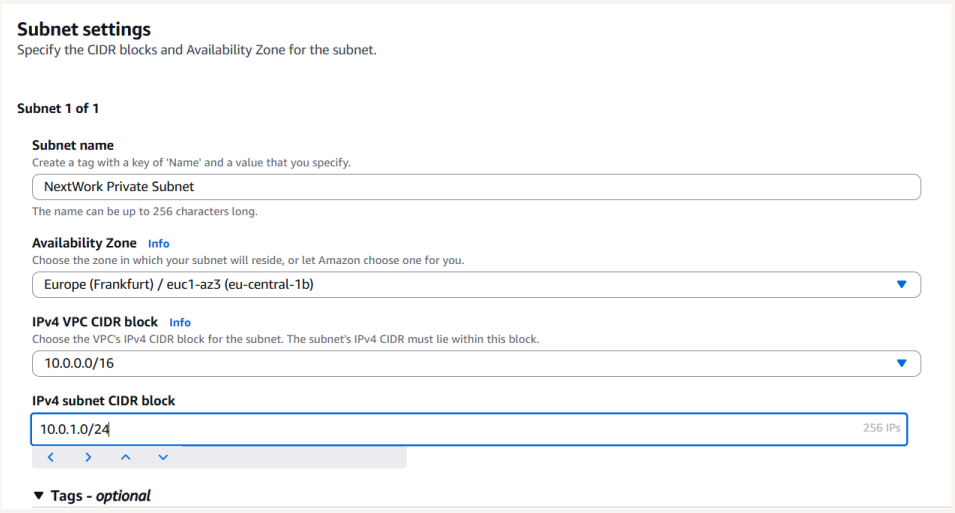
nextwork.org

Creating a Private Subnet

SH shilpa_i_kale@yahoo.com



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is an isolated or private section of the entire AWS. It is useful because resource deployed in VPC are private to the account and cannot be accessed by outside world.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet.

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

One thing I didn't expect in this project is the the IPv4 CIDR block range should be different for each subnet.

This project took me...

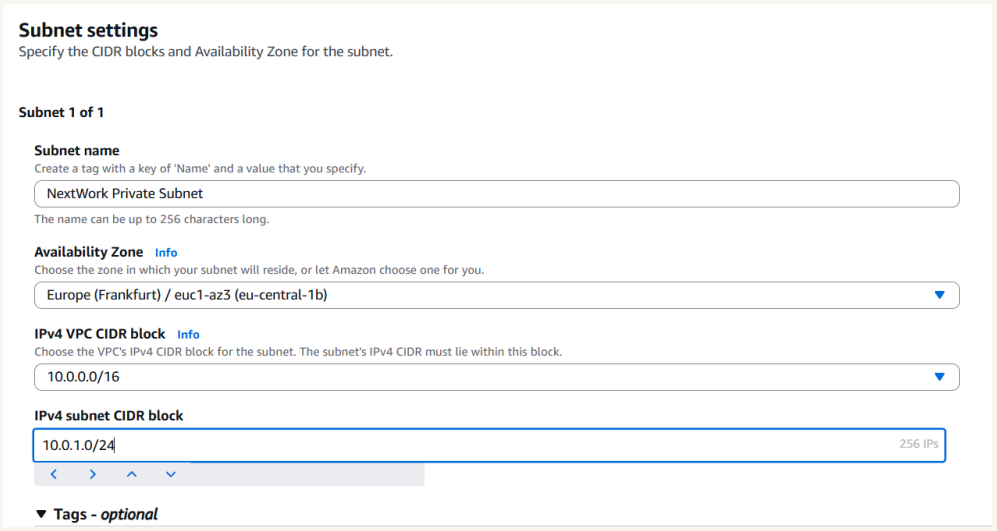
This project took me 2 hrs including demo, documentation and understanding the concept.

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 are completely isolated from internet by default.

Having private subnets are useful because keeping resources away from the internet is extremely important for confidential resources.

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 and cannot overlap with another subnet.

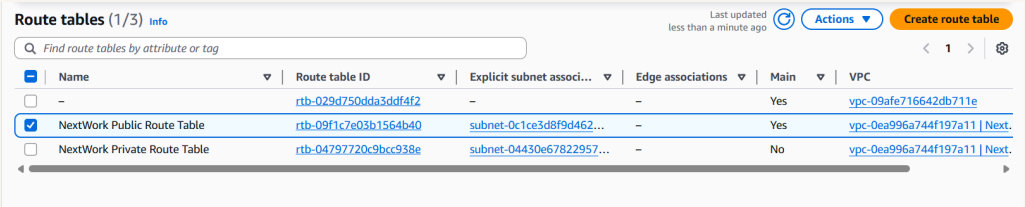

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Europe (Frankfurt) / euc1-az3 (eu-central-1b)
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.1.0/24
256 IPs
Tags - optional

A dedicated route table

By default, my private subnet is associated with default route table of VPC which has access to internet through internet gateway.

I had to set up a new route table because my default route table had access to internet through internet gateway. I wanted to have only private access.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic inside VPC.



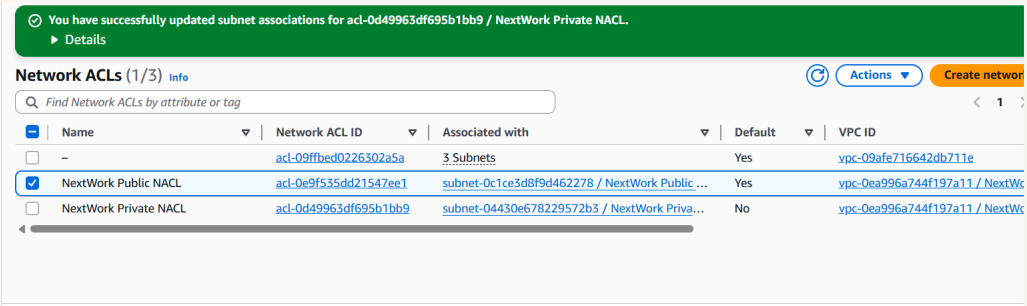
SH
shilpa_i_kale@yahoo.c...
NextWork Student

A new network ACL

By default, my private subnet is associated with the default Network ACL of VPC.

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 can get access to my private subnet if I've network ACL allowing traffi

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



The place to learn & showcase your skills

Check out nextwork.org for more projects