云容器实例（CCI 1.0）

用户指南

文档版本 01

发布日期 2025-09-23

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 权限管理

1.1 CCI 权限说明

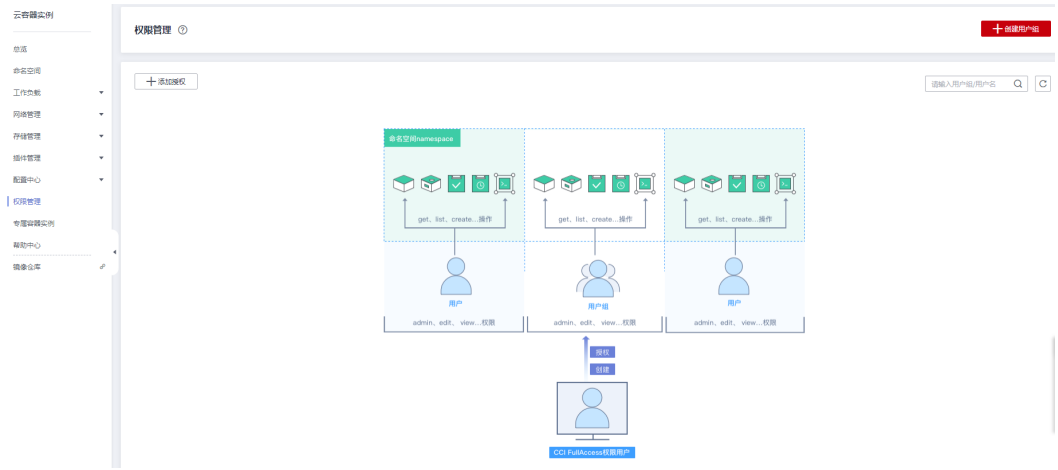
CCI当前认证鉴权是在Kubernetes的角色访问控制（RBAC）与统一身份认证服务（IAM）的能力基础上，提供的基于IAM的细粒度权限控制和IAM Token认证，同时支持命名空间级别及命名空间以下资源的权限控制，帮助用户便捷灵活地对租户下的IAM用户、用户组设定不同的操作权限。

- **命名空间权限：**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指定Namespace下Kubernetes资源的权限。
- **CCI权限：**是基于IAM的细粒度授权。通过命名空间级别权限设置可以控制用户操作Namespace（如创建、删除Namespace等）。更多细粒度权限说明请参见**CCI细粒度鉴权系统策略关联Actions**。

说明

- CCI服务暂不支持Landingzone场景。
- 创建Namespace时，打开RBAC鉴权开关，则此Namespace下资源访问受RBAC鉴权控制；如果未打开RBAC鉴权开关，则RBAC鉴权不生效。
- 创建开启RBAC鉴权的Namespace后，需要先对用户授权后，用户才能使用这个Namespace。
- network、clusterRole和roleBinding资源不受RBAC权限影响，只受IAM细粒度鉴权控制。network受控于network相关action，clusterRole与roleBinding受控于rbac相关action。
- 支持对当前用户下的所有命名空间进行授权，以提供更好的前端显示体验。
- 如果同时基于IAM，授予系统角色（IAM RBAC授权）和授予自定义策略（IAM细粒度授权），则判定CCI权限的优先级顺序为：IAM RBAC授权>IAM细粒度授权。

图 1-1 CCI 权限管理



命名空间权限

Kubernetes RBAC API定义了四种类型：Role、ClusterRole、RoleBinding与ClusterRoleBinding。当前CCI仅支持ClusterRole、RoleBinding，这两种类型之间的关系和简要说明如下：

- **ClusterRole：**描述角色和权限的关系。在Kubernetes的RBAC API中，一个角色定义了一组特定权限的规则。整个Kubernetes集群范围内有效的角色则通过ClusterRole对象实现。
- **RoleBinding：**描述subjects（包含users，groups）和角色的关系。角色绑定将一个角色中定义的各种权限授予一个或者一组用户，该用户或用户组则具有对应绑定ClusterRole定义的权限。

表 1-1 RBAC API 所定义的两种类型

类型名称	说明
ClusterRole	ClusterRole对象可以授予整个集群范围内资源访问权限。
RoleBinding	RoleBinding可以将同一Namespace中的subject（用户）绑定到某个具有特定权限的ClusterRole下，则此subject即具有该ClusterRole定义的权限。

注意

当前仅支持用户使用ClusterRole在Namespace下创建RoleBinding。

CCI的kubernetes资源通过命名空间进行权限设置，目前包含**cluster-admin**、**admin**、**edit**、**view**四种角色，详见**表1-2**。

表 1-2 用户/用户组角色说明

默认的ClusterRole	描述
cluster-admin	具有Kubernetes所有资源对象操作权限。
admin	允许admin访问，可以限制在一个Namespace中使用RoleBinding。如果在RoleBinding中使用，则允许对Namespace中大多数资源进行读写访问。这一角色不允许操作Namespace本身，也不能写入资源限额。
edit	允许对命名空间内的大多数资源进行读写操作。
view	允许对多数对象进行只读操作，但是对secret是不可访问的。

更多Kubernetes RBAC授权的内容可以参考**Kubernetes RBAC官方文档**。

1.2 创建用户并授权使用 CCI

如果您需要对您所拥有的云容器实例（CCI）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，在您的云账号中，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CCI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CCI资源委托给更专业、高效的其他云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果云账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CCI服务的其它功能。

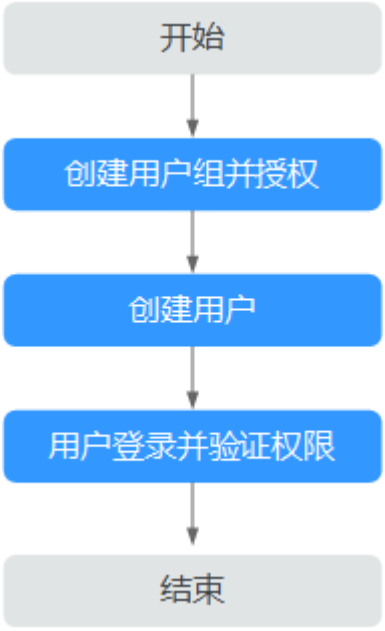
本章节为您介绍对用户授权的方法，操作流程如**图1-2**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的CCI权限，并结合实际需求进行选择，CCI支持的系统策略，请参见**CCI系统策略**。如果您需要对除CCI之外的其它服务授权，IAM支持服务的所有策略请参见**权限策略**。

示例流程

图 1-2 给用户授权 CCI 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组（例如开发人员组），并授予云容器实例普通用户权限“CCI CommonOperations”。因为CCI为项目级服务，所以在给用户授予CCI相关系统策略权限时，还需要给用户授予IAM ReadOnlyAccess。

2. **创建用户并加入用户组**

   在IAM控制台创建用户（例如James），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”中选择云容器实例，进入CCI主界面，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，在右侧页面单击“镜像创建”，如果可以正常创建工作负载，表示“CCI CommonOperations”已生效。
   - 在“服务列表”中选择云容器实例，进入CCI主界面，左侧导航栏中选择“命名空间”，在右侧页面单击“创建命名空间”，如果无法创建命名空间，表示“CCI CommonOperations”已生效。

1.3 为用户/用户组授权命名空间权限

本章节通过简单的命名空间授权方法，将CCI服务的用户和用户组授予操作不同命名空间资源的权限，从而使用户和用户组拥有命名空间的操作权限。设置流程如**示例流程**所示。

配置说明

- 您需要拥有一个主账号，仅主账号、授予了CCIFullAccess权限的用户或拥有RBAC所有权限的用户，才可以对其他用户进行授权操作。

- 本例将对用户和用户组授予操作不同命名空间资源的权限，在您的实际业务中，您可根据业务需求仅对用户或用户组授予不同的权限。
- 本例仅用于给用户或用户组在未授权过的命名空间下新增权限，已授权的用户或用户组的权限可以在“权限管理”的列表“操作”栏中单击“编辑”进行修改。
- 当给用户或用户组添加多个权限时，多个权限会同时生效（取并集）；为用户组设置的权限将作用于用户组下的全部用户。
- 在开启RBAC鉴权场景下，同类权限取并集，不同类权限取交集。例如，IAM细粒度鉴权中给用户组添加了多个权限，此时权限取最高权限，同理CCI权限管理给用户或用户组添加了多个权限，此时权限也取最高权限，即为同类权限取并集。当用户拥有CCI CommonOperations权限时，本可以创建无状态负载，但如该用户以及用户所在用户组未在目标Namespace下被赋予对应RBAC权限，则创建无状态负载会鉴权失败，即为不同类权限取交集。

示例流程

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离，使得它们既可以共享同一个集群的服务，也能够互不干扰。命名空间的一个重要的作用是充当一个虚拟的集群，用于多种工作用途，满足多用户的使用需求。

本章节将沿用**创建用户并授权使用CCI**中创建的IAM用户“James”和用户组“开发人员组”进行说明，为IAM用户“James”和用户组“开发人员组”添加命名空间权限，可以参考如下操作：

- **步骤一：为IAM用户/用户组添加命名空间权限**
- **步骤二：用户登录并验证权限**

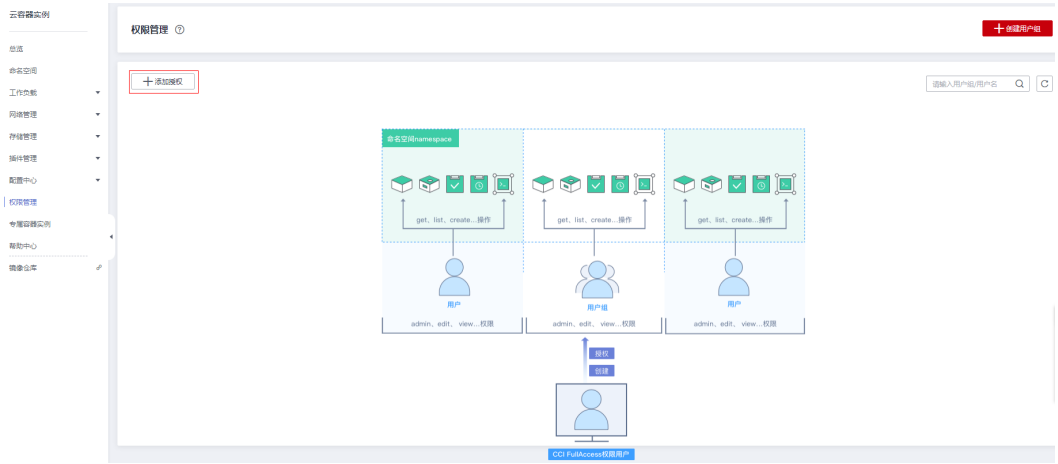
步骤一：为 IAM 用户/用户组添加命名空间权限

本步骤以主账号给CCI CommonOperations用户（James）赋予Namespace下view权限为例，被授权的CCI CommonOperations用户在该Namespace下只有只读权限。

步骤1 登录云容器实例管理控制台，在左侧导航栏中选择“权限管理”，进入权限管理页面。

步骤2 单击“添加授权”，进入添加授权页面。

图 1-3 添加授权



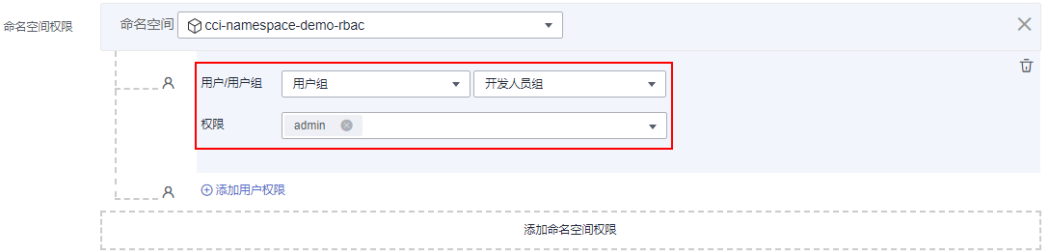
步骤3 在添加授权页面，选择要授权使用的命名空间，此处选择“cci-namespace-demo-rbac”。

图 1-4 选择命名空间

步骤4 为“开发人员组”增加“admin”权限，在展开的选项中进行如下配置：

- 用户/用户组：选择“用户组”，并在二级选项中选择“开发人员组”。
- 权限：选择“admin”。

图 1-5 为用户组授予 admin 权限



步骤5 单击下方的“添加命名空间权限”，为用户“James”增加在另一个命名空间“cci-namespace-demo-rbac01”的权限，在展开的选项中进行如下配置：

- 命名空间：选择“cci-namespace-demo-rbac01”。
- 用户/用户组：选择“用户”，并在二级选项中选择“James”。
- 权限：选择“view”。

图 1-6 添加命名空间权限

步骤6 单击“创建”，完成以上用户和用户组在命名空间中的相应权限设置。

图 1-7 命名空间权限列表

说明

经过以上操作，授权结果如下：

- 由于“开发人员组”包含IAM用户“James”，因此IAM用户“James”也同时获得了在命名空间“cci-namespace-demo-rbac”的“admin”权限。
- 为IAM用户“James”增加了在命名空间“cci-namespace-demo-rbac01”的“view”权限。

----结束

步骤二：用户登录并验证权限

使用IAM用户“James”登录云容器实例控制台，验证授予的命名空间权限，验证步骤如下：

步骤1 在“IAM用户登录”页面，输入账号名、用户名及用户密码，使用新创建的IAM用户登录。

- 账号名为该IAM用户所属云账号的名称。
- 用户名和密码为创建IAM用户James时输入的用户名和密码，首次登录时需要重置密码。

如果登录失败，您可以联系您的账号主体，确认用户名及密码是否正确，或是重置用户名及密码。

步骤2 登录成功后，进入控制台，登录后默认区域为“华东-上海一”，请先切换至授权区域。

步骤3 在“服务列表”中选择“云容器实例CCI”，进入CCI控制台，对IAM用户James的命名空间权限进行验证。

----结束

1.4 为委托账号授权命名空间权限

命名空间下资源权限的授权，是基于Kubernetes RBAC能力的授权。通过权限设置可以让不同的委托账号拥有操作指定Namespace下Kubernetes资源的权限。

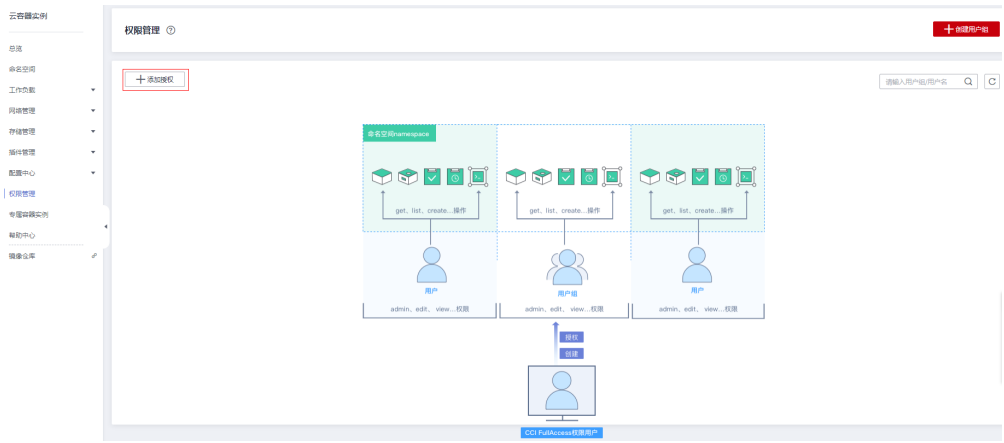
本章节通过简单的命名空间授权方法，将CCI服务的委托账号授予操作不同命名空间资源的权限，从而使委托账号拥有命名空间的操作权限。

操作步骤

步骤1 登录云容器实例管理控制台，在左侧导航栏中选择“权限管理”，进入权限管理页面。

步骤2 单击“添加授权”，进入添加授权页面。

图 1-8 添加授权



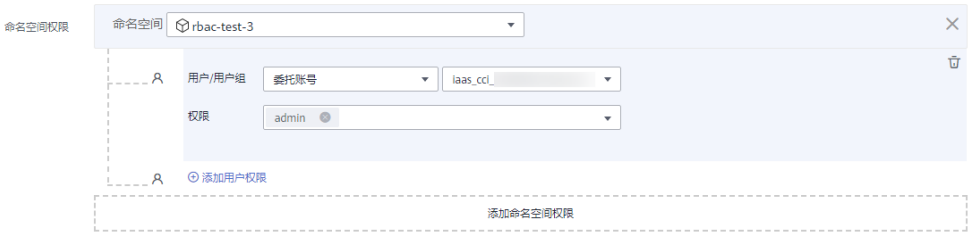
步骤3 在添加授权页面，选择要授权使用的命名空间，此处选择“rbac-test-3”。

图 1-9 选择命名空间

步骤4 为“委托账号”增加“admin”权限，在展开的选项中进行如下配置：

- 用户/用户组：选择“委托账号”，并在二级选项中选择需要授权的委托账号。
- 权限：选择“admin”。

图 1-10 为委托账号授予 admin 权限



步骤5 单击“创建”，完成委托账号在命名空间中的相应权限设置。

----结束

1.5 CCI 自定义策略

如果系统预置的CCI权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限策略和授权项**。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的CCI自定义策略样例。

CCI 自定义策略样例

- 示例1：更新命名空间

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cci:namespace:update"
            ]
        }
    ]
}
```

- 示例2：拒绝用户删除命名空间

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予CCIFullAccess的系统策略，但不希望用户拥有CCIFullAccess中定义的删除命名空间权限（cci:namespace:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为Deny，然后同时将CCIFullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对CCI执行除了删除命名空间外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "cci:namespace:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
```

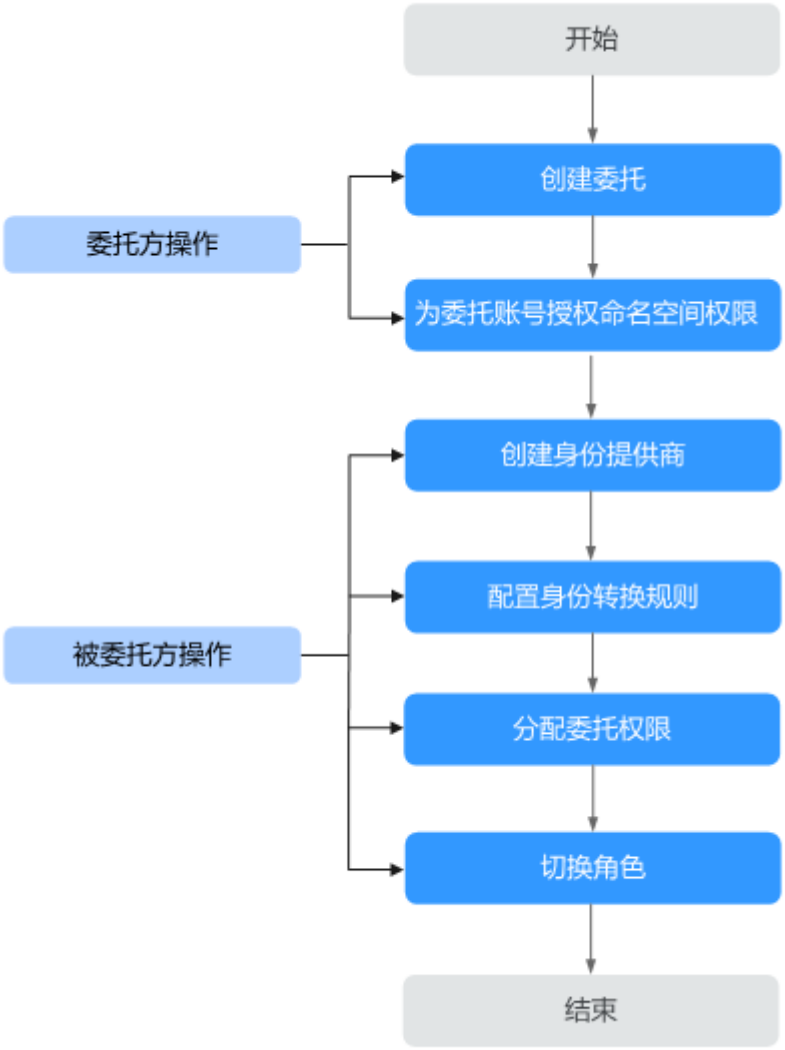
```
                "ecs:cloudServers:resize",
                "ecs:cloudServers:delete",
                "ecs:cloudServers:delete",
                "ims:images:list",
                "ims:serverImages:create"
            ],
            "Effect": "Allow"
        }
    ]
}
```

1.6 委托联邦用户管理资源

如果您需要将账号A的资源委托给账号B的联邦用户进行管理。首先您可以登录账号A，为账号B创建委托并授予命名空间权限。接下来登录账号B，与账号B做联邦身份认证，认证完成后，账号B将委托权限分配给联邦用户，使得联邦用户可以切换为账号A的委托。最后以联邦用户的身份登录到华为云，切换角色之后，就可以管理账号A中的资源。

本章节为您介绍委托联邦用户管理资源的方法，操作流程如图1-11所示。

图 1-11 委托联邦用户管理资源流程



操作步骤

账号A委托账号B以联邦用户的身份管理账号A中的资源，需要完成以下步骤：

步骤1 **创建委托（委托方操作）**

登录委托方（账号A）IAM控制台创建委托，需要填写被委托方（账号B）的账号名称，并授予被委托方（账号B）云容器实例所有权限“CCI FullAccess”，拥有该权限的用户可以执行云容器实例所有资源的创建、删除、查询、更新操作。

步骤2 **为委托账号授权命名空间权限（委托方操作）**

进入委托方（账号A）的CCI控制台，在权限管理页面为被委托方（账号B）授予命名空间下资源的权限，通过权限设置可以让不同的委托账号拥有操作指定Namespace下Kubernetes资源的权限。

步骤3 **联邦身份认证（被委托方操作）**

登录被委托方（账号B），在被委托方（账号B）中进行联邦身份认证操作。

在委托联邦用户管理资源之前，需对被委托方进行联邦身份认证，联邦身份认证过程主要分为两步：建立互信关系并创建身份提供商和在华为云配置身份转换规则。

说明

创建身份提供商时，会创建出默认的身份转换规则，用户需要单击“编辑规则”将默认的身份转换规则更新掉，或者将默认的身份转换规则删除，重新创建新的规则。如果默认的身份转换规则在没有删掉的情况下直接添加新规则，可能会匹配上这条默认规则，添加的新规则就会不生效。

步骤4 分配委托权限（被委托方操作）

如果被委托方（账号B）下的子用户想要切换委托，就必须由被委托方（账号B）分配委托权限。因此，为了使得联邦用户拥有管理委托方（账号A）资源的权限，就需要被委托方（账号B）授予联邦用户所在用户组（federation_group）自定义策略“federation_agency”。“federation_group”用户组为联邦用户所在的用户组，也是配置身份转换规则时，写入规则中的联邦用户组。

步骤5 切换角色（被委托方操作）

账号B以及分配了委托权限的联邦用户，可以切换角色至委托方账号A中，根据权限管理委托方的资源。

----结束

1.7 系统委托说明

由于CCI服务在运行中对弹性负载均衡、容器镜像等各类云服务都存在依赖关系，因此当您首次登录CCI控制台时，CCI将自动请求获取当前区域下的云资源权限，从而更好地为您提供服务。

CCI自动创建的委托：**cci_admin_trust**

cci_admin_trust 委托说明

cci_admin_trust委托具有Tenant Administrator权限。Tenant Administrator拥有除IAM管理外的全部云服务管理员权限，用于对CCI所依赖的其他云服务资源进行调用，且该授权仅在当前区域生效。

说明

由于CCI对其他云服务有许多依赖，如果没有Tenant Administrator权限，可能会因为某个服务权限不足而影响CCI功能的正常使用。因此在使用CCI服务期间，请不要自行删除或者修改cci_admin_trust委托。

当前CCI服务计划对cci_admin_trust委托的Tenant Administrator权限进行收缩，收缩后的权限为CCIFullAccess，CCIFullAccess策略权限详细说明请参见**权限管理**。收缩后的CCIFullAccess权限仅保留CCI服务运行中必要的依赖云服务权限，进一步增强委托的安全性。

cci_admin_trust 委托 CCIFullAccess 权限上线说明

cci_admin_trust委托的CCIFullAccess权限不同区域上线声明将根据发布计划依次声明。

cci_admin_trust 委托重新授权说明

- 对于已上线CCIFullAccess权限的区域，首次使用CCI服务的用户根据提示授权后，服务委托列表cci_admin_trust委托的将是CCIFullAccess权限。
- 对于已上线CCIFullAccess权限的区域，非首次使用CCI服务的用户需手动修改授权，详细切换方案将在CCIFullAccess权限上线声明中同步声明。

1.8 授权云容器实例访问其他云服务的权限

登录云容器实例控制台，并授予云容器实例访问其他云服务的权限。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的选择区域。

云容器实例当前仅支持在“华东-上海一”、“华东-上海二”、“华北-北京四”、“华南-广州”、“西南-贵阳一”区域使用。

说明

云容器实例CCI不支持在子项目创建资源请求。

步骤3 在首页“服务列表”中，选择“容器 > 云容器实例”。

步骤4 首次登录云容器实例控制台，需要授信云容器实例访问其他云服务资源的权限，单击“同意授权”。

授信成功后，将会创建一个委托，委托名称为“cci_admin_trust”，您可以在IAM服务控制台中查看。

----结束

2 命名空间

使用场景

命名空间（Namespace）是用于在多个用户间划分资源的一种方法，特别适用于拥有多个团队或项目的用户。当项目和人员数量较多时，可以根据项目属性（如生产、测试、开发等）创建不同的命名空间，以实现部分环境的隔离。

约束与限制

- 目前，“华南-广州”、“华东-上海二”、“西南-贵阳一”区域暂不支持“GPU加速型”资源。
- 一个账号在同一个区域支持创建5个命名空间，且命名空间的名称在云容器实例中需全局唯一。
- 通用计算型和GPU加速型支持X86镜像。

命名空间与网络的关系

从网络角度，命名空间对应一个虚拟私有云（VPC）中一个子网，如图2-1所示，在创建命名空间时会关联已有VPC或创建一个新的VPC，并在VPC下创建一个子网。后续在该命名空间下创建的容器及其他资源都会在对应的VPC及子网之内。

通常情况下，如果您在同一个VPC下还会使用其他服务的资源，您需要考虑您的网络规划，如子网网段划分、IP数量规划等，确保有可用的网络资源。

图 2-1 命名空间与 VPC 子网的关系

创建方式

您可以**通过控制台创建命名空间**或**使用kubectl创建命名空间**。

通过控制台创建命名空间

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“命名空间”。

步骤2 当前云容器实例提供“通用计算型”和“GPU加速型”两种类型的资源，在对应类型的命名空间下单击“创建”，后续创建的负载中容器将运行在此类型的集群上。

表 2-1 云容器实例类型

云容器实例类型	描述
通用计算型	支持创建含CPU资源的容器实例，适用于通用计算场景。
GPU加速型	支持创建含GPU资源的容器实例，适用于深度学习、科学计算、视频处理等场景。

步骤3 在对应类型的命名空间下单击“创建”。

步骤4 填写命名空间名称。

步骤5 设置RBAC权限。开启RBAC鉴权后，用户使用命名空间下的资源将受到RBAC权限控制，详情请参见**命名空间权限**。

步骤6 选择企业项目。CCI中每个命名空间对应一个企业项目，一个企业项目下可以有多个命名空间。

说明

- 如果您开通了**企业管理**，使用账号登录云容器实例控制台时，您需要在账号下的容器镜像服务中给IAM用户添加权限，IAM用户才能使用账号下的私有镜像。给IAM用户添加权限有如下两种方法：
  - 在镜像详情中为IAM用户添加授权，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限，具体请参见**在镜像详情中添加授权**。
  - 在组织中为IAM用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限，具体请参见**在组织中添加授权**。
- 您开通了企业项目后，自动创建的网络、存储资源与命名空间在同一企业项目中。您在企业项目页面进行资源迁移时，建议一同迁移相关资源。 例如命名空间从项目1迁移至项目2，网络和存储资源也需要一同迁移，否则可能会导致该命名空间下的负载异常。

步骤7 设置VPC。

选择使用已有VPC或新建VPC，新建VPC需要填写VPC网段，建议使用网段：10.0.0.0/8~22，172.16.0.0/12~22，192.168.0.0/16~22。

须知

- 此处VPC和子网的网段不能为10.247.0.0/16，10.247.0.0/16是云容器实例预留给负载访问的网段。如果您使用此网段，后续可能会造成IP冲突，导致负载无法创建或服务不可用；如果您不需要通过负载访问，而是直接访问Pod，则可以使用此网段。
- 命名空间创建完成后，在“网络管理 > 容器网络”中可查看到VPC和子网信息。

步骤8 设置子网网段。

您需要关注子网的可用IP数，确保有足够数量的可用IP，如果没有可用IP，则会导致负载创建失败。

图 2-2 子网设置

说明

- 创建的namespace会在设置的子网中预热部分IP，默认个数为10个。
- 在**高级设置**中可以设置预热的个数。
- 创建namespace后，由于预热了部分IP，会影响设置的subnet和VPC的删除，需要删除namespace之后才能正常删除对应的subnet和VPC。

步骤9 高级设置。

每个命名空间下都提供了一个IP池，申请IP需要一段时间，如果需要快速创建负载，减少IP的申请时间，可通过自定义资源池大小来实现。

例如，某业务线日常的负载数为200，当达到流量高峰时，IP资源池会自动扩容，瞬间将IP资源池扩容到500（IP资源池大小），同时会在回收间隔23h（IP资源池回收间隔）之后，进行回收超过资源池大小的部分即（500-200）个。

图 2-3 高级设置

- 预热IP资源池大小(个)：为每个命名空间预热一个IP池，用来加速负载创建。预热IP资源池的大小不能超过500个。
- 预热IP资源池回收间隔（h）：IP资源池弹性扩容出来的空闲IP资源， 在一定时间内可进行回收。
- 容器网络预准备：容器启动时，可能会没有网络连接。如果容器在启动时，需要立即连接网络， 可开启此处的“容器网络预准备”开关。

步骤10 单击“创建”。

创建完成后，可以在命名空间详情中看到VPC、子网等信息。

----结束

使用 kubectl 创建命名空间

使用kubectl创建命名空间请参见**Namespace和Network**。

后续相关操作

- CCI服务命名空间及对应网络配置，需关联安全组：
  - 通过CCI界面创建命名空间时，会同步创建、关联前缀为kubernetes.io-default-sg的安全组。为保证客户业务正常可运行，该安全组允许负载端口被所有IP地址访问，即放通不限于22、443、3389端口等典型端口。
  - 使用Bursting弹性到CCI使用的安全组继承CCE集群配置。
- 为进行安全加强，您可修改相应安全组规则为只允许IP地址段访问。请结合业务场景，谨慎操作仔细验证：
  - 如果负载使用httpGet类型的健康检查配置，则需要放通VPC下所有子网。如果VPC为192.168.0.0/16，则需要放通此IP端口，可访问负载的端口。
  - 如果VPC内存在VPCEP。请参考相关文档放通VPCEP业务网段，详见**购买终端节点并关联已创建终端节点服务后，无法正常连通如何排查?**
  - 如果业务需要使用ELB，并配置了service/ingress等服务发现相关能力。 请参考相关文档放通ELB业务网段，详情请参考**为什么100或214开头的IP在频繁访问后端服务器?**
- 删除**删除命名空间**。

删除命名空间

须知

删除命名空间将会删除该命名空间相关的所有数据资源（工作负载、ConfigMap、Secret、SSL证书等）。

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“命名空间”，单击要删除的命名空间，进入命名空间详情页面。

步骤2 单击右上角“删除”，并输入DELETE，然后单击“确认”。

说明

如需删除VPC、Subnet请前往**虚拟私有云**。

----结束

3 通过 CCI 控制台和 API 使用 CCI

3.1 工作负载

3.1.1 Pod

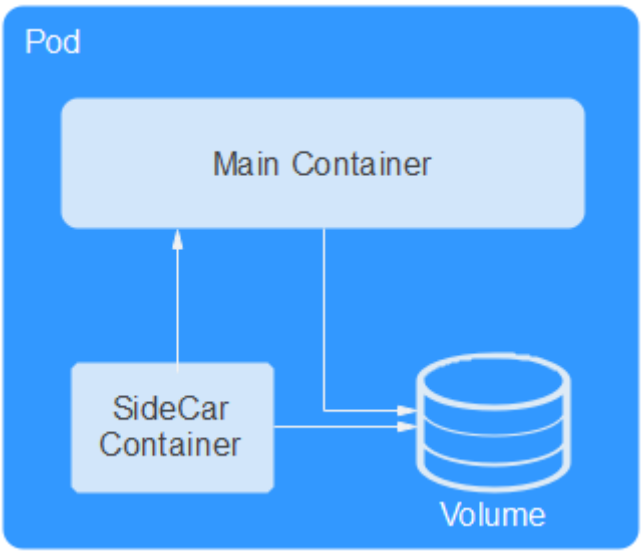
什么是 Pod

Pod是Kubernetes创建或部署的最小单位。一个Pod封装一个或多个容器（container）、存储资源（volume）、一个独立的网络IP以及管理控制容器运行方式的策略选项。

Pod使用主要分为两种方式：

- Pod中运行一个容器。这是Kubernetes最常见的用法，您可以将Pod视为单个封装的容器，但是Kubernetes是直接管理Pod而不是容器。
- Pod中运行多个需要耦合在一起工作、需要共享资源的容器。通常这种场景下是应用包含一个主容器和几个辅助容器（SideCar Container），如图3-1所示，例如主容器为一个web服务器，从一个固定目录下对外提供文件服务，而辅助的容器周期性的从外部下载文件存到这个固定目录下。

图 3-1 Pod



实际使用中很少直接创建Pod，而是使用Kubernetes中称为Controller的抽象层来管理Pod实例，例如Deployment和Job。Controller可以创建和管理多个Pod，提供副本管理、滚动升级和自愈能力。通常，Controller会使用Pod Template来创建相应的Pod。

使用 kubectl 创建 Pod

使用kubectl创建Pod请参见**Pod**章节。

查看 Pod

如果您通过调用**创建Pod**接口或者使用kubectl直接创建Pod，这些Pod并不在某个负载或任务之下，不便通过控制台管理。云容器实例提供了**Pod管理**功能，您可以通过“选择来源”更方便找到需要的Pod。

图 3-2 选择 Pod 来源

您可以查看到所有Pod详情，包括基本信息、Pod中容器组成、Pod的监控信息、事件，以及使用远程终端访问Pod。您还可以对Pod进行删除操作，并查看Pod的日志。

图 3-3 Pod 详情

3.1.2 无状态负载（Deployment）

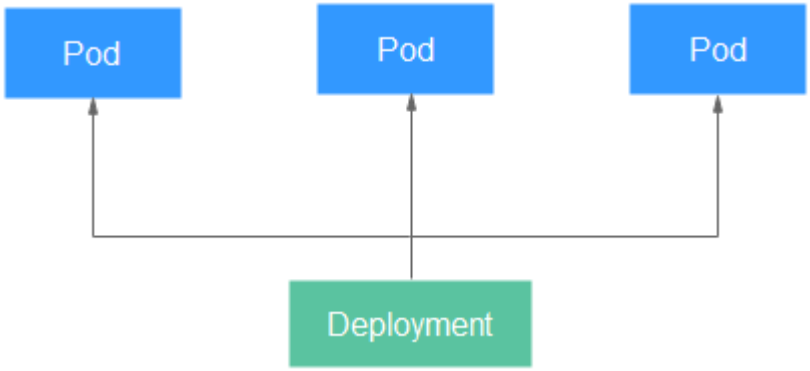
无状态负载与Kubernetes中Deployment Workloads的定义方式相同，是对Pod的服务化封装。一个无状态负载可以包含一个或多个Pod，每个Pod的角色相同，所以系统会自动为无状态负载的多个Pod分发请求。同一无状态负载的所有Pod共享存储卷。

在**Pod**这个章节介绍了Pod，Pod是Kubernetes创建或部署的最小单位，但是Pod是被设计为相对短暂的一次性实体，Pod可以被驱逐（当节点资源不足时）、随着集群的节点fail而消失。同时kubernetes提供了Controller（控制器）来管理Pod，Controller可以创建和管理多个Pod，提供副本管理、滚动升级和自愈能力，其中最为常用的就是Deployment。

一个Deployment可以包含一个或多个Pod副本，每个Pod副本的角色相同，所以系统会自动为Deployment的多个Pod副本分发请求。

Deployment集成了上线部署、滚动升级、创建副本，恢复上线任务，在某种程度上，Deployment可以帮用户实现无人值守的上线，大大降低了上线过程的复杂沟通、操作风险。

图 3-4 无状态负载



创建方式

表 3-1 创建无状态负载方式

创建方式	相关链接
通过控制台创建无状态负载	通过控制台创建无状态负载
使用Kubectl创建无状态负载	使用Kubectl创建无状态负载请参见Deployment。

通过控制台创建无状态负载

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，在右侧页面单击“镜像创建”。

步骤2 添加基本信息。

- **负载名称**

  请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到63字符的字符串。负载名称不支持修改，如需修改名称，需要重新创建。

- **命名空间**

  选择命名空间，如果还未创建命名空间，请参考命名空间创建。

- **负载描述**

  描述信息，少于等于250个字符。

- **Pod数量**

  负载可以有一个或多个Pod，您可以设置具体Pod个数。每个负载Pod都由相同的容器部署而成。设置多个Pod主要用于实现高可靠性，当某个Pod故障时，负载还能正常运行。

- **Pod规格**

  您可以选择使用GPU（只能在GPU型命名空间下）或不使用GPU。

  具体的规格信息请参考约束与限制中的“Pod规格”。

  说明

  - nvidia-smi是一个命令行工具，详细信息请参考NVIDIA System Management Interface。
  - CCI不提供nvidia-smi，您可以将nvidia-smi打包到镜像中，通过nvidia-smi监控GPU使用情况。使用nvidia-smi前需要设置LD_LIBRARY_PATH值。

- **启用镜像快照**

  使用镜像快照（ImageSnapshot），可以避免镜像下载，减少Pod启动时间，要了解镜像快照的工作原理，请参阅镜像快照概述。

  支持以下两种方式：

  - 自动匹配镜像快照

    自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。按以下顺序进行匹配：

    a. 镜像匹配度：优先选择匹配度高的镜像快照，匹配度指的是Pod和镜像快照两者在镜像上的匹配情况。

b. 创建时间：优先选择创建时间更新的镜像快照。

- 明确指定

  指定已有的镜像快照，并在容器配置下的“镜像快照”页签中选择镜像快照中的镜像。该镜像缓存必须为创建完成可用（Available）状态。

- **容器配置**

  一个Pod可以包含一个或多个运行不同镜像的容器，通常情况下一个Pod中只有一个容器，如果您的应用程序需要多个容器，请单击“添加容器”，然后选择镜像。

  须知

  同一个Pod实例中的不同容器如果监听了相同的端口，则会导致端口冲突，Pod可能会启动失败。例如在Pod中添加了一个nginx镜像容器，启动了80端口，如果该Pod中另一个http服务的镜像也启动80端口，那么这个Pod就会出现端口冲突。

  - 我的镜像：展示了您上传到容器镜像服务的镜像。

    说明

    - 如果您开通了**企业管理**，使用账号登录云容器实例控制台时，您需要在账号下的容器镜像服务中给IAM用户添加权限，IAM用户才能使用账号下的私有镜像。给IAM用户添加权限有如下两种方法：
      - 在镜像详情中为IAM用户添加授权，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限，具体请参见**在镜像详情中添加授权**。
      - 在组织中为IAM用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限，具体请参见**在组织中添加授权**。
    - CCI当前暂不支持对接第三方镜像仓库。
    - 镜像单层解压后的实际大小不能超过20G。
  - 开源镜像中心：展示了镜像中心的公共镜像。

- 共享镜像：展示了容器镜像服务中他人共享的镜像。

镜像选择完成后，需要选择镜像的版本、设置容器名称、设置容器占用的CPU和内存规格，并选择是否开启采集标准输出文件（开启后，应用运维管理AOM将根据实际使用量进行计费）。

说明

每个租户一个月有500M的免费日志存储空间，超过500M时AOM将根据实际使用量进行收费，计费规则请参见**产品价格详情**。

对于GPU加速型Pod（仅GPU型命名空间下才可以选择），Pod中只有一个容器能使用GPU，如果您的Pod中有多个容器，您可以通过**开启GPU**这个开关选择哪个容器使用GPU。

您还可以为容器做如下高级设置：

- 存储：支持挂载持久化卷到容器中，以实现数据文件的持久化存储，当前支持云硬盘存储卷、文件存储卷和极速文件存储卷。单击“添加云硬盘存储卷”、“添加文件存储卷”或“添加极速文件存储卷”，输入名称、容量、容器内挂载路径，选择磁盘类型。负载创建完成后，可对存储卷进行管理，具体请参见**云硬盘存储卷**、**文件存储卷 3.0**或**极速文件存储卷**。
- 日志采集：支持根据您配置的日志输出路径，采集应用日志请自行防爆处理。单击添加日志存储，输入容器内日志路径，调整日志存储空间。负载创建完成后，可在AOM界面查看日志，具体请参见**日志管理**。
- 环境变量：在容器中设置环境变量，支持手动输入和引用变量。环境变量为应用提供极大的灵活性，您可以在应用程序中使用环境变量，在创建容器时为环境变量赋值，容器运行时读取环境变量的值，从而做到灵活的配置，而不是每次都重新编写应用程序制作镜像。

  手动输入只需要直接输入变量名称和变量值。

  变量引用支持引用PodIP（Pod的IP地址）、PodName（Pod的名称）以及Secret，输入变量名称，选择引用类型、引用值。其中Secret引用的创建请参见**使用Secret**。
- 健康检查：健康检查是指容器运行过程中，根据您需要，定时检查容器健康状况。详细步骤请参见**健康检查**。
- 生命周期：生命周期脚本定义，在容器的生命周期的特定阶段执行调用。详细步骤请参见**容器生命周期**。
- 启动命令：输入容器启动命令，容器启动后会立即执行。启动命令对应于容器引擎的ENTRYPOINT启动命令，详细内容请参见**容器启动命令**。
- 配置管理：容器支持挂载ConfigMap和Secret。ConfigMap和Secret的创建请参见**使用ConfigMap**和**使用Secret**。

步骤3 单击“下一步：访问配置”，配置负载访问信息。

负载访问有如下三个选项：

- 不启用：将不提供任何从其他负载访问到当前负载的入口，可用于使用自定义的服务发现或简单启用多个Pod的场景。
- 内网访问：内网访问将为当前负载配置一个负载域名或内网域名/虚拟IP，使得当前负载能够为内网中其他负载提供服务，分为Service和ELB两种方式。内网访问的详细内容请参见**内网访问**。
- 公网访问：将提供一个可以从Internet访问的入口，支持HTTP/HTTPS/TCP/UDP协议。公网访问的详细内容请参见**公网访问**。

步骤4 单击“下一步：高级设置”，进行高级设置。

- **升级策略**：升级方式支持“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老的实例上，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。
- **客户端DNS配置**：负载支持替换域名解析配置和追加域名解析配置，参数设置请参见**客户端DNS配置**。

步骤5 配置完成后，单击“下一步：规格确认”，单击“提交”，单击“返回无状态负载列表”。

在负载列表中，待负载状态为“运行中”，负载创建成功。您可以单击负载名进入负载详情界面，按F5查看负载实时状态。

如果需要访问负载，选择“访问配置”Tab页，查看访问地址。

----结束

删除 Pod

负载创建完后，可以对Pod进行手动删除操作，由于Pod是由控制器在控制，单击删除按钮后会立即重新创建一个新的Pod。手动删除Pod在某些场景下非常有用，比如升级到一半出现失败时、想重启业务进程时。

删除Pod如**图3-5**所示。

图 3-5 删除 Pod

删除后立即重新创建Pod，如**图3-6**所示。

图 3-6 删除 Pod 的效果

重新拉取镜像失败问题排查

工作负载详情中，如果事件中提示“重新拉取镜像失败”，请参见**事件一：重新拉取镜像失败**来排查原因。

重新启动容器失败问题排查

工作负载详情中，如果事件中提示“重新启动容器失败”，请参见**事件二：重新启动容器失败**来排查原因。

3.1.3 任务（Job）

任务是负责批量处理短暂的一次性任务(short lived one-off tasks)，即仅执行一次的任务，它保证批处理任务的一个或多个Pod成功结束。

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）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（Pod自动删除）。

任务的这种用完即停止的特性特别适合一次性任务，比如持续集成，配合云容器实例按秒计费，真正意义上做到按需使用。

创建任务

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 任务（Job）”，在右侧页面单击“镜像创建”。

步骤2 添加基本信息。

- **任务名称**

  请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到52字符的字符串。任务名称不支持修改，如需修改名称，需要重新创建。

- **命名空间**

  选择命名空间，如果还未创建命名空间，请参考**命名空间**创建。

- **任务描述**

  描述信息，少于等于250个字符。

- **Pod规格**

  您可以选择使用GPU（只能在GPU型命名空间下）或不使用GPU。

  具体的规格信息请参考**约束与限制**中的“Pod规格”。

- **启用镜像快照**

  使用镜像快照（ImageSnapshot），可以避免镜像下载，减少Pod启动时间，要了解镜像快照的工作原理，请参阅**镜像快照概述**。

  支持以下两种方式：

  - 自动匹配镜像快照

    自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。按以下顺序进行匹配：

    a. 镜像匹配度：优先选择匹配度高的镜像快照，匹配度指的是Pod和镜像快照两者在镜像上的匹配情况。

    b. 创建时间：优先选择创建时间更新的镜像快照。

  - 明确指定

    指定已有的镜像快照，并在容器配置下的“镜像快照”页签中选择镜像快照中的镜像。该镜像缓存必须为创建完成可用（Available）状态。

- **容器配置**

  一个Pod可以包含一个或多个运行不同镜像的容器，通常情况下一个Pod中只有一个容器，如果您的应用程序需要多个容器，请单击“添加容器”，然后选择镜像。

  须知

  同一个Pod实例中的不同容器如果监听了相同的端口，则会导致端口冲突，Pod可能会启动失败。例如在Pod中添加了一个nginx镜像容器，启动了80端口，如果该Pod中另一个http服务的镜像也启动80端口，那么这个Pod就会出现端口冲突。

  - 我的镜像：展示了您上传到容器镜像服务的镜像。

    说明

    - 如果您开通了**企业管理**，使用账号登录云容器实例控制台时，您需要在账号下的容器镜像服务中给IAM用户添加权限，IAM用户才能使用账号下的私有镜像。给IAM用户添加权限有如下两种方法：
      - 在镜像详情中为IAM用户添加授权，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限，具体请参见**在镜像详情中添加授权**。
      - 在组织中为IAM用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限，具体请参见**在组织中添加授权**。
    - CCI当前暂不支持对接第三方镜像仓库。
  - 开源镜像中心：展示了镜像中心的公共镜像。
  - 共享镜像：展示了容器镜像服务中他人共享的镜像。

  镜像选择完成后，需要选择镜像的版本、设置容器名称、设置容器占用的CPU和内存规格，并选择是否开启采集标准输出文件（开启后，应用运维管理AOM将根据实际使用量进行计费）。

说明

每个租户一个月有500M的免费日志存储空间，超过500M时AOM将根据实际使用量进行收费，计费规则请参见**产品价格详情**。

对于GPU加速型Pod（仅GPU型命名空间下才可以选择），Pod中只有一个容器能使用GPU，如果您的Pod中有多个容器，您可以通过**开启GPU**这个开关选择哪个容器使用GPU。

您还可以为容器做如下高级设置：

- 存储：支持挂载持久化卷到容器中，以实现数据文件的持久化存储，当前支持云硬盘存储卷、对象存储卷、文件存储卷和极速文件存储卷。单击“添加云硬盘存储卷”、“添加对象存储卷”、“添加文件存储卷”或“添加极速文件存储卷”，输入名称、容量、容器内挂载路径，选择磁盘类型。任务创建完成后，可对存储卷进行管理，具体请参见**云硬盘存储卷**、**对象存储卷**、**文件存储卷 3.0**或**极速文件存储卷**。
- 日志采集：支持根据您配置的日志输出路径，采集应用日志，请自行防爆处理。单击添加日志存储，输入容器内日志路径，调整日志存储空间。负载创建完成后，可在AOM界面查看日志，具体请参见**日志管理**。
- 环境变量：在容器中设置环境变量，支持手动输入和引用变量。环境变量为应用提供极大的灵活性，您可以在应用程序中使用环境变量，在创建容器时为环境变量赋值，容器运行时读取环境变量的值，从而做到灵活的配置，而不是每次都重新编写应用程序制作镜像。

  手动输入只需要直接输入变量名称和变量值。

  变量引用支持引用PodIP（Pod的IP地址）、PodName（Pod的名称）以及Secret，输入变量名称，选择引用类型、引用值。其中Secret引用的创建请参见**使用Secret**。
- 存活探针：用于容器的自定义监控检查，如果检查失败，云容器实例将关闭该容器，然后根据默认重启策略来决定是否重启容器。详细步骤请参见**健康检查**。
- 生命周期：生命周期脚本定义，在容器的生命周期的特定阶段执行调用。详细步骤请参见**容器生命周期**。
- 启动命令：输入容器启动命令，容器启动后会立即执行。启动命令对应于容器引擎的ENTRYPOINT启动命令，详细内容请参见**容器启动命令**。
- 配置管理：容器支持挂载ConfigMap和Secret。ConfigMap和Secret的创建请参见**使用ConfigMap**和**使用Secret**。

步骤3 单击“下一步：高级设置”，进行任务高级配置。

任务可以分为一次性任务和自定义任务。

- 一次性任务：一次性任务每次创建一个Pod，直至一个Pod成功执行，任务完成。
- 自定义任务：自定义任务的执行次数和每次并行执行的数量。执行次数指任务达到执行完成状态需要成功执行的Pod数量。并行数指任务执行过程中允许同时创建的最大Pod数，并行数应小于执行次数。

任务执行可以设置超时时间，当任务执行超出该时间时，任务将会被标识为执行失败，任务负载下的所有Pod实例都会被删除。为空时表示不设置超时时间。

步骤4 单击“下一步：规格确认”，单击“提交”，单击“返回任务列表”。

在任务列表中，待任务状态为“执行中”，任务创建成功。您可以单击负载名进入任务详情界面，按F5查看任务实时状态。

----结束

使用 kubectl 创建任务

使用kubectl创建任务请参见**创建Job**。

3.1.4 定时任务（CronJob）

定时任务（CronJob）是基于时间控制的任务（Job），类似于Linux系统的crontab，在指定的时间周期运行指定的任务。

创建定时任务

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 定时任务（CronJob）”，在右侧页面单击“镜像创建”。

步骤2 添加基本信息。

- **任务名称**

  请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到52字符的字符串。任务名称不支持修改，如需修改名称，需要重新创建。

- **命名空间**

  选择命名空间，如果还未创建命名空间，请参考**命名空间**创建。

- **任务描述**

  描述信息，少于等于250个字符。

- **Pod规格**

  您可以选择使用GPU（只能在GPU型命名空间下）或不使用GPU。

  具体的规格信息请参考**约束与限制**中的“Pod规格”。

- **启用镜像快照**

  使用镜像快照（ImageSnapshot），可以避免镜像下载，减少Pod启动时间，要了解镜像快照的工作原理，请参阅**镜像快照概述**。

  支持以下两种方式：

  - 自动匹配镜像快照

    自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。按以下顺序进行匹配：

    a. 镜像匹配度：优先选择匹配度高的镜像快照，匹配度指的是Pod和镜像快照两者在镜像上的匹配情况。

    b. 创建时间：优先选择创建时间更新的镜像快照。

  - 明确指定

    指定已有的镜像快照，并在容器配置下的“镜像快照”页签中选择镜像快照中的镜像。该镜像缓存必须为创建完成可用（Available）状态。

- **容器配置**

  一个Pod可以包含一个或多个运行不同镜像的容器，通常情况下一个Pod中只有一个容器，如果您的应用程序需要多个容器，请单击“添加容器”，然后选择镜像。

  须知

  同一个Pod实例中的不同容器如果监听了相同的端口，则会导致端口冲突，Pod可能会启动失败。例如在Pod中添加了一个nginx镜像容器，启动了80端口，如果该Pod中另一个http服务的镜像也启动80端口，那么这个Pod就会出现端口冲突。

  - 我的镜像：展示了您上传到容器镜像服务的镜像。

    说明

    - 如果您开通了**企业管理**，使用账号登录云容器实例控制台时，您需要在账号下的容器镜像服务中给IAM用户添加权限，IAM用户才能使用账号下的私有镜像。给IAM用户添加权限有如下两种方法：
      - 在镜像详情中为IAM用户添加授权，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限，具体请参见**在镜像详情中添加授权**。
      - 在组织中为IAM用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限，具体请参见**在组织中添加授权**。
    - CCI当前暂不支持对接第三方镜像仓库。
  - 开源镜像中心：展示了镜像中心的公共镜像。
  - 共享镜像：展示了容器镜像服务中他人共享的镜像。

  镜像选择完成后，需要选择镜像的版本、设置容器名称、设置容器占用的CPU和内存规格，并选择是否开启采集标准输出文件（开启后，应用运维管理AOM将根据实际使用量进行计费）。

说明

每个租户一个月有500M的免费日志存储空间，超过500M时AOM将根据实际使用量进行收费，计费规则请参见**产品价格详情**。

对于GPU加速型Pod（仅GPU型命名空间下才可以选择），Pod中只有一个容器能使用GPU，如果您的Pod中有多个容器，您可以通过**开启GPU**这个开关选择哪个容器使用GPU。

您还可以为容器做如下高级设置：

- 存储：支持挂载持久化卷到容器中，以实现数据文件的持久化存储，当前支持文件存储卷。单击“添加文件存储卷”，输入名称、容量、容器内挂载路径、挂载子路径，选择磁盘类型。定时任务创建完成后，可对存储卷进行管理，具体请参见**文件存储卷 3.0**。
- 日志采集：支持根据您配置的日志输出路径，采集应用日志，请自行防爆处理。单击添加日志存储，输入容器内日志路径，调整日志存储空间。负载创建完成后，可在AOM界面查看日志，具体请参见**日志管理**。
- 环境变量：在容器中设置环境变量，支持手动输入和引用变量。环境变量为应用提供极大的灵活性，您可以在应用程序中使用环境变量，在创建容器时为环境变量赋值，容器运行时读取环境变量的值，从而做到灵活的配置，而不是每次都重新编写应用程序制作镜像。

  手动输入只需要直接输入变量名称和变量值。

  变量引用支持引用PodIP（Pod的IP地址）、PodName（Pod的名称）以及Secret，输入变量名称，选择引用类型、引用值。其中Secret引用的创建请参见**使用Secret**。
- 存活探针：用于容器的自定义监控检查，如果检查失败，云容器实例将关闭该容器，然后根据默认重启策略来决定是否重启容器。详细步骤请参见**健康检查**。
- 生命周期：生命周期脚本定义，在容器的生命周期的特定阶段执行调用。详细步骤请参见**容器生命周期**。
- 启动命令：输入容器启动命令，容器启动后会立即执行。启动命令对应于容器引擎的ENTRYPOINT启动命令，详细内容请参见**容器启动命令**。
- 配置管理：容器支持挂载ConfigMap和Secret。ConfigMap和Secret的创建请参见**使用ConfigMap**和**使用Secret**。

步骤3 单击“下一步：定时规则”，进行任务高级配置。

- 并发策略
  - Forbid：在前一个任务未完成时，不创建新任务。
  - Allow：定时任务不断新建Job。
  - Replace：已到新任务创建时间点，但前一个任务还未完成，新的任务会取代前一个任务。
- 定时规则：设置任务在何时执行。
- 任务记录：设置保留执行成功任务的个数和保留执行失败任务的个数。

步骤4 单击“下一步：规格确认”，单击“提交”，单击“返回任务列表”。

在任务列表中，待任务状态为“已启动”，任务创建成功。您可以单击负载名进入任务详情界面，按F5查看任务实时状态。

----结束

使用 kubectl 创建定时任务

使用kubectl创建定时任务请参见**创建CronJob**。

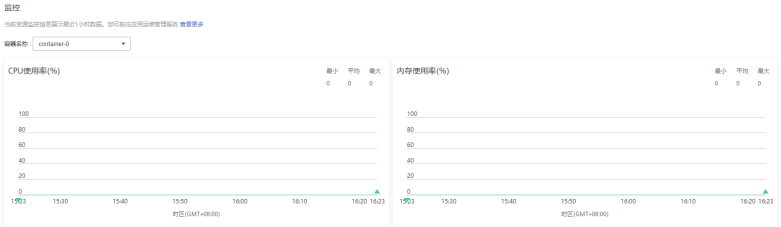
3.1.5 查看资源使用率

当您创建完工作负载后，您也许会非常关心每个Pod的资源利用率。

云容器实例提供了查看CPU/内存、GPU/显存的界面，您只需要在无状态负载、任务、定时任务中Pod列表的“监控”Tab下即可查看资源使用率，如**图3-7**所示。

您也可以在Pod管理中查看所有Pod的资源使用率。

图 3-7 查看监控信息



3.1.6 容器启动命令

启动容器就是启动主进程，但有些时候，启动主进程前，需要一些准备工作。比如MySQL类的数据库，可能需要一些数据库配置、初始化的工作，这些工作要在最终的MySQL服务器运行之前解决。这些操作，可以在制作镜像时通过在Dockerfile文件中设置ENTRYPOINT或CMD来完成，如下所示的Dockerfile中设置了**ENTRYPOINT ["top", "-b"]**命令，其将会在容器启动时执行。

```
FROM ubuntu
ENTRYPOINT ["top", "-b"]
```

须知

启动命令必须为容器镜像支持的命令，否则会导致容器启动失败。

在云容器实例中同样可以设置容器的启动命令，例如上面Dockerfile中的命令，只要在创建负载时配置容器的高级设置，先单击“添加”，输入“top”命令，再单击“添加”，输入参数“-b”，如下图所示。

图 3-8 启动命令

由于容器引擎运行时只支持一条ENTRYPOINT命令，云容器实例中设置的启动命令会覆盖掉制作镜像时Dockerfile中设置的ENTRYPOINT和CMD命令，其规则如下表所示。

镜像Entrypoint	镜像CMD	容器运行命令	容器运行参数	最终执行
[touch]	[/root/test]	未设置	未设置	[touch /root/test]
[touch]	[/root/test]	[mkdir]	未设置	[mkdir]
[touch]	[/root/test]	未设置	[/opt/test]	[touch /opt/test]
[touch]	[/root/test]	[mkdir]	[/opt/test]	[mkdir /opt/test]

3.1.7 容器生命周期

设置容器生命周期

云容器实例基于Kubernetes，提供了**容器生命周期钩子**，在容器的生命周期的特定阶段执行调用，比如容器在停止前希望执行某项操作，就可以注册相应的钩子函数。目前提供的生命周期钩子函数如下所示。

- 启动后处理（PostStart）：容器启动后触发。
- 停止前处理（PreStop）：容器停止前触发。

说明

当前云容器实例仅支持命令行类型（Exec）钩子函数。

登录云容器实例控制台，在创建负载配置生命周期过程中，选择“启动后处理”或者“停止前处理”页签。

例如需要在容器中执行“/postStart.sh all”命令，则在界面上做如下配置即可，第一行是命令行脚本名称，第二行是参数。

图 3-9 命令行脚本

使用 kubectl 设置容器生命周期

使用kubectl设置容器生命周期请参见**生命周期管理**。

3.1.8 健康检查

健康检查是指容器运行过程中，根据需要，定时检查容器中应用健康状况。

云容器实例基于Kubernetes，提供了两种健康检查的方式：

- **应用存活探针（liveness probe），探测应用是否已经启动：**该检查方式用于检测容器是否存活，类似于我们执行ps命令检查进程是否存在。如果容器的存活检查的结果为失败，云容器实例会对该容器执行重启操作；如果容器的存活检查成功则不执行任何操作。
- **应用业务探针（readiness probe），探测应用业务是否已经就绪：**该检查方式用于检测容器是否准备好开始处理用户请求。一些程序的启动时间可能很长，比如要加载磁盘数据或者要依赖外部的某个模块启动完成才能提供服务。这时候程序进程在，但是并不能对外提供服务。这种场景下该检查方式就非常有用。

健康检查方式

- **HTTP请求方式**

  探针往容器发送HTTP请求，如果探针收到2xx或3xx的返回状态码，说明容器是健康。

- **命令行脚本**

  探针执行容器中的命令并检查命令退出的状态码，如果状态码为0则说明健康。

  例如，您如果希望使用“cat /tmp/healthy”命令检查/tmp/healthy目录是否存在，则可以如下图配置。

  图 3-10 检查

公共参数说明

表 3-2 健康检查参数说明

参数	参数说明
延迟时间	延迟时间，单位为秒。例如，设置为10，表示从容器启动后10秒开始探测。
超时时间	超时时间，单位为秒。例如，设置为10，表明执行健康检查的超时等待时间为10秒，如果超过这个时间，本次健康检查就被视为失败。如果设置为0或不设置，默认超时等待时间为1秒。

使用 kubectl 设置健康检查

- 应用存活探针设置请参见**存活探针（liveness probe）**。
- 应用业务探针设置请参见**业务探针（Readiness probe）**。

3.1.9 远程终端

远程终端（web-terminal）提供连接容器功能，帮助您快速调试容器。

约束与限制

- web-terminal 默认是以sh shell登录容器，要求容器支持sh shell。
- 只有状态为“运行中”的容器可终端登录。
- 退出时，请在web-terminal中输入“exit”，否则会导致sh进程残留。

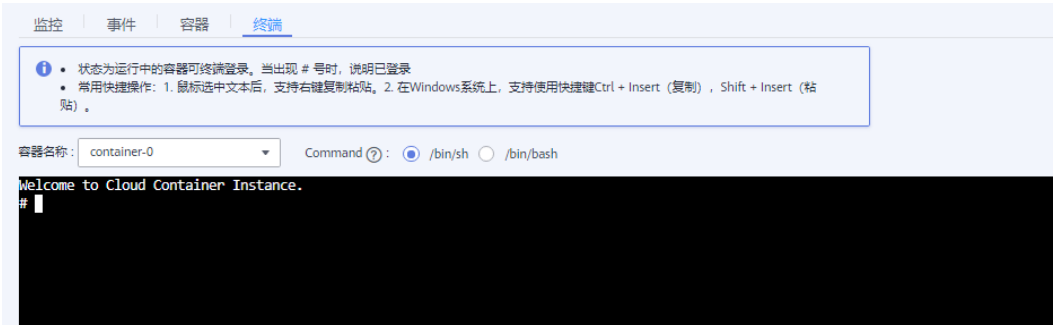
通过远程终端连接容器

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，在右侧页面单击要访问的工作负载。

步骤2 在Pod实例下面选择“终端”页签。

当出现“#” 号时，说明已登录。

图 3-11 容器终端



----结束

3.1.10 升级负载

负载创建成功后，可以对负载更新和升级。当前支持“滚动升级”和“替换升级”两种方式。

- 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老的实例上，因此业务不会中断。
- 替换升级：将先把您工作负载的老版本实例删除，再安装指定的新版本，升级过程中业务会中断。

升级负载

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，进入实例详情页面，单击右上角“升级”。

步骤2 修改Pod规格。

您可以选择使用GPU（只能在GPU型命名空间下）或不使用GPU。

具体的规格信息请参考**约束与限制**中的“Pod规格”。

步骤3 修改容器配置。

1. 单击“更换镜像”可以选择新的镜像，如下图所示。

图 3-12 更换镜像

- 我的镜像：展示了您上传到容器镜像服务的镜像。
- 开源镜像中心：展示了镜像中心的公共镜像。
- 共享镜像：展示了容器镜像服务中他人共享的镜像。

2. 镜像选择完成后，需要选择镜像的版本、设置容器名称、设置容器占用的CPU和内存规格，并选择是否开启采集标准输出文件（开启后，应用运维管理AOM将根据实际使用量进行计费）。

说明

每个租户一个月有500M的免费日志存储空间，超过500M时AOM将根据实际使用量进行收费，计费规则请参见**产品价格详情**。

对于Pod中只有一个容器能使用GPU，如果您的Pod中有个多个容器，您可以通过“开启GPU”这个开关选择哪个容器使用GPU。

您还可以为容器做如下高级设置：

- 存储：支持挂载持久化卷到容器中，以实现数据文件的持久化存储，当前支持云硬盘存储卷、文件存储卷和极速文件存储卷。单击“添加云硬盘存储卷”、“添加文件存储卷”或“添加极速文件存储卷”，输入名称、容量、容器内挂载路径，选择磁盘类型。负载创建完成后，可对存储卷进行管理，具体请参见**云硬盘存储卷**、**文件存储卷 3.0**或**极速文件存储卷**。

- 日志采集：支持根据您配置的日志输出路径，采集应用日志，请自行防爆处理。单击添加日志存储，输入容器内日志路径，调整日志存储空间。负载创建完成后，可在AOM界面查看日志，具体请参见**日志管理**。
- 环境变量：在容器中设置环境变量，支持手动输入和引用变量。环境变量为应用提供极大的灵活性，您可以在应用程序中使用环境变量，在创建容器时为环境变量赋值，容器运行时读取环境变量的值，从而做到灵活的配置，而不是每次都重新编写应用程序制作镜像。

  手动输入只需要直接输入变量名称和变量值。

  变量引用支持引用PodIP（Pod的IP地址）、PodName（Pod的名称）以及Secret，输入变量名称，选择引用类型、引用值。其中Secret引用的创建请参见**使用Secret**。
- 健康检查：健康检查是指容器运行过程中，根据您需要，定时检查容器健康状况。详细步骤请参见**健康检查**。
- 生命周期：生命周期脚本定义，在容器的生命周期的特定阶段执行调用。详细步骤请参见**容器生命周期**。
- 启动命令：输入容器启动命令，容器启动后会立即执行。启动命令对应于容器引擎的ENTRYPOINT启动命令，详细内容请参见**容器启动命令**。
- 配置管理：容器支持挂载ConfigMap和Secret。ConfigMap和Secret的创建请参见**使用ConfigMap**和**使用Secret**。

步骤4 单击“下一步”，选择升级策略。

您可以指定无状态工作负载的升级方式，包括逐步“滚动升级”和整体“替换升级”。

- 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老的实例上，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：将先把您工作负载的老版本实例删除，再安装指定的新版本，升级过程中业务会中断。

步骤5 单击“下一步”，单击“提交”，升级负载。

----结束

使用 kubectl 升级负载

使用kubectl升级负载请参见**Deployment**章节的“升级”部分。

3.1.11 伸缩负载

本节主要讲解工作负载弹性伸缩和手动伸缩的配置方式。请根据实际业务选择。

- 弹性伸缩：支持告警、定时、周期三种策略。配置完成后可基于资源变化、固定时间、固定周期自动触发实例的增减。
- 手动伸缩：配置完成后立即触发实例的增减。

须知

对于挂载了云硬盘存储卷的Pod，实例缩容时不会同步删除云硬盘。且再次创建相同名称的Pod时，无法挂载云硬盘。

弹性伸缩

说明

当前仅支持无状态负载弹性伸缩。

您可以根据业务需求自行定义伸缩策略，降低人为反复调整资源以应对业务变化和高峰压力的工作量，帮助您节约资源和人力成本。当前支持三种弹性伸缩策略：

告警策略：支持根据CPU/内存的使用率，进行工作负载的自动伸缩。工作负载创建完成后即可设置，在CPU/内存超过或少于一定值时，自动增减实例。

定时策略：支持在特定时间点进行工作负载的自动伸缩。适用于秒杀周年庆等活动，例如在秒杀这个时间点增加一定数量的实例个数。

周期策略：支持以天、周、月为周期的伸缩策略。适用于周期性的流量变化。

- **告警策略**：支持根据CPU/内存的使用率，进行工作负载的自动伸缩。
  a. 登录云容器实例控制台，在左侧导航栏中选择“工作负载 > 无状态（Deployment）”，单击工作负载名称进入负载详情。
  b. 在“伸缩”中，单击“弹性伸缩”，单击“添加伸缩策略”。

图 3-13 添加告警策略

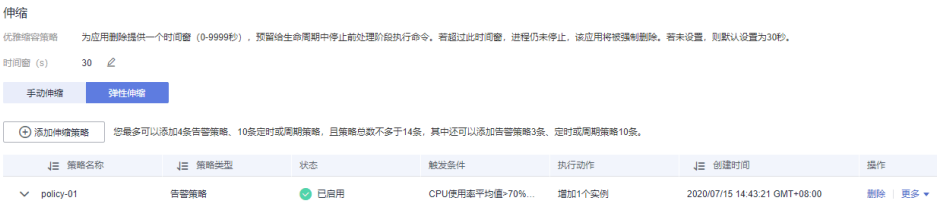
表 3-3 添加告警策略

参数	参数说明
策略名称	请输入伸缩策略的名称。
策略类型	选择“告警策略”。

参数	参数说明
触发条件	支持“CPU使用率”和“内存使用率”。 如果输入“内存使用率”的“平均值>70%”，表示在该条件下触发伸缩策略。
周期时长	指标统计周期。单击下拉选项进行选择。 如果设置为60秒，表示每60秒统计一次。
连续出现次数	如果设置为3，则表示指标数据连续三个统计周期达到了设定的阈值，则触发策略动作。
执行动作	策略触发后执行的动作。增加或减少实例数。

c. 单击“确定”。
在弹性伸缩下，可看到策略已启动。

图 3-14 策略已启动



待到触发条件发生时，弹性伸缩策略会自动启动。

- **定时策略**：支持在特定时间点进行工作负载的自动伸缩。
  a. 单击“弹性伸缩”，单击“添加伸缩策略”，选择“定时策略”。

图 3-15 定时策略

表 3-4 添加定时策略

参数	参数说明
策略名称	请输入伸缩策略的名称。
策略类型	选择定时策略。
触发时间	策略触发时间。
执行操作	策略触发后执行的动作。增加或减少实例数。

b. 单击“确定”。

在弹性伸缩下，可看到策略已启动。

- **周期策略**：支持以天、周、月为周期的伸缩策略。

a. 单击“弹性伸缩”，单击“添加伸缩策略”，选择“周期策略”

图 3-16 周期策略

表 3-5 添加周期策略

参数	参数说明
策略名称	请输入伸缩策略的名称。
策略类型	选择周期策略。
选择时间	选择策略触发的时间。
执行操作	策略触发后执行的动作。

b. 单击“确定”。

在弹性伸缩下，可看到策略已启动。

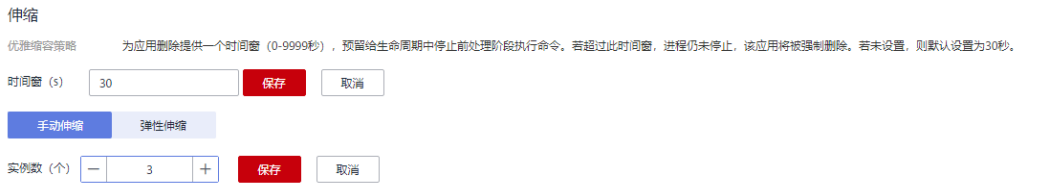
手动伸缩

步骤1 登录云容器实例控制台，在左侧导航栏中选择“工作负载 > 无状态负载（Deployment）”，单击工作负载名称。

步骤2 在“伸缩 > 手动伸缩”策略下，单击修改实例数量，例如修改为“3”，单击“保存”后实例伸缩操作即可生效。

云容器实例为应用删除提供一个时间窗，预留给生命周期中停止前处理阶段执行命令。如果超过此时间窗，进程仍未停止，该应用将被强制删除。

图 3-17 修改实例数



步骤3 在“Pod列表”处，可查看到新的实例在创建中，待状态为运行中时，表示已成功完成实例伸缩操作。

图 3-18 手动伸缩

----结束

3.1.12 客户端 DNS 配置

CCI支持通过dnsPolicy标记每个Pod配置不同的DNS策略。

- **None**：允许Pod忽略CCI预置的DNS设置。这种方式一般用于想要自定义DNS配置的场景，需要和dnsConfig配合一起使用，达到自定义DNS的目的。
- **Default**：使用CCI提供的内网DNS，能够完成服务域名和代理其他公网域名解析，具体请参见**华为云云解析服务提供的内网DNS地址**。

  说明

  使用该策略的前提是用户Pod所在命名空间没有安装CoreDNS插件，否则会被覆盖为ClusterFirst策略。

- **ClusterFirst**：使用命名空间安装的CoreDNS插件服务进行域名解析。任何与配置的集群域后缀（.cluster.local）不匹配的域名查询（例如，www.kubernetes.io）将转发到上游域名服务器（默认为内网DNS）。

  配置存根域和上游域名服务器的解析逻辑请参考**插件管理**。

  说明

  使用该策略的前提是用户Pod所在命名空间已经安装CoreDNS插件，否则会被覆盖为Default策略。

如果未明确指定dnsPolicy，则会根据是否安装CoreDNS插件设置默认值。即安装了CoreDNS，默认使用“ClusterFirst”，否则为“Default”。

dnsConfig字段说明：

dnsConfig为应用设置DNS参数，设置的参数将合并到基于dnsPolicy策略生成的域名解析文件中。当dnsPolicy为“None”，应用的域名解析文件完全由dnsConfig指定；当dnsPolicy不为“None”时，会在基于dnsPolicy生成的域名解析文件的基础上，追加dnsConfig中配置的dns参数。

- **nameservers**：DNS的IP地址列表。当应用的dnsPolicy设置为“None”时，列表必须至少包含一个IP地址，否则此属性是可选的。列出的DNS的IP列表将合并到基于dnsPolicy生成的域名解析文件的nameserver字段中，并删除重复的地址。

- **searches**：域名查询时的DNS搜索域列表，此属性是可选的。指定后，提供的搜索域列表将合并到基于dnsPolicy生成的域名解析文件的search字段中，并删除重复的域名。Kubernetes最多允许6个搜索域。
- **options**：DNS的配置选项，其中每个对象可以具有name 属性（必需）和value属性（可选）。该字段中的内容将合并到基于dnsPolicy生成的域名解析文件的options字段中，dnsConfig的options的某些选项如果与基于dnsPolicy生成的域名解析文件的选项冲突，则会被dnsConfig所覆盖。常见的配置选项有超时时间、ndots等。

通过前端创建负载配置 DNS 策略

图 3-19 客户端 DNS 配置

- 替换域名解析配置：对应None策略，填写的IP地址、搜索域、超时时间、ndots等具体配置将作为dnsConfig生效。
- 追加域名解析配置：对应ClusterFirst或者Default策略，最终值取决于是否安装CoreDNS插件。填写的具体配置将作为dnsConfig生效，会在基于dnsPolicy生成的域名解析文件的基础上，追加dnsConfig中配置的dns参数。

3.2 网络管理

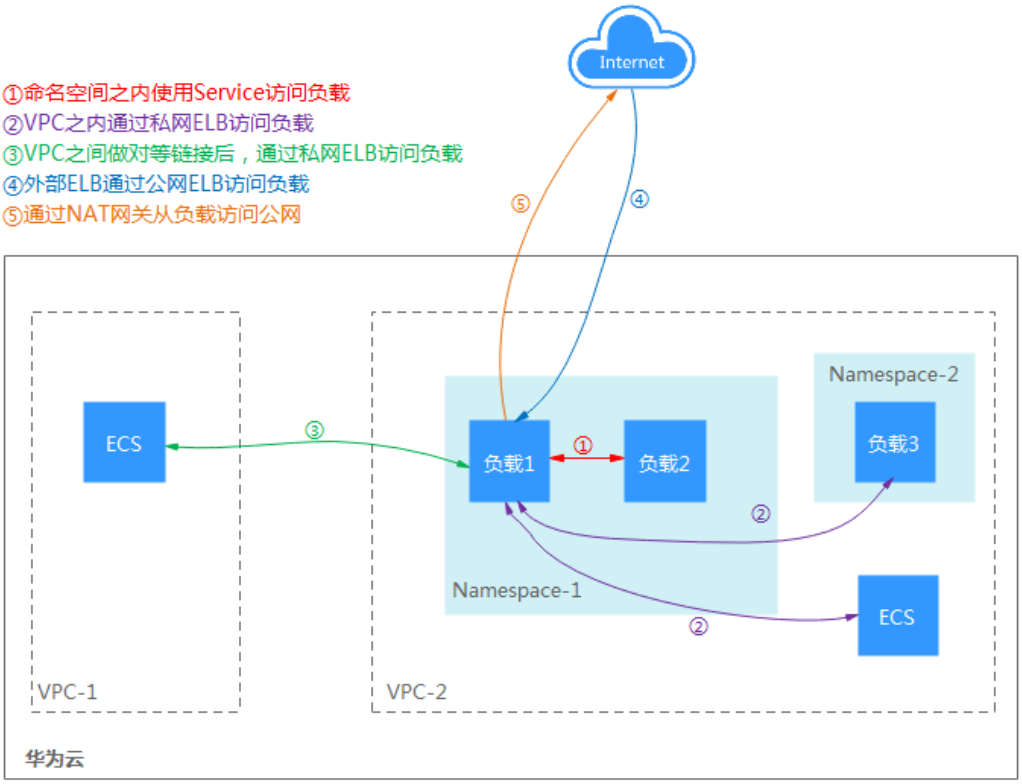
3.2.1 网络访问概述

负载访问可以分为如下几种场景：

- 内网访问：访问内网资源。
  - 使用“Service”方式访问：该方式适合CCI中同一个命名空间中的负载相互访问。
  - 使用ELB（私网）访问：该方式适合云服务内部资源（云容器实例以外的资源，如ECS等）且与负载在同一个VPC内互相访问，另外在同一个VPC不同命名空间的负载也可以选择此种方式。通过内网域名或ELB的“IP:Port”为内网提供服务，支持HTTP/HTTPS和TCP/UDP协议。如果是内网且与负载不在同一个VPC内，也可以选择创建VPC对等连接，使得两个VPC之间网络互通。

- **公网访问**：即给负载绑定ELB（ELB必须与负载在同一个VPC内），通过ELB从公网访问负载。
- **从容器访问公网**：通过在**NAT网关服务**中配置SNAT规则，使得容器能够访问公网。

图 3-20 网络访问示意图



3.2.2 内网访问

内网访问有如下两种情况：

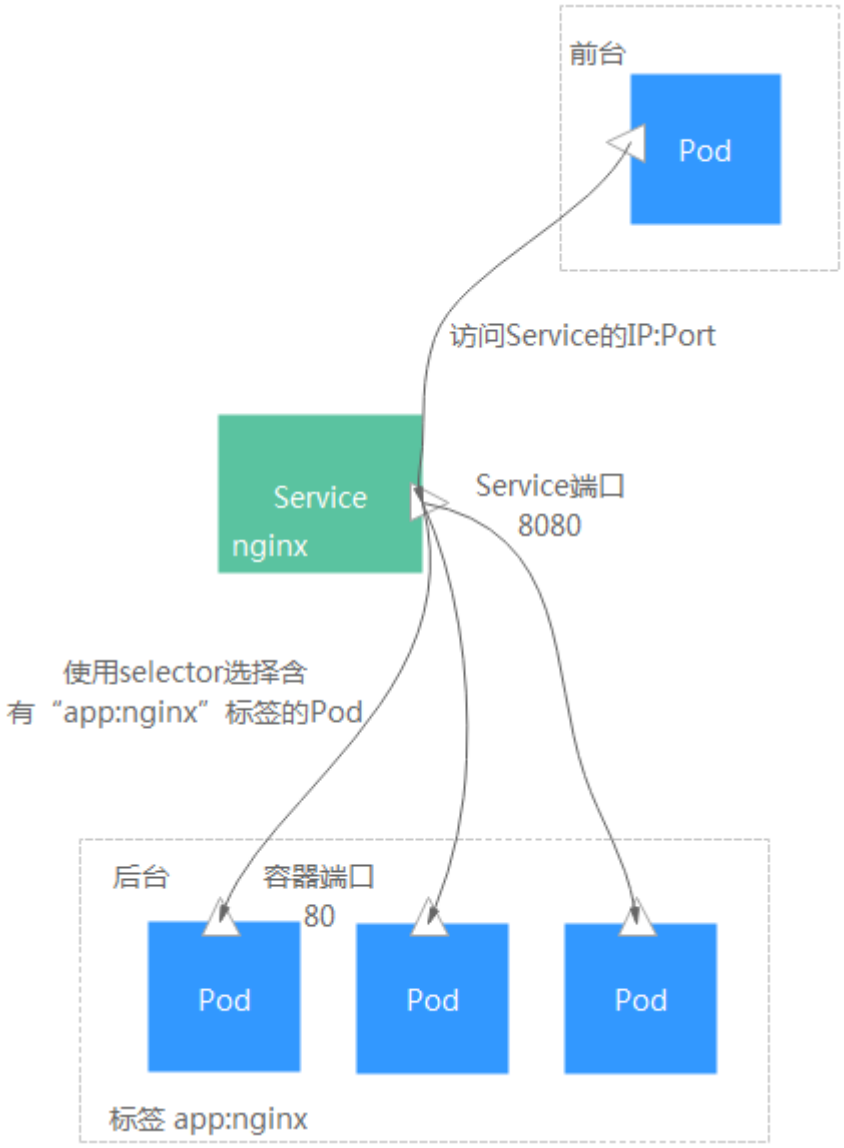
- **使用Service方式访问**：该方式适合CCI中同一个命名空间中的负载相互访问。
- **使用私网ELB访问**：该方式适合云服务内部资源（云容器实例以外的资源，如ECS等）且与负载在同一个VPC内互相访问，另外在同一个VPC不同命名空间的负载也可以选择此种方式。通过内网域名或ELB的“IP:Port”为内网提供服务，支持HTTP/HTTPS和TCP/UDP协议。如果是云服务内部且与负载不在同一个VPC内，也可以选择创建VPC**对等连接**，使得两个VPC之间网络互通。

负载中最小的资源单位就是Pod，访问负载就是访问负载中的Pod。负载中的Pod能够动态地创建和销毁，例如，扩缩容或者执行滚动升级，这时Pod的地址会发生变化，这为访问Pod带来了不便。

为解决该问题，云容器实例提供了coredns（内部域名解析）插件，Pod的变化由负载管理，外部无需感知。

访问负载只需要通过“服务名称:负载访问端口”即可，其中负载访问端口映射到容器端口。如下图所示，前台中的Pod如果要访问后台中的Pod时，只需要访问“nginx:8080”即可。

图 3-21 使用 Service 方式访问



使用 Service 方式访问-创建工作负载时设置

在云容器实例中，您只需要在创建负载时，填写服务名称和负载的端口配置，即可通过“服务名称:负载访问端口”访问到该负载。

- 服务名称：服务名称即Service的名称，Service是用于管理Pod访问的对象。Service的详细信息请参见**Service**。
- 安装coredns：coredns插件为您的其他负载提供内部域名解析服务，如果不安装coredns则无法通过“服务名称:负载访问端口”访问负载。
- 负载端口配置
  - 协议：访问负载的通信协议，可选择TCP或UDP。
  - 负载访问端口：负载提供的访问端口。
  - 容器端口：容器监听的端口，负载访问端口映射到容器端口。

使用 Service 方式访问-工作负载创建完成后设置

在工作负载创建完成后对Service进行配置，此配置对工作负载状态无影响，且实时生效。具体操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 服务（Service）”，在右侧页面单击“添加服务”。

步骤2 在“添加服务”页面，访问类型选择“集群内访问ClusterIP”。

步骤3 设置集群内访问参数。

- 服务名称：服务名称即Service的名称，Service是用于管理Pod访问的对象。
- 命名空间：工作负载所在命名空间。
- 关联工作负载：要添加Service的工作负载。
- 负载端口配置
  - 协议：访问负载的通信协议，可选择TCP或UDP。
  - 访问端口：负载提供的访问端口。
  - 容器端口：容器监听的端口，负载访问端口映射到容器端口。

步骤4 单击“提交”，工作负载已添加“集群内访问（ClusterIP）”的服务。

----结束

使用 kubectl 创建 Service

使用kubectl创建Service请参见**Service**。

使用私网 ELB 访问

如果需要从负载所在命名空间之外（云服务其他资源、云容器实例其他命名空间的负载）访问负载，可以通过绑定私网类型的共享型ELB实例（即创建ELB时类型选择私网），通过私网ELB的VIP访问负载。

此时需要选择私网ELB实例，其余配置方法与**公网访问**完全一致。

图 3-22 使用内网 ELB 访问-创建工作负载时

说明

CCI暂时不支持独享型负载均衡。

使用 Ingress 访问方式

您可以在工作负载创建完成后为其添加Ingress类型的访问方式，此配置对工作负载状态无影响，且实时生效。具体操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 路由（Ingress）”，在右侧页面单击“添加路由”。

步骤2 设置路由参数。

- 路由名称：自定义Ingress名称。
- 命名空间：选择需要添加Ingress的命名空间。
- 负载均衡：可以将互联网访问流量自动分发到工作负载所在的多个节点上。
- 对外端口：开放在负载均衡服务地址的端口，可任意指定。
- 对外协议：支持HTTP和HTTPS。如果选择HTTPS，请选择密钥证书，格式说明请参见**证书格式**。

  说明

  - 选择HTTPS协议时，才需要创建密钥证书ingress-test-secret.yaml。创建密钥的方法请参见**使用Secret**。
  - 同一个ELB实例的同一个端口配置HTTPS时，一个监听器只支持配置一个密钥证书。如果使用两个不同的密钥证书将两个Ingress添加到同一个ELB下的同一个监听器，ELB侧实际只生效最初的证书。

- **路由配置：**
  - **域名：**可选填。实际访问的域名地址，该域名需用户购买并备案，并确保所填域名能解析到所选负载均衡实例的服务地址。一旦配置了域名规则，则必须使用域名访问。
  - 路由匹配规则：当前仅支持前缀路由匹配。

    前缀路由匹配：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。
  - 映射URL：需要注册的访问路径。
  - 服务名称：选择需要添加Ingress的服务。
  - 服务端口：容器镜像中容器实际监听端口，需用户确定。

步骤3 配置完成后，单击“提交”。

创建完成后，在Ingress列表可查看到已创建成功的Ingress。

----结束

更新 Service

您可以在添加完Service后，更新此Service的端口配置，操作步骤如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 服务（Service）”，在Service页面中，选择对应的命名空间，单击需要更新端口配置的Service后的“更新”。

步骤2 更新集群内访问参数。

- **命名空间：**工作负载所在命名空间，此处不可修改。
- **关联工作负载：**要添加Service的工作负载，此处不可修改。

- **服务名称：**服务名称即Service的名称，Service是用于管理Pod访问的对象，此处不可修改。
- **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。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。

步骤3 单击“提交”，工作负载已更新Service。

----结束

更新 Ingress

您可以在添加完Ingress后，更新此Ingress的端口、域名和路由配置。操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 路由（Ingress）”，选择对应的命名空间，单击待更新Ingress后的“更新”。

步骤2 在“更新路由”页面，更新如下参数：

- **对外端口：**开放在负载均衡服务地址的端口，可任意指定。
- **路由配置：**可单击“添加映射”增加新的路由配置。
  - **域名：**可选填。实际访问的域名地址，该域名需用户购买并备案，并确保所填域名能解析到所选负载均衡实例的服务地址。一旦配置了域名规则，则必须使用域名访问。
  - 路由匹配规则：当前仅支持前缀路由匹配。

    前缀路由匹配：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。
  - 映射URL：需要注册的访问路径，例如：/healthz。
  - 服务名称：选择需要更新Ingress的服务。
  - 服务端口：容器镜像中容器实际监听端口，需用户确定。

  说明

  更改协议参数时服务会重新创建导致断连。如果大量创建、删除 、修改资源对象较多，会因为调用ELB流控，导致服务断连的时间较长。

步骤3 单击“提交”，工作负载已更新Ingress。

----结束

3.2.3 公网访问

概述

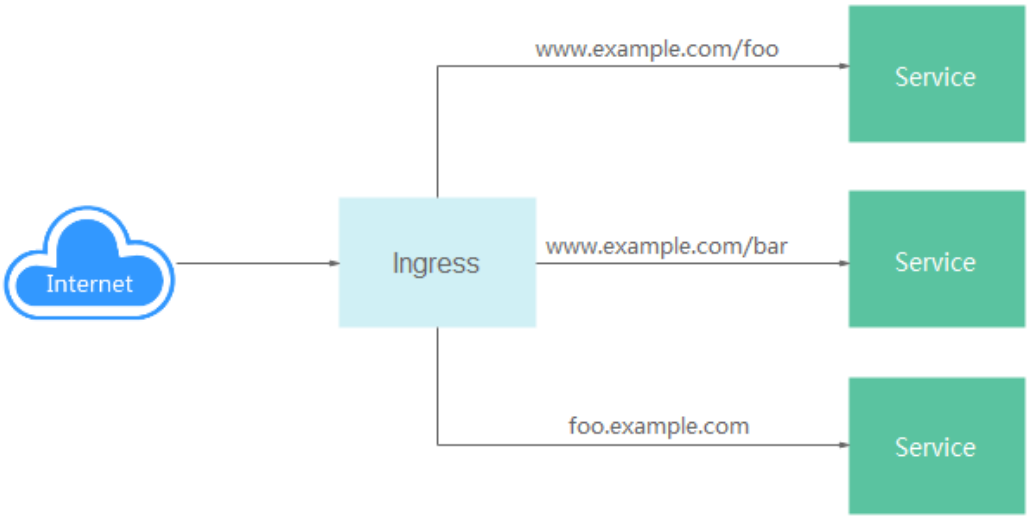
公网访问是指使用外部网络访问负载，您可以给负载绑定共享型ELB实例（ELB必须与负载在同一个VPC内），通过ELB实例访问负载，当前外部访问支持四层和七层负载公网访问。

- 四层公网访问支持TCP和UDP两种协议，设置完成后可以通过“elb公网ip:elb端口”访问负载。

- 七层公网访问支持HTTP和HTTPS两种协议访问，设置完成后，可以通过“http://公网域名(或elb 公网ip):elb端口/映射路径”访问负载。

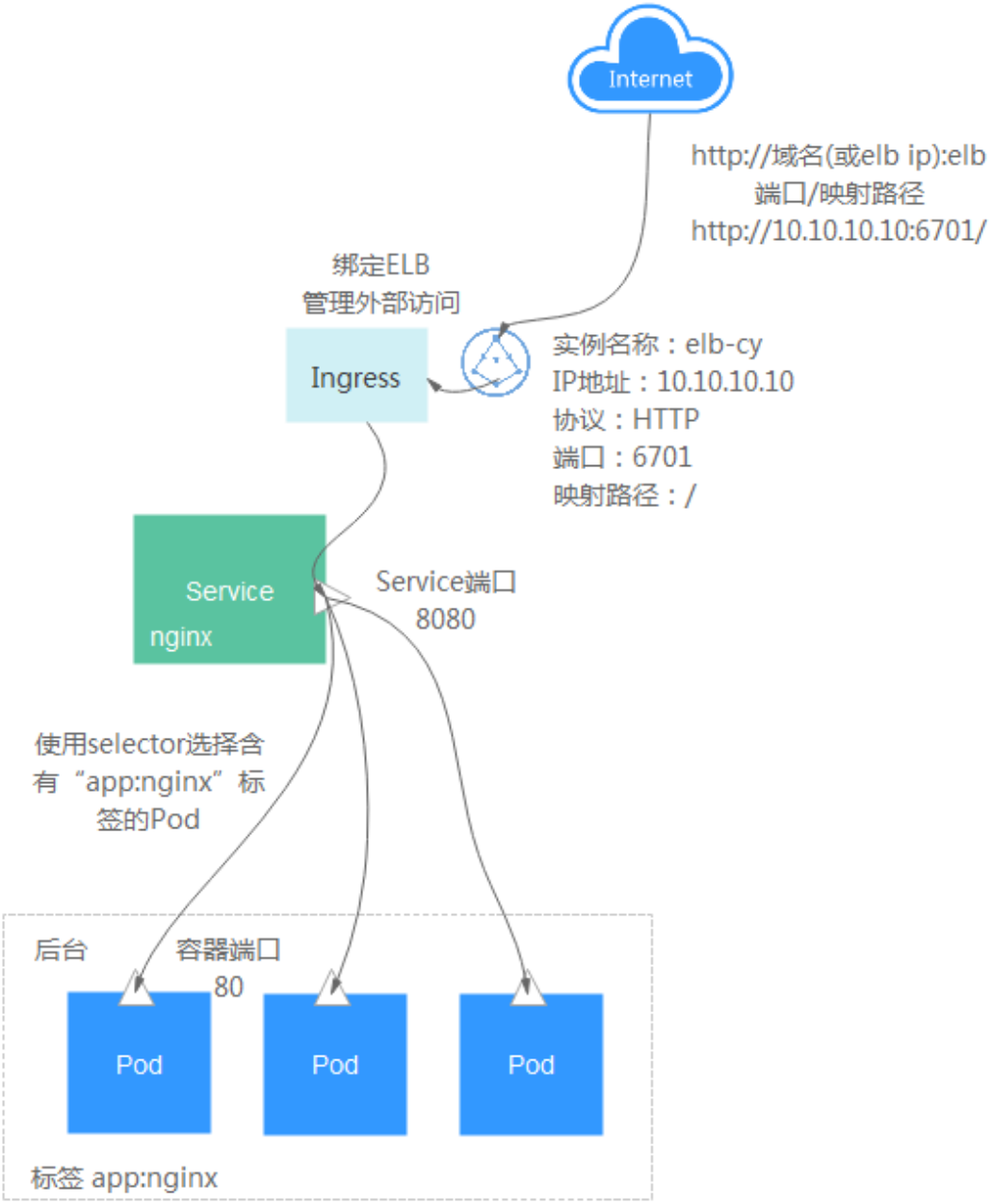
Service是基于四层TCP和UDP协议转发的，Ingress可以基于七层的HTTP和HTTPS协议转发，可以通过域名和路径做到更细粒度的划分，如下图所示。

图 3-23 Ingress-Service



下图是一个通过HTTP协议访问负载的示例。

图 3-24 公网访问



约束与限制

使用弹性公网IP（Elastic IP，简称EIP）前，请先了解EIP的**使用限制**。

配置公网访问-创建工作负载时设置

在云容器实例中，您只需要在创建负载时选择“公网访问”，然后配置如下参数。

- 服务名称：服务名称即Service的名称，Service是用于管理Pod访问的对象。Service的详细信息请参见**Service**。
- 安装coredns：coredns插件为您的其他负载提供内部域名解析服务，如果不安装coredns则无法通过“服务名称:负载访问端口”访问负载。

- ELB实例：选择ELB实例，如没有ELB实例可以单击“创建共享型ELB实例”去创建。

须知

此处创建的ELB需要与负载所在命名空间在同一个VPC内。
CCI暂时不支持独享型负载均衡，建议您创建共享型ELB实例。

- ELB协议：即公网访问使用的通信协议，支持HTTP、HTTPS、TCP和UDP协议。
- Ingress名称：Ingress是用于管理七层协议访问的对象。此处如果不配置，云容器实例会默认负载名称作为Ingress名称。Ingress的详细信息请参见**Ingress**。
- 公网域名（选择HTTP/HTTPS协议时可配置）：通过域名访问负载，公网域名需要您自行购买，并将域名解析指向所选的ELB实例弹性公网IP。
- 证书（选择HTTPS协议时必填）：SSL证书的导入方法请参见**添加SSL证书**。
- ELB端口：选择使用的ELB访问的具体协议和端口。
- 负载端口协议：访问负载的通信协议，可选择TCP或UDP，如果ELB协议选择为HTTP/HTTPS，则负载端口协议为TCP。
- 负载端口配置：
  - 负载访问端口：负载提供的访问端口。
  - 容器端口：容器监听的端口，负载访问端口映射到容器端口。
- HTTP路由配置
  - 映射路径：URL访问的路径，必须以“/”开头，如“/api/web”，也可以是根路径“/”。
  - 负载访问端口：前面设置的负载访问端口。

如下图所示，假如ELB实例的IP地址为“10.10.10.10”，则通过“http://10.10.10.10:6071/”就可以从公网访问到负载。

图 3-25 配置公网访问参数

配置公网访问-工作负载创建完成后设置

在工作负载创建完成后对Service进行配置，此配置对工作负载状态无影响，且实时生效。具体操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 服务（Service）”，在右侧页面单击“添加服务”。

步骤2 在“添加服务”页面，访问类型选择“负载均衡 LoadBalancer”。

步骤3 设置弹性负载均衡访问参数。

- 服务名称：服务名称即Service的名称，Service是用于管理Pod访问的对象。
- 命名空间：工作负载所在命名空间。
- 关联工作负载：要添加Service的工作负载。
- 负载均衡：选择公网ELB实例，如没有ELB实例可以单击“创建ELB实例”去创建。

须知

此处创建的ELB需要与负载所在命名空间在同一个VPC内。

CCI暂时不支持独享型负载均衡，建议您创建共享型ELB实例。

- 负载端口配置
  - 协议：访问负载的通信协议，可选择TCP或UDP。
  - 访问端口：负载提供的访问端口。
  - 容器端口：容器监听的端口，负载访问端口映射到容器端口。

步骤4 单击“提交”，工作负载已添加“负载均衡 LoadBalancer”的服务。

----结束

添加 DNAT 访问方式

工作负载创建后，如果想要使用公网访问Pod，除了使用ELB，还可以添加DNAT访问方式。具体操作如下：

步骤1 创建一个NAT网关。

步骤2 使用kubectl创建DNAT类型的Service，具体创建方式请参考**Service**，下面是一个DNAT类型的Service示例：

```
apiVersion: v1
kind: Service
metadata:
  name: nginx
  namespace: default  # 用户命名空间，默认为default
  annotations:
    kubernetes.io/elb.class: dnat       # 类型DNAT
    kubernetes.io/natgateway.id: 4b8cda3d-3543-4ebd-a55e-ca610b3b3c43 # NAT网关ID
spec:
  loadBalancerIP: 100.85.218.195      # DNAT使用的 EIP
  selector:
    app: nginx
  ports:
  - name: service0
    targetPort: 80     # Pod 暴露的端口
```



```
  port: 8080        # DNAT访问端口
  protocol: TCP
type: LoadBalancer   # Service的类型
```

步骤3 创建成功后，使用kubectl describe <service_name> -n <service_namespace> 可以查看Service更新状态。

----结束

创建并更新成功后，就可以使用EIP+Port的方式访问Pod了。

约束与限制：

1. 由于一条DNAT规则只能转发一个后端，因此一条DNAT Service也只能关联一个后端Pod，超过一个时DNAT规则绑定失败。
2. 一个 NAT 网关只能添加 200 条 DNAT 规则，具体限制参考**NAT**网关文档。
3. DNAT Service创建后前端可以查看到信息，但是请不要在前端进行修改设置。
4. 子网使用非默认路由需要在对应路由表中添加NAT网关的路由。
5. 如果在SNAT规则使用的网关下配置DNAT Service，请确保DNAT Service使用的EIP与SNAT规则绑定的EIP不同。
6. NAT网关的使用，具体可参考**NAT**网关文档。

添加 Ingress 访问方式

您可以在工作负载创建完成后为其添加Ingress类型的访问，此配置对工作负载状态无影响，且实时生效。具体操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 路由（Ingress）”，在右侧页面单击“添加路由”。

步骤2 设置路由参数。

- 路由名称：自定义Ingress名称。
- 命名空间：选择需要添加Ingress的命名空间。
- 负载均衡：可以将互联网访问流量自动分发到工作负载所在的多个节点上。
- 对外端口：开放在负载均衡服务地址的端口，可任意指定。
- 对外协议：支持HTTP和HTTPS。如果选择HTTPS，请选择密钥证书，格式说明请参见**证书格式**。

  说明

  - 选择HTTPS协议时，才需要创建密钥证书ingress-test-secret.yaml。创建密钥的方法请参见**使用Secret**。
  - 同一个ELB实例的同一个端口配置HTTPS时，一个监听器只支持配置一个密钥证书。如果使用两个不同的密钥证书将两个Ingress添加到同一个ELB下的同一个监听器，ELB侧实际只生效最初的证书。
- **域名：**可选填。实际访问的域名地址，该域名需用户购买并备案，并确保所填域名能解析到所选负载均衡实例的服务地址。一旦配置了域名规则，则必须使用域名访问。
- **路由配置：**
  - 路由匹配规则：当前仅支持前缀路由匹配。

    前缀路由匹配：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。

- 映射URL：需要注册的访问路径。
- 服务名称：选择需要添加Ingress的服务。
- 服务端口：容器镜像中容器实际监听端口，需用户确定。

步骤3 配置完成后，单击“提交”。

创建完成后，在Ingress列表可查看到已创建成功的Ingress。

----结束

如何处理公网无法访问

1. 公网能正常访问的前提是负载已处于运行中状态，如果您的负载处于未就绪或异常状态，公网访问将无法正常使用。
2. 从负载开始创建到公网可以正常访问可需要1分钟到3分钟的时间，在此时间内网络路由尚未完成配置，请稍作等待。
3. 负载创建3分钟以后仍然无法访问。单击创建的负载进入详情页，在详情页单击访问配置下面的“事件”标签，查看访问事件，查看是否有告警事件。如下两种常见的事件。
   - Listener port is repeated：ELB监听器端口重复，是由于之前发布公网访问的负载，删除之后立刻创建使用相同ELB端口的公网访问负载，ELB实际删除端口需要一定的时间，因此首次创建失败，可以选择删除负载重新创建，也可以等待5-10分钟，公网访问可正常使用。
   - Create listener failed：创建ELB监听器失败，创建监听器失败的原因一般是超过配额限度，请选择其他配额充足的ELB实例。
4. 负载创建3分钟以后仍然无法访问，且无告警事件，可能原因是用户配置的容器端口实际上没有相应进程在监听，目前云容器实例服务无法检测出该类使用异常，需要您排查镜像是否有监听该容器端口。如果容器端口监听正确，此时无法访问的原因可能为ELB实例本身有问题，请排查ELB实例状态。

使用 kubectl 实现公网访问

公网访问需要配合Service和Ingress两个Kubernetes对象实现，具体请参见**Service**和**Ingress**。

更新 Service

您可以在添加完Service后，更新此Service的端口配置。操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 服务（Service）”，在Service页面中，选择对应的命名空间，单击需要更新端口配置的Service后的“更新”。

步骤2 更新负载均衡参数：

- 命名空间：工作负载所在命名空间，更新时此处不可修改。
- 关联工作负载：要添加Service的工作负载，更新时此处不可修改。
- 服务名称：服务名称即Service的名称，Service是用于管理Pod访问的对象，更新时此处不可修改。
- 负载均衡：更新时此处不可修改。
- 端口配置

- 协议：访问负载的通信协议，可选择TCP或UDP。
- 访问端口：负载提供的访问端口。
- 容器端口：容器监听的端口，负载访问端口映射到容器端口。

步骤3 单击“提交”。工作负载已更新Service。

----结束

更新 Ingress

您可以在添加完Ingress后，更新此Ingress的端口、域名和路由配置。操作如下：

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“网络管理 > 路由（Ingress）”，选择对应的命名空间，单击待更新Ingress后的“更新”。

步骤2 在“更新路由”页面，更新如下参数：

- **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：**可选填。实际访问的域名地址，该域名需用户购买并备案，并确保所填域名能解析到所选负载均衡实例的服务地址。一旦配置了域名规则，则必须使用域名访问。
- **路由配置：**可单击“添加映射”增加新的路由配置。
  - 路由匹配规则：当前仅支持前缀路由匹配。

    前缀路由匹配：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。
  - 映射URL：需要注册的访问路径，例如：/healthz。
  - 服务名称：选择需要更新Ingress的服务。
  - 服务端口：容器镜像中容器实际监听端口，需用户确定。

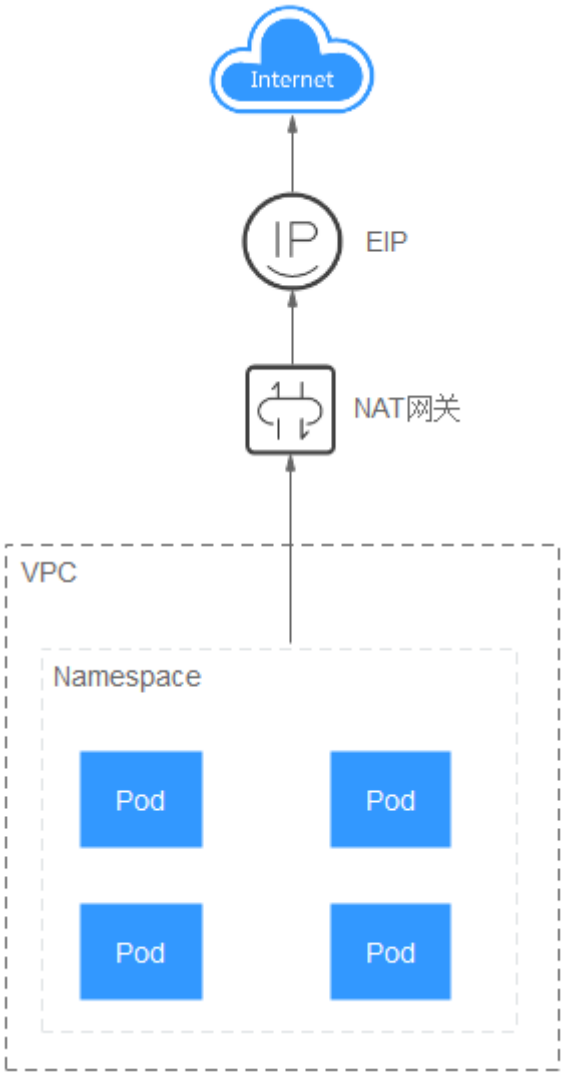
步骤3 单击“提交”，工作负载已更新Ingress。

----结束

3.2.4 从容器访问公网

您可以使用**NAT网关服务**，该服务能够为VPC内的容器实例提供网络地址转换（Network Address Translation）服务，SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内的容器实例共享弹性公网IP访问Internet。其原理如**图3-26**所示。通过NAT网关的SNAT功能，即使VPC内的容器实例不配置弹性公网IP也可以直接访问Internet，提供超大并发数的连接服务，适用于请求量大、连接数多的服务。

图 3-26 SNAT



您可以通过如下步骤实现容器实例访问Internet。

步骤1 “购买”弹性公网IP。

1. 登录管理控制台。
2. 在管理控制台左上角单击图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟私有云”。
4. 在左侧导航树，单击“弹性公网IP和带宽 > 弹性公网IP”。
5. 在“弹性公网IP”界面，单击“购买弹性公网IP”。
6. 根据界面提示配置参数。

说明

此处“区域”需选择容器实例所在区域。

图 3-27 购买弹性公网 IP

步骤2 购买NAT网关，具体请参见**购买NAT网关**。

1. 登录管理控制台。
2. 在管理控制台左上角单击图标，选择区域和项目。
3. 在系统首页，单击“网络 > NAT网关”。
4. 在NAT网关页面，单击“购买NAT网关”，进入NAT网关购买页面。
5. 根据界面提示配置参数。

说明

此处需选择容器实例所在**命名空间**相同的VPC和子网。

图 3-28 购买 NAT 网关

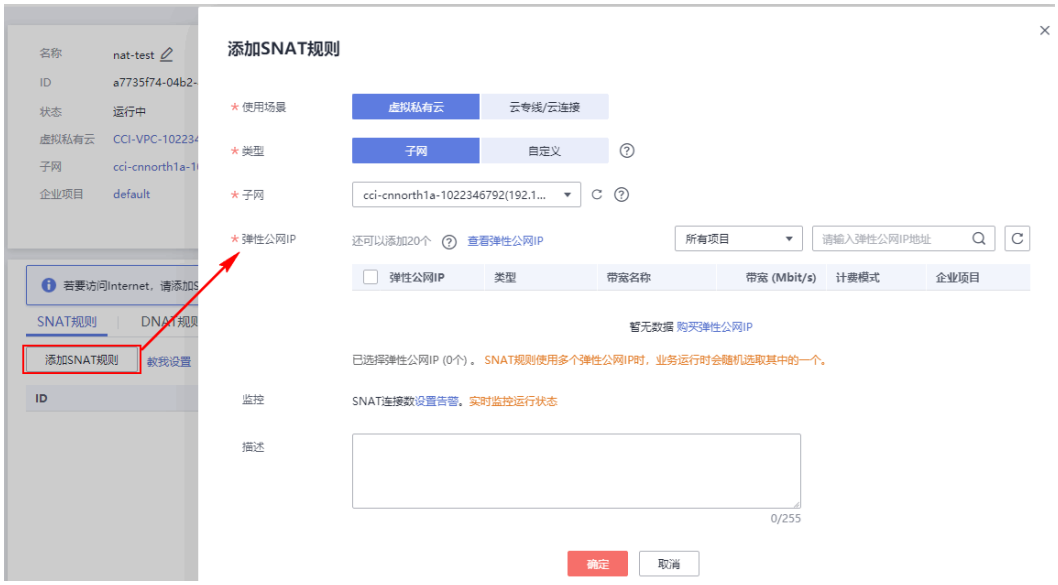
步骤3 配置SNAT规则，为子网绑定弹性公网IP，具体请参见**添加SNAT规则**。

1. 登录管理控制台。
2. 在管理控制台左上角单击图标，选择区域和项目。
3. 在系统首页，单击“网络 >NAT网关”。
4. 在NAT网关页面，单击需要添加SNAT规则的NAT网关名称。
5. 在SNAT规则页签中，单击“添加SNAT规则”。
6. 根据界面提示配置参数。

说明

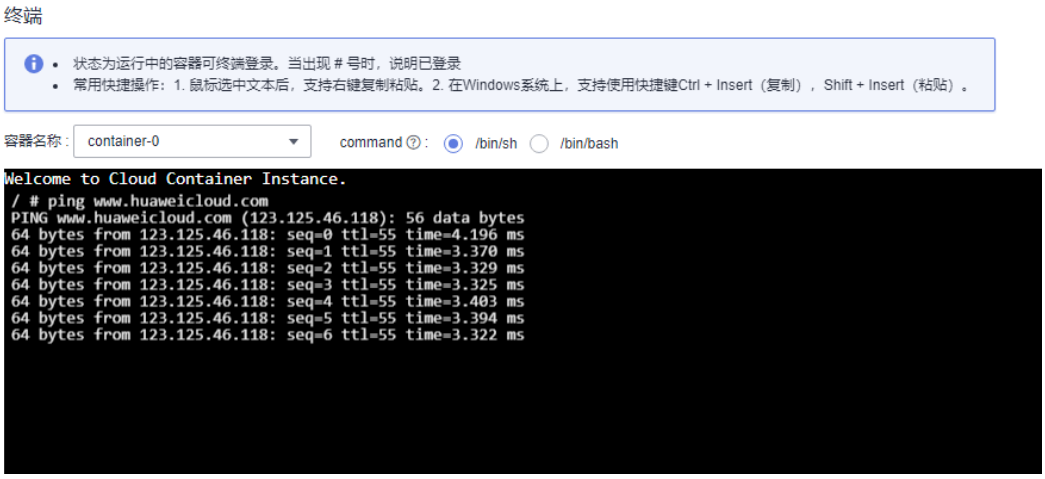
此处需选择容器实例所在**命名空间**相同的子网。

图 3-29 配置 SNAT 规则



SNAT规则配置完成后，您就可以从容器中访问公网了，如下图示例，从容器中能够ping通公网。

图 3-30 从容器中访问公网



----结束

3.3 存储管理

3.3.1 存储概述

云容器实例支持多种类型的持久化存储，满足您不同场景下的存储需求。创建工作负载时，可以使用以下类型的存储。

- **云硬盘存储卷**（EVS）

云容器实例支持将EVS创建的云硬盘存储卷挂载到容器的某一路径下。当容器迁移时，挂载的云硬盘存储卷将一同迁移。这种存储方式适用于需要永久化保存的数据。详情见**云硬盘存储卷**。

说明

使用EVS云硬盘存储卷时，请注意以下事项，否则会导致POD实例无法运行。

- 不支持多个POD挂载相同的EVS磁盘。
- 不支持单个POD同时挂载多个可用区的云硬盘卷。

- **文件存储卷**（SFS）

  云容器实例支持创建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。详情见**文件存储卷 3.0**。

- **极速文件存储卷**（SFS Turbo）

  云容器实例支持创建SFS Turbo极速文件存储卷并挂载到容器的某一路径下，极速文件存储卷具有按需申请，快速供给，弹性扩展，方便灵活等特点，适用于DevOps、容器微服务、企业办公等应用场景。详情见**极速文件存储卷**。

- **对象存储卷**（OBS）

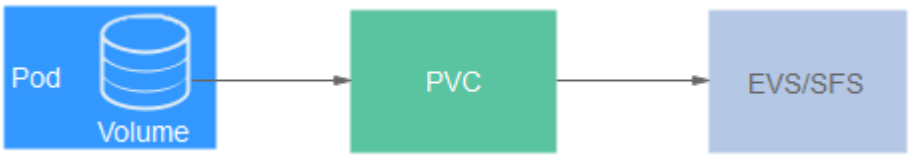
  云容器实例支持将OBS创建的对象存储卷挂载到容器的某一路径下。OBS是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。详情见**对象存储卷**。

PersistentVolumeClaim（PVC）

云容器实例使用PVC申请并管理持久化存储，PVC可以让您无需关心底层存储资源如何创建、释放等动作，而只需要申明您需要何种类型的存储资源、多大的存储空间。

在实际使用中，您可以通过Pod中的Volume来关联PVC，通过PVC使用持久化存储，如**图3-31**所示。

图 3-31 使用持久化存储



在云容器实例控制台，您可以导入已经创建的EVS、SFS和SFS Turbo，导入这些存储资源的同时会创建一个PVC用于这些存储资源。

您还可以在云容器实例控制台直接购买EVS和SFS，购买动作不仅购买实际的存储资源，同时还会创建PVC，也就是在这里购买就会直接导入到云容器实例中。

3.3.2 云硬盘存储卷

为满足数据的持久化需求，云容器实例支持将**云硬盘**（EVS）挂载到容器中。通过云硬盘，可以将存储系统的远端文件目录挂载到容器中，数据卷中的数据将被永久保存，即使删除了容器，只是卸载了挂载数据卷，数据卷中的数据依然保存在存储系统中。

EVS目前支持普通I/O（上一代产品）、高I/O、超高I/O三种规格。

- 普通I/O（上一代产品）：后端存储由SATA存储介质提供，适用于大容量，读写速率要求不高，事务性处理较少的应用场景，如：开发测试、企业办公应用。
- 高I/O：后端存储由SAS存储介质提供，适用于性能相对较高，读写速率要求高，有实时数据存储需求应用场景，如：创建文件系统、分布式文件共享。
- 超高I/O：后端存储SSD存储介质提供，适用于高性能、高读写速率要求、数据密集型应用场景，如：NoSQL、关系型数据库、数据仓库（如Oracle RAC，SAP HANA）。

使用限制

- 待挂载的云硬盘必须是按需付费，更多信息，请参见**云硬盘计费**。
- 云容器实例无法导入以下条件的磁盘：非当前可用区、状态非可用、系统盘、被CCE关联、非SCSI盘、非共享盘、专属存储、冻结盘、HANA服务器专属类型盘（高IO性能优化型/超高IO时延优化型）。
- 云硬盘存储卷只能当一个新盘来用。对于云容器实例没有挂载过的云硬盘存储卷，云硬盘存储卷中的内容对容器不可见。
- 对于已导入的云硬盘，如果在云硬盘控制台中删除该硬盘，云容器实例无法感知，建议您确定没有负载使用时再删除云硬盘。
- 一个云硬盘存储卷只能挂载到一个实例下，否则会存在数据丢失的情况。
- 云容器实例场景下不感知云硬盘扩容，如果需要扩容，请先在云容器实例控制台的“云硬盘存储卷”页面解关联对应的云硬盘，待云硬盘扩容完成后重新导入。

添加云硬盘

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 云硬盘存储卷”。

- 如果您在**云硬盘**中购买了云硬盘，可以这里导入后使用，请执行**步骤2**。
- 如果您还没购买云硬盘存储卷，可以直接在这里购买，请执行**步骤3**。

步骤2 单击“导入”，进入“导入云硬盘”页面，选择需要导入的云硬盘，然后单击“导入”。

说明

一块云硬盘只能导入一个命名空间，不能同时导入多个命名空间。如果一块云硬盘已经被导入到一个命名空间，则在其他命名空间下不可见，不能再次导入。**如果需要导入已经格式化文件系统（ext4）的EVS磁盘，需要确保磁盘没有设置分区，否则可能存在数据丢失的情况。**

导入后，您可以在看到对应的卷。

步骤3 单击“购买云硬盘存储卷”，填写相关参数，然后单击“立即购买”，确认规格后单击“提交”。

- PVC名称：PVC名称。
- 命名空间：PVC所在命名空间。
- 可用区：选择磁盘所在的可用区。
- 类型：磁盘的类型，可以选择高IO、普通IO（上一代产品）和超高IO。
- 磁盘容量：取值范围为[10, 32768]，单位为GiB。
- 加密：“KMS加密”默认不勾选。勾选“KMS加密”后，如果未创建委托请单击“创建委托”，并配置如下参数。

说明

目前“华东-上海一”、“华南-广州”和“华北-乌兰察布一”区域暂不支持“加密”功能。

- 委托名称：委托表示委托方通过创建信任关系，给被委托方授予访问其资源的权限。当“委托名称”为“EVSAccessKMS”时，表示已经成功授权访问EVS访问KMS，授权成功后，EVS可以获取KMS密钥用来加解密云硬盘系统。
- 密钥名称：密钥是一种用于存储应用所需要认证信息、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，可在容器应用中加载使用。如何创建密钥请参见**创建密钥**。
- 密钥ID：默认生成。

----结束

使用云硬盘

在**创建负载**的过程中，在添加容器后，展开“高级设置 > 存储”，选择“云硬盘存储卷”，单击“添加云硬盘存储卷”。

说明

当前云硬盘存储卷仅支持挂载单Pod。

负载创建成功后，可以在“存储管理 > 云硬盘存储卷”中查看到云硬盘与负载的关系。

使用 kubectl 创建云硬盘存储卷

使用kubectl创建云硬盘存储卷请参见**使用PersistentVolumeClaim申请持久化存储**。

3.3.3 对象存储卷

云容器实例支持将对象存储卷挂载到容器中。

对象存储服务（OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。OBS的更多信息，请参见**对象存储服务**。

使用限制

- 待挂载的对象存储必须是按需付费，更多信息，请参见**对象存储计费**。
- 请谨慎执行对象存储的删除操作，以避免造成CCI中容器不可用。
- 使用API方式挂载OBS，配置容器启动命令的限制，请参见**挂载OBS使用限制**“API参考>附录>挂载OBS使用限制”。

注意事项

- 并行文件系统是OBS提供的一种经过优化的高性能文件系统，提供毫秒级别访问时延，以及TB/s级别带宽和百万级别的IOPS，相较于OBS对象存储在稳定性、性能上更具优势。因此如需通过挂载方式，**生产环境中推荐您使用OBS并行文件系统**，而不推荐OBS对象存储。

导入对象存储

云容器实例支持导入已有的对象存储。为了确保对象存储卷的可靠性和稳定性，请在导入对象存储前先配置密钥，详情请参见**访问密钥**。

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 对象存储卷”，在右侧页面中选择命名空间，单击“上传密钥”。

步骤2 选择本地的密钥文件，单击“确认”。

请添加csv格式的文件，且文件大小不能超过2M。如果您在本地没有访问密钥，请前往“我的凭证”的**访问密钥**新增并下载访问密钥。

说明

需要下载主账号的访问密钥。

步骤3 在“对象存储卷”页面，单击“导入”。

步骤4 从列表里选择要导入的对象存储，单击“导入”。

如果无可用的对象存储，请单击“创建并行文件系统”去创建并行文件系统，填写相关参数，然后单击“立即创建”。

创建完成后，进入“导入对象存储”页面，选择新创建的对象存储，然后单击“导入”。

----结束

使用对象存储卷

说明

目前只支持任务（Job）使用对象存储卷，暂不支持Deployment，CronJob使用对象存储卷。

参照**创建任务**，在添加容器后，展开“高级设置 > 存储”，选择“对象存储卷”，单击“添加对象存储卷”，选择已有的对象存储卷。

图 3-32 配置对象存储卷参数

使用已有存储需要提前导入存储，具体步骤请参见**导入对象存储**。

3.3.4 文件存储卷 3.0

云容器实例支持创建**弹性文件存储**3.0（SFS 3.0）挂载到容器中，当前仅支持NFS协议类型的文件系统。SFS 3.0存储卷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。

支持的区域

各区域支持的文件存储卷类型，如下表所示：

表 3-6 各区域支持的存储类型

文件存储卷类型	华北-北京四	华东-上海二	华东-上海一	华南-广州	西南-贵阳一
SFS 3.0	√	x	√	√	x

使用限制

- 待挂载的文件存储必须是按需付费，更多信息，请参见**文件存储计费**。
- 使用文件存储期间，不能修改文件存储关联的VPC配置信息，否则CCI中容器无法访问文件存储。
- 请谨慎执行文件存储的删除操作，以避免造成CCI中容器不可用。

导入 SFS 3.0 容量型文件系统

说明

如需在VPC中访问SFS 3.0容量型，请先在VPC中购买SFS 3.0容量型的VPC终端节点，可参考**配置VPC终端节点**。如果已经购买了VPC终端节点，则不需要购买。

云容器实例支持导入已有的SFS 3.0文件存储。

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 文件存储卷”。

- 如果您在**弹性文件存储**中创建了SFS 3.0文件存储，可以这里导入后使用，请执行**2**。
- 如果您还没创建文件存储，可以直接在这里创建，请执行**步骤3**。

步骤2 单击“导入”，进入“导入文件存储”页面，选择需要导入的文件存储，然后单击“导入”。

步骤3 单击“创建文件存储卷”，填写相关参数，然后单击“立即创建”。

- **PVC名称**：PVC名称。
- **命名空间**：PVC所在命名空间。
- **存储类**：选择SFS 3.0容量型。
- **类型**：文件存储类型，当前支持NFS类型。
- **访问模式**：文件存储的访问模式，当前支持ReadWriteMany，即文件存储卷能够以读写模式被多个节点同时加载。

步骤4 对于SFS 3.0多读场景，数据存在缓存的情况，会导致原数据读取延迟。如果需要实时读取数据，可为已创建的文件系统指定挂载参数。

挂载参数可设置mount命令指定文件系统挂载的选项，当前支持noac，即用于禁止本地的文件和目录缓存，支持客户端实时从远端SFS 3.0读取数据。

说明

此处设置的挂载参数仅对当前命名空间下创建的文件存储卷有效。

图 3-33 设置 SFS 3.0 挂载参数

----结束

使用文件存储卷

参照**无状态负载（Deployment）**、**创建任务**或**创建定时任务**，在添加容器后，展开“高级设置 > 存储”，选择“文件存储卷”，单击“添加文件存储卷”。

可以选自动创建或使用已有文件存储，使用已有存储需要提前导入存储，具体步骤请参见**导入SFS 3.0容量型文件系统**。

默认导入的文件存储类型为SFS 3.0容量型。

图 3-34 默认存储类型为 SFS 3.0

挂载子路径为文件存储根路径下的子路径，如果不存在会自动在文件存储中创建。该路径必须为相对路径。

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，如果目录不为空，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 ，建议使用低权限账号启动，否则可能会造成宿主机高危文件被破坏。

使用 kubectl 创建文件存储卷

使用kubectl创建文件存储卷请参见**使用PersistentVolumeClaim申请持久化存储**。

3.3.5 文件存储卷 1.0（待下线）

云容器实例支持创建**弹性文件存储**1.0（SFS 1.0）挂载到容器中，当前仅支持NFS协议类型的文件系统。SFS 1.0存储卷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。

须知

SFS 1.0容量型文件存储即将下线，请谨慎使用。SFS 3.0与SFS 1.0文件系统规格差异小，可以使用SFS 3.0平滑替换SFS 1.0文件系统。

支持的区域

各区域支持的文件存储卷类型，如下表所示：

表 3-7 各区域支持的存储类型

文件存储卷类型	华北-北京四	华东-上海二	华东-上海一	华南-广州	西南-贵阳一
SFS	√	√	√	√	x

使用限制

- 待挂载的文件存储必须是按需付费，更多信息，请参见**文件存储计费**。
- 使用文件存储期间，不能修改文件存储关联的VPC配置信息，否则CCI中容器无法访问文件存储。
- 请谨慎执行文件存储的删除操作，以避免造成CCI中容器不可用。

导入 SFS 1.0 容量型文件系统

云容器实例支持导入已有的SFS文件存储。

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 文件存储卷”。

- 如果您在**弹性文件存储**中创建了文件存储，可以这里导入后使用，请执行**步骤2**。
- 如果您还没创建文件存储，可以直接在这里创建，请执行**步骤3**。

步骤2 单击“导入”，进入“导入文件存储”页面，选择需要导入的文件存储，然后单击“导入”。

步骤3 单击“创建文件存储卷”，填写相关参数，然后单击“立即创建”。

- **PVC名称**：PVC名称。
- **命名空间**：PVC所在命名空间。
- **类型**：文件存储类型，当前支持NFS类型。
- **总容量**：选择需要的容量，设置为“自动扩容卷”时，创建的文件存储卷容量不受限制。
- **访问模式**：文件存储的访问模式，当前支持ReadWriteMany，即文件存储卷能够以读写模式被多个节点同时加载。
- **加密**：“KMS加密”默认不勾选。勾选“KMS加密”后，如果未创建委托请单击“创建委托”，并配置如下参数。

  说明

  目前“华北-北京四”区域支持“加密”功能。

  - 委托名称：委托表示委托方通过创建信任关系，给被委托方授予访问其资源的权限。当“委托名称”为“EVSAccessKMS”时，表示已经成功授权访问EVS访问KMS，授权成功后，EVS可以获取KMS密钥用来加解密云硬盘系统。
  - 密钥名称：密钥是一种用于存储应用所需要认证信息、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，可在容器应用中加载使用。如何创建密钥请参见**创建密钥**。
  - 密钥ID：默认生成。

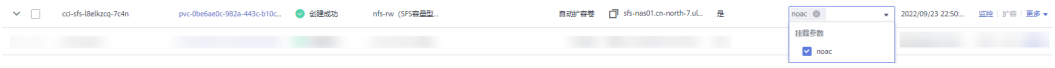
步骤4 对于SFS多读场景，数据存在缓存的情况，会导致原数据读取延迟。如果需要实时读取数据，可为已创建的文件系统指定挂载参数。

挂载参数可设置mount命令指定文件系统挂载的选项，当前仅支持noac，即用于禁止本地的文件和目录缓存，支持客户端实时从远端SFS读取数据。

说明

此处设置的挂载参数仅对当前命名空间下创建的文件存储卷有效。

图 3-35 设置 SFS 挂载参数



----结束

使用文件存储卷

参照**无状态负载（Deployment）**、**创建任务**或**创建定时任务**，在添加容器后，展开“高级设置 > 存储”，选择“文件存储卷”，单击“添加文件存储卷”。

可以选自动创建或使用已有文件存储，使用已有存储需要提前导入存储，具体步骤请参见**导入SFS 1.0容量型文件系统**。

- 选择导入的文件存储类型为SFS容量型。

  说明

  使用SFS容量型文件存储期间，不建议对文件存储进行容量调整，以避免造成数据丢失。

  图 3-36 选择存储类型为 SFS

挂载子路径为文件存储根路径下的子路径，如果不存在会自动在文件存储中创建。该路径必须为相对路径。

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，如果目录不为空，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 ，建议使用低权限账号启动，否则可能会造成宿主机高危文件被破坏。

使用 kubectl 创建文件存储卷

使用kubectl创建文件存储卷请参见**使用PersistentVolumeClaim申请持久化存储**。

3.3.6 极速文件存储卷

云容器实例支持创建**弹性文件存储** SFS Turbo（极速文件存储）并挂载到容器的某一路径下，极速文件存储具有按需申请，快速供给，弹性扩展，方便灵活等特点，适用于DevOps、容器微服务、企业办公等应用场景。

说明

SFS Turbo当前仅支持通用型文件系统，不支持HPC型文件系统。

使用限制

- 待挂载的极速文件存储必须是按需付费。更多信息，请参见**极速文件存储计费**。
- 使用极速文件存储期间，不能修改极速文件存储关联的VPC配置信息，否则CCI中容器无法访问极速文件存储。
- 请谨慎执行极速文件存储的删除操作，以避免造成CCI中容器不可用。

导入极速文件存储

云容器实例支持导入已有的极速文件存储。

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 极速文件存储卷”，在右侧页面中选择命名空间，单击“导入”。

步骤2 从列表里选择要导入的极速文件存储，单击“导入”。

如果无可用的极速文件存储，请单击“创建极速文件存储(SFS Turbo)”去创建。

创建完成后，进入“导入极速文件存储”页面，选择新创建的极速文件存储，然后单击“导入”。

图 3-37 导入极速文件存储卷

步骤3 对于SFS Turbo多读场景，数据存在缓存的情况，会导致原数据读取延迟。如果需要实时读取数据，可为导入的SFS Turbo指定挂载参数。

挂载参数可设置mount命令指定文件系统挂载的选项，当前仅支持noac，即用于禁止本地的文件和目录缓存，支持客户端实时从远端SFS Turbo读取数据。

说明

此处设置的挂载参数仅对当前命名空间下创建的极速文件存储卷有效。

图 3-38 设置 SFS Turbo 挂载参数

----结束

使用极速文件存储卷

参照**无状态负载（Deployment）**或**创建任务**，在添加容器后，展开“高级设置 > 存储”，选择“极速文件存储卷”，单击“添加极速文件存储卷”。

图 3-39 添加极速文件存储卷

说明

- 创建极速文件存储过程中需要创建单独的虚拟机，耗时较长。因此当前仅支持使用已有的极速文件存储卷。
- 挂载子路径为极速文件存储根路径下的子路径，如果不存在会自动在文件存储中创建。该路径必须为相对路径。

解关联极速文件存储卷

导入极速文件存储卷成功后，如果不需要使用极速文件存储，您可以解关联极速文件存储卷。解关联之后，创建工作负载时无法使用该极速文件存储。

说明

如果极速文件存储卷已被工作负载挂载，则无法解关联。

步骤1 登录云容器实例控制台，单击左侧导航栏的“存储管理 > 极速文件存储卷”，在极速文件存储卷列表中，单击极速文件存储卷后的“解关联”。

步骤2 查看系统提示，单击“确定”。

----结束

3.4 插件管理

kubernetes除了必要的支撑组件以外，其他的组件都是以插件的形式运行，如Kubernetes DNS，Kubernetes Dashboard等等。

插件是对现有功能的扩展，当前云容器实例提供了coredns插件供您使用，您可以在云容器实例界面上直接安装插件，从而方便的使用插件提供的功能。

coredns 插件介绍

coredns插件为您的其他负载提供内部域名解析服务。建议您不要对本负载进行删除、升级操作，否则将导致内部域名解析服务无法正常使用。

安装插件

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“插件管理 > 插件市场”，单击右侧页面。

图 3-40 coredns 插件

步骤2 选择“插件版本”，单击“提交”安装插件。

1. 安装2.5.9及以上版本的coredns插件时，还需配置如下参数：
   - 存根域：单击“添加”，您可对自定义的域名配置域名服务器，格式为一个键值对，键为DNS后缀域名，值为一个或一组DNS IP地址，如"acme.local --1.2.3.4,6.7.8.9"。
   - 上游域名服务器：解析除集群内服务域名及自定义域名之外的域名地址，格式为一个或一组DNS IP地址，例如"8.8.8.8","8.8.4.4"。
2. 安装2.5.10及以上版本的coredns插件时，还可配置如下参数：
   - 日志输出选项：您可根据业务需要，灵活配置需要打印的域名解析日志类别，便于发现问题，例如“输出解析成功日志”、“输出解析错误日志”，查看**日志输出选项含义**。

安装完成后，您可以在“插件管理 > 插件实例”中看到已安装的插件，如图。

图 3-41 coredns 插件安装成功

----结束

为 CoreDNS 配置存根域

集群管理员可以修改CoreDNS Corefile的ConfigMap以更改服务发现的工作方式。使用插件proxy可对CoreDNS的存根域进行配置。

如果集群管理员有一个位于10.150.0.1的Consul域名解析服务器，并且所有Consul的域名都带有.consul.local的后缀。在CoreDNS的ConfigMap中添加如下信息即可将该域名服务器配置在CoreDNS中：

```
consul.local:5353 {
        errors
        cache 30
        proxy . 10.150.0.1
    }
```

修改后最终的ConfigMap如下所示：

```
apiVersion: v1
data:
  Corefile: |-
    .:5353 {
        cache 30
        errors
        health
        kubernetes cluster.local in-addr.arpa ip6.arpa {
          pods insecure
          upstream /etc/resolv.conf
          fallthrough in-addr.arpa ip6.arpa
        }
        loadbalance round_robin
        prometheus 0.0.0.0:9153
        proxy . /etc/resolv.conf
        reload
    }

    consul.local:5353 {
        errors
        cache 30
        proxy . 10.150.0.1
    }
kind: ConfigMap
metadata:
```

```
name: coredns
namespace: kube-system
```

集群管理员可以修改CoreDNS Corefile的ConfigMap以更改服务发现的工作方式。使用插件proxy可对CoreDNS的存根域进行配置。

为 CoreDNS 配置日志输出选项

CoreDNS使用**log插件**将域名解析日志打印到标准输出，可通过配置日志输出选项灵活定义输出的日志内容，可在AOM中查看**解析日志**。在域名解析请求量较大的业务场景下，频繁打印域名解析日志到标准输出可能会对CoreDNS的性能造成明显的影响。

当前log插件支持解析成功、解析失败和解析错误三种日志输出选项配置，如图：

图 3-42 选项配置

对应的后端配置格式如下：

```
log [NAMES...] [FORMAT] {
    class CLASSES...
}
```

说明

CLASSES表示应记录的响应类别，是一个以空格分隔的列表。

日志输出选项配置具体含义如下：

- **输出解析成功日志：**

  勾选后将在log插件CLASSES中添加success响应参数，CoreDNS会将解析成功的日志打印到标准输出。

- **输出解析失败日志：**

  勾选后将在log插件CLASSES中添加denial响应参数， CoreDNS会将解析失败的日志，例如NXDOMAIN或nodata响应（名称存在，类型不存在）打印到标准输出。

- **输出解析错误日志：**

  勾选后将在log插件CLASSES中添加error响应参数，CoreDNS会将解析错误的日志打印到标准输出，例如SERVFAIL、NOTIMP、REFUSED等任何表示远程服务器不解析的请求消息，便于及时发现DNS服务器不可用等问题。

- **全不勾选：**

  如果未选中上述任一配置，则将关闭日志插件。

> **注意**
>
> 关闭日志插件仅影响CoreDNS的解析记录，而CoreDNS服务进程的日志记录依然会显示，不过该部分日志量极小，对性能无影响。

以勾选“输出解析成功日志”与“输出解析失败日志”为例，其后端log插件配置为：

```
log . {
    class success denial
}
```

创建成功的CoreDNS对应的ConfigMap如下：

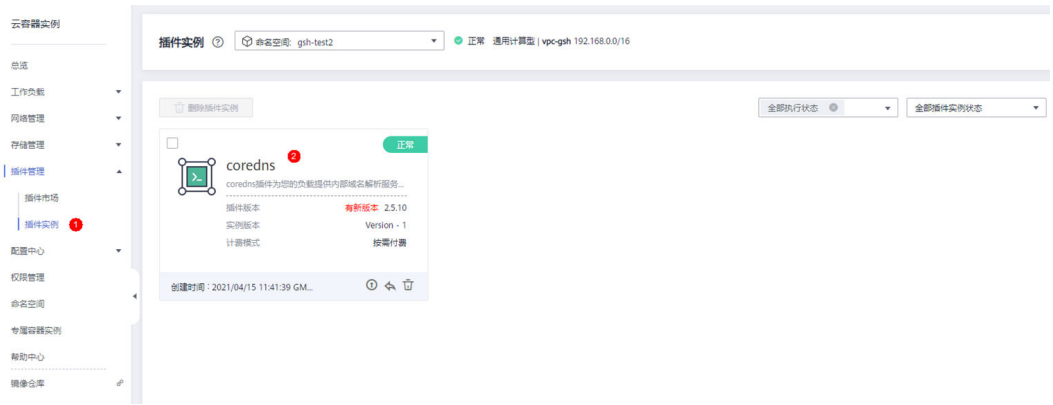
```
apiVersion: v1
data:
  Corefile: |-
    .:5353 {
        cache 30
        errors
        log . {
          classes success denial
        }
        health
        kubernetes cluster.local in-addr.arpa ip6.arpa {
          pods insecure
          upstream /etc/resolv.conf
          fallthrough in-addr.arpa ip6.arpa
        }
        loadbalance round_robin
        prometheus 0.0.0.0:9153
        proxy . /etc/resolv.conf
        reload
    }
kind: ConfigMap
metadata:
  name: coredns
  namespace: kube-system
```

查看解析日志

在配置解析日志插件后，可以通过AOM服务查看解析日志。

步骤1 在云容器实例管理控制台，左侧导航栏中选择“插件管理 > 插件实例”，右侧选择“CoreDNS”插件，进入CoreDNS插件页面。

图 3-43 插件实例列表



步骤2 单击资源列表中的coredns Deployment 进入pod列表。

图 3-44 CoreDNS Deployment

步骤3 在pod列表的操作一栏中选择“查看日志”选项，即可在AOM界面中查看coredns的日志。

图 3-45 Pod 列表

----结束

kubernetes 中的域名解析逻辑

DNS策略可以在每个pod基础上进行设置，目前，Kubernetes支持**Default、ClusterFirst、ClusterFirstWithHostNet和None**四种DNS策略，具体请参见**https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/**。这些策略在pod-specific的**dnsPolicy** 字段中指定。

- **“Default”**：如果dnsPolicy被设置为“Default”，则名称解析配置将从pod运行的节点继承。 自定义上游域名服务器和存根域不能够与这个策略一起使用。
- **“ClusterFirst”**：如果dnsPolicy被设置为“ClusterFirst”，任何与配置的集群域后缀不匹配的DNS查询（例如，www.kubernetes.io）将转发到从该节点继承的上游名称服务器。集群管理员可能配置了额外的存根域和上游DNS服务器。
- **“ClusterFirstWithHostNet”**：对于使用hostNetwork运行的Pod，您应该明确设置其DNS策略“ClusterFirstWithHostNet”。
- **“None”**：它允许Pod忽略Kubernetes环境中的DNS设置。应使用dnsConfigPod规范中的字段提供所有DNS设置 。

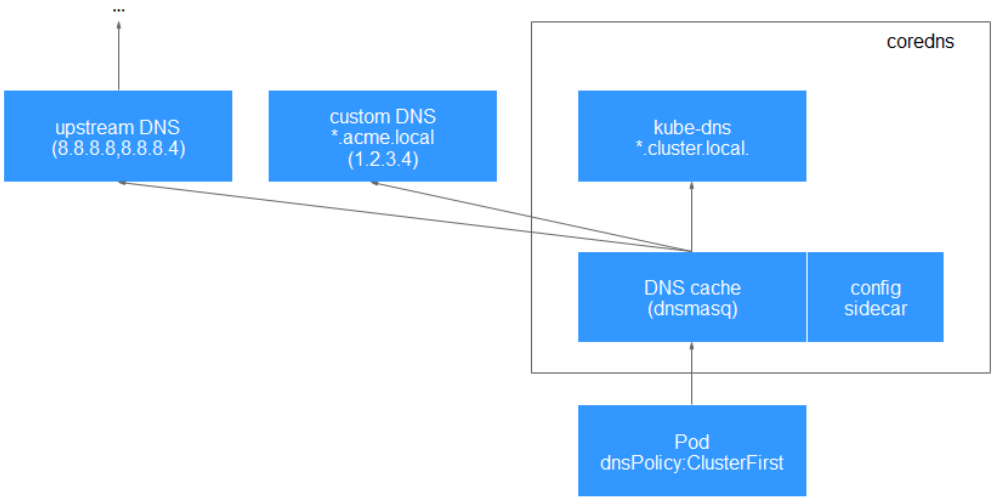
说明

- Kubernetes 1.10及以上版本，支持Default、ClusterFirst、ClusterFirstWithHostNet和None四种策略；低于Kubernetes 1.10版本，仅支持default、ClusterFirst和ClusterFirstWithHostNet三种。
- “Default”不是默认的DNS策略。如果dnsPolicy的Flag没有特别指明，则默认使用**“ClusterFirst”**。

路由请求流程：

- 未配置存根域：没有匹配上配置的集群域名后缀的任何请求，例如“www.kubernetes.io”，将会被转发到继承自节点的上游域名服务器。
- 已配置存根域：如果配置了存根域和上游 DNS 服务器，DNS 查询将基于下面的流程对请求进行路由：
  a. 查询首先被发送到 coredns 中的 DNS 缓存层。
  b. 从缓存层，检查请求的后缀，并根据下面的情况转发到对应的 DNS 上：
     - 具有集群后缀的名字（例如“.cluster.local”）：请求被发送到 coredns。
     - 具有存根域后缀的名字（例如“.acme.local”）：请求被发送到配置的自定义 DNS 解析器（例如：监听在 1.2.3.4）。
     - 未能匹配上后缀的名字（例如“widget.com”）：请求被转发到上游 DNS。

图 3-46 路由请求流程



后续处理

插件安装成功后，您还可以对插件做如下操作。

表 3-8 其他操作

操作	说明
升级	单击，选择要升级的目标版本，然后单击“下一步”，确认新的配置信息，单击“提交”。
回退	单击，选择要回退的目标版本，单击“提交”。
删除	单击，然后单击“确认”。 **须知** 删除操作无法恢复，请谨慎操作。

CoreDNS 域名解析插件版本发布记录

表 3-9 CoreDNS 域名解析插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.30.37	v1.27 v1.28 v1.29 v1.30 v1.31 v1.32 v1.33	支持CCE v1.33集群	1.11.4
1.30.33	v1.25 v1.27 v1.28 v1.29 v1.30 v1.31 v1.32	支持CCE v1.32集群	1.11.4
1.30.30	v1.25 v1.27 v1.28 v1.29 v1.30 v1.31	修复部分问题	1.11.4
1.30.29	v1.25 v1.27 v1.28 v1.29 v1.30 v1.31	支持CCE v1.31集群	1.11.4
1.30.6	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30	• 支持Corefile配置 • 适配CCE v1.30集群	1.10.1

插件版本	支持的集群版本	更新特性	社区版本
1.29.5	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	修复部分问题	1.10.1
1.29.4	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群	1.10.1
1.28.7	v1.21 v1.23 v1.25 v1.27 v1.28	支持插件热更新配置，无需滚动升级	1.10.1
1.28.5	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	1.10.1
1.28.4	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群	1.10.1
1.27.4	v1.19 v1.21 v1.23 v1.25 v1.27	-	1.10.1
1.27.1	v1.19 v1.21 v1.23 v1.25 v1.27	适配CCE v1.27集群	1.10.1

插件版本	支持的集群版本	更新特性	社区版本
1.25.1	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群	1.8.4
1.23.3	v1.15 v1.17 v1.19 v1.21 v1.23	插件依赖例行升级	1.8.4
1.23.2	v1.15 v1.17 v1.19 v1.21 v1.23	插件依赖例行升级	1.8.4
1.23.1	v1.15 v1.17 v1.19 v1.21 v1.23	适配CCE v1.23集群	1.8.4
1.17.15	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群	1.8.4
1.17.9	v1.15 v1.17 v1.19	插件依赖例行升级	1.8.4
1.17.7	v1.15 v1.17 v1.19	同步至社区v1.8.4版本	1.8.4
1.17.4	v1.17 v1.19	适配CCE v1.19集群	1.6.5
1.17.3	v1.17	支持v1.17集群，修复存根域配置问题	1.6.5
1.17.1	v1.17	支持v1.17集群	1.6.5

3.5 配置中心

3.5.1 配置中心概述

ConfigMap

ConfigMap是一种用于存储应用所需配置信息的资源类型。资源创建完成后，可在容器应用中作为文件使用。详情请参见**使用ConfigMap**。

Secret

Secret是Kubernetes中一种加密存储的资源对象，您可以将认证信息、证书、私钥等保存在密钥中，在容器启动时以环境变量加载到容器中，或以文件方式挂载到容器中。详情请参见**使用Secret**。

说明

- Secret与SSL证书共用同一个配额。
- 建议用户对上传的Secret进行加密处理。

SSL 证书

SSL（安全套接层，Secure Sockets Layer）是一种安全协议，云容器实例支持上传SSL证书，通过安装SSL证书可以实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证了双方传递信息的安全性。当在云容器实例服务上部署Web应用需要安全的公网访问时，您可以在创建负载时的访问配置页选择公网访问，ELB协议选择HTTPS协议，再选择该公网访问的证书。详情请参见**添加SSL证书**。

说明

Secret与SSL证书共用同一个配额。

3.5.2 使用 ConfigMap

创建 ConfigMap

步骤1 登录云容器实例控制台，单击左侧导航栏的“配置中心 > 配置项（ConfigMap）”，在右侧页面中选择命名空间，单击“创建配置项”。

CCI控制台上也支持直接使用YAML方式创建配置项，在右上角单击YAML创建，输入ConfigMap的YAML定义内容，单击“确定”即可，YAML定义可以参考**yaml格式**。

步骤2 云容器实例支持“手工输入”和“文件上传”两种方式来创建ConfigMap。

- 方式一：手工输入。参照**表3-10**设置新增配置参数，其中带“*”标志的参数为必填参数。

表 3-10 新建配置参数说明

参数	参数说明
基本信息	

参数	参数说明
*配置项名称	新建的ConfigMap名称。 请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到253字符的字符串
描述	ConfigMap的描述信息。
配置项数据	ConfigMap存储的配置数据。其中，“键”代表文件名；“值”代表文件中的内容。 1. 单击“添加数据”。 2. 输入键、值。
配置项标签	标签以Key/value键值对的形式附加到各种对象上（如负载、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。 **说明** 如您的组织已经设定云容器实例的相关标签策略，则需按照标签策略规则为配置项添加标签。标签如果不符合标签策略的规则，则可能会导致配置项创建失败，请联系组织管理员了解标签策略详情。

- 方式二：文件上传。

  说明

  云容器实例支持json或yaml格式，且文件大小需要小于1MB，详细请参见**ConfigMap文件格式要求**。

  单击“添加文件”，选择已创建的ConfigMap类型资源文件后，单击“打开”。

步骤3 配置完成后，单击“创建”。

----结束

ConfigMap 的使用

配置项创建完成后，可以在创建负载的过程中挂载到容器指定路径下，如下图所示，将名为cci-configmap01的配置项挂载到“/tmp/configmap1”路径下。

图 3-47 使用 ConfigMap

负载创建后，在“/tmp/configmap1”路径下将创建配置文件，配置项的“键”代表文件名；“值”代表文件中的内容。

ConfigMap 文件格式要求

ConfigMap资源文件支持json和yaml两种格式，且数据值大小不得超过1MB。

- json格式

  文件名称为configmap.json，配置示例如下：

```
{
  "kind": "ConfigMap",
  "apiVersion": "v1",
  "metadata": {
    "name": "nginxconf",
    "namespace": "cci-namespace-demo"
  },
  "data": {
    "nginx.conf": "server {\n    listen       80;\n    server_name  localhost;\n\n    location / {\n        root   html;\n        index  index.html index.htm;\n    }\n}"
  }
}
```

- yaml格式

  文件名称为configmap.yaml，配置示例如下：

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: nginxconf
  namespace: cci-namespace-demo
data:
  nginx.conf: |-
    server {
        listen       80;
        server_name  localhost;

        location / {
            root   html;
            index  index.html index.htm;
        }
    }
```

使用 kubectl 创建 ConfigMap

使用kubectl创建ConfigMap请参见**ConfigMap**。

3.5.3 使用 Secret

创建 Secret

步骤1 登录云容器实例控制台，单击左侧导航栏的“配置中心 > 密钥（Secret）”，在右侧页面中选择命名空间，单击“创建密钥”。

步骤2 云容器实例支持“手工输入”和“文件上传”两种方式来创建Secret。

- 方式一：手工输入。参照表3-11设置基本信息，其中带“*”标志的参数为必填参数。

表 3-11 基本信息说明

参数	参数说明
基本信息	
*密钥名称	新建Secret的名称。 以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到253字符的字符串。
描述	密钥的描述信息。
*密钥数据	Secret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“添加数据”。 2. 输入键、值（支持base64自动转码，如果您勾选“自动转码”，则可以输入未转码的Secret值）。
密钥标签	标签以Key/value键值对的形式附加到各种对象上（如应用、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。 **说明** 如您的组织已经设定云容器实例的相关标签策略，则需按照标签策略规则为密钥添加标签。标签如果不符合标签策略的规则，则可能会导致密钥创建失败，请联系组织管理员了解标签策略详情。

- 方式二：文件上传。

  说明

  云容器实例支持json或yaml格式，且文件大小不得超过2MB，详细请参见Secret文件格式说明。

  单击“添加文件”，选择已创建的Secret类型资源文件后，单击“打开”。

步骤3 配置完成后，单击“创建”。

Secret列表中会出现新创建的Secret。

----结束

Secret 的使用

Secret创建完后，可以在创建负载的过程中作为环境变量引用，或以文件方式挂载到容器中。

图 3-48 使用环境变量挂载 Secret

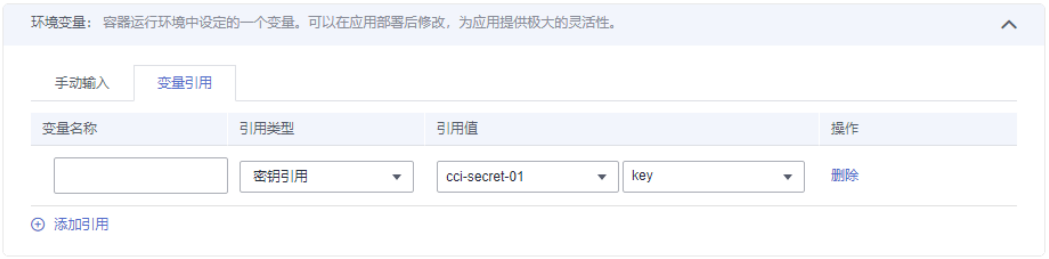


图 3-49 将 Secret 挂载到容器中

说明

挂载路径的字符串长度不能超过256个字符。

Secret 文件格式说明

- secret.yaml资源描述文件

  例如现在有一个应用需要获取下面的key-value并加密，可以通过Secret来实现：

  key1: value1

  key2: value2

  定义的Secret文件secret.yaml内容如下。其中Value需要进行Base64编码，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
  annotations:
    description: "test"
  labels:
    label-01: value-01
    label-02: value-02
data:
  key1: dmFsdWUx    #需要用Base64编码
```



```
  key2: dmFsdWUy    #需要用Base64编码
type: Opaque        # 必须为Opaque
```

- secret.json资源描述文件

  定义的Secret文件secret.json内容如下。

```
{
    "apiVersion": "v1",
    "kind": "Secret",
    "metadata": {
        "annotations": {
            "description": "test"
        },
        "labels": {
            "label-01": "value-01",
            "label-02": "value-02"
        },
        "name": "mysecret"
    },
    "data": {
        "key1": "dmFsdWUx",
        "key2": "dmFsdWUy"
    },
    "type": "Opaque"
}
```

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 "3306" | base64
MzMwNg==
```

使用 kubectl 创建 Secret

使用kubectl创建Secret请参见**Secret**。

3.5.4 添加 SSL 证书

SSL 证书介绍

SSL证书就是遵守SSL（Secure Socket Layer）协议，由受信任的数字证书颁发机构CA，在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能。服务器通过安装SSL证书可以实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证了双方传递信息的安全性，而且可以通过服务器证书验证他所访问的网站是否是真实可靠。

SSL证书分为权威证书和自签名证书。权威证书由权威的数字证书认证机构签发，您可向第三方证书代理商购买，使用权威证书的Web网站，默认客户端都是信任的。自签名证书是由用户自己颁发给自己的，一般可以使用openssl生成，默认客户端是不信任的，浏览器访问时会弹出告警，选择忽略告警可继续正常访问。

使用场景

SSL（安全套接层，Secure Sockets Layer）是一种安全协议，云容器实例支持上传SSL证书，通过安装SSL证书可以实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证了双方传递信息的安全性。当在云容器实例服务上部署Web应用需要安全的公网访问时，您可以在创建负载时的访问配置页选择公网访问，ELB协议选择HTTPS协议，再选择该公网访问的证书。

说明

Secret与SSL证书共用同一个配额。

添加 SSL 证书

步骤1 登录云容器实例控制台，单击左侧导航栏的“配置中心 > SSL证书”，在右侧页面中选择命名空间，单击“添加证书”。

步骤2 填写SSL证书名称和描述信息。

证书名称要求：请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到253字符的字符串。

须知

默认证书的名称为“default-ingress-ssl”，您应避免为SSL证书取名为“default-ingress-ssl”，否则会被默认证书覆盖而无法生效。

步骤3 上传证书文件和私钥文件。

- 证书文件支持“.crt”和“.cer”格式，且大小不超过1MB，文件内容须符合对应的CRT、CER协议。
- 私钥文件支持“.key”和“.pem”格式，且大小不超过1MB，私钥不能加密。

图 3-50 上传 SSL 证书文件

步骤4 单击“添加”，完成上传。

----结束

使用 SSL 证书

当服务有公网访问时，可以使用SSL证书，设置ELB为HTTPS协议。

在**创建负载**的过程中，负载访问方式选择“公网访问”，ELB协议选择“HTTP/HTTPS”，证书选项选择SSL证书，负载创建过程中会将SSL证书自动安装到弹性负载均衡器上，从而实现数据传输加密。

图 3-51 使用 SSL 证书

负载创建完成后，云容器实例将会在ELB中创建与负载名字相同证书。云容器实例服务创建以“beethoveen-cci-ingress”开头名称的证书，请勿删除或更新该类证书，否则引起访问异常。

更新与删除 SSL 证书

- 在证书过期前可以更新相应的证书，使用该证书的负载会同步更新。
- 请勿删除正在被负载使用的证书，否则可能导致应用无法访问。

3.6 镜像快照

3.6.1 镜像快照概述

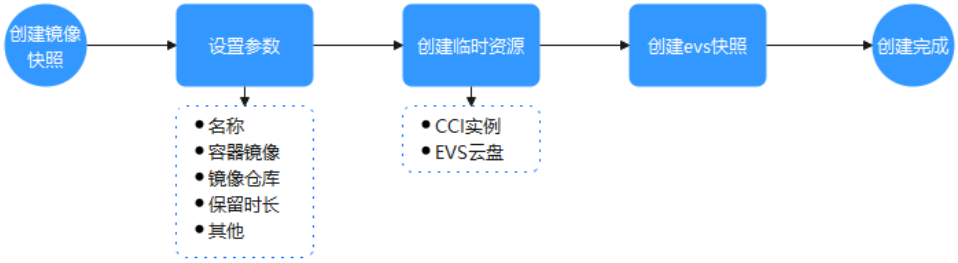
用户通过CCI镜像快照功能，能够实现从SWR镜像仓库、开源镜像仓库、自建镜像仓库拉取镜像制作成相应的镜像快照。在创建负载过程中，使用预先创建的镜像快照，可以跳过镜像拉取动作，提升负载的启动速度。

用户在创建Pod时使用镜像快照（ImageSnapshot），可以避免镜像下载，减少Pod启动时间。本文将介绍镜像快照的基本功能，创建和使用方式等。

约束与限制

- 单个镜像快照最多包含20个镜像。
- 支持私有镜像仓库，但需要提供私有镜像仓库的访问凭证，包括地址、用户名和密码。
- 如果镜像需要通过公网拉取，则需要事先配置NAT网关服务。
- 如果镜像快照中只有部分镜像与Pod中镜像相符，则不相符的镜像仍需通过下载拉取。
- CCI实例运行中镜像信息发生变动，且新镜像与匹配的镜像快照中镜像无相符的场景，则新镜像仍需通过下载拉取。

镜像快照创建过程如下图所示：



使用方式

使用镜像快照创建Pod，支持以下两种方式：

- 自动匹配

自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。按以下顺序进行匹配：

a. 镜像匹配度：优先选择匹配度高的镜像快照，匹配度指的是Pod和镜像快照两者在镜像上的匹配情况。

b. 创建时间：优先选择创建时间更新的镜像快照。

- 明确指定

明确指定使用的镜像快照。该镜像缓存必须为创建完成可用（Available）状态。

3.6.2 创建镜像快照

操作场景

本章介绍了如何在控制台创建镜像快照。要了解镜像快照的工作原理，请参阅**镜像快照概述**。

操作步骤

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“镜像快照”，在右侧页面单击“创建镜像快照”。

步骤2 添加基本信息。

- **镜像快照名称**

  请输入以小写字母或数字开头，小写字母、数字、中划线（-）、点（.）组成（其中两点不能相连，点不能与中划线相连），小写字母或数字结尾的1到63字符的字符串。

- **开启快照保留时间**

  打开开关，填写快照保留天数。未开启开关，默认为永久。

  说明

  快照过期后，仍会占用配额，需定期审核过期镜像快照后删除。

- **容器镜像**

第三方可以直接输入镜像地址，或单击“选择容器镜像”按钮，进入镜像列表，选择镜像。

- 我的镜像：展示了您上传到容器镜像服务的镜像。如果您想要在容器镜像服务中上传镜像，请参考**客户端上传镜像**或**页面上传镜像**。

  说明

  - 如果您开通了**企业管理**，使用账号登录云容器实例控制台时，您需要在账号下的容器镜像服务中给IAM用户添加权限，IAM用户才能使用账号下的私有镜像。给IAM用户添加权限有如下两种方法：
    - 在镜像详情中为IAM用户添加授权，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限，具体请参见**在镜像详情中添加授权**。
    - 在组织中为IAM用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限，具体请参见**在组织中添加授权**。
  - 镜像单层解压后的实际大小不能超过20G。
- 开源镜像中心：展示了镜像中心的公共镜像。
- 共享镜像：展示了容器镜像服务中他人共享的镜像。

镜像指定完成后，需要选择镜像的版本号。您还可以单击下方“添加容器镜像”按钮，添加多个容器镜像。

- **镜像快照大小**

  填写镜像快照大小，最小为10GiB，范围为10-400G。推荐按照所有缓存镜像大小总和的2倍设置快照大小。

步骤3 添加镜像快照构建信息。

- **命名空间**

  选择已有命名空间或单击“创建命名空间”按钮，创建新的命名空间。

  如果您要缓存的镜像包含私有镜像仓库，请确保命名空间绑定的vpc与私有镜像仓库网络互通。如需缓存公网镜像，需要命名空间绑定的vpc配置SNAT规则。

- **镜像仓库访问凭证**

  如果您容器里选择的镜像是私有的，请输入所选镜像的仓库地址、用户名、密码，用来拉取镜像。单击“添加凭证”，可添加多个。

步骤4 勾选“镜像快照默认使用 2核4G 规格的CCI实例进行制作，收取费用为制作过程中产生的费用”。

步骤5 确认镜像快照配置信息和费用显示正常，单击“确认创建”。

----结束

3.6.3 使用镜像快照

使用镜像快照创建CCI实例支持以下两种方式：

- 自动匹配：自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。
- 明确指定：明确指定使用的镜像快照。该镜像缓存必须为创建完成可用（Available）状态。

更多内容，请参考**镜像快照概述**。

操作步骤

容器配置填写完成后，打开“启动镜像快照”开关，选择自动匹配镜像快照或指定镜像快照。

- 自动匹配镜像快照

  自动匹配将从用户创建的所有可用镜像快照中选择最优的镜像。按以下顺序进行匹配：

  a. 镜像匹配度：优先选择匹配度高的镜像快照，匹配度指的是Pod和镜像快照两者在镜像上的匹配情况。

  b. 创建时间：优先选择创建时间更新的镜像快照。

- 明确指定

  指定已有的镜像快照，并在“镜像快照”页签中选择镜像快照中的镜像。该镜像缓存必须为创建完成可用（Available）状态。

查看使用效果

在CCI控制台的Pod页面，找到使用镜像快照创建的实例，进入详情页面。在事件页签下，可以看到该实例匹配了镜像缓存；如果挂载镜像快照失败，也会有相应报错信息。

3.6.4 管理镜像快照

操作场景

本章介绍了如何通过控制台对镜像快照执行查询、删除操作。要了解镜像快照的工作原理，请参阅**镜像快照概述**。

查看镜像快照

当您的镜像快照创建完成后，可以通过如下步骤查看详情。

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“镜像快照”，进入镜像快照列表页。

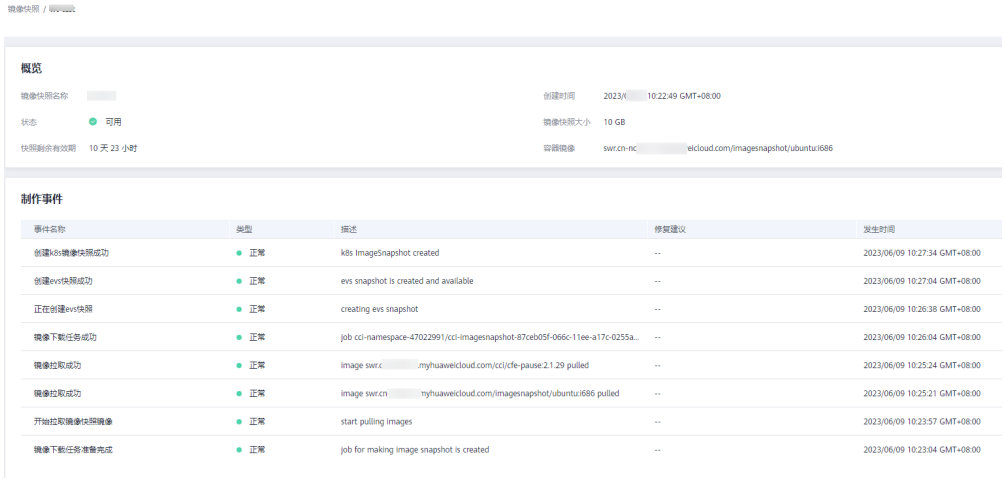
步骤2 单击镜像快照名称，进入镜像快镜像详情页。

步骤3 查看镜像快照的名称、状态、快照剩余有效期、镜像快照大小等信息。查看事件详细信息。

当镜像快照状态为可用时，可以使用该镜像快照。

当镜像快照状态为异常时，您可在详情页面查看事件详细信息。

图 3-52 镜像快照详情



----结束

删除镜像快照

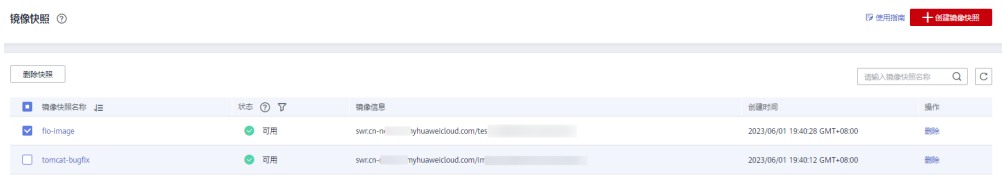
镜像快照对应一份EVS云盘快照，保留镜像快照需要支付相应的EVS云盘快照费用。对于不再使用的镜像快照，如果在创建时未设置保留时长，需手动删除。

当您的镜像快照不再使用时，可以通过如下步骤执行删除操作。

步骤1 登录云容器实例管理控制台，左侧导航栏中选择“镜像快照”，进入镜像快照列表页。

步骤2 勾选待删除的镜像快照，单击左上方“删除快照”按钮。

或直接单击镜像快照操作列下的“删除”。



----结束

3.7 日志管理

云容器实例支持挂载日志存储卷采集日志，您只需要在**创建负载**的时候添加日志存储卷，即可将日志写入到日志存储卷中。

云容器实例对接了**应用运维管理（Application Operations Management，AOM）**，AOM会采集日志存储中的“.log”等格式日志文件，转储到AOM中，方便您查看和检索。

须知

audit.log，oss.icAgent.trace，oss.script.trace，audit_*.log这几类日志默认不采集，请勿使用以上几类名称命名采集日志文件。

用户只要在Pod列表中点击查看日志，即可查看日志。

图 3-53 查看日志

日志采集可靠性说明

日志系统的核心功能在于记录业务组件的全生命周期状态数据（包括启动初始化、退出、运行时信息及异常事件等），主要服务于组件运行状态查看与故障根因分析等运维场景。

请注意标准输出流（stdout/stderr）及本地日志文件采用非持久化存储机制，其数据完整性受制于以下风险因素：

- 日志轮转压缩机制可能触发历史文件清除。
- Kubernetes Pod实例终止导致的临时存储卷回收。
- 节点存储空间限制触发的操作系统自动清理。

尽管云原生日志采集插件通过多级缓冲、优先级队列、断点续传等机制优化采集可靠性，但在以下场景仍存在日志采集丢失的可能：

- 业务日志吞吐量超过采集端处理能力。
- 业务Pod终止并立即被容器引擎回收。
- 日志采集器Pod运行异常。

以下是基于云原生日志管理的最佳实践建议，请您认真考虑并采纳：

- 请通过专用高可靠性通道记录并持久化关键业务数据（如金融交易）。
- 请勿在日志中进行记录客户信息、支付凭证、会话令牌等敏感数据。

添加日志存储

在**创建负载**的时候设置为容器添加日志存储。

- 容器内日志路径：即日志存储挂载到容器内的挂载路径，需要保证应用程序的日志输出路径与该路径一致，这样日志才能写入到日志存储卷中。

  须知

  1. 请确保日志存储卷路径在当前容器内是不存在的，否则会把容器内这个路径下的内容清空。
  2. 目前只支持日志路径下的“.log”、“.trace”、“.out”日志文件。
  3. 最多只能采集20个日志文件，也就是说您的日志最多只能输出到日志路径下的20个文件中。

- 日志存储空间：日志的存储空间大小。

  须知

  1. AOM每月赠送每个租户500M的免费日志存储空间，超过500M时将根据实际使用量进行收费，计费规则请参见**产品价格详情**。
  2. 日志存储空间取值请确保为1或2，后台调api接口创建负载时，请确保取值为1GiB或2GiB。
  3. 该空间为免费空间，超时不采集，如果日志文件超过2G，请您提前做好转储。

图 3-54 使用日志存储

查看日志

负载创建完成后，您可以查看容器日志。

单击已创建的负载，在容器实例所在行，单击“查看日志”。

图 3-55 查看日志

在AOM界面中即可查看对应容器的日志，AOM中日志查询方法请参见**查看日志文件**。

3.8 监控管理

CCI配合AOM对Pod资源进行基础监控，资源基础监控包含CPU/内存/磁盘等。您可以在CCI控制台查看Pod的监控指标数据，也可以在AOM中查看。

监控指标

在AOM控制台，可以查看容器实例的指标，指标内容请参见**表3-12**。

表 3-12 监控指标

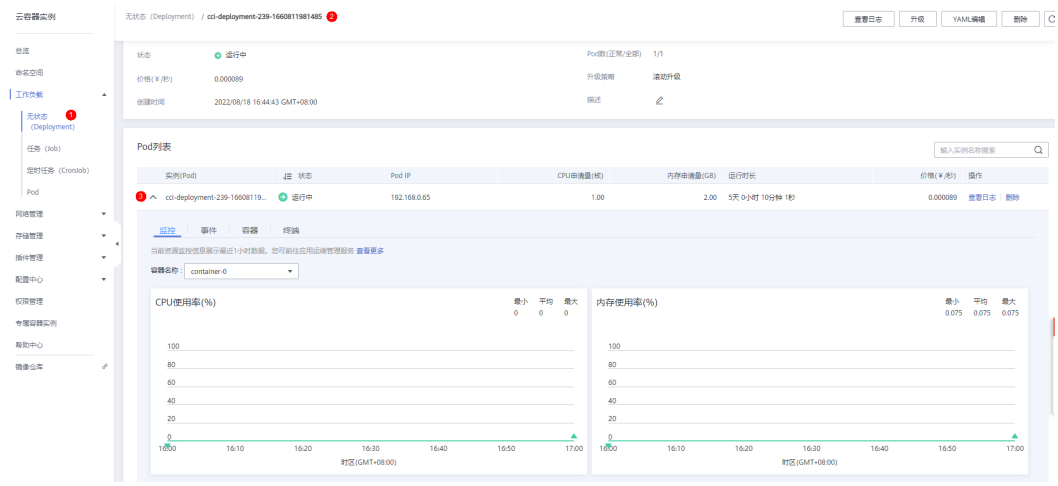
指标ID	指标名称	指标含义	取值范围	单位
cpuUsage	CPU使用率	该指标用于统计测量对象的CPU使用率。服务实际使用的与限制的CPU核数量比率。	0～100%	百分比（Percent）
cpuCoreLimit	CPU内核总量	该指标用于统计测量对象限制的CPU核总量。	≥1	核（Core）
cpuCoreUsed	CPU内核占用	该指标用于统计测量对象已经使用的CPU核个数。	≥0	核（Core）
memCapacity	物理内存总量	该指标用于统计测量对象限制的物理内存总量。	≥0	兆字节（Megabytes）
memUsage	物理内存使用率	该指标用于统计测量对象已使用内存占限制物理内存总量的百分比。	0～100%	百分比（Percent）
memUsed	物理内存使用量	该指标用于统计测量对象实际已经使用的物理内存（Resident Set Size）。	≥0	兆字节（Megabytes）

查看容器实例 Pod 的监控数据

在CCI控制台上，查看Pod监控数据。

进入CCI，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，在右侧页面单击要访问的工作负载。查看Pod实例下面的“监控”页签，该页签显示Pod近一小时的CPU使用率和内存使用率。

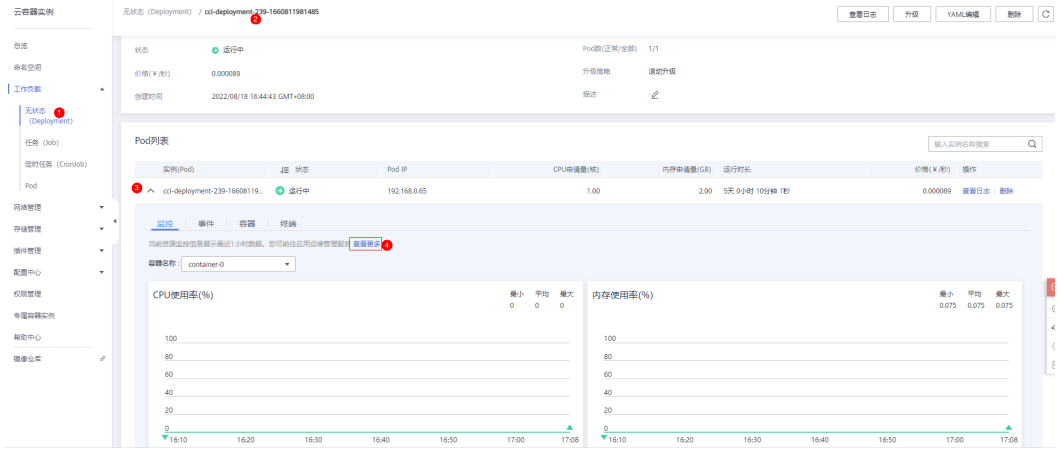
图 3-56 Pod 列表



CCI控制台上的资源监控信息仅展示CPU使用率和内存使用率。您可前往应用运维管理服务AOM查看更多监控指标。

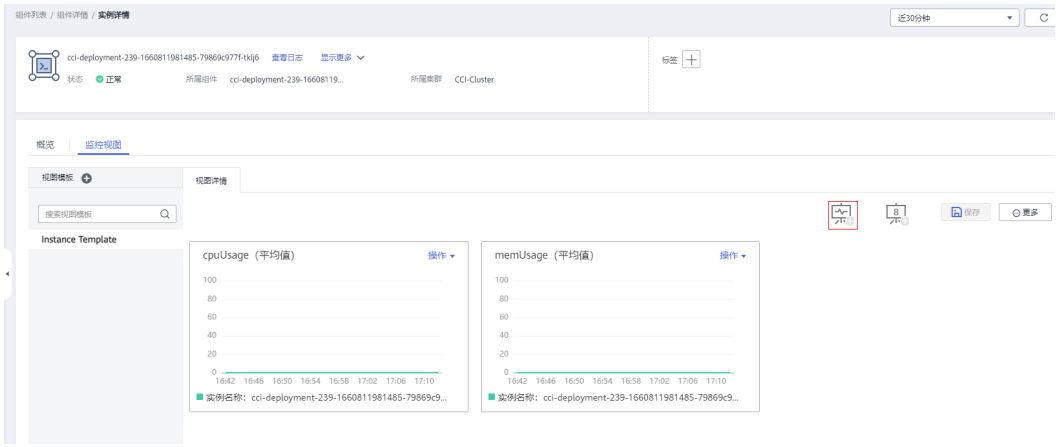
步骤1 单击监控页签下方的“查看更多”，进入AOM控制台。

图 3-57 Pod 监控



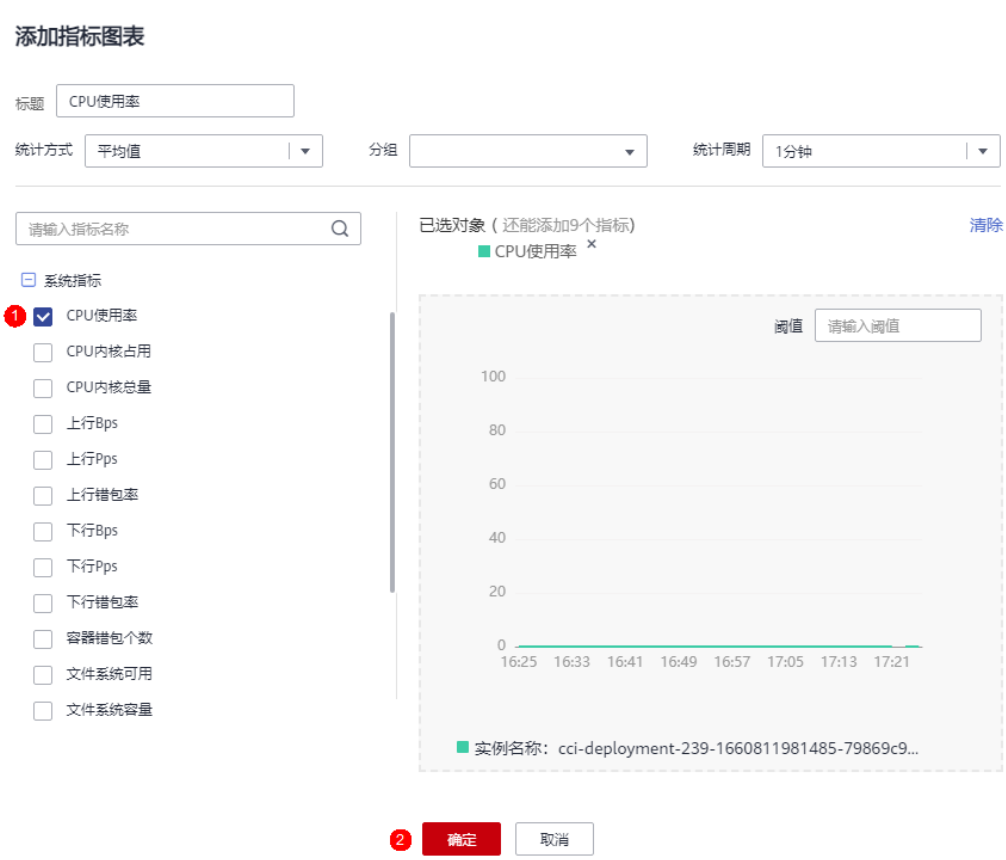
步骤2 单击  ，在视图模板中添加曲线图。

图 3-58 视图模板



步骤3 选择页面左侧系统指标，例如：选择“CPU使用率”，点击确认。

图 3-59 系统指标



步骤4 视图详情中即可查看Pod监控数据。

图 3-60 监控视图

----结束

4 通过 CCE 使用 CCI

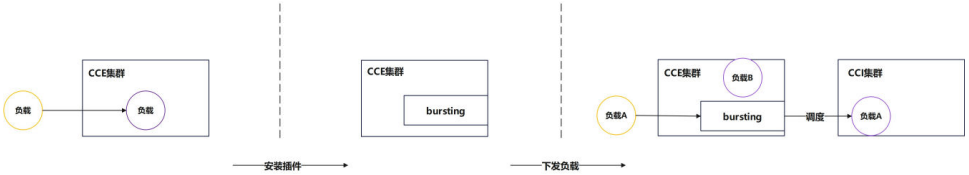
4.1 CCE 突发弹性引擎（对接 CCI）插件功能概览

简介

本章节主要介绍bursting提供的服务功能概览、资源使用说明和自定义注解。

功能概览

使用CCE集群+bursting基于如下模型，用户需要重点关注**下发负载**和**调度**。



⚠ 注意

下发负载涉及到用户给负载进行的配置项，和用户自身的业务高度相关。

工作负载配置项	功能描述	功能规格	相关文档拓展
调度	用户可以通过多种方式来管理CCE集群的工作负载，来控制其调度到CCI服务。通过合理的调度策略配置，提升用户集群的资源利用率。	• 支持4种调度策略。 • 支持2种管理调度策略的方式。 • 支持多个虚拟节点调度。	调度负载到CCI

工作负载配置项	功能描述	功能规格	相关文档拓展
资源配额	用户通过配置pod的cpu、memory等字段约束容器使用资源规格和上限。插件对资源规格进行规整，尽可能为用户降低成本。	提供对pod资源配额进行规整的能力。	实例资源配额
镜像	用户通过镜像配置自身业务镜像，将自己的业务容器运行在华为云CCE集群+CCI服务上。	• 支持修改镜像配置方式。 • 支持原地升级镜像。	镜像
存储	用户通过存储相关的配置为工作负载外挂存储卷，以完成业务中数据持久存储的诉求。	• 支持多种存储类型。 • 支持替换工作负载hostpath配置方式。	存储
网络	用户通过网络配置规划CCE集群和CCI集群之间的网络拓扑。	• 支持CCI侧负载通过service发布。 • 支持CCE集群pod与CCI集群中pod通过service互通。 • 支持指定cluster-dns。	网络
日志	用户可以通过同时安装CCE Log Collector插件和bursting插件，采集CCI侧工作负载的日志。	• 支持弹性CCI的负载通过CCE Log Collector上报日志。 • 支持日志自动转储。	日志
监控	用户可以通过配置插件对接监控平台，提升弹性CCI工作负载的可观测性。	• 支持对接AOM。 • 支持对接普罗米修斯。	监控

资源使用说明

CCE集群+bursting的使用场景涉及到华为云周边服务的搭配使用，如下表格详细描述了涉及到的周边服务。

涉及服务	资源说明	备注
CCI	插件会在CCI服务新建一个名为“cce-burst-”+“CCE集群ID”的命名空间。	• 不建议直接在CCI服务使用该命名空间，如需使用CCI服务，请另外新建命名空间。 • CCI服务命名空间不产生计费。

涉及服务	资源说明	备注
CCE	CCE侧的工作负载、Secret、Congfigmap、PV、PVC会同步到CCI，同时也占用CCE节点的资源。	• CCE集群资源规模1000 pod+1000 configmap建议申请2U4G节点规格。 • CCE集群资源规模2000 pod+2000 configmap建议申请4U8G节点规格。 • CCE集群资源规模4000 pod+4000 configmap建议申请8U16G节点规格。
ELB	开启“支持CCE集群pod与CCI集群pod通过service互通”功能bursting插件会自动创建ELB资源。	• 创建共享型性能保障规格的ELB，名称为cce-lb-xxx。 • 当卸载插件时，该ELB资源也会被自动清除。
VPC	弹性CCI的负载共享使用CCE集群所在VPC。	CCI命名空间Service网段为10.247.0.0/16，CCE集群的VPC子网网段请避开该网段。
SWR	创建弹性到CCI的工作负载选择镜像时，直接对接华为云SWR服务。	创建负载请确认镜像已被正确上传至您的SWR仓库。

Pod annotation

CCE集群+bursting的使用场景涉及到自定义注解，相关注解含义如下表所示。

annotation key	描述	相关文档
scheduling.cci.io/managed-by-profile	标记当前pod被哪个profile资源管理。	调度负载到CCI
virtual-kubelet.cci.io/burst-pod-cpu	标记弹性后规整的cpu资源。	实例资源配额
virtual-kubelet.cci.io/burst-pod-memory	标记弹性后规整的memory资源。	实例资源配额
coordinator.cci.io/inject-volumes	CCI pod日志采集相关，日志采集插件注入。	日志
logconf.k8s.io/fluent-bit-configmap-reference	CCI pod日志采集相关，日志采集插件注入。	日志
logconfigs.logging.openvessel.io	CCI pod日志采集相关，日志采集插件注入。	日志

annotation key	描述	相关文档
sandbox-volume.openvessel.io/volume-names	CCI pod日志采集相关，日志采集插件注入。	日志
coordinator.cci.io/image-replacement	镜像地址前缀替换相关。	镜像

4.2 CCE 对接 CCI

简介

本章节主要指导用户在CCE集群上使用bursting插件，快速帮助用户将负载通过插件从CCE集群弹性到CCI上。

CCE突发弹性引擎（对接 CCI）作为一种虚拟的kubelet用来连接Kubernetes集群和其他平台的API。Bursting的主要场景是将Kubernetes API扩展到无服务器的容器平台（如CCI）。

基于该插件，支持用户在短时高负载场景下，将部署在云容器引擎CCE上的无状态负载（Deployment）、有状态负载（StatefulSet）、普通任务（Job）、定时任务（CronJob）四种资源类型的容器实例（Pod），弹性创建到**云容器实例CCI**服务上，以减少集群扩容带来的消耗。

约束与限制

- 仅支持VPC网络模式的CCE Standard集群和CCE Turbo集群。
- CCE突发弹性引擎（对接 CCI）插件1.5.37及以下版本不支持Arm集群。如果集群中包含Arm节点，插件实例将不会部署至Arm节点。
- 集群所在子网不能与10.247.0.0/16重叠，否则会与CCI命名空间下的Service网段冲突，导致无法使用。
- Volcano调度器1.17.10及以下版本暂不支持使用Volcano调度器将挂载云存储卷的容器实例（Pod）弹性到CCI。
- 使用CCE集群中的Bursting插件对接CCI 2.0服务，支持配置独享型ELB的Ingress和Service。Bursting插件1.5.5以下版本不支持配置ELB类型的Service。

前提条件

- 使用插件前需要用户在CCI界面对CCI服务进行授权。
- 安装bursting插件后会在CCI服务新建一个名为"cce-burst-"+集群ID的命名空间，该命名空间完全由bursting管理，不建议直接在CCI服务使用该命名空间，如需使用CCI服务，请另外新建命名空间。

安装插件

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“插件中心”，进入插件中心首页。

4. 选择“CCE 突发弹性引擎 (对接 CCI)”插件，单击“安装”。
5. 配置插件参数。

表 4-1 插件参数说明

插件参数	说明
选择版本	插件的版本。

规格配置	用于配置插件负载的实例数及资源配额。
	● 选择“系统预置规格”时，您可选择“单实例”或“高可用”规格。
	● 选择“自定义规格”时，您可根据需求修改插件各个组件的副本数以及CPU/内存配置。
	说明
	● CCE 突发弹性引擎 (对接 CCI) 插件在1.5.2及以上版本，将占用更多节点资源，请在升级CCE突发弹性引擎（对接 CCI）插件前预留空间配额。
	  ● 单实例：需要预留一个节点，节点下至少需要有7个Pod空间配额。若开启网络互通，则需要有8个Pod空间配额。
	  ● 高可用：需要预留两个节点，节点下至少需要有7个Pod空间配额，共计14个Pod空间配额。若开启网络互通，则需要有8个Pod空间配额，共计16个Pod空间配额。
	● 弹性到CCI的业务量不同时，插件的资源占用也不相同。业务申请的POD、Secret、ConfigMap、PV、PVC会占用虚机资源。建议用户评估自己的业务使用量，按以下规格申请对应的虚机大小：1000pod+1000CM（300KB）推荐2U4G规格节点，2000pod+2000CM推荐4U8G规格节点，4000pod+4000CM推荐8U16G规格节点。

插件参数	说明
网络互通	开启后，支持CCE集群中的Pod与CCI集群中的Pod通过Kubernetes Service互通，并在插件安装时部署组件proxy。

工作负载下发

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“工作负载”，进入工作负载首页。
4. 单击“创建工作负载”，具体操作步骤详情请参见**创建工作负载**。
5. 填写基本信息。“CCI弹性承载”选择“强制调度策略”。

6. 进行容器配置。
7. 配置完成后，单击“创建工作负载”。
8. 在工作负载页面，选择工作负载名称，单击进入工作负载管理界面。
9. 工作负载所在节点为CCI集群，说明负载成功已调度到CCI。

插件卸载

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“插件中心”，进入插件中心首页。
4. 选择“CCE 突发弹性引擎 (对接 CCI)”插件，单击“卸载”。

表 4-2 特殊场景说明

特殊场景描述	场景现象	场景说明
CCE集群无节点，卸载插件。	插件卸载失败。	bursting插件卸载时会在集群中启动Job用于清理资源，卸载插件时请保证集群中至少有一个可以调度的节点。
用户直接删除集群，未卸载插件。	用户在CCI侧的命名空间中有资源残留，如果命名空间有计费资源，会造成额外计费。	由于直接删除集群，没有执行插件的资源清理Job，造成资源残留。用户可以手动清除残留命名空间及其下的计费资源来避免额外计费。

4.3 调度负载到 CCI

简介

对于使用CCE集群和CCI的使用场景，用户可以按需将工作负载调度到CCE集群节点或者对接CCI的虚拟节点，本文详细介绍如何将CCE集群的工作负载调度到CCI上。

bursting插件当前提供了以下方式管理CCE集群的pod，使其能够调度到CCI：

- **方法一：通过配置labels控制pod调度到CCI**
- **方法二：通过配置profile控制pod调度到CCI**

约束与限制

- 当前只有负载的原生标签能够被ScheduleProfile匹配，使负载能够被ScheduleProfile管理，将CCE集群的Pod调度到CCI。例如通过ExtensionProfile加到负载上的标签不能够被ScheduleProfile匹配，因此不会被ScheduleProfile管理调度功能。
- 通过配置labels控制pod调度到CCI的方式，需要在创建工作负载前添加label，若对已创建的工作负载进行追加label操作，存量工作负载对应的pod不会更新，可选择该工作负载，单击“更多 -> 重新部署”实现更新。

前提条件

- 插件版本：已安装CCE突发弹性引擎（对接 CCI）且插件，如果使用配置profile控制pod调度到CCI的方式请安装CCE突发弹性引擎（对接 CCI）插件版本为1.3.19及以上版本。
- 集群类型：如果使用配置profile控制pod调度到CCI方式仅支持VPC网络模式的CCE Standard集群和CCE Turbo集群。

调度策略

CCE集群工作负载弹性调度到CCI策略有以下几种：

调度策略	策略图解	适用场景
强制调度策略（enforce）		CCE工作负载强制弹性到CCI。
自动调度策略（auto）		根据用户集群调度器实际打分决定是否弹性到CCI。
本地优先调度策略（localPrefer）		工作负载优先调度到CCE集群，集群资源不足时工作负载弹性到CCI。
不开启（off）		工作负载不会弹性到CCI。

方法一：通过配置 labels 控制 pod 调度到 CCI

您可以通过控制台或YAML配置labels控制pod调度到CCI。

通过控制台配置

步骤1 登录CCE控制台，单击集群名称，进入概览页面。

步骤2 选择“工作负载”，单击“创建工作负载”。

步骤3 在基本信息中“弹性至CCI”选择“不开启”以外的任意策略。

- 本地优先调度：Pod优先调度至CCE节点，当CCE节点资源不足时将Pod弹性至CCI。
- 强制调度：所有Pod均会弹性至CCI。

步骤4 勾选相关的CCI资源池。

- CCI 2.0资源池(bursting-node)：新一代Serverless容器资源池。
- CCI 1.0资源池(virtual-kubelet)：存量Serverless容器资源池，即将日落。

说明

在CCE集群控制台（console）创建工作负载时，CCI弹性承载支持勾选“CCI 2.0资源池(bursting-node)”或者“CCI 1.0资源池(virtual-kubelet)”，如果使用CCI 1.0请勾选“virtual-kubelet”，如果使用CCI 2.0请勾选“bursting-node”。目前CCI 2.0仅对白名单用户开放，如需使用CCI 2.0服务，请提交工单申请开启CCI 2.0服务。

步骤5 CCE工作负载具体操作步骤详情请参见**创建工作负载**，完成后单击“确定”即可。

----结束

通过 YAML 文件配置

步骤1 登录CCE控制台，单击集群名称，进入概览页面。

步骤2 选择“工作负载”，单击“YAML创建”。

步骤3 在工作负载的yaml文件中添加virtual-kubelet.io/burst-to-cci标签。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: test
  namespace: default
  labels:
    virtual-kubelet.io/burst-to-cci: 'auto'    # 弹性到CCI
spec:
  replicas: 2
  selector:
    matchLabels:
      app: test
  template:
    metadata:
      labels:
        app: test
    spec:
      containers:
        - image: 'nginx:perl'
          name: container-0
          resources:
            requests:
              cpu: 250m
              memory: 512Mi
            limits:
              cpu: 250m
              memory: 512Mi
          volumeMounts: []
      imagePullSecrets:
        - name: default-secret
```

表 4-3 关键参数说明

参数	类型	描述
virtual-kubelet.io/burst-to-cci	String	表示CCE集群工作负载弹性调度到CCI策略，取值如下： ● enforce，CCE工作负载强制弹性到CCI。 ● auto，根据用户集群调度器实际打分决定是否弹性到CCI。 ● localPrefer，工作负载优先调度到CCE集群，集群资源不足时工作负载弹性到CCI。 ● off，工作负载不会弹性到CCI。

步骤4 完成后单击“确定”。

----结束

方法二：通过配置 profile 控制 pod 调度到 CCI

您可以通过控制台或YAML配置profile控制pod调度到CCI。

通过控制台配置

步骤1 登录CCE控制台，单击集群名称，进入概览页面。

步骤2 选择“策略 > CCI弹性承载策略”。

步骤3 单击“创建CCI弹性承载策略”，并填写相关信息。

表 4-4 创建 CCI 弹性承载策略

参数	参数说明
策略名称	输入策略名称。
命名空间	选择弹性策略生效的命名空间。您可选择命名空间或创建命名空间，创建命名空间操作步骤详情请参见**创建命名空间**。
关联负载	填写键值或引用负载标签。
调度策略	选择调度策略。 • 本地优先调度：Pod优先调度至CCE节点，当CCE节点资源不足时将Pod弹性至CCI。 • 强制调度：所有Pod均会弹性至CCI。
分配策略	• 本地：设置本地CCE集群。 • CCI：设置CCI上运行的“最大实例数”。
最大实例数	设置“本地”或“CCI”运行的最大实例数。
本地缩容优先级	取值范围[-100, 100]，数值越大越先缩容。
CCI缩容优先级	取值范围[-100, 100]，数值越大越先缩容。
CCI资源池	• CCI 2.0资源池(bursting-node)：新一代Serverless容器资源池。 • CCI 1.0资源池(virtual-kubelet)：存量Serverless容器资源池，即将日落。

步骤4 单击“确定”。

步骤5 选择“工作负载”，单击并创建工作负载，其中“高级配置 > 标签与注解”中添加Pod标签，其中键值与**步骤3**创建关联负载中的键值需保持一致，其他操作步骤请参考**创建工作负载**。

步骤6 完成后单击“创建工作负载”即可。

----结束

通过 YAML 配置

步骤1 登录CCE控制台，单击集群名称，进入概览页面。

步骤2 选择“策略 > CCI弹性承载策略”。

步骤3 单击“YAML创建”，创建profile对象。

示例一：限制调度到CCE集群最大负载数，配置local maxNum和scaleDownPriority的profile模板如下：

```
apiVersion: scheduling.cci.io/v1
kind: ScheduleProfile
metadata:
  name: test-cci-profile
  namespace: default
spec:
  objectLabels:
    matchLabels:
      app: nginx
  strategy: localPrefer
  location:
    local:
      maxNum: 20 # 当前暂不支持local/cci同时配置maxNum
      scaleDownPriority: 10
    cci: {}
```

示例二：限制CCI集群最大负载数，配置cci maxNum和scaleDownPriority的profile的模板如下：

```
apiVersion: scheduling.cci.io/v1
kind: ScheduleProfile
metadata:
  name: test-cci-profile
  namespace: default
spec:
  objectLabels:
    matchLabels:
      app: nginx
  strategy: localPrefer
  location:
    local: {}
    cci:
      maxNum: 20 # 当前暂不支持local/cci同时配置maxNum
      scaleDownPriority: 10
```

表 4-5 关键参数说明

参数	类型	描述
strategy	String	表示CCE集群工作负载弹性调度到CCI策略，取值如下： ● enforce，CCE工作负载强制弹性到CCI。 ● auto，根据用户集群调度器实际打分决定是否弹性到CCI。 ● localPrefer，工作负载优先调度到CCE集群，集群资源不足时工作负载弹性到CCI。

参数	类型	描述
maxNum	int	表示pod最大数量配置。 取值范围[0~int32]。
scaleDownPriority	int	表示缩容优先级配置，数值越大所关联的pod越先缩容。 取值范围[-100, 100]。

说明

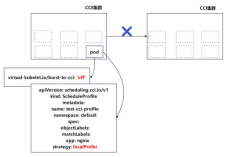
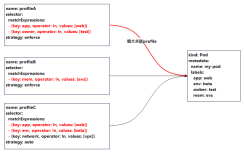
- location配置local字段（CCE侧）和cci字段（CCI侧）控制pod数量和缩容优先级。
- local字段和cci字段不可以同时设置maxNum。
- 缩容优先级为非必填项参数，如果不配置缩容优先级，默认值将为空。

步骤4 单击“确定”。

步骤5 创建无状态负载，使用selector方式选择含有“app：nginx”的pod，关联上文创建的profile。

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: nginx
spec:
  replicas: 10
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: container-1
          image: nginx:latest
          imagePullPolicy: IfNotPresent
          resources:
            requests:
              cpu: 250m
              memory: 512Mi
            limits:
              cpu: 250m
              memory: 512Mi
      imagePullSecrets:
        - name: default-secret
```


表 4-6 特殊场景使用说明

特殊使用场景	使用说明
pod同时使用label和profile控制调度CCI	使用label控制调度CCI的方式优先级高于使用profile控制调度CCI的方式。 例如label中策略为off，profile的策略为enforce，最终pod不会调度到CCI。 
pod同时被多个profile关联	pod有且仅有一个关联profile。当pod被多个profile关联，根据profile匹配pod的label的数量，选出最大关联profile，存在多个时，选择字典序小的profile关联。 pod最终被profileA关联 

步骤6 单击“确定”。

----结束

4.4 实例配置

4.4.1 实例配置规范

通过阅读本章节您可以了解到容器实例（Pod）配置规范的相关内容。

约束与限制

- 暂不支持守护进程集（DaemonSet）。
- 暂不支持HostNetwork网络模式。
- 暂不支持通过配置TCP启动探针进行健康检查。
- 暂不支持动态资源分配（Dynamic Resource Allocation）特性，并在插件1.5.27版本对相关配置进行拦截。

4.4.2 实例资源配额

简介

对于CCE集群中弹性到CCI的pod，bursting插件会根据用户提供的CPU、内存规格，对pod的资源规格做出规整，以达到合理利用资源并满足CCI资源规格的目的。本章节将详细介绍如何进行资源规格的规整。

约束与限制

- 弹性到CCI的pod需要至少有一个容器有指定CPU&Memory的limit或者request资源，或存在“resource.cci.io/pod-size-specs”的注解。
- 本节的资源规整算法仅适用于云原生bursting，CCI 2.0的console和API有独立的Pod规格规整算法。弹至CCI 2.0的pod也需遵循CCI的规格约束，如果未命中CCI 2.0支持的规格，会在CCE侧的pod事件里产生如下类似报错，且对应pod在CCI侧不会被创建。

pod 资源规格算法

弹性CCI的pod规格，根据container资源的Requests和Limits计算，调整至CCI允许范围。

pod规格的计算方式遵循如下规则：

- 所有应用容器和初始化容器对某个资源的Requests和Limits均会被设置为相等的值，如果配置了Limits，则取Limits值；如果没有配Limits，则取Requests值。
- pod对某个资源的Requests和Limits，是取如下两项的较大者：
  - 所有应用容器对某个资源的Limits之和。
  - 所有初始化容器Limits的最大值。

Pod规格约束：

- Pod的CPU需大于0。
- 经过资源自动规整后，Pod的CPU在0.25核~32核范围内，或者等于48核或64核；Memory在1Gi~512Gi范围内，且必须为1Gi的整数倍，且满足CPU/Memory配比值在1:2~1:8之间。

资源规整算法

假设根据pod资源规格算法求得CPU（core）、Memory（Gi），则自动规整规则如下：

1. 将Pod中除了BestEffort的每个应用容器和初始化容器的CPU向上调整至0.25核的整数倍， Memory向上调整至大于等于0.2Gi。

   说明

   CCE突发弹性引擎（对接 CCI）插件1.5.16版本及之后，不再进行容器级别的向上规整，仅进行pod级别的向上规整。
2. 若此时Pod的CPU大于32u或者Memory大于256Gi，则不再继续进行自动调整，否则将继续调整。
3. 将整个pod的CPU配额向上调整至0.25核的整数倍，Memory配额向上调整至1Gi的整数倍。
4. 若pod Memory/CPU的比值小于2，需将pod Memory向上调整至大于等于CPU的2倍，且满足是1Gi的整数倍。
5. 若pod Memory/CPU的比值大于8，需将pod CPU向上调整至大于等于Memory的1/8，且满足是0.25核的整数倍。

以上对pod级别资源向上调整造成的增量CPU和Memory，全部添加到Pod中第一个不为BestEffort的容器上。

⚠ 注意

BestEffort容器是指没有配置Requests和Limits的容器。

经过资源自动规整后，Pod规格约束：

- pod的CPU取值在0.25核~32核范围内，或者等于48核或64核，并且要求值为0.25的整数倍。
- Memory在1Gi~256Gi范围内，或者等于384Gi或512Gi，且Memory是整数。
- 满足Memory/CPU配比值在2~8之间。

用户可以通过CCE侧的pod的annotation查看规整后的规格。

- virtual-kubelet.cci.io/burst-pod-cpu: 0.5u
- virtual-kubelet.cci.io/burst-pod-memory: 1Gi

资源规整用例说明

资源规格（CPU MEM）	规整后规格（CPU MEM）	说明
37U 37Gi	无法创建pod弹性到CCI。	CPU规格无效。
30U 257Gi	无法创建pod弹性到CCI。	存算比大于8，提高CPU。但无法满足CPU规格有效，拦截。
0.35U 0.5Gi	0.5U 1Gi	CPU向上取整0.25的整数倍，MEM向上取整1的整数倍。存算比符合要求，不做调整。
0.35U 1.5Gi	0.5U 2Gi	CPU向上取整0.25的整数倍，MEM向上取整1的整数倍。存算比符合要求，不做调整。
0.45U 18Gi	2.25U 18Gi	CPU向上取整0.25的整数倍，MEM向上取整1的整数倍。存算比大于8，提高CPU。
2U 2Gi	2U 4Gi	存算比小于2，提高MEM。

预留系统开销说明

从bursting弹性到CCI 2.0的Pod，也可以通过pod/podTemplate的annotation "resource.cci.io/memory-reservation"和"resource.cci.io/memory-burst-size"来开启预留系统开销。

4.5 镜像

简介

用户可以通过华为云镜像仓库服务SWR来管理业务镜像。本章节将介绍CCE+bursting插件场景中，涉及到镜像相关的使用场景及用法。通过阅读本章用户可以在CCE+bursting插件场景中：

- **使用SWR拉取用户业务镜像**
- **混合使用华为云SWR + 第三方镜像仓拉取用户业务镜像**

使用 SWR 拉取用户业务镜像

- **方式一：通过console选取SWR镜像**
  a. 用户镜像上传SWR。使用方式请参考：**SWR官方文档**。
  b. 在华为云CCE控制台创建负载选择镜像。

  c. 对接到SWR中的镜像。请确保您的SWR仓库中已正确上传了镜像，SWR服务使用详情请参见：**SWR官方文档**。
- **方式二：通过在CCE集群node选取SWR镜像**
  a. 登录CCE集群节点。
  b. 查看SWR镜像仓库中的镜像地址。
  获取镜像地址：swr.***.com/cci-test/nginx:1.0.0.x86_64_test。
  c. 配置工作负载yaml。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: test
  namespace: default
  labels:
    virtual-kubelet.io/burst-to-cci: 'auto'    # 弹性到CCI
spec:
  replicas: 2
  selector:
    matchLabels:
      app: test
  template:
    metadata:
      labels:
        app: test
    spec:
      containers:
```

```
      - image: swr.***.com/cci-test/nginx:1.0.0.x86_64_test
        name: container-0
        resources:
          requests:
            cpu: 250m
            memory: 512Mi
          limits:
            cpu: 250m
            memory: 512Mi
        volumeMounts: []
      imagePullSecrets:
        - name: default-secret
```

d. 部署工作负载。

```
kubectl apply -f  dep.yaml
```

混合使用华为云 SWR + 第三方镜像仓拉取用户业务镜像

操作场景：

在某些情况下，用户在CCE的工作负载拉取第三方镜像仓库的镜像，拉取的镜像可以同步到SWR服务，当发生业务波峰时，弹性到CCI的工作负载使用SWR镜像，可以极大提高镜像拉取效率，帮助用户更丝滑应对业务波峰。

操作指导：

为配置工作负载yaml配置annotation，示例值如下所示：

```
"coordinator.cci.io/image-replacement": '[
    {"repositoryPrefix":"harbor.domain","replaceWith":"swr.***.com/org1"},
    {"repositoryPrefix":"","replaceWith":"swr.***.com/org1"},
    {"repositoryPrefix":"harbor.domain/a/b/c/d","replaceWith":"swr.***.com/org2"}
]'
```

说明

- 配置策略执行无先后顺序。
- 替换策略可以配置多条，各个策略repositoryPrefix值不允许重复。

替换规则key	字段含义	字段说明
repositoryPrefix	用户希望被匹配并被替换的镜像前缀字段。	• 该字段为空，匹配所有image字段不含"/"的容器。 • 该字段不为空，匹配所有image字段最后一个"/"字符前缀相同的容器。 • 该字段字符校验规则与容器镜像名的规则一致，且不能以"/"字符结尾。
replaceWith	用户希望替换成的镜像前缀字段。	• 该字段字符不能与repositoryPrefix相同 • 该字段字符校验规则与容器镜像名的规则一致，且不能以"/"字符结尾

表 4-7 annotation 说明

annotation	替换前	替换后	说明
"coordinator.cci.io/image-replacement": '[{"repositoryPrefix":"harbor.domain","replaceWith":"swr.***.com/org1"}]'	containers: - name: container-0 image: 'harbor.domain/ubuntu:latest'	containers: - name: container-0 image: 'swr.***.com/org1/ubuntu:latest'	repositoryPrefix匹配第三方仓库域名场景。
"coordinator.cci.io/image-replacement": '[{"repositoryPrefix":"","replaceWith":"swr.***.com/org1"}]'	containers: - name: container-1 image: 'nginx:latest'	containers: - name: container-1 image: 'swr.***.com/org1/nginx:latest'	repositoryPrefix为空场景。
"coordinator.cci.io/image-replacement": '[{"repositoryPrefix":"harbor.domain/a/b/c/d","replaceWith":"swr.***.com/org2"}]'	containers: - name: container-2 image: 'harbor.domain/a/b/c/d/redis:latest'	containers: - name: container-2 image: 'swr.***.com/org2/redis:latest'	repositoryPrefix匹配第三方仓库域名+组织目录场景。

4.6 存储

简介

弹性到CCI的工作负载支持多种华为云存储配置，用于满足客户多样化的存储需求。通过阅读本章用户可以：

- 了解弹性CCI的负载支持的存储类型。
- 了解弹性CCI的负载Hostpath类型的典型场景以及如何使用。

约束与限制

调度到CCI的实例的存储类型支持ConfigMap、Secret、EmptyDir、DownwardAPI、Projected、PersistentVolumeClaims几种Volume类型，其中Projected和DownwardAPI类型仅bursting 1.3.25版本及以上支持。

- EmptyDir：不支持子路径。
- PersistentVolumeClaims：只支持SFS、SFS Turbo云存储类型，且只支持使用CSI类型的StorageClass。1.17.10及以下版本的Volcano调度器不支持调度所有云存储类型。
- Projected：如配置了serviceAccountToken类型的source，那么弹性到CCI后挂载的会是对应service-account-token secret中的token，该token为长期有效的token且没有预期受众，即expirationSeconds和audience两项配置不会生效。

支持的存储类型

用户在配置负载存储类型时，CCE的console有如下选项。

弹性CCI的负载对存储类型的支持情况如下：

volume类型	是否支持	特殊场景说明
HostPath	否	• CCI是共享集群，不直接开放HostPath能力。 • 1.5.9及以上版本可支持配置path为/etc/localtime的HostPath存储，配置后CCI侧容器中挂载的时区将会与CCE节点的时区一致。
ConfigMap	是	-
Secret	是	-
EmptyDir	是	挂载EmptyDir不支持子路径。 EmptyDir的sizeLimit需为1Gi的整数倍，且不能大于Pod CPU核数的10倍。
DownwardAPI	是	-
Projected	是	如配置了serviceAccountToken类型的source，弹性到CCI后会挂载对应service-account-token secret中的token，该token为长期有效，且token没有预期受众，即expirationSeconds和audience两项配置不会生效。
PersistentVolumeClaims	是	只支持SFS、SFS Turbo云存储类型，且只支持使用CSI类型的StorageClass。

负载 Hostpath 配置方式

操作场景

在使用CCE或者其他K8s集群时，用户使用HostPath类型存储。但CCI是共享集群，不开放HostPath能力，因此使用HostPath的Pod通过bursting弹到CCI时，会被拦截。如

无法改变Pod spec.volumes中配置的HostPath，可通过配置Annotation的形式，允许让使用HostPath的Pod弹性到CCI上，bursting在校验时需要去掉Pod中的HostPath或者将HostPath替换为emptyDir。

约束与限制

- EmptyDir的sizeLimit需为1Gi的整数倍，且不能大于Pod CPU核数的10倍。
- LocalDir和flexVolume当前暂不支持。

操作步骤

通过在Pod.Annotations中加入注解可以做到hostPath转emptydir。

- 单个hostPath替换为emptyDir配置方式：
  ```
  "coordinator.cci.io/hostpath-replacement": '[{"name":"source-hostpath-volume-3","policyType":"replaceByEmptyDir","emptyDir":{"sizeLimit":"10Gi"}}]'
  ```
- 单个hostPath忽略：
  ```
  "coordinator.cci.io/hostpath-replacement": '[{"name":"source-hostpath-volume-1","policyType":"remove"}]'
  ```
- 全部HostPath都忽略：
  ```
  "coordinator.cci.io/hostpath-replacement": '[{"name":"*","policyType":"remove"}]'
  ```
- 多个HostPath差异化替换策略：
  ```
  "coordinator.cci.io/hostpath-replacement": '[{"name":"source-hostpath-volume-1","policyType":"remove"},{"name":"source-hostpath-volume-3","policyType":"replaceByEmptyDir","emptyDir":{"sizeLimit":"10Gi"}}]'
  ```

  说明

  对于path为/etc/localtime的HostPath存储，会被单个HostPath替换的策略（策略name为具体的volume name）替换，不会被全部HostPath替换的策略（策略name为"*"）替换。

  参考deployment yaml示例：

  ```
  apiVersion: apps/v1
  kind: Deployment
  metadata:
    annotations:
      description: ''
    labels:
      virtual-kubelet.io/burst-to-cci: enforce
      appgroup: ''
      version: v1
    name: test
    namespace: default
  spec:
    replicas: 2
    selector:
      matchLabels:
        app: test
        version: v1
    template:
      metadata:
        labels:
          app: test
          version: v1
        annotations:
          coordinator.cci.io/hostpath-replacement: '[{"name": "test-log2", "policyType": "remove"}, {"name": "test-log", "policyType": "replaceByEmptyDir", "emptyDir":{"sizeLimit":"10Gi"}}, {"name": "test-log1", "policyType": "remove" }]'
      spec:
        containers:
          - name: container-1
            image: nginx
            imagePullPolicy: IfNotPresent
            resources:
              requests:
  ```



```
          cpu: 250m
          memory: 512Mi
        limits:
          cpu: 250m
          memory: 512Mi
      volumeMounts:
        - name: test-log
          mountPath: /tmp/log
        - name: test-log1
          mountPath: /tmp/log1
        - name: test-log2
          mountPath: /tmp/log2
  volumes:
  - hostPath:
      path: /var/paas/sys/log/virtual-kubelet
      type: ""
    name: test-log
  - hostPath:
      path: /var/paas/sys/log
      type: ""
    name: test-log1
  - hostPath:
      path: /var/paas/sys/log2
      type: ""
    name: test-log2
```

4.7 网络

简介

通过阅读本章节用户可以了解：

- 如何为弹性CCI的pod配置默认使用的指定dns服务器。
- CCE集群pod与CCI集群中pod通过service互通的使用指导。
- 弹性CCI侧pod通过service发布。

约束与限制

- 使用共享VPC的CCE集群不支持开启“网络互通”功能。
- 使用CCE集群中的Bursting插件对接CCI 2.0服务，支持配置独享型ELB的Ingress和Service。Bursting插件1.5.5以下版本不支持配置ELB类型的Service。
- 当前网络互通能力依赖sidecar容器的启动，如需使用以下功能，插件升级到1.5.28及以上版本：
  - 业务容器需要使用postStart功能。
  - 在初始化容器中使用网络互通能力，需要开启**初始化容器网络互通开关**。
- 开启网络互通能力、开启初始化容器网络互通开关等操作需等待相关组件就绪，再下发负载，否则会导致功能异常。
- 跨CCE和CCI实例Service网络互通只支持集群内访问（ClusterIP）类型。不支持在init-container中访问CCE侧ClusterIP service。
- 跨CCE和CCI实例，在对接LoadBalancer类型的Service或Ingress时：
  - 禁止指定健康检查端口，在CCE集群下，由于CCI的容器与CCE的容器在ELB注册的后端使用端口不一致，指定健康检查端口会导致部分后端健康检查异常。
  - 跨集群使用Service对接同一个ELB的监听器时，需确认健康检查方式，避免服务访问异常。

- 在CCE标准集群下对接共享型LoadBalancer类型的Service时，需要放通node安全组下100.125.0.0/16网段的容器端口。

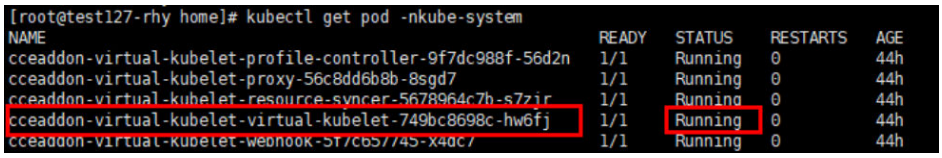
配置默认使用的指定 dns 服务器

操作场景

在某些场景中，用户想要弹性CCI的Pod可以使用指定的dns服务器地址。bursting插件提供配置指定的dns服务器地址的能力，无需在每个Pod上都配置dnsConfig，从而降低用户网络运维成本。

操作步骤

1. 登录CCE集群节点，编辑bursting负载的yaml。
   ```
   kubectl edit deploy cceaddon-virtual-kubelet-virtual-kubelet -nkube-system
   ```
2. 启动参数中增加--cluster-dns=x.x.x.x参数，配置为dns服务器地址。
3. 保存配置修改，等待virtual-kubelet负载重启。



4. 验证方式。

   通过exec进入弹性到CCI运行中的容器内，查看/etc/resolv.conf中首选nameserver是否为cluster-dns配置的地址。

表 4-8 使用场景约束限制

使用场景	约束限制
修改配置前存在弹性CCI的pod	• 修改配置后新创建弹性CCI的pod生效。 • 修改配置前的弹性的pod需要重建之后才生效。
cluster-dns配置上限	• k8s dnsConfig最多只支持配置3个nameservers。 • 保证cluster-dns配置的nameserver数量与Pod的spec.dnsConfig配置的nameserver数量之和不超过3个。

CCE 集群 pod 与 CCI 集群中 pod 通过 service 互通的使用指导

1. 安装插件，勾选”网络互通“功能。

安装成功后租户账号下会自动创建负载均衡器，可以通过网络控制台进行查看。

2. 创建弹性CCI侧pod，并配置service发布。
   - 为了方便验证，镜像选择暴露容器80端口的nginx。
   - 为工作负载配置service。推荐自动创建新的负载均衡器，以避免和插件自动创建的elb产生冲突。

3. 通过CCE集群控制台，获取该负载的访问方式。
4. 创建CCE侧pod，并配置service发布。方法请参考步骤**2**，不选择弹性CCI标签。
5. 验证网络互访。
   创建弹性CCI的工作负载，镜像选择含有curl命令的镜像，如centos。
   通过CCI侧进入该容器，执行图中命令，观测CCI访问CCE service网络打通。

图 4-1 访问 CCE pod 的 service

```
Welcome to Cloud Container Instance.
sh-4.2# curl -kv testcce-ng.default.svc.cluster.local:30001
* About to connect() to testcce-ng.default.svc.cluster.local port 30001 (#0)
*   Trying 10          3...
^C
sh-4.2# curl -kv testcce-ng.default.svc.cluster.local:30002
* About to connect() to testcce-ng.default.svc.cluster.local port 30002 (#0)
*   Trying 10.247.90.173...
* Connected to testcce-ng.default.svc.cluster.local (10.247.90.173) port 30002 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: testcce-ng.default.svc.cluster.local:30002
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.16.0
< Date: Thu, 11 Jan 2024 06:37:40 GMT
< Content-Type: text/html
< Content-Length: 612
< Last-Modified: Tue, 23 Apr 2019 15:11:11 GMT
< Connection: keep-alive
< ETag: "5cbf2b0f-264"
```

6. 同理创建CCE侧pod，镜像选择含有curl命令的镜像，如centos。执行相同的命令。观测CCE访问CCI service网络打通。

图 4-2 访问 CCI pod 的 service

```
sh-4.2#
sh-4.2#
sh-4.2#
sh-4.2# curl -kv testcci-ng.default.svc.cluster.local:30001
* About to connect() to testcci-ng.default.svc.cluster.local port 30001 (#0)
*   Trying 10.247.174.50...
* Connected to testcci-ng.default.svc.cluster.local (10.247.174.50) port 30001 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: testcci-ng.default.svc.cluster.local:30001
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.16.0
< Date: Thu, 11 Jan 2024 06:39:17 GMT
< Content-Type: text/html
< Content-Length: 612
< Last-Modified: Tue, 23 Apr 2019 15:11:11 GMT
< Connection: keep-alive
< ETag: "5cbf2b0f-264"
```

初始化容器网络互通开关配置

初始化容器网络互通开关默认关闭，若要使用，请在开启网络互通功能开关的前提下，根据以下操作进行配置。

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“插件中心”，进入插件中心首页。
4. 选择“CCE 突发弹性引擎 (对接 CCI)”插件，单击“编辑”。

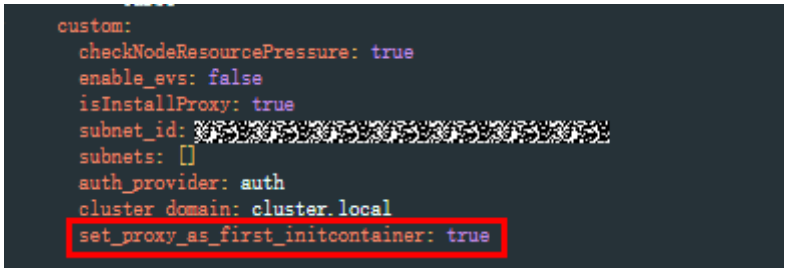
图 4-3 CCE 突发弹性引擎 (对接 CCI)插件

5. 在“网络互通（可选）”开启的条件下，单击“编辑YAML”。

图 4-4 编辑插件

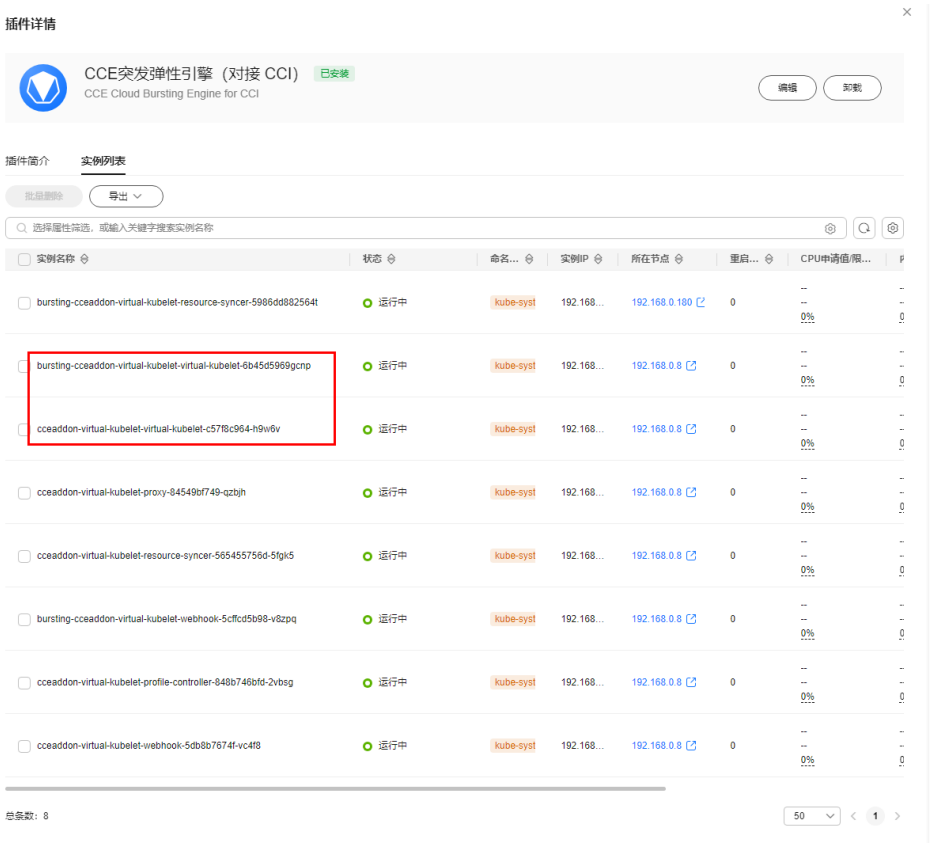
6. 将“set_proxy_as_first_initcontainer”配置为true。

图 4-5 修改参数



7. 在“CCE 突发弹性引擎 (对接 CCI)”插件的实例列表中查看实例名称为“bursting-cceaddon-virtual-kubelet-virtual-kubelet-xxx”、“cceaddon-virtual-kubelet-virtual-kubelet-xxx”状态显示为“运行中”，表示重新部署完毕，该功能可正常运行。

图 4-6 查看插件部署状态



4.8 日志

简介

CCE集群成功将负载弹性到CCI运行起负载后，用户可以通过CCE的“CCE Log Collector”插件来收集pod的日志，提升工作负载的可观测性。通过阅读本章用户可以快速搭建日志平台，在CCE的日志观测CCI侧日志。

须知

弹性到CCI的负载会默认开启容器标准输出采集并上报到**应用运维管理**，AOM每月赠送每个租户500M的免费日志存储空间，超过500M时将根据实际使用量进行收费，计费规则请参见**产品价格详情**。

若要关闭标准输出采集可通过在Pod annotation中指定log.stdoutcollection.kubernetes.io: '{"collectionContainers": []}'实现，参考示例：

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: test
  namespace: default
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        log.stdoutcollection.kubernetes.io: '{"collectionContainers": []}'
    spec:
      containers:
        - name: container-1
          image: nginx:latest
```

日志采集可靠性说明

日志系统的核心功能在于记录业务组件的全生命周期状态数据（包括启动初始化、退出、运行时信息及异常事件等），主要服务于组件运行状态查看与故障根因分析等运维场景。

请注意标准输出流（stdout/stderr）及本地日志文件采用非持久化存储机制，其数据完整性受制于以下风险因素：

- 日志轮转压缩机制可能触发历史文件清除。
- Kubernetes Pod实例终止导致的临时存储卷回收。
- 节点存储空间限制触发的操作系统自动清理。

尽管云原生日志采集插件通过多级缓冲、优先级队列、断点续传等机制优化采集可靠性，但在以下场景仍存在日志采集丢失的可能：

- 业务日志吞吐量超过采集端处理能力。
- 业务Pod终止并立即被容器引擎回收。
- 日志采集器Pod运行异常。

以下是基于云原生日志管理的最佳实践建议，请您认真考虑并采纳：

- 请通过专用高可靠性通道记录并持久化关键业务数据（如金融交易）。
- 请勿在日志中进行记录客户信息、支付凭证、会话令牌等敏感数据。

约束与限制

使用场景	使用说明
CCE内容器日志采集 + CCI集群容器日志采集	CCE集群内的工作负载支持三种日志采集类型： ● 容器标准输出：采集集群内指定容器日志，仅支持Stderr和Stdout的日志。 ● 容器文件日志：采集集群内指定容器内的文件日志。 ● 节点文件日志：采集集群内指定节点路径的文件。 **须知** 弹性到CCI的工作负载仅支持“容器文件日志”类型的采集策略。
不支持采集的日志文件类型	● 不支持容器中软链路径的日志采集。 ● pod通过指定系统、设备、cgroup、tmpfs等挂载目录下的日志无法被采集。
弹性CCI的pod关联多个日志采集策略	为了更好的采集日志，建议为pod预留充足内存。pod被第一个日志策略关联请预留至少50MiB内存。每增加一个关联日志采集策略，建议多预留5MiB内存。
超长日志采集	单条日志最大容量为250KB，超过会被丢弃。
日志采集文件名	audit.log，oss.icAgent.trace，oss.script.trace，audit_*.log这几类日志默认不采集，请勿使用以上几类名称命名采集日志文件。
超长日志文件名	容器中长度超过190的日志文件无法被采集。容器中长度在180~190范围的日志文件仅支持采集第一个文件。
日志采集速率	单个Pod单行日志采集速率不超过10000条/秒，多行日志不超过2000条/秒。
最大采集文件数	单个Pod所有日志采集策略监听的文件数不超过2000个文件。
容器停止前日志采集	当容器被停止时，如果出现因网络延迟、资源占用多等原因导致的采集延时，可能会丢失容器停止前的部分日志。

操作步骤

1. 安装“云原生日志采集插件”和“CCE 突发弹性引擎 (对接 CCI)”插件。
   a. 登录CCE控制台。
   b. 选择CCE集群，单击进入CCE集群总览页面。
   c. 在导航栏左侧单击“插件中心”，进入插件中心首页。
   d. 选择“CCE 突发弹性引擎 (对接 CCI)”插件，单击“安装”。

e. 在安装配置中需要勾选“网络互通”功能。

f. 选择“云原生日志采集插件”，单击“安装”。

2. 创建弹性到CCI的负载。
   a. 在导航栏左侧单击“工作负载”，进入工作负载首页。
   b. 单击“创建工作负载”，具体操作步骤详情请参见**创建工作负载**。
   c. 填写基本信息并完成工作负载创建。更多创建弹性到CCI负载的方式，请参考**调度负载到CCI**。

3. 配置日志采集策略。
   a. 在导航栏左侧单击“日志中心”，进入日志中心首页。
   b. 单击“日志采集策略”，进入日志采集策略创建的界面。
   c. 配置具体日志采集策略，完成后单击“确定”。

说明

弹性到CCI的Pod不支持日志策略热更新，更新日志采集策略后需要重新部署弹性到CCI的Pod才可生效。

4. 查看弹性到CCI的pod yaml。

为支持CCI pod日志被采集到日志中心，CCE插件CCE Log Collector为pod注入了如下四个annotation：

annotation	示例值
coordinator.cci.io/inject-volumes	'[{"name":"log-agent-conf","configMap":{"name":"log-agent-cci-logging-config","defaultMode":384},"namespace":"monitoring"},{"name":"log-agent-cert","secret":{"secretName":"log-agent-ca-secret","defaultMode":384},"namespace":"monitoring"}]'
logconf.k8s.io/fluent-bit-configmap-reference	monitoring-log-agent-cci-logging-config
logconfigs.logging.openvessel.io	'{"testcci001":{"container_files":{"container-1":"/var/test/*/*.log"},"regulation":""}}'
sandbox-volume.openvessel.io/volume-names	log-agent-conf,log-agent-cert

5. 在日志中心查看日志上报。

CCE集群日志中心更详细的用法可以参考CCE插件**CCE Log Collector**相关文档指导。

4.9 监控

简介

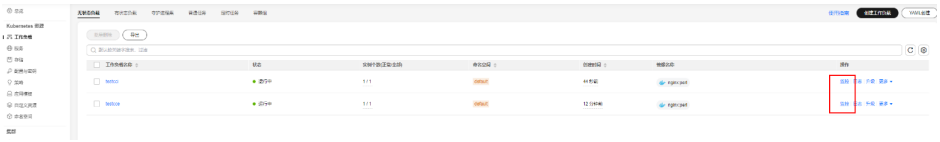
在CCE集群中通过bursting插件弹性CCI的工作负载支持对接云原生观测中的监控中心。通过阅读本章节用户可以快速搭建CCE集群中的监控中心，监控弹性CCI的pod。

约束与限制

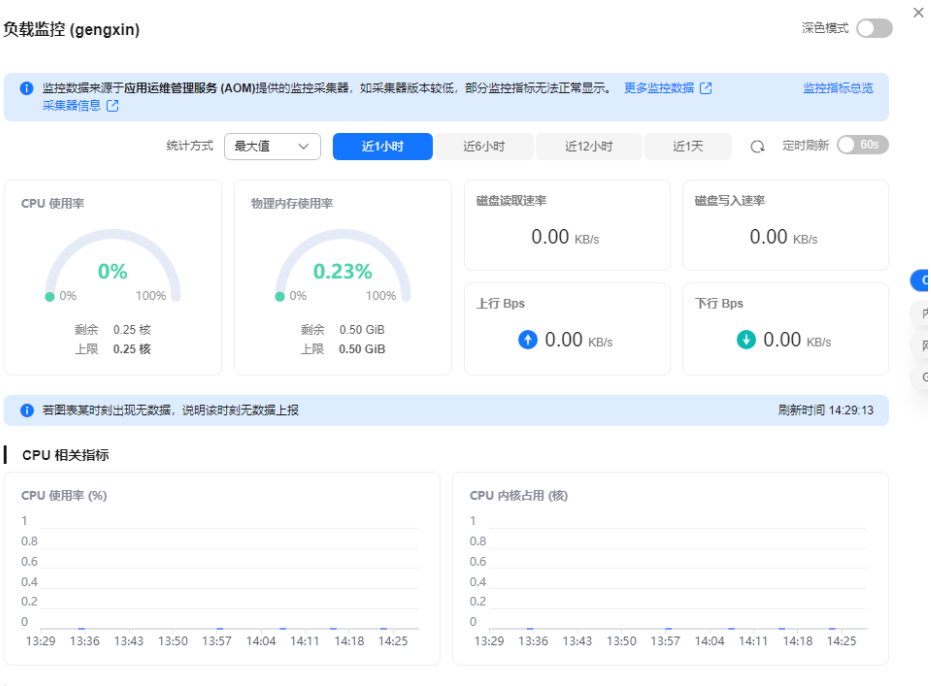
- metrics-server无法采集到通过bursting插件弹性到CCI 2.0上的Pod的监控数据，可能会影响HPA工作。如果HPA无法正常工作，请参考**弹性伸缩**进行处理。
- 从CCE bursting弹到CCI 2.0的pod，与从CCI 2.0前端或API创建的pod，如非必要，命名空间和pod名请勿同时重复，这将导致CCI 2.0侧的pod监控数据异常。从CCE侧查看pod的监控不受影响。

操作步骤

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“监控中心”，进入监控中心首页。
4. 单击“立即开通”。
5. 在导航栏左侧单击“工作负载”，进入工作负载首页。
6. 单击工作负载对应的右侧操作“监控”按钮。



7. 查看负载监控指标，详情请参考**云原生监控插件**。
   关于更多监控中心的用法，请参考**应用运维管理（AOM）服务帮助文档**。



4.10 弹性伸缩

简介

弹性伸缩bursting插件支持CCI 1.0和CCI 2.0。但当Pod通过bursting插件弹性到CCI 2.0上时，metrics-server插件无法采集这部分Pod的指标数据，可能导致HPA无法正常工作。为确保HPA功能正常可用，请使用云原生监控插件替换metrics-server插件。

操作步骤

步骤1 安装“云原生监控插件”。

1. 登录CCE控制台。
2. 选择CCE集群，单击进入CCE集群总览页面。
3. 在导航栏左侧单击“插件中心”，进入插件中心首页。
4. 选择“云原生监控插件”，单击“安装”。

图 4-7 安装云原生监控插件

5. 在安装插件页面，进行规格配置，部署模式选择“Server模式”。

说明

如果需要在Agent部署模式下使用HPA功能，请联系技术支持人员。

步骤2 通过云原生监控插件，提供系统资源指标。

- 如果CCE集群中未安装metrics-server插件，请开启Metric API，详情请参见**通过Metrics API提供资源指标**。配置完成后，可使用Prometheus采集系统资源指标。
- 如果CCE集群中已安装metrics-server插件，可以选择以下任意一种方式进行处理：
  - **方式一：请卸载“Kubernetes Metrics Server”插件后，开启Metric API。**
    i. 登录CCE控制台。
    ii. 选择CCE集群，单击进入CCE集群总览页面。
    iii. 在导航栏左侧单击“插件中心”，进入插件中心首页。
    iv. 选择“Kubernetes Metrics Server”插件，单击“卸载”。

v. 开启Metric API，详情请参见**通过Metrics API提供资源指标**。配置完成后，可使用Prometheus采集系统资源指标。

- **方式二：修改APIService对象。**

  需要更新APIService对象“v1beta1.metrics.k8s.io”：

```
apiVersion: apiregistration.k8s.io/v1
kind: APIService
metadata:
  labels:
    app: custom-metrics-apiserver
    release: cceaddon-prometheus
  name: v1beta1.metrics.k8s.io
spec:
  group: metrics.k8s.io
  groupPriorityMinimum: 100
  insecureSkipTLSVerify: true
  service:
    name: custom-metrics-apiserver
    namespace: monitoring
    port: 443
  version: v1beta1
  versionPriority: 100
```

  可以将该对象保存为文件，命名为metrics-apiservice.yaml，然后执行以下命令：

```
kubectl apply -f metrics-apiservice.yaml
```

  执行kubectl top pod -n monitoring命令，如果显示如下，则表示Metrics API能正常访问：

```
# kubectl top pod -n monitoring
NAME                                          CPU(cores)   MEMORY(bytes)
......
custom-metrics-apiserver-d4f556ff9-l2j2m                38m          44Mi
......
```

须知

卸载插件时，需要执行以下kubectl命令，同时删除APIService对象，否则残留的APIService资源将导致metrics-server插件安装失败。

```
kubectl delete APIService v1beta1.metrics.k8s.io
```

----结束

4.11 常见问题

问题一：用户负载无法调度到 CCI，登录 CCE 节点执行 kubectl get node 发现 virtual-kubelet 节点状态为不可调度。

```
user@imkrz4xzkz30alq-machine:~$ kubectl get node
NAME              STATUS                     ROLES             AGE    VERSION
192.168.182.101   Ready                      <none>            33d    v1.23.0-CCE23.0.1
virtual-kubelet   Ready,SchedulingDisabled   virtual-kubelet   4d5h   v1.19.16-v1.3.4-145-g8114c8a-dev
user@imkrz4xzkz30alq-machine:~$
user@imkrz4xzkz30alq-machine:~$
user@imkrz4xzkz30alq-machine:~$ kubectl uncordon virtual-kubelet
node/virtual-kubelet uncordoned
user@imkrz4xzkz30alq-machine:~$ kubectl get node
NAME              STATUS   ROLES             AGE    VERSION
192.168.182.101   Ready    <none>            33d    v1.23.0-CCE23.0.1
virtual-kubelet   Ready    virtual-kubelet   4d5h   v1.19.16-v1.3.4-145-g8114c8a-dev
user@imkrz4xzkz30alq-machine:~$
```

问题原因：CCI资源售罄导致弹性到CCI的资源调度失败，bursting节点会被锁定半小时（状态变为SchedulingDisabled），期间无法调度至CCI。

解决方案：用户可通过CCE集群控制台，使用kubectl工具查看bursting节点状态，如果节点被锁定，可手动解锁bursting节点。

问题二：弹性 CCI 功能不可用

问题原因：用户CCE集群所在子网与10.247.0.0/16重叠，与CCI命名空间下的Service网段冲突。

解决方案：重新规格CCE集群子网网段。

问题三：插件由 1.5.18 及以上版本回退至低于 1.5.18 后，Pod 通过 Service 访问出现异常

问题原因：插件升级到1.5.18及以上版本之后，新弹性到CCI的Pod中的sidecar无法兼容1.5.18以下版本的插件，因此插件回退版本后会导致这些Pod中的Service访问异常。插件在低于1.5.18版本时弹性到CCI的Pod不受影响。

解决方案：

- 方案一：将插件再升级到1.5.18及以上版本。
- 方案二：将Service访问异常的Pod删除重建，重建后弹性到CCI的Pod Service访问将恢复正常。

问题四：插件无法删除

问题场景：因为误修改swr_addr、swr_user导致的插件卸载失败。

问题原因：插件卸载依赖gc-job执行，镜像拉取失败场景gc-job无法运行成功，导致卸载失败。

解决方案：再次进行卸载操作，依次删除gc-job。

1. 插件处于删除失败状态时，先登录至CCE集群配置有kubectl的节点后，再次单击“卸载”。
2. 在210秒内执行以下命令：

a. 删除resource-gc-jobs。

```
kubectl get job -nkube-system | grep "virtual-kubelet-.*-resource-gc-jobs"
kubectl delete job -nkube-system xxx
```

```
[redacted]# kubectl get job -nkube-system | grep "virtual-kubelet-.*-resource-gc-jobs"
virtual-kubelet-0psor2fajaltllvjfc2b-resource-gc-jobs   Running   0/1           41s         41s
[redacted]# kubectl delete job -nkube-system virtual-kubelet-0psor2fajaltllvjfc2b-resource-gc-jobs
job.batch "virtual-kubelet-0psor2fajaltllvjfc2b-resource-gc-jobs" deleted
```

b. 删除namespace-gc-jobs。

```
kubectl get job -nkube-system | grep "virtual-kubelet-.*-namespace-gc-jobs"
kubectl delete job -nkube-system yyy
```

```
[redacted]# kubectl get job -nkube-system | grep "virtual-kubelet-.*-namespace-gc-jobs"
virtual-kubelet-u91uzeflrw7f6v9rrdfi-namespace-gc-jobs   Running   0/1           30s         30s
[redacted]# kubectl delete job -nkube-system virtual-kubelet-u91uzeflrw7f6v9rrdfi-namespace-gc-jobs
job.batch "virtual-kubelet-u91uzeflrw7f6v9rrdfi-namespace-gc-jobs" deleted
```

3. 其余异常场景请提交工单协助处理。

5 审计

5.1 云审计服务支持的 CCI 操作列表

CCI通过云审计服务（Cloud Trace Service，简称CTS）为您提供云服务资源的操作记录，记录内容包括您从云管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

表 5-1 云审计服务支持的 CCI 操作列表

操作名称	事件名称
创建一个Service对象	createService
删除一个Service对象	deleteService
删除指定Namespace下的所有Service对象	deleteServicesByNamespace
替换指定的Service对象	replaceService
更新指定的Service对象	updateService
创建一个Endpoint对象	createEndpoint
删除一个Endpoint对象	deleteEndpoint
删除指定Namespace下的所有Endpoint对象	deleteEndpointsByNamespace
替换指定Namespace下的Endpoint对象	replaceEndpoint
更新指定Namespace下的Endpoint对象	updateEndpoint
创建一个Deployment对象	createDeployment
删除一个Deployment对象	deleteDeployment
删除指定Namespace下的所有Deployment对象	deleteDeploymentsByNamespace

操作名称	事件名称
替换指定Namespace下的Deployment对象	replaceDeployment
更新指定Namespace下的Deployment对象	updateDeployment
替换Deployment对象伸缩长度	replaceDeploymentScale
更新Deployment对象伸缩长度	updateDeploymentScale
创建一个Statefulset对象	createStatefulset
删除一个Statefulset对象	deleteStatefulset
删除指定Namespace下的所有Statefulset对象	deleteStatefulsetsByNamespace
替换指定Namespace下的Statefulset对象	replaceStatefulset
更新指定Namespace下的Statefulset对象	updateStatefulset
创建一个Job对象	createJob
删除一个Job对象	deleteJob
删除指定Namespace下的所有Job对象	deleteJobsByNamespace
替换指定Namespace下的某个Job对象	replaceJob
更新指定Namespace下的某个Job对象	updateJob
创建一个Cronjob对象	createCronjob
删除一个Cronjob对象	deleteCronjob
删除指定Namespace下的所有Cronjob对象	deleteCronjobsByNamespace
替换指定Namespace下的某个Cronjob对象的状态	replaceCronjob
更新指定Namespace下的某个Cronjob对象的状态	updateCronjob
创建一个Ingress对象	createIngress
删除一个Ingress对象	deleteIngress
删除指定Namespace下的所有Ingress对象	deleteIngressesByNamespace
替换指定Namespace下的特定Ingress对象	replaceIngress
更新指定Namespace下的某个Ingress对象	updateIngress
创建一个Namespace	createNamespace

操作名称	事件名称
删除一个Namespace	deleteNamespace
创建一个Pod	createPod
更新指定Pod	updatePod
替换指定Pod	replacePod
删除一个Pod	deletePod
删除Namespace下所有的Pod	deletePodsByNamespace
删除指定Event	deleteEvent
创建一个Configmap	createConfigmap
更新指定Configmap	updateConfigmap
替换指定Configmap	replaceConfigmap
删除一个Configmap	deleteConfigmap
删除指定Namespace下所有的Configmap	deleteConfigmapsByNamespace
创建一个Secret	createSecret
更新指定Secret	updateSecret
替换指定Secret	replaceSecret
删除指定Secret	deleteSecret
删除指定Namespace下所有的Secret	deleteSecretsByNamespace
删除指定Network	deleteNetwork
创建一个Network	createNetwork
删除指定Namespace下所有的Network	deleteNetworksByNamespace
更新指定Network	updateNetwork
替换指定Network	replaceNetwork
创建network-attachment-definition	createNetworkAttachmentDefinition
删除指定Namespace下所有的network-attachment-definitions	deleteNetworkAttachmentDefinitionsByNamespace
删除指定network-attachment-definition	deleteNetworkAttachmentDefinition
创建PVC	createPersistentvolumeclaim
导入已有PVC	createPersistentvolumeclaimByStorageInfo
删除指定Namespace下所有的PVC	deletePersistentvolumeclaimsByNamespace

操作名称	事件名称
替换指定PVC	replacePersistentvolumeclaim
更新指定PVC	updatePersistentvolumeclaim
删除指定PVC	deletePersistentvolumeclaim
购买一个套餐包	createPackageproduct
查询套餐包	getPackageproducts
购买活动套餐包	createActiveproduct
查询活动套餐包	getActiveproducts
创建Kubeflow job	createKubeflowJob
删除指定Namespace下所有的Kubeflow job	deleteKubeflowJobsByNamespace
替换指定Kubeflow job	replaceKubeflowJob
更新指定Kubeflow job	updateKubeflowJob
删除指定Kubeflow job	deleteKubeflowJob
创建Volcano job	createVolcanoJob
删除指定Namespace下所有的Volcano job	deleteVolcanoJobsByNamespace
替换指定Volcano job	replaceVolcanoJob
更新指定Volcano job	updateVolcanoJob
删除指定Volcano job	deleteVolcanoJob
创建Agency	createAgency
更新配额	modifyQuota
创建一个imagecache对象	createImagecache
删除一个imagecache对象	deleteImagecache
替换指定的imagecache对象	replaceImagecache
更新指定的imagecache对象	updateImagecache
上传模板	createChart
更新指定模板	updateChart
删除指定模板	deleteChart
上传插件	createAddon
更新指定插件	updateAddon
删除指定插件	deleteAddon

操作名称	事件名称
创建模板实例	createRelease
更新模板实例	updateRelease
删除模板实例	deleteRelease
创建插件实例	createAddonInstance
更新插件实例	updateAddonInstance
删除插件实例	deleteAddonInstance
创建插件readme	createAddonReadme
删除插件Readme	deleteAddonReadme
创建Clusterrolebinding	createClusterrolebinding
删除Clusterrolebinding	deleteClusterrolebinding
创建Rolebinding	createRolebinding
删除Rolebinding	deleteRolebinding
替换Rolebinding	replaceRolebinding
更新Rolebinding	updateRolebinding
创建Eippool	createEippool
删除Eippool	deleteEippool
替换Eippool	replaceEippool
更新Eippool	updateEippool
删除指定Namespace下所有的Eippool	deleteEippoolsByNamespace

5.2 查看云审计日志

操作场景

开启了云审计服务后，系统开始记录CCI资源的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的图标，选择区域。

步骤3 单击页面上方的“服务列表”，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

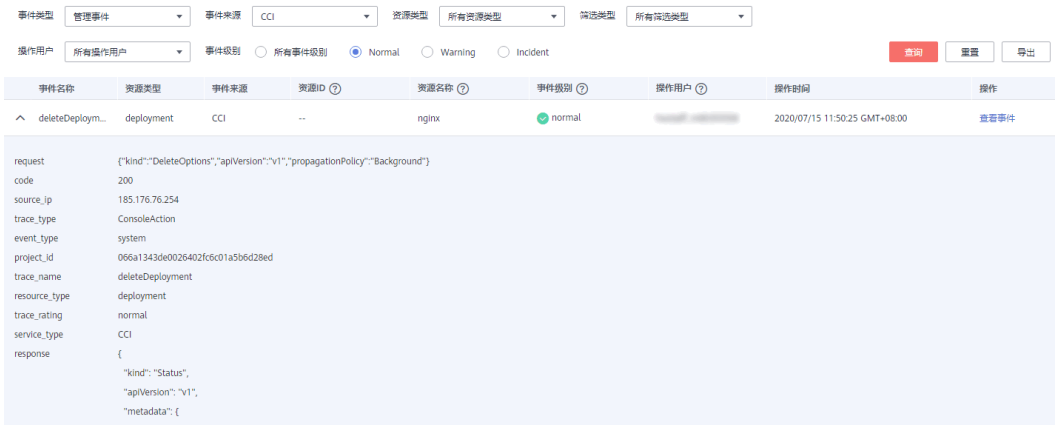
步骤4 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤5 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- 事件类型、事件来源、资源类型和筛选类型。
  在下拉框中选择查询条件。其中，事件来源选择“CCI”。
  当筛选类型选择事件名称时，还需选择某个具体的事件名称。
  选择资源ID时，还需选择或者手动输入某个具体的资源ID。
  选择资源名称时，还需选择或手动输入某个具体的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- 起始时间、结束时间：可通过选择时间段查询操作事件。

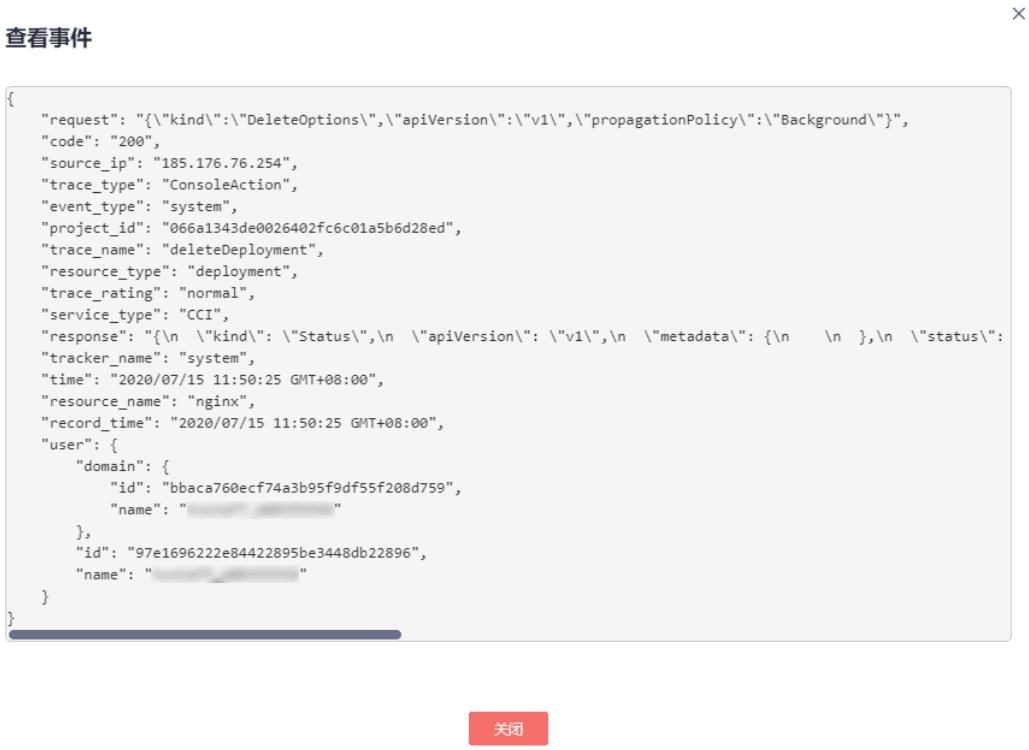
步骤6 在需要查看的记录左侧，单击 展开该记录的详细信息，展开记录如图5-1所示。

图 5-1 展开记录



步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图5-2所示，显示了该操作事件结构的详细信息。

图 5-2 查看事件



----结束

