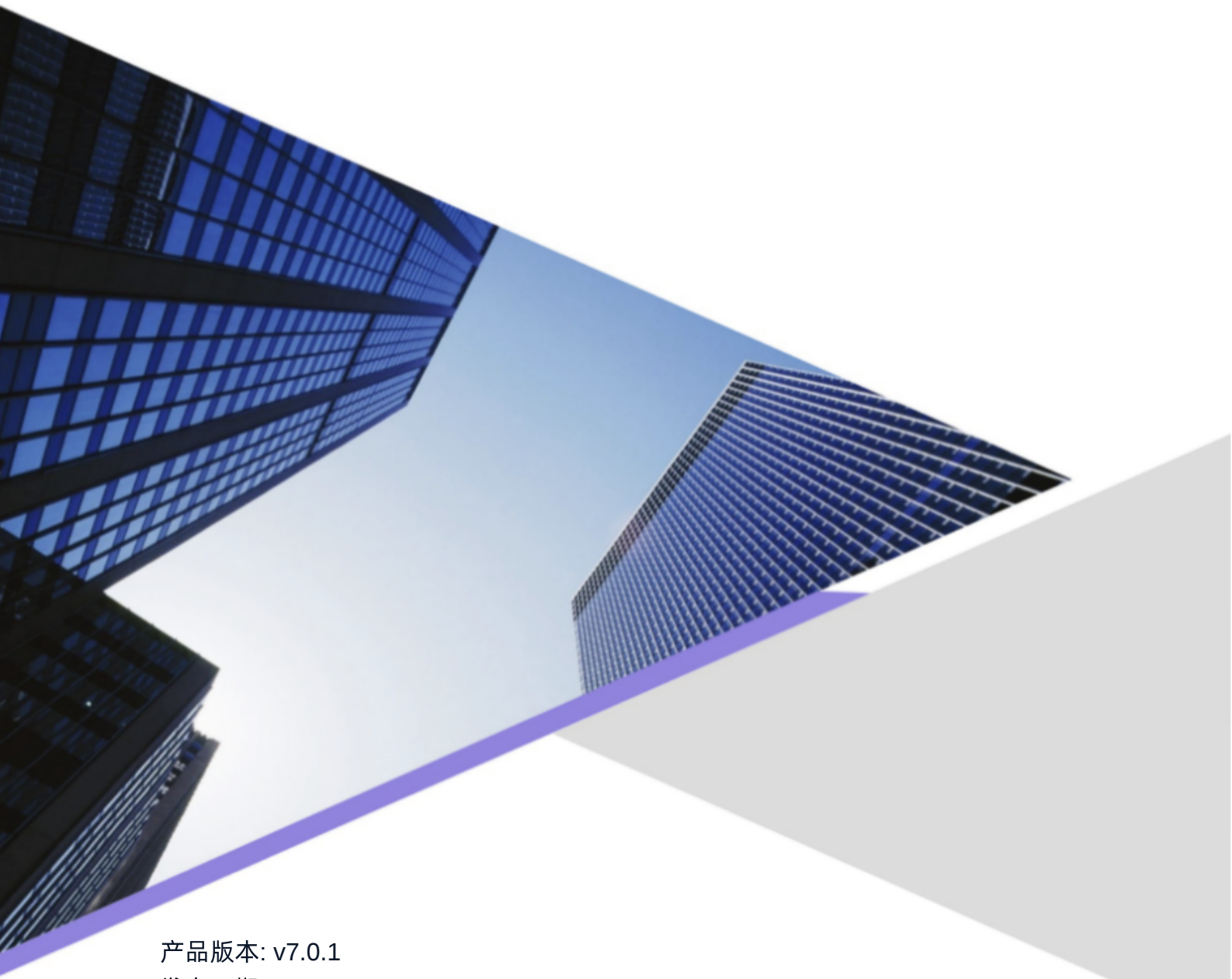
EasyStack
易捷行云

Kubernetes容器服务

快速入门



产品版本: v7.0.1

发布日期: 2026-11-14

© 北京易捷思达科技发展有限公司

目录

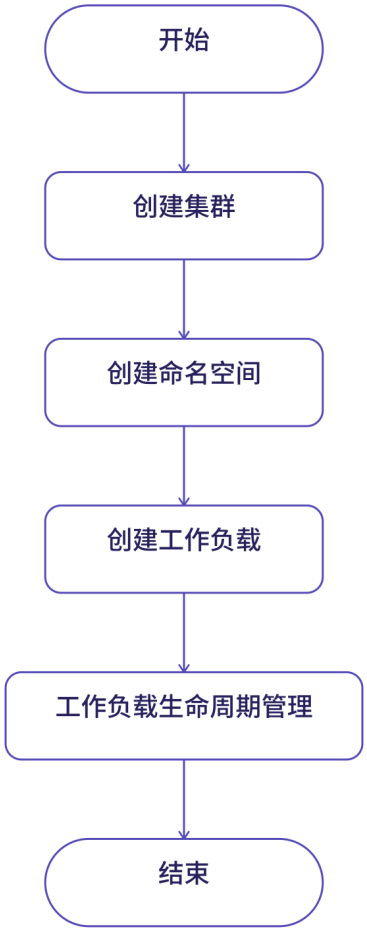
1 快速入门 ---- 1
1.1 操作指引 ---- 1
1.2 创建集群 ---- 3
1.3 创建命名空间 ---- 11
1.4 创建工作负载 ---- 13
1.5 使用Yaml创建资源（可选） ---- 22
1.6 为Kubernetes集群创建准备多活网络-不使用环境公网IP ---- 25

版权所有© 北京易捷思达科技发展有限公司

1 快速入门

1.1 操作指引

Kubernetes容器服务云产品的主线使用流程及具体说明如下：



操作流程	描述
创建集群	集群是提供Kubernetes容器服务的基础，应用将部署在集群中。
创建命名空间	通过命名空间实现同一集群内不同资源之间的隔离。

版权所有© 北京易捷思达科技发展有限公司

操作流程	描述
创建工作负载	工作负载是对一组Pod的逻辑抽象。通过部署各个工作负载实现应用的全部功能。
工作负载生命周期管理	部署后可对工作负载进行升级、伸缩、监控等，详细说明请参考“管理工作负载”章节中的说明。

版权所有© 北京易捷思达科技发展有限公司

1.2 创建集群

本功能用于创建Kubernetes集群。集群内节点将以云主机形态存在，当前暂不支持物理机形态。

前提条件

- 已将用于部署容器集群节点的云主机镜像上传至平台中。可在[产品与服务]-[计算]-[镜像]页面中上传，若还未拥有镜像文件，请联系技术支持人员获取。
- 已规划并创建集群节点所属可用区。可在[产品与服务]-[计算]-[可用区与主机集合]页面进行可用区配置。

操作步骤

1. 在顶部导航栏选择[产品与服务]-[Kubernetes容器服务]-[集群管理]，进入“集群管理”页面。
2. 单击 `创建集群` ，跳转至“创建集群”页面。
3. 配置参数，单击 `创建集群` 完成操作。

参数说明

基础配置



参数	说明
名称	Kubernetes集群名称。
虚拟机镜像	集群节点使用的镜像。
Kubernetes版本	当前仅支持V1.35.3-es。
运行时组件	容器运行时组件是负责运行容器并进行整个生命周期管理的软件，当前仅支持containerd。
SSH密钥对	密钥对由一个公钥和一个私钥组成，用于外部客户端通过SSH远程登录Kubernetes集群的任意节点。在下拉框中选择所需密钥对，若尚不存在，可单击 创建密钥对 进行创建。创建后的密钥对可在[产品与服务]-[计算]-[SSH密钥对]中查看。平台只保存公钥，请妥善保存您的私钥。
可用区	集群节点所在的可用区。②「网络与节点配置」里能选到的子网、③ 组件节点也都跟着它走——子网绑定一个可用区，节点与子网不同区就挂不上网卡。

网络与节点配置

集群网络配置



参数	说明
集群路由器	容器集群运行在所选集群路由器内，集群路由器就是底层平台里的一个路由器，同一个集群路由器可以被多个集群共用。项目内没有可用的集群路由器时，点右侧「创建集群路由器」到 VPC 管理页建一个，建完回到这里选它。VPC 与网络模式一经确定不可修改。
云环境提供公网IP	选是，将会创建节点子网的虚拟IP并绑定公网IP，在控制面节点内部将被高可用组件使用。选否，云环境不创建跳板机，需要自行确定控制面到虚拟机二层打通，否则创建失败。
公网IP	公网 IP 从这个网络里取地址，同时也是集群里 Pod 申请浮动 IP 时的默认来源。
节点网络	集群节点间互通所使用的网络。网络相关配置请查看[产品与服务]-[网络]-[网络]页面。暂不支持IPv6网络。
节点组	集群节点规格按组配置，每一行节点组各自选实例规格与数量，所有节点组共用上方的节点网络。

容器网络配置



参数	说明
网络模式	业务需要直接访问 VPC 内已有资源（数据库、消息队列、传统应用），或希望以 VPC 原生地址访问 Pod、被 VPC 侧的监控与审计记录 → 选 VPC-CNI 模式。VPC 子网可用 IP 不足、集群规模超过子网可分配容量，或需要集群网段与 VPC 完全解耦 → 选 Cilium 模式。两种模式的容器 IP 来源不同，集群创建后不可切换。
系统子网段	控制面 Pod（kube-system、default）从这个段取 IP，业务 Pod 不用它。一般不需要配置——推荐段已经避开同一个路由器下的子网与服务CIDR网络地址；只有报出重叠时才在这里改写。
容器子网	业务Pod IP使用的子网。只有名称以 raptor- 开头的网络才会出现在容器网络候选里，新建网络时网络名请以 raptor- 开头。容器子网可批量选择网络：每勾选一个容器网络，选该网络的 IPv4 子网。业务命名空间要在集群创建后到「命名空间」页绑定容器子网，绑定后其中的 Pod 才能取到 IP。

高级设置



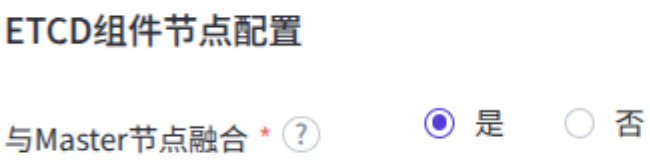
参数	说明
服务CIDR网络地址	Kubernetes Service（ClusterIP）专用网段，不分配给 Pod，与网络模式无关。

版权所有© 北京易捷思达科技发展有限公司

参数	说明
服务转发模式	选择eBPF加速模式，由网络插件通过 eBPF 直接完成 Service 转发，不部署 kube-proxy，性能最优。创建后不可切换。选择nftables模式，由 kube-proxy 的 nftables 后端完成 Service 转发，规则可被 nft list ruleset 审计，兼容存量运维工具。性能低于 eBPF。创建后不可切换。
数据面参数	MTU 在本步骤填写，取值 1200 至 1500；建集群后不可变更：存量 Pod 网卡不会被重建，同一节点上出现两种 MTU 会导致大包静默丢弃。
容器 IP 分配规则	Pod 从哪个容器子网取 IP，由该命名空间绑定的容器子网决定，同一组内取可用 IP 最多的那个，本步骤不提供可选项。业务命名空间在绑定子网前，其中的 Pod 无法取得 IP，请在集群创建后到「命名空间」那一行的「网络配置」完成绑定。

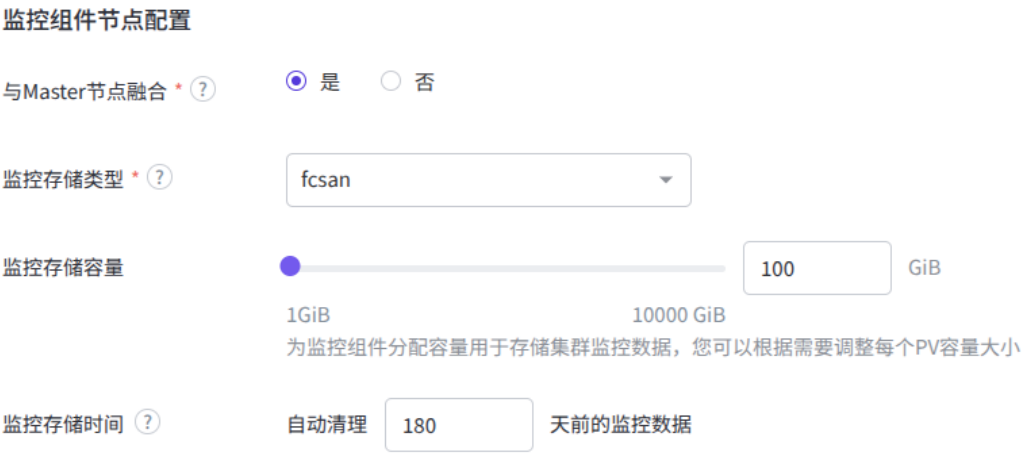
组件配置

ETCD组件节点配置



参数	说明
与Master节点融合	ETCD 与 Master 节点融合部署时，不单独创建 ETCD 节点；选择否时单独创建 ETCD 节点组。

监控组件节点配置



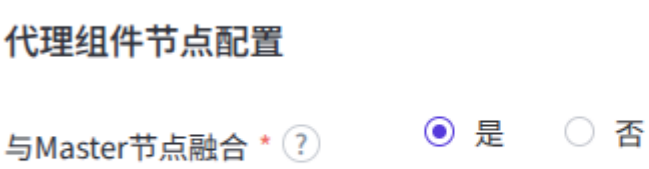
参数	说明
与Master节点融合	是否将集群监控组件部署到Master节点，与Master节点融合部署时不支持扩容。
监控存储类型	监控节点需要设置存储类型用于创建持久卷。
监控存储容量	为监控组件分配容量用于存储集群监控数据，您可以根据需要调整每个PV容量大小。
监控存储时间	平台存储监控数据时间，超出期限的监控数据将被自动清理。

日志组件节点配置



参数	说明
与Master节点融合	是否将集群日志组件部署到Master节点,与Master节点融合部署时不支持扩容。
日志存储类型	日志节点需要设置存储类型用于创建持久卷。
日志存储容量	为日志组件分配容量用于存储集群日志数据，您可以根据需要调整每个PV容量大小。
日志存储时间	平台存储日志数据时间，超出期限的日志将被自动清理。

代理组件节点配置



参数	说明
与Master节点融合	是否将集群代理组件部署到Master节点,与Master节点融合部署时不支持扩容，并且将复用master节点的公网IP。

其他配置



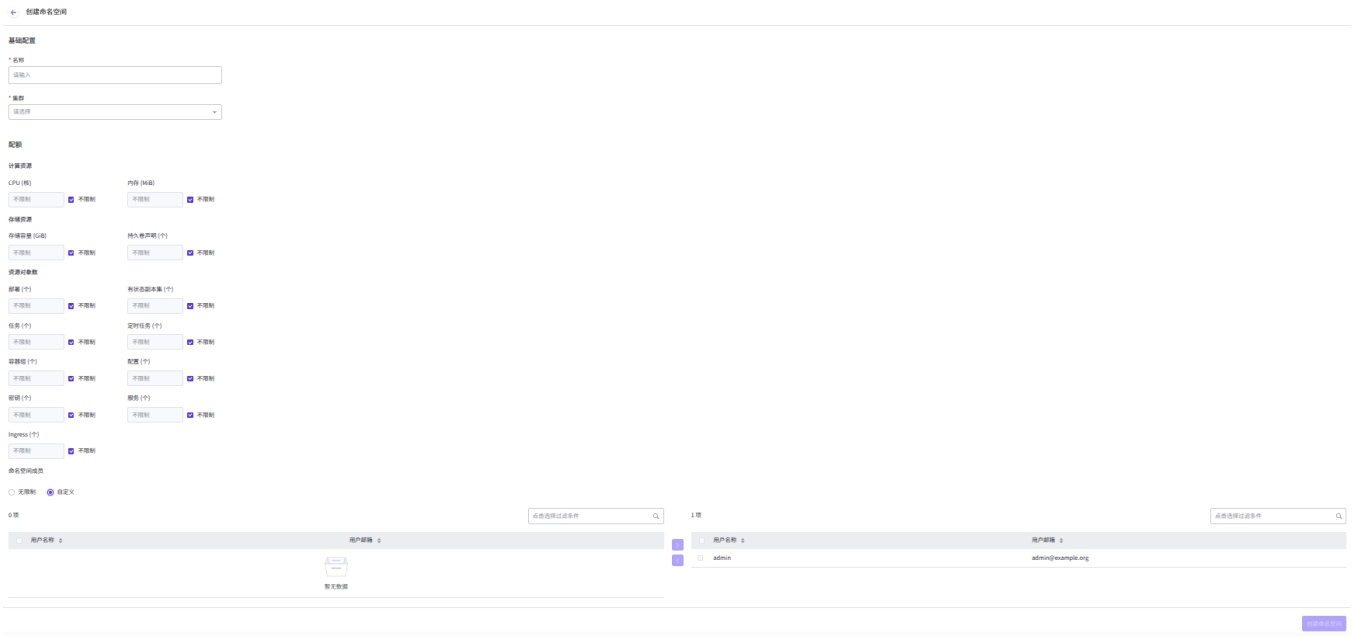
参数	说明
自定义镜像仓库地址	容器集群默认支持DockerHub等公共镜像仓库，您也可以为容器集群配置自有的镜像仓库。如果您填入的镜像仓库地址为域名，则需要保证集群节点的DNS服务能正常解析该域名。
NTP 服务器	用于节点时间同步，填写 NTP 服务器域名或 IP。
节点时区	写入节点时区配置，括号内为相对 UTC 的偏移；平台默认为 Asia/Shanghai。
节点DNS服务器	节点默认采用8.8.8.8作为DNS服务器，您可以为节点添加其他DNS服务器。

版权所有© 北京易捷思达科技发展有限公司

1.3 创建命名空间

通过命名空间实现同一集群内不同项目资源之间的隔离。

1. 在顶部导航栏选择[产品与服务]-[Kubernetes容器服务]-[命名空间]，进入“Kubernetes容器服务”-“命名空间”页面。
2. 单击 `创建命名空间` ，跳转至“创建命名空间”页面。
3. 配置参数，单击 `创建命名空间` 完成操作。



参数	说明
名称	命名空间名称。
集群	选择命名空间所属集群。
配额	根据资源规划设置集群内计算、存储、资源对象数的最大限额。

版权所有© 北京易捷思达科技发展有限公司

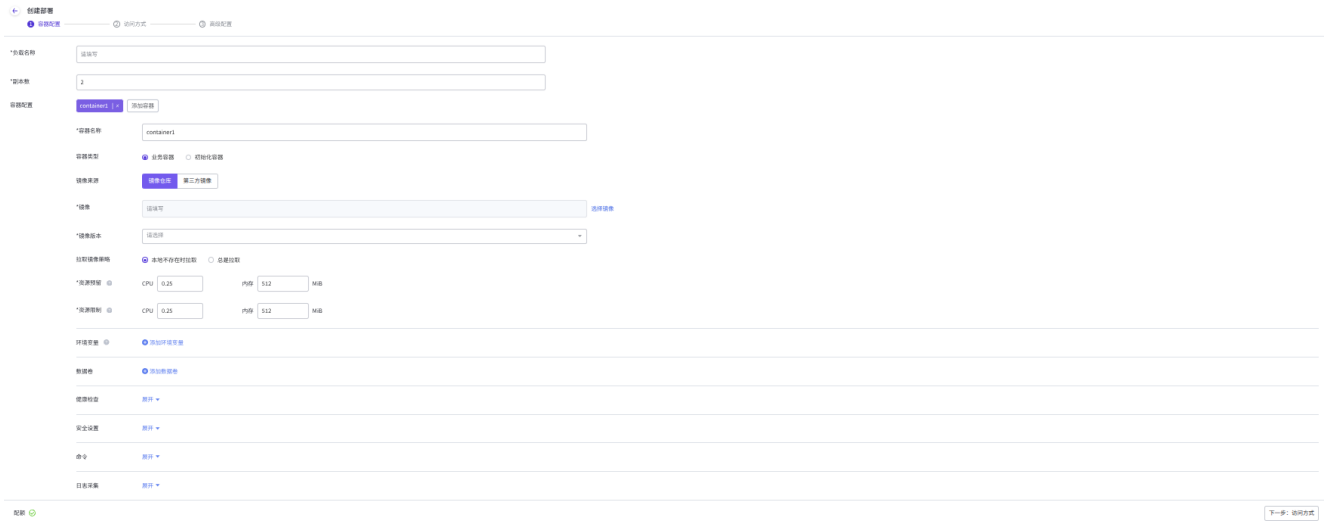
参数	说明
命名空间成员	设置当前项目成员对该命名空间的访问权限。若选择“无限制”则项目内所有成员均可访问；若选择“自定义”，则仅被授权的项目成员可访问。 > 说明： > > * 仅云管理员或部门管理员可配置本参数。 > * 已选用户列表中的管理员用户不可移除。

版权所有© 北京易捷思达科技发展有限公司

1.4 创建工作负载

工作负载是对一组Pod的逻辑抽象。通过部署各个工作负载实现应用的全部功能。创建方式支持界面创建和Yaml创建，本节将以创建“部署”类型工作负载为例介绍界面创建方式，Yaml创建方式请参见 [使用Yaml创建资源]。

1. 在顶部导航栏选择[产品与服务]-[Kubernetes容器服务]-[工作负载]，进入“Kubernetes容器服务”-“工作负载”-“部署”页面。
2. 在左侧导航栏选择目标命名空间。
3. 单击 `创建部署` ，跳转至“创建部署”页面。
4. 填写容器配置参数。



参数	说明
负载名称	创建的“部署”的名称
副本数	仅当负载类型为“部署”或“有状态副本集”时可配置此参数。表示该工作负载包括的容器组个数。每个容器组都由相同的容器部署而成。设置多个容器组主要用于实现高可靠性，当某个实例故障时，工作负载还能正常运行。

版权所有© 北京易捷思达科技发展有限公司

参数		说明
容器配置	容器类型	包括业务容器和初始化容器。业务容器即真正运行业务的容器，初始化容器则运行于业务容器启动期间。若容器组中有多个初始化容器，这些容器会按顺序逐个运行，每个初始化容器必须运行成功，下一个才能够运行，当所有初始化容器运行完成时，集群才会正常运行业务容器。由于一个容器组中的存储卷是共享的，所以初始化容器中产生的数据可以被业务容器使用到。由于初始化容器提供了一种机制来阻塞或延迟业务容器的启动，可以应用于有启动顺序要求的容器组之间。
	镜像来源	包括镜像仓库和第三方镜像两种来源。选择镜像仓库则使用本集群对接的镜像仓库，选择第三方镜像则需要输入第三方镜像地址且保证网络可达。
	密钥认证	仅当镜像来源为“第三方镜像”时可配置。
	密钥	仅当镜像来源为“第三方镜像”且密钥认证为“是”时可配置。
	镜像	若镜像来源为“镜像仓库”，则单击 `选择镜像` ，弹出选择镜像对话框。选择目标镜像，单击 `确定` 完成操作。若镜像来源为“第三方镜像”，则输入格式为ip:port/path/name的镜像地址。
	镜像版本	若镜像来源为“镜像仓库”，则在下拉框中选择目标版本；若镜像来源为“第三方镜像”，则手动输入目标版本。
	拉取镜像策略	包括“本地不存在时拉取”和“总是拉取”两种策略。
	资源预留	保证容器成功调度到节点的最小资源。
	资源限制	容器运行中允许使用的最大资源。

版权所有© 北京易捷思达科技发展有限公司

参数		说明
	环境变量	容器在启动过程中需要的一些配置信息如启动命令、证书等，这类信息需要在容器组故障重启后仍然存在并重新加载到新容器组中，这类信息可以通过环境变量的形式单独存储。当前支持三种类型： * 普通变量：普通变量不需提前创建，直接输入即可。 * 配置：选择已创建好的配置。创建配置的介绍请参考 创建配置。 * 密钥：选择已创建好的密钥。创建密钥的介绍请参考 创建密钥。
	数据卷	单击 添加数据卷 ，弹出“添加数据卷”对话框。配置参数，单击 确定 完成操作。参数说明如下： * 类型： - 持久卷声明：仅工作负载类型为部署、任务、定时任务时可选择本类型。给容器挂载持久化存储，数据不会因容器的销毁或节点异常而消失。适用于需持久化存储、高磁盘IO等场景。持久卷声明需要事先创建，相关介绍请参考 创建持久卷声明。 - 存储类：仅工作负载类型为有状态副本集时可选择。不需事先创建持久卷声明，可直接通过指定存储类及所需存储容量创建持久卷，并挂载到指定的容器路径。 - 主机路径：将容器所在宿主机的文件目录挂载到容器的指定路径。若选择此类型，节点异常无法恢复时，本地磁盘中的数据也将无法恢复。 - 临时路径：将容器所在宿主机的临时目录挂载到容器的指定路径。 - 配置：选择已创建好的配置。创建配置的介绍请参考 创建配置。 - 密钥：选择已创建好的密钥。创建密钥的介绍参考 创建密钥。 * 挂载路径：所选数据卷挂载至容器的绝对路径。
	健康检查	健康检查包括存活检查和就绪检查两项功能。存活检查用于检测容器是否正常，如果容器的存活检查失败，集群会对该容器执行重启操作；若容器的存活检查成功则不执行任何操

版权所有© 北京易捷思达科技发展有限公司

参数		说明
		作。就绪检查用于检查用户业务是否就绪，如果容器的就绪检查失败，则不转发流量到当前容器组；若检查成功，则会开放对该容器组的访问。 * 检查方式： - HTTP/HTTPS方式：适用于提供HTTP/HTTPS服务的容器，集群周期性地对该容器发起HTTP/HTTPS GET请求，如果HTTP/HTTPS 返回状态码小于400，则证明检查成功、容器健康，否则检查失败。例如，方式选择HTTP，路径为/check，端口为80，则集群周期性向容器发起如下请求：`GET http://容器IP:80/check` 。 - TCP方式：适用于提供TCP通信服务的容器，集群周期性地检测端口是否为打开状态，若端口为打开状态，则检查成功、容器健康；若端口为关闭或进程为停止状态，则检查失败。例如：一个提供nginx服务的容器，服务端口为80，则配置TCP检查端口为80，那么集群会周期性检测该容器的80端口打开状态。 - 容器命令方式：该方式要求用户指定一个容器内的可执行命令，集群会周期性地在容器内执行该命令，若进程退出状态码为 0则检查成功、容器健康，否则检查失败。 * 公共参数： - 首次检查延时：容器启动后第一次进行健康检查的延迟时间，这段时间为预留给业务程序正常启动。例如，设置为10，表明容器启动后10秒才开始健康检查。 - 检查间隔：执行健康检查的时间间隔。例如，设置为30，则每间隔30秒执行一次健康检查。 - 超时时间：检查超时后的等待时间。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。 - 健康认定（）次成功：假设本参数设置为N，健康检查失败后，至少连续成功N次会认为容器健康。 - 不健康认定（）次失败：假设本参数设置为X，健康检查失败后，集群将继续尝试X次健康检查，若仍不符合健康条件，则放弃该容器。对于存活检查，放弃意味着重启容器；对于就绪检查，放弃意味着容器组将被标记为未就绪。

参数		说明
	安全设置	* 非root用户运行：要求容器组具有非零runAsUser值，或在镜像中定义了USER环境变量。 * 只读root文件系统：是否必须使用一个只读的root文件系统。 * runAsUser：用户ID。容器中的进程都以该用户ID运行。 * runAsGroup：Group ID。容器中的进程都以该Group ID运行。 * 特权：若选择是，则容器拥有宿主机的root权限。
	命令	* 启动命令：容器启动时运行的第一条命令，将覆盖镜像中的Entrypoint指令。 * 启动命令参数：覆盖镜像中的CMD执行，如已设置了运行命令，该条指令将被附加到运行命令的参数中。 * 启动后执行命令：该命令在创建容器之后立即执行。 * 停止前执行命令：这个命令在停止容器前执行，是否立即调用此命令取决于 API 的请求或者管理事件。
	日志采集	采集应用的运行日志，实现平台内应用与组件日志的全量采集与查询。 * 日志源：选择需采集日志的资源，支持容器标准日志（默认）和应用日志两种。 * 日志文件路径：当“日志源”选择“应用日志”时需配置。日志文件存放路径，需注意，该路径要求已挂载数据卷。

5. 完成一个容器的配置后，若需要添加多个容器可单击添加容器，否则单击下一步：访问方式进入“访问方式”配置页面。



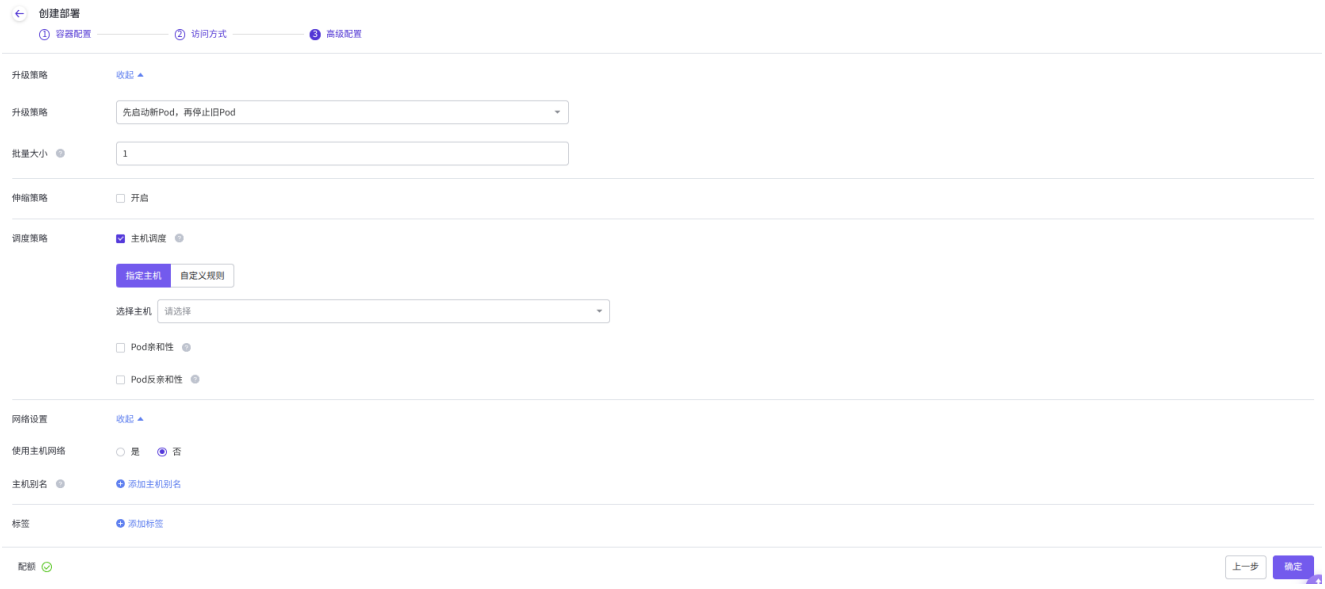
6. 点击 `添加服务` ，打开“添加服务”弹窗，填写访问方式相关参数，点击 `确定` 。

参数		说明
访问方式	ClusterIP	适用于集群内部访问场景，集群为服务分配一个固定的集群内虚拟IP，集群内其它pod可以通过集群内部域名访问，格式为“<服务名称>.<工作负载所在命名空间>.svc.cluster.local:<端口号>”。集群外无效。
	NodePort	适用于集群外部访问场景，集群除了会给服务分配一个内部的虚拟IP，还会在每个节点上为服务分配静态端口号，集群外部可通过集群任一节点IP和静态端口号访问服务。
	LoadBalancer	适用于集群外部访问场景，其实是NodePort的扩展。集群外部通过一个特定的负载均衡器访问Service，这个负载均衡器将请求转发到节点的端口。负载均衡器的访问地址可在[业务视图]-[网络管理]-[服务]页面的列表中“访问地址”字段查看。
容器端口		容器镜像中工作负载实际监听的端口。
访问端口		容器端口映射到节点IP上的端口。当访问方式为“NodePort”时，支持随机生成。
协议		包括TCP、UDP，根据业务类型选择。当访问方式为“LoadBalancer”时仅支持TCP协议。
Ingress配置/Ingress规则		Ingress是kubernetes中的一种HTTP方式的路由转发机制。例如域名填写为example.com，路径填写为/path，则外部可通过 `http://example.com/path` 访问服务。

7. 单击 `下一步：高级配置` ，进入“高级配置”页面。

8. 填写高级配置参数。

版权所有© 北京易捷思达科技发展有限公司


创建部署
1 容器配置
2 访问方式
3 高级配置
升级策略
收起
升级策略
先启动新Pod，再停止旧Pod
批量大小
1
伸缩策略
开启
调度策略
主机调度
指定主机
自定义规则
选择主机
请选择
Pod亲和性
Pod反亲和性
网络设置
收起
使用主机网络
是
否
主机别名
添加主机别名
标签
添加标签
配额
上一步
确定

参数	说明

参数	说明
升级策略	* 工作负载类型为“部署”时，参数说明如下： * 先启动新Pod，再停止旧Pod/先停止旧Pod，再启动新Pod：可定义每次启动或停止Pod的数量。例如选择先启动新Pod，再停止旧Pod，批量大小设置为1，则每次先启动1个新的Pod，新的Pod成功后停止1个旧Pod，以此类推。 * 停止所有Pod，再启动新Pod：先停止所有老版本容器组，再启动新版本容器组，升级过程中业务会中断。 * 自定义： * 最大超量：更新过程中容器组数量可以超过期望副本的数量或百分比。 * 最多不可用数：升级过程中允许的最多不可用容器组数量，如果等于期望副本数量有业务中断风险（最小存活容器组数量=期望副本数量-最多不可用数）。 * 工作负载类型为“有状态副本集”或“守护进程集”时，参数说明如下： * 滚动：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。 * 手动删除时更新：集群不会自动更新工作负载中的容器组，需手动删除容器组以使集群创建新的容器组。 * 最多不可用数：仅当升级策略为“滚动”时需配置，指升级过程中允许的最多不可用容器组数量，如果等于期望副本数量则有业务中断风险（最小存活容器组数量=期望副本数量-最多不可用数）。
伸缩策略	当达到设置的条件后自动扩展或收缩容器组数量。* 最小实例数：期望容器组数量的最小值。 * 最大实例数：期望容器组数量的最大值。 * CPU使用率阈值：所有容器组平均cpu使用率超过阈值自动扩展，n-1（n为容器组总数）个容器组平均内存使用率低于阈值自动收缩。需勾选“开启”后才能输入阈值。 * 内存使用率阈值：所有容器组平均内存使用率超过阈值自动扩展，n-1（n为容器组总数）个容器组平均内存使用率低于阈值自动收缩。需勾选“开启”后才能输入阈值。

版权所有© 北京易捷思达科技发展有限公司

参数		说明
调度策略	主机调度	* 指定主机：可选择集群内任一节点，该工作负载内的容器将被调度到所选节点上。 * 自定义规则：包括必须满足条件和尽量满足条件。必须满足条件是硬性要求，必须满足才能成功调度，支持添加多条规则，多条规则间是“且”的关系，即需要满足所有规则才可以调度；尽量满足条件表示集群会尽量将容器调度到符合规则的主机上，支持添加多条规则，多条规则间是“或”的关系，不满足规则的主机也会进行调度，根据规则的权重值，权重值越高越会被优先调度。
	Pod亲和性/Pod反亲和性	Pod亲和性决定哪些工作负载的Pod部署在同一个拓扑域，可根据业务需求进行工作负载的就近部署，容器间通信就近路由，减少网络消耗。Pod反亲和性决定工作负载的Pod不和哪些工作负载的Pod部署在同一个拓扑域，互相干扰的工作负载反亲和部署，避免干扰，减少宕机影响。拓扑域是由一个或多个节点组成的，这些节点在所指定的属性上具有相同的值，例如拓扑域为kubernetes.io/hostname，则具有相同hostname的节点成为一个拓扑域（即同一节点）。必须满足条件是硬性要求，支持添加多条规则，多条规则间是“且”的关系，即需要满足所有规则才可以调度；尽量满足条件表示集群会尽量将容器调度到符合规则的主机上，多条规则间是“或”的关系，不满足规则的主机也会进行调度，根据规则的权重值，权重值越高越会被优先调度。
网络设置		* 使用主机网络：直接使用宿主机网络，不进行网络虚拟化隔离，容器将直接暴露在宿主机网络环境中，此时容器组IP即为宿主机IP。 * 主机别名：仅当“使用主机网络”选项为否时可设置。增加主机别名后即可通过域名访问对应的主机IP。
标签		通过标签可以方便地标识及筛选对象。

版权所有© 北京易捷思达科技发展有限公司

1.5 使用Yaml创建资源（可选）

本章节主要描述如何使用Yaml创建Kubernetes容器服务资源。可以根据实际的业务场景，灵活选择适合的资源创建方案。

1. 在顶部导航栏选择[产品与服务]-[Kubernetes容器服务]-[任意子菜单]，进入“Kubernetes容器服务”页面。
2. 在左侧导航栏选择[业务视图]页签-选择目标命名空间。
3. 单击页面右下角的“Yaml”图标，进入“导入Yaml”页面。



4. 直接粘贴Yaml文件内容，或单击编辑区域右上角的“导入”图标，选择本地存储的Yaml文件。
5. 请关注调试结果，调试主要针对格式校验，若有错误可点击错误信息，跳至目标行进行修改。
6. 待调试通过后，单击"导入" ，完成操作。

以下是一个示例的YAML文件，用于创建一个名为"deployment-demo"的"Deployment"类型工作负载，并将其与名为"app-demo"的应用关联：

> 注意： 在创建资源时通过 app.kubernetes.io/name：应用名称 标签指定所关联的目标应用。

版权所有© 北京易捷思达科技发展有限公司

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    ecns.es.io/workload: deployment-deployment-demo
   app.kubernetes.io/name: app-demo  #Replace app-demo with the name of the
target application you want to associate with.
  name: deployment-demo
spec:
  replicas: 1
  selector:
    matchLabels:
      ecns.es.io/workload: deployment-deployment-demo
  template:
    metadata:
      labels:
        ecns.es.io/workload: deployment-deployment-demo
    spec:
      containers:
      - env:
        - name: username
          valueFrom:
            secretKeyRef:
              key: username
              name: secrets-demo
        - name: password
          valueFrom:
            secretKeyRef:
              key: password
              name: secrets-demo
        image: hub.ecns.io/wuzs01/nginx:latest
        imagePullPolicy: IfNotPresent
        name: nginx
        volumeMounts:
        - mountPath: /tmp/start.sh
          name: configmap-demo
          readOnly: true
          subPath: start.sh
        - mountPath: /data
          name: pvc-demo
      dnsPolicy: ClusterFirst
```

版权所有© 北京易捷思达科技发展有限公司

```
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
      volumes:
      - configMap:
          defaultMode: 292
          name: configmap-demo
        name: configmap-demo
      - name: pvc-demo
        persistentVolumeClaim:
          claimName: pvc-demo
```

通过使用这个Yaml文件，您可以创建一个部署工作负载。请根据您的实际需求进行适当的修改和配置。

版权所有© 北京易捷思达科技发展有限公司

1.6 为Kubernetes集群创建准备多活网络-不使用环境公网IP

为 Kubernetes 集群创建准备多活网络：不使用环境公网 IP（FIP）

> 版本 1.0 · 2026-11-13 · EasyStack 云平台
> 本文档为面向 EasyStack 云平台用户的通用配置指南，不包含具体环境的 IP 地址、资源 ID、节点名称、VNI、项目等信息。文中示例地址仅用于说明，实施时应按现场规划替换。
> 适用平台：支持多活网络及纯路由模式路由器的 EasyStack 云平台。读者对象：云运维工程师、交付工程师、网络管理员。目标：在不使用 FIP（公网 IP）的前提下完成多活网络准备，并在创建 Kubernetes 集群时直接使用该网络。

目录

- 0. 前置条件
- 1. 核心结论
- 2. 变量与示例
- 3. 总体架构
- 4. 规划原则
- 5. 实施步骤
  - 5.1 创建用户网络与子网
  - 5.2 创建多活互联网络
  - 5.3 创建四台路由器
  - 5.4 连接子网
  - 5.5 配置静态路由
  - 5.6 外部网关 ECMP 回程
  - 5.7 验证
- 6. 创建不使用 FIP 的集群
  - 6.1 关键配置选择
  - 6.2 操作步骤

版权所有© 北京易捷思达科技发展有限公司

- 6.3 容器网络选择
- 6.4 未使用 FIP 时的外部访问
- 6.5 创建后验证
- 7. 常见问题
  - Q1：用户路由器为何不能配置 FIP 或 SNAT？
  - Q2：互联子网为何不配置网关并关闭 DHCP？
  - Q3：三台网络节点路由器是否必须分布于三个不同节点？
  - Q4：三条目的地址相同的 `0.0.0.0/0` 路由是否会冲突？
  - Q5：创建集群时，VPC 默认值不是用户网络所属的 VPC，应如何处理？
  - Q6：未配置 FIP 时，如何访问集群 API？
  - Q7：容器网络候选列表为空或无法选择时，应如何处理？
  - Q8：如何删除或回滚配置？
- 8. 附录
  - 8.1 命令行参考（示例变量）
  - 8.2 配置检查清单
  - 8.3 术语表
  - 8.4 文档信息
  - 8.5 相关文档

0. 前置条件

实施前，请确认以下条件，以确保资源与权限满足要求。

- 云管理员已提供外部网络，并确认其网段、网关、VLAN/Flat 类型及可用外部 IP 地址。
- 网络团队可配合在外部网关配置业务网段的 ECMP 回程路由。
- 平台至少有三个网络节点在线，且当前项目具备创建网络、子网、路由器及端口的权限。
- 已完成地址规划，业务子网、互联段、Pod CIDR、Service CIDR 及系统子网段互不重叠。
- 如需通过命令行实施，应具备 `neutron` 或 `openstack` 客户端；如需进行创建后验证，应获取集群 kubeconfig 或在 VPC 内准备一台云主机。

> **适用范围限制：**本方案不适用于需要从公网直接访问集群 API 或节点的场景。本方案不创建 FIP 或堡垒机；如需公网入访，应另行部署堡垒机，或配置带外部网关的入口路由器。

版权所有© 北京易捷思达科技发展有限公司

1. 核心结论

1. **多活网络采用纯路由模式**：四台路由器（一台用户路由器与三台网络节点路由器）均不绑定 FIP，也不启用 SNAT。
2. **创建集群时无需 FIP**：节点网络应直接选择已创建的用户网络及子网；VPC 应选择该用户网络所属的 VPC；“云环境提供公网 IP”应选择 **否**。
3. **外部回程由外部网关承担**：在外部网关上为业务网段配置三条 ECMP 静态路由，下一跳分别为三台网络节点路由器的外部 IP 地址。
4. **集群 API 使用节点子网内的 VIP**：在 VPC 内创建或验证集群无需 FIP 或堡垒机；若执行创建/验证的客户端位于 VPC 外，需经 VPN 或堡垒机接入；公网主动访问通过外部网关回程实现。

> **适用场景**：若业务仅需集群节点或 Pod 主动出网，无需从公网直接访问 API 或节点，则“不使用 FIP”是符合多活网络前提的推荐方案。

---

2. 变量与示例

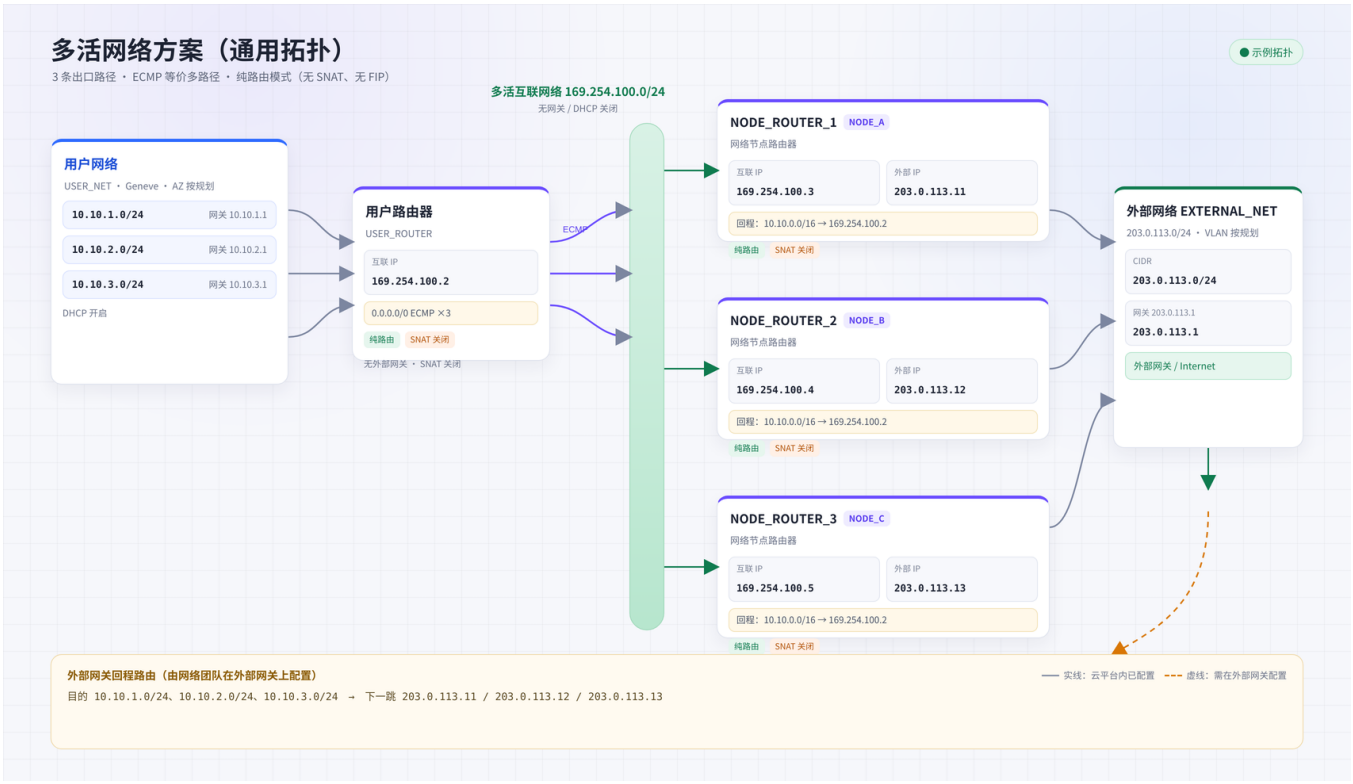
本文档使用大写变量表示需按实际环境替换的参数。表中 IP 地址均为**示例地址**（ `10.10.0.0/16` 为私网示例， `203.0.113.0/24` 为 RFC 5737 文档示例段），请勿直接用于生产环境。

变量	含义	示例
`USER_NET`	用户网络名称	`user-net`
`USER_SUBNET_1/2/3`	用户网络的三个业务子网	`user-subnet-1/2/3`
`MULTI_NET`	多活互联网络名称	`multi-net`
`USER_ROUTER`	用户路由器名称	`user-router`
`NODE_ROUTER_1/2/3`	三台网络节点路由器	`node-router-1/2/3`
`EXTERNAL_NET`	外部网络名称	`external-net`
`EXTERNAL_GW`	外部网络网关	`203.0.113.1`
`EXT_IP_1/2/3`	三台网络节点路由器的外部 IP	`203.0.113.11/12/13`

版权所有© 北京易捷思达科技发展有限公司

变量	含义	示例
`NODE_A/B/C`	三台网络节点名称	按现场网络节点填写
`USER_SUMMARY`	用户网络的汇总路由	`10.10.0.0/16`
`AZ`	可用区	`az-1`

3. 总体架构



多活网络方案（通用拓扑）
3 条出口路径 · ECMP 等价多路径 · 纯路由模式（无 SNAT、无 FIP）
示例拓扑
多活互联网络 169.254.100.0/24
无网关 / DHCP 关闭
用户网络
USER_NET · Geneve · AZ 按规划
10.10.1.0/24
网关 10.10.1.1
10.10.2.0/24
网关 10.10.2.1
10.10.3.0/24
网关 10.10.3.1
DHCP 开启
用户路由器
USER_ROUTER
互联 IP
169.254.100.2
0.0.0.0/0 ECMP ×3
纯路由
SNAT 关闭
无外部网关 · SNAT 关闭
ECMP
NODE_ROUTER_1
NODE_A
网络节点路由器
互联 IP
169.254.100.3
外部 IP
203.0.113.11
回程：10.10.0.0/16 → 169.254.100.2
纯路由
SNAT 关闭
NODE_ROUTER_2
NODE_B
网络节点路由器
互联 IP
169.254.100.4
外部 IP
203.0.113.12
回程：10.10.0.0/16 → 169.254.100.2
纯路由
SNAT 关闭
NODE_ROUTER_3
NODE_C
网络节点路由器
互联 IP
169.254.100.5
外部 IP
203.0.113.13
回程：10.10.0.0/16 → 169.254.100.2
纯路由
SNAT 关闭
外部网络 EXTERNAL_NET
203.0.113.0/24 · VLAN 按规划
CIDR
203.0.113.0/24
网关 203.0.113.1
203.0.113.1
外部网关 / Internet
外部网关回程路由（由网络团队在外部网关上配置）
目的 10.10.1.0/24、10.10.2.0/24、10.10.3.0/24 → 下一跳 203.0.113.11 / 203.0.113.12 / 203.0.113.13
实线：云平台内已配置
虚线：需在外部网关配置

图 1 多活网络通用拓扑（示例地址；实际以现场规划为准）。

流量路径：

1. 业务云主机位于 `10.10.1.0/24`（或 `.2.0/24`、`.3.0/24`），其默认网关为 `10.10.1.1`，即 `USER_ROUTER` 的子网接口。
2. `USER_ROUTER` 配置三条等价的默认路由 `0.0.0.0/0`，下一跳分别为 `169.254.100.3/.4/.5`。
3. 三个下一跳分别位于三台网络节点路由器 `NODE_ROUTER_1/2/3` 上。
4. 网络节点路由器经 `EXTERNAL_NET` 出网，源地址不进行 SNAT。
5. 回程路径由两部分组成：
   - 外部网关将三个业务网段指向 `EXT_IP_1/2/3`；
   - 每台网络节点路由器将 `USER_SUMMARY` 指向 `169.254.100.2`。

---

4. 规划原则

对象	规划要求	示例
用户网络	内部网络，Geneve；至少一个业务子网，建议三个	`USER_NET`
业务子网	配置网关（`.1`），启用 DHCP	`10.10.1.0/24`、`10.10.2.0/24`、`10.10.3.0/24`
多活互联网络	内部网络；**不配置网关，关闭 DHCP**；建议使用链路本地地址段	`169.254.100.0/24`
用户路由器	**不配置外部网关，不启用 SNAT**	`USER_ROUTER`
网络节点路由器	每台配置外部网关；**关闭 SNAT**；手工指定外部 IP；分布于三个网络节点	`NODE_ROUTER_1/2/3`
外部网络	由云管理员提供；需确认网关、可用 IP、VLAN/Flat 类型	`EXTERNAL_NET`
地址规划	业务网段、互联段、Pod/Service 网段、外部段互不重叠	见上表

关键约束：

- 业务子网、 `USER_SUMMARY` 、Pod CIDR、Service CIDR 不得重叠；否则回程或跨网段访问可能出现流量黑洞。
- 互联段仅用于路由器之间的互联，不得分配给云主机，也不得配置网关。
- 三台网络节点路由器应分布于三个不同网络节点；否则 ECMP 仅具有形式上的三条路径，节点故障时可能同时中断。

---

5. 实施步骤

以下操作路径以中文控制台为例；不同版本的菜单名称可能略有差异。

5.1 创建用户网络与子网

操作路径： `[产品与服务] > [网络] > [网络] > 创建网络`

参数	取值
网络类型	内部网络
名称	`USER_NET`
可用区	与节点/网络节点一致的可用区
网络模式	Geneve（VNI 自动分配）
子网 1	`USER_SUBNET_1` ， `10.10.1.0/24` ，网关 `10.10.1.1` ，DHCP 开启
子网 2	`USER_SUBNET_2` ， `10.10.2.0/24` ，网关 `10.10.2.1` ，DHCP 开启
子网 3	`USER_SUBNET_3` ， `10.10.3.0/24` ，网关 `10.10.3.1` ，DHCP 开启

创建第一个子网后，单击“添加 IPv4 子网”继续添加其余子网。

5.2 创建多活互联网络

参数	取值

参数	取值
网络类型	内部网络
名称	`MULTI_NET`
可用区	与网络节点一致
网络模式	Geneve
子网	`MULTI_NET` 的 IPv4 子网，`169.254.100.0/24`，**不配置网关**，**关闭 DHCP**

> **地址段选择说明**：`169.254.100.0/24` 属于链路本地地址段，适用于路由器互联，不承载业务流量。不配置网关并关闭 DHCP，可避免地址误分配或产生额外的默认路由。也可使用其他未占用的 /24 网段，但四台路由器必须使用同一网段。

5.3 创建四台路由器

操作路径：`[产品与服务] > [网络] > [路由器] > 创建路由器`

路由器	外部网关	外部 IP	SNAT	互联 IP（5.4 指定）
`USER_ROUTER`	不配置	—	—	`169.254.100.2`
`NODE_ROUTER_1`	`EXTERNAL_NET`	`EXT_IP_1`（手工指定）	**关闭**	`169.254.100.3`
`NODE_ROUTER_2`	`EXTERNAL_NET`	`EXT_IP_2`（手工指定）	**关闭**	`169.254.100.4`
`NODE_ROUTER_3`	`EXTERNAL_NET`	`EXT_IP_3`（手工指定）	**关闭**	`169.254.100.5`

版权所有© 北京易捷思达科技发展有限公司

平台通常自动将路由器调度至不同网络节点。创建完成后，应在“网络节点”页面确认；若三台路由器集中于同一节点，应先确认创建界面是否提供网络节点/可用区选择项；如未提供，则属于平台自动调度，应联系平台支持核查调度策略，请勿通过反复重建规避问题。

注意：

- `USER_ROUTER` 仅执行内网转发，**不得**配置外部网关或 SNAT。
- 三台网络节点路由器的外部 IP 地址应手工指定，且不得与环境中的现有 IP 地址冲突。
- 创建完成后，应在“网络节点”页面确认三台路由器分别位于三个网络节点。

5.4 连接子网

操作路径：路由器详情 > `[路由器连接]` > `连接子网`

路由器	子网	子网 IP	连接方式
`USER_ROUTER`	`USER_SUBNET_1`	`10.10.1.1`	子网网关
`USER_ROUTER`	`USER_SUBNET_2`	`10.10.2.1`	子网网关
`USER_ROUTER`	`USER_SUBNET_3`	`10.10.3.1`	子网网关
`USER_ROUTER`	`MULTI_NET` 子网	`169.254.100.2`	固定 IP 端口
`NODE_ROUTER_1`	`MULTI_NET` 子网	`169.254.100.3`	固定 IP 端口
`NODE_ROUTER_2`	`MULTI_NET` 子网	`169.254.100.4`	固定 IP 端口
`NODE_ROUTER_3`	`MULTI_NET` 子网	`169.254.100.5`	固定 IP 端口

在“连接子网”对话框中选择 `MULTI_NET` 子网，并填写子网 IP 地址（如 `169.254.100.2` ）。若界面仅允许选择子网，请先按附录中的命令行参考创建固定 IP 端口，再通过该端口连接。

说明：

- 业务子网已配置网关 `.1` ，连接路由器时系统将自动使用该网关 IP，无需手工创建端口；不得为 `.1` 手工创建端口。
- 互联子网未配置网关，需先创建固定 IP 端口，再通过该端口连接（命令参见附录）。

版权所有© 北京易捷思达科技发展有限公司

5.5 配置静态路由

操作路径：路由器详情 > `[静态路由]` > `添加静态路由`

路由器	目的 CIDR	下一跳	条数
`USER_ROUTER`	`0.0.0.0/0`	`169.254.100.3` 、 `.4` 、 `.5`	3（ECMP）
`NODE_ROUTER_1`	`USER_SUMMARY`	`169.254.100.2`	1
`NODE_ROUTER_2`	`USER_SUMMARY`	`169.254.100.2`	1
`NODE_ROUTER_3`	`USER_SUMMARY`	`169.254.100.2`	1

> 回程路由建议使用 `USER_SUMMARY` （如 `10.10.0.0/16` ），而非三条 /24 路由，以覆盖网络节点路由器侧后续新增的业务子网。外部网关仍需为每个新增业务子网添加对应回程路由。前提条件是 Pod/Service 网段不得位于该汇总网段内。

5.6 外部网关 ECMP 回程

本步骤不在云平台内执行，而应在**外部网关**（ `EXTERNAL_GW` 所在的三层设备）上实施，需网络团队配合。

```
ip route add 10.10.1.0/24 \
  nexthop via 203.0.113.11 weight 1 \
  nexthop via 203.0.113.12 weight 1 \
  nexthop via 203.0.113.13 weight 1
ip route add 10.10.2.0/24 \
  nexthop via 203.0.113.11 weight 1 \
  nexthop via 203.0.113.12 weight 1 \
  nexthop via 203.0.113.13 weight 1
ip route add 10.10.3.0/24 \
  nexthop via 203.0.113.11 weight 1 \
  nexthop via 203.0.113.12 weight 1 \
  nexthop via 203.0.113.13 weight 1
```

- 上述地址均为示例，请替换为 `EXT_IP_1/2/3` 及业务网段的实际值。
- 上述路由为临时配置，设备重启后将丢失；请按网关设备的持久化机制进行保存。

版权所有© 北京易捷思达科技发展有限公司

- 验证方法：在外部网关上执行 `ip route get 10.10.1.10` ，应显示三个 nexthop 之一。
- 若网关已存在相同目的网段的路由，可使用 `ip route replace` ，或先删除后添加。

5.7 验证

检查项	位置 / 命令	期望
网络与子网	网络列表	用户网络有 3 个子网；互联网络有 1 个子网
路由器分布	路由器列表 / 网络节点页	三台网络节点路由器在三个不同节点
用户路由器连接	详情 > 路由器连接	4 条（3 个业务子网 + 互联子网）
ECMP 路由	详情 > 静态路由	3 条 `0.0.0.0/0`
回程路由	三台网络节点路由器 > 静态路由	各 1 条 `USER_SUMMARY`
OVN 实际下发	`ovn-nbctl lr-route-list`	3 条带 `ecmp` 的默认路由

命令行核对：

```
neutron router-show "$USER_ROUTER" -f json
neutron router-show "$NODE_ROUTER_1" -f json
ovn-nbctl lr-route-list <USER_ROUTER 的 OVN 逻辑路由器名>
```

执行前，请按 8.1 节设置变量，或将变量替换为实际名称。

---

6. 创建不使用 FIP 的集群

6.1 关键配置选择

字段	取值	说明

版权所有© 北京易捷思达科技发展有限公司

字段	取值	说明
VPC / 集群路由器	**该用户网络所属的 VPC**	即 §5.4 中与该用户网络相连的 `USER_ROUTER` 。**不应选择三台网络节点出口路由器**；若向导默认值不是该 VPC，应先调整 VPC 选择。
节点网络 · 私有网络	`USER_NET`	应直接使用已创建的用户网络，不应选择 `MULTI_NET` 。
节点网络 · IPv4 子网	`USER_SUBNET_1` （如 `10.10.1.0/24` ）	节点云主机从该子网分配 IP 地址；一个集群仅使用一个子网。
云环境提供公网 IP	**否**	不创建 FIP，也不创建堡垒机。
容器网络	VPC-CNI 或 Cilium	参见 6.3 节。
系统子网段	采用向导推荐值	供 Kubernetes 控制面 Pod 使用；不得与业务网段重叠。

前置资源与集群创建字段的对应关系



图 2 前序创建的网络/路由器与集群创建字段的对应关系（示意图）。示例值，实际名称/IP 以现场为准。

前置资源	集群创建字段	配置方式
`USER_NET` / `USER_SUBNET_1`（§5.1）	节点网络 · 私有网络 / IPv4 子网	应选择用户网络及子网。
`USER_ROUTER`（§5.3）	VPC / 集群路由器	应选择该用户网络所属的 VPC，不应选择三台出口路由器。
`NODE_ROUTER_1/2/3` + `EXTERNAL_NET`（§5.3）	不在向导中出现	仅用于多活出口与回程，**不应选择**。
—	云环境提供公网 IP	应选择“否”，即不使用 FIP。

字段映射关系：§5.1 的网络/子网 → 步骤②的节点网络；§5.3 的用户路由器 → 步骤②的 VPC；三台出口路由器和外部网络在用户路由器后面，负责出网与回程，不在集群创建向导中配置。

版权所有© 北京易捷思达科技发展有限公司

> **设计原则**：节点网络应直接使用用户网络及子网；VPC 应选择该用户网络所属的 VPC，无需为本方案新建 VPC；公网 IP 应选择“否”。由此创建的集群不使用 FIP，API Server 使用节点子网内的 VIP。

6.2 操作步骤

1. 进入 `Kubernetes 容器服务 > 集群管理 > 创建集群` 。
2. 在步骤①中填写名称、镜像、Kubernetes 版本、SSH 密钥及可用区。
3. 在步骤②中：
   - VPC 应选择该用户网络所属的 VPC（ `USER_ROUTER` ，无需新建 VPC）；
   - “云环境提供公网 IP”应选择 **否**；
   - 节点网络应选择 `USER_NET` 和 `USER_SUBNET_1` ；
   - 按需填写节点组规格和数量；
   - 选择容器网络（参见 6.3 节）；
   - 系统子网段应保持推荐值。
4. 完成组件及其他配置后，提交创建请求。
5. 创建完成后，集群 API 地址应为节点子网内的 VIP（如 `https://10.10.1.200:6443` ），无需 FIP。

6.3 容器网络选择

模式	适用场景	建议
VPC-CNI	Pod 直接使用 VPC 子网 IP，需与 VPC 内的数据库、消息队列实现三层直通	选择一个 `raptor-` 开头的容器网络及其 IPv4 子网（ `raptor-` 是 VPC-CNI 容器网络的名称前缀）；该网络必须位于同一 VPC 下，且未被其他集群占用。
Cilium	Pod 使用集群自有网段，集群网段与 VPC 解耦；VPC 子网 IP 紧张或大规模集群	无需配置 VPC 容器网络；填写 Pod CIDR（如 `10.244.0.0/16` ），不得与业务网段、互联段、Service CIDR、系统子网段重叠。

两种模式在集群创建后不可切换，请根据业务需求选择。

6.4 未使用 FIP 时的外部访问

版权所有© 北京易捷思达科技发展有限公司

- **集群内部或同一 VPC 内**：直接访问节点子网 VIP（API）或节点 IP。
- **公网主动访问**：通过 5.6 节配置的外部网关回程路由实现；如需 SSH 或 API 入访，应在外部侧另行部署堡垒机，或配置带外部网关的入口路由器。
- **不得**为 `USER_ROUTER` 启用 SNAT 或绑定 FIP，否则将破坏纯路由前提。
- 若执行创建/验证的客户端与节点子网二层可达，创建阶段无需堡垒机；若该客户端位于 VPC 外，应先打通专线或 VPN，或使用临时堡垒机，否则集群创建将失败。

6.5 创建后验证

```
# 节点 IP 应落在 USER_SUBNET_1
kubectl get nodes -o wide

# 节点默认网关应为 USER_ROUTER 的子网接口
ssh <node> ip route

# 验证节点访问外部网络的连通性
ping -c 3 8.8.8.8
```

请从集群详情页下载 kubeconfig，并在 VPC 内云主机或通过 VPN/堡垒机执行上述命令；`<node>` 应替换为 `kubectl get nodes -o wide` 输出的节点名称。

若节点 IP 不在预期子网，请检查步骤②的节点网络选择；若节点已分配 IP 但无法访问外部网络，请依次检查：

1. `USER_ROUTER` 的三条 `0.0.0.0/0` 路由；
2. 三台网络节点路由器的 `USER_SUMMARY` 回程路由；
3. 外部网关的三条业务网段回程路由。

---

7. 常见问题

Q1：用户路由器为何不能配置 FIP 或 SNAT?

多活方案以纯路由为前提。用户路由器仅执行内网转发，出网流量由三台网络节点路由器分担。若用户路由器接入外部网关或启用 SNAT，流量将绕过 ECMP 或产生非对称回程，导致多活架构退化为单出口。

Q2：互联子网为何不配置网关并关闭 DHCP?

版权所有© 北京易捷思达科技发展有限公司

该子网仅承载 `.2` 至 `.5` 四个手工分配的地址。配置网关会产生不必要的直连默认路由；启用 DHCP 可能为误接的云主机分配地址。关闭这两项后，互联段仅用于路由器之间的互联。

Q3：三台网络节点路由器是否必须分布于三个不同节点？

是。ECMP 的价值在于三条路径分布于不同物理节点。若三台路由器位于同一节点，节点故障时三条路径可能同时中断，也无法实现出口带宽的横向扩展。

Q4：三条目的地址相同的 `0.0.0.0/0` 路由是否会冲突？

不会。ECMP 允许同一目的 CIDR 配置多个不同下一跳；OVN 北向数据库将显示为三行带 `ecmp` 标记的路由。

Q5：创建集群时，VPC 默认值不是用户网络所属的 VPC，应如何处理？

应先调整 VPC 选择，再选择节点网络。VPC 必须是用户网络所属的路由器；三台网络节点出口路由器不是集群 VPC。选择错误可能导致节点网络候选列表中无法显示 `USER_NET` ，或将集群创建到错误的 VPC。

Q6：未配置 FIP 时，如何访问集群 API？

API Server 使用节点子网内的 VIP，创建完成后可在集群详情页查看。同一 VPC 内可直接访问；公网访问需通过外部网关回程及 VPN 或堡垒机，无需为路由器绑定 FIP。

Q7：容器网络候选列表为空或无法选择时，应如何处理？

应先确认 VPC 选择的是用户网络所属的 VPC；再确认同一项目下是否存在以 `raptor-` 开头且属于该 VPC 的容器网络。如不存在，应新建或绑定容器网络，或改用 Cilium 模式。

Q8：如何删除或回滚配置？

应按相反顺序执行：先删除静态路由，再断开子网连接（先断开互联端口，再断开业务子网），然后删除四台路由器，最后删除子网和网络。请勿删除外部网络；业务云主机仍占用时，请勿删除业务子网。

8. 附录

8.1 命令行参考（示例变量）

以下命令使用示例变量，执行前请按实际环境替换。 `neutron` 与 `openstack` 客户端参数存在差异，请按环境支持的写法调整。

1. 变量与子网 ID

```
USER_NET=user-net
USER_SUBNET_1=user-subnet-1
USER_SUBNET_2=user-subnet-2
USER_SUBNET_3=user-subnet-3
MULTI_NET=multi-net
MULTI_SUBNET=${MULTI_NET}-subnet
USER_ROUTER=user-router
NODE_ROUTER_1=node-router-1
NODE_ROUTER_2=node-router-2
NODE_ROUTER_3=node-router-3
EXTERNAL_NET=external-net
EXTERNAL_SUBNET=external-subnet
EXT_IP_1=203.0.113.11
EXT_IP_2=203.0.113.12
EXT_IP_3=203.0.113.13
AZ=az-1

EXTERNAL_SUBNET_ID=$(neutron subnet-show "$EXTERNAL_SUBNET" -f value -c id)
```

2. 用户网络与多活互联网络

```
neutron net-create "$USER_NET" --provider:network_type geneve --
availability-zone-hint "$AZ"
neutron subnet-create "$USER_NET" 10.10.1.0/24 --name "$USER_SUBNET_1" --
gateway 10.10.1.1 --enable-dhcp
neutron subnet-create "$USER_NET" 10.10.2.0/24 --name "$USER_SUBNET_2" --
gateway 10.10.2.1 --enable-dhcp
neutron subnet-create "$USER_NET" 10.10.3.0/24 --name "$USER_SUBNET_3" --
gateway 10.10.3.1 --enable-dhcp

neutron net-create "$MULTI_NET" --provider:network_type geneve --
availability-zone-hint "$AZ"
neutron subnet-create "$MULTI_NET" 169.254.100.0/24 --name "$MULTI_SUBNET" -
-no-gateway --disable-dhcp
MULTI_SUBNET_ID=$(neutron subnet-show "$MULTI_SUBNET" -f value -c id)
```

3. 四台路由器

版权所有© 北京易捷思达科技发展有限公司

```
neutron router-create "$USER_ROUTER" --availability-zone-hint "$AZ"
neutron router-create "$NODE_ROUTER_1" --availability-zone-hint "$AZ"
neutron router-create "$NODE_ROUTER_2" --availability-zone-hint "$AZ"
neutron router-create "$NODE_ROUTER_3" --availability-zone-hint "$AZ"
```

4. 外部网关（关闭 SNAT，手工指定 IP）

```
neutron router-gateway-set "$NODE_ROUTER_1" "$EXTERNAL_NET" --disable-snat \
  --fixed-ip subnet_id=$EXTERNAL_SUBNET_ID,ip_address=$EXT_IP_1
```

```
neutron router-gateway-set "$NODE_ROUTER_2" "$EXTERNAL_NET" --disable-snat \
  --fixed-ip subnet_id=$EXTERNAL_SUBNET_ID,ip_address=$EXT_IP_2
```

```
neutron router-gateway-set "$NODE_ROUTER_3" "$EXTERNAL_NET" --disable-snat \
  --fixed-ip subnet_id=$EXTERNAL_SUBNET_ID,ip_address=$EXT_IP_3
```

5. 连接子网（业务子网 + 互联固定 IP 端口）

```
for s in "$USER_SUBNET_1" "$USER_SUBNET_2" "$USER_SUBNET_3"; do
  neutron router-interface-add "$USER_ROUTER" "$s"
done

PORT1=$(neutron port-create "$MULTI_NET" --name "${USER_ROUTER}-multi" \
  --fixed-ip subnet_id=$MULTI_SUBNET_ID,ip_address=169.254.100.2 -f value -c
id)
neutron router-interface-add "$USER_ROUTER" port="$PORT1"

PORT2=$(neutron port-create "$MULTI_NET" --name "${NODE_ROUTER_1}-multi" \
  --fixed-ip subnet_id=$MULTI_SUBNET_ID,ip_address=169.254.100.3 -f value -c
id)
neutron router-interface-add "$NODE_ROUTER_1" port="$PORT2"

PORT3=$(neutron port-create "$MULTI_NET" --name "${NODE_ROUTER_2}-multi" \
  --fixed-ip subnet_id=$MULTI_SUBNET_ID,ip_address=169.254.100.4 -f value -c
id)
neutron router-interface-add "$NODE_ROUTER_2" port="$PORT3"

PORT4=$(neutron port-create "$MULTI_NET" --name "${NODE_ROUTER_3}-multi" \
```

版权所有© 北京易捷思达科技发展有限公司

```
  --fixed-ip subnet_id=$MULTI_SUBNET_ID,ip_address=169.254.100.5 -f value -c
id)
neutron router-interface-add "$NODE_ROUTER_3" port="$PORT4"
```

6. 静态路由

```
neutron router-update "$USER_ROUTER" \
  --route destination=0.0.0.0/0,nexthop=169.254.100.3 \
  --route destination=0.0.0.0/0,nexthop=169.254.100.4 \
  --route destination=0.0.0.0/0,nexthop=169.254.100.5

for r in "$NODE_ROUTER_1" "$NODE_ROUTER_2" "$NODE_ROUTER_3"; do
  neutron router-update "$r" --route
destination=10.10.0.0/16,nexthop=169.254.100.2
done
```

8.2 配置检查清单

- [ ] 用户网络包含 3 个业务子网，网关为 `.1`，DHCP 已启用。
- [ ] 多活互联网络包含 1 个子网，未配置网关，DHCP 已关闭。
- [ ] 四台路由器均已创建；三台网络节点路由器的外部网关配置正常，SNAT 已关闭。
- [ ] 三台网络节点路由器分布于三个不同网络节点。
- [ ] `USER_ROUTER` 具有 4 条连接和 3 条 `0.0.0.0/0` 路由。
- [ ] 每台网络节点路由器具有 1 条 `USER_SUMMARY` 回程路由。
- [ ] 外部网关配置了 3 条业务网段 ECMP 回程路由。
- [ ] 集群创建时，VPC 选择用户网络所属的 VPC，节点网络选择 `USER_NET` / `USER_SUBNET_1`，公网 IP 选择“否”。
- [ ] 集群节点 IP 位于业务子网，API 使用节点子网 VIP，且未使用 FIP。

8.3 术语表

术语	含义
多活网络	多条等价出口路径同时承载流量，单节点故障自动切换，并横向提升出口带宽。
纯路由模式	路由器仅执行三层转发，不绑定 FIP，也不执行 SNAT。

版权所有© 北京易捷思达科技发展有限公司

术语	含义
ECMP	等价多路径，同一目的 CIDR 配多个下一跳，按流哈希分担。
FIP	浮动 IP / 公网 IP；本方案不使用。
网络节点路由器	部署在网络节点上的出口路由器，负责隧道网络与外部网络的转换。

8.4 文档信息

项目	内容
版本	1.0（2026-11-13）
文档类型	用户指南 / 通用配置指南
适用范围	支持多活网络及纯路由模式路由器的 EasyStack 云平台；不适用于需要公网直接访问集群 API 或节点的场景。
维护说明	本文档随平台版本更新；具体菜单及参数以实际环境为准。

8.5 相关文档

- SDN 网络服务：配置多活网络方案（IPv4）
- Kubernetes 容器服务：创建集群、节点网络与容器网络
- 平台网络管理：路由器、公网 IP、网络节点

版权所有© 北京易捷思达科技发展有限公司

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区23号楼华胜天成科研大楼一层东侧120-123
南京分公司：
江苏省南京市雨花台区软件大道168号润和创智中心B栋一楼西101
上海office：
上海黄浦区西藏中路336号华旭大厦22楼2204
成都分公司：
成都市高新区天府五街168号德必天府五街WE602

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)
training@easystack.cn (培训咨询)
hr@easystack.cn (招聘咨询)

版权所有© 北京易捷思达科技发展有限公司