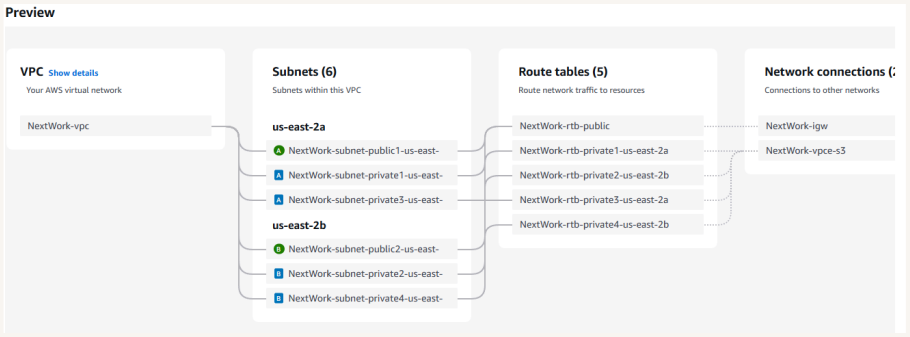
nextwork.org

Launching VPC Resources

Joba Amunigun
https://www.linkedin.com/in/dvoice



Joba Amunigun
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a private, customizable network inside AWS where I can launch and manage cloud resources securely. It’s useful because it gives me full control over my network architecture — including IP address ranges, subnets, route tables, internet access, and security. I get to decide how traffic flows, who can access what, and what stays private or public.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a complete network setup from scratch using the “VPC and more” option in the AWS Console. I launched a new VPC with: 1 public subnet and 1 private subnet A shared route table An internet gateway for public access And custom CIDR blocks for each subnet Using the VPC resource map, I could visualize all my components in one place — making it easier to configure everything in a structured, beginner-friendly way.

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

One thing I didn’t expect was how helpful the VPC resource map would be during setup. It gave me a clear, real-time visual of every component — subnets, route tables, internet gateway — all on one screen. Instead of jumping between pages, I could see how everything connected before hitting "Create."

Joba Amunigun
NextWork Student

This project took me...

This project took me about 60 minutes — including time spent exploring the VPC resource map, configuring subnets, and double-checking CIDR blocks and routing setup.

Joba Amunigun
NextWork Student

Setting Up Direct VM Access

Directly accessing a virtual machine means connecting to your EC2 instance through the command line (usually via SSH), so you can log in, configure, and interact with the server just like you would if it were physically in front of you. This access gives you full control to run commands, install software, check logs, and manage the machine — all from your terminal.

SSH is a key method for directly accessing a VM

SSH traffic means a secure, encrypted connection between your computer and a remote server — like your EC2 instance. SSH stands for Secure Shell, and it's the protocol used to log in to a remote machine using a key pair. When I connect via SSH, AWS checks that I have the private key that matches the public key stored on the instance — only then does it allow access

To enable direct access, I set up key pairs

Key pairs are a set of two linked cryptographic keys — one public and one private — that AWS uses to securely connect you to your EC2 instance. When you launch an instance, AWS stores the public key, and you keep the private key file (usually a .pem file). You use this private key to SSH into your EC2 instance without needing a password.

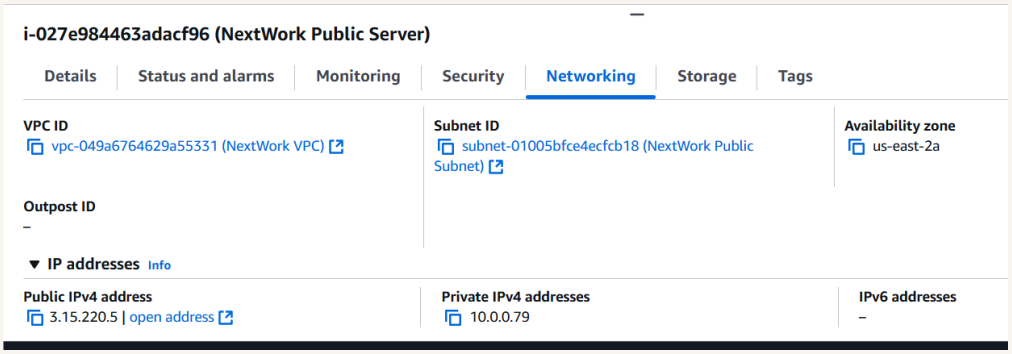
Joba Amunigun
NextWork Student

A private key's file format means the way your private key is saved, similar to how documents can be stored as PDF, DOCX, or TXT — each format working best for certain systems or tools. Not every system recognizes every key format, so choosing the right one is crucial for compatibility and secure access. My private key's file format was .pem, which is what AWS provides by default for connecting to Linux-based EC2 instances via SSH.

Joba Amunigun
NextWork Student

Launching a public server

I had to change my EC2 instance's networking settings by going into the Network settings panel during launch, clicking Edit, and choosing the NextWork VPC from the VPC dropdown list. Instead of launching the instance into the default AWS VPC, I selected the NextWork Public Subnet — to make sure the instance was placed into the right part of my custom network setup. For the firewall settings, I chose “Select existing security group” and applied the NextWork Public Security Group that I had already created for public-facing resources.

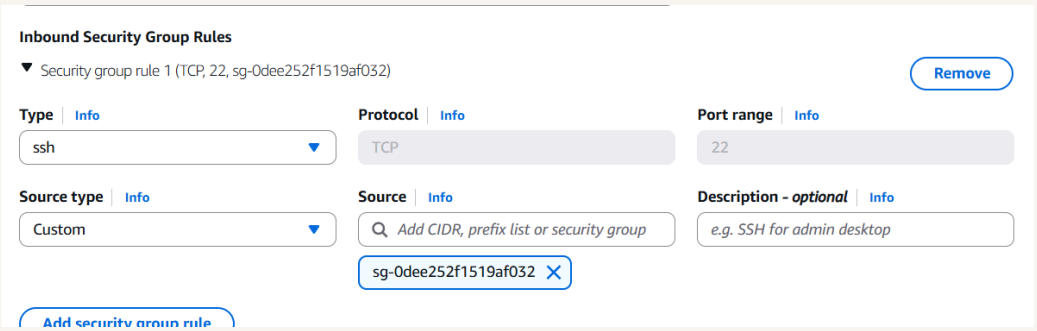


Joba Amunigun
NextWork Student

Launching a private server

My private server has its own dedicated security group because it serves a different purpose and needs stricter access control. While the public server needs to accept traffic from the internet (like HTTP requests), the private server should only accept traffic from trusted sources — such as the public server or internal services within the VPC.

My private server's security group's source is set to the NextWork Public Security Group, which means only resources assigned to that public security group can communicate with my private instance. Instead of allowing access from Anywhere (0.0.0.0/0), I changed the source to a Custom security group — a much safer choice for protecting sensitive resources inside the private subnet.



Joba Amunigun
NextWork Student

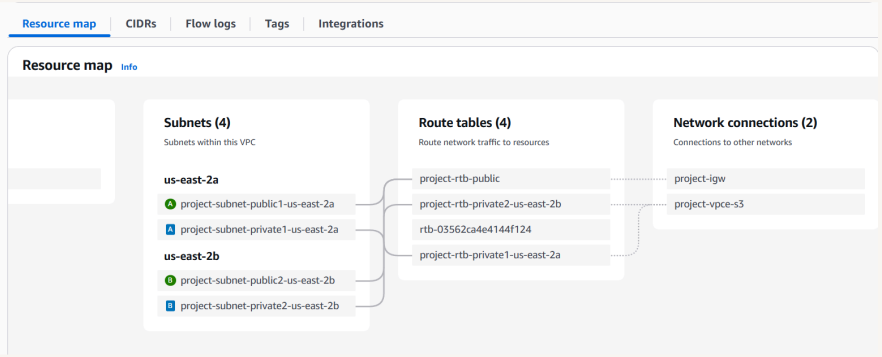
Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I selected the "VPC and more" option — which let me create multiple VPC resources all on the same page using the VPC resource map. I customized the setup by: Choosing 1 Availability Zone Creating 1 public subnet (10.0.0.0/24) and 1 private subnet (10.0.1.0/24) Ensuring no NAT gateway or VPC endpoints were added to keep costs low Reviewing how the resource map automatically updated based on my selections

A VPC resource map is a visual diagram in the AWS Console that shows all the resources being created in your VPC setup — like subnets, route tables, internet gateways, and network connections — in one easy-to-understand flow. It updates in real time as you adjust your VPC configuration, helping you see how everything connects before launching.

My new VPC has a CIDR block of 10.0.0.0/16. It is possible for my new VPC to have the same IPv4 CIDR block as my existing NextWork VPC because each VPC is isolated from the others by default — even if they use the same IP range. Since the VPCs don’t overlap unless explicitly connected (e.g. through VPC peering), AWS treats them as completely separate networks, so duplicate CIDR blocks won’t cause conflicts.

Joba Amunigun
NextWork Student



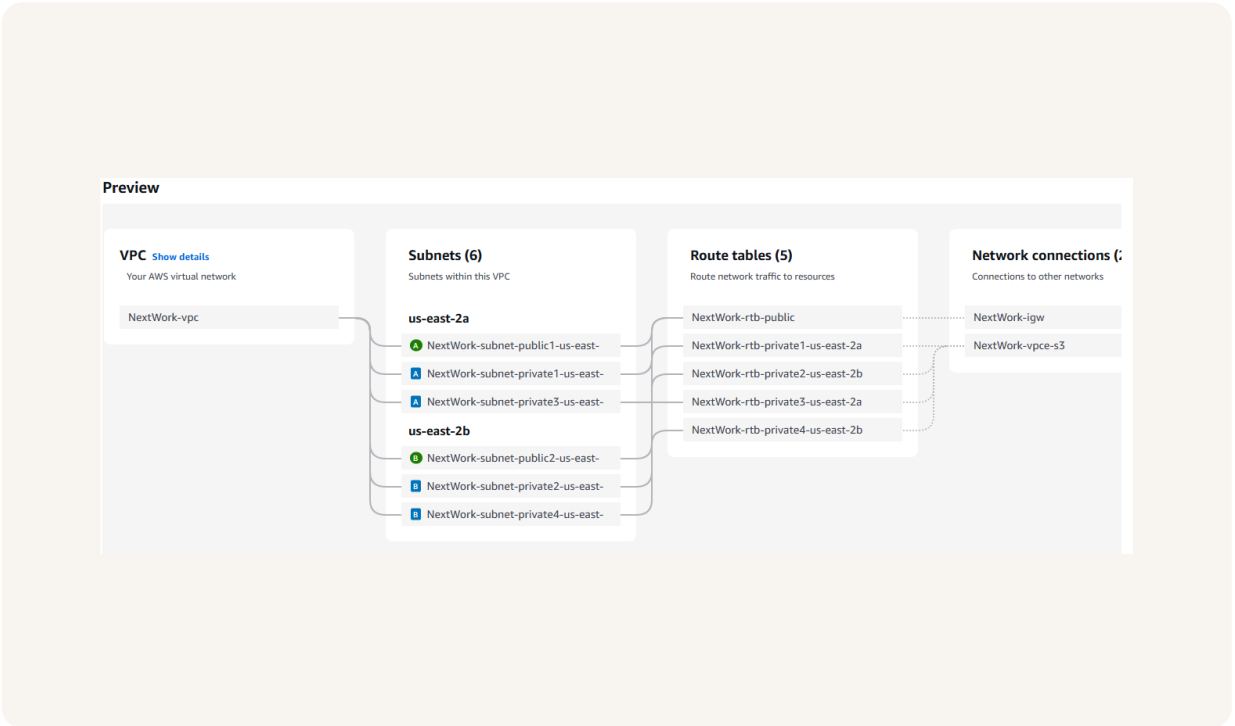
Joba Amunigun
NextWork Student

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: 0 or 2. This was because I selected 2 Availability Zones during setup, and each public subnet must map to a unique AZ to ensure high availability and redundancy.

The setup page also offered to create NAT gateways, which are AWS-managed services that allow private subnets to access the internet for things like software updates — without allowing inbound traffic from the internet. They act as middlemen: resources in private subnets can send requests out (like downloading a patch), and the response comes back — but no one from the outside can initiate a connection back in.



The place to learn & showcase your skills

Check out nextwork.org for more projects