LoadBalancer 直连 Pod 模式 Service 获取真实源 IP Playbook

2025-07-10 16:31

目录

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 `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(deployment.yaml)

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: real-ip-demo
  namespace: default
spec:
  replicas: 3  # 按需调整 Pod 数量
  selector:
    matchLabels:
      app: real-ip-app
  template:
    metadata:
      labels:
        app: real-ip-app
    spec:
      containers:
      - name: real-ip-container
        image: vickytan-demo.tencentcloudcr.com/kestrelli/images:v1.0
        ports:
        - 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

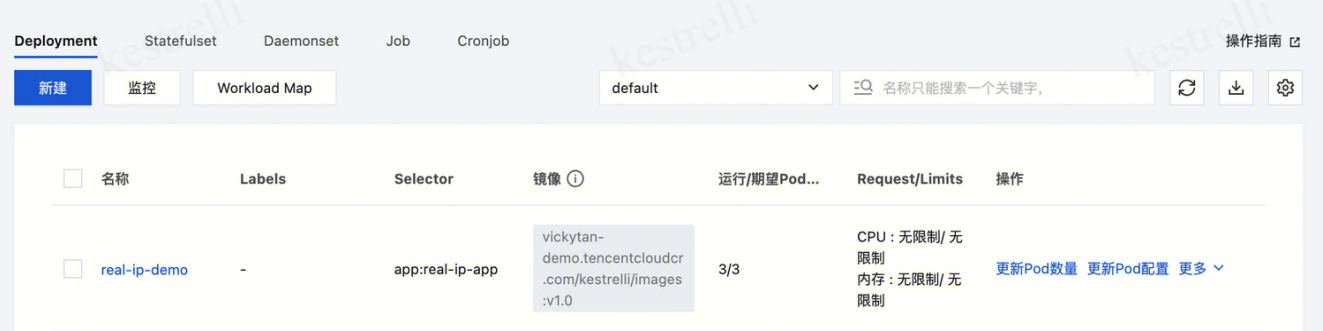
```
kubectl apply -f deployment.yaml
```

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`

```
[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）

```yaml
apiVersion: v1
kind: Service
metadata:
  name: clb-direct-pod
  annotations:
    service.cloud.tencent.com/direct-access: "true"  # 启用直连 Pod 模式
spec:
  selector:
    app: real-ip-app  # 需匹配 Deployment 的标签
  ports:
    - protocol: TCP
      port: 80
      targetPort: 5000
  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

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

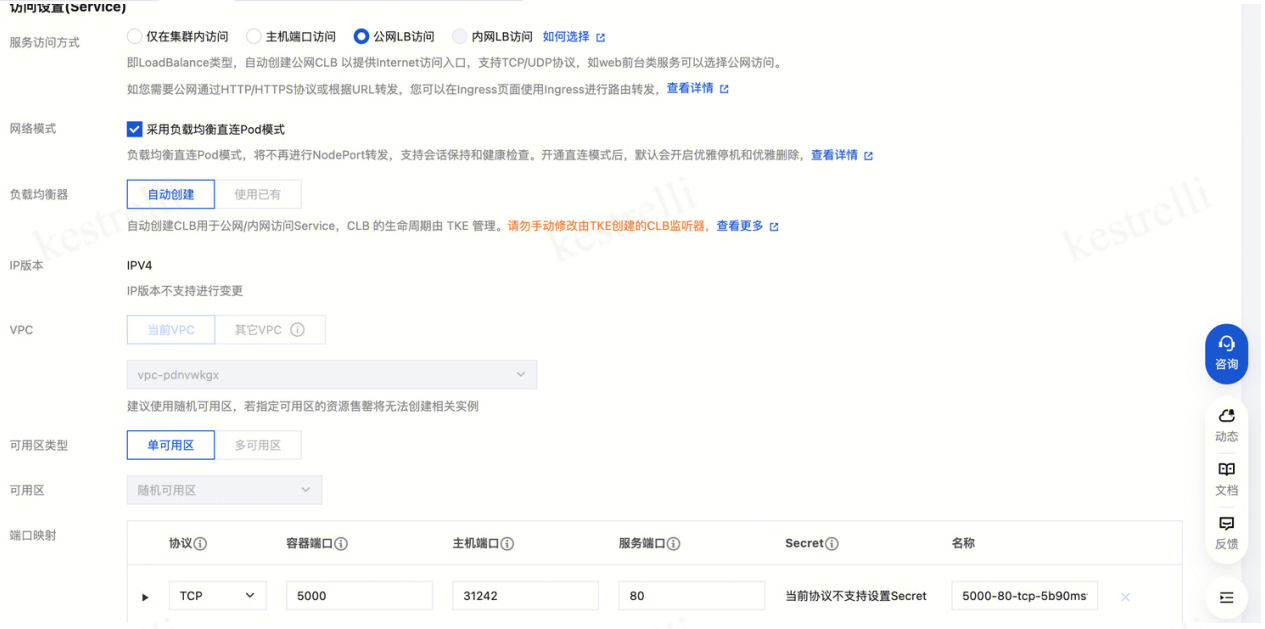
3.验证 Service 配置

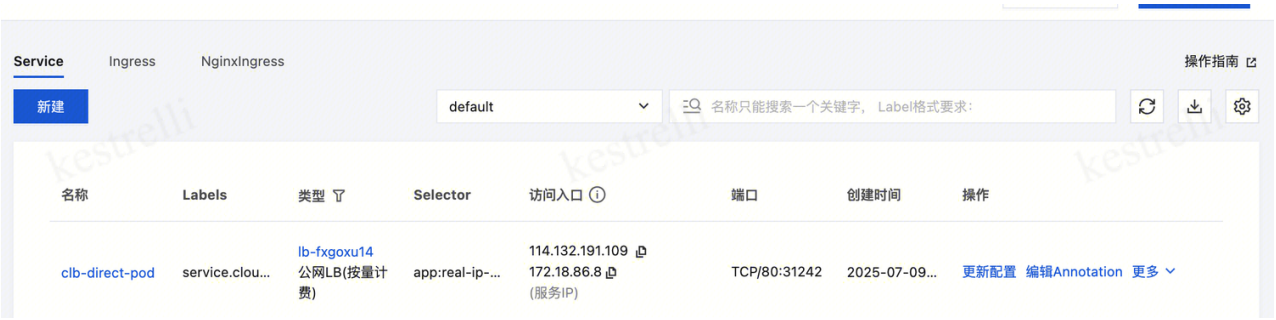
```
kubectl describe svc clb-direct-pod
```

```
[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-fxgoxu14
                          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`

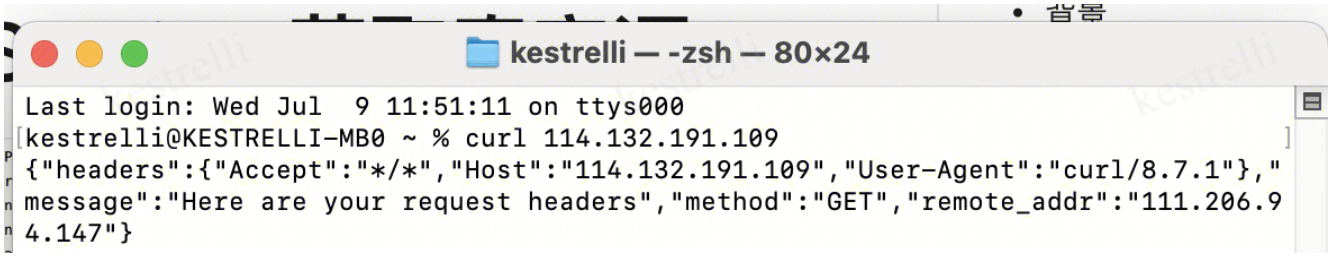




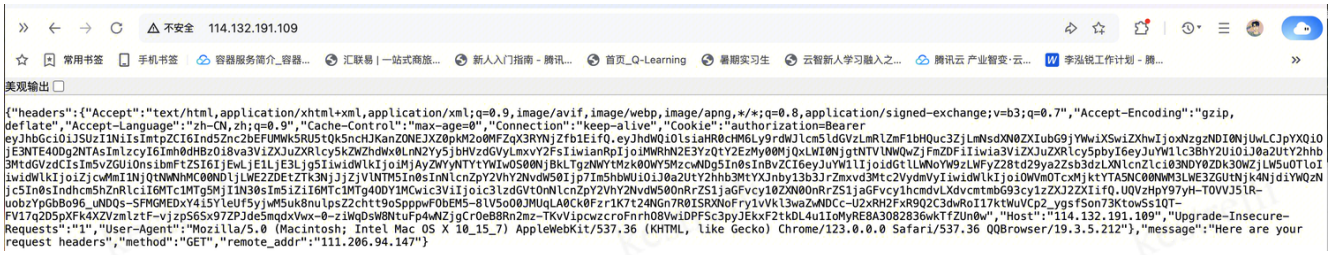
Step 3: 验证真实源 IP 获取

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 `containerPort` 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 `direct-access=true`
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

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