#### 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 集群已存在且需启用 `VPC-CNI` 网络模式

- 确保集群有可用节点且 `kubectl` 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\*\*​

已存放在deployment.yaml文件中

📌 ​\*\*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\*\*​

```

kubectl apply -f deployment.yaml

```

\*\*3.验证 Pod 状态\*\*​

```

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

```

\*\*预期输出\*\*​：所有 Pod 状态为 `Running`

#### Step 2: 创建直连 Pod 模式的 Service

\*\*1.创建 Service YAML 文件\*\*​

已存放在service.yaml文件中

⚠️ ​\*\*核心参数说明\*\*​

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

\*\*2.部署 Service\*\*​

```

kubectl apply -f service.yaml

```

​\*\*3.验证 Service 配置\*\*​

```

kubectl describe svc clb-direct-pod

```

\*\*关键检查项\*\*​：

- `Annotations` 包含 `direct-access: true`

#### 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

清理资源

```

kubectl delete svc clb-direct-pod

kubectl delete deploy real-ip-demo

```

### 故障排查

|问题现象|排查方向|

|:-:|:-:|

|Pod 无法连接|1. 检查 `containerPort` 与业务端口是否一致<br>2. 检查 Pod 安全组是否放通|

|源 IP 仍是节点 IP|检查 Service annotation `direct-access=true`|

|CLB 无公网 IP|1. 检查账户余额/带宽限制<br>2. 确认未启用内网 LB|