**Secure VPC Implementation on AWS**

**1. Project Overview**

1.1 Project Name

Secure VPC Implementation on AWS

1.2 Project Type

Minor Project

**2. Purpose of the Project**

The purpose of this project is to design, configure, and implement a secure Virtual Private Cloud (VPC) on Amazon Web Services (AWS). By completing this project, participants will gain practical experience in setting up a VPC with custom IP ranges, implementing network security measures, provisioning EC2 instances, configuring networking and routing, and ensuring proper access control through IAM roles and policies.


        A VPC with subnets in two Availability Zones.
      

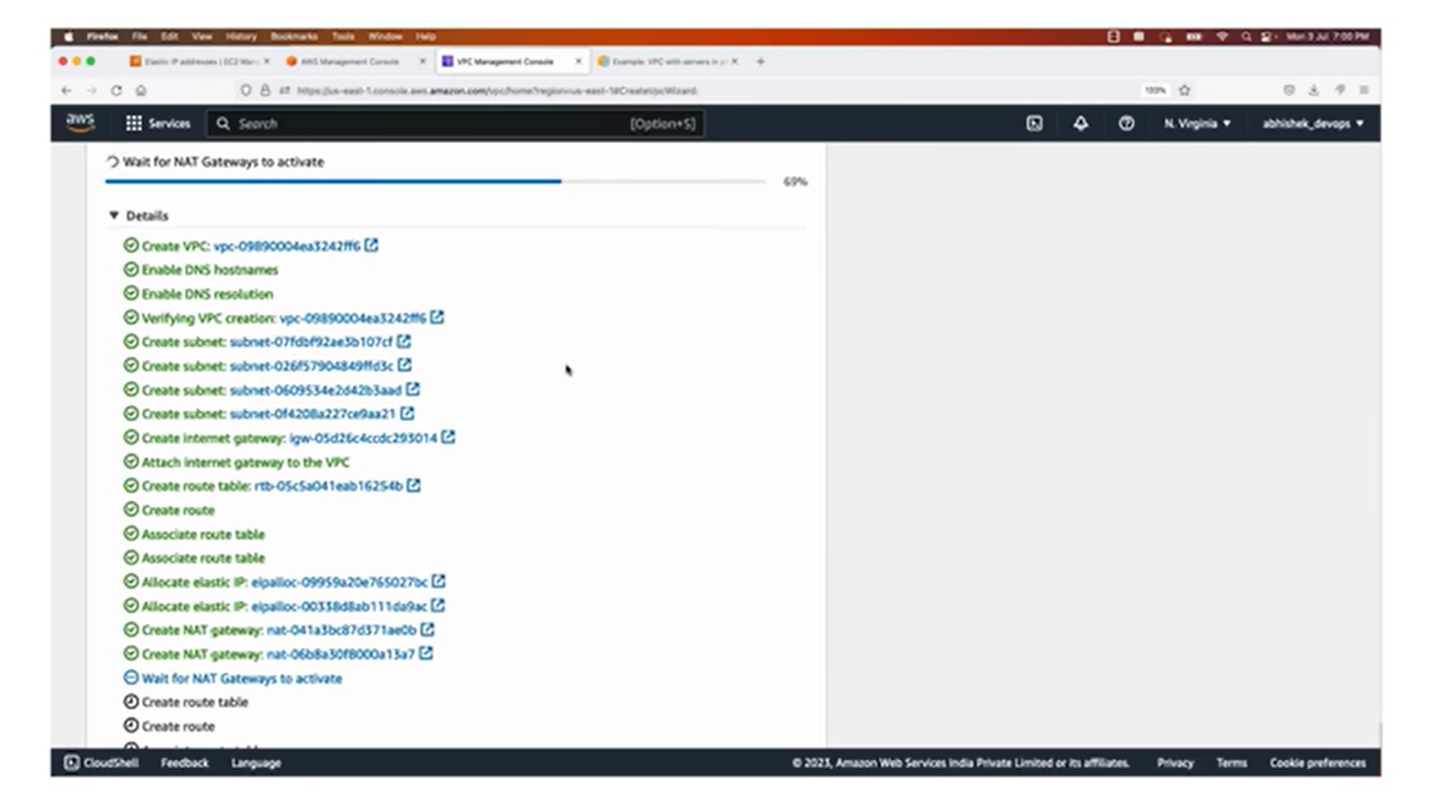
**3. Technology/Services Used**

* Amazon VPC
* Amazon EC2
* IAM (Identity and Access Management)
* Internet Gateway
* NAT Gateway or NAT Instance

**4. Implementation**

4.1 Design and Configure a VPC

* Create a VPC with custom IP ranges
* Set up public and private subnets
* Configure route tables and associate subnets



4.2 Implement Network Security

* Set up Network Access Control Lists (ACLs) to control inbound and outbound traffic
* Configure security groups for EC2 instances to allow specific ports and protocols

4.3 Provision EC2 Instances

* Launch EC2 instances in both public and private subnets
* Configure security groups for instances to allow necessary traffic
* Create and assign IAM roles to instances with appropriate permissions

4.4 Networking and Routing

* Set up an Internet Gateway for internet access in the public subnet
* Configure NAT Gateway or NAT Instance for outbound internet access in the private subnet
* Create and associate route tables with subnets

4.5 SSH Key Pair and Access Control

* Generate an SSH key pair and securely store the private key
* Configure instances to allow SSH access only with the generated key pair

4.6 Test and Validate the Setup

* SSH into EC2 instances using the private key and verify connectivity
* Test network connectivity between instances in different subnets
* Validate security group rules and Network ACL settings

**5. Challenges Faced**

* Configuring security groups and ACLs to allow the required traffic while maintaining a secure environment
* Troubleshooting and resolving connectivity issues between instances in different subnets

**6. Conclusion**

In conclusion, this project provides hands-on experience in setting up a secure VPC on AWS, covering various aspects such as custom IP ranges, network security, EC2 provisioning, networking and routing, SSH access control, and IAM roles. I gain valuable insights into designing and managing a secure and scalable infrastructure for applications hosted on AWS.

