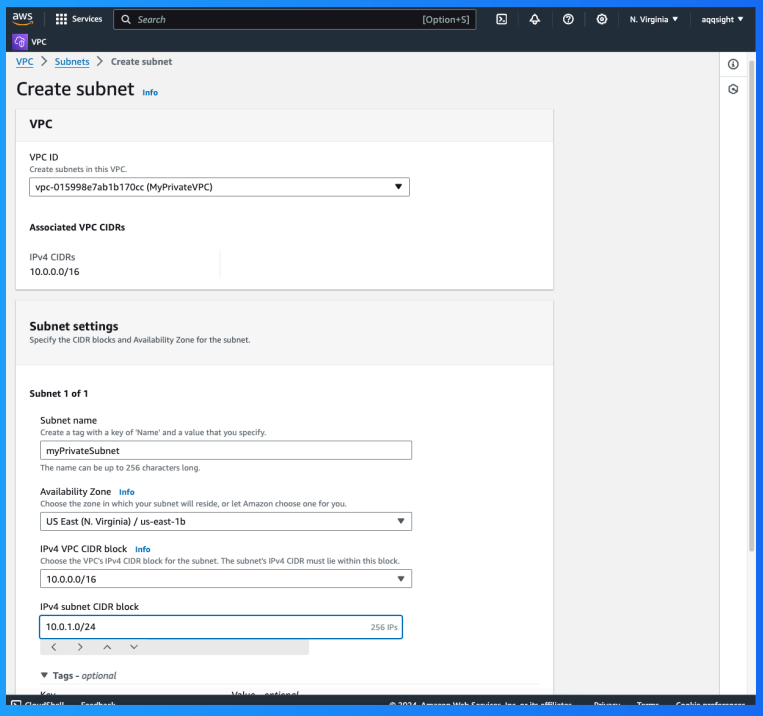
NextWork.org

Creating a Private Subnet

AL alexten3517@gmail.com



AL
alexten3517@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

An Amazon VPC is useful for keeping specific resources at a private level. And not allowing any intrusion to those resources That is not permissioned. This VPC is used to keep specific resources safe.

How I used Amazon VPC in this project

I used it to practice the creation of an IGW, a route table, a NACL and a subnet at a public and private level.

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

I did not expect to truly understand how creating VPC's is really so much fun while educating myself.

This project took me...

I spent about 30 min on this project.

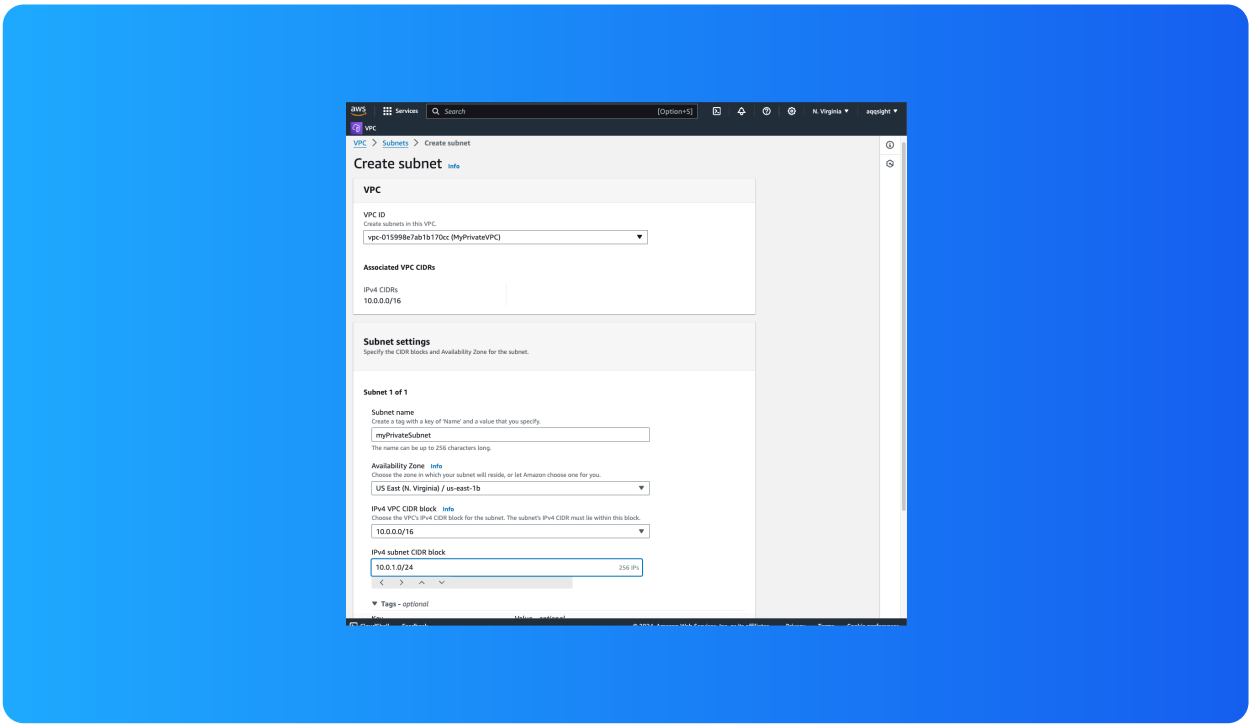
AL
alexten3517@gmail.com
NextWork Student

Private vs Public Subnets

A private subnet allows you to keep resources at a resource level private. It allows us to keep our resources isolated from the internet by default.

Having private subnets are useful because they keep certain resources away from the internet and the security of confidential resources.

My private and public subnets same cannot share the same IPv4 CIDR block i.e the same IP addresses. The CIDR block must be unique and cannot overlap with another subnet.



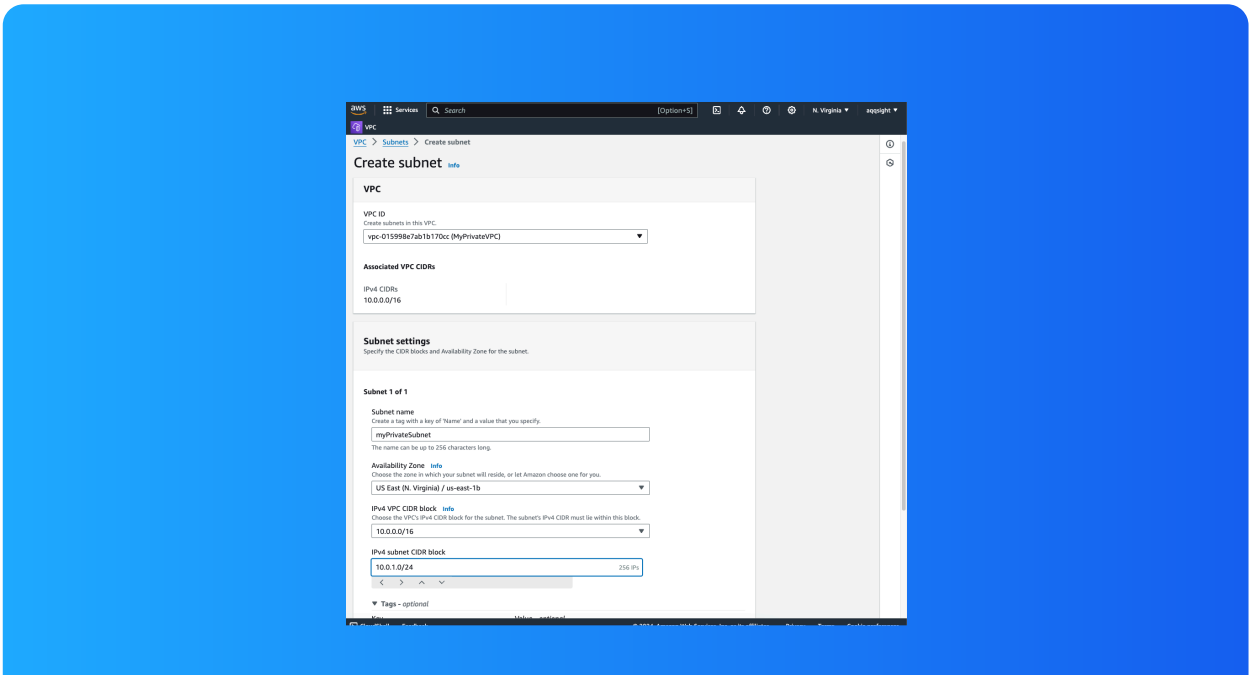
AL
alexten3517@gmail.com
NextWork Student

A dedicated route table

By default, my private subnet is associated with my private route table to allow only specific traffic.It's set for only one inbound and outbound rule.

I had to set up a new route table to allow traffic to reach only resources in my private subnet. Public traffic will not have access to my private subnet due to the new route table.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows only specific traffic to reach the resources that it is set up to reach. This helps prevent unauthorized access and potential security breaches.



A new network ACL

By default, my private subnet is associated with associated with my NACL that is set up for every VPC created in my AWS account.

I set up a dedicated network ACL for my private subnet because this NACL is going to protect my private subnet and at its resources. This private VPC will hold resources that can only be accessed through permissioned protocols.

My new network ACL has two simple rules, to deny all inbound and outbound traffic. This addional layer of security keeps all outside intrusion from getting access to my private VPC.