

# LoadBalancer 直连 Pod 模式 Service获取真实源 IP (eni模式实现clb直连业务pod)

2025-07-03 15:53

网络模式为VPC-CNI  
如图所示

节点和网络信息

节点数量

3个 [查看资源用量](#)

默认操作系统

tlinux4\_x86\_64\_public\_uefi [🔗](#)

系统镜像来源

公共镜像 - 基础镜像

节点hostname命名模式

自动命名 [🔗](#)

节点网络

[vpc-pdnvwkqx](#) [🔗](#)

容器网络插件

VPC-CNI 共享网卡多IP

是否固定Pod IP

否

容器子网

子网ID	子网名称	子网CIDR	可用区	剩余IP	可用区可扩容Pod数
subnet-6coyoz...	kestrel	10.15.17.0/24	广州四区	222	222

Service CIDR

172.17.0.0/17

Kube-proxy 转发模式

ipvs

ClusterIP增强 [🔗](#)

未开启

注册节点能力 [🔗](#)

☐

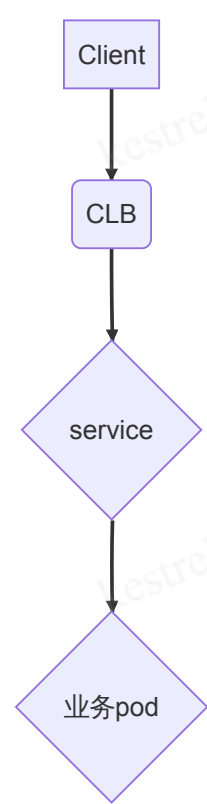
咨询

动态

文档

反馈

业务访问链路：  
clb直连pod 模式：  
客户端-> LB类型svc-> 业务pod（不经过nodeport）  
转发流程如图所示



使用 TKE 原生支持的 CLB 直连 Pod 的转发功能，后端 Pods 收到的请求的源 IP 即为客户端真实源 IP  
容器服务控制台获取源 IP 步骤如下：

1.创建一个工作负载 (Deployment)

名称

cni-direct-pod

最长63个字符。只能包含小写字母、数字及分隔符("-"),且必须以小写字母开头,数字或小写字母结尾

描述

请输入描述信息,不超过1000个字符

命名空间

kestreli

Labels

新增

标签键名称不超过63个字符,仅支持英文、数字、"/","-"且不允许以"/"开头。支持使用前缀,更多说明[查看详情](#)

标签键值只能包含字母、数字及分隔符("-","\_","."),且必须以字母、数字开头和结尾

Annotations

新增

Annotations键名称不超过63个字符,仅支持英文、数字、"/","-"且不允许以"/"开头。支持使用前缀,更多说明[查看详情](#)

Annotations值为字符串类型无长度限制。为保证可读性和可移植性,建议将键限制为较短字符串并避免使用特殊字符(如换行、空格等)。

OS类型

Linux

切换容器OS类型将会初始化配置

数据卷 (选项)

添加数据卷

为容器提供存储,目前支持临时路径、主机路径、云硬盘数据卷、文件存储NFS、配置文件、PVC,还需挂载到容器的指定路径中。[使用指引](#)

实例内容器

connection

+ 添加容器

名称

connection

实例内容器

connection

+ 添加容器

名称

connection

镜像

vickytan-demo.tencentcloudcr.com/kestreli/images

选择镜像

镜像版本 (Tag)

v1.0

选择镜像版本

镜像拉取策略

Always

IfNotPresent

Never

总是从远程拉取该镜像

环境变量

新增变量

变量名为空时,在变量名称中粘贴一行或多行key=value或key: value的键值对可以实现快速批量输入

CPU/内存限制

CPU限制

request 0.25 - limit 0.5 核

内存限制

request 256 - limit 1024 MiB

Request用于预分配资源,当集群中的节点没有request所要求的资源数量时,容器会创建失败。  
Limit用于设置容器使用资源的最大上限,避免异常情况下节点资源消耗过多。

GPU 资源

卡数: 0

配置该工作负载使用的最少GPU资源,请确保集群内已有足够的GPU资源

容器端口

添加容器端口

显示高级设置

此时镜像为腾讯云OrcaTerm构建且推送到镜像仓库的个人版镜像

← 广州 | TKE-test (勿删) | 运行中

新建节点池

YAML创建

基本信息

资源对象

节点管理

命名空间

工作负载

Pod

服务与路由

Deployment

Statefulset

Daemonset

Job

Cronjob

新建

监控

Workload Map

kestreli

名称只能搜索一个关键词

名称

Labels

Selector

镜像

运行/期望Pod...

Request/Limits

操作

☐

cni-direct-pod

k8s-app:cni-dir...  
qcloud-app:cni-...

k8s-app:cni-d...  
qcloud-app:c...

vickytan-demo.tencentcloudcr.com/kestreli/images:v1.0

1/1

CPU : 0.25/ 0.5  
核  
内存 : 256/ 1024  
Mi

更新Pod数量 更新Pod配置 更多

实例管理

资源中心

镜像仓库

Helm Chart

命名空间

运维中心

触发器

镜像仓库

地域 广州 10

实例 vickytan-demo

产品体验, 您说了算

镜像仓库操作指南

当前实例支持网络访问控制(ACL),默认阻断全部访问来源,请参考[网络访问控制](#)接入访问客户端所在私有网络 VPC 或公网 IP 网络。建议优先使用私有网络 VPC 上传下载镜像,高速稳定安全。

新建

删除

请输入仓库名称

☐

名称

命名空间

仓库地址

创建时间

操作

☐

images

kestreli

vickytan-demo.tencentcloudcr.com/kestreli/images

2025-07-02 11:28:12

快捷指令 删除

版本如图所示

←kestrelli/images

产品体验, 您说了算 容器镜像服务文档

版本管理 镜像构建 仓库信息

临时登录指令 删除

请输入镜像版本

<input type="checkbox"/>	镜像版本	大小	安全级别	架构	制品类型	摘要(SHA256)	更新时间	操作
<input type="checkbox"/>	v1.0	49.2 MB		amd64	Docker-Image	sha256:ea3...	2025-07-02 11:31:07	拉取指令 扫描 层信息 删除

共 1 条

20 条 / 页

1 / 1 页

保证此时clb的运行和期望pod的数量满足预期或在pod管理中状态为运行（running）

← 广州 TKE-test (勿删) 运行中

新建节点池 YAML创建

基本信息

Deployment Statefulset Daemonset Job Cronjob

新建 监控 Workload Map

kestrel

名称只能搜索一个关键字

<input type="checkbox"/>	名称	Labels	Selector	镜像	运行/期望Pod...	Request/Limits	操作
<input type="checkbox"/>	cni-direct-pod	k8s-app:cni-dir... qcloud-app:cni-...	k8s-app:cni-d... qcloud-app:c...	vickytan- demo.tencentclou d.cr.com/kestrelli/ima ges:v1.0	1/1	CPU : 0.25/ 0.5 核 内存 : 256/ 1024 Mi	更新Pod数量 更新Pod配置 更多

集群-(广州) / TKE-test (勿删) / Deployment:cni-direct-pod(kestrel)

Pod管理 详情 修订历史 应用性能 事件 日志 YAML

监控 销毁重建

多个过滤器用回车键分隔

<input type="checkbox"/>	实例名称	状态	实例所在节点IP	实例IP	Request/Limits	运行时间	创建时间	重启次数	操作
<input type="checkbox"/>	cni-direct-pod- 776595cdd5- d779h	Running	10.15.17.23	10.15.17.125	CPU : 0.25/ 0.5 核 内存 : 256/ 1024 Mi	0d 0h 27m	2025-07-02 16:...	0 次	查看 登录 更多

2. 创建直连Pod模式service

← 集群-(广州) / TKE-test (勿删) / 新建服务与路由

名称

direct-connection-pod

最长63个字符，只能包含小写字母、数字及分隔符("-"), 且必须以小写字母开头，数字或小写字母结尾

描述

请输入描述信息，不超过1000个字符

命名空间

kestrel

Annotations

新增

Annotations键名称不超过63个字符，仅支持英文、数字、'/'、'-'，且不允许以'/'开头，支持使用缩进，更多说明查看详情

Annotations值为字符串类型无长度限制，为保证可读性和可移植性，建议将值限制为较短字符串并避免使用特殊字符（如换行、空格等）。

访问设置(Service)

服务访问方式

仅在集群内访问

主机端口访问

公网LB访问

内网LB访问

即LoadBalance类型，自动创建公网CLB 以提供Internet访问入口，支持TCP/UDP协议，如web前台类服务可以选择公网访问。  
如您需要公网通过HTTP/HTTPS协议或根据URL转发，您可以在Ingress页面使用Ingress进行路由转发，查看详情

网络模式

采用负载均衡直连Pod模式

负载均衡直连Pod模式，将不再进行NodePort转发，支持会话保持和健康检查。开通直连模式后，默认会开启优雅停机器和优雅删除，查看详情

服务访问方式：选择公网 LB 访问或内网 LB 访问。

网络模式：勾选采用负载均衡直连 Pod 模式

高级选项中ExternalTrafficPolicy勾选Local



运营商类型: ☒ BGP ☐ 中国电信 ☐ 中国移动 ☐ 中国联通

网络计费模式: ☐ 按带宽计费 ☒ 按使用流量 ☐ 共享带宽包

带宽上限:  10 Mbps

实例规格:  共享型

共享型实例中多个实例共享资源, 单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查询数(QPS) 5000。

端口映射

协议①	容器端口①	主机端口①	服务端口①	Secret①	名称
TCP	5000	范围: 30000~32767	5000	当前协议不支持设置 Secret	最长63个字符, 只能包...

添加端口映射

如当前的密钥不合适, 请 [新建密钥](#)

高级设置 (选项)

ExternalTrafficPolicy: ☐ Cluster ☒ Local

能够保留来源IP, 并可以保证公网、VPC内网访问 (LoadBalancer) 和主机端口访问 (NodePort) 模式下流量仅在本节点转发。Local转发使部分没有业务Pod存在的节点健康检查失败, 可能存在流量不均衡转发的风险。

注意: 若您选择了 Local 模式, 当 Pod 从节点调度到超级节点上, 或者反过来, 将导致流量中断。更多请查看 [...](#)。

Session Affinity: ☐ ClientIP ☒ None

引用 Workload : 绑定创建好的工作负载

引用 Workload 资源

资源类型: ☒ deployment ☐ statefulset

资源列表:  cni-direct-pod

无可用资源, 可前往 [资源控制台](#) 新建

Labels: k8s-app: cni-direct-pod  
qcloud-app: cni-direct-pod

广州 | TKE-test (勿删) | 运行中

新建节点池

操作指南

Service Ingress NginxIngress

新建

名称: kestral

名称只能搜索一个关键字, Label格式要求:

名称	Labels	类型	Selector	访问入口	端口	创建时间	操作
direct-connection-pod	k8s-app:cn... qcloud-app... service.clo...	lb-gd12w40a 公网LB(按量计费)	k8s-app:cn... qcloud-app...	1.14.168.2 172.17.57.1 (服务IP)	TCP/80	2025-07-0...	<a href="#">更新配置</a> <a href="#">编辑Annotation</a> <a href="#">更多</a>

第 1 页

20 条 / 页

3. 根据service公网访问入口获取源IP

← 广州 TKE-test (勿删) 运行中

新建节点池 YAML创建

· 基本信息

· 节点管理

· 命名空间

· 工作负载

· Pod

· 服务与路由

· 配置管理

· 存储

· 资源对象浏览器

Service Ingress NginxIngress

新建

名称只能搜索一个关键字, Label格式要求:

名称	Labels	类型	Selector	访问入口	端口	创建时间	操作
direct-connection-pod	k8s-app:cn-qcloud-app-service.cloud	公网LB(按量计费)	k8s-app:cn-qcloud-app-	114.168.2 172.17.57.1 (服务IP)	TCP/80	2025-07-0...	更新配置 编辑Annotation 更多

第 1 页 20 条 / 页

咨询

» < > 114.168.2

常用书签 手机书签 容器服务简介\_容器... 汇联易 | 一站式商... 新人入门指南 - 腾讯... 首页\_Q-Learning 暑期实习生 云智新人学习融入之... 腾讯云 产业智变·云...

美观输出

```
{\"headers\":{\"Accept\":\"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\",\"Accept-Encoding\":\"gzip, deflate\",\"Accept-Language\":\"zh-CN,zh;q=0.9\",\"Connection\":\"keep-alive\",\"Host\":\"1.14.168.2\",\"Upgrade-Insecure-Requests\":\"1\",\"User-Agent\":\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 QQBrowser/19.3.5.212\"},\"message\":\"Here are your request headers\", \"method\":\"GET\", \"remote_addr\":\"111.206.96.144\"}
```