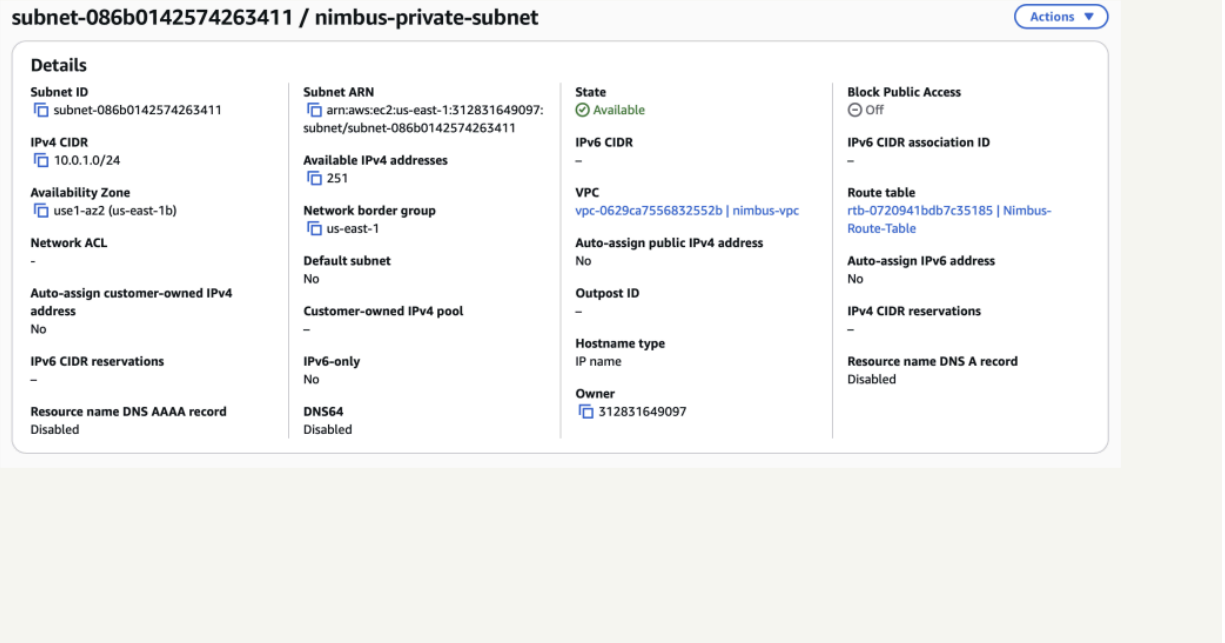
Creating a Private Subnet

Erik Gonzalez



Introducing Today's Project!

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create subnets, routing tables, inbound/outbound rules etc..

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

One thing I didn't expect in this project is how a VPC is already created when setting up an AWS account.

This project took me...

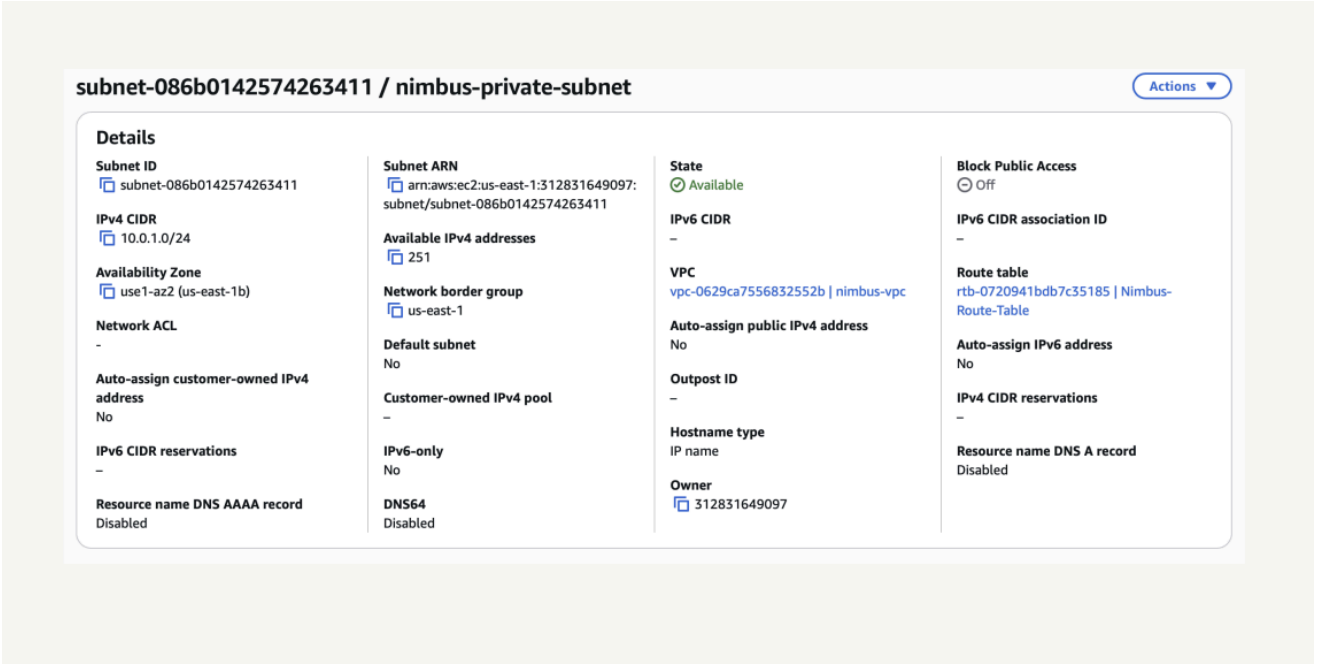
This project took me about one hour to complete.

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet, while private subnets can be completely isolated from the internet.

Having private subnets is useful because keeping resources away from the internet is extremely important for security and confidential resources/data.

My private and public subnets cannot have the same IPv4 CIDR Block i.e. the same range of IP addresses. The CIDR block for every subnet must be unique so as to not cause any overlap.

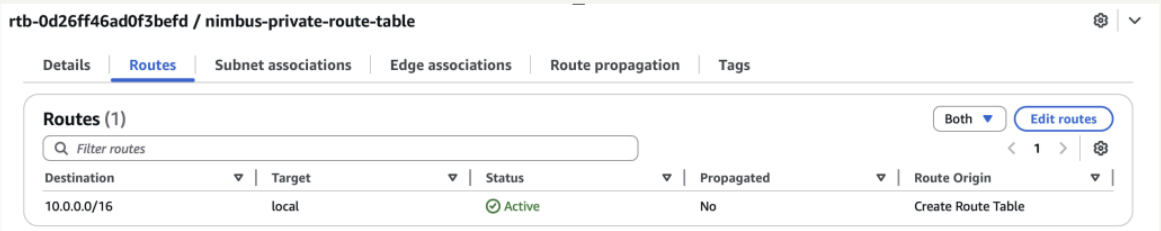


A Dedicated Route Table

By default, my private subnet is associated with the default route table i.e. a route table that has a route to the internet gateway.

I had to set up a new route table because my subnet can't have a route to an internet gateway.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal communication i.e. with another destination of another resource within my VPC.



A New Network ACL

By default, my private subnet is associated with the default network ACL that's set up for every VPC created in my AWS account.

I set up a dedicated network ACL for my private subnet because a network ACL becomes crucial in the event of security breaches—where traffic that has compromised my public subnet could access my private subnet if my network ACL rules allow all inbound and outbound traffic.

My new network ACL has two simple rules - deny all inbound traffic and deny all outbound traffic.