华为云 UCS

最佳实践

文档版本 01

发布日期 2023-09-22

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

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

目 录

1 权限配置 1
1.1 IAM 用户配置权限实践 1
2 集群联邦 8
2.1 多集群应用多活容灾 8
2.2 多集群应用故障倒换 14
2.3 打通 CCE 集群节点间与容器间网络 19
3 本地集群 25
3.1 本地集群接入 UCS 25
3.2 本地集群工作负载获取 IAM Token 36
4 服务网格 41
4.1 第三方注册中心接入能力 41
4.2 UCS 服务网格 集群连通方法 43
4.2.1 同 region 集群打通方法 43
4.2.2 跨 region 集群打通方法 45
4.2.3 如何确认集群连通 49

1 权限配置

1.1 IAM 用户配置权限实践

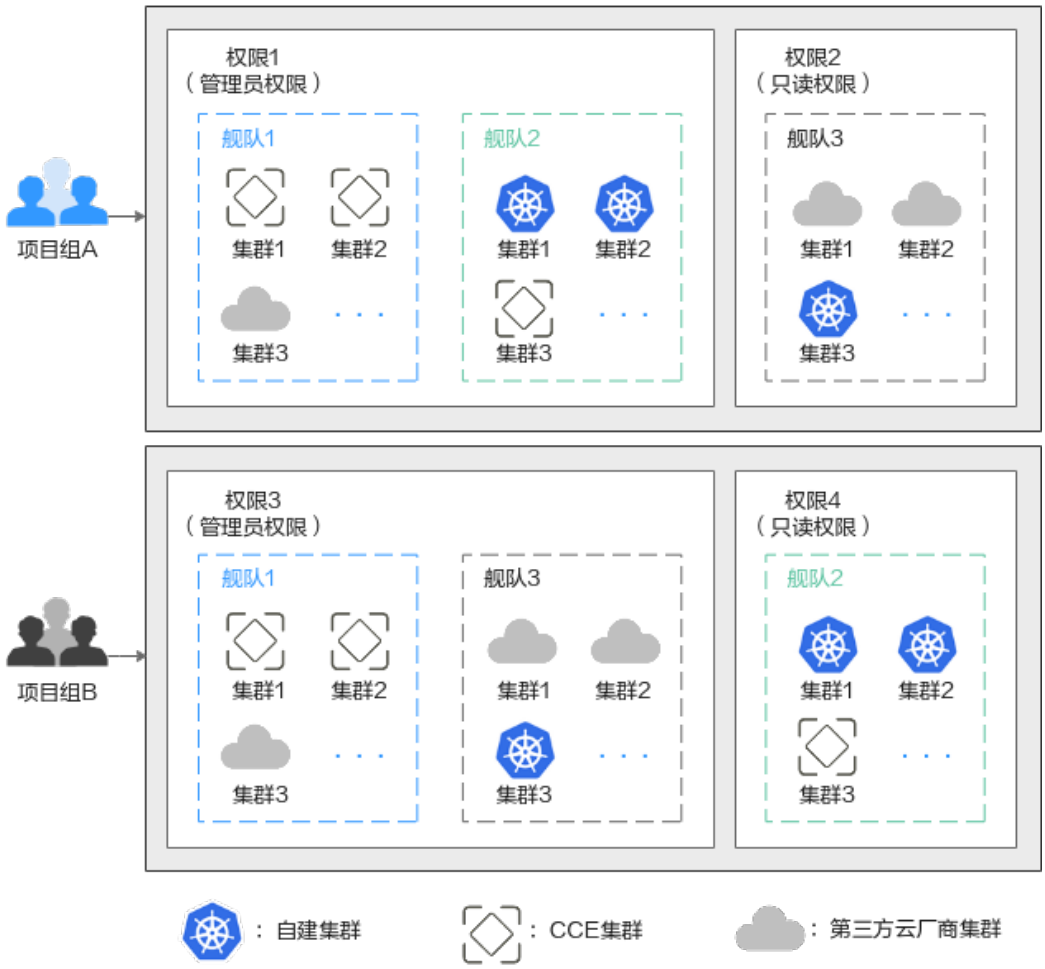
应用场景

UCS在统一身份认证服务（IAM）能力基础上，为用户提供细粒度的权限管理功能，帮助用户灵活便捷地对租户下的IAM用户设置不同的UCS资源权限，结合权限策略和舰队设计，可实现企业不同部门或项目之间的权限隔离。

例如，某公司同时推进两个项目组，每个项目组中有多名成员，权限分配如图1-1所示。

- 项目组A在开发过程中需要舰队1、2的管理员权限以及舰队3的只读权限。
- 项目组B在开发过程中需要舰队1、3的管理员权限以及舰队2的只读权限。

图 1-1 权限设计



解决方案

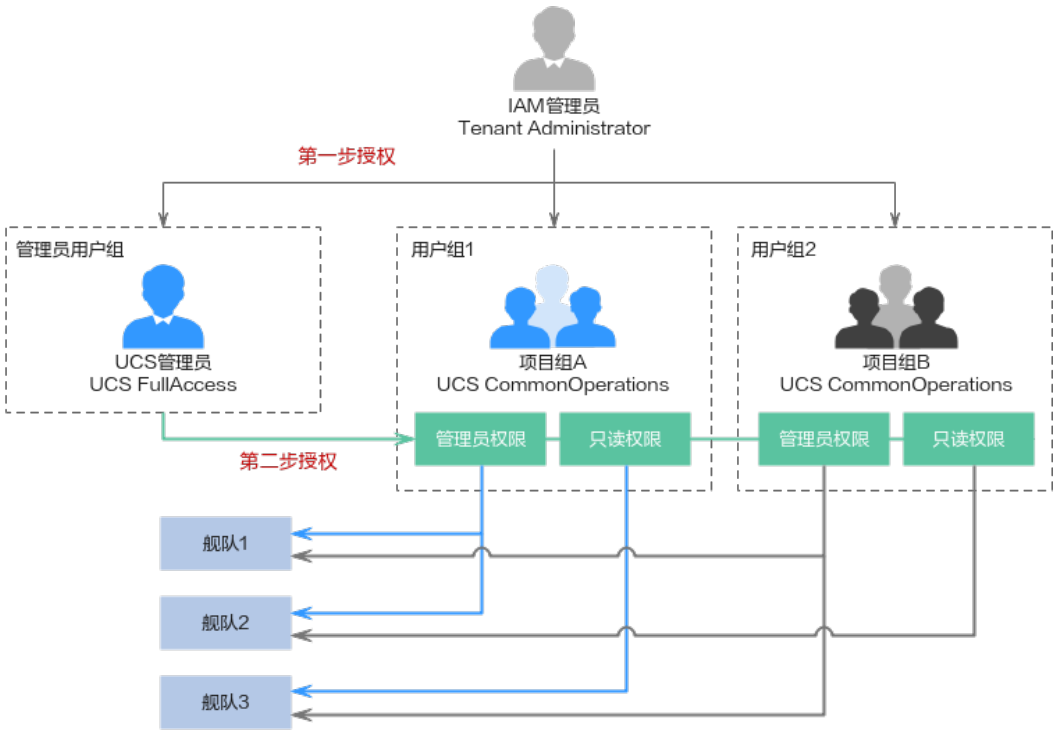
要想实现上述的权限隔离，必须结合使用IAM系统策略和UCS权限管理功能，IAM系统策略控制用户可操作哪些UCS控制台的功能，UCS权限管理控制用户可操作哪些舰队和集群资源。

如图1-2所示，授权包括如下两大步骤。

- 第一步授权（IAM控制台）：拥有Tenant Administrator权限的IAM管理员需要创建三个用户组，一个为管理员用户组，另外两个为项目组A、B所对应的用户组（用户组1、2），分别授予UCS FullAccess和UCS CommonOperations权限。
- 第二步授权（UCS控制台）：拥有UCS FullAccess权限的UCS管理员分别为用户组1、用户组2创建各自的管理员权限、只读权限，然后关联到舰队上。

  具体的关联策略如下：用户组1的管理员权限关联至舰队1、舰队2，只读权限关联至舰队3；用户组2的管理员权限关联至舰队1、舰队3，只读权限关联至舰队2。

图 1-2 授权方案



前提条件

- 帐号已开通UCS服务，并且按照图1-1完成舰队、集群资源的准备工作。
- 按照图1-2完成权限数据的准备工作。

表 1-1 IAM 控制台数据准备

用户组	用户	权限
管理员用户组：UCS_Group_admin	UCS_Group_admin_User1	UCS FullAccess
用户组1：UCS_Group_1	UCS_Group_1_User1、UCS_Group_1_User2 ...	UCS CommonOperations
用户组2：UCS_Group_2	UCS_Group_2_User1、UCS_Group_2_User2 ...	UCS CommonOperations

表 1-2 UCS 控制台数据准备

用户组	用户	权限类型	权限名称
用户组1	UCS_Group_1_User1、UCS_Group_1_User2 ...	管理员权限	ucs-group-1-admin
		只读权限	ucs-group-1-readonly

用户组	用户	权限类型	权限名称
用户组2	UCS_Group_2_User1、UCS_Group_2_User2 ...	管理员权限	ucs-group-2-admin
		只读权限	ucs-group-2-readonly

步骤一：IAM 管理员授权

步骤1 使用IAM管理员帐号登录IAM控制台。

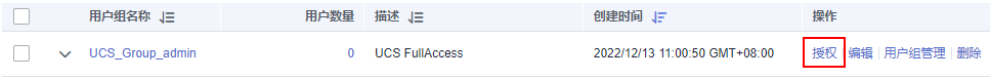
步骤2 左侧导航栏选择“用户组”，单击右上角“创建用户组”。

步骤3 在“创建用户组”界面，输入管理员用户组的名称及描述，单击“确定”，完成用户组创建。

图 1-3 创建用户组

步骤4 在用户组列表中，单击目标用户组右侧的“授权”按钮。

图 1-4 授权



步骤5 搜索并选择权限策略UCS FullAccess。

图 1-5 选择策略

步骤6 单击“下一步”，选择授权范围方案。

选择“所有资源”，不设置最小授权范围，用户可根据权限使用帐号中所有资源，包括企业项目、区域项目和全局服务资源。

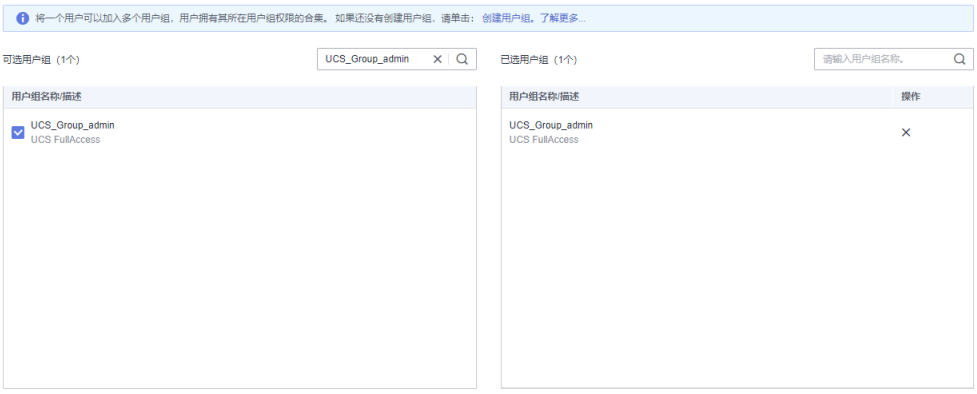
步骤7 单击“确定”完成授权。

步骤8 左侧导航栏选择“用户”，单击右上角“创建用户”，新建一个IAM用户。

填写用户名及初始密码，其余参数说明请参见**创建IAM用户**。

步骤9 单击“下一步”，选择加入**步骤4**中已授权的用户组。

图 1-6 加入用户组



步骤10 单击“创建用户”。

步骤11 重复上述步骤，完成**表1-1**中其他用户组、用户的创建和授权。

----结束

步骤二：UCS 管理员授权

步骤1 使用UCS管理员登录UCS控制台，在左侧导航栏选择“权限管理”。

步骤2 单击右上角的“创建权限”按钮。

步骤3 在弹出页面中填写权限的参数项，如**图1-7**所示。

图 1-7 创建权限

- 权限名称：自定义权限的名称，需以小写字母开头，由小写字母、数字、中划线（-）组成，且不能以中划线（-）结尾。
- 用户：选择权限关联的用户，即上一步创建的IAM用户。实际应用中，一个用户组会有多个用户，创建权限时，可以将这个用户组下的所有用户全部选中，以达到批量授权的目的。
- 权限类型：选择“管理员权限”。管理员权限表示对所有集群资源对象的读写权限。

步骤4 单击“确定”，创建权限。

步骤5 权限创建完成后，可前往“容器舰队”页面，单击目标舰队右上角  按钮。

图 1-8 为舰队关联权限

步骤6 在弹出的页面单击“关联权限”，打开“修改权限”页面，将**步骤3**中创建的权限和舰队的全部命名空间关联起来。

图 1-9 关联权限

步骤7 单击“确定”。完成后，使用该IAM用户登录UCS控制台可使用权限范围内的功能。

步骤8 重复以上步骤，完成表1-2中其他权限的创建，以及权限和舰队的关联。

----结束

2 集群联邦

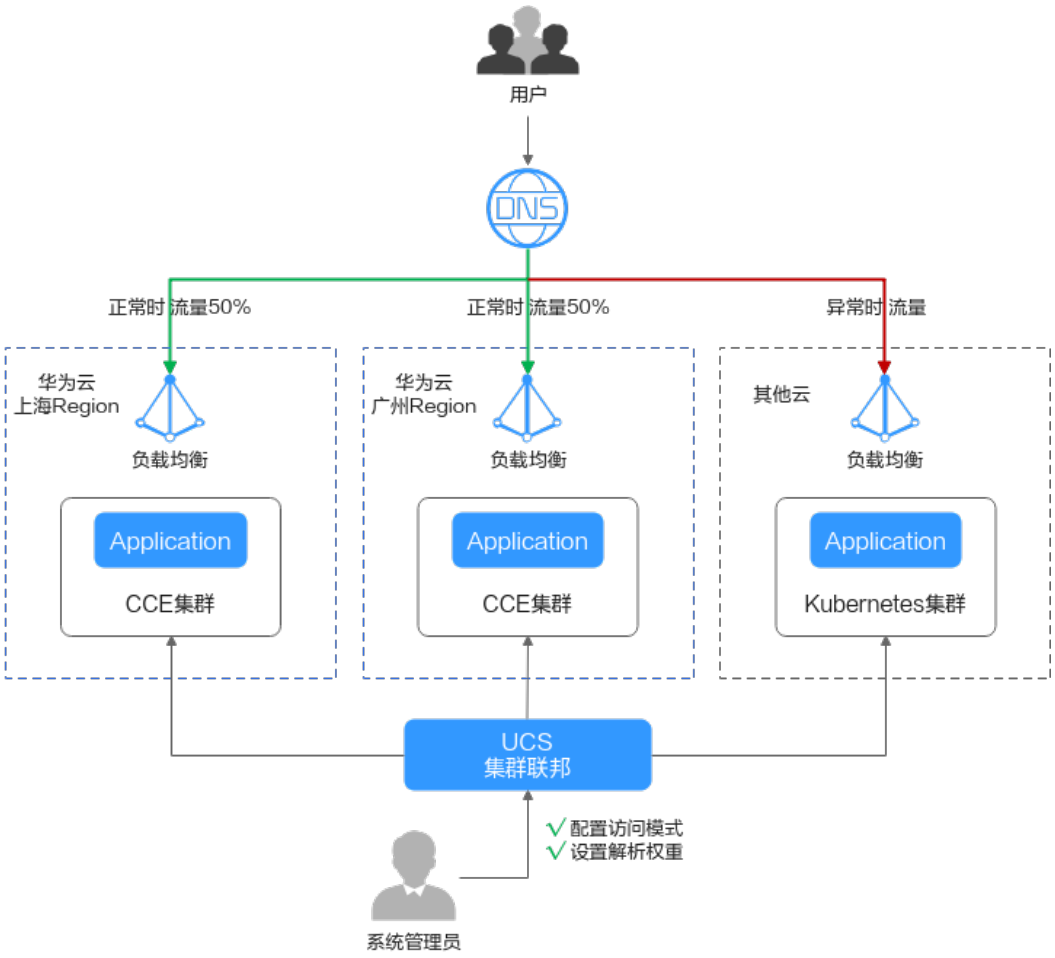
2.1 多集群应用多活容灾

应用场景

为了应对云单点宕机故障，UCS的集群联邦提供多云多活应用、秒级流量接管能力。业务应用的实例可以多云多活的部署在不同云上的容器服务中，当云单点宕机故障发生时，集群联邦可以秒级自动完成应用实例的弹性迁移以及流量的切换，业务的可靠性大大提升。

多活容灾方案示意如图2-1所示，通过创建域名访问规则，将应用分发到3个Kubernetes集群，包括两个华为云CCE集群（部署在不同Region）和一个其他云的Kubernetes集群，实现应用的多活容灾。

图 2-1 多云集群应用多活容灾示意图



准备工作

- 准备应用所运行的集群，本文以CCE集群为例进行演示，参考**购买CCE集群**在两个不同区域（如：华南-广州和华东-上海一）创建CCE集群，要求Kubernetes版本为1.19及以上，并且各个集群中至少拥有一个可用节点。

  说明

  在实际生产环境中，多个集群可位于不同区域、可用区，甚至不同云服务商，实现应用的多活容灾。

- 已购买公网域名，并添加至华为云云解析（DNS）服务，具体操作请参考**快速添加网站域名解析**。

基础环境搭建

步骤1 将集群注册到UCS并接入网络。具体操作请参见**注册集群**。

例如，将集群“ccecluster01”、“ccecluster02”注册到UCS的“ucs-group”容器舰队，并查看集群是否处于正常运行状态。

步骤2 为集群所在舰队开通集群联邦，并确保集群已成功接入集群联邦。具体操作请参见**集群联邦**。

图 2-2 集群管理

步骤3 创建联邦工作负载。

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

- 集群ccecluster01：示例应用使用nginx:gz镜像，返回“ccecluster01 is in Guangzhou.”。
- 集群ccecluster02：示例应用使用nginx:sh镜像，返回“ccecluster02 is in Shanghai.”。

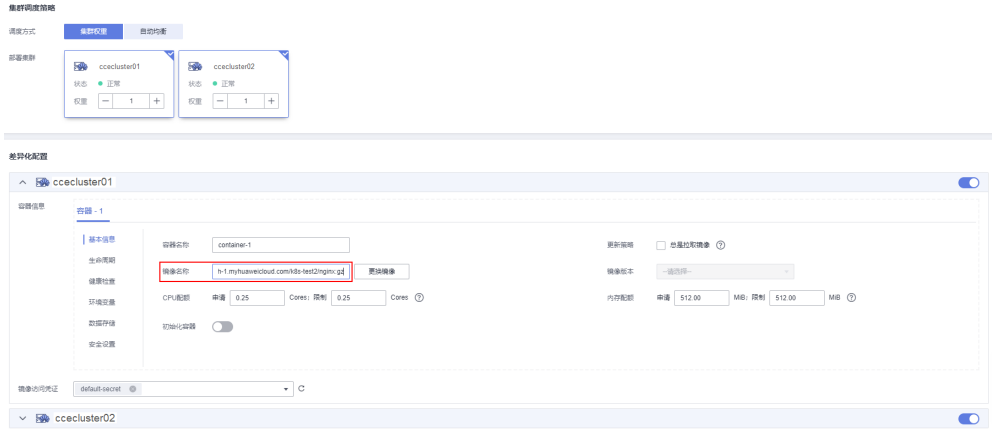
在开始操作之前，您需要将示例应用的镜像上传到对应集群所在区域的SWR镜像仓库中（也就是说，nginx:gz镜像需要上传至华南-广州，nginx:sh镜像上传至华东-上海一），否则联邦工作负载会因拉取不到镜像而异常。

说明

本文中的应用仅作示例，在实际生产环境中需替换为您的自有应用，且对集群的云服务商、区域、数量不作限制。

1. 登录华为云UCS控制台，选择左侧导航栏中的“容器舰队”。
2. 单击已开通集群联邦的舰队名称，进入详情页面。
3. 在左侧导航栏选择“联邦管理 > 工作负载”，单击右上角“镜像创建”。
4. 填写基本信息并配置容器参数，镜像可以任意设置，单击“下一步：调度与差异化”。
5. 设置集群调度策略，完成集群差异化配置，单击“创建工作负载”。
   - 调度方式：选择“集群权重”，并设置两个集群的权重为1:1。
   - 差异化配置：单击集群右侧的  图标开启差异化配置，设置集群ccecluster01的镜像名称为“swr.cn-south-1.myhuaweicloud.com/kubernetes-test2/nginx:gz”（nginx:gz镜像在SWR镜像仓库中的地址），集群ccecluster02的镜像名称为“swr.cn-east-3.myhuaweicloud.com/kubernetes-test2/nginx:sh”。

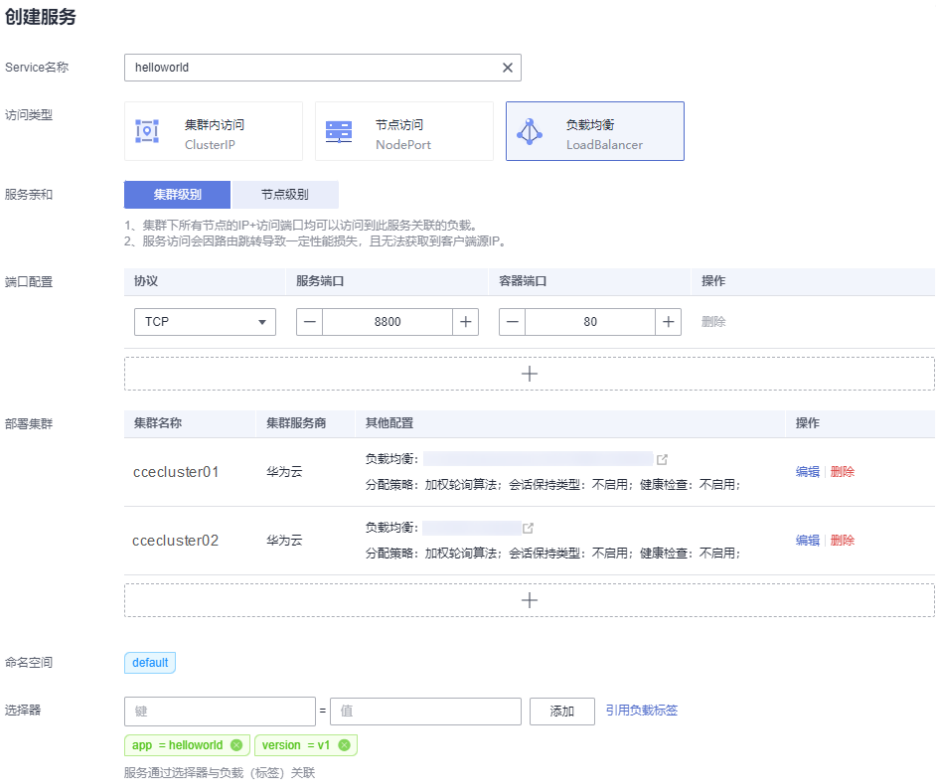
图 2-3 调度与差异化



步骤4 创建LoadBalancer访问。

1. 登录华为云UCS控制台，选择左侧导航栏中的“容器舰队”。
2. 单击已开通集群联邦的舰队名称，进入详情页面。
3. 在左侧导航栏选择“联邦管理 > 服务与路由”，单击右上角“创建服务”。
4. 完成参数填写，单击“确认”。
   - 访问类型：选择“负载均衡”。
   - 端口配置：选择TCP协议，填写服务端口、容器端口，如8800、80。
   - 部署集群：单击 ，依次添加ccecluster01和ccecluster02集群，负载均衡器选择共享型ELB实例，且必须和集群处于相同VPC中，如果列表中无可用ELB实例，单击“创建负载均衡器”前往ELB控制台进行创建。其他参数保持默认即可。
   - 选择器：服务通过选择器与负载标签关联，这里通过引用负载标签的方式来添加标签。

图 2-4 创建服务

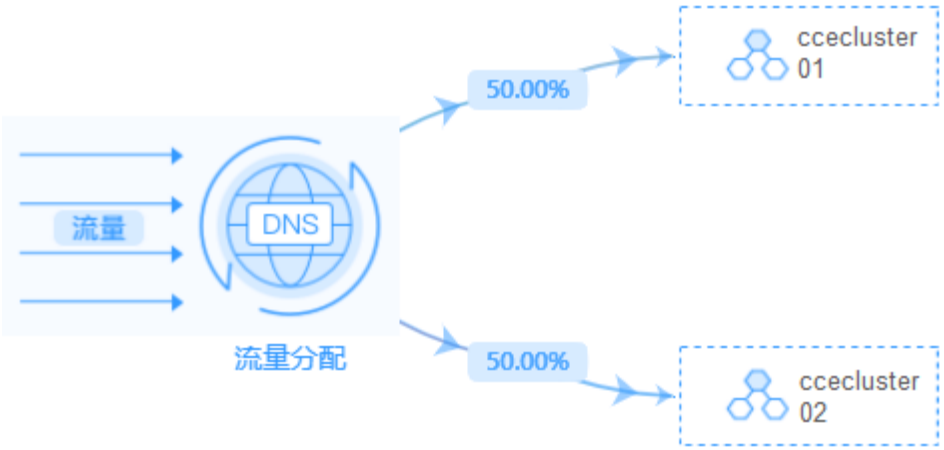


步骤5 创建域名访问。

1. 登录华为云UCS控制台，选择左侧导航栏中的“容器舰队”。
2. 单击已开通集群联邦的舰队名称，进入详情页面。
3. 在左侧导航栏选择“联邦管理 > 域名访问”，添加根域名。
4. 单击右上角“创建域名访问”，完成参数填写。
   - 目标服务：选择**步骤4**中创建的服务。
   - 流量配比模式：选择“自适应模式”，流量解析根据各集群后端实例数量自动分配权重。在本示例中，ccecluster01和ccecluster02集群的实例数均为1，那么正常情况下，两个集群将按照1:1的配比接收流量，如**图2-6**所示。

图 2-5 配置流量配比

图 2-6 流量配比拓扑图



----结束

多活容灾场景验证

按照上述集群应用部署操作，示例应用分别部署在集群“ccecluster01”和“ccecluster02”中，并以“负载均衡”类型的服务对外提供访问。**步骤5**中的域名访问创建成功后，系统自动为所选择的根域名添加解析记录，并且在UCS侧生成一个统一的对外访问路径（域名地址），因此，我们通过访问这个域名地址就可以验证流量的分配情况。

步骤1 获取域名访问地址。

1. 登录华为云UCS控制台，选择左侧导航栏中的“容器舰队”。
2. 单击已开通集群联邦的舰队名称，进入详情页面。
3. 在左侧导航栏选择“联邦管理 > 域名访问”，列表中的“域名地址”即为域名访问地址。

图 2-7 域名地址

步骤2 在一台已连接公网的机器上执行如下命令，持续访问域名地址，查看集群应用处理状态。

- 正常情况下，两个集群上的应用均接收流量，并且各处理50%流量。

```
while true;do wget -q -O- helloworld.default.mcp-xxx.svc.xxx.co:8800; done
ccecluster01 is in Guangzhou.
ccecluster02 is in Shanghai.
ccecluster01 is in Guangzhou.
ccecluster02 is in Shanghai.
ccecluster01 is in Guangzhou.
ccecluster02 is in Shanghai.
...
```

- 当集群ccecluster01上的应用异常时（通过集群节点关机来模拟应用异常），系统将所有的流量路由到ccecluster02集群处理，用户感知不到异常。

```
while true;do wget -q -O- helloworld.default.mcp-xxx.svc.xxx.co:8800; done
ccecluster02 is in Shanghai.
ccecluster02 is in Shanghai.
ccecluster02 is in Shanghai.
```

```
ccecluster02 is in Shanghai.
ccecluster02 is in Shanghai.
ccecluster02 is in Shanghai.
...
```

返回UCS控制台，可以看到域名列表中的集群流量比例发生变化，由ccecluster02集群接管100%的流量，这与我们配置的流量配比模式以及观测到的现象均吻合。

图 2-8 域名列表

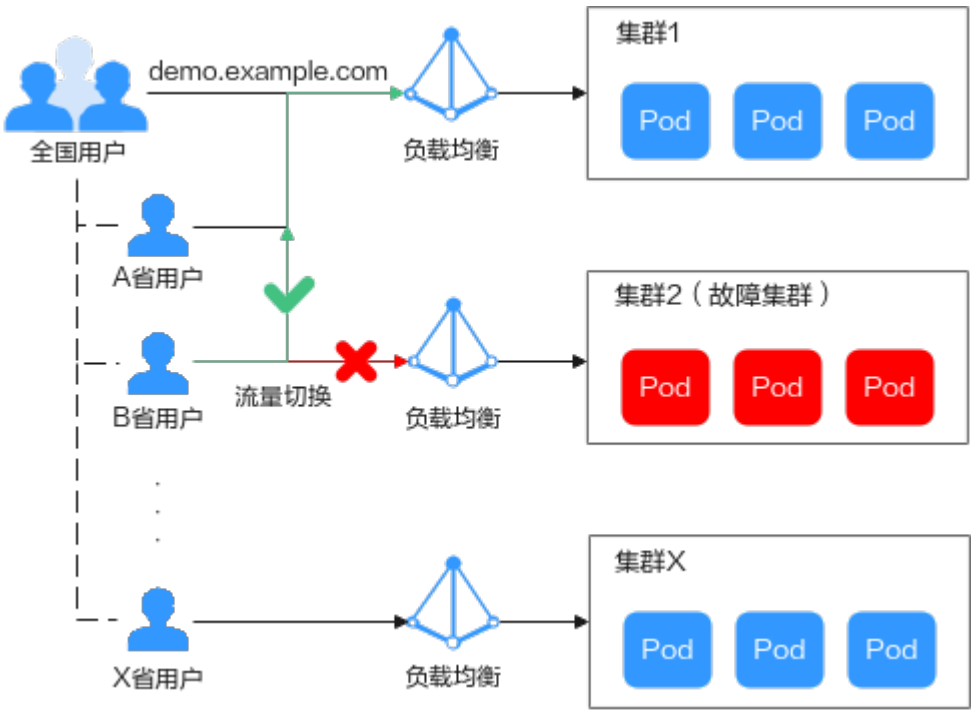
----结束

2.2 多集群应用故障倒换

应用场景

在分布式集群场景下，为了给用户提供低延迟的服务，应用可能部署在不同区域、不同厂商的云端上，在某个地区集群发生故障时，该地区的用户访问也随之会受到影响。利用UCS的流量管理和应用数据管理功能，可以实现多云多集群场景下的应用故障倒换、调度和迁移，故障倒换方案示意如图2-9所示。

图 2-9 多云集群应用故障倒换示意图



约束与限制

- 您需要拥有两个Kubernetes版本为1.19及以上的可用集群，并且各个集群中至少拥有一个可用节点。

- 您需要已有一个公网域名，并添加至华为云云解析（DNS）服务，具体操作请参考**快速添加网站域名解析**。

基础环境搭建

步骤1 将集群注册到UCS并接入网络。具体操作请参见**注册集群**。

例如，将集群“ccecluster01”、“ccecluster02”添加至UCS，并查看集群是否处于正常运行状态。

步骤2 在添加至UCS的两个集群中分别创建一个工作负载。

说明

为展示流量切换的效果，本实践中两个集群的容器镜像版本不同。

- 集群“ccecluster01”：示例应用版本号为1.0.0。
- 集群“ccecluster02”：示例应用版本号为2.0.0。

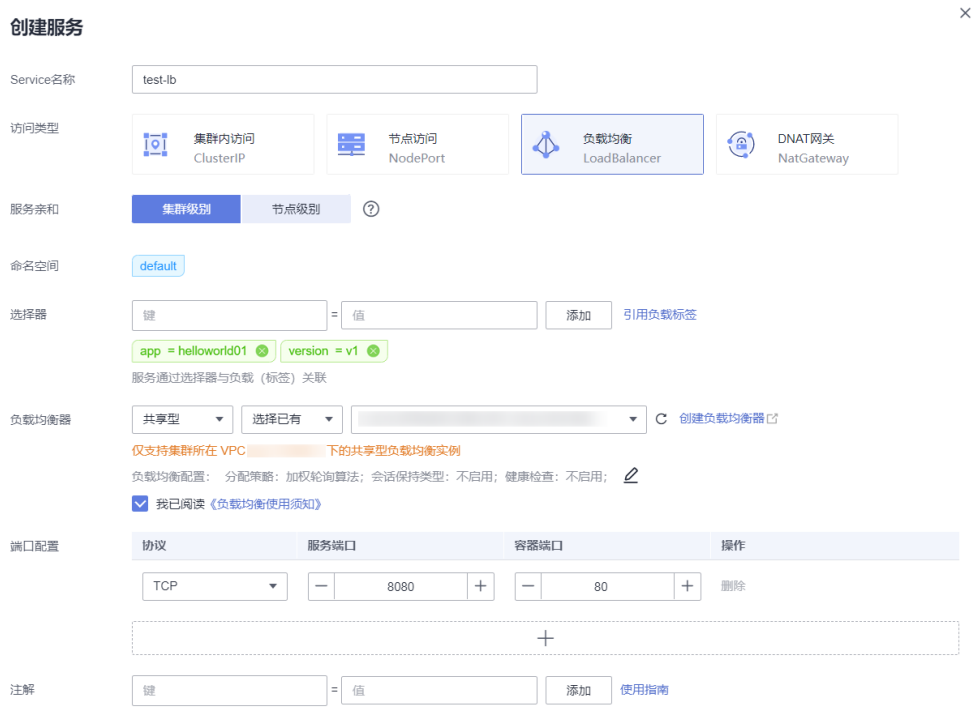
图 2-10 创建工作负载

步骤3 分别为两个集群中的应用创建“负载均衡”类型的服务。

说明

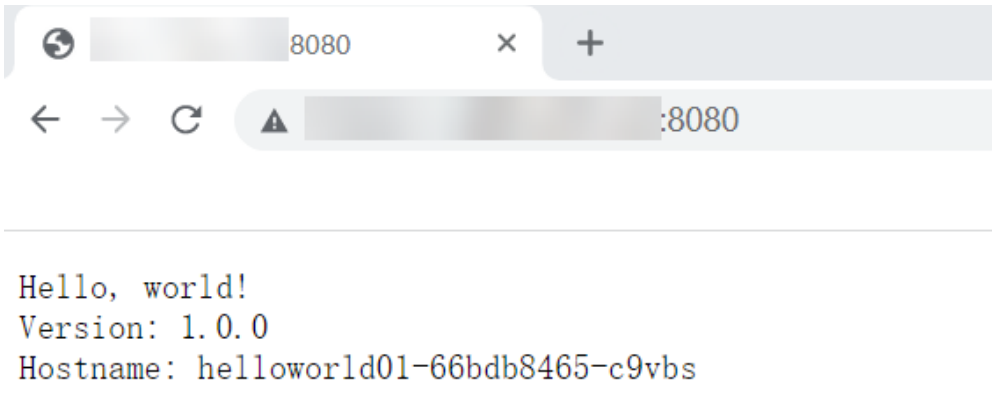
仅支持访问类型为“负载均衡”的服务，其他类型的服务将被自动过滤。

图 2-11 创建服务



步骤4 浏览器访问负载均衡IP地址，查看部署结果。

图 2-12 查看部署结果



----结束

故障倒换场景验证

按照上述集群应用部署操作，示例应用分别部署在集群“ccecluster01”、“ccecluster02”中，并以“负载均衡”类型的服务对外提供访问。

下面将通过UCS的流量分发功能，实现多集群应用的故障倒换，验证应用的高可用容灾能力。

说明

实践中的应用仅作示例，在实际生产环境中可替换为用户自有应用，且对示例集群的提供商、地域、数量不作限制。

步骤1 登录UCS控制台，在左侧导航栏中单击“流量分发”。

步骤2 在流量管理控制台页面，单击右上角“创建流量策略”，填写域名地址解析，设置本例中的测试域名为“demo.example.com”。

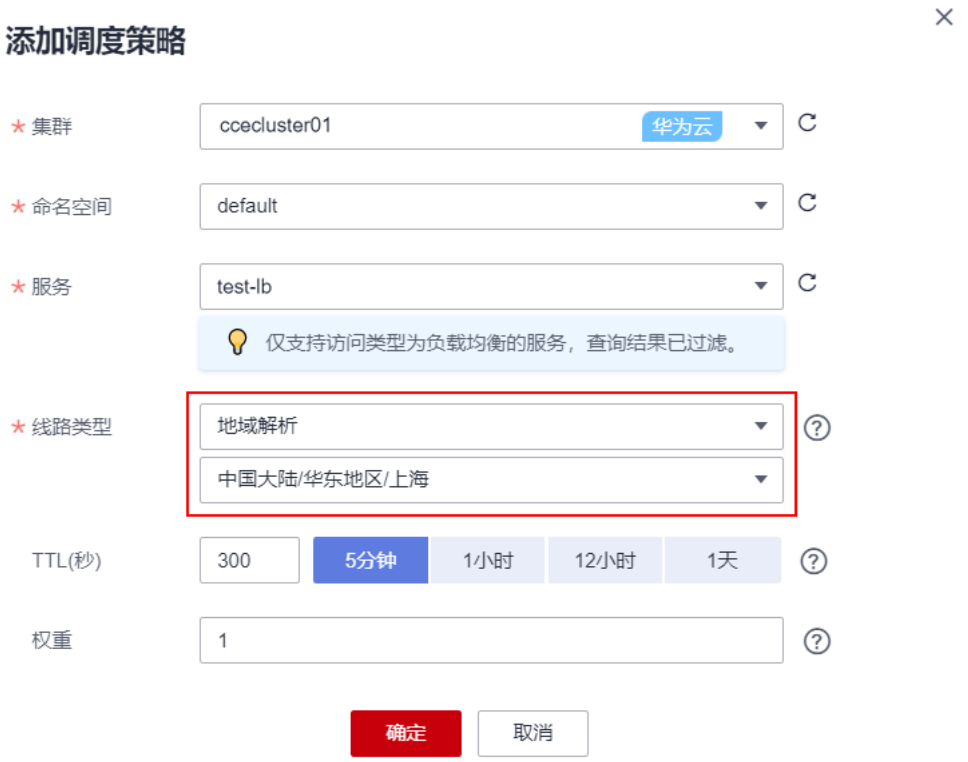
图 2-13 创建流量策略

步骤3 为两个集群服务分别添加调度策略，添加完成后单击“确定”。

本示例中，为模拟不同地域下的集群应用部署，添加三条调度策略：

- 集群“ccecluster01”线路类型设置为“地域解析-中国大陆/华东地区/上海”。
- 集群“ccecluster02”线路类型设置为“地域解析-中国大陆/华南地区/广东”。
- 为域名添加默认线路解析记录，设置集群“ccecluster01”线路类型为“全网默认”。如不设置默认线路解析将会造成指定线路外的地区用户访问失败。

图 2-14 添加调度策略



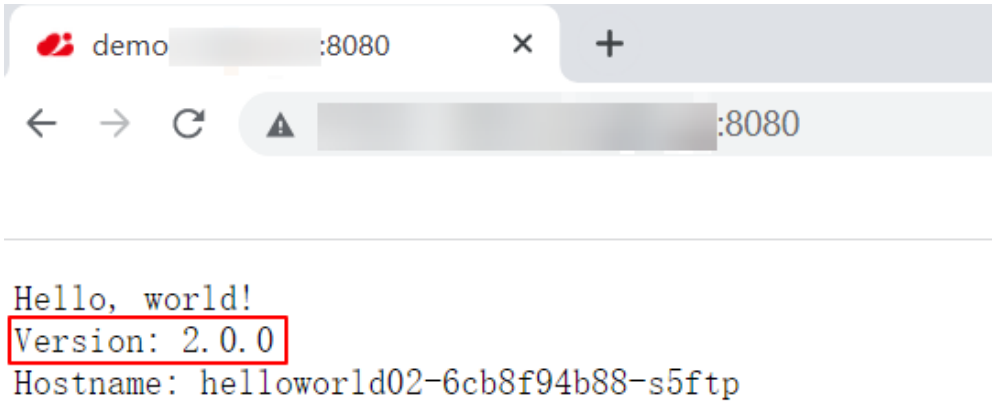
步骤4 此时已为测试域名“demo.example.com”添加了三条解析，用户流量将根据设置的线路类型和权重正常访问两个集群中的应用。

图 2-15 调度策略列表

- 上海地区用户：将访问集群“ccecluster01”中的应用，版本为1.0.0。
- 广东地区用户：将访问集群“ccecluster02”中的应用，版本为2.0.0。
- 其他用户：将默认访问集群“ccecluster01”中的应用，版本为1.0.0。

步骤5 广东地区用户通过域名“demo.example.com”访问应用，版本为2.0.0，说明访问的是集群“ccecluster02”中的应用。

图 2-16 查看访问结果



步骤6 此时手动停止集群“ccecluster02”中的应用，将实例个数调整为0，模拟环境故障。

图 2-17 调整实例个数

步骤7 广东地区用户访问应用时，依旧被解析至集群“ccecluster02”，返回错误。

此时需要在“流量分发”页面单击集群“ccecluster02”对应调度策略的“暂停”按钮，进行应用故障倒换。

图 2-18 暂停调度策略

广东地区用户访问域名“demo.example.com”时，不再解析至集群“ccecluster02”，只会将默认线路解析结果返回，用户访问到集群

“ccecluster01”，访问正常。待运维人员完成故障集群修复后，可单击“启用”按钮重新使用该线路解析。

----结束

2.3 打通 CCE 集群节点间与容器间网络

应用场景

在创建MCS对象前，需要保证集群间网络互通。其中，跨VPC的CCE集群间网络可以通过创建对等连接的方式打通。

本文将介绍如何通过创建对等连接的方式，为跨VPC的CCE集群打通节点间与容器间网络。

设置集群网络类型

将集群的网络类型设置为underlay以支持集群间Pod通信。支持underlay网络的CCE集群类型如下：

表 2-1 支持 underlay 网络的集群类型

CCE集群类型	网络类型	是否支持underlay网络
CCE集群	容器隧道网络	不支持
	VPC网络	支持
CCE Turbo集群	云原生网络2.0	支持

创建对等连接

步骤1 进入**对等连接列表页面**。

步骤2 在页面右上角区域，单击“创建对等连接”，并在弹出的对话框中，根据界面提示设置对等连接参数。参数详细说明请参见**表2-2**。

图 2-19 创建对等连接

表 2-2 创建对等连接参数说明

参数	是否必选	说明
对等连接名称	是	对等连接的名称。由中文字符、英文字母、数字、中划线、下划线等构成，一般不超过64个字符。
本端VPC	是	本端集群的VPC，可以在下拉框中选择已有VPC。
帐户	是	• 当前帐户：当对等连接中的对端VPC和本端VPC位于同一个帐户下时，选择该项。 • 其他帐户：当对等连接中的对端VPC和本端VPC位于不同帐户下时，选择该项。
对端项目	当帐户选择“其他帐户”时必选	对端项目ID是另一个帐户下，对端VPC所在区域对应的项目ID，获取方法请参见**获取对等连接的对端项目ID**。
对端VPC	当帐户选择“其他帐户”时必选	对端VPC ID。获取方法请参见**获取虚拟私有云的ID信息**。

参数	是否必选	说明
描述	否	对该连接的描述信息。描述信息内容不能超过255个字符，且不能包含“<”和“>”。

步骤3 点击所创建的对等连接名称，进入对等连接详情页，单击“添加路由”，为对等连接添加目的地址为对端集群VPC网段的路由。

如图2-20所示，您需要填写的参数为路由中的两个“目的地址”，请参考表2-3进行配置。

图 2-20 添加路由

表 2-3 添加路由参数说明

参数	是否必选	说明
目的地址（对端）	是	对等连接另一端VPC内的地址，此处填写对端集群VPC网段。 集群VPC网段的查找方法如下： 1. 登录VPC控制台。 2. 左侧导航栏选择“虚拟私有云>我的VPC”，找到对应的对端虚拟私有云，复制其IPv4网段信息。 **图 2-21** 查找对端集群 VPC 网段 
目的地址（本端）	是	对等连接另一端VPC内的地址，此处填写本端集群VPC网段。 **注意** 请仔细检查路由中配置的目的地址信息，防止出现网段冲突。
描述	否	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

步骤4 在对等连接详情页单击“添加路由”，为对等连接添加目的地址为对端集群容器网段的路由。

如图2-22所示，您需要填写的参数为路由中的两个“目的地址”，请参考表2-4进行配置。

图 2-22 添加路由

表 2-4 添加路由参数说明

参数	是否必选	说明
目的地址（对端）	是	对等连接另一端VPC内的地址，此处填写对端集群容器网段。 集群容器网段的查找方法如下： 1. 登录CCE控制台。 2. 点击目标集群名称，进入集群详情页，复制“网络信息>默认容器子网”中的IPv4网段信息。 **注意** 若存在多个容器网段，应为每个网段创建路由，以保证容器间的网络通信。 **图 2-23** 查找对端集群容器网段 

参数	是否必选	说明
目的地址（本端）	是	对等连接另一端VPC内的地址，此处填写本端集群容器网段。 **注意** 请仔细检查路由中配置的目的地址信息，防止出现网段冲突。
描述	否	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

----结束

修改安全组

修改本端集群节点的安全组，在入方向规则中允许对端集群节点访问本端集群容器端口。

如图2-24所示，“协议端口”填写本端集群容器端口，“源地址”填写对端集群节点IP地址或网段。修改安全组的具体操作请参见**更改集群节点的默认安全组**。

图 2-24 修改安全组

验证集群间网络互通

步骤1 登录本端集群节点，执行以下命令，验证本端集群节点与对端集群节点的通信情况。

ping *对端集群节点的IP地址*

ping通则表示本端集群节点与对端集群节点间可以通信。

步骤2 进入本端集群容器，执行以下命令，验证本端集群容器与对端集群容器的通信情况。

curl *对端集群Pod的IP地址*

curl通则表示本端集群容器与对端集群容器间可以通信。

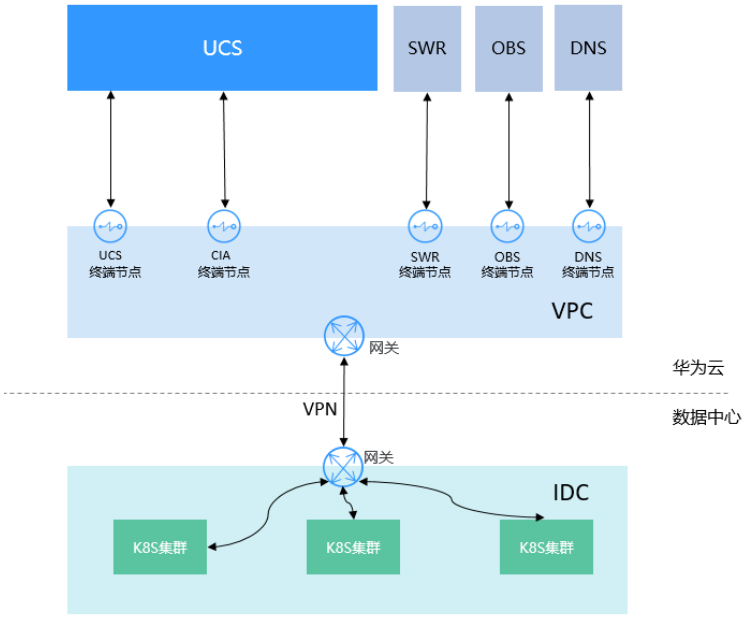
----结束

3 本地集群

3.1 本地集群接入 UCS

概述

用户在线下IDC有kubernetes集群，接入到UCS开启容器智能分析服务，能够与SWR、OBS通信，在无法通过公网连接的情况下，可以先通过VPN与华为云VPC连接，然后通过VPC终端节点服务，让VPC能够在内网访问UCS、SWR、DNS、OBS、CIA。



接入前准备

服务	域名	IP（如涉及）	端口
SWR	swr.cn-north-4.myhuaweicloud.com	从VPCEP中获取。	443
OBS	op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com	不涉及	443、80
CIA	cie-{容器智能分析实例instanceid前八位数字}{当前选择接入的VPC子网ID前八位数字}.cn-north-4.myhuaweicloud.com	从VPCEP中获取。	443
DNS	不涉及	创建VPCEP，选择DNS Endpoint对应的地址。	53

其他区域的SWR及依赖OBS的域名信息

Region	SWR域名	OBS域名
华北-北京四	swr.cn-north-4.myhuaweicloud.com	op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com
华东-上海二	swr.cn-east-2.myhuaweicloud.com	obs.cn-east-2.myhuaweicloud.com
华东-上海一	swr.cn-east-3.myhuaweicloud.com	op-svc-swr-b051-10-147-7-14-3az.obs.cn-east-3.myhuaweicloud.com
华南-广州	swr.cn-south-1.myhuaweicloud.com	op-svc-swr-b051-10-230-33-197-3az.obs.cn-south-1.myhuaweicloud.com

Region	SWR域名	OBS域名
西南-贵阳一	swr.cn-southwest-2.myhuaweicloud.com	op-svc-swr-b051-10-205-14-19-3az.obs.cn-southwest-2.myhuaweicloud.com
华北-乌兰察布一	swr.cn-north-9.myhuaweicloud.com	obs.cn-north-9.myhuaweicloud.com
亚太-新加坡	swr.ap-southeast-3.myhuaweicloud.com	op-svc-swr-b051-10-38-34-172-3az.obs.ap-southeast-3.myhuaweicloud.com
香港	swr.ap-southeast-1.myhuaweicloud.com	obs.ap-southeast-1.myhuaweicloud.com
拉美-墨西哥一	swr.na-mexico-1.myhuaweicloud.com	obs.na-mexico-1.myhuaweicloud.com
拉美-墨西哥二	swr.la-north-2.myhuaweicloud.com	obs.la-north-2.myhuaweicloud.com

接入步骤

步骤1 设置虚拟专用网络（VPN）方案：请参见**通过VPN连接云下数据中心与云上VPC**。

如已设置VPN网络可跳转至**在华为云侧创建VPCEP**。

说明

- 数据中心的私网网段与华为云上连接VPN使用的VPC网段不能有重叠冲突。
- 该VPC子网网段不能与IDC中已使用的网络网段重叠，否则将无法接入集群。例如，IDC中已使用的VPC子网为192.168.1.0/24，那么华为云VPC中不能使用192.168.1.0/24这个子网。

步骤2 在华为云**创建VPN网关**。

登录到华为云控制台，选择“网络控制台”，选择需要接入的IAM子项目，如“北京四（service）”，在总览页面下选择“虚拟专用网络”单击“VPN网关”，然后单击“立即创建”。

表 3-1 规划数据

类别	规划项	规划值
VPC	待互通子网	10.188.1.0/24,100.64.0.0/10（该网段是云上的SWR、OBS等服务所在网段）
VPN网关	互联子网	用于VPN网关和VPC通信，不能和VPC已有子网重叠
		10.188.2.0/24
	EIP地址	EIP地址在购买EIP时由系统自动生成，无需填写，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下：
		主EIP：11.xx.xx.11
		备EIP：11.xx.xx.12
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPSec隧道，配置时两边需要互为镜像。
		VPN连接1：169.254.70.1/30
		VPN连接2：169.254.71.1/30

步骤3 VPN创建完成后，**设置对端网关**，路由模式选择静态路由，公网IP是数据中心侧的公网IP。

步骤4 **创建VPN连接**。

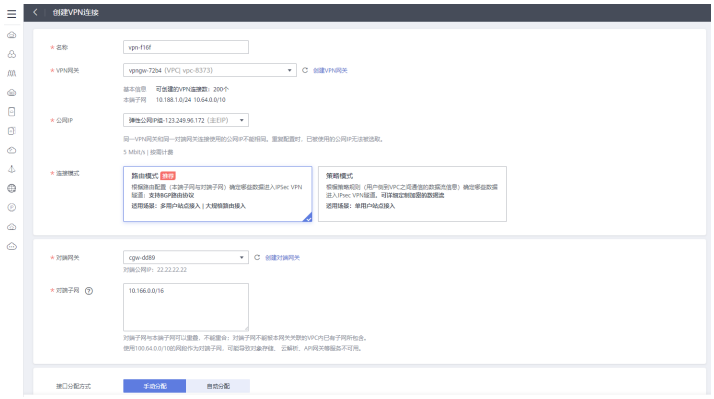


表 3-2 VPN 连接参数说明

参数	说明	参数取值
公网IP	选择VPN网关的主EIP。	11.xx.xx.11
连接模式	选择“路由模式”。	路由模式
对端子网	输入数据中心待和VPC互通的子网。	10.166.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端接口地址	配置VPN网关的Tunnel隧道IP地址。 **说明** 对端网关需要对此处的本端接口地址/对端接口地址做镜像配置。	169.254.70.2/30
对端接口地址	配置对端网关的Tunnel隧道IP地址。	169.254.70.1/30
路由模式	选择“静态路由”。	静态路由
预共享密钥、确认密钥	VPN连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	VPN连接和对端网关配置的策略信息需要一致。	默认配置

步骤5 **配置对端网关设备**。

步骤6 验证网络互通情况：

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“服务列表”，选择“计算 > 弹性云服务器”。
4. 登录弹性云服务器。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

   本示例是通过管理控制台远程登录（VNC方式）。
5. 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

   ping 172.16.0.100

   其中，172.16.0.100为数据中心服务器的IP地址，请根据实际替换。

   回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

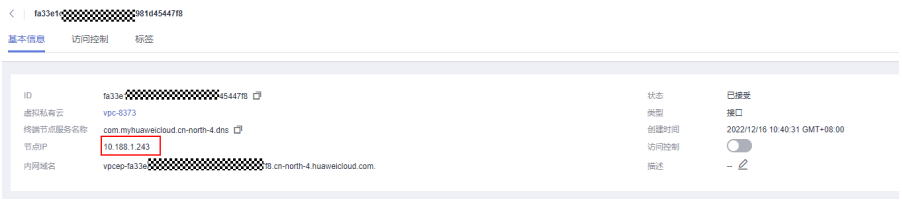
步骤7 在华为云侧创建VPCEP。

数据中心IDC访问华为云上各服务需要在与数据中心互通的VPC中创建VPCEP。需要在华为云终端节点页面分别创建DNS、SWR、OBS、UCS的终端节点：

创建DNS终端节点

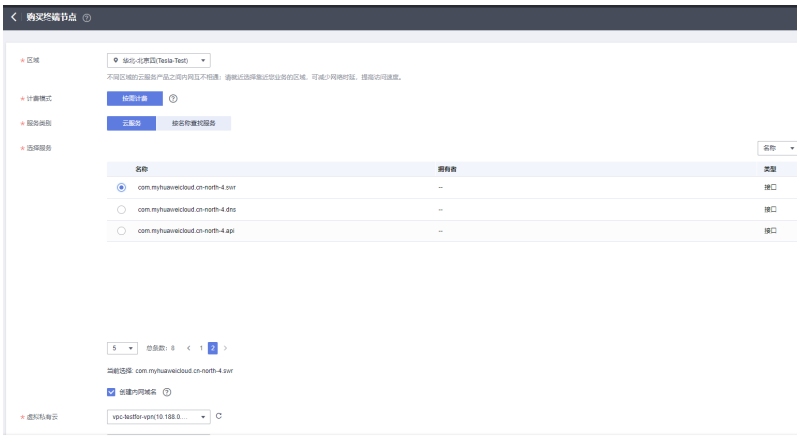
在“服务列表”中，选择“网络 > VPC终端节点”，进入终端节点页面。

1. 在左侧导航栏，选择“VPC终端节点 > 终端节点”。
2. 在终端节点界面，单击“购买终端节点”，创建连接DNS服务的终端节点。
3. 选择“云服务 > com.myhuaweicloud.cn-north-4.dns”。
4. 虚拟私有云选择**步骤2 在华为云创建VPN网关**中进行VPN打通的VPC。
5. 单击生成的终端节点名称详情，查看生成的IP，记录。

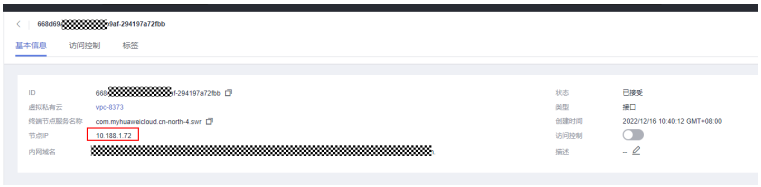


创建SWR终端节点

1. 在“服务列表”中，选择“网络 > VPC终端节点”，进入终端节点页面。
2. 在左侧导航栏，选择“VPC终端节点 > 终端节点”。
3. 在终端节点界面，单击“购买终端节点”，创建连接SWR服务的终端节点。
4. 选择“云服务 > com.myhuaweicloud.cn-north-4.swr”。
5. 虚拟私有云选择**步骤2 在华为云创建VPN网关**中进行VPN打通的VPC。

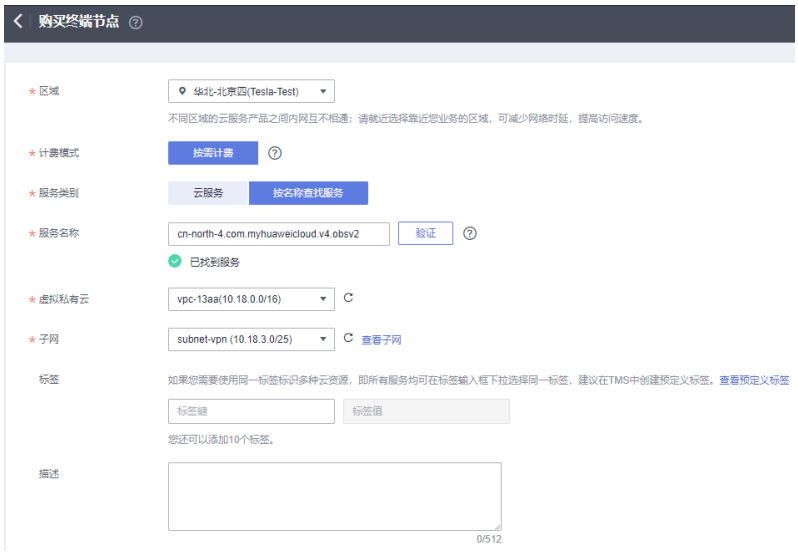


6. 单击创建出来的VPCEP节点名称，查看VPCEP的节点IP。



创建OBS终端节点

1. 在“服务列表”中，选择“网络 > VPC终端节点”，进入终端节点页面。
2. 在左侧导航栏，选择“VPC终端节点 > 终端节点”。
3. 在终端节点界面，单击“购买终端节点”，创建连接OBS服务的终端节点。
4. 选择“按名称查找服务cn-north-4.com.myhuaweicloud.v4.obsv2 >”，并单击“验证”。
5. 虚拟私有云选择**步骤2**中进行VPN打通的VPC。



创建UCS终端节点

1. 在“服务列表”中，选择“网络 > VPC终端节点”，进入终端节点页面。
2. 在左侧导航栏，选择“VPC终端节点 > 终端节点”。

3. 在终端节点界面，单击“购买终端节点”，创建连接UCS服务的终端节点。
4. 选择“按名称查找服务 > cn-north-4.open-vpcep-svc.29696ab0-1486-4f70-ab35-a3f6b1b37c02”，并单击“验证”。
5. 虚拟私有云选择**步骤2**中进行VPN打通的VPC。

步骤8 在IDC的DNS Server中增加华为云的DNS转发器。

1. 配置DNS转发器：在用户线下的DNS服务器配置相应的DNS转发规则，将解析华为云内网域名的请求转发到DNS终端节点。

   以常见的DNS软件Bind为例：/etc/named.conf内，增加DNS转发器的配置，forwarders为DNS终端节点IP地址。xx.xx.xx.xx是**步骤7**中DNS的终端节点IP。

   ```
   options
   {
     forward only;
     forwarders{ xx.xx.xx.xx;};
   }
   ```

2. 增加DNS静态配置，SWR与CIE实例地址，地址是从容器智能分析实例中获取到的。

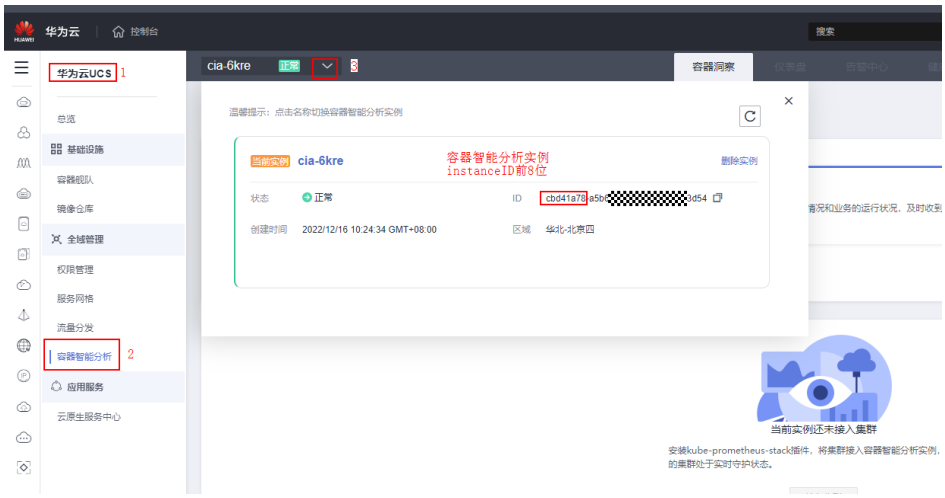
   以北京四为例，如使用dnsmasq为例，在/etc/dnsmasq.conf中添加以下两个静态解析。

   ```
   address=/swr.cn-north-4.myhuaweicloud.com/xx.xx.xx.xx
   ```

   *xx.xx.xx.xx*是**步骤7**中SWR的终端节点IP。

   address=/cie-{容器智能分析实例instanceid前八位数字}{当前选择接入的VPC子网ID前八位数字}.cn-north-4.myhuaweicloud.com

   获取容器智能分析实例instanceid前八位数字。



获取当前选择接入的VPC子网ID前八位数字

步骤9 在UCS注册IDC的kubernetes集群：准备待接入集群的KubeConfig文件，请确保待接入集群的kubeconfig文件中的server字段是私网IP（非公网IP或者域名）。登录UCS控制台，在左侧树状导航栏，选择“容器舰队”。单击本地集群选项卡中的“注册集群”按钮。根据页面提示，选择集群服务商并填写集群参数。具体请参考**安装前准备**。

在完成集群添加后，集群需要终端节点来接入网络才能被UCS接管，单击私网接入，选择在与数据中心IDC打通VPN的VPC。

说明

该VPC只有在完成中的**在华为云侧创建VPCEP**配置才可以被选中。

下载集群代理agent的配置文件，上传到数据中心的kubernetes集群内，待接入集群中执行以下命令部署代理。

```
kubectl apply -f agent.yaml
```

查看集群代理部署状态。

```
kubectl -n kube-system get pod | grep proxy-agent
```

如果部署成功，预期输出如下：

```
proxy-agent-5f7d568f6-6fc4k 1/1 Running 0 9s
```


查看集群代理运行状态。

```
kubectl -n kube-system logs<Agent Pod Name>| grep "Start serving"
```

如果正常运行，日志预期输出如下：

```
Start serving
```

前往UCS控制台刷新集群状态，集群处于“运行中”。

步骤10 将在UCS下创建的待接入数据中心的kubernetes集群接入到容器智能分析服务。

1. 容器智能分析接入集群：登录UCS控制台，在左侧导航栏中单击“容器智能分析”。选择容器智能分析实例，并单击右上角“接入集群”。选择一个数据中心内的待接入附着集群，单击“下一步：接入配置”。

2. 接入方式选择“私网接入”。私网接入点：“虚拟私有云”选择已经与数据中心打通VPN的VPC。

3. 完成插件配置。

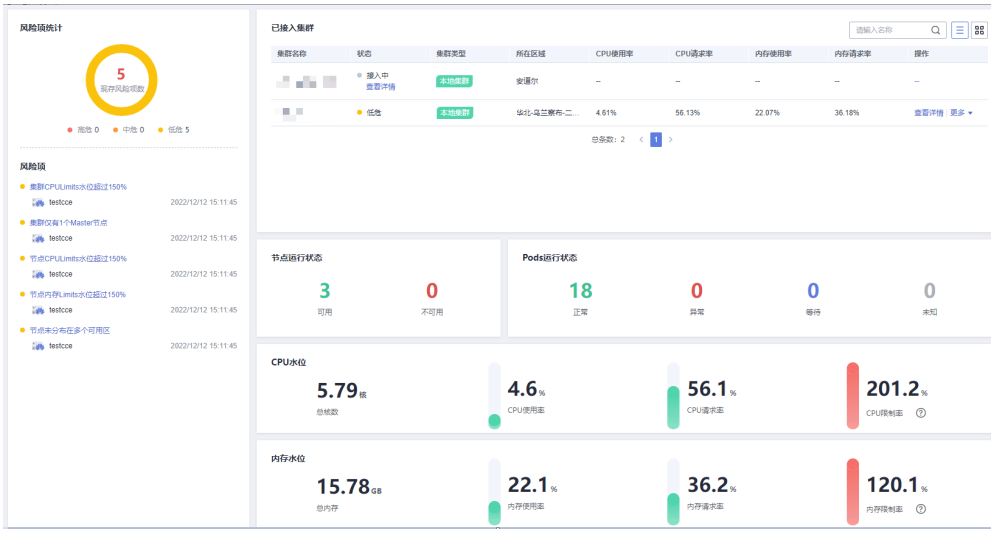
   系统提供默认的插件配置，包括插件规格、采集周期和存储，如果您想修改这些默值，请单击插件参数旁边的 ▼ 按钮，展开配置项。

   插件规格：包括演示规格（100容器以内）、不同规格对集群的CPU、内存等资源要求不同，UCS服务会对集群节点是否能够成功安装插件进行初步检测，当不满足时，会在页面给出提示。不同插件规格占用的资源配额可参考**不同规格的资源配额要求**。

   - 存储：用于普罗数据的临时存储。

- 存储类型：附着集群支持Emptydir和Local Storage两种存储类型。
- 使用Emptydir模式普罗数据将存储在Pod中，请确保prometheus-server-0调度到的节点上的容器存储挂载容量满足所输入的容量大小。
- 使用本地存储将会在您的集群内创建monitoring命名空间（如果不存在），以及local-storage类型的PV及PVC，请保证您指定的节点上存在所输入的目录以及该目录满足所输入的容量大小。
- 容量：为创建PVC时指定的容量大小或者选择Pod存储时的存储最大限制值。

等待集群接入，2-3min最终显示集群接入状态是低危/中危/高危，以及有监控数据。



----结束

3.2 本地集群工作负载获取 IAM Token

工作负载Identity允许集群中的工作负载模拟IAM用户来访问云服务，从而无需直接使用IAM帐号的 AK/SK 等信息，降低安全风险。

本文档介绍如何在UCS中使用工作负载Identity。

使用流程

使用工作负载Identity的流程如图3-1，具体流程如下：

步骤1 前置授权。

1. 在UCS**获取本地集群私钥签发的jwks**，该公钥用于验证集群签发的ServiceAccount Token。
2. 在 IAM **配置身份供应商**，标志当前集群在IAM侧的身份。
3. 为身份提供商配置集群签发的公钥，后续负载使用Token发送请求时，IAM使用该公钥验证Token。
4. 添加 ServiceAccount 与 IAM 账号的映射规则，配置后，当前 ServiceAccount 拥有对应用户的 IAM 权限。

步骤2 工作负载配置Token。

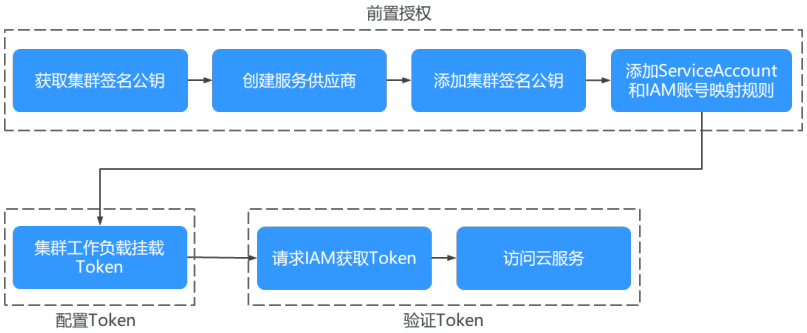
1. 部署应用并配置ServiceAccount。
2. 挂载对应ServiceAccount的Token。

步骤3 验证获取的Token能否正常进行访问。

1. 访问IAM接口获取IAM Token。
2. 使用IAMToken 访问云服务。

----结束

图 3-1 使用工作负载 Identity 流程



获取本地集群私钥签发的 jwks

步骤1 使用kubectl连接本地集群。

步骤2 执行如下命令获取公钥。

```
kubectl get --raw /openid/v1/jwks
```

返回结果为一个 json 字符串，是当前集群的签名公钥，用于访问身份提供商。

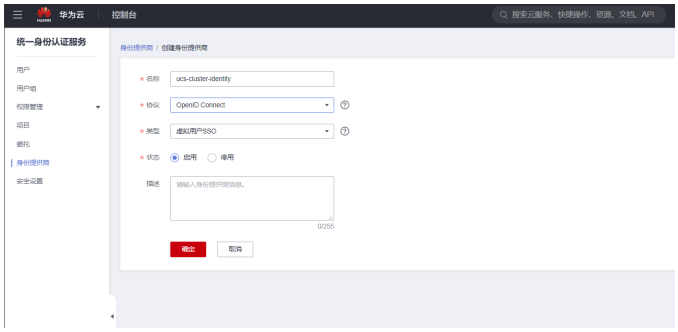
```
{
   "keys": [
      {
         "kty": "RSA",
         "e": "AQAB",
         "use": "sig",
         "kid": "Ew29q....",
         "alg": "RS256",
         "n": "peJdm...."
      }
   ]
}
```

----结束

配置身份提供商

步骤1 登录IAM控制台，创建身份提供商，协议选择OpenID Connect。

图 3-2 创建身份提供商



步骤2 单击“确定”，然后修改身份提供商信息，需要修改的信息如表3-3。若需要创建身份转换规则，单击“创建规则”进行创建。

图 3-3 修改身份提供商信息

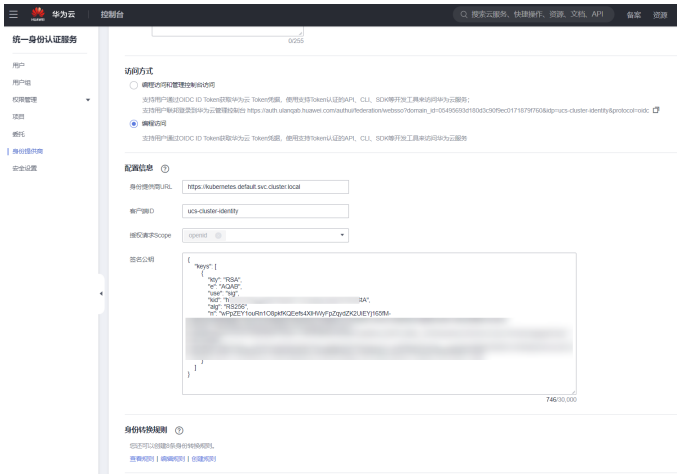


图 3-4 创建身份转换规则

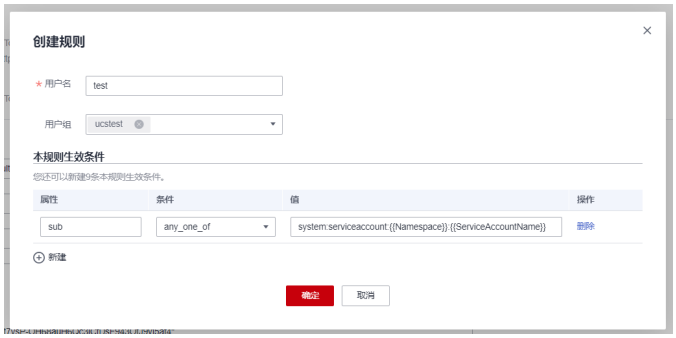


表 3-3 身份提供商配置参数说明

参数	说明
访问方式	选择“编程访问”
配置信息	• 身份提供商 URL：https://kubernetes.default.svc.cluster.local 。 • 客户端 ID：ucs-cluster-identity。 • 签名公钥：本地集群的jwks，获取方法请参见**获取本地集群私钥签发的jwks**。
身份转换规则	身份映射规则是将工作负载的 ServiceAccount 和 IAM 用户组做映射。 例如：在集群default命名空间下创建一个名为 XXX 的 ServiceAccount，映射到 demo 用户组（后续使用身份提供商 ID 访问云服务就具有 demo 用户组的权限）。 值的格式为：system:serviceaccount:*Namespace*:*ServiceAccountName*

步骤3 单击“确定”。

----结束

获取 IAM Token

步骤1 创建 ServiceAccount，此处 ServiceAccount 的名称需要与**步骤2**时填写的 ServiceAccountName 保持一致。

```
apiVersion: v1
kind: ServiceAccount
metadata:
 name: test_sa_name # 与配置身份转换规则处保持一致
```

步骤2 如下所示，在工作负载中新增 ServiceAccount 以及 Volume 相关配置。

```
apiVersion: apps/v1
kind: Deployment
```



```
metadata:
  name: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
      version: v1
  template:
    metadata:
      labels:
        app: nginx
        version: v1
    spec:
      containers:
      - name: container-1
        image: nginx:latest
        volumeMounts
        - mountPath: "/var/run/secrets/tokens" # 将Kubernetes生成的ServiceAccountToken 挂载到 /var/run/
secrets/tokens/token_path 文件内
          name: token-volume
      imagePullSecrets:
      - name: default-secret
      serviceAccountName: test_sa_name   # 上一步创建的ServiceAccount的名称
      volumes:
      - name: token-volume
        projected:
          defaultMode: 420
          sources:
          - serviceAccountToken:
              audience: ucs-cluster-identity   # 此处取值必须为身份提供商的客户端ID
              expirationSeconds: 7200    # 过期时间
              path: token_path    # 路径名称，可自定义
```

步骤3 创建完成后，登录到容器中获取 Token。

步骤4 构造请求体数据，项目ID的获取请参见**获取项目ID**。

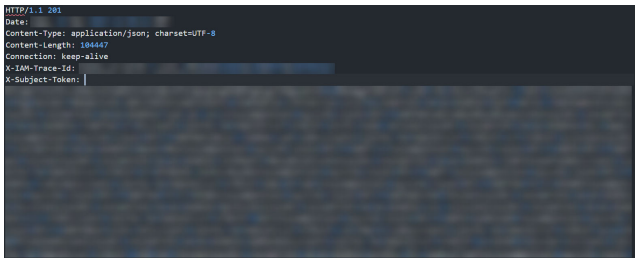
```
{
    "auth" : {
      "id_token" : {
        "id" : "eyJhbGciOiJSUzIXXXXX"   // 上一步获得的 token 内容
      },
      "scope": {
        "project" : {
          "id" : "05495693df80d3c92fa1c01795c2be02", // 项目 ID
          "name" : "cn-north-7"
        }
      }
    }
}
```

步骤5 请求IAM接口以获取IAM Token，IAM的Endpoint信息请参见**地区和终端节点**。

```
curl -i --location --request POST 'https://{{iam endpoint}}/v3.0/OS-AUTH/id-token/tokens'  --header 'X-Idp-
Id: {{workload_identity}}'  --header 'Content-Type: application/json'  --data @token_body.json
```

- workload_identity为**步骤1**中注册的身份提供商名称，此示例内为 ucs-cluster-identity。
- token_body.json 为构造的请求体数据文件。

步骤6 返回体内获取IAM Token，响应消息头中 X-Subject-Token 字段即为 IAM Token。



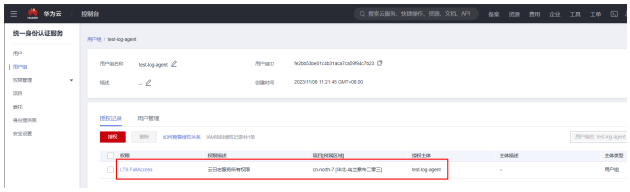
----结束

使用 IAM Token 访问云服务

本小节以请求LTS服务为例，介绍如何使用IAM Token访问云服务。

步骤1 在使用IAM Token访问云服务前，应为用户组配置相应服务的权限。

步骤2 请求LTS服务需要在用户组中加上 LTS FullAccess 权限，如图所示

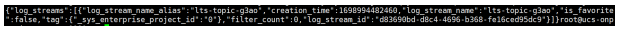


步骤3 执行如下命令，调用对应服务接口。

```
curl --location --request GET 'https://ltsperform.cn-north-7.myhuaweicloud.com/v2/{{项目 ID}}/groups/{{日志组 ID}}/streams' \--header 'Content-Type: application/json;charset=utf-8' \--header 'X-Auth-Token: {{上一步获得的 IAM token}}' \--data-raw ''
```

日志组ID可在LTS服务内进行查询。

期望的返回结果如图所示



----结束

4 服务网格

4.1 第三方注册中心接入能力

ASM提供了服务网格对接Nacos注册中心功能，便于将Nacos上的微服务同步到网格中，实现流量治理等功能。

操作步骤

步骤1 通过**使用kubectl连接网格控制面**获取kubeconofig的证书内容。

步骤2 登录云容器引擎控制面，单击选择任意集群，进入详情页。

说明

建议选择网格对应的VPC下的集群。若连接其他VPC下的集群，则需要参考**UCS服务网格 集群连通方法**打通集群所在VPC和网格对应VPC。

步骤3 在左侧导航栏，单击“配置项与密钥”，单击“密钥”页签，显示集群的密钥信息。

步骤4 选择“命名空间”为“asm-system”，单击右上角“创建密钥”。

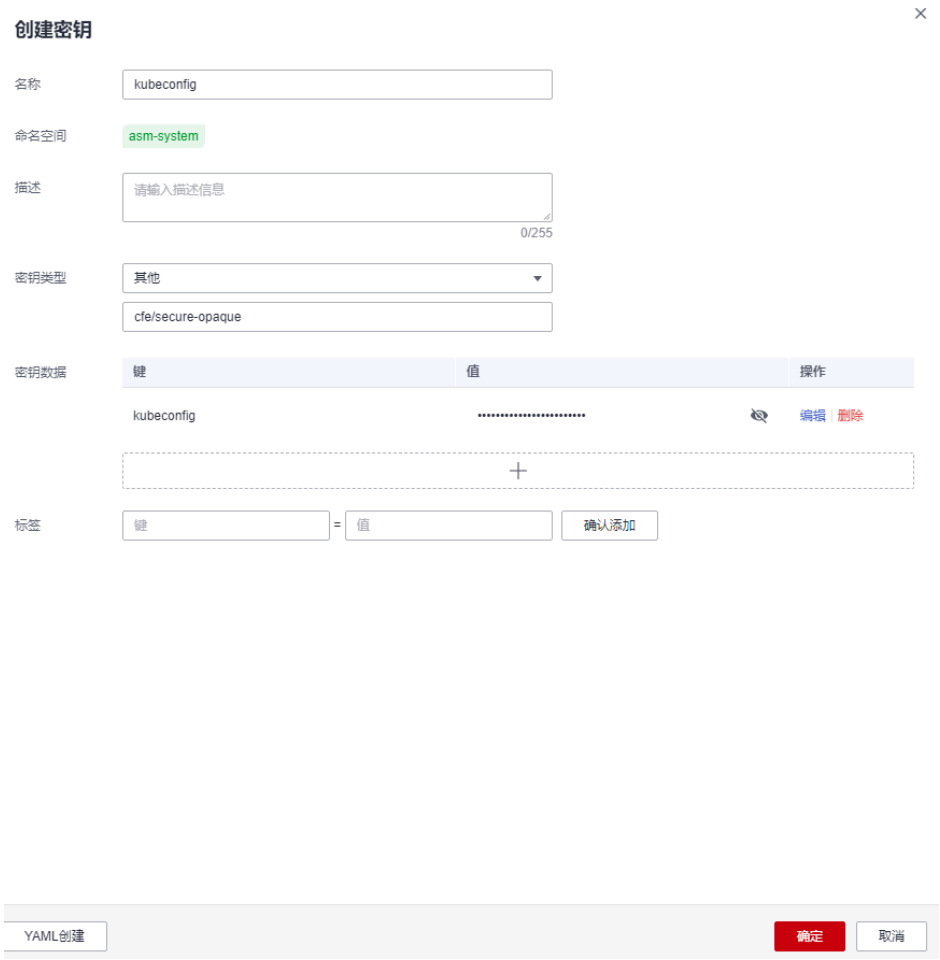
步骤5 设置密钥参数，单击右下角“创建密钥”，完成密钥创建。

- 名称：自定义名称。例如：kubeconfig。

注意

创建的密钥的名称不要使用mesh-kubeconfig，因为apiserver也会自动创建这个名字的密钥，如果使用了这个名称可能会被覆盖。

- 描述：（可选）。
- 密钥类型：选择“其他”，填写密钥类型为“cfe/secure-opaque”。
- 密钥数据：添加密钥数据，键为“kubeconfig”，值为**步骤1**中获取到的kubeconfig证书内容。



步骤6 单击左侧导航栏“插件与模板”，在“可安装插件”页签中找到“asm-service-controller”插件，单击“安装”。

步骤7 填写配置参数，单击右下角“安装”，完成插件安装。

- meshKubeconfigSecret：为步骤**步骤5**中创建的密钥名称。
- source：目前包含“nacos”，代表对接的第三方注册中心nacos的相关信息，其中包含4个参数。
  - name：为该注册中心名称。
  - addr：为nacos的ip及端口。
  - allnamespaces：为是否需要同步nacos全部命名空间中的服务，当allnamespaces为false时，需要填充namespaces，表示需要同步的nacos的命名空间。
  - namespaces：表示需要同步的nacos的命名空间。

⚠ 注意

若插件运行的集群为CCE turbo类型集群，在安装插件完成后，需要参考**为Pod配置EIP**为asm-system命名空间下，名为asm-service-controller的pod绑定eip，才能正常使用该插件功能。

----结束

4.2 UCS 服务网格 集群连通方法

4.2.1 同 region 集群打通方法

以两个北京四集群为例，网格控制面也位于北京四，两个集群在不同的VPC中，需要使用VPC对等连接打通网络以使用网格功能。

网段约束

1. 各集群所在的VPC网段不能冲突。
2. 各集群所设置的容器网段不能冲突。
3. CCE网络插件实现会在路由表中添加路由，为了防止路由冲突造成网络无法联通，集群的VPC网段不能与其他集群的容器网段冲突。

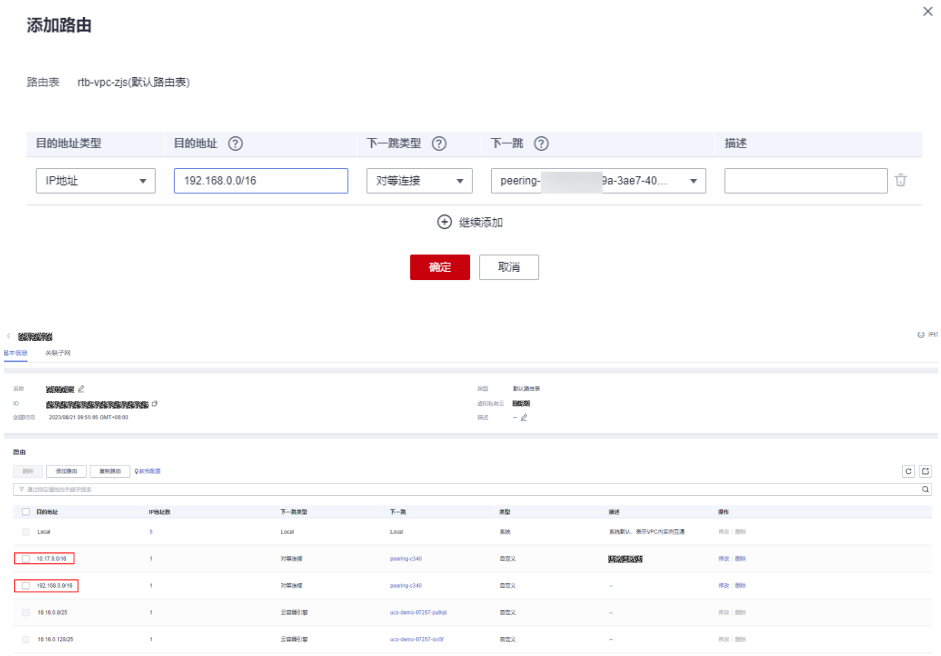
操作步骤

步骤1 登录虚拟私有云控制台，单击“虚拟私有云>对等连接”，单击右上角“创建对等连接”。

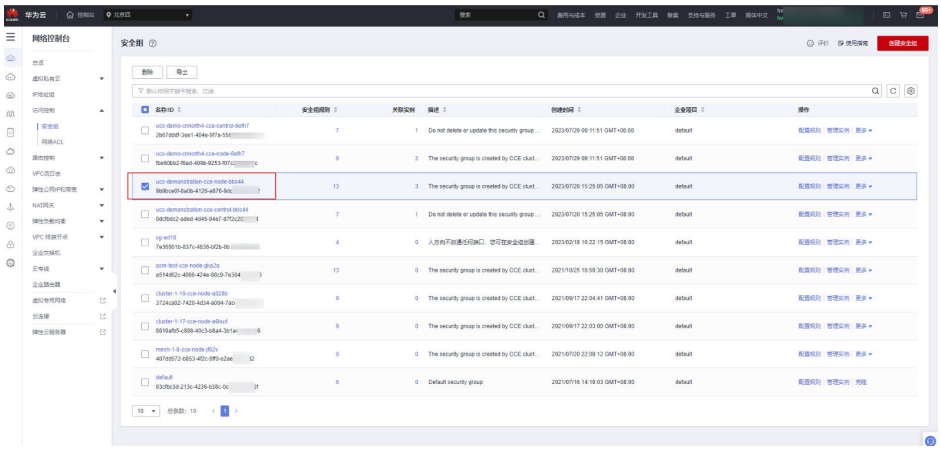
步骤2 填写参数，选择需要打通的两个VPC，单击“确定”，创建对等连接。

步骤3 在弹出的提示信息中，单击“立即添加”，根据VPC对等连接提示在路由表中添加路由。

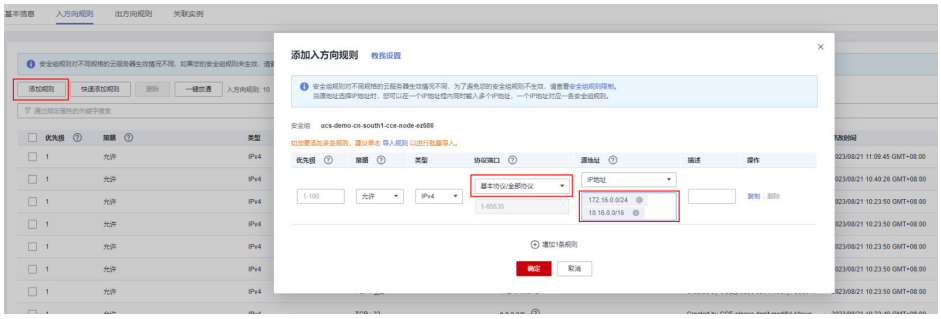
步骤4 单击“添加路由”，目的地址为对端VPC网段路由，下一跳类型为对等连接，下一跳为2创建的对等连接，单击“继续添加”，目的地址为对端集群网段路由，下一跳类型为对等连接，下一跳为2创建的对等连接，单击“确定”，完成路由表配置。需要在对端VPC路由表中做相同的操作。



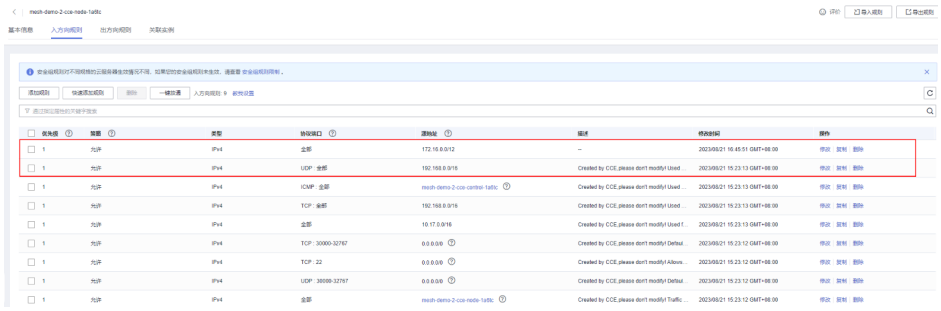
步骤5 登录虚拟私有云控制台，单击“虚拟私有云>访问控制>安全组”，选择 {集群名}-cce-node-xxx 的安全组，单击安全组名称，查看安全组详情。



步骤6 单击“入方向规则”，单击“添加规则”，填写“协议端口”和“IP地址”信息，单击“确定”。放通来自另一个VPC网段以及对应集群的容器网段的请求。（在对端VPC安全组做同样的操作）



步骤7 查看添加的安全组规则。



----结束

4.2.2 跨 region 集群打通方法

以北京四、广州region为例，进行跨region集群引入网格，其中北京四为网格控制面所在region。

网段约束

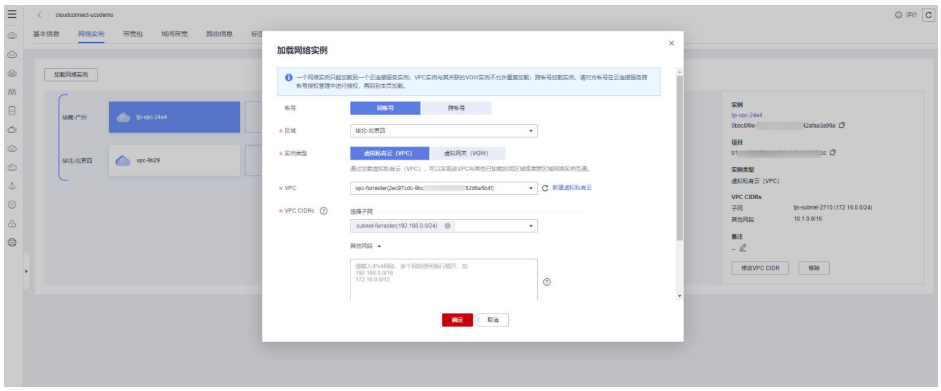
1. 各集群所在的VPC网段不能冲突。
2. 各集群所设置的容器网段不能冲突。
3. CCE网络插件实现会在路由表中添加路由，为了防止路由冲突造成网络无法联通，集群的VPC网段不能与其他集群的容器网段冲突。

操作步骤

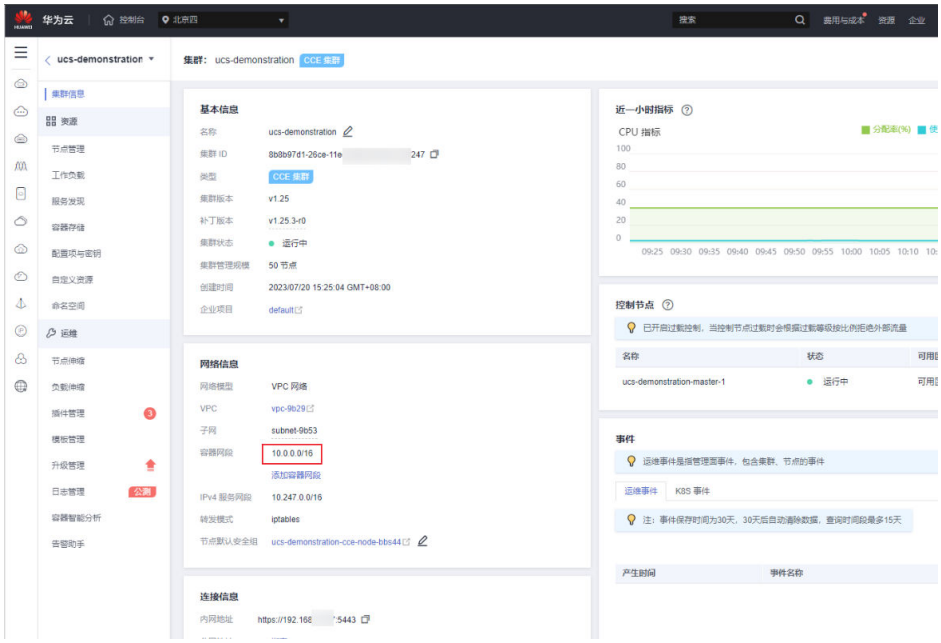
步骤1 登录云连接CC控制台，单击右侧“创建云连接”按钮。

步骤2 弹出创建云连接界面，填写参数信息，单击“确定”，完成创建。

步骤3 单击**步骤2**中创建的云连接，在弹出的页签中，单击“网络实例>加载网络实例”，选择对应region及VPC，并展开其他网段，填写对应region集群的容器网段。

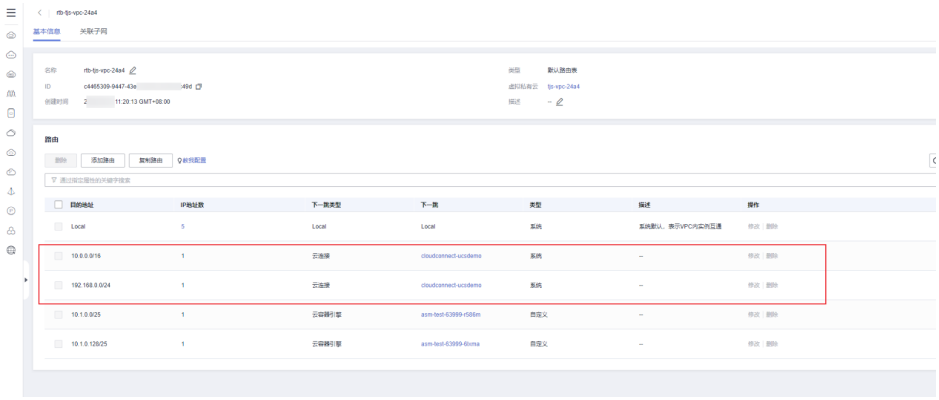


步骤4 登录云容器引擎控制面，单击目标集群>集群信息>网络信息>容器网段，获取到容器网段。

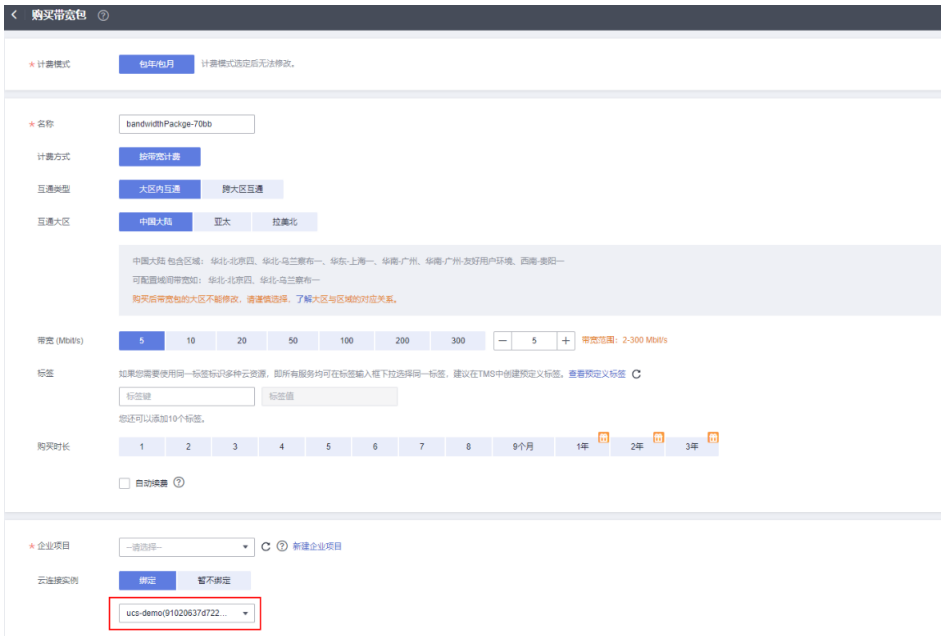


步骤5 所有需要通过云连接打通的集群，其VPC都需要接入到云连接中，查看VPC接入生效的方法如下：

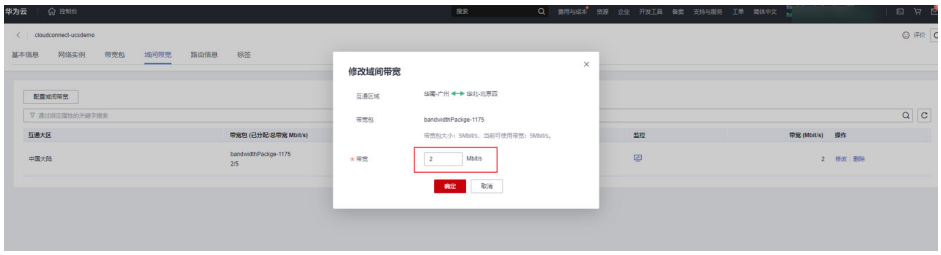
- 登录虚拟私有云控制台，单击“虚拟私有云>路由表>对应VPC实例>基本信息”，云连接会在VPC中添加两条路由。



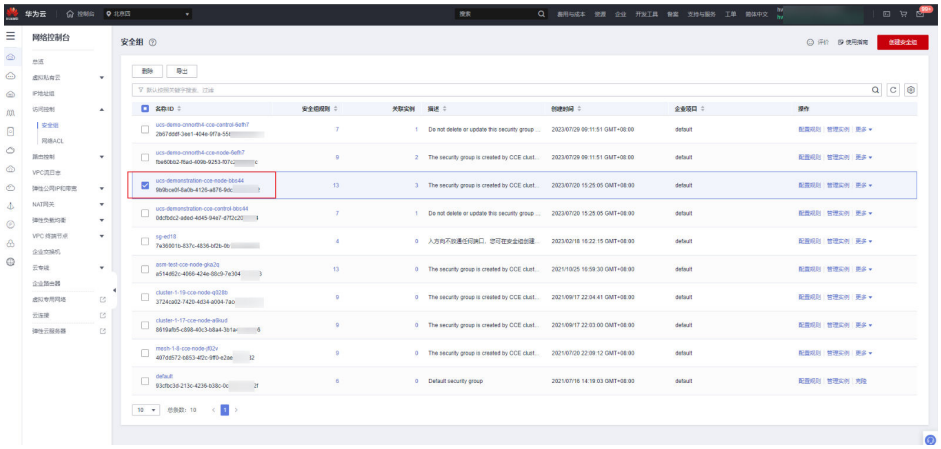
步骤6 单击**步骤2**中创建的云连接，在弹出的页签中单击“带宽包>购买带宽包”，根据实际情况进行配置，注意将带宽包绑定之前创建的云连接实例。



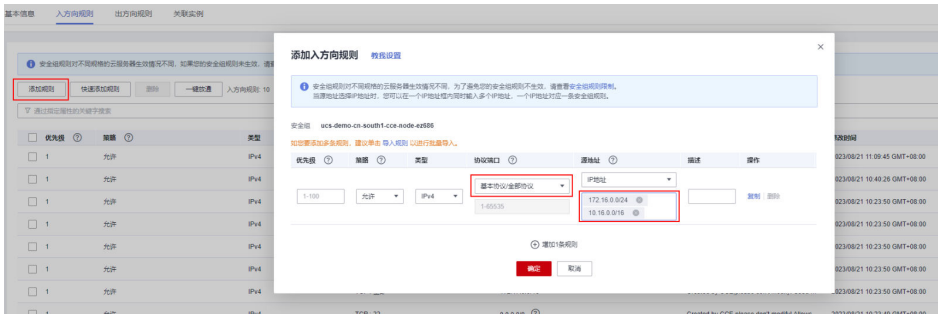
步骤7 单击**步骤2**中创建的云连接，在弹出的页签中单击“域间带宽”，根据使用情况，在region之间分配域间带宽。



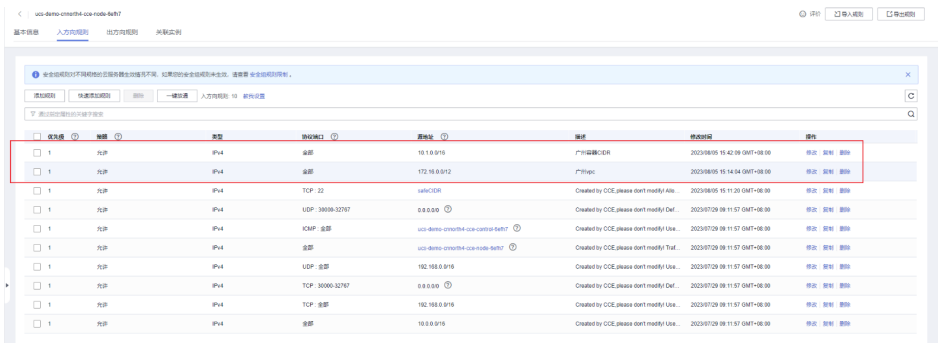
步骤8 登录虚拟私有云控制台，单击“虚拟私有云>访问控制>安全组”，选择 {集群名}-cce-node-xxx 的安全组，单击安全组名称，查看安全组详情。



步骤9 单击“入方向规则”，单击“添加规则”，填写“协议端口”和“IP地址”信息，单击“确定”。用于放通其他region连接控制面istiod与控制面kubeapiserver的请求。例如：在北京四VPC放通广州VPC与容器网段（相同操作**步骤8**-**步骤9**也需要在广州执行）。



步骤10 查看添加的安全组规则。

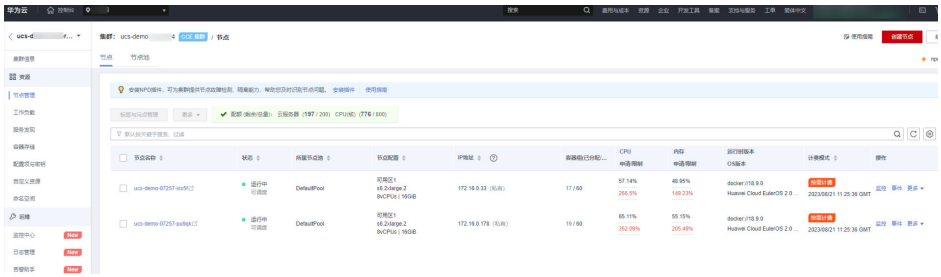


----结束

4.2.3 如何确认集群连通

VPC 网段之间的网络连通

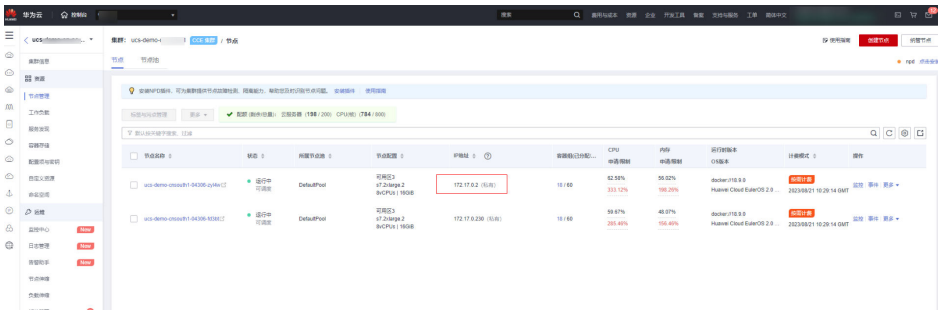
步骤1 登录云容器引擎控制台，选择本端集群，进入集群详情页，单击左侧导航栏“节点管理”，进入节点详情页。



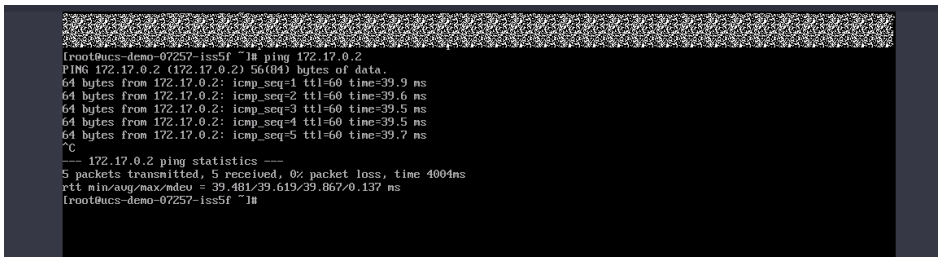
步骤2 单击“节点名称”下的节点，在弹出的页面中单击右上角“远程登录”，选择VNC方式登录。

步骤3 根据界面提示，输入账号和密码，成功进入Linux环境中。

步骤4 在云容器引擎控制台中，选择对端集群，进入集群详情页，单击左侧导航栏“节点管理”，进入节点详情页。



步骤5 在**步骤3**中，使用Linux命令查看网络是否连通。对端集群节点IP为**步骤4**中的节点IP。例如：ping 172.17.0.2。

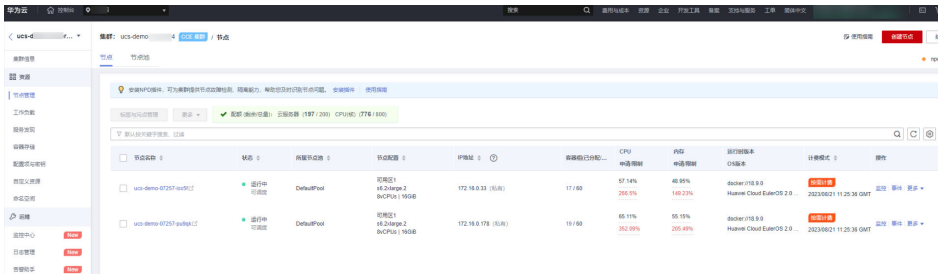


步骤6 在对端集群中执行相同的操作。

----结束

容器网段之间的网络连通

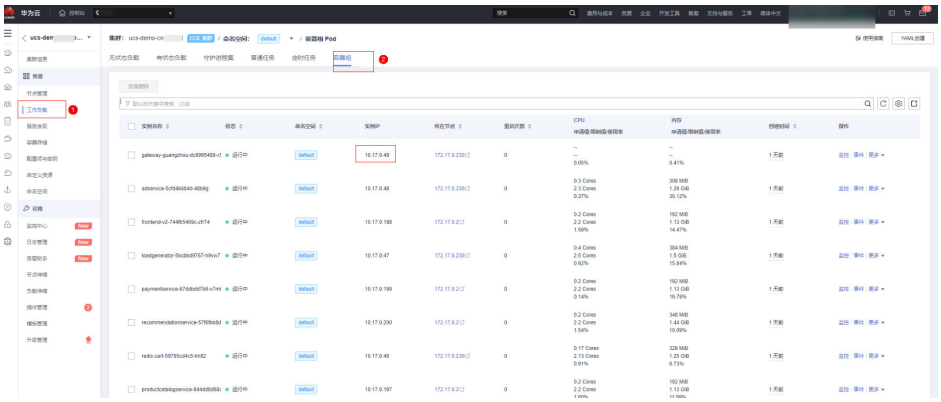
步骤1 登录云容器引擎控制台，选择本端集群，进入集群详情页，单击左侧导航栏“节点管理”，进入节点详情页。



步骤2 单击“节点名称”下的节点，在弹出的页面中单击右上角“远程登录”，选择VNC方式登录。

步骤3 根据界面提示，输入账号和密码，成功进入Linux环境中。

步骤4 在云容器引擎控制台中，选择对端集群，进入集群详情页，单击左侧导航栏“工作负载>容器组”，进入容器Pod详情页。



步骤5 在**步骤3**中，使用Linux命令查看网络是否连通。对端集群PodIP为**步骤4**中的PodIP地址。例如：ping 10.17.0.49。

```
[root@ucs-demo-07257-iss5f ~]# ping 10.17.0.49
PING 10.17.0.49 (10.17.0.49) 56(84) bytes of data.
64 bytes from 10.17.0.49: icmp_seq=1 ttl=60 time=42.7 ms
64 bytes from 10.17.0.49: icmp_seq=2 ttl=60 time=42.4 ms
64 bytes from 10.17.0.49: icmp_seq=3 ttl=60 time=42.3 ms
64 bytes from 10.17.0.49: icmp_seq=4 ttl=60 time=42.4 ms
64 bytes from 10.17.0.49: icmp_seq=5 ttl=60 time=42.4 ms
64 bytes from 10.17.0.49: icmp_seq=6 ttl=60 time=42.3 ms
64 bytes from 10.17.0.49: icmp_seq=7 ttl=60 time=42.3 ms
^C
--- 10.17.0.49 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 42.308/42.408/42.728/0.135 ms
[root@ucs-demo-07257-iss5f ~]#
```

步骤6 在对端集群中执行相同的操作。

----结束

