

LoadBalancer 直连 Pod 模式 Service 获取真实源 IP Playbook

2025-07-10 16:31

目录

背景

前置条件

操作流程

Step 1: 创建业务工作负载 (Deployment)

Step 2: 创建直连 Pod 模式的 Service

Step 3: 验证真实源 IP 获取

故障排查

背景

本 Playbook 旨在指导您通过 Kubernetes 的 **VPC-CNI** 网络模式，实现 **CLB 直连业务 Pod** 的能力，确保业务 Pod 收到的请求源 IP 为客户端真实 IP。本方案完全绕过 NodePort，适用于腾讯云容器服务（TKE）环境。

前置条件

1. 集群环境

- TKE 集群需启用 **VPC-CNI** 网络模式
- 确保集群有可用节点且 **kubect1** 已配置访问权限

2. 镜像准备

- 已构建业务镜像并推送至腾讯云镜像仓库（个人版/企业版）
- 示例镜像版本：**vickytan-demo.tencentcloudcr.com/kestrelli/images:v1.0**

操作流程

Step 1: 创建业务工作负载（Deployment）

1. 创建 Deployment YAML 文件(deployment.yaml)

```
1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: real-ip-demo
5    namespace: default
6  spec:
7    replicas: 3 # 按需调整 Pod 数量
8    selector:
9      matchLabels:
10       app: real-ip-app
11    template:
12      metadata:
13        labels:
14          app: real-ip-app
15      spec:
16        containers:
17          - name: real-ip-container
18            image: vickytan-demo.tencentcloudcr.com/kestrelli/images:v1.0
19            ports:
20              - containerPort: 5000
```

🔑 关键配置

- **metadata.labels** 需与后续 Service 选择器匹配
- **containerPort** 需与业务实际端口一致

2. 部署工作负载

```
1  kubectl apply -f deployment.yaml
```

3.验证 Pod 状态

```
1 kubectl get pods -l app=real-ip-app
```

预期输出：所有 Pod 状态为 **Running**

```
[root@VM-17-154-tlinux ~]# kubectl get pods -l app=real-ip-app
NAME                                READY   STATUS    RESTARTS   AGE
real-ip-demo-677766d8bf-85xkx      1/1     Running   0           67s
real-ip-demo-677766d8bf-bxtnn      1/1     Running   0           67s
real-ip-demo-677766d8bf-gjfdb      1/1     Running   0           67s
```



Step 2: 创建直连 Pod 模式的 Service

1.创建 Service YAML 文件 (service.yaml)

```
1  apiVersion: v1
2  kind: Service
3  metadata:
4    name: clb-direct-pod
5    annotations:
6      service.cloud.tencent.com/direct-access: "true" # 启用直连 Pod 模式
7  spec:
8    selector:
9      app: real-ip-app # 需匹配 Deployment 的标签
10   ports:
11     - protocol: TCP
12       port: 80
13       targetPort: 5000
14   type: LoadBalancer
```

⚠ 核心参数说明

- `annotations.service.cloud.tencent.com/direct-access: "true"` : 启用 CLB 直连 Pod

2.部署 Service

```
1 kubectl apply -f service.yaml
```

3.验证 Service 配置

```
[root@VM-17-154-tlinux ~]# kubectl describe svc clb-direct-pod
Name: clb-direct-pod
Namespace: default
Labels: service.cloud.tencent.com/loadbalance-type=OPEN
Annotations: service.cloud.tencent.com/client-token: ada1382d-0e68-453b-9d61-ad58b9cd3b3d
              service.cloud.tencent.com/console-update-time: 2025-07-09T12:05:35+08:00
              service.cloud.tencent.com/direct-access: true
              service.cloud.tencent.com/local-svc-weighted-balance: false
              service.cloud.tencent.com/sync-begin-time: 2025-07-09T12:05:42+08:00
              service.cloud.tencent.com/sync-end-time: 2025-07-09T12:05:43+08:00
              service.cloud.tencent.com/tke-service-config: clb-direct-pod-service-config-5b8tgnt0y9k
              service.kubernetes.io/loadbalance-id: lb-fxgxou14
              service.kubernetes.io/local-svc-only-bind-node-with-pod: false
Selector: app=real-ip-app
Type: LoadBalancer
IP Family Policy: SingleStack
IP Families: IPv4
IP: 172.18.86.8
IPs: 172.18.86.8
LoadBalancer Ingress: 114.132.191.109 (VIP)
Port: 5000-80-tcp-5b90msfnl30 80/TCP
TargetPort: 5000/TCP
NodePort: 5000-80-tcp-5b90msfnl30 31242/TCP
Endpoints: 10.15.17.127:5000,10.15.17.65:5000,10.15.17.54:5000
Session Affinity: None
External Traffic Policy: Local
Internal Traffic Policy: Cluster
HealthCheck NodePort: 31842
Events: <none>
```

关键检查项：

- Annotations 包含 direct-access: true

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

如何选择

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，

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 and 优雅删除，

负载均衡

自动创建

使用已有

自动创建CLB用于公网/内网访问Service，CLB的生命周期由TKE管理。请勿手动修改由TKE创建的CLB监听器，

IP版本

IPv4

IP版本不支持进行变更

VPC

当前VPC

其它VPC

vpc-pdnvwkgs

建议使用随机可用区，若指定可用区的资源售罄将无法创建相关实例

可用区类型

单可用区

多可用区

可用区

随机可用区

端口映射

协议	容器端口	主机端口	服务端口	Secret	名称
TCP	5000	31242	80	当前协议不支持设置Secret	5000-80-tcp-5b90ms

咨询

动态

文档

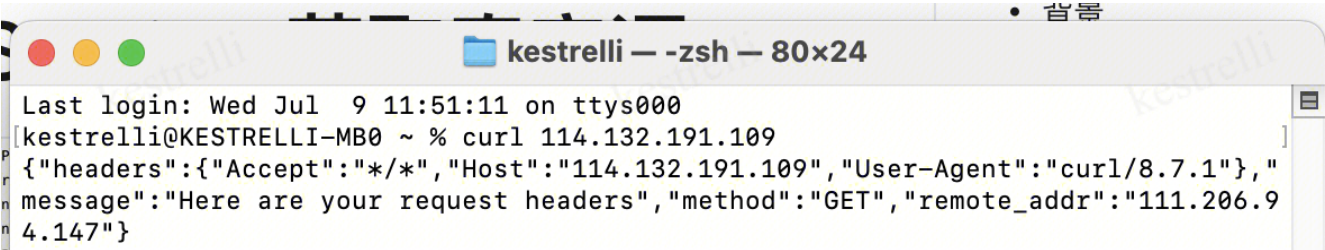
反馈



Step 3: 验证真实源 IP 获取

mac系统在终端/win系统在cmd中输入curl+service公网访问IP（如curl 114.132.191.109）

预期结果：显示的客户端 IP 非节点 IP，而是真实公网 IP



或者在浏览器直接输入公网IP(114.132.191.109)



故障排查

问题现象	排查方向
Pod 无法连接	1. 检查 <code>containerPort</code> 与业务端口是否一致 2. 检查 Pod 安全组是否放通
源 IP 仍是节点 IP	检查 Service annotation <code>direct-access=true</code>
CLB 无公网 IP	1. 检查账户余额/带宽限制 2. 确认未启用内网 LB

清理资源

```
1 kubectl delete svc clb-direct-pod
2 kubectl delete deploy real-ip-demo
```