



# TKE真实源IP获取方案全景指南

2025-07-11 21:43

# 目录

五大业务场景技术矩阵

 五大场景对比

 部署流程总图

 核心配置详解


场景1：VPC-CNI直连（原生节点）


场景2：GlobalRouter直连（原生节点）

场景3：VPC-CNI直连（超级节点）

场景4：VPC-CNI非直连

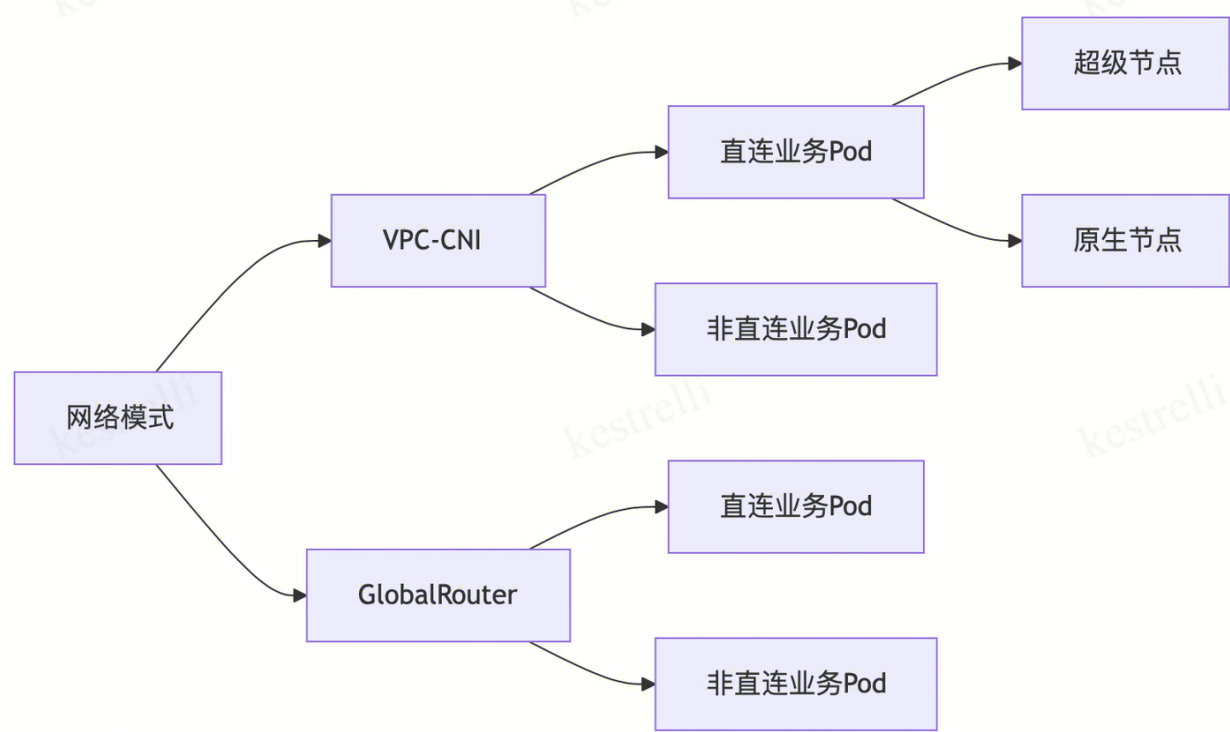
场景5：GlobalRouter非直连

 架构示意图

 统一验证方法

 文档映射表

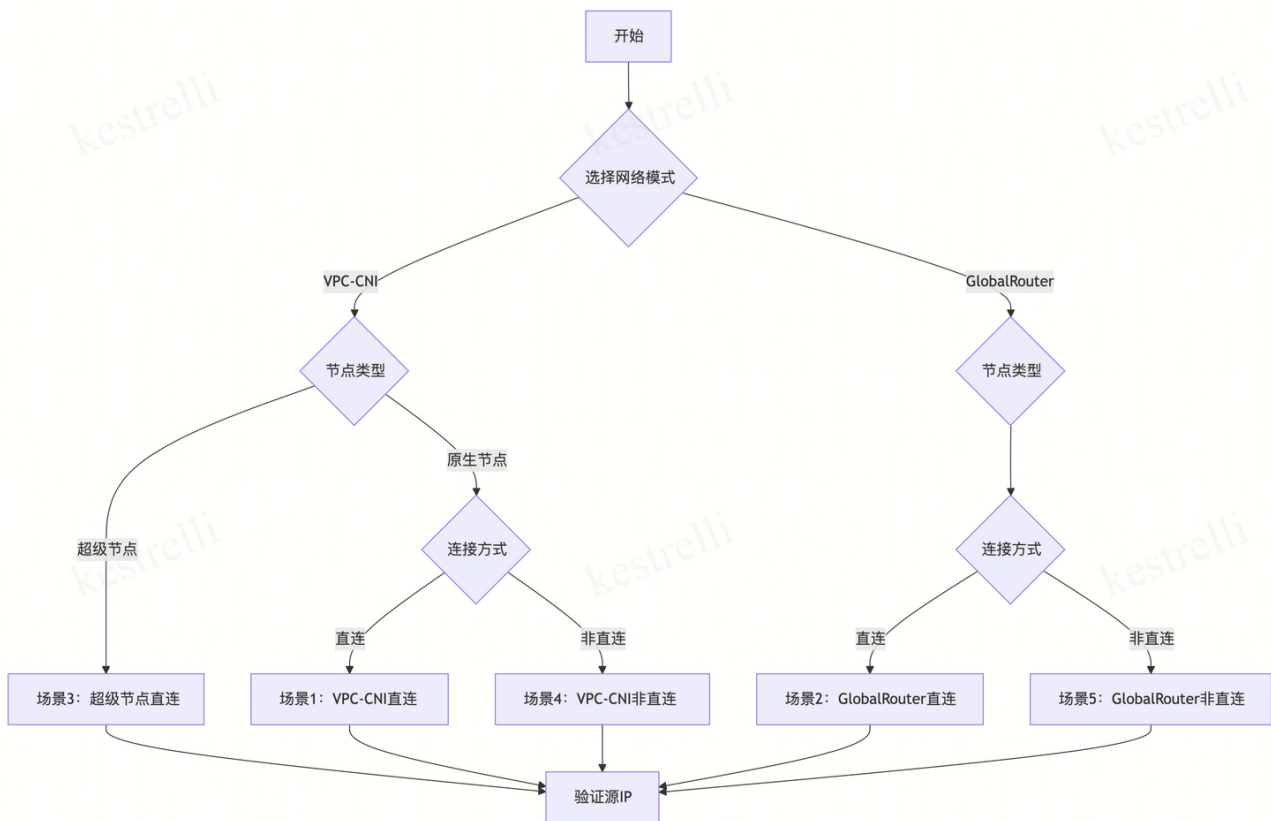
五大业务场景技术矩阵



五大场景对比

场景	网络模式	连接方式	节点类型	核心特征
场景1	VPC-CNI	直连	原生节点	注解 <code>direct-access: true</code>
场景2	GlobalRouter	直连	原生节点	ConfigMap启用 <code>GlobalRouteDirectAccess</code>
场景3	VPC-CNI	直连	超级节点	自动获取源IP，无需节点SSH
场景4	VPC-CNI	非直连	原生节点	需配置X-Forwarded-For头
场景5	GlobalRouter	非直连	原生节点	Ingress注解 <code>ingressClassName: qcloud</code>

部署流程总图



## 🔧 核心配置详解

### 场景1：VPC-CNI直连（原生节点）

```
1 # service.yaml 关键配置
2 metadata:
3   annotations:
4     service.cloud.tencent.com/direct-access: "true" # 直连开关
5 spec:
6   type: LoadBalancer
7   ports:
8     - targetPort: 5000 # 业务实际端口
```

### 场景2：GlobalRouter直连（原生节点）

```
1 # 启用集群级直连能力
2 kubectl patch cm tke-service-controller-config -n kube-system \
3   --patch '{"data":{"GlobalRouteDirectAccess":"true"}}'
```

### 场景3：VPC-CNI直连（超级节点）

```
1 # 特殊限制：不可SSH登录节点
2 spec:
3   template:
4     spec:
5       nodeSelector:
6         node.kubernetes.io/instance-type: SUPER_NODE
```

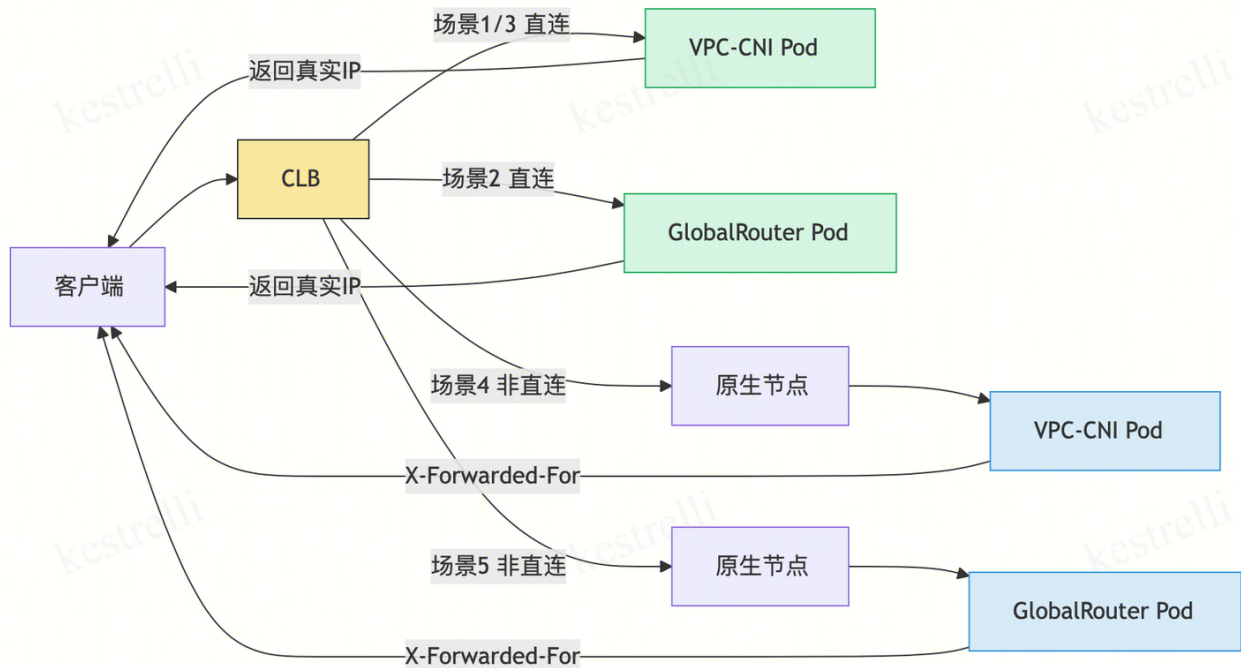
## 场景4：VPC-CNI非直连

```
1 # service.yaml
2 spec:
3   type: NodePort # 非直连必需
```

## 场景5：GlobalRouter非直连

```
1 # ingress.yaml
2 metadata:
3   annotations:
4     kubernetes.io/ingress.class: "qcloud"
5 spec:
6   rules:
7     - http:
8       paths:
9         - backend:
10             service:
11               name: real-ip-svc
12               port:
13                 number: 80
```

## 架构示意图



## ⚙️ 统一验证方法

```

1 # 获取公网IP
2 CLB_IP=$(kubectl get svc -o jsonpath='{.status.loadBalancer.ingress[0].ip}')
3
4 # 测试请求（所有场景通用）
5 curl -s http://$CLB_IP | jq '.headers | {X-Forwarded-For, X-Real-IP}'

```

预期输出：

```

1 {
2   "X-Forwarded-For": "您的客户端源IP",
3   "X-Real-IP": "您的客户端源IP"
4 }

```

## 📖 文档映射表

场景	源文档	关键区别点
VPC-CNI直连（原生节点）	文档LoadBalancer 直连 Pod 模式 Service 获取真实源 IP Playbook	直连注解+普通节点
GlobalRouter直连（原生节点）	文档LoadBalancer直连 Pod模式 Service获取真实源 IP Playbook (gr模式)	ConfigMap全局开关
VPC-CNI直连（超级节点）	文档超级节点Pod源IP获取方案(CLB直连Pod模式) Playbook	超级节点自动生效
VPC-CNI非直连（原生节点）	文档TKE Ingress获取真实源IP Playbook指南	NodePort+Local策略
GlobalRouter非直连（原生节点）	文档TKE Ingress获取真实源IP Playbook指南（gr模式实现CLB非直连业务Pod）	Ingress qcloud注解

所有方案均通过腾讯云TKE 验证

预构建镜像：

- `vickytan-demo.tencentcloudcr.com/kestrelli/images : v1.0`
- `test-angel01.tencentcloudcr.com/kestrelli/kestrel-seven-real-ip:v1.0`