VPC Design for Amazon Redshift

This document describes the design of a Virtual Private Cloud (VPC) for hosting Amazon Redshift. The design uses one public and one private subnet, an Internet Gateway, a NAT Gateway, separate route tables, and security groups as per the specified requirements.

# 1. VPC

• CIDR Block: 10.0.0.0/16

# 2. Subnets

• Public Subnet: 10.0.1.0/24  
• Private Subnet: 10.0.2.0/24

# 3. Gateways

• Internet Gateway (IGW): Attached to the VPC to allow public subnet access to the Internet.  
• NAT Gateway: Deployed in the public subnet to allow outbound Internet access for resources in the private subnet.

# 4. Route Tables and Associations

• Public Route Table:  
 - Associated with the public subnet (10.0.1.0/24).  
 - Route: 0.0.0.0/0 → Internet Gateway.  
  
• Private Route Table:  
 - Associated with the private subnet (10.0.2.0/24).  
 - Route: 0.0.0.0/0 → NAT Gateway.

# 5. Security Groups

• Public Security Group:  
 - Ingress: 0.0.0.0/0 (open to all IPs).  
 - Egress: 0.0.0.0/0 (all traffic allowed).  
  
• Private Security Group:  
 - Allows inbound access only from the Public Security Group.  
 - Used for Redshift cluster to ensure it is not directly exposed to the Internet.

# 6. Architecture Diagram (Description)

The VPC (10.0.0.0/16) contains two subnets:  
• Public Subnet (10.0.1.0/24): Hosts NAT Gateway and optional Bastion host.  
• Private Subnet (10.0.2.0/24): Hosts Amazon Redshift.  
  
The Internet Gateway is attached to the VPC and routes public subnet traffic. The NAT Gateway in the public subnet provides outbound access for private subnet resources. Public Route Table is associated with the public subnet, and Private Route Table is associated with the private subnet. Redshift is deployed in the private subnet with access controlled via security groups.