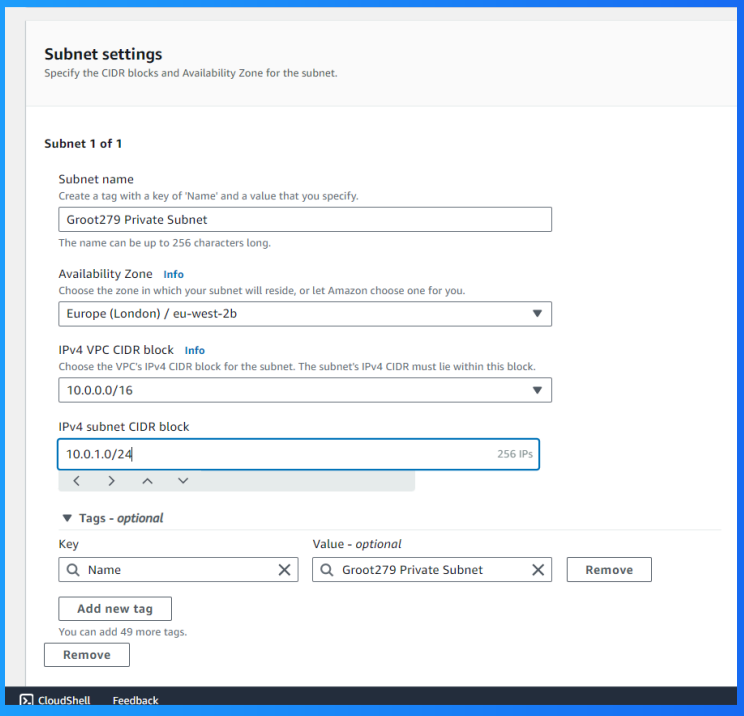
NextWork.org

Creating a Private Subnet

TA tahirgroot@gmail.com



TA
tahirgroot@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a virtual network service that allows you to launch AWS resources in a logically isolated virtual network that you define.

How I used Amazon VPC in this project

Create a VPC to house all resources for the application, providing a secure and segregated network environment

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

default nacls in private subnet

This project took me...

1 hour

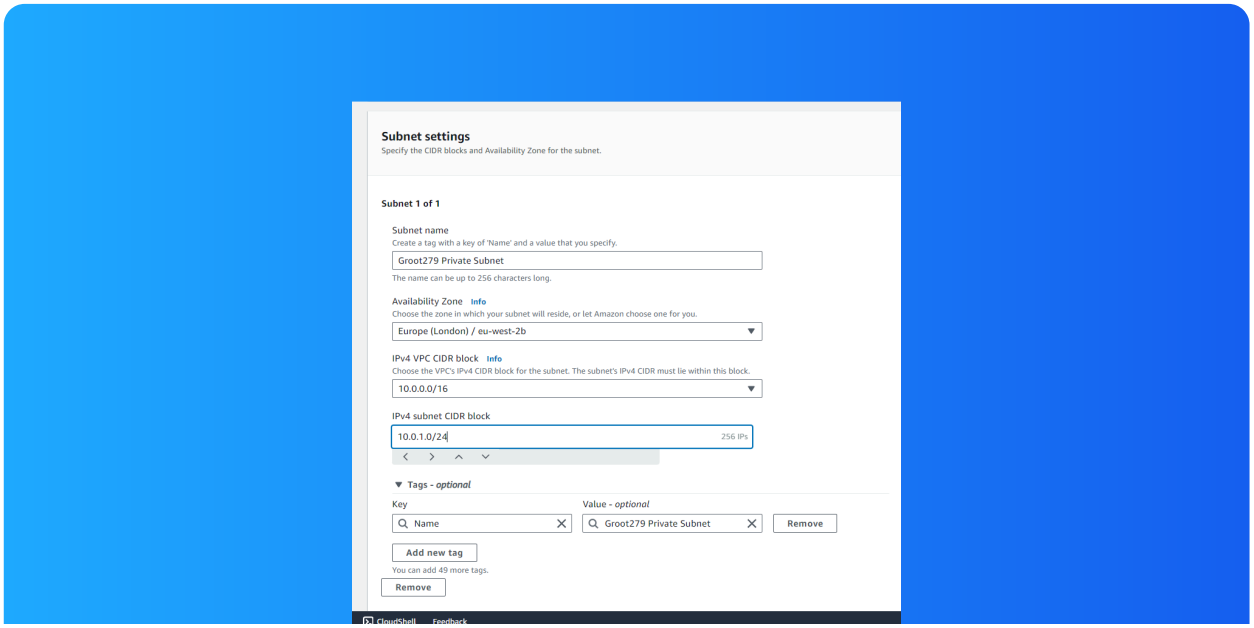
TA
tahirgroot@gmail.com
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have a direct route to the internet, allowing resources within them to be accessed publicly, while private subnets lack this route, requiring a NAT gateway for internet access

Having private subnets are useful because they provide a secure environment for internal resources, protecting them from external threats. By isolating sensitive data and applications, organizations can reduce the risk of unauthorized access and data

My private and public subnets cannot have the same IP address range. Overlapping IP addresses would cause routing conflicts and prevent proper communication between devices within each subnet.

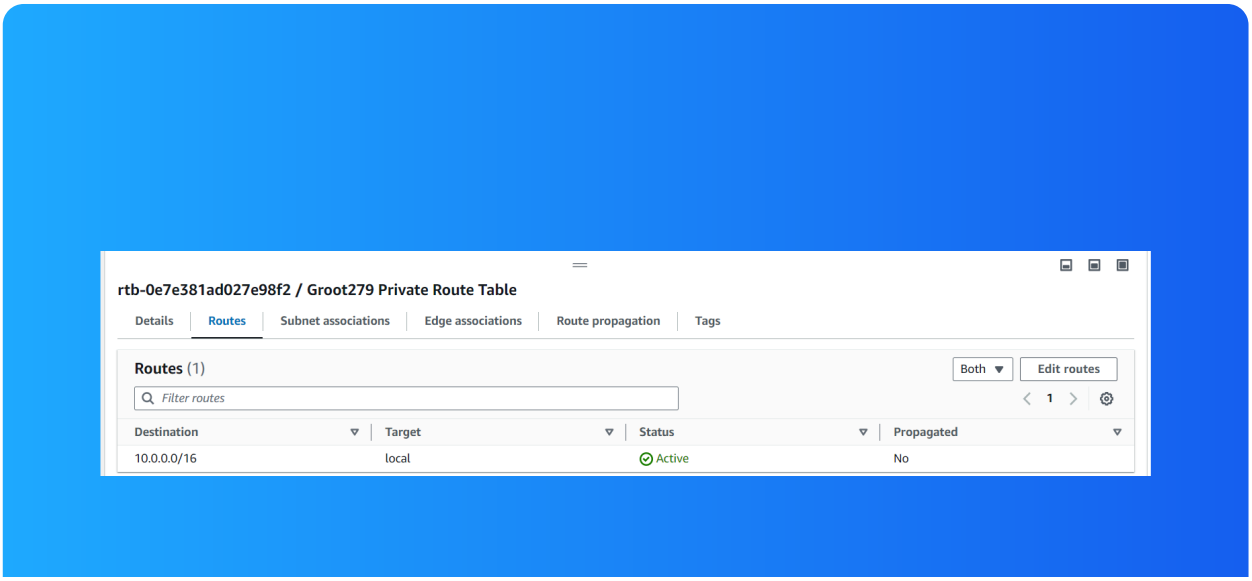


A dedicated route table

By default, my private subnet is associated with the main route table. This table contains default routes for traffic within the VPC and can be modified to direct traffic to other resources or gateways.

I had to set up a new route table because I needed to implement specific routing rules for a particular subnet or group of subnets. This allows me to control traffic flow, isolate resources, and enhance security by defining custom routes.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic to and from the NAT gateway, enabling internet access for resources within the private subnet while maintaining isolation from the public.

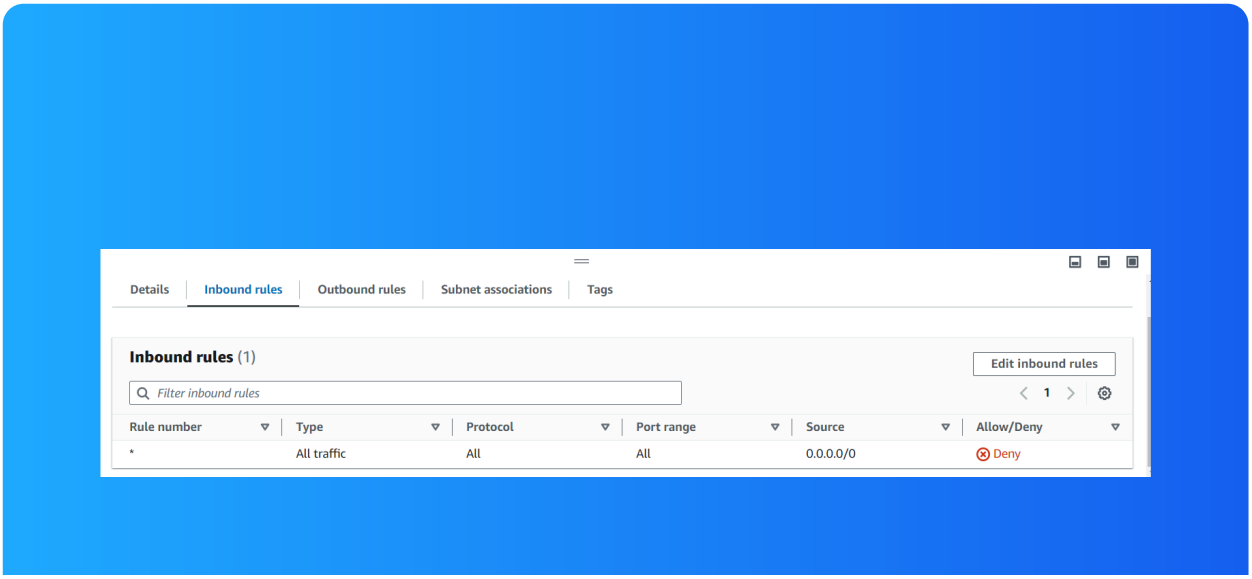


A new network ACL

By default, my private subnet is associated with the default network ACL for the VPC. This ACL typically allows all inbound and outbound traffic, but it's recommended to create a custom ACL with more restrictive rules for enhanced security.

I set up a dedicated network ACL for my private subnet because it provides an additional layer of security by controlling inbound and outbound traffic at the subnet level. This allows me to define granular rules for allowed and denied traffic.

My new network ACL has two simple rules - one inbound rule allowing SSH traffic from my specific IP address for initial configuration, and one outbound rule permitting all traffic to ensure connectivity while I finalize the security configuration.



Everyone should be in a job they love.

Check out nextwork.org for more projects