

分布式云原生

最佳实践

文档版本 02
发布日期 2023-03-30



版权所有 © 华为技术有限公司 2023。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

目录

1 容器舰队管理	1
1.1 IAM 用户配置权限实践.....	1
1.2 多云集群应用多活容灾.....	7
2 流量分发	14
2.1 多云集群应用故障倒换.....	14

1 容器舰队管理

1.1 IAM 用户配置权限实践

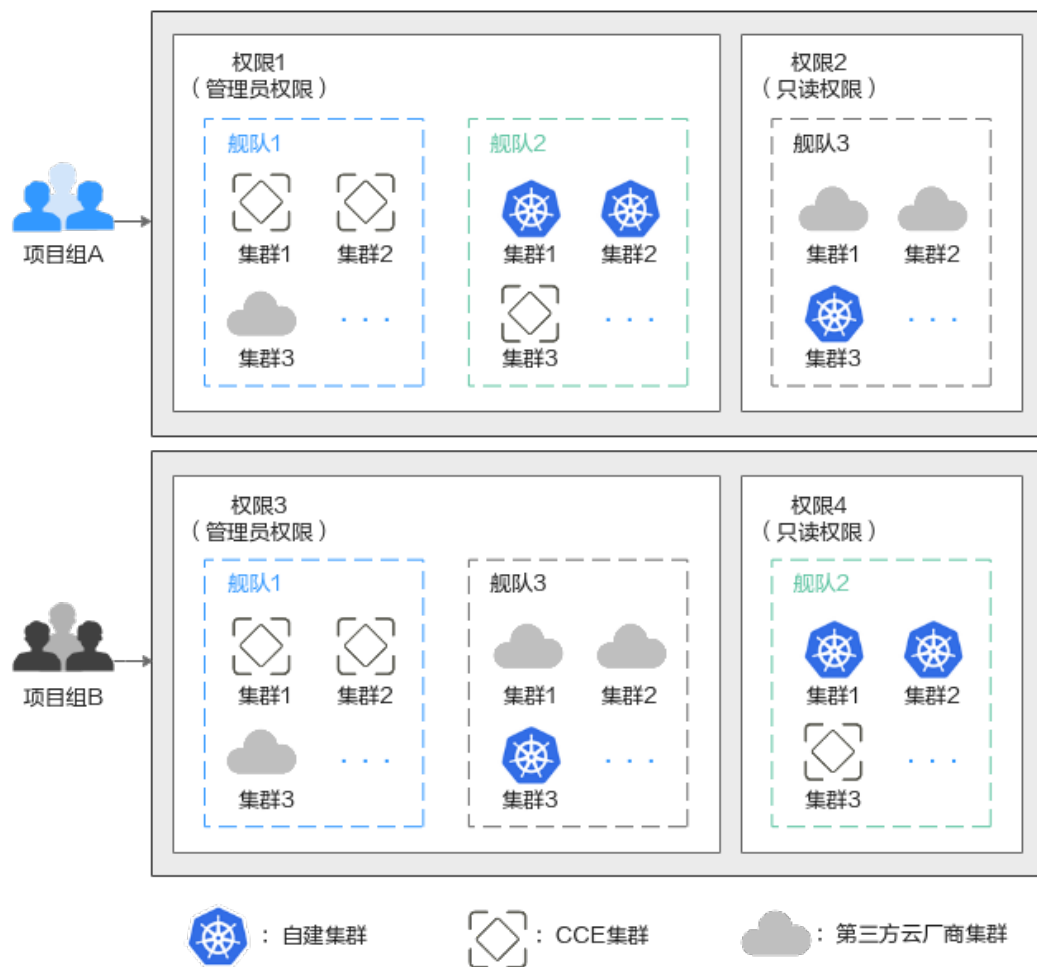
应用场景

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

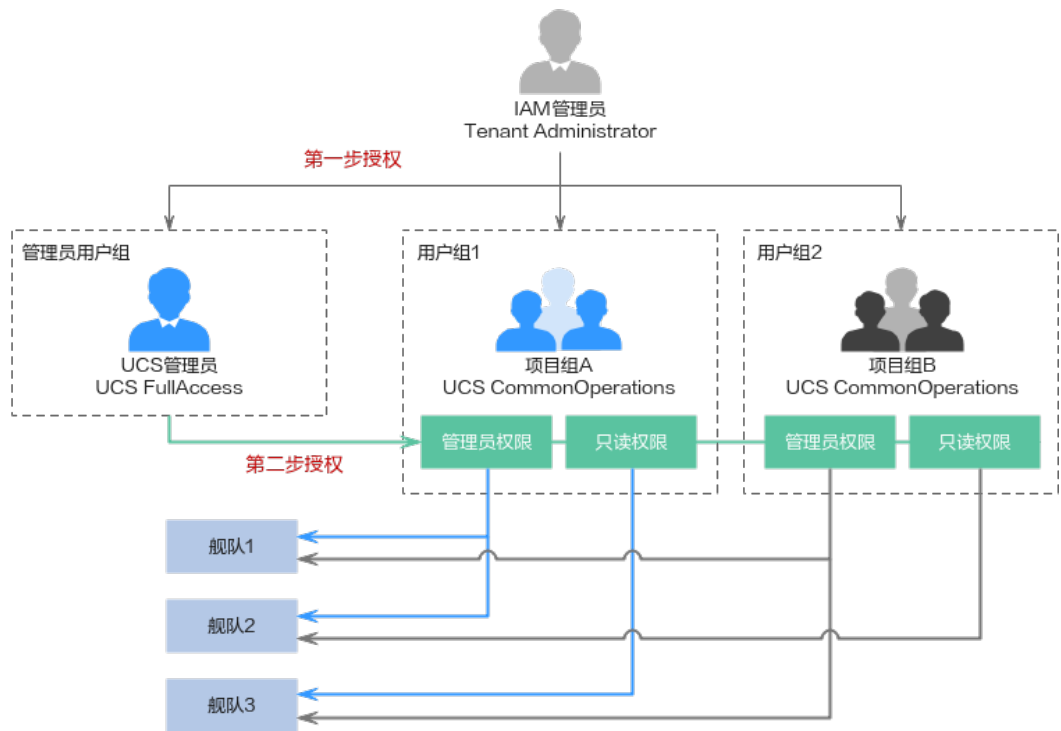
要想实现上述的权限隔离，必须结合使用IAM系统策略和UCS权限管理功能，IAM系统策略控制用户可操作哪些UCS控制台的功能，UCS权限管理控制用户可操作哪些舰队和集群资源。

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_Us er1	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_Us er1、 UCS_Group_1_Us er2 ...	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_Us er1、 UCS_Group_2_Us er2 ...	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

* 用户组名称: UCS_Group_admin

描述: UCS FullAccess

14/255

确定 取消

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

<input type="checkbox"/>	用户组名称	用户数量	描述	创建时间	操作
<input type="checkbox"/>	UCS_Group_admin	0	UCS FullAccess	2022/12/13 11:00:50 GMT+08:00	授权 编辑 用户组管理 删除

步骤5 搜索并选择权限策略UCS FullAccess。

图 1-5 选择策略

用户组UCS_Group_admin将拥有所选策略

搜索已选(1) 从其他区域项目复制权限 全部类型 华为云UCS (UCS) 请输入名称或描述

名称	类型
<input type="checkbox"/> UCS CommonOperations UCS服务基本操作权限,持有该权限的用户可以执行创建工作负载、流量分发等操作。	系统策略
<input checked="" type="checkbox"/> UCS FullAccess UCS服务管理权限,持有该权限的用户 拥有服务的所有权限(包含制定权限策略、安全策略等)。	系统策略
<input type="checkbox"/> UCS ReadOnlyAccess UCS服务只读权限(除容器智能分析只读权限)。	系统策略
<input type="checkbox"/> UCS CIAOperations UCS服务容器智能分析管理员权限。	系统策略

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。

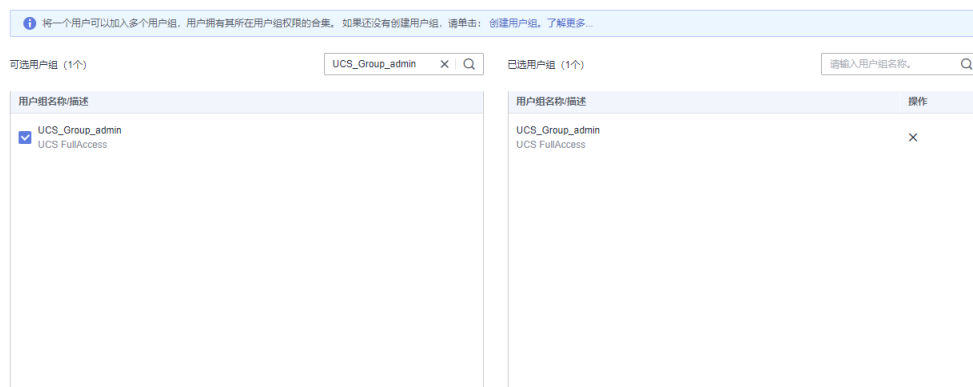
步骤7 单击“确定”完成授权。

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。

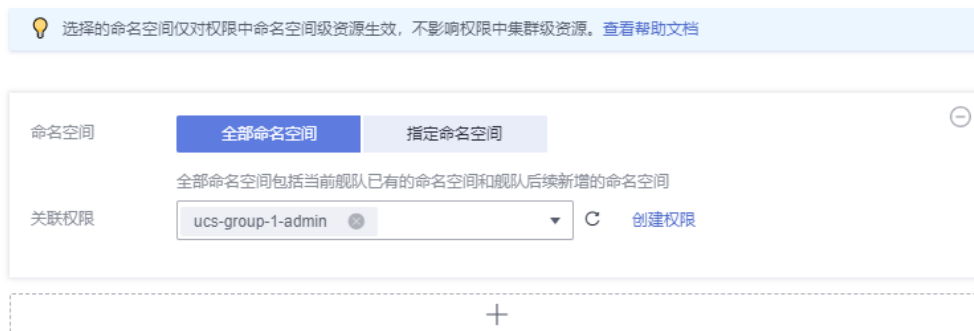
图 1-8 为舰队关联权限



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

修改权限



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

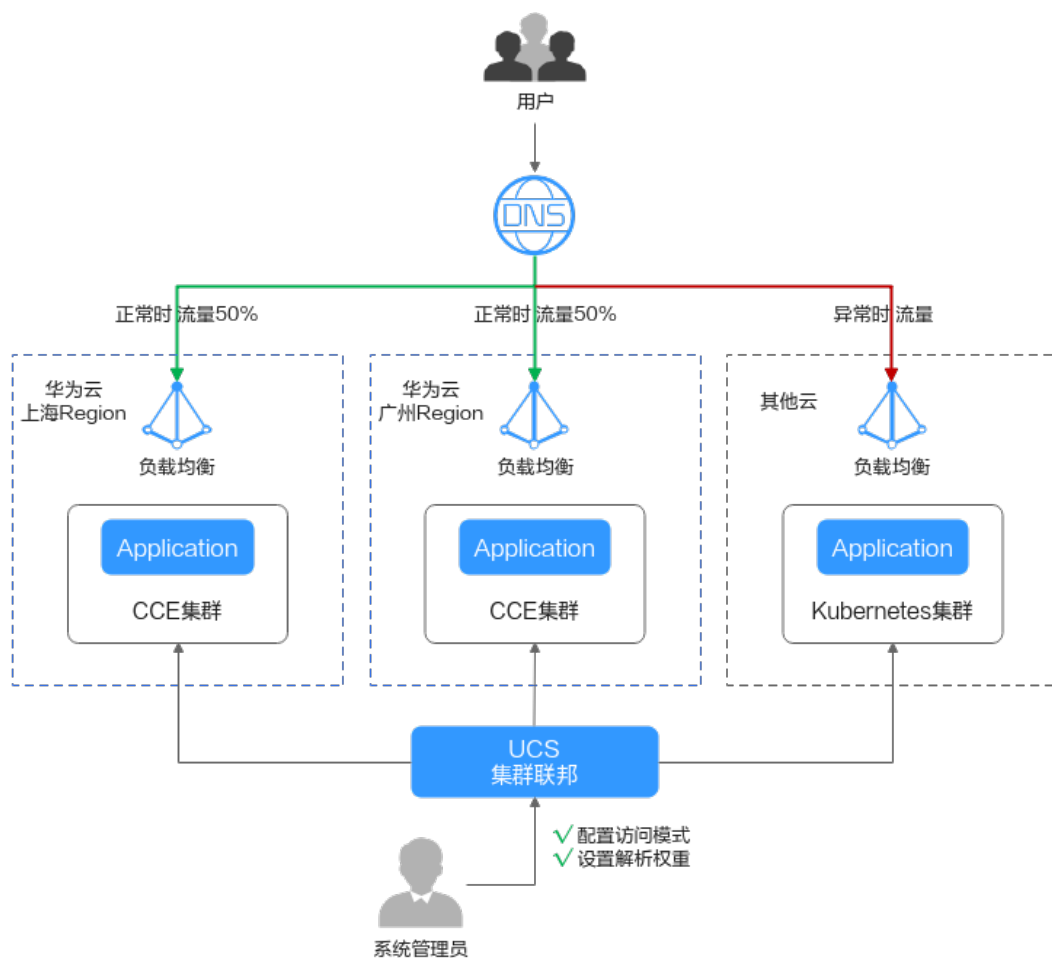
1.2 多云集群应用多活容灾

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1-10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 1-10 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）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[配置网站解析](#)。

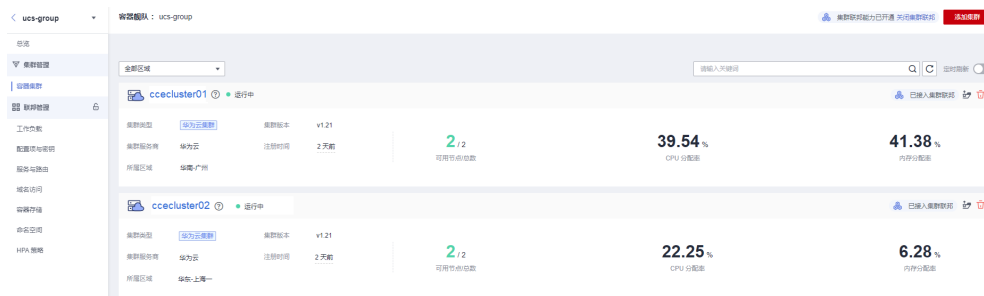
基础环境搭建

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 1-11 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。


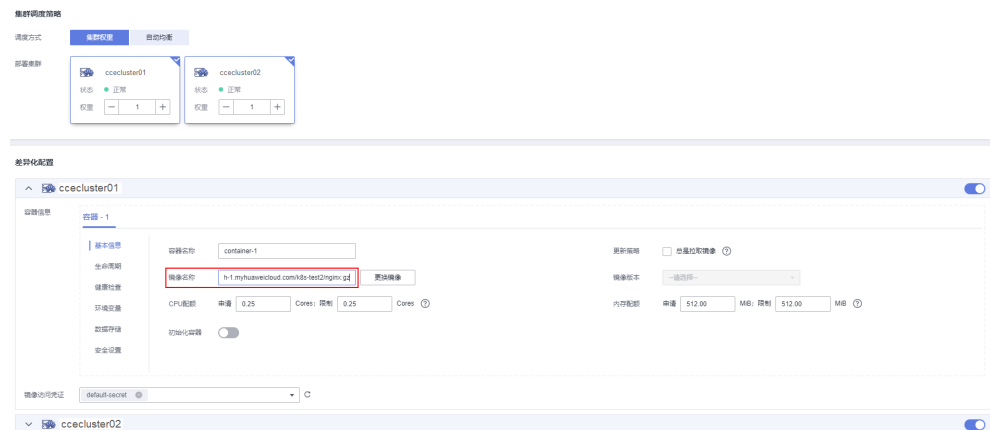
1. 登录华为云UCS控制台，选择左侧导航栏中的“容器舰队”。
2. 单击已开通集群联邦的舰队名称，进入详情页面。
3. 在左侧导航栏选择“联邦管理 > 工作负载”，单击右上角“镜像创建”。
4. 填写基本信息并配置容器参数，镜像可以任意设置，单击“下一步：调度与差异化”。
5. 设置集群调度策略，完成集群差异化配置，单击“创建工作负载”。
 - 调度方式：选择“集群权重”，并设置两个集群的权重为1:1。
 - 差异化配置：单击集群右侧的  图标开启差异化配置，设置集群ccecluster01的镜像名称为“swr.cn-south-1.myhuaweicloud.com/k8s-test2/nginx:gz”（nginx:gz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/k8s-test2/nginx:sh”。

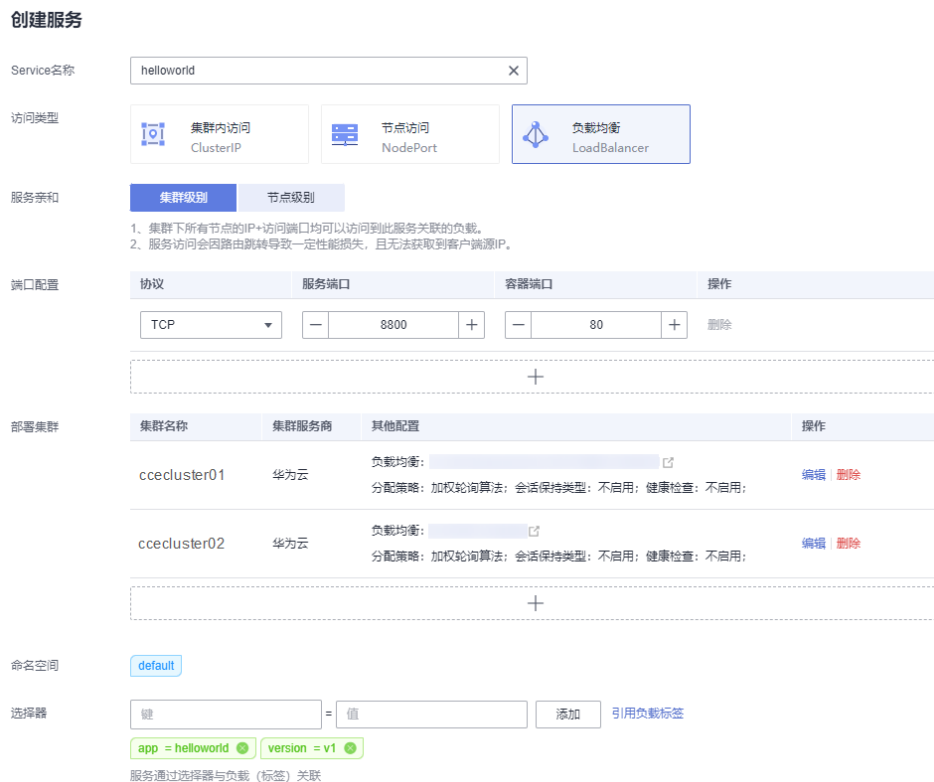
图 1-12 调度与差异化



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 1-13 创建服务



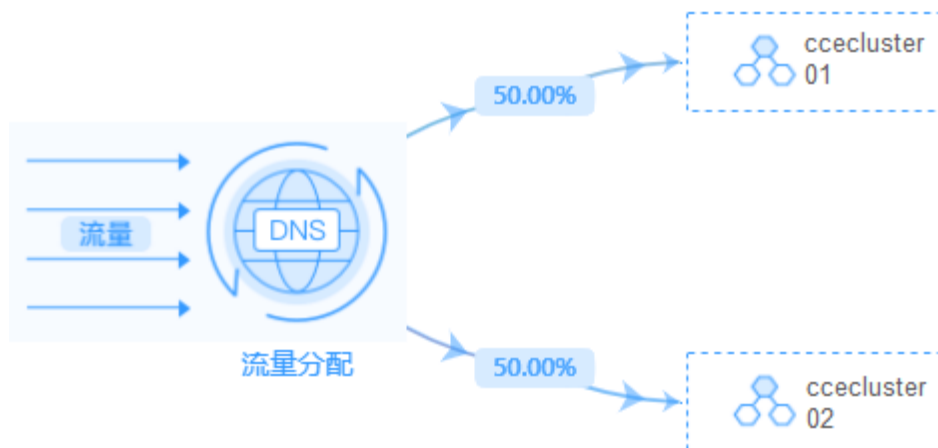
步骤5 创建域名访问。

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1-15所示。

图 1-14 配置流量配比



图 1-15 流量配比拓扑图



----结束

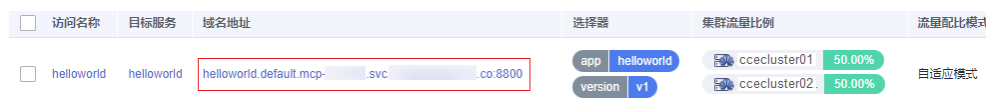
多活容灾场景验证

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 1-16 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 1-17 域名列表

访问名称	目标服务	域名地址	选择器	集群流量比例	流量配比模式	命名空间	操作
<input type="checkbox"/>	helloworld	hell...	helloworld.default.mcp-...	app: helloworld version: v1	ccecluster01: 0.00% ccecluster02: 100.00%	自适应模式	default 删除

----结束

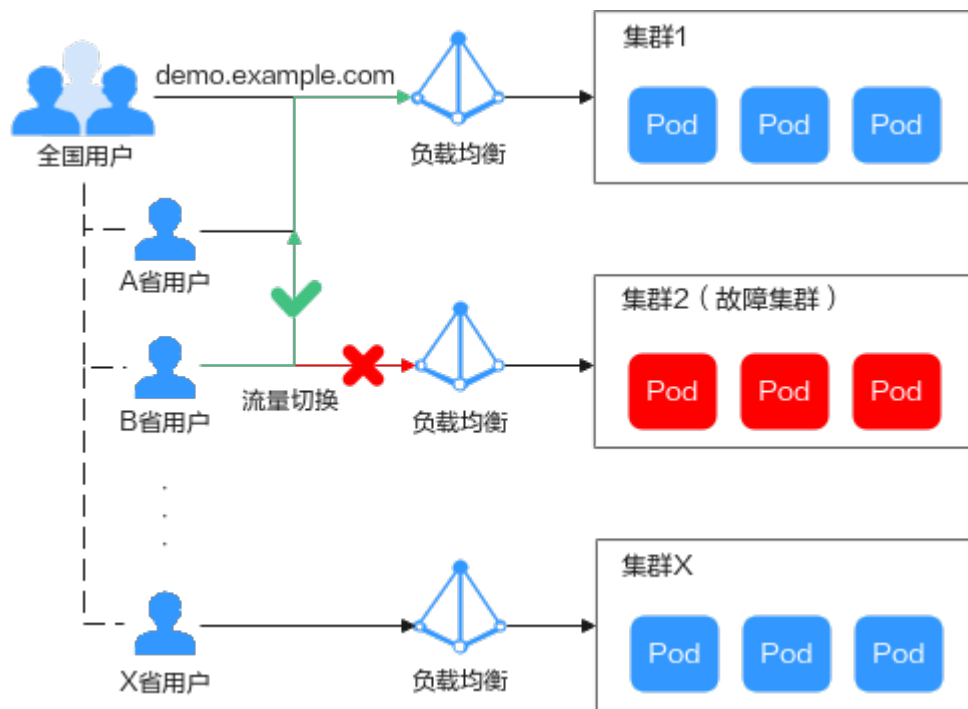
2 流量分发

2.1 多云集群应用故障倒换

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2-1所示。

图 2-1 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[配置网站解析](#)。

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 2-2 创建工作负载

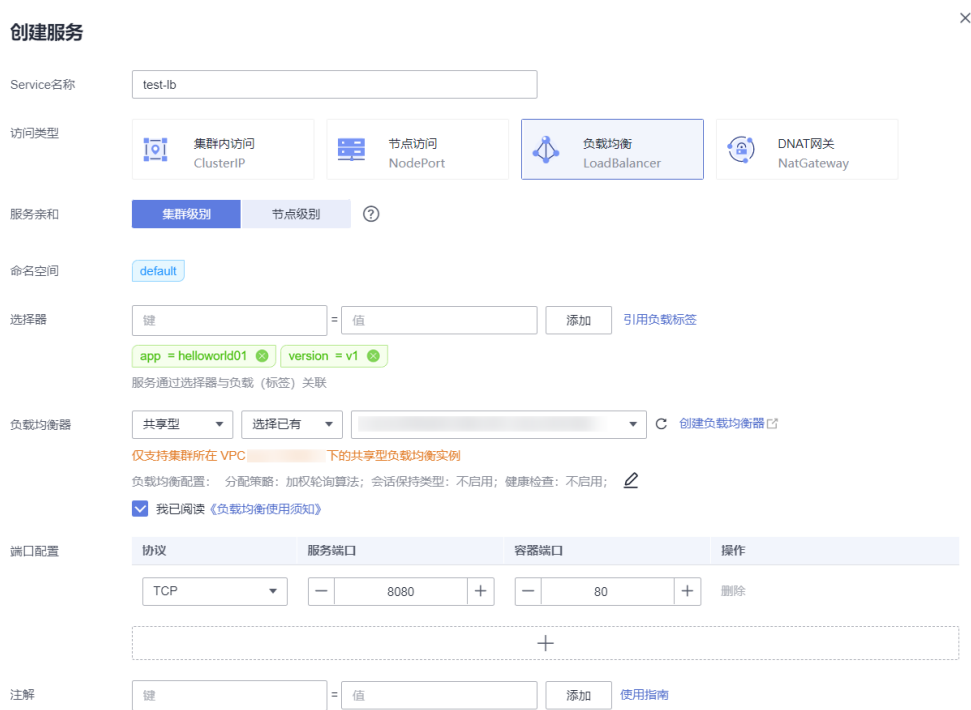


步骤3 分别为两个集群中的应用创建“负载均衡”类型的服务。

📖 说明

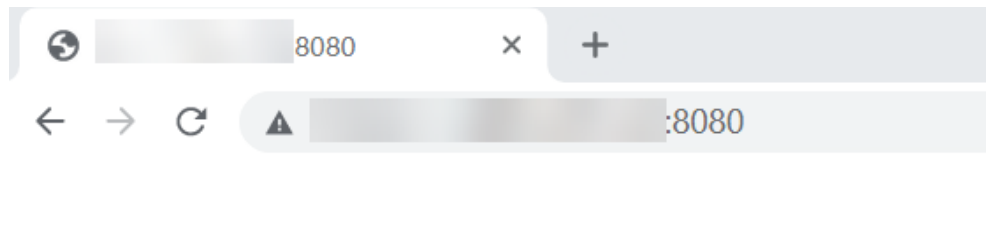
仅支持访问类型为“负载均衡”的服务，其他类型的服务将被自动过滤。

图 2-3 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 2-4 查看部署结果



```

Hello, world!
Version: 1.0.0
Hostname: helloworld01-66bdb8465-c9vbs
    
```

----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 2-5 创建流量策略

创建流量策略

域名 C

调度策略	IP	线路类型	TTL(秒)	权重	操作
+					

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-全球/亚太地区/新加坡”。
- 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 2-6 添加调度策略

添加调度策略 ×

* 集群 华为云 C

* 命名空间 C

* 服务 C

💡 仅支持访问类型为负载均衡的服务，查询结果已过滤。

* 线路类型 ?
 ?

TTL(秒) 5分钟 1小时 12小时 1天 ?

权重 ?

确定 取消

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。

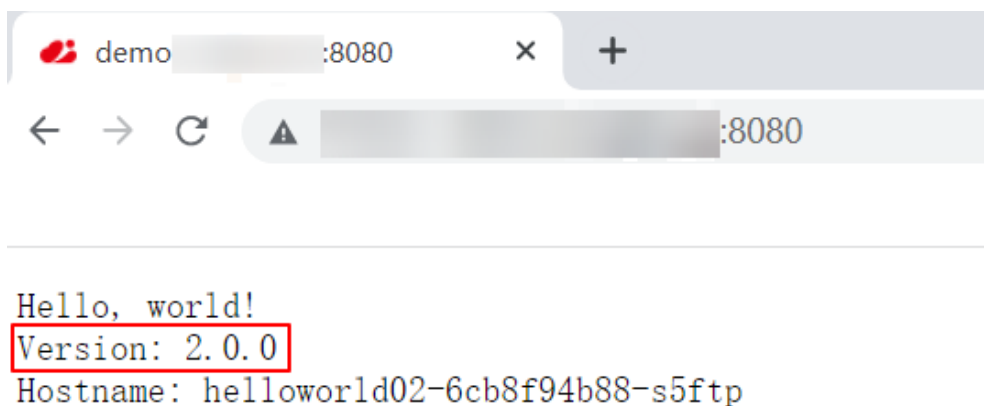
图 2-7 调度策略列表



- 新加坡地区用户：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 2-8 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 2-9 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 2-10 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