

配置 Kubernetes RBAC 权限

步骤 1 登录 CCE 控制台，在左侧导航栏中选择「权限管理」。

步骤 2 点击权限管理页面的「添加权限」按钮

步骤 3　填写详细的权限信息，然后点击保存按钮

步骤 4 保存权限后，需要「关联权限」才会真正生效，以舰队为例子，如下图。

选择需要关联的用户、命名空间和权限

4.6. 生态中心

4.6.1. 容器迁移

4.6.1.1 概述

基于 CCE One 容器迁移能力，帮助业务将本地 IDC 或三方云上的 Kubernetes 容器集群，迁移到天翼云云容器引擎服务；迁移过程安全、可靠、灵活、高效，无需停机，热迁移、对业务零影响。

工作原理

将应用从一个环境迁移到另一个环境是一项具有挑战性的任务，因此仔细的规划和准备至关重要。天翼云 CCE One 的容器迁移服务通过以下五个阶段为您提供全流程迁移指导：

集群评估：在此阶段，您需要评估源集群的规模以决定目标集群的类型和资源规模。

依赖数据迁移：在这个阶段，基于天翼云上的云迁移、云备份等标准云产品服务，您将迁移镜像以及依赖服务的相关数据。

元数据迁移：在此阶段，您需要通过容器备份/恢复功能或集群联邦方式，将应用元数据从源集群迁移到目标集群，从而让应用在目标集群中正常运行起来。

应用迁移：在这个阶段，您可以通过特定方式进行流量调度，例如智能 DNS+单集群 LB 或多集群 Ingress、多集群 Service 等，将业务流量逐步从源集群迁移到目标集群。

业务验证：流量迁移过程中及流量迁移完成后，您可以对迁移后业务允许情况进行验证，以确保服务运行符合预期。

通过遵循天翼云 CCE One 容器迁移服务的全流程迁移指导，您可以更顺利地将应用从一个环境迁移到另一个环境。

迁移方式

天翼云 CCE One 为您提供多种迁移工具及迁移方式可选，以满足您不同场景下对迁移服务的需求。具体来讲，主要为如下两种：

方式一：全量迁移

由 CCE One 提供工具，帮助您自动备份源集群元数据，并在天翼云目标集群中数据恢复，后续再自行逐个应用切流；对应操作流程参考如下：

优势：可实现容器集群的一次性完整复制，操作简单。

缺点：要求目标集群与源集群一开始就 1:1 资源配置，可能存在资源浪费。

适用场景：适合想要快速迁移，或希望单独备份数据的场景。

方式二：增量迁移

基于 CCE One 提供的多集群联邦应用迁移能力，帮助您实现集群中应用按需、有序、无感迁移目的；对应操作流程参考如下：

优势：可应用维度逐步迁移和切流，目标集群规模随切流进度逐步扩大，资源利用合理。

缺点：要求源、目标集群均纳管到天翼云 CCE One，且迁移粒度更细，操作可能相对繁琐。

适用场景：适合需要精细化梳理和迁移应用的场景。

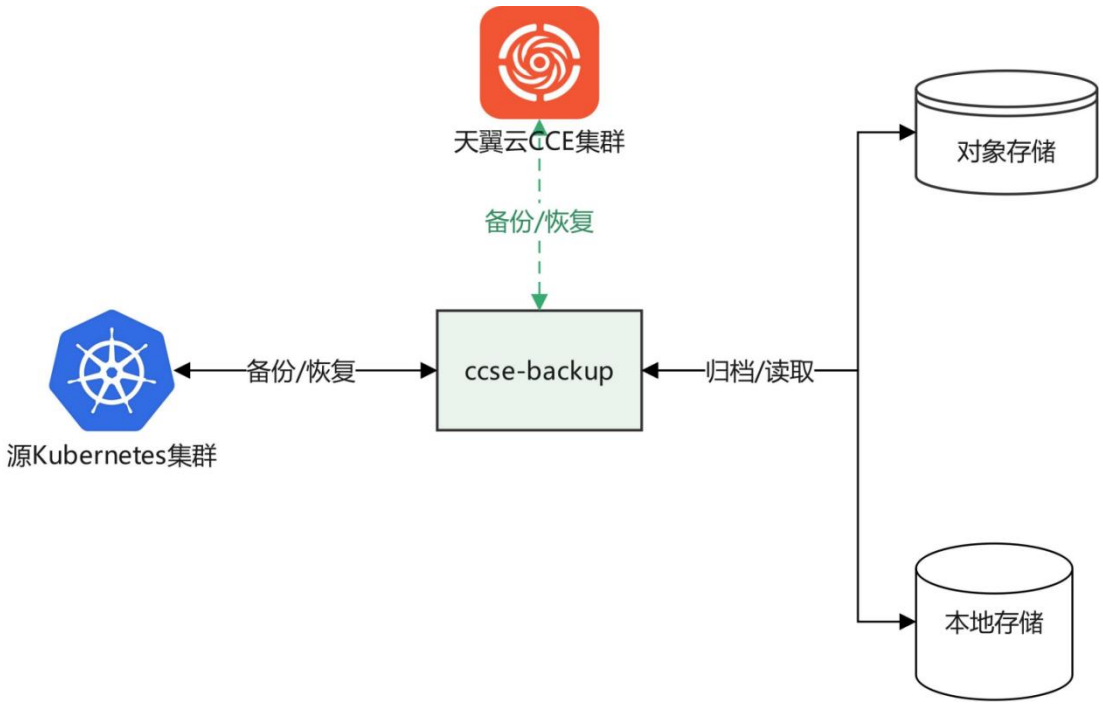
适用场景

天翼云 CCE One 容器迁移服务，支持多种场景下的容器迁移或备份服务，以满足您不同场景下的功能需求。具体参考下表：

场景	说明
备份场景	实现集群中应用（资源 YAML）的备份和恢复，并将备份数据安全地存储在指定的对象存储 OSS Bucket 中；
容灾场景	基于多集群联邦能力，为您提供灾难情况下的应用自动容灾迁移能力，确保服务始终可用、异常后也可快速恢复；

4.6.1.2 集群元数据备份与恢复

天翼云分布式容器云平台 CCE One 提供备份恢复功能，能对已被分布式容器云平台纳管的集群应用进行备份，并在线上其他 CCE 集群恢复，从而快速完成线下应用向线上环境的迁移。本文详细介绍了如何使用备份能力将已接入注册集群的线下自建集群中的应用高效迁移至天翼云容器引擎 CCE 集群中来。



前提条件

- 已开通对象储存（CT-ZOS）服务，并开通公网访问。具体操作，请参考对象储存。
- 将自建 Kubernetes 集群通过注册集群的方式接入分布式容器云平台 CCE One。具体操作，请参见将本地 Kubernetes 接入注册集群。

注意：

- 若源/目标集群无法注册到天翼云 CCE One 注册集群时（公网/内网均不具备打通条件），可考虑手工向成员集群部署 ccse-backup 插件以及 YAML 配置方式进行相关操作，相对前端操作方式会比较繁琐。若有需要，可联系天翼云售前同学咨询。

适用场景

实现业务快速上云，应用备份迁移一体化。

参考指引

本文以 nginx 应用为例，在线下集群中部署应用后进行备份，然后在线上天翼云注册集群中进行恢复。

步骤一：在自建 Kubernetes 集群部署应用

执行以下命令，创建对应的 nginx deployment：

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:latest
        imagePullPolicy: IfNotPresent
        ports:
        - containerPort: 80
---
apiVersion: v1
kind: Service
metadata:
  name: nginx-service
  labels:
    app: nginx
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
```

预期结果：

```
docker@debian:~$ kubectl get pod -A
NAMESPACE            NAME                                READY   STATUS    RESTARTS      AGE
default              nginx-deployment-67dffbbbb-4xqb7    1/1     Running   0             6s
```

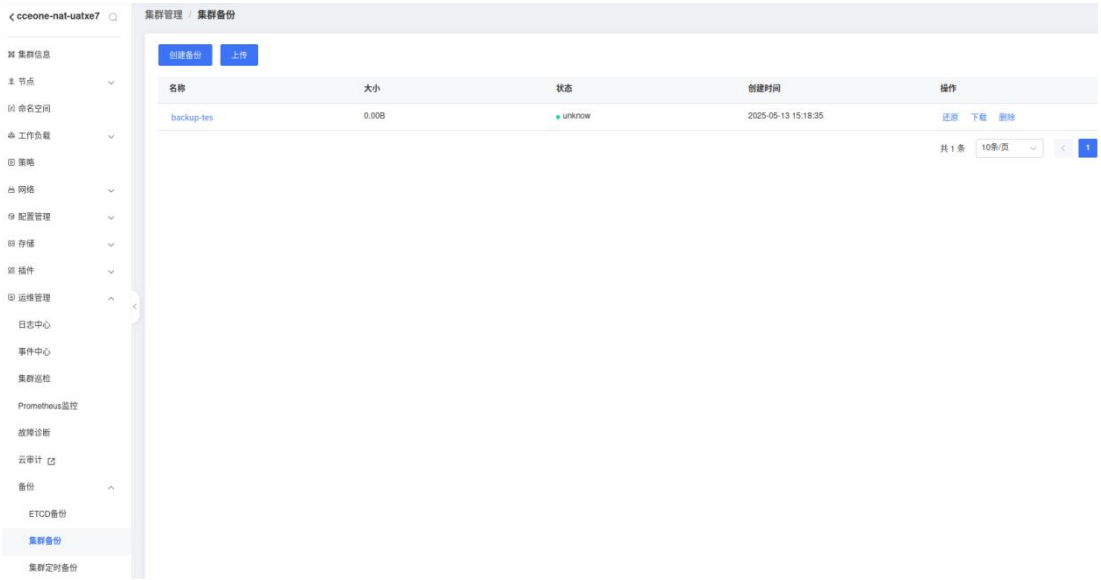
```
docker@debian:~$ kubectl get service -A
NAMESPACE     NAME            TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)                  AGE
default       kubernetes      ClusterIP   10.96.0.1       <none>        443/TCP                  46m
default       nginx-service   ClusterIP   10.96.158.161   <none>        80/TCP                   84s
```

步骤二：在自建 Kubernetes 集群备份应用

由于本地集群已接入分布式容器云平台 CCE One 注册集群，因此可在控制台上进行备份任务操作，具体步骤如下：

- 在 CCE One 集群管理页面，找到对应的本地注册集群，点击进入云上单集群控制台；
- 进入【运维管理】->【备份】，然后按需选择【集群备份】；
- 首次进入该页面，将检查 ccse-backup 插件的安装情况，若当前该插件还未安装，会有对应流程提示；请参考流程指引，部署并配置 ccse-backup 插件的运行参数；
- 创建集群备份任务，等待备份任务执行完成；

具体操作，请参考云容器引擎 - 集群备份



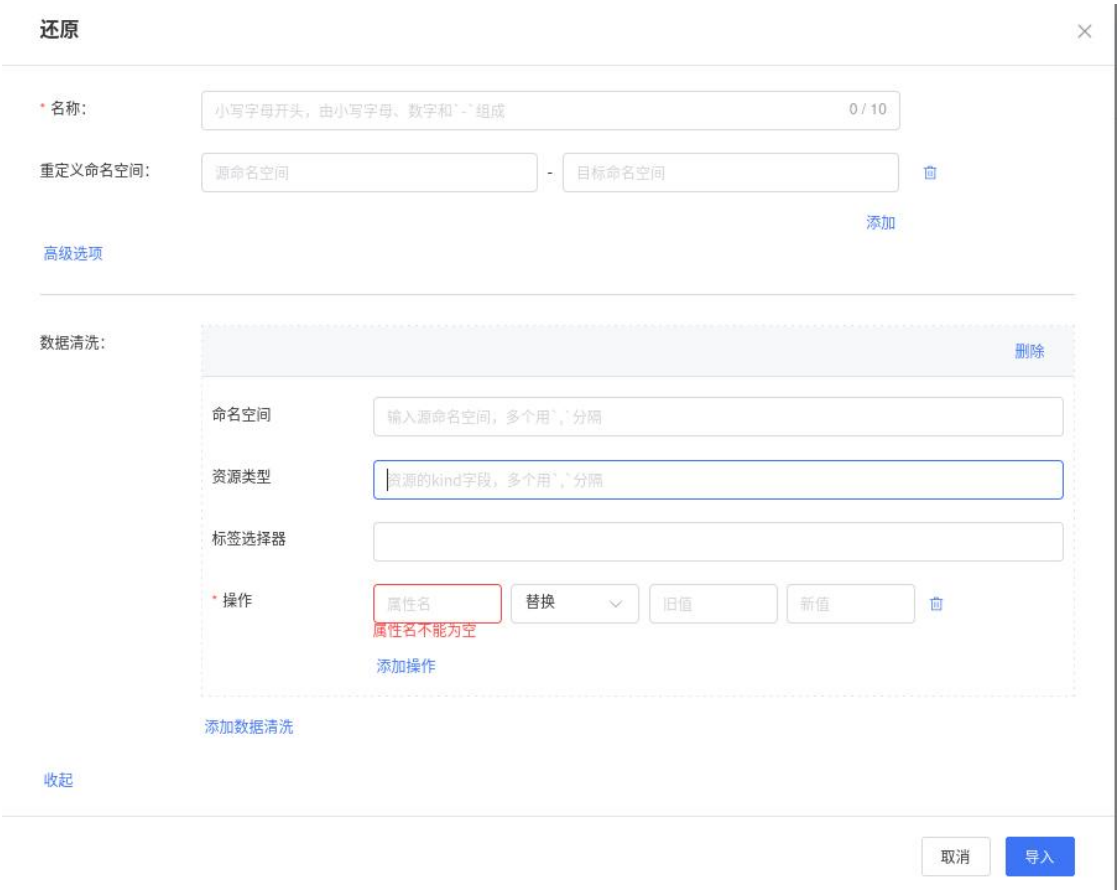
步骤三：在线上 CCE 集群中恢复应用

若只是本集群按需恢复，则可以在对应备份任务操作中，点击【还原】并再次点击确认即可；

若需要在天翼云上的其他 CCE 注册集群中恢复应用，则可以参考如下步骤：

- 将天翼云 CCE 集群关联到 CCE One 注册集群中来；
- 进入天翼云 CCE 注册集群控制台，选择【运维管理】->【备份】->【集群备份】->【上传】，将源集群中备份下载的副本，上传到目标集群的集群备份列表中；
- 点击操作中的【还原】，并按需选择命名空间重命名和数据清洗配置；

跨集群数据恢复场景，建议通过【数据清洗】配置，快速完成镜像地址、PVC StorageClass 等差异化配置的替换；



等待以上【还原】任务执行完成后，进入目标集群中检查 workload 运行状态。预期输出如下：

```
docker@debian:~$ kubectl get pod -A
NAMESPACE           NAME                                READY   STATUS    RESTARTS      AGE
default             nginx-deployment-67dffbbbb-nct47    1/1     Running   0             5s
```

设置 kubectl proxy，尝试访问服务：

```
docker@debian:~$ kubectl proxy
Starting to serve on 127.0.0.1:8001
```

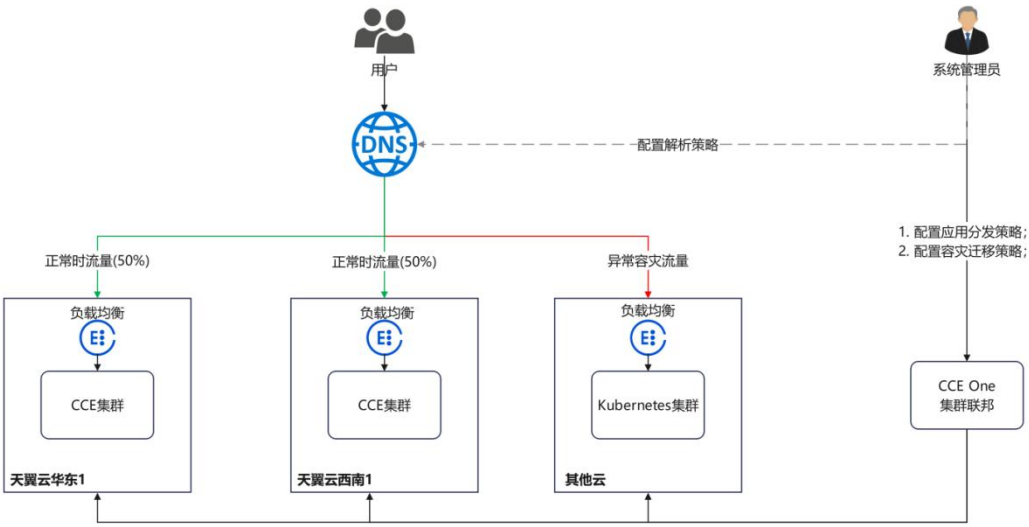
```
docker@debian:~$ curl http://localhost:8001/api/v1/namespaces/default/services/nginx-service/proxy/
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</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>
```

验证目标集群中应用服务访问正常，应用迁移完成；

4.6.1.3 跨集群跨地域容灾迁移

为了应对集群单点宕机故障，分布式容器云平台 CCE One 的集群联邦提供多集群多活应用、秒级流量接管能力。业务应用的实例可以多集群多活的部署在不同容器集群服务中，当集群单点宕机故障发生时，集群联邦可以秒级自动完成应用实例的弹性迁移以及流量的切换，业务的可靠性大幅提升。

多活容灾方案示意如下图所示，通过创建域名访问规则，将应用分发到多个 Kubernetes 集群，包括两个天翼云 CCE 集群（部署在不同 Region）和一个其他云的 Kubernetes 集群，实现应用的多活容灾。



前提条件

已开通一个天翼云 CCE 集群和一个三方云集群。

已订购具备策略解析能力的公网 DNS 服务，例如 GTM 等；天翼云当前无此类产品售卖，因此需要用户自行准备，或找专门的 DNS 服务提供商购买。

适用场景

对应用容灾高可用有较高要求，希望实现业务极致弹性及高可用的场景。

操作指引

本文将基于天翼云 CCE 集群和阿里云 ACK 集群，演示如何实现多集群应用容灾与自动迁移能力。

步骤一：将天翼云 CCE 集群及三方云集群，注册到 CCE One，并加入联邦成员中

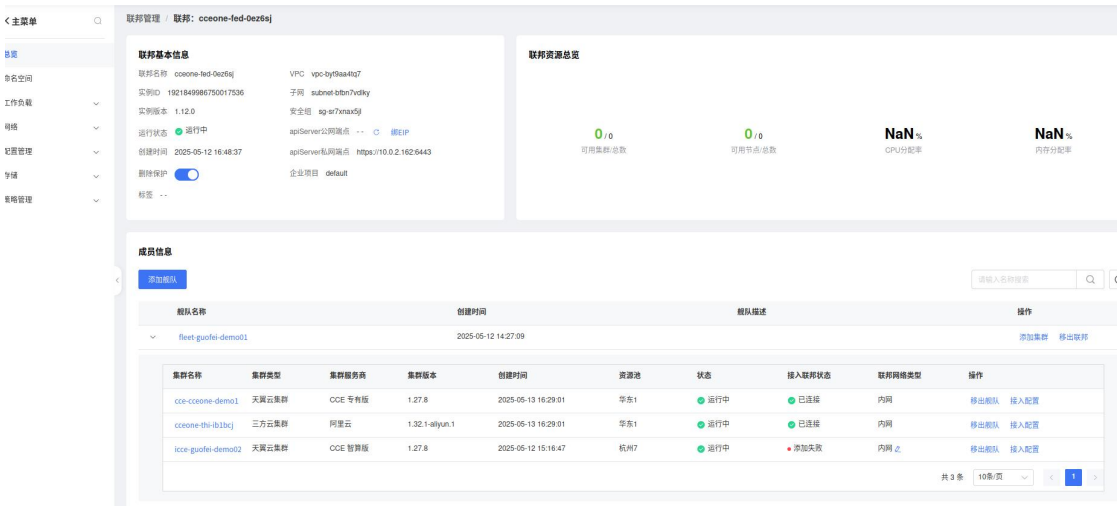
在【集群资源】->【注册集群】页面，选择天翼云类型注册集群，并根据指引将提前创建的天翼云 CCE 集群和阿里云 ACK 集群关联进来；

进入【舰队管理】页面，创建舰队并添加上面关联的两个 CCE One 注册集群；

进入【联邦管理】页面，根据指引订购集群联邦实例，并将联邦实例与上面的舰队进行关联；

由于舰队中成员集群与联邦存在跨资源池情况，联邦联通网络可能需要用户手工干预才能联通；具体可参考指引　打通注册集群与联邦实例之间的联通网络

如下图所示：　已成功注册到联邦的成员集群，其【接入联邦状态】应为“已连接”；若连接状态为“添加失败”，则可以参考上面指引进行网络配置调整，并修改【联邦网络类型】到对应类型后，触发后台再次自动尝试连接。



步骤二：创建联邦工作负载及其访问路由

为展示流量切换的效果，本文中两个集群的容器镜像版本不同（实际生产环境中并不会存在此差异）。

集群 cce-cceone-demo1：示例应用使用 nginx:cce 镜像，返回“this is cce cluster application”。

集群 cceone-thi-ib1bcj：示例应用使用 nginx:aliyun 镜像，返回“this is aliyun cluster application”。

在开始操作之前，您需要将示例应用的镜像上传到对应集群所在区域的镜像仓库中（也就是说，nginx:cce 镜像需要上传至天翼云华东 1，nginx:aliyun 镜像上传至阿里云），否则联邦工作负载会因拉取不到镜像而异常。

登录 CCE One 控制台，选择左侧导航栏中的“舰队联邦”->“联邦管理”。

单击对应联邦实例名称，进入详情页面。

在左侧导航栏选择“工作负载->无状态”，单击右上角“创建 Deployment”。

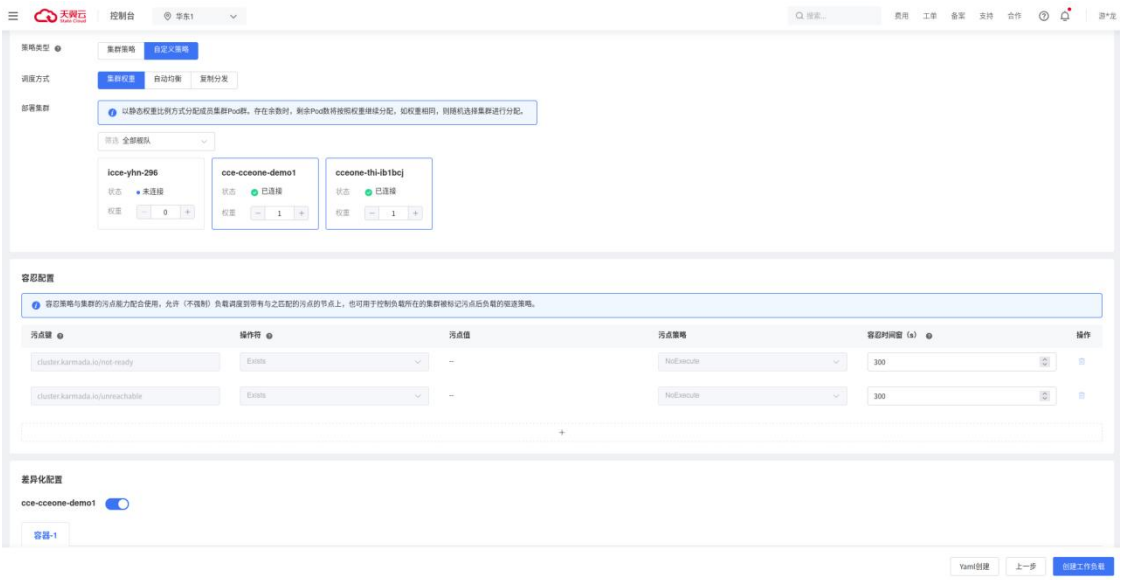
填写基本信息并配置容器参数，镜像可以任意设置，单击“下一步：调度与差异化”。

设置集群调度策略，完成集群差异化配置，单击“创建工作负载”。

调度方式：选择“集群权重”，并设置两个集群的权重为 1:1。

差异化配置：单击集群左侧的开关图标开启差异化配置，设置集群 cce-cceone-demo1 的镜像名称为

“registry-huadong1.crs-internal.ctyun.cn/open-source/nginx:cc”（nginx:cce 镜像在镜像仓库中的地址，请以实际为准），集群 cceone-thi-ib1bcj 的镜像名称请改为上传到阿里云中的实际镜像地址。



6. 创建 LoadBalancer 访问 service

登录天翼云 CCE One 控制台，选择左侧导航栏中的“舰队联邦”->“联邦管理”。

单击对应联邦实例名称，进入详情页面。

在左侧导航栏选择“服务”，单击左上角“创建服务”。

完成参数填写，单击“确认”。

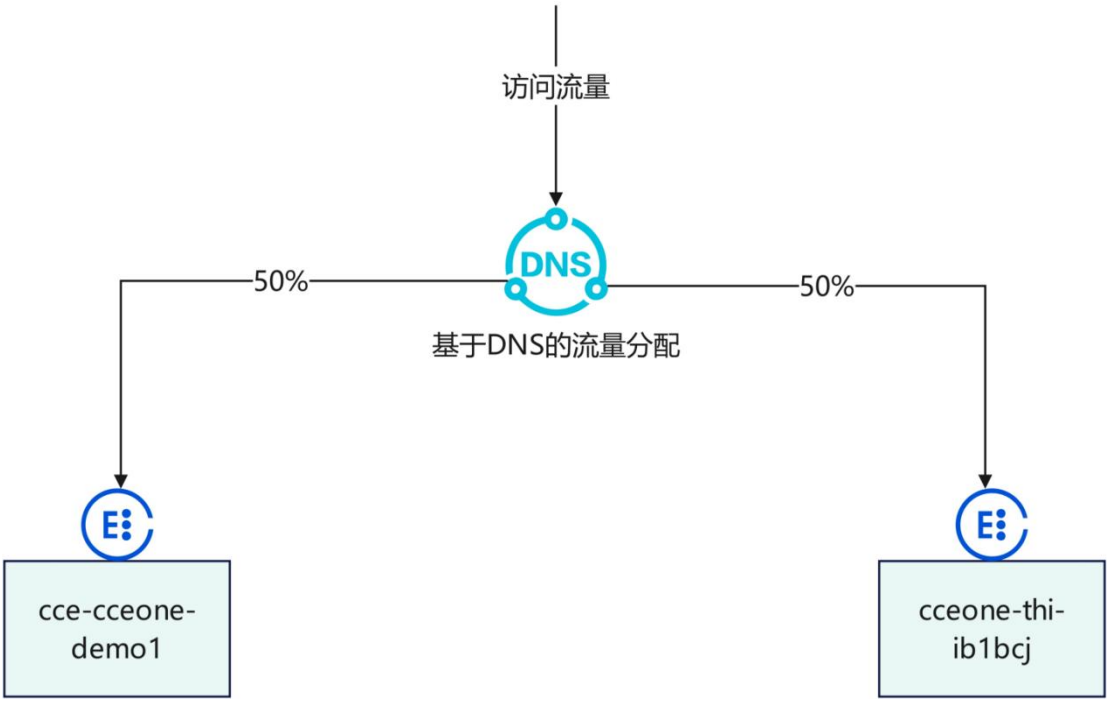
- 访问类型：选择“负载均衡”。
- 端口配置：选择 TCP 协议，填写服务端口、容器端口，如 8800、80。

需要结合差异化策略，确保 service 下发到成员集群后，可以触发对应成员集群中 LB 类型 Service 的正常创建；

7. 创建域名访问

可以基于 IDC 自建 DNS 或专业供应商的 DNS 解析服务进行配置，需要具备策略解析能力；

获取上一步各个成员集群中最终创建 LB 类型 Service 访问 IP，并配置到 DNS 解析记录中，配置对应解析权重 1:1



步骤三：多活容灾场景验证

按照上述集群应用部署操作，示例应用分别部署在集群“cce-cceone-demo1”和“cceone-thi-ib1bcj”中，并以“负载均衡”类型的服务对外提供访问。步骤二中域名访问创建成功后，可以得到一个可以公网解析和访问的域名，我们可以基于该域名来验证其实际访问和容灾能力。

获取验证测试访问域名。假设为“cceone-test.ctyun.cn”；

在一台已连接公网的机器上执行如下命令，持续访问域名地址，查看集群应用处理状态；正常情况下，两个集群上的应用均接收流量，并且各处理 50%流量。

注意： 测试命令应使用 wget 而非 ping，以便每次访问目标服务均可完整的经历域名解析逻辑；

```
while true;do wget -q -O- cceone-test.ctyun.cn:8800; done
this is cce cluster application.
this is cce cluster application.
this is cce cluster application.
this is cce cluster application.
this is cce cluster application.
this is cce cluster application.
```

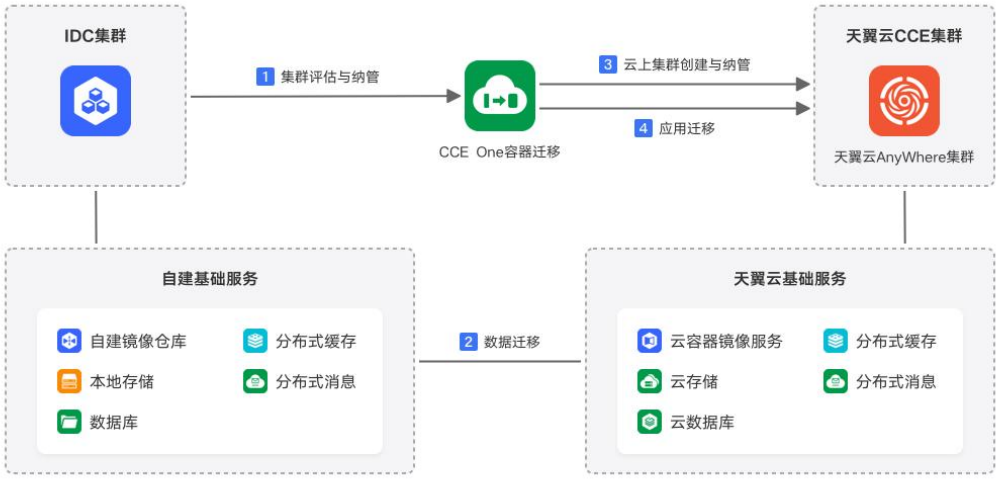
3. 当集群 cceone-thi-ib1bcj 上的应用异常时（通过集群节点关机来模拟应用异常），系统将所有的流量路由到 cce-cceone-demo1 集群处理，用户感知不到异常。

4.6.2. 应用迁移

场景	说明
本地 IDC 迁移上云	本地 IDC 迁移上云：将位于本地数据中心的 Kubernetes 集群迁移到天翼云 CCE One 管理的 Kubernetes 集群，实现应用程序的云端部署和运维管理。
三方云集群跨云迁移	将位于其他云服务提供商的 Kubernetes 集群迁移到天翼云 CCE One 管理的 Kubernetes 集群，实现跨云迁移和统一管理。
天翼云 CCE 集群间迁移（同资源池）	在同一地理区域内的天翼云 CCE One 管理的 Kubernetes 集群间进行迁移，实现资源优化、应用升级或其他管理需求。
天翼云 CCE 集群间迁移（跨资源池）	在天翼云 CCE One 管理的 Kubernetes 集群间进行迁移，将应用程序从一个地理区域迁移到另一个地理区域，以满足数据合规性、延迟和可用性等需求。

4.6.2.1 本地 IDC 集群应用迁移到天翼云 CCE 集群

分布式容器云平台 CCE One 容器迁移功能，支持将本地 IDC 自建的 Kubernetes 集群应用迁移到天翼云 CCE 集群，实现应用程序的云端部署和运维管理。迁移流程如下图所示：



前提条件

已开通天翼云分布式容器云平台 CCE One 及其关联产品的访问权限。

已打通 IDC 集群与天翼云资源池 VPC 网络，可选择公网或内网方式。其中：

- 公网方式：需要您 IDC 集群中 Pod 具备主动访问功能的能力，一般可通过配置集群公网 NAT 出口方式实现；
- 内网方式：需要将您 IDC 集群的网络与天翼云云上 VPC 网络打通，可选云专线、SD-WAN 或 VPN 方式；另还需参考配置指引，配置正确的云上云下网关路由及 DNS 解析转发策略，以确保云下可正常访问云上相关服务；

适用场景

云备份容灾：备份容灾迁移一体化，快速实现应用上云与数据灾备。

操作指引

本场景迁移，主要包含四个步骤：

步骤一：集群评估与纳管

在这个阶段，您将根据源集群的现状来评估适合迁移的目标集群类型。可以基于必要的开源工具自动或手工收集源集群的信息，包括 Kubernetes 版本、规模、工作负载、存储等数据，并根据收集到的数据考虑合适的目标集群信息。

为方便后续的数据备份与恢复，或者基于联邦的细粒度应用迁移，您需要将源集群注册到天翼云 CCE One 注册集群；

步骤二：数据迁移

在这个阶段，您将把镜像和相关依赖服务的数据迁移到云端。可基于天翼云上提供的专业云迁移、云备份等迁移工具，或基于云产品提供的专门迁移指引进行迁移。例如：

- 自建镜像仓库迁移请参考：迁移自建 Harbor 至容器镜像服务企业版
- 自建数据库如 mysql 迁移请参考：本地 MySql 迁移到 RDS For MySQL
- 自建 PostgreSQL 迁移请参考：本地 PostgreSQL 迁移到 RDS For PostgreSQL
- 自建 Redis 迁移请参考：自建 Redis 迁移到 DCS

其他类型存储迁移，请参考天翼云上对应云产品提供的迁移指引；

步骤三：云上集群创建与纳管

在这个阶段，您将评估目标集群所需规格信息并创建对应的天翼云 CCE 集群；然后将该目标集群关联到分布式容器云平台 CCE One 注册集群；

云容器引擎允许用户对集群资源进行个性化选取，以精准匹配其多样化的业务诉

求。如下所示的表中，列举了集群的指标参数，并提供了参考规划选择；用户应依据自身业务的确切需求，对相关设置做出合理调配，其间，我们建议尽可能保持与原集群性能配置的一致性水平。

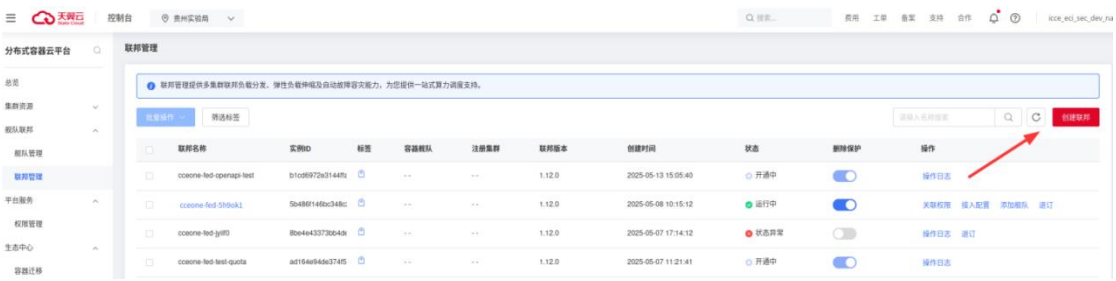
在目标 CCE 集群创建好后，需要进入天翼云分布式容器云平台 CCE One 控制台，将目标 CCE 集群关联到 CCE One 的注册集群以便支持后期的纳管与联邦调度能力；

步骤四：应用迁移

在这个阶段，您将利用 CCE One 集群联邦多集群应用调度能力，将您本地 IDC 中的应用迁移到天翼云 CCE 注册集群。

1．订购天翼云 CCE One 集群联邦实例，并将 IDC 源集群和目标天翼云 CCE 集群作为成员加入联邦（通过舰队绑定）；

应用迁移需要基于集群联邦控制面来完成，因此需要用户首先在 CCE One 联邦管理界面首先创建一个联邦实例。

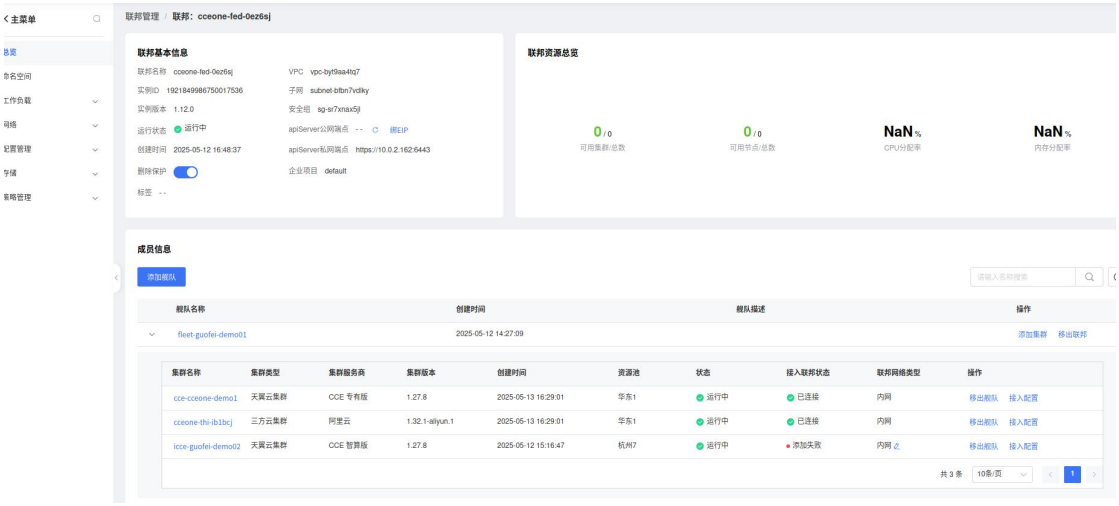


联邦实例只可以关联一个舰队，注册集群可以加入舰队；注册集群加入已关联联邦的舰队时，即自动作为成员集群加入该联邦。

成员集群和联邦实例之间涉及网络链路打通，建议优先将相关注册集群和联邦创建到相同的资源池和 VPC 下，这样可以默认内网互通并且无任何额外成本；若源和目标注册集群的确需要跨资源池，可参考指引《打通注册集群与联邦实例之间的联通网络》配置网络，并选择正确的接入链路类型以确保成员集群、联邦网

络互通。

成员集群加入联邦成功后，在总览页面，可看到成员集群列表的“接入联邦状态”列，均显示为“已联通”。



2. 将需要迁移的工作负载或相关服务，提升到集群联邦控制面管理；

成员集群加入联邦后，其内部署的工作负载、Service、ConfigMap 等还无法通过联邦进行调度，需要首先将相关资源 YAML 作为配置模板提升到联邦控制面管理，此后，才能再基于联邦进行该工作负载的多集群调度分发。

底层集群工作负载提升到联邦控制面管理的方式有两种，对原始工作负载的影响也不同。需要业务按自身需求按需选择：

方式一：工作负载维度接管，并且原集群中工作负载 Pod 不重启；

假设成员集群 member1 中存在工作负载 default/nginx，其状态为 running：

我们可以基于联邦控制面 kubectl 方式，执行以下命令来将其提升到联邦控制面管理：

```
[root@master1]# karmadactl promote deployment nginx -n default -c member1

Resource "apps/v1, Resource=deployments"(default/nginx) is promoted successfully
```

此时，再在联邦控制面中查询该工作负载，可看到已经可以查询到，说明已被联邦实例接管：

```
[root@cluster1]# kubectl get pod
NAME                          READY    STATUS        RESTARTS    AGE
nginx-6799fc88d8-sqjj4        1/1      Running       0           15m
```

检查成员集群中对应 nginx 无状态工作负载，对应 Pod 并未重启：

```
[root@cluster1]# kubectl get deploy nginx
NAME     READY    UP-TO-DATE    AVAILABLE    AGE
nginx    1/1      1             1            66s

[root@cluster1]# kubectl get pod
NAME                          READY    STATUS        RESTARTS    AGE
nginx-6799fc88d8-sqjj4        1/1      Running       0           2m12s
```

方式二：批量提升接管，原集群中工作负载 Pod 会重启；

对于希望批量提升到联邦控制面接管，以及对 Pod 重启无感知的服务或资源，可考虑采用本方式，其执行效率相对更高。

在成员集群中已部署服务非常多或应用较复杂情况下，该方式更适合。可基于更大的粒度，来做资源的接管和提升，例如：

- 以资源为粒度，迁移某种类型的全部资源
- 以应用为粒度，迁移某个应用涉及的所有类型的资源

此时，就需要资源模板结合集群联邦的调度策略 PropagationPolicy，来接管相应资源，可以按如下方式操作。

a.将所有资源的 YAML 配置应用到 集群联邦控制面，作为集群联邦的 ResourceTemplate。此时，资源模板只会存在联邦控制面，并不会下发任何成员集群；

b.编写 PropagationPolicy 调度策略， 并将其应用到集群联邦控制面。 您需

要注意以下两个字段：

- spec.conflictResolution: Overwrite：该字段的值必须是 Overwrite。
- spec.resourceSelectors：指定哪些资源需要被迁移。

如果你希望的是将所有 Deployment 资源提升到联邦控制面管理，则可以配置类似如下的调度策略：

```
apiVersion: policy.karmada.io/v1alpha1
kind: PropagationPolicy
metadata:
  name: deployments-pp
spec:
  conflictResolution: Overwrite
  placement:
    clusterAffinity:
      clusterNames:
      - member1
  priority: 0
  resourceSelectors:
  - apiVersion: apps/v1
    kind: Deployment
  schedulerName: default-scheduler
```

当前，除了 YAML 方式创建外，也支持基于前端页面的引导创建。可进入联邦控制台->策略管理->调度策略->创建调度策略页面进行配置；

在编辑页面中，直接跳过模板配置步骤，进入调度与差异化配置页面。通过设置调整集群调度策略，可将工作负载复制分发到目标集群，或按权重拆分部分副本到新集群。如下：

如上图配置，提交更新后，工作负载将在源集群和目标集群中 1:1 比例部署。

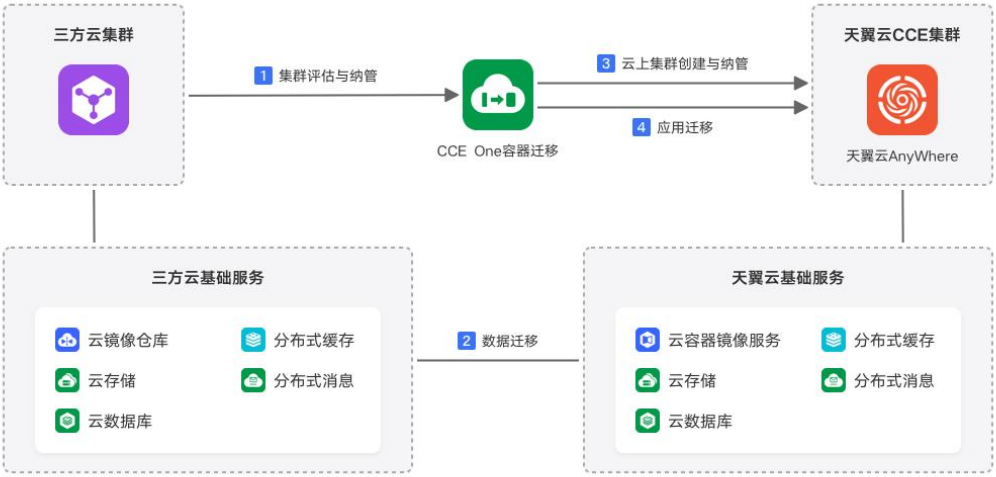
4. 服务验证及终端灰度切流；

该步骤中，用户可基于应用实际架构及服务需求，在验证目标成员服务正常后，实施真实用户流量的逐步切流；

切流过程中，可配合通过调度策略逐步调整工作负载 Pod 副本在源集群与目标集群之间的分布，并最终全部迁移到天翼云上 CCE 集群，以实现完整的切流；

4.6.2.2 三方云集群应用迁移到天翼云 CCE 集群

分布式容器云平台 CCE One 容器迁移功能，支持将三方云标准 Kubernetes 集群应用迁移到天翼云 CCE 集群，实现应用程序的跨云迁移和统一运维管理。迁移流程如下图所示：



前提条件

已开通天翼云分布式容器云平台 CCE One 及其关联产品的访问权限。

已打通三方云容器集群与天翼云资源池 VPC 网络，可选择公网或内网方式。其中：

- 公网方式（推荐）：需要您三方云集群中 Pod 具备主动访问功能的能力，可通过给容器集群 VPC 配置公网 NAT 出口方式实现；
- 内网方式：需要您将三方云容器网络与天翼云云上 VPC 网络打通；可选云专线、SD-WAN 或 VPN 方式；另还需参考配置指引，配置正确的云间网关路由及 DNS 解析转发策略，以确保您三方云容器 Pod 中可正常访问天翼云相关服务；

适用场景

云备份容灾：备份容灾迁移一体化，快速实现应用云间迁移与数据灾备。

操作指引

参考《本地 IDC 集群应用迁移上云》，只数据迁移部分有所差别。

步骤二：数据迁移

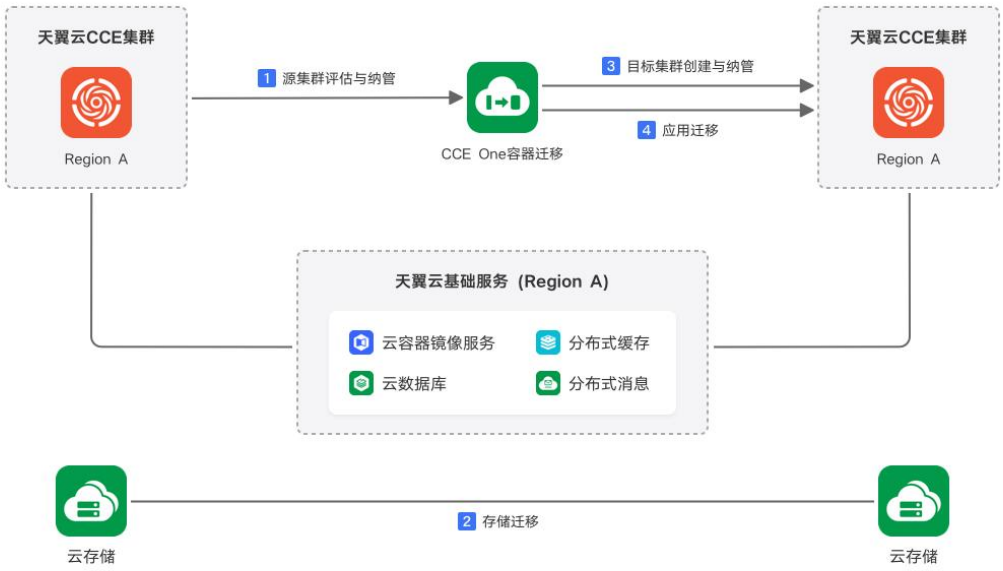
在这个阶段，您将把镜像和相关依赖服务的数据迁移到天翼云对应云产品中。可基于天翼云上提供的专业云迁移、云备份等迁移工具，或基于云产品提供的专门迁移指引进行迁移。例如：

- 三方云镜像仓库迁移参考：第三方镜像仓库导入
- 三方云 MySQL 迁移请参考：其他云 MySQL 迁移到 RDS For MySQL
- 三方云 PostgreSQL 迁移请参考：其他云 PostgreSQL 迁移到 RDS For PostgreSQL

其他类型存储迁移，请参考天翼云上对应云产品提供的迁移指引；

4.6.2.3 天翼云 CCE 集群间应用迁移（同资源池）

在同一地理区域内的天翼云 CCE One 管理的 Kubernetes 集群间进行迁移，实现资源优化、应用升级或其他管理需求。其迁移流程如下图所示：



前提条件

已开通天翼云分布式容器云平台 CCE One 及其关联产品的访问权限。

同资源池情况下，CCE One 联邦自动打通与成员集群之间的管理网络（同 VPC 或跨 VPC 均可），无需用户额外配置操作。

适用场景

云上资源优化、应用升级或其他管理需求场景。

操作指引

具体参考《本地 IDC 集群应用迁移上云》，只数据迁移部分有所差异。

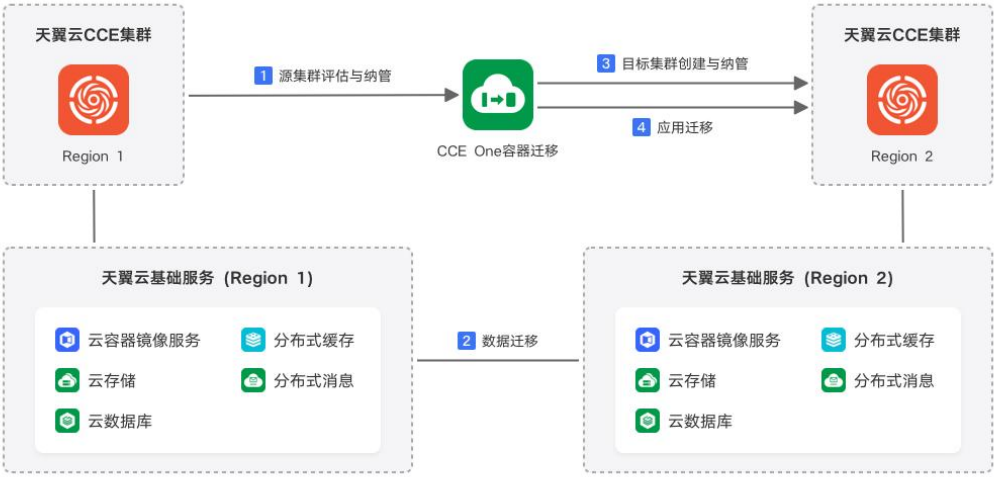
步骤二：数据迁移

若您的集群使用了云硬盘，需要随集群一起迁往目标 AZ，可以通过云备份服务创建云硬盘备份，再使用备份创建新的云硬盘，在配置云硬盘信息时，选择目标可用区即可。

- 具体操作参考：云硬盘备份与恢复 以及 云硬盘数据跨可用区迁移

4.6.2.4 天翼云 CCE 集群间应用迁移（跨资源池）

在天翼云 CCE One 管理的注册集群间进行迁移，将应用程序从一个地理区域迁移到另一个地理区域，以满足数据合规性、延迟和可用性等需求。迁移流程图参考如下：



前提条件

已开通天翼云分布式容器云平台 CCE One 及其关联产品的访问权限。

成员集群跨资源池情况下，需要打通成员集群与联邦实例的控制面网络。可选公网、内网（云间高速）等方式：

- 公网：需要确保成员集群 apiserver ELB 有绑定公网 EIP，以及联邦所在 VPC 有配置公网 SNAT，具备主动访问公网的能力；
- 内网（云间高速）：所源、目的集群所在 VPC 不存在网络冲突，可完全内网打通时，可考虑云间高速内网方式；具体配置方式参考：跨区域 VPC 互通；

适用场景

数据合规性、延迟和可用性等需求场景。

操作指引

详情参考《天翼云 CCE 集群间应用迁移（同资源池）》，只数据迁移部分有差异。

步骤二：数据迁移

本步骤中，您将对集群依赖服务的数据服务，例如镜像及云存储、云数据库、分布式缓存、分布式消息等，进行跨资源池迁移。

容器镜像跨资源池同步参考：同账号跨实例同步；

云数据库迁移，可使用数据复制服务 CT-DRS；CT-DRS 是天翼云为上云用户提供的一种易用、稳定、高效、用于数据库在线迁移的云服务，可解决多场景下数据库之间数据流通问题，满足数据传输业务需求，同时减少数据传输成本；

其他云上数据迁移需求，请参考对应云产品提供的迁移服务及指引。

4.6.2.5 非纳管方式将本地及三方 Kubernetes 集群应用迁移到天翼云 CCE 集群

若本地或三方云集群，无法通过公网/内网方式纳管到天翼云分布式容器云平台 CCE One 时，将不能使用三方单集群控制台相关运维能力，也即无法通过前端操作指引方式对集群应用进行必要的备份和恢复。此时，可考虑通过登录用户集群离线备份恢复方式进行操作。

注意：

- 由于迁移的源/目标集群任意之一无法被纳管到天翼云 CCE One 注册集群，如下备份/恢复操作均为离线操作。理论上可独立于天翼云环境。
- 如下将仅以天翼云提供的 ccse-backup 插件为例进行介绍；当然，您也可以选择基于三方或开源工具来进行集群备份和恢复，例如也可选择开源 Velero，此时操作步骤请参考其官方指引。

1. 创建 ccseone-managed 命名空间和对应的 sa

在迁移源和目标集群均需进行如下 YAML 创建：

```
apiVersion: v1
kind: Namespace
metadata:
  name: ccseone-managed
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: ccseone-backup
rules:
  - apiGroups: ["*"]
    resources: ["*"]
    verbs: ["*"]---
apiVersion: v1
kind: ServiceAccount
metadata:
  labels:
    component: ccseone-backup
  name: ccseone-backup
  namespace: ccseone-managed
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    component: ccseone-backup
  name: ccseone-backup
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ccseone-backup
subjects:
  - kind: ServiceAccount
    name: ccseone-backup
    namespace: ccseone-managed
```

2. 安装 helm，然后使用 helm 安装 ccse-backup-1.0.4.tgz

在迁移源和目标集群均需进行该步骤操作。

通过 helm 创建以及标准创建情况下，依赖从天翼云 CRS 拉取相关 helm 配置及镜像地址，需要打通与云上服务的公网或内网访问通道。

3. 源集群应用备份

提前创建 oss 桶，然后登录到待备份集群，编写备份 job，job 的编写可参考 backupexport.yaml，将存储桶的相关配置填写至 pod 的环境变量当中，注意配置待备份的命名空间以及对象。

```
apiVersion: batch/v1
kind: Job
metadata:
  name: ccseone-backup-01
  namespace: ccseone-managed
spec:  # 如果 job 在 900s 内没有完成，将被系统终止
  activeDeadlineSeconds: 900
  # 自动重试次数设为 0，意味着如果 Job 失败，不会自动重试
  backoffLimit: 0
  # 不用索引模式来处理完成状态
  completionMode: NonIndexed  # Job 完成所需的成功次数设为 1
  completions: 1
  # job 的并行执行个数设为 1，表示同一时间只有一个 Pod 实例在运行
  parallelism: 1
  # Job 是否可被暂停，false 为不可暂停
  suspend: false
  template:
    spec:
      containers:
      - command:
        - ./backup
        - export
        - --exportName=ccseone-backup-01
        - --clusterId=localcluster
        - --jobName=ccseone-backup-01          # 命名空间，按需更改
        - --includeNs=default          # k8s 资源，要求 pv 和 pvc，按需更改
        - --includeRs=pod,PersistentVolume,PersistentVolumeClaim,configmap          # 需声明
需要备份 pv
        - --backupPv=true
        env:
        - name: OSS_PROVIDER
          value: s3
        - name: OSS_ACCESS_KEY_ID
          value: a123456
        - name: OSS_ACCESS_KEY_SECRET
          value: a123456
        - name: OSS_BUCKET
          value: a123456
        - name: OSS_ENDPOINT
          value: 127.0.0.1:1234          # 镜像来源：按需更改
        image: ***.ctyun.cn/library/backup:1.3.1
        imagePullPolicy: IfNotPresent
        name: ccseone-backup-01
      dnsPolicy: ClusterFirst
      restartPolicy: Never
      schedulerName: default-scheduler
      securityContext: {}
      serviceAccount: ccseone-backup
      serviceAccountName: ccseone-backup
      terminationGracePeriodSeconds: 30
```

执行 kubectl apply -f ，将 job 部署在待备份集群

4. 在目标集群中进行应用恢复

登录到待恢复集群，编写恢复 job，job 的编写可参考 backupimport.yaml，将存储桶的相关配置填写至 pod 的环境变量当中，注意配置待备份的命名空间以及对象。

```
apiVersion: batch/v1
kind: Job
metadata:
  name: ccseone-backup-01
  namespace: ccseone-managed
spec:  # 如果 job 在 900s 内没有完成，将被系统终止
  activeDeadlineSeconds: 900
  # 自动重试次数设为 0，意味着如果 Job 失败，不会自动重试
  backoffLimit: 0
  # 不用索引模式来处理完成状态
  completionMode: NonIndexed  # Job 完成所需的成功次数设为 1
  completions: 1
  # job 的并行执行个数设为 1，表示同一时间只有一个 Pod 实例在运行
  parallelism: 1
  # Job 是否可被暂停，false 为不可暂停
  suspend: false
  template:
    spec:
      containers:
      - command:
        - ./backup
        - export
        - --exportName=ccseone-backup-01
        - --clusterId=localcluster
        - --jobName=ccseone-backup-01          # 命名空间，按需更改
        - --includeNs=default          # k8s 资源，要求 pv 和 pvc，按需更改
        - --includeRs=pod,PersistentVolume,PersistentVolumeClaim,configmap          # 需声
明需要备份 pv
        - --backupPv=true
        env:
        - name: OSS_PROVIDER
          value: s3
        - name: OSS_ACCESS_KEY_ID
          value: a123456
        - name: OSS_ACCESS_KEY_SECRET
          value: a123456
        - name: OSS_BUCKET
          value: a123456
        - name: OSS_ENDPOINT
          value: 127.0.0.1:1234          # 镜像来源：按需更改
        image: ***.ctyun.cn/library/backup:1.3.1
        imagePullPolicy: IfNotPresent
        name: ccseone-backup-01
      dnsPolicy: ClusterFirst
      restartPolicy: Never
      schedulerName: default-scheduler
      securityContext: {}
      serviceAccount: ccseone-backup
      serviceAccountName: ccseone-backup
      terminationGracePeriodSeconds: 30
```

执行 kubectl apply -f ，将 job 部署在待恢复集群。

5.验证应用

根据业务规则验证已恢复应用的正确性。

5. 最佳实践

5.1. 通过注册集群统一管理任意环境下的 Kubernetes 集群

CCE One 注册集群可以帮助您快速实现 Kubernetes 集群注册到云端，使用天翼云容器管理控制台对注册集群进行统一管理，赋予云下集群使用云上资源能力。以下介绍如何通过注册集群统一管理任意环境下的 Kubernetes 集群。

5.1.1. 场景描述

统一管理天翼云集群：天翼云 CCE 专有版、托管版、智算版以及 Serverless 容器引擎 SCE 等。

统一管理本地集群：由 CCE 提供的运行在您数据中心基础设施之上的 Kubernetes 集群，以及满足 CNCF 标准的 IDC 自建的 Kubernetes 集群。

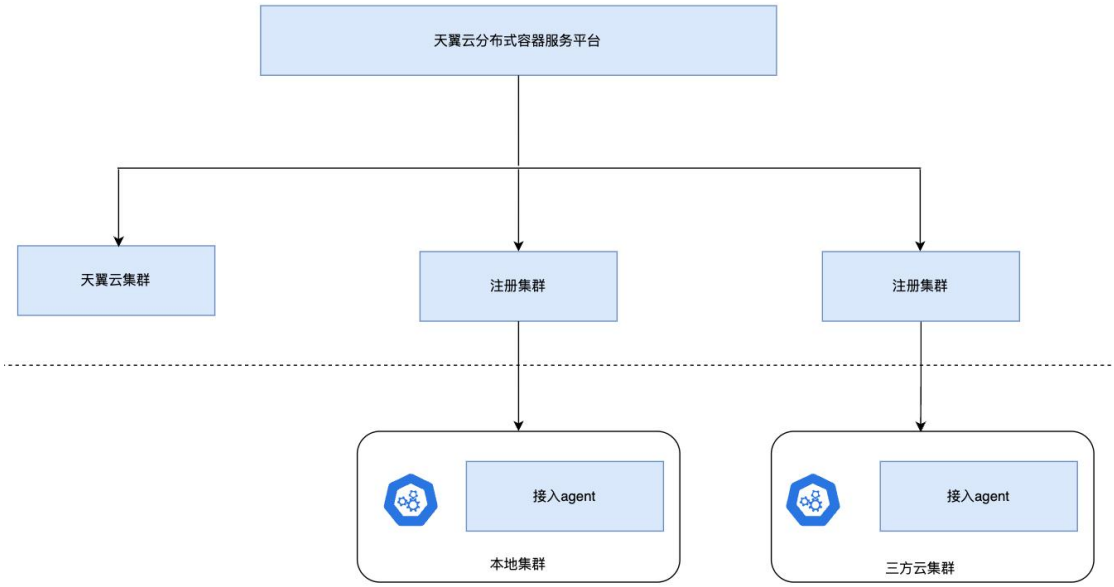
统一管理三方集群：三方公有云上提供的 Kubernetes 集群产品，如阿里云（ACK）、腾讯云（TKE）、GCP (GKE)、AWS（EKS）等。

5.1.2. 产品优势

云上云下集群统一管理，通过天翼云容器管理控制台，赋予云上云下集群可观测、服务治理、安全管理、协同调度等集群管理能力。

云下集群赋予云上能力，如通过接入云上 ECS、虚拟节点等扩展云下集群算力等。

5.1.3. 产品架构



5.1.4. 操作步骤

- 创建注册集群并接入 Kubernetes 集群，详细步骤见 本地注册集群、三方云注册集群。
- 使用天翼云容器管理控制台对接入集群进行管理。

5.2. 基于公司组织架构的权限设计及配置

为方便企业中的管理人员对集群中的资源权限进行管理，分布式容器云平台提供了多种维度的细粒度权限策略和管理方式。CCE 的权限管理包括“统一身份认证服务（IAM）授权”和“Kubernetes RBAC 授权”两种能力，AM 授权与基于 Kubernetes RBAC 能力的，两者是完全独立的，互不影响，但要配合使用。具体解释如下：

统一身份认证服务（IAM）授权： 是基于 IAM 策略的授权，可以让用户拥有集群管理、联邦管理、舰队管理等操作权限。

Kubernetes RBAC 授权：集群中 Kubernetes 资源权限是基于 Kubernetes

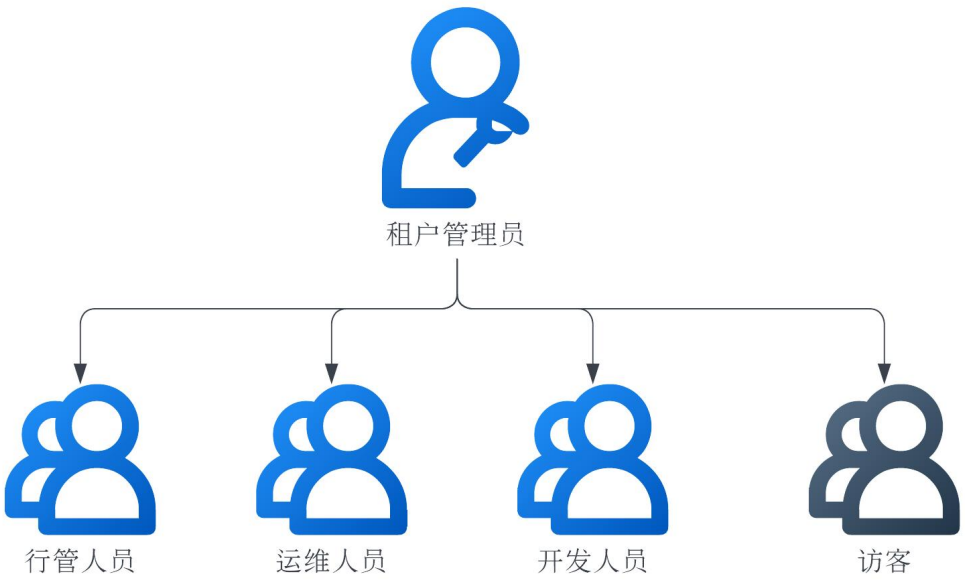
RBAC 能力的授权，通过权限设置可以让不同的用户或用户组拥有操作不同 Kubernetes 资源的权限。

假设 A 公司在分布式容器云平台管理多集群，公司中有多个职能团队，分别负责权限分配、资源管理、创建应用、流量分发、监控运维等。结合使用统一身份认证服务（IAM）与 Kubernetes RBAC 授权的权限管理，可以实现精细化授权的目标。

5.2.1. 权限涉及

下面我们以一个公司为例进行介绍。通常一个公司中有多个部门或项目，每个部门又有多个成员，所以在配置权限前需要先进行详细设计，并在设置权限之前提前为每个成员创建用户名，便于后续对用户进行用户组归属和权限设置。

下图为某公司某部门的结构示意图，我们将按照该设计对每个角色的权限设置进行演示。

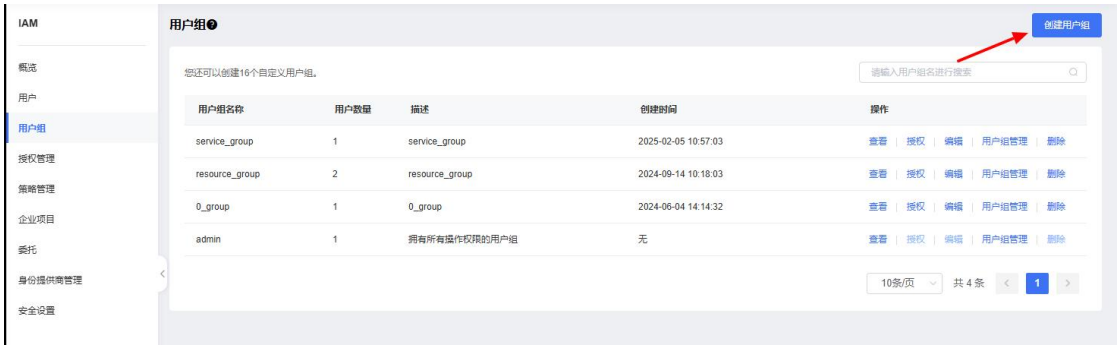


5.2.2. 租户管理员：IAM 授权

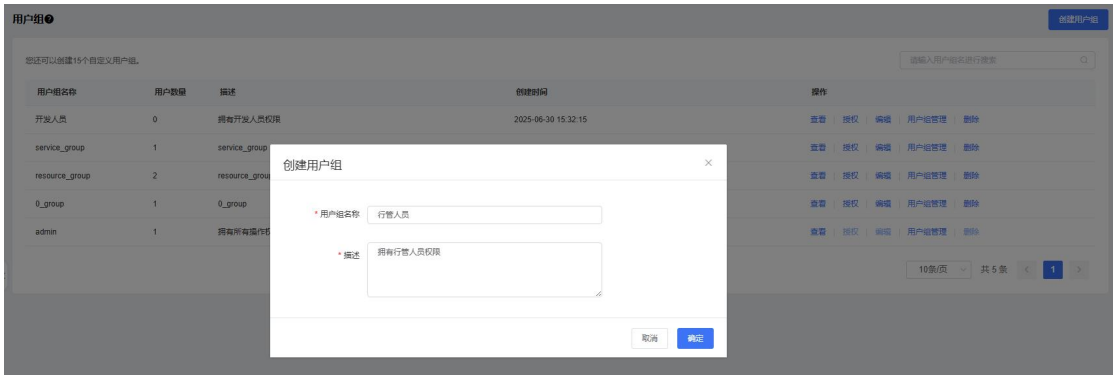
租户管理员拥有所有产品权限，负责给各个职能团队进行 IAM 授权，根据本例子的权限设计，首先创建 4 个用户组，分别是行管人员、运维人员、开发人员、访客人员，方便对员工分组管理。

创建用户组

打开 IAM 控制台页面，在左边侧边栏选择用户组，跳转到用户组页面，点击创建「创建用户组」按钮进行创建。

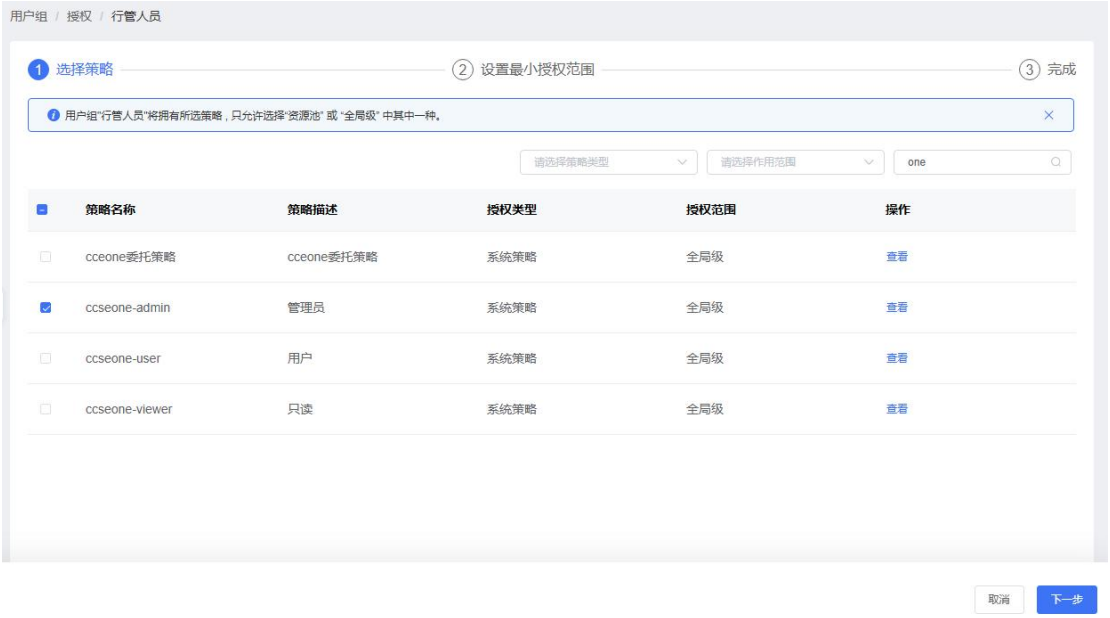


例如，为行管团队创建行管人员用户组



访问 IAM 用户管理页面，点击页面上的授权按钮进行操作，赋予用户组权限。

本例子将赋予「行管人员」用户组 ccseone-admin 权限。



5.2.3. 行管人员：搭建基础设施、配置权限策略

1. 创建注册集群、舰队和联邦

在上述步骤中，租户管理员向行政管理人员分配「ccseone-admin」权限。此权限允许行政管理人员创建注册集群、舰队和联邦等资源，从而利用分布式容器云平台搭建其基础设施。若需批量管理注册集群的权限，可将目标注册集群加入舰队，然后为相应的舰队成员用户赋予权限，实现统一管控。

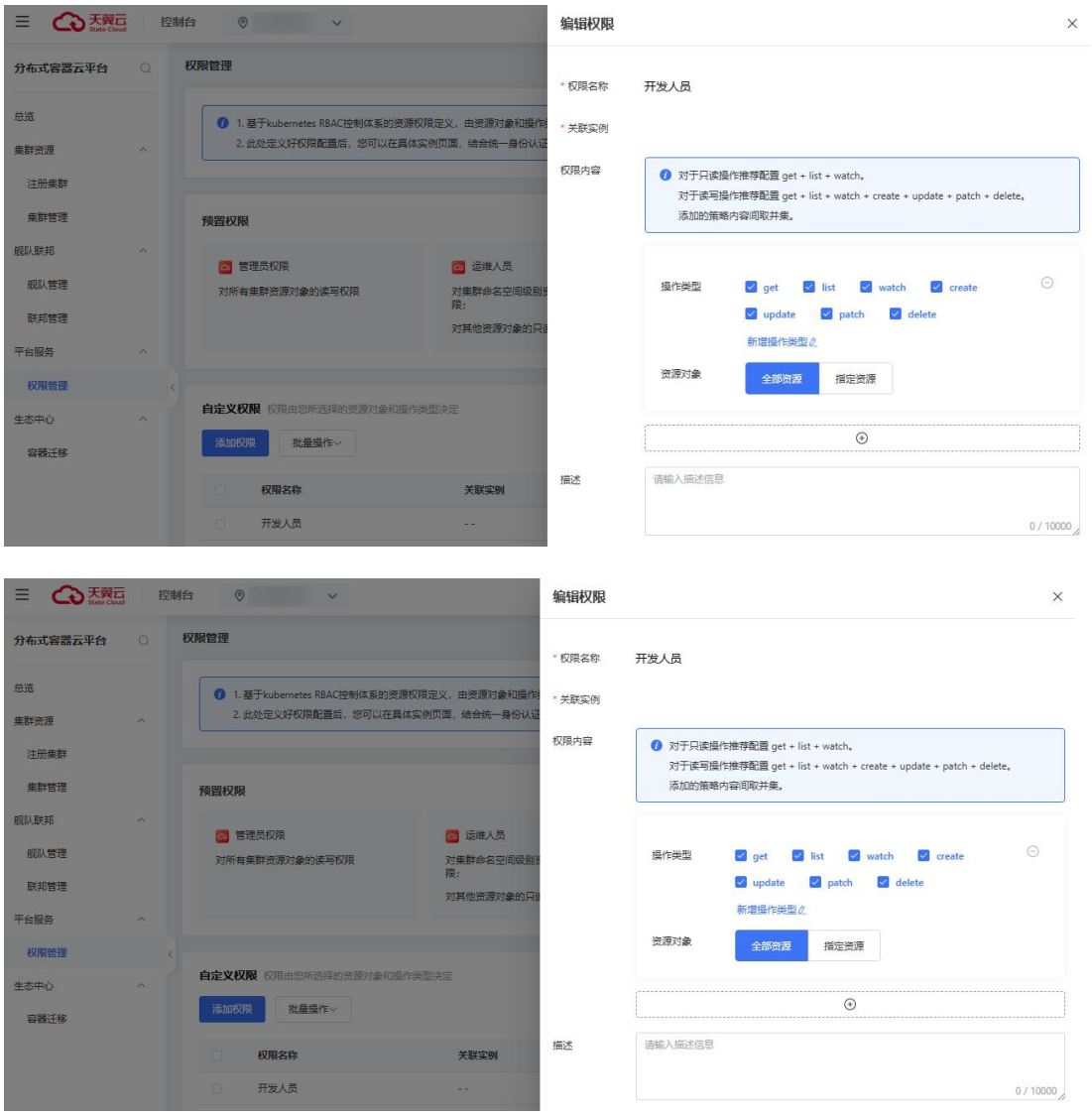
2. Kubernetes RBAC 授权

除了 IAM 授权，用户需要访问 Kubernetes 还需要进行 Kubernetes RBAC 授权。

配置 Kubernetes 权限策略

分布式容器云平台提供四种预置权限，同时支持用户灵活创建自定义权限。创建自定义权限，可访问分布式容器云平台「平台服务」-> 「权限管理」页面，

进行 Kubernetes 权限策略管理。



5.3. 基于集群联邦进行多集群应用分发与管理

CCE One 集群联邦支持通过 PropagationPolicy 定制资源模板分发策略，以及支持通过 OverridePolicy 来定制资源模板分发到不同成员集群的差异化配置。这里，我们以分发一个 Nginx Deployment Web 应用为例，简要介绍如何实现工作负载的多集群应用分发。

5.3.1. 前提条件

- 已开通 CCE One 集群联邦实例，可按需给 apiserver 绑定公网 EIP 以暴露到公网访问；
- 通过集群联邦接入配置，获取到联邦 apiserver 访问的 KubeConfig 文件；
- 联邦中有添加成员集群，且成员集群状态为 Ready（代表已联通）；

```
# 将如下‘/home/ctyun/.kube/cceone-fed.yaml’替换为您本地的联邦 KubeConfig 文件路径
# 集群状态 Ready=True 代表已正常接入，可进行应用分发

$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get cluster
NAME                    VERSION     MODE     READY     AGE
cce-cceone-demo1     v1.27.8     Push     True      16d
cce-cceone-demo2     v1.22.1     Push     True      56d
cceone-c2            v1.22.1     Push     True      55d
cceone-cluster1      v1.22.1     Push     True      55d
icce-yhn-296                     Push     False     16d
```

通过 kubectl 命令查询联邦控制面中成员集群列表及状态，可参考如下命令：

5.3.2. 操作指引

该操作指引以分发一个 nginx deployment 到成员集群为例，若需分发其他资源（包括 CR），只需将 nginx deployment 替换为具体的资源模板即可。

需要注意的是：

- 资源模板和 PropagationPolicy 之间可任意创建顺序不分先后，当二者匹配后即立即触发调度分发逻辑；
- 差异化策略需要在触发调度分发逻辑之前创建好，也即差异化策略不能是最后一个；

如下为详细操作参考：

步骤一： 创建资源模板

执行如下命令，在联邦控制面中创建资源模板：

```
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml create deployment nginx
--image nginx --replicas=3
deployment.apps/nginx created

$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get deployment nginx
NAME    READY   UP-TO-DATE   AVAILABLE   AGE
nginx   0/3     0            0           21s
```

此时，只是将 K8S YAML apply 到联邦控制面，还未分发到成员集群；联邦控制面当前也并不会调谐这些 workload，也即实际看到的 READY 副本数会为 0；

步骤二：创建差异化策略

差异化策略（OverridePolicy）模板参考如下。若不需要做集群间差异化，则可以略过该步骤。

```
# overridepolicy.yaml
apiVersion: policy.karmada.io/v1alpha1
kind: OverridePolicy
metadata:
  name: example
spec:
  resourceSelectors:
    - apiVersion: apps/v1
      kind: Deployment
      name: nginx # If no namespace is specified, the namespace is inherited from the parent
object scope.
  overrideRules:
    - targetCluster:
        clusterNames:
          - cce-cceone-demo1
      overriders:
        labelsOverrider:
          - operator: add
            value:
              cceone.propagationto: cce-cceone-demo1
    - targetCluster:
        clusterNames:
          - cce-cceone-demo2
      overriders:
        labelsOverrider:
          - operator: add
            value:
              cceone.propagationto: cce-cceone-demo2
```

将如上 YAML 文件通过如下命令 apply 到联邦控制面中：

```
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml apply -f overridepolicy.yaml
overridepolicy.policy.karmada.io/example created
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get overridepolicy example
NAME      AGE
example   21s
```

此时，通过命令查看 nginx 工作负载，还是未分发状态

```
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get deployment nginx
NAME    READY   UP-TO-DATE   AVAILABLE   AGE
nginx   0/3     0            0           61m
```

步骤三：创建调度策略

调度策略（PropagationPolicy）模板参考如下，可基于实际需要调整其中的污点容忍及负载拆分策略等：

```
# propagationpolicy.yaml
apiVersion: policy.karmada.io/v1alpha1
kind: PropagationPolicy
metadata:
  name: example-policy # The default namespace is `default`.
spec:
  propagateDeps: true
  resourceSelectors:
    - apiVersion: apps/v1
      kind: Deployment
      name: nginx # If no namespace is specified, the namespace is inherited from the parent
object scope.
  placement:
    clusterAffinity:      # 指定目标集群
      clusterNames:
        - cce-cceone-demo1
        - cce-cceone-demo2
    clusterTolerations:   # 容忍成员集群污点，影响调度逻辑
      - key: cluster.karmada.io/not-ready
        operator: Exists
        effect: NoExecute
        tolerationSeconds: 300
      - key: cluster.karmada.io/unreachable
        operator: Exists
        effect: NoExecute
        tolerationSeconds: 300
    replicaScheduling:   # 指定工作负载副本在成员集群间的分发策略
      replicaSchedulingType: Divided
      replicaDivisionPreference: Weighted
      weightPreference:
        staticWeightList:
          - targetCluster:
              clusterNames:
                - cce-cceone-demo1
            weight: 1
          - targetCluster:
              clusterNames:
                - cce-cceone-demo2
            weight: 2
```

通过如下命令，将调度策略 apply 到联邦控制面中

```
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml apply -f propagationpolicy.yaml
propagationpolicy.policy.karmada.io/example-policy created
ctyun@0000000g-FxXsKxFWUv:~/tmp$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml
get propagationpolicy example-policy
NAME                CONFLICT-RESOLUTION   PRIORITY   AGE
example-policy      Abort                 0          13s
```

此时，通过如下命令，查看工作负载在多集群之间的调度情况：

```
# 查看工作负载成员 Pod Ready 情况
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get deployment nginx
NAME    READY   UP-TO-DATE   AVAILABLE   AGE
nginx   3/3     3            3           10s
# 查询工作负载多集群调度结果
$ kubectl --kubeconfig=/home/ctyun/.kube/cceone-fed.yaml get resourcebinding nginx-deployment -o yaml
apiVersion: work.karmada.io/v1alpha2
kind: ResourceBinding
metadata:
  annotations:
    policy.karmada.io/applied-placement:
'{"clusterAffinity":{"clusterNames":["cce-cceone-demo1","cce-cceone-demo2"]},"clusterTolerations":[{"key":
"cluster.karmada.io/not-ready","operator":"Exists","effect":"NoExecute","tolerationSeconds":300},{"key":"clust
er.karmada.io/unreachable","operator":"Exists","effect":"NoExecute","tolerationSeconds":300}],"replicaSched
uling":{"replicaSchedulingType":"Divided","replicaDivisionPreference":"Weighted","weightPreference":{"static
WeightList":[{"targetCluster":{"clusterNames":["cce-cceone-demo1"]},"weight":1},{"targetCluster":{"clusterNa
mes":["cce-cceone-demo2"]},"weight":2}]}}}'
    propagationpolicy.karmada.io/name: example-policy
    propagationpolicy.karmada.io/namespace: default
    resourcebinding.karmada.io/dependencies: "null"
  creationTimestamp: "2025-05-30T09:52:51Z"
  finalizers:
  - karmada.io/binding-controller
  - karmada.io/binding-dependencies-distributor
  generation: 2
  labels:
    propagationpolicy.karmada.io/permanent-id: bb4b469a-6c93-4ed7-8465-e91564eb33eb
    resourcebinding.karmada.io/permanent-id: 89904db8-95a4-4820-b3b7-cea95b1c3e51
  name: nginx-deployment
  namespace: default
  ownerReferences:
  - apiVersion: apps/v1
    blockOwnerDeletion: true
    controller: true
    kind: Deployment
    name: nginx
    uid: 86da5387-b36b-40c4-99a2-462cbc832c99
  resourceVersion: "44338541"
  uid: 90b31326-7a74-405e-81e3-98ac18969d9f
spec:
  clusters:
  - name: cce-cceone-demo2
    replicas: 2
  - name: cce-cceone-demo1
    replicas: 1
  conflictResolution: Abort
  placement:
    clusterAffinity:
      clusterNames:
```

5.4. 使用集群联邦实现应用多活容灾

CCE One 集群联邦支持将工作负载的实例分发至多个集群中，避免单集群故障引发业务中断，保障业务连续性。

5.4.1. 前提条件

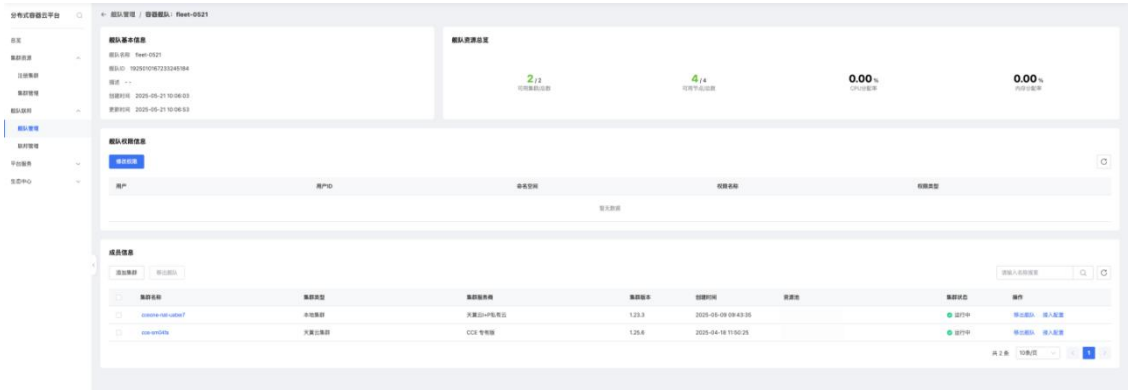
已创建两个及以上的注册集群，具体操作参见 订购注册集群 章节。若已有集群，无需重复操作。

已开通 CCE One 集群联邦实例。

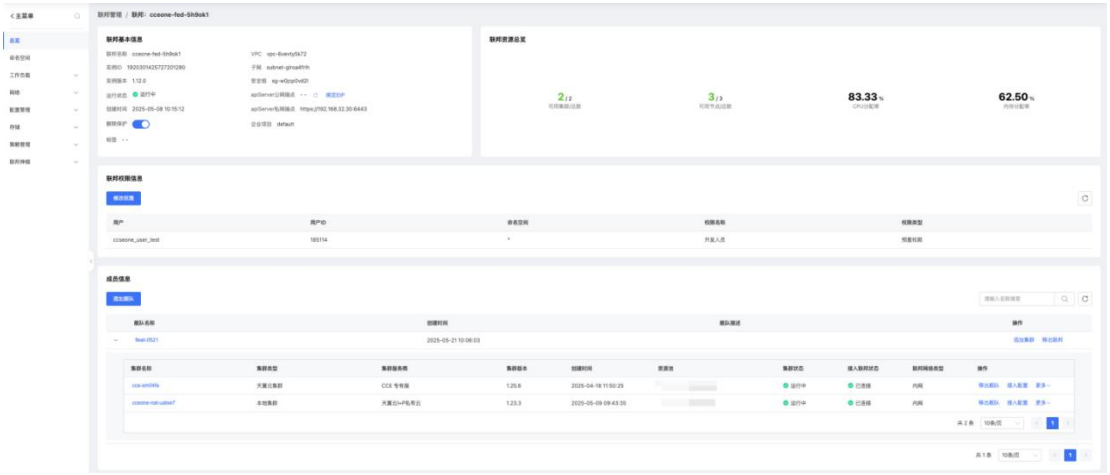
5.4.2. 环境搭建

登录 CCE One 控制台，在左侧导航栏选择“集群资源” > “集群管理”，进入集群管理界面，确认待操作集群均处于“运行中”状态。

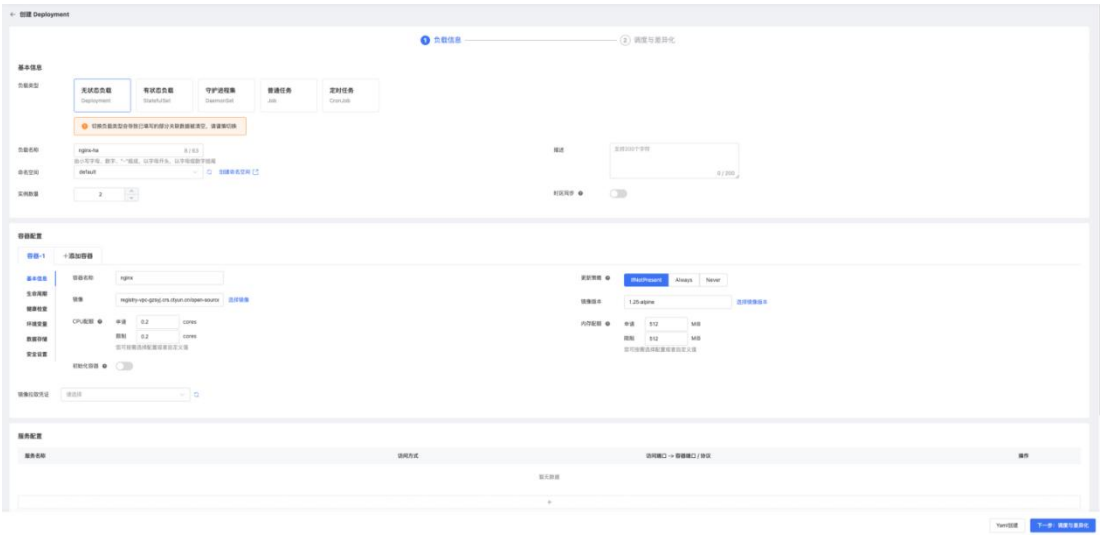
在 CCE One 控制台左侧导航栏选择“舰队联邦” > “舰队管理”，新建一个容器舰队，并将待操作集群添加至舰队中。



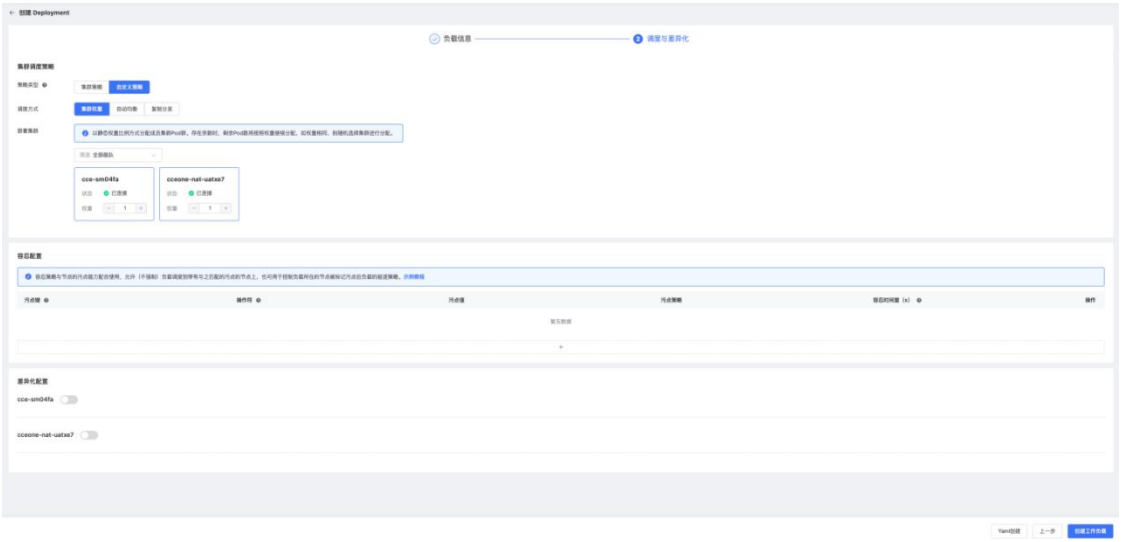
在 CCE One 控制台左侧导航栏选择“舰队联邦” > “联邦管理”，选择待操作联邦实例，进入联邦管理界面，查看“成员信息”，确认舰队及其下集群已接入联邦。



在联邦管理界面左侧导航栏选择“工作负载” > “无状态”，创建一个 nginx 无状态负载。



填写负载名称、命名空间、实例数量、容器镜像等信息后，点击“下一步：调度与差异化”



调度与差异化配置中，调度方式选择“集群权重”，并将两个集群权重设置为1:1。

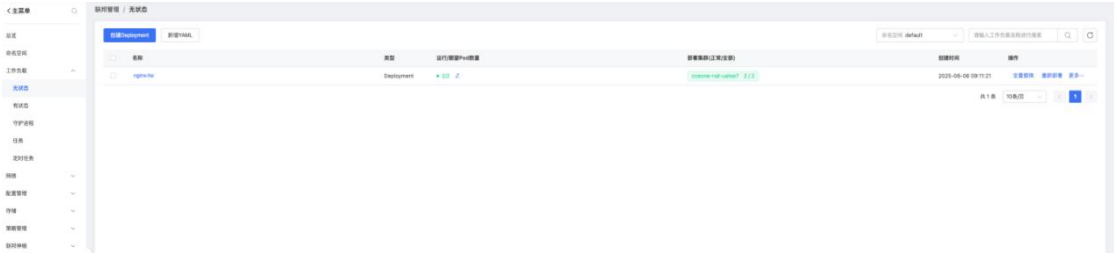
请注意：如果待操作的多个集群位于不同资源池，建议打开“差异化配置”，按集群所在的资源池配置对应容器镜像，避免镜像拉取失败。

配置完成后，点击“创建工作负载”进行创建，等待工作负载运行。

5.4.3. 容灾验证

将其中一个集群的控制面节点关机，模拟集群故障场景，观察工作负载调度情况。

可以发现工作负载自动进行重调度，所有实例均调度至正常集群中。



6. 常见问题

6.1. 注册集群常见问题

6.1.1. 注册集群是否收费？

接入分布式容器云平台注册集群，其计费项由集群管理服务费与部分关联云资源费用组成。其中，集群管理服务费由分布式容器云平台向您收取，而部分关联云资源产生的费用，则由云资源直接向您收取。

6.1.2. 注册集群接入对云下用户集群本身有什么要求？

注册集群接入对成员集群并无特别要求，理论上只需要确保其符合 CNCF 规范即可。但为确保接入注册集群后，云上其他关联功能可正常使用，建议参照以下约束规范执行：

- 云下 Kubernetes 版本，建议 >= 1.19；若考虑后续接入集群联邦使用多集群分发能力，建议云下 Kubernetes 版本 >=1.21 。
- 云下容器集群对应发行版符合 CNCF 规范，例如开源 K8S、K3S，或天翼云 Anywhere 发行版等。

6.1.3. 注册集群接入对网络连通性有什么要求？

天翼云分布式容器云平台注册集群提供公网和内网两种接入方式。默认支持内网方式接入，可通过给注册集群 APIServer 绑定 EIP 方式，启用公网接入能力。在以下场景必须使用内网接入，否则可能导致功能异常：

- 使用注册集群节点池功能为云下集群扩容天翼云 ECS 或弹性裸金属服务器。

- 使用注册集群 virtual-node 组件为云下集群弹性扩容云上 ECI 实例。
- 后续考虑接入集群联邦，通过联邦南北向多集群服务/路由实现流量跨集群自动调度。

请确保云下集群网络可以正常访问注册集群接入端点的 9443 端口，以及云下集群需可正常访问公网（日志、监控及部分插件，依赖公网访问方式与云上互通）。

6.1.4. 本地数据中心的 Kubernetes 集群可以扩容云上弹性资源吗？

可以，构建云上云下混合弹性容器集群后，云下 Kubernetes 集群可按需弹性云上 ECS 或 ECI 资源。

6.2. 集群联邦常见问题

6.2.1. 集群联邦是否收费？

集群联邦实例及其相关功能本身免费，分布式容器云平台不会向您收取任何费用。但涉及的部分关联云资源会产生费用，例如 ELB、EIP 等，相关费用将由具体云产品直接向您收取。

6.2.2. 集群联邦是否支持关联多个容器舰队？

一个集群联邦，默认限制只允许关联一个容器舰队。

若您存在多舰队启用联邦调度的需求，可考虑：

方式一：多舰队分别关联不同联邦实例，基于不同联邦实现单舰队内的多集群调度；

方式二：将相关注册集群统一加入一个容器舰队并关联一个集群联邦，在联邦中

通过成员集群打 Label 方式，将成员集群进行联邦场景下的分组管理；

6.2.3. 集群联邦管理关联的成员集群对集群间的连通性有什么要求？

联邦实例所在 VPC 需可以访问关联集群的 API Server 端点；

不同资源位置组合下，可考虑不同的网络联通方式：

- 若集群联邦和成员集群属于同资源池不同 VPC，则默认尝试内网互通（有启用 VPC 对等连接情况下），若内网不互通则后台自动尝试创建 VPCE 方式打通内网访问；
- 若集群联邦和成员集群属于不同资源池，则默认尝试内网互通（可通过云间高速打通），也可选择公网方式（需联邦 VPC 配置 SNAT 出口，并确保成员集群 APIServer 有绑定 EIP 以暴露到公网）；

6.2.4. 是否支持使用 Kubectl CLI 对集群联邦实例内资源进行操作？

可以使用 Kubectl CLI 下发资源进行操作。

集群联邦完全兼容 Kubernetes API Server，支持原生 Kubernetes 资源的下发；

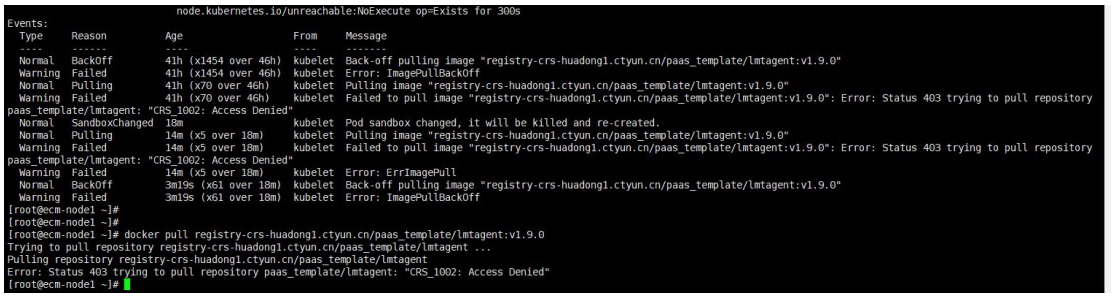
您也可以使用 Helm 打包应用并使用 Helm CLI 下发应用到集群联邦实例。

7. 故障修复

7.1. 注册集群使用中的常见问题和处理

7.1.1. 通过插件市场安装的插件，镜像拉取失败，报 403 错误

7.1.1.1 现象



7.1.1.2 原因及解决办法

插件市场中相关镜像地址，默认均属于公共镜像在任意地方均可正常拉取；若出现以上 403 错误，请检查您本地 Docker 版本及相关配置：若 Docker 版本较低请升级到最新版 Docker 后重试，若有添加镜像加速等个性化配置，请恢复默认配置并重新加载配置后重试。