【爱卡汽车】回环问题排查

先说结论：

1.北京tke集群
1)cls-1buzjf75 使用 “externalTrafficPolicy=local ”有回环问题，并且体现出回环问题
2)cls-27hke42h 使用 “externalTrafficPolicy=cluster ”无回环问题
3)cls-37au35kt 使用 “externalTrafficPolicy=local ”有回环问题，但没有体现出回环问题，原因是 client pod 和 nginx-ingress 不在同一个节点上
2.广州tke集群:
1)cls-cq4e4na6 使用的是公网clb，无回环问题，不通的原因已排查清楚，是因为安全组设置问题

排查问题原理：

如果是内网clb(北京三个集群)：

回环触发关键点：PodA（client） -> CLB(内网) -> 节点nodeport（nginx-ingress nodeport,且节点是 PodA 所在节点 ）

为啥使用 “externalTrafficPolicy=local ”有回环问题，而使用“externalTrafficPolicy=cluster ”无回环问题？

原因：

iptables 差异：

配置了“externalTrafficPolicy=local ” 此配置后自动插入的 iptables 规则(NAT 表)：

对比不同配置的 规则发现，设置了 “externalTrafficPolicy=local ” 的节点会多出两个“ externalTrafficPolicy local” 的iptables 规则。

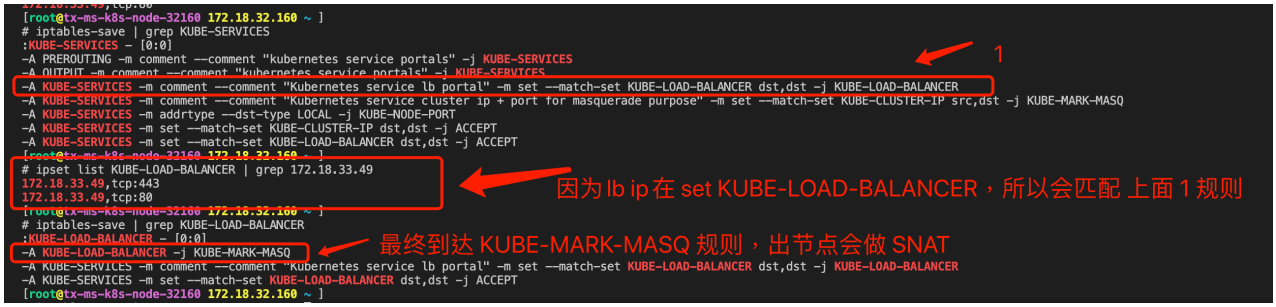
iptables 的差异如何影响 出节点 包的转发：

从iptables 规则可以看出，当要出节点时，都要先命中如下 OUTPUT chain，

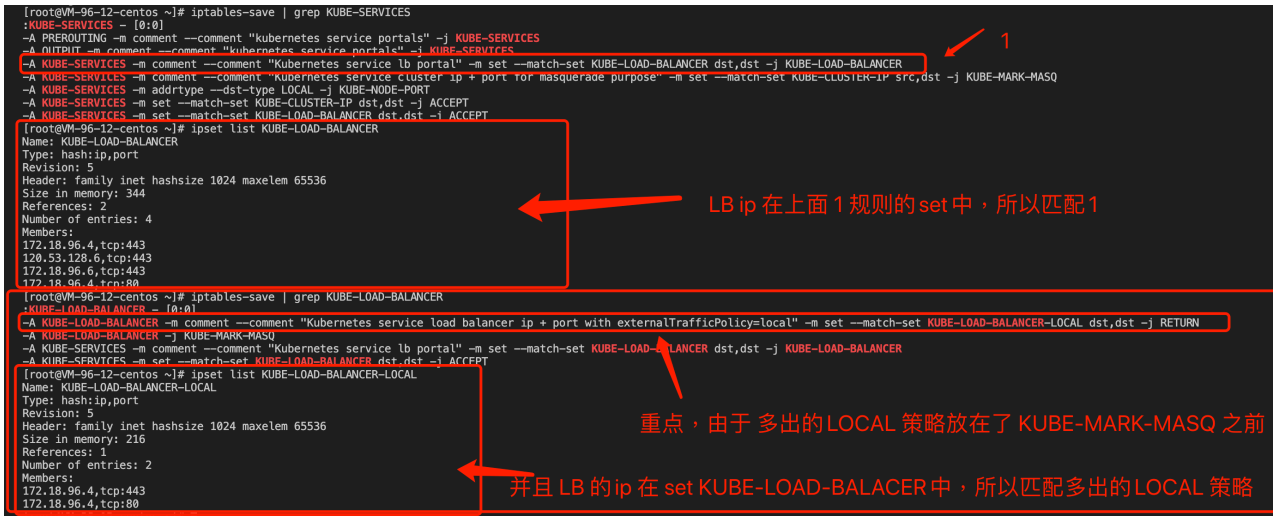
-A OUTPUT -m comment --comment "kubernetes service portals" -j KUBE-SERVICES

然后一路找转发规则就好了：

默认 “externalTrafficPolicy=cluster ” 的节点，做了SNAT 的情况：



设置了 “externalTrafficPolicy=local ” 的节点，不做SNAT 的情况：



如果是外网clb(广州tke集群) ：

本身么有回环问题，原因见材料：

CLB 回环问题总结.pdf

描述截图：

> ## 为什么公网 CLB 没这个问题?
>
> 使用公网 Ingress 和 LoadBalancer 类型公网 Service 没有回环问题，我的理解主要是公网 CLB 收到的报文源 IP 是子机的出口公网 IP，而子机内部感知不到自己的公网 IP，当报文转发回子机时，不认为公网源 IP 是本机 IP，也就不存在回环。