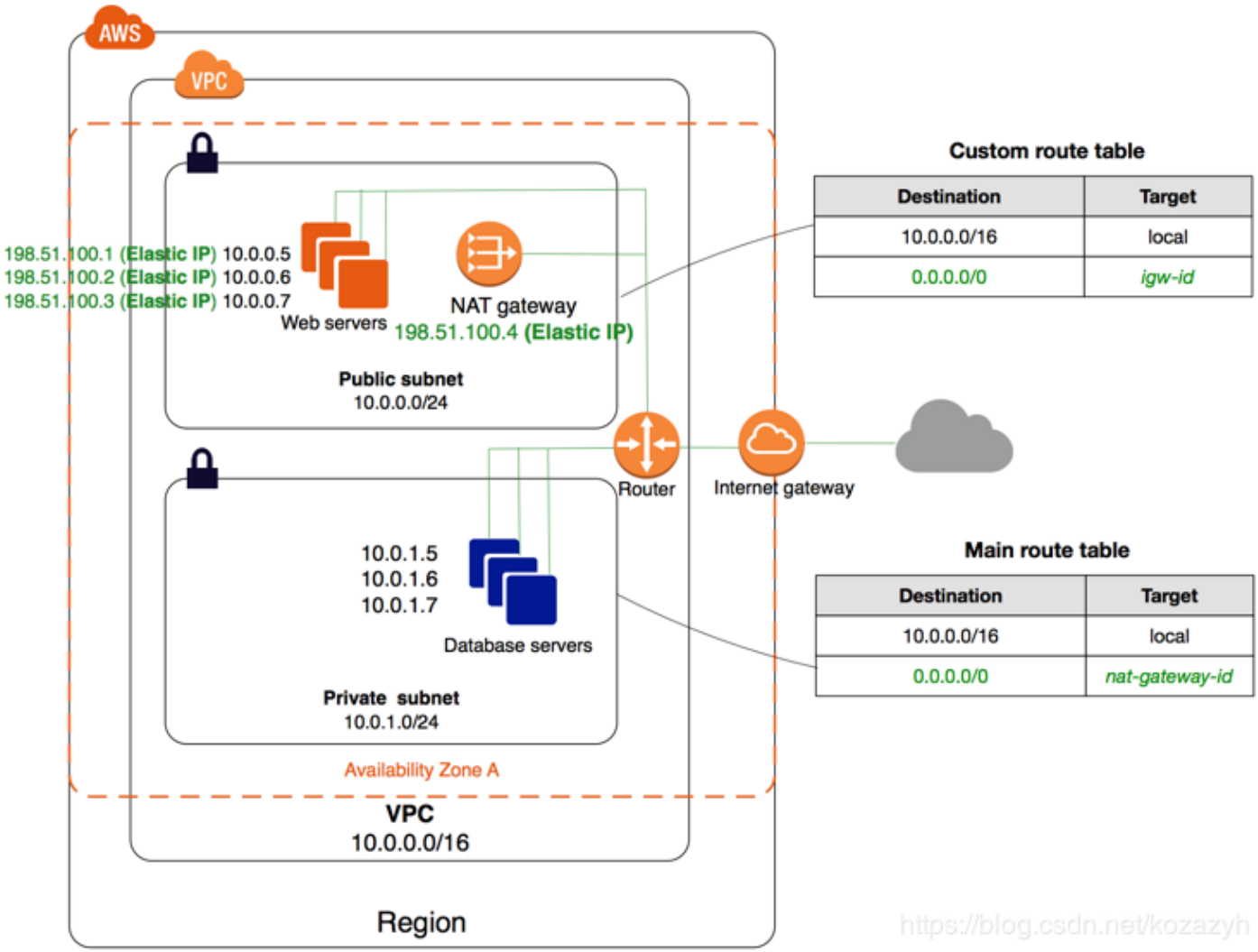
如果您希望运行面向公众的 Web 应用程序，并同时保留不可公开访问的后端服务器，我们建议您配置包括一个有公有子网和私有子网的 Virtual Private Cloud (VPC)。常用例子是一个多层网站，其 Web 服务器位于公有子网之内，数据库服务器则位于私有子网之内。您可以设置安全性和路由，以使 Web 服务器能够与数据库服务器建立通信。

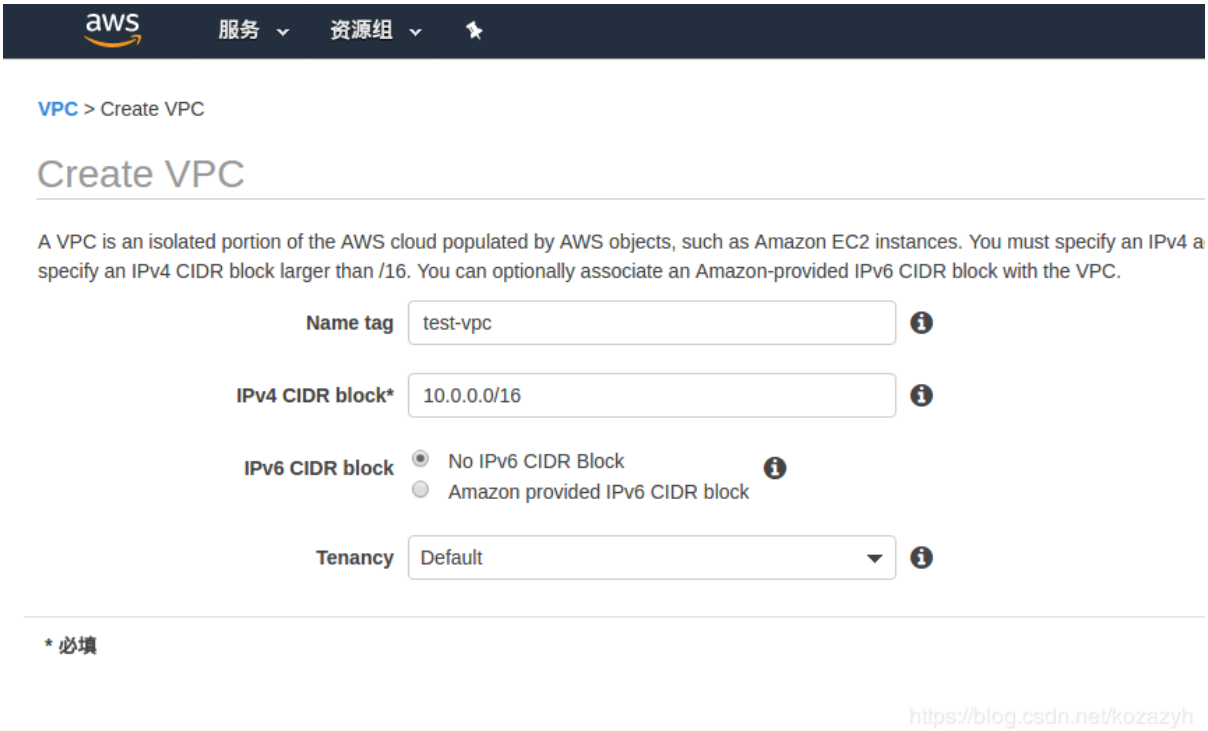
公有子网中的实例可直接将出站流量发往 Internet，而私有子网中的实例不能这样做。但是，私有子网中的实例可使用位于公有子网中的网络地址转换 (NAT) 网关访问 Internet (不建议使用NAT实例)。数据库服务器可以使用 NAT 网关连接到 Internet 进行软件更新，但 Internet 不能建立到数据库服务器的连接。

主要组成部分如下图：

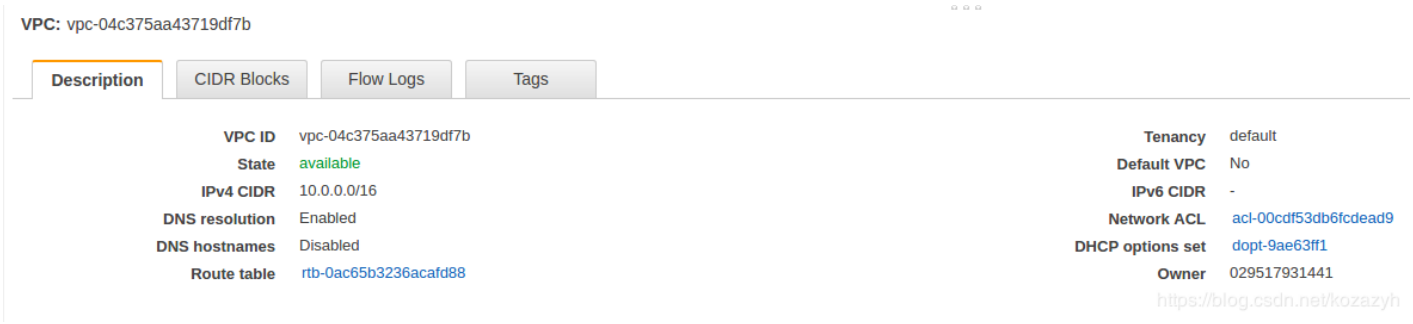


注意：NAT gateway必须位于公有子网中，否则流量不能路由到公网。

一、创建VPC



创建后的vpc信息（VPC ID：vpc-04c375aa43719df7b）

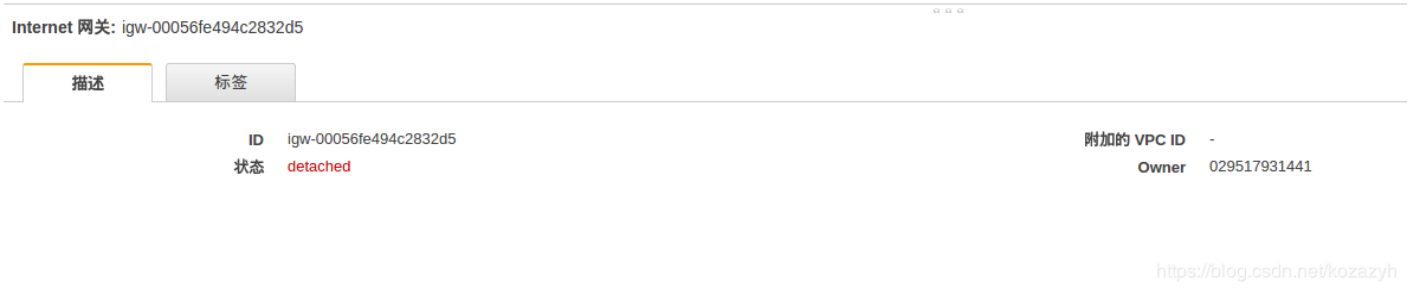


二、创建公有子网

子网ID：subnet-0fc0ea7528ef94ea9

创建Internet 网关：

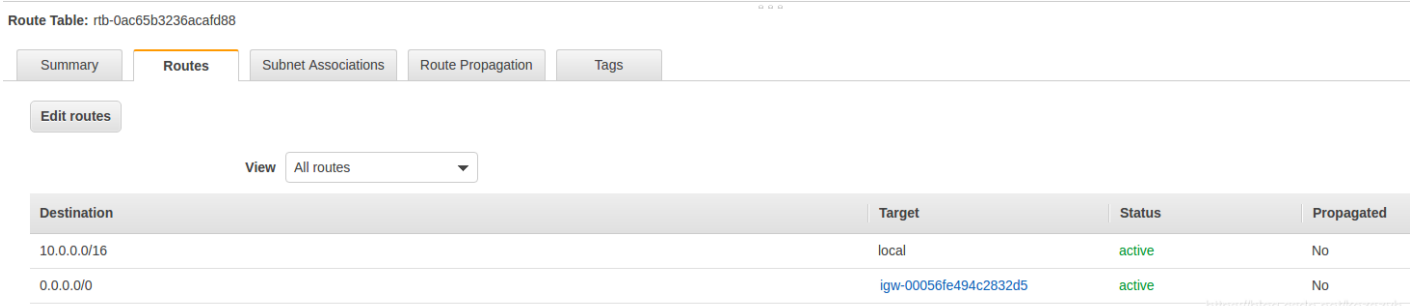
Internet 网关ID： igw-00056fe494c2832d5



把该网关附加到VPC:

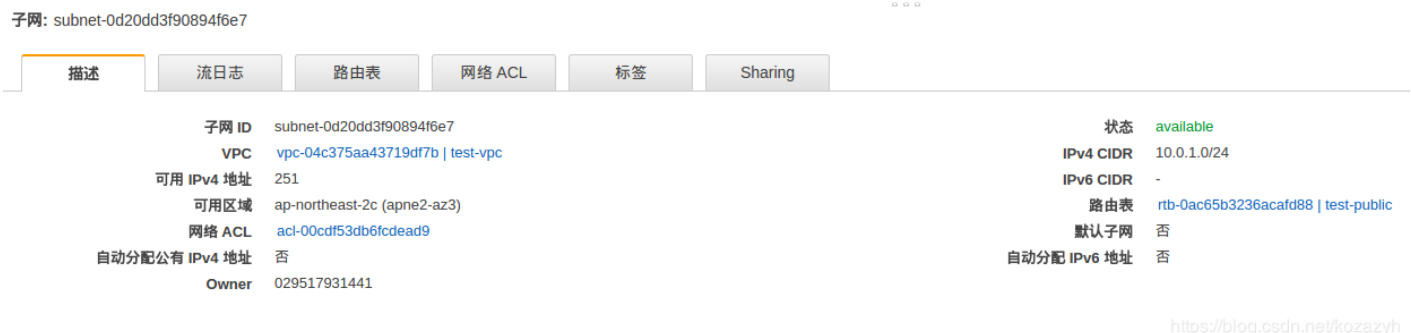
附加到vpc后,如下：

修改子网的路由表，增加缺省路由的目的为:internet 网关(igw-00056fe494c2832d5)：

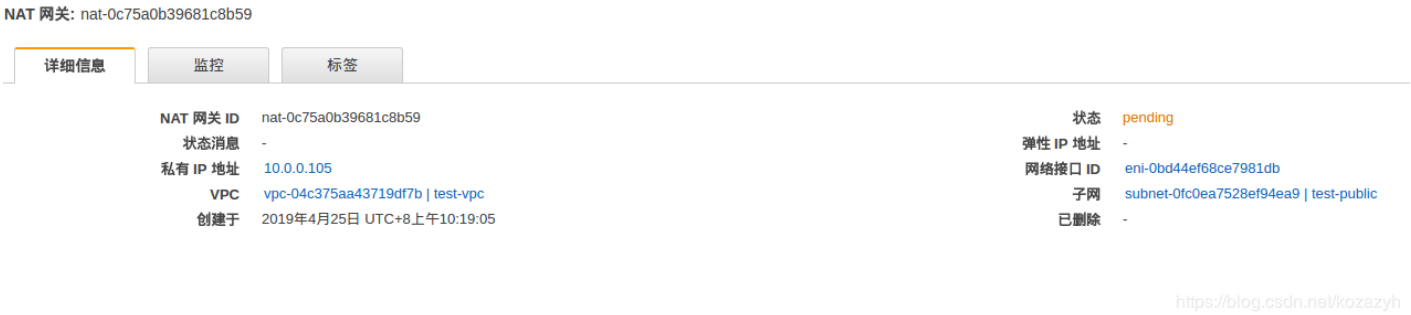


到目前位置，此公有子网下的EC2经过附加公网IP后，都可以访问互联网或从互联网访问该实例。

三、创建私有子网 （外部不能访问ec2,但是ec2可以访问互联网）

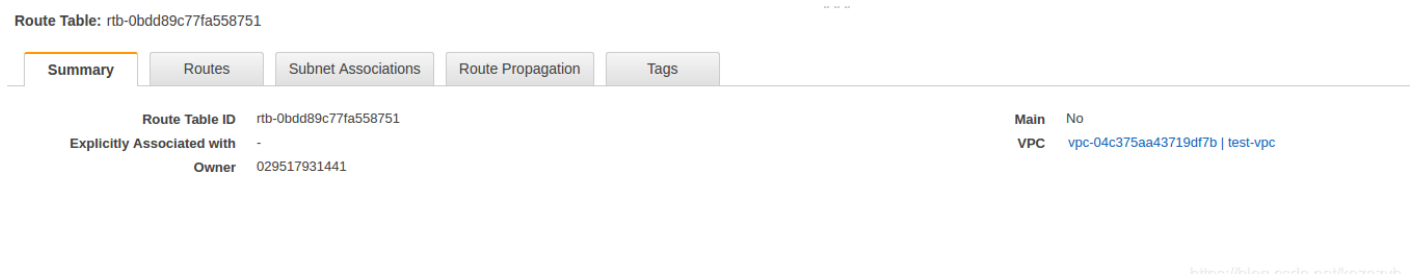


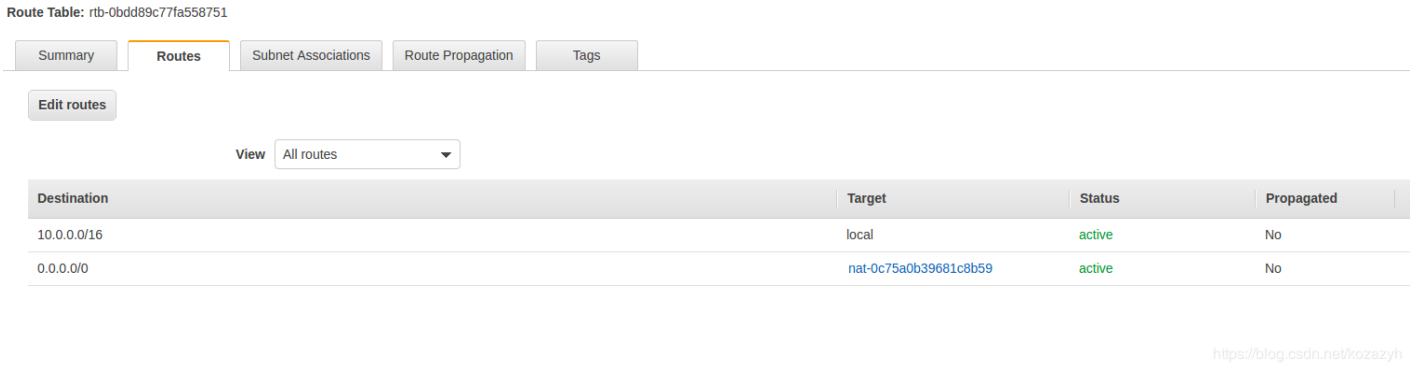
由于私有子网，需要通过NAT-网关访问外部互联网，所有我们需要创建一个NAT网关：



注意：NAT网关必须附加在上面创建的公有子网中

创建私有子网的路由，并配置该路由的缺省路由指向NAT-网关(NAT-Gateway ID: nat-0c75a0b39681c8b59)：





修改子网的路由，改为使用上面创建的路由（ROUTE ID: rtb-0bdd89c77fa558751）：

到目前位置，此私有子网下的EC2经过NAT-gateway 访问互联网，但是从互联网不能访问该实例。

参考：https://docs.aws.amazon.com/zh_cn/vpc/latest/userguide/VPC_Scenario2.html