超级节点Pod源IP获取方案(CLB直连Pod模式) Playbook

2025-07-11 19:37

目录

适用场景：腾讯云容器服务(TKE) + 超级节点 + VPC-CNI网络
镜像版本：`vickytan-demo.tencentcloudcr.com/kestrelli/images:v1.0`(可自设镜像替换)

一、背景

当客户端通过CLB访问业务Pod时，默认请求源IP会被替换为节点IP。

本方案通过**CLB直连Pod**模式，绕过NodePort转发层，使Pod直接获取客户端真实源IP，适用于对源IP敏感的审计、风控等业务场景。

二、前置条件

1.集群环境

- 已创建TKE集群，且启用**超级节点**（控制台路径：节点管理 → 节点池 → 启用超级节点）
- 集群网络模式为 **VPC-CNI**（创建集群时需选择）

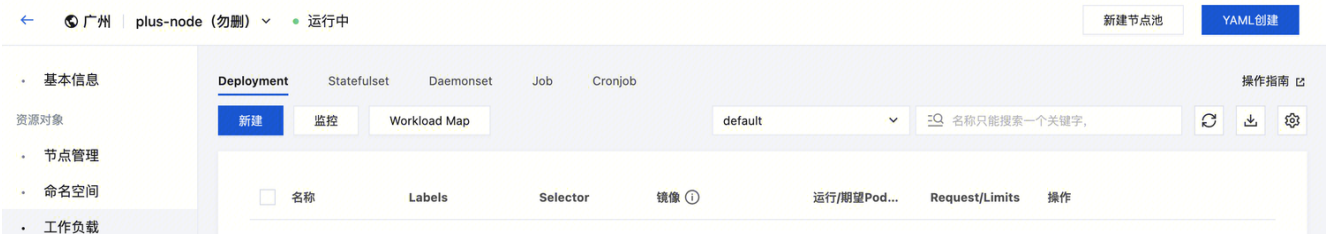
2.资源与节点限制

- 账户余额充足，无带宽限制
- 在腾讯云 TKE（Tencent Kubernetes Engine）中，超级节点（Super Node） 是一种无需用户管理节点底层资源的节点类型，它由腾讯云自动管理，用户无需登录节点本身进行操作。因此，超级节点不支持直接通过 SSH（如使用 orca term 或其他终端工具）登录到节点本身进行命令行操作。

三、操作流程

Step 1: 创建业务工作负载（Deployment）

工作负载->Deplyment->YAML新建，创建`deployment.yaml`文件



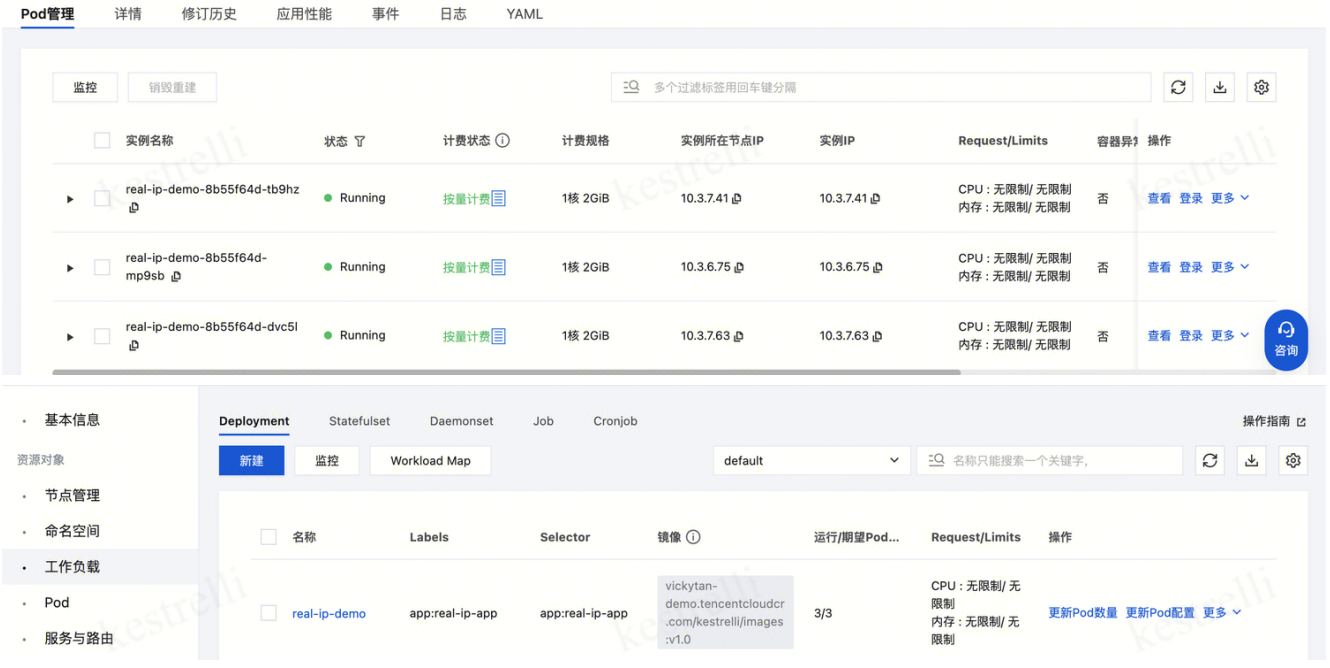
键入下面代码

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: real-ip-demo
  labels:
    app: real-ip-app  # 需与Service选择器匹配
spec:
  replicas: 3
  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  # 指定您的业务镜像
        ports:
        - containerPort: 5000  # 必须与业务实际端口一致
```

预期输出：

```
NAME  READY   STATUS    RESTARTS   AGE
real-ip-demo-xxx-xxx 1/1 Running 0 xxs
real-ip-demo-xxx-xxx 1/1 Running 0 xxs
real-ip-demo-xxx-xxx 1/1 Running 0 xxs
```

验证输出结果



Step 2: 创建直连Pod模式的Service

服务与路由->Service->YAML新建，创建`Service.yaml`文件

键入下面代码

```yaml
apiVersion: v1
kind: Service
metadata:
  name: clb-direct-pod
  annotations:
    service.cloud.tencent.com/direct-access: "true"  # 关键！启用CLB直连Pod
spec:
  type: LoadBalancer  # 公网访问
  selector:
    app: real-ip-app  # 匹配Deployment的Pod标签
  ports:
    - protocol: TCP
      port: 80          # Service对外端口
      targetPort: 5000  # 映射到Pod的业务端口
```

验证Service

Step 3: 获取CLB客户端源IP

Step 4: 验证真实源IP

1.通过curl测试

```
curl 119.91.243.11  # 替换为您的公网IP
```

预期输出：

```
{
  "headers": {
    "Accept": "*/*",
    "Host": "119.91.243.11",
    "User-Agent": "curl/8.7.1"
  },
  "message": "Here are your request headers",
  "method": "GET",
  "remote_addr": "111.206.96.146"  # 此处显示您的真实公网IP（非节点IP）
}
```

验证输出：

```
kestrelli@KESTRELLI-MB0 ~ % curl 119.91.243.11
{"headers":{"Accept":"*/*","Host":"119.91.243.11","User-Agent":"curl/8.7.1"},"message":"Here are your
 request headers","method":"GET","remote_addr":"111.206.96.144"}
```

2.通过浏览器访问

直接输入公网IP（如 `119.91.243.11`），页面将返回请求头信息，检查 `remote_addr` 是否为客户端公网IP。

四、故障排查

问题现象	排查方向
Pod状态非`Running`	1. 检查镜像地址是否正确 2. 检查 `containerPort` 是否匹配业务端口
源IP仍是节点IP	1. 确认Service注解 `direct-access: "true"`
无法访问公网IP	1. 检查安全组是否放通80端口 2. 确认账户余额/带宽未超限

五、清理资源

```
集群控制台删除Service
集群控制台删除Deployment
```