

2. Create Subnets

Design is to use 2 AZs for HA Route Tables

Name	VPC	AZ	IPv4 CIDR Block
10.42.4.0/27 Compute	vpc_...	us-west-2a	10.42.4.0/27
10.42.4.32/27 Compute	vpc_...	us-west-2b	10.42.4.32/27
10.42.4.64/27 Redshift	vpc_...	us-west-2a	10.42.4.64/27

3. Route Tables

- a. rt-default: (DO NOT USE): This is main route table that any subnet not assigned in VPC will be a member of. It allows routing to the defined VPC CIDR block.
- b. Rt-private: All subnets in VPC should be members of this route table.

4. IGW, Elastic IP, NAT Gateway

Not applicable. This VPC does not have Internet connectivity.

5. Endpoint

- a. Created for VPC peering to S3 bucket.
- b. Added to rt-private so instances and Redshift can reach bucket over private link
- c. Policy: default allow all

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

4.5. Set Up Security

4.5.1. NACL: Default