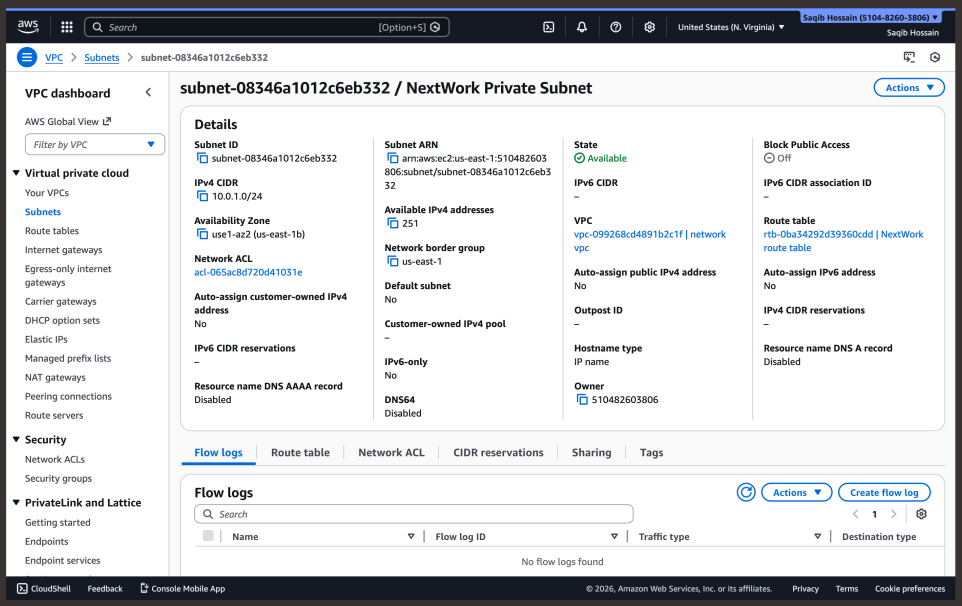
nextwork.org

Creating a Private Subnet

saqibh49@gmail.com



saqibh49@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual network in AWS that lets you create an isolated cloud environment to launch and manage your resources, and it is useful because it gives you control over IP addressing, subnets, routing, and security to protect and organize your infrastructure.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet, along with a route table, and network ACL.

One thing I didn't expect in this project was...

One thing I didn't expect in this project is that a private subnet is exactly the same as apublic subnet, just without the internet gateway.

This project took me...

This project took me 30 minutes

saqibh49@gmail.com
NextWork Student

Private vs Public Subnets

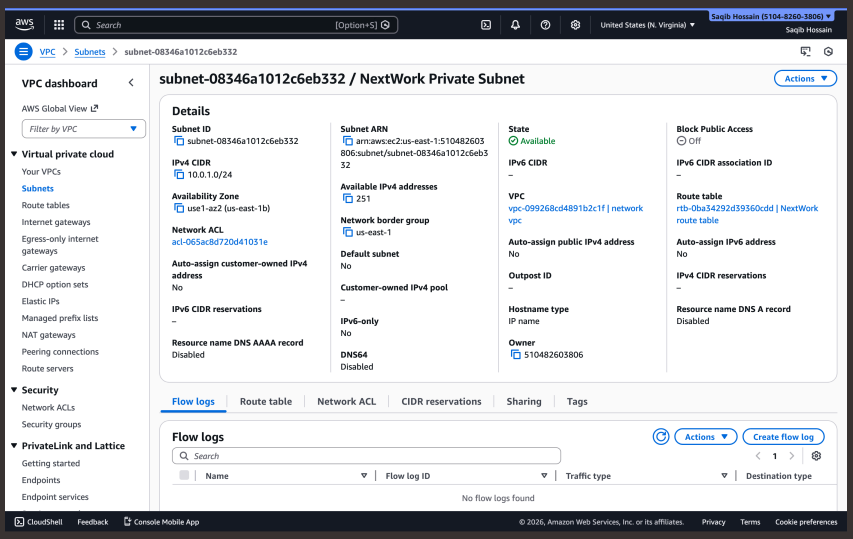
The difference between public and private subnets is that private subnets do not have an internet gateway connected to their route tables, so outside access is not allowed or possible. Public subnets have an internet gateway attached to their route table so outside internet access is available.

Having private subnets are useful because they work as the backend for the frontend parts of VPC housed in oublic subnets. For example, an S3 site might be stored in a public subnet, but all the customer data might be stored in a private subnet.

My private and public subnets cannot have the same CIDR blocks.

saqibh49@gmail.com
NextWork Student

nextwork.org



A dedicated route table

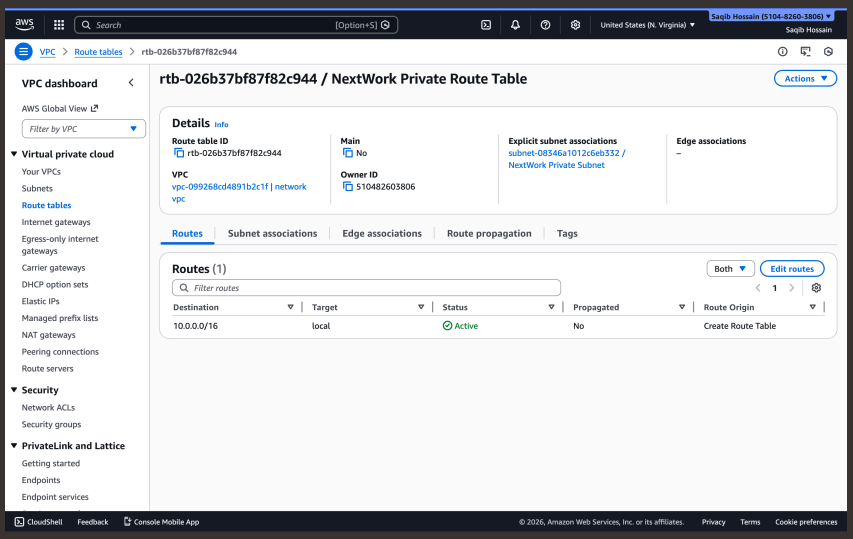
By default, my private subnet is associated with the prublic route table I built earlier, or if no route tables built by me exist, then it will use the default one that AWS includes in the account.

I had to set up a new route table because the public route table has a connection to an internet gateway, but the private subnet needs to be self contained so only internal traffic gets through.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic, nothing from the internet

saqibh49@gmail.com
NextWork Student

nextwork.org



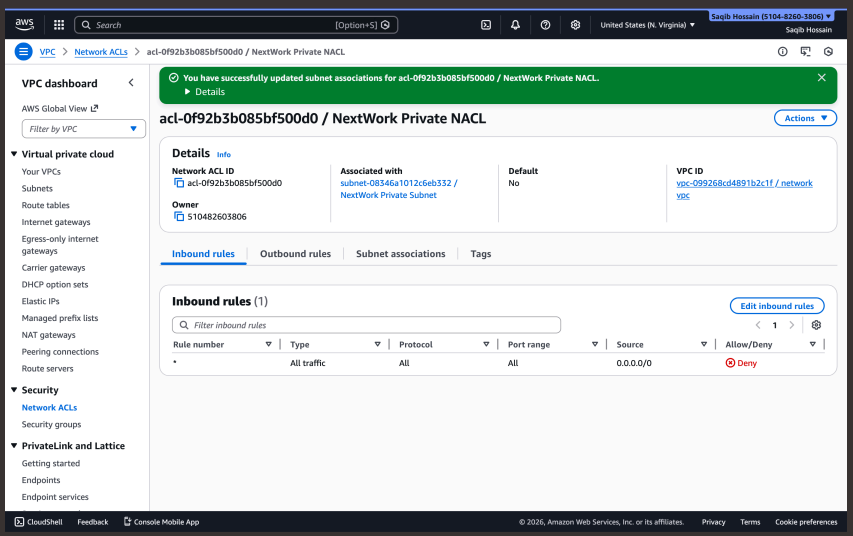
saqibh49@gmail.com
NextWork Student

A new network ACL

By default, my private subnet is associated with the Network ACL associated with your private route subnet by default is the VPC's default Network ACL, which automatically allows all inbound and outbound traffic unless you modify it.

I set up a dedicated network ACL for my private subnet because this acts as an extra form of security alongside the route table not being connected to an internet gateway.

My new network ACL has two simple rules - All inbound traffic is blocked, and all outbound traffic is blocked.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects