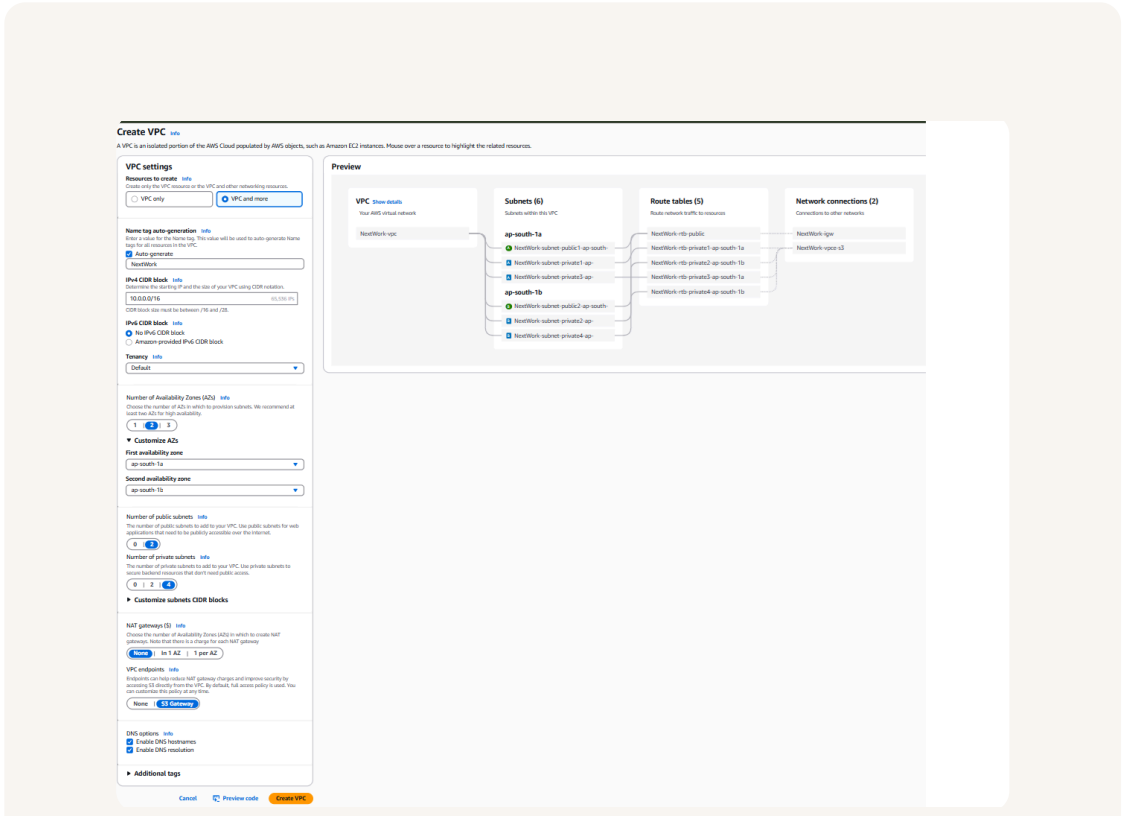
nextwork.org

Launching VPC Resources

Sanjana Tripathy



Sanjana Tripathy
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you launch AWS resources in a secure, isolated network you define. It gives control over IP ranges, subnets, route tables, and gateways, enabling you to securely build and manage cloud infrastructure.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to quickly set up a secure network with public and private subnets. I launched instances in each, configured route tables and gateways, enabling isolated access control.

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

One thing I didn't expect in this project was being able to complete a full VPC setup—subnets, route tables, gateways, and more—in just a few minutes. I was excited to see how seamlessly AWS enables quick and secure network configuration.

This project took me...

This project took me approximately 3 hours to complete, including setting up the VPC, configuring subnets, route tables, gateways, and security components, along with reviewing and validating each step for a clear understanding.


Sanjana Tripathy
NextWork Student

Setting Up Direct VM Access

Directly accessing an EC2 instance means logging into its operating system via SSH or RDP to perform admin-level tasks like installing software or running scripts. Unlike the AWS Console, this gives you full control for deep configuration.

SSH is a key method for directly accessing a VM

SSH (Secure Shell) is a secure protocol used to remotely access and manage servers over a network. It encrypts the connection, allowing users to safely run commands, transfer files, and configure systems like EC2 instances from their local machines.

To enable direct access, I set up key pairs

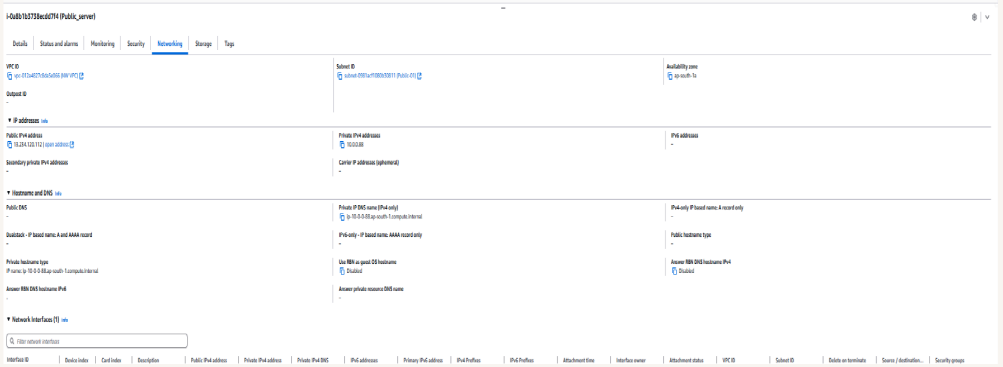
A key pair in AWS is a set of two cryptographic keys: a public key and a private key. The public key is stored by AWS, while the private key is downloaded by the user and used to securely connect (SSH) to EC2 instances.

A private key is usually stored in PEM format with a .pem file extension. This format is widely used for SSH access to EC2 instances. In my case, the private key was in .pem format, which is required for Linux-based EC2 connections using SSH.

Sanjana Tripathy
NextWork Student

Launching a public server

By default, all resources are launched into the default VPC that AWS has set up for your account. So to change that, I had to change my EC2 instance's networking settings by selecting the VPC,subnet and security group(Firewall) which I created.

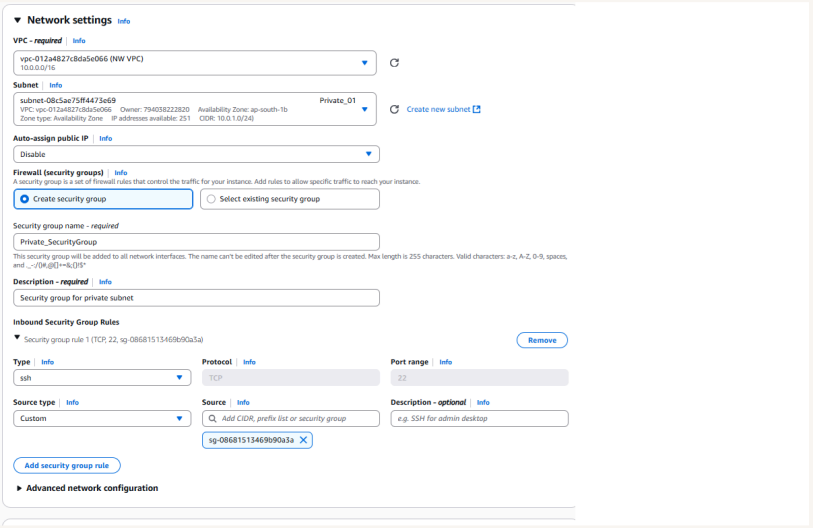


Sanjana Tripathy
NextWork Student

Launching a private server

The private server uses a different security group from the one used by the public subnet's instances(NZ_SecurityGroup_Public) This limits access, allowing only trusted internal communication and blocking public internet traffic for added security.

My new security group's source is the NZ_SecurityGroup_Public.This means only instances associated with that public security group can send traffic to the private instance, ensuring secure, internal communication only.



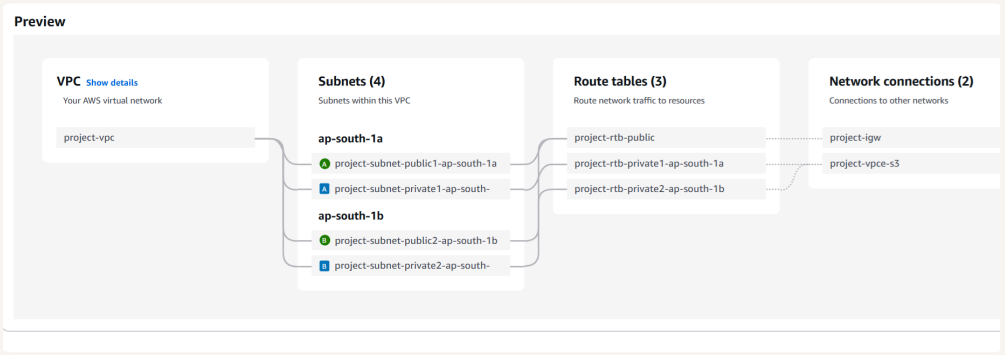
Sanjana Tripathy
NextWork Student

Speeding up VPC creation

I set up my new VPC using the Launch Instance wizard, which allowed me to configure the VPC, subnets, route tables, and security settings all in one place—quickly setting up a complete VPC environment without switching pages.

A VPC resource map is a visual diagram in the AWS Console that shows all the components inside your VPC—like subnets, route tables, internet gateways, NAT gateways, and more—and how they're connected.

My new VPC can have the same IPv4 CIDR block as the NextWork VPC because VPCs are isolated from each other. Even with overlapping IP ranges, they don't conflict unless connected (like through peering), where unique CIDRs are then required.



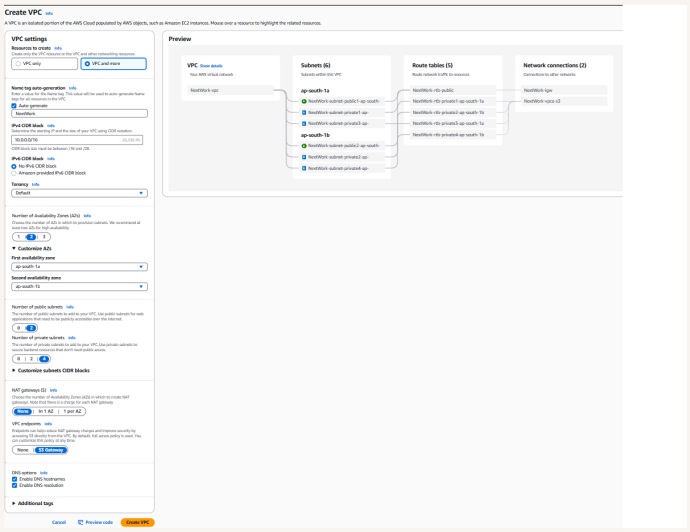
Sanjana Tripathy
NextWork Student

Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options because I selected two Availability Zones during setup. AWS creates one public subnet per AZ to ensure high availability and redundancy, following best practices.

NAT gateways allow instances in private subnets to access the internet for updates or downloads, while preventing inbound traffic from reaching them. This keeps resources secure while enabling necessary outbound communication.



The place to learn & showcase your skills

Check out nextwork.org for more projects