Assignment 2—vpc

Problem Statement: You work for XYZ Corporation, and based on the expansion requirements of your company, you have been asked to create and setup distinct Amazon VPCs for production and development teams.

You are expected to perform the following tasks for the respective VPCs: For the production network:

1. Design and build a four-tier architecture

2. Create five subnets. Among them, four should be private with names app1, app2, dbcache, and db, and the fifth one should be public with the name web

3. Launch instances in all subnets, and name them as per the subnet as they are launched in

4. Allow the dbcache instance and the app1 subnet to send Internet requests

5. Manage security groups and NACLs

6. Create a VPC Endpoint for the S3 service, and access the objects in any bucket from within the VPC

For the development network:

1. Design and build a two-tier architecture with two subnets named web and db, and launch instances in both subnets, naming them as per the subnet names

2. Make sure that only web subnet can send Internet requests

3. Create a peering connection between the production network and the development network

4. Setup a connection between the db subnets of both the production network and the development network, respectively

ANSWERS:-

VPC:

1. Design and Build a Four-Tier Architecture:

   - A typical four-tier architecture includes a web tier, app tier, caching tier, and a database tier.

2. Create Five Subnets:

   - Create five subnets with appropriate CIDR blocks:

     - Public Subnet (web)

     - Private Subnets (app1, app2, dbcache, db)

3. Launch Instances in All Subnets:

- Launch EC2 instances in each subnet and name them as per the subnet they are in. For example, an instance in the "app1" subnet can be named "App1Instance."

4. Allow Internet Requests:

   - For instances in the "app1" subnet and the "dbcache" instance to send Internet requests, you need to associate the relevant security groups and Network ACLs (NACLs). Configure the security groups to allow outgoing traffic, and adjust NACL rules accordingly.

5. Manage Security Groups and NACLs:

   - Define security groups to control inbound and outbound traffic for your instances.

   - Configure NACLs to control traffic at the subnet level.

6. Create a VPC Endpoint for S3:

   - Create a VPC endpoint for the S3 service in your VPC.

   - Ensure that the necessary routing and security group configurations are in place.

   - Instances in your VPC should be able to access objects in S3 buckets without going through the public internet.

1. Design and Build a Two-Tier Architecture:

   - Create a two-tier architecture with subnets for web and database.

2. Create Subnets and Launch Instances:

   - Create two subnets, one for the web tier and one for the database tier.

   - Launch instances in both subnets and name them according to their subnets.

3. Allow Internet Requests for the Web Subnet:

   - Configure the security groups and routing rules to allow instances in the web subnet to send Internet requests.

4. Create a Peering Connection:

   - Set up a VPC peering connection between the production network VPC and the development network VPC.

- Ensure that the routing and security group configurations allow the necessary communication between these VPCs.

5. Set Up a Connection Between Database Subnets:

- Create a connection (possibly using a peering connection) between the database subnets of both the production network and the development network.

- Configure the routing and security group settings to allow the required communication between these subnets.

********************COMPLETE THE ASSIGNMENT*************************

I HAVE SOME PROBLEM SO I AM SENDING ONLY ANSWE HOW TO DO AND STEP BY STEP