



nextwork.org

Launching VPC Resources

M

Mohammed Dawoud Mota

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. On the left, the 'VPC settings' tab is selected, displaying fields for VPC name ('nextwork'), CIDR block ('10.0.0.0/16'), and tenancy ('Default'). It also shows options for IPv4 and IPv6 CIDR blocks and availability zones ('1 2 3'). On the right, the 'Preview' tab shows a detailed view of the VPC structure. It includes a 'VPC' section with 'Show details' for 'nextwork-vpc', a 'Subnets (6)' section listing 'us-east-1a' and 'us-east-1b' subnets with their respective private and public IP ranges, and a 'Route tables (5)' section listing five route tables connected to the subnets.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private network in the AWS cloud that lets me launch resources in an isolated network and control security routing and connectivity.

How I used Amazon VPC in this project

I used Amazon VPC to create public and private subnets launch EC2 instances in each and control how they communicate with each other and the internet.

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

I didn't expect how quickly the VPC resource map would update and show all connections between subnets route tables and gateways visually.

This project took me...

This project took me 25 minutes.

Setting Up Direct VM Access

It means connecting to my EC2 instance through SSH or RDP so I can control it directly like logging into a computer remotely.

SSH is a key method for directly accessing a VM

SSH means Secure Shell. It is a protocol used to securely connect and communicate with remote servers over a network.

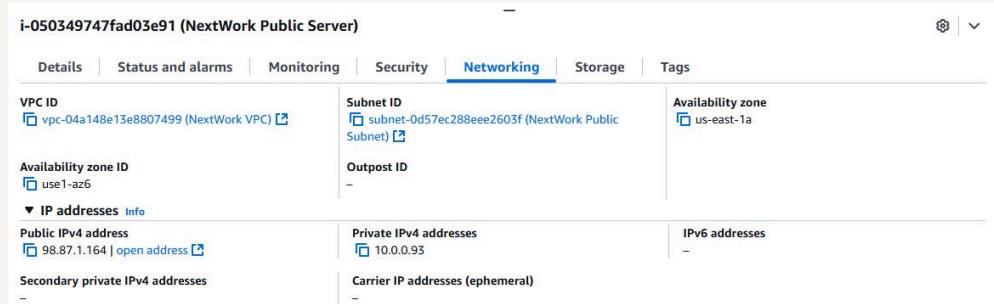
To enable direct access, I set up key pairs

A key pair is a set of security credentials with a public key and a private key that I use to securely connect to my EC2 instance using SSH.

A private key's file format is usually PEM or PPK. My private key was in the PEM format.

Launching a public server

I went to the EC2 console selected my instance then chose Networking and clicked Manage IP Addresses to edit the settings.



Launching a private server

My private server uses a different security group to restrict direct internet access and only allow traffic from the public server for better security.

The new security group's source is the NextWork Public Security Group, allowing only the public server to communicate with the private server.

The screenshot shows the 'Inbound Security Group Rules' section of a network configuration tool. It displays a single rule: 'Security group rule 1 (TCP, 22, sg-042f6045371b77cd2)'. The rule is set to be removed, as indicated by the 'Remove' button. The configuration fields are as follows:

- Type:** ssh
- Protocol:** TCP
- Port range:** 22
- Source type:** Custom
- Source:** sg-042f6045371b77cd2
- Description - optional:** e.g. SSH for admin desktop

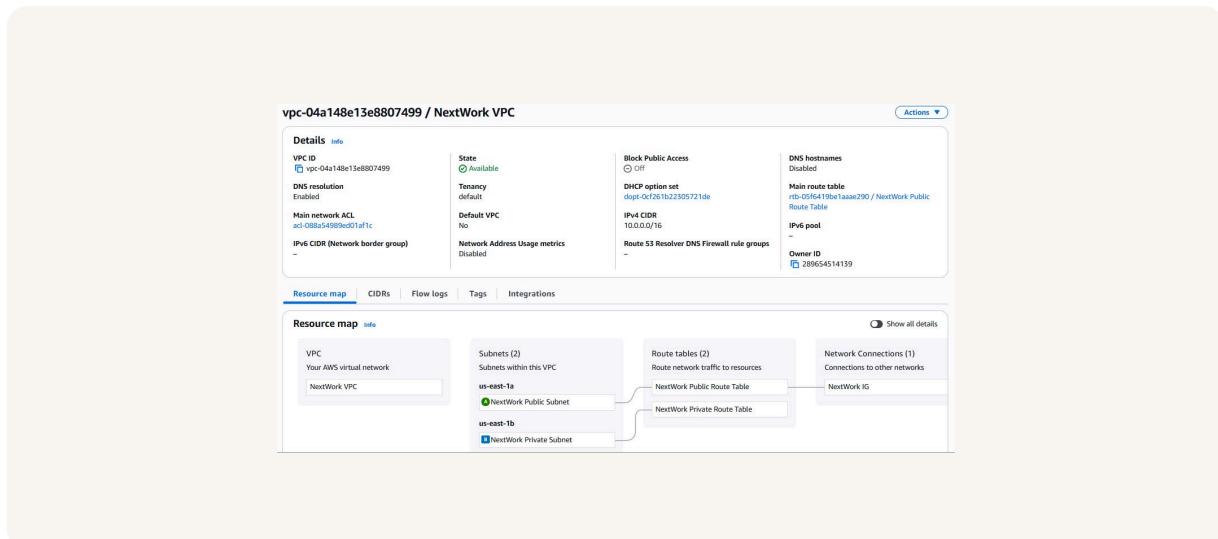
At the bottom, there are buttons for 'Add security group rule' and 'Advanced network configuration'.

Speeding up VPC creation

I used the VPC wizard to create a new VPC with public and private subnets, route tables, an internet gateway, and enabled name tag auto-generation to organize all resources.

A VPC resource map is a visual diagram that shows how all components like subnets route tables and gateways are connected within a VPC.

The new VPC can have the same IPv4 CIDR block because VPCs are isolated networks and do not conflict unless connected through peering.

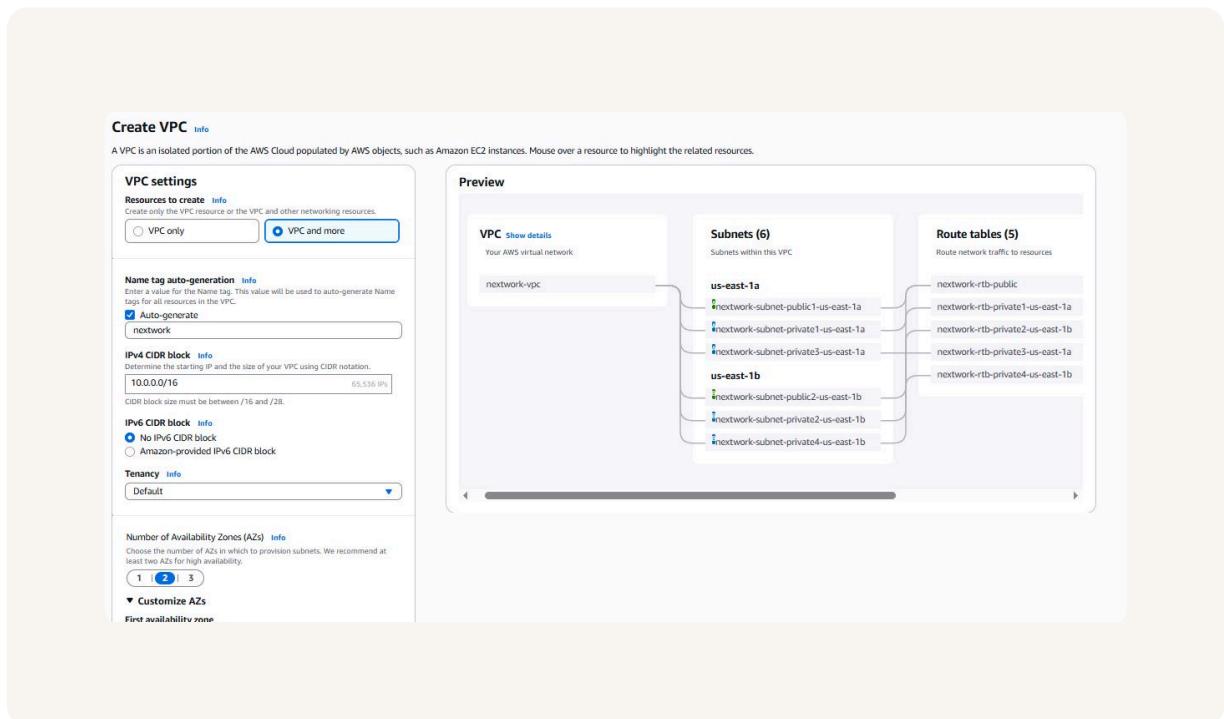


Speeding up VPC creation

Tips for using the VPC resource map

I could create up to two public subnets, one for each availability zone, to maintain redundancy and high availability.

NAT gateways allow instances in private subnets to access the internet for updates while keeping their IP addresses hidden and blocking inbound traffic.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

