

AWS PROJECT

Project Title – AWS Multi-Tier VPC Architecture

In this project, I have build a simple, multi-tier custom VPC in AWS. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. Also I have created a multi-tier VPC subnets. Bastion host and NAT gateway is created and private network access is done through this NAT Gateway.

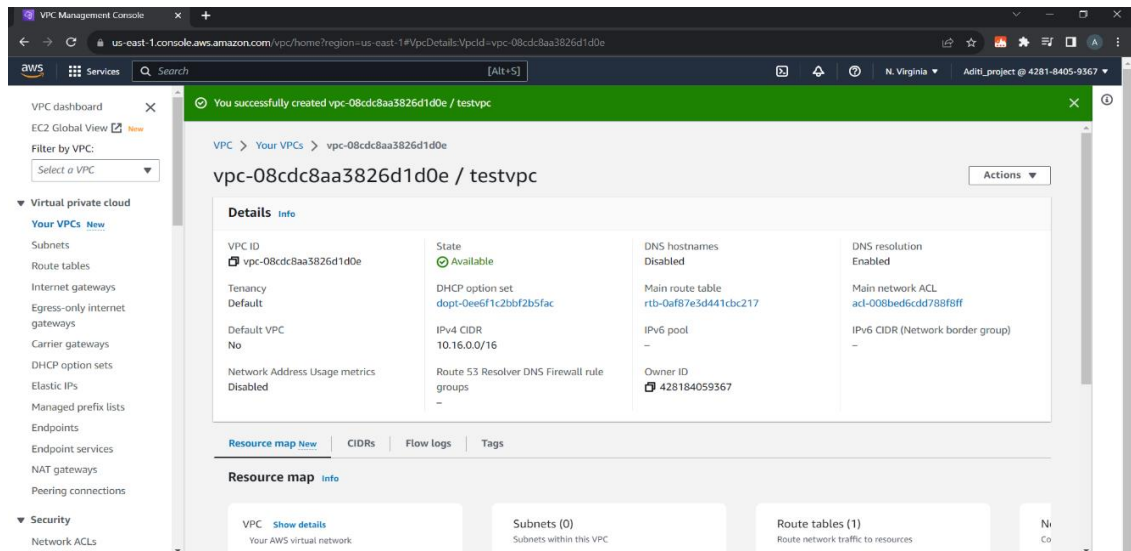
Services used-

- VPC
- Subnet
- Internet Gateway
- NAT Gateway
- Route table
- Bastion host

Steps-

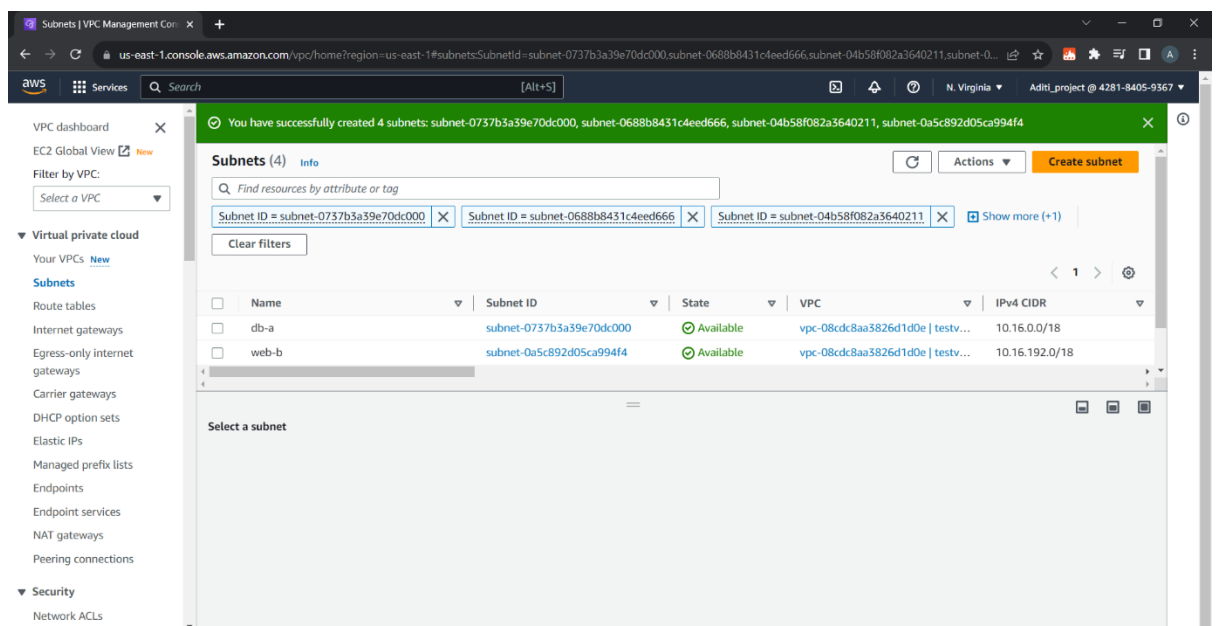
1. Create a Custom VPC

Cloud is a service used to create private networks inside AWS you can provision other services like EC2, EFS etcetera to run from a VPC. VPC are also the service used to connect your AWS private networks from your on premises network when you're creating a hybrid environment or it is a service which lets you connect your other cloud platforms, when you're creating a multi cloud deployment. for custom VPC you need to configure everything end to end in detail and there are 100% private by default. You can have multiple custom VPCs per region. You will see custom VPCs in almost all series of AWS deployment because you can configure them exactly how you need. They can be configured in a variety of sizes and structures. They can be linked with other VPC s and even configured to communicate with other cloud platforms and tear on premises networks.



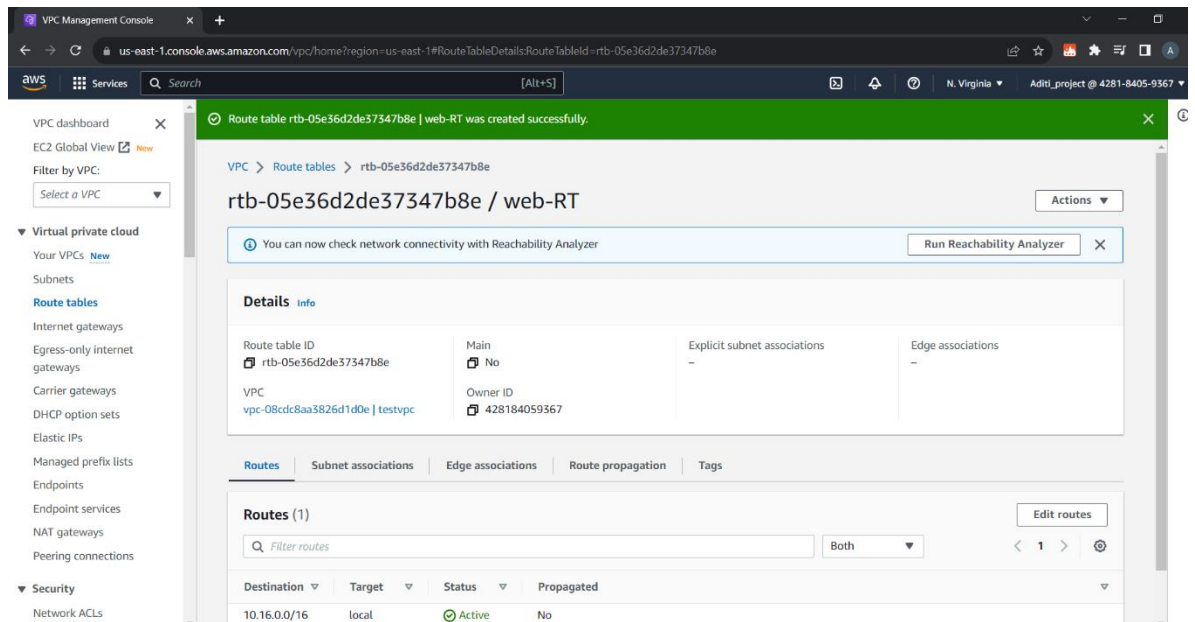
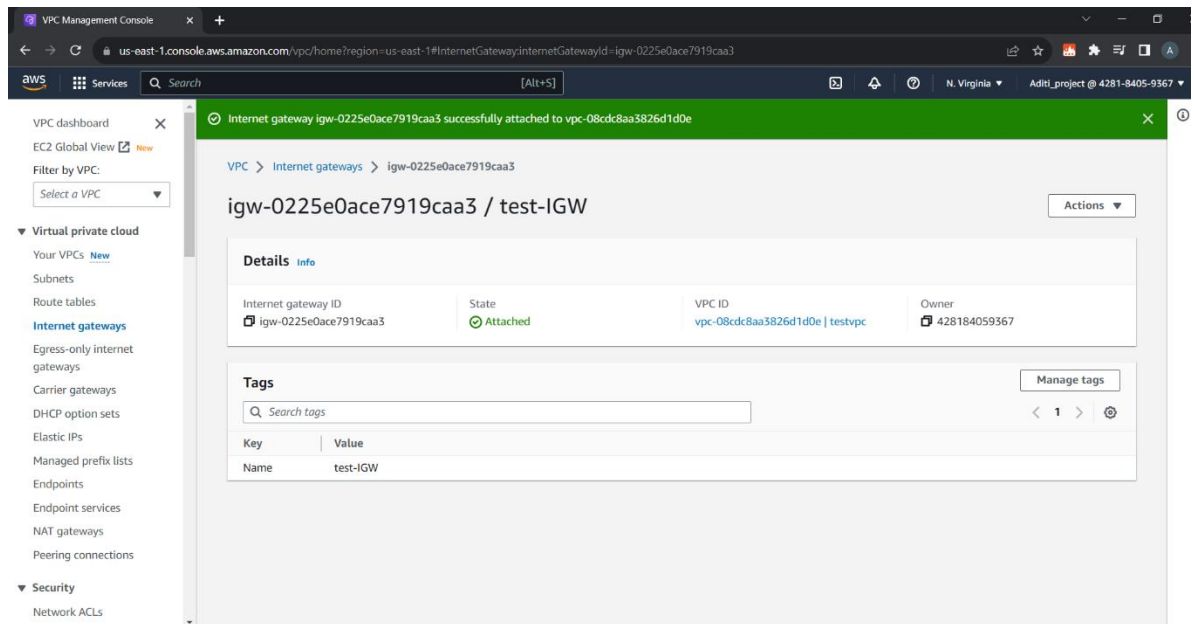
2. Implement Multi-Tier VPC subnets

In this step, I have created subnets inside a VPC. It is an availability zone resilient feature of VPC a part of VPC that is inside a specific availability zone, it is the place from which the devices we are going to deploy inside the VPC will run from, It is created within one availability zone and it can never be changed. Subnets cannot span across different availability zones. There are two availability zone A and B. And I have created a private and the public subnets inside an availability zone. I have created two database subnet and two web subnet.



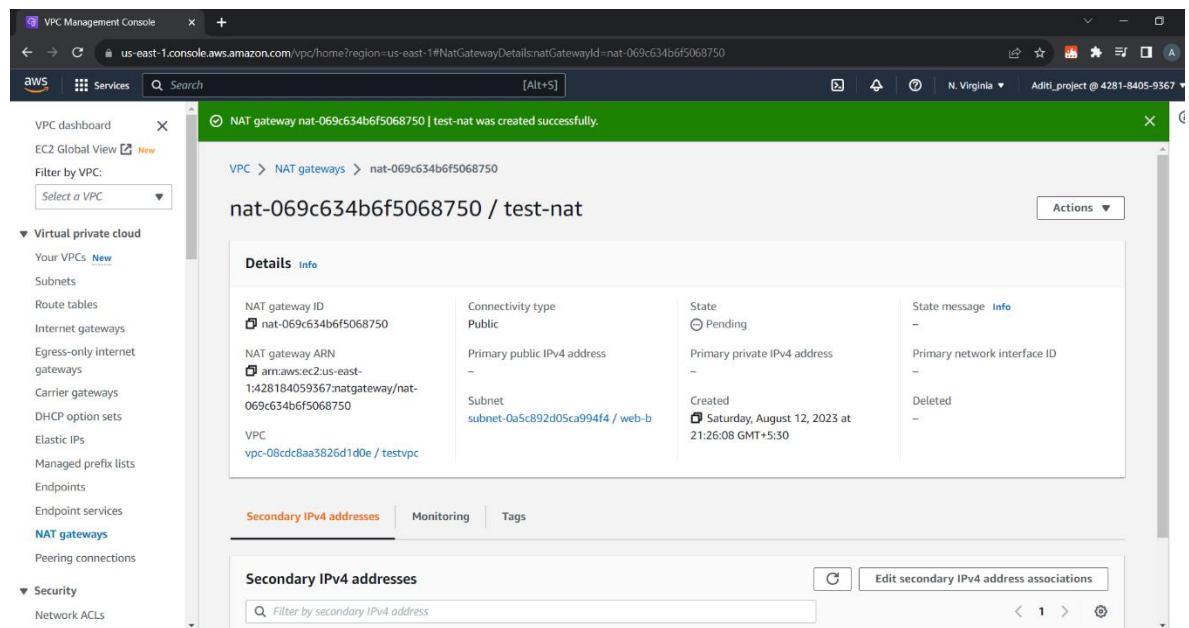
3. Configuring one tier in VPC to be public

I have created an internet gateway and attached it to the VPC. Just by attaching an internet gateway to the VPC doesn't mean that the subnets inside the VPC will be public for that. You need a round table. So if you want to make the web -tier public, i.e. if the device is you're going to deploy inside this web tier want to communicate to and from internet, you need to create a round table for the same and you need to configure the routes and attach it to the VPC. So I have created a route table and attached it to the VPC. The route table will decide where the traffic should go when it leaves a particular subnet.



4. Configure Network Address Translation (NAT) Gateway

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.



5. Access Private instance through Bastion Host

A bastion host is a server used to manage access to an internal or private network from an external network - sometimes called a jump box or jump server. Because bastion hosts often sit on the Internet, they typically run a minimum amount of services in order to reduce their attack surface. They are also commonly used to proxy and log communications, such as SSH sessions.

