### 背景

本Playbook专门针对腾讯云容器服务(TKE)集群环境，指导您通过Orca Term终端实现CLB直连Pod模式的配置。

所有操作均在腾讯云Orca Term上执行，确保在TKE集群环境中，业务Pod能够获取客户端真实源IP。

本方案通过GlobalRouter网络模式实现，无需NodePort转发，适用于需要真实客户端IP的应用场景（如安全审计、日志分析）。

### 前置条件

在Orca Term中开始操作前，请确保满足以下条件：

|类别|要求|验证方式|

|:-:|:-:|:-:|

|​\*\*集群环境\*\*​|• TKE集群已创建且启用GlobalRouter网络模式<br>• 集群节点状态正常<br>• kubectl已配置访问权限|• 在TKE控制台确认网络模式<br>• `kubectl get nodes`检查节点状态<br>• `kubectl cluster-info`验证连接|

|​\*\*镜像准备\*\*​|• 业务镜像已推送至腾讯云镜像仓库<br>• 有权限拉取镜像|• 确认镜像地址格式：`<仓库>.tencentcloudcr.com/<命名空间>/<镜像>:<标签>`<br>• 在Orca Term测试：`docker pull <镜像地址>`|

|​\*\*访问权限\*\*​|• 已绑定集群节点<br>• 拥有操作kubectl的权限<br>• 账户有创建CLB的配额|• 确认节点登录状态<br>• 尝试运行`kubectl get pods`验证权限<br>• 检查腾讯云账号余额和CLB配额|

|​\*\*业务准备\*\*​|• 已知业务服务端口<br>• 准备测试客户端|• 确认Deployment的containerPort<br>• 准备可访问公网的设备（验证用）|

#### 操作流程

以下步骤均在腾讯云Orca Term登录后执行，专为TKE集群环境优化。

##### Step 1: 启用集群GlobalRoute直连能力

在Orca Term中配置集群级直连开关

```

# 1. 编辑ConfigMap

kubectl edit configmap tke-service-controller-config -n kube-system

# 2. 定位到data字段，添加新行

GlobalRouteDirectAccess: "true"

# 3. 保存退出

# 按ESC键，输入:wq保存

# 4. 验证配置

kubectl get configmap tke-service-controller-config -n kube-system -o yaml | grep GlobalRouteDirectAccess

```

\*\*预期输出\*\*​：`GlobalRouteDirectAccess: "true"`

\*\*关键点\*\*​：此配置启用集群维度的直连能力，是后续操作的基础。

##### Step 2: 创建业务工作负载（Deployment）

在Orca Term中通过命令行创建业务Deployment：

\*\*1.创建 Deployment YAML 文件\*\*

代码指令已存放在deployment.yaml文件中

​\*\*2.部署工作负载\*\*

```

kubectl apply -f deployment.yaml

```

\*\*3.验证 Pod 状态\*\*

```

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

```

📌 ​\*\*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

- `replicas`：根据业务需求调整副本数

- ` image`：若有需要替换为您的腾讯云镜像仓库地址

\*\*验证要求\*\*​：所有Pod状态为`Running`（按Ctrl+C退出watch）

##### Step 3: 创建直连Pod模式的Service

在Orca Term中创建LoadBalancer Service并启用直连模式：

\*\*1.创建 Service YAML 文件\*\*

代码指令已存放在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

```

\*\*确认以下输出\*\*​：

- Annotations包含 `service.cloud.tencent.com/direct-access: "true"`

- `LoadBalancer Ingress`显示公网IP

##### Step 4: 验证真实源IP获取

\*\*1. 获取CLB公网IP\*\*

```

CLB\_IP=$(kubectl get svc clb-direct-pod -o jsonpath='{.status.loadBalancer.ingress[0].ip}')

echo "测试地址: http://$CLB\_IP"

```

\*\*2. Orca Term中快速测试（需业务支持IP回显）\*\*

```

curl -s http://$CLB\_IP

```

\*\*若业务不支持支持IP回显，可直接curl+CLB公网IP\*\*

\*\* 3. 若有需要，可在外部设备验证\*\*

```

echo "请在外部设备执行:"

echo " curl http://$CLB\_IP"

echo "或浏览器访问 http://$CLB\_IP"

```

\*\*预期结果\*\*​：

- 回显内容包含客户端真实公网IP（非节点IP）

- 示例输出：`"remote\_addr":"172.19.0.65"`

\*\*验证技巧\*\*​：

- 在手机5G网络下访问，确认IP与公网IP一致

- 对比`kubectl get nodes -o wide`显示的节点IP，确保不同

#### 清理资源

释放资源避免费用：

\*\*1. 删除Service（保留Deployment可复用）\*\*

```

kubectl delete svc clb-direct-pod

```

\*\*2. 删除Deployment\*\*

```

kubectl delete deploy real-ip-demo

```

\*\*3. 可选：重置ConfigMap\*\*

```

kubectl patch cm tke-service-controller-config -n kube-system --patch '{"data":{"GlobalRouteDirectAccess":"false"}}'

```

### TKE环境最佳实践

​\*\*1.操作优化\*\*​：

- 使用`watch`命令实时监控资源状态（如`watch -n 2 kubectl get pods`）

- 用`alias k=kubectl`简化命令输入

- 重要操作前创建屏幕快照（Orca Term截图功能）

​\*\*2.安全建议\*\*​：

- 为CLB配置安全组规则，限制访问源IP

- 定期轮转镜像仓库访问凭证

- 生产环境使用独立服务账号操作kubectl

​\*\*3.性能监控\*\*​：

```

# 直连模式性能检查

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

# 查看CLB监控指标（腾讯云控制台）

```

#### 故障排查

|现象|原因|解决方案|

|:-:|:-:|:-:|

|ConfigMap保存失败|vi操作不熟练|使用`kubectl patch`命令替代：<br>`kubectl patch cm tke-service-controller-config -n kube-system --patch '{"data":{"GlobalRouteDirectAccess":"true"}}'`|

|Pod状态异常|镜像拉取失败|1. `kubectl describe pod <pod-name>`查看事件<br>2. 在Orca Term手动拉取：`docker pull <镜像>`<br>3. 检查镜像仓库权限|

|Service无公网IP|配额不足或注解错误|1. `kubectl describe svc`查看事件<br>2. 确认注解`direct-access: "true"`存在<br>3. 检查腾讯云账号CLB配额|

|访问返回节点IP|直连未生效|三重检查：<br>1. ConfigMap中GlobalRouteDirectAccess=true<br>2. Service注解direct-access=true

|Orca Term连接断开|会话超时|1. 使用`tmux`创建持久会话<br>2. 关键操作前刷新Orca Term连接|